Tenable One Cloud Exposure ユーザーガイド

最終更新日: 11月 12, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Tenable One Cloud Exposure へようこそ **84**

ライセンス 84

ライセンスページ 84

クラウド サイバーエクスポージャー ライセンス使 用 状 況 85

リソース別 のライセンス使 用 状 況 データのエクスポート 87

Tenable One プラットフォームのライセンス使 用 状 況 87

ライセンスタイプ 88

Tenable One ライセンス 88

Foundation 88

Advanced 89

CNAPP Complete 89

レガシーライセンス 89

Tenable JIT 89

CIEM 90

Standard 90

Enterprise 90

Cloud Vulnerability Management 91

請 求 対 象 のリソース 91

請 求 対 象 のコンピューティングおよびスキャンベースのリソース 92

JIT リクエスト者の請求対象リソース 99
ライセンスのダウングレード 99
ダウングレードに備える 99
猶予期間 100
ダウングレード後の完了 101
ライセンスのないデータの自動クリーンアップ 101
残りの構成への影響 102
管理者のためのダウングレード後のチェックリスト 102
猶予期間を手動で終了する 103
ライセンスの回収 103
FAQ (よくある質問) 104
脆弱性管理 104
ライセンス別機能比較 105
環境のセットアップ 114
EA とパブリックプレビュー 115
早期公開とは何ですか? 116
パブリックプレビューとは 116
パブリックプレビュー機能の識別方法 116
EA とパブリックプレビューの主な違い 116
FAQ (よくある質問) 117
サポートへの問い合わせ 119

テクニカルサポートでケースをオープンする 119
Tenable Connect への登録 119
Tenable Office Hours 120
Tenable One 120
Tenable One Cloud Exposure の Tenable One への拡張 121
環境サイジングガイド 123
請求対象のリソース 123
AWS 130
前提条件 130
ダウンロード 131
手順 132
Alibaba Cloud 133
前提条件 133
ダウンロード 134
手順 134
Azure 135
前提条件 135
ダウンロード 136
手順 136
GCP 137
前提条件 137

ダウンロード 138
手順 138
OCI 139
前提条件 139
ダウンロード 139
手順 139
Snowflake 140
前提条件 141
ダウンロード 141
手順 141
ほかのリソース 141
コンソール(UIを使用) **143**
概要 143
コンソールの操作 143
左側のナビゲーションメニュー 143
コンソールのフォーカスを選択します 144
製品内ヘルプ 146
ヘルプツール 147
ユーザープロファイル 148
コンソール全体の検索 149
リソースプロファイルの概要ビュー 150

リスク深刻度の色分け 152
Hexa AI 154
Hexa AI を使用する理由 154
Hexa AI の設定 155
Hexa AIにアクセスする 155
会話にファイルを追加する 155
コアアビリティ 156
一般的なユースケース 157
高度なユースケース 158
MCP サーバーを介した Hexa AI 163
始める前に 164
MCP サーバーに接続する 164
Claude Desktop 165
トラブルシューティング 166
Claude Code 168
Cursor 168
VS Code/GitHub Copilot 169
その他の MCP クライアント 171
信頼、安全性、ガバナンス 171
データのフィルタリング 172
テーブル内のデータのフィルタリング 172

アカウント範囲によるデータのフィルタリング 174
ダッシュボード 175
ダッシュボードを管理する 175
ダッシュボードの範囲と可視性 176
すべてのダッシュボードを表示する 177
カスタムダッシュボードを作成する 178
フィルター付きウィジェットで的を絞ったダッシュボードを作成 179
高度なフィルターを使用する 179
ダッシュボードの複製 180
レポートの作成 181
ダッシュボードの編集 183
ウィジェット 184
クエリ 184
コンプライアンス 185
データ 186
検出結果 186
IaC 190
IAM 190
インベントリ 193
脅威 193
ワークロード 194

危険な組み合わせ 194
危険な組み合わせとは 195
重大な脆弱性と高い権限を持つパブリックワークロード 196
パブリックデータリソースと機密データ 196
外部プリンシパルと高い権限 197
パブリック関数と高い権限 197
危険な組み合わせのリスト 198
調査 199
エクスプローラー 199
保存されたクエリ 199
新規クエリを作成する 200
オブジェクトの選択 201
ネイティブオブジェクトと汎用オブジェクト 201
結果のフィルタリング 202
オブジェクトプロパティでフィルター 202
エンティティ特性でフィルタリング 203
空白値のクエリプロパティ 203
未加工のクラウドプロバイダーソースデータでフィルタリング 203
複数のオブジェクト プロパティでフィルター 205
関係でフィルター 206
クエリグループの非表示 / 表示 206

フィルターと演算子の組み合わせ 207
関係を追加する 208
リレーションシップフィルターの使用 209
結合を作成する 209
[グループ化] を使用した結果の集計 210
クエリの保存 211
クエリウィジェット 212
クエリを編集する 212
クエリからのカスタムポリシーの作成 213
サポートされているオブジェクト 214
クエリデータからのレポートの作成 215
クエリからの検出結果の自動化の作成 216
クエリデータのエクスポート 218
クエリ結果を表示する 219
テーブルビュー 219
グラフビュー 219
サンプルクエリ 220
コンプライアンス基準に違反する検出結果のクエリ 220
一般向け仮想マシンのクエリ 221
非アクティブな所有者を持つリソースのクエリ 222
参照: 検出結果のプロパティ 223

FAQ (よくある質問) 224
クエリ 225
クエリテーブル 225
Explorer でクエリを開く 226
クエリのモニタリング 227
クエリウィジェット 227
クエリの複製 227
カスタムクエリの削除 228
インベントリ 228
資産インベントリの表示 228
資産インベントリのフィルタリング 230
スケジュールされたレポートの作成 232
インベントリデータのエクスポート 233
インベントリ全体を検索する 234
一般的なインベントリユースケース 235
パブリックリソースを検出する 235
データを保護する暗号化キーの検索 238
インベントリ内のリスクを検出する 239
リソースの詳細の表示 240
クラウドコンソールでリソースを表示する 240
機密度の高いリソースをマークする 240

ラベルのリソースへの適用 241
リソースに関する詳細の取得 242
リソースの関係を確認する 243
関連するリスクの表示と管理 244
センシティブデータの表示 244
ネットワークデータの表示 244
ネットワークエクスポージャーの視覚化 (グラフ) 245
ネットワークエンドポイント 246
ネットワークスキャンステータス 247
サポートされているリソース 247
リソースアクティビティの調査 249
設定スナップショット 249
リソースのソースコードの表示 249
対応リソース 250
コンピュート 279
仮想マシン 279
すべての仮想マシンを表示する 280
オンデマンドスキャンの実行 280
仮想マシンの列データ 281
脆弱性のスキャンステータス 284
AWS Marketplace AMI から起動された EC2 インスタンス 288

アカウント内スキャン 288
仮想マシンイメージ 289
すべての仮想マシンイメージを表示する 289
オンデマンドスキャンの実行 290
仮想マシンイメージの列データ 291
脆弱性のスキャンステータス 294
コンテナイメージ 296
すべてのコンテナイメージを表示する 296
オンデマンドスキャンの実行 297
コンテナイメージの列データ 299
Kubernetesクラスター 302
クイックリンク 302
クラスターの表示 303
クラスターを管理する 303
Helm をアップグレードするまたは新機能をインストールする 304
Tenable からクラスターを切断する 304
クラスターを別のアカウントに移動する 304
追加機能でクラスターをアップグレードする 305
クラスター列データ 305
リソース同期ステータス 307
オンプレミスクラスターの脆弱性管理ステータス 308

クラスターステータス 309
ソフトウェア 309
すべてのソフトウェアパッケージを表示する 310
ソフトウェアパッケージの列データ 310
特定のワークロードのソフトウェアパッケージを表示する 311
IAM 312
概要 312
最小権限ポリシーの生成とロール 312
AWS: 最小権限ポリシーの生成 313
AWS リソース粒度 316
リソース粒度でサポートされているリソース 316
ユーザーまたはサービスアイデンティティの最小権限カスタムロールの生成 317
GCP および Microsoft Entra ID グループの最小権限カスタムロールの生成 318
サポートされているリソース 319
重複するロールの割り当てまたはバインディングを監視する 320
アクセス許可マッピングの視覚化 321
過剰または使用されたアクセス許可 322
監査されないアクセス許可 323
マップレイアウトと例 323
マップの操作と使用 324
アクセス許可を付与するメカニズム 328

アイデンティティインテリジェンス 328
環境内のアイデンティティを表示する 328
ID 列データ 330
アクセス許可クエリ 332
アクセス許可クエリの実行 333
アクセス許可クエリのテーブルのフィールド 335
AWS フェデレーションのアクセス許可 338
AWS フェデレーションアクセス許可列データ 339
ネットワークエンドポイント 340
ネットワークエンドポイントの確認 341
データリソース 343
すべてのデータリソースを表示する 343
データインベントリの列データ 345
データスキャンステータス 347
リソースとデータベースの詳細 349
データの概要 349
分類されたデータ 350
オンデマンドスキャンの実行 351
感度レベル 352
Events 353
イベント 353

イベントタイプ 354
イベントを表示 354
イベントデータのエクスポート 355
クラウドイベント 355
クラウドイベントの列データ 356
ランタイムイベント 357
ランタイムイベントの列データ 357
ランタイムファイルオープンイベントの列データ 358
ランタイムプロセス実行イベントの列データ 360
Kubernetes アドミッションコントローラーイベント 361
アドミッションコントローラーイベントの列データ 362
リスク 363
クラウドの検出結果 363
検出結果ページの操作 363
検出結果データのエクスポート 367
定期レポートの作成 368
検出結果を無視する 368
検出結果を無視しない 372
検出結果を手動でクローズする 372
検出結果を再オープンする 373
検出結果に基づくアクションのトリガー 374

1 つの検出結果に対してアクションをトリガーする 374
複数の検出結果に対するアクションのトリガー 376
Jira および ServiceNow チケットを追跡する 378
検出結果の詳細の表示 379
検出結果からシークレットを除外する 380
除外されたシークレットの表示と管理 381
ソースコードの表示 382
検出結果のアクティビティの表示 383
検出結果の修正 384
検出結果を手動で修正する 384
検出結果の自動修正 386
ワンタイム認証情報による修正 388
IaC を使用した検出結果の修正 388
コード変更の確認 389
プルリクエストを使用して検出結果を修正する 390
サポートされているポリシー 391
参照: データの検出 392
リソース削除の推奨事項を伴う検出結果 392
自動解決されない検出結果タイプ 393
削除された検出結果 393
OTC による修正のサポート対象の検出結果 394

IaC 検出結果 396
検出結果ライフサイクルの例 397
IaC 検出結果ページの操作 398
IaC 検出結果のステータス 400
未解決の検出結果 401
無視した検出結果 401
解決済みの検出結果 402
IaC 検出結果の管理 403
検出結果の詳細の表示 404
検出結果の例 404
検出結果を手動でクローズする 405
検出結果を再オープンする 406
検出結果データのエクスポート 406
定期レポートの作成 407
検出結果のアクティビティの表示 408
削除された検出結果 408
過剰なアクセス許可 409
過剰なアクセス許可を持つアイデンティティの表示 410
アイデンティティの列データ 411
脅威検出 413
脅威検出を表示する 413

脅威検出の列データ 413
脅威検出の詳細を表示する 414
脅威ストーリー 415
脅威事例を表示する 415
脅威事例の列データ 416
脅威事例の詳細を表示する 417
脆弱性 417
すべての脆弱性を表示する 418
脆弱性ページのソート順序 418
脆弱性の列データ 419
脆弱性の詳細の表示 422
脆弱性スライド式パネル 423
悪用される可能性 426
タイムラインイベント 428
プラグイン 429
プラグインの詳細を表示 429
プラグインメタデータ 430
プラグインの脆弱性 431
プラグインの悪用可能性 434
プラグインの脆弱性 435
脆弱性データのエクスポート 436

特定のワークロードの脆弱性を表示する 436
脆弱性関連の検出結果 437
脆弱性の検出結果を表示およびドリルダウンする 437
検出結果の脆弱性の列データ 438
サポートケース用のリソースインベントリデータのエクスポート 439
FAQ (よくある質問) 440
Vulnerability Priority Rating (VPR) に対する理解 440
VPR の仕組み 441
VPR と他のリスクスコアリング手法の比較 442
悪意のあるファイル 443
サポートされているファイルタイプ 443
悪意のあるファイルの表示 445
悪意のあるファイルの列データ 446
悪意のあるファイルの詳細 447
コード CI/CD 448
はじめに 449
ローカルでスキャンを実行する 450
組織階層 452
スキャン結果を表示する 453
コードスキャンの列データ 456
スキャン結果の列データ 458

IaC CI/CD スキャン結果のエクスポート 459
コンテナイメージ CI/CD 460
コンテナイメージ CI/CD スキャンの列データ 460
スキャン結果を表示する 462
概要データ 462
脆弱性の列データ 463
ソフトウェアの列データ 464
JSON 出力の例 464
ポリシー 467
クラウドポリシー 467
ポリシーを管理する 467
ポリシーの列データ 470
ポリシーの有効化と無効化 471
検出結果作成を遅延させる 472
評価期間とパスワード要件を変更する 474
サポートされているポリシー 475
無効なアイデンティティの検出結果の作成 480
サポートされているポリシー 481
招待保留中の Microsoft Entra ID ゲストユーザーの検出結果を作成する 482
アクセス許可使用状況の学習期間を変更する 483
グループから非アクティブなプリンシパルを削除することが推奨されます 483

サポートされているポリシー 485
メンバーアカウントのルートユーザーの検出結果を作成する 486
ポリシーからリソースを除外する 487
ポリシーからシークレットを除外する 487
パブリック Lambda 関数ポリシーからの API ゲートウェイパスの除外 489
ポリシーデータのエクスポート 490
Azure で非アクティブなシステムマネージド ID の検出結果を作成する 490
削除できるシステムマネージド ID 490
ポリシーカテゴリ 492
クラウドポリシー: カスタム 493
カスタムポリシーの追加 493
カスタム Rego ポリシー (早期アクセス) 496
ポリシー評価 497
ヘルパー関数 498
カスタムポリシーテンプレート 499
IaC ポリシー 506
ポリシーの管理 507
IaC ポリシーの列データ 508
IaC ポリシーの有効化と無効化 509
IaC スキャンで除外を設定する 511
IaC ポリシーデータのエクスポート 513

アドミッションコントローラーポリシー 513
アドミッションコントローラーポリシーの設定 515
アドミッションコントローラーポリシーリスト 516
脆弱なコンテナイメージ 526
前提条件 527
脆弱なコンテナイメージの仕組み 527
脆弱なコンテナイメージの有効化 528
脆弱性のあるコンテナイメージの設定 529
ポリシーの列データ 530
脅威検出ルール 531
脅威ルールを表示する 531
脅威ルールの列データ 532
除外 532
除外ライフサイクル 533
検出結果と今後の検出結果の特定 535
除外を定義する 536
範囲 538
アクション 539
除外を作成する 540
除外の管理 544
[除外] ページに表示される内容 544

除外ステータス 545
既存の除外に追加するためのルール 546
競合の解決 547
業務 548
自動化 548
サードパーティツールにリスクデータを送信 549
サードパーティツールへの監査データの送信 553
自動化を有効または無効にする 555
既存の自動化の複製 556
レポート 557
レポート 557
レポートの作成 557
既存のレポートを複製する 559
レポートタイプ 559
スケジュールされたレポートを表示および編集する 563
履歴レポートへのアクセス 563
その他のデータエクスポート方法 564
コンプライアンス 564
コンプライアンス基準を表示する 565
標準での結果を表示する 565
コンプライアンス評価を表示する 567

標準を有効または無効にする 568
標準をエクスポートする 568
コンプライアンス態勢の改善 569
カスタム標準の追加 570
標準の複製 571
参照: コンプライアンスデータ 572
規格一覧 572
コンプライアンステーブルデータ 577
スライド式パネルのデータ 578
設定 579
アクセス管理 579
ユーザーとグループ 579
新しいユーザーの追加 580
新しいグループを追加する 583
継承されたユーザー 586
組み込みのロールとアクセス許可 587
ロール 592
一般的なユースケース 593
カスタムロールの作成 594
カスタムロールの編集 594
ロールを複製する 595

カスタムロールの削除 595
利用可能なアクセス許可 596
アクセス許可の依存関係 599
サービスアカウント 599
セカンダリシークレットローテーション 600
サービスアカウントを表示する 600
サービスアカウントの作成 601
シークレットを作成する 602
シークレットを削除する 602
ロールの割り当てを追加する 603
サービスアカウントを編集する 603
サービスアカウントを削除する 604
サービスアカウントの詳細の表示 604
監査ログ 605
シングルサインオン 605
Tenable One経由でのログインを有効にする 606
AWS Identity Center 経由でのログインの有効化 (SAML 2.0) 606
Google 経由でのログインを有効化 609
OIDC を使用した Google 経由でのログインの有効化 609
SAML を使用した Google 経由でのログインの有効化 609
Google グループのサポートを追加する 611

Microsoft Entra ID 経由でのログインの有効化 611
OIDC を使用した Microsoft Entra ID 経由でのログインの有効化 611
SAML を使用した Microsoft Entra ID 経由でのログインの有効化 613
Microsoft Entra ID グループのサポートの追加 615
OIDC を使用した Microsoft Entra ID グループのサポートの追加 616
SAML を使用して Microsoft Entra ID グループのサポートを追加する 616
Okta 経由でのログインの有効化 617
Okta グループのサポートの追加 618
OneLogin 経由でのログインを有効にする 619
OneLogin ロールのサポートの追加 621
Ping Identity 経由でのログインの有効化 622
Ping Identity グループのサポートの追加 624
JumpCloud 経由でのログインの有効化 624
JumpCloud グループのサポートの追加 626
カスタム SAML 2.0 プロバイダー経由でのログインの有効化 627
グループのサポートの追加 629
コンソールのタイムアウト設定 629
非アクティブタイムアウト 629
セッションタイムアウト 630
組織 630
プロジェクト 630

プロジェクトを作成できるユーザー 630
サポートされている機能 631
プロジェクトフォルダーを追加する 632
プロジェクトを追加する 632
プロジェクトスコープへのアクセスを付与する 635
プロジェクトを移動する 636
プロジェクトの削除 637
コンソールデータをプロジェクトでフィルタリングする 637
プロジェクトの表示 639
プロジェクトデータのエクスポート 639
アカウント 640
アカウントを管理する 640
アカウントの列データ 641
コードアカウントを管理する 641
アカウントの詳細の表示 642
アカウントの管理のオプション 643
オンボーディングの問題のトラブルシューティング 644
アカウントステータス 644
コード 645
フォルダーを追加して移動する 647
管理オプション 648

コードリポジトリのステータス 650
セキュリティ 652
データ 652
バケットスキャン 653
バケットのスキャン範囲の設定 653
プライベートバケットのスキャン範囲の設定 654
Azure Storage アカウントのプライベートネットワークアクセスの設定 654
データベース 655
マネージドデータベースのスキャン範囲の設定 656
データプラットフォーム 656
データプラットフォームのスキャン範囲の設定 657
スキャンの除外 657
データスキャンの除外の表示と管理 658
データスキャンの除外ステータス 658
データスキャンの除外を作成する 659
分類の除外 660
分類除外の作成 660
分類の除外を管理する 661
データタイプ 662
カスタムデータ型の作成 663
データ型を編集する 664

デフォルト分類の復元 (ビルトインデータタイプ) 665
カスタムデータタイプの削除 665
IaC 666
スキャン失敗しきい値の設定 666
IAM 667
アクセス許可使用のラーニング期間 667
影響を受けるポリシー 670
Microsoft Entra ID 特権ロール 672
ネットワーク 674
内部 IP アドレス 674
ネットワークスキャナー 674
ベンダー 675
ベンダーの管理 675
新しいベンダーの追加 676
ベンダーを編集する 676
ベンダーを削除する 676
信頼できるベンダー 677
コンソール全体でのベンダーの可視性 678
ベンダーテーブルの列 679
ワークロード 680
仮想マシンの設定 680

仮想マシンスキャンからアカウントを除外する 681
仮想マシンデータスキャンの有効化 681
仮想マシンのデータディスクスキャンを有効にする 682
スキャンから仮想マシンを除外する 683
仮想マシンをポリシーから除外する 683
仮想マシンディスクの最大サイズ 684
仮想マシンイメージ 684
仮想マシンイメージスキャンからアカウントを除外する 684
仮想マシンイメージデータスキャンの有効化 685
仮想マシンイメージをスキャンから除外する 686
仮想マシンイメージをポリシーから除外する 686
仮想マシンイメージディスクの最大サイズ 687
コンテナレジストリの設定 687
コンテナレジストリの脆弱性スキャンを Tenable で有効化する 687
コンテナイメージの最大サイズ 688
スキャンの除外 688
スキャンの除外の表示と管理 688
スキャンの除外ステータス 689
スキャンの除外を作成する 689
脆弱性設定 690
脆弱性の深刻度のメトリクス 690

検出結果の最小脆弱性深刻度 691
修正なしの脆弱性の検出結果 692
終末期の設定 692
オペレーティングシステムのサポート終了検出結果のしきい値 692
Malicious File Settings 693
スキャンからアカウントを除外する 693
信頼できるファイルを追加する 694
秘密 694
シークレットマスキング 695
統合 695
統合の詳細を表示する 696
統合テーブル 696
新しい統合を追加する 697
監査 698
インベントリ(プロパティとラベル) 699
カスタムプロパティを管理する 700
リソース所有者 701
カスタムプロパティの継承 703
カスタムプロパティの追加 703
コンソールでカスタムプロパティを表示する 704
インベントリのカスタムプロパティの編集 706

ラベルを管理する 707
ラベルを追加する 709
ラベルを編集する 710
組み込みシステムラベル 711
コアコンセプト 714
概要 714
アイデンティティ第一のクラウドネイティブアプリケーション保護 714
アーキテクチャとデータ処理 715
プラットフォームのコンポーネント 718
サービス 718
コンソール 718
公開 API 718
環境の分析方法 719
データの同期と更新の頻度 720
データ保持期間と学習期間 720
データ保持 720
過剰なアクセス許可 721
アクティビティログと異常な動作 722
許可が必要な Tenable IP アドレス 722
クラウドサイバーエクスポージャーのコアサービス用 IP アドレス 722
ワークロード保護用とデータ保護用の追加 IP アドレス 725

AWS: 追加 IP アドレス 725
Azure: 追加 IP アドレス 727
GCP: 追加 IP アドレス 730
OCI: 追加 IP アドレス 732
Alibaba Cloud: 追加の IP アドレス 733
許可が必要な Tenable アカウント ID 734
製品のセキュリティとプライバシー 735
ホストリージョン 735
Tenable コンソール URL 736
データ分離 736
データ暗号化 736
高可用性と障害復旧 736
コンプライアンスと認証 737
年次ペネトレーションテスト 737
キー管理 737
認証 737
パスワードポリシー 738
タイムアウト設定 738
スキャン方法 738
用語 739
環境別のスキャン方法 740

クラウドのスキャン方法 742
エージェントレスのリソース同期 743
エージェントレスのワークロードスキャン 743
エージェントレスのデータスキャン 744
アカウント内スキャン (ワークロードとデータ) 745
コードのスキャン方法 745
エージェントレスのコードスキャン 746
CI/CD スキャン (IaC と脆弱性) 746
クラウド、アンマネージド、オンプレミスの Kubernetes スキャン方法 747
エージェントベースの Kubernetes ワークロードスキャン 747
アカウント階層とフォルダー 748
フォルダー構造を自動的に更新 751
高度なユースケースの例 751
よくある質問 752
アカウントフォルダーの作成 752
アカウントの範囲 754
アカウント範囲によるコンソールデータのフィルタリングおよび機能の設定 755
サポートされている機能 757
アカウントの継承 757
プロジェクトの仕組み 757
プロジェクトの仕組み 758

プロジェクトを使用するタイミング 759
プロジェクトの一般的なユースケース 759
製品グループのプロジェクトの作成 760
ビジネス機能用のプロジェクトの作成 760
開発アカウントと本番アカウント用のプロジェクトを作成する 761
アプリケーションおよびサービス境界用のプロジェクトを作成する (Azure) 763
サポートされている機能 764
プロジェクトのアクセス許可と機能 765
プロジェクトのアクセス許可 765
伝播 765
有効なアクセス許可 766
検出結果のライフサイクル 766
検出結果ライフサイクルの例 766
検出結果のステータス 767
未解決の検出結果 768
無視した検出結果 769
解決済みの検出結果 770
コンプライアンスの仕組み 771
ベンチマークガイドラインとポリシーマッピング 771
CIS ベンチマーク 772
手動と自動化された推奨事項 772

コンプライアンススコアを理解する 773
例: コンプライアンススコアの計算 774
検出結果の深刻度 778
動的な深刻度と静的な重大度 779
IAM 検出結果の深刻度 779
AWS 780
アクセス許可の深刻度 780
検出結果タイプごとの AWS の深刻度 781
ユーザーとグループ 781
ロール 781
SSO アクセス許可セット 782
未使用のアクセス許可セットが割り当てられた SSO ユーザーおよびグループ 783
Azure 785
アクセス許可の深刻度 785
Azure 検出結果の深刻度 785
GCP 786
アクセス許可の深刻度 787
GCPの所見の重大度 788
IAM 788
アクセスレベル 789
AWS アクセスレベル 790

Azure アクセスレベル 791
GCP アクセスレベル 792
アクセスレベル機能 793
アクセスレベルフィルター 794
アクセス許可カテゴリ別のアクセスレベル 794
[アクセスレベル] 列 795
過剰なアクセス許可と非アクティブな ID 795
過剰なアクセス許可の定義 796
非アクティブなアイデンティティの定義 796
未使用ロールの定義 797
権限が過剰なアイデンティおよび非アクティブなアイデンティティの作成を検出する 798
アクセス許可の分析とリスクレベル 798
アクセス許可カテゴリ 799
アクセス許可カテゴリリスクレベル 800
FAQ - IAM ガバナンス 801
Tenable での権限のない Microsoft Entra ID グループの検出方法 802
「グラフが大きすぎます」という動作を理解する 802
権限の過剰なアイデンティ検出結果でのアクセス許可の違いを理解する 803
ワークロード保護 804
エージェントレススキャンとエージェントベーススキャンの比較 805
エージェントレススキャン 805

エージェントベースのスキャン 806
エージェントレスワークロードスキャン 807
エージェントレスのワークロードスキャンについて 807
サポートされていないリージョン 809
暗号化されたリソースのサポート 810
サポートされている Azure ディスク暗号化方式 811
Azure の必要なアクセス許可 811
セキュリティとコンプライアンス 812
BitLocker ディスクのデータアクセス認証 812
Azure Policy 設定 812
非ルートボリュームスキャン 813
部分的なスキャンステータス 813
非ルートボリュームスキャンの無効化 813
スキャンのワークフロー図 813
AWS 814
Azure 814
GCP 815
OCI 815
Tenable の検出対象 816
スキャンで使用されるポリシー 817
Tenable がソフトウェアと脆弱性を特定する方法 817

データソースの選択 818
CVSS 深刻度の基本値 818
Linux 819
Linux OS のバージョン 819
Linux 対応言語 821
Linux でサポートされるファイルシステム 822
Windows 822
Windows OS のバージョン 822
Windows でのファーストパーティとサードパーティのアプリ 823
エージェントベースの Kubernetes ワークロードスキャン 825
エージェントベースの Kubernetes ワークロードスキャンについて 826
スキャンのワークフロー図 827
Tenable によるスキャナーの更新方法 828
Tenable の検出対象 828
スキャンで使用されるポリシー 830
Tenable がソフトウェアと脆弱性を特定する方法 830
データソースの選択 831
CVSS 深刻度の基本値 831
Linux 832
Linux OS のバージョン 832
Linux 対応言語 834

Linux でサポートされるファイルシステム 835
コンテナイメージスキャン 835
コンテナイメージレジストリスキャン 836
コンテナレジストリポリシー 838
スナップショットスキャン費用計算ツール 838
ワークロード保護 (アカウント内スキャン) 839
Tenable の検出内容 839
AWS アーキテクチャのサンプル 841
サンプル Azure アーキテクチャ 841
GCP のサンプルアーキテクチャ 842
サンプル OCI アーキテクチャ 842
よくある質問: 脆弱性管理 843
仮想マシンのスキャン 843
停止された VM の検出結果の深刻度 843
スキャンされた VM ボリューム 844
対応 OS バージョン 845
スキャン頻度 845
スキャン時間 845
スキャン結果の高速化 846
データ転送ポリシー質問: 自分のデータがアカウント外に出ることはありますか? 846
ワークロードへの影響 847

スナップショットの削除 847
月次スキャンコスト 847
プラグインとCVEの脆弱性深刻度メトリクスの選択方法 847
解決済みの脆弱性情報 848
検出結果におけるOSサポート終了 848
パッチ未適用のOS検出結果基準 849
修正データ 849
仮想マシンイメージスキャン (AMI) 849
AMIスキャンの範囲とカバレッジ 850
コンテナイメージ CI/CD のスキャン 850
CI/CD スキャンモード 850
CI/CD データ保持 850
Docker-in-Docker (DinD) 850
コンテナイメージサイズの制限 851
サードパーティの脆弱性の不一致 851
データの不一致を引き起こす期限切れのレジストリ認証情報 851
Windows イメージのサポート 852
コンテナイメージレジストリのスキャン 853
スキャン頻度 853
Docker-in-Docker (DinD) 853
レジストリイメージの脆弱性更新頻度 854

サポートされているコンテナイメージアーキテクチャ 854
Amazon ECS の AWS Fargate サポート 854
Windows イメージのサポート 855
コンテナイメージアカウントの割り当て 855
オンプレミス Kubernetes ワークロードスキャン 857
センサーのアクセス許可 857
センサースキャン頻度 857
エフェメラルディスクを使用した AKS クラスタのスキャン 857
CoreOS サポート 857
ディスクストレージ要件 858
ロジックとトリガーのスキャン 858
スキャン結果の可視性 858
スキャン結果の可視性 858
アカウント内ワークロードスキャン 858
アカウント内オンボーディング: カスタマーマネージドキー (CMK) 858
アカウント内オンボーディング: 顧客管理対象イメージ 859
アカウント内オンボーディング: 顧客管理ネットワーク 859
地域リソースプロビジョニング 859
オンプレミスと AWS Outpost の互換性 860
ネットワーク 860
ネットワークのエクスポージャー 861

ネットワーク評価 862
ネットワーク評価の範囲と制限 863
ネットワークスキャナー 863
検出結果の深刻度への影響 864
サポートされているリソース 865
ネットワークエンドポイント 867
ネットワークエンドポイントの作成方法 867
ポートスキャンロジック 868
共通サービスポート 868
FAQ: ネットワーク 872
ネットワークスキャナーの有効化 872
ネットワーク評価とネットワークスキャナー 872
ネットワークエンドポイント 873
ポートとプロトコル 874
サポートされているリソースとオリジン IP 874
対象範囲と制限 875
検出結果 875
データ保護 876
Tenable によるデータのスキャン方法 876
サポートされているリソースとスキャンのアプローチ 877
サポートされている AWS RDS クラスタ (Aurora) データベースエンジンのバージョン 878

サポートされている AWS RDS インスタンスのデータベースエンジンバージョン 879
サポートされている AWS S3 バケットストレージクラス 879
サポートされている Azure SQL 層 879
サポートされている GCP BigQuery データセット 880
サポートされている GCP SQL インスタンスのデータベースエンジンバージョン 880
サポートされている OCI オブジェクトストレージバケット 880
サポートされている Snowflake テーブル 881
サポートされているAlibaba Cloud OSSバケットストレージクラス 881
スキャンのアプローチ 881
直接スキャン 881
間接スキャン 882
ワークロードベースのスキャン (仮想マシンと仮想マシンイメージ) 883
セキュリティとプライバシー 884
Tenable が検出するデータ 885
Tenable が検出するデータ 885
スキャン対象ファイル形式 886
スキャン対象データタイプ 887
スキャン対象データタイプ: 運転免許証 891
スキャン対象データタイプ: 国民 ID 894
スキャン対象データタイプ: 納税者番号 895
スキャン対象データタイプ: 社会保障番号 896

スキャン対象データタイプ: シークレット 896
分類の除外 896
除外の例 897
分類除外の仕組み 897
分類の除外とスキャンの除外の比較 898
詳細はこちら 898
秘密のデータ型 899
データスキャンコスト 939
直接スキャンの推定コスト 939
間接スキャンの推定コスト 939
クラウドプロバイダーおよびサービス別のコスト 940
ワークロードベースのスキャンの推定コスト 940
データリソースのアカウント内スキャン 940
アカウント内直接スキャン 941
間接アカウント内スキャン 942
よくある質問 - データ保護 943
対象プラットフォーム/環境 943
スキャンされるリソースタイプ 943
スキャンされたファイル形式 943
スキャンされるデータタイプ 944
データスキャン頻度 944

スキャン後の請求が無効になっている 944
データストレージポリシー 945
検出されたデータの表示 945
正規表現とデータ分類 945
データ保護のアクセス許可 946
暗号化されたデータベースのスキャン 948
スキャンステータスのトラブルシューティング 948
テストデータとシンセティックデータ 949
定期スキャンとメンテナンス 950
データベースの範囲と検出 950
アーキテクチャと地域の挙動 951
データ境界と監視データのスプロール 951
ライセンス 952
仮想マシンのデータスキャン 953
脅威検出 954
モニタリング方法 954
分析と検出 955
Tenable による環境内の脅威の監視方法 955
サポートされている範囲 955
要件 956
クラウドアカウント 957

Kubernetes クラスタ 957
モニタリング方法 957
エージェントレス 957
ランタイム検出 (eBPF センサーベース) 958
セキュリティとプライバシー 958
最低限必要なアクセス許可 958
データの分離と常駐 958
データの暗号化と安全な通信 959
Tenable が検出する脅威 959
脅威検出タイプ 959
脅威検出ファミリー 960
不審なアクティビティ 960
異常検出 960
異常カテゴリ 961
異常検出ポリシー 961
学習期間 962
異常検出結果の管理 962
マルウェアの実行 962
脅威の検出 MITRE ATT&CK マッピング 963
脅威ストーリー 963
脅威事例の概要 963

脅威ストーリー生成ロジック 964
FAQ: 脅威の検出と脅威事例 964
脅威検出 964
ライセンスと請求 964
アカウント内スキャン 965
近リアルタイム(NRT)検出 965
データ保持 965
学習期間 966
カスタム検出ルール 966
修正 966
API サポート 967
脅威ストーリー 967
脅威ストーリーと脅威検出の違い 967
イベントの相関 967
調査ワークフロー 967
ステータスの追跡 968
Kubernetes 968
クイックリンク 968
コアの可視性と分析 969
Helm チャートによるリソースの同期方法 970
ネットワークアクセス 970

アイデンティティアクセス 971
Kubernetesランタイムの検出 971
Kubernetes アドミッションコントローラー 972
Kubernetes 脆弱性スキャン 973
ライセンス要件 973
アドミッションコントローラーの概要 973
アドミッション制御のユースケース: 非 root ユーザー権限の強制 975
よくある質問 - Kubernetes 975
オンプレミスまたはセルフマネージドクラスタのクラスタコネクタ要件 976
Tenable での Kubernetes Cluster Connector API キーのアクセス許可 976
クラスタアカウントの関連付け 976
コンソールでのリソースの可視性 977
新しいコンテナイメージのスキャン 977
OpenShift クラスタのサポート 977
クラスタの移動 978
カスタムクラスター名 978
エージェントのバージョン 978
アドミッションコントローラー 978
プライベートリポジトリから クラウドサイバーエクスポージャー Helm チャートをデプロイする 980
Kubernetes クラスタに特定のセンサーバージョンを使用する方法 981
コード 981

IaC ワークフロー 982
プルリクエストスキャン 983
コア機能 983
サポートされている IaC ツール 984
Terraform 984
Terraform モジュール 985
Terraform コードのモジュールスキャン 985
Terraform の統合リポジトリ内のプライベートモジュールスキャン 989
動的設定スキャン 991
制限 991
CloudFormation 992
制限 992
ARM 992
制限 993
Bicep 993
制限 993
Helm 994
制限 994
Kubernetes 994
制限 994
IaC 互換性マトリクス 994

リポジトリ 994
パイプライン 995
スキャンで使用される Tenable ポリシー 997
AWS 997
Azure 1010
GCP 1022
OCI 1031
Kubernetes 1032
その他 1035
よくある質問: 除外 1035
除外の定義 1036
除外を定義する方法 1036
除外されたリソースを表示する 1037
ポリシーごとの除外 1037
除外が有効になるタイミング 1037
除外の有効期限と削除 1038
競合する除外 1038
検出結果を既存の除外に追加する 1038
AI-SPM 1039
Tenable はどのような AI リソースとテクノロジーを検出しますか? 1039
ドメイン別 AI-SPM のユースケース 1040

サンプル AI-SPM 攻撃経路フロー 1041

接続 **1042**

Alibaba Cloud 1042

Alibaba Cloudの概要 1042

組織と個人のアカウントの接続に関する考慮事項 1042

アカウントアーキテクチャ 1042

組織アーキテクチャ 1043

アリユンと国際環境 1043

Alibaba Cloudの必要なアクセス許可 1043

モニタリングポリシー 1046

データ保護ポリシー 1047

ワークロード保護ポリシー 1047

Alibabaクラウド組織の接続 1049

前提条件 1049

Alibabaクラウド組織の接続 1050

Alibaba Cloud 組織を手動でデプロイする 1053

RAM ユーザーとアクセスキーを作成する 1053

Tenable の RAM ロールを作成する 1054

カスタムポリシーの作成 1054

ポリシーの割り当て 1055

メンバーアカウントでロールを設定する 1055

Alibaba Cloud アカウントの接続 1056
前提条件 1056
Alibaba Cloud アカウントの接続 1057
Alibaba Cloud アカウントを手動でデプロイする 1059
RAM ユーザーとアクセスキーを作成する 1060
Tenable の RAM ロールを作成する 1060
カスタムポリシーの作成 1061
ポリシーの割り当て 1062
ポリシーの割り当て 1062
Alibaba Cloud の FAQ とトラブルシューティング 1062
フォルダーまたはアカウントを組織から除外する 1062
近日公開機能を有効にする 1063
デプロイメント環境 1063
RAM ユーザーと RAM ロールのアーキテクチャ 1063
アカウントステータスとトラブルシューティング 1064
組織のステータスとトラブルシューティング 1066
AWS 1068
AWS の概要 1068
組織と個人のアカウントの接続に関する考慮事項 1068
アカウントアーキテクチャ 1069
モニタリングや修正のアクセス許可を持つアカウント 1069

CloudTrail が接続されている図 1069
CloudTrail が接続されていない図 1070
CloudTrail のアクセス許可を持つアカウント 1070
AWS の必要なアクセス許可 1071
付録 I: AWS IAM ポリシー 1072
Tenable モニタリングポリシー (読み取り専用) 1072
Tenable 修正ポリシー (読み取りと書き込み) 1077
CloudTrail ポリシー 1078
データリソーススキャンポリシー (データ保護) 1079
EC2 インスタンススキャン (ワークロード保護) 1080
ECR スキャンワークロード保護ポリシー 1083
Terraform ポリシー 1083
Amazon Bedrock 呼び出しログ 1084
AWS アカウントアクセスの JIT ポリシー 1084
アカウントアクセス用の管理アカウント 1085
アカウントアクセス用の委任された管理者アカウント 1086
アプリケーションアクセスの JIT ポリシー 1086
アプリケーションアクセス用の管理アカウント 1087
アプリケーションアクセス用の委任された管理者アカウント 1087
AWS CloudTrail 1088
CloudTrail アクセスを付与するメリット 1089

データイベントに基づく詳細な推奨事項の有効化 1090
CloudTrail のデプロイメント 1091
異なるアカウントの KMS キー 1093
AWS アカウントの接続 1094
AWS 中国アカウントのオンボーディング 1101
AWS 組織の接続 1104
AWS 組織の接続 1104
前提条件 1104
組織の接続 1104
次のステップ 1109
AWS の FAQ (よくある質問) とトラブルシューティング 1109
us-east-1 リージョンへのアクセス 1109
AWS コンソールのアカウントへのアクセス 1109
組織から OU またはアカウントを除外する 1110
Elastic Beanstalk バケットの GetObject アクセス許可 1110
カスタムポリシーと SecurityAudit ポリシーの両方の必要性 1111
AWS の新しいサービスとアクセス許可 1111
組織の統合名の更新 1111
インベントリの ECS タスク定義 1112
マルチリージョンの CloudTrail 1112
アカウントステータスとトラブルシューティング 1112

CloudTrail のステータス 1114
Azure 1115
Azure の概要 1115
接続の考慮事項 1116
Azure の必要なアクセス許可 1116
Microsoft Entra ID のアクセス許可 1116
Tenable アプリのアクセス許可の更新 1117
Azure アクセス許可 1118
Microsoft Entra ID テナントの接続 1128
Microsoft Entra ID テナントの接続 1128
手動のアプリ登録 (中国のみ) 1130
次のステップ 1131
Azure 組織の接続 1131
前提条件 1132
組織の接続 1132
Azure 組織の手動デプロイ 1135
次のステップ 1136
Azure サブスクリプションの接続 1136
前提条件 1137
サブスクリプションの接続 1137
Azure サブスクリプションの手動デプロイ 1139

次のステップ 1140
Azure の FAQ (よくある質問) とトラブルシューティング 1141
Azure サブスクリプションおよび組織の FAQ (よくある質問) 1141
組織と Microsoft Entra ID のペアリング 1141
フォルダーまたはサブスクリプションを組織から除外する 1142
Microsoft Entra ID ユーザーの最小限のアクセス許可 1142
Key Vault 閲覧者ロールの割り当て 1142
組織の統合名の更新 1143
Microsoft Entra ID の FAQ (よくある質問) 1143
使用されていない PII の処理 1143
アプリの認証に必要なユーザーのアクセス許可 1144
パブリック版と中国の Microsoft Entra ID テナントの接続の違い 1144
ジャスト インタイム (JIT) アクセスのサポート 1144
サブスクリプションのステータスとトラブルシューティング 1144
Google 1145
GCP の概要 1145
クラウド イベント データ 1146
VPC Service Controls の例外の追加 1147
Google の必要なアクセス許可 1148
Google Workspace のアクセス許可 1148
必要なアクセス許可 1149

GCP プロジェクトと組織のアクセス許可 1150
単一プロジェクト接続用の組織レベルのカスタムロール 1153
Google Workspace の接続 1154
前提条件 1154
Workspace の追加 1155
カスタムロールを使用してアクセス許可を付与する (推奨) 1157
ドメイン全体の委任を使用してアクセス許可を付与する (アドバンス) 1158
Google Workspace の手動デプロイ 1159
Tenable を許可されたドメインとして追加する 1160
ドメイン全体の委任による追加の IAM 機能 1161
統合名の更新 1162
GCP 組織の接続 1162
前提条件 1163
組織の接続 1163
GCP 組織の手動デプロイ 1166
Tenable のサービスアカウントを作成する 1167
組織レベルでサービスアカウントを承認する 1168
監査ログを設定する 1168
GCP プロジェクトの接続 1171
前提条件 1171
プロジェクトの接続 1172

GCP プロジェクトの手動デプロイ 1174
Tenable のサービスアカウントを作成する 1174
組織レベルでサービスアカウントを承認する 1176
プロジェクトレベルでサービスアカウントを承認する 1176
監査ログを設定する 1177
組織レベルのアクセス許可を持つカスタムロールを作成する 1179
Google の FAQ (よくある質問) とトラブルシューティング 1179
GCP の FAQ (よくある質問) 1180
フォルダーまたはプロジェクトを組織から除外する 1180
組織レベルのアクセス許可を付与する 1180
プロジェクトは削除の保留中です 1181
ドメイン内のユーザーが外部と見なされる 1181
組織の統合名の更新 1181
Terraform のデプロイメント 1182
Google Workspace の FAQ (よくある質問) 1182
サービスアカウントトークン作成者ロール 1182
サービスアカウントの権限借用とサービスアカウントキー 1182
スーパー管理者ユーザー (アドバンス) 1183
ドメイン全体の委任 (アドバンス) 1183
割り当て管理者ロール (レガシー) 1185
プロジェクトステータスとトラブルシューティング 1185

ワークスペースのステータスとトラブルシューティング 1187
OCI 1188
OCI の必要なアクセス許可 1188
モニタリング 1188
ワークロード保護 1188
暗号化ボリューム 1189
OCI テナンシの接続 1189
前提条件 1190
テナンシの接続 1191
OCI テナンシの手動デプロイ 1192
グループの作成 1193
ポリシーを作成してグループにポリシー割り当て 1194
ユーザーの作成 1195
ユーザー認証情報の作成 1196
OCI の FAQ (よくある質問) とトラブルシューティング 1198
テナンシからフォルダーまたはコンパートメントを除外する 1198
サポートされている OCI リソース 1199
統合名の更新 1199
テナンシステータスとトラブルシューティング 1199
テナントステータス 1199
コンパートメントステータス 1201

Snowflake 1202
Snowflake の接続 1202
Snowflake アカウントの接続 1202
Tenable にネットワークアクセス権を付与する 1205
Snowflake FAQ とトラブルシューティング 1207
アクセス許可と統合 1207
定期スキャンとメンテナンス 1208
データベースの範囲と検出 1209
組織支援 1209
認証とセキュリティ 1209
ライセンス 1210
Snowflake 機能サポート 1210
ネットワークアクセス 1210
アカウントステータスとトラブルシューティング 1211
IaC 1211
コードリポジトリの接続 1211
リポジトリの接続 1212
Azure Repos 組織の追加 1212
Bitbucket ワークスペースの追加 1216
GitHub 組織の追加 1218
GitHub Enterprise Server の追加 1221

GitLab グループの追加 1223
GitLab セルフマネージドサーバーの追加 1225
クラウドからコードまで同期 1226
AWS: Terraform のアクセス許可を付与する 1226
Azure: Terraform のアクセス許可を付与する 1228
GCP: Terraform のアクセス許可を付与する 1229
プルリクエストスキャン 1230
セットアップと要件 1231
仕組み 1231
プルリクエストスキャンを無効にする 1232
CI/CD の接続 1232
パイプラインの接続 1232
パイプラインの接続について 1233
範囲指定された CI/CD パイプラインのサポート 1234
Azure Pipelines の追加 1234
Azure Pipelines 用の Tenable Step 1238
GitHub アクションを追加する 1238
GitLab パイプラインの追加 1241
IaC スキャンを設定し、GitLab で SAST 形式の結果を表示する 1243
Jenkins パイプラインの追加 1244
非 Git リポジトリの追加変数 1248

Terraform Cloud Run タスクの追加 1249
合理化された実行タスクレビューで詳細な結果を表示する 1250
別のパイプラインを追加する 1251
非 Git リポジトリの追加変数 1254
スキャンの設定 1255
スキャン設定とポリシー設定の違い 1256
Azure Pipelines パラメーター 1256
Azure Pipelines スキャンパラメーター 1257
Azure Pipelines 同期パラメーター 1264
GitHub Actions パラメーター 1267
GitHub Actions スキャンパラメーター 1267
GitHub Actions 同期パラメーター 1274
GitLab CI/CD パラメーター 1277
GitLab CI/CD スキャンパラメーター 1277
Tenable Docker イメージの CLI 1283
コマンドのリスト 1283
IaC スキャン 1284
IaC Terraform 同期 1285
IaC list-policies 1285
version 1286
グローバルフラグ 1286

フラグを環境変数として使用する 1286
フラグと環境変数の構文 1287
Terraform Cloud エンドポイント URL の設定 1287
サンプル URL 1288
従来のリリースパイプラインを使用している場合に必要な追加のパラメーター 1288
構成例 1289
出力例 1289
JSON 1289
CSV 1291
クラウドからコードまで同期 1291
ワークロード 1291
ワークロードの接続 1291
AWS: EC2 インスタンスおよび内部 AMI スキャン (ワークロード保護) 1292
AWS EC2 インスタンススキャンワークロード保護ポリシー 1293
Azure: 仮想マシンスキャンのアクセス許可を付与する 1295
組み込みロールを使用した Windows アクセス許可の付与 1296
カスタムロールを使用した特定の Azure アクセス許可の付与 1296
GCP: ワークロード保護のアクセス許可を付与する 1297
OCI: ワークロード保護のアクセス許可を付与する 1298
Alibaba Cloud: ワークロード保護のアクセス許可を付与する 1298
オンプレミスワークロードの接続 1300

コンテナイメージ CI/CD パイプラインの接続 1300
Azure Pipelines の追加 1300
GitHub アクションを追加する 1303
GitLab パイプラインの追加 1304
Jenkins パイプラインの追加 1306
非 Git リポジトリの追加変数 1309
別のパイプラインを追加する 1309
非 Git リポジトリの追加変数 1311
スキャンの設定 1312
Azure Pipelines パラメーター 1312
GitHub アクションパラメーター 1317
GitLab CI/CD パラメーター 1328
Tenable Docker イメージの CLI 1333
フラグを環境変数として使用する 1334
Container Image Registries の接続 1335
AWS: ECR スキャンのアクセス許可を付与する 1336
AWS: ECR スキャンポリシー 1337
JFrog Organization を追加する 1338
Cloudsmith Organization を追加する 1339
サードパーティレジストリの追加 1340
Tenable でコンテナレジストリスキャンを有効または無効にする 1342

脅威検出 1342
脅威検出の要件 1343
要件 1343
クラウドアカウント 1343
Kubernetes クラスタ 1343
センサーリソース 1344
アクセス許可と接続性 1344
脅威検出の設定 1344
AWS: CloudTrail アクセスの設定 1345
Azure: アクティビティログのアクセス許可を付与する 1346
GCP: 監査ログのアクセス許可を付与する 1346
Kubernetes: Kubernetes センサーのインストール 1347
Kubernetes クラスタ 1348
Kubernetesの概要 1348
クラスター検出 1349
Kubernetesのセキュリティ機能 1349
Helm Chart の統合が必要な場合 1350
Kubernetesクラスターを接続する 1351
Kubernetes のリソース同期とワークロード保護 1351
ランタイム検出 1352
アドミッションコントローラー 1352

クラウドごとの Kubernetes 要件 1352
Amazon EKS クラスタの接続 1355
要件 1356
Tenable ロールクラスターアクセス許可を付与する 1356
AWS コンソールを使用してクラスタのアクセス許可を付与する (推奨) 1356
CLI を使用したクラスタのアクセス許可の付与 1357
Tenable へのネットワークアクセスを許可する 1361
Azure AKS クラスタの接続 1362
要件 1362
クラスタへの Tenable アクセス許可の付与: Azure RBAC 対応の Microsoft Entra ID 1363
組み込みのロールバインディングを Tenable に割り当てる 1364
カスタム Tenable ロールを追加する 1365
クラスタに Tenable アクセス許可を付与する: Kubernetes RBAC 対応の Microsoft Entra ID 1366
Tenable へのネットワークアクセスを許可する 1367
Google GKEクラスターを接続する 1367
要件 1368
Tenable へのネットワークアクセスを許可する 1368
Oracle OKEクラスタの接続 1369
要件 1369
クラスタのアクセス許可を付与する 1370

CLI を使用したクラスタのアクセス許可の付与 1370
OCI ポリシーを使用したクラスタのアクセス許可の付与 1372
Tenable へのネットワークアクセスを許可する 1373
Helm チャートを介してクラスタを接続する 1374
Helm チャートメソッドを使用するタイミング 1374
Kubernetes クラスタの接続 1375
Kubernetes リソース同期および脆弱性管理 1375
ランタイム検出 1376
アドミッションコントローラー 1376
Kubernetes クラスタコネクタ (API トークン) を追加する 1377
クラウドマネージドクラスタのリソースを同期する 1377
オンプレミスまたはマネージド (プライベート) クラスタのリソースの同期 1378
Kubernetes ランタイム検出センサーのインストール 1379
アドミッションコントローラーのインストール 1379
Vulnerability Management Sensor for Kubernetes をインストールする 1380
クラスターを追加する 1381
要件 1381
許可されたデスティネーション 1382
Helm コマンドを設定して実行する 1384
デプロイメントの検証 1386
API 経由でのクラウドマネージドクラスタの接続 1387

高度なクラスター設定 1388
Helm のオプションのコマンドパラメーター (CLI) 1388
values.yaml ファイル 1391
共通 values.yaml パラメーター 1391
カスタム CA 証明書 1399
クラスタアカウントの場所 1400
Helm チャートのトラブルシューティング 1400
helm のインストールが失敗する 1401
インストール前フックの失敗 (プロキシ/ネットワークのブロック) 1401
イメージプルの失敗 (403 Forbidden) 1402
アカウント検証の失敗 (TenantNotExist) 1403
helm のインストールは成功するが、何か問題がある 1404
間違ったアカウントに関連付けられたクラスタ 1404
リソース同期のハングアップ 1404
デプロイ後にポッドが失敗する、または接続が切断される 1404
コネクタ Pod のエラーとリバーストンネルの障害 1405
センサーのアクセス許可拒否 (PSS) 1406
循環的再起動 (オンプレミス) 1406
プライベートレジストリを持つクラスタ 1406
Tenable コンポーネントリポジトリへのアクセス 1407
新しい Chart バージョンにアップグレードする 1408

GitOps ツールによる Helm チャートのデプロイメント 1408
フラックスセットアップ 1409
フラックスの初期化 1409
リポジトリのレイアウトを設定する 1409
設定マニフェストの追加 1409
tenable-repo.yaml 1410
tenable-release.yaml 1410
tenable-secrets.yaml 1411
kustomization.yaml 1411
エントリポイントの作成 1412
Argo CD セットアップ 1412
Argo CD のインストール 1412
便利な Argo CD アクション 1413
Argo CD アプリケーションマニフェスト 1413
アプリケーションマニフェストの適用 1414
アプリケーションステータスの確認 1414
Helm チャートオーケストレーションの詳細を表示する 1415
アプリケーションを削除する 1415
複数のクラウドマネージド Kubernetes クラスタの接続 1415
要件 1415
クラスターを追加する 1416

チケッティングとITSM 1417
Azure Boards 1417
始める前に 1417
組織の追加 1418
組織アクセス許可を付与 1419
プロジェクトの追加 1419
検出結果のAzure Boards作業項目の詳細 1420
作業項目の更新を同期する 1421
サポートされている作業項目の種類とフィールド 1421
Azure Boards 作業項目のサンプル 1421
Jira 1422
始める前に 1423
OAuth 2.0 認証情報の設定 1423
Jira ユーザーのセットアップ 1424
Jira インスタンスの追加 1425
Jira スペースの追加 1426
Jira 課題のトランジションを許可する 1427
サンプル Jira 課題 1430
ServiceNow 1430
始める前に 1430
インスタンスの追加 1431

インシデントの状態と検出結果のステータスの同期 1433
インシデントの追加フィールドの使用 1434
サポートされているフィールド 1436
ServiceNow インシデントのサンプル 1436
コラボレーション 1437
Slack 1437
Workspace の追加 1438
JIT 用のワークスペースを再認証する 1441
Slack で検出結果を表示する 1442
Microsoft Teams 1443
Teams 組織の追加 1443
SIEM (セキュリティ情報イベント管理) 1444
データドッグ 1444
Datadog 組織の追加 1444
Datadog で Tenable の検出結果を表示する 1445
JSON のサンプル 1445
QRadar 1447
QRadar サーバーの追加 1447
QRadar での Tenable 検出結果の表示 1449
JSON のサンプル 1451
Splunk 1452

Splunk インスタンスの追加 1452
Splunk で Tenable の検出結果を表示する 1454
JSON のサンプル 1454
SQS キュー 1456
SQS キューの追加 1456
JSON のサンプル 1459
Webhook 1460
Webhook 1460
Webhook の追加 1461
Microsoft Sentinel (Webhook 経由) 1461
ログ分析ワークスペースを作成する 1462
ロジックアプリを作成する 1463
Tenable で Sentinel Webhook 統合を作成する 1469
Microsoft Sentinel でデータを表示する 1470
Sumo Logic (Webhook 経由) 1473
Sumo Logic へのデータ送信 1473
JSON のサンプル 1475
Telegram (Webhook 経由) 1476
BotFather で新しい Telegram ボットを作成する 1476
AWS を使用した CloudFormation スタックの作成 1478
SSM パラメーターを設定する 1478

CloudFormation スタックの作成 1479
Tenable で Telegram Webhook 統合を作成する 1481
データリソースの接続 1482
AWS: データ保護アクセス許可の付与 1483
AWS データ保護ポリシー 1484
Azure: データ保護アクセス許可の付与 1485
GCP: データ保護アクセス許可の付与 1488
OCI: データ保護アクセス許可の付与 1490
Snowflake: データ保護アクセス許可の付与 1491
Snowflake で必要なアクセス許可 1491
Okta 組織の接続 1492
OneLogin アカウントの接続 1494
Ping Identity 環境の接続 1495
クラウドアカウントのオフボーディング 1499
AWS アカウントのオフボーディング 1499
Azure サブスクリプションのオフボーディング 1501
GCP プロジェクトのオフボーディング 1501
OCI テナンシのオフボーディング 1502
アカウント内スキャンの設定 1502
必要な AWS アクセス許可 1503
必要な Azure アクセス許可 1506

必要な GCP アクセス許可 1509
必要な OCI アクセス許可 1509
リージョンごとにプロビジョニングされるリソース 1510
AWS 1510
Azure 1512
GCP 1513
OCI 1515
ネットワーク分離されたサーバーの接続 1516
Tenable のサーバーへの接続方法 1517
コネクタの追加 1517
高度なコネクタ設定 1518
values.yaml の内容 1519
プレイブックとチュートリアル 1521
クイックスタートガイド 1521
ステップ 1: 環境のセットアップ 1521
ステップ 2: 関連するセキュリティ領域の所有者の特定 1522
自動化ルールによって検出結果を所有者に割り当てる 1523
所有者に送信するために、レポートの作成をスケジュール化する 1523
ステップ 3: 重大な検出結果への対処 1524
サードパーティアクセス 1525
機密データへのアクセス権を持つサードパーティアイデンティティの検索 1525

過剰な権限を持つサードパーティアイデンティティの検索 1526
MFA を使用しないルートアカウント 1527
[検出結果] ページを使用して、MFA を使用しないルートアカウントを特定する 1527
一般に公開されているリソース 1527
ダッシュボードの [パブリックリソース] ウィジェットを使用してパブリックリソースを素早く表示する 1527
本番環境で露出しているシークレット 1528
本番環境で「高」と「重大」の検出結果 1529
ステップ 4:「容易に解決できる問題」への対処 1529
非アクティブなアイデンティティ 1529
未使用の認証情報 1530
未使用のセキュリティグループ 1531
ステップ 5: 検出結果のレビュー 1531
ステップ 6: 検出結果の修正 1532
検出結果の手動修正 1532
検出結果の自動修正 1533
AI リスクを検出する方法 1534
ステップ 1: インベントリで AI 資産を検出する 1534
ステップ 2: AI リソースとトレーニングデータを関連付ける 1535
脆弱性のある特権 VM を保護する 1536
ステップ 1: リスクの表面化 (ビルトインクエリ) 1537

ステップ 2: 検出を運用可能にする 1538
カスタムポリシーの作成 1538
レポートの作成 1538
無視された検出結果からのパターンベースの除外の作成 1539
ステップ 1: 無視された検出結果のパターンを監査する 1539
ステップ 2: パターンベースの除外を構築する 1540
除外を監査して維持する 1542
ステップ 1: 警告サインがないか各除外を確認する 1542
ステップ 2: 削除する前に無効にする 1543
ステップ 3: 除外の所有権を確認する 1544
独自の機密データの管理 1544
目的 1544
ステップ 1: ビジネス固有のデータを定義する (カスタムデータタイプ) 1545
ステップ 2: 検出と正確性を検証する 1547
ステップ 3: ガバナンスを実施する (カスタムクラウドポリシー) 1548
ライセンス数の増加または超過に対処 1549
ステップ 1: ライセンスの使用状況を確認する 1550
ステップ 2: 一般的な原因を除外する 1550
ステップ 3: 増加を追跡する 1551
ステップ 4: 消費を減らすか、超過に対処する 1551
クラウドオンボーディングのアクセス許可とロールのエラーを解決する (AWS、Azure、GCP) 1552

ステップ 1: ロールとサービスアカウントの設定を検証する 1552
ステップ 2: クラウド固有のブロッカーを確認する 1553
AWS 1553
Azure 1553
GCP 1554
ステップ 3: 接続を確認する 1554
常設管理者アクセスをジャストインタイムアクセスに変換する 1554
前提条件 1555
ステップ 1: 使用状況の決定 1555
ステップ 2: 最小権限のアクセス許可セットを生成する 1556
ステップ 3: アクセス許可セットの JIT 使用資格の作成 1557
ステップ 4: 資格が機能することを確認する 1558
ステップ 5: スタンディングアクセスを取り外す 1558
ステップ 6: 結果を確認する 1559
サンプル修正ワークフロー 1560
エンドツーエンドの検出結果ワークフローのサンプル 1561
アイデンティティの影響範囲を視覚化 1568
ステップ 1: エクスポージャーの範囲の定義 (カスタムクエリ) 1568
ステップ2: エクスポージャーマップを表示する (Organic Graph) 1569
ステップ 3: 値が高いターゲットを特定する 1569
製品のユースケース 1570

マルチクラウドの可視化 1570
最小権限の適用 1570
リスクの評価と優先順位付け 1571
リスクの高い権限と不具合のある設定の軽減 1571
クラウドコンプライアンスのモニタリング 1571
クラウド検出と対応 1571
セルフサービスのジャストインタイムアクセス 1571
JIT アクセス 1572
Tenable JIT ユーザーインターフェース 1572
JIT ポータルにアクセスできるユーザー 1573
JIT を使い始める 1575
JIT ペルソナとワークフロー 1575
JIT ワークフロー 1575
Tenable JIT アクセス許可を付与する 1577
JIT 用に AWS Identity Center に接続する 1578
に JIT 関連のアクセス許可を付与する Tenable 1579
AWS アカウントアクセスの JIT ポリシー 1579
アカウントアクセス用の管理アカウント 1580
アカウントアクセス用の委任された管理者アカウント 1581
アプリケーションアクセスの JIT ポリシー 1582
アプリケーションアクセス用の管理アカウント 1582

アプリケーションアクセス用の委任された管理者アカウント 1582
JIT 用に Azure を接続する 1583
JIT 用に GCP を接続する 1583
JIT 用に Microsoft Entra ID を接続する 1584
Tenable JIT アプリに必要なアクセス許可 1585
JIT 用に Google Workspace を接続する 1586
JIT 用に Okta を接続 1587
JIT 用に OneLogin を接続する 1588
JIT 用に Ping Identity を接続する 1589
SSO 経由の JIT ポータルログインを有効化 1590
AWS Identity Center 経由でのログインの有効化 (SAML 2.0) 1590
Google 経由でのログインを有効化 1593
OIDC を使用した Google 経由でのログインの有効化 1593
SAML を使用した Google 経由でのログインの有効化 1593
Microsoft Entra ID 経由でのログインの有効化 1594
OIDC を使用した Microsoft Entra ID 経由でのログインの有効化 1595
SAML を使用した Microsoft Entra ID 経由でのログインの有効化 1596
Okta 経由でのログインの有効化 1598
OneLogin 経由でのログインを有効にする 1598
Ping Identity 経由でのログインの有効化 1600
カスタム SAML 2.0 プロバイダー経由でのログインの有効化 1601

Slack と JIT の統合 1602
JIT アクセス用に Slack を有効化 1603
JIT 用の Slack を使用できるユーザー 1604
メッセージの送信先 1604
Teams と JIT の統合 1605
JIT アクセス用に Teams を有効にする 1606
Tenable Teams 用のアプリに必要なアクセス許可 1606
JIT アクセスを管理する 1607
資格の追加 1607
Azure 所有者の使用資格 1611
使用資格の管理 1612
複数レベルの承認ワークフロー 1614
Slack での複数レベルの承認 1615
JIT アクティビティの監査 1617
アクセス許可資格監査イベントテーブル 1617
アクセス許可リクエスト監査イベントテーブル 1618
JIT 監査ビデオ 1620
資格管理 JIT ビデオ 1620
アクセスをリクエストする 1621
JIT ポータル経由でのアクセスのリクエスト 1622
クラウドまたは IdP アカウントに接続する 1625

アクセスの再リクエスト 1626
Slack 経由でアクセスをリクエストする 1626
前提条件 1626
Teams 経由でアクセスをリクエストする 1629
前提条件 1629
リクエストの表示と管理 1630
アクセスリクエスト 1630
アクセスレビュー 1631
アクセスのリクエスト ビデオ 1632
アクセスの確認 1632
JITポータルからアクセスを確認する 1633
Slack 経由でアクセスを確認する 1635
前提条件 1635
Slack の [ホーム] タブ 1636
Slack の [メッセージ] タブ 1636
Teams 経由のアクセスの確認 1636
前提条件 1636
アクセスビデオの確認 1638
一般的な JIT のユースケース 1638
AWS アカウントへのアクセスのリクエスト 1638
Azure アカウントへのアクセスをリクエストする 1642

GCP アカウントへのアクセスをリクエストする 1645
SaaS アプリケーションへのアクセスのリクエスト 1648
EKS クラスターへのアクセスのリクエスト 1651
EKS クラスターアクセスを許可するための AWS IAM を設定する 1651
よくある質問 JIT 1654
AWS アクセス割り当て 1654
Azure アクセス割り当て 1654
定期的なアクセスリクエスト 1655
Azure 所有者ロール 1656
大規模環境で Jit Access を管理する 1657
JIT Source IPs (JIT ソース IP) 1658

Tenable One Cloud Exposure へようこそ

Tenable One Cloud Exposure について

完全な資産検出や詳細なリスク分析から、ランタイム脅威検出やコンプライアンスまで、Tenable のクラウドネイティブアプリケーション保護プラットフォーム (CNAPP) は、最も複雑なクラウドセキュリティの課題でさえも簡素化します。独自のアイデンティティ第一のアプローチにより、クラウドのアタックサーフェスを大幅に縮小し、最小権限を大規模に適用します。

ライセンス

この記事では、プラットフォーム全体のライセンスタイプ、機能サポート、リソース請求ロジックに関する包括的な情報を提供します。

- ライセンスページ。ライセンスの使用状況を確認します。
- ライセンスタイプ。利用可能なすべてのライセンスタイプについて確認します。
- 請求対象のリソース。どのリソースがどのように請求されるかについて確認します。
- ライセンスの回収。ライセンスの回収方法と、ライセンス消費の管理方法について確認します。
- FAQ (よくある質問)。ライセンスに関連する、よくある質問を紹介します。

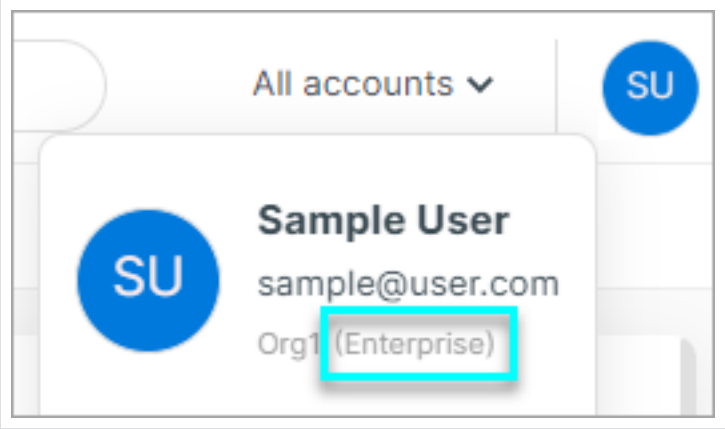
各ライセンスタイプでサポートされている機能をまとめた包括的なリストについては、ライセンス別機能比較を参照してください。

ライセンスページ

[ライセンス] ページにアクセスするには、Tenable One Cloud Exposure コンソールで **[設定] > [ライセンス]** の順に移動します。このページを使用すると、クラウドサイバーエクスポージャーのライセンスに関連する以下の情報を確認できます。

- 更新日。
- クラウドサイバーエクスポージャーライセンス使用状況。左側のアカウントツリーで範囲を選択すると、各アカウント範囲に関する使用状況が表示されます。
- 契約しているライセンスタイプ。

  ライセンスタイプは、クラウドサイバーエクスポージャーコンソールの右上にあるユーザープロファイルでも確認できます。



- 各ライセンスタイプでサポートされている機能に関する一般的な情報。クラウドサイバーエクスポージャー機能の各ライセンスタイプへの完全なマッピングについては、ライセンス別機能比較を参照してください。

クラウドサイバーエクスポージャーライセンス使用状況

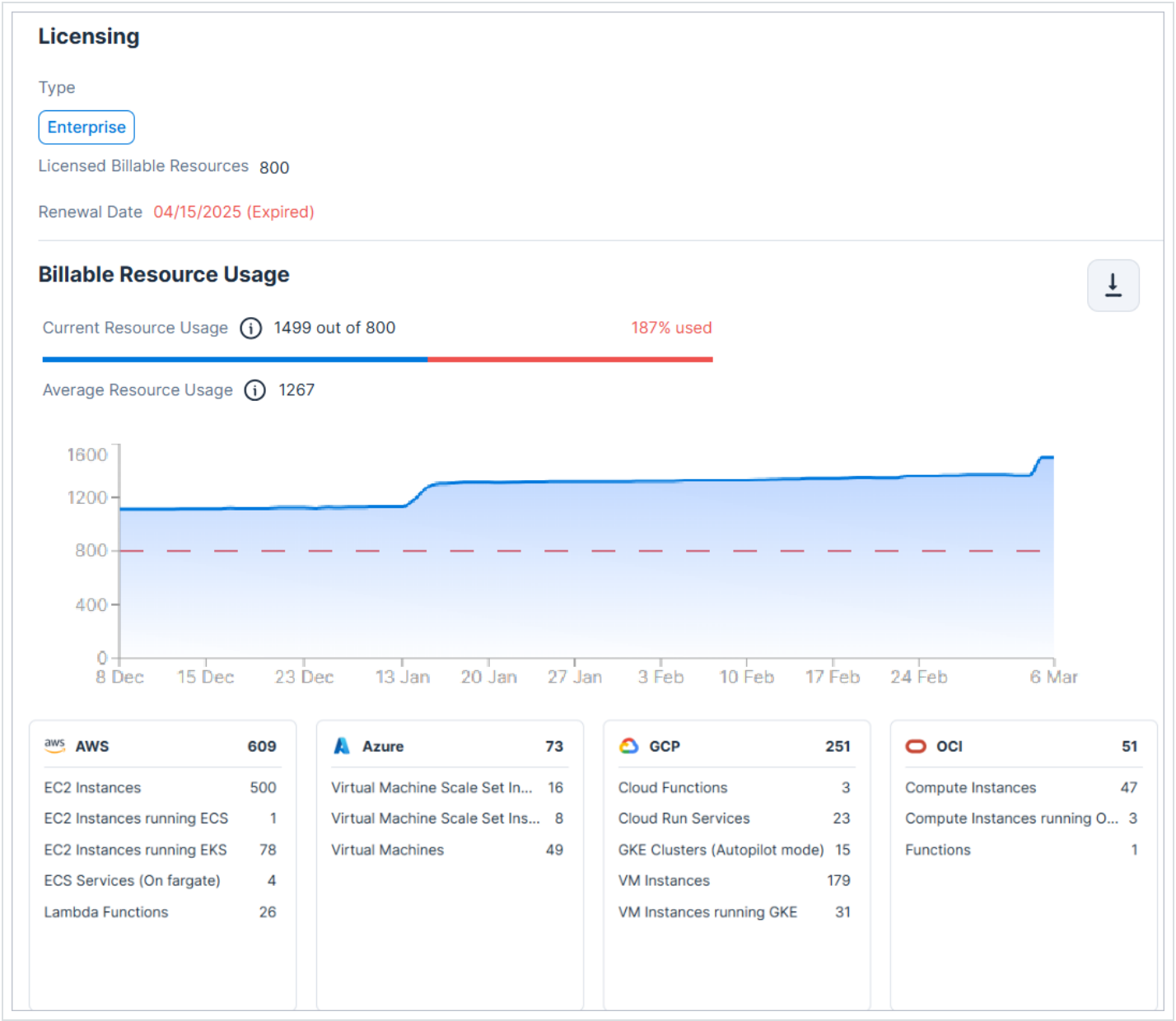
[ライセンス] ページには、クラウドサイバーエクスポージャーのライセンス使用状況の全内訳が表示されます。左側のアカウントツリーで範囲を選択すると、各アカウント範囲に関する使用状況が表示されます。

- **現在のリソースの使用量**。クラウドサイバーエクスポージャーが取得した前回のスナップショットの時点での、購入した合計数のうち現在使用している請求対象のリソースの数。前回作成されたスナップショットの日付は、横にあるツールチップに表示されます。
- **リソースの平均使用量**。リソース数は、オンボーディングアカウントのリソースの過去最大 90 日間の平均使用量に基づいています。
- **使用状況のトレンドのグラフ**。請求対象のリソースの使用数を過去 90 日までさかのぼって表示するグラフ。

- **青い線** = 使用されたリソース
- **赤い線** = 購入されたリソース

- **請求対象のリソースの内訳**。環境内にある請求対象のリソースの内訳が表示されます。

> **注意:** 次のリソース請求比率に注意してください。
> - **オンプレミス K8s ワーカーノード**: 1 リソース = 2 請求対象のリソース
> - **サーバーレス関数**: 10 リソース = 1 請求対象のリソース
>
> コンソール内の内訳は請求対象のリソースを示しており、リソースの合計数ではありません。



リソースごとの請求対象ユニットを表示する方法

- **[探索] > [インベントリ]** に移動し、**[請求対象の使用状況]** 列を追加します。
- **[探索] > [エクスプローラー]** に移動し、リソースと[グループ化] を使用した結果の集計 (**請求対象の使用状況**別) を見つけるクエリを作成します。
- **[設定] > [ライセンス]** に移動し、リソースを選択します。**[探索] > [インベントリ]** ページを開き、**[請求対象の使用状況] を [はい]** でフィルタリングして、**[請求対象の使用状況]** 列を追加します。

リソース別のライセンス使用状況データのエクスポート

ライセンスデータを CSV にエクスポートして、リソースタイプ別の使用状況の内訳を表示します。リソースタイプ別に、直近 (最新) リソース数と平均リソース数 (90 日) の両方を確認できます。

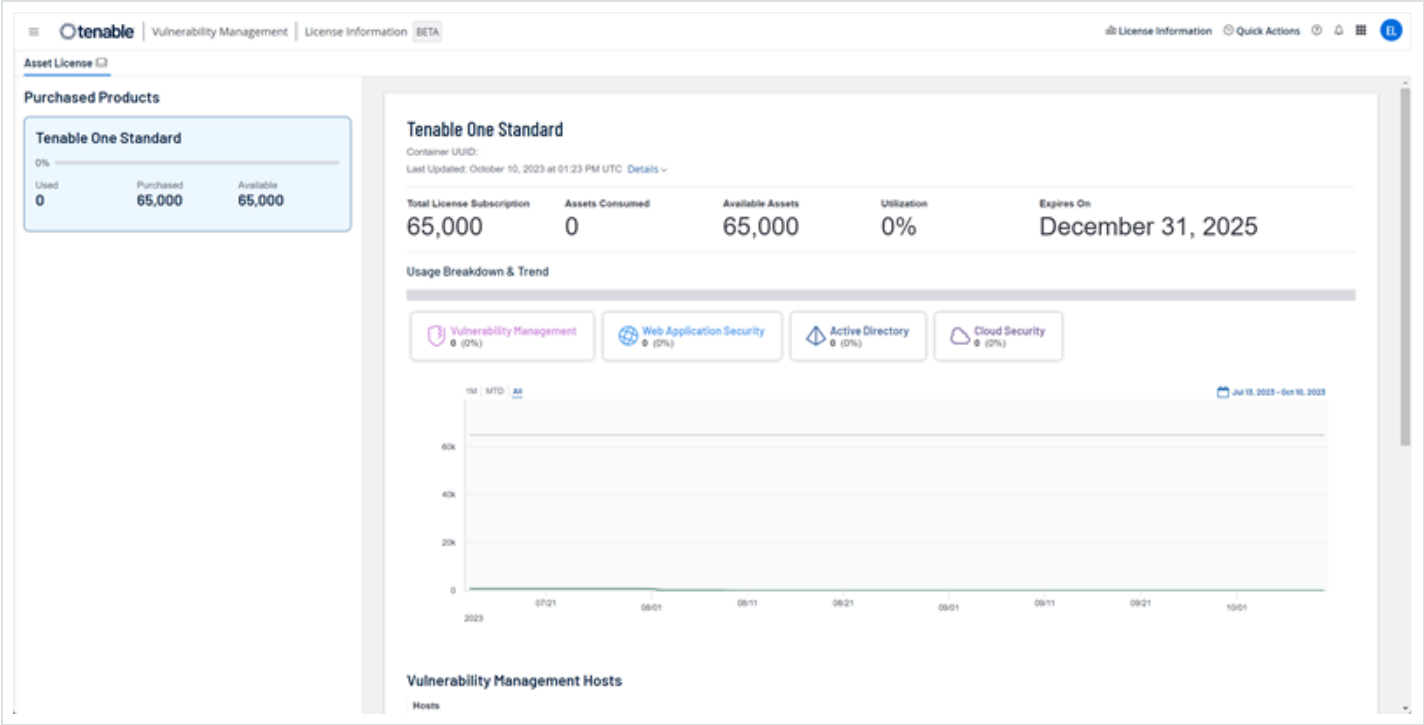
A	B	C	D	E	F	G	H
Provider	Scope	Name	Id	Type	Resource Type	Last Resource Count	Average Resource Count (90 days)
Azure	Organizati	[illegible]		Account	Storage Account Blob Containe	4	3
Azure	Organizati	[illegible]		Account	Virtual Machine Scale Set Insta	2	2
Azure	Organizati	[illegible]		Account	Virtual Machine Scale Set Insta	2	2
Azure	Organizati	[illegible]		Account	Virtual Machines	3	1
Code	Organizati	[illegible]		Folder	Container Image Repositories	0	1
Code	Organizati	[illegible]		Folder	Container Image Repositories	0	1
Code	Organizati	[illegible]	[illegible]	Code Repository	Container Image Repositories	0	1
Container	Organizati	[illegible]		Folder	Container Image Repositories	24	22
GCP	Organizati	[illegible]		Folder	Artifact Container Image Repos	29	26
GCP	Organizati	[illegible]		Folder	BigQuery Datasets (Data Protec	3	2
GCP	Organizati	[illegible]		Folder	Cloud Functions	3	3

ライセンス使用状況データのエクスポート方法

1. クラウドサイバーエクスポージャーコンソール内で、**[設定] > [ライセンス]** の順に移動します。
2. (オプション) [組織] ドロップダウンから範囲を選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [請求対象のリソース使用量] セクションで、**[エクスポート]** ボタンをクリックします。

Tenable One プラットフォームのライセンス使用状況

脆弱性管理の [ライセンス情報] ページでは、すべての Tenable 製品とそのライセンスの使用状況の全内訳を確認することができます。詳細については、関連するドキュメント{target=_blank}を参照してください。



ライセンスタイプ

クラウド サイバーエクスポージャー では複 数 のライセンスを提 供しており、お客 様 はビジネスニーズに最 適 なオプションを選 択 できます。ライセンスで提 供 される機 能 は、ライセンスに応じて段 階 的 に高くなります。つまり、上 位 レベルのライセンスには、前 のレベルに含 まれているすべての機 能 に加 えて新 たな機 能 が付 属します。

クラウド サイバーエクスポージャー 機 能 の各 ライセンスタイプへの完 全 なマッピングについては、ライセンス別 機 能 比 較 を参 照 してください。

Tenable One ライセンス

Tenable One ライセンスでは、他 の Tenable One 機 能 とともにさまざまなクラウド セキュリティ機 能 を利 用 できます。

詳 細 については、Tenable One のライセンスを参 照 してください。

Foundation

Foundation ライセンスには、オンプレミスおよびクラウド資産向けの統合された脆弱性管理が含まれます。このライセンスは、組織内の脆弱性管理を優先する組織に最適です。

主な機能: すべてのクラウド資産における完全なインベントリ、エージェントレスの脆弱性管理、脆弱性インテリジェンス、SBOM、コンプライアンス。ライセンス別機能比較。

Advanced

Advanced ライセンスはは、ネットワークインフラ、アプリケーション、およびクラウド環境のリスクを分析して文脈を示す必要があるエクスポージャー管理チーム向けです。このライセンスは、プロアクティブなリスク軽減を優先するために、脆弱性と設定ミスが複雑な攻撃経路に結びつく状況を理解する必要がある組織に最適です。

主な機能: CSPM、KSPM、CWP、AI-SPM、ネットワーク。ライセンス別機能比較。

CNAPP Complete

CNAPP Complete ライセンスは、クラウドサイバーエクスポージャープラットフォームの無制限かつ完全な機能を必要とする Foundation または Advanced クラスのお客様向けのプレミアムアドオンです。このツールは、広範囲に利用でき、詳細な文脈を提供するため、クラウド資産全体のセキュリティポスチャーを管理するのに適しています。

主な機能: 完全かつ無制限のクラウドサイバーエクスポージャープラットフォームと提供中のすべての機能を利用可能。ライセンス別機能比較。

レガシーライセンス

これらのライセンスは、クラウドサイバーエクスポージャースタンドアロンのクラウドセキュリティ製品を指します。特定のモジュール要件がある組織や既にレガシーライセンスを所有している組織に、クラウドネイティブの専用機能を提供します。

Tenable JIT

Tenable JIT ライセンスにより、AWS、Azure、GCP 全体のクラウドアカウント、および Okta、Microsoft Entra ID、Ping Identity などのアイデンティティプロバイダー (IdP) グループへの時間制限付きのオンデマンドアクセスが可能になります。アクセス承認ワークフローを簡素化しながら、権限露出の期間を短縮する

ことでリスクを最小限に抑えることができます。一般的なリクエストの承認を自動化し、すべてのアクティビティを監査して、セルフサービスポータルまたはSlackやTeamsなどの統合コラボレーションツールを通じてアクセスを管理します。詳細については、セルフサービスのジャストインタイムアクセスを参照してください。

対象者: 広範なクラウドセキュリティツールを必要とせずに、クラウドアカウントに最小権限とジャストインタイムのアクセスを導入することで、最小限の負担でアクセスセキュリティを強化したい組織

CIEM

CIEM ライセンスには **Tenable JIT** ライセンスのすべての機能が含まれており、さらに、人とサービスのアイデンティティ、アクセス許可、アクティビティを継続的にモニタリングできる機能によって拡張されています。IAMリスクを表面化、視覚化、軽減するのに役立ちます。**CIEM** ライセンスは、資産管理からリスク評価、異常検出、ガイド付き自動修正、コンプライアンスまで、クラウドアイデンティティを保護するための完全なソリューションです。

対象者: ワークロード保護とCSPMツールをすでに導入しており、その環境のアイデンティティ関連リスクと権限リスクに対処することを求めている組織

Standard

Standard ライセンスには **CIEM** ライセンスのすべての機能が含まれており、さらに以下の機能によって拡張されています。

- クラウドの設定ミスを検出し、業界標準へのコンプライアンスを強化する数百のポリシー
- クラウドセキュリティリスクの統合ビューと最も詳細で正確な修正機能を提供する、エージェントレスの脆弱性管理、ワークロード保護、およびデータ保護

このライセンスには、AI-SPM、KSPM、IaCセキュリティ、さらにはアクティビティログ保持期間の延長も含まれています。

対象者: CIEM、CSPM、ワークロード保護、データ保護、その他の種類のリスク保護を1つのツールに統合した、完全で一元化されたプラットフォームを必要とする組織

Enterprise

Enterprise ライセンスには **Standard** ライセンスのすべての機能が含まれており、さらに以下のエンタープライズ機能と保護の強化によって拡張されています。

- クラウドの脅威検出
- Snowflake の接続のデータ保護
- アカウント内のワークロードスキャン (データが環境外に出ないようにする)
- Kubernetes アドミッションコントローラー
- オンプレミスの Kubernetes クラスタのセンサーベース脆弱性診断

対象者: CIEM、CSPM、ワークロード保護、アカウント内スキャン、その他の種類のリスク保護を 1 つのツールに統合した、完全で一元化されたエンタープライズプラットフォームを必要とする組織

Cloud Vulnerability Management

Cloud Vulnerability Management (VM) ライセンスは、広範な CNAPP プラットフォームの全体的な複雑さなしで、基礎的なクラウドワークロード保護を必要とする組織向けに設計された特殊なツールです。スムーズなエージェントレススキャンを活用して、クラウドプロバイダー全体の脆弱性や設定ミスを詳細に可視化します。本ライセンスにより、ワークロードのリスク評価と Tenable の業界をリードするリサーチを統合することで、チームはオンプレミス資産とともにクラウドエクスポージャーに優先順位を付け、修正できるようになります。

対象者: 専用のワークロードとコンテナスキャンを使用して脆弱性管理のベストプラクティスをクラウドに拡張したい組織

請求対象のリソース

請求対象のリソースには、以下のようにさまざまなタイプがあります。

- **[請求対象のコンピューティングリソース]**(#compute-and-scan-based-billable-resources)。これは環境の規模を判断し、規模とライセンスの階層を擦り合わせます。クラウドサイバーエクスポージャー が (このような特定のリソースを超えて) クラウド環境全体をスキャンするのに対して、この標準化されたメトリクスではクラウドフットプリントの全体的な規模が反映されます。これはサイズ設定モデルであり、リソースごとのカウントではないため、包含または除外する個別のリソースを選択でき

ません。ただし必要に応じて、クラウドアカウントをアカウントまたはクラウドアカウントのオフボーディングすることができます。

- **[請求対象のスキャンベースのリソース]**(#compute-and-scan-based-billable-resources)。これは、付加価値を提供する機能 (ワークロード保護やデータ保護など) によってスキャンされるリソースのことであり、この機能は必ず有効になっている必要があります。請求は、これらの機能がスキャンしたリソースのみに基づいて行われます。請求対象に特定のリソースを選択することはできませんが、機能を有効または無効にすると、スキャン対象のリソース数に直接影響し、それが請求に反映されます。スキャンベースの機能を特定の範囲で有効または無効にすることで、Tenable でどのアカウントをスキャンするかを微調整できます。
- **[JIT リクエスト者の請求対象リソース]**(#jit-requester-billable-resources)とは、1 つ以上の使用資格に割り当てられた一意のユーザーまたはアイデンティティを指します。

請求対象のコンピューティングおよびスキャンベースのリソース

次の表は、コンピューティングおよびスキャンベースの請求対象リソースすべてについて、クラウドプロバイダーとリソースカテゴリ別に分類したものです。

[請求対象のリソース] テーブルには、コンピューティングおよびスキャンベースの請求対象リソースが一覧表示されています。特に記載がない限り、請求は **1:1 の比率** (1 つのリソースにつき 1 つのライセンス) で計算されます。

1:1 比率の例外

リソース	比率	詳細	影響を受けるライセンス
サーバーレス関数	10:1	Tenable リソースが 1 つのライセンスを消費	すべて
コンテナホスト	1:2	1 つのリソースで 2 つのライセンスを消費 (仮想マシン用に 1 つ、コンテナホスト用に 1 つ)	レガシーライセンス
DynamoDB	5:1	5 つのリソースが 1 つのライセンスを消費	レガシーライセンス

次のツールは、クラウドサイバーエクスポージャーダウンロードページ{target=_blank}で入手できます。

- **サイジングガイド**: サイジングスクリプトを実行して環境内の請求対象のワークロードの数を検出する手順
- **サイジングスクリプト**: AWS、Azure、GCP 向けのサイジングスクリプト

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
コンピュート *Foundation*、*Advanced*、*CNAPP Complete*、*Cloud VM*、*CIEM*、*Standard*、*Enterprise*	**仮想マシン**	EC2 インスタンス	仮想マシン、VM スケールセットインスタンス	仮想マシンインスタンス	ACK を実行している ECS インスタンス	コンピューティングインスタンス	-
	コンテナホスト[2]	EKS/ECS を実行する EC2 インスタンス	AKS を実行する VM スケールセット	GKE を実行する仮想マシンインスタンス	ACK を実行している ECS	OKE を実行するコンピューティング	Kubernetes ノード

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
			インスタンス		インスタンス	インスタンス	
	サーバーレス関数[3]	Lambda 関数	App Services	Cloud Functions	-	Functions	-
	サーバーレスコンテナ[3]	ECS サービス	コンテナインスタンス	Cloud Run、GKE Autopilot	-	-	-
スキャンベース ワークロード保護 *Foundation*、*Advanced*、*CNAPP Complete*、*Cloud*	**コンテナリポジトリ**[4]、[5]	ECR リポジトリ	コンテナリポジトリ	アーティファクトコンテナイメージリポジトリ	コンテナレジストリリポジトリ	-	CI/CD[3]、サードパーティレジストリの追加

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
VM、Standard、Enterprise							
	仮想マシンイメージ	EC2 イメージ	-	-	ACK を実行している ECS イメージ	-	-
	データディスク	EC2 インスタンスデータボリューム	• 仮想マシンデータディスク	VM インスタンスデータディスク	ECS ディスク	コンピューティングインスタンスデータボリューム	

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
			• 仮想マシンスケールセットインスタンスデータディスク				

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
スキャンベース データ保護 *CNAPP Complete、Standard、Enterprise*	**バケット**[3]	S3 バケット	ストレージアカウント Blob コンテナ	ストレージバケット	OSS バケット	オブジェクトストレージバケット	-
	マネージドデータベース[3]	• DynamoDB • RDS インスタンス • RDS クラスタ	Azure SQL Server	• BigQuery データセット • SQL インスタンス	-	-	-
	データプラット	-	-	-	-	-	Snowflake の接続ローカル、共有、マーケットプレ

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
	フォームデータベース[3]						イス
JIT リクエスト者 *JIT、CIEM、Standard、CNAPP Complete、Enterprise*	**ユーザー**	AWS SSO ユーザー	Azure AD ユーザー	GCP ユーザー	-	-	• Okta ユーザー • OneLogin ユーザー • PingIdentity ユーザー

[1] リストされているライセンスのリソースは、請求対象の使用量としてカウントされます。リストにないライセンスのリソースも対象ですが、請求対象ではありません。

[2] これには、請求対象ユニットとして**仮想マシン** (1:1) が含まれます。

[3] これらのリソースは、**Cloud Vulnerability Management** ライセンスに関連していません。

[4] これらのリソースタイプは、**コンテナリポジトリ**内のイメージではなく、コンテナリポジトリ自体に基づいています。たとえば、コンテナ**リポジトリ**は、**同じコンテナの**イメージが 15 個でも 150 個でも、1 つの請求対象リ

ソースと見なされます。

[5] 同じ**コンテナリポジトリ**が **CI/CD パイプライン**と**レジストリスキャン**の両方でモニタリングされている場合、これは 2 つの異なる請求対象リソースとして扱われます。

JIT リクエスト者の請求対象リソース

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

JIT リクエスト者は、1 つ以上の使用資格に割り当てられた一意のユーザー (メールアドレスに基づく) です。これらのユーザーは、JIT 経由で一時的かつ期限付きのアクセスを開始する権限を付与されています。グループが使用資格でプリンシパルとして選択された場合、そのグループ内のそれぞれの一意のユーザーは、アクセスをリクエストしたかどうかにかかわらず、請求対象のリソースの JIT リクエスト者としてカウントされます。

JIT は、AWS、Azure、GCP のクラウドアカウント、および Okta、Microsoft Entra ID、Ping Identity などのアイデンティティプロバイダー (IdP) グループでサポートされています。現在、JIT は OCI ではサポートされていません。

カテゴリ	比率
JIT リクエスト者	1:1

ライセンスのダウングレード

ライセンスタイプをより少ない機能を持つタイプに変更すると (たとえば、CNAPP Complete から Advanced へ)、クラウドサイバーエクスポージャーは 30 日間の猶予期間を開始します。この期間により、データが即座に失われるのを防ぎ、移行に向けて環境を準備する時間を確保できます。

ダウングレードに備える

運用の中断を回避するために、Tenable では猶予期間が始まる前に次のアクションの実行を推奨しています。

- **ジャストインタイム (JIT) アクセス**: 新しい階層にJITが含まれていない場合は、次の手順を実行します。
    - ダウングレード後もJIT監査証跡を保持する場合は、監査証跡をエクスポートします。
    - すべての使用資格が削除されるため、ユーザーには別のアクセス方法を確保するようにしてください。
- **Kubernetes クラスタ**: 新しい階層にKSPMが含まれておらず、現在 Helm チャートを介してクラスタを接続するを使用してKubernetes クラスタを接続している場合は、次の手順を実行します。
    - クラスタからHelm チャートをアンインストールします。これを怠ると、コンテナはTenable バックエンドからの応答の受信を停止するため、継続的に再起動してしまう可能性があります。
- **除外とレポート保持**: ダウングレード後に存在しないポリシーにのみ割り当てられたレポートと除外は、猶予期間が終了すると自動的に削除されます。次を実行します。
    - 重大度の高い除外とカスタムレポートを確認します。これらを維持するには、ダウングレードの完了前に、新しいライセンスの階層でサポートされている少なくとも1つの追加ポリシーにクロス割り当てされるようにしてください。*
- **履歴レポート**: 猶予期間が終了すると、新しい階層外の機能のレポートを生成する機能は無効になるため、次の手順を実行します。
    - ダウングレードが完了する前、有効な猶予期間中に、監査履歴に必要なコンプライアンス履歴またはサマリーをエクスポートします。

猶予期間

この30日間、製品はバックグラウンド操作を維持しながら、新しいライセンスレベルに合わせてコンソールとAPIのアクセスを制限します。

- **猶予期間通知バナー**: コンソールのすべての画面に、猶予期間の残り日数を示すバナーが表示されます。
- **アクセス制限**: 新しいライセンスの階層に含まれていないすべてのコンソール画面とAPIエンドポイントが削除またはブロックされます。これには、ライセンスがない場合、JITポータルが含まれます。
- **機能ブロック**: 新しいライセンスの階層でサポートされていないレポート、自動化、統合は作成できません。編集や削除は可能です。

- **継続スキャン**: それまでにライセンスされたすべてのセキュリティスキャンは、猶予期間中も引き続き実行されます。

  > **注意:** スキャンは継続されますが、クラウドプロバイダーからサードパーティ料金 (データ転送やコンピューティングなど) が継続的に発生する可能性があります。

- **ポリシーと検出結果**: ライセンスのない機能に関連する検出結果とポリシーは、検出結果画面に引き続き表示されます。これにより、移行中の動的な深刻度とコンプライアンススコアが正確な状態に保たれます。
- **カスタム設定**: 新しいライセンスでサポートされていないウィジェットまたはセクションは、プレースホルダーに置き換えられます。次を実行します。
  - 必要に応じて、カスタムダッシュボードとレポートを確認し、プレースホルダーを削除し、形式を調整します。

ダウングレード後の完了

30 日間の猶予期間が終了 (または猶予期間を手動で終了する) すると、クラウドサイバーエクスポージャーは新しいライセンス階層への移行を完了します。次の自動化アクションと構成変更は直ちに行われます。

> **注意:** 猶予期間の終了時に、バックグラウンドクリーンアッププロセスが完全に完了するまでに最大 24 時間かかる場合があります。このタイムラインは、猶予期間が自然に期限切れになるか、管理者によって猶予期間を手動で終了するするかにかかわらず、同様に適用されます。

ライセンスのないデータの自動クリーンアップ

現在のライセンスでサポートされなくなったデータや設定が自動的に削除されます。

- **検出結果とポリシー:** ライセンスのない機能に関連するすべての検出結果と組み込みポリシーは、コンプライアンスマッピングおよび検出結果画面から削除されます。
- **スキャン:** ライセンスのない機能に対するすべてのセキュリティスキャンが、完全に停止されます。
- **レポートと除外:** ダウングレード後に存在しないポリシーに一意に割り当てられた既存のレポートまたは除外はすべて、完全に削除されます。
- **統合:** 新しいライセンス階層に含まれていない統合は削除されます。

残りの構成への影響

一部の項目はコンソールに残りますが、基礎となるライセンスデータなしでは機能が異なります。

- **カスタムポリシー:** 既存のカスタムポリシーはそのまま残りますが、その中のライセンスのないコンポーネントにはプレースホルダーが表示されます。猶予期間が経過すると、これらのポリシーは、ライセンスのない情報の結果を返さなくなります。
- **検出結果の自動化:** ライセンスのない検出結果に基づく自動化は、結果を返さなくなりますが、削除されません。Tenable では、ダウングレード後にこれらを確認し、収集されなくなったデータを追跡しようとしていないことを確認するよう推奨しています。
- **監査の自動化:** ライセンスのない機能に基づく自動化は、結果を返さなくなりますが、削除されません。

  > **注意:** 自動化内では、[アクション] セクションに関連する次の動作に注意してください。
  > - ライセンスのないプラットフォーム機能に関連するアクションタイプは、関連する設定画面に引き続き表示されますが、結果は返されなくなります。
  > - JIT のライセンスが終了した場合、[JIT 利用資格] および [JIT アクセスリクエスト] のアクションタイプは表示されなくなります。

- **JIT:** JIT 利用資格とアクセスリクエストは、既存の自動化から削除されます。
- **検索およびクエリツール:** プラットフォーム全体 (エクスプローラー、カスタムダッシュボードなどを含む) でクエリベースのフィルタリングおよび検索メカニズムを引き続き使用できますが、ライセンスのない機能ではデータ結果が返されなくなります。

管理者のためのダウングレード後のチェックリスト

クリーンな環境を確保し、技術的なエラーを防ぐために、管理者は次の作業を手動で実行する必要があります。

- **ライセンスのないアウトポストの削除:** ライセンスの対象外となった機能のためにアウトポストをデプロイしている場合は、手動で削除する必要があります。
- **適切な規模のクラウドアクセス許可:** Tenable では、新しい階層に合わせてクラウド IAM ロールとアクセス許可を更新することを推奨しています。クラウド環境内で Tenable に付与されるアクセス許可を減らすには、更新されたオンボーディングスクリプトを確認し、そのスクリプトに基づいて環境認

証をスケールダウンするか、製品のドキュメントを使用して新しいライセンス階層に必要な正確なアクセス許可を確認します。

猶予期間を手動で終了する

移行は**30日後**に永続的になります。その時点で、ライセンスのない機能に関連するすべてのデータ、検出結果、カスタムポリシー、レポート、自動化は完全に削除されます。

新しいライセンスにすぐに移行してサードパーティ¯からのスキャン料金を停止したい場合は、管理者ロールを持つユーザーが猶予期間バナーの**[猶予期間の終了]**を手動でクリックできます。このアクション(最大24時間かかる場合があります)によって、ライセンスのないスキャンが停止し、ライセンスのないデータが削除されます。

ライセンスの回収

リソース使用量がライセンスの制限を超えた場合、クラウドサイバーエクスポージャーではさまざまな方法でライセンス消費を積極的に管理し、削減することができます。Tenableはリソースがインベントリから削除されたとき(次回のデータの同期と更新の頻度中に)、ライセンスを自動的に回収しますが、以下に概説する戦略により、ライセンスのフットプリントを直接管理することもできます。現在のライセンス消費の詳細については、クラウドサイバーエクスポージャーライセンス使用状況およびリソース別のライセンス使用状況データのエクスポートを参照してください。

次の表ではライセンスの回収方法と、ライセンス数を削減するために利用できるその他のメカニズムについて説明しています。

> **注意:** 以下の表のプロアクティブな方法を実行する場合、お使いの環境で次にデータの同期と更新の頻度ときに、ライセンス数の更新が反映されます。

特定のリソースタイプと請求対象の比率の詳細については、請求対象のリソースを参照してください。

製品の機能	ライセンスの回収方法
モニタリング	AWS、Azure、GCP、またはOCIのアカウントを除外する

製品の機能	ライセンスの回収方法
ワークロード保護	ワークロード
データ保護[1]	• データ[2] • データ[2] • データ • データ
JIT アクセス[1]	使用資格のあるリクエスト者の数を減らすために、使用資格の管理する

[1] これらのリソースは、**Cloud Vulnerability Management** ライセンスには関係ありません。

[2] スキャン後の請求が無効になっている

FAQ (よくある質問)

このセクションでは、ライセンスに関連する、よくある質問を紹介します。

脆弱性管理

> 本番コンテナリポジトリの請求対象のリソース (ACR、ECR など) はどのように計算されますか?

クラウドプロバイダー管理でもサードパーティでも、コンテナリポジトリの請求は、次のように計算されます。

- リポジトリ内のイメージの数ではなく、**リポジトリの数**に基づいて請求されます。
- 毎日、Tenable は過去 2 日間にスキャンされたリポジトリをチェックし、それらを請求対象のリソースとしてカウントします。
- アカウントごとに、ワークロード設定で**リポジトリスキャンを無効**にできます。

> CI/CD コンテナリポジトリの請求対象のリソース (JFrog、GitLab など) はどのように計算されますか?

回答: CI/CD コンテナリポジトリの請求書は、次のように計算されます。

- 定義された保持期間中に保持された個別のリポジトリ名の数に基づいて計算されます。
- Tenable は、デフォルトで少なくとも 1 か月分のスキャン履歴を保持しますが、スキャンボリュームによって最大 2 か月分を保持することもあります。
- 保持期間とスキャンされた個別のリポジトリ名の数の両方に基づいて、請求対象のリソース数が増えます。

> CI/CD コンテナリポジトリのスキャンデータの保持期間はどれくらいで、その期間は請求にどのように影響しますか?

回答: CI/CD コンテナリポジトリのスキャンデータはデフォルトで **30 日**保持されますが、ご要望に応じて延長可能です。保持期間が長いほど、保存される履歴が多くなり、カウントされる固有のリポジトリも増えるため、請求も増えます。1 つのリポジトリが同じ保持期間内に複数回スキャンされた場合は、1 回としてカウントします。ただし、リポジトリの名前が変更されると、別のエンティティとしてカウントされ、コストも増加します。

例: 30 日間の保持期間

- **12 月**: 合計 10 個のリポジトリがスキャンされました。
- **1 月末**: 12 月の 10 個のリポジトリと一緒に、1 月から新しい 5 つのリポジトリが保持されました (合計 15 個)。
- **2 月 1 日**: 12 月のデータが削除され、1 月からの 5 つのリポジトリだけが残ります。

ライセンス別機能比較

各ライセンスは、以下の表に示すとおり、異なる一連の機能をサポートしています。ライセンスの詳細については、Tenable の担当者までお問い合わせください。

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
対象プラットフォーム/環境	AWS、Alibaba Cloud、Azure、GCP、OCI	✓	✓	✓	✓	✓	✓
	フェデレーションアイデンティティプロバイダー (例: Ping Identity、Microsoft Entra ID、Okta)	✓	✓	✗	✓	✓	✓
	ソブリンクラウド (例: 米国ガバメントクラウド)	✓	✓	✓	✓	✓	✓
リスク評価と修正	クラウドインベントリの検出	✓	✓	✓	✓	✓	✓
	組み込みリ	✗	CIEM	VM	ワークロー	✓	✓

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
	スクポリシー				ド、 コンピュート、 Kubernetes、 シークレット、ログ、 管理、モニタリング、 およびネットワーク		
	カスタムリスクポリシー	✗	CIEM	✗	ワークロード、 コンピュート、 Kubernetes、 シークレット、ログ、 管理、モニタリング、 およびネットワーク	✓	✓
	除外	✓	✓	✓	✓	✓	✓

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
	動的ネットワークエクスポージャー	✗	✗	✗	✓	✓	✓
	コンプライアンス管理	✓	CIEM	VM	✓	✓	✓
	AI-SPM	✗	✗	✗	✓	✓	✓
コードとインフラのコード化	CI/CD パイプライン / リポジトリ	✗	✗	✗	✗	✓	✓
KSPM	インベントリ	✗	✗	✗	✓	✓	✓
	設定ミス	✗	✗	✗	✓	✓	✓
	最小権限の推奨事項	✗	✗	✗	✗	✓	✓
	アドミッションコントローラー	✗	✗	✗	✗	✗	✓
高度なアイデンティティと	アイデンティティ関連最小権限の推奨事項	✗	✓	✗	✗	✓	✓

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
アクセス管理							
	リソースベース最小権限の推奨事項	✗	✓	✗	✗	✓	✓
	オンデマンド最小権限の推奨事項	✗	✓	✗	✗	✓	✓
	アクセス許可クエリ	✗	✓	✗	✗	✓	✓
	アイデンティティインテリジェンス	✗	✓	✗	✗	✓	✓
	過剰なアクセス許可	✗	✓	✗	✗	✓	✓
	アクティビティログイベント	✗	30 日	✗	✗	30 日	30 日
脆弱性管理[1]	脆弱性診断 - エージェントレス	✗	✗	✓	✓	✓	✓
	脆弱性診	✗	✗	✓	✓	✗	✓

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
	断 - アカウント内						
	脆弱性診断 - エージェント経由 (Kubernetes、オンプレミス)	✗	✗	✗	✓	✗	✓
	脆弱性診断 - コンテナレジストリ	✗	✗	✓	✓	✓	✓
	保存された機密データ (シークレット、PII、PCI、PHI)	✗	✗	✗	✓	✓	✓
	CI/CD コンテナイメージのスキャン	✗	✗	✗	✓	✓	✓
	SBOM (ソフトウェアインベントリ)	✗	✗	✓	✓	✓	✓

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
データ保護	マネージドデータベース	✗	✗	✗	✗	✓	✓
	オブジェクトストレージ (バケット)	✗	✗	✗	✗	✓	✓
	保存された機密データ (シークレット、PII、PCI、PHI)	✗	✗	✗	✗	✓	✓
	データプラットフォーム (Snowflake など)	✗	✗	✗	✗	✗	✓
	ディスクとボリューム	✗	✗	✗	✗	✓	✓
クラウド検出と対応	クラウドイベント (エージェントレスモニタリング)	✗	✗	✗	✗	✗	90 日
	ランタイムイベントと検出	✗	✗	✗	✗	✗	90 日

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
	(センサーベースのモニタリング)						
	異常検出	✗	✗	✗	✗	✓	✓
	悪意のあるファイルの検出	✗	✗	✗	✓	✓	✓
プラットフォーム	API アクセス	✓	✓	✓	✓	✓	✓
	エクスプローラー	✓	✓	✓	✓	✓	✓
	プロジェクト	✓	✓	✓	✓	✓	✓
	Hexa AI	✓ [2]	✓ [2]	✓	✓	✓ [2]	✓
	ダッシュボード	✓	CIEM	VM	ワークロード、脆弱性、コンプライアンス、管理	✓	✓
	レポート	✗	CIEM	VM	ワークロード、	✓	✓

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
					脆弱性、コンプライアンス、管理		
	統合	✓	✓	CSP、コンテナレジストリ、チケッティングとITSM、コラボレーション、SIEM、Webhook	CSP、コンテナレジストリ、チケッティングとITSM、コラボレーション、SIEM、Webhook、ネットワーク、Kubernetes	✓	✓
	自動修正	✗	✓	✗	✓	✓	✓
	ロールベースのアクセス制御	✓	✓	✓	✓	✓	✓
	SSO	✓	✓	✓	✓	✓	✓
	グラフベースの分析	✗	アイデンティ	✗	ネットワークグラフ	✓	✓

カテゴリ	機能	JIT	CIEM	Cloud VM/ Foundation	Advanced	Standard	Enterprise/ CNAPP Complete
			ティグラフ				
Tenable JIT アクセス	使用資格の管理	✓	✓	✗	✗	✓	✓
	アクセスのリクエスト	✓	✓	✗	✗	✓	✓
	アクセスリクエストのレビュー	✓	✓	✗	✗	✓	✓
	監査証跡情報の表示	✓	✓	✗	✗	✓	✓

[1] 仮想マシンとコンテナ化されたワークロードが対象

[2] Hexa AI は、Tenable One ライセンスの一部として購入されたすべてのライセンスで利用できます。

Tenable のツールに関する上記の情報は、一般的な情報提供のみを目的としています。お客様の組織に適用可能なツールは、Tenable とお客様の組織との間で締結された注文書またはその他の契約書に従うものとします。この製品は、それぞれの注文書またはその他の契約書に含まれるいかなる条項や条件の修正、補足、改正も意図したものではありません。

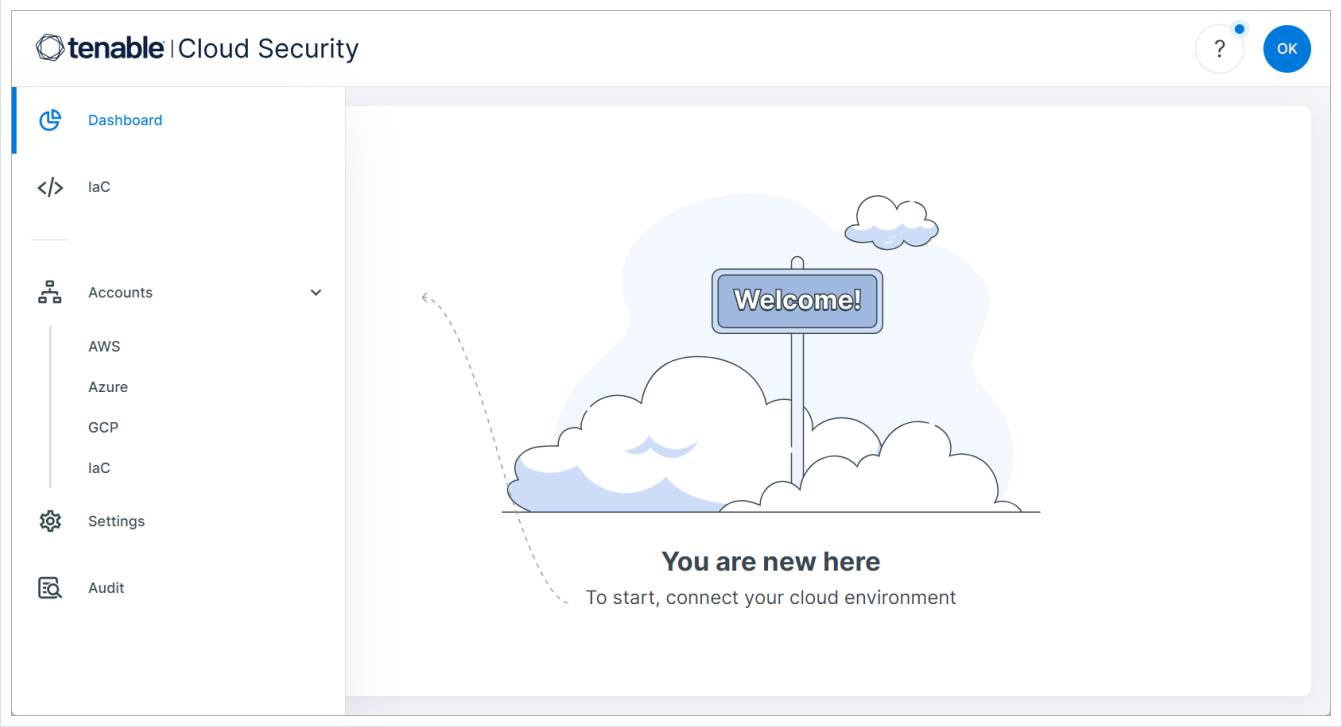
環境のセットアップ

Tenable One Cloud Exposure で作業を開始できるように環境をセットアップする方法

1. リージョンに基づいて提供されたURLを使用して、クラウドサイバーエクスポージャーにログインします。

   詳しくは、リージョン別のTenableコンソールURLを参照してください。

   注意: URLに反映されたリージョンによって、クラウドサイバーエクスポージャーAPIへのアクセス時に使用されるAPIエンドポイントが決まります。



2. 統合をクラウドサイバーエクスポージャーに接続します。
3. 統合 (IdP) をクラウドサイバーエクスポージャーと統合します。
4. SSO経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効化します。
5. アカウント階層とフォルダーをクラウドサイバーエクスポージャーで行います。
6. 必要に応じて、ユーザーとグループを追加設定します。
7. オプションのインバウンドとアウトバウンドの統合を設定します。

EAとパブリックプレビュー

Tenable One Cloud Exposure では、環境のセキュリティに役立つ新機能を定期的に導入しています。これらの機能への早期アクセスを提供するために、Tenable は 2 つの異なるフェーズで特定の機能をリリースしています。

- **早期公開 (EA)**
- **パブリックプレビュー**。

早期公開とは何ですか?

早期公開は、Tenable が一部のお客様のグループに新機能へのクローズドアクセスを提供するゲートフェーズです。すべてのユーザーに公開されるパブリックプレビューとは異なり、EA の特長は通常「オンデマンド」であり、ユースケースが機能の開発目標と一致している組織向けに特に有効です。

パブリックプレビューとは

パブリックプレビューとは、まだ調整段階の Tenable の新しいコンセプトや機能をユーザーに紹介するフェーズです。この段階で機能をリリースするのは、機能の目的を理解してもらい、機能が一般公開 (GA) される前にフィードバックを収集するためです。

パブリックプレビューの機能は利用できますが、次の点で GA 機能とは異なる場合があります。

- **機能の進化:** ユーザーインターフェース、機能性、基盤となるロジックは、フィードバックに基づいて頻繁に変更される可能性があります。
- **機能的なギャップ:** 特定の側面またはサブ機能は、Tenable が GA 機能で提供するものと異なる場合があります。

パブリックプレビュー機能の識別方法

これらの機能は、クラウドサイバーエクスポージャーメニュー内の機能名の横にある**プレビュー**タグで簡単に識別できます。これらのタグは、機能が利用可能であるものの、お客様のフィードバックに基づいて積極的に調整されているフェーズにあることを示します。

EA とパブリックプレビューの主な違い

どちらのフェーズもフィードバックを収集することを目的としていますが、範囲とサポートが異なります。

- **アクセス**: EA はリクエストまたは招待に応じて利用できる**クローズドベータ版**ですが、パブリックプレビューの機能は**プレビュー**タグを介してメニュー内のすべてのユーザーに表示されます。
- **サポート**: パブリックプレビューは、既存のサポートチャネルを通じてサポートされています。対照的に、EA の機能は公式サポートなしで提供されます。代わりに、Tenable は参加しているお客様と協力してコンセプトを改善します。
- **リリースまでの道のり:** EA の機能は、パブリックプレビューフェーズに移行することも、改良後に直接一般公開 (GA) に移行することもあります。
- **コミットメント**: EA は「約束なし」のフェーズであり、より広範な顧客基盤にとってはまだ関心がない可能性のあるコンセプトを検証するために使用されます。

FAQ (よくある質問)

> Tenable がプレビューで機能をリリースするのはなぜですか?

パブリックプレビューによって新しいツールへの早期アクセスを提供することで、Tenable は特定の機能や API 構造に対する最終的なコミットを行わなくても、開発を加速させることができます。このアプローチにより、以下が可能になります。

- コラボレーションによるフィードバックループを構築する
- 将来の機能に関する情報を早期に共有できる
- お客様の懸念事項に、より適切に対処するのに役立つ
- 一般公開する前に、市場のニーズに合わせて機能を調整する能力を高める

> プレビューの機能は、いつ一般公開 (GA) されますか?

開発タイムラインは機能の複雑さと受け取ったフィードバックによって異なりますが、パブリックプレビューの機能は通常数か月以内に GA に移行します。

> プレビューの機能を使用する際、データのセキュリティは確保されますか?

はい。機能はプレビュー段階であっても、Tenable のコアデータ保護、プライバシー保護、セキュリティ標準は通常と同じように完全に有効です。

プレビューの機能についてサポートを受けるには、どうすればよいですか?

プレビューの機能に関して技術的サポートが必要な場合やご質問がある場合は、既存のサポートチャネルを通じて、クラウドサイバーエクスポージャーにお問い合わせください。Tenable サポートチームが、お客様による新機能の評価に応じてガイダンスを提供いたします。

フィードバックを行うにはどうすればいいですか?

Tenable は、最終的な GA で質の高い機能をリリースするために、プレビュー段階でのご意見およびご感想を歓迎します。プラットフォーム内で提供されているフィードバック機能または標準のサポートチャネルを使用してフィードバックをお寄せください。

早期公開に参加する理由は何ですか?

EA の機能を活用することで、次のことが可能になります。

- **Tenable のプロダクトマネージャーとの共同フィードバックループ**を通じて、製品ロードマップに直接影響を与えます。
- 特定のニッチな環境ニーズに対応する今後実装予定の機能を、ファイナライズされる前に試します。
- 今後実装予定の機能がユースケースに役立つように、フィードバックを提供します。

機能が早期公開 (EA) 中かどうかを確認するにはどうすればよいですか?

EA の機能は、2 つの方法で識別できます。

- **ドキュメント**: EA の機能は、リリースノートまたは特定の機能のドキュメント内で EA フェーズにあるものとして明示的に記載されます。
- **招待**: Tenable の担当者から、特定の機能に関する EA フェーズへの参加に直接招待される場合があります。

サポートへの問い合わせ

Tenable のサポート専門家は 24 時間 365 日体制で対応しています。Tenable Connect、電話、チャットなど、お客様にとってご都合のよい方法でお問い合わせいただけます。

テクニカルサポートでケースをオープンする

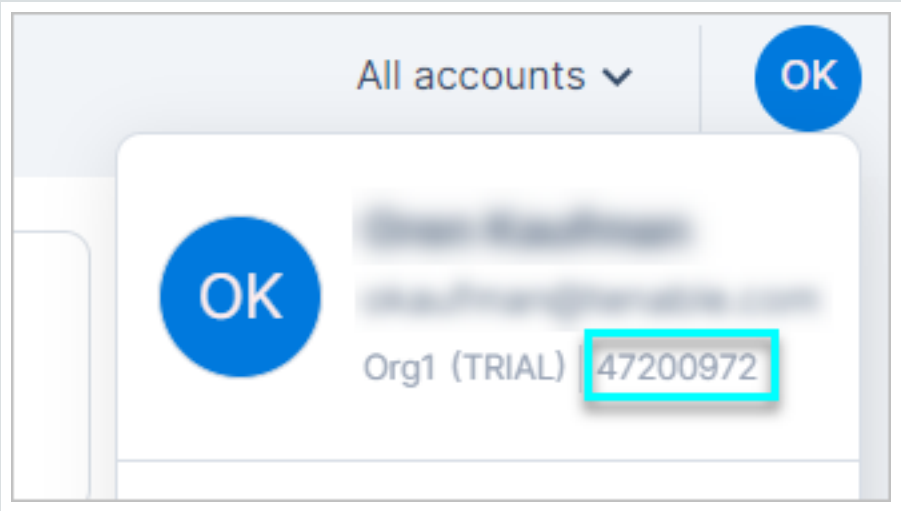
テクニカルサポートでケースをオープンする方法

- Tenable Connect (https://connect.tenable.com) にログインし、**[サポート]** > **[テクニカルサポート]** の順に移動します。現在の登録ステータスによっては、お客様はすでに Connect アカウントを持っている可能性があります。登録する場合は、Tenable Connect への登録を参照してください。
- こちらをクリックすると、テクニカルサポートに関するその他の情報や Tenable へのお問い合わせ方法などを確認できます。
- Tenable Connect にログインできない場合は、所属組織のプライマリ連絡先に連絡して、アカウントが正しく設定されているかご確認ください。
- テクニカルサポートに電話で問い合わせる場合は、こちらに記載されている番号のいずれかをご使用ください。

Tenable Connect への登録

Tenable Connect に登録する方法

1. ページ右上にある **[登録]** を選択します。
    - **顧客 ID** (注文書メールに記載) を入力します。顧客 ID は、Tenable One Cloud Exposure コンソールのユーザープロファイルにも表示されています。



- 注文書に表示されている正確な会社名を入力します。
- メールアドレスのドメインは、アカウントで承認されたドメインと一致する必要があります。

> **重要:** 顧客 ID がわからない場合は、フォームに入力しないでください。誤った情報を送信すると、アカウントの連携に遅延が生じる場合があります。

2. 登録すると、パスワード作成のためのメールが送信されます。
3. リセット後、同じ認証情報を使用して、コミュニティ (connect.tenable.com) にログインします。

Tenable Office Hours

Tenable のセキュリティエンジニアが毎週開催するセッションで、皆さまのご質問にお答えし、クラウドサイバーエクスポージャー や他の Tenable 製品の使用に関するベストプラクティスを紹介しています。

Tenable のツールについてご質問がある場合は、毎週開催されるウェビナー「Office Hours」にご参加ください。Tenable のセキュリティエンジニアが主導するこのセッションは、ディスカッションやデモを通じて課題に対処し、ベストプラクティスを共有するオープンなフォーラムです。

参加をご希望の場合は、こちらでご登録ください。Tenable Community ではすべてのセッションのリプレイをご覧いただけます。

Tenable One

Tenable One は、世界で唯一の AI 搭載型サイバーエクスポージャー管理プラットフォームです。Tenable One は、アタックサーフェス全体にわたるセキュリティの可視性、インサイト、アクションを根本的に一元化し、現代の組織が IT インフラからクラウド環境、重要インフラ、そしてそれらの間のあらゆる場所まで、優先度の高いサイバー空間に露呈されたリスクを分離して根絶できるようにします。

Tenable One Cloud Exposure の Tenable One への拡張

> **必要なライセンス:** この拡張には Tenable One のライセンスが必要です。Tenable One の試用に関する詳細については、Tenable One を参照してください。

クラウド サイバーエクスポージャー を Tenable One と統合すると、次の機能を活用できます。

- Lumin Exposure View で、ビジネス上の重要な文脈を得て、クラウドとハイブリッドのサービス、プロセス、機能に関するビジネスに即した CES (サイバーエクスポージャースコア) を取得します。全体的なクラウドリスクを追跡し、総合的な Cyber Exposure Score (CES) に対するクラウド資産とアイデンティティのリスクの影響を、資産タイプ別、クラウド ベンダー別、またはタグ別などで確認します。
  - **グローバル**のエクスポージャーカードを確認して、総合的なスコアを把握します。**[サイバーエクスポージャーごと]** をクリックすると、スコアに影響を与えている要因とその程度を把握できます。
  - **クラウド サイバーエクスポージャー**のエクスポージャーカードを確認します。
  - Exposure View を設定して、自社のポリシーに基づいて**修正 SLA** と **SLA 効率**を設定します。
  - ビジネス上の文脈 (クラウド リソースタイプ、資産重要度、アプリケーションをサポートするリソース、内部/外部のウェブアプリケーション、開発/テスト/本番環境など) に基づいて、カスタムエクスポージャーカードを作成します。
- Tenable Inventory では、資産のインテリジェンスを強化し、関連する攻撃経路、タグ、エクスポージャーカード、ユーザー、関係性など、資産に関するより深いインサイトを取得します。総合的な資産リスクと資産重大度を評価する AES (資産のエクスポージャースコア) により、資産のエクスポージャーをより包括的に把握することで、リスクスコアリングを改善します。
  - クラウド サイバーエクスポージャー の資産を確認して、インターフェースの戦略的性質を理解します。これは、Tenable Inventory 内でどの機能をいつ使用するかについて想定するのに役

立ちます。

- 使用、編集、ブックマークできるTenableクエリを確認します。
- グローバル検索クエリビルダーとそのオブジェクトおよびプロパティについて理解を深めます。後で使用できるようにカスタムクエリをブックマークします。

  > **注意:** 利用可能なプロパティをすばやく表示する方法
  > - クエリビルダーで、**has** と入力します。候補の資産プロパティのリストが表示されます。
  > - 列を追加してリストをカスタマイズします。利用可能な列/プロパティのリストが表示されます。

- 「資産の詳細」ページにドリルダウンして、資産のプロパティと関連するすべての詳細情報ビューを表示します。
- (オプション) 異なる資産クラスを組み合わせたタグを作成します。

- Attack Path Analysis で、マルチクラウド環境とハイブリッド環境全体にわたるリスクの高い攻撃経路を明らかにすることでリスクの優先順位付けを最適化し、重大な影響を回避します。軽減策ガイダンスを使用して攻撃経路を遮断するためのチョークポイントを特定することで軽減策を合理化し、AI インサイトを使用して深い専門知識を取得します。
  - Attack Path Analysis ダッシュボードで、脆弱な資産の概要を示すビューを表示します。これには、これらの重要資産に至る攻撃経路の数、未解決の検出結果の数とその深刻度、さまざまなソースノードのエクスポージャースコアや ACR ターゲット値のさまざまな組み合わせを持つ経路を表示するマトリクス、トレンドとなっている攻撃経路のリストなどがあります。
    - **上位の攻撃経路マトリクス**を確認し、**上位の攻撃経路**のタイルをクリックして「重要資産」、すなわち機密ラベルを持つクラウドリソースに関する詳細情報を表示します。

    必要に応じてこれらを調整し、最も危険度の高い攻撃経路のデータと検出結果を表示できます。
  - 「検出結果」ページでは、データを高度なグラフ分析および MITRE ATT&CK® フレームワークと組み合わせて検出結果を作成し、1 つ以上の重要資産につながる 1 つ以上の攻撃経路で見られたすべての攻撃手法を確認できます。これにより、資産や情報に対する脅威の影響を発生させそれを増幅させる未知の要素を把握し、対処することができます。
  - 「検出」ページで、次のように攻撃経路クエリを生成し、資産を潜在的な攻撃経路の一部として表示します。

- ビルトインクエリを使用して攻撃経路を生成する
- 資産クエリビルダーを使用して資産クエリを生成する
- 攻撃経路クエリビルダーを使用して攻撃経路クエリを生成する

その後、攻撃経路クエリと資産クエリのデータをクエリ結果リストとインタラクティブなグラフから表示して操作できます。

環境サイジングガイド

このガイドでは、AWS、Azure、GCP、OCI、Snowflake などのマルチクラウド環境全体で請求対象のリソースを検出するためのサイジングスクリプト実行方法について説明します。これらのスクリプトは、過去の平均ではなく、環境の「リアルタイム」のポイントインタイムスナップショットをキャプチャします。結果を確認する際は、リソース数が想定と一致することを確認し、潜在的な有機的成長を考慮してから、最終出力ファイルを Tenable の担当者と共有して価格設定を確認してください。

注意: サイジングスクリプトはほかのリソースを検出できません。それらのリソースは追加のコストが発生するため、手動で集計するようにしてください。

請求対象のリソース

Tenable One Cloud Exposure は、環境内で検出されたリソースに基づいてスケーリングを行います。請求対象のリソースには、以下のようにさまざまなタイプがあります。

- **コンピューティングリソース:** VM、コンテナホスト、サーバーレス機能などのコアワークロード
- **スキャンベースのリソース (オプトイン):** アクティブスキャンが有効な場合にのみ請求される追加リソース (コンテナリポジトリ、VM イメージ、データ保護 (バケット/データベース) など)

スクリプトは、未加工のリソース数 (Lambda 関数または S3 バケットの総数など) を提供します。これらの合計は、特定の比率 (サーバーレス関数の場合は 10:1 など) に基づいて請求対象ユニット数に変換されます。

これらの比率の内訳全体および最終的なライセンス数に与える影響については、**請求対象のコンピューティングおよびスキャンベースのリソース** セクションを参照してください。

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
コンピュート *Foundation*、*Advanced*、*CNAPP Complete*、*Cloud VM*、*CIEM*、*Standard*、*Enterprise*	**仮想マシン**	EC2 インスタンス	仮想マシン、VM スケールセットインスタンス	仮想マシンインスタンス	ACK を実行している ECS インスタンス	コンピューティングインスタンス	-
	コンテナホスト[2]	EKS/ECS を実行する EC2 インスタンス	AKS を実行する VM スケールセットインスタンス	GKE を実行する仮想マシンインスタンス	ACK を実行している ECS インスタンス	OKE を実行するコンピューティングインスタンス	Kubernetes ノード
	サーバー	Lambda 関数	App Servic	Cloud Functions	-	Functions	-

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
	レス関数[3]		es				
	サーバーレスコンテナ[3]	ECS サービス	コンテナインスタンス	Cloud Run、GKE Autopilot	-	-	-
スキャンベース ワークロード保護 *Foundation*、*Advanced*、*CNAPP Complete*、*Cloud VM*、*Standard*、*Enterprise*	**コンテナリポジトリ**[4]、[5]	ECR リポジトリ	コンテナリポジトリ	アーティファクトコンテナイメージリポジトリ	コンテナレジストリリポジトリ	-	CI/CD[3]、サードパーティレジストリの追加

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
	仮想マシンイメージ	EC2 イメージ	-	-	ACK を実行している ECS イメージ	-	-
	データディスク	EC2 インスタンスデータボリューム	• 仮想マシンデータディスク • 仮想マシ	VM インスタンスデータディスク	ECS ディスク	コンピューティングインスタンスデータボリューム	

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
			インスタンスデータディスクスケールセットインスタンスデータディスク				
スキャンベース データ保	**バケット**[3]	S3 バケット	ストレージアカウント	ストレージバケット	OSS バケット	オブジェクトストレージ	-

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
護 *CNAPP Complete、Standard、Enterprise*			Blob コンテナ			バケット	
	マネージドデータベース[3]	• DynamoDB • RDS インスタンス • RDS クラスタ	Azure SQL Server	• BigQuery データセット • SQL インスタンス	-	-	-
	データプラットフォームデー	-	-	-	-	-	Snowflake の接続ローカル、共有、マーケットプレイス

リソースタイプ/請求対象ライセンス[1]	カテゴリ	AWS	Azure	GCP	Alibaba Cloud	OCI	オンプレミス/その他
	タベース[3]						
JIT リクエスト者 *JIT、CIEM、Standard、CNAPP Complete、Enterprise*	**ユーザー**	AWS SSO ユーザー	Azure AD ユーザー	GCP ユーザー	-	-	• Okta ユーザー • OneLogin ユーザー • PingIdentity ユーザー

[1] リストされているライセンスのリソースは、請求対象の使用量としてカウントされます。リストにないライセンスのリソースも対象ですが、請求対象ではありません。

[2] これには、請求対象ユニットとして**仮想マシン** (1:1) が含まれます。

[3] これらのリソースは、**Cloud Vulnerability Management** ライセンスに関連していません。

[4] これらのリソースタイプは、**コンテナリポジトリ**内のイメージではなく、コンテナリポジトリ自体に基づいています。たとえば、コンテナ**リポジトリ**は、**同じコンテナの**イメージが 15 個でも 150 個でも、1 つの請求対象リソースと見なされます。

[5] 同じ**コンテナリポジトリ**が **CI/CD パイプライン**と**レジストリスキャン**の両方でモニタリングされている場合、これは 2 つの異なる請求対象リソースとして扱われます。

AWS

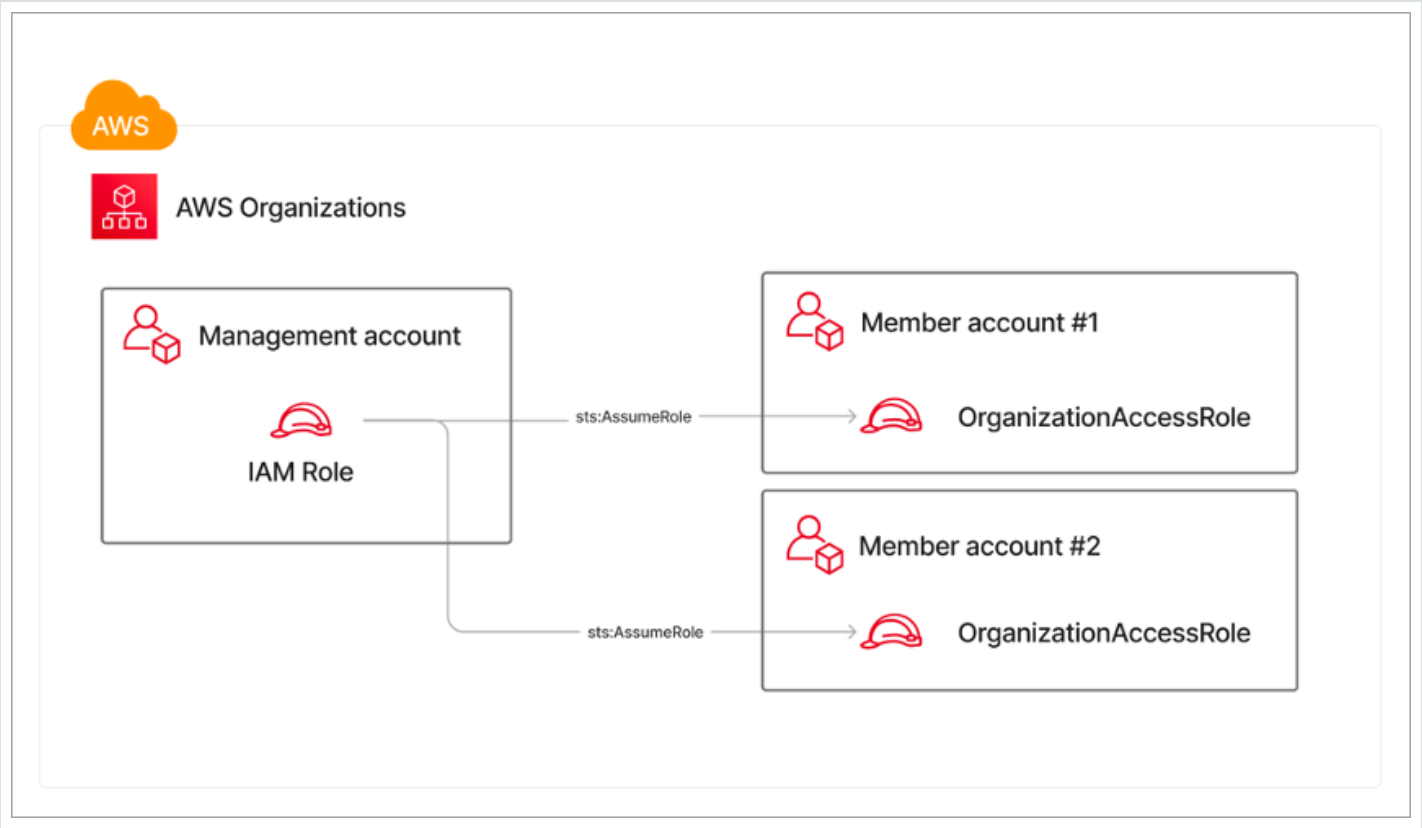
このセクションでは、AWS 環境内でサイジングスクリプトを実行するために必要な前提条件と実行手順を説明します。

前提条件

推奨設定

サイジングスクリプトは、単一の AWS 組織内の複数アカウントをスキャンするために次のアーキテクチャを前提としています。

> AWS 組織サイジング設定の図



上の図の説明

- サイジングスクリプトの実行に使用される IAM ロールは、管理アカウントに属しています。
- その IAM ロールには、すべてのメンバーアカウントの `sts:AssumeRole` に対するアクセス許可と、管理アカウント (ECS、EKS、EC2、Lambda、組織) でリソースのクエリを実行するためのアクセス許可が必要です。

上のアーキテクチャの例では、IAM ロールを使用してリソースのクエリを行い、メンバーアカウントでロールを引き受けています。また、サイジングスクリプトは、メンバーアカウントでロールを引き受ける IAM ユーザーの使用もサポートします。これには `--user-access-key-id` と `--user-secret-access-key`、または `--profile-name` フラグが使用されます。
さらに、メンバーアカウントで OrganizationAccountAccessRole とは異なるロール名を使用できます。これは `--organization-account-access-role-name` フラグを使用することで実現できます。

重要: AWS 組織を使用していない場合、またはすべてのメンバーアカウントで組織ロールが設定されていない場合でも、個々の AWS アカウントでサイジングスクリプトを実行し、結果を共有することができます。

- **CLI**: サイジングスクリプトを実行するには、次のツールをインストールします。
  - Python 3: インストール手順
  - pip: インストール手順
- **アクセス許可**
  - スクリプトを実行するには、次のアクセス許可を持つアイデンティティ (IAM ユーザーまたは IAM ロール) が必要です。
    - OrganizationAccountAccessRole IAM ロール (または類似) に対する sts:assumeRole アクセス許可
    - 請求対象のリソースにリストされているすべてのリソースの読み取り許可

  一元化されたアカウントからアクセスできる IAM ロールがない場合は、代わりに個別のアカウントでスクリプトを実行できます。

ダウンロード

URL https://tenable-utilities.s3.amazonaws.com/Sizing/AWS.zip から AWS サイジングスクリプトをダウンロードし、.zip を解凍してください。

手順

AWS 環境の請求対象のリソース数を収集するには、次の手順を実行します。

1. **pip を使用して必要なパッケージをインストールします**。
    - pip で必要なパッケージをインストールするには、次のコマンドを実行します。
      ```
      pip3 install -r requirements.txt
      ```
    - オプションの実行フラグ

カテゴリ	フラグ	説明
データ保護	`--exclude-data-resources`	オプション。データリソースを除外。
リージョン	`--use-optional-public-regions`	オプション。オプションのリージョンをスキャン。
Gov アカウント	`--us-gov`	オプション。US Gov アカウントをスキャン。

2. **次のいずれかのオプションでサイジングスクリプトを実行します**。
    - **デフォルトの認証情報を使用**: デフォルトの AWS CLI 認証情報を使用してスクリプトを実行するには、コマンド `python3 sizing.py -o <outputDir>` を実行します。
    - **IAM ユーザーのアクセスキーとシークレットを使用**: コマンド `python3 sizing.py -i <keyId> -k <keySecret> -o <outputDir>` を実行します。
        - パラメーター
            - `keyId` は、AWS 組織の管理アカウントにおける IAM ユーザーの AWS アクセスキー ID です。
            - `keySecret` は、同じアクセスキーのシークレットです。
    - **名前付きプロファイルを使用**: AWS CLI スクリプトを実行するために名前付きプロファイルを使用している場合は、`--profile-name` (または `-p`) パラメーターを使用してコマンド `python3 sizing.py -p <profileName> -o <outputDir>` を実行します。

3. **出力を確認します**。エラーと警告のスクリプト出力を確認します。アカウントの数が想定と一致することを確認してください。アクセス許可エラーまたはその他の問題により、一部のリソースにアクセスできないことがあります。

Alibaba Cloud

このセクションでは、Alibaba Cloud 環境内でサイジングスクリプトを実行するために必要な前提条件と実行手順を説明します。

前提条件

推奨設定

サイジングスクリプトは、単一の Alibaba Cloud リソースディレクトリ内の複数アカウントをスキャンするために次のアーキテクチャを前提としています。

- サイジングスクリプトの実行に使用される RAM ユーザーは、管理アカウントに属しています。
- その RAM ユーザーには、すべてのメンバーアカウントの `sts:AssumeRole` に対するアクセス許可と、管理アカウント (ECS、リソースマネージャー) でリソースのクエリを実行するためのアクセス許可が必要です。
- 各メンバーアカウントでは、`ResourceDirectoryAccountAccessRole` という名前の RAM ロール (アカウントがリソースディレクトリに追加されたときにデフォルトで作成) がクロスアカウントアクセスに使用されます。

`--organization-account-access-role-name` フラグを使用することで、メンバーアカウントで `ResourceDirectoryAccountAccessRole`以外のロール名を使用できます。

- スクリプトは、リソースディレクトリの管理アカウントから実行する必要があります。ルートユーザーまたは Alibaba Cloud アカウントの認証情報を直接使用しないでください。ルートユーザーにはロールを引き受けるアクセス許可がありません。代わりに、適切なアクセス許可を持つ RAM ユーザーを作成してください。

- リソースディレクトリを使用していない場合、またはすべてのメンバーアカウントで組織ロールが設定されていない場合でも、個々の Alibaba Cloud アカウントでサイジングスクリプトを実行し、結果を共有することができます。
- **CLI**: サイジングスクリプトを実行するには、次のツールをインストールします。
  - Python 3: インストール手順
  - pip: インストール手順
- **アクセス許可**
  - スクリプトを実行するには、次のアクセス許可を持つ、管理アカウントの RAM ユーザーが必要です。
    - `ecs:DescribeInstances` – 管理アカウントの ECS インスタンスをリストする
    - `sts:AssumeRole` – メンバーアカウントの `ResourceDirectoryAccountAccessRole` を引き受ける
    - `resourcemanager:GetResourceDirectory` – 組織メンバーシップを検出する
    - `resourcemanager:ListAccounts` – リソースディレクトリ内のすべてのアカウントをリストする

ダウンロード

URL https://tenable-utilities.s3.amazonaws.com/Sizing/Alibaba.zip から Alibaba Cloud サイジングスクリプトをダウンロードし、.zip コンテンツを解凍してください。

手順

Alibaba Cloud 環境の請求対象リソース数を収集するには、次の手順を実行します。

1. **pip を使用して必要なパッケージをインストールします**。
   - pip で必要なパッケージをインストールするには、次のコマンドを実行します。
     ```
     pip3 install -r requirements.txt
     ```
   - オプションの実行フラグ

カテゴリ	フラグ	説明
組織	`--organization-account-access-role-name`	オプション。メンバーアカウントで引き受けるカスタムロール名 (デフォルト: `ResourceDirectoryAccountAccessRole`)。

2. **次のいずれかのオプションでサイジングスクリプトを実行します**。
   - **環境変数を使用する**: 以下の環境変数を設定して、スクリプトを実行します。

     ```
     export ALIBABA_CLOUD_ACCESS_KEY_ID=<accessKeyId>
     export ALIBABA_CLOUD_ACCESS_KEY_SECRET=<accessKeySecret>
     python3 sizing.py -o <outputDir>
     ```

   - **CLI 引数を使用する**: 次のコマンドを実行します。

     ```
     python3 sizing.py -i <accessKeyId> -k <accessKeySecret> -o <outputDir>
     ```

     - パラメーター
       - `accessKeyId` は、管理アカウントの RAM ユーザーのアクセスキー ID です。
       - `accessKeySecret` は、同じ RAM ユーザーのアクセスキーのシークレットです。
       - `outputDir` は、スクリプトが出力ファイルを書き込むディレクトリです。
3. **出力を確認します**。エラーと警告のスクリプト出力を確認します。アカウントの数が想定と一致することを確認してください。アクセス許可エラーまたはその他の問題により、一部のリソースにアクセスできないことがあります。

Azure

このセクションでは、Azure 環境内でサイジングスクリプトを実行するために必要な前提条件と実行手順を説明します。

前提条件

- **CLI**: サイジングスクリプトを実行するには、次のツールをインストールします。
  - Python 3: インストール手順
  - pip: インストール手順
- **アクセス許可**
  - サイジングスクリプトを実行するためのアイデンティティには、閲覧者およびストレージ Blob データ閲覧者の組み込みロールが必要です。
  - (すべてのサブスクリプションからデータを収集するには) ルート管理グループにロールが割り当てられる必要があります。または、サイジング情報を取得する組織のサブセットごとに、スクリプトを複数回実行することもできます。

ダウンロード

URL https://tenable-utilities.s3.amazonaws.com/Sizing/Azure.zip から Azure サイジングスクリプトをダウンロードし、.zip を解凍してください。

手順

Azure 環境の請求対象のリソース数を収集するには、次の手順を実行します。

1. **pip を使用して必要なパッケージをインストールします**。
   - pip で必要なパッケージをインストールするには、次のコマンドを実行します。
     ```
     pip3 install -r requirements.txt
     ```
   - オプションの実行フラグ

カテゴリ	フラグ	説明
データ保護	`--exclude-data-resources`	オプション。データリソースを除外。
クラウド環境	`--cloud-environment`	オプション。デフォルトではパブリックパーティションをスキャン。可能な値は、**public**、**china**、**us_gov** です。

2. **サイジングスクリプトを実行します**。サイジングスクリプトを実行するには、コマンド `python3 sizing.py -t %TenantId% -o %OutputDir%` を実行します。
    - パラメーター
        - `%OutputDir%` は、スクリプトの出力パスです。
        - `%TenantId%` は、サイジングに必要な Azure AD テナント ID です。
3. **出力を確認します**。エラーと警告のスクリプト出力を確認します。サブスクリプションの数が想定と一致することを確認してください。アクセス許可エラーまたはその他の問題により、一部のリソースにアクセスできないことがあります。

GCP

このセクションでは、GCP 環境内でサイジングスクリプトを実行するために必要な前提条件と実行手順を説明します。

前提条件

- **CLI**: サイジングスクリプトを実行するには、次のツールをインストールします。
    - Python 3: インストール手順
    - pip: インストール手順
    - gcloud: インストール手順
- **アクセス許可**
    - 以下の手順を実行できるのは、組織内のすべてのプロジェクトに対して**ビューワー**のアクセス許可を持つユーザーです。
    - サイジングスクリプトを実行するアイデンティティには、次の組織スコープのロールバインディングが必要です。
        - ブラウザ
        - Cloud Asset ビューワー
        - Service Usage コンシューマ

- スクリプトの実行に使用されるクォータプロジェクトで Cloud Asset API を有効にする必要があります。

ダウンロード

URL https://tenable-utilities.s3.amazonaws.com/Sizing/GCP.zip から GCP サイジングスクリプトをダウンロードし、.zip を解凍してください。

手順

GCP 環境の請求対象のリソース数を収集するには、次の手順を実行します。

1. **pip を使用して必要なパッケージをインストールします**。
   - pip で必要なパッケージをインストールするには、次のコマンドを実行します。
     ```
     pip3 install -r requirements.txt
     ```
   - オプションの実行フラグ

カテゴリ	フラグ	説明
データ保護	`--exclude-data-resources`	オプション。データリソースを除外。

2. **サイジングスクリプトを実行します**。サイジングスクリプトを実行するには、コマンド `python3 sizing.py -oid <organization_id> -qpid <project_id> -o <output_dir>` を実行します。
   - パラメーター
     - `<organization_id>` は、サイジングに必要な GCP 組織 ID です。
     - `<project_id>` は、クォータプロジェクト ID です (API クォータはこのプロジェクトによって消費されます)。
     - `<output_dir>` は、スクリプトの出力パスです。

- オプションのパラメーター
    - `-pid <project_id>` は、サイズを設定する個別のプロジェクト ID です。
    - `-fid <folder_id>` は、サイズを設定するフォルダーの ID です (-pid と一緒には使用できません)。
3. **出力を確認します**。エラーと警告のスクリプト出力を確認します。プロジェクトの数が想定と一致することを確認してください。アクセス許可エラーまたはその他の問題により、一部のリソースにアクセスできないことがあります。

OCI

このセクションでは、OCI 環境内でサイジングスクリプトを実行するために必要な前提条件と実行手順を説明します。

前提条件

スクリプトを実行するには、次のアクセス許可を持つアイデンティティが必要です。`read all-resources`

ダウンロード

URL https://tenable-utilities.s3.amazonaws.com/Sizing/OCI.zip から OCI サイジングスクリプトをダウンロードし、.zip を解凍してください。

手順

以下に概説するように、必要な認証情報を使用して OCI CloudShell 内で、またはお使いのマシンでローカルにスクリプトを実行できます。次の手順で、OCI 環境の請求対象リソースの数を判断します。

オプションの実行フラグ

カテゴリ	フラグ	説明
データ保護	`--exclude-data-resources`	オプション。データリソースを除外。

OCI 環境の請求対象のリソース数を収集するには、次のオプションの手順を実行します。

- **OCI Cloud Shell でサイジングスクリプトを実行します**。
    1. **OCI コンソール**にログインして、**OCI Cloud Shell** を開きます。
    2. **設定アイコン**をクリックして、サイジングとユーティリティのスクリプトをアップロードし、**[Upload]** をクリックします。
    3. 次のコマンドを実行します。`python3 sizing.py --out-dir`
    4. 出力ファイルをダウンロードするには、**設定アイコン**をクリックし、**[Download]** を選択して、出力パスを指定します (例: `oci_sizing_2024-05-02-19-20-32/summary.csv`)。または、ホームディレクトリにアクセスします。
    5. エラーと警告のスクリプト出力を確認します。テナンシやのコンパートメントの数が想定と一致することを確認してください。アクセス許可エラーまたはその他の問題により、一部のリソースにアクセスできないことがあります。
- **ローカルマシンでサイジングスクリプトを実行します**。ローカルマシンでサイジングスクリプトを実行するには、まず関連する認証情報を取得する必要があります。
  設定ファイルの作成方法については、OCI ドキュメントを参照してください。
    1. サイジングスクリプトを実行する前に、次のツールがインストールされていることを確認します。
        - Python 3: インストール手順
        - pip: インストール手順
    2. コマンド `pip3 install -r requirements.txt` を使用して pip 経由で必要なパッケージをインストールします。
    3. サイジングスクリプトを実行するには、次のコマンドを実行します。
       `python3 sizing.py --user-ocid <UserOCID> --fingerprint <Fingerprint> --tenancy-ocid <TenancyOCID> --private-key-file-path <PrivateKeyFilePath> --region <Region> -o %OutputDir%.`
    4. **出力を確認します**。エラーと警告のスクリプト出力を確認します。コンパートメントの数が想定と一致することを確認してください。アクセス許可エラーまたはその他の問題により、一部のリソースにアクセスできないことがあります。

Snowflake

このセクションでは、Snowflake 環境内でサイジングスクリプトを実行するために必要な前提条件と実行手順を説明します。

前提条件

スクリプトを実行するには、**AccountAdmin** アクセス許可を持つアイデンティティが必要です。

ダウンロード

URL https://tenable-utilities.s3.amazonaws.com/Sizing/Snowflake.zip から Snowflake サイジングスクリプトをダウンロードし、.zip を解凍してください。

手順

請求対象のリソースの数を収集する方法

1. Snowflake ポータルを開いて、新しい Python ワークシートを作成します。
2. ワークシートにサイジングスクリプトコードをコピーして実行します。
3. エラーと警告のスクリプト出力を確認します。リソースの数が想定と一致することを確認してください。アクセス許可エラーまたはその他の問題により、一部のリソースにアクセスできないことがあります。

ほかのリソース

次の請求対象なリソースは、このサイジングスクリプトの範囲外です。これらのリソースの見積もりを手動で入力するか、環境が最終計算のために完全にオンボードされるまで待ちます。

カテゴリ	リソース
VM[1]	Kubernetes ノード
コンテナを実行している VM[1]	Kubernetes ノード

カテゴリ	リソース
コンテナを実行している VM[1]	セルフマネージド Kubernetes ノード (AWS、Azure、GCP)
コンテナリポジトリ[2]	コンテナリポジトリ
コンテナリポジトリ[3]	CI/CD 経由で検出されたコンテナリポジトリ

[1] **スキャン対象のリソース**にのみ適用されます。

[2] **スキャン対象のリポジトリ**のみが、請求対象とみなされます。

[3] 同一の**コンテナリポジトリ**が **CI/CD パイプライン**と**レジストリスキャン**の両方でモニタリングされる場合、2 つの異なる請求対象リソースとして扱われます。

コンソール (UI を使用)

概要

コンソールの操作

コンソールは、Tenable の中央コントロールパネルです。コンソールは、クラウド環境全体のセキュリティポスチャーを管理および評価するための包括的なインターフェイスを提供します。この記事では、必要な情報を見つけるのに役立つ主要なナビゲーション要素について説明します。

左側のナビゲーションメニュー

コンソールにログインすると、ダッシュボードページが表示されます。ここから、[ダッシュボード] ウィジェットを使用して環境内の潜在的なリスクを調査したり、左側のナビゲーションメニューを使用して製品の関連エリアに移動したりできます。

Administrator ユーザーの場合は、[Settings] メニューも表示されます。

> **注意:** 以下にリストされているメニュー項目は、選択したコンソールのフォーカスを選択しますでフィルター処理される場合があります。

メニュー項目	説明
ダッシュボード	資産数とセキュリティポスチャーのスナップショットを提示し、クラウド環境の包括的な概要を示します。
探索	Tenable One Cloud Exposureによって特定されたすべてのクラウドリソースの一元化された資産ビューと、セキュリティデータの分析と調査、アクセス許可のクエリ、アクティビティログのレビュー、異常な動作の特定のための追加ツール。
リスク	検出結果、過剰なアクセス許可、脆弱性、CI/CD スキャンなどのセキュリティリスクを評

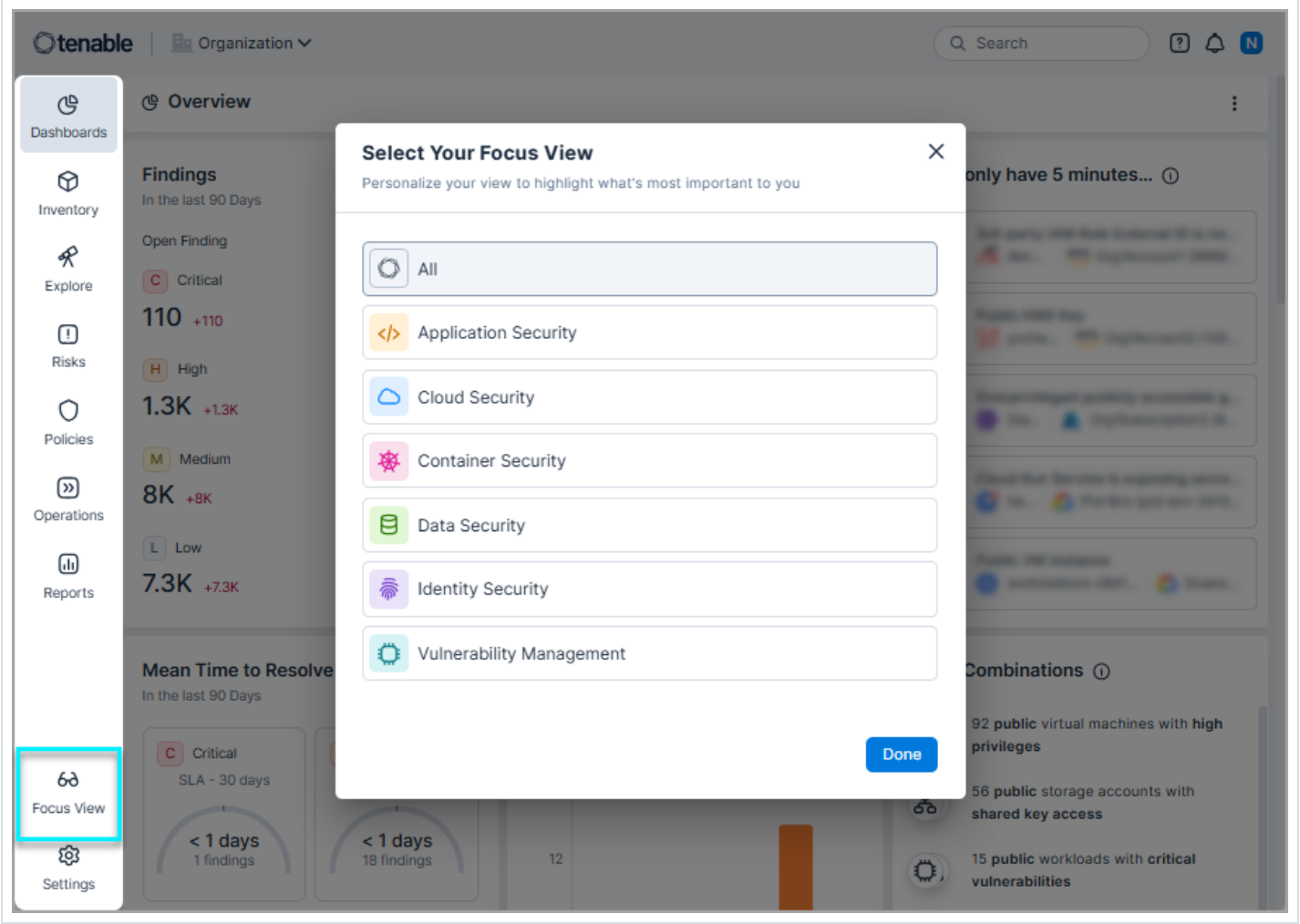
メニュー項目	説明
	価し、優先順位を付けます。
ポリシー	アイデンティティ、リソース、ネットワーク設定の自動ガードレールを定義して適用し、クラウド環境への不正アクセスを防止します。
業務	サードパーティのツールと統合し、サードパーティのツールにクラウドサイバーエクスポージャーデータを送信する自動化ルールを作成します。
レポート	資産インベントリ、設定ミス、サマリー、コンプライアンス情報に関する包括的なレポートを作成します。一般的な業界標準とセキュリティのベストプラクティスに関するコンプライアンスを確保します。

コンソールのフォーカスを選択します

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

コンソールビューをパーソナライズして、最も重要な機能を強調表示できます。**フォーカス**を設定すると、表示されているメニュー項目、ダッシュボードウィジェット、レポートをフィルタリングして選択したドメインに関連する情報にすることでユーザーエクスペリエンスを調整できるため、複雑さが軽減され、効率が向上します。

たとえば、データ保護を担当している場合は、フォーカスを **データセキュリティ** に設定して、機密データ漏洩に関連する検出結果、ダッシュボード、レポートのみがコンソールに表示されるようにすることができます。これにより、関連のない脆弱性やアクセスの問題を選別する必要がなくなり、自分のロールにとって最も重要なことに集中できるようになります。



フォーカス領域を選択するには:

1. 右上にあるユーザープロファイルアイコンをクリックし、**[フォーカスを選択]** をクリックします。
2. 次の重点分野から選択します。

重点分野	説明	関連するロール
	すべて	すべてのドメインをまとめて表示し、アイデンティティ、データ、ワークロード、設定など、組織のクラウドセキュリティ態勢を統合して表示
	アプリケー	IaC と CI/CD パイプラインの設定ミス、コード内のシークレット、ポリシー

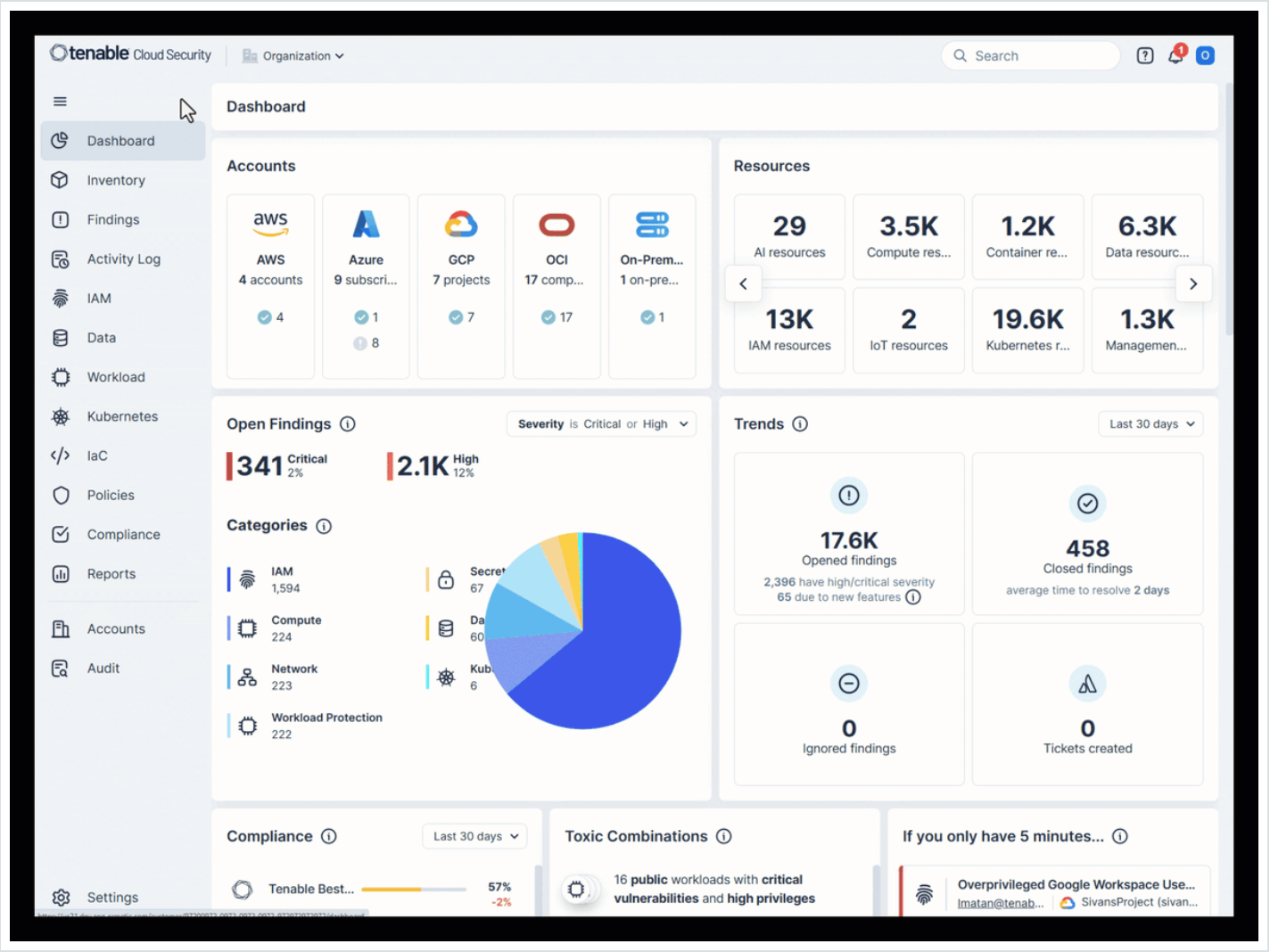
重点分野	説明	関連するロール
	ションセキュリティ	違反を特定することで、コードからクラウドまでのソフトウェア開発ライフサイクルのセキュリティに重点を置いています
	クラウドサイバーエクスポージャー	すべてのクラウドリソースにわたる設定ミス、コンプライアンスのギャップ、リスクを可視化し、全体的なクラウドポスチャーを強化します。クラウドセキュリティアーキテクト、セキュリティプラットフォームエンジニア
	コンテナセキュリティ	Kubernetesクラスタとコンテナ化されたワークロードのリスクと設定ミスをハイライトし、セキュアなオーケストレーションとデプロイメント を確保します。DevSecOpsエンジニア、ソフトウェアセキュリティエンジニア
	データセキュリティ	は、クラウド環境全体で機密データを検出、分類、保護することで、サイバーエクスポージャーを減らし、適切なデータ境界を確保することに重点を置いています
	ID およびアクセス管理	アイデンティティ、ロール、アクセス許可を調べて「誰が何ができるか」に答え、過剰な権限やリスクの高いアクセスパスの検出に役立ちます
	脆弱性管理	ホスト、コンテナ、ソフトウェア全体に脆弱性を浮かべて、修正に優先順位を付け、ワークロードのセキュリティ強化します。脆弱性管理エンジニア、セキュリティリスクアナリスト

製品内ヘルプ

コンソールから直接アプリ内ヘルプにアクセスします。製品ドキュメントは次のどちらからでもアクセスできます。

- コンソール全体の検索
- コンテキストヘルプリンク
  Open Findings

完全なドキュメントのサイトにアクセスするには、スライド式パネルの上部にある**ドキュメントポータル**リンクをクリックします。



ヘルプツール

コンソールの右上にあるクエスチョンマークのアイコンをクリックすると、各種のヘルプツールにアクセスできます。

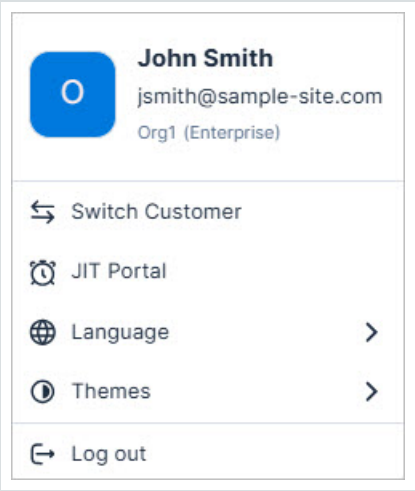
- **リリースノート**。最新リリースで クラウド サイバーエクスポージャー に追加された最新の機能と改善の説明。更新がないか頻繁に確認してください。リリースノートを参照してください。
- **ドキュメント**。技術的な質問に対する回答の検索や、クラウド サイバーエクスポージャー の使用方法の学習に役立つ包括的な製品ドキュメント。
- **API Explorer**。ブラウザ内ツールの GraphiQL を使用して、GraphQL クエリの記述、バリデーション、テストを実行します。詳細については、API を参照してください。
- **フィードバック**。コンソールから直接、クラウド サイバーエクスポージャー 製品チームにフィードバックを送信します。
- **お問い合わせ**。サポートへの問い合わせを参照してください。

ユーザープロファイル

コンソールの右上にあるアイコンをクリックして、自分のユーザープロファイルを開きます。ここから、以下のようなさまざまなアクションを実行できます。

- ユーザーの詳細の表示:
  - ユーザー名/メールアドレス
  - 会社・団体名
  - ライセンス
  - 顧客 ID。Tenable Community への登録に使用。詳細については、サポートへの問い合わせを参照してください。
- ナビゲーション:
  - [JIT ユーザーのみ] **JIT ポータル / コンソール**に移動します。クラウド サイバーエクスポージャー コンソールと JIT ポータルの両方にアクセスできる場合は、その間を容易に行き来できます。
  - [マルチテナントのみ]顧客 **を切り替えて**、別の組織のデータを表示します。
- 言語
  - 英語
  - 日本語

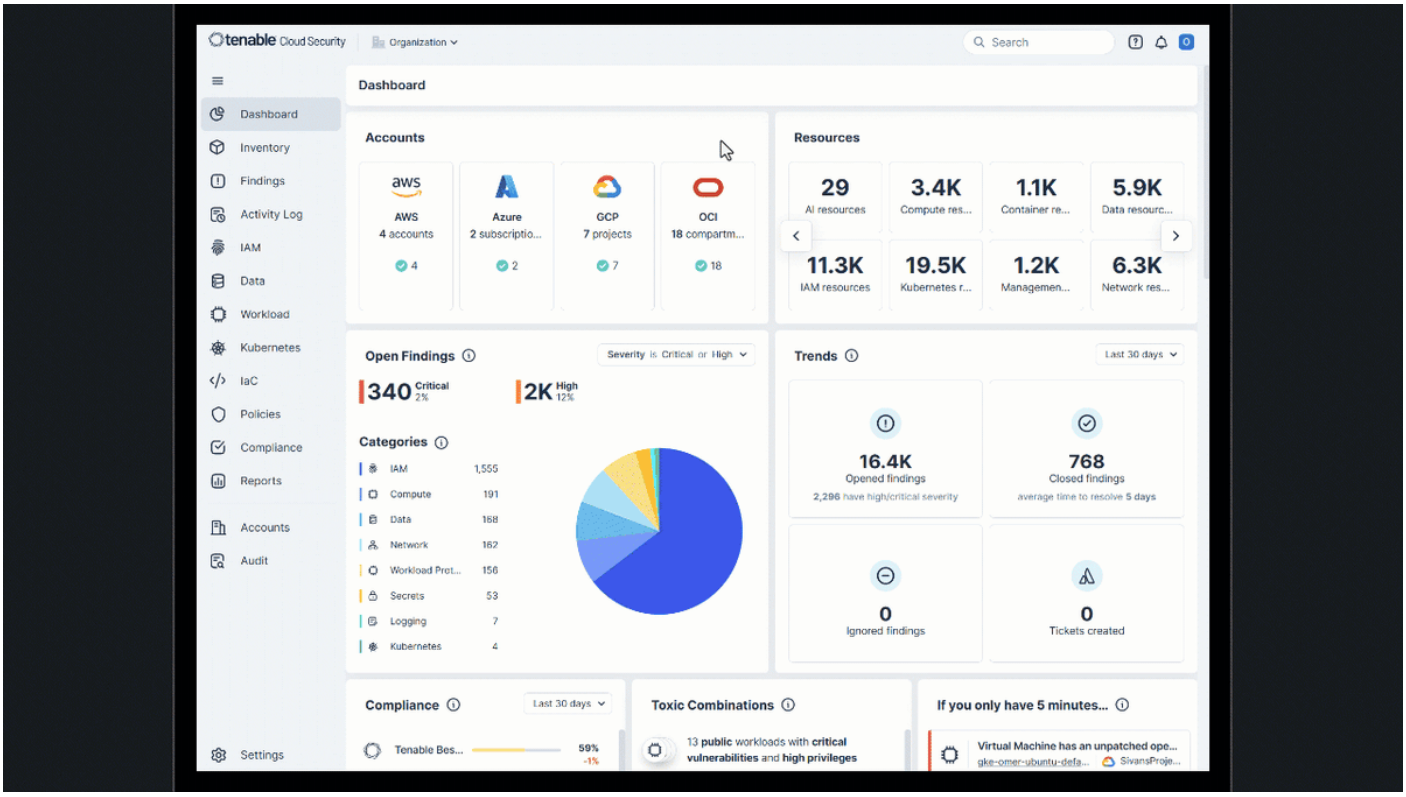
- テーマ
    - ライトモード
    - ダークモード
    - アクセス
- ログアウト



コンソール全体の検索

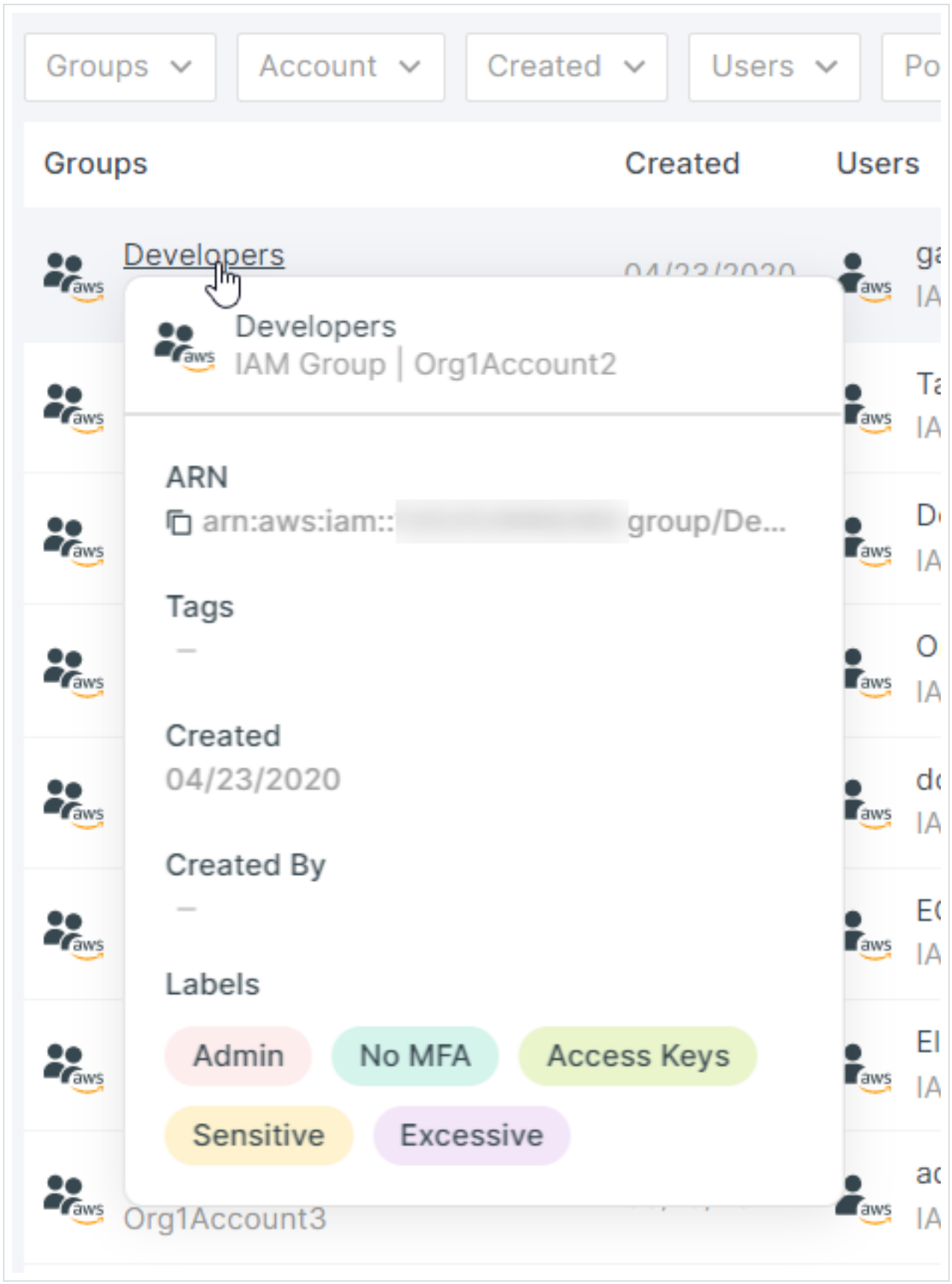
グローバル検索を使用して、環境全体のリソース (インベントリ)、脆弱性、ポリシー、ページ、ドキュメントを検索できます。必要な情報を見つけるための単一で合理化された方法を提供しています。

- 検索バーは、表示中のページに関係なく、クラウドサイバーエクスポージャーコンソールの右上に表示されます。
- キーボードのショートカットでアクセスするには、**Ctrl + K** を使用します。
- (オプション) 検索対象をアカウントのサブセットに絞り込むには、アカウント範囲のドロップダウンで範囲を選択します。
- インベントリ結果は、すべてのクラウドを対象に、カテゴリ別 (コンピューティングや IAM など) で分類されます。たとえば「VM」で検索すると、AWS EC2 インスタンス、Azure 仮想マシン、GCP VM インスタンスの結果が返されます。



リソースプロファイルの概要ビュー

インベントリ、アクセスグラフ(アクセス許可マッピング)、アクティビティログ、または検出結果ページ内で任意のリソース名にカーソルを合わせると、リソースに関する重要な情報を抜粋したミニプロファイルビューが表示されます。このビューでリソースに関する詳細を確認できるため、別のページに移動してコンテキストを切り替える必要がありません。


Groups
Account
Created
Users
Groups
Created
Users
Developers
Developers
IAM Group | Org1Account2
ARN
arn:aws:iam::
group/De...
Tags
Created
04/23/2020
Created By
Labels
Admin
No MFA
Access Keys
Sensitive
Excessive
Org1Account3

リスク深刻度の色分け

コンソール全体で、異なる色とアイコンを使用して、リソースと検出結果が組織にもたらすさまざまなリスクの深刻度レベルを示します。次の表では、各色とそれに対応する深刻度レベル、クラウド環境内でのその意味について説明しています。

色	アイコン	ステータス	説明	例
		**重大**	早急なアクションが必要	機密データへのアクセス許可を持っている管理者ユーザーがいるが、そのアクセス許可が使用されていない。
		**高**	できるだけ早く処理	機密データへのアクセス許可を持っている非管理者ユーザーがいるが、そのアクセス許可が使用されていない。

色	アイコン	ステータス	説明	例
	Medium	**中**	潜在的なリスク	バケットリストなど、機密性の高いリソースへのアクセス許可を持っているユーザーがいるが、バケットの内容を読み取るアクセス許可は持っていない。
	Low	**低**	昇格のモニタリング	割り当てられたアクセス許可の使用が制限されているユーザーがいる。
	Informational	**情報**	役立つ情報	新しいGCPプロジェクトが組織に追加された。
	該当なし	**コンプライアンス内**	アクションの必	過剰なアクセス許可な

色	アイコン	ステータス	説明	例
		(完全準拠)	要なし	し。ポリシールールとベストプラクティスに適合。

Hexa AI

HexaAI は、Tenable One Cloud Exposure コンソールに直接統合された AI を活用したアシスタントです。自然言語を使用してクラウド環境を調査、理解、推論するための会話型インターフェースを提供します。これにより、複雑なクエリを手動で記述したり、深いメニューを操作したり、さまざまなセキュリティツール間を移動したりする必要がなくなります。

> **注意:**
>
> - Hexa AI は、**Foundation** および **Advanced** ライセンスではデフォルトで有効になっています。Foundation または Advanced を使用されていない場合、**Tenable One のお客様は 90 日間の無料評価版をリクエストできます**。使用を開始するには、担当者にお問い合わせください。
> - Hexa AI はガバメントクラウド環境では利用できません。

Hexa AI を使用する理由

Hexa AI は、次の方法でセキュリティ運用の合理化を支援します。

- **調査の加速**手動でフィルターや Explorer クエリを作成する代わりに、数秒で即座に回答を得ることができます。
- **反復分析**: 特定のリスクをより深く掘り下げるためにフォローアップの質問をすることで、セキュリティリーダーを会話で追跡します。
- **複雑なデータの簡素化**: GraphQL スキーマや特定のクエリ構文を学習することなく、技術データにアクセスできます。

- **コンテキストの統合**: Hexa AI は、資産、調査結果、コンプライアンス フレームワーク、公式文書からデータを同時に取得して関連付けることができます。
- **障壁の軽減**: 自然言語インターフェイスにより、新しいアナリストや部門横断的なチームメンバーがプラットフォームにアクセスしやすくなります。

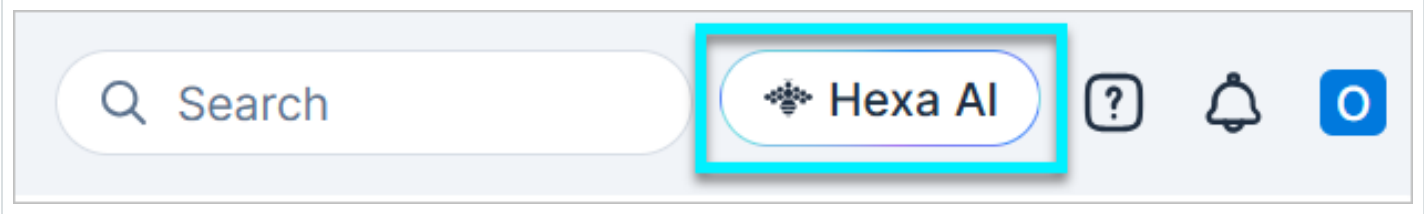
> **注意:** Hexa AI は提案を行いますが、意思決定を行いアクションを実行するには、ループ内の人間が必要です。クラウド環境や Tenable の設定を変更することはできません。修正のために、関連する検出結果を特定し、適切なコンソールワークフローに誘導します。

Hexa AI の設定

Tenable Hexa AI の設定は、Tenable Vulnerability Management を介して制御されます。詳細については、Vulnerability Management のドキュメントを参照してください。

Hexa AIにアクセスする

アシスタントを起動するには、クラウド サイバーエクスポージャーコンソールヘッダーの右上隅にある**Hexa AI** アイコンをクリックします。



Hexa 会話を開始するには、プロンプトを入力するか、**[ディクテーション]** をクリックして音声テキスト変換を使用します。

会話にファイルを追加する

Hexa は、会話で直接アップロードまたはドラッグ アンド ドロップしたファイルを操作できるため、データを手動で再フォーマットしたり、すでにお持ちのドキュメントを説明したりする必要はありません。スプレッドシート、レポート、または図 (リソースとその所有者のエクスポート、ネットワークトポロジーの図など) を添付し、Hexa にそこからの分析、要約、または情報の抽出を依頼します。

アップロードしたファイルは、その会話の残りの部分で引き続き使用でき、会話間で共有されることはありません。Hexaは後のメッセージでそれらを参照することができ、いつでもチャットからダウンロードして、不要になったら削除することができます。

Hexa でサポートされるファイルタイプは、`.csv`、`.gif`、`.html`、`.jpeg`、`.jpg`、`.md`、`.pdf`、`.png`、`.txt.`、`.webp` です。

会話ごとに最大 10 個のファイルをアップロードでき、各ファイルの長さは 2 MB を超えてはなりません。

コアアビリティ

機能	説明
監査クエリ	GraphQL インターフェースを介して監査証跡とアクティビティデータを取得
自動化の提案	クエリとターゲットの範囲を含め、一致するクラウドまたはコードの検出結果をチームに送信するための自動化を提案します。自動化を確認して保存します。
クラウド資産の調査	クラウドプロバイダー全体でクラウドリソース (EC2 インスタンス、S3 バケット、IAM ロール、VM、データベースなど) に対してクエリと探索を行います
コンプライアンスレポート	フレームワークに対するコンプライアンス態勢をまとめ、構造化されたレポートを生成
ドキュメント検索	製品のハウツーに関する質問や、Tenable の公式ドキュメントから質問に回答します
除外の提案	適用する範囲、アクション、パラメーターを含め、有効だがアクションの対象とならない検出結果に対して、ポリシー除外を推奨および作成します。
アイデンティティとアクセスのレビュー	IAM プリンシパル、ロール、アクセス許可、アクセスパスを調査する
ポリシーとレ	Explorer ベースのクエリを構築して、カスタムポリシーやエクスポート可能なレポー

機能	説明
ポートの作成	トを作成します
関係のトラバーサル	エンティティが相互にどのように関係しているかを理解します。たとえば、どのワークロードが公開されているか、どのアイデンティティが機密データにアクセスできるかです。
リスクと検出結果の分析	セキュリティの検出結果、ポリシー違反、設定ミス、脆弱性を取得し、理由を当てる。

一般的なユースケース

ユースケース	例
セキュリティ調査	• 公開アクセス可能で暗号化されていないすべてのS3バケットを表示します。 • 重大な脆弱性があり、インターネットに接続しているEC2インスタンスはどれですか?
アイデンティティとアクセス	• 90日間アクセス権を使用していない管理者権限を持つIAMユーザーをリストします。 • *GCPでロールが過剰に寛容なサービスアカウントはどれですか?*
コンプライアンスとレポート	• CIS AWS Foundationsに対するコンプライアンス態勢をまとめます。 • 本番環境のすべての深刻度の高い検出結果のレポートを生成します。
クラウド資産検出	• すべてのリージョンでいくつのRDSインスタンスがありますか? • AWS us-east-1にあるタグのないリソースをすべて表示します。
ポリシー構築	• 一般に公開されているデータベースを暗号化なしで検出するポリシーを構築します。
除外管理	• 開発、ステージング、ラボタグ付けされたリソースで検出結果のうち、アクション

ユースケース	例
	不可能として表示され続けているものについて、除外を提案する。 • QA アカウントでパブリックロードバランサーの検出結果を除外する代わりに、深刻度のダウングレードを推奨する。
自動化セットアップ	• 一般に公開されている S3 バケットの自動化を作成します。 • 暗号化されていない RDS インスタンスの自動化を作成しますが、これは本番環境の AWS アカウントに対してのみです。 • 重大深刻度の IaC 検出結果に対する自動化を作成します。
ハウツーと製品ガイダンス	• 新しい AWS アカウントをオンボーディングする方法 • Tenable はどのようにして有効なアクセス許可を計算しますか?

高度なユースケース

Hexa AI を使用して、詳細なペルソナベースのプロンプトを提供することで、高レベルの分析を実行し、複雑なアーティファクトを生成できます。以下は、高度なセキュリティおよび運用タスクに Hexa AI を活用する方法の例です。

次の表は、複雑なセキュリティ分析や運用タスクに Hexa AI を活用する方法の高度な例を示しています。

ユースケース	説明	例
SLA 監視	厳密に定義された組織の解決タイムラインに照らして未解決の検出結果を分析し、違反を特定	「IT 運用およびコンプライアンス アナリストとして行動します。未解決の問題/チケットのデータセットを提供しています。私の SLA (サービスレベル契約) ポリシーは次のように厳密に定義されています。 • 優先度: 重大 -> 4 日以内に解決する。

ユースケース	説明	例
	して修正計画を作成します。	• 優先度: 高 -> 7 日以内に解決。 データを分析し、以下を提供してください。 1. **SLA 違反の特定**: 現在の日付 ([今日の日付を挿入]) に基づいて、割り当てられた SLA を現在超えているすべての検出結果を特定します。 2. **エグゼクティブサマリー**: 最もリスクの高い、最も重大な「SLA 未履行」の検出結果は何ですか? これらを経過日数別にグループ化します (例:「30+ 日の期限を越える」)。 3. **即時アクションプラン**:特定された項目について、これらの違反を直ちに修正するために実行する必要がある次の3つの戦術的ステップは何ですか? 4. **Markdown テーブル**: チケット/検出結果 ID、優先度、経過日数 (オープン日数)、SLA の過去の日数、現在の所有者 / 担当者、問題のサマリーを含む、すべての違反項目の詳細なリスト。」
AI ワークロード検出	機密データアクセス権を持つ AI ソフトウェア、機械学習ライブラリ、マネージドクラウド AI サービスをインベントリするための包括的な検出計画を提供します。	「クラウドセキュリティアーキテクトおよびデータガバナンスのエキスパートとして行動します。クラウド環境全体で AI 関連のすべてのワークロードを見つけてインベントリするための包括的な検出計画が必要です。検出には、次の 2 つの特定の基準を含める必要があります。 1. **AI ソフトウェアとパッケージ (アプリケーション層):** 機械学習のフレームワークとライブラリを含む仮想マシン (EC2/GCE/Azure VM) とコンテナイメージ (ECR/GCR/ACR) を特定します。特に、pytorch、

ユースケース	説明	例
		tensorflow、jupyter、scikit-learn、keras、pandas、transformers (HuggingFace)、および「openclaw」やOllamaなどのオープンソースツールをスキャンします。 2. **マネージド AI サービスとデータアクセス (インフラストラクチャ層):** 使用中のすべてのネイティブクラウド AI サービスと、それに関連付けられている IAM アクセス許可/リソースリンクを一覧表示します。確認: SageMaker (AWS)、Vertex AI (GCP)、Azure Machine Learning、Bedrock/OpenAI API の統合。 **重大な要件**: 検出された各サービスについて、「機密」または「PII」としてタグ付けされた機密データバケット (S3/GCS/Blob) またはデータベース (RDS/BigQuery) に対する「許可」アクセス許可があるかどうかを特定します。 出力結果は、手動コンソール監査のチェックリストとサマリーテーブルを含む構造化された計画になります。」
有害な組み合わせの修正	パブリックエクスポージャー、重大な脆弱性、高い権限を持つロールに対処するための、多段階にわたるキルチェーン根絶計画を策定します。	「シニアクラウドセキュリティアーキテクトとして行動します。公開されており、OS レベルの重大な脆弱性を含み、高い権限を持つ IAM ロールにアタッチされている EC2 インスタンス (ENTER NAME HERE) があります。このキルチェーンを根絶するための段階的な修正計画を提供してください。含まれるもの: • **即時封じ込め**: アプリケーションを破損させずにインスタンスを分離する手順。 • **権限の削減**: 現在のロールから最小権限ポリシーに移行するための戦略。 • **脆弱性根絶**: パッチ適用と再プラットフォーム化のオプショ

ユースケース	説明	例
		ン。 • **予防**: AWS サービスコントロールポリシー (SCP) を使用して、この「有害な組み合わせ」の再発を防ぐ方法
キルチェーンとトレードオフ分析	複雑なリスクベクトルを分析し、攻撃コストと修正の容易さに基づいて、最も影響力のある単一の修正アクションを決定し、正当性を証明します。	「リードクラウドセキュリティアーキテクトとして行動します。EC2 インスタンス (ENTER NAME HERE) に重大なリスクがあります。パブリックアクセス可能で、パッチ未適用の重大な脆弱性があり、過剰な IAM 権限 (AdministratorAccess) があります。タスクの広範なリストを提供する代わりに、キルチェーンを分析し、最初に実行する最も影響力のある修正アクションを 1 つ決定していただきたいと思います。回答を次のように構成してください。 • **決定事項**: 3 つのベクトル (ネットワーク、パッチ、アイデンティティ) のどちらを最初に中和するのか、およびその理由を明確に述べてください。 • **ロジック**: 各ベクトルの「攻撃コスト」と「修正の容易さ」を比較して、選択を正当化します。 • **実装**: この「単一の」修正を実行するための特定の技術的手順 (CLI またはコンソール) を指定します。 • **残存リスク**: この1つの修正が適用された後にどの脅威が残っているかを簡単に述べてください。」
オペレーショナルエクセレンス	クラウドアカウントの統合の問題のトラブルシューティングと、「接続に問題あり」ステータスを解決するための段階的な	「AWS Account ID (ENTER ACCOUNT HERE) に関連する統合の問題を調査および解決します。Tenableに [Connected with issue] と表示される理由を説明してください。統合を修正するための段階的な修正計画を提供します。」

ユースケース	説明	例
	計画を提供します。	
コストの最適化	EBS ボリューム、Elastic IP、アイドル状態のロードバランサーなどの「孤立した」または未使用の AWS リソースを特定し、毎月のクラウド支出を削減します。	「シニア AWS ソリューションアーキテクトおよび FinOps スペシャリストとして行動します。現在コストが発生している AWS アカウント内の「孤立」リソースまたは未使用リソースを特定するためのソリューションが必要です。次のリソースの種類を Markdown テーブルに指定します [リソースの種類、リソース ID、リージョン、理由、推定コスト]。 1. アタッチされていない EBS ボリューム (ステータス: 使用可能)。 2. 関連付けられていないエラスティック IP アドレス。 3. ターゲットのないアイドル状態の Elastic Load Balancer (ALB/NLB)。 4. 「古い」EBS スナップショット (90 日以上経過しており、AMI に関連付けられていない)。 5. タッチされた Elastic Network Interfaces (ENI)。 [Price] (価格) 列では、標準の AWS US-East-1 価格見積もりを使用して、概算的な数値を提供します。これらのリソースを安全に削除するために必要な AWS CLI コマンドを含む短い「クリーンアップ」セクションを含めます。」
クラウドワークロードの健全性	24 時間以上経過した古いスキャンを含むワークロードをリスト表示することでスキャンの健全性を監視し、継続的な	「最終スキャン日」が現在のタイムスタンプから 24 時間より古いすべてのワークロードをリストします。ワークロード ID、名前、最後に正常にスキャンした正確な時刻を含めます。最初に最も古いスキャンで結果を並べ替えます。」

ユースケース	説明	例
	可視性と保護を確保します。	
カスタムデータ型の定義	データセキュリティ体制管理をサポートするために、専用または地域の識別形式の検証ロジックと正規表現パターンを定義します。	「タスク: 台湾識別番号 (ROC National ID) のカスタムデータタイプと検証ロジックを定義する。 • **書式**: ちょうど 10 文字です。構造: [A-Z][1-2][0-9]{8}。 • **文字 1**:大文字(地域事務所)。 • **文字 2**: 数字 (男性は 1、女性は 2)。 • **文字 3 から 9**: ランダムな 7 桁の数字。 • **文字 10**: チェックサムの数字。 **検証ロジック**: 先頭文字をコードに変換します (A=10、B=11...)。重みを割り当てます: L1=1、L2=9、D1=8、D2=7、D3=6、D4=5、D5=4、D6=3、D7=2、D8=1、D9=1。積を合計します。S mod 10 = 0 の場合に有効です。 出力: 5 つの有効な例と分類用の正規表現パターンを提供します。」

MCP サーバーを介した Hexa AI

> **注意:** これらの手順を完了するには、有効な Tenable One Cloud Exposure サービスアカウントが必要です。

Tenable Hexa AI MCP サーバーは、Tenable がホストするインターフェースで、クラウドサイバーエクスポージャーの構造化されたツールを任意の MCP 互換 AI クライアントに公開します。これは、お好みの大規模言語モデル (LLM) とクラウドセキュリティ環境の間の安全なアダプターとして機能し、AI クライアントがクラウドリソース、検出結果、アイデンティティ、コンプライアンスデータに直接アクセスできるようにします。

MCP サーバーを使用すると、Claude Desktop、Claude Code、Cursor などの AI クライアントを クラウド サイバーエクスポージャー に直接接続できます。その後、AI アシスタント が Tenable ツールを発見して呼び出し、クラウド資産の検索、検出結果の調査、IAM アクセス許可の確認、コンプライアンス体制のクエリ、カスタムワークフローの構築を行うことができます。これらのすべてを、ライブクラウド セキュリティデータを使用して実行できます。

重要: MCP サーバーには独自の LLM が含まれていません。AI クライアントを提供します。Tenableはツールとデータを提供します。

始める前に

Tenable Hexa AI MCP サーバーに接続する前に、以下が揃っていることを確認してください。

- サービスアカウントにアクセスできる クラウド サイバーエクスポージャー アカウント
- クラウド サイバーエクスポージャー サービスアカウントトークン。

  注意: サービスアカウントを作成または取得するには、クラウド サイバーエクスポージャー コンソールで、**[Settings > Access Management]** に移動します。

- 以下のような、MCP と互換性のある AI クライアント
  - Claude Desktop
  - Claude Code
  - Cursor
  - HTTP 経由で Model Context Protocol をサポートする任意のクライアント

注意: ローカルソフトウェアをインストールしたり、サーバーを設定したりする必要はありません。Tenable は MCP サーバーを完全にホストします。

MCP サーバーに接続する

Tenable Hexa AI MCP サーバーは、HTTP MCP エンドポイントとして利用できます。接続するには、サーバー URL と クラウド サイバーエクスポージャー サービスアカウントトークンを使用して MCP クライアントを設定します。

- **サーバー URL:** `https://app.tenable.com/api/mcp`
- **認証**: ベアラートークン承認ヘッダーとサービスアカウントトークン

  `Authorization: Bearer <YOUR_SERVICE_ACCOUNT_TOKEN>`

Claude Desktop

Claude Desktop は、`mcp-remote` npm パッケージを使用して、ローカルの stdio-to-HTTP ブリッジ経由でリモート MCP サーバーに接続します。

前提条件

次の Node.js がインストールされている必要があります。

- **macOS:** ターミナルで `brew install node` を実行します。
- **Windows:**nodejs.org からインストーラーをダウンロードして実行します。

`node -v` を実行して、インストールを確認します。「トラブルシューティング」の証明書オプションを利用できるように、バージョン 22.15 以降を推奨します。

Tenable Hexa AI MCP サーバーを Claude Desktop に追加するには:

1. Claude Desktop 設定ファイルを開きます。最も簡単な方法は、**Settings > Developer > Edit Config**、ファイルが存在しない場合はファイルを開き作成することです。ファイルは次の場所にあります。
   - **macOS:** `~/Library/Application Support/Claude/claude_desktop_config.json`
   - **Windows:** `%APPDATA%\Claude\claude_desktop_config.json`

   > **注意:** WindowsのMicrosoft StoreからClaude Desktopをインストールした場合、ファイルは上記のパスではなくパッケージフォルダ内に存在します。**[構成の編集]** ボタンを使用して開きます。

2. 次のエントリを [`mcpServers`] セクションに追加します。`<YOUR_SERVICE_ACCOUNT_TOKEN>`クラウドサイバーエクスポージャー サービスアカウントのトークンに置き換えます。

   JSON

   ```
   {
   ```

```
  "mcpServers": {
    "tenable-cloud-security": {
      "command": "npx",
      "args": [
        "-y",
        "mcp-remote",
        "https://app.tenable.com/api/mcp",
        "--header",
        "Authorization: Bearer <YOUR_SERVICE_ACCOUNT_TOKEN>"
      ]
    }
  }
}
```

ファイルにすでにmcpServersセクションが含まれている場合は、その中にtenable-cloud-securityエントリのみを追加します。

3. Claude Desktopを完全に終了して再起動します。macOSでは、**Cmd+Q**キーを押します。Windowsで、システムトレイアイコンを右クリックして**[終了]**を選択します。ウィンドウを閉じるだけでは十分ではありません。Claude Desktopは、利用可能なTenableツールを自動的に検出します。接続を確認するには、Claudeにクラウドアカウントをリストするか、オープンの検出結果を検索するように依頼します。

> **注意:** 最初の起動には、npxのダウンロードmcp-remoteで約30秒かかる場合があります。

トラブルシューティング

接続が表示されない場合は、まず完全に終了し、Claude Desktopを再起動したことを確認します。次に、ログを確認します。

- **macOS:** `~/Library/Logs/Claude/mcp-server-tenable-cloud-security.log`
- **Windows:** `%APPDATA%\Claude\logs\mcp-server-tenable-cloud-security.log`

ログのメッセージは原因を示しています。

`'C:\Program' is not recognized` (Windows)。npxコマンドは、起動時に中断されるスペース(`Program Files`)を含むパスに解決されます。command値を短いパス形式に変更します。

JSON

```
  "command": "C:\\PROGRA~1\\nodejs\\npx.cmd",
```

お使いのマシンで PROGRA~1 解決されない場合は、フルパス C:\\Program Files\\nodejs\\npx.cmdを使用してください。

SELF_SIGNED_CERT_IN_CHAIN - ネットワークは TLS トラフィックを検査し、デフォルトで Node が信頼しない内部認証局で再署名します。ノード 22.15 以降で、サーバーエントリに env ブロックを追加して、オペレーティングシステムの証明書ストアを信頼するようにノードに指示します。

JSON

```
"tenable-cloud-security": {
  "command": "npx",
  "args": [
    "-y",
    "mcp-remote",
    "https://app.tenable.com/api/mcp",
    "--header",
    "Authorization: Bearer <YOUR_SERVICE_ACCOUNT_TOKEN>"
  ],
  "env": {
    "NODE_USE_SYSTEM_CA": "1"
  }
}
```

403 Forbidden - GET https://registry.npmjs.org/mcp-remote - 組織がパブリック npm レジストリをブロックしており、承認済みの内部 npm レジストリを使用することを期待しています。そのレジストリで npm をポイントしてから、Claude Desktop を再起動します:

```
npm config set registry <YOUR_ORG_REGISTRY_URL>
```

レジストリに認証が必要な場合は、最初にログインします。npm login --registry=<YOUR_ORG_REGISTRY_URL> --auth-type=web。レジストリの URL とアクセス権については、IT チームまたはプラットフォームチームに問い合わせてください。npm config get registryで変更を確定します。

注意: マシンでコマンドプロンプトが無効になっている場合は、代わりにPowerShellでこれらのコマンドを実行します。コマンドは同じです。

401またはOAuth検出を繰り返す可能性があります。 authorizationヘッダーが受け入れられていません。`Authorization: Bearer <YOUR_SERVICE_ACCOUNT_TOKEN>`を使用していることと、トークンが有効であることを確認してください。

初回起動時のみ「取り付けられませんでした」。 Claude Desktopが、npxがまだ`mcp-remote`をダウンロードしている間に接続を試みました。30〜60秒待ってからトレイを終了して、再起動します。パッケージは、その後の起動時にキャッシュされます。

注意: サービスアカウントトークンは、`claude_desktop_config.json`にプレーンテキストで保存されます。ファイルを共有ドライブから遠ざけてください。トークンが漏洩した場合は、クラウドサイバーエクスポージャーコンソールの **[Settings > Access Management]** でトークンをローテーションします。

Claude Code

Tenable Hexa AI MCPサーバーをClaude Codeに追加するには:

1. ターミナルで次のコマンドを実行します。と`<YOUR_ACCESS_KEY>`を置換します`<YOUR_SECRET_KEY>`をクラウドサイバーエクスポージャーAPIキーに置き換えます。

   ```
   claude mcp add \
     --transport http tenable-cloud-security https://app.tenable.com/api/mcp \
     --header "X-ApiKeys: accessKey=<YOUR_ACCESS_KEY>;secretKey=<YOUR_SECRET_KEY>"
   ```

   Claude Codeは、次のセッションで利用可能なTenableツールを自動的に検出します。

Cursor

Tenable Hexa AI MCPサーバーをCursorに追加するには:

1. Open Cursor Settings:
   - **macOS: Cmd+**を押します。
   - **Windows: Ctrl+**を押します。

2. **[MCP Servers]** (MCP サーバー) > **[Add Server]** (サーバーを追加) に移動します。
3. 次の設定を行います。<YOUR_ACCESS_KEY> と <YOUR_SECRET_KEY> をTenable クラウド サイバーエクスポージャー API キーに置き換えます。

設定	意義
輸送	HTTP
URL	`https://app.tenable.com/api/mcp`
ヘッダー	`X-ApiKeys: accessKey=<YOUR_ACCESS_KEY>;secretKey=<YOUR_SECRET_KEY>`

VS Code/GitHub Copilot

VS Code の GitHub Copilot では、エージェント モードで MCP サーバーがサポートされています。

> **注意:** GitHub Copilot 拡張機能がインストールされた VS Code 1.99 以降を実行していることを確認します。MCP サポートにはエージェント モードが必要であり、インライン モードまたは編集モードでは利用できません。

Tenable Hexa AI MCP サーバーを VS Code に追加するには:

1. VS Code User Settings (JSON) を開きます。
   - **macOS: Cmd+Shift+P** キーを押してから、**[Preferences: Open User Settings (JSON)]** を選択します。
   - **Windows: Ctrl+Shift+P** キーを押してから、**[Preferences: Open User Settings (JSON)]** を選択します。
2. 以下を `settings.json` に追加します。と <YOUR_ACCESS_KEY> を置換します <YOUR_SECRET_KEY> を クラウド サイバーエクスポージャー API キーに置き換えます。

```JSON
{
```

```
  "mcp": {
    "servers": {
      "tenable-cloud-security": {
        "type": "http",
        "url": "https://app.tenable.com/api/mcp",
        "headers": {
          "X-ApiKeys": "accessKey=<YOUR_ACCESS_KEY>;secretKey=<YOUR_SECRET_KEY>"
        }
      }
    }
  }
}
```

または、ワークスペースルートで `.vscode/mcp.json` ファイルを作成または編集します。

JSON

```
{
  "servers": {
    "tenable-cloud-security": {
      "type": "http",
      "url": "https://app.tenable.com/api/mcp",
      "headers": {
        "X-ApiKeys": "${input:tenableApiKeys}"
      }
    }
  },
  "inputs": [
    {
      "id": "tenableApiKeys",
      "type": "promptString",
      "description": "Tenable API Keys (format: accessKey=...;secretKey=...)",
      "password": true
    }
  ]
}
```

> **注意:** `.vscode/mcp.json` アプローチでは、VS Code 入力変数を使用して実行時に認証情報の入力を求めるため、ハードコードされたシークレットは回避されます。に `.vscode/mcp.json` を追加する `.gitignore` 設定を共有しない場合。

3. ツールを使用するには、Copilot チャット パネル (Windows の場合は **Ctrl+Shift+I**、macOS では **Cmd+Shift+I**) を開き、**エージェント** モードに切り替えて、Copilot にクラウド サイバーエクスポージャーとの対話を依頼します。例:「AWS で未解決の重大な検出結果をリストします。」

その他の MCP クライアント

HTTP トランスポートをサポートする他の MCP 互換クライアントについては、次の設定を行います。<YOUR_ACCESS_KEY> と <YOUR_SECRET_KEY> をTenable クラウド サイバーエクスポージャー API キーに置き換えます。

設定	意義
トランスポートの種類	HTTP
URL	`https://app.tenable.com/api/mcp`
ヘッダー	`X-ApiKeys: accessKey=<YOUR_ACCESS_KEY>;secretKey=<YOUR_SECRET_KEY>`

注意: 具体的な設定方法はクライアントによって異なります。HTTP MCP サーバーの追加の詳細については、MCP クライアント ドキュメントを参照してください。

信頼、安全性、ガバナンス

Tenable Hexa AI MCP サーバーは、すべてのアクションを完全に制御できるように設計されています。

重要: MCP サーバーは Bring Your Own LLM モデルを使用するため、Tenable は選択した LLM プロバイダーにデータを送信します。組織のセキュリティとコンプライアンス要件を満たすデータ処理プラクティスを持つ LLM プロバイダーを選択してください。

コントロール	説明
認証	すべての API 呼び出しは、クラウド サイバーエクスポージャー API キーを使用して認証され、HTTP リクエスト ヘッダーを介して安全に送信されます。
RBAC と	すべてのアクションは、認証された API トークンに割り当てられた特定の範囲とロールに

コントロール	説明
アクセス許可	基づいて実行されます。MCP サーバーに昇格権限はありません。
データフロー	外部 AI クライアントがツール呼び出しリクエストを Tenable Hexa AI MCP サーバーに送信します。MCP サーバーは Tenable の API に対してリクエストを実行し、構造化された結果を返します。データは、このフローの一部として外部 LLM にトラバースされます。

データのフィルタリング

特定のリソース、検出結果、アクティビティ、その他のデータを見つけるために、さまざまな方法でコンソール全体のデータをフィルタリングできます。

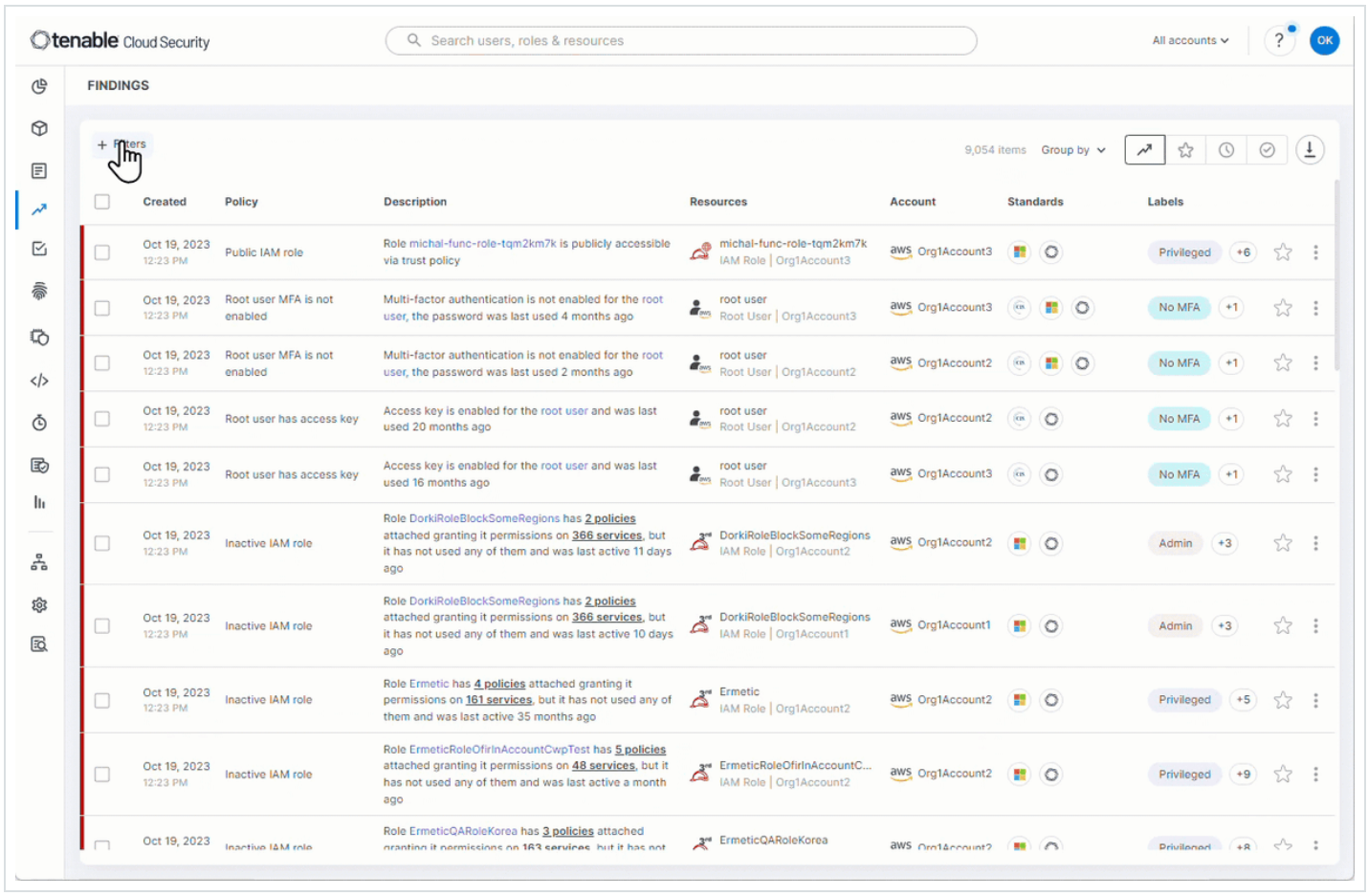
テーブル内のデータのフィルタリング

コンソール内すべてのテーブルの上部にあるフィルターを使用して、表示するデータの範囲を絞り込むことができます。

- コンソールの各ページには、そのページの一般的な使用状況に基づいてデフォルトで表示されるフィルターセットがあります。
- フィルターを追加するには、＋ Filters ボタンをクリックして、項目を選択するか、関連する検索用語を入力します。
- フィルターを追加または削除すると、変更が保存され、次回そのページにアクセスした際にデフォルトでそのフィルターが表示されます。保存されるのはフィルターのみです。ページを離れると、そのフィルターで選択された値は保存されません。
- 特定のフィールドに値を持たないエントリ(空の値)で表をフィルタリングするには、次のいずれかを選択します。
    - **空白**。たとえば、チケット (Jira 課題など) を持たないすべての検出結果をフィルタリングできます。

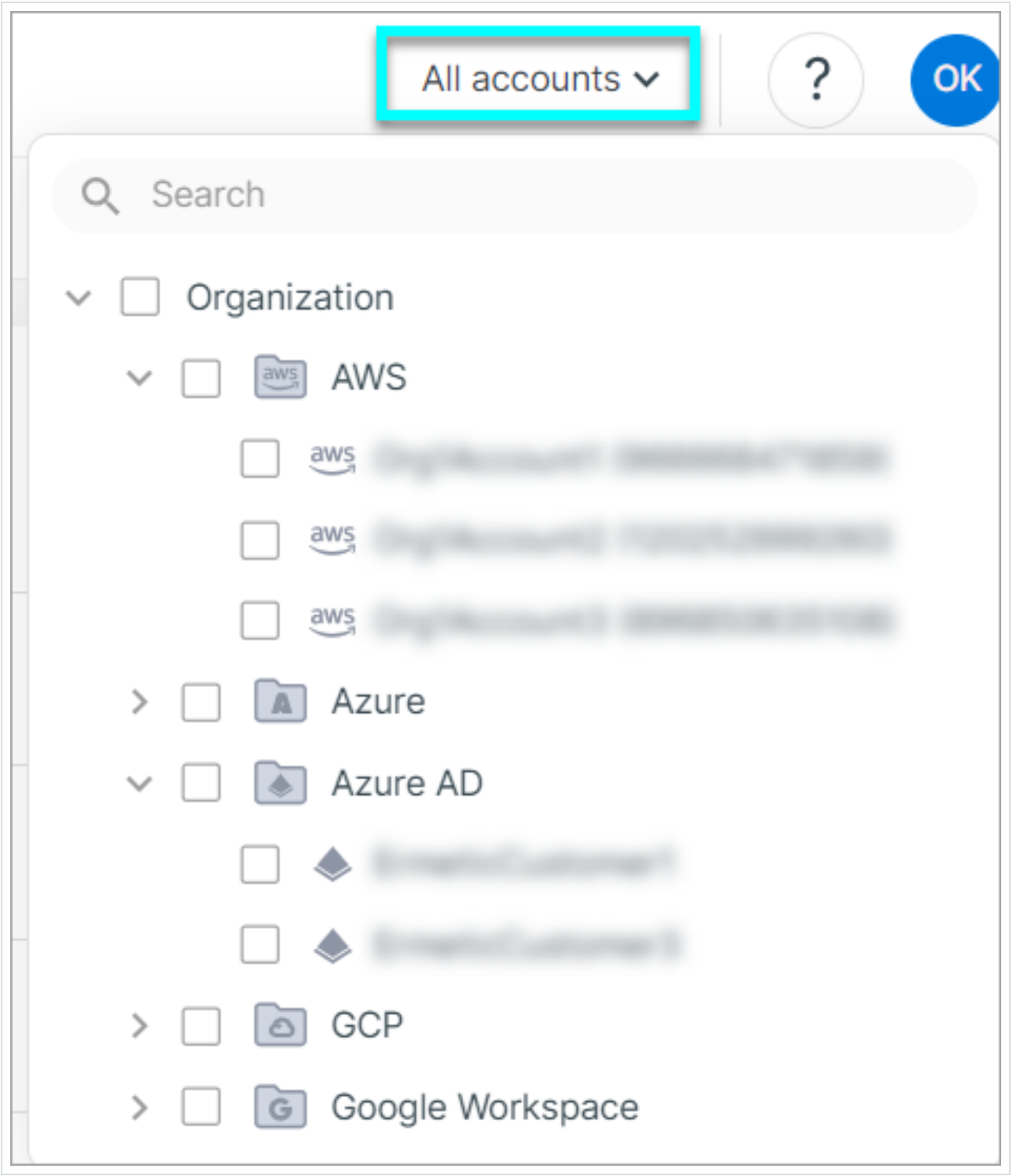
- **設定なし** (日付フィールドに使用され、日付ではない値が含まれることがある)。たとえば、[無視] の検出結果で、[無視の期限] の日付が設定されていない (つまり、永続的に無視される) 検出結果をすべてフィルタリングできます。または、[有効期限] が [なし] であるエンティティをフィルタリングできます。

- 検索語に一致するエントリでテーブルをフィルタリングするには、**[一致するものを選択]** をクリックします。このオプションは、最大 65,000 個のエントリを返すことができます。さらに多くのエントリが返される場合は、このオプションは無効になり、この機能を使用するには検索を絞り込む必要があります。
- 通常、多くの値を含む一部のフィルターでは、値の右側に **ある [のみ]** をクリックして、その値でのみフィルターを行い、以前に選択した他の値を効果的にクリアできます。
- 一部のエンティティには、特定のフィルターや列に一致する値がない場合があります。フィルターの「いずれか」の値を含むエンティティすべてでテーブルをフィルタリングするには、**[すべて選択]** をクリックします。
- フィルターから項目を選択すると、次にフィルターに戻ったときには選択された項目が一番上に表示されます。
- **[クリア]** をクリックして、選択したフィルターを削除します。
- 無効にされているコンプライアンス標準は、関連レポートに表示されません。詳細については、コンプライアンスを参照してください。



アカウント範囲によるデータのフィルタリング

コンソール右上にある **[すべてのアカウント]** ドロップダウンを使用して、コンソール全体でアカウントスコープ (IdP を含む) でデータをフィルタリングできます。詳細については、アカウント階層とフォルダー参照してください。



ダッシュボード

ダッシュボードを管 理する

この記事では、Tenable One Cloud Exposure でダッシュボードを表示、作成、カスタマイズ、管理する方法について説明します。

はじめに

開始するには、次の手順に従ってください。

1. 以下について詳しく知る:
    - ダッシュボードの範囲と可視性
2. [すべてのダッシュボード] ページからは、次の操作を実行できます。
    - すべてのダッシュボードを表示する
    - カスタムダッシュボードを作成する
    - ダッシュボードの複製
    - レポートの作成
    - ダッシュボードの編集

ダッシュボードの範囲と可視性

- 新しいダッシュボードを作成する前に、グローバル範囲のドロップダウンからその範囲を選択できます。

    > **重要:** 新しいダッシュボードを作成した後に範囲を変更することはできません。

- この範囲選択により、ダッシュボードを表示および管理できるユーザーが決まります。
- ダッシュボードの可視性は、ユーザーの全体的な範囲に結びついています。ダッシュボードがユーザーの範囲内にあると仮定すると、ユーザーはそのユーザーのどの範囲でもダッシュボードを表示できます。たとえば、ダッシュボードが Project A の範囲で作成された場合、両方のプロジェクトがユーザーの範囲内にあると仮定すると、ユーザーは Project B の範囲内でダッシュボードを表示することもできます。
- 特定のダッシュボードのデータは、現在選択されている範囲に従ってフィルタリングされます。たとえば、現在の範囲が Project Aの場合、ダッシュボードには Project Aに関連するデータのみが表

示されます。

- ダッシュボードは、作成元と異なる範囲に複製できます。

すべてのダッシュボードを表示する

すべてのダッシュボード (組み込みおよびカスタム) は、[すべてのダッシュボード] ページから表示できます。

すべてのダッシュボードを表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ダッシュボード]** > **[すべてのダッシュボード]** の順に移動します。
2. (オプション) 範囲を選択します。
3. ダッシュボードを表示および管理します。次のデータが表で確認できます。

縦棒	説明
名前	ダッシュボードの名前。
範囲	ダッシュボードが属する組織レベルまたはアカウントパスを示します。選択した範囲内でアクセス許可を持つユーザーはダッシュボードにアクセスできます。
可視性	ダッシュボードがパブリックアクセスか非公開かを表示します。 • **パブリック**: ダッシュボードの範囲内のすべてのユーザーに表示されます。 • **プライベート**: ダッシュボード作成者にのみ表示されます。 カスタムダッシュボードの表示を変更するには、ダッシュボードを ダッシュボードの編集 します。
変更者	ダッシュボードに最後変更を加えたユーザーを特定します。作り込みダッシュボードは、Tenable によって変更されたとおりに一覧表示されます。
ホーム / お気に	• **ホーム**: [ダッシュボード] メニュー項目をクリックすると表示されるデフォルトのダッシュボードを設定します。これにより、最も重要なセキュリティ情報を最も

縦棒	説明
入り 	目立つところで確認できます。 • **お気に入り**: 最もよく使用するダッシュボードをお気に入りとしてマークします。これにより、必要性の高いダッシュボードに簡単にアクセスして情報を確認することができます。
3つのドット	• ダッシュボードの編集 • ダッシュボードの複製 • 削除 • ホームとして設定

カスタムダッシュボードを作成する

カスタムダッシュボードを作成して、次のことができます。

- ダッシュボードをデザインしてカスタマイズし、関連するメトリクス、検出結果、ビジュアライゼーションを表示できます。
- プライベートまたはパブリックにして、可視性をコントロールします。

カスタムダッシュボードを作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ダッシュボード]** > **[すべてのダッシュボード]** の順に移動します。
2. (オプション) 範囲を選択します。

   > **重要:** 新しいダッシュボードを作成した後に範囲を変更することはできません。

3. **[+ New Dashboard]** をクリックします。
4. ボードの名前を入力します。
5. ボードを **プライベート** または **パブリック**のどちらにするかを選択します。

> **注意:** [公開] を選択した場合、このダッシュボード (または「ダッシュボード - 管理」権限を含むカスタムロール) を作成、編集、削除できるのは、「コラボレータ」または「管理者」ユーザーのみです。すべての クラウド サイバーエクスポージャー ユーザーが自分の範囲内で表示できます。

6. **[+ ウィジェットを追加]** をクリックします。ウィジェットの内容の詳細については、「 ウィジェット を参照してください。

   > **注意:** MTTR ウィジェットには、深刻度ごとに設定可能な SLA 設定フィールドが含まれています。

   1. ライブラリ内のウィジェットをカテゴリ別にフィルタリングします。
   2. ライブラリからウィジェットをドラッグアンドドロップします。
   3. ボード上のウィジェットを再配置します。
   4. ボードからウィジェットを**複製**または**削除**します。
7. 完了したら、**[保存]** をクリックします。

フィルター付きウィジェットで的を絞ったダッシュボードを作成

同じウィジェットを複数回追加し、それぞれに異なるフィルターを適用することで、特定のデータサブセットを並べて比較できます。

カスタムダッシュボードを使用すると、セキュリティデータを比較参照した非常に具体的なビューを作成できます。有効な手法は、1 つのダッシュボードに同じウィジェットを複数回追加し、インスタンスごとに異なるフィルター (高度なフィルターを使用する を参照) を適用することです。これにより、特定のデータサブセットを並べて比較でき、ダッシュボードから移動することなく、即座に分析情報を得られます。

たとえば、次のことが可能です。

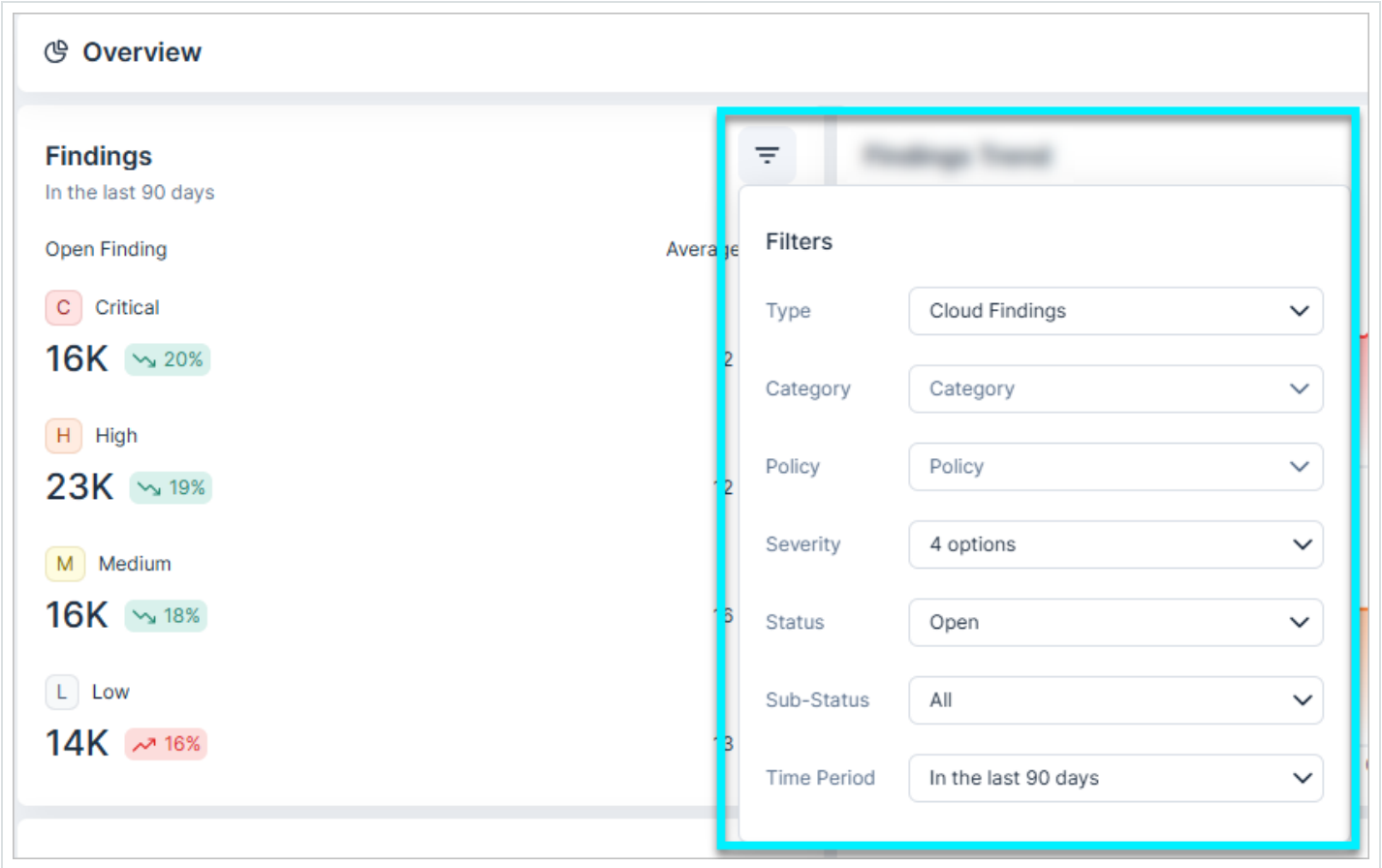
- 複数の [未解決の検出結果] ウィジェットを追加し、それぞれをフィルタリングして、深刻度レベル別に検出結果を表示します。
- 複数の [コンプライアンス] ウィジェットを追加し、それぞれをフィルタリングして、期間別のデータを表示します。

高度なフィルターを使用する

ダッシュボードウィジェットに強力なフィルターを適用すると、必要なデータを正確に絞り込むことができます。この機能により、セキュリティ体制を監視して分析するための、カスタマイズされた効率的な方法が提供されます。

これらのフィルタリングオプションは、次のウィジェットで使用できます。

- 検出結果
- 検出結果のトレンド
- 平均処理時間
- 処理された検出結果



ダッシュボードの複製

既存のダッシュボード (ビルトインまたはカスタム) を複製して、新しいダッシュボードを作成するためのベースラインとして使用できます。

注意: カスタムダッシュボードを複製すると、新しいコピーが現在の範囲で作成されます。これは次のことを意味します。

- 新しいダッシュボードには、現在選択された範囲に関連するデータのみが表示されます。
- 元のダッシュボードが別の(より狭い)範囲で設定されている場合、その元の範囲のみに関連付けられているデータまたは特定の設定は、新しいバージョンに含まれません。

この動作により、新しいダッシュボードに現在のコンテキストが正確に反映され、無関係な情報が表示されなくなります。

ダッシュボードを複製する方法

1. クラウドサイバーエクスポージャーコンソールで、次のいずれかに移動します。
    - **ダッシュボード>すべてのダッシュボード**
    - 複製する特定のダッシュボード。
2. (オプション) 範囲を選択します。

    重要: 新しいダッシュボードを作成した後に範囲を変更することはできません。
3. 三点リーダーアイコンをクリックしてから、**[複製]** をクリックします。
4. ボードの名前を編集します。
5. ボードを **プライベート** または **パブリック**のどちらにするかを選択します。
6. **[+ ウィジェットを追加]** をクリックします。ウィジェットの内容の詳細については、「 ウィジェット を参照してください。
    1. ライブラリ内のウィジェットをカテゴリ別にフィルタリングします。
    2. ライブラリからウィジェットをドラッグアンドドロップします。
    3. ボード上のウィジェットを再配置します。
    4. ボードからウィジェットを**複製**または**削除**します。
7. 完了したら、**[保存]** をクリックします。

レポートの作成

公開ダッシュボードに基づいてスケジュールされたレポートまたはオンデマンドのレポートを作成し、ステークホルダーとインサイトを共有する方法を簡素化します。たとえば、エグゼクティブの概要や検出結果の傾

向に関するレポートを作成して、ステークホルダーが実用的なプラットフォームデータを自動的に受け取れるようにすることができます。

- **動的更新**: レポートが特定のダッシュボードに接続されると、同期が維持されます。ウィジェットを更新したり、ダッシュボード名を変更したりすると、レポートには次回の配信でそれらの変更が自動的に反映されます。
- **削除保護**: レポートの一貫性を維持するために、パブリックダッシュボードがスケジュールされたレポートで現在使用されている場合、そのダッシュボードを削除したり、プライベートとしてマークしたりすることはできません。

レポートを作成する方法

1. クラウドサイバーエクスポージャーコンソールで、次のいずれかに移動します。
    - **ダッシュボード>すべてのダッシュボード**
    - レポートを作成したい特定の公開ダッシュボード。
2. (オプション) 範囲を選択します。
3. 関連するダッシュボード (公開のみ) で、三点リーダーアイコンをクリックして **から、[レポート]** をクリックします。[Create Report] (レポートの作成) ページが開きます。
4. 意味のある **名前**を入力します。
5. **配達時間**を選択してください:
    - **さて**。1回限りのレポートを生成します。
    - **スケジュール**。特定の時間にレポートを生成するための頻度を定義します。カスタム間隔 (たとえば、3週間ごとまたは6か月ごと) と週次配信の特定の曜日を設定して、チームが必要とするときに正確にデータが届くようにすることができます。
6. **[配信方法の追加]** を使用して、レポートのコピーを特定の受信者に送信します。詳細については、「 Slack または Teams 」を参照してください。
    - メールアドレス

        > **注意:**

> - 検出結果レポートの場合、**リソースの所有者ごとにメール**を送信するように選択できます。これにより、各 インベントリ(プロパティとラベル) に、自身のリソースに関連する検出結果のレポートが送信されます。
> - メールでレポートを送信する場合、ファイルサイズは 14.5MB に制限されています。レポートのサイズが大きい場合は圧縮されるか、ダウンロードリンク経由で提供されます。

- Slack チャンネル
- Teams チャネル

7. **[作成]** または **[スケジュール]** をクリックします。

ダッシュボードの編集

コラボレータ / 管理者、またはプライベートダッシュボードを作成した場合は、カスタムダッシュボードを編集できます。

ダッシュボードを編集して以下を行います。

- 可視性を変更する (プライベート / パブリック)
- ウィジェットを追加または削除する
- ダッシュボードの名前を変更する

ダッシュボードを編集する方法

1. クラウドサイバーエクスポージャーコンソールで、次のいずれかに移動します。
   - **ダッシュボード>すべてのダッシュボード**
   - 編集する特定のダッシュボード。
2. (オプション) 範囲を選択します。
3. 三点リーダーアイコンをクリックしてから、**[編集] をクリックします**。
4. ボードの名前を編集します。
5. (管理者/共同作成者のみ)ボードを **プライベート** または **パブリック**のどちらにするかを選択します。
6. **[+ ウィジェットを追加]** をクリックします。ウィジェットの内容の詳細については、「 ウィジェット を参照してください。

1. ライブラリ内のウィジェットをカテゴリ別にフィルタリングします。
2. ライブラリからウィジェットをドラッグアンドドロップします。
3. ボード上のウィジェットを再配置します。
4. ボードからウィジェットを**複製**または**削除**します。

7. 完了したら、**[保存]**をクリックします。

ウィジェット

ダッシュボードウィジェットは、ユーザーがクラウドセキュリティポスチャーを監視および評価しやすいように設計されています。これらのウィジェットは、接続されているアカウント、リソースの内訳、オープンの検出結果、コンプライアンスステータス、インフラのコード化 (IaC) の詳細、アイデンティティおよびアクセス管理 (IAM) の傾向などに関するインサイトを提供します。これにより、ユーザーはリスクを特定して優先順位を付け、時間の経過に伴うアクティビティを追跡し、クラウド環境全体でセキュリティのベストプラクティスを確実に遵守できるようになります。

- クエリ
- コンプライアンス
- データ
- 検出結果
- IaC
- IAM
- インベントリ
- 脅威
- ワークロード

クエリ

クエリウィジェットには、保存済みクエリの監視履歴からのデータが表示されます。保存済みのすべてのクエリには、**アイテム数**と**テーブル**のウィジェットが含まれます。モニタリング対象クラウド/IaC 検出結果およびクラウドリソースクエリには、追加のウィジェットが含まれます。

ウィジェット	説明
アイテム数[1]	最後の日次スナップショットの時点でクエリに一致する結果の総数。
表[1]	前回の日次スナップショットのクエリ結果の表形式ビュー。
深刻度別の検出結果[2]	クエリ内の検出結果の深刻度レベル別の内訳。最後の日次スナップショットに基づいて、各深刻度の検出結果の数と平均経過日数を表示します。
検出結果の傾向[2]	クエリ内の検出結果の推移。日次スナップショット間で検出結果数がどのように変化するかを追跡できます。
検出結果 MTTR[2]	クエリ内の検出結果の解決までの平均時間 (深刻度別に分類)。ウィジェットをカスタムダッシュボードに追加する際に、深刻度レベルごとに最大 365 日の SLA しきい値を設定できます。
検出結果アクティビティ[2]	クエリ内でオープンまたは解決された検出結果の数を、深刻度別にセグメント化したもので、時間の経過とともに表示したもの。未解決の検出結果と解決済みの検出結果の両方を含み、期間別にグループ化された棒グラフとして表示されます。
トレンド[2] [3]	日次スナップショットに基づく、クエリ結果カウントの経時的なスナップショット。

[1] 監視の有無にかかわらず、保存されたすべてのクエリで利用できます。

[2] 監視対象のクラウド/IaC 検出結果クエリで使用できます。

[3] 監視対象クラウドリソースクエリに利用可能

コンプライアンス

ウィジェット	説明
コンプライアンス	一般的な業界標準とセキュリティのベストプラクティスに関するコンプライアンスを確保できます。 • 各標準で表示されるパーセンテージは、関連するポリシー要件にどの程度準拠しているかを示しています。 • 標準をクリックすると、完全なコンプライアンスを妨げるポリシー違反が表示されます。 無効になっている標準はここに表示されません。詳細については、コンプライアンステーブルデータを参照してください。

データ

ウィジェット	説明
データリソース	環境内の機密性の高いデータ保護をすばやく特定します。ドリルダウンして、特定のデータカテゴリにマッピングされているリソース、または特定の機密度を持つリソースをすべて表示します。たとえば、PII データや、社外秘に該当する機密データを持つリソースをすべて表示します。

検出結果

ウィジェット	説明
検出結果[1][2]	検出結果を深刻度別に分類し、その平均経過日数とともに統合ビューを表示します。これは、セキュリティ問題の分布と日数を素早く把握するのに役立ちます。
検出結	指定された期間における検出結果の傾向を視覚化します。これにより、セキュリティイ

ウィジェット	説明
	ニシアチブの効果を追跡し、新たなパターンを特定できます。
検出結果 MTTR[1][2]	検出結果の深刻度に基づいて、チームが検出結果をどれだけ迅速に処理しているかを明確にします。[重大]、[高]、[中]、[低] の検出結果に対して SLA しきい値を最大 365 日まで設定できます。これは、修正効率を監視し、改善するのに役立ちます。
解決済みの検出結果[1][2]	対処された (クローズまたは無視された) 検出結果の数を、深刻度別にセグメント化して時系列で参照できます。チームのワークロードと解決率の過去の推移を把握できます。
未解決の検出結果	Tenable One Cloud Exposure の未解決の検出結果について全体的な概要が表示されます。検出結果には、見つけるのが難しい危険な組み合わせを含む、リスクのあるアイデンティティやリソースが表示されます。 • ウィジェットの右上にある [深刻度] ドロップダウンを使用して、[重大]、[高]、[中]、[低] の各深刻度の検出結果を任意に組み合わせて表示します。 • 未解決の検出結果の深刻度レベル別の数と、未解決の全検出結果のうち各レベルが占める割合 (%) が表示されます。数字をクリックすると、検出結果の一覧が表示されます。 • カテゴリ (IAM など) をクリックすると、検出結果のカテゴリ別の内訳が表示されます。
トレンド	設定期間のアクティビティデータのスナップショットを表示して、検出結果のステータスを追跡します。 • ウィジェットの右上にあるフィルターを使用して、過去 7 日、30 日、90 日のデータをフィルタリングできます。 • [新規オープン] / [解決済み] / [スター付き] / [スヌーズ] の各検出結果の数が表示されます。 • 新規オープンの検出結果について、高の深刻度または重大の深刻度を持つ数

ウィジェット	説明
	と、この期間中にクラウドサイバーエクスポージャーに追加された新しいポリシーの結果として未解決となった数を確認できます。 • (検出結果が作成されないようにする) ポリシーで除外されたリソースの数が表示されます。 • 検出結果に基づく作成済み (手動または自動化ルールによる) チケットの数が表示されます。
有害な組み合わせ	組み合わせた場合に、見つけるのが難しく、組織に大きな脅威をもたらす複数のリスクを持つリソースを表示します。詳細については、危険な組み合わせを参照してください。クラウドセキュリティドメイン全体にわたるいくつかの危険な組み合わせの詳細や、プラットフォーム内の危険な組み合わせの全リストなどを確認できます。 • アイコンにカーソルを合わせると、リスクをもたらす全カテゴリが表示されます。 • 組み合わせをクリックすると、[インベントリ] ビューのすべての関連リソースからフィルタリングされたビューが表示されます。 • 1 つの組み合わせに異なるタイプのリソースが含まれている場合はポップアップが表示され、表示するリソースタイプを選択できます。
5 分しか時間がない場合…	時間がない場合や、最も深刻な問題に集中したい場合は、このリストを使用して、環境内で最も優先度が高い検出結果を評価し、修正することができます。 • 評価し、修正するには、該当する検出結果をクリックします。 • 関連するリソースをクリックすると、詳細を確認できます。
シークレットを露出するリソース	重要なシークレット (パスワード、認証情報、キーなど) を露出する脆弱なリソースを評価し修正します。このようなリソースはよく見過ごされるため、攻撃者に悪用される可能性があります。リソースタイプをクリックすると、関連するすべての検出結果が表示されます。

ウィジェット	説明
パブリックリソース	タイプ別に分類され、リスク深刻度で優先順位付けされたパブリックリソースに関連する検出結果を評価し修正します。 • 数字をクリックすると、特定のリソースをすばやく見つけることができます。 • [さらに表示] をクリックすると、そのカテゴリに関するリソースの完全なリストが表示されます。
リスクのある上位のアカウント	組織内のリスクが最も高いアカウントと、深刻度レベルごとの検出結果数の内訳を表示し、評価および修正できるようにします。 • アカウント名をクリックすると、そのアカウントに関する検出結果がすべて表示されます。 • 特定の数字をクリックすると、その深刻度レベルに対応する色別の検出結果が表示されます。
上位の検出結果タイプ	最もリスクの高い検出結果タイプと、深刻度レベルごとの検出結果数の内訳を表示して、評価および修正できるようにします。 • 検出結果タイプをクリックすると、そのタイプの検出結果がすべて表示されます。 • 特定の数字をクリックすると、その深刻度レベルに対応する色別の検出結果が表示されます。

[1] これらのウィジェットには、次の日付からの環境内のデータが表示されます。データは削除されません。

- **クラウドの検出結果**: 2025 年 7 月中旬
- **コードの検出結果**: 2025 年 10 月中旬

[2] ダッシュボードの検出結果ウィジェットのほとんどのデータは、データの日次スナップショット (UTC) を表します。それに対して、クラウドの検出結果 には常にライブデータが表示されます。結果として、これら 2 つ

の場所の検出数に相違が出る可能性があります。[検出結果] および [検出結果のトレンド] ウィジェットにあるクリック可能な検出結果の合計は、ライブデータを表し、[検出結果] ページのデータと一致します。

IaC

ウィジェット	説明
クラウドからコードまで	コードのオリジンまで遡ったクラウドリソースをすべて確認します。
リポジトリ	クラウドサイバーエクスポージャーに接続されているコードリポジトリ。
オープンの IaC 検出結果	IaC スキャンで検出されたすべての未解決の検出結果について、大まかな概要を表示します。検出結果はリスクのあるアイデンティティやリソースを表します。現在未解決のすべての検出結果、各検出結果タイプの数 (トリガーしたポリシー別に分類)、カテゴリ別の検出結果またはタイプの内訳が表示されます。
リスクのある上位リポジトリ	組織内の重大なリスクのあるリポジトリと、深刻度レベルごとの検出結果数の内訳が表示されます。検出結果を評価するには、リポジトリまたは特定の番号をクリックします。

IAM

ウィジェット	説明
プリンシパル	すべてのプリンシパル (ユーザー、サービスアイデンティティ、グループ、AWS アクセス許可セット) のステータスの概要を、過剰な権限を持つ検出結果の深刻度でフィルタリングで

ウィジェット	説明
	きます。各タイルには、合計数、特権プリンシパルの数、過剰な権限を持つ検出結果があるプリンシパルの数が表示されます。検出結果カウントをクリックすると、[過剰なアクセス許可] ページにリダイレクトされます。[1]
過剰な権限の傾向	過剰なアクセス許可を持つ過剰な権限のアイデンティティ数のトレンドを表示します。すべてのアカウントにわたる進捗状況の詳細な推移と、アカウントごとの変化のスナップショットを確認します。 • セクションをフィルタリングして、特定の **アイデンティティのタイプ** やタイムフレーム (**過去 7 日間、30 日間、または 90 日間**) のデータを表示します。 • **アカウント別の変更**。 • ウィジェットのエントリをクリックしてドリルダウンし、関連するオープンの検出結果のリストを表示します。検出結果ページの [オープン時刻] フィルターは、[過剰な権限の傾向] ウィジェットのドロップダウンで選択した期間に応じてフィルタリングされます。 • 下 : 非アクティブまたは過剰な権限を持つプリンシパルの増加により、選択した時間枠で最も大きく減少したアカウント • 上 : 選択した時間枠で最も改善したアカウント (非アクティブまたは過剰な権限を持つプリンシパルの減少)。 ダッシュボードウィジェットは初期状態と最終状態を比較しますが、[Findings] (検出結果) ページには特定の時点における特定の状態が反映されます。たとえば、検出結果がオープンされ、クローズされて、その後再オープンされた場合、ウィジェットではそれが変更としてカウントされない可能性がありますが、検出結果ページではオープンとしてリストされます。その結果、ウィジェット内の検出結果の数は、選択したタイムフレーム内でクローズされてから再オープンされた検出結果が原因で、ドリルダウン後にリストされる検出結果と異なる場合があります。
サード	ベンダーごとのサードパーティの概要が表示されます。現在、ウィジェットには、サードパー

ウィジェット	説明
パーティベンダー	ティとして識別されたAWSロール、Microsoft Entra IDアプリケーション、GCPサービスアカウントが表示されます。特定のクラウドのベンダーコンポーネントをクリックすると、フィルタリングされたビューが開きます。このビューを使用して、アクセス許可、アクセス許可の深刻度、カテゴリなど、サードパーティのアイデンティティに関するデータを調査します。
危険な組み合わせ	複数のIAM関連のリスクを持つリソースを表示します。これらのリスクは組み合わせた場合に、見つけるのが難しく、組織に大きな脅威をもたらします。詳細については、危険な組み合わせを参照してください。クラウドセキュリティドメイン全体にわたるいくつかの危険な組み合わせの詳細や、プラットフォーム内の危険な組み合わせの全リストなどを確認できます。 • アイコンにカーソルを合わせると、リスクをもたらす全カテゴリが表示されます。 • 組み合わせをクリックすると、[インベントリ]ビューのすべての関連リソースからフィルタリングされたビューが表示されます。 • 1つの組み合わせに異なるタイプのリソースが含まれている場合はポップアップが表示され、表示するリソースタイプを選択できます。
IAM検出結果	検出結果の深刻度レベルで並べ替えられた、最も多くの検出結果をトリガーしたIAMポリシー。検出結果の深刻度レベルでセクションをフィルタリングします。

[1] **サービスアイデンティティ**のカウント:
アクセス許可の計算方法や継承されたロールの表示方法が異なるため、アイデンティティの数はビュー間で異なる場合があります。

- **IAMダッシュボード**ビュー: アクセスが付与されたアイデンティティ(フィルタリングされた範囲でのアクセス許可評価および有効なアクセス許可)のみをカウントします。
- Explorerビュー: アクセス許可のないものも含めて、すべてのアイデンティティを表示し、アイデンティティを2回リストすることもできます。

インベントリ

ウィジェット	説明
アカウント	各クラウドサービスプロバイダー(CSP)組織の接続済みアカウントの概要。 • タイルをクリックすると、その特定のCSPに接続されているアカウントがすべて表示されます。 • アカウントのステータスは次のとおりです。1) 赤色の場合、アカウントが接続されていないことを意味します。2) 黄色の場合、アカウントは接続されていますが、表示されている理由により一部の機能が欠落しています。3) 緑色の場合、アカウントは接続されています。
リソース	環境内の資産のリソースカテゴリ別の内訳。 • カテゴリをクリックすると、関連するクラウドサービスプロバイダーによってグループ化された、リソースタイプ別の内訳が表示されます。 • リソースタイプをクリックすると、そのタイプの全資産インベントリが表示されます。

脅威

ウィジェット	説明
異常検出	未解決の異常に関連する検出結果の数を時系列(過去7日、30日、または90日)で表示し、環境内の不審なアクティビティを追跡します。検出結果の内訳をアクティビティカテゴリ別に表示します。これはクラウドアイデンティティに一般的な一連の動作パターンに関連するものです。各カテゴリの横にある括弧内に表示される検出結果の数は、選択された日付フィルターに関係なく、現在の検出結果の数を反映しています。関連する検出結果の解決を確認し、セキュリティポスチャーを改善します。

ワークロード

ウィジェット	説明
仮想マシンの脆弱性ステータス	検出された脆弱性の深刻度別 (最も高いもの順) のマシンの内訳が、オープンの検出結果の数とともに表示されます。
重大な脆弱性のステータス	マシンで見つかった重大な CVE を表示します。既知のエクスプロイトがあるものと最近確認されたものを優先します。
オペレーティングシステムのステータス	インストールされている OS のステータス別に、マシンの内訳を表示します。このような問題はワークロードのセキュリティ侵害を示している可能性があるため、OS を更新して修正する必要があります。

危険な組み合わせ

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

Tenable One Cloud Exposure は、環境内において潜在的に危険な組み合わせとはがないか検索します。これらの組み合わせの一部またはすべてが、通常、[危険な組み合わせ] のダッシュボードウィジェットに表示されます。

この項では、クラウドセキュリティドメインにまたがるいくつかの危険な組み合わせについて詳しく説明します。それぞれの例では、各コンポーネントに関連する個別のリスクと、要素が組み合わさった場合にもたらされる脅威の高まりを詳しく説明しています。さらに、プラットフォーム内の危険な組み合わせのリストを確認できます。

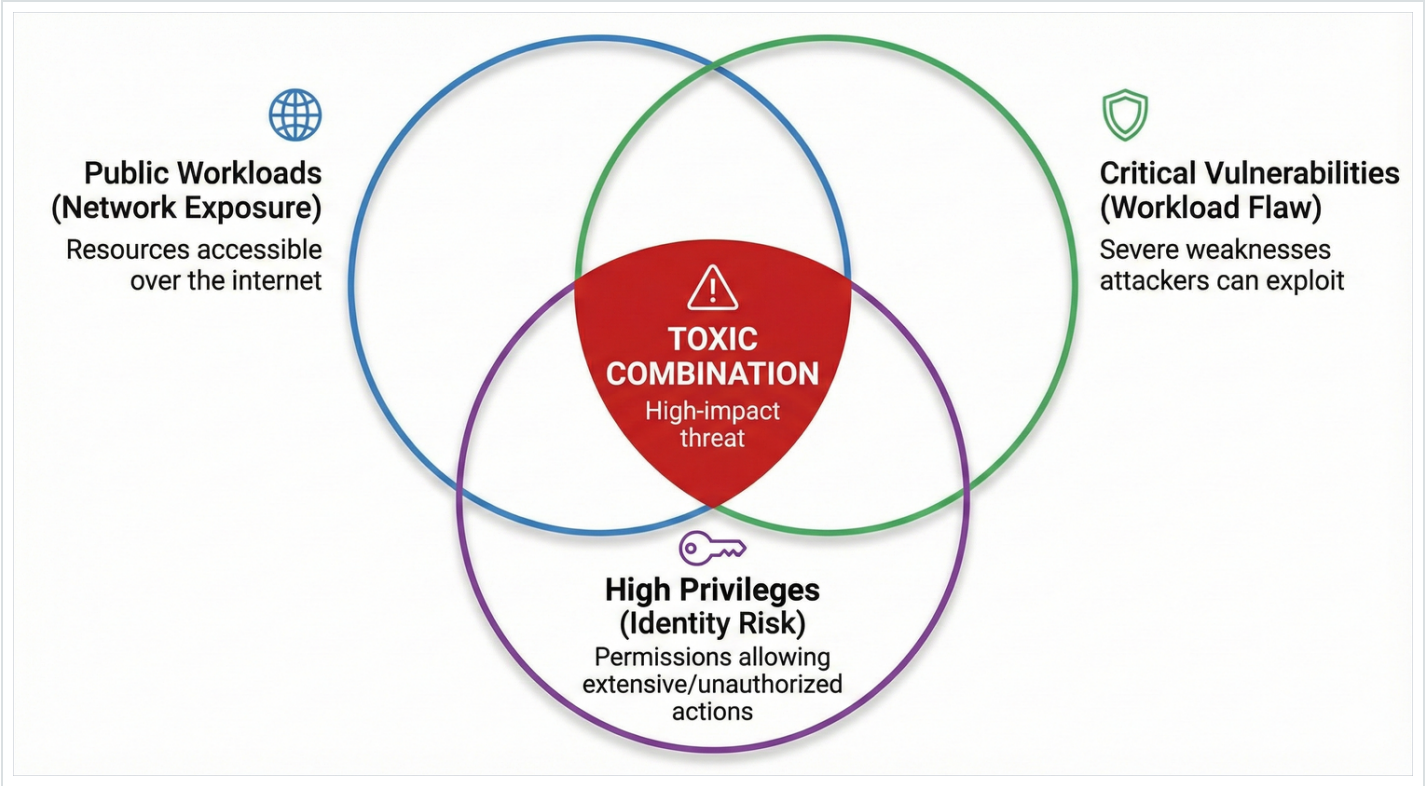
- **ワークロード保護**
    - 重大な脆弱性と高い権限を持つパブリックワークロード

- **データ保護**
    - パブリックデータリソースと機密データ
- CIEM (IAM ガバナンス)
    - 外部プリンシパルと高い権限
- CSPM/CIEM
    - パブリック関数と高い権限

危険な組み合わせとは

クラウドセキュリティにおいて危険な組み合わせとは、アクセス許可、属性、または条件が組み合わさることで、それぞれが単独でもたらすよりも大きなセキュリティリスクが生じることです。多くの場合、これらの組み合わせにより、ユーザーはセキュリティコントロールの回避、不正アクションの実行、適切な監視なしでの機密性の高いデータへのアクセスが行えます。危険な組み合わせを特定して管理することは、クラウド環境で最小権限を適用し、権限昇格や不正アクセスを防ぐために不可欠です。

たとえば危険な組み合わせとは、ゲストユーザーが高い権限を持つ場合です。最小限のアクセス権を付与されるべきユーザーアカウントに広範なアクセス権が付与されることで、偶発的または意図的に誤使用やその他のセキュリティインシデントが引き起こされる可能性があります。



重大な脆弱性と高い権限を持つパブリックワークロード

- **パブリックワークロード**
  - 説明: インターネット経由でアクセス可能なワークロード。
  - リスク: これらのリソースをスキャンして標的とすることができる攻撃者に対する露出が増加する。
- **重大な脆弱性**
  - 説明: 攻撃者が悪用できる深刻なセキュリティ上の弱点。
  - リスク: 攻撃者がこれらの脆弱性を利用してワークロードを侵害する可能性がある。
- **複合リスク**
  - 攻撃者がこの脆弱性を悪用した場合、高い権限により、秘密性の高いシステムが不正にコントロールされ、侵害の影響を及ぼしている可能性があります。

パブリックデータリソースと機密データ

- **パブリックデータリソース**
  - 説明: インターネットに公開されているストレージまたはデータリポジトリ。
  - リスク: インターネットにアクセスできるすべてのユーザーに対してデータが露呈するため、権限のない閲覧や漏洩のリスクが増加する。
- **機密データ**
  - 説明: PII や財務データなどの機密にすべき情報。
  - リスク: 機密データの開示は、コンプライアンス問題、評判の低下、金銭的損失につながる可能性がある。
- **複合リスク**
  - 公開されている秘密データは攻撃者にとって非常に誘導され、データの侵害や誤用の可能性が大幅に高まります。

外部プリンシパルと高い権限

- **外部プリンシパル**
  - 説明: クラウド環境へのアクセス権が付与されている外部のユーザーまたはエンティティ(請負業者やパートナーなど)。
  - リスク: 外部ユーザーに対してはモニタリングやコントロールがより困難なため、データ誤使用のリスクが増加する。
- **高い権限**
  - 説明: 環境内での広範なアクセスとアクションを許可するアクセス許可。
  - リスク: 高い権限により、潜在的な機密リソースを含む広範囲のアクセスが可能になる。
- **複合リスク**
  - 高い権限を持つ外部プリンシパルが、誤ってまたは意図的にアクセスまたは操作して、内部コントロールおよびデータセキュリティにリスクを与える可能性があります。

パブリック関数と高い権限

- **パブリック関数**
    - 説明: インターネットに公開されているサーバーレス関数またはAPI。
    - リスク: パブリック関数には誰もがアクセスできるため、攻撃を受ける可能性が増加する。
- **高い権限**
    - 説明: 機密タスクの実行や制限されたリソースへのアクセスを可能にする、昇格したアクセス許可。
    - リスク: 侵害された場合、高い権限を介して、承認されていないアクションが広範に行われる可能性がある。
- **複合リスク**
    - 高い権限を持つパブリック関数が関数の悪用に成功した場合、他のセキュリティコントロールをバイパスすることで、攻撃者が大きな影響を与えるアクションへのダイレクトパスを攻撃者に提供します。

危険な組み合わせのリスト

クラウドサイバーエクスポージャーは、環境内に以下の潜在的に危険な組み合わせがないか検索します。これらの組み合わせの一部またはすべてが、通常、[危険な組み合わせ] のダッシュボードウィジェットに表示されます。

- **サードパーティ**アイデンティティと**機密データ**へのアクセス権
- App Engine サービスにおける**重大な脆弱性**と**高い権限**
- Cloud Run サービスにおける**重大な脆弱性**と**高い権限**
- ECS サービスにおける**重大な脆弱性**と**高い権限**
- **外部**プリンシパルと**高い権限**
- **外部**プリンシパルと**機密データ**へのアクセス権
- **ゲスト**ユーザーと**高い権限**
- **ゲスト**ユーザーと**機密データ**へのアクセス権
- **MFA なし**で**高い権限**を持つ IAM ユーザー
- **パブリック** Cloud Run サービスと**重大な脆弱性 / 高い権限**

- **パブリック**データリソースと**機密データ**
- **パブリック**データリソースと、**保存時の暗号化**なし
- **パブリック**ストレージアカウントと**共有キーアクセス**
- **パブリック** ECS サービスと**重大な脆弱性 / 高い権限**
- **パブリック関数**と**高い権限**
- **パブリック**仮想マシンと**高い権限**
- **パブリック**ワークロードと**重大な脆弱性 / 高い権限**
- **パブリック**ワークロードと**サポートが終了した、またはサポート終了が近い OS**
- **パブリック**ワークロードと**パッチが適用されていない OS / 高い権限**

調査

エクスプローラー

探索ページは、クラウド環境を調査する中心的な場所です。すべてのリソースと検出結果にわたるクエリを使用し、幅広いフィルターとプロパティを使用してリスクを正確に特定し、優先順位を付け、修正します。

[エクスプローラー] ページに入ったら、検索を開始するにはいくつかの方法があります。

- [人気クエリ] リストから**クエリを選択します**。このリストには、最初に最近使用 保存されたクエリ が表示され、その後に一連の推奨のビルトインクエリが表示されます。
- [保存済みクエリ] セクションから **保存されたクエリを選択します**。
- オブジェクトを選択し、フィルターを適用して、**新規クエリを作成するを構築し**ます。

クエリが開かれたら、クエリを変更し、**[保存]** または **[名前を付けて保存]** を選択して、新しいカスタムクエリを作成できます。

クエリ結果は、テーブルまたはグラフで表示できます。クエリ結果を表示する。

保存されたクエリ

保存済みクエリを使用すると、特定のクエリ設定を毎回再構築することなく再利用できます。

保存されたクエリをここから開く方法

- **Explorer ページ**:
    1. **[エクスプローラー>調査]** に移動します。
    2. [**保存済み] クエリ** ボタンをクリックします。
    3. 次のいずれかを使用してフィルタリングまたは検索します。
        - カテゴリ
        - 検索バー
        - クエリタイプ (すべて、ビルトイン、パブリック、プライベート) でフィルターを表示します
- クエリ:
    1. [>**クエリの調査] に移動します**。
    2. 開くクエリをクリックします。

使用できる保存済みクエリには 2 つのタイプがあります。

- **ビルトインクエリ**: Tenable One Cloud Exposure によって提供される標準装備のクエリ。これらのクエリは編集または削除できません。変更して **[名前を付けて保存]** をクリックし、カスタムクエリを作成できます。
- **カスタムクエリ**: 自分または他のユーザーによって作成されます。カスタムクエリは、パブリックまたはプライベートにすることができます。任意のカスタムクエリを更新または複製できます。

新規クエリを作成する

調査するオブジェクトを選択し、フィルター、演算子、関係性を使って結果を絞り込むことで、新しいクエリを作成します。以下のセクションでは、各ステップについて説明します。

1. オブジェクトの選択
2. 結果のフィルタリング
3. フィルターと演算子の組み合わせ

4. 関係を追加する
5. [グループ化] を使用した結果の集計
6. クエリの保存
7. クエリを編集する

オブジェクトの選択

すべてのクエリは、仮想マシン、アイデンティティ、コンテナ、ポリシーなどのオブジェクトから始まります。このオブジェクトによって、フィルタリングできるプロパティとリレーションシップが決まります。

オブジェクトを選択するには

1. **[エクスプローラー>調査]** に移動します。
2. 「**リソースの検索**」コントロールを選択して、オブジェクト・セレクタを開きます。次のことができます。
    - オブジェクトの名前で**検索**します。
    - **最近使用したオブジェクトから選択**します。
    - **カテゴリを参照して**関連オブジェクトを表示します (たとえば、Kubernetes を選択するとすべての Kubernetes リソースが表示されます)。
    - 利用可能なオブジェクトの完全なリストを**スクロール**します。

オブジェクトを選択すると、クエリビルダーが開き、フィルター、演算子、関係を追加して結果を絞り込むことができます。

ネイティブオブジェクトと汎用オブジェクト

カスタムクエリを作成するときには、さまざまなタイプのオブジェクトから選択して環境を探索できます。これらのオブジェクトタイプは、範囲を示すアイコンで区別されます。

- **ネイティブオブジェクト** (クラウド固有のアイコン (例: 、Azure):
    - これらは、特定のクラウドプロバイダーに固有のオブジェクトや、特定のプラットフォームのサービス (AWS EC2 インスタンス、Azure 仮想マシンスケールセットなど) の詳細を提供するオブジェクトを表します。ネイティブオブジェクトを選択すると、その特定のクラウド環境のオブジェクトの

みをクエリできます。これらは、単一のクラウドプラットフォームの固有のプロパティや詳細をターゲットにする必要がある場合に使用します。

- 接続されたクラウド環境から利用可能なすべてのリソースがサポートされていますが、すべてのリソースですべてのプロパティをフィルタリングできるわけではありません。クエリするすべてのリソースには、少なくとも、特定の統合リソースタイプから継承されたプロパティに加えて、クラウドリソースオブジェクトのすべてのプロパティがあります (たとえば、GCP VM インスタンスはクラウドリソースタイプと仮想マシンタイプの両方から継承します)。

- **汎用オブジェクト** (アイコン:)。
  - これらのオブジェクトは、複数のクラウドプラットフォーム (仮想マシンやアイデンティティなど) または単一のプラットフォーム (Google アイデンティティなど) 内に存在する一般的なリソースタイプを表します。汎用オブジェクトをクエリすると、関連するすべてのインスタンス (プラットフォーム間または単一のプラットフォーム内) が 1 つの統合ビューに表示されます。これは、複数のクラウドをまたがる広範な概要を把握する場合に最適です。
  - **クラウドリソース**オブジェクトは、最上位レベルの汎用オブジェクトです。汎用型かプラットフォーム固有の型かにかかわらず、すべてのリソースに適用できるプロパティの基本セットを定義します。

結果のフィルタリング

クエリの中核となるオブジェクトを選択したら、そのオブジェクトのプロパティに基づいてフィルタリングを開始できます。

オブジェクトプロパティでフィルター

> **定義した:** インベントリ (プロパティとラベル) は、フィルターとしても表示されます。

オブジェクトプロパティでフィルタリングする方法

1. 選択したオブジェクトの右側にある **+** (**フィルターの追加**) をクリックします。
2. **[プロパティ]** セクションで、関連するプロパティを検索またはスクロールして見つけます。たとえば、「名前」と入力します。

3. プロパティ名をクリックして基準として追加し、プロパティ演算子と値を選択します。たとえば、[名前]にoperator=**Contains**とvalue=**dev**を選択できます。

エンティティ特性でフィルタリング

クラウドリソースとエンティティを機能 (特性) でフィルタリングすることで、特定のサービスタイプに関係なく、共通の特性を共有するリソースをすばやく見つけることができます。

1. 選択したオブジェクトの右側にある **+** (**フィルターの追加**) をクリックします。
2. 「**プロパティ**」セクションで、「**特性**」を検索または選択します。
3. プロパティ名をクリックして、条件として追加します。
4. 演算子を選択します (例: **[Is]**と**[Not]**)。
5. フィルタリングする特定の特性 (**暗号化可能**、**タグ付け可能**など) を選択します。

空白値のクエリプロパティ

特定のプロパティに定義された値がないリソース/検出結果を検索するには、`is empty` 演算子を使用します。たとえば、この演算子を使用すると、すべてのクラウド環境にわたって、タグが欠落しているすべての公開仮想マシンを検索できます。

未加工のクラウドプロバイダーソースデータでフィルタリング

クラウドサイバーエクスポージャーは、最も一般的なリソース属性をプロパティとしてモデル化します (**名前**、**オペレーティングシステムタイプ**など)。プロパティではない属性が必要な場合は、代わりに**[ソースデータ]**でフィルタリングします。このプロパティには、リソースに関してTenableがクラウドプロバイダーから受け取ったJSONが含まれます。

クラウドプロバイダーは、このJSONのコンテンツと構造を定義します。Tenableはそれを制御せず、プロバイダーはいつでもフィールド名、値、または構造を変更できます。

ソースデータでは、次の演算子がサポートされています。

演算子	これを使用してください
含まれるもの	JSON にテキスト文字列が含まれるリソースを任意の場所で検索します。大文字と小文字を区別する一致は、**[Aa]** をクリックします。
パターンに一致する	JSON がパターンに一致するリソースを検索します。大文字と小文字を区別する一致は、**[Aa]** をクリックします。
JSON パスと一致する	JSON 内の特定の場所にある値でフィルタリングします。
空である	未加工の JSON がないリソースを検索します。

一致するリソースを除外するには、演算子の横にある **[なし]** をクリックします。

始める前に

- クエリするタイプのリソースを開き、**[JSON]** タブをクリックします。これを使用して、正確なキー名と構造を見つけます。キー名は大文字と小文字が区別され、クラウドプロバイダーの API ドキュメントとは異なる場合があります。

特定の JSON 値でフィルタリングする方法

1. 選択したオブジェクトの右側にある **+** (フィルターの追加) をクリックします。
2. **[プロパティ]** セクションで、**[ソース データ]** を検索してクリックします。
3. 演算子ドロップダウンボックスで、**[JSON パスに一致]** を選択します。
4. **[JSON パス]** ボックスに、`$` で始まる JSONPath 式を入力します。たとえば、詳細AWSモニタリングされていない EC2 インスタンスを検索するには、「`$.monitoring.state`」と入力して **[文字列]** と **[等しい]** を選択して、「`disabled`」と入力します。[未定:コンソールでこれを一度実行して、結果が返されることを確認します]
5. **[条件付きロジック]** で、複数の値を返すパス (配列など) を処理する方法を選択します。
    - すべて**に一致**: すべての値が一致する必要があります。これはデフォルトです。
    - **Match any**: 少なくとも 1 つの値が一致する必要があります。

6. **[タイプ]**ドロップダウンボックスで、値のデータタイプ(**文字列**、**数値**、**ブール値**)を選択します。
7. **[演算子]**ドロップダウンボックスで、演算子を選択します。使用可能な演算子は、タイプによって異なります。次の表を参照してください。

タイプ	演算子
文字列	等しい、含む、次で始まる、次で終わる、一致パターン
数字	等しい、より大きい、以上または等しい、より小さい、より小さい
ブール値	等しい

8. 値を設定します。
    - **[文字列]**または**[数値]**で、**[値]**ボックスに値を入力します。
    - **Boolean**の場合、**True**または**False**を選択します。

フィルターがクエリに表示されます(例:`Source Data matches JSON Path $.monitoring.state equals disabled`)。

> **注意:** JSONパスでは大文字と小文字が区別され、大文字と小文字が間違っているパスは、エラーなしで結果を返しません。たとえば、`$.architecture`は一致するが、`$.Architecture`は一致しません。キー名は、クラウドプロバイダーのAPIドキュメントではなく、リソースの**JSON**タブから常にコピーしてください。

> **注意:** 一部のクラウドプロバイダーは、trueとfalseをテキストとして保存します(例:`"ebsOptimized": "false"`)。**ブール**型はこれらの値と一致しません。**[JSON]**タブで値が引用符で囲まれている場合は、**[文字列]**と**[等しい]**を選択し、「`true`」または「`false`」と入力します。**数値**タイプは、`"coreCount": "1"`などの引用符で囲まれている数値に一致します。

複数のオブジェクト プロパティでフィルター

プロパティをいくつでもフィルタリングできます。

複数のプロパティでフィルタリングする方法

1. 選択したオブジェクトの右側にある + (**フィルターの追加**) をクリックします。
2. **[プロパティ]** セクションで、関連するプロパティを検索またはスクロールして見つけます。たとえば、[作成時刻] などです。
3. プロパティ名をクリックして基準として追加し、プロパティ演算子と値を選択します。
4. これらの手順を繰り返して、追加のプロパティを追加します。

> **注意:** デフォルトでは、複数のフィルターの接続に And 演算子が使用されます。これを変更するには、フィルターの右側にある三点リーダーアイコンをクリックして Or を選択します。

関係でフィルター

オブジェクトの直接プロパティによるフィルタリングに加えて、他のリソースとの接続に基づいてフィルタリングできます。

リレーションでフィルタリングする方法

1. 選択したオブジェクトの右側にある + (**フィルターの追加**) をクリックします。
2. **[リレーション]** セクションで、関連するリレーションシップを検索またはスクロールして見つけます。たとえば、クラウドリソースに関連しています。
3. 関係の横にあるインラインの **[フィルター]** ボタンをクリックします。または、**[参加]** をクリックして結合を作成することもできます。

クエリグループの非表示 / 表示

フィルターセットは、クエリから削除せずに一時的に無効にすることができます。これは、テストとトラブルシューティングに役立つ強力な機能です。グループを非表示にすると、そのフィルターはクエリのロジックから削除され、検索結果に影響しなくなります。グループは保存されたままなので、[グループをいつでも表示] を選択することで、フィルターを即座に再度有効にすることができます。

クエリのどのレベルでグループも非表示にできます。たとえば、親グループ全体を非表示にしたり (これにより、そのグループ内にネストされているすべてのフィルターも無効になります)、グループ内の個々のフィルターを非表示にしたりできます。

クエリグループを非表示/表示する方法

関連するグループの横にある三点リーダーアイコンをクリックし、**[グループを非表示**にする] をクリックします。

フィルターと演算子の組み合わせ

クエリにフィルターを追加すると、フィルターは論理演算子を使用して相互作用します。

演算子	記	例
そしてロジック	デフォルトでは、複数のプロパティフィルター (たとえば、名前にdev が含まれ、ラベルが特権) を追加すると、それらは自動的にAND ロジックと組み合わされます。つまり、エンティティは、結果に含めるには、指定されたフィルターをすべて満たす必要があります。	本番環境で実行されているAWS 個のEC2 インスタンスをすべて検索する方法 `AWS EC2 Instance` + `Status` が `Running` + `Labels` が `Production` です (このクエリは、本番環境としてタグ付けされた実行中のEC2 インスタンスのみを返します)。
またはロジック	検索を拡大するには、Or ロジックを使用します。これを選択すると、代替のフィルターセットを定義できます。クエリでは、最初の条件セットまたは定義した代替セットのいずれかに一致するエンティティが返されます。	AWS、パブリックにアクセス可能な、または暗号化されていないS3 バケットを検索する方法 `AWS S3 Bucket` + (`Access Level` は `Public` + `OR` + `Encrypted` は `False` に等しい) (このクエリは、パブリックにアクセス可能な、暗号化されていない、またはその両方であるS3 バケットを返します)。
Of Type Logic	`Of Type`演算子は、より具体的なリソースタイプでフィルタリングすることで、ネイティブオブジェクトと汎用オブジェクトに対	特にAWS EC2 インスタンスタイプに属し、パブリックネットワークエクスポージャーがあるすべての仮想マシンを検索する方法 `Virtual Machine` + `Of Type` + `AWS EC2 Instance` + `Network Exposure is`

演算子	記	例
	するクエリを絞り込みます。これにより、その特定のリソースタイプに固有のプロパティを選択できます。	Public (このクエリは、より広範な「仮想マシン」リソースから開始した場合でも、指定された条件に一致する AWS つの EC2 インスタンスのみを返します)。
非論理	「ない」演算子を使用すると、特定の条件を満たすエンティティを除外できます。これを選択すると、その直後にあるフィルターまたはフィルターのグループのロジックを反転できます。クエリでは、Not 演算子の後に指定された条件を満たさないエンティティのみが返されます。	特権ラベルが付いていない仮想マシンを検索するには、Virtual Machine + NOT + Labels is Privileged (このクエリは、特権ラベルのない仮想マシンを返します)。
複雑なクエリ	And (暗黙)、Or、Not演算子を組み合わせることで、非常に具体的なクエリまたは広範なクエリを作成して、必要なものをピンポイントで正確に特定できます。	インターネットに直接さらされているウェブサーバーではない仮想マシン、または非アクティブなラベルの Windows マシンを検索する方法 Virtual Machine + NOT + OR (Name contains webserver + Network Exposure is Internet (direct) + Operating System Type is Windows + Labels is Inactive) (このクエリは、一般に公開されている Web サーバーでも、非アクティブな Windows マシンでもない仮想マシンを返します)。

関係を追加する

オブジェクト間の関係を照会する機能は、Explorer の心臓部です。強力なクエリを構築できるには、次の 2 つの異なる方法でこれらのつながりを活用できます。

- リレーションシップフィルターの使用
- 結合を作成する

リレーションシップフィルターの使用

この方法を使用すると、関連オブジェクトの特定のプロパティに基づいてエンティティを検索できます。このメソッドを使用する場合も、1 つのオブジェクトタイプを照会しますが、その接続に基づいてフィルタリングします。クエリにいくつものリレーションシップフィルターを追加して、検索を正確に絞り込むことができます。

クエリの例 - 重大な検出結果を持つすべてのアイデンティティを検索する

> **注意:** クエリは、条件を満たすアイデンティティのリストを返します。結果の表には、アイデンティティ自体に関する情報のみが表示されます。

1. プライマリオブジェクトとして **[アイデンティティ]** を選択します。
2. リレーションシップフィルターを追加し、**[検出結果あり]** を選択します。
3. [検出結果あり] フィルターで、ネストされた条件を **[深刻度]** に追加し、**[重大]** を選択します。

結合を作成する

この方法では、2 つの異なるオブジェクトタイプのデータを 1 つの結果セットに結合でき、各行には結合されたオブジェクトからのデータの一意の組み合わせが表示されます。1 つのクエリに最大 10 個の結合を追加して、非常に複雑で詳細な結果セットを作成できます。複数の結合は、**並列** (同じオブジェクトから分岐する複数の結合) または **線形** (後続の結合オブジェクトから分岐する結合) に追加できます。

クエリの例 - 重大な検出結果を持つすべての検出結果とそれに関連付けられたアイデンティティを検索します。

- `Join`,を使用すると、クエリは組み合わせた情報を含む単一のテーブルを返します。この例では、各行に、条件を満たすアイデンティティと検出結果の一意の組み合わせが表示され、両方のオブジェクトのデータが同時に表示されます。
- `Join`を `Left Join` に切り替えると、結合されたオブジェクトに一致するデータがなくても、(クエリの左側にある) プライマリオブジェクトからすべての結果が返されます。これは、プライマリオブジェクトのすべてのアイテムの完全なリストを確認する場合に便利です。

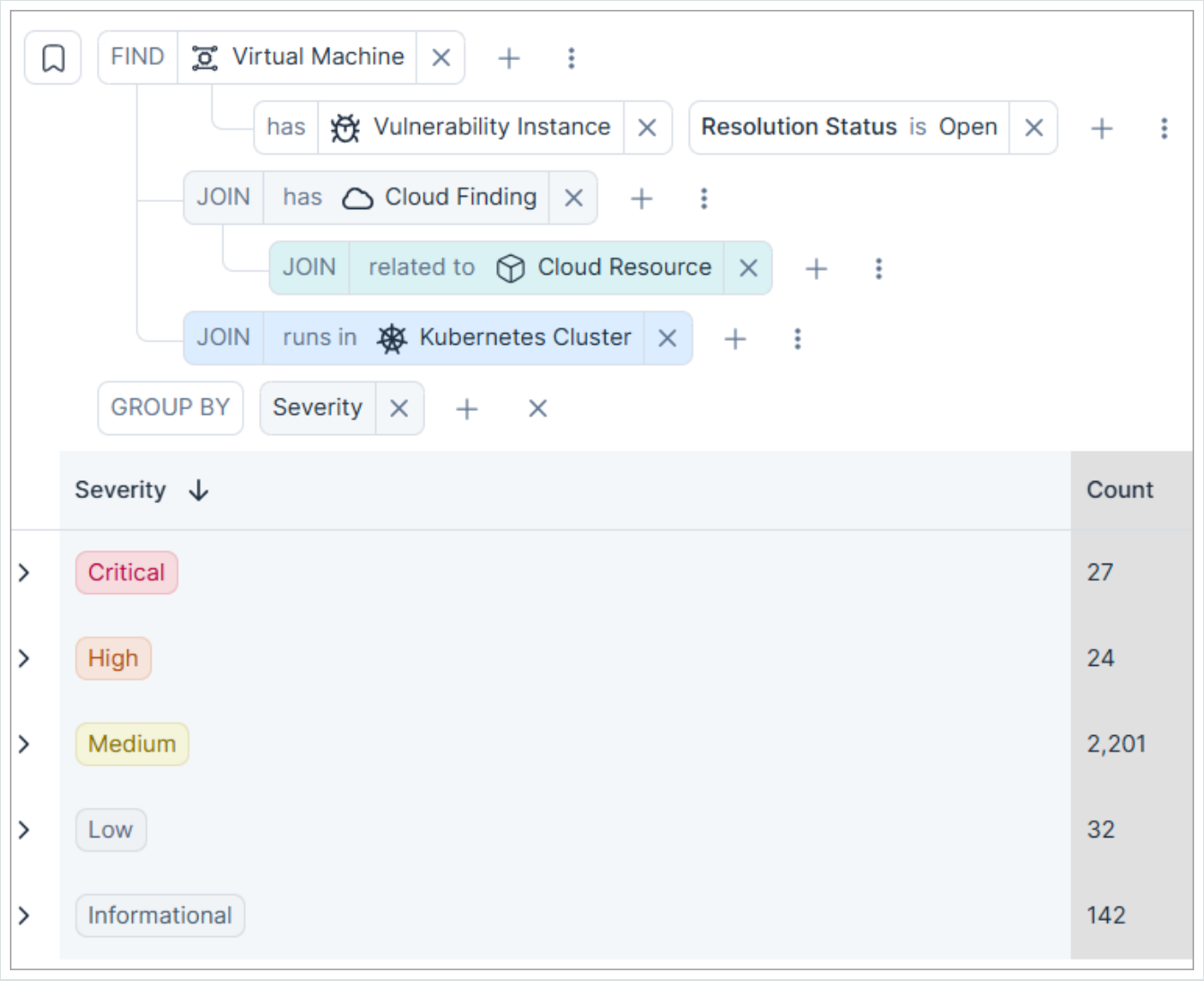
1. プライマリオブジェクトとして **[アイデンティティ]** を選択します。
2. 選択したオブジェクトの右側にある **+** (**フィルターの追加**) をクリックします。
3. **[リレーション]** セクションで、関連するリレーションシップを検索またはスクロールして見つけます。たとえば、検出結果に関連するものです。
4. 関係の横にあるインラインの **[結合]** ボタンをクリックします。
5. 結合された検出結果オブジェクト内で、深刻 **度** のネストされた条件を追加し、**[重大]** を選択します。

[グループ化] を使用した結果の集計

特定のプロパティごとにクエリデータを集計し、結果をカウントとして簡略化されたテーブルビューで表示します。たとえば、検出結果関連のクエリを深刻度別にグループ化すると、結果の内訳を深刻度レベル別に表示できます。

1. ルートエンティティの横にある三点リーダーアイコンをクリックし、**[グループ化]** を選択します。GROUP BY 要素がクエリの下部に追加されます。
2. GROUP BY 要素の横にある **+** (追加) ボタンをクリックし、グループ化ターゲットを選択します。ルートエンティティごとにデータをグループ化するか、結合された任意のオブジェクトでデータをグループ化

するかを選択できます。



クエリの保存

エクスプローラー>エクスプローラーでクエリを作成または変更した後、後で再利用するために保存できます。

保存済みクエリに加えた変更は、保存するまで一時的に残ります。

クエリを保存する方法

1. **[保存]** または **[名前を付けて保存]** を選択します。
    - **[保存]** は現在のカスタムクエリを更新します。ビルトインクエリでは保存が無効になっています。
    - **[名前を付けて保存]** は、新しいカスタムクエリを作成します。
2. [クエリの保存] ウィンドウで、次のように入力します。
    1. 名前
    2. カテゴリ
    3. 可視化:
        - **パブリック:** 組織内のすべてのユーザーに表示されます。
        - **プライベート:** 自分だけが閲覧できます。
    4. モニタークエリ
        - **監視**: Tenable は、監視を有効にしてから開始されるクエリ結果の日次スナップショットをキャプチャし、クエリプロファイルでトレンド追跡とウィジェットを有効にします。

          > **注意:** クエリを監視するには、クエリをパブリックにし、結合またはグループのプロパティがない必要があります。

        - 監視**しない** (デフォルト)
3. **[Save]** (保存) をクリックします。後で クエリ管理できます。

クエリウィジェット

監視対象クエリでは、履歴データがクエリプロファイルのウィジェットとして表示され、**[調査]** > **[クエリ]** で表示できます。ウィジェットバンクはカスタムダッシュボードで使用することもできます。

クエリを編集する

カスタムクエリの名前、カテゴリ、または表示は Explorer ページから直接更新できます。

クエリを編集する方法

1. **[調査]** > **Explorer** で、変更するカスタムクエリを開きます。
2. ページ上部のクエリ名の横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
3. [クエリの編集] ウィンドウで、以下を更新できます。
    - **名前**
    - **カテゴリー**
    - **可視性**: **プライベート** (自分にのみ表示) と **パブリック** (組織に表示) を切り替えます。
4. [保存] をクリックします。

クエリからのカスタムポリシーの作成

クエリをカスタムポリシーに変換して、アドホック検索を自動セキュリティ監視に変換します。たとえば、公開されている EC2 インスタンスを「機密」タグで追跡するためのポリシーを作成します。

クエリベースのポリシーを使用すると、以下が可能になります。

- 名前、説明、カスタムの修正ステップ (外部リンクを含む) を割り当てて、セキュリティチームに明確なガイダンスを提供できます。
- 固有の環境制約を定義し、問題解決のために手動でレポートを共有する必要性をなくすことで、修正ワークフローを改善できます。

> **注意:**
>
> - 保存すると、ご使用の環境内で Tenable が次回 データの同期と更新の頻度 ときに、ポリシーがトリガーされ、一致するすべてのリソースの検出結果が生成されます。
> - 現時点では、クラウドリソースに対する単一のリソースクエリのみをサポートしています。詳細については、サポートされているオブジェクト 。
> - 結合クエリのカスタムポリシーを作成することはできません。関連するエンティティでフィルターを適用するには、リレーションシップを追加するときに [結合] ではなく **[フィルター]** をクリックします。

クエリからカスタムポリシーを作成する方法

1. コンソールで、エクス**プローラー**> **[調査]** に移動します。
2. (オプション)[組織] ドロップダウンで範囲を選択します。

3. 既存のクエリを選択するか、新しいクエリを作成します。詳細については、サポートされているオブジェクト 。
4. **[Add > Custom Policy]** をクリックします。[Add Custom Policy] (カスタムポリシーの追加) 画面が開きます。
5. 意味のある **名前** と **説明** を入力します (オプション)。
6. ポリシーに深刻度を割り当てます。深刻 **度** は、ポリシーによってトリガーされた検出結果の深刻度を決定します。
7. (オプション)セキュリティチームに明確なガイダンスを提供するように、カスタム **修正** 手順を入力します。
8. (オプション)必要に応じて、クエリエディターから選択したクエリを微調整します。
9. **[保存]** をクリックします。

サポートされているオブジェクト

次のクエリからカスタムポリシーを作成できます。

- 単一リソースクエリ
- クラウドリソース

`Join`演算子を使用したクエリや、リスクやポリシーなどのクラウド以外のエンティティをターゲットとするクエリはサポートされていません。次のオブジェクトは現在サポートされていません。

カテゴリー	オブジェクト
アプリケーション	ソフトウェア ソフトウェアインスタンス
データ	データオブジェクト データタイプ データベーステーブル ファイル

カテゴリー	オブジェクト
IAM	AWS フェデレーションアクセス許可
ネットワーク	ネットワークエンドポイント
ポリシー	ポリシー
リスク	クラウド検出結果 IaC 検出結果 脆弱性インスタンス

クエリデータからのレポートの作成

クエリデータのエクスポートするだけでなく、調査結果を自動レポートに変換して、継続的に監視することもできます。

クエリデータからレポートを作成する方法

1. コンソールで、エクス**プローラー**> **[調査]** に移動します。
2. (オプション)[組織]ドロップダウンで範囲を選択します。
3. 必要に応じてクエリを作成します。
4. **列ピッカー**を使用して、エクスポートに含めるデータを選択します。
5. **[レポート>追加]** をクリックします。[レポートの作成]画面が開きます。
6. 意味のある **名前**を入力します。
7. **納期**:
    - **さて**。1 回限りのレポートを生成します。
    - **スケジュール**。特定の日時にレポートを生成するよう、日次、週次、月次といった頻度を定義します。
8. **[配信方法の追加]** を使用して、レポートのコピーを特定の受信者に送信します。詳細については、「Slack または Teams」を参照してください。

- メールアドレス

  > **注意:** メールでレポートを送信する場合、ファイルサイズは 14.5MB に制限されています。レポートのサイズが大きい場合は圧縮されるか、ダウンロードリンク経由で提供されます。

- Slack チャンネル
- Teams チャネル

9. **[作成]** または **[スケジュール]** をクリックします。

クエリからの検出結果の自動化の作成

自動化を作成して、検出結果ベースのクエリを永続的なルールに変換できます。

1. コンソールで、エクス**プローラー**> **[調査]** に移動します。
2. (オプション)[組織]ドロップダウンで範囲を選択します。
3. 必要に応じてクエリを作成します。
4. **[検出結果の自動化>追加]** をクリックします。[検出結果の自動化を作成] ページが開きます。
5. 自動化設定を行います (左ペイン):
   1. 自動化ルールを正確に説明する **[名前]** と **[説明]** (オプション) を入力します。
   2. ステータス: **[有効]** または **[無効]** のいずれかを選択します。
   3. タイプ: このルールの対象となる検出結果のタイプを定義します。
      - **クラウドの検出結果**
      - **IaC 検出結果**
   4. クエリ
      - **既存のクエリへのリンク**自動化は元のクエリと同期したままになります。リンクされると、クエリを削除したり、非表示にしたり、サポートされていない構文で編集したりすることはできません。
      - **スタンドアロンクエリ**。独立したコピーを作成するか、一から書き込みます。

5. 自動化をトリガーする**ターゲット範囲**を選択します。フォルダー全体を選択すると、そのフォルダー内にあるすべての既存アカウントと今後作成されるアカウントの自動化がトリガーされます。
6. **既存の検出結果に適用**するかどうかを選択します。これを有効にすると、今後の新しい検出結果に加えて、システム内の既存の検出結果すべてに自動化が適用されます。

   > **注意:** このオプションは、新しい検出結果の自動化を作成するとき、または自動化が以前に無効になっていた場合にのみ使用できます。

7. **配信**: **[メソッドの追加]**をクリックして、通知の送信先を設定します。特定の配信方法を統合リストに表示するには、まず統合する必要があります(自動的に表示されるメールアドレスを除く)。

   > メールアドレス

   固定メールリストに送信するには**静的**を選択し、リソース所有者に通知するには**所有者による動的**を選択します。リソースの所有者への送信には、多数の受信者が含まれる場合があります。たとえば、関連付けられたメールアドレスのないグループが所有者になっている場合、Tenable がグループメンバー全員にメールを送信します。

   > Slack チャンネル

   固定チャネルに送信するには**Static**を選択し、リソース所有者に直接通知するには**Dynamic by Owner**を選択します。この場合、受信者数が多くなる可能性があります。

   > Teams チャネル

   固定チャネルに送信するには**Static**を選択し、リソース所有者に直接通知するには**Dynamic by Owner**を選択します。この場合、受信者数が多くなる可能性があります。

   > Jira

統合を有効にしてから、**プロジェクト**、**課題タイプ**、**担当者** (オプション)、[**ラベル**]、[**エピック** (オプション) **環境** (Jiraインスタンスの URL) を選択します。ラベルの場合、Jira インスタンスですでに設定されているラベルのリストから選択するか、Jira に送信される新しいラベルを手動で追加できます。ラベル名にスペースを含めることはできません。

> ServiceNow

統合を有効にしてから、**インスタンス**と**担当者**を選択します。

Datadog 組織

QRadar サーバー

SQS キュー

Splunk イベントコレクター

Webhook

6. **[Create]** (作成) をクリックします。

クエリデータのエクスポート

カスタムクエリの結果を CSV ファイルにエクスポートして、オフラインでの分析、レポート、共有を行うことができます。この機能を使用すると、現在のビューに基づいてクエリデータの完全なスナップショットをキャプチャできます。エクスポートには、現在選択され、ページに表示されている列のすべてのデータが含まれ、エクスポートされたファイルが特定のビューに合わせて調整されます。エクスポートできる行数に制限はありません。

クエリデータをエクスポートする方法

1. コンソールで、エクス**プローラー**> **[調査]** に移動します。
2. (オプション)[組織]ドロップダウンで範囲を選択します。
3. 必要に応じてクエリを作成します。
4. **列ピッカー**を使用して、エクスポートに含めるデータを選択します。
5. **[エクスポート** ⤓] をクリックします。

クエリ結果を表示する

クエリ結果は、**テーブル**または**グラフ**の2つの形式で表示できます。結果領域の右上にあるトグル を使用して、ビューを切り替えます。

テーブルビュー

テーブルビューでは、クエリ結果が構造化された列ベースのレイアウトで表示されます。列は、クエリ内のオブジェクトに応じて自動的に調整されます。

列を追加または削除して、テーブルに表示されるデータを制御できます。

列をカスタマイズする方法

1. クエリを実行します。
2. [列ピッカー] をクリックします。
3. 表示する列を選択します。
    - Joinを使用している場合、列ピッカーに複数のオブジェクトが表示されます。それぞれをクリックして展開し、列を選択します。
    - (オプション)クリックすると、特定のオブジェクトのすべての列 **が選択** されます。

クエリ結果をエクスポートする場合、CSVには現在選択されている列のみが含まれます。

グラフビュー

グラフビューでは、クエリから返されたオブジェクトとそれらの間の関係が視覚化されます。これにより、リソースが検出結果、アイデンティティ、設定を通じてどのように接続、相互に依存している、または関連しているかを理解しやすくなります。

> **注意:** グラフは、Joinを使用するクエリのみをサポートします。結合は、関係グラフとして表現できる結合結果セット (アイデンティティ + 検出結果のペアなど) を生成します。

グラフを操作して、データ構造を探索できます。

- **ノードをドラッグ**して再配置します
- 関係ブランチを**展開または折りたたむ**(可能な場合)。
- **左側のコントロールを使用して**、ズーム、リセット、または全画面表示にします。

グラフの配置方法を変更するには、**[レイアウトの変更]**を使用して、使用可能な視覚化スタイルのいずれかを選択します。

- **シーケンシャル**: 上から下または左から右の明確なフローでノードを配置します。階層パスに適しています。
- **オーガニック**:ノードを均等に広げて、重複を減らします。一般的な人間関係を探るのに適しています。
- **レンズ**:高度に接続されたノードを中央に押し出し、接続の少ないノードを外側に押します。ネットワーク内のハブをハイライトします。
- **構造: 類似の**接続を持つノードをグループ化します。クラスターやパターンを見つけるのに役立ちます。

各レイアウトではノードを編成する方法が異なるため、重要な関係に集中しやすくなります。

サンプルクエリ

以下のサンプルクエリは、Unified Explorer の機能をフル活用するための出発点となります。これらの例を使用して、プロパティと演算子を組み合わせて一般的なセキュリティ上の課題を解決し、独自のカスタムクエリを作成する方法を理解します。

コンプライアンス基準に違反する検出結果のクエリ

特定のコンプライアンス基準に違反する検出結果を特定します。たとえば、SOC2 Type II 基準に違反する、深刻度が重大なオープンクラウド検出結果をすべてクエリします。

クエリをビルドします。

1. まず、**[Cloud Finding]**を選択して、環境内のすべてのクラウド検出結果に対してクエリを実行します。
2. グループ**を追加する**には、三点リーダーをクリックします。

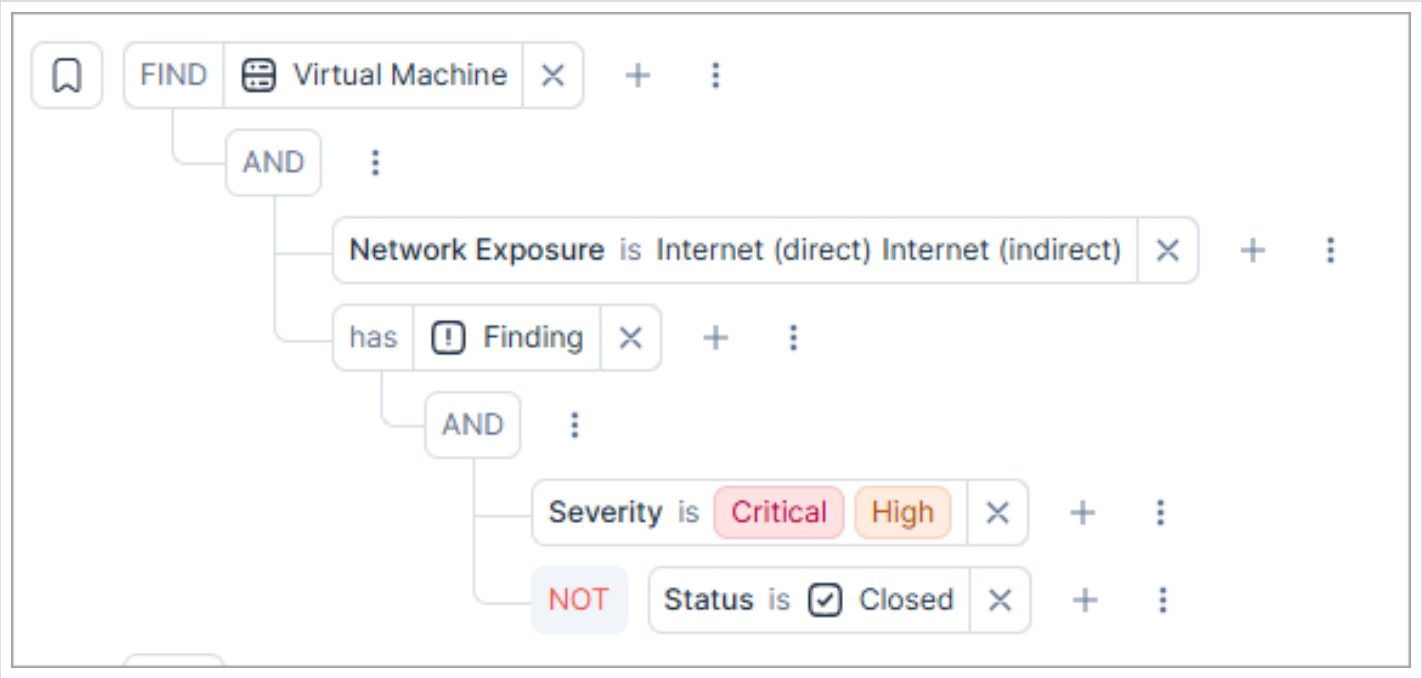
3. 新しいグループで、**[深刻度]** のフィルターを追加し、**[重大]** を選択します。
4. **[ステータス]** のフィルターを追加して、**[開く]** を選択します。
5. 関係フィルターを追加して、**クラウドリソースに関連する**検出結果のみを検出します。
6. **[結合]** をクリックし、**[コンプライアンス違反]** を選択します。
7. [JOIN] で、**[System ID]** のフィルターを追加し、関連する標準を選択します。

一般向け仮想マシンのクエリ

このクエリを使用すると、早急な対応が必要な一般のリスクをもつ仮想マシンを検索できます。

クエリをビルドします。

1. まず、**[仮想マシン]** を選択して、環境内のすべての仮想マシンに対してクエリを実行します。
2. **[ネットワークエクスポージャー]** のフィルターを追加して、**インターネット (直接)** と**インターネット (間接)** を含めます。
3. 関係フィルターを追加して、**検出結果**が関連付けられている VM のみを検出します。
4. **[グループの追加]** をクリックし、And 演算子を使用して、検出結果自体に固有の一連の条件を適用します。このネストされたグループでは、次の条件でフィルタリングします。
    - 深刻**度には、[重大]** および **[高]** の検出結果が含まれます。
    - **[ステータス]** を選択し、**[クローズされた**検出結果] を選択し、Not演算子を適用して除外します。



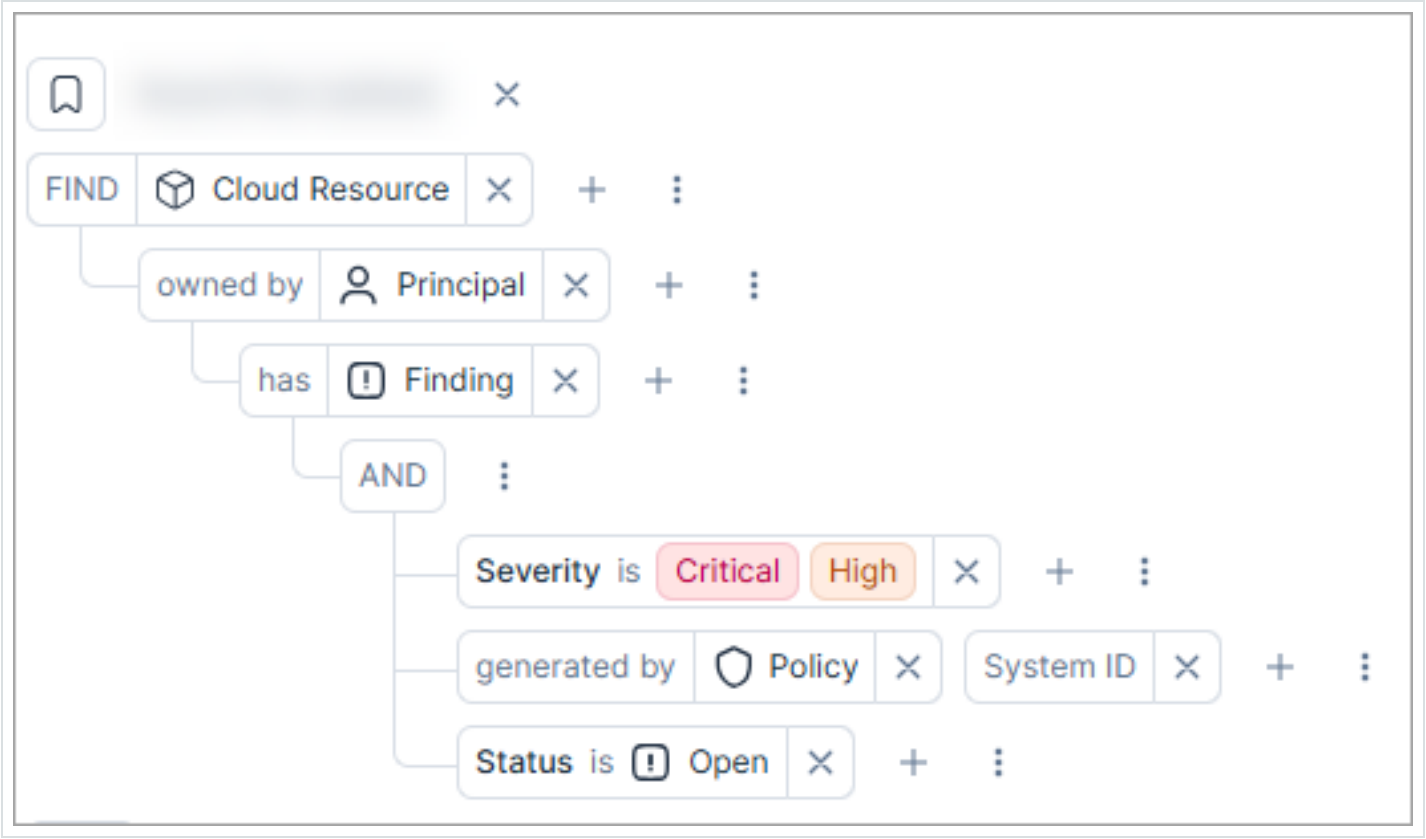
非アクティブな所有者を持つリソースのクエリ

非アクティブポリシーにリンクされたユーザーが所有する、未解決の、高深刻度/重大の検出結果を持つクラウドリソースを検索します。

クエリをビルドします。

1. まず、**[クラウドリソース]** を選択して、環境内のすべてのクラウドリソースタイプに対してクエリを実行します。詳細については、汎用オブジェクトとプラットフォーム固有のオブジェクト を参照してください。
2. 関係フィルターを追加して、**プリンシパル**が所有するリソースを検索します。この文脈におけるプリンシパルは、リソース所有者を表します。
3. 2 つ目の関係フィルターを追加して、検出結果が関連付けられているリソースを見つけます。
4. **[グループの追加]** をクリックし、And 演算子を使用して、検出結果自体に固有の一連の条件を適用します。このネストされたグループでは、次の条件でフィルタリングします。
    - 深刻**度には、[重大]** および **[高]** の検出結果が含まれます。

- 非アクティビティ関連の **ポリシー**によって生成された検出結果。ポリシーのリストを絞り込むには、**[システム ID]** (または **検索ポリシー**) プロパティを使用して、特定のポリシーを選択できます。
- **ステータスにより**、**オープン** の検出結果のみが含まれます。



参照: 検出結果のプロパティ

次のプロパティで検出結果をフィルタリングできます。

プロパティ	説明
無視の有効期限	検出結果が手動で無視される場合、その検出結果が無視される期間を設定できます。この期間は永続的または指定された日付 (例: 1 日、7 日、30 日、90 日、またはカスタムの日付) にすることができます。無視した検出結果が有効期限に達すると、ステー

プロパティ	説明
日	タスは [オープン] に戻ります
オープン時刻	このプロパティは、検出結果が最後にオープンされた日時を示します。これにより、検出結果がいつ再オープンされたか、無視されなかったかが明確に可視化されます。
深刻度	検出結果に割り当てられたリスクレベル。必要なアクションの即時性を示します。可能な値: 重大、高、中、低、情報
スター付き	重要な検出結果にスターを付けて、後で確認できるようにマークできます。
ステータス	検出結果の主なステータス。全体的な状態と進行状況を理解するのに役立ちます。可能な値: Open、Ignored、Closed。
ステータス更新時刻	検出結果のステータスが最後に更新された日時。
サブステータス	検出結果の主なステータスに詳細情報を記載し、そのステータスの具体的な理由を記述します。詳細については、クラウドの検出結果 を参照してください。
システム ID	クラウド サイバーエクスポージャー での検出結果の一意の ID。

FAQ (よくある質問)

> 探索ページの「オブジェクト」とは何ですか、「汎用」オブジェクトと「プラットフォーム固有」オブジェクトの違いは何ですか?

回答: [探索] ページのすべてのクエリは、探索するリソースタイプ (仮想マシンなど) またはポリシーを表すオブジェクトで始まります。さまざまなオブジェクトタイプの詳細については、「汎用オブジェクトとプラットフォーム固有のオブジェクト」を参照してください。

> クエリの一部を削除せずに一時的に無効にすることはできますか?

回答: はい、クエリグループの非表示 / 表示にすることができます。

質問: 「リレーションシップフィルター」と「結合」とは何ですか? また、クエリ結果ではどのように異なりますか?

回答: これらは、オブジェクト間の関係を照会するための 2 つの強力な方法です。詳細については、「関係を追加する」を参照してください。

> クエリ結果の経時変化を追跡できますか?

回答: はい。クエリの保存するときに監視を有効にして、結果の日次スナップショットをキャプチャできます。監視対象クエリでは、過去のトレンドデータがクエリプロファイルのウィジェットとして表示されます。

クエリ

[クエリ] ページでは、利用可能なすべての保存済みクエリを一元的に表示できます。クエリの参照、管理、監視、および個別のクエリプロファイルのクエリベースのウィジェットの表示を行うために使用します。クエリを選択するとクエリプロファイルが開き、詳細とウィジェットを確認できます。

クエリテーブル

[クエリ] テーブルの各行は保存されたクエリを表し、次のものが含まれます。

縦棒	説明
名前	保存済みクエリの名前。
カテゴリー	クエリの保存時に選択されたカテゴリ (例: コンピューティング、コンテナ、データ)。

縦棒	説明
範囲	クエリの主な範囲 (特定のクラウドプロバイダーや環境など)。
可視性	クエリが **パブリック** (組織内のすべてのユーザーに表示) または **プライベート** (作成者にのみ表示) であるかどうかを設定します。
モニタリング済み	Tenable がクエリ結果のスナップショットを毎日キャプチャしているかどうか。監視対象クエリは、クエリプロファイルにウィジェットを表示します。
変更者	クエリを最後に更新したユーザー。ビルトインクエリには常に **Tenable** が表示されます。
変更時刻	クエリが最後に更新された日時。
お気に入り	星のアイコンを切り替えて、頻繁に使用されるクエリをマークします。

星のアイコンを使用してクエリをお気に入りとしてマークし、**[お気に入り]** でフィルタリングして素早く見つけることができます。

Explorer でクエリを開く

保存済みクエリを **Explorer** で開いて、クエリを実行したり、設定を調整したりできます。

クエリを開く方法

1. [>**クエリの調査**] に移動します。
2. 実行するクエリを見つけます。
3. 行を選択するか、三点リーダーメニューを開いて **[エクスプローラーに移動]** を選択します。

選択したクエリが適用された状態で Explorer ページが読み込まれます。そこから、フィルター、リレーションシップ、その他の設定を変更し、必要に応じて **[保存]** または **[名前を付けて保存]** を使用できます。詳細については、「 クエリの保存 」を参照してください。

クエリのモニタリング

クエリを監視すると、監視を有効にした時点から、結果のスナップショットを毎日キャプチャするようにTenableに指示されます。この履歴データは、クエリプロファイルにウィジェットとして表示され、カスタムダッシュボードで使用するためにウィジェットバンクで利用できます。

Explorerにクエリを保存するときに監視を有効にできます。

クエリウィジェット

各クエリプロファイルには、そのクエリで使用可能なウィジェットを表示する**[ウィジェット]**タブがあります。ウィジェットにはモニタリングを通じて取得された履歴データが反映され、クエリタイプによって異なります。

クエリタイプ	ウィジェット
すべてのクエリ	アイテム数、テーブル
クラウド/IaCの検出結果(監視対象)	深刻度別の検出結果、検出結果のトレンド、検出結果のMTTR、検出結果アクティビティ、トレンド
クラウドリソース(監視対象)	トレンド

ウィジェットバンクはカスタムダッシュボードで使用することもできます。

クエリの複製

クエリを複製して、ビルトインまたは既存のカスタムクエリを新しいクエリのテンプレートとして使用する。

クエリを複製する方法

1. [>**クエリの調査**]に移動します。
2. 複製するクエリを見つけます。
3. 行を選択するか、三点リーダーメニューを開いて**[複製]**を選択します。

4. [クエリ] ダイアログで、必要に応じて次の値を調整します。
    1. **名前**
    2. **カテゴリー**
    3. **可視化:**
        - **パブリック:** 組織内のすべてのユーザーに表示されます。
        - **プライベート:** 自分だけが閲覧できます。
5. **[追加]** をクリックします。

カスタムクエリの削除

[クエリ] ページからカスタムクエリを削除して、ワークスペースを整理できます。ビルトインクエリはシステムによって提供され、削除または変更することはできません。

> **警告:** クエリの削除は永続的です。
>
> - クエリが [パブリック] とマークされている場合、削除すると組織内のすべてのユーザーに対してそのクエリが削除されます。
> - クエリが監視されている場合、削除すると保存されている履歴データもすべて完全に削除されます。

クエリを削除する方法

1. [>**クエリの調査**] に移動します。
2. 削除する 1 つまたは複数のクエリの横のチェックボックスを選択します。
3. **[削除]** をクリックします。

インベントリ

資産インベントリの表示

> **注意:** 一部のビューは、Cloud Vulnerability Management ライセンスでは使用できません。

[Inventory] (インベントリ) ビューを使用すると、マルチクラウド環境に関するさまざまな重要事項を確認できます。たとえば、次のことが可能です。

- インターネットに公開されているが、高い権限を持つサービスアカウントで実行されている、AWS 環境内の実行中の EC2 インスタンスすべてを表示します。
- Microsoft Entra ID で、ゲストユーザーであり、Azure サブスクリプションまたは AWS アカウントで高い権限を持っているすべてのユーザーを表示します。
- x 日数の間に使用されていない、機密性の高いアクセス許可を持つすべての過剰な権限を持つユーザーを表示します。

[インベントリ] ビューが解決するのに役立つ重要なユースケースについては、一般的なインベントリユースケースを参照してください。

[インベントリ] ビューには、クラウドプロバイダーやアイデンティティプロバイダーで区切ることなく、すべてのリソースカテゴリがまとめて一覧表示されます。特定のプロバイダーのリソースを表示するには、コンソール上部にある組織セレクターを使用します。インベントリ全体を検索する、マルチクラウド環境全体のリソースを見つけることもできます。

各ビューは、すべてのクラウドプロバイダーと IdP に関連する製品カテゴリ別に分類されます。

- AI
- コンピューティングリソース
- コンテナ
- データ
- IAM
- Kubernetes
- 管理
- ネットワーク
- セキュリティ

上記の各カテゴリには、環境内の実際のリソースに応じて、ベンダー固有のリソースタイプが含まれています。たとえば、**[IAM]** カテゴリには、AWS IAM ユーザー、Azure サービスプリンシパル、Google Cloud ロールを含めることができ、これらは可視性を容易にするためにすべてグループ化されます。

資産インベントリを表示する方法

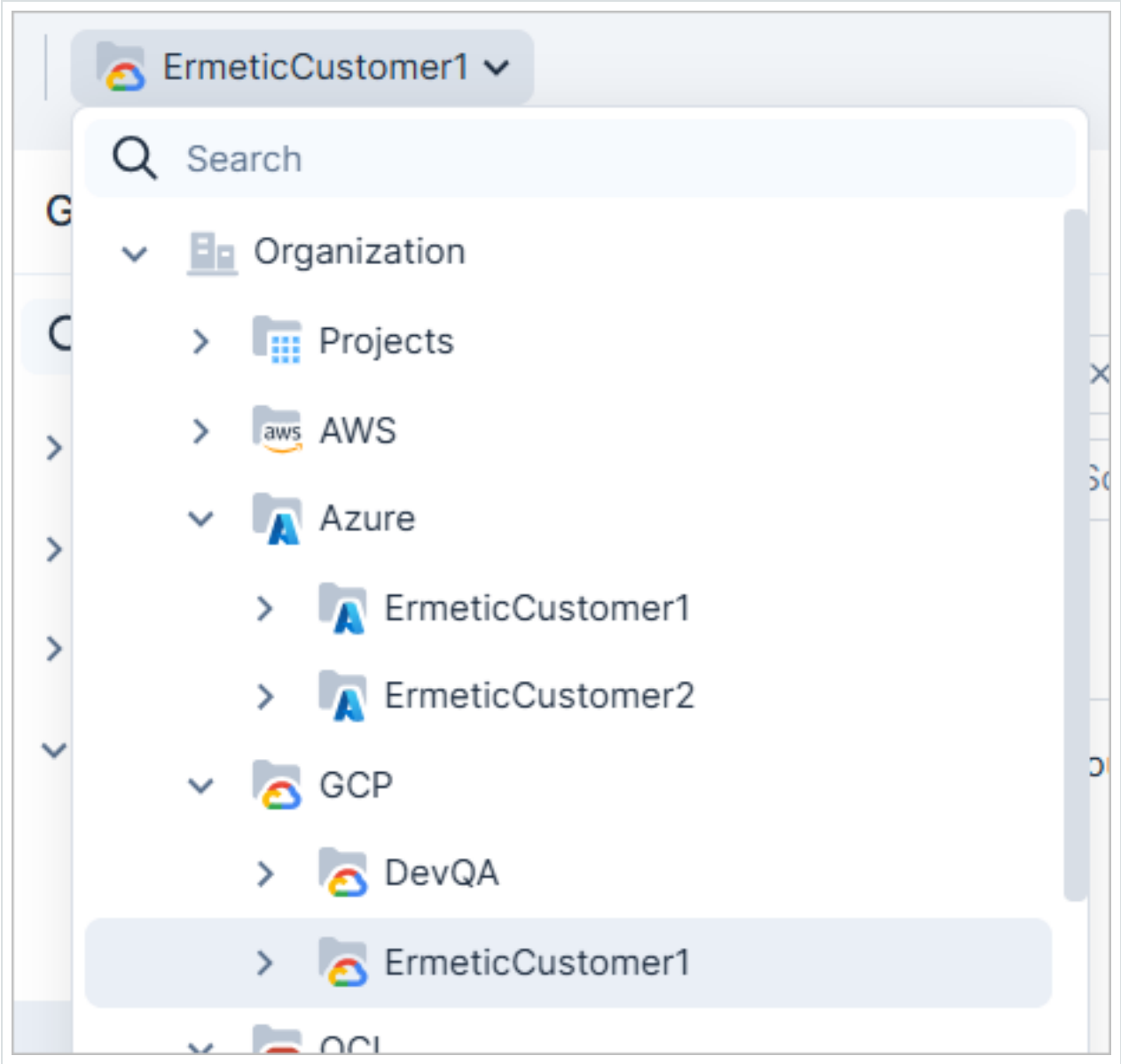
1. Tenable One Cloud Exposure コンソールで、**[調査]** に移動し、**[インベントリ]** をクリックします。
2. [Inventory] (インベントリ) ビューで、表示する関連カテゴリとリソースタイプを検索して選択します (たとえば、**[コンピューティング]** > **[AWS EC2 インスタンス]** などです。
3. テーブル右上の列ピッカーを使用して、どの列を表示するか選びます。
4. 資産インベントリのフィルタリング 、表示されるデータの範囲を変更します。表示されるリソース要素 (フィルターや列) はリソースタイプごとに異なります。たとえば、EC2 インスタンスの場合、特定のタグでフィルタリングできます (タグは、クラウドサービスプロバイダーで定義され、クラウドサイバーエクスポージャー内でインポートされます)。
5. ドリルダウンして、リソースの詳細の表示 。

資産インベントリのフィルタリング

表上部にあるフィルターを使用して、表示されるデータの範囲を絞り込みます (詳細については、データのフィルタリング参照してください)。

- **[+]** ボタンをクリックして、フィルターを追加します。
- 検索語句で表をフィルタリングするには、**[一致するものを選択]** をクリックします。
- 一部のリソースには、特定のフィルターや列に一致する値がない場合があります。フィルターの値がある すべてのリソースで表をフィルタリングするには、**[すべて選択]** をクリックします。

特定のアカウントまたはアカウントグループのリソースのみを表示するように、[インベントリ] ページの上部で組織またはアカウントでフィルタリングすることもできます。詳細については、アカウント階層とフォルダー参照してください。



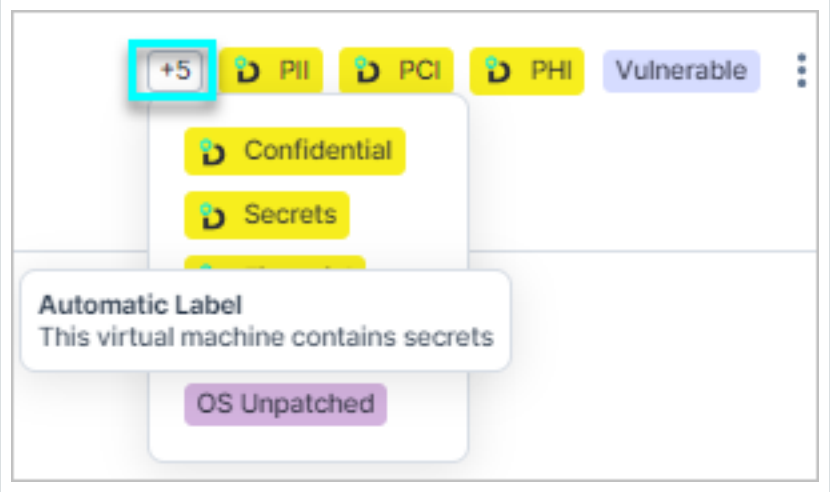
利用可能なフィルターは各リソースタイプによって異なりますが、以下のグローバルフィルターはすべてのリソースタイプで使用できます:

- **ラベル**。適用されているかどうかに関わらず、リソースに適用されているすべてのラベルを表示します。
    - 手動 (**[設定]** > **[インベントリ]** > **[ラベル]** から)
    - タグ、またはタグキーと値に基づいて自動的に実行されます (**[設定]** > **[インベントリ]** > **[ラベ**

ル] を介して)。この方法で作成されたラベルの横にフラグアイコン が表示されます。

- 自動適用。システムによって適用される。

ラベルのタグにカーソルを合わせると、詳細を確認できます。リソースに複数のラベルがある場合、アイコンをクリックするとその他のラベルが表示されます。



詳細については、ラベルのリソースへの適用 参照してください。

- **検出結果**。指定されたリソースタイプのリソースに関連するすべての検出結果が表示されます。
- **検出結果の深刻度**。リソースに関連する検出結果の深刻度を示します。

  Critical

  High

  Medium

  Low

  Informational

  リソースの検出結果が複数の場合は、最も深刻度の高い検出結果が表示されます。たとえば、リソースに関連する検出結果が2つあり、1つの深刻度が「重大」で、もう1つの深刻度が「中」である場合、[検出結果] 列には [重大] と表示されます。

スケジュールされたレポートの作成

[インベントリ] ビューから直接、スケジュールされたレポートを作成します。このとき、レポートのコンテンツは表に適用した特定のフィルターに基づいています。たとえば、秘密を漏洩するインターネットに公開されているすべてのEC2インスタンスについてスケジュールされたレポートを作成できます。レポートは、その時点でテーブルに適用されているフィルターに従って作成されます。出力データはCSV形式で、クラウドサイバーエクスポージャーコンソールの各リソースページのURLなど、関連するリソースデータがすべて含まれます。

スケジュールされたレポートの作成方法

1. クラウドサイバーエクスポージャーコンソールで、**[調査]** > **[インベントリ]** に移動します。
2. [Inventory] (インベントリ) ビューで、表示する関連カテゴリとリソースタイプを選択します (たとえば、**[コンピューティング]** > **[EC2 インスタンス]** などです。
3. 関連する資産インベントリのフィルタリングを適用します。
4. 表の右上にある **[Report] (レポート)** ボタンをクリックします。
5. レポートの詳細を入力します。詳細は、レポートの作成 参照してください。
6. **[スケジュール]** または **[の生成]** をクリックします。
7. [Reports] (レポート) ページでレポートの詳細情報を確認できます。

インベントリデータのエクスポート

リソースタイプ別に、任意のインベントリビューのすべてのデータをエクスポートします。たとえば、すべての仮想マシンインベントリデータをエクスポートします。データは、その時点でテーブルに適用されているフィルターに従ってエクスポートされます。出力データはCSV形式で、クラウドサイバーエクスポージャーコンソールの各リソースページのURLなど、関連するリソースデータがすべて含まれます。エクスポートできる結果の数は無制限です。

または、特定のアカウント階層とフォルダー内のすべてのリソースタイプのスケジュールされたレポートの作成こともできます。

インベントリデータのエクスポート方法

1. クラウドサイバーエクスポージャーコンソールで、**[調査]** > **[インベントリ]** に移動します。
2. [Inventory] (インベントリ) ビューで、表示する関連カテゴリとリソースタイプを選択します (たとえば、[コンピューティング] > [EC2 インスタンス] などです。
3. 関連する資産インベントリのフィルタリングを適用します。
4. テーブルの右上にある **[Export]** ボタンをクリックします。

インベントリ全体を検索する

グローバル検索を使用して、マルチクラウド環境全体のユーザー、ロール、リソースを検索します。検索は、組織セレクターで選択された組織またはアカウント範囲に応じてフィルタリングされます。たとえば、Azure アカウントのみを表示するフィルターを適用した場合、AWS または GCP のリソースはインベントリ検索で表示されません。

検索では、入力として以下を含むリソースプロパティの全範囲がサポートされています。

- Resource name
- Email
- IP アドレス
- ARN (AWS 用)
- アクセスキー
- Azure Application ID

表示しているページに関係なく、検索バーがクラウドサイバーエクスポージャーコンソールの上部に表示されます。

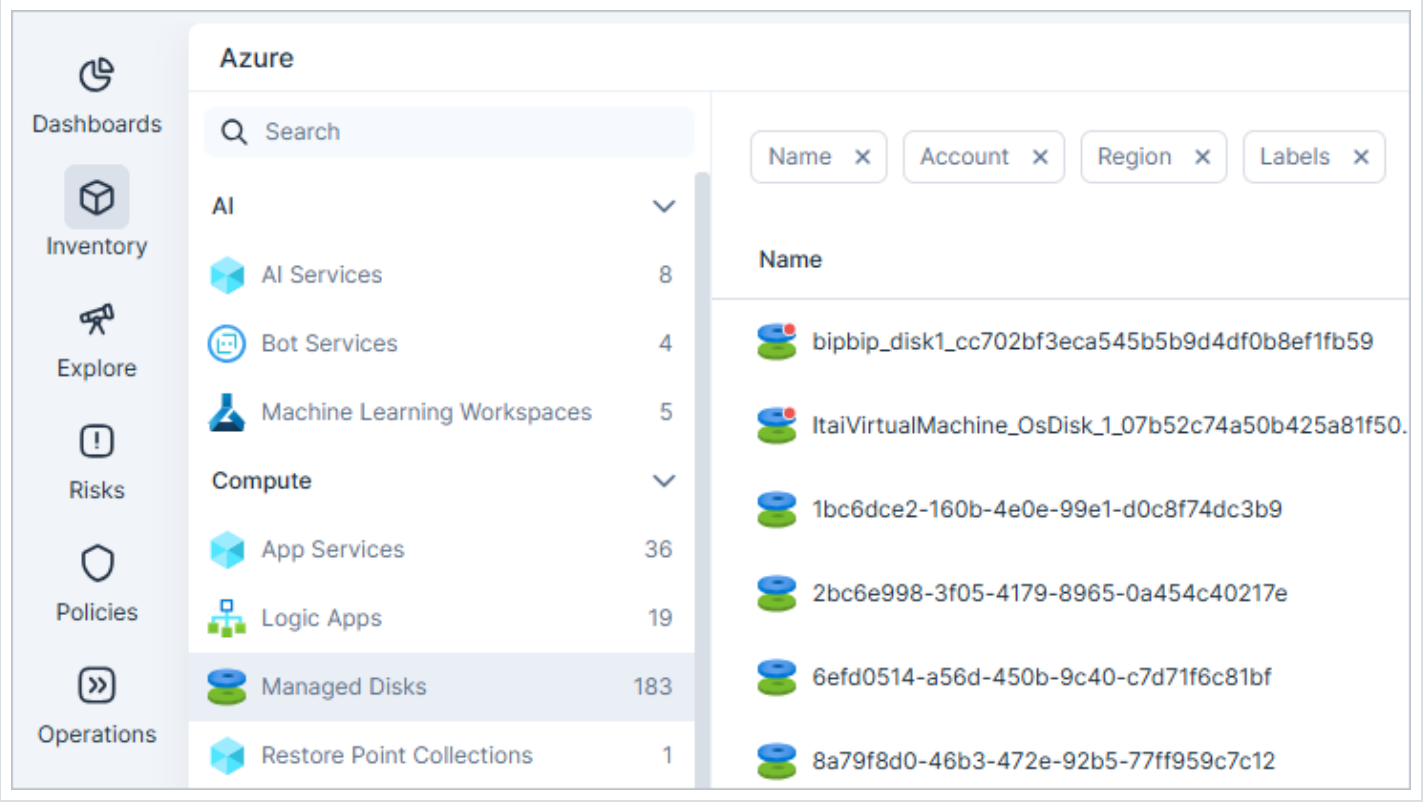
> **注意:** 検索を使用して、環境全体のポリシー、ページ、ドキュメント、脆弱性を見つけることもでき、必要なものを操作し、見つけるための単一の合理化された方法を提供します。

インベントリ全体を検索する方法

1. (オプション) 検索対象をアカウントのサブセットに限定するには、組織セレクターで範囲を選択します。
2. コンソールの上部にある検索ボックスに検索する語句を入力します。

入力すると、結果のリストと、その時点の検索語句の結果の総数が表示されます。また、結果はリソースタイプ別に分類されるため、一致するすべての結果をタイプ別に確認できます。リストをスクロールすると結果のすべてを閲覧できます。

3. 検索に最も一致する関連リソースをクリックします。



一般的なインベントリユースケース

このセクションでは、[Inventory] (インベントリ) ビューが役立つ一般的なユースケースの概要について説明します。

パブリックリソースを検出する

[Inventory] (インベントリ) ビューを使用して、インターネットに公開されているリソースを以下のいずれかで検出します。

- **ネットワーク。** 以下に例を挙げます。
  - Azure の SQL サーバー (データ)
  - AWS の EC2 インスタンス (コンピューティング)
  - AWS の RDS インスタンス (データ)
  - GCP の VM インスタンス (コンピューティング)
- **IAM ポリシー**IP アドレスを持たず、エクスポージャーを把握する唯一の方法がアクセス許可を通じてのみであるリソースです。以下に例を挙げます。
  - GCP のストレージバケット (データ)
  - AWS の S3 バケット (データ)

一般に公開されているリソースを検出する方法

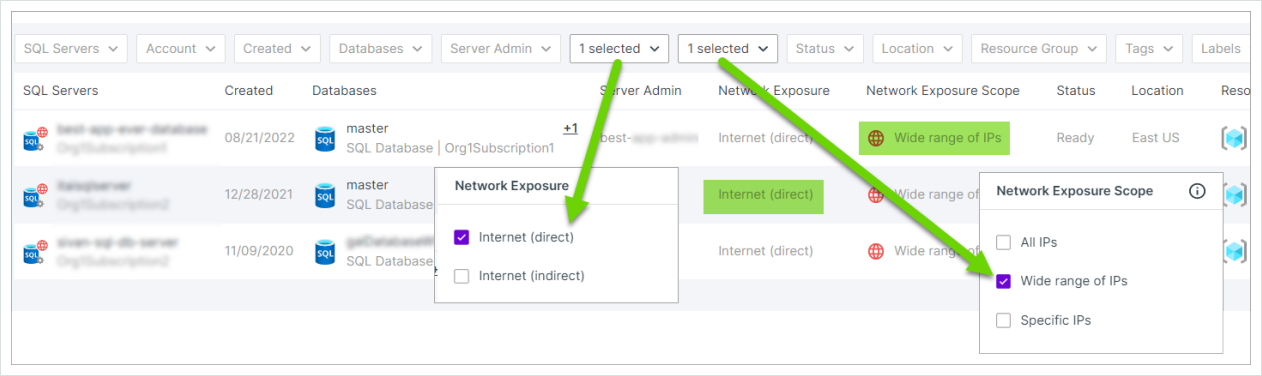
1. 資産インベントリを表示します。
   1. Tenable One Cloud Exposureコンソールで、**[インベントリの調査>]** に移動します。
   2. [Inventory] (インベントリ) ビューで、表示する関連カテゴリとリソースタイプを選択します (たとえば、**Azure SQL Server >データ**です。
2. ネットワークを介して公開されているリソースの場合は、次のフィルターを選択して 資産インベントリのフィルタリング 。
   1. [ネットワークエクスポージャー] フィルターで、**[インターネット (直接)]** をクリックして、インターネットに直接公開されているリソースをフィルタリングします。

      > **注意: インターネット (間接))** は、ロードバランサーなどを介してインターネットに間接的に公開していることを示します。

   2. [Network Exposure Scope] (ネットワークエクスポージャー範囲) フィルターで、**[広範囲の IP]** をクリックして、広範囲の IP アドレスに公開されているリソースをフィルタリングします。

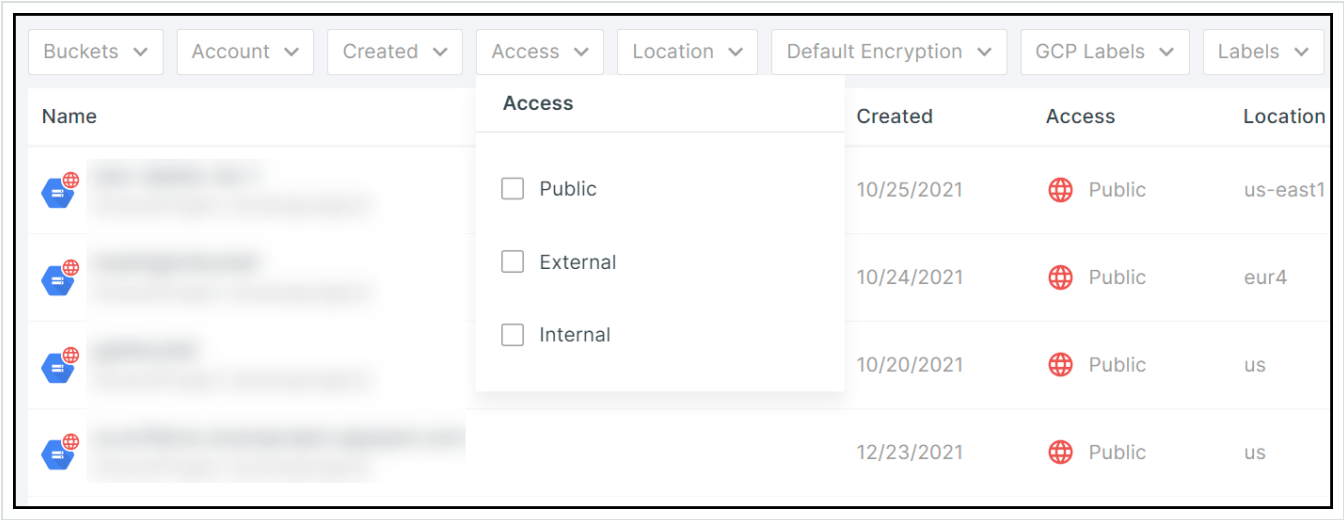
      > **注意:** この文脈での**広範囲** とは、リソースが 255 を超える IP アドレスに公開されており、また

そのリソースにアクセスできるユーザーが不 明 であることを意 味します。



3. IAM ポリシーを介して公 開されているリソースの場 合 は、次 のようにアクセスフィルターを使 用して 資産 インベントリのフィルタリング 。

    1. Public (パブリック)。リソースはー 般 に公 開されています。
    2. External (外 部) (GCP のみ)。リソースは、Workspace でローカルに定 義されていない外 部 の Google グループおよびユーザーに公 開されています。
    3. Internal (内 部)。リソースは内 部 に定 義されたリソースにのみ公 開されています。



注 意 : [Cross account] (クロスアカウント) オプションが [Access] (アクセス) フィルターに表 示される場 合もあります。これは、1 つのアカウント から複 数 の異なるアカウント のアイデンティティに対してアクセスを公 開しているリソースについてフィルターを適 用 するために使 用されます。

4. リソースをドリルダウンして、ネット ワークエクスポージャーの視 覚 化 (グラフ)します。

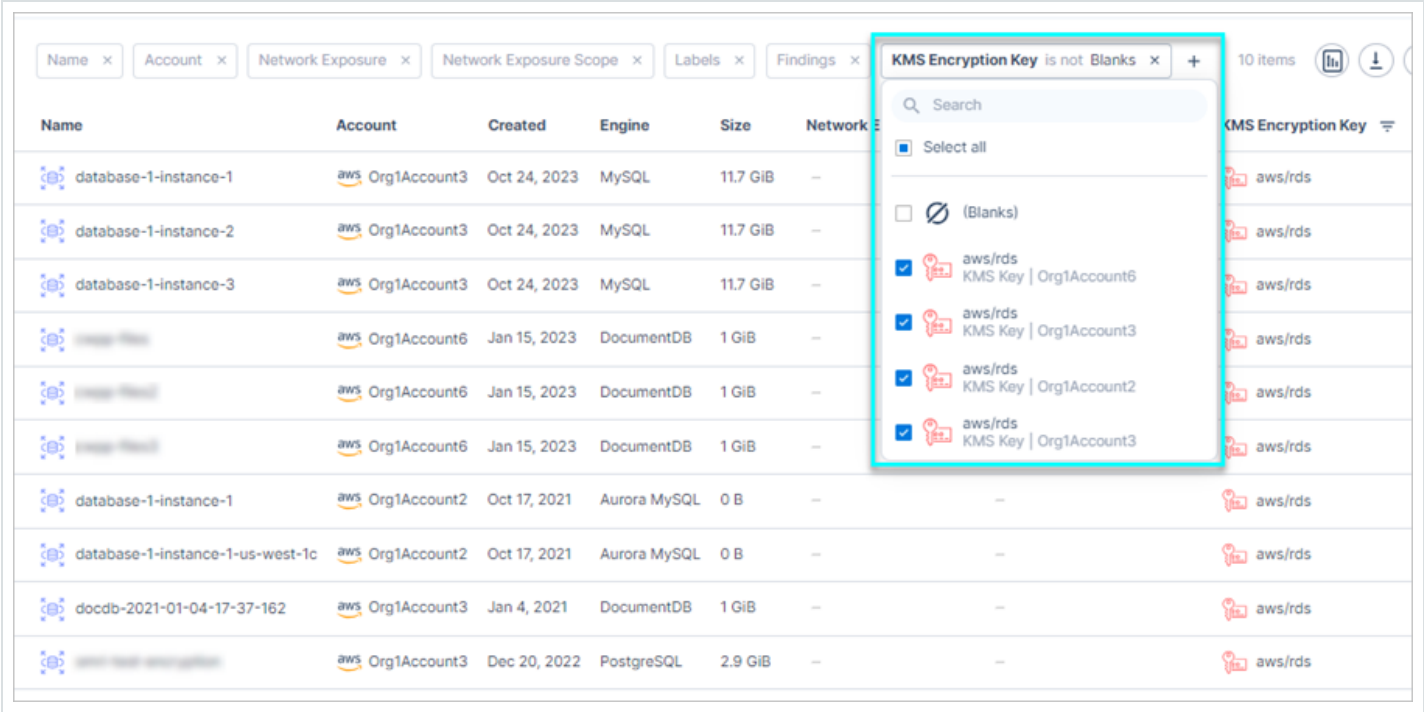
データを保護する暗号化キーの検索

[インベントリ] ビューを使用して次の操作を行います。

- データ保護のために使用される暗号化キーを検索し、機密度の高いデータすべてが暗号化されていることを確認する。
- 各リソースが独自の暗号化キーを使用していることを確認するために、どのキーがどのデータを暗号化するかについてモニタリングする。

暗号化キーを見つけるには

1. 資産インベントリの表示。
    1. クラウドサイバーエクスポージャーコンソールで、**[インベントリの調査>]** に移動します。
    2. [Inventory] (インベントリ) ビューで、表示する関連カテゴリとリソースタイプを選択します (たとえば、**RDS インスタンスAWSデータ>**です。
2. **KMS 暗号化キー**フィルターを追加して資産インベントリのフィルタリング、指定したリソースタイプに使用されるすべてのキーのリストを表示します。
3. 特定のキーを 1 つ以上選択すると、そのキーによって保護されているリソースが表示されます。
    - キーを持つすべてのリソースを表示するには、**[すべて選択]** をクリックし、**[(空白)]** オプションのチェックを外します。
    - キーを持っていないすべてのリソースを表示するには、**[(空白])** オプションのみクリックします。

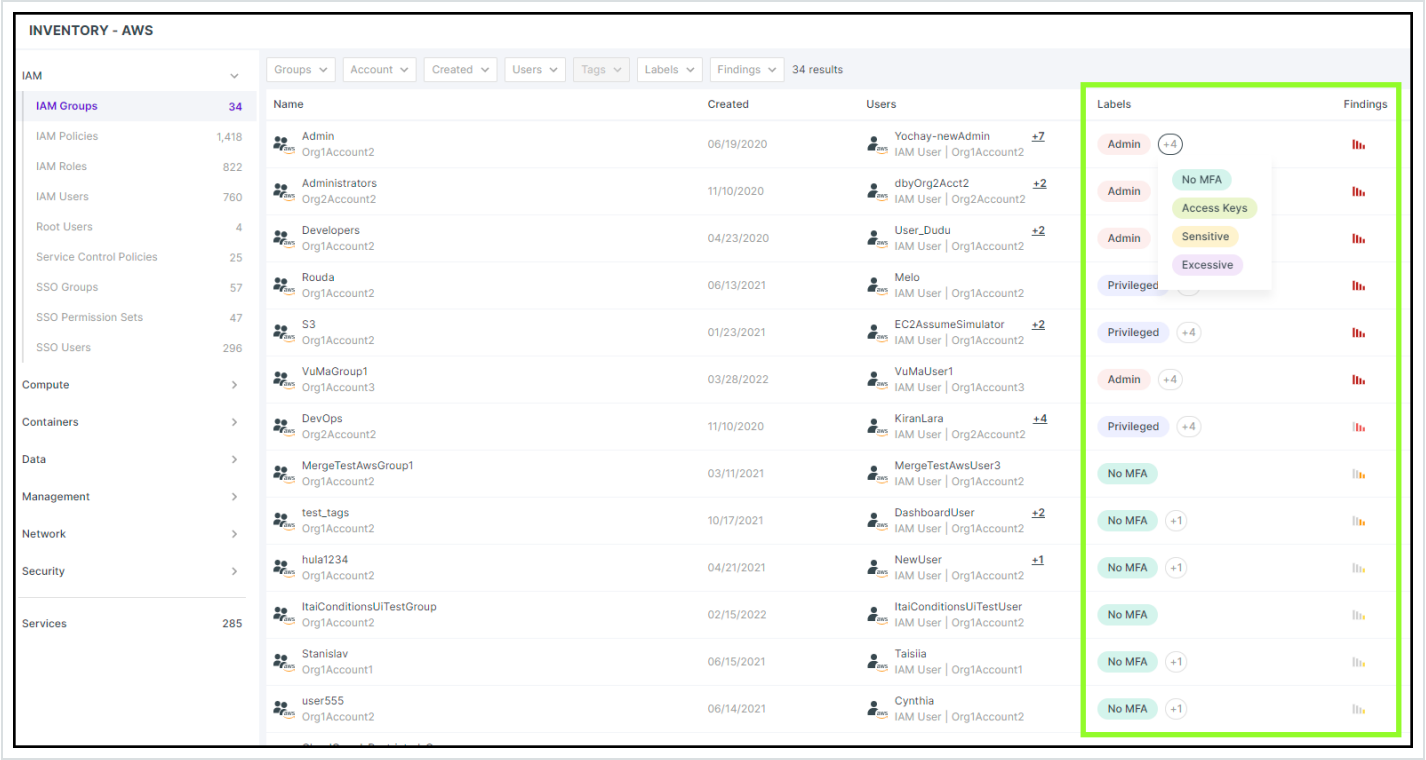


インベントリ内のリスクを検出する

[Inventory] (インベントリ) ビューを使用して、環境内のリソース間のリスクを検出します。

インベントリでリスクのあるリソースを見つける方法

1. 資産インベントリの表示。
    1. クラウドサイバーエクスポージャーコンソールで、**[インベントリの調査>]** に移動します。
    2. [Inventory] (インベントリ) ビューで、表示する関連カテゴリとリソースタイプを選択します (たとえば、**IAM > AWS IAM グループ**です。
2. ラベルや検出結果でフィルタリングまたはソートすることで、資産インベントリのフィルタリングします。
    1. [Admin] (管理者) や [No MFA] (MFA なし) など、高リスクであることを示すラベルを持つリソースを表示します。
    2. 関連する検出結果を持つリソースを深刻度に従って一覧表示します。

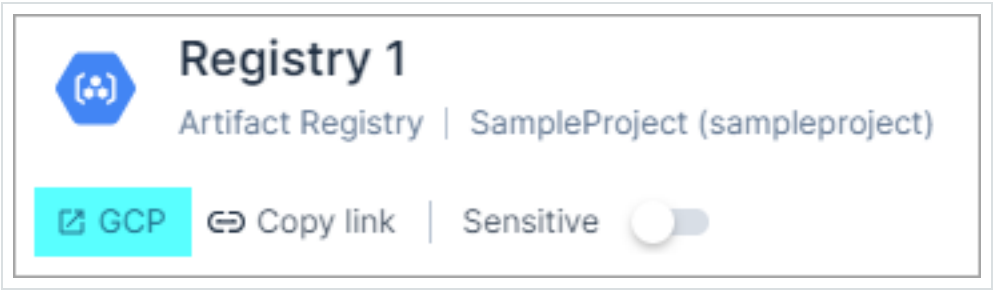


リソースの詳細の表示

インベントリ内のリソースをクリックすると、そのリソースに関する詳細な情報が表示されます。

クラウドコンソールでリソースを表示する

リソース名の下にあるリンクをクリックすると、関連するクラウドコンソールにリソースが表示されます。



機密度の高いリソースをマークする

リソースを次の目的で機密としてマークします。

- リソースに関連する検出結果、またはリソースにアクセス権を持つアイデンティティの優先度を上げる。
- リソースに次の場所で機密性が高いというラベルを付ける Tenable One Cloud Exposure

たとえば、コンプライアンスのリソース (PII、PCI、HIPAA など) を機密としてマークできます。

リソースをセンシティブとしてマークする機能は、すべてのクラウドサービスプロバイダーのほとんどのリソースカテゴリ (IAM を除く) で利用できます。

リソースをセンシティブとしてマークするには

1. 資産インベントリの表示。
    1. クラウドサイバーエクスポージャーコンソールで、**[Inventory] (インベントリ)** にカーソルを合わせて展開します。
    2. 表示するクラウドプロバイダーまたは IdP のインベントリをクリックします (**例: GCP**)。
    3. [Inventory] (インベントリ) ビューで、表示する関連カテゴリとリソースタイプを選択します (たとえば、**コンテナ** > **アーティファクトレジストリ** (GCP 内) です。
2. リソースをクリックしてドリルダウンします。
3. ページ上部のリソース名の下にある **[機密]** トグルをクリックします。

    クラウドサイバーエクスポージャーコンソール全体のリソースアイコンの右上に、このリソースが機密としてマークされていることを示す赤い円が表示されるようになりました。



ラベルのリソースへの適用

関連するインベントリ(プロパティとラベル)リソースに適用して、リスク評価のための文脈情報を追加します。ラベルを過剰なアクセス許可やネットワークエクスポージャーなどの要因と関連付けることで、クラウドサイバーエクスポージャー環境をさらに充実させることができます。たとえば、機密度の高いバケットやデータベース、または脆弱性のあるインスタンスにラベルを適用できます。

> **注意:** クラウドサイバーエクスポージャーでは、組み込みのシステムラベルもリソースに自動的に適用されます。完全なリストについては、組み込みシステムラベルを参照してください。

前提条件

- インベントリ(プロパティとラベル)

ラベルをリソースに手動で適用する方法

1. 資産インベントリの表示。
    1. クラウドサイバーエクスポージャーコンソールで、**[Inventory] (インベントリ)** にカーソルを合わせて展開します。
    2. 表示するクラウドプロバイダーまたはIdPのインベントリをクリックします(例: AWS)。
    3. [Inventory] (インベントリ)ビューで、表示する関連カテゴリとリソースタイプを選択します(たとえば、**コンピューティング> EC2インスタンス** (AWS)などです。
2. 関連するページからは、次の操作を実行できます。
    - **複数のリソースにラベルを追加します**。
        1. 関連するリソースの横にあるチェックボックスを選択します。
        2. ページ下部にある**[ラベルの追加]**をクリックします。
        3. 関連するラベルを選択し、**[追加]**をクリックします。
    - **単一リソースのラベルを編集する**
        1. リソースの横にある三点リーダーアイコンをクリックし、**[ラベルの編集]**をクリックします。
        2. 関連するラベルを選択して、選択したラベルを追加またはチェック解除し、**[保存]**をクリックします。

リソースに関する詳細の取得

[概要] をクリックすると、以下のようなリソースに関する詳細が表示されます。

- 一般的なリソースの詳細 (リソースタイプ、アカウント、割り当てられたタグなど)
- インベントリ (プロパティとラベル)。関連するクラウドプロバイダー環境において、フィールドで定義されたパターンに一致するキーと値のペアでタグ付けされたリソースに値が設定されます。
- (該当する場合) リソースを作成したアイデンティティやオリジネータ (作成者)
- 関連するネットワーク情報 (VPC、サブネット、セキュリティグループなど)
- 関連付けられているポリシー、ユーザー、グループ
- 履歴データ

リソースに関連付けられた詳細の多くは、それ自体がクラウドサイバーエクスポージャー内のリソースであり、クリックするとドリルダウンできます。たとえばEC2リソースが表示されているときに、[Network] (ネットワーク) エリアのサブネットをクリックすると、その詳細を確認できます。

リソースの関係を確認する

[調査] の下の **[グラフ]** タブには、リソースと他のクラウドエンティティとの関係が表示されます。グラフを使用して、リソースがアイデンティティ、検出結果、関連リソースにどのように接続しているかを追跡できます。これにより、アクセスパスを調査し、リスクの影響を評価できます。

プロファイルのリソースが、グラフの中心エンティティとして表示されます。このエンティティを削除することはできず、クラウドサイバーエクスポージャーは追加したエンティティとは異なる方法でマークします。

> **注意:** この **[グラフ]** タブは、ネットワークエクスポージャーマップとは異なります。リソースのネットワークパスのマップについては、「ネットワークエクスポージャーの視覚化 (グラフ)」を参照してください。

リソースの関係を探索する方法

1. **[インベントリ>調査]** をクリックします。
2. リソースを検索し、クリックしてプロファイルページを開きます。
3. 左側のメニューの **[調査]** で、**[グラフ]** をクリックします。

   [グラフ] タブが開き、リソースが中央エンティティとして表示されます。
4. エンティティの横にある + ボタンをクリックします。

利用可能な関係のリストがカテゴリ別にグループ化されて開きます。

5. リレーションシップを選択します。

   関連エンティティはグラフ上に表示され、ラベル付けされたエッジ (例: has、relates to、involved in) によってリソースに接続されます。

6. (オプション)エンティティの横にある + ボタンをクリックして、グラフをさらに展開します。

> **注意:** グラフにプロファイルリソースのみが表示されている場合、**[+]** ボタンはカーソルを合わせずに表示されたままになるため、探索の開始点が常に表示されます。

関連するリスクの表示と管理

左側の [リスク] メニューセクションで次のいずれかをクリックして、リソースに関連する潜在的なリスクを表示します (該当する場合)。

- **クラウドの検出結果**
- **脅威検出**
- **脆弱性**
- **悪意のあるファイル**

センシティブデータの表示

左側の [データ] メニューセクションで次のいずれかをクリックして、スキャン済みリソースで検出された機密データを表示します。

- **概要**
- **機密データ**
  詳細については、データリソースを参照してください。

ネットワークデータの表示

[ネットワーク] セクションを使用して、クラウドリソースのネットワーク接続を表示および分析します。このセクションは、すべてのクラウドにわたる重要なリソースの範囲で使用できます。たとえば、AWS EC2 および

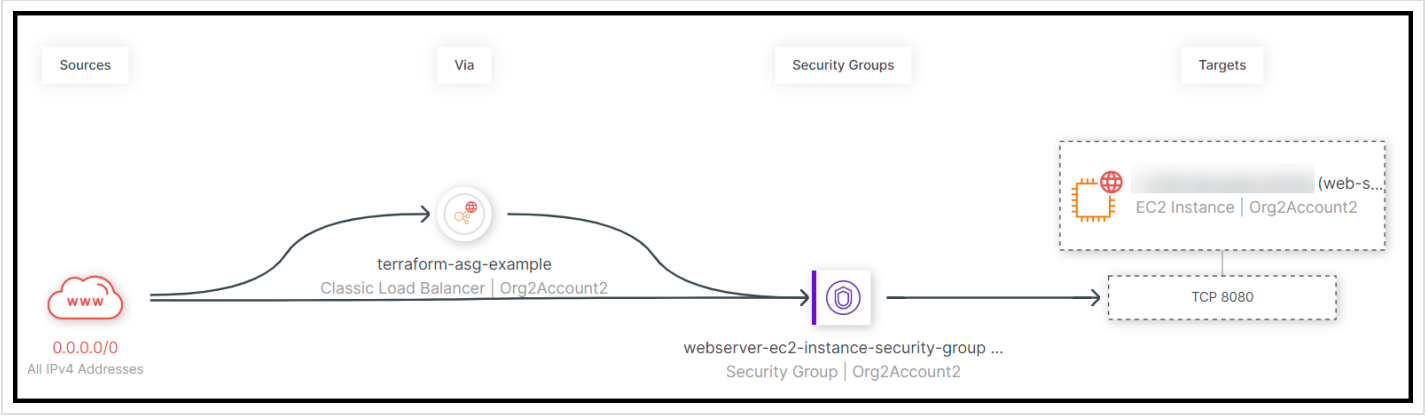
RDS インスタンス、Azure 仮想マシン、GCP VM インスタンスおよびインスタンスグループなどです。リソースの完全なリストについては、「サポートされているリソース を参照してください。

ネットワークエクスポージャーの視覚化 (グラフ)

[グラフ] タブは、リソースへのネットワークパスを視覚的にマップします。これは、リソースが直接、またはロードバランサーなどの中間コンポーネントを介してインターネットにどのように公開されているかを理解するのに役立ちます。

マップは以下の 4 つの一般エリアに分かれています:

- **ソース**。リソースにアクセスできる IP アドレス範囲 (CIDR ブロック) です。
- **経由**。ロードバランサーなどを介してインターネットに間接的に公開されているリソースの場合、トラフィックをルーティングするメカニズムを示す列「Via (経由)」が追加で表示されます。
- **セキュリティグループ / ネットワークセキュリティグループ / セキュリティ境界** リソースインスタンスへの送受信トラフィックを制御する仮想ファイヤーウォールです。
- **ターゲット**。指定されたリソースのターゲットポートです。センシティブなポートは赤でマークされています。



ネットワークマップを操作するには

1. リソースプロファイルビューで、「**ネットワーク**」をクリックし、「**グラフ**」タブに移動します。
2. マップ内を移動するには、マウスをクリックしてドラッグします。

3. マップを拡大および縮小するには、[Ctrl]キーを押しながらマウスホイールをスクロールします(またはマップをダブルクリックして拡大します)。 をクリックすると、ズームアウトしてマップ全体が表示されます。
4. グラフ上のリソースに関する詳細を確認する、またはリソースに基づいてグラフをフィルタリングするには、リソースアイコンを右クリックします。
5. マップをフィルタリングするには、マップの上部にあるフィルターを使用します。
    - IP アドレス範囲、セキュリティグループ、またはポートでフィルタリングします。
    - 広範囲 (255 を超える) の IP アドレスのセットに公開されているポートをフィルタリングするには、**[広い範囲]** をクリックします。

ネットワークエンドポイント

[ネットワークエンドポイント] タブには、特定のリソースについて確認済みで到達可能なエントリポイントのリストが表示されます。このビューでは、ネットワークスキャナーによって検証されたエンドポイントのみがリストされます。

列	説明
ネットワークエンドポイント	宛先ホストとポートの組み合わせ (例: `10.0.0.5:443`)。
ソース IP アドレス範囲	リソースのネットワークルールで定義されている許可されたソース IP 範囲。これは、リソースにアクセスできる範囲です。
プロトコル	テストされたプロトコル (現在 TCP)。
スキャン時間	最後に成功した検証のタイムスタンプ。

確認されたエンドポイントを表示するには

1. リソースプロファイルビューで、 Network
2. **[ネットワークエンドポイント]** タブに移動します。
3. 表で確認されたライブエクスポージャーを確認します。

> **注意:** エンドポイントがリストにない場合は、ネットワークのエクスポージャーか、スキャナーが接続を確立できなかった、またはリソースタイプがネットワークのエクスポージャーされていないことを意味します。

ネットワークスキャンステータス

[ネットワークスキャンステータス] 列/フィールドは、リソースの現在のスキャンステータスを示します。次の表は、さまざまなステータスとそれに関連する理由の表示を示しています (理由の一部はステータスの横にツールチップとして表示されます)。

ネットワークスキャンステータス	Reasons
無効	設定でリソースのスキャンが無効になっています
サポート対象外	スキャンは、直接 IP アドレスとポートを持つサポートされているリソースでのみサポートされます。詳細は、ネットワークスキャナーを参照してください。
保留中	リソースはスキャン待ちです。
スキャン済み	リソースは正常にスキャンされました。

サポートされているリソース

[ネットワーク] タブと [ネットワークスキャンステータス] は、次のリソースで使用できます。

クラウド	リソース
AWS	Application Load Balancer

クラウド	リソース
	Auto Scaling グループ
	Classic Load Balancer
	EC2 インスタンス
	ECS サービス
	Network Load Balancer
	RDS インスタンス
	Redshift クラスタ
Azure	アプリケーションゲート ウェイ
	CosmosDB アカウント
	ロード バランサー
	MySQL データベースフレキシブルサーバー
	MySQL データベース単 一 サーバー
	PostgreSQL データベースフレキシブルサーバー
	PostgreSQL データベース単 一 サーバー
	SQL Server
	仮 想 マシン
	仮 想 マシンスケールセット
GCP	インスタンスグループ

クラウド	リソース
	ロードバランサー
	SQL インスタンス
	VM インスタンス

リソースアクティビティの調査

[イベント] タブをクリックすると、リソースに関連するすべてのアクティビティの完全なリストが表示されます。このリストには、以下のカテゴリのアクティビティが含まれます。

- アイデンティティまたはオリジネータによって、指定されたリソース上で実行するすべてのアクティビティ。
- リソースがアイデンティティまたはオリジネータとして機能して実行されたアクティビティ。

たとえば、アイデンティティとして機能する特定のリソースによって実行されたすべてのアクティビティを表示するには、[Identity] (アイデンティティ) フィルターに移動して、ドロップダウンから当該リソースを選択します。

この情報は、リソースの調査や監査の際に使用します。詳細については、「クラウドイベントを参照してください。

設定スナップショット

IAM リソースの場合、リソースに加えられた設定変更の履歴レコードを表示します。これには、たとえば、複数の日時にリソースにアタッチされたポリシーの完全なリストが含まれます。このデータは、特定の時点の特定の設定データを復元する必要がある場合の参照として使用できます。

スナップショットを表示する方法

1. リソースプロファイルビューで、**[IAM]** をクリックします。
2. **[ポリシースナップショット]** タブをクリックします。

リソースのソースコードの表示

</> IaC

クラウド サイバーエクスポージャー は、あるリポジトリでコードによって管 理されているものとして検 出されたリソースに IaC 組み込みシステムラベル を適 用します。このようなリソースについては、[IaC] タブをクリックして関 連するコード スニペット を表 示し、リソースをそのコード のオリジンまでトレースすることができます。詳 細については、「 コード を参 照してください。

対 応リソース

プロバイダー	カテゴリー	リソースタイプ
Alibaba Cloud	コンピュート	ECS ディスク
Alibaba Cloud	コンピュート	ECS スナップショット ポリシー
Alibaba Cloud	コンピュート	スナップショット
Alibaba Cloud	コンテナ	コンテナイメージ
Alibaba Cloud	コンテナ	コンテナレジストリ
Alibaba Cloud	コンテナ	Container Registry インスタンス
Alibaba Cloud	コンテナ	コンテナレジストリの名 前空 間
Alibaba Cloud	データ	OSS バケット
Alibaba Cloud	ネット ワーク	SSL 証 明 書
Alibaba Cloud	セキュリティ	KMS インスタンス
Alibaba Cloud	セキュリティ	KMS キー
Alibaba Cloud	セキュリティ	KMS シークレット
AWS	AI	Bedrock アクショングループ

プロバイダー	カテゴリー	リソースタイプ
AWS	AI	Bedrock エージェント
AWS	AI	Bedrock AgentCore ゲートウェイ
AWS	AI	Bedrock AgentCore ハーネス
AWS	AI	Bedrock AgentCore メモリ
AWS	AI	Bedrock AgentCore 送信認証 API キー
AWS	AI	Bedrock AgentCore 送信認証 OAuth
AWS	AI	Bedrock AgentCore 送信認証支払い
AWS	AI	Bedrock AgentCore ポリシーエンジン
AWS	AI	Bedrock AgentCore ランタイム
AWS	AI	Bedrock AgentCore ワークロードアイデンティティ
AWS	AI	Bedrock カスタムモデル
AWS	AI	Bedrock データソース
AWS	AI	Bedrock ガードレール
AWS	AI	岩盤知識バスデ
AWS	AI	SageMakerドメイン
AWS	AI	SageMaker ノートブックインスタンス
AWS	コンピューティング	Auto Scaling グループ
AWS	コンピューティング	Batch ジョブ

プロバイダー	カテゴリー	リソースタイプ
AWS	コンピューティング	EBS スナップショット
AWS	コンピューティング	EBS ボリューム
AWS	コンピュート	EC2 インスタンス
AWS	コンピューティング	EC2 マシンイメージ
AWS	コンピューティング	Elastic Beanstalk 環境
AWS	コンピューティング	EMR クラスタ
AWS	コンピューティング	Lambda 関数
AWS	コンピューティング	起動設定
AWS	コンピューティング	起動テンプレート
AWS	コンテナ	コンテナイメージ
AWS	コンテナ	ECR リポジトリ
AWS	コンテナ	ECS サービス
AWS	コンテナ	ECS タスク定義
AWS	データ	アクティビティログアラート
AWS	データ	Amazon MQ Broker
AWS	データ	Athena ワークグループ
AWS	データ	Data Firehose ストリーム
AWS	データ	DAX クラスタ

プロバイダー	カテゴリー	リソースタイプ
AWS	データ	DMS 証明書
AWS	データ	DMS データベースマイグレーションタスク
AWS	データ	DMS エンドポイント
AWS	データ	DMS レプリケーションインスタンス
AWS	データ	DocumentDB クラスタ
AWS	データ	DocumentDB クラスタスナップショット
AWS	データ	DocumentDB グローバルクラスタ
AWS	データ	DocumentDB インスタンス
AWS	データ	DynamoDB テーブル
AWS	データ	EFS アクセスポイント
AWS	データ	EFS ファイルシステム
AWS	データ	EFS マウントターゲット
AWS	データ	ElastiCache Redis OSS キャッシュ
AWS	データ	Elasticsearch ドメイン
AWS	データ	Kinesis データストリーム
AWS	データ	MKS クラスタ
AWS	データ	Neptune クラスタ
AWS	データ	Neptune クラスタスナップショット

プロバイダー	カテゴリー	リソースタイプ
AWS	データ	Neptune グローバルクラスタ
AWS	データ	Neptune インスタンス
AWS	データ	OpenSearch コレクション
AWS	データ	OpenSearch ドメイン
AWS	データ	RDS Aurora グローバルクラスタ
AWS	データ	RDS クラスタ
AWS	データ	RDS インスタンス
AWS	データ	RDS スナップショット
AWS	データ	Redshift クラスタ
AWS	データ	Redshift Serverless 名前空間
AWS	データ	S3 バケット
AWS	データ	SSM マネージドノード
AWS	データ	SNS サブスクリプション
AWS	データ	SNS トピック
AWS	データ	SQS キュー
AWS	データ	Timestream データベース
AWS	データ	Timestream テーブル
AWS	IAM	AWS フェデレーションアクセス許可

プロバイダー	カテゴリー	リソースタイプ
AWS	IAM	IAM グループ
AWS	IAM	IAM ポリシー
AWS	IAM	IAM ロール
AWS	IAM	IAM サーバー証明書
AWS	IAM	IAM ユーザー
AWS	IAM	リソース制御ポリシー (組織のポリシー)
AWS	IAM	ルートユーザー
AWS	IAM	サービス制御ポリシー (組織のポリシー)
AWS	IAM	SSO アプリケーション
AWS	IAM	SSO グループ
AWS	IAM	SSO アクセス許可セット
AWS	IAM	SSO ユーザー
AWS	Kubernetes	EKS クラスタ
AWS	Kubernetes	EKS ノードグループ
AWS	Kubernetes	K8s ユーザー
AWS	Kubernetes	Kubernetes クラスタロール
AWS	Kubernetes	Kubernetes クラスタロールバインディング
AWS	Kubernetes	Kubernetes 設定マップ

プロバイダー	カテゴリー	リソースタイプ
AWS	Kubernetes	Kubernetes グループ
AWS	Kubernetes	Kubernetes イングレス
AWS	Kubernetes	Kubernetes 名前空間
AWS	Kubernetes	Kubernetes ネットワークポリシー
AWS	Kubernetes	Kubernetes ノード
AWS	Kubernetes	Kubernetes 永続ボリューム
AWS	Kubernetes	Kubernetes Pod セキュリティポリシー
AWS	Kubernetes	Kubernetes ロール
AWS	Kubernetes	Kubernetes ロールバインディング
AWS	Kubernetes	Kubernetes サービス
AWS	Kubernetes	Kubernetes サービスアカウント
AWS	Kubernetes	Kubernetes ワークロード
AWS	Kubernetes	セルフマネージド クラスタ
AWS	マネジメント	アカウント
AWS	マネジメント	CloudFormation スタック
AWS	マネジメント	CloudTrail 証跡
AWS	管理	GuardDuty ディテクタ
AWS	ネットワーク	API ゲートウェイ API

プロバイダー	カテゴリー	リソースタイプ
AWS	ネットワーク	API ゲートウェイのカスタムドメイン名
AWS	ネットワーク	CloudFront ディストリビューション
AWS	ネットワーク	カスタマーゲートウェイ
AWS	ネットワーク	Direct Connect ゲートウェイ
AWS	ネットワーク	EC2 Elastic IP
AWS	ネットワーク	Glue の接続
AWS	ネットワーク	インターネットゲートウェイ
AWS	ネットワーク	ロードバランサー
AWS	ネットワーク	NAT ゲートウェイ
AWS	ネットワーク	ネットワーク ACL
AWS	ネットワーク	ネットワークファイヤーウォール
AWS	ネットワーク	ネットワークファイヤーウォールポリシー
AWS	ネットワーク	Network Firewall ルールグループ
AWS	ネットワーク	Route53 ホストゾーン
AWS	ネットワーク	セキュリティグループ
AWS	ネットワーク	Site-to-Site VPN 接続
AWS	ネットワーク	サイト間コンセントレータ
AWS	ネットワーク	サブネット

プロバイダー	カテゴリー	リソースタイプ
AWS	ネットワーク	Tranist ゲートウェイ
AWS	ネットワーク	トランジットゲートウェイの添付ファイル
AWS	ネットワーク	トランジットゲートウェイのルートテーブル
AWS	ネットワーク	VPC
AWS	ネットワーク	仮想プライベートゲートウェイ
AWS	ネットワーク	VPC ブロックパブリックアクセス設定
AWS	ネットワーク	VPC エンドポイント
AWS	ネットワーク	VPC ピアリング接続
AWS	ネットワーク	WAF ウェブ ACL
AWS	セキュリティ	ACM 証明書
AWS	セキュリティ	KMS キー
AWS	セキュリティ	Secrets Manager シークレット
AWS	セキュリティ	Systems Manager パラメーター
AWS	セキュリティ	ユーザーアクセスキー
Azure	AI	AI Search
Azure	AI	ボットサービス
Azure	AI	Machine Learning ワークスペース
Azure	AI	Microsoft Foundry Agent

プロバイダー	カテゴリー	リソースタイプ
Azure	AI	Microsoft Foundry 接続
Azure	AI	Microsoft Foundry データセット
Azure	AI	Microsoft Foundry ガードレール
Azure	AI	Microsoft Foundry ファイル
Azure	AI	Microsoft Foundry インデックス
Azure	AI	Microsoft Foundry ナレッジベース
Azure	AI	Microsoft Foundry ナレッジソース
Azure	AI	Microsoft Foundry メモリ
Azure	AI	Microsoft Foundry モデルのデプロイメント
Azure	AI	Microsoft Foundry プロジェクト
Azure	AI	Microsoft ファウンドリツール
Azure	AI	Microsoft Foundry ベクトルストア
Azure	コンピューティング	アプリサービス
Azure	コンピュート	アプリサービス環境
Azure	コンピューティング	Batch アカウント
Azure	コンピューティング	クラシック仮想マシン
Azure	コンピュート	ハイブリッドコンピューティングマシン
Azure	コンピューティング	ロジックアプリ

プロバイダー	カテゴリー	リソースタイプ
Azure	コンピューティング	Machine Learning ワークスペース
Azure	コンピューティング	マネージドディスク
Azure	コンピューティング	Quantum ワークスペース
Azure	コンピューティング	復元ポイントコレクション
Azure	コンピューティング	スナップショット
Azure	コンピュート	SQL 仮想マシン
Azure	コンピュート	Static Web Apps
Azure	コンピュート	Step Functions ステートマシン
Azure	コンピューティング	Virtual Desktop アプリケーショングループ
Azure	コンピューティング	Virtual Desktop ホストプール
Azure	コンピューティング	Virtual Desktop スケーリングプラン
Azure	コンピューティング	Virtual Desktop ワークスペース
Azure	コンピューティング	仮想マシン
Azure	コンピューティング	仮想マシンスケールセット
Azure	コンピューティング	仮想マシンスケールセットインスタンス
Azure	コンピューティング	VMware 仮想マシン
Azure	コンテナ	コンテナアプリ
Azure	コンテナ	コンテナイメージ

プロバイダー	カテゴリー	リソースタイプ
Azure	コンテナ	コンテナインスタンス
Azure	コンテナ	コンテナレジストリ
Azure	コンテナ	コンテナリポジトリ
Azure	データ	アクティビティログアラート
Azure	データ	AppSync GraphQL API
Azure	データ	Backup Vault
Azure	データ	Cassandra クラスタ
Azure	データ	クラシックストレージアカウント
Azure	データ	CosmosDB アカウント
Azure	データ	Data Explorer クラスタ
Azure	データ	Data Factory
Azure	データ	Data Factory V2
Azure	データ	データレイクストレージ
Azure	データ	データ共有
Azure	データ	データベースマイグレーションプロジェクト
Azure	データ	データベースマイグレーションサービス
Azure	データ	Databricks ワークスペース
Azure	データ	Event Hubs 名前空間

プロバイダー	カテゴリー	リソースタイプ
Azure	データ	MariaDB データベースサーバー
Azure	データ	メディアサービス
Azure	データ	MySQL データベースサーバー
Azure	データ	Notification Hub
Azure	データ	PostgreSQL データベースサーバー
Azure	データ	レコメンデーションサービス
Azure	データ	Red Hat OpenShift クラスタ
Azure	データ	Redis キャッシュ
Azure	データ	Service Bus
Azure	データ	Service Hub コネクタ
Azure	データ	SignalR サービス
Azure	データ	SQL データベース
Azure	データ	SQL Managed Instance
Azure	データ	SQL サーバー
Azure	データ	ストレージアカウント
Azure	データ	ストレージアカウント Blob コンテナ
Azure	データ	Synapse ワークスペース
Azure	IAM	Azure Automation アカウント

プロバイダー	カテゴリー	リソースタイプ
Azure	IAM	Azure マネージド ID
Azure	IAM	Azure PIM Role Settings
Azure	IAM	Azure ロール
Azure	IAM	Azure ロールの割り当て
Azure	IAM	Azure サービスプロバイダーの委任
Azure	IAM	Azure サービスプロバイダーのオファー
Azure	IoT	IoT Hub
Azure	IoT	IoT Hub デバイスプロビジョニングサービス
Azure	IoT	IoT Hub デバイス更新アカウント
Azure	IoT	IoT Hub デバイス更新インスタンス
Azure	Kubernetes	AKS クラスタ
Azure	Kubernetes	AKS クラスタノードプール
Azure	Kubernetes	K8s クラスタロール
Azure	Kubernetes	K8s クラスタロールバインディング
Azure	Kubernetes	K8s 設定マップ
Azure	Kubernetes	K8s グループ
Azure	Kubernetes	K8s イングレス
Azure	Kubernetes	K8s 名前空間

プロバイダー	カテゴリー	リソースタイプ
Azure	Kubernetes	K8s ネットワークポリシー
Azure	Kubernetes	K8s ノード
Azure	Kubernetes	K8s 永続ボリューム
Azure	Kubernetes	K8s Pod セキュリティポリシー
Azure	Kubernetes	K8s サービス
Azure	Kubernetes	K8s サービスアカウント
Azure	Kubernetes	K8s ユーザー
Azure	Kubernetes	セルフマネージドクラスタ
Azure	マネジメント	API Management サービス
Azure	マネジメント	アプリ設定
Azure	マネジメント	アプリケーションインサイトワークブック
Azure	管理	管理グループ
Azure	マネジメント	リソースグループ
Azure	管理	ルート
Azure	マネジメント	サブスクリプション
Azure	管理	サブスクリプション
Azure	ネットワーク	アプリケーションゲートウェイ
Azure	ネットワーク	アプリケーションセキュリティグループ

プロバイダー	カテゴリー	リソースタイプ
Azure	ネットワーク	Bastion ホスト
Azure	ネットワーク	CDN Front Door プロファイル
Azure	ネットワーク	CDN Front Door プロファイルのカスタムドメイン
Azure	ネットワーク	CDN Front Door プロファイルエンドポイント
Azure	ネットワーク	CDN プロファイル
Azure	ネットワーク	CDN プロファイルエンドポイント
Azure	ネットワーク	クラシックネットワークセキュリティグループ
Azure	ネットワーク	クラシック予約済み IP アドレス
Azure	ネットワーク	クラシック仮想ネットワーク
Azure	ネットワーク	DNS ゾーン
Azure	ネットワーク	ファイヤーウォール
Azure	ネットワーク	ファイヤーウォールポリシー
Azure	ネットワーク	Front Door
Azure	ネットワーク	フロントドア WAF ポリシー
Azure	ネットワーク	IP グループ
Azure	ネットワーク	ロードバランサー
Azure	ネットワーク	ローカルネットワークゲートウェイ
Azure	ネットワーク	NAT ゲートウェイ

プロバイダー	カテゴリー	リソースタイプ
Azure	ネットワーク	ネットワークインターフェース
Azure	ネットワーク	ネットワークマネージャー
Azure	ネットワーク	ネットワークセキュリティグループ
Azure	ネットワーク	ピアリング
Azure	ネットワーク	プライベート DNS ゾーン
Azure	ネットワーク	プライベートエンドポイント
Azure	ネットワーク	プライベートリンクサービス
Azure	ネットワーク	ルートテーブル
Azure	ネットワーク	サブネット
Azure	ネットワーク	Traffic Manager プロファイル
Azure	ネットワーク	仮想ネットワーク
Azure	ネットワーク	仮想ネットワークゲートウェイ
Azure	ネットワーク	仮想 WAN
Azure	ネットワーク	VMware 仮想ネットワーク
Azure	ネットワーク	VPN ゲートウェイ
Azure	ネットワーク	WAF ポリシー
Azure	セキュリティ	ハードウェアセキュリティモジュール
Azure	セキュリティ	Key Vault

プロバイダー	カテゴリー	リソースタイプ
Azure	セキュリティ	Key Vault 証明書
Azure	セキュリティ	Key Vault キー
Azure	セキュリティ	Key Vault シークレット
Azure	セキュリティ	リカバリサービス Vault
Azure	セキュリティ	SSH 公開鍵
コンテナイメージレジストリ	コンテナ	コンテナイメージ
コンテナイメージレジストリ	コンテナ	コンテナリポジトリ
GCP	AI と機械学習	Vertex AI Workbench インスタンス
GCP	コンピューティング	App Engine アプリケーション
GCP	コンピューティング	App Engine サービス
GCP	コンピューティング	Cloud Build トリガー
GCP	コンピューティング	Cloud Functions
GCP	コンピューティング	コンピューティングディスク
GCP	コンピューティング	コンピューティングイメージ
GCP	コンピューティング	コンピューティングノードグループ
GCP	コンピューティング	コンピューティングノードテンプレート
GCP	コンピューティング	コンピューティングスナップショット
GCP	コンピューティング	Dataflow ジョブ

プロバイダー	カテゴリー	リソースタイプ
GCP	コンピュート	Dataproc クラスタ
GCP	コンピューティング	インスタンスグループ
GCP	コンピューティング	インスタンステンプレート
GCP	コンピューティング	VM インスタンス
GCP	コンテナ	アーティファクト コンテナイメージリポジトリ
GCP	コンテナ	アーティファクト パッケージリポジトリ
GCP	コンテナ	アーティファクト レジストリ
GCP	コンテナ	Cloud Run サービス
GCP	コンテナ	Kubernetes ノードプール
GCP	データ	BigQuery データセット
GCP	データ	BigQuery データセット テーブル
GCP	データ	BigQuery モデル
GCP	データ	Bigtable クラスタ
GCP	データ	Bigtable インスタンス
GCP	データ	Bigtable テーブル
GCP	データ	Filestore インスタンス
GCP	データ	ログバケット
GCP	データ	Memcache インスタンス

プロバイダー	カテゴリー	リソースタイプ
GCP	データ	Metastore サービス
GCP	データ	Pub/Sub スナップショット
GCP	データ	Pub/Sub サブスクリプション
GCP	データ	Pub/Sub トピック
GCP	データ	Redis インスタンス
GCP	データ	Spanner データベース
GCP	データ	Spanner インスタンス
GCP	データ	SQL インスタンス
GCP	データ	ストレージバケット
GCP	データ	ストレージ HMAC キー
GCP	IAM	GCP ロール
GCP	IAM	サービスアカウント
GCP	IAM	サービスアカウント (外部)
GCP	IAM	Workforce Identity プール
GCP	IAM	Workload Identity プール
GCP	Kubernetes	GKE クラスタ
GCP	Kubernetes	GKE ノードプール
GCP	Kubernetes	K8s クラスタロール

プロバイダー	カテゴリー	リソースタイプ
GCP	Kubernetes	K8s クラスタロールバインディング
GCP	Kubernetes	K8s 設定マップ
GCP	Kubernetes	K8s グループ
GCP	Kubernetes	K8s イングレス
GCP	Kubernetes	K8s 名前空間
GCP	Kubernetes	K8s ネットワークポリシー
GCP	Kubernetes	K8s ノード
GCP	Kubernetes	K8s 永続ボリューム
GCP	Kubernetes	K8s Pod セキュリティポリシー
GCP	Kubernetes	K8s ロール
GCP	Kubernetes	K8s ロールバインディング
GCP	Kubernetes	K8s サービス
GCP	Kubernetes	K8s サービスアカウント
GCP	Kubernetes	K8s ユーザー
GCP	Kubernetes	K8s ワークロード
GCP	Kubernetes	セルフマネージドクラスタ
GCP	管理	フォルダー
GCP	マネジメント	ログシンク

プロバイダー	カテゴリー	リソースタイプ
GCP	管理	組織
GCP	マネジメント	プロジェクト
GCP	ネットワーク	API ゲートウェイ
GCP	ネットワーク	クラシック VPN ゲートウェイ
GCP	ネットワーク	DNS マネージドゾーン
GCP	ネットワーク	外部 VPN ゲートウェイ
GCP	ネットワーク	ファイヤーウォールポリシー
GCP	ネットワーク	ファイヤーウォールポリシー
GCP	ネットワーク	ロードバランサー
GCP	ネットワーク	ロードバランサーのバックエンドバケット
GCP	ネットワーク	ロードバランサーのバックエンドサービス
GCP	ネットワーク	ロードバランサー転送ルール
GCP	ネットワーク	ロードバランサーターゲットプール
GCP	ネットワーク	ロードバランサーターゲットプロキシ
GCP	ネットワーク	ロードバランサー URL マップ
GCP	ネットワーク	ネットワークエンドポイントグループ
GCP	ネットワーク	サブネット
GCP	ネットワーク	VPC ネットワーク

プロバイダー	カテゴリー	リソースタイプ
GCP	ネットワーク	VPC ピアリング接続
GCP	ネットワーク	VPN ゲートウェイ
GCP	セキュリティ	API キー
GCP	セキュリティ	Cloud KMS キー
GCP	セキュリティ	Cloud KMS キーリング
GCP	セキュリティ	Secrets Manager シークレット
GCP	セキュリティ	サービスアカウントのユーザー管理キー
GCP	セキュリティ	SSL 証明書
GCP	セキュリティ	SSL ポリシー
Google Workspace	IAM	Google Workspace 管理者ロール
Google Workspace	IAM	Google Workspace グループ
Google Workspace	IAM	Google Workspace グループ (外部)
Google Workspace	IAM	Google Workspace ユーザー
Google Workspace	IAM	Google Workspace ユーザー (外部)
Google Workspace	マネジメント	アカウント
Microsoft Entra ID	IAM	管理者ロール
Microsoft Entra ID	IAM	アプリ登録
Microsoft Entra ID	IAM	アプリ登録証明書

プロバイダー	カテゴリー	リソースタイプ
Microsoft Entra ID	IAM	アプリ登録シークレット
Microsoft Entra ID	IAM	条件付きアクセスポリシー
Microsoft Entra ID	IAM	認証コンテキスト
Microsoft Entra ID	IAM	アプリケーション
Microsoft Entra ID	IAM	グループ
Microsoft Entra ID	IAM	PIM 使用資格のある割り当て
Microsoft Entra ID	IAM	PIM グループの設定
Microsoft Entra ID	IAM	ユーザー
Microsoft Entra ID	マネジメント	Tenant (テナント)
OCI	コンピューティング	自動スケーリング設定
OCI	コンピューティング	ブロックボリューム
OCI	コンピューティング	ブートボリューム
OCI	コンピューティング	コンピューティングイメージ
OCI	コンピューティング	コンピューティングインスタンス
OCI	コンピューティング	Functions
OCI	コンピューティング	インスタンス設定
OCI	コンピューティング	インスタンスプール
OCI	データ	自律型データベース

プロバイダー	カテゴリー	リソースタイプ
OCI	データ	Exadata インフラストラクチャ
OCI	データ	ファイルシステム
OCI	データ	マウントターゲット
OCI	データ	マウントターゲットエクスポート
OCI	データ	NoSQL データベーステーブル
OCI	データ	オブジェクトストレージバケット
OCI	データ	Oracle データベース DB システム
OCI	データ	PostgreSQL データベース
OCI	IAM	動的グループ
OCI	IAM	グループ
OCI	IAM	アイデンティティドメイン
OCI	IAM	ポリシー
OCI	IAM	ユーザー
OCI	Kubernetes	クラスタノードプール
OCI	Kubernetes	K8s クラスタロールバインディング
OCI	Kubernetes	K8s クラスタロール
OCI	Kubernetes	K8s 設定マップ
OCI	Kubernetes	K8s グループ

プロバイダー	カテゴリー	リソースタイプ
OCI	Kubernetes	K8s グループ
OCI	Kubernetes	K8s イングレス
OCI	Kubernetes	K8s 名前空間
OCI	Kubernetes	K8s 名前空間
OCI	Kubernetes	K8s ネットワークポリシー
OCI	Kubernetes	K8s ノード
OCI	Kubernetes	K8s ノード
OCI	Kubernetes	K8s 永続ボリューム
OCI	Kubernetes	K8s Pod セキュリティポリシー
OCI	Kubernetes	K8s ロール
OCI	Kubernetes	K8s ロールバインディング
OCI	Kubernetes	K8s ロールバインディング
OCI	Kubernetes	K8s ロール
OCI	Kubernetes	K8s サービス
OCI	Kubernetes	K8s サービスアカウント
OCI	Kubernetes	K8s サービスアカウント
OCI	Kubernetes	K8s サービス
OCI	Kubernetes	K8s ユーザー

プロバイダー	カテゴリー	リソースタイプ
OCI	Kubernetes	K8s ユーザー
OCI	Kubernetes	K8s ワークロード
OCI	Kubernetes	K8s ワークロード
OCI	Kubernetes	OKE クラスタ
OCI	マネジメント	コンパート メント
OCI	マネジメント	ロググループ
OCI	ネット ワーク	インターネット ゲート ウェイ
OCI	ネット ワーク	ロード バランサー
OCI	ネット ワーク	ローカルピアリングゲート ウェイ
OCI	ネット ワーク	NAT ゲート ウェイ
OCI	ネット ワーク	Network Load Balancer
OCI	ネット ワーク	ネット ワークセキュリティグループ
OCI	ネット ワーク	ルート テーブル
OCI	ネット ワーク	セキュリティリスト
OCI	ネット ワーク	サービスゲート ウェイ
OCI	ネット ワーク	サブネット
OCI	ネット ワーク	仮 想 クラウド ネット ワーク
OCI	ネット ワーク	仮 想 ネット ワークインターフェースカード

プロバイダー	カテゴリー	リソースタイプ
OCI	シークレット	API キー
OCI	シークレット	認証トークン
OCI	シークレット	顧客秘密キー
OCI	シークレット	Vault
OCI	シークレット	Vault マスター暗号化キー
OCI	シークレット	Vault シークレット
OCI	セキュリティ	データベースパスワード
Okta	IAM	Okta グループ
Okta	IAM	Okta ユーザー
OneLogin	IAM	OneLogin グループ
OneLogin	IAM	OneLogin ロール
OneLogin	IAM	OneLogin ユーザー
オンプレミス	Kubernetes	K8s クラスタロール
オンプレミス	Kubernetes	K8s クラスタロールバインディング
オンプレミス	Kubernetes	K8s 設定マップ
オンプレミス	Kubernetes	K8s グループ
オンプレミス	Kubernetes	K8s イングレス
オンプレミス	Kubernetes	K8s 名前空間

プロバイダー	カテゴリー	リソースタイプ
オンプレミス	Kubernetes	K8s ネットワークポリシー
オンプレミス	Kubernetes	K8s ノード
オンプレミス	Kubernetes	K8s 永続ボリューム
オンプレミス	Kubernetes	K8s Pod セキュリティポリシー
オンプレミス	Kubernetes	K8s ロール
オンプレミス	Kubernetes	K8s ロールバインディング
オンプレミス	Kubernetes	K8s サービス
オンプレミス	Kubernetes	K8s サービスアカウント
オンプレミス	Kubernetes	K8s ユーザー
オンプレミス	Kubernetes	K8s ワークロード
オンプレミス	Kubernetes	オンプレミスクラスタ
オンプレミス	Kubernetes	OpenShift ビルド設定
オンプレミス	Kubernetes	OpenShift カタログソース
オンプレミス	Kubernetes	OpenShift イメージストリーム
オンプレミス	Kubernetes	OpenShift プロジェクト
オンプレミス	Kubernetes	OpenShift ルート
オンプレミス	Kubernetes	OpenShift セキュリティコンテキスト制約
オンプレミス	Kubernetes	OpenShift テンプレート

プロバイダー	カテゴリー	リソースタイプ
Ping Identity	IAM	Ping Identity グループ
Ping Identity	IAM	Ping Identity ユーザー
Snowflake	データ	ローカルデータベース
Snowflake	データ	Marketplace データベース
Snowflake	データ	共有データベース
Snowflake	管理	アカウント

コンピュート

仮想マシン

> **注意:** 一部の機能は、Cloud Vulnerability Management ライセンスでは使用できません。

環境内の仮想マシンを表示および管理します。

- 各仮想マシンについて、ネットワークエクスポージャーの明確な全体像を確認し、インストールされているソフトウェアパッケージを特定し、関連する脆弱性を分析します。
- どの仮想マシンに深刻な脆弱性があるかを把握し、これらのリスクを修正できるようにします。
- 仮想マシンのオンデマンドスキャンを実行します。
- 環境内の仮想マシンにインストールされているすべてのソフトウェアパッケージ、または特定のワークロードにインストールされているパッケージを表示します。

これは、仮想マシンの表示と管理に関するハウツーガイドです。

- ワークロード保護機能の概念概要については、「ワークロード保護を参照してください。
- VM 設定を構成するには、「Virtual Machine Settings」を参照してください。
- よくある質問については、「FAQ: ワークロード保護」を参照してください。

すべての仮想マシンを表示する

仮想マシンを表示する方法

1. Tenable One Cloud Exposure コンソールで、**[Explore > Compute > Virtual Machines]** に移動します。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、「仮想マシンの列データ」を参照してください。
3. 仮想マシンの名前をクリックしてリソースの詳細の表示。
4. リソースページで、**[ワークロード]** をクリックします。
5. 次のいずれかのタブをクリックします。
    - **ソフトウェア**。マシンにインストールされているソフトウェアパッケージを表示します。
    - **脆弱性**。マシンにインストールされているパッケージに関連する脆弱性を表示します。
    - **悪意のあるファイル**。マシンで検出された悪悪意のあるファイルを表示します。

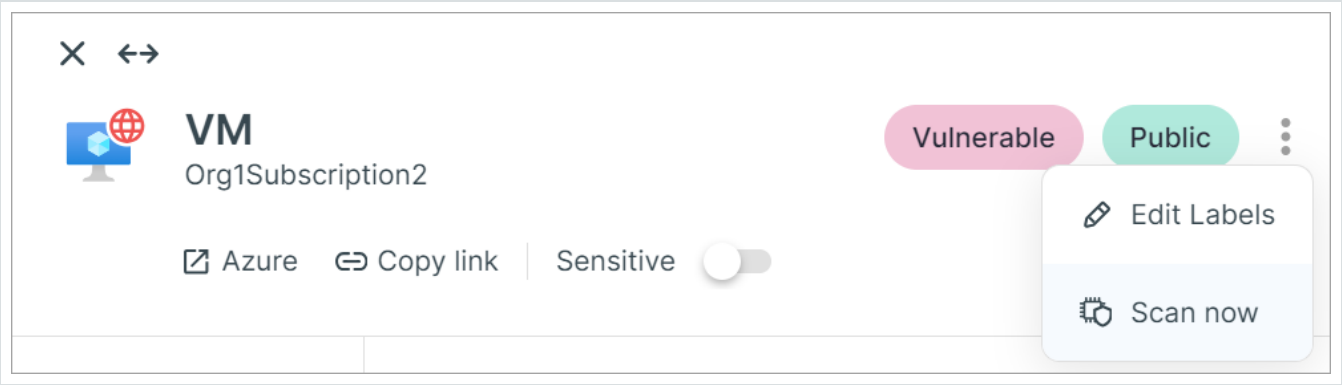
オンデマンドスキャンの実行

Tenable は、すべての仮想マシンを少なくとも 24 時間に 1 回、自動的にスキャンします。特定のワークロードをそれよりも早くスキャンしたい場合は、オンデマンドスキャンをリクエストできます。スキャンを開始すると、そのスキャンはキューの先頭にプッシュされます。スキャン結果は、Tenable によって次回定期的にデータの同期と更新の頻度が実行された後にクラウドサイバーエクスポージャーコンソールに表示されます。

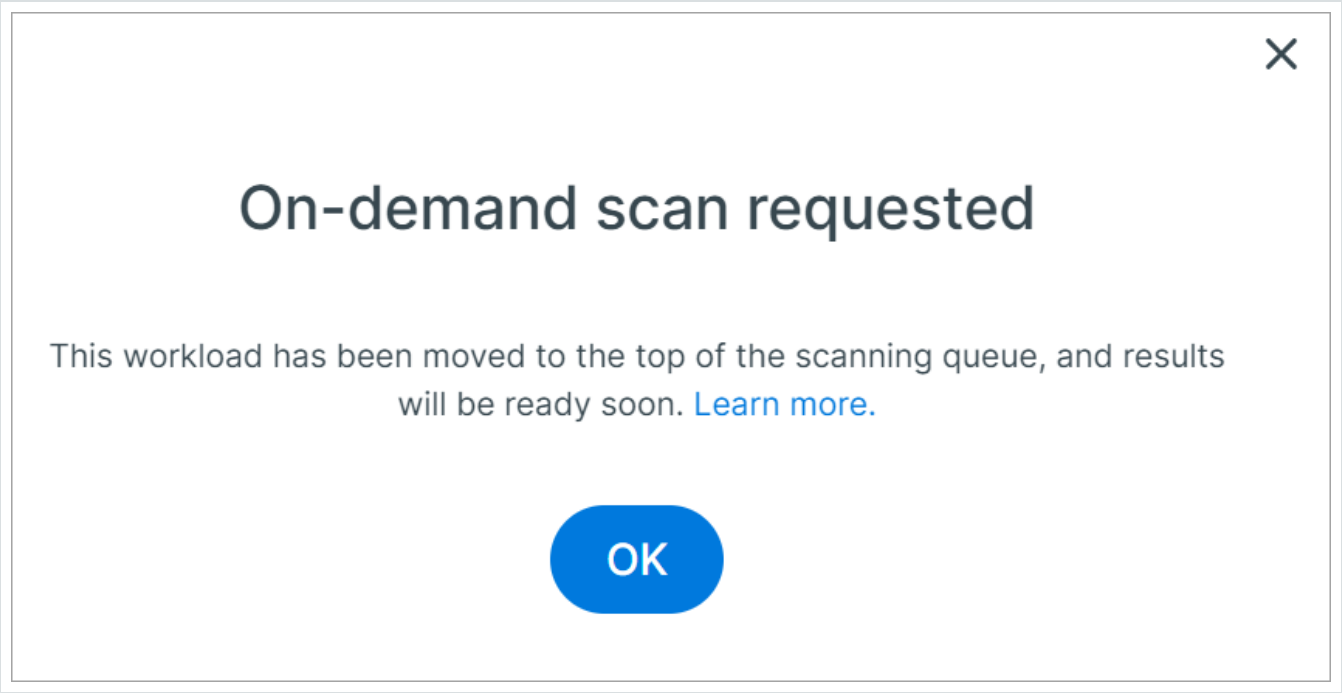
関連する仮想マシンのデータディスクスキャンを有効にするまたはワークロードの接続をスキャンから除外した場合、オンデマンドスキャンは利用できません。

オンデマンドスキャンを実行する方法

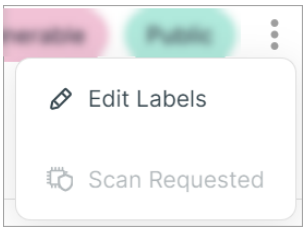
1. 関連する仮想マシンに移動し、クリックします。仮想マシンは、**[Explore > Compute]** > **[Virtual Machines]**、または関連するクラウドプロバイダーのインベントリビューにあります (例: **[Explore > Inventory]** > **[Compute > Azure Virtual Machines]**)。
2. 三点リーダーアイコンをクリックし、**[今すぐスキャン]** をクリックします。



スキャンが正常にリクエストされたことを示すダイアログが表示されます。



3. [OK] をクリックします。
   スキャンがすでにリクエストされている場合、ボタンは無効になり、**[スキャンをリクエスト済み]** と表示されます。



仮想マシンの列データ

次の列は [Virtual Machines] (仮想マシン) ページのテーブルに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

縦棒	説明
名前	仮想マシンの名前。
アカウント	仮想マシンが存在するクラウドアカウント。
オペレーティングシステム	仮想マシンで実行されているオペレーティングシステムとバージョン。
ソフトウェア	ワークロードにインストールされているすべてのソフトウェアパッケージのリスト。必要に応じて、パッケージのファイルパスも表示されます。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
脆弱性	ワークロードで見つかった脆弱性の内訳 (リスク深刻度の色分け)。数字をクリックすると、特定の深刻度レベルの脆弱性リストが表示されます。
プラグイン	仮想マシンで検出された脆弱性に関連するプラグイン。**プラグインのリンク**をクリックして、プラグインの詳細を表示します。
ネットワークのエクスポージャー	ワークロードがインターネットに公開されている仕組み • **インターネット (直接接続)**: インターネットに直接公開されているワークロード。 • **インターネット (間接)**: ロードバランサーなどを介して、間接的にインターネットに公開されているワークロード。
ネットワークのエクスポー	ワークロードがインターネットに公開されている範囲 • **すべてのIP**: すべてのIPv4またはIPv6アドレス [0.0.0.0/0, :/0]

縦棒	説明
ジャー範囲	• **幅広いIPアドレス範囲**：65,536個以上のアドレス • **特定のIPアドレス**：65,535件以下
アイデンティティリスク	すべてのアイデンティティには、アイデンティティが環境にもたらすリスクに対応する総合的なリスクレベルが割り当てられます。リスクは複数の重み付けされた要因に基づいて計算され、アイデンティティ固有のアクセス許可のリスクレベルと、環境におけるアイデンティティの全体的な文脈 (多くの場合、ラベルに反映されます) の両方が考慮されます。詳細については、「アイデンティティインテリジェンス」を参照してください。
状態	仮想マシンの現在の状態。可能な値：Running、Stopped
脆弱性のスキャンステータス	ワークロードが正常にスキャンされたかどうかを示します。また、ワークロードがスキャンされなかった理由を示します。詳細については、「脆弱性のスキャンステータス」を参照してください。
脆弱性のスキャン時間	クラウドサイバーエクスポージャーが前回マシンをスキャンした時刻を示すタイムスタンプ。マシンがまだスキャンされていない場合、値はダッシュ (-) になります。
スキャンソース	仮想マシンがエージェントベースの方法とエージェントレスの方法のどちらを使用してスキャンされたかを示します。このフィールドはデフォルトでは非表示になっていますが、列セレクタを使用して追加できます。このフィールドは、エージェントベースのスキャンが有効になっている場合にのみ表示されます。
検出結果	マシンに関連する検出結果数の深刻度別内訳。数字をクリックすると、検出結果について検索可能なリストが表示されます。
データタイプ	リソースで検出された機密性の高いデータタイプ。完全なリストについては スキャン対象データタイプ 。
データカ	リソースで検出された機密性の高いデータタイプにマッピングされるデータカテゴリ。

縦棒	説明
テゴリ	
データの機密性	すべてのスキャン対象データから検出された最も高い機密レベル。詳細については、「感度レベル」を参照してください。
データスキャンステータス	リソースが正常にスキャンされたかどうかを示します。リソースがスキャンされなかった理由を示します。詳細については、「データスキャンステータス」を参照してください。
データスキャン時間	前回 クラウドサイバーエクスポージャー がリソースをスキャンした時刻を示すタイムスタンプ。リソースがまだスキャンされていない場合、値はダッシュ (-) になります。
ラベル	手動による適用、タグに基づく自動適用、システムによる適用のいずれかにかかわらず、ワークロードに適用されたラベルのリソースへの適用 が表示されます。ラベルのタグにカーソルを合わせると、詳細を確認できます。ワークロードに複数のラベルがある場合、アイコンをクリックするとその他のラベルが表示されます。以下のラベルはワークロード保護に固有のものであり、以下の状況で表示されます。 • **OSにパッチが適用されていない**: このワークロードでは、多数の既知の脆弱性が存在するバージョンのオペレーティングシステムが実行されています。 • **脆弱性あり**: このワークロードには、少なくとも1つの重大な脆弱性が存在します。 • **OSのサポート終了**: このワークロードで使用されているオペレーティングシステムのサポートが終了しているか、または終了まで30日以内となっています。 • **脆弱性(エクスプロイト)**: このワークロードには、既知のエクスプロイトに関連する重大な脆弱性が少なくとも1つ存在します。

脆弱性のスキャンステータス

[脆弱性スキャンのステータス] 列には、マシンに関する現在のスキャンのステータスが示されます。以下の表は、ステータスの種類と、そのステータスが表示される理由を示しています。理由は通常、ツールチップとしてステータスの横に表示されます。

スキャンステータス	理由
保留中	仮想マシンはキューに入っています。
	オンオンデマンドスキャンの実行がリクエストされました。
	このスキャンは、必要な Marketplace イメージをサブスクライブするために Tenable による手動ステップを保留しています。数時間後にもう一度ご確認ください。
無効	この仮想マシンは ワークロードの接続。
	ワークロード保護スキャン 仮想マシンのデータディスクスキャンを有効にする。
	この仮想マシンは、関連する vault に対する `Azure Key Vault` 権限がないため、スキャンされていません。これは、**BitLocker** を備えた Windows 仮想マシンまたは **DM-Crypt** (Ubuntu でのみサポートされている) ディスク暗号化を備えた Linux 仮想マシンで発生する可能性があります。必要なアクセス許可を付与するには、「 仮想マシンスキャンのアクセス許可を付与する」を参照してください。
	この仮想マシンは、関連する vault に対する `Key Vault Crypto User` 権限がないため、スキャンされていません。これは、**BitLocker** キー暗号化キーを使用する Windows 仮想マシンで発生する可能性があります。必要なアクセス許可を付与するには、「 仮想マシンスキャンのアクセス許可を付与する」を参照してください。
	この仮想マシンは、`Key Vault` のアクセス許可がないため、スキャンされていません。これは、仮想マシンディスクが CMK (カスタマーマネージドキー) で暗号化されている場合に発生する可能性があります。詳細については、サポートへの問い合わせ。を参照してください。

スキャンステータス	理由
	この仮想マシンは、スナップショットでデータアクセス認証を無効にできないようにするAzureポリシーにより、スキャンされていません。必要なアクセス許可を付与するには、専用のスナップショットリソースグループを設定し、それをポリシーから除外します。
	この仮想マシンは、ワークロード保護のアクセス許可がないため、スキャンされていません。必要なアクセス許可を付与するには、「ワークロードの接続を参照してください。
	(アカウント内スキャン)このイメージをスキャンするには、AWS Marketplaceのサブスクリプションが必要です。アカウント内スキャンに使用する専用のAWSアカウントにログインしてAWS Marketplaceに移動し、関連するAMIを見つけて[Continue to Subscribe] (サブスクリプションを続行する)をクリックします。詳細についてはアカウント内スキャンを参照してください。
	この仮想マシンは、設定されたスナップショットリソースグループが削除されたため、スキャンされていません。
	この仮想マシンは、ワークロード保護のアクセス許可をブロックするSCPが存在するため、スキャンされていません。
	この仮想マシンは、ドメイン制限共有ポリシーのためスキャンされていません。
	この仮想マシンは、クラウドアカウントにディスクスナップショットを作成するために必要なアクセス許可がないため、スキャンされていません。
サポート対象外	オペレーティングシステムディスクが管理されていないため、この仮想マシンに対するスキャンはサポート対象外です。
	ディスクにサポートされているパーティションがないため、この仮想マシンに対するスキャンはサポート対象外です。

スキャンステータス	理由
	この仮想マシンは、AWS Marketplace の AMI から起動されましたが、製品 ID が見つからなかったため、スキャンされていません。
	この仮想マシンは、この仮想マシンに関連するスナップショットについてアウトバウンドネットワークアクセスがブロックされているため、スキャンされていません。
	このインスタンスは、サポートされていないインスタンス仕様で AWS Marketplace の AMI から起動されたため、スキャンされていません。
	ディスクはインスタンスストアであり、EBS ボリュームではないので、このワークロードに対するスキャンはサポート対象外です。
	オペレーティングシステムの暗号化が有効になっているため、この仮想マシンに対するスキャンはサポート対象外です。
	スナップショットが削除されないようにロックするリソースグループにリソースが属しているため、この仮想マシンはスキャンされません。
	この仮想マシンは、ディスクの最大サイズを超過しているため、スキャンされていません。
	オペレーティングシステムディスクが管理されていないため、この仮想マシンに対するスキャンはサポート対象外です。
	Marketplace から削除された AWS イメージに基づいているため、この仮想マシンに対するスキャンはサポート対象外です。最新イメージにアップグレードすることをお勧めします。 **注意**: この制限は、AWS Marketplace から直接取得されたスナップショットやイメージ (AMI) には、スキャン操作でコピーしたり共有したりできない、特定のライセンスと所有権の制限があるために発生します。
	この仮想マシンは Amazon DevPay のイメージに基づいているため、スキャンはサポート対象外です。これは販売者や商品の新規受け入れを停止したレガシーサービスです。

スキャンステータス	理由
	オペレーティングシステムディスクが一時的なものであるため、この仮想マシンに対するスキャンはサポート対象外です。
	クラウドプロバイダーの制限により、このリージョンのこの仮想マシンに対するスキャンはサポート対象外です。
	この仮想マシンは、ディスクアクセスを制限するプロバイダー管理アプリケーションの一部であるため、スキャンはサポート対象外です。
スキャン済み	マシンは正常にスキャンされました。

AWS Marketplace AMI から起動された EC2 インスタンス

クラウドサイバーエクスポージャー は、AWS Marketplace AMI から起動された EC2 インスタンスのスキャンをサポートしています。スキャンは、標準のワークロードスキャンと ワークロード保護 (アカウント内スキャン)。このような EC2 インスタンスで発生する可能性がある問題のトラブルシューティングの詳細については、「 スキャンステータス 」を参照してください。

アカウント内スキャン

Marketplace イメージ (AMI) を使用している場合 、Tenable では、`license-manager:ListReceivedLicenses` アクセス許可を追加することを強く推奨します。これにより、Tenable は、ライセンスされたイメージをスキャンするために、専用スキャンアカウントに関連付けられているライセンスを確認できます。詳細については アカウント内スキャンの設定 を参照してください。

イメージをスキャンするには、スキャンに使用される専用アカウントに AWS Marketplace サブスクリプションが必要です。サブスクリプションがなく、イメージの スキャンステータス が [無効] になっている場合は、ツールチップの指示に従ってサブスクリプション登録してください。登録後 、サブスクリプションが クラウドサイバーエクスポージャー で更新されるまでに約 15 分かかります。マシンが過去 24 時間以内にスキャンされてい

る場合、次のスキャンサイクルまで再スキャンされません。そのため、オンデマンドスキャンの実行 て、イメージをより早くスキャンしたい場合があります。

仮想マシンイメージ

環境内の仮想マシンイメージを表示および管理します。

- 仮想マシンイメージごとに、ネットワークエクスポージャーの明確な全体像を確認し、インストールされているソフトウェアパッケージを特定し、関連する脆弱性を分析します。
- どの仮想マシンイメージに深刻な脆弱性があるかを把握し、これらのリスクを修正できるようにします。
- 環境内の仮想マシンイメージにインストールされているすべてのソフトウェアパッケージ、または特定の仮想マシンイメージにインストールされているパッケージを表示します。

仮想マシンイメージの表示と管理に関するハウツーガイドです。

- ワークロード保護機能の概念概要については、「ワークロード保護を参照してください。
- VM イメージの設定を構成するには、「仮想マシンイメージ Settings」を参照してください。
- よくある質問については、「FAQ: ワークロード保護」を参照してください。

すべての仮想マシンイメージを表示する

> **注意:** Tenable One Cloud Exposure は現在、AWS 仮想マシンイメージ (AMI) のみのスキャンをサポートしています。

仮想マシンイメージを表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Explore > Compute > Virtual Machine Images]** に移動します。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、「仮想マシンイメージの列データ」を参照してください。
3. 仮想マシンイメージの名前をクリックして、リソースの詳細の表示。
4. リソースページで、**[ワークロード]** をクリックします。

5. 次のいずれかのタブをクリックします。
    - **ソフトウェア**。マシンにインストールされているソフトウェアパッケージを表示します。
    - **脆弱性**。マシンにインストールされているパッケージに関連する脆弱性を表示します。
    - **悪意のあるファイル**。マシンで検出された悪意のあるファイルを表示します。

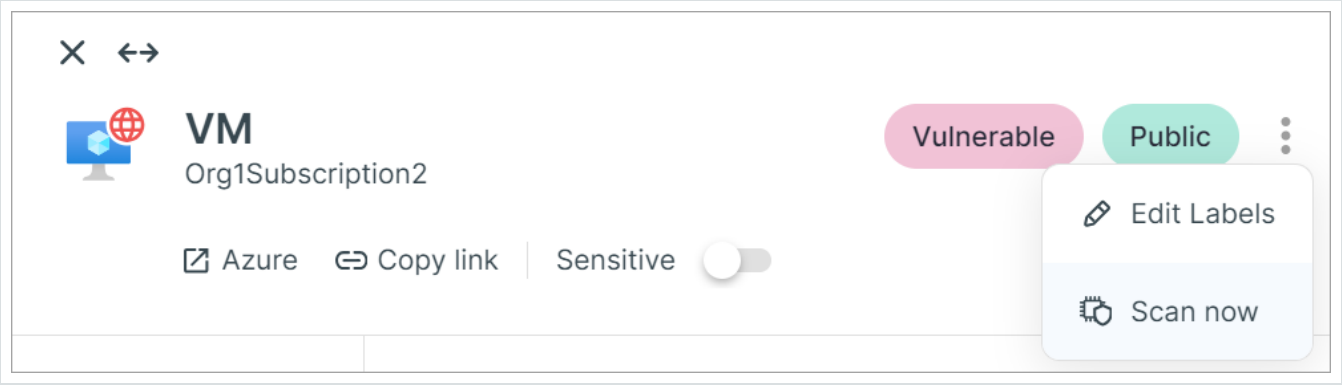
オンデマンドスキャンの実行

Tenable は、すべての仮想マシンを少なくとも 24 時間に 1 回、自動的にスキャンします。特定のワークロードをそれよりも早くスキャンしたい場合は、オンデマンドスキャンをリクエストできます。スキャンを開始すると、そのスキャンはキューの先頭にプッシュされます。スキャン結果は、Tenable によって次回定期的にデータの同期と更新の頻度が実行された後にクラウドサイバーエクスポージャーコンソールに表示されます。

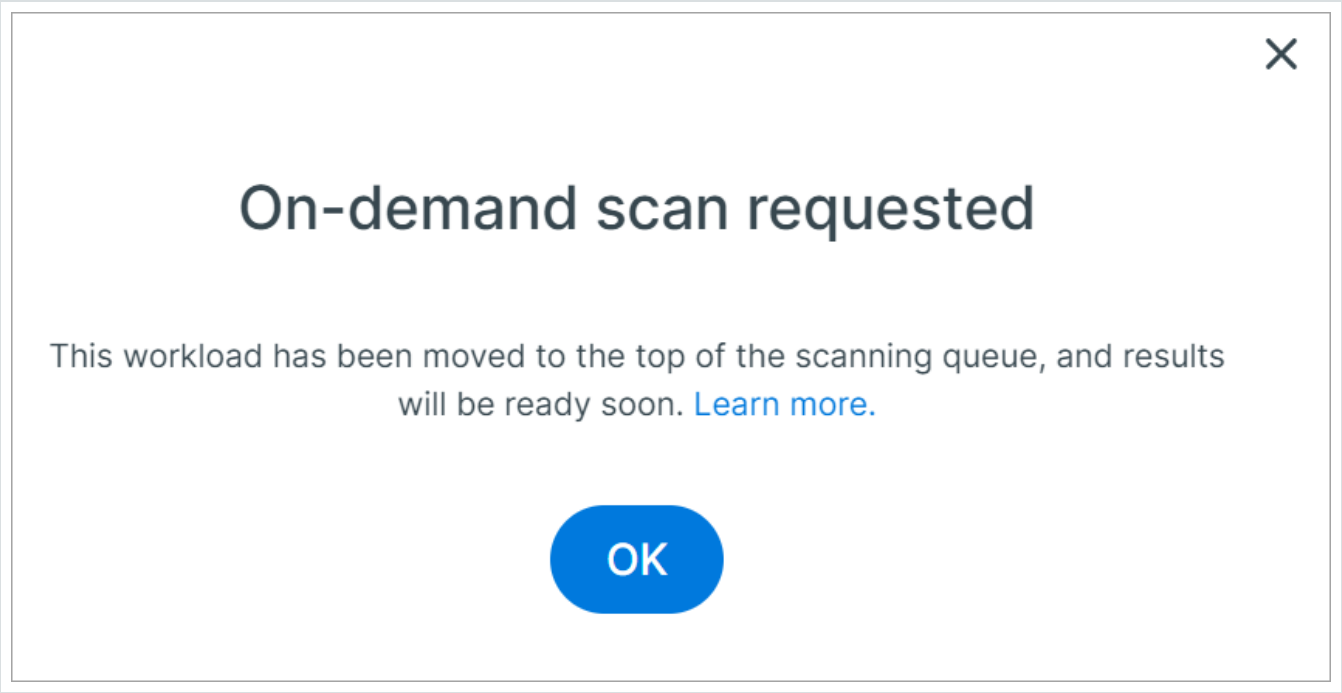
関連する仮想マシンのデータディスクスキャンを有効にするまたはワークロードをスキャンから除外した場合、オンデマンドスキャンは利用できません。

オンデマンドスキャンを実行する方法

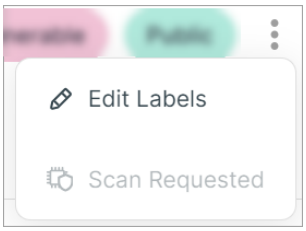
1. 関連する仮想マシンに移動し、クリックします。仮想マシンは、イン **ベントリ** > **仮想マシンイメージ**、または関連するクラウドプロバイダーのインベントリビューにあります (**例:** > **Inventory** > **Compute** > **Azure Virtual Machine Images**)。
2. 三点リーダーアイコンをクリックし、**[今すぐスキャン]** をクリックします。



スキャンが正常にリクエストされたことを示すダイアログが表示されます。



3. **[OK]** をクリックします。
   スキャンがすでにリクエストされている場合、ボタンは無効になり、**[スキャンをリクエスト済み]** と表示されます。



仮想マシンイメージの列データ

次の列は [Virtual Machine Images] (仮想マシンイメージ) ページのテーブルに表示され、そのほとんどがテーブルのデータのフィルターにも使用できます。

縦棒	説明
名前	仮想マシンイメージの名前。
ID	仮想マシンイメージ ID。

縦棒	説明
アカウント	仮想マシンイメージが存在するクラウドアカウント。
日付を追加しました	仮想マシンイメージが追加された日付。
管理	仮想マシンイメージの管理方法
アクセス	仮想マシンイメージのネットワークアクセスの種類。
仮想マシン	仮想マシンイメージに含まれる仮想マシン
オペレーティングシステム	仮想マシンイメージで実行されているオペレーティングシステムとバージョン。
ソフトウェア	仮想マシンイメージにインストールされているすべてのソフトウェアパッケージのリスト。必要に応じて、パッケージのファイルパスも表示されます。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
脆弱性	仮想マシンイメージで見つかった脆弱性の内訳 (リスク深刻度の色分け)。数字をクリックすると、特定の深刻度レベルの脆弱性リストが表示されます。
プラグイン	仮想マシンイメージで検出された脆弱性に関連付けられているプラグイン。**プラグインのリンク**をクリックして、プラグインの詳細を表示します。
検出結果	仮想マシンイメージに関連する検出結果数の深刻度別内訳。数字をクリックすると、検出結果について検索可能なリストが表示されます。

縦棒	説明
脆弱性のスキャンステータス	仮想マシンイメージが正常にスキャンされたかどうかを示します。仮想マシンイメージがスキャンされなかった理由を示します。詳細については、「脆弱性のスキャンステータス」を参照してください。
脆弱性のスキャン時間	クラウドサイバーエクスポージャーが前回仮想マシンイメージをスキャンした時刻を示すタイムスタンプ。イメージがまだスキャンされていない場合、値はダッシュ(-)になります。
データタイプ	リソースで検出された機密性の高いデータタイプ。完全なリストについては「スキャン対象データタイプ」。
データカテゴリ	リソースで検出された機密性の高いデータタイプにマッピングされるデータカテゴリ。
データの機密性	すべてのスキャン対象データから検出された最も高い機密レベル。詳細については、「感度レベル」を参照してください。
データスキャンステータス	リソースが正常にスキャンされたかどうかを示します。リソースがスキャンされなかった理由を示します。詳細については、「データスキャンステータス」を参照してください。
データスキャン時間	前回 クラウドサイバーエクスポージャーがリソースをスキャンした時刻を示すタイムスタンプ。リソースがまだスキャンされていない場合、値はダッシュ(-)になります。
ラベル	手動による適用、タグに基づく自動適用、システムによる適用のいずれかにかかわらず、仮想マシンイメージに適用された「ラベルのリソースへの適用」が表示されます。ラベルのタ

縦棒	説明
	グにカーソルを合わせると、詳細を確認できます。仮想マシンイメージに複数のラベルがある場合、アイコンをクリックするとその他のラベルが表示されます。以下のラベルはワークロード保護に固有のものであり、以下の状況で表示されます。 • **OS パッチ未適用**: ワークロードが、既知の脆弱性が多数存在するバージョンのオペレーティングシステムを実行しています。 • **脆弱性**: ワークロードに少なくとも 1 つの重大な脆弱性があります。 • **OS サポート終了**: ワークロードのオペレーティングシステムはサポートが終了しているか、終了間近 (30 日以内) です。 • **Vulnerable (Exploit)**: ワークロードに、既知のエクスプロイトに関連する重大な脆弱性が少なくとも 1 つあります。
リージョン	仮想マシンイメージが属する AWS リージョン。
タグ	仮想マシンイメージに割り当てられたタグ。

脆弱性のスキャンステータス

[脆弱性スキャンのステータス] 列には、仮想マシンイメージの現在のスキャンステータスが示されます。以下の表は、ステータスの種類と、そのステータスが表示される理由を示しています。理由は通常、ツールチップとしてステータスの横に表示されます。

スキャンステータス	理由
保留中	仮想マシンイメージはキューに入っています。
	このスキャンは、必要な Marketplace イメージをサブスクライブするために Tenable による

スキャンステータス	理由
	手動ステップを保留しています。数時間後にもう一度ご確認ください。
無効	この仮想マシンイメージはワークロードの接続されます。
	仮想マシンイメージのワークロード保護スキャン仮想マシンイメージスキャンからアカウントを除外する。
	この仮想マシンイメージは、ワークロード保護のアクセス許可がないため、スキャンされていません。
	(アカウント内スキャン)このイメージをスキャンするには、AWS Marketplace のサブスクリプションが必要です。アカウント内スキャンに使用する専用の AWS アカウントにログインして AWS Marketplace に移動し、関連する AMI を見つけて [Continue to Subscribe] (サブスクリプションを続行する) をクリックします。詳細についてはワークロード保護 (アカウント内スキャン) を参照してください。
	この仮想マシンイメージは、設定されたスナップショットリソースグループが削除されたため、スキャンされていません。
	この仮想マシンイメージは、ワークロード保護のアクセス許可をブロックする SCP が存在するため、スキャンされていません。
サポート対象外	ディスクにサポートされているパーティションがないため、この仮想マシンイメージに対するスキャンはサポート対象外です。
	この仮想マシンイメージは AWS Marketplace で取得されたものですが、製品 ID が見つからなかったため、スキャンされていません。
	ディスクはインスタンスストアであり、EBS ボリュームではないため、この仮想マシンイメージに対するスキャンはサポート対象外です。

スキャンステータス	理由
	オペレーティングシステムの暗号化が有効になっているため、この仮想マシンイメージに対するスキャンはサポート対象外です。
	スナップショットが削除されないようにロックするリソースグループにリソースが属しているため、この仮想マシンイメージはスキャンされません。
	この仮想マシンイメージは、ディスクの最大サイズを超過しているため、スキャンされていません。
	Marketplace から削除された AWS イメージに基づいているため、この仮想マシンイメージに対するスキャンはサポート対象外です。最新イメージにアップグレードすることをお勧めします。 **注意**: この制限は、AWS Marketplace から直接取得されたスナップショットやイメージ (AMI) には、スキャン操作でコピーしたり共有したりできない、特定のライセンスと所有権の制限があるために発生します。
	この仮想マシンイメージはクラウドサービスによって完全に管理されるため、スキャンはサポート対象外です。
スキャン済み	仮想マシンイメージが正常にスキャンされました。

コンテナイメージ

これは、コンテナイメージの表示と管理に関するガイドです。

- ワークロード保護機能の概念概要については、「ワークロード保護を参照してください。
- コンテナレジストリの設定を構成するには、「Container Registry Settings」を参照してください。
- よくある質問については、「FAQ: ワークロード保護」を参照してください。

すべてのコンテナイメージを表示する

必要なライセンス: この機能は、CSPM、Standard、Enterprise ライセンスのいずれかで利用できます。

Tenable One Cloud Exposure環境内のすべてのコンテナイメージを表示します。

コンテナイメージを表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Explore > Compute > Container Images]** に移動します。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、「コンテナイメージの列データを参照してください。
3. イメージの名前をクリックすると、リソースの詳細の表示。
4. リソースページで、**[ワークロード]** をクリックします。

   注意: Tenable ベースのスキャンは、コンテナイメージに対して追加のコンテキストを提供します。これは、クラウドプロバイダーによって実行されるスキャンでは利用できません。Tenable によってスキャンされたコンテナイメージでは、リソースビューに追加のWorkload タブがあり、関連する修正とともに、1) イメージにインストールされたソフトウェアパッケージと2) イメージ上で検出された脆弱性に関する情報を提供します。
5. 次のいずれかのタブをクリックします。
   - **ソフトウェア**。マシンにインストールされているソフトウェアパッケージを表示します。
   - **脆弱性**。マシンにインストールされているパッケージに関連する脆弱性を表示します。

オンデマンドスキャンの実行

クラウドサイバーエクスポージャー は、すべてのコンテナイメージとコンテナリポジトリを少なくとも 24 時間に 1 回、自動的にスキャンします。特定のワークロードをそれよりも早くスキャンしたい場合は、オンデマンドスキャンをリクエストできます。スキャンを開始すると、そのスキャンはキューの先頭にプッシュされます。スキャン結果は、Tenable によって次回定期的にデータの同期と更新の頻度が実行された後にクラウドサイバーエクスポージャーコンソールに表示されます。

- **コンテナイメージ**。イメージをスキャンすると、その特定のイメージ、親リポジトリ内の最新の 10 個のイメージ、現在使用中のすべてのイメージのスキャンがトリガーされます。

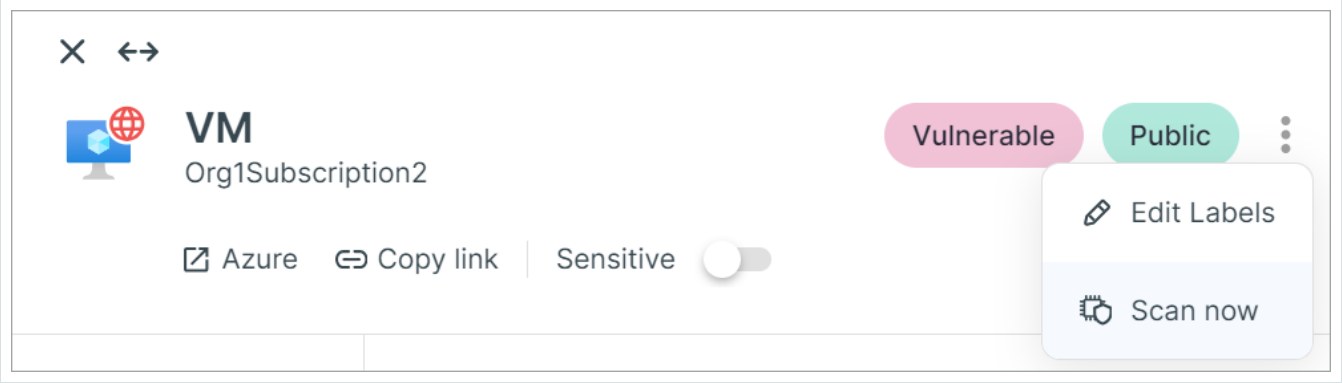
- **コンテナリポジトリ**。リポジトリのスキャンには、最新の 10 個のイメージと、そのリポジトリ内で現在使用されているすべてのイメージが含まれます。

注意:

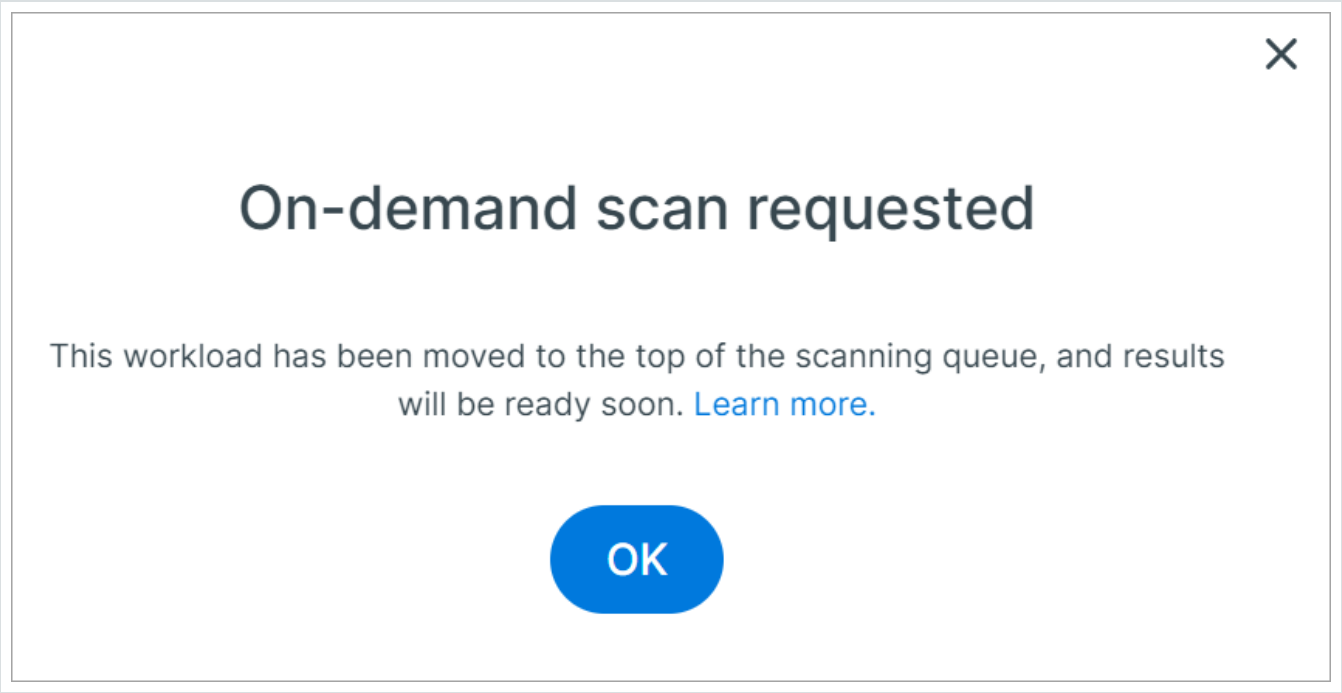
- 関連する 仮想マシンのデータディスクスキャンを有効にする をスキャンから除外した場合、オンデマンドスキャンは利用できません。
- アクセス許可が付与されていない外部リポジトリでは、オンデマンドスキャンはサポートされていません。

オンデマンドスキャンを実行する方法

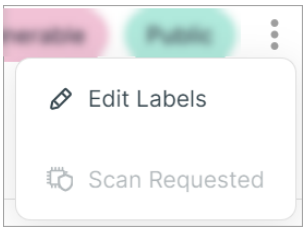
1. 関連する仮想マシンに移動し、クリックします。仮想マシンは、**[Explore > Compute]** > **[Virtual Machines]**、または関連するクラウドプロバイダーのインベントリビューにあります (例: **[Explore > Inventory]** > **[Compute > Azure Virtual Machines]**)。
2. 三点リーダーアイコンをクリックし、**[今すぐスキャン]** をクリックします。



スキャンが正常にリクエストされたことを示すダイアログが表示されます。



3. **[OK]** をクリックします。
   スキャンがすでにリクエストされている場合、ボタンは無効になり、**[スキャンをリクエスト済み]** と表示されます。



コンテナイメージの列データ

次の列は [Container Images] (コンテナイメージ) ページのテーブルに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

縦棒	説明
名前	イメージの名前。
アカウン	イメージに関連付けられているクラウドアカウント。イメージは、それを実行するすべてのア

縦棒	説明
ト	カウントの下に表示されます。クラウドサイバーエクスポージャーに同期していないレジストリ(docker.io や quay.io など) からプルされたイメージは、**コンテナレジストリ**という名前の 1 つのアカウントの下に表示されます。
リポジトリ	イメージが保存されているリポジトリのリスト。
イメージタグ	イメージに割り当てられたタグ。
ダイジェスト	コンテナイメージ識別子 (SHA256)。
イメージラベル	イメージの Docker コンテナラベルのリスト (`key:value`別に一覧表示)。キーまたは値のサイズが 5KB を超えるラベルはリストされません。
作成時間	イメージが作成されたタイムスタンプ。
クラスタ	コンテナイメージを使用するクラスタ
仮想マシン	コンテナイメージを使用する仮想マシン。
ワークロード	イメージがデプロイされるワークロード。たとえば、仮想マシン、Kubernetes ワークロード、コンテナサービスソリューションなどです。
オペレーティングシステム	イメージで実行されているオペレーティングシステムとバージョン。

縦棒	説明
オペレーティングシステムタイプ	イメージの特定のオペレーティングシステムのディストリビューション。
ソフトウェア	ワークロードにインストールされているすべてのソフトウェアパッケージのリスト。必要に応じて、パッケージのファイルパスも表示されます。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
脆弱性	ワークロードで見つかった脆弱性の内訳 (リスク深刻度の色分け)。数字をクリックすると、特定の深刻度レベルの脆弱性リストが表示されます。
検出結果	アイデンティティに関連付けられた検出結果の数。数字をクリックすると、検出結果について検索可能なリストが表示されます。
プラグイン	イメージで検出された脆弱性に関連するプラグイン。**プラグインのリンク**をクリックして、プラグインの詳細を表示します。
スキャン時間	クラウドサイバーエクスポージャーが前回マシンをスキャンした時刻を示すタイムスタンプ。マシンがまだスキャンされていない場合、値はダッシュ (-) になります。
ラベル	手動による適用、タグに基づく自動適用、システムによる適用のいずれかにかかわらず、イメージに適用されたラベルのリソースへの適用 が表示されます。ラベルのタグにカーソルを合わせると、詳細を確認できます。イメージに複数のラベルがある場合、アイコンをクリックするとその他のラベルが表示されます。以下のラベルはワークロード保護に固有のものであり、以下の状況で表示されます。 • **OS パッチ未適用**: ワークロードが、既知の脆弱性が多数存在するバージョンのオペレーティングシステムを実行しています。

縦棒	説明
	• **脆弱性**:ワークロードに少なくとも 1 つの重大な脆弱性があります。 • **OS EOL**: ワークロードのオペレーティングシステムはサポートが終了しているか、終了間近 (30 日以内) • **Vulnerable (Exploit)**: ワークロードに、既知のエクスプロイトに関連する重大な脆弱性が少なくとも 1 つあります。
コンテナイメージの使用 (フィルターのみ)	スキャンされたコンテナイメージがワークロードによって使用されているかどうかを示します。 **可能な値**: Unused、Used。 詳細については、FAQ をご覧ください。

注意: コンテナイメージは、複数のアカウントに表示できます。イメージを実行する各アカウントには、イメージの脆弱性、パッケージ、リスクがアカウントのワークロードに関連付けられた状態で、独自のインベントリに表示されます。同期されていないレジストリまたはパブリックレジストリからのイメージは、最初にイメージをプルしたクラウドアカウントではなく、**コンテナレジストリ**アカウントの下に統合されます。

Kubernetesクラスター

注意: この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

クイックリンク

これは Kubernetes クラスターを表示および管理するためのハウツーガイドです。

- Kubernetes 機能の概念上の概要については、Kubernetes参照してください。
- クラスターを Tenableに接続する方法に関するガイドについては、関連ガイドを参照してください。Via Helm チャートを介してクラスタを接続する、Amazon EKS クラスタの接続、Azure AKS クラスタの接続、Google GKEクラスターを接続する、Oracle OKEクラスタの接続。

- VM 設定を構成するには、仮想マシンの設定参照してください。
- よくある質問については、「FAQ: Kubernetes 」を参照してください。

専用のクラスターページには Tenable One Cloud Exposure、に接続されているすべてのクラスターが表示されます。クラスターの接続方法の詳細については、Kubernetes クラスターを参照してください。

注意: Helm チャートを介してインストールされたクラスターの場合、インストール後に次回 データの同期と更新の頻度 ときに、コンソールにリソースが表示されます。

クラスターの表示

クラスターを表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[調査]** > **[コンピューティング]** > **[Kubernetes クラスター]** に移動します。
2. 表内で、以下のオプションのタスクを実行できます。
    - [Organization] ドロップダウンで アカウント階層とフォルダー を選択して、その範囲のクラスターを表示します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
    - 表をフィルタリングして、表示されるデータの範囲を変更します。詳細は クラスター列データ 参照してください。
    - テーブルを CSV に**エクスポートします** 。
    - このページを使用して、クラスターを接続したり、すでに接続されているクラスターに新しい機能をインストールしたりできます。詳細は、Helm チャートを介してクラスタを接続する 参照してください。
    - (オンプレミスクラスター) クラスターに関連する同期されたリソースと検出結果を削除するには、クラスターの横にある 3 つの点のアイコンをクリックし、**[削除]** をクリックします。環境で次回 データの同期と更新の頻度 ときに、リソース/検出結果が削除されます。

    注意: リソース/調査結果を削除する場合、Helm チャートを介してクラスタを接続する使用して、接続されたクラスターもアンインストールすることが強く推奨されます。

クラスターを管理する

次のアクションを使用して、クラスターを維持および更新します。

- Helm をアップグレードするまたは新機能をインストールする
- Tenable からクラスターを切断する
- クラスターを別のアカウントに移動する

Helm をアップグレードするまたは新機能をインストールする

Helmチャートがすでにインストールされているクラスターに **Runtime Detection**、**Admission Controller**、**Vulnerability Management** などの機能をインストールする方法、または Helm バージョンを更新する方法

1. クラウドサイバーエクスポージャーコンソールで、**[調査]** > **[コンピューティング]** > **[Kubernetes クラスター]** に移動し、関連するクラスターを見つけます。
2. **3 つのドットの** メニュー (サード) をクリックし、**[Upgrade Helm]** を選択します。
3. ウィザードの手順に従って、目的の機能またはバージョンを選択します。
4. CLI で、ローカルリポジトリを更新します。
   ```
   helm repo update tenable
   ```
5. ウィザードによって提供される生成された Helm コマンドを実行して、追加されたクラスターの構成を更新します。

> **注意:** Tenable イメージを少なくとも **2 週間ごとに** 更新して、が環境内の最新の脆弱性とセキュリティリスクを特定できるようにしてください。

Tenable からクラスターを切断する

クラスターの接続を解除するには、環境から Helm チャートをアンインストールします。Tenable は、次のデータの同期と更新の頻度中に、コンソールからクラスターを削除します。

1. **次のコマンドを実行してください**:
   ```
   helm uninstall -n tenable-cloud-security-kubernetes-cluster
   ```
2. (オンプレミスクラスター) 同期されたリソースと検出結果をすぐに削除するには、クラスターの横にある 3 つのドットメニュー (、) をクリックし、**[削除]** をクリックします。

クラスターを別のアカウントに移動する

場合によっては、クラスターを別のアカウントの場所に移動する必要があるかもしれません。たとえば、クラウドアカウントを Tenableに接続する前に Helm 経由でクラウドベースのクラスターを接続すると、コンソールはクラスターをオンプレミスのデフォルトアカウントに自動的にマップします。

警告: クラスターを移動すると、元のアカウントスコープで作成された構成がすべて失われます。新しい範囲でこれらの設定を再設定する必要があります。さらに、Tenable は自動的に元の範囲の検出結果と対応するチケットをクローズし、新しい範囲で再度開きます。

クラスターを別のアカウントに移動する方法

1. 次のコマンドを実行してクラスターをアンインストールします。
    - `helm uninstall -n tenable-cloud-security-kubernetes-cluster`
2. 標準のインストールプロセスを使用して、クラスターを正しい場所に再追加します 。

追加機能でクラスターをアップグレードする

お客様は、新しい機能を含めるためにクラスターをアップグレードする必要があります。クラスターに新しい機能をインストールするには、次の手順に従ってください。

1. クラウドサイバーエクスポージャーコンソールにログインします。
2. 左側のナビゲーションペインで、**[調査]** > **[計算]** > **[Kubernetes クラスター]** をクリックします。
3. 関連するクラスターの右側にある 3 つのドットメニュー **(サード)** > **[Upgrade Helm]** をクリックします。
4. ウィザードの指示に従います。

repo がすでに追加されているマシンの場合:

- 以下を実行して、repo を最新のチャートに更新してください。`helm repo update tenable`
- 最適なパフォーマンスを得るために、イメージが少なくとも **2 週間ごとに** 更新されるようにしてください。

クラスター列データ

次の列は [Clusters] ページのテーブルに表示され、そのほとんどはテーブル内のデータのフィルタリングにも使用できます。

列	説明
名前	クラスターの名前
アカウント	クラスターが配置されているアカウント。
プラットフォーム	可能な値: Kubernetes、OpenShift
作成時間	クラスターが作成された日付。
リソース同期	Tenable がクラスターのリソースを可視化しており、検出された設定ミスの検出結果をトリガーできるかどうかを示します。接続されている場合、Tenable は Kubernetes API に接続できます。ネットワークが切断されている、またはアクセス許可がない場合は、クラスタータイプに関連する統合手順に従ってください。表示されるステータスについては、リソース同期ステータスを参照してください。
リソース同期時刻	Tenable がクラスターリソースを最後に同期した日時。この列はデフォルトでは非表示です。
ランタイム検出	eBPF センサーがインストールされており、クラスターワークロードのイベントを監視して疑わしいアクティビティを検出しているかどうかを示します。
アドミッションコントローラー	Tenable アドミッションコントローラーが Kubernetes クラスターにインストールされ、実行されているかどうかを示します。 この機能は Enterprise ライセンスでのみ利用できます。詳細については、ライセンス参照してください。
ワークロード保護	Tenable がオンプレミスクラスターのノードとコンテナイメージの脆弱性をスキャンできるかどうかを示します。[Running] (実行中) の場合、Tenable センサーはインストールされ、クラスタで実行されています。表示されるステータスについては、ワークロード保護ステー

列	説明
	タスを参照してください。 **注意**: この機能はEnterpriseライセンスでのみ利用可能です。詳細については、ライセンス参照してください。
Helmバージョン	クラスターへの接続に使用された関連するKubernetes Cluster Helmのバージョンの名前 (該当する場合)、およびネットワーク/IDアクセスが設定されているかどうか。この列はデフォルトでは非表示です

リソース同期ステータス

各 Kubernetes クラスターについて、クラウドサイバーエクスポージャー がKubernetes API に接続できるかどうかを示す **リソース同期ステータスを** 確認できます。

- 接続されている場合、クラウドサイバーエクスポージャー はクラスターのリソースを可視化し、検出された設定ミスの発見をトリガーできます。
- ネットワークが切断されている場合、またはアクセス許可がない場合は、関連するクラスタータイプの統合手順に従ってください。

ステータス:

> **注意:** オンプレミスクラスターが接続されており、同じクラスターのクラウド管理対象バージョンも検出されると、**重複した** 表示が表示されることがあります。たとえば、オンプレミスクラスターのステータスは **[接続済み (複製)]** と表示されます。

- **接続済み**: Tenable Kubernetes API に正常に接続されました。
- **問題と接続済み** (Azure): クラスターは接続されていますが、カスタム Tenable ロールを追加するが追加されていないため、IAM の可視性はありません。
- **接続に失敗しました**: Tenable 不明なエラーのため、クラスターに接続できません。サポートへの問い合わせ。サポートが必要です。
- **接続の消失**: 接続は過去 48 時間以内に失われ、自動的に再接続する可能性があります。
- **非アクティブなクラスター**: Tenable が非アクティブであるため、クラスターに接続できません。

- **アクセス許可がありません**
  - Tenable IAM ロール / アプリ (Azure) には、クラスターへのアクセス許可が付与されていません。クラウドが管理するパブリッククラスターに対してこれらのアクセス許可を付与する方法については、Kubernetes クラスターを参照してください。
  - Tenable クラスターにアクセスするための ID ベースのアクセス許可がないため、はクラスターにアクセスできません。これは、Azure クラスタがローカルアカウント認証で設定されている場合に発生する可能性があります。Azure AD 認証と連携するようにクラスターを変更するか、Helm Chartを介して接続します。
- **ネットワークアクセスなし**
  - Tenable は、ネットワーキングトンネルがないか、トンネルに到達できないため、クラスターにアクセスできません。これは、クラスターがプライベートで、通信トンネルが Helm Chartを介して構成されなかった場合に発生する可能性があります。
  - Tenableクラウドサイバーエクスポージャーの IP アドレスを許可していないため、はクラスターにアクセスできません。
- **Pending**: クラスターステータスは次のデータの同期と更新の頻度で更新されます。

AKS Clusters	Created	Status	Kubernetes Version	Connection Status	Authentication and Authorization
[redacted]	Feb 22, 2022	Running	1.21.9	Missing Permissions	Local accounts with Kubernetes RBAC
[redacted]	Jul 14, 2022	Running	1.22.11	Missing Permissions	No RBAC
[redacted]	Jul 13, 2023	Running	1.25.6	Connected	Azure AD with Azure RBAC
[redacted]	Apr 9, 2023	Running	1.24.15	No network access	Azure AD with Azure RBAC
[redacted]	Jul 12, 2023	Running	1.25.11	Missing Permissions	Azure AD with Azure RBAC
[redacted]	May 18, 2023	Running	1.25.11	Connected	Azure AD with Azure RBAC

オンプレミスクラスターの脆弱性管理ステータス

必要なライセンス: この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

各オンプレミス Kubernetes クラスターの **ワークロード保護** ステータスを表示して、Tenable がノードとコンテナイメージの脆弱性をスキャンできるかどうかを判断できます。[実行中] ステータスは、センサーが正常にインストールされ、クラスターにアクティブであることを示します。

詳細については、クラスターステータスを参照してください。

クラスターステータス

ステータス	説明
接続済み (複製)	このステータスは、オンプレミスクラスターは現在接続されているが、同じクラスターの重複するクラウド管理バージョンが検出されたことを示します。
インストールされていない	Tenable センサーがインストールされていません。クラスターの横にある [機能のインストール] をクリックし、手順に従い、オンプレミスワークロード保護を有効にして クラスターを追加する 。
実行されていない	センサーはインストールされましたが、この機能は現在アクティブではありません。このステータスは、Tenable が想定されるタイムフレーム内にポッドから「ハートビート」信号を受信しなかったことを示します。これは、ポッドがダウンしているか、システムと通信できない可能性を示唆しています。通常の動作に戻すには、トラブルシューティングが必要な場合があります。
実行中	Tenable センサーはインストールされており、クラスタのノードとコンテナイメージをスキャンして脆弱性を検出できます。

ソフトウェア

仮想マシンイメージの表示と管理に関するハウツーガイドです。

- ワークロード保護機能の概念概要については、「ワークロード保護を参照してください。
- よくある質問については、「FAQ: ワークロード保護」を参照してください。

すべてのソフトウェアパッケージを表示する

お使いの環境のワークロードにインストールされているソフトウェアパッケージを表示します。任意のパッケージについて、パッケージバージョン、パッケージの種類 (オペレーティングシステムなど)、関連する脆弱性を表示できます。1 つのパッケージの異なるバージョンはそれぞれ、テーブル内に独立したパッケージとして表示されます。

ソフトウェアパッケージを表示するには:

1. Tenable One Cloud Exposure コンソールで、**[Explore > Compute > Software]** (**コンピューティングソフトウェアの調査**) に移動します。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、「ソフトウェアパッケージの列データ」を参照してください。

ソフトウェアパッケージの列データ

以下の列は [ソフトウェア] ページのテーブルに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

縦棒	説明
名前	ソフトウェアパッケージの名前。
パス	(ライブラリのみ)パッケージのファイルパス。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
タイプ	パッケージのタイプ。可能な値: Operating System、Library。 オペレーティングシステムパッケージには、カーネル、`glibc`、`openssl`、`systemd`、`apt` などの Windows と Linux OS の両方のコンポーネントが含まれています。オペレーティン

縦棒	説明
	グシステムでフィルタリングして、修正中にOSレベルのパッケージに焦点を当てます。
エクスポージャー	
リソース	パッケージが確認された仮想マシン。
リソースアカウント	パッケージが確認されたコンテナイメージ。
脆弱性	パッケージに関連付けられている脆弱性のリストで、CVE ID別に一覧表示されます。(例: CVE-2021-3177) IDにカーソルを合わせると、脆弱性の詳細 (説明や関連する情報ソースなど) についての概要ビューが表示されます。
プラグイン名	パッチの名前とバージョン。**パッチのリンク**をクリックすると、パッチの詳細が表示されます。
プラグインID	ソフトウェアの脆弱性の修正を含むパッケージの一意の識別子またはビルド文字列。
オペレーティングシステムタイプ	特定のオペレーティングシステムのフレーバー。

特定のワークロードのソフトウェアパッケージを表示する

特定のワークロードにインストールされているソフトウェアパッケージを表示する方法

1. 特定のワークロードにドリルダウンします。
2. ワークロードのリソースページで、**[ソフトウェア]** タブをクリックします。
3. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。

以下のデータを利用できます。

縦棒	説明
名前	パッケージの名前。
バージョン	パッケージのバージョン。
パス	(ライブラリのみ)パッケージのファイルパス。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
タイプ	パッケージのタイプ。可能な値: Operating System、Library。
脆弱性	パッケージに関連付けられている脆弱性のリストで、CVE ID 別に一覧表示されます。(例: CVE-2021-3177) クリックすると、CVE を一目で確認できるビューが表示されます。

IAM

概要

最小権限ポリシーの生成とロール

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

クラウドのアイデンティティとリソース用のきめの細かいオンデマンドポリシーを作成し、最小権限ポリシーを生成してセキュリティのベストプラクティスを実施します。これらのポリシーでは、必要なタスクの実行に必要なアクセス許可のみを付与するため、過剰なアクセスのリスクを軽減できます。AWS、Azure、GCP の

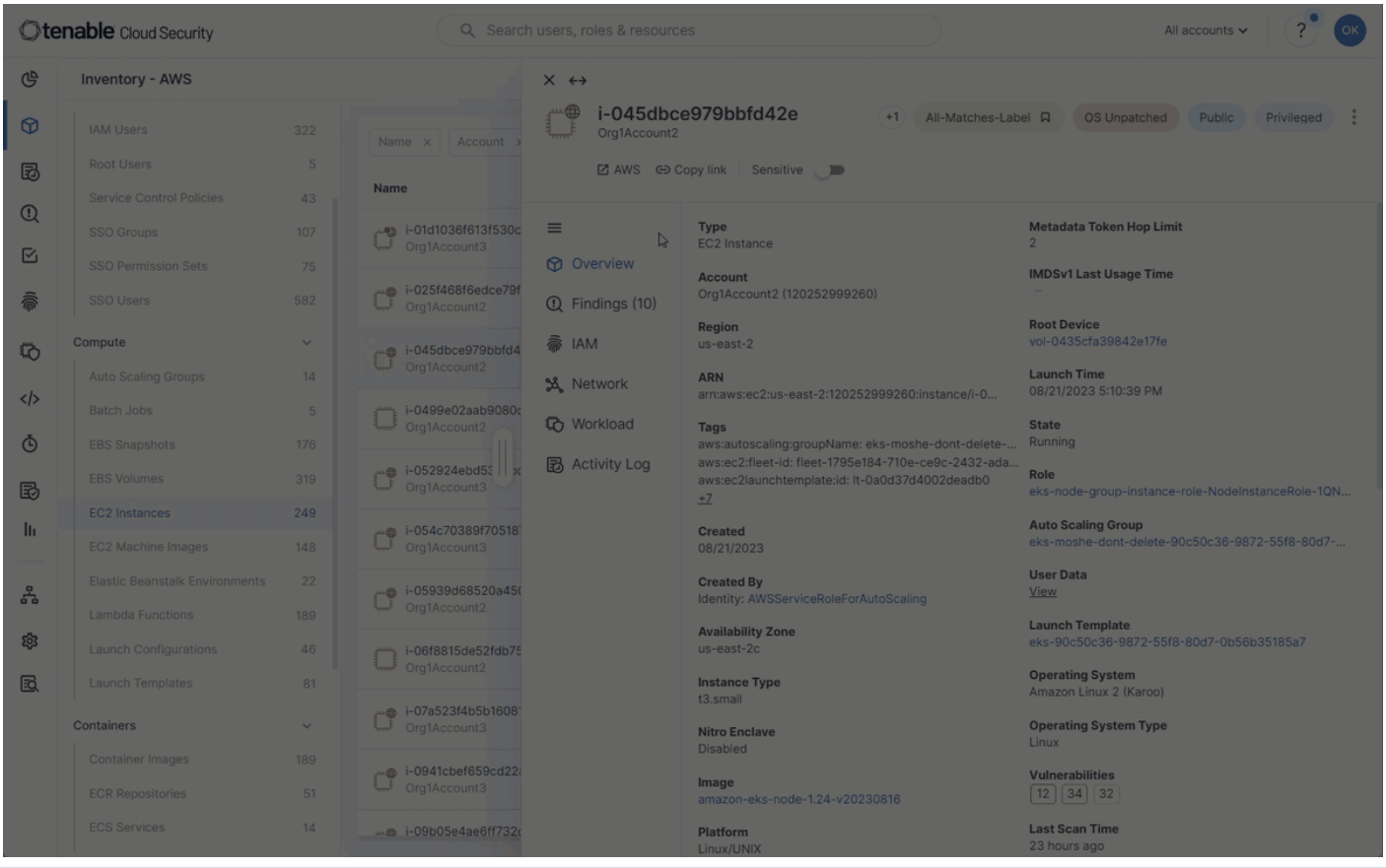
いずれを使用しているかにかかわらず、この機能を使用すると、リソースのアクティビティと設定に基づいて、カスタマイズされたAWS: 最小権限ポリシーの生成 、またはAzureまたはGCPのカスタムロールを生成できます。アクセス許可を調整することにより、組織は運用効率を維持しながら、セキュリティ標準に準拠することができます。

サポートされているリソースに対して最小権限ポリシーを生成できます。

AWS: 最小権限ポリシーの生成

アイデンティティやリソースについて、オンデマンドのきめ細かいポリシーを生成し、必要なタスクの実行に必要な最小権限を付与します。

開発者が開発環境で作業する際、通常は広範なアクセス許可から開始し、ワークロードが落ち着くにつれて、実際に使用されるサービス、リソース、アクションのみのアクセス許可に縮小していきます。これにより、ワークロードが開発環境から本番環境に移行される際、セキュリティのベストプラクティスに沿ったポリシーを適用できます。

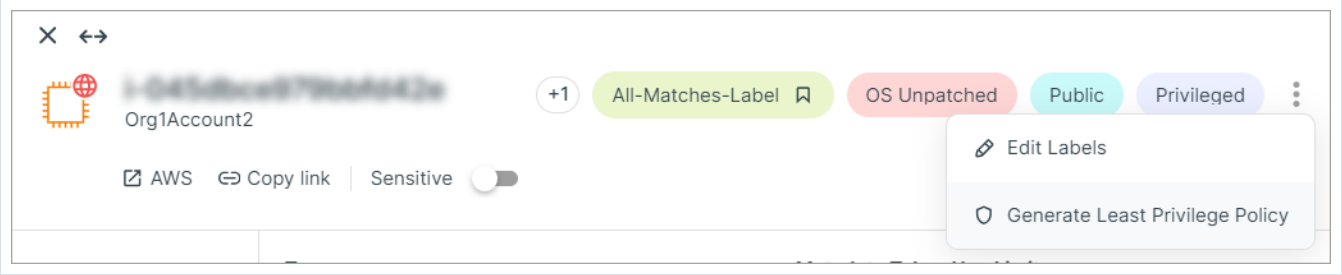


必要な Tenable One Cloud Exposure ユーザーロール: オンデマンドポリシーの生成は、ユーザーやロールの作成から 24 時間後に利用可能になります。この機能を使用するには**コラボレータ**または**管理者**ロールが必要です。

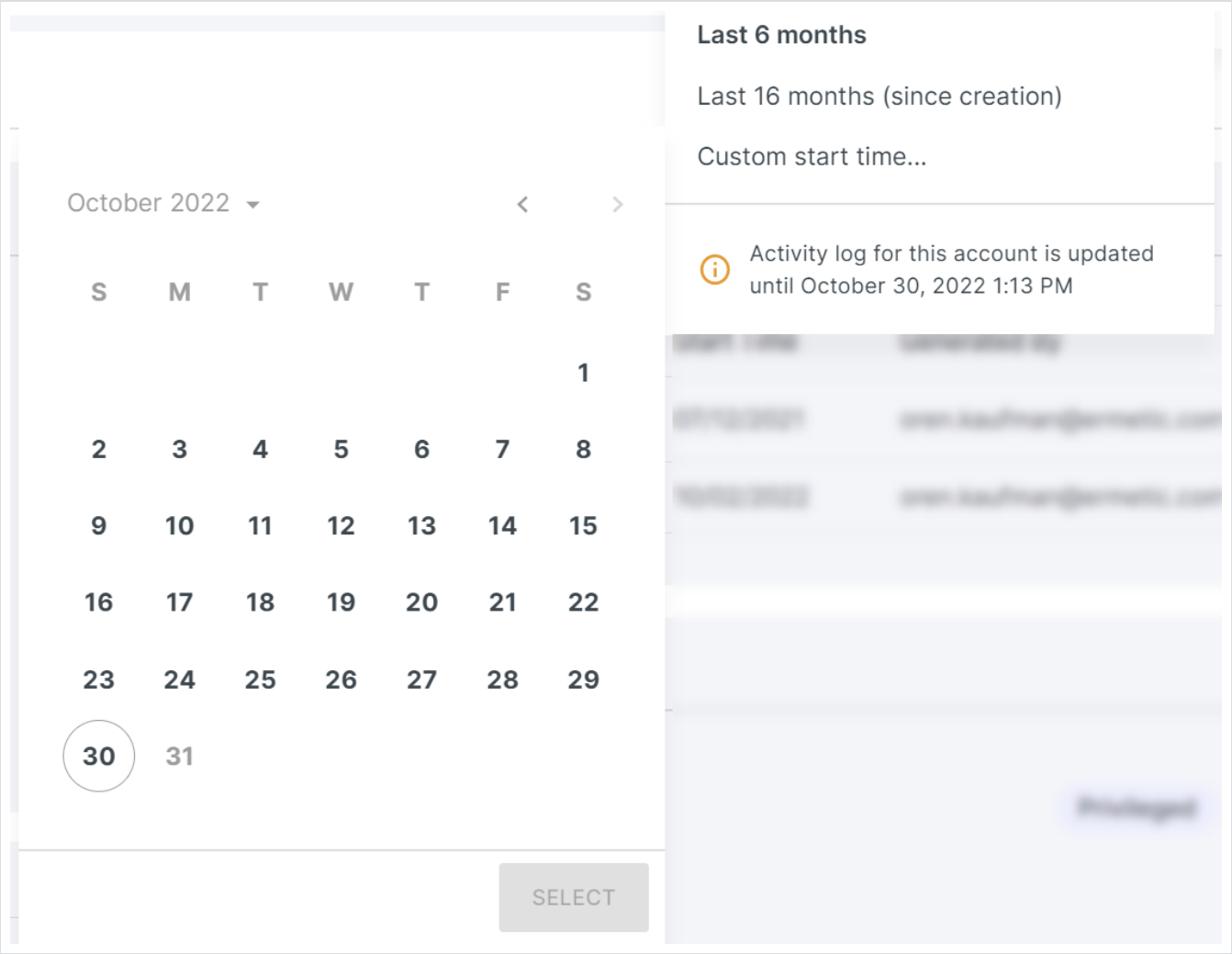
[Identity Intelligence] (アイデンティティインテリジェンス) ページ (**[IAM] > [Identity Intelligence]** の調査 >) でも最小権限ポリシーを生成することができます。

最小権限ポリシーを生成する方法

1. 資産インベントリの表示。
    1. クラウドサイバーエクスポージャーコンソールで、**[インベントリ]** をクリックします。
    2. [Inventory] (インベントリ) ビューで、AWS サポートされているリソースタイプのいずれかを選択します (**IAM ロール**や **EC2 インスタンスなど**)。
2. 関連するリソースをクリックしてドリルダウンします。
3. 三点リーダーアイコンをクリックし、**[最小権限ポリシーの生成]** をクリックします。



4. 学習期間の日付範囲を指定します。利用可能な日付の範囲は、ユーザーやロールが作成された日時、または EC2 インスタンスの起動日時によって異なります。また、**[カスタム開始時刻]** を選択することもできます。これにより、定義された開始日から現在の日付までのデータに基づいてポリシーが作成されます。リソースのアクティビティログがどの程度最新のものであるかを示すインジケーターが表示されます。リソースの



日付を選択すると、クラウドサイバーエクスポージャーは、選択した日付範囲のアクティビティに基づいて最小権限ポリシーを生成します。

5. **グループメンバーシップ経由で付与されたアクセス許可を含める**か、無視するか(デフォルト)を選択します。
6. **ワイルドカードの代わりに特定のリソースを使用する**かどうかを選択します。詳細については、「リソース粒度」を参照してください。
7. 必要に応じて、ポリシーをコピーまたはダウンロードします。

注意: AWSにはポリシーの最大許容サイズがあります。生成されたポリシーがこのサイズを超える場合、クラウドサイバーエクスポージャーは必要に応じて複数のポリシーを生成します。ポリシーの数は、JSONポリシーアイコンの横の括弧内に示されます。

AWS リソース粒度

AWS では、すべてのサポート対象サービスに対して常にワイルドカードを使用する代わりに、特定のリソースを含むポリシーを生成できます。

AWS: 最小権限ポリシーの生成を生成するときに、**[ワイルドカードの代わりに特定のリソースを使用する]** オプションを選択できます。このオプションでは、ポリシーの特定のリソースを含めるためにリソース粒度を使用します。生成されたポリシーには、リソース粒度でサポートされているリソース リストのリソースを含めることができます。

リソース粒度によって、AWS の文字制限を超えるポリシーが作成される可能性があることに注意してください。このポリシーをアタッチしても、新しいリソースへのアクセスは許可されません。新しいリソースへのアクセスを許可する必要がある場合は、このオプションを選択せずにワイルドカードを使用することをお勧めします。

リソース粒度でサポートされているリソース

Tenable は、次の AWS サービスで最も重要かつ一般的なリソースをサポートしています。

- CloudFormation
- CloudTrail
- DynamoDB
- ECR
- IAM
- KMS
- S3
- Secrets Manager
- SNS
- SSM
- SSO
- STS

ユーザーまたはサービスアイデンティティの最小権限カスタムロールの生成

ユーザーまたはサービスアイデンティティ用にオンデマンドのカスタムポリシーを生成し、それを Azure や GCP で使用して、ユーザーがタスクを実行するために必要な最小権限を付与できます。

> **注意:** Azure と GCP の過剰な権限の検出結果については、(既存のロールを使用する代わりに) これらのカスタムロールを使用して、問題のあるロールの割り当てを修正できます。関連する検出結果の専用の修正タブを使用すると、容易に修正を行えます。

[Identity Intelligence] (アイデンティティインテリジェンス) ページ (**[IAM] >> [Identity Intelligence] の調査**) でも最小権限ポリシーを生成することができます。

ユーザーまたはサービスアイデンティティのカスタムロールを生成する方法

1. 資産インベントリの表示。クラウドサイバーエクスポージャーコンソールで、サポートされているリソースを選択します。
    1. **Azure**: **[インベントリ]** > IAM をクリックし、**[Azure マネージド ID]** を選択します。
    2. **Microsoft Entra ID**: **[Inventory] (インベントリ)** をクリックし、サポートされているリソースのいずれかを選択します。
    3. **GCP**: [イン **ベントリ]** > **[IAM]** をクリックし、**[GCP サービスアカウント]** を選択します。
    4. **Google Workspace**: **[インベントリ]** をクリックし、**[Google Workspace ユーザー]** を選択します。
2. 関連するリソースをクリックしてドリルダウンします。
3. 三点リーダーメニュー ⋮ クリックし、[**カスタムロールの生成]** をクリックします。
4. 範囲 **レベル** を選択して、分析に含めるリソースと、アイデンティティにロールを割り当てるレベルを決定します。次のいずれかを選択できます。
    1. **Azure** および **Microsoft Entra ID**:
        - 管理グループ
        - サブスクリプション
        - リソースグループ

2. GCP とGoogle Workspace:
    - 組織
    - フォルダー
    - プロジェクト

    選択された範囲について、その範囲またはそれ以上ですでに付与されているすべてのアクセス許可クラウドサイバーエクスポージャー考慮されます。それ未満の範囲で付与されていたアクセス許可は無視されます。

5. ロール学習期間の**タイムフレーム**を選択します。最も早い開始時間として使用できる日付は、アイデンティティが作成された日付、またはそのアイデンティティで最初にログ記録されたイベントの日付のどちらか遅い方になります。
6. **グループメンバーシップ経由で付与されたアクセス許可を含める**か、無視するか(デフォルト)を選択します。
7. GCP とGoogle Workspace リソースの場合のみ: **プロジェクトレベルで割り当てられた基本ロール(プロジェクト所有者など)を介して付与されたアクセス許可を含める**(デフォルト)か、無視するかを選択します。
8. **[生成]**をクリックします。カスタムロールが表示されます。ロールを**コピー**して使用します。

GCP および Microsoft Entra ID グループの最小権限カスタムロールの生成

オンデマンドのカスタムポリシーグループを生成して、グループが GCP および Microsoft Entra ID でタスクを実行するために必要な最小権限を付与できます。

> **注意:** GCP とMicrosoft Entra ID の過剰な権限の検出結果については、これらのカスタムロールを使用して、問題のあるロールの割り当てを修正できます。このプロセスを容易にするために、関連する検出結果には専用の**[修正]**タブがあります。

最小権限ポリシーは、[Identity Intelligence] (アイデンティティインテリジェンス) ページ (**[IAM]** > **[Investigation]** >) でも生成できます。

グループのカスタムロールを生成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>クラウドの検出結果]** に移動します。
2. 次のいずれかで表を絞り込みます。
    - **GCP**: プロジェクトポリシーで ワークスペースグループGoogle過剰な権限を持つ。
    - **Microsoft Entra ID**: サブスクリプションポリシーで過剰な権限を持つ Microsoft Entra ID グループ。
3. 結果の表で、最小権限のカスタムロールを作成する検出結果をクリックします。検出結果の詳細のサイドペインが開きます。
4. [修正] で、**[新しいロール経由]** タブをクリックします。

    > **注意: [Via New Roles]** タブは、ロールを置き換える必要がある場合にのみ表示されます。ロールに置換が必要ない場合は、修正手順のみが表示されます。

5. 修正手順で、カスタムロールのリンクをクリックします。
6. **範囲レベル**を選択します。
7. **グループメンバーシップ経由で付与されたアクセス許可を含める**か、無視するかを選択します。
8. **プロジェクトレベルで割り当てられた基本ロール (プロジェクト所有者など) を介して付与されたアクセス許可を含める** (デフォルト) か、無視するかを選択します。
9. **[生成]** をクリックします。カスタムロールが表示されます。ロールを[Copy] (コピー) して使用します。

サポートされているリソース

次のリソースタイプがサポートされています。

- AWS
    - IAM ユーザー
    - IAM ロール
    - EC2 インスタンス
    - Lambda 関数
    - DynamoDB

- Azure
    - マネージド ID
- Microsoft Entra ID
    - ユーザー
    - アプリケーション
- GCP
    - サービスアカウント
    - Google Workspace グループ
    - Google Workspace グループ (外部)
- Google Workspace
    - ユーザー

重複するロールの割り当てまたはバインディングを監視する

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

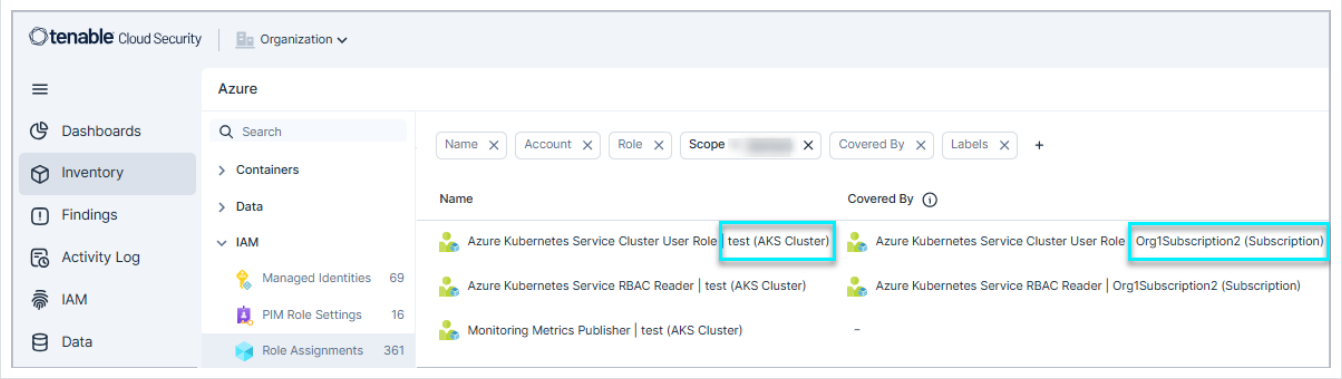
重複するロールの割り当てまたはバインディングとは、ユーザー、グループ、サービス ID などのプリンシパルが、多くの場合、異なるパス (直接またはグループ経由など) を介して、同じロールを複数回受け取るケースを指します。このような場合、ロールの割り当てまたはバインドは、より高いスコープレベルまたはグループメンバーシップからの他のロール割り当てまたはバインディングによって「カバー」される可能性があります。これらの重複は、組織レベルのアクセスとルートレベルでの個別の割り当てを持つグループなど、より広い範囲をカバーするグループメンバーシップに起因する場合があります。

重複するロールの割り当てまたはバインディングを表示するには

1. クラウドプロバイダー固有のロール割り当てに移動します。
    - Azure の場合は、**[調査]** > **[インベントリ]** > **[IAM]** > **[Azure ロールの割り当て]** に移動します。
    - GCP の場合は、**[探索する]** > **[インベントリ]** > **[IAM]** > **[GCP ロールバインディング]** に移動します。

2. **[Covered By] フィルターの利用**: **[Covered By]** フィルターを適用すると、すべてのロール割り当てを統一形式で表示できます。これにより、以下に基づいて簡単にフィルタリングできます。
    - **ロール**: 同じロールが複数に割り当てられているインスタンスを特定します。
    - **Scope**: 重複が存在する可能性がある特定の範囲に検索を絞り込みます。
    - **プリンシパル**: 特定のユーザー、グループ、またはサービスアイデンティティが、異なる割り当てで同じアクセス許可を付与されているかどうかを確認します。
3. **追跡および自動化の**強化: このメソッドにより、アクセス許可をより適切に追跡できます。また、重複するロール割り当ての自動監視および管理を行うために、API を介してレポートをスケジュールしたり、データにクエリを実行したりすることもできます。

    例:



あるいは、[調査] > [インベントリ] > [Google Workspace/Microsoft Entra ID ユーザー] に移動し、**[カバーされた GCP ロールバインディング] / [カバーされた Azure ロール割り当て]** の列を追加して、そのアイデンティティの「カバーされた」すべてのアクセス許可を表示できます。ただし、これには重複している可能性があるため **手動のマッピング** が必要になり、「対象となるロールの割り当て」を正確に追跡する効果が低下します。

アクセス許可マッピングの視覚化

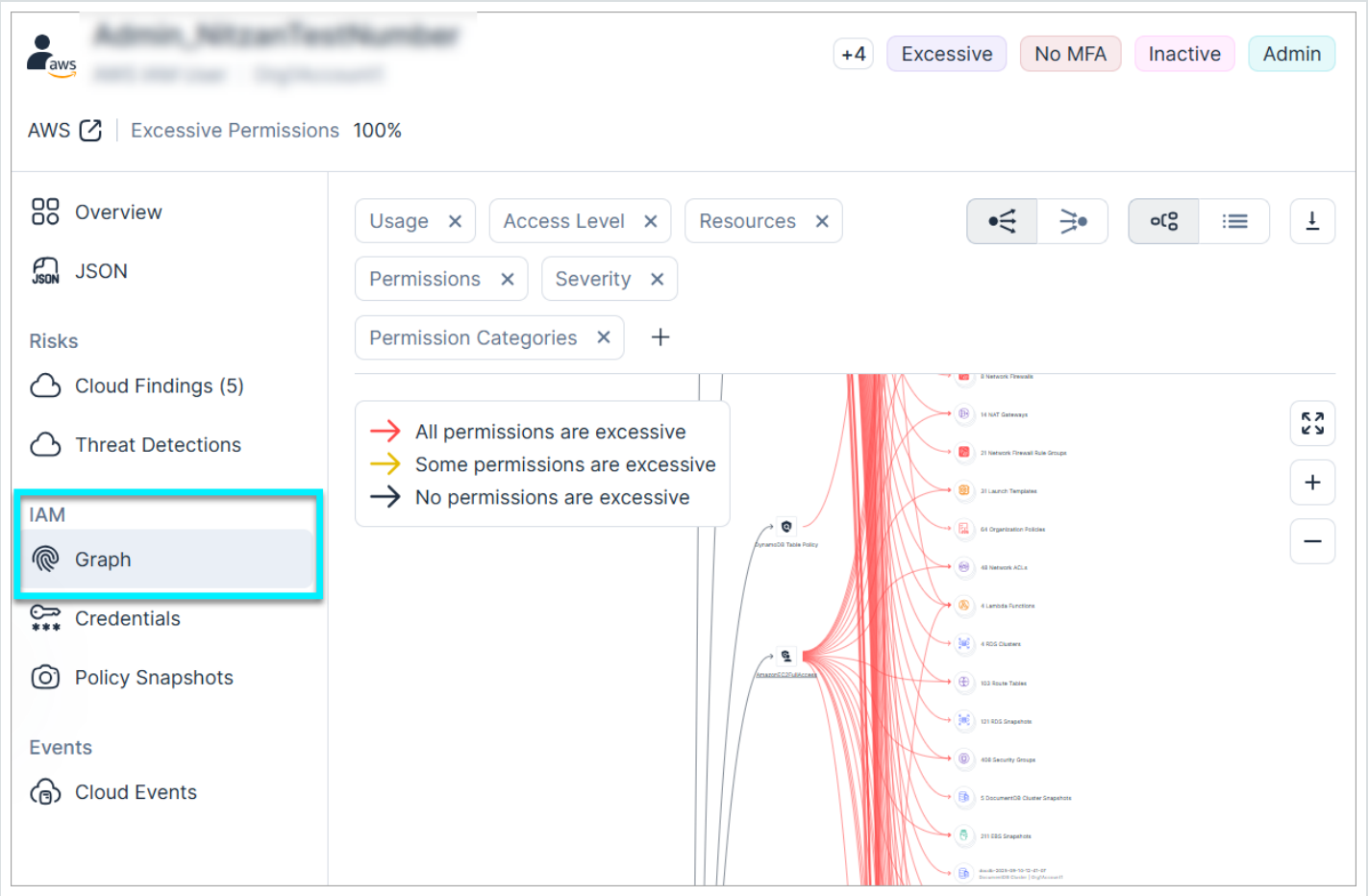
> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

リソースプロファイルビューで、**[IAM] > [グラフ]** タブをクリックし、特定のリソースに存在する権限マッピングを表示します。これは、オリジネータまたはアイデンティティとして動作するリソースが、(ポリシーで付与された

アクセス許可を通じて) 環境内のロールを引き受けて他のリソースにアクセスする方法をより詳しく理解するのに役立ちます。

たとえば、アクセス許可マッピングを使用して以下を実行できます。

- AWS の Azure AD ユーザーがアクセスできるすべてのリソースを視覚化
- 特定のリソースに付与された管理者のアクセス許可 (深刻度フィルター) を特定する
- データの読み取り/書き込みを行うアクセス許可を持つアイデンティを検索する (データの読み取り/書き込みカテゴリ)



過剰または使用されたアクセス許可

リソースへのアクセスを許可するアクセス許可は、次のいずれかです。

- **過剰な**。サービスやマシンのアイデンティティの場合は過去 90 日間、人間のアイデンティティの場合は 180 日間使用されなかったすべてのアクセス許可。
- **を使用しました**。特定のリソースで、あるアクションを実行するために使用されたアクセス許可。

重要: 権限は、関連する CSP からの **明示的なクラウドログ証拠** に基づくか、**暗黙的な証拠** (つまり、**Tenable One Cloud Exposure 権限が過剰である証拠を持たない**) のいずれかに基づいて、「使用済み」として決定されます。

監査されないアクセス許可

アクセス許可マップでは、Azure の ID が通常、アクセス許可とアクセス可能なリソースの間に黄色の接続線で表示され、「一部のアクセス許可が過剰」であることを示しています。

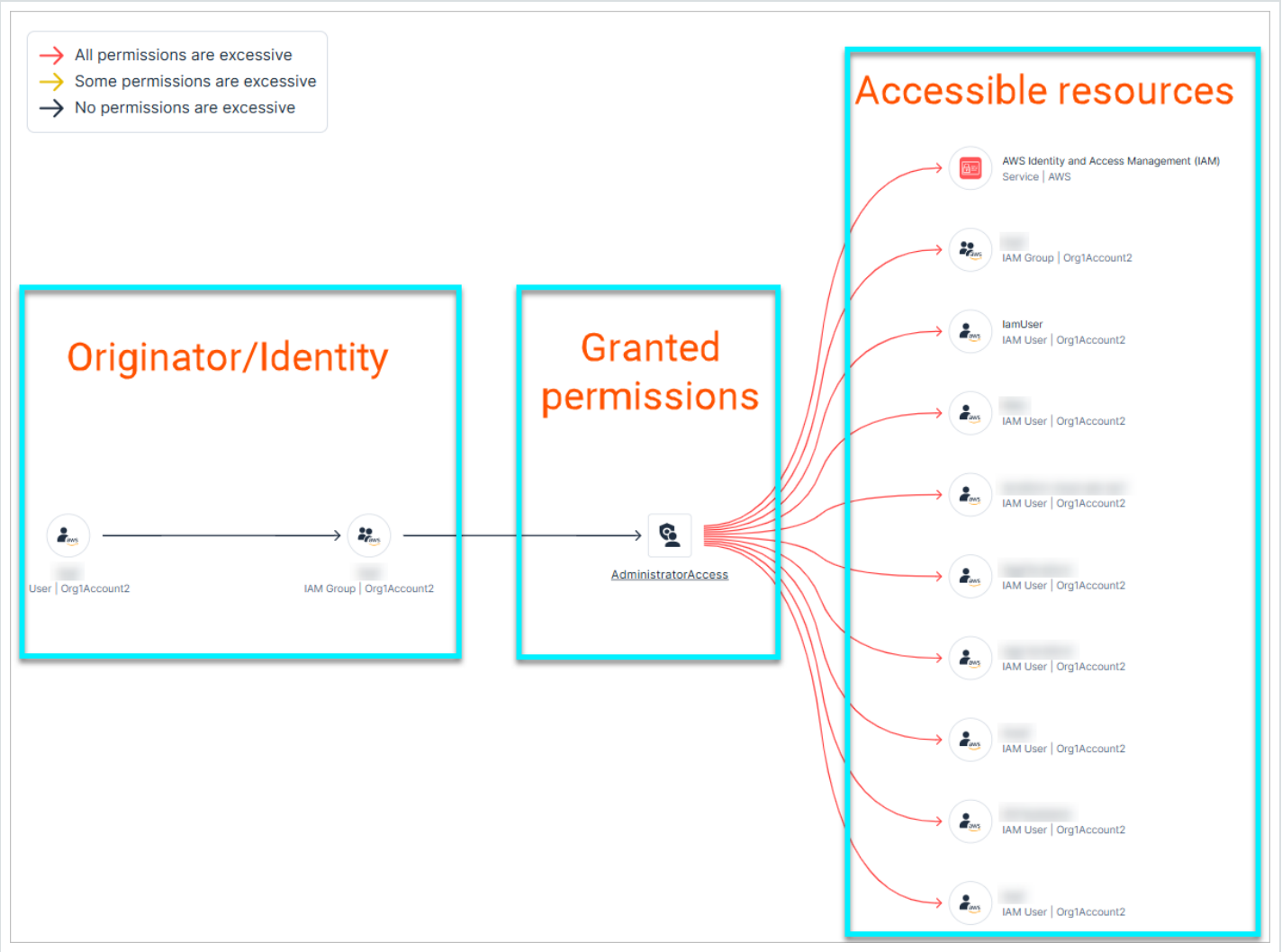
Azure では、読み取りアクセス許可は監査されません。結果として、黙示的な反証がない限り、クラウドサイバーエクスポージャーは読み取りのアクセス許可が使用されていると仮定します。これは、リソースに関連付けられている他の一部のアクセス許可 (読み取り、削除など) が過剰な場合でも、読み取りアクセス許可が存在することで「一部のアクセス許可が過剰」という全体的な関係に変換されることを意味します。これは通常、[データの読み取り] および [インフラの読み取り] カテゴリのアクセス許可に発生します。

これはまた、AWS の特定のアクセス許可にも当てはまり、AWS CloudTrail ではログに記録されません。たとえば、IAM PassRole アクセス許可 (このアクセス許可の監査の詳細については、当社のブログ投稿をご覧ください)

マップレイアウトと例

マップは次の 3 つの一般領域に分割されます。

- **オリジネータ/identity です**。アクセス許可が直接付与されているか、別のアイデンティティを引き継ぎ、その引き継いだアイデンティティのアクセス許可を使用して機能するクラウドアイデンティティ。
- **付与されているアクセス許可**。特定のアクティビティを実行するために、オリジネータやアイデンティティによって使用されているポリシーやロールまたはアクセス許可。
- **アクセス可能なリソース**.オリジネータやアイデンティティによってアクセスが可能なリソース。リソースへのアクセスを許可するアクセス許可は、過剰であるか、使用済みである可能性があります。



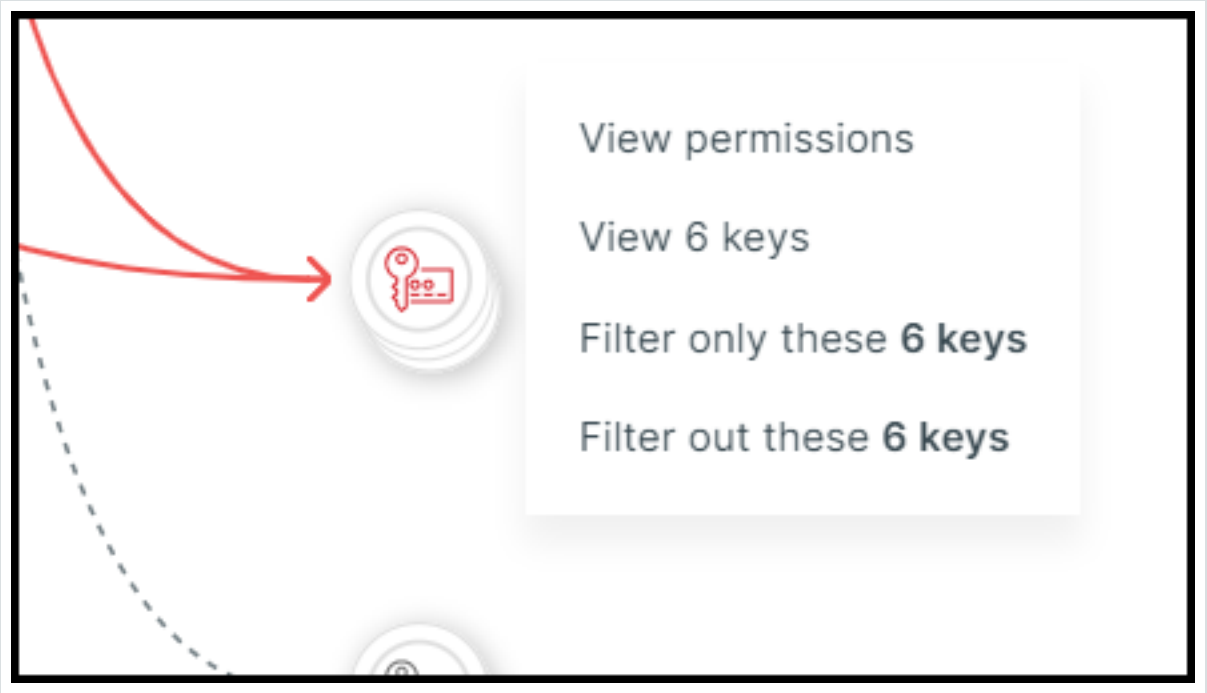
上記の例では、以下について確認できます。

- AWS ユーザー *オリジネータ*が IAM グループを引き受けました。
- このグループには、アクセス許可を付与する 1 つのポリシーがあります。
- ポリシーは、10 個のリソースにアクセスするアクセス許可をユーザーに付与します。
- 付与されるすべてのアクセス許可が過剰です。

マップの操作と使用

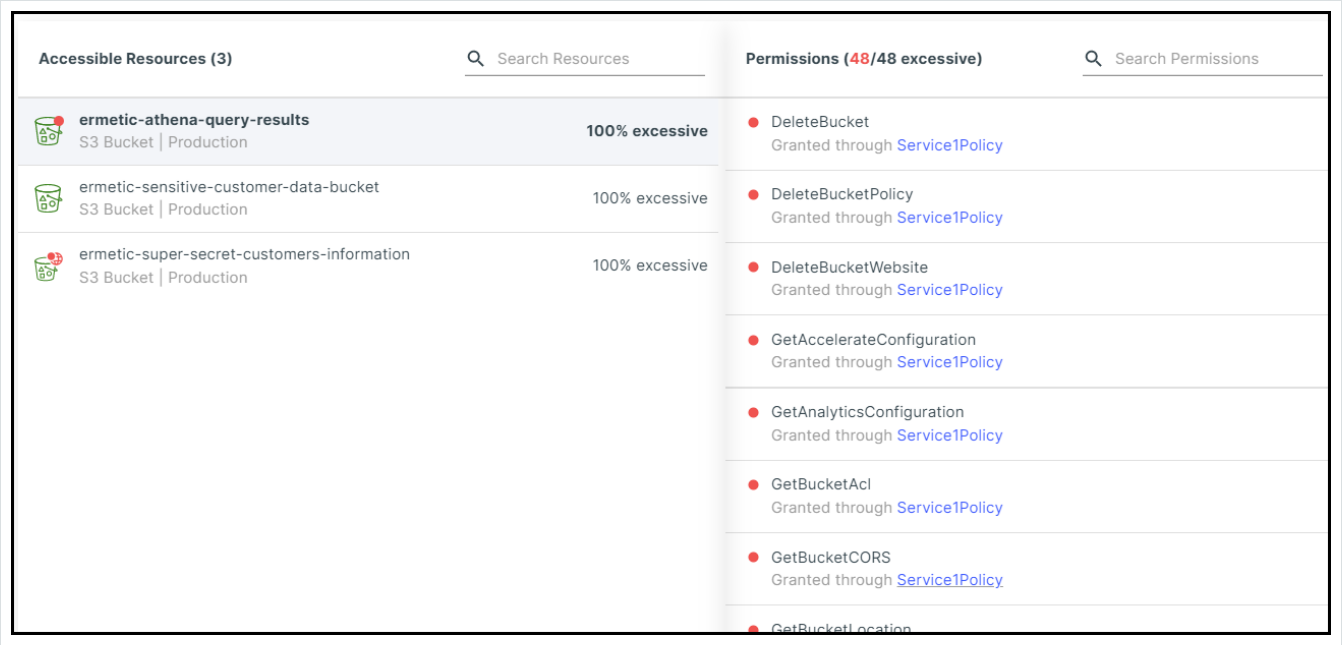
マップを操作し、アクセス許可やリソースに関する詳細を確認するには

1. マップ内を移動するには、マウスをクリックしてドラッグします。
2. マップを拡大および縮小するには、[Ctrl] キーを押しながらマウスウィールをスクロールします (またはマップをダブルクリックして拡大します)。 をクリックしてズームアウトし、マップ全体を表示
3. デフォルトでは、マップには、マップ内のすべてのリソースに関する過剰なアクセス許可のマッピングが表示されます。特定のアクセス許可またはリソースのアイコンをクリックすると、そのリソースのみに関する過剰なアクセス許可のマッピングに焦点が当てられます。
4. グラフ上のリソースに関する詳細を確認する、またはリソースに基づいてグラフをフィルタリングするには、リソースアイコンを右クリックします。使用できるアクション項目は、リソースタイプ、およびリソースが許可されているアクセス許可であるかアクセス可能なリソースであるかによって異なります。

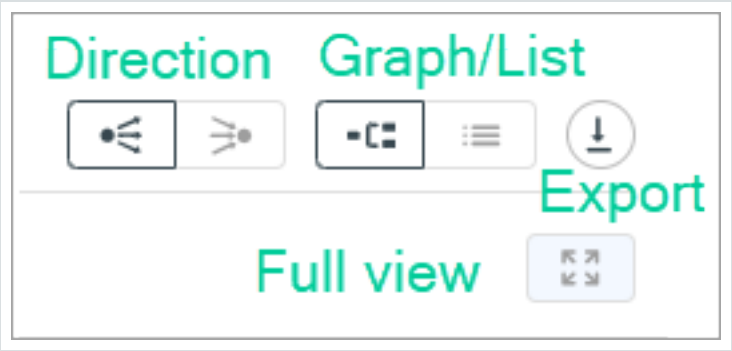


   - ほとんどの付与されているアクセス許可では、リソースインベントリページに移動したり、JSON形式でアクセス許可を表示したり、リソースに基づいてマップをフィルター処理したりできます。
   - ほとんどのアクセス可能なリソースについては、リソースインベントリページに移動したり、アクセス許可の全リストを表示したり、リソースに基づいてマップをフィルタリングしたりできます。
5. アクセス可能なリソースのアクセス許可の完全なリストを表示するには、リソースアイコンを右クリックし、**[アクセス許可の表示]** をクリックします。表示されたダイアログボックスで、アクセス可能なリソースをクリックするか検索することで、そのリソースに対するアクセス許可をすべて表示できます。各アク

セス許可の下に、アクセス許可を付与するメカニズム表示され、アクセスできます。



6. マップを絞り込むには、マップの上部にあるフィルターを使用します。使用可能なフィルターは特定のリソースによって異なりますが、すべてのリソースで表示される次のフィルターが含まれます。
    - **使用法**デフォルトでは、マップにはすべてのアクセス許可マッピングが表示されますが、過剰なアクセス許可のみを表示する、または使用済みのアクセス許可のみを表示するようにフィルターできます。
    - **アクセスレベル**。リソースまたはアイデンティティに付与するアクセスの範囲を定義します。アイデンティティとリソース間のアクセス範囲に基づいて、アクセス許可をフィルタリングできます。たとえば、「cross-account」(クロスアカウント) のアクセス許可のみを表示することができます。詳しくは、アクセスレベル参照してください。
    - **リソース**.クラウドサイバーエクスポージャーによってモニタリングされている特定のリソースをフィルタリングします。
    - リスク深刻度の色分け度たとえば、特定のリソースに付与されている管理者権限 (重大深刻度) を特定するには、このフィルターを使用します。
    - アクセス許可の分析とリスクレベル。たとえば、このフィルターを使用して、承認なしでデータを送信するアクセス許可 (データの読み取り / 書き込み) を持つリソースを特定します。
7. さまざまなマップオプションと追加のフィルターが、フィルターを介して、マップ右上にある



マップオプション	説明
追加のフィルター	リソースタイプに応じて、次のフィルターの 1 つ以上がここに表示される場合があります: • **クロスアカウント**。(AWS) 別のアカウントでロールを引き受けているあるアカウントからのリソースでフィルタリングします。<br br これにより、必要に応じて環境の安全な分離を特定し、維持することができます。たとえば、開発および生産環境。[デスティネーションアカウント] フィルターを使用してビューを絞り込むこともできます。<br br 特定の宛先アカウントにダウングレードします。 • **サードパーティの**。サードパーティのリソースをフィルタリングします。 • **外部**. (GCP) ワークスペースでローカルで定義されていない、外部 Google グループおよびユーザーを表示します。
フルビュー	ズームアウトしてマップ全体を表示します。
方向	デフォルトでは、選択したリソースがアクセスできるリソースがマップに示されます。後方にピボットし、マッピングを逆にして、選択したリソースにアクセスできるすべてのリソースを表示することもできます関連する場合。
グラフ/リストトグ	グラフ表示デフォルトとテキストベースのリスト表示の間でマップを切り替えます。

マップオプション	説明
ル	
エクスポート	外部ツールで処理するためにマップデータを CSV にエクスポートします。

アクセス許可を付与するメカニズム

次の表はクラウドサイバーエクスポージャー、のリソースに権限を付与するメカニズム/ポリシーを一覧表示しています。

CSP	メカニズム
AWS	アイデンティティベースのポリシー、サービスコントロールポリシー (SCP)、リソースコントロールポリシー (RCP) アクセス許可境界、リソースベースのポリシー、条件
Azure	RBAC、特権アイデンティティ管理 (PIM)、Key Vault アクセスポリシー、ストレージアカウントアクセスキー
GCP	RBAC、ACL、レガシーメカニズム (BigQuery、ストレージバケットなど)

アイデンティティインテリジェンス

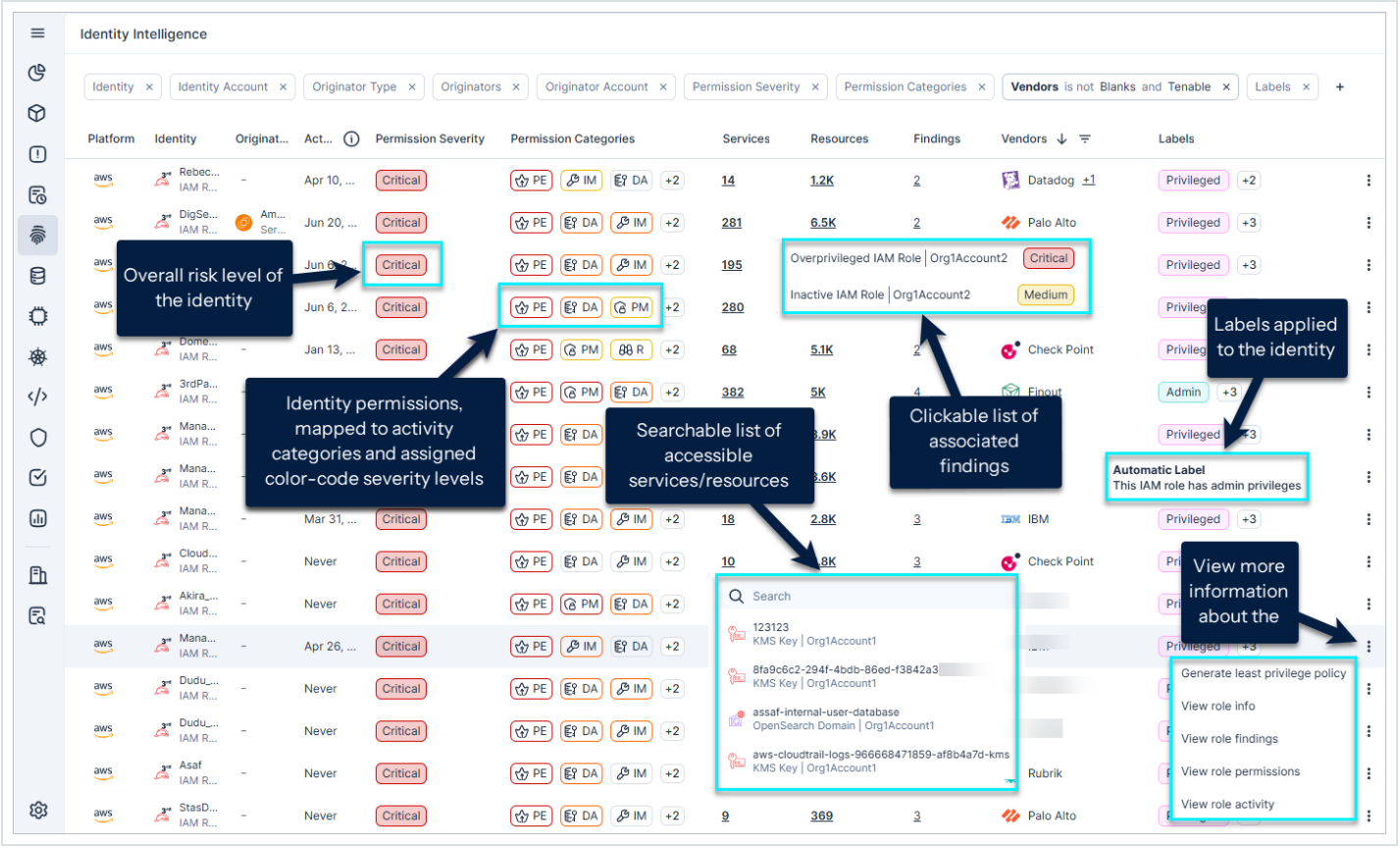
> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

アイデンティティがクラウド環境にもたらすリスクを調査し、評価します。Tenable One Cloud Exposure **ID インテリジェンスを**使用すると、ID の内訳を深刻度レベル別に表示し、ID とそれに関連付けられているアクセス許可を環境内の潜在的なリスクにマッピングできます。アイデンティティには、ユーザー、ロール、サービスアイデンティティ、サードパーティアイデンティティ、フェデレーションアイデンティティが含まれます。

環境内のアイデンティティを表示する

ID インテリジェンスページを使用して、環境内のアイデンティティに関する重要な情報を確認することができます。たとえば、次のことが可能です。

- 権限のあるサードパーティの ID をすべて表示します。
- アクセスキーが有効になっているが、多要素認証 (MFA) が有効になっていない管理者ユーザーを参照してください。



ID を表示するには

1. クラウドサイバーエクスポージャーコンソールで、**[調査]** > **[IAM]** > **[アイデンティティインテリジェンス]** をクリックします。
2. ページの上部にあるアイデンティティウィジェットをスキャンして、すべてのアイデンティティにわたるリスク深刻度レベル、および特定のタイプのアイデンティティ(ユーザー、サービスアイデンティティ、フェデレーションアイデンティティ、サードパーティアイデンティティ) にわたるリスク深刻度レベルの分布を確認します。

3. テーブルのデータのフィルタリング 、表示されるデータの範囲を変更します。たとえば、組み込みシステムラベルで、**サードパーティ**を選択すると、サードパーティの ID が表示されるようフィルタリングできます。テーブルで利用可能なデータについては、ID 列データ 参照してください。
4. アイデンティティが環境にもたらすリスクを分析します。アクセス許可の分析とリスクレベルを参照してください。
5. リソースの詳細の表示 アイデンティティに関する詳細な情報を表示します。

ID 列データ

[アイデンティティインテリジェンス] ページの表に次の列が表示されます。

縦棒	説明
プラットフォーム	アイデンティティが属するクラウドサービスプロバイダー。
アイデンティティ	アイデンティティの名前名前の下には、リソースのタイプとアカウント名が表示されます。
オリジネータ	クラウド ID (IAM ユーザー / ロール、IdP ユーザー、またはコンピューティングリソース) は、アクセス許可を直接付与されるのではなく、問題の ID を推測し、推測したアイデンティティのアクセス許可を使用して実行することができます。たとえば、マネージド ID を使用してアクティビティを実行する Azure 仮想マシンや、アクションを実行するために AWS で IAM ロールを引き受ける Azure AD ユーザーなどがあります。
アクティビティ日	アイデンティティによって実行された最後のアクティビティ詳しくは、よくある質問を 参照してください。
アクセス許可の深刻度	アイデンティティに割り当てられている最も高い深刻度のアクセス許可のリスクの深刻度レベル。詳細については、アクセス許可の分析とリスクレベル 参照してください。
アクセス	各アクセス許可カテゴリのリスクの深刻度レベルに関する色分けされた内訳詳細につい

縦棒	説明
許可カテゴリ	ては、アクセス許可の分析とリスクレベル参照してください。
サービス	アイデンティティがアクセス可能なサービスの数数字をクリックすると、サービスについて検索可能なリストが表示されます。
リソース	アイデンティティがアクセスできるリソースの数数字をクリックすると、リソースについて検索可能なリストが表示されます。
ベンダー	ベンダーごとのサードパーティの識別
検出結果	アイデンティティに関連する検出結果の数。数字をクリックすると、検出結果について検索可能なリストが表示されます。
ラベル	手動で適用されたか、タグに基づいて自動で適用されたか、システムによって適用されたかにかかわらず、アイデンティティに適用されているすべてのラベルが表示されます。ラベルのタグにカーソルを合わせると、詳細を確認できます。リソースに複数のラベルがある場合、アイコンをクリックするとその他のラベルが表示されます。詳細については、ラベルのリソースへの適用 参照してください。
:を設定します	• **最小権限ポリシーの生成**: ユーザーがタスクを実行するために必要な最小権限を付与するために、オンデマンドの AWS: 最小権限ポリシーの生成 を生成します。AWS ポリシーで利用可能です。 • **最小権限のカスタムロールを生成**: オンデマンドの Azure および GCP の最小権限カスタムロールを生成して、ユーザーがタスクを実行するために必要な最小権限を付与します。Azure ロールと GCP ロールで利用可能です。 • **管理されたアイデンティティ情報を表示する**: アイデンティティの リソースの詳細の表示 を開きます。 • **管理されたアイデンティティの検出結果を表示する**: そのアイデンティティに関連付けられているすべての検出結果を表示します。

縦棒	説明
	• **管理されたアイデンティティのアクセス許可の表示**: アイデンティティの アクセス許可マッピングの視覚化 を表示します。 • **管理されたアイデンティティアクティビティを表示する**: アイデンティティの リソースアクティビティの調査 を開きます。

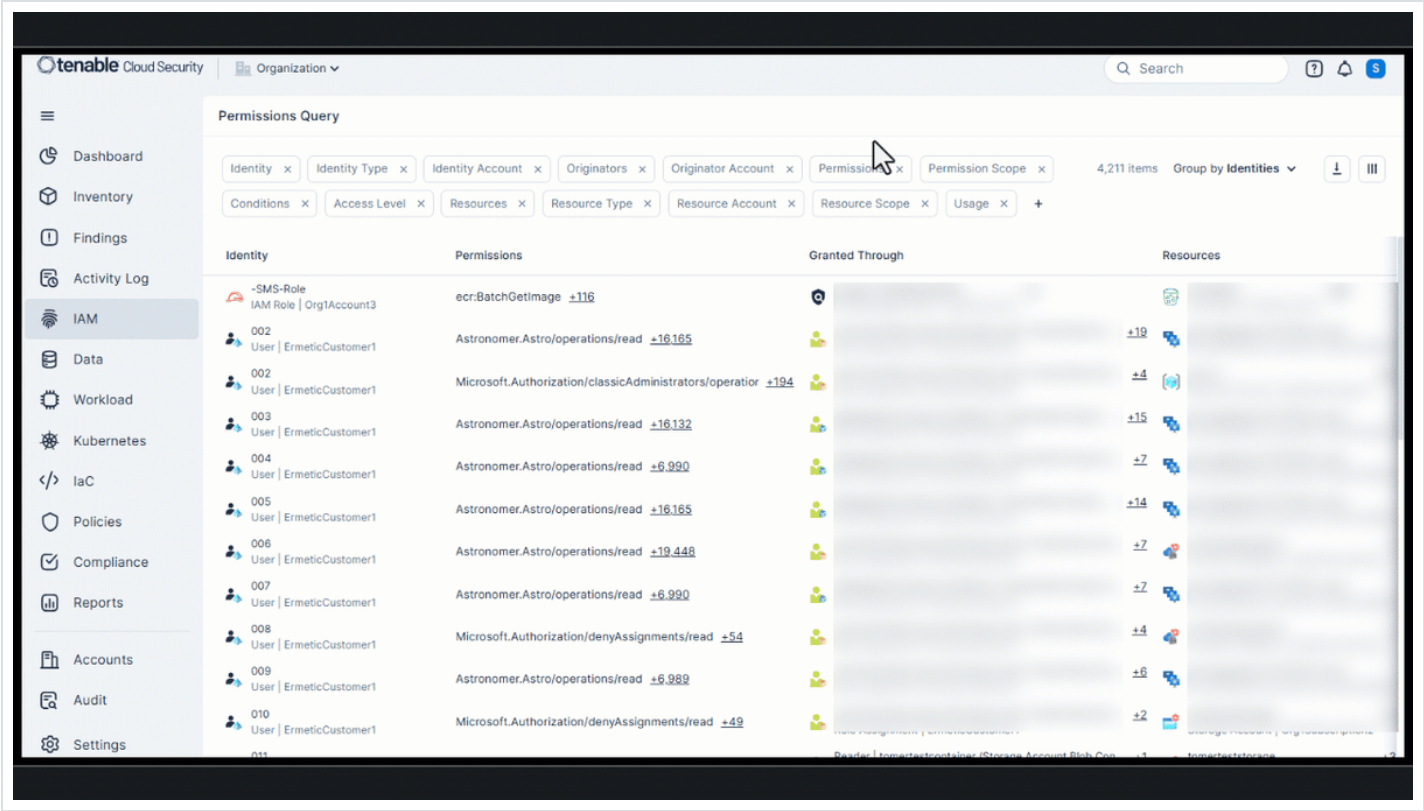
アクセス許可クエリ

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

すべてのクラウドアイデンティティにわたって柔軟で詳細なクエリを実行し、付与されているアクセス許可に関連する重要な問題を迅速に明らかにします。広範で直感的なフィルターにより、探している対象を迅速かつ簡単に見つけることができます。特定のクエリを実行すると、アイデンティティのオリジネータ、関連するアクセス許可、アイデンティティがアクセスできるリソースなど、関連するさまざまなコンテキスト情報を表示できます。

たとえば、次を検索できます。

- 無制限のリソーススコープを持つ、本番アカウントでアクセス許可を持つ非本番アカウントのアイデンティティ。
- 特定のアイデンティティがオブジェクトを削除するアクセス許可を持つストレージバケット。
- 特定のリソース ID に対するデータ読み取りアクセス許可を持つユーザーを特定します。

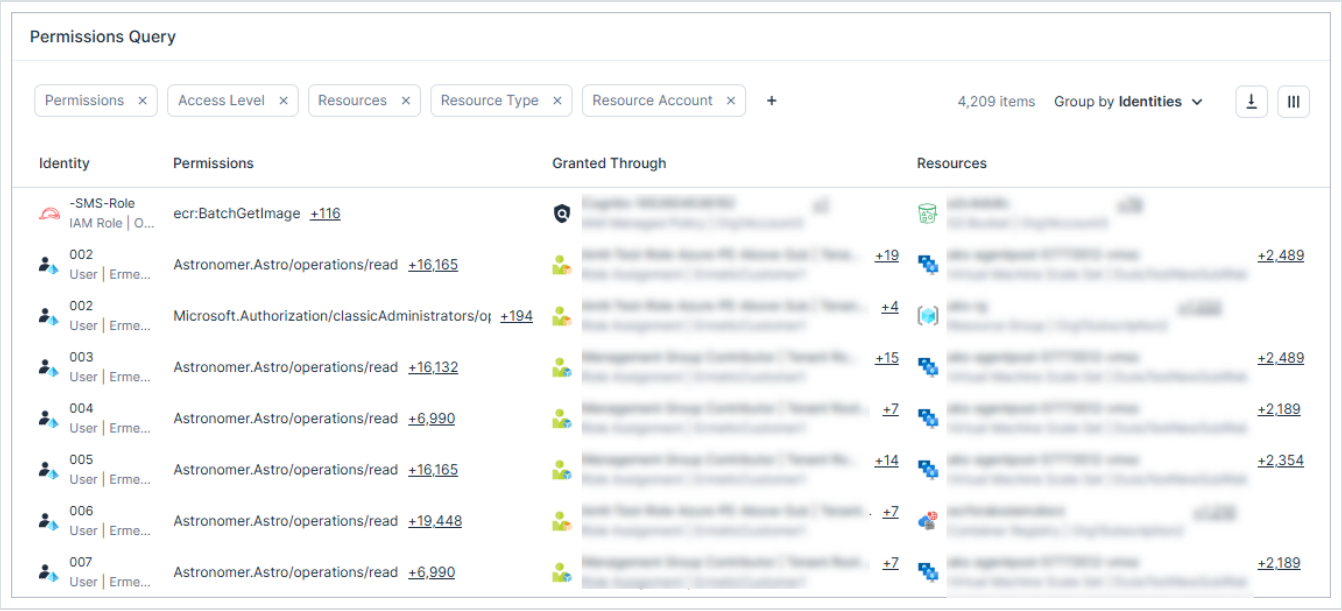


アクセス許可クエリの実行

注意: API 経由でクエリを実行する方法については、API 例のドキュメントの すべてのアイデンティにまたがるクエリのアクセス許可を 参照してください。

アクセス許可をクエリするには

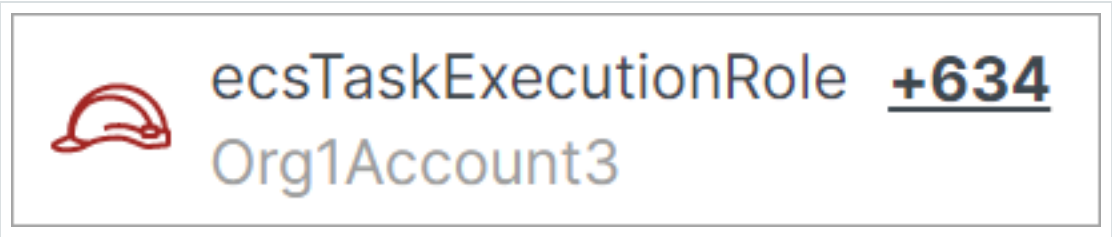
1. Tenable One Cloud Exposure コンソールで、**[調査]** > **[IAM]** > **[アクセス許可クエリ]** をクリックします。



2. [アイデンティティ] または [リソース] **でグループ化** するかどうかを選択すると、検索のフォーカスをアイデンティティからリソースにピボットできます。
3. テーブル内のデータをフィルタリングし、表示可能なデータの範囲を変更します。テーブルで使用可能なデータに関する詳細については、アクセス許可クエリのテーブルのフィールドを参照してください。たとえば、いくつかの特定のユースケースに対処したり、お客様の環境に関連性の高いクエリのヒントを与えたりする可能性のある、いくつかのサンプルクエリを以下に示します。
    - アイデンティティタイプ: `IAM Role` ;権限 `s3:GetObject` ;リソーススコープ `All resources`
    - アイデンティティタイプ: `IAM User` ;アイデンティティラベル `No MFA` 。権限カテゴリ: `Data Read` ; リソーススコープ `All resources`
    - 権限カテゴリ: `Data Read` ;リソースラベル `PII/Highly Confidential`インベントリ(プロパティとラベル)
    - アクセス許可サービス別 : `Amazon API Gateway` ;条件 `Without`
    - アイデンティティタイプ: `Managed Identity`;アクセスレベル: `Cross Account`

    クラウドサイバーエクスポージャーでのデータのフィルタリングに関する詳細については、データのフィルタリング参照してください。
4. 一部のアイデンティティには、複数のリソースまたはポリシーが関連付けられている場合があります。エントリの横にある数字をクリックして、関連するすべてのエンティティの検索可能なリストを表示しま

す。



5. リソースの詳細の表示 それに関する詳細な情報を表示します。
6. クエリデータをエクスポートするには、表の右上にある **[エクスポート]** ボタンをクリックします。データは、テーブルに適用されている現在のフィルターに従ってエクスポートされます。複数のエントリがある項目の場合、エクスポートされるファイルには最大で 100 のエントリが表示されます。

アクセス許可クエリのテーブルのフィールド

次のフィールドを使用して、アクセス許可クエリページの表のデータをフィルタリングできます。

縦棒	説明
アイデンティティ	アイデンティティの名前名前の下には、リソースのタイプとアカウント名が表示されます。
アイデンティティタイプ	アイデンティティのタイプ
アイデンティティアカウント	そのアイデンティティが属するアカウント。
アイデンティティラベル	手動で、タグに基づいて自動で、またはシステムによって適用されたかに関わらず、クラウドサイバーエクスポージャーのアイデンティティに適用されるラベルです。詳細については、ラベルのリソースへの適用 参照してください。

縦棒	説明
オリジネータ	クラウド ID (IAM ユーザー / ロール、IdP ユーザー、またはコンピューティングリソース) は、アクセス許可を直接付与されるのではなく、問題の ID を推測し、推測したアイデンティティのアクセス許可を使用して実行することができます。たとえば、マネージド ID を使用してアクティビティを実行する Azure 仮想マシンや、アクションを実行するために AWS で IAM ロールを引き受ける Azure AD ユーザーなどがあります。
オリジネータアカウント	が オリジネータ 所属するアカウント 。
オリジネータタイプ	の オリジネータリソースカテゴリ。
アクセス許可	アイデンティティに付与されているすべてのアクセス許可のリスト。これにより、特定のリソースにアクセスできます。テーブルに複数のアクセス許可がある場合、エントリの横にある数字をクリックすると、すべてのアクセス許可について検索可能なリストが表示されます。
アクセス許可 (サービス別)	サービスによって表のアクセス許可をフィルタリングします。たとえば、条件のないアイデンティティに付与されたすべての API ゲートウェイサービスのアクセス許可を検索できます。
アクセス許可範囲	ポリシー経由でアイデンティティに付与されたアクション / アクセス許可の範囲: • **すべてのアクション**: 特定のサービスのすべてのアクションへのアクセス権を付与するために使用されるワイルドカード (*)。 • **アクションパターン**: 特定のサービスの指定されたパターンに一致するアクションへのアクセス権を与えるために、アクション名の一部として使用されるワイルドカード (*)。 • **特定のアクション**: サービスの特定のアクションへのアクセス権を付与するために使

縦棒	説明
	用される個別の値 ( )
アクセス許可カテゴリ	クラウドアイデンティティに共通の広範囲の動作パターンを反映する、アクセス許可 / のアクティビティカテゴリ。詳細については、アクセス許可の分析とリスクレベル参照してください。
リソース	アイデンティティがアクセスできるすべてのリソースのリストテーブルに複数のリソースがある場合、エントリの横にある数字をクリックすると、すべてのリソースについて検索可能なリストが表示されます。
IAM アクセス	リソースに付与されるアクセスの範囲。可能な値： • **公開** • **外部** • **クロスアカウント** • **信頼できる外部** • **内部** 各値の定義は、クラウドプロバイダーによって異なります。詳しくは、[アクセスレベル] を参照してください。
リソースタイプ	リソースのリソースカテゴリ。
リソースアカウント	リソースが属するアカウント。
リソースタグ	クラウドサービスプロバイダープラットフォームでリソースに割り当てられたタグ。各タグは、ユーザー定義のキーと値で構成されるラベルです。
リソース	クラウドサイバーエクスポージャーのリソースに適用されるラベル (手動で、タグに基づいて

縦棒	説明
ラベル	自動で適用されるか、システムによって適用されるか)。詳細については、ラベルのリソースへの適用 参照してください。
リソース範囲	ポリシーで定義された、アイデンティティがアクセスできるリソースの範囲: • **すべてのリソース**: 特定のサービスのすべてのリソースをカバーするために使用されるワイルドカード (*)。 • **リソースのグループ**: 特定のサービスの指定されたパターンに一致するリソースを定義するために、ARN セグメントの一部として使用されるワイルドカード (*)。 • **特定のリソース**: サービスの特定のリソースを定義するために使用される個別の値 / 。
使用ガイドライン	• **すべての** • **未使用 (過剰)** • **使用済み** 詳細については、過剰なアクセス許可を参照してください。
付与元	そのアイデンティティにアクセス許可を付与するすべてのポリシーのリスト。テーブルに複数のポリシーがある場合、エントリの横にある数字をクリックすると、すべてのポリシーについて検索可能なリストが表示されます。
条件	ポリシーに、ポリシーが有効になるタイミングを指定する条件が含まれているかどうか。たとえば、`AssumeRole` のような機密度の高いアクセス許可は、条件なしで付与される場合があります。

AWS フェデレーションのアクセス許可

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

AWS サービスにアクセスするために、他の IdP からフェデレーションされ、IAM ロールが付与されたすべてのユーザーを表示します。これにより、全体的なクラウド間のセキュリティポスチャーをより適切に把握し、不要なロールやロール割り当てを削除できるようになります。

GraphQL API 経由で Workload Protection データにプログラムでアクセスすることもできます。

AWS フェデレーションのアクセス許可を表示する方法

1. Tenable One Cloud Exposure コンソールで、**[調査]** > **[IAM]** > **[AWS フェデレーションアクセス許可]** をクリックします。
2. テーブルのデータのフィルタリング、表示されるデータの範囲を変更します。たとえば、**[ロールラベル]** で、**[管理者]** を選択して、AWS の管理者権限が割り当てられたフェデレーションアイデンティティを表示するようフィルタリングできます。テーブルで利用可能なデータについては、ID 列データを参照してください。
3. リソースの詳細の表示 アイデンティティに関する詳細な情報を表示します。
4. 表示されているすべての列データを CSV に**エクスポートします** 。

AWS フェデレーションアクセス許可列データ

[AWS フェデレーションアクセス許可] ページの表に、次の列が表示されます。

縦棒	説明
AWS フェデレーションアクセス許可	フェデレーションユーザーを AWS にマッピングします。
ユーザー	フェデレーションユーザーの名前
ロール	割り当てられた AWS IAM ロールの名前。
フェデレーションタイプ	ユーザーが AWS にフェデレーションされる方法 可能な値 • **レガシー** (正規 SAML/OIDC)

縦棒	説明
	• **AWS Identity Center** (AWS SSO の後継)
AssumeRole 時間	ユーザーが最後にロールを引き受けた日時。 可能な値: • 最後アクティビティの日付 • より前の最終アクティビティの日付 より前の • **日付 不明**: 関連するデータがあり • **ません** ロールが利用可能な最も早いイベントデータより前に作成された場合、「より前のアクティビティの日付より前」は表示されません。この状況の場合、Tenable では、初期期間中にそのロールが引き受けられたかどうかを確認できません。
未使用	フェデレーションは、分析期間にトリガーされる場合には使用されません。詳細は、過剰なアクセス許可 を参照してください。
割り当て先グループ	ユーザーにロールを付与するグループの名前。
初回確認時刻	Tenable が最初にフェデレーションアクセス許可を検出した時刻。アカウント統合前にアクセス許可が作成された場合、接続時間が反映されます。 可能な値: • 初回確認日
オリジネータユーザー	ユーザーがオリジンであるかどうかを示します。詳細については、アクセス許可クエリのテーブルのフィールドを参照してください。

ネットワークエンドポイント

このセクションでは、ネットワークエンドポイントの詳細な概要について説明します。

- ネットワークエクスポージャーとネットワークエンドポイントの概要については、「ネットワークのエクスポージャー」を参照してください。
- スキャン設定を構成するには、「ネットワークスキャナー」を参照してください。
- よくある質問については、「FAQ: ネットワーク」を参照してください。

ネットワークエンドポイントは、ネットワーク評価によってフラグが立てられたリソースが、ネットワークネットワークスキャナーを介してインターネットから実際に到達できることをTenable One Cloud Exposureが確認したときに作成されます。

各ネットワークエンドポイントは、宛先ホスト (IP アドレスまたは DNS 名) とポートの一意の組み合わせを表します。エンドポイントは接続の試行が成功した場合にのみ作成されるため、リソースが設定で公開されるだけでなく、外部から到達可能であることを示す信頼性の高い証拠を提供します。

サポートされているコンピューティングリソースの場合、確認済みの HTTP エンドポイントと HTTPS エンドポイントにはアプリケーション層データも含まれます。これには、HTTP ステータスコード、SSL/TLS プロトコルバージョン、ランディングページのスクリーンショット、HTML レスポンスが含まれます。詳細は、ネットワークスキャナー。

次の点に注意してください。

- エンドポイントは、IP アドレスとポートを持つ直接リソースに対してのみ作成されます。
- 最新のスキャン結果のみが表示されます。ネットワークエンドポイントは履歴に保存されません。
- ネットワークエンドポイントは検出結果ではありません。外部からの実際の到達可能性を確認するスキャン結果です。

ネットワークエンドポイントの確認

[ネットワークエンドポイント] ページには、ネットワーク評価によってフラグが立てられたリソースが一覧表示され、ネットワークスキャンにより外部アクセスへの露出が確認されたかどうかが表示されます。

このビューでは、どのリソースが実際に公開されているか、どのリソースが設定のみの公開であるかを確認できます。

縦棒	説明
ネットワークエンドポイント	プロトコルプレフィックスを含む、確認されたエンドポイントの完全な URL (例: `https://10.0.0.5:443`)。
リソース	エンドポイントに関連付けられているクラウドリソース。
タイプ	リソースタイプ (例: EC2 インスタンス)。
HTTP メソッド	アプリケーションレイヤーのスキャン中に使用される HTTP メソッド (現在は GET)。
HTTP ステータス	リソースによって返される HTTP ステータスコード (例: `200`、`301`、`403`)。
プロトコル	テストされたプロトコル (現在 HTTPS または HTTP)。
ウェブページタイトル	アプリケーションレイヤーのスキャン中にキャプチャされた、ランディングページの HTML ページタイトル。
リダイレクトカウント	最終エンドポイントに到達するまでにたどった HTTP リダイレクトの数。
SSL/TLS プロトコル	接続中にネゴシエートされた SSL/TLS プロトコルのバージョン (例: TLS 1.3)。
SSL/TLS暗号スイート	接続中にネゴシエートされた暗号スイート (例: TLS_AES_128_GCM_SHA256)。
ネットワークスキャン時間	最新スキャンのタイムスタンプ。
ホスト	エンドポイントの IP アドレスまたはホスト名。
ポート	テストされたポート。
ソース IP アドレス範囲	ネットワークルールで定義されているように、リソースにアクセスできるソース IP 範囲。

注意:

- 追加の列を使用できますが、デフォルトビューでは非表示になります。これらには、証明書フィールド、およびアカウント、リージョン、タグなどのリソースプロパティが含まれます。
- HTTP メソッド、HTTP ステータス、SSL/TLS 情報、およびスクリーンショット列は、HTTP エンドポイントと HTTPS エンドポイントで ネットワークのエクスポージャー に対してのみ入力されます。

データリソース

注意: この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

これは、データリソースの表示と管理に関するハウツーガイドです。

- データ保護機能の概念の概要については、「 データ保護を参照してください。
- コンテナレジストリの設定を構成するには、「 Container Registry Settings」を参照してください。
- よくある質問については、「FAQ: データ保護 」 を参照してください。

クラウドリソースで検出されたデータを特定して評価することで、データの機密レベルと文脈を理解し、業界標準に準拠できます。

すべてのデータリソースを表示する

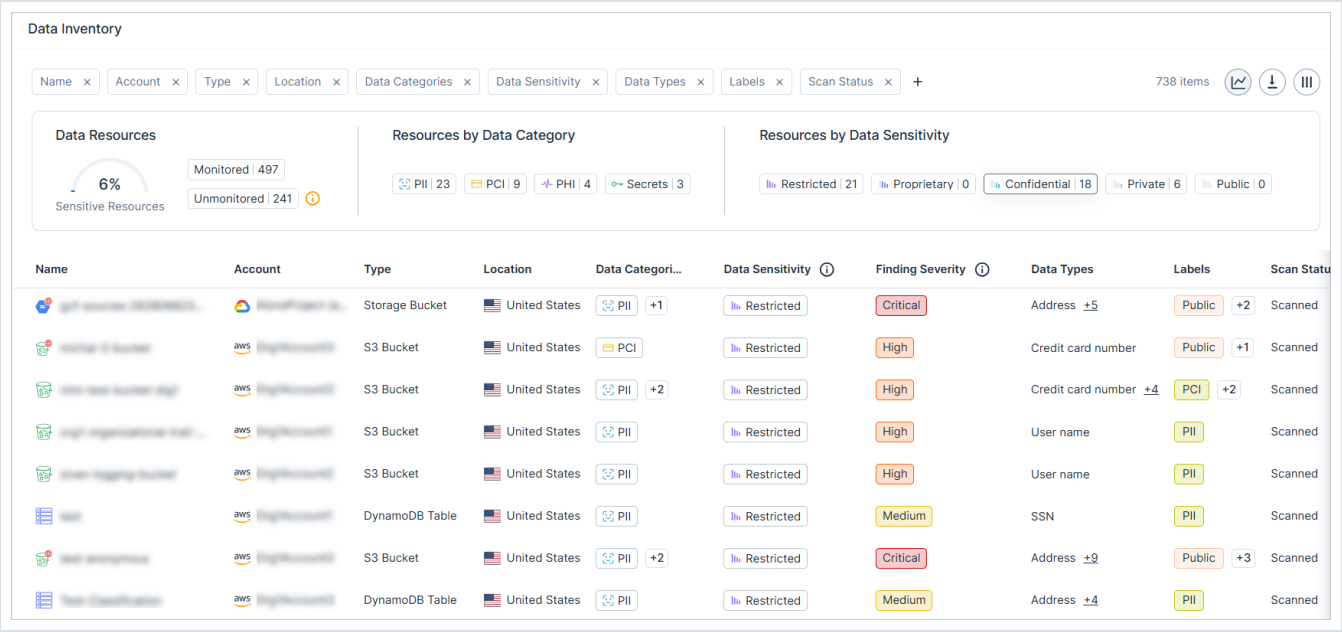
[データインベントリ] ページを使用すると、すべてのデータリソースを 1 か所で簡単に確認し、管理できます。

たとえば、次の内容を表示できます。

- PII データを含むスキャンされたリソース
- [Restricted] (制限付き) に分類されたデータを含むスキャンされたリソース
- 必要なアクセス許可を Tenable に付与しなかったためにスキャンされなかったリソース。

すべてのデータリソースを表示する方法

1. Tenable One Cloud Exposure コンソールで、左側のメニューから **[調査]** > **[データリソース]** をクリックします。



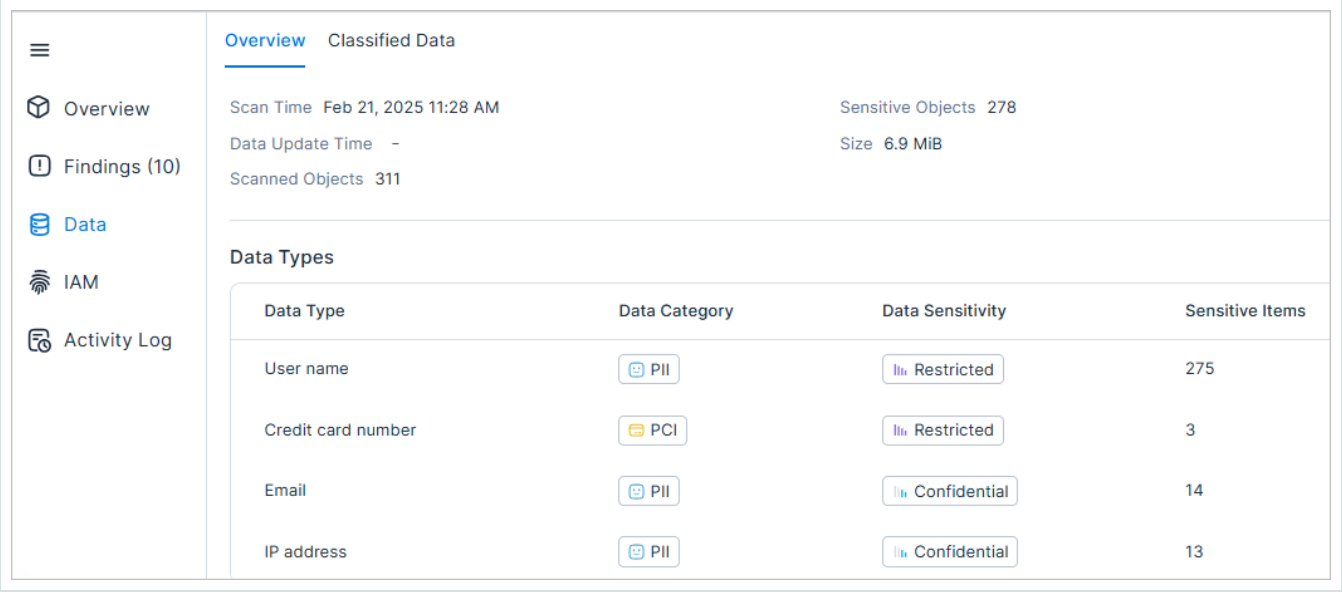
2. クイックフィルターウィジェットを使用して、環境内の機密性の高いデータリソースを特定します。以下に例を挙げます。

   - 監視対象リソースでフィルタリングします。

     > **注意:**
     > - [監視対象] は、データ分析が利用可能で、リソースがすでにスキャンされているか、スキャンされるのを待っていることを意味します。
     > - 監視されていない は、スキャンが無効になっているか、スキャンが何らかの理由で失敗しているために、リソースのデータ分析が利用できないことを意味します。

   - [Data Category] (データカテゴリ) フィルターを使用して、スキャンされた財務データを含むリソースを表示します。
   - [Data Sensitivity] (データの機密度) フィルターを使用して、[Restricted] (制限付き) または [Confidential] (社外秘)の深刻度を持つデータカテゴリに属しているスキャン対象データを含むリソースを表示する。

3. データインベントリの列データフィルタリングして、表示するデータの範囲を細かく調整します。以下に例を挙げます。
4. リソースをクリックし、Data **[データ]** タブをクリックします。



5. **[概要]** タブを使用すると、リソースで検出されたオブジェクトの概要をデータタイプ別の内訳とともに表示できます。詳細については、データ概要の列データを参照してください。
6. **[Classified Data]** タブを使用すると、特定のデータタイプについて検出されたオブジェクトの詳細リストを確認できます。詳細については、「機密データの列データ」を参照してください。
    - データをフィルタリングして、表示するデータの範囲を細かく調整します。
    - 表データをエクスポートする
    - 番号にカーソルを合わせて、検出された機密データの **サンプル** を表示します。

データインベントリの列データ

縦棒	説明
名前	リソース名。
アカウント	リソースが存在するクラウドアカウント。
タイプ	スキャンされたリソースのタイプ。完全なリストについては、スキャン対象リソースタイプを参照してください。
Location	スキャンされたリソースが存在する場所。

縦棒	説明
データタイプ	リソースで検出された機密性の高いデータタイプ。完全なリストについては スキャン対象データタイプ 。
データカテゴリ	リソースで検出された機密性の高いデータタイプにマッピングされるデータカテゴリ。
データの機密性	すべてのスキャン対象データから検出された最も高い機密レベル。詳細については、「 感度レベル を参照してください。
データスキャンステータス	リソースが正常にスキャンされたかどうかを示します。リソースがスキャンされなかった理由を示します。詳細については、「 スキャンステータス」を参照してください。
データスキャンステータスの理由	リソースのデータスキャンステータスの背後にある特定の理由 (アクセス許可がない、サポートされていない設定など) を示します。列はデフォルトでは非表示になっており、列セレクタから有効にすることができます。
検出結果の深刻度	リソースに関連付けられたすべての検出結果の中で最も高い深刻度レベル。
作成日	クラウドプロバイダー環境でリソースが作成された日付。
タグ	クラウドサービスプロバイダーのプラットフォームのリソースに割り当てられたタグ。各タグは、ユーザー定義のキーと値で構成されるラベルです。
ラベル	手動による適用、タグに基づく自動適用、システムによる適用のいずれかにかかわらず、リソースに適用された ラベルのリソースへの適用 が表示されます。ラベルのタグにカーソルを合わせると、詳細を確認できます。リソースに複数のラベルがある場合、アイコンをクリックするとその他のラベルが表示されます。
データスキャン時間	前回 クラウドサイバーエクスポージャー がリソースをスキャンした時刻を示すタイムスタンプ。リソースがまだスキャンされていない場合、値はダッシュ (-) になります。
データ読み	アクセス許可カテゴリごとのすべてのアクセスパスにわたる、プリンシパルからリソースへ

縦棒	説明
取りアクセスレベル	の最高アクセスレベル(内部からパブリック)を表します。詳細については、こちらのアクセスレベルを参照してください。
データ書き込みアクセスレベル	アクセス許可カテゴリごとのすべてのアクセスパスにわたる、プリンシパルからリソースへの最高アクセスレベル(内部からパブリック)を表します。詳細については、こちらのアクセスレベルを参照してください。

データスキャンステータス

[データスキャンステータス]列には、マシンの現在のスキャンステータスが表示されます。以下の表は、ステータスの種類と、そのステータスが表示される理由を示しています。理由は通常、ツールチップとしてステータスの横に表示されます。

スキャンステータス	Reasons
無効	このリソースのデータ分析は無効になっています。詳細については、「Configure Data Scanning Settings」を参照してください。
	リソースはデータスキャンから除外されています。詳細については、データ。
	プライベートバケットのデータ分析が無効です。詳細については、データを参照してください。
	プライベートネットワークアクセスを必要とするリソースに対してはデータ分析が無効です。詳細については、「データを参照してください。
失敗	データ保護のアクセス許可がないため、データ分析スキャンを完了できませんでした。詳細については、「Configure Data Scanning Settings」を参照してください。

スキャンステータス	Reasons
	ネットワーク制限により、データ分析スキャンを完了できませんでした。
	内部的な理由により、データ分析スキャンが失敗しました。
サポート対象外	データ分析は、リソースのサービス/ストレージレベルではサポートされていません。サポートされている GCP SQL インスタンスのデータベースエンジンバージョンおよびサポートされている OCI オブジェクトストレージバケットでサポートされている設定を参照してください。
	データ分析は、このリソースアーキテクチャではサポートされていません。「サポートされている設定」を参照してください。
	リソース設定がロックされているため、このリソースのデータ分析はサポート対象外です。「サポートされている設定」を参照してください。
	データ分析は、その構成により、このリソースではサポートされていません。「サポートされている設定」を参照してください。
	永続的または永続的なオプションの基礎となる設定のため、このリソースのデータ分析はサポート対象外です。「サポートされている設定」を参照してください。
	データ分析は、このリソースエンジンおよび/またはバージョンではサポートされていません。「サポートされている設定」を参照してください。
	RDS (Aurora) クラスタ内のリソースは個別にスキャンできません。RDS クラスタ全体をスキャンするか、スタンドアロンの RDS インスタンスをスキャンすることができます。
	データ暗号化にカスタマーマネージドキー (CMK) を使用するリソースはスキャンできません。
	データリソースのアカウント内スキャン内のリソースはスキャンできません。

スキャンステータス	Reasons
	データ分析は、大きなリソースではサポートされていません。
保留中	リソースはスキャン待ちです。これは、リソースが一度もスキャンされていない場合や、スキャンされていても定期スキャンのために再びマークされている場合に表示されます。
	このレルムはスキャンではサポートされていません。「サポートされている設定」を参照してください。
スキャン済み	データ分析が完了し、サポートされているファイル形式がスキャンされ、分類の詳細がリソースレベルで利用可能になっています。「スキャン対象ファイル形式を参照してください。
	リソースにデータが含まれていません。

リソースとデータベースの詳細

「データインベントリ」ページでリソースまたはデータベースをクリックすると、選択したアイテムに関する詳細情報を含むスライド式パネルが表示されます。このパネルには、[データの概要] と [分類されたデータ] の2つのタブがある **[データ]** セクションがあります。各タブで、検出されたデータが表示され異なります。

データの概要

[概要] タブには、リソースまたはデータベースの一般的なスキャンの詳細と統計情報の概要が表示されます。

表示フィールド:

フィールド	説明
スキャン時間	機密データがないかリソースまたはデータベースがスキャンされた時

フィールド	説明
	間。
データの更新時間	リソースまたはデータベース上のデータが最後に更新された日時。
スキャンされたオブジェクトまたはテーブル	スキャンされたファイルまたはオブジェクト (またはデータベースが表示されている場合はテーブル) の数。
機密性の高いオブジェクトまたはテーブル	機密データを含むスキャンされたファイルまたはテーブルの数
データサイズ	リソースまたはデータベースでスキャンされたデータの合計サイズ。

表の列

縦棒	説明
データタイプ	リソースで検出されたデータのタイプ。詳細については、スキャン対象データタイプ。
データカテゴリ	データタイプが属するカテゴリ。詳細については、スキャン対象データタイプ。
センシティブなオブジェクト	見つかった機密オブジェクトまたはファイルの数。詳細については、スキャン対象ファイル形式。
データの機密性	検出されたデータタイプにマッピングされる機密レベル。詳細については、「感度レベルを参照してください。

分類されたデータ

[機密データ] タブには、機密データが検出された個別のファイル、オブジェクト、またはテーブルのテーブルが表示されます。

縦棒	説明
パス	検出されたオブジェクトの名前またはパス。
データタイプ	検出されたオブジェクトに含まれるすべてのデータタイプのリスト。詳細については、スキャン対象データタイプ 。
データカテゴリ	検出されたオブジェクトに含まれるすべてのデータカテゴリのリスト。詳細については、スキャン対象データタイプ 。
データの機密性	検出された最も高い機密レベルを持つデータタイプにマッピングされる機密レベル。たとえば、E メール、IP アドレス、クレジットカードが検出された場合、他の 2 つのタイプが「社外秘」レベルのみでも、レベルは「制限付き」となります。詳細については、「 感度レベルを参照してください。
サンプル	検出された機密データの 1 つ以上のサンプル。番号にカーソルを合わせると、サンプルが表示されます。

オンデマンドスキャンの実行

特定のデータリソースに対してオンデマンドスキャンを開始する場合は、手動でリクエストできます。スキャンを開始すると、リソースがキューの先頭にプッシュされます。スキャン結果は、Tenable によって次回定期的にデータの同期と更新の頻度が実行された後にクラウドサイバーエクスポージャーコンソールに表示されます。

[Data Scanning Settings] で関連アカウントをデータ保護スキャンから除外している場合、オンデマンドスキャンは利用できません。

オンデマンドスキャンを実行する方法

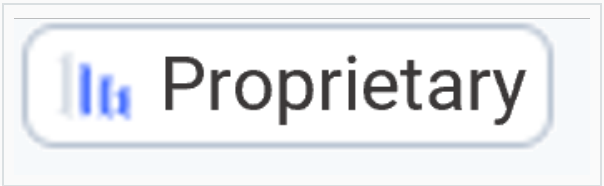
1. 関連するデータリソースに移動します。データ・リソースは、「 **調査** 」>「 **データ** 」>「 **データ・リソース**」にあります。

2. 三点リーダーアイコン (アクションメニュー) をクリックし、**[今すぐスキャン]** をクリックします。**[スキャンをリクエスト済み]** ボタンがグレー表示されている場合は、そのリソースのスキャンがすでにリクエストされていることを意味します。
3. スキャンが正常にリクエストされたことを示すダイアログが表示されます。完了したら、**[OK]** をクリックします。

感度レベル

この表に、スキャン対象データタイプにマッピングされたスキャン対象データの機密レベルを示します。

データをスキャンされたリソース (またはリソースにアクセスできるアイデンティティ) に関連する検出結果の深刻度は、検出されたデータの機密性によって影響されます。機密レベルが「社外秘」、「専有」、「制限付き」の場合、検出結果の深刻度は 1 レベル上げられます。たとえば、「暗号化されていない S3 バケットトラフィック」の検出結果は、(機密レベルが「社外秘」の) IP アドレスが、関連する S3 バケットで検出された場合、深刻度が「高」から「重大」に引き上げられます。

感度レベル	サマリー	説明
	規制対象の機密データ	制限付きデータは非常に機密度が高く、通常、個人を特定できる情報 (PII)、政府機密情報、その他の重要なデータが含まれます。このデータの不正アクセスや露出は、法的、財務的、または評判に重大な影響を及ぼす可能性があります。
	機密度の高い知的財産	専有データとは、特定の組織によって所有および保護されている情報を指します。このレベルは、自社のビジネスに固有の知的財産、営業秘密、または製品設計を識別するために使用されるカスタムデータ型の作

感度レベル	サマリー	説明
		成 用に予約されています。組み込みデータ型は含まれません。
Confidential	ビジネス上の機密 (知る必要がある)	社外秘データは、不正アクセスから保護する必要があります。このカテゴリには通常、財務データ、従業員の記録、ビジネス戦略などの情報が含まれます。社外秘データへのアクセスは、権限のある担当者に限られます。
Private	社内	内部データは組織内での使用を意図しています。公開利用には適していないものの、機密性が高いとは言えない情報が含まれる場合があります。このデータへの不正アクセスは、依然としてある程度のリスクをもたらす可能性もありますが、そのレベルは機密度の高いデータほど重大ではありません。
Public	パブリックに共有可能	公開データとは、一般の人々と自由に共有できる情報です。社外秘情報やプライベートな詳細は一切含まれておらず、通常、露出しても悪影響を受けることはありません。

Events

イベント

[イベント] 画面は、環境内のすべてのイベントタイプに対する単一のアクティビティログです。クラウドプロバイダーのアクティビティ、ランタイムセンサーのアクティビティ、Kubernetes アドミッションコントローラーのアクティビティを 1 か所にまとめるため、別々の画面を切り替えることなく、アクティビティの調査と監査、異常への対応、データフォレンジックのサポートを行うことができます。

[イベント] 画面は、クラウド環境での大量のイベントデータのために開発されており、特にイベントに関する高速で焦点を絞ったクエリエクスペリエンスを提供します。

イベントタイプ

画面左上のイベントタイプセレクターを使用して、表示するイベントを選択します。利用可能なイベントタイプは次のとおりです。

イベントタイプ	説明
イベント	すべてのソースからのすべてのイベントタイプ。
クラウドイベント	クラウドプロバイダーから収集されたアクティビティ (エージェントレス)。クラウドクラウドイベント。
ランタイムイベント	ランタイムセンサーによって収集されるすべてのアクティビティ。これには現在、ランタイムファイルオープンイベントとランタイムプロセス実行イベントが含まれます。
ランタイムファイルオープンイベント	ランタイムセンサーによって収集されるファイルオープンアクティビティ。
ランタイムプロセス実行イベント	ランタイムセンサーによって収集されたプロセス実行アクティビティ。
Kubernetes アドミッションコントローラーイベント	アドミッションコントローラーポリシーによって評価されたクラスタ内のアクション。「 Kubernetes アドミッションコントローラーイベント」を参照してください。

イベントを表示

イベントを表示するには

1. Tenable One Cloud Exposureコンソールで、**イベント**画面を開きます。
2. イベントタイプセレクターを使用して、表示するイベントのタイプを選択します (**クラウドイベント** や **ランタイムプロセス実行イベント**など)。
3. テーブルの上部にあるフィルターを使用して、表示するデータの範囲を絞り込みます。「 データのフィルタリングを参照してください。
    - **[Time]** (時間) フィルターは常に適用され、削除することはできません。デフォルトでは、**過去1日間**に設定されています。任意の日付範囲を設定できます。イベントは、検出または脅威ストーリーにリンクされていない限り90日間保持されます。
4. テーブル内で値を右クリックして、その値でテーブルをフィルタリングしたり、フィルターで除外したりします。この方法でフィルターを複数回適用すると、結果をさらに絞り込むことができます。
5. イベントをクリックするとスライド式パネルが開き、詳細が表示されます。
6. 未加工のイベントを JSON 形式で表示して、アクティビティの完全な記録を確認します。

イベントデータのエクスポート

イベントデータをカンマ区切り値 (CSV) ファイルにエクスポートします。データは、現在テーブルに適用されているフィルターに従ってエクスポートされます。

> **注意:** エクスポート機能は、10,000件の結果に制限されています。テーブルにさらに結果が含まれている場合は、追加のフィルターを適用してデータを絞り込むか、最初の10,000件の結果をエクスポートします。

イベントデータをエクスポートする方法

1. (オプション)アカウントのドロップダウンから アカウント階層とフォルダー を選択して、特定のクラウドアカウントにデータの範囲を設定します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。
3. テーブルの右上隅にある **[エクスポート]** をクリックします。

クラウドイベント

クラウドイベントタイプは、クラウド環境内のアイデンティティによって実行されたすべてのアクションの詳細なビューを提供します。アクティビティとサービスへの変更の文脈と時系列に沿った記録です。これは、異常の異常検出、クラウドアクティビティの調査と監査、データフォレンジックのサポートに使用します。

たとえば、クラウドイベントを使用して次のことができます。

- 他のアイデンティティを引き受け、引き受けたアイデンティティのアクセス許可 (*オリジネータ*) を使用して動作するクラウドアイデンティティを検索し、これらがどのようなアクティビティを実行するかを確認します。この情報は、AWS CloudTrail では利用できません。
- 「AccessDenied」の結果を含むイベントを見つけて、特定のリソースにアクセスできないステークホルダーからのリクエストのトラブルシューティングを行います。

> **注意:** Tenable には、AWS AccessDenied イベントを解析し、イベントが発生した理由を説明して、実行可能な修正を提供するオープンソースツールがあります。「AWS での Access Undenied」を参照してください。

クラウドイベントの列データ

次の列はクラウドイベントに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

列	説明
時刻	クラウドイベントが実行された日時。直近のイベントが最初に一覧表示されます。**注意**: (AWS/GCP) それぞれ 1 分以内に発生した同一のイベントは、1 つのエントリにグループ化されます。表示可能なすべてのクラウドイベントデータが同一である場合にのみ、イベントは同一と見なされます (未加工のイベント JSON を除く)。
アクター	アクションを実行したアイデンティティの名前名前の下には、アイデンティティのタイプとアカウント名が表示されます。
アクターの IP アドレス	アクションを実行したアイデンティティのソース IP アドレス。

列	説明
IP アドレスの場所	国旗で示されるアクター IP アドレスの原産国。国名を表示するには、国旗にカーソルを合わせます。
アクション	クラウドプロバイダーのログ値 (AWS `eventName`、Azure `operationName`、GCP `methodName`) から取得された、クラウド内でアイデンティティが実行したイベント。
リソース	イベントが実行されたリソース (該当する場合)。
アカウント	アクションが実行されたクラウドアカウント。
結果	クラウドプロバイダーのログ値 (AWS `errorMessage`、Azure `statusMessage`、GCP `status.code`) から取得されたイベントの結果。結果にカーソルを合わせると、詳細を確認できます。**注意**: AWS では、エラーのないアクションに [Success] (成功) の値が割り当てられます。
Raw イベント	ログイベントの JSON ファイルを表示して、アクションの完全な記録を確認します。

ランタイムイベント

ランタイムイベントは、クラスターにインストールされたランタイムセンサー (eBPF) によって収集され、ワークロードレベルのアクティビティを詳細に可視化します。ラン **タイム・イベント** を選択してすべてのランタイム・アクティビティを表示するか、特定のランタイム・イベント・タイプを選択します。

- **ランタイムファイルオープンイベント** - ワークロード内のファイルオープンアクティビティ。
- **ランタイムプロセス実行イベント** – ワークロード内のプロセス実行アクティビティ。

列の可用性は、ランタイムイベントタイプによって異なります。以下の各表の **[デフォルト]** は、列がデフォルトで表示されるかどうかを示します。列ピッカーを使用して、任意の列を表示または非表示にできます。

ランタイムイベントの列データ

列	説明	デフォルト
時刻	イベントが発生した日時。直近のイベントが最初に一覧表示されます。	必要
アクター	アクティビティを実行したアイデンティティ	必要
プロセス名	イベントに関連するプロセスの名前。	必要
プロセス引数	プロセスに渡されるコマンドライン引数。	必要
Kubernetes リソース	アクティビティが発生した Kubernetes リソース (ポッドやワークロードなど)。	必要
クラスタ	アクティビティが発生した Kubernetes クラスタ。	必要
アカウント	アクティビティが発生したクラウドアカウント。	必要
イベント数	エントリに集計された同一イベントの数。	不要
名前	イベントの名前。	不要
発生元	イベントのソース。	不要
親プロセス ID	親プロセスのプロセス ID (PID)。	不要
親プロセス名	親プロセスの名前。	不要
プロセス ID	プロセスのプロセス ID (PID)。	不要
システム ID	Tenable がイベントに割り当てる一意の識別子。	不要
仮想マシン	アクティビティが発生した仮想マシン。	不要

ランタイムファイルオープンイベントの列データ

列	説明	デフォルト
時刻	ファイルが開かれた日時直近のイベントが最初に一覧表示されます。	必要
アクター	アクティビティを実行したアイデンティティ	必要
プロセス名	ファイルを開いたプロセスの名前。	必要
フラグ	ファイルを開く操作で使用されるフラグ。	必要
ファイルパス	開かれたファイルのパス。	必要
Kubernetes リソース	アクティビティが発生した Kubernetes リソース (ポッドやワークロードなど)。	必要
クラスタ	アクティビティが発生した Kubernetes クラスタ。	必要
アカウント	アクティビティが発生したクラウドアカウント。	必要
成功	ファイルを開く操作が成功したかどうか。	必要
イベント数	エントリに集計された同一イベントの数。	不要
モード	操作に関連するファイルモード。	不要
名前	イベントの名前。	不要
発生元	イベントのソース。	不要
親プロセス ID	親プロセスのプロセス ID (PID)。	不要
親プロセス名	親プロセスの名前。	不要
プロセス引数	プロセスに渡されるコマンドライン引数。	不要
プロセス ID	プロセスのプロセス ID (PID)。	不要

列	説明	デフォルト
システム ID	Tenable がイベントに割り当てる一意の識別子。	不要
UMask	操作に適用されるユーザーファイル作成モードのマスク(umask)。	不要
仮想マシン	アクティビティが発生した仮想マシン。	不要

ランタイムプロセス実行イベントの列データ

列	説明	デフォルト
時刻	プロセスが実行された日時。直近のイベントが最初に一覧表示されます。	必要
アクター	アクティビティを実行したアイデンティティ	必要
プロセス名	実行されたプロセスの名前。	必要
プロセス引数	プロセスに渡されるコマンドライン引数。	必要
Kubernetes リソース	アクティビティが発生した Kubernetes リソース (ポッドやワークロードなど)。	必要
クラスタ	アクティビティが発生した Kubernetes クラスタ。	必要
アカウント	アクティビティが発生したクラウドアカウント。	必要
判定	実行されたプロセスに対する Tenable のマルウェア分析の結果。	必要
コンテナドリフト	デプロイされたコンテナイメージと比較して、実行されたプロセスに対して検出されたドリフトのタイプ (ファイルの作成、変更、削除、所有権の変更、アクセス許可の変更)。	不要

列	説明	デフォルト
イベント数	エントリに集計された同一イベントの数。	不要
ファイルパス	実行されたファイルのパス。	不要
名前	イベントの名前。	不要
発生元	イベントのソース。	不要
親プロセス ID	親プロセスのプロセス ID (PID)。	不要
親プロセス名	親プロセスの名前。	不要
プロセス ID	プロセスのプロセス ID (PID)。	不要
システム ID	Tenable がイベントに割り当てる一意の識別子。	不要
仮想マシン	アクティビティが発生した仮想マシン。	不要

Kubernetes アドミッションコントローラーイベント

- アドミッションコントローラーポリシーの設定については、アドミッションコントローラーポリシーを参照してください。
- 概念の概要については、「アドミッションコントローラーの概要」を参照してください。

Kubernetes アドミッションコントローラーイベントタイプには、アドミッションコントローラーポリシーによって評価された、クラスタ内で実行されたアクションが表示されます。アドミッションコントローラーポリシーの設定とアドミッションコントローラーのインストール、ここでアクションを確認できます。

ログに記録されたアクションをクリックして、スライド式パネルを開きます。**[概要]** タブにはポリシー情報が表示されます。**[YAML のリクエスト]** タブには、アクションに使用された YAML が表示されます。

デフォルトでは、このビューはフィルタリングされており、アラートをトリガーしたアクション、または拒否されたアクションのみが表示されます。ログは 30 日から 60 日後に削除されます。

アドミッションコントローラーイベントの列データ

列	説明
時刻	アクションが発生した時刻。
アクション	Kubernetesリソースで実行される操作のタイプ(作成、更新、削除など)。
リソース	アクションが発生したリソースは、名前空間とその後にリソース名が続くものとして表示されます。
クラスタ	アクションが発生したクラスター。
アカウント	クラスタに関連付けられているアカウント。
結果	アドミッションコントローラーの評価結果: **[合格]** (すべてのポリシー要件を満たし、許可)、**[アラート]** (要件を満たしていないが許可、アラート付き、ポリシーが[アラート]効果を使用している場合にのみ)、**または[拒否]** (要件を満たさずブロック、ポリシーが[拒否]効果を使用している場合にのみ)。
ポリシー違反	アクションによって違反されたポリシー。赤は、アクションを拒否したポリシーを示します。オレンジは、アラートを発行したポリシーを示します。
評価されたポリシー	アクションを評価したすべてのポリシーのリスト。
所有者リソース	アクションを開始したリソース。
アイデンティティ	アクションを開始したユーザーまたはサービスアカウント

リスク

クラウドの検出結果

これは、クラウドの検出結果を表示および管理するためのハウツーガイドです。

- 検出結果のステータスと検出結果のライフサイクルの概念概要については、「検出結果のライフサイクル」を参照してください。
- 検出結果の深刻度の仕組みの概念概要については、「検出結果の深刻度」を参照してください。
- 検出結果の作成方法を設定するには、「クラウドポリシー」を参照してください。

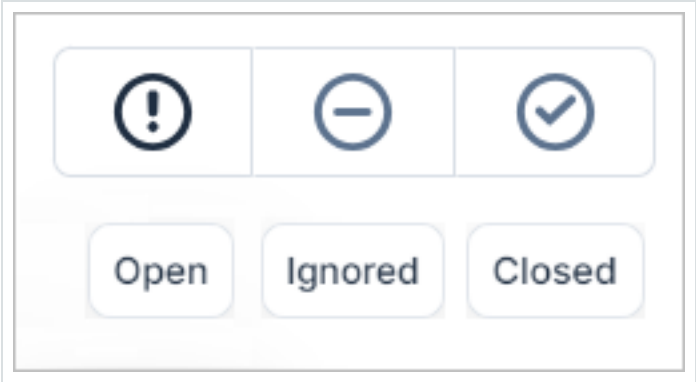
[クラウドの検出結果] ページを使用すると、クラウドアカウントの検出結果のトリアージを効果的かつ効率的に実行できます。たとえば、次のことが可能です。

- 本番環境の重大な検出結果を検出して修正する
- パブリック S3 バケットを検出して修正する
- 特定のコンプライアンスを満たさない検出結果を発見して修正する

検出結果ページの操作

[検出結果] ページでは、現在のステータスによって検出結果がグループ分けされて検出結果を表示します。

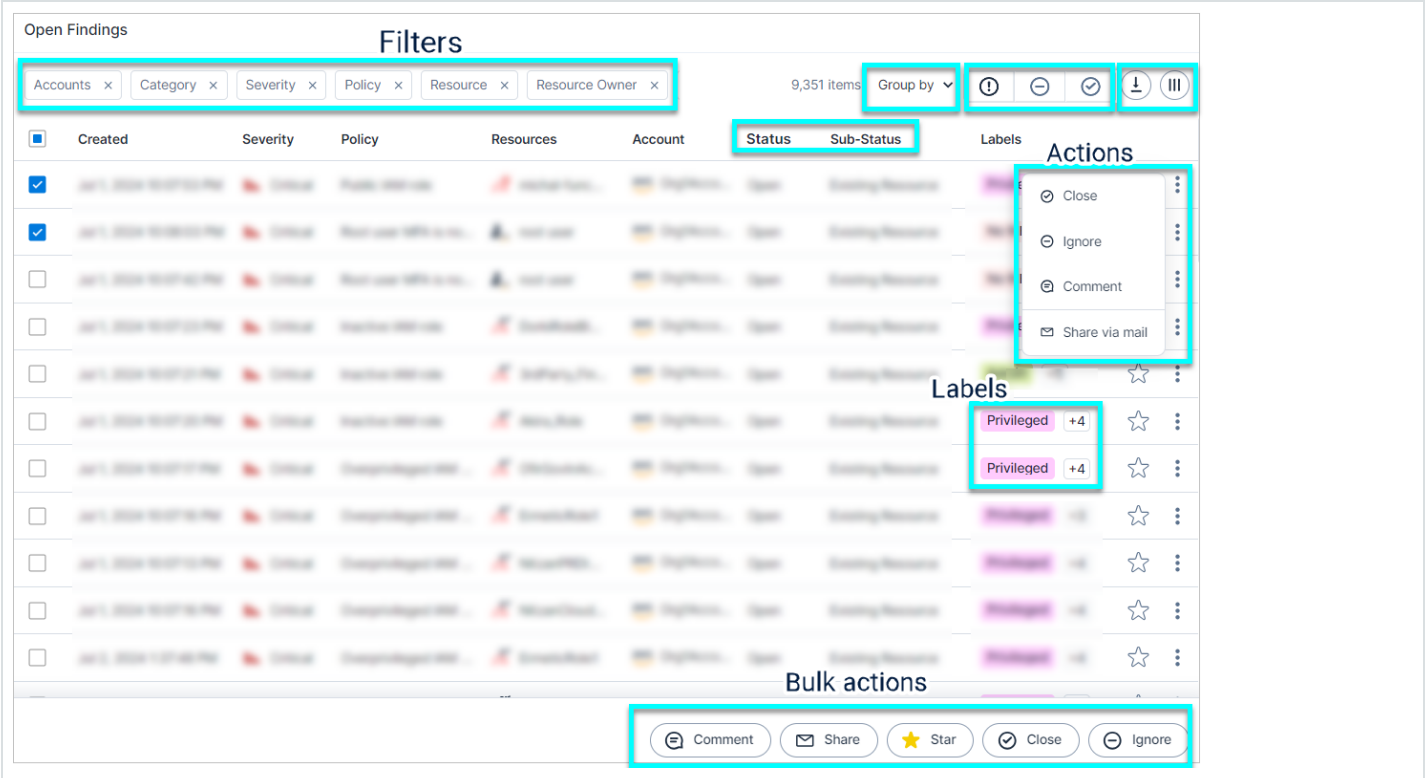
- **を開きます**。環境内のすべてのアクティブな検出結果を表示します。
- **無視**。今すぐ処理しなくてもよい検出結果が表示されます。関連するリソースは永久に、または設定された期間、除外されます。
- **閉じました**。手動または Tenable によって自動でクローズされた検出結果が表示されます。



注意:

- オープンまたは無視の検出結果は、クラウド環境に対する潜在的な脅威の深刻度順に一覧表示されます。
- 複数の検出結果の深刻度が同じ場合でも (たとえば「高」)、テーブルの上位に表示される検出結果は、Tenable によってより高いリスクをもたらすと評価されたものです。

この図では、[検出結果] ページで利用できる主なナビゲーション要素がハイライトされています。これらの要素を使用することで、結果を絞り込んで整理できるため、探している結果を見つけやすくなります。



項目	説明
ステータス別の表示 	オープン、無視、またはクローズの検出結果を表示します。
深刻度	検出結果のリスク検出結果の深刻度 表示。デフォルトビューで検出結果を絞り込むために使用されます ([Group by] (グループ別) が適用されていない場合)。
ステータス/サブステータス列 / フィルター	詳細については、「検出結果のライフサイクルを参照してください。
すべて選択	(適用されたフィルターに応じて) すべての検出結果を選択することにより、一括操作を実行しやすくなります。たとえば、特定のグループの検出結果を無視するか手動でクローズしたい場合などに便利です。ただし最大 1 万件の検出結果に限られます。
フィルター	使用できるフィルターはページごとにやや異なりますが、以下のフィルターがあります。 • 作成時刻 • オープン時刻 • アカウント • カテゴリ • 深刻度 • ポリシー • リソース • サブステータス • コンプライアンス • ラベル

項目	説明
	• スター • 付き • チケット
次でグループ化	検出結果のグループ化: • **アカウント**。属する接続済みアカウントに従って、すべての検出結果をグループ化します。 • **ポリシー**。検出結果をトリガーしたポリシーに従って、すべての検出結果をグループ化 どちらのフィルターも、グループに含まれる深刻度の高い検出結果の割合に基づいた順番で、グループ分けされた検出結果が一覧表示されます。たとえば、75% が深刻度「重大」である検出結果グループは、100% が深刻度「高」である検出結果グループの前に表示されます。
ラベル	検出結果に関連するリソースに適用されたラベルのリソースへの適用は、検出結果に伝播されます。**注意**: 検出結果タイプを直接反映する OOTB システムラベルは、重複を避けるため、検出結果には伝播されません。たとえば、「過剰な権限を持つ IAM ロール」の検出結果には、関連付けられているリソースにラベルが適用されている場合でも、[Excessive] (過剰) または [Privileged] (特権) ラベルは付与されません_。
スターを付ける	後で確認するのを忘れないように、重要な検出結果にスターを付ける。
アクション	• **を閉じ** • る無視。検出結果を無視するする。 • **メールで共有します**。検出結果の情報を 1 つ以上のメールアドレスに送信します。 • **Jira 課題の作成/更新、または ServiceNow インシデントの作成/更新。**

項目	説明
	チケット統合がインストールされている場合利用できます。詳細については、検出結果に基づくアクションのトリガーを参照してください。
一括アクション	複数の検出結果に一度にアクションを適用します。
エクスポート	外部ツールで分析または処理するために、マップデータを CSV にエクスポートします。
列ピッカー	テーブルに表示する列を選択します。

検出結果データのエクスポート

検出結果データをエクスポートして、環境内の検出結果のサマリーレポートを作成します。データは、その時点でテーブルに適用されているフィルターに従ってエクスポートされます。出力データは CSV 形式で、修正手順など、関連する検出結果データをすべて含みます。

たとえば、次のことが可能です。

- クローズの検出結果すべてを対象とするレポートを作成できます。これにはクローズの理由に関するサブステータス情報 (たとえばリソースの削除) を含めることができ、企業の関連するステークホルダーにレポートを共有できます。
- オープン/スター付き/無視の検出結果、または検出結果の他のサブセット (フィルターを使用) のレポートを作成できます。

> **注意:** 追加の非標準の情報を含む特定の検出結果タイプ (ポリシー) のデータをエクスポートすることもできます。ページがポリシー別にグループ化されている場合、関連するタイプの [エクスポート] ボタンが利用可能になります。たとえば、「過剰な権限を持つ IAM グループポリシー」のすべての検出結果データをエクスポートできます。このタイプには、検出結果ページ全体をエクスポートする際に抽出されない追加のパラメーターが含まれています。

検出結果のレポートを作成する方法

1. Tenable One Cloud Exposure コンソールで、**関連する[クラウドのリスク>検出結果]** ページ (オープン/無視/クローズ) に移動します。
2. (オプション) 追加のフィルターを適用して、ニーズに合わせて検出結果のリストを絞り込みます。
3. 追加の非標準の情報を含む特定の検出結果タイプのデータをエクスポートするには以下を実行します。
    1. **[グループ化]** ドロップダウンをクリックし、**[ポリシー]** をクリックします。
    2. 関連するタイプをクリックして、セクションを展開します。たとえば、過剰な権限を持つ IAM グループをクリックします。
    3. セクション右上の [Export] (エクスポート) ボタンをクリックします。
4. **[Export]** をクリックします。CSV サマリーレポートが作成されます。

定期レポートの作成

[検出結果] ページから直接、スケジュールされたレポートを作成します。このページのレポートの内容は、テーブルに適用した特定のフィルターに基づきます。出力データは CSV 形式で、クラウドサイバーエクスポージャーコンソールの各リソースページの URL など、関連するリソースデータがすべて含まれます。

スケジュールされたレポートの作成方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>クラウドの検出結果]** をクリックします。
2. 関連する データのフィルタリングを適用します。
3. テーブルの右上にある **[Create Scheduled Report]** ボタンをクリックします。
4. レポートの詳細を入力します。詳細については レポート を参照してください。
5. **[スケジュール]** または **[生成]** をクリックします。
6. [Reports] (レポート) ページでレポートの詳細情報を確認できます。

検出結果を無視する

オープンの検出結果を無視して、リソースをポリシーから永久に、または設定された期間除外します。たとえば、既存の検出結果を[Open Findings] (オープンの検出結果) ページには今すぐ表示せず、後で追

跡する場合は、検出結果を後日まで延期することができます。日付になると、検出結果のステータスは **[オープン]** に戻ります。

検出結果は、除外の対象になると無視されます。[検出結果] ページでは、次の操作を行うことで検出結果を無視できます。

- 特にこれらの検出結果を対象とする新しい除外を作成します。
- 検出結果を既存の除外に追加する

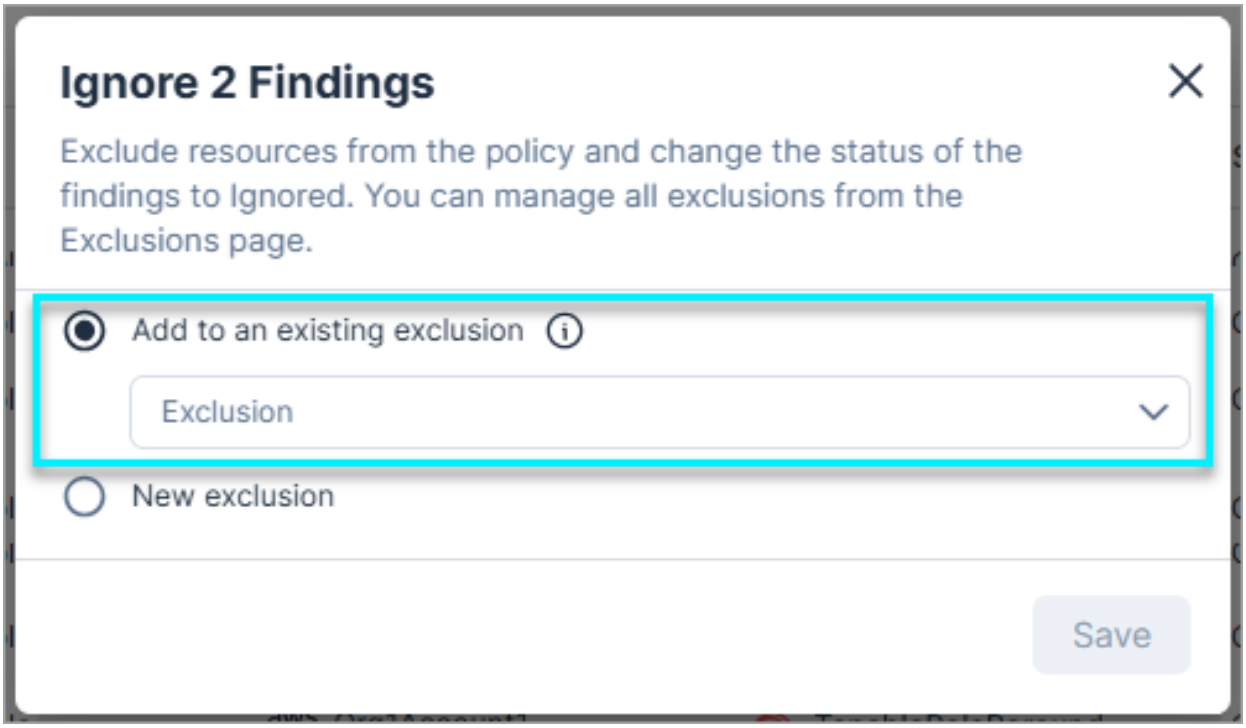
検出結果を新しいまたは既存の除外に追加すると、直ちに有効になります。対象となる検出結果は直ちに無視されます。

> **注意:** [検出結果] ページで新しい除外を作成する前に、検出結果を既存の除外に追加できるかどうか、または除外作成する方がよいかを確認してください。
> [検出結果] ページから作成された除外は事後対応的で、個々の検出結果に重点を置いています。この方法は、一貫性のないカバレッジや除外の重複を避けるため、迅速で限定的な調整を行う場合にのみ使用してください。カバレッジを拡大するには、無視された検出結果からのパターンベースの除外の作成方法を確認してください。

検出結果を新しいまたは既存の除外に追加する方法

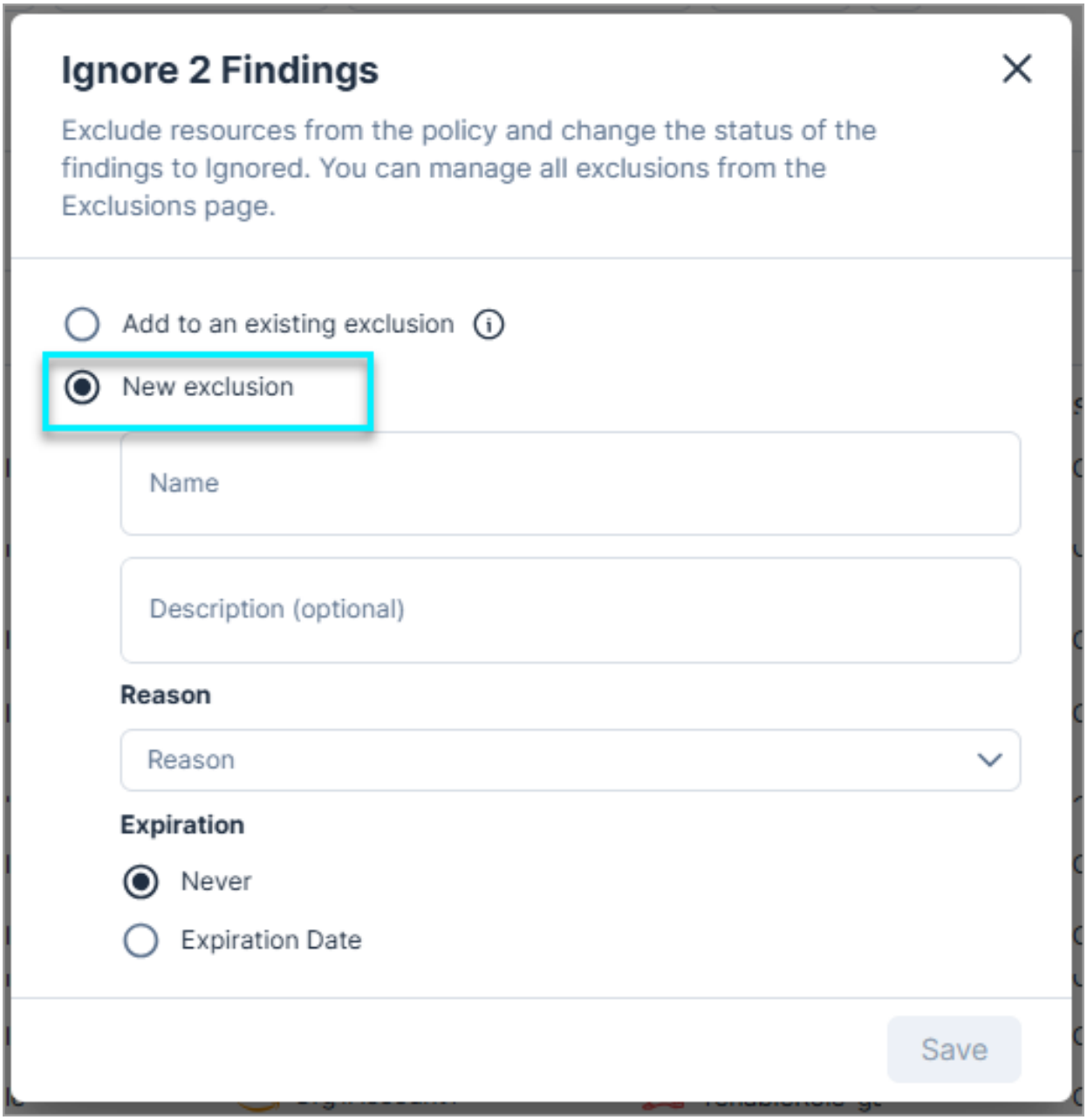
1. **[リスク]** › **[クラウドの検出結果]** または **[IaC の検出結果** > **オープン]** に移動します。
2. 検出結果の表から以下を行います。
    - 単一の検出結果: その横にある三点リーダーアイコンをクリックし、**[無視]** を選択します。
    - 複数の検出結果: 関連する検出結果を選択し、下部にある **[無視]** をクリックします。検出結果を一括で無視できるのは、同じポリシーに属している場合のみです。
3. [検出結果を無視] ダイアログで、次を選択します。
    - **既存の除外に追加します**。

        > 既存の除外に追加する画像を見る



  - ドロップダウンには、同じポリシーと範囲にすでに適用されている除外のみがリストされます。除外がない場合は、除外できます。
  - 対象となるものがない場合、このオプションは無効になります。既存の除外に追加するためのルールを参照してください。
- **新しい除外**。除外のアクションは [無視] であることに注意してください。[検出結果] ページから検出結果の深刻度を変更することはできません。

> [検出結果を無視] ウィンドウの画像を参照



1. **名前** (Dev1 Lab public EC2s など) を入力します
2. 目的を説明する **説明** を追加します。たとえば、QA によって使用される、一般にアクセス可能なテストインスタンスです
3. 検出結果を無視する理由 (例外、設計別、誤検知

4. から選択します。[有効期限で、有効期限なしまたは特定の終了日を選択します。除外の有効期限が切れると、後続のスキャンサイクルの検出結果に適用されなくなります。

4. **[保存]** をクリックします。

[検出結果] ページの変更は直ちに適用されます。無視した検出結果は、定義されたサブステータス (理由) とともに、**[無視の検出結果]** の下に表示されます。

検出結果を無視しない

無視した検出結果は、除外によって抑制されます。無視すべきではなくなった検出結果がある場合は、関連する除外を確認して更新できます。これは、[Findings] (検出結果) ページまたは [Exclusions] (除外) ページから直接実行できます。除外を 除外を監査して維持するする方法をご確認ください。

検出結果を無視しない方法

1. **[リスク]** › **[クラウドの検出結果]** または **[IaC の検出結果]** に移動します。
2. **[無視されたもの]** タブをクリックします。
3. 無視を元に戻したい無視された検出結果の 1 つを見つけます。
4. その横にある三点リーダーアイコンをクリックし、**[除外を管理]** を選択します。
5. [除外の編集] ページで、除外を更新して、検出結果の対象にならないようにします。
6. 除外を保存します。

検出結果を手動でクローズする

検出結果の修正し、根本的なセキュリティ問題を解決すると、検出結果は クラウド サイバーエクスポージャー コンソールで自動的に **[クローズ (修正済み)]** とマークされます。ただし、一部のケースでは、オープンまたは無視の検出結果を **手動でクローズ** したい場合もあります。以下に例を挙げます。

- 検出結果を自動的に識別して「解決済み」としてマークするには時間がかかることがあります。その方が手動で解決した方が、検出結果ページからその検出結果を早く削除することができます。
- 一部の検出結果タイプは、クラウド サイバーエクスポージャー によって自動的に解決済みとしてマークされません (完全なリストについては、自動解決されない検出結果タイプを参照してください)。こ

れは、異常検出結果など、主にアラートとして機能する検出結果に当てはまります。異常検出結果はその独自の性質により、他の多くの検出結果のようにTenable内で従来の方法で修正することができません。代わりに、環境にとって実際の脅威となるかどうかを調査した後、手動で解決済みとしてマークすることができます。

検出結果を手動でクローズすると、検出結果は**[クローズ(手動でクローズ)]**とマークされます。ただしこれを行った場合、問題は実際には修正されておらず、次回データの同期と更新の頻度するときに、検出結果のステータスは**[Open (Reopened)] (オープン(再オープン))に戻ります**。

クローズの検出結果をマークして表示する方法

1. 検出結果の表から以下を行います。
    1. 単一の検出結果: 各検出結果の横にある三点リーダーアイコンをクリックし、**[閉じる]**をクリックします。
    2. 複数の検出結果: 複数の検出結果を選択し、下部にある**[閉じる]**をクリックします。
2. [Close Finding] (検出結果のクローズ) ダイアログで、クローズの理由を示すコメントを追加します。これは検出結果のアクティビティに追加されます。
3. **[閉じる]**をクリックします。
4. クローズされたすべての検出結果を表示するには、**[検出結果] > [クローズ]**に移動します。

検出結果を再オープンする

検出結果を手動でクローズするした検出結果は再度オープンできます。入力すると、検出結果は**[Open (Reopened)] (オープン(再オープン))**とマークされます

検出結果を再オープンする方法

1. 検出結果の表から以下を行います。
    1. 単一の検出結果: 各検出結果の三点リーダーアイコンをクリックし、**[Open]**をクリックします。
    2. 複数の検出結果: 複数の検出結果を選択し、下部にある**[オープン]**をクリックします。
2. [Open Finding] (検出結果のオープン) ダイアログで、再オープンの理由を示すコメントを追加します。これは検出結果のアクティビティに追加されます。

3. **[開く]** をクリックします。
4. 再オープンされたすべての検出結果を表示するには、[検出 **結果]** > **[オープン]** に移動してから、サブステータスを **[再オープン]** でフィルタリングします。

検出結果に基づくアクションのトリガー

サードパーティツールにプッシュ通知を送信するプロセスを自動化する自動化を作成するだけでなく、チケッティング統合に関連するアクションを手動でトリガーしたり、個別の検出結果についてメール通知を送信したりすることもできます。

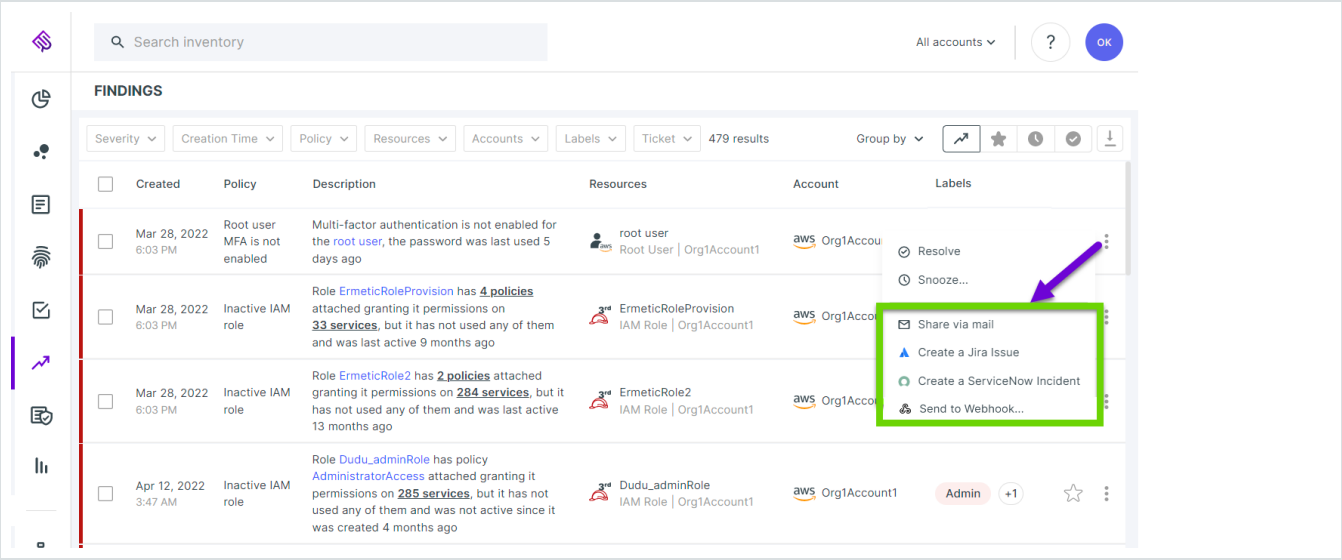
通知を送信するときに、開発者がコードに手動で適用できるように、JSON、Terraform、または CloudFormation 形式で (修正手順に従って) 修正されたポリシーの提案があれば、そのコピーを含めることができます。これは特に、クラウドサイバーエクスポージャーにより自動で実行された修正が開発者のコードで上書きされる可能性がある場合の、インフラのコード化 (IaC) ワークフローで役立ちます。修正されたポリシーの提案を添付することで、Tenable が推奨する内容をお使いのコーディング環境に合わせて直接実装できるようになります。

> **必要なクラウドサイバーエクスポージャーユーザーロール:** このアクションを実行するには、クラウドサイバーエクスポージャーで**コラボレータ**または**管理者**ロールが必要です。詳細については、ユーザーとグループを参照してください。

1 つの検出結果に対してアクションをトリガーする

1 つの検出結果に対してアクションを手動でトリガーする方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>クラウドの検出結果]** または **[リスク> IaC の検出結果]** ページに移動します。
2. 検出結果の横にある三点リーダーメニューアイコンをクリックし、関連するアクションを選択します。



(手順については、アクションごとに、以下の▶アイコンをクリックしてください)

メールで共有します

1. 1つ以上のメールアドレスを入力します。リソース所有者に検出結果情報を送信することも選択できます。この場合、受信者数が多くなる可能性があります。たとえば、関連付けられたメールアドレスのないグループが所有者の場合、Tenableはグループメンバー全員にメールを送信します
2. (オプション)受信者へのメッセージを入力します
3. 送信をクリックします。

Jira問題を作成する

1. **プロジェクト**、**課題タイプ**、**担当者** (オプション)、**ラベル**、**エピック** (オプション)、および **環境** (Jira インスタンスのURL) を選択します。選択したプロジェクトによって、他のフィールドドロップダウンで使用できる値が決まります。ラベルの場合、Jira インスタンスですでに設定されているラベルのリストから選択するか、Jira に送信される新しいラベルを手動で追加できます。ラベル名にスペースを含めることはできません
2. (オプション)**サマリー**フィールドや**説明**フィールドの事前定義コンテンツを編集します。
3. (オプション)[オプションフィールドの追加]をクリックして、ラベル、担当者、エピックなどの必須ではないデータを含めます

4. (オプション)JSON、Terraform、またはCloudFormation形式で(修正手順に従って)修正されたポリシーの提案のコピーを含めるには、**添付ファイル**を追加します
5. [課題を作成](Create Issue)をクリックします。

> ServiceNowインシデントを作成します

1。**インスタンス**と**担当者**を選択します
2. インシデントの**影響**と**緊急度**を選択します
3. (オプション)**サマリー**フィールドや**説明**フィールドの事前定義コンテンツを編集します。
4. (オプション)JSON、Terraform、またはCloudFormation形式で(修正手順に従って)修正されたポリシーの提案のコピーを含めるには、**添付ファイル**を追加します
5. [インシデントの作成]をクリックします。

> Webhook

1に送信します。複数のWebhookを設定している場合は、検出結果を送信するWebhookを選択します。
2. [はい](Yes)をクリックして確認します。

複数の検出結果に対するアクションのトリガー

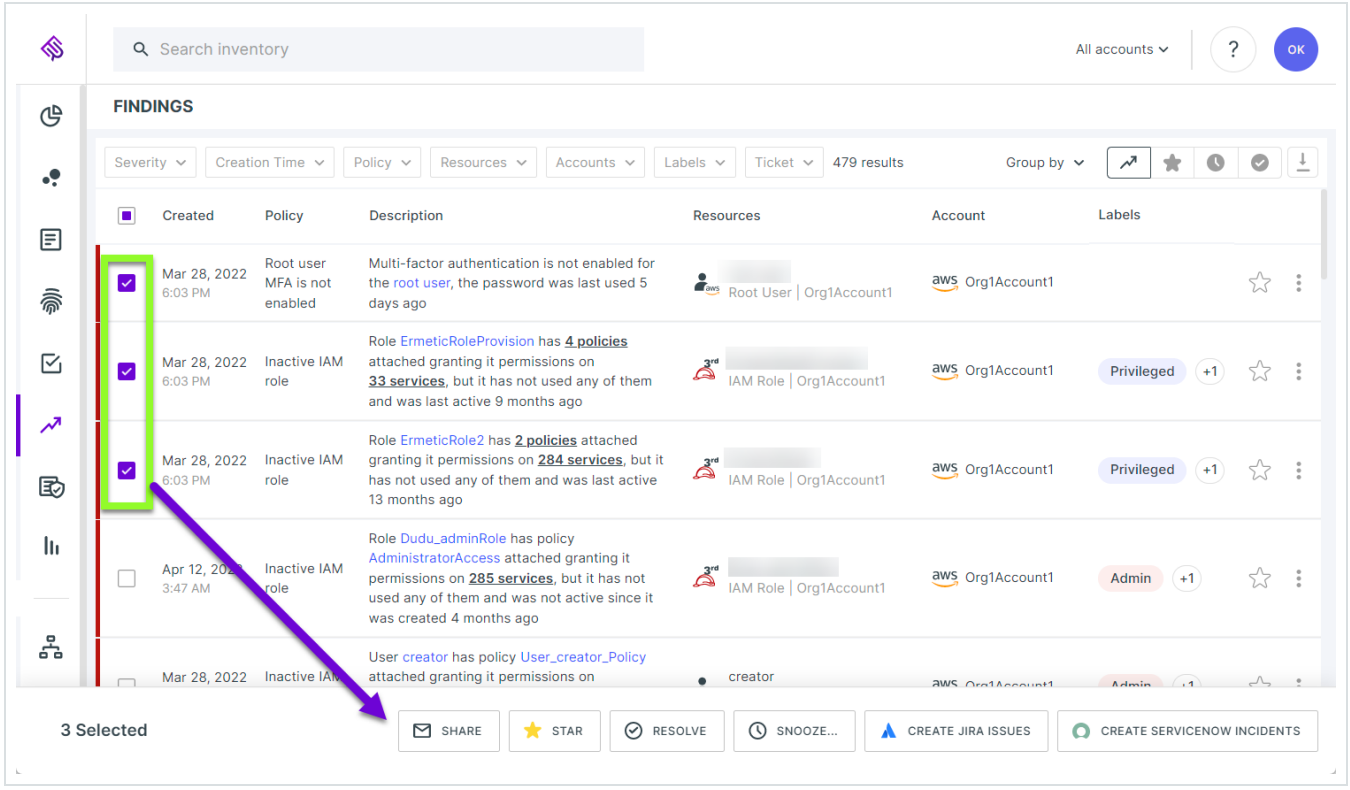
複数の検出結果に対してアクションを手動でトリガーするJira/ServiceNowの場合、次のいずれかを選択できます。

- 選択したすべての検出結果を含む、1つの統合されたチケットを作成します。
- 選択した検出結果ごとに1枚のチケットを個別に作成します

> **注意:** 複数のJira課題またはServiceNowインシデントを一度にトリガーする場合、サマリーまたは説明フィールドを編集することはできません。各課題やインシデントには、クラウドサイバーエクスポージャーが提供するデフォルトのサマリーや説明が含まれます。

複数の検出結果に対してアクションを手動でトリガーする方法

1. クラウド サイバーエクスポージャー コンソールで、**[リスク>クラウドの検出結果]** または **[リスク> IaC の検出結果]** ページに移動します。
2. アクションをトリガーする検出結果の横にあるチェックボックスを選択します。



3. 表示される下部のメニューパネルから、関連するアクションを選択します。
   - **Webhook に送信**
     1. 複数の Webhook を設定している場合は、検出結果を送信する Webhook を選択します。
     2. **[はい]** をクリックして確認します。
   - **メールで共有する**
     1. 1 つ以上のメールアドレスを入力します。リソース所有者に検出結果情報を送信することもできます。この場合、受信者数が多くなる可能性があります。たとえば、関連付けられたメールアドレスのないグループが所有者になっている場合、Tenable がグループメンバー全員にメールを送信します。

2. (オプション) 受信者へのメッセージを入力します。
3. **[送信]** をクリックします。

- **Jira 課題の作成**
  1. 次のいずれかを選択します。
     - **すべての検出結果を含む統合された Jira 課題を作成します**
     - **検出結果ごとに 1 件の Jira 課題を個別に作成します**
  2. **プロジェクト**、**課題タイプ**、**担当者**、**エピック** (オプション)、**環境** (Jira インスタンスの URL)、**ラベルを選択します**。選択したプロジェクトによって、他のフィールドドロップダウンで使用できる値が決まります。
  3. (オプション)「**オプション・フィールドの追加**」をクリックして、ラベル、担当者、エピックなどの非必須データを含めます。
  4. **[問題の作成]** をクリックします。
- **ServiceNow インシデントの作成**
  1. 次のいずれかを選択します。
     - **すべての検出結果を含む統合された ServiceNow 課題を作成します**
     - **検出結果ごとに 1 件ずつ、個別の ServiceNow 課題を作成します**
  2. **インスタンス**と**担当者**を選択します。
  3. インシデント**の影響と緊急性**を選択します。
  4. **[インシデントの作成]** をクリックします。

Jira および ServiceNow チケットを追跡する

チケッティング 統合 (Jira、ServiceNow) を接続し、修正ワークフローを効率化する 自動化 と、外部チケットが作成されたシステムで作成されます。これらの外部チケットは、[Findings] (検出結果) ページから直接簡単に追跡できます。

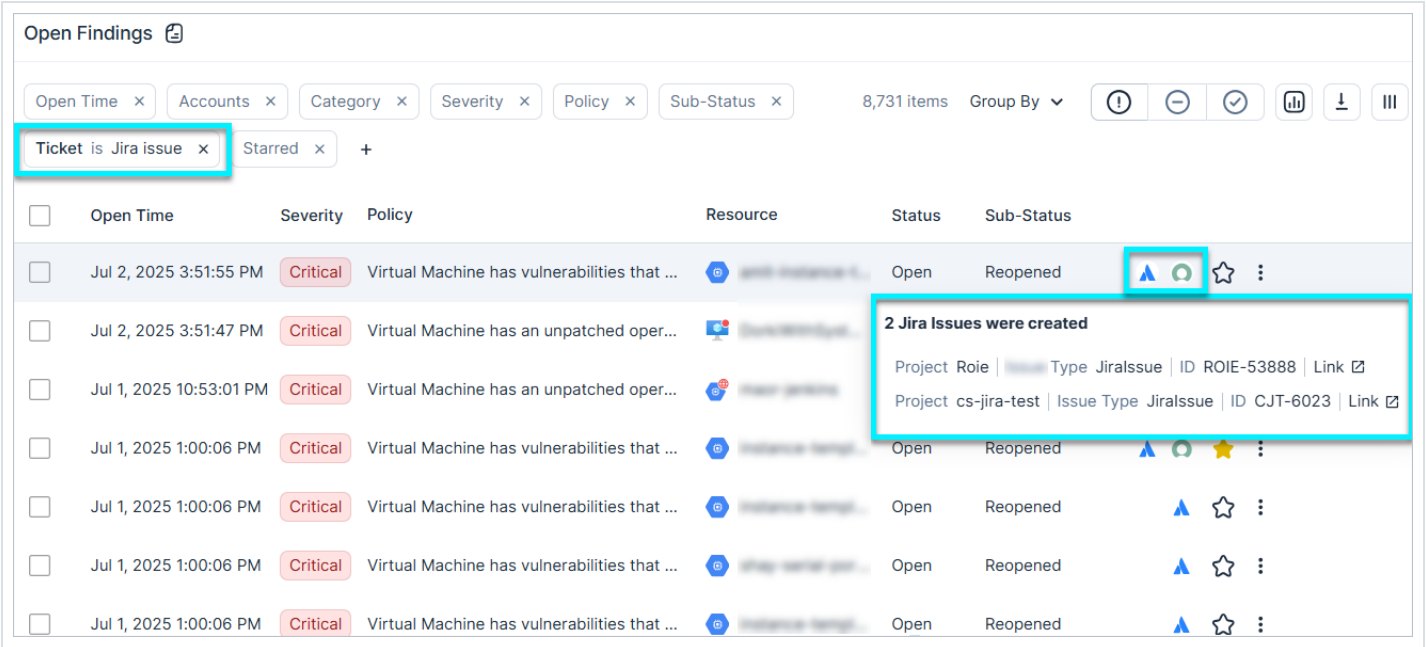
この統合ビューにより、インシデント管理が合理化され、運用チームとのコラボレーションが改善されます。また、セキュリティの検出結果にリンクされた外部チケットに直接アクセスできるため、トレーサビリティが強化されます。

外部チケットを追跡する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>クラウドの検出結果]** をクリックします。
2. 必要に応じて、**[オープン]**、**[無視]**、**[クローズ]** の検出結果ページに移動します。



3. **[チケット]** フィルターで、**[Jira 課題]** や **[ServiceNow インシデント]** を選択して、チケットが作成された検出結果でテーブルをフィルタリングします。
4. (オプション)検索を絞り込むには、必要に応じて他のフィルターを適用します。
5. 関連する検出結果の横にある アイコンまたは ServiceNow アイコンにカーソルを合わせると、チケットの詳細が表示されます。



検出結果の詳細の表示

検出結果をクリックして詳細な情報を表示し、それに関連するリスクを修正します。イベントの詳しい履歴説明、イベントがもたらす潜在的なリスクの幅広い根拠、具体的な修正手順が表示されます。各検

出結果には、検出結果の種類に応じたさまざまな情報と、検出結果の作成をトリガーした具体的な状況が表示されます。

以下のような検出結果の詳細情報とその他の関連情報を確認して、理解を深めます。

- 検出結果の根本的な原因
- 検出結果の範囲
- 環境にもたらされる潜在的なリスク
- 検出結果の深刻度の説明

> **注意:** カスタムポリシー違反は最初の1万件の結果に制限されます。

検出結果からシークレットを除外する

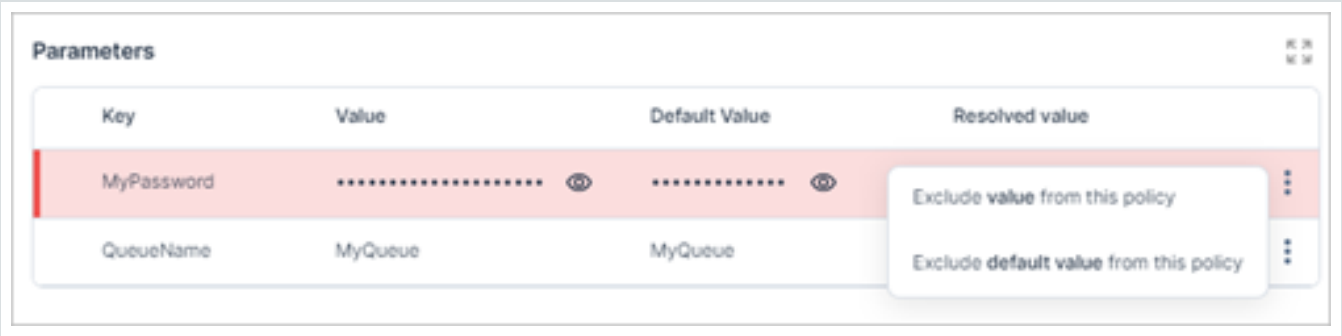
検出された誤検出に対処するために、検出結果からシークレットを除外します。シークレットは通常、キーと値のペアとして表され、キーまたは値のいずれかに機密情報が含まれている可能性があります。

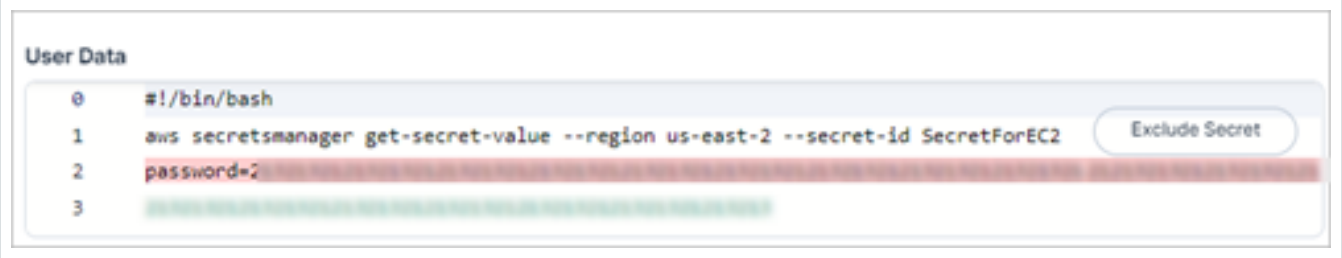
パターンを入力することで、特定のシークレットを検出結果のトリガーから除外できます。パターンがシークレットと一致した場合、クラウドサイバーエクスポージャーはそのシークレットを除外します。たとえば、値パターン `https://*` を使用して、誤ってシークレットとしてフラグが立てられたURLを除外します。

このオプションは、シークレットの公開に関連する検出結果で利用できます。たとえば、CloudFormationスタックでシークレットが公開されています。

検出結果からシークレットを除外する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>クラウドの検出結果]** をクリックします。
2. 関連する検出結果をクリックしてオープンします。
3. [Overview] (概要) ページで、除外するシークレットを特定します。シークレットは赤でハイライトされます。シークレットマスキングして非表示にすることができます。
4. 三点リーダーアイコンをクリックし、**[Exclude value/default from this policy]** をクリックします。





5. **キーパターンと値パターン**を入力します。これらのフィールドには、現在のキーと値が自動的に入力されます。パターンでは次のワイルドカード文字を使用できます。
    - アスタリスク * - 0 文字以上と一致
    - クエスチョンマーク ? - 1 文字と一致
6. (オプション) **コメント**を追加します。
7. **[大文字と小文字を無視** する] (大文字と小文字を同一の文字として処理する) かどうかを選択します。
8. **[除外]** をクリックします。

除外されたシークレットの表示と管理

検出結果からシークレットを除外するした後、特定のポリシーで除外されたすべてのシークレットを確認または管理することができます。これは、[Policies] ページから関連するポリシー内の **[Secret Exclusion]** タブに直接アクセスして実行できます。

ポリシーの除外されたシークレットを表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー]** > **[クラウドポリシー]** の順にクリックします。
2. **[Organization] (組織)** ツリーのドロップダウンから、関連するアカウント階層とフォルダーを選択します。
3. 確認するポリシーを見つけます。
4. ポリシーの横にある三点リーダーメニューアイコンをクリックし、**[編集]** をクリックします。
5. ポリシーエディターで、**[シークレットの除外]** タブをクリックします。
6. そのポリシーの除外されたシークレットのリストを確認します。次のことができます。
    - 必要に応じて、キー/値のパターンとコメントを表示し、除外を管理または削除します。
    - シークレットマスキングして非表示にします。

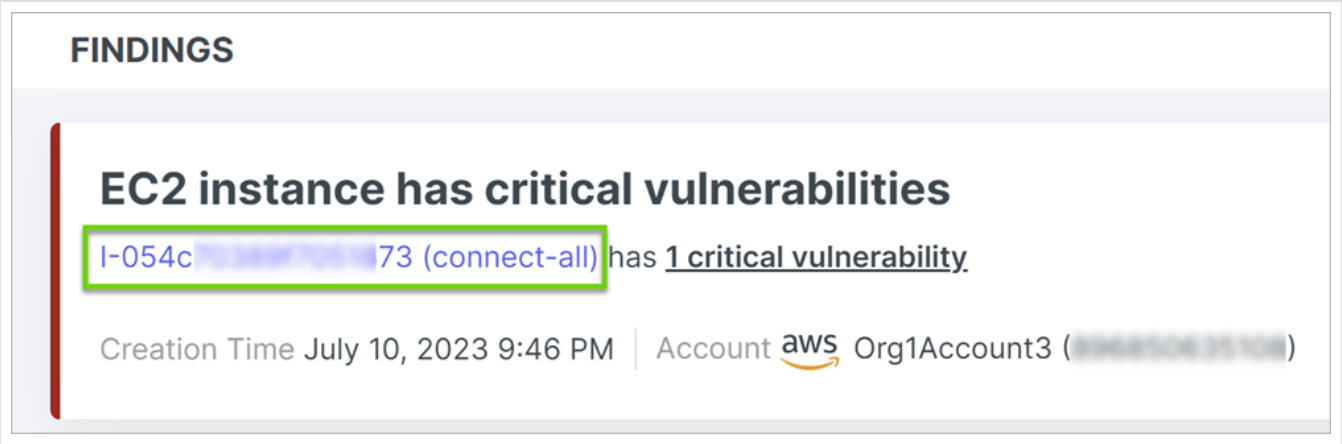
ソースコードの表示



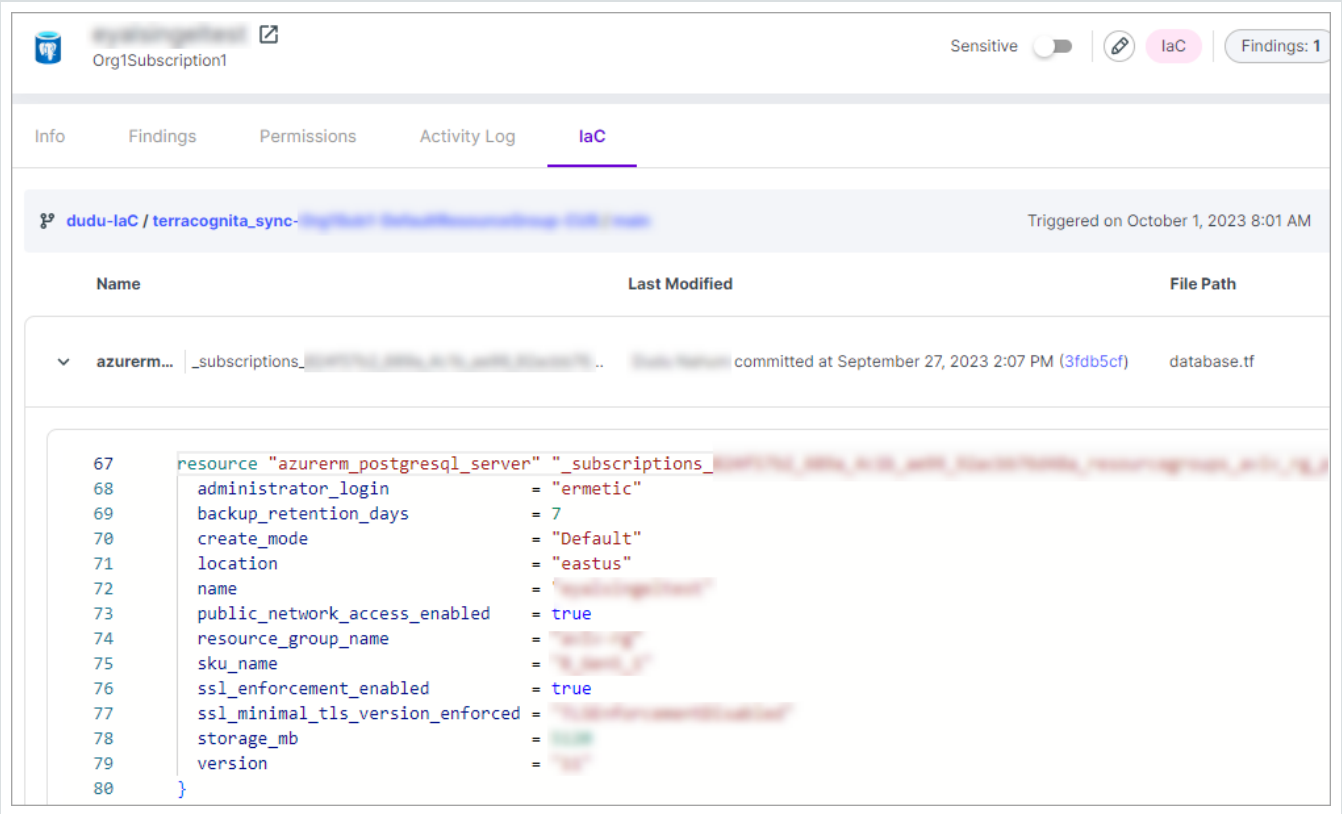
クラウドサイバーエクスポージャーは、あるリポジトリでコードによって管理されているものとして検出されたリソースに関連する検出結果にIaC組み込みシステムラベルを適用します。このような検出結果については、**[IaC]** タブをクリックして関連するコードスニペットを表示し、リソースをそのコードのオリジンまでトレースすることができます。

リソースソースを表示するには code:

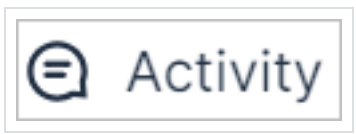
1. クラウドサイバーエクスポージャーコンソールで、**[リスク>クラウドの検出結果]** をクリックします。
2. ラベルフィルターから、その他の関連するフィルターとともにIaCを選択します。詳細については、「検出結果ページの操作」を参照してください。
3. クリックして関連する検出結果を開き、関連情報を分析します。
4. 検出結果のタイトルの下にある、影響を受けるリソースを特定してクリックします。



5. リソースページで、**[IaC]** タブをクリックします。
6. エントリを展開すると、リソースのソースコードが表示されます。



検出結果のアクティビティの表示



クラウドサイバーエクスポージャー内の検出結果のライフサイクルに関する情報を確認するには、検出結果のアクティビティを表示します。たとえば、次の場合を参照してください。

- 検出結果が作成されました。
- ステータスの変更 (システムによる、またはユーザーによる手動による)
- サードパーティ統合用にチケットが作成されました。

検出結果のアクティビティを表示する方法

1. 検出結果の表で、関連する検出結果をクリックします。
2. **[アクティビティ]** をクリックします。
3. (オプション) **コメントを書き**、**[保存]** をクリックします。

検出結果の修正

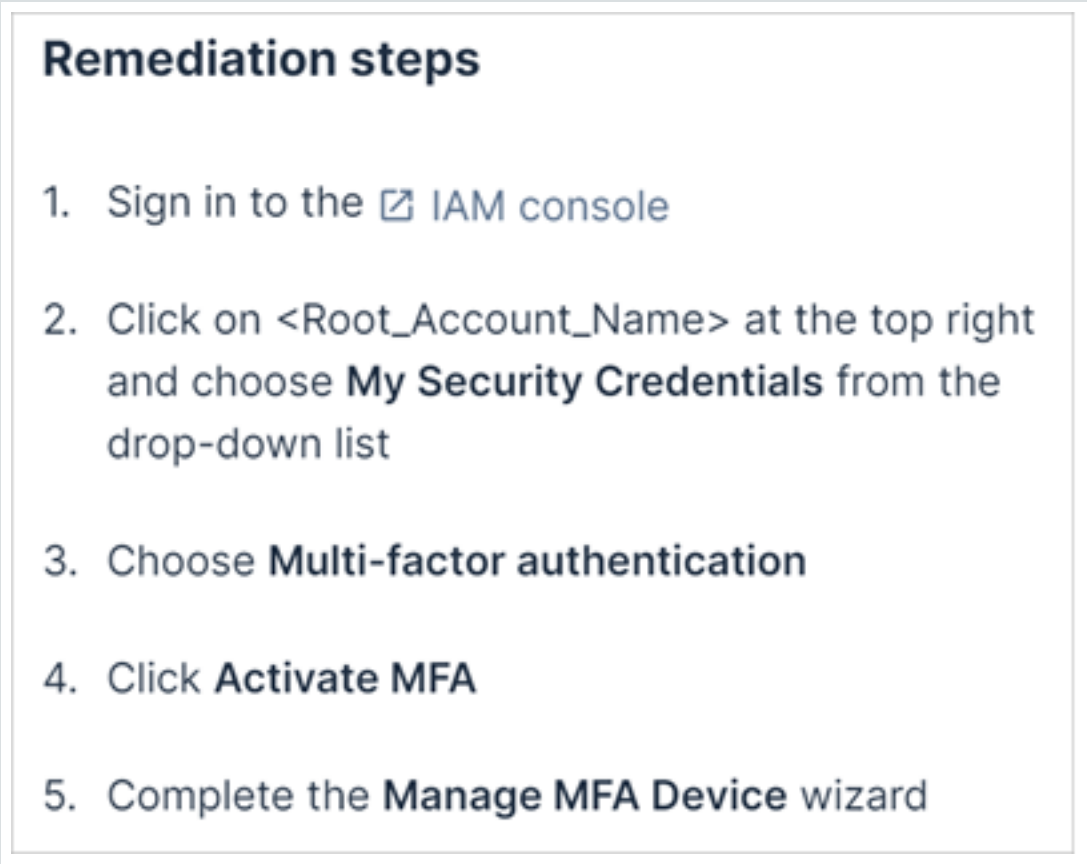
クラウドサイバーエクスポージャー検出結果を検出結果の自動修正クリックで自動修正したり、必要に応じて検出結果を手動で修正する修正を実行したりできます。

検出結果を手動で修正する

検出結果によっては、関連する問題をクラウドサイバーエクスポージャー以外で修正する方が、Tenable 検出結果の自動修正するよりも適切な場合があります。これは特に、Tenable により自動で実行された修正が開発者のコードで上書きされる可能性がある場合の、インフラのコード化 (IaC) ワークフローで役立ちます。修正されたポリシーの提案をアタッチすることで、Tenable の推奨事項をコーディング環境に合わせて直接実装できるようになります。

検出結果を手動で修正する方法

1. [検出結果] ページで、関連する検出結果をクリックしてオープンします。
2. **[修正]** 領域に移動します。
3. 修正 **手順** を 1 つずつ実行します。例:



4. 修正ステップに提案されたポリシー変更が含まれる場合、ステップの横に次のボタンの一部またはすべてが表示され、改訂されたポリシーをさまざまな形式で表示およびダウンロードしたり、古いポリシーと新しいポリシーを並べて差分ビューしたりできます。



- JSON
- Diff
- Terraform
- CloudFormation

開発者が手動でコードに適用できるように、これらの提案のコピーを開発者に送信 (たとえば、Eメール経由、検出結果に基づくアクションのトリガーによる添付ファイル) に送信することができます。

5. [検出結果を修正した後、手動でクローズし、Open Findings] (オープンの検出結果) ページから削除します。

検出結果の自動修正

クラウドサイバーエクスポージャー では、ボタン (*ワンクリック修正*) をクリックするだけで検出結果を自動的に修正して、リスク緩和のプロセスを効率化できます。Tenable では、クラウド環境内で関連する修正ステップをプロアクティブに実行することで、時間と労力を節約できます。これにより、脅威に迅速に対応できるようになります。自動修正は、それぞれのクラウドサービスプロバイダープラットフォーム内で段階的なアクティビティを必要とする手動修正の代替手段として機能します。

たとえば、過剰な権限を持つアイデンティティに関連する検出結果を自動的に修正し、過剰なアクセス許可と脆弱な設定を削除することができます。

注意: この機能は多くの検出結果で使用できますが、すべての検出結果に対応できるわけではありません。Tenable は継続的に検出結果タイプを追加し、サポートしていきます。詳細については、リリースノートを参照してください。

- アカウント接続中にクラウドサイバーエクスポージャー 管理アクセス許可 (オプション) を付与した場合は、この機能が利用可能なアカウントに関連付けられた検出結果であれば、追加の設定を行わなくても、自動的に修正できます。
- アカウント接続中にクラウドサイバーエクスポージャー 読み取り専用アクセス許可のみを付与した場合でも、検出結果を自動的に修正できますが、最初にワンタイム認証情報をTenableに提供する必要があります。

  注意: 管理アクセス許可が付与されている場合でも、ワンタイム認証情報を使用して自動修正するオプションは利用できます。

- (GCP)検出結果によっては、プロジェクトレベル (フォルダーレベルまたは組織レベル) より上のレベルで特定の修正手順を実行する必要があります。Tenable がプロジェクトレベルの管理アクセス許可のみを持っていて、組織レベルのアクセス許可を持たない場合は、1 回限りの認証情報を Tenable

に提供することで、Tenableこれらの手順も実行できるようになります。それ以外の場合は、Tenable ではアクセス許可がある修正手順のみが実行されます。

Microsoft Entra ID の変更を必要とする修正アクション (グループからのユーザーの削除など) は、Tenable に Microsoft Entra グループを管理するアクセス許可がないため (センシティブな性質のため)、自動的には実行されません。このような手順はすべて、Microsoft Entra 管理者が手動で実行する必要があります。自動修正プロセスを開始すると、このような手順がページに表示されますが、グレー表示されます。

検出結果を自動修正する方法

1. [検出結果] ページで、関連する検出結果をクリックしてオープンします。サポートされている検出結果の完全なリストについては、OTC による修正のサポート対象の検出結果 を参照してください。
2. **[修正]** 領域に移動します。
3. Remediate ボタンをクリックします。
4. さまざまなステップをクリックして、たとえば以下を行います。
    - 問題のリソースに関する詳細情報を表示する
    - 提案されたポリシー変更の表示と編集を行う。
    - 提案されたポリシー変更を編集する場合は、**[編集]** をクリックし、関連する変更を加えてから **[保存]** をクリックする。
    - アクセスキーを無効にするか削除するかを選択する (_IAM ユーザーの未使用の認証情報_ というポリシーによってトリガーされる検出結果の場合など)。
5. **[次へ]** をクリックします。
6. アカウント接続中にクラウドサイバーエクスポージャー 読み取り専用アクセス許可のみを付与した場合は、次の情報を入力することで、Tenableにワンタイム認証情報を入力する よう求められます。
    - AWS
        - **アクセスキー ID** (IAM ユーザーを対象)
        - **シークレットアクセスキー** (IAM ユーザーに関連)
        - **セッショントークン** (IAM ロールに関連)

- GCP
  - **アクセストークン**。必要なユーザー認証情報を使用して認証されている間に、Google Cloud CLI で次のコマンドを実行することで、トークンを生成します。

    ```
    gcloud auth print-access-token
    ```

    このコマンドの詳細については、関連する Google ドキュメント を参照してください。
  - **現在のセッションの認証情報を保存**するかどうかを決定します。
7. 適用される手順を確認し、**[適用]** をクリックします。

ワンタイム認証情報による修正

アカウントの接続中にクラウドサイバーエクスポージャー管理アクセス許可を付与する代わりに、Tenable が検出結果を自動的に修正できるようにする一時的なワンタイム認証情報を提供することもできます。

- AWS IAM ユーザーの場合、一時的な認証情報はアクセスキーの形式を取り、IAM ロールの場合、アクセスキーとセッショントークンの組み合わせになります。IAM ユーザー/ロールには、問題のアカウント内で特定の修正アクションを実行できるアクセス許可が必要です (多くの場合、管理アクセス許可が必要です)。必要なアクセス許可は検出結果によって異なる場合があります。
- GCP の場合、一時的な認証情報は、Google Cloud CLI を介して生成できるアクセストークンの形式を取ります。詳細については、検出結果の自動修正 を参照してください。

デフォルトでは、指定した認証情報は、入力した特定の検出結果の修正にのみ適用されます。現在のブラウザセッションの期間中持続するように認証情報を延長するには、検出結果ごとに認証情報を入力しなくても済むように認証情報を保存します。これにより、1) ブラウザウィンドウを閉じるか、2) クラウドサイバーエクスポージャーコンソールからログアウトするまで、認証情報を使用して他の検出結果を自動的に修正できます。Tenable では、複数のアカウントの認証情報の保存をサポートしています。

> **注意:** 認証情報を保存しない限り、認証情報はどこにも保存されないため、修正の完了後に安全に削除または取り消すことができます。

IaC を使用した検出結果の修正

IaC で検出されたクラウドサイバーエクスポージャーの検出結果を修正するために必要となる正確なコード変更を確認し、Tenable で開かれたプルリクエストを介して自動的にそれらを適用します。これにより、

関連するクラウドコンソールを介してデプロイした後ではなく、コード内で設定ミスを修正できるため、設定ミスの原因を簡単に特定できるようになります。

これは次のことに役立ちます。

- 設定ミスの根本原因を簡単に特定
- 開発者が追加のチケットを処理する代わりに、日常的なツールを使用できるようにします
- 大規模な問題解決
- IaC セキュリティのベストプラクティスに従う

前提条件

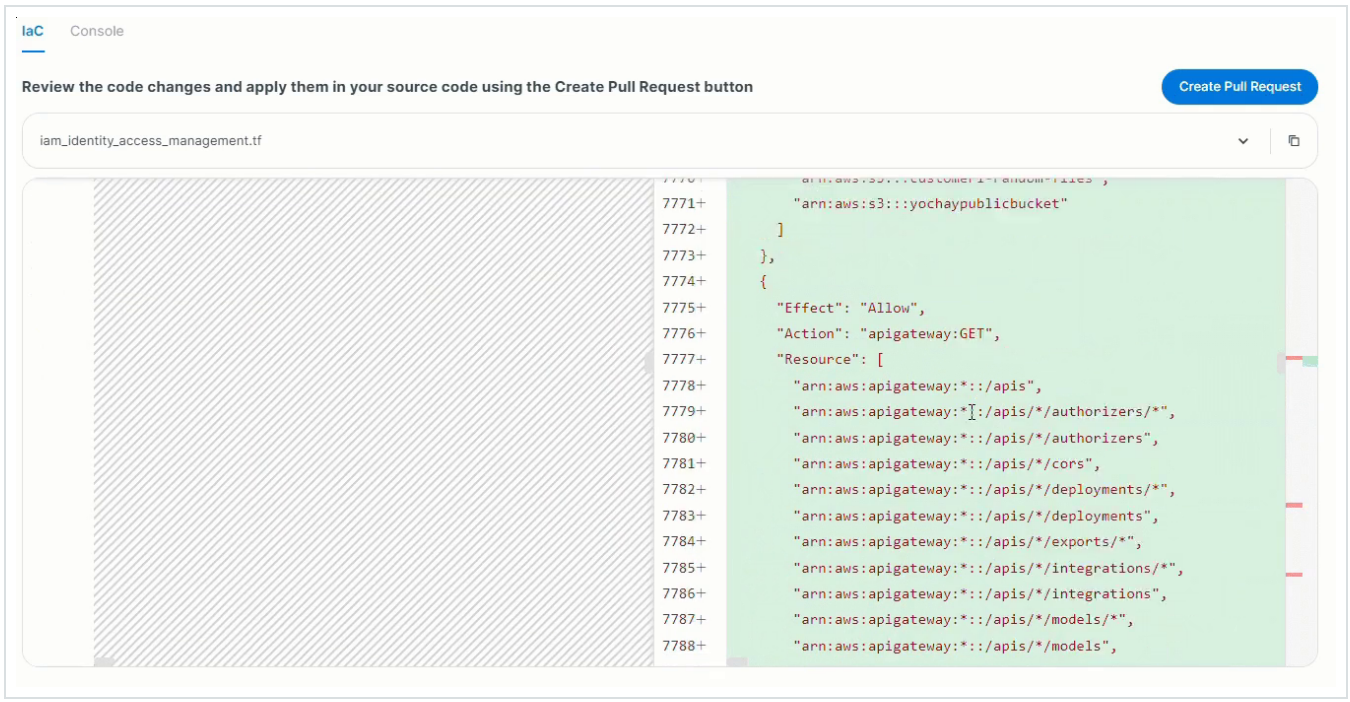
- コードリポジトリの接続や CI/CD の接続 の接続
- クラウドサイバーエクスポージャー ユーザーには、関連する IaC スコープへのアクセス権が必要です。詳細については、「 ユーザーとグループ 」を参照してください。
- サポートは現在、以下のツールで管理されているリソースで利用できるものです。
    - クラウド: **AWS/Azure/GCP** (サポートされているポリシー
    - コードフレームワーク: **Terraform**

コード変更の確認

IaC で検出されたクラウドサイバーエクスポージャー検出結果を修正するために必要となる正確なコード変更を表示します。

IaC コードの変更を確認するには

1. [検出結果] ページで、関連する検出結果をクリックします。利用可能な検出結果タイプのリストについては、サポートされているポリシー 。
2. 検出結果のプロファイルビューで、[Remediation] をクリックします。
3. **[IaC]** タブをクリックします。
4. コード差分を確認して、コード変更の推奨事項を確認します。右側にある赤/緑のインジケーターをクリックすると、関連するコードスニペットに素早く移動できます。



5. [ ] をクリックして、修正したコードファイルをコピーします。

次のステップ: プルリクエストを使用して検出結果を修正するする

プルリクエストを使用して検出結果を修正する

必要な変更を含むプルリクエストを作成して、コードの設定ミスを修正します。

> **重要: 重要な注意事項**:
>
> - プルリクエストによる検出結果の修正は、関連するコードリポジトリを クラウド サイバーエクスポージャー に接続している場合にのみ利用できます。
> - このアクションを実行するには *ラボレータまたは管理者* ロールが必要です。詳細については、「ユーザーとグループ」を参照してください。
> - **Bitbucket**: Bitbucket の既知の制限により、プルリクエストを介した IaC 検出結果の修正は、2.5MB 未満のファイルに対してのみ可能です。

プルリクエストを使用して IaC の検出結果を修正する方法

1. コード変更の確認。
2. **[Create Pull Request]** をクリックします。

3. 左側のさまざまなステップをクリックして、たとえば以下を行います。
    - 問題のリソースに関する詳細情報を表示する
    - 提案されたポリシー変更を表示する
4. **[次へ]** をクリックします。
5. プルリクエストの詳細を入力します。
    - **コミットメッセージ**を入力するか、自動生成されたデフォルトメッセージを使用します。
    - 説明 **を入力するか**、自動生成されたデフォルトメッセージを使用します。
    - プルリクエストの作成後 7 日間、検出結果をスヌーズするかどうかを選択します。
6. **[作成]** をクリックします。

成功ダイアログのリンクをクリックして、プルリクエストにアクセスします。プルリクエストが承認された後、変更は次のリリースでクラウドに展開され、クラウドサイバーエクスポージャー の検出結果のステータスは [Resolved] (解決済み) に変更されます。

サポートされているポリシー

現在、以下の Tenable Cloud 組み込みポリシー がサポートされています (IaC ポリシーではありません)。

AWS

- IAM ユーザーの未使用パスワード
- IAM ユーザーの未使用アクセスキー
- 非アクティブな IAM ユーザー
- 非アクティブな IAM ロール
- 過剰な権限を持つ IAM グループ
- 過剰な権限の IAM ユーザー
- 過剰な権限の IAM ロール
- 過剰な権限の SSO アクセス許可セット
- 未使用の SSO アクセス許可セット
- 未使用のセキュリティグループ

Microsoft Entra ID

- サブスクリプションで非アクティブな Microsoft Entra ID アプリケーション
- サブスクリプションで非アクティブな Microsoft Entra ID ユーザー

GCP

- 非アクティブなサービスアカウント

Google Workspace

- 無効な Google Workspace ユーザー

参照: データの検出

このセクションでは、データの検出に関連する詳細な参照情報を提供します。

リソース削除の推奨事項を伴う検出結果

次の検出結果タイプには、ポリシールールに違反するリソースを削除するための推奨される修正手順が含まれます。リソースが削除された場合、関連する検出結果のサブステータスは、[Resource deleted] (リソースの削除) ではなく、[Fixed] (修正済み) とマークされます。

- 未使用のセキュリティグループ
- 未使用の SSO アクセス許可セット
- 未使用の GCP プロジェクト
- 非アクティブな IAM ロール
- 非アクティブな IAM ユーザー
- サブスクリプションで非アクティブな Microsoft Entra ID アプリケーション
- サブスクリプションで非アクティブな Microsoft Entra ID ユーザー
- サブスクリプションで非アクティブなマネージド ID
- プロジェクトで非アクティブなサービスアカウント
- プロジェクトで非アクティブなユーザー

自動解決されない検出結果タイプ

以下の検出結果タイプ (ポリシー) は、クラウドサイバーエクスポージャーによって自動的に**[クローズ (修正済み)]**とマークされます。

クラウド	カテゴリ	ポリシー
AWS	IAM	新しい特権アイデンティティ
		ルートユーザーアクティビティが検出されました
	異常検出	異常なデータアクセス
		異常なネットワークアクセス管理
		異常なアクセス許可管理
		異常な権限昇格
		異常な偵察
Azure	IAM	サブスクリプションの新しい特権アイデンティティ
	管理	新しい Azure サブスクリプション
	異常検出	異常なネットワークアクセス管理
		異常なアクセス許可管理
GCP	IAM	プロジェクトでの新しい特権アイデンティティ
	管理	新しい GCP プロジェクト
	異常検出	異常なアクセス許可管理

削除された検出結果

一般に、検出結果は解決した後でも、クラウドサイバーエクスポージャー内で制限なくアクセスできます。ただし、検出結果がクラウドサイバーエクスポージャーから削除されることがあります。以下は、検出結果が削除される理由の一部をまとめたリストです。

理由	説明	例
誤検出	Tenableは、誤検出のために誤って作成された検出結果を削除しました。注: Tenableは、できる限り誤検出を回避できるよう、識別メカニズムを継続的に改善しています。	シークレットの漏洩に関連する検出結果: 文字列が誤ってシークレットとして識別された場合。たとえば、文字列 `rds_pass_reference_id` がただのパスワードのリファレンスであっても、パスワードとして識別されるなどです。
ポリシー集約ロジックの変更	Tenableは、同じ問題を持つすべてのリソースを集約した単一の検出結果ではなく、リソースごとに個別の検出結果を作成するように検出結果を修正しました。この場合、元の集約された検出結果は削除されます。	パブリックEC2インスタンス
ポリシー評価ロジックの変更	Tenableは、精度を向上させるために検出結果のロジックを修正し、検出基準を追加しました。この場合、以前作成された一部の検出結果が削除されることがあります。	無効化された自動ローテーションに関連する検出結果: Tenableは、作成されてから1か月以上経過したリソースだけを検出するように検出結果の論理を改善しました。

OTCによる修正のサポート対象の検出結果

自動修正は次の検出結果に対して利用できます。

プロバイダー	ポリシー
AWS	IAM ユーザーの未使用アクセスキー
	IAM ユーザーの未使用パスワード
	非アクティブな IAM グループ
	非アクティブな IAM ロール
	非アクティブな IAM ユーザー
	過剰なアクセス許可のある ECR リポジトリ
	過剰なアクセス許可のある S3 バケット
	過剰なアクセス許可を持つ Secrets Manager シークレット
	過剰な権限を持つ IAM グループ
	過剰な権限の IAM ロール
	過剰な権限の IAM ユーザー
	過剰な権限の SSO アクセス許可セット
	未使用のアクセス許可セットの割り当てを持つ SSO グループ
	未使用のアクセス許可セットの割り当てを持つ SSO ユーザー
	未使用の SSO アクセス許可セット
	未使用のセキュリティグループ
	VPC エンドポイントがデフォルトの IAM ポリシーを使用している (以前の「過剰なアクセス許可を持つ VPC エンドポイント」)
Azure	非アクティブなマネージド ID

プロバイダー	ポリシー
	サブスクリプションで過剰な権限を持つ Microsoft Entra ID アプリケーション
	サブスクリプションで過剰な権限を持つ Microsoft Entra ID グループ
	サブスクリプションで過剰な権限の Microsoft Entra ID ユーザー
	サブスクリプションで過剰な権限を持つマネージド ID
GCP	無効なサービスアカウント
	プロジェクトで過剰な権限を持つ Google Workspace グループ
	プロジェクトで過剰な権限のサービスアカウント
	プロジェクトで過剰な権限を持つユーザー
Google Workspace	無効な Google Workspace サーバー
Microsoft Entra ID	無効な Microsoft Entra ID アプリケーション
	無効な Microsoft Entra ID ユーザー

IaC 検出結果

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

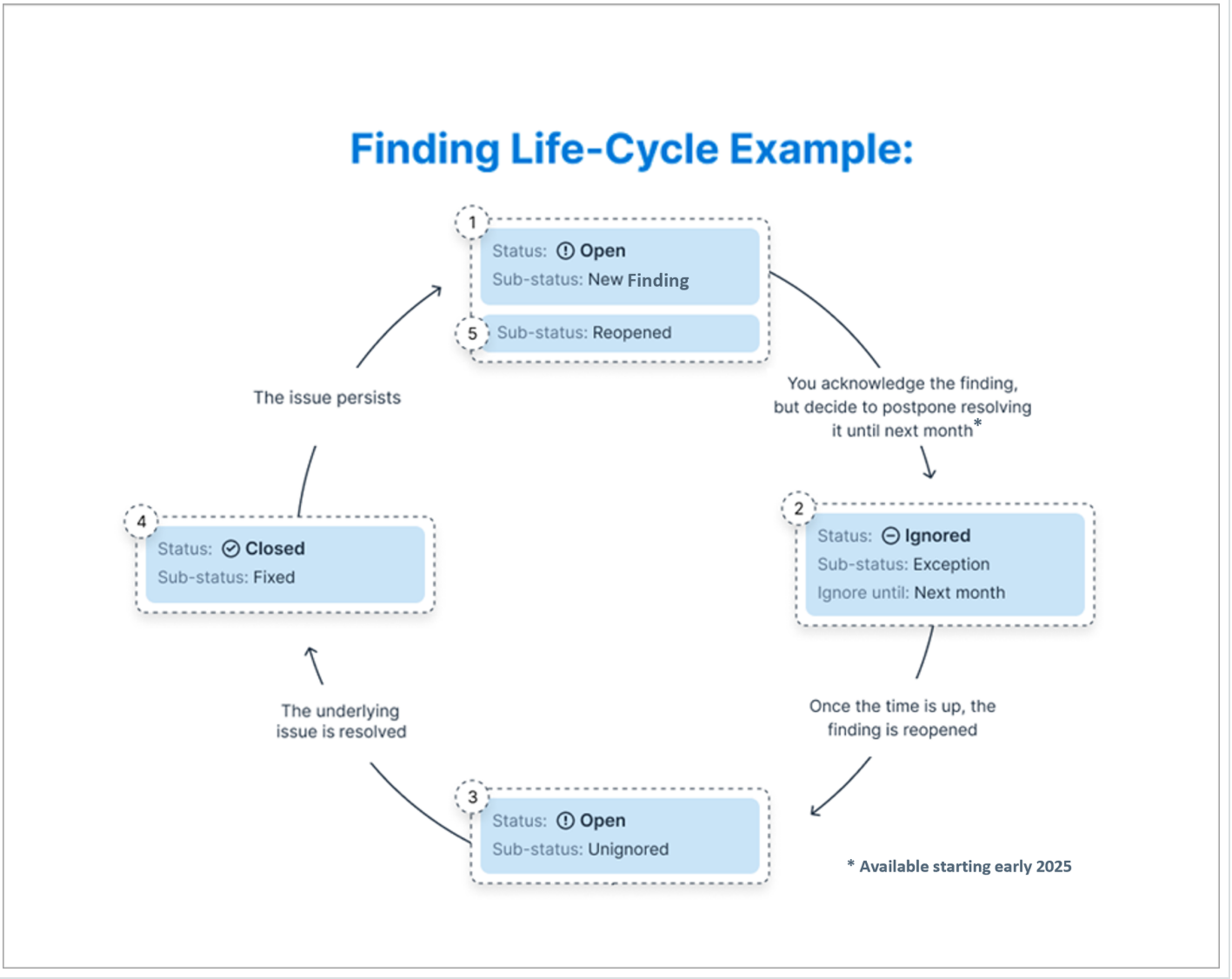
これは、IaC 検出結果を表示および管理するためのハウツーガイドです。

- 検出結果の深刻度の仕組みの概念概要については、「検出結果の深刻度」を参照してください。
- 検出結果の作成方法を設定するには、IaC ポリシーを参照してください。

IaC の検出結果ページを使用して、コード内の検出結果のトリアージを効果的かつ効率的に実行できます。たとえば、特定のコンプライアンスを満たさない検出結果を検出して修正できます。Tenable One Cloud Exposure 、インフラのセキュリティに対して予測されるリスクをもたらす、コードリポジトリ内の状況を特定します。これらの *検出結果には* 、見つけるのが難しい危険な組み合わせを含む、リスクのあるアイデンティティやリソースが表示されます。

検出結果ライフサイクルの例

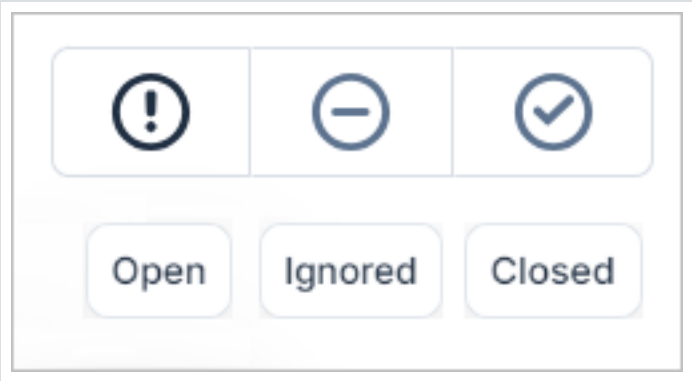
この画像は、環境内で検出された検出結果のフローと進行状況の例を示しています。特定のステータスとサブステータスの詳細については、検出結果のステータスを参照してください。



IaC 検出結果ページの操作

IaC の検出結果ページでは、現在のステータスによって検出結果がグループ化されます。

- 未解決の検出結果。環境内のすべてのアクティブな検出結果を表示します。
- 無視無視した検出結果 今すぐ処理しなくてもよい検出結果が表示されます。関連するリソースは永久に、または設定された期間、除外されます。
- 解決済みの検出結果。手動または Tenable によって自動でクローズされた検出結果が表示されます。



注意:

- オープンまたは無視の検出結果は、クラウド環境に対する潜在的な脅威の深刻度順に一覧表示されます。
- 複数の検出結果の深刻度が同じ場合でも (たとえば「高」)、テーブルの上位に表示される検出結果は、Tenable によってより高いリスクをもたらすと評価されたものです。

これらは IaC 検出結果ページで利用できる主なナビゲーション要素です。これらの要素を使用することで、結果を絞り込んで整理できるため、探している結果を見つけやすくなります。

項目	説明
ステータス別の表示	オープン、無視、またはクローズの検出結果を表示します。

項目	説明
深刻度	検出結果のリスク検出結果の深刻度 表示。デフォルトビューで検出結果を絞り込むために使用されます ([Group by] (グループ別) が適用されていない場合)。
ステータス/サブステータス列 / フィルター	「 IaC 検出結果のステータスを参照してください。
すべて選択	(適用されたフィルターに応じて) すべての検出結果を選択することにより、一括操作を実行しやすくなります。たとえば、特定のグループの検出結果を手動でクローズしたい場合などに便利です。ただし最大 1 万件の検出結果に限られます。
フィルター	使用できるフィルターはページによってやや異なりますが、以下のフィルターがあります。 • 作成時刻 • 深刻度 • ポリシー • リポジトリ • リソース名 • カテゴリ • リソースタイプ • ファイルコンプライアンス • スター付き
次でグループ化	検出結果を次の基準でグループ化 • **します。リポジトリ**。属するリポジトリに従って、すべての検出結果をグループ化 • **ポリシー**。検出結果をトリガーしたポリシーに従って、すべての検出結果を

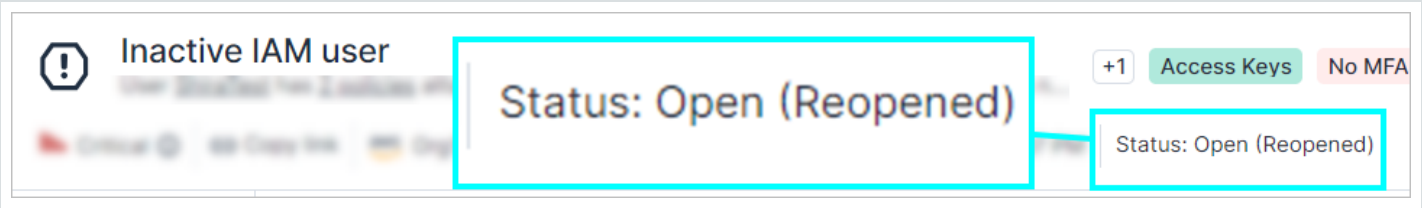
項目	説明
	グループ化 どちらのフィルターも、グループに含まれる深刻度の高い検出結果の割合に基づいた順番で、グループ分けされた検出結果が一覧表示されます。たとえば、75% が深刻度「重大」である検出結果グループは、100% が深刻度「高」である検出結果グループの前に表示されます。
スターを付ける	後で確認するのを忘れないように、重要な検出結果にスターを付ける。
アクション	**無視** • **検出結果を手動でクローズする** • る。検出結果を無視するする。 • **コメント** • **メールで共有**します。検出結果の情報を 1 つ以上のメールアドレスに送信します。 • **Jira 課題の作成/更新、または ServiceNow インシデントの作成/更新。** チケット統合がインストールされている場合利用できます。詳細については、検出結果に基づくアクションのトリガーを参照してください。
一括アクション	複数の検出結果に一度にアクションを適用します。
列ピッカー	テーブルに表示する列を選択します。

IaC 検出結果のステータス

検出結果のステータスを確認することで、以下の 2 点を把握しやすくなります。

- 組織におけるリスクの全体的な状態 (ウィジェットの [トレンド] ウィジェット)。
- 特定の検出結果がオープン/クローズされた理由。これは、行った作業と、検出結果の解決とクローズまでの進行状況を追跡するのに役立ちます。

ステータスは、メイン **のステータス** (オープン/無視/クローズ) とサブステータスで構成されます。サブ **ステータス**には詳細情報と、検出結果が現在のステータスである理由が記載されています。この例では、ステータスが「オープン」、サブステータスが「再オープン」になっています。



未解決の検出結果

未解決の検出結果は、環境内で検出されたアクティブな問題を表しています。これには、リスクのあるアイデンティティやリソース、見つけるのが難しい有害な危険な組み合わせが含まれます。

この表は、オープンの検出結果のサブステータス一覧です。サブステータスには詳細情報と、検出結果が現在のステータスである理由が記載されています。

サブステータス	定義
新しい検出結果	ポリシー違反があり、検出結果がトリガーされました。
再開されました	検出結果が **[クローズ]** から **[オープン]** に移行しました。 • システム - 問題が解決していない。以前解決したが再び発生。 • 手動 - 検出結果は検出結果を手動でクローズするが、ユーザーが手動で再オープンしました。
無視されていません	**無視**から**オープン**に移行した検出結果: • 有効期限日が過ぎました。 • ユーザーが手動で除外を削除した。

無視した検出結果

無視された検出結果は、すぐに処理しなくてもよい問題を表します。関連するリソースは永久に、または設定された期間、除外されます。

この表は、無視の検出結果のサブステータス一覧です。サブステータスには詳細情報と、検出結果が現在のステータスである理由が記載されています。

直ちに実装される除外の変更、またはリソースを除外するには、**[IaC Findings] (IaC の検出結果)** ページでオープンの検出結果を無視することができます。

検出結果を無視する から、または 除外 ことで、検出結果を無視できます。

サブステータス	定義
例外	検出結果がユーザーによって例外としてマークされたか、またはポリシー ポリシーからリソースを除外するコードファイルが除外されました。
誤検出	検出結果がユーザーによって誤検出としてマークされました。
設計上	検出結果がユーザーによって「設計による」としてマークされました。

解決済みの検出結果

クローズの検出結果は、ユーザーによって手動で、またはTenableによって自動でクローズされた問題を表しています。

この表は、クローズの検出結果のサブステータス一覧です。サブステータスには詳細情報と、検出結果が現在のステータスである理由が記載されています。

サブステータス	定義
修正	検出結果は解決されました

サブステータス	定義
済み	• : リソースがポリシールールと一致しなくなった。 • Tenable のポリシーの推奨事項に従って、リソースが削除された。たとえば、アクティブでない GCP サービスアカウントが削除された場合など。関連する検出結果タイプの一覧については、リソース削除の推奨事項を伴う検出結果 を参照してください。
誤検出	検出結果が Tenable によって誤検出としてマークされました。
手動で閉じられました	ユーザーが検出結果を手動で「クローズ」としてマークしました。

IaC 検出結果の管理

次のアクションを使用して、リストの検出結果のステータスを管理および変更します。

- 検出結果を手動でクローズする。検出結果を手動でクローズする
- 検出結果を再オープンするします。手動でクローズされた検出結果を再オープンする。
- **スター**。後で確認するのを忘れないように、重要な検出結果にスターを付ける。
- 検出結果に基づくアクションのトリガーします。メール、Webhook、またはチケッティング統合を使用して、検出結果を手動で共有する。
- 検出結果データをエクスポートします。環境内の検出結果のサマリーレポートを作成する。

検出結果テーブルから、または検出結果をドリルダウンした後に、これらの操作を実行できます。検出結果をドリルダウンした後にのみ修正が可能です。

検出結果の詳細の表示

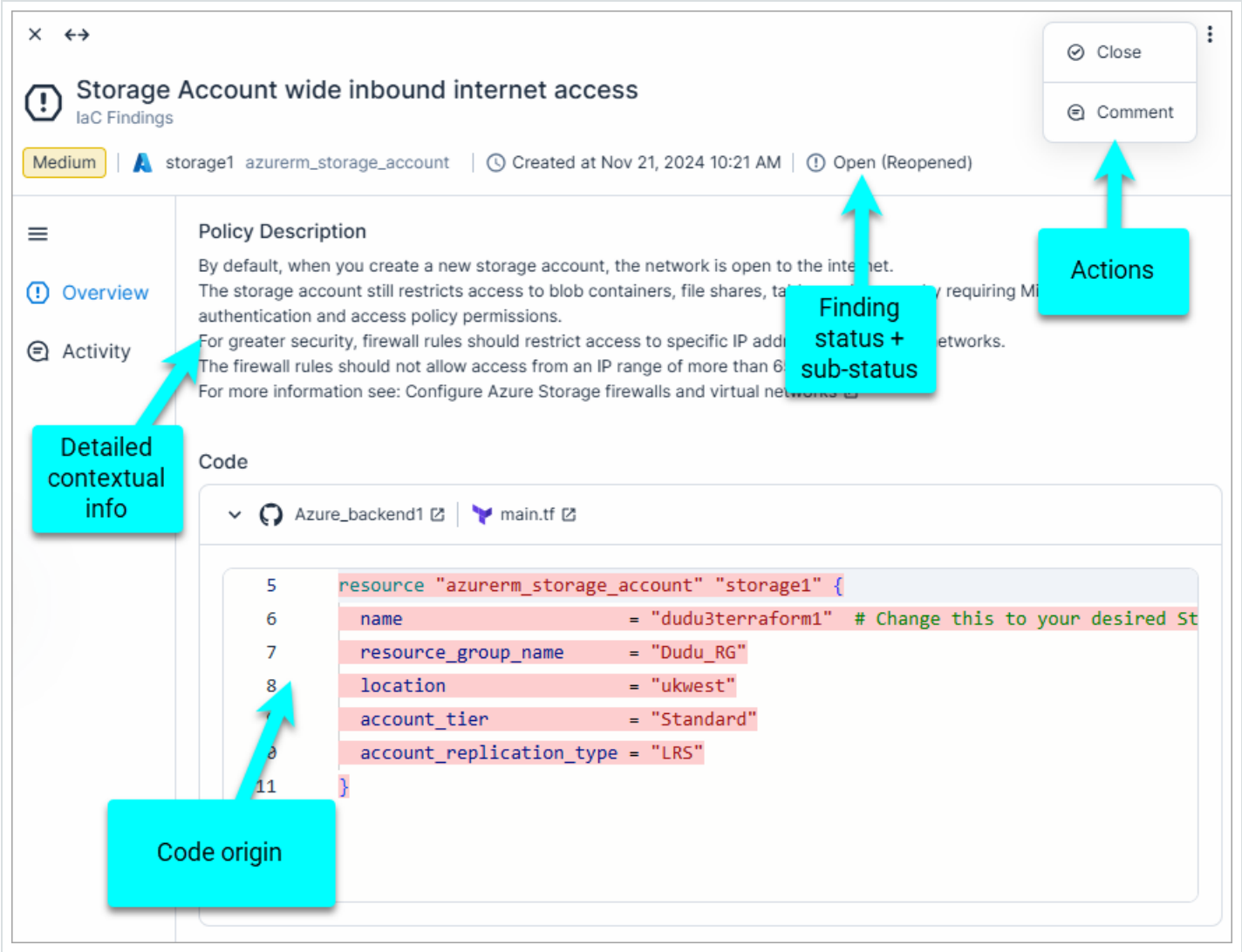
検出結果をクリックして詳細な情報を表示し、それに関連するリスクを修正します。イベントの詳しい履歴説明、イベントがもたらす潜在的なリスクの幅広い根拠、具体的な修正手順が表示されます。各検出結果には、検出結果の種類に応じたさまざまな情報と、検出結果の作成をトリガーした具体的な状況が表示されます。

以下のような検出結果の詳細情報とその他の関連情報を確認して、理解を深めます。

- 検出結果の根本的な原因
- 検出結果の範囲
- 環境にもたらされる潜在的なリスク

> **注意:** カスタムポリシー違反は最初の１万件の結果に制限されます。

検出結果の例



検出結果を手動でクローズする

コード内の潜在的なセキュリティの問題を解決すると、検出結果はクラウドサイバーエクスポージャーコンソールで自動的に**[クローズ (修正済み)]**とマークされます。ただし、一部のケースでは、オープンまたは無視の検出結果を**手動でクローズ**したい場合もあります。たとえば、検出結果が自動的に解決済みとマークされるまでに時間がかかることがあります。その場合、手動でクローズすると[IaC Findings] (IaC の検出結果) ページからすぐに削除できます。

検出結果を手動でクローズすると、検出結果は**[クローズ (手動でクローズ)]**とマークされます。ただしこれを行った場合、問題は実際には修正されておらず、次回データの同期と更新の頻度するときに、検出結果のステータスは**[Open (Reopened)] (オープン (再オープン)) に戻ります**。

クローズの検出結果をマークして表示する方法

1. IaC 検出結果テーブルから以下を行います。
    1. 単一の検出結果: 各検出結果の横にある三点リーダーアイコンをクリックし、**[閉じる]** をクリックします。
    2. 複数の検出結果: 複数の検出結果を選択し、下部にある **[閉じる]** をクリックします。
2. [Close Finding] (検出結果のクローズ) ダイアログで、クローズの理由を示すコメントを追加します。これは検出結果のアクティビティに追加されます。
3. **[Close]** (閉じる) をクリックします。
4. クローズされたすべての検出結果を表示するには、**[リスク > IaC 検出結果] > [クローズ]** に移動します。

検出結果を再オープンする

検出結果を手動でクローズするした検出結果は再度オープンできます。入力すると、検出結果は **[Open (Reopened)] (オープン (再オープン)**) とマークされます

検出結果を再オープンする方法

1. 検出結果の表から以下を行います。
    1. 単一の検出結果: 各検出結果の三点リーダーアイコンをクリックし、**[Open]** をクリックします。
    2. 複数の検出結果: 複数の検出結果を選択し、下部にある **[オープン]** をクリックします。
2. [Open Finding] (検出結果のオープン) ダイアログで、再オープンの理由を示すコメントを追加します。これは検出結果のアクティビティに追加されます。
3. **[開く]** をクリックします。
4. 再オープンされたすべての検出結果を表示するには、**[リスク>] [IaC 検出結果 > オープン]** に移動してから、サブステータスを **[再オープン]** でフィルタリングします。

検出結果データのエクスポート

検出結果データをエクスポートして、環境内の検出結果のサマリーレポートを作成します。データは、その時点でテーブルに適用されているフィルターに従ってエクスポートされます。出力データはCSV形式で、関連する検出結果データをすべて含みます。

たとえば、次のことが可能です。

- クローズの検出結果すべてを対象とするレポートを作成できます。これにはクローズの理由に関するサブステータス情報 (たとえばリソースの削除) を含めることができ、企業の関連するステークホルダーにレポートを共有できます。
- オープン/スター付き/無視の検出結果、または検出結果の他のサブセット (フィルターを使用) のレポートを作成できます。

検出結果のレポートを作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク> IaC 検出結果]** ページ ([オープン]/[無視]/[クローズ]) に移動します。
2. (オプション) 追加のフィルターを適用して、ニーズに合わせて検出結果のリストを絞り込みます。
3. **[Export]** をクリックします。CSV サマリーレポートが作成されます。
4. 特定のポリシータイプのデータをエクスポートする方法
    1. **[グループ化]** ドロップダウンをクリックし、**[ポリシー]** をクリックします。
    2. 関連するタイプをクリックして、セクションを展開します。たとえば、過剰な権限を持つIAMグループをクリックします。
    3. セクション右上の [Export] (エクスポート) ボタンをクリックします。

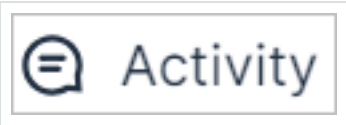
定期レポートの作成

[IaC 検出結果] ページから直接、スケジュールされたレポートを作成します。このページのレポートの内容は、テーブルに適用した特定のフィルターに基づきます。出力データはCSV形式で、クラウドサイバーエクスポージャーコンソールの各リソースページのURLなど、関連するリソースデータがすべて含まれます。

スケジュールされたレポートの作成方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク> IaC の検出結果]** に移動します。
2. 関連する資産インベントリのフィルタリングを適用します。
3. テーブルの右上にある **[Create Scheduled Report]** ボタンをクリックします。
4. レポートの詳細を入力します。詳細については、「レポート を参照してください。
5. **[スケジュール]** または **[生成]** をクリックします。
6. [Reports] (レポート) ページでレポートの詳細情報を確認できます。

検出結果のアクティビティの表示



クラウドサイバーエクスポージャー内の検出結果のライフサイクルに関する情報を確認するには、検出結果のアクティビティを表示します。たとえば、次の場合を参照してください。

- 検出結果が作成されました。
- ステータスの変更 (システムによる、またはユーザーによる手動による)
- サードパーティ統合用にチケットが作成されました。

検出結果のアクティビティを表示する方法

1. 検出結果の表で、関連する検出結果をクリックします。
2. **[アクティビティ]** をクリックします。
3. (オプション) **コメントを書き** 、**[保存]** をクリックします。

削除された検出結果

一般に、検出結果は解決した後でも、クラウドサイバーエクスポージャー内で制限なくアクセスできます。ただし、検出結果がクラウドサイバーエクスポージャーから削除されることがあります。以下は、検出結果が削除される理由の一部をまとめたリストです。

理由	説明	例
誤検出	Tenable は、誤検出のために誤って作成された検出結果を削除しました。注: Tenable は、可能な限り誤検出を回避できるよう、識別のメカニズムを継続的に改善しています。	シークレットの漏洩に関連する検出結果: 文字列が誤ってシークレットとして識別された場合。たとえば、文字列 `rds_pass_reference_id` がただのパスワードのリファレンスであっても、パスワードとして識別されるなどです。
ポリシー集約ロジックの変更	Tenable は、同じ問題を持つすべてのリソースを集約した単一の検出結果ではなく、リソースごとに個別の検出結果を作成するように検出結果を修正しました。この場合、元の集約された検出結果は削除されます。	パブリック EC2 インスタンス
ポリシー評価ロジックの変更	Tenable は、精度を向上させるために検出結果のロジックを修正し、検出基準を追加しました。この場合、以前作成された一部の検出結果が削除されることがあります。	無効化された自動ローテーションに関連する検出結果: Tenable は、作成されてから 1 か月以上経過したリソースだけを検出するように検出結果の論理を改善しました。

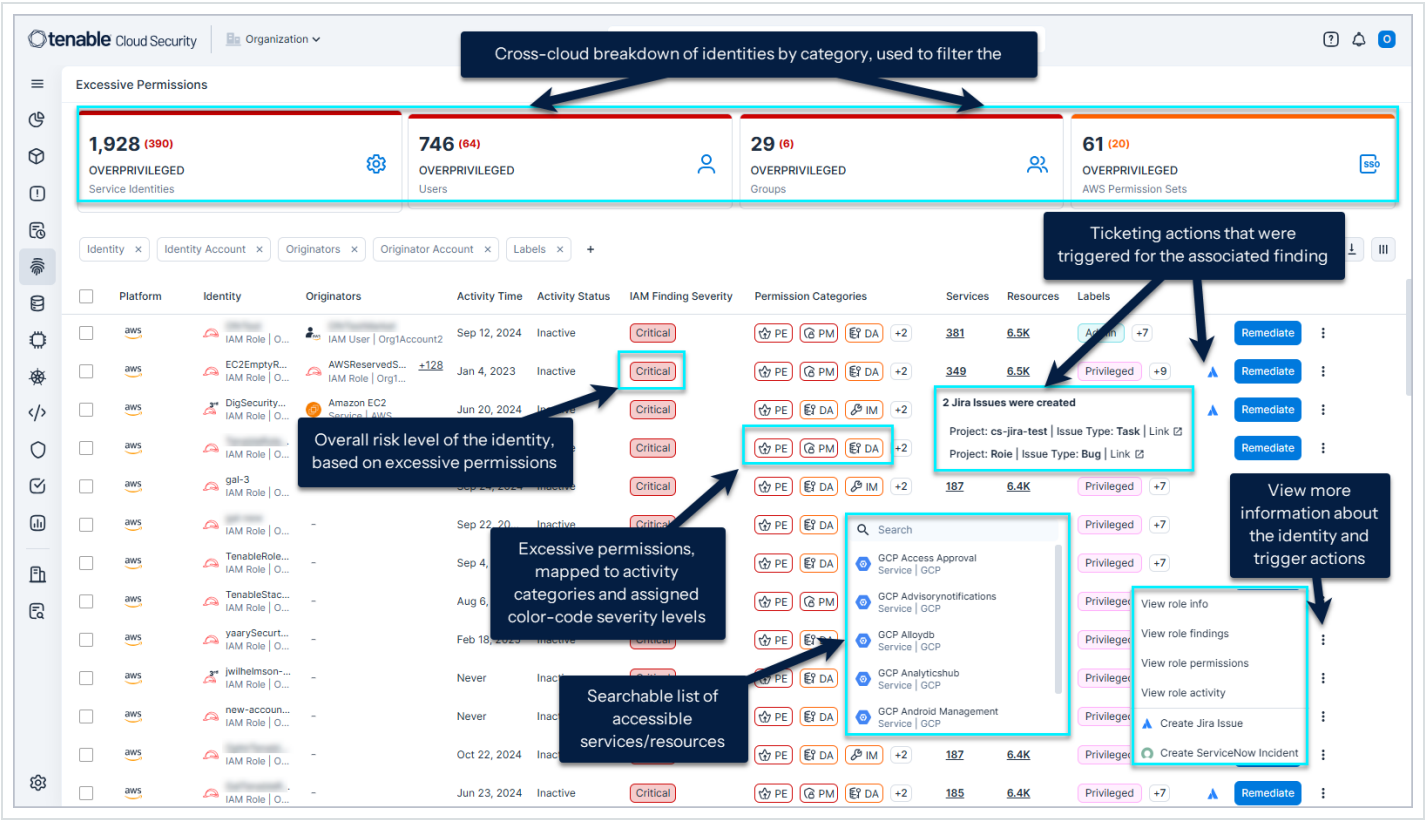
過剰なアクセス許可

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

[過剰なアクセス許可] ページを使用すると、環境で過剰な権限を持つアイデンティティに関する重要な情報を確認できます。たとえば、多要素認証が有効になっていない、過剰な権限を持つ非アクティブなユーザーをすべて表示することができます。

過剰なアクセス許可を管理するためのハウツーガイドです。

- 概念の概要については、過剰なアクセス許可と非アクティブなアイデンティティを参照してください。
- よくある質問については、「FAQ - IAM ガバナンスを参照してください。



過剰なアクセス許可を持つアイデンティティの表示

1. Tenable One Cloud Exposureコンソールで、**[過剰なアクセス許可のリスク>]** をクリックします。
2. ページ上部にあるウィジェットをスキャンすると、過剰なアクセス許可を持つアイデンティティの内訳がアイデンティティカテゴリ別に表示されます。これらのカテゴリは複数のクラウドを対象としており、クラウドサービスプロバイダー (CSP) に応じて特定のポリシーにマッピングされます。最初にアイデンティティの総数がリストされ、その後にリスクレベルが重大であるアイデンティティの数が赤で表示されます。
3. ウィジェットをクリックすると、そのアイデンティティカテゴリ別にテーブルがフィルタリングされます。デフォルトで、最もリスクの高い過剰なアクセス許可を持つカテゴリ (通常は、重大なアクセス許可の数が最も多いカテゴリ) 別に、テーブルは動的にフィルタリングされます。

4. テーブル内のデータのフィルタリングし、表示可能なデータの範囲を変更します。たとえば、**[Labels] (ラベル)** で **[No MFA] (MFA なし)** を選択すると、過剰なアクセス許可を持つが、多要素認証が有効になっていないアイデンティティをフィルタリングできます。テーブルで使用可能なデータの詳細については、アイデンティティ列データを参照してください。
5. アイデンティティが環境にもたらすリスクを分析します。「過剰なアクセス許可と非アクティブなアイデンティティ」を参照してください。
6. リソースの詳細の表示して、詳細な情報を表示します。
7. アイデンティティの横にある **[修正]** ボタンをクリックすると、それに関連付けられている過剰なアクセス許可の検出結果検出結果の自動修正されます。
8. アイデンティティの横にある三点リーダーをクリックして、そのアイデンティティに関する詳細情報を表示 (たとえば、そのアイデンティティに関連付けられているすべての検出結果を表示) したり、手動でアクションをトリガーしたりできます。

アイデンティティの列データ

[過剰なアクセス許可] ページの表には、次の列が表示されます。

縦棒	説明
プラットフォーム	アイデンティティが属するクラウドサービスプロバイダー。
名前	アイデンティティの名前。名前の下には、リソースのタイプとアカウント名が表示されます。
オリジネータ	アクセス許可が直接付与されるのではなく、問題となっているアイデンティティを引き受け、引き受けたアイデンティティのアクセス許可を使用して動作できるクラウドアイデンティティ (IAM ユーザー/ロール、IdP ユーザー、またはコンピューティングリソース)。たとえば、マネージド ID を使用してアクティビティを実行する Azure 仮想マシンや、アクションを実行するために AWS で IAM ロールを引き受ける Azure AD ユーザーなどがあります。
最後のアクティビ	このアイデンティティによって実行された前回のアクティビティ。

縦棒	説明
ティ	
アクティビティステータス	アイデンティティがアクティブであるか非アクティブであるかを示します。
IAM 検出結果の深刻度	アイデンティティに関連付けられている過剰な権限を持つ検出結果のリスクの深刻度。検出結果が複数のアカウントに存在する場合、最も高い深刻度が表示されます。
アクセス許可カテゴリ	詳細については アクセス許可の分析とリスクレベル 。
サービス	アイデンティティがアクセスできるサービスのうち、過剰と見なされるサービスの数。数字をクリックすると、サービスについて検索可能なリストが表示されます。
リソース	アイデンティティがアクセスできるリソースのうち、過剰と見なされるリソースの数。数字をクリックすると、リソースについて検索可能なリストが表示されます。
ラベル	手動による適用、タグに基づく自動適用、システムによる適用のいずれかにかかわらず、アイデンティティに適用されたすべてのラベルが表示されます。ラベルのタグにカーソルを合わせると、詳細を確認できます。リソースに複数のラベルがある場合、アイコンをクリックするとその他のラベルが表示されます。詳細は、ラベルのリソースへの適用 を参照してください。
修正	過剰なアクセス許可検出結果の自動修正します。

View more info (詳細情報の表示)/Manually Trigger Actions (縦三点リーダー ⋮)	• アイデンティティの詳細が表示されます。例:
	  • アイデンティティのリソースの詳細の表示
	  • アイデンティティに関連付けられているすべての検出結果
	  • アイデンティティのアクセス許可マッピングの視覚化
	  • アイデンティティのリソースアクティビティの調査
	• 検出結果に基づくアクションのトリガー

脅威検出

必要なライセンス: この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

Tenable One Cloud Exposure を使用して、クラウド環境における潜在的なセキュリティ脅威を検出し、調査できます。

脅威検出を表示する

脅威検出結果を表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク > 脅威の検出]** をクリックします。
   [脅威の検出] ページが表示されます。このページには、Tenable が特定したすべての潜在的な脅威が表示されます。この表のデータの詳細については、「脅威検出の列データ」を参照してください。
2. (オプション)**[グループ化]** ドロップダウンメニューを使用して、検出結果が表に表示される方法を整理します。
   - **ルール**: トリガーされた特定の検出ルールで検出をグループ化します。このビューでは、それぞれ固有のセキュリティルールの検出数と影響を受けているアカウントの合計数を確認できます。
   - **アカウント**: 接続されたクラウドアカウント別に検出をグループ化します。このビューは、潜在的な脅威の数が最も多い特定の環境を特定するのに役立ちます。
3. (オプション)テーブルをフィルタリングして、データの範囲を絞り込みます。
4. (オプション)テーブルに表示する列を選択するには、テーブルの右上にある列ピッカーアイコンをクリックします。
5. (オプション)フィルタリングされたデータをカンマ区切り値 (CSV) ファイルにエクスポートするには、**[エクスポート]** をクリックします。

脅威検出の列データ

次の表では、[脅威検出] ページで使用できる列とフィルターについて説明します。

列	説明
作成時間	Tenableが脅威を最初に検出した日時。
深刻度	脅威検出に割り当てられているリスクレベル(例: 重大、高、中、低)。
ルール	検出をトリガーした特定の脅威ルール。
アクター	疑わしいアクションを実行したエンティティ(ユーザーやサービスアカウントなど)。
アカウント	検出されたアクティビティが発生したクラウドアカウント。
ラベル	リソースに関連付けられたユーザー定義のタグまたはシステム生成のタグ。
IP アドレス	脅威アクターまたはアクティビティに関連付けられたソース IP アドレス。
クライアント	脅威検出に関与する特定のアプリケーションまたはサービス。
MITRE 戦術	MITRE ATT&CK フレームワークで定義されている、攻撃者の高レベルの目標。
MITRE テクニック	MITRE ATT&CK フレームワークで定義されている、目標を達成するためにアクターが使用する特定の方法。
リンク	このエントリをクリックして、選択した検出の脅威検出スライド式パネルを開きます。
アクティビティ	脅威の検出に関連するアクションと更新の監査 (コメントやチケットの作成など)。
チケット	この脅威検出にリンクされているサードパーティのサービスデスクチケット (Jira や ServiceNow など)。
スター付き	脅威検出をクイックアクセス用にお気に入りとしてマークしたかどうかを示します。

脅威検出の詳細を表示する

脅威検出をクリックすると、アクティビティに関する詳細な詳細が表示され、ランタイムクラウド環境内の特定のセキュリティイベントが調査されます。検出の運用サマリー、露出リスクの説明、関連するエンティティメタデータ、関連する履歴検出結果を表示します。各脅威検出には、その作成をトリガーした正確なAPI呼び出しまたはアクションに基づいた詳細情報が表示されます。

以下の詳細を使用して、以下を理解できます。

- 特定のクラウドアクティビティに関連する根本原因と露出リスク。
- 関連するエンティティのメタデータ(アクター作成タイムフレーム、ソースIPアドレス、使用されたクライアントなど)。
- 攻撃目標は、MITRE ATT&CKの戦術と手法に直接マッピングされます。
- アクティビティの影響を受けた特定のクラウドリソースと、関連するユーザーの関連する検出結果のより広範な履歴。

脅威ストーリー

> **必要なライセンス:** この機能は**Enterprise**ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

Tenable One Cloud Exposureを使用して、ワークロードやクラウド環境内での脅威ストーリーと呼ばれる潜在的なセキュリティインシデントをモニタリング、追跡、分析します。脅威ストーリーは、複数の関連するイベントや動作を統合して、クラウド環境における全体的な攻撃パターンの可視性を提供します。

脅威事例を表示する

脅威ストーリーの結果を表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>脅威ストーリー]**をクリックします。
   [脅威ストーリー]ページが表示されます。このページには、Tenableによって特定されたすべての潜在的な脅威が表示されます。この表のデータの詳細については、「脅威事例の列データ」を参照してください。
2. (オプション)テーブルをフィルタリングして、データの範囲を絞り込みます。たとえば、**[ステータス]**でフィルタリングすると、脅威ストーリーが[未解決]または[進行中]のみを表示できます。

3. (オプション)テーブルに表示する列を選択するには、テーブルの右上にある列ピッカーアイコンをクリックします。
4. (オプション)特定の脅威ストーリーをお気に入りに保存して、すばやくアクセスできるようにするには、その脅威ストーリーの行にある星のアイコンをクリックします。

脅威事例の列データ

列	説明
脅威ストーリー	関連するセキュリティイベントのわかりやすい名前
更新時間	脅威ストーリーに追加された最新のアクティビティのタイムフレーム
深刻度	脅威ストーリーに割り当てられたリスクレベル(重大、高、中、低など)
MITRE 戦術	MITRE ATT&CK フレームワークで定義されている、ストーリーに関与する攻撃者の高レベルの目標
MITRE テクニック	MITRE ATT&CK フレームワークで定義されている、攻撃者が目標を達成するために使用した特定の方法
攻撃者	IAM ユーザーやサービスアカウントなど、疑わしいアクションを実行したエンティティ
リソース	脅威ストーリーのアクティビティによって影響を受ける特定のクラウドリソース
ステータス	調査の現在の状態 ([未解決] や [進行中] など)
アカウント	検出されたアクティビティが発生した特定のクラウドアカウント
イベントオリジン	Tenable がアクティビティを検出したソースログまたはサービス
潜在的な影響	このアクティビティがセキュリティ状態に与える影響に関する説明

列	説明
スター付き	脅威のストーリーをお気に入りとしてマークしたかどうかを示します
ステータス更新時刻	脅威ストーリーのワークフローステータスが最後に変更された特定のタイムフレーム
サマリー	AI によって生成された、アクション、影響を受けるリソース、脅威ストーリーの範囲の概要説明
タイトル	検出に基づいて AI が生成したタイトル
判定	脅威ストーリーを調査した後に下された最終的な分析上の決定または結論

脅威事例の詳細を表示する

脅威ストーリーをクリックすると、アクティビティに関する詳細な詳細が表示され、ランタイム クラウド環境内に関連する検出とセキュリティ イベントが調査されます。検出結果の概要、セキュリティ上の影響の分析的説明、脅威の関係をマッピングする視覚的なグラフ、および基礎となる特定の検出を表示します。各脅威ストーリーには、その作成のきっかけとなった関連イベントからまとめられた包括的な詳細が表示されます。

以下の詳細を使用して、以下を理解できます。

- 関連するイベント全体に関係する特定のアクターとリソース。
- クラウドアカウントのセキュリティイベントのタイムラインと発生源。
- MITRE ATT&CK の戦術と手法に直接マッピングされる攻撃パターン。
- インタラクティブなビジュアルグラフによる、脅威アクター、脅威ストーリー、影響を受けるリソース間の関係。

脆弱性

アクティブなワークロードのうち、パッチ適用が必要な既知のソフトウェア脆弱性を持つものを特定します。関連するソフトウェアやオペレーティングシステムを更新するなど、パッチを適用するために必要なことを確認します。

> **注意:** Linux インスタンスでは、さまざまなフレーバーが利用できるため、OS パッケージの脆弱性検出は難しい場合があります。Tenable One Cloud Exposure は OS パッケージに関連する一般的な脆弱性リストを維持し、定期的に更新します。パッチ未適用の OS に関連する検出結果は、このリストの脆弱性に当てはまります。

これは、クラウドサイバーエクスポージャーの脆弱性を監視するためのハウツーガイドです。

- クラウドサイバーエクスポージャーのワークロード保護機能の概念概要については、「ワークロード保護を参照してください。
- 脆弱性を含むワークロード設定の構成に関するハウツーガイドについては、「ワークロード」を参照してください。
- よくある質問については、「FAQ: ワークロード保護」を参照してください。

すべての脆弱性を表示する

クラウドサイバーエクスポージャー環境のワークロードにインストールされたソフトウェアパッケージで検出されたすべての脆弱性を表示します。

脆弱性を表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>脆弱性]** に移動します。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、「脆弱性の列データ」を参照してください。

   > **注意:** テーブルは **[修正のみ]** で自動的にフィルタリングされるため、すぐに修正可能な脆弱性にすばやく集中できます。

3. 脆弱性をクリックすると、その脆弱性の詳細情報を含むビューが展開されます。詳細については、「脆弱性の詳細の表示」を参照してください。

脆弱性ページのソート順序

[脆弱性] ページのエントリは、次の優先順位で並び替えられます。

1. **深刻度** (降順)
2. **スコア** (選択スコアの降順 - CVSS または VPR)
3. **ID** (降順)

脆弱性の列データ

次の列は [脆弱性] ページのテーブルに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

列	説明
ID	脆弱性に関連する CVE ID (例: CVE-2021-3177)。 • ID にカーソルを合わせると、脆弱性の詳細 (説明や深刻度スコアなど) についての概要ビューが表示されます。 • ID をクリックするとスライド式パネルが開き、関連する脆弱性の詳細がすべて表示されます。 • 注意: 脆弱性のメインテーブルに記載されている CVSS スコアは脆弱性が検出されたソフトウェアパッケージ/OS バージョンのベンダーから取得したスコアですが、スライド式パネルには、その CVE に関連するすべてのベンダーからのスコアが記載されています。
名前	CVE の名前。
プラグイン名	プラグインの名前とバージョンを表示します。プラグイン **名** のリンクをクリックすると、プラグインの詳細が表示されます。
プラグイン ID	脆弱性の修正を含むパッケージの一意の識別子またはビルド文字列を表示します。
深刻度	対象のベンダーから提供された評価に基づく脆弱性の重大度評価。ベンダーからの

列	説明
	提供がない場合はNational Vulnerability Database (NVD) が提供する重大度。この評価は脆弱性によってもたらされる脅威のレベルを示し、(文脈を踏まえた他の要因とともに) 検出結果の全体的な深刻度レベルに影響を与えます。1つのCVEが複数のワークロードで見つかり、その各ワークロードで異なるベンダーのオペレーティングシステムが実行されている場合、深刻度はそれぞれ異なる可能性があります。このような場合、クラウドサイバーエクスポージャーは最も高い深刻度を表示します。
VPR スコア	VPR スコアの値の範囲は0.1から10.0で、値が大きいほど悪用の可能性が高くなります。VPR スコアは、VPR の深刻度の値に次のようにマッピングされます。 • 重大 = 9.0から10.0、 • 高 = 7.0から8.9、 • 中 = 4.0から6.9、 • 低 = 0.1から3.9、
CVSS スコア	CVSS 深刻度スコアを0.0から10.0の範囲で示します。このスコアは脆弱性によってもたらされる脅威のレベルを示し、検出結果の全体的な深刻度レベルに影響を与えます。
ソフトウェア	脆弱なソフトウェアパッケージの名前とバージョン。
パス	(ライブラリのみ)パッケージのファイルパス。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
修正者	脆弱性が修正されたパッケージのバージョン。
CVSS による深刻度	NVD (主要なソース)、Tenable 定義済みのメトリクス (NVD に同意しない場合)、ベンダーのメトリクス、または機械学習を利用して CVSS ベクトルを生成する自動化プロセスを使用するバックアップオプションに基づく脆弱性の深刻度評価。CVSS ベクト

列	説明
	ルと対応するスコアは、脆弱性が悪用され、優先度のデータポイントとして頻繁に使用された場合に、どの程度深刻な影響があるかを示しています。
VPR Severity	Tenable は、ほとんどの脆弱性について動的な VPR (脆弱性優先度格付け) を計算します。Tenable は現在の脅威状況を反映するように VPR を更新するため、VPR は脆弱性の CVSS スコアが示すデータに追従します。 可能な値 • 緊急 • 高 • 中 • 低
EPSS スコア	実際の脅威インテリジェンスと機械学習に基づいて、脆弱性が今後 30 日間に悪用される可能性を推定します。スコアが高いほど悪用される可能性が高いことを示し、これを踏まえてリスクに基づく修正の優先順位を付けることができます。
説明	CVE の説明。
オペレーティングシステムタイプ	イメージの特定のオペレーティングシステムフレーバー。
攻撃手法	脆弱性の悪用が可能な文脈情報を示します。スコアが高いほど、よりリモート (論理的または物理的に) から攻撃される可能性があることを示します。 可能な値: • ネットワーク • 隣接 • ローカル • 物理

列	説明
既知のエクスプロイト	脆弱性が既知のエクスプロイトと関連しているかどうかを示します (CISA カタログに基づく)。
アカウント	脆弱性が確認されたクラウドアカウント。コンテナイメージの脆弱性の場合、これにはイメージを実行するすべてのアカウントが含まれます。同期されていないレジストリまたはパブリックレジストリからのイメージは、**コンテナレジストリ**アカウントに表示されます。
スキャン済みリソース	脆弱性が確認されたワークロード。
ソフトウェアタイプ	脆弱なソフトウェアのタイプ。可能な値: Library、Operating System、Package。
初回スキャン時間	最初のスキャンのタイムスタンプ。

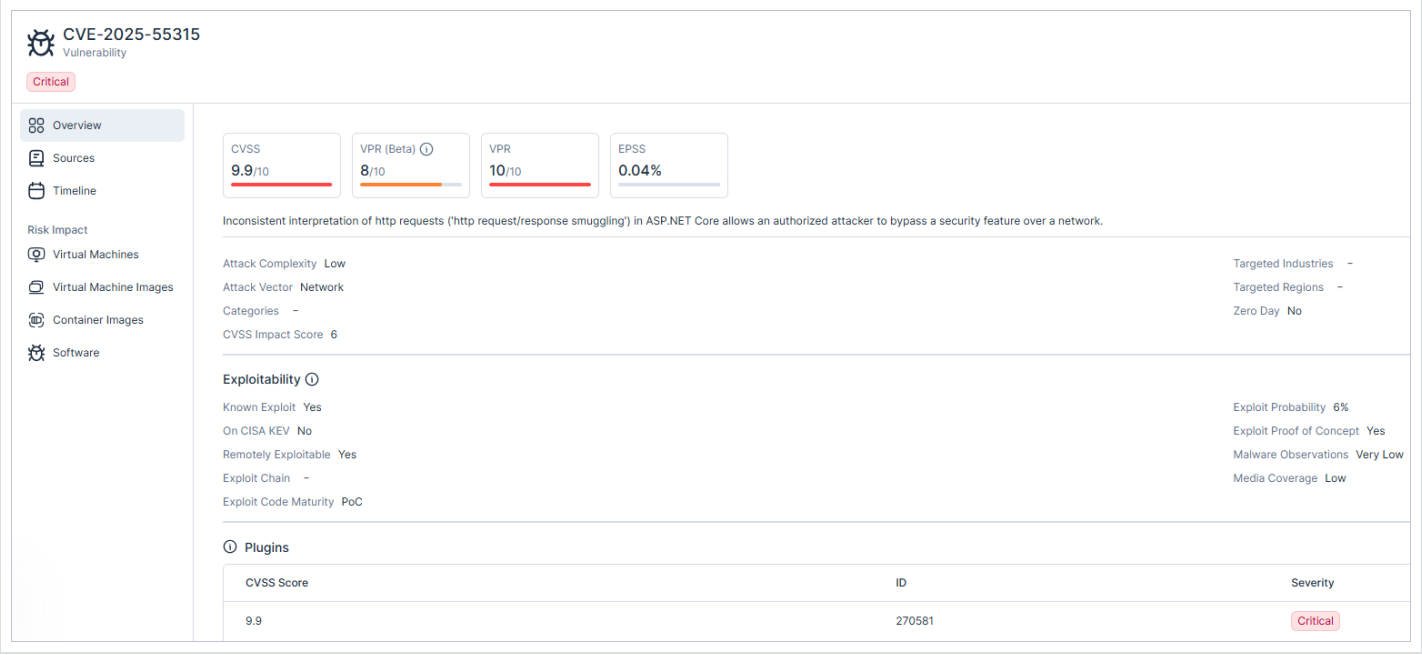
脆弱性の詳細の表示

脆弱性をクリックすると、脆弱性スライド式パネルにその脆弱性に関する詳細な情報が表示されます。このページには、Tenableの業界をリードする脆弱性データベースからあらゆる情報が統合されて表示されます。以下のオプションがあります。

- **概要**:
    - CVSS、VPR、EPSS の深刻度スコア
    - 脆弱性の説明
    - 脆弱性脆弱性スライド式パネル。より効果的に脆弱性を優先順位付けするために役立つ重要なインサイト。
    - 悪用される可能性。脆弱性の攻撃の可能性を測定するために使用される詳細。

- プラグイン ベンダーアドバイザリごとに複数の CVE をグループ化して統合された修正パスを提供し、ユーザーが 1 回のソフトウェア更新で複数の脆弱性に対処できるようにします。
- CVSS 深刻度メトリクス脆弱性の深刻度の評価に影響するさまざまなメトリクスに関する詳細情報。

- **ソース**。セキュリティアドバイザリなどの文脈を踏まえたインテリジェンスを、掲載されている外部ウェブサイトで確認します。
- **タイムライン**。Vulnerability Priority Rating (VPR) と Exploit Prediction Scoring System (EPSS) のスコアの推移を表示します。また、脆弱性に関連する重要なイベントを表示することもできます。詳細は、「タイムラインイベント を参照してください。
- **リスクの影響**。脆弱性の影響を受ける仮想マシン、仮想マシンイメージ、コンテナイメージ、ソフトウェアを一覧表示し、環境がこの脆弱性によってどのように影響を受けるかを示します。



脆弱性スライド式パネル

脆弱性リスクプロファイルは、より効果的に脆弱性を優先順位付けするために役立つ重要な文脈情報を提供します。

要因	説明	意義
攻撃の複雑性	このメトリクスは、攻撃者が自らのコントロールのみでは攻撃できず、脆弱性を悪用するために必要な条件を表します。	可能な値: Low、High
攻撃手法	脆弱性の悪用が可能な文脈情報。スコアが高いほど、よりリモート (論理的または物理的に) から攻撃される可能性があることを示します。	可能な値: Adjacent、Local、Network、Physical
カテゴリ	脆弱性を定義するカテゴリ。	可能な値 • CISA Known Exploited: CISA の既知の悪用された脆弱性カタログ に記載されている脆弱性。CISA では、これらの脆弱性は直ちに害を及ぼすことが知られているため、修正作業を優先するよう推奨しています。 • Ransomware: TenableResearch チームによって収集された証拠から判断された、現在または過去のランサムウェア攻撃で使用された脆弱性。 • Emerging Threats: 3 つの領域で Tenable One Cloud Exposure によってアクティブにモニタリングされている脆弱性: • **モニタリングされている脆弱性** 公に議論されているが、エクスプロイトまたは概念実証は開示され

要因	説明	意義
		ていません。 • **対象となる脆弱性**: 公に議論され、攻撃者による広範な使用につながる可能性のある概念実証があります。 • **懸念される脆弱性**: 広く議論され、攻撃者による大規模なエクスプロイトが観察されています。 • `Persistently Exploited`: 標的型攻撃、ランサムウェア、またはマルウェアキャンペーンで、攻撃者が長期間悪用している脆弱性。これらの脆弱性は、Tenable One Cloud Exposure Research チームによって手動で選別されています。 • `Recently Exploited`: 過去 30 日間にマスコミに大きく取り上げられた、Tenable が実際の悪用の証拠を持っている脆弱性。 • `In the News`: 過去 30 日間にマスコミで広く報道され、注目を浴びた脆弱性。
CVSS 影響スコア	脆弱性の CVSS (共通脆弱性評価システム) 影響スコア。高度な VPR 深刻度の計算に使用されます。	可能な値: `0.0-10.0`
検出時間	お客様の資産で脆弱性が最初に検出された日時。	

要因	説明	意義
対象業界	特定の業界を標的にしている証拠が脆弱性の要因になっているかどうか。	可能な値: AI 生成。例: Consulting、Energy、Engineering
対象地域	脆弱性が、特定の地域で観察されたアクティブな悪用の一部であるかどうか。	可能な値: AI 生成。例: Asia、Middle East、North America
ゼロデイ	ベンダーのパッチが利用可能になる前に脆弱性が開示されたことを示す静的フラグ。一度設定されると、このフィールドの値は恒久的に残り、公式の修正またはパッチがリリースされた後でも変更されません。	可能な値: Yes、No
公開時刻	Tenable が信頼できるソースで初めて CVE についての言及を確認した日、または NVD の公開日のいずれか早い日。	

悪用される可能性

[悪用される可能性] セクションには、脆弱性の攻撃可能性を測定するために使用された特定の詳細情報が表示されます。これらのパラメーターにより、悪用される可能性が最も高いセキュリティ欠陥を特定しやすくなるため、優先順位を付けられます。

要因	説明	値
既知のエクスプロイト	脆弱性が既知のエクスプロイトと関連しているかどうかを示します (CISA カタログに基づく)。	可能な値: Yes、No

要因	説明	値
CISA KEV 上	CISA は、実際に悪用された脆弱性の信頼できるソースを維持しています。	可能な値：Yes、No
リモートから悪用可能	脆弱性がリモートネットワークから悪用できるかどうか。	可能な値：Yes、No
エクスプロイトチェーン	脆弱性がエクスプロイトチェーンの一部として存在するかどうかを示します。	可能な値：CVE ID
エクスプロイトコード成熟度	内部および外部のソースのエクスプロイトインテリジェンスの存在、巧妙さ、流行に基づく、脆弱性の可能性があるエクスプロイトの相対的な成熟度。	可能な値：High、Functional、PoC、Unproven
エクスプロイトの可能性	VPR スコアが脆弱性悪用の可能性の推定値による影響を主に受けている検出結果。	可能な値：0-100%
エクスプロイトの概念実証	Tenable がこの脆弱性の概念実証を特定したかどうか。	可能な値：Yes、No
マルウェアの観察	過去 30 日間に関連するマルウェア観察が大量にあったため、VPR が高くなった検出結果。	可能な値：Very Low、Low、Medium、High、Very High
メディア報道	過去 30 日間におけるメディアの言及の量または頻度が多いために、VPR が上がった検出結果。	可能な値：Very Low、Low、Medium、High、Very High

タイムラインイベント

タイムラインイベントは、脆弱性に関連する重要なイベントを表します。

イベント	説明
CISA の既知のエクスプロイト	アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁 (CISA) が脆弱性を既知の悪用された脆弱性カタログに追加した日時。
CISA 対処期限日	連邦機関が CISA の既知の悪用された脆弱性 (KEV) リストに掲載されている脆弱性を修正しなければならない期限の日時。
検出日	Tenable が最初に脆弱性を確認した日時。
新たな脅威	公開されており、実行可能な概念実証があるか広く使用されているため、脆弱性が Tenable によってアクティブに監視されていることを示します。
出回っているエクスプロイト	脆弱性がサイバー攻撃に利用されたことを示します。
最初の概念実証	Tenable が最初に脆弱性の概念実証 (PoC) を確認した日時。
最初の Tenable のカバレッジ	Tenable が脆弱性のカバレッジを初めて提供した日時。
最初の機能的エクスプロイト	脆弱性の機能的エクスプロイトが初めてリリースされた日時。
マルウェア	Tenable が脆弱性のマルウェアイベントを初めて確認した日時。
公開済み NVD	National Vulnerability Database (NVD) が脆弱性を公開した日時。

イベント	説明
ランサムウェア	Tenable が脆弱性のランサムウェアイベントを初めて確認した日時。

プラグイン

プラグインは、特定のリソース内の脆弱性やバグに対処するために設計されたソフトウェア更新です。Tenable では、プラグインは複数の CVE に対する包括的な修正を提供するようにグループ化されます。

プラグイン (Tenable Vulnerability Management ではプラグイン ID とも呼ばれます) は、通常、特定のセキュリティアドバイザリに応じてベンダーによってリリースされます。単一の欠陥をターゲットとする個別のセキュリティ更新とは異なり、Tenable はプラグインを、複数の CVE を同時に修正する修正のコレクションとして分類します。Tenable は、これらのプラグインを特定のリソースにマッピングして、プラグインを適用するときに、そのベンダーアドバイザリ内に関連するすべての脆弱性を確実に解決できるようにします。

- **脆弱性テーブル** 脆弱性テーブルには、Tenable に行ごとに 1 つのプラグインが表示されます。各行は、CVE と特定のソフトウェアインスタンスの一意の組み合わせを表します。
- 脆弱性**のスライド式パネル**: 脆弱性のスライド式パネルには、複数のプラグインが表示されます。このビューには、リソース全体の CVE のコンテキストが表示されます。1 つの CVE が同じリソースの異なるソフトウェアパッケージに影響を与える場合、スライド式パネルには影響を受ける各ソフトウェアに必要な一意のプラグインが一覧表示されます。

プラグインの詳細を表示

関連する CVE やベンダーアドバイザリなど、プラグインに関する詳細な情報は、コンソール内の脆弱性テーブルから直接表示できます。

プラグインの詳細を表示する方法

1. 左側のナビゲーションプレーンで、**[リスク > 脆弱性]** をクリックします。脆弱性の表が表示されます。
2. (オプション)**[プラグイン]** 列が表示されていない場合は、**[列]** アイコンをクリックして列を表に追加します。

3. **[プラグイン]** 列で、表示する特定のプラグインのリンクをクリックします。プラグインのスライド式パネルが表示されます。このパネルには、次のタブがあります。

    - **概要**:
        - CVSS、VPR、EPSS の深刻度スコア
        - プラグインの説明。
        - プラグインプラグインメタデータ。は、プラグインに関する追加情報を提供します。
        - プラグインの脆弱性脆弱性。より効果的に脆弱性を優先順位付けするために役立つ重要なインサイト。
        - プラグインの悪用可能性。脆弱性の攻撃の可能性を測定するために使用される詳細。
        - 修正影響を受けるリソースにインストールするセキュリティ更新プログラムの名前を提供します。
        - プラグインの脆弱性脆弱性。は、特定のプラグインが修正したすべての CVE のリストを表示します。
    - **リスクの影響**。脆弱性の影響を受ける仮想マシン、コンテナイメージ、ソフトウェアを一覧表示し、環境がこの脆弱性によってどのように影響を受けるかを示します。

プラグインメタデータ

プラグインメタデータセクションには、プラグインに関する追加情報が表示されます。

フィールド	説明
ID	Tenable脆弱性データベース内でプラグインに割り当てられた一意の識別番号。
ファミリー	プラグインが属するカテゴリまたはグループ。通常はオペレーティングシステムまたはベンダー別に分類されます。
参照	プラグインに関する追加のコンテキストを提供する、ベンダードキュメント、サポート記事、またはセキュリティアドバイザリへの外部リンク。

フィールド	説明
公開時刻	プラグインエントリが Tenable 脆弱性データベースに最初に追加された日時を示すタイムスタンプ。
更新時間	タイムスタンプは、新しい CVE マッピングや更新された修正手順を含めるためにデータベースでプラグインエントリが最後に変更された日時を示します。
パッチ公開時刻	タイムスタンプは、ベンダーのパッチが公開された日時を示します。

プラグインの脆弱性

脆弱性リスクプロファイルは、より効果的に脆弱性を優先順位付けするために役立つ重要な文脈情報を提供します。

要因	説明	意義
攻撃の複雑性	このメトリクスは、攻撃者が自らのコントロールのみでは攻撃できず、脆弱性を悪用するために必要な条件を表します。	可能な値: `Low`、`High`
攻撃手法	脆弱性の悪用が可能な文脈情報。スコアが高いほど、よりリモート (論理的または物理的に) から攻撃される可能性があることを示します。	可能な値: `Adjacent`、`Local`、`Network`、`Physical`
カテゴリ	脆弱性を定義するカテゴリ。	可能な値 • `CISA Known Exploited`: CISA の既知の悪用された脆弱性カタログ に記

要因	説明	意義

		載されている脆弱性。CISA では、これらの脆弱性は直ちに害を及ぼすことが知られているため、修正作業を優先するよう推奨しています。
		• `Ransomware`: TenableResearch チームによって収集された証拠から判断された、現在または過去のランサムウェア攻撃で使用された脆弱性。
		• `Emerging Threats`: 3 つの領域で Tenable One Cloud Exposure によってアクティブにモニタリングされている脆弱性:
		  • **モニタリングされている脆弱性**公に議論されているが、エクスプロイトまたは概念実証は開示されていません。
		  • **対象となる脆弱性**: 公に議論され、攻撃者による広範な使用につながる可能性のある概念実証があります。
		  • **懸念される脆弱性**: 広く議論され、攻撃者による大規模なエクスプロイトが観察されています。
		• `Persistently Exploited`: 標的型攻撃、ランサムウェア、またはマルウェアキャンペーンで、攻撃者が長期間悪用している脆弱性。これらの脆弱性は、Tenable One Cloud Exposure

要因	説明	意義
		Research チームによって手動で選別されています。 • `Recently Exploited`: 過去 30 日間にマスコミに大きく取り上げられた、Tenable が実際の悪用の証拠を持っている脆弱性。 • `In the News`: 過去 30 日間にマスコミで広く報道され、注目を浴びた脆弱性。
CVSS 影響スコア	脆弱性の CVSS (共通脆弱性評価システム) 影響スコア。高度な VPR 深刻度の計算に使用されます。	可能な値: `0.0-10.0`
検出時間	お客様の資産で脆弱性が最初に検出された日時。	
対象業界	特定の業界を標的にしている証拠が脆弱性の要因になっているかどうか。	可能な値: AI 生成。例: `Consulting`、`Energy`、`Engineering`
対象地域	脆弱性が、特定の地域で観察されたアクティブな悪用の一部であるかどうか。	可能な値: AI 生成。例: `Asia`、`Middle East`、`North America`
ゼロデイ	ベンダーのパッチが利用可能になる前に脆弱性が開示されたことを示す静的フラグ。一度設定されると、このフィールドの値は恒久的に残り、公式の修正またはパッチがリリースされた後でも変更されません。	可能な値: `Yes`、`No`

要因	説明	意義
公開時刻	Tenable が信頼できるソースで初めて CVE についての言及を確認した日、または NVD の公開日のいずれか早い日。	

プラグインの悪用可能性

[悪用される可能性] セクションには、脆弱性の攻撃可能性を測定するために使用された特定の詳細情報が表示されます。これらのパラメーターにより、悪用される可能性が最も高いセキュリティ欠陥を特定しやすくなるため、優先順位を付けられます。

要因	説明	値
既知のエクスプロイト	脆弱性が既知のエクスプロイトと関連しているかどうかを示します (CISA カタログに基づく)。	可能な値: `Yes`、`No`
CISA KEV 上	CISA は、実際に悪用された脆弱性の信頼できるソースを維持しています。	可能な値: `Yes`、`No`
リモートから悪用可能	脆弱性がリモートネットワークから悪用できるかどうか。	可能な値: `Yes`、`No`
エクスプロイトチェーン	脆弱性がエクスプロイトチェーンの一部として存在するかどうかを示します。	可能な値: `CVE ID`
エクスプロイトコード成	内部および外部のソースのエクスプロイトインテリジェンスの存在、巧妙さ、流行に基づく、脆弱性の可能性があるエクスプロイトの相対的な成熟度。	可能な値: `High`、`Functional`、`PoC`、`Unproven`

要因	説明	値
熟度		
エクスプロイトの可能性	VPR スコアが脆弱性悪用の可能性の推定値による影響を主に受けている検出結果。	可能な値: 0-100%
エクスプロイトの概念実証	Tenable がこの脆弱性の概念実証を特定したかどうか。	可能な値: Yes、No
マルウェアの観察	過去 30 日間に関連するマルウェア観察が大量にあったため、VPR が高くなった検出結果。	可能な値: Very Low、Low、Medium、High、Very High
メディア報道	過去 30 日間におけるメディアの言及の量または頻度が多いために、VPR が上がった検出結果。	可能な値: Very Low、Low、Medium、High、Very High

プラグインの脆弱性

[脆弱性] セクションには、特定のプラグインによって修正されるすべての CVE のリストが表示されます。これにより、プラグインがセキュリティ体制に与える影響を直接的に確認できます。表の内容は次のとおりです。

- **脆弱性:** CVE ID。脆弱性の一意の識別子。
- 深刻**度**: 脆弱性に割り当てられているリスク評価。
- **名前**: 脆弱性の名前。
- **VPR スコア**: 悪用される可能性に基づいて修正の優先順位付けを行うのに役立つ Tenable の脆弱性優先度格付け。
- **CVSS スコア**: 脆弱性の深刻度を表す数値スコア

脆弱性データのエクスポート

脆弱性データを CSV ファイルにエクスポートします。データは、テーブルに適用されている現在のフィルターに従ってエクスポートされ、関連するすべての脆弱性データを含みます

> **注意:** エクスポート機能は、10,000件の結果に制限されています。環境内の脆弱性の量や、テーブルのフィルター方法によっては、テーブルに表示される結果がこれよりも多くなる場合があります。このような場合、追加のフィルターを適用して結果をさらに絞り込むか、最初の 10,000 件の結果をエクスポートすることをお勧めします。

脆弱性データをエクスポートする方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>脆弱性]** に移動します。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、「 脆弱性の列データ 」を参照してください。

   > **注意:** テーブルは **[修正のみ]** で自動的にフィルタリングされるため、すぐに修正可能な脆弱性にすばやく集中できます。

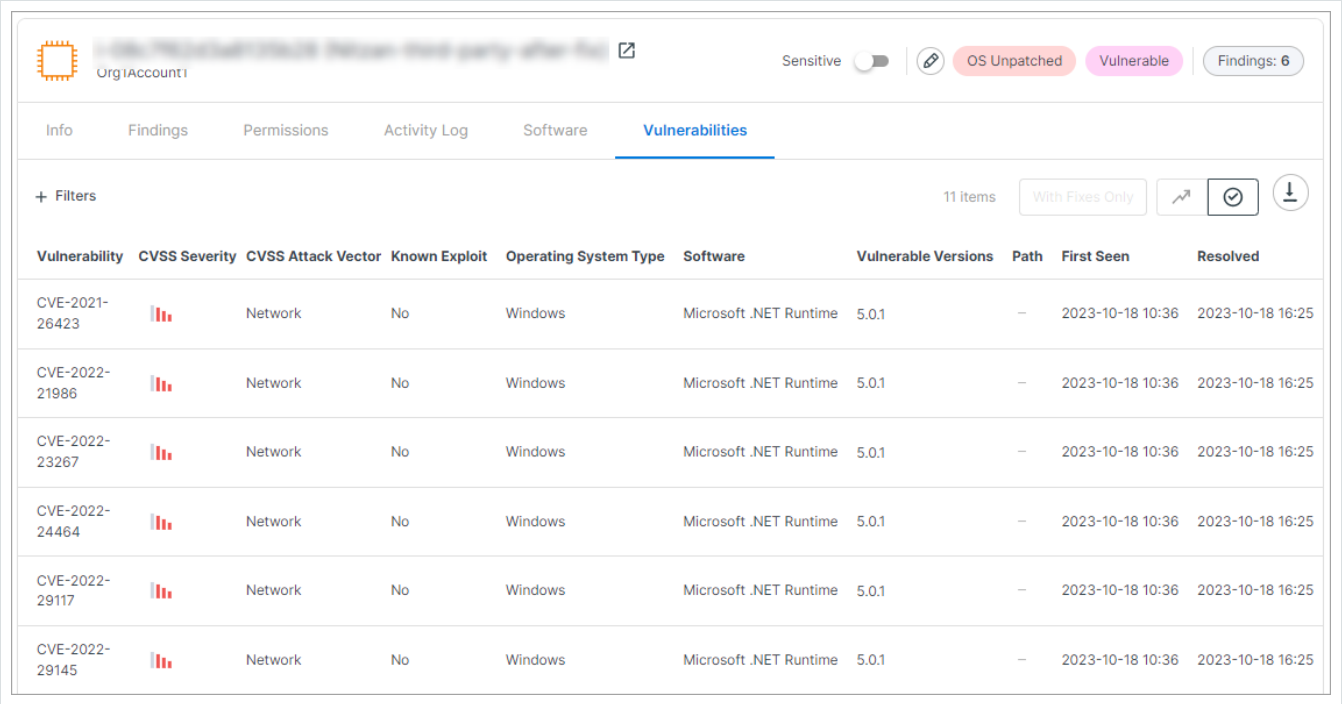
3. 表の右上にある **[エクスポート]** ボタン をクリックします。

特定のワークロードの脆弱性を表示する

特定のワークロードにインストールされているソフトウェアパッケージを クラウドサイバーエクスポージャー インベントリビューで表示します。

1. 特定のワークロードにドリルダウンします。
2. ワークロードのリソースページで、**[脆弱性]** タブをクリックします。
3. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。利用可能な列の詳細については、「 脆弱性の列データ 」を参照してください。
4. (VM/EC2 のみ)**[解決済み]** トグルを使用して、仮想マシンで最近解決された脆弱性を基準にフィルタリングし、それらに関連するデータを表示します。脆弱性が解決された日時を確認でき、修正

作業の効果の確認に役立ちます。



Vulnerability	CVSS Severity	CVSS Attack Vector	Known Exploit	Operating System Type	Software	Vulnerable Versions	Path	First Seen	Resolved
CVE-2021-26423		Network	No	Windows	Microsoft .NET Runtime	5.0.1	–	2023-10-18 10:36	2023-10-18 16:25
CVE-2022-21986		Network	No	Windows	Microsoft .NET Runtime	5.0.1	–	2023-10-18 10:36	2023-10-18 16:25
CVE-2022-23267		Network	No	Windows	Microsoft .NET Runtime	5.0.1	–	2023-10-18 10:36	2023-10-18 16:25
CVE-2022-24464		Network	No	Windows	Microsoft .NET Runtime	5.0.1	–	2023-10-18 10:36	2023-10-18 16:25
CVE-2022-29117		Network	No	Windows	Microsoft .NET Runtime	5.0.1	–	2023-10-18 10:36	2023-10-18 16:25
CVE-2022-29145		Network	No	Windows	Microsoft .NET Runtime	5.0.1	–	2023-10-18 10:36	2023-10-18 16:25

脆弱性関連の検出結果

次のいずれかの状況で、脆弱なワークロードの検出結果が作成されます。

- 脆弱性のCVE深刻度レベルが重大。
- 深刻度が重大/高の脆弱性が10個を超えている
- ワークロードのオペレーティングシステムのサポートが終了しているか、終了間近 (30日以内)

ワークロードを対象にして作成された脆弱性関連の検出結果には、そのワークロードで検出されたすべての脆弱性が含まれます。検出結果の深刻度は、それぞれのCVEの深刻度レベルとリソースが機密度の高いリソースをマークするされているかどうかを組み合わせた関数です。ワークロードで複数の脆弱性が検出された場合、検出結果の深刻度スコアには最も深刻度の高い脆弱性のスコアが反映されます。

脆弱性の検出結果を表示およびドリルダウンする

脆弱性の検出結果を表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>クラウドの検出結果]** をクリックします。
2. 関連する他のフィルターを適用して、表示される検出結果の範囲を絞り込みます。脆弱性に特に関連するワークロード保護の検出結果を表示するには、[Label] (ラベル) フィルターから以下のいずれかを選択します。
    - **脆弱性**
    - **脆弱性のあるコンピューティング**

検出結果の脆弱性の列データ

縦棒	説明
脆弱性	脆弱性に関連するCVE ID (例: CVE-2021-3177)。 • IDにカーソルを合わせると、脆弱性の詳細 (説明や深刻度スコアなど) についての概要ビューが表示されます。 • IDをクリックするとスライド式パネルが開き、関連する脆弱性の詳細がすべて表示されます。
CVSSによる深刻度	対象のベンダーから提供された評価に基づく脆弱性の重大度評価。ベンダーからの提供がない場合はNational Vulnerability Database (NVD) が提供する重大度。この評価は脆弱性によってもたらされる脅威のレベルを示し、(文脈を踏まえた他の要因とともに) 検出結果の全体的な深刻度レベルに影響を与えます。
CVSSスコア	CVSS深刻度スコアを0.0から10.0の範囲で示します。このスコアは脆弱性によってもたらされる脅威のレベルを示し、検出結果の全体的な深刻度レベルに影響を与えます。
CVSS攻撃経路	脆弱性の悪用が可能な文脈情報を示します。スコアが高いほど、よりリモート (論理的または物理的に) から攻撃される可能性があることを示します。可能な値: Network、Adjacent、Local、Physical
既知のエクスプロイ	脆弱性が既知のエクスプロイトと関連しているかどうかを示します (CISAカタログに基づく)。

縦棒	説明
ト	
ソフトウェア	脆弱なソフトウェアパッケージの名前。
インストールされているバージョン	リソースにインストールされているパッケージのバージョン。
修正済みバージョン	脆弱性が修正されたパッケージのバージョン。
パス	(ライブラリのみ)パッケージのファイルパス。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。

サポートケース用のリソースインベントリデータのエクスポート

この機能は、Tenable 脆弱性管理サポートのトラブルシューティングを簡素化します。リソースのインベントリデータをプロファイルから直接 JSON ファイルとしてエクスポートし、サポートチケットに添付できます。このオプションは、正常にスキャンされたリソースで利用でき、表示アクセス許可を持つユーザーに表示されます。リソースがスキャンされていない場合は灰色になります。

> **注意:** このデータはサポートでの使用のみを目的としており、一般使用を目的としていません。

リソースインベントリデータのダウンロード方法

1. コンソール クラウド サイバーエクスポージャー 、**[Inventory]** > **[Virtual Machines]** に移 動します。

   > **注 意:** エクスポート オプションは、**仮 想 マシンイメージ** と**コンテナイメージ** のリソースでもサポート されています。

2. スキャンしたリソースをクリックして、そのプロファイルを開きます。
3. プロファイルビューで、**三 点 リーダー** メニューアイコン> **[インベントリデバッグデータのダウンロード]** をクリックします。
   デバッグデータは JSON 形 式 でダウンロードされます。

FAQ (よくある質 問)

以 下 は、クラウド サイバーエクスポージャー の Vulnerability Intelligence に関 連 するよくある質 問 です。

Vulnerability Priority Rating (VPR) に対 する理 解

> Vulnerability Priority Rating (VPR) とは何 ですか?

Vulnerability Priority Rating (VPR) は、脅 威 のコンテキストと現 実 世 界 の悪 用 可 能 性 に基 づいて脆 弱 性 に優 先 順 位 を付 ける Tenable 独 自 の動 的 リスクスコアです。組 織 が修 正 の効 率 と効 果 を向 上 させるのに役 立 ちます。

> VPR の拡 張 バージョンが元 の VPR よりも効 果 的 な理 由 は何 ですか?

回 答: VPR の最 新 バージョンでは、強 化 された機 械 学 習 モデル、拡 張 されたデータソース、より優 れたコンテキスト認 識 スコアリング、より洗 練 された深 刻 度 帯 域 が搭 載 されており、ノイズを減 らし、精 度 を向 上 させ、より自 信 を持 って意 思 決 定 ができるようになります。

- **さらに焦 点 を絞 った優 先 順 位 付 け** - 静 的 な CVSS スコアでは CVE の 60% が「高 」または「重 大 」とフラグされますが、元 の VPR では焦 点 が 3% に絞 り込 まれました。現 在 、VPR の機 能 強 化 により効 率 がさらに向 上 し、よりリアルタイムのデータを利 用 して、チームは本 当 に重 要 なわずか 1.6% の脆 弱 性 に集 中 できます (出 典)。
- **データソース** - VPR の拡 張 バージョンでは、National Vulnerability Database (NVD)、CVSS、エクスプロイト データベース、脅 威 インテリジェンス パートナーなど、VPR ですでに使 用 されているデータ

入力に加えて、Tenable Research Special Operations チーム、Tenable Vulnerability Intelligence、サイバーセキュリティの Web 記事や AI ニュース機能、CISA、Github、Mastodon から提供されたデータが使用されます。これらの新しいデータソースにより、どの脆弱性が実際に悪用されているかをより明確に把握できます。

- **AI の統合** - 生成 AI は、厳選された Web 記事を大規模に処理し、ランサムウェアの標的として CVE をタグ付けするために使用されます。このデータは、新しいモデルが悪用の可能性を短期的に予測するために使用されます。
- **CVE 脅威要因の更新** - 強化された VPR により、脆弱性に関する新しい主な要因と情報が導入され、CVE 深刻度の計算の説明が容易になります

VPR の仕組み

> VPR スコアはどのように計算されますか?

回答: VPR は、脅威アクターのアクティビティ、エクスプロイトコードの成熟度、脆弱性の経過日数など、複数の動的要因を分析する機械学習モデルを使用して、予測されるエクスプロイトの可能性を生成します。これを CVSS 影響スコアと組み合わせて、最終的な VPR を導き出します。たとえば、スコアが低い場合 (0.1 から 3.9) 場合、既知の悪用がほとんどまたはまったくないことを示します。ただし、スコアが高い (9.0 から 10.0) 場合、武器化された悪用が観察されており、この脆弱性を標的としたアクティブなキャンペーンがあることを示します。

> VPR の拡張バージョンでは、どのようなデータソースが使用されていますか?

回答: このモデルは、脅威インテリジェンス フィード、パブリックおよびプライベート エクスプロイト データベース、オープンソース データ、独自の調査を活用しています。具体的には、データソースには、NVD、CVSS、Tenable Vulnerability Intelligence、Tenable Research Special Operations (RSO)、ウェブ記事、AI ニュース機能、AI ドメイン分類、Mastodon、CISA、GitHub などがあります。

> VPR スコアが付与される脆弱性はどれですか?

有効な CVE ID を持つすべての脆弱性 (NVD にまだ公開されていないものを含む) に VPR スコアが割り当てられます。

VPR スコアはどのくらいの頻度で更新されますか?

VPR スコアは、最新の脅威インテリジェンスと実際の悪用可能性の変化を反映するために毎日更新されます。

セキュリティチームは、VPR スコアが高いか低いかをどのように解釈する必要がありますか?

回答: VPR スコアが高い場合 (例: 7.0-10.0) は、悪用のリスクが高いため、緊急のアクションが必要であることを示します。スコアが低い場合は、現在の脅威アクティビティが制限されているか、まったくないことを示し、優先順位が下がっている可能性があります。

VPR の機能強化は、誤検出やアラート疲れの軽減にどのように役立ちますか?

回答: VPR の機能強化により、スコアリングアルゴリズムが改良され、優先度の高い脆弱性と低リスクの脆弱性の区別がしやすくなり、不要なアラートが減り、修正ワークフローが効率化されました。CVSSは、CVEの60%に「高」または「重大」のフラグを立てますが、これは膨大な数であり、最初に何を効果的に修正すべきかの優先順位を付けることができません。当初の VPR では、CVSS によって「高」または「重大」とフラグが立てられた CVE のうち 60% からわずか 3% に絞り込み、チームが修正作業に集中するのに大きく役立ちました。VPR の機能強化により、効率性をさらに高め、ビジネスにとって実際のリスクをもたらすわずか 1.6% の脆弱性にチームを集中できるようになりました。詳細については、テクニカルホワイトペーパーをお読みください。

VPR と他のリスクスコアリング手法の比較

VPR は CVSS や EPSS とどう違うのですか?

回答: CVSSは、固有の技術的重大度を測定します。EPSS は、悪用の可能性を推定します。VPR は、機械学習を使用した脅威インテリジェンスとエクスプロイト予測をビジネスインパクトと組み合わせて、より運用性の高いリアルタイムの優先順位付けを提供します。詳細については、テクニカルホワイトペーパーをお読みください。

VPR スコアは CVSS または EPSS のどちらに置き換わりますか?

回答: VPR は、現実世界の脅威データと資産コンテキストを組み込むことで CVSS と EPSS を補完し、より包括的で実用的なリスクのビューを提供します。

> VPR は CVSS や EPSS とどのように連携しますか?

回答: CVSS は技術的な深刻度を理解するために使用され、EPSS はエクスプロイトの可能性を統計的に適用し、VPR は実際の脅威の可能性とビジネスへの影響に基づく運用上の優先順位付けに使用されます。

> VPR 深刻度帯域と CVSS 深刻度帯域の違いは何ですか?

回答: VPR 深刻度帯は、技術的な属性だけでなく、現実世界のリスクを反映するように調整されています (本当にリスクの高い問題に注意を集中することで、アラート疲れを軽減するのに役立ちます)。

悪意のあるファイル

Tenable One Cloud Exposure を使用して、ワークロード内の悪意のある可能性があるファイルを検出します。

これは、クラウド サイバーエクスポージャー で悪意のあるファイルを監視するためのハウツーガイドです。

- クラウド サイバーエクスポージャー での脆弱性管理機能の概念概要については、「ワークロード保護を参照してください。
- 悪意のあるファイルを含むワークロード設定の構成に関するハウツーガイドについては、「 ワークロード」を参照してください。
- よくある質問については、「 FAQ: 脆弱性管理」を参照してください。

サポートされているファイルタイプ

クラウド サイバーエクスポージャー マルウェアスキャンは次のファイルを検査します。

カテゴリー	ファイルタイプ	スキャンされた場所
バイナリ(コンテンツによって検出)	Linux ELF バイナリ、Windows PE バイナリ、および shebang スクリプト (`#!` で始まるファイル)	どこでも
スクリプト(拡張別)	`.bash`、`.bat`、`.cmd`、`.csh`、`.hta`、`.jse`、`.ksh`、`.lua`、`.pl`、`.ps1`、`.psd1`、`.psm1`、`.r`、`.sh`、`.vbe`、`.vbs`、`.wsc`、`.wsf`、`.wsh`、`.zsh`	どこでも
コードの依存関係	`.js`, `.cjs`, `.mjs`	`node_modules/` または Chrome `Extensions/` ディレクトリ
コードの依存関係	`.py`、`.pyw`	`site-packages/` ディレクトリ
コードの依存関係	`.rb`	`vendor/bundle/` ディレクトリ

クラウド サイバーエクスポージャー では、次のルールも適用されます。

- 実行可能アクセス許可を持つファイルは、一致する拡張子がなくてもスキャンされます。
- Linux では、クラウド サイバーエクスポージャー はタイプに関係なく、`/tmp` 下のすべてのファイルをスキャンします。
- クラウド サイバーエクスポージャー では、100 MB を超えるファイルはスキャンされません。

[Malicious Files] (悪意のあるファイル) ページの **[Type]** (タイプ) 列は、各ファイルについて検出されたフォーマット (ELF、PE、スクリプト、その他の実行可能ファイル) を報告します。

スキャンから除外されたパス

スキャンを高速かつ関連性のあるものに保つために、クラウドサイバーエクスポージャーでは、キャッシュ、パッケージストアとアーティファクトストア、CI/CD 作業ディレクトリ、コンテナランタイムデータ、監視エージェントデータなど、関連する実行可能ファイルがほとんど含まれないパスをスキップします。カテゴリ別の例

- **一般:** `.cache`、`.git`、`dev`、`proc`、`sys`
- **Linux:** コンテナとオーケストレーションのパス (例: `var/lib/kubelet/pods`)、CI/CD ワークスペース (例: `var/lib/jenkins/workspace`)、パッケージまたはアーティファクトストア (例: `ostree/repo/objects`)
- **Windows:** システムディレクトリ (`Windows/assembly` など)、コンテナランタイム (`ProgramData/docker` など)、ソフトウェア配布ストア (`SCCMContentLib` など)

このリストはすべてを網羅しているわけではありません。

悪意のあるファイルの表示

スキャン結果を表示するには:

1. クラウドサイバーエクスポージャーコンソールで、**[悪意のあるファイルのリスク>]** をクリックします。[Malicious Files] (悪意のあるファイル) ページには、Tenable によって特定された、悪意のある可能性があるすべてのファイルが表示されます。詳細については、「 悪意のあるファイルの列データ 」を参照してください。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。テーブル右上の列ピッカーを使用して、どの列を表示するか選びます。
3. ファイルを信頼できるものとしてマークするには、エントリの横にある三点リーダーをクリックし、**[信頼できるものとしてマークする]** をクリックします。
4. (オプション)(適用されたフィルターに基づき) 表示可能なすべてのデータを CSV ファイルに **エクスポート** します。
5. SHA-256 エントリをクリックすると、そのファイルに関する詳細情報が表示されます。結果はスライド式パネルで開きます。

> **注意:** ファイルを信頼できるものとしてマークするには、エントリの横にある三点リーダーアイコンをクリックし、**[信頼できるものとしてマークする]** をクリックします。

悪意のあるファイルの列データ

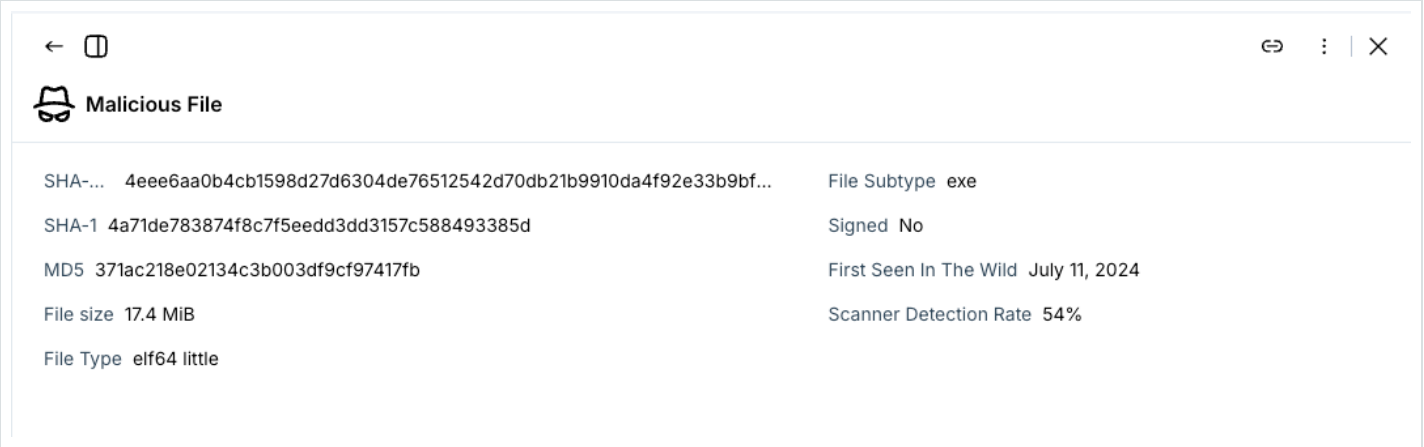
次の列/フィルターは [Malicious Files] (悪意のあるファイル) ページのテーブルに表示され、テーブルのデータのフィルターにも使用できます。

縦棒	説明
SHA-256	ファイルの SHA-256 ハッシュ。
初回スキャン時間	お使いの環境でファイルが最初に確認されたときを示します。
パス	(ライブラリのみ)パッケージのファイルパス。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
アカウント	スキャン対象のリソースが存在するクラウドアカウント。コンテナイメージの場合、これにはイメージを実行するすべてのアカウントが含まれます。同期されていないレジストリまたはパブリックレジストリからのイメージは、**コンテナレジストリ**アカウントに表示されます。
スキャン済みリソース	ファイルが見つかったスキャンされたクラウドリソース。
実行可能ファイルのタイプ	実行可能ファイルのファイル形式の種類可能な値: ELF、PE、Script、その他の実行可能ファイル。
オペレー	特定のオペレーティングシステムのフレーバー。

縦棒	説明
ティング システム タイプ	

悪意のあるファイルの詳細

[Malicious Files] (悪意のあるファイル) ページで SHA-256 エントリをクリックすると、スライド式が開き、そのファイルに関する詳細情報が表示されます。この情報は、ファイルとは何か、またどの程度広範囲で悪意があると認識されているのかを把握するのに役立ちます。



スライド式パネルには、以下の情報が含まれています。

フィールド	説明
SHA-256	ファイルの SHA-256 ハッシュ。
SHA-1	ファイルの SHA-1 ハッシュ。
MD5	ファイルの MD5 ハッシュ。

フィールド	説明
ファイルサイズ	ファイルのサイズ。
ファイルタイプ	ファイルの詳細なフォーマット (例: elf64 little)。
ファイルサブタイプ	ファイルのサブタイプ (例: exe)。
署名済み	ファイルにデジタル署名があるかどうかを示します。
最初に確認された時	脅威インテリジェンスプロバイダーがこのハッシュを文書化した最も早い日付。
スキャナー検出率	ファイルを悪意のあるものとして検出したサードパーティウイルス対策スキャナーの割合。 割合が高いほど、より多くのスキャナーがファイルにフラグを立てたことを意味します。

注意: スライド式の **[ファイルタイプ]** フィールドには、詳細なファイル形式が表示されます。これは、一般的なファイル形式 (ELF、PE、スクリプト、またはその他の実行可能ファイル) を表示する [悪意のあるファイル] テーブルの [実行 **可能ファイル**の種類] 列とは異なります。

コード CI/CD

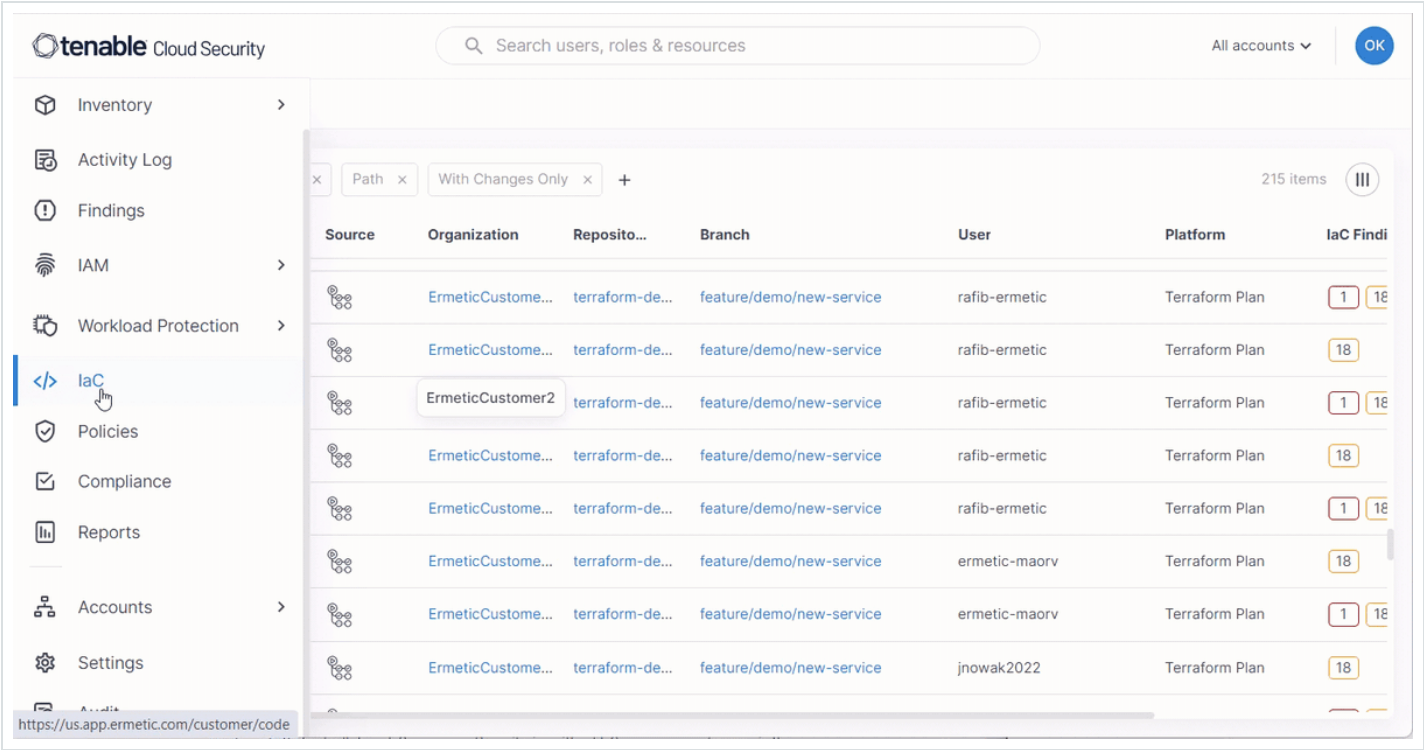
注意: この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

これは、Tenable One Cloud Exposure でのスキャン結果の表示と分析に関するハウツーガイドです。

- Tenable への CI/CD パイプラインの接続/設定に関する統合ガイドについては、CI/CD の接続を参照してください。
- Tenable の CI/CD とコード機能の概要については、「コード」を参照してください。

クラウドサイバーエクスポージャーコンソールを使用してコードをスキャンし、スキャン結果を分析して、潜在的な問題を特定します。(スキャンが実行された時間とリポジトリでソートされた) 各スキャンについて、深刻度に基づいて検出された問題数の内訳を確認できます。

注意: Tenable は、少なくとも 1 か月分のスキャン履歴を保持します。スキャンの量によっては最大 2 か月分のスキャン履歴を保持します。



はじめに

コードをスキャンして、設定ファイルの問題を検出して修正します。

前提条件

- Terraform 環境またはCloudFormation テンプレートが設定されていることを確認します。
- IaC 互換性マトリクスを確認し、各 IaC 機能でサポートされているプラットフォームとツールを確認します。

開始方法

1. IaC をクラウドサイバーエクスポージャーに接続して、code:
    - CI/CD の接続。
    - コードリポジトリの接続
2. スキャンで使用されるポリシーなど、Tenableが環境をスキャンする方法を微調整するようにスキャンSettingsを設定します。
3. Tenableに結果を送信せずにローカルでスキャンを実行する場合は、「ローカルでスキャンを実行するを参照してください。
4. スキャンが完了したら、クラウドサイバーエクスポージャーコンソールを使用して IaC 検出結果。

> **重要:** コンソールを使用してコードをクラウドサイバーエクスポージャーに接続するには、管理者ロールのユーザーとして、組織全体のアカウント範囲に対応できる必要があります。すべてのユーザーは、スキャン結果から IaC 検出結果を分析できます。ユーザーロールとアクセス許可の詳細については、「ユーザーとグループ」を参照してください。

ローカルでスキャンを実行する

(クラウドサイバーエクスポージャーに結果を送信せずに) ローカルでスキャンを実行する場合は、関連するパイプラインステップで一覧表示される環境変数のサブセットのみを含める必要があります。[別のパイプラインを追加する] ウィザードのステップ 3 にリストされている残りの変数は、クラウドサイバーエクスポージャーコンソールで関連データをカタログ化して表示するために使用されるため、ローカルでスキャンを実行する場合は必要ありません。

ローカルでスキャンを実行する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Integrations]** に移動し、**[Generic (Docker)]** をクリックします。
2. **[開始]** をクリックします。

> **注意:** パイプラインをすでに設定している場合は、**[Add pipeline (Docker)]** をクリックします。

3. **APIトークンを作成します** (ウィザードのステップ 1)。トークンの名前を入力し、「**次へ**」をクリックしてトークンを作成します。

   > **注意:** 複数のマシンに同じ APIトークンを使用できます。

4. **APIトークンを保存します** (ウィザードのステップ 2)。生成されたトークンをコピーして安全な場所に保存します。この情報は、ウィザードの次のステップで必要になります。完了したら、**[次へ]** をクリックします。

5. **環境変数を追加します** (ウィザードのステップ 3)。関連するパイプラインステップに以下の環境変数を追加し、結果を Tenable に報告します。

   - ウィザードに一覧表示される変数は、クラウドサイバーエクスポージャーコンソールで関連データをカタログ化して表示するために使用されるため、ローカルでスキャンを実行する場合は必要ありません。
   - スキャンの詳細情報を共有し、関連するデータをクラウドサイバーエクスポージャーコンソールで表示する場合、グローバルフラグなど、Tenable Docker イメージに含まれる任意のフラグを環境変数として設定して、スキャン設定をさらに微調整できます。変数として使用するためにフラグを変換する方法など、詳しくは「フラグを環境変数として使用する」を参照してください。

   ```
   TENABLE_API_TOKEN='--api-token here--' # Replace with the value displayed in the add-pipeline wizard
   TENABLE_API_URL='https://{region}.app.ermetic.com'
   ```

   region に入力する値は、Tenable One Cloud Exposure コンソールにログインする際に使用する URL の値に依存します。リージョン別の Tenable コンソール URL を参照してください。

   完了したら、**[次へ]** をクリックします。

6. **Docker コマンドを実行します** (ウィザードのステップ 4)。コンテナイメージをスキャンするには、次のステップをパイプラインに追加し、環境に応じて調整します。[TENABLE_API_TOKEN] フィールドは機密であるため、シークレットとして扱う必要があります。

```
docker run --workdir /tmp/tenable --volume </home/user/code>:/tmp/tenable --env-file
environment.variables --pull=always tenable/cloud-security-scanner:latest iac scan
```

重要: 上記のステップ例は、次のことを前提としています。

- docker run を使用して、コンテナで Tenable のスキャナーを実行しています。
- スキャンしているコードは `/home/user/code` にあります。
- `environment.variables` という名前の Docker env ファイルを作成した
- デフォルトのフラグでスキャンを実行しています。

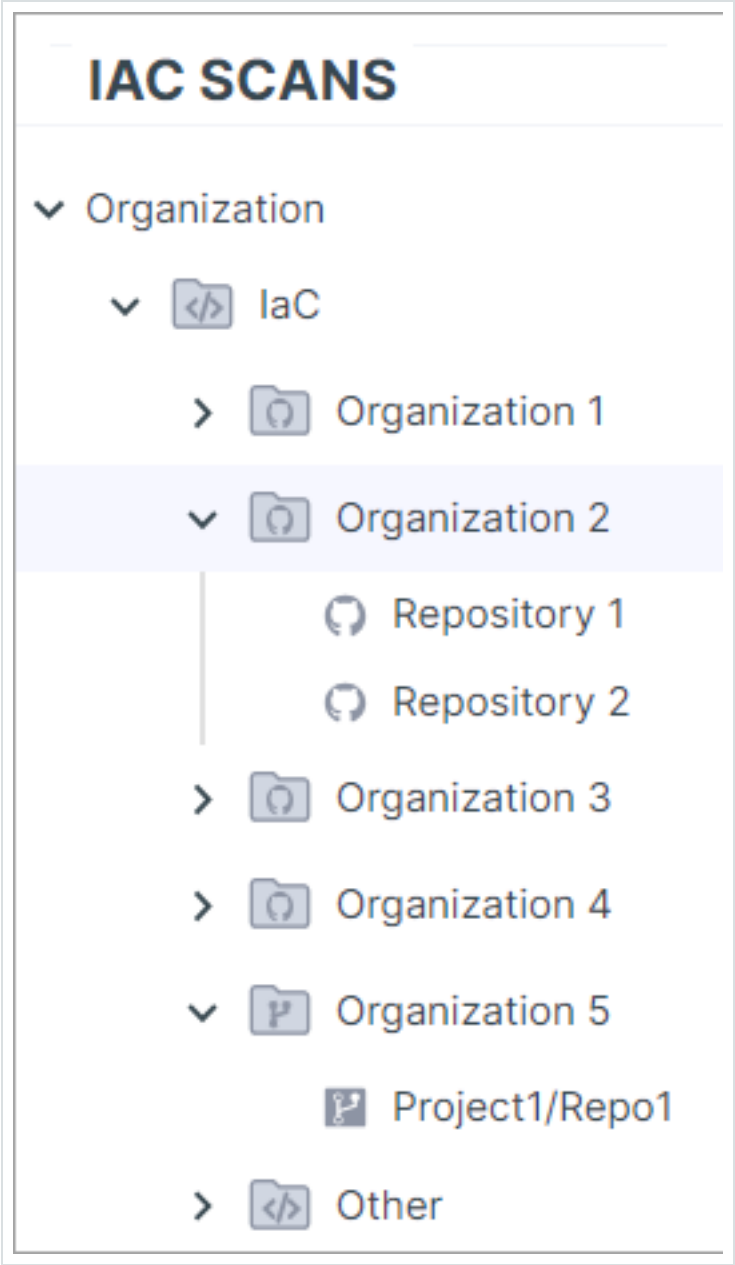
7. 完了したら、**[完了]** をクリックします。

組織階層

クラウドサイバーエクスポージャーコードのスキャン結果では、コードが管理されている IaC 組織の階層と、そこに含まれるリポジトリを確認できます。そのような組織は、GitHub、GitLab、Bitbucket、Azure DevOps が基になっている可能性があります。Tenable は関連する `organization` と `repository` のデータを抽出し、それに応じてマッピングします。何らかの理由で Tenable が組織データを抽出できない場合、リポジトリは階層の最下部にある [Other] (その他) フォルダーにマッピングされます。階層のマッピングとその結果は、Tenable によって自動的に実行され、手動で構成または調整することはできません。

Tenable は、IaC リソースを持つリポジトリのみをスキャンするため、ユーザーは実際に IaC リソースを持つ IaC テナントに集中しやすくなります。IaC リソースのないリポジトリは、ここの IaC 階層には表示されませんが、**Settings** > **アカウント** > **IaC** には引き続き表示されます (リソースがないことを示すステータス付き)。

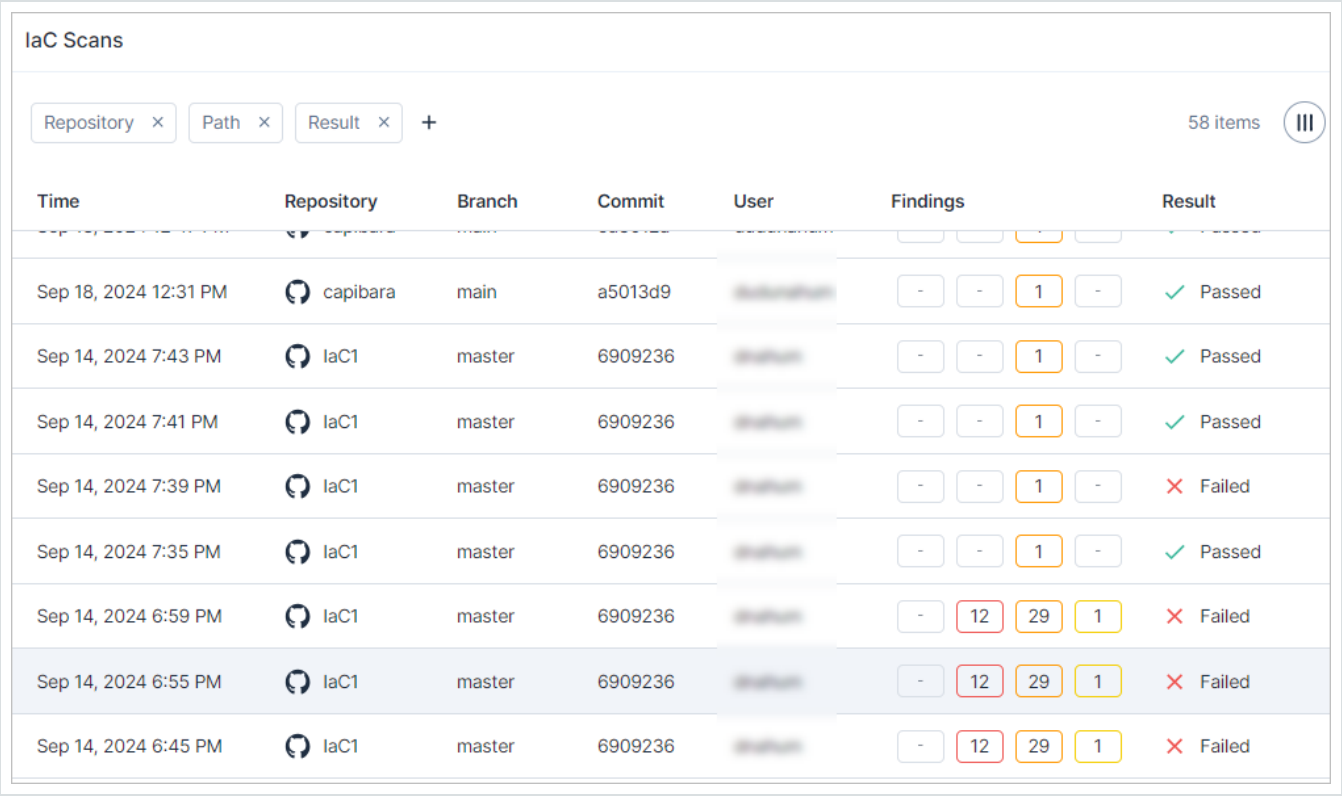
注意: Azure DevOps の場合、子オブジェクトは三層形式の `<organization>/<project>/<repository>` で表示されます (他はすべて二層形式)。



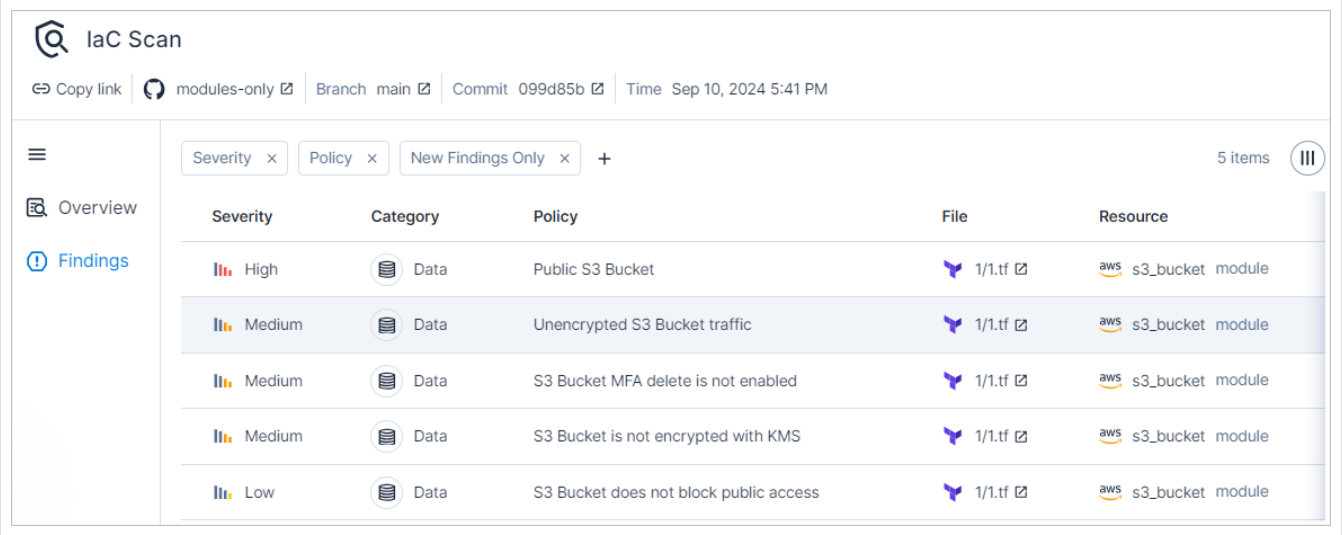
スキャン結果を表示する

スキャン結果を表示するには:

1. クラウドサイバーエクスポージャーコンソールで、**[Risk > Code Scans]** をクリックします。[Code CI/CD Scans] (コード CI/CD スキャン) ページには、パイプライン/リポジトリ全体でTenableによって実行されたすべてのスキャンが表示されます。



2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、IaC スキャンの列データを参照してください。
3. エントリをクリックすると、特定のスキャンに関する詳細情報が表示されます。[IaC Scans] (IaC スキャン) スライドアウトが表示されます。**[検出結果]** タブをクリックして、スキャンで特定されたすべての検出結果のリストを表示します。



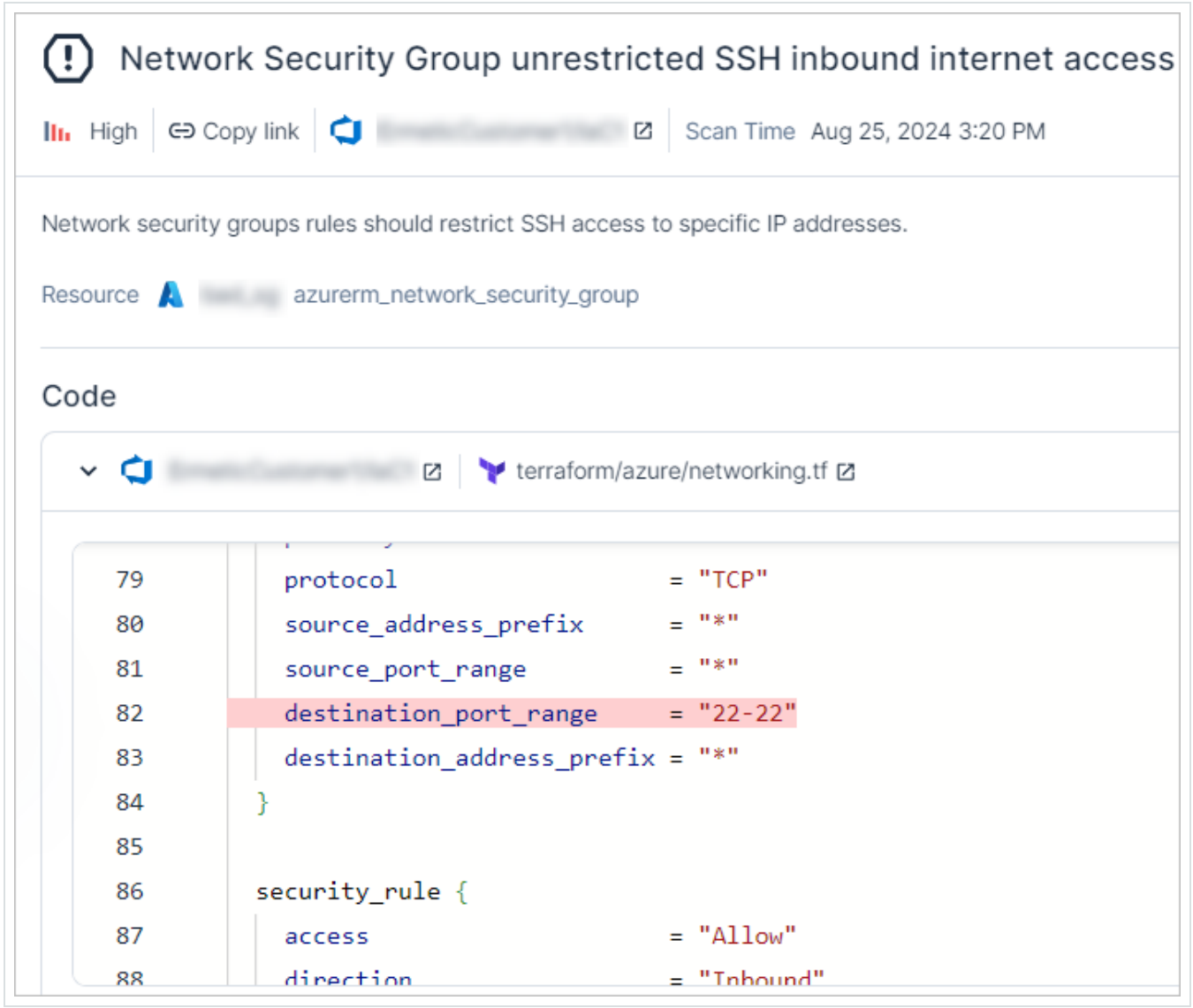
4. 検出結果の表をフィルタリングして、表示するデータの範囲を絞り込みます。

   - テーブルの上部にある **[新規検出結果のみ]** をクリックして、前回のスキャン以降に見つかった IaC 検出結果でテーブルをフィルタリングします。

5. 検出結果をクリックして、特定の問題をドリルダウンします。ここから、影響を受けるリソース全体について、検出結果の概要と説明、および検出結果が見つかった特定のコード部分を確認できます。

   検出結果のタイプにもよりますが、Tenable 次のようにコードがハイライト表示されます。

   - **問題**: グローバル設定がありません。たとえば、アカウントレベルで設定する必要がある VPC フローログや CloudTrail。**ハイライト**:メインファイルの最初の行。
   - **問題**: リソースにフラグがありません。たとえば、暗号化を有効にするフラグがない。**ハイライト**: リソースが定義されている行、またはフラグが欠落しているオブジェクトの最初の行。
   - **問題**:フラグ値の設定ミス。たとえば、インバウンドアドレス範囲のハイ `0.0.0.0/0` **ライト**: リソースの設定ミスがある特定の行。



コードスキャンの列データ

以下の列は、[Risk > Code Scans] (リスク [コードスキャン)] ページのテーブルに表示され、そのほとんどがテーブルのデータのフィルターにも使用できます。

フィルター	説明	デフォルト
時刻	スキャンが実行された日時	○

フィルター	説明	デフォルト
リポジトリ	Tenableによってスキャンされるリポジトリの名前です。	○
ブランチ	スキャンされたブランチの名前。	○
コミット	コミットの数。	○
作者	• **CI/CD パイプラインスキャン**: スキャンをトリガーしたパイプラインイベントを実行したユーザー。 • **リポジトリのスキャン:** コミットを実行したユーザー。	○
検出結果	検出されたIaC検出結果数の深刻 リスク深刻度の色分け別の内訳。	○
結果	スキャンワークフローの合格または失敗のどちらか。ビルドが失敗となる最小ポリシー深刻度のスキャン設定に基づく。	
フレームワーク	解析され、Tenable結果を返したファイルのタイプ。可能な値はCloudFormation、Terraform Code、Terraform Planです。詳細については、「サポートされているプラットフォーム」を参照してください。	いいえ
統合	スキャンされたcode: • **CI/CD パイプライン**の統合名 スキャン: リポジトリが属するパイプラインの名前。 • **リポジトリのスキャン**: ホスティングサービスの名前 (例: GitHub) とそれに続くリポジトリの名前	いいえ
パス	Tenableによってスキャンされたリポジトリのパス。Terraform Cloudの場合、この値はNULLです。これはユーザーの環境内ではなく、実行タスクのコンテキスト内でTenableがスキャンを実行するためです。	いいえ

フィルター	説明	デフォルト
IaC スキャン済みリソース	クラウド サイバーエクスポージャーによってスキャンされた IaC リソースの数。	いいえ
トリガー	スキャンをトリガーしたアクション。	いいえ

スキャン結果の列データ

次の列は、[Scan Results] (スキャン結果) ページのテーブルに表示される列です (特定のスキャンの結果をドリルダウンした後)。そのほとんどが、テーブルのデータのフィルターにも使用できます。

フィルター	説明
クラウド	クラウド サービスプロバイダー (CSP): AWS、Azure、GCP
カテゴリ	ポリシーの ポリシーカテゴリ 。
ポリシー	IaC 検出結果にマッピングされ、検出結果をトリガーした Tenable ポリシーの名前。IaC セキュリティスキャンで使用されるすべてのポリシーのリストについては、IaC ポリシー 。
ファイル	Tenableによってスキャンされた Terraform コード またはプランファイルへのリンク。 Terraform Cloud の場合、この値は NULL です。これはユーザーの環境内ではなく、実行タスクのコンテキスト内で Tenable がスキャンを実行するためです。 **注意**: 作業ディレクトリがリポジトリの root ディレクトリでない場合、ファイルへのリンクが機能しない可能性があります。*
リソース	IaC 検出結果の影響を受けるクラウドリソース。
リソース	IaC 検出結果の影響を受けるクラウドリソースのタイプ。

フィルター	説明
タイプ	
標準	ポリシーのベンチマークにマッピングされるコンプライアンスとセキュリティのベストプラクティス。
新規	この IaC 検出結果が新しいかどうか (以前のスキャンでは検出されなかったかどうか) を示します。これにより、スキャン間の差異を素早く特定し、未解決の可能性がある IaC 検出結果に対処しやすくなります。 • **重要**: このインジケーターは個別のブランチのコンテキスト内で計算されるため、ブランチを初めてスキャンするとき、設定ミスの可能性のあるコード自体がすでに別の場所に存在する場合でも、すべての IaC 検出結果に Tenable 新規としてフラグが立てられます。次回ブランチをスキャンするときには、新しい IaC 検出結果のみがタグ付けされます。

IaC CI/CD スキャン結果のエクスポート

IaC CI/CD スキャン結果を CSV ファイルにエクスポートします。データは、テーブルに適用されている現在のフィルターに従ってエクスポートされ、すべてのテーブル列 (表示または非表示) が含まれます。

IaC CI/CD スキャン結果をエクスポートする方法

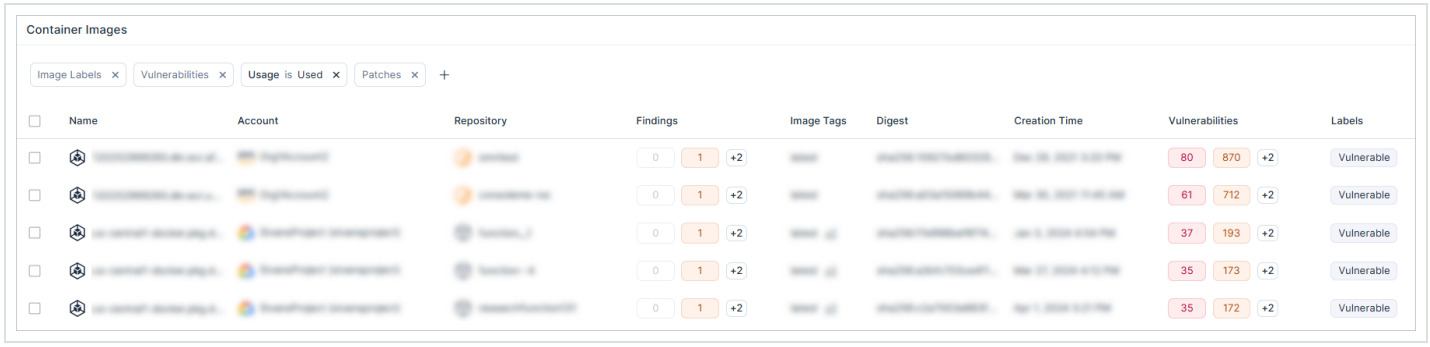
1. **[コード CI/CD >リスク]** に移動します。
2. (オプション)[Organization] (組織) ドロップダウンでコードテナントを選択し、クラウドアカウントの特定のサブセットに関連するポリシーを表示します。デフォルトでは、組織全体 (すべての組織/リポジトリ) が選択されています。
3. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。
4. テーブルの右上隅にある **[Export**] ボタンをクリックします。

1 つの CI/CD スキャン結果をエクスポートすることもできます。

1. **[コード CI/CD >リスク]** に移動します。
2. (オプション)[Organization] (組織) ドロップダウンでコードテナントを選択し、クラウドアカウントの特定のサブセットに関連するポリシーを表示します。デフォルトでは、組織全体 (すべての組織/リポジトリ) が選択されています。
3. テーブル内の特定のスキャンをクリックして、スキャン結果を開きます。
4. 左側のペインで **[検出結果]** をクリックします。
5. テーブルの右上隅にある **[Export]** ボタンをクリックします。

コンテナイメージ CI/CD

Tenable One Cloud Exposureコンソールを使用してスキャン結果を分析し、発生し得る潜在的な問題を特定します。(スキャンが実行された時間とリポジトリでソートされた) 各スキャンについて、深刻度に基づいて検出された問題数の内訳を確認できます。



これは、コンテナイメージの CI/CD スキャン結果を Tenable で表示するためのハウツーガイドです。

- コンテナイメージ CI/CD パイプラインの接続に関する統合ガイドについては、コンテナイメージ CI/CD パイプラインの接続を参照してください。
- Tenable のコンテナイメージスキャン機能の概要については、コンテナイメージスキャンを参照してください。

コンテナイメージ CI/CD スキャンの列データ

次の列は、[Container Image CI/CD Scans]
(コンテナイメージ CI/CD スキャン) ページのテーブルに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

列	説明
時刻	最後のスキャンのタイムスタンプ。
リポジトリ	イメージを含むリポジトリの名前。
ブランチ	リポジトリ内のブランチの名前。
プラグイン名	プラグインの名前とバージョン。プラグイン名のリンクをクリックすると、プラグインの詳細が表示されます。
プラグイン ID	脆弱性の修正を含むパッケージの一意の識別子またはビルド文字列です。
作成者	ビルドまたはスキャンをトリガーしたユーザーのユーザー名
コンテナリポジトリ	コンテナイメージがホストされているレジストリまたは保管場所です。
画像タグ	コンテナイメージに割り当てられた特定のバージョンまたはエイリアス。
ダイジェスト	特定のイメージバージョンの一意で変更不可能な SHA-256 識別子。
イメージラベル	ビルドプロセス中にイメージに割り当てられたメタデータのキーと値のペアです。
イメージ ID	特定のコンテナイメージに割り当てられた一意の識別子 (通常は SHA-256 ハッシュ)。
脆弱性	イメージ内で検出されたセキュリティリスクのサマリー (深刻度別に分類)。
ソフトウェア	コンテナイメージ内で識別されたパッケージ、ライブラリ、または依存関係のリスト。
オペレーティングシ	イメージの特定のオペレーティングシステムのディストリビューション。

列	説明
ステム	
結果	最後のスキャンの結果。
無視された脆弱性	イメージ内で検出された、無視したセキュリティリスクのサマリー(深刻度別に分類)。

スキャン結果を表示する

スキャン結果を表示するには:

1. クラウドサイバーエクスポージャーコンソールで、**[Risk > Container Image CI/CD]** をクリックします。[コンテナイメージ CI/CD のスキャン] ページには、パイプライン全体で Tenable によって実行されたすべてのスキャンが表示されます。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。テーブル右上の列ピッカーを使用して、どの列を表示するか選びます。
3. (オプション)(適用されたフィルターに基づき) 表示可能なすべてのデータを CSV ファイルに **エクスポート** します。
4. エントリをクリックすると、特定のスキャンで特定されたすべての問題が表示されます。結果はスライド式パネルで開きます。
5. 詳細については、次のいずれかのタブをクリックしてください。
   - 概要データ。 Overview
   - 脆弱性の列データ。 Vulnerabilities
   - ソフトウェアの列データ。 Software

概要データ

次の列は [概要] タブに表示され、テーブルのデータのフィルターにも使用できます。

列	説明
コンテナリポジトリ	コンテナイメージがホストされているレジストリまたは保管場所です。
タグ	コンテナイメージに割り当てられた特定のバージョンまたはエイリアス。
ダイジェスト	特定のイメージバージョンの一意で変更不可能な SHA-256 識別子。
イメージラベル	ビルドプロセス中にイメージに割り当てられたメタデータのキーと値のペアです。
解決パッチ	イメージに関連付けられているパッチ。
オペレーティングシステム	イメージの特定のオペレーティングシステムのディストリビューション。
脆弱性	イメージ内で検出されたセキュリティリスクのサマリー(深刻度別に分類)。
結果	最後のスキャンの結果。

[スキャンパラメーター] セクションには、スキャン応答に含まれるパラメーターが一覧表示されます。詳細については、「 Configure Scan Settings」を参照してください。

脆弱性の列データ

次の列は [脆弱性] タブのテーブルに表示され、テーブルのデータのフィルターにも使用できます。

列	説明
ID	CVE の ID。
深刻度	CVE の深刻度。
CVSS スコア	CVE の CVSS スコア。
VPR スコア	Tenableの Vulnerability Priority Rating は、0.1 から 10.0 のスケールで脆弱性

列	説明
	の修正作業に優先順位を付けます。
ソフトウェア	CVE が見つかったソフトウェア。
プラグイン名	プラグインの名前とバージョン。
ソフトウェア修正バージョン	ソフトウェア修正のバージョン。

オープンまたは無視をフィルタリングするには、**[エクスポート]** ボタンの横にある **[開く]** または **[無視]** をクリックします。

ソフトウェアの列データ

次の列は [ソフトウェア] タブのテーブルに表示され、テーブルのデータのフィルターにも使用できます。

列	説明
名前	ソフトウェアパッケージの名前とバージョン。
パス	(ライブラリのみ)パッケージのファイルパス。この情報は、パッケージの入手元と、潜在的な問題を修正する方法を特定する際に役立ちます。たとえば、パッケージがベースイメージの一部としてインストールされているかどうか、またはパッケージがベースイメージに追加されているかどうかを識別できます。
タイプ	パッケージのタイプ。可能な値: Operating System、Library。
脆弱性	パッケージに関連付けられている脆弱性のリストで、CVE ID 別に一覧表示されます。(例: CVE-2021-3177) ID にカーソルを合わせると、脆弱性の詳細 (説明や関連する情報ソースなど) についての概要ビューが表示されます。

JSON 出力の例

以下は、スキャンのレポート出力ファイル(JSON 形式)の例です。

JSON


```
{
    "ImageId": "a97c45fa7217",
    "ConfigurationJson": "{\"config\":{\"Env\":
[\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\"],\"Entrypoint\":[],\"Cmd\":
[\"bash\"]},\"created\":\"2026-08-03T00:00:00Z\",\"history\":[{\"created\":\"2026-08-
03T00:00:00Z\",\"created_by\":\"# debian.sh --arch 'amd64' out/
'bookworm' '@1785715200'\",\"comment\":\"debuerreotype 0.17\"}],\"rootfs\":{\"type\":\"layers\",\"diff_
ids\":
[\"sha256:63ecca237e30aca8ae79232ae01dddab7d8b42302f654f343f7cc7ddae60d57c\"]},\"os\":\"linux\",\"
architecture\":\"amd64\"}\n",
    "Digest": "sha256:813017f3d62be4b5891a7acca6a01bdcd4b8513daa81b1ab99d3a50385b26931",
    "EndTime": "2026-08-06T00:29:48.689087+03:00",
    "IgnoredVulnerabilities": [
        {
            "AttackVector": "Network",
            "CreationTime": "2023-12-12T15:15:00Z",
            "CvssScore": 6.5,
            "CvssVersion": "CVSS3.1",
            "Description": "NCurse v6.4-20230418 was discovered to contain a segmentation fault via the
component _nc_wrap_entry().",
            "Exploitable": false,
            "Layers": [
                {
                    "Command": "# debian.sh --arch 'amd64' out/ 'bookworm' '@1785715200'",
                    "Digest": "sha256:3af9207d37990175f61d5ce9faa0c7373ffcd2d6da1b6ba0a9ca9d61f8f47cc9"
                }
            ],
            "Software": [
                {
                    "Path": "",
                    "Name": "libtinfo6",
                    "Type": "Package",
                    "Version": "6.4-4"
                }
            ],
            "Id": "CVE-2023-50495",
            "Links": [
                "https://lists.gnu.org/archive/html/bug-ncurses/2023-04/msg00020.html"
            ],
            "Resolvable": false,
            "Severity": "Medium",
            "PatchId": "227011"
        }
```

```
    ],
    "OperatingSystem": "debian 12.15",
    "Repository": "docker.io/library/debian",
    "IgnoredVulnerabilitySeverities": {
        "Low": 0,
        "Medium": 1,
        "High": 0,
        "Critical": 0,
        "Information": 0
    },
    "VulnerabilitySeverities": {
        "Low": 0,
        "Medium": 0,
        "High": 0,
        "Critical": 1,
        "Information": 0
    },
    "ScanTime": "2026-08-06T00:29:44.243689+03:00",
    "Success": true,
    "Tag": "12",
    "Link": "http://localhost/customer/Risks/CodeContainerImageScan#workloadAnalysisCodeScan/b4bba018-
280e-4fb6-b7c4-fde1f4b7b8cc",
    "Version": "0.0.0",
    "Vulnerabilities": [
        {
            "AttackVector": "Network",
            "CreationTime": "2026-03-19T15:16:00Z",
            "CvssScore": 9.8,
            "CvssVersion": "CVSS3.1",
            "Description": "The infocmp command-line tool in ncurses before 6.5-20251213 has a stack-based
buffer overflow in analyze_string in progs/infocmp.c.",
            "Exploitable": false,
            "Layers": [
                {
                    "Command": "# debian.sh --arch 'amd64' out/ 'bookworm' '@1785715200'",
                    "Digest": "sha256:3af9207d37990175f61d5ce9faa0c7373ffcd2d6da1b6ba0a9ca9d61f8f47cc9"
                }
            ],
            "Software": [
                {
                    "Path": "",
                    "Name": "libtinfo6",
                    "Type": "Package",
                    "Version": "6.4-4"
                }
            ],
            "Id": "CVE-2025-69720",
```

```
            "Links": [
                "https://github.com/Cao-Wuhui/CVE-2025-69720"
            ],
            "Resolvable": false,
            "Severity": "Critical",
            "PatchId": "303220"
        }
    ]
}
```


ポリシー

クラウドポリシー

これは、検出結果の作成方法を決定するポリシーを管理するためのハウツーガイドです。

- カスタムポリシーを作成するには、「クラウドポリシー: カスタム」を参照してください。
- クラウドの検出結果を表示および管理するには、「クラウドの検出結果」を参照してください。
- 検出結果のステータスと検出結果のライフサイクルについては、「検出結果のライフサイクル」を参照してください。
- 検出結果の深刻度の仕組みについては、「検出結果の深刻度」を参照してください。

標準装備のポリシーとカスタムポリシーの一覧を表示して、Tenable One Cloud Exposure がどのように環境をモニタリングし、ポリシーによってどのように検出結果がトリガーされるのかを確認できます。すべてのポリシーについて、ポリシーのベンチマークにマッピングされる特定のコンプライアンス基準と、そのベンチマークに合格または不合格になったリソースの数が表示されます。

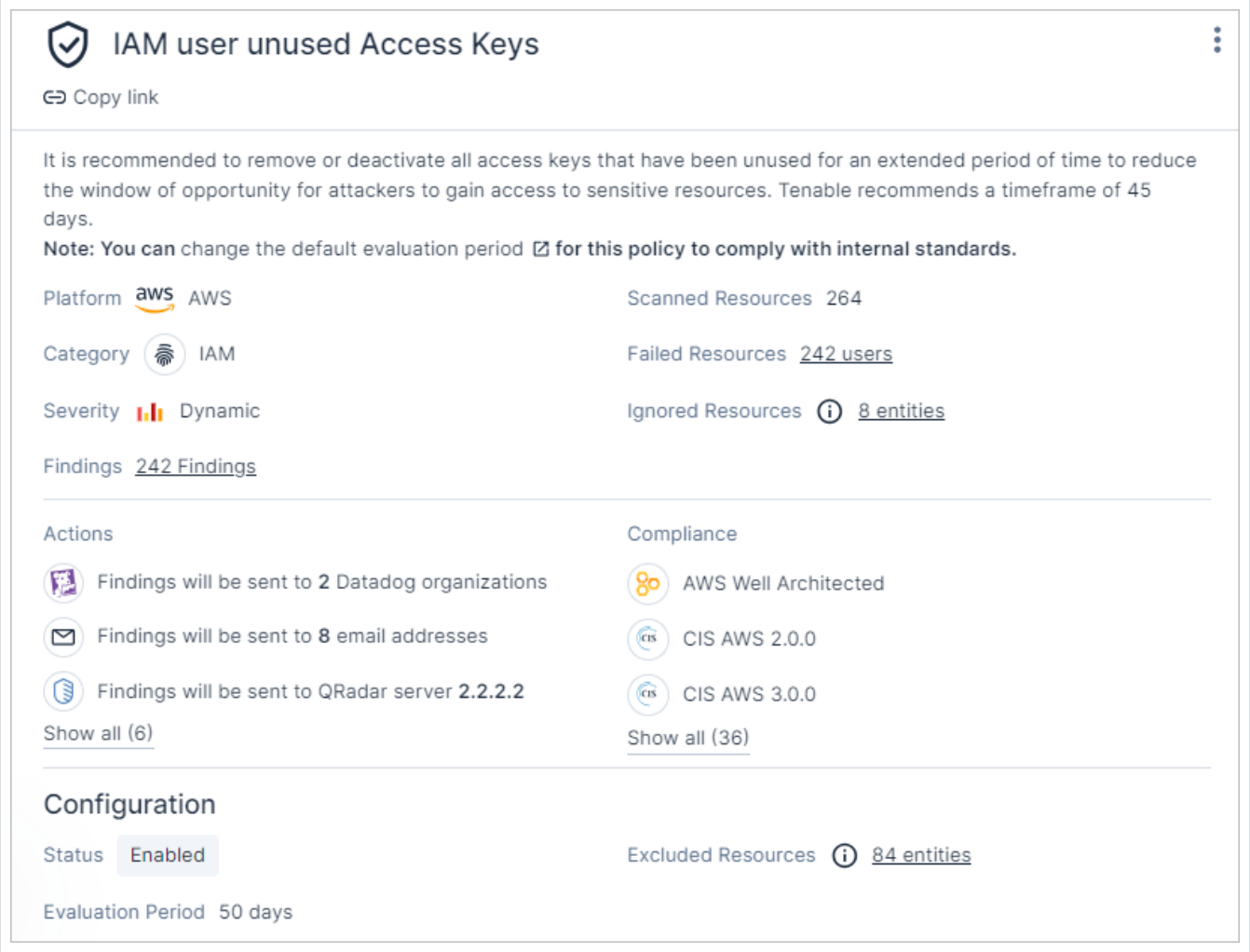
> **注意:** 設定ミス、ネットワークの露出、露出したシークレットに関連するポリシーは、**Standard** および **Enterprise** ライセンスでのみ利用可能です。**CIEM** や **Cloud Vulnerability Management** ライセンスでは利用できません。詳細については、「ライセンス」を参照してください。

ポリシーを管理する

ポリシーを表示および管理する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択して、クラウドアカウントの特定のサブセットまたは IdP のポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. ポリシーを **ビルトイン** または **カスタム** のどちらのポリシーを表示するかを選択します。
4. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。テーブル右上の列ピッカーを使用して、どの列を表示するか選びます。詳細については、ポリシーの列データ を参照してください。
5. ポリシーをクリックすると、詳細情報を含むスライド式パネルが開きます。ポリシーを確認し、管理します。詳細については、ポリシーの列データ を参照してください。スライド式パネルには、次のようなポリシーの詳細が記載されています。
    - **アクション**: 自動化によって作成されるプッシュ通知のリスト。このポリシーによって検出結果がトリガーされたときに統合されたサードパーティツールに送信されます。
    - **構成**: ポリシー用に構成されたすべての設定。たとえば、ポリシーが有効かどうかや、関連するリソースがスキャン、無視、失敗した数が含まれます。
    - **除外**: ポリシーに関連付けられているすべての 除外 。

> スライド式パネルの画像を見る



6. ポリシーの設定を**編集**します。次のポリシー管理アクティビティを実行できます。これらの設定の一部は、特定のポリシーでのみ使用できます。

    - ポリシーの有効化と無効化
    - 検出結果作成を遅延させる
    - 評価期間とパスワード要件を変更する
    - 無効なアイデンティティの検出結果の作成
    - 招待保留中の Microsoft Entra ID ゲストユーザーの検出結果を作成する
    - アクセス許可使用のラーニング期間
    - グループから非アクティブなプリンシパルを削除することが推奨されます
    - メンバーアカウントのルートユーザーの検出結果を作成する

- ポリシーからリソースを除外する
- ポリシーからシークレットを除外する
- パブリック Lambda 関数ポリシーからの API ゲートウェイパスの除外
- ポリシーデータのエクスポート

ポリシーの列データ

次の列は [Policies] (ポリシー) ページのテーブルに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

フィルター	説明
プラットフォーム	たとえば、クラウドサービスプロバイダーや IdP などです。可能な値: AWS、Azure、Microsoft Entra ID、GCP、OCI。
カテゴリ	ポリシーが属する論理カテゴリ。「ポリシーカテゴリ」を参照してください。
名前	ポリシーの名前。
深刻度	ポリシーの深刻度。ポリシーによってトリガーされた検出結果の深刻度を決めます。詳細については、動的な深刻度と静的な重大度を参照してください。
コンプライアンス	ポリシーのベンチマークにマッピングされるコンプライアンス標準とセキュリティのベストプラクティス。
ステータス	ポリシーが有効か無効か。ポリシーを ポリシーの有効化と無効化 にして、ポリシーが対象アカウントのリソースに対して検出結果をトリガーしないようにすることができます。
スキャン済みリソース	ポリシーによってチェックされるリソースの総数。
失敗したリソース	ポリシーのベンチマークに合格できなかったリソースの数。リソースごとに検出結果を分けるポリシーの場合、不合格のリソースの数は検出結果の数と同じになります。リ

フィルター	説明
	ンクをクリックすると、検出結果の一覧が表示されます。
ポリシー Settings	• **検出結果の表示** • **Edit**

ポリシーの有効化と無効化

デフォルトでは、標準装備のポリシーは有効になっており(*モニタリング*ポリシーを除く)、組織内のすべてのアカウントに適用されます。微調整したい場合は、組織全体でポリシーを無効にするか、アカウントやフォルダーの特定のサブセットのみポリシーを無効にすることができます。フォルダーを使用したアカウントのグループ化については、「アカウント階層とフォルダー」を参照してください。たとえば、VPC フローログの問題など、修正の必要がない深刻度の低い設定ミスが検出される場合は、ポリシーを無効にするとよいでしょう。

警告: ポリシーを無効にすると、そのポリシーに関連する検出結果が対象アカウントからすべて削除され、新しい検出結果が作成されなくなります。このアクションは次回 データの同期と更新の頻度 後に実行され、元に戻すことはできません。

注意:

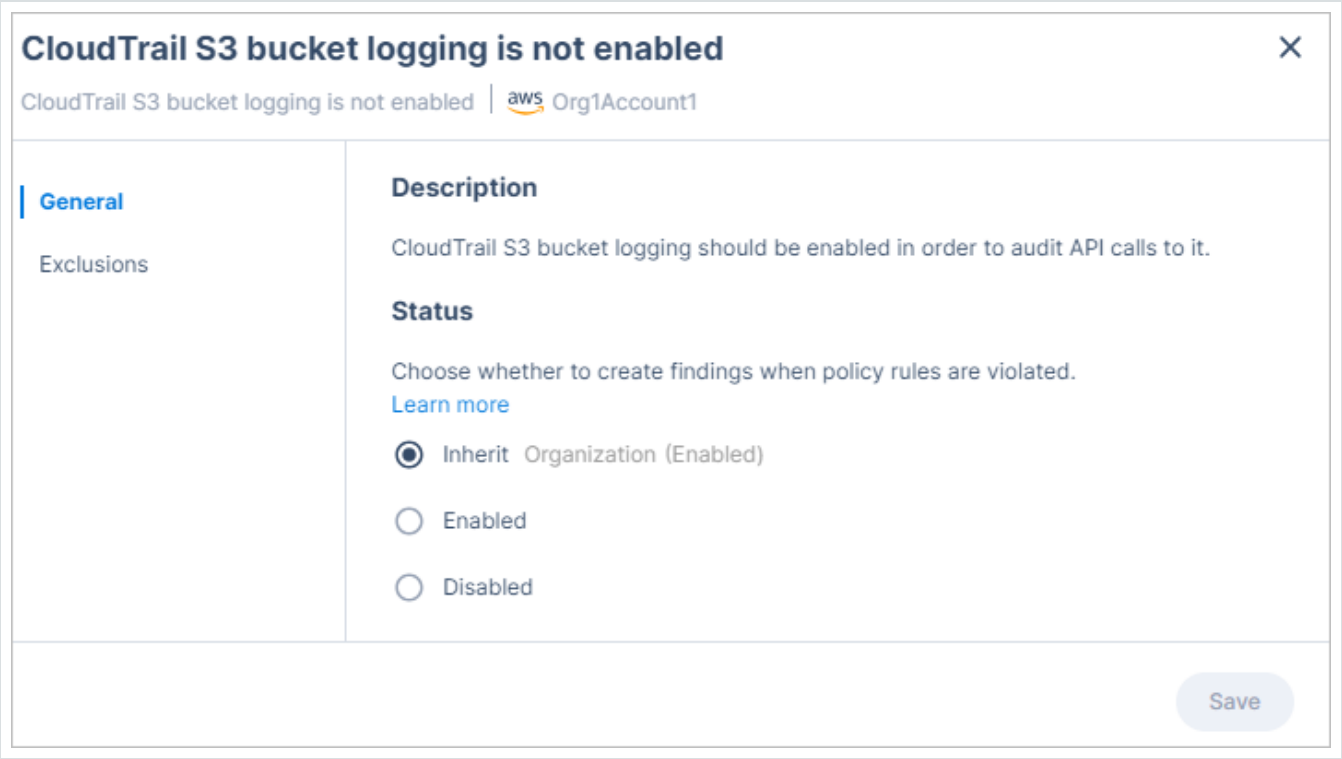
- ポリシーの有効化と無効化は、「管理者」ロールを持つユーザーだけが使用できます。
- たとえば、深刻度の低い問題に関連する一部のポリシーは、デフォルトで無効化されていますが、コンプライアンス準拠のためやその他のセキュリティ目的で有効化が必要な場合は有効にできます。

ポリシーを有効または無効にする

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットでポリシーを有効または無効にします。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. 関連するポリシーに移動します。

4. 三点リーダーメニュー ⋮ をクリックし、**[編集]** をクリックします。

> ポリシー編集ウィンドウの画像を参照してください



親レベルの構成をオーバーライドする場合、親レベルの範囲で行われた変更に関係なく、固有の構成は残ります。

5. **[保存]** をクリックします。

検出結果作成を遅延させる

ポリシールールに違反した後、検出結果の作成を指定した時間延期します。設定された遅延は、その設定が行われた後に作成された新しいリソースにのみ適用されます (リソースの作成時間に基づきます)。この設定は、特定のアカウント範囲のポリシーごとに行われます。この設定は、すべてのポリシーで利用できるわけではありません。

一般的に、検出結果の作成を遅らせないことを クラウドサイバーエクスポージャー は推奨していますが、遅らせた方がよい場合もいくつかあります。たとえば、お使いの環境のメンテナンス中に大量のリソースを作成または削除する場合や、一時的なリソースに関連するノイズを減らす場合などです。

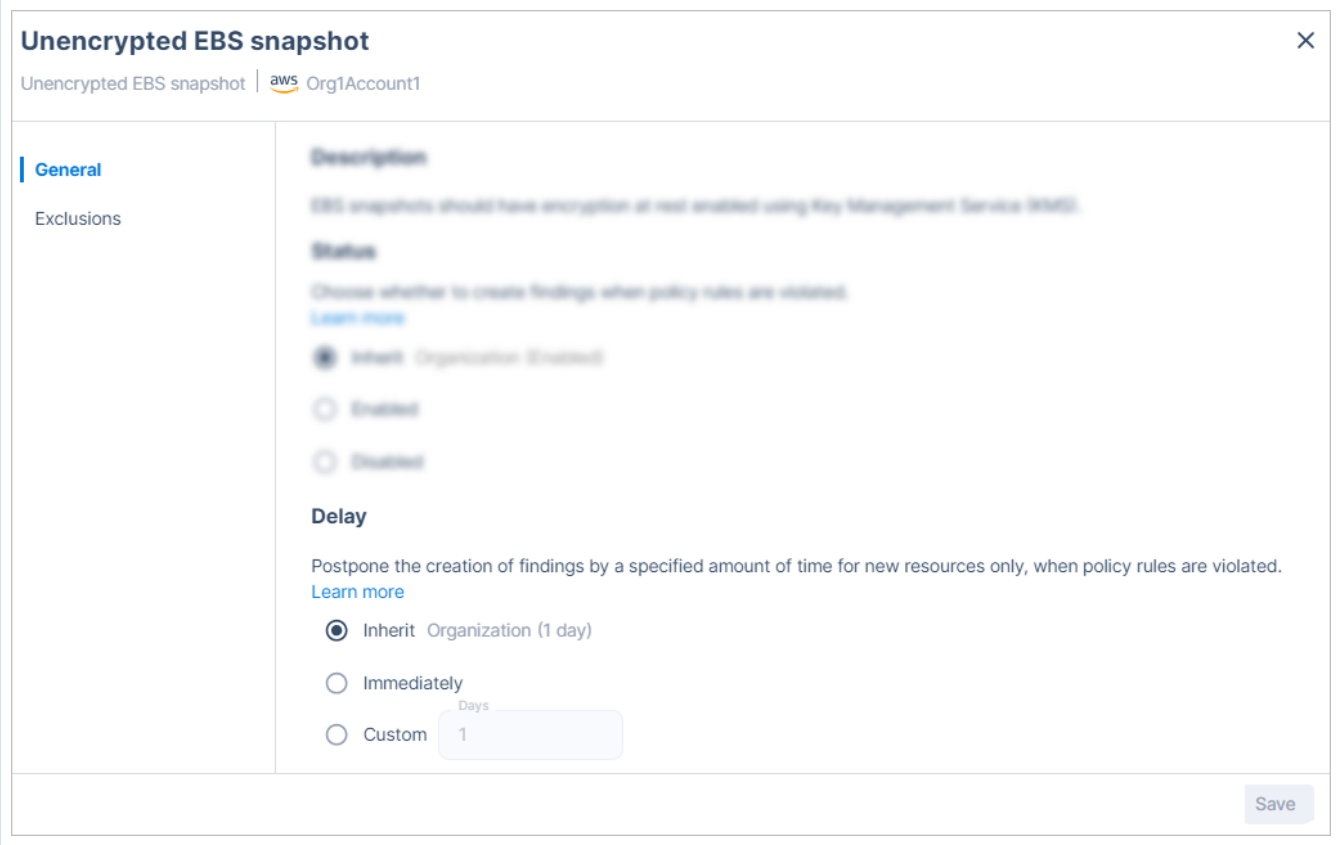
注意: デフォルトでは、Tenable ポリシーはポリシールール違反の直後に検出結果を作成するよう設定されていますが、次の 2 つのポリシーは例外です。ただし、次の 2 つのポリシーは、常に一時的なリソースに関連するため、デフォルトの遅延期間は 1 日です。

- **暗号化されていない EBS スナップショット**
- **暗号化されていない EBS ボリューム**

検出結果の作成を遅らせる方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットでポリシーを有効または無効にします。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. 関連するポリシーに移動します。
4. 三点リーダーメニュー ⋮ をクリックし、**[編集]** をクリックします。

> ポリシー編集ウィンドウの画像を参照してください



親レベルの構成をオーバーライドする場合、親レベルの範囲で行われた変更に関係なく、固有の構成は残ります。

5. **[保存]** をクリックします。

評価期間とパスワード要件を変更する

クラウドサイバーエクスポージャー は、特定のポリシーに対してデフォルトの評価期間とパスワード要件を使用します。組織はこれらのポリシーをカスタマイズして、内部ポリシー基準を定義できます。たとえば、キーのローテーションをデフォルトの 12 か月ではなく、6 か月ごとに設定できます。

- **評価期間**とは、検出結果をトリガーする前にポリシーを評価するために使用される時間設定を指します。これには、**ローテーション期間**、**保持期間**、**非アクティブ期間**があり、それぞれでポリシーを適用する特定の期間を定義します。これにより、検出結果がオープンになる前に時間をかけてリソースを分析できます。

- **パスワード要件**とは、文字長さなどのパスワード設定のことで、アカウントのパスワードを作成するときにパスワードがパスワードポリシーの要件に確実に適合するようにします。パスワードの長さはデフォルトで 14 文字ですが、たとえばこれを 20 文字にすることができます。

評価期間またはパスワード要件を変更する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. サポートされているいずれか サポートされているポリシーに移動します。
3. 三点リーダーメニュー ⋮ をクリックし、**[編集]** をクリックします。
4. **[詳細]** をクリックします。
5. セクションのタイトルは、ポリシー設定のタイプによって異なります。
    - ローテーション期間: ローテーション期間のカスタム日数を選択します。
    - 保持期間: 保持期間のカスタム日数を選択します。
    - 非アクティブ期間: 非アクティブ期間のカスタム日数を選択します。
    - パスワード要件: デフォルト値を更新します。
6. アカウントの範囲が [組織] にない場合は、該当するオプションを選択します。
    - **継承。** 親レベルのアカウント範囲の設定を継承 (デフォルト)。継承された設定は、親レベル範囲の名前の横の括弧内に表示されます。組織全体を範囲として選択した場合、このオプションは表示されません。
    - **カスタム** (親レベルの設定をオーバーライド)。評価期間のカスタム日数 (1 ~ 365) を選択します。

    > **注意:** 親レベルの構成をオーバーライドする場合、親レベルの範囲で行われた変更に関係なく、固有の構成は残ります。
7. **[保存]** をクリックします。

サポートされているポリシー

内部基準に準拠するために、次のポリシーのデフォルトの評価期間とパスワード要件を変更できます。

プラットフォーム	ポリシー設定の種類	ポリシー名	デフォルト値
AWS	非アクティブの期間	IAM ユーザーの未使用アクセスキー	45日
AWS	非アクティブの期間	IAM ユーザーの未使用パスワード	45日
AWS	非アクティブの期間	未使用のセキュリティグループ	30 日
AWS	パスワード要件	パスワードの長さが最小要件を満たしていません	14 文字
AWS	パスワード要件	パスワード再利用ポリシーが最小要件を満たしていません	24 個のパスワード
AWS	保持期間	DocumentDB クラスタの自動バックアップ保持期間が最小要件を満たしていません	7 日
AWS	保持期間	Elastic Beanstalk 環境が CloudWatch Logs にログを公開していません	7 日
AWS	保持期間	ElastiCache Redis OSS クラスタキャッシュの自動バックアップ保持期間が最小要件を満たしていません	1日
AWS	保持期間	Neptune クラスタの自動バックアップ保持期間が最小要件を満たしていません	7 日
AWS	保持期間	RDS クラスタの自動バックアップ保持期間が最小要件を満たしていません	7 日

プラットフォーム	ポリシー設定の種類	ポリシー名	デフォルト値
AWS	保持期間	RDS インスタンスの自動バックアップ保持期間が最小要件を満たしていません	7 日
AWS	保持期間	Redshift クラスタの自動バックアップ保持期間が最小要件を満たしていません	7 日
AWS	ローテーション期間	IAM ユーザーのアクティブなアクセスキーがローテーションされていません	90 日
AWS	ローテーション期間	KMS キーの自動キーローテーションが有効になっていない	365日
AWS	ローテーション期間	KMS キーがローテーションされていません	365日
Azure	保持期間	ストレージアカウントの SQL Server 監査保持が設定されていません	90 日
Azure	ローテーション期間	Key Vault 証明書の自動ローテーションが有効になっていない	730日
Azure	ローテーション期間	Key Vault 証明書がローテーションされていません	365日
Azure	ローテー	Key Vault キーの自動キーローテーションが有効になって	730日

プラットフォーム	ポリシー設定の種類	ポリシー名	デフォルト値
	ション期間	いません	
Azure	ローテーション期間	Key Vault キーがローテーションされていません	730日
Azure	ローテーション期間	Key Vault シークレットがローテーションされていない	365日
GCP	非アクティブの期間	未使用の GCP プロジェクト	30 日
GCP	ローテーション期間	Cloud KMS キーローテーションが設定されていません	90 日
GCP	ローテーション期間	プロジェクト API キーがローテーションされていません	90 日
GCP	ローテーション期間	Secret Manager のシークレットのローテーションが設定されていません	90 日
GCP	ローテーション期間	サービスアカウントのユーザーマネージドキーがローテーションされていない	90 日

プラットフォーム	ポリシー設定の種類	ポリシー名	デフォルト値
Microsoft Entra ID	ローテーション期間	アプリ登録証明書がローテーションされていない	365日
Microsoft Entra ID	ローテーション期間	アプリ登録シークレットがローテーションされていません	180日
OCI	パスワード要件	パスワード期限切れポリシーが最小要件を満たしていません	365日
OCI	パスワード要件	パスワード長ポリシーが最小要件を満たしていません	14 文字
OCI	パスワード要件	パスワード再利用ポリシーが最小要件を満たしていません	24 個のパスワード
OCI	ローテーション期間	ユーザー API キーがローテーションされていません	90 日
OCI	ローテーション期間	ユーザー認証トークンがローテーションされていません	90 日
OCI	ローテーション期間	ユーザーの顧客秘密キーがローテーションされていません	90 日

プラットフォーム	ポリシー設定の種類	ポリシー名	デフォルト値
OCI	ローテーション期間	ユーザーのデータベースパスワードがローテーションされていません	90 日
OCI	ローテーション期間	Vault マスター暗号化キーがローテーションされていません	365日

無効なアイデンティティの検出結果の作成

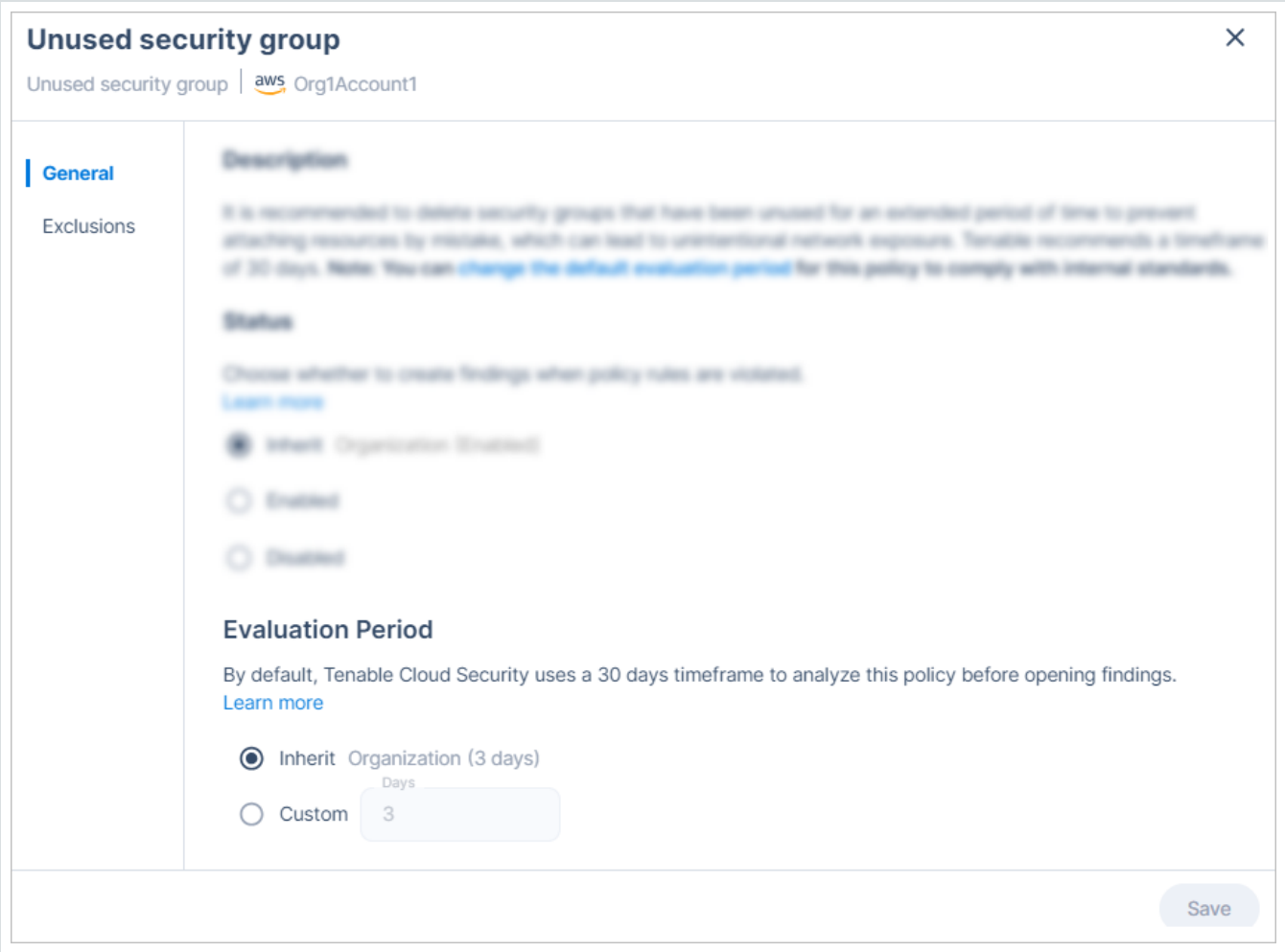
無効なアイデンティティに非アクティブなIAMポリシーを適用するかどうかを選択します。非アクティブなユーザーをデフォルトで無効にしたくない場合は、無効なアイデンティティにポリシーを適用できます。

- ポリシーに対してこのオプションを有効にすると、無効なアイデンティティの検出結果も作成されます。すべてのポリシーの検出結果の修正手順として、アイデンティティの削除が推奨されます。
- ポリシーに対してこのオプションを無効にすると(デフォルトの動作)、無効なアイデンティティの検出結果は作成されません。すべてのポリシーの検出結果の修正手順として、アイデンティティの削除または無効化が推奨されます。

無効なアイデンティティの検出結果を作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットでポリシーを有効または無効にします。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. サポートされているいずれか サポートされているポリシー に移動します。
4. 三点リーダーメニュー ⋮ アイコンをクリックし、**[編集]** をクリックします。

ポリシー編集ウィンドウの画像を参照してください



親レベルの構成をオーバーライドする場合、親レベルの範囲で行われた変更に関係なく、固有の構成は残ります。

5. **[保存]** をクリックします。

サポートされているポリシー

次のポリシーで、無効なアイデンティティの検出結果作成を有効または無効にできます。

- GCP
  - 非アクティブなサービスアカウント

- Google Workspace
    - 非アクティブな Google Workspace ユーザー
- Microsoft Entra ID
    - 非アクティブな Microsoft Entra ID アプリケーション
    - 非アクティブな Microsoft Entra ID ユーザー

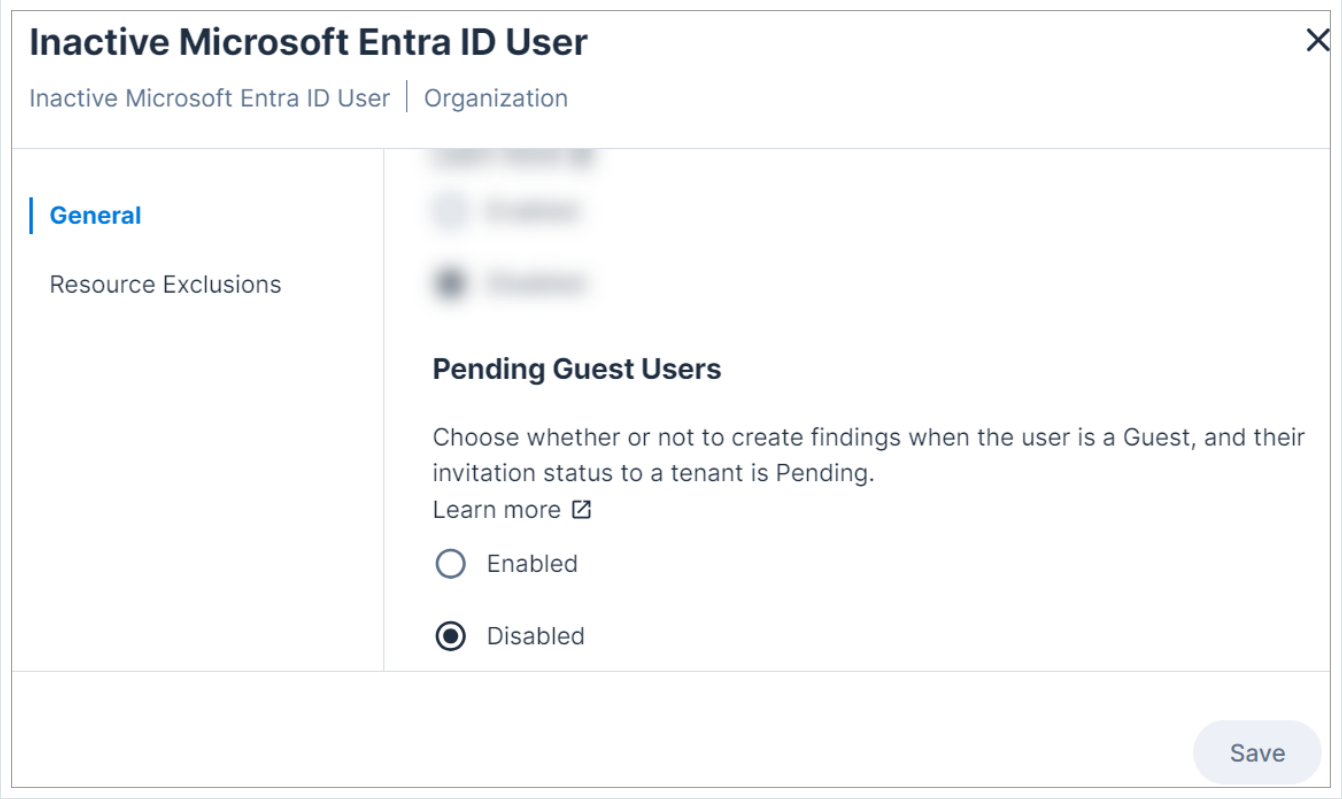
招待保留中の Microsoft Entra ID ゲストユーザーの検出結果を作成する

ユーザーがゲストで、テナントへの招待ステータスが保留中の場合に、検出結果を作成するかどうかを選択します。これにより、非アクティブな Microsoft Entra ID ユーザーから、テナント参加招待をまだ承諾していない Microsoft Entra ID ゲストユーザーを除外できます。

招待保留中のゲストユーザーの検出結果を作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットでポリシーを有効または無効にします。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. 「非アクティブな Microsoft Entra ID ユーザー」ポリシーに移動します。
4. 三点リーダーメニュー ⋮ アイコンをクリックし、**[編集]** をクリックします。

> ポリシー編集ウィンドウの画像を参照してください



親レベルの構成をオーバーライドする場合、親レベルの範囲で行われた変更に関係なく、固有の構成は残ります。

5. **[保存]** をクリックします。

アクセス許可使用状況の学習期間を変更する

過剰なアクセス許可と非アクティブなアイデンティティに関する記事のアクセス アクセス許可使用のラーニング期間 を参照してください。

グループから非アクティブなプリンシパルを削除することが推奨されます

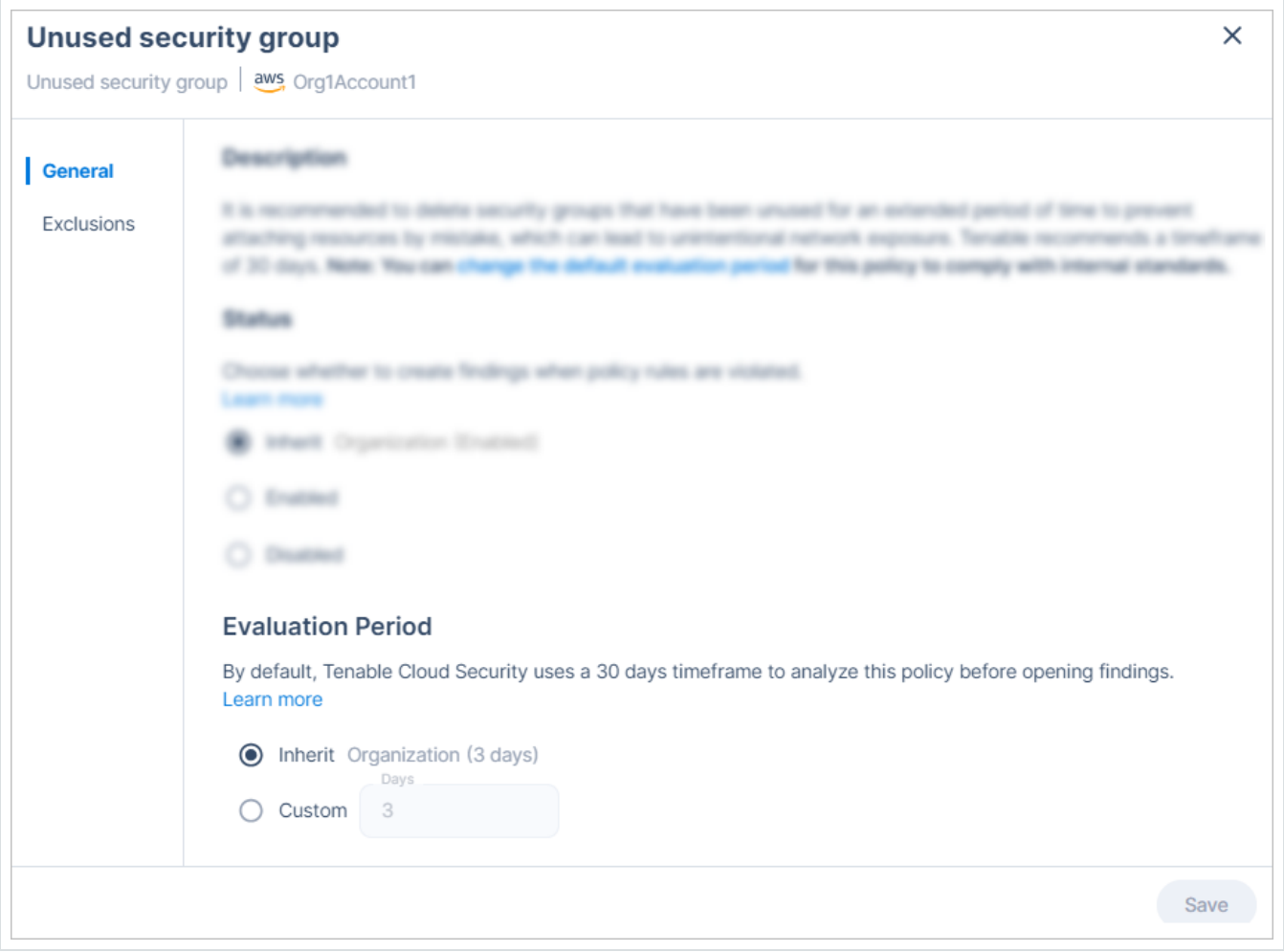
プリンシパルが非アクティブなときに、過剰な権限の検出結果 検出結果の修正 で Tenable がグループからプリンシパルを削除することを推奨するかどうかを選択します。組織の IdP グループが、クラウドアクセス許可の管理以外の目的で使用されている場合 (SaaS アプリケーションや組織構造の管理など)、このオプションを無効にできます。

- 2024 年 8 月 11 日より前にクラウドサイバーエクスポージャーの使用を開始したお客様の場合、このオプションはデフォルトで有効になっています (「サブスクリプションで過剰な権限を持つ Microsoft Entra ID グループポリシーを除く」)。
- 2024 年 8 月 11 日以降にクラウドサイバーエクスポージャーの使用を開始したお客様の場合、このオプションはデフォルトで無効になっています。

グループから非アクティブなプリンシパルを削除することを推奨する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットでポリシーを有効または無効にします。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. サポートされているいずれか サポートされているポリシー に移動します。
4. 三点リーダーメニュー ⋮ アイコンをクリックし、**[編集]** をクリックします。

> ポリシー編集ウィンドウの画像を参照してください



クラウドサイバーエクスポージャーは、ユーザーが非アクティブな場合、検出結果 検出結果の修正 でユーザーをグループから削除することを推奨します。

5. **無効化** (親レベルの設定をオーバーライド)。クラウドサイバーエクスポージャーは、ユーザーが非アクティブの場合、検出結果 検出結果の修正 でユーザーをグループから削除することは推奨しません。

   > **注意:** 親レベルの構成をオーバーライドする場合、親レベルの範囲で行われた変更に関係なく、固有の構成は残ります。

6. **[保存]** をクリックします。

サポートされているポリシー

次のポリシーで、非アクティブなプリンシパルをグループから削除することを推奨するかどうかを設定できます。

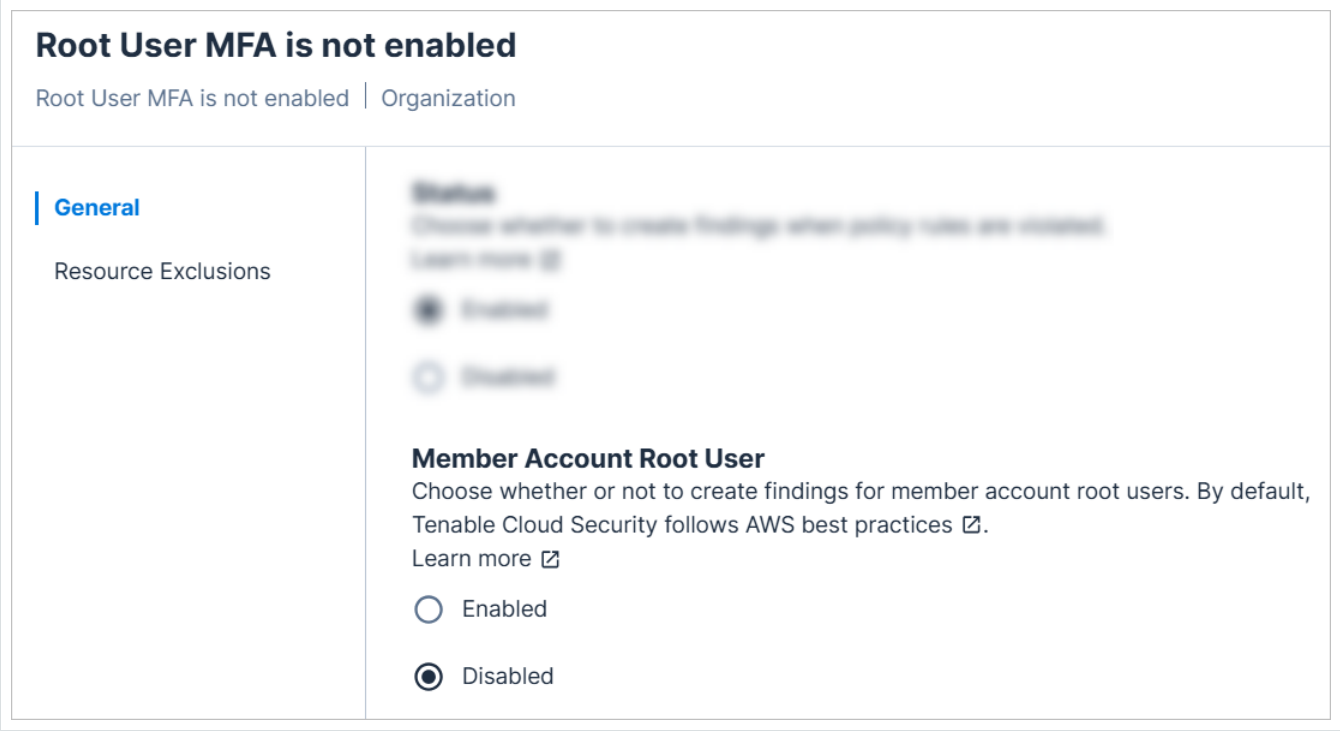
- Azure
    - サブスクリプションで過剰な権限を持つマネージド ID
    - サブスクリプションで過剰な権限を持つ Microsoft Entra ID アプリケーション
    - サブスクリプションで過剰な権限を持つ Microsoft Entra ID グループ
    - サブスクリプションで過剰な権限を持つ Microsoft Entra ID ユーザー
- GCP
    - プロジェクトで過剰な権限のサービスアカウント
    - プロジェクトで過剰な権限を持つユーザー

メンバーアカウントのルートユーザーの検出結果を作成する

[Root User MFA is not enabled] (ルートユーザーの MFA が有効になっていない) ポリシーで、メンバーアカウントのルートユーザーの検出結果を作成するかどうかを選択します。デフォルトでは、このオプションは**無効**になっており、AWS のベストプラクティスに従っています。

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットでポリシーを有効または無効にします。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. **[Root User MFA is not enabled] (ルートユーザーの MFA が有効になっていない)** ポリシーに移動します。
4. 三点リーダーメニュー ⋮ アイコンをクリックし、**[編集]** をクリックします。

> ポリシー編集ウィンドウの画像を参照



クラウドサイバーエクスポージャー、メンバーアカウントのルートユーザーに関する検出結果を作成します。

5. **無効化** (親レベルの設定をオーバーライド)。クラウドサイバーエクスポージャーでは、メンバーアカウントのルートユーザーの検出結果は作成されません。

   > **注意:** 親レベルの構成をオーバーライドする場合、親レベルの範囲で行われた変更に関係なく、固有の構成は残ります。

6. **[保存]** をクリックします。

ポリシーからリソースを除外する

除外、ポリシーからリソースを除外したり、関連する検出結果の深刻度を変更したりできます。検出結果ごとに、または無視された検出結果からのパターンベースの除外の作成に基づいて作成し、除外を監査して維持することで正確性を保つことができます。

ポリシーからシークレットを除外する

検出された誤検出に対処するために、ポリシーからシークレットを除外します。シークレットはキーと値のペアで構成され、どちらかにシークレットが含まれます。除外したいパターンを入力します。パターンがシークレットと一致した場合、クラウドサイバーエクスポージャーはそのシークレットを除外します。たとえば、値パターン `https://*` を使用した場合、シークレットとして誤検出されたURLはすべて除外されます。

このオプションは、シークレットの公開に関連するポリシーで利用できます。たとえば、CloudFormationスタックでシークレットが公開されています。

> **注意:**
>
> - ポリシーからのシークレット除外は、「コラボレータ」または「管理者」ロールのいずれかを持つユーザーが利用できます。
> - [ポリシー] ページからシークレットを除外する場合
>   - 除外は次回のシステムデータの同期と更新の頻度時に更新されます。
>   - 除外は永続的です(手動で削除しない限り)。
>
>   直ちに実装される除外の変更を行うには、[Findings] (検出結果) ページからシークレットを除外します。

ポリシーからシークレットを除外する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットについてリソースを除外します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. 関連するポリシーに移動します。
4. 三点リーダーメニュー ⋮ アイコンをクリックし、**[編集]** をクリックします。
5. 設定ダイアログで、**[シークレットの除外]** に移動します。
6. **キーパターン**と**値パターン**を入力します。パターンでは次のワイルドカード文字を使用できます。
   - アスタリスク * - 0文字以上と一致
   - クエスチョンマーク ? - 1文字と一致
7. (オプション) **コメント**を追加します。

8. **[大文字と小文字を無視** する] (大文字と小文字を同一の文字として処理する) かどうかを選択します。
9. **[保存]** をクリックします。

パブリック Lambda 関数ポリシーからの API ゲートウェイパスの除外

意図した設定を反映するように、API ゲートウェイリソースパスとメソッドを設計上パブリックとして定義します。リソースパスパターンと HTTP メソッド (例: Get) を入力します。検出されたパスとメソッドが一致する場合、Tenable はそれらを設計上パブリックとして分類し、関連する検出結果をクローズします。たとえば、Get で「/health」と入力すると、この組み合わせが意図的にパブリックとしてマークされます。

除外は次回のシステムデータの同期と更新の頻度時に更新されます。

API ゲートウェイパスを除外するには

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー] > [クラウドポリシー]** の順にクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットについてリソースを除外します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. **パブリック Lambda 関数**ポリシーに移動します。
4. 三点リーダーメニュー ⋮ アイコンをクリックし、**[編集]** をクリックします。
5. 設定ダイアログで、**API ゲートウェイのパスの除外**に移動します。
6. **パスパターン**を入力します。パターンでは次のワイルドカード文字を使用できます。
    - アスタリスク * - 0 文字以上と一致
    - クエスチョンマーク ? - 1 文字と一致
7. HTTP メソッドを選択します。
8. (オプション) **コメント**を追加します。
9. **[大文字と小文字を無視** する] (大文字と小文字を同一の文字として処理する) かどうかを選択します。
10. **[保存]** をクリックします。

ポリシーデータのエクスポート

CSV ファイルにポリシーデータをエクスポートします。データは、テーブルにその時点で適用されているフィルターに従ってエクスポートされます。データには、ポリシーによってトリガーされる特定の検出結果でフィルタリングされた [Findings] (検出結果) ページの URL など、関連するすべてのポリシーデータが含まれます。

ポリシーデータをエクスポートする方法

1. (オプション)[Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択し、クラウドアカウントの特定のサブセットに関連するポリシーを表示します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。詳細については、ポリシーの列データ を参照してください。
3. ポリシーの表の右上隅にある **[Export** ⤓ **]** ボタンをクリックします。

Azure で非アクティブなシステムマネージド ID の検出結果を作成する

Azure では、一部のシステムマネージド ID は、たとえ非アクティブであっても削除できません。このような場合でも、Tenable はこれらのアイデンティティについて、深刻 検出結果の深刻度 が **情報** 修正手順が不要であることを発見しました。
削除できるシステムマネージド ID の場合は、修正手順があり、深刻度レベルが高い可能性があります。

削除できるシステムマネージド ID

非アクティブ時に Azure で削除できるシステムマネージド ID は次のとおりです。

- AI サービス
- API Management サービス
- アプリ設定
- アプリサービス
- Automation アカウント

- Azure Database for MySQL フレキシブル サーバー
- Backup Vault
- CDN プロファイル
- コンテナアプリ
- コンテナインスタンス
- コンテナレジストリ
- CosmosDB アカウント
- データ収 集 ルール
- Data Explorer クラスタ
- Data Factory V2
- Digital Twins インスタンス
- Grafana
- IoT Hub
- ロジックアプリ
- Maps アカウント
- PostgreSQL データベースフレキシブルサーバー
- リカバリサービス Vault
- Redis キャッシュ
- 検 索 サービス
- SignalR サービス
- SQL Managed Instance
- SQL Server
- 静 的 サイト
- 仮 想 マシン
- 仮 想 マシンスケールセット
- Web PubSub

ポリシーカテゴリ

クラウドサイバーエクスポージャーには論理的に次のカテゴリに分類された、標準装備のポリシーが多数あります。

- **AI**。クラウド環境でのAIサービスやAI活用型リソースの使用に関連するセキュリティ、ガバナンス、設定のリスクを検出するポリシーが含まれます。
- **コンピューティング**。たとえば、「EC2インスタンスメタデータサービスは安全でないバージョンをサポートする」ポリシーが含まれます。これは、IMDSv2ではなくインスタンスメタデータサービスバージョン1 (IMDSv1)を通じてIAMロール認証情報を取得するEC2インスタンスを識別します。IMDSv1とIMDSv2の両方が利用可能で、デフォルトで有効になっていますが、IMDSv2のみを使用する必要があります。
- **データ**。たとえば、パブリックにアクセス可能なリソースや暗号化されていないデータリソースを検出するポリシーが含まれます。
- **IAM**。たとえば、過剰な権限を持つIAMアイデンティティを検出するポリシーが含まれます。
- **Kubernetes**。Kubernetesコンテナの設定ミスを検出するポリシーが含まれます。
- **ロギング。**クラウドログに関連する設定ミスを検出するポリシーが含まれます。
- **管理**。新しいアカウントがクラウド環境に追加されたことを検出するポリシーが含まれます。
- **モニタリング。**AWS CloudWatchアラームの欠落を検出するポリシーが含まれます。このアラームは環境にさまざまな変更が行われた際に通知するために使用されます。
- **ネットワーク**。たとえば、パブリックネットワークへの露出や安全でないネットワークの設定を検出するポリシーが含まれます。
- **シークレット**。シークレットを露出するリソースを検出するポリシーが含まれます。
- **ワークロード保護**。ワークロードの脆弱性を特定、評価、処理、報告するポリシーが含まれます。
- **異常検出**アイデンティティによって実行される異常な動作を検出するポリシーが含まれます。
- **カスタムポリシー**作成したカスタムポリシーがすべて含まれます。「クラウドポリシー: カスタム」を参照してください。

注意:

- ワークロード保護ポリシーは、Standard ライセンスと Enterprise ライセンスでのみ使用できます。
- 設定ミス、ネットワークの露出、および露出したシークレットに関連するポリシーは、CSPM、Standard、Enterprise のライセンスでのみ利用可能です。CIEM ライセンスでは利用できません。詳細については、ライセンスを参照してください。

クラウドポリシー: カスタム

これは、カスタムクラウドポリシーを作成するためのハウツーガイドです。

- ポリシーを管理するには、「クラウドポリシーを参照してください。
- クラウドの検出結果を表示および管理するには、「クラウドの検出結果を参照してください。
- 検出結果のステータスと検出結果のライフサイクルについては、「検出結果のライフサイクルを参照してください。
- 検出結果の深刻度の仕組みについては、「検出結果の深刻度を参照してください。

組織に関連する特定の問題に対処するためのカスタムポリシーを作成します。カスタムポリシーは、以下に基づいて設定できます。

- 使いやすいカスタムポリシーテンプレート。
- Explorer クエリ。探索 エクスプローラーの詳細については、こちらをご覧ください。
- 新規またはインポートされたカスタム Rego ポリシー (早期アクセス) (早期アクセス)。

組織レベルまたはアカウント (フォルダー) のグループ内で作成されたカスタムポリシーは、今後作成される子アカウントを含め、すべての子アカウントに継承されます。カスタムポリシーを クラウドの検出結果 できるのは、自分が作成した元のフォルダーやアカウントからのみです。たとえば、最上位の AWS フォルダーからカスタムポリシーを作成した場合、その AWS フォルダー内の子フォルダー/アカウントからポリシーを有効化/無効化することはできません。この場合、上位の AWS フォルダーで定義したステータスは、すべての子フォルダーや子アカウントに反映されます。フォルダーの詳細については、「アカウント階層とフォルダー を参照してください。

自動化を作成して [**すべての**ポリシー] に適用することを選択した場合、選択した自動化ターゲット (アクション) は作成するカスタムポリシーにも適用されます。

カスタムポリシーの追加

カスタムポリシーを追加する方法

1. (オプション)**[Organization] (組織)** ドロップダウンでアカウント階層とフォルダーを選択して、カスタムポリシーの範囲をクラウドアカウントの特定のサブセットに制限します。デフォルトでは、組織全体(すべてのアカウント)が選択されています。
2. 左側のナビゲーションペインで、[ポリシー] > **[クラウドポリシー]** の順にクリックします。
3. **[カスタム]** タブを選択します。
4. **[+ カスタムポリシーの作成]** をクリックします。[Create Custom Policy] (カスタムポリシーの作成) ウィザードが開きます。
5. ポリシーのタイプを選択します。

   クエリ

   クエリからのカスタムポリシーの作成 クエリをカスタムポリシーに変換します。たとえば、一般に公開されている EC2 インスタンスを機密タグで追跡するためのポリシーを作成します。クエリを使用するには、**クエリの選択** をクリックして既存のクエリを選択するか、ゼロから作成します。

   - リンクされたクエリを削除したり、プライベートにしたり、サポートされていない構文で編集したりすることはできません。
   - 既存のクエリを選択して編集する場合は、三点リーダーメニューを開き、[**リンク解除** をクリックしてフィルターを変更します。ポリシーは元のクエリと同期されなくなります。

   テンプレート

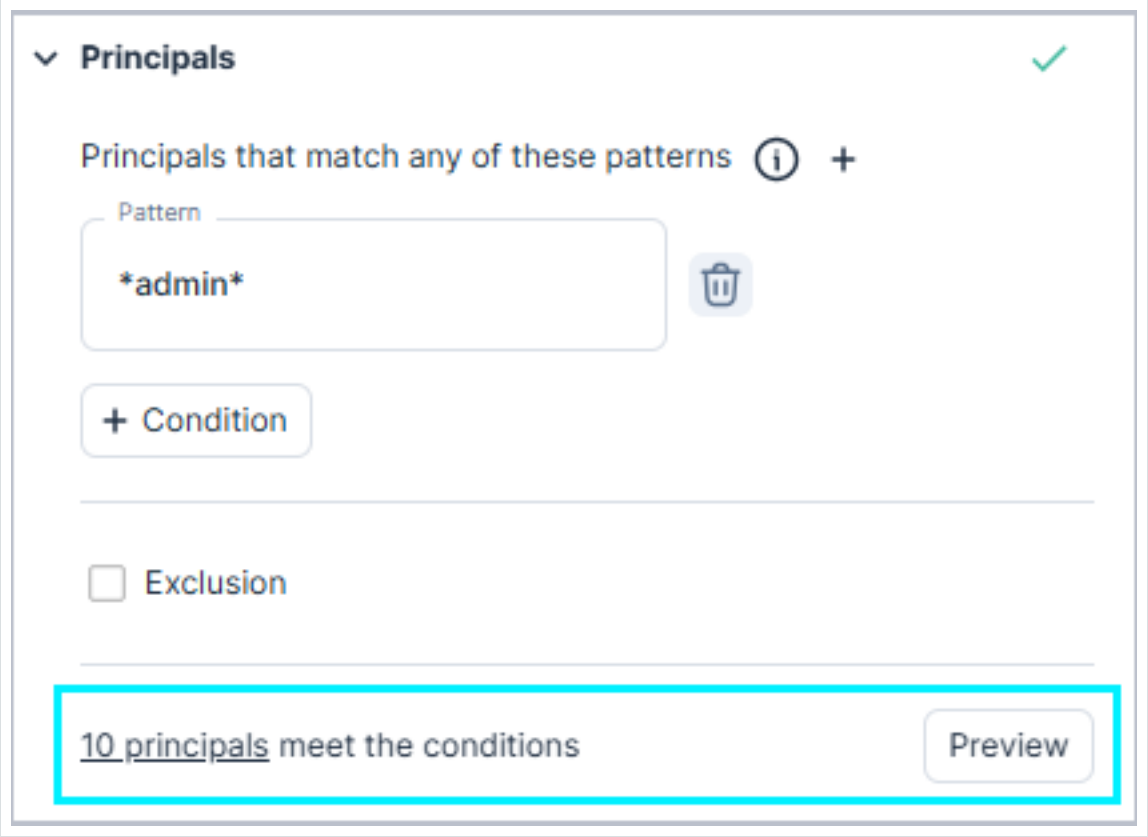
   組織に関連する特定の問題に対処するための使いやすいカスタムポリシーテンプレート

   1. このポリシーに使用するテンプレートを選択し、**選択** をクリックします。
   2. 選択したテンプレートに応じて、ポリシーを適用するタイミングを定義する条件を選択する必要があります。たとえば、**アクセス許可のモニタリング** > **これらのプリンシパルはこれらのリソースに対してこれらのアクセス許可を持つべきではない** を選択した場合、ポリシーが適用されるプリンシパル、アクセス許可 (特定のアクションまたは大きなカテゴリのいずれか)、リソースを選択

する必要があります。任意の条件に対して、1つ以上のエンティティを選択できます。

> **Explorer ベースのテンプレート:** 一部のテンプレートでは、個別のパラメーターピッカーの代わりにエクスプローラークエリエディターが使用されます。これらのテンプレートの場合、右側のパネルに事前構築済みのクエリが表示されます。Explorer クエリエディターを使用してクエリを調整できます。詳細は、エクスプローラーを参照してください。

3. ポリシーを作成する前に**プレビュー**ボタンをクリックすると、一致する**プリンシパル**と**リソース**の数が表示されます。カウントをクリックすると、一致する特定のエンティティが表示されます。



複数選択用の論理演算子

- ***タグ/ラベル***: 複数のタグまたはラベルを選択すると(たとえば、*これらのタグを持つリソース*)、ALL 論理演算子が適用され、ポリシーは指定されたすべてのタグまたはラベルが識別された場合にのみトリガーされます。このコンテキストで ANY ロジックをタグ/ラベルに適用するには、複数のカスタムポリシーを作成し、トリガーとする特定のタグ/ラベルを使用して各ポリシーを設

定します。

- **その他すべての条件**: 複数のエンティティ/リソースを選択した場合、ANY 論理演算子が適用されます。これは、指定されたリソースのいずれかが識別された場合にポリシーがトリガーされることを意味します。
- 次のテンプレートでは、ALL 演算子とANY 演算子のどちらを適用するかを選択できます。また、これらのテンプレートの除外を定義することもできます。
    - これらのプリンシパルのみが、これらのリソースに対してこれらのアクセス許可を持つ必要がある
    - これらのプリンシパルはこれらのリソースで、これらのアクセス許可を持つべきではない
    - これらのプリンシパルはこれらのリソースに対してこれらのロールを持つべきではない

> Rego (早期アクセス)

標準の Rego v2 構文でカスタムポリシーを記述します。

1. ポリシーが評価するリソースタイプを選択します。
2. 新しいポリシーを作成するか、**既存のポリシーから変更をインポート** をクリックして組み込みポリシーを検索して選択します。
3. コードをテスト実行するには、[テスト データ] セクションで [**単一** または **バッチ** をクリックして 1 つ以上の既存のリソースを選択し、[出力] セクションで [**実行** をクリックします。

6. わかりやすい名前を入力し、オプションで説明を入力します。
7. ポリシーに深刻度を割り当てます。深刻度は、ポリシーによってトリガーされた検出結果の深刻度レベルを決定します。
8. (オプション)セキュリティチームに明確なガイダンスを提供するため、カスタム修正手順を入力します。
9. 完了したら、**[作成]** をクリックします。

カスタム Rego ポリシー (早期アクセス)

カスタム Rego ポリシーは、Open Policy Agent (OPA) ポリシー言語である Rego を使用して、単一のリソースに対して属性レベルのチェックを記述します。これらは、事前定義されたパラメーターを通じて一般的なチェックをカバーするカスタムポリシーテンプレートと、リソースを視覚化する簡単な方法を提供する探索 エクスプローラーの間に配置されています。

次のいずれかに当てはまる場合は、Rego を使用します。

- あなたはすでに Rego の専門知識を持っており、テンプレートやグラフクエリよりも Rego を好みます。
- テンプレートやグラフクエリがサポートする範囲を超える条件が必要です。
- Rego で記述された既存のポリシーがあり、それを Tenable One Cloud Exposure で再利用したいと考えています。

クロスリソースロジックが必要な場合は、代わりに Explorer クエリを使用します。

組み込みポリシーかカスタムポリシーかにかかわらず、Rego で記述された既存のポリシーから開始することで、カスタムポリシーの開発をスピードアップします。このアプローチを使用して、組み込みポリシーをニーズに合わせて調整することもできます。組み込みポリシーをコピーし、コピー内のロジックを調整し、元のポリシーを無効にします。

Rego ベースのポリシーは作成されると、他のカスタムポリシーと同じように動作します。調査結果は、同じ形式、ダッシュボード、レポート、自動化、チケッティング、除外、コンプライアンスのフレームワークに従い、同じロールベースのアクセス制御を使用します。詳細については クラウドの検出結果 。

ポリシー評価

Rego ベースの各カスタムポリシーは、一度に 1 つのリソースを評価します。ポリシーは、未加工のプロバイダー JSON 形式でリソースを入力として受け取ります。ポリシーは、評価中に他のリソースを取得、トラバース、または参照することはできません。すべての評価は、1 つの状態で終了します。

状態	意味
スキップ	リソースはポリシーのタイプと一致しますが、エントリ条件外です。

状態	意味
合格	リソースがポリシー評価に合格した。
失敗	リソースはポリシー評価に失敗し、検出結果が生成されます。
エラー	ランタイムエラー (例: 無効なリソース JSON、ロジックが合格と不合格の両方を返す) のために評価が完了しませんでした。この状態はエンジンによって割り当てられます。

ヘルパー関数

ヘルパー関数は、自分で記述する代わりにカスタム Rego ポリシーから呼び出す、事前に構築された小さなロジックです。値がnullであるか、空であるか、または大文字と小文字でしか異なるかを確認するには、通常、数行のRegoが必要です。ヘルパー関数がそのチェックを 1 つの呼び出しにラップします。

クラウド サイバーエクスポージャー は、ネットワーク、ファイル、ホストへのアクセスなしの副作用のない動作に関するすべての許可リストに登録されたヘルパー関数を作成および監査します。許可リストは OPA が更新されるたびに再検証されるため、新しいヘルパー関数はそのレビュー後にのみ使用可能になります。

ヘルパー関数を使用するには、Rego エディターの上にある **[ヘルパー関数]** をクリックし、関数をポリシーにコピーします。

次の表に、許可リストに登録された各ヘルパー関数とその動作を示します。

ヘルパー関数	動作
`equals_ignore_case(value_1, value_2)`	大文字と小文字を無視して、`value_1` と`value_2` が等しいかどうかを判断します。大文字と小文字に関係なく一致する場合は`true` を返します。それ以外の場合は`false`です。
`get_days_ns (days)`	指定された日数をナノ秒の期間で返します。
`is_false`	表される値が`false`かどうかを判断します。文字列形式が "false" (大文字と

ヘルパー関数	動作
(value)	小文字を区別しない) に等しい場合にtrueを返します。それ以外の場合はfalseです。
is_true(value)	表される値がtrueかどうかを判断します。文字列形式が"true" (大文字と小文字を区別しない) に等しい場合にtrueを返します。それ以外の場合はfalseです。
is_null_or_empty(value)	値が欠落しているか空であるかを判別します。null、空の文字列、空の配列、または空のオブジェクトの場合、trueを返します。それ以外の場合はfalseです。

カスタムポリシーテンプレート

クラウドサイバーエクスポージャーは、カスタムポリシーの作成に使用できる多数のテンプレートを提供しています。これらのテンプレートを使用すると、モニタリングするリソースとその方法を柔軟に定義できます。たとえば、「*これらのアイデンティティのアクティビティをすべてモニタリングする*」というテンプレートを使用して、緊急アクセス用アカウントでのアクティビティをモニタリングするカスタムポリシーを作成し、そのアカウントが認証されていないアイデンティティに使用されないようにすることができます。または、バケット/キー/シークレットの変更をモニタリングするテンプレートを使用して、環境内の重要な「価値のある」資産をモニタリングすることもできます。

> **注意:** どのテンプレートでもサポートされていないカスタムポリシーの構成を検討している場合は、クラウドサイバーエクスポージャーの担当者にお問い合わせください。

以下のカテゴリ別のテンプレートは、特定のユースケースに対処するカスタムポリシーの作成に使用できます。

カテゴリ	クラウド	テンプレート	潜在的なユースケース
アクセ	AWS	これらのプリンシパルのみがこ	最重要データの保護特定の

カテゴリ	クラウド	テンプレート	潜在的なユースケース
ス許可のモニタリング		れらのアクセス許可を持つ必要がある	アイデンティティが機密度の高いリソースにアクセスできないようにします。
	AWS	これらのプリンシパルのみがこれらのリソースで、これらのアクセス許可を持つ必要がある	職務の分離。特定のアイデンティティのみがこのリソースにアクセスできる必要がある。
	Azure/GCP	これらのプリンシパルのみがこれらのリソースで、これらのアクセス許可を持つ必要がある	職務の分離。特定のアイデンティティのみがこのリソースにアクセスできる必要がある。
	AWS/Azure/GCP	これらのプリンシパルはこれらのリソースで、これらのアクセス許可を持つべきではない	最重要データの保護特定のアイデンティティが機密度の高いリソースにアクセスできないようにします。
	Azure/GCP	これらのプリンシパルはこれらのリソースで、これらのロールを持つべきではない	なりすまし。機密度の高いロールへのアクセスの変更をモニタリングします。
	AWS	これらのロールには、この参照ロールに一致するポリシーがある必要があります **注意**: 組織のロールを使用し、ロールのアカウントごとのインスタンスを事前定義されたテンプレートに準拠させたい場合は、このテンプレートを使用することで、アタッチされたポ	

カテゴリ	クラウド	テンプレート	潜在的なユースケース
		リシーのセットが選択した参照ロールから逸脱したときにアラートを受け取れます。	
	AWS	これらのバケットのポリシー、ACL、ブロックパブリックアクセスの設定変更をモニタリングする	最重要データの保護機密度の高いバケット設定の変更に関するアラートを受け取ります。
	AWS	これらのキーのアクセス許可変更をモニタリングする	最重要データの保護キーのポリシーの変更に関するアラートを受け取ります。
	AWS	これらのシークレットのポリシー変更をモニタリングする	最重要データの保護特定のシークレットポリシーの変更に関するアラートを受け取ります。
	AWS	これらのプリンシパルにアタッチされたアイデンティティ関連ポリシーの変更をモニタリングする	権限昇格を防ぐための、影響の大きいプリンシパルに対するIMonitorポリシーの変更。
	AWS	これらのロールにおける信頼ポリシーの変更をモニタリングする	なりすまし。機密度の高いロールへのアクセスの変更をモニタリングします。
	Azure	これらのマネージドIDは、これらのリソースに対してこれらのアクセス許可を持つべきではない	最重要データの保護特定のアイデンティティが機密度の高いリソースにアクセスできないようにします。

カテゴリ	クラウド	テンプレート	潜在的なユースケース
アクティビティをモニタリング	AWS/Azure/GCP	これらのアイデンティティのアクティビティをすべてモニタリングする **重要な注意事項**: • **GCP**: GCP アクティビティログデータへのアクセス権を必要とするこのポリシーを使用するには、クラウドサイバーエクスポージャーへの GCP の概要の一環として、監査ログ転送ステップを設定する必要があります。 • **Azure**: アクティビティモニタリングは、Azure の管理書き込みログのみに依存します。	緊急アクセス用アカウントをモニタリングします。緊急アクセス用アカウントの使用についてアイデンティティのアクティビティをモニタリングします。
機密データの監視	AWS/Azure/GCP	この機密データはこれらのリソースにあるべきではありません	本来保存されるべきでない制限**された境界内に**保存されている機密データを検出します。データスプロールをモニタリングし、データ境界のコンプライアンスを遵守するために使用します。データ境界と監視データのスプロール。

カテゴリ	クラウド	テンプレート	潜在的なユースケース
	AWS/Azure/GCP	この機密データはこれらのリソースにのみ存在すべきです	データの保存が許可されている**境界の外部に保存され**ている機密データを検出します。データスプロールをモニタリングし、機密データが承認されたストレージまたは環境内に確実に残るようにするために使用します。データ境界と監視データのスプロール。
リソースをモニタリング	AWS	これらのセキュリティグループのルール変更をモニタリングする	ネットワークセキュリティ。機密度の高いセキュリティグループへの変更をモニタリングします。
	AWS	これらのバケットのポリシー、ACL、ブロックパブリックアクセスの設定変更をモニタリングする	最重要データの保護機密度の高いバケット設定の変更に関するアラートを受け取ります。
	AWS	これらのキーのアクセス許可変更をモニタリングする	最重要データの保護キーのポリシーの変更に関するアラートを受け取ります。
	AWS	これらのシークレットのポリシー変更をモニタリングする	最重要データの保護特定のシークレットポリシーの変更に関するアラートを受け取ります。
	AWS	作成されたこれらのタイプのIAMプリンシパルをモニタリン	アクセスのモニタリング新しく作成されたアイデンティティをモニ

カテゴリ	クラウド	テンプレート	潜在的なユースケース
		グする	タリングします。
	AWS	これらのロールにおける信頼ポリシーの変更をモニタリングする	なりすまし。機密度の高いロールへのアクセスの変更をモニタリングします。
	AWS/Azure/GCP	これらのリソースはコードとして管理される必要がある	コードを介して管理されるリソースを特定します。
	すべて	これらのリソースには次のタグを付ける必要があります	ベストプラクティスを実施する。組織のタグ付けポリシーを強制します。
	AWS	これらのアクセス許可セット がユーザーまたはグループに割り当てられるタイミングをモニタリングする	アクセスのモニタリングAWS Identity Center のアクセス許可セットの変更をモニタリングします。
	AWS	これらのアクセス許可セットが作成または更新されるタイミングをモニタリングする	アクセスのモニタリングAWS Identity Center のアクセス許可セットの変更をモニタリングします。
	すべて	これらのリソースは、これらのキーを使用して暗号化される必要があります	保存データのセキュリティコントロールを実施します。
ネットワークをモニタリング	AWS	これらのVPCには 、インターネットゲートウェイを接続すべきではありません	ネットワークセキュリティ。内部ネットワークの露出を制限

カテゴリ	クラウド	テンプレート	潜在的なユースケース
	AWS	これらのサブネットはインバウンドインターネット接続を許可すべきではない	ネットワークセキュリティ。内部ネットワークの露出を制限
	AWS	これらのセキュリティグループのルール変更をモニタリングする	ネットワークセキュリティ。機密度の高いセキュリティグループへの変更をモニタリングします。
	AWS/Azure/GCP	リソースは、これらのIPv4アドレス範囲からこれらのポートへのインバウンドインターネット接続を許可すべきではない **注意**: このポリシーは以下のリソースに適用されます: • **GCP**: インスタンスグループおよびVMインスタンス • **Azure**: 仮想マシン、仮想マシンスケールセット、ロードバランサー、アプリケーションゲートウェイ • **AWS**: EC2インスタンス、EC2サービス、ロードバランサー、RDSインスタンス、Redshiftクラスタ	ネットワークセキュリティ。外部ネットワークからのアクセスを制限します。

カテゴリ	クラウド	テンプレート	潜在的なユースケース
	AWS	これらのセキュリティグループは、これらの IP アドレス範囲からこれらのポートへのインバウンドのインターネットアクセスを許可すべきではありません。	ネットワークセキュリティ。内部または外部ネットワークからのアクセスを制限します。
	AWS	これらのセキュリティグループは、これらの IP アドレス範囲からこれらのポートへのインバウンドのインターネットアクセスを許可する必要があります。	ネットワークセキュリティ。内部または外部ネットワークからのアクセスを制限します。

IaC ポリシー

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

これは、ポリシーを管理し、Tenable One Cloud Exposure で検出結果を作成する方法を設定するためのハウツーガイドです。

- IaC 検出結果の表示とモニタリングに関するハウツーガイドについては、IaC 検出結果を参照してください。
- 検出結果の深刻度の仕組みの概念概要については、「検出結果の深刻度」を参照してください。

設定ファイルの問題を検出して修正するようにクラウドサイバーエクスポージャー IaC セキュリティを設定すると、IaC ポリシーの表示や管理を行いながら環境をモニタリングできます。

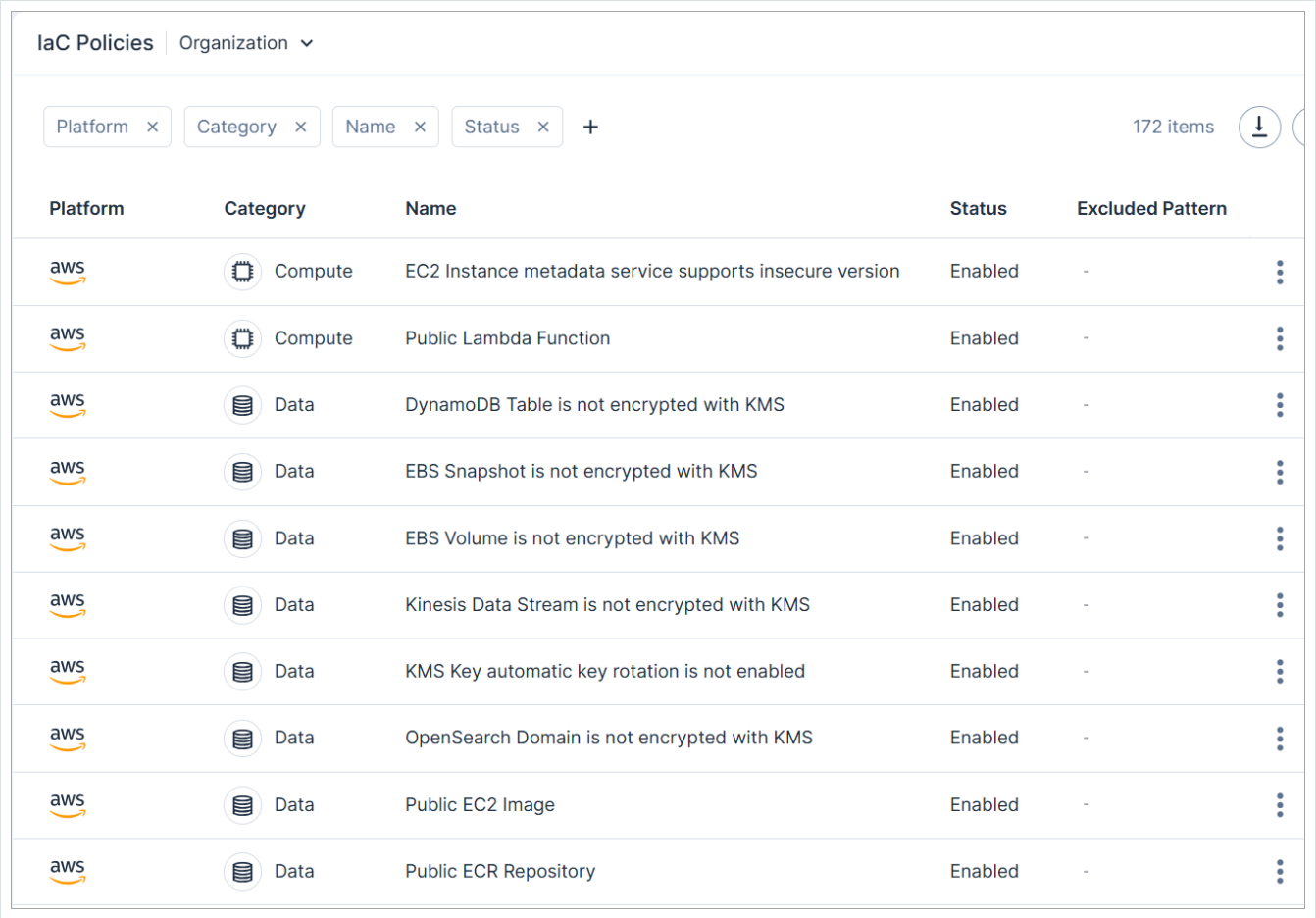
IaC/コードポリシー IaC ポリシーは、**[Exclusions]** (除外) ページと **[Policies] (ポリシー)** ページから無効化/除外できます。以下のように、設定した除外は常にすべての包含を上書きすることに注意してください。

- **[除外]** ページのパラメーターでポリシーを除外したが、**[ポリシー]** ページでポリシーが有効になっている場合、ポリシーはスキャンから **除外** されます。
- **[ポリシー]** ページでポリシーを無効にした (または クラウドポリシーした) が、**[除外]** ページ経由でポリシーが (明示的または暗黙的に) 含まれている場合、そのポリシーはスキャンから **除外** されます。

ポリシーの管理

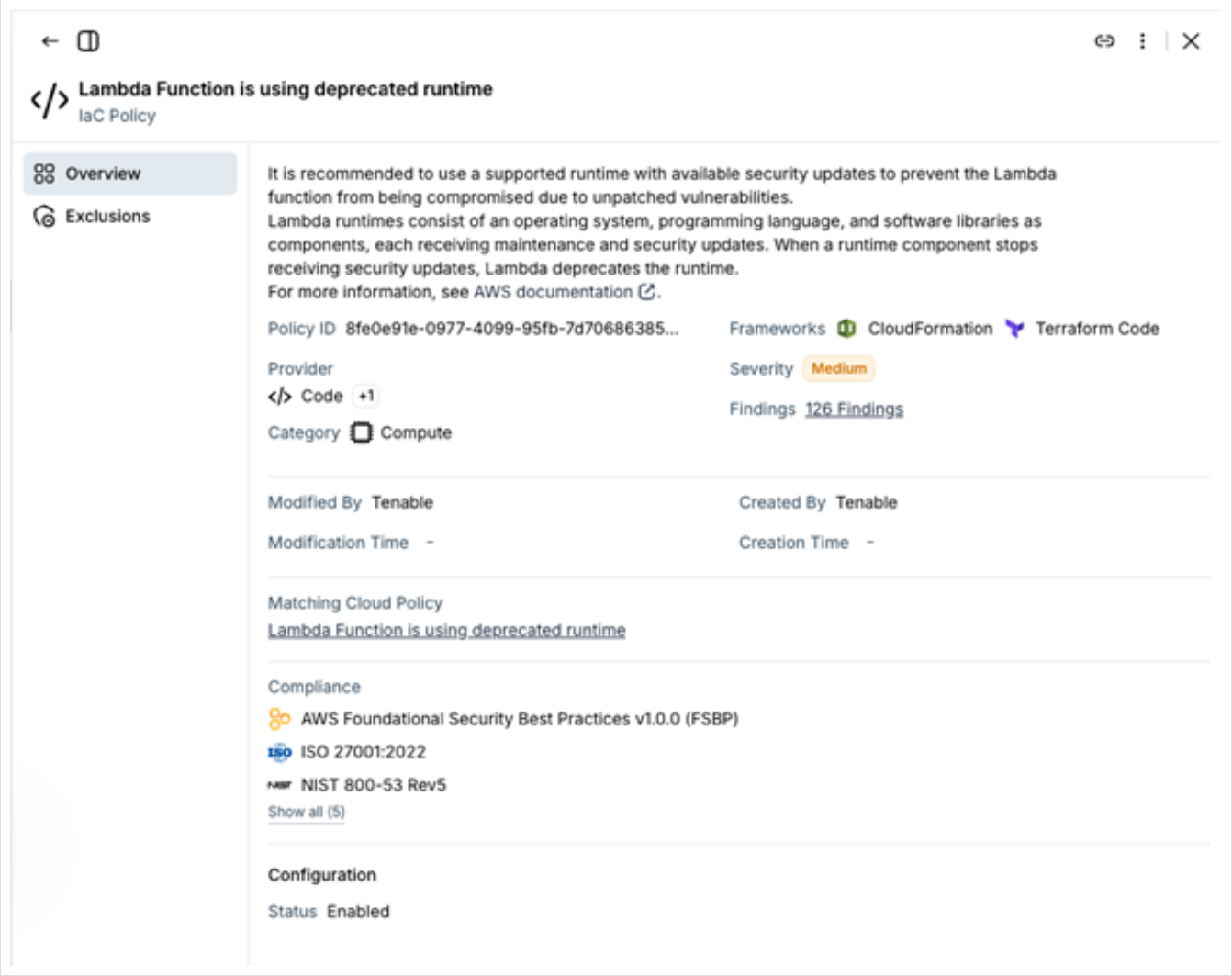
ポリシーを表示および管理する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Policies]** > **[IaC Policies]** の順にクリックします。



2. 組織/リポジトリの特定のサブセットに対するポリシーを表示および管理するには、[Organization] (組織) ドロップダウンでコードテナントを選択します。デフォルトでは、組織全体 (すべての組織/リポジトリ) が選択されています。

3. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。テーブル右上の列ピッカーを使用して、どの列を表示するか選びます。詳細については、IaC ポリシーの列データを参照してください。
4. ポリシーをクリックすると、詳細情報を含むスライド式パネルが開きます。ポリシーを確認し、管理します。詳細については、IaC ポリシーの列データを参照してください。



5. ポリシーの設定を**編集**します。次のポリシー管理アクティビティを実行できます。
    - IaC ポリシーの有効化と無効化
    - IaC スキャンで除外を設定する
    - IaC ポリシーデータのエクスポート

IaC ポリシーの列データ

次の列がページ上のテーブルに表示されます。そのほとんどが、テーブルのデータのフィルターにも使用できます。

フィルター	説明
プラットフォーム	たとえば、クラウドサービスプロバイダーやIdPなどです。可能な値: AWS、Azure、Microsoft Entra ID、コード (IaC固有のポリシー)、GCP、またはOCI。
深刻度	ポリシーの深刻度レベル。
カテゴリ	ポリシーが属する論理カテゴリ。「ポリシーカテゴリを参照してください。
名前	ポリシーの名前
コンプライアンス	ポリシーのベンチマークにマッピングされるコンプライアンス標準とセキュリティのベストプラクティス。
ステータス	ポリシーが有効か無効か。ポリシーが対象アカウントのリソースに対して検出結果をトリガーしないように、IaCポリシーの有効化と無効化できます。
検出結果	ポリシーについてオープンなIaC検出結果の数が表示されます。
ポリシーSettings ⋮	• IaCポリシーの有効化と無効化
フレームワーク	各IaCポリシーによってサポートされているIaCフレームワークを確認します。

IaCポリシーの有効化と無効化

デフォルトでは、標準装備のポリシーは有効になっており(*モニタリング*ポリシーを除く)、組織内のすべてのアカウントに適用されます。微調整したい場合は、組織全体でポリシーを無効にするか、アカウントやフォルダーの特定のサブセットのみポリシーを無効にすることができます。

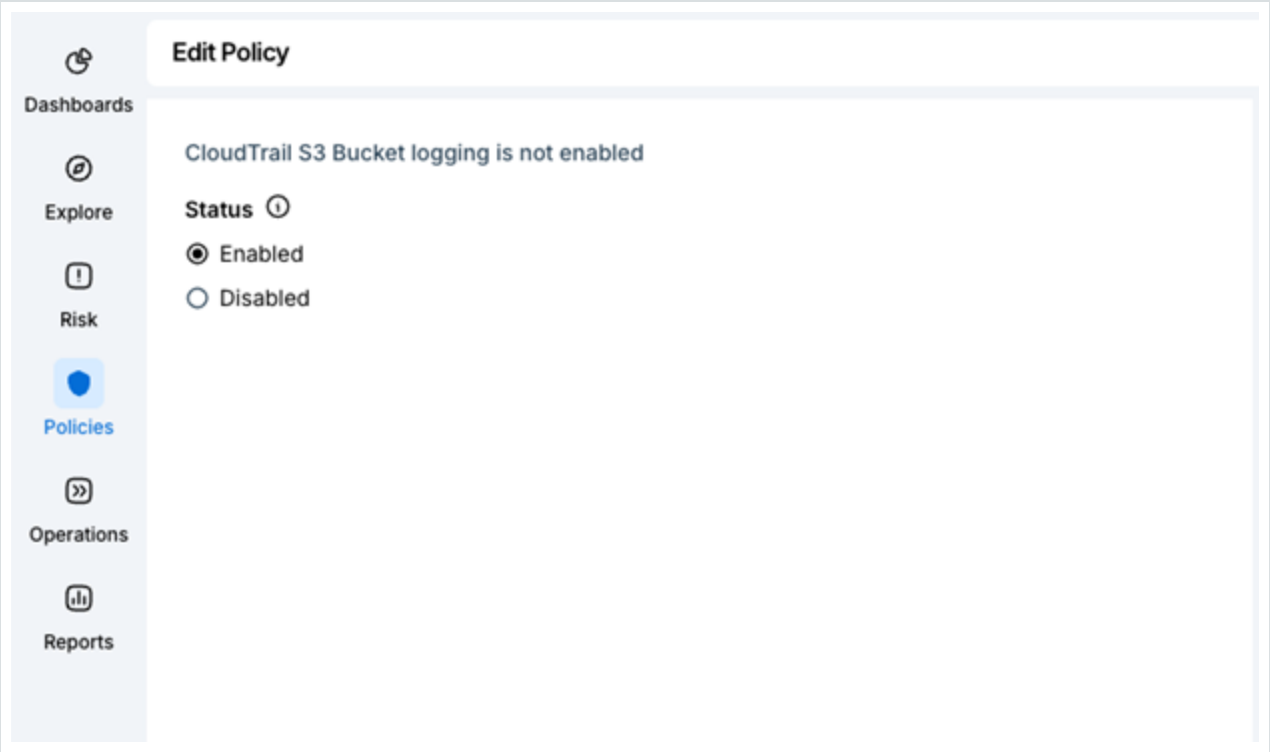
警告: ポリシーを無効にすると、そのポリシーに関連する検出結果が対象アカウントからすべて削除され、新しい検出結果が作成されなくなります。このアクションは次回 データの同期と更新の頻度 後に実行され、元に戻すことはできません。

注意:

- ポリシーの有効化と無効化は、「管理者」ロールを持つユーザーだけが使用できます。
- たとえば、深刻度の低い問題に関連する一部のポリシーは、デフォルトで無効化されていますが、コンプライアンス準拠のためやその他のセキュリティ目的で有効化が必要な場合は有効にできます。
- 無効にできないポリシーの小サブセットが存在します。これらのポリシーは、過剰な権限を持つ ID や非アクティブな ID に関連し、コアシステム機能を提供します。

ポリシーを有効または無効にする

1. クラウドサイバーエクスポージャーコンソールで、**[リスク>スキャン]> [コードスキャン]** の順にクリックします。
2. [Organization] (組織) ドロップダウンでコードテナントを選択し、クラウドアカウントの特定のサブセットのポリシーを有効化または無効化します。デフォルトでは、組織全体 (すべての組織/リポジトリ) が選択されています。
3. 関連する IaC ポリシーに移動します。
4. ⋮アイコンをクリックしてから、**[編集]** をクリックします。
5. [ステータス] セクションで、関連するオプションを選択します。
    - **継承。** 親レベルのアカウント範囲の設定を継承 (デフォルト)。継承された設定は、親レベル範囲の名前の横の括弧内に表示されます。組織全体を範囲として選択した場合、このオプションは表示されません。
    - **有効** (親レベルの設定をオーバーライド)。ポリシールールに違反すると、検出結果が作成されます。
    - **無効化** (親レベルの設定をオーバーライド)。ポリシールールに違反しても、検出結果は作成されません。



6. **[保存]** をクリックします。

IaC スキャンで除外を設定する

コードベースのスキャンから特定の **パス**、**リソースタイプ**、**またはリソース名** のパターンを除外して、これらのリソースに関連する潜在的な検出結果を防ぐことができます。除外オプションごとに、除外するパターンを入力します。パターンが関連するオプションと一致する場合、クラウドサイバーエクスポージャーはそのパターンをスキャンから除外します。構成オプションは AND 条件を使用して組み合わされ、すべてオプションです。また、リソースを除外する理由を説明するコメントを追加できます。詳細は、「除外を参照してください。

> **必要なクラウドサイバーエクスポージャーユーザーロール:** ポリシーからのリソース除外は、「コラボレータ」または「管理者」ロールのいずれかを持つユーザーが利用できます。

IaC スキャンの除外を作成する方法

1. **[ポリシー]** > **[除外]** に移動します。
2. **[Organization] (組織)** ドロップダウンで、アカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. **[除外の追加]** をクリックします。

   > **注意:** 除外の作成を開始した後は、アカウント範囲を変更できません。

4. **名前**と**説明**を入力します。
   - 明確でビジネスに焦点を当てた名前を使用します (例: QA の公知の EC2 インスタンス)。
   - 除外の理由または正当性を説明してください。
5. 除外 で、検出結果が除外と一致した場合の動作を選択します。
   - **無視** – 一致する検出結果を **[オープンの検出結果]** リストから除外します。
     - 検出結果を無視する理由を入力します。検出結果が無視されると、サブステータスは **[例外]**、**[設計上]**、**[誤検出]** のいずれかになります。
   - 深刻**度を変更** – 一致する検出結果の深刻度を下げたり上げたりします。
6. **ターゲットとなる検出結果**の範囲を定義します。
   1. **[タイプ]** で **[IaC]** を選択します。
   2. **[ポリシー]** で、**[すべてのポリシー]** または [ターゲットとする **特定のポリシー]** を選択します。

      ヒント: 定義されたビジネスケースに一致する特定のポリシーを選択します。
   3. 必要に応じて深刻 **度** フィルターを追加して、特定の深刻度の検出結果のみを含めることもできます。
7. **ターゲットリソース**を定義します。

   [コード] フィールドに、次のワイルドカード文字を使用してパターンを入力します。
   - * (アスタリスク) - 0 文字以上と一致
   - ? (クエスチョンマーク) - 1 文字と一致

   たとえば、パターン `aol-*` の名前です。
8. **[有効期限]** で、**[なし]** または [有効期限] を選択します。

有効期限を過ぎると、除外は検出結果に適用されなくなります。他の除外がこれらの検出結果に影響を与えない場合、検出結果は再オープンされるか、深刻度が元に戻されます。

9. 対象となるオープンの検出結果をすべて一覧表示する **[検出結果] プレビュー** パネルで設定を確認します。保存する前に、フィルター、保持、範囲が意図した結果を正確にターゲットにしていることを確認してください。
10. **[保存]** をクリックします。

除外は次のスキャンサイクルに有効になり、一致するすべての検出結果が更新されます。

IaC ポリシーデータのエクスポート

CSV ファイルにポリシーデータをエクスポートします。データは、テーブルにその時点で適用されているフィルターに従ってエクスポートされます。データには、ポリシーによってトリガーされる特定の検出結果でフィルタリングされた [Findings] (検出結果) ページの URL など、関連するすべてのポリシーデータが含まれます。

IaC ポリシーデータをエクスポートする方法

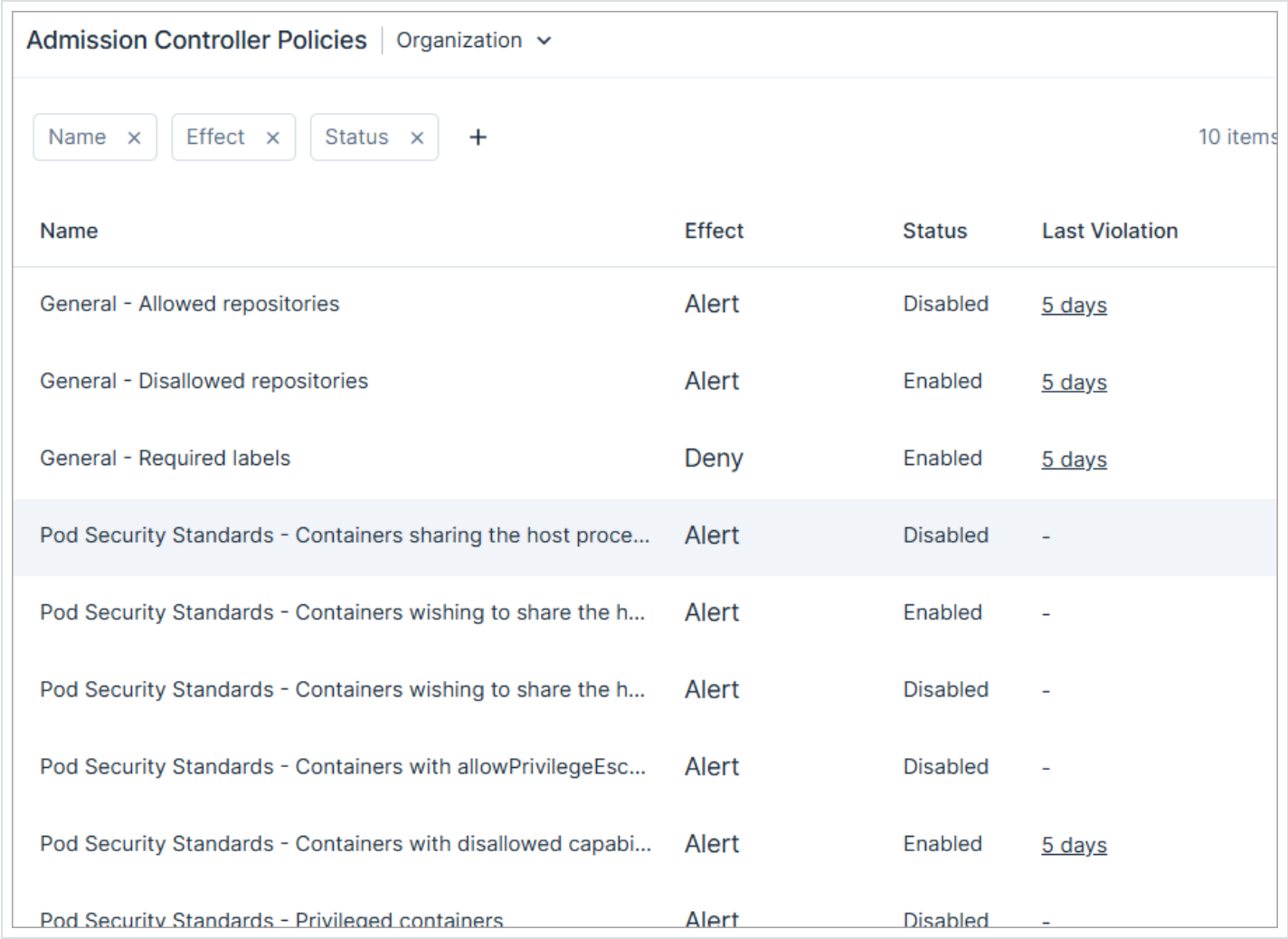
1. (オプション)[Organization] (組織) ドロップダウンでコードテナントを選択し、クラウドアカウントの特定のサブセットに関連するポリシーを表示します。デフォルトでは、組織全体 (すべての組織/リポジトリ) が選択されています。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。
3. テーブルの右上隅にある **[Export** ⬇ **]** ボタンをクリックします。

アドミッションコントローラーポリシー

この記事は、Tenable One Cloud Exposure でのアドミッションコントローラーポリシーの構成に関するハウツーガイドです。

- イベントの探索に関するハウツーガイドについては、「Kubernetes アドミッションコントローラーイベント」を参照してください。
- クラウドサイバーエクスポージャー のアドミッションコントローラー機能の概念概要については、「アドミッションコントローラーの概要を参照してください。

アドミッションコントローラーポリシーの完全なリストについては、[Admission Controller Policies] (アドミッションコントローラーポリシー) ページを参照してください。このページでは、ポリシーの詳細の確認やアドミッションコントローラーポリシーの設定を行うことができます。

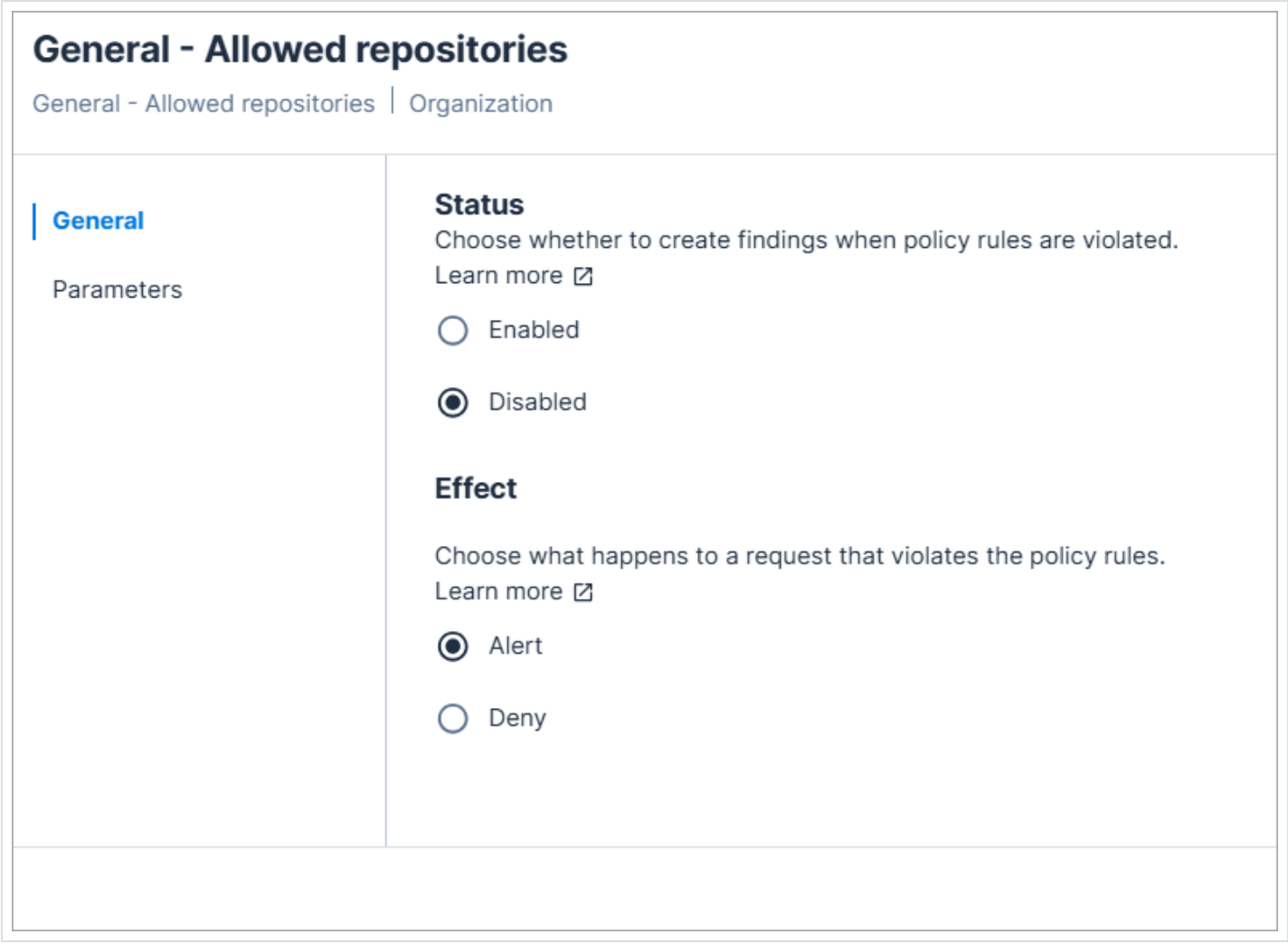


ポリシーを管理するには

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー]** > **[アドミッションコントローラーポリシー]** に移動します。
2. [組織] ドロップダウンでアカウント階層とフォルダーを選択して、アカウントの特定のサブセットのポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. ポリシーをクリックすると、詳細情報を含むスライド式パネルが開きます。

4. 設定するポリシーを見つけて、三点リーダーメニュー ⋮ をクリックします。次のポリシー管理アクティビティを実行できます。
    - アドミッションコントローラーポリシーの設定 (以下が含まれます):
        - ポリシーを有効または無効にします。
        - 違反の影響の設定
        - ポリシーパラメーターの編集
    - イベント。これにより、Kubernetes アドミッションコントローラーイベントページが開き、そのポリシーの違反ログのみが表示されるようフィルタリングされます。

アドミッションコントローラーポリシーの設定



デフォルトでは、新しいアドミッションコントローラーポリシーは無効になっています。ポリシーを有効にすると、アカウント階層とフォルダー内に存在する、アドミッションコントローラーのインストールクラスタにのみそのポリシーが適用されます。

また、違反が発生した場合の各ポリシーの違反の影響も設定することができます。

アドミッションコントローラーポリシーを有効にして設定する方法

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー]** > **[アドミッションコントローラーポリシー]** をクリックします。
2. 設定するポリシーを見つけて、三点リーダーメニュー ⋮ **[編集]** をクリックします。
3. **[全般]** タブで、**[ステータス]** を **[有効]** に設定します。
4. [Violation Effect] (違反の影響) で、ポリシー違反があった場合の動作を選択します。

    1. アクション**を拒否します**。

    2. アクションを許可するが、 **アラート**を受け取る。違反アラートは、[[Admission Controller Events] (アドミッションコントローラーイベント) ページ](/v1/docs/ja/kubernetes-admission-controller-events)に表示されます。

5. **[パラメーター]** タブで、ポリシーパラメーターを設定します。各ポリシーで、設定できるパラメーターは異なります。各ポリシーの詳細については、アドミッションコントローラーポリシーリスト を参照してください。
6. **[保存]** をクリックします。
   有効なポリシーは、アドミッションコントローラーのインストールクラスタにのみ適用されます。

アドミッションコントローラーポリシーリスト

このセクションでは、Tenable がサポートするアドミッションコントローラーポリシーの概要と、それぞれで利用可能な設定可能なパラメーターについて説明します。アドミッションコントローラーポリシーを使用すると、Kubernetes リソースに対して固有のコントロールを調整し、デプロイメントをセキュリティとコンプライアンス要件に合わせることができます。

ポリシー名	検証タイプ	説明	パラメーター
脆弱なコンテナイメージ	全般	既知の脆弱性のあるコンテナイメージを使用するKubernetesワークロードについてアラートまたはブロックします。このポリシーは、アドミッション時にTenable Cloud Workload Protectionのスキャン結果に照らしてイメージを評価します。完全な設定の詳細については、「脆弱なコンテナイメージを参照してください。	「脆弱なコンテナイメージ Settings」を参照してください。
許可されたリポジトリ	一般	コンテナイメージは、許可されたリポジトリのパターンと一致する必要があります。	**許可されたリポジトリ**: 使用できるリポジトリのパターン。このリストのパターンに一致しないリポジトリが使用されている場合、ポリシー違反になります。
Podのサービスアカウントトークンの自動マウント	全般	`automountServiceAccountToken` を `false` に設定しても、ポッドがサービスアカウントトークンを自動的にマウントしないようにします。	設定可能なパラメーターなし
ブロックエンドポイント編集デフォルトロール	全般	デフォルトのロールがエンドポイントリソースへの編集または書き込みアクセス権を付与しないようにする必要があります。	設定可能なパラメーターなし

ポリシー名	検証タイプ	説明	パラメーター
NodePort のブロック	全般	クラスタ内のすべてのノードの静的ポートでワークロードを公開する NodePort タイプをサービスで使用しないようにする必要があります。	設定可能なパラメーターなし
サービスアカウントの更新をブロックする	全般	ポッドの作成後にポッドのサービスアカウントを変更できない必要があります。	設定可能なパラメーターなし
ワイルドカードイングレスのブロック	全般	ワイルドカード (*) サブドメインを使用しない、ホストを空白のままにする、または完全に省略するには、イングレスホスト定義が必要です。これらの設定により、サービスが意図しないトラフィックや不正なトラフィックに応答する可能性があります。	設定可能なパラメーターなし
コンテナイメージにはダイジェストが必要です	全般	コンテナイメージには、ダイジェストが必要です。	設定可能なパラメーターなし
匿名アクセスを許可しない	全般	ロール/クラスターロールをユーザーまたは `system:unauthenticated` グループ `system:anonymous` 関連付けないようにする必要があります。	設定可能なパラメーターなし
対話的な TTY コンテナを許可しない	全般	tty と stdin の両方を true に設定して、コンテナで対話的な TTY セッ	設定可能なパラメーターなし

ポリシー名	検証タイプ	説明	パラメーター
		ションが有効にならないようにする必要があります。コンテナへのインタラクティブなシェルアクセスを防ぐために、これらのフィールドは false に設定するか、設定せずににしておく必要があります。	
許可されていないリポジトリ	一般	コンテナイメージは、許可されていないリポジトリのパターンと一致しない必要があります。	**許可されていないリポジトリ**: 使用できないリポジトリ。このリストのパターンに一致するリポジトリが使用されている場合、ポリシー違反になります。
外部 IP	全般	サービスに許可された外部 IP リストの外部 IP のみを含める必要があります。	許可された IP アドレスのコンマ区切りリスト
HTTPS のみ	全般	イングレスリソースは HTTPS 経由のみでサービスを公開する必要があります。これにより、トラフィックの暗号化が保証され、暗号化されていない HTTP 経由の偶発的なエクスポージャーを防止できます。	TLS が必要
必須ラベル	一般	**リソースタイプ**リストのリソースには、指定されたラベルと、**必要なラベル**リストのキーと値が含まれている必	• **リソースタイプ**: 強制されるリソースタイプ。

ポリシー名	検証タイプ	説明	パラメーター
		要があります。	• **必須ラベル**: 特定のリソースタイプで使用する必要があるラベル。選択したリソースタイプに必須ラベルがない場合、ポリシー違反となります。
必須の要求と制限の範囲	全般	コンテナにはリソースリクエストと制限が定義されている必要があります。制限やリクエストに対して指定する必要があるリソースタイプ (**CPU**、**メモリ**) を設定可能。オプションで、リソース制限とリクエストの最大値を適用します。	必要な制限: • **CPU**: CPU の最大制限 • **メモリ**: メモリの最大制限 必要なリクエスト: • **CPU**: CPU の最大制限 • **メモリ**: メモリの最大制限
許可されたユーザー	ポッドセキュリティ標準	コンテナは、対応するパラメーターリストから該当する **runAsUser**、**runAsGroup**、**supplementalGroups**、または **fsGroup** を指定する必要があります。詳細は、ドキュメント	• 許可されたユーザー • 許可されたグループ • 許可された F5 グ

ポリシー名	検証タイプ	説明	パラメーター
		Kubernetesを参照してください。	ループ • 許可された補助グループ
AppArmor	ポッドセキュリティ標準	使用が許可されているAppArmorプロファイルコンテナを制御します。AppArmorプロファイルがないと、コンテナはホスト上のファイル、ネットワークソケット、Linux機能に無制限にアクセスでき、侵害されたコンテナが機密ファイルを読み取ったり、不正なネットワーク接続を確立したり、意図した範囲を超えて権限を昇格したりする可能性があります。	• **許可されるプロファイル**: 許可されるプロファイルタイプ: RuntimeDefault、Localhost、Unconfined。 • **許可されるローカルホストプロファイル**: ローカルホストが選択されたプロファイルである場合にのみ使用できます。任意のローカルホストプロファイルに対して * を使用します。
ホスト **プロセス ID** 名前空間を共有するコンテナー	ポッドセキュリティ標準	コンテナの [`hostPID`] フィールドは、**true** に設定してはなりません。詳細は、ドキュメントKubernetesを参照してください。	設定可能なパラメーターなし

ポリシー名	検証タイプ	説明	パラメーター
ホスト IPC 名前空間の共有を希望するコンテナ	ポッドセキュリティ標準	コンテナの [hostPID] フィールドは、**true** に設定してはなりません。詳細は、ドキュメント Kubernetesを参照してください。	設定可能なパラメーターなし
ホストネットワークの名前空間の共有を希望するコンテナ	ポッドセキュリティ標準	コンテナの [hostNetwork] フィールドは、**true** に設定してはなりません。詳細は、ドキュメント Kubernetesを参照してください。	設定可能なパラメーターなし
allowPrivilegeEscalation のあるコンテナ	ポッドセキュリティ標準	コンテナの [allowPrivilegeEscalation] フィールドを **false** に設定する必要があります。詳細は、ドキュメント Kubernetesを参照してください。	設定可能なパラメーターなし
許可されていない機能を持つコンテナ	ポッドセキュリティ標準	コンテナには許可された機能リストの機能のみを含め、削除する機能リストのすべての機能を削除する必要があります。詳細は、ドキュメント Kubernetesを参照してください。	• **許可されている機能**: コンテナが持つことができる機能。 • **削除する機能**: コンテナーから削除する必要がある機能。
許可されていないタグ	ポッドセキュリティ標準	コンテナイメージでは、許可されていないタグリストのタグを使用しないようにします。詳細は、ドキュメント Kubernetesを参照してください。	タグのコンマ区切りリスト。

ポリシー名	検証タイプ	説明	パラメーター
ホストファイルシステム	ポッドセキュリティ標準	明示的に許可されたホストファイルシステムパスのみをマウントするようにポッドを制限します。無制限の hostPath ボリュームにより、コンテナは kubelet 認証情報、コンテナランタイムソケット、クラウドプロバイダートークンなどの機密性の高いノードファイルに直接アクセスできるため、侵害されたコンテナは分離を逃れ、基盤となるノードを危険にさらす可能性があります。	**許可されたホストパス**: ポッドがマウントできるホストパスのプレフィックス。すべての hostPath ボリュームは、これらのプレフィックスの 1 つで始める必要があります。一致では、プレフィックスとパスセグメントが考慮され、最も具体的な一致プレフィックスが優先されます。ポリシーが空のリストで有効になっている場合、すべての hostPath ボリュームがブロックされます。各プレフィックスは読み取り専用に設定でき、パスをマウントするすべてのコンテナーが読み取り専用としてマウントを宣言する必要があります。
読み取り専用ルートファイルシステム	ポッドセキュリティ標準	readOnlyRootFilesystem を true に設定することにより、コンテナを読み取り専用のルートファイルシステムで実行する必要がありま	設定可能なパラメーターなし

ポリシー名	検証タイプ	説明	パラメーター
		す。	
特権コンテナ	ポッドセキュリティ標準	コンテナの [privileged] フィールドは、true に設定してはなりません。詳細は、ドキュメント Kubernetes を参照してください。	設定可能なパラメーターなし
ルートコンテナ	ポッドセキュリティ標準	[runAsNonRoot] フィールドを true として定義するか、runAsUser を 0 以外の任意の値として定義することで、コンテナを非ルートにしておく必要があります。詳細は、ドキュメント Kubernetesを参照してください。	設定可能なパラメーターなし
Seccomp	ポッドセキュリティ標準	使用が許可されている seccomp プロファイルコンテナを制御します。seccompプロファイルがないと、コンテナが無制限のLinuxカーネル syscallを実行し、侵害されたコンテナがカーネルの脆弱性を悪用したり、ファイルシステムのマウントや他のプロセスのトレースといった危険な操作を実行したりする可能性があります。	• **許可されたプロファイル**: 許可されるプロファイルタイプ: RuntimeDefault、Localhost、Not configured、Unconfined。空のリストはすべてのワークロードをブロックします。 • **許可されたローカルホストファイル**:

ポリシー名	検証タイプ	説明	パラメーター
			ローカルホストが選択されたプロファイルである場合にのみ使用できます。ファイル名の動的リスト。すべてのファイルを許可するには * を使用します。
ホストネットワーキングポート	ポッドセキュリティ標準	ホストネットワークの使用時にコンテナをバインドさせる可能性のあるホストポートを制限します。無制限のホストポートバインディングにより、コンテナはノード上の特権ポートまたは予約済みポートを直接リッスンし、ポッドネットワークの分離をバイパスできます。	最小ポート 最大ポート
FlexVolume	ポッドセキュリティ標準	Pod で使用できる FlexVolume ドライバーを制限します。FlexVolumeドライバーは、昇格した権限で実行されるノードに直接インストールされる実行可能ファイルです。承認されていないドライバーを許可すると、ポッドが任意のストレージバックエンドをマウントできるようになり、ノード上でデータが	**許可された flex ボリュームドライバー:** 各エントリは、`vendor/driver` 形式の 1 つのドライバー文字列である必要があります。ワイルドカードは使用できません。リストが空の場合、

ポリシー名	検証タイプ	説明	パラメーター
		流出したり、悪意のあるコードが実行されたりする可能性があります。	FlexVolumeのすべての使用がブロックされます。
禁止されているsysctls	ポッドセキュリティ標準	変更が許可されているLinuxカーネルパラメーター(sysctls)ポッドを制御します。sysctlアクセスを無制限にすると、ポッドはネットワークスタックの挙動やIPC制限など、ノード全体のカーネル設定を変更して、ノードを不安定にしたり、他のワークロードに影響を及ぼしたり、権限昇格を有効にしたりする可能性があります。	**許可されたsysctls**: ポッドが設定できるsysctls。
ボリュームタイプ	ポッドセキュリティ標準	Podにマウントが許可されているボリュームのタイプを制限します。たとえば、hostPathなどのボリュームタイプはコンテナにノードファイルシステムへの直接アクセスを許可し、侵害されたコンテナが機密性の高いホストファイルを読み込んだり、コンテナの分離をエスケープしたりできるようにします。	**ボリュームタイプ**: ポッドがvolumes.specで設定できるボリュームタイプ。

脆弱なコンテナイメージ

脆弱なコンテナイメージアドミッションコントローラーポリシーを使用すると、既知の脆弱性を持つコンテナイメージを使用するKubernetesワークロードをアラートしたりブロックしたりできます。Kubernetesアドミッショ

ンレイヤーで Tenable Cloud Workload Protection (CWP) のスキャンデータと統合することにより、脆弱なイメージがクラスターに到達する前に、ポリシーはデプロイ時に脆弱性ゲートを強制します。

> **注意:** このポリシーは、デフォルトでは無効になっています。

前提条件

このポリシーを有効にする前に、以下を確認してください。

- クラウドサイバーエクスポージャー アドミッションコントローラーがターゲットクラスタにデプロイされます。
- Tenable Kubernetes Helm チャートバージョン 1.1.6 以降がインストールされており、アドミッションコントローラーにクラスタのシークレットに対する読み取りアクセス許可があります。
- アドミッションコントローラーポッドは、シークレットアクセスを有効にしてデプロイされます (`--set admissionController.readSecrets=true`)。
- アドミッションコントローラーポッドには、コンテナレジストリへのネットワーク接続があります。
- `KubernetesClusterConnectorRead` アクセス許可があります。

また、コンテナ コンテナイメージ CI/CD パイプラインの接続 またはアウトポスト/センサーベースのスキャンを設定し、コンテナイメージをアクティブにスキャンすることも Tenable では推奨しています。ポリシーが機能するためにスキャンカバレッジを必要としませんが、スキャン結果のないイメージは未スキャンとして扱われます。ポリシーがそれらのイメージを処理する方法を制御するには、[Trust Unscanned Container Images] 設定 を参照してください。

脆弱なコンテナイメージの仕組み

ワークロードがクラスタに送信 (Create または Update) されると、アドミッションコントローラーはリクエストをインターセプトし、各コンテナイメージを評価します。このポリシーは、cronjobs、daemonsets、deployments、jobs、replicasets、statefulsets、deploymentconfigs、podsのワークロードタイプに適用されます。

コンテナイメージごとに、アドミッションコントローラーは次の操作を実行します。

1. レジストリからイメージダイジェストを解決します。
2. そのダイジェストの最新のスキャン結果を Tenable CWP から取得します。

3. スキャンが設定された最大経過時間内にあるかどうか、およびイメージに設定された深刻度しきい値以上の脆弱性が含まれているかどうかをチェックします。除外されたCVEパターンに一致する脆弱性は無視します。
4. 違反が検出された場合に、構成した効果を適用します。
    - **[Deny]**: デプロイはブロックされ、エラーメッセージを返します。
    - **アラート**: デプロイメントが続行され、アドミッション制御イベントが記録されます。

30秒後に評価がタイムアウトすると、ポリシーはオープンに失敗します。デプロイメントは許可され、調査のためにタイムアウトイベントが記録されます。

> **注意:** すでに本番環境で実行されているワークロードの場合、ポリシーは自動的に**[拒否]**から**[アラート]**にフォールバックします。

脆弱なコンテナイメージの有効化

ポリシーを有効にするには

1. クラウドサイバーエクスポージャーコンソールで、**[ポリシー]** > **[アドミッションコントローラーポリシー]**に移動します。
2. **[一般 - 脆弱なコンテナイメージ]**という名前のポリシーを見つけて、三点リーダーメニューをクリックして、**[編集]**をクリックします。
3. **[ステータス]**で、**[有効]**を選択します。
4. **[詳細設定]**を展開し、**[効果]**で次のいずれかを選択します。
    - **アラート**: アドミッションコントローラーはデプロイを許可し、警告イベントを記録します。
    - **Deny**: アドミッションコントローラーがデプロイメントをブロックします。
      Tenableでは、**Alert**から始めて、**拒否**に切り替える前に少しだけ実行することを推奨しています。
5. (オプション)**[Parameters] (パラメーター)**パネルで、**[Container Image Validation] (コンテナイメージの検証)**を展開して、「Vulnerable Container Images Settings」で説明されている設定を構成します。

6. (オプション)**[除外]** を展開して、コンテナイメージの URL または CVE パターンの除外を設定します。
7. **[保存]** をクリックします。

> **注意:** 選択した範囲内のすべてのクラスタに適用されてから、最大 5 分かかります。

脆弱性のあるコンテナイメージの設定

次の設定は、**[コンテナイメージの検証]** で利用できます。

設定	デフォルト	Description (説明)
脆弱性の最小深刻度	高	違反の深刻度しきい値。このレベル以上の脆弱性を含むイメージが、設定された効果をトリガーします。オプション: 重大、高、中、低。
脆弱性スキャンの最大経過時間 (日数)	7	有効なスキャン結果の最大有効期間 (日数) このしきい値より古いスキャンは、未スキャンのイメージとして扱われます。有効範囲: 3 ～ 14 日。
スキャンされていないコンテナイメージを信頼する	オフ (未選択)	ポリシーがスキャン結果のないイメージを処理する方法を制御します。オフを選択すると、スキャン結果のないイメージが違反として扱われます。選択すると、スキャン結果のない画像が通過します。

次の除外設定も利用できます。

設定	Description (説明)
除外されるコンテナイメージの URL パ	ポリシー評価から除外するイメージ URL の Glob または正規表現パターン。これらのパターンに一致するイメージは、脆弱性チェックをバイパスします。信頼できる内部イメージまたはインフラストラクチャコンポーネントには、この設定を使用します。

設定	Description (説明)
ターン	
除外された CVE パターン	ポリシー評価から除外する CVE 識別子の Glob または正規表現パターン。ポリシーがイメージを評価するときには、除外されたパターンに一致する脆弱性はカウントされません。設定された深刻度以上のすべての脆弱性が除外パターンに一致する場合、イメージはアドミッションをクラスターに渡します。この設定を使用して、評価して許可することを選択した特定の CVE を受け入れます。

注意: ポリシーが評価するイメージでは、除外された CVE はカウントされません。CVE は、環境内でのリスクを評価した後にのみ除外してください。

ポリシーの列データ

次の列は、[Admission Controller Policies] (アドミッションコントローラーポリシー) ページのテーブルに表示されます。ほとんどの列をテーブルのデータのフィルターにも使用できます。

フィルター	説明
名前	ポリシーの名前
コンプライアンス	ポリシーのベンチマークにマッピングされるコンプライアンス標準とセキュリティのベストプラクティス。
効果	アドミッションコントローラーポリシーの設定が検出された場合の動作違反の影響には以下のものがあります。 • **拒否**: アドミッションコントローラーがアクションをブロックした。 • **[アラート]**: アドミッションコントローラーはアクションを許可しますが、アラートをトリガーします。
ステータス	ポリシーがアドミッションコントローラーポリシーの設定。ポリシーが有効である場合、

フィルター	説明
	違反アクションは違反の影響をトリガーします。
Last Violated	前回ポリシー違反があった日時。前回の違反の値をクリックすると、その特定のポリシーでフィルタリングされた [アドミッションコントローラーイベント] ページが開きます。これにより、ポリシーに違反したアクションをすべて表示できます。

Settings	• **ログの表示**
	• **アドミッションコントローラーポリシーの設定**:
	  • ポリシーを有効および無効にします。
	  • ポリシーパラメーターを編集する

脅威検出ルール

Tenable One Cloud Exposure を使用して、環境内の脅威検出をトリガーするルールを表示および管理できます。

脅威ルールを表示する

脅威ルールを表示する方法

1. クラウドサイバーエクスポージャーで、**[リスク>脅威ルール]** をクリックします。
   [脅威ルール] ページが表示されます。このページには、潜在的な脅威を特定するために使用されるすべてのルール Tenable 表示されます。この表のデータの詳細については、「 脅威ルールの列データ」を参照してください。
2. (オプション)テーブルをフィルタリングして、データの範囲を絞り込みます。
3. (オプション)テーブルに表示する列を選択するには、テーブルの右上にある列ピッカーアイコンをクリックします。
4. (オプション)ルールリストをカンマ区切り値 (CSV) ファイルにエクスポートするには、**[エクスポート]** をクリックします。

脅威ルールの列データ

次の表では、**[脅威ルール]** ページで使用できる列とフィルターについて説明します。

列	説明
プロバイダー	ルールが適用されるクラウドサービスプロバイダー (AWS、Azure、GCP など)。
深刻度	ルールに割り当てられているリスクレベル (例: 重大、高、中、低)。
名前	検出ルールの名前。
MITRE 戦術	MITRE ATT&CK フレームワークで定義されている、攻撃者の高レベルの目標。
MITRE テクニック	MITRE ATT&CK フレームワークで定義されている、目標を達成するために使用される特定の方法。
脅威検出	この特定のルールが環境内で検出をトリガーした合計回数。
ステータス	ルールが有効か無効かを示します。
変更者	ルール設定を最後に更新したユーザーまたはシステム。
変更時刻	ルールが最後に更新された日時。
作成者	ルールを最初に作成したユーザーまたはシステム。
作成時間	ルールが作成された日時。

除外

セキュリティおよびコンプライアンスプログラムは多くの場合、特定のビジネス状況において有効でありながら許容できる検出結果を生成します。たとえば、ロードバランサーは設計上パブリックにアクセス可能である場合や、開発環境で意図的に緩和されたアクセス許可が使用されている場合があります。除外と呼ばれるこれらの承認されたケースを管理することで、不必要なノイズ発生を防ぐことなく、リスクの全体像を正確に把握できます。

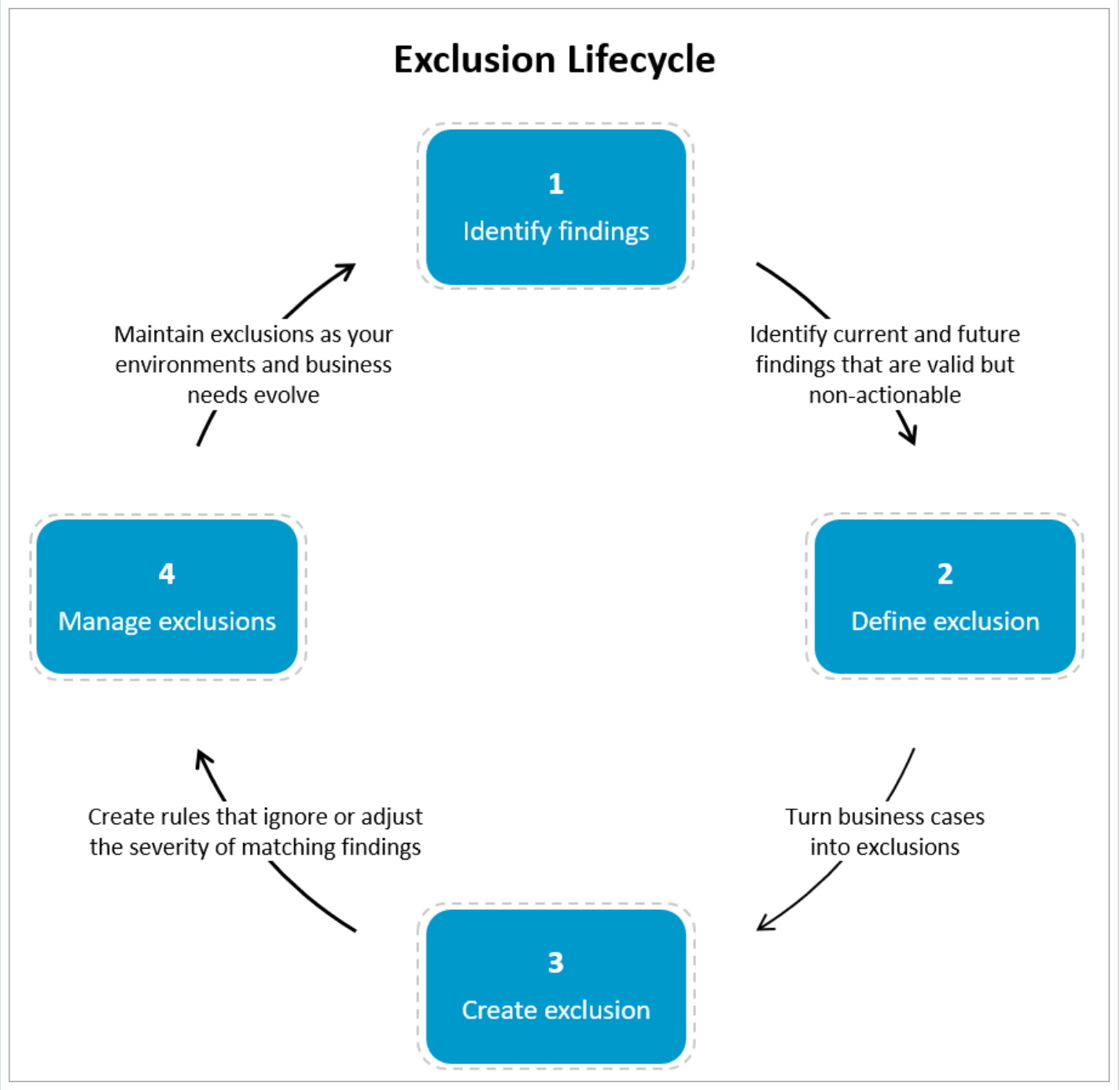
除外を使用すると、例外管理フレームワークが提供され Tenable One Cloud Exposure 、可視性と説明責任を維持しながら、これらの決定を承認、追跡、監査できます。

除外を使用することで、次のことが可能になります。

- **ノイズを減らす**: 未解決の検出結果から誤検出や意図的な設定を削除します。
- **大規模に適用する**: ビジネスニーズに合わせて 1 つの除外ルールを定義し、関連するすべての検出結果に適用します。
- **ガバナンスの維持**: 各除外を作成したユーザー、いつ、なぜ作成したかを記録します。
- **フォーカスの向上**: 未解決の検出結果に実用的なリスクのみが反映されるようにします。

除外ライフサイクル

> ライフサイクルのイメージを見る



除外は、4 段階のライフサイクルに従います。各段階で、例外が意図的に作成され、定期的に確認され、セキュリティモデルに適合するようになります。

1. **検出結果と今後の検出結果の特定**: 有効であるものの対処の対象とならない検出結果を見つけ、発生する可能性のある同様のケースを予測します。

2. **除外を定義する**: これらの検出結果を明確なビジネスケースにグループ化し、その **範囲**、**アクション**、**理由**を決定します。
3. **除外を作成する**: 各ビジネスケースを除外に変更し、一致する検出結果の深刻度を無視するか調整します。
4. **除外の管理**: 除外を維持、更新、または廃止して、例外管理を最新の状態に保ち、監査可能に保ちます。

検出結果と今後の検出結果の特定

検出結果の深刻度を無視したり調整したりする前に、設定を見直して、有効であるものの対処の対象とならない現在または潜在的な検出結果を特定します。これらには、意図的にパブリック設定、許容設定、または一時的な設定が含まれ、それらを除外したり深刻度をダウングレードしたりする予定です。

一般的な例:

- **環境**: テストのためのより広範なアクセスを許可する開発、QA、またはサンドボックス。
- **アーキテクチャ**: パブリックロード バランサー、インターネットに接続する API、またはデモテナント。
- **運用上のニーズ**: 緊急ロール、一時的なデバッグ設定、移行期間
- **データパイプライン**: ステージングバケット、一時キュー、または有効期間の短いスナップショット。
- **名前付けとタグ**: 意図を示す `env:dev`、`qa-*`、`lab-*` などの規則。

[検出結果] ページのフィルターを使用して、次のパターンを特定します。

フィルタータイプ	例	目的
ポリシー	パブリック EC2 インスタンス	意図的な設定または許容された設定を表す可能性のある特定のポリシーからの検出結果を特定します。
環境またはアカウント	Dev1 アカウントの中程度の検出結果	リスク許容度や可視性のニーズが環境によって異なる検出結果に焦点を当てます。

フィルタータイプ	例	目的
重大度の調整	ステージング環境の重大な検出結果を中に変更	有効だが非本番環境の設定でリスクの低い検出結果を再分類します。

これらのパターンを確認した後で、その処理方法を決定します。

- 意図的な検出結果や誤検出の検出結果は**無視**します。無視 無視された検出結果からのパターンベースの除外の作成方法を学習します。
- 検出結果が有効であるが、文脈上のリスクが低い場合、**深刻度を変更**します。

除外を定義する

既存または将来の検出結果を特定したら、それぞれが1つの明確に定義されたビジネスケースを表す除外にグループ化します。

典型的な除外の使用例

- テスト環境のパブリックエンドポイントなど、**意図的な設定**を反映した検出結果。
- 検証後に検出結果が**誤検出** であることが確認されました。
- 修正作業の進行中に付与された**一時的な例外**。

除外を定義するには、以下のようにして検出結果と今後の検出結果をグループ化します。

- **範囲**: 除外が適用される場所 (組織、アカウント、フォルダー)、および対象となるポリシー、リソース、深刻度を定義します。
- **アクション**: 定義された範囲内で対象となる検出結果の処理を決定します。深刻度を無視または変更します。

1つの検出結果は、アクションタイプごとに1つずつ、合計最大2つの除外による影響を受けます。同じアクションの複数の除外が同じ検出結果をターゲットとする場合、1つの除外のみが適用されます。詳細については、「 競合の解決 」を参照してください。

> 例: 検出結果を除外にグループ化する

最新のセキュリティスキャンで報告された検出結果:

- 顧客トラフィックに対応するために意図的に公開された**パブリックロードバランサー**の場合は 50 件。
- 5 緊急アクセスに使用され、厳密に制御されている**緊急アクセス用の IAM ロール**。
- テスト用に QA が使用する Dev1 アカウントの **パブリック S3 バケット** の場合は 15。

これらの検出結果はすべてセキュリティの観点からは妥当ですが、設定ミスではなく承認された設計上の選択を反映しています。

それぞれを手動で無視する代わりに、ビジネス上の正当性、範囲、期間を定義する 3 つの除外を作成します。

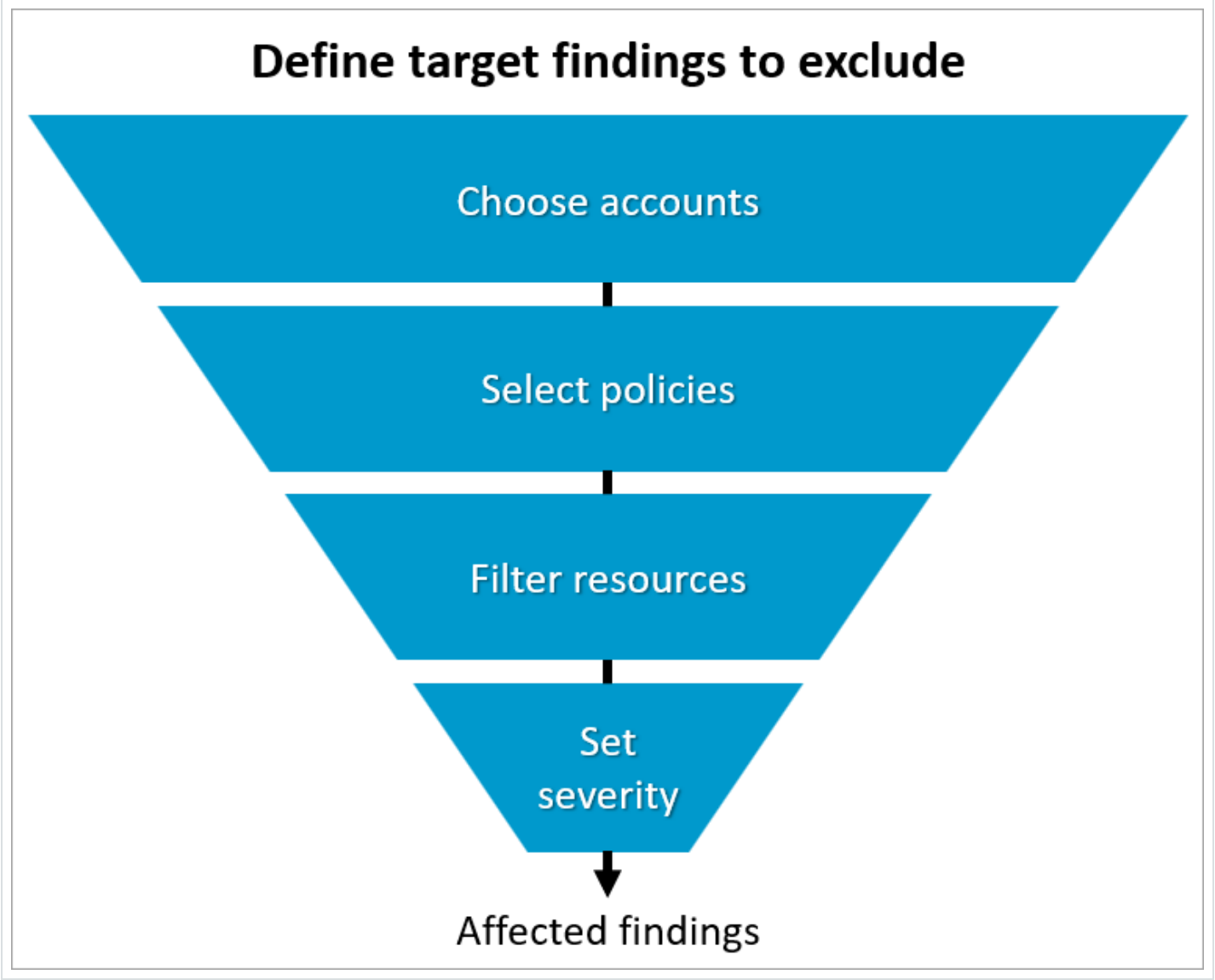
- **設計上**: パブリックロードバランサー用。
- **例外**: 緊急 IAM ロールの場合、1 年間有効です。
- **設計上**: Dev1 テストバケットの場合、パブリック S3 バケットポリシーに制限されます。

除外を定義するためのベストプラクティス

- 除外をできるだけ具体的にして、監視対象と監視対象外を明確にします。
- 同じ除外内で無関係のポリシーやリソースタイプを混在させないようにしてください。たとえば、「パブリック IAM ロール」や「パブリック EC2 インスタンス」などです。除外ごとに、1 つの問題またはビジネスケースに対処する必要があります。
- 適切な範囲の選択: 除外の範囲が広すぎると、実際の問題が隠されて監査が困難になる可能性がありますが、除外が狭すぎると、不要な複雑さとメンテナンスが行われる可能性があります。
- 意図せずに重複する可能性のある命名パターンは使用しないでください。たとえば、名前が `prod-` で始まるリソースを除外すると、新しく追加された、まだ監視が必要な本番リソースもキャプチャされる可能性があります。
- 重複するアラートを抑えるためのショートカットとして除外を使用しないでください。たとえば、プロジェクト内のすべての「重大」の検出結果を除外します。代わりに、根本的な原因を調査するか、明確な正当性を定めて深刻度の変更を適用してください。

範囲

> スコープ階層の画像を参照



範囲を定義することで、除外が意図した場合にのみ適用されるようになります。

- 複数のアカウントまたはポリシーをカバーするような **広範な除外** は、同じ条件が多くのリソースに当てはまる場合に、管理を簡素化し、反復作業を減らすことができます。ただし、広範な除外により、重要な検出結果が意図せずに非表示になるリスクも高まり、意図しないリソースが含まれる場合、監査がより困難になる可能性があります。

- 除外を**狭く**すると、より多くの制御と精度が得られます。これは、除外の理由が限られたリソースのセットにのみ適用される場合に便利です。ただし、狭い除外が多すぎると、時間の経過とともに追跡して維持することが難しくなる可能性があります。

組織のレビューとガバナンスのプロセスに適したバランスを選択します。各除外は、影響を制限する定義された条件を通じて検出結果を対象としています。

要素	説明
アカウント	除外を適用するアカウントを選択します。これは、組織全体に適用することも、特定のフォルダーまたは個別のアカウントに制限することもできます。
ポリシー	[すべてのポリシー] (All policies) を幅広く選択するのではなく、ビジネス上の理由に合致する特定のポリシーを選択します。関連のないポリシータイプ (IAM や EC2 など) を混在させると、重複が発生し、メンテナンスが複雑になる可能性があります。
リソース	除外がカバーするリソースを定義します。たとえば、名前が `LabUs-` で始まるすべての EC2 インスタンスや、`us-east-1` で `env:dev` というタグが付けられたリソースなどです。
深刻度	(オプション)除外を特定の深刻度の検出結果に限定します (たとえば、[低] または [中] の検出結果のみを無視し、[高] と [重大] は表示されたままにするなど)。

アクション

各除外によって、その条件に一致する検出結果の処理が決まります。

- **無視**: 一致する検出結果のステータスを「オープン」から「無視」に変更します。検出結果を無視する場合、理由も指定する必要があります。
    - **設計上:** 構成は意図的なものであり、機能のために必要です。
    - **例外**: 検出結果は、修正が完了するまで一時的に許容されます。
    - **誤検出**: 検出結果が不正確または無関係であることが確認されました。

    選択した理由は、無視された各検出結果の検出結果の表に表示される **サブステータス** にもなります。

- 深刻**度の変更**: 一致する検出結果の深刻度レベルを、選択したレベルに置き換えます。たとえば、[Critical] (重大) の検出結果を [Medium] (中) に変更します。これにより、問題の優先順位付けと報告方法を調整しながら、問題の可視性を維持できます。これは [除外] ページでのみ設定できます。

除外を作成する

ビジネス上の理由、範囲、およびアクションを定義したら、次のステップは除外を作成することです。この段階では、計画が作業ルールに変わり、一致する検出結果の深刻度を無視するか調整します。

除外は次の2つの場所で作成できます。

- **[除外] ページ (推奨):** [除外] ページから除外を作成すると、一元化された可視化と完全なコントロールが提供されます。これにより、正確なフィルター、範囲、有効期限を定義して、各除外が明確なビジネスケースを反映し、正確で監査可能かつ保守可能なガバナンスをサポートするようにします。
- **検出結果を無視する**: 選択した検出結果を特に対象とする除外を作成することで、検出結果を素早く無視できます。[検出結果] ページから作成された除外の作成はすぐに有効になります。これは、次のスキャンサイクルの前に特定の項目を非表示にする必要がある場合に適していますが、設定オプションは限られています。[検出結果] ページを頻繁に使用して結果を無視する場合は、一部の除外をより広く定義または調整する必要があることを示している可能性があります。

[除外] ページから除外を作成すると、組織全体の一貫性とビジネス目的との整合性を確保できます。次のスキャンサイクル後にターゲット検出結果が更新されます。

> 例: 除外を作成する

組織で複数のAWSアカウントを管理しています。そのうちの1つである **Dev1** は、意図的にインターネットに公開されているテスト環境をホストしています。これらの EC2 インスタンスのほとんどは、ラボリソースの識別に使用される `LabUs-` で始まる命名パターンに従います。ただし、`JohnD` という名前の手動で作成されたインスタンスも1つあり、同じテスト目的を果たしますが、規則に従っていません。リスクレポートを正確に保つためには、どちらも無視する必要があります。

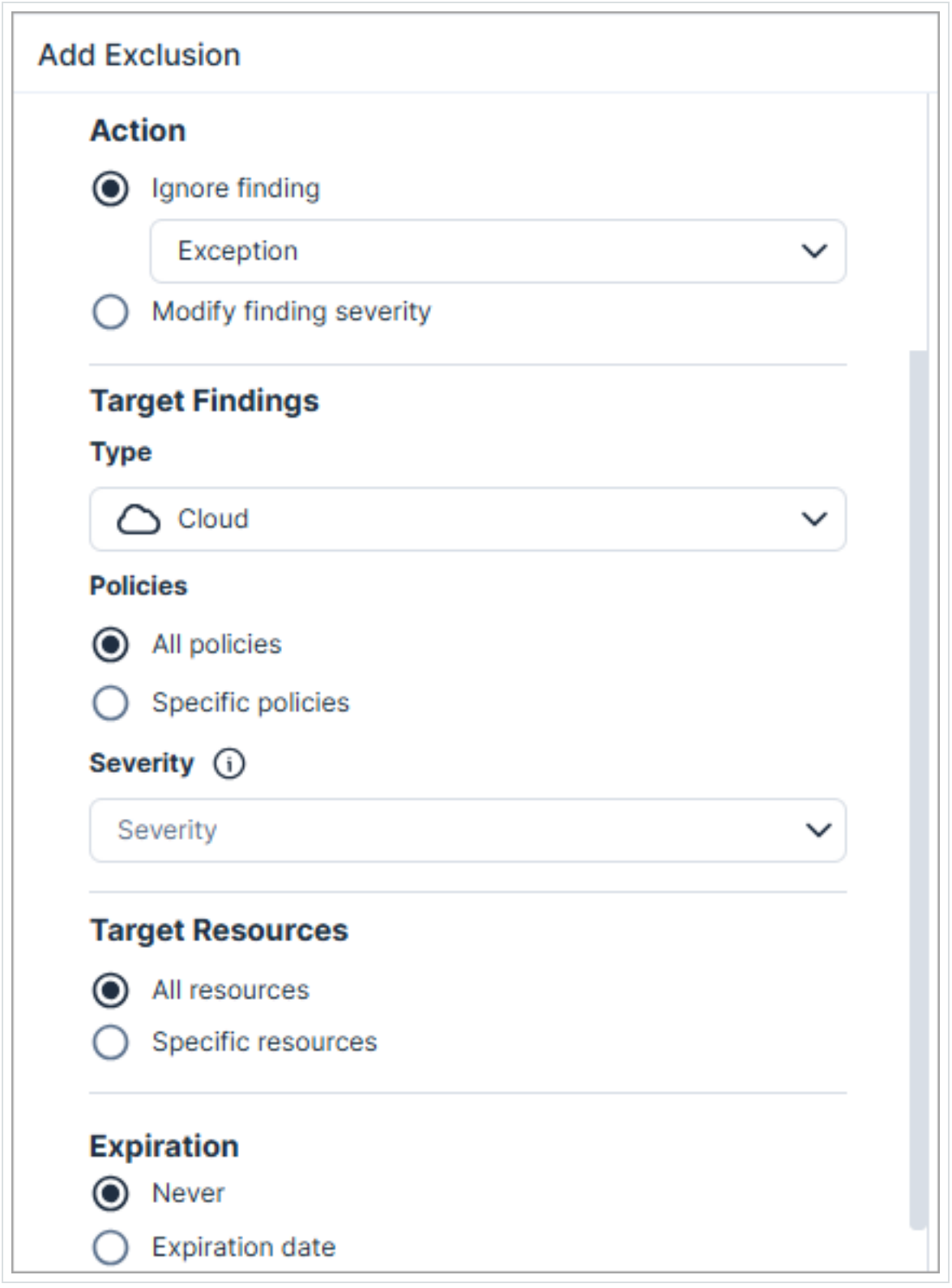
これらの既知の非本番リソースからの繰り返しのノイズを回避するために、これらのインスタンスのすべての検出結果を無視する除外を作成することにします

- **ビジネス上の必要性**: Dev1 アカウントの EC2 インスタンスへのパブリックアクセスは、テストのために意図されています。
- **目標**: このパターンに一致する Dev1 のパブリック EC2 インスタンスの検出結果をすべて無視する。

除外設定:

- **名前:** 既知のパブリック EC2 インスタンス
- **説明:** QA によって使用されるパブリックにアクセス可能なテストインスタンス
- **アクション:** 無視
- **検出結果タイプ:** クラウド
- **ポリシー:** パブリック EC2 インスタンス>特定のポリシー
- **リソース:** 名前が `LabUs-` OR リソース名が `JohnD` で始まる特定のリソース>- **有効期限:** なし

> [除外の追加] ウィンドウの画像を参照


Add Exclusion
Action
Ignore finding
Exception
Modify finding severity
Target Findings
Type
Cloud
Policies
All policies
Specific policies
Severity
Severity
Target Resources
All resources
Specific resources
Expiration
Never
Expiration date

除外を作成する方法

1. **[ポリシー]** > **[除外]** に移動します。
2. [組織] ドロップダウンで アカウント階層とフォルダー を選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. **[除外の追加]** をクリックします。除外の作成後は、アカウントの範囲を変更できません。
4. **名前**と**説明**を入力します。
    - 明確でビジネスに焦点を当てた名前を使用します (例: QA の公知の EC2 インスタンス)。
    - 除外の理由または正当性を説明してください。
5. [**アクション**] で、検出結果が除外と一致した場合の動作を選択します。
    - **無視**: 一致する検出結果を [オープンの検出結果] リストから除外します。
        - 検出結果を無視する理由を入力します。検出結果が無視されると、サブステータスは [例外]、[設計による]、[誤検出] のいずれかになります。
    - 深刻**度を変更する**: 一致する検出結果の深刻度を下げたり上げたりします。
6. **ターゲットとなる検出結果**の範囲を定義します。
    1. **タイプ**として、クラウドまたは IaC を選択します。
    2. **[ポリシー]** で、[すべてのポリシー] または [ターゲットとする特定のポリシー] を選択します。定義されたビジネスケースに一致する特定のものを選択することをお勧めします。
    3. 必要に応じて深刻 **度** フィルターを追加して、特定の深刻度の検出結果のみを含めることもできます。
7. **ターゲットリソース**を定義します。
   以下の除外を作成する場合:
    - クラウド: 関連するリソースを選択します。
    - コード: パターンには次のワイルドカード文字を使用します。
        - アスタリスク * - 0 文字以上と一致
        - クエスチョンマーク ? - 1 文字と一致
          たとえば、パターン付きの名前 `aol-*`

8. **[有効期限]** で、[なし] または [有効期限] のいずれかを選択します。有効期限を過ぎると、除外は検出結果に適用されなくなります。他の除外がこれらの検出結果に影響を与えない場合、検出結果は再オープンされるか、深刻度が元に戻されます。
9. 除外を作成する前に、設定を慎重に確認してください。[検出結果] プレビューパネルには、対象となるすべての未解決の検出結果が一覧表示されます。これを使用して、保存する前にフィルター、保持、範囲が意図した結果を正確にターゲットにしていることを検証します。
10. **[保存]** をクリックします。保存後、除外は次のスキャンサイクルで有効になり、一致するすべての検出結果が更新されます。

除外の管理

[除外] ページを使用すると、環境やビジネスニーズの変化に合わせて除外を確認および管理できます。定期的なレビューにより、結果を正確に保つことができ、古いルールによって有効なリスクが隠されるのを防ぐことができます。

除外を管理する方法

- 毎 **月確認** し、各除外が現在の設定とリスク許容度を反映していることを確認します。
- 除外を**編集**し、必要に応じてフィルター、範囲、有効期限を更新します。
- 除外がカバーする検出結果が多すぎる場合は、**フィルターを厳格** にするか、焦点を絞った小規模な除外に分割します。
- 除外を一時的に **無効** にして、その影響を評価します。
- 有効期限が切れた、または有効なビジネスケースでなくなった除外を**更新または削除**します。
- 定期的に **監査** を行い、監査ログを使用して所有権、作成時間、正当性を検証します。

また、検出結果を無視するすることで、[検出結果] ページから直接除外を管理することもできます。除外の管理の詳細については、競合の解決 と除外ステータスを参照してください。

[除外] ページに表示される内容

[除外] ページには、すべての除外とその設定、現在のステータスが一元的に表示されます。これは、組織全体で除外がどのように動作するかを検証し、除外が長期にわたって正確であることを確認するために使用します。

このページから、除外を作成、編集、複製、無効化、削除したり、除外を作成したユーザーと影響を受ける検出結果を確認したりできます。

テーブルの各行は、監査および管理に必要な重要な情報を含む1つの除外を表します。

縦棒	説明
名前	除外の名前。クリックすると、フルプロファイルが開きます。
説明	除外のビジネス上の理由または目的。
範囲	除外が適用される場所: 組織、アカウント、フォルダー
アクション	一致する検出結果に適用されたアクション: 深刻度を無視または変更します。
検出結果タイプ	検出結果のソース: クラウドまたは IaC。
ポリシー	すべて、または対象ポリシーのリストのいずれか。
有効期限日	除外の有効期限が切れる日付、有効期限がない場合はダッシュ(-)。
作成者	除外を作成したユーザー。
作成時間	除外が作成された日時。
ステータス	除外ステータス。
検出結果	現在除外の影響を受けている検出結果の数。クリックするとリストが表示されます。

除外ステータス

各除外には、システムでの現在の状態を反映するステータスがあります。[除外] ページの [ステータス] 列でこれらを表示し、各除外がどのように適用されているかを追跡します。

ステータス	説明
有効	除外が有効で、期限切れでない場合は、次回のスキャンに適用されます。除外の有効期限が切れると、他の除外が適用されない限り、検出対象の検出結果は再オープンされるか元に戻されます。
無効	除外は無効な状態ですが、再度有効にすることができます。
更新を保留中	変更があったため、次回のスキャンで更新されます。
無効化を保留中	このあと無効になりますが、スキャンが完了するまでは有効な状態です。
削除の保留中	削除のキューに登録されています。スキャンが完了するまでは有効な状態です。

既存の除外に追加するためのルール

[検出結果を無視] ダイアログを開いて **[既存の除外に追加]** を選択すると、ドロップダウンに選択した検出結果と互換性のある除外のみが表示されます。

これにより、検出結果は、タイプ、ポリシー、範囲に一致する除外にのみ追加でき、競合や意図しない動作を防ぐことができます。

次のすべての条件が満たされた場合にのみ、除外がドロップダウンに表示されます。

ルール	説明
書き込みアクセス許可	除外の範囲に対する書き込みのアクセス許可がある
アクションを無視に設定*	除外のアクションは [無視] (Ignore) に設定されています。
検出結果タイプ	除外の検出結果タイプ (クラウドまたは IaC) が、選択した検出結果と一致します。
ポリシーの一致	除外は、選択した検出結果とまったく同じポリシーを対象とします。
単一ポリシーの範囲	除外は 1 つのポリシーに適用され、複数のポリシーには適用されません。
深刻度フィルター	除外には定義された深刻度フィルターがありません。
一括選択ルール	複数の検出結果が選択されている場合、すべてが同じポリシーからのものである必要があります。

競合の解決

場合によっては、複数の除外が同じ検出結果を対象にできます。この場合、優先度は**範囲**と**作成時間**によって決定されます。

除外は、アクションごとに個別に評価されます (深刻度は無視または変更)。検出結果には、アクションタイプごとに 1 つずつ、合計 2 つのアクティブな除外を含めることができます。

同じアクションの複数の除外が同じ検出結果をターゲットとする場合、優先順位は次の順番になります。

1. **範囲の特異性**: より明確な除外が優先されます。たとえば、アカウントレベルで定義された除外は、組織レベルで定義された除外よりも優先されます。

2. **作成時刻**: 2 つの除外が同じ範囲とアクションを共有する場合は、最初に作成された除外が優先されます。

> 例: 競合の解決

組織では、共有 OrgA と Dev1 という開発アカウントを含む複数の AWS アカウントを運用しています。

最初に、**組織** レベルで除外を作成して、名前が `Test-` から [低] に始まるリソースのパブリック EC2 インスタンスの検出結果の深刻度を下げます。これにより、QA に使用される非本番インスタンスからのノイズを低減できます。

その後、セキュリティエンジニアが同じポリシーの **Dev1 アカウント** レベルで別の除外を作成し、同じ `Test-*` インスタンスの深刻度を中に設定して、そのアカウントで公開されている資産の可視性を向上させます。

Dev1 の除外はより狭い範囲で定義されているため、優先されます。

結果として以下

- Dev1 アカウントの `Test-*` EC2 インスタンスの検出結果は、深刻度 [中] で表示されます。
- 他のアカウントの同じパターンの検出結果は、低のままです。

業務

自動化

> **必要な Tenable One Cloud Exposure ユーザーロール:** このアクションを クラウド サイバーエクスポージャー で実行するには、**管理者** ロールが必要です。詳細については、ユーザーとグループを参照してください。

次の状況で、統合 にプッシュ通知を送信する自動化ルールを作成します。

- 特定のリスク (検出結果または脅威ストーリー) が クラウド サイバーエクスポージャー で特定された場合 サードパーティ サードパーティツールにリスクデータを送信を参照してください。

- ユーザーアクションが クラウド サイバーエクスポージャー で実 行 されたとき。サード パーティ サード パーティツールへの監 査 データの送 信 を参 照してください。

重 要: 自 動 化 ルールは、新しいリスクとアクティビティに対してのみトリガーされ、遡 及 的 に適 用 されません。

サード パーティツールにリスクデータを送 信

クラウド サイバーエクスポージャー が特 定 のリスクを特 定 したときに、統 合 されたサード パーティツールにプッシュ通 知 を送 信 する自 動 化 ルールを作 成 します。リスク自 動 化 ルールは、選 択 した **タイプ** に応じて、クラウドの検 出 結 果 、IaC の検 出 結 果 、または脅 威 ストーリーに適 用 できます。

リスク自 動 化 ルールごとに、次 のコア要 素 が定 義 されます。

- **ターゲットの範 囲**: 自 動 化 をトリガーする特 定 のアカウント範 囲 。
- **タイプ**: 自 動 化 が適 用 されるリスクのカテゴリ(**クラウドの検 出 結 果** 、 **IaC の検 出 結 果** 、 **脅 威 ストーリー**)。このタイプによって、オートメーションクエリで使 用 できるフィールドとデフォルトのフィルターが決まります。
- **自 動 化 クエリ**: ルールをトリガーする特 定 のリスク (深 刻 度 、ステータス、リソースタイプ、アクター、脅 威 検 出 など) を定 義 する探 索 エクスプローラークエリ。
- **配 信 方 法**: 通 知 またはチケット が送 信 される1つ以 上 のサード パーティツール統 合 。

注 意: 会 話 から自 動 化 を開 始 するには、Hexa AI に自 動 化 の作 成 を依 頼 します。Hexa AI は、名 前 、説 明 、クエリ、およびターゲット スコープを提 案 します。提 案 の **[オートメーションの作 成]** をクリックすると、これらの値 が入 力 された [オートメーションの作 成] ページが開 きます。設 定 を確 認 し、配 信 方 法 を追 加 して、 **[作 成]** をクリックします。詳 細 については、「 Hexa AI」を参 照 してください。

新しい自 動 化 ルールを追 加 する方 法

1. クラウド サイバーエクスポージャーコンソールで、**[Operations > Risk Automations]** に移 動 します。
2. (オプション)**[組 織]** ドロップダウンで範 囲 を選 択 します。選 択 した範 囲 内 でアクセス許 可 を持 つユーザーは自 動 化 にアクセスできます。
3. **[自 動 化 の作 成]** をクリックします。

4. 自動化設定を行います。
    1. 自動化ルールを正確に説明する **[名前]** と、オプションで **[説明]** を入力します。
    2. **[ステータス]** で、**[有効]** または **[無効]** のいずれかを選択します。
    3. **[タイプ]** には、**[クラウドの検出結果]** (デフォルト)、**[IaC の検出結果]**、または **[脅威ストーリー]** を選択します。

        > **注意:** ドロップダウンには、ライセンスとアクセス許可がカバーする種類のみが表示されます。

    4. [クエリの選択] をクリックして既存のクエリを選択するか、最初から作成します。クエリビルダーは、選択した **タイプ** に基づいてデフォルトのフィルターを適用します。
        - リンクされたクエリを削除したり、プライベートにしたり、サポートされていない構文で編集したりすることはできません。
        - 既存のクエリを選択して編集する場合は、三点リーダーメニューを開き、[リンク解除] をクリックしてフィルターを変更します。ポリシーは元のクエリと同期されなくなります。
    5. **[ターゲットの範囲]** で、自動化をトリガーする範囲を選択します。フォルダー全体を選択すると、そのフォルダー内にあるすべての既存アカウントと今後作成されるアカウントの自動化がトリガーされます。
    6. **既存のリスクに適用** するかどうかを選択します。これを有効にすると、今後検出される新しいリスクに加えて、選択したタイプのすべての現在のリスクに自動化が適用されます。

        > **注意:** このオプションは、新しい自動化を作成するとき、または自動化が以前に無効になっていた場合にのみ使用できます。

    7. **[配信]** で、**[メソッドの追加]** をクリックして、通知の送信先を設定します。特定の配信方法を統合リストに表示するには、まず 統合 する必要があります(自動的に表示されるメールアドレスを除く)。

        以下の設定手順は、**タイプ** に関係なく同じです。変更されるのは、各チャネルに送信されるコンテンツです。脅威ストーリー用に作成された Jira チケットには脅威固有のフィールド (アクター、脅威検出) が含まれますが、クラウドまたは IaC の検出結果のチケットには代わりにリソースと深刻度のフィールドが載せられます。

メールアドレス

1 つ以上のメールアドレスを手動で入力するには **受信者を指定** を選択し、リソース所有者にリスクを送信するには **カスタムプロパティから受信者を抽出** を選択します

- **受信者を指定します。** To フィールドに 1 つ以上のメールアドレスを入力します
- **カスタムプロパティから受信者を抽出します。** **所有者カスタムプロパティ** を選択して、リソース所有者データから受信者のメールアドレスを解決します。また、カスタムプロパティに有効なメールアドレスが見つからない場合に使用する **フォールバック受信者** も入力する必要があります。フォールバック受信者は、アドレスを解決できなかったすべての所有者のすべてのリスクを受け取ります。

CC フィールドは両方のオプションで使用できます。

各メール配信方法で、1 つの所有者カスタムプロパティがサポートされます。複数のプロパティをカバーするには、メール配信方法を追加します。複数の配信方法で同じ所有者カスタムプロパティを選択することはできません

> **注意: カスタムプロパティから受信者を抽出** を使用する場合、クラウドサイバーエクスポージャーは自動化スコープ内のすべてのリスクではなく、各所有者のリソースに関連付けられたリスクのみを送信します。

Slack

ワークスペース(単一選択)を選択し、受信者を設定します。

- **受信者を指定します。** 選択したワークスペースから1つ以上のチャンネルを選択します。
- **カスタムプロパティから受信者を抽出します。** **所有者カスタムプロパティ** を選択して、Slack ユーザーとしてリソース所有者に直接リスクを送信します。所有者を解決できない場合の **フォールバックチャネル**を指定します

注意：カスタムプロパティから受信者を抽出 を使用する場合、クラウドサイバーエクスポージャーは各所有者に自分のリソースに関連付けられているリスクのみを送信します。

Microsoft Teams

組織を選択し(単一選択)、受信者を設定します。

- **受信者を指定します。** 選択した組織から1つ以上のチャンネルを選択します。
- **カスタムプロパティから受信者を抽出します。所有者カスタムプロパティ**を選択して、Teams ユーザーとしてリソース所有者に直接リスクを送信します。所有者を解決できない場合の**フォールバックチャネル**を指定します

注意：カスタムプロパティから受信者を抽出 を使用する場合、クラウドサイバーエクスポージャーは各所有者に自分のリソースに関連付けられているリスクのみを送信します。

Jira

統合を有効にしてから、**プロジェクト**、**課題タイプ**、**ラベル**、**エピック** (オプション)、**環境** (Jira インスタンスの URL) を選択します。ラベルの場合、Jira インスタンスですでに設定されているラベルのリストから選択するか、Jira に送信される新しいラベルを手動で追加できます。ラベル名にスペースを含めることはできません。

担当者には、次のいずれかを選択します。

- **担当者を指定します。** ドロップダウンからJiraユーザーを選択します。Jiraプロジェクトで[担当者] フィールドがオプションの場合、このフィールドはオプションです。
- **カスタムプロパティから担当者を抽出します。所有者カスタムプロパティ**を選択して、リソース所有者データから担当者を解決します。所有者のメールアドレスを解決できない場合には、オプションで **フォールバック担当者** を指定できます。Jira で [Assignee] (担当者) フィールドがオプションである場合、このオプションはオプションです。

ServiceNow

統合を有効にし、**インスタンス**を選択して、担当者を設定します。

- **割り当て先**。そのグループから**割り当てグループ** (ServiceNow インスタンスで必要な場合にのみ表示) と**割り当て先** ユーザーを選択します。
- **カスタムプロパティからアドレスを抽出します。所有者カスタムプロパティ**を選択して、リソース所有者データから担当者を解決します。お使いの ServiceNow インスタンスで割り当てグループが必要な場合は、**[Fallback Assignment Group]** フィールドも表示され、指定する必要があります。

Datadog 組織

QRadar サーバー

SQS キュー

Splunk イベントコレクター

Webhook

5. クエリをビルドしてプレビューします:

> **注意:**
> - クエリの作成は、以前に**スタンドアロンクエリ**を選択した場合のみ関連します。
> - システムは、選択した**タイプ**に一致するベースラインフィルターをクエリビルダーに自動的に入力します。

   1. クエリビルダーを使用して、リスク基準を定義します。詳細は、「エクスプローラー」を参照してください。
   2. ビルダーの下の表を確認し、現在クエリロジックに一致するリスクのプレビューをリアルタイムで確認します。
6. **[Create]** をクリックします。

サードパーティツールへの監査データの送信

自動化ルールを作成して、ユーザーアクションがクラウドサイバーエクスポージャーで実行されたときに、クラウドサイバーエクスポージャー監査データを以下のいずれかのサードパーティツールに送信します。

- SIEM ツール:
    - Datadog
    - Splunk
    - QRadar
- 通知ツール:
    - Slack
    - Microsoft Teams
- Webhook 経由のその他のサードパーティツール

監査ベースの自動化ルールごとに、次のコア要素が定義されます。

- 自動化をトリガーする特定のアカウント範囲。詳細については、アカウント階層とフォルダーを参照してください。
- 自動化をトリガーする一連のユーザーアクションです。
- Tenable と統合したサードパーティツールに応じた自動化ターゲット。

新しい自動化ルールを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Operations (操作)] > [Audit Automations] (監査の自動化)** に移動します。
2. (オプション)[組織]ドロップダウンで 範囲 を選択します。選択した範囲内でアクセス許可を持つユーザーは自動化にアクセスできます。
3. **[ルールの追加]** をクリックします。
4. 自動化ルールを正確に説明する **[名前]** と **[説明]** (オプション) を入力します。
5. ステータス: **[有効]** または **[無効]** のいずれかを選択し、**[保存]** をクリックします。
6. 自動化をトリガーする **クラウドアカウントターゲット** を選択します。フォルダー全体を選択すると、そのフォルダー内にあるすべての既存アカウントと今後作成されるアカウントの自動化がトリガーされます。

7. 自動化ルールをトリガーするユーザー**アクション**を選択します。
    - **すべて**。ユーザーアクション、および今後 Tenable によって追加されるすべてのアクションが含まれます。
    - **具体的なアクション**カテゴリ別に整理された 1 つ以上のユーザーアクションを個別に選択します。
        - プラットフォーム。
        - JIT 使用資格。詳細については、JIT ドキュメントの資格の追加 。
        - JIT アクセスリクエスト詳細は、JIT ドキュメントのアクセスをリクエストする を参照してください。
8. **システム生成のアクションも含める**かどうかを選択します。
9. **[配信方法の追加]** をクリックして、通知の送信先を設定します。特定の配信方法を統合のリストに表示するには、まず統合 する必要があります(自動的に表示されるメールアドレスを除く)。
    - **Datadog 組織**
    - **Splunk イベントコレクター**
    - **QRadar サーバー**
    - **SQS キュー**
    - **Slack チャンネル**
    - **Teams チャネル**
    - **Webhook**

自動化を有効または無効にする

自動化ルールを有効または無効にすると、設定を失うことなく、自動化ワークフローを一時的に柔軟に一時停止できます。データまたは通知の送信を再開する準備ができたら、ルールをオンに戻すことができます。

自動化を有効または無効にする方法

1. クラウドサイバーエクスポージャーコンソールで、次のいずれかに移動します。
    - **運用>リスクの自動化**
    - **オペレーション>監査の自動化**
2. (オプション)[組織]ドロップダウンで アカウント階層とフォルダー を選択します。選択した範囲内でアクセス許可を持つユーザーは自動化にアクセスできます。
3. テーブル内の関連する自動化の横にある三点リーダーをクリックし、**[編集]** をクリックします。
4. [ステータス] で **[有効]** または **[無効]** を選択し、**[保存]** をクリックします。

既存の自動化の複製

以前生成された自動化 (リスクデータまたは監査データ) を複製して、新しい自動化を作成するためのベースラインとして使用するこれにより、以前の自動化と同じ設定で新しい自動化をすばやく作成できるため、時間と手間を節約できます。たとえば、AWS 検出結果用の ServiceNow 自動化があり、同様の自動化が Azure 用に必要な場合、AWS の自動化を複製して、範囲を Azure 環境に変更します。

アイテムを複製するとき、関連する設定はすべて元の範囲に基づいて処理されます。

- これは送信方法やラベルなどの設定に適用されます。
- 関連する設定が現在の設定よりも狭い範囲で設定されている場合、その設定がアイテムとともに複製されることはありません。
- たとえば、特定の範囲から、より広い組織の範囲にアイテムを複製した場合、その狭い範囲にのみ関連付けられている設定は引き継がれません。

これにより、無関係のデータや設定ミスのあるデータが新しい範囲で作成されるのを防ぐことができます。これらの特定の設定が必要な場合は、現在の範囲内で手動で再設定する必要があります。

既存の自動化を複製する方法

1. クラウドサイバーエクスポージャーコンソールで、次のいずれかに移動します。
    - **運用>リスクの自動化**
    - **オペレーション>監査の自動化**

2. (オプション)[組織]ドロップダウンで アカウント階層とフォルダー を選択します。選択した範囲内でアクセス許可を持つユーザーは自動化にアクセスできます。
3. テーブル内の関連する自動化の横にある三点リーダーをクリックし、**[複製]** をクリックします。
4. 必要に応じて自動化を変更し、**[追加]** をクリックします。

レポート

レポート

レポートを作成して、関連する Tenable One Cloud Exposure データの 1 回限りのレポートまたはスケジュールされたレポートを生成します。各レポートは、レポートの目的に応じてさまざまな形式で生成されます。

- **CSV**。編集可能な作業ドキュメントとして使用したり、他のユーザーとの共同作業やフィードバックを受け取ったりするのに適しています。
- **PDF**です。データを可視化して、経営幹部やその他の関連するステークホルダーと共有するのに最適です。

レポートの作成

新規レポートを作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[レポート] > [生成されたレポート]** をクリックします。
2. (オプション)[組織]ドロップダウンで 範囲 を選択し、レポートのデータに反映させるアカウント/IdP テナントのグループを定義します。選択した範囲内でアクセス許可を持つユーザーはレポートにアクセスできます。選択した **範囲** が [New Report] (新規レポート) ダイアログに表示されます。
3. **[レポートの作成]** をクリックします。
4. 意味のある名前を入力します。
5. ドロップダウンからレポート レポートタイプ を選択します。
6. 選択したレポートタイプによっては、追加のフィールドを設定する必要があります。以下に例を示します。

- **クエリ。**[クエリの選択]をクリックして既存のクエリを選択するか、最初から作成します。
  - リンクされたクエリを削除したり、プライベートにしたり、サポートされていない構文で編集したりすることはできません。
  - 既存のクエリを選択して編集する場合は、三点リーダーメニューを開き、[リンク解除]をクリックしてフィルターを変更します。ポリシーは元のクエリと同期されなくなります。
- **コンプライアンス**コンプライアンスタイプを選択します。
- **インベントリ**。オプションで特定の**リソースタイプ**を選択して、そのタイプのすべてのリソース(すべてのAWS EC2インスタンスなど)にレポートを制限できます。さらに、選択したリソースタイプの利用可能な関連データでレポートをフィルタリングできます。たとえば、リソースタイプとして**EC2インスタンス**を選択した場合、特定のアカウントやインスタンスの状態でさらにフィルタリングして、条件に一致するリソースのみがレポートに表示されるようにすることができます。

7. **配達時間**を選択してください:
   - **さて**。1回限りのレポートを生成します。
   - **スケジュール**。特定の時間にレポートを生成するための頻度を定義します。カスタム間隔(たとえば、3週間ごとまたは6か月ごと)と週次配信の特定の曜日を設定して、チームが必要とするときに正確にデータが届くようにすることができます。
8. **[配信方法の追加]**を使用して、レポートのコピーを特定の受信者に送信します。詳細については、「Slackまたは Teams」を参照してください。
   - メールアドレス

     > **注意:**
     > - 検出結果レポートの場合、**リソースの所有者ごとにメール**を送信するように選択できます。これにより、各インベントリ(プロパティとラベル)に、自身のリソースに関連する検出結果のレポートが送信されます。
     > - メールでレポートを送信する場合、ファイルサイズは14.5MBに制限されています。レポートのサイズが大きい場合は圧縮されるか、ダウンロードリンク経由で提供されます。

   - Slackチャンネル
   - Teamsチャネル
9. **[作成]**または**[スケジュール]**をクリックします。

既存のレポートを複製する

以前に生成されたレポート (1 回限りのものかスケジュールされたものかを問わず) を複製して、新しいレポートを作成するためのベースラインとして使用します。これにより、以前のレポートと同じ設定で新しいレポートをすばやく作成でき、時間と手間を節約できます。たとえば、AWS 用の検出結果の週次レポートがあり、同様のレポートが Azure 用に必要な場合、そのレポートを複製して、範囲を Azure 環境に変更します。

アイテムを複製するとき、関連する設定はすべて元の範囲に基づいて処理されます。

- これは、配送方法やラベルなどの設定に適用されます。
- 関連する設定が現在の設定よりも狭い範囲で設定されている場合、その設定がアイテムとともに複製されることはありません。
- たとえば、特定の範囲から、より広い組織の範囲にアイテムを複製した場合、その狭い範囲にのみ関連付けられている設定は引き継がれません。

これにより、無関係のデータや設定ミスのあるデータが新しい範囲で作成されるのを防ぐことができます。これらの特定の設定が必要な場合は、現在の範囲内で手動で再設定する必要があります。

既存のレポートを複製する方法

1. クラウドサイバーエクスポージャーコンソールで、**[レポート] > [生成されたレポート]** をクリックします。
2. (オプション)[組織]ドロップダウンで 範囲 を選択し、レポートのデータに反映させるアカウントのグループを定義します。選択した範囲内でアクセス許可を持つユーザーはレポートにアクセスできます。
3. テーブル内の関連するレポートの横にある三点リーダーをクリックし、**[複製]** をクリックします。
4. 必要に応じてレポートを変更し、**[作成]** をクリックします。詳細については レポートの作成 」を参照してください。

レポートタイプ

[レポート] ページからは、以下のレポートタイプを作成できます。

レポート	説明
クエリ	(CSV)調査結果のポータブルスナップショット。すべてのアクティブな行と列 (プリンシパル、ラベル、タグなど) がキャプチャされ、オフラインでの分析や監査のためのポイントインタイムデータが提供されます。
クラウドの検出結果	(CSV) クラウドサイバーエクスポージャーにおけるクラウド検出結果のリスト。レポートには、各検出結果について、アカウントの詳細、作成時間、検出結果のカテゴリ/深刻度、影響を受けるリソースに関する情報などが含まれます。
コンプライアンスアカウントのサマリー	(CSV)特定の標準について、組織内のアカウント全体におけるコンプライアンススコアリングの内訳を表示します。7 日前、30 日前、90 日前のスナップショットを使用して、コンプライアンススコアを経時的に追跡します。この情報を使用することで、特定のアカウントの高リスク領域を特定し、対処できます。
コンプライアンスの詳細な結果	(CSV)すべてのコンプライアンス評価 (合格、不合格、除外) のタイムスタンプ付きの完全な記録を含むレポート。各行にはリソースレベルとセクションレベルの詳細な情報が含まれているため、手動で調査することなく、失敗した評価や特定のリソースを直接フィルタリングできます。
コンプライアンス要件のサマリー	(PDF または CSV)標準に対応するすべてのポリシーの詳細、ポリシーによって評価されたリソースの総数の内訳、ポリシーベンチマークに合格または不合格になったリソースの割合 (深刻度別にグループ化) を示すサマリーレポートを生成します。各標準の詳細については、規格一覧 を参照してください。
ダッシュボード	(PDF)公開ダッシュボードからレポートを生成して、インサイトの共有を簡素化します。エグゼクティブの概要や検出結果の傾向など、実用的なデータをステークホルダーに自動的に提供する。レポートはダッシュボードに動的に接続されたままになり、ウィジェットや名前の更新が今後の配信に反映されます。
インベントリ	(CSV)クラウドサービスプロバイダー (CSP)、アカウント、リソースタイプなどの属性ごとにグループ化された、クラウドサイバーエクスポージャーで識別されるすべてのクラウドリソースの完全なリスト。(オプション)特定の **リソースタイプ** を選択して、そのタイプのすべ

レポート	説明
	てのリソース (すべての AWS EC2 インスタンスなど) にレポートを制限できます。これを行うと、出力にはリソース固有のデータを含む列が追加されます。[Inventory] (インベントリ) ビューから直接レポートを作成することもできます。詳細については、「資産インベントリの表示」を参照してください。
管理	(PDF)アカウントと全体的なセキュリティポスチャーのスナップショットを提示し、クラウド環境の包括的な概要を示します。過剰なアクセス許可、公開されているリソース、コンプライアンスなど、セキュリティの一般的な懸念事項に関するインサイトを取得します。重要なメトリクスを時系列で追跡し、どのような進捗があったかや、修正が必要な領域があるかどうかを確認できます。
設定ミス	(PDF) クラウドサイバーエクスポージャーポリシーによるリソースの評価方法に関する大まかなスナップショット。各ポリシーにどのコンプライアンス標準がマッピングされているかを簡単に確認できます。ポリシーのベンチマークに合格できなかったリソースの数と、不合格となった結果の深刻度レベルを表示して、そのような設定ミスの範囲に関するインサイトを取得できます。
脆弱性	スキャンされた各リソースについて、ソフトウェアパッケージごとのすべての脆弱性のリスト。このデータを使用して、アクティブなワークロードのうち、パッチ適用が必要な既知のソフトウェア脆弱性を持つものを特定します。レポートには、各脆弱性について、アカウント、OS、パッケージ、CVE などに関する詳細が含まれます。
AWS アクセスキー	(CSV)アカウントごとにグループ化された、AWS アカウント内のすべてのアクセスキーの完全なリスト。関連付けられているユーザー、付与されるアクセス許可の深刻度レベル、キーが有効か無効かなどの詳細が含まれます。この情報は、永続的かつ静的な認証情報を環境から削除するのに役立ちます。
AWS Identity Center の割り当て	(CSV)AWS Identity Center (旧 SSO) のアクセス許可セットとその割り当ての完全なリスト。レポートには、アクセス許可セットが割り当てられたユーザーのリスト、アクセス許可セットの名前、アクセス許可セットの割り当て方法 (プリンシパルに直接割り当てられているか、グループ経由か) の表示、およびアカウント ID が含まれます。この情報

レポート	説明
	を使用すると、たとえば、次のことが可能になります。 • グループ経由ではなく、個々のユーザーに直接割り当てられたアクセス許可セットを特定し • アカウントの 2 つの異なるグループを介してユーザーに同じアクセス許可セットが割り当てられている、重複する割り当てを特定します
AWS ポリシーの割り当て	(CSV)環境内の AWS アイデンティティのすべてのポリシー割り当ての完全なリスト (アカウントごとにグループ化)。レポートには、すべてのアイデンティティについて、アイデンティティ名 /ARN/タイプ (IAM ユーザー/ロール)、関連付けられているポリシー名 /タイプ (マネージド/インライン)、ポリシーがアタッチされているアイデンティティ、データ保持期間と学習期間にポリシーが使用されたか未使用であったかなどの情報が含まれます。
Azure ロールの割り当て	(CSV)環境内の Azure アイデンティティのすべてのロールの割り当ての完全なリスト (サブスクリプションごとにグループ化)。レポートには、すべてのアイデンティティについて、アイデンティティのタイプ (Microsoft Entra ユーザー、マネージド ID など)、関連付けられているロール、割り当てのステータス (アクティブ、資格)、このアイデンティティが Azure でこの特定のアクティビティを実行したのが最後に確認された時刻などの情報が含まれます。
IaC 検出結果	(CSV) お使いの環境のコードリポジトリスキャン経由で検出された検出結果のサマリー。レポートには、各検出結果について、リポジトリの詳細、作成時間、検出結果のカテゴリ/深刻度、影響を受けるリソースに関する情報などが含まれます。このレポートタイプは、コードリポジトリを含む選択されたアカウント範囲で使用できます。たとえば、root「Code」フォルダーまたは特定のコードリポジトリなどです。
GCP IAM ロールバインディング	(CSV)環境内の GCP アイデンティティのすべてのロールバインディングの完全なリスト (プロジェクトごとにグループ化)。レポートには、すべてのアイデンティティについて、プロジェクトの詳細 (名前、ID、パス)、アイデンティティの種類 (サービスアカウント、Google Workspace ユーザーなど) 、グループの割り当て、範囲情報、関連付けられている

レポート	説明
	ロールなどの情報が含まれます。グループの割り当てがない場合、[Assigned to] (割り当て先) 列には、アイデンティティのメールアドレスの値が表示されます。
GCP ユーザー管理キー	(CSV)GCP アカウント内のすべてのユーザー管理キーの完全なリスト (プロジェクトごとにグループ化)。関連付けられているサービスアカウント、付与されるアクセス許可の深刻度レベル、キーが有効か無効かなどの詳細が含まれます。この情報は、永続的かつ静的な認証情報を環境から削除するのに役立ちます。

注意: 無効にされたコンプライアンス標準は、関連レポートに表示されません。詳細については、コンプライアンスを参照してください。

スケジュールされたレポートを表示および編集する

レポートをスケジュールした後、レポートのスケジュールと配信方法を表示および編集できます。

スケジュールされたレポートを表示および編集する方法

1. クラウドサイバーエクスポージャーコンソールで、**[レポート] > [スケジュールされたレポート]** をクリックします。
2. **[Scheduled Reports]** タブに移動します。
3. [組織] ドロップダウンで アカウント階層とフォルダー を選択し、レポートにアクセスするアカウント/IdP テナントのグループを定義します。
4. 必要に応じて、**[タイプ]** フィルターを使用してリストを絞り込み、関連するレポートを検索します。
5. **[Edit]** ボタンをクリックして、スケジュールされたレポートに変更を加えます。
6. **[Delete]** ボタンをクリックして、スケジュール済みのレポートを削除します。

履歴レポートへのアクセス

新しいレポートを作成するたびに (1 回限りのレポートでもスケジュールされたレポートでも)、レポートのコピーが将来の参照用に保存されます。

履歴レポートにアクセスする方法

1. クラウド サイバーエクスポージャーコンソールで、**[レポート] > [生成されたレポート]** をクリックします。
2. [組織] ドロップダウンで アカウント階層とフォルダー を選択し、レポートにアクセスするアカウント/IdP テナントのグループを定義します。
3. フィルターを使用して、レポートの作成 **時刻** と**レポートのタイプ** に応じてレポートのリストを絞り込みます。
4. **[レポートの表示]** をクリックして、履歴レポートのコピーをブラウザーに表示します。
5. **[ ]** ボタンをクリックして、レポートのコピーをダウンロードします。
6. **[Delete]** ボタンをクリックして、レポートのコピーを削除します。

その他のデータエクスポート方法

[レポート] ページは クラウド サイバーエクスポージャー コンソールでレポートを作成するための中心的なハブとして機能しますが、コンソールではその他の方法でもレポートを作成できます。

- 検出結果データのエクスポート。検出結果データをエクスポートして、環境内の検出結果のサマリーレポートを作成します。データは、その時点でテーブルに適用されているフィルターに従ってエクスポートされます。
- インベントリデータのエクスポート。[レポート] ページで作成できる *インベントリレポート* に加えて、特定のインベントリのビューに合わせてすべてのデータをリソースタイプ別に CSV 形式でエクスポートできます。たとえば、すべての Azure 仮想マシンのインベントリデータをエクスポートできます。
- コンプライアンスデータを CSV 形式でエクスポートします。[Reports] (レポート) ページから作成できるコンプライアンスレポートの PDF コピーに加えて、[Compliance] (コンプライアンス) ページから特定の標準に合わせてデータを CSV 形式でエクスポートすることもできます。

コンプライアンス

これは、コンプライアンスを監視するためのハウツーガイドです。概念の概要については、「 コンプライアンスの仕組み」を参照してください。

このセクションでは、Tenable One Cloud Exposure内のさまざまなコンプライアンス基準に対するクラウド環境の準拠状況をモニタリングおよび管理する実践的な手順について説明します。組み込みのコンプライアンス基準やカスタムのコンプライアンス基準を表示、整理、操作してコンプライアンス態勢を効果的に管理し、監査用の証拠を取得する方法を学習します。

コンプライアンス基準を表示する

環境内のすべてのコンプライアンス標準を確認し、以下を実行できます。

- 有効になっている標準を特定し、無関係な標準を標準を有効または無効にするする。
- 各標準について、高レベルのコンプライアンススコアが表示されます。
- ドリルダウンして、特定の標準に関する詳細情報を表示します。
- 特定の標準の標準をエクスポートするする

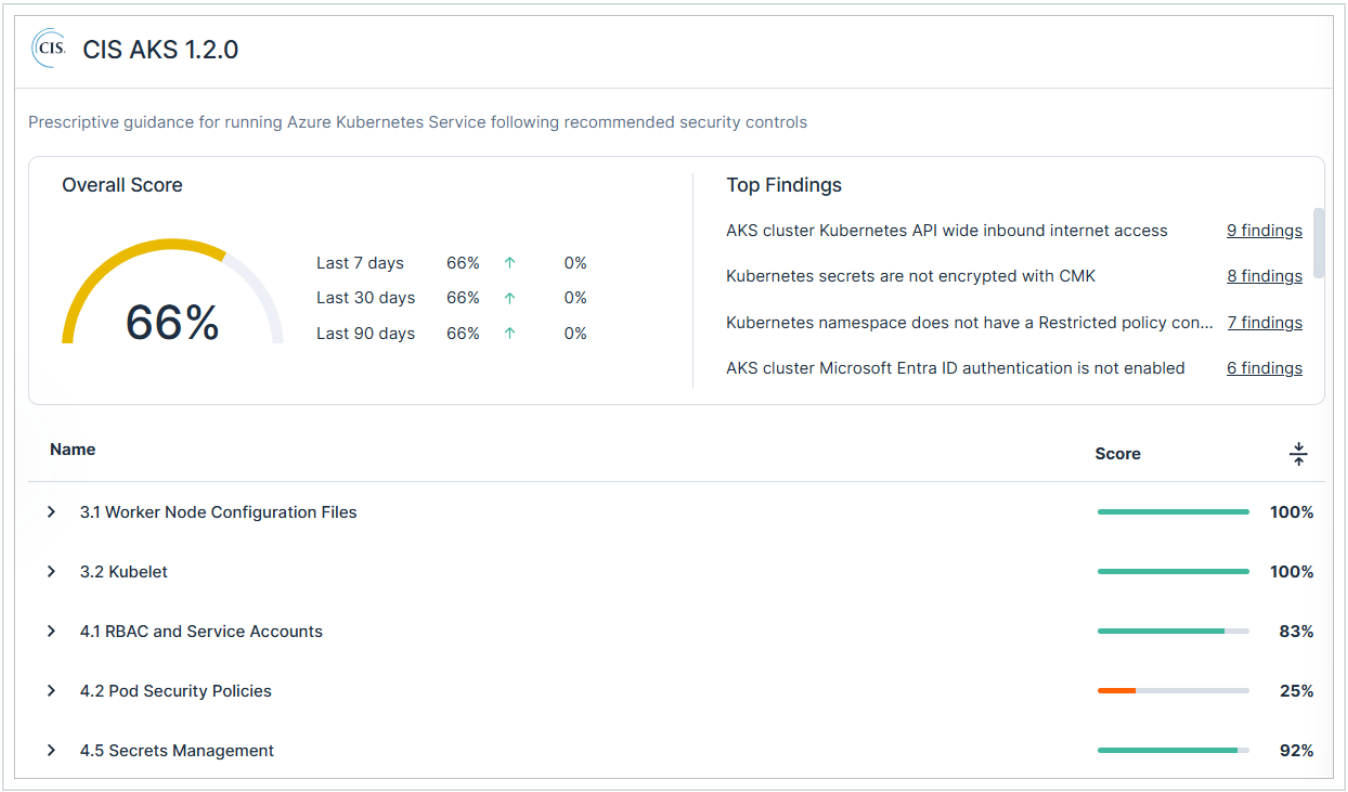
アカウントのコンプライアンスをモニタリングする方法

1. クラウドサイバーエクスポージャーコンソールで、**[コンプライアンス>レポート]** をクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択して、クラウドアカウントの特定のサブセットのコンプライアンスポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. クリックすると、**[組み込み]** または **[カスタム]** のいずれかの標準が表示されます。
4. 表示するデータの範囲を絞り込むには、**[名前]** や **[ステータス]** でテーブルを絞り込みます。
5. この表から、次の操作を行うことができます。
    - コンプライアンス標準のステータスと総合的なスコアを表示します。テーブルに表示されるデータの詳細については、コンプライアンステーブルデータ を参照してください。
    - 標準の標準の複製、標準を有効または無効にする、標準をエクスポートする
6. 標準をクリックすると標準での結果を表示する。

標準での結果を表示する

すべての標準について、マッピングされたポリシー、スキャンされたリソースの合計数の内訳、およびベンチマークに合格したリソースの割合を表示できます。

1. クラウドサイバーエクスポージャーコンソールで、**[コンプライアンス>レポート]** をクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択して、クラウドアカウントの特定のサブセットのコンプライアンスポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. クリックすると、**[組み込み]** または **[カスタム]** のいずれかの標準が表示されます。
4. 標準をクリックすると、その結果を含むスライド式パネルが開きます。



5. **[概要]** タブを開き、以下を表示します。
   - 標準の **総合スコア** (過去 7 日間、30 日間、90 日間)
   - **上位の検出結果**。標準のうち最も多くの検出結果をトリガーしたポリシー 10 個。
   - 標準の要件のリスト。スライドに表示されるデータの詳細については、「 スライド式パネルのデータ を参照してください。セクションをクリックすると、要件に対応するポリシーが表示されます。

- ポリシーをクリックすると **[Policies]** (ポリシー) ページが表示され、ポリシーに関する詳細の確認、ポリシーの有効化と無効化、ポリシーからリソースを除外することができます。
- **[不合格のリソース]** 列のエントリをクリックすると、リソースのリストが表示されます。

6. **[評価]** タブを開くと、合格した評価と除外された評価など、このビューのスコアの背後にあるすべてのポリシー評価が表示されます。「コンプライアンス評価を表示するを参照してください。
7. **[↕展開]** をクリックすると、標準に対応するすべてのポリシーが表示されます。
8. クラウドの検出結果からコンプライアンス情報を表示することもできます。
   - 特定の検出結果に対応するすべての標準を表示します。
   - 検出結果の表を特定の標準でフィルタリングし、その標準に関連するすべての課題を特定して分離します。

コンプライアンス評価を表示する

評価とは、ある時点で1つのリソースに対して評価された1つのポリシーの記録です。クラウドサイバーエクスポージャーは、リソースが合格、不合格、除外されたかどうかに関係なく、すべての評価を保持するため、検出結果がないからコントロールを推測するのではなく、コントロールが評価されたことを示すタイムスタンプ付きの証明を生成できます。

[Assessments] タブを使用して以下を行います。

- リソースレベルおよびセクションレベルのデータを可視化し、それに基づいて行動します。
- 監査人または調達レビュー担当者に、合格した統制の日付入りの記録を手渡します。
- 各ポリシーを開かずに、失敗したセクションの背後にあるリソースを見つけます。
- 想定されるリソースに除外が適用されていることを確認します。

標準のコンプライアンス評価を表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[コンプライアンス>レポート]** をクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択して、クラウドアカウントの特定のサブセットのコンプライアンスポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。

3. クリックすると、**[組み込み]** または **[カスタム]** のいずれかの標準が表示されます。
4. 基準をクリックし、**[評価]** タブを選択します。表に、標準に関するすべての評価が表示されます。
5. (オプション)**[エクスポート]** をクリックして、以前のすべての評価の CSV をエクスポートし、コンプライアンス監査の証明を生成します。

評価データをスケジュールに従って提供したり、外部のステークホルダーに渡したりするには、**コンプライアンス評価** レポートを作成します。

標準を有効または無効にする

組み込みのコンプライアンス標準を有効または無効にできます。標準を無効にすると、クラウド サイバーエクスポージャー コンソール全体の関連する場所からその標準が削除されます。たとえば、[Dashboard Compliance] (ダッシュボードのコンプライアンス) ウィジェット、レポート、関連するフィルターから削除されます。カスタム標準は無効にできません。標準を無効にするには、組織の範囲に対するアクセス許可があり、それを選択する必要があります。

標準を有効または無効にする方法

1. クラウド サイバーエクスポージャーコンソールで、**[コンプライアンス>レポート]** をクリックします。
2. クリックすると、**[Built-in standards] (ビルト イン** 標準) が表示されます。
3. 関連する標準の横にある三点リーダーをクリックし、**[Enable]** または **[Disable]** のいずれかをクリックします。

標準をエクスポートする

標準のデータをエクスポートすると、標準にマッピングされたすべてのポリシーの詳細、ポリシーによって評価されたリソースの総数の内訳、ポリシーベンチマークに合格または不合格になったリソースの割合 (深刻度別にグループ化) が記載された CSV または PDF サマリーレポートが生成されます。[Report] (レポート) ページで、コンプライアンス標準に関するスケジュールされたレポートを生成することもできます。

- **CSV**。編集可能な作業ドキュメントとして使用したり、他のユーザーとの共同作業やフィードバックを受け取ったりするのに適しています。

- **PDF**です。データを可視化して、経営幹部やその他の関連するステークホルダーと共有するのに最適です。

エクスポートされた標準には、ポリシーとリソース数がまとめられます。合格したものも含めて、すべての個別の評価の行レベルのレコードについては、レポートの作成 。

標準をエクスポートする方法

1. クラウドサイバーエクスポージャーコンソールで、**[コンプライアンス>レポート]** をクリックします。
2. [Organization] (組織) ドロップダウンで アカウント階層とフォルダー を選択して、クラウドアカウントの特定のサブセットのコンプライアンスポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. クリックすると、**[組み込み]** または **[カスタム]** のいずれかの標準が表示されます。
4. テーブル内の関連する標準の横にある三点リーダーをクリックし、**[エクスポート]** をクリックして **CSV** または **PDF** を選択します。

コンプライアンス態勢の改善

関連する検出結果を修正してコンプライアンス態勢を改善します。

1. コンプライアンス基準を表示する 、コンプライアンスチェックで不合格となったリソースを特定します。
2. 不合格のリソースについて開かれた検出結果を特定します。コンプライアンス標準のビューから、次のいずれかを実行します。
    - **ポリシー**をクリックします。
        - ポリシーのページで、**[検出結果]** リンクをクリックします。
    - **不合格のリソース**をクリックします。
        1. 特定のリソースを検索または選択します。
        2. リソースページで **[Findings] (検出結果**) タブをクリックし、次に関連する検出結果をクリックします。

3. 検出結果を修正します:
    1. 関連する検出結果を開きます。
    2. **[修正]** タブをクリックします。
    3. 検出結果を手動または自動で修正します。詳細については クラウドの検出結果 。

カスタム標準の追加

規格一覧を使用するだけでなく、独自の標準を作成して、組織の目標に沿った特定のポリシーセットへの準拠状況をモニタリングできます。これらの標準は、セクションとサブセクションの複数のレイヤーを含む階層型にし、それぞれを特定のポリシーにマッピングする (対応させる) ことができます。たとえば、次のような特定のカスタムポリシーを強制する標準を作成できます。

- 組織固有のコンプライアンスルールをモニタリングする。
- 特定の課題セットに対処する組織のプロジェクトを追跡する。

重要: Tenable の組み込みコンプライアンスフレームワークは、特定の標準に対する完全なコンプライアンスを保証するものではありません。組織には、評価が法的要件および規制要件を確実に満たすようにする責任があります。コンプライアンスのニーズは製品、ドメイン、ビジネスプラクティスによって異なるため、関連する カスタム標準の追加 ことをお勧めします (標準の複製 することで、組み込み標準をベースにすることができます)。

カスタム標準を追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[コンプライアンス>レポート]** をクリックします。
2. 左側の [Organization] (組織) ツリーで アカウント階層とフォルダー を選択して、クラウドアカウントの特定のサブセットのコンプライアンスポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. 次のいずれかを選択します。
    - **既存の標準をベースラインとして使用する**: 標準の複製 。
    - **ゼロから始める**:
        1. **[カスタム]** タブをクリックします。
        2. **[Add Custom Compliance]** ボタンをクリックします。

4. **[編集]** をクリックし、標準の **[名前]** と **[説明]** (オプション) を入力します。
5. 最上位のセクションを追加する場合
    1. **[セクションの追加]** をクリックします。
    2. セクションの **[名前]** と **[説明]** (オプション) を入力し、**[追加]** をクリックします。
    3. 追加するセクションごとにこの手順を繰り返します。
6. ポリシーをセクションに追加する場合
    1. セクションにカーソルを合わせてプラス [+] アイコンをクリックし、**[ポリシーの追加]** をクリックします。
    2. セクションにマッピングする個別のポリシーを 1 つ以上選択します。ポリシーは、プラットフォーム、ポリシー (名)、カテゴリ、深刻度でフィルタリングできます。
    3. **[追加]** をクリックします。
7. サブセクションを追加します:
    1. サブセクションを追加するセクションにカーソルを合わせ、プラス [+] アイコンをクリックして、**[セクションを追加]** をクリックします。
    2. セクションの **[名前]** と **[説明]** (オプション) を入力し、**[追加]** をクリックします。
8. セクションやサブセクションを編集するには、編集アイコン をクリックします。
9. セクションやサブセクションを削除するには、[削除] アイコン をクリックします。
10. ポリシーを別のセクションやサブセクションに移動させるには、ポリシーを選択してページの下部にある **[移動]** をクリックします。
11. 完了したら、**[作成]** をクリックします。

標準の複製

任意の標準 (組み込みまたはカスタム) を複製して、独自の標準を作成するためのベースラインとして使用できます。

標準を複製する方法

1. クラウドサイバーエクスポージャーコンソールで、**[コンプライアンス>レポート]** をクリックします。
2. 左側の [Organization] (組織) ツリーで アカウント階層とフォルダー を選択して、クラウドアカウントの特定のサブセットのコンプライアンスポリシーを表示および管理します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. クリックすると、**[組み込み]** または **[カスタム]** のいずれかの標準が表示されます。
4. テーブル内の関連する標準の横にある三点リーダーをクリックし、**[複製]** をクリックします。[Add Custom Compliance] (カスタムコンプライアンスの追加) フォームが開きます。
5. 必要に応じて、コンプライアンス標準を変更します。カスタム カスタム標準の追加 を参照してください。

参照: コンプライアンスデータ

このセクションでは、クラウドサイバーエクスポージャーコンソールのコンプライアンス機能内に表示されるデータに関する詳細な参照情報を提供します。サポートされているコンプライアンス基準の包括的なリストと、表およびスライド式パネルにあるさまざまな列とフィールドの説明が含まれています。

規格一覧

以下の標準は、標準 クラウドサイバーエクスポージャー 用意されています。

Standard	説明
Tenable のベストプラクティス	Tenableが厳選したポリシーで環境を保護します。この標準は、多くのお客様に使用されるポリシーを含んでおり、クラウドセキュリティ問題を解決しているTenable の幅広い経験に基づいています。
AWS Foundational Security Best Practices v1.0.0 (FSBP)	AWS アカウントとリソースがセキュリティのベストプラクティスから逸脱していることを検出するコントロールセットです。

Standard	説明
AWS Well Architected	6 つの柱 (オペレーショナルエクセレンス、セキュリティ、信頼性、パフォーマンス効率、コスト最適化、持続可能性) を中心に構築されたフレームワークで、クラウドでワークロードを設計および実行するための主要な概念、設計原則、アーキテクチャのベストプラクティスを説明しています。
CIS AKS 1.2.0 および 1.8.0	推奨されるセキュリティ制御に従って Azure Kubernetes Services を実行するための規範的ガイダンス。
CIS AWS 6.0.0、5.0.0、4.0.0、3.0.0、2.0.0	Amazon Web Services クラウドプロバイダー向けの客観的でコンセンサスに基づいたセキュリティベンチマーク。AWS サービスのサブセットにセキュリティオプションを設定するための規範的なガイダンスを提供します。基礎的で、テスト可能な、アーキテクチャにとらわれない設定に重点を置いています。
CIS Azure 6.0.0、5.0.0、4.0.0、3.0.0、2.0.0	Microsoft Azure クラウドプロバイダー向けの客観的でコンセンサスに基づいたセキュリティベンチマーク。
CIS EKS 1.2.0 および 1.8.0	推奨されるセキュリティコントロールに従って Elastic Kubernetes Service を実行するための規範的ガイダンス。
CIS GCP 4.0.0、3.0.0、2.0.0、1.3.0	GCP 上のインフラストラクチャを設計する際の重要なセキュリティの考慮事項を提供する、客観的でコンセンサスに基づいた Google Cloud Platform のセキュリティ ベンチマーク。このベンチマークのリリースで提供される推奨事項のほとんどは、個々のプロジェクトレベルでのセキュリティの考慮事項のみを対象としており、組織レベルでの考慮事項は対象としていません。
CIS GKE 1.3.0 および 1.8.0	推奨されるセキュリティコントロールに従って Google Kubernetes Engine を実行するための規範的ガイダンス。
CIS Kubernetes 2.0.1、1.12.0、	Kubernetes の安全な設定ポスチャーを確立するための規範的ガイダンス。

Standard	説明
1.8.0	
CIS OCI 2.0.0	Oracle Cloud Infrastructureクラウド・プロバイダ向けの客観的でコンセンサスに基づいたセキュリティ・ガイドライン。
CIS OKE 1.5	推奨されるセキュリティ制御に従ってOracle Kubernetes Engineを実行するための規範的ガイダンス。
CIS Red Hat OpenShift Container Platform 1.8.0 および v1.5.0	OpenShift の安全な設定ポスチャーを確立するための規範的ガイダンス
CSA CCM 4.0.2	クラウドコンピューティング用のセキュリティコントロールフレームワーク。クラウドセキュリティアライアンス(CSA)のベストプラクティスに準拠しており、クラウドセキュリティとプライバシーのデファクトスタンダードと見なされています。
Essential Eight	サイバー攻撃に対するレジリエンスを強化し、オーストラリア政府の基準へのコンプライアンスを確保するために組織が実装する必要がある、一連の重要な軽減戦略とコントロールを提供するフレームワークです。
GDPR	欧州連合のデータ保護、セキュリティ、コンプライアンスに関する基準を強化し、統一する一連の厳格な要件。GDPR では、企業は個人データを処理する前に、対象者に明示的な許可を求める必要があります。
HIPAA	保護対象医療情報 (PHI) のセキュリティとプライバシーを保護するために使用される一連のルール。これは通常、医療提供者および医療関連企業が、患者およびその正式な代理人以外の者に、患者の同意なしに保護された情報を開示することを禁止しています。
ISMS-P (韓国)	公的機関向け情報セキュリティマネジメントシステム (ISMS-P) は、公的機関

Standard	説明
	が管理する情報のセキュリティを強化するために韓国で導入されたフレームワークです。その主な目的は、機密情報を不正アクセス、改ざん、開示、破壊から保護することです。
ISO 27001	情報セキュリティの管理方法に関する要件を規定する標準。これにより、あらゆる種類の組織が、財務情報、知的財産、従業員の詳細、サードパーティから委託された情報などの資産のセキュリティを管理できるようになります。情報セキュリティマネジメントシステムを確立、導入、運用、モニタリング、レビュー、維持、改善するためのモデルを提供します。
LGPD (ブラジル)	ブラジルのデータ保護法は、個人データの処理を規制し、プライバシーとデータ保護に対する個人の権利を保証することを目的としています。
Microsoft クラウドセキュリティベンチマーク v1	Azure とマルチクラウド環境のワークロード、データ、サービスのセキュリティ向上に役立つ規範的なベスト プラクティスと推奨事項。
MITRE ATT&CK v13	脅威ハンター、ディフェンダー、レッドチームのために攻撃の分類、攻撃の属性と目的の特定、組織のリスクの評価を支援するために設計された戦術と手法のフレームワーク。
NIS2 指令	高い共通レベルのセキュリティを確立することにより、欧州連合全体のサイバーセキュリティを強化するために設計されたフレームワーク。これにより、対象となるエンティティの範囲が拡大され、より広範囲の不可欠かつ重要な業界が含まれるようになります。
NIST 800-171 Rev2	管理対象非分類情報 (CUI) が非連邦のシステムおよび組織に存在する場合、その機密性を保護するために推奨されるセキュリティ要件を各機関に提供します。
NIST 800-53 Rev5	組織の運営と資産、個人、他の組織、および国家を、敵対的攻撃、ヒューマンエラー、自然災害、構造的障害、外国諜報機関、プライバシーリスクなど、

Standard	説明
	さまざまな脅威やリスクから保護するための情報システムおよび組織のセキュリティおよびプライバシー管理。 注:NIST 800-171の対象が非連邦ネットワークであるのに対して、NIST 800-53はすべての連邦組織に適用されます。
NIST CSF 2.0 および 1.1	サイバーセキュリティフレームワーク (CSF) は、組織がサイバーセキュリティリスクをより適切に管理して軽減するための既存の標準、ガイドライン、プラクティスに基づく自発的なガイダンスです。組織がリスクを管理して低減することに役立つだけではなく、組織内外のステークホルダー間においてリスクやサイバーセキュリティ管理に関するコミュニケーションを促進するように設計されています。
NIST SP 800-190	コンテナの一般的な実行時に存在するコンポーネント (イメージ、レジストリ、オーケストレータ、コンテナ、ホスト OS) に関するセキュリティコントロールと対策。
NYDFS 23 NYCRR 500	ニューヨーク州金融サービス局 (NYDFS) が公布した法律で、Web サイトやアプリを保護するために最適なデータセキュリティ基準の施行を義務付けています。企業は、すべてのセキュリティプロセスを評価し、発見された脆弱性を軽減するための計画を実施することが義務付けられています。この規制は、ニューヨーク州に拠点を置き、銀行や保険会社などの金融サービスを提供するすべての企業に適用されます。
PCI DSS 4.0	カード会員データのセキュリティを促進および強化し、グローバルなレベルで一貫したデータセキュリティ対策を広く採用するために策定された一連の要件。この要件は、カード会員データを保存、処理、送信するすべての事業体に適用されます。また、これらの取引に使用されるアプリケーションやデバイスのソフトウェア開発者および製造業者に対する要件も含まれます。
SOC2 Type II	セキュリティ、可用性、処理の整合性、機密性、プライバシーに関連するサービス組織におけるコントロールセット。これらのコントロールを組み合わせることで、データを保護するためのフレームワークが提供されます。組織は SOC 2 を

Standard	説明
	使用して現在のセキュリティポスチャーを測定し、SOC 2 レポートで概説されているベストプラクティスを通じてサイバーセキュリティを改善する機会を特定します。

コンプライアンステーブルデータ

[コンプライアンス] ページの表には、次のデータが表示されます。

縦棒	説明
名前	コンプライアンス標準の名前。
ステータス	組み込み標準が有効になっているか無効になっているか。
スコア	ポリシーのベンチマークに合格したリソースの割合。
三点リーダーアイコン **エクスポート**	コンプライアンス標準のレポートを生成します。標準の標準をエクスポートするを参照してください。
三点リーダーアイコン **有効化 / 無効化**	組み込み標準を標準を有効または無効にする。標準を無効にすると、クラウドサイバーエクスポージャーコンソール全体の関連する場所からその標準が削除されます。たとえば、[Dashboard Compliance] (ダッシュボードのコンプライアンス) ウィジェット、レポート、関連するフィルターから削除されます。カスタム標準は無効にできません。標準を無効にするには、次の要件を満たす必要があります。 • 左側のツリーで**組織**の範囲が表示されている (表示されていない場合は、**[ステータス]** 列と無効になっている標準が表示されません)

縦棒	説明
	• の範囲全体に対するアクセス許可を持っている
三点リーダーアイコン **複製**	任意の標準 (組み込みまたはカスタム) を 標準の複製 して、独自の標準を作成するためのベースラインとして使用できます。

スライド式パネルのデータ

特定の規格のスライド式パネルには、次のデータが表示されます。

縦棒	説明
名前	コンプライアンス標準の名前。
プラットフォーム	クラウドサービスプロバイダーまたはアイデンティティプロバイダー。
ポリシー	特定の要件に対応するポリシーの名前。名前をクリックして [Policies] (ポリシー) ページに移動し、トリガーされた検出結果のリストなど、ポリシーに関する詳細情報を確認できます。
失敗したリソース	ポリシーのベンチマークに合格できなかったリソースの数。リンクをクリックすると、リソースの一覧が表示されます。
スキャン済みリソース	ポリシーによってチェックされるリソースの総数。
スコア	ポリシーのベンチマークに合格したリソースの割合。「 コンプライアンススコアを理解する を参照してください。

設定

アクセス管理

ユーザーとグループ

新しいユーザーまたはグループを追加し、Tenable One Cloud Exposureコンソール内で特定のアクセス許可を割り当てます。

> **注意:** API を介してユーザーを追加することもできます。

Tenable One のお客様:

- Tenable 管理者ロールを持つ1人のユーザーには、クラウドサイバーエクスポージャーコンソールでそのようなアクセス許可が明示的に付与されていない場合でも、組織全体へのアクセス権を持つ管理者ロールのアクセス許可がクラウドサイバーエクスポージャー内で自動的に割り当てられます。
- 管理者以外のユーザー/グループがクラウドサイバーエクスポージャーコンソールにアクセスできるようにするには、まずTenable Oneでユーザーまたはグループを定義してアクセス権を付与してから、クラウドサイバーエクスポージャーコンソール新しいユーザーの追加する必要があります。
- Tenable 新しいユーザーの追加 新しいグループを追加するを追加する際に、任意のロールを持つ1人のユーザーに希望する範囲を割り当てることで、アカウント階層とフォルダーでクラウドサイバーエクスポージャーへのアクセス権を付与できます。

新しいユーザーまたはグループは、ユーザーがクラウドサイバーエクスポージャーでアクセスできるアカウントを定義する特定の範囲内で追加されます。たとえば、ユーザーを組織全体 (すべてのアカウント) に追加することも、アカウントのサブセットに追加することもできます。詳細については、アカウント階層とフォルダーを参照してください。

個別に追加したユーザーが、追加したグループのメンバーでもある場合、そのユーザーには、ユーザー/グループに割り当てられたロール/範囲のアクセス権のうち、最高レベルのアクセス権が付与されます (それらのアクセス権が異なる場合)。たとえば、次の状況です。

- ユーザー X: ロール = 管理者。範囲 = すべての AWS アカウント
- グループ Y (ユーザー X がメンバー): ロール = コラボレータ。範囲 = 組織全体

ユーザー X は、組織全体に対する管理者のアクセス許可を持ちます。

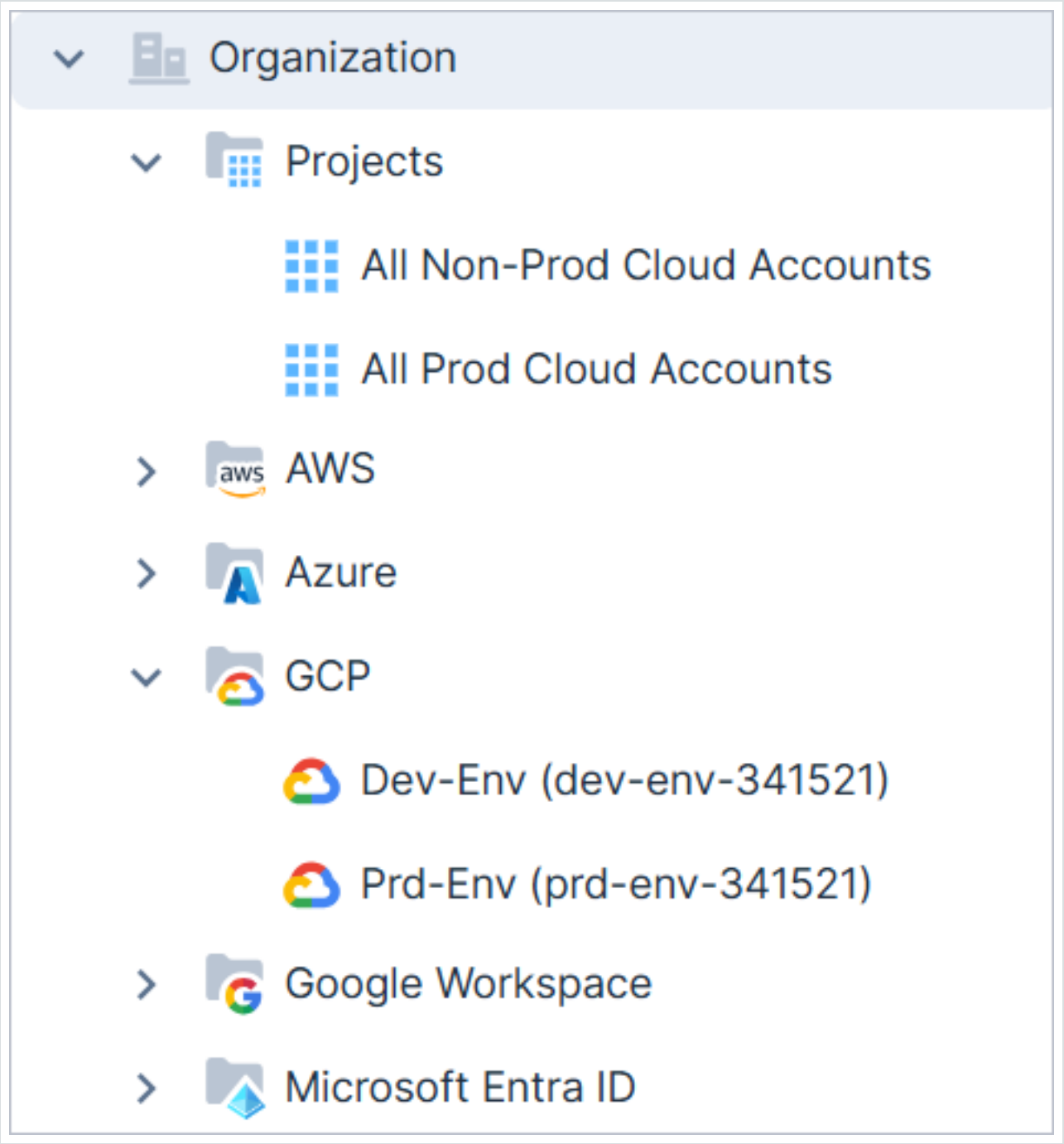
> **注意:** クラウド サイバーエクスポージャー へのログインに SSO が構成されている場合、追加するユーザーのメールアドレスは組織内の既存のユーザーのものである必要があります。

新しいユーザーの追加

> **注意: Tenable Oneのお客様**: ユーザーが クラウド サイバーエクスポージャー コンソールにアクセスできるようにするには、まずTenable Oneでユーザーを定義してアクセス権を付与してから、クラウド サイバーエクスポージャー コンソールに追加する必要があります。

新しいユーザーを追加する方法

1. **[Settings > User Management]** に移動します。
2. ページ上部にある組織ツリーで、ユーザー アカウント階層とフォルダー を選択します。



範囲は以下のいずれかになります。

1. 組織全体 (クラウドサイバーエクスポージャーにオンボーディングされたすべてのアカウント)。
2. アカウントのグループ。たとえば、特定のクラウドプロバイダー (すべての AWS アカウント) またはアイデンティティプロバイダー (すべての Microsoft Entra テナント) に属するすべてのアカウント、

あるいは特定のクラウドプロバイダー内のアカウントのグループ (アカウント階層とフォルダー別にグループ化) などです。

3. 特定のアカウントやアイデンティティプロバイダーのテナント。
4. プロジェクトまたはプロジェクトのフォルダー。
5. すべての IaC 組織、または個々のリポジトリのサブセット。これにより、特定の範囲のコードスキャン結果を表示するためのアクセスが付与されます。

> **注意:** IaC の範囲内にユーザーを追加すると、ユーザーには IaC 関連の機能へのアクセス権 **のみ** が付与されます。このようなユーザーは、クラウドリソースや、ダッシュボードなどのその他の機能にはアクセスできません。IaC 階層は、Tenable RBAC (ユーザー/グループの追加) のコンテキスト内でのみ使用でき、他のコンテキスト (ポリシーやレポートなど) では表示されません。

親レベルで作成されたユーザーが子アカウントに継承される方法の詳細については、「 継承されたユーザー 」を参照してください。

3. **[ロールの割り当てを追加]** をクリックし、**[プリンシパル]** で **[ユーザー]** を選択します。
4. ボックスで、ユーザーのメールアドレスを検索して選択します。

   クラウドサイバーエクスポージャー へのログインに SSO が構成されている場合、追加するユーザーのメールアドレスは組織内の既存のユーザーのものである必要があります。
5. ユーザーに **ロール** を割り当て、**[保存]** (Save) をクリックします。
   1. **閲覧者** - クラウドサイバーエクスポージャー へのアクセスを表示します ([管理] タブを除く)
   2. **Collaborator (コラボレータ)** - すべての Viewer (閲覧者) のアクセス許可に加えて、リソースを分類し検出結果に対応することが可能。
   3. 管理者 **- すべての**コラボレータのアクセス許可に加えて、クラウドサイバーエクスポージャー管理 (アカウントの追加、設定の構成、監査証跡の表示) が可能です。
   4. **JIT 管理者** - JIT 使用資格を管理し、JIT ポータル経由で JIT 監査証跡を表示。

   カスタムロールは、**[ロール]** ドロップダウンボックスにも表示されます。カスタムロールの作成と管理の詳細については、「 ロールを参照してください。
   各組み込みロールによって付与されるアクセス許可の詳細なリストについては、「 ロールとアクセス許可 」を参照してください。
6. ユーザーのアクセス許可レベルを変更する必要がある場合は、ユーザーの横にある [編集] アイコン ✎ を選択し、新しいロールを選択してから、**[保存]** を選択します。

> **注意:** 自分のロールを [Administrator] (管理者) から [Collaborator] (コラボレータ) または [Viewer] (閲覧者) に変更すると、[User Management] (ユーザー管理) にアクセスしてロールを編集することができなくなります。

新しいグループを追加する

> **注意: Tenable Oneのお客様**: グループメンバーがクラウドサイバーエクスポージャーコンソールにアクセスできるようにするには、まずTenable Oneで関連グループを定義してから、クラウドサイバーエクスポージャーコンソールに追加する必要があります。

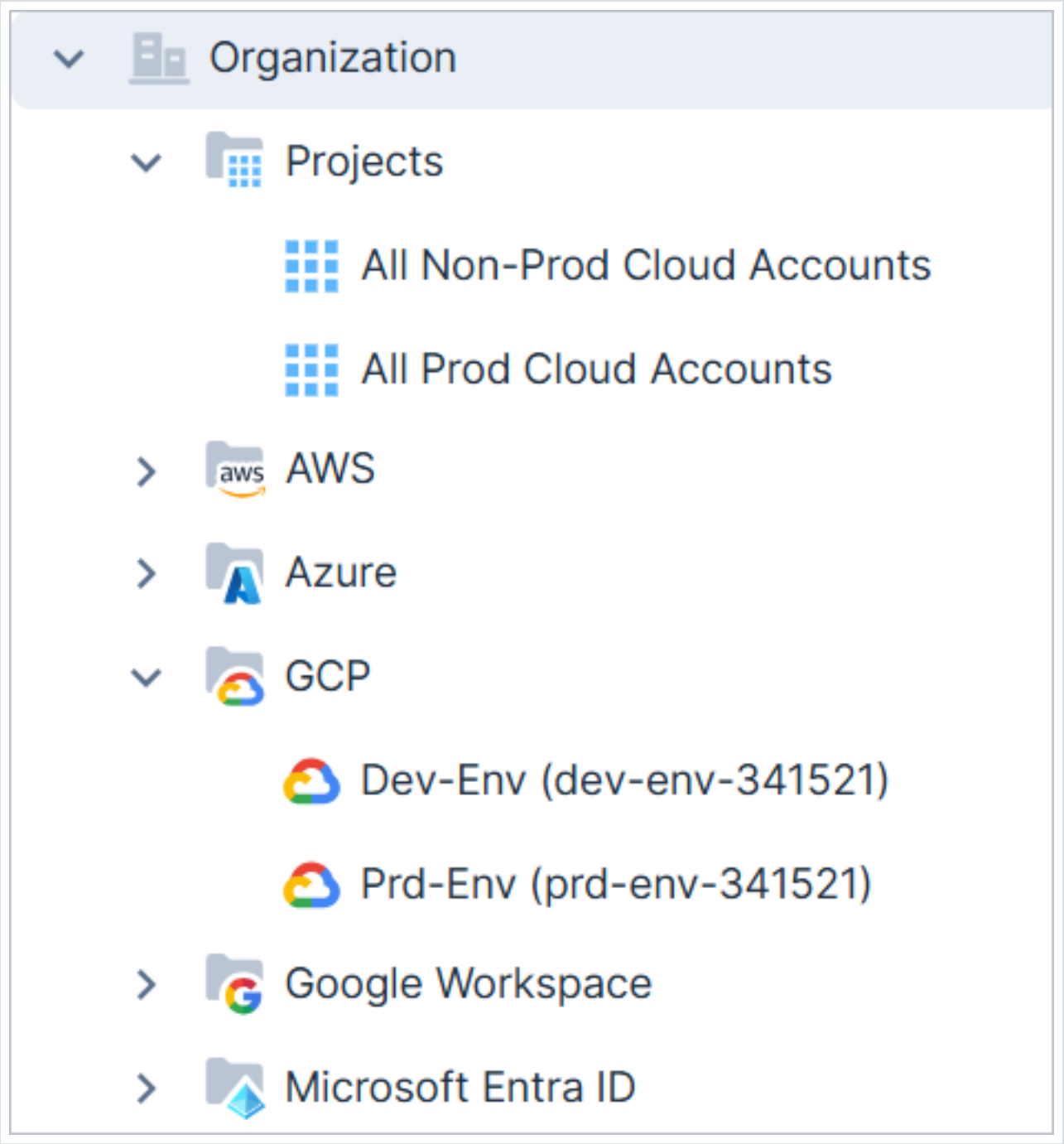
前提条件

クラウドサイバーエクスポージャーコンソールで新しいグループを追加する前に、次の手順に従ってシングルシングルサインオンします。

- IdPとTenableの間に信頼を確立する
- IdPがグループのクレームをクラウドサイバーエクスポージャーに送信するようにグループマッピングを設定する

新しいグループを追加する方法

1. **[Settings > User Management]** に移動します。
2. 左側の組織ツリーで アカウントの範囲 。



範囲は以下のいずれかになります。

1. 組織全体 (クラウドサイバーエクスポージャーにオンボーディングされたすべてのアカウント)。
2. アカウントのグループ。たとえば、特定のクラウドプロバイダー (すべての AWS アカウント) またはアイデンティティプロバイダー (すべての Microsoft Entra テナント) に属するすべてのアカウント、

あるいは特定のクラウドプロバイダー内のアカウントのグループ (アカウントフォルダーの作成別にグループ化) などです。

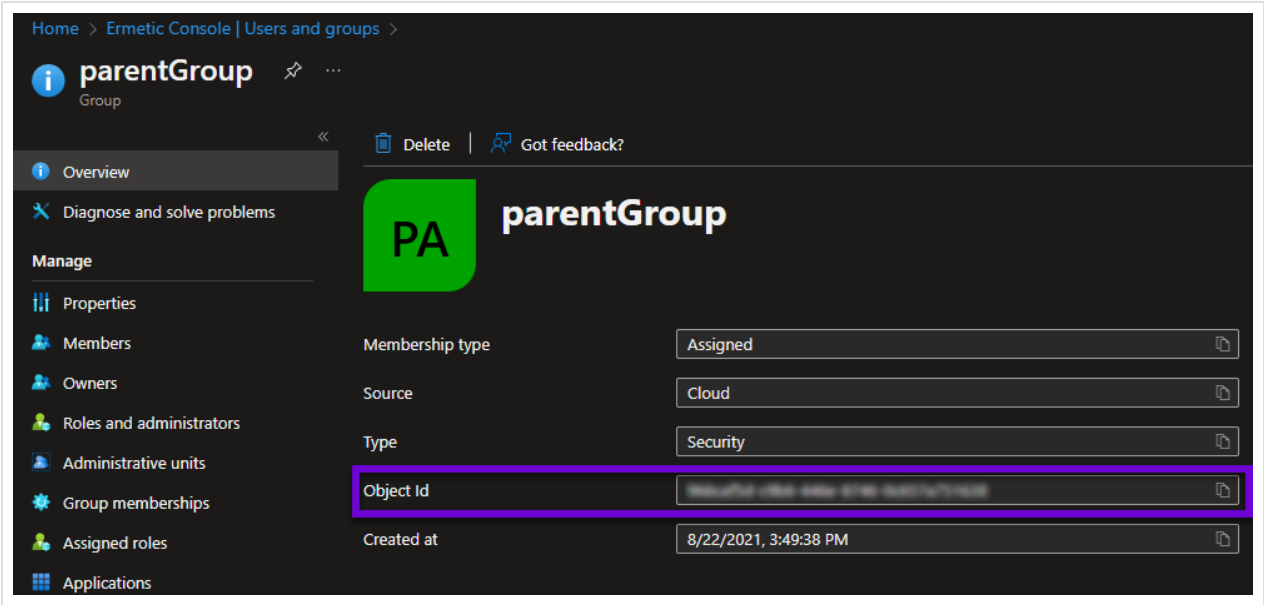
3. 特定のアカウントやアイデンティティプロバイダーのテナント。
4. プロジェクトまたはプロジェクトのフォルダー。
5. すべての IaC 組織、または個々のリポジトリのサブセット。これにより、特定の範囲のコードスキャン結果を表示するためのアクセスが付与されます。

> **注意:** IaC の範囲内にユーザーを追加すると、ユーザーには IaC 関連の機能へのアクセス権**のみ**が付与されます。このようなユーザーは、クラウドリソースや、ダッシュボードなどのその他の機能にはアクセスできません。IaC 階層は、Tenable RBAC (ユーザー/グループの追加) のコンテキスト内でのみ使用でき、他のコンテキスト (ポリシーやレポートなど) では表示されません。

親レベルで作成されたユーザーが子アカウントに継承される方法の詳細については、「継承されたユーザー」を参照してください。

3. **[ロールの割り当てを追加]** をクリックし、**[プリンシパル]** で以下を選択します。
   - **グループ**。このオプションは、アイデンティティプロバイダーで定義されたグループに対して使用します。
   - **Microsoft Entra ID グループ**(Microsoft Entra ID 統合が設定されている場合にのみ利用可能)。Microsoft Entra ID グループにはグループ名に加えてグループ ID が必要なため、このオプションを選択するのは、次のとおりです。
4. グループ情報を入力します。フィールドは、ステップ 3 で選択したオプションによって異なります。
   - **グループ名**。**[グループ]** オプションを使用して追加されたグループの場合、これはアイデンティティプロバイダーで定義されているグループ名になります。**[Microsoft Entra ID グループ]** オプションを使用して追加したグループの場合、この名前がクラウドサイバーエクスポージャーコンソールに表示されます。
   - **グループ ID** (**Microsoft Entra ID グループ** のみ) 追加するグループの Microsoft Entra ID グ

ループ **オブジェクト ID** (GUID)。



5. グループに**ロール**を割り当て、[保存] (**Save**) をクリックします。
    1. **閲覧者** - クラウド サイバーエクスポージャー へのアクセスを表示します ([管理] タブを除く)
    2. **Collaborator (コラボレータ)** - すべての Viewer (閲覧者) のアクセス許可に加えて、リソースを分類し検出結果に対応することが可能。
    3. 管理者 - **すべての**コラボレータのアクセス許可に加えて、クラウド サイバーエクスポージャー管理 (アカウントの追加、設定の構成、監査証跡の表示) が可能です。
    4. **JIT 管理者** - JIT 使用資格を管理し、JIT 監査証跡を表示。

    カスタムロールは、**[ロール]**ドロップダウンボックスにも表示されます。カスタムロールの作成と管理の詳細については、「 ロールを参照してください。
    各ロールに付与されるアクセス許可の詳細なリストについては、「 ロールとアクセス許可」を参照してください。
6. グループのアクセス許可レベルを変更する必要がある場合は、グループの横にある [編集] アイコン を選択し、新しいロールを選択してから、**[保存]** を選択します。

> **注意:** 自分のロールを [Administrator] (管理者) から [Collaborator] (コラボレータ) または [Viewer] (閲覧者) に変更すると、[User Management] (ユーザー管理) にアクセスしてロールを編集することができなくなります。

継承されたユーザー

組織レベルまたはアカウントのグループ内で作成されたユーザーは、今後作成される子アカウントを含め、すべての子アカウントに継承されます。たとえば、組織レベルで「ユーザー X」を作成し、これに [Collaborator] (コラボレータ) ロールを割り当てると、同じロールを持つ「ユーザー X」が存在し、すべての子アカウントに対するアクセス許可を持つことになります。後から組織に新しいアカウントを追加すると、「ユーザー X」には新しいアカウントに対するアクセス許可も持つことになります。

[User Management] (ユーザー管理) テーブルの子アカウントの下に「ユーザー X」が表示され、ロール列にユーザーが継承されたことが示されます。

子アカウント内では、継承されたユーザーのロールを編集してユーザーのアクセス許可レベルを上げることのみを実行できます。たとえば、[Collaborator] (コラボレータ) ロールを持つユーザーを [Administrator] (管理者) に変更することはできますが、[Viewer] (閲覧者) に変更することはできません。同様に、親アカウント/グループ内で [Administrator] (管理者) ロールを付与されたユーザーのロールを変更することはできません。詳細については、ロールとアクセス許可を参照してください。

組み込みのロールとアクセス許可

ユーザー/グループに割り当てることができる組み込みロールは 3 つあります。

- **ビューワー**
- **コラボレータ**
- **Administrator (管理者)**

さらに、**所有者** ロールは、常にクラウドサイバーエクスポージャー環境の所有と管理を担当する 1 人の担当者により明確かつ明確に説明できるようにするために存在します。

- 所有者ロールには、管理者と同じアクセス許可があります。
- 一度に 1 人ユーザーのみが所有者ロールを持つことができます。
- このロールを持つユーザーは、所有権を別のユーザーに譲渡できます。

管理者は、モジュールレベルの詳細なアクセス許可を持つカスタムロールを作成することもできます。詳細については、「 ロール を参照してください。

各ロールは、クラウドサイバーエクスポージャーコンソール内で異なるレベルのアクセス権を提供します。次の表に、各ロールによって付与されるアクセス許可の詳細を示します。

アクセス許可	サブアクセス許可	ビューワー	コラボレータ	Administrator (管理者)	JIT 管理者
ダッシュボード					
	ビュー	✓	✓	✓	–
	管理 – プライベートダッシュボード	✓	✓	✓	–
	管理 - 公開ダッシュボード	–	✓	✓	–
インベントリ					
	ビュー	✓	✓	✓	–
	管理	–	✓	✓	–
ワークロードリソース					
	今すぐスキャン	–	✓	✓	–
データリソース					
	スキャン	–	✓	✓	–
イベント					
	ビュー	✓	✓	✓	–
CI/CD スキャ					

アクセス許可	サブアクセス許可	ビューワー	コラボレータ	Administrator (管理者)	JIT 管理者
ン					
	ビュー	✓	✓	✓	–
クエリ					
	ビュー	✓	✓	✓	–
	管理 - プライベートクエリ	✓	✓	✓	–
	管理 - パブリッククエリ	–	✓	✓	–
リスク					
	ビュー	✓	✓	✓	–
	管理 – コメント	–	✓	✓	–
	管理 – ステータス	–	✓	✓	–
	管理 – スター	–	✓	✓	–
	管理 – 修正	–	✓	✓	–
	管理 – 共有	–	✓	✓	–
脅威					
	ビュー	✓	✓	✓	–
	管理 – コメント	–	✓	✓	–
	管理 – ステータスの変更	–	✓	✓	–

アクセス許可	サブアクセス許可	ビューワー	コラボレータ	Administrator (管理者)	JIT 管理者
	管理 – 共有	–	✓	✓	–
	管理 – スター	–	✓	✓	–
脆弱性					
	ビュー	✓	✓	✓	–
悪意のあるファイル					
	ビュー	✓	✓	✓	–
ポリシー					
	ビュー	–	✓	✓	–
	管理	–	✓	✓	–
除外事項					
	ビュー	✓	✓	✓	–
	管理	–	✓	✓	–
AI アクティビティ					
	ビュー	✓	✓	✓	–
	管理	–	✓	✓	–
オートメーション					

アクセス許可	サブアクセス許可	ビューワー	コラボレータ	Administrator (管理者)	JIT 管理者
	ビュー	✓	✓	✓	–
	管理	–	✓	✓	–
レポート					
	ビュー	✓	✓	✓	–
	管理	–	✓	✓	–
コンプライアンス					
	ビュー	✓	✓	✓	–
	管理	–	✓	✓	–
統合					
	ビュー	✓	✓	✓	–
	管理	–	–	✓	–
設定					
	ビュー	–	–	✓	–
	管理	–	–	✓	–
設定 - 組織					
	ビュー	✓	✓	✓	–
	管理	–	–	✓	–

アクセス許可	サブアクセス許可	ビューワー	コラボレータ	Administrator (管理者)	JIT 管理者
設定 - 監査					
	ビュー	✓	✓	✓	–
JIT - 利用資格					
	ビュー	–	–	✓	✓
	管理	–	–	✓	✓
JIT - 監査					
	ビュー	–	–	✓	✓

* 限定されたアカウント範囲(組織全体未満)が割り当てられた管理者は、特定の Settings ページへの部分的なアクセス権を持つ場合があります。詳細については、設定への管理者のアクセス: 全体の範囲と制限された範囲 を参照してください。

統合 + 組織の依存関係:[統合を作成] ボタンを使用するには、**統合** と **組織** の両方のアクセス許可が必要です。これら 2 つのうち 1 つのみを保持しているユーザーは、統合を作成することはできません。

ロール

カスタムロールを使用すると、ユーザーまたはグループが Tenable One Cloud Exposure コンソールのどの領域にアクセスできるかを正確に定義できます。コンソールモジュールのリストから個別のアクセス許可を選択してロールを作成し、ユーザーとグループでユーザーまたはグループに割り当てます。

組み込みロール(閲覧者、コラボレータ、管理者)がユーザーに必要な以上のアクセス権を付与する場合は、カスタムロールを使用します。たとえば、コラボレータに含まれる広範なアクセス権を付与せずに、読み取り専用のコンプライアンスロールを作成できます。組み込みロールとそれらに含まれるアクセス許可の詳細については、「 ユーザーとグループを参照してください。

一般的なユースケース

次の表は、一般的なカスタムロールと、それらをサポートするために必要な最小限のアクセス許可を示しています。

ユースケース	対象者	最小限のアクセス許可
監査ビューアー	他の製品領域にアクセスできずにコンソールアクティビティをレビューする必要があるコンプライアンス担当者または外部監査人。	**監査 – 表示**
レポートビューアー	広範なコンソールアクセスなしでレポートを生成およびダウンロードする必要があるエグゼクティブステークホルダーまたはコンプライアンスレビュー担当者	**レポート - 表示**
コンプライアンスビューアー	コンプライアンス ベンチマークのステータスとスコアを監視するユーザーは、コンプライアンスルールを作成または変更することはできません。	**コンプライアンス – 表示**
読み取り専用検出結果レビュー担当者	リスクの検出結果、脅威、脆弱性を可視化する必要のあるステークホルダーですが、それらに対応したり修正したりすることはできません。	• **リスク** – • **脅威を表示する** – 脆弱性を**表示する** • **– 表示**
JIT の可視性	資格を管理したり、JIT 管理者ロールを保持したりせずに、コンソールを介して JIT 使用資格設定とイベントを監査する必要があるユーザー。	• **JIT - 使用資格** –

ユースケース	対象者	最小限のアクセス許可
		• **表示 JIT - 監査 – 表示**
オートメーションマネージャー	完全な管理者アクセス権なしで自動化ルールを作成および管理する必要がある DevSecOps チームメンバーまたは統合所有者。	• **自動化 –** • **表示 自動化 – 管理**

カスタムロールの作成

カスタムロールを作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings** > Access Management > **Roles]** (**アクセス管理**ロール) に移動します。
2. **[+ ロールの作成]** をクリックします。
3. **[名前]** ボックスにロールの名前を入力します。
4. **[Permissions] (アクセス許可**) セクションで、含めるモジュールのチェックボックスを選択します。

   モジュールのサブアクセス許可を表示するには、展開矢印をクリックします。たとえば、**インベントリ**には個別の **[表示]** と **[管理]** のサブアクセス許可が含まれています。

   一部のアクセス許可は、選択した他のアクセス許可もサポートされるため、自動的に選択され、**[必須]** とマークされます。**[必須]** バッジにカーソルを合わせると、選択したアクセス許可が依存するが表示されます。
5. **[Create]** をクリックします。

カスタムロールの編集

カスタムロールを編集し、ロールの名前またはアクセス許可のマッピングを変更します。

カスタムロールを編集する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings** > Access Management > **Roles]** (**アクセス管理**ロール) に移動します。
2. ロールのリストで、編集するロールの横にあるオプションメニューをクリックします。
3. **[編集]** をクリックします。
4. 必要に応じてロール名またはアクセス許可を更新します。
5. **[Save]** (保存) をクリックします。

ロールを複製する

組み込みロールまたはカスタムロールを複製して、既存のアクセス許可マッピングに基づいて新しいロールを作成します。

1. クラウドサイバーエクスポージャーコンソールで、**[Settings** > Access Management > **Roles]** (**アクセス管理**ロール) に移動します。
2. ロールのリストで、編集するロールの横にあるオプションメニューをクリックします。
3. **[複製]** をクリックします。
4. 必要に応じてロール名またはアクセス許可を更新します。
5. **[Create]** をクリックします。

カスタムロールの削除

カスタムロールを削除すると、そのロールを付与されたすべてのユーザーのアクセス許可がただちに取り消されます。

カスタムロールを削除する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings** > Access Management > **Roles]** (**アクセス管理**ロール) に移動します。
2. ロールのリストで、削除するロールの横にあるオプションメニューをクリックします。

3. **[削除]** をクリックします。
4. 確認ウィンドウで、**[削除]** をクリックします。

利用可能なアクセス許可

次の表に、カスタムロールを作成または編集するときに使用できるアクセス許可を示します。最上位の各アクセス許可は、コンソールのモジュールにマッピングされます。アクセス許可にサブアクセス許可が含まれている場合、親を選択しても子は自動的に選択されません。各サブアクセス許可を個別に選択する必要があります。

アクセス許可	コントロール対象
ダッシュボード	• **表示**: ダッシュボードとウィジェットのデータを表示します。 • **管理**: ダッシュボードを作成、編集、削除します。**プライベートダッシュボード**と**パブリックダッシュボード**それぞれに個別のサブアクセス許可があります。
インベントリ	• **表示**: クラウドリソース、IAM プリンシパル、アクセスグラフ、ネットワークグラフ、エンティティの詳細を表示します。 • **管理**: リソースにラベルを追加し、リソースを機密としてマークし、カスタムプロパティ値を設定します。
ワークロードリソース	• **今すぐスキャン:** ワークロードリソースのオンデマンドスキャンをリクエストします。
データリソース	• **スキャン**: データリソースのオンデマンドスキャンをリクエストします。
イベント	• **表示**: クラウドイベントと Kubernetes アドミッションコントローラーイベントを参照してください。
CI/CD スキャン	• **表示**: コンテナイメージ、コードパイプライン、プルリクエストのセキュリティスキャン結果を表示します。

アクセス許可	コントロール対象
クエリ	• **表示**: 保存したクエリを表示して実行します。 • **管理:** クエリを作成、編集、削除します。**プライベートクエリ**と**パブリッククエリ**用に個別のサブアクセス許可があります。

検出結果	• **表示**: クラウドとIaCの検出結果を表示します。
	• **管理**: 以下のサブアクセス許可が含まれます。
	  • **コメント** (検出結果のコメントを追加および削除)
	  • **ステータス**: 検出結果の状態を[オープン]または[クローズ]に更新します(検出結果を無視するには、[除外] > [管理]アクセス許可を使用します)
	  • **スター** (検出結果にスター)
	  • **修正:** 自動クラウド修正をトリガーします。
	  • **共有** (検出結果からJira課題およびServiceNowインシデントを作成)

脅威検出	• **表示**: 脅威検出結果を表示します。 • **管理**: 次のサブアクセス許可が含まれます: **コメント** (コメントの追加と削除)。Change **Status** (脅威ステータスの変更); **共有** (脅威からのJira課題とServiceNowインシデントの作成) **スター** (スターの脅威)。
脆弱性	• **表示**: 脆弱性の検出結果、パッケージ、CVEの詳細を表示します。
悪意のあるファイル	• **表示**: 悪意のあるファイルの検出を表示します。
ポリシー	• **表示**: 組み込みのリスクポリシーとカスタムのリスクポリシーを表示します。 • **管理**: カスタムリスクポリシーを作成および削除します。組み込みポリシーを有効または無効にします。
除外事項	リスク/検出結果の除外にのみ適用されます。データ/ワークロードの除外は、Settingsアクセス許可を通じて管理されます。

アクセス許可	コントロール対象
	• **表示**: リスクの除外を参照してください。 • **管理**: リスク除外を作成、更新、削除し、個々の検出結果を手動で無視します。
オートメーション	• **表示**: 自動化ルールを参照してください。 • **管理**: 自動化ルールを作成、更新、削除します。
レポート	• **表示**: レポートを表示、生成、ダウンロードします。 • **管理:** レポートをスケジュールして削除します。
コンプライアンス	• **表示**: コンプライアンスのベンチマークとスコアを表示します。 • **管理:** カスタムコンプライアンスルールを作成および削除します。組み込みのコンプライアンスベンチマークを有効または無効にします。
設定	すべての子ページを含む [Settings] の Access Management、Inventory、Security、Licensing ページをカバーします。 • **表示**: ユーザーとロールの割り当て、およびライセンスデータを表示します。 • **管理**: ユーザーおよびグループのロールの割り当てを追加、編集、削除し、カスタムロールを作成または更新します。
設定 - 組織	• **表示**: プロジェクトとアカウントとフォルダーの階層を表示します。 • **管理**: プロジェクトを作成、更新、削除し、アカウントとフォルダー階層を整理します。
設定 - 統合	• **表示**: 設定された統合を表示します。 • **管理:** 統合を作成、更新、削除します。Kubernetesクラスタの接続が含まれます。これは、**Explore > Inventory > Kubernetes Clusters** からアクセスできますが、Inventory アクセス許可ではなくこのアクセス許可によって制御されます。

アクセス許可	コントロール対象
設定 - 監査	• **表示**: コンソール監査イベントログを参照してください。
JIT - 利用資格	• **表示**:「JIT 使用資格設定」を参照してください。 • **管理**: JIT 使用資格を作成、更新、削除します。
JIT - 監査	• **表示**: JIT アクセスリクエスト監査イベントを参照してください。

アクセス許可の依存関係

一部のアクセス許可を選択すると、自動的に必要となります。たとえば **ダッシュボードを選択するには**、**自動的にインベントリ**(表示)、**クエリ**、**リスク**、**脆弱性**が必要になります。自動選択したアクセス許可の **[必須]** バッジにカーソルを合わせると、そのアクセス許可に依存するアクセス許可が表示されます。

サービスアカウント

サービスアカウントは、アプリケーションが Tenable One Cloud Exposure API に対する認証に使用する、人間以外の ID です。各サービスアカウントには、一意の ID、1 つ以上の割り当てられたロール、および独自のシークレットがあります。

シークレットとは、アプリケーションが API に送信する認証情報です。以前のリリースでは、この認証情報はトークンと呼ばれていました。各サービスアカウントは同時に最大 2 つのアクティブなシークレットを保持できるため、実行中のアプリケーションを中断することなく認証情報をローテーションできます。

サービスアカウントは、**[Settings** > **Access Management]** にある **[Service Accounts]** ページで管理します。シークレットを使用して API の呼び出しを開始するには、「API の概要」を参照してください。

> **注意**: サービスアカウントを作成して管理するには、**Settings** アクセス許可が必要です。

サービスアカウントは、アカウント範囲内で動作します。コンソールの上部にあるスコープセレクターから、コンソールの他の場所と同じように範囲を設定します。デフォルトでは、組織全体が選択されています。

セカンダリシークレットローテーション

2 つのシークレットスロットを使用して、ダウンタイムなしで認証情報を置き換えることができます。サービスアカウントで許可されているシークレットが 1 つだけの場合、新しいシークレットを作成する前にアクティブなシークレットを削除する必要があり、接続されたアプリケーションはスイッチオーバー中に認証できませんでした。

ダウンタイムなしでシークレットをローテーションする方法

1. アプリケーションは **シークレット A** で認証されます。
2. **シークレット B** を作成します。これで、サービスアカウントに 2 つのアクティブなシークレットが含まれるようになりました。
3. **シークレット B** を使用するように、アプリケーションコードまたは環境変数を更新します。
4. アプリケーションが **シークレット B** で動作することを確認したら、**シークレット A** を削除します。

サービスアカウントには、0 個、1 個、または 2 つのシークレットを保持できます。シークレットのないサービスアカウントは引き続き有効ですが、シークレットを作成するまで、アプリケーションはそのサービスアカウントで認証できません。

サービスアカウントを表示する

[Service Accounts] (サービスアカウント) ページに、選択した範囲内のすべてのサービスアカウントが一覧表示されます。

サービスアカウントを表示する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management] > [Service Accounts] (サービスアカウント)** をクリックします。
2. (オプション)行を展開すると、そのサービスアカウントに割り当てられた範囲が表示されます。

この表には、次の列が含まれています。

列	説明
名前	サービスアカウントの名前
Description (説明)	サービスアカウントの説明 (オプション)
範囲	サービスアカウントが動作する範囲。
利用時間	サービスアカウントのシークレットが最後に使用されたタイムスタンプ。
変更時刻	サービスアカウントが最後に変更された日付
変更者	サービスアカウントを変更したユーザー

[作成時刻] と **[作成者]** 列はデフォルトでは非表示になっています。

サービスアカウントの各行には、次のオプションを含むアクションメニューが含まれています。**ロールの割り当ての追加**、**新しいシークレットの作成**、**編集**、**削除**。

サービスアカウントの作成

クラウドサイバーエクスポージャーは、コンソール上部にある範囲セレクターで現在選択されている範囲内にサービスアカウントを作成します。

サービスアカウントを作成する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management]** > **[Service Accounts] (サービスアカウント)** をクリックします。
2. **[Create]** をクリックします。

   [新しいサービスアカウントの作成] ウィンドウが表示されます。
3. **[名前]** ボックスに、サービスアカウントの意味のある名前を入力します。
4. (オプション) **[説明]** ボックスに説明を入力します。
5. (オプション)**[ロール]** ドロップダウンボックスで、ロールを選択します。ロールは後で追加できます。詳細については、「サービスアカウントを編集する」を参照してください。

6. **[Create]** をクリックします。

   [新しいシークレットの作成] ウィンドウに、サービスアカウントの最初のシークレットが表示されます。

7. シークレットを安全な場所にコピーします。
8. **[Close]** (閉じる) をクリックします。

警告: シークレットは作成時に一度だけ表示されます。ウィンドウを閉じた後は、シークレットを再度表示することはできません。紛失した場合は、シークレットを削除して新しいシークレットを作成してください。

シークレットを作成する

2 つ目のシークレットを作成して認証情報をローテーションするか、何も持たないサービスアカウントのシークレットを作成します。シークレットは、[アクション] メニューまたは **[サービスアカウントの編集]** ウィンドウから作成できます。

シークレットを作成する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management]** > **[Service Accounts] (サービスアカウント)** をクリックします。
2. テーブルで、サービスアカウントを見つけます。
3. サービスアカウントのアクションメニューをクリックし、**[新しいシークレットの作成]** をクリックします。

   [新しいシークレットの作成] ウィンドウに新しいシークレットが表示されます。

4. シークレットを安全な場所にコピーします。
5. **[Close]** (閉じる) をクリックします。

注意: サービスアカウントは、最大 2 つのアクティブなシークレットを保持します。サービスアカウントにすでに 2 つある場合にシークレットを作成するには、まず既存のシークレットの 1 つを削除します。

シークレットを削除する

シークレットに依存しているアプリケーションがないことを確認した後、**[サービスアカウントの編集]** ウィンドウからシークレットを削除します。

シークレットを削除する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management] > [Service Accounts] (サービスアカウント)** をクリックします。
2. テーブルで、サービスアカウントを見つけます。
3. サービスアカウントのアクションメニューをクリックし、**[編集]** をクリックします。
4. **[シークレット]** セクションで、削除するシークレットの横にある削除アイコンをクリックします。
5. **[シークレットを削除しますか?]** ウィンドウで、**[シークレットの削除]** をクリックします。

警告: シークレットの削除は永続的であり、元に戻すことはできません。削除されたシークレットは復元できず、現在使用しているコードは直ちに動作を停止します。

ロールの割り当てを追加する

ロールは、サービスアカウントがアクセスできる対象を制御します。サービスアカウントは複数のロールを保持することができ、各ロールは独自の範囲に適用されます。

ロールの範囲は、コンソールの上部にある範囲セレクタで選択された全範囲、または任意の狭いサブセットにすることができます。これにより、あるロールで特定のフォルダーまたはアカウントへのアクセス権を付与し、別のロールで範囲全体をカバーできます。

ロールの割り当てを追加する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management] > [Service Accounts] (サービスアカウント)** をクリックします。
2. テーブルで、サービスアカウントを見つけます。
3. サービスアカウントのアクションメニューをクリックし、**[ロールの割り当ての追加]** をクリックします。

   [ロールの割り当ての追加] ウィンドウが表示されます。
4. **[割り当てられた範囲]** ドロップダウンボックスで、ロールが適用される範囲を選択します。
5. **[ロール]** ドロップダウンボックスで、ロールを選択します。
6. **[Save]** (保存) をクリックします。

サービスアカウントを編集する

[サービスアカウントの編集] ウィンドウを使用して、名前または説明を更新し、シークレットを作成または削除します。

サービスアカウントを編集する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management] > [Service Accounts] (サービスアカウント)** をクリックします。
2. テーブルで、サービスアカウントを見つけます。
3. サービスアカウントのアクションメニューをクリックし、**[編集]** をクリックします。
4. **名前**または**説明**を更新します。
5. **[Save]** (保存) をクリックします。

ウィンドウの **[シークレット]** セクションには、既存のシークレットが、**[作成者]**、**[作成時間]**、**[使用時間]** の値とともに一覧表示されます。このセクションから、**[新しいシークレットの作成]** でシークレットを作成したり、削除アイコンでシークレットを削除したりできます。

サービスアカウントを削除する

サービスアカウントを削除する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management] > [Service Accounts] (サービスアカウント)** をクリックします。
2. テーブルで、サービスアカウントを見つけます。
3. サービスアカウントのアクションメニューをクリックし、**[削除]** をクリックします。
4. プロンプトが表示されたら、削除を確定します。

> **警告:** サービスアカウントは完全に削除されます。サービスアカウントを削除するとそのシークレットが削除され、そのシークレットを使用するコードは直ちに動作を停止します。

サービスアカウントの詳細の表示

サービスアカウントプロファイルは読み取り専用です。このアカウントを使用すると、変更せずにサービスアカウントを確認します。

サービスアカウントの詳細を表示する方法

1. 左側のナビゲーションバーで、**Settings [> Access Management] > [Service Accounts] (サービスアカウント)** をクリックします。
2. テーブルにあるサービスアカウント名をクリックします。

プロファイルには次の詳細が表示されます。

- **説明**、**範囲**、**使用時間**、**変更時間**
- **変更者**、**作成時間**、**作成者**
- 割り当てられた各ロールとその**範囲**を一覧表示する**ロール割り当てテーブル**
- 各シークレットを、**その作成者**、**作成者**、**作成時間**、**使用時間**とともに一覧表示する**シークレット**テーブル

監査ログ

クラウドサイバーエクスポージャーのレコードシステム監査のサービスアカウントに対するアクション**の作成**と**削除**。サービスアカウントに割り当てられたロールに対するアクションは、サービスアカウント監査イベントとして記録されません。

シングルサインオン

重要:

- **新規の Tenable One** のお客様は、Tenable One 経由で SSO を設定する必要があります。ただし、アイデンティティプロバイダー (IdP) グループを使用する場合は、この記事のガイドラインに従ってグループのサポートを追加する必要があります。
- **JIT アクセス:** SSO 経由で JIT ポータルのログインを有効にするには、次のガイドラインに従います。

外部アイデンティティプロバイダー (IdP) と Tenable の間に信頼を確立し、個々のユーザーまたはグループメンバーが SSO 経由で Tenable One Cloud Exposure コンソールにログインできるようにします。このプロセスでは、ユーザーの既存の企業アイデンティティを利用して、簡単にユーザーのプロビジョニングを実行できるようにします。ただし、自動ユーザープロビジョニングは提供されないため、信頼が確立された後も、コンソールまたは API を介して新しいユーザーの追加または新しいグループを追加するを追加する必要があります。

既存の IdP グループを利用して、グループに関連付けられているすべてのユーザーに クラウド サイバーエクスポージャー で同一のアクセス許可を付与します。Tenable で IdP グループのサポートを追加するには、まず、下記の関連する手順を使用して、グループのクレームを Tenable に送信するように IdP のグループマッピングを構成してから、Tenableで新しいグループを追加する。

コンソールのログインは、次のいずれかの IdP を使用して有効にできます。

- AWS Identity Center
- Google 経由でのログインを有効化
- Microsoft Entra ID
- Okta 経由でのログインの有効化
- OneLogin 経由でのログインを有効にする
- Ping Identity 経由でのログインの有効化
- ジャンプクラウド

上記以外のプロバイダーを使用する場合は、SAML 2.0 のアイデンティティ仕様を利用することで、そのプロバイダー経由での クラウド サイバーエクスポージャー コンソールへのログインを有効にすることができます。詳細については、カスタム SAML 2.0 プロバイダー経由でのログインの有効化 を参照してください。

SSO ログインの有効化の詳細については、サポートへの問い合わせ。。

Tenable One経由でのログインを有効にする

新規の Tenable One のお客様は、Tenable One 経由で SSO を設定するには、以下のガイドライン に従ってください。

AWS Identity Center 経由でのログインの有効化 (SAML 2.0)

アイデンティティプロバイダー (IdP) として AWS Identity Center を使用して、SAML 2.0 経由での クラウド サイバーエクスポージャー コンソールへのログインを有効にします。

始める前に

- **前提条件: 認証ドメイン** AWS Identity Center ユーザーが使用する電子メールドメインを、クラウドサイバーエクスポージャーで認証ドメインとして追加する必要があります。ドメインが設定されていない場合、SSO のセットアップ中に SAML メタデータのアップロードが失敗します。

AWS Identity Center (SAML 2.0) を使用したログインを有効にする方法

1. AWS で、**AWS Identity Center** を開きます。
2. **[アプリケーション]** に移動し、**[アプリケーションの追加]** をクリックします。
3. **[セットアップするアプリケーションがあります]**、**[SAML 2.0]** を選択して、**[次へ]** をクリックします。
4. [アプリケーションの設定] で、**[表示名]** と **[説明]** を入力します (例: SSO 経由でのコンソールアクセスの有効化 クラウドサイバーエクスポージャー)。
5. [アプリケーションのプロパティ] で、**アプリケーションの開始 URL** の値を入力します。
   - **グローバル (すべてのリージョン)**: `app.tenable.com`
   - **米国ガバメントクラウド**: `app.tenable.us`
6. [Application metadata] で以下を行います。
   1. **アプリケーション ACS URL** の値を入力します。

      https://{URL}/api/console/authentication/saml2/customer/acs

      {URL} の場合
      - **グローバル (すべてのリージョン)**: `app.tenable.com`
      - **米国ガバメントクラウド**: `app.tenable.us`
   2. **[Application SAML audience] (アプリケーション SAML オーディエンス)** に、次のように入力します

      urn:app.ermetic.com

      > **注意:** アプリケーション SAML オーディエンス (エンティティ ID とも呼ばれます) は、クラウドサイバーエクスポージャーをサービスプロバイダーとして一意に識別します。この値はリージョン固有ではありません。
7. 「**送信**」をクリックしてアプリケーションを作成します。
8. **[ユーザーとグループの割り当て]** をクリックして、クラウドサイバーエクスポージャーコンソールにアクセスする必要があるユーザーまたはグループを割り当てます。

1. 検索バーから、関連するユーザーまたはグループを追加します。
2. **[割り当て]** をクリックします。

9. アプリケーションが作成されたら、それを開き、**[アクション] > [属性マッピングの編集]** を選択します。
    1. 次の属性マッピングを確認または追加します*

アプリケーションのユーザー属性	この文字列の値またはユーザーにマップされます IAM Identity Center の属性	フォーマット
サブジェクト (NameID)	`${user:email}`	電子メールアドレス
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	`${user:email}`	指定なし
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	`${user:givenName}`	指定なし
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	`${user:familyName}`	指定なし
グループ (オプション)	`${user:groups}`	指定なし

    *__グループ__属性では大文字と小文字が区別されます。AWS グループを使用する場合は、表示されているとおりに入力してください。

    2. **[変更を保存]** をクリックします。

10. アプリケーションページで、**[アクション] > [設定の編集]** を選択し、**IAM Identity Center SAML メタデータファイル**をダウンロードします。
11. クラウド サイバーエクスポージャー コンソールで、**Settings > Access Management > Single Sign-On** に移動します。
12. **[アイデンティティプロバイダーの追加]** をクリックし、**[SAML]** を選択します。
13. **[アプリケーションの選択]** ドロップダウンで、**[クラウド サイバーエクスポージャー]** を選択します。
14. **[ファイル]** を選択し、AWS Identity Center からダウンロードしたメタデータファイルをアップロードして、**[追加]** をクリックします。

Google 経由でのログインを有効化

次のいずれかのアイデンティティ仕様を使用して、Google経由でのクラウド サイバーエクスポージャー コンソールへのログインを有効にします。

- OpenID Connect (OIDC)
- SAML

> **注意:** Google を IdP として使用してクラウド サイバーエクスポージャー内の新しいグループを追加するを操作するには、OIDC ではなくSAML を使用する必要があります。

OIDC を使用した Google 経由でのログインの有効化

OIDC を使用したログインを有効にするには

1. クラウド サイバーエクスポージャー コンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
2. **[アイデンティティプロバイダーの追加]**、**[Google]** の順にクリックします。
3. [Add Identity Provider] ダイアログで、**[Add]** をクリックします。

> **注意:** この方法で Google を IdP として追加すると、クラウド サイバーエクスポージャー コンソールと JIT ポータルの両方へのログインが有効になります。

SAML を使用した Google 経由でのログインの有効化

SAML を使用したログインを有効にする方法

1. Google管理コンソールで、**[アプリ] > [ウェブアプリとモバイルアプリ]** に移動します。
2. **[アプリの追加] > [カスタム SAML アプリの追加]** をクリックします。
3. **[アプリ名]** を入力し、**[続行]** をクリックします。
4. [Google ID プロバイダの詳細] ページで、**[メタデータをダウンロード]** をクリックします。
5. クラウド サイバーエクスポージャー コンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
6. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
7. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、ドロップダウンから **[クラウド サイバーエクスポージャー]** を選択します。
8. **[ファイル]** を選択し、Google からダウンロードしたメタデータをアップロードして、**[追加]** をクリックします。
9. Google 管理コンソールの [サービス プロバイダの詳細] ページで、それぞれのフィールドに次の値を入力します。
    - ACS URL: **https://{URL}/api/console/authentication/saml2/customer/acs**

      {URL} の場合
        - **グローバル (すべてのリージョン)**: app.tenable.com
        - **米国ガバメント クラウド**: app.tenable.us
    - エンティティ ID: **urn:app.ermetic.com**
    - 名前 ID の形式: **メール**
    - 名前 ID: **基本情報>プライマリメール**
10. **[続行]** をクリックします。
11. [属性マッピング] ページで **[マッピングの追加]** をクリックし、次の属性を追加します。

    Google マッピングに対するディレクトリ属性 (アプリ属性):

- **名:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
- **姓:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
- **プライマリメール:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

12. (オプション) Google グループのサポートを追加する。
13. **[終了]** をクリックします。

Google グループのサポートを追加する

Google を IdP として使用している 新しいグループを追加する を操作するには、OIDC ではなく SAML を使用する必要があります。

Google グループのサポートを追加するには:

1. Google 管理コンソールで、**[アプリ] > [ウェブアプリとモバイルアプリ]** に移動し、設定した SAML アプリケーションを開きます (SAML を使用した Google 経由でのログインの有効化を有効にするを参照)。
2. **[SAML 属性マッピング]** セクションを展開します。
3. [グループメンバーシップ (オプション)] で、以下を入力します。
    - クラウド サイバーエクスポージャーでグループとして使用する**Googleグループ**。
    - [アプリ属性] に「**groups**」と入力します。
4. **[保存]** をクリックします。
5. 完了したら、クラウド サイバーエクスポージャーコンソールで新しいグループを追加する。

Microsoft Entra ID 経由でのログインの有効化

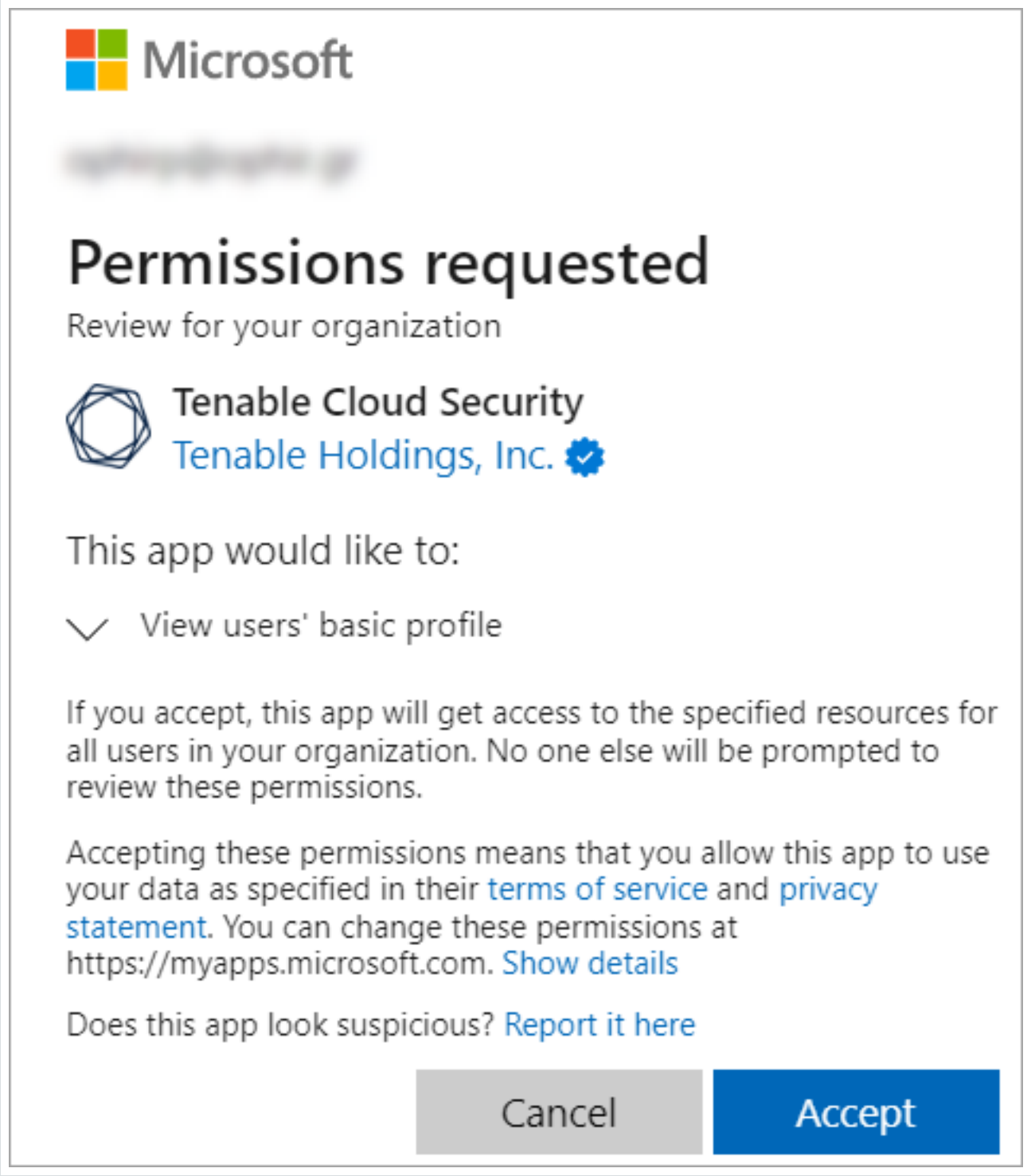
次のいずれかのアイデンティティ仕様を使用して、Microsoft Entra ID 経由での クラウド サイバーエクスポージャー コンソールへのログインを有効にします。

- OpenID Connect (OIDC)
- SAML

OIDC を使用した Microsoft Entra ID 経由でのログインの有効化

OIDC を使用したログインを有効にするには

1. クラウド サイバーエクスポージャー コンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
2. **[アイデンティティ プロバイダーの追加]** をクリックし、**[Microsoft]** をクリックします。
3. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、**クラウド サイバーエクスポージャー**のリンクをクリックしてアクセス権を付与します。
4. 組織で クラウド サイバーエクスポージャー 管理者に関連付けられているアカウントを選択します。
5. リクエストされたアクセス許可を**受け入れ**ます。



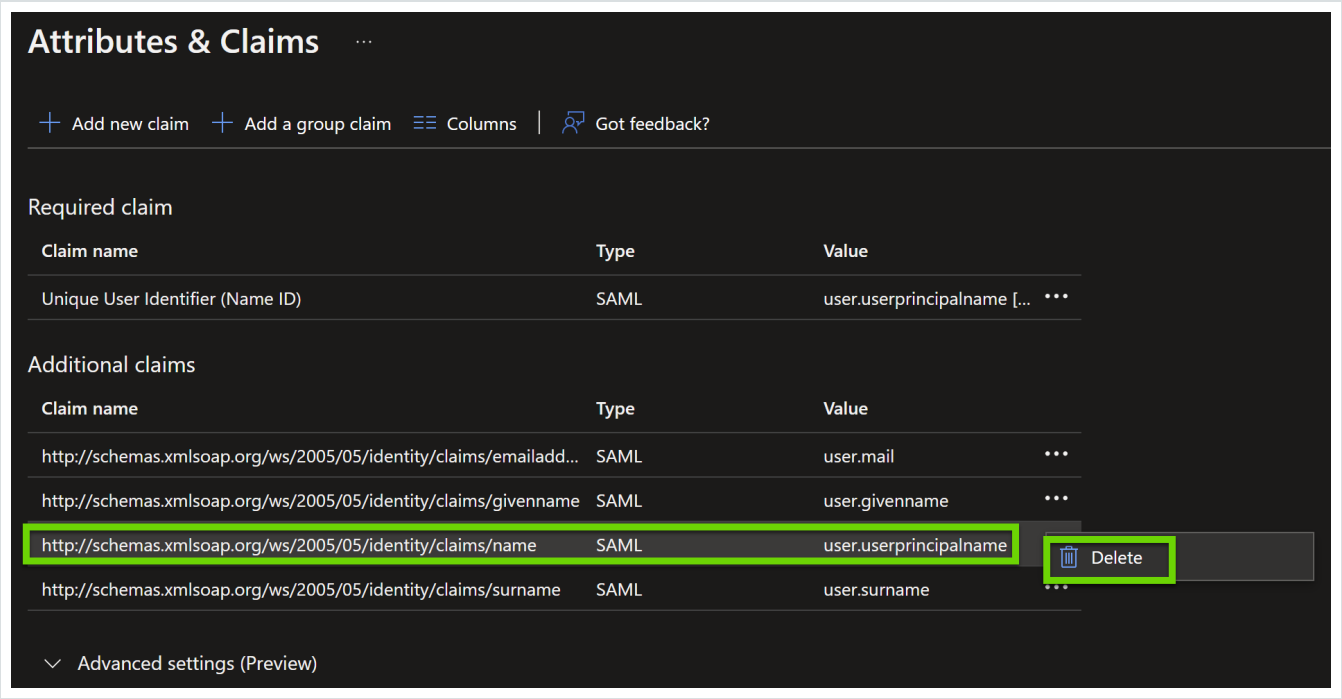
6. **[アクセス権を許可したことを確認する]** が選択されていることを確認し、**[追加]** をクリックします。

SAML を使用した Microsoft Entra ID 経由でのログインの有効化

SAML を使用したログインを有効にする方法

1. Azure portal で、**[エンタープライズ アプリケーション]** に移動し、**[新しいアプリケーション]** を追加します。
2. **[独自のアプリケーションの作成]** をクリックし、アプリの名前を入力します。
3. **[ギャラリーに見つからない他のアプリケーションを統合する (ギャラリー以外)]** の既定値を選択し、**[作成]** をクリックします。
4. 表示されるアプリの [概要] ページの [シングル サインオンの設定] ステップで、**[開始]** をクリックします。
5. SSO 方法として **[SAML]** を選択します。
6. [基本的な SAML 構成] で、**[編集]** をクリックし、それぞれのフィールドに以下の値を入力します。
    - 識別子 (エンティティ ID): **urn:app.ermetic.com**
    - 応答 URL (アサーション コンシューマ サービス URL): **https://{URL}/api/console/authentication/saml2/customer/acs**

      {URL} の場合
        - **グローバル (すべてのリージョン)**: `app.tenable.com`
        - **米国ガバメント クラウド**: `app.tenable.us`
7. **[保存]** をクリックします。
8. [属性と要求] で **[編集]** をクリックし、[追加の要求] で **user.userprincipalname** 要求を削除します。



9. [SAML 証明書] で、**フェデレーションメタデータ XML** をクリックしてダウンロードします。
10. クラウド サイバーエクスポージャー コンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
11. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
12. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、ドロップダウンから **[クラウド サイバーエクスポージャー]** を選択します。
13. **[ファイル]** を選択し、Azure からダウンロードしたメタデータをアップロードして、**[追加]** をクリックします。

Microsoft Entra ID グループのサポートの追加

Microsoft Entra ID グループのサポートを追加するには、Microsoft Entra ID で使用するアイデンティティプロトコルに応じて、以下の関連手順を実行します。

- OIDC
- SAML

これにより、関連するグループのクレームがクラウドサイバーエクスポージャーに送信され、新しいグループを追加するを Tenable に追加して、グループに関連付けられているすべてのユーザーに Tenable で同一のアクセス許可を付与できるようになります。

OIDC を使用した Microsoft Entra ID グループのサポートの追加

> **注意:** この手順は、グループに直接割り当てられているユーザーにのみ適用され、たとえば別のグループ内にネストされているグループには適用されません。

Microsoft Entra ID グループのサポートを追加する方法

1. Microsoft Entra ID 経由でのコンソールログインが有効になっていることを確認します。
2. Azure ポータルで、**[エンタープライズ アプリケーション]** ページに移動し、**クラウドサイバーエクスポージャー** アプリケーションを選択します。
3. [管理] で、**[ユーザーとグループ]** をクリックします。
4. **[ユーザー/グループの追加]** をクリックします。
5. [割り当ての追加] ページの [ユーザーとグループ] で、**[選択なし]** をクリックします。
6. ユーザーとグループのリストから関連するグループを選択し、**[選択]** をクリックします。
7. 完了したら、クラウドサイバーエクスポージャーコンソールで新しいグループを追加する。

SAML を使用して Microsoft Entra ID グループのサポートを追加する

次の手順を使用して、クラウドサイバーエクスポージャーで次のいずれかを送信してグループのサポート (SAML) を追加します。

- クラウドサイバーエクスポージャー SAML アプリケーションに割り当てられたグループ
- すべてのグループ (アプリに割り当てられていません)

使用するオプションを選択する際は、関連する制限に注意してください。たとえば、すべてのグループを選択した場合、この方法で送信できるグループの数には制限があります。または、アプリケーションに割り当てられているグループを選択した場合、アプリケーションに手動でグループを割り当てる必要があり、ネストされているグループはサポートされません。詳細は、関連する Microsoft ドキュメント を参照してください。

Microsoft Entra ID グループのサポートを追加する方法

1. カスタム SAML 2.0 プロバイダー経由でのログインの有効化になっていることを確認します。
2. Azure ポータルで、**[エンタープライズ アプリケーション]** ページに移動し、ログインを有効にしたときにクラウド サイバーエクスポージャー用に作成した関連する SAML アプリケーションを選択します。
3. (オプション) クラウド サイバーエクスポージャーで使用する特定のグループを選択します。
    1. [管理] で、**[ユーザーとグループ]** をクリックします。
    2. **[ユーザー/グループの追加]** をクリックします。
    3. [割り当ての追加] ページの [ユーザーとグループ] で、**[選択なし]** をクリックします。
    4. ユーザーとグループのリストから関連するグループを選択し、**[選択]** をクリックします。
4. SAML アプリケーションの **シングルサインオン** ページに移動します。
5. [属性 & クレーム] で、**[編集]** をクリックします。
6. **[グループの要求の追加]** をクリックします。
7. クレームでユーザーに関連付けられているどのグループを返す必要があるかを選択します。次のいずれかのオプションを選択します。
    - **すべてのグループ**。このオプションを選択すると、すべてのグループが Tenable に移動します。
    - アプリケーションに割り当てられているグループ。このオプションを選択すると、この手順の前半で Tenable SAML アプリケーションに割り当てたグループが Tenable に送信されます。
      詳細は、関連する Microsoft ドキュメントを参照してください。
8. ソース属性については、**グループ ID** のデフォルト値を維持します。
9. **[詳細オプション]** を開きます。
10. **[グループ クレームの名前のカスタマイズ]** を選択し、[名前] に「**グループ**」と入力します。

    > **重要:** [名前] フィールドでは大文字と小文字が区別されます。groups の値はそのまま正確に入力する必要があります。

11. **[保存]** をクリックします。
12. 完了したら、クラウド サイバーエクスポージャーコンソールで新しいグループを追加する。

Okta 経由でのログインの有効化

SAML 2.0 のアイデンティティ仕様を利用して、Okta 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にします。

Okta 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にする方法

1. Okta 管理コンソールで、**[アプリケーション] > [アプリケーション]** の順に移動します。
2. **[アプリカタログを参照]** をクリックします。
3. [検索] フィールドに「**クラウドサイバーエクスポージャー**」と入力し、アプリケーションタイルをクリックして、**[統合の追加]** をクリックします。
4. [General Settings] タブで、**コンソールドメイン**を入力します。ここで入力する値は、クラウドサイバーエクスポージャーコンソールへのログインに使用する URL の値によって異なります。
   - `app.tenable.com`
   - `app.tenable.us`

   > **注意:** 値を入力しない場合、デフォルトで app.tenable.com になります。
5. [SAML セットアップ] セクションで、**[SAML セットアップ手順の表示]** をクリックします。
6. [Configuration Steps] (構成ステップ) で、ステップ 2 にリストされている URL の値をコピーします。
7. クラウドサイバーエクスポージャーコンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
8. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
9. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、ドロップダウンから **[クラウドサイバーエクスポージャー]** を選択します。
10. **URL** を選択し、Okta の URL 値を貼り付けて、**[追加]** をクリックします。

Okta グループのサポートの追加

Okta グループのサポートを追加するには

1. Okta 管理コンソールで、「Okta 経由でのログインの有効化」で追加した **Tenable Cloud** Security アプリケーションに移動します

2. **[サインオン]** タブに移動し、Settings の横にある **[編集]** をクリックし、[SAML 2.0] で **[属性]** セクションを展開します。
3. [グループ属性ステートメント] の [名前] フィールドに「**グループ**」と入力し、関連するフィルターを入力して、クラウドサイバーエクスポージャーに送信するグループを定義します。たとえば、すべてのグループを送信する場合は、値 **.*** の**正規表現の一致を選択できます**。

   > **重要:** [名前] フィールドでは大文字と小文字が区別されます。groups の値はそのまま正確に入力する必要があります。

4. **[保存]** をクリックします。
5. 完了したら、クラウドサイバーエクスポージャーコンソールで新しいグループを追加する。

OneLogin 経由でのログインを有効にする

SAML 2.0 のアイデンティティ仕様を利用して、OneLogin 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にします。

OneLogin 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にする方法

1. OneLogin 管理コンソールで、**[アプリケーション] > [アプリケーション]** の順に移動します。
2. **[アプリの追加]** をクリックします。
3. **[SAML Custom Connector (Advanced)]** を検索して選択します。
4. [設定] ページで、**[表示名]** (「クラウドサイバーエクスポージャー」など) を入力し、**[保存]** をクリックします。
5. [Configuration] (**構成**) タブに移動し、これらのアプリケーションの詳細に次の値を入力します。
   - オーディエンス (エンティティ ID): **urn:app.ermetic.com**
   - ACS (コンシューマー) URL Validator/ACS (コンシューマー) URL: **https://{URL}/api/console/authentication/saml2/customer/acs**

     {URL} の場合
     - **グローバル (すべてのリージョン)**: app.tenable.com
     - **米国ガバメントクラウド**: app.tenable.us

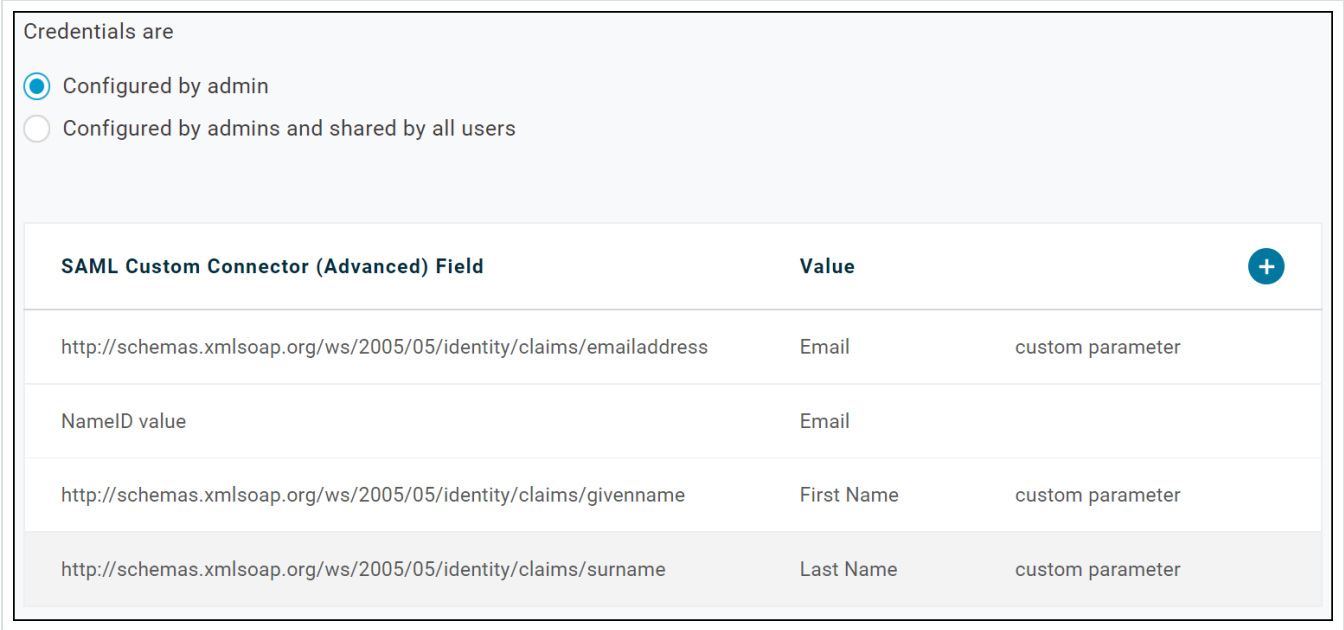
6. **[パラメーター]** タブに移動し、⊕ をクリックして次の新しいフィールド/値を追加します。

   フィールド名と値:

   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress:** E メール
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname:** 名
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname:** 姓

   重要: 各フィールド/値で **[Include in SAML assertion] (SAML アサーションに含める)** フラグが有効になっていることを確認します。

   注意: [NameID value] (NameID の値) フィールドは、OneLogin に標準装備で表示されます。このフィールドはそのままにしておくことができます。



7. [SSO] タブに移動し、**SAML 署名アルゴリズム** を **SHA-256** に設定します。
8. [その他のアクション] ドロップダウンをクリックし、**[SAML メタデータ]** を選択します。メタデータをコピーします。
9. クラウドサイバーエクスポージャーコンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
10. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。

11. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、ドロップダウンから **[クラウドサイバーエクスポージャー]** を選択します。
12. **[ファイル]** を選択し、OneLogin からコピーしたメタデータをアップロードして、**[追加]** をクリックします。

OneLogin ロールのサポートの追加

OneLoginでは、**ロールを使用して**ユーザーを1つ以上のアプリケーションに割り当て、**グループ**はユーザーセキュリティポリシーをユーザーに割り当てます。OneLogin ユーザーは、一度に 1 つの OneLogin グループにしか属することができません。

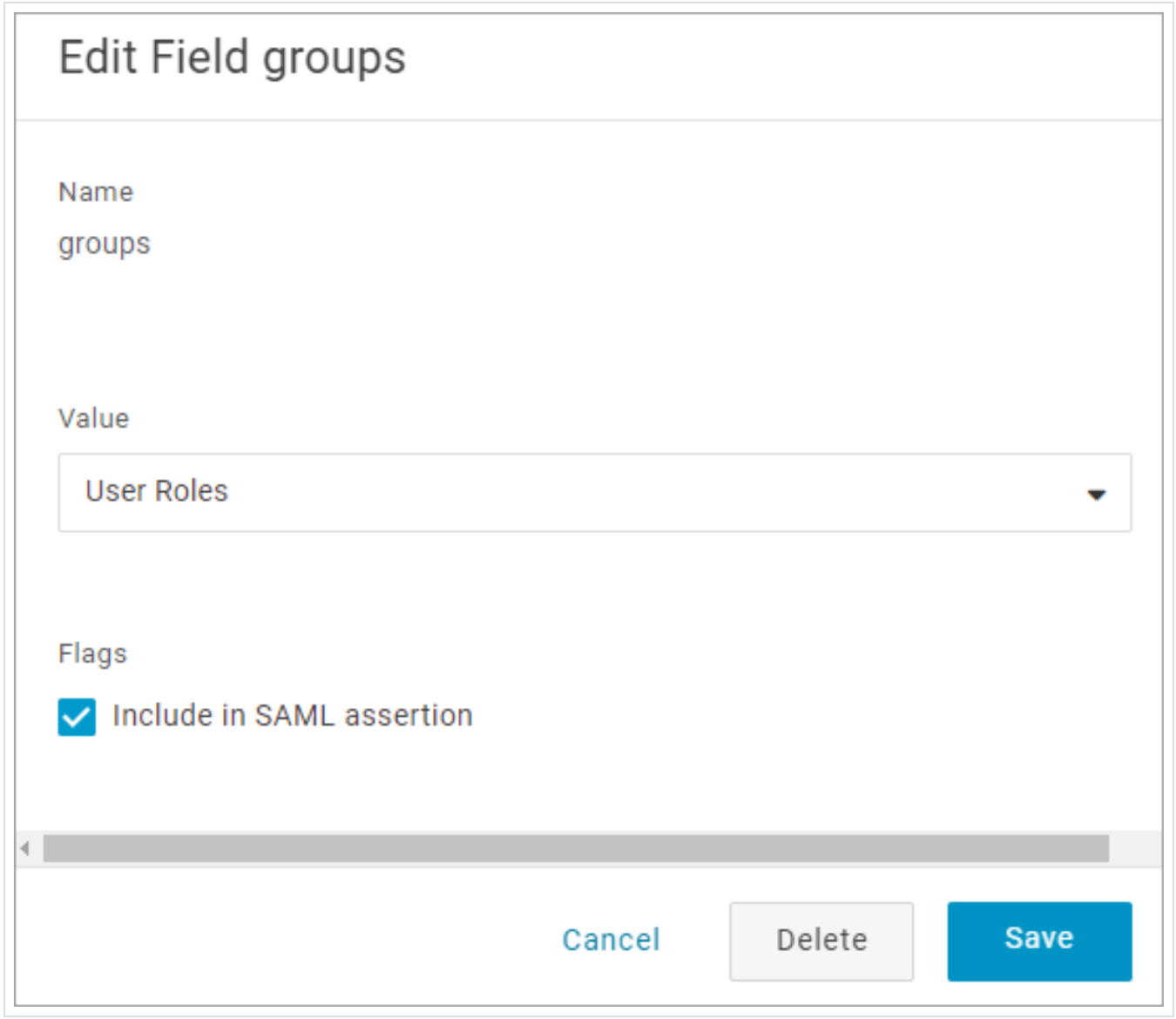
OneLoginグループは他のほとんどのアプリケーションとは異なる方法で機能するため、クラウドサイバーエクスポージャーで新しいグループを追加するを操作するには、OneLoginグループではなく、OneLoginロールをクラウドサイバーエクスポージャーグループにマッピングする可能性が高くなります。

OneLogin ロールのサポートを追加するには

1. OneLogin 管理コンソールで、**[アプリケーション] > [アプリケーション]** の順に移動し、[OneLogin 経由でのログインを有効にする] で追加したクラウドサイバーエクスポージャー SAML アプリケーションを開きます。
2. **[パラメーター]** タブに移動し、⊕ をクリックして次の新しいフィールド/値を追加します。
    - フィールド名: **groups**

      > **重要:** 名前フィールドでは大文字と小文字が区別されます。groups の値はそのまま正確に入力する必要があります。

    - 値: **ユーザーロール**
    - フラグ: **SAML アサーションに含めるが**有効
3. **[保存]** をクリックします。



4. 完了したら、クラウドサイバーエクスポージャーコンソールで新しいグループを追加する。

Ping Identity 経由でのログインの有効化

SAML 2.0 のアイデンティティ仕様を利用して、Ping Identity 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にします。

Ping Identity 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にする方法

1. Ping Identity 管理コンソールで、**[接続] > [アプリケーション]** に移動します。
2. ⊕ をクリックしてアプリケーションを追加します。

3. **アプリケーション名**を入力します。たとえば、「クラウドサイバーエクスポージャー」と入力します。
4. [アプリケーションタイプ] として **[SAML アプリケーション]** を選択し、**[構成]** をクリックします。
5. [SAML Configuration] (SAML 構成) で、**[Manually Enter] (手動入力)** を選択し、次の詳細を入力します。
    - **ACS の URL**:https://{URL}/api/console/authentication/saml2/customer/acs

      {URL} の場合
        - **グローバル (すべてのリージョン)**: app.tenable.com
        - **米国ガバメントクラウド**: app.tenable.us
    - **エンティティ ID**: urn:app.ermetic.com
6. **[保存]** をクリックします。
7. [Attribute Mappings] (属性マッピング) タブに移動し、![Edit consoleSSO8] (コンソールSSO8 の編集) をクリックして、次の属性を追加します。

   PingOne マッピングの属性:
    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress:** メールアドレス
    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname:** 名
    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname:** 姓
8. ラジオボタンをクリックしてアプリを有効にします。



9. [構成] タブに移動し、**[メタデータのダウンロード]** をクリックします。
10. クラウドサイバーエクスポージャー コンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
11. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
12. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、ドロップダウンから **[クラウドサイバーエクスポージャー]** を選択します。

13. **[ファイル]** を選択し、OneLogin からコピーしたメタデータをアップロードして、**[追加]** をクリックします。

Ping Identity グループのサポートの追加

Ping Identity グループのサポートを追加するには

1. Ping Identity 管理コンソールで、**[接続] > [アプリケーション]** に移動し、Ping Identity 経由でのログインの有効化 で追加したクラウドサイバーエクスポージャー SAML アプリケーションを開きます。
2. [Attribute Mappings] (属性マッピング) タブに移動し、( ) をクリックして、次の属性を追加します。
   - 属性: **グループ**
   - PingOne マッピング: **グループ名**

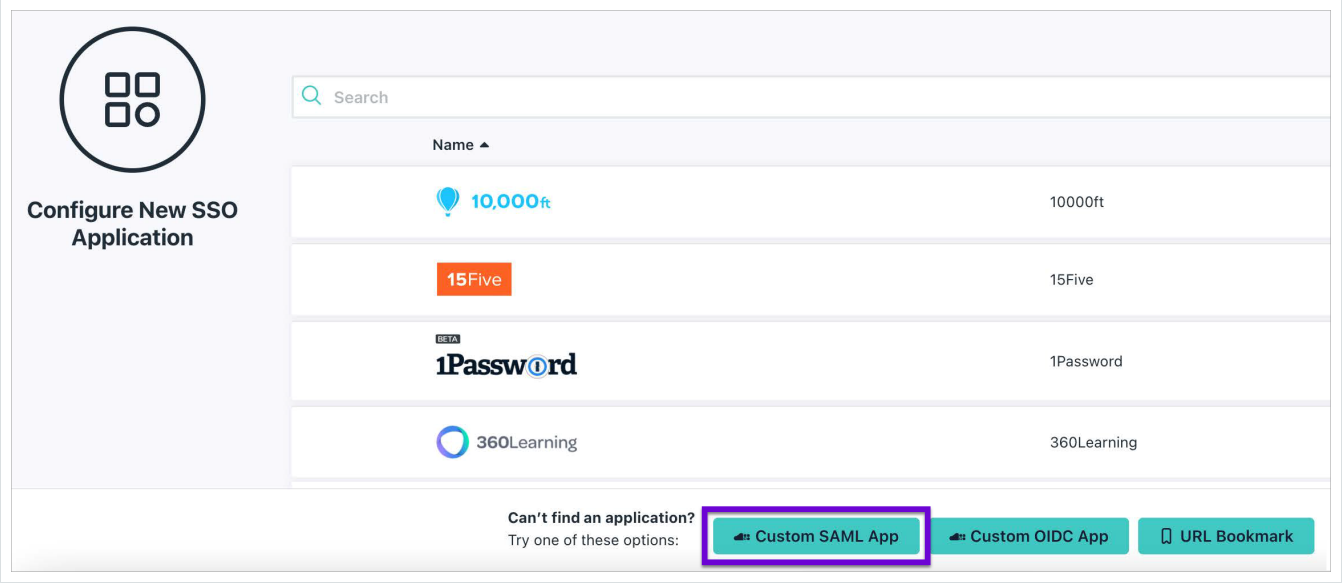
   > **重要:** [属性] フィールドでは大文字と小文字が区別されます。groups の値はそのまま正確に入力する必要があります。
3. **[保存]** をクリックします。
4. 完了したら、クラウドサイバーエクスポージャーコンソールで新しいグループを追加する。

JumpCloud 経由でのログインの有効化

SAML 2.0 のアイデンティティ仕様を利用して、JumpCloud 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にします。

JumpCloud 経由でのクラウドサイバーエクスポージャーコンソールへのログインを有効にする手順

1. JumpCloud 管理ポータルで、**[ユーザーグループ]** ([ユーザー管理] の下) に移動し、クラウドサイバーエクスポージャー SSO アプリケーションの新しいグループを作成してから、関連するユーザーを追加します。
2. **SSO** に移動し、**[新しいアプリケーションの追加]** をクリックします。
3. **[カスタム SAML アプリ]** を検索して選択します。



4. [一般情報] タブで、**表示ラベル**を入力します (例: *Tenable_SSO)。
5. **[SSO]** タブに移動し、各フィールドに次の値を入力します。

フィールド	値
IdP エンティティ ID	urn:{your-domain.com} ここで、`your-domain.com` は会社のプライマリドメイン名です。たとえば、urn:ermetic.com.
SP エンティティ ID	urn:app.ermetic.com
ACS の URL	**https://{URL}/api/console/authentication/saml2/customer/acs** `{URL}` の場合 • **グローバル (すべてのリージョン)**: `app.tenable.com` • **米国ガバメントクラウド**: `app.tenable.us`
SAMLSubject NameID	email
SAMLSubject	urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified (デフォ

フィールド	値
NameID format	ルト)
署名アルゴリズム	RSA-SHA256
符号アサーション	有効化/選択済み

6. **[属性] > [ユーザー属性マッピング]** で、**[属性の追加]** をクリックし、以下の各マッピングを追加します。

サービスプロバイダー属性名	JumpCloud 属性名
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	メール
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	firstname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	姓

7. **[ユーザーグループ]** タブに移動し、先ほど作成したグループを追加して、**[アクティブ化]** をクリックします。
8. 作成したアプリをクリックし、**[SSO]** に移動して、**[メタデータのエクスポート]** をクリックします。
9. クラウドサイバーエクスポージャーコンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
10. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
11. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、ドロップダウンから **[クラウドサイバーエクスポージャー]** を選択します。
12. **[ファイル]** を選択し、JumpCloud からコピーしたメタデータをアップロードして、**[追加]** をクリックします。

JumpCloud グループのサポートの追加

JumpCloud グループのサポートを追加するには

1. JumpCloud 管理コンソールで、**[SSO]** に移動し、[JumpCloud 経由でのログインの有効化] で追加した クラウド サイバーエクスポージャー SAML アプリケーションを開きます。
2. **[SSO]** タブに移動し、[GROUP ATTRIBUTES] で **[include group attribute]** を選択してから、「**groups**」と入力します。

   > **重要:** [Attribute] (属性) フィールドでは大文字と小文字が区別されます。groups の値はそのまま正確に入力する必要があります。

3. **[保存]** をクリックします。

カスタム SAML 2.0 プロバイダー経由でのログインの有効化

上記のセクションで説明されていないプロバイダーを使用する場合は、SAML 2.0 のアイデンティティ仕様を利用することで、そのプロバイダー経由での クラウド サイバーエクスポージャー コンソールへのログインを有効にすることができます。

> **注意:** 各プロバイダーでは、以下にリストされている詳細、パラメーター、属性を参照する際に、若干異なる名前や用語が使用される場合があります。以下の値が正しいパラメーターに構成されていることを確認してください。

カスタム SAML プロバイダー経由での クラウド サイバーエクスポージャー コンソールへのログインを有効にする方法

1. 対象プロバイダーごとに概説しているステップに従って、クラウド サイバーエクスポージャー 専用のアプリケーションを追加します。必要に応じて、関連するドキュメントを参照してください。
2. アプリケーションで、以下の SAML の詳細を設定します。

SAML パラメーター	値
エンティティ ID	urn:app.ermetic.com
ACS (リダイレクト URL)	https://{URL}/api/console/authentication/saml2/customer/acs

SAML パラメーター	値
	{URL} の場合 • **グローバル (すべてのリージョン)**: app.tenable.com • **米国ガバメントクラウド**: app.tenable.us
暗号化	**SHA-256**
SAML NameID の形式	**メール**

3. 以下の SAML 属性を追加し、必要に応じてそれらを指定されたプロバイダーにマッピングします:

属性	マッピング	名前の形式
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	メールアドレス	指定なし
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	名	指定なし
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	姓	指定なし

4. メタデータをダウンロードします。
5. クラウド サイバーエクスポージャー コンソールで、**Settings** > **Access Management** > **Single Sign-On** に移動します。
6. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。

7. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、ドロップダウンから **[クラウドサイバーエクスポージャー]** を選択します。
8. **[ファイル]** を選択し、前にダウンロードしたメタデータをアップロードして、**[追加]** をクリックします。

グループのサポートの追加

カスタム SAML 2.0 プロバイダーを使用するグループのサポートを追加する方法

ネイティブ IdP グループ属性を クラウドサイバーエクスポージャー **グループ** 属性にマッピングします。

> **重要: グループ**属性では大文字と小文字が区別されます。値はそのまま正確に入力する必要があります。

コンソールのタイムアウト設定

アカウントのセキュリティを強化し、不正アクセスのリスクを低減するために、管理者はウェブコンソールに2種類のタイムアウトを設定できます。

- 非アクティブタイムアウト。一定時間ユーザーが操作しなかった場合、セッションを終了します。
- セッションタイムアウト。ユーザーのアクティビティに関係なく、一定の時間が経過するとセッションを終了します。

これらの設定は、組織のセキュリティとコンプライアンスのニーズに応じて調整できます。

非アクティブタイムアウト

非アクティビティタイムアウトは、一定時間コンソールとのやり取りがないと、ユーザーを自動的にサインアウトします。デフォルト値は **12 時間** です。

> **注意:** タイムアウト期間の構成変更は、各ユーザーが次回ログインしたときに有効になります。

非アクティビティタイムアウトを設定するには

1. Tenable One Cloud Exposure コンソールで、**[設定]** > **[アクセス管理]** > **[シングルサインオン]** に移動します。
2. [非アクティビティタイムアウト] セクションに、数値 (分) を入力し、**[保存]** をクリックします。

セッションタイムアウト

セッションタイムアウトは、アクティビティに関係なく、ログインの時点からのユーザーセッションの有効期限を定義します。セッション期間が終了すると、ユーザーはログアウトされ、再度サインインする必要があります。この設定は、デフォルトでは無効になっています。

> **注意:** タイムアウト期間の構成変更は、各ユーザーが次回ログインしたときに有効になります。

セッションタイムアウトの設定手順

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アクセス管理]** > **[シングルサインオン]** に移動します。
2. [セッションタイムアウト] セクションで、ラジオボタンをクリックしてセッションタイムアウトを有効にします。
3. 分単位の数字を入力し、**[保存]** をクリックします。

組織

プロジェクト

プロジェクトは、論理的にグループ化することでアカウントとリソースの管理を簡素化し、コンソールデータを組織構造に合わせて調整することができます。

これはプロジェクトを構成するためのハウツーガイドです。概念上の概要については、プロジェクトの仕組み参照してください。

プロジェクトを作成できるユーザー

プロジェクトを作成または編集するには、ユーザーは次の両方で管理者ロールを持っている必要があります。

- プロジェクトが作成または変更されている **プロジェクトまたはフォルダーのスコープ** 。
- プロジェクトに含まれる各アカウントの **アカウントスコープ** 。

これは次のことを意味します。

- 組織スコープを割り当てられた管理者ユーザーは、任意のスコープでプロジェクトを作成または編集できます。
- ルートのプロジェクトフォルダースコープに割り当てられた管理者ユーザーは、そのルート内の任意のプロジェクトまたはフォルダーを管理できます。
- 特定のプロジェクトフォルダースコープに割り当てられた管理者ユーザーは、そのフォルダー内の任意のプロジェクトまたはサブフォルダーを管理できます。
- 特定のプロジェクトに割り当てられた管理者ユーザーは、新しいプロジェクトを作成できません。割り当てられたプロジェクトの編集のみ行えます。

例: プロジェクトの所有権の委任

たとえば、自分の環境の組織レベルの管理者で、プロジェクトの所有権を別のチームメンバーに委任するとします。次のことができます。

1. プロジェクトフォルダーを追加する。たとえば、「Development」と入力します。
2. 新しいユーザーの追加 新しい Development フォルダーでユーザーに管理者ロールを付与します。

   > **注意:** このユーザーがプロジェクトに含まれるべきアカウントの管理者も持っていることを確認します。

3. そのユーザーは現在、Development内でプロジェクトまたはサブフォルダーを作成および管理できるようになりました。

サポートされている機能

Tenable One Cloud Exposure の多くの機能はプロジェクトをサポートしており、特定のプロジェクトスコープ内でアクションを実行できます。一致するプロジェクト範囲が割り当てられたユーザーのみがこれらの機能を表示/管理できます。

たとえば、プロジェクトスコープに対して以下を実行できます。

- クラウドサイバーエクスポージャーユーザーにアクセス権を付与します
- 統合
- レポート
- コンプライアンス

- APIトークンの作成 を行い、クラウド サイバーエクスポージャー APIをクエリします
- ライセンス
- クラウド ポリシー: カスタム

したがって、たとえば、プロジェクト A に割り当てられたユーザーのみが、そのスコープの API トークンを作成できます。

プロジェクト フォルダーを追加する

> **必要な クラウド サイバーエクスポージャー ユーザーロール:** このアクションを実行するには、管理者ロールが必要です。プロジェクトを作成できるユーザー を参照してください。詳細については、および ユーザーとグループ 参照してください。

プロジェクト のフォルダーを追加して、1 つ以上 のプロジェクトを論理的に整理します。プロジェクト のフォルダーへのアクセス権 が付与されたコンソールユーザーは、すべての子 プロジェクト にアクセスできます。たとえば、組織内の製品グループごとにプロジェクトを作成し、それらをリージョンごとにフォルダーでグループ化することができます。その後、関連するユーザーに特定のプロジェクト またはプロジェクト のフォルダー全体へのアクセス権を付与できます。

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[アカウント]** > **[プロジェクト]** に移動します。

   既存のフォルダーとプロジェクト は、ページの左側にあるツリーに表示されます。
2. フォルダーを追加する場所に移動します。
3. **[追加]** > **[フォルダーの追加]** をクリックします。
4. **フォルダー名** を入力し、**[追加]** をクリックします。

プロジェクト を追加する

プロジェクト を追加する前に、プロジェクト に必要なクラウド リソースを含むアカウントをオンボードしてください。プロジェクト を追加した後で使用できるのは、環境内の次の データの同期と更新の頻度 の後でのみです。

> **必要な クラウド サイバーエクスポージャー ユーザーロール:** このアクションを実行するには、管理者ロールが必要です。プロジェクトを作成できるユーザー を参照してください。詳細については、および ユーザーとグループ 参照してください。

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アカウント]** > **[プロジェクト]** に移動します。既存のプロジェクトは、ページの左側にあるツリーに表示されます。
2. プロジェクトを追加する場所に移動します。
3. **[追加]** > **[プロジェクトの追加]** をクリックします。
4. [プロジェクトの追加] ダイアログで、プロジェクトの詳細を入力します:
    1. クラウドサイバーエクスポージャーに表示する一意で意味のある **名前** を入力します。
    2. (オプション) **[説明]** を入力します。
5. **適用範囲**。1つ以上の範囲グループを定義します。プロジェクトに割り当てられたユーザーは、これらのスコープのリソースにアクセスできます。
    1. プロジェクトに含める **アカウント** を選択します。アカウントの範囲は、たとえば、オンボードのクラウドアカウント、IdP テナント、コードリポジトリなどです。

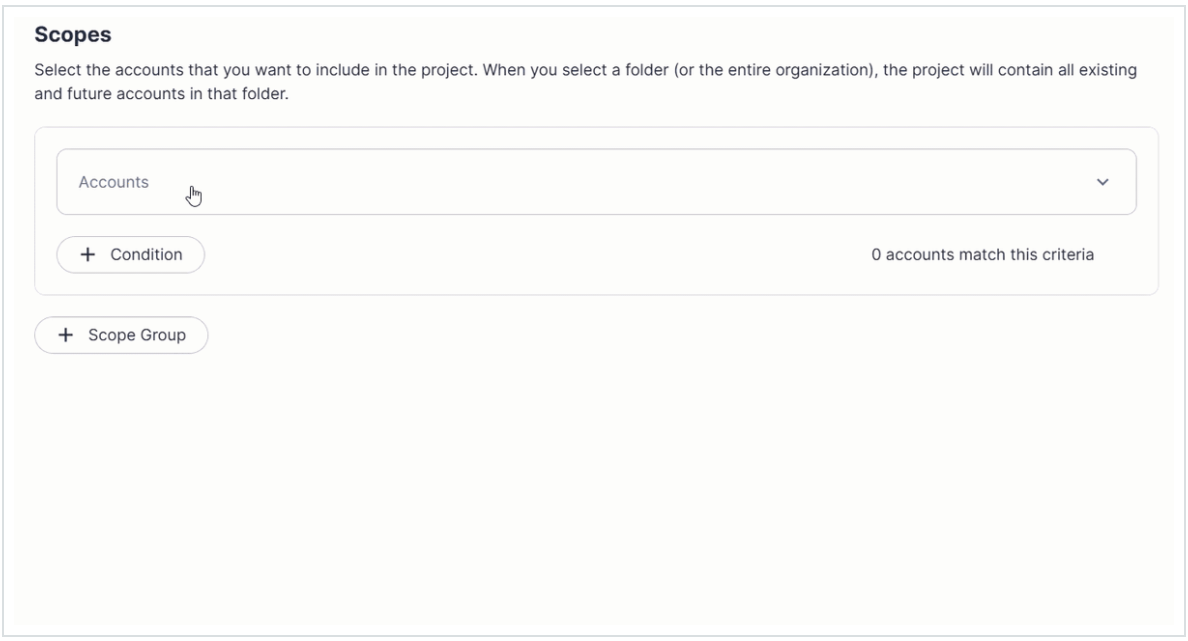
        > **注意:** フォルダーまたは組織全体を選択すると、プロジェクトにはそのフォルダーにある既存のアカウントおよび将来利用されるアカウントすべてが含まれます。

    2. 1つ以上の **条件** を定義して、プロジェクトの範囲を絞り込む必要があります。
        - **アカウント名のパターン**。クラウドアカウント名にあるテキストパターンに基づいて、名前のパターンを入力します。定義したパターンと一致する名前のパターンを含むアカウントがプロジェクトに含められます。たとえば、`dev*` と入力すると、`development` という名前のアカウントが一致します。
        - **アカウントタグパターン**。アカウントのタグキーまたはパターンで見つかったテキストパターンに基づくタグキーと値のペアを入力します。定義したパターンと一致するキーと値のペアでタグ付けされたアカウントがプロジェクトに含められます。たとえば、`type` のキーと `prod` の値を入力すると、そのキーと値のペアを持つアカウントが一致します。
        - **リソースタグパターン**。リソースのタグキーまたはパターンで見つかったテキストパターンに基づくタグキーと値のペアを入力します。定義したパターンと一致するキーと値のペアでタグ付けされたリソースがプロジェクトに含められます。たとえば、`business_unit` のキーと `finance` の値を入力すると、そのキーと値のペアを持つリソースが照合されます。

- **Azure リソースグループ名 のパターン**。リソースグループの名 前 にあるテキスト パターンに基 づいて、名 前 のパターンを入 力します。定 義したパターンと一 致する名 前 のパターンを含 むリソースグループがプロジェクト に含 められます。たとえば、`cust-facing-apps-*` と入 力すると、`cust-facing-apps-europe-prod` という名 前 のリソースグループが一 致します。
- **Azure リソースグループのタグ パターン**。Azure リソースグループのタグキーまたはパターンで見 つかったテキスト パターンに基 づいて、タグのキーと値 のペアを入 力します。定 義したパターンに一 致 するキーと値 のペアでタグ付 けされたリソースグループがプロジェクト に含 まれます。たとえば、`environment` のキーと `production` の値 を入 力 すると、そのキーと値 のペアを持 つリソースグループが一 致します。

  > **重 要**: プロジェクト にリソースベースの条 件 を定 義 すると、条 件 に直 接 一 致 するリソースだけでなく、関 連 するリソースも含 まれます。これらは、一 致したリソースと意 味 のある関 係 を持 つ追 加 リソースであり、関 連 する依 存 関 係 をより広 く可 視 化 できます。たとえば、Key Vault が定 義 された条 件 に一 致 する場 合 、それに関 連 付 けられたシークレットも関 連 リソースとして含 まれることがあります。これにより、コンソールをプロジェクト 別 にフィルタリングするときに、より全 体 像 を把 握 できるようになります。

- プロジェクト 作 成 時 に条 件 を使 用 する一 般 的 な方 法 の例 を確 認 するには、一 般 的 なプロジェクト の使 用 例 を参 照 してください。
- 0 個 または複 数 の文 字 を指 定 するには「*」を、単 一 文 字 を指 定 するには「?」を使 用 します。
- 必 要 に応 じて、「is」演 算 子 または「is not」演 算 子 のいずれかを使 用 します。キーと値 のペアの場 合 、それぞれに異 なる演 算 子 を使 用 できます。たとえば、リソースタグ **キー** パターン `is': 'environment'` で、`**value**` パターン is not: test` がある場 合 、これには、テスト 用 ではない本 番 リソースのみが含 まれます。
- 複 数 の条 件 を選 択 する場 合 は、**および** (デフォルト) または **または** 演 算 子 ロジックを使 用 できます。
- 条 件 を入 力 すると、入 力 している条 件 に一 致 するアカウント の数 が表 示 されます。



3. **[スコープグループ]** をクリックして、アカウントの別の論理グループをプロジェクトに追加します。

   > **注意:** 複数の範囲グループを追加する場合、使用される演算子ロジックは **または** です。

6. **プロジェクト でスコープへのユーザーアクセスを拡張する**かどうかを決定します。これにより、このプロジェクトに割り当てられたユーザーが、プロジェクト内のアカウントにも自動的に割り当てられるかどうかが決まります。

   > **注意:** これは、このプロジェクトで定義されたリソースベースの条件でフィルタリングされていないアカウントにのみ適用されます。

   - **自動割り当てを有効にしない**
   - **資格取得可能な範囲に自動で割り当てる**

7. 完了したら、**[追加]** をクリックします。

プロジェクトを追加すると、環境内の次回の データの同期と更新の頻度 の後に使用可能になります。

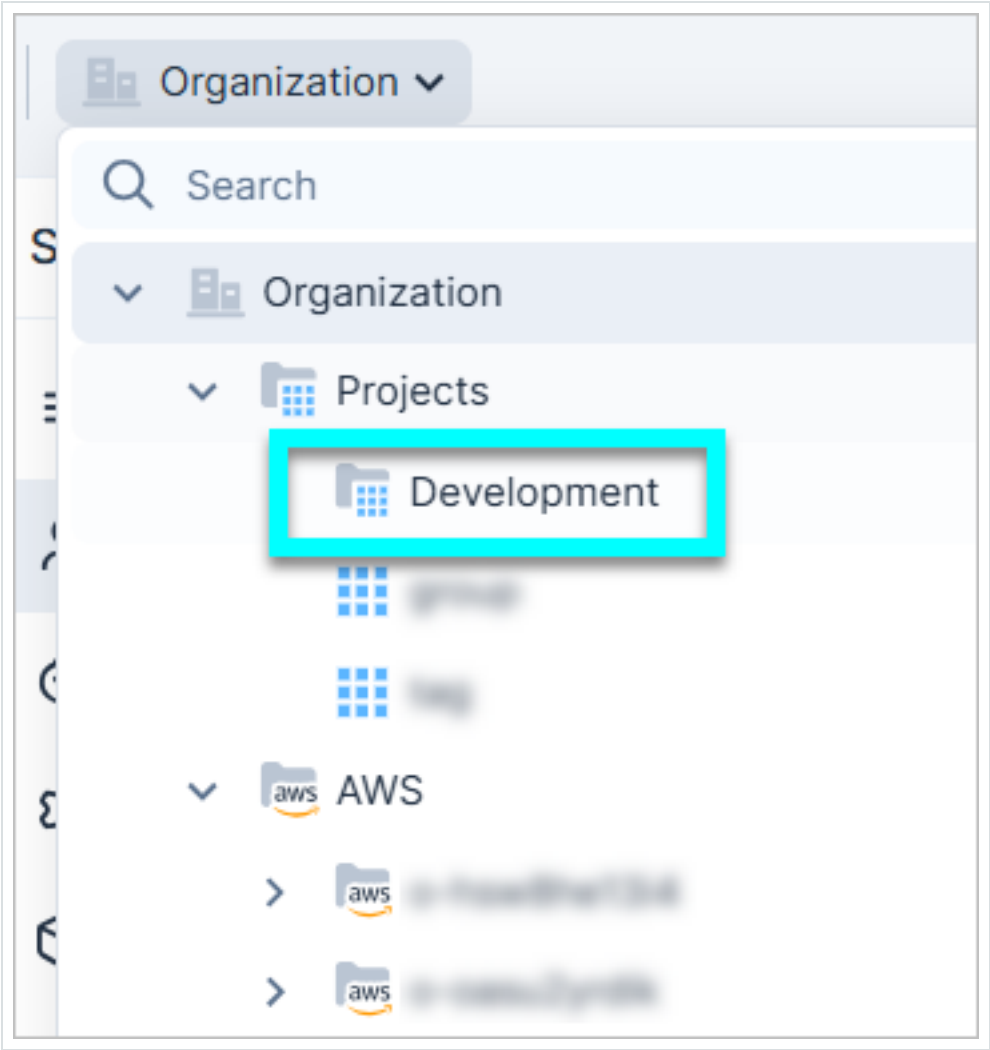
プロジェクトスコープへのアクセスを付与する

システムユーザーによる特定のプロジェクトまたはプロジェクトフォルダーの管理または表示を許可するには、関連するプロジェクトスコープで管理者や閲覧者などのロールを割り当てる必要があります。

注意: ユーザーをプロジェクトスコープに直接割り当てることに加えて、プロジェクトからその含まれるアカウントへユーザー割り当てを自動的に拡張 (伝播) することもでき、これにより手動設定が削減され、一貫したアクセスが確保されます。詳細については、プロジェクトを追加する参照してください。

たとえば、Development プロジェクトへのアクセスを委任するには:

1. **[設定]** > **[アクセス管理]** > **[ユーザー管理]** に移動し、ロールの割り当てを追加します。
2. スコープとして Development プロジェクトを選択します。



3. 適切なロールを選択します。

詳細については、ユーザーとグループ参照してください。

プロジェクトを移動する

必要な Tenable One Cloud Exposure ユーザーロール: このアクションを実行するには、管理者のロールが必要です。詳細については、ユーザーとグループを参照してください。

移動できるのは次の項目です。

- 既存のフォルダーに接続するプロジェクトまたはプロジェクトフォルダー
- root プロジェクトフォルダーに、プロジェクトまたはプロジェクトフォルダー

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アカウント]** > **[プロジェクト]** に移動します。

   既存のプロジェクトは、ページの左側にあるツリーに表示されます。
2. 移動するプロジェクトまたはプロジェクトのフォルダーを選択します。
3. ページの下部で、**[移動]** をクリックします。
4. 移動先フォルダーの場所を選択するか、**[プロジェクト]** を選択してルートフォルダーに移動します。

プロジェクトの削除

必要な Tenable One Cloud Exposure ユーザーロール: このアクションを実行するには、管理者のロールが必要です。詳細については、ユーザーとグループを参照してください。

子プロジェクト/フォルダーを含むフォルダーを削除するには、まず子プロジェクト/フォルダーを削除または移動してください。

プロジェクトを削除する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アカウント]** > **[プロジェクト]** に移動します。
2. 削除するプロジェクトまたはプロジェクトのフォルダーを選択します。
3. ページの下部で、**[削除]** をクリックします。

コンソールデータをプロジェクトでフィルタリングする

コンソール全体のデータは、すべてのコンソールページに表示されるドロップダウンを介して、範囲によってフィルタリングされます。特定の単一のプロジェクト範囲のロールが割り当てられたユーザーには、その範囲でフィルタリングされたクラウドサイバーエクスポージャーコンソールが自動的に表示されます。複数のプロ

ジェクト範囲が割り当てられたユーザーは、特定のプロジェクト範囲内でクラウドサイバーエクスポージャーコンソールの特定の機能を表示および構成できます。

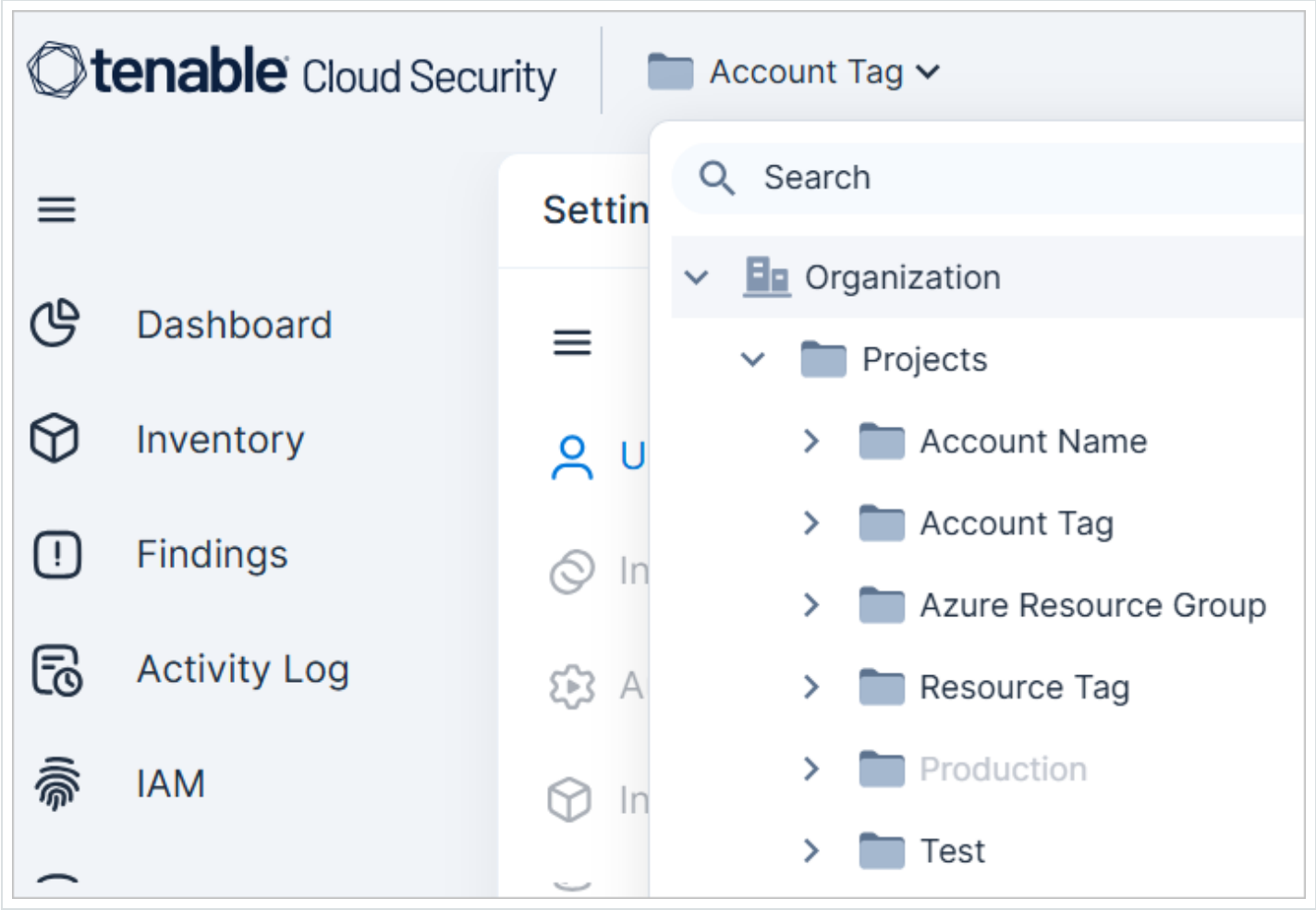
プロジェクト / プロジェクトフォルダーを使用して、次の操作を行うことができます。

- クラウドサイバーエクスポージャーコンソール全体でデータをフィルタリングします。
- クラウドサイバーエクスポージャーコンソールで特定の機能を表示および構成します。

注意: 選択したプロジェクト範囲は、コンソールのページ間を移動しても保持されます。選択した範囲に設定されたままになり、手動で変更しない限りデフォルトに戻ることはありません。

プロジェクトでデータをフィルタリングする方法

- 関連するコンソールページで、スコープドロップダウンをクリックし、プロジェクトまたはプロジェクトフォルダーをスコープとして選択します。

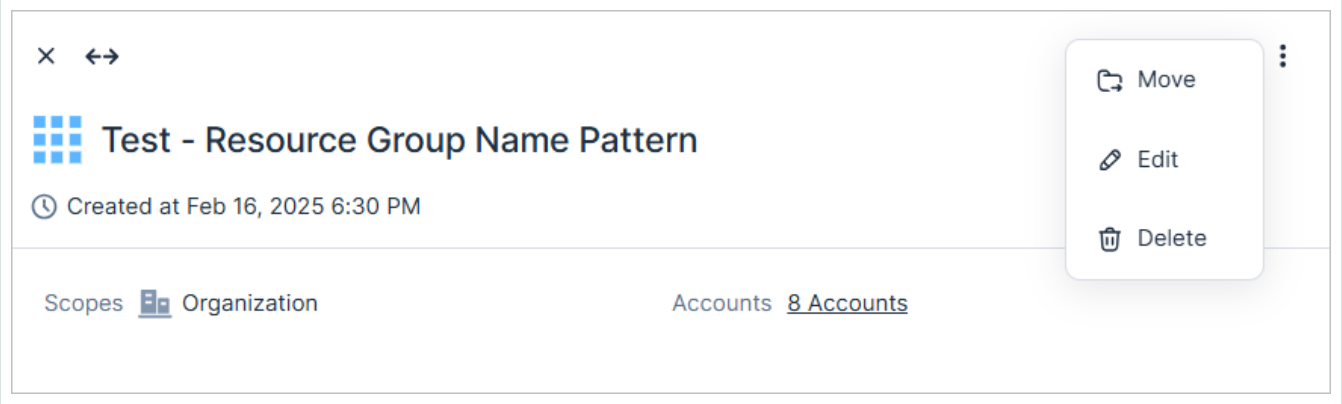


プロジェクトの表示

デフォルトでは、[プロジェクト] ページにはルートフォルダーにプロジェクトとプロジェクトフォルダーが表示されます。

プロジェクトを表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アカウント]** > **[プロジェクト]** に移動します。
2. 次のいずれかを行います。
   - **[平面図]** をクリックすると、すべての子フォルダーで作成されたプロジェクトが表示されます。**[パス]** 列を使用して、各プロジェクトの場所を特定します。
   - 特定のプロジェクトフォルダーをクリックすると、そのフォルダーで作成されたプロジェクトおよびサブフォルダーが表示されます。
3. 特定のプロジェクトをクリックすると、プロジェクトの詳細が表示されます。たとえば、次のことが可能です。
   - プロジェクトが作成された日時を表示します。
   - プロジェクトに含まれるスコープとアカウントを確認します。
   - プロジェクトプロジェクトを移動する 。
   - プロジェクトを編集します。
   - プロジェクトプロジェクトの削除



プロジェクトデータのエクスポート

プロジェクトデータを CSV 形式でエクスポートします。データは、その時点でテーブルに適用されているフィルターに従ってエクスポートされます。

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アカウント]** > **[プロジェクト]** に移動します。
2. 対象のフィルターを適用します。**[平面図]** をクリックすると、すべての子フォルダーで作成されたプロジェクトが表示されます。
3. **[エクスポート]** をクリックします。

アカウント

これは、アカウントを Tenable に接続した後の管理方法ガイドです。

- アカウントの接続方法に関するハウツーガイドについては、サポートされているプロバイダーのリストの統合 を参照してください。
- アカウント階層の概念概要については、「 アカウント階層とフォルダーを参照してください。

[アカウント] ページは、Tenable One Cloud Exposure が監視するすべてのサードパーティアカウントを管理するための中心ハブです。これらのアカウントを一元化することで、スキャン可能なインフラ全体の健全性と接続性を 1 つの統合ビューでモニタリングできます。

- Cloud providers
- アイデンティティプロバイダー
- データプラットフォーム
- オンプレミス
- コンテナレジストリ
- コードリポジトリ

アカウントを管理する

オンボーディングによって クラウドサイバーエクスポージャー に正常に接続されると、そのアカウントは [アカウント] テーブル (Settings [組織] > [アカウント]>) に表示されます。

[アカウント] テーブルからは、次の操作を実行できます。

- アカウントの詳細の表示
- 接続の監視
- 問題のトラブルシューティング
- プロジェクトとフォルダー構造の作成

統一された表には、プロバイダーの種類に関係なく、すべての統合アカウントが表示されます。左側のナビゲーションツリーを使用して、特定のカテゴリで表をフィルタリングできます。

アカウントの列データ

統合されたアカウントの表には、プロバイダーの種類に関係なく、すべての統合アカウントが表示されます。左側のナビゲーションツリーを使用して、特定のカテゴリで表をフィルタリングできます。

列	説明
名前	アカウント名またはリポジトリ名と、関連するプロバイダーアイコン。
ID	アカウントの一意の識別子。
範囲	アカウントが存在する親フォルダーまたは組織レベル。
ステータス	標準化された接続の正常性ステータス。「オンボーディングの問題のトラブルシューティング」を参照してください。
問題	アクセス許可がない、接続の失敗など、特定のエラーを表示します。

コードアカウントを管理する

リポジトリを接続すると、[アカウント] ページの表に表示されます (**Settings [組織] > [アカウント]**>)。

- コードリポジトリの接続を使用してリポジトリを接続した場合、リポジトリはこのページにフォルダーとして追加されます。
- CI/CD の接続を使用してパイプラインを接続した場合、Tenable は関連するプロバイダーと組織に関する情報を識別しようとします。

- 成功すると、リポジトリはこのページにフォルダーとして追加されます。すでにコードリポジトリ統合を使用して追加されている場合は、既存のフォルダーがそのまま残り、再度追加されることはありません。
- 利用可能な情報がない場合、リポジトリは [Other] (その他) フォルダーに追加されます。

組織に多数のリポジトリがある場合は、フォルダーを使用して、クラウドサイバーエクスポージャー内で構造化された階層を維持することが重要です。この構造は、以下の方法で作成できます。

- (推奨)オンボーディングされた組織のリポジトリ構造に基づいて、クラウドサイバーエクスポージャーのフォルダー構造を自動的に更新します。
- Tenable にフォルダーを手動で作成して、オンボーディングされたリポジトリを論理的にグループ化します。たとえば、リポジトリを場所別にグループ化することができます。

> **重要:**
> - リポジトリ: リポジトリフォルダーを追加または移動するには、関連するソースと宛先の組織の [フォルダー構造を自動的に更新する] オプションを無効にする必要があります。このオプションの詳細については、「コードリポジトリの接続」を参照してください。
> - **CI/CD パイプライン**: パイプラインフォルダーは自由に追加または移動できます。

アカウントの詳細の表示

[アカウント] ページでアカウントをクリックすると、詳細なスライド式パネルが表示されます。このパネルにより、1 か所で関連するすべてのアカウントのインサイトに簡単にアクセスできるようになるため、可視性が向上し管理しやすくなります。

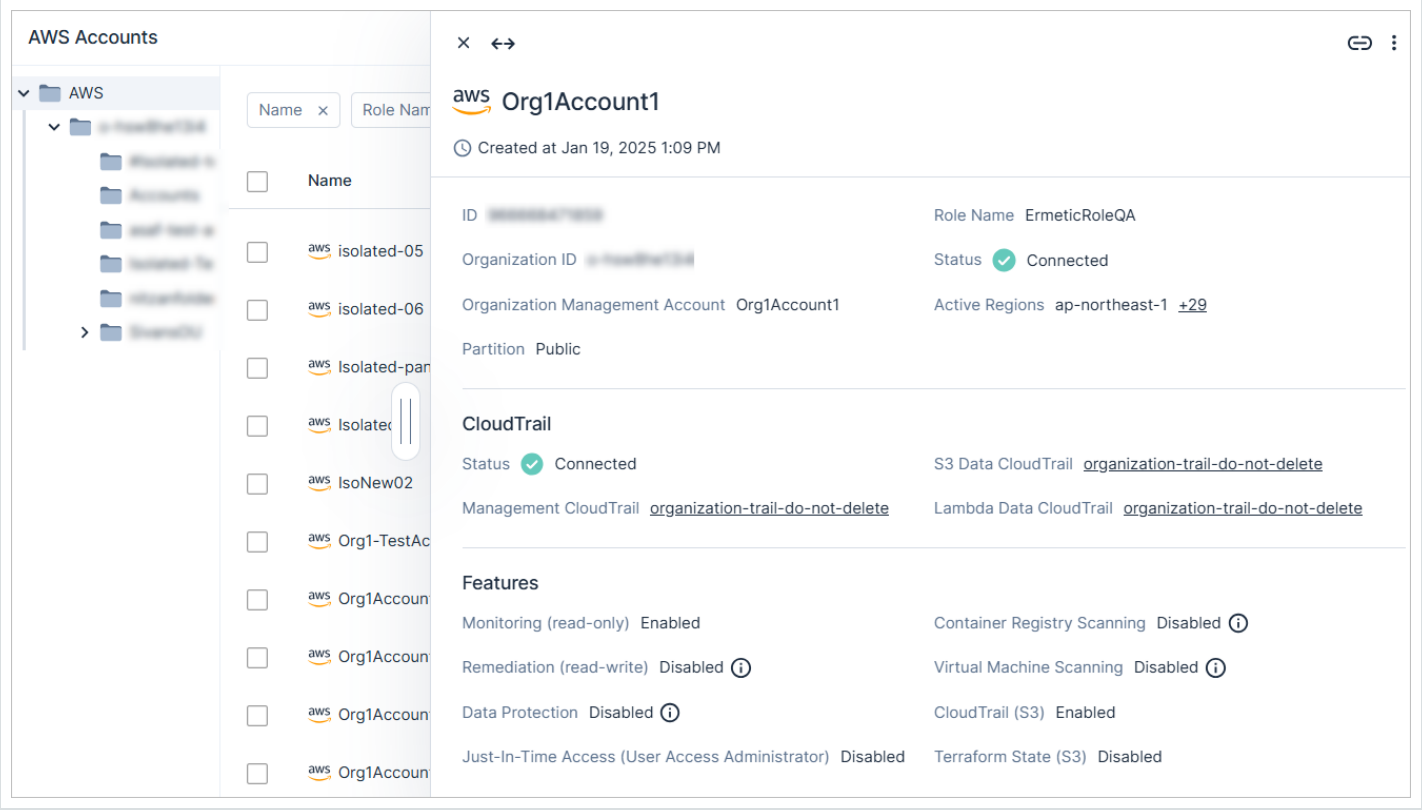
このパネルには以下のような詳細が含まれます。

- アカウント情報。
- 関連付けられている親組織に関する情報。
- クラウドプロバイダーのみ:
  - **CloudTrail** (AWS)。証跡の接続ステータスと、管理、S3 データ、Lambda データの証跡のリスト。詳細については、CloudTrail ログを参照してください。
  - **機能**。関連するプラットフォーム機能のステータス。各機能について、以下を確認できます。

- 有効化または無効化されたかどうか
- 必要なアクセス許可が実際に付与されたかどうかを示すツールチップ

以下に例を挙げます。

- 機能を有効にした場合でも、必要なアクセス許可が実際には付与されていなければ、その機能はアクティブになりません。
- 逆に、機能を無効にしても、必要なアクセス許可がまだ付与されており、その機能が必要ない場合には、アクセス許可の削除を検討することをお勧めします。



アカウントの管理のオプション

[アカウント] テーブルのツールバーでは、次のグローバルアクションを使用できます。

オプション	説明
フォルダー	アカウントを論理的に整理するための新しいフォルダーを追加します。詳細について

オプション	説明
を作成	は、「アカウント階層とフォルダー」を参照してください。
アカウントの追加	クラウドサイバーエクスポージャーに新しい統合を追加します。
プロジェクトを作成	1つ以上のアカウントを選択し、クリックして新しいプロジェクト範囲を開始します。
フラットビュー	デフォルトでは、選択した範囲と親の範囲で定義された項目がテーブルに表示されます。**[フラットビュー]**をクリックすると、子の範囲で定義されている項目も表示されます。
移動	アカウントをクラウドサイバーエクスポージャーフォルダー階層内の別の場所に移動します。ターゲットフォルダーにソースフォルダーと同じ設定済みの統合がない場合は、アカウントを移動できません。
Delete (削除)	クラウドサイバーエクスポージャーからフォルダーまたはアカウントを削除します。アカウントの削除には最大1時間かかる場合があります。クラウドプロバイダーの場合、クラウドアカウントのオフボーディングの一環としてアカウントの削除が必要になる場合があります。

オンボーディングの問題のトラブルシューティング

クラウドサイバーエクスポージャーは、アカウントのオンボーディングプロセス中に問題が発生した場合にトラブルシューティングできるよう、コンソール内にモニタリングとステータスのインジケーターを備えています。アカウントに表示されるステータスから、潜在的な問題を即座に把握できます。

アカウントのオンボーディングを試みた後、通常はコンソールの[アカウント]ページでステータスを確認できます。このステータスは、Tenableがアカウントに正常に接続されているかどうかを示し、注意が必要な領域を特定するのに役立ちます。

アカウントステータス

ステータス	説明
接続済み	統合は健全な状態にあり、想定通りに通信しています。
問題との関連	アカウントは現在運用されていますが、注意が必要な重大ではない問題が検出されました。
失敗	接続は現在切断されているか、通信を妨げる重大なエラーが発生しました。
削除済み	アカウントまたは統合が削除対象としてマークされていますが、現在システムからの削除が保留されています。
除外	アカウントがユーザーによってスキャンまたはモニタリングから除外されました。「除外を参照してください。
現在のライセンスではサポートされていません	既存のサブスクリプション階層内の制限により、アカウントをモニタリングできません。

オンボーディング中によく発生する一般的な問題を以下に挙げます。

- **アクセス許可**: IAM ロール、ポリシー、サービスアカウントのアクセス許可の不適切な設定または欠落。この場合、Tenable がクラウド環境で必要なデータにアクセスしたり、変更を加えたりすることが妨げられる可能性があります。
- **接続性**: クラウドサイバーエクスポージャーとクラウドプロバイダーの間の接続を確立する際の問題。
- **設定**: CloudTrail の設定、アクティブなリージョン、命名規則などの設定でのエラー。

各クラウドプロバイダー固有の詳細なトラブルシューティング手順については、各プロバイダーの関連記事を参照してください。サポートされているプロバイダーのリストについては、「統合を参照してください。

コード

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

これはTenable One Cloud Exposureで、すでに接続されているreposを管理する方法に関するガイドです。

- リポジトリをTenableに接続するためのオンボーディングガイドについては、コードリポジトリの接続参照してください。
- IaC検出結果の監視の方法ガイドについては、IaC検出結果参照してください。
- TenableのCI/CDおよびコード機能の概要については、コード参照してください。

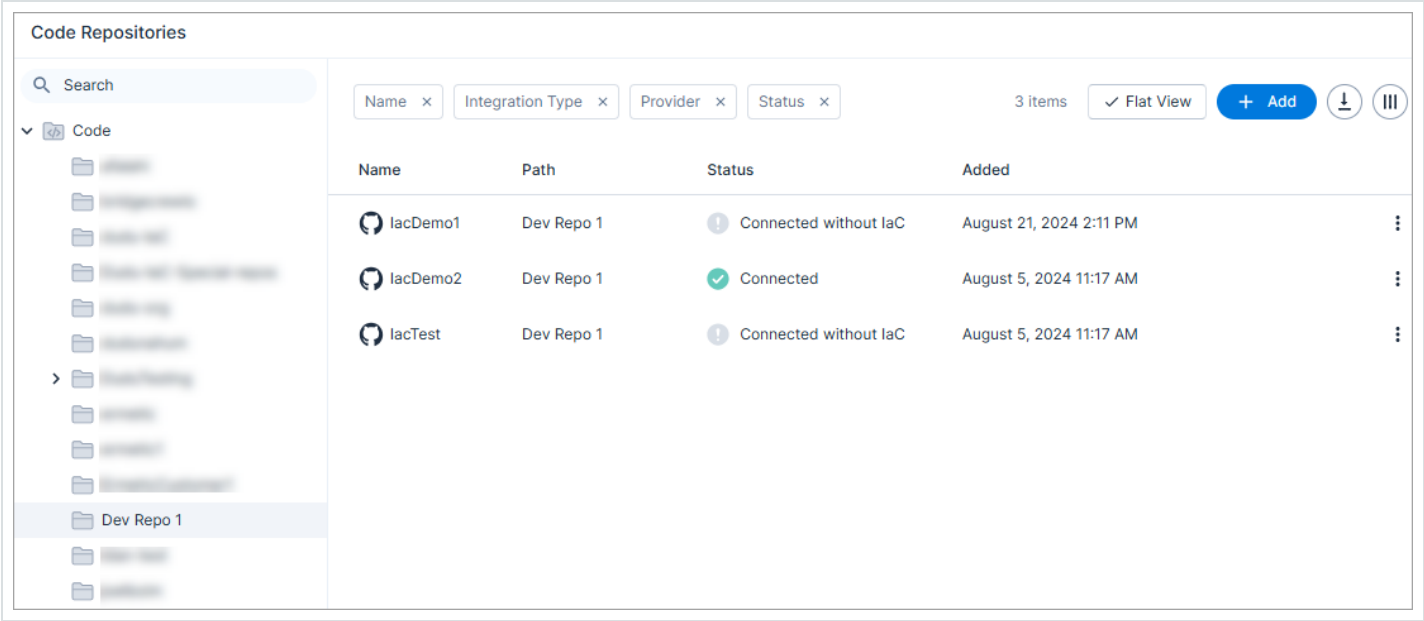
リポジトリを接続すると、[コードリポジトリ] ページの表に表示されます (**[設定]** > **[アカウント]** > **[コード]**)。

- コードリポジトリの接続 を使用してリポジトリを接続した場合、リポジトリはこのページにフォルダーとして追加されます。
- CI/CDの接続 を使用してパイプラインを接続した場合、Tenableは関連するプロバイダーと組織に関する情報の特定を試みます。
    - 成功すると、リポジトリがこのページにフォルダーとして追加されます。すでにコードリポジトリ統合を使用して追加されている場合は、既存のフォルダーがそのまま残り、再度追加されることはありません。
    - 情報が使用できない場合、リポジトリは[その他] フォルダーに追加されます。

コードリポジトリページから、すべてのコードリポジトリの表示、オンボーディング問題のトラブルシューティング、クラウドサイバーエクスポージャーリポジトリの追加、内にフォルダー構造の作成、その他のリポジトリ関連のアクティビティの実行が可能です。

組織に多数のリポジトリがある場合は、フォルダーを使用して、クラウドサイバーエクスポージャー内で構造化された階層を維持することが重要です。この構造は、以下の方法で作成できます。

- (推奨) オンボードされた組織のリポジトリ構造に基づいて、クラウドサイバーエクスポージャーのアカウント階層とフォルダー。
- オンボードリポジトリを論理的にグループ化するために、Tenableにフォルダーを追加して移動する。



フォルダーを追加して移動する

クラウドサイバーエクスポージャーにフォルダーを手動で追加し、オンボードリポジトリを論理的にグループ化できます。たとえば、リポジトリを場所別にグループ化することができます。

重要:

- **リポジトリ**- リポジトリフォルダーを追加または移動するには、関連するソースと宛先の企業に対して[フォルダー構造を自動的に更新]オプションを無効にする必要があります。このオプションの詳細については、コードリポジトリの接続 参照してください。
- **CI/CD パイプライン**: パイプラインフォルダーを自由に追加または移動できます。

フォルダーを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アカウント]** > **[コード]** に移動します。
2. 左側のコードツリーで、フォルダーを作成する場所に移動します。フォルダーは、選択した場所に子フォルダーとして追加されます。デフォルトでは、ルート [Code] (コード) フォルダーが選択されています。
3. **[追加]** > **[フォルダーの追加]** をクリックします。
4. **フォルダー名** を入力し、**[Add] (追加)** をクリックします。

5. オンボードされたリポジトリを新しいフォルダーに移動するには、リポジトリに移動し、3 つのドットメニューをクリックし、**[移動]** をクリックします。
6. 移動先フォルダーを選択し、**[移動]** をクリックします。

管理オプション

[コードリポジトリ] テーブルでは、次のフィールド/オプションを使用できます。

フィールド/オプション	説明
コードツリー	論理カテゴリ別のクラウドサイバーエクスポージャー内のオンボードリポジトリの階層グループ化。詳細については、アカウント階層とフォルダー参照してください。以下のフォルダータイプがコードツリーに表示される場合があります。 • クラウドサイバーエクスポージャーによって自動的に検出されたリポジトリ組織。詳細については、アカウント階層とフォルダー参照してください。 • をフォルダーを追加して移動するフォルダー • Tenable が関連するリポジトリを識別したものの、リポジトリタイプを識別できなかった CI/CD パイプラインを含むその他のフォルダー。
フィルター	関連する検索パラメーターで表をフィルタリングします。 • **名前**。コードリポジトリの名前。 • **統合タイプ**。可能な値: `CI/CD`、`Git organization` • **プロバイダー**。可能な値: `Azure DevOps`、`GitHub`、`GitLab`、`Code` コードは、Tenable が関連するプロバイダーと企業を特定できなかった CI/CD パイプラインを表します。 • **ステータス**。コードリポジトリのステータス

フィールド/オプション	説明
	参照
• **Azure DevOps 組織を追加** • **Bitbucket ワークスペースを追加** • **GitHub 組織を追加** • **GitLab グループを追加** • **フォルダ**  を追加	• Azure DevOps 組織を追加 • Bitbucket ワークスペースを追加 • GitHub 組織の追加 • GitLab グループの追加 • フォルダーを追加して移動する
フラットビュー	デフォルトでは、選択した範囲と親の範囲で定義された項目がテーブルに表示されます。**[フラットビュー]** をクリックすると、子の範囲で定義されている項目も表示されます。
エクスポート	リポジトリデータをエクスポートします。データは、その時点でテーブルに適用されているフィルターに従ってエクスポートされます。出力データは CSV 形式で、関連するアカウントデータをすべて含みます。
列ピッカー	テーブルにどの列を表示するか選択します。
移動	リポジトリを クラウド サイバーエクスポージャー フォルダー階層内で別の場所に移動します。

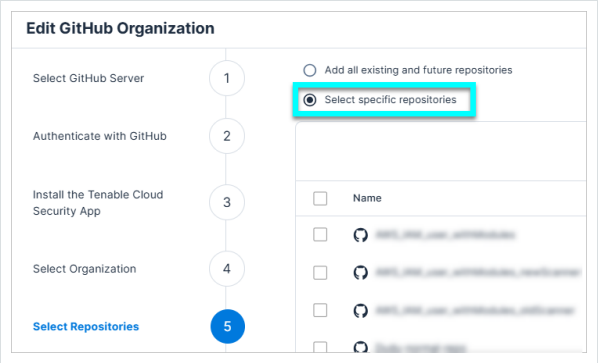
フィールド/オプション	説明
Delete (削除) 	フォルダーまたは CI/CD ベースのリポジトリを から削除します クラウド サイバーエクスポージャーコードリポジトリ統合を介して作成されたリポジトリを削除するには、**[設定]** > **[統合]** > **[コードリポジトリ]** ページで、次のいずれかを実行できます。 • 統合を削除して、組織に関連付けられているすべてのリポジトリを削除します。 • 統合を編集し、関連するリポジトリを除外する。

コードリポジトリのステータス

統合された各コードリポジトリの **ステータス** が確認できます。これは、クラウド サイバーエクスポージャー がリポジトリに接続できるかどうかを示します。

- 接続されると、クラウド サイバーエクスポージャー はリポジトリのコードをスキャン/同期できます。
- 切断されている場合は、関連するリポジトリの コードリポジトリの接続 に従ってください。

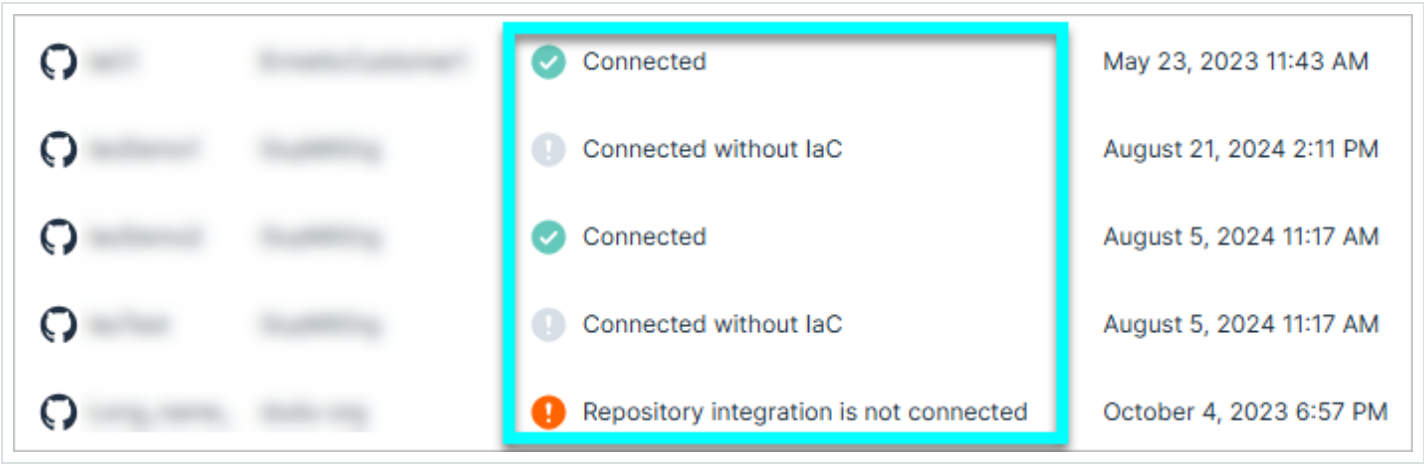
ステータス	説明
接続済み	Tenable はリポジトリに正常に接続され、コードをスキャン / 同期できます。
削除しています...	リポジトリは クラウド サイバーエクスポージャーで削除されましたが、プロセスはまだ完了していません。
IaC なしで接続済み	Tenable は、リポジトリで IaC リソース[1] を見つけることができませんでした。
リポジトリ統合が接続されていません	Tenable はリポジトリに接続できなくなります。関連するリポジトリのすべての コードリポジトリの接続 を実行したことを確認します。

ステータス	説明
リポジトリが見つかりません	Tenable がリポジトリを見つけることができません。これは、クラウドサイバーエクスポージャーで Git プロバイダー統合を構成する際に、特定のリポジトリを選択した後に、Git プロバイダーコンソールでいずれかのリポジトリが削除された場合に発生する可能性があります。
リポジトリがアーカイブされたか、停止されました	リポジトリが、Git プロバイダーコンソールでアーカイブされたか、一時停止されました。

[1] IaC リソース:

- CloudFormation では、IaC リソースは `Resources` セクションで定義されたリソースです。
- Terraform では、IaC リソースは次のようにブロックとして定義されるリソースです。

```
resource <type>  <name> {
...
}
```



セキュリティ

データ

次の設定と範囲を構成して、Tenable One Cloud Exposure がデータをスキャンする方法を微調整します。

- バケットのスキャン範囲の設定
- プライベートバケットのスキャン範囲の設定
- データプラットフォームのスキャン範囲の設定
- スキャンの除外
- 分類の除外
- データタイプ

データスキャンの除外を使用して、アカウント全体または特定のリソースを除外できます。

次の点に注意してください。

- アカウントの除外またはスキャンの無効化によってオプトアウトされたリソースは請求されません。詳細については、「スキャン後の請求が無効になっているをご覧ください。
- これらの設定を行うには、クラウドサイバーエクスポージャーで管理者ロールを持つユーザーである必要があります。

これは、クラウド サイバーエクスポージャー でデータ設定を構成するためのハウツーガイドです。

- データ保護機能の概念の概要については、「 データ保護を参照してください。
- データリソースを Tenableに接続する方法については、「 データリソースの接続を参照してください。
- データリソースの表示と管理に関するハウツーガイドについては、「 データリソースを参照してください。

バケット スキャン

パブリック バケット とプライベート バケット を含むクラウド バケット を クラウド サイバーエクスポージャー がスキャンする方法を設定します。次のことができます。

- **特定のアカウント** または**アカウント スコープ** のスキャンを有効または無効にする
- **プライベート バケット** のスキャンを有効または無効にする
- **プライベート ネットワークアクセス** を使用して、制限された Azure ストレージアカウント へのアクセスを設定する

> **注意:** どのレベルでもスキャンを無効にすると、その範囲内のすべてのデータプラットフォームリソースのスキャンが直ちに停止されます。スキャンが再度有効になるまで、これらのリソースは請求から除外されます。

バケット のスキャン範囲の設定

デフォルト では、クラウド サイバーエクスポージャー は、データのアクセス許可を付与したアカウント のバケット をスキャンします。

特定のアカウント またはアカウント スコープ を除外 するか、親レベルの設定をオーバーライド できます。

この設定は OCI には適用されないことに注意してください。すべてのOCIバケット は、デフォルト でプライベート として扱われます。

バケット スキャンを設定する方法

1. **[Settings > クラウド サイバーエクスポージャー > Data > Buckets]** に移動します。

2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体(すべてのアカウント)が選択されています。これにより、階層内の特定のアカウントまたはアカウントグループに対して、以下の設定を適用できます。
3. [Bucket Scanning] (バケットスキャン) セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。組織全体を範囲として選択した場合、**[継承]** オプションは使用できません。
    - この範囲のスキャンを**有効**または**無効**にします。これにより、親レベルの範囲の設定が、このアカウント範囲固有の設定でオーバーライドされます。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

プライベートバケットのスキャン範囲の設定

クラウドサイバーエクスポージャーが、有効な範囲内でプライベートバケットをスキャンするかどうかを設定できます。

プライベートバケットスキャンを使用するには、バケットスキャンを有効にする必要があります。バケットスキャンが無効になっている場合、プライベートバケットスキャンは自動的に無効になります。

プライベートバケットのスキャンを設定する方法

1. **[Settings > クラウドサイバーエクスポージャー > Data > Buckets]** に移動します。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体(すべてのアカウント)が選択されています。これにより、階層内の特定のアカウントまたはアカウントグループに対して、以下の設定を適用できます。
3. [プライベートバケットのスキャン] セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。組織全体を範囲として選択した場合、[Inherit] (**継承**) オプションは使用できません。
    - この範囲のスキャンを**有効**または**無効**にします。これにより、親レベルの範囲の設定が、このアカウント範囲固有の設定でオーバーライドされます。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

Azure Storage アカウントのプライベートネットワークアクセスの設定

ネットワーク制限のある (プライベートネットワーク経由でのみアクセスできるなど) Azure **ストレージアカウント Blob コンテナ** をスキャンする場合、クラウドサイバーエクスポージャー にはプライベートエンドポイントを使用してデータにアクセスしてスキャンするオプションが用意されています。

デフォルトでは、Azure ネットワークモデルの制限により、クラウドサイバーエクスポージャー はネットワーク制限のある BLOB コンテナにアクセスできません。プライベートエンドポイントを使用すると、他の方法ではアクセスできないセキュリティで保護されたデータを可視化できます。ただし、プライベートエンドポイントの作成時に Azure が DNS レコードを更新する可能性があり、特定の環境のストレージアカウントへのアクセスがブロックされる可能性があるため、この設定を有効にするには DNS 設定を慎重に確認する必要があります。VNet ID を使用して、ルーティング動作を制御し、DNS の問題を解決することもできます。詳細については、クラウドサイバーエクスポージャー サポート担当者にお問い合わせください。

> **重要:** この設定を有効にする前に、Azure ネットワークを確認し、設定 DNSしてください。一部の構成では、Azure がストレージアカウントの DNS 解決をリダイレクトする場合があるため、接続エラーが発生する可能性があります。Azure プライベート DNS ゾーン のインターネットにフォールバックする方法について説明します。

プライベートネットワークアクセスを設定する方法

1. **[Settings > クラウドサイバーエクスポージャー > Data > Buckets]** に移動します。
2. [組織] または **[Azure ツリー]** のドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。これにより、階層内の特定のアカウントまたはアカウントグループに対して、以下の設定を適用できます。
3. [プライベートネットワークアクセス] セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。組織全体を範囲として選択した場合、[Inherit] (**継承**) オプションは使用できません。
    - この範囲のスキャンを**有効**または**無効**にします。これにより、親レベルの範囲の設定が、このアカウント範囲固有の設定でオーバーライドされます。この固有の設定は、親レベルの scope.pe で行われた変更に関係なく、子レベルの範囲に残ります。

データベース

クラウド サイバーエクスポージャー がマネージド データベース環境をスキャンする方法を設定します。**特定のアカウント**または**アカウント スコープ**のスキャンを有効または無効にできます

> **注意:** どのレベルでもスキャンを無効にすると、その範囲内のすべてのデータプラットフォームリソースのスキャンが直ちに停止されます。スキャンが再度有効になるまで、これらのリソースは請求から除外されます。

マネージド データベースのスキャン範囲の設定

デフォルトでは、クラウド サイバーエクスポージャー は、データリソースの接続されたアカウントのマネージド データベースに対してデータ分析スキャンを実行します。

マネージド データベースのスキャンを設定する方法

1. **[Settings > クラウド サイバーエクスポージャー > Data > Managed Database]** に移動します。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。これにより、階層内の特定のアカウントまたはアカウント グループに対して、以下の設定を適用できます。
3. [マネージド データベースのスキャン] セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。組織全体を範囲として選択した場合、[Inherit] (**継承**) オプションは使用できません。
    - この範囲のスキャンを**有効**または**無効**にします。これにより、親レベルの範囲の設定が、このアカウント範囲固有の設定でオーバーライドされます。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

データプラットフォーム

Snowflake から始めて、クラウド サイバーエクスポージャー がデータプラットフォーム環境をスキャンする方法を設定します。**特定のアカウント**または**アカウント スコープ**のスキャンを有効または無効にできます

> **注意:**
>
> - どのレベルでもスキャンを無効にすると、その範囲内のすべてのデータプラットフォームリソースのスキャンが直ちに停止されます。スキャンが再度有効になるまで、これらのリソースは請求から除外されます。

- Snowflakeアカウントでネットワーク制限が実施されている場合は、スキャンを有効にする前にTenable IPからのアクセスを許可してください。必要なスクリプトと手順については、「ネットワークアクセスの許可」を参照してください。

データプラットフォームのスキャン範囲の設定

デフォルトでは、クラウドサイバーエクスポージャーは、データアクセス許可が付与されている、接続されているすべてのSnowflakeアカウントをスキャンします。アカウントまたはフォルダーレベルでスキャンを無効にできます。

データプラットフォームのスキャンを設定する方法

1. **Settings > クラウドサイバーエクスポージャー** > **Data** > **Data Platform** に移動します。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体(すべてのアカウント)が選択されています。これにより、階層内の特定のアカウントまたはアカウントグループに対して、以下の設定を適用できます。
3. [Data Platform Scanning] (データプラットフォームのスキャン) セクションで、以下のいずれかを選択します。

- 親レベルのアカウント範囲の設定を**継承** (デフォルト)。組織全体を範囲として選択した場合、[継承] オプションは使用できません。
- この範囲のスキャンを**有効**または**無効**にします。これにより、親レベルの範囲の設定が、このアカウント範囲またはフォルダー固有の設定でオーバーライドされます。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

スキャンの除外

データスキャンの除外を使用して、データスキャン中にスキップするクラウドリソースクラウドサイバーエクスポージャー定義します。

一般的なユースケースは次のとおりです。

- **コストの最適化**: ライセンス容量を維持するために、重要でない開発またはテストリソースを除外します。

- **環境分離**:「サンドボックス」環境や、すでに他のツールによって監視されているリソースを除外します。
- **機密性の高いサイロ**:「ツールなし」ポリシーを強制する、規制の厳しい環境を除外します。

データスキャンの除外の表示と管理

[データスキャンの除外] テーブルには、アクティブな除外と非アクティブな除外がすべて一元的に表示されます。

1. **Settings > クラウドサイバーエクスポージャー > [Data > Data Scan Exclusions]** に移動します。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。
3. デフォルトでは、選択した範囲と親の範囲で定義された項目がテーブルに表示されます。**[フラットビュー]** をクリックすると、子の範囲で定義されている項目も表示されます。
4. 現在ターゲットとなっている特定のリソースなど、除外に関する詳細を表示するには、除外の行をクリックして詳細ペインを開きます。
5. 除外を管理するには、行の最後にある三点リーダーメニューをクリックして、**[編集]**、**[有効化/無効化]**、**[削除]** のいずれかを行います。

データスキャンの除外ステータス

ステータス	説明
有効	除外が有効で、期限切れでない場合は、次回のスキャンに適用されます。除外の有効期限が切れると、他の除外が適用されない限り、検出対象の検出結果は再オープンされるか元に戻されます。
無効	除外は無効な状態ですが、再度有効にすることができます。
更新を保留中	変更があったため、次回のスキャンで更新されます。

ステータス	説明
無効化を保留中	このあと無効になりますが、スキャンが完了するまでは有効な状態です。
削除の保留中	削除のキューに登録されています。スキャンが完了するまでは有効な状態です。

データスキャンの除外を作成する

除外を作成するときは、エクスプローラー クエリビルダーを使用してターゲットリソースを定義します。このロジックは動的であり、その後クエリパラメーターに一致するリソースは、次のスキャンサイクルから自動的に除外されます。

データスキャンの除外を作成する方法

1. **Settings > クラウドサイバーエクスポージャー** > **[Data > Data Scan Exclusions]** に移動します。
2. [組織] ドロップダウンで アカウント階層とフォルダー を選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. **[+ 除外を追加]** をクリックします。
4. **名前**と**説明**を入力します。
5. **[Excluded Resources] (除外されたリソース)** セクションで、エクスプローラー を使用してターゲットを選択します。
    - **リソースの検索**: ネイティブオブジェクトと汎用オブジェクト (AWS S3 バケットやマネージドデータベースなど) を選択します。
    - **フィルターの追加**: **[+]** をクリックして、リージョン、アカウント ID、タグなどの特定の属性を追加します。

- プレビュー**の確認**: クエリの作成時に、現在ターゲットとなっているリソースのリストが表示されます。

6. **[Save]** (保存) をクリックします。

分類の除外

分類の除外により、Tenable に無視させるデータとその無視する場所を微調整できます。除外する対象 (データタイプ、カテゴリ、機密度、特定の値) と、除外が適用される正確なリソースとデータオブジェクトを定義します。スキャンは引き続きリソース上で実行されるため、他の機密データは引き続き機密扱いされ、請求には影響しません。除外の仕組みの詳細については、「分類の除外」を参照してください。

分類除外の作成

分類除外を作成して Tenable が特定の場所にある特定の機密データを分類しないようにすることで、既知の安全または無関係な一致が検出結果を生成しないようにします。

始める前に

- 範囲を設定するリソースに対してデータ保護が有効になっていることを確認します。

分類の除外を作成する方法

1. クラウド サイバーエクスポージャー コンソールで、**[Settings > Data]** に移動します。
2. **[分類の除外]** タブをクリックします。

   [分類の除外] セクションが既存の除外とともに表示されます。
3. **[+ 分類の除外を追加]** をクリックします。
4. **[名前]** ボックスに、除外の名前を入力します。
5. (オプション) **[説明]** ボックスに説明を入力します。
6. **[データ]** セクションの **[タイプ]** で、次のいずれかのオプションを選択します。
   - **すべてのデータタイプ**を無視します。
   - **特定のデータカテゴリを選択して**から、1 つ以上のカテゴリを選択します。

- **特定のデータの機密性を指定**してから、1 つ以上の機密レベルを選択します。
- **特定のデータタイプを選択して**から、1 つ以上のデータタイプを選択します。

7. **[値]** で、次のいずれかを実行します。
   - 選択したタイプのすべての値を無視するには、**[すべての値]** を選択します。
   - 特定の値のみを無視するには、**[特定の値]** を選択し、ボックスにRE2 正規表現パターンを入力します。正規表現はRE2 構文 に従う必要があります。
8. **[リソース]** セクションで、次のいずれかを行います。
   - スコープ内のすべてのリソースに除外を適用するには、**[すべてのリソース]** を選択します。
   - 除外を特定のリソースに適用するには、**[特定のリソース]** を選択し、クエリを作成してそれらを選択します。
9. **[Data Objects]** セクションで、Tenable がデータを無視する場所を定義します。
   - リソース全体に除外を適用するには、**[すべてのデータオブジェクト]** を選択します。
   - 正確な場所をターゲットにするには、「 **特定のデータ・オブジェクト** 」を選択し、「 **+追加** 」をクリックしてから、1つ以上の場所条件(データベース名 、データベース・スキーマ名 、データベース・テーブル名 、ファイル拡張子 、またはオブジェクト・パス)を追加します。各条件は複数の RE2 正規表現値を受け入れ、Tenable は条件間にOR ロジックを適用します。正規表現はRE2 構文 に従う必要があります。

   手順 6 で **[すべてのデータ タイプ]** を選択した場合 、**[すべてのデータ オブジェクト]** オプションは無効になります。**[特定のデータオブジェクト]** を選択して続行します。
10. **[保存]** をクリックします。

    Tenable が分類の除外を作成し、**[有効]** としてリストします。**[保存] は**、必要な選択を完了した後にのみ使用可能になります。

次の手順

- 除外を変更、無効化、または削除するには、以下の管理手順を参照してください。

分類の除外を管理する

リストから既存の分類除外を編集、有効化、無効化、または削除できます。

分類の除外を管理する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Data]** に移動し、**[Classification Exclusions]** タブをクリックします。

   [分類除外] セクションが表示されます。
2. 除外の行で、アクションメニューをクリックします。
3. 次のいずれかを行います。
   - 除外を変更するには、**[編集]** をクリックし、設定を更新してから **[保存]** をクリックします。
   - 除外のオンまたはオフを切り替えるには、**[有効化]** または **[無効化]** をクリックします。
   - 除外を削除するには、**[削除]** をクリックしてから確認します。

   Tenable が変更を適用し、**[Status]** 列を更新します。

データタイプ

データタイプは、スキャン中にクラウドサイバーエクスポージャーが機密データを識別および分類する方法を定義します。各データタイプには検出ロジックが含まれており、カテゴリ(PCI や PII など) と感度レベルにマッピングされます。これらを組み合わせることで、検出結果のラベル付け方法やリスク深刻度の計算方法が決まります。

データタイプはデータスキャン中に評価され、検出結果、ダッシュボード、リスク計算で使用されます。

クラウドサイバーエクスポージャー サポートされるデータタイプには、次の 2 つのタイプがあります。

- **組み込みデータ型**: メールアドレス、IP アドレス、国別識別子などの一般的な機密データを検出するためにクラウドサイバーエクスポージャーによって提供される事前定義のデータ型。組み込みデータタイプには、デフォルトの検出ロジック、カテゴリ、機密度があり、これらは組織の要件に合わせて設定できます。
- **カスタムデータ型**: 内部識別子、メンバーシップ ID、トランザクションコードなど、組織固有の機密データを検出できるようにするユーザー定義のデータ型です。カスタムデータタイプを作成するときは、検出ロジックを定義し、カテゴリと機密性を割り当てます。

[データタイプ] テーブルには、組み込みデータタイプとカスタムデータタイプの両方と、それらの現在の構成が一覧表示されます。このビューは、アカウント階層とフォルダー が **[組織]** に設定されている場合にのみ

使用できます。**[タイプ]** フィルターを使用して、ソース (組み込みまたはカスタム) 別にデータ型を表示できます。

データ型を編集するして、スキャン中に分類するかどうかを制御できます。

カスタムデータ型の作成

カスタムデータタイプを作成して、内部識別子、メンバーシップ ID、トランザクションコードなど、組織に固有の機密データを分類できます。

機密レベルは検出結果の深刻度に影響するため、カスタムデータタイプを作成するときは、最初に感度レベルを [パブリック] または [プライベート] として選択することをお勧めします。データタイプに他のレベル (社外秘、専有、制限付きなど) が割り当てられている場合、検出されたデータに関連する検出結果の深刻度は 1 レベル上げられます。初期検証時に低い感度を選択すると、リスクの深刻度に影響を与える前に正確な分類を確認できます。

カスタムデータタイプを作成すると、デフォルトで有効になり、次回のデータスキャン後に有効になります。カスタムデータタイプを後で編集し、無効にすることができます。

カスタムデータ型を作成する方法

1. アカウント階層とフォルダーが **[組織]** に設定されていることを確認します。
2. **Settings > クラウドサイバーエクスポージャー > [データ>データタイプ]** に移動します。
3. **[カスタムデータタイプの追加]** をクリックします。
4. 名前 **と** (オプション) **説明** を入力します。
5. **カテゴリ**を選択します。
6. **機密性**レベルを選択します。
7. 次の正規表現フィールドを 1 つ以上設定します。
    - **正規表現を含める**: このデータ型の値を識別するために使用されるパターンを定義します。
    - **正規表現を除外** (オプション): 特定の値を分類対象から除外します。
    - **コンテキスト正規表現** (オプション): ファイル内の列名やパスなど、値の近くにあるキーワードまたはコンテキストを照合します。
      次の点に注意してください。

- 正規表現はRE2構文に従う必要があります。
- 除外は選択したデータタイプにのみ適用されます。

8. **[作成]**をクリックします。

データ型を編集する

組み込みデータ型とカスタムデータタイプの設定を、所属組織の要件に合わせて変更できます。これには、分類や機密レベルの更新、データタイプの有効化または無効化などの変更が含まれます。

これらの調整は、ラベル付けや、検出結果やダッシュボード上でのデータの表示方法には影響しますが、コアスキャンの動作には影響しません。データタイプを編集するには、管理者である必要があります。

次のプロパティを調整できます。

- **カテゴリ**: データ型に別の分類を割り当てます。
- **機密度**: データ型に適用される機密度レベルを設定します。
- **ステータス**:
  - **有効**: データタイプが分類され、検出結果に表示されます。
  - **無効**: データタイプは分類されておらず、検出結果やリスク計算に表示されません。
- **正規表現を除外** (オプション): このデータタイプの分類対象から特定の値を除外します。

カスタムデータタイプの場合、以下を更新することもできます。

- **正規表現を含める**: このデータ型の値を識別するために使用されるパターンを定義します。
- **コンテキスト正規表現**: 列名やファイルパスなど、値の近くにあるキーワードまたはコンテキストと一致します。

データ型を編集する方法

1. アカウント階層とフォルダーが**[組織]**に設定されていることを確認します。
2. **Settings > クラウドサイバーエクスポージャー > [データ>データタイプ]**に移動します。
3. 変更するデータ型を見つけて、三点リーダーメニューを開いて、**[編集]**をクリックします。
4. 必要に応じて、**カテゴリ**、**機密度**、**またはステータス**を更新します。

5. **[値]** で **[正規表現を除外]** を指定して、一致する値を分類から除外します。カスタムデータタイプの場合、**[Include regex]** または **[Context] regex** を更新して検出ロジックを変更することもできます。

   注意:

   - 正規表現は RE2 構文に従う必要があります。
   - 除外は選択したデータタイプにのみ適用されます。
   - 組み込みデータタイプのデフォルト設定に戻すと、設定されたすべての除外正規表現が削除されます。
6. **[保存]** をクリックします。変更は、次回のデータスキャン後に有効になります。

デフォルト分類の復元 (ビルトインデータタイプ)

組み込みデータ型が変更されている場合は、デフォルト設定に戻すことができます。データ型を復元すると、すべてのカスタマイズが即座にクリアされます。

データタイプに **[除外] 正規表現** が含まれている場合、デフォルト設定を復元すると除外正規表現も削除されます。

データタイプのデフォルト設定に戻す方法

1. アカウント階層とフォルダーが **[組織]** に設定されていることを確認します。
2. **Settings > クラウドサイバーエクスポージャー > [データ>データタイプ]** に移動します。
3. データ型を見つけて、三点リーダーメニューを開き、**[デフォルトに戻す]** をクリックします。
4. **[はい]** をクリックして確認します。

カスタムデータタイプの削除

不要になったカスタムデータタイプを削除できます。

現在 クラウドポリシー: カスタムで使用されているカスタムデータタイプは削除できません。

カスタムデータタイプを削除する方法

1. **Settings > クラウド サイバーエクスポージャー** > **[データ>データタイプ]** に移動します。
2. カスタム データ型を見つけて、三点リーダー メニューを開いて、**[削除]** をクリックします。
3. データタイプが使用されている場合は、参照先のカスタムポリシーを一覧表示するメッセージが表示されます。削除を確定するには、**[はい]** をクリックします。

IaC

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

IaC 設定ページで次の設定を行います。
[設定] > **[クラウド サイバーエクスポージャー]** > **[IaC]**

- スキャン失敗しきい値の設定

スキャン失敗しきい値の設定

IaC スキャンエラーがワークフローエラーをトリガーするしきい値を設定します。この設定は、特定のコード アカウントの範囲に対して設定できます。

> **注意:** これらの設定は、統合テーブルで統合の **[編集]** をクリックし、**[組織の選択]** タブに移動して行うこともできます。

スキャン失敗しきい値を設定する方法

1. Tenable One Cloud Exposure コンソールで、**[設定]** > **[クラウド サイバーエクスポージャー]** > **[IaC]** に移動します。
2. [Organization] ツリーのドロップダウンで、[Code] アカウントの範囲 を選択します。
3. [スキャン失敗のしきい値] セクションで、次のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

      > **注意:** 組織全体を範囲として選択した場合、[継承] オプションは使用できません。

- このアカウントスコープ用の一意の設定 (**有効**/**無効**) で、親レベルスコープの設定を**オーバーライドします**。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

4. この設定 **を有効にした** 場合は、ドロップダウンからポリシーの深刻度を選択します。

IAM

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

IAM 設定ページで次の設定を行います。
[設定] > **[クラウドサイバーエクスポージャー]** > **[IAM]**

- アクセス許可使用のラーニング期間
- Microsoft Entra ID 特権ロール

これは Tenable One Cloud Exposureで IAM 設定を構成するためのハウツーガイドです。

- IAM 機能の概念上の概要については、IAMを参照してください。
- 環境内のアイデンティティリスクの調査に関する方法ガイドについては、アイデンティティインテリジェンス参照してください。
- 環境内の特権を持たないアイデンティの処理に関する方法ガイドについては、過剰なアクセス許可参照してください。

アクセス許可使用のラーニング期間

過剰なアクセス許可と非アクティブなアイデンティティに関連するポリシーの評価に使用されるラーニング期間を設定できます。この期間は、検出結果をトリガーするまでに が経過しなければならない時間を決定します。**期間の変更は、検出結果、ラベル、その他のシステム動作に影響します。** たとえば、ラーニング期間を延長した場合、以前にオープンした一部の検出結果がクローズされる可能性があります。。次回の環境で データの同期と更新の頻度 ときに、コンソールに設定変更が適用されます。

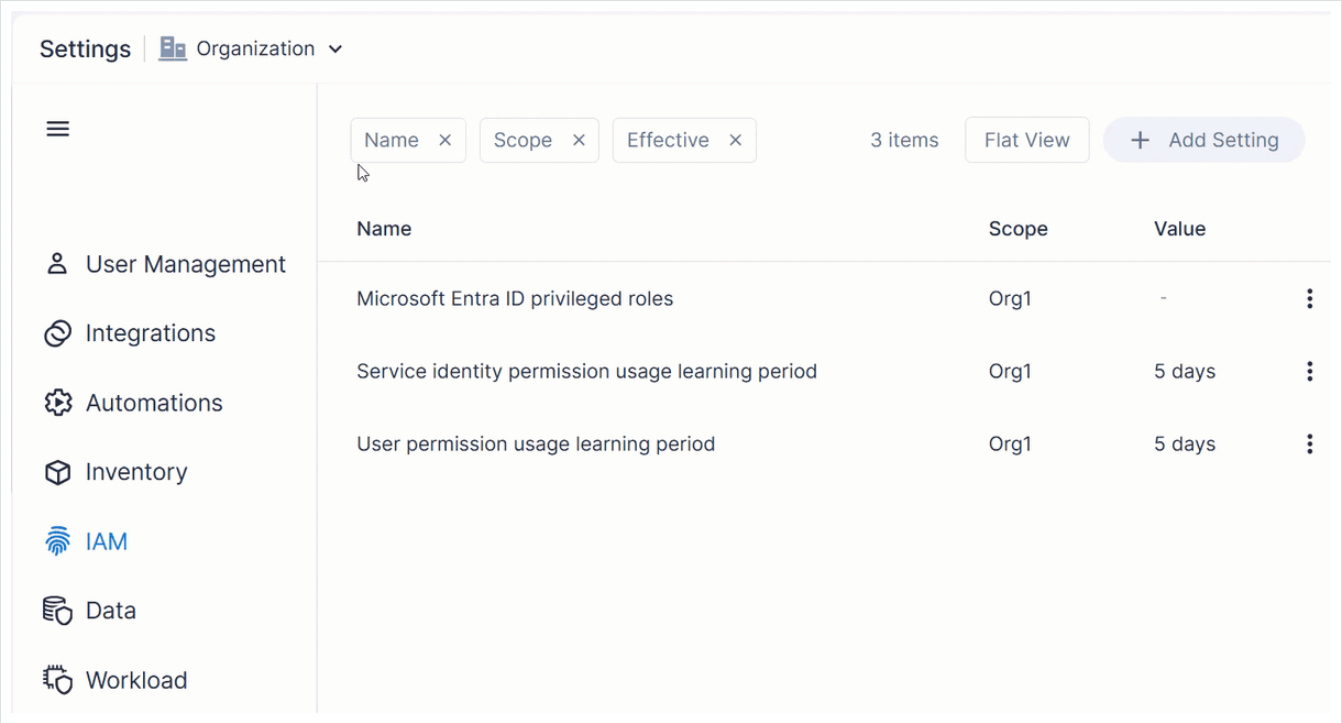
デフォルトでは、クラウドサイバーエクスポージャー は以下のセクションで説明されている期間を使用します。

- 過剰なアクセス許可の定義
- 非アクティブなアイデンティティの定義

アカウント範囲ごとに異なる学習期間を設定できます。特定のスコープに対してラーニング期間を設定する場合は、次のことに注意してください。

- デフォルトでは、子スコープは親レベルのアカウントスコープの設定値を継承します。
- 子スコープに対して独立したラーニング期間を設定した場合、継承された値はそのスコープでオーバーライドされます。
- AWS では、個別のアカウントに対して一意のラーニング期間を設定できます。Azure と GCP の場合、クラウドプロバイダーのすべてのアカウントに対してそれぞれ 1 つの学習期間を構成できます。Azure と GCP で構成された値は、Microsoft Entra ID および Google Workspace ポリシーにそれぞれ影響を与えます。詳細については、影響を受けるポリシーを参照してください。
- 特定の範囲内で、**[有効]** フィルターを使用して、その範囲に適用される実際の学習期間を表示します。たとえば、AWS の範囲内で、「サービスアイデンティティのアクセス許可使用状況の学習期間」に、ルート組織の値とは異なる値を設定したとします。この場合、名前は同じで範囲や値が異なる 2 つのエントリが表示されます。[有効] をクリックすると、ドロップダウンで選択した範囲に適用さ

れるエントリのみが表示されます。



ラーニング期間を変更するには

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[クラウドサイバーエクスポージャー]** > **[IAM]** に移動します。
2. [組織]ドロップダウンで アカウント階層とフォルダー を選択して、アカウントの特定のサブセットの期間を変更します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
    - **AWS**: 個別のアカウントに対して一意の期間を設定できます。
    - **Azure/GCP**: クラウドプロバイダーレベルでのみラーニング期間を設定できます。
3. 次のいずれかを実行します。
    - スコープの新しい設定を追加するには、**[設定の追加]** をクリックします。
    - 既存の設定を編集するには、必要に応じて **[サービス ID]** または **[ユーザーアクセス許可の使用]** のいずれかの横にある 3 つのドットのアイコンをクリックし、**[編集]** をクリックします。

    > **注意:** 構成の編集は、[適用範囲] 列で指定された [適用範囲] に適用され、[適用範囲] ドロップダウンで選択した範囲には適用されません。

4. [設定の追加/編集] ダイアログで、**日数** (1～365) を変更してから **[完了]** をクリックします。

影響を受けるポリシー

次の表は、各クラウド / IdP に対して定義されたラーニング期間 の影響を受けるリソースとポリシーを示しています。

Cloud/IdP	ユーザー/サービス ID	関連するアイデンティティ	影響を受けるポリシー
AWS	ユーザー	• ユーザー • グループ • SSO 権限設定 • IAM ロールサインイン SAML • AWS フェデレーション権限 • SSO ユーザー • SSO グループ	• 非アクティブな IAM ユーザー • 権限のない IAM ユーザー • 非アクティブな IAM グループ • 権限のない IAM グループ • 未使用の SSO 権限セット • 権限のない SSO 権限セット • 非アクティブな IAM ロール SAML でサインイン • 権限のない IAM ロール SAML でサインイン • 権限のない ECR リポジトリ • 権限のない S3 バケットの • 権限のない Secrets Manager のシークレット • 未使用のアクセス許可セットが割り当てられた SSO ユーザー • 未使用のアクセス許可セット

Cloud/IdP	ユーザー/サービス ID	関連するアイデンティティ	影響を受けるポリシー
			が割り当てられた SSO グループ
	サービスアイデンティティ	• IAM ロール • Organization IAM ロール	• 非アクティブな IAM ロール • 権限のない IAM ロール • 権限のない組織 IAM ロール • 権限のない ECR リポジトリ • 権限のない S3 バケットの • 権限のない Secrets Manager のシークレット
Azure/Microsoft Entra ID	ユーザー	• ユーザー • グループ	• サブスクリプションで権限を越える Microsoft Entra ID グループ • サブスクリプションの権限を越える Microsoft Entra ID ユーザー サブスクリプションの • 非アクティブな Microsoft Entra ID ユーザー • 非アクティブな Microsoft Entra ID グループ
	サービスアイデンティティ	• アプリケーション • が管理する ID	• 非アクティブな管理されたアイデンティティによる • 権限のない管理されたアイデンティティ、サブスクリプションに

Cloud/IdP	ユーザー/サービス ID	関連するアイデンティティ	影響を受けるポリシー
			おける権限のない管理された • ID 非アクティブな Microsoft Entra ID アプリケーション、 • サブスクリプションにおける権限のある Microsoft Entra ID のアプリケーション • 非アクティブな Microsoft Entra ID グループ
GCP/Google Workspace	ユーザー	• ユーザー • グループ • Workforce Identity プール	• プロジェクト内の特権 Google Workspace グループ • プロジェクト内の特権 Google Workspace ユーザー • 非アクティブな Google Workspace ユーザー • 非アクティブな Google Workspace グループ
	サービスアイデンティティ	• サービスアカウント • ワークロード ID	• プロジェクト内の • 非アクティブなサービスアカウントの • 非アクティブな Google Workspace グループ

Microsoft Entra ID 特権ロール

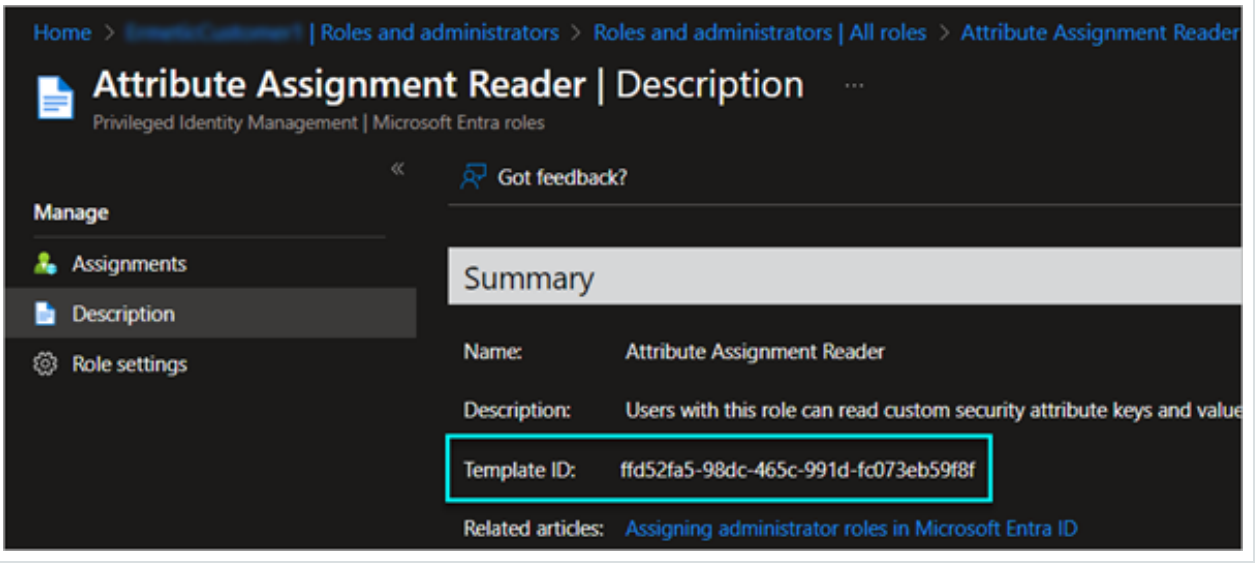
Microsoft は、Microsoft Entra のビルトインロールのサブセットに特権ラベルを割り当てます。これらのロールは、クラウドサイバーエクスポージャー内で特権ロールと見なされます。他の Microsoft Entra 管理ロールも特権ロールとして扱う場合は、Tenable でそのように定義できます。

(Microsoft によって、またはクラウドサイバーエクスポージャーコンソールで定義されるいずれかで) 権限が定義されたロールを持つ Microsoft Entra ID:

- は、関連するポリシーを通じてそのように監視され、検出されます。
- には、**Microsoft Entra ID 権限** ラベルが割り当てられています。

Microsoft Entra 管理ロールを特権として追加するには

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[クラウドサイバーエクスポージャー]** > **[IAM]** に移動します。この構成は、グローバルの組織範囲でのみ使用でき、子の範囲では使用できません。
2. **[ロールの追加]** をクリックし、以下を入力します。
    - **名前**。クラウドサイバーエクスポージャーに表示されるロールの名前。
    - **テンプレート ID**。Azure ポータルで ID を見つけるには、**[Microsoft Entra ID]** > **[ロールと管理者]** に移動し、ロールをクリックし、[管理] で **[説明]** をクリックします。



3. **[追加]** をクリックします。
4. 以前に追加されたロールは **編集** または **削除** できます。

ネットワーク

このセクションでは、Tenable One Cloud Exposure でネットワーク設定を構成する方法について詳しく説明します。

- ネットワークエクスポージャーの概要については、「ネットワークのエクスポージャーを参照してください。
- よくある質問については、「FAQ: ネットワークを参照してください。

[ネットワーク設定] ページで次の設定を行います。

- 内部 IP アドレス
- ネットワークスキャナー

内部 IP アドレス

内部 IP アドレス範囲を許可リストに追加すると、その IP はクラウドサイバーエクスポージャー内でパブリックとは見なされなくなります。信頼できる IP や企業の IP などの IP を追加することで、Tenable でこれらの IP に関連付けられているリソースがパブリックとしてフラグ付けされるのを防ぐことができます。パブリックリソースは、インベントリ、検出結果、ダッシュボード (たとえば、有害な組み合わせウィジェット) に反映されます。

内部 IP アドレス範囲を追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > クラウドサイバーエクスポージャー > Network]** に移動します。この構成は、グローバルの組織範囲でのみ使用でき、子の範囲では使用できません。
2. **[内部 IP アドレス範囲の追加]** をクリックし、次のように入力します。
    1. 意味のある説明的な **名前**。たとえば、企業 IP です。
    2. **内部 IP アドレス範囲**。たとえば、「203.0.113.0/24」と入力します。
3. **[追加]** をクリックします。
4. 以前に追加したロールの編集または削除を行うことができます。

ネットワークスキャナー

有効にすると、ネットワークスキャナーはネットワーク評価でフラグが立てられたリソースを自動的にテストし、確認されたエクスポージャーについてネットワークエンドポイントを作成します。

詳細については、「ネットワークのエクスポージャーを参照してください

ネットワークスキャナーを有効にするには

1. クラウドサイバーエクスポージャーコンソールで、正しい範囲にいることを確認します。
2. **Settings > クラウドサイバーエクスポージャー >ネットワーク**に移動します。
3. **[ネットワークスキャナー]** タブをクリックします。
4. スキャナー行で、三点リーダーメニューアイコンをクリックし、**[編集]** を選択します。
5. [設定の編集] ウィンドウで、**[有効化]** をクリックします。
6. **[保存]** をクリックします。

ベンダー

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

ベンダーとは、通常、AWS IAM ロール、Microsoft Entra ID アプリケーション、GCP サービスアカウント、または統合を通じて、クラウド環境内で運用するサードパーティを指します。これらのエンティティは、サービスを提供するために環境にアクセスする必要があります。ベンダーを正確にマッピングすることで、外部アクセスの可視性が向上し、全体的なセキュリティポスチャーが強化されます。

ベンダー機能を使用すると、サードパーティベンダーのマッピングを管理でき、クラウド環境への外部アクセスの可視性と制御が向上します。

> **注意:**
>
> - ベンダー設定は、**組織** の範囲でのみ使用できます。
> - 現在、この機能でサポートされているのは、AWS アカウントと Microsoft Entra ID アプリケーションのみです。

ベンダーの管理

ベンダーマッピングを追加、編集、または削除して、環境への外部アクセスを正確に把握できます。

新しいベンダーの追加

> **注意:** ベンダーリストは、**ビルトイン** ベンダー(Tenableによってマッピング)と**カスタム** ベンダー(ユーザーが手動で追加)で構成されています。

新しいベンダーを追加する方法

1. Tenable One Cloud Exposureコンソールで、**コンソール> [クラウド サイバーエクスポージャー>ベンダー > Settings**に移動します。
2. **[+ベンダーの追加]** ボタン(右上)をクリックします。
3. 以下を設定します。
    1. ベンダーの名前を入力します。
    2. **[+ 追加]** をクリックして、関連する **AWS アカウント/Microsoft Entra ID アプリケーション/Microsoft Entra ID アプリケーションの所有者/GCP サービスアカウント**を追加します。

        > **注意:** 複数の値を同じベンダーにマッピングできます。
4. (オプション)ベンダーが信頼できる場合は、**[信頼できるものとしてマークする]** を選択します。
   詳細については、「信頼できるベンダー」を参照してください。
5. **[追加]** をクリックします。

ベンダーを編集する

ベンダーを編集する方法

1. クラウド サイバーエクスポージャー コンソールで、[コンソール] > **[クラウド サイバーエクスポージャー>ベンダー>Settings**に移動します。
2. ベンダーエントリの右側にある三点リーダーメニューをクリックし、**[編集]** をクリックします。

ベンダーを削除する

ベンダーを削除する方法

1. クラウド サイバーエクスポージャー コンソールで、[コンソール] > **[クラウド サイバーエクスポージャー>ベンダー>Settings**に移動します。
2. ベンダーエントリの右側にある三点リーダーメニューをクリックし、**[削除]** をクリックします。

> **注意:** 削除できるのは **カスタム** ベンダーのみです。

信頼できるベンダー

信頼できるベンダー機能を使用すると、環境への外部アクセスのタイプを区別できます。

- 不明な外部アクセスがある場合は、調査または削除が必要な場合があります。
- 既知の外部アクセスとは、Tenable またはお客様によってサードパーティベンダーにマッピングされたベンダーを指します。

ベンダーを信頼できるものとして明示的にマークできるため、本当に重要な外部アクセスの監視に集中できます。デフォルトでは、どのベンダーも信頼できるものとして事前設定されていません。信頼できるステータスは、ベンダー 新しいベンダーの追加 で手動で割り当てることができ、コンソールに明確に表示されます。ベンダーを信頼できるものとして設定すると、次回 データの同期と更新の頻度 後に Tenable が変更を適用します。

ベンダーを信頼できるものとして設定すると、次の影響があります。

機能	効果
検出結果	• そのベンダーに関連する**検出結果 1 の深刻度**を自動的に**1 レベル下げ**ます。たとえば、深刻度が [重大] の検出結果が [高] に変わります。 • 外部 AWS アカウント ID を信頼できるベンダーとして設定すると、**外部 IAM ロールの検出結果が生成されなくなります**。
危険な組み合わせ	ベンダーが信頼できると設定されている場合、設定されたベンダーに関連付けられている 危険な組み合わせ はすべて自動的に **クローズ** されます。機密データへのアクセス権を持つサードパーティアイデンティティポリシーに関連しています。

機能	効果
強化された監視	IAM **ダッシュボード**、**インベントリ**、**IAM** ページなど、製品全体の外部アクセスのモニタリングが改善されました。[1]

[1] これは、次のポリシーに影響します。

- AWS
    - 過剰なアクセス許可のある ECR リポジトリ
    - 過剰なアクセス許可のある S3 バケット
    - 過剰なアクセス許可を持つ Secrets Manager シークレット
    - 過剰な権限の IAM ロール
    - Systems Manager パラメーターでシークレットが公開されています
    - EC2 インスタンスでシークレットが公開されています
    - 非アクティブな IAM ロール
- Azure
    - サブスクリプションで過剰な権限を持つ Microsoft Entra ID アプリケーション
    - ロジックアプリでシークレットが公開されている
- GCP
    - プロジェクトで過剰な権限を持つサービスアカウント
    - サービスアカウントは、プロジェクト内のすべてのサービスアカウントになりすますことができます
    - サービスアカウントはプロジェクトで特権を得ています

コンソール全体でのベンダーの可視性

ベンダーマッピングは、Tenable全体のいくつかの機能に影響を与えます。コンソール全体に反映されるのは、環境内に存在し、ベンダー設定 (組み込みまたはカスタムのいずれか) で定義されているサードパー

ティベンダーのみです。これらのベンダーは主要分野に登場し、可視性を高め、サードパーティ追跡を簡素化し、検出結果の精度を向上させています。

- **IAM ダッシュボード**: 特定されたすべてのベンダーは、**[サードパーティベンダー]** というタイトルのウィジェットの下にグループ化されます。詳細については、こちらのドキュメントを参照してください。
- **アイデンティティインテリジェンス**: ベンダーは、アイコン付きで **[Identity Intelligence > Vendor]** 列 > **[Explore** Identity Intelligence] に表示されます。これは、ベンダー設定 (組み込みまたはカスタム) で定義されたベンダーが、サービスアイデンティティを通じて環境にアクセスできる場合に発生します。
- **アクセス許可クエリ**: 外部 AWS アカウントの場合、追加のアカウント ID をベンダーにマッピングすると、そのアカウントはベンダーの名前に関連付けられ、環境への外部アクセスを調査できるようになります。ベンダーが追加されると、[アクセス許可クエリ] ビューで現在 "不明" とマークされているベンダーの名前がベンダーの名前に置き換えられます。
- **インベントリ**: サードパーティベンダーとしてクラウド環境内で動作するアイデンティティは自動的に識別され、関連するインベントリテーブルでマークされます。これらのエントリは、ベンダー名と識別アイコンとともに **[ベンダー]** 列に表示されます。**[ベンダー]** フィルターを使用すると、環境にアクセスできるサードパーティを簡単に特定できます。

ベンダーテーブルの列

縦棒	説明
名前	ビルトインベンダーのベンダーのロゴと名前、またはカスタムベンダーのプレースホルダーのロゴが表示されます
範囲	常に **[組織]** として表示
変更済み	カスタムまたは変更されたビルトインベンダーの場合は **[Yes]** と表示され、その他すべての場合は "-" と表示されます
信頼性	ベンダーが信頼できるか信頼できないかは、**Yes/No** と表示されます
リンクされたサービスアイデンティティ	アイデンティティがベンダーにリンクされているかどうかを示します

ワークロード

[Workload settings] (ワークロード設定) ページで次の設定を行います。
Settings > クラウドサイバーエクスポージャー > ワークロード

- 仮想マシンの設定
- 仮想マシンイメージ
- コンテナレジストリ
- スキャンの除外 (早期利用可能)
- 脆弱性設定
- 終末期の設定
- 悪意のあるファイル

これは、ワークロード設定を構成するためのハウツーガイドです。

- Tenable One Cloud Exposure のワークロード保護機能の概念概要については、「ワークロード保護を参照してください。
- ワークロードの表示と管理に関するハウツーガイドについては、「 VM、VM イメージ、コンテナイメージ、ソフトウェア」を参照してください。
- よくある質問については、「 FAQ: ワークロード保護」を参照してください。

仮想マシンの設定

次の設定を構成して、クラウドサイバーエクスポージャー が環境内の仮想マシンをスキャンする方法を微調整します。

- 仮想マシンのデータディスクスキャンを有効にする
- スキャンから仮想マシンを除外する
- スキャンから仮想マシンを除外する
- スキャンから仮想マシンを除外するかどうか

- 仮想マシンをポリシーから除外する
- 仮想マシンディスクの最大サイズ

仮想マシンスキャンからアカウントを除外する

デフォルトでは、クラウドサイバーエクスポージャーはワークロード ワークロードの接続したアカウントのすべてのインスタンスをスキャンします。ただし、特定のアカウントまたはアカウント範囲をスキャンプロセスから除外するように微調整することもできます。この設定を行うには、クラウドサイバーエクスポージャーで管理者ロールを持つユーザーである必要があります。

> **注意:** このオプションは仮想マシンのスキャンのみを有効化/無効化し、コンテナイメージスキャン有効化/無効化しません。

スキャンからアカウントを除外する方法

1. クラウドサイバーエクスポージャーコンソールで、**[仮想マシン>セキュリティ>ワークロード Settings>]** をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体(すべてのアカウント)が選択されています。
3. [仮想マシンの脆弱性のスキャン] セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

      > **注意:** 組織全体を範囲として選択した場合、[Inherit] (継承) オプションは使用できません。

    - 親レベルの範囲の設定を、このアカウント範囲固有の設定 (**有効** / **無効**) でオーバーライドします。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

仮想マシンデータスキャンの有効化

ワークロード保護の一部として、クラウドサイバーエクスポージャーが仮想マシンの機密データをスキャンするかどうかを設定します。この機能は、既存のワークロード保護スキャンインフラとデータ保護分類エンジンを利用して、シークレット、パスワード、API キーなどの制限付き機密データを含む可能性のあるファイルをサンプリングします。

ワークロード保護を提供する一環として、クラウドサイバーエクスポージャーが仮想マシンの機密データをスキャンするかどうかを管理します。この機能は、既存のワークロード保護スキャンインフラとデータ保護分類エンジンを活用し、シークレット、パスワード、API キーなどのスキャン対象データタイプサンプルファイルを実行します。

注意: 仮想マシンデータのスキャンは、選択した範囲 (継承経由を含む) に対して仮想マシン脆弱性 仮想マシンのデータディスクスキャンを有効にする が有効になっている場合にのみ利用できます。仮想マシン脆弱性スキャンが無効になっている場合、このオプションはグレー表示され変更できません。

仮想マシンデータスキャンを設定する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > クラウドサイバーエクスポージャー > Workload > Virtual Machines]** をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [仮想マシンデータのスキャン] で、**[有効化]** または **[無効化]** のどちらを選択するかを選択します。選択した範囲で 仮想マシンのデータディスクスキャンを有効にする が無効になっている場合、このオプションはグレー表示されます。

仮想マシンのデータディスクスキャンを有効にする

デフォルトでは、Tenable は、仮想マシンに接続されているルートボリュームと、対象となるルート以外のすべてのボリュームをスキャンします。別々のディスクにインストールされているアプリケーションとデータベースは、脆弱性評価に含まれます。ただし、特定のアカウントまたはアカウント範囲をスキャンプロセスから除外するように微調整することもできます。

データディスクスキャンを有効にする方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Security > Workload > Virtual Machines> Virtual Machine Data Disk Scanning]** をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。

3. Virtual Machine Data Disk Scanning セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

      > **注意:** 組織全体を範囲として選択した場合、[Inherit] (継承) オプションは使用できません。

    - 親レベルの範囲の設定を、このアカウント範囲固有の設定 (**有効** / **無効**) でオーバーライドします。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

スキャンから仮想マシンを除外する

デフォルトでは、クラウドサイバーエクスポージャーはワークロード ワークロードの接続したアカウントのすべてのインスタンスをスキャンします。ただし、特定の仮想マシンをスキャンプロセスから除外するように微調整することもできます。除外は、クラウドプロバイダーのタグに基づきます。

> **注意:** お使いのアカウントで [Scan Exclusions] (早期利用可能) にアクセスできる場合は、除外タグの代わりに [Scan Exclusions] (スキャンの除外) を使用してください。スキャンの除外は、タグだけでなくあらゆるリソース属性で一致でき、除外タグがサポートしていないコンテナレジストリもカバーします。

除外タグを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > クラウドサイバーエクスポージャー > Workload > Virtual Machine > Exclusion Tags]** に移動します。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [仮想マシンの除外タグ] セクションで、**[仮想マシンの除外タグの追加]** をクリックします。
4. **タグキー**と**タグ値** (オプション) を入力し、**[追加]** をクリックします。

> **注意:** スキャンからワークロードを除外するために、デフォルトのタグ `tenable-cwp-scan-disabled` が提供されています。このデフォルトタグを使用するか、独自のカスタムタグを作成して、仮想マシンスキャンの除外を管理できます。

仮想マシンをポリシーから除外する

デフォルトでは、クラウドサイバーエクスポージャーポリシーはポリシーの範囲内にあるすべてのリソースに適用されます。これを微調整するために、ポリシーからリソースを除外するして、そのリソースに関連する潜在的な検出結果が作成されないようにすることができます。たとえば、次のことが可能です。

- 特定の仮想マシンを脆弱性のスキャンから除外する
- 除外パターンを定義することによって、一連の仮想マシンを脆弱性のスキャンから除外します。

仮想マシンディスクの最大サイズ

ワークロード保護は、ディスクサイズが最大 600 GiB の仮想マシンに対して有効になっています。詳細を確認するか、この値を変更するには、サポートへの問い合わせ。してください。

仮想マシンイメージ

次の設定を行い、環境内でクラウドサイバーエクスポージャーが仮想マシンイメージをスキャンする方法を微調整します。

- 仮想マシンイメージスキャンからアカウントを除外する
- スキャンから仮想マシンを除外する
- スキャンから仮想マシンイメージを除外する
- 仮想マシンイメージデータスキャンの有効化
- 仮想マシンイメージをスキャンから除外する

仮想マシンイメージスキャンからアカウントを除外する

デフォルトでは、クラウドサイバーエクスポージャーはワークロード ワークロードの接続したアカウントのすべてのインスタンスをスキャンします。ただし、特定のアカウントまたはアカウント範囲をスキャンプロセスから除外するように微調整することもできます。この設定を行うには、クラウドサイバーエクスポージャーで管理者ロールを持つユーザーである必要があります。

> **注意:** このオプションは仮想マシンイメージのスキャンのみを有効化/無効化し、コンテナイメージスキャン有効化/無効化しません。

スキャンからアカウントを除外する方法

1. クラウドサイバーエクスポージャーコンソールで、[Settings > **クラウドサイバーエクスポージャー** > Workload > 仮想マシン**イメージ** > 仮想マシン**イメージ**スキャン] をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [仮想マシン] セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

      > **注意:** 組織全体を範囲として選択した場合、[Inherit] (継承) オプションは使用できません。

    - 親レベルの範囲の設定を、このアカウント範囲固有の設定 (**有効** / **無効**) でオーバーライドします。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

仮想マシンイメージデータスキャンの有効化

ワークロード保護を提供する一環として、クラウドサイバーエクスポージャーが仮想マシンの機密データをスキャンするかどうかを管理します。この機能は、既存のワークロード保護スキャンインフラとデータ保護分類エンジンを活用し、シークレット、パスワード、API キーなどの スキャン対象データタイプサンプルファイルを実行します。

> **注意:** 仮想マシンイメージデータのスキャンは、選択した範囲 (継承経由を含む) に対して仮想マシン脆弱性 仮想マシンイメージスキャンからアカウントを除外する が有効になっている場合にのみ利用できます。無効な場合、このオプションはグレー表示され変更できません。

仮想マシンイメージデータスキャンを設定する方法

1. クラウドサイバーエクスポージャーコンソールで、[Settings > **クラウドサイバーエクスポージャー** > Workload > Virtual Machine Images] をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [仮想マシンデータのスキャン] で、**[有効化]** または **[無効化]** のどちらを選択するかを選択します。選択した範囲で仮想マシンの脆弱性イメージスキャンが無効になっている場合、このオプションはグレー表示されます。

仮想マシンイメージをスキャンから除外する

デフォルトでは、クラウドサイバーエクスポージャーはワークロード ワークロードの接続したアカウントのすべてのインスタンスをスキャンします。ただし、特定の仮想マシンイメージをスキャンプロセスから除外するように微調整することもできます。除外は、クラウドプロバイダーのタグに基づきます。

注意: お使いのアカウントで [Scan Exclusions] (早期利用可能) にアクセスできる場合は、除外タグの代わりに [Scan Exclusions] (スキャンの除外) を使用してください。スキャンの除外は、タグだけでなくあらゆるリソース属性で一致でき、除外タグがサポートしていないコンテナレジストリもカバーします。

除外タグを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > クラウドサイバーエクスポージャー > Workload > [Virtual Machine Images] > [Virtual Machine Image Exclusion Tags]** に移動します。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [仮想マシンイメージの除外タグ] セクションで、**[仮想マシンイメージの除外タグの追加]** をクリックします。
4. **タグキー**と**タグ値** (オプション) を入力し、**[追加]** をクリックします。

注意: スキャンからワークロードを除外するために、デフォルトのタグ `tenable-cwp-scan-disabled` が提供されています。このデフォルトのタグを使用するか、独自のカスタムタグを作成して、仮想マシンイメージスキャンの除外を管理できます。

仮想マシンイメージをポリシーから除外する

デフォルトでは、クラウドサイバーエクスポージャーポリシーはポリシーの範囲内にあるすべてのリソースに適用されます。これを微調整するために、ポリシーからリソースを除外して、そのリソースに関連する潜在的な検出結果が作成されないようにすることができます。たとえば、次のことが可能です。

- 特定の仮想マシンイメージを脆弱性スキャンから除外する
- 除外パターンを定義することによって、一連の仮想マシンイメージを脆弱性のスキャンから除外します。

仮想マシンイメージディスクの最大サイズ

ワークロード保護は、ディスクサイズが最大 600 GiB の仮想マシンイメージに対して有効になっています。詳細を確認するか、この値を変更するには、サポートへの問い合わせ。してください。

コンテナレジストリの設定

次の設定を行い、クラウドサイバーエクスポージャー が環境内のコンテナレジストリをスキャンする方法を微調整します。

- 仮想マシンイメージをポリシーから除外する
- 仮想マシンイメージディスクの最大サイズ

コンテナレジストリの脆弱性スキャンを Tenable で有効化する

デフォルトでは、レジストリスキャンは組織全体で クラウドサイバーエクスポージャー で無効になっています。コンソール設定からスキャンを有効にでき、特定のアカウントまたはアカウントスコープで機能を有効/無効にして微調整できます。この設定を行うには、クラウドサイバーエクスポージャー で管理者ロールを持つユーザーである必要があります。

コンテナレジストリのスキャンを有効にする方法

1. クラウドサイバーエクスポージャー コンソールで、**[Settings > クラウドサイバーエクスポージャー > Workload > Container Registries]** をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. **[Container Registry Vulnerability Scanning]** セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

      > **注意:** 組織全体を範囲として選択した場合、[Inherit] (継承) オプションは使用できません。

    - 親レベルの範囲の設定を、このアカウント範囲固有の設定 (**有効** / **無効**) でオーバーライドします。この固有の設定は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

コンテナイメージの最大サイズ

ワークロード保護は、サイズが 2 GiB までのコンテナイメージに対して有効になっています。詳細を確認するか、この値を変更するには、サポートへの問い合わせ。してください。

スキャンの除外

> **注意:** この機能は早期リリース版として提供されており、変更される可能性があります。機能およびサポートが制限される場合があります。アクセス権のリクエストやフィードバックの提供については、Tenable の担当者までご連絡ください。

[スキャンの除外] を使用して、ワークロードスキャン中にスキップ クラウドサイバーエクスポージャー 仮想マシン、仮想マシンイメージ、コンテナレジストリを定義します。

一般的なユースケースは次のとおりです。

- **コストの最適化**: ライセンス容量を維持するために、重要でない開発またはテストのリソースを除外します。
- **環境分離:** サンドボックス環境や、すでに他のツールによって監視されているリソースを除外します。
- **機密性の高いサイロ**:「ツールなし」ポリシーを適用する、規制の厳しい環境を除外します。

> **注意:** アカウントで除外 タグを使用して仮想マシンまたは仮想マシンイメージをスキャンから除外する場合、Tenable がユーザーに代わって既存のタグベースの除外をスキャンの除外に移行します。除外タグは移行が完了するまで引き続き適用されるため、移行中にスキャン範囲は変更されません。除外タグは、コンテナレジストリをサポートしていません。

スキャンの除外の表示と管理

[スキャンの除外] テーブルでは、アクティブな除外と非アクティブな除外がすべて一元的に表示されます。

1. クラウドサイバーエクスポージャー コンソールで、**[Settings > クラウドサイバーエクスポージャー > Workload > Scan Exclusions]** をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。
3. デフォルトでは、選択した範囲と親の範囲で定義された項目がテーブルに表示されます。**[フラットビュー]** をクリックすると、子の範囲で定義されている項目も表示されます。

4. 現在ターゲットとなっている特定のリソースなど、除外に関する詳細を表示するには、除外の行をクリックして詳細ペインを開きます。
5. 除外を管理するには、行の最後にある三点リーダーメニューをクリックして、**[編集]**、**[有効化/無効化]**、**[削除]** のいずれかを行います。

スキャンの除外ステータス

ステータス	説明
有効	除外が有効で、期限切れでない場合は、次回のスキャンに適用されます。除外の有効期限が切れると、他の除外が適用されない限り、検出対象の検出結果は再オープンされるか元に戻されます。
無効	除外は無効な状態ですが、再度有効にすることができます。
更新を保留中	変更があったため、次回のスキャンで更新されます。
無効化を保留中	このあと無効になりますが、スキャンが完了するまでは有効な状態です。
削除の保留中	削除のキューに登録されています。スキャンが完了するまでは有効な状態です。

スキャンの除外を作成する

除外を作成するときは、エクスプローラー クエリビルダーを使用してターゲットリソースを定義します。このロジックは動的で、次のスキャンサイクル以降、クエリパラメーターに一致するリソースは自動的に除外されます。

注意: 保存された除外は、即時ではなく次のスキャンサイクルに有効になります。クエリに一致するリソースは、そのサイクルが実行されるまでスキャンされ続けられます。

スキャンの除外を作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > クラウドサイバーエクスポージャー > Workload > Scan Exclusions]** をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体(すべてのアカウント)が選択されています。
3. **[+スキャンの除外を追加]** をクリックします。
4. **名前と説明**を入力します。
5. **[Excluded Resources] (除外されたリソース)** セクションで、エクスプローラーを使用してターゲットを選択します。
    - **リソースの検索**: **ワークロードリソース**を選択するか、その下にある特定のタイプ(**仮想マシン**、**仮想マシンイメージ**、**コンテナイメージ**)を選択します。
    - **フィルターの追加**: **[+]** をクリックして、リージョン、アカウント ID、タグなどの特定の属性を追加します。
    - **プレビューの確認**: クエリを構築すると、現在ターゲットとなっているリソースのリストが表示されます。
6. **[Save]** をクリックします。

脆弱性設定

次の設定を行い、クラウドサイバーエクスポージャーが環境内の脆弱性をスキャンする方法を微調整します。

- 脆弱性の深刻度のメトリクス
- 検出結果の最小脆弱性深刻度
- 修正なしの脆弱性の検出結果

脆弱性の深刻度のメトリクス

多様なリスク評価のニーズに対応するために、お客様は希望の脆弱性の深刻度メトリクスを選択できます。利用できるオプションは次のとおりです。

- CVSS (共通脆弱性評価システム)
- VPR (脆弱性優先度格付け)

デフォルトでは、特に指定のない限りCVSSが使用されます。この柔軟性により、組織は深刻度スコアを社内の優先順位付け戦略に合わせることができます。一貫性と信頼性を確保するために、すべてのCVSSスコアはTenable Vulnerability Database (TVDB) のみに基づいています。特定のCVEで複数のCVSSバージョンが利用できる場合は、最も高いバージョンのスコアがデフォルトで選択されます。脆弱性の深刻度評価は、ベンダーが提供する評価に基づいています。それらが利用できない場合は、National Vulnerability Database (NVD) の評価が使用されます。

脆弱性の深刻度メトリクスを選択するには

1. クラウドサイバーエクスポージャーコンソールで、[**Settings** > **クラウドサイバーエクスポージャー** > **Workload** > **Vulnerabilities**] をクリックします。
2. 脆弱性の深刻度メトリクスを選択します。

検出結果の最小脆弱性深刻度

検出結果を作成するには最小深刻度を設定します。デフォルトでは、重大な脆弱性に対して検出結果が作成されます。しきい値を下げると、検出結果の数が増える可能性があります。

検出結果を作成するための最小深刻度を設定する方法

1. クラウドサイバーエクスポージャーコンソールで、[**Settings** > **クラウドサイバーエクスポージャー** > **Workload** > **Vulnerabilities**] をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [検出結果の最小脆弱性深刻度] セクションで、関連する深刻度レベルを選択します。
    - **情報**
    - **低**

- **中**
- **高**
- **重大**

修正なしの脆弱性の検出結果

重大な脆弱性の検出結果の作成方法を設定します。修正のある脆弱性の検出結果のみを作成することで、未解決の検出結果の数を減らせる可能性があります。

重大な脆弱性の検出結果の作成方法を設定する方法

1. クラウドサイバーエクスポージャーコンソールで、[**Settings** > **クラウドサイバーエクスポージャー** > **Workload** > **Vulnerabilities**] をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [修正のない脆弱性の検出結果] セクションで、関連するオプションを選択します。
   - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。
   - **有効** (親レベルの設定をオーバーライド)。**修正あり**の重大な脆弱性の検出結果のみを作成。
   - **無効化** (親レベルの設定をオーバーライド)。**すべて**の重大な脆弱性の検出結果を作成 (修正**なし**のものを含む)。

> **注意:**
> - **[有効]** または **[無効]** を選択すると、親レベルの範囲の設定が、このアカウント範囲固有の設定でオーバーライドされます。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。
> - 組織全体を範囲として選択した場合、[継承] オプションは使用できません。
> - この設定を行うには、クラウドサイバーエクスポージャーで管理者ロールを持つユーザーである必要があります。

終末期の設定

次の設定を構成して、OS EOL 検出結果のしきい値を微調整します。

オペレーティングシステムのサポート終了検出結果のしきい値

仮想マシン、仮想マシンイメージ、コンテナイメージに対するオペレーティングシステム (OS) のサポート終了 (EOL) 検出結果のしきい値を設定できます。Tenable がサポートするこの機能強化により、ユーザーはリソースの OS サポートが終了するとき、またはサポート終了が近づいたときに検出結果をトリガーするしきい値を定義できます。これにより、可視性が向上し、プロアクティブなリスク管理が可能になります。

しきい値を設定するには

1. クラウド サイバーエクスポージャー コンソールで、**[Settings > クラウド サイバーエクスポージャー > Workload > End-of-Life]** に移動します。
2. 必要な EOL しきい値を設定します。

> **注意:** サポート終了アラートのしきい値のデフォルト値は **30 日** です。

Malicious File Settings

次の設定を行い、環境内で悪意のあるファイルを クラウド サイバーエクスポージャー がスキャンする方法を微調整します。

- スキャンからアカウントを除外する
- 信頼できるファイルを追加する

スキャンからアカウントを除外する

デフォルトでは、クラウド サイバーエクスポージャー は、ワークロードの接続したアカウントにあるすべてのワークロードをスキャンします。ただし、特定のアカウントまたはアカウント範囲をスキャンプロセスから除外するように微調整することもできます。この設定を行うには、クラウド サイバーエクスポージャー で管理者ロールを持つユーザーである必要があります。

スキャンからアカウントを除外する方法

1. クラウド サイバーエクスポージャー コンソールで、**[Settings > クラウド サイバーエクスポージャー > Workload > Malicious Files]** をクリックします。
2. **[組織]** ツリーのドロップダウンでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。

3. [Malware Scanning] (マルウェアのスキャン) セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

      > **注意:** 組織全体を範囲として選択した場合、[Inherit] (継承) オプションは使用できません。

    - 親レベルの範囲の設定を、このアカウント範囲固有の設定 (**有効** / **無効**) でオーバーライドします。この固有の設定は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

信頼できるファイルを追加する

信頼できると見なされるファイルの SHA-256 ハッシュを指定します。この設定を行うには、クラウドサイバーエクスポージャーで管理者ロールを持つユーザーである必要があります。

> **注意:** (一元化された Settings 領域を介して) 次の手順で説明されているハッシュを入力するだけでなく、アドホックベースで次の場所にあるファイルを信頼できるものとしてマークすることもできます。
>
> - [Malicious Files] ページ経由で送信されます。
> - [Overview] (概要) または [Remediation] (修正) タブの関連する検出結果を使用します。

信頼できるファイルを追加するには

1. クラウドサイバーエクスポージャーコンソールで、[**Settings** > **クラウドサイバーエクスポージャー** > **Workload** > **Malicious Files**] をクリックします。
2. 左側の **[Organization] (組織)** ツリーでアカウント階層とフォルダーを選択し、除外が適用されるアカウントを決定します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [信頼できるファイル SHA-256 ハッシュ] セクションで、**[追加]** をクリックします。
4. ファイルの **SHA-256** ハッシュを入力します。
5. (オプション) **コメント**を入力します。
6. **[追加]** をクリックします。テーブルにエントリが表示されます。
7. エントリを削除するには、エントリの横にある三点リーダーアイコンをクリックし、**[削除]** をクリックします。

秘密

注意: この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

Tenable One Cloud Exposure は、クラウドリソース設定やインフラコードに埋め込まれている、漏洩したシークレット (アクセスキー、トークン、パスワードなど) をスキャンします。これらのシークレットは検出されると、関連する検出結果に表示され、セキュリティチームがリスクを評価して修正するのに役立ちます。

秘密を管理するその他の方法:

- 検出結果からシークレットを除外する: 特定のキー/値のパターンを検出から除外し、誤検出を減らします。
- 除外されたシークレットの表示と管理各ポリシーの除外されたシークレットを表示および管理します

シークレットマスキング

シークレットの値は、通常はクラウド環境でアクセスできないユーザーでも、**[検出結果]** ビューまたは **[インベントリ]** ビューで直接表示できることがあります。

平文のシークレットが漏洩するリスクを軽減するため、シークレットマスクにより、組織はクラウドサイバーエクスポージャーコンソール全体でシークレットの値を修正することができます。有効にすると、すべての秘密値が `<REDACTED>` に置き換えられます。

注意: シークレットマスクは、IaC または KSPM ポリシーによって検出されたシークレットに適用されません。

Secret Master を有効にする方法

1. クラウドサイバーエクスポージャーコンソールで、**[組織の]** アカウント階層とフォルダー が選択されていることを確認します。
2. **[設定]** > **[クラウドサイバーエクスポージャー]** > **[シークレット]** に移動します。
3. [Secret] マスク行で、3 つのドットのメニューアイコンをクリックし、**[編集]** を選択します。
4. [設定の編集] ウィンドウで、**[を有効にする]** をクリックします。
5. **[保存]** をクリックします。

統合

[統合] ページでは、組織内のすべてのサードパーティ接続を一元的に表示できます。このページから、外部データソースの状態をモニタリングし、接続の問題を特定し、新しい統合を追加することでセキュリティエコシステムを拡張できます。

> **注意:** 一部の統合は、Cloud Vulnerability Management ライセンスでは使用できません。

統合の詳細を表示する

統合の詳細を表示する方法

- 特定の統合を見つける方法
  - **フィルター**: テーブルの上部にあるフィルターをクリックすると、特定の条件に基づいてリストを絞り込みます。
  - **フラットビュー**:

    デフォルトでは、選択した範囲と親の範囲で定義された項目がテーブルに表示されます。**[フラットビュー]** をクリックすると、子の範囲で定義されている項目も表示されます。
- 接続の問題をトラブルシューティングするには、**[ステータス]** 列と **[問題]** 列を確認します。
- テーブル内の任意の統合をクリックしてプロファイルスライド式パネルを開き、主要な設定と接続の詳細を確認できます。
- 組織 (クラウドプロバイダー、コンテナレジストリ、コードリポジトリ) の場合は、**[アカウント]** タブも表示できます。このタブには、組織が管理しているすべての関連付けられているアカウントに関する重要な詳細が一覧表示され、アカウントごとの管理機能が提供されます。

統合テーブル

[統合] テーブルには、各接続に関する次の情報が表示されます。

列	説明
名前	特定の統合インスタンスのユーザー定義名。
範囲	統合が適用される組織レベルまたはアカウント。

列	説明
タイプ	特定のプロバイダー、サービス、またはアカウント。たとえば、AWS、Jira、ServiceNow など
カテゴリー	クラウドプロバイダー、SIEM、アイデンティティプロバイダーなどの機能分類。
作成時間	統合が最初に設定された日時。
問題	接続が中断した場合に、特定のエラーメッセージまたはアラートを表示します。
ステータス	[接続済み] (緑) や [失敗] (赤) などのリアルタイムの正常性インジケーター。

新しい統合を追加する

追加のリソース、ツール、サードパーティ製品を Tenable に接続することで、可視性を広げます。

統合を追加する方法

1. [統合] ページで、右上にある **[統合の追加]** をクリックします。
2. 統合ライブラリで、関連する統合を検索または選択します。統合ライブラリには、組織レベルとアカウントレベルの両方の統合 (AWS、Azure、GCP アカウントなど) が含まれています。

これらの統合を接続する方法に関するハウツーガイドについては、以下の記事を参照してください。

カテゴリ	統合
クラウドプロバイダー	AWS の概要、Alibaba Cloudの概要、Azure の概要、GCP の概要、OCI テナンシの接続 の組織とアカウント
アイデンティティプロバイダー	Microsoft Entra ID テナントの接続、Google Workspace の接続、Okta 組織の接続、OneLogin アカウントの接続、Ping Identity 環境の接続
データプラット	Snowflake の接続

カテゴリ	統合
フォーム	
コンテナレジストリ	コンテナイメージレジストリ: サードパーティ、JFrog、Cloudsmith
コードリポジトリ	GitHub 組織の追加、GitLab グループの追加、Azure Repos 組織の追加、Bitbucket ワークスペースの追加
CI/CD	CI/CD の接続、コンテナイメージ CI/CD パイプラインの接続: Azure Pipelines、GitHub Actions、GitLab CI/CD、Jenkins Pipelines、Terraform Cloud、汎用
Kubernetes	Helm チャートを介してクラスタを接続する、Amazon EKS、Azure AKS、Google GKE による設定
チケッティング	Jira、ServiceNow
コラボレーション	Slack、Microsoft Teams
SIEM	Datadog、QRadar、Splunk、SQS キュー、Webhooks: Microsoft Sentinel、Sumo Logic、Telegram
ネットワーク	ネットワーク分離されたサーバーの接続

監査

Tenable One Cloud Exposure コンソール内で実行されたユーザーアクションに関する監査ログ情報を表示します。たとえば、以下を監視できます。

- ユーザー管理、クラウドアカウントのオンボーディング、クラウドサイバーエクスポージャーとサードパーティツールとの統合などの管理アクティビティ
- 未解決の検出結果と解決済みの検出結果
- 検出結果の修正

注意: 次の操作も実行できます

- 監査ログデータをサードパーティツールに送信するオートメーションを作成します。詳細については、自動化 参照してください。
- GraphQL API 経由で監査ログデータにプログラムでアクセスします 。

監査ログ情報を表示する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[監査]** に移動します。
2. テーブルをフィルタリングして、表示するデータの範囲を絞り込みます。各アクションエントリには、以下に関する情報が一覧表示されます。
    - 時間 - アクションが実行された日時 (監査ログを表示するユーザーのローカル時間に基づく)。
    - User - アクションを実行した人 デフォルトでは、すべてのユーザーがフィルターで選択されています。デフォルトでは選択されていませんが、システムアクション (検出結果が作成または更新されたときなど) をフィルタリングすることもできます。
    - アクション - 実行されたアクション。以下に例を挙げます。
        - アカウントの追加
        - ユーザーを追加
        - 作成/更新された自動化ルール
        - 検出結果の更新
        - ユーザーのサインイン / サインアウト
    - 結果 - アクションが成功したか失敗したか
    - 範囲 - アクションが実行されたアカウント デフォルトでは、すべてのアカウントがフィルターに含まれています。
    - 記
3. 現在フィルタリングされている監査ログの結果を CSV ファイルにエクスポートします。

インベントリ (プロパティとラベル)

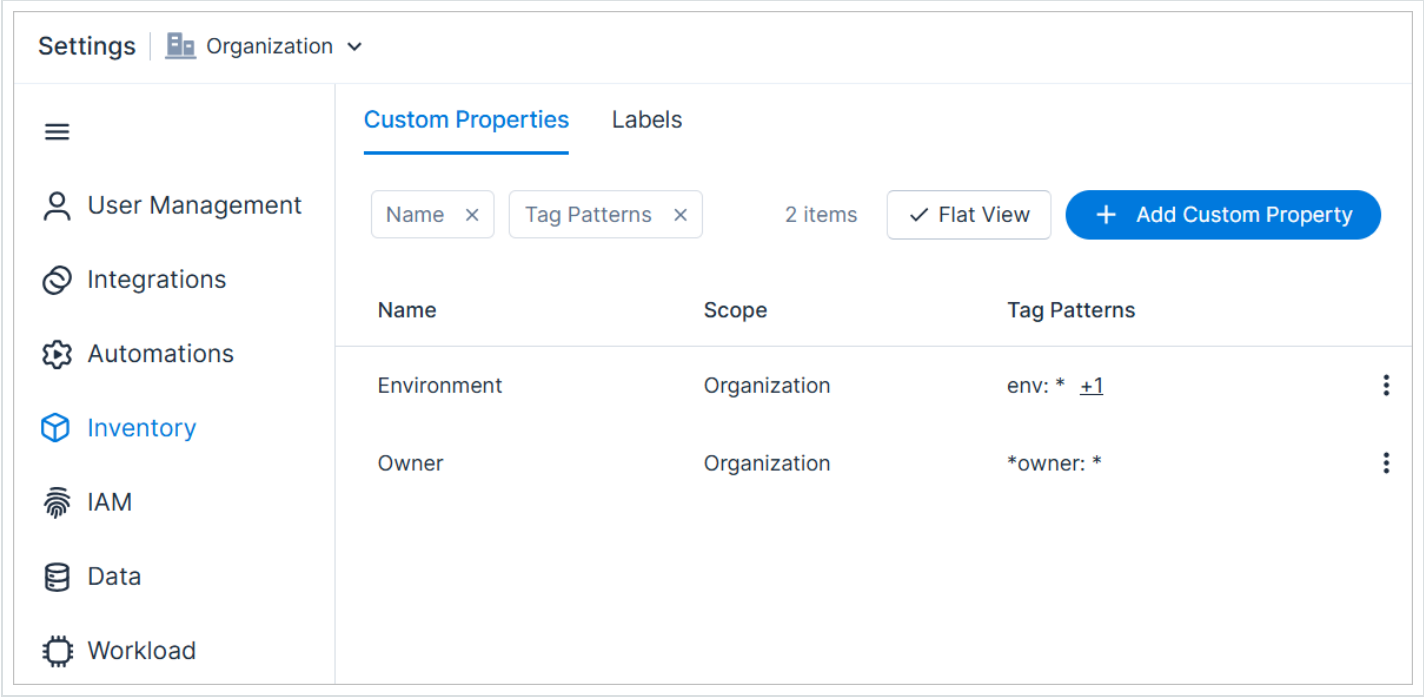
リソースに適用できる カスタムプロパティを管理する と ラベルを管理する を追加して、次の操作を行います。

- リスク評価の追加コンテキストを追加します。
- 過剰なアクセス許可やネットワークの露出 (ラベル) などの要素と相関関係を取れるようにすることで、環境をさらに強化することができます。
- Tenable One Cloud Exposure (カスタムプロパティ) で特定の検出結果が作成された場合、リソースの所有者に通知を送信します。

たとえば、機密度の高いバケットやデータベース、または脆弱性のあるインスタンスにラベルを適用できます。

カスタムプロパティを管理する

カスタムプロパティは、クラウドタグパターン (キーと値のペア) を使用して自動的に入力することも、ユーザーが インベントリのカスタムプロパティの編集 することもできます。**Settings > [インベントリ] > [カスタムプロパティ]** のテーブルからカスタムプロパティを管理します。



項目	説明
名前	カスタムプロパティの名前。

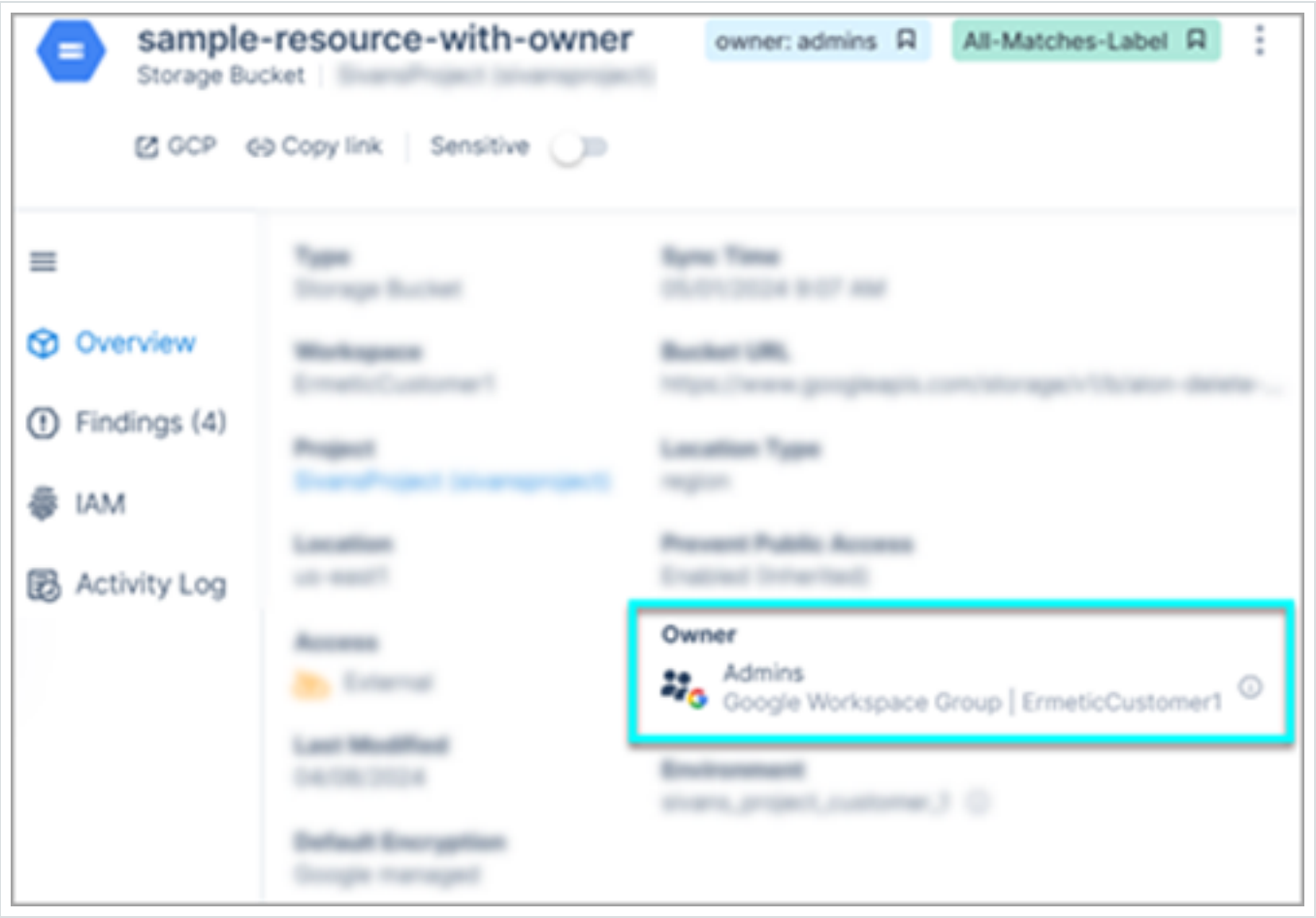
項目	説明
範囲	クラウドサイバーエクスポージャーフォルダー構造内のアカウント階層とフォルダー。カスタムプロパティが設定されたアカウントの範囲を示します。アカウントのパスは動的であり、アカウントが別のフォルダーに移動されると変更されます。
タグパターン	タグのキーまたはパターンで見つかったテキストパターンに基づくタグのキーと値のペア。0個以上の文字を示す場合は * を使用し、単一の文字を示す場合は ? を使用します。定義したパターンに一致するキーと値のペアでタグ付けされたリソースには、カスタムプロパティが入力されます。
フラットビュー	デフォルトでは、選択した範囲と親の範囲で定義されたプロパティがテーブルに表示されます。**[フラット ビュー]** をクリックすると、子スコープで定義されているラベルも表示されます。
カスタムプロパティを作成	新しいカスタムプロパティを作成します。
編集	プロパティを編集します。現在選択されている範囲で作成されたカスタムプロパティで使用できます。
Delete (削除)	プロパティを削除します。現在選択されている範囲で作成されたカスタムプロパティで使用できます。

リソース所有者

所有者タグは、クラウドプロバイダー全体で使用され、特定のリソースの所有者とメインユーザーを示します。所有者タグには、単一のユーザーまたはグループを設定できます。

Tenable は、統合されているすべての統合内でユーザー/グループを検索し、タグパターンに一致するエンティティを表示します。Tenable はまず、タグパターンに基づいて一致するメールアドレスを検索します。次に、グループの場合、Tenable は関連するグループ名を検索します。何も見つからない場合、所有者は「不明なプリンシパル」としてリストされます。

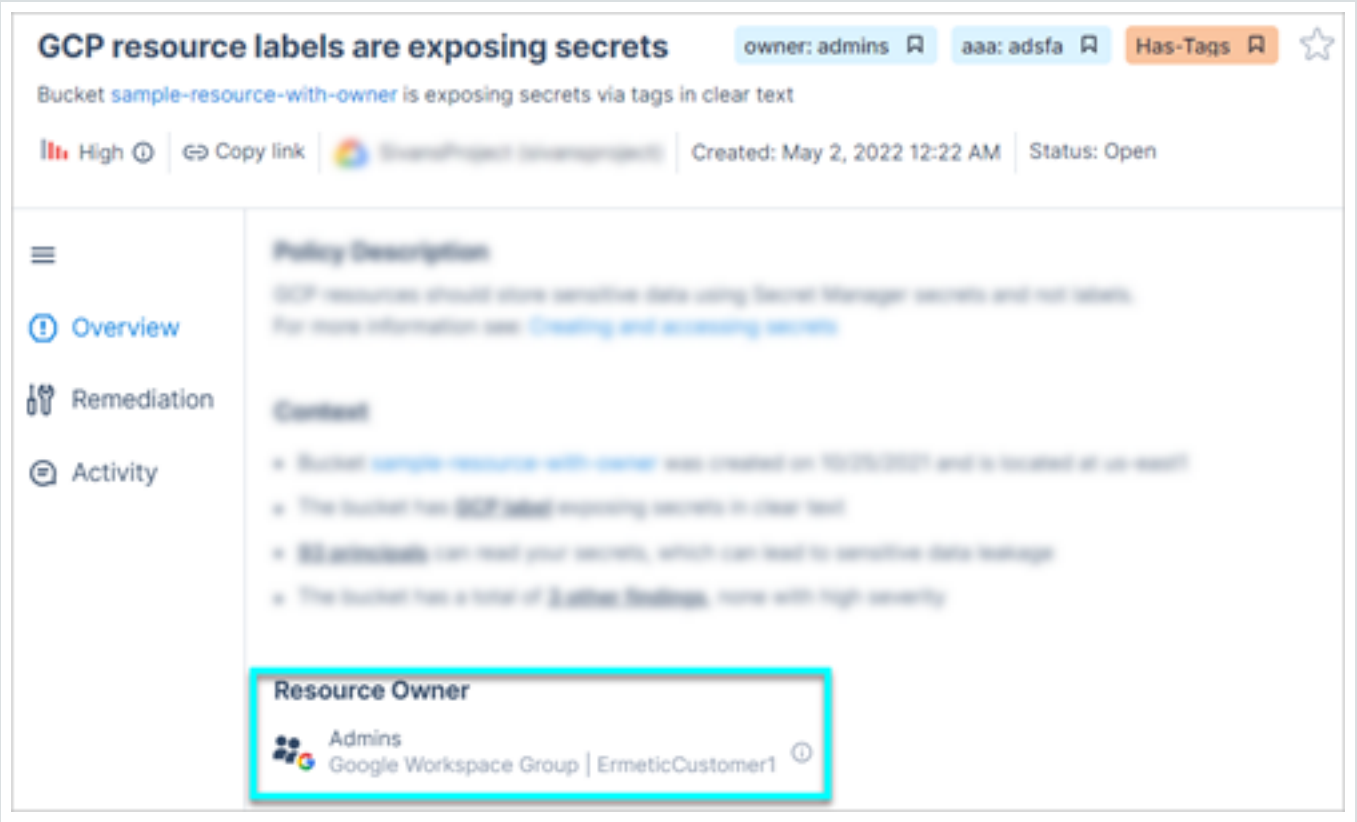
クラウド サイバーエクスポージャー では、複数の個別の所有者を 1 つのリソースに割り当てて、複雑な責任共有モデルを反映させることができます。これにより、問題の連絡は、その問題に関連のある所有者に届くようになり、アラート疲れが軽減されます。たとえば、アプリケーション所有者とプラットフォームエンジニアの両方を定義できます。



インベントリのカスタムプロパティの編集に表示されるだけでなく、次のことを行います。

- 所有者カスタムプロパティは、所有者プロパティが適用されているリソースが関連付けられた検出結果に表示されます。
- このような検出結果をメールで共有する場合、すべてのリソースの所有者に送信することができます。詳細については、自動化とクラウドの検出結果を参照してください。

- 検出結果レポートを作成するときに、**リソースの所有者ごとにメールを送信する**ことを選択すると、各リソースの所有者に自身のリソースに関連付けられた検出結果のレポートを送信することができます。



カスタムプロパティの継承

アカウントレベルやプロジェクトレベルなど、より高い組織範囲で定義されたカスタムプロパティは、その範囲内のすべてのリソースに継承されます。これにより、個別に定義することなく、多数のリソースにまたがってプロパティを効率的に適用できます。この継承メカニズムにより、コンテキスト情報で環境を強化する強力な方法が提供されます。たとえば、GCP プロジェクトに `product:security-tool` がタグ付けされている場合、仮想マシンなど、そのプロジェクト内のすべてのリソースが自動的に `product:security-tool` タグを継承します。

カスタムプロパティの追加

プロパティを作成すると、環境内で次回 データの同期と更新の頻度 されるときに、関連するリソースに反映されます。

カスタムプロパティを作成する方法

1. **[Settings > Inventory] > [Custom Properties]** に移動します。
2. 左側の組織ツリーで アカウントの範囲 を選択して、アカウントの特定のサブセットのカスタムプロパティを作成します。
3. **[カスタムプロパティの作成]** をクリックします。
4. 意味のある **名前**を入力します。
5. 定義するカスタムプロパティの **タイプ** を選択します。
   - **所有者**
   - **カスタム**
6. **タグを使用する**かどうかを決定します。
7. タグを使用している場合は、**[タグキーパターン]** と **[タグ値パターン]** を入力します。

   > **注意:**
   > - 0個以上の文字を示す場合は * を使用し、単一の文字を示す場合は ? を使用します。
   > - デフォルトでは、値のパターンは * に設定されていますが、必要に応じて変更できます。
   > - 複数のパターンを追加できます。
   > - 定義したパターンに一致するキーと値のペアでタグ付けされたリソースには、それに応じてプロパティの値が入力されます。

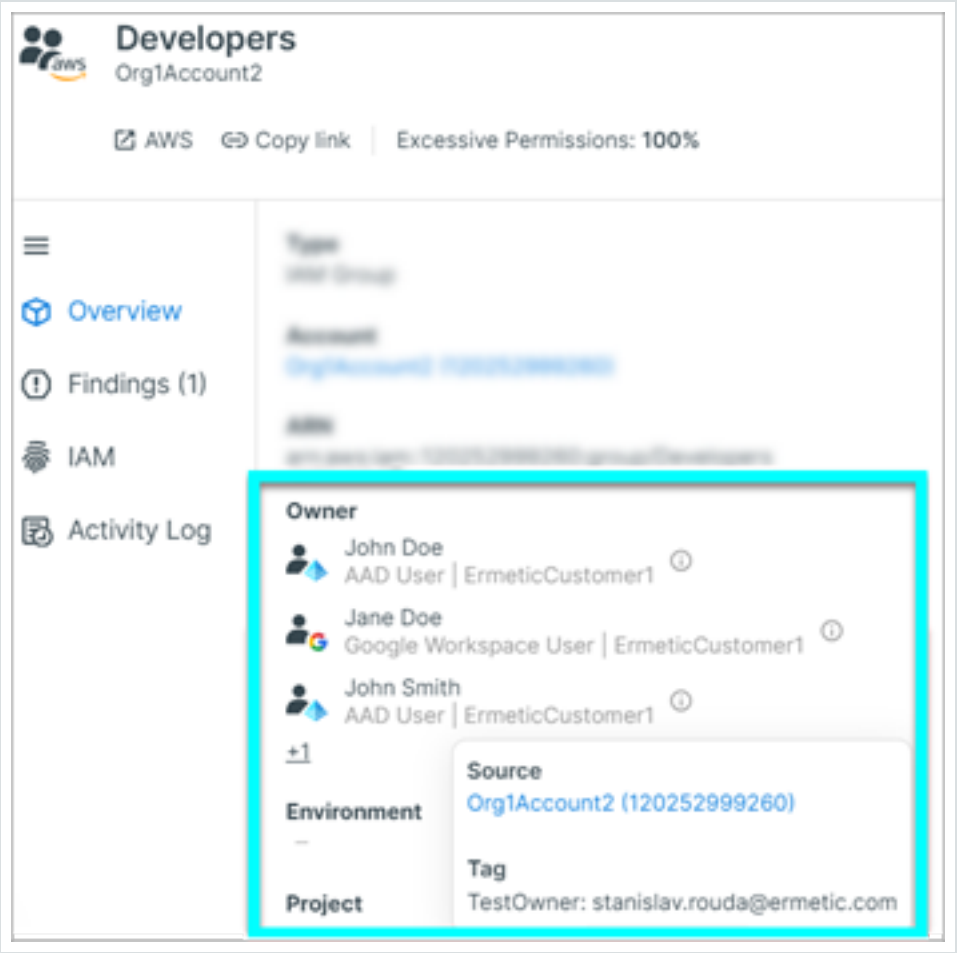
8. **[大文字と小文字を無視** する] (大文字と小文字を同一の文字として処理する) かどうかを選択します。
9. **[Create]** をクリックします。

コンソールでカスタムプロパティを表示する

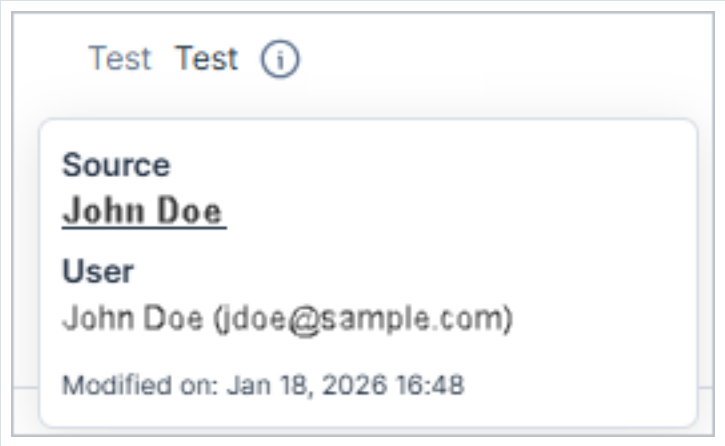
コンソールでカスタムプロパティを確認できます (AWS、Azure、GCP の場合)。

- Explorer のフィルターおよびリレーション基準として。
- リソースの 資産インベントリのフィルタリング として。
- リソースに関する詳細の取得する場合。一致した値の横に、以下を示すツールチップが表示されます。

- **自動値** (タグ)
  - **ソース**。クラウドプロバイダーでタグが定義されているリソース/アカウント。Tenable はまず、リソース自体で定義されているタグを検索します。リソースにタグが存在しない場合は、親レベルのリソースまたはアカウントレベルで定義されたタグ Tenable 検索します。
  - **タグ**。プロパティへの入力に使用されるクラウドタグのキーと値。



- **手動の値**:
  - **ソース / ユーザー**。変更を行ったユーザーの名前とメールアドレス



カスタムプロパティは、そのカスタムプロパティがカスタムプロパティの追加アカウント範囲で表示されます。

インベントリのカスタムプロパティの編集

クラウドタグとは無関係に、クラウドサイバーエクスポージャー Inventory を介してカスタムプロパティを手動で割り当て、一括編集します。たとえば、タグ付けされていない重要な S3 バケットに所有者を即座に割り当てられます。これにより、クラウドメタデータがない場合や正しくない場合でも、クラウドプロバイダーのタグの更新に DevOps を必要とせず、正確なセキュリティ情報とルーティングを確保できます。

より高いレベルで設定されたプロパティは、特別にオーバーライドされない限り、そのスコープ内のすべてのリソースに自動的に伝播されます。

カスタムプロパティを編集する方法

1. **[Explore > Inventory] (インベントリの調査)** に移動します。
2. 関連するインベントリを検索するか、関連するページに移動します。
3. 関連するリソースの横にある三点リーダーアイコンをクリックし、**[カスタムプロパティの編集]** をクリックします。
4. 関連するプロパティを選択します。

5. [プロパティの編集] ダイアログで、次を選択します。
    - **自動値 (デフォルト)。** クラウドタグパターンを介して自動的に入力される値を使用します (キーと値のペア)。
    - **手動値**。クラウドタグとは無関係に、値を手動で割り当てます。
6. 手動値の場合は、次のいずれかを実行します。
    1. 1 つの値を入力します。
    2. **Enter** キーを押して複数の値を入力します (たとえば、1 つのリソースに複数のステークホルダーがある場合)。
    3. 空の値を使用して特定のデータをクリアするには、**[空の値]** ボタンをクリックします。
7. **[保存]** をクリックします。

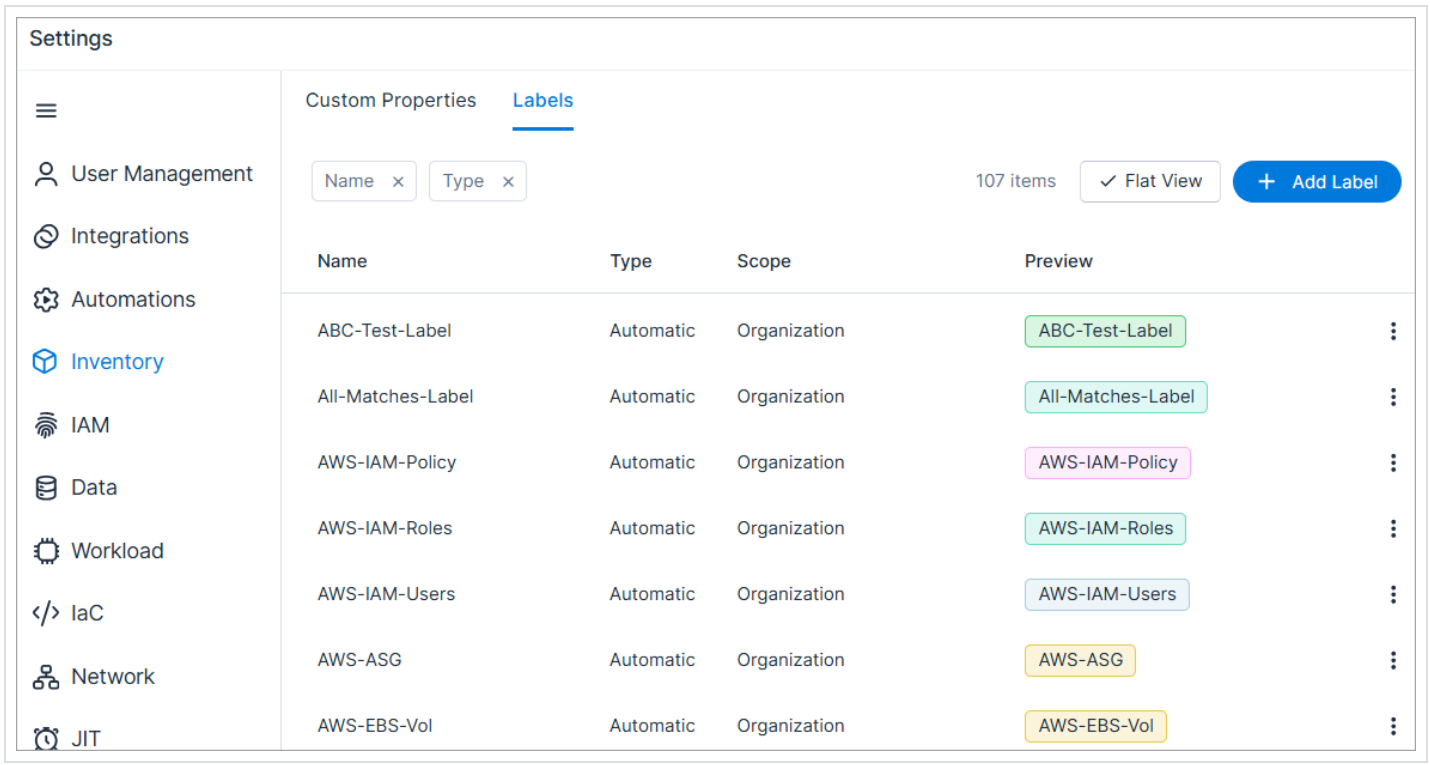
ラベルを管理する

次の方法でリソースに適用できるラベルを作成します。

- ラベルのリソースへの適用
- 自動適用 (タグに基づく)

> **注意:** クラウドサイバーエクスポージャーでは、組み込みのシステムラベルもリソースに自動的に適用されます。詳細については、「組み込みシステムラベル」を参照してください。

[Settings> Inventory > Labels] のテーブルからカスタムラベルを表示および管理します。



項目	説明
名前	ラベルの名前。
タイプ	• **手動**。リソースにラベルのリソースへの適用で適用 • **自動**。タグキー、またはタグキーと値に基づいて自動的に適用されます。
パス	ラベルが設定されたアカウントの範囲を示す、クラウドサイバーエクスポージャーフォルダー構造内のアカウント階層とフォルダー。アカウントのパスは動的であり、アカウントが別のフォルダーに移動されると変更されます。
プレビュー	ラベルがリソースに適用された後、クラウドサイバーエクスポージャーコンソールでどのように表示されるかを示すプレビュー。ラベル名が長い場合は、プレビューの上にカーソルを合わせると完全な名前が表示されます。
フラットビュー	デフォルトでは、選択した範囲と親の範囲で定義された項目がテーブルに表示されます。**[フラットビュー]**をクリックすると、子の範囲で定義されている項目も表示されます。

項目	説明
ラベルの追加	ラベルを追加する。
編集	ラベルを編集する。現在選択されている範囲で作成されたラベルで使用できます。
Delete (削除)	ラベルを削除します。現在選択されている範囲で作成されたラベルで使用できます。
ビュー	ラベルの読み取り専用ビュー。親レベルの範囲で作成されたラベルで使用できます。

ラベルを追加する

タグに基づいて自動ラベルを作成すると、次回環境で データの同期と更新の頻度 されるときに、関連するラベルがリソースに適用されます。

カスタムラベルを作成する方法

1. **Settings > [インベントリ] > [ラベル]** に移動します。
2. 左側の [Organization] (組織) ツリーで アカウントの範囲 を選択すると、アカウントの特定のサブセットのラベルを表示および管理できます。
3. **[ラベルの追加]** をクリックします。
4. ラベルの色を選択します。
5. 定義するラベルのタイプを選択します。
    - **手動ラベル**。ラベル名を入力します。
    - **正確なタグキーに基づく自動ラベル**。タグキーを選択します。定義したキーを持つリソースには、それに応じて自動的にラベルが付けられます。
    - **正確なタグキーと値に基づく自動ラベル**。タグのキーと値のペアを選択し、オプションでラベルに名前を付けます。定義した特定のキーと値のペアを持つリソースには、それに応じて自動的にラベルが付けられます。
    - **タグキーと値のパターンに基づく自動ラベル**。

- ラベルに **名前** を付けます。動的ラベル名を作成するには、名前に {key} や {value} のプレースホルダーを使用します。または静的な名前を入力して、単一のラベル名を使用します。たとえば、ラベル名として `dynamicLabel:{value}` と入力すると、タグ値が `32` であるー致するリソースには クラウドサイバーエクスポージャー で `dynamicLabel:32` のラベル名が付けられます。
- タグのキーまたはパターンで見つかったテキストパターンに基づいて、タグ **キーと値** のペアを選択します。0 個以上の文字を示す場合は * を使用し、単一の文字を示す場合は ? を使用します。定義したパターンにー致するキーと値のペアでタグ付けされたリソースには、それに応じて自動的にラベルが付けられます。
- 大文字と小文字を区別しない (大文字と小文字を同一の文字として処理する) かどうかを選択します。

> **注意:** 自動ラベルの場合、入力する値を空白 **のみ** にすることはできません。

6. **[作成]** をクリックします。

ラベルを編集する

ラベルの色、名前、その他の詳細を変更できます。

- 自動ラベルの場合、ラベルのロジックを変更できます。たとえば、**正確なタグキーに基づく自動ラベル** から、**タグキーと値のパターンに基づく自動ラベル** に変更できます。
- 自動ラベルを手動ラベルに変換したり、手動ラベルを手動ラベルに変換したりすることはできません。
- 自動ラベルへの変更は、環境内で次回 データの同期と更新の頻度 ときに有効になります。

カスタムラベルを編集する方法

1. **>ラベルSettings** に移動します。
2. 左側の [Organization] (組織) ツリーで アカウントの範囲 を選択すると、アカウントの特定のサブセットのラベルを表示および管理できます。
3. 三点リーダーメニュー ⋮ をクリックし、**[編集]** をクリックします。
4. 必要な変更を加え、**[保存]** をクリックします。

組み込みシステムラベル

以下のシステムラベルは、クラウドサイバーエクスポージャーに組み込まれており、必要に応じてリソースに自動的に適用されます。

ラベル	意味
サードパーティ	サードパーティのベンダーが使用するアイデンティティ
Microsoft Entra ID 外部	別の Microsoft Entra 組織または外部 ID プロバイダーを介して認証する Microsoft Entra ユーザー
Microsoft Entra ID 特権	特権 Microsoft Entra 管理ロールが割り当てられているアイデンティティ。Microsoft では、Microsoft Entra 組み込みロールのサブセットに特権ラベルを割り当てます。他の Microsoft Entra ロールも クラウドサイバーエクスポージャー 内で特権ロールとして扱う場合は、そのように定義できます。
管理者	管理者権限を持つプリンシパル • **AWS** - プリンシパルは可能なすべてのアクセス許可の少なくとも 99% と、深刻度が「重大」のマークが付いたアクセス許可を少なくとも 1 つ持つ必要があります。 • **Azure** - アイデンティティにサブスクリプションレベル (またはそれ以上) の所有者ロールがあるか、所有者ロールに含まれるすべてのアクセス許可が付与されています。 • **GCP** - プリンシパルは、GCP プロジェクトロール所有者に含まれるすべてのアクセス許可の 99% 以上と、深刻度が「重大」のマークが付いたアクセス許可を 1 つ以上持っている必要があります。 **管理者ラベルが特権**ラベルよりも優先される: プリンシパルは、アカウントごとにこれらのラベルを 1 つ持つことができます。ただし、プリンシパルは異なるアカウントにまた

ラベル	意味
	がって両方のラベルを持つことができます。たとえば、1 つのアカウントで [Admin] ラベルを保持し、別のアカウントで [Privileged] ラベルを保持するなどです。
異常	リソースが異常な動作を実行することが確認されました
アクセスキー	アクティブなアクセスキーを持つアイデンティティ
無効	無効になっているアイデンティティ
過剰	深刻度の高い過剰なアクセス許可を持つアイデンティティ
ゲスト	ゲストユーザーであるアイデンティティ
IaC	いずれかのリポジトリでコードによって管理されるリソース。
非アクティブ	非アクティブなアイデンティティ
JIT	JIT 使用資格は、このアクセス許可またはグループに対してリクエストできます
認証情報なし	パスワードまたはアクティブなアクセスキーがないアイデンティティ
MFA なし	MFA が有効になっていないアイデンティティ
OS パッチ未適用	既知の脆弱性が多数あるバージョンのオペレーティングシステムを実行しているリソース
OS サポート終了	サポート終了、または終了が近づいているバージョンのオペレーティングシステムを実行しているリソース
特権	• 深刻度の高いアクセス許可を持つリソース • アイデンティティには、深刻度が高または重大のアクセス許可が少なくとも 1 つ必要です。

ラベル	意味
	管理者 ラベルが **特権** ラベルよりも優先される: プリンシパルは、アカウントごとにこれらのラベルを 1 つ持つことができます。ただし、プリンシパルは異なるアカウントにまたがって両方のラベルを持つことができます。たとえば、1 つのアカウントで [Admin] ラベルを保持し、別のアカウントで [Privileged] ラベルを保持するなどです。
パブリック	IAM: あらゆるアイデンティティがアクセスできるリソース ネットワーク: インターネットに直接的または間接的に公開されているリソース **パブリック**としてラベル付けするには、仮想マシンが実行されている必要があります。
パブリックコンピューティング	広範囲のパブリック IP アドレスからアクセスできるコンピューティングリソースにリンクされたアイデンティティ。
機密	機密性の高いリソースに対する過剰なアクセス許可。機密としてマークされているリソースとそのリソースにアクセスできるリソースに適用されます。
信頼されているサービス	信頼できる AWS サービスによって使用
未使用	未使用の GCP プロジェクト
脆弱性	重大な脆弱性があるリソース
脆弱性のあるコンピューティング	重大な脆弱性があるコンピューティングリソースにリンクされているアイデンティティ

コアコンセプト

概要

Tenable CNAPP は、複雑なクラウドインフラのセキュリティ運用を自動化します。完全な資産検出、詳細なリスク分析、ランタイム脅威検出、コンプライアンスレポートが、詳細なビジュアライゼーションおよびステップバイステップのガイダンスとともに統合されています。アイデンティティ第一のアプローチを使用して、Tenable One Cloud Exposure はクラウドのアタックサーフェスを大幅に縮小し、最小権限を大規模に適用します。

詳細

機能	詳細はこちらから
Core プラットフォーム	• スキャン方法 • プロジェクトの仕組み • 検出結果の深刻度 • アーキテクチャとデータ処理 • 製品のセキュリティとプライバシー
セキュリティドメイン	• IAM • ワークロード保護 • データ保護 • Kubernetes • コード • コンプライアンス

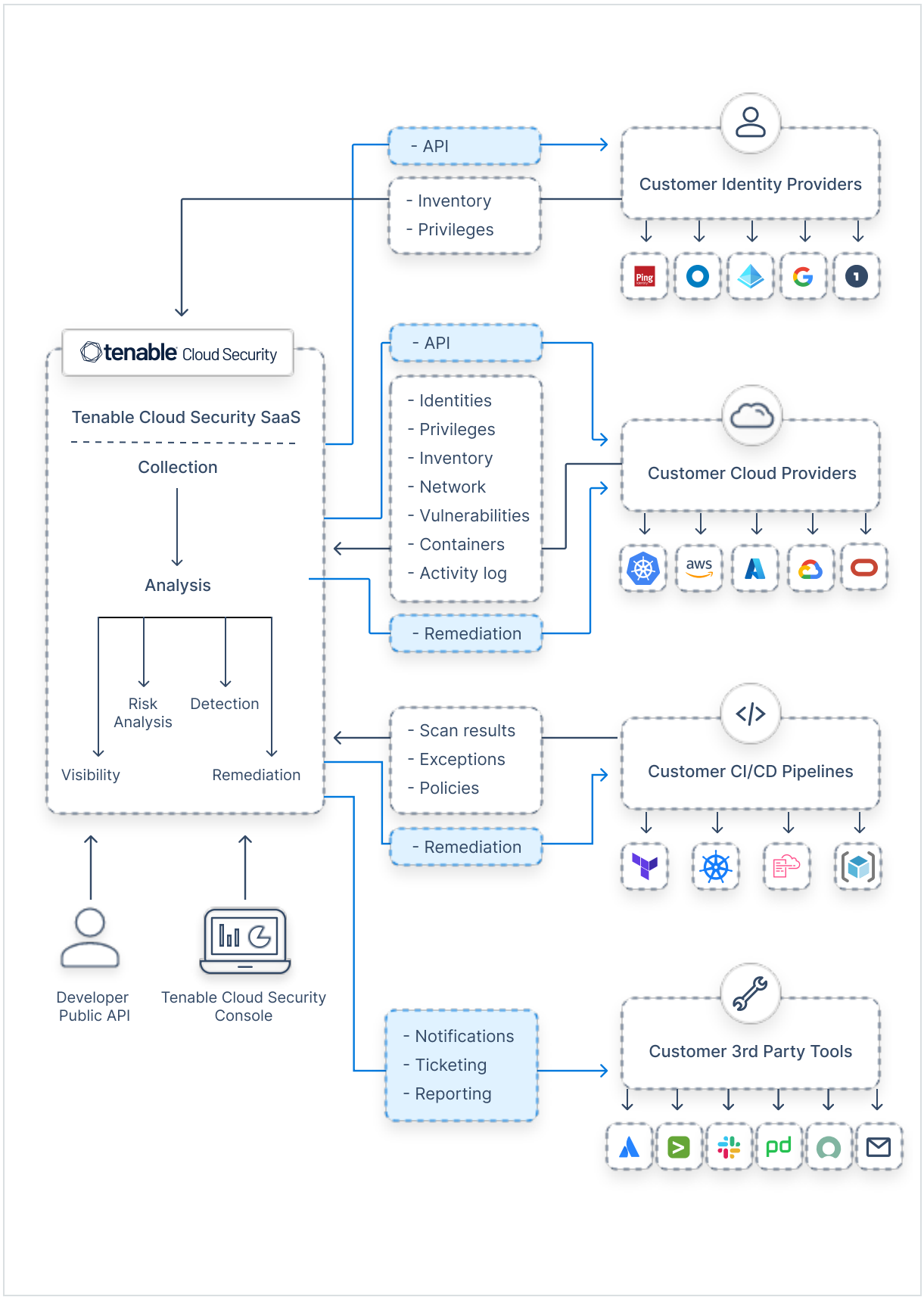
アイデンティティ第一のクラウドネイティブアプリケーション保護

- **マルチクラウドの資産管理と統一された可視性。**クラウド環境内のアイデンティティ、データ、インフラ、ワークロードのすべてを、詳細で一元化された可視性をもって活用できます。
- **クラウドワークロード保護 (CWP)**。仮想マシン、コンテナ、サーバーレス関数にわたって脆弱性、露出したシークレットまたは機密データ、マルウェア、設定ミスを特定し、重大なリスクをスキャンして検出します。
- **セキュアなクラウドアイデンティティと権限 (CIEM)**。手動では検出がほぼ不可能な検出結果を提示し、正確で自動化された修正を可能にします。
- **セルフサービスのジャストインタイム (JIT) アクセス**。必要に応じて迅速にアクセスを承認し、クラウドのアタックサーフェスを最小限に抑え、長期間権限が取り消されずに残るリスクを回避します。
- **Kubernetesのポスチャー管理 (KSPM)**。Kubernetes クラスタがデフォルトで安全であることを確認します。設定ミスが検出された場合は、問題について先行的に警告し、関連するステークホルダーがすぐに問題を軽減できるようにします。
- **自動修正**。クラウドインフラのリスクの修正をスピードアップさせるため、問題を修正する自動対応アクションを実行します。
- **フルスタックのリスク分析と優先順位付け**。フルスタック分析を活用して、機密データを露出する可能性のある危険なシナリオなどのリスクを明らかにし、実用的なインサイトを提供します。
- **ガバナンスとコンプライアンス (CSPM)**。複数のクラウドにわたる設定とリソースを継続的にスキャンし、違反を特定し、修正を自動化する単一のプラットフォームにより、クラウドのコンプライアンスを簡素化します。
- **シフトレフトに対する IaC セキュリティ**。インフラのコード化 (IaC) の設定ミスやその他のリスクを明らかにし、CI/CD パイプラインの一部としてクラウドインフラ環境を強化します。
- **クラウド検出と対応**。継続的な挙動分析と異常検出を適用して、クラウド脅威をすばやく特定し、調査します。

アーキテクチャとデータ処理

Tenable One Cloud Exposure は、API 経由で主要なパブリッククラウドサービスプロバイダーに接続する、クラウドでホストされたプラットフォームに基づいています。クラウドインフラのセキュリティの全体像を形成するために、Tenable はアイデンティティとクラウドプロバイダーを統合します。また、Tenable はサードパーティのチケッティング、通知、SIEM ツールと統合して、可視性を強化し、修正を容易にします。

次の図は、クラウドサイバーエクスポージャーとお客様の統合システム間の通信フローを示しています。


- API
- Inventory
- Privileges
Customer Identity Providers
tenable Cloud Security
Tenable Cloud Security SaaS
Collection
Analysis
Risk Analysis
Detection
Visibility
Remediation
- API
- Identities
- Privileges
- Inventory
- Network
- Vulnerabilities
- Containers
- Activity log
- Remediation
Customer Cloud Providers
- Scan results
- Exceptions
- Policies
- Remediation
Customer CI/CD Pipelines
Developer Public API
Tenable Cloud Security Console
- Notifications
- Ticketing
- Reporting
Customer 3rd Party Tools

プラットフォームのコンポーネント

クラウドサイバーエクスポージャープラットフォームは次のコンポーネントで構成されています。

- サービス
- コンソール
- 公開 API

サービス

クラウドサイバーエクスポージャーは、AWS でホストされているマルチテナントサービスです。このサービスは組織の IdP およびクラウドインフラの環境と統合され、アイデンティティ、権限、リソース、ネットワーク、アクティビティログの設定メタデータを継続的に収集します。収集されたデータは独自のデータ構造で処理および保存され、アイデンティティの権限とアクティビティが詳細に可視化されます。これにより、高度なアイデンティティ分析プロセスが可能になり、アクセス関連の脅威と過剰な権限を修正しやすくなります。クラウドサイバーエクスポージャーではこのようなリスクを排除するために、適切なサイズの IAM 設定に関する推奨事項が生成されます。クラウドサイバーエクスポージャーでは、完全自動化や半自動化にかかわらず、スケーラブルで継続的なリスク修正プロセスをサポートしています。チケッティング、通知、SIEM ツール (Jira、Slack、Splunk など) と統合することで、クラウドサイバーエクスポージャーは組織の自然なワークフローにリスク修正を組み込みます。

コンソール

コンソールはクラウドサイバーエクスポージャーの管理アプリケーションであり、以下をサポートします。

- 組織のクラウドインフラアカウントのオンボーディング
- 容易なクラウドアイデンティティプロバイダーとサードパーティのワークフロー製品との統合
- クラウドインフラ環境におけるリスクと脅威の特定、モニタリング、対策実施、管理、調査、修正

公開 API

公開 API により、プログラム的にクラウドサイバーエクスポージャーサービスと連携することで、クラウド環境のオンボーディングや、アクセス許可、リスク、脅威のエクスポート、多くの文脈によるクラウドサイバーエクスポージャープラットフォームの強化が可能になります。

環境の分析方法

環境内のセキュリティ問題を検出して解決するために、クラウドサイバーエクスポージャーでは次の操作が実行されます。

1. **リソース、アイデンティティ、アクセス許可、接続を含む、環境のスナップショットを取得します。**
    - このプロセスでは、API経由で環境内のアイデンティティ、アカウント、サービス、リソースのすべてでクエリを実行する必要があります。
    - サービスの多くは一括操作をサポートしていないため、環境内のリソースすべてに対して個別のAPI呼び出しをトリガーする必要があります。
    - お客様の環境には、デプロイされたリソースが数百から数百万含まれる可能性があります。
    - すべてのクラウドサービスプロバイダー(CSP)のAPIは、クォータとスロットリングの対象です。セキュリティツールとして、クラウドサイバーエクスポージャーではAPI呼び出しが可能な限り最適化され、スロットリングがお客様の環境に影響を与えないようにします。
    - お客様が生成したAPI呼び出しがスロットリングの影響を受けないようにするために、クラウドサイバーエクスポージャーではAPI呼び出しのレートを制御するメカニズムを実装しています。
2. **設定ミスや過剰な権限に関連するポリシーを含む、利用可能なポリシーすべてに対する全リソースを分析します。**
    - たとえば、アイデンティティが過剰な権限を付与されているかどうかを判断するために、クラウドサイバーエクスポージャーでは以下のような幅広い文脈情報が考慮されます。
        1. そのアイデンティティに対してアクセス許可を付与するメカニズム
        2. そのアイデンティティによって過去に実行されたすべてのアクティビティ
        3. どのリソースベースのアクセス許可が利用可能かを判断するため、クラウドサイバーエクスポージャーでは環境内の各リソースに関する情報をすべて取得する
    - 評価プロセスは、クロスアカウントアクセスを含め、CSPで利用可能なアイデンティティ、サービス、リソース、アクションのすべてに対して行われます。
    - 必要な文脈を分析せずに、アイデンティティに過剰な権限が付与されているかどうかを判断する方法はありません。

3. **各タイプの分析が完了すると、プラットフォームはどの問題が作成、修正、部分的修正されたか、または変更されていないかを判断し、これらの変更を反映してクラウドサイバーエクスポージャーコンソールを更新します。**

注意: クラウドサイバーエクスポージャーは、リソース検出と、個別にスケジュールされたプロセスとして、アクセス許可の評価やネットワークの評価など、異なるタイプの分析を実行します。その結果、環境のセキュリティポスチャーのさまざまな部分に、単一の同期されたスナップショットではなく、異なる時点で収集されたデータが反映される可能性があります。

データの同期と更新の頻度

クラウドサイバーエクスポージャーは、マルチクラウド環境全体で継続的にデータを同期します。ほとんどの環境では、クラウド環境の規模と必要な分析の量に応じて、完全な分析は数時間で完了します (詳細については、環境の分析方法を参照してください)。

重要: ワークロード保護機能を使用する場合、クラウドサイバーエクスポージャーはすべての仮想マシンを少なくとも 24 時間に 1 回スキャンすることに注意してください。

注意: 分析の品質とデータの同期にかかる時間の両方を最適化するために、Tenable では使用するメカニズムとプロセスを常に改善しています。異なるタイプのデータが独立して、異なる頻度で同期および分析されるようになりました。

データ保持期間と学習期間

重要: 以下に記載されているデータ保持期間は、クラウドサイバーエクスポージャーのアクティブユーザーのみが対象です。 クラウドサイバーエクスポージャーからクラウドアカウント、アイデンティティプロバイダー、または統合を削除すると、すべての関連データが完全に削除され、Tenable で保持されなくなります。

データ保持

クラウドサイバーエクスポージャーでは、選択したデータオブジェクトのグループについて、次のデータが保持されます。

- 検出結果
  - 未解決の検出結果と無視した検出結果: **無期限**
  - 解決済みの検出結果: **365 日**
- 監査ログ: **無期限**
- 設定スナップショット (IAM リソース): **無期限**
- アクティビティログ
  - **最大 30 日**: CIEM または Standard ライセンス
  - **最大 90 日**: Enterprise ライセンス

  詳細については、「 ライセンス を参照してください。

> **注意:**
>
> - 現在の保持期間は多数のデータオブジェクトで無期限ですが、Tenable は将来このポリシーを変更する可能性があります。
> - GCP でプロジェクトを削除した後、そのプロジェクトが完全に削除されるまでに 30 日かかります。Tenable はこの期間が経過するまでシステムからデータを削除しません。

過剰なアクセス許可

クラウドサイバーエクスポージャー は以下のアクティビティに対して分析期間 (学習期間) をトリガーします。この期間には、過剰なアクセス許可に関連する新しい検出結果は作成されません。

- AWS
  - 新規のユーザーアイデンティティが作成された場合 - 180 日
  - 新規のサービスアイデンティティまたはマシンアイデンティティが作成された場合 - 90 日
- Azure または GCP
  - 新規のアイデンティティが作成された場合 - 90 日
- **すべてのクラウドプロバイダー**

- アイデンティティのアクセス許可が変更された場合 - 30 日
  - アイデンティティが非アクティブの場合
    - 最初のアクセス許可が追加されると、Tenable は 30 日の学習期間を実施
    - その後にアクセス許可が変更されても、学習期間の追加実施はなし
  - アイデンティティがアクティブの場合
    - アクセス許可が変更されると、Tenable は 30 日の学習期間を実施するか、追加で 30 日の新しい学習期間を開始

> **注意:** (Azure)アクセス許可の変更では、分析期間または学習期間はサブスクリプションごとに計算されます。

アクティビティログと異常な動作

クラウドサイバーエクスポージャーは、最大 12 か月分のユーザーアクティビティを分析します。クラウドサイバーエクスポージャーは、アイデンティティについて少なくとも 30 日間学習した後、異常な動作について警告します。特定の動作に対して異常な検出結果がオープンされた後、類似の異常な動作が検出されると、すべて次のように処理されます。

- 30 日以内 - その動作は既存の検出結果に追加され、以前に解決済みとしてマークされていた場合はその検出結果が再オープンされます。
- 30 日経過後 - 新しい検出結果がオープンされます。

許可が必要な Tenable IP アドレス

クラウドサイバーエクスポージャーの適切な機能とネットワークアクセスを確保するために、ファイヤーウォールで特定の IP アドレスを許可する必要がある場合があります。このセクションでは、利用する機能に応じて必要な IP アドレスについて概要を説明します。

- クラウドサイバーエクスポージャーのコアサービス用 IP アドレス
- ワークロード保護用とデータ保護用の追加 IP アドレス

クラウドサイバーエクスポージャーのコアサービス用 IP アドレス

以下のようなさまざまな状況で、クラウドサイバーエクスポージャーのネットワークアクセスを許可するために、ファイヤーウォールで Tenable リージョンに関連付けられた IP アドレスを許可する必要があります。以下に例を挙げます。

- Jira などのオンプレミス開発ツールを使用する場合。
- Kubernetes クラスタを クラウドサイバーエクスポージャーに接続するとき。詳細については、Kubernetesを参照してください。
- VPC Service Controls を使用して、オンボーディングするプロジェクトや組織の Google 管理サービスに対するアクセスを制限する場合。詳細については、VPC Service Control の例外の追加を参照してください。
- ネットワークアクセスに制限のあるコンテナレジストリに関連付けられた Azure コンテナリポジトリを表示するとき。レジストリの **ネットワーキング** 設定でパブリックネットワークアクセスを設定して、**選択されたネットワーク** からのアクセスを許可し、関連するアドレスを以下のとおりに追加します。詳細については、関連する Microsoft のドキュメントを参照してください。

上記のいずれの状況においても、以下の表に記載されているように、リージョンに関連付けられている IP アドレスをすべて追加する必要があります。必要に応じて、上記のリンク先ドキュメントの詳細な手順に従ってください。

IP アドレス	コード	リージョン
13.55.8.134	ap-southeast-2	オーストラリア
13.238.234.158	ap-southeast-2	オーストラリア
15.229.113.7	sa-east-1	ブラジル
18.230.107.160	sa-east-1	ブラジル
15.222.42.59	ca-central-1	カナダ
3.96.102.218	ca-central-1	カナダ

IP アドレス	コード	リージョン
18.192.163.94	eu-central-1	ヨーロッパ
3.67.105.194	eu-central-1	ヨーロッパ
3.111.211.8	ap-south-1	インド
13.233.15.138	ap-south-1	インド
13.114.192.130	ap-northeast-1	日本
54.249.244.19	ap-northeast-1	日本
13.213.26.143	ap-southeast-1	シンガポール
54.169.55.8	ap-southeast-1	シンガポール
54.180.11.78	ap-northeast-2	韓国
52.79.145.86	ap-northeast-2	韓国
3.28.116.1	me-central-1	アラブ首長国連邦
51.112.62.204	me-central-1	アラブ首長国連邦
18.133.145.176	eu-west-2	英国
35.178.50.225	eu-west-2	英国
18.118.214.30	us-east-2	米国
18.189.244.216	us-east-2	米国
3.142.27.15	us-east-2	米国
3.143.179.156	us-east-2	米国

IP アドレス	コード	リージョン
15.205.53.205	us-gov-west-1	米国ガバメントクラウド
3.30.64.189	us-gov-west-1	米国ガバメントクラウド

クラウドサイバーエクスポージャーコンソールへのログインに使用するURLに基づいて、リージョンを特定できます。

詳しくは、リージョン別のTenableコンソールURLを参照してください。

ワークロード保護用とデータ保護用の追加IPアドレス

ネットワークポリシーを適用して環境を保護し、ワークロード保護やデータ保護の機能を使用する場合は、スキャン対象のリソースが配置されているリージョンに関連付けられたIPアドレスを、ネットワークポリシーで許可する必要があります。以下のAWS、Azure、GCP、OCI、Alibaba Cloudの関連表を参照してください。

AWS: 追加IPアドレス

AWSリソースの場合は、スキャン対象のリソースが配置されているリージョンに関連付けられたIPアドレスを許可します。

IP アドレス	コード
13.244.47.171, 13.247.41.46	af-south-1
54.46.41.61, 54.46.18.102	ap-east-1
13.158.66.42, 13.158.121.198	ap-northeast-1
3.35.85.139, 15.164.71.91	ap-northeast-2
56.155.20.153, 15.168.230.70	ap-northeast-3

IP アドレス	コード
3.108.153.42, 65.0.200.62	ap-south-1
40.192.75.236, 98.130.91.166	ap-south-2
175.41.159.66, 13.250.195.115	ap-southeast-1
13.55.43.203, 52.65.72.80	ap-southeast-2
16.79.53.198, 16.79.53.90	ap-southeast-3
16.26.36.30, 16.26.107.43	ap-southeast-4
43.217.167.99, 43.217.173.190	ap-southeast-5
52.60.245.247, 15.156.1.141	ca-central-1
40.177.114.116, 40.177.125.207	ca-west-1
3.73.221.188, 63.178.204.81	eu-central-1
51.96.117.232, 51.96.13.168	eu-central-2
13.50.63.67, 16.170.31.188	eu-north-1
35.152.179.48, 15.161.18.202	eu-south-1
18.101.30.42, 51.48.29.154	eu-south-2
63.35.143.32, 18.202.10.182	eu-west-1
18.170.252.124, 18.130.97.168	eu-west-2
13.37.116.12, 13.38.181.150	eu-west-3
51.84.187.199, 51.17.102.160	il-central-1

IP アドレス	コード
3.29.193.243, 40.172.90.226	me-central-1
157.175.117.169, 15.184.164.203	me-south-1
52.67.25.160, 54.232.54.71	sa-east-1
52.0.48.165, 44.197.60.179	us-east-1
18.188.85.13, 18.116.179.123	us-east-2
52.8.98.134, 54.183.70.244	us-west-1
52.13.227.219, 44.225.61.163	us-west-2

Azure: 追加 IP アドレス

Azure リソースの場合は、スキャン対象のリソースが配置されているリージョンに関連付けられた IP アドレスを許可します。

IP アドレス	コード
40.126.151.132	australiacentral
20.227.144.80	australiacentral2
20.213.11.159	australiaeast
20.211.197.238	australiasoutheast
20.197.230.190	brazilsouth
20.206.42.162	brazilsoutheast
20.48.224.16	canadacentral

IP アドレス	コード
20.104.133.30	canadaeast
172.212.226.78	centralus
20.244.9.79	centralindia
20.42.93.227	eastus
20.62.2.243	eastus2
20.205.137.189	eastasia
20.199.72.104	francecentral
52.136.130.122	francesouth
20.113.192.12	germanynorth
20.218.152.250	germanywestcentral
70.153.24.139	indonesiacentral
20.217.82.48	israelcentral
4.232.161.55	italynorth
4.216.184.220	japaneast
20.89.233.148	japanwest
20.39.195.131	koreacentral
20.200.168.89	koreasouth
20.17.176.43	malaysiawest

IP アドレス	コード
158.23.168.37	mexicocentral
20.221.222.135	northcentralus
98.71.41.54	northeurope
20.251.144.118	norwayeast
20.215.40.163	polandcentral
20.173.105.45	qatarcentral
102.37.151.13	southafricanorth
20.87.161.83	southafricawest
40.124.87.130	southcentralus
20.205.169.174	southeastasia
52.172.33.171	southindia
68.221.169.249	spaincentral
135.225.57.168	swedencentral
20.208.130.139	switzerlandnorth
40.125.29.102	uaecentral
20.174.16.21	uaenorth
20.90.146.119	uksouth
20.254.192.157	ukwest

IP アドレス	コード
13.88.174.166	westus
13.77.210.60	westcentralus
20.98.112.63	westus2
20.14.91.213	westus3
74.234.169.27	westeurope

GCP: 追加 IP アドレス

GCP リソースの場合は、スキャン対象のリソースが配置されているリージョンに関連付けられた IP アドレスを許可します。

IP アドレス	コード
34.35.9.85	africa-south1
34.80.224.113	asia-east1
34.96.128.207	asia-east2
34.146.217.16	asia-northeast1
34.97.44.199	asia-northeast2
34.64.248.74	asia-northeast3
34.93.208.104	asia-south1
34.131.72.88	asia-south2
34.143.211.157	asia-southeast1

IP アドレス	コード
34.101.212.40	asia-southeast2
34.151.121.76	australia-southeast1
34.129.145.96	australia-southeast2
34.118.126.246	europe-central2
34.88.77.52	europe-north1
34.51.163.143	europe-north2
34.175.112.191	europe-southwest1
104.155.64.32	europe-west1
34.17.84.136	europe-west12
34.147.174.110	europe-west2
34.141.31.117	europe-west3
34.32.158.128	europe-west4
34.65.38.205	europe-west6
34.154.102.105	europe-west8
34.163.2.180	europe-west9
34.32.35.180	europe-west10
34.18.110.39	me-central1
34.166.87.226	me-central2

IP アドレス	コード
34.165.117.101	me-west1
34.51.1.131	northamerica-south1
34.47.21.190	northamerica-northeast1
34.130.211.148	northamerica-northeast2
34.95.251.39	southamerica-east1
34.176.113.165	southamerica-west1
35.194.13.48	us-central1
35.237.237.96	us-east1
34.86.114.209	us-east4
34.162.52.135	us-east5
34.174.145.164	us-south1
34.145.53.242	us-west1
34.94.85.48	us-west2
34.106.221.217	us-west3
34.16.238.165	us-west4

OCI: 追加 IP アドレス

OCI リソースの場合は、スキャン対象のリソースが配置されているリージョンに関連付けられた IP アドレスを許可します。

IP アドレス	コード
80.225.208.77	ap-mumbai-1
140.83.62.67	ap-osaka-1
138.2.94.25	ap-singapore-1
140.245.38.245	ap-singapore-2
138.3.222.76	ap-tokyo-1
152.70.23.162	eu-frankfurt-1
79.72.27.154	eu-marseille-1
79.72.19.117	eu-stockholm-1
144.24.245.89	eu-zurich-1
137.131.149.97	sa-saopaulo-1
138.2.246.157	sa-vinhedo-1
141.147.93.58	uk-london-1
150.230.178.200	us-ashburn-1
64.181.194.46	us-chicago-1
129.153.74.174	us-phoenix-1
146.235.207.179	us-sanjose-1

Alibaba Cloud: 追加の IP アドレス

Alibaba Cloud リソースの場合は、スキャン対象のリソースが配置されているリージョンに関連付けられた IP アドレスを許可します。

IP アドレス	コード
8.211.178.205	ap-northeast-1
43.108.104.143	ap-northeast-2
8.219.199.56	ap-southeast-1
8.217.136.209	CN-香港
47.245.162.168	eu-central-1
47.85.91.110	us-east-1

許可が必要な Tenable アカウント ID

クラウド サイバーエクスポージャー では複数のアカウント ID を使用して API リクエストを行います。これらの ID を認識することで、以下が保証されます。

- これらの ID から受信した API リクエストを信頼できるものとしてバリデーションできます。このようなリクエストを Tenable が使用するのは、たとえば、オンボーディング目的で環境に接続する際にアカウントのロールを引き継ぐ場合です。
- ワークロード保護を使用する場合、これらの ID をあらゆるアラートやブロックのメカニズムから除外することを検討します。これは、Tenable がスナップショットをスキャン目的でこれらのアカウントと共有するためです。

アカウント ID
081802104111
631729062255

アカウント ID
632762758154
980664881829

製品のセキュリティとプライバシー

このセクションでは、Tenable One Cloud Exposure の主要なセキュリティ機能について説明します。

ホストリージョン

クラウド サイバーエクスポージャー サービスのインスタンスは、次の広範な地理的リージョンでそれぞれホストされています。

- 米国
- オーストラリア
- ブラジル
- カナダ
- ヨーロッパ
- インド
- 日本
- シンガポール
- 韓国
- アラブ首長国連邦
- 英国
- 米国ガバメントクラウド

指定のリージョンに保存されたデータはそのリージョンに留まり、別のリージョンに送信されることはありません。

クラウド サイバーエクスポージャー はマルチテナント SaaS プラットフォームであり、上記の各サービスインスタンスは、顧客間を論理的に分離して複数のテナントにサービスを提供します。また Tenable では、リクエストに応じてシングルテナントインスタンスのサポートを提供しており、これはツールの価格に反映されます。

Tenable コンソール URL

クラウド サイバーエクスポージャー のリージョン	URL
グローバル (すべてのリージョン)	https://app.tenable.com
米国ガバメントクラウド	https://app.tenable.us

データ分離

インスタンス内ではデータの完全な分離が導入されており、各お客様のデータはデータベースレベルに基づき完全に分離されます。これをサポートするために、Tenable は各お客様のデータを独立した、論理的に分離されたデータベースまたはデータベースのセットに保存します。このような分離により、互いのデータにアクセスすることを厳格に防止しながら、マルチテナントサービスのスケールと利点を得ることができます。

データ暗号化

オープンネットワークで転送されるデータはすべて、TLS 1.2 を使用して暗号化されます。同様に、すべてのデータは AES-256 を使用して保存時に暗号化されます。

高可用性と障害復旧

クラウド サイバーエクスポージャー の各サービスインスタンスは可用性が高く、すべてのコンポーネント (コンピューティング、データベース、ネットワーキングなど) が複数の可用性ゾーンに分散しています。Tenable ではロードバランサーを使用して、受信するアプリケーショントラフィックを複数のインスタンスと可用性ゾーンに自動的に分配します。

お客様のデータは1日に1回継続的にバックアップされ、さらに週に1回、外部永続ストレージ経由で外部にもバックアップされます。

コンプライアンスと認証

クラウドサイバーエクスポージャーは、データ保護とプライバシーに関する最も厳しい情報セキュリティ要件を満たす内部コントロールを維持しています。Tenableは次の認証を取得しています。

- **SOC 2 Type II**。このレポートは、Tenableが業界で最も厳格なセキュリティ、可用性、処理、機密性、プライバシーの各基準に取り組んでいることを実証し、当社のセキュリティ管理がAICPA (米国公認会計士協会) に準拠していることを証明するものです。
- **ISO/IEC 27001**。ISO/IEC 27001:2013は業界で高く評価されている情報セキュリティ認証の1つであり、Tenableがクラウド提供のCNAPPサービスを保護する最高基準を満たしていることを実証しています。

年次ペネトレーションテスト

Tenableはサードパーティ企業と協力して、少なくとも年1回、本番環境のペネトレーションテストを実施しています。結果はTenableによってレビューが行われ、優先度の高い検出結果は解決まで追跡されます。

キー管理

Tenableでは確立されたキー管理プロセスを導入しており、AWS Key Management Service (KMS) を使用して、組織による暗号技術の使用をサポートしています。

認証

Tenableは、クラウドサイバーエクスポージャーコンソールへのログインに対して以下の認証モードをサポートしています。

- Microsoft Entra ID
- Google SSO

- IdP SAML SSO
- ユーザー名とパスワード (パスワードポリシーを参照してください)

ユーザーが SSO 経由で クラウド サイバーエクスポージャー コンソールにログインできるのは、外部アイデンティティプロバイダー (IdP) と Tenable の間に信頼が確立されているからです。この信頼により、ユーザーの既存の企業アイデンティティを利用して、ユーザープロビジョニングが容易に実行されるのです。ただし、自動ユーザープロビジョニングはサポートされていません。信頼が確立された後も、新規の Tenable ユーザーまたはグループの追加をコンソールまたは API 経由で行う必要があります。SSO ログインの有効化に関する詳細については、SSO 経由でのコンソールへのログインの有効化を参照してください。

パスワードポリシー

クラウド サイバーエクスポージャー パスワードポリシーでは、パスワードは 8 文字以上の長さで、以下を含む必要があります。

1. 大文字
2. 小文字
3. 数字

タイムアウト設定

アカウントのセキュリティを強化し、不正アクセスのリスクを低減するために、管理者はウェブコンソールに 2 種類のタイムアウトを設定できます。

- **非アクティビティタイムアウト** 。一定時間ユーザーが操作しなかった場合、セッションを終了します。デフォルト値は **12 時間** です。
- **セッションタイムアウト** 。ユーザーのアクティビティに関係なく、一定の時間が経過するとセッションを終了します。この設定は、デフォルトでは無効になっています。

これらの設定は、組織のセキュリティとコンプライアンスのニーズに応じて調整できます。詳細については、コンソールのタイムアウト設定を参照してください。

スキャン方法

Tenable One Cloud Exposure は、さまざまなスキャンおよび同期プロセスを通じて、クラウド環境全体に包括的な可視性とセキュリティを提供します。これらの方法により、Tenable はさまざまな視点から、ライフサイクルのさまざまな段階で環境を分析できます。この記事では、各スキャンタイプ、収集されるデータ、実行頻度、相互依存性について説明します。

大まかに言うと、これらのプロセスは**継続的**または**オンデマンド**のいずれかに分類でき、**エージェントレス**と**エージェントベース**の両方の分析手法を活用します。これらの基本的なアプローチを理解することは、以下に説明する特定のスキャンタイプを把握するための強固な基盤を築くことになります。

> **注意:** この記事で説明されているスキャンの方法と用語はクラウドサイバーエクスポージャーに固有のものです。なじみのあるコンセプトもありますが、実装と詳細については他の Tenable 製品と異なる場合があります。

用語

用語	説明
同期	クラウドサイバーエクスポージャーは、クラウドプロバイダー API からクラウドリソースに関する最新の設定データを継続的に直接取得します。この情報は、定義されたセキュリティポリシーに照らしてリソースを評価することで、設定ミスや潜在的なセキュリティ問題を特定するための基準となります。このプロセスは、オーケストレーションプロセスの主要コンポーネントです。
スキャン中	クラウドサイバーエクスポージャーは独自の検査方法を使用して、クラウドリソースの状態や設定に関する詳細な情報を取得します。これには多くの場合、API 呼び出しよりも詳細な分析が含まれます。このアクティビティでは、脆弱性、設定ミス、マルウェアの兆候など、セキュリティポスチャーに関する情報が収集されます。
エージェントレス分析	エージェントレス分析 (スキャンまたは同期) では、ソフトウェアエージェントをインストールせずにリソースをチェックおよびモニタリングします。エージェントレス分析は、API またはリモートアクセスプロトコル (SSH、WMI、RDP など) を使用して外部から接続します。システムの内部にアクセスせずに、外部からセキュリティポスチャーに関する情報 (脆弱性、設定ミス、マルウェアの兆候など) を収集します。

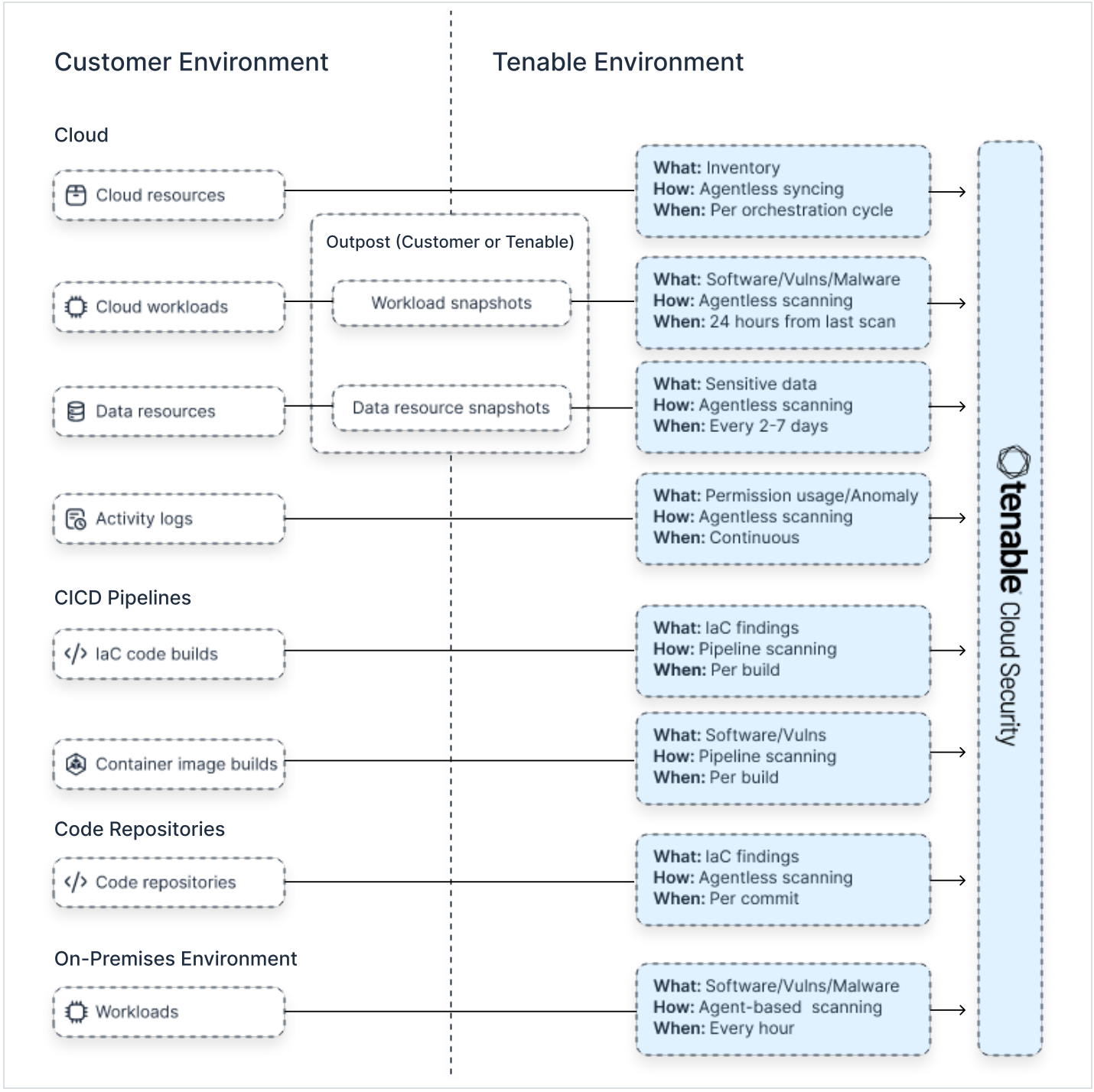
用語	説明
エージェントベースの分析	エージェントベースの分析では、エージェントと呼ばれる小さなソフトウェアをリソースにインストールします。エージェントは、セキュリティ関連のデータやポリシーをモニタリングし、収集し、場合によっては適用します。エージェントは、セキュリティチームにリアルタイムの可視性と、システム内部からの制御を提供します。
オーケストレーションプロセス	オーケストレーションは、クラウドおよびアイデンティティプロバイダーのリソースをインベントリにする継続的なプロセスです。このプロセスでは、結果を分析して、設定ミスやセキュリティ問題を特定します。これは、リソース検出や異なる種類のリスク評価など、独立したスケジュールで実行される複数のプロセスで構成されます。これらのプロセスは、環境ごとに実施されるクラウドサイバーエクスポージャーの中核となる運用プロセスを構成し、相関関係、検出結果の計算、優先順位付けが含まれます。

環境別のスキャン方法

クラウドサイバーエクスポージャーはさまざまな方法を採用して、多様な環境をモニタリングし、保護します。以下の表はこれらのアクティビティの詳細な内訳を示しており、付随する図ではアーキテクチャフローを示しています。

環境	対象	結果	スキャン方法	タイミング
クラウド	リソース	インベントリ	エージェントレスのリソース同期	継続的
	ワークロード	ソフトウェア/脆弱性/マルウェア	エージェントレスのワークロードスキャン/ アカウント内スキャン (ワークロードとデータ)	前回のスキャンから24時間後
	コンテナイメージレジストリ	ソフトウェア/脆弱性/マルウェア	エージェントレスのワークロードスキャン/	前回のスキャンから24時間後

環境	対象	結果	スキャン方法	タイミング
			アカウント内スキャン (ワークロードとデータ)	
	データリソース	機密データ	エージェントレスのデータスキャン/ アカウント内スキャン (ワークロードとデータ)	2 ~ 7 日ごと
	アクティビティログ	アクセス許可の使用/異常	エージェントレススキャン	継続的
CI/CD パイプライン	IaC コードビルド	IaC 検出結果	パイプラインスキャン	ビルドごと
	コンテナイメージビルド	ソフトウェア/脆弱性	パイプラインスキャン	ビルドごと
コードリポジトリ	コードリポジトリ	IaC 検出結果	エージェントレスのコードスキャン	コミットごと
オンプレミス	ワークロード	ソフトウェア/脆弱性/マルウェア	エージェントベースのスキャン	1 時間ごと



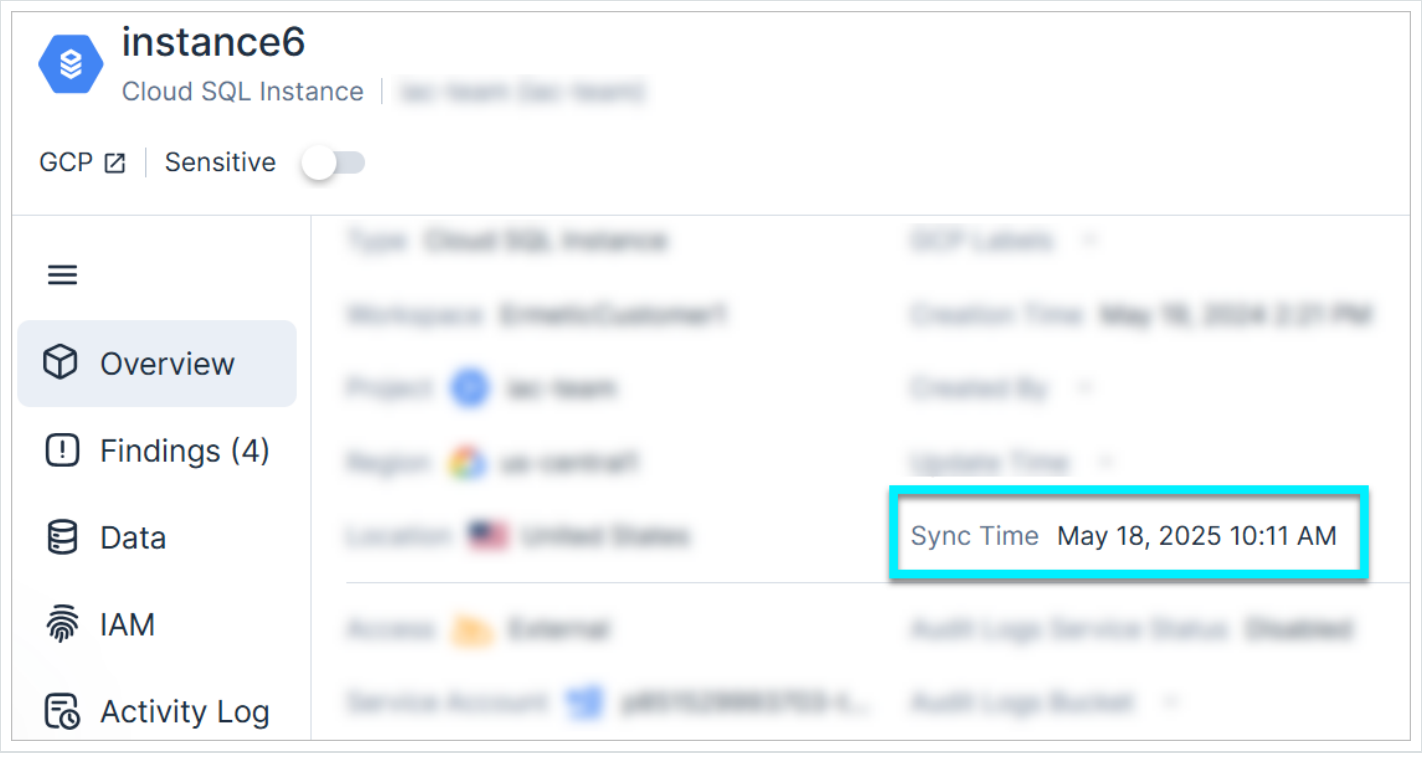
クラウド のスキャン方 法

クラウド サイバーエクスポージャー では、次 の方 法 を使 用してクラウド リソースをスキャンします。

- エージェントレスのリソース同期
- エージェントレスのワークロードスキャン
- エージェントレスのデータスキャン
- アカウント内スキャン (ワークロードとデータ)

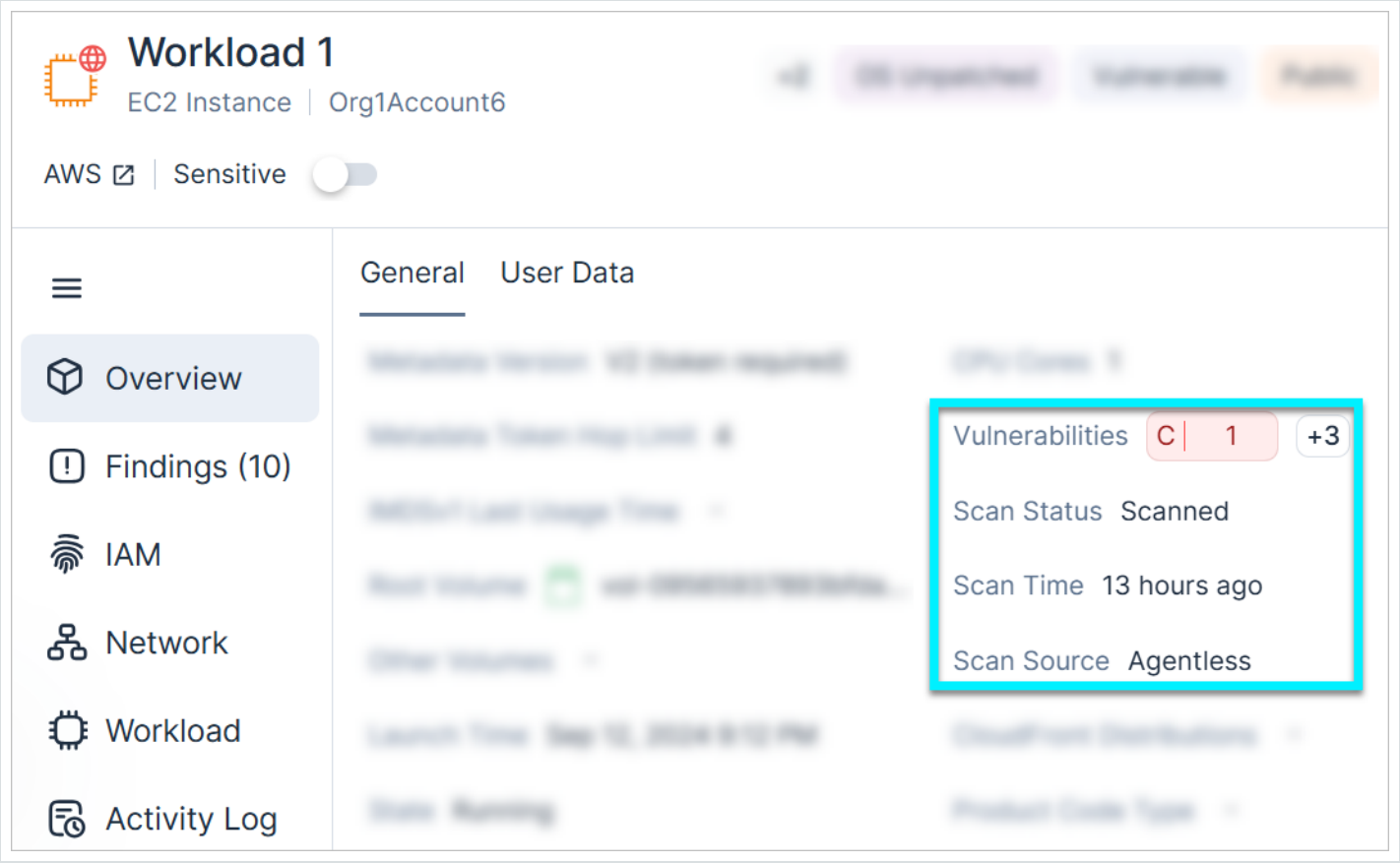
エージェントレスのリソース同期

クラウドサイバーエクスポージャー はエージェントレス分析を使用して、クラウドプロバイダー API からクラウドリソースに関する最新の設定データを継続的に直接取得します。このプロセスは、オーケストレーションプロセスによって駆動され、クラウドサイバーエクスポージャー内に基礎的なリソースインベントリを構築します。検出された各リソース (「クラウドリソース」など) について、関連するすべての設定の詳細が抽出され、リソースのプロファイルに表示されます。このリッチなデータセットで、設定ミスやその他のセキュリティ問題を検出するセキュリティポリシーを強化できます。リソース検出は継続的に実行され、インベントリとセキュリティポスチャーに環境の最新状態が反映されるようにします。リソースのプロファイルページで、前回の同期日時を確認できます。



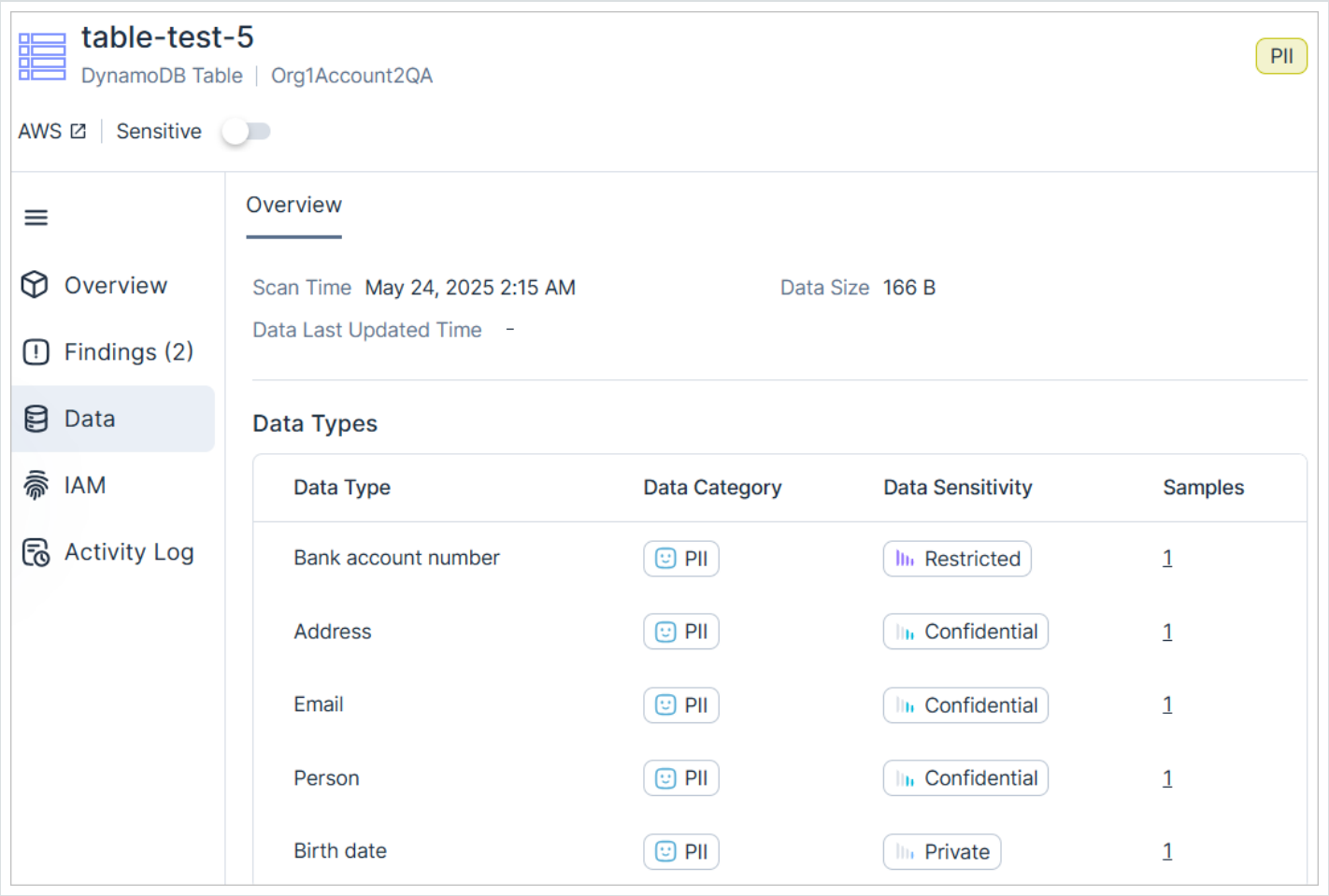
エージェントレスのワークロードスキャン

脆弱性スキャンが有効になっている場合、クラウドサイバーエクスポージャーはエージェントレス分析を実行して、前回のスキャンから24時間経過するとすぐに、脆弱性、ソフトウェア、悪意のあるファイルについて各ワークロードをスキャンします。このプロセスでは、これらのワークロードにデプロイされたコンテナイメージも検出します。ワークロードは独自のスキャン結果を持つ独立したワークロードとして扱われます。ワークロードのプロファイルページで、ワークロードの前回のスキャン日時を確認できます。詳細については、エージェントレスワークロードスキャンを参照してください。



エージェントレスのデータスキャン

データセキュリティのスキャンが有効になっている場合、クラウドサイバーエクスポージャーはエージェントレス分析を使用して、機密データのデータリソースを定期的にスキャンします。スキャン頻度は、リソースタイプ、サイズ、データ更新など、複数の要因によって決まります。一般的に、スキャンは2 ~ 7日に1回実行されます。このプロセスにより、リソースのプロファイルの[データ]タブに表示される機密データに関する情報が更新され、関連するラベルに反映されます。詳細については、Tenableによるデータのスキャン方法を参照してください。



アカウント内スキャン (ワークロードとデータ)

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

デフォルトでは、脆弱性とデータセキュリティのスキャンは、アウトポストと呼ばれる Tenable 所有のスキャンクラウド環境で実行されます。スキャン環境の所有をご希望の場合は、アカウント内スキャンをご利用いただけます。アカウント内スキャンを使用すると、スナップショットが環境から出ることなく、エージェントレススキャンを活用できます。アカウント内のスキャンは、オーケストレーションに影響を与えません。クラウドサイバーエクスポージャーからクラウドプロバイダーへの API 呼び出しは、スキャンアウトポストではなく、Tenable インフラストラクチャから引き続き実行されます。詳細については、アカウント内スキャンの設定を参照してください。

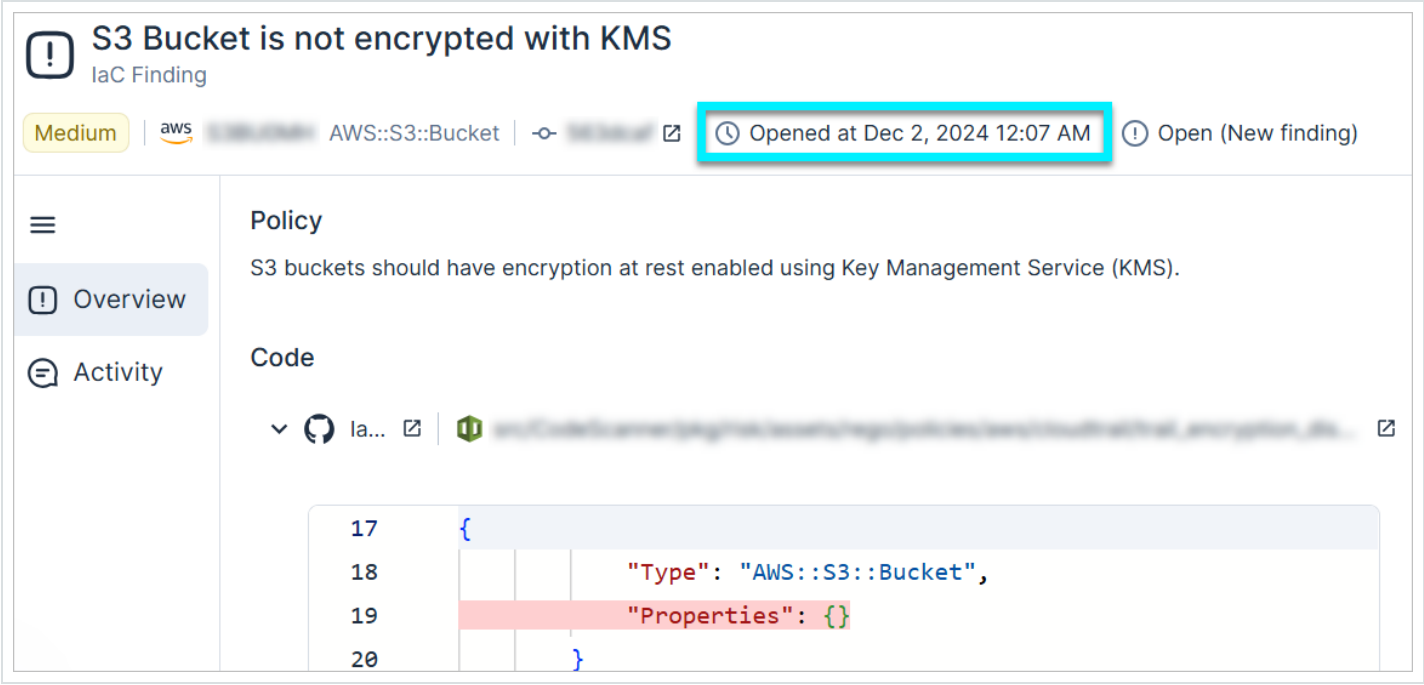
コードのスキャン方法

クラウド サイバーエクスポージャー では、次 の方 法 を使 用してコードをスキャンします。code:

- エージェントレスのコード スキャン
- CI/CD スキャン (IaC と脆 弱 性)

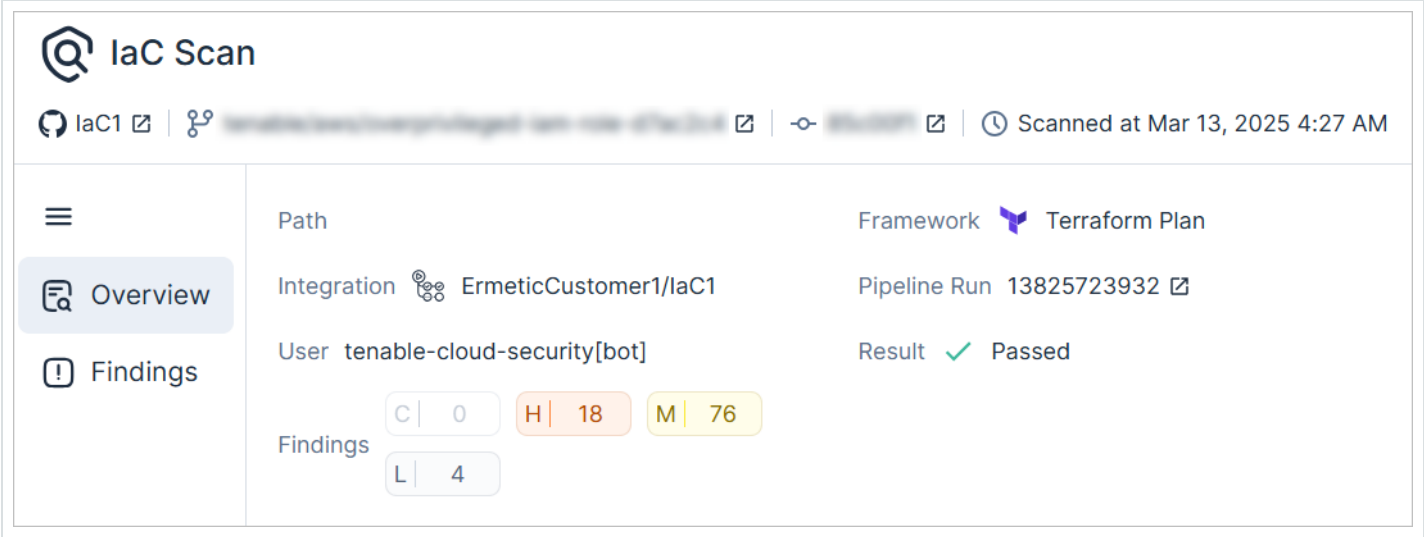
エージェントレスのコード スキャン

コードリポジトリが接 続 され、コード スキャンが有 効 になっている場 合 、クラウド サイバーエクスポージャー は プライマリブランチ (メインブランチなど) へのコードコミット に関 してコードリポジトリを継 続 的 にモニタリングし ます。コミット が行 われると、クラウド サイバーエクスポージャー は設 定 ミスやその他 の問 題 がないか IaC を スキャンします。コードに問 題 が含 まれている場 合 、クラウド サイバーエクスポージャー によって、対 応 する 検 出 結 果 がオープンになります。コード スキャンはコードコミット によってトリガーされ、通 常 はコードの最 新 バージョンが反 映 されるため、現 時 点 ではコード スキャンがいつ行 われたかを表 示 することはできません。 ただし、IaC の検 出 結 果 が最 初 に識 別 された日 時 は、検 出 結 果 がオープンされた時 間 から判 断 できま す。詳 細 については、「 コードリポジトリの接 続 」を参 照 してください。



CI/CD スキャン (IaC と脆 弱 性)

CI/CD パイプラインスキャンは、通常、ビルドプロセス中に開発パイプライン内で実行されるオンデマンドのプロセスです。クラウドサイバーエクスポージャーは、IaC の設定ミスやコンテナイメージの脆弱性を検出するためのスキャナーを提供します。開発者は、これらのスキャナーをビルドパイプライン (GitHub Actions など) 内に埋め込みます。スキャン結果はビルドフローの一部として返され、自動応答 (重大な検出結果に対するビルドの失敗など) が可能になります。これらの結果はまた、数分のうちにクラウドサイバーエクスポージャーコンソールでも入手できます。詳細については、CI/CD の接続を参照してください。



クラウド、アンマネージド、オンプレミスの Kubernetes スキャン方法

クラウドサイバーエクスポージャーでは次の方法を使用して、クラウド、アンマネージド、オンプレミスの Kubernetes ワークロードをスキャンします。

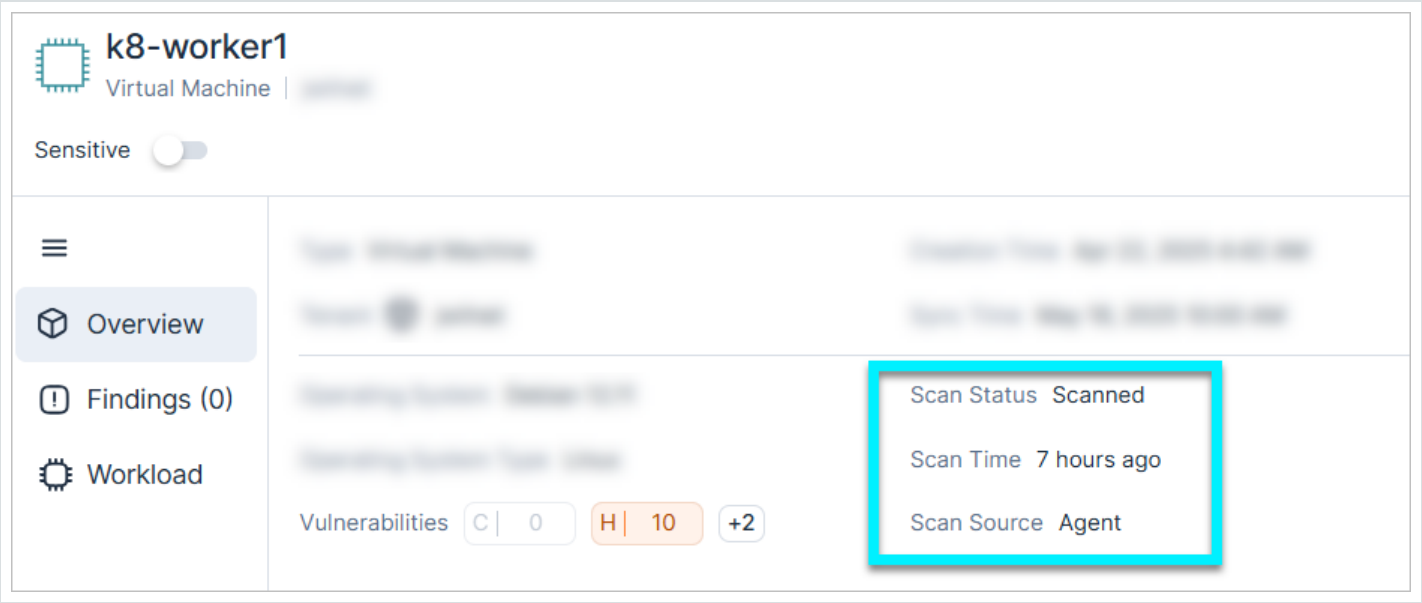
- エージェントベースの Kubernetes ワークロードスキャン

エージェントベースの Kubernetes ワークロードスキャン

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

コンテナベースのワークロード用に、クラウドサイバーエクスポージャーでは Helm チャート経由でインストールされたエージェントを提供しています。このセンサーは、すべてのクラスタノードで DaemonSet として実行され、エージェントベースの分析を実行して脆弱性、ソフトウェア、マルウェアをスキャンします。約30分以

内にノードをスキャンして新規または更新されたコンテナイメージを探します。ノードのプロファイルページには、前回のスキャン時刻と、ソースがエージェントであったことが表示されます。詳細については、エージェントベースの Kubernetes ワークロードスキャンを参照してください。



アカウント階層とフォルダー

Tenable One Cloud Exposure では、コンソール全体にアカウント階層が表示されます。この階層は、Tenable 内の以下のエンティティの管理方法と操作方法に影響を与えます (アカウントの範囲)。

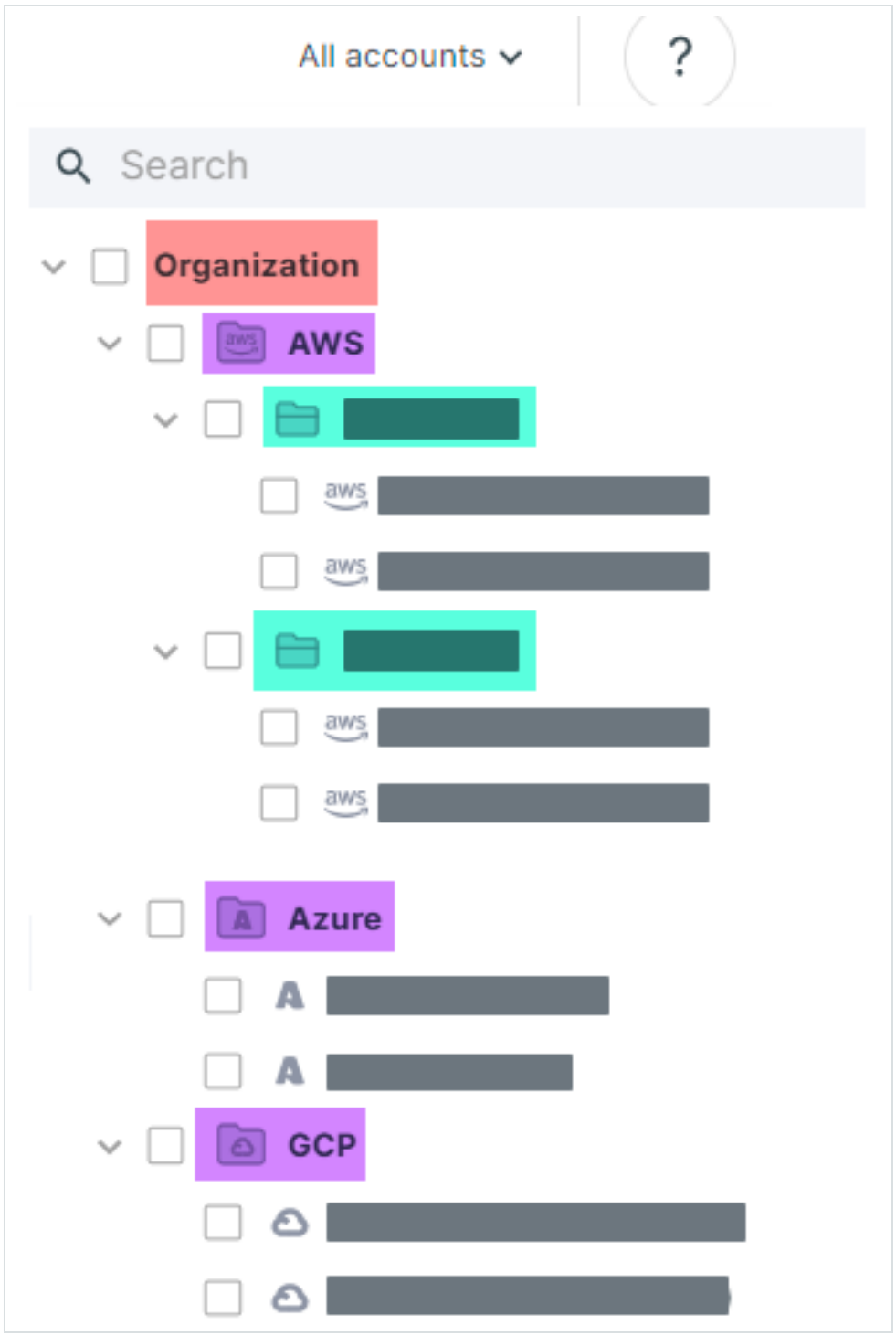
- プロジェクト
- クラウドアカウント
- アイデンティティプロバイダー
- コードリポジトリ
- コンテナレジストリ

Tenable により、組織内の他のすべてのフォルダーを含む最上位の **組織** フォルダーが自動的に作成されます。それぞれのクラウドプロバイダー (またはアイデンティティプロバイダー) に属する最初のアカウントを追加すると、[Organization] (組織) フォルダーの下に追加のフォルダーが自動的に作成されます。

組織に多数のアカウントがある場合は、フォルダーを使用して、クラウドサイバーエクスポージャー内で構造化されたアカウント階層を維持することが重要です。この構造は、以下の方法で作成できます。

- (推奨)オンボーディングされた組織のクラウドフォルダー構造に基づいて、Tenableのフォルダー構造を自動的に更新します。
- Tenableにアカウントフォルダーの作成して、オンボーディングされたクラウドアカウントを論理的にグループ化します。

重要: クラウドサイバーエクスポージャーにオンボーディングするアイデンティティプロバイダーテナントは組織ツリーにも表示されますが、アカウントフォルダーの作成することはできません。



注意: Organization (組織)、AWS、Alibaba Cloud、Azure、GCP、または OCI の親フォルダーを削除、名前変更、または移動することはできません。異なるクラウドプロバイダーのアカウントをグループ化することはできません。AWS 監査ログアカウントは、コンソール全体のアカウントフォルダツリーには表示されません。

フォルダー構造を自動的に更新

クラウドプロバイダー、アイデンティティプロバイダー、コードリポジトリのオンボーディング中に、クラウドサイバーエクスポージャーのフォルダー構造を自動的に更新するかどうかを選択できます。このオプションを**有効**にすると、以下のようになります。

- オンボーディングされた組織のフォルダー構造はプラットフォームにコピーされます。アカウント階層はそのまま維持され、継続的に同期されます。たとえば、AWS 内で既存のアカウントを新しく作成されたフォルダーに移動した場合、その変更は Tenable で反映されます。
- アカウント構造の変更は、環境内で次回データの同期と更新の頻度ときにクラウドサイバーエクスポージャーに反映されます。
- 環境に存在しないフォルダーはすべて削除されます。
- 環境内の空のフォルダーはすべて削除されます。
- クラウドサイバーエクスポージャー内の組織のフォルダーやアカウントを移動、編集、または作成することはできません。
- 新しいアカウントはルートの **組織** フォルダーにのみ手動で追加でき、特定の組織には追加できません。
- アカウントがクラウドプロバイダー内の別の組織に移動された場合
    - 別の組織が Tenable にオンボーディングされていない場合、アカウントは Tenable 内の現在の場所に残ります。アカウントの削除を選択できます。
    - 別の組織が Tenable にオンボーディングされている場合、アカウントは Tenable 内の新しい場所に移動します。
- クラウドサイバーエクスポージャー ユーザーアクセス許可は、アクセス許可が定義されたアカウント範囲に紐づけられます。たとえば、ユーザーに特定のフォルダーレベルの範囲 (**フォルダー 1**) に対して付与された [コラボレータ] のアクセス許可があり、**フォルダー 1** がクラウド内の新しい場所に移動された場合でも、同じアクセス許可が保持されます。詳細については、高度なユースケースの例 を参照してください。

高度なユースケースの例

- **例 #1** - 自動化:
    1. 複数の子アカウントを含む特定のフォルダーレベルの範囲 (**フォルダー 1**) で統合 (**Slack**) を設定しました。
    2. 子アカウントの 1 つ (**アカウント 1**) で、この Slack 統合を使用する自動化を定義しました。
    3. その後、AWS 環境でアカウント 1 を別のフォルダー (**フォルダー 2**) に移動しました。
    4. **結果**: Tenable は、既存の自動化フローを損なわないように、アカウントを新しいフォルダーに移動しません。
- **例 #2** - アクセス許可:
    1. クラウドサイバーエクスポージャーユーザーには、複数の子アカウントを含む特定のフォルダーレベルの範囲 (**フォルダー 1**) に対して付与された「コラボレータ」のアクセス許可があります。
    2. その後、AWS 環境でアカウント 1 を別のフォルダー (**フォルダー 2**) に移動しました。
    3. **結果** アクセス許可がアカウント自体ではなく親レベルの範囲 (**フォルダー 1**) に定義されているため、ユーザーは**アカウント 1** へのアクセス許可を失います。

よくある質問

> 組織の構造がクラウドと同期されないのはなぜですか?

回答:

1. アカウント構造の変更は、環境内で次回データの同期と更新の頻度ときにクラウドサイバーエクスポージャーに反映されます。
2. 高度なユースケースの例 #1 を参照してください

> Tenable でフォルダーやアカウントを編集/削除/移動できないのはなぜですか?

クラウド組織のオンボーディング中に「フォルダー構造の自動更新」オプションを有効にした場合、これらのエンティティはクラウド環境と同期されるため、Tenable内のフォルダーやアカウントを編集/削除/移動することはできません。

アカウントフォルダーの作成

アカウントフォルダーを作成して、たとえば以下に基づいて、オンボーディングされたクラウドアカウントを手動で論理的にグループ化します。

- 開発環境または本番環境
- 製品
- 一意の所有者を持つビジネスユニット

これらのフォルダーを使用すると、クラウドサービスプロバイダー内の既存の階層と同じように、アカウント (および他のフォルダー) をネストできます。

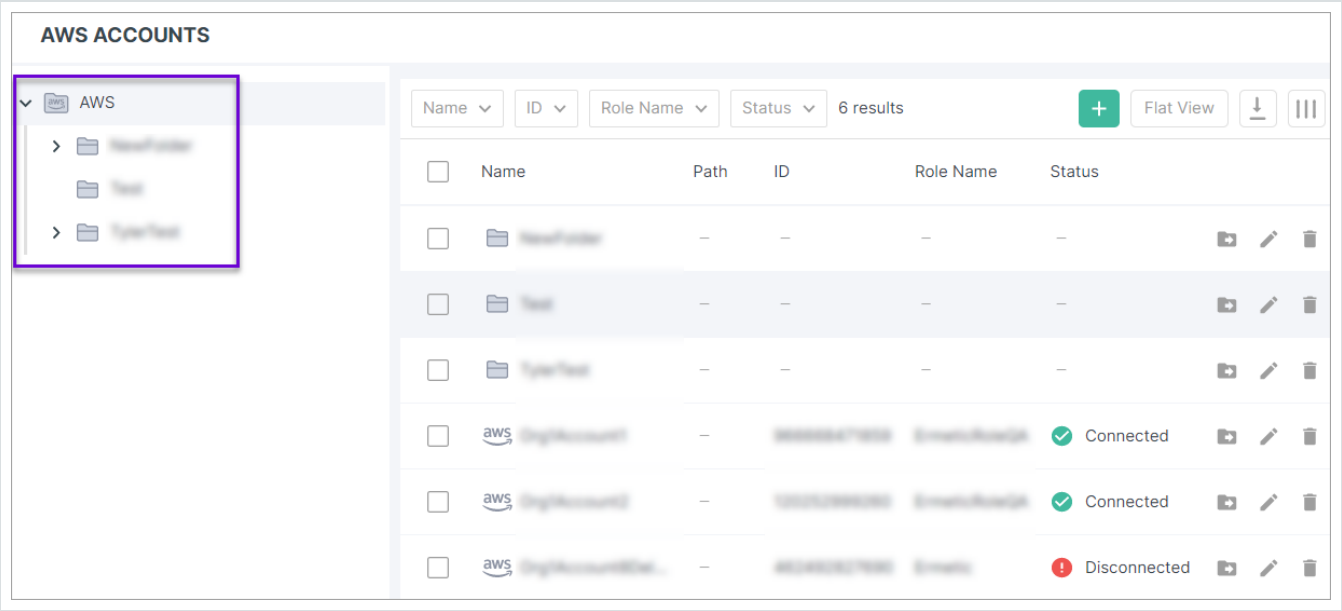
- AWS 組織単位 (OU)
- Alibabaクラウド組織
- Azure 管理グループ
- GCP フォルダー
- OCI テナンシ

カスタムフォルダーはツリー構造内でフォルダーアイコンでマークされ、アカウントにはそれぞれのクラウドプロバイダーのアイコンでマークされます。

フォルダーを操作するには

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Accounts]** に移動して、いずれかのプロバイダーを選択します。

   既存のフォルダーは、ページの左側にあるツリーに表示されます。



2. フォルダーを追加する場所に移動します。たとえば、ルート AWS フォルダーの下に追加する場合は、ツリーで AWS フォルダーを選択します。

   フォルダーを選択すると、そのフォルダーに属するすべてのアカウント (およびネストされたフォルダー) がメインテーブルに表示されます。

3. [+]、**[フォルダーの作成]** の順にクリックします。

4. 新しいフォルダに一意の名前を入力し、**[フォルダの作成]** をクリックします。

   左側のツリー階層と、アカウントとフォルダーのメインテーブルにフォルダーが表示されます。

5. フォルダーの名前を変更するには、フォルダーの横にある **[編集]** ボタンをクリックし、新しい名前を入力します。

6. フォルダーを削除するには、フォルダーの横にある **[削除]** ボタンをクリックし、削除を確定します。

7. フォルダーを移動するには、フォルダーの横にある **[移動]** ボタンをクリックし、関連するフォルダーを選択してフォルダーの新しい場所を選択します。

注意: Organization (組織)、AWS、Alibaba Cloud、Azure、GCP、または OCI の親フォルダーを削除、名前変更、または移動することはできません。異なるクラウドプロバイダーのアカウントをグループ化することはできません。

アカウントの範囲

アカウント範囲は、オンボーディングされたクラウドアカウント、アイデンティティプロバイダーテナント、IaC リポジトリ、またはそのようなアカウントのグループを表し、次のいずれかになります。

- 組織全体 (クラウドサイバーエクスポージャーにオンボーディングされたすべてのアカウント)。
- アカウントのグループ。たとえば、特定のクラウドプロバイダー (すべての AWS アカウント) またはアイデンティティプロバイダー (すべての Microsoft Entra ID テナント) に属するすべてのアカウント、あるいは特定のクラウドプロバイダー内のアカウントのグループ (アカウントフォルダーの作成別にグループ化) などです。
- 特定のアカウントやアイデンティティプロバイダーのテナント。
- プロジェクト
- すべての IaC 組織、または個々のリポジトリのサブセット。これにより、特定の範囲のコードスキャン結果を表示するためのアクセスが付与されます。

特定のアカウント範囲においてコンソールアカウント範囲によるコンソールデータのフィルタリングおよび機能の設定クラウドサイバーエクスポージャーコンソールで機能を設定できます。

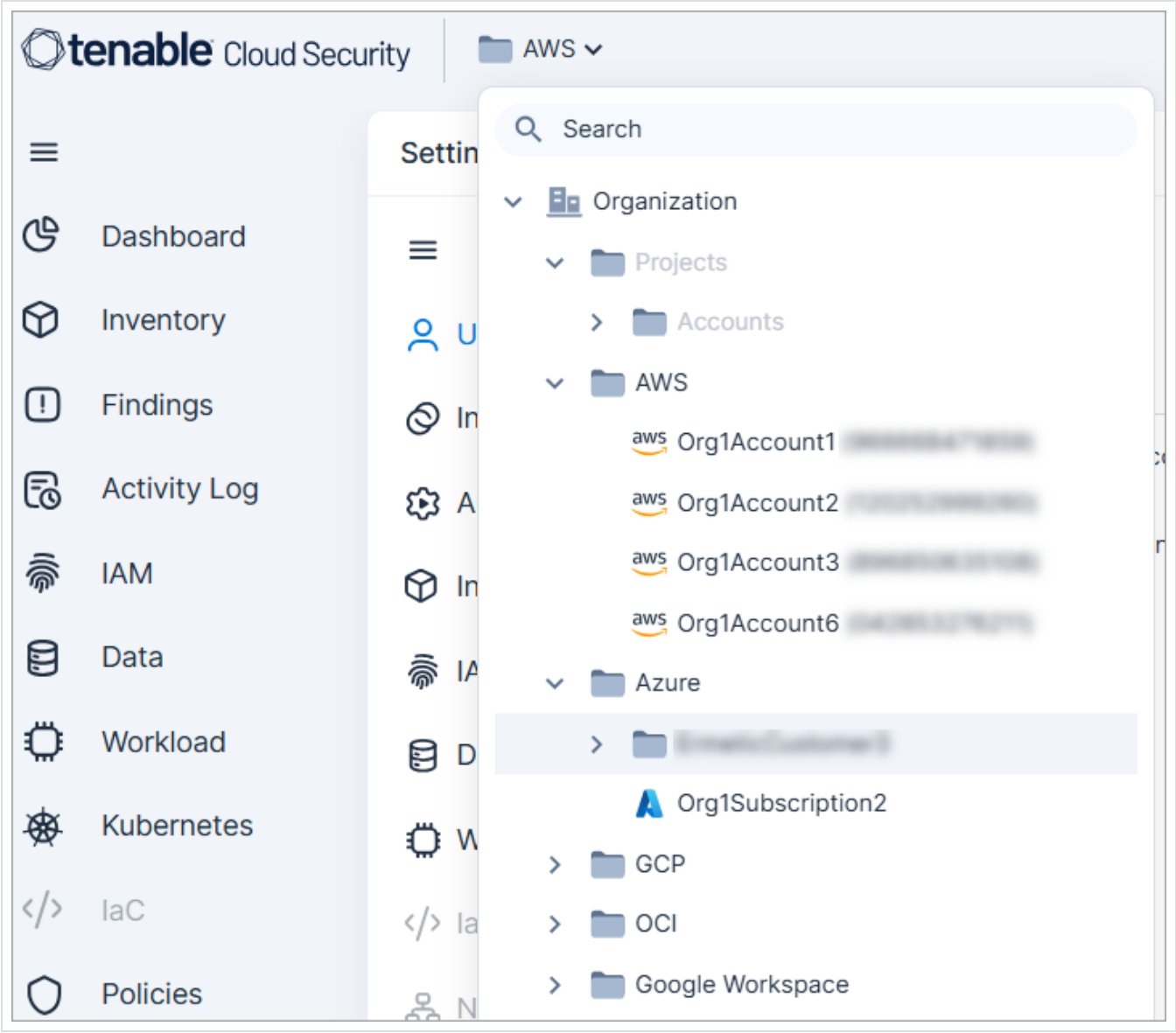
アカウント範囲によるコンソールデータのフィルタリングおよび機能の設定

特定のアカウント範囲内において、クラウドサイバーエクスポージャーコンソールで特定の機能を表示および構成します。たとえば、特定の Azure アカウントの違反をモニタリングするカスタムポリシーを作成できます。

- 選択したアカウント範囲は、コンソールのページ間を移動しても保持されます。選択した範囲に設定されたままになり、手動で変更しない限りデフォルトに戻ることはありません。
- アカウント範囲のフィルターでは、一度に 1 つの範囲のみ選択できます。このフィルターでは、複数のアカウント範囲を一度に選択することはサポートされていません。**代わりの方法を教えてください。**
    1. 目標とする範囲を含むプロジェクトを作成し、プロジェクト別にフィルタリングします。
    2. 関連するコンソールのページ内で、[アカウント] フィルターを使用すると、複数のアカウント範囲を一度にフィルタリングできます。たとえば、検出結果ページ内や、データ/ワークロードページ全体です。デフォルトでフィルターが表示されない場合は、フィルターを追加する必要があります。

アカウント範囲ごとに機能を表示/設定する方法

- コンソールの任意のページから、アカウント範囲のドロップダウンをクリックし、範囲を選択します。



選択した範囲により、実行できるアクションはさまざまな影響を受けます。たとえば、次の点を考慮します。

- **カスタムポリシー**: カスタムポリシーを有効または無効にできるのは、そのポリシーを作成した元のフォルダーやアカウントからのみです。たとえば、最上位の AWS フォルダーからカスタムポリシーを作成し

た場合、そのAWSフォルダー内の子フォルダー/アカウントからポリシーを有効化/無効化することはできません。詳細については、「クラウドポリシー: カスタムを参照してください。

サポートされている機能

ほとんどのコンソール機能は、次のようなアカウント範囲で表示および設定できます。

- クラウドサイバーエクスポージャーユーザーを追加する
- 統合を追加する
- レポートの作成
- ライセンス使用状況データの表示
- Kubernetesクラスタを表示する
- JIT使用資格の追加 (クラウドアカウントのみ)
- ワークロード保護の設定を行う(クラウドアカウントのみ)
- ポリシーの有効化/無効化 (クラウドアカウントのみ)
- 自動化ルールの作成 (クラウドアカウントのみ)
- コンプライアンススコアを表示する(クラウドアカウントのみ)
- IaCコードのスキャン結果を表示する(IaC組織のみ)

アカウントの継承

組織レベルまたはアカウント (フォルダー) のグループ内で作成されたエンティティは、今後作成される子アカウントを含め、すべての子アカウントに継承されます。たとえば、継承されたユーザーです。

プロジェクトの仕組み

これは、プロジェクトの仕組みに関する概念上の概要です。プロジェクトを設定する方法については、プロジェクト参照してください。

複数のプロバイダーにわたる多数のクラウドアカウントまたはリソースを管理することは容易ではなく、特にアカウントの作成と削除が頻繁に行われる場合には困難です。Tenable One Cloud Exposureのプロ

ジェクトは、アカウントまたはリソースを論理的にグループ化することで、アクセスの管理を簡素化し容易にします。

たとえば、プロジェクトを使用すると、クラウド環境の組織の異なる運用グループに基づいてコンソールデータを表示できます。アカウントまたはリソースをプロジェクトに整理することで、可視性とアクセス許可を既存の組織構造に合わせて調整でき、より直感的で効率的な管理エクスペリエンスを実現できます。プロジェクトでは、ユーザーに必要なアカウントやリソースに固有のアクセス許可を付与できるため、アクセス制御も合理化され、手作業の労力が削減され、クラウド管理が改善されます。

開始方法

1. プロジェクトの仕組み、サポートされている機能、およびプロジェクトの一般的なユースケースについて説明します。
2. プロジェクトを追加するとプロジェクトフォルダーを追加するを追加します。
3. アカウント階層とフォルダーことで、ユーザーに特定のプロジェクトスコープへのコンソールアクセス権を付与します。

プロジェクトの仕組み

プロジェクトは、クラウド環境内のリソースを論理的にグループ化したものであり、複数のクラウドプロバイダーにまたがる場合でも柔軟な組織化と管理が可能になります。1つのアカウントが複数のプロジェクトに属することができるため、さまざまな運用ニーズに応じてアクセスや可視性を構築できます。プロジェクトを作成した後、その範囲内でコンソールデータを表示するアクセス許可をコンソールユーザーに割り当てることができます。さらに、プロジェクトの設定により、プロジェクトに割り当てられたユーザーが、そのプロジェクトのスコープ内のアカウントへのアクセス権を自動的に取得することもできます。

プロジェクトは、1つ以上のスコープグループで構成されます。各範囲グループは以下で構成されます。

- **クラウドアカウントのグループ***. これは、次のうちの1つ以上の任意の組み合わせです。
    - アカウント (AWS など)
    - ID プロバイダーテナント (Google Workspace など)。
    - コードリポジトリの接続 (GitHub 企業など)

上記のそれぞれに対して、ルートフォルダー全体 (AWS など)、個別のフォルダー、個別のアカウントなど、任意の範囲を選択できます。たとえば、範囲グループは、すべての AWS と Azure の開発アカウントで構成できます。さらに、企業全体を範囲グループとして選択できます。

- (オプション) **1 つ以上の論理条件***。
    - 含めるアカウントが一致するパターンを指定して、プロジェクトの範囲を制限します。
    - 条件パターンは、アカウント名、アカウントタグ、リソースタグ、Azure リソースグループ名に基づく場合があります。これらの設定方法の詳細については、プロジェクトを追加する参照してください。

プロジェクトを使用するタイミング

プロジェクトの作成かどうかと方法を決定する際は、クラウドアカウントのフォルダー構造を自動的に更新選択しているかどうかを検討してください。

- **このオプションを有効にした場合**、オンボード組織のフォルダー構造は、プラットフォームにそのままコピーされ、組織でフォルダーやアカウントを移動、編集、作成することはできなくなります。その結果、アカウントのグループ化の柔軟性をさらに高めるために、プロジェクトは役立つことがわかりました。
- **このオプションを無効にすると**、各プロバイダーのフォルダー構造内でアカウントを整理しやすくなります。この場合、Tenable では、可能な限りプロバイダー固有のフォルダー内でアカウントを手動でグループ化し、手動のグループ化がニーズを満たさない場合にのみプロジェクトを使用することを推奨します。

プロジェクトの一般的なユースケース

このセクションでは、企業がプロジェクトとプロジェクトフォルダーを使用してクラウドアカウント管理を合理化する一般的な方法をいくつか紹介します。たとえば、次のようなプロジェクトを作成できます。

- **所有権と責任別にアカウントを整理します**。
    - プロジェクト
    - プロジェクト

- **インフラとオペレーション別にアカウントを整理します**。
    - プロジェクト
    - アプリケーションおよびサービス境界用のプロジェクトを作成する (Azure)

製品グループのプロジェクトの作成

大規模な企業には多くの場合、独自のクラウドアカウントを管理する複数の製品チーム (グループ A、グループ B、グループ C など) があります。各グループは、アカウントを区別するために異なるアカウント命名規則またはアカウントタグを使用する場合があります。

実装方法

1. 製品グループごとにプロジェクトを追加します (例:「グループ A プロジェクト」、「グループ B プロジェクト」)。
2. 条件を追加し、**アカウントタグ** または **命名** 規則を使用してアカウントを適切なプロジェクトに動的に割り当てます。
    - タグキー/値パターンの例
        - キーは `product`、値は `GroupA`
        - キーは `team`、値は `GroupB`
    - 名前パターンの例:
        - `group-a-prod-001`
        - `group-b-dev-002`
3. プロジェクトフォルダーを追加して、地域または他の関連カテゴリ別にプロジェクトを整理します。
4. ユーザーとグループことで、ユーザーに特定のプロジェクトスコープへのコンソールアクセス権を付与します。以下に例を挙げます。
    - 地域の管理者に、プロジェクトフォルダーレベルですべての子プロジェクトを一度に管理するアクセス権を付与します。
    - 個別のプロジェクトへのチーム固有のアクセス権を付与します。

ビジネス機能用のプロジェクトの作成

多くの企業は、財務、コンプライアンス、オペレーションなどの事業の機能に基づいてクラウドリソースを分類します。リソースタグパターンを利用することで、事前定義されたタグキーと値のペアに基づいてアカウントをプロジェクトに動的に割り当て、ビジネス機能に基づいてプロジェクトを作成できます。

実装方法

1. 各事業の機能に対してプロジェクトを追加します。
2. 条件を追加し、**リソースタグ**パターンを使用して適切なプロジェクトにアカウントを動的に割り当てます。
    - タグキー/値パターンの例
        - キーは `business_unit`、値は `finance`
        - キーは `compliance_level`、値は `high*`
3. (オプション) プロジェクトフォルダーを追加し、プロジェクトをより広いカテゴリでグループ化します。
4. ユーザーとグループことで、ユーザーに特定のプロジェクトスコープへのコンソールアクセス権を付与します。以下に例を挙げます。
    - すべての環境でより広いアクセスを許可するには、プロジェクトフォルダーレベルでアクセス権を付与します。
    - プロジェクト固有のアクセス権を付与します。

開発アカウントと本番アカウント用のプロジェクトを作成する

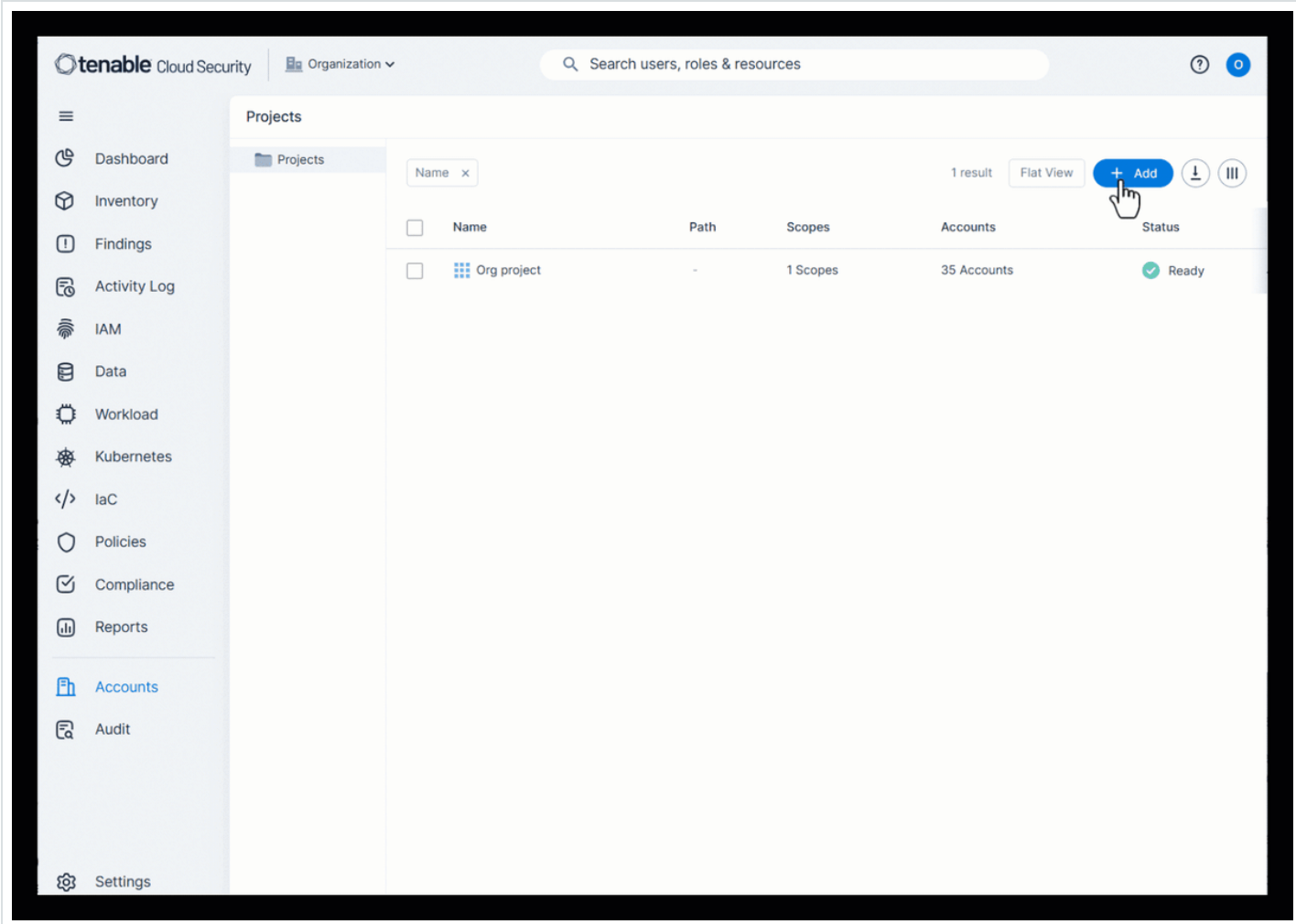
多くの企業では、開発環境と本番環境を厳格に分離しています。これを徹底するには、環境タイプに基づいてアカウントをグループ化するプロジェクトを作成し、本番プロジェクトにテスト関連のアカウントが含まれないようにします。

実装方法

1. **開発**アカウント用のプロジェクトを追加します。
2. 条件を追加し、**アカウントタグ**または**名前**パターンを使用して適切なプロジェクトにアカウントを動的に割り当てます。

- タグキー/値パターンの例
    - キーは environment、値は dev*
    - キーは stage、値は staging*
- 名前パターンの例
    - dev*

3. テストアカウントをプロジェクトから除外します。
    - 名前パターンの除外の例
        - ない test
4. プロジェクトから実稼働アカウントを除外します。
    - タグキー/値パターンの除外の例
        - キーは typeではありません、値は prod*ではありません
5. **本番環境** のアカウントにプロジェクトを追加します 。
6. アカウントタグまたは命名規則を使用して、アカウントを適切なプロジェクトに動的に割り当てるための条件を追加します。
    - **実稼働** タグの鍵/値のパターンの例:
        - キーは environment、値は prod*
        - 名前パターンの例
        - prod*
7. (オプション) **開発** プロジェクトフォルダーを追加して、すべての開発プロジェクトを整理します。
8. (オプション) **生産** プロジェクトフォルダーを追加して、すべての開発プロジェクトを整理します。
9. ユーザーとグループことで、ユーザーに特定のプロジェクトスコープへのコンソールアクセス権を付与します。以下に例を挙げます。
    - すべての環境でより広いアクセスを許可するには、プロジェクトフォルダーレベルでアクセス権を付与します。
    - プロジェクト固有のアクセス権を付与します。



アプリケーションおよびサービス境界用のプロジェクトを作成する (Azure)

Azure を使用する企業の場合、リソースグループは、クラウド資産を管理するための主要な組織構造として機能します。Azure リソースグループの名前のパターンを利用することで、アプリケーションの所有権、ワークロードのタイプ、地理的リージョンなどの運用境界に合わせたプロジェクトを作成できます。

実装方法

1. 関連する Azure グループごとにプロジェクトを追加します (例:「顧客向けのアプリ」または内部 IT サービス)。
2. 条件を追加し、**Azure リソースグループ名の** パターンを使用して適切なプロジェクトにアカウントを動的に割り当てます。

- リソースグループ名のパターンの例
    - `cust-facing-apps-*` (外部向けのアプリケーション用)
    - `internal-it-*` (内部 IT サービス用)

3. (オプション) プロジェクトフォルダーを追加し、プロジェクトをより広いカテゴリでグループ化します。
4. ユーザーとグループことで、ユーザーに特定のプロジェクトスコープへのコンソールアクセス権を付与します。以下に例を挙げます。
    - すべての環境でより広いアクセスを許可するには、プロジェクトフォルダーレベルでアクセス権を付与します。
    - プロジェクト固有のアクセス権を付与します。たとえば、開発者にはお客様向けアプリへのアクセス権のみを付与し、IT 管理者には内部 IT サービスプロジェクトへのアクセス権を付与します。

サポートされている機能

クラウドサイバーエクスポージャーの多くの機能はプロジェクトをサポートしており、特定のプロジェクトスコープ内でアクションを実行できます。一致するプロジェクト範囲が割り当てられたユーザーのみがこれらの機能を表示/管理できます。

たとえば、プロジェクトスコープに対して以下を実行できます。

- プロジェクトスコープへのアクセスを付与する
- 統合
- レポートの作成
- カスタム標準の追加
- APIトークンを作成し、クラウドサイバーエクスポージャー APIをクエリする
- ライセンス
- クラウドポリシー: カスタム

したがって、たとえば、プロジェクト A に割り当てられたユーザーのみが、そのスコープの API トークンを作成できます。

プロジェクトのアクセス許可と機能

プロジェクトのアクセス許可は、プロジェクト内で論理的にグループ化されたリソースに対してユーザーが実行できるアクションを定義します。これらのアクセス許可は、直接ロール割り当てを使用して明示的に付与されたり、プロジェクトスコーププロパゲーションを介して自動的に拡張されたりすることができます。このセクションでは、プロジェクト関連のアクセス許可の合計数が決定される方法と、それらのアクセス許可によって有効になる特定のアクションについて説明します。

プロジェクトのアクセス許可

プロジェクト権限により、プロジェクト内で何を実行できるかが決まります。これらのロールは、管理者がプロジェクトスコープへのアクセスを付与すると、あなたに直接付与されます。このロールにより、プロジェクト自体を表示および管理できますが、プロジェクト内の個別のスコープを設定するアクセス権は自動的に付与されません。

プロジェクトのアクセス許可:

- 主に、データの整理やフィルタリングのための表示専用アクセスを提供します。
- プロジェクトのスコープ内でほとんどの設定変更を許可しないようにします。たとえば、に組み込まれているポリシーでは設定変更できません。

> **注意:** ただし、以下の操作は実行できます。
> - リソースを機密としてマークします。
> - 検出結果のステータスを変更します。

プロジェクト内のアカウントに対するユーザーの有効なアクセス許可は、それらのアカウントに対して他の直接割り当てがある場合、より高くなる可能性があります。

伝播

プロパゲーションは、プロジェクトからユーザー権限を自動的に拡張し、そのプロジェクトにスコープも含める機能です。プロジェクトが伝播を有効にして設定されると、そのプロジェクト内のすべての対象範囲にプロジェクトレベルのロールが自動的に適用されます。

重要: 伝播は、このプロジェクトで定義されたリソースベースの条件でフィルターされていない範囲にのみ適用されます。

仕組み

- **伝播なし**: アクセス許可はプロジェクト自体にのみ適用されます。
- **伝播ありの場合**: アクセス許可が拡張されます。伝播が有効になっているプロジェクトの管理者である場合、そのプロジェクト内のすべての対象範囲で自動的に管理者になります。これにより、アクセス管理が合理化され、管理する必要があるリソース全体で一貫したアクセス許可が得られます。つまり、プロジェクトレベルで自分に割り当てられたロールに基づいて、伝播されたアカウントで設定の変更やその他のアクションを実行できるようになります。

有効なアクセス許可

複数のロールが割り当てられている場合、最後のアクセス許可 (有効なアクセス許可) が常に、自分に付与される最高レベルのアクセス権となります。たとえば、あるスコープの表示者であるが、プロジェクト プロジェクトを通じて同じスコープへの管理者アクセス権を取得した場合、そのアカウントの有効なアクセス許可は管理者となります。より高いレベルのアクセス許可が常に優先されます。

検出結果のライフサイクル

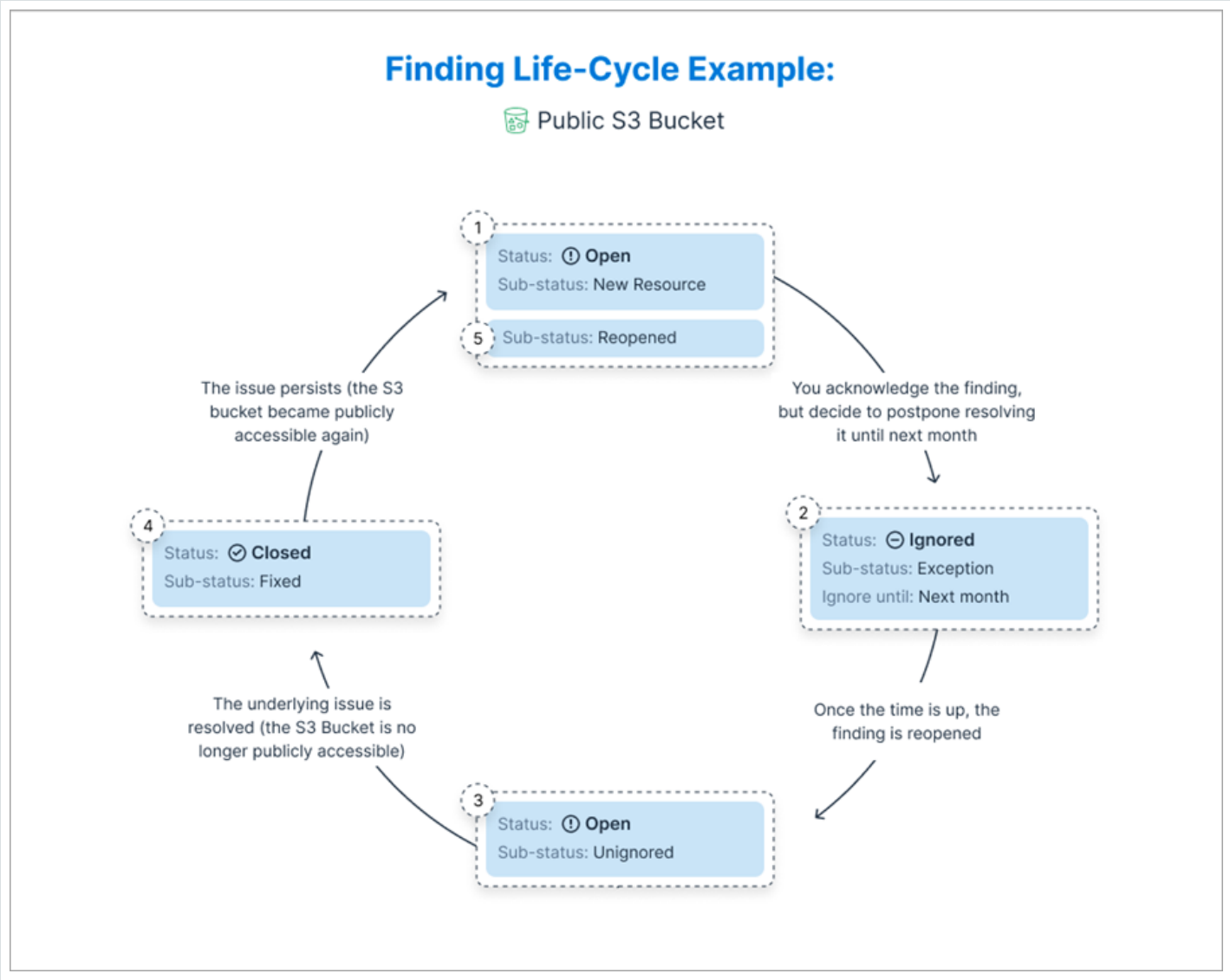
検出結果は、個別のステータスとサブステータスでライフサイクル全体にわたって進行します。これは、リスクの全体的な状態と、検出結果が現在のステータスになっている理由を理解するのに役立ちます。

これは、検出結果のステータスと検出結果のライフサイクルに関する概念です。

- 検出結果の表示と管理に関するハウツーガイドについては、クラウドの クラウドの検出結果 または IaC 検出結果。
- 検出結果の深刻度の仕組みの概念概要については、「 検出結果の深刻度」を参照してください。
- (ポリシーを介して) 検出結果を作成する方法を設定するには、クラウドポリシー や IaC ポリシーを参照してください。

検出結果ライフサイクルの例

この画像は、環境内で検出された検出結果 (パブリック S3 バケット) のフローと進行状況の例を示しています。特定のステータスとサブステータスの詳細については、検出結果のステータスを参照してください。

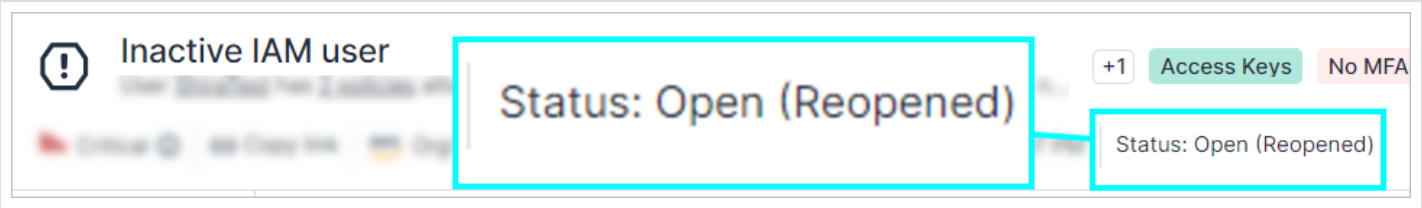


検出結果のステータス

検出結果のステータスを確認することで、以下の 2 点を把握しやすくなります。

- 組織におけるリスクの全体的な状態 (ダッシュボードを管理するの [トレンド] ウィジェット)。
- 特定の検出結果がオープン/クローズされた理由。これは、行った作業と、検出結果の解決とクローズまでの進行状況を追跡するのに役立ちます。

ステータスは、メイン **のステータス** (オープン/無視/クローズ) とサブステータスで構成されます。サブ **ステータス**には詳細情報と、検出結果が現在のステータスである理由が記載されています。この例では、ステータスが「オープン」、サブステータスが「再オープン」になっています。



未解決の検出結果

未解決の検出結果は、環境内で検出されたアクティブな問題を表しています。これには、リスクのあるアイデンティティやリソース、見つけるのが難しい有害な危険な組み合わせが含まれます。

この表は、オープンの検出結果のサブステータス一覧です。サブステータスには詳細情報と、検出結果が現在のステータスである理由が記載されています。

サブステータス	定義
新しいリソース	リソースは過去 1 週間以内に作成され、ポリシールールに一致しています。作成時間が取得できず、リソースが最新のデータの同期と更新の頻度 (過去 1 週間以内) で検出されたが、それ以前のスキャンでは検出されない場合、そのリソースは新しいリソースと見なされます。
既存のリソース	Tenable は以前にこのリソースをスキャンしましたが、ポリシールールと一致したのは今回が初めてです。アカウントがオンボーディングされた後の最初のデータの同期と更新の頻度であり、リソースの作成時間を取得できない場合は、リソースは既存のリソースと見なされます。
再開されまし	検出結果が **[クローズ]** から **[オープン]** に移行しました。

サブステータス	定義
た	• システム - 問題が解決していない。以前解決したが再び発生。 • 手動 - 検出結果は検出結果を手動でクローズするが、ユーザーが手動で再オープンしました。
無視解除	無視する除外が更新、無効化、削除、または期限切れとなった場合、検出結果は無視から**オープンに移行**しました。
異常	Tenable は、アイデンティティまたはリソースアクティビティに基づいて異常を検出しました。すべての 異常検出 ポリシーにこのサブステータスが割り当てられます。

無視した検出結果

無視された検出結果は、すぐに処理しなくてもよい問題を表します。関連するリソースは永久に、または設定された期間、除外されます。

この表は、無視の検出結果のサブステータス一覧です。サブステータスには詳細情報と、検出結果が現在のステータスである理由が記載されています。

サブステータス	定義
例外	検出結果は、修正が完了するまで一時的に受け入れられます。
誤検出	検出結果が不正確または無関係であることが確認されました。
設計上	この構成は意図的なものであり、機能のために必要です。

無視した検出結果は除外されるため、検出結果を無視したり、ビジネスニーズに基づいて深刻度を調整したりできます。無視 無視された検出結果からのパターンベースの除外の作成 方法、除外を監査して維持するする方法を説明します。

解決済みの検出結果

クローズの検出結果は、ユーザーによって手動で、またはTenableによって自動でクローズされた問題を表しています。

この表は、クローズの検出結果のサブステータス一覧です。サブステータスには詳細情報と、検出結果が現在のステータスである理由が記載されています。

サブステータス	定義
修正済み	検出結果は解決されました • リソースがポリシールールと一致しなくなった。 • Tenable のポリシーの推奨事項に従って、リソースが削除された。たとえば、アクティブでない GCP サービスアカウントが削除された場合など。関連する検出結果タイプの一覧については、リソース削除の推奨事項を伴う検出結果 を参照してください。
誤検出	検出結果が Tenable によって誤検出としてマークされました。
手動で閉じられました	ユーザーが検出結果を手動で「クローズ」としてマークしました。
リソースが削除されました	リソースは削除されましたが、Tenable のポリシーでは削除は推奨されていません。

サブステータス	定義
自己解決済み	リソースの状態またはそのアクセス許可が変更されたため、Tenable は問題がまだ解決されていないかどうかを判断するために別の評価サイクルを実行する必要があります。例: • 過剰な権限を持つアイデンティティのアクセス許可が変更された • 再びアクティブになった非アクティブな IAM ロール • ユーザーが過剰な権限を持つ IAM グループに追加された (新しく作成されたメンバーがグループに追加されたため再分析) • アクセス許可セットが新しいアカウントに割り当てられた

コンプライアンスの仕組み

Tenable One Cloud Exposure は、堅牢な評価プロセスを通じて、クラウド環境のさまざまなコンプライアンス基準への準拠状況を監視するのに役立ちます。これらの評価の仕組みを理解することが、コンプライアンス態勢を効果的に管理する上で重要です。

これは、コンプライアンス評価の仕組みの概要です。コンプライアンスの監視に関するメソッドガイドについては、コンプライアンス参照してください。

ベンチマークガイドラインとポリシーマッピング

クラウドサイバーエクスポージャーにおけるコンプライアンスは、CIS、AWS ウェルアーキテクチャード、GDPR 規格一覧のさまざまな標準から、業界で認められたベンチマークガイドラインに基づいています。これらのベンチマークは、セキュリティ設定とベストプラクティスを定義します。Tenable その後、これらのガイドラインを特定のクラウドポリシーに変換します。各ポリシーは詳細なチェックとして機能し、特定のベンチマークに対してクラウドリソースを評価します。

重要: Tenable の組み込みコンプライアンスフレームワークは、特定の標準に対する完全なコンプライアンスを保証するものではありません。企業は、評価が法および規制の要件に適合するようにする必要がありま

す。コンプライアンスのニーズは製品、ドメイン、ビジネスプラクティスによって異なるため、関連するカスタム標準の追加 ことをお勧めします (標準の複製ことで、作り込みのカスタム標準をベースにできます)。

CIS ベンチマーク

CIS ベンチマークは、企業のコンプライアンス態勢を測定する上で最適な開始点になります。クラウドサイバーエクスポージャー で標準装備のこれらのスコアを使用して、クラウドプロジェクト やアカウント のコンプライアンススコアを比較したり、全体的なコンプライアンスポリシーと統合したりできます。

Tenable は設定を希望の設定に適合させることに重点を置き、強力なセキュリティのベースラインを提供します。CIS の推奨事項に、直接優先順位付けをするための深刻度が割り当てられていることはありませんが、CIS はベンチマークを以下のレベルに分割することで優先順位付けを容易にします。

- レベル 1 は重要な推奨事項をカバーします
- レベル 2 (および場合により 3) は、より厳格なセキュリティ設定に対応しています。

注意: Tenable は、最新の CIS ベンチマークのサポートを継続的に更新するために作業しています。規格一覧のリストを参照してください。ベンチマークサポートに関連する緊急リクエストの場合、サポートへの問い合わせ。。

手動と自動化された推奨事項

CIS ベンチマークの推奨には、CIS ベンチマークの推奨が自動チェックで環境状態を評価できるか、または手動の調査が必要かどうかを表す評価ステータスが含まれています。それぞれの推奨事項について、CIS ベンチマークは手動または自動としてラベル付けします。

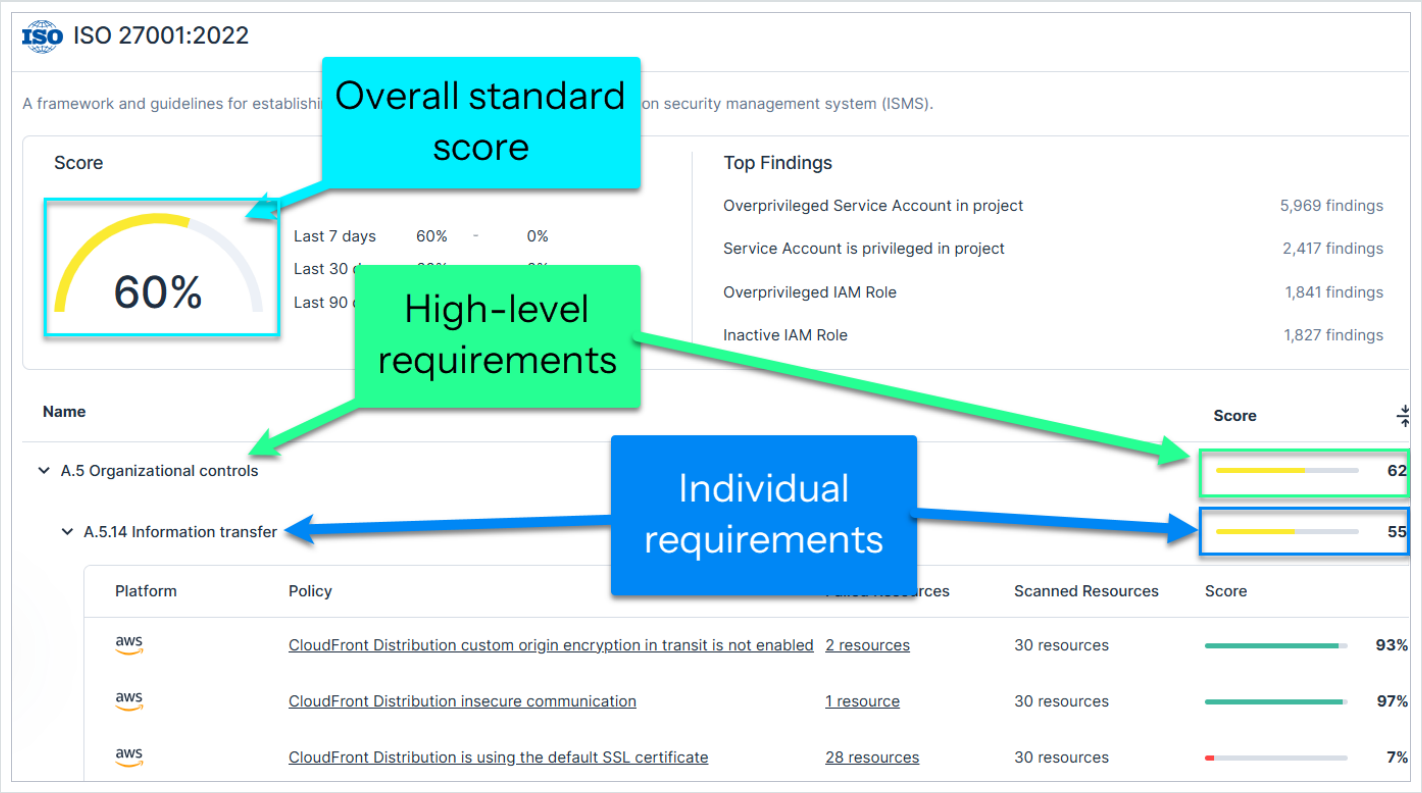
- **マニュアル**. 環境の設定状態が想定どおりであるかどうかを判断するために、手動の手順が必要です。合否の評価結果を自動的に達成することはできません。クラウドサイバーエクスポージャー は通常、技術的な複雑性からマニュアルの推奨事項に対応できませんが、特定の場合には部分的に対応する場合があります。
- **を自動化しました**。構成評価ツールを使って、環境状態を推奨状態に照らして自動的に評価できます。自動的に合否の評価結果を得ることができます。

詳細については、CIS のウェブサイト を参照してください。

コンプライアンススコアを理解する

コンプライアンススコアは、ポリシーベンチマークに合格したリソースの割合を表します。

- **総合的な標準スコア**: 全体的な標準のパーセンテージは、関連するすべての個別の要件のパーセンテージを平均して計算されます。
- **高レベルの要件スコア**: 同様に、高レベルの要件 (複数の個別の要件をグループ化したもの) についても、割合はその特定の高レベルの要件の下のすべての個別の要件の割合を平均することで計算されます。
- **個別の要件スコア**: 個別の要件の割合は、要件に関連するすべてのポリシーの割合を平均して計算されます。

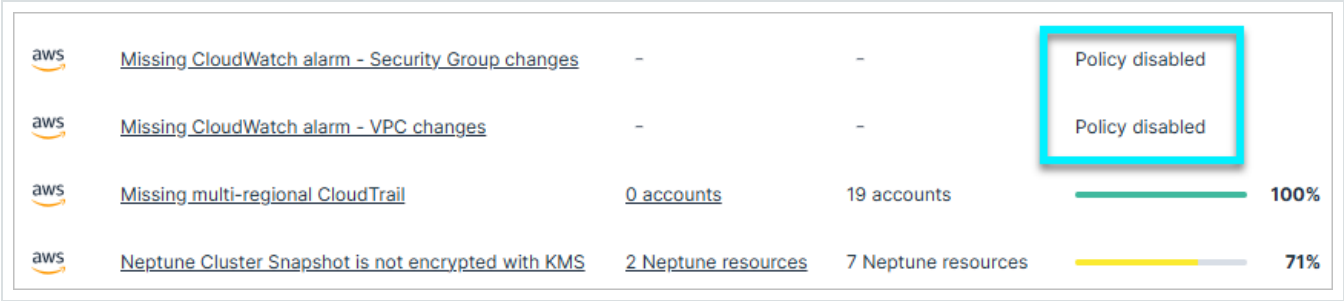


スコアが 100% の場合、以下を表します。

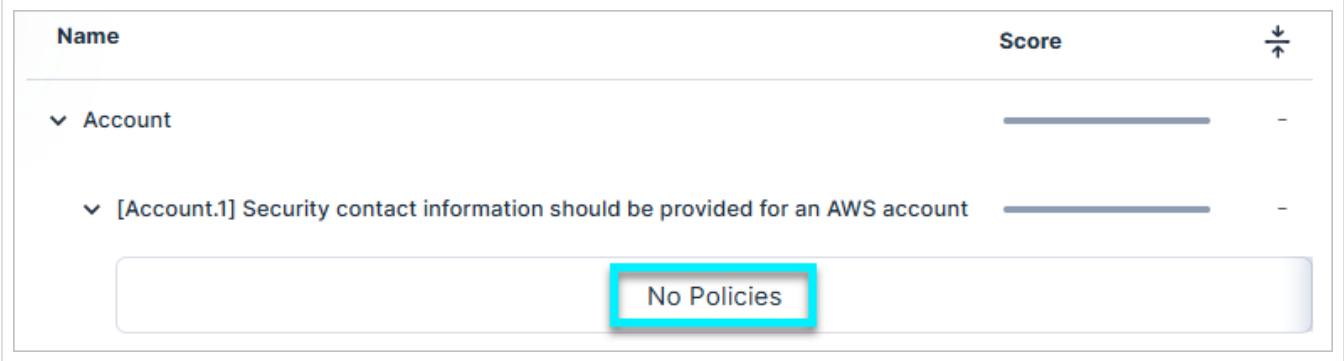
- すべてのリソースが要件に合格しました (0 失敗)。
- リソースがスキャンされませんでした。

以下の状況では、コンプライアンススコアに個別の要件は考慮されません。

- ポリシーが標準を有効または無効にする
  いる場合



- 個別の要件

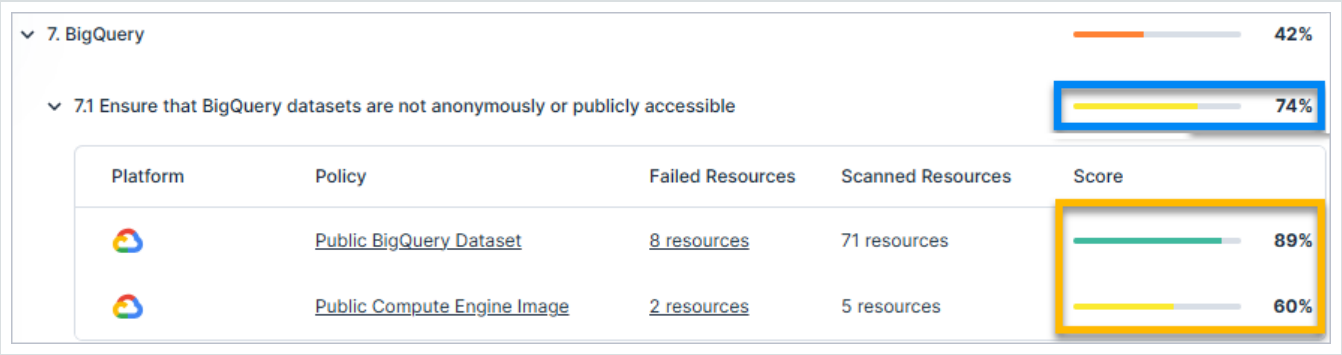


  にマッピングされたポリシーがない場合

例：コンプライアンススコアの計算

次の例は、さまざまな詳細レベルでの単純な平均に基づいて、コンプライアンススコアがどのように計算されるかを示しています。

1. **個別の要件スコアの計算** 個別の要件スコアは、それに関連するすべてのポリシーの割合を平均することで決定されます。

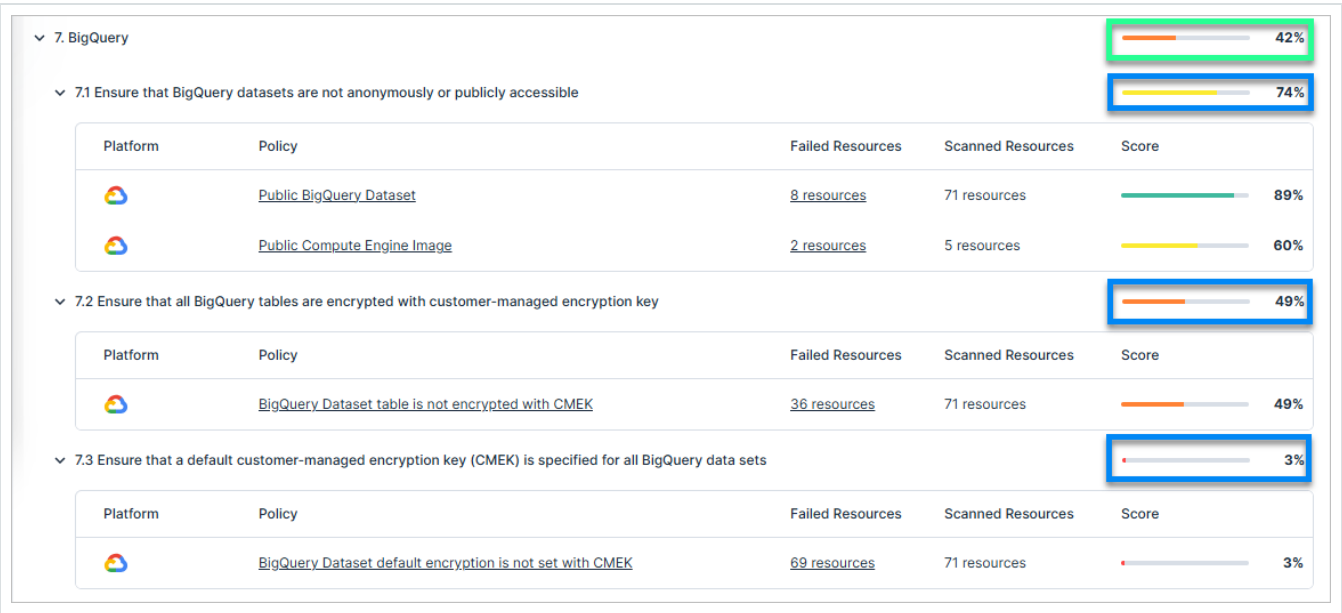


- **例**: 7.1 BigQuery データセットが匿名または一般公開されないようにします

ポリシー名	スコア
パブリック BigQuery データセット	89%
パブリック Compute Engine イメージ	60%

- 個別の要件の計算:
  (89% + 60%) / 2 = 149% / 2 = 74.5% **74%**

2. **高レベル要件スコアの計算**。高レベルの要件のスコアは、その下にあるすべての個別の要件のスコアを平均して計算されます。

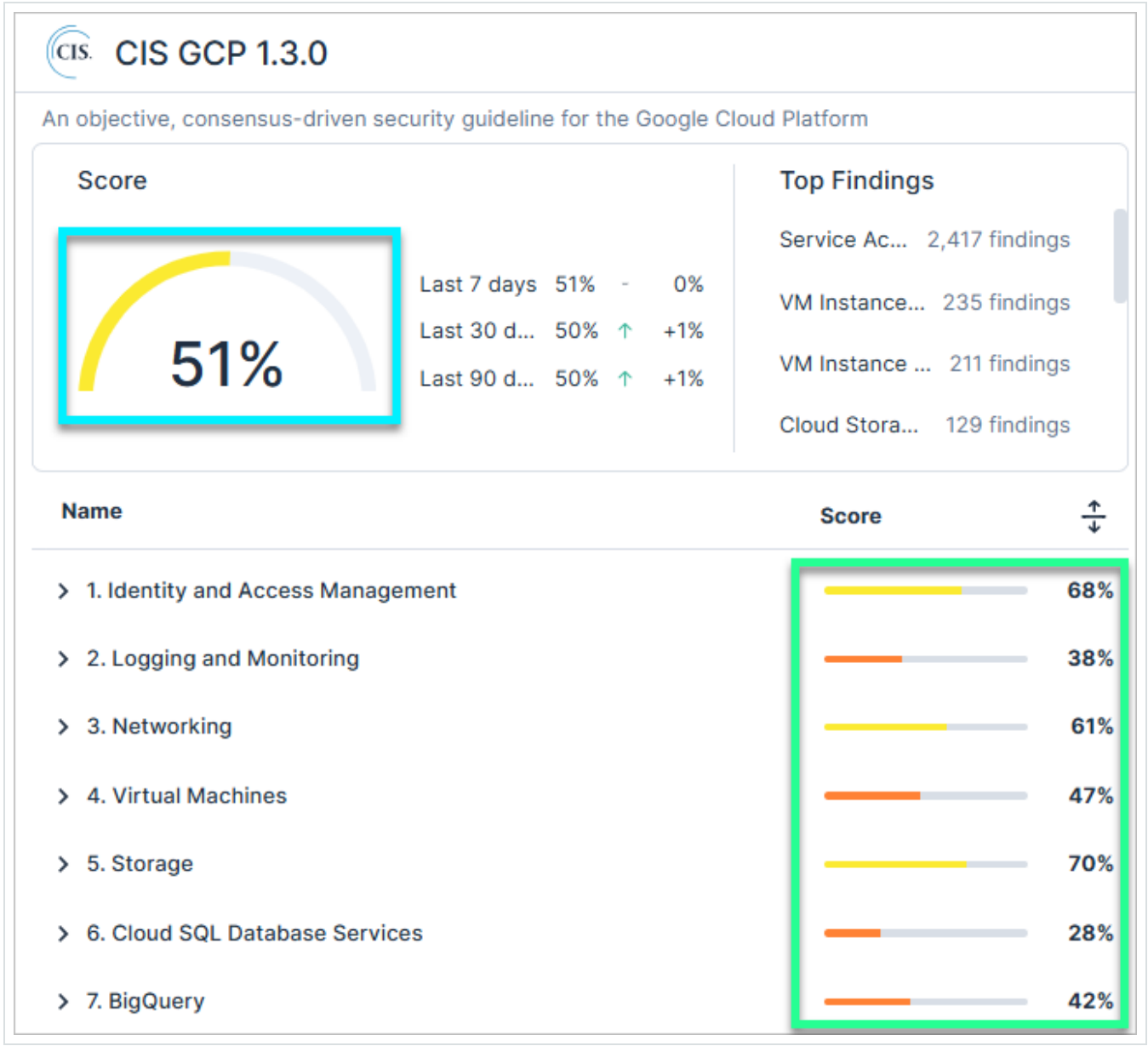


- **例**: 7. BigQuery (高レベル要件)

個別の要件	スコア
7.1 (匿名でない BigQuery データセット)	74%
7.2 (CMK で暗号化された BigQuery テーブル)	49%
7.3 (BigQuery データセットに対してデフォルトの CMK を指定)	3%

- 高レベル要件の計算:
  (74% + 49% + 3%) / 3 = 126% / 3 = **42%**

3. **全体的な標準スコア計算**。総合的な標準スコアは、コンプライアンス基準全体の個別の要件スコアの平均です。


CIS GCP 1.3.0
An objective, consensus-driven security guideline for the Google Cloud Platform
Score
51%
Last 7 days 51% - 0%
Last 30 d... 50% ↑ +1%
Last 90 d... 50% ↑ +1%
Top Findings
Service Ac... 2,417 findings
VM Instance... 235 findings
VM Instance ... 211 findings
Cloud Stora... 129 findings
Name
Score
1. Identity and Access Management 68%
2. Logging and Monitoring 38%
3. Networking 61%
4. Virtual Machines 47%
5. Storage 70%
6. Cloud SQL Database Services 28%
7. BigQuery 42%

- **例**: CIS GCP 1.3.0 規格

重要度高の要件	スコア
IDおよびアクセス管理 (アイデンティティアクセス管理)	68%
ログとモニタリング	38%
ネットワーキング	61%
仮想マシン	47%
ストレージ	70%
クラウド SQL データベースサービス	28%
BigQuery	42%

- 総合的な標準の計算:
  (68% + 38% + 61% + 47% + 70% + 28% + 42%) / 7 = 354 / 7 = **51%**

検出結果の深刻度

異なる色とアイコンを使用して、リソースとアイデンティティが組織にもたらすさまざまなリスクの深刻度レベルを示します。次の表は、各アイコンとそれに対応する深刻度レベル、およびクラウド環境内での意味を示しています。

ステータス	説明	例
Critical	早急なアクションが必要	機密データへのアクセス許可を持っている管理者ユーザーがいるが、そのアクセス許可が使用されていない。

ステータス	説明	例
High	できるだけ早く処理	機密データへのアクセス許可を持っている非管理者ユーザーがいるが、そのアクセス許可が使用されていない。
Medium	潜在的なリスク	バケットリストなど、機密性の高いリソースへのアクセス許可を持っているユーザーがいるが、バケットの内容を読み取るアクセス許可は持っていない。
Low	昇格のモニタリング	割り当てられたアクセス許可の使用が制限されているユーザーがいる。
Informational	役立つ情報	新しいGCPプロジェクトが組織に追加された。

注意: 検出結果の深刻度が想定レベルと異なる場合は、除外使用して上書きできます。

動的な深刻度と静的な重大度

各ポリシーには、関連付けられている深刻度レベルがあります。この深刻度レベルによって、ポリシーによってトリガーされる検出結果の深刻度レベルが決まります。

一部のポリシーには *静的な* 重大度レベル ([重大]、[高]、[中]、[低]、[情報] のいずれか) がありますが、ほとんどのポリシーには *動的な* 重大度レベルあります。つまり、ポリシーによってトリガーされる検出結果の深刻度レベルは、検出結果の特定の状況と文脈に応じて動的に決まります。たとえば、使用されていない認証情報を持つIAMユーザーを検出するポリシーでは、ユーザーが管理者のアクセス許可を持っている場合は深刻度 [重大]/[高] の検出結果がトリガーされ、ユーザーがセンシティブでないアクセス許可をいくつか持っている場合は深刻度 [低] の検出結果がトリガーされる可能性があります。

IAM検出結果の深刻度

Tenable One Cloud Exposure は、過剰な権限を持つアイデンティに関連する検出結果のリスクの深刻度を計算して表示します。このセクションでは、異なるクラウドプロバイダー (AWS、Azure、GCP) 間での計算方法について説明します。このような検出結果の深刻度は、次の場所のクラウドサイバーエクスポージャーコンソールに表示されます。

- **[検出結果]** ページの **[深刻度]** 列の下で、それぞれの検出結果内にある。
- **[IAM] > [過剰なアクセス許可]** ページの **[IAM 検出結果の深刻度]** 列詳細は、過剰なアクセス許可 を参照してください。
- 選択したリソースのそれぞれの検出結果内の、**[インベントリ]** ページ。

アクティビティカテゴリやカテゴリリスクレベルを含む、特権を持たないアイデンティのアクセス許可分析の詳細については、アクセス許可の分析とリスクレベル参照してください。

AWS

このセクションでは、権限の昇格された AWS Identity に関連する検出結果のリスクの深刻度の計算方法について説明します。各テーブルは異なるアイデンティティタイプに関連しています。

アクセス許可の深刻度

次の表は、AWS アクセス許可の深刻度レベルがアクション基準から派生し、このセクションのすべてのアイデンティティタイプに関連していることを示しています。

基準	アクセス許可の深刻度
なりすましアクション	重大
重大なアクション	高
機密性の高いリソースと機密性の高いアクション	高
アイデンティティは別のアイデンティティを偽装することができます	Dynamic[2]
広範なリソースと機密性の高いアクション	中/高[3]

基準	アクセス許可の深刻度
広範なリソースとアクションは危険なカテゴリ[1]です	中
その他すべて	低

[1] アクセス管理またはインフラストラクチャ書き込み
[2] その他のアイデンティの深刻度に応じて
[3] アクションの深刻度に基づく

検出結果タイプごとの AWS の深刻度

ユーザーとグループ

この表は、権限のない AWS ユーザーおよびグループに関連付けられている検出結果のリスクの深刻度の計算方法を示しています。計算は、ユーザーのアクセス許可のリスクの深刻度 (詳細については アクセス許可の深刻度 を参照) と認証情報に関連する要素に基づいて行われます。たとえば、あるユーザーのアクセス許可の深刻度が [高] で、ユーザーが MFA が設定されたパスワードを持っている場合、検出結果の深刻度は [中] となります。

アクセス許可の深刻度	パスワード/キーなし	MFA のあるパスワード	アクセスキー	MFA とアクセスキーでパスワード	MFA[1]のないパスワード
低	低	低	低	低	中
中	低	低	中	中	中
高	低	中	高	高	高
重大	低	中	高	高	重大

[1] アクセスキーの有無

ロール

この表は、権限の昇格されたAWSロールに関連付けられている検出結果についてリスクの深刻度がどのように計算されるかを示しています。計算は、ロールのアクセス許可のリスクの深刻度 (詳細については アクセス許可の深刻度 を参照) に基づいて、他の要素と組み合わせて行われます。たとえば、特定のロールについて、アクセス許可の深刻度が[高] であるのに、そのロールが公開されている場合、検出結果の深刻度は[重大] になります。

> **注意:** ロールに複数の関連する要因がある場合、最も深刻度が高いファクターが適用されます。

アクセス許可の深刻度	なしまたは信頼できる外部	Tenable/Customer によって定義されたサードパーティロール	不明なアカウント	パブリックコンピューティング	パブリックロール	脆弱性のあるコンピューティング
低	低	中	中	中	中	中
中	低	中	高	高	高	高
高	中	高	高	高	重大	重大
重大	中	重大	重大	重大	重大	重大

SSO アクセス許可セット

この表は、特権 AWS SSO アクセス許可セットに関連付けられている検出結果についてリスクの深刻度を計算する方法を示しています。計算は、アクセス許可セットのリスクの深刻度 (詳細については アクセス許可の深刻度 参照) に基づいて、リスクの深刻度 (非過剰) と割り当て/アカウントの数を組み合わせて行われます。たとえば、特定のアクセス許可セットでは、アクセス許可の深刻度が[高] であるものの、アクセス許可セットにある割り当ての数が 10 未満、アカウントの数が 10 未満で、そのすべての深刻度が「中」のアクセス許可を持つ場合、検出結果の深刻度は「中」になります。

割り当てられていないアクセス許可セットに関連付けられている検出結果には、深刻度「低」が割り当てられます。

最大 10 個の割り当ておよび最大 10 個のアカウント

割り当て/アカウントの深刻度 → (残りのアクセス許可)	低	中	高	重大
アクセス許可の深刻度 ↓ (アクセス許可を削除)				
低	低	低	低	低
中	低	低	低	低
高	中	中	中	低
重大	高	高	高	中

10 個以上の割り当てまたは 10 つ以上のアカウント

割り当て/アカウントの深刻度 → (残りのアクセス許可)	低	中	高	重大
アクセス許可の深刻度 ↓ (アクセス許可を削除)				
低	低	低	低	低
中	中	中	低	低
高	高	高	高	低
重大	重大	重大	重大	中

未使用のアクセス許可セットが割り当てられた SSO ユーザーおよびグループ

この表は、未使用のアクセス許可セットが割り当てられている AWS SSO **グループおよびユーザー**に関連する検出結果のリスクの深刻度の計算方法を示しています。計算は、使用済みおよび未使用の AWS SSO アクセス許可セットの割り当てを通じてユーザーが引き受けることができるロールのアクセス許可の深

刻度 (詳細については アクセス許可の深刻度 を参照) と、割り当ての数に基づいて行われます。たとえば、グループまたはユーザーに、未使用の深刻度高のアクセス許可セットの割り当てがあり、これは **削除できる**が、使用済みの割り当てが **残りのアクセス許可** である場合、ユーザーは深刻度中権限のあるロールを引き受け、グループまたはユーザーのアクセス許可がより少ない場合、割り当て数 10、検出結果の深刻度は [中]

削除されたアクセス許可セットの割り当て (未使用のアクセス許可セット) が、グループまたはユーザーに対して有効なアクセス許可を付与しない場合、検出結果の深刻度は [情報] になります。

最大 10 件の割り当て

残りのアクセス許可 →	低	中	高	重大
アクセス許可を削除した↓				
低	低	低	低	低
中	低	低	低	低
高	中	中	中	低
重大	高	高	高	中

10 件以上の割り当て

残りのアクセス許可 →	低	中	高	重大
アクセス許可を削除した↓				
低	低	低	低	低
中	中	中	低	低
高	高	高	高	低
重大	重大	重大	重大	中

Azure

このセクションでは、権限の過剰な Azure ID に関連する検出結果に対してリスクの深刻度を計算する方法について説明します。

アクセス許可の深刻度

Azure では、アクセス許可の深刻度レベルはアクションベースの基準の組み合わせに基づいて決定されます。これらの基準には、アクションまたはリソースの機密性が高いかどうか、アクセス許可の範囲が広いかどうか、サービスが一般的に使用されているかどうかなどの要素があります。さらに、MFA が有効でない Entra ID ユーザーが見つかった場合、アクセス許可の深刻度レベルは上がります。以下の表は、アクセス許可の[重大]と[高]の深刻度レベルにこうした基準がどのように影響するか、例を示しています。

影響を受けるアクションは[1]	リソースは重要度高[2]	ワイドスコープ[3]に付与されたアクセス許可	サービスはインベントリ[4]でサポートされています	権限昇格アクション[5]	深刻度
✓	-	✓	-	✓	重大
✓	-	✓	-	✗	高
✓	✓	-	✓	-	高

[1] データの読み取り、データの書き込み、インフラストラクチャの書き込み、アクセス管理、またはなりすましに関連するアクション (約 4,300 件のアクション)
[2] ユーザーが 機密度の高いリソースをマークする、または クラウド サイバーエクスポージャー がリソース内の機密データを識別したかどうかに基づいて、
[3] 広範な範囲: root 管理グループ、管理グループ、サブスクリプション
[4] クラウド サイバーエクスポージャー インベントリ
のサービスによると、一般的に使用される Azure サービス[5]
`Microsoft.Authorization/classicAdministrators/write` または
`Microsoft.Authorization/roleAssignments/write`

Azure 検出結果の深刻度

このセクションでは、権限の過剰な Azure ID に関連する検出結果に対してリスクの深刻度を計算する方法について説明します。Azure では、検出結果の深刻度は、削除できるアクセス許可の深刻度 と削除後に残るアクセス許可の深刻度 **とともに** 計算されます。たとえば、ユーザーに削除可能な「低」の深刻度のアクセス許可があり、削除された後でもそのユーザーには「高」の深刻度のアクセス許可があり、変更の影響は低いため、検出結果の深刻度は「低」になります。

この表は、その論理の仕組みを示しています。

残りのアクセス許可 →	なし (非アクティブ)	低	中	高	重大
アクセス許可を削除した↓					
低	低	低	低	低	低
中	低	低	低	低	低
高	高	高	中	低	低
重大	高	高	高	中	低

> **注意:** 以下の条件により、ベースラインの深刻度が 1 レベルだけ上昇します。
>
> - アプリケーションはサードパーティです
> - パブリックコンピューティングインスタンスに関連付けられた ID
> - 悪用可能な脆弱性のあるコンピューティングインスタンスに関連付けられた ID
> - MFA が有効になっていない内部メンバーまたはゲスト
>
> たとえば、本来であれば深刻度が「低」である検出結果が、サードパーティのアプリケーションに関連する場合には「中」として深刻度が割り当てられます。

上記のロジックに関係なく、以下のすべてのシナリオで、検出結果の深刻度は [低] です。

- アプリケーションは無効です
- Microsoft アプリケーション
- 有効なシークレットまたは証明書がないファーストパーティアプリケーション

GCP

このセクションでは、権限のない GCP Identity に関連する検出結果のリスクの深刻度計算方法について説明します。

アクセス許可の深刻度

GCP では、アクセス許可の深刻度レベルはさまざまなアクション基準の組み合わせから派生します。これらの基準には、アクセス許可の範囲が広いかどうかなどがあります。この表は、アクセス許可の深刻度レベルにアクション基準がどのように影響するかを示す例です。

	機密性の高いリソース/サービスアカウント[1]	機密でないリソース/サービスアカウント[1]	機密性の高いプロジェクトのフォルダーと企業[2]	機密性の高いフォルダーと企業[2]
ワイドスコープの権限管理のアクセス許可[3]	-	-	重大	重大
特別に機密性の高いアクセス許可[4]	高	高	高	高
機密性の高いアクセス許可[5]	高	中	高	中

[1] サービスアカウントがリソースとして扱われ、別のプリンシパルがそれを操作するアクセス許可を持っている場合、サービスアカウントのアクセス許可の中で最大の深刻度レベルが適用されます。
[2] サービスアカウント、プロジェクトフォルダー、または組織に `GcpActions.GcpIam.ServiceAccounts.ImplicitDelegation` アクセス許可がある場合、このアカウントは、なりすましが可能なすべてのプリンシパルから間接的なアクセス許可の最も高い深刻度を継承します。
[3] `SetIamPolicy` プロジェクトフォルダーおよび組織のアクセス許可を付与します。
[4] `GcpContainer.Clusters.GetCredentials`など、機密として定義されているデータ漏洩、インフラ書き込み、アクセス管理、なりすましに関連する 20 個未満のアクセス許可のリスト。

[5]データ漏洩、インフラに対する書き込み、アクセス管理、またはなりすましに関連するアクション (約 1,800 件のアクション) です。

GCPの所見の重大度

このセクションでは、GCP で権限のないアイデンティの検出結果の深刻度を決定する方法について説明します。深刻度は、次の表に示す **アクセス許可の深刻度** に基づいて計算されます。アカウントが外部のものかパブリックアクセスを持っているかなどの追加の要因によって、ベースラインの深刻度が上がる可能性があります。

過剰なアクセス許可の深刻度	検出結果の深刻度
重大	高
高	中
中	低
低	低

> **注意:** 次の条件により、ベースラインの深刻度が 1 レベルだけ増加します。
>
> - **外部エンティティ**: ユーザー、サービスアカウント、またはグループは外部です。
> - **パブリックアクセス**: サービスアカウントが有効化され、内部化されていますが、パブリックアクセス権を持つオリジンがあります。

上記のロジックに関係なく、以下のすべてのシナリオで、検出結果の深刻度は [Low] です。

- ユーザーが無効です
- サービスアカウントが無効になっている

IAM

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

Tenable One Cloud Exposure このセクションでは、の IAM 機能の概念概要を説明します。

- 環境内のアイデンティティリスクの調査に関する方法ガイドについては、アイデンティティインテリジェンス参照してください。
- 環境内の特権を持たないアイデンティの処理に関する方法ガイドについては、過剰なアクセス許可参照してください。
- クラウドサイバーエクスポージャーのIAM設定の構成に関するハウツーガイドについては、IAMを参照してください。

クラウドサイバーエクスポージャーを使用して特権アイデンティティを管理すると、使用されていないアイデンティティや過剰な権限またはリスクのある権限を持つアイデンティティを明らかにし、組織に及ぼすリスクを効果的に最小限に抑えることができます。Tenableは、アクセスキーの使用、多要素認証の欠如、インターネットへの露出など、アイデンティティに関連するリスク要因に関する詳細を提供します。この情報は、ID盗取などのアイデンティティ関連のリスクや、その潜在的な侵害の影響範囲を検出するのに役立ちます。

詳細

- 過剰なアクセス許可と非アクティブなアイデンティティ
- アクセス許可の分析とリスクレベル
- よくある質問: IAMガバナンス

アクセスレベル

誰がどこからクラウドリソースにアクセスできるかを理解することは、セキュリティポスチャーを評価する上で基本的な部分になります。アクセスレベルを使用すると、関連するクラウドプロバイダーやアイデンティティのタイプに関係なく、リソースに付与されるアクセスの範囲を統一して分類できます。リソースが公開されているか、外部からアクセス可能であるか、アカウント間で共有されているか、内部IDに限定されているかを迅速に判断できます。これらのアクセス範囲を標準化することで、アクセスレベルは一貫した分析、より明確な可視性、そして環境全体の潜在的にリスクの高いアクセスパスの特定を容易にします。

アクセスレベルは、リソースに到達できるアイデンティティの範囲を定義します。パブリックエクスポージャーから、外部アクセス、クロスアカウントアクセス、信頼できるアクセス、内部アクセスまであります。以下のリストは、各値の一般的な定義を示しています。各値の正確な定義はクラウドプロバイダーによって異なりま

す。AWS アクセスレベル、Azure アクセスレベル、GCP アクセスレベル のアクセスレベルの定義については、関連セクションを参照してください。

- **パブリック。** アクセスは、認証済みか未認証かに関係なく、あらゆるアイデンティティに制限なく開放されています。
- **外部**。パートナーアカウント、サードパーティベンダー、同期されていないアカウント、外部アイデンティティプロバイダー (IDP) など、組織外のアイデンティティにアクセスが付与されます。
- **クロスアカウント**。同じ組織内の他のアカウントまたはサブスクリプション (Tenable One Cloud Exposure アカウントに接続されている) のアイデンティティにアクセスが付与されます。
- **信頼できる外部。** 信頼できるものとして明示的にマークされた外部ベンダーにアクセス権が付与され、既知の外部アクセスと未知の外部アクセスを区別するのに役立ちます。
- **Internal (内部)。** アクセスは、同じアカウントまたはサブスクリプション内のアイデンティティに制限されます。

AWS アクセスレベル

以下に、アクセスレベルフィルターで可能な値のリストと、各値の AWS 固有の定義を示します。

アクセスレベル	定義
パブリック	ワイルドカードプリンシパル * へのアクセスを条件なしで付与するリソースベースのポリシーを持つリソース。
外部	クラウドサイバーエクスポージャーに接続されていないアカウントからプリンシパルへのアクセスを付与するリソースベースのポリシーを持つリソース。すべてのサードパーティベンダー (AWS を除く) がこのカテゴリに該当します。
クロスアカウント	両方のアカウントがクラウドサイバーエクスポージャーに接続されている場合、アカウント B のユーザー、ロール、グループがアカウント A のリソースにアクセスできます。

アクセスレベル	定義
信頼できる外部	信頼できるものとして明示的にマークされた、サードパーティベンダーのプリンシパルへのアクセスを許可するリソースベースのポリシーを持つリソース。
内部	リソースには、同じ AWS アカウント内のユーザー、ロール、グループがアクセスできます。

Azure アクセスレベル

以下に、アクセスレベルフィルターで可能な値のリストと、各値の Azure 固有の定義を示します。

アクセスレベル	定義
パブリック	Blob ストレージにのみ適用されます。
外部	エンタープライズアプリケーション (Microsoft を除く)、同期されていないプリンシパル、または Microsoft Entra ID ゲストユーザーがリソースにアクセスできます。
クロスアカウント	両方のサブスクリプションが クラウド サイバーエクスポージャー に接続されている場合 、サブスクリプション B のマネージド ID (MI) がサブスクリプション A のリソースにアクセスできます。さらに、Azure サブスクリプションと Microsoft Entra ID テナントがリンクされていない場合でも、Microsoft Entra ID プリンシパルはリソースにアクセスできます。
信頼できる外部	エンタープライズアプリケーション (Microsoft を除く) からアクセスでき、信頼されているものとして明示的にマークされているリソース。

アクセスレベル	定義
内部	Azure サブスクリプションと Microsoft Entra ID テナントがリンクされている場合、Microsoft Entra ID プリンシパル (ユーザー、アプリケーションなど) がリソースにアクセスできます。これには、同じサブスクリプションまたは Microsoft マネージドアプリケーション内のマネージド ID がアクセスできるリソースも含まれます。

GCP アクセスレベル

以下に、[Access level] (アクセスレベル) フィルターで可能な値のリストと、各値の GCP 固有の定義を示します。

アクセスレベル	定義
パブリック	リソースには、`AllUsers` または `AllAuthenticatedUsers`でアクセスできます。
外部	リソースには、外部サービスアカウント、ユーザー、またはグループ (Google プリンシパルを除く) がアクセスできます。
クロスアカウント	両方のプロジェクトが クラウドサイバーエクスポージャー に接続されている場合、プロジェクト B のサービスアカウントアイデンティティ、ワークプールアイデンティティ、またはGoogleワークスペースプリンシパルが、プロジェクト A のリソースにアクセスできます。さらに、GCP プロジェクトと Google Workspace テナントがリンクされていない場合でも、Google Workspace プリンシパルは GCP リソースにアクセスできます。
内部	GCP プロジェクトと Google Workspace がリンクされている場合、Google Workspace プリンシパル (ユーザー、グループなど) がリソースにアクセスできます。これには、同じプロジェクト

アクセスレベル	定義
	内でサービスアカウントアイデンティティまたはワークプールアイデンティティがアクセスできるリソースも含まれます。

アクセスレベル機能

Tenable は、クラウド環境全体のアクセス範囲を理解して分析するのに役立つ、3 つの補完的なアクセスレベル機能を提供しています。

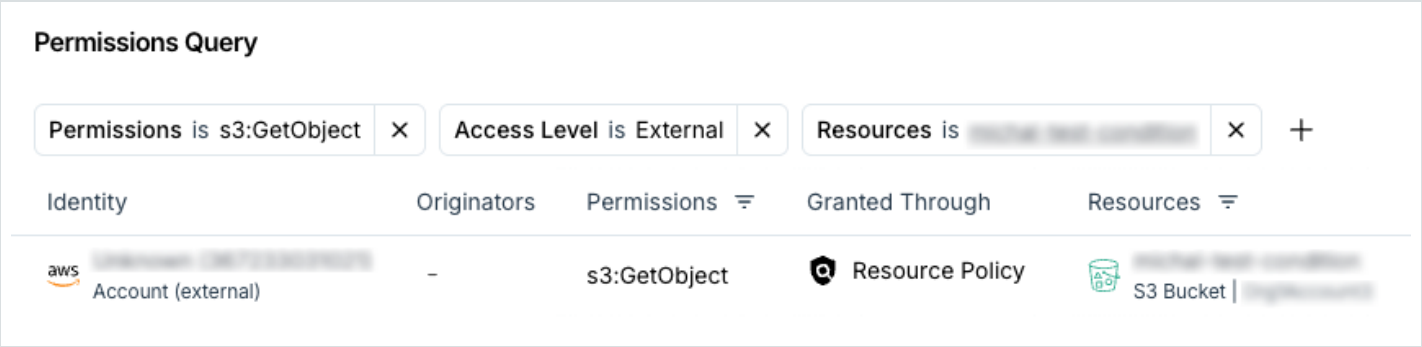
機能	目的	コンソール内の場所
アクセスレベルフィルター	プリンシパルとリソースの関係を個別にマッピング	• **アクセス許可クエリ**。詳細については、「アクセスレベル」を参照してください。 • **アクセス許可マッピング** (アクセスグラフ)。詳細については、「アクセス許可マッピングの視覚化」を参照してください。 • **Explorer**。詳細は、Explorer を参照してください。
アクセス許可カテゴリ別のアクセスレベル	各アクセス許可カテゴリのすべてのプリンシパルの最高アクセスレベルを特定のリソースにマッピングする	• **Explorer**。詳細は、Explorer を参照してください。 • **データリソース**。詳細については、「データリソースを参照してください。
[アクセスレベル] 列	すべてのアクセス許可カテゴリのすべてのプリンシパルの最高アクセスレベルを特定のリソースにマッピングする	• **インベントリ** • **Explorer**。詳細は、Explorer を参照してください。

アクセスレベルフィルター

[インベントリ] ビューと [アクセス許可マッピング] ビューの [アクセスレベル] フィルターはプリンシパルとリソースの関係に焦点を当て、特定のアクセス許可について視覚化します。フィルターを使用してグラフの表示を絞り込んだり、特定の監視対象リソースへの外部アクセスなど、関心のある特定のユースケースを調べたりすることができます。

以下に例を示します。

- **権限**:`S3:GetObject`;**アクセスレベル**:`External`;**リソース**: [監視対象リソース]

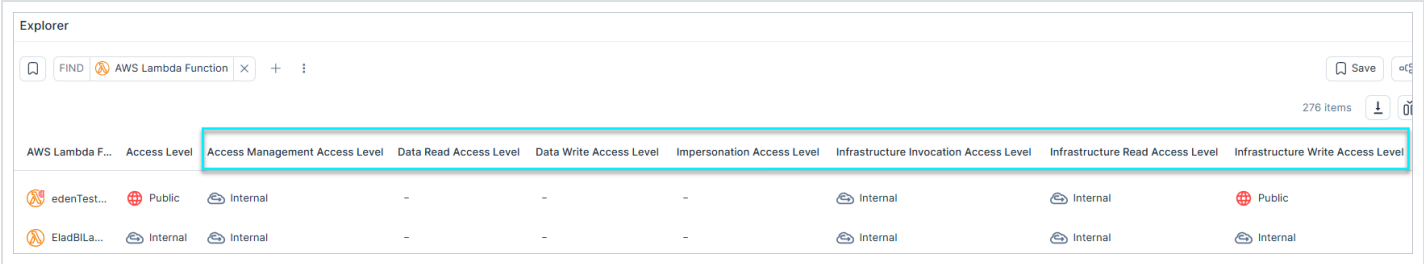


アクセス許可カテゴリ別のアクセスレベル

アクセス許可カテゴリごとのアクセスレベルは、特定のアクセス許可カテゴリ内でリソースに付与される最高レベルのアクセスを表します。アクセスレベルは、プリンシパルがリソースに持つアクセスの範囲を示し、アクセス許可カテゴリは、リソースにどれだけ広範囲にアクセスできるかだけでなく、どのタイプのアクセスが可能か (データの読み取り、データの書き込みなど) も示すことで、このインサイトを強化します。

Tenable は、監視対象の各リソースについて、カテゴリごとのプリンシパル全体の**最高**アクセスレベルを評価します。これにより、アクセスの範囲とタイプの両方が明確に可視化され、潜在的なリスクの特定に役立ちます。また、特にクラウドポリシー: カスタムと組み合わせると、アクセス許可クエリ、アクセス許可マッピングの視覚化グラフ)、アイデンティティインテリジェンス、過剰なアクセス許可などの機能を使用する場合、調査プロセスがより効率的になります。

たとえば、[探索] ビューから各カテゴリごとの Lambda 関数のアクセスレベルを評価できます。

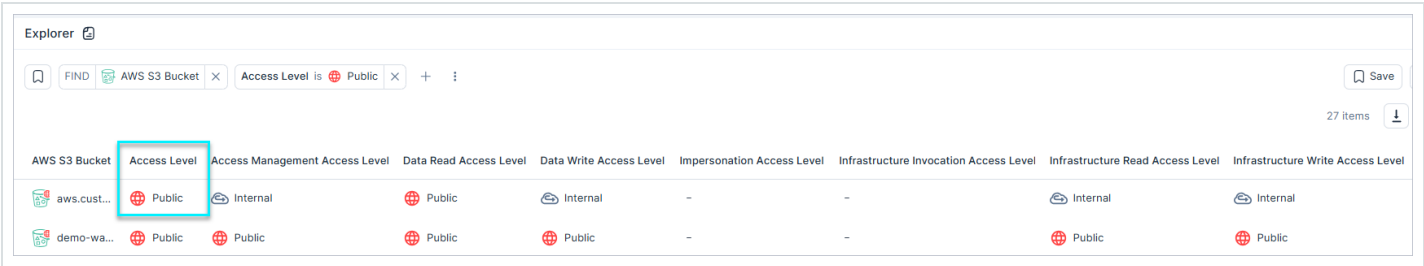


[アクセスレベル] 列

[アクセスレベル] 列は、付与された最高レベルのアクセスを評価することにより、**すべての**アクセス許可カテゴリにおいて、すべてのプリンシパルと特定のリソースの間の最高アクセス関係を表示します。

この機能を使用すると、特定のプリンシパルとリソースの関係 (内部、信頼できる外部、クロスアカウント、外部、パブリック) で付与されるアクセスレベルを判断し、そのリソースに付与されている最も広範なアクセス範囲を調査できます。リソースに複数のアクセスパスがある場合、[アクセスレベル] 列にはそれらの中で最も高いアクセスレベルが反映されます。

たとえば、S3 バケットにはさまざまなカテゴリのアクセスレベルが異なる場合がありますが、[Access Level] (アクセスレベル) 列には最も高いアクセスレベルのみが表示されます。



過剰なアクセス許可と非アクティブな ID

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

クラウド環境で最小権限を適用します。Tenable One Cloud Exposure **[過剰なアクセス許可]** ページでは、必要以上のアクセス許可を割り当てられているアイデンティティの内訳を表示し、それらのアイデンティティが組織にもたらすリスクを最小限に抑えることができます。このページには、そのようなアイデンティティの

アクティビティステータスに関するインサイトも表示され、非アクティブなアイデンティティの定義を表示することができます。

過剰なアクセス許可の定義

クラウドサイバーエクスポージャーでは、デフォルトで、サービスIDとユーザーの両方に対する過剰なパーミッションは、過去 90 日間に**使用されなかったパーミッション**として定義されます。アクセス許可使用のラーニング期間を変更して、この期間を調整できます。

注意: 2025 年 2 月 2 日より前にクラウドサイバーエクスポージャーの作業を開始したお客様については、デフォルト値が異なる場合があります。たとえば、AWS の人のアイデンティティの場合、デフォルトの定義は 180 日間でした。

重要: 権限は、関連する CSP からの**明示的なクラウドログ証拠**に基づくか、**暗黙的な証拠** (つまり、**クラウドサイバーエクスポージャー権限が過剰である証拠を持たない**) のいずれかに基づいて、「使用済み」として決定されます。ログされアクセス許可マッピングの視覚化どのようにTenableが過剰な権限と使用を決定する方法に影響を与えるかについての詳細は、ログされない権限を参照してください。

過剰なアクセス許可を持つすべてのアイデンティティには、少なくとも 1 つの検出結果が関連付けられています。これらの検出結果は、多くの場合、「過剰な権限を持つ」ポリシー (過剰な権限を持つ IAM ロールなど) によってトリガーされます。これらの検出結果は、[調査結果] (検出結果) ページで処理できるほか、[権限の過剰付与] (過剰なアクセス許可) ページから表示して、自動的に修正することもできます。

Azure と GCP のアカウントの場合、検出結果はサブスクリプションまたはプロジェクトごとにオープンになります。同じアイデンティティが複数のサブスクリプションまたはプロジェクトに存在する場合、Tenable はサブスクリプションまたはプロジェクトごとに、そのアイデンティティに対する個別の検出結果をオープンします。これらは、[調査結果] (検出結果) ページに個別の項目として表示されます。ただし、[権限の過剰付与] (過剰なアクセス許可) ページでは、そのような複数の検出結果は 1 つのテーブルエントリに統合されます。これに伴い、次の点が変更になります。

- このページから ID を自動的に修正すると、すべての検出結果が解決されます。
- そのアイデンティティのアクションを手動でトリガーすると、検出結果ごとに複数のチケットが作成されます。

非アクティブなアイデンティティの定義

クラウド サイバーエクスポージャーでは、デフォルト で、サービス ID とユーザーの両 方 の非 アクティブな ID は、過 去 90 日 間 に**アクティビティがなかった ID** として定 義 されます。アクセス許 可 使 用 のラーニング期 間 を変 更 して、この期 間 を調 整 できます。

- 2025 年 2 月 2 日 より前 に クラウド サイバーエクスポージャー の使 用 を開 始 した場 合 は、デフォルト 値 が異 なる場 合 があります。たとえば、AWS の人 のアイデンティティの場 合 、デフォルト の定 義 は 180 日 間 でした。
- **AWS**: クラウド サイバーエクスポージャー は、認 証 情 報 の使 用 やロールを引 き受 けようとする試 みを含 む、あらゆるアクティビティを監 視 します。
- **Azure/Microsoft Entra ID**
  - 非 アクティブなアプリケーションは、ユーザーまたはサービスプリンシパルのサインインログがない ことで識 別 されますが、非 アクティブな管 理 されたアイデンティティは、サービスプリンシパルのみ のサインインログがないことで識 別 されます。
  - プロビジョニングを実 行 している非 アクティブなアプリケーションは、ポリシーの検 出 から除 外 され ます。
  - Tenable エンタープライズアプリケーションのアクティビティを監 視 することはできません。これは、 アプリケーションにサインオンイベント がないためです。
- **GCP/Google Workspace**: クラウド サイバーエクスポージャー は成 功 したサインインログとアクティビ ティの時 間 をチェックし、使 用 率 を検 証 します。

未 使 用 ロールの定 義

クラウド サイバーエクスポージャーでは、GCP と Azure の未 使 用 のロールが識 別 され、不 要 なロールを減 らし、クラウド 環 境 のセキュリティと管 理 性 を向 上 させるのに役 立 ちます。

ロールにアクティブなバインド や割 り当 てがない場 合 、**未 使 用** としてマークされます。GCP のみ、ロールの バインド すべてに 30 日 以 上 「未 使 用 」としてフラグが立 てられている場 合 、「未 使 用 」としてマークされま す。

これにより、使 用 されなくなったロールを素 早 く特 定 して削 除 できるようになります。非 アクティブなアイデン ティティや過 剰 なアクセス許 可 を把 握 し、最 小 権 限 の適 用 が可 能 になります。

権限が過剰なアイデンティおよび非アクティブなアイデンティティの作成を検出する

次の表は、権限のないアイデンティや非アクティブなアイデンティティの検出結果が作成される方法を示しています。

シナリオ	結果
ID が **アクティブで** あり、**権限があります**	権限昇格の結果のみが作成される
アイデンティティは **非アクティブで**あるが、**権限を昇格されていない**	非アクティブな検出結果のみが作成されます。非アクティブなラベルがアイデンティティと関連する検出結果に適用されます。
ID が **非アクティブで** あり、**権限が過剰です**	[過剰な権限] と [非アクティブ] の両方の検出結果が作成されます。非アクティブなラベルがアイデンティティと関連する、過剰な権限を持つ非アクティブな検出結果に適用されます。

アクセス許可の分析とリスクレベル

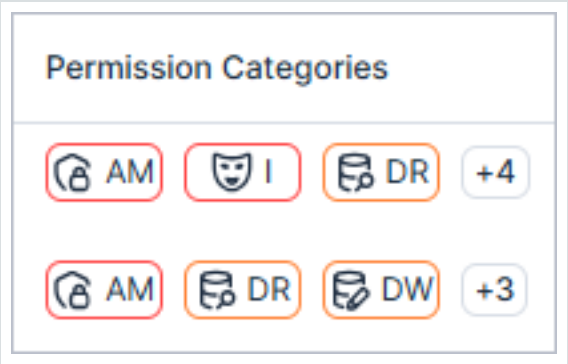
> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

クラウド ID には、特定のリソースにアクセスすることを許可するさまざまなレベルの権限が付与されます。Tenable One Cloud Exposure は環境内のすべてのアイデンティティを分析し、特定のリソースに対してどのアクセス許可を持っているかを判断します。この権限評価プロセスの一部として、Tenable

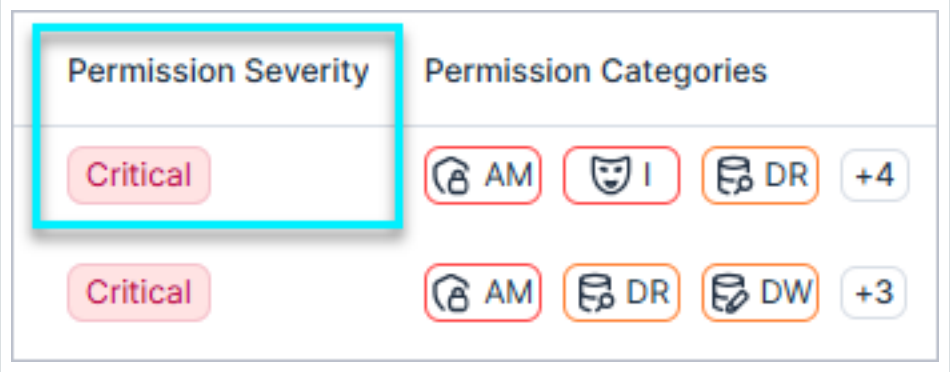
1. 各アクセス許可をアクティビティタイプ (アクセス許可カテゴリ) にマッピングします。これらの アクセス許可カテゴリ クラウドアイデンティティに一般的な広範囲の動作パターンを反映しています。各カテゴリアイコンは、深刻度レベルに応じて色付きで表示されます。

   > **注意:** 権限カテゴリアイコンをクリックすると、カテゴリと深刻度でフィルタリングされたアクセスグラフが表示されるサイドパネルが開きます。

2. 各アクセス許可カテゴリに色分けされた深刻度レベル(アクセス許可カテゴリ)を割り当てます。詳細については、アクセス許可カテゴリリスクレベル参照してください。



3. 特定のアクセス許可カテゴリのリスクレベルと環境内のアイデンティティの全体的な文脈の両方を考慮して、全体的なリスクレベルをアイデンティティに割り当てます。



詳細については、アイデンティティインテリジェンスを参照してください。過剰なアクセス許可のコンテキスト内でのこの計算方法については過剰なアクセス許可参照してください。

> **注意:** カテゴリのアイコンは、アイデンティティにそのカテゴリに関連付けられたアクセス許可がある場合にのみ表示されます。

アクセス許可カテゴリ

カテゴリ	説明
データ読み取り(DR)	データベース、バケット、シークレット、暗号化などに保存されているデータを表示できます。

カテゴリ	説明
データ書き込み (DW)	クラウドサービスまたはアプリケーションのデータを追加または変更する権限を付与します。
インフラストラクチャ書き込み (IW)	インフラリソースを作成、変更、削除できます。
アクセス管理 (AM)	ユーザー、ロール、リソースのアクセス許可やポリシー (IAM など) を変更できます。
なりすまし	他のロールまたはアイデンティティを引き受けることができます。
インフラに関する記事 (IR)	インフラリソース (VM、ネットワーク、サービスなど) の設定およびメタデータを表示できます。
インフラストラクチャの起動 (II)	関数の呼び出し、コンテナの実行、ジョブ/ワークフローのトリガーを含みます。

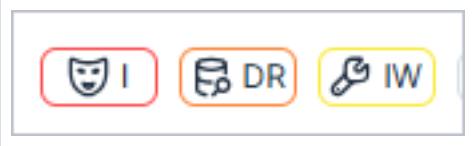
アクセス許可カテゴリリスクレベル

[アイデンティティインテリジェンス] ページと [過剰なアクセス許可] ページの両方の表で、これらのカテゴリには色分けされた深刻度レベルが割り当てられ、特定のアイデンティティに割り当てられたアクセス許可から検出された潜在的なリスクを反映します。

- **重要度最高**。管理者権限を持った、または管理者に権限を昇格できるアイデンティです。
- **重要度高**。機密性の高いリソースまたは広範なリソースに対する次のアクションを実行するアクセス許可を持つ ID です。1) データの読み取り、2) リソースの破壊、3) アクセス許可の付与。
- **重要度中** 広範囲のリソースに限定的な影響を与えるアクセス許可を持つアイデンティ
- **重要度低**。限られた数の機密でないリソースに対して限定的な影響を及ぼすアクセス許可を持つアイデンティティ。

以下のスクリーンショットの例では、次のカテゴリごとにさまざまなリスクレベルが割り当てられたアイデンティティを確認できます。

- **なりすましI**重要度最高
- **データの読み取り(DR)**: 重要度高
- **インフラストラクチャ書き込みIW**重要度中



FAQ - IAM ガバナンス

> [最終アクティビティ] フィールドに、Azure ID は通常、「5 か月以上前」などの具体的な情報を表示せず、まったく表示しない (「不明」) 場合があるのはなぜですか?

Azure では読み取りアクセス許可が記録されないためです。結果として、前回のアクティビティとは、前回実行された管理書き込みアクティビティを指します。

> アイデンティティ関連のアクティビティに学習期間はありますか?

過剰なアクセス許可のコンテキスト内で、Tenable One Cloud Exposure は以下のアクティビティについての学習期間を強制します。この期間に過剰なアクセス許可に関連する新しい発見は作成されません

- 新しい人間のアイデンティティが作成される場合 - デフォルトは 90 日です (IAMで構成可能)。
- 新しいサービス/マシン ID の作成時 - デフォルトは 90 日です IAMで構成可能です。
- アイデンティティまたはリソースのアクセス許可が変更された場合 - 30 日間

> クラウドサービスプロバイダーが新しいサービスやアクセス許可を追加した後、いつアクセス許可の分析とリスクレベルのいずれかにマッピングされますか?

継続的に新しいサービスとアクセス許可をフィルタリングして分類する自動メカニズムがあります。さらに、クラウドサイバーエクスポージャー は新しいサービスの定期的な手動レビューを実行し、自動分類が可能

な限り正確であることを確認します。

Tenable での権限のない Microsoft Entra ID グループの検出方法

> Tenable は Microsoft Entra ID グループが権限を昇格しているかどうかをどのように判断していますか?

は Tenable 、Microsoft Entra ID グループがそのメンバーによってアクティブに使用されていないアクセス許可を持っているかどうかを評価します。グループ自体はアクションを直接実行しないため、グループのメンバーが使用するアクセス許可に基づいて分析されます。

> グループに独自のアクセス許可がありますか?

技術的にはアクセス許可はグループに割り当てられていますが、それを使用できるのはメンバーのみです。クラウドサイバーエクスポージャー は、メンバーが実際に使用している権限を分析し、グループに割り当てられた権限のいずれかが不要かどうかを判断します。

> 分析は個別のメンバーまたはグループ全体に基づいていますか?

個々のメンバーを基にしています。1 人のメンバーがグループに割り当てられた特定のアクセス許可を使用している場合、そのアクセス許可は使用中と見なされ、削除用のフラグが立てられません。

> 異なるメンバーが異なるアクセス許可を使用した場合はどうなりますか?

Tenable はすべてのメンバーが使用するアクセス許可を集約します。メンバー A が権限 X を使用し、メンバー B が権限 Y を使用する場合、X と Y の両方が使用中と見なされ、グループは両方を保持することが推奨されます。

「グラフが大きすぎます」という動作を理解する

> 通常のグラフやテーブルではなく、「グラフが大きすぎます」というメッセージが表示されるのはなぜですか?

特定の場合では、プリンシパル(ユーザーやグループなど)に関連付けられているアクセス許可データが、システムで処理できる安全なしきい値を超えて拡大する可能性があります。この状況が発生すると、ブラウザのパフォーマンスの問題を防ぐために、データのロードまたはレンダリングの試行を回避します。そのため、グラフとテーブルビューの両方が使用できなくなります。

> さまざまなタイプの「グラフが大きすぎる」シナリオがありますか?

はい、2つの異なるシナリオがあります。

- **シナリオ1**: まれに、データは正常に読み込まれたものの、大きすぎてグラフとして表示できない場合があります。引き続き、テーブル(リスト)形式で表示できます。
- **シナリオ2**: データセットサイズがシステム制限を超える例外的なケースでは、パフォーマンスの問題を回避するためにグラフとテーブルの両方が保留されます。代わりにメッセージが表示されます。

> データがすでに存在するシナリオに回避策はありますか?

場合によっては、データが正常にフェッチされた場合、より小さいリソースセットを選択するなどしてクエリの範囲を絞り込むことで、データを表示するのに必要なだけデータサイズを縮小できることがあります。

権限の過剰なアイデンティ検出結果でのアクセス許可の違いを理解する

> 「過剰なサービス」と「合計サービス」のカウントが異なるのはなぜですか?

回答: サマリーは**完全に未使用のサービス**のみをハイライトします。アイデンティティがサービス(S3やEC2など)内で少なくとも1つのアクセス許可を使用している場合、そのサービスは「過剰」カウントから除外されます。たとえ、未使用のアクションが含まれているとしても。

> ポリシーに含まれない一部のサービスがリストされているのはなぜですか?

システムは、**機能的影響**に基づいてアクセス許可をマッピングします。たとえば、特定のEC2アクセス許可は、ACM証明書を管理する機能も付与します。そのため、ポリシーがEC2のみを明示的に記載している場合でも、ACMがグラフに表示されます。

> アクセス許可の数はリスクを表していますか?

不正確です。総数 (例: 1,000 のアクセス許可) は、そのアイデンティティが実行できる**範囲すべて**を表します。これには、すべてのサービスで必要 (使用) と過剰 (未使用) のアクセス許可の両方が含まれます。

ワークロード保護

Tenable One Cloud Exposure このセクションでは、のワークロード保護機能の概念概要を説明します。

- ワークロードの表示と管理に関する方法ガイドについては、VM、VM イメージ、コンテナイメージ、および ソフトウェアを参照してください。
- ワークロード設定を構成するには、ワークロード参照してください。
- よくあるご質問については、「FAQ: Workload Protection 」を参照してください。

クラウド サイバーエクスポージャー Workload Protection を使用して、ワークロードの脆弱性を継続的に特定、評価、処理、報告することができます。これにより、セキュリティのベストプラクティスを実装し、業界標準へのコンプライアンス確保する両方が可能になります。セキュリティの弱点と欠陥を特定して環境内のサーバーワークロードを保護し、センシティブデータの侵害や漏洩から組織を保護します。

クラウド ワークロードとは、クラウド ベースのリソース (コンピューティング能力やメモリ能力など) を消費するアプリケーション、サービス、機能、または指定された量の作業です。クラウド サイバーエクスポージャー では、仮想マシンや Kubernetes クラスタなどのリソースをクラウド ワークロードと見なします。これらの各リソースについて、Tenable は、システム情報、ソフトウェアインベントリ、脆弱なソフトウェア、パッチ未適用または EOL オペレーティングシステム (OS) を検出します。Tenable は、一般に公開されているベンダーアドバイザリから脆弱性データを抽出します。ベンダーアドバイザリからデータを入手することで、Tenable は脆弱性が公開されたらすぐに脆弱性カバレッジを提供できます(NVD でデータが利用できるようになるのを待っていたら、数日または数週間遅れる可能性があります)。

クラウドソフトウェアを実行している組織は、通常、数千のワークロードにまたがって数百のサービスをデプロイします。クラウドソフトウェアは、さまざまなバージョンでリリースされるオープンソースパッケージに大きく依存しています。これらのバージョンには欠陥が含まれていることが多く、ハッカーはそれを悪用してシステ

ムやセンシティブデータへのアクセス権を取得しようとします。セキュリティコミュニティは定期的にこれらの脆弱性を発見して報告し、各ベンダーは通常、修正対応として新しいバージョンをリリースします。

GraphQL API 経由で Workload Protection データにプログラムでアクセスすることもできます。

> **注意:** (ライセンス) この機能は **Standard** および **Enterprise** のライセンスでのみ利用できます。**CIEM** ライセンスでは利用できません。詳細については、ライセンスを参照してください。

詳細

- エージェントレススキャンとエージェントベーススキャンの比較
- エージェントレスワークロードスキャン
- エージェントベースの Kubernetes ワークロードスキャン
- コンテナイメージスキャン
- コンテナイメージレジストリスキャン
- スナップショットスキャン費用計算ツール
- よくある質問: Workload Protection
- Workload Protection のためのアカウントスキャン

エージェントレススキャンとエージェントベーススキャンの比較

> **注意:** エージェントベースのスキャンは、**Cloud Vulnerability Management** ライセンスでは使用できません。

クラウドワークロード保護には、エージェントベースまたはエージェントレスのスキャンを使用できます。それぞれ、セキュリティのニーズ、コンプライアンス要件、運用上の制約に応じて異なる利点があります。

エージェントレススキャン

エージェントレスの保護は、クラウドプロバイダーの API を通じてワークロードをスキャンするため、エージェントを必要とせず、パフォーマンスに影響を与えることなく、セキュリティを迅速に評価することができます。詳細については、エージェントレスワークロードスキャンを参照してください。

仕組み

- をクラウドプロバイダーのAPIと統合することで、ワークロードをスキャンします。インストールは不要です。
- パフォーマンスに影響を与えずに迅速なセキュリティ評価を行います。

エージェントレスを選ぶ理由

- **高速デプロイメント**。エージェントのインストールやメンテナンスが不要
- **操作上のオーバーヘッドを減らします**。管理の複雑さが軽減されます。
- **コンプライアンスチェックに最適です**。迅速なセキュリティ態勢評価を可能にします。

エージェントベースのスキャン

エージェントベースの保護は、各ワークロードに軽いセンサーをデプロイすることで詳細な可視性とリアルタイムのセキュリティを提供します。これは、継続的なモニタリングとアクティブな脅威防御に最適です。詳細については、エージェントベースのKubernetesワークロードスキャン参照してください。

仕組み

- 各ワークロードに軽量センサーをデプロイして、高度な可視性とリアルタイムの監視を実現します。
- KubernetesとRed Hat OpenShiftの両方のコンテナオーケストレーションプラットフォームにデプロイできます。
- クラウド管理対象のクラスター、管理されていないクラスター、オンプレミスのクラスターをサポートしました。

エージェントベースを選ぶ理由

- **ほぼリアルタイムのセキュリティ**。継続的なモニタリング、脅威の検出、アクティブな防御が可能です。ワークロードに対する詳細な可視性を提供します。
- **オンプレミスカバレッジ**。オンプレミスのKubernetesクラスターをスキャンします。特に、エージェントレススキャンがサポートされていないか不適切な環境にあります。
- **コンプライアンス要件**。プライベートデータを環境外に送信できない組織の場合、エージェントレスのアウトポストスキャンよりもエージェントベースのスキャンの方がお勧めです。

注意: オンプレミスの Kubernetes クラスタは、Nessus スキャナーを使用してエージェントレスでスキャンできます。しかし、これは Nessus Agent によるスキャンとは異なります。わかりやすく言うと、これは Nessus Agent を使用した従来のエージェントベースのスキャンではなく、クラウドワークロード保護のことです。

エージェントレスワークロードスキャン

注意: 一部の機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

クラウドワークロード保護には、**エージェントベース** または **エージェントレス** のスキャンを使用できます。それぞれ、セキュリティのニーズ、コンプライアンス要件、運用上の制約に応じて異なる利点があります。この記事では、**エージェントレススキャンについて説明します**。エージェントベースのワークロードスキャンの詳細については、エージェントベースの Kubernetes ワークロードスキャンを参照してください。2 つの手法の比較については、エージェントレススキャンとエージェントベーススキャンの比較を参照してください。

この記事では、Tenable One Cloud Exposure で使用される特定のスキャン方法の詳細について説明します。さまざまなリソースタイプと運用段階で使用されるすべてのスキャンおよび同期方法 (コード、データ、ワークロードなどの異なるターゲットで使用されるエージェントレス、エージェントベース、パイプライン手法を含む) の広範な概要については、スキャン方法を参照してください。

エージェントレスのワークロードスキャンについて

- ディスクタイプがスナップショットをサポートしないため、エージェントレススキャンは、**エフェメラル**ディスクを使用する **Azure VM** をサポートしていません。この制限は、既定でエフェメラルディスクを使用する AKS クラスターに影響します。
- デフォルトでは、Tenable は、仮想マシンに接続されているルートボリュームと、対象となるルート以外のすべてのボリュームをスキャンします。ボリュームは、サイズが 600 GB を超えない場合に対象となります。Tenable は、仮想マシンごとにルートボリュームを含めて最大 4 つのボリュームをスキャンします。1 つ以上の非ルートボリュームが適格でない場合、Tenable はルートボリュームのみをスキャンし、仮想マシンのスキャンステータスは **「部分的」** と表示されます。この設定を管理するには、ワークロードを参照してください

Tenable One Cloud Exposure は API を利用してクラウドワークロードに接続し、マシンのストレージボリュームのスナップショットを抽出します。これらのボリュームは次に、スキャンを実行するマシンにマウントされ、以下が抽出されます。

1. インベントリ情報 (ソフトウェアパッケージ、ファイル署名など)。
2. 検出された脆弱性のセット。潜在的なリスクを露出するのに役立ちます。
3. 悪意のあるファイル。

暗号化されているボリュームは、Tenable によって復号化されます。抽出されたボリュームのスナップショットは、Tenable によってスキャン用にマウントされる前に、KMS キー (顧客アカウントで作成されたもの) で暗号化されます。キーポリシーは、ボリュームのコンテンツを復号化するためのアクセス権を Tenable アカウントと顧客アカウントのみに付与します。これによりボリュームが保護され、Tenable スキャナーのみがボリュームにアクセスして使用できるようになります。この抽出されたデータは クラウドサイバーエクスポージャーコンソールに表示され、必要に応じて分析と修正を行うことができます。

- 接続中に、Tenable はそのアプリケーション専用の KMS キーを生成します。このキーは、仮想マシンを作成し、スナップショットからボリュームをアタッチするために必要です。Tenable アウトポストではこのキーのみが使用され、カスタマーマネージドキーは共有されません。KMS キーへのアクセスはアプリケーションに制限され、スナップショットの作成に人間が介入することを防ぎます。スナップショットの作成は完全に自動化されているため、悪意のあるアクティビティのリスクが最小限に抑えられます。
- スナップショットの作成中に、Tenable によって各スナップショットに次のタグが自動的に適用されます。
    - `ErmeticContext: WorkloadAnalysis`
    - `ErmeticNamespace: Prd<Region><Deployment>` 例: `PrdUse2Dep2`、`PrdAps1Dep1`

注意:

- SIEM ツールを使用する場合、Tenableによって抽出またはマウントされたスナップショットに関連するアクティビティやアラートが表示される可能性があります。これには、Tenable ロールに関連する API の詳細などが含まれます。
- Tenable は NVD API を使用しますが、NVD によって推奨または認定されていません。

データ出力:

このスキャンプロセスにより、次のデータ出力が作成され、クラウドサイバーエクスポージャーコンソールのワークロード保護領域に表示されます。

- ソフトウェアパッケージ
- 脆弱性
- マルウェア

サポートされていないリージョン

スキャンはアウトポストベースかつリージョン固有です。スキャンを実行する Tenable アウトポストは、スキャン対象のマシンと同じリージョンにあります。Tenable は、ほとんどのリージョンでアウトポストをプロビジョニングします。クラウドプロバイダーの制限により、Tenable は現在これらのリージョンでアウトポストをプロビジョニングできません。

リソースがサポートされていないリージョンに存在する場合、Tenable はそれをスキャンせず、スキャンステータスは **[Unsupported]** と表示されます。詳細は、脆弱性のスキャンステータスを参照してください。

クラウドプロバイダー	リージョン名	リージョン識別子
AWS	中国(北京)	`cn-north-1`
AWS	中国 (寧夏)	`cn-northwest-1`
Azure	障害復旧 (DR)	すべてのリージョン
Azure	西インド	`westindia`
Azure	Jio インド西部	`jioindiawest`
Azure	ニュージーランド北部	`newzealandnorth`
Azure	スウェーデン南部	`swedensouth`

クラウドプロバイダー	リージョン名	リージョン識別子
Azure	台湾北部	`taiwannorth`
GCP	米国中部 2	`us-central2`
OCI	EU 専用クラウド (DCC) リージョン	`eu-dcc-*`
OCI	クリシエ、スイス	`eu-crissier-1`
OCI	EU ソブリン南部 (マドリード)	`eu-madrid-2`
OCI	EU ソブリン中央部 (フランクフルト)	`eu-frankfurt-2`
OCI	米国政府東部 (アッシュバーン)	`us-langley-1`
OCI	米国政府西部 (フェニックス)	`us-luke-1`

暗号化されたリソースのサポート

クラウドサイバーエクスポージャーでは、AWS、Azure、GCP の暗号化された仮想マシンボリュームのスキャンがサポートされます。ボリュームが暗号化されると、Tenable は抽出されたスナップショットを復号化し、クラウドアカウントで生成された専用 KMS キーで再暗号化します。Tenable では、カスタマーマネージドキーにアクセスする必要はありません。

暗号化されたリソースをスキャンするための要件は、クラウドプロバイダーによって異なります。

クラウドプロバイダー	サポートされている暗号化	必要な追加のアクセス許可
AWS	Amazon AWS マネージドキーまたはカスタマーマネージドキーで暗号化された Elastic Block Store (Amazon EBS) ボリューム	**なし** (標準のオンボーディングアクセス許可以外)

クラウドプロバイダー	サポートされている暗号化	必要な追加のアクセス許可
Azure	Azure Disk Encryption (ADE) を使用して暗号化されたマネージド仮想マシン。サポートされている Azure Disk Encryption 方式を参照してください。	Azure Key Vault ロール「Azure の必要なアクセス許可を参照してください。
GCP	顧客管理の暗号化キー (CMEK) で暗号化されたディスク	標準のオンボーディングアクセス許可を超えるものなし[1]

[1] Cloud KMS CryptoKey Decrypter ロールが付与する `cloudkms.cryptoKeyVersions.useToDecrypt` アクセス許可を含め、追加の Cloud Key Management Service (Cloud KMS) アクセス許可は必要ありません。

サポートされている Azure ディスク暗号化方式

Azure Disk Encryption (ADE) は、シークレット暗号化キーを使用するか、Key Vault のキーでディスク暗号化シークレットを暗号化することによって実行されます。サポートされている設定は以下のとおりです。

- **Windows (BitLocker 経由):** シークレット暗号化キーと、Key Vault のキーを使用した暗号化シークレットの両方がサポートされています。
- **Linux(DM-Crypt経由):** 秘密の暗号化キーはUbuntuでサポートされています。

Microsoft が Azure Disk Encryption (ADE) でサポートするオペレーティングシステムの詳細については、公式 の Microsoft ドキュメント を参照してください。

> **注意:**
>
> - 権限がないためにスキャンが失敗した場合、スキャンステータスは **[無効]** に更新され、ツールチップが表示されます。
> - 単一のディスク上での複数の暗号化パーティションはサポートされていません。

Azure の必要なアクセス許可

暗号化されたリソースデータを分析するには、Tenable 必要なアクセス許可を付与する必要があります。これらのアクセス許可は、以下を使用して割り当てることができます。

- `Key Vault Secrets User` 組み込みロール: シークレット暗号化キーに必要
- `Key Vault Crypto User` 組み込みロール: Key Vault (Key Encryption Key) のキーでシークレットを暗号化する場合に必要です
- 適切なアクセス許可を持つカスタムロール

これらのアクセス許可を追加する方法の詳細な手順については、「ワークロードの接続」を参照してください。

セキュリティとコンプライアンス

Tenable は、業界標準の暗号化方式と安全なアクセスプロトコルを使用して暗号化された VM ボリュームを分析し、全体を通じて完全なデータ保護を維持します。この機能は、暗号化が中核的な要件であるセキュリティフレームワークに準拠する必要がある組織をサポートします。

BitLocker ディスクのデータアクセス認証

BitLocker で暗号化されたディスクでは、脆弱性スキャン用に Shared Access Signature (SAS) BLOB コピーパスが必要です。これらのディスクタイプの仮想マシン (VM) でデータアクセス認証を有効にすると、スキャンが失敗する場合があります。

スキャンを確実に成功させるために、Tenable はこの `DataAccessAuthMode` をオーバーライドし、BitLocker で暗号化されたディスクのスナップショット作成プロセス中に `None` に設定します。

Azure Policy 設定

Azure ポリシー **ディスクまたはスナップショットへのエクスポートまたはアップロード時に認証要件でデータを保護する** と、`DataAccessAuthMode` が `None` に設定されないようにします。この制限により、スナップショットの作成が失敗します。

この問題を解決し、脆弱性スキャンを許可するには

1. 専用の **ディスクスナップショットリソースグループ**を設定します。
2. Azure ポリシーから必要な **ディスクスナップショットリソースグループ** を除外します。

非ルートボリュームスキャン

デフォルトでは、Tenable は、仮想マシンに接続されているルートボリュームと、対象となるルート以外のすべてのボリュームをスキャンします。別々のディスクにインストールされているアプリケーションとデータベースは、脆弱性評価に含まれます。

非ルートボリュームスキャンには、次の制限が適用されます。

- **最大ディスクサイズ**: 600 GB (個別のディスク)
- **仮想マシンあたりの最大ボリューム:** ルートボリュームを含めて 4

部分的なスキャンステータス

Tenable は、非ルートボリュームに対してオール・オア・ナッシングのアプローチを使用します。1 つ以上の非ルートボリュームが適格でない場合 (たとえば、ディスクのサイズ制限が 600 GB を超えた場合)、Tenable はすべての非ルートボリュームをスキップし、ルートボリュームのみをスキャンします。仮想マシンのスキャンステータスが **[部分]** と表示されます。

仮想マシンに接続されている各ディスクのスキャンステータスを表示するには、仮想マシンのプロファイルページに移動し、**[概要]** タブを開きます。**[ディスク/ボリューム]** テーブルには、ボリュームごとのステータスが表示されます。

非ルートボリュームスキャンの無効化

非ルートボリュームスキャンはデフォルトで有効になっています。無効にするには

- **[Settings > Security** > **Workload]** に移動し、**[Extended Disk Scanning]** をオフに切り替えます。

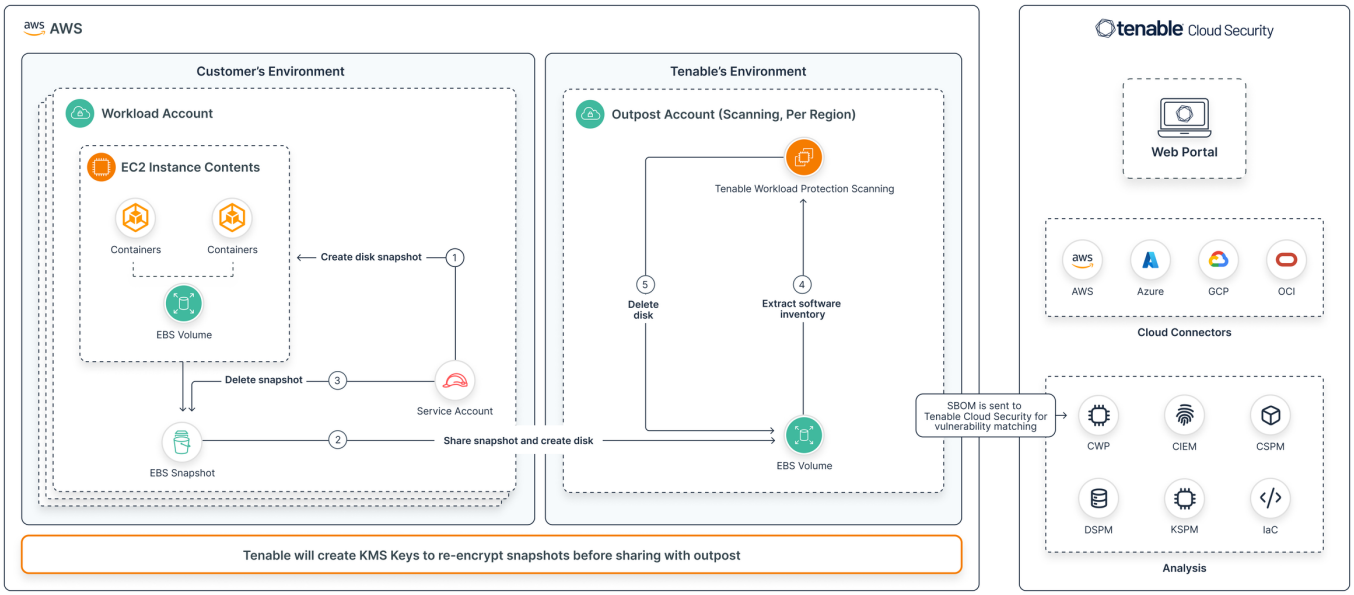
非ルートボリュームの請求方法については、「FAQ: ワークロード保護」を参照してください。

スキャンのワークフロー図

次の図では、各クラウドプロバイダーのスキャンワークフローを示しています。

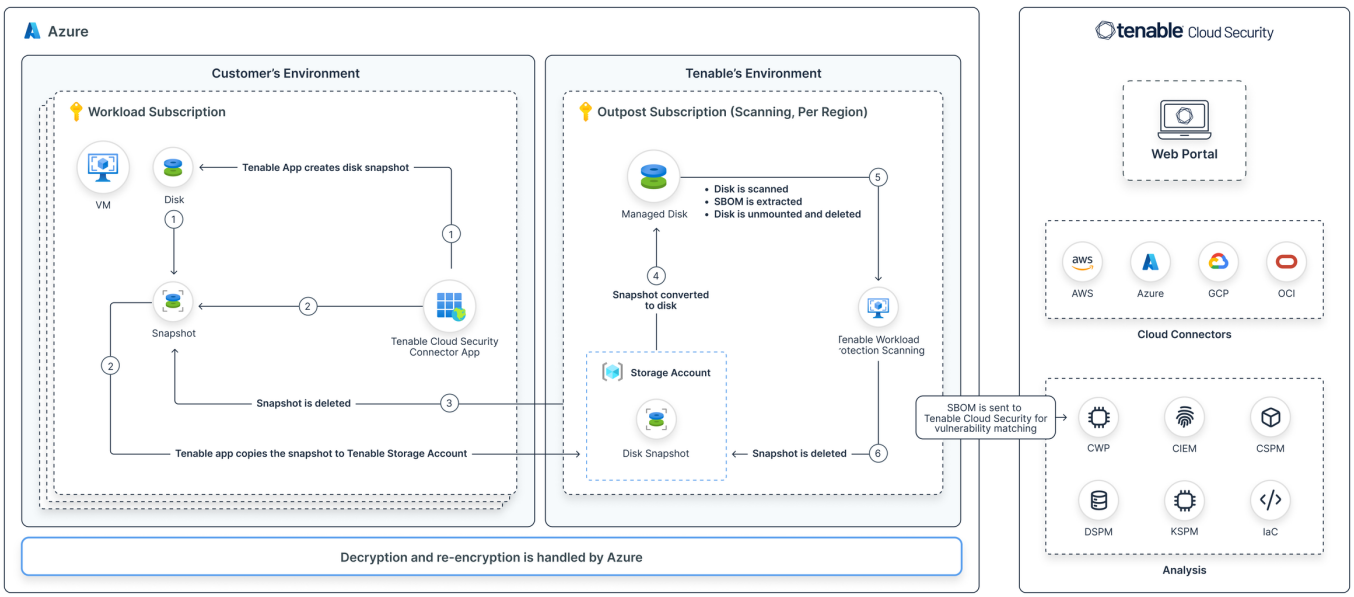
AWS

次の図は、AWS のスキャンワークフローを示しています。



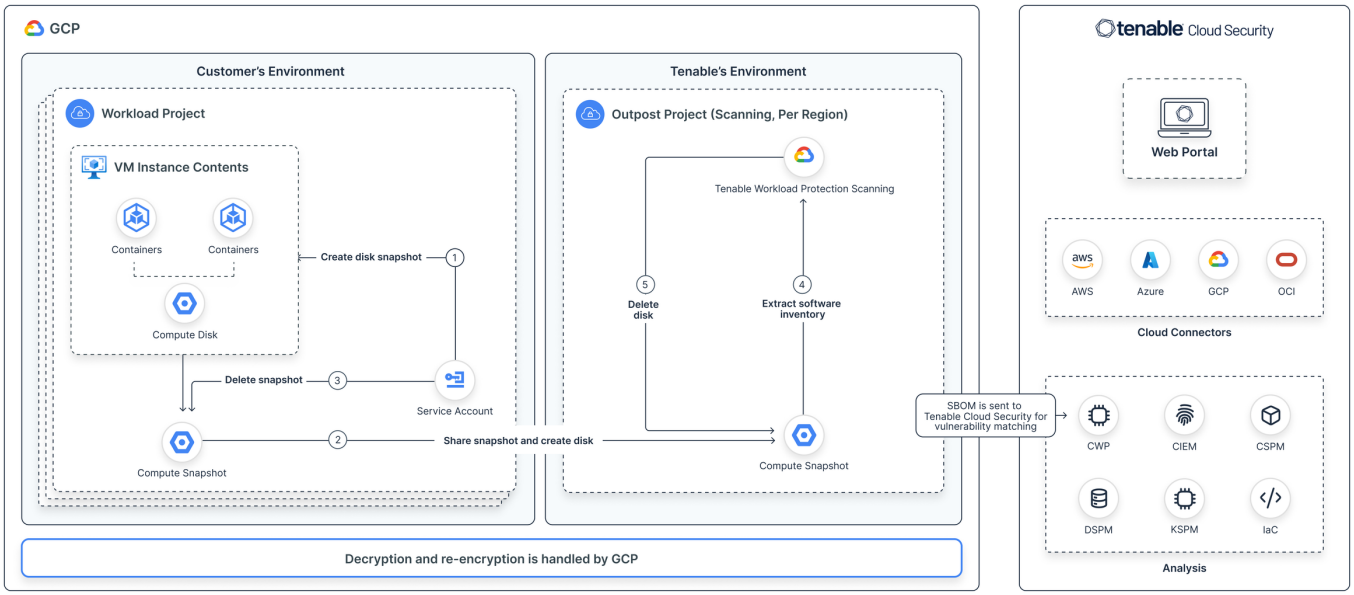
Azure

次の図は、Azure のスキャンワークフローを示しています。

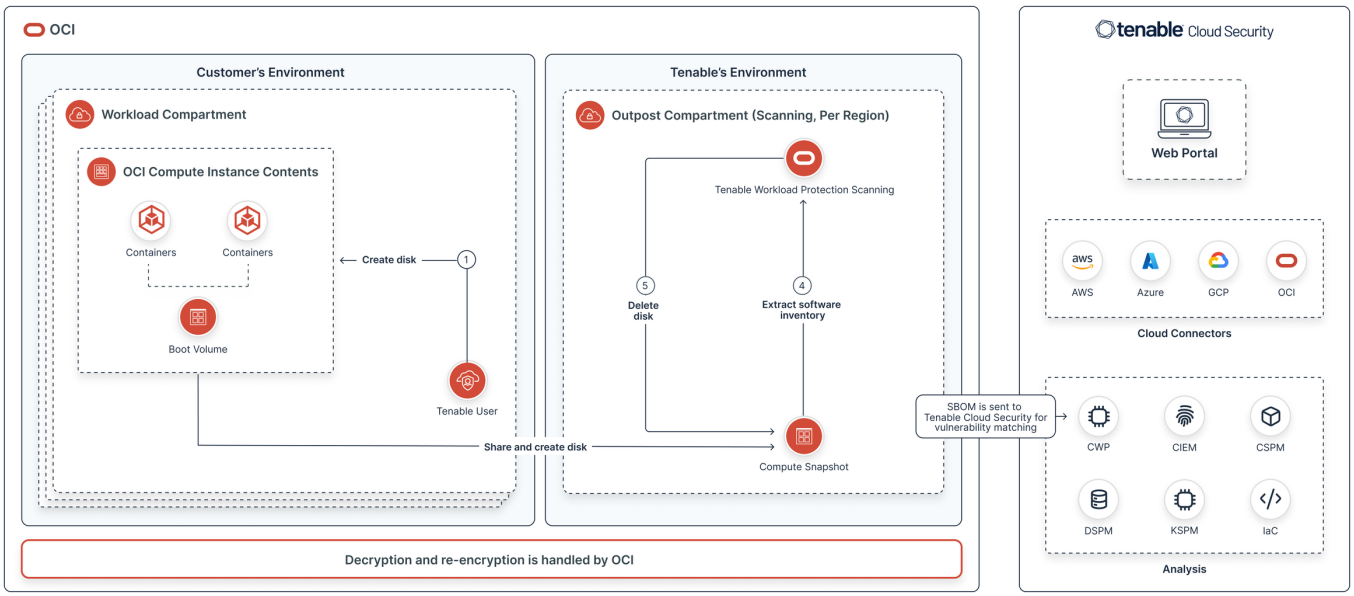


GCP

次の図は、GCP のスキャンワークフローを示しています。



OCI



Tenable の検出対象

Tenable は現在、以下のクラウドワークロードコンポーネントをスキャンできます。

コンポーネント	Tenable のスキャン対象
ワークロード	• 仮想マシン • 仮想マシンイメージ (AWS のみ) • コンテナイメージ • コンテナレジストリ • Kubernetes クラスタ
オペレーティングシステム	Linux、Windows
クラウドプロバイダー	AWS、Azure、GCP、OCI

- Tenable は、ディスクサイズが 600GiB までの仮想マシンをスキャンします。この値を変更したい場合は、サポートにお問い合わせください。
- Tenable は、コンテナの仮想マシンインスタンスもスキャンできます。
    - これらのインスタンスで見つかったコンテナは、関連するパッケージや脆弱性とともに、Tenable でのコンテナイメージとして表示されます。
    - Tenable がモニタリングするクラウドベースのコンテナレジストリ (Amazon ECR、Azure ACR など) でコンテナがホストされている場合、リポジトリへのリンクが表示されます。

  Tenable は現在、サーバーレスインフラ (例: AKS 仮想ノード、GKE Autopilot、OKE 仮想ノード、EKS Fargate) で実行されているコンテナはスキャンしません。
- **Azure**: Tenable が環境でリソースロックを検出した場合、影響を受ける仮想マシンのスキャンが一時的に無効になります。通常の動作を復元するには、ロックを解除してスキャンが自動的に再開されるようにすることをお勧めします。
- **OCI**: コンテナレジストリのスキャンはサポートされていません。

これらの各コンポーネントについて、Tenable は次を検出します。

- 一般情報 (OS のタイプやバージョンなど)
- インストールされているソフトウェア
- ソフトウェアまたは OS カーネルは攻撃に対して脆弱か
- 脆弱である場合、どの脆弱性に当てはまるか
- OS が古いまたは EOL か (そのため、アップグレードする必要があるか)

これらの機能は継続的に更新されます。使用している特定のワークロードまたはコンポーネントがあり、確認したい場合は、サポートへの問い合わせ。

スキャンで使用されるポリシー

ワークロード保護カテゴリに属する以下の組み込みクラウドサイバーエクスポージャーポリシーは、環境のスキャンに使用されます。クラウドサイバーエクスポージャーでのポリシーの使用方法に関する詳細については、クラウドポリシーを参照してください。

- コンテナイメージのオペレーティングシステムのサポート期間が終了、または終了が近づいています
- コンテナイメージのオペレーティングシステムにパッチが適用されていません
- コンテナイメージに、対処する必要がある脆弱性が含まれています
- 仮想マシンのオペレーティングシステムのサポート期間が終了、または終了が近づいています
- 仮想マシンのオペレーティングシステムにパッチが適用されていません
- 仮想マシンに、対処する必要がある脆弱性が含まれています

注意:

- パッチ未適用のオペレーティングシステムに関連するポリシーは、既知の修正がある脆弱性のみに警告を発します。
- オペレーティングシステムは、正式なサポート終了日の 30 日前に、サポート終了間近と見なされます。
- 仮想マシンが 30 日以上停止されていた場合、関連する検出結果の深刻度はレベルが 1 つ下がります。たとえば、重大から高に変わります。

Tenable がソフトウェアと脆弱性を特定する方法

Tenable は、幅広い公開データソース (Windows の場合は MSRC、Linux の場合は NVD など) から既知の脆弱性情報を抽出し、次のような完全な脆弱性データベースをコンパイルします。

- 脆弱なオペレーティングシステム/ソフトウェアバージョン
- これらの脆弱性に対処する KB またはアップグレードバージョン (可能な場合)

並行して、Tenable は仮想マシン (すべての Windows ユーザーアカウント/プロファイルを含む) のレジストリ/パッケージマネージャーから次の情報を抽出します。

- OS 情報 (CPU アーキテクチャ、バージョンなど)
- インストールされている KB のリスト (Windows のみ)
- インストール済みのソフトウェアのリスト (Windows Workloads にあるファーストパーティとサードパーティのアプリを参照)

Tenable はその後、マシンにインストールされている OS のバージョンと既知の脆弱性のリストを比較し、特定の VM に関連する脆弱性のリストと、推奨される修正を強調表示します。

データソースの選択

Tenable は、適切な OS ベンダーのアドバイザリデータベースを使用します。たとえば、yum (Amazon Linux) からインストールされた Python パッケージの場合、Tenable は ALAS のアドバイザリのみを取得します。OS パッケージマネージャーからインストールされたパッケージ (dpkg、yum、apk など) の場合、これは誤検出を防ぐのに役立ちます。その理由は、OS ベンダーは通常、新しいアップストリームバージョンから以前のバージョンに修正をバックポートしており、修正されたバージョンが上流の修正済みバージョンと異なる可能性があるためです。
パッケージマネージャー以外でインストールされた製品の場合、アドバイザリは通常、脆弱性が最初に公開される場所であるため、可能な限り最速のカバレッジを提供することができます。

CVSS 深刻度の基本値

> **注意:** 深刻度は、選択した深刻度メトリクスに基づいて計算されます。深刻度メトリクスを設定するには、脆弱性の深刻度のメトリクスを参照してください。

深刻度は以下のように CVSS スコアに基づいて決定されます。

基本値範囲	深刻度
0.1 ~ 3.9	低
4.0 ~ 6.9	中
7.0 ~ 8.9	高
9.0 ~ 10.0	重大

- CVSS スコアもない場合は、NVD の深刻度が使用されます。

Linux

- Linux OS のバージョン
- Linux 対応言語
- Linux でサポートされるファイルシステム

Linux OS のバージョン

は クラウド サイバーエクスポージャー 、以下の Linux バージョンの脆弱性を特定し、**検出** します。

OS	対応バージョン	パッケージマネージャー
Alpine Linux	2.2 - 2.7、3.0 - 3.18、edge	apk
Wolfi Linux	(該当なし)	apk
Chainguard	(該当なし)	apk
Red Hat Enterprise Linux	6、7、8、9	dnf/yum/rpm

OS	対応バージョン	パッケージマネージャー
Red Hat Enterprise Linux CoreOS	4.x	(該当なし)
CentOS	6, 7, 8	dnf/yum/rpm
AlmaLinux	8、9	dnf/yum/rpm
Rocky Linux	8、9	dnf/yum/rpm
Oracle Linux	5、6、7、8、9	dnf/yum/rpm
CBL-Mariner	1.0、2.0、3.0	dnf/yum/rpm
Amazon Linux	1、2、2023	dnf/yum/rpm
openSUSE Leap	42、15	zypper/rpm
SUSE Enterprise Linux	11、12、15	zypper/rpm
Photon OS	1.0、2.0、3.0、4.0	tndf/yum/rpm
Debian GNU/Linux	7、8、9、10、11、12、13	apt/dpkg
Ubuntu	• 24.04 LTS (Noble Numbat) • 22.04 LTS (Jammy Jellyfish) • 20.04 LTS (Focal Fossa) • 18.04 LTS (Bionic Beaver)	apt/dpkg

OS	対応バージョン	パッケージマネージャー
	• 16.04 LTS (Xenial Xerus) • 14.04 LTS (Trusty Tahr)	
Bottlerocket	**注意**: この OS は、拡張ディスクスキャンが有効になっている場合 (デフォルト) にスキャンされます。**[設定]** > **[セキュリティ]** > **[ワークロード]** の順に移動し、**[拡張ディスクスキャン]** をオンにします。	(該当なし)
Google Container-Optimized OS (COS)	**注意**: サポートは、**ソフトウェアインベントリの可視性**に限定されます。Tenable One Cloud Exposure は Google COS ホスト上にインストールされているすべてのパッケージとコンポーネントを正確に検出して報告しますが、このオペレーティングシステム向けのアドバイザリベースの脆弱性診断も開発中です。現時点では、誤検出をなくすため、Google COS の脆弱性検出結果が意図的に制限されています。完全な脆弱性検出は、今後のリリースで利用可能になる予定です。	(該当なし)

Linux 対応言語

クラウドサイバーエクスポージャー では、ソフトウェアおよび Linux マシンの脆弱性に関して、次の言語をサポートしています。

言語	CI/CD スキャン	レジストリスキャン	ワークロードスキャン
DotNet	✓	✓	✓
移動	✓	✓	✓
Java	✓	✓	✓

言語	CI/CD スキャン	レジストリスキャン	ワークロードスキャン
JavaScript	✓	✓	✓
PHP	✓	✓	✓
Python	✓	✓	✓
Ruby	✓	✓	✓
Rust	✓	✓	✓

Linux でサポートされるファイルシステム

クラウドサイバーエクスポージャーは、標準 (非 LVM) と LVM の両方の設定で、**XFS** および **ext4** ファイルシステムを使用するクラウドワークロードのスキャンをサポートしています。

詳細については、論理ボリューム・マネージャー (Linux)を参照してください。

Windows

- Windows OS のバージョン
- Windows でのファーストパーティとサードパーティのアプリ

Windows OS のバージョン

Tenable は、次の Windows バージョンの**脆弱性を特定**し、**検出**します。

サポート対象の Windows バージョン			
Windows 10 バージョン 1507	Windows 10 バージョン 1607	Windows 10 バージョン 1809	Windows 10 バージョン 21H2
Windows 10 バージョン	Windows 11 バー	Windows 11 バー	Windows 11 バージョン

サポート対象の Windows バージョン			
22H2	ジョン 21H2	ジョン 23H2	25H2
Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server バージョン 23H2

Windows でのファーストパーティとサードパーティのアプリ

Tenable は、Windows ワークロードにインストールされているファーストパーティおよびサードパーティのアプリをスキャンしてレポートします。スキャンのサポートは現在、Windows Server にデプロイされて広く使用されているアプリ(以下の表に記載)で利用でき、今後のリリースで追加のサポートが計画されています。よく表示されるアプリは、[ソフトウェア] ページで次のフィルターを適用することで確認できます。

- タイプ = パッケージ、ライブラリ、オペレーティングシステム
- オペレーティングシステムのタイプ = Windows

> **注意:** このリストには、Windows でサポートされるソフトウェアのサブセットのみが含まれます。

上位のサポート対象アプリケーション							
Microsoft .NET Desktop	Microsoft .NET Runtime	Microsoft ASP.NET Core	Microsoft Azure CLI	Microsoft Edge	Microsoft FSLogix Apps	Microsoft Intune	Microsoft Office

上位のサポート対象アプリケーション							
Runtime		Runtime					
Microsoft Visual Studio Code	7-Zip	Adobe Acrobat Reader	Adobe Dreamweaver	Amazon CloudWatch Agent	Amazon SSM Agent	Apache Tomcat	Autodesk AutoCAD
Autodesk Revit	Dell Wyse Management Suite	DotNet	FileZilla Client	FortiClient VPN	Foxit Reader	FSlogix	Git
Go	Google Chrome	IBM InfoSphere	IBM MQ	IntelliJ IDEA	Java	JetBrains Rider	JetBrains Toolbox
KeePass Password Safe	MobaXterm	Mozilla Firefox	MySQL Server	Nessus Agent (x64)	Node.js	Nmap	Notepad++
OpenE	OpenSS	Opera	Opsview	Oracle	Powers	PRTG	PuTTY

上位のサポート対象アプリケーション							
dge	L		NSClient++ Windows Agent (x64)	VM VirtualBox	hell	Network Monitor	
Python	Qualys クラウド サイバーエクスポージャー Agent	Rapid7 Insight Agent	RARLAB WinRAR	SoapUI	SolarWinds SCP Server	SOLIDWORKS eDrawings	TeamViewer
Tenable Nessus (x64)	TightVNC	Veeam Agent	Veeam Backup	VLC media player	VMware Tools	VMware Workstation	Websphere MQ
WinMerge	WinSCP	WireShark	XAMPP	Xming			

エージェント ベースの Kubernetes ワークロード スキャン

> **注意:** エージェント ベースのスキャンは、**Cloud Vulnerability Management** ライセンスでは使用できません。

クラウドワークロード保護には、**エージェントベース**または**エージェントレス**のスキャンを使用できます。それぞれ、セキュリティのニーズ、コンプライアンス要件、運用上の制約に応じて異なる利点があります。この記事では、**エージェントベースのスキャンについて説明します**。エージェントレスのワークロードスキャンの詳細については、「エージェントレスワークロードスキャンを参照してください。2 つの手法の比較については、エージェントレススキャンとエージェントベーススキャンの比較を参照してください。

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

この記事では、Tenable One Cloud Exposure で使用される特定のスキャン方法の詳細について説明します。さまざまなリソースタイプと運用段階で使用されるすべてのスキャンおよび同期方法 (コード、データ、ワークロードなどの異なるターゲットで使用されるエージェントレス、エージェントベース、パイプライン手法を含む) の広範な概要については、スキャン方法を参照してください。

- 接続中に、Tenable はそのアプリケーション専用の KMS キーを生成します。このキーは、仮想マシンを作成し、スナップショットからボリュームをアタッチするために必要です。Tenable アウトポストではこのキーのみが使用され、カスタマーマネージドキーは共有されません。KMS キーへのアクセスはアプリケーションに制限され、スナップショットの作成に人間が介入することを防ぎます。スナップショットの作成は完全に自動化されているため、悪意のあるアクティビティのリスクが最小限に抑えられます。
- スナップショットの作成中に、Tenable によって各スナップショットに次のタグが自動的に適用されます。
    - `ErmeticContext: WorkloadAnalysis`
    - `ErmeticNamespace: Prd<Region><Deployment>` 例: `PrdUse2Dep2`、`PrdAps1Dep1`

エージェントベースの Kubernetes ワークロードスキャンについて

Helm チャートコマンドを活用して環境内の関連するクラスタを接続することで、次の **Kubernetes ワークロード** の脆弱性をスキャンできます。

- クラウドマネージド (EKS/AKS/GKE/OKE)
- アンマネージド (Kubernetes クラスタを実行している仮想マシン)

この機能は、コマンドを使用してクラスタ内にセンサーをインストールすることで有効にできます。

センサーは package-manager とインストールされているライブラリのクエリを実行し、ホストにインストールされているソフトウェアと、ノードで実行されているコンテナイメージを特定します。その後、センサーはこのソフトウェアインベントリをさらに分析するために Tenable に送信します。

注意: センサーは、新しいコンテナイメージがないかクラスタノードを継続的に監視し、新しいイメージごとに約 30 分以内にスキャンします。これには、CronJob やその他の一時的な Pod によって作成されたものなど、有効期間の短いイメージが含まれます。検出結果のアップデートは、オーケストレーションサイクルによって異なります。

注意: センサーは、設計要件に応じて、**Kubernetes** と **Red Hat OpenShift** の両方のコンテナオーケストレーションプラットフォームにデプロイできます。Kubernetes はオープンソースプラットフォームであり、コンテナオーケストレーションの基盤として機能します。一方、OpenShift は追加機能で Kubernetes を拡張します。

はじめに:

ワークロードKubernetesの脆弱性をスキャンするを参照してください。

データ出力:

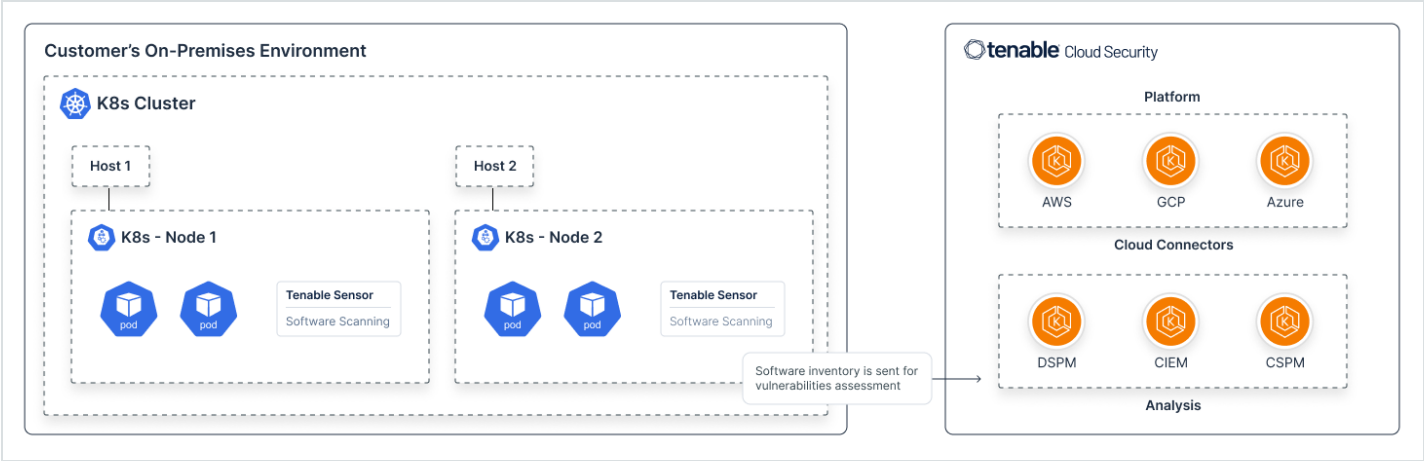
このスキャンプロセスにより、次のデータ出力が作成され、Tenable One Cloud Exposure コンソールのワークロード保護領域に表示されます。

- ソフトウェアパッケージ
- 脆弱性

注意: Tenable は NVD API を使用していますが、NVD の推奨または認定を受けていません。

スキャンのワークフロー図

次の図は、クラウドサイバーエクスポージャー センサーが DaemonSet として各 Kubernetes ノードにインストールされる方法を示しています。これらのセンサーは、ノードをホストしている仮想マシンを含む、オンプレミスの Kubernetes 環境をスキャンします。スキャンプロセスが完了すると、収集されたソフトウェアインベントリ(SBOM) は脆弱性評価のために Tenable に送信されます。



Tenable によるスキャナーの更新方法

センサーは、クラウドサイバーエクスポージャー の新しいバージョンがリリースされるたびに自動的に更新されます。互換性とスキャン機能を維持するために、最新バージョンに更新する必要があります。
更新プロセスは以下のようになっています。

1. 各バージョンのリリースに合わせて、クラウドサイバーエクスポージャー は更新されたセンサーイメージを提供します。
2. 実行中のセンサーは古くなったことを検出し、自身のプロセスを終了して、ポッドの再起動をトリガーします。
3. 再起動時に、daemonset は最新のイメージをプルするように設定され、リポジトリの新しいバージョンを指します。AWS ECR の Tenable のプライベートコンテナレジストリからこのイメージを取得し、Tenable バックエンドからトークンを介して認証を行います。
4. ポッドは新しいイメージを使用して再起動し、センサーがスキャンを再開して結果を Tenable バックエンドに送信できるようになります。

Tenable の検出対象

クラウドサイバーエクスポージャー は現在、以下のワークロードコンポーネントをスキャンできます。

要素	スキャン Tenable 対象
プラットフォームタイプ	• オンプレミス • AWS • Azure • GCP
ワークロード	ホストを含む Kubernetes ノードと、ノード上で実行されているコンテナイメージ。
オペレーティングシステム	Linux

注意: Tenable はコンテナのノードもスキャンします

- これらのノードで見つかったコンテナは、関連するパッケージと脆弱性とともに、Tenable の仮想マシンとして表示されます。
- Tenableモニタリングするクラウドベースのコンテナレジストリ (Amazon ECR、Azure ACR など) でコンテナがホストされている場合、リポジトリへのリンクが表示されます。

警告: OCI センサーベースエージェントベースのスキャンはサポートされていません。

これらの各コンポーネントについて、Tenable は以下を検出します。

- 一般情報 (OS のタイプやバージョンなど)
- どのソフトウェアがインストールされていますか?
- ソフトウェアまたは OS カーネルは攻撃に対して脆弱か?
- 脆弱である場合、どの脆弱性に当てはまるか。
- OS が古いまたは EOL か (そのため、アップグレードする必要がありますか)

これらの機能は継続的に更新されます。使用している特定のワークロードまたはコンポーネントがあり、Tenable がサポートしているか確認するには、テクニカルサポートまでお問い合わせください。サポートへの問い合わせ。

スキャンで使用されるポリシー

_ワークロード保護_カテゴリに属する以下の組み込みクラウドサイバーエクスポージャーポリシーは、環境のスキャンに使用されます。クラウドサイバーエクスポージャーでのポリシーの操作方法に関する詳細については、「クラウドポリシーを参照してください。

プラットフォーム	カテゴリ	名前
AWS/Azure/GCP/オンプレミス	ワークロード保護	コンテナイメージのオペレーティングシステムのサポート期間が終了、または終了が近づいています
		コンテナイメージのオペレーティングシステムにパッチが適用されていません
		コンテナイメージに、対処する必要がある脆弱性が含まれています
		仮想マシンのオペレーティングシステムのサポート期間が終了、または終了が近づいています
		仮想マシンのオペレーティングシステムにパッチが適用されていません
		仮想マシンに、対処する必要がある脆弱性が含まれています

注意: パッチ未適用のオペレーティングシステムに関連するポリシーは、既知の修正がある脆弱性のみに警告を発します。

Tenable がソフトウェアと脆弱性を特定する方法

Tenable は、幅広い公開データソース (Windows の場合は MSRC、Linux の場合は NVD など) から既知の脆弱性情報を抽出し、次のような完全な脆弱性データベースをコンパイルします。

- 脆弱なオペレーティングシステム/ソフトウェアバージョン
- これらの脆弱性に対処するKBまたはアップグレードバージョン(可能な場合)

並行して、Tenableは仮想マシン(すべてのWindowsユーザーアカウント/プロファイルを含む)のレジストリ/パッケージマネージャーから次の情報を抽出します。

- OS情報(CPUアーキテクチャ、バージョンなど)
- インストールされているKBのリスト(Windowsのみ)
- インストール済みのソフトウェアのリスト(Windows Workloadsにあるファーストパーティとサードパーティのアプリを参照)

Tenableはその後、マシンにインストールされているOSのバージョンと既知の脆弱性のリストを比較し、特定のVMに関連する脆弱性のリストと、推奨される修正を強調表示します。

データソースの選択

Tenableは、適切なOSベンダーのアドバイザリデータベースを使用します。たとえば、yum (Amazon Linux)からインストールされたPythonパッケージの場合、TenableはALASのアドバイザリのみを取得します。OSパッケージマネージャーからインストールされたパッケージ(dpkg、yum、apkなど)の場合、これは誤検出を防ぐのに役立ちます。その理由は、OSベンダーは通常、新しいアップストリームバージョンから以前のバージョンに修正をバックポートしており、修正されたバージョンが上流の修正済みバージョンと異なる可能性があるためです。
パッケージマネージャー以外でインストールされた製品の場合、アドバイザリは通常、脆弱性が最初に公開される場所であるため、可能な限り最速のカバレッジを提供することができます。

CVSS深刻度の基本値

> **注意:** 深刻度は、選択した深刻度メトリクスに基づいて計算されます。深刻度メトリクスを設定するには、脆弱性の深刻度のメトリクスを参照してください。

深刻度は以下のようにCVSSスコアに基づいて決定されます。

基本値範囲	深刻度
0.1 ~ 3.9	低
4.0 ~ 6.9	中
7.0 ~ 8.9	高
9.0 ~ 10.0	重大

- CVSS スコアもない場合は、NVD の深刻度が使用されます。

Linux

- Linux OS のバージョン
- Linux 対応言語
- Linux でサポートされるファイルシステム

Linux OS のバージョン

は Tenable 、以下の Linux バージョンの脆弱性を特定し、**検出** します。

OS	対応バージョン	パッケージマネージャー
Alpine Linux	2.2 - 2.7、3.0 - 3.18、edge	apk
Wolfi Linux	(該当なし)	apk
Chainguard	(該当なし)	apk
Red Hat Enterprise Linux	6、7、8、9	dnf/yum/rpm

OS	対応バージョン	パッケージマネージャー
Red Hat Enterprise Linux CoreOS	4.x	(該当なし)
CentOS	6, 7, 8	dnf/yum/rpm
AlmaLinux	8、9	dnf/yum/rpm
Rocky Linux	8、9	dnf/yum/rpm
Oracle Linux	5、6、7、8、9	dnf/yum/rpm
CBL-Mariner	1.0、2.0、3.0	dnf/yum/rpm
Amazon Linux	1、2、2023	dnf/yum/rpm
openSUSE Leap	42、15	zypper/rpm
SUSE Enterprise Linux	11、12、15	zypper/rpm
Photon OS	1.0、2.0、3.0、4.0	tndf/yum/rpm
Debian GNU/Linux	7、8、9、10、11、12、13	apt/dpkg
Ubuntu	• 24.04 LTS (Noble Numbat) • 22.04 LTS (Jammy Jellyfish) • 20.04 LTS (Focal Fossa) • 18.04 LTS (Bionic Beaver)	apt/dpkg

OS	対応バージョン	パッケージマネージャー
	• 16.04 LTS (Xenial Xerus) • 14.04 LTS (Trusty Tahr)	
Bottlerocket	**注意**: この OS は、拡張ディスクスキャンが有効になっている場合 (デフォルト) にスキャンされます。**[設定]** > **[セキュリティ]** > **[ワークロード]** の順に移動し、**[拡張ディスクスキャン]** をオンにします。	(該当なし)
Google Container-Optimized OS (COS)	**注意**: サポートは、**ソフトウェアインベントリの可視性**に限定されます。Tenable One Cloud Exposure は Google COS ホスト上にインストールされているすべてのパッケージとコンポーネントを正確に検出して報告しますが、このオペレーティングシステム向けのアドバイザリベースの脆弱性診断も開発中です。現時点では、誤検出をなくすため、Google COS の脆弱性検出結果が意図的に制限されています。完全な脆弱性検出は、今後のリリースで利用可能になる予定です。	(該当なし)

Linux 対応言語

Tenable では、ソフトウェアおよび Linux マシンの脆弱性に関して、次の言語をサポートしています。

言語	CI/CD スキャン	レジストリスキャン	ワークロードスキャン
DotNet	✓	✓	✓
移動	✓	✓	✓
Java	✓	✓	✓

言語	CI/CD スキャン	レジストリスキャン	ワークロードスキャン
JavaScript	✓	✓	✓
PHP	✓	✓	✓
Python	✓	✓	✓
Ruby	✓	✓	✓
Rust	✓	✓	✓

Linux でサポートされるファイルシステム

Tenable は、標準 (非 LVM) と LVM の両方の設定で、XFS および ext4 ファイルシステムを使用するクラウドワークロードのスキャンをサポートしています。
詳細については、論理ボリューム・マネージャー (Linux)を参照してください。

コンテナイメージスキャン

> **注意:** 一部の機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Tenable One Cloud Exposureを使用して、コンテナイメージのソフトウェア脆弱性をスキャンします。本番前環境でコンテナを可視化し、コンテナ化されたアプリケーションの潜在的なリスクをデプロイメント前に特定します。プロセスのできるだけ早い段階で、コンテナイメージとレジストリの脆弱性を迅速に修正するために必要な情報を DevOps チームに提供します。

コンテナイメージスキャンは、次の 3 つのステージのいずれか、またはすべてで実装でき、コンテナのライフサイクル全体を通じて継続的なセキュリティを確保します。

スキャン	ライフサイクルステージ	説明	サポート対象
コンテナイメージ CI/CD	ビルド	コンテナイメージをスキャンして、デプロイメント前に脆弱性に対処します。CI/CD パイプラインの最初のこのステージでは、ビルドプロセス中に自動スキャンが行われ、デプロイメント前にコンテナイメージに脆弱性がないことを確認します。	Windows ベースおよび Linux ベースのコンテナー
コンテナイメージレジストリスキャン	ストレージ	コンテナレジストリリポジトリに保存されている脆弱なコンテナイメージを検出し、警告します。このステージでは、レジストリに保存されているコンテナイメージをスキャンし、潜在的なリスクを体系的に特定して対処します。	Windows ベースおよび Linux ベースのコンテナー
ワークロード保護	ランタイム	最終ステージでは、本番環境で実行中のコンテナの継続的なモニタリングとスキャンを行い、脆弱性と脅威を迅速に検出して軽減できるようにします。	Linux ベースのコンテナのみ

注意:

- クラウドサイバーエクスポージャーは、**コンテナランタイム** (Docker、**Podman**、**containerd**、**CRI-O**) を利用する仮想マシン内のコンテナを検出します。
- ワークロードスキャンのステージは、現時点では記事に含まれていません。Tenable がワークロードをスキャンする方法の詳細については、エージェントレススキャンとエージェントベーススキャンの比較。

注意: コンテナイメージスキャンのコンテキストでは、以下が請求可能なリソースと見なされます。

- (CI/CD スキャン)ビルドプロセスの一部としてコンテナがプッシュされる各コンテナリポジトリ
- (レジストリスキャン)各スキャンされたコンテナリポジトリ

コンテナイメージレジストリスキャン

これは Tenable によるレジストリのスキャン方法の概念上の概要です。

- コンテナイメージレジストリの接続に関する統合ガイドについては、コンテナイメージレジストリの接続を参照してください。
- コンテナイメージの表示と管理に関するハウツーガイドについては、「コンテナイメージを参照してください。

Tenable コンテナレジストリリポジトリに保存されているコンテナイメージをスキャンし、レジストリ内の潜在的なリスクを特定します。Tenable スキャン

- クラウドホスト型レジストリ
  - AWS Elastic Container Registry (ECR)
  - Azure Container Registry (ACR)
  - Google Container Registry (GCR)
  - Alibaba クラウドコンテナレジストリ (ACR)
- 独立したレジストリ:
  - JFrog Artifactory
  - Red Hat岸壁
  - Sonatype Nexus リポジトリ
  - ハーバー
- リポジトリ内の最新の 10 個までのイメージと、現在使用中のすべてのイメージ
- タグ付けされた画像

スキャンしたイメージを表示するには、「コンテナイメージ」を参照してください。

注意:

- レジストリスキャンは、2 GiB 以下のコンテナイメージで有効になっています。詳細について、またはこの値を変更するには、サポートへの問い合わせ。
- Tenableベースのスキャンは、コンテナイメージに対して追加のコンテキストを提供します。これは、クラウドプロバイダーによって実行されるスキャンでは利用できません。Tenable によってスキャンされたコンテナイメージでは、リソースビューに追加のWorkload タブがあり、関連する修正とともに、1) イメージにインストールされたソフトウェアパッケージと 2) イメージ上で検出された脆弱性に関する情報を提供します。

コンテナレジストリポリシー

必要なライセンス: 脆弱性管理全体はCNAPPライセンスでのみ利用可能ですが、この機能はすべてのライセンスタイプで利用できます。

次の組み込みTenable One Cloud Exposureポリシーは環境をスキャンし、脆弱なコンテナレジストリリポジトリについてアラートを通知するために使用されます。

- **コンテナイメージのリポジトリに、対処する必要がある脆弱性が含まれています**

このポリシーは、レジストリで最後にスキャンされたコンテナイメージを調べ、タグ付けされたイメージのみを調べます。これには実際に置換できるコンテナイメージのバージョンが反映されるため、より実用的な検出結果が得られます。

スナップショットスキャン費用計算ツール

クラウドアカウントでTenableが一時的に作成するスナップショットは請求の対象です。ただし、スナップショットはスキャンが完了するとすぐに削除され、どのスナップショットも存在する時間が最短になるようにスキャンプロセスが最適化されます。VMが1,000個の環境の場合、このコストは1か月あたり100ドルかからない計算です。

注意: (AWS) 誤って削除したスナップショットをごみ箱から復元するための保持ルールを作成した場合、追加コストが発生する可能性があります。価格設定の詳細については、AWS documentationを参照してください。

- 何らかの理由でスキャンプロセスが完了しなかった場合、スナップショットは12時間後に削除されます。
- スキャンは、マシンと同じリージョンで実行されます (Tenableはすべてのリージョンでクラスタ (アウトポスト と呼ばれる) をセットアップします)。したがって、エグレスコストは発生しません。

以下の計算機を使用すると、ワークロードスキャンに関連する追加の月次コストを見積もることができます。

注意: 以下の計算機では、標準のAmazon S3価格に基づいてGiB/月あたり0.02ドルのデフォルトのコスト値を使用していますが、請求明細書を確認し、お使いの環境に適した値を入力することをお勧めしま

す。クラウドプロバイダーの価格設定の詳細は、関連する AWS、Azure、GCP のドキュメントを参照してください。

Cost $ (GiB/Month) (コスト $ (GiB/月))	
平均ディスクサイズ (GiB)	
Number of VMs (VM の数)	
Monthly Cost	

ワークロード保護 (アカウント内スキャン)

標準デプロイメントの代替品として、ワークロードスキャンにアカウントからディスクのスナップショットを抽出し、それを によってホストされているマシンにマウントする必要があります Tenable One Cloud Exposure スキャンが実行されます Tenable はアカウント内のワークロードスキャンもサポートしており、スキャンが実行されます(専用アカウントを使用) 環境内にあるデータが環境から離れることはありません。

- 接続中に、Tenable がそのアプリケーション専用の KMS キーを生成します。このキーは、仮想マシンを作成し、スナップショットからボリュームをアタッチするために必要です。Tenable アウトポストではこのキーのみが使用され、カスタマーマネージドキーは共有されません。KMS キーへのアクセスはアプリケーションに制限され、スナップショットの作成に人間が介入することを防ぎます。スナップショットの作成は完全に自動化されているため、悪意のあるアクティビティのリスクが最小限に抑えられます。
- スナップショットの作成中に、Tenable が各スナップショットに以下のタグを自動的に適用します。
  - `ErmeticContext: WorkloadAnalysis`
  - `ErmeticNamespace: Prd<Region><Deployment>` eg `PrdUse2Dep2`、`PrdAps1Dep1`

Tenable の検出内容

Tenable は現在、以下のクラウドワークロードコンポーネントをスキャンできます。

コンポーネント	Tenable のスキャン対象
ワークロード	• 仮想マシン • 仮想マシンイメージ (AWS のみ) • コンテナイメージ • コンテナレジストリ • Kubernetes クラスタ
オペレーティングシステム	Linux、Windows
クラウドプロバイダー	AWS、Azure、GCP、OCI

- Tenable は、ディスクサイズが 600GiB までの仮想マシンをスキャンします。この値を変更したい場合は、サポートにお問い合わせください。
- Tenable は、コンテナの仮想マシンインスタンスもスキャンできます。
    - これらのインスタンスで見つかったコンテナは、関連するパッケージや脆弱性とともに、Tenable でのコンテナイメージとして表示されます。
    - Tenable がモニタリングするクラウドベースのコンテナレジストリ (Amazon ECR、Azure ACR など) でコンテナがホストされている場合、リポジトリへのリンクが表示されます。

  Tenable は現在、サーバーレスインフラ (例: AKS 仮想ノード、GKE Autopilot、OKE 仮想ノード、EKS Fargate) で実行されているコンテナはスキャンしません。
- **Azure**: Tenable が環境でリソースロックを検出した場合、影響を受ける仮想マシンのスキャンが一時的に無効になります。通常の動作を復元するには、ロックを解除してスキャンが自動的に再開されるようにすることをお勧めします。
- **OCI**: コンテナレジストリのスキャンはサポートされていません。

これらの各コンポーネントについて、Tenable は次を検出します。

- 一般情報 (OS のタイプやバージョンなど)
- インストールされているソフトウェア

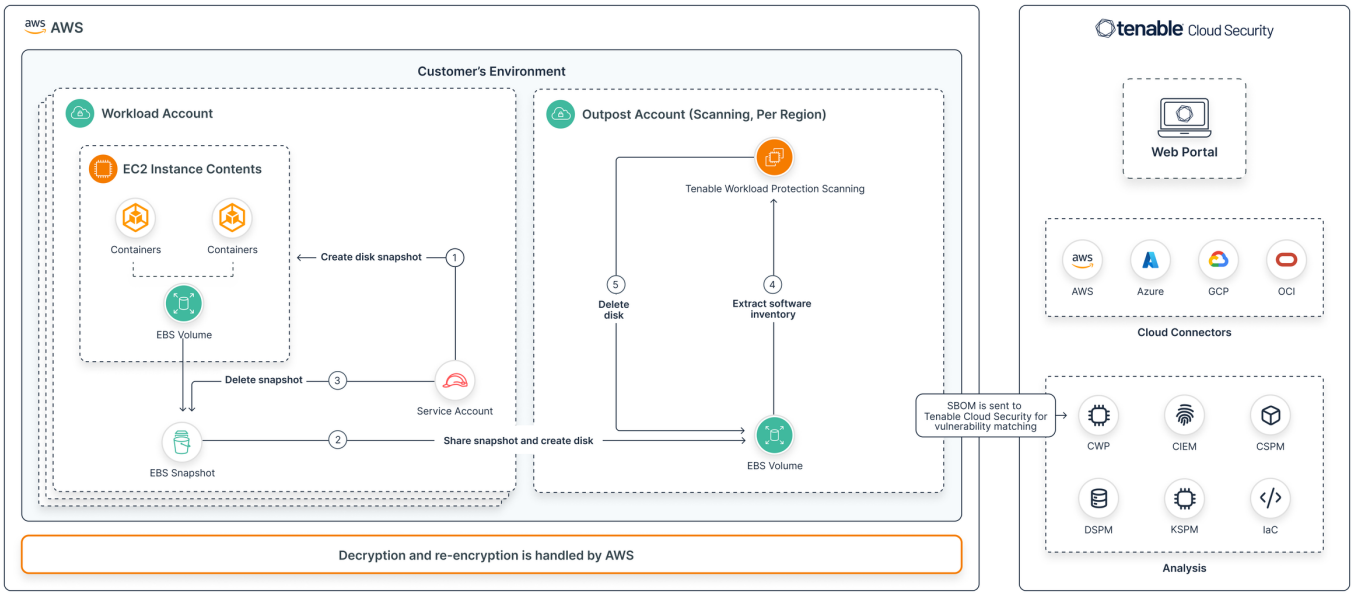
- ソフトウェアまたは OS カーネルは攻撃に対して脆弱か
- 脆弱である場合、どの脆弱性に当てはまるか
- OS が古いまたは EOL か (そのため、アップグレードする必要があるか)

これらの機能は継続的に更新されます。使用している特定のワークロードまたはコンポーネントがあり、確認したい場合は、サポートへの問い合わせ。

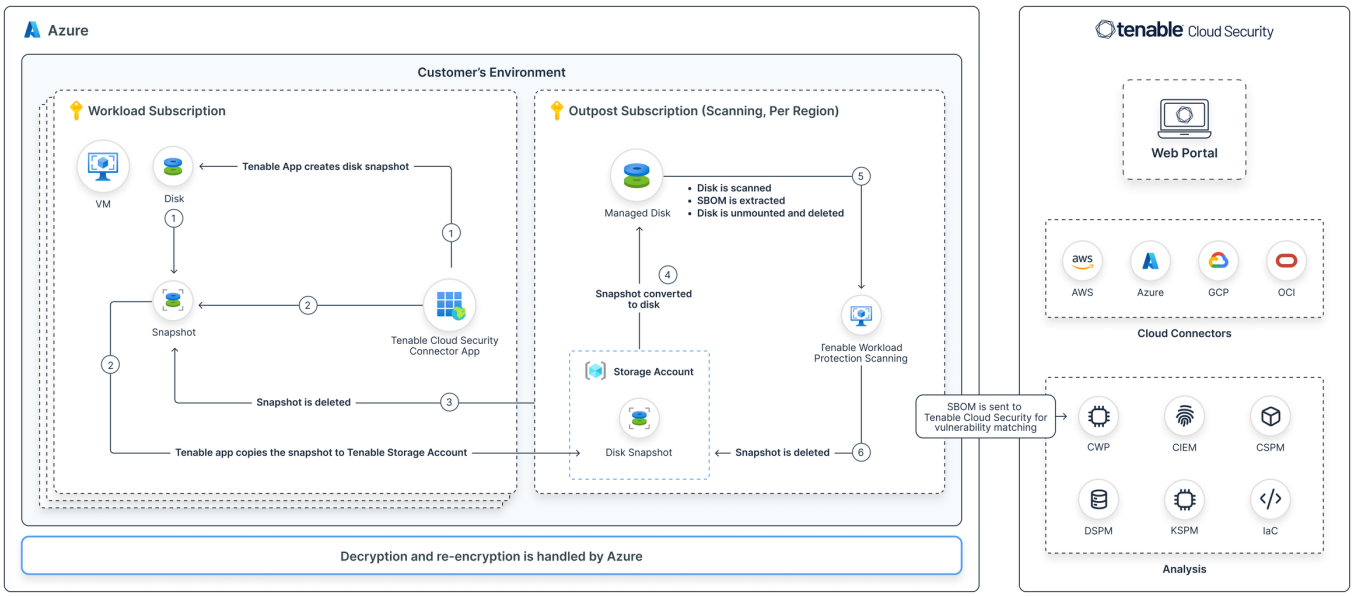
Tenable は、標準のワークロードスキャンと同じワークロードコンポーネントをアカウント内スキャンでスキャンします。詳細については、Tenable の検出内容参照してください。

AWS アーキテクチャのサンプル

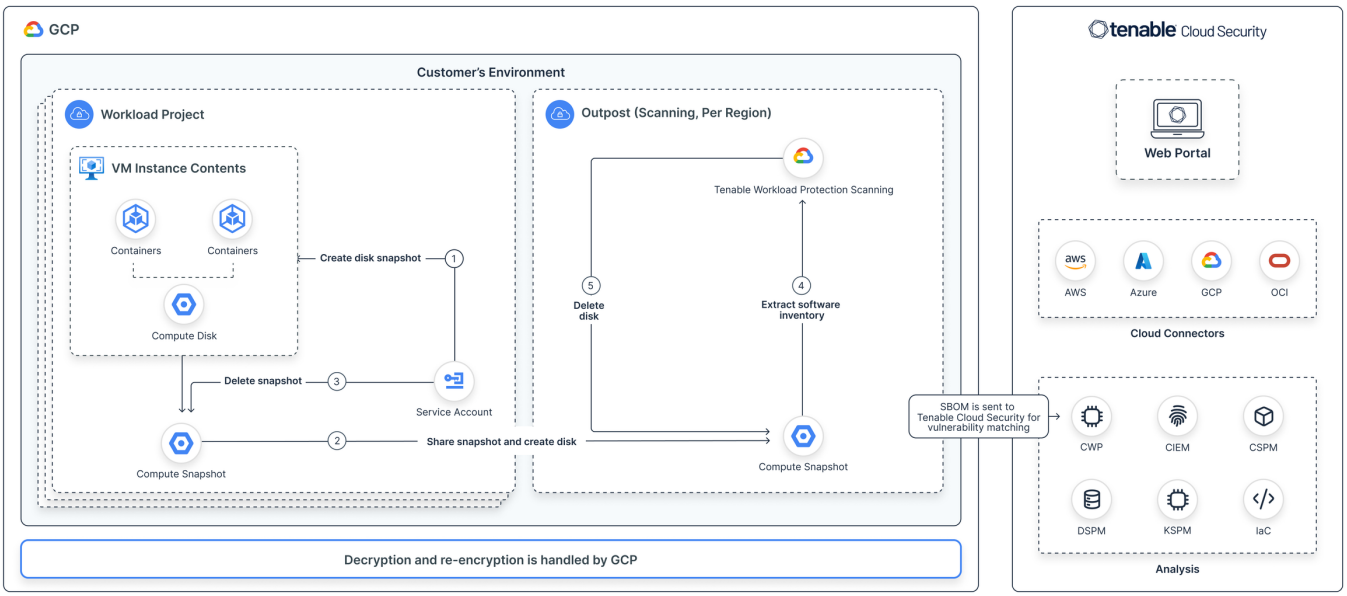
次の図では、AWS のアカウント内スキャンのワークフローを説明します。



サンプル Azure アーキテクチャ



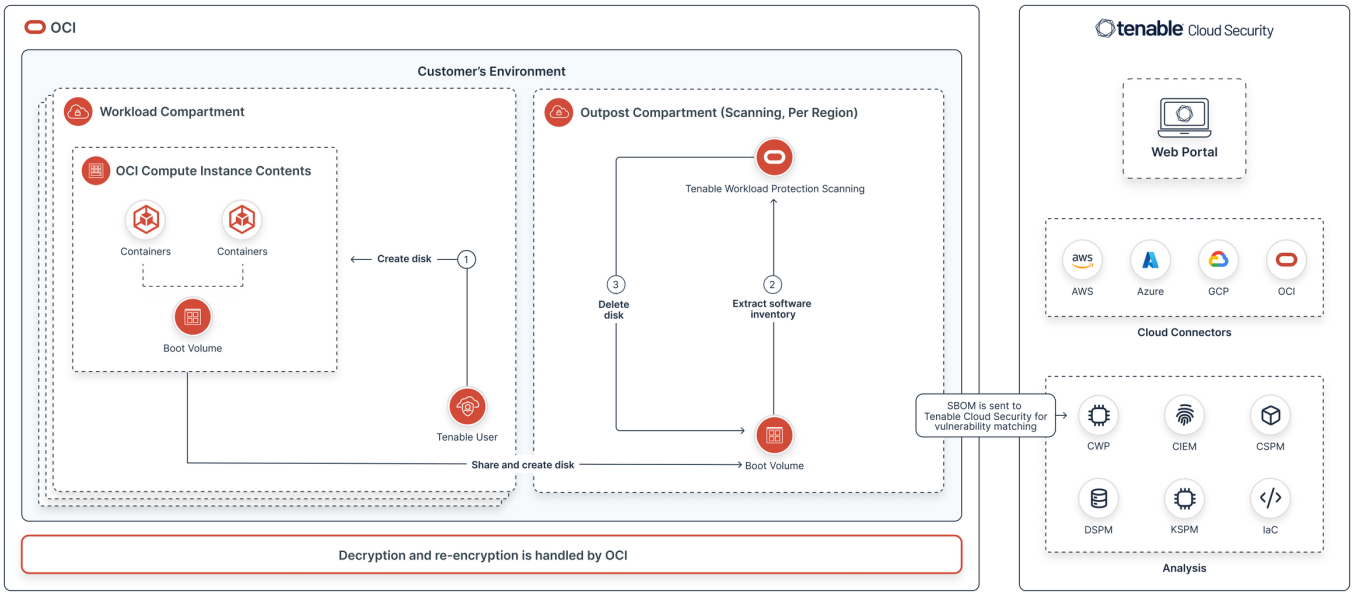
GCP のサンプルアーキテクチャ



サンプル OCI アーキテクチャ

注意: Tenable はOCI でスナップショットを作成しません。詳細については、Workload Protectionセクションの専用 OCI 図を参照してください。アカウント内デプロイメントの場合、必要なコンパートメントのアクセス許可により、特に、アプリケーションを実行するためにクラスターを作成できます (つまり、outpost アカウント)。

次の図は、OCI のアカウントスキャンワークフローを示しています。



よくある質問: 脆弱性管理

仮想マシンのスキャン

このセクションでは、仮想マシンのスキャンに関連する、よくある質問を紹介します。

停止されたVM の検出結果の深刻度

> 停止された仮想マシンの検出結果のステータスが「重大」になることがあるのはなぜですか?

回答: 仮想マシンの検出結果の深刻度は、30 日間連続してシャットダウンされた後にのみ軽減されます。この 30 日のしきい値を過ぎると、VM が停止しても、検出結果は「重大」などの元の深刻度レベル (重大) を保持します。

スキャンされた VM ボリューム

> Tenable がスキャンするのはどの仮想マシンボリュームですか?

回答: デフォルトでは、Tenable は仮想マシンに接続されているルートボリュームと、対象となるルート以外のすべてのボリュームをスキャンします。ボリュームは、サイズが 600 GB を超えない場合に対象となります。

> サポートされる最大ディスクサイズとボリューム数を教えてください。

次の制限が適用されます。

- 最大ディスクサイズ: 600 GB (個別のディスク)
- 仮想マシンあたりの最大ボリューム: ルートボリュームを含めて 4

> 非ルートボリュームスキャンロジックはどのように機能しますか。また、部分スキャンステータスは何を示しますか?

回答: Tenable では、非ルートボリュームに対してオール・オア・ナッシングのアプローチを使用します。仮想マシンごとに、次のいずれか Tenable します。

- ルートボリュームのみをスキャンするか、
- ルートボリュームを、対象となるすべての非ルートボリュームとともにスキャンします

Tenable は、ルートでないボリュームのサブセットはスキャンしません。

ディスク容量が 600 GB を超えるなど、ルートボリュームがスキャンされたものの 1 つ以上の非ルートボリュームがスキップされた場合、仮想マシンのスキャンステータスは「**部分的**」と表示されます。

> 特定の仮想マシンに接続されているディスクのスキャンステータスを表示するにはどうすればよいですか?

回答: 仮想マシンのプロファイルページに移動します。**[Overview]** タブで、**[Disks/Volumes]** テーブルを表示します。

質問: 非ルートボリュームのスキャンを無効にできますか?

回答: はい。**[Settings > Security > Workload]** に移動し、**[Extended Disk Scanning]** をオフに切り替えます。

> **注意:** 拡張ディスクスキャンはデフォルトで有効になっています。

> 非ルートボリュームスキャンはどのように請求されますか?

回答: 非ルートディスクは、**[ライセンス]** ページの **[データディスク]** カテゴリで請求されます。このカテゴリは、各クラウドプロバイダー (AWS、Azure、GCP、OCI) に固有です。

対応 OS バージョン

> Tenable スキャンするのはどの OS バージョンですか?

回答: Windows OS のバージョン」と Linux OS のバージョンを参照してください。

スキャン頻度

> Tenable はどのくらいの頻度で仮想マシンをスキャンしますか?

回答: Tenable は、前回のスキャンから 24 時間が経過するとすぐに各仮想マシンのスキャンを試みます。

スキャン時間

> 各スキャンにかかる時間はどれくらいですか?

回答: 平均スキャン時間はインスタンス 1 つあたり約 15 分です。この時間は、いくつかの要因が影響する可能性があります。

- **AWS スナップショットの制限**: AWS では、アカウントあたり最大 20 個のスナップショットを同時に許可します。顧客が開始したスナップショットへの干渉を防ぐために、Tenable ではスナップショット作成を 15 に制限しています。
- **スキャンされるインスタンスの数**: アカウントあたりのスキャンされるインスタンスが多いほど、各インスタンスのボリュームに独自のスナップショットが必要になるため、スナップショットの作成にかかる時間は

長くなります。これにより、特にAWS の同時スナップショットの制限に近づいている場合、遅延が発生する可能性があります。

- **インスタンスのボリュームサイズ**: ボリュームが大きいほど、スナップショットにかかる時間は長くなります。これがインスタンスの数やAWS の制限と組み合わさると、スナップショットの合計時間に大きく影響する可能性があります。

スキャン結果の高速化

ワークロードのスキャンステータスがスキャンの終了直後に更新されるようになり、脆弱性、マルウェア、ソフトウェアの検出結果に素早くアクセスできるようになりました。Tenable では、メイン エージェントレスのリソース同期からワークロードのスキャンステータスが切り離されたため、結果を確認するためにシステム全体が同期されるのを待つ必要がなくなりました。リソースプロファイルページでは、スキャンのステータス/日時と同期日時の両方を確認できます。

> 独立したワークロード保護スキャンの利点は何ですか?

これにより、システムは、データ同期の完了を待たずに、新たに検出された脆弱性などの技術的なデータをより迅速に表示できるようになります。

> これは、リスクの検出結果が作成またはクローズされるタイミングに影響しますか?

はい。根本的な脆弱性がスキャンデータですでに検出または解決されている場合であっても、検出結果はこれまでと同様に、オーケストレーションプロセスの完了後に作成またはクローズされます。

> これにより、一時的な不一致が発生する可能性がありますか?

潜在的に。関連する検出結果がリスクビューに反映されるのはデータ同期の完了後のため、その前にスキャンデータに脆弱性が表示されることがあります。

データ転送ポリシー質問: 自分のデータがアカウント外に出ることはありますか?

回答: Tenable は、ルートボリュームと対象となる非ルートボリュームの両方をスキャンします。スキャンは、ファイルシステムのメタデータ、ソフトウェアパッケージ、ファイル署名を読み取り、脆弱性とマルウェアを特定

します。Tenable では、スキャンされたボリュームからアプリケーションデータやユーザーコンテンツが抽出されることはありません。

ワークロードへの影響

> スキャンによって実行中のワークロードが何らかの悪影響を受けることはありますか?

回答: スキャンはエージェントレスであるため、実行中のワークロードに対して比較的透過的です。ボリュームのスナップショットを取得するために使用されるメカニズムは、可能な限り無停止です。スナップショットが作成されると、スナップショットは Tenable の環境と共有され (Azure の場合は環境にコピーされます)、ボリュームに変換された後、Tenable マシンによってスキャンされます。後者の手順は、ワークロードにまったく影響を与えません。

スナップショットの削除

> 私のアカウント内で Tenable によって作成されたスナップショットは削除されますか?

回答: はい。スナップショットはスキャンが完了するとすぐに削除され、どのスナップショットも存在する時間が最短になるようにスキャンプロセスが最適化されます。AWS では、誤って削除したスナップショットをごみ箱から復元するための保持ルールを作成した場合、追加コストが発生する可能性があります。価格設定の詳細については AWSドキュメントを参照してください。

月次スキャンコスト

> ワークロードスキャンに関連して、追加の月次コストは発生しますか?

回答: スナップショットスキャン費用計算ツールを参照してください。

プラグインと CVE の脆弱性深刻度メトリクスの選択方法

> プラグインと CVE に使用する脆弱性の深刻度メトリクスをどのように選択しますか?

深刻度メトリクスは、Tenable One Cloud Exposure コンソールで **[Workload** > **Vulnerabilities]** > **[Vulnerability Severity Metric] (ワークロード脆弱性の深刻度メトリクス)** に移動して選択できます。

Tenable は、選択されたメトリクスに基づいて、CVE とプラグイン両方の深刻度値を動的に更新します。

たとえば [VPR] を選択した場合、すべての CVE とプラグインは、VPR 深刻度がメインの深刻度レベルとして一貫して表示されます。

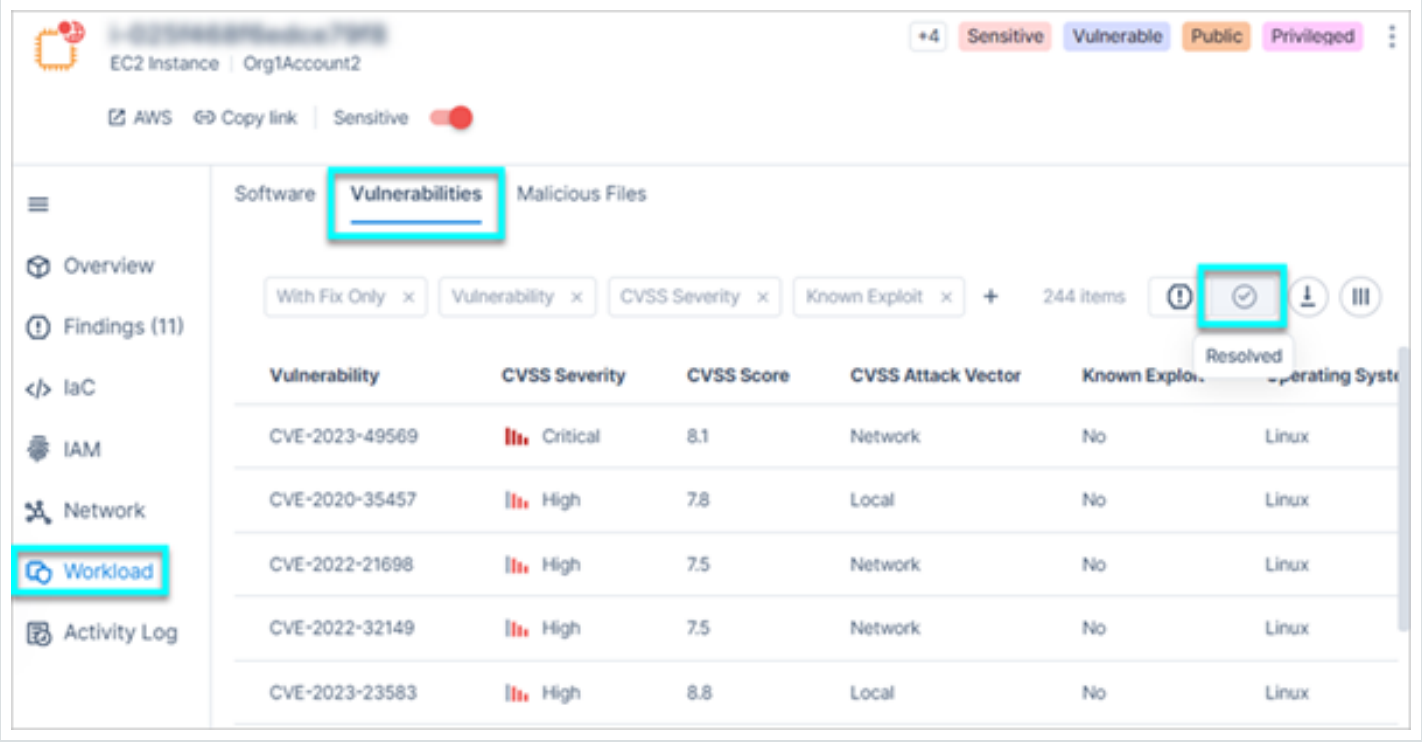
> **注意:** プラグインの深刻度は、そのプラグインに関連付けられている最も高い深刻度の CVE によって決まります。

詳細については、こちらの脆弱性の深刻度のメトリクスを参照してください。

解決済みの脆弱性情報

> 仮想マシンの解決済みの脆弱性に関する情報を確認できますか?

回答: はい。仮想マシンのプロファイルビュー内で、**[Workload > Vulnerabilities]** に移動し、**[Resolved] (解決済み)** フィルターをクリックします。この情報は 30 日間保持されます。



検出結果における OS サポート終了

> 検出結果を作成する際、オペレーティングシステムがサポート終了間近と見なされるのはいつですか?

回答: オペレーティングシステムは、正式なサポート終了日の30日前に、サポート終了間近と見なされます。

パッチ未適用のOS検出結果基準

> Tenableはいつ Windows ワークロードとLinux ワークロード上のパッチ未適用のオペレーティングシステムに関する検出結果を作成しますか?

パッチ未適用のオペレーティングシステムを識別する基準は、オペレーティングシステムによって異なります。

- **Windows ワークロード**: オペレーティングシステムの未処理のKB更新が1つ以上ある場合に、検出結果が作成されます。
- **Linux ワークロード。** Tenableは、ほとんどの既知のLinuxディストリビューションをマッピングして、どのパッケージがベースOSイメージの一部であるかを識別しています (Amazonベースイメージをガイドとして使用)。
  - **マップされた** Linuxディストリビューションの場合、深刻度が重大または高の脆弱性を持つ**OS関連パッケージが10個**以上ある場合に検出結果が作成されます。
  - **マッピングされていない** Linuxディストリビューションの場合、深刻度が重大または高の脆弱性を持つ**OS関連パッケージが20**個以上ある場合に検出結果が作成されます。

修正データ

> 修正データを取得するにはどうすればよいですか?

回答: 一般的な修正情報については、クラウドサイバーエクスポージャー脆弱性関連の検出結果のリスト API エンドポイントをクエリできます。プラグインの追加情報については、Tenable One get plugin details API エンドポイントをクエリすることもできます。

仮想マシンイメージスキャン (AMI)

このセクションでは、Amazon Machine Image (AMI) スキャンに関連するよくある質問への回答を紹介します。

AMI スキャンの範囲とカバレッジ

> Tenable はどのタイプの Amazon マシンイメージ (AMI) をスキャンしますか、また、カスタマーマネージドのマシンイメージとクラウドマネージドのマシンイメージのスキャン範囲はどう違うのですか?

Tenable は、クラウドマネージドとカスタマーマネージドの両方の AMI をスキャンしますが、スキャンの対象となる基準はイメージタイプによって異なります。

- **カスタマーマネージド (プライベート) AMI**: 使用状況に関係なく、すべてのイメージがスキャンされます。
- **クラウドマネージド (パブリック) AMI**: 現在 **使用中** (アクティブ) のイメージのみがスキャンされます。

コンテナイメージ CI/CD のスキャン

このセクションでは、コンテナイメージ CI/CD のスキャンに関連する、よくある質問を紹介します。

CI/CD スキャンモード

> CI/CD スキャンは非同期ですか、それともコンテナのビルドを停止させますか?

回答: スキャンは同期しますが、通常は非常に高速です。通常、1 分もかかりません。

CI/CD データ保持

> CI/CD スキャンのデータ保持ポリシーとは何ですか?

Tenable は、少なくとも 1 か月分のスキャン履歴を保持します。スキャンの量によっては最大 2 か月分のスキャン履歴を保持します。この期間を変更するには、サポートへの問い合わせ。

> **注意:** データ保持期間は、CI/CD リソースつまり、リポジトリの数の請求に影響を与えます。保持期間が長いほど、請求対象のリソースの数が増えます。

Docker-in-Docker (DinD)

> CI/CD パイプライン内のコンテナイメージのスキャンには Docker-in-Docker (DinD) が必要ですか?

いいえ、CI/CD パイプライン内のコンテナイメージのスキャンに通常、Docker-in-Docker (DinD) は必要ありません。DinD なしでこれらのスキャンを実行する柔軟な方法がいくつかあります。

- **コンテナランタイムソケットのマッピング**: コンテナランタイムソケット (Docker ソケットなど) をパイプラインコンテナにマッピングして、スキャナーがホストのコンテナデーモンと対話できるようにすることができます。
- **イメージをアーカイブとして渡す:** コンテナイメージを tar アーカイブまたは同様の形式でスキャナーに渡すことができます。
- **リモートからイメージをプルする**: スキャナーは、分析のためにリモートレジストリからコンテナイメージを直接プルできます。

コンテナイメージサイズの制限

> CI/CD イメージのサイズ制限はエージェントレススキャンと同じですか (たとえば 2GB)?

いいえ。CI/CD スキャンには画像サイズの制限はありません。

サードパーティの脆弱性の不一致

> ソースリポジトリに検出結果が含まれているにもかかわらず、コンテナイメージのコンソールに「脆弱性なし」と表示されるのはなぜですか?

スキャンが **7** 日以内に正常に更新されない場合、検出結果は自動的に削除され、古くなった情報が表示されないようになります。コンソールにデータがこの欠落すると、サードパーティ (外部) レジストリの認証情報の有効期限が切れた場合に発生し、自動スキャンが停止する可能性があります。認証情報を更新すると、スキャンプロセスが再起動し、脆弱性データがインベントリに復元されます。

データの不一致を引き起こす期限切れのレジストリ認証情報

> リポジトリの検出結果に脆弱性が表示されていないのに、コンテナイメージリポジトリに脆弱性の検出結果が表示されるのはなぜですか?

回答: この不一致は、認証情報の有効期限が切れ、Tenable とレジストリ間の接続が中断されたときに発生します。認証に失敗すると、次のようになります。

- **レジストリの無効化:** レジストリのステータスが [無効] に変わり、脆弱性分析プロセスが停止します。
- **スキャンの停止:** Tenable はそのリポジトリ内のイメージのスキャンを停止します。
- **データ保持:** コンテナイメージのスキャン結果が 7 日以内に更新されない場合、Tenable はデータベースから削除します。

> **注意:** リポジトリの検出結果では、このデータ削除によって脆弱性は表示されない可能性がありますが、個別のコンテナで以前に特定された脆弱性は、次のデータの同期と更新の頻度成功するまで表示されたままになります。

Windows イメージのサポート

> Tenable は、CI/CD パイプライン内の Windows ベースのコンテナイメージスキャンをサポートしていますか?

回答: はい。Tenable は、CI/CD パイプライン内の Windows ベースのコンテナイメージスキャンをサポートしています。

質問: 使用済み画像と未使用画像の技術的な違いは何ですか?

回答: Tenable は、アクティブな環境モニタリングに基づいてコンテナイメージの使用量を分類します。

- **使用済み**: Tenable は、この特定のイメージを参照する環境でアクティブに実行中またはデプロイされているライブランタイムワークロード (ポッド、タスク、サービスなど) を検出しました。
- **未使用**: イメージはコンテナレジストリに存在しますが、最新のインベントリスキャン中にイメージを参照しているアクティブなクラウドワークロード Tenable 見つかりませんでした。

> 使用量の計算にはどのようなデータソースが使用されますか?

回答: Tenable は、クラウドコネクタとセンサーを介して、レジストリ (AWS ECR、Azure ACR など) とランタイム環境 (Kubernetes、EKS、AKS AWS ECS) の両方からインベントリデータを引き出します。

質問: 画像に最終確認日のタイムスタンプはありますか?

回答: はい。`Last Seen` / `First Seen` タイムスタンプは追跡され、コンソールのリソースサイドパネルで表示したり、Tenable API 経由でエクスポートしたりできます。

質問: アクティブなイメージまたはデプロイ済みのイメージが未使用と表示されるのはなぜですか?

回答: 既知の環境制限により、画像に未使用のフラグが立てられる可能性があります。

- **一時的なワークロード**: 有効期間の短い `CronJobs`、サーバーレス関数、または Tenable の定期されたインベントリスキャンの間に完了して終了したバッチジョブ。
- **未接続の環境**: イメージは、クラウドコネクタ経由で Tenable に接続されていないステージングクラスター、リージョン、またはクラウドアカウントにデプロイされます。
- **デプロイ前の段階**: イメージは、インフラのコード化 (IaC) テンプレートまたは CI/CD パイプラインでビルドおよび参照されますが、まだライブ環境にデプロイされていません。

> Tenable は未使用のイメージを自動的に削除しますか?

いいえ。Tenable によってレジストリリソースが削除されることはありません。イメージのクリーンアップとライフサイクルの有効期限は、コンテナレジストリ内で設定する必要があります。

コンテナイメージレジストリのスキャン

このセクションでは、コンテナイメージレジストリスキャンに関連する、よくある質問を紹介します。

スキャン頻度

> Tenable はどのくらいの頻度でコンテナレジストリをスキャンしますか?

回答: Tenable は、前回のスキャンから 24 時間が経過するとすぐに各仮想マシンのスキャンを試みます。

Docker-in-Docker (DinD)

> コンテナレジストリのスキャンには Docker-in-Docker (DinD) が必要ですか?

いいえ、コンテナレジストリのスキャンには Docker-in-Docker (DinD) は必要ありません。エージェントレススキャンプロセスでは、コンテナイメージを直接取得し、分析のためにそのレイヤーアーカイブを読み取りま

す。

レジストリイメージの脆弱性更新頻度

> レジストリに存在し、最近更新されていない古いコンテナイメージについて、脆弱性リストはどのくらいの頻度で更新されますか?

スキャンプロセスでは、仮想マシン (VM) の下のイメージとリポジトリ内のイメージを区別します。

VM の下で見つかったコンテナイメージ: 最終更新時刻に関係なく、VM 下のすべての**コンテナイメージ**がスキャンされます。スキャンが完了すると、脆弱性リストは定期的に更新されます。

リポジトリの下にあるコンテナイメージが見つかりました。スキャンでは最近の使用状況に重点を置き、データの同期と更新の頻度ごとに**最新の 10 枚のイメージ**をターゲットにします。ただし、10 枚のイメージの制限に関係なく、現在使用されているイメージがスキャンに含まれます。

サポートされているコンテナイメージアーキテクチャ

> スキャンでサポートされているコンテナイメージアーキテクチャ (x86、x86-64、ARM など) は何ですか?

Tenable は、amd64 (x86-64) と arm64 アーキテクチャのスキャンをサポートしています。マルチアーキテクチャイメージに両方が含まれている場合は、最初に見つかったサポート対象のアーキテクチャのみがスキャンされます。

Amazon ECS の AWS Fargate サポート

> Tenable は AWS Fargate コンテナの脆弱性をどのように特定しますか?

回答: Tenable は、コンテナイメージレジストリ (Amazon ECR など) 内のイメージをスキャンすることで、AWS Fargate コンテナの脆弱性を特定します。次に、Tenable はこれらのスキャン結果を、Fargate タスクをデプロイするために使用される Amazon ECS タスク定義と関連付けて、本番環境のリスクを特定します。

> ECS サービス (Fargate 上) が含まれるのはなぜですか?

回答: AWS Fargate で実行されているリソースは、イメージスキャンを超えたセキュリティの可視性を提供するため Tenable ライセンス数を消費します。イメージがレジストリレベルでスキャンされる場合でも、Tenable はライブサービスを継続的に監視し、次について確認できます。

- **設定ミス**: セキュリティのベストプラクティスの自動チェック
- アイデンティティ (IAM): Fargate タスクに割り当てられたアクセス許可の分析。
- **ネットワークアクティビティ**: ネットワーク到達可能性の監視。

Windows イメージのサポート

> Tenable は、コンテナレジストリ内の Windows ベースのコンテナイメージスキャンをサポートしていますか?

回答: はい。Tenable は、コンテナレジストリ内の Windows ベースのコンテナイメージスキャンをサポートしています。

コンテナイメージアカウントの割り当て

> アカウントが所有しているコンテナイメージと使用しているコンテナイメージを見分けるにはどうすればよいですか?

2 つのフィルターは使い分けて使用します。

- **アカウントが何を使用しているかを確認するには アカウント** に対してグローバル範囲フィルター (ページ上部にある **[組織]** ドロップダウン) を設定します。これにより、他のアカウントが所有する共有イメージも含めて、アカウントで実行するすべてのコンテナイメージの混合ビューが返されます。
- **アカウントが所有するイメージのみを表示する方法** [脆弱性]、[ソフトウェア]、[悪意のあるファイル]、または [コンテナイメージ] ページの表内に **[アカウント]** フィルターを適用します。

このデータは表からエクスポートできます。スケジュールされた脆弱性レポートでは、範囲フィルターは同じように機能します。範囲を選択すると、イメージが別の範囲に属している場合でも、コンテナイメージを使用するその範囲内のワークロードの脆弱性がレポートから返されます。

> 自分のアカウントが所有するコンテナイメージのみの脆弱性をクエリするにはどうすればよいですか?

探索 > Explorer で、次のクエリを作成します。

- **検出:** 脆弱性インスタンス
- **各部の説明**
  - **解決ステータス**は**オープン**です
  - 以下 **を満たすリソース** に関連付けられます。
    - のタイプ コンテナ **イメージ**
    - コンテナ**リポジトリ**に含まれている

> どのコンテナイメージが Container Registries アカウントに移動しますか?

クラウド サイバーエクスポージャーが知られているレジストリにないコンテナイメージのみ。これには、クラウドベースのレジストリ (Amazon ECR や Azure ACR など) を通じて同期されず、コンテナレジストリ統合 (JFrog や汎用 Docker レジストリなど) を通じて同期されないイメージが含まれます。同期されたレジストリのイメージは、既存のアカウントに関連付けられたままになります。

> スケジュールされた脆弱性レポートでは、コンテナイメージの範囲ごとにどのような情報が返されますか?

選択した範囲で使用されたコンテナイメージのすべての脆弱性がレポートに返されます。たとえば、範囲フィルター Org1Account1 の場合、レポートには、Org1Account1 が所有するコンテナイメージと、他のアカウントが所有するが Org1Account1 で使用されているコンテナイメージが含まれます。

[イメージプレースホルダー: Org1Account1 スコープでスケジュールされている脆弱性レポートの例]

> この変更は GraphQL/Entities API に影響しますか?

返されるコンテナイメージの数は変わりません。同期されていないイメージまたはパブリックイメージに関連付けられているアカウントは、そのようなイメージが **コンテナレジストリ** アカウントに統合されるため、変更される場合があります。統合でコンテナイメージのアカウントレベルのフィールドが読み取られる場合は、その変更がワークフローに影響するかどうかを確認します。アカウントごとの可視性は、各イメージを実行するワークロードのアカウントから導き出されます。

オンプレミス Kubernetes ワークロードスキャン

このセクションでは、オンプレミスの Kubernetes ワークロード スキャンに関連する、よくある質問を紹介します。

センサーのアクセス許可

> センサーを実行するにはどのようなアクセス許可が必要ですか?

回答: センサーには、特権アクセス許可を持つ ClusterRole が必要です。これらのアクセス許可により、センサーは必要なクラスタリソースにアクセスし、Kubernetes 環境全体から包括的なセキュリティデータを収集できるようになります。

センサースキャン頻度

> Tenable はどのくらいの頻度でオンプレミスKubernetesワークロードをスキャンして脆弱性を検出しますか?

Tenable は、1 時間に 1 回、すべてのワークロードのスキャンを試みます。お使いの環境で次にデータの同期と更新の頻度 ときに、コンソールがスキャン結果データで更新されます。

エフェメラルディスクを使用した AKS クラスタのスキャン

> センサーはエフェメラルディスクを備えた AKS クラスタをスキャンできますか?

はい。エージェントベースの (センサー) スキャンはこのユースケースをサポートします。エフェメラルディスクは、エージェントレススキャンプロセスに必要なスナップショットをサポートしていません。

CoreOS サポート

> Tenable は CoreOS を実行しているワークロードをスキャンしますか?

回答: はい、Tenable は、OpenShift Container Platform クラスタにデプロイメントするために設計されたオペレーティングシステム Red Hat Enterprise Linux CoreOS (RHCOS) を実行しているワークロードをス

キャンします。

ディスクストレージ要件

> `/var/lib/tenable` ディレクトリのディスクストレージ要件は何ですか?

回答: Tenable では、最大サイズの **1.5 倍** のディスクストレージを割り当てることをお勧めします。

ロジックとトリガーのスキャン

> センサーはどのようにスキャンを実行し、どのようにトリガーされるのですか?

センサーはコンテナレベルでスキャンを開始します。このプロセスは、コンテナイメージと仮想マシン (VM) を識別します。これには、VM 内に存在するコンテナイメージも含まれます。次に、センサーはファイルシステムを分析して、脆弱性検出用のソフトウェア部品表 (SBOM) を生成します。

スキャン結果の可視性

センサーは新しいコンテナを即座にスキャンしますか?

スキャン結果の可視性

回答: センサーは、通常の 1 時間から 2 時間のサイクルの一部として、新しいコンテナを自動的にスキャンします。オーケストレーションサイクルにより、更新された検出結果が 4 時間ごとにコンソールに表示されます。

アカウント内ワークロードスキャン

このセクションでは、ワークロード保護 (アカウント内スキャン)に関連する、よくある質問を紹介します。

アカウント内オンボーディング: カスタマーマネージドキー (CMK)

> アカウント内スキャンに独自のマネージドキー (CMK) を使用できますか?

回答: はい。Tenable は、次のシナリオで CMK をサポートしています。

- イメージスナップショットの再暗号化
- アウトポストノードの暗号化 (スキャナーサービス)

アカウント内オンボーディング: 顧客管理対象イメージ

> アカウント内スキャンに独自のネットワークアーキテクチャを使用できますか?

回答: はい。クラウドサイバーエクスポージャーは、次のシナリオで、Amazon Web Services (AWS) および Oracle Cloud Infrastructure (OCI) のカスタマーマネージドイメージをサポートしています。

- Kubernetes ノードの基本イメージとして使用するために選択されたカスタムイメージ

サポートされているシナリオ、必要なアクセス許可、オンボーディングの詳細については、サポートへの問い合わせ。をご覧ください。

アカウント内オンボーディング: 顧客管理ネットワーク

> アカウント内スキャンに独自のネットワークアーキテクチャ (VPC) を使用できますか?

回答: はい。Tenable は、次のシナリオで AWS、GCP、OCI のカスタマーマネージドネットワークをサポートしています。

- **カスタム・ネットワーク・アーキテクチャ**: 特定の仮想プライベート・クラウド (VPC)または仮想クラウド・ネットワーク(VCN)設定を使用するようにアカウント内スキャンを構成できます。これにより、すべてのスキャントラフィックが、組織の内部ネットワークおよびセキュリティポリシーに準拠していることが保証されます。

サポートされているシナリオ、必要なアクセス許可、オンボーディングの詳細については、サポートへの問い合わせ。をご覧ください。

地域リソースプロビジョニング

> クラウドサイバーエクスポージャーではどのようにして複数のデータセンターに複数のクラスタをデプロイしますか?

回答: Tenable は、仮想マシンがある各リージョンに必要なコンピューティングリソースをプロビジョニングします。詳細については、リージョンごとにプロビジョニングされるリソースとサンプル AWS アーキテクチャを参照してください。

オンプレミスと AWS Outpost の互換性

> AWS アウトポストを使用して、これをオンプレミスの仮想化データセンターにデプロイできますか?

回答: いいえ。アウトポストは、クラウドホスト仮想マシンのスキャンにのみ使用できます。

ネットワーク

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

このセクションでは、の Tenable One Cloud Exposureネットワーク漏洩機能の概念概要を説明します。

- ネットワークエクスポージャーの概要については、ネットワークのエクスポージャー参照してください。
- スキャン設定を構成するには、ネットワークスキャナー参照してください。
- よくある質問については、FAQ: ネットワーク を参照してください。

クラウドサイバーエクスポージャー ネットワーク機能を使用して、クラウド環境の潜在的なインターネットエクスポージャーを継続的に特定、評価、検証、報告します。設定分析とアクティブスキャンを組み合わせることで、公開されているように見えるリソースと実際にはインターネットから到達可能なリソースを区別できます。これにより誤検出を減らすことができ、セキュリティチームは外部からの真のリスクを明確に把握できるようになります。

クラウドサイバーエクスポージャー のネットワークサイバーエクスポージャー分析は、次のコンポーネントで構成されています。

- **ネットワーク評価**: クラウドリソース構成の静的分析により、インターネットに接続していると思われるリソースにフラグを立てます。
- **ネットワークスキャナー**: 実際の到達可能性を確認するために、フラグが立てられたリソースへの直接接続を試みるアクティブ検証。

- **ネットワークエンドポイント**: ライブ接続が成功した場合にのみ作成される、確認されたエクスポージャーのレコード。

企業では、複数のプロバイダーで数千個のクラウドリソースを運用しており、複雑なネットワークルールが頻繁に変更されます。小さな設定ミス (過剰な許可のセキュリティグループやファイヤーウォールルールなど) によって、リソースが意図せずパブリックインターネットに漏洩する可能性があります。クラウドサイバーエクスポージャー のネットワーク機能は、これらのサイバーエクスポージャーを早期に検出し、アタックサーフェスを減らし、侵害を防ぐのに役立ちます。

詳細

- ネットワークのエクスポージャー
- ネットワークエンドポイント
- ネットワークスキャナー
- よくある質問: Network Exposure
- 共通サービスポート

ネットワークのエクスポージャー

このセクションでは、Tenable One Cloud Exposure のネットワークエクスポージャー機能の詳細な概要を説明します。

- スキャン設定を構成するには、「ネットワークスキャナーを参照してください。
- [ネットワークエンドポイント] ページで実行できることについては、「ネットワークエンドポイント」を参照してください。
- よくある質問については、「FAQ: ネットワークを参照してください。

クラウドサイバーエクスポージャー のネットワークエクスポージャーは、検証済みの到達可能性モデルを通じて評価されます。モデルはリソースへのアクセスを試み、成功した場合、リソースはパブリックとして分類されます。

このモデルには、次のコンポーネントが統合されています。

- ネットワーク評価: クラウド構成の静的分析により、インターネットに接続している可能性のあるリソースを特定します。
- ネットワークスキャナー: アクティブな接続試行を実行してエクスポージャーを検証する権威コンポーネント。
- ネットワークエンドポイント: 確認された露出された各リソースの、特定のホストとポートの組み合わせのレコード。

これらのコンポーネントを組み合わせることで、誤検出が減り、実際の外部リスクの明確な全体像が得られます。

ネットワーク評価

ネットワーク評価は、潜在的なエクスポージャーを評価するためにクラウドサイバーエクスポージャー が使用する初期のコンポーネントです。スキャン方法中に収集されたクラウドリソース設定を分析し、リソースがインターネットに接続しているように見えるかどうかを判断します。

ネットワーク評価の役割は、リソースタイプによって異なります。

- **直接リソース:** EC2 インスタンスや RDS データベースなどのリソースの場合、ネットワーク評価は検出メカニズムとして機能し、ネットワークスキャナーで検証する潜在的なエクスポージャーを特定します。これらのリソースについては、スキャンが成功した後にのみパブリックステータスが確認されます。サポートされているリソースのリストを参照してください。
- **間接リソース**: ロードバランサーまたは API ゲートウェイの背後にあるリソースの場合、リソースがパブリックかどうかを判断する主要な方法は依然としてネットワーク評価です。

ネットワーク評価は構成データに依存するため、各サイクルで自動的に実行され、追加の設定は必要ありません。ただし、この方法では、WAF、サードパーティのファイアウォール、マネージドプロキシなどの外部セキュリティレイヤーは考慮できません。

たとえば、EC2 インスタンスは、パブリック IP と、`0.0.0.0/0` からのポート 22 への着信トラフィックを許可するセキュリティグループを使用して起動されます。次のオーケストレーションサイクル中に、クラウドサイバーエクスポージャー はこの設定を取得し、インスタンスに潜在的に公開されているものとしてフラグを立てます。

インスタンスが接続をブロックするファイアウォールまたはプロキシによって保護されている場合、ネットワークスキャナー はハンドシェイクを確立できません。この場合、インスタンスは非パブリックとしてマークされます。スキャナーが到達可能性を正常に検証した場合にのみ、リソースはパブリックとして分類されます。

ネットワーク評価の範囲と制限

ネットワーク評価は、すべての統合クラウドプロバイダーをサポートしています。インターネットに接続している可能性のある次のようなリソースの範囲を評価します。

- パブリック IP を持つ仮想マシンとインスタンス
- ロードバランサーとゲートウェイ。
- クラウドワークロードへのアクセスを制御するその他のネットワークコンポーネント。

制限事項:

- **IPv4のサポート**: IPv4のみがサポートされています。IPv6 は現在サポートされていません。
- **コンテナネットワーキング**: Kubernetes サービスとコンテナネットワーキングオブジェクトは現在、評価に含まれていません。
- **サードパーティのコントロール**: ネットワーク評価では、サードパーティのファイアウォールまたは管理されたプロキシによって制御されているアクセスを検出できません。これらの問題は、到達可能性の検証を通じて、ネットワークスキャナー によって対処されます。

ネットワークスキャナー

ネットワークスキャナーは、ネットワークスキャナー、ネットワークエクスポージャー分析の信頼できるコンポーネントになります。ネットワーク評価、インターネットに接続されている可能性があるリソースにフラグが立てられた後、ネットワークスキャナーはインターネットからの直接接続を試行することで、それらのリソースを検証します。

スキャナーは 2 つのレイヤーで動作します。

- **トランスポート層**: TCP 接続を試みて、リソースがインターネットから到達可能であることを確認します。サポートされているリソース。

- **アプリケーション層**: 確認された HTTP エンドポイントと HTTPS エンドポイントでサポートされているコンピューティングリソースの場合、スキャナーは HTTP GET リクエストを送信し、HTTP ステータスコード、SSL/TLS プロトコルバージョン、ランディングページのスクリーンショット、HTML レスポンスなどのレスポンスをキャプチャします。サポートされているリソース。

IP アドレスとポートを持つ直接リソースのみがスキャンされます。ロードバランサー (ALB、NLB) や API ゲートウェイの背後にあるリソースなどの間接リソースは現在サポートされておらず、エクスポージャーステータスについてはネットワーク評価に依存しています。

たとえば EC2 インスタンスには、そのセキュリティグループがポート 443 への `0.0.0.0/0` からの着信トラフィックを許可するため、フラグが立てられます。ネットワークスキャナーがポート 443 への接続を試みます。成功した場合、クラウドサイバーエクスポージャー はネットワークエンドポイントを作成し、リソースをパブリックとして分類します。EC2 インスタンスはアプリケーションレイヤーのスキャンもサポートされているため、スキャナーは GET リクエストを送信し、HTTP ステータス、SSL/TLS バージョン、ランディングページのスクリーンショット、HTML レスポンスを記録します。

検出結果の深刻度への影響

ネットワークスキャナーは、検出結果の深刻度に直接影響します。

たとえば、EC2 インスタンスなどのパブリックリソースはパブリックとして分類されました。次の表は、深刻度がどのように影響を受けるかを示しています。

深刻度	条件
重大	なし
高	ネットワークエンドポイントを含む + 脆弱性 深刻度が**重大** + 検出結果の深刻度が**高**
中	**次のうちのいずれかです。** - ネットワークエンドポイントを含む + 脆弱性 深刻度 **が重大** または - ネットワークエンドポイントを含む + アクセス許可の深刻度が **高**
低	ネットワーク評価によりインターネットに接続していると判断される

サポートされているリソース

次の直接リソースタイプは、ネットワークスキャナーのトランスポート層やアプリケーション層のスキャンをサポートします。

プロバイダー	リソース名	トランスポート層スキャン	アプリケーション層スキャン
AWS	DocumentDB インスタンス	✓	
	EC2 インスタンス	✓	✓
	ECS サービス	✓	✓
	Elastic Beanstalk 環境	✓	
	Classic Load Balancer	✓	✓
	Network Load Balancer	✓	✓
	Application Load Balancer	✓	✓
	Neptune インスタンス	✓	
	RDS インスタンス	✓	
	Redshift クラスタ	✓	
Azure	Application Gateway	✓	
	Network Load Balancer	✓	✓
	仮想マシン	✓	✓
	仮想マシンスケールセットインスタンス	✓	✓

プロバイダー	リソース名	トランスポート層スキャン	アプリケーション層スキャン
	App Service		✓
GCP	ロードバランサー	✓	
	VM インスタンス	✓	✓
	Cloud SQL インスタンス	✓	
	Cloud Run サービス		✓
	アプリエンジン		✓
OCI	Compute インスタンス	✓	✓
	Network Load Balancer	✓	✓
	ロードバランシングロードバランサー	✓	✓

注意: ロードバランサー (ALB、NLB、Application Gateway) や API ゲートウェイの背後にあるものを含む間接リソースは、ネットワークスキャナーでサポートされていません。これらのリソースは、ネットワーク評価 (静的設定分析) を使用して、パブリックかどうかを判断します。

ネットワークスキャナーは、次のパブリック IP アドレスからトラフィックを送信します。

IP アドレス
3.147.184.122
3.19.220.21
15.205.53.205 (米国ガバメントクラウド)
3.30.64.189 (米国ガバメントクラウド)

ネットワークエンドポイント

ネットワークエンドポイントは、ネットワーク評価によってフラグが立てられたリソースがインターネットから到達可能であることをネットワークネットワークスキャナーが確認したときに作成されます。

各ネットワークエンドポイントは、宛先ホスト (IP アドレスまたは DNS 名) とポートの一意の組み合わせを表します。サポートされているコンピューティングリソースの場合、確認済みの HTTP エンドポイントと HTTPS エンドポイントには、スキャナーによってキャプチャされたアプリケーション層データも含まれます。これらのエンドポイントは、直接リソースをパブリックに分類するために検証済み到達可能性モデルに必要な決定論的証拠を提供します。

次の点に注意してください。

- **直接リソースのみ**: エンドポイントは、IP アドレスとポートを持つ直接リソースに対してのみ作成されます。
- **分類トリガー**: サポートされている直接リソースの場合、ネットワークエンドポイントの存在は、リソースがパブリックとして分類される唯一の方法です。
- **最近の結果**: ネットワークエンドポイントには、最新のスキャン結果のみが表示されます。エンドポイントは現在、履歴的に保存されません。
- **検出結果の影響**: エンドポイントはスキャン結果であり、検出結果そのものではありませんが、ネットワークベースの検出結果の深刻度が影響を受けるかどうかを決定します。

ネットワークエンドポイントの作成方法

ネットワーク評価、インターネットに接続されている可能性があるリソースにフラグが立てられると、ネットワークスキャナーは直接接続を試みます。

接続の試行が成功した場合、クラウドサイバーエクスポージャーは特定のホストとポートのネットワークエンドポイントを作成します。この確認された到達可能性により、リソースのステータスは自動的にパブリックに更新され、関連する検出結果の深刻度が調整されます。

HTTP エンドポイントと HTTPS エンドポイントでサポートされているコンピューティングリソースの場合、スキャナーは GET リクエストも送信し、アプリケーション層のレスポンスデータを記録します。

たとえば、EC2 インスタンスには、そのセキュリティグループが `0.0.0.0/0` からのポート 443 への着信トラフィックを許可しているため、フラグが立てられることがあります。スキャナーが正常に接続すると、クラウドサイバーエクスポージャーレコードがネットワークエンドポイントとして `<instance-IP>:443` されます。これにより、リソースが公開されており、アクティブに到達可能として設定されていることが確認されます。これにより、パブリック分類になります。

> **注意:** 特定のリソースがスキャンされたり、エンドポイントとして表示されたりしないようにしたい場合は、[除外] で管理できます。

ポートスキャンロジック

ネットワークスキャナーは 共通サービスポート のリストでリソースをテストします。

- リソースのオープンポートの合計数 (既知とその他) が既知のポートの数以下の場合、スキャナーはそれらすべてをテストします。
- 開いているポートの合計数が既知のポートの数を超えると、スキャナーは既知のポートのみをテストします。

このアプローチにより、過剰なスキャンオーバーヘッドなしで、広い範囲をカバーできます。

共通サービスポート

アプリケーションプロトコル	ポート	プロトコルタイプ
AzureSqlManagedInstance	3342	Tcp
Cassandra	7000	Tcp
CassandraSsl	7001	Tcp
DNS	53	Tcp
Elasticsearch	9200	Tcp
FTP	21	Tcp

アプリケーションプロトコル	ポート	プロトコルタイプ
ジュネーブ	6081	Tcp
Grafana	3000	Tcp
HTTPアドレス	• 80 • 591 • 7990 • 8000 • 8001 • 8008 • 8080 • 8081 • 8082 • 8088 • 8800 • 8808 • 8880 • 8881 • 8882 • 8888 • 9000 • 9090 • 10000	Tcp
https	• 443 • 1443	Tcp

アプリケーションプロトコル	ポート	プロトコルタイプ
	• 2443 • 3443 • 4443 • 5443 • 6443 • 7443 • 8443 • 11434	
Imap	143	Tcp
Imaps	993	Tcp
IpSecKeyExchange	500	Tcp
Istio	• 15006 • 15010 • 15012 • 15021	Tcp
Kubernetes	• 10250 • 10255 • 6443	Tcp
LDAP	389	Tcp
Memcached	11211	Tcp
MongoDb	27017	Tcp

アプリケーションプロトコル	ポート	プロトコルタイプ
MSSQL	1433	Tcp
MysqlAurora	3306	Tcp
NFS	2049	Tcp
OracleRDS	1521	Tcp
ポップ3	110	Tcp
Pop3S	995	Tcp
PostgreSQL	5432	Tcp
RDP	3389	Tcp
Redis	6379	Tcp
Redshift	5439	Tcp
SFTP	990	Tcp
SMB	445	Tcp
SMTP	25	Tcp
SMTPS	465	Tcp
SSH	22	Tcp
Telnet	23	Tcp
UPnP	5000	Tcp
VNC	5900	Tcp

アプリケーションプロトコル	ポート	プロトコルタイプ
WinrmHttp	5985	Tcp
WinrmHttps	5986	Tcp

FAQ: ネットワーク

このセクションでは、ネットワークのエクスポージャーに関するよくある質問を紹介します。

- ネットワークエクスポージャーの概要については、「ネットワークのエクスポージャー」を参照してください。
- スキャン設定を構成するには、「ネットワークスキャナー」を参照してください。

ネットワークスキャナーの有効化

> ネットワークスキャナーを有効にするとどうなりますか?

スキャナーを有効にすると、検証済みの到達可能性モデルに Tenable One Cloud Exposure されます。スキャナーは、ネットワーク評価でフラグが立てられた直接リソースへの接続を試みます。接続に成功すると、リソースはパブリックとして分類され ネットワークエンドポイント が作成されます。

> スキャナーを有効にすると、既存の検出結果は変わりますか?

はい。有効にすると、スキャナーは直接リソースの管理ソースになります。スキャナーが到達可能性を検証できない場合、リソースをパブリックにする必要がある検出結果 (「EC2 インスタンスはインターネットに公開されている」など) の深刻度が影響を受けます。

> ネットワークスキャナーを有効にした後、追加の設定が必要ですか?

いいえ。有効にすると、スキャナーは約 24 時間ごとに実行され、手動操作は必要ありません。

ネットワーク評価とネットワークスキャナー

ネットワーク評価はネットワークスキャナーとどう違うのですか?

ネットワーク評価は、クラウド構成の静的分析を実行し、インターネットに接続しているように見えるリソースを特定する検出ツールです。ネットワークスキャナーは、ネットワークスキャナー、権威バリデーターです。直接リソースの場合、スキャナーの結果は最終的なものになります。リソースは、スキャナーがインターネットからの直接パスを確認した場合にのみパブリックとして分類されます。

ネットワーク評価でフラグが立てられたリソースがパブリックとして表示されないのはなぜですか?

検証済み到達可能性モデルでは、ネットワークスキャナーが接続を正常に確立した場合にのみ、直接リソースはパブリックとして分類されます。スキャナーが接続できない場合 (たとえば、ファイヤーウォール、WAF、プロキシが試行をブロックしているなどの理由で)、リソースは非パブリックとしてマークされ、誤検出をなくします。

ネットワークエンドポイント

ネットワークエンドポイントは何を表しますか?

各ネットワークエンドポイントは、インターネットから到達可能な確認された一意のホストとポートの組み合わせです。エンドポイントはライブ接続が成功した場合にのみ作成されるため、リソースをパブリックに分類し、リスク深刻度の昇格をトリガーするために検証済み到達可能性モデルに必要な決定論的証明を提供します。

リソースのエンドポイントが表示されないのはなぜですか?

いくつかの理由が考えられます。

- ネットワークスキャナー。
- ネットワーク評価中にリソースが漏えいする可能性があることは見つかりませんでした。
- 間接リソース: リソースは間接リソースです (ロードバランサーや API ゲートウェイなど)。現在、スキャナーは、IP とポートが割り当てられているダイレクトリソースのみをサポートします。

- リソースタイプは、検証済みの到達可能性ではサポートされていません。ネットワークのエクスポージャーを参照してください。
- リソースは、スキャナーの接続試行をブロックする外部セキュリティコントロール (WAF やファイヤーウォールなど) によって保護されています。

> [ネットワークエンドポイント] ページに最近の結果しか表示されないのはなぜですか?

このページには、直近のスキャンサイクルで確認されたエンドポイントが表示されます。以前に表示されていたエンドポイントが表示されない場合は、サイバーエクスポージャーが解決されたか、到達できなくなっていることを意味します。クラウドサイバーエクスポージャーは、アクティブに公開されなくなったエンドポイントの履歴ログを保持しません。

ポートとプロトコル

> ネットワークスキャナーはどのポートをテストしますか?

スキャナーは、定義された共通サービスポート。リソースにこのリスト外の他のオープンポートがある場合、オープンポートの合計数が共通サービスポートの数を超えない限り、それらのポートもスキャンされます。合計数がこれより大きい場合は、共通サービスポートのみがスキャンされます。

以下に例を示します。

- 10 個の共通ポートと5 個の非一般ポートを公開しているリソース: 15 個すべてがスキャンされます。
- 50 個の共通ポートと40 個の一般的でないポートを公開しているリソース: 50 個の一般的ポートが、いくつかの一般的でないポートとともにスキャンされます。

> ネットワークスキャナーは UDP をサポートしていますか?

いいえ。現在、スキャナーは TCP ポートのみをテストします。

サポートされているリソースとオリジン IP

ネットワークスキャナーはどのクラウドリソースをサポートしていますか?

スキャナーは、仮想マシンやデータベースインスタンスなどの直接的なリソースを対象とします。クラウドプロバイダーごとの内訳については、ネットワークのエクスポージャーを参照してください。

ネットワークスキャナーはどの IP アドレスからトラフィックを生成しますか?

スキャナーは、次のパブリック IP アドレスからトラフィックを引き起こします。

- `3.147.184.122`
- `3.19.220.21`

対象範囲と制限

ネットワークスキャナーは IPv6 をサポートしていますか?

いいえ。IPv4 のみがサポートされています。

VM がロードバランサーの背後または API ゲートウェイの背後にあることがスキャンされなかったのはなぜですか?

ロードバランサーと API ゲートウェイは直接リソースと見なされ、スキャンされます。

ロードバランサーまたは API ゲートウェイの背後にある VM は、間接リソースと見なされます。これらは、到達可能性の検証のためにネットワークスキャナーでサポートされていません。これらのリソースは、ネットワーク評価 (静的設定分析) を使用して、パブリックかどうかを判断します。

検出結果

ネットワークスキャナーは検出結果の深刻度に影響しますか?

回答: はい。ネットワークスキャナーは、検出結果の深刻度を判別する要素です。検出結果の深刻度への影響。

データ保護

この記事では、データ保護機能の概念について説明します。

- データリソースを Tenableに接続する方法については、「データリソースの接続を参照してください。
- データスキャン設定を構成するには、「データ」を参照してください。
- データリソースの表示と管理に関するハウツーガイドについては、「データリソースを参照してください。
- よく寄せられる質問については、「FAQ: データ保護」を参照してください。

Tenable One Cloud Exposure データ保護を使用すると、環境を継続的にモニタリングして、新しいデータリソースを特定し、これらのリソースにセンシティブデータがあるかスキャンできます。発見されたセンシティブデータは既知のデータタイプにマッピングされ、個人を特定できる情報 (PII)、保護対象保健情報 (PHI)、デジタルアイデンティティ識別子などのさまざまなカテゴリにグループ化されます。この処理により、データの機密レベルとコンテキストを理解し、業界標準に準拠できるようになります。

> **必要なライセンス:** この機能は **Standard** および **Enterprise** のライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

参考資料

- Tenable によるデータのスキャン方法
- Tenable が検出するデータ
- データリソースのアカウント内スキャン
- よくある質問 - データ保護

Tenable によるデータのスキャン方法

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

リソースのタイプに応じて、Tenable One Cloud Exposure では直接スキャン スキャンや間接スキャン スキャンなど、さまざまなスキャンアプローチが利用されます。次のセクションは、サポートされているリソース、それぞれに使用されるスキャン方法、アカウント内スキャンが利用可能かどうかを示しています。

この記事では、Tenable One Cloud Exposure で使用される特定のスキャン方法の詳細について説明します。さまざまなリソースタイプと運用段階で使用されるすべてのスキャンおよび同期方法 (コード、データ、ワークロードなどの異なるターゲットで使用されるエージェントレス、エージェントベース、パイプライン手法を含む) の広範な概要については、スキャン方法を参照してください。

サポートされているリソースとスキャンのアプローチ

Tenable は、一般的に使用される次のファイル形式を優先的にスキャンしながら、すべてのファイルタイプをスキャンします。

カテゴリー	リソースタイプ	スキャンのアプローチ	アカウント内スキャンをサポート
マネージドデータベースリソース	AWS RDS クラスタ	間接	✓
	サポートされている AWS RDS インスタンスのデータベースエンジンバージョン	間接	✓
	AWS DynamoDB の表	直接	✓
	サポートされている Azure SQL 層	間接	✓
	サポートされている GCP BigQuery データセット	直接	✓
	サポートされている GCP SQL インスタンスのデータベースエンジンバージョン	間接	✓
バケット (パブリックおよびプライベート)	サポートされている AWS S3 バケットストレージクラス	直接	✓

カテゴリー	リソースタイプ	スキャンのアプローチ	アカウント内スキャンをサポート
	Azure ストレージアカウント Blob コンテナ	直接	✓
	GCP ストレージバケット	直接	✓
	サポートされている OCI オブジェクトストレージバケット	直接	✓
	Alibabaクラウドオブジェクトストレージサービス	直接	✗
データプラットフォームスキャン	ローカルデータベース	直接	✗
	共有データベース	直接	✗
	Marketplace データベース	直接	✗
ワークロード[1]	スキャンから仮想マシンを除外する	間接的 (ワークロード保護経由)	✓
	ワークロード	間接的 (ワークロード保護経由)	✓

[1] スキャンは、機密性レベル **が制限** されたデータタイプに限定されます。

サポートされている AWS RDS クラスタ (Aurora) データベースエンジンのバージョン

AWS RDS クラスタでは、次のデータベースエンジンがスキャンでサポートされています。

- **MySQL**:
    - 5.7, 8.0, 8.1
- **PostgreSQL**:
    - 9, 10, 11, 12, 13, 14, 15, 16, 17

サポートされている AWS RDS インスタンスのデータベースエンジンバージョン

AWS RDS インスタンスでは、次のデータベースエンジンバージョンがスキャンでサポートされています。

- **MySQL**:
    - 5.7, 8.0, 8.1
- **PostgreSQL**:
    - 9, 10, 11, 12, 13, 14, 15, 16, 17
- **SQL Server**:
    - 12 (2014), 13 (2016), 14 (2017), 15 (2019), 16 (2022)
- **Oracle** Standard Edition 2 および Enterprise Edition:
    - 19c

サポートされている AWS S3 バケットストレージクラス

次の Amazon S3 ストレージクラス がスキャンでサポートされています。

- S3 Express One ゾーン
- S3 One Zone-IA
- S3 標準
- S3 Standard-IA

サポートされている Azure SQL 層

次を除き、すべての Azure SQL レベルがサポートされています。

- Azure SQL サーバーレス
- ビジネスクリティカル
- データウェアハウス
- ハイパースケール
- プレミアム

サポートされている GCP BigQuery データセット

GCP に保存されているネイティブの BigQuery データセットのみがサポートされます。BigQuery Omni を通じてアクセスまたは管理されるデータセット (AWS S3 や Azure Blob Storage など) はサポートされていません

サポートされている GCP SQL インスタンスのデータベースエンジンバージョン

GCP SQL インスタンスでは、次のデータベースエンジンバージョンがスキャンでサポートされています。

- **MySQL**:
  - 5.7, 8.0
- **PostgreSQL**:
  - 9.6, 10, 11, 12, 13, 14, 15, 16, 17
- **SQL Server**:
  - 14 (2017), 15 (2019), 16 (2022)

GCP SQL の特別な考慮事項

- **GCP SQL リードレプリカ** インスタンスはサポートされていません。

サポートされている OCI オブジェクトストレージバケット

OCIオブジェクト・ストレージ・バケットをスキャンするときは、次の制限が適用されます。

- スキャンは Standard 層 のみをサポートします。

- グローバルスキャンは、**OC1** レルム (Oracle の商用レルム) のみをサポートします。他のレルム (**OC2** や **OC3** など) のリソースをスキャンするには、データリソースのアカウント内スキャンを使用します。

サポートされている Snowflake テーブル

次の Snowflake テーブルタイプがスキャンでサポートされています。

- テーブル (永続テーブル)
- 一時テーブル
- ハイブリッドテーブル

サポートされているAlibaba Cloud OSSバケットストレージクラス

以下の Alibaba Cloud OSS バケットストレージクラス がスキャンでサポートされています。

- 標準
- 低頻度アクセス (IA)

スキャンのアプローチ

クラウドサイバーエクスポージャー では、クラウドリソースの機密データをスキャンするために、**直接** スキャンと**間接** スキャンの 2 種類のアプローチを使用します。どちらのアプローチでも、機密データの安全性が保たれ、環境外に保存されることはありません。使用するアプローチは、スキャンされるクラウドリソースのタイプによって異なります。

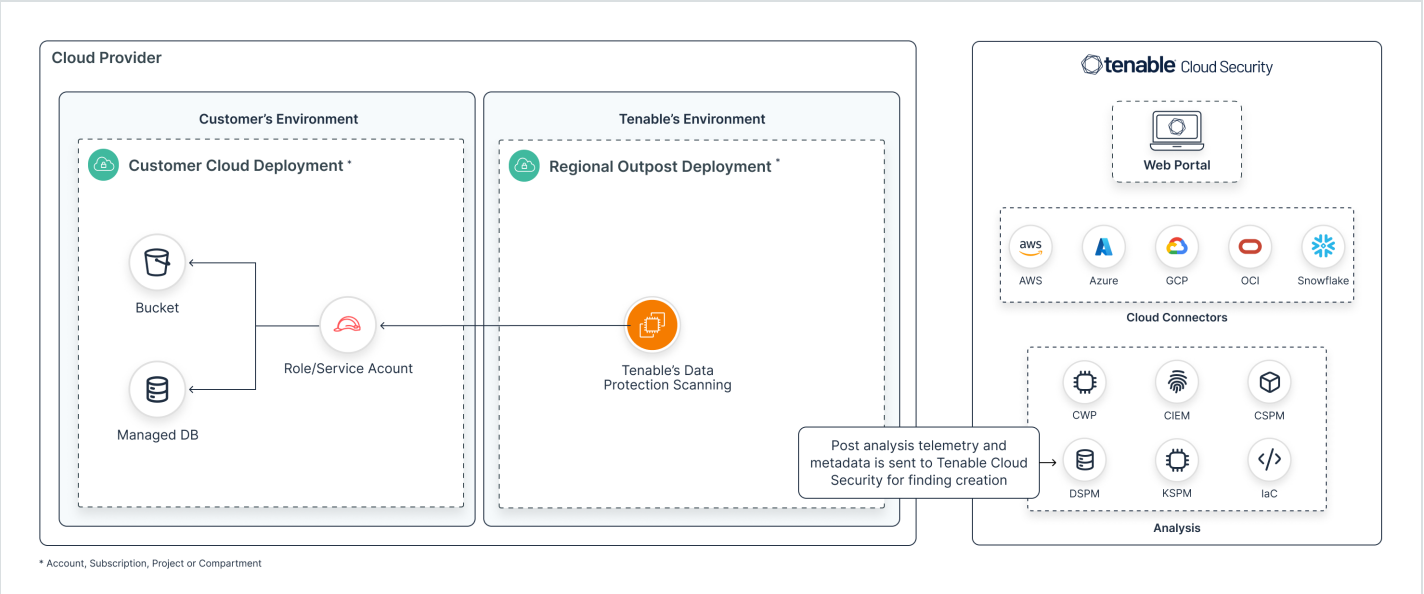
直接スキャン

クラウドサイバーエクスポージャー は、スキャン目的で API を利用してクラウドリソースに接続します。

- 付与されたロールまたはサービスアカウントを利用して、Tenable の地域のアウトポストはオブジェクト (バケット内) とテーブル (マネージドデータベース内) をスキャンして、データを機密性の高いデータタイプに分類します。

- テレメトリとメタデータ (特定のデータタイプの存在と場所) はアウトポストで収集され、グローバルクラウドサイバーエクスポージャープラットフォームに送信されますが、機密データが他の場所に保存される**ことはありません**。
- オブジェクトやテーブルにセンシティブデータが存在すると、それらのオブジェクトやテーブルが検出されたリソースに関連する検出結果の深刻度に影響を与えます。

次の図では、サポートされているすべてのクラウドプロバイダーに関する直接スキャンのワークフローを示しています。



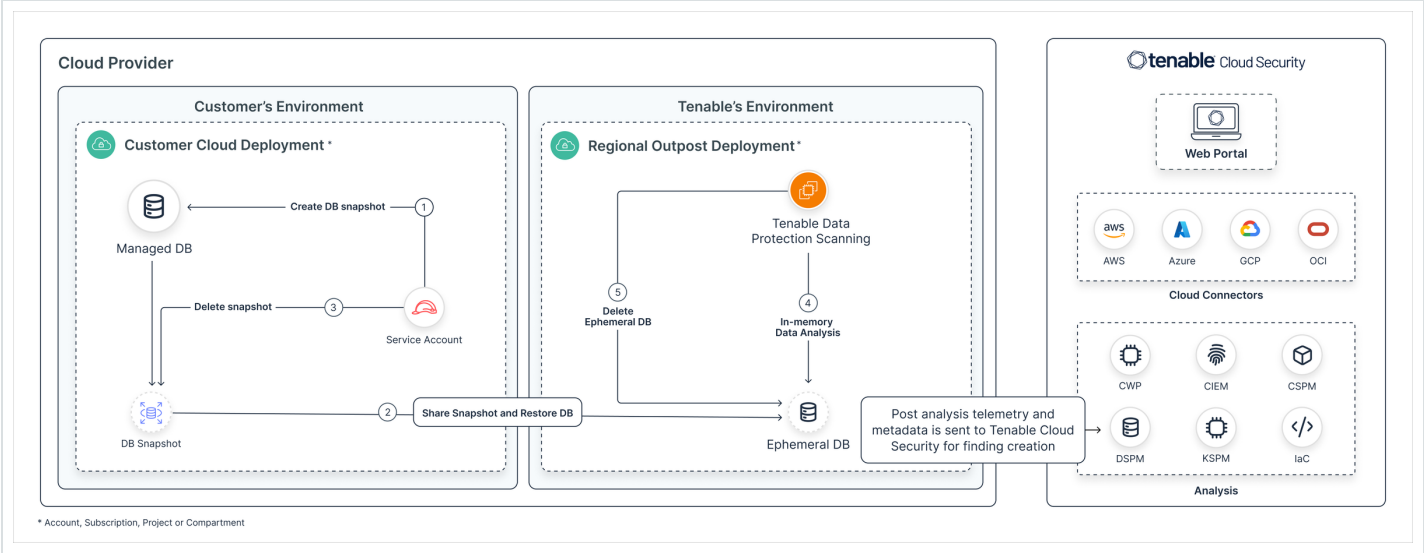
間接スキャン

クラウドサイバーエクスポージャーはスキャン目的でクラウドリソースのスナップショットまたはバックアップを利用します。

- 付与されたロールまたはサービスアカウントを利用して、マネージドデータベースのスナップショットまたはバックアップをクラウドサイバーエクスポージャーの地域のアウトポストと共有し、DB テーブルをスキャンして、データを機密性の高いデータタイプに分類します。
- テレメトリとメタデータ (特定のデータタイプの存在と場所) はアウトポストで収集され、グローバルクラウドサイバーエクスポージャープラットフォームに送信されますが、機密データが他の場所に保存される**ことはありません**。

- テーブルにセンシティブデータが存在すると、それらのテーブルが検出されたリソースに関連する検出結果の深刻度に影響を与えます。

次の図では、サポートされているすべてのクラウドプロバイダーに関する間接スキャンのワークフローを示しています。



ワークロードベースのスキャン (仮想マシンと仮想マシンイメージ)

Tenable は、既存のワークロード保護の脆弱性スキャンワークフローを利用して、仮想マシンおよび仮想マシンイメージの機密データをスキャンします。これらのスキャンは特に、感度レベルデータタイプをターゲットとします。

- 要件: 仮想マシンおよび仮想マシンイメージのデータのスキャンは、対応するワークロード保護スキャンが有効になっている場合にのみ利用できます。
  - 仮想マシンスキャンから仮想マシンを除外するを参照してください。
  - 仮想マシンワークロードを参照してください。
- **ワークロードで機密データが検出された場合**
  - 関連する検出結果の深刻度レベルは 1 レベル上げられますが (**たとえば、[中]** から **[高]**) ですが、**[高]** に制限されています。すでに **[高]** または **[重大]** になっている検出結果の深刻度レベルはそのまま維持され、それ以上昇格することはありません。

- 検出されたデータが機密**データのモニタリングテンプレート**を使用してカスタムクラウドポリシー: カスタムをトリガーした場合、新しい検出結果が作成されます。

- **サポートされるプラットフォーム**
  - **AWS**: EC2 インスタンスとイメージ
  - **Azure**: 仮想マシン
  - **GCP**: VM インスタンスとコンピューティングイメージ
  - **OCI**: コンピューティング・インスタンスおよびイメージ
  - **オペレーティングシステム**:LinuxおよびWindows

セキュリティとプライバシー

次のセクションでは、Tenable Data Protection ソリューション内で顧客データを保護し、コンプライアンスを確保するために実装されているセキュリティとプライバシーのプラクティスの概要を説明します。

- テレメトリとメタデータ (特定のデータタイプの存在と場所) はアウトポストで収集され、グローバルクラウドサイバーエクスポージャープラットフォームに送信されますが、センシティブデータが他の場所に保存されることはありません。
- デフォルトでは、Tenable はアカウントの関連リソースに対してデータ分析スキャンを実行します。これはデータのアクセス許可が付与されたすべてのアカウントに対して実行されます。ただし、データを作成して、カスタムロジックに基づいて特定のリソース、リージョン、または環境をスキップすることで、これを微調整できます。詳細については、「 Configure Data Scanning Settings 」を参照してください。
- オープンネットワークで転送されるデータはすべて、TLS 1.2 または同等のものを使用して暗号化されます。
- クラウドサイバーエクスポージャーは、スキャンされた顧客データの操作に必要な最小限のアクセス許可を使用し、可能な限りデータへの読み取り専用アクセスに重点を置いています。
- クラウドサイバーエクスポージャーコンソールに表示される顧客データのスニペットはすべて、コンプライアンスおよび規制要件に厳格に従い、文字列の機密でない部分のみを表示するために切り捨てられます。このアプローチにより、必要なインサイトを提供しながら、機密データが保護されます。

クラウドプロバイダー	リージョン名	リージョン識別子
AWS	中国(北京)	`cn-north-1`
AWS	中国 (寧夏)	`cn-northwest-1`
Azure	障害復旧 (DR)	すべてのリージョン
Azure	西インド	`westindia`
Azure	Jio インド西部	`jioindiawest`
Azure	ニュージーランド北部	`newzealandnorth`
Azure	スウェーデン南部	`swedensouth`
Azure	台湾北部	`taiwannorth`
GCP	米国中部 2	`us-central2`
OCI	EU 専用クラウド (DCC) リージョン	`eu-dcc-*`
OCI	クリシエ、スイス	`eu-crissier-1`
OCI	EU ソブリン南部 (マドリード)	`eu-madrid-2`
OCI	EU ソブリン中央部 (フランクフルト)	`eu-frankfurt-2`
OCI	米国政府東部 (アッシュバーン)	`us-langley-1`
OCI	米国政府西部 (フェニックス)	`us-luke-1`

Tenable が検出するデータ

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Tenable が検出するデータ

スキャンされた各リソースタイプについて、Tenable は以下を検出します。

- スキャン対象ファイル形式
- スキャン対象データタイプ

スキャン対象ファイル形式

Tenable は、一般的に使用される次のファイル形式を優先的にスキャンしながら、すべてのファイルタイプをスキャンします。

分類	タイプ	サポートされている拡張
構造化	スプレッドシートとデータベース	csv、parquet、tsv、xlsx、xls
半構造化	構成ファイル	env、json、properties、tfstate、xml、yaml、yml
非構造化	コード	cshtml、html、ps1、py、sh
	コマンド履歴	シェル履歴ファイル[1]
	ドキュメント	pdf、docx、doc、txt、log
	イメージ	bmp、gif、jpeg、jpg、png、tiff
	シークレット	asc、jks、key、keys、keystore、p12、pem、pfx、ppk、rsa、secret``secrets
圧縮[2]	アーカイブ	bz2、gz (gzip)

[1] curl、wget、git、mysql、sshpass などのコマンドのパスワードパターン (-p、--password、username:password@host など) を検出します。
[2] 圧縮ファイルは、サポートされているファイル形式が含まれている場合にのみサポートされます。

注意: 拡張子のないファイルもサポートされています。これらのファイルが分析され、コンテンツがサポートされている形式と一致するかどうかが判断されます。

スキャン対象データタイプ

Tenable は、組み込みデータタイプをスキャンし、カテゴリと機密度にデフォルトの分類を適用します。

各組み込みデータタイプには、事前定義された検出ロジックとデフォルトのマッピングが含まれており、データタイプで構成できます。

また、独自の検出ロジックを定義し、カテゴリと機密度を割り当てることで、組織固有のデータを検出するための カスタムデータ型の作成 を作成することもできます。

機密レベルは、リスクの深刻度に影響します。機密レベルが **社外秘**、**専有**、制限付き **の場合、関連する**検出結果の深刻度は 1 レベル上げられます。

機密性値の詳細については、「 感度レベル」を参照してください。

一部の組み込みデータタイプは、専用の表にグループ化されています。参照:

- スキャン対象データタイプ: 運転免許証
- スキャン対象データタイプ: 国民 ID
- スキャン対象データタイプ: 納税者番号
- スキャン対象データタイプ: 社会保障番号
- 秘密のデータ型

カテゴリー	データタイプ	説明	機密度
PCI	CVV	クレジットカード認証番号	制限付き
	クレジットカード番号	個人アカウント番号	制限付き

カテゴリー	データタイプ	説明	機密度
	フルマグネットストライプ	クレジットカード磁気ストライプ (完全な追跡データ)	制限付き
	マスクされたクレジットカード番号	省略された個人アカウント番号	パブリック
PHI	DEA	麻薬取締局番号	制限付き
	DICOM	デジタルイメージと通信	制限付き
	HL7	臨床と管理の医療データの転送に関するグローバル基準	制限付き
	MBI	米国メディケア受益者識別子	制限付き
	MRN	医療記録番号	制限付き
	国民健康保険	ニュージーランド保健省インデックス番号	制限付き
	NHSの	英国国民保健サービス番号	制限付き
	ニノ	英国国民保険番号	制限付き
	NPI	NPI (National Provider Identifier)	制限付き

カテゴリー	データタイプ	説明	機密度
	HICN	医療保険請求番号	社外秘
PII	銀行口座番号	個人の銀行口座番号 (米国およびカナダ)	制限付き
	BTC	Bitcoin アドレス	制限付き
	EIN	米国雇用主証明番号	制限付き
	IBAN	国際銀行口座番号	制限付き
	ITIN	個人納税者識別情報	制限付き
	個人 ID	スキャン対象データタイプ: 国民 IDの完全なリストを見る	制限付き
	パスポート番号	アイデンティティと市民権のドキュメント ID	制限付き
	社会保障番号	スキャン対象データタイプ: 社会保障番号の完全なリストを見る	制限付き
	納税者番号	スキャン対象データタイプ: 納税者番号の完全なリストを見る	制限付き
	VIN	車両識別番号	制限付き

カテゴリー	データタイプ	説明	機密度
	アドレス	エンティティを特定するために使用される物理アドレス	極秘
	請求	エンティティを特定するために使用されるトランザクションステートメント	極秘
	クライアント案件 ID	クライアントケースの一意の法的識別子	極秘
	運転免許証	スキャン対象データタイプ: 運転免許証の完全なリストを見る	社外秘
	Email	メールアドレス (デジタルアイデンティティ)	社外秘
	ESN	電子シリアル番号	極秘
	ゲイド	Google 広告 ID	社外秘
	Google プレイス ID	場所を示す一意のテキスト識別子	極秘
	IMEI	国際移動体装置識別番号	社外秘
	IMSI	国際移動体加入者識別番号	社外秘
	請求書	エンティティを特定するために使用される商品/サービスの署名済みリスト	極秘
	IP アドレス	デバイスインターネットプロトコル識別子	社外秘
	Location	緯度および/または経度	社外秘
	MAC	マシンの一意の識別子	極秘
	人	エンティティを識別するために使用される特定の名前	社外秘

カテゴリー	データタイプ	説明	機密度
	電話番号	個人の連絡先番号	社外秘
	Salesforce ユーザー ID	Salesforce の一意のエンティティ識別子	極秘
	ユーザー名	エンティティを特定するために使用される電子名	極秘
	Zendesk ID	Zendesk の一意のエンティティ識別子	極秘
	生年月日	個人の生年月日	プライベート
	性別	エンティティを特定するために使用されるジェンダーの詳細	プライベート
	国籍	市民権または国籍の識別子	プライベート
	出生地	個人が生まれた場所を示す国名	プライベート
	日本法人番号	日本の国税庁によって割り当てられた企業識別子	パブリック
シークレット	シークレットデータ型	秘密のデータ型	

スキャン対象データタイプ: 運転免許証

すべての運転免許証のデータタイプについて、カテゴリは **PII** であり、感度レベルは **機密です**。

国	状態
米国	アリゾナ州
米国	コロラド州
米国	グアム
米国	ニュージャージー州
米国	アイダホ州
米国	イリノイ州
米国	インディアナ州
米国	オクラホマ州
米国	アイオワ州
米国	カンザス州
米国	ハワイ
米国	モンタナ州
米国	ケンタッキー州
米国	メイン州
米国	マサチューセッツ州
米国	ミシガン州
米国	ミネソタ州
米国	メリーランド州

国	状態
米国	フロリダ
米国	カリフォルニア州
米国	ニューヨーク
米国	ミズーリ州
米国	ネブラスカ州
米国	ネバダ州
米国	ニューハンプシャー州
米国	ノースダコタ州
米国	オハイオ州
米国	ロードアイランド州
米国	オレゴン
米国	バーモント州
米国	バージニア州
米国	ワシントン
米国	ウェストバージニア州
米国	ウィスコンシン州
フランス	
ドイツ	

国	状態
アイルランド	
イスラエル	
イタリア	
日本	
オランダ	
スペイン	
英国	

スキャン対象データタイプ: 国民 ID

すべての国民 ID データタイプの場合、カテゴリは **PII** で、感度レベルは**「制限付き」**です。

国	サブタイプ	説明
ブラジル	RG	ブラジル一般登録番号
ブルガリア	EGN	ブルガリア統一市民番号
カナダ	SIN	カナダの社会保険番号
フランス	INSEE	フランス語 INSEE コード
ドイツ	NID	ドイツの国民ID(Personalausweis)
インド	アーダール	インド Aadhaar 番号
International	ISIN	国際証券識別番号

国	サブタイプ	説明
International	LEI	法人識別子
アイルランド	PPS	アイルランド個人公共サービス番号
イスラエル	テウダット・ゼフット	イスラエルの身分証明書
日本	マイナンバー	日本の国民番号
メキシコ	CURP	メキシコの固有人口登録コード
オランダ	BSN	オランダ市民サービス番号 (Burgerservicenummer)
ロシア	OGRN	ロシアの企業の国家登録番号
ロシア	NID	ロシア国内の個人番号
シンガポール	NRIC	シンガポール国民登録IDカード
南アフリカ	ID	南アフリカID
スペイン	NIE	スペイン外国人識別番号(非居住者用)
トルコ	TCKN	トルコの国民ID
ウクライナ	ID	ウクライナの身分証明書
英国	選挙人名簿	英国の選挙人名簿番号
英国	ニノ	英国国民保険番号

スキャン対象データタイプ: 納税者番号

すべての納税者番号データタイプの場合、カテゴリは **PII** であり、感度レベルは**「制限付き」**です。

国	サブタイプ	説明
オーストラリア	TFN	納税者番号
ブラジル	CNPJ	ブラジル法人登録局
ブラジル	CPF	個人納税者番号 (Cadastro de Pessoas Físicas)
ドイツ	ブリキ	ドイツの納税者番号 (Steuer Identifikationsnummer)
イタリア	Codice Fiscale	イタリアの納税者番号
ニュージーランド	IRD	内国歳入局番号
スペイン	NIF	スペインの納税者番号 (Número de Identificación Fiscal)
英国	UTR	固有の納税者参照

スキャン対象データタイプ: 社会保障番号

すべてのSSNデータタイプの場合、カテゴリは**PII**で、感度レベルは**[制限付き]**です。

- ドイツ
- ロシア
- スペイン
- スイス
- 米国

スキャン対象データタイプ: シークレット

シークレットデータタイプの完全なリストについては、「秘密のデータ型を参照してください

分類の除外

データ保護は、クラウドリソース全体で PII、PCI、PHI、シークレットなどの機密データを検出して分類します。一部のデータは、機密データタイプに一致しますが、内部メールドメインや既知のテストデータベースの機密値など、お使いの環境では実際のリスクではありません。これらの一致を放っておくと、行動を起こさない検出結果が作成されます。

分類の除外により、Tenable に無視させるデータとその無視する場所を微調整できます。除外する対象(データタイプ、カテゴリ、機密度、特定の値)と、除外が適用される正確なリソースとデータオブジェクトを定義します。スキャンは引き続きリソース上で実行されるため、他の機密データは引き続き機密扱いされ、請求には影響しません。

> **注意: (クイックリンク)** このセクションでは、分類除外の仕組みについて説明します。作成して管理するには、[分類除外を作成する]を参照してください。

除外の例

- 任意の .pdf ファイルの Secret カテゴリのすべてのデータタイプで `password123` 値を無視します。
- `Test` という名前のデータベーステーブルの制限されたデータ型を無視します。
- 特定のリージョンのすべてのデータリソースにおいて、[メール] データタイプの企業ドメイン (`@acme.com`) を無視する。

分類除外の仕組み

各分類除外は、3つのスコープディメンションを組み合わせたものです。これらを組み合わせることで、Tenable が何をどこで無視するかを正確に決定します。

1. **データ。** 何を無視するか。データのタイプを選択し、次に値を選択します。
    - 型: **すべての** データ型、データカテゴリ、機密性レベル、または 1 つ以上の特定のデータ型。
    - **値**: 選択したタイプのすべての値、または RE2 正規表現パターンとして定義された特定の値(企業のメールドメインなど)。
2. **リソース。** 除外を適用する場所: スコープ内のすべてのリソース、またはクエリで選択された特定のリソース

3. **データオブジェクト**。それらのリソース内の正確な場所。すべてのデータ・オブジェクト、または1つ以上のロケーション条件として定義された特定のデータ・オブジェクトを選択します。
    - データベース名
    - データベーススキーマ名
    - データベーステーブル名
    - ファイル拡張子
    - オブジェクトパス

各ロケーション条件は1回使用され、それぞれが複数のRE2正規表現値を受け入れます。Tenableは条件間にORロジックを適用するため、いずれかの条件に一致する場合、データは無視されます。

[すべてのデータタイプ]を選択すると、**[すべてのデータオブジェクト]**オプションが無効になります。すべてのデータオブジェクトですべてのデータタイプを除外すると、リソースの分類が完全に停止されます。これは、分類の除外ではなくスキャンの除外の動作です。

分類の除外とスキャンの除外の比較

どちらの機能もノイズを低減しますが、異なる段階で作用します。

機能	機能	スキャンへの影響	請求への影響
データ	リソースに対するスキャンの実行を停止します	スキャンが実行されない	リソースはスキャンされていません
分類除外	は、定義した場所内で、定義したデータの分類を抑制します	スキャンは引き続き実行されます。その他のデータはまだ機密扱いです	なし

リソースのスキャンは継続したいが、リソース内の特定のデータは無視したい場合に、分類除外を使用します。リソースのスキャンを完全に停止する場合は、スキャン除外を使用します。

詳細はこちら

- 除外を作成、編集、有効化、無効化、または削除するには、「分類除外の作成」を参照してください。

秘密のデータ型

データタイプ	説明	重大度
1Password 秘密鍵	マスターパスワードと一緒に 1Password Vault を復号化するために使用されるマスターキー	制限付き
1Password サービスアカウントトークン	1Password Vault とシークレットへの自動アクセスのためのプログラムトークン	制限付き
Adafruit API キー	Adafruit IO IoT プラットフォームサービスとデータフィードにアクセスするための API キー	プライベート
Adobe クライアント ID	Adobe OAuth と API の統合フローで使用されるパブリックアプリケーション識別子	パブリック
Adobe クライアントシークレット	サーバー側の OAuth 認証のために Adobe Client ID とペアで使用されるシークレット	制限付き
経過日数シークレットキー	age ファイル暗号化ツール用のプライベート復号化キー	制限付き
合気道 CI トークン	Aikido Security CI パイプラインスキャンと脆弱性検出統合のトークン	制限付き
合気道クライアントシークレット	Aikido Security プラットフォーム OAuth 認証のクライアントシークレット	制限付き
Airtable API キー	Airtable のベースとレコードへの読み取り/書き込みアクセス権を付与する認証キー	極秘
Airtable個人用アクセス	API 経由で Airtable ワークスペースデータにアクセスするた	極秘

データタイプ	説明	重大度
トークン	めのユーザー範囲指定のトークン	
Aiven 認証トークン	Aiven マネージドクラウドデータベースとストリーミングサービスの認証トークン	制限付き
Algolia API Key	クライアント側で検索クエリによく使用される Algolia 検索サービス用のキー	プライベート
Alibaba アクセスキー ID	クラウドリソースへのアクセス権を付与する Alibaba Cloud IAM 認証情報の識別子	極秘
Alibaba シークレットキー	クラウド API 認証のために Alibaba Access Key ID とペアで使用されるシークレットキー	制限付き
Amazon Bedrock API キー	Amazon Bedrock 基盤 AI モデルにアクセスするための API キー	制限付き
Amplitude Secret Key	Amplitude 製品の分析データ取り込みと管理のためのサーバー側の秘密キー	極秘
Anthropic API キー	Claude およびその他の Anthropic AI モデルエンドポイントにアクセスするための API キー	制限付き
Apideck APIキー	複数の SaaS 統合に接続する Apideck 統合 API プラットフォーム用のキー	極秘
Apify API トークン	Apify ウェブスクレイピングと自動化クラウドプラットフォーム用のトークン	極秘
Artifactory API キー	JFrog Artifactory のアーティファクトリポジトリとビルドパッケージにアクセスするためのキー	制限付き
Artifactory 参照トークン	JFrog Artifactory サービスに対する認証を行うための参	制限付

データタイプ	説明	重大度
	照ベースのトークン	き
Asaas APIトークン	Asaasの決済処理と金融サービスプラットフォームAPIのトークン	制限付き
Asana クライアント ID	Asana OAuth 統合フロー用のパブリックアプリケーション識別子	パブリック
Asana クライアントシークレット	サーバー側のAsana OAuth認証とトークン交換用のシークレットキー	極秘
AssemblyAI API キー	AssemblyAI音声テキスト変換とオーディオインテリジェンスサービスのAPIキー	極秘
Atlassian APIトークン	Jira APIとConfluence APIおよびワークスペースデータにアクセスするための個人用トークン	極秘
Authress サービスクライアントのアクセスキー	Authress承認とアイデンティティ管理プラットフォームのサービス認証情報	制限付き
AWS アクセストークン	AWS APIリクエストを認証するための一時的または長期的認証情報	制限付き
AWS S3 署名付き URL	特定のS3オブジェクトへの一時的なアクセスを許可する、期限付きの事前署名 URL	極秘
AWS シークレットアクセスキー	APIリクエストに署名するためにAWS Access Key IDとペアで使用されるシークレット認証情報	制限付き
AWS セッショントークン	AWS STS ベース認証の一時的なセッション認証情報	制限付き
Azure Active Directory クラ	アイデンティティアクセス管理で使用されるAzure ADアプ	制限付

データタイプ	説明	重大度
イアントシークレット	リ登録用のシークレット	き
Azure アプリ構成の接続文字列	Azure App Configuration のキーと値のストアと機能フラグ管理用のエンドポイントとシークレットを含む接続文字列	制限付き
Azure Batch 共有キー	Azure Batch コンピューティングサービスに対する認証用の共有キー	極秘
Azure Cache for Redis のアクセスキー	Azure が管理する Redis キャッシュインスタンスに接続するためのキー	極秘
Azure Container Registry パスワード	コンテナイメージを Azure Container Registry にプルおよびプッシュするためのパスワード	制限付き
Azure CosmosDB キー	Azure CosmosDB データベースアカウントへのフルアクセス用のプライマリまたはセカンダリキー	制限付き
Azure DevOps 個人用アクセストークン	Azure DevOps リポジトリ、CI/CD パイプライン、ワークアイテムにアクセスするためのトークン	制限付き
Azure 関数キー	Azure サーバーレス関数エンドポイントを呼び出すための認証キー	極秘
Azure メッセージングサービスキー	Azure Service Bus または Event Hub メッセージングサービス用のキー	極秘
Azure Search 管理者キー	Azure Cognitive Search サービスへの完全な管理アクセス権を付与する管理者キー	制限付き
Azure Search クエリキー	Azure Cognitive Search インデックスをクエリするための読み取り専用キー	プライベート
Azure Service Bus 接続	Azure Service Bus メッセージング キューとトピックの共有	制限付

データタイプ	説明	重大度
文字列	アクセスキーを含む接続文字列	き
Azure ストレージアカウントキー	Azure Storage アカウントとそのすべてのデータへのフルアクセス権を付与するマスターキー	制限付き
Azure Storage SAS (共有アクセス署名)	Azure Storage リソースへの委任アクセス用の範囲付き期間限定トークン	極秘
Bash 変数パスワード	bash シェル変数またはスクリプトに保存されているパスワード	制限付き
Beamer API トークン	Beamer のアプリ内変更ログおよび通知サービス用のトークン	プライベート
Bitbucket クライアント ID	Bitbucket OAuth 統合フロー用のパブリックアプリケーション識別子	パブリック
Bitbucket クライアントシークレット	ソースコードリポジトリへのアクセス権を付与する Bitbucket OAuth のシークレット	制限付き
Bitly アクセストークン	Bitly URL 短縮とリンク管理プラットフォーム API のトークン	極秘
Bitriseアクセストークン	ビルドとワークフローを管理するための Bitrise モバイル CI/CD プラットフォームのトークン	制限付き
Bittrex アクセスキー	Bittrex 暗号通貨取引とアカウントアクセス用の API キー	制限付き
Bittrex シークレットキー	交換 API リクエストに署名するために Bittrex アクセスキーとペアで使用されるシークレットキー	制限付き
Box API アクセストークン	Box クラウドコンテンツ管理とファイル共有プラットフォーム	極秘

データタイプ	説明	重大度
	API のトークン	
Brave Search API Key	ウェブ検索の結果とデータを提供する Brave Search API の API キー	プライベート
Buildkite API トークン	パイプラインを管理し、エージェントをビルドする Buildkite CI/CD プラットフォーム用のトークン	制限付き
Buildkite サービストークン	Buildkite CI/CD エージェント登録、ジョブ実行、パッケージ管理のサービスレベルトークン	制限付き
Buildkite ユーザーアクセストークン	パイプラインとビルド、組織データへの Buildkite CI/CD プラットフォーム API アクセス用のユーザースコープトークン	制限付き
Canadian Digital Service Notify API Key	Canadian Digital Service の Notify 政府向けメッセージングプラットフォーム用の API キー	制限付き
Canvaクライアントシークレット	Canva デザインプラットフォームの OAuth 認証と API アクセス用のクライアントシークレット	制限付き
Cerebras API Key	Cerebras AI 高性能推論プラットフォームの API キー	制限付き
Checkout.com シークレットキー	Checkout.com の決済処理と取引 API のサーバー側の秘密キー	制限付き
CircleCI API トークン	ビルドとプロジェクト設定を管理する CircleCI CI/CD プラットフォーム用のトークン	制限付き
CircleCI 個人アクセストークン	パイプラインと設定への完全なユーザーレベルの API アクセスを許可する、CircleCI CI/CD プラットフォームの個人用トークン	制限付き

データタイプ	説明	重大度
CircleCI プロジェクトトークン	CircleCI のビルドステータスとアーティファクトへの読み取り専用アクセス用のプロジェクト範囲のトークン	極秘
Cisco Meraki API キー	API 経由で Cisco Meraki ネットワークインフラとデバイスを管理するためのキー	制限付き
Civo API キー	Kubernetes のクラスタとインフラを管理する Civo クラウドプラットフォームの API キー	制限付き
事務員シークレットキー	Clerk 認証とユーザー管理バックエンド API の秘密キー	制限付き
Clickhouse Cloud API 秘密鍵	ClickHouse Cloud 分析データベースインスタンスにアクセスするためのシークレットキー	制限付き
ClickUp 個人用 APIトークン	ClickUp プロジェクト管理と生産性プラットフォーム API の個人用トークン	極秘
Clojars APIトークン	Clojars リポジトリで Clojure ライブラリを公開し管理するためのトークン	制限付き
Cloudflare API キー	Cloudflare CDN、DNS、セキュリティサービスを管理するための範囲付き APIトークン	制限付き
Cloudflare CA キー	Cloudflare オリジン証明書を発行するための認証局キー	制限付き
Cloudflare Global API Key	Cloudflare アカウントに対する完全な制御を許可するフルアクセスキー	制限付き
Cloudflare Origin CA キー	オリジンとエッジの間の TLS で使用される Cloudflare オリジン CA 証明書のキー	制限付き

データタイプ	説明	重大度
Cloudinary API シークレット	Cloudinary メディア管理と画像変換 API の秘密キー	極秘
Cloudsmith API キー	Cloudsmith パッケージとアーティファクトリポジトリ管理の API キー	制限付き
CockroachDB クラウド API キー	CockroachDB クラウド分散データベース管理と運用の API キー	制限付き
Codecov アクセストークン	CI/CD パイプラインと統合された Codecov コードカバレッジレポート用のトークン	極秘
Cohere API トークン	Cohere 自然言語処理と AI モデルエンドポイント用の API トークン	制限付き
Coinbaseアクセストークン	Coinbase 暗号通貨アカウントと取引へのアクセス権を付与するトークン	制限付き
ConfigCat SDK キー	ConfigCat 機能フラグと設定管理サービスの SDK キー	プライベート
ConfigCat SDK キーの拡張	ConfigCat 機能フラグサービス設定用のプロキシ URL 付き拡張 SDK キー	プライベート
Confluent アクセストークン	Confluent マネージド Apache Kafka ストリーミングプラットフォーム用のトークン	極秘
Confluent シークレットキー	Confluent Cloud Kafka サービスに対する認証のためのシークレットキー	極秘
コンテンツフル配信 API トークン	Contentful CMS から公開されたコンテンツを取得するための読み取り専用トークン	プライベート

データタイプ	説明	重大度
Couchbase Capella API キー	Couchbase Capella が管理する NoSQL データベースクラウドプラットフォームの API キー	制限付き
カバーオール個人用 API トークン	Coveralls コードカバレッジの追跡とレポートサービスの個人用トークン	極秘
Crates.io API キー	Crates.io レジストリで Rust クレートを公開および管理するための API キー	制限付き
Curl Auth ヘッダー	curl コマンド承認ヘッダーに埋め込まれた認証情報	極秘
Curl 認証ユーザー	curl コマンドの基本認証で使用されるユーザー名とパスワードの認証情報	極秘
Cursor API Key	Cursor AI 搭載コードエディターとアシスタントサービスの API キー	極秘
Data.gov API キー	Data.gov 米国政府オープンデータプラットフォームへのアクセス用の API キー	プライベート
Databento APIキー	Databento リアルタイムと過去の金融市場データサービスの API キー	極秘
Databricks API トークン	データアクセスを備えた Databricks データエンジニアリングと分析プラットフォーム用のトークン	制限付き
Datadog アクセストークン	Datadog インフラモニタリングとオブザーバビリティプラットフォーム API 用のトークン	制限付き
Datadog API キー	メトリクスとイベント、ログ、トレースを Datadog モニタリングプラットフォームに送信するための API キー	制限付き
Datadog アプリケーション	API キーと組み合わされた場合に、Datadog アカウントに	制限付

データタイプ	説明	重大度
キー	完全なデータアクセスを許可するアプリケーションキー	き
DataStax Astraアプリケーショントークン	DataStax Astra が管理する Cassandra データベースプラットフォームのアプリケーショントークン	制限付き
Deepgram API キー	Deepgram 音声テキスト変換と音声分析 AI サービスの API キー	制限付き
DeepSeek API キー	DeepSeek AI 言語モデルと推論サービスの API キー	制限付き
定義済みネットワーキング APIトークン	Defined Networking オーバーレイネットワーク管理プラットフォーム用のトークン	極秘
Deno アカウントトークンのデプロイ	Deno Deploy サーバーレス JavaScript プラットフォーム管理用のアカウントトークン	制限付き
DevCycle クライアント SDK キー	アプリケーションでの DevCycle 機能フラグ評価のクライアント側 SDK キー	プライベート
DevCycle Mobile SDK キー	モバイルデバイス上の DevCycle 機能フラグ評価のモバイル SDK キー	プライベート
DevCycle Server SDK キー	フルアクセスが許可された DevCycle 機能フラグ管理のサーバー側 SDK キー	制限付き
Devin Personal API Key	Devin AI ソフトウェアエンジニアリングエージェントプラットフォームの個人用 API キー	制限付き
Devin サービス API キー	Devin AI エージェントの自動化およびオーケストレーションのサービスレベル API キー	制限付き
Devin サービスユーザートー	Devin AI エージェントのプラットフォームオペレーションの	極秘

データタイプ	説明	重大度
クン	ユーザー範囲指定サービストークン	
DigitalOcean アクセストークン	DigitalOcean クラウドインフラとリソースへのフルアクセス権を付与するトークン	制限付き
DigitalOcean OAuthアクセストークン	クラウドリソースへの DigitalOcean API アクセスのための OAuth トークン	制限付き
DigitalOcean OAuthリフレッシュトークン	DigitalOcean OAuth アクセストークンを更新するための更新トークン	制限付き
DigitalOcean 個人アクセストークン	完全な DigitalOcean アカウントとインフラ API アクセスのための個人用トークン	制限付き
DigitalOcean リフレッシュトークン	新しい DigitalOcean アクセストークンの取得に使用されるトークン	制限付き
Discord API キー	サーバーおよびメッセージングへの Discord ボットまたはアプリケーション API アクセス用のキー	制限付き
Discord クライアント ID	OAuth フローで使用される Discord アプリケーションのパブリック識別子	パブリック
Discord クライアントシークレット	Discord OAuth サーバー側認証とトークン交換用のシークレット	制限付き
Discord Webhook	自動メッセージを特定の Discord チャネルに投稿するための URL エンドポイント	極秘
Disqus API キー	Disqus コメントおよびコミュニティエンゲージメントプラットフォームの API キー	プライベート
Docker Hub アクセストーク	Docker Hub レジストリでコンテナイメージをプルおよびプッ	制限付

データタイプ	説明	重大度
ン	シュするためのトークン	き
Docker Hub 組織のアクセストークン	チーム全体のイメージアクセスが可能な Docker Hub コンテナレジストリ用の組織範囲指定トークン	制限付き
Docker Hub 個人アクセストークン	Docker Hub コンテナレジストリイメージのプッシュとプル操作用の個人用トークン	制限付き
Docker Swarm Join トークン	ノードがマネージャーまたはワーカーとして Docker Swarm クラスタに参加することを許可するトークン	制限付き
Docker Swarm アンロックキー	保存時の Docker Swarm マネージャー Raft ログと TLS キーのロックを解除するための暗号化キー	制限付き
Doppler API トークン	アプリケーションシークレットを保存する Doppler シークレット管理プラットフォーム用のトークン	制限付き
Dropbox API シークレット	Dropbox API OAuth 認証とファイルアクセス用のアプリシークレット	制限付き
Dropbox Long Lived API トークン	継続的な Dropbox ファイルストレージと API アクセス共有のための永続トークン	制限付き
Dropbox Short Lived API Token	期限付き Dropbox ファイルストレージ API アクセスための一時トークン	制限付き
Duffel API トークン	フライト予約および航空会社データアクセスのための Duffel トラベル API 用のトークン	極秘
Dynatrace API トークン	Dynatrace アプリケーションのパフォーマンスモニタリングとオブザーバビリティ API 用のトークン	極秘
EasyPost API トークン	ラベル生成と追跡のための EasyPost 配送とロジスティク	極秘

データタイプ	説明	重大度
	スAPI用のトークン	
EasyPostテストAPIトークン	EasyPost配送 APIの開発とテストのためのテスト環境トークン	プライベート
eBayクライアントシークレット	eBayマーケットプレイスのOAuth認証およびコマースAPIのクライアントシークレット	制限付き
Elastic Cloud API Key	Elastic Cloudが管理するElasticsearchおよびオブザーバビリティプラットフォームのAPIキー	制限付き
ElevenLabs APIキー	ElevenLabs AI音声合成およびテキスト読み上げサービスのAPIキー	制限付き
Endor Labs APIキー	Endor LabsソフトウェアサプライチェーンセキュリティプラットフォームのAPIキー	制限付き
Endor Labs APIシークレット	サプライチェーンセキュリティ認証用のEndor Labs APIキーとペアになった秘密キー	制限付き
Etsyアクセストークン	店舗とリスティングを管理するEtsyマーケットプレイスAPI用のOAuthトークン	極秘
Etsy Open API Key	ショップデータ、リスト、注文情報へのアクセスを許可するEtsy Open API v3のAPIキー	極秘
Exoscale APIキー	Exoscale欧州クラウドインフラおよびコンピューティングサービスのAPIキー	制限付き
Facebookページアクセストークン	Graph APIを介してFacebookページを管理し、コンテンツを公開するためのトークン	制限付き
Facebookシークレット	Facebook/Metaアプリケーションのサーバー側認証用のア	制限付

データタイプ	説明	重大度
	プリシークレット	き
Facebookトークン	Facebook Graph API ユーザーまたはアプリデータアクセス用の一般アクセストークン	制限付き
Fastly API キー	Fastly CDN とエッジクラウドプラットフォームの設定と管理のためのキー	制限付き
Figma アクセストークン	API を介して Figma 設計ファイルとプロジェクトデータにアクセスするためのトークン	極秘
Figma 個人アクセスヘッダートークン	Figma API デザインファイルのフルアクセスのために X-Figma-Token ヘッダー経由で送信されたパーソナルアクセストークン	極秘
Figma 個人アクセストークン	設計ファイルやプロジェクト、チームデータへのFigma API のフルアクセスのための個人トークン	極秘
Finicity APIトークン	Finicity 財務データ集約とオープンバンキングサービス用のトークン	制限付き
Finicity クライアントシークレット	財務データサービスへの Finicity API 認証用のクライアントシークレット	制限付き
Finnhub アクセストークン	Finnhub 株式市場と財務データ API 用のトークン	極秘
Firebase クラウドメッセージング API キー	Firebase Cloud Messaging サービス経由でプッシュ通知を送信するためのキー	プライベート
Flickr アクセストークン	Flickr 写真共有プラットフォーム API アクセス用のトークン	プライベート
Flutterwave 暗号化キー	Flutterwave 決済取引を保護するための暗号化キー	制限付

データタイプ	説明	重大度
		き
Flutterwave 公開鍵	Flutterwave 決済フォーム統合のためのクライアント側の公開可能キー	パブリック
Flutterwave の秘密鍵	Flutterwave 決済取引を処理するためのサーバー側のシークレットキー	制限付き
Fly.io アクセストークン	Fly.io アプリケーションのホスティングとデプロイメントプラットフォーム管理用のトークン	制限付き
Frame.io API トークン	Frame.io のビデオレビューとコラボレーションプラットフォーム API 用のトークン	極秘
Freemius シークレットキー	Freemius ソフトウェアライセンスとマネタイズプラットフォームのシークレットキー	極秘
Freshbooks アクセストークン	請求書と財務データにアクセスする Freshbooks 会計プラットフォームのトークン	制限付き
FullStory API キー	FullStory デジタルエクスペリエンス分析およびセッションリプレイプラットフォームの API キー	極秘
GCP API キー	Google Cloud Platform サービスへのリクエストを認証するためのキー	制限付き
GCP アプリケーションのデフォルトの認証情報	Google Cloud Platform API に永続的にアクセスするための OAuth2 リフレッシュトークンを含む JSON 認証情報ファイル	制限付き
GCP Gemini API Key	Google Gemini 生成 AI モデル推論と関連する Google Cloud サービスの API キー	制限付き

データタイプ	説明	重大度
GCP サービスアカウントキー	Google Cloud Platform サービスへのプログラムによるアクセス用の秘密鍵を含む JSON キーファイル	制限付き
汎用 API キー	コード内で検出された、サービス範囲が不明の未指定 API キー	極秘
汎用 DB 暗号化キー	データベースレベルまたはフィールドレベルのデータの暗号化に使用される暗号化キー	極秘
汎用パスワード	コードまたは設定ファイル内で検出されたプレーンテキストのパスワード	制限付き
汎用パスワードの割り当て	コードまたは構成の変数に割り当てられたパスワード値	極秘
Gitea アクセストークン	Gitea セルフホスト型 Git リポジトリプラットフォーム API アクセスのトークン	制限付き
GitHub アプリトークン	リポジトリと API へのアクセスを付与する GitHub アプリ用のインストールトークン	制限付き
GitHub Fine-grained Personal Access Token	GitHub リポジトリアクセスについて詳細なアクセス許可を持つ、範囲が指定された個人用トークン	制限付き
GitHub OAuth トークン	リポジトリとユーザーデータへの GitHub API アクセス用の OAuth トークン	制限付き
GitHub 個人アクセストークン	リポジトリとアカウント機能への GitHub API アクセス用の個人用トークン	制限付き
GitHub リフレッシュトークン	GitHub OAuth アクセストークンを更新するためのトークン	制限付き
GitLab CI ビルドトークン	GitLab CI パイプラインビルド実行中に使用される短期	制限付

データタイプ	説明	重大度
	トークン	き
GitLab CI/CD ジョブトークン	単一の GitLab CI/CD パイプラインジョブに範囲を限定した一時トークン	制限付き
GitLab トークンのデプロイ	GitLab リポジトリとコンテナレジストリへの読み取り専用アクセス用のトークン	制限付き
GitLab 機能フラグクライアントトークン	アプリケーションの GitLab 機能フラグを評価するためのクライアント側トークン	プライベート
GitLab フィードトークン	プロジェクトアクティビティの GitLab RSS フィードにアクセスするためのトークン	プライベート
GitLab 受信メールトークン	GitLab メールベースの問題とマージリクエスト作成用のトークン	極秘
GitLab Kubernetes エージェントトークン	GitLab にクラスタを接続している GitLab Kubernetes エージェント用のトークン	制限付き
GitLab OAuth アプリのシークレット	GitLab サードパーティアプリケーション認証用の OAuth アプリシークレット	制限付き
GitLab 個人アクセストークン	リポジトリとプロジェクトデータへの GitLab API アクセス用の個人用トークン	制限付き
GitLab 個人アクセストークン (ルーティング可能なバージョンあり)	GitLab API アクセス用のインスタンスルーティングメタデータを含むバージョン管理された個人用アクセストークン	制限付き
GitLab パイプライントリガートークン	API 経由で GitLab CI/CD パイプラインをトリガーするためのトークン	制限付き

データタイプ	説明	重大度
GitLab Runner 認証トークン	GitLab インスタンスに対して登録された GitLab CI ランナーを認証するトークン	制限付き
GitLab Runner 登録トークン	新しい GitLab CI ランナーをプロジェクトまたはグループに登録するためのトークン	制限付き
GitLab SCIM トークン	GitLab SCIM ベースの自動ユーザープロビジョニングと管理のためのトークン	制限付き
GitLab セッション Cookie	GitLab インスタンスへの認証されたアクセス権を付与するブラウザセッション Cookie	制限付き
Gitter アクセストークン	Gitter 開発者チャットプラットフォーム API アクセス用のトークン	プライベート
GoCardless API トークン	GoCardless ダイレクトデビットと銀行決済処理 API 用のトークン	制限付き
Google OAuth アクセストークン	ユーザーの代わりに Google API にアクセスするための OAuth トークン	制限付き
Google OAuth2 クライアントシークレット	Google OAuth2 サーバー側の認証フロー用のクライアントシークレット	制限付き
Grafana API キー	Grafana モニタリングダッシュボードとデータソース管理 API 用のキー	制限付き
Grafana Cloud API トークン	Grafana クラウドがホストするモニタリングとオブザーバビリティサービス用のトークン	制限付き
Grafana サービスアカウントトークン	自動化された Grafana API オペレーションのためのサービスアカウントトークン	制限付き

データタイプ	説明	重大度
Greptile API Key	Greptile の AI を活用したコードベースの理解および検索プラットフォームの API キー	極秘
Groq API キー	Groq 高性能 AI 推論プラットフォーム用の API キー	制限付き
Gumroad アクセストークン	Gumroad デジタル製品販売およびクリエイターコマースプラットフォーム API のトークン	極秘
Harness API Key	Harness CI/CD とソフトウェア配信プラットフォーム管理用のキー	制限付き
Hashicorp Terraform API トークン	Terraform Cloud/Enterprise インフラのコード化管理用のトークン	制限付き
Hashicorp Terraform パスワード	Terraform Enterprise またはバックエンドステートストレージアクセス用のパスワード	制限付き
Hashicorp Vault バッチトークン	HashiCorp Vault シークレット管理オペレーション用のバッチトークン	制限付き
Hashicorp Vault ルートトークン	すべての HashiCorp Vault シークレットへの無制限のアクセスを付与するルートトークン	制限付き
Hashicorp Vault サービストークン	アプリケーションレベルの HashiCorp Vault シークレットアクセス用のサービストークン	制限付き
Heroku API キー	Heroku PaaS プラットフォームアプリケーションのデプロイメントと管理用のキー	制限付き
Highnote シークレットライブキー	Highnote カード発行および決済処理プラットフォームのライブ秘密キー	制限付き

データタイプ	説明	重大度
Honeycomb API Key	Honeycomb 可観測性および分散トレースプラットフォームの API キー	極秘
HubSpot APIトークン	HubSpot CRM とマーケティングプラットフォーム API アクセス用のトークン	制限付き
Huggingface アクセストークン	Hugging Face AI モデルハブと推論 API アクセス用のトークン	制限付き
Huggingface 組織 API トークン	Hugging Face チームのモデルとデータセット管理のための組織レベルのトークン	制限付き
IBM Cloud ユーザー API キー	IBM Cloud プラットフォームインフラおよびサービス管理のユーザーレベル API キー	制限付き
InfluxDB APIトークン	InfluxDB 時系列データベースの読み取り/書き込み操作および管理用のトークン	極秘
Infomaniak APIトークン	Infomaniak クラウドホスティングおよび Web サービスプラットフォーム管理用のトークン	制限付き
インフラコスト APIトークン	Infracost クラウドインフラコスト予測サービス用のトークン	プライベート
Intercom API キー	Intercom カスタマーメッセージとサポートプラットフォーム API 用のキー	極秘
Intercom APIトークン	Intercom 顧客コミュニケーションプラットフォーム API アクセス用のトークン	極秘
Intra42 クライアントシークレット	42 School イントラネット API 認証用 OAuth クライアントシークレット	極秘

データタイプ	説明	重大度
Ionic 個人用アクセストークン	Ionic モバイルアプリ開発プラットフォームと Appflow サービスの個人用トークン	極秘
Java キーストア(.jks)	TLS/署名の秘密鍵と証明書を含む Java キーストアファイル	制限付き
Jenkins API トークン	ビルドとパイプラインを管理する Jenkins CI/CD サーバー API 用のトークン	制限付き
JFrog API キー	JFrog プラットフォームアーティファクト管理とバイナリリポジトリアクセス用のキー	制限付き
JFrog Identity トークン	サービス間での JFrog プラットフォーム認証のためのアイデンティティトークン	制限付き
JSON ウェブトークン (JWT)	ステートレス API 承認の認証クレームを保持する署名済みトークン	極秘
JSON ウェブトークン (JWT) Base64	API 承認のための認証クレームを保持する Base64 でエンコードされた JWT	極秘
JumpCloud API キー	JumpCloud アイデンティティとデバイス管理プラットフォームの API キー	制限付き
Kagi API Key	Kagi 検索エンジンと AI アシスタントサービスの API キー	極秘
Kimi API Key	Moonshot AI Kimi 言語モデルと会話型 AI サービスの API キー	制限付き
Klaviyo API キー	Klaviyo マーケティング自動化と顧客データプラットフォームの API キー	極秘
Kraken アクセストークン	Kraken 暗号通貨取引とアカウントアクセス用の API トー	制限付

データタイプ	説明	重大度
	クン	き
Kubernetes シークレット (YAML)	認証情報または証明書が含まれる可能性のある Kubernetes シークレットマニフェスト	制限付き
Kucoinアクセストークン	KuCoin 暗号通貨取引とアカウントアクセス用の API トークン	制限付き
Kucoin シークレットキー	KuCoin 交換 API リクエストに署名するためのシークレットキー	制限付き
LangSmith 個人用アクセストークン	LangSmith LLM 可観測性と評価プラットフォームの個人用トークン	極秘
LangSmith サービスキー	LangSmith の自動 LLM トレースとモニタリング操作のサービスキー	制限付き
Lark アプリのシークレット	Lark ワークプレイスコラボレーションプラットフォーム API 認証のアプリケーションシークレット	制限付き
Launchdarkly アクセストークン	LaunchDarkly 機能フラグ管理および実験プラットフォーム用のトークン	極秘
Lichess 個人アクセストークン	Lichess オープンソースチェスプラットフォームの API アクセス用の個人用トークン	プライベート
LightOn Paradigm API Key	LightOn Paradigm エンタープライズ AI モデルプラットフォームの API キー	制限付き
Linear API Key	Linear プロジェクト管理と課題追跡 API 用のキー	極秘
リニア API トークン	Linear プロジェクト管理 API アクセス用のトークン	極秘
線形クライアントシークレッ	Linear アプリケーション認証用の OAuth クライアントシーク	極秘

データタイプ	説明	重大度
ト	レット	
LinkedIn クライアント ID	LinkedIn OAuth 統合フロー用のパブリックアプリケーション識別子	パブリック
LinkedIn クライアントシークレット	LinkedIn OAuth サーバー側認証とトークン交換用のシークレット	極秘
Llamacloud API キー	LlamaCloud が管理する LLM および RAG サービス用の API キー	制限付き
Lob API キー	自動物理郵便のための Lob 印刷と郵便 API 用のキー	極秘
Lob 公開 API キー	Lob アドレス検証統合用のクライアント側の公開可能キー	パブリック
Looker クライアント ID	Looker BI プラットフォーム API 統合のクライアント識別子	プライベート
Looker クライアントシークレット	Looker BI およびアナリティクスプラットフォーム API 認証用のクライアントシークレット	極秘
Mailchimp API キー	Mailchimp メールマーケティングプラットフォームと連絡先リスト管理 API 用のキー	極秘
MailerSend API トークン	MailerSend のトランザクションメール配信と管理 API 用のトークン	極秘
Mailgun プライベート API トークン	Mailgun メール送信および管理 API 用のプライベートトークン	極秘
Mailgun 公開鍵	クライアント側の Mailgun メールアドレス検証用の公開鍵	パブリック

データタイプ	説明	重大度
Mailgun 署名鍵	Mailgun Webhook イベント署名を検証するためのキー	プライベート
MapBox API トークン	クライアント側でよく使用される MapBox マッピングおよびジオロケーションサービス用のトークン	プライベート
Mattermost アクセストークン	Mattermost チームのメッセージングおよびコラボレーションプラットフォーム API 用のトークン	極秘
Maxmind ライセンスキー	MaxMind GeoIP データベースダウンロードとウェブサービスアクセス用のライセンスキー	極秘
Mercury Production API トークン	Mercury バンキングと金融サービス API の本番トークン	制限付き
アプリケーションキーをマージファイ	Mergify の自動プルリクエストのマージとワークフロープラットフォームのアプリケーションキー	極秘
MessageBird API トークン	MessageBird 通信プラットフォーム SMS および音声 API 用のトークン	極秘
MessageBird クライアント ID	MessageBird API 統合のパブリッククライアント識別子	パブリック
Microsoft Teams Webhook	自動メッセージを Teams チャネルに送信するための受信 Webhook URL	極秘
Midtrans プロダクションサーバーキー	Midtrans ペイメントゲートウェイ処理用のサーバー側の本番キー	制限付き
MiniMax APIキー	MiniMax AI モデルおよびコンテンツ生成サービスの API キー	制限付き

データタイプ	説明	重大度
Mistral AI API キー	Mistral AI 言語モデルの推論およびチャットサービスの API キー	制限付き
MongoDB Atlas サービスアカウントシークレット	MongoDB Atlas が管理するデータベースプラットフォーム管理のサービスアカウントシークレット	制限付き
MongoDB 接続文字列	MongoDB データベースの認証およびアクセス用の認証情報を含む接続 URI	制限付き
Neon API キー	Neon サーバーレス Postgres データベースプラットフォーム管理用の API キー	制限付き
Netlify アクセストークン	Netlify ウェブホスティングとデプロイメントプラットフォーム管理 API 用のトークン	制限付き
New Relic Browser API トークン	New Relic の実際のユーザーをモニタリングするためのクライアント側ブラウザエージェントトークン	プライベート
New Relic Ingest Browser API トークン	New Relic のモニタリングテレメトリデータを取り込むためのブラウザに埋め込まれたトークン	プライベート
New Relic 挿入キー	カスタムイベントとメトリクスを New Relic に送信するための挿入専用キー	プライベート
New Relic Synthetics キー	New Relic Synthetics モニタリングスクリプト化ブラウザチェック用のキー	プライベート
New Relic ユーザー API ID	New Relic アカウント API アクセス用のユーザーレベルの識別子	極秘
New Relic ユーザー API キー	完全な New Relic アカウントとデータ管理 API アクセス用のユーザーレベルキー	極秘

データタイプ	説明	重大度
Notion APIトークン	ページとデータベースへのNotionワークスペースAPIアクセス用のトークン	極秘
NPMアクセストークン	NPMレジストリでパッケージを公開および管理するためのトークン	制限付き
Nuget APIキー	.NETパッケージをNuGetパッケージレジストリに公開するためのキー	制限付き
Nuget設定パスワード	プライベートパッケージフィードへのアクセスのためにNuGet設定に保存されたパスワード	制限付き
NVIDIA APIキー	Nvidiaクラウド AIおよびGPUコンピューティングサービス用のAPIキー	制限付き
nytimesアクセストークン	New York Timesの記事とデータAPIアクセスのためのトークン	プライベート
Octopus Deploy APIキー	Octopus Deployの自動デプロイメントおよびリリース管理プラットフォーム用のキー	制限付き
Oktaアクセストークン	Oktaアイデンティティアクセス管理プラットフォームAPI用のトークン	制限付き
Ollama APIキー	Ollamaローカルおよびホスト型 AIモデルの推論とサービングのAPIキー	制限付き
OneSignal認証トークン	OneSignalプッシュ通知およびメッセージングプラットフォームAPIのトークン	制限付き
Onfidoライブ APIトークン (CA)	カナダリージョンのOnfidoアイデンティティ検証サービス用のライブ APIトークン	制限付き

データタイプ	説明	重大度
Onfido Live APIトークン (EU)	EU リージョンの Onfido アイデンティティ検証サービス用のライブ API トークン	制限付き
Onfido Live APIトークン(米国)	US リージョンの Onfido アイデンティティ検証サービス用のライブ API トークン	制限付き
OpenAI API キー	OpenAI GPT と AI モデルエンドポイントの API キー	制限付き
OpenAI プロジェクト API キー	プロジェクトレベルの請求がある OpenAI サービスに対するプロジェクト範囲指定の API キー	制限付き
OpenRouter API キー	OpenRouter 統合 AI モデルルーティングおよびアクセスプラットフォームの API キー	制限付き
Openshift ユーザートークン	Red Hat OpenShift コンテナプラットフォームとクラスタ管理のユーザートークン	制限付き
OpenWeather API キー	OpenWeather 気象データおよび予報 API サービスの API キー	プライベート
OVH アプリケーションシークレット	OVH クラウドインフラおよびホスティングプラットフォーム API のアプリケーションシークレット	制限付き
Paddle Live API キー	Paddle のサブスクリプション請求および決済処理用のライブ API キー	制限付き
Perplexity API キー	Perplexity AI 検索および言語モデルサービス用の API キー	制限付き
ペルソナ本番 API キー	Persona アイデンティティ検証および KYC プラットフォーム用の本番 API キー	制限付き

データタイプ	説明	重大度
PGP メッセージ	機密性の高い暗号化コンテンツを含む PGP 暗号化メッセージブロック	プライベート
PGP 秘密鍵ブロック	復号化とデジタル署名操作に使用される PGP 秘密鍵	制限付き
Pinecone API キー	Pinecone ベクトルデータベースおよび類似性検索プラットフォームの API キー	制限付き
Pinterest アクセストークン	Pinterest ソーシャルメディアおよび広告プラットフォーム API アクセス用のトークン	極秘
PKCS12 ファイル (.p12、.pfx)	TLS/署名の秘密鍵と証明書を含む証明書バンドル	制限付き
Plaid API トークン	Plaid 財務データ集約とバンキング統合 API 用のトークン	制限付き
Plaid クライアント ID	Plaid 財務サービス API 統合のクライアント識別子	極秘
チェック柄の秘密鍵	銀行口座データにアクセスするための Plaid API 認証のシークレットキー	制限付き
Planetscale APIトークン	PlanetScale サーバーレス MySQL データベースプラットフォーム管理用のトークン	制限付き
Planetscale データベースのパスワード	PlanetScale データベースブランチエンドポイントに接続するためのパスワード	制限付き
Planetscale OAuthトークン	PlanetScale データベースプラットフォーム API アクセス用の OAuth トークン	制限付き
Planetscale パスワード	PlanetScale データベース認証用の一般パスワード	制限付

データタイプ	説明	重大度
		き
Plivo 認証トークン	Plivo クラウド通信 SMS および音声 API の認証トークン	制限付き
Polar OAuthアクセストークン	Polar オープンソースファンディングおよび収益化プラットフォーム用の OAuth トークン	極秘
Polar 組織のアクセストークン	Polar オープンソース収益化プラットフォーム管理用の組織範囲指定トークン	極秘
Polar 個人アクセストークン	Polar 開発者向けファンディングおよびオープンソースプラットフォーム API の個人用トークン	極秘
Polymarket API キー	Polymarket 予測市場およびイベント取引プラットフォームの API キー	極秘
Polymarket 秘密鍵	Polymarket 予測市場の商取引に署名するための秘密キー	制限付き
Polymarketウォレットアドレス	Polymarket 予測市場 API 認証のコンポーネント資格情報として使用されるイーサリアム ウォレット アドレス	プライベート
Postgres データベースパスワード	PostgreSQL データベースインスタンスに対して認証するためのパスワード	制限付き
PostHog 個人用 API キー	PostHog 製品分析および機能フラグプラットフォームの個人用 API キー	極秘
PostHog プロジェクト API キー	PostHog のイベントの取り込みと分析用のプロジェクトレベル API キー	プライベート
Postman API トークン	コレクションとワークスペースを管理する Postman API プ	極秘

データタイプ	説明	重大度
	ラットフォーム用のトークン	
Powershell 変数パスワード	PowerShell 変数またはスクリプトに保存されているパスワード	制限付き
Prefect API トークン	Prefect ワークフローオーケストレーションとデータパイプライン管理 API 用のトークン	極秘
プライベートキー (RSA/PEM)	TLS、SSH、コード署名に使用される PEM 形式の RSA 秘密鍵	制限付き
Privateai API トークン	プライベート AI PII 検出およびリダクションサービス API 用のトークン	制限付き
証明のフルアクセス API キー	Proof アイデンティティ検証および公証プラットフォーム用のフルアクセス API キー	制限付き
Pubnub サブスクライブキー	PubNub リアルタイムメッセージングチャネルに登録するためのクライアント側のキー	プライベート
Pulumi API トークン	Pulumi インフラのコード化クラウド管理プラットフォーム用のトークン	制限付き
PuTTY (PPK) プライベートキー	リモートサーバーへの SSH 認証に使用する PuTTY 秘密鍵ファイル	制限付き
PyPI アップロードトークン	Python パッケージを PyPI パッケージレジストリに公開するためのトークン	制限付き
Rainforest Pay Production API キー	Rainforest Pay 決済処理およびマーチャントサービスの本番 API キー	制限付き
ランプクライアントシークレッ	Ramp コーポレートカードおよび支出管理プラットフォーム	制限付

データタイプ	説明	重大度
ト	API のクライアントシークレット	き
RapidAPI アクセストークン	サードパーティ API サブスクリプションにアクセスするための RapidAPI マーケットプレイス用のトークン	極秘
Readme API トークン	Readme 開発者ドキュメントプラットフォーム管理 API 用のトークン	プライベート
Redirect.pizza API トークン	Redirect.pizza URL リダイレクトおよびドメイン転送管理のトークン	極秘
API キーのレンダリング	Render クラウドホスティングおよびアプリケーションデプロイメントプラットフォームの API キー	制限付き
API トークンの複製	Replicate クラウド AI モデルホストおよび推論 API 用のトークン	制限付き
Rootly API キー	Rootly インシデント管理および対応自動化プラットフォームの API キー	極秘
RSA Private Key	復号化、デジタル署名、SSH 認証に使用される RSA 秘密鍵	制限付き
Rubygems API トークン	RubyGems レジストリで Ruby gems を公開および管理するためのトークン	制限付き
RunPod API キー	RunPod GPU クラウドコンピューティングおよび AI インフラプラットフォームの API キー	制限付き
ランタイムシークレット	bash 履歴のシークレット検出 (実行コマンド)	制限付き
Salesforce アクセストークン	顧客データとビジネスオブジェクトへのユーザーレベルのア	制限付

データタイプ	説明	重大度
	クセスを許可する、Salesforce CRM API のアクセストークン	き
Salesforce リフレッシュトークン	顧客データへの永続的な Salesforce CRM API アクセス用の更新トークン	制限付き
Samsara API トークン	Samsara フリート管理および産業用 IoT プラットフォーム API のトークン	極秘
Scaleway シークレットキー	Scaleway 欧州クラウドインフラおよびコンピューティングサービスの秘密キー	制限付き
Scalingo API トークン	Scalingo European PaaS プラットフォームのデプロイメントと管理用のトークン	制限付き
Scalr API アクセストークン	Scalr Terraform 自動化およびインフラ管理プラットフォームのトークン	制限付き
秘密キー	トークンの生成と認証のための永続的なシークレット	制限付き
公開 API トークンのセグメント化	Segment 顧客データプラットフォームイベント収集用のパブリック API トークン	プライベート
Sendbird アクセス ID	Sendbird アプリ内メッセージングプラットフォームのアプリケーション識別子	プライベート
Sendbird アクセストークン	Sendbird アプリ内チャットとメッセージングプラットフォーム API アクセス用のトークン	極秘
Sendgrid API トークン	SendGrid トランザクションとマーケティングメール配信 API 用のトークン	極秘

データタイプ	説明	重大度
Sendinblue APIトークン	Brevo (Sendinblue) メールマーケティングとCRM プラットフォーム API 用のトークン	極秘
機密性の高いURL	機密性の高いパス、認証パラメーター、または埋め込まれたトークンを含むURL の検出	制限付き
Sentry アクセストークン	Sentry のエラー追跡とアプリケーションモニタリングプラットフォーム API 用のトークン	極秘
セントリー組織トークン	Sentry エラー追跡プラットフォーム管理用の組織範囲指定のトークン	極秘
Sentry ユーザートークン	Sentry アプリケーションモニタリング API アクセス用のユーザー範囲指定のトークン	極秘
Settlemint アプリケーションアクセストークン	SettleMint ブロックチェーンプラットフォーム API アクセス用のアプリケーショントークン	極秘
Settlemint 個人アクセストークン	SettleMint ブロックチェーン開発プラットフォーム API 用の個人用トークン	極秘
Settlemint サービスアクセストークン	SettleMint ブロックチェーンミドルウェアと API アクセス用のサービストークン	極秘
シェルパスワード	シェルコマンドまたはスクリプトに埋め込まれたパスワード	制限付き
Shippo APIトークン	Shippo マルチキャリア配送とロジスティクス API 用のトークン	極秘
Shopifyアクセストークン	顧客の PII と注文を含む Shopify ストアデータへのアクセス権を付与するトークン	制限付き

データタイプ	説明	重大度
Shopifyカスタムアクセストークン	コマースデータと顧客データへのShopifyストアAPIアクセス用のカスタムアプリトークン	制限付き
Shopifyプライベートアプリアクセストークン	Shopifyストアバックエンド APIと顧客データアクセス用のプライベートアプリトークン	制限付き
Shopify共有シークレット	Shopify Webhook署名とアプリの信頼性を検証するための共有シークレット	プライベート
Sidekiqシークレット	Sidekiqバックグラウンドジョブ処理ウェブダッシュボードを保護するためのシークレット	極秘
Sidekiqの機密性の高いURL	Sidekiq Redis接続またはウェブインターフェースの認証情報を含むURL	極秘
Slackアプリトークン	ワークスペースメッセージングとデータへのSlackアプリAPIアクセス用のトークン	制限付き
Slackアプリレベルのトークン	Slack WebSocket接続とイベントサブスクリプション用のアプリレベルトークン	制限付き
Slackボットトークン	Slackワークスペースメッセージングとチャネル操作用のボットユーザートークン	制限付き
Slack設定アクセストークン	Slackアプリ設定とマニフェスト管理 API用のトークン	制限付き
Slack設定リフレッシュトークン	Slack設定アクセストークンを更新するための更新トークン	制限付き
Slackレガシーボットトークン	Slack APIワークスペースアクセス用の非推奨ボットトークン	制限付き

データタイプ	説明	重大度
Slack レガシートークン	Slack API フルワークスペースアクセス用の非推奨レガシートークン	制限付き
Slack レガシーワークスペーストークン	Slack 管理 API オペレーション用のワークスペースレベルの非推奨トークン	制限付き
Slack セッション Cookie	ブラウザセッション Cookie により、再認証なしですべてのユーザーワークスペースにわたって永続的な Slack 認証が有効になります	制限付き
Slack セッショントークン	セッション Cookie とペアの場合、ユーザーレベルの Slack API に完全にアクセスできるセッショントークン	制限付き
Slack ユーザートークン	認証ユーザーとして機能する Slack API アクセス用のユーザーレベルトークン	制限付き
Slack Webhook	自動メッセージを Slack チャンネルに投稿するための Incoming Webhook URL	極秘
Slack Webhook URL	自動通知を Slack チャンネルに送信するための URL エンドポイント	極秘
Slack ワークフロー Webhook	Slack Workflow Builder の自動化をトリガーするための Webhook URL	極秘
Snowflake プログラムによるアクセストークン	Snowflake クラウドデータウェアハウスおよび分析プラットフォーム用のプログラムトークン	制限付き
Snyk API トークン	コードの依存関係とコンテナイメージの Snyk セキュリティスキャン用のトークン	制限付き
Sonar API トークン	SonarQube/SonarCloud コードの品質およびセキュリティ分析プラットフォーム用のトークン	極秘

データタイプ	説明	重大度
Sourcegraph アクセストークン	Sourcegraph コード検索およびインテリジェンスプラットフォーム API 用のトークン	極秘
Square アクセストークン	Square 決済処理と POS API アクセス用のトークン	制限付き
Square OAuth シークレット	Square 決済プラットフォームのサーバー側認証用の OAuth シークレット	制限付き
Squarespace アクセストークン	Squarespace ウェブサイトと e コマースプラットフォーム API 管理用のトークン	極秘
SSLMate API キー	SSLMate 証明書管理およびモニタリングサービスの API キー	極秘
安定性 AI API キー	Stability AI 画像生成およびクリエイティブ AI モデルサービスの API キー	制限付き
Stripe アクセストークン	Stripe 決済処理プラットフォーム API アクセス用のトークン	制限付き
Stripe API キー	Stripe 決済ゲートウェイと財務業務の API キー	制限付き
Stripe Secret Key	Stripe の決済処理とアカウント管理のためのサーバー側のシークレットキー	制限付き
Sumologic アクセス ID	Sumo Logic ログ管理と分析プラットフォームのアクセス識別子	極秘
Sumologic アクセストークン	Sumo Logic クラウド SIEM とログ分析 API アクセス用のトークン	極秘

データタイプ	説明	重大度
Supabase 管理トークン	Supabase プラットフォームレベルのプロジェクトおよびデータベース管理用の管理トークン	制限付き
Supabaseプロジェクト API キー	Supabase Backend-as-a-Service データベースおよび認証用のプロジェクトレベル API キー	極秘
Tableau 個人用アクセストークン	Tableau データ視覚化および分析プラットフォーム API の個人用トークン	極秘
Tailscale API キー	Tailscale メッシュ VPN およびネットワークアクセス管理プラットフォームの API キー	制限付き
Teamwork API キー	Teamwork プロジェクト管理およびコラボレーションプラットフォーム API 用のキー	極秘
Telegram Bot API トークン	Telegram ボットを制御し、メッセージング API にアクセスするためのトークン	極秘
Telnyx API キー	Telnyx クラウド通信、SMS、および音声テレフォニーサービスの API キー	極秘
Temporal Cloud API Key	Temporal Cloud ワークフローオーケストレーションおよびマイクロサービスプラットフォームの API キー	制限付き
Thunderstore API トークン	Thunderstore ゲーム mod リポジトリの公開および管理用トークン	極秘
Tines Webhook	Tines セキュリティ自動化ワークフローをトリガーするための Webhook URL	極秘
Together AI API キー	Together AI オープンソースモデル推論および微調整プラットフォームの API キー	制限付き

データタイプ	説明	重大度
トークン	認証に使用される一時的なシークレット	制限付き
Travis CI アクセストークン	Travis CI の継続的な統合とビルドプラットフォーム API のためのトークン	制限付き
Twilio API キー	Twilio 通信プラットフォーム SMS、音声およびビデオ API 用のキー	極秘
Twitch API トークン	Twitch ストリーミングプラットフォーム API アクセスとボットオペレーション用のトークン	極秘
Twitter アクセスシークレット	Twitter/X API 認証リクエスト用の OAuth アクセスシークレット	極秘
Twitter アクセストークン	Twitter/X API ユーザーレベル操作用の OAuth アクセストークン	極秘
Twitter API キー	Twitter/X アプリケーション認証用のコンシューマー API キー	極秘
Twitter API シークレット	Twitter/X アプリケーションサーバー側認証用のコンシューマーシークレット	極秘
Twitterベアラートークン	Twitter/X API 読み取りレベルアクセス用のアプリ専用 Bearer トークン	極秘
Typeform API トークン	Typeform アンケートとフォームビルダープラットフォーム API アクセス用のトークン	極秘
Ubidotsトークン	Ubidots IoT データ分析およびデバイス管理プラットフォーム用のトークン	プライベート

データタイプ	説明	重大度
root キーのキーを解除する	Unkey API キー管理およびレート制限インフラのルートキー	制限付き
UpCloud API トークン	UpCloud 欧州クラウドインフラおよびサーバー管理用トークン	制限付き
Upstage API キー	Upstage AI ドキュメント理解および LLM サービスの API キー	制限付き
Val Town API トークン	Val Town サーバーレス JavaScript 関数のホスティングおよび実行プラットフォーム用のトークン	極秘
Vault バッチトークン	HashiCorp Vault シークレットエンジンオペレーション用のバッチトークン	制限付き
ボールトサービストークン	アプリケーションレベルの HashiCorp Vault シークレットアクセス用のサービストークン	制限付き
Vercel AI ゲートウェイキー	Vercel AI SDK ルーティングとモデルプロバイダーアクセス用のゲートウェイキー	制限付き
Vercel APIトークン	Vercel デプロイメントプラットフォームとプロジェクト管理 API のトークン	制限付き
Vercelアプリアクセストークン	Vercel プラットフォームリソースアクセス用のアプリケーション範囲指定トークン	制限付き
Vercelアプリリフレッシュトークン	Vercel アプリケーションアクセストークンを更新するための更新トークン	制限付き
Vercel 統合トークン	Vercel マーケットプレイスの統合とサードパーティアプリへのアクセス用トークン	制限付き

データタイプ	説明	重大度
Vercel 個人アクセストークン	Vercel デプロイメントとプロジェクト管理 API アクセス用の個人用トークン	制限付き
WakaTime API キー	WakaTime 開発者の生産性とコーディング時間追跡の API キー	極秘
Weatherstack API キー	Weatherstack リアルタイムと過去の気象データサービスの API キー	プライベート
重みと偏り API キー	Weights & Biases の ML 実験追跡とモデル管理の API キー	制限付き
Workato 開発者 API トークン	Workato エンタープライズ自動化と統合プラットフォームの開発者トークン	制限付き
WorkOS 本番環境 API キー	WorkOS のエンタープライズ認証とディレクトリ同期用の本番 API キー	制限付き
X.AI API キー	xAI Grok 言語モデルと AI サービスエンドポイント用の API キー	制限付き
Yandex アクセストークン	Yandex クラウドとサービスプラットフォーム API アクセス用のトークン	極秘
Yandex API キー	Yandex 開発者サービスと API アクセス用のキー	極秘
Yandex AWS アクセストークン	バケット用の AWS S3 API と互換性のある Yandex Cloud アクセストークン	制限付き
Zai API Key	Zai 決済インフラと金融サービスプラットフォームの API キー	制限付き
Zapier Webhook	Zapier 自動化ワークフローをトリガーするための	極秘

データタイプ	説明	重大度
	Webhook URL	
Zendesk Secret Key	Zendesk カスタマーサポートおよびヘルプデスクプラットフォーム API のシークレットキー	極秘
Zuplo コンシューマー API キー	Zuplo API ゲートウェイと管理プラットフォームのコンシューマー API キー	極秘

データスキャンコスト

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

データスキャンにより、クラウドプロバイダーから追加のストレージコストや処理コストが発生する場合があります。これらのコストは、サポートされているリソースとスキャンのアプローチ (直接スキャンか間接スキャンか) によって異なります。

直接スキャンの推定コスト

- **AWS**、**Azure**、**GCP**、**OCI**、**Alibaba Cloud**: 直接スキャン では、スキャンの最適化とサンプリング戦略を使用して、コストを無視できるレベルに削減します。
- **Snowflake** (Enterprise ライセンスで利用可能): コストを低く抑えるために、Tenable はスキャンに X-Small ウェアハウスを使用し、必要な場合にのみ実行します。詳細については、請求明細書を参照するか、Snowflakeの価格を参照してください。

間接スキャンの推定コスト

間接スキャン は、マネージドデータベースの一時的なスナップショットを作成し、ライブデータベースに直接アクセスせずに機密データをスキャンします。スナップショットの存続期間が短く、不要になったらすぐに削除されるようにスキャンプロセスが最適化されていますが、クラウドプロバイダーは、スナップショットがアカウントに保存されている期間に対して課金する場合があります。

次の点に注意してください。

- 料金は、スナップショットのサイズ、スキャンされたデータベースの数、スキャン頻度などの要因によって異なります。
- スキャンはリソースと同じリージョンで実行されるため、エグレス料金はかかりません。

クラウドプロバイダーおよびサービス別のコスト

- **ほとんどのクラウドプロバイダー:**
  - 一時スナップショットがアカウントで作成され、Tenable の地域のアウトポストに転送されます。
  - 200 個のマネージドデータベース (それぞれ平均 100 GiB) をスキャンする場合、データスキャンで発生する可能性のある推定コストは **1 か月あたり 100 ドル**です。価格の詳細については、AWS Backup Pricing または GCP Pricing を参照してください。

    > **注意: AWS**: 保持ルール (AWS ごみ箱など) を使用する場合、追加料金が表示される場合があります。

- Azure
  - 一時的なスナップショットは、Tenable の地域のアウトポスト内で直接作成されます。
  - アカウントにはスナップショットは作成されないため、**追加費用はかかりません**。

ワークロードベースのスキャンの推定コスト

スキャンから仮想マシンを除外するとワークロードのワークロードベースのデータスキャンでは、既存の**ワークロード保護**の脆弱性スキャンワークフローを活用します。

つまり、仮想マシンのデータスキャン **によって、ワークロード保護のスキャンで発生するコストを超える追加コストが発生することはありません**。

ワークロード保護スキャンの一部としてのスナップショット関連コストの計算方法の詳細については、スナップショットスキャン費用計算ツールを参照してください。

データリソースのアカウント内スキャン

注意: この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

データスキャンが Tenable One Cloud Exposure によってホストされているマシンで実行される標準のデプロイメントの代わりに、Tenable はアカウント内データスキャンもサポートしています。このスキャンはお使いの環境で (専用アカウントを使用して) 実行され、データが環境外に出ることはありません。

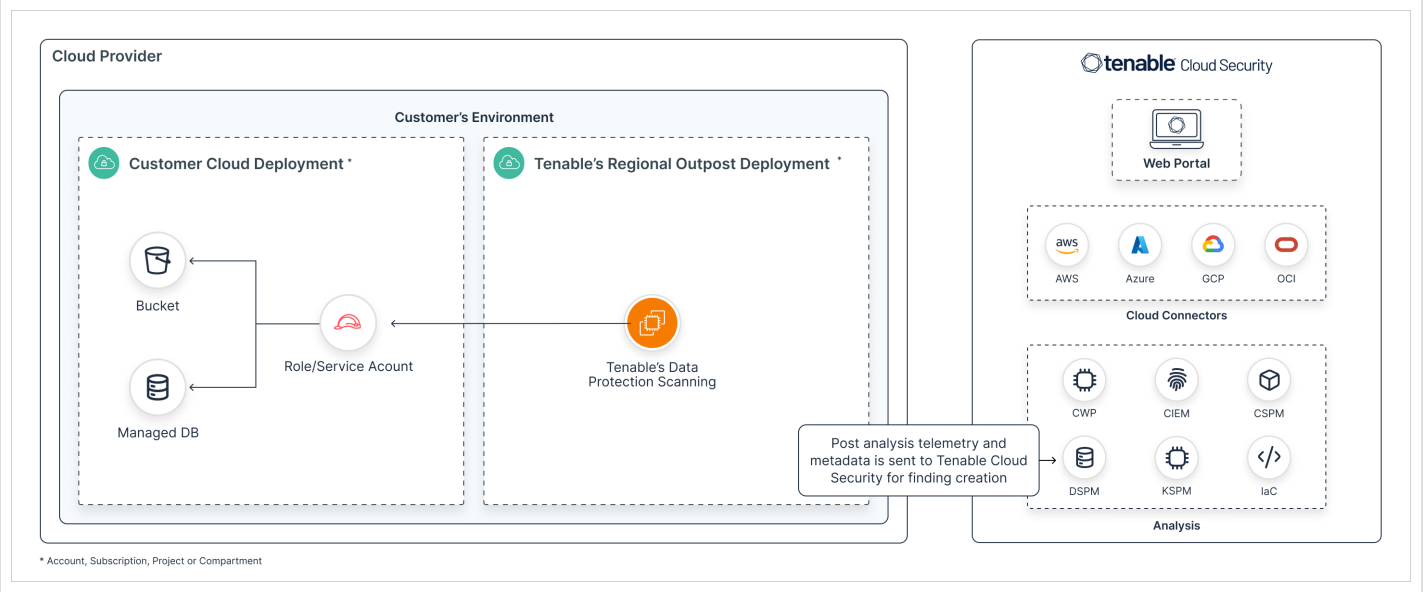
サポートされているすべてのリソースタイプを表示し、アカウント内スキャンがサポートされているかどうかを確認するには、「サポートされているリソースとスキャン方法」を参照してください。

アカウント内直接スキャン

クラウドサイバーエクスポージャーは、スキャン目的で API を利用してクラウドリソースに接続します。

- 付与されたロール/サービスアカウントを利用して、Tenable のアカウント内アウトポストはオブジェクト (バケット内) とテーブル (マネージドデータベース内) をスキャンし、データを機密性の高いデータタイプに分類します。
- テレメトリとメタデータ (特定のデータタイプの存在と場所) はアウトポストで収集され、グローバルクラウドサイバーエクスポージャープラットフォームに送信されますが、機密データが他の場所に保存される **ことはありません** 。
- オブジェクトやテーブルにセンシティブデータが存在すると、それらのオブジェクトやテーブルが検出されたリソースに関連する検出結果の深刻度に影響を与えます。

次の図では、サポートされているすべてのクラウドプロバイダーに関する直接アカウント内スキャンのワークフローを示しています。

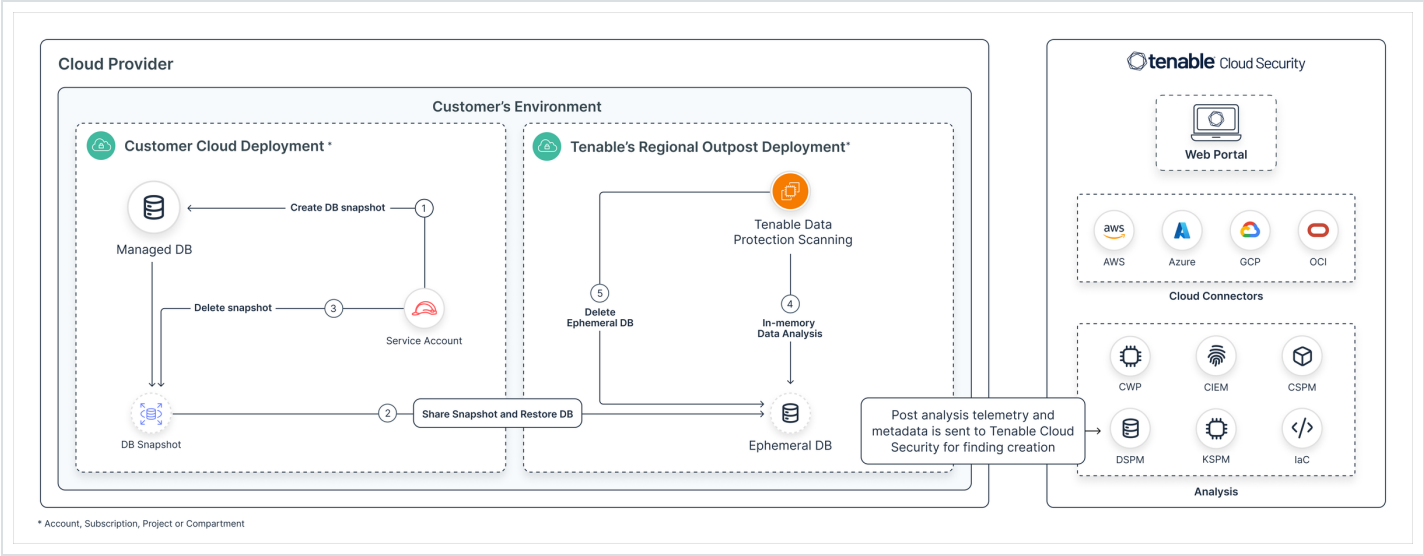


間接アカウント内スキャン

クラウドサイバーエクスポージャーはスキャン目的でクラウドリソースのスナップショットまたはバックアップを利用します。

- 付与されたロールまたはサービスアカウントを利用して、マネージドデータベースのスナップショットまたはバックアップをTenableのアカウント内アウトポストと共有し、DBテーブルをスキャンして、データをセンシティブデータタイプに分類します。
- テレメトリとメタデータ(特定のデータタイプの存在と場所)はアウトポストで収集され、グローバルクラウドサイバーエクスポージャープラットフォームに送信されますが、機密データが他の場所に保存される**ことはありません**。
- テーブルにセンシティブデータが存在すると、それらのテーブルが検出されたリソースに関連する検出結果の深刻度に影響を与えます。

次の図では、サポートされているすべてのクラウドプロバイダーに関する間接アカウント内スキャンのワークフローを示しています。



よくある質問 - データ保護

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

以下は、Tenable One Cloud Exposure 内のデータ保護に関連するよくある質問です。

対象プラットフォーム/環境

このセクションでは、サポートされるリソースタイプ、ファイル形式、データタイプを含む、クラウドサイバーエクスポージャーのデータスキャンの範囲について概要を説明します。

スキャンされるリソースタイプ

> Tenable はどのリソースタイプをスキャンしますか?

回答: サポートされているリソースタイプのリストについては、スキャン済みリソースタイプを参照してください。

スキャンされたファイル形式

> Tenable はどのファイル形式をスキャンしますか?

回答: サポートされているファイル形式のリストについては、スキャン対象ファイル形式参照してください。

スキャンされるデータタイプ

> Tenable はどのデータタイプを分類しますか?

回答: サポートされているビルトインデータタイプのリストについては、スキャン対象データタイプ参照してください。データこともできます。

データスキャン頻度

> Tenable はどのくらいの頻度で、リソースのデータをスキャンしますか?

回答: スキャン頻度は、リソースタイプ、サイズ、データの更新などの複数の要因によって異なります。一般的に、スキャンは 2 ~ 7 日に 1 回実行されます。この頻度の変更に関する詳細は、サポートへの問い合わせ。を参照してください。

スキャン後の請求が無効になっている

> リソースのスキャンが無効になった場合、または不可能になった場合、請求はどうなりますか?

回答: リソースがスキャンされるとすぐに請求対象のリソース開始されます。次のいずれかが発生した場合

- スキャンは後で無効になる
- リソースがオプトアウトされています
- クラウドサイバーエクスポージャーリソースへのアクセスが失われる

クラウドサイバーエクスポージャーは、通常のスキャンサイクル中に最大 2 回リソースのスキャンを試行します。これらの試行後もリソースがスキャンできない場合、そのリソースは請求レポートから削除されます。

> **注意:** 請求はリソースの平均使用量に基づいています。詳細については、クラウドセキュリティライセンスの使用状況を参照してください。

データストレージポリシー

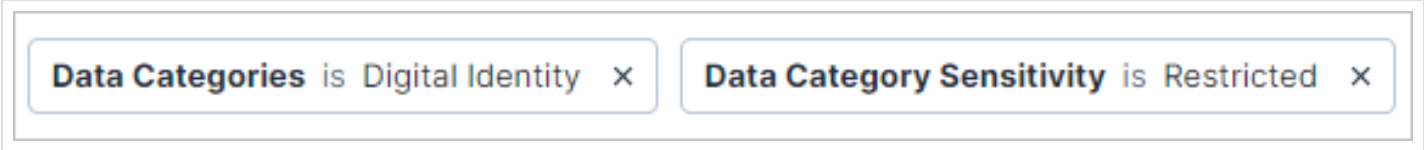
> Tenable データは保存されますか?

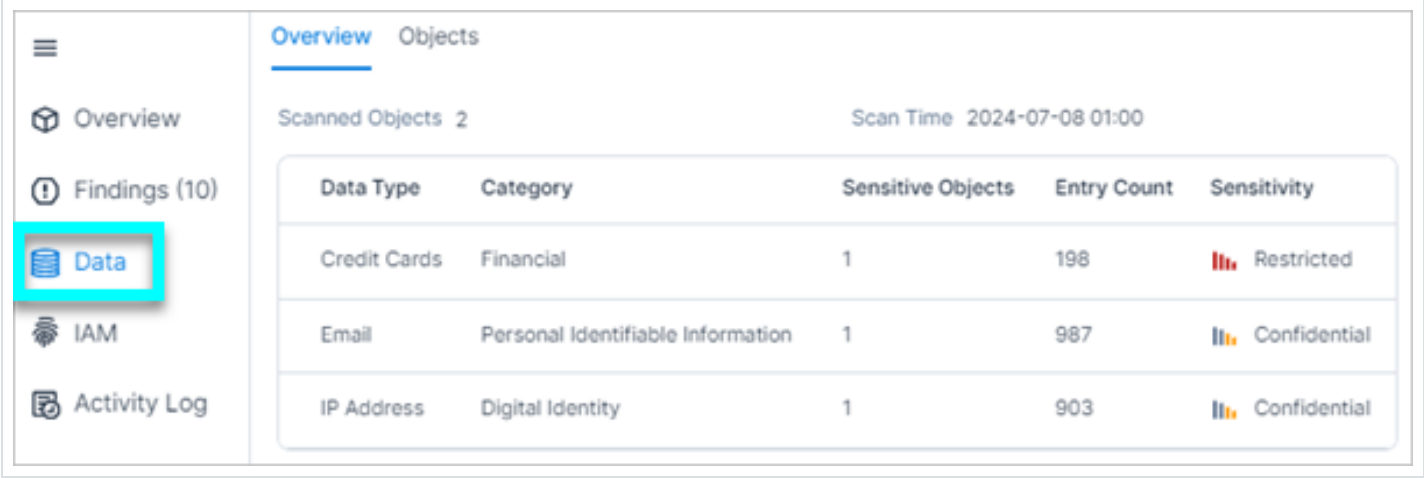
回答: いいえ。テレメトリとメタデータ特定のデータタイプの存在と場所が outpost で収集され、グローバルクラウドサイバーエクスポージャープラットフォームに送信されますが、機密データが他の場所に保存されることはありません。

検出されたデータの表示

> クラウドリソースで検出されたデータに関する情報は、どこで確認できますか?

回答: はい。スキャンされたリソースタイプの [インベントリ] ビューで、データカテゴリ情報でフィルタリングすることで、機密データを持つリソースを表示できます。次に、特定のリソースのプロファイルビューで、**[データ]** タブに移動します。詳しくは、データリソース参照してください。





正規表現とデータ分類

> 既存のデータタイプがニーズを完全に満たしていない場合はどうすればよいですか?

データ か、データできます。

> 特定のタイプのデータのカスタム正規表現クエリを追加できますか?

データ 、自社に固有の機密データの検出正規表現を定義できます。

> メールアドレスやアカウント ID など、特定の値を除外できますか?

はい。データタイプ を使用して、特定の値をデータタイプの分類から除外できます。

たとえば、そのデータタイプの他のすべての値をスキャンして分類しながら、既知のテストメールアドレス、サービスアカウント、内部識別子を除外することができます。

データ保護のアクセス許可

> クラウドサイバーエクスポージャー がデータスキャンの書き込みアクセス許可を必要とする場合があるのはなぜですか? 読み取り専用権限だけではだめですか?

回答: Tenable は、必要最小限の権限、主に読み取り専用の権限を使用することを目的としています。ただし、一部のサービスでは、間接スキャンを有効にするために制限付きの書き込みアクセス許可が必要です。これらのアクセス許可により、バックアップの作成やネットワークアクセスの調整など、範囲指定された操作が可能になります。

現在は、以下の書き込みアクセス許可が必要です。

クラウド	リソース	アクセス許可	詳細

AWS	RDS クラスターとインスタンス	`rds:CreateDBClusterSnapshot`
		`rds:CreateDBSnapshot`
		`rds:ModifyDBClusterSnapshotAttribute`
		`rds:ModifyDBSnapshotAttribute`
			間接データスキャンを有効にするデータベーススナッ

クラウド	リソース	アクセス許可	詳細
			プショットを作成する
Azure	ストレージ Account Blob Container	`Microsoft.Storage/storageAccounts/privateEndpointConnections/write`	ネットワーク制限のあるストレージアカウント Blob コンテナの場合、Tenable はプライベートエンドポイントを使用して、保存されたオブジェクトにアクセスします。このアクセス許可は、Tenable によって開始された保留中のプライベートエンドポイント接続リクエストを承認するために必要です。

クラウド	リソース	アクセス許可	詳細
Azure	SQL Server	`Microsoft.Sql/servers/databases/write`	間接データスキャンを有効にするためにデータベースバックアップを作成する

> クラウドサイバーエクスポージャーにはOCI用の一意のデータ保護権限が必要ですか?

回答: いいえ。クラウドサイバーエクスポージャーは、OCIテナンシの接続時に定義されているものと同じアクセス許可を使用します。OCIリソースをスキャンするためにクラウドサイバーエクスポージャーへのアクセスをすでに設定している場合、データ保護に追加のアクセス許可は必要ありません。

暗号化されたデータベースのスキャン

> クラウドサイバーエクスポージャーは、データベースやオブジェクトストレージなどの暗号化されたリソースのスキャンをサポートしていますか?

回答: クラウドサイバーエクスポージャーは、クラウドサービスプロバイダー(CSP)暗号化オプションを利用して、データベースやオブジェクトストレージなどの暗号化されたリソースのDSPMスキャンをサポートします。ただし、顧客が管理するキー(CMK)は現在、スキャンではサポートされていません。

スキャンステータスのトラブルシューティング

> スキャン失敗ステータスを解決する方法

回答: 失敗したスキャンのツールチップに**アクセス許可がないこと**が示されている場合は、データスキャンにデータリソースの接続を確認し、それらがリソースレベルで付与されていることを確認してください。

注意: 権限が不足している場合は、リソースレベルで有効な権限を確認し、上記のリンクで説明されているように、不足している権限を付与します。

[サポートされていない] ステータスを解決するにはどうすればよいですか?

回答: **[Not Supported]** ステータスは、設定、暗号化方法またはサービス層が原因で、リソースを現在スキャンできないことを示します。このタイプのリソースにサポートを追加する必要があると思われる場合は、リクエストを送信して、当社の製品チームに確認させることができます。詳細については、サポートされているリソースを参照してください。

ステータスが [無効] の解決方法

回答: **無効の** ステータスは、特定のアカウントスコープのスキャン設定で、またはデータスキャンの除外によって、リソースのデータスキャンがオフになっていることを意味します。スキャンを再度有効にするには、スキャン範囲を確認し、**[データスキャン除外]** タブをチェックして、ルールが特定のリソースをターゲットにしているかどうかを確認します。

ストレージアカウント Blob コンテナのアクセス許可がない問題はどのように解決しますか?

回答: ブロブコンテナのアクセス許可の問題を解決するには、次の手順を実行してください。

- Tenable データロールと必要なビルトインロールは、リソースレベルで付与されます。
- ブロブコンテナ、そのリソースグループ、またはサブスクリプションで拒否割り当てがデータアクセスを防止されていません。
- ストレージアカウントのネットワークアクセスが制限されていないある場合は、データを有効にすることを検討してください。

テストデータとシンセティックデータ

テストデータまたは合成データが分類されなかったのはなぜですか?

回答: クラウドサイバーエクスポージャーは、実在する機密データを検出するように設計されています。テスト値 (例: 1234-1234-1234-1234、support@example.com) や既知のテストパターン (公開クレジット

カードテスト番号など) は分類されません。同様に、合成データ (機密性の高い値の構造に従いますが、実際の識別子は含まれていないデータ) も分類から除外されます。

これにより、高い精度を確保し、誤検出を減らすことができます。プラットフォームをテストしている場合は、実在するコンテンツに似た実際の (ただし機密性が低い) データサンプルを使用することを推奨します。

> **注意:** テストおよび合成データは、実際のデータに似ていますが、真の機密情報の既知のパターンと一致しない限りは分類されません。

定期スキャンとメンテナンス

> クラウドサイバーエクスポージャーが専用タスクを使用するのはなぜですか? 無効にするとどうなりますか?

クラウドサイバーエクスポージャーは Snowflake のスケジュールされたタスクを使用して、新しく検出されたデータベースを自動的に接続します。タスクを無効化または削除するとスキャンの実行が停止し、クラウドサイバーエクスポージャーがアカウントのデータ保護の検出結果を更新できなくなります。

> 「データ保護のアクセス許可なし」のステータスを解決するにはどうすればよいですか?

アカウントのステータスがデータ保護のアクセス許可なしの場合、以下の手順を実行します。

- 統合スクリプトを再実行し、必要なロールとアクセス許可を再適用します。
- ネットワークアクセスが正しく設定されていて、クラウドサイバーエクスポージャーの IP アドレスが許可されることを確認します。詳細については、ネットワークアクセス権の付与を参照してください。

データベースの範囲と検出

> クラウドサイバーエクスポージャーは新しいデータベースの自動検出と統合をサポートしていますか?

はい。スケジュールされたタスクが有効になっている場合、クラウドサイバーエクスポージャーは、Marketplace を通じて共有されているものや、他のアカウントから共有されているものを含め、Snowflake で新しく作成されたデータベースを自動的に検出して接続します。

新しい Snowflake アカウントを接続する場合は、必要なアクセス許可を付与し、そのアカウント用の統合プロセスを別途完了する必要があります。

> アカウント内スキャンは Snowflake でサポートされていますか?

いいえ。データリソースのアカウント内スキャンは、Snowflake でサポートされていません。すべてのスキャンは、Tenable One Cloud Exposure が関連するクラウドリージョンから外部で実行します。

アーキテクチャと地域の挙動

> Spring アカウントデータベースが クラウドサイバーエクスポージャー スキャンされるのはどのリージョンからですか?

Data Protection スキャンは常に、Snowflake アカウントと同じクラウドプロバイダーおよびリージョンから実行されます。

たとえば、Snowflake アカウントが AWS `us-east-1`にある場合 Tenable は AWS からスキャンします `us-east-1`。これにより、リージョンが一致することを確認し、データの所在地の要件をサポートします。

データ境界と監視データのスプロール

> 環境内のデータのスプロールを監視するためにデータ境界を定義するにはどうすればよいですか?

クラウドサイバーエクスポージャーで **カスタムポリシーテンプレート** を使用して、データ境界を定義して適用できます。これらのポリシーは、開発アカウント、パブリックストレージ、その他の認証されていない環境など、定義された境界外や制限された境界内で、秘密データが存在すべきでない場所に秘密データが格納されているのを検出するのに役立ちます。

データのスプロールを監視するには、**[慎重な扱いが必要なデータの監視]** カテゴリで、次のいずれかのテンプレートを使用してカスタムポリシーを作成します。

- **この機密データはこれらのリソースに存在するべきではありません**: 存在すべきでない定義された境界内で機密データが見つかったときに、検出結果を生成します。

- **この機密データは、次のリソースにのみ存在する必要があります**: 定義された境界外で機密データが見つかった場合に、検出結果を生成します。

1. **[リスク] > [クラウドポリシー]** に移動し、**[カスタム]** タブを開きます。
2. **[カスタムポリシーの追加]** をクリックします。
3. **[Choose Policy Template] (ポリシーテンプレートを選択)** 画面で、**[Monitor Sensitive Data] (機密データの監視)** を選択します。
4. 関連するテンプレートを選択し、**[Next]** をクリックします。
5. ポリシー名を入力します (**オプション**)。
6. **[深刻度]** を選択します。これは、生成されたときの検出結果の深刻度です。
7. **[秘密データ]** で、ポリシーを適用するデータの種類を選択します (たとえば、PCI や PII などの特定のカテゴリ) を選択します。
8. **[リソース]** で、特定のデータリソース、リソースタイプ、タグ別のリソース、ラベル別のリソースなどのリソースを選択して、データ境界を定義します。
9. **[Done]** をクリックしてポリシーを保存します。

作成後、ポリシーはクラウド環境を継続的に評価し、選択したテンプレートに従って、存在すべきでない場所に保存されている機密データを検出したときに検出結果を生成します。

ライセンス

> Tenable One Cloud Exposure で Snowflake スキャンを使用するには、どのようなライセンスが必要ですか?

回答: Snowflake スキャンは、Enterpriseでのみ利用可能です。別のライセンス層を使用している組織の方で、Snowflake のサポートを有効したいという場合は、Tenable の担当者にお問い合わせください。詳細については、ライセンスを参照してください。

> データの仮想マシンまたは仮想マシンイメージをスキャンすると、追加のライセンスコストが発生しますか?

いいえ。Workload Protection スキャンが有効になっている場合、スキャンから仮想マシンを除外するおよびワークロードスキャンベースの請求可能なリソースとして請求されます。これらの仮想マシンでデータスキャンを有効にしても、同じ基盤となるスキャンを使用するため、請求可能なリソースの数は増えません。

つまり、Workload Protection が有効になっている場合、データスキャンは既存の仮想マシンの脆弱性スキャンの一部として含まれます。

スキャンベースの請求可能なリソースの詳細については、ライセンス参照してください。

仮想マシンのデータスキャン

> クラウドサイバーエクスポージャー仮想マシン (VM) の機密データをスキャンできますか?

はい。Tenable は、アクティブな **仮想マシン** と **仮想マシンイメージの** 両方をスキャンして、パスワード、API キー、トークンなどの秘密情報や認証情報を含む機密データを取得できます。詳細は、ワークロードベースのスキャンを参照してください。

> 仮想マシンのデータスキャンを有効にする方法

VM のデータスキャンは、Workload Protection の設定に関連付けられています。次のデータスキャンを有効にできます。

- スキャンから仮想マシンを除外する
- ワークロード

> スキャンが仮想マシンまたはイメージ上の機密データを検出した場合、どうなりますか?

スキャンが仮想マシンまたはイメージ上の機密データ (パスワード、API キー、トークンなど) を識別する場合、[機密性 **が制限されている]**(/v1/docs/ja/assess-data-scans#sensitivity-levels) データタイプのみが分類されます。検出結果は次のように処理されます。

- **既存の検出結果**: 深刻度レベルが 1 レベル上げられましたが、**高** に抑えられています。以下に例を挙げます。

- **中レベルの**検出結果は、**高**にエスカレートされます。
- **[高]** および **[重大] の**検出結果の深刻度レベルは、そのままです。

- **新しい検出結果**: 検出結果は、検出されたデータが **[秘密データの監視]** テンプレートを使用して クラウドポリシー: カスタム をトリガーする場合にのみ生成されます。この場合、検出結果は、その特定のポリシーで定義された深刻度レベルで作成されます。

脅威検出

必要なライセンス: この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

注意: 脅威検出を有効にしても 請求対象のリソースの数は増えません。

最新のクラウドセキュリティに必要なのは、設定ミスを特定するだけではありません。これには、クラウドインフラとコンテナ化されたワークロード全体にわたるアクティブな悪用の試みを検出する能力が必要です。

クラウド脅威検出は、静的なセキュリティポスチャーを侵害後のアクティビティをほぼリアルタイムで分析することで補完することで、この重要なレイヤーを提供します。Tenable は、ユーザーアクティビティと不審なアクティビティイベントを監視することで、従来のセキュリティコントロールを超えた総合的な可視性を提供し、ハイブリッド環境全体の脅威を特定できます。

Tenable クラウド脅威検出を使用すると、クラウド環境と Kubernetes リソース全体にわたる不審なアクティビティを継続的に監視し、特定できます。セキュリティイベントをほぼリアルタイムで分析することで、従来の脆弱性スキャンでは見逃されがちなリスクの高いアクティビティや潜在的な脅威を特定できます。

モニタリング方法

Tenable は、セキュリティ要件に応じて、クラウド環境を監視するために 2 つの主要な脅威検出方法を提供しています。

- **センサーベース (eBPF):** この方法では、センサーをKubernetesリソースに直接インストールすることで、ランタイムの詳細な可視性が得られます。eBPF テクノロジーを使用して、最小限のパフォーマ

ンスオーバーヘッドでシステムレベルでユーザーアクティビティを監視し、リソースをほぼリアルタイムで可視化できます。

- **エージェントレス**: この方法では、API 統合を使用してクラウドログを分析します。ソフトウェアをインストールしなくてもユーザーのアクティビティを監視できます。

クラウド環境を接続する方法の詳細については、以下を参照してください。

- **センサーベース (eBPF):**Helm チャートを介してクラスタを接続する。
- **エージェントレス** (クラウド環境による): AWS 組織の接続、Azure 組織の接続、GCP 組織の接続。

分析と検出

Tenableは、**アクティビティ**レベルで潜在的な脅威にフラグを立て、各検出結果をクラウドネイティブのコンテキストで強化し、cloud の MITRE フレームワークにマッピングします。これらの検出結果は**検出**として分類され、監視対象のクラウドログまたは Tenable eBPF センサーを介してリスクのある**アクティビティ**が**特定**された場合に、特定のルールに基づいて生成されます。

イベントがルールに一致すると、Tenable は、アイデンティティやリソースメタデータなどのクラウドネイティブコンテキストで強化された検出を生成します。

Tenable による環境内の脅威の監視方法

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

Tenable は、クラウドログ内の不審なアクティビティを分析し、ユーザーのアクティビティを観察することで、クラウドインフラとコンテナ化されたワークロードを監視します。監視方法は、環境の種類と、環境全体のアクティブな脅威をほぼリアルタイムで特定するために管理レベルのアクティビティとランタイムアクティビティのどちらを追跡しているかによって異なります。

サポートされている範囲

Tenable は、クラウドプロバイダーとコンテナプラットフォーム全体で脅威検出範囲を提供します。使用する方法は、環境の種類と、検出に必要な特定のログまたはイベントによって決まります。

脅威検出を有効にするアカウントをまだ接続していない場合は、以下の記事を使用して関連するクラウドプロバイダーを接続してください。

クラウドプロバイダー	記事
AWS	AWS 組織の接続
Azure	Azure 組織の接続
GCP	GCP 組織の接続

次の表は、サポートされているコンテナプラットフォームとそれぞれの監視方法の内訳を示しています。クラスタをまだ接続していない場合は、関連記事を使用してクラスタを接続します。

環境タイプ	プラットフォーム	モニタリング方法
マネージド (パブリック)	• EKS クラスタの接続 • AKS クラスタの接続 • GKE クラスタの接続	エージェントレス
マネージド (プライベート)	• EKS クラスタの接続 • AKS クラスタの接続 • GKE クラスタの接続	センサーベース (eBPF)
アンマネージド (クラウド)	プライベートマネージドの Kubernetes クラスタの接続	センサーベース (eBPF)
オンプレミス (アンマネージド)	Kubernetes と OpenShift クラスタの接続	センサーベース (eBPF)

要件

脅威の検出を有効にするには、クラスタタイプに応じて、関連するアクティビティログをエクスポートするか、Kubernetes センサーをインストールするように環境を設定する必要があります。

クラウドアカウント

クラウドインフラ内の疑わしいアクティビティを監視するには、クラウドプロバイダーアカウントのアクティビティログを有効にする必要があります。これにより、Tenable がクラウド環境全体のイベントを収集して分析できるようになります。次の表は、各クラウドプロバイダーに必要なログの内訳を示しています。

プラットフォーム	要件
AWS	AWS CloudTrail を設定する
Microsoft Azure	Azure の必要なアクセス許可にアクセスするためのアクセス許可を付与する
GCP	Google の必要なアクセス許可にアクセスするためのアクセス許可を付与する

Kubernetes クラスタ

コンテナ化されたワークロード内の不審なアクティビティを監視し、特定するには、Kubernetes センサーをインストールする必要があります。センサーは、クラウドベースの環境とオンプレミス環境の両方で、Kubernetes クラスタの不審なアクティビティイベントを可視化します。このセンサーをインストールするには、Helm Chart を介してクラスタを接続するを参照してください。

センサーの要件に関する詳細については、「センサーリソースを参照してください。

モニタリング方法

Tenable では、2 つの主要な脅威検出方法を使用して、ユーザーアクティビティを収集して分析します。

エージェントレス

この方法では、API 統合を使用して、ソフトウェアをインストールすることなくアクティビティログを収集して分析します。

- **エージェントレスデプロイメント**: API ベースのログ収集を通じて動作し、環境にソフトウェアがインストールされていないことを確認します。
- **ユーザーレベルのモニタリング**: クラウドインフラ全体の不審なアクティビティを追跡します。
- **一元化された可視性**: 接続されているすべてのクラウドアカウントにわたって不審なアクティビティを検出します。

ランタイム検出 (eBPF センサーベース)

この方法では、クラスタにセンサーをインストールすることで、ランタイムの可視性を提供します。eBPF テクノロジーを使用して、カーネルレベルでのユーザーアクティビティを監視します。

- **詳細な可視性**: クラスタ内のユーザーアクティビティをほぼリアルタイムで可視化します。
- **ユーザーレベルのインサイト**: クラウドプロバイダーのアクティビティログには表示されないワークロード内の不審なアクティビティを特定します。
- **デプロイメント:**Tenable の Helm チャートを使用してクラスタ間で簡単にデプロイできます。

セキュリティとプライバシー

次のセクションでは、顧客データを保護し、Tenable One Cloud Exposure 脅威検出ソリューションの整合性を確保するために実装されているセキュリティとプライバシーの実践方法の概要を説明します。

最低限必要なアクセス許可

Tenable は厳格な **最小権限** セキュリティモデルに従って、効果的な監視に必要なセキュリティコンテキストを維持しながら、セキュリティリスクを軽減します。

- **ログ分析**: Tenable は、CloudTrail、Azure Monitor、GCP 監査ログなど、クラウドプロバイダーログの収集と分析に必要な最小限AWSクラウドアクセス許可を利用します。
- **センサーの監視**: ランタイムセンサーは、広範な管理アクセス権を付与せずに、脅威検出アクティビティを監視するために必要な最小限のアクセス許可で設定されます。

データの分離と常駐

- **リージョン データ レジデンシー**: データは、Tenable コンテナがデプロイされているリージョン (米国、EMEA、APAC など) に格納されます。これにより、地域のデータ要件へのコンプライアンスを確保でき、セキュリティアクティビティデータを優先地理的境界内に維持できます。
- **安全なログ ストレージ**: クラウド ログとイベントは、Tenable の安全なデータ ストア内に保存されます。

データの暗号化と安全な通信

- **転送中のデータ**: ランタイムセンサーアクティビティデータやクラウドイベントログなど、オープンネットワーク間を移動するすべてのデータは、TLS 1.2 以上を使用して暗号化されます。ランタイムセンサーは、クラウド サイバーエクスポージャー Vulnerability Management および Kubernetes Security Posture Management と同じセキュリティ通信プロトコルを使用します。
- **保存データ**: 保存されているすべてのデータとイベント データは AES-256 を使用して保存時に暗号化され、セキュリティ メタデータが不正アクセスから確実に保護されます。

Tenable が検出する脅威

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

Tenable は、さまざまなタイプのアクティビティをモニタリングすることで、環境の包括的な可視性を提供します。個々のアクションと長期的なパターンの両方を分析することで、潜在的なセキュリティ侵害、設定ミス、不正なアクティビティを特定します。

脅威検出タイプ

脅威検出は、次の主なタイプに分類されます。

検出タイプ	データ ソース	説明
イベント	クラウドプ	クラウドプロバイダー (AWS、Azure、GCP など) 内で発生した単一のイベントに基づいて不審なアクティビティを検出します。

検出タイプ	データソース	説明
	ロバイダーのログ	
センサーベースのイベント	eBPF ランタイムセンサー	eBPF ランタイムセンサーイベントに基づいてアクティビティを検出し、ワークロードレベルのアクティビティを詳細に可視化します。これには、プロセス実行イベントとファイルオープンイベントのサポートが含まれます。

脅威検出ファミリー

クラウドベースおよびセンサーベースのイベントソース内で、Tenable は、動作パターンに基づいて脅威を特定の検出ファミリーにグループ化します。

- 不審なアクティビティ
- 異常検出
- マルウェアの実行

不審なアクティビティ

既知の攻撃者の行動やセキュリティのベストプラクティスの違反と一致するリスクのあるイベントをほぼリアルタイムで特定します。履歴ベースラインに依存する異常とは異なり、これらの検出は、過剰な管理ロールの作成や重要なセキュリティログサービスの無効化など、特定の事前定義されたルールによってトリガーされます。

異常検出

> **注意:** 異常検出は、Tenable One Cloud Exposure コンソール内の**クラウドポリシー**と**クラウド検出結果**でのみ管理されます。

Tenable は、継続的なリスク分析を通じてセキュリティポスチャーを改善します。クラウドアクティビティログ全体を処理することで、Tenable はユーザーとサービスのアイデンティティごとに一意の動作プロファイルを構築します。

異常カテゴリ

Tenable は、確立されたベースラインからの逸脱に基づいて、いくつかの種類の異常を検出します。

カテゴリー	説明	例	
データとリソースへのアクセス	通常の職務外のデータとのやり取り	初めて S3 バケットのコンテンツにアクセスする	
アイデンティティとアクセス	アイデンティティのアクセス許可と機能に対する通常とは異なる変更	• 予期しないアクセス許可の変更 • 権限昇格 • アクセスキーの不正使用/窃盗	
インフラと監査	クラウド環境のモニタリング設定またはネットワークセキュリティコントロールに対する変更	ネットワーク構成 (セキュリティグループ / VNet) の変更、またはログおよび監査設定の変更	
偵察	攻撃者が環境をマッピングしていることを示唆する検出パターン	すべてのリソース、ユーザー、またはセキュリティグループを一覧表示するための異常な API 呼び出し	

異常検出ポリシー

Tenable は、クラウドアイデンティティに一般的な動作パターンに関連する異常検出ポリシーを、アクティビティカテゴリにマッピングして標準装備しています。これらのポリシーには、次のようなものがあります。

- **異常なデータアクセス**: データにアクセスした履歴がなくてもアクセスしたアイデンティティを検出します。これは、盗んだ認証情報を使用しようとする攻撃者がよく使用する手法です。
- **異常なアクセス許可管理**: 同様のアクションを実行した履歴がなくてもアクセス許可を変更したアイデンティティを検出します。これは、攻撃者が環境内で足場を築くためによく使用されます。

ポリシーの完全なリストについては、クラウドサイバーエクスポージャーコンソールの **[ポリシー]** に移動し、**[Anomaly Detection] (異常検出)** カテゴリでフィルタリングしてください。

学習期間

不審な不審なアクティビティと異常検出の両方について、正確性を確保するために、Tenable 特定の学習ライフサイクルに従います。

- **分析期間**: Tenable は最大 12 か月分の履歴データを分析し、アイデンティティのベースラインを確立するには少なくとも 30 日間のアクティブな観察が必要です。
- **反復する動作**: 最初の検出結果または検出をオープンした後に、同様の異常な動作が検出された場合
    - **30 日以内**: Tenable は既存の検出結果または検出に動作を追加し、以前に解決された場合は再度開きます。
    - **30 日後:**Tenable によって新しい検出結果または検出結果が生成されます。

異常検出結果の管理

異常検出結果は、静的な設定ミスではなく動作の逸脱を表しているため、従来の修正スクリプトでは修正できません。

- **手動解決:** 調査後、検出結果が正当なアクティビティを示している場合は、手動で解決済みとしてマークする必要があります。
- **自動化:**Tenable では、自動化を作成して、深刻度が「高」または「重大」の異常検出結果を、選択した通知または SIEM 統合にルーティングすることを推奨しています。

マルウェアの実行

既知または疑わしいマルウェアとしてフラグが立てられたバイナリのプロセス実行を検出します。

クラウド サイバーエクスポージャー には、SHA-256 ファイルハッシュに基づいてマルウェアのレピュテーション データを提供する、業界をリードするセキュリティプロバイダーとの統合が組み込まれています。

脅威の検出 MITRE ATT&CK マッピング

Tenable は、セキュリティフレームワークの包括的なライブラリを使用して、すべての検出タイプにわたる脅威を分類します。Tenable は、攻撃者の戦術と手法を説明するための世界的に認められた標準である MITRE ATT&CK® を利用することで、識別されたすべての脅威に対して完全なセキュリティコンテキストを提供します。各検出は、調査と対応を迅速化するために、MITRE ATT&CK® Enterprise Matrix の特定の戦術と手法に明示的にマッピングされています。

- **攻撃者の目的を特定する**: 攻撃者が初期アクセスを求めているのか、システムへの長期アクセスを確保しているのか、機密データを盗もうとしているのか、何を達成しようとしているのかを確認します。
- **テクニックを特定する**: 使用されている特定の方法を明確に理解します。
- **攻撃経路の視覚化**: 脅威の進行状況を把握し、発生している攻撃のステージを確認します。

脅威ストーリー

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

クラウド環境では、セキュリティアラートと呼ばれることが多い大量の個別の脅威検出が、すぐに管理不能になってしまう可能性があります。このようなコンテキストの欠如は、企業が実際の重大な脅威に集中する能力に深刻な影響を与えます。運用効率を最大化し、セキュリティチームが侵害後のアクティビティを特定できるように、Tenable は脅威ストーリーを導入しました

脅威事例の概要

脅威ストーリーは、フラグが立てられた検出の全体像を提供します。Tenable は、独自のロジックを使用して 24 時間以内に統合します。関連する検出とイベントをグループ化することで、脅威ストーリーは、潜在的な実際の脅威に焦点を当て、インシデントの根本原因を明らかにし、トリアージと応答の管理プロセスを加速するのに役立ちます。

脅威ストーリーは、多数の孤立した検出を、時間の経過とともに少数の一元化された潜在的なインシデントに統合することで、チームに明確で実行可能な優先順位を与え、最も重要なことに集中できるようにします。脅威ストーリーページは、インシデントのモニタリング、脅威の調査、初期対応の調整を行うための主要なエントリポイントとして機能します。

脅威ストーリー生成ロジック

脅威検出ルールエンジンは、潜在的なリスク、相関しきい値、クラウド環境のコンテキストに基づいて受信検出を自動的に評価し、脅威ストーリーを作成して更新します。

脅威ストーリーの関連性と正確性を確保するために、Tenableでは、24時間のスライディングウィンドウ内で1つ以上の検出が行われた場合に、このロジックを適用します。これらの検出は、エンティティを共有し、次のような特定の基準を満たす必要があります。

- 深刻度レベルが[高]または[重大]の1つの検出。
- 特定の相関シグネチャを共有する複数の検出。

FAQ: 脅威の検出と脅威事例

> **必要なライセンス:** この機能は**Enterprise**ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

この記事では、Tenable One Cloud Exposure内のクラウド脅威検出とクラウド脅威ストーリーに関連するよくある質問を一覧表示します。

脅威検出

このセクションでは、クラウドサイバーエクスポージャー内のクラウド脅威検出に関連する、よくある質問を紹介します。

ライセンスと請求

> クラウド脅威検出のライセンス要件と請求への影響は何ですか?

クラウド脅威検出は、クラウドサイバーエクスポージャー Enterprise ライセンスの一部として含まれています。これらの機能を有効にしても、追加コストは発生せず、請求対象のリソースの数が増えることもありません。

アカウント内スキャン

> アカウント内スキャンは脅威検出に対応していますか?

アカウント内スキャンは脅威の検出には関係ありません。アカウント内スキャンは脆弱性とデータのスキャンをお客様のインフラ内でローカルに実行しますが、Tenable はセンサーアクティビティイベントとクラウドプロバイダーのログを クラウドサイバーエクスポージャー プラットフォームを通じて直接分析することで脅威を検出します。そのため、すべての脅威の特定は、アカウント内のスキャンインフラではなく、クラウドサイバーエクスポージャー プラットフォーム内で行われます。

近リアルタイム(NRT)検出

> Tenable は脅威をほぼリアルタイムで検出しますか?

回答: はい。Tenable は、近リアルタイム (NRT) アプローチを利用しています。クラウドイベントとセンサーデータを継続的に収集して処理することで、Tenable は不審なアクティビティを特定し、特定されたらそれを警告します。

データ保持

> 脅威やイベントのデータ保持ポリシーは何ですか?

回答: **Enterprise / CNAPP Complete** ライセンスのデータ保持期間は、データの種類によって異なります。

- **クラウドイベント** (エージェントレスモニタリング): 90 日
- **ランタイムイベント** (センサーベースの監視) : 90 日
- **検出:** 1 年間

> **注意:** 特定の検知に関連するイベントは、その検知と同じ期間(1年間) 保存されます。

学習期間

> 脅威検出の学習期間はどのくらいで、どの検出に適用されますか?

学習期間とは、Tenable が逸脱を正確に特定する前に、アイデンティティの通常の動作のベースラインを確立する必要がある時間のことです。これは、次のソースから表面化した脅威に適用されます。

- **クラウドポリシー**: **異常検出**のポリシー。一致するリソースが **[クラウドの検出結果]** に表示されます。
- **脅威検出ルール**: 動作パターンに基づいて脅威を検出するルールです。ルールに一致する不審なアクティビティは、**[脅威検出]** の検出として表示されます。

Tenable は、次の学習ライフサイクルに従います。

- **分析期間**: Tenable は最大 12 か月分の履歴データを分析し、アイデンティティのベースラインを確立するには少なくとも 30 日間のアクティブな観察を必要とします。
- **反復する動作**: 最初の検出結果または検出をオープンした後に、同様の異常な動作が検出された場合
    - **30 日以内**: Tenable は既存の検出結果または検出に動作を追加し、以前に解決済みの場合は再度オープンします。
    - **30 日後:** Tenable が新しい検出結果または検出を生成します。

カスタム検出ルール

> 独自のカスタム検出ルールを作成できますか?

カスタム検出ルールは現在製品ロードマップに記載されており、将来の更新プログラムとして利用可能になる予定です。

修正

> Tenable は脅威検出結果に対する修正を提供していますか?

修正機能は現在製品ロードマップに記載されており、今後の更新プログラムとして利用可能になる予定です。

API サポート

> Tenable は脅威検出検出結果に対して API サポートを提供していますか?

回答: 脅威検出検出結果に対する API サポートは、現在製品ロードマップに記載されており、今後のアップデートとして利用可能になる予定です。

脅威ストーリー

このセクションでは、クラウドサイバーエクスポージャー内の脅威ストーリーに関連するよくある質問を紹介します。

脅威ストーリーと脅威検出の違い

> 脅威検出と脅威ストーリーの違いは何ですか?

回答: 脅威検出は、変更されたセキュリティグループなど、クラウドランタイム環境内の疑わしいアクティビティを 1 つ特定します。脅威ストーリーは、共有アクターなどの関連エンティティによって経時的に観察された複数の関連する検出を結び付け、潜在的な攻撃の全範囲を示します。

イベントの相関

> Tenable はどのようにしてさまざまなセキュリティイベントを 1 つの脅威ストーリーにまとめますか?

回答: Tenable は、共有されたコンテキスト データを分析することで、セキュリティ イベントを自動的に関連付けます。このデータには、特定のアクター ID、イベントのタイムフレーム、影響を受けるクラウド リソース、ランタイム クラウド環境全体でのイベントの進行状況が含まれます。

調査ワークフロー

> 脅威ストーリーを調査する際、最初に何をすべきですか?

回答: 脅威事例の詳細を表示するビューを開き、次の手順に従ってイベントを調査します。

- **概要の詳細を確認します**。上部のメタデータパネルのすぐ下にある [概要] セクションと [影響] セクションを参照して、何が起きたのか、セキュリティポスチャーにどのような影響を与えるのかを理解します。
- **リレーションシップマップを分析する**: ページのさらに下にあるインタラクティブなビジュアルグラフを使用して、脅威アクター、脅威ストーリー、影響を受けるリソース間のつながりをトレースします。
- **データの検査**: ページ下部の [Detections] (検出) テーブルにリストされている個々のレコードを表示して、イベントの各特定のステップを確認します。

ステータスの追跡

> 脅威ストーリーの調査ステータスを変更できますか?

回答: はい。脅威ストーリーのワークフローステータスを更新することで、調査を追跡できます。内部のトリアージと修復の取り組みに基づいて、脅威ストーリーが [オープン]、[進行中]、[解決済み] のいずれであるかを反映するようにステータスを設定できます。

> **注意:** ステータスを変更するとき(特に、ストーリーをクローズまたは解決するとき)、脅威の性質を正確に分類するために、アナリストの評決を選択するように求められます。

Kubernetes

> **必要なライセンス:** この機能は **Standard** および **Enterprise** のライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

クイックリンク

この記事はKubernetes機能の概念上の概要です。

- クラスタをTenableに接続する方法については、関連するガイド (Helmチャートを介してクラスタを接続する、Amazon EKSクラスタの接続、Azure AKSクラスタの接続、Google GKEクラスターを

接続するOracle OKEクラスタの接続 経由) を参照してください。

- Kubernetes クラスタの表示と管理に関するハウツーガイドについては、「 Kubernetesクラスターを参照してください。
- よく寄せられる質問については、「 FAQ: Kubernetes」を参照してください。
- Helm チャートによるセキュリティについては、Helm チャートを介してクラスタを接続するを参照してください。

Tenable では **Kubernetes Security Posture Management (KSPM)** を使用して、クラスタ内のリスクを特定し、優先順位を付けることができます。Tenable は、クラウドインフラ、ユーザーアクセス許可、コンテナワークロード間の関係を分析することで、早急な対応が必要な重大なセキュリティ問題を明らかにします。

KSPM は以下の領域からのデータを統合し、Kubernetes のセキュリティに関する統一されたビューを提供します。

- **インフラ設定:** Amazon EKS、Azure AKS、Google GKE、Oracle OKE などのクラウドプラットフォームに設定ミスがないかスキャンします。
- **ランタイム検出**: eBPF センサーを介してユーザーアクティビティをモニタリングし、ほぼリアルタイムで疑わしいアクティビティを検出します。
- **アドミッションコントローラー**: セキュリティポリシーを適用し、高リスクのデプロイメントを阻止します。
- **脆弱性管理**: すべてのクラスタリソースで脆弱性を検出します。
- **アイデンティティとアクセス**: クラスタ内のリソースやサービスへの過剰な権限アクセスを特定します。

これらの文脈情報を Kubernetes 固有のポリシーと組み合わせることにより、単一のインターフェースからコンテナリソースをモニタリングできます。Tenable は、Kubernetes 固有のリソースデータとプラットフォーム全体の文脈情報を関連付けます。これにより、ユーザーはリスクに優先順位を付け、関連するチームに通知して緩和策を加速させることができます。

まず、Kubernetes クラスタを Tenable に接続して、リソースとそれに関連するコンテナイメージを可視化します。

コアの可視性と分析

クラスタを接続すると、プラットフォームは環境からデータを即座に抽出して分析し、Kubernetes インフラストラクチャ全体のリスクを特定します。Tenable は、次の 2 つの主要なソースからKubernetes関連データを収集します。

- **クラウドプロバイダー API**: AWS、Azure、GCP、OCI 全体でクラスタと実行中のコンテナイメージに関する情報を収集します。
- **Kubernetes クラスタ API:** クラスタ API を使用して、環境内からアーキテクチャデータと設定データを取得します。

この統合により、Kubernetes リソースとそれに関連するコンテナイメージを完全に可視化できます。Kubernetes リソースの場合、プラットフォームはアクセス許可、アカウントの使用状況、セキュリティ設定に関する詳細情報を取得します。

Helm チャートによるリソースの同期方法

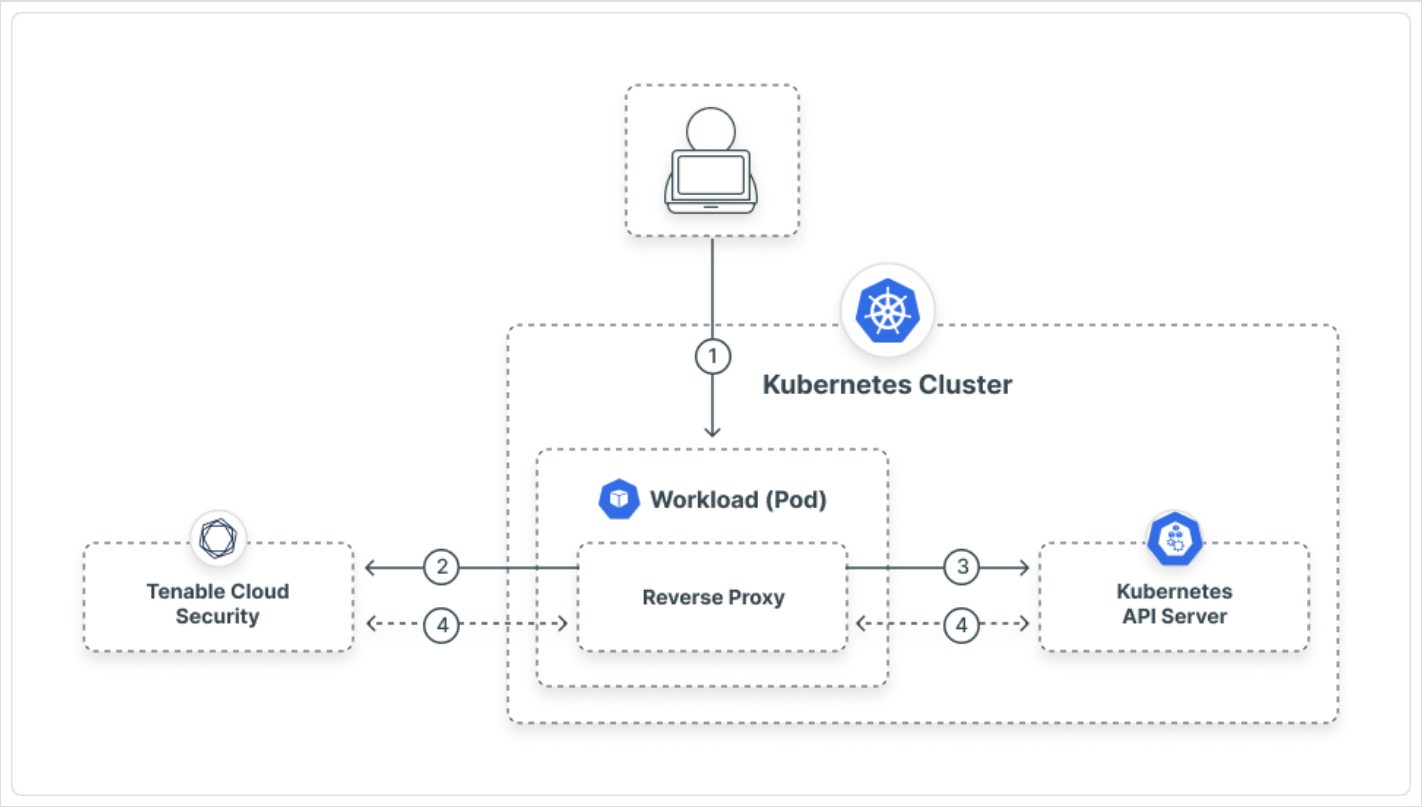
Helm チャートメソッドを使用すると、Tenable は必要なアクセスタイプに基づいてクラスタデータを同期します。このアーキテクチャアプローチにより、制限環境でも詳細な可視性が得られます。

ネットワークアクセス

ネットワークベースのアクセスがパブリックにアクセス可能でない場合、Tenable は次のプロセスを使用してデータを同期します。

1. Kubernetes クラスタコネクタを追加すると、Tenable によってクラスタで実行されるワークロード (デプロイメント) が作成されます。このワークロードはポートを外部に公開せず、インターネットからアクセスできません。
2. ワークロードは、リバースプロキシを使用して Tenable との安全な専用接続を開始します。
3. ワークロードは、Kubernetes API サーバーと Tenable のバックエンドの間でトラフィックをルーティングします。これにより、Tenable API サーバーをインターネットに公開することなく、データの同期と更新の頻度できます。

重要: このプロセスは、Kubernetes API サーバーをインターネットに公開しません。すべての外部通信は、作成されたワークロードを経由してのみ実行されます。



アイデンティティアクセス

割り当てられたロールにクラウド API 経由でクラスタにアクセスするアクセス許可がない場合、Tenable は次のプロセスを使用してデータを同期します。

1. Kubernetes クラスタコネクタを追加すると、Tenable はクラスタ内にサービスアカウントを作成します。
2. サービスアカウントは、読み取り専用アクセス許可を使用してリソースメタデータを取得します。Tenable は、書き込みアクセス許可を作成したり使用したりしません。
3. Tenable は、このサービスアカウントを使用して データの同期と更新の頻度 し、更新されたインベントリを維持します。

Kubernetesランタイムの検出

Kubernetes ランタイム検出は、コンテナ化されたアクティブなワークロードを可視化し、静的スキャンで見逃される可能性のある認証されていないユーザーアクティビティを特定します。エージェントレスのモニタリン

グとは異なり、この方法では、Helm チャートを使用して Kubernetes リソースに直接センサーをインストールする必要があります。

このセンサーは、eBPF センサーテクノロジーを使用して、最小限のパフォーマンスオーバーヘッドでユーザーアクティビティを監視します。

主な機能

- **ランタイムの検出**: Kubernetes 環境内の不審なアクティビティを特定します。
- **ランタイムの可視性**: クラスタ内のユーザーアクティビティに関する詳細なインサイトを取得します。
- MITRE マッピング: 特定されたすべての脅威をクラウドネイティブコンテキストで強化し、検出を MITRE フレームワークにマッピングして、調査を迅速化します。

詳細については、「Tenable による環境内の脅威の監視方法」をご覧ください。

Kubernetes アドミッションコントローラー

Kubernetes アドミッションコントローラーは、クラスターがリソースを作成または更新する前に API リクエストを傍受して評価することで、クラスターのセキュリティゲートキーパーとして機能します。このコントロールレイヤーを使用すると、詳細なポリシーを適用して、すべてのコンテナ、ポッド、サービスがセキュリティと設定標準に準拠しないようにすることができます。

主な機能

- **コンプライアンスの徹底**: リソースを自動的に検証して、設定ミスを防ぎます。たとえば、root 権限で実行を試行するコンテナをブロックできます。
- **ポリシー適用モード**: 違反の処理方法を選択します。[拒否] を選択して非準拠リソースを完全にブロックするか、[アラート] を選択して、監査のために記録しながらアクションを許可することができます。
- **運用の可視性**: 専用ログを通じて傍受されたすべてのアクションを追跡および分析し、安全で透明性の高い Kubernetes 環境を維持します。

詳細については、「アドミッションコントローラーの概要を参照してください。

Kubernetes 脆弱性スキャン

コンテナベースのワークロード用に、Tenable はセンサーを提供しています Helm チャートを介してクラスタを接続する チャートを使用してインストールできます。センサーはすべてのクラスタノードで **DaemonSet** として実行され、脆弱性とソフトウェアのスキャンを実行します。CronJobs やその他の一時的なポッドからの有効期間の短いイメージも含めて、約 30 分以内にノードをスキャンして新規または更新されたコンテナイメージを探します。この方法は、クラウドマネージドクラスタとアンマネージドクラスタ (オンプレミスを含む) でサポートされているため、実行中のワークロードを包括的に可視化できます。

詳細については、「 エージェントベースの Kubernetes ワークロードスキャン」を参照してください。

ライセンス要件

ライセンスタイプ	含まれる機能
スタンダード	Kubernetes インベントリの可視性、設定リスク評価、クラウドプロバイダー API 分析が含まれます。
Enterprise	すべての標準機能に加えて、Kubernetes アドミッションコントローラー、アンマネージドクラスタ (オンプレミスを含む) のセンサーベースのスキャン、コンテナイメージの詳細なワークロード分析が含まれています。

アドミッションコントローラーの概要

必要なライセンス: この機能は **Enterprise** ライセンスで利用できます。詳細については、ライセンスを参照してください。

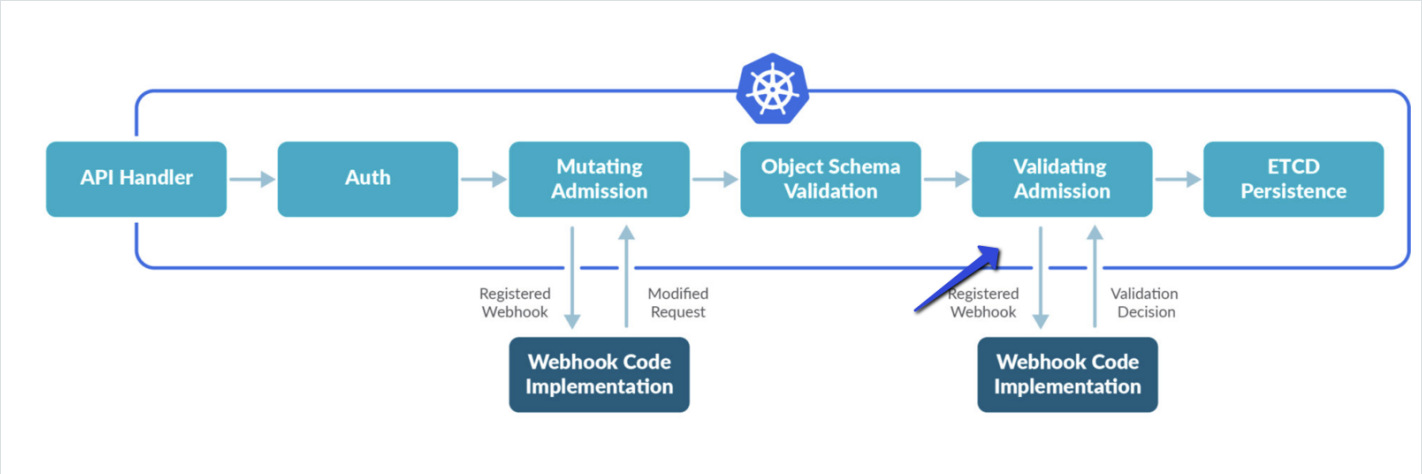
注意: この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

この記事では、Tenable One Cloud Exposure のアドミッション コントローラー機能の概念概要について説明します。

- イベントの探索に関するハウツーガイドについては、「Kubernetes アドミッションコントローラーイベント」を参照してください。
- ポリシーの設定に関するハウツーガイドについては、アドミッションコントローラーポリシーを参照してください。

Kubernetes アドミッションコントローラーは、クラスタ内で作成および変更するリソースに対する重要なコントロールレイヤーを提供します。アドミッションコントローラーは API リクエストをインターセプトします。これにより、ユーザーは次のアクションを実行できます。

- セキュリティポリシーを適用し、設定を検証します。
- システムがコンテナ、ポッド、サービスなどの準拠リソースのみを作成または削除できるようにしてください。
- [拒否] (アクションをブロック) や [アラート] (アクションを許可して違反をログに記録する) などの違反効果を適用します。



[Admission Controller Policies] (アドミッションコントローラーポリシー) ページで、アドミッションコントローラーポリシー アドミッションコントローラーポリシーの設定 、ポリシー違反の結果を定義できます。違反の影響として、[拒否] または [アラート] を設定できます。有効なポリシーは、アドミッションコントローラーのインストール をインストールし済み、選択した範囲内に存在するクラスタにのみ適用されます。

> **注意:** これらのポリシーを適用する前に、クラスタ Tenable アドミッションコントローラーをインストールする必要があります。

Tenable は、アドミッションコントローラーポリシーによって分析されたすべての Kubernetes アクションを、イベント ページに記録します。

アドミッション制御のユースケース: 非 root ユーザー権限の強制

アドミッションコントローラーを使用すると、Kubernetes クラスタにデプロイするすべてのコンテナが非 root ユーザー権限で実行されるようにすることができます。これを強制するには、[Pod Security Standards - Root Containers] ポリシーを **[Deny]** に設定します。

ルートとして実行されているコンテナでポッドをデプロイしようとすると (たとえば、`runAsUser` フィールドが `0` (ルートユーザー ID) に設定されているか、省略されている場合)、アドミッションコントローラーがリクエストをインターセプトし、デプロイメントをブロックします。

次のポッドマニフェストは非ルートユーザーポリシーに違反しています。

YAML

```
apiVersion: v1
kind: Pod
metadata:
    name: root-container-pod
spec:
    Containers:
    - name: insecure-container
      image: nginx
      securityContext:
            runAsUser: 0  # これは、コンテナが root として実行されることを指定します。
```

この例では、「ポッドセキュリティ標準 - ルートコンテナ」ポリシーがポッドのデプロイメントをブロックします。このポリシーを強制することで、権限昇格の脆弱性を防ぎ、ルートコンテナに関連するリスクを軽減して安全な Kubernetes 環境を維持できます。

よくある質問 - Kubernetes

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

この記事では、Tenable One Cloud Exposure内のKubernetesに関連するよくある質問を紹介します。

オンプレミスまたはセルフマネージドクラスタのクラスタコネクタ要件

> 質問: オンプレミスまたはセルフマネージドクラスタを接続する前にクラスタコネクタを追加する必要があるのはなぜですか?

回答: コネクタは、クラウドサイバーエクスポージャーがクラスタに接続するために必要な API トークンとして機能します。環境内のすべての関連クラスタにコネクタを 1 つ追加してください。

Tenable での Kubernetes Cluster Connector API キーのアクセス許可

> 質問: Tenable の Kubernetes Cluster Connector とは何ですか? またその目的は何ですか?

回答: Tenable の Kubernetes Cluster Connector は、Kubernetes クラスタとクラウドサイバーエクスポージャープラットフォーム間の安全な通信を認証し有効化するために使用される API キーです。その主な役割は、監視および分析のために Kubernetes 環境と Tenable の統合を促進することです。

> 質問: Kubernetes Cluster Connector API キーにはどのようなレベルのアクセス権がありますか? また、非常に制限されているのに「コネクタ」と呼ばれるのはなぜですか?

回答: Kubernetes Cluster Connector API キーは、その名前にもかかわらず、範囲が **狭く特定のものです**。これは**Kubernetes関連の操作に厳格に制限**されており、エンティティデータのクエリやアカウントレベルのアクションの実行など、より広範な Tenable API へのアクセスは**付与されません**。プラットフォームの他の部分へのアクセスなど、本来の目的以外で使用する試みは拒否されます。

クラスタアカウントの関連付け

> 質問: Tenable では、クラスタが関連付けられているアカウントをどのように判断しますか?

回答:
Helm チャートがクラスタにインストールされると、クラウドサイバーエクスポージャーは以下のようにクラスタアカウントの場所を検出します。

- 関連付けられているクラウドアカウントがすでに接続されている場合、クラスタはクラウドプロバイダーの関連するアカウント範囲 (フォルダー) に追加されます。
- 関連付けられているクラウドアカウントが接続されていない場合、Tenable はワーカーノードのアカウントに基づいて場所の特定を試みます。
- 関連付けられたアカウントが検出されない場合、Tenable はクラスタをオンプレミスのデフォルトアカウントに追加します。

  > **注意:** ほとんどの場合、このデフォルトアカウントに追加されるクラスターはオンプレミスですが、他のクラスタータイプもこのフォルダーにマッピングされる場合があります。たとえば、クラウドサイバーエクスポージャーによってサポートされていないクラウドプロバイダーに属するクラスタなどです。

- `--set accountId={accountId}` を Helm コマンドに追加することで、検出されたアカウントの場所をオーバーライドできます。詳細については クラスターを追加する を参照してください。

コンソールでのリソースの可視性

> 質問: Helm チャートのインストール後、クラスタリソースがコンソールに表示されるまでにどれくらいの時間がかかりますか?

回答: お使いの環境で データの同期と更新の頻度 ときに、リソースが表示されます。

新しいコンテナイメージのスキャン

> Tenable は、ノード上で実行中の新しいコンテナイメージまたは更新されたコンテナイメージをどのくらいの速さでスキャンしますか?

センサーは約 30 分以内にノードをスキャンして新規または更新されたコンテナイメージを探します。検出結果はご使用の環境内で Tenable が次回 データの同期と更新の頻度 ときに更新されます。

OpenShift クラスタのサポート

> 質問: OpenShift クラスタを接続できますか?

回答: はい。Helm チャートを介してクラスタを接続する。

クラスタの移動

> 質問: クラスタを別のアカウントに移動するにはどうすればよいですか?

Helm チャートを使用してクラスタをアンインストールしてから、再インストールしてください。アンインストールするには、クラスタで次のコマンドを実行します。`helm uninstall tenable-kubernetes-cluster-connector -n tenable`

カスタムクラスター名

> 質問: クラスタのデフォルト名をオーバーライドできますか?

回答: はい。セルフマネージド/オンプレミスクラスターを接続する場合、デフォルトの名前は DNS 名になります。`--set name={name}` を Helm コマンドに追加することで、この名前をオーバーライドできます。詳細については、オプションのコマンドパラメーターを参照してください。

エージェントのバージョン

> 質問: エージェントログからエージェントのバージョンを取得するにはどうすればよいですか?

バージョンを取得するには、クラスタで `kubectl` を実行し、ワークロード Pod ログを確認します。`kubectl logs <tenable connector pod name> -n <namespace> | grep Version`

コネクタポッドの場合は、出力で `Version` を検索します。バージョンは、それぞれアドミッションコントローラーポッドとセンサーポッドの出力で `BuildVersion` と `buildVersion` で表されます。

アドミッションコントローラー

> 質問: アドミッションコントローラー Webhook がポート 8443 でリッスンするのはなぜですか?

回答: ポート 8443 がKubernetesアドミッション Webhook に一般的に使用される安全な HTTPS ポートであるため、Webhook はデフォルトでポート 8443 でリッスンします。これにより、ワーカーノードからのすべての受信コントロールリクエストが安全に処理されます。

> 質問: プライベート GKE セットアップのポート 8443 では、どのような問題が発生する可能性がありますか?

回答: プライベート GKE セットアップでは、ファイヤーウォールルール、VPC 設定、その他のセキュリティメカニズムなどのネットワーク制限により、ワーカーノードがブロックされてポート 8443 の Webhook に到達できない場合があります。これにより、アドミッションコントローラーが適切に機能しなくなる可能性があります。

> 質問: ワーカーノードがポート 8443 で Webhook に確実に到達できるようにするにはどうすればよいですか?

回答: ワーカーノードに Webhook へのアクセスを許可するには

1. **ファイアウォールルール**: ファイアウォールルールが、すべてのワーカーノードからポート 8443 の Webhook エンドポイントへのトラフィックを許可するようにします。
2. **VPC ピアリング**: Webhook が別の VPC で実行されている場合は、適切なピアリングとルーティングを設定します。
3. **ネットワークポリシー**: Kubernetesで、通信をブロックしている可能性のある `NetworkPolicy` がないか確認して、変更します。
4. **エンドポイントのアクセシビリティ**: Webhook サービスが正しく公開され、クラスタ内で到達可能であることを確認します。

> 質問: 別のポートを使用するように Webhook を設定できますか?

回答: はい、必要に応じて別のポートでリッスンするように Webhook を設定できます。ただし、そのためには Kubernetes で Webhook 設定を更新し、ファイヤーウォールルールで新しいポートへのトラフィックが許可される必要があります。

> 質問: この場合、顧客の上書きオプションは何ですか?

回答: デフォルトのポート(8443)にアクセスできない場合、顧客の上書きオプションにより、ユーザーはカスタム設定を指定できます。これには、別のポートを定義したり、接続を確保するための代替ネットワークルールを設定したりすることが含まれます。

> 質問: アドミッションコントローラーがシークレットにアクセスする必要があるのはなぜですか?

回答: 脆弱なコンテナイメージポリシーを有効にするために、アドミッションコントローラーはイメージプルシークレットを読み取ることで、デプロイされているコンテナイメージを識別します。Tenableはシークレットをリストするアクセス許可を付与しますが、アドミッションコントローラーはイメージプルシークレットのみを調べます。このアクセスは、デフォルトでは無効になっています。`--set admissionController.readSecrets=true`で有効にします。これにはTenable Kubernetes Helmチャートバージョン1.1.6以降が必要です。

プライベートリポジトリからクラウドサイバーエクスポージャーHelmチャートをデプロイする

> 質問: プライベートリポジトリからクラウドサイバーエクスポージャーHelmチャートをデプロイするにはどうすればよいですか?

プライベートGitリポジトリからクラウドサイバーエクスポージャーHelmチャートをデプロイするには、次の手順に従います。

1. 以下を実行して、公式Tenable repoからHelmチャートのクローンを作成します。
   `helm repo add <local path/cloned repo>`または、コピーを指すようにサードパーティの継続デプロイメントプラットフォームを設定します。

   > **注意:** 必要に応じて、チャートをインストールしたい場所へリポジトリ/チャートをコピーします。

2.`helm install`コマンドを更新して、TenableのパブリックGitHubリポジトリではなく、プライベートリポジトリまたはローカルパスをポイントします。

> 質問: 顧客はプライベートのHelmリポジトリを最新の状態に保つ必要がありますか?

回答: はい。Tenableでは、少なくとも2週間に1回、プライベートリポジトリを最新のHelmチャートリリースと同期することを推奨しています。これにより、最新の機能、機能改善、セキュリティ更新を確実に利用できます。

> 質問: Helmチャートが使用するコンテナイメージについて教えてください。

回答: デプロイメントでプライベートコンテナレジストリを使用する必要がある場合、顧客はTenableのコンテナイメージもプライベートレジストリにミラーする必要があります。これには、必要に応じてHelm値のイメージ参照を更新することも含まれます。
詳細については、こちらのドキュメントを参照してください。

Helmチャートと同様に、イメージには、機能、パフォーマンス、セキュリティに関する更新を頻繁に受け取る実際のランタイムコンポーネントが含まれているため、イメージも定期的に更新する必要があります。

Kubernetesクラスタに特定のセンサーバージョンを使用する方法

> 質問: Kubernetesクラスタに特定のセンサーバージョンを使用するにはどうすればよいですか?

ダウンロードできるのは、Tenableが公開している最新バージョンのセンサーのみです。ただし、クラスタとプライベート プライベートレジストリを持つクラスタを使用することで、特定のバージョンを自分で管理および固定できます。

最新バージョンをダウンロードしたら、プライベートレジストリにプッシュし、バージョン管理のニーズに応じてタグ付けします。ここから、クラスタがプルするタグを制御します。

コード

(クイックリンク) Tenable One Cloud Exposure このセクションでは、のコードスキャン機能の概念概要を説明します。

- コードをTenableに接続するには、CI/CDの接続 またはコードリポジトリの接続参照してください。
- Tenableでスキャン結果を表示して分析するには、コード CI/CD参照してください。
- IaCの検出結果を表示および管理するには、IaC検出結果参照してください。
- クラウドの検出結果でソースコードを表示し、IaCを介して検出結果を修正するには、クラウドの検出結果参照してください。

クラウドサイバーエクスポージャー IaC Security to を使用して

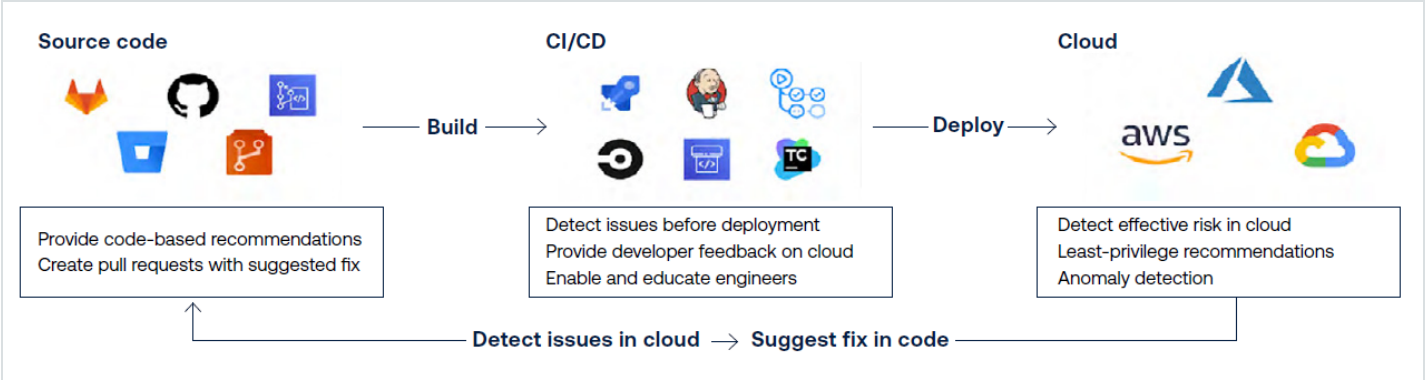
- インフラのコード化 (IaC)**をスキャンし**、クラウドリソースがデプロイされる前に、によって検出されたクラウドサイバーエクスポージャーIaCの結果を分析することで構成の問題に対処します。開発者とDevOps は、ネイティブツール内で即座にフィードバックを受け取り、安全なアプリケーションを作成できます。クラウドの設定ミスを早期に検出することにより、シフトレフトセキュリティプラクティスを実装します。
- クラウドリソースに関連付けられたコードを**同期して**、それらのリソースを元の場所に**トレースします** (Cloud to Code)。ソースコードを明らかにすることで、クラウドの検出結果をより効率的に特定して修正します。コードとして管理されているリスクのあるリソースや設定ミスがあるリソースについて、関連するコードスニペットを素早く見つけたり、プルリクエストを使用して IaC の検出結果を自動的に修正したりできます。
- **プルリクエストをスキャンして**、設定ミスが本番コードにマージされないようにセキュリティゲートを提供します。デフォルトのブランチだけでなく、すべてのブランチにわたって開発者ワークフロー内で高忠実度ポリシーを直接実施します。Tenable は検出結果をインラインのプルリクエストコメントとして表示し、[スキャン失敗しきい値] 設定を使用してセキュリティ要件を満たしていないマージをブロックします。

必要なライセンス: この機能は **Standard** および **Enterprise** のライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

IaC ワークフロー

次のワークフローは クラウドサイバーエクスポージャー、IaC Security が CI/CD ワークフローに統合され、クラウドをデプロイする前のコードスキャンを促進する方法を示しています。

- **CI/CD** パイプライン: Tenable は、デプロイされる前にコードをスキャンすることで、IaC フレームワーク内の新しい IaC 検出結果 を検出します。
- **クラウド** 環境: Tenable は、アカウント全体の広範囲の危険な状況を特定することで、クラウド環境にある既存の クラウドの検出結果 を検出します。



プルリクエストスキャン

プルリクエスト (PR) スキャンは、設定ミスが本番環境に到達するのを防ぐためのセキュリティゲートを提供します。リポジトリスキャンは、デフォルトブランチのセキュリティ態勢を監視し、CI/CD スキャンは深いパイプライン統合を提供しますが、PR スキャンはセキュリティを開発プロセスのさらに左にシフトします。

この機能により、すべてのプルリクエストがスキャンされ、セキュリティ標準を満たすことが確実に検証されます。これらのポリシーを実施することで、パイプライン設定という手動の作業を行うことなく、非準拠コードのマージを安全にブロックできます。

コア機能

- **継続的スキャン**: はすべてのブランチにわたって新規および更新されたすべての PR を自動的にスキャンします。
- **完全なコンテキスト分析**: 変更された行だけでなく、ブランチの各ファイルのコンテンツ全体を評価します。
- **開発者インラインフィードバック**: スキャン失敗しきい値を満たすまたはそれを超えた検出結果は、即座の可視性のために PR 内にインラインコメントとして直接投稿されます。他のすべての検出結果は、クラウドサイバーエクスポージャーコンソールで引き続きアクセスできます。
- **一元化されたレポート作成**: 各スキャンの詳細な結果は、クラウドサイバーエクスポージャーコンソールの **[リスク] > [CI/CD スキャン]** で、**[トリガー]** 列に [プルリクエスト] の値で記録されます。
- **ポリシーの適用**: 少なくとも 1 つの検出結果が IaC ページで定義された [スキャン失敗しきい値] を満たすか、それを超えている場合、スキャンは自動的に [失敗] ステータスをトリガーします。デフォル

トでは、スキャンが失敗しても PR のマージは妨げられません。ゲートとして使用し、問題が解決されるまでマージを防ぐには、リポジトリ設定でスキャンを **必須** としてマークする必要があります。必要な設定とアクセス許可に関する詳細については、Pull Request Scanning を参照してください。

> **注意:** 既存の CI/CD 統合がある場合、ここで設定されたスキャン失敗しきい値は、CI/CD パイプラインのしきい値設定をオーバーライドします。

サポートされている IaC ツール

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Tenable One Cloud Exposure では、次のコードフレームワークがサポートされます。

- Terraform (スキャン/同期)
- CloudFormation (スキャン)
- Azure Resource Manager (ARM)
- Bicep
- Helm
- Kubernetes

近い将来、追加の IaC フレームワークのサポートが計画されています。使用している特定のフレームワークがあり、サポートされているか確認する場合は、サポートへの問い合わせ。

Terraform

クラウドサイバーエクスポージャー は、Terraform HCL コードと Terraform plan ファイルの両方のスキャンをサポートしています。

- HCL ファイルには、`.tf` 拡張子があり、`terraform.tfvars`を使用する入力変数、または `.tf` ファイルと同じディレクトリにある `.auto.tfvars` 拡張子を持つファイルが必要です。環境変数の評価の詳細については、「制限を参照してください。

- Terraform plan ファイルは JSON 形式である必要があります。`planned_values` が抽出され、Tenable が理解できる形でビルトされた後、通常の terraform ファイルとしてスキャンされます。結果は plan ファイルを指します。

plan ファイルの作成方法については、関連する Terraform のドキュメントを参照してください。

plan ファイルを取得したら、以下のコマンドを実行して terraform plan を JSON 形式で取得します。

```
Bash

terraform show -json terraform.tfplan | jq '.' > terraform_plan.json
```

その後、この JSON plan を `paths` パラメーターの値として使用して、Tenable によってスキャンされるリポジトリパスを定義できます。詳細については、「GitHub アクションパラメーター を参照してください。

Terraform モジュール

クラウド サイバーエクスポージャー は、以下のように Terraform モジュールのスキャンをサポートします。

- **Terraform コード**:
  - 同じリポジトリ内のすべてのプライベート モジュール。
  - Terraform レジストリからのすべてのパブリックモジュール。
  - 統合された外部プライベートリポジトリ内のすべてのプライベート モジュール。詳細については、Terraform の統合リポジトリ内のプライベート モジュールスキャンを参照してください

  > **注意:** CI/CD 内の統合プライベート モジュールにアクセスするには、**git-tokens** というパラメーターをアクセストークンとして渡す必要があります。

- **Terraform plan**
  - すべてのモジュール。

Terraform コードのモジュールスキャン

Terraform コード用の Terraform モジュールスキャンは、モジュール化されたコードのより広範なコンテキストを考慮することで、セキュリティポスチャーを強化します。Tenable は、Terraform コードファイルによって呼び出されているすべてのモジュール (ローカルまたはリモート) を再帰的に分析し、モジュール内の変数と

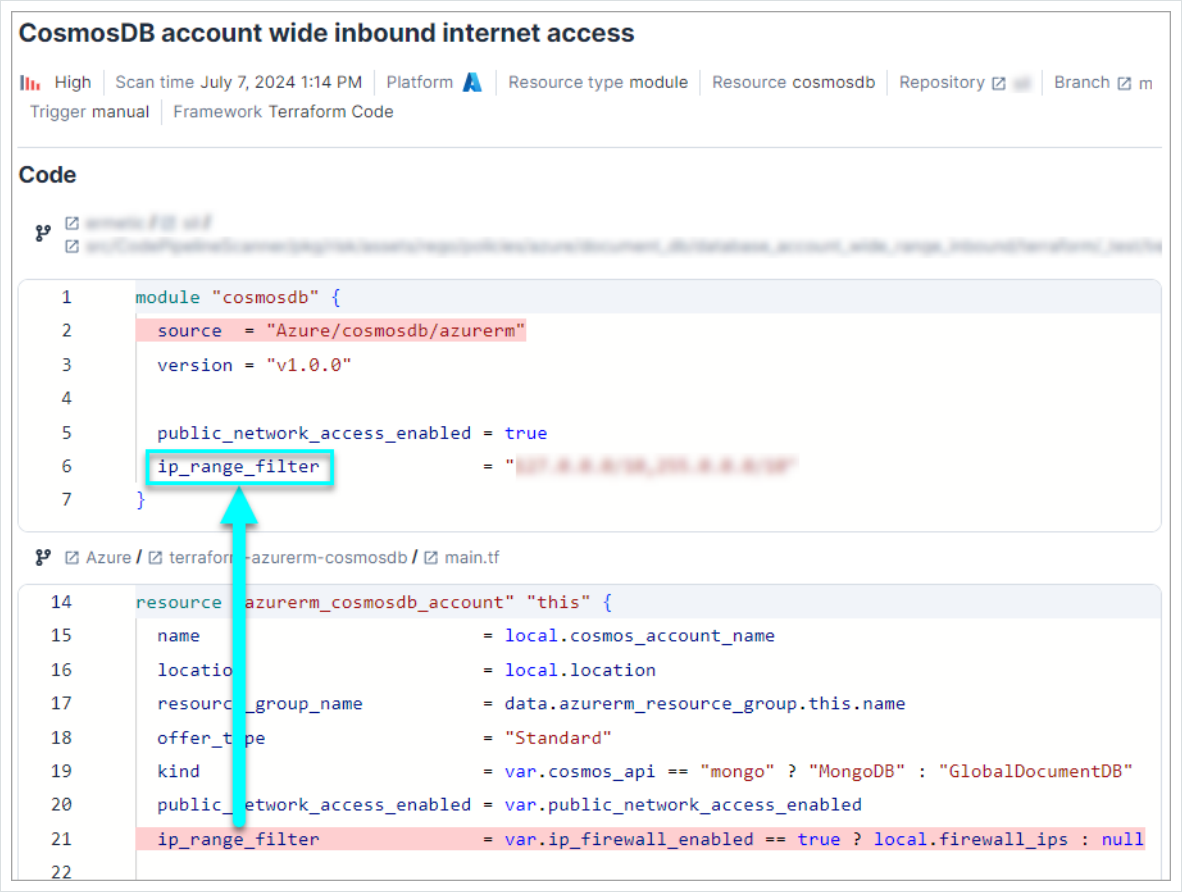
リソース定義を解決して、コード内の潜在的な設定ミスを検出します。Tenable はモジュールの階層全体をトレースし、すべてのリソースとその中で定義されている設定を特定します。

1 つの IaC 検出結果に複数のコードスニペットが表示されることがありますが、これは設定ミスを含むコードによって参照されるモジュールを表しています。

スキャンされたモジュールを表示するには

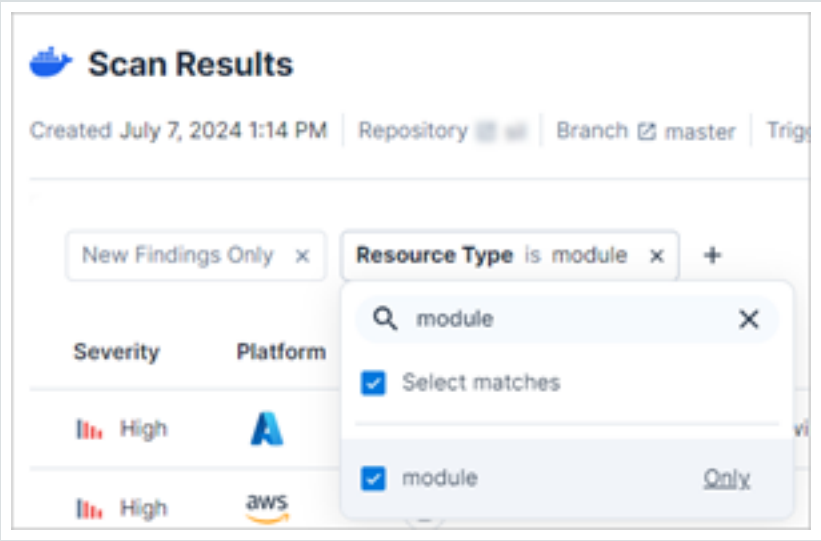
1. コードを接続した方法に応じて、次のいずれかを実行します。
    - **コードリポジトリの統合**
        1. クラウドサイバーエクスポージャーコンソールで、**[リスク> IaC の検出結果]** をクリックします。
        2. **[リソースタイプ]** フィルターを追加し、**モジュール**という単語を検索して選択することで、モジュールを含むものに結果を絞り込みます。
        3. 検出結果をクリックして、スキャンの詳細を表示します。コードによって参照されるモジュールごとに、追加のコードスニペットが表示されます。モジュール内で強調表示されている部分は、特定されたポリシーの設定ミスを表しており、コードの該当部分と関連

付けることができます。



- **CI/CD 統合**

  1. クラウド サイバーエクスポージャーコンソールで、**[コード スキャン>リスク]** をクリックします。
  2. 関連するスキャンを特定してクリックします (Terraform コード)。
  3. **[検出結果]** タブをクリックします。
  4. **[リソースタイプ]** フィルターを追加し、**モジュール**という単語を検索して選択することで、モジュールを含むものに結果を絞り込みます。



5. 検出結果をクリックして、スキャンの詳細を表示します。コードによって参照されるモジュールごとに、追加のコードスニペットが表示されます。モジュール内で強調表示されている部分は、特定されたポリシーの設定ミスを表しており、コードの該当部分と関連付けることができます。



Terraform の統合リポジトリ内のプライベートモジュールスキャン

Tenable は、CI/CD とリポジトリの両方で、認証されたプライベートリポジトリからプライベートモジュールのスキャンをサポートします。

- **CI/CD スキャン**: CI/CD で IaC スキャンを実行する場合は、**git-tokens** パラメーターを使用して、プライベートリポジトリに必要なアクセストークンを指定します。
- **リポジトリのスキャン**: 統合されたリポジトリの場合、Tenable は既存の認証を使用してプライベートモジュールにアクセスします。

以下は、CI/CD スキャンで **git-tokens** パラメーターを使用する方法の例です。

- 1 つのトークンを使用する

```
code-scanner iac scan --git-tokens "https://github.com/org=ghp_token123"
```

- 複数のトークンの使用:

```
code-scanner iac scan \
--git-tokens "https://github.com/org1=ghp_token1" \
--git-tokens "https://gitlab.com/org2=glpat_token2"
```

- コンマで区切られた複数のトークンの使用

```Bash
code-scanner iac scan \n  --git-tokens "https://github.com/org1=ghp_token1,https://gitlab.com/org2=glpat_token2"
```

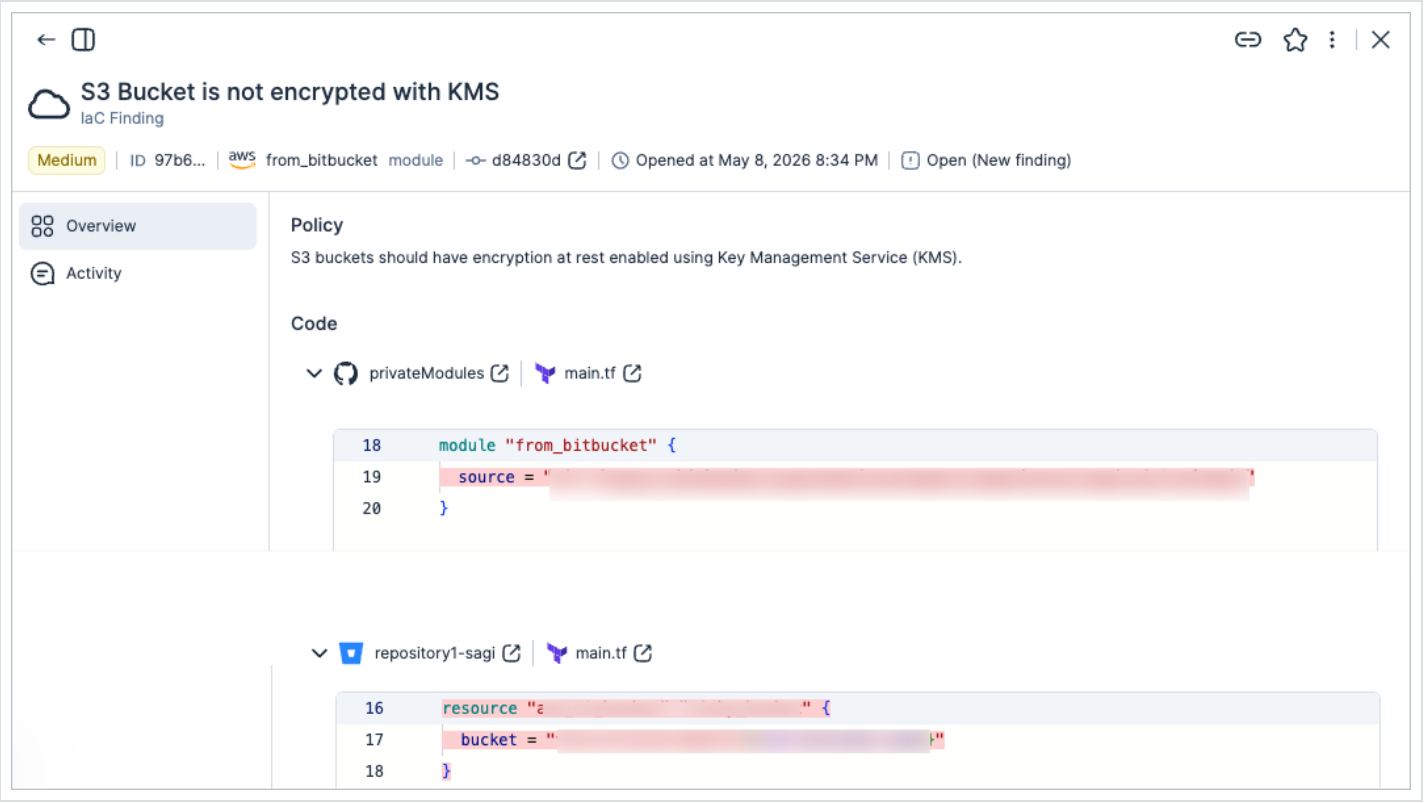
各部の説明

- **git-tokens** は、統合プライベートリポジトリ内のプライベートTerraformモジュールにアクセスするために使用されるパラメーターです。
- URL(<https://github.com/org1=ghp_token1>)値をリポジトリのアクセストークンに置き換えてください。

> **注意:** URL に「=」が含まれている場合は、「%3D」のパーセントエンコーディングに置き換えます。

スキャンされたプライベートモジュールの検出結果は、検出結果のコードセクションにも表示されます。

次の画像は、他のプライベートリポジトリにリンクされたプライベートリポジトリからの検出結果の例を示しています。



動的設定スキャン

Tenable では、動的な Terraform 設定のスキャンがサポートされます。Tenable は、ソースコードまたは変数ファイルのデフォルト値を使用して、カウント、for_each引数、および動的ブロックを分析します。これにより、拡張されたリソースや複雑なインフラ定義を可視化できます。

制限

クラウドサイバーエクスポージャー は変数と補間をサポートしていますが、関数と環境変数はサポートされていません。パイプラインを実行して特定の環境変数を割り当てると、Tenable はコードで見つかった設定を正しいものと見なします。

関数パラメーターとして使用される変数の場合は、以下の関数呼び出しで見られるように、ラップされた式として解析されます。

HCL

```
resource "aws_launch_configuration" "example" {
```

```
    image_id      = data.aws_ami.ubuntu.id
    instance_type = "${concat(list("${var.name}", "${var.other_name}"), var.node_tags)}"
    spot_price    = var.price
    user_data_base64 = "${var.data}=="
}
```

var.data = "a123B" とvar.price = 1.023 とすると、以下の例のように解析されます。

HCL

```
resource "aws_launch_configuration" "example" {
    image_id      = data.aws_ami.ubuntu.id
    instance_type = "${concat(list("${var.name}", "${var.other_name}"), var.node_tags)}"
    spot_price    = 1.023
    user_data_base64 = "a123B=="
}
```

CloudFormation

クラウドサイバーエクスポージャーでは、.json または .yaml 拡張子を持つCloudFormation テンプレートのスキャンがサポートされています。

制限

クラウドサイバーエクスポージャーは現在、以下のサポートを提供していません。

- 条件
- ネストされたスタックのスキャン
- 環境変数
- マクロ
- モジュールの使用
- 定義済みパラメーター
- 組み込み関数参照

ARM

クラウド サイバーエクスポージャー は、IaC セキュリティの一 環として Azure テンプレートをスキャンするために Azure Resource Manager (ARM) フレームワークをサポートしています。

制限

クラウド サイバーエクスポージャー は現 在 、以 下 の ARM 機 能をサポートしていません。

- コピーループにより作 成 された複 数 のリソースインスタンス (クラウド サイバーエクスポージャー は最 初 のインスタンスのみをスキャンします。
- 範 囲 とデプロイメント 機 能
    - `resourceGroup()`
    - `subscription()`
    - `tenant()`
    - `managementGroup()`
    - `deployment()`
    - `environment()`
- リソース機 能:
    - `resourceId()`
    - `pickZones()`
    - リスト 関 数 (例: `listKeys()`、`listSecrets()`)
- `reference()` 関 数
- リンクされたテンプレート または外 部 テンプレート
- ユーザー定 義 関 数
- パラメーターファイル (`parameters.json`)

Bicep

クラウド サイバーエクスポージャー は、IaC セキュリティの一 環として Azure Bicep のスキャンをサポートしています。

制限

クラウド サイバーエクスポージャー は現 在 、次 の Bicep 関 数 をサポートしていません。

- 拡 張 宣 言 (拡 張 性 プロバイダー)
- インポート宣 言 (コンパイル時 のインポート)
- モジュールループ (クラウド サイバーエクスポージャー は最 初 のインスタンスのみをスキャン)
- `existing` キーワードで宣 言 されたリソース
- リソースループによって作 成 された複 数 のリソースインスタンス (クラウド サイバーエクスポージャー は最 初 のインスタンスのみをスキャン)
- パラメーターファイル (`.bicepparam`)

Helm

制 限

クラウド サイバーエクスポージャー は現 在 、名 前 にテンプレート値 が含 まれているリソースや、テンプレート関 数 (`lookup` など) を呼 び出 すリソースをサポートしていません。

Kubernetes

制 限

クラウド サイバーエクスポージャー は現 在 、名 前 に変 数 が含 まれているリソースや動 的 に (`generateName` など) 生 成 されるリソースをサポートしていません

IaC 互 換 性 マトリクス

以 下 の表 に、各 クラウド サイバーエクスポージャー IaC 機 能 でサポートされているプラットフォームとツールを示します。

リポジトリ

機能	プラットフォーム	リポジトリ			
		Azure Repos 組織の追加	Bitbucket ワークスペースの追加	GitLab グループの追加	GitHub 組織の追加
Scan (スキャン)	Terraform コード	✓	✓	✓	✓
	Terraform plan	✕	✕	✕	✕
	CloudFormation	✓	✓	✓	✓
	ARM	✓	✓	✓	✓
	Bicep	✓	✓	✓	✓
問題をコードまでトレース (同期)	Terraform コード	✓	✓	✓	✓
検出結果の修正 (プルリクエスト経由)	Terraform コード	✓	✓	✓	✓

パイプライン

機能	プラットフォーム	パイプライン					
		GitHub アクションを追加する	Jenkins パイプラインの追加	Terraform Cloud Run タスクの追加	GitLab パイプラインの追加	Azure Pipelines の追加	別のパイプライ

機能	プラットフォーム	パイプライン					
							ンを追加する
Scan (スキャン)	Terraform コード	✓	✓	✕	✓	✓	✓
	Terraform plan	✓	✓	✓	✓	✓	✓
	CloudFormation	✓	✓	✕	✓	✓	✓
	ARM	✓	✓	✕	✓	✓	✓
	Bicep	✓	✓	✕	✓	✓	✓
問題をコードまでトレース (同期)	Terraform コード	✓	✓	✕	✕	✓	✓
検出結果の修正 (プルリクエスト	Terraform コード	✕	✕	✕	✕	✕	✕

機能	プラットフォーム	パイプライン					
経由)							

スキャンで使用される Tenable ポリシー

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

次のビルトイン Tenable One Cloud Exposure IaC ポリシーが、環境をスキャンするために使用されます。これらのポリシーは、Tenable ポリシーのサブセットにマッピングされます。

- AWS
- Azure
- GCP
- OCI
- Kubernetes
- その他

AWS

クラウドサイバーエクスポージャーは、次のビルトインポリシーを使用して AWS リソースをスキャンします。

カテゴリ	名前	ID	サポートされているフレームワーク
コンピューティング	EC2 インスタンスメタデータサービスが安全ではないバージョンをサポート	`aws-ec2-instance-metadata-service-version`	

カテゴリ	名前	ID	サポートされているフレームワーク
	Lambda 関数は複数の可用性ゾーンで動作しません	`aws-lambda-function-configuration-multi-availability-zone-not-exist`	
	Lambda 関数で非推奨のランタイムが使用されています	`aws-lambda-function-configuration-deprecated-runtime`	
	パブリック Lambda 関数	`aws-lambda-function-configuration-public-access-exists`	
データ	Athena ワークグループのクエリ結果が暗号化されていません	`aws-athena-workgroup-encryption-disabled`	
	Data Firehose ストリームが KMS で暗号化されていない	`aws-firehose-delivery-stream-encryption-disabled`	
	DMS エンドポイントの転送中の暗号化が有効になっていない	`aws-dms-endpoint-ssl-mode-disabled`	
	Redis OSS TLS の DMS エンドポイントが有効になっていない	`aws-dms-endpoint-redis-ssl-security-protocol-not-ssl-encryption`	
	DMS エンドポイント MongoDB の認証メカニズムが有効になっ	`aws-dms-endpoint-mongo-db-authentication-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	ていない	`disabled`	
	DMS レプリケーションインスタンスのマイナーバージョン自動アップグレードが有効になっていない	`aws-dms-replication-instance-minor-version-upgrade-disabled`	
	DMS レプリケーションインスタンスのパブリックアクセスが有効になっている	`aws-dms-replication-instance-public-ip-address-enabled`	
	DocumentDB クラスタのバックアップ保持期間が最小要件を満たしていない	`aws-doc-db-cluster-backup-retention-time-frame`	
	DocumentDB クラスタの削除保護が有効になっていない	`aws-rds-doc-db-cluster-delete-protection-disabled`	
	DynamoDB の削除保護が有効になっていない	`aws-dynamodb-table-delete-protection-disabled`	
	DynamoDB テーブルは KMS で暗号化されません	`aws-dynamodb-table-encryption-disabled`	
	EBS スナップショットは KMS で暗号化されません	`aws-ec2-snapshot-encryption-disabled`	
	EBS ボリュームは KMS で暗号	`aws-ec2-volume-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	化されません	encryption-disabled	
	ElastiCache Redis OSS クラスタキャッシュの自動バックアップが最小要件を満たしていません	aws-elasticache-replication-group-automatic-backups	
	ElastiCache Redis OSS クラスタキャッシュの自動フェイルオーバーが有効になっていません	aws-elasticache-replication-group-automatic-backups-disabled	
	ElastiCache Redis OSS クラスタキャッシュのマイナーバージョン自動アップグレードが有効になっていません	aws-elasticache-replication-group-auto-upgrade-minor-versions-disabled	
	ElastiCache Redis OSS クラスタキャッシュの転送中の暗号化が有効になっていません	aws-elasticache-replication-group-transit-encryption-mode-not-required	
	ElastiCache Redis OSS クラスタキャッシュがデフォルトのサブネットグループを使用しています	aws-elasticache-replication-group-default-subnet-group	
	EFS File System が KMS で暗号化されていません	aws-elastic-file-system-file-system-encryption-disabled	

カテゴリ	名前	ID	サポートされているフレームワーク
	Kinesis データストリームが KMS で暗号化されません	`aws-kinesis-stream-encryption-disabled`	
	KMS キーの自動キーローテーションが有効になっていません	`aws-kms-key-rotation-disabled`	
	Neptune クラスタのバックアップ保持期間が最小要件を満たしていない	`aws-rds-neptune-cluster-backup-retention-time-frame`	
	Neptune クラスタの削除保護が有効になっていない	`aws-rds-neptune-cluster-delete-protection-disabled`	
	OpenSearch ドメインノード間の転送中の暗号化が有効になっていない	`aws-es-domain-node-communication-encryption-disabled`	
	OpenSearch ドメインが KMS で暗号化されていない	`aws-es-domain-encryption-disabled`	
	公開 EC2 イメージ	`aws-ec2-image-public-access-exists`	
	公開 ECR リポジトリ	`aws-ecr-repository-public-access-exists`	
	公開 KMS キー	`aws-kms-key-public-access-exists`	

カテゴリ	名前	ID	サポートされているフレームワーク
	公開 OpenSearch ドメイン	`aws-es-domain-public-access-exists-cloud-formation`	
	公開 RDS スナップショット	`aws-rds-snapshot-public-access-exists`	
	パブリック S3 バケット	`aws-s3-bucket-public-access-exists`	
	公開のためのスキャントピック	`aws-sns-topic-public-access-exists`	
	パブリック SQS キュー	`aws-sqs-queue-public-access-exists`	
	RDS クラスタのマイナーバージョン自動アップグレードが有効になっていません	`aws-rds-cluster-minor-version-upgrade-disabled`	
	RDS クラスタのバックアップ保持期間が最小要件を満たしていない	`aws-rds-cluster-backup-retention-time-frame`	
	RDS クラスタの削除保護が有効になっていない	`aws-rds-cluster-delete-protection-disabled`	
	RDS クラスタが KMS で暗号化されていません	`aws-rds-cluster-storage-encryption-disabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	RDS インスタンスのマイナーバージョン自動アップグレードが有効になっていない	`aws-rds-database-instance-minor-version-upgrade-disabled`	
	RDS インスタンスのバックアップ保持期間が最小要件を満たしていない	`aws-rds-database-instance-backup-retention-time-frame`	
	RDS インスタンスの削除保護が有効になっていない	`aws-rds-database-instance-delete-protection-disabled`	
	RDS インスタンスが KMS で暗号化されません	`aws-rds-database-instance-storage-encryption-disabled`	
	Redshift クラスタのバックアップ保持期間が最小要件を満たしていない	`aws-redshift-cluster-backup-retention-time-frame`	
	Redshift クラスタが KMS で暗号化されていません	`aws-redshift-cluster-encryption-disabled`	
	S3 バケットのパブリックアクセスのブロックが有効になっていない	`aws-s3-bucket-block-public-access-disabled`	
	S3 バケットの転送中の暗号化が有効になっていない	`aws-s3-bucket-https-only-disabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	S3 バケットの MFA Delete が有効になっていません	`aws-s3-bucket-object-delete-mfa-disabled`	
	S3 バケットが KMS で暗号化されていません	`aws-s3-bucket-encryption-disabled`	
	SNS トピックが KMS で暗号化されません	`aws-sns-topic-encryption-disabled`	
	SQL サーバーの透過的データ暗号化が CMK で暗号化されていません	`azure-sql-server-default-encryption`	
	SQS キューが KMS で暗号化されません	`aws-sqs-queue-encryption-disabled`	
IAM	サードパーティの IAM ロールの外部 ID が設定されていません	`aws-iam-role-vendor-assume-role-policy-document-external-id-condition-not-exist`	
	EC2 インスタンス IAM Instance Profile が設定されていない	`aws-ec2-instance-instance-profile-not-exist`	
	完全な管理権限を持つ IAM ポリシーに「」が添付されています	`policies-aws-iam-principal-attached-policy-permission-scope-any`	

カテゴリ	名前	ID	サポートされているフレームワーク
	IAM ユーザーにポリシーが添付されています	`aws-iam-user-attached-policy`	
	パスワードの長さが最小要件を満たしていません	`aws-iam-password-length-policy`	
	公開 IAM ロール	`aws-iam-role-public-access-exists`	
Kubernetes	Kubernetes シークレットが KMS で暗号化されていません	`aws-eks-cluster-kubernetes-secret-encryption-disabled`	
ログ	API ゲートウェイ X-Ray のトレースが有効になっていない	`aws-api-gateway-v1-api-stages-x-ray-tracing-disabled`	
	Athena ワークグループは CloudWatch にログを公開していない	`aws-athena-workgroup-logging-disabled`	
	CloudFront ディストリビューションロギングが有効になっていません	`aws-cloudfront-distribution-logging-disabled`	
	CloudTrail ログが CMK で暗号化されていません	`aws-cloudtrail-trail-encryption-disabled`	
	CloudTrail ログが CloudWatch	`aws-cloudtrail-trail-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	にログを公開していない	`log-group-disabled`	
	CloudTrail S3バケットログファイル検証が有効になっていません	`aws-cloudtrail-trail-digest-disabled`	
	CloudTrail S3 バケットロギングが有効になっていません	`aws-cloudtrail-trail-bucket-event-disabled`	
	DocumentDB クラスタが CloudWatch Logs にログを公開していない	`aws-rds-doc-db-cluster-cloudwatch-logging-disabled`	
	Elastic Beanstalk 環境が CloudWatch Logs にログを公開していません	`aws-elastic-beanstalk-environment-cloudwatch-logging-disabled`	
	Neptune DB クラスタが CloudWatch Logs にログを公開していない	`aws-rds-neptune-cluster-cloudwatch-logging-disabled`	
	OpenSearch ドメインが CloudWatch Logs にログを公開していません	`aws-es-domain-cloudwatch-logging-disabled`	
	パブリック CloudTrail S3 バケット	`aws-cloudtrail-trail-bucket-public-access-enabled`	
	RDS クラスタが CloudWatch	`aws-es-domain-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	Logs にログを公開していない	`cloudwatch-logging-disabled`	
	RDS インスタンスが CloudWatch Logs にログを公開していない	`aws-rds-cluster-cloudwatch-logging-disabled`	
	VPC フローログが設定されていません	`aws-ec2-vpc-reject-flow-log-not-exist`	
ネットワーク	API ゲートウェイ API が WAF のウェブ ACL に関連付けられていません	`aws-api-gateway-api-web-acl-not-exists`	
	CloudFront ディストリビューションのカスタムオリジンで転送中の暗号化が有効になっていない	`aws-cloudfront-distribution-origin-https-only-disabled`	
	CloudFront ディストリビューションのデフォルトのルートオブジェクトが設定されていません	`aws-cloudfront-distribution-root-object-not-exists`	
	CloudFront ディストリビューションの安全でない通信	`aws-cloudfront-distribution-insecure-tls-protocol`	
	CloudFront ディストリビューションが WAF のウェブ ACL と関連付けられていません	`aws-cloudfront-distribution-web-acl-not-exists`	

カテゴリ	名前	ID	サポートされているフレームワーク
	CloudFront ディストリビューションはデフォルトの SSL 証明書を使用している	`aws-cloudfront-distribution-default-ssl-certificate`	
	CloudFront ディストリビューションの S3 オリジンアクセス制御が有効になっていない	`aws-cloudfront-distribution-s3-bucket-origin-access-control-disabled`	
	CloudFront ディストリビューションビューワーの転送中の暗号化が有効になっていない	`aws-cloudfront-distribution-https-only-disabled`	
	Lambda 関数が VPC に関連付けられていません	`aws-lambda-function-configuration-vpc-not-exists`	
	ロードバランサーのセキュアでない通信	`aws-ec2-load-balancer-listener-insecure-ssl-protocol-exists`	
	ネットワーク ACL の無制限のインバウンドインターネットアクセス	`policies-aws-ec2-network-acl-inbound-rule-subnet-any-exists`	
	EC2 インスタンスがインターネットに公開されています	`aws-ec2-instance-inbound-external-access`	
	パブリックロードバランサー	`aws-elb-load-balancer-`	

カテゴリ	名前	ID	サポートされているフレームワーク
		`inbound-external`	
	公開 RDS インスタンス	`aws-rds-database-instance-inbound-external-access`	
	公開 Redshift クラスター	`aws-redshift-cluster-inbound-external-access`	
	Route 53 ホストゾーン DNSSEC が有効になっていません	`aws-route-53hosted-zone-signing-disabled`	
	セキュリティグループの無制限インバウンドインターネットアクセス	`aws-ec2-security-group-inbound-rule-subnet-any-exists`	
シークレット	CloudFormation スタックは、機密情報を漏洩しています	`aws-cloudformation-stack-secret-exists`	
	EC2 インスタンスがシークレットを漏洩しています	`aws-ec2-instance-user-data-secret-exists`	
	ECS タスク定義は、シークレットを漏洩しています	`aws-ecs-task-definition-environment-variable-secret-exists`	
	Lambda 関数が機密情報を漏洩しています	`aws-lambda-function-configuration-`	

カテゴリ	名前	ID	サポートされているフレームワーク
		`environment-variable-secret-exists`	
	パブリック Secrets Manager シークレット	`aws-secrets-manager-secret-public-access-exists`	
	Secrets Manager のシークレット自動ローテーションが有効になっていません	`aws-secrets-manager-secret-rotation-disabled`	
	System Manager パラメーターは、秘密情報を漏洩しています	`aws-ssm-parameter-secret-exists`	

Azure

クラウド サイバーエクスポージャー は、次のビルト インポリシーを使用して Azure リソースをスキャンします。

カテゴリ	名前	ID	サポートされているフレームワーク
コンピューティング	App Service の FTP の暗号化が有効になっていない	`azure-web-application-ftp-status-all-allowed`	

カテゴリ	名前	ID	サポートされているフレームワーク
	App Service の HTTP バージョンが最小要件を満たしていない	`azure-web-application-http-min-version`	
	App Service Microsoft Entra ID の登録が設定されていない	`azure-web-application-managed-identity-not-exists`	
	App Service のリモートデバッグが有効である	`azure-web-application-remote-debugging-enabled`	
	仮想マシンが管理されていないディスクを使用しています	`azure-compute-virtual-machine-unmanaged-disk-exists`	
	仮想マシンのトラステッド起動が有効になっていない	`azure-compute-virtual-machine-trusted-launch-disabled`	
データ	アプリサービスの安全でない通信	`azure-web-application-insecure-tls-protocol`	
	Event Hubs 名前空間全体のインバウンドインターネットアクセス	`azure-event-hub-namespace-inbound-external-wide-range`	
	Key Vault 証明書の自動ローテーションが有効になって	`azure-key-vault-vault-certificate-rotation-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	いない	`disabled`	
	キーボールト削除保護が有効になっていません	`azure-key-vault-vault-soft-delete-disabled`	
	Key Vault キーの自動キーローテーションが有効になっていません	`azure-key-vault-vault-key-not-rotated`	
	キーボールトキーの有効期限が設定されていない	`azure-key-vault-vault-key-expiration-disabled`	
	Key Vault キーがローテーションされていません	`azure-key-vault-vault-key-not-rotated`	
	Key Vault シークレットがローテーションされていない	`azure-key-vault-vault-secret-not-rotated`	
	マネージドディスクのデータアクセス認証が有効になっていない	`azure-compute-disk-data-access-authentication-disabled`	
	マネージドディスクはパブリックアクセスをブロックしない	`azure-compute-disk-network-access-policy-allow-all`	
	MySQL データベースサーバーで、Microsoft Entra ID のみの認証が有効になって	`azure-mysql-flexible-server-aad-only-authentication-disabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	いません		
	PostgreSQLデータベースサーバーで、Microsoft Entra IDのみの認証が有効になっていません	`azure-postgresql-flexible-server-aad-only-authentication-disabled`	
	パブリックストレージアカウントblobコンテナ	`azure-storage-storage-account-blob-container-public-access-exists`	
	SQL データベースが透過的データ暗号化で暗号化されません	`azure-sql-server-database-encryption-disabled`	
	ストレージアカウントの SQL Server 監査保持が設定されていません	`azure-server-event-retention-time-frame`	
	SQL Server の Microsoft Defender が有効になっていません	`azure-sql-server-microsoft-defender-disabled`	
	SQL サーバー Microsoft Entra ID 管理者が設定されていません	`policies-azure-sql-server-aad-authentication-administrator-principal-not-exists`	

カテゴリ	名前	ID	サポートされているフレームワーク
	SQL サーバー Microsoft Entra ID のみの認証が有効になっていません	`azure-sql-server-aad-only-authentication-disabled`	
	ストレージアカウントのクロステナントレプリケーションが有効になっている	`azure-storage-storage-account-cross-tenant-replication-enabled`	
	ストレージアカウントインフラの暗号化が有効になっていない	`azure-storage-storage-account-infrastructure-encryption-disabled`	
	ストレージアカウントが CMK で暗号化されません	`azure-storage-storage-account-default-encryption`	
	ストレージアカウントのソフトデリート保護が有効になっていません	`azure-storage-storage-account-soft-delete-disabled`	
	App Service の転送中の暗号化が有効になっていない	`azure-web-application-https-only-disabled`	
	MySQL データベースサーバーの転送中の暗号化が有効になっていない	`azure-mysql-server-https-only-disabled`	
	PostgreSQL データベースサーバーの転送中の暗号化	`azure-postgresql-server-https-only-disabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	が有効になっていない		
	転送中のストレージアカウントが有効になっていない	`azure-storage-storage-account-https-only-disabled`	
IAM	コンテナレジストリ管理者ユーザーが有効になっている	`azure-container-registry-registry-access-key-enabled`	
	CosmosDB アカウントキー管理アクセスが有効になっている	`azure-document-db-database-account-management-key-access-enabled`	
	キーボールトロールベースのアクセスコントロールが有効になっていません	`azure-key-vault-vault-rbac-disabled`	
	サブスクリプションで管理者ロールを持つ Microsoft Entra ID 外部ユーザーまたはゲストユーザー	`azure-directory-guest-user-administrator`	
	ストレージアカウントの共有キーアクセスが有効になっている	`azure-storage-storage_account_shared_key_access_enabled`	
Kubernetes	Kubernetes シークレットが CMK で暗号化されていません	`azure-container-service-managed-cluster-kubernetes-secret-encryption-disabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
ログ	アクティビティログブロブコンテナが CMK で暗号化されません	`azure-insights-diagnostic-settings-storage-account-blob-container-default-encryption`	
	キーボールトログが有効になっていません	`azure-key-vault-vault-event-disabled`	
	MySQL データベースサーバーのパラメーター audit_log_enabled が有効になっていません	`azure-mysql-flexible-server-audit-log-disabled`	
	MySQL データベースサーバーのパラメーター audit_log_events が最小要件を満たしていません	`azure-mysql-flexible-server-audit-log-connection-event-disabled`	
	PostgreSQL データベースサーバー log_retation_day が最小要件を満たしていません	`azure-postgresql-server-log-retention`	
	PostgreSQL データベースサーバーパラメーターの接続スロットリングが有効化されていません	`azure-postgresql-server-connection-throttling-disabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	PostgreSQL データベースサーバーパラメーター log_checkpoints が有効になっていません	`azure-postgresql-server-log-checkpoints-disabled`	
	PostgreSQL データベースサーバーパラメーター log_connections が有効になっていません	`azure-postgresql-server-log-connections-disabled`	
	PostgreSQL データベースサーバーパラメーター log_disconnections が有効になっていません	`azure-postgresql-server-log-disconnections-disabled`	
	公開アクティビティログブロブコンテナ	`azure-insights-diagnostic-settings-storage-account-blob-container-public-access-enabled`	
	SQL サーバー監査が有効になっていません	`azure-sql-server-event-disabled`	
	ストレージアカウントブロブサービスのログが有効になっていません	`azure-storage-storage-account-blob-service-diagnostic-settings-log-category-not-enabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	ストレージアカウントキューサービスのログが有効になっていません	azure-storage-storage-account-queue-service-diagnostic-settings-log-category-not-enabled	
	ストレージアカウントテーブルサービスのログが有効になっていません	azure-storage-storage-account-table-service-diagnostic-settings-log-category-not-enabled	
ネットワーク	アプリサービスのSCMサイト全体のインバウンドインターネットアクセス	azure-web-application-scm-inbound-external-wide-range	
	コンテナレジストリのワイドインバウンドインターネットアクセス	azure-container-registry-registry-inbound-external-wide-range	
	CosmosDBアカウントがプライベートエンドポイントに関連付けられていません	azure-document-db-database-account-private-endpoint-not-exists	
	CosmosDBアカウント全体のインバウンドインターネットアクセス	azure-document-db-database-account-wide-range-inbound	
	キーボールトファイアウォール	azure-key-vault-vault-wide-	

カテゴリ	名前	ID	サポートされているフレームワーク
	のワイドインバウンドインターネットアクセス	`range-inbound`	
	Key Vault がプライベートエンドポイントに関連付けられていません	`azure-key-vault-vault-private-endpoint-not-exists`	
	ロジックアプリ全体のインバウンドインターネットアクセス	`azure-logic-workflow-inbound-external-wide-range`	
	MySQL データベースサーバーのパラメーター tls_version が最小要件を満たしていません	`azure-mysql-flexible-server-insecure-tls-protocol`	
	MySQL データベースサーバー全体のインバウンドインターネットアクセス	`azure-mysql-server-wide-range-inbound`	
	サービスタグ経由のネットワークセキュリティグループの安全でないインバウンドインターネットアクセス	`policies-azure-network-network-security-group-inbound-rule-insecure-service-tag`	
	ネットワークセキュリティグループの制限されない RDP インバウンドのインターネットアクセ	`azure-network-network-security-group-inbound-rule-subnet-any-rdp-exists`	

カテゴリ	名前	ID	サポートされているフレームワーク
	ス		
	ネットワークセキュリティグループの制限されない SSH インバウンドのインターネットアクセス	azure-network-network-security-group-inbound-rule-subnet-any-ssh-exists	
	ネットワークセキュリティグループの無制限 UDP インバウンドインターネットアクセス	azure-network-networksecuritygroup-inbound-rule-subnet-any-udp-exists	
	PostgreSQL データベースサーバーのワイドインバウンドインターネットアクセス	azure-postgresql-server-wide-range-inbound	
	パブリックアプリサービス	azure-web-application-inbound-external-wide-range	
	SQL サーバーワイドインバウンドインターネットアクセス	azure-sql-server-wide-range-inbound	
	ストレージアカウント Azure の信頼できるサービスへのアクセスが有効になっていません	azure-storage-storage-account-allow-any-azure-trusted-services-network-access-disabled	
	ストレージアカウントの安全で	azure-storage-storage-	

カテゴリ	名前	ID	サポートされているフレームワーク
	ない通信	`account-insecure-tls-protocol`	
	ストレージアカウントがプライベートエンドポイントに関連付けられていません	`azure-storage-storage-account-private-endpoint-not-exists`	
	ストレージアカウントワイドのインバウンドインターネットアクセス	`azure-storage-storage-account-wide-range-inbound`	
	サブネットの無制限のインバウンドインターネットアクセス	`azure-network-virtual-network-subnet-unrestricted-inbound-access`	
シークレット	アプリサービスでシークレットが公開されている	`azure-application-app-settings-secret-exists`	
	キーボールトシークレットの有効期限が設定されていません	`azure-key-vault-vault-secret-expiration-disabled`	
	論理アプリが機密情報を漏洩しています	`azure-logic-workflow-secret-exists`	
	仮想マシンでシークレットが公開されています	`azure-compute-virtual-machine-user-data-secret-exists`	

GCP

クラウド サイバーエクスポージャー は、次 のビルト インポリシーを使 用して GCP リソースをスキャンします。

カテゴリ	名 前	ID	サポートされているフレームワーク
コンピューティング	ロード バランサーのバックエンド サービスログが有 効になっていません	`gcp-compute-backend-service-logging-not-enabled`	
	プロジェクト OS ログインが有効になっていません	`gcp-compute-project-ssh-iam-not-enabled`	
	パブリック Cloud Functions	`gcp-functions-function-public-access-exists`	
	パブリック Cloud Run サービス	`gcp-cloud-run-service-public-access-exists`	
	公 開 用 Compute Engine イメージ	`gcp-compute-image-public-access-exists`	
	VM インスタンスの「プロジェクトワイド SSH キーをブロック」が有 効になっていない	`gcp-compute-instance-block-project-wide-ssh-keys-not-enabled`	
	VM インスタンスの機 密 情 報コンピューティングが有 効になっていない	`gcp-compute-instance-memory-encryption-not-enabled`	
	VM インスタンスの IP フォワー	`gcp-compute-instance-ip-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	ディングが有効になっている	`forwarding-enabled`	
	VM インスタンスの保護された VM が有効になっていない	`gcp-compute-instance-shielded-not-enabled`	
	VM インスタンスはデフォルトのサービスアカウントを使用しています	`gcp-compute-instance-default-service-account`	
	VM インスタンスのシリアルポートアクセスが有効化されている	`gcp-compute-instance-ssh-serial-port-enabled`	
データ	App Engine サービスの転送中の暗号化が有効になっていない	`gcp-app-engine-application-service-unencrypted-transport-exists`	
	BigQuery データセットのデフォルトの暗号化が CMEK で設定されていません	`gcp-big-query-dataset-encryption-disabled`	
	BigQuery データセットテーブルが CMEK で暗号化されていません	`gcp-big-query-dataset-table-encryption-disabled`	
	クラウド KMS キーローテーションが設定されていません	`gcp-kms-key-ring-key-rotation-time-frame`	
	クラウド SQL インスタンスの「ク	`gcp-sql-instance-sql-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	ロスデータベースオーナー権限チェーン」フラグが有効になっています	`server-cross-database-implicit-permissions-enabled`	
	Cloud SQL インスタンスの転送中の暗号化が有効になっていない	`gcp-sql-instance-https-only-disabled`	
	クラウド SQL インスタンスの「外部スクリプトの有効化」フラグが有効化されている	`gcp-sql-instance-sql-server-script-execution-enabled`	
	クラウド SQL インスタンスの「リモートアクセス」フラグが有効になっている	`gcp-sql-instance-sql-server-cross-instance-procedure-execution-enabled`	
	Cloud SQL インスタンスの「user options」フラグが有効化されている	`gcp-sql-instance-sql-server-user-options-enabled`	
	クラウド SQL インスタンスの自動バックアップが有効になっていません	`gcp-sql-instance-backup-disabled`	
	クラウド SQL MySQL インスタンスの「local_infile」フラグが有効化されている	`gcp-sql-instance-mysql-load-client-file-enabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	クラウド SQL MySQL インスタンスの「skip_show_database」フラグが有効になっていない	`gcp-sql-instance-mysql-list-databases-permission-required-disabled`	
	クラウドストレージのバケットロックポリシーが設定されていない	`gcp-storage-bucket-locked-retention-policy-not-enabled`	
	パブリックアーティファクトレジストリ	`gcp-artifact-registry-public-access-exists`	
	公開 BigQuery データセット	`gcp-big-query-dataset-public-access-exists`	
	パブリッククラウド KMS キー	`gcp-kms-key-ring-key-public-access-exists`	
	パブリッククラウド KMS キーリング	`gcp-kms-key-ring-public-access-exists`	
	パブリッククラウドストレージバケット	`gcp-storage-bucket-public-access-exists`	
	パブリック KMS キー	`gcp-kms-key-public-access-exists`	
	公開 KMS キーリング	`gcp-kms-key-ring-public-access-exists`	

カテゴリ	名前	ID	サポートされているフレームワーク
	Public Pub/Sub サブスクリプション	`gcp-pub-sub-subscription-public-access-exists`	
	公開 Pub/Sub トピック	`gcp-pub-sub-topic-public-access-exists`	
IAM	クラウド SQL インスタンスの「コンテナデータベース認証」フラグが有効化されている	`gcp-iam-service-account-user-managed-key-exists`	
	クラウドストレージバケットの統一アクセスポリシーが有効になっていません	`gcp-storage-bucket-uniform-access-control-disabled`	
	プロジェクト API キーの API 制限が設定されていません	`gcp-api-keys-key-service-restriction-not-exists`	
	プロジェクト API キーのアプリケーション制限が設定されていません	`gcp-api-keys-key-client-restriction-not-exists`	
	サービスアカウントはプロジェクト内のすべてのサービスアカウントになりすますことができます	`gcp-principal-service-account-wide-scope-impersonate-service-account-action-exists`	
	サービスアカウントにユーザー管理のキーがある	`gcp-iam-service-account-user-managed-key-exists`	

カテゴリ	名前	ID	サポートされているフレームワーク
	サービスアカウントがプロジェクトで権限がある	`gcp-principal-service-account-wide-scope-administrator-role`	
	サービスアカウントユーザーが管理するキーがローテーションされない	`gcp-iam-service-account-unrotated-user-managed-key`	
	ユーザーは、プロジェクト内のすべてのサービスアカウントになりすますことができます	`gcp-principal-user-wide-scrope-impersonate-service-account-action-exists`	
Kubernetes	Kubernetes シークレットが CMEK で暗号化されていません	`gcp-container-cluster-kubernetes-secret-encryption-disabled`	
ログ	監査ログが有効になっていません	`gcp-logging-audit-log-tenant-default-not-enabled`	
	クラウド SQL インスタンス「3625トレースフラグ」フラグが有効になっていません	`gcp-instance-sql-server-log-mask-parameters-disabled`	
	クラウド SQL PostgreSQL インスタンスの「cloudsql.enable_pgaudit」フラグが有効になって	`gcp-sql-instance-postgresql-audit-disabled`	

カテゴリ	名前	ID	サポートされているフレームワーク
	いません		
	クラウド SQL PostgreSQL インスタンスの「log_connections」フラグが有効になっていません	`gcp-sql-instance-postgresql-log-connections-disabled`	
	クラウド SQL PostgreSQL インスタンスの「log_disconnections」フラグが有効になっていません	`gcp-sql-instance-postgresql-log-disconnections-disabled`	
	Cloud SQL PostgreSQLインスタンスの「log_error_verbosity」フラグが最小要件を満たさない	`gcp-sql-instance-postgresql-log-error-verbosity`	
	クラウド SQL PostgreSQL インスタンスの「log_hostname」フラグが有効になっていない	`gcp-sql-instance-postgresql-log-connections-host-name-disabled`	
	クラウド SQL PostgreSQL インスタンス「log_min_duration_statement」フラグが有効化されている	`gcp-sql-instance-postgresql-min-duration-log-query-enabled`	
	Cloud SQL PostgreSQLインスタンスの「log_min_error_	`gcp-sql-instance-postgresql-min-log-level-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	statement」フラグが最小要件を満たさない	`log-query`	
	Cloud SQL PostgreSQLインスタンスの「log_min_messages」フラグが最小要件を満たさない	`gcp-sql-instance-postgresql-log-min-level`	
	Cloud SQL PostgreSQLインスタンスの「log_statement」フラグが最小要件を満たさない	`gcp-sql-instance-postgresql-statement-log-disabled`	
ネットワーク	クラウド SQL インスタンスの「ユーザー接続」フラグが最小要件を満たさない	`gcp-sql-instance-sql-server-user-max-connections-exists`	
	クラウド SQL インスタンスのワイドインバウンドインターネットアクセス	`gcp-sql-instance-wide-range-inbound`	
	ロードバランサー SSL ポリシーの安全でない通信	`gcp-compute-load-balancer-insecure-ssl-policy`	
	VPC フローログが有効になっていません	`gcp-compute-vpc-flow-logs-not-enabled`	
	VPC ネットワークの制限されない ICMP インバウンドインター	`gcp-compute-vpc-unrestricted-icmp-`	

カテゴリ	名前	ID	サポートされているフレームワーク
	ネットアクセス	`inbound-access`	
	VPC ネットワークの制限されない RDP でのインバウンドインターネットアクセス	`gcp-compute-vpc-unrestricted-rdp-inbound-access`	
	VPC ネットワークの制限されていない SSH インバウンドのインターネットアクセス	`gcp-compute-vpc-unrestricted-ssh-inbound-access`	
シークレット	App Engine サービスは、機密情報を漏洩しています	`gcp-app-engine-application-service-environment-variable-secret-exists`	
	Cloud Functions でシークレットが公開されています	`gcp-functions-function-environment-variable-secret-exists`	
	Cloud Run サービスは、シークレットを漏洩しています	`gcp-cloud-run-service-environment-variable-secret-exists`	
	Secret Manager のシークレットのローテーションが設定されていません	`gcp-secret-manager-secret-rotation-time-frame`	
	VM インスタンスがシークレットを漏洩しています	`gcp-compute-instance-startup-script-secret-`	

カテゴリ	名前	ID	サポートされているフレームワーク
		exists	

OCI

クラウド サイバーエクスポージャー は、次 のビルト インポリシーを使 用して OCI リソースをスキャンします。

カテゴリ	名前	ID	サポートされているフレームワーク
データ	起動ボリュームが CMK で暗号化されません	oci-block-storage-boot-volume-default-encryption	
	ファイルシステムが CMK で暗号化されていません	oci-fss-file-system-default-encryption	
	ファイルシステムのルートユーザーアクセスが制限されていない	oci-fss-file-system-mount-target-export-option-identity-squash-root-not-enabled	
IAM	パスワード期限切れポリシーが最小要件を満たしていません	oci-iam-domain-password-expiration-policy	
	パスワード長ポリシーが最小要件を満たしていません	oci-iam-domain-password-length-policy	
	パスワード再利用ポリシーが最	oci-iam-domain-password-reuse-	

カテゴリ	名前	ID	サポートされているフレームワーク
	小要件を満たしていません	policy	
ログ	オブジェクトストレージバケットのオブジェクトのログが有効になっていない	oci-object-storage-bucket-log-category-write-not-exists	
ネットワーク	ネットワークセキュリティグループの無制限の RDP インバウンドインターネットアクセス	oci-networking-network-security-group-inbound-rule-subnet-any-rdp-exists	
	セキュリティグループの無制限の SSH インバウンドインターネットアクセス	oci-networking-network-security-group-inbound-rule-subnet-any-ssh-exists	
	セキュリティリストの無制限の RDP インバウンドインターネットアクセス	oci-networking-security-list-inbound-rule-subnet-any-rdp-exists	
	セキュリティリストの無制限の SSH インバウンドインターネットアクセス	oci-networking-security-list-inbound-rule-subnet-any-ssh-exists	
	VCN フローログが有効化されていない	oci-networking-vcn-flow-logs-not-enabled	

Kubernetes

次のビルトインポリシーは、よくある設定ミスやセキュリティリスクに対して Kubernetes 設定をスキャンします。

名前	ID	サポートされているフレームワーク
Kubernetes クラスタには、過剰な権限を持つ Role と ClusterRole が含まれています	`kubernetes-cluster-pattern-role-exists`	
Kubernetes クラスタに、クラスタ管理者ロールを割り当てるロールバインディングが含まれている	`kubernetes-cluster-cluster-admin-role-binding-exists`	
Kubernetes クラスタにより、デフォルトの名前空間が使用されています	`kubernetes-cluster-default-namespace-used`	
Kubernetes に特権として実行するコンテナがあります	`kubernetes-workload-resource-container-privileged`	
Kubernetes 名前空間デフォルトサービスアカウントが頻繁に使用されています	`kubernetes-namespace-default-service-account-role-binding-exists`	
Kubernetes 名前空間に制限付きポリシーが設定されていません	`kubernetes-namespace-restricted-pod-security-standard-not-exist`	
Kubernetes 名前空間に機能が割り当てられたコンテナがあります	`kubernetes-namespace-workload-resource-container-capability`	
Kubernetes Pod に権限昇格を許可するコンテナがあります	`kubernetes-namespace-workload-resource-container-privilege-`	

名前	ID	サポートされているフレームワーク
	escalation	
Kubernetes Pod にルートユーザーとして実行するコンテナがあります	kubernetes-namespace-workload-resource-container-root-user-enabled	
Kubernetes Pod にホスト IPC 名前空間を共有するコンテナがあります	kubernetes-namespace-workload-resource-host-namespace-inter-process-communication-enabled	
Kubernetes Pod にホストネットワーク名前空間を共有するコンテナがあります	kubernetes-namespace-workload-resource-host-namespace-network-enabled	
Kubernetes Pod にホストプロセス ID 名前空間を共有するコンテナがあります	kubernetes-namespace-workload-resource-host-namespace-process-id-enabled	
Kubernetes Pod に HostPath ボリュームを使用するコンテナがあります	kubernetes-namespace-workload-resource-volume-host-path-exists	
Kubernetes Pod に hostPort を使用するコンテナがあります	kubernetes-namespace-workload-resource-container-host-port-exists	
Kubernetes Pod に書き込み可能なルートファイルシステムを含むコンテナがあります	kubernetes-namespace-workload-resource-container-read-only-root-filesystem-disabled	

名前	ID	サポートされているフレームワーク
Kubernetes Pod に機密性の高いホストファイルシステムがマウントされたコンテナがあります	`kubernetes-namespace-workload-resource-volume-sensitive-host-path-exists`	
Kubernetes シークレットは環境変数として使用されます	`kubernetes-workload-resource-environment-variable-secret-reference`	
Kubernetes クラスタ内の過剰な権限を持ちパブリックにアクセスできるグループまたはユーザー	`kubernetes-cluster-authentication-principal-role-binding-exists`	

その他

次のポリシーは、単一のクラウドプロバイダーに固有でない一般的な IaC 設定に適用されます。

名前	ID	サポートされているフレームワーク
Terraform 設定の DNS データブロック	`code-terraform-dns-record-set-exists`	
Terraform 設定の外部データブロック	`code-terraform-external-exists`	

よくある質問: 除外

除外により、検出結果を無視したり、ビジネスの文脈に基づいて検出結果の深刻度を調整したりできます。除外の仕組みに関する詳細な説明は、**除外** のドキュメントを参照してください。

> FAQ インデックス

- 除外の定義
- 除外を定義する方法
- 除外されたリソースを表示する
- ポリシーごとの除外
- 除外が有効になるタイミング
- 除外の有効期限と削除
- 2 つの除外が同じ検出結果を対象としている場合はどうなりますか? 誰が勝つか?
- 検出結果を既存の除外に追加する

除外の定義

> 除外とは何ですか?

除外は、アカウント、ポリシー、リソース、深刻度などの定義された条件に基づいて、検出結果を **無視** するか、**深刻度を変更** することで、検出結果の処理方法を調整するルールです。

除外を使用すると、可視性と監査可能性を維持しながら、意図的な設定または許容された設定が認められます。

たとえば、Dev アカウントがロードバランサーを意図的にインターネットに公開した場合、env:dev のタグ付けされたリソースのロードバランサーがインターネットポリシーに公開されていることからのすべての検出結果を無視する除外を作成できます。

詳細については、「 除外を定義する」を参照してください。

除外を定義する方法

> 除外のターゲットはどのように判断すればよいですか?

明確なビジネスケースに一致する検出結果のみをターゲットにします。どの設定が意図的、一時的、または低リスクであるかを特定し、それらの検出結果に対応するために必要な条件を設定します。

たとえば、開発環境が意図的にパブリック S3 バケットを使用している場合、以下をターゲットにできます。

- Dev アカウント、
- パブリック S3 バケットポリシー
- タグ付けされたリソース env:dev

詳細については、「除外を定義するを参照してください。

除外されたリソースを表示する

> 除外されているリソースを確認するにはどうすればよいですか?

[除外] ページで、確認する除外をクリックします。スライドアウトの [リソース] タブを開くと、除外の条件に現在一致するすべてのリソースが表示されます。

このリストは、各スキャンサイクルの後に更新されます。

ポリシーごとの除外

> 特定のポリシーに影響を与えているすべての除外を確認するにはどうすればよいですか?

[Policies] (ポリシー) ページで、確認するポリシーをクリックします。ポリシーのスライド式パネルで [除外] タブを開くと、そのポリシーを対象とするすべての除外が、その範囲やアクションなどに表示されます。

除外が有効になるタイミング

> 除外を作成または編集した後、いつ有効になりますか?

[除外] ページで作成または更新された除外は、次のスキャンサイクルの後に有効になります。スキャンが完了すると、一致するすべての検出結果が除外のアクション (無視または深刻度の変更) に基づいて更新されます。

[検出結果] ページから作成した除外は、選択した検出結果に即座に適用されますが、完全なカバレッジは次回のスキャンで完了します。

詳細については、「除外」を参照してください。

除外の有効期限と削除

> 除外の有効期限が切れたり削除されたりするとどうなりますか?

いずれの場合も、除外は次のスキャンサイクルで適用されなくなります。無視された検出結果や深刻度が変更された検出結果は、別の除外が引き続き適用されない限り、元の状態に戻ります。

競合する除外

> 2 つの除外が同じ検出結果を対象としている場合はどうなりますか? 誰が勝つのか?

複数の除外が同じ検出結果を対象としている場合は、より明確な範囲を持つものが優先されます。範囲が同様に明確である場合は、前の除外 (最初に作成された除外) が適用されます。

優先度は、アクションタイプ (深刻度 [無視] と [変更] の深刻度) ごとに個別に評価されます。検出結果は、アクションごとに 1 つの除外設定できます。

優先順位:

- より具体的な範囲での優先
- 範囲が一致する場合は、古い除外が優先されます

詳細については、「競合の解決」を参照してください。

検出結果を既存の除外に追加する

既存の除外に特定の検出結果を追加できますか?

はい。[検出結果] ページで、1 つ以上の検出結果を選択し、**[無視]** を選択します。検出結果が対象となる除外と一致する場合は、ダイアログに **[既存の除外に追加]** がオプションとして表示されます。

このオプションが使用できない場合は、それらの検出結果と互換性のない既存の除外がないことを意味します。互換性は、次のような要因によって異なります。

- 同じポリシー
- 同じ範囲
- [Action] セット [Ignore] (無視)
- 深刻度フィルターなし
- 同じ検出結果タイプ (クラウドまたは IaC)

詳細については、「除外を作成する」を参照してください。

AI-SPM

注意: これは Tenable の AI-SPM 機能の概念上の概要です。Tenable One Cloud Exposure コンソールを介して AI リスクを検出する方法については、AI リスクを検出する方法参照してください。

AI-SPM(人工知能を活用したセキュリティ態勢管理 は、AI/ML システムのセキュリティと整合性を維持するための包括的なアプローチです。これには、AI モデル、データ、インフラのセキュリティ態勢の継続的なモニタリング、評価、改善が含まれます。従来のセキュリティの範囲を超えて、データポイズニング、モデル盗取、攻撃者攻撃など、AI に固有のリスクに対処します。

AI の迅速な導入によりアタックサーフェスが拡大し、多くの従来型セキュリティドメインに新たなリスクが導入されています。クラウド サイバーエクスポージャー AI-SPM を使用して、これらの領域をそれぞれ保護します。

Tenable はどのような AI リソースとテクノロジーを検出しますか?

クラウド サイバーエクスポージャー は、次の AI 関連のリソースを検出します。

- **AI ワークロード**。従来のクラウドスキャンによって検出されたクラウドネイティブ AI サービスか、管理されていない (シャドウ AI) と見なされる。
- **AI ソフトウェア**。ワークロードスキャンによって検出された、ワークロードにインストールされている AI 関連のライブラリ。たとえば、PyTorch、TensorFlow、LlamaIndex などです。
- **データリポジトリ**。トレーニングデータセット、システムプロンプト、取得で使用されるアップロードされたファイルなどの機密性の高い資産を含むリポジトリ。

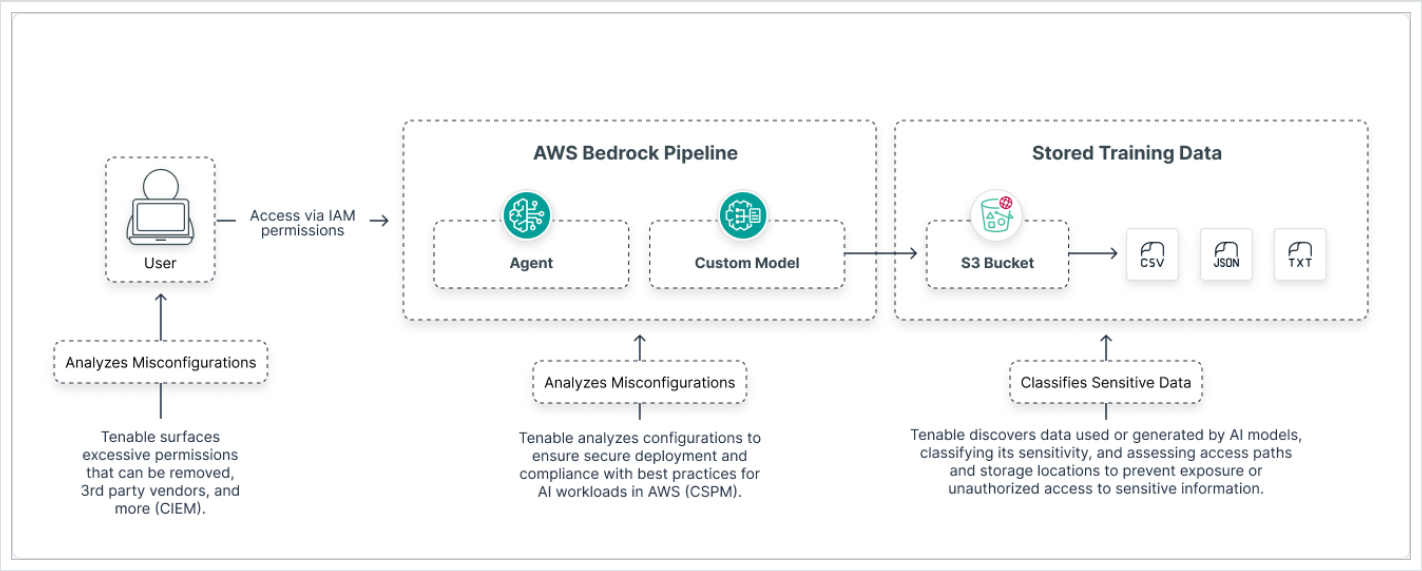
ドメイン別 AI-SPM のユースケース

以下の AI-SPM のユースケースは、AI の実装によって従来のアタックサーフェスがどのように拡大されたかを示しています。

ドメイン	ユースケース (リスク)
データ保護	• 機密データの漏洩 • トレーニング済みデータ • の漏洩 プロンプト インジェクション • モデルの盗用と操作を防止
CSPM	• ネットワーク漏洩 • AI パイプラインと関連するリソースとの相関 • 設定ミス
ワークロード保護	• モデルのトレーニングに使用されるサプライチェーンの脆弱性 • AI ワークロードにデプロイされた脆弱性は何ですか? • Shadow AI の可視性
アイデンティティ	• 権限のないアクセス • 権限を越えるエージェントおよびワークロード

サンプル AI-SPM 攻撃経路フロー

次のサンプルの攻撃経路のフローではクラウドサイバーエクスポージャー、が機密データでトレーニングされた権限のオーバーフローの AWS Bridge パイプラインを検出する方法について説明しています。



1. クラウドサイバーエクスポージャーは、Bedrock パイプラインにアクセスできるユーザーの IAM アクセス許可を分析した後、CIEM 機能を活用して次のことが可能になります。
    - 削除できる過剰なアクセス許可を特定します。
    - サードパーティベンダーなどからのリスクを検出します。
2. ユーザーは、特定された IAM のアクセス許可を介して AWSbedrock パイプライン (エージェントとカスタムモデルで構成される) にアクセスします。
3. Tenable はパイプラインの設定を分析し、CSPM 機能を活用して、AWS の AI ワークロードの安全なデプロイメントとベストプラクティスのコンプライアンスを確保します。
4. カスタムモデルは、S3 バケット (CSV、JSON、TXT などのファイルタイプを含む) からの保存されたトレーニングデータを使用します。
5. Tenable は、AI モデルによって使用または生成されたデータを検出し、その機密性を分類し、アクセス経路と保管場所を評価して、機密情報への漏洩や不正アクセスを回避します。

接続

Alibaba Cloud

Alibaba Cloudの概要

Alibaba Cloud 組織または Tenable One Cloud Exposure の個別のアカウントを接続して、アクセス許可、アカウントの使用状況、セキュリティ設定に関する情報など、すべてのクラウドアイデンティティとリソースに対する完全な可視性とリスク評価を取得します。Tenable は、Alibaba Cloud API からインベントリと設定データを収集します。

- Alibabaクラウド組織の接続
- Alibaba Cloud アカウントの接続

接続が完了すると、クラウドサイバーエクスポージャーに各アカウントのステータスが表示されます。これは Tenable アカウントに接続できるかどうかを示し、潜在的な問題のトラブルシューティングに役立ちます。アカウントのステータス情報とよくある質問については、Alibaba Cloud の FAQ とトラブルシューティング 。

組織と個人のアカウントの接続に関する考慮事項

Alibaba Cloud 組織を接続すると、個別に追加することなく、現在および将来のすべてのメンバーアカウントが自動的にオンボーディングされます。Tenable は、組織全体を接続して、Alibaba Cloud 環境全体を完全かつ継続的に可視化することを推奨しています。

組織ではなく個別のアカウントを接続する場合は、環境の拡大に合わせてアカウントごとに個別に追加し、戻って新しいアカウントを追加する必要があります。

アカウントアーキテクチャ

次に、Alibaba Cloud 環境とクラウドサイバーエクスポージャーの間に確立される信頼関係について説明します。

Tenable アカウントで次の 2 つの RAM リソースを使用します。

- **tenable-user** - Tenable が API 呼び出しの認証に使用するアクセスキーを保持する RAM ユーザー。
- **tenable-role** - クラウドリソースにアクセスするために Tenable が使用するアクセス許可を保持する RAM ロール。ロールの信頼ポリシーにより、tenable-user ロールを引き受けるアクセス許可が付与されます。

クラウド サイバーエクスポージャー は環境にアクセスする際、tenable-user からのアクセスキーを使用して Cloud STS Alibaba呼び出し、tenable-roleを引き受けます。結果として生成される一時的な認証情報の有効範囲は、ロールのポリシーで定義されたアクセス許可に限定されます。認証 (tenable-user) と承認 (tenable-role) の分離は、クラウド セキュリティAlibabaベストプラクティスに従っており、アクセスキーを変更せずにロールのポリシーを更新することでアクセス許可を変更できます。

組織アーキテクチャ

組織接続の場合、tenable-user とtenable-role は管理アカウントでプロビジョニングされます。メンバーアカウントごとに個別の tenable-role が作成され、その信頼ポリシーは管理アカウントの tenable-user ARN を参照します。これにより、1 式の認証情報で Tenable に組織内のすべてのアカウントへのアクセス権を与えることができます。

設定手順については、「 Alibaba Cloud 組織の接続 」を参照してください。

アリユンと国際環境

Alibaba Cloudは、2つの別々の環境を運用しています。組織またはアカウントを接続する場合は、デプロイメントに一致する環境タイプを選択します。

- **Aliyun** – Alibaba Cloud China リージョンのアカウント。
- **国際** – Alibaba Cloud 国際リージョンのアカウント。

同じ統合内で Aliyun と国際アカウントを接続することはできません。組織が両方の環境にまたがっている場合は、別々の統合として接続します。

Alibaba Cloudの必要なアクセス許可

機能	AlibabaのRAM権限	注記
モニタリング(読み取り専用)	カスタムポリシー(以下のアクセス許可を使用) • cr:Get* • cr:List* • cs:Describe* • cs:GetClusters • ecs:Describe* • ims:GenerateCredentialReport • kms:Describe* • kms:List* • oss:GetBucket* • oss:ListBuckets • ram:Get* • ram:List* • resourcecenter:ListResourceTypes • resourcecenter:SearchResources • resourcemanager:Get* • resourcemanager:List* • tag:ListTagResources	常に適用されます。Alibaba Cloud組織を接続する場合、これらの権限は組織レベルで付与する必要があります。正確なポリシーJSONについては、以下のモニタリングポリシーを参照してください。
データリソーススキャン(データ保護)	カスタムポリシー(以下のアクセス許可を使用) • kms:Decrypt • oss:GetObject • oss:ListObjects	詳細についてはデータ保護を参照してください。正確なポリシーJSONについては下記データ保護ポリ

機能	AlibabaのRAM権限	注記
		シーを参照してください。
ワークロード保護	カスタムポリシー(以下のアクセス許可を使用) • ecs:CreateSnapshot • ecs:DeleteSnapshot • resourcesharing:AssociateResourceShare • resourcesharing:CreateResourceShare • resourcesharing:DisassociateResourceShare • resourcesharing:ListResourceShareAssociations • resourcesharing:ListResourceShares	この機能を使用するにはStandardまたはEnterpriseのライセンスが必要です。上記のスナップショットとリソース共有のアクセス許可のいくつかは、Tenableのワークロード分析用にタグ付けされたリソースにのみ適用されます。それらのタグ条件を含め、正確なポリシーJSONについては、以下のワークロード保護ポリシーを参照してください。このポリシーを付与する手順

機能	AlibabaのRAM権限	注記
		については、ワークロードの接続を参照してください。

モニタリングポリシー

JSON

```
{
  "Statement": [
    {
      "Action": [
        "cr:Get*",
        "cr:List*",
        "cs:Describe*",
        "cs:GetClusters",
        "ecs:Describe*",
        "ims:GenerateCredentialReport",
        "kms:Describe*",
        "kms:List*",
        "oss:GetBucket*",
        "oss:ListBuckets",
        "ram:Get*",
        "ram:List*",
        "resourcecenter:ListResourceTypes",
        "resourcecenter:SearchResources",
        "resourcemanager:Get*",
        "resourcemanager:List*",
        "tag:ListTagResources"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    }
  ],
  "Version": "1"
}
```

データ保護ポリシー

JSON

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "kms:Decrypt",
        "oss:GetObject",
        "oss:ListObjects"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    }
  ]
}
```

ワークロード保護ポリシー

JSON

```
{
  "Statement": [
    {
      "Action": [
        "ecs:CreateSnapshot",

      ],
      "Condition": {
        "StringEquals": {
          "acs:RequestTag/TenableContext": [
            "WorkloadAnalysis"
          ]
        }
      },
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    },
```



```
    {
      "Action": [
        "ecs:DeleteSnapshot"
      ],
      "Condition": {
        "StringEquals": {
          "acs:ResourceTag/TenableContext": [
            "WorkloadAnalysis"
          ]
        }
      },
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    },
    {
      "Action": [
        "resourcesharing:CreateResourceShare",
      ],
      "Condition": {
        "StringEquals": {
          "acs:RequestTag/TenableContext": [
            "WorkloadAnalysis"
          ]
        }
      },
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    },
    {
      "Action": [
        "resourcesharing:DeleteResourceShare"
      ],
      "Condition": {
        "StringEquals": {
          "acs:ResourceTag/TenableContext": [
            "WorkloadAnalysis"
          ]
        }
      },
      "Effect": "Allow",
      "Resource": [
        "*"
```

```
      ]
    },
    {
      "Action": [
        "resourcesharing:AssociateResourceShare",
        "resourcesharing:DisassociateResourceShare",
        "resourcesharing:ListResourceShareAssociations",
        "resourcesharing:ListResourceShares"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    }
  ],
  "Version": "1"
}
```

Alibabaクラウド組織の接続

Alibaba Cloud 組織を接続して、現在および将来のすべてのアカウントを個別に追加せずに自動的にオンボーディングします。

前提条件

始める前に

- Alibaba Cloud アカウントに十分な権限を付与し、Resource Manager ディレクトリをクエリし、ROS スタックとスタックグループを作成し、RAM ロール、ユーザー、ポリシー、ポリシー添付ファイルを作成し、メンバーアカウント全体で RAM アクセスキーを生成します。
- ROS 展開スクリプトを実行する前に、有効な認証情報を使って Aliyun CLI をインストールし、設定してください。
- Terraform 固有
  - Terraform CLI v0.13 以上をインストールしていることを確認します。
  - `terraform init`が既存の設定と競合することなく、クラウドプロバイダー v1.252+ Alibabaダウンロードしてインストールできるようにします。

- アクセスキーファイルが安全に処理できる場所で Terraform が実行されていることを確認します。

Alibabaクラウド組織の接続

Alibaba Cloud 組織を接続するには:

1. Tenable One Cloud Exposure コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Alibaba Cloud Organization]** をクリックします。[Alibaba Cloud Organization] ウィザードが開きます。
3. **設定**ステップ (ステップ 1/2) で、次の操作を実行します。
    1. 統合の名前を入力します。
    2. 組織に一致する Alibaba Cloud 環境タイプを選択します。
        - **Aliyun**: Alibaba Cloud China リージョンのアカウント。
        - **国際**: Alibaba Cloud 国際リージョンのアカウント。
    3. **[機能]** で、有効にする機能を選択します。この選択により、必要なアクセス許可が決定され、デプロイメントスクリプトが動的に更新されます。詳細については、「Alibaba Cloudの必要なアクセス許可を参照してください。

        > **注意:** Tenable では、最も包括的なセキュリティカバレッジを提供するために、利用可能なすべての機能 (近日公開予定と表示されている機能を含む) を有効にすることを推奨しています。これらを有効にすると、デプロイメントスクリプトが最初から必要なアクセス許可を付与するようになりました。後でこれらを有効にする場合は、スクリプトを再デプロイして、Tenableに付与されているアクセス許可を更新する必要があります。

        - **モニタリング (読み取り専用)**: デフォルトで選択されています。すべてのクラウド資産について完全な可視性を確保します。これにはアクセス許可、コンパートメント使用状況、データとセキュリティの設定に関する情報が含まれます。
        - **データリソーススキャン (データ保護):** クラウドリソースをスキャンして分類します。
        - **ワークロード保護**: 仮想マシンインスタンスとコンテナイメージレジストリをスキャンして、脆弱性と設定ミスがないか確認します。*(近日公開)*

4. **[デプロイメント]** で、次のいずれかのデプロイオプションを選択します。
    - **ROS。** スクリプトベースのデプロイ。Aliyun CLI を使用して、Alibaba Cloud 環境のウィザードに表示されているスクリプトを実行します。詳細を見る
    - **Terraform** - モジュールベースのデプロイメント。デプロイする前に、Terraform 固有の前提条件 を参照してください。
        1. クラウドサイバーエクスポージャー ウィザードに表示される最初の呼び出しをコピーし、Terraform 設定に追加して、`terraform apply` を実行します。モジュールにより、RAM ユーザーとアクセスキーが作成されます。
        2. Terraform の出力からユーザー ARN を取得し、**[User ARN] (ユーザー ARN)** フィールドに入力します。
        3. クラウドサイバーエクスポージャー ウィザードに表示される 2 つ目の呼び出しをコピーし、Terraform メンバーアカウント設定に追加して、`terraform apply`を実行します。このモジュールは RAM ロールを作成し、環境に接続してスキャンするアクセス許可を Tenable に付与します。
    - **手動** - 手動で、Alibaba Cloud RAMコンソールから。ステップバイステップの手順については、「 Alibaba Cloud 組織を手動でデプロイする を参照してください。

> **警告:** 手動のデプロイメントが完了したら、ウィザードに戻り、「ポスト・デプロイメント」と「ステップ 2: スコープ」を完了します。

5. **[デプロイメント後]** に、次の値を入力します。
    - **値を取得する方法**
        - ROS: スタック作成の完了後にスクリプト出力の値をコピーします。
        - Terraform: Terraform 出力から値を取得します。
        - 手動: これらの値を取得する方法については、Alibaba Cloud 組織を手動でデプロイする を参照してください。
    - **共通の統合値**
        - これらの値は、組織およびそのすべてのメンバーアカウントで同一である必要があります。

- 組織が接続されている場合、これらのフィールドは組織レベルでのみ更新できます。変更はすべてのメンバーアカウントに自動的に反映されます。
- **メインアカウントロール ARN**: 管理アカウントで作成された RAM ロールの ARN。
- **アクセスキー ID**: Tenable RAM ユーザー用に作成されたアクセスキーの ID。Terraform の場合は、Terraform によって保存されたアクセスキーファイルから ID を取得します。
- **Access Key Secret**: Tenable RAM ユーザー用に作成されたアクセスキーのシークレット。Terraform の場合は、Terraform によって保存されたアクセスキーファイルからシークレットを取得します。

6. 完了したら、**[次へ]** をクリックします。

4. **範囲** ステップ (ステップ 2/2) で、次の操作を実行します。
   1. (オプション) [コンパートメント構造を自動的に更新] を選択して、コンパートメントの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます。詳細については、アカウント階層とフォルダーを参照してください。
   2. **[範囲]** で、オンボーディングするコンパートメントを選択します。
      - **現在および将来のすべてのアカウントを同期する (推奨)**
      - **特定のフォルダーとアカウントを含める**
      - **特定のフォルダーとアカウントを除外する**

      > **注意:**
      > - フォルダー全体を含めたり除外したりすると、そのフォルダー内の現在および将来のアカウントすべてが含まれるか、または除外されます。
      > - フォルダーで特定のアカウントを含めたり除外したりすると、選択したアカウントのみが含まれるか、または除外されます。

5. **[終了]** をクリックします。

> **注意:** ROS スタックの作成後、アクセス許可の変更が Alibaba Cloud 組織全体に反映されるまでに数分かかる場合があります。**[完了]** をクリックしたときにエラーが表示された場合は、数分待ってからもう一度お試しください。

次のステップ

組織が正常に接続されたら次の操作を実行します。

- 組織は、**[Settings > 統合]** で確認できます。
- 組織に属するアカウントは、**Settings > [組織] > [アカウント] > Alibaba クラウド** で確認できます。ここから、アカウントしたり、アカウントの詳細を表示したりして、どの機能が有効になっているか、必要なアクセス許可が付与されているか、などを確認できます。

アカウントリソースに関するデータがクラウドサイバーエクスポージャーに表示されるようになります。すべてのデータが表示されるまでにかかる時間は、クラウド環境の規模によって異なります。

Alibaba Cloud 組織を手動でデプロイする

> **注意:** 手動のデプロイメントが完了したら、ウィザードに戻り、「**ポスト・デプロイメント**」と「**ステップ 2: スコープ**」を完了します。

ROS スクリプトの代わりに、Alibaba Cloud RAM コンソールを使用して Alibaba Cloud 組織を手動でデプロイできます。これらの手順は、Alibaba Cloud組織の接続時にデプロイメントタイプとして「**手動**」を選択した場合に適用されます。

1. RAM ユーザーとアクセスキーを作成する
2. Tenable の RAM ロールを作成する
3. カスタムポリシーの作成
4. ポリシーの割り当て
5. メンバーアカウントでロールを設定する

RAM ユーザーとアクセスキーを作成する

専用 RAM ユーザーを作成し、Tenable が認証に使用するアクセスキーを生成します。最初にこのステップを完了してください。RAM ロールを作成するときに、ユーザー ARN が必要になります。

1. RAM コンソールで、**[アイデンティティ] > [ユーザー]** に移動します。
2. **[ユーザーの作成]** をクリックします。
3. **[ユーザーログイン名]** に `tenable-user` と入力します。
4. **[アクセス設定]** セクションで、**[永続的なアクセスキー]** を選択します。
5. AccessKey を作成する必要があることを確認します。

6. **[OK]** をクリックします。
7. 確認ページに表示されている **AccessKey ID** と **AccessKey Secret** をコピーして保存します。シークレットは後で取得できません。Tenable ウィザードの [Post **Deployment]** セクションに両方の値を入力します。
8. **[ユーザー]** ページで、[`tenable-user`] をクリックして詳細を開きます。
9. **[アクセス許可]** タブを選択し、**[アクセス許可の付与]** をクリックします。
10. **[リソース範囲]** で、**[アカウント]** を選択します。
11. **AliyunSTSAssumeRoleAccess** ポリシーを選択し、**[OK]** をクリックします。

Tenable の RAM ロールを作成する

Tenable が組織へのアクセスと監視に使用する専用の RAM ロールを作成します。ロールの信頼ポリシーにより、`tenable-user` ロールを引き受けるアクセス許可が付与されます。

1. RAM コンソールで、**[アイデンティティ]** > **[ロール]** に移動します。
2. **[ロールの作成]** をクリックします。
3. **[プリンシパルタイプ]** で、**[クラウドアカウント]** を選択します。
4. **[ポリシーエディターに切り替える]** をクリックします。
5. **[クラウドアカウント]** で、**[編集]** をクリックします。
6. **[アイデンティティタイプ]** で、[RAM ユーザー] を選択します。
7. **[ユーザー名]** に `tenable-user` と入力します。
8. **[OK]** をクリックします。
9. **[アクション]** で、**sts:AssumeRole** を選択します。
10. **[OK]** をクリックします。
11. **[ロール名]** に「 `tenable-role` 」と入力して **[OK]** をクリックします。
12. **[ロール]** ページで、[`tenable-role`] をクリックして詳細を開きます。
13. **ARN** をコピーして保存します。この値は、Tenable ウィザードの [デプロイ**メント後]** セクションにメイン **アカウントロール ARN** として入力します。

カスタムポリシーの作成

ウィザードで選択した各機能のカスタムRAMポリシーを作成します。機能ごとの必要なアクセス許可の完全なリストについては、「Alibabaの必要なアクセス許可」を参照してください。

1. RAMコンソールで、**[アクセス許可]** > **[ポリシー]** に移動します。
2. 「**ポリシーの作成**」をクリックし、「**JSONエディター**」を選択します。
3. JSONエディターにAlibaba Cloudの必要なアクセス許可のポリシーを貼り付けて、**モニタリング(読み取り専用)** ポリシーを作成します。
4. **[OK]** をクリックします。
5. **[ポリシー名]** に`tenable-monitoring-policy`と入力し、**[OK]** をクリックします。
6. (オプション)**[Policies]** (**ポリシー**) ページに戻り、**ワークロード保護** ポリシーを作成します。
    1. JSONエディターにAlibaba Cloudの必要なアクセス許可のポリシーを貼り付けます。
    2. **[OK]** をクリックします。
    3. **[ポリシー名]** に`tenable-workload-policy`と入力し、**[OK]** をクリックします。
7. (オプション)**[ポリシー]** ページに戻り、**データリソーススキャン(データ保護)** ポリシーを作成します。
    1. JSONエディターにAlibaba Cloudの必要なアクセス許可のポリシーを貼り付けます。
    2. **[OK]** をクリックします。
    3. **[ポリシー名]** に`tenable-data-scanning-policy`と入力し、**[OK]** をクリックします。

ポリシーの割り当て

作成したポリシーを`tenable-role`に割り当てます。

1. RAMコンソールで、**[アイデンティティ]** > **[ロール]** に移動します。
2. `tenable-role`を開き、**[アクセス許可の付与]** をクリックします。
3. [Policy] (**ポリシー**) セクションで、カスタムポリシーの作成作成したポリシーを選択します。
4. **[OK]**、**[閉じる]** の順にクリックします。

メンバーアカウントでロールを設定する

上記の手順は、管理アカウントでのみ tenable-role とtenable-user をプロビジョニングします。メンバーアカウントを クラウド サイバーエクスポージャー 可視化するには、各メンバーアカウントに tenable-role を複製し、同じポリシーを付与する必要があります。

各メンバーアカウントについて:

1. RAM コンソールを開き、メンバーアカウントにログインします。
2. カスタム カスタムポリシーの作成 の手順を繰り返して、そのアカウントに同じポリシーを作成します。
3. 「Create a RAM Role for Tenable 」の手順を繰り返して、Tenable ロールを作成します。**クラウドアカウントを**編集する場合は、**その他のアカウント**を選択し、管理アカウントのアカウント ID を入力します。**[ユーザー名]** に tenable-user を入力します。
4. ポリシーの ポリシーの割り当て の手順を繰り返して、同じポリシーをメンバーアカウントの tenable-roleに割り当てます。

Alibaba Cloud アカウントの接続

個々の Alibaba Cloud アカウントを接続して、そのリソース、構成、セキュリティ体制を可視化します。

> **注意:** 複数のアカウントを個別に追加せずに接続するには、「 Alibaba Cloud 組織の接続 」を参照してください。

前提条件

始める前に

- ロール、ユーザー、アクセスキー、ROSスタックを作成するAlibaba Cloudアカウントに十分な権限を付与します。
- ROS 展開スクリプトを実行する前に、有効な認証情報を使って Aliyun CLI をインストールし、設定してください。

- Terraform 固有
  - Terraform CLI v0.13 以上をインストールしていることを確認します。
  - `terraform init`が既存の設定と競合することなく、クラウドプロバイダー v1.252+ Alibabaダウンロードしてインストールできるようにします。
  - アクセスキーファイルが安全に処理できる場所で Terraform が実行されていることを確認します。

Alibaba Cloud アカウントの接続

Alibaba Cloud アカウントを接続するには:

1. Tenable One Cloud Exposure コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Alibaba Cloud Account]** をクリックします。Alibaba Cloud アカウントウィザードが開きます。
3. ウィザードで次の操作を実行します。
   1. 統合の名前を入力します。
   2. 組織に一致する Alibaba Cloud 環境タイプを選択します。
      - **Aliyun**: Alibaba Cloud China リージョンのアカウント。
      - **国際**: Alibaba Cloud 国際リージョンのアカウント。
   3. **[機能]** で、有効にする機能を選択します。この選択により、必要なアクセス許可が決定され、デプロイメントスクリプトが動的に更新されます。詳細については、「Alibaba Cloudの必要なアクセス許可を参照してください。

      > **注意:** Tenable では、最も包括的なセキュリティカバレッジを提供するために、利用可能なすべての機能 (近日公開予定と表示されている機能を含む) を有効にすることを推奨しています。これらを有効にすると、デプロイメントスクリプトが最初から必要なアクセス許可を付与するようになりました。後でこれらを有効にする場合は、スクリプトを再デプロイして、Tenableに付与されているアクセス許可を更新する必要があります。

      - **モニタリング (読み取り専用)**: デフォルトで選択されています。すべてのクラウド資産について完全な可視性を確保します。これにはアクセス許可、コンパートメント使用状況、

データとセキュリティの設定に関する情報が含まれます。

- **データリソーススキャン (データ保護):** クラウドリソースをスキャンして分類します。
- **ワークロード保護**: 仮想マシンインスタンスとコンテナイメージレジストリをスキャンして、脆弱性と設定ミスがないか確認します。*(近日公開)*

4. **[デプロイメント]** で、次のいずれかのデプロイオプションを選択します。
    - **ROS。** スクリプトベースのデプロイ。Aliyun CLI を使用して、Alibaba Cloud 環境のウィザードに表示されているスクリプトを実行します。詳細を見る
    - **Terraform** - モジュールベースのデプロイメント。デプロイする前に、Terraform 固有の前提条件 を参照してください。
        1. クラウドサイバーエクスポージャー ウィザードに表示される最初の呼び出しをコピーし、Terraform 設定に追加して、`terraform apply` を実行します。モジュールにより、RAM ユーザーとアクセスキーが作成されます。
        2. Terraform の出力からユーザー ARN を取得し、**[User ARN] (ユーザー ARN)** フィールドに入力します。
        3. クラウドサイバーエクスポージャー ウィザードに表示される 2 つ目の呼び出しをコピーし、Terraform メンバーアカウント設定に追加して、`terraform apply`を実行します。このモジュールは RAM ロールを作成し、環境に接続してスキャンするアクセス許可を Tenable に付与します。
    - **手動** - 手動で、Alibaba Cloud RAMコンソールから。ステップバイステップの手順については、「 Alibaba Cloud アカウントを手動でデプロイする を参照してください。

> **警告:** 手動のデプロイメントが終了したら、ウィザードに戻ってポスト・デプロイメントを完了し、**「完了」**をクリックします。

5. **[デプロイメント後]** に、次の値を入力します。

> **注意:**
> - ROS: スタック作成の完了後にスクリプト出力の値をコピーします。
> - Terraform: Terraform 出力から値を取得します。

> - 手動: これらの値を取得する方法については、Alibaba Cloud アカウントを手動でデプロイする を参照してください。

- **ロール ARN**: アカウントで作成された RAM ロールの ARN。
- **アクセスキー ID**: Tenable RAM ユーザー用に作成されたアクセスキーの ID。Terraform の場合は、Terraform によって保存されたアクセスキーファイルから ID を取得します。
- **Access Key Secret**: Tenable RAM ユーザー用に作成されたアクセスキーのシークレット。Terraform の場合は、Terraform によって保存されたアクセスキーファイルから ID を取得します。

4. **[終了]** をクリックします。

> **注意:** アクセス許可の変更が Alibaba Cloud アカウントに反映されるまで、数分かかる場合があります。**[完了]** をクリックしたときにエラーが表示された場合は、数分待ってからもう一度お試しください。

次のステップ

アカウントが正常に接続されると、そのアカウントは **Alibaba Cloud Settings>** > **[組織]** > **[アカウント]** に表示されます。ここから、アカウント したり、アカウントの詳細を表示したりして、どの機能が有効になっているか、必要なアクセス許可が付与されているかなどを確認できます。

アカウントリソースに関するデータがクラウドサイバーエクスポージャーに表示されるようになります。すべてのデータが表示されるまでにかかる時間は、クラウド環境の規模によって異なります。

Alibaba Cloud アカウントを手動でデプロイする

> **注意:** 手動のデプロイメントが終了したら、ウィザードに戻り、「デプロイメント後のデプロイメント」セクションを完了します。

ROS スクリプトの代わりに、Alibaba Cloud RAM コンソールから Alibaba Cloud アカウントを手動でデプロイできます。これらの手順は、Alibaba Cloud アカウントの接続時にデプロイメントタイプとして **[手動]** を選択した場合に適用されます。

1. RAM ユーザーとアクセスキーを作成する
2. Tenable の RAM ロールを作成する

3. カスタムポリシーの作成
4. ポリシーの割り当て

RAM ユーザーとアクセスキーを作成する

専用 RAM ユーザーを作成し、Tenable が認証に使用するアクセスキーを生成します。最初にこのステップを完了してください。RAM ロールを作成するときに、ユーザー ARN が必要になります。

1. RAM コンソールで、**[アイデンティティ]** > **[ユーザー]** に移動します。
2. **[ユーザーの作成]** をクリックします。
3. **[ユーザーログイン名]** に `tenable-user` と入力します。
4. **[アクセス設定]** セクションで、**[永続的なアクセスキー]** を選択します。
5. AccessKey を作成する必要があることを確認します。
6. **[OK]** をクリックします。
7. 確認ページに表示されている **AccessKey ID** と **AccessKey Secret** をコピーして保存します。シークレットは後で取得できません。Tenable ウィザードの [Post **Deployment]** セクションに両方の値を入力します。
8. **[ユーザー]** ページで、[`tenable-user`] をクリックして詳細を開きます。
9. **[アクセス許可]** タブを選択し、**[アクセス許可の付与]** をクリックします。
10. **[リソース範囲]** で、**[アカウント]** を選択します。
11. **AliyunSTSAssumeRoleAccess** ポリシーを選択し、**[OK]** をクリックします。

Tenable の RAM ロールを作成する

アカウントへのアクセスと監視のために Tenable が使用する専用の RAM ロールを作成します。ロールの信頼ポリシーにより、`tenable-user` ロールを引き受けるアクセス許可が付与されます。

始める前に、Alibaba Cloud アカウント ID を見つけます。Alibaba Cloud コンソールの右上隅にあります。

1. RAM コンソールで、**[アイデンティティ]** > **[ロール]** に移動します。
2. **[ロールの作成]** をクリックします。
3. **[プリンシパルタイプ]** で、**[クラウドアカウント]** を選択します。

4. **[ポリシーエディターに切り替える]** をクリックします。
5. **[クラウドアカウント]** で、**[編集]** をクリックします。
6. **[アイデンティティタイプ]** で、[RAM ユーザー] を選択します。
7. **[ユーザー名]** に `tenable-user` と入力します。
8. **[OK]** をクリックします。
9. **[アクション]** で、**sts:AssumeRole** を選択します。
10. **[OK]** をクリックします。
11. **[ロール名]** に「`tenable-role`」と入力して **[OK]** をクリックします。
12. **[ロール]** ページで、[`tenable-role`] をクリックして詳細を開きます。
13. **ARN** をコピーして保存します。この値は、Tenable ウィザードの [デプロイメント後] セクションにメイン **アカウントロール ARN** として入力します。

カスタムポリシーの作成

ウィザードで選択した各機能のカスタム RAM ポリシーを作成します。機能ごとの必要なアクセス許可の完全なリストについては、「Alibaba Cloudの必要なアクセス許可を参照してください。

1. RAM コンソールで、**[アクセス許可]** > **[ポリシー]** に移動します。
2. 「**ポリシーの作成**」をクリックし、「**JSON エディター**」を選択します。
3. JSON エディターに Alibaba Cloud の必要なアクセス許可 のポリシーを貼り付けて、**モニタリング (読み取り専用)** ポリシーを作成します。
4. **[OK]** をクリックします。
5. **[ポリシー名]** に `tenable-monitoring-policy` と入力し、**[OK]** をクリックします。
6. (オプション)**[Policies] (ポリシー)** ページに戻り、**ワークロード保護** ポリシーを作成します。
    1. JSON エディターに Alibaba Cloud の必要なアクセス許可 のポリシーを貼り付けます。
    2. **[OK]** をクリックします。
    3. **[ポリシー名]** に `tenable-workload-policy` と入力し、**[OK]** をクリックします。

7. (オプション)**[ポリシー]** ページに戻り、**データリソーススキャン (データ保護)** ポリシーを作成します。
    1. JSON エディターに Alibaba Cloud の必要なアクセス許可 のポリシーを貼り付けます。
    2. **[OK]** をクリックします。
    3. **[ポリシー名]** に `tenable-data-scanning-policy` と入力し、**[OK]** をクリックします。

ポリシーの割り当て

作成したポリシーを `tenable-role` にアタッチします。

ポリシーの割り当て

作成したポリシーを `tenable-role` に割り当てます。

1. RAM コンソールで、**[アイデンティティ]** > **[ロール]** に移動します。
2. `tenable-role`を開き、**[アクセス許可の付与]** をクリックします。
3. [Policy] (**ポリシー**) セクションで、カスタムポリシーの作成 作成したポリシーを選択します。
4. **[OK]**、**[閉じる]** の順にクリックします。

Alibaba Cloud の FAQ とトラブルシューティング

この記事の内容

- Alibaba Cloud の Tenable One Cloud Exposure への接続に関連する、よくある質問のリスト
- アカウントステータスとトラブルシューティング

フォルダーまたはアカウントを組織から除外する

> すでに接続した企業から、特定のフォルダーまたはアカウントを除外するにはどうすればよいですか?

企業の範囲を変更して特定のエンティティを削除する方法

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[統合]** に移動します。
2. 組織の横にある三点リーダーをクリックし、**[編集]** をクリックします。
3. **[次へ]** をクリックしてウィザード (スコープ) の最後のステップに移動します。

4. **[特定のフォルダーとアカウントを除外する]** を選択し、関連するフォルダーまたはアカウントを選択します。
5. **[終了]** をクリックします。除外されたエンティティは、次回のデータ同期後にコンソールから削除されます。

近日公開機能を有効にする

> データリソーススキャンとワークロード保護がまだ利用できないのに、初期セットアップ時にTenableで有効にすることを推奨しているのはなぜですか?

ROS デプロイメントスクリプトは、デプロイ時に選択したすべての機能に対するアクセス許可を付与します。最初のデプロイ後にデータリソーススキャン (データ保護) またはワークロード保護を有効にした場合は、スクリプトを再デプロイして、Tenableに付与されたアクセス許可を更新する必要があります。初期セットアップ時にこれらの機能を有効にすると、機能が利用可能になったときに余分な手順を踏む必要がなくなります。

デプロイメント環境

> `www.alibabacloud.com` 経由で作成した国際アカウントがあり、そのアカウントは国際リージョンとアリユンリージョンの両方を使用しています。オンボーディング時にウィザードでどの環境を選択する必要がありますか?

国際ウェブサイト経由で作成されたアカウントの場合は、環境として **[国際]** を選択する必要があります。これにより、アリユンを含むすべての地域がカバーされます。

RAM ユーザーと RAM ロールのアーキテクチャ

> RAM ユーザー (`tenable-user`) と RAM ロール (`tenable-role`) の両方が必要なのはなぜTenableですか? アクセスキーをリソースへのアクセスに直接使用できますか?

RAM ユーザーと RAM ロールは異なる目的を果たします。`tenable-user` は、Tenable が認証に使用するアクセスキーを保持します。`tenable-role` は、Tenable がアクセスできるものを定義するアクセス許可を保持します。クラウドサイバーエクスポージャー環境にアクセスする必要がある場合、アクセスキー

を使用して Alibaba Cloud STS を呼び出し、`tenable-role`を引き受けます。こうすることで、ロールのポリシーの範囲が指定された一時的な認証情報が発行されます。

この分離により、2 つのメリットがあります。1 つ目は、アクセスキーを変更せずにロールのポリシーを変更することで、アクセス許可を更新できます。2 つ目のメリットとして、組織接続の場合、管理アカウントの 1 セットの認証情報ですべてのメンバーアカウントにわたるロールを引き継ぐことができるため、アカウントごとに個別の認証情報をプロビジョニングする必要はありません。

> 組織をオンボーディングするときに、すべてのメンバーアカウントで RAM ロールを作成する必要がありますか?

ROS スクリプトを使用して組織レベルで統合すると、スクリプトによってすべてのアカウントにロールが自動的に作成されます。ただし、手動デプロイメントを選択した場合は、アカウントごとにロールを作成する必要があります。

アカウントステータスとトラブルシューティング

クラウドサイバーエクスポージャーは、**[アカウント > Alibaba]** ページに各アカウントの**ステータス**を表示します。これはTenableアカウントに接続できるかどうかを示し、潜在的な問題のトラブルシューティングに役立ちます。

ステータス	問題	Description (説明)
接続済み	該当なし	クラウドサイバーエクスポージャーはアカウントに正常に接続され、アカウントは実行されています。
問題との関連		アカウントは接続されていますが、対処する必要がある特定の問題があります。
失敗	アクセスが拒否されました	クラウドサイバーエクスポージャーは 1 つ以上のリソースタイプを同期できませんでした。これは、RAM ロールに必要な読み取りアクセス許可がないことが原因である可能性があります。

ステータス	問題	Description (説明)
		アカウントのオンボーディング中に作成されたRAMロールにアタッチされているポリシーを確認し、必要なすべてのアクセス許可が含まれていることを確認します。Alibaba Cloudの必要なアクセス許可を参照してください。
失敗	アクセス許可なし	アカウントのオンボーディング中に作成されたRAMロールに問題があります。ロールが必要なオペレーションを実行できないロールが存在すること、信頼ポリシーが正しく設定されていること、および必要なポリシーがアタッチされていることを確認してください。Alibaba Cloudの必要なアクセス許可を参照してください。
失敗	見つかりません。削除保留中です	Alibaba Cloudアカウントはリソースディレクトリに存在しなくなりました。削除または閉鎖されている可能性があります。アカウントがクラウドサイバーエクスポージャーから削除されます。
失敗	組織が接続されていません	リソースディレクトリ組織には接続の問題があり、クラウドサイバーエクスポージャー がメンバーアカウントに接続できません。最初に組織レベルで問題を解決する – 管理アカウントのRAMユーザー認証情報とロール設定を検証します。
失敗	ロールAssumeRolePolicyにユーザーアクセス許可がありません	RAMロールの信頼ポリシーにより、設定済みのRAMユーザーが引き受けることはできません。Alibaba Cloud RAMコンソールでロールの信頼ポリシーを更新して、RAMユーザーにロールを引き受けるアクセス許可を付与します。
失敗	ロールが見つかりません	アカウントのオンボーディング中に作成されたRAMロールが存在しません。削除された可能性があります。ロールを再作成するか、クラウドサイバーエクスポージャーで設定されているロールARNを確認します。

ステータス	問題	Description (説明)
失敗	ユーザーアクセスキーが見つかりません	オンボーディング時に設定されたRAMユーザーアクセスキーIDが存在しません。削除またはローテーションされた可能性があります。Alibaba Cloud RAMコンソールでAccessKey IDを確認し、クラウドサイバーエクスポージャーで更新します。
失敗	ユーザー認証情報が無効です	オンボーディング中に設定されたRAMユーザーアクセスキーシークレットが正しくないか、ローテーションされています。クラウドサイバーエクスポージャーに正しいアクセスキーシークレットを再入力してください。
失敗	ユーザーに引き受けるロールのアクセス許可がありません	RAMユーザーには、設定されたRAMロールを引き受ける権限がありません。Alibaba Cloud RAMコンソールで、`AliyunSTSAssumeRoleAccess`ポリシーをRAMユーザーにアタッチします。
除外	該当なし	企業の範囲設定に基づいて、アカウントが同期から除外されました。スコープ設定を変更するには、「Alibaba Cloud組織の接続」を参照してください。
削除済み	該当なし	このアカウントは、リソースディレクトリ組織のメンバーではなくなりました。削除または転送された可能性があります。削除されたアカウントに関連付けられているリソースと検出結果は、クラウドサイバーエクスポージャーでは非表示になります。

組織のステータスとトラブルシューティング

クラウドサイバーエクスポージャーは、**Settings** > **統合**で各組織の**ステータス**を表示します。これは、管理アカウントに接続できるかどうかを示すTenable、潜在的な問題のトラブルシューティングに役立ちます。

ステータス	問題	Description (説明)
接続済み	該当なし	クラウドサイバーエクスポージャーは組織に正常に接続され、組織は稼働しています。
問題との関連	該当なし	組織はつながっていますが、対処する必要のある特定の問題があります。
失敗	アクセス許可なし	管理アカウントに設定されたRAMロールに問題があります。ロールが必要なオペレーションを実行できない信頼ポリシーが正しく設定され、必要なポリシーが添付されていることを確認してください。Alibaba Cloudの必要なアクセス許可を参照してください。
失敗	ロールAssumeRolePolicyにユーザーアクセス許可がありません	RAMロールの信頼ポリシーにより、設定済みのRAMユーザーが引き受けることはできません。Alibaba Cloud RAMコンソールでロールの信頼ポリシーを更新して、RAMユーザーにロールを引き受けるアクセス許可を付与します。
失敗	ロールが見つかりません	管理アカウントに設定されているRAMロールが存在しません。削除された可能性があります。ロールを再作成するか、クラウドサイバーエクスポージャーで設定されているロールARNを確認します。
失敗	ユーザーアクセスキーが見つかりません	オンボーディング時に設定されたRAMユーザーアクセスキーIDが存在しません。削除またはローテーションされた可能性があります。Alibaba Cloud RAMコンソールでAccessKey IDを確認し、クラウドサイバーエクスポージャーで更新します。
失敗	ユーザー認証情報が無効です	オンボーディング中に設定されたRAMユーザーアクセスキーシークレットが正しくないか、ローテーションされています。クラウドサイバーエクスポージャーに正しいアクセスキーシークレットを

ステータス	問題	Description (説明)
		再入力してください。
失敗	ユーザーに引き受けるロールのアクセス許可がありません	RAM ユーザーには、設定された RAM ロールを引き受ける権限がありません。Alibaba Cloud RAM コンソールで、`AliyunSTSAssumeRoleAccess` ポリシーを RAM ユーザーにアタッチします。

AWS

AWS の概要

Tenable One Cloud Exposure の AWS 組織全体や個別のアカウントを接続して、組織やアカウントに関連付けられているすべてのクラウドアイデンティティとリソース (アクセス許可、アカウントの使用状況、セキュリティ設定に関する情報を含む) の完全な可視性とリスク評価を取得します。Tenable は、AWS API からインベントリと設定データ、AWS CloudTrail ログからアクティビティデータを収集します。

- AWS アカウントの接続
- AWS 組織の接続

接続が完了すると、クラウドサイバーエクスポージャーにアカウントステータスとトラブルシューティングが表示されます。これはたとえば、Tenable がアカウントに接続できるかどうかを示すもので、接続に関する潜在的な問題のトラブルシューティングに役立ちます。

確立される IAM の信頼関係の視覚的な概要 (必要なアクセス許可を含む) については、アカウントアーキテクチャを参照してください。AWS の接続に関連するよくある質問のリストについては、AWS の FAQ (よくある質問) とトラブルシューティング を参照してください。

組織と個人のアカウントの接続に関する考慮事項

個別のアカウントではなくAWS 組織全体を接続するかどうかを決定する場合、この決定がクラウドサイバーエクスポージャーの機能にどのように影響するかを考慮することが重要です。Tenable では、管理アカウントが確実にTenable に接続され、以下の機能に関連する可視性が失われないように、組織全体を接続することを推奨しています。

- **AWS Identity Center (旧 AWS SSO)** - ユーザー、グループ、アクセス許可のセット、およびこれらの効果的な使用、さらには最小権限の推奨事項の可視性に影響が及びます。
- **サービスコントロールポリシー (SCP) とリソースコントロールポリシー (RCP)** - 制限された権限の表示。
- **クロスアカウントの可視性** - *Tenable は、組織の一部であるアカウント (ただし接続されていない) と、そうでないアカウントを区別できなくなります。*
- **最小限の権限** - *Tenable は、最も正確な推奨事項を提供できなくなります。*

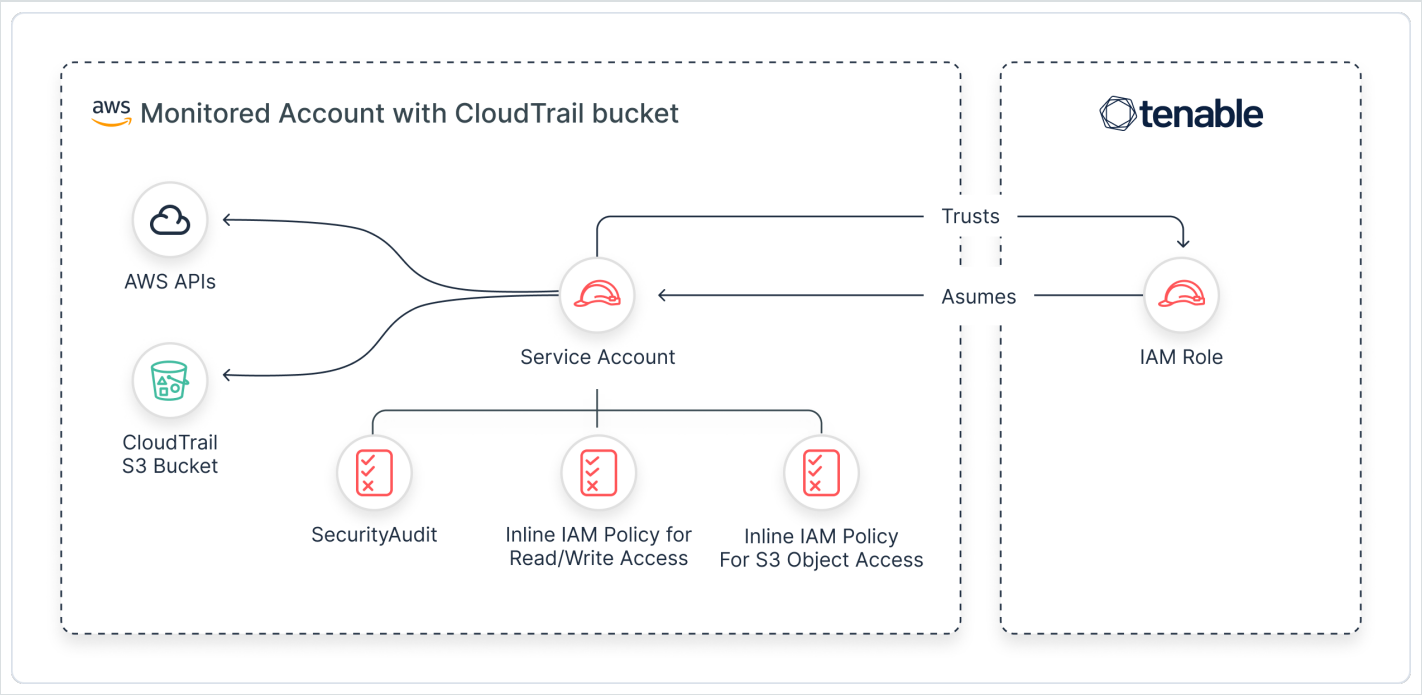
アカウントアーキテクチャ

モニタリングや修正のアクセス許可を持つアカウント

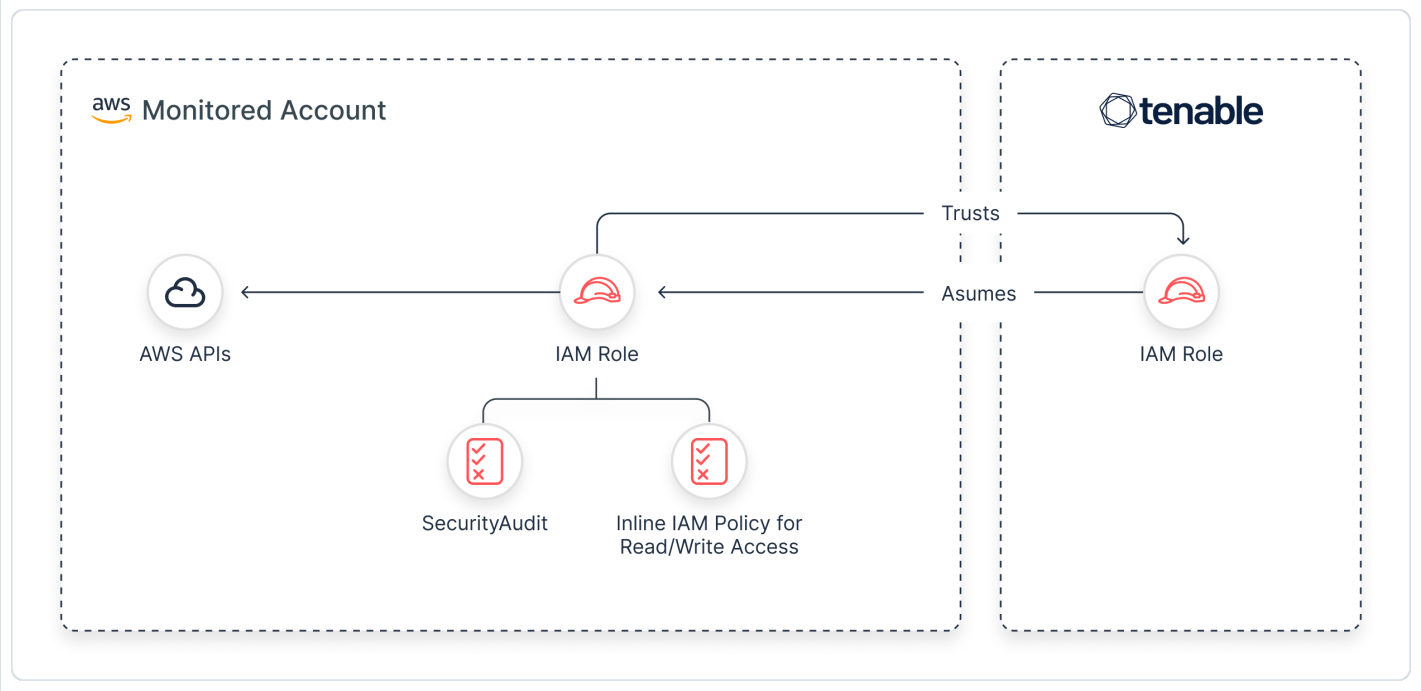
以下の図は、モニタリングや修正のアクセス許可を持つアカウントアーキテクチャの概要です。これらの図は、CloudTrail に接続されているアカウントと、接続されていないアカウントとの違いを示しています。詳細については、AWS CloudTrail を参照してください。

これらの図は、接続するアカウントに関連付けられたIAM ロールとクラウドサイバーエクスポージャーの間に確立された信頼関係を示しています。クラウドサイバーエクスポージャーは、独自のIAM ロールを使用して付与されたアクセス許可経由で環境とやり取りし、データを収集します。

CloudTrail が接続されている図



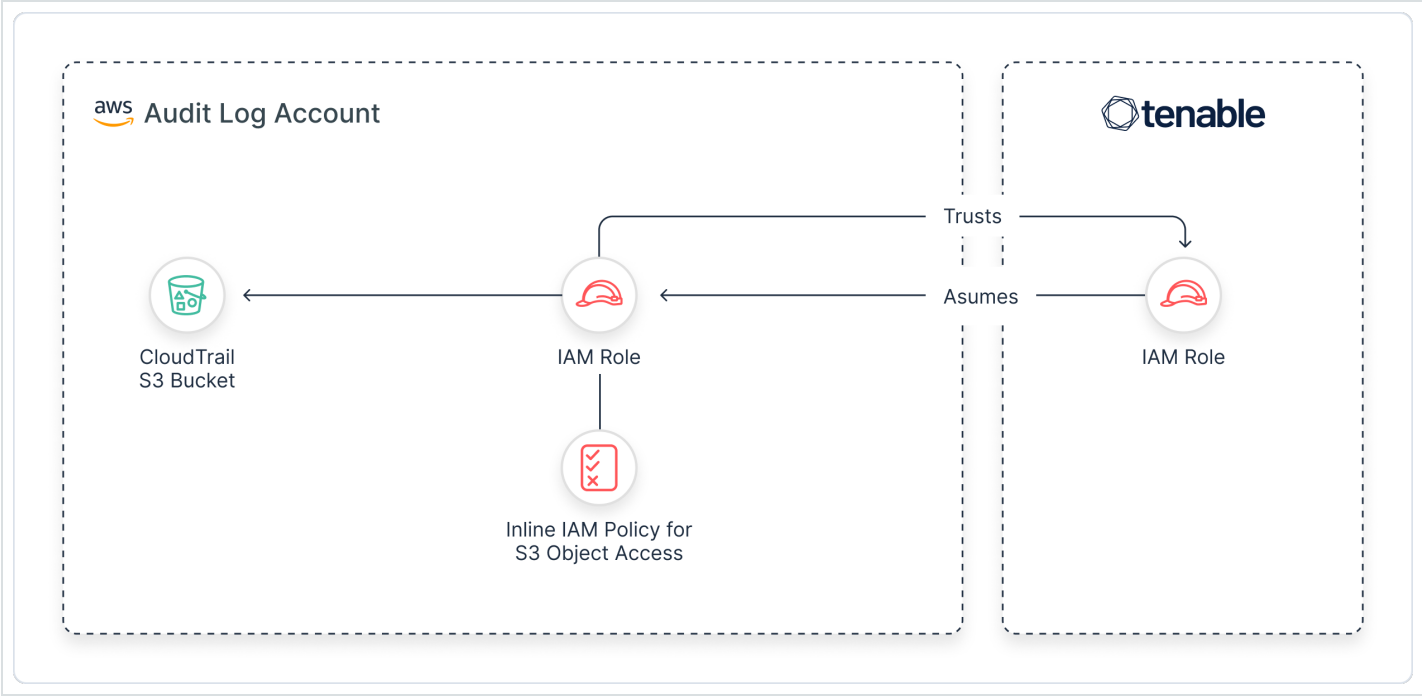
CloudTrail が接続されていない図



CloudTrail のアクセス許可を持つアカウント

この図は、接続したアカウントに関連付けられたIAMロールと、接続されたAWSアカウントとやり取りしてデータを収集するために独自のIAMロールを使用するクラウドサイバーエクスポージャーとの間に確立された信頼関係を示しています。

注意: 監査ログアカウントは、**モニタリング**アクセス許可のない、**CloudTrail**アクセス許可のみが有効または付与されたアカウントです。このようなアカウントはアクティビティログの収集専用であり、セキュリティ目的でモニタリングされることはありません。クラウドサイバーエクスポージャーはこのような方法で接続アカウントをサポートしていますが、クラウド資産のセキュリティを完全に可視化するために、すべてのアカウントに**モニタリング**のアクセス許可を付与して接続することが推奨されます。



AWSの必要なアクセス許可

アカウントを完全に可視化するために、Tenable One Cloud ExposureはAWS管理ポリシーとインラインポリシーの両方を使用して、関連するメタデータを収集する必要があります。これらのポリシーは、アカウントまたは組織を接続した際にIAMでTenable用に作成した専用ロールにアタッチされています。

- **モニタリング**アクセス許可
  - **SecurityAudit**アクセス許可。AWS管理ポリシー。セキュリティ設定メタデータの読み取り許可を付与します。

- カスタム Tenable モニタリングアクセス許可 (読み取り専用)。インラインポリシー。
  SecurityAudit ポリシーに含まれていない追加の読み取り専用アクセス許可を Tenable に付与します。

  SecurityAudit ポリシーとカスタムインラインポリシーの両方が Tenable に必要な理由の詳細は、AWS の FAQ を参照してください。

- (オプション) カスタム Tenable **修正** アクセス許可 (読み取りと書き込み)。インラインポリシーは Tenable に管理のアクセス許可を付与し、Tenable が環境を変更できるようにします。たとえば、この許可により Tenable は検出結果を AWS で直接自動で修正できるようになります (管理のアクセス許可を付与しない場合でも、ワンタイム認証情報をオンデマンドで提供することで、検出結果を手動で修正できます)。
- **CloudTrail (S3)** アクセス許可。詳細については、CloudTrail を参照してください。

お使いの AWS 組織でサービスコントロールポリシー (SCP) またはリソースコントロールポリシー (RCP) を使用している場合は、必ず既存の SCP または RCP に除外を追加して、クラウドサイバーエクスポージャー用に作成した専用の IAM ロールが含まれないようにしてください。詳細については、AWS の FAQ {target=_blank} を参照してください。

付録 I: AWS IAM ポリシー

- Tenable モニタリングポリシー (読み取り専用)
- Tenable 修正ポリシー (読み取りと書き込み)
- CloudTrail ポリシー
- データリソーススキャンポリシー (データ保護)
- EC2 インスタンススキャン (ワークロード保護)
- ECR スキャンワークロード保護ポリシー
- Terraform ポリシー
- Amazon Bedrock 呼び出しログ
- AWS アカウントアクセスの JIT ポリシー
- アプリケーションアクセスの JIT ポリシー

Tenable モニタリングポリシー (読み取り専用)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm:Describe*",
        "acm:List*",
        "aoss:BatchGet*",
        "aoss:List*",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "autoscaling:Describe*",
        "batch:Describe*",
        "batch:List*",
        "bedrock:Get*",
        "bedrock:List*",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudfront:Get*",
        "cloudfront:ListDistributions*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetMetric*",
        "cloudwatch:ListMetrics",
        "codebuild:BatchGet*",
        "codebuild:List*",
```

```
            "cognito-idp:ListResourcesForWebACL",
            "cognito-identity:Describe*",
            "cognito-identity:List*",
            "cognito-idp:List*",
            "cognito-sync:GetCognitoEvents",
            "config:Describe*",
            "dax:Describe*",
            "directconnect:Describe*",
            "dms:Describe*",
            "docdb-elastic:Get*",
            "docdb-elastic:List*",
            "dynamodb:Describe*",
            "dynamodb:GetResourcePolicy",
            "dynamodb:List*",
            "ec2:Describe*",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:SearchTransitGatewayRoutes",
            "ecr:Describe*",
            "ecr:GetRegistryScanningConfiguration",
            "ecr:GetRepositoryPolicy",
            "ecr:List*",
            "ecr:StartImageScan",
            "ecr-public:Describe*",
            "ecr-public:GetRepositoryPolicy",
            "ecr-public:List*",
            "ecs:Describe*",
            "ecs:List*",
            "eks:Describe*",
            "eks:List*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticbeanstalk:Describe*",
            "elasticbeanstalk:List*",
            "elasticfilesystem:Describe*",
            "elasticloadbalancing:Describe*",
            "elasticmapreduce:Describe*",
            "elasticmapreduce:List*",
            "es:Describe*",
            "es:List*",
            "events:ListRules",
            "firehose:Describe*",
            "firehose:List*",
            "glue:BatchGet*",
            "glue:Get*",
            "glue:List*",
            "guardduty:GetDetector",
            "guardduty:ListDetectors",
```

```
            "iam:Generate*",
            "iam:Get*",
            "iam:List*",
            "identitystore:Describe*",
            "identitystore:List*",
            "inspector2:List*",
            "iot:GetTopicRule",
            "kafka:ListClustersV2",
            "kms:Describe*",
            "kms:GetKey*",
            "kms:List*",
            "kinesis:Describe*",
            "kinesis:List*",
            "lambda:Get*Policy",
            "lambda:GetAccountSettings",
            "lambda:List*",
            "logs:Describe*",
            "mq:DescribeBroker",
            "mq:ListBrokers",
            "organizations:Describe*",
            "organizations:List*",
            "rds:Describe*",
            "rds:List*",
            "redshift:Describe*",
            "redshift:List*",
            "redshift-serverless:List*",
            "route53:Get*",
            "route53:List*",
            "route53domains:Get*",
            "route53domains:List*",
            "route53resolver:Get*",
            "route53resolver:List*",
            "s3:Describe*",
            "s3:GetAccessPoint*",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucket*",
            "s3:GetEncryptionConfiguration",
            "s3:GetJobTagging",
            "s3:GetLifecycleConfiguration",
            "s3:ListAccessPoints",
            "s3:ListAllMyBuckets",
            "s3:ListBucketVersions",
            "s3:ListJobs",
            "s3:ListTagsForResource",
            "sagemaker:Describe*",
            "sagemaker:List*",
            "secretsmanager:Describe*",
```

```
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "ssm:Describe*",
        "ssm:List*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "states:List*",
        "sts:DecodeAuthorizationMessage",
        "tag:Get*",
        "timestream:List*",
        "timestream:Get*",
        "timestream:Describe*",
        "wafv2:Get*",
        "wafv2:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET",
        "apigateway:ListRoutingRules"
      ],
      "Resource": [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*:*:/domainnames/*/routingrules/*",
        "arn:aws:apigateway:*::/restapis",
```

```
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ]
    }
  ]
}
```

Tenable 修正ポリシー (読み取りと書き込み)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyInstanceMetadataOptions",
        "ec2:ModifyVpcEndpoint",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ecr:DeleteRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeactivateMFADevice",
        "iam:DeleteAccessKey",
        "iam:DeleteGroup",
        "iam:DeleteGroupPolicy",
        "iam:DeleteLoginProfile",
        "iam:DeletePolicy",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DeleteServerCertificate",
        "iam:DeleteServiceSpecificCredential",
        "iam:DeleteSigningCertificate",
        "iam:DeleteSSHPublicKey",
        "iam:DeleteUser",
```

```
        "iam:DeleteUserPermissionsBoundary",
        "iam:DeleteUserPolicy",
        "iam:DetachGroupPolicy",
        "iam:DetachRolePolicy",
        "iam:DetachUserPolicy",
        "iam:PutGroupPolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:RemoveUserFromGroup",
        "iam:UpdateAccessKey",
        "iam:UpdateAssumeRolePolicy",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "sso:DeleteAccountAssignment",
        "sso:DeleteInlinePolicyFromPermissionSet",
        "sso:DeletePermissionSet",
        "sso:DetachManagedPolicyFromPermissionSet",
        "sso:ProvisionPermissionSet",
        "sso:PutInlinePolicyToPermissionSet"
      ],
      "Resource": "*"
    }
  ]
}
```

CloudTrail ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3LogAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
```

```
        "arn:aws:s3:::YOUR_CLOUDTRAIL_BUCKET_NAME",
        "arn:aws:s3:::YOUR_CLOUDTRAIL_BUCKET_NAME/*"
      ]
    },
    {
      "Sid": "AllowKMSDecrypt",
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:REGION:ACCOUNT_ID:key/KMS_KEY_UUID"
    }
  ]
}
```

データリソーススキャンポリシー (データ保護)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:Scan",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBSnapshotAttribute",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "rds:AddTagsToResource",
      "Resource": [
        "arn:aws:rds:*:*:snapshot:*",
```

```
        "arn:aws:rds:*:*:cluster-snapshot:*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/TenableContext": "DataAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "rds:DeleteDBSnapshot",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:snapshot-tag/TenableContext": "DataAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "rds:DeleteDBClusterSnapshot",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:cluster-snapshot-tag/TenableContext": "DataAnalysis"
        }
      }
    }
  ]
}
```

EC2 インスタンススキャン (ワークロード保護)

以下の IAM ポリシーでは、ec2:CopySnapshot が 3 回表示されます。これらの各エントリは、それぞれ異なる目的で必要です。

1. **リクエストタグ付きでコピー** (条件: aws:RequestTag/ErmeticContext)
    - 特定のリクエストタグが指定されている場合にのみ、スナップショットのコピーを許可します。
    - デスティネーションスナップショットが自動的にタグ付けされるようにします。
    - **ユースケース**: 新しいスナップショットのタグ付けが必要なインスタンスと AMI。

2. **任意のスナップショットをソースとしてコピー** (`Resource: arn:aws:ec2:*::snapshot/snap-*`)
    - 既存のスナップショットをコピーのソースとして使用することを許可します。
    - **ユースケース**: 既存のスナップショットをコピーする必要があるプライベート AMI。
3. **リソースタグ付きでコピー** (条件: `aws:ResourceTag/ErmeticContext`)
    - すでに特定のリソースタグが付いているスナップショットのコピーを許可します。
    - **ユースケース**: 特定のタグが付いたスナップショットのみのコピーが許可されるインスタンス。

IAM ステートメントにおけるソーススナップショットとデスティネーションスナップショットの AWS の処理の詳細については、Amazon EBS スナップショットのコピーに関するリソースレベルのアクセス許可の強化 {target=_blank}を参照してください。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect": "Allow",
      "Action": "kms:CreateAlias",
      "Resource": "arn:aws:kms:*:*:alias/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "kms:CreateKey",
        "kms:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/ErmeticContext": "WorkloadAnalysis"
        }
      }
```

```
    },
    {
      "Effect": "Deny",
      "Action": "kms:TagResource",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/ErmeticContext": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CopySnapshot",
      "Resource": "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "kms:CreateAlias",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:EnableKeyRotation",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ErmeticContext": "WorkloadAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

ECR スキャンワークロード保護ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource": "*"
    }
  ]
}
```

Terraform ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>",
        "arn:aws:s3:::<bucket_name>/*",
```

```
      ]
    }
  ]
}
```

<bucket_name> は関連する S3 バケットの名前です。

Amazon Bedrock 呼び出しログ

> **注意:** 以下のポリシーには、モニタリング対象となるすべてのリージョンにおいて、Amazon Bedrock がログの送信先として使用するすべての Amazon S3 バケットとすべての AWS KMS キーを含める必要があります。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucketName",
        "arn:aws:s3:::bucketName/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "bucketKeyArn"
    }
  ]
}
```

<bucketName> は関連する S3 バケットの名前です。

AWS アカウントアクセスの JIT ポリシー

これらのポリシーを使用すると、AWS Identity Center を介した AWS アカウントとアクセス許可セットへの JIT アクセスを Tenable One Cloud Exposure で管理できるようになります。

AWS Identity Center がアカウントアクセス用の管理アカウントから直接管理されているか、アカウントアクセス用の委任された管理者アカウントを介して管理されているかに応じて、環境ごとに 1 つのポリシーのみを使用します。

アカウントアクセス用の管理アカウント

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider",
                "iam:UpdateSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO__DO_NOT_DELETE"
        },
        {
            "Effect": "Allow",
            "Action": [
                "identitystore:Describe*",
                "identitystore:List*",
```

```
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeletePermissionSet",
                "sso:Describe*",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:Get*",
                "sso:List*",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso-directory:List*",
                "sso-directory:Search*"
            ],
            "Resource": "*"
        }
    ]
}
```

アカウントアクセス用の委任された管理者アカウント

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet"
            ],
            "Resource": "*"
        }
    ]
}
```

アプリケーションアクセスの JIT ポリシー

これらのポリシーを使用すると、AWS Identity Center によって管理されるアプリケーションへの JIT アクセスを Tenable One Cloud Exposure で管理できるようになります。

AWS Identity Center がアプリケーションアクセス用の管理アカウントから直接管理されているか、アプリケーションアクセス用の委任された管理者アカウントを介して管理されているかに応じて、環境ごとに 1 つのポリシーのみを使用します。

アプリケーションアクセス用の管理アカウント

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "identitystore:Describe*",
        "identitystore:List*",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso-directory:List*",
        "sso-directory:Search*"
      ],
      "Resource": "*"
    }
  ]
}
```

アプリケーションアクセス用の委任された管理者アカウント

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:CreateApplicationAssignment",
```

```
        "sso:DeleteApplicationAssignment",
      ],
      "Resource": "*"
    }
  ]
}
```

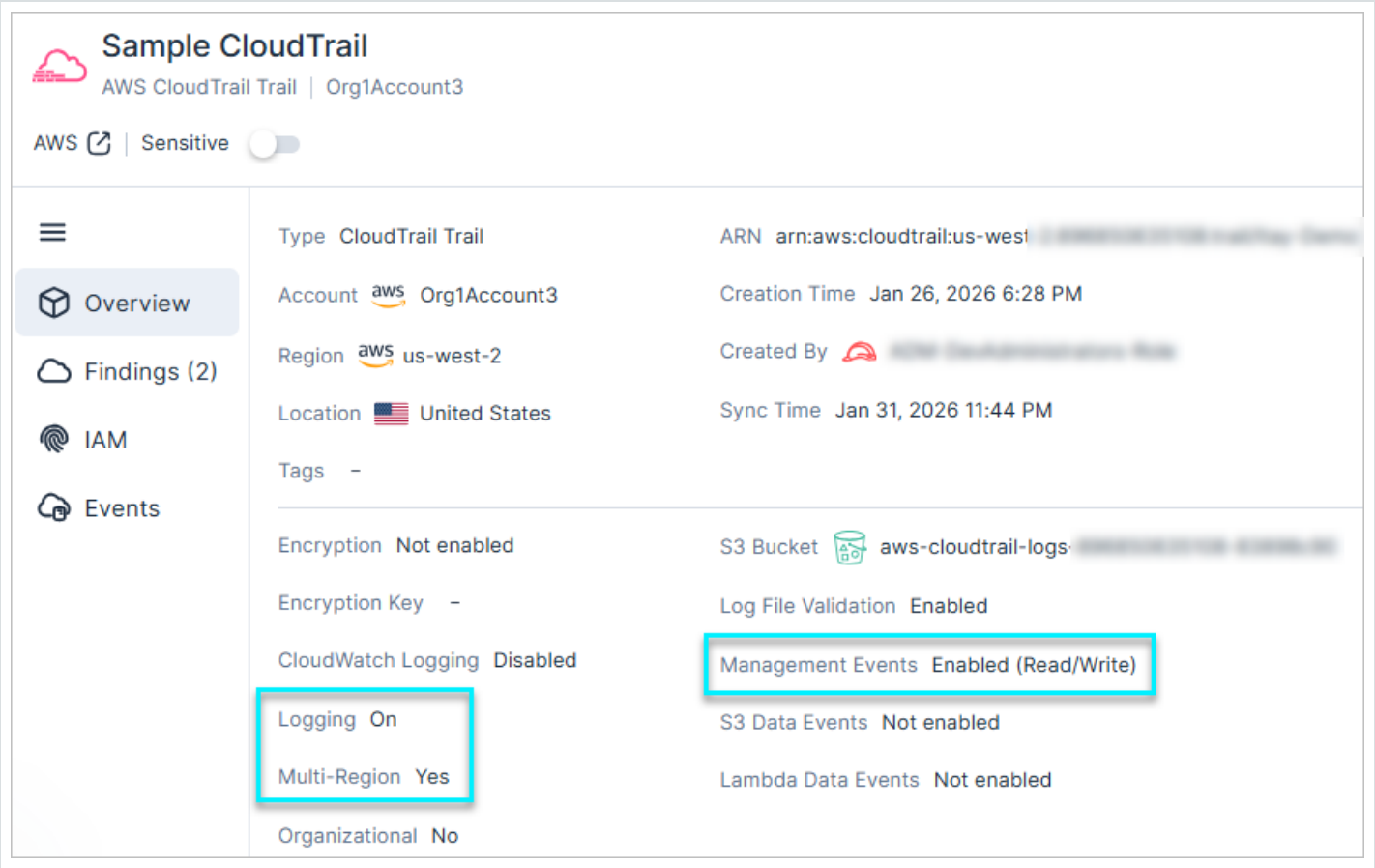
AWS CloudTrail

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

モニタリングプロセスの一環として、Tenable One Cloud Exposure は、接続したアカウントのアクティビティを記録する CloudTrail からデータを読み取る必要があります。アカウントの接続プロセス中に、使用する証跡を選択し、IAM ロールを経由して、証跡が配置されている S3 バケットへのアクセス権を Tenable に付与する必要があります。アカウントおよび組織の接続ステップのガイドラインに従ってください。

接続中に、Tenable は以下の有効な証跡を特定し、表示します。

- **マルチリージョン**。マルチリージョンの証跡が必要な理由の詳細については、AWS の FAQ を参照してください。
- **管理による読み取りおよび書き込みイベントをログに記録するよう設定**。
- **ログの有効化**。



通常、接続された各アカウントには 1 つの CloudTrail が関連付けられますが、アカウントが 2 つ以上の証跡を持つ場合もあります。

CloudTrail ファイルを保存している S3 バケットが、接続しているアカウントと同じアカウントにない場合は、そのアカウントを個別に接続してから、別のアカウント用の CloudTrail として選択する必要があります。別の AWS アカウントを「ログアーカイブアカウント」として使用して、他のアカウントのアクティビティをログに記録する場合、Tenable では、次のベストプラクティスに従うことを推奨しています。

- **モニタリング**と **CloudTrail** 両方のアクセス許可を持つログアーカイブアカウントを接続して、すべての AWS アカウントを完全に可視化します。ただし、何らかの理由でセキュリティモニタリングのためにそのようなアカウントを クラウド サイバーエクスポージャー でスキャンしたくない場合は、**CloudTrail** のアクセス許可のみで接続できます。

CloudTrail アクセスを付与するメリット

アカウントの接続時には、CloudTrail を含む S3 バケットへのアクセスを Tenable に常に付与することをおすすめします。これにより、以下を含むいくつかの重要なメリットが得られます。

- 脅威検出
    - クラウド環境内でアイデンティティによって実行されたアクティビティを可視化 (クラウドイベント)。
    - 動作ベースラインに対して異常をチェックする継続的なリスク分析 (異常検出)。
- アクティビティに基づくアクセス許可の効果的な使用の可視化 (使用済みアクセス許可)。
- 使用状況に基づく詳細な最小権限の推奨事項。詳細については、データイベントに基づく詳細な推奨事項の有効化を参照してください。

データイベントに基づく詳細な推奨事項の有効化

クラウドサイバーエクスポージャー内でアクションおよびリソースの詳細な推奨事項を有効にするには、S3 バケットやオブジェクト、および Lambda 関数に対して CloudTrail データの読み取り/書き込みイベントログを有効化します。その後、クラウドサイバーエクスポージャーで関連する証跡を選択します。
これにより、特定の AWS サービスへのアクセスに関する一般的な情報を表示するだけでなく、以下に関する非常に貴重な情報も分析できます。

- 特定のアイデンティティがサービスで特定のアクションを使用した時期
- アイデンティティがサービス内で使用した正確なリソース

これにより、クラウドサイバーエクスポージャーはこのデータに関連する特定の最小権限の推奨事項を提供できます。たとえば Tenable は、アプリケーションが使用する特定の S3 バケットまでの最小権限について推奨事項を提示できます。

データイベントを有効にしているかどうかに応じて、次のいずれかの方法で CloudTrail と連携するようにクラウドサイバーエクスポージャーを設定できます。

- 管理イベントとデータイベント (S3、Lambda、またはその両方) のいずれも有効にして単一の CloudTrail を使用する場合は、**[管理イベント]** ドロップダウンからその証跡を選択します。**[S3 データイベント]** や **[Lambda データイベント]** フィールドには、ここで選択した CloudTrail 情報が自動的に入力されます。

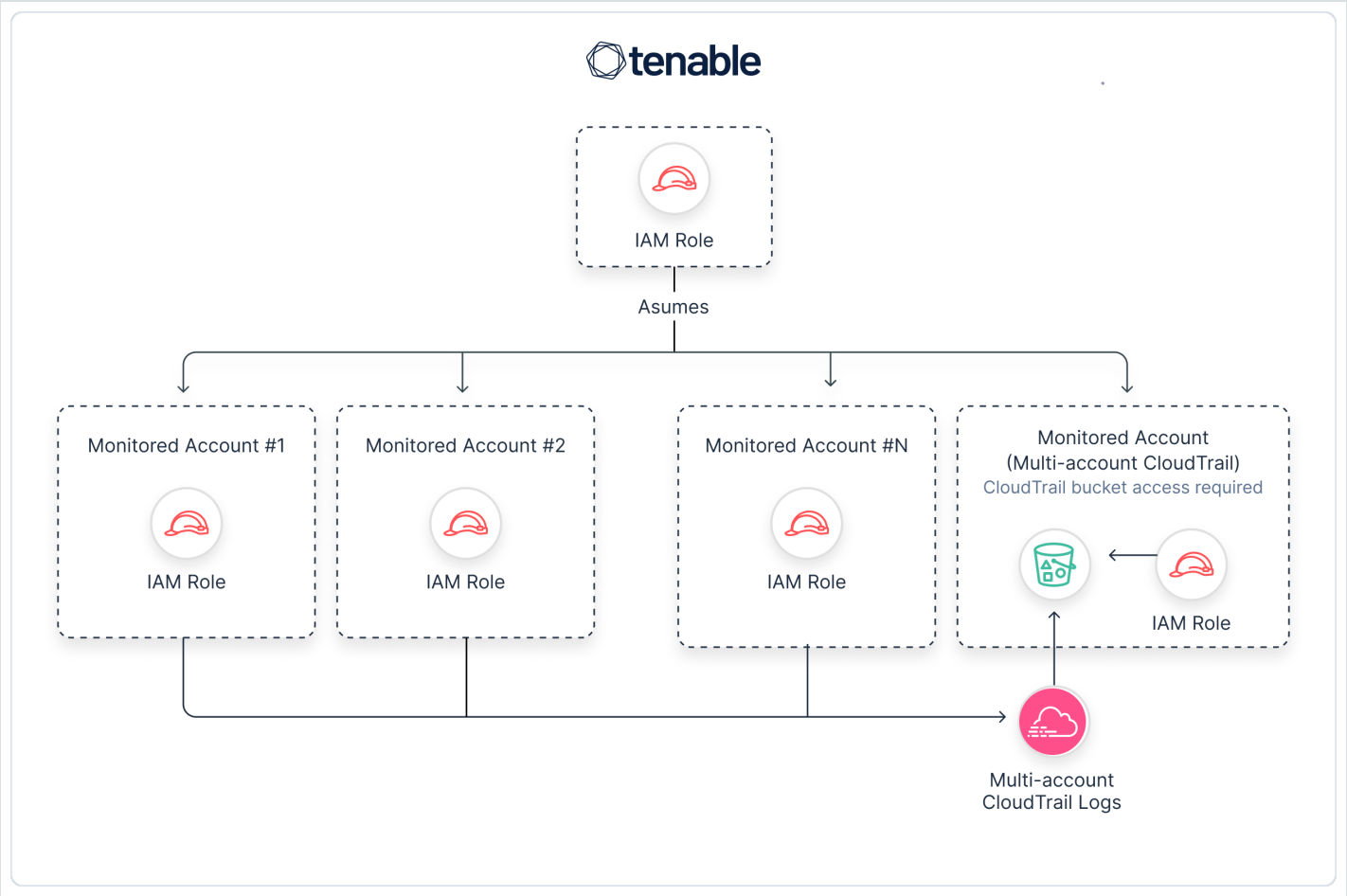
- 管理イベントとデータイベント (S3、Lambda、またはその両方) に別々の証跡を使用する場合は、**[管理イベント]**ドロップダウンから有効にした管理イベントのある CloudTrail を選択し、それぞれのフィールドでデータイベント証跡を選択します。

CloudTrail のデプロイメント

次の図は、複数のアカウントを持つ環境に CloudTrail をデプロイする方法を示し、複数のアカウント専用の CloudTrail (組織の証跡) を維持する環境と、アカウントごとに個別の CloudTrail がある環境の違いに焦点を当てています。

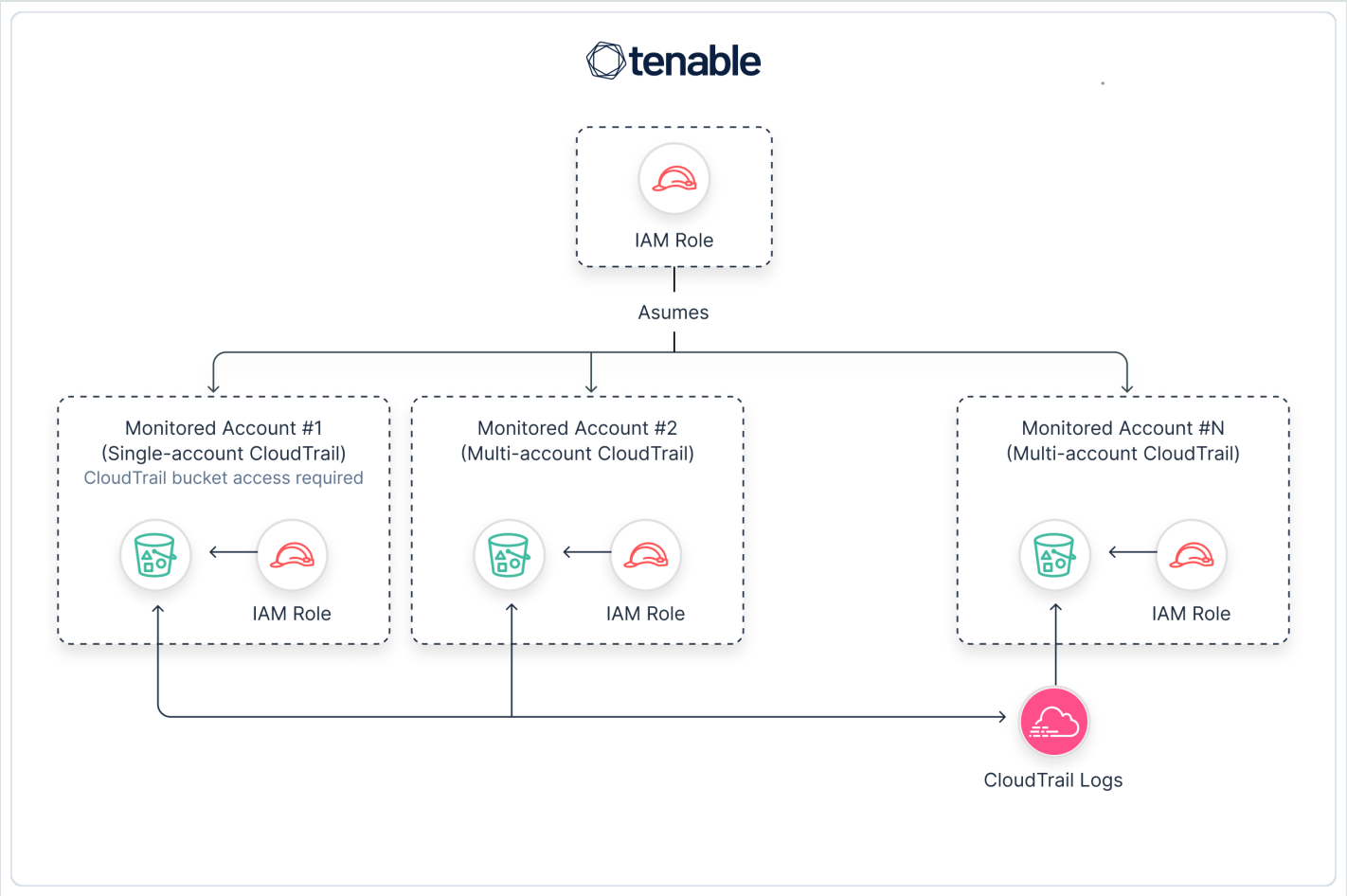
複数アカウント専用の組織の証跡

このシナリオでは、個別の専用 AWS アカウントが、組織の証跡 (他のアカウントのアクティビティを記録する) を含むログアーカイブアカウントとして使用されます。この専用アカウントは、モニタリングアクセス許可を用いてクラウドサイバーエクスポージャーに個別に接続する必要があります。その後、その組織の証跡を、Tenable に接続する他のアカウントの共有 CloudTrail として使用できます。組織全体を接続する場合、組織の接続を完了してから関連するアカウントを編集し、IAM ロール経由で Tenable に CloudTrail のアクセス許可を付与します。



アカウントごとの単一 CloudTrail バケット

このシナリオでは、接続された各アカウントは、独立した CloudTrail (どのアカウントも同じ名前が付けられます) に接続されます。



異なるアカウントの KMS キー

CloudTrail の KMS キーが、追加するアカウントとは別の AWS アカウントにある場合は、キーへのアクセス許可をクラウドサイバーエクスポージャーに付与する必要があります。

異なるアカウントにある KMS キーへのアクセスを許可する方法

1. CloudTrail KMS キーがある AWS アカウントに移動します。
2. **[KMS] > [カスタマーマネージドキー]** の順に移動し、対象の KMS キーを開きます。
3. キーポリシーを**編集**し、以下のステートメントを [ステートメント] セクションに追加します。

```JSON
{
```

```
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "{ErmeticRoleARN}"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

ここで ErmeticRoleARN は、このウィザードで先ほど作成したロールのロール ARN です。

4. **[変更を保存]** をクリックします。

AWS アカウントの接続

この手順を使用して、個別のアカウントをオンボーディングします。AWS 組織の接続する場合、組織のオンボーディングを続行する前に、まずこの手順に従って管理アカウントを個別にオンボーディングする必要があります。

AWS アカウントをオンボーディングする方法

> **注意:** ウィザードの実行中は、Tenable One Cloud Exposure コンソールと AWS マネジメントコンソールの両方を操作する必要があります。

1. **[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. [統合ライブラリ] で、**[AWS アカウント]** を選択します。
3. **[アカウントの詳細]** で、次の手順を実行します。
    1. クラウドサイバーエクスポージャーコンソールに表示するアカウントの**名前**を入力します。

        > **注意:** AWS マネジメントコンソールとクラウドサイバーエクスポージャーコンソールの両方で同じ命名規則を使用するかどうかを選択できます。別の名前を使用する場合は、必ずコンソール間でアカウント名をマッピングできるようにしておきます。

    2. 適切な **AWS パーティション**が選択されていることを確認します (AWS グローバルまたは AWS 中国)。AWS アカウントが属するパーティション。パーティションは AWS リージョンのグループです。詳細については、AWS ドキュメントを参照してください。
    3. リソースをデプロイしている**アクティブなリージョン**をすべて選択します。

> **注意:** 組織で使用している特定のリージョンのみが選択されていることを確認してください。選択されていないリージョンは無視されます。SCP や RCP によって無効化されていない、またはブロックされていないリージョンすべてをスキャン用に有効化します。後の段階でデプロイメントを他のリージョンに拡張する場合は、クラウドサイバーエクスポージャー でアカウントを編集し、それらのリージョンを追加する必要があります。

4. **[次へ]** をクリックします。

4. **[アクセス許可]** で、各種機能を有効にするために必要なアクセス許可を Tenable に付与します。

> **注意:** この選択は、最初のオンボーディングの後でも変更できます。Tenable にアクセス許可を付与する必要がある理由の詳細については、必要なアクセス許可を参照してください。

- **モニタリング (読み取り専用)**: すべてのクラウド資産について完全な可視性を確保します。これにはアクセス許可、アカウント使用状況、セキュリティ設定に関する情報が含まれます。オンボーディングアカウントの CloudTrail を読み取るためにアクセス許可の追加が必要になる場合があります。必要なアクセス許可の詳細については、こちらのドキュメントを参照してください。
- **データ保護**: 機密データを保護するために、クラウドリソースのスキャンと分類を行います。

> **注意:** この機能は、クラウドサイバーエクスポージャー データ保護を使用しているユーザーを対象としています。詳細については、データ保護を参照してください。JSON 形式のポリシーについては、データリソーススキャンポリシー (データ保護)を参照してください。

- **EC2 インスタンスと AMI スキャン (ワークロード保護とデータ保護)**: EC2 インスタンスと AMI (プライベートマシンイメージとパブリックマシンイメージ) をスキャンして、脆弱性、設定ミス、シークレットや機密データがないか確認します。必要なアクセス許可の詳細については、こちらのドキュメントを参照してください。

> **重要:** 重要な注意点
> - この機能は、クラウドサイバーエクスポージャー ワークロード保護を使用しているユーザーを対象としています。詳細については、ワークロード保護を参照してください。JSON 形式のポリシーについては、付録を参照してください。
> - Tenable は、タグに基づいて**バックアップ AMI** として識別される AMI のスキャンを防止するために、デフォルトで除外ルールを追加しました。

- **ECR スキャン (ワークロード保護)**: コンテナレジストリをスキャンして、脆弱性と設定ミスがないか確認します。

  > **注意:** クラウドサイバーエクスポージャー ワークロード保護 (Standard または Enterprise のライセンスが必要) を使用しているユーザーを対象としています。詳細については、ワークロード保護を参照してください。JSON 形式のポリシーについては、付録を参照してください。

- **修正 (読み取りと書き込み)**: Tenable が環境に変更を加えることを許可します。これにより、たとえば、ワンクリックで検出結果を自動的に修正できます (これらのアクセス許可がなくても、OTP を経由してワンクリック修正が可能です)。必要なアクセス許可の詳細については、こちらのドキュメントを参照してください。

- **アカウント割り当てのジャストインタイムアクセス (AWS Identity Center)**: ユーザーにアカウントへのアクセスを、あらかじめ決められた期間、かつ必要に応じて許可します。オンボーディングを行っているアカウントが管理アカウントである場合、またはそのアカウントに AWS Identity Center を管理するアクセス許可がある場合、追加のアクセス許可が必要になります。必要なアクセス許可の詳細については、こちらのドキュメントを参照してください。

- **アプリケーション割り当てのジャストインタイムアクセス (AWS Identity Center)**: ユーザーに AWS Identity Center によって管理されるアプリケーションへの一時的なアクセスを、あらかじめ決められた期間、かつ必要に応じて許可します。オンボーディングを行っているアカウントが管理アカウントである場合、またはそのアカウントに AWS Identity Center を管理するアクセス許可がある場合、追加のアクセス許可が必要になります。必要なアクセス許可の詳細については、こちらのドキュメントを参照してください。

- **CloudTrail (S3)**: クラウドアクティビティログを分析するには、CloudTrail データを保存する S3 バケットから読み取るアクセス許可が必要です。バケットが現在オンボーディングしているアカウントに属している場合は、このオプションを選択します。詳細については、CloudTrail を参照してください。

  1. 証跡データが保存されている**バケットの名前**を入力します。
  2. 証跡バケットが**AWS KMS で暗号化されている**かどうかを示し、暗号化されている場合は **KMS キー ARN** を入力します。

  バケットが別のアカウントに属している場合は、このウィザードの完了後に次のいずれかを行う必要があります。

1. **個別のアカウント** のオンボーディングのみの場合は、他方のアカウントを個別にオンボーディングし、IAM ロール経由で Tenable **CloudTrail** のアクセス許可を付与します。
2. **組織全体** のオンボーディングの場合は、組織のオンボーディングを完了してから関連するアカウントを編集し、IAM ロール経由で Tenable **CloudTrail** のアクセス許可を付与します。

- **Amazon Bedrock モデル呼び出しログ (S3)**: Amazon Bedrock で AI アクティビティをモニタリングするには、モデル呼び出しログを保存する S3 バケットから読み取るアクセス許可が必要です。Amazon Bedrock で AI アクティビティをモニタリングするには、モデル呼び出しログを保存している S3 バケットから読み取るアクセス許可が必要です。詳細については、Amazon Bedrock アクティビティモニタリングの有効化を参照してください。

  > **注意:** この機能を使用する前に、Amazon Bedrock でモデル呼び出しログをオンにします。ステップ 1: Amazon Bedrock モデル呼び出しログの有効化を参照してください。

  > **注意:** Amazon Bedrock アクティビティのモニタリングは、Tenable One AI Exposure の Amazon Bedrock と Bedrock 資産の AI セキュリティポスチャー管理 (AI-SPM) のカバレッジを完了するランタイム機能です。Amazon Bedrock アクティビティのモニタリングは現在、AI ガバナンスアドオンライセンスで追加料金なしで利用できます。

5. **[次へ]** をクリックします。
6. 新しい **IAM ロール**を作成します。これには、CloudFormation (AWS コンソールまたは AWS CLI 経由) を使用するか、AWS コンソールで手動で作成します。

   - **CloudFormation (AWS コンソール)**

     1. オンボーディングする AWS アカウントにログインします。
     2. ここをクリックしてスタックを作成し、AWS のスタックの作成ウィザードで以下の手順を実行します。

        > **重要:** ここに表示されているリンク、またはウィザードのリンクを使用できます。ただし、ここに表示されているリンクを使用する場合は、Tenable の各ポリシーの true 値や false 値がウィザードのステップ 2 で選択したアクセス許可を反映していることを確認してください。

3. (オプション) **RoleName** パラメーターを変更して、IAM ロールに別の名前を選択します。
4. [I acknowledge that AWS CloudFormation might create IAM resources with custom names] を選択して、**[Create Stack]** をクリックします。
5. スタックの作成が完了するまで待ちます。**[更新]** ボタンをクリックすると進捗状況を追跡できます。
6. **[出力]** タブに移動し、**TenableRoleArn** キーに対応する値をコピーします。
7. IAM **ロール ARN** をウィザードに貼り付け、**[次へ]** をクリックします。

- **CloudFormation (AWS CLI)**
  1. AWS CLI の最新バージョンで新しいシェルセッションを開きます。CloudFormation スタックを作成するには、管理者権限が必要です。
  2. ウィザードのステップ B に表示されるコマンドをコピーし、お使いのシェルで実行します。

     > **重要:** 以下はコマンドの例ですが、パラメーターと値は選択したアクセス許可によって異なる場合があることに注意してください。

     ```bash
     aws cloudformation create-stack --stack-name TenableStack --template-url
     https://tenable-             utilities.s3.us-east-
     2.amazonaws.com/Onboarding/AWS/CloudFormation/Template.json --   capabilities
     CAPABILITY_NAMED_IAM --parameters
     ParameterKey=RoleName,ParameterValue=TenableRole
     ParameterKey=RoleExternalId,ParameterValue=ba2edce3-d9e1-4ae4-8b33-ecd3961aed8c
     ParameterKey=RoleTrustedPrincipalId,ParameterValue=<aws_account_id>
     ParameterKey=RoleMonitoringPolicy,ParameterValue=true
     ParameterKey=RoleRemediationPolicy,ParameterValue=false
     ParameterKey=RoleJitPolicy,ParameterValue=false
     ParameterKey=RoleWorkloadProtectionPolicy,ParameterValue=true
     ParameterKey=CloudTrailBucketName,ParameterValue=-
     ParameterKey=CloudTrailKeyArn,ParameterValue=-;aws cloudformation wait stack-create-
     complete --stack-name TenableStack;aws cloudformation describe-stacks --stack-name
     TenableStack --query "Stacks[].Outputs"
     ```

  3. スタックの作成完了後、**TenableRoleArn** キーに対応する **OutputValue** をシェルから

コピーします。

4. IAM **ロール ARN** をウィザードに貼り付け、**[次へ]** をクリックします。

- **手動 (AWS コンソール)**

1. AWS マネジメントコンソールで、**[IAM] > [ロール]** の順に移動し、**[ロールを作成]** をクリックします。
2. [信頼できるエンティティタイプ] については、**[AWS アカウント]** を選択します。
3. AWS アカウントについては、**別の AWS アカウント**を選択し、AWS 環境のタイプに応じて、ウィザードのステップ 1 に表示される値を反映した、以下のいずれかの数字をアカウント ID として入力します。
   - パブリッククラウド: **081802104111**
   - US Gov クラウド: **757023926892**

   これは Tenable のアカウント ID です。この ID は 12 桁です。余分なスペースが含まれないようにしてください。
4. [Options] にある **[Require external ID]** にチェックを入れます。
5. アカウントの追加ウィザードのステップ 3 で提供されたロールの外部 ID を入力します。

   > **注意:** ロールの外部 ID は、クラウドサイバーエクスポージャー が顧客アカウントに割り当てる一意の識別子です。この ID は組織用に作成する各アカウントの ID と同一になります。詳細については、https://docs.aws.amazon.com/IAM/latest/UserGuide/confused-deputy.html を参照してください。

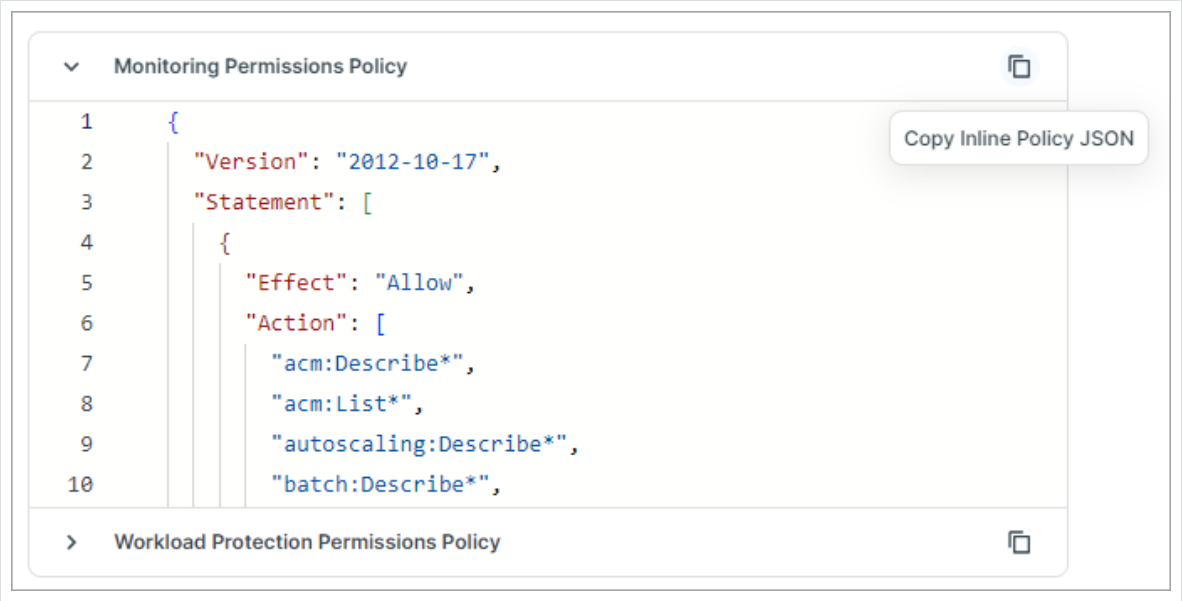
6. ポリシーのリストにある **SecurityAudit アクセス許可** ポリシーを検索して選択し、ロールの作成を完了します。Tenable にアクセス許可を付与する必要がある理由の詳細については、必要なアクセス許可を参照してください。

   g. 新しく作成したロールを開きます。

   9.クラウドサイバーエクスポージャー コンソールでウィザードのステップ 3 (IAM ロール) に表示されるポリシーごとに、次の手順を実行してインラインポリシーを作成します。

   1. **[アクセス許可の追加] > [インラインポリシーの作成]** の順にクリックします。
   2. ウィザードに表示されるポリシーをコピーして、JSON エディターに貼り付けます。以下

に例を挙げます。



3. **[次へ]** をクリックしてポリシーの作成を完了します。

- IAM **ロール ARN** をウィザードに貼り付け、**[次へ]** をクリックします。

7. **CloudTrail を選択します**。管理イベント (必須) および S3/Lambda データイベントの CloudTrail を選択します (ウィザードのステップ 5)。Tenable に証跡へのアクセス許可を付与することに関する重要な情報とベストプラクティスについては、CloudTrail を参照してください。

   1. **[管理イベント]** で、クラウドサイバーエクスポージャー がアクティビティログを読み取れるように、管理イベントが有効になっているプライマリ CloudTrail を選択します。

      > **注意:** ここには有効な証跡のみが表示されます。詳細については、CloudTrail を参照してください。

      - 管理イベントとデータイベント (S3、Lambda、またはその両方) のいずれも有効にして単一の CloudTrail を使用する場合は、ドロップダウンからその証跡を選択します。**[S3 データイベント]** や **[Lambda データイベント]** フィールドには、ここで選択した CloudTrail 情報が自動的に入力されます。
      - 管理イベントとデータイベント (S3、Lambda、またはその両方) に別々の証跡を使用する場合は、ここで有効にした管理イベントのある CloudTrail を選択し、それぞれのフィールドでデータイベント証跡を選択します。

2. (オプション) **[S3 データイベント]** や **[Lambda データイベント]** で、関連する CloudTrail を選択します。詳細については、データイベントに基づく詳細な推奨事項の有効化を参照してください。
3. 証跡ログが保存されている S3 バケットへのアクセス許可をまだ付与していない場合は、画面の指示に従って付与します。
4. CloudTrail の KMS キーが S3 バケットを含むアカウントとは別の AWS アカウントにある場合は、キーへのアクセス権を クラウド サイバーエクスポージャー に付与する必要があります。

8. **[終了]** をクリックします。

次のステップ

アカウントが正常に追加されると、そのアカウントは [アカウント] > [AWS] のテーブルに表示されます。ここからアカウント やアカウントの詳細を表示して、どの機能が有効になっているか、必要なアクセス許可が付与されているか、などを確認できます。

アカウントリソースに関するデータが クラウド サイバーエクスポージャー に表示されるようになります。すべてのデータが表示されるまでにかかる時間は、クラウド環境の規模によって異なります。

AWS 中国アカウントのオンボーディング

個別の AWS 中国アカウントを クラウド サイバーエクスポージャー にオンボーディングします。アカウントをオンボーディングする際に、クラウド サイバーエクスポージャー がアカウントからデータをコピーすることはありません。Tenable は、設定メタデータと CloudTrail イベントログ (オプション) のみをコピーします。この情報は、クラウド サイバーエクスポージャー をデプロイしたリージョンに保存されます。

- オンボーディングは個別アカウントでのみ利用可能です。組織では利用できません。
- AWS 中国アカウントは、次の特徴と機能をサポートしています。
    - CIEM/CSPM
    - アカウント内スキャンの設定 (Enterprise ライセンス)
    - アカウント内スキャンの設定 (Enterprise ライセンス)
- Tenable は AWS 中国にサーバーを展開していません。代わりに、資産設定 (およびオプションでイベントログ) は、AWS 中国から Tenable ホストリージョン別の地域 (米国など) にコピーされます。このデータは、中国以外のアカウントから同期されたデータと一緒に保存されます。

AWS 中国アカウントをオンボーディングする方法

1. **IAM ユーザーの作成**
    1. お使いの中国アカウントの AWS マネジメントコンソールで、**[IAM] > [ユーザー]** の順に移動します。

        > **注意:** 中国アカウントを複数お持ちの場合、どのアカウントでもユーザーを作成できます。どれでも構いません。

    2. **[ユーザーの作成]** をクリックします。
    3. 意味のある**ユーザー名**を入力します。
    4. [AWS マネジメントコンソールへのユーザーアクセスを提供する] チェックボックスが選択されて**いないこと**を確認します。
    5. **[次へ]** をクリックします。
    6. [許可を設定] ページで、設定を変更せずに **[次へ]** をクリックします。
    7. ユーザーの詳細を確認し、**[ユーザーの作成]** をクリックします。
2. **インラインポリシーを追加します。**
    1. [ユーザー] テーブルで、作成したばかりのユーザーをクリックします。
    2. [アクセス許可] で、**[アクセス許可を追加] > [インラインポリシーを作成]** の順にクリックします。
    3. ポリシーエディターで **JSON** をクリックし、以下のコードをエディターに貼り付けます。

        JSON

        ```
        {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Effect": "Allow",
              "Action": "sts:AssumeRole",
              "Resource": "arn:aws-cn:iam::*:role/tenable-cs-role"
            }
          ]
        }
        ```

        > **注意:**

> - `tenable-cs-role` は上記のポリシーでロール名として使用されていますが、必要に応じて名前を変更できます。
> - この後アカウントのオンボーディング中に必要となるため、このロール名を保存します (デフォルト: `tenable-cs-role`)。

4. **[次へ]** をクリックします。
5. 意味のある**ポリシー名**を入力してから **[ポリシーの作成]** をクリックします。

3. **アクセスキーを作成します。**

> **注意:** 複数のアカウントに対して 1 つのアクセスキーを作成できます。アカウントを追加するたびにこの手順を繰り返す必要はありません。

1. 作成したユーザーについて、[セキュリティ認証情報] で **[アクセスキーを作成]** をクリックします。
2. **[サードパーティーサービス]** を選択し、**[次へ]** をクリックします (チェックボックスを選択して確定します)。
3. **[アクセスキーを作成]** をクリックします。
4. [アクセスキーを取得] ページで**アクセスキー**と**シークレットアクセスキー**の値を安全に保存し、**[完了]** をクリックします。

4. サポートへの問い合わせ。し、作成した IAM ロールのアクセスキーとシークレットを安全に提供してください。
5. サポートはこの情報を使用して、アカウントのオンボーディング中に AWS 中国をパーティションとして使用できるようにします。
6. AWS 中国アカウントを接続し、次のことに留意してください。
   - オンボーディングウィザードのステップ 1 で、[AWS パーティション] から **[中国]** を選択します。
   - オンボーディングウィザードのステップ 3 で、作成する IAM ロールに、以前作成したポリシーのロールと同じ名前が付けられていることを確認してください (デフォルト: `tenable-cs-role`)。

次のステップ

アカウントが正常に追加されると、そのアカウントは [アカウント] > [AWS] のテーブルに表示されます。ここからアカウントやアカウントの詳細を表示して、どの機能が有効になっているか、必要なアクセス許可が付与されているか、などを確認できます。

アカウントリソースに関するデータがクラウドサイバーエクスポージャーに表示されるようになります。すべてのデータが表示されるまでにかかる時間は、クラウド環境の規模によって異なります。

AWS 組織の接続

AWS 組織の接続

AWS 組織全体を接続することで、多数のアカウントがあるクラウド環境での接続プロセスを迅速化かつ自動化できます。これにより、以下が可能になります。

- すべてのアカウントを同時に Tenable に接続できる。
- 後の段階で AWS に追加された新しいアカウントを自動的に接続できる。
- プラットフォーム機能の全範囲に関連する可視性を確保できる (組織と個人のアカウントの接続に関する考慮事項を参照してください)

前提条件

AWS アカウントの接続手順で、組織の管理アカウントを Tenable One Cloud Exposure にオンボーディングします。

組織の接続

AWS 組織を接続する方法

ウィザードの実行中は、クラウドサイバーエクスポージャーコンソールと AWS マネジメントコンソールの両方を操作する必要があります。

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** の順に移動し、**[統合を追加]** をクリックします。
2. [統合ライブラリ] で、**[AWS 組織]** を選択します。
3. **[管理アカウントを選択]** で、すでにオンボーディングされている管理アカウントを選択します。前提条件を参照してください。

   組織の管理アカウントをオンボーディングしていない場合は、ドロップダウンに表示されません。

4. **[組織の詳細]** で、次の手順を実行します。

    1. **組織名とロール名** が正しいことを確認します。

        > **注意:**
        > - 組織名とは組織の ID です。AWS Organizations コンソールで確認できます。
        > - 過去に個別のアカウントを クラウド サイバーエクスポージャー に接続したことがある場合は、ここで選択する IAM ロールの名前が、それらのアカウントに使用されているロール名とは異なることを確認してください。使用されていた他のロールは、このウィザードで StackSets をデプロイした後に安全に削除できます。

    2. メンバーアカウントにデフォルト名を使用している場合、すべてのメンバーアカウントで使用される **CloudTrail の名前** を選択します。すべてのメンバーアカウントで CloudTrail のデフォルト名を使用していない場合でも、組織の接続後に個別のアカウントに対して CloudTrail を設定できます。このフィールドにはワイルドカード文字 (*) を入力できます (例: `Organization-Trail-*` は `Organization-Trail-1234` を選択します)。

        > **重要:** 組織の接続が完了した後、証跡を含む S3 バケットへのアクセス権を Tenable に付与する必要があります。そのためには、クラウド サイバーエクスポージャー で、バケットが配置されている対象アカウントを編集し、IAM ロールを介して Tenable に CloudTrail のアクセス許可を付与します。バケットが管理アカウントにある場合は、アカウントの接続時にすでにアクセス許可を付与してある可能性があります。

    3. リソースをデプロイしている **アクティブなリージョン** をすべて選択します。

        組織で使用している特定のリージョンのみが選択されていることを確認してください。選択されていないリージョンは無視されます。SCP や RCP によって無効化されていない、またはブロックされていないリージョンすべてをスキャン用に有効化します。後の段階でデプロイメントを他のリージョンに拡張する場合は、クラウド サイバーエクスポージャー でアカウントを編集し、それらのリージョンを追加する必要があります。

    4. **フォルダー構造を自動的に更新するかどうか** を選択します。

        AWS 組織単位のフォルダー構造をプラットフォームにコピーし、アカウント階層は維持したままで、継続的に同期します。詳細は、アカウント階層とフォルダーを参照してください。

5. **[次へ]** をクリックします。

6. **[アクセス許可]** で、各種機能を有効にするために必要なアクセス許可を Tenable に付与します。詳細については、必要なアクセス許可を参照してください。

   - **モニタリング (読み取り専用)**: すべてのクラウド資産について完全な可視性を確保します。これにはアクセス許可、アカウント使用状況、セキュリティ設定に関する情報が含まれます。オンボーディングアカウントの CloudTrail を読み取るためにアクセス許可の追加が必要になる場合があります。
   - **データ保護**: 機密データを保護するために、クラウドリソースのスキャンと分類を行います。

     > **注意:** この機能は、クラウド サイバーエクスポージャー データ保護を使用しているユーザーを対象としています。詳細については、データ保護を参照してください。JSON 形式のポリシーについては、データリソーススキャンポリシー (データ保護)を参照してください。

   - **EC2 インスタンスと AMI スキャン (ワークロード保護とデータ保護)**。EC2 インスタンスと AMI (プライベートマシンイメージとパブリックマシンイメージ) をスキャンして、脆弱性、設定ミス、シークレットや機密データがないか確認します。必要なアクセス許可の詳細については、こちらのドキュメントを参照してください。

     > **重要:** 重要な注意点
     > - この機能は、クラウド サイバーエクスポージャー ワークロード保護を使用しているユーザーを対象としています。詳細については、ワークロード保護を参照してください。JSON 形式のポリシーについては、付録を参照してください。
     > - Tenable は、タグに基づいて**バックアップ AMI** として識別される AMI のスキャンを防止するために、デフォルトで除外ルールを追加しました。

   - **ECR スキャン (ワークロード保護)**: コンテナレジストリをスキャンして、脆弱性と設定ミスがないか確認します。

     クラウド サイバーエクスポージャー ワークロード保護 (Standard または Enterprise のライセンスが必要) を使用しているユーザーを対象としています。詳細については、ワークロード保護を参照してください。JSON 形式のポリシーについては、付録を参照してください。

   - **修正 (読み取りと書き込み)**: Tenable が環境に変更を加えることを許可します。この許可により、検出結果をワンクリックで自動修正できるようになります。必要なアクセス許可の詳細については、こちらのドキュメントを参照してください。

7. **[次へ]** をクリックします。

8. **CloudFormation** (AWS コンソールまたは AWS CLI 経由) を使用して **IAM ロールを作成します**。
    - **CloudFormation (AWS コンソール)**
        1. 組織の AWS 管理アカウントにログインします。
        2. **[CloudFormation] > [StackSets]** の順に移動します。
        3. **[StackSets の作成]** をクリックします。
        4. ステップ 1 (テンプレートの選択) で、[アクセス許可] セクションと [前提条件 - テンプレートの準備] セクションのデフォルト値はそのままにして、[テンプレートの指定] セクションでデプロイメントタイプに応じて以下のいずれかを入力します。両方のタイプで、次の S3 URL/テンプレートを使用します。`https://tenable-utilities.s3.us-east-2.amazonaws.com/Onboarding/AWS/CloudFormation/Template.json`
            - 標準 AWS 企業 (商用): **Amazon S3 の URL** を選択し、上記の URL を入力します。
            - AWS GovCloud (米国) 組織: **[テンプレートファイルをアップロード]** を選択します。上記のテンプレートを JSON ファイルとしてダウンロードし、ここにアップロードします。
        5. **[次へ]** をクリックします。
        6. ステップ 2 (StackSets の詳細を指定) で、**StackSets 名** と、必要に応じて説明を入力します。
        7. クラウドサイバーエクスポージャー コンソールの [AWS 組織を追加] ウィザードに記載されているパラメーター値を入力します。
        8. **[次へ]** をクリックします。
        9. ステップ 3 (StackSets オプションの設定) では、デフォルト値をそのまま変えずに **[次へ]** をクリックします。
        10. ステップ 4 (デプロイメントオプションの設定) で、**[組織へのデプロイ]** か **[組織単位 (OU) へのデプロイ]** のいずれかを選択します。他のデフォルト値はそのままにします。
        11. [リージョンの指定] セクションで単一のリージョンを選択します (IAM ロールはリージョンを特定するものではありません)。

12. **[次へ]** をクリックします。
13. ステップ 5 (レビュー) で StackSets の設定を確認します。**[AWS CloudFormation によって IAM リソースがカスタム名で作成される場合があることを承認します]** を選択して、**[送信]** をクリックします。
14. スタックの作成が完了するまで待ちます。**[更新]** ボタンをクリックすると進捗状況を追跡できます。
15. [クラウドサイバーエクスポージャーコンソール] **[次へ]** をクリックします。

- **CloudFormation (AWS CLI)**
  1. 組織の AWS 管理アカウントにログインします。
  2. AWS CLI の最新バージョンで新しいシェルセッションを開きます。CloudFormation スタックを作成するには、管理者権限が必要です。
  3. クラウドサイバーエクスポージャーコンソールに表示されるコマンドをコピーし、お使いのシェルで実行します。

3. AWS マネジメントコンソールで、**[CloudFormation] > [StackSets]** の順に移動し、新しく作成した StackSets を開きます。
4. スタックの作成が完了するまで待ちます。**[更新]** ボタンをクリックすると進捗状況を追跡できます。
5. [クラウドサイバーエクスポージャーコンソール] **[次へ]** をクリックします。

9. **[範囲を設定]** で、オンボーディングする組織単位 (OU) とアカウントを選択します。
   - **すべてのアカウントを同期する (推奨)**
   - **特定の OU とアカウントを含める**
   - **特定の OU とアカウントを除外する**

   > **注意:**
   > - OU 全体を含めると OU 内の現在および将来的なアカウントがすべて含まれ、OU 全体を除外するとすべて除外されます。
   > - 特定のアカウントを含めるとそのアカウントのみが含まれ、特定のアカウントを除外するとそのアカウントのみが除外されます。

10. **[終了]** をクリックします。

次のステップ

組織が正常に追加された後

- 組織は、[組織] > [アカウント] ページで確認できます。
- 組織に属するアカウントは、[アカウント] > [AWS] ページで確認できます。ここからアカウントやアカウントの詳細を表示して、どの機能が有効になっているか、必要なアクセス許可が付与されているか、などを確認できます。

アカウントリソースに関するデータがクラウドサイバーエクスポージャーに表示されるようになります。すべてのデータが表示されるまでにかかる時間は、クラウド環境の規模によって異なります。

AWS の FAQ (よくある質問) とトラブルシューティング

この記事の内容

- Tenable One Cloud Exposure への AWS のオンボーディングに関連する、よくある質問のリスト
- アカウントステータスとトラブルシューティング

us-east-1 リージョンへのアクセス

> リソースをデプロイしていないのに、Tenable が米国東部 (バージニア北部) (us-east-1) リージョンにアクセスする必要があるのはなぜですか? また、そのリージョンでアクセス許可をブロックするサービスコントロールポリシー (またはその他のメカニズム) を設定できないのはなぜですか?

回答: 組織が使用しているリージョン内で必要なすべてのアクセス許可を Tenable に付与している場合でも、一部の AWS のサービスはグローバルであるため、Tenable にはグローバルエンドポイント (us-east-1) をクエリするアクセス許可が必要です。詳細については、こちら やこちら にある AWS の関連ドキュメントを参照してください。

お使いの AWS 組織でサービスコントロールポリシー (SCP) を使用している場合は、必ず既存の SCP に除外を追加して、Tenable 用に作成した専用の IAM ロールが含まれないようにしてください。

AWS コンソールのアカウントへのアクセス

> Tenable が AWS コンソールで私のアカウントにアクセスしようとしているというアラートが (GuardDuty などで) 表示されています。クラウドサイバーエクスポージャーのような API ベースのツールがこのようなアクセス権を必要とするのはなぜですか?

回答: 一般的に言えば、クラウドサイバーエクスポージャーは API 経由でのみ情報を引き出します。ただし一部のデータ (Lambda トリガーや AWS SSO など) は、Amazon のドキュメント化されたパブリック API 経由では利用できません。こうした情報を取得するために、Tenable では AWS コンソールでよく使用される API 呼び出しを使用します。この呼び出しにより、表示されているアラートが発生します。これらは本質的にドキュメント化されていない API です。アラートはまったく正常であり、実際に想定された動作です。いかなる場合も、Tenable が手動でコンソールにアクセスすることはありません。すべてのアクセスは厳密に API 経由で行われます。

組織から OU またはアカウントを除外する

> すでにオンボーディングした企業から、特定の OU またはアカウントを除外するにはどうすればよいですか?

回答: 組織の範囲を変更し、特定のエンティティを削除する方法は次のとおりです。

1. コンソールで、**[設定]** > **[統合]** に移動します。
2. 組織の横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
3. **[次へ]** をクリックしてウィザード (スコープ) の最後のステップに移動します。
4. **[特定の OU とアカウントを除外する]** を選択してから、対象の OU またはアカウントを選択します。
5. **[終了]** をクリックします。コンソールから削除されます (ご使用の環境内で Tenable が次回 データの同期と更新の頻度 ときに)。

Elastic Beanstalk バケットの GetObject アクセス許可

> Tenable が、オンボーディングしたアカウントの Elastic Beanstalk バケットに GetObject アクセス許可を必要とするのはなぜですか?

回答: Elastic Beanstalk の設定は S3 バケットに保存されています。そのため、このアクセス許可以外に、このサービスの設定にアクセスできる方法はありません。

カスタムポリシーとSecurityAudit ポリシーの両方の必要性

> インラインポリシーのほぼすべてのアクセス許可が SecurityAudit ポリシーに存在しているのに、Tenable ではカスタムの読み取り専用インラインポリシーと AWS が管理する SecurityAudit ポリシーの両方を追加する必要があるのはなぜですか?

回答: Tenable は、自社製品に新しい機能を継続的に追加しています。これをサポートするために、カスタムインラインポリシーは Tenable によって随時更新されます。SecurityAudit ポリシーにはさらに広範なアクセス許可セットが含まれており、これをインラインポリシーと併用することで、クラウドサイバーエクスポージャーに次々と追加され拡大していく新機能へのサポートを確実なものにできます。Tenable の現在と今後の全機能に対する完全かつ継続的なサポートを確保し、アクセス許可セットの追跡や更新を頻繁に行う作業負荷を軽減するためには、両方のポリシーが必要です。

AWS の新しいサービスとアクセス許可

> AWS が新しいサービスやアクセス許可を追加してから Tenable に反映されるまで、どのくらい時間がかかりますか?

回答: 新しいサービスやアクセス許可が提供され次第、すぐに反映されるようにしていますが、クラウドサイバーエクスポージャーコンソールに表示されるまでには最大 1 週間かかる場合があります。このような変更を検出するプロセスは、手動ではなくプログラムによって行われます。

組織の統合名の更新

> クラウドサイバーエクスポージャーでは AWS 組織の統合の表示名を変更できますか?

回答: はい。名前の変更は、複数の組織がある場合、識別に役立ちます。

名前を変更する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. 関連する統合の横にある三点リーダーをクリックして、**[編集]** をクリックします。

3. ウィザードのステップ 2 に移動し、**[組織名]** フィールドを更新します。
4. **[次へ]** をクリックしてウィザードの最後のステップに移動し、**[更新]** をクリックします。

インベントリの ECS タスク定義

> 資産インベントリの表示 に表示されない ECS タスク定義があるのはなぜですか?

回答: インベントリの焦点を最新に保つために、Tenable は次の条件のうち少なくとも 1 つを満たすタスク定義のみを同期します。

- ステータスが**アクティブ**である
- **非アクティブ**の定義が、現在アクティブな ECS サービスまたはタスクによって参照されている

データに実際のアタックサーフェスを反映させるため、非アクティブおよび未使用のタスク定義はインベントリから自動的に除外されます。これらの除外されたリソースに関連する検出結果は、自動的にクローズされます。

マルチリージョンの CloudTrail

> Tenable がデータを読み取る必要がある CloudTrail をマルチリージョンにする必要があるのはなぜですか?

回答: クラウド サイバーエクスポージャー では、使用されていないアクセス許可の削除を推奨するためなどの理由から、すべてのリージョンで管理イベントを継続的に監査する必要があります。このような推奨事項を自信を持って提供するために、Tenable では、使用されていないアクションやアクセス許可を確認することを目的に、環境全体にわたる全範囲のログの可視性を必要としています。

アカウント ステータスとトラブルシューティング

クラウド サイバーエクスポージャー では、[アカウント] > [AWS] ページで各アカウントの**ステータス**が表示されます。これはたとえば、Tenable がアカウントに接続できるかどうかを示すもので、オンボーディングに関する潜在的な問題のトラブルシューティングに役立ちます。

ステータス	説明
アクセスが拒否されました	クラウドサイバーエクスポージャーは1つ以上のリソースタイプを同期できませんでした。これにはさまざまな理由が考えられますが、よくある原因は、AWSでクラウドサイバーエクスポージャー読み取り専用ポリシー(アカウントのオンボーディング中に追加)を更新する必要があることです。
アカウントが見つかりません	
接続済み	クラウドサイバーエクスポージャーはアカウントに正常に接続され、アカウントは実行されています。
接続に問題あり	クラスタは接続されていますが、対処の必要がある特定の問題があります。 • JITアクセス許可が付与されていない • データリソーススキャンポリシー(データ保護)が付与されていない • EC2インスタンススキャン(ワークロード保護)が付与されていない • ECRスキャンワークロード保護ポリシーが付与されていない • Terraform (S3) のアクセス許可が付与されていない • イベントの読み取りに必要なアクセス許可がない
削除中...最大で1時間かかる場合があります	クラウドサイバーエクスポージャーでアカウントを削除しましたが、そのプロセスはまだ完了していません。
切断	クラウドサイバーエクスポージャーにアクセス許可を委任するために、アカウントのオンボーディング中に作成したIAMロールに問題があります。削除されたか、Tenableがロールを引き受けられないようにする信頼ポリシーが変更された可能性があります。

ステータス	説明
無効なアクセス許可	クラウドサイバーエクスポージャーにアクセス許可を委任するために、アカウントのオンボーディング中に作成したIAMロールに問題があります。一部のアクセス許可がありません。必要なアクセス許可をIAMロールに追加してください。
リージョンのクエリに失敗しました	クラウドサイバーエクスポージャーは、アカウントのオンボーディングで選択したアクティブなリージョンをクエリできませんでした。1つ以上のリージョンが無効になっている可能性があります。リージョンリストを変更するか、SCPとRCPからIAMロールの除外を追加してください。詳細については関連するAWSドキュメントを参照してください。
削除の保留中	アカウントはAWSで閉鎖待ちの状態です。最終的には削除されます。削除を保留中のアカウントに関連付けられているリソースと検出結果は、クラウドサイバーエクスポージャーでは非表示になります。
読み取り専用ポリシーが正しくありません	クラウドサイバーエクスポージャーの読み取り専用ポリシーに、以下のアクションが少なくとも1つありません。 • AwsCloudTrail.Actions.DescribeTrails • AwsCloudTrail.Actions.GetEventSelectors • AwsCloudTrail.Actions.GetTrail • AwsCloudTrail.Actions.GetTrailStatus
一時停止	アカウントはAWSで一時停止されています。最終的には削除されます。一時停止されているアカウントのリソースと検出結果はクラウドサイバーエクスポージャーでは非表示になります。

CloudTrail のステータス

CloudTrail 関連の問題の詳細については、AWS CloudTrail を参照してください。

ステータス	説明
接続済み	CloudTrail ログの分析
重複イベント	CloudTrail に重複イベントが含まれています。証跡が正しく設定されていることを確認してください。これは、重複するイベントタイプをカバーする複数の証跡を同じアカウントに設定した場合に生じる可能性があります。
無効な CloudTrail が設定されています	無効な CloudTrail が設定されています。有効な証跡を選択するか、設定を変更してください。
アクセス許可なし	CloudTrail サービスへの権限がありません (証跡のリストを取得できません)
バケットへのアクセス許可がありません	ターゲット S3 バケットから CloudTrail イベントを読み取る権限がありません (別のアカウントに属している可能性があります)。
未設定	CloudTrail ログは分析されていません。有効な証跡を設定してください。

Azure

Azure の概要

Azure 組織の接続 (ルート管理グループ) または個別のサブスクリプションを Tenable One Cloud Exposure に接続して、サブスクリプションに関連付けられているすべてのリソースの可視性とリスク評価 (サブスクリプションの使用状況、セキュリティ設定に関する情報を含む) を取得します。Tenable は、Azure API からインベントリと設定データを収集します。

ユーザー、アクセス許可、アクセス関係などのアイデンティティ関連の表示には、別の Microsoft Entra ID テナントの接続が必要です。

接続が完了すると、Tenable にサブスクリプションのステータスとトラブルシューティングが表示されます。これはたとえば、Tenable がアカウントに接続できるかどうかを示すもので、潜在的な問題のトラブルシューティングに役立ちます。

接続の考慮事項

Azure をクラウドサイバーエクスポージャーに接続する場合、接続の選択がカバレッジと利用可能な集約情報にどのように影響するかを考慮することが重要です。

Azure リソースの接続により、クラウドインフラ、設定リスク、セキュリティポスチャーを可視化できます。Azure に加えて Microsoft Entra ID を接続すると、ユーザー、アクセス許可、最小権限の分析など、アイデンティティ関連の情報を可視化し、Microsoft クラウド環境全体のより包括的なリスク評価が可能になります。

環境の構造と管理方法に応じて、個別のサブスクリプションまたは Azure 組織全体 (ルート管理グループ) を接続できます。**Tenable では、Azure の組織全体を接続し、Microsoft Entra ID を設定する**ことで、クラウドリソースとアイデンティティの両方を包括的に可視化し、現在および将来のサブスクリプションをすべて含めることを推奨しています。

Azure の必要なアクセス許可

Microsoft Entra ID および Azure サブスクリプション/組織を Tenable One Cloud Exposureに接続するには、次のアクセス許可が必要です。

Microsoft Entra ID のアクセス許可

Microsoft Entra ID のクラウドサイバーエクスポージャーコネクタアプリケーションに必要な設定をデプロイすると、Tenable に以下のアクセス許可が付与されます。

- **ユーザーの基本プロファイルの表示** (`profile`)。ユーザーの基本プロファイル (名前、写真、ユーザー名、メールアドレスなど) をアプリで表示できるようにします。
- **すべての監査ログデータの読み取り** (`AuditLog.Read.All`)。サインインしたユーザーがいなくても、アプリで監査ログアクティビティを読み取り、クエリできるようにします。

- **ディレクトリデータの読み取り** (`Directory.Read.All`)。サインインしたユーザーがいなくても、アプリで組織のディレクトリ内のデータ (ユーザー、グループ、アプリなど) を読み取ることができるようにします。
- **組織のポリシーの読み取り** (`Policy.Read.All`)。サインインしたユーザーがいなくても、アプリが組織のポリシーをすべて読み取ることができます。
- **Azure AD グループへのアクセスに関する割り当てスケジュールの読み取り** (`PrivilegedAssignmentSchedule.Read.AzureADGroup`)。サインインしたユーザーがいなくても、アプリで Microsoft Entra ID グループへのアクセスに関する時間ベースの割り当てスケジュールを読み取ることができます。
- **Azure AD グループへのアクセスに関する資格スケジュールの読み取り** (`PrivilegedEligibilitySchedule.Read.AzureADGroup`)。サインインしたユーザーがいなくても、アプリで Microsoft Entra ID グループへのアクセスに関する時間ベースの資格スケジュールを読み取ることができます。
- **すべての RBAC プロバイダーのロール管理データの読み取り** (`RoleManagement.Read.All`)。サインインしたユーザーがいなくても、アプリですべての RBAC プロバイダーのロールベースのアクセス制御 (RBAC) 設定を読み取ることができるようにします。これには、ロールの定義とロールの割り当ての読み取りが含まれます。
- **グループの PIM におけるすべてのポリシーの読み取り** (`RoleManagementPolicy.Read.AzureADGroup`)。サインインしたユーザーがいなくても、アプリでグループの特権アイデンティティ管理のポリシーを読み取ることができます。

これらのアクセス許可は、Tenable が関連の Microsoft Entra ID リソースに関連するデータを収集してレポートを作成するために必要です。

> **重要:** デプロイメントスクリプトを実行すると、テナントでサービスプリンシパルが作成または更新されます。サービスプリンシパルは、ディレクトリ内の クラウド サイバーエクスポージャー コネクタアプリケーションを表し、割り当てられたアクセス許可とロールに基づいて、必要な Microsoft Entra ID および Azure リソースにアクセスできるようにします。
> Microsoft Entra ID のアプリケーションおよびサービスプリンシパルオブジェクトの詳細については、Microsoft ドキュメントを参照してください。

Tenable アプリのアクセス許可の更新

Microsoft によって行われた変更に伴い、クラウドサイバーエクスポージャーコネクタアプリのアクセス許可を更新するか、Tenable によって導入された新しいサービスをサポートする必要がある場合があります。クラウドサイバーエクスポージャーは読み取り専用アクセスでエージェントレスに動作するため、これらのアクセス許可は自動的に更新できません。すべての更新は、アクセス許可を更新することによって、Azure アカウント内で手動で行う必要があります。

1. 関連するテナントの Azure ポータルにログインします。
2. **[Microsoft Entra ID]** に移動します。
3. [管理] で、**[エンタープライズアプリケーション]** をクリックします。
4. **クラウドサイバーエクスポージャーコネクタ**アプリを検索して選択します。
5. **[セキュリティ]** > **[アクセス許可]** の順に移動します。
6. **[管理者の同意を付与]** をクリックします。
7. Microsoft アカウントのサインインページで、テナント Tenable が属する管理アカウントを選択します。

Azure アクセス許可

この表は、以下の各 クラウドサイバーエクスポージャー機能について、Azure を クラウドサイバーエクスポージャー に接続するために必要なアクセス許可 (Azure ロール) を示しています。

機能	説明	Azure ロール	注記
モニタリング (読み取り専用)	クラウド資産の可視性を確保します。これに	• `Reader` • `Key Vault Reader` • `Azure Kubernetes Service Cluster User Role` • `Azure Kubernetes Service RBAC Reader` • `Cognitive Services Data Reader`	• **Key Vault 閲覧者**ロールにより、

機能	説明	Azure ロール	注記
	はサブスクリプション使用状況、セキュリティ設定が含まれます。		Key Vault のメタデータとその証明書、キー、シークレットへの読み取りアクセスのみが許可されます。シークレットコンテンツやキーマテリアルなど機密性の高い

機能	説明	Azure ロール	注記
			めのアクセス権は付与されません。詳細については、関連する Microsoft のドキュメントを参照してください。 • 2 つの **Kubernetes** ロールは、AKS クラスタに関

機能	説明	Azure ロール	注記
			連付けられているクラウドアイデンティティとリソースの可視性とリスク評価を提供します。AKS クラスタの接続と要件の詳細 (1. IAM を完全に可視化

機能	説明	Azure ロール	注記
			可、2. ネットワークアクセス要件、など) については、Azure AKS クラスタの接続を参照してください。 • Tenable は **Cognitive Services データ閲覧者**を使用

機能	説明	Azure ロール	注記
			し、メタデータのみを読み取ることで AI Foundry リソースをリストします。

データリソーススキャン (データ保護)	機密データが含まれていないか、クラウドリソースをスキャンして分類します。詳細について	• `Storage Blob Data Reader` 組み込みロール
		• `Tenable Data Scanning` カスタムロール (以下のアクセス許可を使用)
		  • `Microsoft.Storage/storageAccounts/privateEndpointConnections/write`
		  • `Microsoft.Sql/servers/databases/write`
			詳細については、データ保護を参照してください。

機能	説明	Azure ロール	注記
	は、データ保護を参照してください。		
ワークロード保護	仮想マシンをスキャンして、脆弱性や設定ミスがないか確認します。	• `Disk Snapshot Contributor` 組み込みロール 組み込みロールの代わりに、次のアクセス許可を持つカスタムロールを付与できます。 • `Microsoft.Compute/snapshots/beginGetAccess/action` • `Microsoft.Compute/disks/beginGetAccess/action` • `Microsoft.Compute/snapshots/write` • `Microsoft.Compute/snapshots/endGetAccess/action` • `Microsoft.Compute/snapshots/delete` **BitLocker** を備えた Windows 仮想マシンまたは **DM-Crypt** (Ubuntu のみ) ディスク暗号化を備えた Linux 仮想マシンをスキャンするには、以下も付与します。 • `Key Vault Secrets User` 組み込みロール、または `Microsoft.KeyVault/vaults/secrets/getSecret/action` カスタムアクセス許可 Key Vault (KEK) のキーを使用して **BitLocker** 暗号化シークレッ	この機能を使用するには Standard または Enterprise のライセンスが必要です。Key Vault アクセス許可は、サブスクリプションごとまたは Key Vault ごとに付与できます。これらのアクセス許可を付与する手順については、ワークロードの接続を参

機能	説明	Azure ロール	注記
		トをスキャンするには、以下も付与します。 • `Key Vault Crypto User` 組み込みロールまたは `Microsoft.KeyVault/vaults/keys/unwrap/action` カスタムアクセス許可	照してください。
修正 (読み取りと書き込み)	Tenable が環境に変更を加えることを許可します。これにより、たとえば、ワンクリックで検出結果を自動的に修正できます (これらのアクセス許	`Owner`	

機能	説明	Azure ロール	注記
	可がなくても、OTP を経由してワンクリック修正が可能です)。		
ジャストインタイム (JIT) アクセス	ユーザーにクラウドアカウントへのアクセスを、あらかじめ決められた期間にわたり必要に応じて許可します。	`User Access Administrator`	

機能	説明	Azure ロール	注記
	この機能を使用するには、Microsoft Entra ID 統合もオンボードする必要があります。		
IaC - 問題をコードまでトレース		`Storage Blob Data Reader`	このアクセス許可は、正常に接続された後にアカウントを編集しないと有効にできません。

重要: デプロイメント スクリプトを実行すると、テナントでサービスプリンシパルが作成または更新されます。サービスプリンシパルは、ディレクトリ内の クラウド サイバーエクスポージャー コネクタアプリケーションを表し、割り当てられたアクセス許可とロールに基づいて、必要な Microsoft Entra ID および Azure リソースにアクセ

スできるようにします。
Microsoft Entra ID のアプリケーションおよびサービスプリンシパルオブジェクトの詳細については、Microsoft ドキュメントを参照してください。

Microsoft Entra ID テナントの接続

Microsoft Entra (旧 Azure Active Directory) テナントを Tenable One Cloud Exposure と接続して、アイデンティティ関連の可視化と分析を可能にします。この接続から、Microsoft クラウド環境全体のアイデンティティ、アクセス許可、アクセス関係に関する情報が得られます。

Microsoft Entra ID を接続して、アイデンティティの可視性、アイデンティティポスチャー管理、権限管理を有効にします。

Microsoft Entra ID 接続により、次の資産が可視化されます。

- ユーザーとグループ
- アプリケーションとアプリケーション登録
- 管理者ロール
- ロールの割り当てとアクセス関係
- Microsoft Entra ID を接続しても、Azure サブスクリプションまたはリソースへのアクセスは クラウド サイバーエクスポージャー に付与されません。Azure サブスクリプションと組織は別々に接続されています。
- このセクションで取り上げるのは、SSO 経由での クラウド サイバーエクスポージャー コンソールのログインを目的にしたアイデンティティプロバイダーの統合ではありません。コンソールアクセス用に SSO を設定するには、シングルサインオンを参照してください。
- この接続は CIEM で必須ですが、セキュリティポスチャーを最大化する上ですべてのライセンスタイプに推奨されます。

Microsoft Entra ID テナントの接続

注意: パブリッククラウドの場合、デプロイメントスクリプトによって、Tenable のマルチテナントアプリが Graph API からデータを取得できるようにするサービスプリンシパルが作成されます。中国のクラウドでは、データを取得するために手動でアプリを登録する必要があります。

Microsoft Entra ID テナントの接続方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** の順に移動し、**[統合を追加]** をクリックします。
2. **Microsoft Entra ID** を選択します。
3. 統合の**名前**を入力します。
4. Microsoft Entra ID **テナント ID** を入力します。
5. Azure クラウド**環境**を選択します。
    - **パブリック**: グローバルな Microsoft Entra ID クラウドでホストされているテナントに使用します。デプロイメントスクリプトによって、Tenable のマルチテナントアプリが Graph API からデータを取得できるようにするサービスプリンシパルが作成されます。選択したら、次の操作を実行します。
        1. **[テナントアクセスの検証]** をクリックします。アクセスを検証するため、Microsoft Entra ID テナントのサインインにリダイレクトされます。

            注意: テナント組織のメンバー、またはグローバル管理者 ロールを持つゲストユーザーである必要があります。

        2. 終了したら、このウィザードに戻り、手順を完了します。
    - **中国**: Azure China クラウド環境でホストされているテナントに使用します。この場合、アプリケーションを手動で登録する必要があります。デプロイメントスクリプトによって、アプリが Graph API からデータを取得できるようにするサービスプリンシパルが作成されます。選択したら、次の操作を実行します。
        1. 専用手動のアプリ登録 (中国のみ)を作成します。
        2. **アプリケーション (クライアント) ID** をコピーします。
        3. **クライアントシークレット**を入力します。

6. **[デプロイメント]** で、指定の PowerShell スクリプトを Azure CLI または Azure Cloud Shell にコピーし、サービスプリンシパルを作成して必要な Microsoft Graph アクセス許可を付与できるようにします。
7. **[終了]** をクリックします。

手動のアプリ登録 (中国のみ)

Azure China は別のクラウド環境で動作しているため、クライアントシークレットを使用して クラウド サイバーエクスポージャー で認証するために専用アプリケーションの登録が必要です。

China Cloud 認証用の専用アプリケーションを登録する方法

1. Entra ID テナント にログインします。
2. **[Microsoft Entra ID]** に移動し、**[+ New registration]** をクリックします。
3. アプリケーションの**名前**を入力します。たとえば クラウド サイバーエクスポージャー China です。
4. 他のすべての設定はそのままにして、**[Register]** をクリックします。
5. 新しく作成されたアプリで、**[API permissions]** に移動し、**[+ Add a permission]** をクリックします。

   > **注意:** デフォルトで設定されている `User.Read` アクセス許可は必要ありません。そのままにしておくことも、削除することもできます。

6. **[Microsoft Graph]** をクリックし、**[Application permissions]** をクリックします。
7. 以下のアクセス許可を検索して選択し、**[Add permissions]** をクリックします。
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `Policy.Read.All`
   - `PrivilegedAssignmentSchedule.Read.AzureADGroup`
   - `PrivilegedEligibilitySchedule.Read.AzureADGroup`
   - `RoleManagementPolicy.Read.AzureADGroup`
   - `RoleManagement.Read.All`
8. **[Certificates & Secrets]** をクリックし、[Client Secrets] で、**[+ New client secret]** をクリックします。

- シークレットの **[Client Secrets]** を入力します。
- シークレットの **[Expires]** を定義します。
- 完了したら、**[Add]** をクリックします。

> **注意:** 組織のポリシーに準拠した有効期限を選択します。シークレットの有効期限が切れたら、新しいシークレットを作成し、Tenable で値を編集して更新します。

9. シークレットの**値**をコピーします。この値は、クラウドサイバーエクスポージャーコンソールに入力する必要があります。
10. **[Overview]** をクリックし、**[Application (client) ID]** の値をコピーします。この値は、クラウドサイバーエクスポージャーコンソールに入力する必要があります。
11. ポータルの上部にある **[Settings]** をクリックし、[Directories + subscriptions] で、テナントの**ディレクトリ ID** を検索してコピーします。この値は、クラウドサイバーエクスポージャーコンソールに入力する必要があります。
12. クラウドサイバーエクスポージャーコンソールに移動し、Microsoft Entra ID テナントの接続手順を完了します。

次のステップ

Microsoft Entra ID テナントの接続後

- アイデンティティデータはクラウドサイバーエクスポージャーに表示され始めます。これには、ユーザー、グループ、ロール、アクセス関係が含まれます。
- アクセス許可分析やジャストインタイムアクセスの可視性など、アイデンティティに関連するリスクと分析情報が利用可能になります。

Azure のリソース、設定、ワークロードを可視化するには、Azure 組織またはサブスクリプションを接続します。

Azure 組織の接続

Azure 組織全体を接続することで、多数のアカウントがあるクラウド環境での統合プロセスを迅速化かつ自動化できます。これにより、以下が可能になります。

- Azure 組織で現在および将来のすべてのサブスクリプションを自動的に接続するため、サブスクリプションを個別に追加する必要はありません。
- Azure 環境全体で一貫した可視性とカバレッジを確保し、潜在的な盲点を排除します。

前提条件

始める前に

- 接続する Azure 組織 (ルート管理グループ) へアクセスできることを確認します。
- Azure API に対する認証のために Microsoft Entra ID のアプリケーションアイデンティティを作成または使用するアクセス許可があることを確認します。
- (パブリック環境のみ) テナントアクセスを検証するために、テナント組織のメンバー、またはグローバル管理者 ロールを持つゲストユーザーであることを確認します。

> **注意:** Tenable では、Microsoft Entra ID テナントの接続を設定してアイデンティティ関連の可視性とリスク分析を有効にすることを推奨しています。

組織の接続

Azure 組織の接続方法

1. Tenable One Cloud Exposure コンソールで、**[設定] > [統合]** の順に移動し、**[統合を追加]** をクリックします。
2. [統合ライブラリ] で、**[Azure 組織]** をクリックします。[Azure 組織] ウィザードが開きます。
3. **設定** ステップ (ステップ 1/2) で、次の操作を実行します。
    1. 統合の名前を入力します。
    2. 対象の Azure クラウド環境として、**[パブリック]** または **[中国]** を選択します。
        - **パブリック**: デプロイメントスクリプトにより、テナント内に、Tenable のマルチテナントアプリに関連付けられたサービスプリンシパルが作成されます。これは、Microsoft Graph API 経由でデータを抽出するために使用されます。
        - **中国**: ウィザードの [アプリケーション] セクションで説明されているように、Microsoft Entra ID に専用のアプリ登録を手動で作成する必要があります。デプロイメントスクリプトによ

り、アプリ登録に関連付けられたサービスプリンシパルが作成されます。これは、Microsoft Graph API 経由でデータを抽出するために使用されます。

3. **[Microsoft Entra ID]** で、既存の Microsoft Entra ID 統合を使用するかどうかを選択します。Microsoft Entra ID に接続して、アイデンティティを完全に可視化することをおすすめします。
    - 統合が存在しない場合は、ここで **[+ 追加]** をクリックして追加できます。
    - **[Microsoft Entra ID 統合を使用しない]** を選択している場合は、対象の Azure 組織に関連付けられている**テナント ID** を入力し、Tenable が適切な組織を識別できるようにします。
4. **[アクセス検証]** で **[検証]** をクリックします。Microsoft Entra ID テナントのサインインにリダイレクトされます。この手順により、統合を作成するユーザーがターゲットテナントのメンバーであるか、前提条件を持つゲストユーザーであることが確認されます。このステップは、パブリック環境でのみ必要です。
5. (中国環境のみ) **[アプリケーション]** で、手動のアプリ登録 (中国のみ) Microsoft Entra ID で専用のアプリ登録を作成し、説明に沿って対象の値をコピーして保存します。このステップは、前述の手順で既存の Entra ID 統合を使用しないことを選択した場合にのみ必要です。

    - アプリ登録を作成したら、アプリケーション (クライアント) ID とクライアントシークレットを入力します。
6. **[機能]** で、有効にする機能を選択します。この選択により、必要なアクセス許可が決定され、デプロイメントスクリプトが動的に更新されます。Tenable では、最も包括的なセキュリティカバレッジを提供するために、すべての機能を有効にすることを推奨しています。詳細については、Azure アクセス許可を参照してください。
7. **[デプロイメント]** で、次のいずれかのデプロイオプションを選択します。
    - **PowerShell** - スクリプトベースのデプロイメント。ウィザードに表示されるスクリプトをコピーし、Azure CLI または Azure Cloud Shell で実行して、必要なアクセス許可をクラウドサイバーエクスポージャーに付与します。
        - ロールを割り当てるには、Azure のルート管理グループ範囲に対する `Microsoft.Authorization/roleAssignments/*` アクセス許可が必要です。このアクセス許可は、`Owner` または `User Access Administrator` ロール

によって付与されます。

- このアクセス許可/ロールを持っていないが、Microsoft Entra ID で `Global Administrator` ロールを持っている場合は、アクセスを一時的に昇格して、すべての Azure サブスクリプションと管理グループに対する管理アクセス許可を取得することができます。

- **手動** - Azure ポータルを使用して、手動で設定します。カスタムロールを作成し、アクセス許可を割り当てる詳細な手順については、Azure 組織の手動デプロイを参照してください。

8. **[デプロイメント後]** で、プライマリドメイン名とサービスプリンシパル ID を入力します。

> **注意: 値を取得する方法** - PowerShell: スクリプトの出力から値をコピーして貼り付けます。 - 手動: これらの値を取得する方法については、Azure 組織の手動デプロイを参照してください。**共通の統合値** - これらの値は、組織およびそのすべてのメンバーサブスクリプションで同一である必要があります。 - 組織が接続されている場合、これらのフィールドは組織レベルでのみ更新できます。変更は、すべてのメンバーサブスクリプションに自動的に適用されます。

9. 完了したら、**[次へ]** をクリックします。

4. **範囲** ステップ (ステップ 2/2) で、次の操作を実行します。

1. (オプション) [コンパートメント構造を自動的に更新] を選択して、コンパートメントの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます。詳細については、アカウント階層とフォルダーを参照してください。

2. **[範囲]** で、オンボーディングするコンパートメントを選択します。

- **現在と将来のサブスクリプションをすべて同期する (推奨)**
- **特定のグループとサブスクリプションを含める**
- **特定のグループとサブスクリプションを除外する**

> **注意:**
> - フォルダー全体を含めるとグループ内の現在と将来のプロジェクトのすべてが含まれ、フォルダー全体を除外するとそれらのプロジェクトすべてが除外されます。
> - フォルダーで特定のプロジェクトを含めるとそのプロジェクトのみが含まれ、フォルダーで特定のプロジェクトを除外するとそのプロジェクトのみが除外されます。

> **注意:** オンボーディング中に、クラウドサイバーエクスポージャーは組織内のすべてのサブスクリプションを検出します。これにはキャンセルされたサブスクリプションや削除されたサブスクリプションが含まれますが、クラウドサイバーエクスポージャーはそれらを自動的にフィルタリングして除外し、オンボーディングを行いません。その結果として、検出されたサブスクリプションの数が、[アカウント] ページに表示される数よりも多くなることがあります。

5. **[終了]** をクリックします。

Azure 組織の手動デプロイ

Azure ポータルを使用して、Azure 組織を手動でデプロイします。これは、Azure 組織を追加する際にデプロイメントタイプとして**手動**を選択した場合の手順です。

1. 接続する組織の Azure ポータルにログインします。
2. (組織の接続際に、前述の手順で **Microsoft Entra ID 統合を使用しない**ことを選択した場合にのみ該当) 次の手順を実行します。
    - **サービスプリンシパル ID** を取得します。
        1. Azure CLI または Azure Shell を使用して次のコマンドを実行します。`az ad sp create --id 2608e51d-866a-43c9-99ab-3e44347ccb38 --query id`
        2. **サービスプリンシパル ID** をコピーして保存します。この値は、組織の接続際にクラウドサイバーエクスポージャーコンソールに入力する必要があります。
    - **プライマリドメイン名**を取得します。
        1. **[Microsoft Entra ID]** に移動します。
        2. **[Overview]** > **[Basic information]** に移動し、**プライマリドメイン**を見つけます。値をコピーして保存します。この値は、組織の接続際にクラウドサイバーエクスポージャーコンソールに入力する必要があります。
3. ルート管理グループ内の [Access control (IAM)] タブに移動します。
4. `Tenable Data Scanning` というカスタムロールを作成して次のアクセス許可を追加します。
    - `Microsoft.Storage/storageAccounts/privateEndpointConnections/write`
    - `Microsoft.Sql/servers/databases/write`

5. 使用する機能に関連するすべてのロールに対して、以下の手順を繰り返し、クラウドサイバーエクスポージャーコネクタアプリにロールを割り当てます。
    1. **[Add] > [Add role assignment]** の順にクリックします。
    2. リストからロールを検索して選択し、**[Next]** をクリックします
    3. **[+ Select members]** をクリックします。
    4. **クラウドサイバーエクスポージャーコネクタ** を検索して選択し、**[選択]** をクリックします。
    5. **[次へ]** をクリックし、**[レビューと割り当て]** をクリックして終了します。追加するすべてのロールに対してこのステップを繰り返します。
6. クラウドサイバーエクスポージャーコンソールに移動し、ウィザードのステップ 1 に次の値を入力します。
    - **プライマリドメイン名**
    - **サービスプリンシパル ID**
7. **[次へ]** をクリックし、ウィザードのステップ 2 を続行します。

次のステップ

Azure 組織が接続されると、組織に属するサブスクリプションが **[アカウント]** ページの [Azure] フォルダーに表示されます。ここから、サブスクリプションを管理したり、接続ステータスや有効になっている機能を表示したりできます。

クラウドサイバーエクスポージャーに Azure リソースデータが表示されるまでの所要時間は、環境の規模と複雑さによって異なります。

アイデンティティ関連の可視性、アクセス許可分析、ジャストインタイムのアクセス情報を有効にするには、Microsoft Entra ID テナントの接続を設定します (まだ設定していない場合)。

Azure サブスクリプションの接続

この手順を使用して個別のサブスクリプションを接続します。または、組織全体を接続することもできます。ウィザードに従って有効にする機能を選択し、Azure にロールの割り当てを追加して、Tenable One Cloud Exposure アプリケーションにサブスクリプションへのアクセス許可を付与します。

前提条件

始める前に

- 接続する Azure サブスクリプションへアクセスできることを確認します。
- Azure API に対する認証のために Microsoft Entra ID のアプリケーションアイデンティティを作成または使用するアクセス許可があることを確認します。
- (パブリック環境のみ) テナントアクセスを検証するために、テナント組織のメンバー、またはグローバル管理者 ロールを持つゲストユーザーであることを確認します。

> **注意:** Tenable では、Microsoft Entra ID テナントの接続を設定してアイデンティティ関連の可視性とリスク分析を有効にすることを推奨しています。

サブスクリプションの接続

Azure サブスクリプションの接続方法

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. [統合ライブラリ] で、**[Azure サブスクリプション]** を選択します。[Azure サブスクリプション] ウィザードが開きます。
3. ウィザードで次の操作を実行します。
    1. 関連するサブスクリプション ID を入力します。サブスクリプション ID は、Azure ポータルの **[Subscriptions]** で確認できます。
    2. 対象の Azure クラウド環境として、**[パブリック]** または **[中国]** を選択します。
        - **パブリック**: デプロイメント スクリプトにより、テナント内に、Tenable のマルチテナント アプリに関連付けられたサービスプリンシパルが作成されます。これは、Microsoft Graph API 経由でデータを抽出するために使用されます。
        - **中国**: このウィザードの [アプリケーション] セクションで説明されているように、Microsoft Entra ID に専用のアプリ登録を手動で作成する必要があります。デプロイメント スクリプ

トにより、アプリ登録に関連付けられたサービスプリンシパルが作成されます。これは、Microsoft Graph API 経由でデータを抽出するために使用されます。

3. **[Microsoft Entra ID]** で、既存の Entra ID 統合を使用するかどうかを選択します。統合が存在しない場合は、**[作成]** をクリックして作成できます。
    - **[Microsoft Entra ID 統合を使用しない]** を選択していない場合は、対象の Azure サブスクリプションに関連付けられているテナント ID を入力し、Tenable がそのサブスクリプションを持つ組織を識別できるようにします。
4. **[アクセスの検証]** で **[検証]** をクリックします。Microsoft Entra ID テナントのサインインにリダイレクトされます。この手順により、統合を作成するユーザーがターゲットテナントのメンバーであるか、前提条件を持つゲストユーザーであることが確認されます。このステップは、パブリック環境でのみ必要です。
5. (中国環境のみ) **[アプリケーション]** で、手動のアプリ登録 (中国のみ) Microsoft Entra ID で専用のアプリ登録を作成し、説明に沿って対象の値をコピーして保存します。このステップは、前述の手順で既存の Entra ID 統合を使用しないことを選択した場合にのみ必要です。
    - アプリ登録を作成したら、アプリケーション (クライアント) ID とクライアントシークレットを入力します。
6. **[機能]** で、有効にする機能を選択します。この選択により、必要なアクセス許可が決定され、デプロイメントスクリプトが動的に更新されます。Tenable では、最も包括的なセキュリティカバレッジを提供するために、すべての機能を有効にすることを推奨しています。詳細については、Azure アクセス許可を参照してください。
7. **[デプロイメント]** で、次のいずれかのデプロイオプションを選択します。
    - **PowerShell** - スクリプトベースのデプロイメント。ウィザードに表示されるスクリプトをコピーし、Azure CLI または Azure Cloud Shell で実行して、必要なアクセス許可をクラウドサイバーエクスポージャーに付与します。
        - ロールを割り当てるには、Azure のルート管理グループ範囲に対する `Microsoft.Authorization/roleAssignments/*` アクセス許可が必要です。このアクセス許可は、`Owner` または `User Access Administrator` ロールによって付与されます。

- このアクセス許可/ロールを持っていないが、Microsoft Entra ID で `Global Administrator` ロールを持っている場合は、アクセスを一時的に昇格して、すべての Azure サブスクリプションと管理グループに対する管理アクセス許可を取得することができます。

- **手動** - Azure ポータルを使用して、手動で設定します。カスタムロールを作成し、アクセス許可を割り当てる詳細な手順については、Azure サブスクリプションの手動デプロイを参照してください。

8. **[デプロイメント後]** で、プライマリドメイン名とサービスプリンシパル ID を入力します。

   値を取得する方法 - PowerShell: スクリプトの出力から値をコピーして貼り付けます。- 手動: これらの値を取得する方法については、Azure サブスクリプションの手動デプロイを参照してください。**共通の統合値** - これらの値は、組織およびそのすべてのメンバーサブスクリプションで同一である必要があります。- 関連するすべてのサブスクリプション統合を更新してこれらの値を変更し、環境全体でそれらが同一に保たれるようにするには、クラウドサイバーエクスポージャー のアクセス権限が必要です。- 組織が接続されている場合、これらのフィールドは組織レベルでのみ更新できます。変更は、すべてのメンバーサブスクリプションに自動的に適用されます。

9. 完了したら、**[終了]** をクリックします。

Azure サブスクリプションの手動デプロイ

Azure ポータルを使用して、Azure 組織を手動でデプロイします。これは、Azure サブスクリプションを接続する際にデプロイメントタイプとして**手動**を選択した場合の手順です。

1. 接続するサブスクリプションの Azure ポータルにログインします。
2. (組織の接続際に、前述の手順で **Microsoft Entra ID 統合を使用しない**ことを選択した場合にのみ該当) 次の手順を実行します。
   - **サービスプリンシパル ID** を取得します。
     - Azure CLI または Azure Shell を使用して次のコマンドを実行します。`az ad sp create --id 2608e51d-866a-43c9-99ab-3e44347ccb38 --query id`
     2. **サービスプリンシパル ID** をコピーして保存します。この値は、Azure サブスクリプション

を接続する際にクラウドサイバーエクスポージャーコンソールに入力する必要があります。

- **プライマリドメイン名**を取得します。
    1. **[Microsoft Entra ID]** に移動します。
    2. **[Overview]** > **[Basic information]** に移動し、**プライマリドメイン**を見つけます。値をコピーして保存します。この値は、Azure サブスクリプションを接続する際にクラウドサイバーエクスポージャーコンソールに入力する必要があります。

3. **Tenable データスキャン**という名前のカスタムロールを作成して、次のアクセス許可を追加します。
    - `Microsoft.Storage/storageAccounts/privateEndpointConnections/write`
    - `Microsoft.Sql/servers/databases/write`
4. 使用する機能に関連するすべてのロールに対して、以下の手順を繰り返し、クラウドサイバーエクスポージャーコネクタアプリにロールを割り当てます。
    1. [アクセス制御 (IAM)] に移動し、**[追加] -> [ロール割り当てを追加]** の順にクリックします
    2. ウィザードのリストからロールを検索して選択し、**[Next]** をクリックします。

        > **注意:** アクセス管理者 (JIT 用) ロールは [Privileged administrator roles] タブにあります。
        > ユーザーアクセス管理者 (JIT 用) ロールは [Privileged administrator roles] タブにあります。

    3. **[+Select members]** をクリックします。[クラウドサイバーエクスポージャー Connector] を検索して **[Select]** をクリックします。
    4. **クラウドサイバーエクスポージャーコネクタ**を検索して選択し、**[Select] **をクリックします。
    5. **[Next]** をクリックし、**[Review + assign]** をクリックして終了します。追加するすべてのロールに対してこのステップを繰り返します。
5. クラウドサイバーエクスポージャーコンソールに移動し、サブスクリプションの接続の [デプロイメント後] セクションを完了します。

次のステップ

- Azure リソースのデータはクラウドサイバーエクスポージャーに表示されるようになります。所要時間は、環境の規模と複雑さによって異なります。

- 以下のルールに従い、有効化された機能とアプリケーションの詳細を後から更新できます。
  - サブスクリプションがAzure組織の一部として接続されている場合、更新は組織レベルで行う必要があります。
  - サブスクリプションのみが接続されている場合、更新は関連するすべてのサブスクリプションに適用されるため、すべてのサブスクリプションを更新するためのアクセス許可が必要です。
- Microsoft Entra IDなしでAzureを接続した場合、Microsoft Entra IDが接続されるまでアイデンティティ関連の分析情報 (アクセス許可の分析やジャストインタイムアクセスなど) は利用できません。アイデンティティ関連の可視性、アクセス許可分析、ジャストインタイムのアクセス情報を有効にするには、Microsoft Entra IDテナントの接続を設定します。

AzureのFAQ (よくある質問) とトラブルシューティング

> **注意:** 一部の質問は、**Cloud Vulnerability Management**ライセンスには関係ありません。

この記事の内容

- Tenable One Cloud ExposureへのAzureの接続に関連する、よくある質問のリスト
- サブスクリプションのステータスとトラブルシューティングの情報

Azureサブスクリプションおよび組織のFAQ (よくある質問)

このセクションでは、Azureサブスクリプション/組織の接続に関連する、よくある質問を紹介します。

組織とMicrosoft Entra IDのペアリング

> Tenableに組織を接続する場合、Microsoft Entra IDとペアリングする必要がありますか?

回答: Tenableでは、Microsoft Entra IDテナントを組織とペアリングすることを推奨しています。これにより以下が可能になります。

- ユーザー、アクセス許可、最小権限の分析など、アイデンティティ関連の情報を可視化し、Microsoftクラウド環境全体のより包括的なリスク評価が可能になります。

- アイデンティティ、アクセス許可、アクセス関係を可視化できるため、リソースの可視化に加えて、セキュリティポスチャー管理も強化されます。
- 現在および将来のすべてのサブスクリプションを含め、クラウドリソースとアイデンティティの両方が包括的に可視化されます。

フォルダーまたはサブスクリプションを組織から除外する

> すでに接続した企業から、特定のフォルダーまたはサブスクリプションを除外するにはどうすればよいですか?

回答

1. コンソールで、**[設定]** > **[統合]** に移動します。
2. 組織の横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
3. **[次へ]** をクリックしてウィザード (スコープ) の最後のステップに移動します。
4. **[特定のフォルダーとサブスクリプションを除外する]** を選択してから、対象のフォルダーまたはサブスクリプションを選択します。
5. **[終了]** をクリックします。ご使用の環境内で Tenable が次回 データの同期と更新の頻度 ときに、コンソールから削除されます。

Microsoft Entra ID ユーザーの最小限のアクセス許可

> Microsoft Entra ID テナントを Tenable に追加する際に、Microsoft Entra ID ユーザーが Azure のクラウドサイバーエクスポージャー アプリを認証するために必要とする最小限のロールやアクセス許可は何ですか?

管理者の同意を付与するには、組織を代表して同意することを許可されたユーザーとして Azure にサインインする必要があります。これを実行するのに必要な特定のロールに関する詳細は、Microsoft のドキュメントを参照してください。

Key Vault 閲覧者ロールの割り当て

> Tenable に Key Vault Reader ロールの割り当てを付与する必要があるのはなぜですか? このロールはキーマテリアルへのアクセス権を Tenable に付与しますか?

Key Vault 閲覧者ロールにより、Key Vault のメタデータとその証明書、キー、シークレットへの読み取りアクセスのみが許可されます。シークレットコンテンツやキーマテリアルなど機密性の高い値を読み取るためのアクセス権は付与されません。詳細については、関連する Microsoft のドキュメントを参照してください。

組織の統合名の更新

Azure 組織の統合の名前を変更し、その名前をクラウドサイバーエクスポージャーに表示することができます。名前の変更は、特に複数の組織がある場合、識別に役立ちます。

名前を変更する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. 関連する統合の横にある三点リーダーメニューをクリックして、**[編集]** をクリックします。
3. ウィザードのステップ 2 に移動し、**[組織名]** フィールドを更新します。
4. **[次へ]** をクリックしてウィザードの最後のステップに移動し、**[更新]** をクリックします。

Microsoft Entra ID の FAQ (よくある質問)

このセクションでは、Microsoft Entra ID の接続に関連する、よくある質問を紹介します。

使用されていない PII の処理

> クラウドサイバーエクスポージャーは製品機能に直接使用されていない PII をどのように処理しますか? ログまたはデータベースに保存されますか?

クラウドサイバーエクスポージャーは、Microsoft Entra ID (および他のアイデンティティプロバイダー) の製品機能に必要な最低限のユーザー属性のセットのみを同期します。

Microsoft Entra ID の birthday など、同期されない属性は、クラウドサイバーエクスポージャーのデータベースやログで受信されたり、保存されたりすることはありません。したがって、使用されていない PII は保持されません。

Microsoft Entra ID からデフォルトで同期される属性の詳細なリストについては、Microsoft Entra ID の公式ドキュメントを参照してください。この情報は、Microsoft の更新に基づいて変更される可能性があります。

アプリの認証に必要なユーザーのアクセス許可

> 接続時にクラウドサイバーエクスポージャーアプリを認証するために必要な Microsoft Entra ID ユーザーの最低限のロール/アクセス許可は何ですか?

回答: Azure でクラウドサイバーエクスポージャーアプリに対して管理者の同意を付与するには、組織を代表して同意することを許可されたユーザーである必要があります。これを実行するのに必要な特定のロールに関する詳細は、Microsoft のドキュメントを参照してください。

パブリック版と中国の Microsoft Entra ID テナントの接続の違い

> Microsoft Entra ID のパブリックテナントと中国テナントで接続手順は異なりますか?

はい。次の手順を参照してください。

ジャストインタイム (JIT) アクセスのサポート

> Microsoft Entra ID 統合はジャストインタイム (JIT) アクセスをサポートしていますか?

はい。JIT 用 Microsoft Entra ID のオンボーディングを参照してください。

サブスクリプションのステータスとトラブルシューティング

クラウドサイバーエクスポージャーでは、各サブスクリプションの**ステータス**が表示されます。これはたとえば、Tenable がサブスクリプションに接続できるかどうかを示すもので、接続に関する潜在的な問題のトラブルシューティングに役立ちます。

ステータス	説明
Microsoft Entra	Microsoft Entra ID テナントが接続されていません。詳細については、Microsoft

ステータス	説明
ID が接続されていません	Entra ID テナントの接続を参照してください。
接続済み	クラウドサイバーエクスポージャーはサブスクリプションに正常に接続され、サブスクリプションが実行されています。
削除中...最大で 1 時間かかる場合があります	クラウドサイバーエクスポージャーでサブスクリプションを削除しましたが、そのプロセスはまだ完了していません。
接続に失敗しました	クラウドサイバーエクスポージャーはサブスクリプションに接続できませんでした。この原因は以下のいずれかである可能性があります。 • サブスクリプションが Azure で削除されたが、クラウドサイバーエクスポージャーコンソールからは削除されていない • サービスプリンシパルが認証されていない
アクセス許可がありません	リストされたロールの 1 つ以上が欠落しており、サブスクリプションに追加する必要があります。詳細については、Azure の必要なアクセス許可を参照してください。
サブスクリプションは有効化されていません	Azure でサブスクリプションの期限が切れている、期限が超過している、または警告を受けています。サブスクリプションの状態に関する詳細は、Azure の関連ドキュメントを参照してください。
サブスクリプションは削除の保留中です	サブスクリプションが Azure で削除済みまたは無効にされています。サブスクリプションの状態に関する詳細は、Azure の関連ドキュメントを参照してください。

Google

GCP の概要

Tenable One Cloud Exposure に GCP 環境を接続して、組織やプロジェクトに関連付けられているすべてのクラウドアイデンティティとリソース (アクセス許可、アカウントの使用状況、セキュリティ設定に関する情報を含む) の完全な可視性とリスク評価を取得します。Tenable は、GCP API からインベントリと設定データを収集します。

接続が完了すると、Tenable にプロジェクトステータスとトラブルシューティングが表示されます。これはたとえば、Tenable がプロジェクトに接続できるかどうかを示すもので、潜在的な問題のトラブルシューティングに役立ちます。

統合に関連するよくある質問のリストについては、GCP の FAQ を参照してください。

以下のいずれかを接続する手順を実行します。

- 1 つのプロジェクト
- 組織全体

GCP リソースの クラウドサイバーエクスポージャー アクティビティログデータを表示するには、ウィザードで監査ログ転送ステップを設定していることを確認してください。これは、組織レベルで、または個々のプロジェクトレベルで実行できます。クラウドイベントデータを参照してください。

アカウントを接続する前に、Pub/Sub の価格設定を十分に理解しておくことが大切です。公式の最新価格情報については、Pub/Sub の料金{target=_blank} を参照してください。たとえば、次のような点について考慮します。

- **メッセージスループットコスト**: 料金はパブリッシュおよび配信されたデータ量に基づいており、GB 単位で測定されます。
- **データ転送コスト**: Google Cloud のゾーンまたはリージョン間で転送されるデータは課金されます。
- **ストレージコスト**: メッセージ、スナップショット、または確認済みメッセージの保持には料金が発生します。

クラウドイベントデータ

GCP リソースの クラウドサイバーエクスポージャー クラウドイベント (アクティビティログデータ) を表示するには、ウィザードで監査ログ転送ステップを設定していることを確認してください。この手順では、Pub/Sub ト

ピックを作成し、そのPub/Subトピックを送信先とするシンクを作成してから、サブスクリプションを作成して、Tenableがトピックにパブリッシュされたメッセージを受信できるようにする必要があります。これは、組織レベルで、または個々のプロジェクトレベルで実行できます。

VPC Service Controlsの例外の追加

VPC Service Controlsを使用して、接続するプロジェクトや組織でGoogleが管理するサービスへのアクセスを制限する場合は、例外を定義して、お使いのリージョンのTenableIP アドレスへのAPIアクセスを許可する必要があります。これにより、Tenableサービスアカウントがプロジェクトにアクセスでき、統合を正常に続行できるようになります。

VPC Service Controlsでサービス境界を作成する方法についての詳細は、関連するGoogle Cloud のドキュメントを参照してください。

例外を追加する方法

> **重要:** クラウドサイバーエクスポージャーに接続するプロジェクトや組織に関連付けられたすべてのVPC境界について例外を追加する必要があります。

1. 組織レベルでの**VPC Service Controls**に移動します。
2. 関連するアクセスポリシーを選択します。
3. **[境界を編集]**をクリックして、関連するVPCサービス境界を編集します。
4. **イングレスポリシー**で**[アイデンティティ]**フィールド([APIクライアントのFROM属性]セクション)を更新し、Google Workspaceをクラウドサイバーエクスポージャーに追加したとき、および以下のTenableサービスアカウントを追加したときにTenable用に作成したサービスアカウントの両方が含まれるようにします。
    - `ermeticapp@sil-prd.iam.gserviceaccount.com`
5. **アクセスレベル**で**[アクセスレベルを選択します]**ドロップダウンをクリックし、アクセスレベルが設定されているかどうかを確認します。設定されている場合は、この後の手順で必要になるため、画面に表示される関連するアクセスレベルの情報を記録します。
6. **[保存]**をクリックします。

7. Tenable IP アドレスを関連するアクセスレベルに追加します。
    - 組織レベルで **Access Context Manager** に移動し、以前に特定したアクセスレベルを見つけます。
    - 関連するアクセスレベルを**編集**し、**[IP サブネットワーク]** で、許可が必要な Tenable IP アドレスを追加します。
    - **[保存]** をクリックします。
    - 他のアクセスレベルに対してこのプロセスを繰り返します。
8. (ワークロード保護) 以下を確実に行います。
    1. 検出中に使用されるタグリストとメタデータ呼び出しをカバーできるように、IP 制限なしで `artifactregistry.googleapis.com` のすべてのメソッドを許可します。
    2. クロスプロジェクトのスナップショット API 読み取り呼び出しに対して `compute.googleapis.com` のすべての操作を許可するエグレスルールを追加します。
    3. `compute.snapshots.setIamPolicy` のイングレスルールを追加します。これはスナップショットの IAM バインディングステップです。
    4. (オプション) `sil-prd` アカウントが関連するプロジェクトに属することを確認します。
    5. `ermeticapp@sil-prd.iam.gserviceaccount.com`と委任されたカスタマーサービスアカウントの両方が関連するプロジェクトに属することを確認します。

Google の必要なアクセス許可

Google Workspace と GCP プロジェクト/組織を Tenable One Cloud Exposure に接続するには、次のアクセス許可が必要です。

Google Workspace のアクセス許可

Tenable のサービスアカウントを作成する必要があります。Google Workspace の接続際、次の 2 つの方法のいずれかで、サービスアカウントにアクセス許可を付与できます。

- **カスタムロール**: ほとんどの組織に推奨されます。
- **ドメイン全体の委任**: ドメイン全体の委任による追加の IAM 機能を必要とする組織に推奨されます。

どちらの方法でも、JIT アクセスを含むすべてのコア製品機能がサポートされます。

必要なアクセス許可

ステップ	アクセス許可	説明
1. **サービスアカウントの作成**	`resourcemanager.projects.get`	プロジェクト名、ID、関連ラベルを含むプロジェクトメタデータへの読み取りアクセスを許可します。
	`serviceusage.services.enable` `serviceusage.services.list`	Google Cloud プロジェクト内でサービス (API) を表示および有効化できます。これは、クラウドサイバーエクスポージャーが依存する特定の API をアクティブ化する場合に必要です。
	`Service Account Token Creator`	Tenable に API と通信するためのアクセストークンの生成を許可します。このアクセス許可が必要な理由の詳細については、サービスアカウントトークン作成者ロールを参照してください。
2a.**カスタムロール (推奨)**	`Manage customer: Read customer` (すべて)	プライマリドメイン名を取得する読み取りアクセスを許可します。このプロパティは、GCP アクセス許可の評価に使用されます。

ステップ	アクセス許可	説明
	`Groups: Read`	グループへの読み取りアクセスを許可します。
	`Organization Units: Read`	組織単位への読み取りアクセスを許可します。
	`Users: Read`	ユーザーへの読み取りアクセスを許可します。
	(オプション) `Groups: Update`	ジャストインタイムアクセスを活用して、Google Workspace グループにユーザーを一時的に追加できます。

2b.**ドメイン全体の委任 (アドバンス)**	OAuth スコープ
	`cloud-identity.groups.readonly`
	`admin.directory.customer.readonly`
	`admin.directory.domain.readonly`
	`admin.directory.group.readonly`
	`admin.directory.orgunit.readonly`
	`admin.directory.rolemanagement.readonly`
	`admin.directory.user.readonly`
	`admin.reports.audit.readonly`
	`cloud-identity.inboundsso.readonly`
		組織単位、グループ、ユーザー、および管理者ロールや SSO プロファイルなどの高度な IAM 機能への読み取りアクセスを許可します。詳細については、ドメイン全体の委任による追加の IAM 機能を参照してください。

GCP プロジェクトと組織のアクセス許可

機能	GCP ロール	注記
モニタリング (読	• `App Engine Viewer`	GCP 組織の接続場合、こ

機能	GCP ロール	注記
み取り専用)	• Artifact Registry Reader • BigQuery Metadata Viewer • Cloud Asset Viewer • Compute Network Viewer • Compute Viewer • Kubernetes Engine Viewer • Organization Policy Viewer • Organization Viewer • Security Reviewer	れらのアクセス許可は組織レベルで付与される必要があります。 プロジェクトを含め、組織レベルで Organization Viewer を割り当てます。
データ保護	カスタムロール (以下のアクセス許可を使用) • bigquery.datasets.get • bigquery.datasets.getIamPolicy • bigquery.models.export • bigquery.models.getData • bigquery.models.getMetadata • bigquery.models.list • bigquery.routines.get • bigquery.routines.list • bigquery.tables.createSnapshot • bigquery.tables.export • bigquery.tables.get • bigquery.tables.getData • bigquery.tables.getIamPolicy • bigquery.tables.list	詳細については、データ保護を参照してください。

機能	GCP ロール	注記
	• bigquery.tables.replicateData • cloudsql.backupRuns.create • cloudsql.backupRuns.delete • cloudsql.backupRuns.get • cloudsql.backupRuns.list • cloudsql.instances.get • dataplex.projects.search • resourcemanager.projects.get • resourcemanager.projects.list • storage.folders.get • storage.folders.list • storage.managedFolders.get • storage.managedFolders.list • storage.objects.get • storage.objects.list	
ワークロード保護	カスタムロール (以下のアクセス許可を使用) • compute.disks.createSnapshot • compute.disks.use • compute.snapshots.create • compute.snapshots.delete • compute.snapshots.setIamPolicy • compute.snapshots.setLabels • compute.snapshots.useReadOnly	この機能を使用するには Standard または Enterprise のライセンスが必要です。詳細については、ワークロード保護を参照してください。

機能	GCP ロール	注記
修正 (読み取りと書き込み)	• BigQuery Data Owner • Security Admin • Service Account Admin	
ジャストインタイムアクセス (ユーザーアクセス管理者)	Security Admin	
監査ログ	Pub/Sub Subscriber	具体的な手順については、プロジェクトまたは組織の監査ログを設定する手順を参照してください。

単一プロジェクト接続用の組織レベルのカスタムロール

親組織を接続せずに個々の GCP プロジェクトを接続する場合も、クラウドサイバーエクスポージャーでは、以下のアクセス許可を持つカスタムロールを介して、組織レベルで付与される基本的なアクセス許可セットが必要です。

- `cloudasset.assets.searchAllIamPolicies`
- `compute.firewallPolicies.list`
- `iam.roles.get`
- `iam.roles.list`
- `iam.workforcePools.list`
- `iam.workforcePoolProviderKeys.list`
- `iam.workforcePoolProviders.list`
- `recommender.iamPolicyInsights.list`

- `recommender.iamPolicyRecommendations.list`
- `resourcemanager.folders.getIamPolicy`
- `resourcemanager.folders.list`
- `resourcemanager.organizations.get`
- `resourcemanager.organizations.getIamPolicy`
- `resourcemanager.projects.list`

このロールを作成する手順については組織レベルのアクセス許可を持つカスタムロールを作成するを、必要な理由についてはGCP のFAQを参照してください。

Google Workspace の接続

Google Workspace を Tenable One Cloud Exposure に接続することで、関連する資産の完全なインベントリが明らかになります。

- このセクションで取り上げるのは、SSO 経由でのクラウドサイバーエクスポージャーコンソールのログインを目的にしたIdP の統合ではありません。コンソールにアクセスする必要があるユーザーに対してSSO 経由のログインを有効にする方法の詳細については、シングルサインオンを参照してください。
- Tenable では、Workspace でローカルに定義されていない外部の Google グループとユーザーに関する情報も識別して表示します。
- Google Workspace を使用しない場合でも、同じ手順を使用してクラウドアイデンティティの接続を進める必要があります。コンソール全体で、Google Workspace という用語はクラウドアイデンティティと同じ意味で使用されます。

Tenable を使用して GCP 環境をモニタリングしている場合は、プロジェクト/組織を接続する前に Google Workspace に接続する必要があります。

この統合中に特定のアクセス許可を Tenable に付与する際に生じる可能性のある一般的な質問への回答については、GCP のFAQを参照してください。

前提条件

始める前に

- Google Cloud コンソールでプロジェクトの作成、サービスアカウントの作成、サービスアカウントの承認を行うユーザーに適切なアクセス許可を付与します。
- Google Workspace 管理コンソールでアクションを実行するユーザーに管理者権限を付与します。
- Tenable が使用するサービスアカウントをホストする Google Workspace ごとに専用のプロジェクトを作成します。
- Google Cloud コンソールで専用プロジェクトの請求を有効にします。手順については、請求の有効化に関する Google のドキュメントを参照してください。
- Terraform 固有
    - Terraform CLI v0.13 以上をインストールしていることを確認します。
    - `terraform init` が既存の設定と競合することなく、Google Cloud プロバイダー v7.11 以上をダウンロードしてインストールできることを確認します。

> **注意:** 専用プロジェクト
>
> - **API スロットリングの防止**。GCP は、プロジェクトレベルで API レート制限を適用します。他のサービスアカウントとプロジェクトを共有すると、制限に達してブロックされるリスクが高まります。
> - **経費の分離**。共有プロジェクトでは、請求データや使用状況データが不明瞭になり、Tenable サービスアカウントによって生成されたコストを正確に追跡することが難しくなります。

Workspace の追加

ここで説明されている手順に沿って、クラウドサイバーエクスポージャーに Google Workspace を追加します。このプロセスには以下が含まれます。

- GCP 組織で Tenable のサービスアカウントを作成する
- サービスアカウントにアクセス許可を割り当てる

> **注意:** 1 人のユーザーが両方のコンソールを使用する場合は、そのユーザーが必要なすべてのアクセス許可を持っていることを確認してください。

Google Workspace を追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Google Workspace]** をクリックします。Google Workspace ウィザードが開きます。
3. ウィザードで次の操作を実行します。
    1. 統合の名前を入力します。
    2. **顧客 ID** を取得するため、Google 管理コンソールを開き、**[Account]** > **[Account settings]** の順に移動し、**[Customer ID]** の値をコピーします。
    3. **[Deployment]** で、次のデプロイメントオプションのいずれかを選択して、専用プロジェクトで Tenable のサービスアカウントを作成します。
        - **Cloud Shell** - スクリプトベースのデプロイメント。ウィザードに表示されるスクリプトをコピーし、専用の GCP プロジェクトで実行して、必要なアクセス許可をクラウドサイバーエクスポージャーに付与します。
            1. Google Cloud コンソールで、Tenable の新しいプロジェクトを作成します。
            2. 新しく作成されたプロジェクト内で **Cloud Shell** をアクティブ化します。
            3. クラウドサイバーエクスポージャーウィザードに表示されるスクリプトをコピーし、Cloud Shell で実行します。
            4. スクリプトが正常に完了するまで待機し、出力から**サービスアカウントのメール**をコピーします。
        - **Terraform** - モジュールベースのデプロイメント。デプロイする前に、Terraform 固有の前提条件を参照してください。
            1. **管理プロジェクト ID** を入力します。これは、この統合のサービスアカウントをホストする前提条件の ID です。
            2. Google Cloud コンソールで、作成したプロジェクトに移動します。
            3. **[IAM & Admin]** > **[Labels]** に移動し、**[+ Add label]** をクリックし、クラウドサイバーエクスポージャーウィザードに表示されるキーと値のペアを追加します。
            4. クラウドサイバーエクスポージャーウィザードに表示されるモジュール呼び出しをコピーして Terraform 設定に追加し、`terraform apply` を実行します。このモ

ジュールはアイデンティティを作成し、環境に接続してスキャンするアクセス許可を Tenable に付与します。

- **手動** - Google Cloud コンソールを使用し、手動で設定します。詳細な手順については、Google Workspace の手動デプロイを参照してください。

> **警告:** 手動デプロイメントが完了したら、ウィザードに戻り、デプロイメント後の手順を完了します。

4. **[デプロイメント後の GCP 設定]** で、サービスアカウントのメールアドレスを入力します。前の手順で選択したデプロイメント方法に応じて、次のいずれかの方法でメールを取得します。
   - **Cloud Shell** - スクリプトが正常に完了するまで待機し、生成された出力からサービスアカウントのメールをコピーして貼り付けます。
   - **Terraform** - Terraform の出力からサービスアカウントのメール (`tenable_service_account_mail`) を取得します。
   - **手動** - Google Workspace の手動デプロイを参照してください。
5. **[デプロイメント後の Google Workspace 設定]** で、Google ワークスペースへのアクセス許可を Tenable に付与します。
   1. カスタムロールを使用してアクセス許可を付与する (推奨): クラウドサイバーエクスポージャー内のすべてのコア機能をサポートします。このオプションは、ほとんどの組織に推奨されます。
   2. ドメイン全体の委任を使用してアクセス許可を付与する (アドバンス): 高度な IAM 機能を必要とする組織に適しています。詳細については、ドメイン全体の委任による追加機能を参照してください。

   これらのアクセス許可が必要な理由についての詳細は、必要なアクセス許可を参照してください。
4. **[終了]** をクリックします。

カスタムロールを使用してアクセス許可を付与する (推奨)

カスタムロールを使用してアクセス許可を Google Workspace に付与します。

この方法は、ジャストインタイムアクセスを含むクラウドサイバーエクスポージャー内のすべてのコア機能をサポートします。このオプションは、ほとんどの組織に推奨されます。

1. Google Admin コンソールで、**[Account]** > **[Admin roles]** に移動し、**[Create new role]** をクリックします。
2. **[Name]** と **[Description]** を入力してから、**[CONTINUE]** をクリックします。
3. [Select Privileges] > [Admin API privileges] で、**「Required Permissions」** の [2a. Custom role (Recommended)] に一覧表示されている権限を選択します。

   > **注意:** オプションの [Groups] > [Update] 権限により、ジャストインタイムアクセスを活用して、Google Workspace グループにユーザーを一時的に追加できます。

4. **[CONTINUE]**、**[CREATE ROLE]** の順にクリックします。
5. 新しく作成されたロールの [管理者ロール] ページで、**[サービスアカウントへの割り当て]** をクリックします。
6. クラウドサイバーエクスポージャー ウィザードのステップ 2 で作成したサービスアカウントのメールアドレスを入力し、**[追加]** をクリックしてから、**[ロールを割り当て]** をクリックします。

ドメイン全体の委任を使用してアクセス許可を付与する (アドバンス)

ドメイン全体の委任を使用してアクセス許可を Google Workspace に付与します。

高度な IAM 機能を必要とする組織に適しています。また、ジャストインタイムアクセスもサポートしています。詳細については、ドメイン全体の委任による追加機能を参照してください。

1. Google Cloud コンソールで、クラウドサイバーエクスポージャー ウィザードのステップ 2 で作成したサービスアカウントに移動し、[Details] タブで、**[Advanced settings]** セクションをクリックして展開します。
2. **クライアント ID** をコピーしたら、**[Google Workspace 管理コンソールを表示]** をクリックします。
3. 管理コンソールで、**[セキュリティ]** > **[アクセスとデータコントロール]** > **[API コントロール]** に移動します。
4. **[ドメイン全体の委任の管理]** をクリックし、**[新規追加]** をクリックします。
5. 先ほどコピーした**クライアント ID** を貼り付けます。

6. 次の **OAuth スコープ**をコピーして貼り付けます。

```
https://www.googleapis.com/auth/cloud-identity.groups.readonly,
https://www.googleapis.com/auth/admin.directory.customer.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.orgunit.readonly,
https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
https://www.googleapis.com/auth/admin.reports.audit.readonly,
https://www.googleapis.com/auth/cloud-identity.inboundsso.readonly
```

7. (オプション) ジャストインタイム (JIT) を利用して、この組織の Google Workspace グループにユーザーを一時的に追加する場合は、OAuth スコープ `JIT OAuth scope` を追加します。
8. **[承認]** をクリックします。
9. クラウドサイバーエクスポージャー ウィザードで、関連する Google 管理コンソールユーザーの**ユーザーメール**を入力します。
    - ユーザーにはスーパー管理者ロールが割り当てられる必要があります。
    - このロールをユーザーに割り当てる、またはこのロールを持つユーザーを表示するには、**[アカウント]** > **[管理者ロール]** に移動し、**[スーパー管理者]** にカーソルを合わせて、**[管理者を割り当て]** または **[管理者を表示]** をクリックします。
    - Tenable に実際に付与されるアクセス許可は、以前に付与された OAuth スコープに制限されます。

Google Workspace の手動デプロイ

Google Cloud コンソールを使用して、Workspace を手動でデプロイします。これは、Workspace の追加際にデプロイメントタイプとして**手動**を選択した場合の手順です。

1. Google Cloud コンソールで、Tenable の新しいプロジェクトを作成するか、既存のプロジェクトに移動します (非推奨)。
2. 新しく作成されたプロジェクト内で、**[IAM & Admin]** > **[Roles]** の順に移動し、**[+Create Role]** をクリックします。
3. **[Title]**、**[Description]**、**[ID]** を入力します。

4. **[+ Add Permissions]** をクリックし、「Required Permissions」の **[Create Service Account]** にリストされているアクセス許可を追加します。
5. **[Create]** をクリックしてロールの作成を完了します。
6. **[Service Accounts]** タブをクリックしてから、**[+ Create service account]** をクリックします。
7. **[Service account name]**、**[ID]**、**[Description]** を入力してから、**[Create and continue]** をクリックします。
8. 作成したカスタムロールを選択して、**[Continue]**、**[Done]** をクリックします。
9. 新しく作成したサービスアカウントをクリックし、**[Principals with access]** タブに移動して、**[+ Grant access]** をクリックします。

   > **重要:** アクセス権を付与できない場合は、IAM ポリシーでプリンシパルとして Tenable を選択できないようにするドメイン制限制約を含む組織ポリシーが存在している可能性があります。これにより、Tenable では作成されたサービスアカウントのなりすましが防止されます。この場合は、Tenable を許可されたドメインとして追加するで説明されている手順に従います。

10. [New principals] フィールドに **ermeticapp@sil-prd.iam.gserviceaccount.com** を挿入し、[Service Account Token Creator] ロールを選択します。**[Save]** をクリックして終了します。
11. 作成したサービスアカウントのメールをコピーして保存します。[IAM & Admin] > [Service Accounts] の [Email] フィールドで確認できます。これは、クラウドサイバーエクスポージャーコンソールに入力する必要があります。
12. **[IAM & Admin]** > **[Labels]** に移動し、**[+ Add label]** をクリックし、クラウドサイバーエクスポージャーウィザードに表示されるキーと値のペアを追加します。
13. **[Save]** をクリックして終了します。
14. **[APIs & Services]** > **[Enabled APIs & services]** の順に移動し、**[Service Usage API]** を選択して、**[ENABLE]** をクリックします。
15. [クラウドサイバーエクスポージャーコンソール] ウィザードに戻り、デプロイメント後の GCP 設定を続行します。Workspace の追加を参照してください。

Tenable を許可されたドメインとして追加する

作成したサービスアカウントにアクセス権を付与できない場合は、IAM ポリシーでプリンシパルとしてクラウドサイバーエクスポージャーを選択できないようにするドメイン制限制約を含む組織ポリシーが存在している可能性があります。これにより、Tenable では作成されたサービスアカウントのなりすましが防止されます。この場合は、こちらで説明されている手順に従います。

許可されたドメインとして Tenable を追加する方法

1. Google Cloud コンソールのサービスアカウントが作成されたプロジェクト内で、**[IAM & Admin] > [Organization Policies]** の順に移動します。

   > **注意:** すべてのプロジェクトでワークロードスキャンに Tenable を使用する場合は、**最上位の組織ポリシーで**許可されたドメインとして Tenable を追加する必要があります。

2. フィルターで、**[Domain restricted sharing]** を検索して選択し、ポリシーをクリックして開きます。
3. **[ポリシーの管理]** をクリックします。
4. [ルール] セクションで、**[ルールを追加]** をクリックします。
5. [ポリシーの値] で、**[カスタム]** を選択します。
6. [ポリシーの種類] で、**[許可]** を選択します。
7. [カスタム値] で、次の値を入力します。`C00ndl9ht`

ドメイン全体の委任による追加の IAM 機能

ドメイン全体の委任でサービスアカウントにアクセス許可を付与する場合、以下の追加の IAM 機能がサポートされます。

> **注意:**
>
> - 組織に適したアクセス許可の付与方法を確認するには、Google Workspace のアクセス許可を参照してください。
> - ドメイン全体の委任の詳細については、ドメイン全体の委任 (アドバンス)を参照してください。

- **管理者ロール**。Google Workspace 管理者ロールを可視化します。管理者ロールは、管理者が管理できる設定、データ、管理機能など、組織の環境に対する管理者のアクセスと制御のレベルを定義します。ドメイン全体の委任により、以下を表示できます。

- 環境に存在する管理者ロール
- ロールの割り当て (管理アクセスと権限の配布に関するインサイトを提供します)

- **SSO プロファイル**。ワークスペースの SSO 設定を可視化し、MFA 関連の検出結果の精度を改善します。SSO プロファイルは、多要素認証 (MFA) がサードパーティのアイデンティティプロバイダー (IdP) を通じて適用されているかどうかを示します。
  - **「MFA なし」ラベルの挙動**。SSO プロファイルが検出されると、クラウドサイバーエクスポージャー は MFA がサードパーティの IdP レベルで適用されていると想定し、影響を受けるアイデンティティに [MFA なし] のラベルを割り当てません。
  - **検出結果の深刻度への影響**。この可視性がなければ、MFA の適用に関連する検出結果の深刻度の粒度が詳細に行われず、リスク評価に影響する可能性があります。
- **非アクティブなユーザー**。本当に非アクティブなユーザーと、API アクセスを通じてアクティブなユーザーを区別することで、非アクティブの検出結果の誤検出を減らします。ドメイン全体の委任を使用することで、以下を行うことができます。
  - クラウドサイバーエクスポージャー は、ユーザーが UI にログインしていなくても、**API のみのアクティビティ**を検出できます。
  - これにより、本当に非アクティブなプリンシパルのみにフラグが立てられ、非アクティビティ関連の検出結果の関連性と精度が向上します。

統合名の更新

Google Workspace 統合の名前を変更でき、その名前を クラウドサイバーエクスポージャー に表示することができます。特に複数のアイデンティティプロバイダーの統合がある場合、整理や識別に役立ちます。

名前を変更する方法

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[Google Workspace]** をクリックします。
2. 関連する統合の横にある三点リーダーをクリックして、**[編集]** をクリックします。
3. ウィザードのステップ 1 (ワークスペースの詳細) に移動し、**[名前]** フィールドを更新します。
4. **[次へ]** をクリックして最後のステップに移動し、**[更新]** をクリックします。

GCP 組織の接続

GCP 組織全体を接続することで、個別に追加しなくても、現在と将来のプロジェクトをすべて自動的にオンボーディングできます。

前提条件

始める前に

- Google Cloud コンソールでプロジェクトの作成、サービスアカウントの作成、サービスアカウントの承認、ログの有効化を行うユーザーに適切なアクセス許可を付与します。
- VPC Service Controls を使用して Google が管理するサービスへのアクセスを制限する場合、例外を定義して Tenable にネットワークアクセスを許可する必要があります。
- Tenable が使用するサービスアカウントをホストする Google 組織ごとに専用のプロジェクトを作成します。Tenable にプロジェクトを接続する際にすでにプロジェクトを作成している場合は、そのプロジェクトを使用します。
- Google Cloud コンソールで専用プロジェクトの請求を有効にします。手順については、請求の有効化に関する Google のドキュメントを参照してください。
- Terraform 固有
  - Terraform CLI v0.13 以上をインストールしていることを確認します。
  - `terraform init` が既存の設定と競合することなく、Google Cloud プロバイダー v7.11 以上をダウンロードしてインストールできることを確認します。

注意: 専用プロジェクト

- **API スロットリングの防止**。GCP は、プロジェクトレベルで API レート制限を適用します。他のサービスアカウントとプロジェクトを共有すると、制限に達してブロックされるリスクが高まります。
- **経費の分離**。共有プロジェクトでは、請求データや使用状況データが不明瞭になり、Tenable サービスアカウントによって生成されたコストを正確に追跡することが難しくなります。

組織の接続

GCP 組織を接続する方法

1. Tenable One Cloud Exposure コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. [統合ライブラリ] で、**[GCP 組織]** をクリックします。[GCP 組織] ウィザードが開きます。
3. **設定**ステップ (ステップ 1/2) で、次の操作を実行します。
    1. 統合の名前を入力します。
    2. 組織の ID を入力します。
    3. **[Google Workspace]** で、既存の Google Workspace 統合を使用するかどうかを選択します。統合が存在しない場合は、**[作成]** をクリックして作成できます。

        > **注意:** Tenable では、アイデンティティ関連の可視性と完全なリスク評価を可能にするために、組織の Google Workspace を使用することを推奨しています。これにより以下が可能になります。
        > - ユーザー、アクセス許可、最小権限の分析など、アイデンティティ関連の情報を可視化し、GCP クラウド環境全体のより包括的なリスク評価が可能になります。
        > - アイデンティティ、アクセス許可、アクセス関係を可視化できるため、リソースの可視化に加えて、セキュリティポスチャー管理も強化されます。

    4. **[機能]** で、有効にする機能を選択します。この選択により、必要なアクセス許可が決定され、デプロイメントスクリプトが動的に更新されます。Tenable では、最も包括的なセキュリティカバレッジを提供するために、すべての機能を有効にすることを推奨しています。詳細については、Google の必要なアクセス許可を参照してください。
    5. **[デプロイメント]** で、次のいずれかのデプロイオプションを選択します。
        - **Cloud Shell** - スクリプトベースのデプロイメント。
            1. **管理プロジェクト ID** を入力します。これは、この統合のサービスアカウントをホストする前提条件の ID です。
            2. クラウドサイバーエクスポージャー ウィザードに表示されるスクリプトをコピーし、スクリプトの内容を含むファイルを作成します。次に、それを Cloud Shell で実行し、クラウドサイバーエクスポージャーに必要なアクセス許可を付与します。
        - **Terraform** - モジュールベースのデプロイメント。デプロイする前に、Terraform 固有の前提条件を参照してください。

1. **管理プロジェクト ID** を入力します。これは、この統合のサービスアカウントをホストする前提条件の ID です。
2. Google Cloud コンソールで、作成したプロジェクトに移動します。
3. **[IAM & Admin]** > **[Labels]** に移動し、**[+ Add label]** をクリックし、クラウド サイバーエクスポージャー ウィザードに表示されるキーと値のペアを追加します。
4. クラウド サイバーエクスポージャー ウィザードに表示されるモジュール呼び出しをコピーして Terraform 設定に追加し、`terraform apply` を実行します。このモジュールはアイデンティティを作成し、環境に接続してスキャンするアクセス許可を Tenable に付与します。

- **手動** - Google Cloud コンソールを使用し、手動で設定します。詳細な手順については、GCP 組織の手動デプロイを参照してください。

> **警告:** 手動デプロイメントが完了したらウィザードに戻り、デプロイメント後の手順と、ステップ 2 の範囲と階層を完了します。

6. **[デプロイメント後]** に、次の値を入力します。
   - **値を取得する方法**
     - Cloud Shell: スクリプトの出力から値をコピーして貼り付けます。
     - Terraform: Terraform の出力から値を取得します。
     - 手動: これらの値を取得する方法については、GCP 組織の手動デプロイを参照してください。
   - **共通の統合値**
     - これらの値は、組織およびそのすべてのメンバープロジェクトで同一である必要があります。
     - 組織が接続されている場合、これらのフィールドは組織レベルでのみ更新できます。変更は、すべてのメンバープロジェクトに自動的に適用されます。
   - **サービスアカウントのメール**
   - **Pub/Sub サブスクリプション名**
7. 完了したら、**[次へ]** をクリックします。

4. **範囲**ステップ (ステップ 2/2) で、次の操作を実行します。
    1. (オプション) [コンパートメント構造を自動的に更新] を選択して、コンパートメントの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます。詳細については、アカウント階層とフォルダーを参照してください。
    2. **[範囲]** で、オンボーディングするコンパートメントを選択します。
        - **現在と将来のプロジェクトをすべて同期する (推奨)**
        - **特定のフォルダーとプロジェクトを含める**
        - **特定のフォルダーとプロジェクトを除外する**

        > **注意:**
        > - フォルダー全体を含めるとグループ内の現在と将来のプロジェクトがすべて含まれ、フォルダー全体を除外するとすべて除外されます。
        > - フォルダーで特定のプロジェクトを含めるとそのプロジェクトのみが含まれ、フォルダーで特定のプロジェクトを除外するとそのプロジェクトのみが除外されます。
5. **[終了]** をクリックします。

> **注意:** GCP のアクセス変更のプロパゲーションにより、アクセス許可の変更がクラウド環境に適用されるまでに時間がかかる場合があります。[終了] をクリックしようとしたときに、「サービスアカウントのアクセス許可がないか、設定ミスです」というエラーが表示された場合は、数分待ってから再試行してください。

次の手順

組織が正常に追加された後

- 組織は、**[統合] > [GCP 組織]** ページで確認できます。
- 組織に属するアカウントは、**[アカウント] > [GCP]** ページで確認できます。ここからアカウントやプロジェクトの詳細を表示して、どの機能が有効になっているか、必要なアクセス許可が付与されているか、などを確認できます。

プロジェクトリソースに関するデータがクラウドサイバーエクスポージャーに表示されるようになります。すべてのデータが表示されるまでにかかる時間は、クラウド環境の規模によって異なります。

GCP 組織の手動デプロイ

注意: 手動デプロイメントが完了したら、組織の接続デプロイメント後の手順と、ステップ 2 の範囲と階層を完了します。

スクリプトベースのデプロイメントの代わりに、Google Cloud コンソールから GCP 組織を手動でデプロイすることもできます。これは、GCP 組織を接続する際にデプロイメントタイプとして**手動**を選択した場合の手順です。

1. Tenable のサービスアカウントを作成する
2. 組織レベルでサービスアカウントを承認する
3. 監査ログを設定する

Tenable のサービスアカウントを作成する

Tenable が組織へのアクセスとモニタリングに使用する専用の GCP プロジェクトとサービスアカウントを作成します。

1. Google Cloud コンソールで、作成した前提条件に移動します。
2. **[IAM & Admin]** > **[Roles]** に移動し、**[+ Create custom role]** をクリックします。
3. タイトル、説明、ID を入力します。
4. **[+ Add permissions]** をクリックし、「Required Permissions」の **[Create Service Account]** にリストされているアクセス許可を追加します。
5. **[Create]** をクリックしてロールの作成を完了します。
6. **[IAM & Admin]** > **[Service Accounts]** に移動し、**[+ Create service account]** をクリックします。
7. **[Service account name]**、**[ID]**、**[Description]** を入力します。
8. 生成されたサービスアカウントのメールをコピーして保存します。この値は、クラウドサイバーエクスポージャーに組織の接続ときに、ウィザードの [デプロイメント後] セクションに入力する必要があります。
9. **[Create and continue]** をクリックします。
10. 作成したカスタムロールを選択して、**[Continue]**、**[Done]** をクリックします。

11. 新しく作成したサービスアカウントを選択し、**[Principals with access]** タブ、**[Grant access]** の順にクリックします。

    > **重要:** アクセス権を付与できない場合は、IAM ポリシーでプリンシパルとして Tenable を選択できないようにするドメイン制限制約を含む組織ポリシーが存在している可能性があります。これにより、Tenable では作成されたサービスアカウントのなりすましが防止されます。この場合は、Tenable を許可されたドメインとして追加するで説明されている手順に従います。

12. [Add principals] セクションで、**ermeticapp@sil-prd.iam.gserviceaccount.com** を [New principals] フィールドに入力します。
13. [Assign roles] セクションで、**[Service Account Token Creator]** ロールを選択し、**[Save]** をクリックして終了します。
14. **[IAM & Admin]** > **[Labels]** に移動し、**[+ Add label]** をクリックし、クラウドサイバーエクスポージャーウィザードに表示されるキーと値のペアを追加します。
    - **キー**: `ermetic-external-id`
    - **値**: クラウドサイバーエクスポージャー ウィザードの [デプロイメント] セクションに表示
15. **[Save]** をクリックしてサービスアカウントの作成を完了します。

組織レベルでサービスアカウントを承認する

組織のスキャンとモニタリングを行うために Tenable が必要とするアクセス許可をサービスアカウントに付与します。

1. Google Cloud コンソールで、画面の左上にあるプロジェクトピッカーを使用して、Tenable に接続する組織を選択します。
2. **[IAM & Admin]** > **[IAM]** に移動し、**[Grant access]** をクリックします。
3. [Add principals] セクションで、先ほど保存したサービスアカウントのメールを [New principals] フィールドに入力します。
4. [Assign roles] セクションで、必要な機能に応じて関連するロールを選択します。
5. **[Save]** をクリックして終了します。

監査ログを設定する

Pub/Sub トピック、サブスクリプション、ログシンクを設定して、GCP 監査ログを Tenable にストリーミングします。

警告: Pub/Sub トピックとサブスクリプションはプロジェクトレベルで作成されますが、ログシンクは組織レベルで作成する必要があります。

1. Google Cloud コンソールで、プロジェクトピッカーを使用して関連するプロジェクトを選択し、次の手順に従って Pub/Sub トピックを作成します。
    1. **[Pub/Sub] > [Topics]** に移動し、**[+ Create topic]** をクリックします。
    2. [Topic ID] フィールドに `tenable-audit-logs` を入力します。
    3. **[Add a default subscription]** のチェックを外します。
    4. **[Enable message retention]** を選択し、期間を 1 日以上に設定します。
    5. **[Create]** をクリックします。
2. 次の手順に従って Pub/Sub サブスクリプションを作成します。
    1. **[Pub/Sub] > [Subscriptions]** に移動し、**[+ Create subscription]** をクリックします。
    2. [Subscription ID] フィールドに `tenable-audit-logs-sub` を入力します。
    3. 先ほど作成したトピックを選択します。
    4. [Delivery type] セクションで、**[Pull]** を選択します。
    5. [Message retention duration] セクションで、期間を 1 日以上に設定します。
    6. [Retry policy] セクションで、**[Retry after exponential backoff delay]** を選択し、デフォルト値のままにします。
    7. [Expiration period] セクションで、**[Never expire]** を選択します。
    8. **[Create]** をクリックします。
    9. 新しく作成されたサブスクリプションの [Permissions] タブで、**[Add principal]** をクリックします。
    10. [Add principals] セクションで、先ほど保存したサービスアカウントのメールを [New principals] フィールドに入力します。
    11. [Assign roles] セクションで、**[Pub/Sub Subscriber]** ロールを選択し、**[Save]** をクリックして終了します。

12. Pub/Sub サブスクリプション名をコピーして保存します。この値は、クラウドサイバーエクスポージャーに組織の接続ときに、ウィザードの [デプロイメント後] セクションに入力する必要があります。

3. 次の手順に従って組織レベルのログシンクを作成します。

    1. プロジェクトピッカーで関連する組織を選択し、**[Logging] > [Configure] > [Log router]** の順に移動します。
    2. **[Create sink]** をクリックします。
    3. [Sink name] フィールドに `tenable-audit-logs` を入力し、**[Next]** をクリックします。
    4. シンクサービスの場合は、**[Cloud Pub/Sub topic]**、**[Use a Cloud Pub/Sub topic in a project]** の順に選択します。
    5. [Sink destination] フィールドで、`[PROJECT_ID]` と `[TOPIC_ID]` を関連する ID と置き換え、**[Next]** をクリックします。
    6. [Include logs ingested by this organization and all child resources] を選択し、包含フィルターに以下を貼り付けます。

    ```
    LOG_ID(cloudaudit.googleapis.com/activity) OR
    LOG_ID(cloudaudit.googleapis.com/data_access) OR
    LOG_ID(cloudaudit.googleapis.com/policy)
    ```

    7. **[Next]** をクリックします。
    8. **[+ Add exclusion]** をクリックします。
    9. [Exclusion filter name] フィールドで、`exclude-k8s-internal` を入力し、以下を除外フィルターに貼り付けます。

    ```
    protoPayload.authenticationInfo.principalEmail-:* OR
    protoPayload.authenticationInfo.principalEmail=~"^system:" OR
    protoPayload.authenticationInfo.principalEmail=~"@container-engine-
    robot.iam.gserviceaccount.com$" OR
    protoPayload.authenticationInfo.principalEmail=~"@security-center-
    api.iam.gserviceaccount.com$"
    ```

    10. **[Create sink]** をクリックします。

> **重要:** GCP 組織の管理者またはスーパー管理者であっても、Google Cloud ではデフォルトでログのアクセス許可が分離されています。シンクを作成する際に **[Permission `logging.sinks.create` denied on resource]** というエラーが表示された場合は、組織レベルで [Logging Admin] または [Logs Configuration Writer] ロールをユーザーアカウントに明示的に付与する必要があります。

4. 組織レベルで、**Pub/Sub パブリッシャ**ロールをサービスアカウントに割り当てます。
    1. **[IAM & Admin] > [IAM]** に移動します。
    2. サービスアカウントを見つけて、**[Edit principal]** をクリックします。
    3. **[+ Add another role]** をクリックします。
    4. **[Pub/Sub Publisher]** を選択します。
    5. **[Save]** をクリックします。

GCP プロジェクトの接続

個別の GCP プロジェクトを Tenable に接続して、そのクラウドリソースとセキュリティポスチャーをモニタリングします。組織内のすべてのプロジェクトを一度に接続するには、GCP 組織の接続を参照してください。

前提条件

始める前に

- Google Cloud コンソールでプロジェクトの作成、サービスアカウントの作成、サービスアカウントの承認、ログの有効化を行うユーザーに適切なアクセス許可を付与します。
- VPC Service Controls を使用して Google が管理するサービスへのアクセスを制限する場合、例外を定義して Tenable にネットワークアクセスを許可する必要があります。
- 組織に IAM ポリシーでプリンシパルとしての Tenable をブロックするドメイン制限ポリシーがないことを確認してください。このポリシーがある場合は、Tenable を許可されたドメインとして追加します。
- Tenable が使用するサービスアカウントをホストする Google 組織 (そのすべてのプロジェクトを含む) ごとに専用のプロジェクトを作成します。
- Google Cloud コンソールで専用プロジェクトの請求を有効にします。手順については、請求の有効化に関する Google のドキュメントを参照してください。

注意: 専用プロジェクト

- **API スロットリングの防止**。GCP は、プロジェクトレベルで API レート制限を適用します。他のサービスアカウントとプロジェクトを共有すると、制限に達してブロックされるリスクが高まります。
- **経費の分離**。共有プロジェクトでは、請求データや使用状況データが不明瞭になり、Tenable サービスアカウントによって生成されたコストを正確に追跡することが難しくなります。

プロジェクトの接続

注意: 設定に応じて、共有フィールドの管理方法は異なります。

- **親組織の統合が Tenable に存在する場合:** 一部のセクションには、組織レベルで管理されるフィールドが含まれます。これらのフィールドを変更するには、組織の統合を編集します。
- **親組織の統合が Tenable に存在しない場合:** 一部のセクションには、組織のすべてのプロジェクト統合で共有されるフィールドが含まれます。これらのフィールドは、統合の編集時にのみ変更できます。

GCP プロジェクトを接続する方法

1. Tenable One Cloud Exposure コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[GCP プロジェクト]** をクリックします。[GCP プロジェクト] ウィザードが開きます。
3. ウィザードで次の操作を実行します。
    1. 接続する GCP プロジェクトのプロジェクト ID を入力します。
    2. 組織 ID を入力します。クラウド サイバーエクスポージャー は現在、組織に含まれないプロジェクトをサポートしていません。
    3. **[Google Workspace]** で、既存の Google Workspace 統合を使用するかどうかを選択します。統合が存在しない場合は、**[作成]** をクリックして作成できます。

        注意: Tenable では、アイデンティティ関連の可視性と完全なリスク評価を可能にするために、組織の Google Workspace を使用することを推奨しています。これにより以下が可能になります。
        - ユーザー、アクセス許可、最小権限の分析など、アイデンティティ関連の情報を可視化し、GCP クラウド環境全体のより包括的なリスク評価が可能になります。

- アイデンティティ、アクセス許可、アクセス関係を可視化できるため、リソースの可視化に加えて、セキュリティポスチャー管理も強化されます。

4. **[機能]** で、有効にする機能を選択します。この選択により、必要なアクセス許可が決定され、デプロイメントスクリプトが動的に更新されます。Tenable では、最も包括的なセキュリティカバレッジを提供するために、すべての機能を有効にすることを推奨しています。詳細については、Google の必要なアクセス許可を参照してください。
5. **[デプロイメント]** で、次のいずれかのデプロイオプションを選択します。
   - **Cloud Shell** - スクリプトベースのデプロイメント。
     1. **管理プロジェクト ID** を入力します。これは、この統合のサービスアカウントをホストする前提条件の ID です。
     2. クラウドサイバーエクスポージャー ウィザードに表示されるスクリプトをコピーし、スクリプトの内容を含むファイルを作成します。次に、それを Cloud Shell で実行し、クラウドサイバーエクスポージャーに必要なアクセス許可を付与します。
   - **手動** - Google Cloud コンソールを使用し、手動で設定します。詳細な手順については、GCP プロジェクトの手動デプロイを参照してください。

     警告: 手動デプロイメントが完了したら、ウィザードに戻り、デプロイメント後の手順を完了します。
6. **[デプロイメント後]** に、次の値を入力します。

注意:
- **値を取得する方法**
  - Cloud Shell: スクリプトの出力から値をコピーして貼り付けます。
  - 手動: これらの値を取得する方法については、GCP プロジェクトの手動デプロイを参照してください。
- **共通の統合値**
  - これらの値は、同一組織内のすべてのプロジェクトで同じである必要があります。
  - 親組織の統合が存在する場合、これらのフィールドは組織レベルで管理されます。変更は、すべてのメンバープロジェクトに自動的に適用されます。

- **サービスアカウントのメール**
- **Pub/Sub サブスクリプション名**

4. **[終了]** をクリックします。

> **注意:** GCP のアクセス変更のプロパゲーション により、アクセス許可の変更がクラウド環境に適用されるまでに時間がかかる場合があります。[終了] をクリックしようとしたときに「組織が存在しません」というエラーが表示された場合は、数分待ってから再試行してください。

次の手順

プロジェクトが正常に追加された後

- プロジェクトは、**[アカウント] > [GCP]** ページで確認できます。ここからアカウントやプロジェクトの詳細を表示して、どの機能が有効になっているか、必要なアクセス許可が付与されているか、などを確認できます。

プロジェクトリソースに関するデータがクラウドサイバーエクスポージャーに表示されるようになります。すべてのデータが表示されるまでにかかる時間は、クラウド環境の規模によって異なります。

GCP プロジェクトの手動デプロイ

> **注意:** 手動デプロイメントが完了したら、プロジェクトの接続 デプロイメント後の手順を完了します。

スクリプトベースのデプロイメントの代わりに、Google Cloud コンソールから GCP プロジェクトを手動でデプロイすることもできます。これは、GCP プロジェクトを接続する際にデプロイメントタイプとして**手動**を選択した場合の手順です。

1. Tenable のサービスアカウントを作成する
2. 組織レベルでサービスアカウントを承認する
3. プロジェクトレベルでサービスアカウントを承認する
4. 監査ログを設定する
5. 組織レベルのアクセス許可を持つカスタムロールを作成する

Tenable のサービスアカウントを作成する

Tenable がプロジェクトへのアクセスとモニタリングに使用する専用の GCP プロジェクトとサービスアカウントを作成します。

1. Google Cloud コンソールで、作成した前提条件に移動します。
2. **[IAM & Admin]** > **[Roles]** に移動し、**[+ Create custom role]** をクリックします。
3. タイトル、説明、ID を入力します。
4. **[+ Add permissions]** をクリックし、「Required Permissions」の **[Create Service Account]** にリストされているアクセス許可を追加します。
5. **[Create]** をクリックしてロールの作成を完了します。
6. **[IAM & Admin]** > **[Service Accounts]** に移動し、**[+ Create service account]** をクリックします。
7. **[Service account name]**、**[ID]**、**[Description]** を入力します。
8. 生成されたサービスアカウントのメールをコピーして保存します。この値は、クラウドサイバーエクスポージャーに組織の接続ときに、ウィザードの [デプロイメント後] セクションに入力する必要があります。
9. **[Create and continue]** をクリックします。
10. 作成したカスタムロールを選択して、**[Continue]**、**[Done]** をクリックします。
11. 新しく作成したサービスアカウントを選択し、**[Principals with access]** タブ、**[Grant access]** の順にクリックします。

    > **重要:** アクセス権を付与できない場合は、IAM ポリシーでプリンシパルとして Tenable を選択できないようにするドメイン制限制約を含む組織ポリシーが存在している可能性があります。これにより、Tenable では作成されたサービスアカウントのなりすましが防止されます。この場合は、Tenable を許可されたドメインとして追加するで説明されている手順に従います。

12. [Add principals] セクションで、**ermeticapp@sil-prd.iam.gserviceaccount.com** を [New principals] フィールドに入力します。
13. [Assign roles] セクションで、**[Service Account Token Creator]** ロールを選択し、**[Save]** をクリックして終了します。
14. **[IAM & Admin]** > **[Labels]** に移動し、**[+ Add label]** をクリックし、クラウドサイバーエクスポージャーウィザードに表示されるキーと値のペアを追加します。

- **ラベルキー**: `ermetic-external-id`
- **値**: クラウド サイバーエクスポージャー ウィザードの [デプロイメント] セクションに表示

15. **[Save]** をクリックしてサービスアカウントの作成を完了します。

組織レベルでサービスアカウントを承認する

GCP 環境の評価とモニタリングを行うために Tenable が必要とする組織レベルのアクセス許可をサービスアカウントに付与します。

この手順におけるロールバインディングは、Tenable のベストプラクティスの推奨事項に従って、組織レベルで付与されます。組織全体の接続を予定していない場合 (たとえば試用版の一部である場合)、Tenable は、代わりにプロジェクトレベルでこのロールバインディングの付与をサポートします。その場合も、カスタムロールを通じて組織レベルの基本的なアクセス許可セットを付与し、統合を完了するために サポートへの問い合わせ。する必要があります。詳細については、GCP の FAQ を参照してください。

1. Google Cloud コンソールで、画面の左上にあるプロジェクトピッカーを使用して、Tenable に接続する組織を選択します。
2. **[IAM & Admin] > [IAM]** に移動し、**[Grant access]** をクリックします。
3. [Add principals] セクションで、先ほど保存したサービスアカウントのメールを [New principals] フィールドに入力します。
4. [Assign roles] セクションで、次のロールを追加します。
    - `Cloud Asset Viewer`
    - `Security Reviewer`
    - `Organization Policy Viewer`
    - `Organization Viewer`
5. **[Save]** をクリックして終了します。

プロジェクトレベルでサービスアカウントを承認する

プロジェクトのスキャンとモニタリングを行うために Tenable が必要とするプロジェクトレベルのアクセス許可をサービスアカウントに付与します。

1. Google Cloud コンソールで、画面の左上にあるプロジェクトピッカーを使用して、関連するプロジェクトを選択します。
2. **[IAM & Admin] > [IAM]** に移動し、**[Grant access]** をクリックします。
3. [Add principals] セクションで、先ほど保存したサービスアカウントのメールを [New principals] フィールドに入力します。
4. [Assign roles] セクションで、必要な機能に応じて関連するロールを選択します。
5. **[Save]** をクリックして終了します。

> **注意:** [機能] セクションでワークロード保護を有効にした場合は、ワークロード保護のアクセス許可を付与する追加の手順を行います。詳細については、関連するワークロード保護のドキュメントを参照してください。

監査ログを設定する

Pub/Sub トピック、ログシンク、サブスクリプションを設定して、GCP 監査ログを Tenable にストリーミングします。

1. Google Cloud コンソールで、プロジェクトピッカーを使用して関連するプロジェクトを選択し、次の手順に従って Pub/Sub トピックを作成します。
    1. **[Pub/Sub] > [Topics]** に移動し、**[+ Create topic]** をクリックします。
    2. [Topic ID] フィールドに `tenable-audit-logs` を入力します。
    3. **[Add a default subscription]** のチェックを外します。
    4. **[Enable message retention]** を選択し、期間を 1 日以上に設定します。
    5. **[Create]** をクリックします。
2. 次の手順に従って Pub/Sub サブスクリプションを作成します。
    1. **[Pub/Sub] > [Subscriptions]** に移動し、**[+ Create subscription]** をクリックします。
    2. [Subscription ID] フィールドに `tenable-audit-logs-sub` を入力します。
    3. 先ほど作成したトピックを選択します。
    4. [Delivery type] セクションで、**[Pull]** を選択します。
    5. [Message retention duration] セクションで、期間を 1 日以上に設定します。

6. [Retry policy] セクションで、**[Retry after exponential backoff delay]** を選択し、デフォルト値のままにします。
7. [Expiration period] セクションで、**[Never expire]** を選択します。
8. **[Create]** をクリックします。
9. 新しく作成されたサブスクリプションの [Permissions] タブで、**[Add principal]** をクリックします。
10. [Add principals] セクションで、先ほど保存したサービスアカウントのメールを [New principals] フィールドに入力します。
11. [Assign roles] セクションで、**[Pub/Sub Subscriber]** ロールを選択し、**[Save]** をクリックして終了します。
12. Pub/Sub サブスクリプション名をコピーして保存します。この値は、クラウド サイバーエクスポージャー にプロジェクトの接続ときに、ウィザードの [デプロイメント後] セクションに入力する必要があります。

3. 次の手順に従ってログシンクを作成します。
    1. **[Logging] > [Configure] > [Log router]** に移動します。
    2. **[Create sink]** をクリックします。
    3. [Sink name] フィールドに `tenable-audit-logs` を入力し、**[Next]** をクリックします。
    4. シンクサービスについて、**[Cloud Pub/Sub topic]** と関連するトピックを選択し、**[Next]** をクリックします。
    5. 包含フィルターに以下を貼り付けます。

```
LOG_ID(cloudaudit.googleapis.com/activity) OR
LOG_ID(cloudaudit.googleapis.com/data_access) OR
LOG_ID(cloudaudit.googleapis.com/policy)
```

    6. **[Next]** をクリックします。
    7. **[+ Add exclusion]** をクリックします。
    8. [Exclusion filter name] フィールドで、`exclude-k8s-internal` を入力し、以下を除外フィルターに貼り付けます。

```
protoPayload.authenticationInfo.principalEmail-:* OR
protoPayload.authenticationInfo.principalEmail=~"^system:" OR
protoPayload.authenticationInfo.principalEmail=~"@container-engine-
robot.iam.gserviceaccount.com$" OR
protoPayload.authenticationInfo.principalEmail=~"@security-center-
api.iam.gserviceaccount.com$"
```

9. **[Create sink]** をクリックします。

組織レベルのアクセス許可を持つカスタムロールを作成する

上記の手順では、クラウドサイバーエクスポージャー のベストプラクティスに従って、ロールバインディングが組織レベルで付与されます。ただし、どの時点でも組織全体の接続を予定していない場合 (たとえば試用版の一部である場合)、クラウドサイバーエクスポージャー は、代わりにプロジェクトレベルでこのロールバインディングの付与をサポートします。プロジェクトレベルでロールバインディングを付与することにした場合でも、クラウドサイバーエクスポージャー では、組織レベルでの基本的なアクセス許可セットの付与が必要です。

カスタムロールを作成する方法

1. Google Cloud コンソールで、画面の左上にあるプロジェクトピッカーを使用して、関連する組織を選択します。
2. **[IAM & Admin]** > **[Roles]** に移動し、**[+ Create custom role]** をクリックします。
3. タイトル、説明、ID を入力します。
4. **[+ Add permissions]** をクリックし、「Org-Level Custom Role for Single-Project Connections」に一覧表示されているアクセス許可を追加します。
5. **[Create]** をクリックしてロールの作成を完了します。
6. 組織レベルで、Tenable サービスアカウントにカスタムロールを追加します。

カスタムロールの作成についての詳細は、関連する Google Cloud ドキュメントを参照してください。個別のプロジェクトを接続する際に、クラウドサイバーエクスポージャー に組織レベルのアクセス許可が必要な理由についての詳細は、GCP の FAQ を参照してください。

Google の FAQ (よくある質問) とトラブルシューティング

この記事の内容

- への GCP と Google Workspace のオンボーディングに関連する、よくある質問のリスト Tenable One Cloud Exposure
- GCP および Google Workspace のステータスとトラブルシューティングの情報

GCP の FAQ (よくある質問)

このセクションでは、GCP プロジェクトと組織のオンボーディングに関連する、よくある質問を紹介します。

フォルダーまたはプロジェクトを組織から除外する

> すでにオンボーディングした組織から、特定のフォルダーまたはプロジェクトを除外するにはどうすればよいですか?

回答

1. コンソールで、**[設定]** > **[統合]** に移動します。
2. 組織の横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
3. **[次へ]** をクリックしてウィザード (スコープ) の最後のステップに移動します。
4. **[特定のフォルダーとプロジェクトを除外する]** を選択してから、対象のフォルダーまたはプロジェクトを選択します。
5. **[終了]** をクリックします。ご使用の環境内で Tenable が次回 データの同期と更新の頻度 ときに、コンソールから削除されます。

組織レベルのアクセス許可を付与する

> 個別のプロジェクトをオンボーディングする際に、なぜ Tenable サービスアカウントに組織レベルのアクセス許可を付与する必要があるのですか?

回答: 関連するすべてのロールバインディングを表示するために、Tenable に親レベルの範囲 (組織) でアクセス許可を付与する必要があります。この機能がないと、Tenable は GCP リソースに関する重要なセキュリティ情報 (有効なアクセス許可など) を提供できません。ロールバインディングは組織レベルで付与されますが、Tenable は組織自体、または組織内の特定のプロジェクトが Tenable にオンボーディングされ

ていない限り、他の組織レベルのデータにアクセスすることができません。

プロジェクトは削除の保留中です

> GCP で削除したプロジェクトが Tenable で実際に削除されるまで、ステータスが長い間 [プロジェクトは削除の保留中です] になっているのはなぜですか?

GCP でプロジェクトを削除した後、そのプロジェクトが完全に削除されるまでに 30 日かかります。30 日が経過すると、Tenable はプロジェクトをシステムから自動的にオフボーディングします。Google Cloud ではこの期間中の削除を取り消すことができるため、必要に応じて GCP でプロジェクトを復元できるよう、Tenable では 30 日を経過するまでシステムからデータを削除しません。詳細については、関連する Google ドキュメント{target=_blank}を参照してください。

ドメイン内のユーザーが外部と見なされる

> 自社のドメイン内のユーザーが、Tenable インベントリで [ユーザー (外部)] リソースタイプカテゴリに表示されるのはなぜですか? 内部のユーザーが外部 (Workspace でローカルに定義されていない) と見なされるのはなぜですか?

組織のメンバーが、組織のドメインを使用して、独自に Google アカウントを作成した可能性があります。このようなアカウントは、Google によって管理されていないユーザーアカウントと見なされ、Tenable はそれを外部アカウントとして分類します。詳細については、Google ドキュメント{target=_blank} を参照してください。

組織の統合名の更新

GCP 組織の統合の名前を変更し、その名前をクラウドサイバーエクスポージャーに表示することができます。名前の変更は、特に複数の組織がある場合、識別に役立ちます。

名前を変更する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. 関連する統合の横にある三点リーダーをクリックして、**[編集]** をクリックします。
3. ウィザードのステップ 2 に移動し、**[組織名]** フィールドを更新します。
4. **[次へ]** をクリックしてウィザードの最後のステップに移動し、**[更新]** をクリックします。

Terraform のデプロイメント

> Terraform 経由の GCP プロジェクトのオンボーディングはサポートされていますか?

Terraform は GCP 組織の接続でのみサポートされています。

Google Workspace の FAQ (よくある質問)

このセクションでは、Google Workspace のオンボーディングに関連する、よくある質問を紹介します。

サービスアカウントトークン作成者ロール

> Google Workspace を追加する際に、Tenable の環境へのアクセスを許可する、サービスアカウントにアクセスできるプリンシパル (ermeticapp@sil-prd.iam.gserviceaccount.com) にサービスアカウントトークン作成者ロールを付与する必要があるのはなぜですか?

回答: このロールの名前で誤解を招くかもしれませんが、このロールによって Tenable は、クエリ経由で環境とやり取りを行うサービスアカウントに効果的になりすます{target=_blank} こと (権限の借用) ができます。

これは、サードパーティの GCP 環境に接続するうえで最も安全な方法であると Tenable は考えています。

他のベンダーが使用する別の方法として、ユーザーマネージドアクセスキーの作成があります。この場合は手動のローテーションが必要なため、危険にさらされる可能性があります。ここで権限借用を使用する利点は、Tenable のサービスアカウントに静的な認証情報を関連付けないことで、サイバーエクスポージャーのリスクを軽減できることです。サービスアカウントの権限借用とサービスアカウントキーを参照してください。

サービスアカウントの権限借用とサービスアカウントキー

> Tenable がサービスアカウントキーではなくサービスアカウントの権限借用を使用するのはなぜですか?

回答: GCP ドキュメント{target=_blank}によると、サービスアカウントの権限借用は、権限借用に事前に認証されたアイデンティティが必要であり、作成された認証情報は保持されないため、サービスアカウントキーを使用する場合よりも安全です。これに対し、サービスアカウントキーによる認証では事前の認証は必要ありませんが、永続的なキーが漏洩した場合は、リスクの高い認証情報となります。

スーパー管理者ユーザー (アドバンス)

> **注意:** ドメイン全体の委任 (アドバンス) でアクセス許可を付与する場合にのみ関連します。クラウドサイバーエクスポージャーでは、ほとんどの組織に対して、カスタムロールによりアクセス許可を付与することを推奨しています。

> Google Workspace を追加する際に、Tenable がスーパー管理者ユーザーのメールアドレスを必要とするのはなぜですか? Tenable ではこのような幅広いアクセスに関連するリスクをどのように抑制していますか? また、なぜ Tenable にメールアドレスが必要なのですか?

回答: Tenable はお使いの環境でスーパー管理者ユーザーを必要とする、特定の Google API にアクセスする必要があります。これは、アイデンティティおよびその他の一般的なクラウドセキュリティ機能に必要です。以下は API のリストの一部です。

- https://developers.google.com/admin-sdk/reference-overview
- https://cloud.google.com/identity/docs/ja/apis

ただし、Tenable に実際に付与されるアクセス許可は、お使いのワークスペースを追加する際に付与される OAuth スコープに制限されます。これらのアクセス許可はすべて読み取り専用です。したがって、Tenable には必要な API にアクセスできるスーパー管理者の権限が必要ですが、実際には読み取り専用のアクセス許可のみが付与されるため、リスクを抑制できます。

Tenable Google Workspace のオブジェクトをクエリする唯一の方法は、ドメイン全体の委任とユーザーのなりすましを使用することであり、これにはユーザーのメールアドレスが求められるため、Tenable にメールアドレスが必要となります。サービスアカウントが Google Workspace にアクセスする方法の詳細については、Google のドキュメント{target=_blank}を参照してください。このユーザーにメールボックスは必要ありません。

ドメイン全体の委任 (アドバンス)

注意: ドメイン全体の委任 (アドバンス) でアクセス許可を付与する場合にのみ関連します。クラウドサイバーエクスポージャーでは、ほとんどの組織に対して、カスタムロールによりアクセス許可を付与することを推奨しています。

ドメイン全体の委任とは何ですか? また、Google Workspace を追加する際に、ドメイン全体の委任を使用して Tenable にアクセス権を付与する必要があるのはなぜですか?

回答: ドメイン全体の委任は、アプリケーションに関連ユーザーデータへのドメイン全体のアクセス権を付与するために使用される Google Workspace のメカニズムです。この権限の委任は、OAuth 2.0 のサービスアカウントを使用して行われます。Google Workspace は本質的に GCP に接続されているため、この委任を通じて付与されるアクセスにより、Tenable は GCP 資産を理解するための基本的な情報を収集および提供できるようになります。

このアクセスがない場合、Tenable は以下を実行できません。

- Google Workspace ユーザーを、使用する GCP リソースにマッピングする。
- GCP のアクセス許可はグループに付与できるため、Google Workspace ユーザーをグループにマッピングする。
- ユーザー/グループのアクセス許可グラフを作成する。
- GCP で権限を昇格できる強力な Google Workspace アクセス許可を持つユーザーを特定する (スーパー管理者など)。

ドメイン全体の委任により、Tenable は管理者を含む、任意の Google Workspace ユーザーの権限を借用できます。厳密に言うと、Tenable にスーパー管理者のアクセス許可があるように見えるかもしれませんが、実際にはそうではありません。Tenable には Google Workspace 内での管理者のアクセス許可がありません。Tenable に付与される実際の権限は、ドメイン全体の委任の設定時に定義された特定の OAuth スコープに制限されます。これらのアクセス許可は Google Workspace への読み取りアクセスのみを Tenable に付与します。

重要: このアクセスは、カスタムロールではなく、スーパー管理者ユーザーの形式で Tenable に付与する必要があります。一部のアクセス許可はスーパー管理者のみが使用でき、カスタムロールを作成する場合には使用できません。たとえば、次の OAuth スコープです。
https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly
https://www.googleapis.com/auth/admin.reports.audit.readonly

詳細については、関連する Google Workspace のドキュメントを参照してください。
https://developers.google.com/admin-sdk/directory/v1/guides/delegation

割り当て管理者ロール(レガシー)

> **注意:** このセクションは、2025 年 4 月 27 日より前に Google Workspace をオンボードした場合にのみ関連します。

> Google Workspace を追加する際に、Tenable に環境へのアクセスを許可する、サービスアカウントへの割り当て管理者ロールを追加する必要があるのはなぜですか?

回答: このロールには、Tenable が以下を行うために必要な Tenable サービスアカウントの API アクセスを管理する権限が含まれています。

- お使いの環境で現在使用している一部のサービスについてクエリを実行する
- 新しい GCP サービスがリリースされ次第、自動的にサポートする

このロールの名前で誤解を招く恐れがあるものの、このロールによって Tenable は GCP 環境から設定データを収集するために必要な API を効果的に有効化できます。この機能がないと、Tenable は上記の機能を実行できません。

割り当てはプロジェクトごとに GCP で管理され{target=_blank}、Tenable のサービスアカウントは単一のプロジェクトに割り当てられるため、このロールに含まれるアクセス許可の範囲は制限されます。別のプロジェクトでサービスの API アクセスを明示的に有効にしない限り、Tenable はそれにアクセスできません。Tenable のサービスアカウントは、オンボーディングプロセス中に追加された専用プロジェクトから新しいサービスをクエリできますが、環境のクォータを変更することはできません。

クラウド サイバーエクスポージャー は現在、GCP 環境のすべてのサービスとアクセス許可をプログラムでマッピングしています。つまり、新しい GCP サービスがリリースされるとすぐに、基本的なアクセス許可を付与され Tenable で確認できます。

プロジェクト ステータスとトラブルシューティング

クラウド サイバーエクスポージャー は、**[アカウント] > [GCP]** ページで各プロジェクトの**ステータス**を表示します。これはたとえば、Tenable がプロジェクトに接続できるかどうかを示すもので、オンボーディングに関する潜在的な問題のトラブルシューティングに役立ちます。

ステータス	説明
接続済み	Tenable プロジェクトに正常に接続され、プロジェクトは実行されています。
削除中...最大で 1 時間かかる場合があります	Tenable でプロジェクトを削除しましたが、そのプロセスはまだ完了していません。
接続に失敗しました	Tenable プロジェクトに接続できませんでした。これは、プロジェクトが GCP で削除されたものの、クラウド サイバーエクスポージャー コンソールからは削除されていない場合に発生することがあります。
Google Workspace が接続されていません	Google Workspace が接続されていません。詳細については、Google Workspace の接続を参照してください。
アクセス許可がありません	リストされたロールの 1 つ以上が欠落しており、Tenable サービスアカウントに追加する必要があります。
プロジェクトが削除されました	Tenable でプロジェクトを削除しました。このプロジェクトは、でデータが次回同期されるTenableタイミングで削除されます。
プロジェクトは削除の保留中です	GCP でプロジェクトを削除した後、そのプロジェクトが完全に削除されるまでに 30 日かかります。30 日が経過すると、Tenable はプロジェクトをシステムから自動的にオフボーディングします。Google Cloud ではこの期間中の削除を取り消すことができるため、必要に応じて GCP でプロジェクトを復元できるよう、Tenable では 30 日を経過するまでシステムからデータを削除しません。詳細については、関連

ステータス	説明
	する Google ドキュメントを参照してください。
プロジェクトが停止されました	GCP でプロジェクトが一時停止されています。このプロジェクトは、GCP で進展があるまでこの状態のままです。
一部の機能が無効になっています	Tenable サービスアカウントを作成したプロジェクトで、GCP の課金が無効になっています。これにより、このアカウントへのクエリが制限されます。非アクティブなサービスアカウントの検出結果、Kubernetes の可視性とセキュリティなど一部のクラウドサイバーエクスポージャー機能は、請求先アカウントが接続されるまで無効になります。プロジェクトの課金についての詳細は、関連する Google Cloud ドキュメントを参照してください。
サブスクリプションは設定されていません	GCP プロジェクトから監査ログ (アクティビティログ) を収集するために使用される Pub/Sub サブスクリプションが設定されていません。このため、監査ログはクラウドサイバーエクスポージャーに送信されません。監査ログの設定を参照してください。

ワークスペースのステータスとトラブルシューティング

クラウドサイバーエクスポージャーは、**[統合] > [Google Workspace]** ページにある各ワークスペースの**ステータス**を表示します。これはたとえば、Tenable がワークスペースに接続できるかどうかを示すもので、オンボーディングに関する潜在的な問題のトラブルシューティングに役立ちます。

ステータス	説明
Service Usage API が有効になっていません	サービスアカウントが作成されたプロジェクトレベルで有効化します。
アクセス許可がありません	• Tenable サービスアカウントに必要なアクセス許可があることを確認します。

ステータス	説明
	• クラウドサイバーエクスポージャープリンシパルに**サービスアカウントトークン作成者**のロールが付与されていることを確認します。
ラベルがありません	ラベルが存在し、関連するキー/値ペアがあることを確認します。
OAuth スコープがありません	すべての必要な OAuth スコープがドメイン全体の委任により追加されるようにします。

OCI

OCI の必要なアクセス許可

ここでは、Tenable One Cloud Exposure 機能に必要な OCI ポリシーステートメントを説明します。

モニタリング

このステートメントは、クラウド資産、アクセス許可、コンパートメントの使用状況、セキュリティ設定を可視化するため、Tenable にテナンシ内のリソースへの読み取り専用アクセスを付与します。

次のステートメントを、テナンシのオンボーディング中に作成するポリシーに追加します。

```
Allow group 'TenableCS' to read all-resources in tenancy
```

このポリシーを作成する手順については、OCI テナンシの接続を参照してください。

ワークロード保護

この機能を使用するには Standard または Enterprise のライセンスが必要です。これらのアクセス許可を付与する手順については、ワークロードの接続を参照してください。

これらのステートメントは、Tenable のスキャングループにテナンシ内のボリュームを使用するためのアクセス許可を付与します。これにより、ワークロード保護でスキャンされるディスクスナップショットの作成と読み込みが可能になります。

OCI ワークロードをスキャンするためのアクセス許可を クラウドサイバーエクスポージャー に付与するために、統合時に作成した OCI ポリシーに以下のステートメントを追加します。

```
define tenancy TenableOutpostTenancy as
ocid1.tenancy.oc1..aaaaaaaasv6dlhkapckiivrlno4udf5s5faqc3pnrii5vrycyxwj2qxg7niq
define group CWPVMScanning as
ocid1.group.oc1..aaaaaaaay6qcowhmfjzh44kdxzx7ld6z66lkno5qnk4afy7ktlmi7j67b4uq
admit group CWPVMScanning of tenancy TenableOutpostTenancy to use volumes in tenancy
```

暗号化ボリューム

デフォルトでは、Oracle 暗号化ブートボリュームは、Oracle Cloud によって管理される暗号化キーを使用します。これらの暗号化ボリュームは設計に組み込まれているため、スキャンのためにアクセス許可を追加する必要はありません。

所有し管理するキーで暗号化されたボリュームをスキャンするには、以下のステートメントもワークロード保護ポリシーに追加します。これにより、キーの委任を使用し、キーをテナンシ内のボリュームに関連付けるためのアクセス許可が付与されるため、クラウドサイバーエクスポージャー は暗号化されたスナップショットにアクセスできるようになります。

```
admit group CWPVMScanning of tenancy TenableOutpostTenancy to use key-delegate in tenancy
admit group CWPVMScanning of tenancy TenableOutpostTenancy to associate keys in tenancy with volumes in
tenancy TenableOutpostTenancy
```

OCI テナンシの接続

Tenable One Cloud Exposure で Oracle Cloud テナンシ全体を接続し、テナンシに関連付けられたクラウドアイデンティティとリソースを完全に可視化します。Tenable は Oracle Cloud API からインベントリと設定データを収集します。

テナンシ全体を接続することで、多数のアカウントがあるクラウド環境でのオンボーディングプロセスを迅速化かつ自動化できます。これにより、以下が可能になります。

- すべてのコンパートメントを同時にTenableに接続
- 後の段階でOracle Cloudに追加された新しいコンパートメントを自動的に接続
- 全範囲のプラットフォーム機能を可視化

統合が完了すると、Tenableにテナンシステータスとトラブルシューティングが表示されます。これはたとえば、Tenableがテナンシに接続できるかどうかを示すもので、潜在的な問題のトラブルシューティングに役立ちます。

> **注意:**
> - サポートされているOCIリソースの検索可能なリストについては、対応リソースを参照してください。
> - ライセンス付与で請求対象となるOCIリソースのリストについては、請求対象のリソースを参照してください。

前提条件

始める前に

- ルート権限を確認します。OCIテナンシがルートコンパートメントにオンボーディングされています。
- ルートコンパートメントにグループ、ユーザー、APIキー、ポリシーを作成するアイデンティティに対して、十分なアクセス許可を付与します。
- ユーザー、グループ、ポリシーを作成するアクセス許可を持つ、関連するOracle Cloudテナンシへの管理者アクセスがあることを確認します。
- Terraform固有
    - Terraform CLI v0.13以上をインストールしていることを確認します。
    - `terraform init`が既存の設定と競合することなく、次のプロバイダーをダウンロードしてインストールできることを確認します。

- OCI プロバイダー v6.0 以上
- TLS プロバイダー v4.0 以上
- ローカルプロバイダー v2.2 以上

- 秘密鍵の PEM ファイルを安全に処理できる場所で Terraform が実行されることを確認します。

テナンシの接続

OCI テナンシの接続方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[OCI テナンシ]** をクリックします。[OCI テナンシ] ウィザードが開きます。
3. **設定** ステップ (ステップ 1/2) で、次の操作を実行します。
    1. 統合の名前を入力します。
    2. **[テナンシ OCID]** に、テナンシの ID を入力します。
    3. **[機能]** で、有効にする機能を選択します。この選択によって、必要なアクセス許可が決まります。
        - **モニタリング (読み取り専用)**: デフォルトで選択されています。すべてのクラウド資産について完全な可視性を確保します。これにはアクセス許可、コンパートメント使用状況、データとセキュリティの設定に関する情報が含まれます。
        - **コンピューティングインスタンススキャン (ワークロード保護)**: コンピューティングインスタンスをスキャンして、脆弱性と設定ミスがないか確認します。必要なアクセス許可については、OCI の必要なアクセス許可を参照してください。
    4. **[デプロイメント]** で、次のいずれかのデプロイオプションを選択します。
        - **Terraform** - モジュールベースのデプロイメント。デプロイする前に、Terraform 固有の前提条件を参照してください。
            - クラウドサイバーエクスポージャー ウィザードに表示されるモジュール呼び出しをコピーして Terraform 設定に追加し、`terraform apply` を実行します。このモ

ジュールはアイデンティティを作成し、環境に接続してスキャンするアクセス許可を Tenable に付与します。

- **手動** - OCI コンソールを使用し、手動で設定します。詳細な手順については、OCI テナンシの手動デプロイを参照してください。

5. **[デプロイメント後]** に、次の値を入力します。
    - **Tenable ユーザー OCID** (`user`): Tenable 用に作成したユーザーの OCID
    - **フィンガープリント** (`fingerprint`): ユーザーに追加された公開キーのフィンガープリント
    - **秘密鍵**: Terraform 出力で指定されたパスから、または手動でユーザー認証情報の作成した場合は Oracle Cloud から、秘密鍵 PEM ファイルをアップロードします。
    - **ホームリージョン** (`region`): Oracle Cloud Infrastructure のリージョン。
6. **[次へ]** をクリックします。

4. **範囲** ステップ (ステップ 2/2) で、次の操作を実行します。
    1. (オプション) **[コンパートメント構造を自動的に更新]** を選択して、コンパートメントの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます。詳細については、アカウント階層とフォルダーを参照してください。
    2. **[範囲]** で、オンボーディングするコンパートメントを選択します。
        - **現在と将来のコンパートメントをすべて同期する (推奨)**
        - **特定のコンパートメントを除外する**

        > **注意:**
        > - コンパートメント全体を除外すると、コンパートメント内の現在と将来のアカウントがすべて除外されます。
        > - コンパートメントで特定のアカウントを除外すると、選択したアカウントのみが除外されます。

5. **[終了]** をクリックします。

OCI テナンシの手動デプロイ

> **注意:** 手動デプロイメントが完了したら、テナンシの接続 デプロイメント後の手順を完了します。

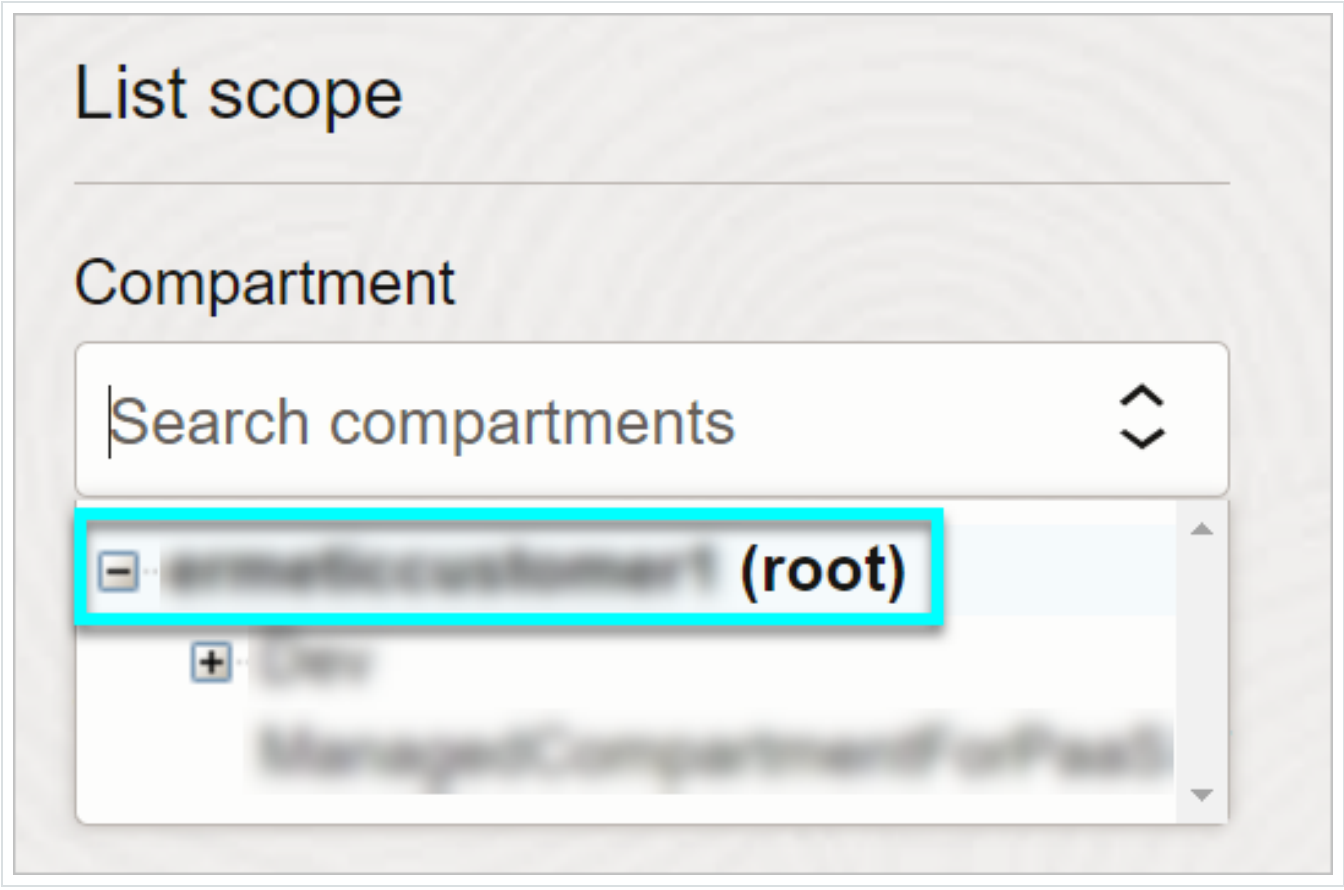
Terraform デプロイメントの代わりに、OCI コンソールを使用して OCI テナンシを手動でデプロイすることもできます。これは、テナンシを接続する際にデプロイメントタイプとして **[手動]** を選択した場合の手順です。

1. グループの作成
2. ポリシーを作成してグループにポリシー割り当て
3. ユーザーの作成
4. ユーザー認証情報の作成

グループの作成

OCI で クラウド サイバーエクスポージャー のグループを作成します。

1. OCI コンソールにログインし、**[Identity & Security] > [Identity] > [Domains]** の順に移動します。
2. 左側のメニューの [List scope] > [Compartment] でルートコンパートメントを選択します。



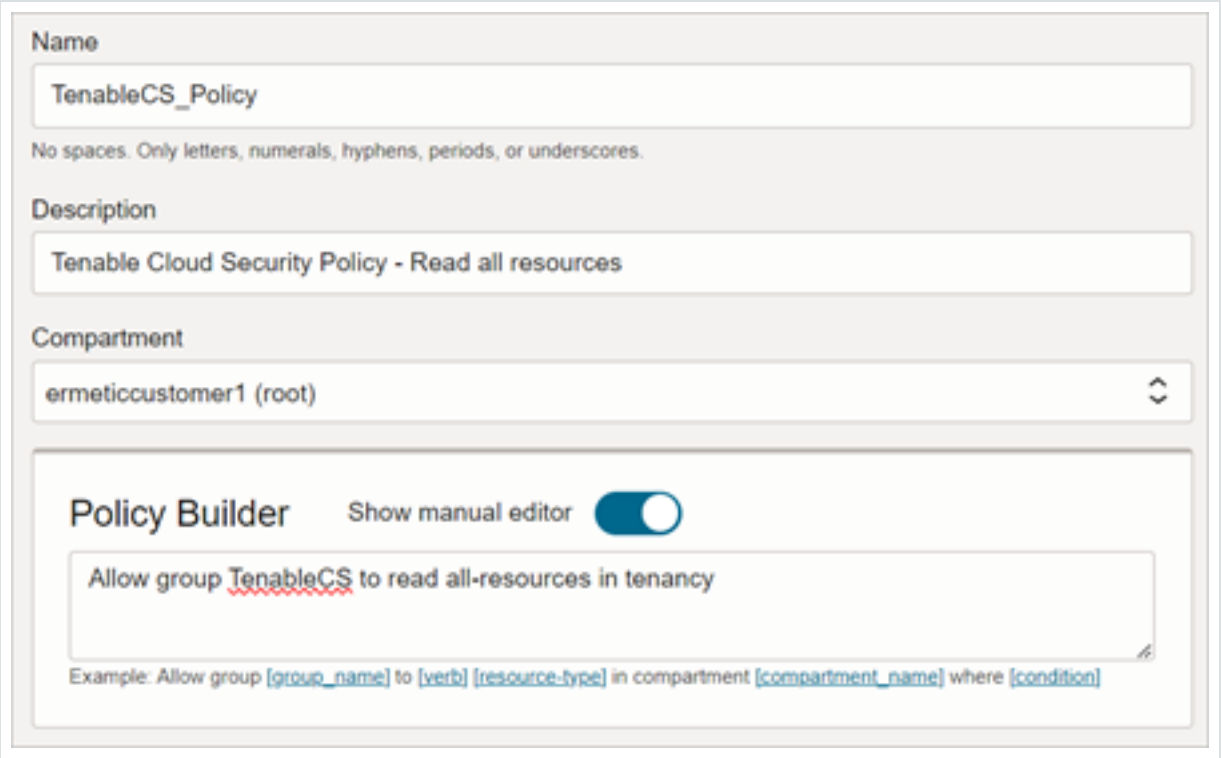
3. ドメインのリストで、**[Default]** ドメイン名をクリックします。
4. **[グループ]** をクリックしてから、**[グループの作成]** をクリックします。
5. **[名前]** に TenableCSと入力し、**[作成]** をクリックします。

ポリシーを作成してグループにポリシー割り当て

クラウドサイバーエクスポージャーに対して作成したグループに、OCI のリソースを読み取るために必要なアクセス許可を付与します。

1. **[アイデンティティとセキュリティ] > [アイデンティティ] > [ポリシー]** の順に移動します。
2. **[ポリシーの作成]** をクリックし、以下の詳細を入力します。
    1. **名前**: 意味のある名前を入力します。
    2. **説明**: わかりやすい説明を入力します。
    3. **コンパートメント**: root コンパートメントを選択します。
3. ポリシービルダーで **[手動エディターの表示]** をクリックし、「OCI の必要なアクセス許可」にリストされているモニタリングステートメントを追加します。

> **注意:** グループの作成した際にグループ名として TenableCS を使用していない場合は、TenableCS を使用した名前に置き換えます。



4. **[Create]** をクリックします。

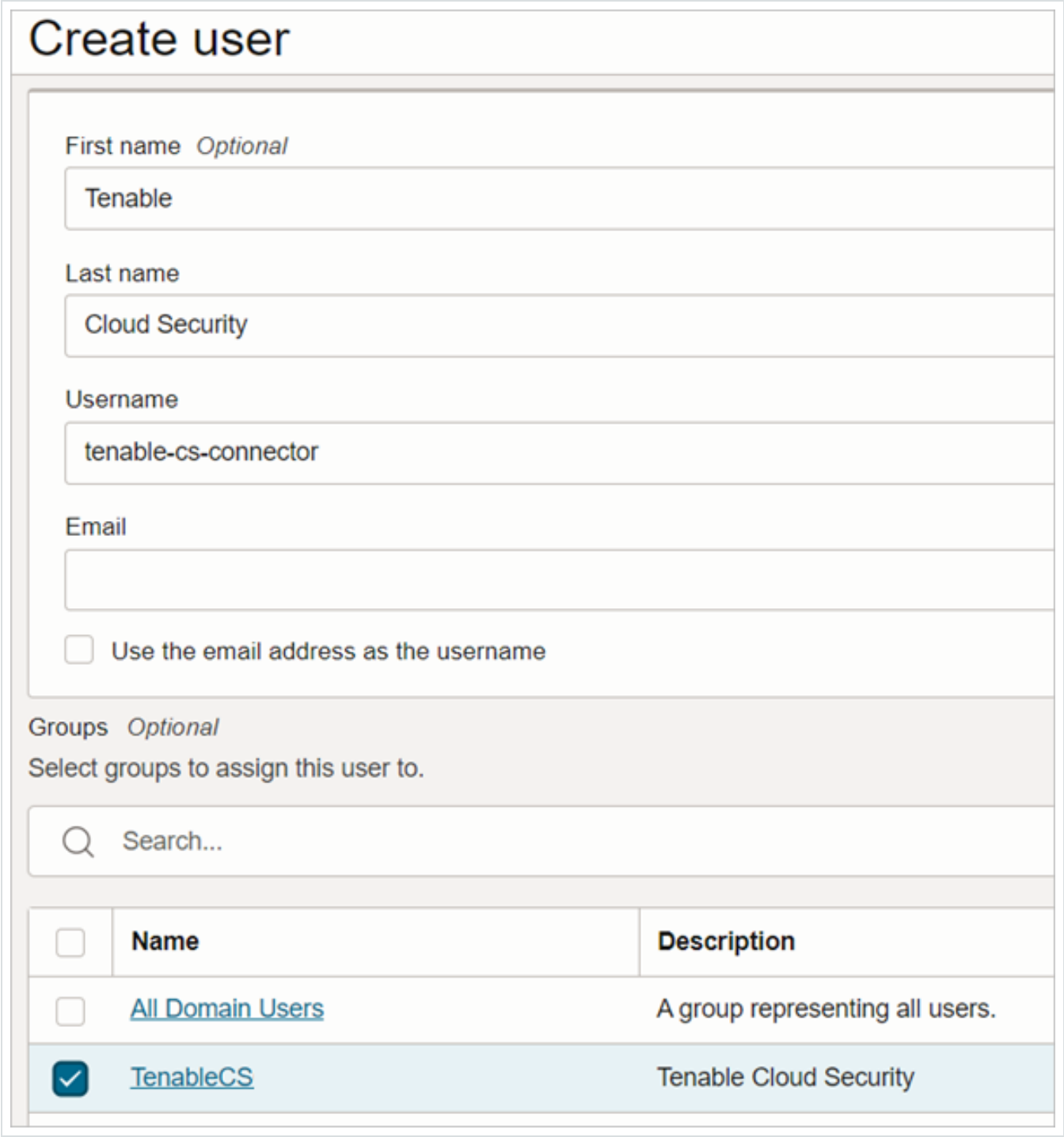
ユーザーの作成

ユーザーを作成します。このユーザーを使って、この後 OCI への API アクセスを クラウド サイバーエクスポージャー に許可するユーザー認証情報を作成します。

1. **[アイデンティティとセキュリティ] > [アイデンティティ] > [ドメイン]** の順に移動します。
2. ドメインのリストで、**[Default]** ドメイン名をクリックします。
3. 左側のメニューで、**[ユーザー]** をクリックします。
4. **[Create user]** をクリックし、以下の詳細を入力します。
    1. **名**、**姓**、**ユーザー名**、**メールアドレス**

        > **注意:** メールアドレスが必要な場合は、ここに入力するか、**[Settings] > [Domain Settings]** に移動して **[Primary email address required]** チェックボックスのチェックを外すことで、強制的に無効にできます。

    2. グループには、グループの作成を選択します。



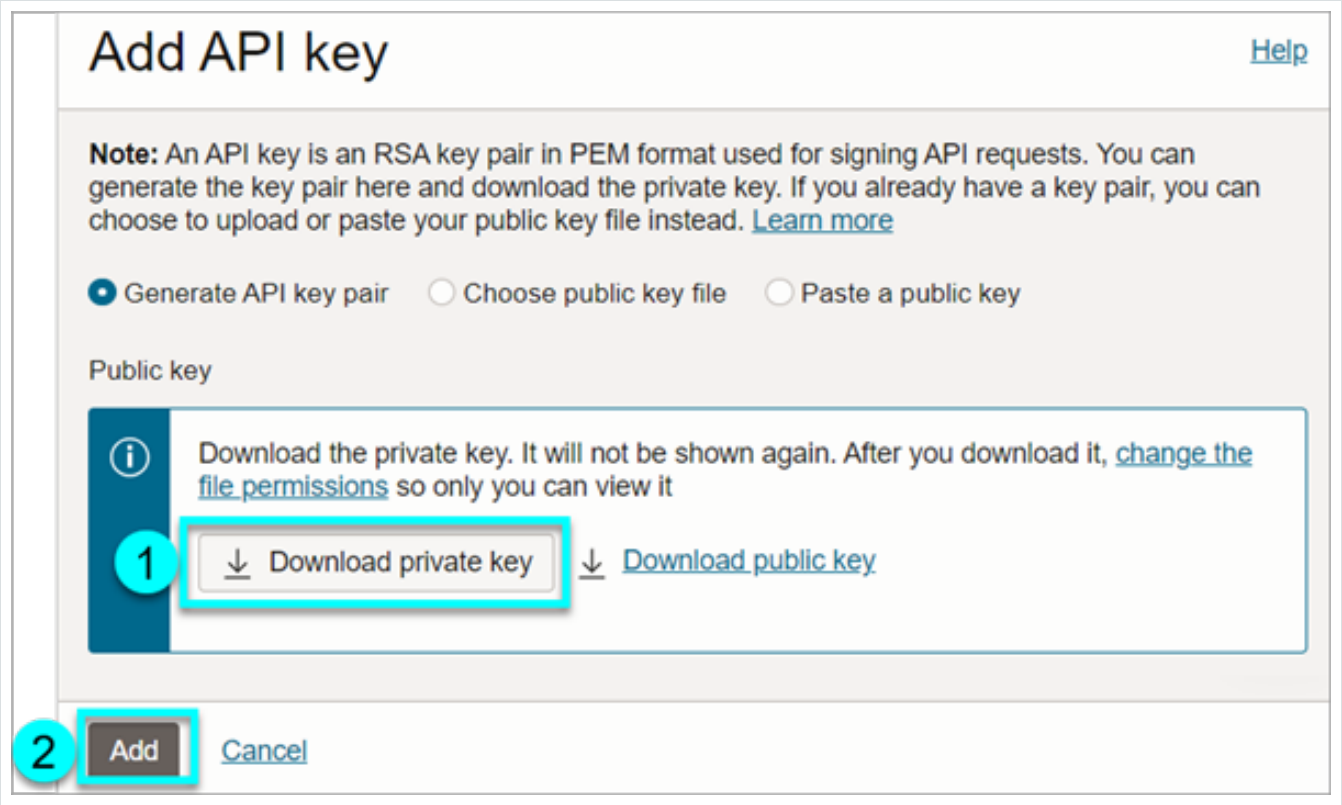
5. **[Create]** をクリックします。

ユーザー認証情報の作成

ユーザー認証情報を作成して OCI への API アクセスを クラウド サイバーエクスポージャー に許可します。

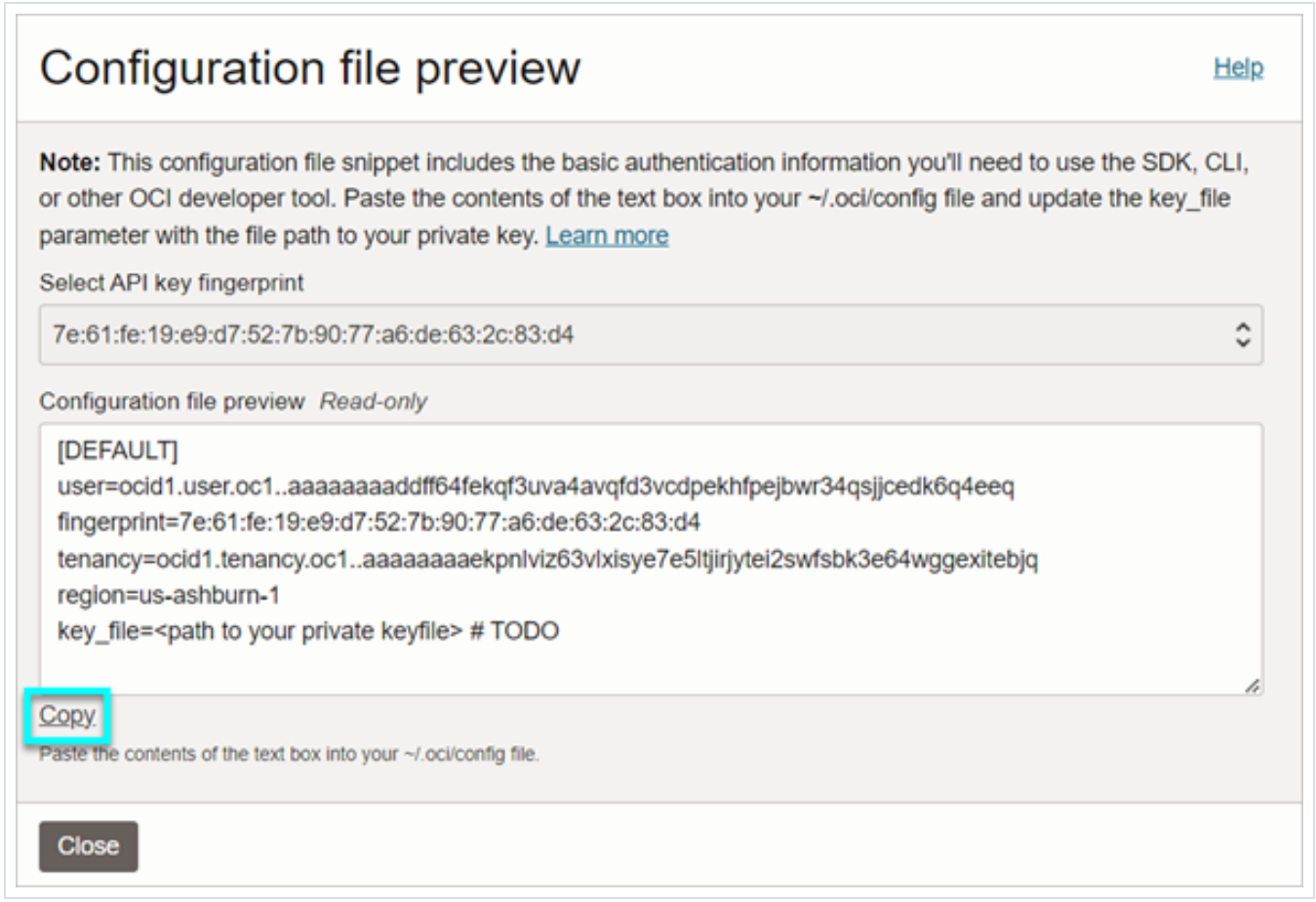
1. ユーザーのリストから ([アイデンティティ] > [ドメイン] > [Default ドメイン] > [ユーザー]) でユーザーの作成をクリックします。
2. 左側のメニューの [リソース] で、**[API キー]** をクリックします。
3. **[API キーの追加]** をクリックします。
4. **[秘密キーのダウンロード]** をクリックしてから **[追加]** をクリックします。

> **注意:** このファイルは、クラウド サイバーエクスポージャー が OCI サーバーに対して認証を行うために必要です。このキーは、Oracle Cloud の統合を完了するために必要になります。



5. **[Copy]** をクリックして、設定ファイルのコンテンツをコピーします。

> **注意:** Tenable が認証を完了するには、設定ファイルに含まれている基本認証情報が必要です。この情報を クラウド サイバーエクスポージャー コンソールに入力する必要があります。



6. ファイル (**oci_config.txt** など) にコピーしたコンテンツを貼り付けて、ファイルを保存します。

OCI の FAQ (よくある質問) とトラブルシューティング

この記事の内容

- Tenable One Cloud Exposure への OCI の接続に関連する、よくある質問のリスト
- テナンシステータスとトラブルシューティング

テナンシからフォルダーまたはコンパートメントを除外する

> すでに接続したテナンシから、特定のフォルダーまたはコンパートメントを除外するにはどうすればよいですか?

回答

1. コンソールで、**[設定]** > **[統合]** に移動します。
2. テナンシ名の横にある三点リーダーメニューをクリックし、**[編集]** をクリックします。
3. **[次へ]** をクリックしてウィザード (スコープ) の最後のステップに移動します。
4. **[特定のフォルダーおよびコンパートメントを除外する]** を選択してから、対象のフォルダーまたはコンパートメントを選択します。
5. **[終了]** をクリックします。ご使用の環境内で Tenable が次回 データの同期と更新の頻度 ときに、コンソールから削除されます。

サポートされている OCI リソース

> クラウドサイバーエクスポージャー はどの OCI リソースをサポートしていますか?

回答: サポートされている OCI リソースの検索可能なリストについては、対応リソースを参照してください。

統合名の更新

OCI テナンシ統合の名前を変更し、その名前を クラウドサイバーエクスポージャー に表示することができます。名前の変更は、特に複数の統合がある場合、整理や識別に役立ちます。

名前を変更する方法

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** に移動します。
2. 関連する統合の横にある三点リーダーをクリックして、**[編集]** をクリックします。
3. ウィザードのステップ 1 で、**[名前]** フィールドを更新します。
4. ウィザードの最後のステップに移動し、**[終了]** をクリックします。

テナンシステータスとトラブルシューティング

クラウドサイバーエクスポージャー に各テナンシやコンパートメントの**ステータス**が表示されます。これはたとえば、Tenable がテナンシやコンパートメントに接続できるかどうかを示すもので、潜在的な問題のトラブルシューティングに役立ちます。

テナントステータス

クラウド サイバーエクスポージャー コンソールで、**[設定] > [統合]** に移動し、テナンシのステータスを確認できます。

ステータス	説明
接続済み	クラウド サイバーエクスポージャー テナンシに正常に接続され、アカウントは実行されています。
削除中...最大で 1 時間かかる場合があります	クラウド サイバーエクスポージャー でアカウントを削除しましたが、そのプロセスはまだ完了していません。
接続に失敗しました	クラウド サイバーエクスポージャー はテナンシに接続できませんでした。これは、公開キーのフィンガープリント、ユーザーの OCID またはテナンシの OCID が正しくない場合に発生する可能性があります。ユーザーが、テナンシのホームリージョンにあるアイデンティティ ドメイン内に作成されていること、またはアイデンティティ ドメインがテナンシのホームリージョンにレプリケートされていることを確認してください。
ユーザーが承認されていません	ユーザーには、OCI で十分なアクセス許可がありません。
ユーザー認証情報	入力された公開キーが秘密キーと一致しません。

ステータス	説明
が無効です	

コンパートメントステータス

クラウドサイバーエクスポージャーコンソールで、**[アカウント] > [OCI]** に移動してコンパートメントのステータスを確認できます。

ステータス	説明
接続済み	クラウドサイバーエクスポージャーはコンパートメントに正常に接続され、アカウントは実行されています。
アクセスが拒否されました	クラウドサイバーエクスポージャーは 1 つ以上のリソースタイプを同期できませんでした。これにはさまざまな理由が考えられます。たとえば、特定のコンパートメントにネットワーク境界がある場合です。
削除中です...これには時間がかかる場合があります	クラウドサイバーエクスポージャーでテナンシを削除しましたが、そのプロセスはまだ完了していません。
テナンシが接続されていません	テナンシに問題があります。テナントステータスをチェックして詳細と修正を確認してください。
コンパートメントは削除の保留中です	コンパートメントは OCI で削除対象としてマークされ (ステータス = 削除中)、最終的に削除されます。削除を保留中のコンパートメントに関連付けられているリソースは、クラウドサイバーエクスポージャーでは非表示になります。
コンパートメント	コンパートメントは、OCI で「非アクティブ」のステータスになっています。

ステータス	説明
がアクティブではありません	
コンパートメントが削除されました	コンパートメントは OCI で削除されました。

Snowflake

Snowflake の接続

Tenable One Cloud Exposureで Snowflake アカウントを接続して Snowflake リソースの可視性を取得し、データプラットフォーム環境全体のデータ分類をサポートします。Tenable は Snowflake API からメタデータと設定の詳細を収集して、スキャンとモニタリングを有効にします。

オンボーディング後、Tenable に各 Snowflake アカウントのステータスが表示されます。これは Tenable アカウントに接続できるかどうかを示し、オンボーディングに関する潜在的な問題のトラブルシューティングに役立ちます。

- ネットワークアクセスが制限されている場合は、オンボーディング後に Tenable プラットフォームからのアクセスを許可します。「ネットワークアクセスを許可する」を参照してください。
- 最初の Snowflake アカウントを接続すると、デフォルトでアカウント全体がスキャン対象として選択されます。[データ] ページでスキャンターゲットを調整できます。
- Snowflake リソースタイプの検索可能なリストについては、「対応リソース」を参照してください。
- ライセンスとしてカウントされるSnowflakeリソースのリストについては、「請求対象のリソース」を参照してください。
- SnowflakeスキャンはEnterpriseライセンスで利用できます。

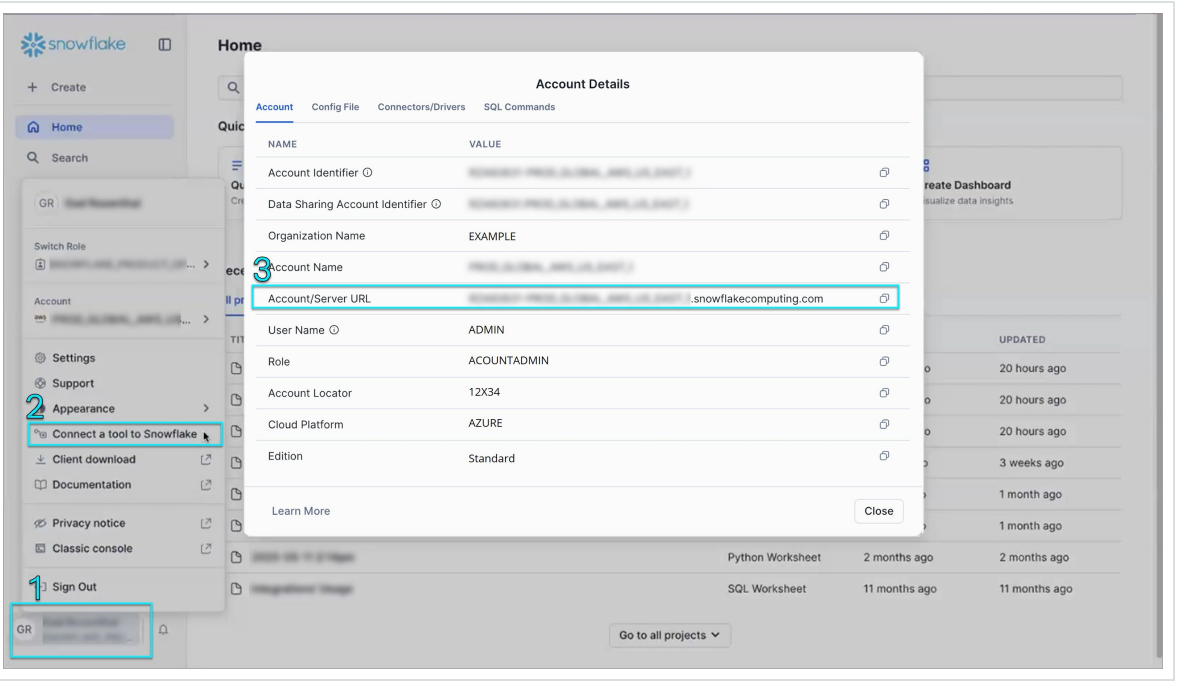
Snowflake アカウントの接続

ヒント: オンボーディング中は、クラウドサイバーエクスポージャーコンソールとSnowflakeアカウントの両方を開いたままにしておくことをお勧めします。これにより、2つのプラットフォーム間で設定データをコピーできます。

Snowflakeアカウントを接続する方法

1. クラウドサイバーエクスポージャーコンソールで以下を実行します。
    - 最初または追加のアカウントを接続するには、**Settings** > **統合に移動します。**
        - **「データプラットフォーム」**で、「**Snowflake**」をクリックします。
        - **[Add Snowflake Account]**をクリックします。
    - または、追加のアカウントを接続するには、**Snowflake** >**アカウント**に移動します。
        - **[+追加]**、**[アカウントの追加]**の順にクリックします。
2. **[Add Snowflake Account] (Snowflakeアカウントの追加**)ウィンドウで次の操作を実行します。
    1. **Snowflakeアカウント/サーバーのURL**を入力します。これはSnowflakeアカウントのURLです。URLを取得するには
        1. Snowflakeアカウントに移動します。
        2. **[ユーザー]メニュー**をクリックします。
        3. **[ツールをSnowflakeに接続する]**をクリックします。

4. [アカウントの詳細] ウィンドウで、**アカウント/サーバーの URL** をコピーします。



2. **デフォルト名をカスタマイズします (オプション)。** Tenable作成するSnowflakeオブジェクトには、名前が事前入力されています。デフォルトを使用することも、名前を変更することもできます。

   オブジェクト名:

フィールド	説明
ロール名	Tenableユーザーに付与されているロール。付与されたアクセス許可を参照してください。
ユーザー名	ユーザーが引き受け、Tenable ロールを付与されたTenable。ロールのアクセス許可の範囲内で動作します。ユーザー名は Snowflake アカウントレベルで**一意である必要があります**。
ウェアハウス名	Tenableユーザーに割り当てられた専用のTenableコンピューティングウェアハウス。コンピューティング コストを低く抑えるために、ウェアハウス サイズは X-

フィールド	説明
	Small です。
データベース名	Tenableタスクをホストして実行するために使用される専用Tenableデータベース。
タスク名	新たに検出されたデータベースへの読み取り専用アクセスを Tenable ロールに付与する定期的なジョブ。付与されたアクセス許可を参照してください。

3. **[次へ]** をクリックします。
4. 提供されたスクリプトをコピーします。
5. 提供されたスクリプトをSnowflakeで実行します。
    1. アクティブな**ウェアハウス**が選択された状態で、**ACCOUNTADMIN** ロールを使用してSnowflakeアカウントにログインします。
    2. **[ワークシート]** に移動し、新しい **SQL ワークシート**を作成します。
    3. 提供されたスクリプトを貼り付けて、クラウドサイバーエクスポージャーコンソールから実行します。
    4. Snowflakeアカウントがネットワーク制限を実施する場合は、Tenable IPからのアクセスを許可します。詳細については、「 ネットワークアクセスの許可 」を参照してください。
6. スクリプトが正常に完了したら、クラウドサイバーエクスポージャーコンソールに戻り、**[完了]** をクリックします。

Tenable にネットワークアクセス権を付与する

Snowflakeアカウントでネットワークアクセスが制限されている場合は、Tenable プラットフォームからのアクセスを許可するネットワークポリシーを定義する必要があります。これにより、Tenable 環境に接続してオンボーディングを正常に完了できます。

Snowflakeネットワークルールの詳細をご覧ください。

SQL スクリプトをコピーするときは、次の点に注意してください。:

- 個別の **IP アドレス**または **CIDR 範囲**を使用します。
- **複数の IP アドレスは**コンマ区切りが必要です。
- **オンボーディング中にデフォルトのユーザー名を変更**した場合は、提供されたスクリプトのTENABLE_USER値を更新して、**[Snowflake >アカウント]** に表示されているユーザー名と一致させます。無効にしないと、ポリシーが正しく適用されなくなります。

ネットワークポリシーを追加する方法

1. ACCOUNTADMIN ロールを使用して Snowflake アカウントにログインします。
2. **[プロジェクト]** > **[ワークシート]** に移動し、新しい **SQL ワークシート**を作成します。
3. 次のスクリプトを貼り付けます。

```
SQL

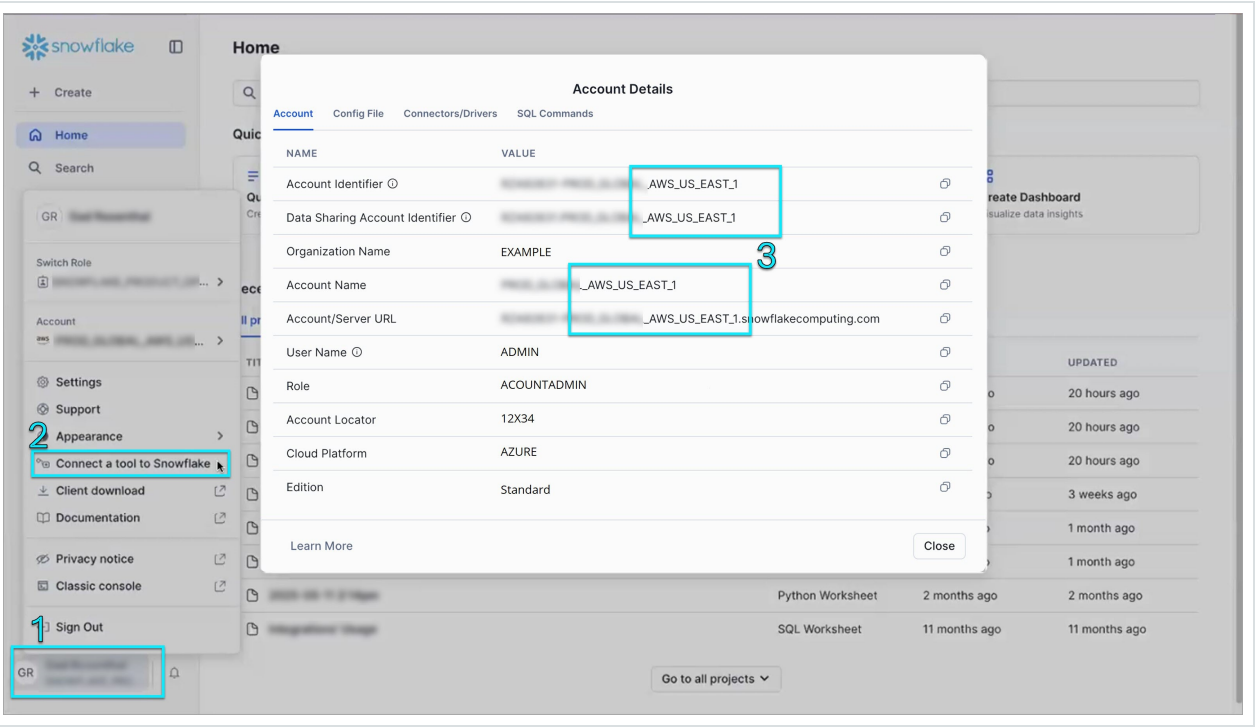
DECLARE
TENABLE_NETWORK_POLICY VARCHAR DEFAULT 'TENABLE_POLICY';
TENABLE_USER VARCHAR DEFAULT '"<paste_user_name_here>"';
BEGIN
EXECUTE IMMEDIATE 'ALTER USER ' || TENABLE_USER || ' SET NETWORK_POLICY=""';
CREATE OR REPLACE NETWORK POLICY IDENTIFIER(:TENABLE_NETWORK_POLICY)
  ALLOWED_IP_LIST=
  (
      '<ip1_core_service, ip2_core_service>',
      '<ip1_data_protection, ip2_data_protection>'
  );
EXECUTE IMMEDIATE 'ALTER USER ' || TENABLE_USER || ' SET NETWORK_POLICY=' || TENABLE_NETWORK_POLICY;
END;
```

4. スクリプトのプレースホルダーを置き換えます。
    1. <paste_user_name_here>:実際の Tenable ユーザー名を入力します(二重引用符で囲まれます)。

       例: TENABLE_USER varchar default '"Pete Mitchell"';
    2. <ip1_core_service, ip2_core_service>: クラウド サイバーエクスポージャー のコアサービス用 IP アドレスからすべての IP アドレスを追加します。
    3. <ip1_data_protection, ip2_data_protection>: [Additional IP addresses for Workload and Data Protection] (ワークロードおよびデータ保護用の追加 IP アドレス) セク

ションで、Snowflake アカウントのリージョンとプロバイダーに一致する IP アドレスのみを追加します。

Snowflake リージョンは、[Account Details] (アカウントの詳細) ウィンドウで確認できます



5. SQLコードを実行します。
6. ネットワークアクセスが機能していることを確認します。問題が解決しない場合は、サポートに問い合わせてください。

Snowflake FAQ とトラブルシューティング

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

この記事の内容

- Snowflake の Tenable One Cloud Exposure への接続に関連するよくあるご質問の一覧です。詳細な統合手順については、Snowflake の接続参照してください。
- アカウントステータスとトラブルシューティング

アクセス許可と統合

Snowflake アカウントを接続して監視するために必要なアクセス許可は何ですか?

回答: 統合中、Tenable には Snowflake 環境をスキャンするために必要なアクセス許可が付与されます。これらには以下が含まれます。

- **MONITOR USAGE (アカウント)**: アカウントレベルの使用量情報を Tenable で表示できるようになります。
- **MONITOR (アカウント)**: アカウントリソースの稼働ステータスとメタデータを Tenable で表示できるようになります。
- **USAGE (Tenable 専用ウェアハウス)**: スキャンに使用されるコンピューティングリソースへのアクセスを許可します。
- **IMPORT SHARE (アカウント)**: 統合を許可し、アカウントレベルで共有データをインポートできます。このアクセス許可は、DSPM オンボーディング時に自動的に付与されます。
- **IMPORTED PRIVILEGES(データベース)**: アカウントレベルの IMPORT SHARE アクセス許可が付与された後に、共有データベースへのアクセスを有効にします。
- **USAGE (データベースおよび現在および将来のすべてのスキーマ)**: データベース構造の可視化を許可します。
- **SELECT (データベースの現在および将来のすべてのテーブル)**: 分類のためにデータ値を読み取る必要があります。
- **SNOWFLAKE.GOVERNANCE_VIEWER (データベース)**: 適用されたオブジェクトタグ、マスキングポリシー、および行アクセスポリシーを検査する場合に必要です。
- **SNOWFLAKE.OBJECT_VIEWER (データベース)**: 包括的な資産検出とインベントリのために、オブジェクトのメタデータに対するアカウント全体の可視化を許可します。
- **SNOWFLAKE.SECURITY_VIEWER (データベース)**: セキュリティリスクを特定するために、ユーザーロール、権限、ネットワーク設定の分析を有効にします。

Snowflake の接続 プロセスの一部として、すべてのアクセス許可が自動的に付与されます。追加の設定は必要ありません。

定期スキャンとメンテナンス

クラウドサイバーエクスポージャーが専用タスクを使用するのはなぜですか? 無効にするとどうなりますか?

回答 クラウドサイバーエクスポージャーは、Snowflakeのスケジュールされたタスクを使用して、新しく検出されたデータベースを自動的に統合します。タスクを無効化または削除するとスキャンの実行が停止し、Tenableがアカウントのデータ保護の検出結果を更新できなくなります。

「データ保護のアクセス許可なし」のステータスを解決するにはどうすればよいですか?

アカウントのステータスがデータ保護のアクセス許可なしの場合、以下の手順を実行します。

- 統合スクリプトを再実行し、必要なロールとアクセス許可を再度適用してください。
- ネットワークアクセスが正しく設定されていて、TenableのIPアドレスが許可されることを確認します。詳細については、ネットワークアクセス権の付与を参照してください。

データベースの範囲と検出

アカウント内スキャンはSnowflakeでサポートされていますか?

いいえ。データリソースのアカウント内スキャンは、Snowflakeでサポートされていません。すべてのスキャンは、Tenable One Cloud Exposureが関連するクラウドリージョンから外部で実行します。

クラウドサイバーエクスポージャーはSnowflakeの外部テーブルをスキャンしますか?

回答: いいえ。外部の表はのスキャンではサポートされていません。

組織支援

クラウドサイバーエクスポージャーはSnowflake組織をサポートしていますか?

クラウドサイバーエクスポージャーは現在、組織レベルの統合をサポートしていません。各Snowflakeアカウントは個別に統合し、必要なアクセス許可を付与する必要があります。

認証とセキュリティ

クラウドサイバーエクスポージャーはSnowflake環境でどのように認証しますか?

クラウドサイバーエクスポージャーは、一意の顧客固有の4096ビット秘密鍵と公開鍵のペアを使用して、Snowflake環境への認証を行います。この安全な鍵ベースの認証は統合プロセス中に確立され、データ分類とインベントリスキャンのための継続的なアクセスを可能にします。

ライセンス

Tenable One Cloud ExposureでSnowflakeスキャンを使用するには、どのようなライセンスが必要ですか?

回答: Snowflakeスキャンは、Enterpriseでのみ利用可能です。別のライセンス層を使用している組織の方で、Snowflakeのサポートを有効したいという場合は、Tenableの担当者にお問い合わせください。詳細については、ライセンスを参照してください。

Snowflake機能サポート

Snowflakeアカウントではどのような クラウドサイバーエクスポージャー機能を利用できますか?

回答 クラウドサイバーエクスポージャーは現在、Snowflakeの**インベントリ**および**データ保護**をサポートしています。CSPM、CIEM、ポリシー機能は現在、Snowflakeでは利用できません。

追加機能や新機能などの拡張サポートをリクエストする場合は、機能リクエストを製品チームに送信してください。

ネットワークアクセス

Springアカウントにネットワーク制限がある場合はどうすればよいですか?

回答: Snowflakeアカウントでネットワーク制限が適用される場合、スキャンを有効にするためにTenable IPアドレスからのアクセスを明示的に許可する必要があります。

必要なスクリプトと手順については、ネットワークアクセスを許可するを参照してください。

アカウントステータスとトラブルシューティング

クラウドサイバーエクスポージャーでは、**[アカウント] > [Snowflake]** ページに各 Snowflake アカウントの **[Status]** が表示されます。これは、たとえば、Tenable がアカウントに接続できるかどうかを示し、統合の問題のトラブルシューティングに役立ちます。

ステータス	説明
接続済み	クラウドサイバーエクスポージャーは Snowflake アカウントに正常に接続されました。
削除しています。これには時間がかかる場合があります...	クラウドサイバーエクスポージャーでアカウントを削除しましたが、プロセスはまだ進行中です。
アクセスが拒否されました	Tenable ユーザーは、無効な認証情報または権限がないため、Snowflake に接続できません。
接続に問題あり	アカウントは接続されていますが、アクセス許可がないために 1 つ以上の機能が動作していません。データ保護のアクセス許可を付与するを参照してください。

IaC

コードリポジトリの接続

これは、リポジトリを Tenable One Cloud Exposure に接続するための統合ガイドです。

- Tenable ですでに接続されているリポジトリを管理する方法については、「コード」を参照してください。
- IaC 検出結果のモニタリングに関するハウツーガイドについては、IaC 検出結果を参照してくださ

い。

- Tenable の CI/CD とコード機能の概要については、「コード」を参照してください。

コードリポジトリのスキャンを開始するには

1. リポジトリの接続。組織を接続して、コードリポジトリ全体を クラウド サイバーエクスポージャー に追加します。
2. リポジトリコード。リポジトリの管理とトラブルシューティング、フォルダー経由でのリポジトリの整理、関連するタスクの実行を行います。
3. IaC 検出結果。インフラのセキュリティに対して予測されるリスクをもたらすコードリポジトリ内の状況を追跡および監視します。

リポジトリの接続

CI/CD の接続する代わりに、組織を接続してコードリポジトリ全体を クラウド サイバーエクスポージャー に追加することもできます。

- Azure Repos 組織の追加
- Bitbucket ワークスペースの追加
- GitHub 組織の追加
- GitLab グループの追加

リポジトリを接続すると、Tenable は関連するサービス (Azure Repos など) に定期的に接続し、最後の接続以降にメイン ブランチへの新しいコミットをチェックします。コミットが存在する場合、Tenable はメイン ブランチのすべてのコードをスキャンし、クラウド サイバーエクスポージャー コンソールに問題を表示します。同じコミットが CI/CD とリポジトリスキャンの両方でスキャンされた場合、両方が別々のスキャンとして表示されます。

> **注意:** 各リポジトリタイプでサポートされている IaC 機能を確認するには、IaC 互換性マトリクス を参照してください。

Azure Repos 組織の追加

Azure Repos 組織を追加して、組織内のコードリポジトリ全体における IaC 関連の問題を完全に可視化します。リポジトリに追加するには、クラウドサイバーエクスポージャー アプリにアクセス許可を付与し、Azure Repos 組織を Tenable に接続します。

必要なアクセス許可

Tenable Azure Repos アプリには、次のアクセス許可が必要です。

- **コード (読み取り)。** コミット、変更セット、ブランチ、およびその他のバージョン管理アーティファクトに関するソースコードとメタデータを読み取る権限を付与します。また、サービスフックを介して、コードを検索し、バージョン管理イベントに関する通知を受け取る権限も付与します。
- **プロジェクトとチーム (読み取り)。** プロジェクトとチームを読む権限を付与します。
- **サインインしてユーザープロファイルを読みます**。ユーザーのアプリへのサインインを許可します。アプリはサインインしたユーザーのプロファイルを読み取ることができます。また、アプリはサインインしているユーザーの基本的な会社情報も読み取ることができます。

Azure Repos 組織に接続するには、次のようにします。

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Azure Repos 組織]** をクリックします。[Add Azure Repos Organization] (Azure Repos 組織の追加) ウィザードが開きます。
3. **管理者の同意を付与** します (ウィザードのステップ 1):
    - **[同意の付与]** をクリックして Azure で Azure Repos アプリを クラウドサイバーエクスポージャー 承認し、必要なアクセス許可を付与します。組織を代表して同意することを許可されたユーザーとしてサインインする必要があります。
    - **[許容]** をクリックします。同意が承認されると、クラウドサイバーエクスポージャー ウィザードにリダイレクトされます。

    > **注意:** Azure ポータルで **Entra ID** > **Enterprise Applications** に移動し、クラウドサイバーエクスポージャー Azure Repos を検索することで、同意が付与されたことを確認できます。
4. [コンソールクラウドサイバーエクスポージャー] **組織を選択します** (ウィザードのステップ 2)。追加する組織をドロップダウンメニューから選択し、以下の設定を行います。

- **フォルダー構造を自動的に更新します**。リポジトリの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます (デフォルトで有効)。詳細は、アカウント階層とフォルダーを参照してください。
- **クラウドからコードまで同期します**。クラウドリソースをコードのオリジンまでトレースします (デフォルトで有効)。詳細については クラウドからコードまで同期 を参照してください。
- **プルリクエストをスキャンします**。すべてのプルリクエストに対して自動セキュリティスキャンを有効にして、セキュリティポリシーに照らしてコード変更を評価します。この機能を有効にすると、定義したスキャン失敗しきい値を満たすか、それを超えるセキュリティ設定ミスが含まれている場合、マージをブロックできます。詳細については、「プルリクエストスキャンを参照してください。
  - [Scan Failure Threshold] (スキャン失敗のしきい値) セクションで、以下のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。
    - このアカウント範囲の親レベルの範囲の設定を**オーバーライド**します。
  - この **設定を有効にした場合** は、ドロップダウンからポリシーの深刻度を選択します。

    > **注意:** この機能は早期リリース版として提供されており、変更される可能性があります。機能およびサポートが制限される場合があります。アクセス権のリクエストやフィードバックの提供については、Tenable の担当者までご連絡ください。

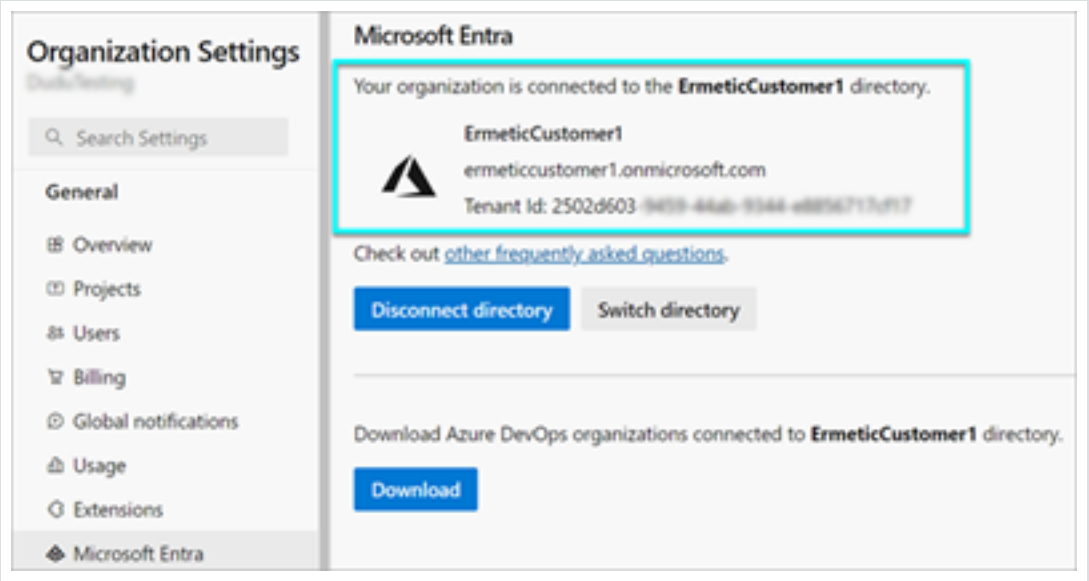
    > **注意:**
    > - 既存の CI/CD 統合がある場合、ここで設定されたスキャン失敗しきい値は、CI/CD パイプラインのしきい値設定をオーバーライドします。
    > - スキャン失敗しきい値は、**Settings > クラウドサイバーエクスポージャー > IaC** で更新できます。
- **[次へ]** をクリックします。

5. (Azure DevOps ポータル) **組織にアクセス許可を付与します** (ウィザードのステップ 3):
   1. Azure DevOps にログインし、左下にある **[組織の設定]** をクリックします。
   2. **[一般 >ユーザー]** に移動し、**[ユーザーの追加]** をクリックします。

3. 次のユーザーの詳細を入力します。

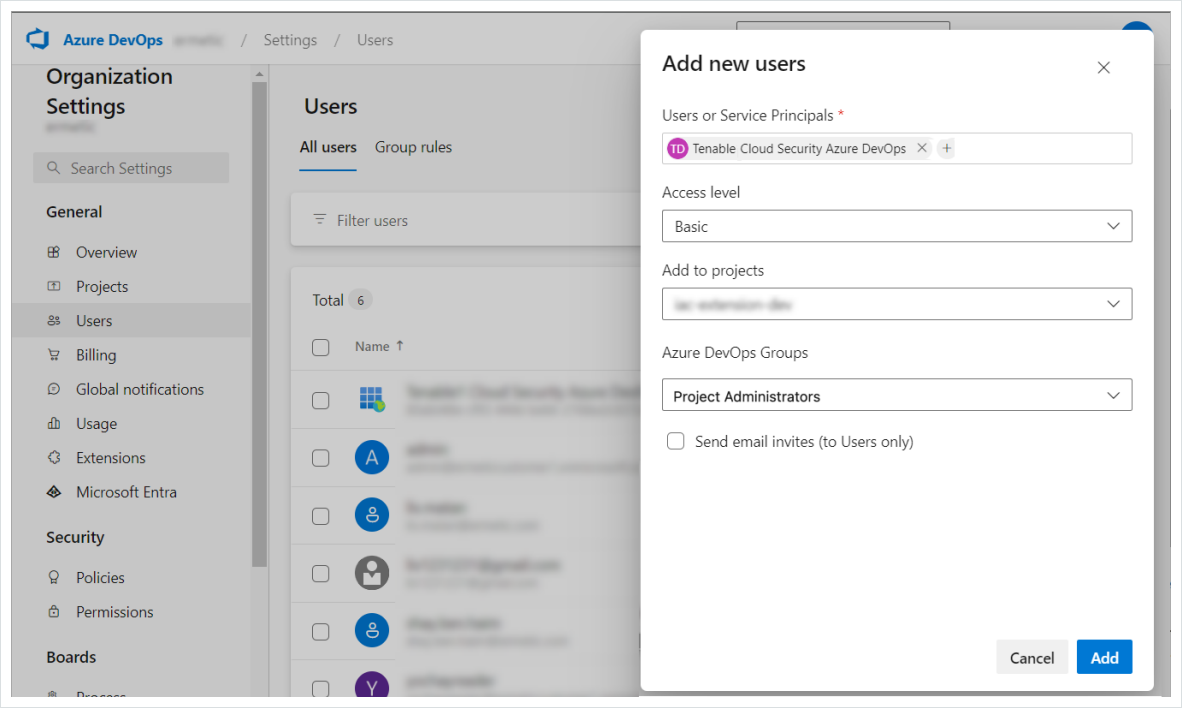
    1. ユーザーまたはサービスプリンシパル: **[クラウド サイバーエクスポージャー Azure DevOps]** を選択し、objectID を含むサービスプリンシパルのポップアップを必ずクリックします。

        このサービスプリンシパルが表示されない場合は、先ほど (ステップ 3) 管理者の同意を付与したときに使用したものと同じ Azure Active Directory (Microsoft Entra) テナントに Azure Repos 組織が接続されていることを確認してください。これは、Azure DevOps ポータルの **[Organization Settings]** > **[General** > **Microsoft Entra]** で確認できます。

    2. アクセスレベル: **[基本]** を選択します。
    3. [Add to projects] (プロジェクトに追加): クラウド サイバーエクスポージャー で使用するプロジェクトを選択します。
    4. Azure DevOps グループ: **[プロジェクト管理者]** を選択します。

5. **[追加]** をクリックします。



6. リポジトリを**選択します** (ウィザードのステップ 4)。スキャン Tenable リポジトリを選択します (許可されたプロジェクト内):
   - **すべてのリポジトリを同期する (推奨)**
   - **特定のフォルダーとリポジトリを含める**
   - **特定のフォルダーとリポジトリを除外する**

   > **注意:**
   > - すべてのリポジトリを同期する場合、またはフォルダー全体を含める/除外する場合、フォルダー内の現在および将来のすべてのリポジトリが含まれるか、または除外されます。
   > - フォルダー内の特定のリポジトリを含める/除外する場合、選択したリポジトリのみが含まれます/除外されます。

7. **[終了]** をクリックします。

Bitbucket ワークスペースの追加

Bitbucket ワークスペースを追加して、ワークスペース内のコードリポジトリ全体における IaC 関連の問題を完全に可視化します。

要件

- Bitbucket Cloud プレミアム プラン
- 次のワークスペースアクセストークンのアクセス許可が必要です。
  - アカウント > **読み取り**
  - 書き込み>リポジトリ
  - プルリクエスト > **書き込み**

ワークスペースを接続するには

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Bitbucket ワークスペース]** をクリックします。[Add Bitbucket Workspace] (Bitbucket Workspace の追加) ウィザードが開きます。
3. **ワークスペースを設定します** (ウィザードのステップ 1):
   1. Bitbucket にログインし、接続するワークスペースのワークスペースページに移動します。
   2. 右上にある **[ワークスペース設定 > Settings]** をクリックします。
   3. サイドバーで、**[セキュリティ]**> **[アクセストークン]** をクリックします。
   4. **[Create Workspace Access Token]** (ワークスペースのアクセストークンを作成) をクリックします。
   5. 次の詳細を入力します。
      - 名前: Bitbucketで クラウド サイバーエクスポージャー アプリケーションに割り当てる名前。
      - 範囲: **書き込み>リポジトリを選択し、書き込み >プルリクエストを選択します。**
   6. **[作成]** をクリックします。
   7. [コピー] ボタンを使用して **ワークスペースアクセストークン** をコピーし、クラウド サイバーエクスポージャー コンソールウィザードに貼り付けます。

8. [Tenable] ウィザードで、次の設定を行います。
    1. **クラウドからコードまで同期します**。クラウドリソースをコードのオリジンまでトレースします (デフォルトで有効)。詳細については クラウドからコードまで同期 を参照してください。
    2. **フォルダー構造を自動的に更新します**。リポジトリの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます (デフォルトで有効)。詳細は、アカウント階層とフォルダーを参照してください。
9. [**次へ**] をクリックします。

4. リポジトリを**選択します** (ウィザードのステップ 2)。スキャン Tenable リポジトリを選択します (許可されたプロジェクト内):
    - **すべてのリポジトリを同期する (推奨)**
    - **特定のフォルダーとリポジトリを含める**
    - **特定のフォルダーとリポジトリを除外する**

    > **注意:**
    > - すべてのリポジトリを同期する場合、またはフォルダー全体を含める/除外する場合、フォルダー内の現在および将来のすべてのリポジトリが含まれるか、または除外されます。
    > - フォルダー内の特定のリポジトリを含める/除外する場合、選択したリポジトリのみが含まれます/除外されます。

5. [**終了**] をクリックします。

GitHub 組織の追加

クラウドサイバーエクスポージャー GitHub アプリをインストールして GitHub リポジトリを追加すると、組織内のコードリポジトリ全体における IaC 関連の問題を完全に可視化できます。リポジトリが GitHub Enterprise Server でセルフホストされている場合、またはデータ常駐のある GitHub Enterprise Cloud でホストされている場合は、組織の追加に進む前にサーバーを クラウドサイバーエクスポージャーに追加する必要があります。

必要なアクセス許可

リポジトリをスキャンし、自動修正機能を使用し、チェックステータス Tenable レポートするには、GitHubアプリに次のアクセス許可が必要です。

- **リポジトリスキャンのアクセス許可**
    - への読み取りアクセス `metadata`
    - への読み取りアクセス `code`
- **自動修正機能のアクセス許可**
    - への書き込みアクセス `code`
    - への書き込みアクセス `commit statuses`
    - への書き込みアクセス `pull requests`
- **プルリクエストステータスレポートアクセス許可**
    - への読み取りと書き込みのアクセス権 `checks`
    - への読み取りアクセス `commit statuses`
    - への読み取りアクセス `pull requests`

GitHub リポジトリを接続するには

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[GitHub 組織]** をクリックします。[GitHub組織] ウィザードが開きます。
3. **GitHub Server を選択します** (ウィザードのステップ 1)。リポジトリがホストされている場所を選択します。
    - **GitHub.com**
    - **GitHub Enterprise Server (セルフホスト型)** または **データレジデンシー (GHE.com) を備えた GitHub Enterprise Cloud**。サーバーがドロップダウンに表示されない場合、組織の追加に進む前に Tenable に追加する必要があります。
4. **GitHub で認証します** (ウィザードのステップ 2)。接続する組織のアプリインストールにアクセスできる GitHub ユーザーで認証します。**[GitHub ユーザーの認証]** をクリックします。
5. **クラウドサイバーエクスポージャーをインストールするアプリ** (ウィザードのステップ 3):
    1. ここをクリックして、クラウドサイバーエクスポージャーアプリページに移動します。
    2. **[インストール/構成]** をクリックします。

3. [Install クラウド サイバーエクスポージャー] (インストール) ページで組織名をクリックします。
4. すべてのリポジトリに Tenable アクセスを付与する場合は、**[すべてのリポジトリ]** を選択します。それ以外の場合は、**[選択したリポジトリのみ]** を選択し、少なくとも 1 つのリポジトリを選択します。
5. **[インストール]** をクリックします。必要に応じてパスワードを入力し、アプリがインストールされていることを確認します。上記のアプリに必要なアクセス許可の完全なリストを確認できます。
6. [クラウド サイバーエクスポージャー コンソール] ウィザードで、**[次へ]** をクリックします。

6. **組織を選択します** (ウィザードのステップ 4)。追加する組織をドロップダウンメニューから選択し、次の設定を行います。
   - **フォルダー構造を自動的に更新します**。リポジトリの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます (デフォルトで有効)。詳細は、アカウント階層とフォルダーを参照してください。
   - **クラウドからコードまで同期します**。クラウドリソースをコードのオリジンまでトレースします (デフォルトで有効)。詳細については クラウドからコードまで同期 を参照してください。
   - **プルリクエストをスキャンします**。**すべての**プルリクエストに対して自動セキュリティスキャンを有効にします。この機能を有効にすると、定義したスキャン失敗しきい値を満たすか、それを超えるセキュリティ設定ミスが含まれている場合、マージをブロックできます。詳細については、「プルリクエスト スキャンを参照してください。
     - [組織] ツリーのドロップダウンで、[コード] アカウントの範囲 を選択します。
     - [Scan Failure Threshold] (スキャン失敗のしきい値) セクションで、以下のいずれかを選択します。
       - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

         > **注意:** 組織全体を範囲として選択した場合、[継承] オプションは使用できません。

       - 親レベルの範囲の設定を、このアカウント範囲固有の設定 (**有効** / **無効**) で**オーバーライド**します。この固有の構成は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。
     - この **設定を有効にした場合** は、ドロップダウンからポリシーの深刻度を選択します。

> **注意:** この機能は早期リリース版として提供されており、変更される可能性があります。機能およびサポートが制限される場合があります。アクセス権のリクエストやフィードバックの提供については、Tenable の担当者までご連絡ください。

> **注意:**
> - 既存の CI/CD 統合がある場合、ここで設定されたスキャン失敗しきい値は、CI/CD パイプラインのしきい値設定をオーバーライドします。
> - スキャン失敗しきい値は、**Settings > クラウドサイバーエクスポージャー > IaC** ::: で更新できます

7. **[次へ]** をクリックします。
8. リポジトリ**を選択します** (ウィザードのステップ 5)。スキャン Tenable リポジトリを選択します。
    - **すべてのリポジトリを同期する (推奨)**
    - **特定のフォルダーとリポジトリを含める**
    - **特定のフォルダーとリポジトリを除外する**

    > **注意:**
    > - すべてのリポジトリを同期する場合、またはフォルダー全体を含める/除外する場合、フォルダー内の現在および将来のすべてのリポジトリが含まれるか、または除外されます。
    > - フォルダー内の特定のリポジトリを含める/除外する場合、選択したリポジトリのみが含まれます/除外されます。
9. **[終了]** をクリックします。

GitHub Enterprise Server の追加

リポジトリが GitHub Enterprise Server でセルフホストされている場合、またはデータ所在地 (GHE.com) のある GitHub Enterprise Cloud でホストされている場合は、組織の追加に進む前にサーバーを クラウドサイバーエクスポージャー に追加する必要があります。

この統合では以下がサポートされます。

- GitHub Enterprise Server、インターネットに接続し、ネットワーク分離の両方。ネットワーク分離サーバーの操作の詳細については、「 ネットワーク分離されたサーバーの接続 を参照してください。
- EU リージョンにデータ所在地を持つ GitHub Enterprise Cloud。

企業で IP 許可リストを使用している場合は、リージョンの IP アドレス クラウドサイバーエクスポージャー を追加します。「許可が必要な Tenable IP アドレス」を参照してください。

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**GitHub Enterprise** をクリックします。[GitHub Enterprise の追加] ウィザードが開きます。
3. **サーバーの詳細を設定します** (ウィザードのステップ 1):
    1. クラウドサイバーエクスポージャーコンソールに表示する**サーバーの名前を入力します**。
    2. Tenable のサーバーへの接続方法を選択します。サーバーがネットワークから分離されている場合、Tenable エンドポイントコネクタを使用して接続を確立します。データ所在地のある GitHub Enterprise Cloud の場合は、**[エンドポイント (インターネット向け)]** を選択します。エンドポイントコネクタも SSL 証明書の設定も必要ありません。
        - **エンドポイント (internet-facing)**。GitHub Enterprise Server エンドポイントを入力します (`https://` プロトコルプレフィックスなし)。たとえば、「`github.tenable.com`」や「`192.82.156.1:8443`」と入力します。
        - **エンドポイントコネクタ (ネットワーク分離)**。ドロップダウンから関連するコネクタを選択します。このオプションが無効になっている場合は、まだコネクタを追加していないということです。追加方法については、「ネットワーク分離されたサーバーの接続 を参照してください。
    3. サーバーで SSL が有効になっている場合は、**すべてのサーバー SSL 証明書を受け入れる** にチェックを入れます。
    4. クラウドサイバーエクスポージャーコンソールで、**[次へ]** をクリックします。
4. **アプリの詳細を設定します** (ウィザードのステップ 2):
    1. クラウドサイバーエクスポージャー GitHub アプリをホストする組織の **[アプリケーション組織名] (Application Organization Name)** を入力します。これは、Tenable に接続した組織とは異なる場合があります。
    2. **[GitHub アプリの登録]** をクリックします。

> **注意:** 組織を クラウドサイバーエクスポージャー に正常に追加している場合、GitHub アプリは すでに設定されているため、この手順をスキップできます。

3. (GitHub)開いた [新しい GitHub アプリの登録] ページで、下にスクロールして **[GitHub アプリの作成]** をクリックします。

   > **重要:** 自動入力されている設定を編集または変更しないでください。統合が機能しなくなる可能性があります。

   > **注意:** クラウドサイバーエクスポージャー GitHub アプリに関する以下の詳細は、GitHub Enterprise Server または GHE.com 組織の設定 (**Settings** > **[開発者設定]** > **[GitHubアプリの一般]** ページで確認できます)。

4. App ID を入力します。
5. **クライアント ID** を入力します。
6. **クライアントシークレット**を生成してコピーし、ウィザードに入力します。
7. **プライベートキー**を生成してダウンロードし、ウィザードに入力します。
8. **[終了]** をクリックします。

5. 正常に終了したら、GitHub 組織の追加できます (まだ追加していない場合)。

GitLab グループの追加

GitLab グループを追加して、グループ内のコードリポジトリ全体における IaC 関連の問題を完全に可視化します。リポジトリが **GitLab Self-Managed Server** でセルフホストされている場合は、組織の追加に進む前にサーバーを クラウドサイバーエクスポージャーに追加する必要があります。

要件:

- プレミアムSaaSプラン以上

GitLab グループを接続するには

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。

2. 統合ライブラリで、**[GitLab Group]** をクリックします。[Add GitLab Group] (GitLab グループの追加) ウィザードが開きます。
3. **GitLab Server を選択します** (ウィザードのステップ 1)。プロジェクトがホストされている場所を選択します。
    - **GitLab.com**
    - **GitLab セルフマネージドサーバー**。サーバーがドロップダウンに表示されない場合は、組織の追加に進む前に [クラウドサイバーエクスポージャーに追加] を行う必要があります。
4. **[次へ]** をクリックします。
5. **グループを設定します** (ウィザードのステップ 2):
    1. GitLab にログインし、**[グループ]** をクリックします。
    2. 接続するルート、親グループをクリックします。サブグループは接続できません。
    3. 左側のメニューで、**[Settings > アクセストークン]** をクリックします。
    4. **[新しいトークンの追加]** をクリックします。
    5. 次の詳細を入力します。
        1. [Token name] (トークン名)。
        2. [Expiration date] (有効期限日): この日付以降、トークンの更新と Tenable の設定の更新が必要になります。
        3. ロールの選択: **[開発者]** を選択します。
        4. [スコープの選択]: **api** を選択します。
    6. **[グループアクセストークンの作成]** をクリックしてトークンをコピーします。
    7. [クラウドサイバーエクスポージャー] コピーした **ルートグループのアクセストークン** を入力します。
    8. [Tenable] ウィザードで、次の設定を行います。
        - **クラウドからコードまで同期します**。クラウドリソースをコードのオリジンまでトレースします (デフォルトで有効)。詳細については クラウドからコードまで同期 を参照してください。
        - **フォルダー構造を自動的に更新します**。リポジトリの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます (デフォルトで有効)。詳細は、アカウント階層とフォルダーを参照してください。

9. **[次へ]** をクリックします。

6. **プロジェクトを選択します** (ウィザードのステップ 3): Tenable スキャンするプロジェクトを選択します。
    - **すべてのリポジトリを同期する (推奨)**
    - **特定のフォルダーとリポジトリを含める**
    - **特定のフォルダーとリポジトリを除外する**

    > **注意:**
    > - すべてのリポジトリを同期する場合、またはフォルダー全体を含める/除外する場合、フォルダー内の現在および将来のすべてのリポジトリが含まれるか、または除外されます。
    > - フォルダー内の特定のリポジトリを含める/除外する場合、選択したリポジトリのみが含まれます/除外されます。

7. **[終了]** をクリックします。

GitLab セルフマネージドサーバーの追加

グループが GitLab Self-Managed Server でセルフホストされている場合は、グループの追加に進む前にサーバーを クラウドサイバーエクスポージャー に追加する必要があります。

この統合は、インターネット向けサーバーとネットワーク分離されたサーバーの両方をサポートしています。ネットワーク分離サーバーの操作の詳細については、「 ネットワーク分離されたサーバーの接続 を参照してください。

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[GitLab Self-Managed Server]** をクリックします。[Add GitLab Self-Managed Server] (GitLab Self-Managed Server の追加) ウィザードが開きます。
3. **サーバーの詳細を設定します** (ウィザードのステップ 1):
    1. クラウドサイバーエクスポージャーコンソールに表示する**サーバーの名前を入力します**。
    2. Tenable のサーバーへの接続方法を選択します。サーバーがネットワークから分離されている場合、Tenable エンドポイントコネクタを使用して接続を確立します。
        - **エンドポイント (internet-facing)**。GitLab Self-Managed Server エンドポイントを入力します (`https://` プロトコルプレフィックスなし)。たとえば、「`gitlab.tenable.com`」や

「192.82.156.1:8443」と入力します。

- **エンドポイントコネクタ (ネットワーク分離)。**ドロップダウンから関連するコネクタを選択します。このオプションが無効になっている場合は、まだコネクタを追加していないということです。追加方法については、「ネットワーク分離されたサーバーの接続を参照してください。

3. サーバーで SSL が有効になっている場合は、**すべてのサーバー SSL 証明書を受け入れる**にチェックを入れます。
4. クラウドサイバーエクスポージャーコンソールで、**[次へ]** をクリックします。

4. 正常に終了すると、GitLab グループの追加できます (まだ追加していない場合)。

クラウドからコードまで同期

問題をコードのオリジンまでトレースするには、コードリポジトリをクラウドサイバーエクスポージャーに接続して、クラウドリソースに関連付けられたコードを同期します (クラウドからコードまで)。

> **注意:** コードまで問題をトレースするのにサポートされているプラットフォーム/リポジトリについては、IaC 互換性マトリクスを参照してください。

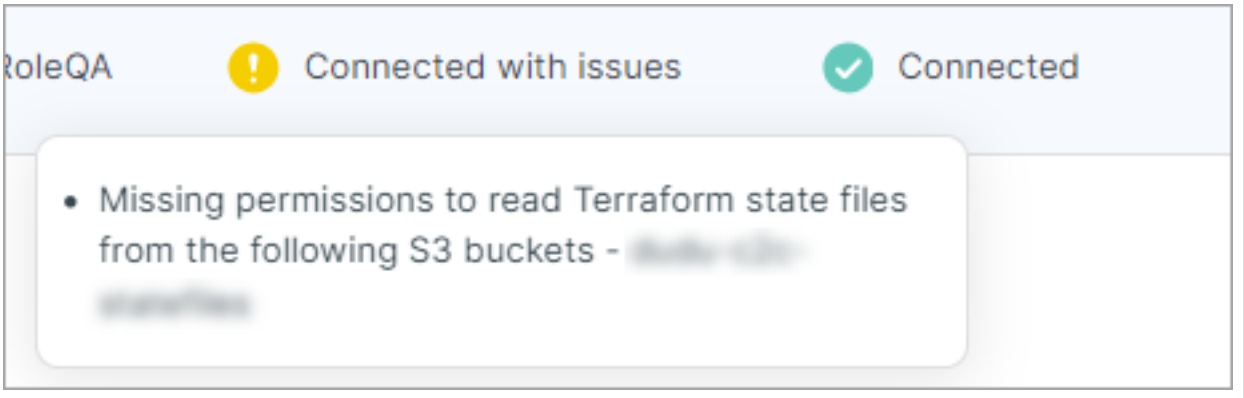
Terraform コードの状態データファイルを保存しているクラウドストレージリソース (S3 バケットなど) を読み取るアクセス許可を Tenable に付与します。状態ファイルには、データファイルの保存を定義するバックエンドが設定されている必要があります。

- AWS: Terraform のアクセス許可を付与する
- Azure: Terraform のアクセス許可を付与する
- GCP: Terraform のアクセス許可を付与する

AWS: Terraform のアクセス許可を付与する

1. トレースする Terraform の状態データを含む S3 バケットがすべてクラウドサイバーエクスポージャーに対して可視化されることを確認します。バケットは、Tenable に接続されているアカウントにある必要があります。

2. コードリポジトリをクラウド サイバーエクスポージャー に接 続します。[Sync Cloud to Code] (クラウド からコードまで同 期) チェックボックスが有 効になっていることを確 認します。
3. **AWS> [Settings** > **Accounts]** に移 動し、S3バケット があるアカウントを見 つけます。[Status] (ステータス) 列 は、関 連 するバケット のリストとともに、Terraform の状 態 ファイルを読み取 るためのアクセス許 可 がないことを示しているはずです。



4. アカウント の横 にある三 点 リーダーアイコンをクリックし、**[編 集]** をクリックします。
5. ウィザード で、[Next] (**次 へ**) をクリックしてステップ 2 (アクセス許 可) に移 動し、**Terraform (S3)** を有 効 にします。接 続 済 みのアカウント に関 連 付 けられているバケット のリスト が表 示されます。
6. [Next] (**次 へ**) をクリックしてステップ 3 (IAM ロール) に移 動し、表 示される **Terraform アクセス許 可 ポリシー** JSON (3B) をコピーします。
7. AWS 管 理コンソールで、**[IAM]** > **[ロール]** に移 動し、アカウント を接 続したときに作 成したロールを検 索します (ロール名 は クラウド サイバーエクスポージャー ウィザード のステップ 3 で表 示されます)。
8. [アクセス許 可] タブで、**[アクセス許 可 の追 加]** > **[インラインポリシーの作 成]** をクリックします。
9. 先 ほどコピーしたポリシーを [JSON] エディター に貼り付 けます。
10. **[次 へ]** をクリックして、ポリシーの作 成を完 了します。

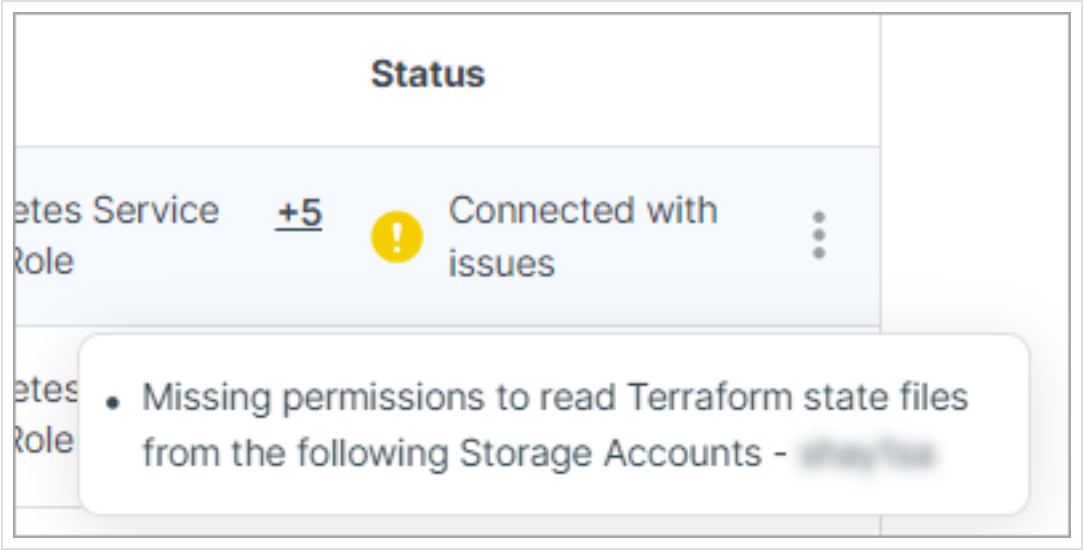
JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>",
        "arn:aws:s3:::<bucket_name>/*",
      ]
    }
  ]
}
```

Azure: Terraform のアクセス許可を付与する

1. トレースする Terraform の状態データを含む Blob コンテナがすべて クラウド サイバーエクスポージャー に対して可視化されることを確認します。コンテナは、Tenable に接続されたサブスクリプションに含まれている必要があります。
2. コードリポジトリをクラウド サイバーエクスポージャー に接続します。[Sync Cloud to Code] (クラウドからコードまで同期) チェックボックスが有効になっていることを確認します。
3. **Azure > Settings > アカウント** に移動し、Blob コンテナがあるサブスクリプションを見つけます。[Status] (ステータス) 列は、Blob コンテナがある関連するストレージアカウントのリストとともに、Terraform の状態ファイルを読み取るためのアクセス許可がないことを示しているはずです。

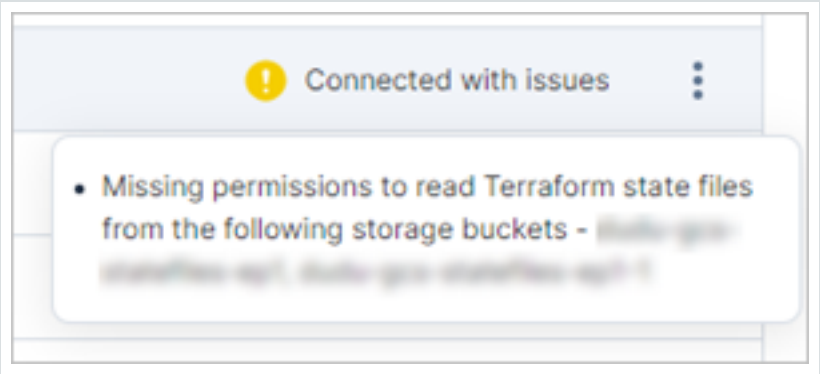


4. サブスクリプションの横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。

5. ウィザードで、[Next] (**次へ**) をクリックしてステップ 3 (アクセス許可) に移動し、 **Terraform (Blob コンテナ)** を有効にします。接続されているサブスクリプションに関連付けられている Blob コンテナのリストが表示されます。ストレージアカウントと Blob コンテナ名をコピーします。
6. Azure ポータルで、前の手順で一覧表示されたストレージアカウントに移動します。
7. [データストレージ] の下にある **[コンテナ]** に移動し、クラウド サイバーエクスポージャー ウィザードに一覧表示されている Blob コンテナをクリックします。
8. **[アクセス制御 (IAM)]** に移動し、**[追加]** > **[ロール割り当ての追加]** をクリックします。
9. ウィザードのリストから **ストレージ BLOB データ閲覧者** ロールを検索して選択し、**[次へ]** をクリックします。
10. **[+ メンバーを選択する]** をクリックします。
11. **クラウド サイバーエクスポージャー コネクタ** を検索して選択し、**[選択]** をクリックします。
12. **[次へ]** をクリックし、**[レビューと割り当て]** をクリックして終了します。追加するすべてのロールに対してこのステップを繰り返します。

GCP: Terraform のアクセス許可を付与する

1. トレースする Terraform の状態データを含むバケットがすべて クラウド サイバーエクスポージャーに対して表示されていることを確認します。バケットは、Tenable に接続されているプロジェクト内にある必要があります。
2. コードリポジトリをクラウド サイバーエクスポージャー に接続します。[Sync Cloud to Code] (クラウドからコードまで同期) チェックボックスが有効になっていることを確認します。
3. **GCP** > **[Settings > Accounts]** (アカウント) に移動し、バケットがあるプロジェクトを見つけます。[Status] (ステータス) 列は、関連するバケットのリストとともに、Terraform の状態ファイルを読み取るためのアクセス許可がないことを示しているはずです。



4. アカウントの横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
5. ウィザードで、[Next] (**次へ**) をクリックしてステップ 3 (アクセス許可) に移動し、**Terraform の状態 (ストレージバケット)** を有効にします。接続済みのアカウントに関連付けられているバケットのリストが表示されます。
6. **[次へ]** を 2 回クリックして、手順 5 (ロールの割り当て) に移動します。以降の手順でここの情報が必要になるため、このページは開いたままにしておきます。
7. Google Cloud コンソールで、**[Cloud Storage > Buckets]** に移動します。
8. Tenableウィザードのステップ 5 (ロールの割り当て) で一覧表示されているバケットの名前の横にあるボックスにチェックを入れます。
9. 上部にある [buckets selected] (選択済みのバケット) バーで、**[Permissions]** をクリックします。
10. 右側のサイドビューで、**[プリンシパルの追加]** をクリックします。
11. Tenableウィザードの値のステップ 5 (ロールの割り当て) にリストされているサービスアカウントのメール値をコピーして、[新しいプリンシパル] フィールドに貼り付けます。
12. 次のロールをコピーして [ロール] フィールドに 1 つずつ貼り付けます。追加のロールごとに **[+ 別のロールを追加]** をクリックします。
    - `Storage Insights Collector Service`
    - `Storage Object Viewer`
13. **[保存]** をクリックします。
14. (クラウドサイバーエクスポージャーコンソール) ウィザードで **[次へ]** (Next) をクリックし、**[完了]** (Finish) をクリックします。

プルリクエストスキャン

設定ミスが本番環境に反映されるのを防ぐには、開発者のワークフロー内ですべてのプルリクエストを直接スキャンして、セキュリティゲートを自動化します。

機能の詳細については、「プルリクエストスキャン

セットアップと要件

PR スキャンを有効にし、セキュリティゲートとして適用するには、次の要件が満たされていることを確認します。

コードリポジトリ	必要なアクセス許可	ゲートに必要な設定
GitHub	読み取り/書き込みアクセス	リポジトリルールセットを作成し、**[ステータス チェックに合格する]** を選択します。Tenable スキャンステータスを必須要件として追加します。
Azure DevOps (ADO)	• 読み取り/書き込みアクセス。 • **プロジェクト管理者** ロールが必要です。	ブランチ保護設定にステータスポリシーを追加します。**continuous-integration/TenableCloudSecurity** オプションを選択し、**[必須]** に設定します。

仕組み

Tenable は、イベント駆動型アーキテクチャを使用して Tenable のインフラ上のコードをスキャンするため、ローカルのコンピューティングリソースが不要になります。

1. **イベントトリガー**: 統合を有効にすると、Tenable はリポジトリに Webhook を作成し、新しい PR または更新された PR をプラットフォームに通知します。

2. **リモートスキャンの実行**: イベントを受信すると、Tenable はパイプラインを手動で設定しなくても、コードを安全に複製して分析します。
3. **結果の配信**: スキャン結果はクラウドサイバーエクスポージャーコンソールに報告され、PR 内でインラインコメントとして直接投稿されます。

> **注意:** PR スキャンはコードの差分のみを評価してスピードと開発者の効率を最大化しますが、標準リポジトリスキャンはリポジトリ全体を評価します。

プルリクエストスキャンを無効にする

特定のリポジトリのスキャンを無効にする必要がある場合、または統合を削除する必要がある場合

1. **設定を無効に**します。特定のリポジトリのクラウドサイバーエクスポージャーコンソール内の [プルリクエストスキャン] 設定をオフにします。
2. **Webhook の削除**: 統合が無効化されると、Tenable はコードリポジトリ用に作成された Webhook を自動的に削除します。

CI/CD の接続

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

これは、CI/CD パイプラインを Tenable に接続するための統合ガイドです。

- Tenable の CI/CD とコード機能の概要については、「コードを参照してください。
- コードのスキャンに関するハウツーガイドについては、「 Code CI/CD」を参照してください。

CI/CD スキャンを開始する方法

1. パイプラインの接続。CI/CD パイプラインを Tenable One Cloud Exposure に接続します。
2. スキャンの設定。Tenable が環境をスキャンする方法を微調整します。

パイプラインの接続

CI/CD パイプラインを クラウドサイバーエクスポージャー に接続し、関連するコードリポジトリへのアクセスを許可します。

- Azure Pipelines の追加
- GitHub アクションを追加する
- GitLab パイプラインの追加
- Jenkins パイプラインの追加
- Terraform Cloud Run タスクの追加
- 別のパイプラインを追加する

個別のパイプラインを追加するだけでなく、コードリポジトリの接続Tenable に接続することもできます。

重要: 各パイプラインでサポートされている IaC 機能を確認するには、IaC 互換性マトリクスを参照してください。

パイプラインの接続について

必要な クラウド サイバーエクスポージャー ユーザーロール: クラウド サイバーエクスポージャー コンソールを使用してパイプラインを接続するには、クラウド サイバーエクスポージャー の管理者ロールが必要です。

クラウド サイバーエクスポージャー コンソールの関連するウィザードの手順に従って、使用するパイプラインの統合を追加します。パイプラインを接続するために必要なステップはベンダーごとに異なりますが、概略としては、ほとんどのベンダーで次の手順が含まれます。

1. API トークンを作成し、スキャン結果を Tenable に報告します。
2. 環境変数を追加し、スキャンをカスタマイズして、基本的なレポート機能を提供します。
3. パイプラインにステップを追加して、**スキャン** 自体を実行したり、クラウドリソースに関連付けられたコードを **同期** して、それらのリソースをオリジンまでトレースしたりします (クラウドからコードまで)。

   スキャン結果にスキャンに関連するコミット情報を含める場合は、リポジトリ (git) ルートのコンテキストからスキャナーを実行する必要があります。この設定の詳細については、「Configure Scan Settings」を参照してください。たとえば、GitHub アクションパラメーターでは、これは `skip-code-commit-history` パラメーターによって制御されます。

パイプラインを Tenable に接続した後、**[Settings > Integrations]** (統合) ページで関連タイルをクリックすると、統合されたパイプラインを表示できます。各パイプラインについて、API トークン**パラメーターの名前**、

Tenable で**作成された**日時、前**回使用**された日時 (API キーの使用状況を監視するため) を確認できます。

範囲指定された CI/CD パイプラインのサポート

Tenable は、ルートの「組織」範囲より下のレベルの CI/CD パイプライン統合をサポートします。この更新により、サブユニットは、より広い組織に影響を与えない明確に定義された範囲を使用して、CI/CD スキャンプロセスを個別に管理できるようになります。

ルートの「組織」範囲より下のレベルで CI/CD パイプラインをスキャンする方法

1. コンソール内クラウドサイバーエクスポージャー、**[Settings** > **Integrations]** に移動します
2. (オプション)[組織]ドロップダウンで **[コード]** 範囲を選択します。
3. 関連する CI/CD 統合を追加します。

> **注意:**
>
> - クラウドサイバーエクスポージャーコンソールで作成された API トークンを使用して、Git プロバイダー内でスキャンのスコープを設定します。
> - CI/CD 統合は、**コード** ルートフォルダーの下の任意の範囲で設定できます。

機能の動作:

- **Git 組織**: リポジトリが Git プロバイダーで指定された組織またはサブグループに属している場合にのみ、スキャンが承認されます。
- **手動フォルダーの範囲**: スキャンは、リポジトリが Git プロバイダーで定義されたフォルダーの下にネストされている場合にのみ承認されます。
- **リポジトリの範囲**: スキャンは、テナントにすでに接続されている特定のリポジトリに対してのみ承認されます。

この機能を使用すると、チームは、より広い組織環境に影響を与えたり、アクセスする必要とせずに、フォルダーやビジネス単位などの特定の範囲内で CI/CD スキャンを設定して実行できます。

Azure Pipelines の追加

次の目的へのパイプラインの追加

- インフラのコード化 (IaC) パイプラインを**スキャンして**セキュリティ問題を検出します。
- クラウドリソースに関連付けられたコードを**同期**して、それらのリソースをオリジンまで**トレース**します (クラウドからコードまで)。

Azure Pipelines でパイプラインを追加した後、Azure Pipelines パラメーターを使用して、スキャン/同期設定を構成し、クラウドサイバーエクスポージャー が環境をスキャンする方法を微調整できます。

要件:

- `Node.js` と `npm` をビルドエージェントにインストールする必要があります。

  > **注意:** Microsoft がホストするエージェントにはデフォルトで含まれていますが、セルフホストのビルドエージェントを使用している場合は、環境の PATH 変数で明示的にインストールまたはアクティブ化する必要があります。これを行うには、Microsoft の NodeTool タスクを追加します。行わなかった場合、以下のエラーが発生する可能性があります。`Parameter 'toolPath' cannot be null or empty`

- Docker をインストールする必要があります。詳細は関連する Azure ドキュメントを参照してください。

Azure Pipelines を使用してパイプラインを追加するには:

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Integrations]** に移動し、**[Add Integration]** をクリックします。
   統合ライブラリ、**[Azure Pipeline の追加]** をクリックします。[Add Azure pipeline] (Azure Pipeline の追加) ウィザードが開きます。
2. **API トークンを作成します** (ウィザードのステップ 1):
   - スキャン結果を Tenable に報告するために、スキャナーには API トークンパラメーターが必要です。
   - トークンを作成するには、「**トークン名**」を入力し、「**次へ**」をクリックします。
3. **API トークンを保存します** (ウィザードのステップ 2)。生成された**トークン**をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。

4. **TenableをインストールするAzure DevOps 拡張機能** (ウィザードのステップ 3):
    1. このリンクをクリックして、Visual Studio マーケットプレースから拡張機能にアクセスします。
    2. **[Get it Free]** をクリックします。拡張機能の使用に追加料金はかかりません。
    3. 関連する Azure DevOps 組織を選択し、**[インストール]** をクリックします。
    4. これで拡張機能がインストールされたので、**[組織に進む]** をクリックして Azure DevOps サイトに移動できます。
5. (推奨) **シークレット変数を追加します** (ウィザードのステップ 4)。UI を使用してシークレット変数を設定するには、次の手順に従います。

    > **注意:** Tenable の API トークンを保護するには、シークレット変数、または代替シークレットストア (現在使用している場合) のいずれかを使用することをお勧めします。Azure Pipelines 変数は、Tenable のスキャンの利用方法に応じてさまざまな範囲で保存できます。Tenable のトークンは、IaC コードとともにリポジトリにリンクされたワークフローのみに関連付けることが推奨されていますが、必須ではありません。

    1. Azure DevOps にログインし、**[パイプライン]** をクリックします。
    2. 関連するパイプラインを選択し、**[編集]** をクリックします。
    3. **[変数]** をクリックします。
    4. プラス記号 (+) または [New variable] (新しい変数) をクリックします
    5. 以下の詳細を入力し、**[OK]** をクリックします。
        - **名前**を **TENABLE_API_TOKEN** に設定します。
        - 前のステップで作成したトークンを **[値]** として貼り付けます。
        - **[Keep this value secret]** にチェックを入れます。

    完了したら、クラウドサイバーエクスポージャーコンソールウィザードの **次へ** をクリックして続行します。
6. **タスクを追加します**。関連するタスクを Azure Pipelines に追加します (ウィザードの手順 5)。
    - **IaC スキャン**IaC をスキャンしてスキャン結果を分析するには、次のタスクを Azure Pipeline に追加します。

1. Azure DevOps にログインし、**[パイプライン]** をクリックします。
2. 関連するパイプラインの横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
3. コードで、Tenable のタスクを追加するステージを選択します。
4. タスクアシスタントで、**[クラウドサイバーエクスポージャー IaC Scan]** タスクを検索してクリックします。
5. タスクを追加するには、これらの値を入力してから、**[追加]** をクリックします。
    - API トークン: **$(TENABLE_API_TOKEN)**
    - API URL: **https://app.tenable.com/**
    - 必要に応じて、**任意の詳細** 設定を使用します (詳細については、「Azure Pipelines パラメーター を参照してください)。
6. 更新されたパイプライン YAML を**保存**します。スキャンがトリガーされると、[CI/CD] にスキャン結果が表示されます。
7. コンソールクラウドサイバーエクスポージャーウィザードで **[次へ]** をクリックします。

- **IaC 同期**。クラウドリソースに関連付けられているコードを同期し、それらのリソースをオリジンまでトレースする (クラウドからコードまで) には、次のタスクを Azure pipeline に追加します。
    1. Azure DevOps にログインし、**[パイプライン]** をクリックします。
    2. 関連するパイプラインの横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
    3. コードで、Tenableタスクを追加するステージを選択します。このタスクは、「terraform apply」ステージ内の「apply」コマンドの後に追加する必要があります。
    4. タスクアシスタントで、**[クラウドサイバーエクスポージャー IaC Terraform の同期]** タスクを検索してクリックします。
    5. タスクを追加するには、これらの値を入力してから、**[追加]** をクリックします。
        - API トークン: **$(TENABLE_API_TOKEN)**
        - API URL: **https://app.tenable.com/**

- 必要に応じて、**任意の詳細** 設定を使用します (詳細については、「Azure Pipelines パラメーター を参照してください)。

6. 更新されたパイプライン YAML を**保存**します。同期がトリガーされたら、クラウド サイバーエクスポージャー に IaC ラベルでタグ付けされたリソース/検出結果が表示されます。関連するリソースの [Inventory] (インベントリ) ビューに [IaC] タブがあり、関連するコード スニペット が表示されます。

7. コンソール クラウド サイバーエクスポージャー ウィザード で、**[完了]** をクリックします。

Azure Pipelines 用の Tenable Step

次の手順は、スキャン結果を クラウド サイバーエクスポージャー に報告するために使用されます。このステップは、Tenableのタスクをパイプラインに追加すると自動的に追加されます (Azure Pipelines の追加)。

YAML

```
jobs:
  - job: ermetic_scan
    pool:
      vmImage: ubuntu-latest
    steps:
        - task: ErmeticIacScan@1
          inputs:
            apiToken: '$(TENABLE_API_TOKEN)'
            apiUrl: 'https://app.tenable.com/'
```

GitHub アクションを追加する

クラウド サイバーエクスポージャーGitHubアクションを使用して、次のことができます。

- インフラのコード化 (IaC) パイプラインを**スキャンして**セキュリティ問題を検出する
- クラウド リソースに関連付けられたコードを**同期**して、それらのリソースをオリジンまで**トレース**します (クラウド からコード まで)。

アクションを追加した後、GitHubアクション パラメーター を使用して、スキャン/同期設定を行い、Tenable が環境をスキャンする方法を微調整できます。

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**GitHub Actions** をクリックします。[Add GitHub Actions] ウィザードが開きます。
3. **APIトークンを作成します** (ウィザードのステップ 1):
    - スキャン結果を Tenable に報告するために、GitHubアクションにAPIトークンパラメーターが必要です。
    - トークンを作成するには、「**トークン名**」を入力し、「**次へ**」をクリックします。
4. **APIトークンを保存します** (ウィザードのステップ 2)。生成された**トークン**をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。
5. (推奨) **GitHub シークレットを追加します** (ウィザードのステップ 3)。GitHub リポジトリで新しいシークレットを作成するには、以下の手順に従います。

    > **注意:** Tenable の APIトークンを保護するには、GitHub アクションシークレット、または他のシークレットストア (現在使用している場合) のいずれかを使用することをお勧めします。GitHub シークレットは、Tenable のスキャンの利用方法に応じて複数のレベルで保存できます。Tenable のトークンは、IaC コードとともにリポジトリにリンクされたワークフローのみに関連付けることが推奨されていますが、必須ではありません。

    1. GitHub.com から、リポジトリのメインページに移動します。
    2. リポジトリ名の下にある **[Settings]** をクリックします。
    3. サイドバーの「セキュリティ」セクションで、「**シークレット**」を選択し、「**アクション**」をクリックします。
    4. **[新しいリポジトリシークレット]** をクリックします。
    5. [名前] 入力ボックスに「**TENABLE_API_TOKEN**」と入力します。
    6. 前のステップで作成したトークンの値を入力します。
    7. **[シークレットの追加]** をクリックします。

    完了したら、クラウドサイバーエクスポージャーコンソールウィザードの **次へ** をクリックします。
6. **アクションを追加します** (ウィザードのステップ 4)。スキャン結果を生成するには、関連するアクションを GitHub ワークフローに追加します。

- **IaC スキャン** IaC をスキャンするには、次のアクションを GitHub ワークフロー に追加します (必要に応じて調整します)。

  YAML

  ```
  steps:
  - uses: actions/checkout@v3
  - name: Scan IaC with Tenable One Cloud Exposure
    uses: tenable/cloud-security-actions/iac/scan@v1
    with:
      api-token: ${{ secrets.TENABLE_API_TOKEN }}
      api-url: https://app.tenable.com/
  ```

  アクションがトリガーされたら、**[CI/CD]** にスキャン結果がクラウドサイバーエクスポージャー表示されます。

- **IaC 同期**。クラウドリソースに関連付けられたコードを同期し、それらのリソースをオリジンまでトレースする (クラウドからコードまで) には、次のアクションを GitHub ワークフロー (YAML ファイル) に追加します。

  > **重要:** このアクションは、「terraform apply」ステップの実行後に追加する必要があります。

  YAML

  ```
  steps:
  - uses: actions/checkout@v3
  - name: Pull remote terraform state
    run: terraform state pull > terraform.tfstate
    shell: bash
  - name: Sync IaC with Tenable One Cloud Exposure
    uses: tenable/cloud-security-actions/iac/sync/terraform@v1
    with:
      api-token: ${{ secrets.TENABLE_API_TOKEN }}
      api-url: https://app.tenable.com/
  ```

  ワークフローで [Terraform の設定] GitHubアクションを使用している場合、Tenable では、パイプラインの実行時の問題を防ぐために stdout Terraform ラッパーを無効にすることを強くお勧めします。矢印マークが付いた以下の推奨コードを参照してください。

```yaml
- name: Setup Terraform
uses: hashicorp/setup-terraform@v2.0.3
with:
  terraform_wrapper: false
```

同期がトリガーされたら、クラウドサイバーエクスポージャーにIaCラベルでタグ付けされたリソース/検出結果が表示されます。関連するリソースの[Inventory] (インベントリ) ビューに[IaC] タブがあり、関連するコードスニペットが表示されます。

- **コンテナイメージのスキャン**詳細については、コンテナイメージスキャンを参照してください。

7. 完了したら、**[完了]** をクリックします。

GitLab パイプラインの追加

GitLab パイプラインを追加した後、Docker イメージで CLI を使用して、スキャン設定を行い、クラウドサイバーエクスポージャー が環境をスキャンする方法を微調整できます。

GitLab の CI/CD YAML 設定の設定オプションの詳細については、GitLab のドキュメントを参照してください。

GitLab パイプラインを追加するには

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[GitLab CI/CD]** をクリックします。[Add GitLab CI/CD] (GitLab CI/CD の追加) ウィザードが開きます
3. **APIトークンを作成します** (ウィザードのステップ 1):
    - スキャン結果を Tenable に報告するために、スキャナーには API トークンパラメーターが必要です。
    - トークンを作成するには、「**トークン名** 」を入力し、「**次へ**」をクリックします。
4. **APIトークンを保存します** (ウィザードのステップ 2)。生成された**トークン** をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。

5. (推奨) **変数を追加します** (ウィザードのステップ 3)。プロジェクトで CI/CD 変数を定義するには、次の手順に従います。

   > **注意:** Tenable の API トークンを保護するには、マスクされた変数、または他のシークレットストア (現在使用している場合) のいずれかを使用することをお勧めします。GitLab CI/CD 変数は、Tenable のスキャンの利用方法に応じて複数のレベルで保存できます。Tenable のトークンは、IaC コードとともにリポジトリにリンクされたパイプラインのみに関連付けることが推奨されていますが、必須ではありません。

   1. GitLab にログインします。
   2. プロジェクトの **Settings** > **CI/CD** に移動します。
   3. [変数] で、**[展開]** をクリックします。
   4. **[変数の追加]** をクリックします。
   5. 次の詳細を入力します。
      1. **[キー]** を TENABLE_API_TOKEN に設定します。
      2. 前のステップで作成したトークンを **[値]** として貼り付けます。
      3. 該当する場合は、**[環境範囲]** を選択します。
      4. **[フラグ]** の下にある **[変数をマスク]** というボックスにチェックを入れます。
      5. **[変数の追加]** をクリックします。

         YAML

         ```yaml
         include:
         - component: $CI_SERVER_FQDN/tenb/cloud-security/components/iac-scan@1
           inputs:
             api-token: $TENABLE_API_TOKEN
             api-url: https://app.tenable.com/
             stage: tenable-cloud-security

         stages:
         - tenable-cloud-security
         ```

         スキャンがトリガーされたら、[CI/CD] の クラウドサイバーエクスポージャー にスキャン結果が表示されます。
      6. クラウドサイバーエクスポージャー コンソールウィザードで **[完了]** をクリックします。

完了したら、クラウドサイバーエクスポージャーコンソールウィザードの **[次へ]** をクリックします。

6. **ステージを追加します** (ウィザードのステップ 4)。次のステップを .gitlab-ci.yml ファイルに追加します。

IaC スキャンを設定し、GitLab で SAST 形式の結果を表示する

GitLab マージリクエストで実行するように CI/CD スキャンを設定し、GitLab がネイティブに解析する SAST 形式で結果を表示することができます。

1. 次のプロパティを .gitlab-ci.yml ファイルに追加します。
    - `output-file-formats`
    - `artifacts`
    - `rules`

> **注意:** `output-file-formats` および `artifacts` は、スキャン結果を SAST 形式で表示するために必要な唯一のプロパティです。GitLab マージリクエストで CI/CD スキャンを設定するには、`rules` プロパティを追加します。

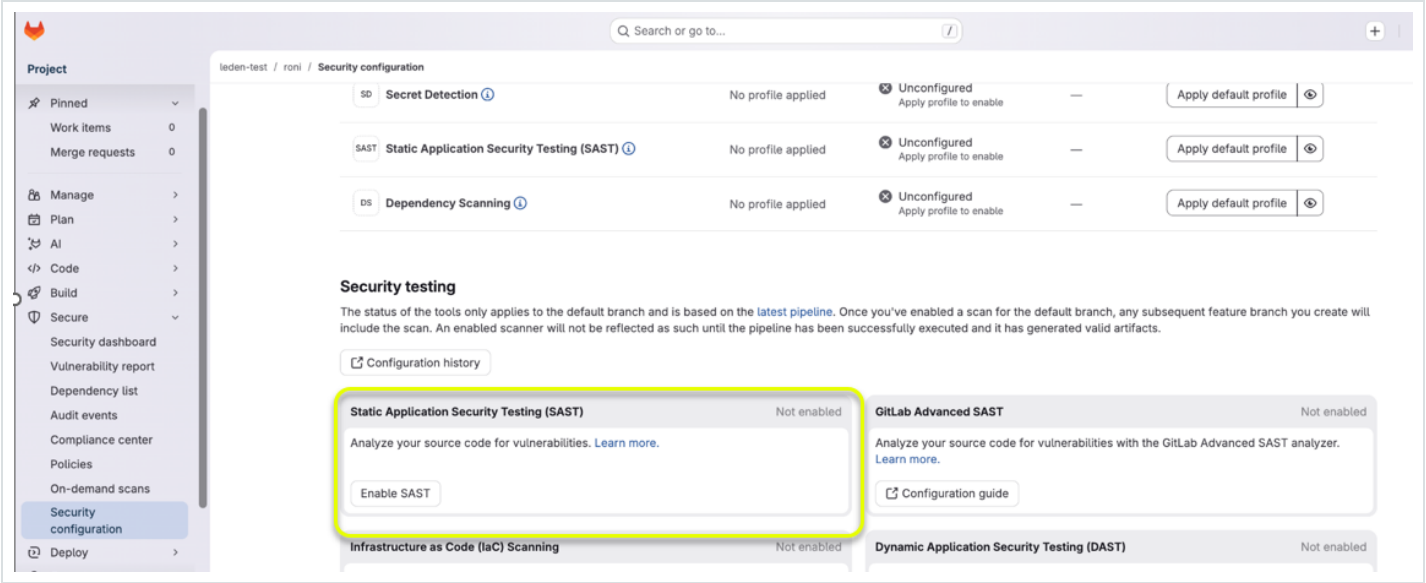
YAML

```
include:
  - component: $CI_SERVER_FQDN/tenb/cloud-security/components/iac-scan@1
inputs:
  api-token: $TENABLE_API_TOKEN
  api-url: https://app.dev.t.io/
  stage: tenable-cloud-security
  output-file-formats: GitLabSast

stages:
  - tenable-cloud-security

tenable-iac-scan:
  rules:
- if: '$CI_PIPELINE_SOURCE == "merge_request_event"'
- if: '$CI_COMMIT_BRANCH == $CI_DEFAULT_BRANCH'
  artifacts:
when: always
paths:
  - results.json
reports:
  sast: results.json
```

2. GitLab にログインします。
3. 左側のナビゲーションバーで、**[セキュア > セキュリティ設定]** に移動します。**[セキュリティ設定]** ページが表示されます。
4. **[セキュリティテスト]** セクションで、**[SAST の有効化]** をクリックして静的アプリケーション セキュリティ テスト (SAST) を有効にします。クラウド サイバーエクスポージャー は GitLab マージリクエストをスキャンし、検出された結果を表示します。



Jenkins パイプラインの追加

以下を行う Jenkins パイプラインを追加します。

- インフラのコード化 (IaC) パイプラインを**スキャンして**セキュリティ問題を検出します。
- クラウド リソースに関連付けられたコードを**同期**して、それらのリソースをオリジンまで**トレース**します (クラウド からコードまで)。

Jenkins パイプラインを追加した後、Docker イメージで CLI を使用して、スキャン/同期設定を行い、クラウド サイバーエクスポージャー が環境をスキャンする方法を微調整できます。

要件:

- Docker がホストにインストールされていること
- Docker プラグインを Jenkins にインストールする必要があります

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Jenkins Pipeline]** をクリックします。[Add Jenkins Pipeline] (パイプラインの追加) ウィザードが開きます。
3. **API トークンを作成します** (ウィザードのステップ 1):
    1. スキャン結果を Tenable に報告するために、スキャナーには API トークンパラメーターが必要です。
    2. トークンを作成するには、「**トークン名** 」を入力し、「**次へ**」をクリックします。
4. **API トークンを保存します** (ウィザードのステップ 2)。生成された**トークン** をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。
5. (推奨) **Jenkins 認証情報を追加します** (ウィザードのステップ 3)。新しいグローバル認証情報を Jenkins に追加するには、以下の手順に従います。

    注意: Tenable の API トークンを保護するには、Jenkins 認証情報、または他のシークレットストア (現在使用している場合) のいずれかを使用することをお勧めします。Jenkins 認証情報は、Tenable のスキャンの利用方法に応じて複数のレベルで保存できます。Tenable のトークンは、IaC コードとともにリポジトリにリンクされたパイプラインのみに関連付けることが推奨されていますが、必須ではありません。

    1. Jenkins にログインします ([Credentials] (認証情報) > [Create permission] (権限の作成) を通じてユーザーとして)。
    2. ホームページで、**[Manage Jenkins > Manage Credentials]** をクリックします。
    3. 右側の **[ストアスコープを Jenkins]** で、**[Jenkins]** をクリックします。
    4. **[System]** (システム) で、**[Global credentials (unrestricted)]**(グローバル認証情報 (無制限)) リンクをクリックして、デフォルトのドメインにアクセスします。
    5. 左側にある **[Add Credentials]** (認証情報の追加) をクリックします (認証情報が存在しない場合は、**認証情報を追加**します)。

1. **[種類]** フィールドから、**[シークレット テキスト]** を選択します。
2. **[Scope]**(範囲) フィールドで、**[Global]** (グローバル) を選択します。
3. ウィザードで以前に作成した **API トークン** をコピーし、**[Secret]** (シークレット) フィールドに貼り付けます。
4. [ID] フィールドで、**[tenable-api-token]** を指定します。
5. トークンについてオプションの**説明**を追加します。
6. **[OK]** をクリックして認証情報を保存します。

完了したら、クラウド サイバーエクスポージャー コンソール ウィザードの **次へ** をクリックします。

6. **ステージを追加します** (ウィザードのステップ 4)。スキャン結果を生成するには、関連するステップを Jenkins パイプラインに追加します。

> **注意:** Git リポジトリ内でスキャンまたは同期を実行することをお勧めします。何らかの理由でこれが不可能な場合は、「非 Git リポジトリの追加変数」を参照してください。

- **IaC スキャン**IaC をスキャンするには、以下のステップをパイプラインに追加します (必要に応じて調整します)。

```groovy
pipeline {
    agent any
    stages {
        stage('Checkout') {
            steps {
                git '<PLACE YOUR REPOSITORY URL HERE>'
            }
        }
        stage('Scan IaC with Tenable One Cloud Exposure') {
            environment {
                TENABLE_API_TOKEN = credentials('ermetic-api-token')
                TENABLE_API_URL = 'https://app.tenable.com'
                TENABLE_CODE_BRANCH = "${env.CHANGE_BRANCH ?: env.GIT_BRANCH}"
                TENABLE_CODE_COMMIT_HASH = "${env.GIT_COMMIT}"
                TENABLE_CODE_COMMIT_USER = "${env.CHANGE_AUTHOR}"
                TENABLE_PIPELINE_RUN_ID = "${env.BUILD_ID}"
                TENABLE_PIPELINE_RUN_TRIGGER = "${currentBuild.getBuildCauses()
[0].shortDescription}"
```

```
                TENABLE_PIPELINE_RUN_URL = "${env.BUILD_URL}"
            }
            steps {
                script {
                    docker.image('tenable/cloud-security-scanner:latest').inside("--
entrypoint='' --pull=always") {
                        sh 'tenable iac scan \
                            --no-color \
                            --output-file-formats JUnit \
                            --output-path .'
                        junit skipPublishingChecks: true, testResults: 'results.junit.xml'
                    }
                }
            }
        }
    }
}
```

アクションがトリガーされたら、[CI/CD] のクラウドサイバーエクスポージャーにスキャン結果が表示されます。

- **IaC 同期**。リソースと問題をコードのオリジンまでトレースするには、Jenkins パイプラインに以下のステップを追加し、環境の必要性に応じて調整します。

> **注意:**
>
> - このステップは、`terraform apply` ステップ内の「apply」コマンドの後に追加する必要があります。
> - 同期結果を生成するには、前述のように環境変数が追加されていることを確認してください。
> - `TENABLE_API_TOKEN`フィールドは機密性が高いため、シークレットとして扱う必要があります。

Groovy

```
pipeline {
    agent any
    stages {
        stage('Checkout') {
            steps {
                git '<PLACE YOUR REPOSITORY URL HERE>'
            }
        }
```

```
        stage('Terraform Apply') {
            steps {
                script {
                    // This step is required if your state file is stored remotely.
                    // Add 'state pull' after the 'terraform apply' script.
                    sh 'terraform state pull > terraform.tfstate'
                }
            }
        }
        stage('Sync IaC with Tenable One Cloud Exposure') {
            environment {
                TENABLE_API_TOKEN = credentials('tenable-api-token')
                TENABLE_API_URL = 'https://app.tenable.com'
                TENABLE_CODE_BRANCH = "${env.CHANGE_BRANCH ?: env.GIT_BRANCH}"
                TENABLE_CODE_COMMIT_HASH = "${env.GIT_COMMIT}"
                TENABLE_CODE_COMMIT_USER = "${env.CHANGE_AUTHOR}"
                TENABLE_PIPELINE_RUN_ID = "${env.BUILD_ID}"
                TENABLE_PIPELINE_RUN_TRIGGER = "${currentBuild.getBuildCauses()
[0].shortDescription}"
                TENABLE_PIPELINE_RUN_URL = "${env.BUILD_URL}"
            }
            steps {
                script {
                    docker.image('tenable/cloud-security-scanner:latest').inside("--
entrypoint='' --pull=always") {
                        sh 'tenable iac sync terraform \
                            --no-color'
                        junit skipPublishingChecks: true, testResults: 'results.junit.xml'
                    }
                }
            }
        }
    }
}
```

> **注意:** 上記の例では、Docker Pipelines プラグインを使用していることを前提としています。

同期がトリガーされたら、クラウド サイバーエクスポージャーに IaC ラベルでタグ付けされたリソース/検出結果が表示されます。関連するリソースの [Inventory] (インベントリ) ビューに [IaC] タブがあり、関連するコード スニペットが表示されます。

- **コンテナイメージのスキャン**詳細については、コンテナイメージスキャンを参照してください。

7. 完了したら、**[完了]** をクリックします。

非 Git リポジトリの追加変数

Git リポジトリ内でスキャンまたは同期を実行することをお勧めします。何らかの理由でこれが不可能な場合は、[Add Jenkins Pipeline] (Jenkins パイプラインの追加) ウィザードで一覧表示される変数に加えて、次の変数を追加する必要があります (「 Jenkins パイプラインの追加」を参照)。

```
TENABLE_CODE_REPOSITORY_URL=https://github.com/acme/repo1
```

上記のサンプル値を以下のように置き換えます。
TENABLE_CODE_REPOSITORY_URL:コードリポジトリのURLに置き換えます

Terraform Cloud Run タスクの追加

Terraform Cloud Run タスクを使用すると、実行ライフサイクルの特定の段階でサードパーティのツールやサービスを統合できます。クラウドサイバーエクスポージャー は、計画後段階で Terraform Plan をスキャンします。必要な Terraform Cloud のアクセス許可 (ワークスペースの実行タスクを管理する権限を含む) があることを確認します。これにより、実行タスクをワークスペースに関連付けることができます。

実行タスクの設定中に、Tenable が環境をスキャンする方法を微調整する追加のパラメーターでエンドポイント URL 値を修正できます (以下のステップ 3、4 を参照してください)。

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**Terraform Cloud** をクリックします。[Add Terraform Cloud] (Terraform Cloud の追加) ウィザードが開きます。
3. API トークンを作成します (ウィザードのステップ 1):
    - スキャン結果を Tenable に報告するために、スキャナーには API トークンパラメーターが必要です。
    - トークンを作成するには、「 **トークン名** 」を入力し、「 **次へ**」をクリックします。
4. Terraform Cloud で実行タスクを作成します (ウィザードのステップ 2):
    1. 実行タスクを管理する権限を持つユーザーで Terraform Cloud にサインインします。
    2. **[設定]** メニューを開きます。
    3. **[タスクの実行]** をクリックします。

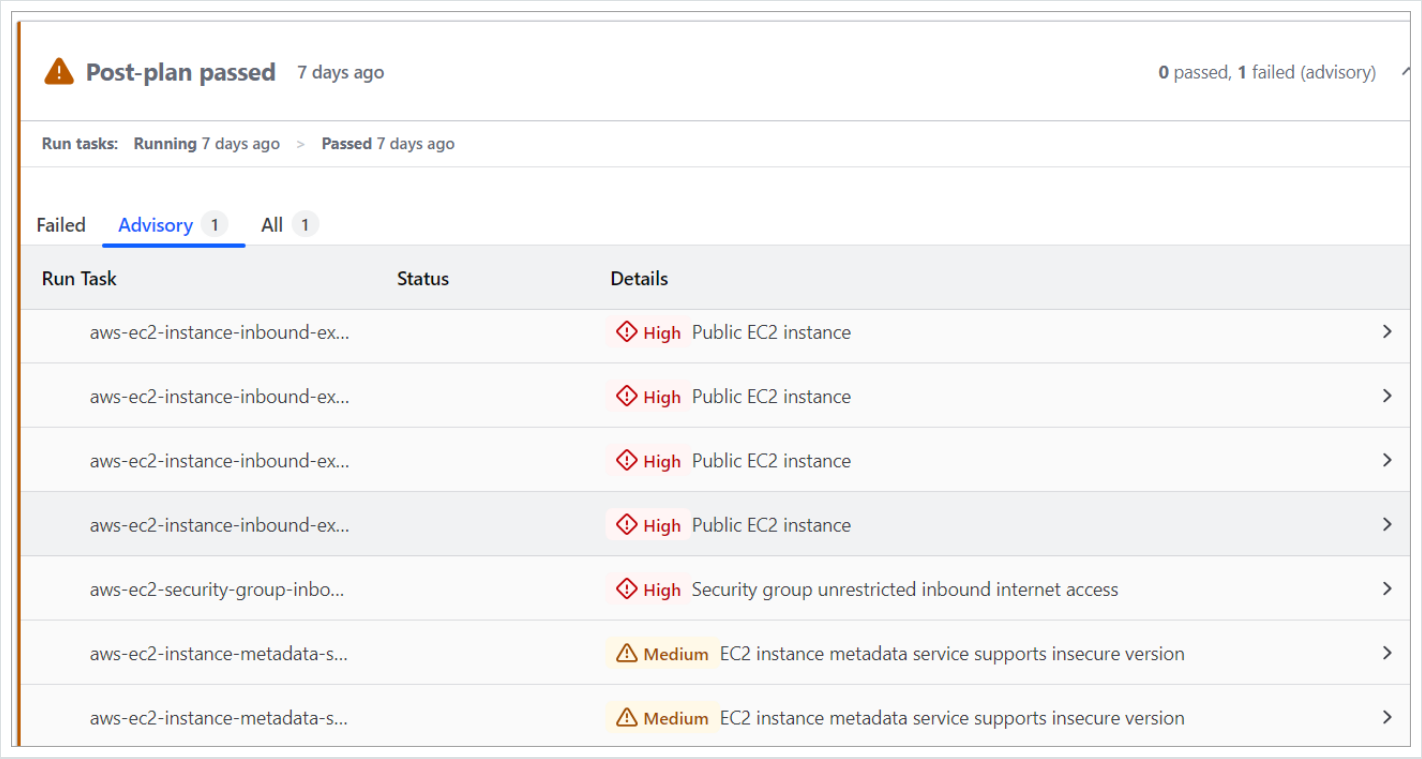
4. **[実行タスクの作成]** をクリックし、次のように実行タスクを構成します。
    - **[有効]** チェックボックスを選択します。
    - 実行 **タスクの名前を入力します** (例: *Tenable*)
    - Tenableウィザードに表示される**エンドポイント URL** 値をコピーして貼り付けます。Tenable が環境をスキャンする方法を微調整するために、追加のパラメーターでこの URL を修正します。詳細は、Terraform Cloud エンドポイント URL の設定 を参照してください。
    - (オプション) **説明**を入力します。
    - Tenableウィザードに表示される **HMAC キー**の値をコピーして貼り付けます。
    - **[実行タスクの作成]** をクリックします。
5. 実行タスクをワークスペースと関連付けます:
    1. **[ワークスペース]** をクリックし、保護するワークスペースをクリックします。
    2. 左側のメニューで、**[Settings]** をクリックします。
    3. [Workspace Settings] で、**[タスクの実行]** をクリックします。
    4. [利用可能な実行タスク] で、Tenable 用に作成した実行タスクの横にあるプラス記号 **(+)** をクリックして、ワークスペースに追加します。
    5. 次の手順に従って実行タスクを関連付けます。
        1. 実行ステージ で、**計画後** を選択します。
        2. [強制レベル] で、次のいずれかを選択します。
            - **アドバイザリ**タスクが失敗した場合、警告が表示されますが、実行は続行され完了を妨げることはありません。
            - **必須です。** タスクが失敗した場合 (タイムアウトや予期しないリモートエラー状態が発生した場合など)、警告が表示され、実行が停止されます。
        3. **[作成]** をクリックします。

アクションがトリガーされたら、**[CI/CD]** にスキャン結果がクラウドサイバーエクスポージャー表示されます。

合理化された実行タスクレビューで詳細な結果を表示する

Terraform Cloud 内で、強化され詳細なスキャン結果を表示できます。これらの結果には、検出された問題の完全なリスト (詳細については「スキャンで使用される Tenable ポリシー」を参照) と、各問題に関する詳細情報が含まれます。これにより、クラウドサイバーエクスポージャーコンソールにアクセスすることなく、スキャン結果を表示しながら文脈を把握することができます。

> **注意:** 詳細な結果を表示するために、場合によっては、Terraform Cloud 内でこの機能を有効にする必要があります。



別のパイプラインを追加する

上記にリストされているパイプラインに加えて、クラウドサイバーエクスポージャーは汎用ワークフローを介した他の CI/CD パイプラインの接続をサポートしています。以下の手順は、docker ベースのパイプラインを接続するための一般的な手順を示していますが、環境変数を追加して Docker スキャンを実行するときに使用される実際の構文は特定のパイプラインによるため、それに応じて調整する必要があります。

このワークフローを使用して、次のことができます。

- インフラのコード化 (IaC) パイプラインを**スキャンして**セキュリティ問題を検出する
- クラウドリソースに関連付けられたコードを**同期**して、それらのリソースをオリジンまで**トレース**します (クラウドからコードまで)。

汎用パイプラインを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[汎用 (Docker)]** をクリックします。[Add Generic (Docker)] (汎用の追加 (Docker)) ウィザードが開きます。
3. **APIトークンを作成します** (ウィザードのステップ 1):
    - スキャン結果を Tenable に報告するために、スキャナーには API トークンパラメーターが必要です。
    - トークンを作成するには、「**トークン名**」を入力し、「**次へ**」をクリックします。
4. **APIトークンを保存します** (ウィザードのステップ 2)。生成された**トークン**をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。
5. **環境変数を追加します** (ウィザードのステップ 3)。以下のコードで `environment.variables` という名前のファイルを作成します (必要に応じて調整)。

    > **注意:** Tenable 内で基本的なレポート機能を提供するために必要な、ここに一覧表示されている環境変数に加えて、グローバルフラグを含む Tenable Docker イメージに含まれるすべてのフラグを環境変数として設定して、スキャン/同期設定をさらに微調整できます。変数として使用するためにフラグを変換する方法など、詳しくは「フラグを環境変数として使用する」を参照してください。

    ```
    TENABLE_API_TOKEN=<api-token here>
    TENABLE_API_URL=https://app.tenable.com
    TENABLE_PIPELINE_RUN_ID=134235
    TENABLE_PIPELINE_RUN_TRIGGER=pull_request
    TENABLE_PIPELINE_RUN_URL=https://github.com/acme/repo1/actions/runs/134235
    ```

    > **注意:** 上記のサンプル値を以下のように置き換えます。`TENABLE_API_TOKEN`: add-pipeline ウィザードに表示される値に置き換えます `TENABLE_PIPELINE_RUN_ID`: パイプラインの実行 ID に置き

> 換えます TENABLE_PIPELINE_RUN_TRIGGER: ワークフローの実行をトリガーしたイベントの名前に置き換えます TENABLE_PIPELINE_RUN_URL: この実行の結果がある URL に置き換えます

完了したら、クラウドサイバーエクスポージャーコンソールウィザードの **次へ**をクリックして続行します。

6. **Docker コマンドを実行します** (ウィザードのステップ 4)。環境に応じて調整しながら、関連するコマンドを CI/CD パイプラインに追加します。

> **注意:** Git リポジトリ内でスキャンまたは同期を実行することをお勧めします。何らかの理由でこれが不可能な場合は、「非 Git リポジトリの追加変数を参照してください。

- **IaC スキャン**IaC をスキャンするには、次のステップをパイプラインに追加します (必要に応じて調整します)。

```
docker run --workdir /tmp/tenable --volume /home/user/code:/tmp/tenable --env-file
environment.variables --pull=always tenable/cloud-security-scanner:latest iac scan
```

> **重要:** 上記の手順で、スキャンしているコードの実際の場所に `/home/user/code` を置き換える必要があります。

各部の説明

- `--env-file` は、`environment.variables` 前のステップで作成したファイルが見つかります。
- `--volume` 左側 (「:」の前) を、コードがあるパスに変更します。右側はそのままにします。

上記のステップ例は、次のことを前提としています。

- コンテナで Tenable のスキャナーを実行するために docker run を使用している
- スキャンしているコードは `/home/user/code` にあります。
- `environment.variables` という名前の Docker env ファイルを作成した
- デフォルトのフラグでスキャンを実行している

スキャンがトリガーされると、[CI/CD] にスキャン結果が表示されます。

- **IaC 同期**。クラウドリソースに関連付けられたコードを同期して、それらのリソースをオリジンまでトレースする (クラウドからコードまで) には、次のステップをパイプラインに追加します (必要に応じて調整します)。

  Dockerfile

  ```
  terraform state pull > terraform.tfstate
  docker run --workdir /tmp/tenable --volume /home/user/code:/tmp/tenable --env-file
  environment.variables --pull=always tenable/cloud-security-scanner:latest iac sync terraform
  ```

  重要: 上記の手順で、スキャンしているコードの実際の場所に `/home/user/code` を置き換える必要があります。

  ここで:

  - `--env-file` は、前の手順で作成した `environment.variables` ファイルが存在するパスです。
  - `--volume` 左側 (「:」の前) をコードがあるパスに変更します。右側はそのままにします。

  上記のステップ例は以下を前提としています。

  - コンテナで Tenable のスキャナーを実行するために docker run を使用している
  - 同期しているコードが `/home/user/code` にある - `environment.variables` という名前の Docker env ファイルを作成した。
  - デフォルトのフラグでスキャンを実行している

  同期がトリガーされたら、クラウドサイバーエクスポージャーに IaC ラベルでタグ付けされたリソース/検出結果が表示されます。関連するリソースの [Inventory] (インベントリ) ビューに [IaC] タブがあり、関連するコードスニペットが表示されます。

- **コンテナイメージのスキャン**詳細については、コンテナイメージスキャン を参照してください。

7. 完了したら、クラウドサイバーエクスポージャーコンソールウィザードで **[完了]** をクリックします。

非 Git リポジトリの追加変数

Git リポジトリ内でスキャンまたは同期を実行することをお勧めします。何らかの理由でこれが不可能な場合は、[汎用 (Docker) の追加] ウィザードで一覧表示される変数に加えて、次の変数を追加する必要があります (別のパイプラインを追加する を参照)。

```
TENABLE_CODE_BRANCH=main
TENABLE_CODE_COMMIT_HASH=fa4e0ef3e25b89e1f6c348afd51b073f2bbcf1bb
TENABLE_CODE_COMMIT_USER=john-doe
TENABLE_CODE_REPOSITORY_URL=https://github.com/acme/repo1
```

上記のサンプル値を以下のように置き換えます。

- TENABLE_CODE_BRANCH:ブランチ名に置き換える
- TENABLE_CODE_COMMIT_HASH:コードのコミットハッシュに置き換えます
- TENABLE_CODE_COMMIT_USER: 最初のワークフローの実行をトリガーしたユーザーのユーザー名に置き換える
- TENABLE_CODE_REPOSITORY_URL: コードリポジトリの URL に置き換える

スキャンの設定

スキャンの設定を行い、クラウドサイバーエクスポージャー が環境をスキャンする方法を微調整します。たとえば、以下の設定が可能です。

- スキャンで使用される Tenable ポリシー。
- スキャン結果に基づくビルドワークフローを失敗させるかどうか、および失敗をトリガーするポリシーの最小深刻度を指定します。
- Tenableによってスキャンされるパス。

お使いの CI/CD パイプラインに該当する方法を使用します。

- **GitHub アクション**。
  - **スキャン**: ネイティブの GitHub Actions スキャンパラメーターを使用します。
  - **同期**: ネイティブの GitHub Actions 同期パラメーターを使用します。
- **GitLab CI/CD**。
  - **スキャン**: GitLab CI/CD スキャンパラメーターを使用します。
- **Jenkins/Generic Docker**。Tenable Docker イメージの CLI を使用します。
- **Terraform Cloud**。エンドポイントの URL を設定します。

- **Azure Pipelines**。
    - **スキャン**: Azure Pipelines スキャンパラメーターを使用します。
    - **同期**: Azure Pipelines 同期パラメーターを使用します。

スキャン設定とポリシー設定の違い

この記事で概説するさまざまなスキャン設定 (パラメーター) に加えて、コンソールの [Policies] (ポリシー) ページから IaC ポリシーを管理できます。コンソールでは、特定の IaC 範囲に対して次の基本アクティビティを実行できます。

- ポリシーの有効化 / 無効化
- IaC スキャンで除外を設定する

詳細は、ポリシーの表示と管理を参照してください 。

ポリシーは、スキャン設定パラメーターと [ポリシー] ページの両方から無効化または除外できます。以下のように、設定した除外は常にすべての包含を上書きすることに注意してください。

- スキャン設定パラメーターを使用してポリシーを除外したが、[Policies] (ポリシー) ページでポリシーが有効になっている場合、ポリシーはスキャンから **除外されます** 。
- [ポリシー] ページでポリシーを無効にした (または 関連する除外を定義した) が、スキャン設定でポリシーが (明示的または暗黙的に) 含まれている場合、そのポリシーはスキャンから **除外** されます。

Azure Pipelines パラメーター

Azure Pipelines の関連するパイプラインの YAML スキーマで次の `task` 入力パラメーターを構成して、クラウド サイバーエクスポージャー が環境をスキャンまたは同期する方法を微調整します。YAML スキーマの設定について詳しくは、関連する Microsoft ドキュメント を参照してください。例については 構成例 。

- Azure Pipelines スキャンパラメーター
- Azure Pipelines 同期パラメーター

> **注意:** 従来のリリースパイプラインを使用している場合は、スキャンタスクと同期タスクの両方に追加のパラメーターが必要になることに注意してください。詳細については、従来のリリースパイプラインを使用している場合に必要な追加のパラメーターを参照してください。

Azure Pipelines スキャンパラメーター

Azure Pipelines の関連するパイプラインの YAML スキーマで次の task 入力パラメーターを構成して、クラウド サイバーエクスポージャー が環境をスキャンする方法を微調整します。

パラメーター	説明	デフォルト	例
apiToken	(必須)Tenable との通信に使用される APIトークン。Azure Pipelines の初期セットアップ中に、クラウド サイバーエクスポージャー コンソールで生成されます。		
apiUrl	(必須)Tenable API の URL。		`https://app.tenable.com/`
excludePaths	スキャンから特定のパスを除外します。		`dev/`
excludePolicies	スキャンから除外する Tenable ポリシーの ID。このパラメーターは `policies` と相互に排他的であるため、入力できる		`aws-iam-role-public-access-exists`

パラメーター	説明	デフォルト	例
	のは 2 つのうち 1 つの値のみです。glob パターンをワイルドカードとして使用して、ポリシーの範囲を定義できます。たとえば、以下のようになります。`excludePolicies aws-s3-*` は、AWS S3 バケットに関連するすべてのポリシーをスキャンから除外します。		
failOnMinSeverity	0 以外の終了コードを返し、ビルドワークフローを失敗とするポリシーの最小深刻度。可能な値: • `none` • `information` • `low` • `medium`	`none`	`critical`

パラメーター	説明	デフォルト	例
	• high • critical		
gitトークン	スキャン中にクラウドサイバーエクスポージャーが必要とするプライベートコードリポジトリのアクセストークン。たとえば、プライベートTerraformモジュールにアクセスするには、これらのトークンが必要になる場合があります。複数のトークンがある場合は、コンマで区切ります。形式：ORGANIZATION_URL=YOUR_TOKEN		`https://dev.azure.com/org=YOUR_TOKEN`
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ログメッセージには、ス	`false`	`true`

パラメーター	説明	デフォルト	例
	キャナーの実行プロセスに関する情報や、スキャンされたファイル数や行数などのデバッグ情報が含まれる。可能な値は次のとおりです。 `true` `false`		
分深刻度	スキャンに含めるTenableポリシーの最小深刻度です。可能な値: • `information` • `low` • `medium` • `high` • `critical`	`information`	`medium`
outputFileFormats (出力ファイル・フォーマット)	エクスポートされるレポート出力ファイルの形式。複数の形式の値を入力して、複数の形式でレポートを出力でき	`json`	`json,csv`

パラメーター	説明	デフォルト	例
	ます。可能な値: • csv • json • junit • sarif • md		
outputFileName (出力ファイル名)	エクスポートされるレポート出力ファイルの名前。複数の形式を選択すると、すべてのファイルに同じ名前が付くようになります。	results	results
outputJunitTestNamePrefix	JUnitテスト出力名のプレフィックス。テスト結果に第1レベルの階層を作成するために使用される。junitが出力ファイル形式として定義されている場合に使用できます。		Scan1
出力パス	レポート出力ファ		results/

パラメーター	説明	デフォルト	例
	イルのエクスポートパス。		
パス	Tenableによってスキャンされるリポジトリパス。空白のままにすると、リポジトリ全体 Tenable スキャンされます。		`prod/,stg/`
ポリシー	コンマ区切りリストとして入力された、リポジトリのスキャンに使用される Tenable ポリシーの ID。値を入力しない場合、すべてのポリシーがスキャンされます。このパラメーターは `excludePolicies` と相互に排他的であるため、入力できるのは 2 つのうち 1 つの値のみです。glob パターンをワイルド		`aws-iam-role-public-access-exists-terraform,aws-sqs-queue-encryption-disabled`

パラメーター	説明	デフォルト	例
	カードとして使用して、含めるポリシーの範囲を定義できます。たとえば、以下のようになります。`policies aws-s3-*` は、AWS S3 バケットに関連するすべてのポリシーをスキャンに含めます。glob パターンをワイルドカードとして使用して、含めるポリシーの範囲を定義できます。たとえば `policies aws-s3-*` の場合、AWS S3 バケットに関連するすべてのポリシーがスキャンに含まれます。		
サイレント	スキャン結果の内容を標準ワークフロー出力に出力するかどうか。	`false`	`false`

パラメーター	説明	デフォルト	例
	スキャン結果の出力には、スキャン中に見つかった問題に関する詳細情報が含まれる。ログから独立している。可能な値は次のとおりです。`true` `false`		
types	スキャンを Tenable する IaC フレームワークです。値を入力しない場合、Tenable はすべてのフレームワークをスキャンします。可能な値は次のとおりです。`terraform` `terraform-plan` `cloudformation`		`terraform`

Azure Pipelines 同期パラメーター

パラメーター	説明	デフォルト	例
apiToken	(必須) Tenableとの通信に使用されるAPIトークン。Azure Pipelinesの初期セットアップ中に、クラウドサイバーエクスポージャーコンソールで生成されます。	-	-
apiUrl	(必須) クラウドサイバーエクスポージャーAPIのURL。	-	`https://app.tenable.com/`
gitトークン	同期時にクラウドサイバーエクスポージャーが必要とするプライベートコードリポジトリのアクセストークン。たとえば、プライベートTerraformモジュールにアクセスするには、これらのトークンが必	-	`https://dev.azure.com/org=YOUR_TOKEN`

パラメーター	説明	デフォルト	例
	要になる場合があります。複数のトークンがある場合は、コンマで区切ります。形式：`ORGANIZATION_URL=YOUR_TOKEN`		
パス	コンマ区切りリストとして入力された、Tenableによって同期されるTerraformルートモジュールのパス。空白のままにすると、Tenableは作業ディレクトリを同期します。	-	`prod/、stg/`
stateFilePath	Terraformの状態ファイルのパス。	`terraform.tfstate`	`terraform.tfstate`
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ロ	`true`	`true`

パラメーター	説明	デフォルト	例
	グメッセージには、実行プロセスに関する情報とデバッグ情報が含まれます。可能な値: `true`、`false`		
サイレント	同期結果の内容を標準ワークフロー出力に出力するかどうか。同期結果の出力には、オリジンまでトレースされたファイルに関する情報が含まれます。ログから独立している。可能な値: `true`、`false`	`false`	`false`

GitHub Actions パラメーター

入力パラメーターを設定して、クラウドサイバーエクスポージャー が環境をスキャンする方法を微調整します。

- GitHub Actions スキャンパラメーター
- GitHub Actions 同期パラメーター

GitHub Actions スキャンパラメーター

GitHub アクションで以下の入力パラメーターを設定して、クラウドサイバーエクスポージャー が環境をスキャンする方法を微調整します。

パラメーター	説明	デフォルト	例
api-token (必須)	クラウドサイバーエクスポージャーとの通信に使用される APIトークン。GitHubアクションの初期セットアップ中に、クラウドサイバーエクスポージャー コンソールで生成されます。		
api-url (必須)	クラウドサイバーエクスポージャー API の URL。		`https://app.tenable.com/`
exclude-paths	スキャンから特定のパスを除外します。		`dev/`
exclude-policies	スキャンから除外する Tenable ポリシーの ID。このパラメーターは `policies` と相互に排他的であるため、入力できるのは 2 つのうち 1 つの値のみです。glob パターンをワイルドカードとして使用して、ポリシーの範囲を定義できます。たとえば、以下のようになりま		`aws-iam-role-public-access-exists`

パラメーター	説明	デフォルト	例
	す。`exclude-policies aws-s3-*` は、AWS S3 バケットに関連するすべてのポリシーをスキャンから除外します。		
fail-on-min-severity	0 以外の終了コードを返し、ビルドワークフローを失敗とするポリシーの最小深刻度。値が定義されていない場合、ワークフローは失敗しない。可能な値: • `information` • `low` • `medium` • `high` • `critical`		`critical`
gitトークン	スキャン中にクラウドサイバーエクスポージャーが必要とするプライベートコードリポジトリのアクセストークン。たとえば、プライベート Terraform モジュールにアクセスするに		`https://github.com/org=YOUR_TOKEN`

パラメーター	説明	デフォルト	例
	は、これらのトークンが必要になる場合があります。複数のトークンがある場合は、コンマで区切ります。形式：`ORGANIZATION_URL=YOUR_TOKEN`		
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ログメッセージには、スキャナーの実行プロセスに関する情報や、スキャンされたファイル数や行数などのデバッグ情報が含まれる。可能な値は次のとおりです。`true` `false`	`false`	`true`
min-severity	スキャンに含めるTenableポリシーの最小深刻度です。可能な値： • `information` • `low` • `medium` • `high` • `critical`	`information`	`medium`

パラメーター	説明	デフォルト	例
output-file-formats	エクスポートされるレポート出力ファイルの形式。複数の形式の値を入力して、複数の形式でレポートを出力できます。可能な値: • `csv` • `json` • `junit` • `sarif` • `md`	`json`	`json,csv`
出力ファイル名	エクスポートされるレポート出力ファイルの名前。複数の形式を選択すると、すべてのファイルに同じ名前が付くようになります。	`results`	`results`
output-junit-test-name-prefix	JUnitテスト出力名のプレフィックス。テスト結果に第1レベルの階層を作成するために使用される。`junit`が出力ファイル形式として定義されている場合に使用できます。		`Scan1`
出力パス	レポート出力ファイルのエ	`results/`	

パラメーター	説明	デフォルト	例
	クスポートパス。		
パス	Tenableによってスキャンされるリポジトリパス。空白のままにすると、リポジトリ全体 Tenable スキャンされます。		`prod/`
ポリシー	コンマ区切りリストとして入力された、リポジトリのスキャンに使用される Tenable ポリシーの ID。値を入力しない場合、すべてのポリシーがスキャンされます。このパラメーターは `exclude-policies` と相互に排他的であるため、入力できるのは 2 つのうち 1 つの値のみです。glob パターンをワイルドカードとして使用して、含めるポリシーの範囲を定義できます。たとえば、以下のようになります。`policies aws-s3-*` は、AWS S3 バケットに関連するすべてのポリシーをスキャンに		`aws-iam-role-public-access-exists,aws-sqs-queue-encryption-disabled`

パラメーター	説明	デフォルト	例
	含めます。CLI からポリシー ID 情報を取得する方法については、クラウドサイバーエクスポージャーのドキュメントを参照してください。		
サイレント	スキャン結果の内容を標準ワークフロー出力に出力するかどうか。スキャン結果の出力には、スキャン中に見つかった問題に関する詳細情報が含まれる。ログから独立している。可能な値は次のとおりです。`true` `false`	`false`	`false`
types	スキャンを Tenable する IaC フレームワークです。値を入力しない場合、Tenable はすべてのフレームワークをスキャンします。可能な値は次のとおりです。 • `terraform` • `terraform-plan` • `cloudformation`		`terraform`

注意: `output-file-name` パラメーターを使用して結果を **junit** 形式に出力する場合、Tenable は生成されたファイル名に `junit` プレフィックスを追加します。たとえば、名前を `results` に設定した場合、生成されるファイル名は `junit-results.xml` になります。

注意: `output file formats` パラメーターを使用して IaC およびコンテナイメージスキャンの`sarif`出力を生成すると、クラウドサイバーエクスポージャーの検出結果が GitHub の **[コードスキャン]** セクションに直接表示されます。検出結果には、深刻度分類、相対ファイルパス、リッチテキストの説明、関連するタグが含まれます。スキャン結果には、次のタグが含まれます。

- `security`
- `tenable iac`
- カテゴリタグ (例: `tenable iac iam` や `tenable iac compute`)

GitHub Actions 同期パラメーター

GitHub アクションで以下の入力パラメーターを設定して、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整します。

パラメーター	説明	デフォルト	例
api-token (必須)	Tenable との通信に使用される API トークン。GitHubアクションの初期セットアップ中に、クラウドサイバーエクスポージャーコンソールで生成されます。	-	
api-url (必須)	クラウドサイバーエクスポージャー API の URL。	-	`https://app.tenable.com/`

パラメーター	説明	デフォルト	例
gitトークン	同期時にクラウドサイバーエクスポージャーが必要とするプライベートコードリポジトリのアクセストークン。たとえば、プライベートTerraformモジュールにアクセスするには、これらのトークンが必要になる場合があります。複数のトークンがある場合は、コンマで区切ります。形式：ORGANIZATION_URL=YOUR_TOKEN	-	`https://github.com/org=YOUR_TOKEN`
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ログメッセージには、スキャナーの実行プロセスに関する情報や、スキャンされたファイル数や行数などのデバッグ情報が含	-	`true`

パラメーター	説明	デフォルト	例
	まれる。可能な値は次のとおりです。 `true` `false`		
パス	コンマ区切りリストとして入力された、Tenableによって同期されるTerraform ルートモジュールのパス。空白のままにすると、Tenable は作業ディレクトリを同期します。	-	`prod/`
サイレント	同期結果の内容を標準ワークフロー出力に出力するかどうか。同期結果の出力には、オリジンまでトレースされたファイルに関する情報が含まれます。ログから独立している。可能な値は次のとおりです。 `true` `false`	`false`	`false`
状態ファイルパス	Terraform の状態ファイルのパス。	`terraform.tfstate`	`terraform.tfstate`

GitLab CI/CD パラメーター

入力パラメーターを設定して、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整します。

- GitLab CI/CD スキャンパラメーター

GitLab CI/CD スキャンパラメーター

GitLab CI/CD で以下の入力パラメーターを設定し、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整します。

パラメーター	説明	デフォルト	例
api-token (必須)	クラウドサイバーエクスポージャーとの通信に使用される API トークン。GitLab CI/CD の初期セットアップ中に、クラウドサイバーエクスポージャーコンソールで生成されます。		
api-url (必須)	クラウドサイバーエクスポージャー API の URL。		`https://app.tenable.com/`
ステージ (必須)	ジョブを実行するための GitLab CI/CD パイプラインステージ。		`tenable-cloud-security`
exclude-paths	スキャンから特定のパスを除外します。		`dev/`

パラメーター	説明	デフォルト	例
exclude-policies	スキャンから除外するTenableポリシーのID。このパラメーターは「policies」と相互に排他的であるため、入力できるのは2つのうち1つの値のみです。globパターンをワイルドカードとして使用して、ポリシーの範囲を定義できます。たとえば、`exclude-policies aws-s3-*` AWS S3バケットに関連するすべてのポリシーがスキャンから除外されます。		`aws-iam-role-public-access-exists`
fail-on-min-severity	0以外の終了コードを返し、ビルドワークフローを失敗とするポリシーの最小深刻度。値が定義されていない場合、ワークフローは失敗しない。可能な値: • `information` • `low` • `medium` • `high`		`critical`

パラメーター	説明	デフォルト	例
	• `critical`		
gitトークン	スキャン中にクラウドサイバーエクスポージャーが必要とするプライベートコードリポジトリのアクセストークン。たとえば、プライベート Terraform モジュールにアクセスするには、これらのトークンが必要になる場合があります。複数のトークンがある場合は、コンマで区切ります。形式：`ORGANIZATION_URL=YOUR_TOKEN`		`https://gitlab.com/org=YOUR_TOKEN`
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ログメッセージには、スキャナーの実行プロセスに関する情報や、スキャンされたファイル数や行数などのデバッグ情報が含まれる。可能な値は次のとおりです。`true` `false`	`false`	`true`
min-	スキャンに含める	`information`	`medium`

パラメーター	説明	デフォルト	例
severity	Tenable ポリシーの最小深刻度です。可能な値: • `information` • `low` • `medium` • `high` • `critical`		
output-file-formats	エクスポートされるレポート出力ファイルの形式。複数の形式の値を入力して、複数の形式でレポートを出力できます。可能な値: • `csv` • `json` • `junit` • `sarif`[^1] • `md`	`json`	`json,csv`
出力ファイル名	エクスポートされるレポート出力ファイルの名前。複数の形式を選択すると、すべてのファイルに同じ名前が付くようになります。	`results`	`results`

パラメーター	説明	デフォルト	例
output-junit-test-name-prefix	JUnit テスト出力名のプレフィックス。テスト結果に第 1 レベルの階層を作成するために使用される。junitが出力ファイル形式として定義されている場合に使用できます。		`Scan1`
出力パス	レポート出力ファイルのエクスポートパス。		`results/`
パス	Tenableによってスキャンされるリポジトリパス。空白のままにすると、リポジトリ全体 Tenable スキャンされます。		`prod/`
ポリシー	コンマ区切りリストとして入力された、リポジトリのスキャンに使用されるクラウド サイバーエクスポージャー ポリシーの ID。値を入力しない場合、すべてのポリシーがスキャンされます。このパラメーターは「exclude-policies」と相互に排他的であるため、入力できるのは 2 つ		`aws-iam-role-public-access-exists-terraform,aws-sqs-queue-encryption-disabled`

パラメーター	説明	デフォルト	例
	のうち 1 つの値のみです。glob パターンをワイルドカードとして使用して、含めるポリシーの範囲を定義できます。たとえば `policies aws-s3-*` の場合、AWS S3 バケットに関連するすべてのポリシーがスキャンに含まれます。CLI からポリシー ID 情報を取得する方法については、クラウドサイバーエクスポージャーのドキュメントを参照してください。		
サイレント	スキャン結果の内容を標準ワークフロー出力に出力するかどうか。スキャン結果の出力には、スキャン中に見つかった問題に関する詳細情報が含まれる。ログから独立している。可能な値は次のとおりです。`true` `false`	`false`	`true`
types	スキャンを Tenable する IaC フレームワークです。		`terraform`

パラメーター	説明	デフォルト	例
	値を入力しない場合、Tenable はすべてのフレームワークをスキャンします。可能な値は次のとおりです。 • `terraform` • `terraform-plan` • `cloudformation`		

注意: `output-file-name` パラメーターを使用して結果を **junit** 形式に出力する場合、Tenable は生成されたファイル名に `junit` プレフィックスを追加します。たとえば、名前を `results` に設定した場合、生成されるファイル名は `junit-results.xml` になります。

注意: `output-file-formats` パラメーターを使用して IaC およびコンテナイメージスキャンの`sarif`出力を生成すると、GitLab **の [パイプラインセキュリティ]** タブと**セキュリティダッシュボード**に検出結果が表示されます。詳細は、GitLab のドキュメントを参照してください。検出結果には、深刻度分類、相対ファイルパス、リッチテキストの説明、関連するタグが含まれます。スキャン結果には次のタグが含まれます。

- `security`
- `tenable iac`
- スキャンカテゴリタグ (例: `tenable iac iam` や `tenable iac compute`)

Tenable Docker イメージの CLI

Tenable Docker イメージ CLI を使用して以下のコマンドを設定し、Tenable が環境をスキャンする方法を微調整します。

注意: CI/CD パイプラインを Tenable に接続する際にイメージが抽出されます。

コマンドのリスト

次のコマンドを使用して、スキャンを実行し、Tenable IaC ポリシーを一覧表示し、CLI バージョンを出力します。各コマンドで一覧表示されているフラグ (または グローバルフラグ) を使用して、コマンドの実行方法を微調整します。

- iac scan
- iac sync terraform
- IaC list-policies
- version

IaC スキャン

Tenable IaC スキャンを実行します。

使用

```
tenable iac scan [flags]
```

フラグ

```
      --api-token string
      --api-url string
      --code-branch string                    (auto detected)
      --code-commit-hash string               (auto detected)
      --code-commit-user string               (auto detected)
      --code-repository-url string            (auto detected)
      --exclude-paths strings
      --exclude-policies strings
      --fail-on-min-severity string           minimum severity that should return an exit code different
from 0
      --git-tokens stringToString              (default [])
-h, --help                                    help for scan
      --min-severity string                   Information,Low,Medium,High,Critical (default "information")
      --output-file-formats strings           Csv,Json,JUnit,Md,Sarif (default [json])
      --output-file-name string                (default "results")
      --output-junit-test-name-prefix string
      --output-path string
      --path string                            (default ".")
      --pipeline-run-id string
```

```
    --pipeline-run-trigger string
    --pipeline-run-url string
    --policies strings
    --types strings
Arm,Bicep,CloudFormation,Helm,Kubernetes,Terraform,TerraformPlan
```

注意: 結果を **junit** 形式に出力するために `output-file-name` フラグを使用する場合、Tenable は生成されたファイル名に `junit` プレフィックスを追加します。たとえば、名前を `results` に設定した場合、生成されるファイル名は `junit-results.xml` になります。

IaC Terraform 同期

使用

```
tenable iac sync terraform [flags]
```

フラグ

```
--api-token string
--api-url string
--code-branch string            (auto detected)
--code-commit-hash string       (auto detected)
--code-commit-user string       (auto detected)
--code-repository-url string    (auto detected)
--git-tokens stringToString     (default [])
--help, -h                      help for terraform
--path string                   terraform root module path (default ".")
--pipeline-run-id string
--pipeline-run-trigger string
--pipeline-run-url string
--state-file-path string        (default "terraform.tfstate")
```

IaC list-policies

スキャンで使用される Tenable ポリシーを一覧表示します。

使用

```
tenable iac list-policies [flags]
```

フラグ

```
  --clouds strings   list policies for specific clouds aws,azure,gcp
  --help, -h         help for list-policies
  --types strings    list policies for specific code types cloud-formation,kubernetes,terraform,terraform-
  plan
```

version

Tenable CLI のバージョンを出力します。

使用

```
  tenable version [flags]
```

フラグ

```
  --help, -h   help for version
```

グローバルフラグ

上記のコマンドのいずれかで、次のグローバルフラグを使用します。

```
  --logs       print log messages to standard output
  --no-color   print output without color
  --silent     do not print output to standard output (edited)
```

フラグを環境変数として使用する

Jenkins パイプラインの追加または汎用 Docker パイプラインを クラウドサイバーエクスポージャー に追加するときは、一連の環境変数を設定します。コンソールウィザードとパラレルドキュメントの両方に一覧表示される変数は、クラウドサイバーエクスポージャー コンソール内で基本的なレポート機能を提供するように設計されています。より高度な構成要件に準拠したり、スキャン設定をさらに微調整したりするために、グ

ローバルフラグなど、Tenable Docker イメージに含まれるすべてのフラグを環境変数として構成することもできます。

フラグと環境変数の構文

CLI フラグと環境変数は異なる構文を使用します。次の手順を使用して、特定のフラグを環境変数に変換します。

フラグ構文を環境変数として使用するための変換方法

1. フラグ名の前のダッシュを削除します。
2. ダッシュをアンダースコアに置き換えます。
3. プレフィックスとして「TENABLE_」(アンダースコア付き) を入力します。
4. すべて大文字を使用します。
5. ブーリアンフラグ (フラグを環境変数として使用するを参照) をアクティブ化するには、TRUE に設定する必要があります。

したがって、たとえば --code-repository-url フラグを環境変数として使用する場合、TENABLE_CODE_REPOSITORY_URL になります。

Terraform Cloud エンドポイント URL の設定

Terraform Cloud パイプラインでは、実行タスクのエンドポイント URL を設定して、クラウドサイバーエクスポージャー が環境をスキャンする方法を微調整できます。これを行うには、以下のパラメーターを 1 つ以上使用してエンドポイント URL を修正します。これらのパラメーターを URL に変更する方法の例については サンプル URL を参照してください。

エンドポイント URL の設定を含む、完全な実行タスク設定については、Terraform Cloud Run タスクの追加 を参照してください。

- failOnMinSeverityで共有されます。実行ワークフローを失敗とするポリシーの最小深刻度。可能な値

- information
- low
- medium
- high
- critical

- excludePolicies。スキャンから除外する](/docs/ja/iac-policies)[TenableポリシーのID。このパラメーターは相互に排他的です。policies入力できるのは2つのうち1つの値のみです。
- policies. コンマ区切りリストとして入力された、リポジトリのスキャンに使用されるTenableポリシーのID。値を入力しない場合、すべてのポリシーがスキャンされます。このパラメーターは相互に排他的です。excludePolicies入力できるのは2つのうち1つの値のみです。

サンプルURL

- https://app.tenable.com/api/terraformcloud/runtasks/scan?apiToken={API token}&excludePolicies=52ffcfa6-6c70-4ea6-8376-d828d3961669&failOnMinSeverity=Critical
- https://app.tenable.com/api/terraformcloud/runtasks/scan?apiToken={API token}&policies=52ffcfa6-6c70-4ea6-8376-d828d3961669,586f29d7-e60e-4211-858c-b1c06d339fa2,5d9e3164-9265-470c-9a10-57ae454ac0c7&failOnMinSeverity=High

従来のリリースパイプラインを使用している場合に必要な追加のパラメーター

パラメーター	説明	デフォルト	例
codeCommitUser	コミットを実行した作成者のユーザー名。		

パラメーター	説明	デフォルト	例
codeRepositoryUrl	リポジトリURL。		`https://github.com/orgName/repoName`
pipelineRunTrigger	パイプライン実行をトリガーしたアクティビティ。		`Manual`, `PullRequest`, `BuildCompletion`

構成例

Azure Pipelinesの次のサンプル構成では、`terraform`スキャンの`./terraform_resources`パスをスキャンし、深刻度が`high`以上のポリシーのビルド ワークフローを失敗させるようにTenableに指示します。

YAML

```
-task: ErmeticIacScan@1
 inputs:
    apiToken: '$(TENABLE_API_TOKEN)`
    apiURL: `https://app.tenable.com`
    failOnMinSeverity: `high`
    path: `./terraform_resources`
    types: `terraform`
```

出力例

- JSON
- CSV

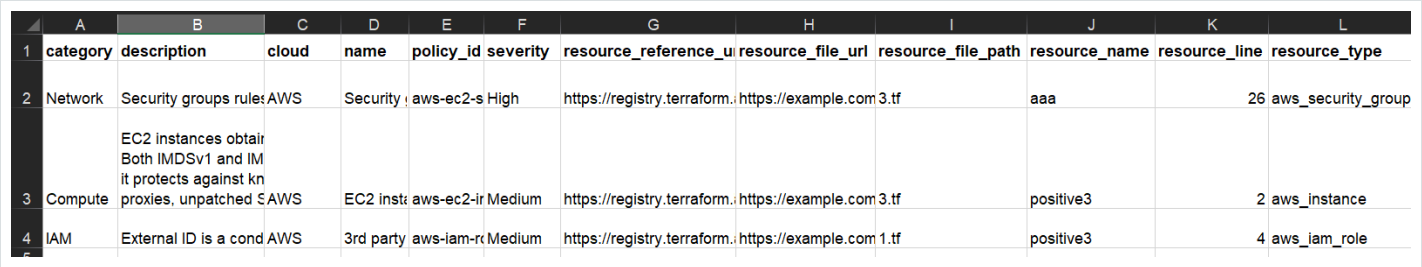
JSON

JSON


```
{
  "end_time": "2024-07-07T13:35:07.940626+03:00",
  "file_count": 22,
  "iac_findings": [
    {
      "cloud": "AWS",
      "description": "At least one stage of your API Gateway API should be associated with AWS WAF web
ACL.\nDoing so protects web applications and APIs from threats, and enables you to control how traffic
reaches your applications.\nThis policy is only applicable to REST APIs.",
      "name": "API Gateway API is not associated with WAF web ACL",
      "policy_category": "Network",
      "policy_id": "aws-api-gateway-api-web-acl-not-exists",
      "resources": [
        {
          "file_path": "1.json",
          "file_url": "https://example.com/foo/bar/blob/afasdfasdfasdfasdfasdf/api_web_acl_not_
exists/1.json",
          "line": 5,
          "name": "positive1",
          "reference_url": "https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-
apigateway-restapi.html",
          "type": "AWS::ApiGateway::RestApi"
        }
      ],
      "severity": "Low"
    }
  ],
  "iac_findings_by_severity": {
    "Critical": 0,
    "High": 0,
    "Information": 0,
    "Low": 1,
    "Medium": 0
  },
  "iac_findings_count": 8,
  "parsed_file_count": 14,
  "path": "api_web_acl_not_exists",
  "policies": [
    {
      "category": "Network",
      "codeTypes": [
        "TerraformPlan",
        "Terraform",
        "CloudFormation"
      ],
      "description": "At least one stage of your API Gateway API should be associated with AWS WAF web
```

```
ACL.\nDoing so protects web applications and APIs from threats, and enables you to control how traffic
reaches your applications.\nThis policy is only applicable to REST APIs.",
      "id": "aws-api-gateway-api-web-acl-not-exists",
      "infrastructureTenantType": "Aws",
      "name": "API Gateway API is not associated with WAF web ACL",
      "severity": "Low"
    }
  ],
  "resource_count": 58,
  "start_time": "2024-07-07T13:35:07.5278667+03:00",
  "success": true,
  "version": "1.124.1"
}
```


CSV



	A	B	C	D	E	F	G	H	I	J	K	L
1	category	description	cloud	name	policy_id	severity	resource_reference_u	resource_file_url	resource_file_path	resource_name	resource_line	resource_type
2	Network	Security groups rules	AWS	Security	aws-ec2-s	High	https://registry.terraform.	https://example.com	3.tf	aaa	26	aws_security_group
3	Compute	EC2 instances obtair Both IMDSv1 and IM it protects against kn proxies, unpatched S	AWS	EC2 insta	aws-ec2-ir	Medium	https://registry.terraform.	https://example.com	3.tf	positive3	2	aws_instance
4	IAM	External ID is a cond	AWS	3rd party	aws-iam-r	Medium	https://registry.terraform.	https://example.com	1.tf	positive3	4	aws_iam_role

クラウドからコードまで同期

問題をコードのオリジンまでさかのぼってトレースするには、CI/CD パイプラインを クラウドサイバーエクスポージャー

> **注意:** コードまで問題をトレースするのにサポートされているプラットフォーム/パイプラインを確認するには、IaC 互換性マトリクス を参照してください。

CI/CD パイプラインを Tenable に接続する際に同期ステップ/タスクを追加することで、クラウドリソースに関連付けられたコードを同期します (Cloud to Code)。現在、AWS、Azure/Microsoft Entra ID、GCP、Google Workspace リソースがサポートされています。

ワークロード

ワークロードの接続

特定のアカウントでワークロード保護を有効にするには、アカウントをオンボーディングして Tenable One Cloud Exposure し、そのアカウント Tenable ワークロードスキャンのアクセス許可を付与する必要があります。

- AWS
- Azure: 仮想マシンスキャンのアクセス許可を付与する
- GCP: ワークロード保護のアクセス許可を付与する
- OCI: ワークロード保護のアクセス許可を付与する
- Alibaba Cloud: ワークロード保護のアクセス許可を付与する
- オンプレミスワークロードの接続

AWS: EC2 インスタンスおよび内部 AMI スキャン (ワークロード保護)

Tenable IAM ロールに追加されたカスタムのインラインポリシーを使用して、AWSワークロードをスキャンするアクセス許可をクラウドサイバーエクスポージャーに付与します。これらのアクセス許可は、Tenable ウィザードでの AWS 統合プロセスの一部として (EC2 インスタンススキャンのアクセス許可を通じて) 付与されますが、アカウントをオンボーディングした時期によっては、まだ付与されていない場合もあります。

- ワークロードをスキャンする AWS アカウントをすでにオンボーディングしているものの、EC2 インスタンススキャンのアクセス許可がまだ追加されていない場合は、以下の手順に従います。
- ワークロードをスキャンする AWS アカウントをまだオンボーディングしていない場合は、「AWS アカウントの接続」に記載されている手順に従います。

EC2 インスタンススキャンのアクセス許可がすでに追加されているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **[Settings > Accounts > AWS]** に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [Connected with issues] (接続に問題あり) であり、ツールチップにワークロード保護のアクセス許可が付与されていないことが示されている場合は、以下の手順に従います。

EC2 インスタンスと内部 AMI スキャンのアクセス許可を付与する方法

1. 関連するアカウントの AWS 管理コンソールで、[IAM > **Roles**] (**IAM** ロール) に移動し、アカウントのオンボーディング時に Tenable 用に作成したロールを開きます。
2. [アクセス許可] タブで、**[アクセス許可の追加]** > **[インラインポリシーの作成]** をクリックします。
3. クラウドサイバーエクスポージャーコンソールの [AWS Add Account (アカウントの追加)] ウィザードのステップ 3 (IAM ロール) で提供されたポリシーをコピーし、[JSON] タブに貼り付けて既存のテキストを置き換えます。JSON 形式のポリシーを確認するには、AWS EC2 インスタンススキャンワークロード保護ポリシー を参照してください。
4. **[ポリシーのレビュー]** をクリックします。
5. ポリシーの名前 (例: TenableWorkloadProtection) を入力し、**[ポリシーの作成]** をクリックします。
6. クラウドサイバーエクスポージャーコンソールで、**[Settings > Accounts > AWS]** に移動し、アカウントのステータスが [Connected] (接続済み) であることを確認します。

注意: ステータスが [接続済み] に変わるまで数分かかる場合があります。またブラウザでハードリフレッシュの実行が必要になる場合もあります。

AWS EC2 インスタンススキャンワークロード保護ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect": "Allow",
      "Action": "kms:CreateAlias",
      "Resource": "arn:aws:kms:*:*:alias/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "kms:CreateKey",
```

```
        "kms:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/ErmeticContext": "WorkloadAnalysis"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "kms:TagResource",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/ErmeticContext": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CopySnapshot",
      "Resource": "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "kms:CreateAlias",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:EnableKeyRotation",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ErmeticContext": "WorkloadAnalysis"
        }
      }
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Azure: 仮想マシンスキャンのアクセス許可を付与する

`Disk Snapshot Contributor`ロールを割り当てることで、Azure ワークロードをスキャンするために必要なアクセス許可をクラウドサイバーエクスポージャーに付与します。これらのアクセス許可は通常、ウィザードでの Azure サブスクリプションの接続 の一部として付与 Tenable 。ただし、組織またはサブスクリプションがオンボーディングされたタイミングによっては、アクセス許可がまだ付与されていないことがあります。

- ワークロードをスキャンする Azure サブスクリプションをすでにオンボーディングしているものの、仮想マシンスキャンのアクセス許可がまだ追加されていない場合は、以下の手順に従います。
- ワークロードをスキャンする Azure サブスクリプションをまだオンボーディングしていない場合は、Azure サブスクリプションの接続に記載されている手順に従います。

仮想マシンスキャンのアクセス許可を付与するには:

1. Azure ポータルで、**[サブスクリプション]** ページに移動し、関連するサブスクリプションをクリックします。
2. **[アクセス制御 (IAM)]** をクリックし、**[追加]** > **[ロール割り当ての追加]** をクリックします。
3. [ロールの割り当ての追加] ページで、**ディスク スナップショット コントリビューター** ロールを検索して選択し、**[次へ]** をクリックします。または、カスタムロールを使用した特定の Azure アクセス許可の付与。

組み込みロールを使用したWindowsアクセス許可の付与

- **BitLocker**を備えた仮想マシンまたは**DM-Crypt** (Ubuntuでのみサポートされている) ディスク暗号化を備えたLinux仮想マシンWindowsスキャンをサポートするには、TenableにKey Vault Secrets Userロールを付与する必要があります。
- Key Vault (KEK) のキーを含む**BitLocker**暗号化シークレットを持つ仮想マシンWindowsスキャンをサポートするには、TenableにKey Vault Crypto Userロールも付与する必要があります。
- これらのアクセス許可は、サブスクリプションごとまたはKey Vaultごとに付与できます。
- アクセス許可が付与されていない場合、関連する仮想マシンのスキャンステータスは**[無効]**になります。
- アクセス許可を付与した後すぐに仮想マシンがスキャンされるわけではありません。Tenableは、前回のスキャンから24時間が経過するとすぐに各仮想マシンのスキャンを試みます。

4. [*アクセスの割り当て先*] は、デフォルトの選択**[ユーザー、グループ、またはサービスプリンシパル]**のままにします。
5. [*メンバー*] で、**[+メンバーを選択]**をクリックします。
6. **クラウドサイバーエクスポージャーコネクタアプリ**を検索して選択し、**[選択]**をクリックします。
7. **[次へ]**をクリックし、新しいロールを確認して**[レビューと割り当て]**をクリックします。

カスタムロールを使用した特定のAzureアクセス許可の付与

ディスクスナップショット共同作成者ロールを介してAzureワークロードをスキャンするアクセス許可をクラウドサイバーエクスポージャーに付与する代わりに、カスタムロールを使用して、より制限されたアクセス許可セットを付与できます。暗号化された仮想マシンのスキャンに必要な追加のKey Vaultアクセス許可を含む、カスタムロールのアクセス許可の完全なリストについては、「Azureの必要なアクセス許可」を参照してください。

カスタムロールを使用して特定のAzureアクセス許可を付与する方法:

1. Azureの必要なアクセス許可に記載されているアクセス許可を持つカスタムロールを作成します。
2. 仮想マシンスキャンのアクセス許可を付与するの手順に従いますが、「**ディスクスナップショット共同作成者**」ロールを選択する代わりに、作成したカスタムロールを選択します。

GCP: ワークロード保護のアクセス許可を付与する

カスタムポリシーを使用して、GCP ワークロードをスキャンするアクセス許可をクラウドサイバーエクスポージャーに付与します。これらのアクセス許可は、Tenable ウィザードでの GCP オンボーディングプロセスの一部として付与されますが、組織またはプロジェクトをオンボーディングした時期によっては、まだ付与されていない場合もあります。

- ワークロードをスキャンする GCP の組織またはプロジェクトをすでにオンボーディングしているものの、ワークロード保護のアクセス許可がまだ追加されていない場合は、以下の手順に従います。
- ワークロードをスキャンする GCP の組織またはプロジェクトをまだオンボーディングしていない場合は、Google Workspace の接続に記載されている手順に従います。

ワークロード保護のアクセス許可がすでに追加されているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **GCP** > **[Settings** > **Accounts]** (アカウント) に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが[Missing workload protection permissions] (ワークロード保護のアクセス許可なし) の場合は、以下の手順に従って不足しているアクセス許可を追加します。

ワークロードのアクセス許可を付与するには

1. 関連する環境の GCP コンソールで、**[組織]** スコープに移動します。
2. 左上にある三本線メニューをクリックして、**[IAM]** > **[IAM]** の順にクリックします。
3. 左側のメニューで **[ロール]** をクリックします。
4. **[+ ロールを作成]** をクリックします。
5. ロールの意味のある **タイトル**、**説明**、**ID** を入力します。たとえば、タイトルとして「 **Tenable Workload Scanning Permissions** 」と入力できます。
6. **[+ 権限を追加]** をクリックします。
7. **[ワークロード保護]** の Google の必要なアクセス許可にリストされているアクセス許可を追加します。フィルターを使用して各アクセス許可を検索して選択し、**[追加]** をクリックします。

完了すると、7 つのアクセス許可がすべて割り当てられていることが確認できるはずです。

8. **[作成]** をクリックします。
9. 左側のメニューで **[IAM]** をクリックします。
10. **[+アクセスを許可]** をクリックします。
11. Tenableウィザードのステップ 4 (ワークロードスキャンのアクセス許可を付与する) に表示されるサービスアカウントをコピーし、**[プリンシパルの追加]** セクションに貼り付けます
12. [ロールの割り当て] セクションで、先ほど作成したカスタムロールをフィルタリングして選択します。
13. **[保存]** をクリックします。

OCI: ワークロード保護のアクセス許可を付与する

新しい OCI ポリシーを作成し、ポリシーステートメントを使用して必要なアクセス許可を割り当てることで、クラウドサイバーエクスポージャーに OCI ワークロードをスキャンするアクセス許可を付与します。

ワークロード保護のアクセス許可を付与する方法

1. クラウドサイバーエクスポージャーコンソールで、オンボーディングウィザードの **[OCI ワークロード保護]** トグルが有効になっていることを確認します。
2. Oracleコンソールで、**[アイデンティティとセキュリティ]** > **[アイデンティティ > ポリシー]** の順に移動します。
3. **[ポリシーの作成]** をクリックし、以下の詳細を入力します。
    1. **名前**: 意味のある名前を入力します。
    2. **説明**: わかりやすい説明を入力します
    3. **コンパートメント**: root コンパートメントを選択します
4. ポリシー・ビルダーで、「 **手動エディタの表示** 」をクリックし、「 OCIの必要なアクセス許可 」にリストされているステートメントを追加します。

> **注意:** 所有および管理するキーで暗号化されたボリュームをスキャンする必要がある場合は、同じ記事の暗号化ボリュームにリストされているステートメントも追加します。

Alibaba Cloud: ワークロード保護のアクセス許可を付与する

Tenable RAM ロールに追加されたカスタムのインラインポリシーを使用して、Alibaba Cloud ワークロードをスキャンするアクセス許可を クラウド サイバーエクスポージャー に付与します。これらのアクセス許可は、Tenable ウィザードでの Alibaba Cloud 統合プロセスの一部として付与されますが、アカウントをオンボーディングした時期によっては、まだ付与されていない場合もあります。

- ワークロードをスキャンする Alibaba Cloud アカウントをすでにオンボーディングしているものの、ワークロード保護のアクセス許可がまだ追加されていない場合は、以下の手順に従います。
- ワークロードをスキャンする Alibaba Cloud アカウントをまだオンボーディングしていない場合は、「Alibaba Cloud アカウントの接続」に記載されている手順に従います。

ワークロード保護のアクセス許可がすでに追加されているかどうかを確認するにはSettings、クラウド サイバーエクスポージャーコンソールで **[> Organization > Accounts > Alibaba Cloud]** に移動し、アカウントのステータスを確認します。

- ステータスが **[接続済み]** の場合、必要なアクセス許可はすでに付与されています。
- ステータスが **[Connected with issues] (接続に問題あり)** であり、ツールチップにワークロード保護のアクセス許可が付与されていないことが示されている場合は、以下の手順に従います。

ワークロード保護のアクセス許可を付与する方法

1. 関連するアカウントの RAM コンソールで、**[Permissions > Policies]** に移動します
2. 「**ポリシーの作成**」をクリックし、「**JSON エディター**」を選択します。
3. JSON エディターに Alibaba Cloud の必要なアクセス許可 のポリシーを貼り付けます。
4. **[OK]** をクリックします。
5. **[ポリシー名]** に `tenable-workload-policy` と入力し、**[OK]** をクリックします。
6. **[アイデンティティ] > [ロール]** に移動し、組織のオンボーディング中にTenable用に作成したロールを開きます。
7. **[アクセス許可の付与]** をクリックします。
8. **[ポリシー]** セクションで、作成したばかりのポリシーを選択します。
9. **[OK]**、**[閉じる]** の順にクリックします。

10. クラウド サイバーエクスポージャーコンソールで、**Settings > [Organization > Accounts > Alibaba Cloud]** に移 動し、アカウント のステータスが **[Connected] (接 続 済 み)** であることを確 認します。

注 意: ステータスが **[接 続 済 み]** に変 わるまで数 分 かかる場 合 があります。またブラウザでハードリフレッシュ の実 行 が必 要 になる場 合 もあります。

オンプレミスワークロード の接 続

Helm チャート を使 用してオンプレミスワークロードをスキャンするアクセス許 可 を クラウド サイバーエクスポージャー に付 与します。詳 細 については、Helm チャートを介してクラスタを接 続 する を参 照してください。

コンテナイメージ CI/CD パイプライン の接 続

注 意: この機 能 は、**Cloud Vulnerability Management** ライセンスでは使 用 できません。

CI/CD パイプライン を Tenable One Cloud Exposure に接 続し、関 連 するコードリポジトリへのアクセスを許 可 します。

- Azure Pipelines の追 加
- GitHub アクションを追 加 する
- GitLab パイプライン の追 加
- Jenkins パイプライン の追 加
- 別 のパイプラインを追 加 する

これは、コンテナイメージ CI/CD パイプライン を Tenable に接 続 するための統 合 ガイド です。

- スキャン結 果 の表 示 に関 するハウツーガイド については、コンテナイメージ CI/CD を参 照してくださ い。
- Tenable のコンテナイメージスキャン機 能 の概 要 については、コンテナイメージスキャンを参 照してくだ さい。

Azure Pipelines の追 加

Azure Pipelines でパイプラインを追加した後、Azure Pipelines パラメーターを使用して、スキャン/同期設定を構成し、クラウド サイバーエクスポージャー が環境をスキャンする方法を微調整できます。

要件:

- Node.js と npm をビルド エージェントにインストールする必要があります。

  > **注意:** Microsoft がホストするエージェントにはデフォルトで含まれていますが、セルフホストのビルド エージェントを使用している場合は、環境の PATH 変数で明示的にインストールまたはアクティブ化する必要があります。これを行うには、Microsoft の NodeTool タスクを追加します。行わなかった場合、以下のエラーが発生する可能性があります。`Parameter 'toolPath' cannot be null or empty`

- Docker をインストールする必要があります。詳細は関連する Azure ドキュメントを参照してください。

パイプラインを追加する方法

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Azure Pipelines]** をクリックします。[Azure Pipelines の追加] ウィザードが開きます。
3. **API トークンを作成します** (ウィザードのステップ 1)。トークンを作成するには、「**トークン名**」を入力し、「**次へ**」をクリックします。
4. **API トークンを保存します** (ウィザードのステップ 2)。生成された**トークン**をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。
5. **TenableをインストールするAzure DevOps 拡張機能** (ウィザードのステップ 3):
   1. このリンクをクリックして、Visual Studio マーケットプレースから拡張機能にアクセスします。
   2. **[Get it Free]** をクリックします。拡張機能の使用に追加料金はかかりません。
   3. 関連する Azure DevOps 組織を選択し、**[インストール]** をクリックします。
   4. これで拡張機能がインストールされたので、**[組織に進む]** をクリックして Azure DevOps サイトに移動できます。

6. (推奨) **シークレット変数を追加します** (ウィザードのステップ 4)。UI を使用してシークレット変数を設定するには、次の手順に従います。

   > **注意:** Tenable の API トークンを保護するには、シークレット変数、または代替シークレットストア (現在使用している場合) のいずれかを使用することをお勧めします。Azure Pipelines 変数は、Tenable のスキャンの利用方法に応じてさまざまな範囲で保存できます。Tenable のトークンは、IaC コードとともにリポジトリにリンクされたワークフローのみに関連付けることが推奨されていますが、必須ではありません。

   1. Azure DevOps にログインし、**[パイプライン]** をクリックします。
   2. 関連するパイプラインを選択し、**[編集]** をクリックします。
   3. **[変数]** をクリックします。
   4. プラス記号 (+) または [New variable] (新しい変数) をクリックします
   5. 以下の詳細を入力し、**[OK]** をクリックします。
      - **名前**を **TENABLE_API_TOKEN** に設定します。
      - 前のステップで作成したトークンを **[値]** として貼り付けます。
      - **[Keep this value secret]** にチェックを入れます。

   完了したら、クラウド サイバーエクスポージャー コンソール ウィザードの **次へ** をクリックして続行します。

7. **タスクを追加します**。クラウド サイバーエクスポージャー **コンテナー イメージのスキャン** タスクを Azure Pipelines に追加します (ウィザードの手順 5)。
   1. Azure DevOps にログインし、**[パイプライン]** をクリックします。
   2. 関連するパイプラインの横にある三点リーダーアイコンをクリックし、**[編集]** をクリックします。
   3. コードで、Tenable のタスクを追加するステージを選択します。
   4. タスクアシスタントで、**[クラウド サイバーエクスポージャー Container Image Scan]** タスクを検索してクリックします。
   5. タスクを追加するには、これらの値を入力してから、**[追加]** をクリックします。
      - API トークン: **$(TENABLE_API_TOKEN)**
      - API URL: **https://app.tenable.com/**
      - 名前:(ここに画像名を入力します)

- 必要に応じて、**任意の詳細** 設定を使用します (詳細については、「Azure Pipelines パラメーター」を参照してください)。

6. 更新されたパイプライン YAML を**保存**します。アクションがトリガーされたら、**[Risks > Container Image CI/CD Scans] (コンテナイメージ CI/CD スキャンのリスク)** にスキャン結果が表示されます。

8. コンソール クラウド サイバーエクスポージャー ウィザードで、**[完了]** をクリックします。

GitHub アクションを追加する

アクションを追加した後、GitHub アクションパラメーターを使用して、スキャン設定を行い、Tenable が環境をスキャンする方法を微調整できます。

GitHub アクションを追加するには

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**GitHub Actions** をクリックします。[Add GitHub Actions] ウィザードが開きます。
3. **API トークンを作成します** (ウィザードのステップ 1)。トークンの名前を入力し、「**次へ**」をクリックしてトークンを作成します。
4. **API トークンを保存します** (ウィザードのステップ 2)。生成されたトークンをコピーして安全な場所に保存します。この情報は、ウィザードの次のステップで必要になります。完了したら、**[次へ]** をクリックします。
5. (推奨) **GitHub シークレットを追加します** (ウィザードのステップ 3)。API トークンを安全に格納するには、GitHub Actions シークレット、または他のシークレット ストア (現在使用している場合) のいずれかを使用することをお勧めします。

   GitHub リポジトリに新しいシークレットを作成するには、以下の手順を実行します。

   1. GitHub.com から、リポジトリのメインページに移動します。
   2. リポジトリ名の下にある **[Settings]** をクリックします。
   3. サイドバーの「セキュリティ」セクションで、「**シークレット**」を選択し、「**アクション**」をクリックします。

4. **[新しいリポジトリシークレット]** をクリックします。
5. [名前] 入力ボックスに「**TENABLE_API_TOKEN**」と入力します。
6. 前のステップで作成したトークンの値を入力します。
7. **[シークレットの追加]** をクリックします。
   完了したら、クラウドサイバーエクスポージャーコンソールウィザードの **[次へ]** をクリックします。

6. **アクションを追加します** (ウィザードのステップ 4)。次のコンテナイメージのスキャンアクションを GitHub ワークフローに追加します。

```yaml
steps:
- uses: actions/checkout@v3
- name: Scan container image with Tenable One Cloud Exposure
  uses: tenable/cloud-security-actions/container-image/scan@v1
  with:
    api-token: ${{ secrets.TENABLE_API_TOKEN }}
    api-url: https://app.tenable.com/
    name: <place your image name here>
```

   アクションがトリガーされたら、**[Risks > Container Image CI/CD Scans] (コンテナイメージ CI/CD スキャン**のリスク) にスキャン結果がクラウドサイバーエクスポージャー表示されます。

7. 完了したら、**[完了]** をクリックします。

GitLab パイプラインの追加

GitLab パイプラインを追加した後、Docker イメージTenable CLI を使用してスキャン設定を行い、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整できます。

GitLab の CI/CD YAML 設定の設定オプションの詳細については、GitLab のドキュメントを参照してください。

GitLab パイプラインを追加するには

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。

2. 統合ライブラリで、**[GitLab CI/CD]** をクリックします。[Add GitLab CI/CD] (GitLab CI/CD の追加) ウィザードが開きます。
3. **API トークンを作成します** (ウィザードのステップ 1)。トークンを作成するには、「**トークン名**」を入力し、「**次へ**」をクリックします。
4. **API トークンを保存します** (ウィザードのステップ 2)。生成された**トークン**をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。
5. (推奨) **変数を追加します** (ウィザードのステップ 3)。プロジェクトで CI/CD 変数を定義するには、次の手順に従います。

   > **注意:** Tenable の API トークンを保護するには、マスクされた変数、または他のシークレットストア (現在使用している場合) のいずれかを使用することをお勧めします。GitLab CI/CD 変数は、Tenable のスキャンの利用方法に応じて複数のレベルで保存できます。Tenable のトークンは、IaC コードとともにリポジトリにリンクされたパイプラインのみに関連付けることが推奨されていますが、必須ではありません。

   1. GitLab にログインします。
   2. プロジェクトの **Settings** > **CI/CD** に移動します。
   3. [変数] で、**[展開]** をクリックします。
   4. **[変数の追加]** をクリックします。
   5. 次の詳細を入力します。
      1. **[キー]** を **TENABLE_API_TOKEN** に設定します。
      2. 前のステップで作成したトークンを **[値]** として貼り付けます。
      3. 該当する場合は、**[環境範囲]** を選択します。
      4. **[フラグ]** の下にある **[変数をマスク]** というボックスにチェックを入れます。
      5. **[変数の追加]** をクリックします。

   完了したら、クラウドサイバーエクスポージャーコンソールウィザードの **[次へ]** をクリックします。
6. **ステージを追加します** (ウィザードのステップ 4)。次のコンテナイメージスキャンの手順を .gitlab-ci.yml ファイルに追加します。

YAML

```
include:
- component: $CI_SERVER_FQDN/tenb/cloud-security/components/container-image-scan@1
inputs:
  api-token: $TENABLE_API_TOKEN
  api-url: https://app.tenable.com/
  name: <place your image name here>
  stage: tenable-cloud-security

stages:
- tenable-cloud-security
```

スキャンがトリガーされたら、**[コンテナイメージ CI/CD スキャンのリスク]** > クラウド サイバーエクスポージャーにスキャン結果が表示されます。

7. クラウド サイバーエクスポージャー コンソールウィザードで **[完了]** をクリックします。

Jenkins パイプラインの追加

Jenkins パイプラインを追加した後、Docker イメージで CLI を使用してTenable スキャン/同期設定を行い、クラウド サイバーエクスポージャー が環境をスキャンする方法を微調整できます。

要件:

- Docker がホストにインストールされていること
- Docker プラグインを Jenkins にインストールする必要があります

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[Jenkins Pipeline]** をクリックします。[Add Jenkins Pipeline] (パイプラインの追加) ウィザードが開きます。
3. **API トークンを作成します** (ウィザードのステップ 1)。トークンを作成するには、「**トークン名** 」を入力し、「**次へ**」をクリックします。
4. **API トークンを保存します** (ウィザードのステップ 2)。生成された**トークン** をコピーして安全な場所に保存し、**[次へ]** をクリックします。この情報は、ウィザードの次のステップで必要になります。生成されたトークンは、Tenable への API アクセスを許可するため、シークレットとして扱う必要があります。

5. (推奨) **Jenkins 認証情報を追加します** (ウィザードのステップ 3)。新しいグローバル認証情報を Jenkins に追加するには、以下の手順に従います。

   > **注意:** Tenable の API トークンを保護するには、Jenkins 認証情報、または他のシークレットストア (現在使用している場合) のいずれかを使用することをお勧めします。Jenkins 認証情報は、Tenable のスキャンの利用方法に応じて複数のレベルで保存できます。Tenable のトークンは、IaC コードとともにリポジトリにリンクされたパイプラインのみに関連付けることが推奨されていますが、必須ではありません。

   1. Jenkins にログインします ([Credentials] (認証情報) > [Create permission] (権限の作成) を通じてユーザーとして)。
   2. ホームページで、**[Manage Jenkins > Manage Credentials]** をクリックします。
   3. 右側の **[ストア スコープを Jenkins]** で、**[Jenkins]** をクリックします。
   4. **[System]** (システム) で、**[Global credentials (unrestricted)]**(グローバル認証情報 (無制限)) リンクをクリックして、デフォルトのドメインにアクセスします。
   5. 左側にある **[Add Credentials]** (認証情報の追加) をクリックします (認証情報が存在しない場合は、**認証情報を追加**します)。
      1. **[種類]** フィールドから、**[シークレット テキスト]** を選択します。
      2. **[Scope]**(範囲) フィールドで、**[Global]** (グローバル) を選択します。
      3. ウィザードで以前に作成した **API トークン** をコピーし、**[Secret]** (シークレット) フィールドに貼り付けます。
      4. [ID] フィールドで、**[tenable-api-token]** を指定します。
      5. トークンについてオプションの**説明**を追加します。
      6. **[OK]** をクリックして認証情報を保存します。

   完了したら、クラウド サイバーエクスポージャー コンソールウィザードの **次へ** をクリックします。

6. **ステージを追加します** (ウィザードのステップ 4)。スキャン結果を生成するには、次のコンテナイメージスキャンの手順を Jenkins パイプラインに追加し、必要に応じて環境に合わせて調整します。

   > **注意:**

- スキャン結果を生成するには、環境変数が含まれていることを確認してください。
- TENABLE_API_TOKENフィールドは機密性が高いため、シークレットとして扱う必要があります。
- Gitリポジトリ内でスキャンを実行することをお勧めします。何らかの理由でこれが不可能な場合は、「非 Gitリポジトリの追加変数」を参照してください。

Groovy

```
pipeline {
   agent any
    stages {
        stage('Checkout') {
            steps {
                git '<PLACE YOUR REPOSITORY URL HERE>'
            }
        }
        stage('Scan container image with Tenable One Cloud Exposure') {
            environment {
                TENABLE_API_TOKEN = credentials('tenable-api-token')
                TENABLE_API_URL = 'https://app.tenable.com/'
                TENABLE_CODE_BRANCH = "${env.CHANGE_BRANCH ?: env.GIT_BRANCH}"
                TENABLE_CODE_COMMIT_HASH = "${env.GIT_COMMIT}"
                TENABLE_CODE_COMMIT_USER = "${env.CHANGE_AUTHOR}"
                TENABLE_PIPELINE_RUN_ID = "${env.BUILD_ID}"
                TENABLE_PIPELINE_RUN_TRIGGER = "${currentBuild.getBuildCauses()
[0].shortDescription}"
                TENABLE_PIPELINE_RUN_URL = "${env.BUILD_URL}"
            }
            steps {
                script {
                        docker.image('tenable/cloud-security-scanner:latest').inside("--
entrypoint='' -u 0 --pull=always") {
                            sh 'tenable container-image scan \
                                --name <place you image name here> \
                                --no-color \
                                --output-file-formats JUnit \
                                --output-path .'
                            junit skipPublishingChecks: true, testResults: 'results.junit.xml'
                           }
                    }
                }
            }
        }
    }
```

アクションがトリガーされたら、**[コンテナイメージ CI/CD スキャンのリスク]** > }**クラウド サイバーエクスポージャー** にスキャン結果が表示されます。

> **注意:** 上記の例では、Docker Pipelines プラグインを使用していることを前提としています。

7. 完了したら、**[完了]** をクリックします。

非 Git リポジトリの追加変数

Git リポジトリ内でスキャンまたは同期を実行することをお勧めします。何らかの理由でこれが不可能な場合は、[Add Jenkins Pipeline] (Jenkins パイプラインの追加) ウィザードで一覧表示される変数に加えて、次の変数を追加する必要があります (「Jenkins パイプラインの追加」を参照)。

```
TENABLE_CODE_REPOSITORY_URL=https://github.com/acme/repo1
```

上記のサンプル値を以下のように置き換えます。
TENABLE_CODE_REPOSITORY_URL:コードリポジトリのURLに置き換えます

別のパイプラインを追加する

上記にリストされているパイプラインに加えて、クラウド サイバーエクスポージャー は汎用ワークフローを介した他の CI/CD パイプラインの接続をサポートしています。以下の手順は、docker ベースのパイプラインを接続するための一般的な手順を示していますが、環境変数を追加して Docker スキャンを実行するときに使用される実際の構文は特定のパイプラインによるため、それに応じて調整する必要があります。

汎用パイプラインを追加する方法

1. クラウド サイバーエクスポージャー コンソールで、**[設定]** > **[統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**[汎用 (Docker)]** をクリックします。[Add Generic (Docker)] (汎用の追加 (Docker)) ウィザードが開きます。
3. **API トークンを作成します** (ウィザードのステップ 1)。トークンの名前を入力し、「**次へ**」をクリックしてトークンを作成します。

4. **APIトークンを保存します** (ウィザードのステップ2)。生成されたトークンをコピーして安全な場所に保存します。この情報は、ウィザードの次のステップで必要になります。完了したら、**[次へ]** をクリックします。

5. **環境変数を追加します** (ウィザードのステップ3)。関連するパイプラインステップに以下の環境変数を追加し、結果をTenableに報告します。

   > **注意:**
   > - クラウドサイバーエクスポージャーコンソールでスキャン結果を表示する際に、Tenableが関連データをカタログ化して表示するためにこれらの変数を使用するため、すべての変数は必須です。
   > - ここに挙げる変数に加え、グローバルフラグなどTenable Dockerイメージに含まれる任意のフラグを環境変数として設定し、スキャン設定をさらに微調整することができます。変数として使用するためにフラグを変換する方法など、詳しくは「フラグを環境変数として使用する」を参照してください。

   ```
   TENABLE_API_TOKEN=<api-token here>
   TENABLE_API_URL=https://app.tenable.com/
   TENABLE_PIPELINE_RUN_ID=134235
   TENABLE_PIPELINE_RUN_TRIGGER=pull_request
   TENABLE_PIPELINE_RUN_URL=https://github.com/acme/repo1/actions/runs/134235
   ```

   > **注意:** 上記のサンプル値を以下のように置き換えます。`TENABLE_API_TOKEN`: add-pipelineウィザードに表示される値に置き換えます `TENABLE_PIPELINE_RUN_ID`: パイプラインの実行IDに置き換えます `TENABLE_PIPELINE_RUN_TRIGGER`: ワークフローの実行をトリガーしたイベントの名前に置き換えます `TENABLE_PIPELINE_RUN_URL`: この実行の結果があるURLに置き換えます

   完了したら、**[次へ]** をクリックします。

6. **Dockerコマンドを実行します** (ウィザードのステップ4)。コンテナイメージをスキャンするには、次のステップをパイプラインに追加し、環境に応じて調整します。スキャン結果をTenableに報告するには、このウィザードで前述のように環境変数が追加されていることを確認してください。[TENABLE_API_TOKEN] フィールドは機密であるため、シークレットとして扱う必要があります。

   > **注意:** Gitリポジトリ内でスキャンを実行することをお勧めします。何らかの理由でこれが不可能な場合は、「非Gitリポジトリの追加変数を参照してください。

Dockerfile

```
docker run --workdir /tmp/tenable --volume /home/user/code:/tmp/tenable --env-file
environment.variables --pull=always tenable/cloud-security-scanner:latest container-image scan --
name <your image name>
```

上記のステップ例は、以下を前提としています。

- docker run を使用して、コンテナで Tenable のスキャナーを実行しています。
- `environment.variables` という名前の Docker env ファイルを作成した
- デフォルトのフラグでスキャンを実行しています。
- `--env-file`: 前の手順で作成した environment.variables ファイルが存在するパス。
- `--name`: イメージ名。
- `--volume`:左側(「:」の前)をコードがあるパスに変更します。右側はそのままにします。

7. 完了したら、**[完了]** をクリックします。

非 Git リポジトリの追加変数

Git リポジトリ内でスキャンまたは同期を実行することをお勧めします。何らかの理由でこれが不可能な場合は、[汎用 (Docker) の追加] ウィザードで一覧表示される変数に加えて、次の変数を追加する必要があります (別のパイプラインを追加するを参照)。

```
TENABLE_CODE_BRANCH=main
TENABLE_CODE_COMMIT_HASH=fa4e0ef3e25b89e1f6c348afd51b073f2bbcf1bb
TENABLE_CODE_COMMIT_USER=john-doe
TENABLE_CODE_REPOSITORY_URL=https://github.com/acme/repo1
```

上記のサンプル値を以下のように置き換えます。

- TENABLE_CODE_BRANCH:ブランチ名に置き換える
- TENABLE_CODE_COMMIT_HASH:コードのコミットハッシュに置き換えます
- TENABLE_CODE_COMMIT_USER: 最初のワークフローの実行をトリガーしたユーザーのユーザー名に置き換える
- TENABLE_CODE_REPOSITORY_URL: コードリポジトリの URL に置き換える

スキャンの設定

入力パラメーターを設定して、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整します。お使いのパイプラインに該当する方法を使用します。

- Azure Pipelines パラメーター
- GitHub アクションパラメーター
- GitLab CI/CD パラメーター
- 汎用 Docker

Azure Pipelines パラメーター

Azure Pipelines の関連するパイプラインの YAML スキーマで次の `task` 入力パラメーターを構成して、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整します。YAML スキーマの設定について詳しくは、関連する Microsoft ドキュメントを参照してください。

パラメーター	説明	デフォルト	例
apiToken (必須)	クラウドサイバーエクスポージャーとの通信に使用される API トークン。GitHub Actions の初期セットアップ中に、クラウドサイバーエクスポージャーコンソールで生成されます。		
apiUrl (必須)	クラウドサイバーエクスポージャー API の URL。		`https://app.tenable.com/`
excludeVulnerabilities	スキャンから除外する脆弱性 ID。コンマ区切りリストとして入力されます。		`CVE-2021-44228`
failOnMinSeverity	0 以外の終了コードを返し、ビルドワークフローを失敗とする、最小 CVE 深刻度。値が定義さ		`critical`

パラメーター	説明	デフォルト	例
	れていない場合、ワークフローは失敗しない。可能な値は次のとおりです。 • information • low medium • high • critical		
failOnMinCvssScore	検出された脆弱性の最小 CVSS スコア。0 以外の終了コードを返し、ビルドワークフローを失敗とする。値が定義されていない場合、ワークフローは失敗しない。可能な値: 0.0 から 10.0 までの任意の数字 (小数点を含む)		
failOnMinVprスコア	検出された脆弱性の最小 VPR スコア。0 以外の終了コードを返し、ビルドワークフローを失敗とする。値が定義されていない場合、ワークフローは失敗しない。可能な値: 0.0 から 10.0 までの任意の数字 (小数点を含む)		7.8
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ログメッセージには、スキャナーの実行プロセスに関する情報とデバッグ情報が含まれる。可能な値は次のとおりです。 • true • false		true
分深刻度	スキャンに含める最小の CVE 深刻度。可能な値は次のとおりです。	information	medium

パラメーター	説明	デフォルト	例
	• information • low • medium • high • critical		
minCvssスコア	スキャンに含める検出された脆弱性の最小CVSSスコア。可能な値: 0.0 から 10.0 までの任意の数字 (小数点を含む)		7.8
minVprスコア	スキャンに含める検出された脆弱性の最小VPRスコア。可能な値: 0.0 から 10.0 までの任意の数字 (小数点を含む)		7.8
name	コンテナ名 (alpine:latest / alpine / alpine@sha256:51b67269f354137895d43f3b3d810bfacd3945438e94dc5ac55fdac340352f48 / f8c20f8bbcb6)	alpine:latest	alpine:latest
outputFileFormats (出力ファイル・フォーマット)	エクスポートされるレポート出力ファイルの形式。可能な値は次のとおりです。 • cyclonedx • json • junit • md	json	json,csv
outputFileName (出力ファイル名)	エクスポートされるレポート出力ファイルの名前。複数の形式を選択すると、すべてのファイ	results	results

パラメーター	説明	デフォルト	例
	ルに同じ名前が付くようになります。		
outputIncludeIgnored脆弱性	無視した脆弱性をスキャン結果に含めるかどうかを決定するブーリアン値 (cyclonedx の出力には影響なし)。	`false`	
outputJunitTestNamePrefix	JUnit テスト出力名のプレフィックス。テスト結果に第 1 レベルの階層を作成するために使用される。`junit`が出力ファイル形式として定義されている場合に使用できます。		`Scan1`
出力パス	レポート出力ファイルのエクスポートパス。		`results/`
registryPassword	プライベートコンテナレジストリのパスワード。Tenable にプライベートレジストリの認証を許可するために使用される。		
registryUsername	プライベートコンテナレジストリのユーザー名。Tenable にプライベートレジストリの認証を許可するために使用される。		
serverCertificateValidationEnabled	リモート サーバーに接続するときに、Azure Pipeline エージェントまたはタスクが完全な SSL/TLS 証明書検証を実行する必要があるかどうかを指定します。 可能な値は次のとおりです。 • `true` • `false`	`true`	
サイレント	スキャン結果の内容を標準ワークフロー出力に	`false`	`false`

パラメーター	説明	デフォルト	例
	出力するかどうか。スキャン結果の出力には、スキャン中に見つかった問題に関する詳細情報が含まれる。ログから独立している。可能な値は次のとおりです。 • `true` • `false`		

従来のリリースパイプラインを使用している場合に必要な追加のパラメーター

パラメーター	説明	デフォルト	例
codeCommitUser	コミットを実行した作成者のユーザー名。		
codeRepositoryUrl	リポジトリURL。		`https://github.com/orgName/repoName`
pipelineRunTrigger	パイプライン実行をトリガーしたアクティビティ。		`Manual, PullRequest, BuildCompletion`

例: プロキシサーバー経由でスキャン結果を送信する

プロキシサーバー経由でスキャン結果をクラウドサイバーエクスポージャーに送信するには、HTTP_PROXY環境変数とHTTPS_PROXY環境変数を使用します。以下は、これらの変数を含むAzure Pipelinesタスクの例です。

YAML

```
trigger:
- main
pool:
  vmImage: ubuntu-latest
  steps:
  - task: ErmeticContainerImageScan@1
    env:
      HTTP_PROXY: http://localhost:80
      HTTPS_PROXY: https://localhost:443
    inputs:
      apiToken: '$(TENABLE_API_TOKEN)'
      apiUrl: 'https://app.tenable.com/'
      name: 'mongo:7.0.4'
      excludePaths: '/Dev'
      excludeVulnerabilities: 'CVE-2023-22946'
      failOnMinCvssScore: '9.0'
      failOnMinSeverity: 'high'
      logs: true
      minCvssScore: '7.0'
      minSeverity: 'medium'
      outputFileFormats: 'json'
      outputFileName: 'output'
      outputJunitTestNamePrefix: 'jprefix'
      outputPath: '/Dev'
      registryPassword: 'Password1234'
      registryUsername: 'Username1234'
```

GitHub アクションパラメーター

GitHubアクションで以下の入力パラメーターを設定し、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整します。

パラメーター	説明	デフォルト	例
api-token (必須)	クラウド サイバーエクスポージャーとの通信に使用される API トークン。GitHub アクションの初期セットアップ中に、クラウド サイバーエクスポージャー コンソールで生成されます。		
api-url (必須)	クラウド サイバーエクスポージャー API の URL。		`https://app.tenable.com/`
exclude-paths	特定のファイルまたはディレクトリをスキャンから除外する機能		

パラメーター	説明	デフォルト	例
exclude-unresolvable	ベンダー提供の修正プログラムまたはパッチのない、スキャンから除外する脆弱性 ID のコンマ区切りリスト。	`false`	
exclude-vulnerabilities	スキャンから除外する脆弱性 ID のコンマ区切りリスト		`CVE-2021-44228`
fail-on-min-severity	0 以外の終了コードを返し、ビルドワークフローを失敗とする、最小 CVE 深刻度。値が定義されていない場合、ワークフロー		`critical`

パラメーター	説明	デフォルト	例
	は失敗しない。可能な値は次のとおりです。 • `information` • `low` • `medium` • `high` • `critical`		
fail-on-min-cvss-score	検出された脆弱性の最小 CVSS スコア。0 以外の終了コードを返し、ビルドワークフローを失敗とする。値が定義されていない場合、ワークフ		`7.8`

パラメーター	説明	デフォルト	例
	ローは失敗しない。可能な値: `0.0` から `10.0` までの任意の数字 (小数点を含む)		
fail-on-min-vpr-score	検出された脆弱性の最小 VPR スコア。0 以外の終了コードを返し、ビルドワークフローを失敗とする。値が定義されていない場合、ワークフローは失敗しない。可能な値: `0.0` から `10.0` までの任意の数字 (小数		`7.8`

パラメーター	説明	デフォルト	例
	点を含む)		
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ログメッセージには、スキャナーの実行プロセスに関する情報や、スキャンされたファイル数や行数などのデバッグ情報が含まれる。可能な値は次のとおりです。 • `true` • `false`		`true`
min-severity	スキャンに含める最小	`information`	`medium`

パラメーター	説明	デフォルト	例
	のCVE 深刻度。可能な値は次のとおりです。 • `information` • `low` • `medium` • `high` • `critical`		
min-cvss-score	スキャンに含める検出された脆弱性の最小CVSS スコア。可能な値: `0.0` から `10.0` までの任意の数字 (小数点を含む)		`7.8`

パラメーター	説明	デフォルト	例
min-vpr-score	スキャンに含める検出された脆弱性の最小 VPR スコア。可能な値: `0.0` から `10.0` までの任意の数字 (小数点を含む)		`7.8`
name	コンテナ名		`alpine:latest / alpine / alpine@sha256:51b67269f354137895d43f3b3d810bfacd3945438e94dc5ac55fdac340352f48 / f8c20f8bbcb6`
output-file-formats	エクスポートされるレポート出力ファイルの形式。可能な値は次のとおりです。 • `cyclonedx` • `json`	`json`	`json,csv`

パラメーター	説明	デフォルト	例
	• `md`		
出力ファイル名	エクスポートされるレポート出力ファイルの名前。複数の形式を選択すると、すべてのファイルに同じ名前が付くようになります。	`results`	`results`
output-include-ignored-vulnerabilities	無視した脆弱性をスキャン結果に含めるかどうかを決定するブーリアン値 (cyclonedxの出力には影響なし)。	`false`	
出力パス	レポート出力ファイルのエクスポート		`results/`

パラメーター	説明	デフォルト	例
	パス。		
registry-password	プライベートコンテナレジストリのパスワード。Tenable にプライベートレジストリの認証を許可するために使用される。		
registry-username	プライベートコンテナレジストリのユーザー名。Tenable にプライベートレジストリの認証を許可するために使用される。		
サイレント	スキャン結果の内容を	`false`	`false`

パラメーター	説明	デフォルト	例
	標準ワークフロー出力に出力するかどうか。スキャン結果の出力には、スキャン中に見つかった問題に関する詳細情報が含まれる。ログから独立している。可能な値は次のとおりです。 • `true` • `false`		
summary	このパラメーターを使用すると、パイプラインステップ実行の最後にサ	`true`	`false`

パラメーター	説明	デフォルト	例
	マリー出力を印刷できます。可能な値は次のとおりです。 • true • false		

例: プロキシサーバー経由でスキャン結果を送信する

プロキシサーバー経由でスキャン結果をクラウドサイバーエクスポージャーに送信するには、HTTP_PROXY環境変数とHTTPS_PROXY環境変数を使用します。以下は、これらの変数を含むGitHubアクションの例です。

YAML

```
steps:
  - uses: actions/checkout@v3
  - name: Set PROXY environment variables
    run: echo "HTTP_PROXY=http://localhost:80" >> $GITHUB_ENV && echo "HTTPS_PROXY=https://localhost:443"
>> $GITHUB_ENV
  - name: Scan IaC with Tenable One Cloud Exposure
    uses: ermetic/actions/iac/scan@v1
    with:
      api-token: ${{ secrets.TENABLE_API_TOKEN }}
      api-url: https://app.tenable.com/
```

GitLab CI/CD パラメーター

GitLab CI/CDで以下の入力パラメーターを設定し、クラウドサイバーエクスポージャーが環境をスキャンする方法を微調整します。

パラメーター	説明	デフォルト	例
api-token (必須)	クラウドサイバーエクスポージャーとの通信に使用される API トークン。GitLab CI/CD の初期セットアップ中に、クラウドサイバーエクスポージャーコンソールで生成されます。		
api-url (必須)	クラウドサイバーエクスポージャー API の URL。		`https://app.tenable.com/`
name (必須)	コンテナ名 (alpine:latest / alpine / alpine@sha256:51b67269f354137895d43f3b3d810bfacd3945438e94dc5ac55fdac340352f48 / f8c20f8bbcb6)		`alpine:latest`
ステージ (必須)	ジョブを実行するための GitLab CI/CD パイプラインステージ。		`tenable-cloud-security`
exclude-paths	特定のファイルまたはディレクトリをスキャンから除外する機能		
exclude-unresolvable	ベンダー提供の修正プログラムまたはパッチのない、スキャンから除外する脆弱性 ID のコンマ区切りリスト。	`false`	
exclude-vulnerabilities	スキャンから除外する脆弱性 ID のコンマ区切りリスト		`CVE-2021-44228`
fail-on-	検出された脆弱性の最小 CVSS スコア。0 以外の終		`7.8`

パラメーター	説明	デフォルト	例
min-cvss-score	了コードを返し、ビルドワークフローを失敗とする。値が定義されていない場合、ワークフローは失敗しない。可能な値: `0.0` から `10.0` までの任意の数字 (小数点を含む)		
fail-on-min-vpr-score	検出された脆弱性の最小 VPR スコア。0 以外の終了コードを返し、ビルドワークフローを失敗とする。値が定義されていない場合、ワークフローは失敗しない。可能な値: `0.0` から `10.0` までの任意の数字 (小数点を含む)		`7.8`
fail-on-min-severity	0 以外の終了コードを返し、ビルドワークフローを失敗とする、最小 CVE 深刻度。値が定義されていない場合、ワークフローは失敗しない。可能な値: • `information` • `low` • `medium` • `high` • `critical`		`critical`
ログ	ログメッセージを標準ワークフロー出力に出力するかどうか。ログメッセージには、スキャナーの実行プロセスに関する情報や、スキャンされたファイル数や行数などのデバッグ情報が含まれる。可能な値は次のとおりです。`true` `false`	`false`	`true`
min-cvss-	スキャンに含める検出された脆弱性の最小 CVSS スコア。可能な値: `0.0` から `10.0` までの任意の数字 (小		`7.8`

パラメーター	説明	デフォルト	例
score	数点を含む)		
min-vpr-score	スキャンに含める検出された脆弱性の最小 VPR スコア。可能な値: `0.0` から `10.0` までの任意の数字 (小数点を含む)		`7.8`
min-severity	スキャンに含める最小の CVE 深刻度。可能な値: • `information` • `low` • `medium` • `high` • `critical`	`information`	`medium`
output-file-formats	エクスポートされるレポート出力ファイルの形式。可能な値は次のとおりです。 • `cyclonedx` • `json` • `junit` • `md`	`json`	`json,csv`
出力ファイル名	エクスポートされるレポート出力ファイルの名前。複数の形式を選択すると、すべてのファイルに同じ名前が付くようになります。	`results`	`results`
output-include-ignore	無視した脆弱性をスキャン結果に含めるかどうかを決定するブーリアン値 (cyclonedx の出力には影響なし)。	`false`	

パラメーター	説明	デフォルト	例
d-vulnerabilities			
output-junit-test-name-prefix	JUnit テスト出力名のプレフィックス。テスト結果に第 1 レベルの階層を作成するために使用される。`junit`が出力ファイル形式として定義されている場合に使用できます。		`Scan1`
出力パス	レポート出力ファイルのエクスポートパス。		`results/`
registry-password	プライベートコンテナレジストリのパスワード。Tenableにプライベートレジストリの認証を許可するために使用される。		
registry-username	プライベートコンテナレジストリのユーザー名。Tenableにプライベートレジストリの認証を許可するために使用される。		
サイレント	スキャン結果の内容を標準ワークフロー出力に出力するかどうか。スキャン結果の出力には、スキャン中に見つかった問題に関する詳細情報が含まれる。ログから独立している。可能な値は次のとおりです。 • `true` • `false`	`false`	`true`

Tenable Docker イメージの CLI

Tenable Docker イメージ CLI を使用して以下のコマンドを設定し、Tenable が環境をスキャンする方法を微調整します。

> **注意:** CI/CD パイプラインを Tenable に接続する際にイメージが抽出されます。

使用

```
tenable container-image scan [flags]
```

フラグ

```
--api-token string                        It is required to provide these parameters in order to send the
scan results to Tenable for CVE detection
--api-url string                          It is required to provide these parameters in order to send the
scan results to Tenable for CVE detection
--archive-path string                     path to image tar archive
--code-branch string                      (auto detected)
--code-commit-hash string                 (auto detected)
--code-commit-user string                 (auto detected)
--code-repository-url string              (auto detected)
--exclude-unresolvable strings            exclude vulnerability IDs that do not have a fix or patch
(default "false")
--exclude-vulnerabilities strings         exclude vulnerability IDs
--fail-on-min-cvss-score float            minimum cvss score that should return an exit code different
from 0
--fail-on-min-vpr-score float             minimum vpr score that should return an exit code different from
0
--fail-on-min-severity string             minimum severity that should return an exit code different from
0
--help, -h                                help for scan
--json-version-legacy
--min-cvss-score float                    The minimum CVSS score of detected vulnerabilities that you want
included in the scan
--min-vpr-score float                     The minimum VPR score of detected vulnerabilities that you want
included in the scan
--min-severity string                     information ,low, medium, high, critical (default "information")
--name string                             image name alpine:latest / alpine /
alpine@sha256:51b67269f354137895d43f3b3d810bfacd3945438e94dc5ac55fdac340352f48 / f8c20f8bbcb6
--output-file-formats strings             cyclone-dx,json,j-unit,md (default [json])
```

```
--output-file-name string                (default "results")
--output-include-ignored-vulnerabilities  A boolean value determining whether to include ignored
vulnerabilities in the scan results
--output-junit-test-name-prefix string
--output-path string
--pipeline-run-id string
--pipeline-run-trigger string
--pipeline-run-url string
--registry-password string
--registry-username string
--server-certificate-validation-enabled    (default "true")
```

重要: docker コマンドをローカルで実行しているときに `--output-path` フラグを使用して出力ファイルにアクセスする場合は、コマンドで `-v` 引数を使用して、docker フォルダーとローカルフォルダー間のマッピングを作成します。以下の例では、`local-output` はローカルでファイルを保存する場所を表し、`docker-output` は対応する docker ディレクトリを表します。

```
docker run -v ./local-output:/docker-output--env-file environment.variables --pull=always tenable/cloud-
security-scanner:latest container-image scan --name storm:latest --output-file-formats json --output-path
/docker-output
```

グローバルフラグ

```
--logs       print log messages to standard output
--no-color   print output without color
--silent     do not print output to standard output
```

フラグを環境変数として使用する

汎用 Docker パイプラインを クラウド サイバーエクスポージャー に追加する場合は、一連の環境変数を設定します。Tenable は、これらの変数を使用して、Tenable コンソールでスキャン結果を表示するときに関連データをカタログ化し表示します。より高度な構成要件に準拠したり、スキャン設定をさらに微調整したりするために、グローバルフラグなど、Tenable Docker イメージに含まれるすべてのフラグを環境変数として構成することもできます。

フラグと環境変数の構文

CLI フラグと環境変数は異なる構文を使用します。次の手順を使用して、特定のフラグを環境変数に変換します。

フラグ構文を環境変数として使用するための変換方法

1. フラグ名の前のダッシュを削除します。
2. ダッシュをアンダースコアに置き換えます。
3. プレフィックスとして「TENABLE_」(アンダースコア付き) を入力します。
4. すべて大文字を使用します。
5. ブーリアンフラグ (フラグを環境変数として使用するを参照) をアクティブ化するには、TRUE に設定する必要があります。

したがって、たとえば `--code-repository-url` フラグを環境変数として使用する場合、`TENABLE_CODE_REPOSITORY_URL` になります。

Container Image Registries の接続

これは、コンテナイメージレジストリを Tenableに接続するための統合ガイドです。

- コンテナイメージの表示と管理に関するガイドについては、コンテナイメージを参照してください。
- Tenable によるレジストリのスキャン方法の概念概要については、Container Image Registry Scanning を参照してください。

コンテナレジストリのスキャンを有効または無効にするには、次の手順を実行します。

1. (AWS のみ) Tenable One Cloud ExposureにECR スキャンのアクセス許可を付与します 。

   > **注意:** Azure (ACR) とGCP (Artifact Registry) の場合、追加のアクセス許可を付与する必要はありません。基本的な VM スキャンのアクセス許可で十分です。VM スキャンのアクセス許可の付与に関する詳細については、ワークロードの接続 を参照してください。

2. クラウドサイバーエクスポージャーにレジストリを追加
   - JFrog 組織をに追加しますクラウドサイバーエクスポージャー。
   - Cloudsmith 組織をクラウドサイバーエクスポージャーに追加します。

> **注意:** Cloudsmith は、組織統合フローを介してのみ追加できます。

- サードパーティレジストリの追加 を クラウド サイバーエクスポージャーに追加。

3. (すべてのレジストリ) Tenable でコンテナレジストリスキャンを有効または無効にする。

AWS: ECR スキャンのアクセス許可を付与する

クラウド サイバーエクスポージャー IAM ロールに追加されたカスタムインラインポリシーを介して、AWS コンテナレジストリをスキャンする Tenable アクセス許可を付与します。これらのアクセス許可は、Tenable ウィザードの AWS 統合プロセスの一部として (ECR スキャンアクセス許可を介して) 付与されますが、アカウントを接続した日時によっては、まだ付与されていない可能性があります。

- コンテナレジストリをスキャンする AWS アカウントを既に接続しているが、コンテナレジストリのスキャンのアクセス許可をまだ追加していない場合は、次の手順を実行します。
- コンテナレジストリをスキャンする AWS アカウントをまだ接続していない場合は、AWS アカウントの接続に記載されている手順を実行します。

コンテナレジストリのスキャンのアクセス許可を既に追加しているかどうかを確認するには、クラウド サイバーエクスポージャー コンソールで **[設定]** > **[アカウント]** > **[AWS]** に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [問題あり] で、コンテナレジストリのスキャンのアクセス許可が付与されていないとツールチップに表示される場合は、次の手順を実行します。

アクセス許可を付与するには:

1. 関連するアカウントの AWS 管理コンソールで、**[IAM]** > **[ロール]** に移動し、アカウント統合の間に Tenable に対して作成したロールを開きます。
2. [アクセス許可] タブで、**[アクセス許可の追加]** > **[インラインポリシーの作成]** をクリックします。
3. 次のポリシーをコピーして、[JSON] タブに貼り付け、既存のテキストを置き換えます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource": "*"
    }
  ]
}
```

4. **[ポリシーのレビュー]** をクリックします。
5. ポリシーの名前 (TenableWorkloadProtection など) を入力し、**[ポリシーの作成] を**クリックします。
6. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[アカウント]** > **[AWS]** に移動し、アカウントの [ステータス] が [接続済み] であることを確認します。

注意: ステータスが [接続済み] に変わるまでに最大で数分かかる場合があり、ブラウザでハードリフレッシュを実行する必要がある場合があります。

AWS: ECR スキャンポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource": "*"
    }
  ]
}
```

JFrog Organization を追加する

JFrog 組織を追加して、組織内のすべてのコンテナレジストリをスキャンします。

クラウドサイバーエクスポージャー は、インターネットに接続するサーバーとネットワークで隔離されたサーバーの両方を持つ企業をサポートします。ネットワーク分離されたサーバーの接続 参照してください。

組織を追加した後、Tenable

1. 企業内のレジストリに接続します。
2. 各レジストリ内のリポジトリのリストをプルします。
3. リポジトリのインベントリ項目をスキャンします。
4. イメージの脆弱性をスキャンします。
5. イメージとリポジトリをインベントリの対応リソース として表示します。
6. クラウドサイバーエクスポージャー コンソール内のアカウント階層の一部としてレジストリを表示することで、特定のレジストリまたはレジストリグループの アカウント階層とフォルダー できます。

JFrog 組織を追加するには:

1. クラウドサイバーエクスポージャー コンソールで、**[設定] > [統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**JFrog Organization**をクリックします。[JFrog Organization の追加] ウィザードが開きます。
3. [アカウント] および [設定] ページに表示されるレジストリの表示 **名** を入力します。
4. Tenable のサーバーへの接続方法を選択します。サーバーがネットワークで区切られている場合は、Tenable Endpoint Connector を使用して接続を確立します。
   - **エンドポイントインターネットに接続するレジストリ**。レジストリのホスト名/IP を入力します。
   - **エンドポイントコネクタネットワーク分離レジストリ経由** 。ドロップダウンから関連するコネクタを選択します。何も使用できない場合は、1 つ追加します。

   SSL がサーバーで有効になっている場合、**[サーバーの SSL 証明書を受け入れる]** にチェックを入れます。

5. 組織の以下の情報を入力します。
    - **ユーザー名**。レジストリのユーザー名です。
    - **Password**. これはレジストリにログインするためのパスワードとして使用できます。もしくは、ベンダーのプラットフォーム内で特定のトークンを設定することもできます。
6. **フォルダー構造 を自動更新します**。レジストリの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます (デフォルトで有効)。詳細は、アカウント階層とフォルダーを参照してください。
7. **[終了]** をクリックします。

Cloudsmith Organization を追加する

Cloudsmith コンテナレジストリ組織を追加して、組織内のすべてのコンテナレジストリをスキャンします。

クラウドサイバーエクスポージャー は、インターネットに接続するサーバーとネットワークで隔離されたサーバーの両方を持つ企業をサポートします。ネットワーク分離されたサーバーの接続 参照してください。

組織を追加した後、Tenable

1. 企業内のレジストリに接続します。
2. 各レジストリ内のリポジトリのリストをプルします。
3. リポジトリのインベントリ項目をスキャンします。
4. イメージの脆弱性をスキャンします。
5. イメージとリポジトリをインベントリの対応リソース として表示します。
6. クラウドサイバーエクスポージャー コンソール内のアカウント階層の一部としてレジストリを表示することで、特定のレジストリまたはレジストリグループの アカウント階層とフォルダー できます。

Cloudsmith の組織を追加するには

1. クラウドサイバーエクスポージャー コンソールで、**[設定]** > **[統合]** に移動し、**[統合の追加]** をクリックします。
2. 統合ライブラリで、**Cloudsmith Organization を**クリックします。[Cloudsmith Organization] ウィザードが開きます。

3. [アカウント] および [設定] ページに表示されるレジストリの表示名を入力します。
4. Tenable のサーバーへの接続方法を選択します。サーバーがネットワークで区切られている場合は、Tenable Endpoint Connector を使用して接続を確立します。
    - **Cloudsmith のデフォルトエンドポイント** docker.cloudsmith.io:443。Cloudsmith のデフォルトエンドポイントを入力します。
    - **エンドポイントインターネットに接続します**。レジストリのホスト名/IP を入力します。
    - **エンドポイントコネクタネットワーク分離レジストリ経由**。ドロップダウンから関連するコネクタを選択します。何も使用できない場合は、1 つ追加します。
    - SSL がサーバーで有効になっている場合は、**[サーバーの SSL 証明書を受け入れる] にチェックを入れます**。
5. Cloudsmith サービスアカウントの **API キー**を入力します。
6. **フォルダー構造を自動更新します**。レジストリの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます (デフォルトで有効)。詳細は、アカウント階層とフォルダーを参照してください。
7. **[終了]** をクリックします。

サードパーティレジストリの追加

クラウドプロバイダー環境内でネイティブにホストされていないサードパーティレジストリを操作するには、レジストリを クラウドサイバーエクスポージャーに追加する必要があります。Tenable は Docker Registry HTTP API V2 仕様を利用しています。その結果、通常、このプロトコルをサポートする任意のコンテナレジストリを統合できます。

次のベンダーがテストされ、承認されました

- JFrog

    > **注意:** 個々のレジストリを追加するだけでなく、JFrog 組織全体を追加して、組織内のすべてのレジストリを接続することもできます。

- Red Hat Quay

- Sonatype Nexus リポジトリ
- Harbor

クラウドサイバーエクスポージャー は、インターネットに接続されたサーバーとネットワークで分離されたサーバーの両方でレジストリをサポートします。ネットワーク分離されたサーバーの接続 参照してください。

レジストリを追加すると、Tenable

1. レジストリに接続します。
2. レジストリ内のリポジトリのリストをプルします。
3. リポジトリのインベントリ項目をスキャンします。
4. イメージの脆弱性をスキャンします。
5. イメージとリポジトリをインベントリの対応リソースとして表示します。
6. クラウドサイバーエクスポージャー コンソール内のアカウント階層の一部としてレジストリを表示することで、特定のレジストリまたはレジストリグループの アカウント階層とフォルダー できます。

独立したレジストリを追加するには

1. クラウドサイバーエクスポージャー コンソールで、**[設定] > [統合]** の順に移動し、**[統合を追加]** をクリックします。
2. 統合ライブラリで、**Cloudsmith Organization** をクリックします。[Cloudsmith Organization の追加] ウィザードが開きます。
3. [アカウント] および [設定] ページに表示されるレジストリの表示 **名** を入力します。
4. Tenable のサーバーへの接続方法を選択します。サーバーがネットワークで区切られている場合は、Tenable Endpoint Connector を使用して接続を確立します。
    - **Direct (インターネットに接続するレジストリ) をダイレクトします**。レジストリのエンドポイントを入力します。Quay レジストリの場合は、次を入力します `quay.io`。
    - **エンドポイントコネクタネットワーク分離レジストリ経由** 。ドロップダウンから関連するコネクタを選択します。何も使用できない場合は、1 つ追加します。
      SSL がサーバーで有効になっている場合は、**[サーバーの SSL 証明書を受け入れる] にチェックを入れます** 。

5. レジストリに関する以下の情報を入力します。
    - **ユーザー名**。レジストリのユーザー名です。
    - **Password**. これはレジストリにログインするためのパスワードとして使用できます。もしくは、ベンダーのプラットフォーム内で特定のトークンを設定することもできます。
6. **フォルダー構造を自動更新します**。レジストリの構造を Tenable 内のフォルダーとしてミラーリングし、その階層を維持して、ビューを同期させます (デフォルトで有効)。詳細は、アカウント階層とフォルダーを参照してください。
7. **[終了]** をクリックします。

Tenable でコンテナレジストリスキャンを有効または無効にする

デフォルトでは、組織全体のクラウドサイバーエクスポージャーでレジストリスキャンが無効になっています。コンソール設定からスキャンを有効にでき、特定のアカウントまたはアカウントスコープで機能を有効/無効にして微調整できます。この設定を行うには、クラウドサイバーエクスポージャーで管理者ロールを持つユーザーである必要があります。

コンテナレジストリのスキャンを有効にする方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[ワークロード]** > **[コンテナレジストリ]** をクリックします。
2. 左側の組織ツリーでアカウント階層とフォルダーを選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。
3. [Container Registry Scanning] セクションで、次のいずれかを選択します。
    - 親レベルのアカウント範囲の設定を**継承** (デフォルト)。

      > **注意:** 組織全体を範囲として選択した場合、[継承] オプションは使用できません。

    - このアカウントスコープ用の一意の設定 (**有効**/**無効**) で、親レベルスコープの設定をオーバーライドします。この固有の設定は、親レベルの範囲で行われた変更に関係なく、子レベルの範囲に残ります。

脅威検出

脅威検出の要件

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

Tenable 脅威検出は、セキュリティイベントのほぼリアルタイムの分析を提供し、クラウドログとKubernetesセンサーによって収集されたアクティビティを分析することでランタイムリスクを特定します。

設定および統合の要件は、ご使用の環境によって異なります。

- クラウドアカウント: アクティビティデータを収集するために、Tenable にネイティブログサービスへのアクセス権を付与します。
- Kubernetes クラスタHelm チャートを介してクラスタを接続する を使用してランタイム検出センサーをインストールします。

要件

脅威の検出を有効にするには、クラスタタイプに応じて、関連するアクティビティログをエクスポートするか、Kubernetes センサーをインストールするように環境を設定する必要があります。

クラウドアカウント

クラウドインフラ内の疑わしいアクティビティを監視するには、クラウドプロバイダーアカウントのアクティビティログを有効にする必要があります。これにより、Tenable がクラウド環境全体のイベントを収集して分析できるようになります。次の表は、各クラウドプロバイダーに必要なログの内訳を示しています。

プラットフォーム	要件
AWS	AWS CloudTrail を設定する
Microsoft Azure	Azure の必要なアクセス許可にアクセスするためのアクセス許可を付与する
GCP	Google の必要なアクセス許可にアクセスするためのアクセス許可を付与する

Kubernetes クラスタ

コンテナ化されたワークロード内の不審なアクティビティを監視し、特定するには、Kubernetes センサーをインストールする必要があります。センサーは、クラウドベースの環境とオンプレミス環境の両方で、Kubernetes クラスタの不審なアクティビティイベントを可視化します。このセンサーをインストールするには、Helm Chart を介してクラスタを接続するを参照してください。

センサーリソース

ランタイム検出センサーには、次のポッドレベルのリソースが必要です。

カテゴリー	要件/利用状況
CPU (Pod 制限)	1コア(1000m)
メモリ (RAM)	1GiB
API アクセス許可	Kubernetes クラスタをクエリするための読み取り専用アクセス。全リストは こちらを参照してください。

アクセス許可と接続性

ランタイム検出センサーには、次のクラスタアクセス許可とネットワークアクセス権が必要です。

- **API アクセス**: センサーには、ポッド、ノード、名前空間などのリソースを `get`、`list`、`watch` するアクセス許可を持つ ClusterRole が必要です。全リストは こちらを参照してください。
- **ネットワーク**: センサーは送信 HTTPS 経由で Tenable One Cloud Exposure プラットフォーム に到達できる必要があります。詳細は、Helm の要件を参照してください。

脅威検出の設定

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

特定のアカウントで脅威対策を有効にするには、アカウントを Tenable One Cloud Exposure に接続し、検出に必要な特定のログまたはイベントを Tenable 付与する必要があります。この機能は、次のプラットフォームで有効にできます。

- AWS
- Azure: アクティビティログのアクセス許可を付与する
- GCP: 監査ログのアクセス許可を付与する
- Kubernetes

AWS: CloudTrail アクセスの設定

Tenable は、AWS CloudTrail からアクティビティログを読み取り、接続済みアカウントのアクティビティをモニタリングします。アカウントの接続プロセス中に、証跡を選択し、Tenable にその証跡へのアクセス権を付与する必要があります。

- 脅威検出を有効にする AWS アカウントをすでに接続しているものの、必要なアクセス許可がまだ追加されていない場合は、以下の手順に従います。
- 脅威検出を有効にする AWS アカウントをまだ接続していない場合は、「AWS アカウントの接続」に記載されている手順に従います。

脅威検出のアクセス許可がすでに追加されているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **[Settings > Accounts > AWS]** に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [接続に問題あり] であり、ツールチップに **モニタリング (読み取り専用)** アクセス許可が付与されていないことが示されている場合は、以下の手順に従います。

脅威検出のアクセス許可を付与する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Accounts] > AWS**に移動します。
2. 関連するアカウントを見つけて、**[編集]** をクリックします。
3. ウィザードの手順 2 (アクセス許可) に移動し、**監視 (読み取り専用)** アクセス許可を有効にして、**[次へ]** をクリックします。

4. **[終了]** をクリックします。
5. アカウントのステータスが [接続済み] であることを確認します。

Azure: アクティビティログのアクセス許可を付与する

Tenable は Azure アクティビティログを読み取り、接続済みアカウントのアクティビティをモニタリングします。アカウント接続プロセス中に、**Tenable へのモニタリング (読み取り専用)** アクセス権を付与する必要があります。

- 脅威検出を有効にする Azure アカウントをすでに接続しているものの、必要なアクセス許可がまだ追加されていない場合は、以下の手順に従います。
- 脅威検出を有効にする Azure アカウントをまだ接続していない場合は、「Azure サブスクリプションの接続」に記載されている手順に従います。

脅威検出のアクセス許可がすでに追加されているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **[Settings > Accounts > Azure]** に移動し、**アカウントのステータスを確認します。**

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [接続に問題あり] であり、ツールチップに **モニタリング (読み取り専用)** アクセス許可が付与されていないことが示されている場合は、以下の手順に従います。

脅威検出のアクセス許可を付与する方法

1. クラウドサイバーエクスポージャーコンソールで、**Azure > Settings > アカウント** に移動します。
2. 関連するアカウントを見つけて、**[編集]** をクリックします。
3. ウィザードのステップ 3 (アクセス許可) に移動し、**モニタリング (読み取り専用)** アクセス許可を有効にして、**[次へ]** をクリックします。
4. **[終了]** をクリックします。
5. アカウントのステータスが [接続済み] であることを確認します。
6. Azure の必要なアクセス許可記事に従って、`AuditLog.Read.All`アクセス許可が付与されていることを確認します。

GCP: 監査ログのアクセス許可を付与する

Tenable は GCP 監査ログを読み取り、接続済みアカウントのアクティビティをモニタリングします。アカウント接続プロセス中に、**Tenable へのモニタリング (読み取り専用)** アクセス権を付与する必要があります。

- 脅威検出を有効にする GCP アカウントをすでに接続しているものの、必要なアクセス許可がまだ追加されていない場合は、以下の手順に従います。
- 脅威検出を有効にする GCP アカウントをまだ接続していない場合は、「GCP プロジェクトの接続」に記載されている手順に従います。

脅威検出のアクセス許可がすでに追加されているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **GCP > > アカウント Settings**に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [接続に問題あり] であり、ツールチップに **モニタリング (読み取り専用)** アクセス許可が付与されていないことが示されている場合は、以下の手順に従います。

脅威検出のアクセス許可を付与する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings** > **Accounts]** > **GCP** に移動します。
2. 関連するアカウントを見つけて、**[編集]** をクリックします。
3. ウィザードのステップ 3 (アクセス許可) に移動し、**モニタリング (読み取り専用)** アクセス許可を有効にして、**[次へ]** をクリックします。
4. **[終了]** をクリックします。
5. アカウントのステータスが [接続済み] であることを確認します。
6. Google の必要なアクセス許可記事に従い、監査ログのアクセス許可が付与されていることを確認します。

Kubernetes: Kubernetes センサーのインストール

Tenable は、Kubernetes センサーを介してイベントを収集することで、コンテナ化されたワークロード内の不審なアクティビティを特定します。クラスターの脅威検出を有効にするには、eBPF センサーベースのテクノロジーをインストールする必要があります。

- 脅威検出を有効にするクラスタをすでに接続しているものの、センサーがまだインストールされていない場合は、「Kubernetes ランタイム検出センサーのインストール」に記載されている手順に従います。
- クラスタをすでに接続してセンサーを有効にしている場合、ランタイム検出機能を持たせるために再インストールする必要があります。
- クラスタをまだ接続していない場合は、Helm チャートを介してクラスタを接続するに記載されている手順に従ってください。

センサーがすでにインストールされて脅威検出が有効になっているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **[Explore > Kubernetes Clusters]** (クラスタの調査) に移動し、クラスタのステータスを確認します。

- ステータスが [接続済み] の場合、センサーはアクティブであり、アクセス許可が付与されています。
- 異なるステータスが表示され、ツールチップにクラスタに問題があることを示している場合は、以下の手順に従います。

センサーをインストールまたは更新する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Explore > Kubernetes Clusters]** に移動します。
2. 関連するクラスタを見つけて、**[Edit > Install / Upgrade Helm]** をクリックします。
3. ウィザードの手順に従って、Helm チャートを介してクラスタを接続するします。
4. **[閉じる]** をクリックします。
5. クラスタのステータスが [接続済み] であることを確認します。

Kubernetes クラスタ

Kubernetesの概要

Tenable では、Kubernetes 環境 を接続するためのさまざまな方法 を提供しています。所属組織に最適な方法は、クラスターアーキテクチャ、セキュリティ要件、および有効にする Kubernetes Admission Controller やセンサーベースのスキャンなどの特定の機能によって異なります。

- **クラウドベース** (エージェントレス): この方法では、クラウドネイティブ API (Amazon EKS、Azure AKS、Google GKE、Oracle OKEなど) を使用して、クラウド IAM を通じて Kubernetes API にアクセスします。この方法を使用すると、環境にソフトウェアをインストールすることなくクラスターを検出してスキャンできます。
- **Helm チャートベース** (センサーベース): このメソッドは、プライベートまたはオンプレミスクラスターに必要です。また、アドミッションコントローラーの概要 や他の Kubernetesのセキュリティ機能を有効にする必要もあります。

詳細については、Kubernetesを参照してください。

クラスター検出

Tenable は、ホスティング環境に基づいて、3 つの異なる方法で、**インベントリ** ページにクラスターを検出して表示します。

- **クラウド管理クラスター** (AWS、Azure、GCP、OCI): Tenable が自動的にこれらのクラスターを検出し、関連するクラウドアカウントを接続するとすぐに、**[インベントリ]** ページにそれらを表示します。
- **サポートされていないクラウドプロバイダー**: プラットフォームが現在 API ベースの検出でサポートしていないクラウドプロバイダーを使用している場合、Helm チャートを介してクラスタを接続する チャートを使用してクラスターを接続できます。この方法で接続されたクラスターは、コンソール内でオンプレミスとして分類されるアカウントに関連付けられます。
- **管理 (プライベート) およびオンプレミス** クラスター: これらの環境は、Helm チャートを介してクラスタを接続する チャートを介してクラスターを Tenable に接続した後にのみ **[インベントリ]** ページに表示されます。

Kubernetesのセキュリティ機能

検出は高いレベルの可視性を提供しますが、追加のセキュリティ機能を有効にして環境をより強力に保護できます。

- Resource Sync: クラスターデータを と同期することで、Kubernetes リソースの可視性を提供します Tenable。これにより、リソースインベントリに環境の現在の状態が確実に反映されます。

- 脅威検出: eBPF センサーを介してシステムレベルのアクティビティを監視し、ほぼリアルタイムで悪意のあるまたは不審なアクティビティを検出します。
- アドミッションコントローラーの概要: API リクエストを傍受し、セキュリティポリシーに基づいて準拠するリソースのみがデプロイされるようにします。
- ワークロード保護: Kubernetes ノードと実行中のコンテナイメージをスキャンして、脆弱性とセキュリティ設定ミスを検出します。

> **注意:** Kubernetes 脅威検出、アドミッションコントローラーの概要 、センサーベースのワークロード保護を有効にするには、Helm チャートを介してクラスタを接続する チャートを使用してセンサーをインストールする必要があります。これは、すべてのクラウドプロバイダーとクラスタタイプに適用されます。

以下のセクションを使用して、リソース同期、ランタイム検出、ワークロード保護、および追加のセキュリティ機能を行うために、Helm チャート (センサーベース) とクラウドネイティブ (エージェントレス) のどちらの方法を使用するかを決定します。

Helm Chart の統合が必要な場合

Helm チャートの統合により、セキュリティポスチャーが基本的なメタデータ検出だけでなく、包括的なディープスキャン分析に拡張されます。次のシナリオでは、この統合方法を選択する必要があります。

- **接続の確立**: クラスタが以下の場合は、このメソッドを使用します。
  - **マネージド (プライベート):** API サーバーがインターネットからアクセスできないマネージド (プライベート) クラスタを使用します。
  - **オンプレミス:** プライベートデータセンターなど、カスタマーマネージドのリソースでインフラをホストします。
- **Kubernetes 固有の機能の有効化**: 脅威検出、アドミッションコントローラーの概要、脆弱性管理などの機能を有効化します。
- 以下に挙げるような**高度なセキュリティ要件またはコンプライアンス要件**に対応します。
  - **リアルタイムポリシーの実施:** Kubernetes アドミッションコントローラーの概要に必要です。
  - **詳細な設定の可視性:** ロールベースのアクセス制御 (RBAC) とクラスタ設定に関する詳細な文脈情報を提供します。

詳細については、Kubernetesクラスターを接続するを参照してください。

Kubernetesクラスターを接続する

クラスタを接続する前に、デプロイメントモデルにHelmチャートメソッドが必要かどうかを確認してください。プライベートクラスタ、オンプレミス環境、およびクラウドネイティブAPIメソッドがサポートされていない特定のセキュリティ機能には、Kubernetesクラスタ Helmチャートを使用します。

Kubernetesのリソース同期とワークロード保護

クラウドプロバイダー	マネージド (パブリック)	マネージド (プライベート)	アンマネージド
AWS [1]	適切なアクセス許可の付与 (エージェントレス)	Helmチャートからのインストール (センサー)	Helmチャートからのインストール (センサー)
Azure [2]	適切なアクセス許可の付与 (エージェントレス)	Helmチャートからのインストール (センサー)	Helmチャートからのインストール (センサー)
GCP [3]	適切なアクセス許可の付与 (エージェントレス)	Helmチャートからのインストール (センサー)	Helmチャートからのインストール (センサー)
OCI	クラスタのアクセス許可を付与する (エージェントレス)	Helmチャートからのインストール (センサー)	Helmチャートからのインストール (センサー)
オンプレミスと、サポートされていないクラウドプラットフォームすべて	該当なし	該当なし	Helmチャートからのインストール (センサー)

以下の機能は、**脆弱性管理**スキャンで現在**サポートされていません**。
AWS [1] - Fargateは脆弱性管理でサポートされていません。

Azure [2] - 仮想ノードは脆弱性管理でサポートされていません。

GCP [3] - Autopilot は脆弱性管理でサポートされていません。

> **注意:** エージェントレスの統合は、脆弱性管理スキャンをサポートするうえで最も一般的かつ推奨されるアプローチですが、特定のシナリオではセンサーベースの設定が必要です。詳細については、エージェントレススキャンとエージェントベーススキャンの比較を参照してください。

ランタイム検出

脅威検出を使用するには、Helm を使用してセンサーをインストールする必要があります。この要件は、パブリック、プライベート、アンマネージド Kubernetes と OpenShift クラスタにおける、サポート対象のすべてのクラウドプロバイダーに適用されます。

接続用に Helm ベースのセンサーを使用している場合、別途インストールを行う必要はありません。代わりに、既存のデプロイメントをランタイムフラグで更新してください。インストールまたは更新を実行するときには、ランタイムセキュリティを有効にするために `--set sensor.runtimeDetection=true` フラグを含めてください。

詳細については、Kubernetes ランタイム検出センサーのインストールを参照してください。

アドミッションコントローラー

アドミッションコントローラーの概要を使用するには、Helm を使用してセンサーをインストールする必要があります。この要件は、パブリック、プライベート、アンマネージド Kubernetes と OpenShift クラスタにおける、サポート対象のすべてのクラウドプロバイダーに適用されます。

詳細については、アドミッションコントローラーのインストールを参照してください。

クラウドごとの Kubernetes 要件

次の表は、各クラウドプロバイダーのクラスターの処理に必要なアクセス許可とネットワーク設定をまとめたものです。詳細および特定の接続手順については、各プロバイダーのドキュメントのリンクを参照してください。

注意: Azure では、クラスタの設定に使用する認証および承認方法に応じて、異なる方法でアクセス許可が付与されます。ローカルアカウントの認証方法は、Tenable Kubernetes Cluster Connector の使用のみでサポートされており、AKS クラスターのクラウドベースの接続手順経由ではありません。

	AWS	Azure (Azure RBAC のある Microsoft Entra ID)	Azure (Kubernetes RBAC のある Microsoft Entra ID)	GCP	OCI
必要なアクセス許可	Tenable IAM ロール用の `ClusterRole` および `ClusterRoleBinding` を作成します。	• Tenable App[1] へのビルトインロールバインディングを割り当てます。 • Tenable カスタムロールをク	`ClusterRole` [] 用の および `ClusterRoleBindingTenable`を作成	GCP 接続中に `Kubernetes Engine Viewer` ロールを追加します	Tenable OCI グループロール用の `ClusterRole` および `ClusterRoleBinding` を作成します。

	AWS	Azure (Azure RBAC のある Microsoft Entra ID)	Azure (Kubernetes RBAC のある Microsoft Entra ID)	GCP	OCI
		ラスター/サブスクリプションに追加します。			
ネットワークアクセス	クラスターネットワーキングを **パブリックおよびプライベート**に設定し、許可する Tenable One Cloud Exposure IP アドレスを指定します。クラスターネットワークが **プライベート**の場合は、Tenable Connector 経由で接続できます。	**[許可された IP 範囲を設定]** を有効にし、許可する Tenable IP アドレスを指定します。	**[許可された IP 範囲を設定]** を有効にし、許可する Tenable IP アドレスを指定します。	**コントロールプレーン認証ネットワーク**を有効にし、許可する Tenable IP アドレスを指定します。	クラスターネットワークを設定し、許可する クラウドサイバーエクスポージャー IP アドレスを指定します。Tenable へのネットワークアクセスを許可する参照してください。

	AWS	Azure (Azure RBAC のある Microsoft Entra ID)	Azure (Kubernetes RBAC のある Microsoft Entra ID)	GCP	OCI
ドキュメント	EKS クラスタ	AKS クラスター: Azure RBAC	AKS クラスター: K8S RBAC	GKE クラスタ	OKE クラスタ

必要なロール[1]

- `Azure Kubernetes Service Cluster User Role`
- `Azure Kubernetes Service RBAC Reader`

> **注意:** Tenable はパブリックアクセスを有効にしてクラスターにアクセスできますが、この構成はセキュリティのベストプラクティスに従っていません。安全な態勢を維持し、プライベートクラスターを監視するために、プラットフォームは Helm チャートを介してクラスタを接続する チャート接続を使用することを推奨しています。

Amazon EKS クラスタの接続

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Tenable One Cloud Exposure で Amazon EKS クラスタを接続して、アクセス許可、サブスクリプション使用状況、セキュリティ設定に関する情報など、クラスタに関連付けられたすべてのクラウドアイデンティティとリソースに対する完全な可視性とリスク評価を取得します。

統合を完了するまで、クラスターに関連するオブジェクトや構成は分析されず、Tenable での調査にも利用できません。関連するインベントリビューに各 Kubernetesクラスタの リソース同期ステータス が表示されます。これは、Kubernetes API に接続できるかどうかを示す Tenable、接続に関する潜在的な問題のトラブルシューティングに役立ちます。

要件

モニタリングするクラスタごとに、次の両方の手順を実行します。これらのステップのいずれかまたは両方を実行することが不可能または実用的でない場合、Tenable は Helm チャートを介してクラスタを接続する代替の接続パスを提供します。

- Tenable IAM ロールをクラスタに追加することで、Tenable ロールクラスターアクセス許可を付与するします。
- **Tenableロールにクラスタにアクセスするアクセス許可がない場合は、代わりに Helm チャートを介してクラスタを接続する。** AWSではアイデンティティ関連の設定が必要です。場合によっては、この設定が従来のクラウドベースの統合でサポートされていないことがあります。
- Tenable へのネットワークアクセスを許可するします。
- **クラスタコントロールプレーンがパブリックにアクセスできない場合は、代わりに Helm チャートを介してクラスタを接続するしてください。** たとえば、プライベートクラスタの場合などです。

> **注意:** Kubernetes 脅威検出、アドミッションコントローラーの概要、センサーベースのワークロード保護を有効にするには、Helm チャートを介してクラスタを接続する チャートを使用してセンサーをインストールする必要があります。これは、すべてのクラウドプロバイダーとクラスタタイプに適用されます。

Tenable ロールクラスターアクセス許可を付与する

次のいずれかの方法を使用して、Tenable ロールクラスターのアクセス許可を付与します。

- AWS コンソールを使用してクラスタのアクセス許可を付与する (推奨)
- CLI を使用したクラスタのアクセス許可の付与

AWS コンソールを使用してクラスタのアクセス許可を付与する (推奨)

Tenable IAM ロールに必要なアクセス許可を付与して、クラスタへのTenableアクセスを提供します。これを行うには、認証モードを **EKS API および ConfigMap** に設定し、IAM アクセスエントリを設定してから、適切なアクセスポリシーを割り当てます。

> **注意:**

- リソースのアクセス許可セットがより制限されたロールを使用することもできますが、この場合、今後関連するアクセス許可が追加されると手動で追加しなければなりません。
- IAM ロールは、Tenable 読み取りアクセス許可のみを付与します。

AWS コンソールを使用してクラスタのアクセス許可を付与する方法

1. AWS マネジメントコンソールにログインします。
2. **Elastic Kubernetes Service** に移動します。
3. 左側のメニューで、**[Clusters]** をクリックします。
4. 関連するクラスタを選択します。
5. **[アクセス]** タブをクリックします。
6. アクセス設定認証モードとして、**EKS API** または **EKS API と ConfigMap** を選択します。

   注意: Amazon は、今後のリリースで ConfigMap を廃止する予定です。詳細については、公式の AWS ドキュメントを参照してください。

7. IAMアクセスエントリを設定するには:
   1. **[アクセスエントリの作成]** をクリックします。
   2. **IAM プリンシパル**: 統合プロセス中に作成された **IAM ロール ARN** を選択します。
   3. **[次へ]** をクリックします。
8. アクセスポリシーを追加するには
   1. **ポリシー名**: ドロップダウンリストから `AmazonEKSAdminViewPolicy` を選択します。
   2. **アクセス範囲**: **[クラスタ]** を選択します。
   3. **[次へ]** をクリックします。
9. **[作成]** をクリックします。

CLI を使用したクラスタのアクセス許可の付与

Tenable IAM ロールのアクセス許可をクラスタに付与して、クラスタへのTenableアクセスを提供します。このために、Tenable IAM ロールを EKS クラスタ ConfigMap に追加し、クラスタロールとクラスタロールバインディングを作成します。以下の手順では、`kubectl` コマンドを使用してこれを行う方法を示していますが、

eksctl またはその他の方法を使用することもできます。詳細は、Amazon EKS のドキュメントで説明されているガイドラインに従ってください。

> **注意:**
>
> - リソースのアクセス許可セットがより制限されたロールを使用することもできますが、この場合、今後関連するアクセス許可が追加されると手動で追加しなければなりません。
> - IAM ロールは、Tenable 読み取りアクセス許可のみを付与します。

前提条件

- このアクションを実行するために必要なアクセス許可があることを確認してください。
- 次のツールがインストールされていることを確認します。
  - AWS CLI
  - kubectl

EKS クラスタの接続手順

1. AWS CLI から次のコマンドを実行します。

   ```
   aws eks --region {your_region} update-kubeconfig --name {your_cluster_name}
   ```

   ここで、{your_region} は AWS リージョンを表し、{your_cluster_name} は EKS クラスタの名前を表しています。
2. 次のコマンドを実行してください。

   ```
   cd ~/.kube
   ```
3. **クラスターロール** YAML ファイルを作成します。
   - 次のコマンドを実行してファイルを編集します。

     ```
     vim {clusterRole}.yaml
     ```

     ここで、{clusterRole} はファイルに付けるために選択した名前です。

- 以下の clusterRoleを追加します。

```
YAML

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: ermetic-kube-connector-cluster-role
rules:
  - apiGroups: ["*"]
    resources: ["*"]
    verbs: ["get", "list", "watch"]
```

4. **クラスターロールバインディング** YAML ファイルを作成します。
   - 次のコマンドを実行してファイルを編集します。

     vim {clusterRoleBinding}.yaml

     ここで、{clusterRoleBinding} はファイルに付けるために選択した名前です。
   - 以下の clusterRoleBindingを追加します。

```
YAML

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: ermetic-kube-connector-cluster-role-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ermetic-kube-connector-cluster-role
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: ermetic-kube-connector
```

5. 次のコマンドを実行して、作成した clusterRole/clusterRoleBinding をクラスタに適用します。

   kubectl apply -f ./{clusterRole}.yaml
   kubectl apply -f ./{clusterRoleBinding}.yaml

   ここで、{clusterRole}と{clusterRoleBinding} は YAML ファイルに付けた名前です。

6. (オプション)次のコマンドを実行して、clusterRole/clusterRoleBinding が適用されていることを検証します。

   ```
   kubectl get clusterroles
   kubectl get clusterrolebindings
   ```

   関連する値が存在することを確認します。たとえば、次の画像は Tenable clusterRole 値を示しています。

   ```
   NAME                                                   CREATED AT
   admin                                                  2023-03-13T10:44:15Z
   aws-node                                               2023-03-13T10:44:24Z
   cluster-admin                                          2023-03-13T10:44:15Z
   edit                                                   2023-03-13T10:44:15Z
   eks:addon-manager                                      2023-03-13T10:44:24Z
   eks:certificate-controller-approver                    2023-03-13T10:44:20Z
   eks:certificate-controller-signer                      2023-03-13T10:44:20Z
   eks:cloud-controller-manager                           2023-03-13T10:44:20Z
   eks:cloud-provider-extraction-migration                2023-03-13T10:44:20Z
   eks:cluster-event-watcher                              2023-03-13T10:44:20Z
   eks:fargate-manager                                    2023-03-13T10:44:24Z
   eks:fargate-scheduler                                  2023-03-13T10:44:20Z
   eks:k8s-metrics                                        2023-03-13T10:44:20Z
   eks:node-bootstrapper                                  2023-03-13T10:44:24Z
   eks:node-manager                                       2023-03-13T10:44:24Z
   eks:nodewatcher                                        2023-03-13T10:44:20Z
   eks:pod-identity-mutating-webhook                      2023-03-13T10:44:20Z
   eks:tagging-controller                                 2023-03-13T10:44:20Z
   ermetic-kube-connector-cluster-role                    2023-03-13T12:01:51Z
   ```

7. 次のコマンドを実行して aws-auth ConfigMapを編集します。

   ```
   kubectl edit configmap/aws-auth --namespace kube-system
   ```

8. 以下のように、Tenable IAM ロールの詳細を mapRoles セクションに追加します。

   重要: 追加する新しい groups 要素が、フォーマットなど、既存のグループと同じレベルに適切に配置されていることを確認します。

   YAML

   ```
   mapRoles: |
               ...
         <existing groups>
   ```

```
        ...
    - groups:
      - ermetic-kube-connector
      rolearn: arn:aws:iam::{111122223333}:role/{tenable-role-name}
      username: ermetic-kube-connector
```

ここで、{111122223333} と {tenable-role-name} は Tenable ロール ARN に関連する値です。

以下の例は、mapRoles セクションのコンテキストで Tenable IAM ロールの詳細を示しています。

```
#
apiVersion: v1
data:
  mapRoles: |
    - rolearn: <ARN of instance role (not instance profile)>
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
    - groups:
      - ermetic-kube-connector
      rolearn: arn:aws:iam::[redacted]:role/[redacted]
      username: ermetic-kube-connector
```

Tenable へのネットワークアクセスを許可する

クラウドサイバーエクスポージャーがクラスタにアクセスするには、クラスタエンドポイントをパブリックにアクセス可能にし、関連する許可が必要な Tenable IP アドレスする必要があります。

ネットワークアクセスを許可するには

1. AWS 管理コンソールで、**[EKS > Clusters]** に移動します。
2. 対象の **クラスタ名** をクリックします。
3. **[ネットワーク]** タブに移動し、**[ネットワークの管理]** をクリックします。クラスタエンドポイントへのアクセスの設定方法によっては、次のように設定の編集が必要になる場合があります。

- **パブリック。** アクセスがパブリックに設定されている場合、Tenable はクラスタにアクセスできますが、クラスタにアクセスするためのセキュリティのベストプラクティスには従いません。代わりに、アクセスを **パブリックとプライベート** に設定し、承認済みネットワークを Tenable に関連付けられているものなど、特定の IP アドレスに制限する必要があります。
- **パブリックとプライベート** 。パブリックが選択されている場合は、**[Advanced settings] (詳細設定)** をクリックし、**[CIDR block] (CIDR ブロック)** で、Tenableリージョンに関連付けられているすべての許可が必要な Tenable IP アドレスを追加します。
- **プライベート** 。このようなクラスタを Tenable 監視する場合は、クラスタをパブリックに切り替えるか、パブリックとプライベートに切り替えて、パブリックに公開する必要があります。

4. 完了したら、**[変更の保存]** をクリックします。

Azure AKS クラスタの接続

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Tenable One Cloud Exposure で Azure AKS クラスターを接続して、アクセス許可、サブスクリプションの使用状況、セキュリティ構成に関する情報など、クラスターに関連付けられているすべてのクラウド アイデンティティとリソースの完全な可視性とリスク評価を取得します。

統合を完了するまで、クラスターに関連するオブジェクトや構成は分析されず、Tenable での調査にも利用できません。関連するインベントリビューに各Kubernetesクラスタの リソース同期ステータス が表示されます。これは、Kubernetes API に接続できるかどうかを示す Tenable、接続に関する潜在的な問題のトラブルシューティングに役立ちます。

> **注意:** ディスクタイプがスナップショットをサポートしないため、エージェントレススキャンは、**エフェメラル** ディスクを使用する **Azure VM を** サポートしていません。この制限は、既定でエフェメラルディスクを使用する AKS クラスターに影響します。

要件

モニタリングする各クラスタについて、以下の手順に従って次の操作を行います。

- クラスタの設定に使用する認証および承認方法に応じて、次のいずれかの方法で Tenable アクセス許可を付与します。
  - Azure RBAC 対応の Microsoft Entra ID:
    - 組み込みロールバインディングを クラウド サイバーエクスポージャー アプリに割り当てる
    - クラスタ/サブスクリプションにカスタム Tenable ロールを追加する
  - Kubernetes RBAC 対応の Microsoft Entra ID:
    - の `ClusterRole` と `ClusterRoleBinding` の作成 Tenable
  - **ローカルアカウント認証**この方法は、Helm チャートを介してクラスタを接続するする場合のみサポートされます。

  重要: Tenable ロールにクラスタにアクセスするアクセス許可がない場合は、代わりに Helm チャートを介してクラスタを接続する します。 Azure ではアイデンティティ関連の設定が必要ですが、場合によってはこの設定が従来のクラウドベースの統合でサポートされていないことがあります。たとえば、Azure でローカル認証を使用する場合などです。

- Tenable へのネットワークアクセスを許可するします
- **クラスタコントロールプレーンがパブリックにアクセスできない場合は、代わりに Helm チャートを介してクラスタを接続するします。** たとえば、プライベートクラスタの場合などです。

注意: Kubernetes 脅威検出、アドミッションコントローラーの概要 、センサーベースのワークロード保護を有効にするには、Helm チャートを介してクラスタを接続する チャートを使用してセンサーをインストールする必要があります。これは、すべてのクラウドプロバイダーとクラスタタイプに適用されます。

クラスタへの Tenable アクセス許可の付与: Azure RBAC 対応の Microsoft Entra ID

Kubernetes クラスタ承認に Azure RBAC を使用する場合は、クラスタに Tenable アクセス許可を付与するために次の手順を行う必要があります。

- Kubernetes 関連の組み込みロールバインディングを Tenable に割り当てます。

  これらのロールは、Azure サブスクリプションを Tenable に接続したときに割り当てられますが、サブスクリプションを接続したかどうか、またいつ接続したかによって、まだ割り当てられていない可能性があります。

- カスタム Tenable ロールを追加する。

前述の箇条書きで挙げたロールバインディングは範囲が限定されており、クラウド サイバーエクスポージャー 内で IAM は可視化されません。すべての機能を利用するには、カスタムロールを追加して、名前空間 Tenable ほとんどのオブジェクトを表示するための読み取り専用アクセス許可を追加で付与する必要もあります。

注意: リソースのアクセス許可セットがより制限されたロールを使用することもできますが、この場合、今後関連するアクセス許可が追加されると手動で追加しなければなりません。

組み込みのロールバインディングを Tenable に割り当てる

- クラスタが存在する Azure サブスクリプションをすでに Tenable に接続していて、Kubernetes関連のアクセス許可をクラスタに追加する必要がある場合は、以下の手順に従います。
- クラスタが存在する Azure サブスクリプションをまだ接続していない場合は、「Azure サブスクリプションの接続」に記載されている手順に従います。

ロールバインディングを割り当てる方法

1. Azure ポータルで、**[サブスクリプション]** ページに移動し、関連するサブスクリプションをクリックします。
2. **[アクセス制御 (IAM)]** をクリックし、**[ロールの割り当ての追加]** をクリックします。
3. [ロールの割り当ての追加] ページで、次のいずれかのロールを検索して選択し、**[次へ]** をクリックします。

   注意: 追加できるロールは一度に 1 つだけであるため、これらの手順をロールごとに 1 回ずつ、つまり 2 回実行する必要があります。

   - **Azure Kubernetes サービスクラスタユーザーロール**
   - **Azure Kubernetes サービス RBAC リーダー**
4. [*アクセスの割り当て先*] は、デフォルトの選択 **[ユーザー、グループ、またはサービスプリンシパル]** のままにします。
5. [*メンバー*] で、**[+メンバーを選択]** をクリックします。
6. **クラウド サイバーエクスポージャー コネクタアプリ**を検索して選択し、**[選択]** をクリックします。
7. **[次へ]** をクリックし、新しいロールを確認して **[レビューと割り当て]** をクリックします。
8. 手順 3 で既に選択したロールに応じて、手順 1 から 7 までを繰り返して他のロールを追加します。

カスタム Tenable ロールを追加する

Kubernetes クラスタ承認に Azure RBAC を使用しており、組み込みのロールバインディングを Tenable に割り当てるによって提供されないTenable内で IAM の可視性を得る場合は、以下のカスタムロール JSON をサブスクリプションに追加します。カスタムロールの詳細については、Azure のドキュメント を参照してください。

Tenableロールを追加するには

1. Azure ポータルで、**[サブスクリプション]** ページに移動し、関連するサブスクリプションをクリックします。
2. **[アクセス制御 (IAM)]** をクリックして、**[追加] > [カスタムロールの追加]** の順にクリックします。
3. **[JSON]** タブに移動し、**[編集]** をクリックします。
4. 次のロールを貼り付けて、JSON のコンテンツを置き換えます。

> **重要:** 以下の `{subscription Id}` を Azure **サブスクリプション ID** に置き換えてください。

JSON

```
{
    "properties": {
        "roleName": "Tenable Azure Kubernetes Service Reader",
        "description": "Allows read-only access to see most objects in a namespace.",
        "assignableScopes": [
            "/subscriptions/{subscription Id}"
        ],
        "permissions": [
            {
                "actions": [
                    "Microsoft.ContainerService/managedClusters/listClusterUserCredential/action"
                ],
                "notActions": [],
                "dataActions": [
                    "Microsoft.ContainerService/managedClusters/*/read"
                ],
                "notDataActions": []
            }
        ]
    }
}
```

5. **[保存]** をクリックし、**[確認 + 作成]** をクリックします。
6. 新しいカスタムロールを確認し、**[作成]** をクリックします。
7. **[アクセス制御 (IAM)]** ページに戻り、**[追加] > [ロール割り当ての追加]** をクリックします。
8. **[Tenable Azure Kubernetes Service Reader]** を検索して選択し、**[次へ]** をクリックします。
9. [アクセスの割り当て先] は、デフォルトの選択 **[ユーザー、グループ、またはサービスプリンシパル]** のままにします。
10. [メンバー] で、**[+ メンバーを選択する]** をクリックします。
11. **Ermetic App** を検索して選択し、**[選択]** をクリックします。
12. **[次へ]** をクリックし、新しいロールの割り当てを確認し、**[確認 + 割り当て]** をクリックします。

クラスタに Tenable アクセス許可を付与する: Kubernetes RBAC 対応の Microsoft Entra ID

Kubernetes クラスター承認に Kubernetes RBAC を使用して、クラスターに Tenable アクセス許可を付与する場合は、Tenable 用の `ClusterRole` と `ClusterRoleBinding` を作成する必要があります。たとえば、kubectl コマンドラインツールを使用して、Tenable用に以下の`ClusterRole`と`ClusterRoleBinding`を作成します。

> **注意:** リソースのアクセス許可セットがより制限されたロールを使用することもできますが、この場合、今後関連するアクセス許可が追加されると手動で追加しなければなりません。

YAML

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: ermetic-kube-connector-cluster-role
rules:
  - apiGroups: ["*"]
    resources: ["*"]
    verbs: ["get", "list", "watch"]
```

YAML

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
```

```
metadata:
  name: ermetic-kube-connector-cluster-role-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ermetic-kube-connector-cluster-role
subjects:
  - apiGroup: rbac.authorization.k8s.io
    kind: User
    name: <ermetic-microsoft-entra-id-application-object-id>
```

Tenable へのネットワークアクセスを許可する

Tenableがクラスタにアクセスするには、クラスタエンドポイントをパブリックにアクセス可能にし、関連する許可が必要な Tenable IP アドレスする必要があります。

ネットワークアクセスを許可するには

1. Azure ポータルで、**Kubernetes サービス**に移動します。
2. 対象の **クラスタ名** をクリックします。
3. [Settings] で、**[Networking]** をクリックします。
4. [セキュリティ] で、**[承認済みの IP 範囲を設定する]** チェックボックスをクリックします。

   > **注意:** この設定が無効になっている場合、Tenable クラスタにアクセスできますが、クラスタにアクセスするためのセキュリティのベストプラクティスには従いません。代わりに、この設定を有効にし、承認済みネットワークを特定の IP アドレス (Tenable に関連付けられているものなど) に制限する必要があります。

5. 表示される **[IP 範囲を指定]** フィールドに、Tenableリージョンに関連付けられているすべての許可が必要な Tenable IP アドレスを追加します。
6. **[適用]** をクリックします。

Google GKEクラスターを接続する

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Tenable One Cloud Exposure で Google GKE クラスターを接続すると、アクセス許可、サブスクリプション使用率、セキュリティ設定に関する情報を含む、クラスターに関連付けられているすべてのクラウドアイデンティティとリソースの完全な可視性とリスク評価を得ることができます。

統合を完了するまで、クラスターに関連するオブジェクトと構成は、Tenableで分析されたり、調査に利用されたりすることはありません。各 Kubernetes クラスターについては、関連するインベントリビューで リソース同期ステータス が表示されます。これは、Tenable がKubernetes API に接続できるかどうかを示し、潜在的な接続の問題のトラブルシューティングに役立ちます。

要件

監視する各クラスターに対して、次の手順を実行します。

- クラスターを含む関連する Google 環境 (組織 / プロジェクト) に正常に接続され、Kubernetes Engine Viewer ロールが指示に従って追加されたことを確認します。
- Tenable へのネットワークアクセスを許可するには、次の手順に従います。
    - **クラスターコントロールプレーンが公開されない場合、代わりに Helm Chart を介してクラスターを接続します** 。たとえば、プライベートクラスターの場合などです。

> **注意:** Kubernetes 脅威検出、アドミッションコントローラーの概要 、センサーベースのワークロード保護を有効にするには、Helm チャートを介してクラスタを接続する チャートを使用してセンサーをインストールする必要があります。これは、すべてのクラウドプロバイダーとクラスタタイプに適用されます。

Tenable へのネットワークアクセスを許可する

クラウドサイバーエクスポージャー の場合、クラスターにアクセスするには、クラスターエンドポイントがパブリックアクセス可能である必要があり、関連する 許可が必要な Tenable IP アドレス。

ネットワークアクセスを許可するには

1. Google Cloud コンソールで、**Kubernetes Engine** に移動し、関連するクラスターの **名前** をクリックします。
2. [ネットワーク] セクションで、**[コントロールプレーンの認証済みネットワーク]** 設定が **[有効]** になっていることを確認します。

> **ヒント:** この設定が無効になっている場合、Tenable はクラスタにアクセスできますが、クラスタにアクセスするためのセキュリティのベストプラクティスには従いません。代わりに、この設定を有効にし、承認済みネットワークを特定の IP アドレス (Tenable に関連付けられているものなど) に制限する必要があります。

3. **[コントロールプレーン] 認証ネットワーク** 設定を編集し、[認証ネットワーク] セクションで **[ADD AUTHORIZED NETWORK]** をクリックします。
4. Tenable 地域に関連するすべての許可が必要な Tenable IP アドレス 認証済みネットワークとして追加し、各 IP アドレスの後に **[DONE]** をクリックします。
5. **[Save Changes]** をクリックします。

Oracle OKEクラスタの接続

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Oracle OKE クラスタを Tenable Tenable One Cloud Exposure で接続して、アクセス許可、サブスクリプション使用状況、セキュリティ設定に関する情報など、クラスタに関連付けられているすべてのクラウドアイデンティティとリソースに対する完全な可視性とリスク評価を取得します。

統合を完了するまで、クラスターに関連するオブジェクトや構成は分析されず、Tenable での調査にも利用できません。各 Kubernetes クラスタの リソース同期ステータス が関連するインベントリビューに表示されます。これは、Tenable が Kubernetes API に接続できるかどうかを示し、潜在的な接続の問題のトラブルシューティングに役立ちます。

要件

モニタリングするクラスタごとに、次の両方の手順を実行します。これらのステップのいずれかまたは両方を実行することが不可能または実用的でない場合、Tenable は Helm チャートを介してクラスタを接続する代替統合パスを提供します。

- Grant Cluster Permissions.
- **Tenable ロールにクラスタにアクセスするためのアクセス許可がない場合は、代わりに Helm チャートを介してクラスタを接続する します。**

- Tenable へのネットワークアクセスを許可するします
- **クラスタコントロールプレーンがパブリックにアクセスできない場合は、代わりにHelm チャートを介してクラスタを接続するします。**たとえば、プライベートクラスタの場合などです。

> **注意:** Kubernetes 脅威検出、アドミッションコントローラーの概要 、センサーベースのワークロード保護を有効にするには、Helm チャートを介してクラスタを接続する チャートを使用してセンサーをインストールする必要があります。これは、すべてのクラウドプロバイダーとクラスタタイプに適用されます。

クラスタのアクセス許可を付与する

Kubernetesクラスタを Tenableに接続するには、CLI を使用したクラスタのアクセス許可の付与 とOCI ポリシーを使用したクラスタのアクセス許可の付与の両方を使用してアクセス許可を付与する必要があります。

> **注意:**
>
> - CLI **を使用してアクセス** 許可を付与すると、特定のクラスターで `ClusterRole` と `ClusterRoleBinding` が作成されるため、これはクラスターごとに個別に実行する必要があります。
> - **OCI ポリシー**を使用したクラスタのアクセス許可の付与は、テナンシレベルでグローバルに 1 回実行されます。

CLI を使用したクラスタのアクセス許可の付与

グループTenable **ロール**のアクセス許可をクラスタに付与して、クラスタへのTenableアクセスを提供します。これを行うには、Tenable グループロールを OKE クラスタに追加し、`ClusterRole` と `ClusterRoleBinding`を作成します。次の手順は、`kubectl` コマンドを使用してこれを行う方法を示しています。詳細は、Oracle OKE のドキュメント で説明されているガイドラインに従ってください。

> **注意:**
>
> - リソースのアクセス許可セットがより制限されたロールを使用することもできますが、この場合、今後関連するアクセス許可が追加されると手動で追加しなければなりません。
> - グループロールは、Tenable 読み取りアクセス許可のみを付与します。

前提条件

- このアクションを実行するために必要なアクセス許可があることを確認してください。
- 次のツールがインストールされていることを確認します。
  - OCI CLI
  - kubectl

OKE クラスタの接続手順

1. OCI CLI を介して次のコマンドを実行します。

   ```
   oci ce cluster create-kubeconfig cluster-id {your_cluster_ocid} --file $HOME/.kube/config region {your_region} --token-version {your_token_version} --kube-endpoint {your_endpoint_type}
   ```

   > **注意:**
   > - `--token-version`:詳細については、公式のOracleドキュメントを参照してください。
   > - `--kube-endpoint`:詳細については、公式のOracleドキュメントを参照してください。

2. 次のコマンドを実行してください。

   ```
   cd ~/.kube
   ```

3. **クラスターロール**YAML ファイルを作成します。
   - 次のコマンドを実行してファイルを編集します。

     ```
     vim {clusterRole}.yaml
     ```

     ここで、`{clusterRole}` はファイルに付けるために選択した名前です。
   - 以下の`clusterRole`を追加します。

     YAML

     ```yaml
     apiVersion: rbac.authorization.k8s.io/v1
     kind: ClusterRole
     metadata:
       name: tenable-kube-connector-cluster-role
     rules:
       - apiGroups: ["*"]
         resources: ["*"]
         verbs: ["get", "list", "watch"]
     ```

4. **クラスターロールバインディング** YAML ファイルを作成します。

   - 次のコマンドを実行してファイルを編集します。

     ```
     vim {clusterRoleBinding}.yaml
     ```

     ここで、{clusterRoleBinding} はファイルに付けるために選択した名前です。

   - 以下の clusterRoleBindingを追加します。

     YAML

     ```
     apiVersion: rbac.authorization.k8s.io/v1
     kind: ClusterRoleBinding
     metadata:
       name: tenable-kube-connector-cluster-role-binding
     roleRef:
       apiGroup: rbac.authorization.k8s.io
       kind: ClusterRole
       name: tenable-kube-connector-cluster-role
     subjects:
     - apiGroup: rbac.authorization.k8s.io
       kind: Group
       name: {tenable_group_ocid}
     ```

     > **注意:** tenable_group_ocid = OCI 統合プロセスを介して作成したグループ ID。詳細については、こちらのグループの作成を参照してください。

5. 次のコマンドを実行して、作成した clusterRole/clusterRoleBinding をクラスタに適用します。

   ```
   kubectl apply -f ./{clusterRole}.yaml
   kubectl apply -f ./{clusterRoleBinding}.yaml
   ```

   ここで、{clusterRole}と{clusterRoleBinding} は YAML ファイルに付けた名前です。

6. (オプション)次のコマンドを実行して、clusterRole/clusterRoleBinding が適用されていることを検証します。

   ```
   kubectl get clusterroles
   kubectl get clusterrolebindings
   ```

OCI ポリシーを使用したクラスタのアクセス許可の付与

新しいOCIポリシーを作成し、ポリシーステートメントを使用して必要なアクセス許可を割り当てることで、クラウドサイバーエクスポージャーにOCI Kubernetesをスキャンするアクセス許可を付与します。

Kubernetesクラスタリソースに読み取りアクセス許可を付与するには

1. Oracleコンソールで、**[アイデンティティとセキュリティ]** > **[アイデンティティ** > **ポリシー]** の順に移動します。
2. **[ポリシーの作成]** をクリックし、以下の詳細を入力します。
    1. **名前**: 意味のある名前を入力します。
    2. **説明**: わかりやすい説明を入力します
    3. **コンパートメント**: rootコンパートメントを選択します
3. ポリシービルダーで **[手動エディターの表示]** をクリックし、次のステートメントを追加します。
    - `Allow group {tenable_group_name} to use clusters in tenancy`

      > **注意:** `tenable_group_name` = OCI統合プロセスを使用して作成したグループ名。詳細については、こちらのグループの作成を参照してください。

Tenableへのネットワークアクセスを許可する

クラウドサイバーエクスポージャーがクラスタにアクセスするには、クラスタエンドポイントをパブリックにアクセス可能にし、関連する許可が必要なTenable IPアドレスする必要があります。

ネットワークアクセスを許可するには

1. OCI管理コンソールで、「開発者 **サービス]** >「 **コンテナおよびアーティファクト** 」> **OKE**に移動します。
2. 対象の **クラスタ名** をクリックします。
3. **[編集]** をクリックし、**[API エンドポイントにパブリック IP アドレスを割り当てる]** を選択します。
    - **パブリックとプライベート**。選択した場合は、クラスタの **[Virtual Cloud Network]** 設定 > **[Security > Cluster's K8s API Endpoint Rule]** > **[Security rules]** に移動し、Tenableリージョンに関連付けられている許可が必要なTenable IPアドレスからのトラフィックのみを許可するようにイングレスルールを編集できます。

4. 完了したら、**[変更の保存]** をクリックします。

Helm チャートを介してクラスタを接続する

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

これは、Helm チャートを使用してクラスタを Tenable に接続するためのハウツーガイドです。

- Kubernetes 機能の概念概要については、「Kubernetes」を参照してください。
- Kubernetes クラスタの表示と管理に関するハウツーガイドについては、「Kubernetesクラスター」を参照してください。
- よく寄せられる質問については、「FAQ: Kubernetes」を参照してください。

Tenable では、クラウドネイティブの API メソッドの代わりに Helm チャートを使用して Kubernetes クラスタを接続できます。この方法は、アイデンティティベースまたはネットワークベースのアクセスが制限されているプライベートクラスタ、オンプレミス環境、またはマネージドクラスタに必要です。さらに、センサーベースの脆弱性管理やアドミッションコントローラーなどの Kubernetes 機能には Helm が必要です。

次のセクションを使用して、リソース同期、ランタイム検出、ワークロード保護、追加のセキュリティ機能に Helm チャート (センサーベース) とクラウドネイティブ (エージェントレス) のどちらの方法を使用するかを判断します。

Helm チャートメソッドを使用するタイミング

Helm チャートの統合により、セキュリティポスチャーが基本的なメタデータ検出だけでなく、包括的なディープスキャン分析に拡張されます。次のシナリオでは、この統合方法を選択する必要があります。

- **接続の確立**: クラスタが以下の場合は、このメソッドを使用します。
  - **マネージド (プライベート):** API サーバーがインターネットからアクセスできないマネージド (プライベート) クラスタを使用します。
  - **オンプレミス:** プライベートデータセンターなど、カスタマーマネージドのリソースでインフラをホストします。

- **Kubernetes 固有の機能の有効化**: 脅威検出、アドミッションコントローラーの概要、脆弱性管理などの機能を有効化します。
- 以下に挙げるような**高度なセキュリティ要件またはコンプライアンス要件**に対応します。
  - **リアルタイムポリシーの実施:** Kubernetes アドミッションコントローラーの概要に必要です。
  - **詳細な設定の可視性:** ロールベースのアクセス制御 (RBAC) とクラスタ設定に関する詳細な文脈情報を提供します。

詳細については、Kubernetesクラスターを接続するを参照してください。

Kubernetes クラスタの接続

クラスタを接続する前に、デプロイメントモデルにHelm チャートメソッドが必要かどうかを確認してください。プライベートクラスタ、オンプレミス環境、およびクラウドネイティブ API メソッドがサポートされていない特定のセキュリティ機能には、Kubernetes クラスタ Helm チャートを使用します。

Kubernetes リソース同期および脆弱性管理

クラウドプロバイダー	マネージド (パブリック)	マネージド (プライベート)	アンマネージド
AWS [1]	適切なアクセス許可の付与 (エージェントレス)	Helm チャートからのインストール (センサー)	Helm チャートからのインストール (センサー)
Azure [2]	適切なアクセス許可の付与 (エージェントレス)	Helm チャートからのインストール (センサー)	Helm チャートからのインストール (センサー)
GCP [3]	適切なアクセス許可の付与 (エージェントレス)	Helm チャートからのインストール (センサー)	Helm チャートからのインストール (センサー)
OCI	クラスタのアクセス許可	Helm チャートから	Helm チャートから

クラウドプロバイダー	マネージド (パブリック)	マネージド (プライベート)	アンマネージド
	を付与する (エージェントレス)	のインストール (センサー)	のインストール (センサー)
オンプレミスと、サポートされていないクラウドプラットフォームすべて	該当なし	該当なし	Helm チャートからのインストール (センサー)

以下の機能は、**脆弱性管理**スキャンで現在**サポートされていません**。

AWS [1] - Fargate は脆弱性管理でサポートされていません。

Azure [2] - 仮想ノードは脆弱性管理でサポートされていません。

GCP [3] - Autopilot は脆弱性管理でサポートされていません。

> **注意:** エージェントレスの統合は、脆弱性管理スキャンをサポートするうえで最も一般的かつ推奨されるアプローチですが、特定のシナリオではセンサーベースの設定が必要です。詳細については、エージェントレススキャンとエージェントベーススキャンの比較を参照してください。

ランタイム検出

脅威検出を使用するには、Helm を使用してセンサーをインストールする必要があります。この要件は、パブリック、プライベート、アンマネージド Kubernetes と OpenShift クラスタにおける、サポート対象のすべてのクラウドプロバイダーに適用されます。

接続用に Helm ベースのセンサーを使用している場合、別途インストールを行う必要はありません。代わりに、既存のデプロイメントをランタイムフラグで更新してください。インストールまたは更新を実行するときには、ランタイムセキュリティを有効にするために `--set sensor.runtimeDetection=true` フラグを含めてください。

詳細については、Kubernetes ランタイム検出センサーのインストールを参照してください。

アドミッションコントローラー

アドミッションコントローラーの概要を使用するには、Helm を使用してセンサーをインストールする必要があります。この要件は、パブリック、プライベート、アンマネージド Kubernetes と OpenShift クラスタにおける、サポート対象のすべてのクラウドプロバイダーに適用されます。

詳細については、アドミッションコントローラーのインストールを参照してください。

Kubernetes クラスタコネクタ (API トークン) を追加する

> **注意:** 環境内のすべてのクラスタに対して 1 つのコネクタを追加できます。クラスターごとまたはクラスターグループごとにこの手順を繰り返す必要はありません。

Helm を使用してクラスタ クラスターを追加する する前に、クラスタコネクタを作成する必要があります。これは、クラスタと Tenable間の安全な通信を認証するための API トークンとして機能します。

コネクタを追加する方法

1. Tenable One Cloud Exposure コンソールで、**[Settings** > **Integrations]** > [Add **Integration** > **Kubernetes Cluster]** に移動します。
2. [組織] ドロップダウンで アカウントの範囲 を選択します。デフォルトでは、組織全体 (すべてのアカウント) が選択されています。

   > **注意:**
   > - クラスターを追加するときには、コネクタを選択する必要があります。選択した範囲によって、コネクタを使用できる場所が決まります。たとえば、コネクタを AWS フォルダーに追加した場合、その範囲内でのみ選択できます。
   > - [Kubernetes クラスタ] ページの **[リソース同期]** 列は、コネクタアイコンを介してコネクタを使用するすべてのクラスタを Kubernetes で示します。

3. コネクタに意味のある **名前** を入力します。
4. **[追加]** をクリックします。

クラウドマネージドクラスタのリソースを同期する

Tenable では、EKS、AKS、GKE、OKE のドキュメントで説明されているクラウドベースの方法を使用して、クラウドマネージドクラスタを接続することを推奨しています。

ただし、これらの方法が実行できない場合は、Kubernetes クラスタ Helm チャートを使用してクラスタリソースを同期できます。この方法により、クラウド間直接接続が利用できない場合でも、コンテナリソースの更新されたインベントリを Tenable が確実に受け取ることができます。

次のような理由により、Helm チャート経由で同期することを選択できます。

- **アイデンティティ関連のアクセス許可がない**。これは、Tenable ロールにクラスタへのアクセス許可がない場合に発生します。GCP と OCI にはこれらのアクセス許可は必要ありませんが、他のプロバイダーには必要であり、一部の設定 (Azure でのローカル認証など) は従来の統合ではサポートされていません。
- **ネットワークベースのアクセスがありません**。これは、プライベートクラスタなど、クラスタコントロールプレーンがパブリックにアクセスできない場合に発生します。

Helm をパッケージマネージャーとして使用し、安全な通信を確立することで、これらのクラスタを Tenable に接続できます。

Helm チャートを使用してクラウドマネージドクラスタのリソースを同期する方法

1. Kubernetes クラスタコネクタを追加する
2. クラスターを追加する

オンプレミスまたはマネージド (プライベート) クラスタのリソースの同期

オンプレミスまたはプライベートマネージドクラスタを Tenable に接続して、クラスタに関連付けられているすべてのアイデンティティとリソースを完全に可視化します。この接続により、アクセス許可、サブスクリプション使用状況、セキュリティ設定に関するデータが得られます。

これらのクラスタを同期するには、Helm チャートを使用してワークロード (デプロイメント) をインストールします。この Helm チャートには、データを同期し、セキュリティ設定をクラスタに適用するために必要な Kubernetes リソースが含まれています。詳細については、「Tenable が Helm チャートを使用してクラスタに接続する方法」を参照してください。

> **注意:** 統合を完了するまで、Tenable はクラスタに関連付けられているオブジェクトや設定を分析または調査できません。[Kubernetes クラスタ] ページの リソース同期ステータス は、Tenable が Kubernetes API に接続できるかどうかを示します。

Helm チャートを使用してオンプレミスクラスタを同期する方法

1. Kubernetes クラスタコネクタを追加する
2. クラスターを追加する

Kubernetes ランタイム検出センサーのインストール

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

> **注意:** この機能は早期リリース版として提供されており、変更される可能性があります。機能およびサポートが制限される場合があります。アクセス権のリクエストやフィードバックの提供については、Tenable の担当者までご連絡ください。

ランタイム検出センサーは eBPF テクノロジーを使用して、システムレベルのアクティビティを監視し、クラスター内の不審なアクティビティを特定します。その後、センサーはこれらのイベントを Tenable に送信して、ほぼリアルタイムで分析します。詳細については、「脅威検出」を参照してください。

Kubernetes ワークロードを監視して不審なアクティビティがないか確認する方法

1. ランタイム検出用のアクセス許可と接続性など、すべての脅威検出の要件を満たしていることを確認します。
2. 次のいずれかを実行します。
    - **クラスタが Helm 経由で接続されていない場合**: クラスターを追加するし、Helm コマンドに `--set sensor.runtimeDetection=true` パラメーターを含めます。
    - **クラスタがすでに Helm 経由で接続されている場合** クラスタ追加機能でクラスターをアップグレードするし、Helm コマンドに `--set sensor.runtimeDetection=true` パラメーターを含めます。

アドミッションコントローラーのインストール

Helm チャートコマンドを使用してアドミッションコントローラーをインストールし、環境内の関連する Kubernetes クラスタを接続します。この設定により安全な接続が確保され、アドミッションコントローラーがポリシーを管理できるようになります。

アドミッションコントローラーは、クラスタ接続の初期時または後でこの機能でクラスタをアップグレードすることによってインストールできます。

アドミッションコントローラーを有効にして Helm チャートをインストールすると、システムによって CA 証明書、サーバーキー、サーバー証明書が生成されます。これらの証明書により、`kube-apiserver` と Tenable アドミッションコントローラー Webhook サーバーの間に安全な通信と信頼が確立されます。証明書は生成日から 3 年間有効です。

脆弱なコンテナイメージポリシーを有効にするには、アドミッションコントローラーがイメージプルシークレットを読み取って、デプロイされているコンテナイメージを識別する必要があります。これには Tenable Kubernetes Helm チャートバージョン 1.1.6 以降が必要です。シークレットアクセスは、デフォルトでは無効になっています。オンにするには、Helm コマンドに `--set admissionController.readSecrets=true` パラメーターを含めます。Tenable はシークレットをリストするアクセス許可を付与しますが、アドミッションコントローラーはイメージプルシークレットのみを調べます。

詳細な手順については、「クラスターを追加する」を参照してください。

Vulnerability Management Sensor for Kubernetes をインストールする

> **必要なライセンス:** この機能は **Enterprise** ライセンスでのみ利用できます。詳細については、ライセンスを参照してください。

Helm チャート付きのワークロード保護センサーをインストールして、オンプレミスおよびクラウドマネージドの Kubernetes クラスタの脆弱性をスキャンします。センサーは、クラスタで実行されている仮想マシン (ノード) とコンテナイメージの脆弱性を特定します。

センサーはパッケージマネージャーとインストールされているライブラリのクエリを実行し、ホストにインストールされているソフトウェアと、ノードで実行されているコンテナイメージを特定します。次に、センサーはこのソフトウェアインベントリを分析のために Tenable に送信します。

詳細については、「エージェントベースの Kubernetes ワークロードスキャン」を参照してください。

Kubernetes ワークロードの脆弱性をスキャンする方法

1. ワークロードスキャンの追加要件も含め、すべての要件を満たしていることを確認します。
2. 次のいずれかを実行します。
    - **クラスタがHelm経由で接続されていない場合**: クラスターを追加するし、Helmコマンドに `--set sensor.vulnerabilityManagement=true` パラメーターを含めます。
    - **クラスタがすでにHelm経由で接続されている場合** クラスタ追加機能でクラスターをアップグレードするし、Helmコマンドに `--set sensor.vulnerabilityManagement=true` パラメーターを含めます。

クラスターを追加する

クラスタを追加するには、動的に生成されたコマンドを使用してTenable提供のHelmチャートをインストールします。

要件

インストールする前に、クラスタが次の要件を満たしていることを確認してください。

クラスター基準	要件
Helmバージョン	• 最小 3.9.0 • Tenable 3.16.4 以上を推奨
一般リソース	• 最小 100m CPU(0.1 vCPU またはシングルコアの 10%) • クラスタあたり512 MiB (メビバイト) のメモリ
ワークロードスキャン	• (追加) ワーカーノードあたり1000m CPUと1GiBメモリ。 • サポートされているランタイムには、containerd、CRI-O、Dockerが含まれます
ランタイム検出	• CPU (Pod制限): 1コア (1000m) • メモリ(RAM): 1 GiB

クラスター基準	要件
接続性	• [許可されたデスティネーション] にリストされているTenable宛先への送信アクセスファイヤーウォール、プロキシ、またはネットワークポリシーによってクラスタからの送信トラフィックが制限されている場合は、これらの宛先を許可します。 • 無制限の送信アクセスもサポートされていますが、Tenable ではセキュリティ上の理由から、リストされている送信先への送信トラフィックを制限することを推奨しています。 • プロキシサーバーは、Helm のオプションのコマンドパラメーターを介してサポートされます。

プライベートレジストリ: Kubernetes環境でプライベート・レジストリを使用している場合は、インストールを開始する前に、プライベートレジストリを持つクラスタを使用してミラーリングまたはプルスルーを構成してください。

許可されたデスティネーション

クラスタからの送信トラフィックを制限する場合は、次の宛先を許可します。ワイルドカードエントリは、Tenableドメインにのみ適用されます。

デスティネーション	目的
`containers.tenable.com`	Helm チャートがデプロイするコンテナイメージをプルします。
`charts.tenable.com`	Tenable Helm リポジトリをホストします。`helm repo add`を実行する必要があります。プライベートレジストリを持つクラスタを使用する場合は必要ありません。
`app.tenable.com`	クラスタとクラウドサイバーエクスポージャー間の通信

デスティネーション	目的
*.app.tenable.com	クラスタとサイトのクラウドサイバーエクスポージャーエンドポイント間の通信 (<site-code>.app.tenable.com など)。
<site-code>-tunnel.internal.app.tenable.com	クラスタとクラウドサイバーエクスポージャー間の接続専用のトンネルエンドポイントです。
app.tenable.us と*.app.tenable.us	米国ガバメントクラウド環境でのみ必要です。

- ワイルドカード *.app.tenable.com はサブドメインのみに適合します。app.tenable.comー致しないので、両方を許可します。
- Kubernetes ネットワークポリシーなどの一部のツールは、ワイルドカード FQDN をサポートしていません。その場合は、ワイルドカードエントリの代わりに明示的なホスト名を許可します。たとえば、シンガポールサイト (1sg) の場合、次のことを許可します。
    - containers.tenable.com
    - charts.tenable.com
    - app.tenable.com
    - sg1.app.tenable.com
    - sg1-tunnel.internal.app.tenable.com sg1 をサイトコードに置き換えてください。

地域	サイトコード
米国	us1
オーストラリア	au1
ブラジル	br1
カナダ	ca1

地域	サイトコード
ヨーロッパ	`eu1`
インド	`in1`
日本	`jp1`
シンガポール	`sg1`
韓国	`kr1`
アラブ首長国連邦	`ae1`
英国	`uk1`
米国ガバメントクラウド	`usgov1`

Helm コマンドを設定して実行する

クラスタを追加するには、クラスタ上で `helm install` コマンドを設定して実行します。

クラスタを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Explore > Kubernetes Clusters]** に移動します。
2. (オプション)組織ツリーで、アカウントの範囲を選択します。デフォルトでは、コンソールは組織全体(すべてのアカウント)を選択します。

   > **注意:** 選択する範囲は、Tenable Kubernetes Cluster Connector の範囲と一致する必要があります。たとえば、AWS フォルダーにコネクタを追加した場合、そのコネクタはその範囲内でのみ選択できます。

3. 次のいずれかのアクションを実行します。
   - 複数のクラスタ(Tenable によってまだ検出されていないアンマネージドクラスタを含む)を一度に接続するには、**[Helm 経由でクラスタの追加]** をクリックします。

- (管理者のみ) Tenableによってすでに検出された個別のクラスタを接続するには、**[Kubernetesクラスタ]** テーブルでクラスタを検索し、**三点リーダー** メニューをクリックして **[Install Helm]** を選択します。
- (管理者のみ)クラスタがすでに接続されているが、新しい機能をインストールする場合は、「**Kubernetesクラスタ**」テーブルでクラスタを検索し、三点リーダーアイコンをクリックして、「**Upgrade Helm**」をクリックします。

4. Kubernetes のパッケージマネージャーとして Helm をインストールします。使用を開始するには、Helm のドキュメント を参照してください。
5. クラスタに接続するように `kubectl` を設定します。
6. 次のコマンドを実行して、Tenable リポジトリを追加します。

   ```
   helm repo add tenable https://charts.tenable.com
   ```

   (プライベートレジストリを持つクラスタを使用している場合は、この手順をスキップして、チャートが内部リポジトリで利用可能であることを確認してください)。

   注意:
   - リポジトリをすでに追加している場合は、`helm repo update tenable` を実行して最新のチャートに更新します。
   - 以前の URL (`https://charts.ermetic.com`) は廃止されるため、`https://charts.tenable.com` を使用する必要があります。

7. 関連するコネクタを選択します。コネクタがない場合は、続行する前にコネクタを追加 してください。すべてのクラスタに対して 1 つのコマンドを使用できます。
8. クラスタに関連付けるアカウントを選択します。アカウントは手動で選択するか、クラスタアカウントの場所を使用できます。
9. 使用する機能を選択します。選択した内容は、次のステップで生成されるコマンドに影響を与えます。
   - **リソース同期**。クラスタリソースの可視性を提供し、検出された設定ミスに関する検出結果をトリガーします。
   - (Enterprise ライセンスのみ) **ランタイムの検出**。eBPF センサーを使用してクラスターワークロードのイベントを監視し、不審なアクティビティを検出します。詳細については、「脅威検出」を参照してください。

- (Enterprise ライセンスのみ) **アドミッションコントローラー**。API リクエストをインターセプトして、ポリシーを強制し、設定を検証します。詳細については、「アドミッションコントローラーの概要」を参照してください。
- (Enterprise ライセンスのみ)**脆弱性管理**クラスタノードとコンテナイメージをスキャンして脆弱性を検出します。追加要件など、詳細については、「Kubernetes のワークロード保護センサーのインストール」を参照してください。

10. Tenable に接続してデータを送信するには、[Add Clusters via Helm] (Helm を介してクラスタを追加する) ダイアログに表示されるコマンドを実行します。このコマンドにより、クラスタに Kubernetes コネクタチャートがインストールされます。コマンドは、選択されたコネクタ、アカウント範囲、有効な機能に基づいて動的に生成されます。
11. (オプション) オプションのパラメーター をコマンドに追加します。
    次の画像は、オンプレミスワークロードスキャンが有効になっている場合の、このコマンドのサンプル出力を示しています。

```
bash-4.4 ~ $ helm install tenable-cloud-security-kubernetes-cluster tenable/cloud-security-kubernetes-cluster -n tenable-cloud-security-kubernetes-cluster --create-namespace --set apiKeyToken=YWYyY2M
1ZjctMWI1MS00NzUxLWExNjQtMTdmNDNhOTdhMzJkLjE5OWRjY2EwLWM4YzUtNDk5OC1iNWFlLWU2ZmQ0OTFmYzAzMC4zMXhNRWx0QTcvcWF1WC91NVBmV3R1Zk42Yi9qZVA4YQ== --set apiUrl=https://us.app.ermetic.com/ --set sensor.enabled
=true
WARNING: Kubernetes configuration file is group-readable. This is insecure. Location: /home/user/.kube/config
WARNING: Kubernetes configuration file is world-readable. This is insecure. Location: /home/user/.kube/config
W1027 13:04:47.644673     171 warnings.go:70] would violate PodSecurity "restricted:v1.24": host namespaces (hostPID=true), privileged (container "kubernetes-cluster-sensor-container" must not set se
curityContext.privileged=true), allowPrivilegeEscalation != false (container "kubernetes-cluster-sensor-container" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities
(container "kubernetes-cluster-sensor-container" must set securityContext.capabilities.drop=["ALL"]), restricted volume types (volume "kubernetes-cluster-sensor-data" uses restricted volume type "hos
tPath"), runAsNonRoot != true (pod or container "kubernetes-cluster-sensor-container" must set securityContext.runAsNonRoot=true), runAsUser=0 (container "kubernetes-cluster-sensor-container" must no
t set runAsUser=0)
NAME: tenable-cloud-security-kubernetes-cluster
LAST DEPLOYED: Sun Oct 27 13:04:36 2024
NAMESPACE: tenable-cloud-security-kubernetes-cluster
STATUS: deployed
REVISION: 1
TEST SUITE: None
bash-4.4 ~ $
```

デプロイメントの検証

センサーがデプロイされ、実行されていることを検証するには、次のコマンドを実行します。

- `kubectl get pods -n tenable-cloud-security-kubernetes-cluster`

> **注意:** 通常、PodがRunning状態になるまでに1～2分かかります。センサーは Kubernetes クラスタノードごとに実行されます。

以下の例では、2 つのノードがあります。

```
bash-4.4 ~ $ kubectl get pods -n tenable-cloud-security-kubernetes-cluster
NAME                                                  READY   STATUS    RESTARTS   AGE
kubernetes-cluster-connector-deployment-564cf5bc6-qpsfz   1/1     Running   0          7m9s
kubernetes-cluster-sensor-daemonset-q9ftp             1/1     Running   0          7m9s
kubernetes-cluster-sensor-daemonset-z6m2z             1/1     Running   0          7m9s
kubernetes-cluster-updater-deployment-6fbc959df8-bhfls    1/1     Running   0          7m9s
```

問題のトラブルシューティングについては、Helm チャートのトラブルシューティングを参照してください。

API 経由でのクラウドマネージドクラスタの接続

クラスタを追加するには、マネージドクラスタを自動的に検出して同期するために必要なクラウドアクセス許可をクラウドサイバーエクスポージャーに付与します。

クラスタを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Explore > Kubernetes Clusters]** に移動します。
2. *(オプション)* 組織ツリーで、アカウントの範囲を選択します。デフォルトでは、コンソールは組織全体 (すべてのアカウント) を選択します。

   > **注意:** 選択する範囲は、Tenable Kubernetes Cluster Connector の範囲と一致する必要があります。たとえば、AWS フォルダーにコネクタを追加した場合、そのコネクタはその範囲内でのみ選択できます。

3. 接続方法オプションから **[クラウド管理]** をクリックします。
4. **[Select Clusters] (クラスタの選択)** ステップで、テーブル内のターゲットクラスタを見つけます。[名前] または [アカウント] フィルターを使用して、リストを絞り込むことができます。
5. 接続する各クラスタの横にあるチェックボックスを選択します。

   > **注意:** この方法は通常、リソース **同期** ステータスが [アクセス許可なし] または [接続失敗] と表示されている検出されたクラスタに対して使用されます。

6. **[次へ]** をクリックして、[スクリプト] のステップに進みます。
7. 異なるクラウドアカウントでクラスタを選択した場合は、スクリプトウィンドウの上部にある関連するアカウントタブを選択します。アカウントごとに個別にスクリプトを実行する必要があります。

8. ローカルのターミナルまたはCloud Shell環境が次の要件を満たしていることを確認します。
    - クラウドプロバイダーCLIがインストールされ、アクティブなプロファイルまたはCloudShell経由で認証されます。
    - `kubectl`がインストールされています。
    - 認証されたアカウント/プロファイルには、接続しているターゲットKubernetesクラスタへの明示的な書き込み許可があります。
9. コンソールボックスに表示されている動的に生成されたbashスクリプトをコピーします。
10. ターミナルでローカルでスクリプトを実行するか、プロバイダーのクラウドシェルから直接スクリプトを実行し、Tenableとクラスタの間に安全な接続アクセスエントリを確立します。

高度なクラスター設定

特定の環境に合わせてHelmチャートのインストールをカスタマイズできます。ワークフローに最適な方法を選択してください。

- Helmのオプションのコマンドパラメーター(CLI) 1回限りの素早い変更や、初期インストール時の簡単なオーバーライド(クラスタ名やプロキシの設定など)に最適です。
- values.yamlファイル: 複雑な設定やバージョン管理されたデプロイメント、または詳細なリソース制限、アフィニティルール、セキュリティコンテキストを定義する必要がある場合に最適です。
- **プライベートレジストリ**: カスタムコンテナレジストリを使用する場合は、プライベートレジストリを持つクラスタを参照してください。
- カスタムCA証明書: コンポーネントがインスペクションプロキシまたは内部認証局を信頼できるようにTenable CA証明書を提供します。

Helmのオプションのコマンドパラメーター(CLI)

これらのパラメーターを`helm install`コマンドに追加して、設定をカスタマイズします。

パラメーター	説明	例
`--set name`	デフォルトの	`--set name="cluster1.mycompany.internal"`

パラメーター	説明	例
	クラスタ名 (DNS 名) をオーバーライドします。	
`--set accountId`	別のアカウント ID またはオンプレミスのデフォルトアカウント (`opDefault`) を選択することで、検出されたアカウントの場所をオーバーライドします。詳細については、「クラスタアカウントの場所を参照してください。	`--set accountId="123456789012"`、`--set accountId=opDefault`
`--set configureIdentity`、`--set configureNetwork`	デフォルトでは、Tenable はクラスタに接	`--set configureIdentity="false"`

パラメーター	説明	例
	続して、アイデンティティ関連のアクセスとネットワークベースのアクセスの両方を設定します。このデフォルトをオーバーライドし、これらの形式のアクセスの 1 つを無効にするには、必要に応じて、**次のいずれかを**コマンドに追加し、値を `false` に追加します。詳細については、「Tenable のクラスターへの接続方法」を参照してくださ	

パラメーター	説明	例
	い。	
`--set proxyUrl`	プロキシサーバーを使用して接続します。	• **認証なしの場合**: `--set proxyUrl="http://your-proxy:<port>"` • **認証あり** `--set proxyUrl="http://<username>:<password>@your-proxy:<port>"`

values.yaml ファイル

高度なユースケースでは、`values.yaml` ファイルを使用して設定をカスタマイズできます。

`values.yaml`ファイルを使用してクラスタを設定する方法

1. ファイルを取得します。
   `helm show values tenable/cloud-security-kubernetes-cluster`
2. 必要に応じて values.yaml ファイルを構成し、保存します。
3. ファイルを `helm install` コマンドに追加します。
   `helm install {...} -f custom-values.yaml`

   > **注意:** {...}は、[Add Clusters]ダイアログから動的に生成されたコマンドを表します。

共通 values.yaml パラメーター

`values.yaml` ファイルには次の共通するパラメーターが含まれています。

パラメーター	説明	デフォルト
アイデンティティ	デフォルトで	`true`

パラメーター	説明	デフォルト
	は、Tenable はクラスタに接続して アイデンティティアクセス を設定します。このデフォルトをオーバーライドしてアクセス権を無効にするには、`false` に変更します。	
ネットワーク	デフォルトでは、Tenable はクラスタに接続して ネットワークアクセス を設定します。このデフォルトをオーバーライドしてアクセス権を無効にするには、`false` に変更します。	`true`
レジストリ	デプロイメントに独自のコンテナイメージレジストリを使用す	`containers.tenable.com`

パラメーター	説明	デフォルト
	る場合は、このパラメーターを使用して設定できます。このパラメータは、すべてのコンポーネントに共通です。	
リポジトリ	デプロイメントに独自のコンテナイメージリポジトリを使用する場合は、このパラメーターを使用してパスを設定できます。このパラメーターは、各コンポーネントに対して個別に編集できます。	`cloud-security/kubernetes-cluster-manager`
アフィニティ	ラベルと条件に基づいて、Podをノードに割り当てるためのルールを定義します。	

パラメーター	説明	デフォルト
注釈	任意の非識別メタデータをポッドに添付するために使用されるキーと値のペア。	
ラベル	Podを識別および選択し、Pod間の関係を指定するために使用されるキーと値のペア。	
リソース	CPUやメモリなど、Podのコンピューティングリソースの要件と制限を指定します。	
tolerations	taintのあるノードにPodをスケジュールできる条件を指定します。	
resourceNamePrefix	Tenableによってクラスターで	`kubernetes-cluster`

パラメーター	説明	デフォルト
	作成された各リソースにカスタムプレフィックスを追加します。	
proxyUrl	プロキシサーバーを使用して接続します。	• **認証なし:** `proxyUrl: "http://your-proxy:<port>"` • **認証がある場合** `proxyUrl: "http://<username>:<password>@your-proxy:<port>"`
containerCaCertificate	インスペクションプロキシまたは内部認証局の背後にある環境で、すべてのTenableコンポーネントにカスタムCA証明書を提供します。pemを使用して証明書をインラインで設定するか、secretNameを使用して既存	

パラメーター	説明	デフォルト
	のクラスタシークレットを参照します。カスタムカスタムCA証明書を参照してください。	

アドミッションコントローラーのオプションのパラメーター

パラメーター	説明	デフォルト
webhook.port	Webhookがリッスンしているポート番号。クラスタ内でポートにアクセスできることを確認します。	8443
webhook.replicas	アドミッションコントローラーのポッドインスタンスの数。	3
readSecrets	アドミッションコントローラーにシークレットをリストするアクセス許可を付与します。これにより、脆弱なコンテナイメージポリシー用にデプロイされているコンテナイメージを識別できるようになります。アドミッションコントローラーは、イメージプルシークレットのみを調べます。`--set admissionController.readSecrets=true`で設定します。チャートバージョン1.1.6以降が必要です。	false

Values.YAML デフォルト値

YAML

```
accountId: null
admissionController:
  containerImage:
    repository: cloud-security/kubernetes-cluster-admission-controller
```

```
    tag: null
  enabled: false
  healthPort: 9090
  logLevel: "information"
  readSecrets: false
  networkPolicy:
    enabled: false
    ingress: {}
  pod:
    affinity: {}
    annotations: {}
    containers:
      securityContext: {}
    labels: {}
    resources:
      limits:
        cpu: "100m"
        memory: "256Mi"
      requests:
        cpu: "100m"
        memory: "256Mi"
    tolerations: []
  replicas: 3
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
  webhook:
    failurePolicy: Ignore
    port: 8443
    timeoutSeconds: 3
apiKeyToken: ""
apiUrl: ""
clusterId: null
connector:
  enabled: true
  identity: true
  network: true
  pod:
    affinity: {}
    annotations: {}
    containers:
      securityContext: {}
    labels: {}
    resources: {}
    tolerations: []
```

```
containerCaCertificate:
  pem: null
  secretName: null
containerEnvironmentVariables: []
containerImage:
  pullSecrets: []
  registry: containers.tenable.com
  registryPassword: null
  registryUsername: null
  repository: cloud-security/kubernetes-cluster-manager
  tag: null
containerSecrets:
  apiKeyTokenName: null
  injectExternally: false
  volumeMountPath: "/var/run/secrets/application"
hooks:
  pod:
    affinity: {}
    annotations: {}
    containers:
      securityContext: {}
    labels: {}
    resources: {}
    tolerations: []
name: null
pod:
  affinity: {}
  annotations: {}
  containers:
    securityContext:
      runAsUser: 1000
  labels: {}
  resources:
    limits:
      cpu: "100m"
      memory: "512Mi"
    requests:
      cpu: "100m"
      memory: "512Mi"
  tolerations: []
proxyUrl: null
resourceNamePrefix: kubernetes-cluster
sensor:
  containerImage:
    repository: cloud-security/kubernetes-cluster-sensor
    tag: null
```

```
    dataPath: "/var/lib/tenable"
    enabled: false
    pod:
      affinity: {}
      annotations: {}
      labels: {}
      resources:
        limits:
          cpu: "1"
          memory: "1Gi"
        requests:
          cpu: "300m"
          memory: "256Mi"
      tolerations: []
  updater:
    pod:
      affinity: {}
      annotations: {}
      containers:
        securityContext: {}
      labels: {}
      resources: {}
      tolerations: []
```

カスタムCA証明書

インスペクションプロキシ経由でトラフィックをルーティングする環境や、内部認証局に依存する環境では、カスタムCA証明書を提供して、Tenableコンポーネントが信頼できる接続を確立できるようにすることができます。Tenableは、デプロイされたコンポーネントにのみ証明書をインストールします。クラスター全体の信頼は変更されません。

values.yamlファイルのcontainerCaCertificateセクションで証明書を設定します。

YAML

```
  containerCaCertificate:
    pem: <CA certificate in PEM format>
    secretName: <name of an existing cluster secret that holds the certificate>
```

証明書をインラインでpemを指定するか、既存のクラスタシークレットをsecretNameで参照します。

コマンドラインから証明書を設定することもできます。

- `--set-file containerCaCertificate.pem=<path>`を使用して証明書ファイルを提供します。
- `--set containerCaCertificate.secretName=<name>`を使用して、既存のクラスタシークレットを参照します。

> **注意:** Helm 設定の長さが制限されているため、Tenable では、証明書がバンドルされている場合やサイズが大きい (200 KB を超える場合)、pem でインラインで埋め込むのではなく、`secretName` で証明書を参照することを推奨しています。

クラスタアカウントの場所

クラスタを追加すると、Tenable はクラスタがあるアカウントを検出しようとします。

- **接続されたクラウドアカウント**: 関連付けられているクラウドアカウントがすでに接続されている場合、クラスタはそのクラウドプロバイダーの関連するアカウント範囲 (フォルダー) に追加されます。
- **未接続のクラウドアカウント**: 関連付けられているクラウドアカウントが接続されていない場合、Tenable はワーカーノードのアカウントに基づいて場所の特定を試みます。
- **手動関連付け:** アカウントを検出できない場合 Tenable、クラスタを別の接続済みアカウントまたはオンプレミスのデフォルトアカウントに関連付けることができます。これを行うには、Helm コマンドの設定中にドロップダウンメニューからアカウントを選択するか、Helm コマンドを設定して実行するコマンドの `--set accountId` パラメーターを使用します。

  > **注意:** 通常、オンプレミスのデフォルトアカウントに追加されたクラスタはオンプレミスですが、他のアカウントが検出されない場合は、他のタイプのクラスタもこのフォルダーにマッピングされることがあります。

検出されたアカウントの場所をオーバーライドすると、Tenable は定義したアカウント範囲にクラスタを追加します。パラメーターを使用して場所をオーバーライドする方法の詳細については、Helm のオプションのコマンドパラメーターを参照してください。

Helm チャートのトラブルシューティング

このガイドでは、Tenable Kubernetes Helm チャートのデプロイ中によく発生する一般的な問題について説明します。

ここから開始:

- ターミナルでエラーが発生して `helm install` 終了した場合は、「helm install fails」を参照してください。
- コマンドが完了したがクラスタが欠落している、または間違ったアカウントで表示されている場合は、「helm install succeeds but something is wrong」を参照してください。
- デプロイが成功した後にポッドがクラッシュしている場合、または接続が切断された場合は、「デプロイ後にポッドが失敗する、または接続が切断される」を参照してください。

helm のインストールが失敗する

これらのエラーは `helm install` 中に発生します。プレインストールフック (チャートのデプロイ中に実行される検証ジョブ) を完了できないか、指定されたアカウントの詳細が正しくないために、コマンドがターミナルで失敗します。

インストール前フックの失敗 (プロキシ/ネットワークのブロック)

症状: `helm install` コマンドが失敗し、タイムアウトまたはフックが失敗したことを示すエラーが表示されます。

端末出力:

```
Error: UPGRADE FAILED: pre-upgrade hooks failed: 1 error occurred: job kubernetes-cluster-pre-install-job
failed: BackoffLimitExceeded
```

診断: 失敗したジョブのログを調べて、原因を特定します。

> **注意:** Pod 名には、ランダムなサフィックス (例: `kubernetes-cluster-pre-install-job-vkknz`) が付きます。

1. 正確なポッド名を見つけます。

   ```
   kubectl get pods -n <your-namespace>
   ```

2. ログを確認します。

```
kubectl logs job/kubernetes-cluster-pre-install-job-<suffix> -n <your-namespace>
```

ログエラーを探す:

```
System.Net.Http.HttpRequestException
```

原因: これは、ネットワークが詰まる可能性があることを示します。企業のプロキシ、ファイアウォール、ディープパケット検査ツールがTenableのバックエンド(`app.tenable.com`)への接続を傍受しているか、ポッドがプロキシ経由で内部Kubernetes APIトラフィックをルーティングしようとしています。

解決策

- **プロキシの設定** `values.yaml`で、`proxyUrl`が正しく設定されていることを確認します。Helm のオプションのコマンドパラメーター (CLI) を参照してください。
- **設定NO_PROXY:** Kubernetes API サーバードメイン (例: `kubernetes.default.svc`) を含めるように`NO_PROXY` 環境変数を設定する必要があります。これがない場合、ジョブはプロキシを介してローカル API へのアクセスを試みますが、失敗します。

> **注意:** `NO_PROXY`設定していない場合、インストール前ジョブは内部 Kubernetes APIトラフィックを企業プロキシ経由でルーティングし、失敗します。これは、プロキシ環境におけるフック障害の最も一般的な原因です。

JSON

```
"containerEnvironmentVariables": [
  {
    "name": "NO_PROXY",
    "value": "kubernetes.default.svc,10.0.0.0/8,.svc.cluster.local"
  }
]
```

イメージプルの失敗(403 Forbidden)

症状:`helm install`がハングするか、ポッドがステータス`ImagePullBackOff`または`ErrImagePull`で失敗します。

イベント出力: `Failed to pull image... 403 Forbidden`

原因:

- **ファイアウォール:** 企業のファイアウォールがパブリックレジストリcontainers.tenable.comへのアクセスをブロックしています。
- **キャッシング:** Helm クライアントが、サポートされている最新バージョンではなく、古いチャートバージョン (1.1.2 など) をローカルキャッシュから抽出しようとしています。

解決策

- リポジトリ**の更新:**`helm repo update tenable`を実行して、クライアントに最新のタグを強制的にフェッチさせます。
- **テスト接続:** クラスター内のノードまたはポッドから `wget` または `curl -v https://containers.tenable.com` を実行して、到達可能性を確認します。
- **プライベートレジストリ:** クラスタがエアギャップされている場合は、イメージをプライベートレジストリにミラーリングし、`values.yaml`の`registry`、`registryUsername`、`registryPassword`値を更新します。プライベート プライベートレジストリを持つクラスタを参照してください。

アカウント検証の失敗 (TenantNotExist)

症状:`helm install`は`BackoffLimitExceeded`で失敗しますが、ジョブログはネットワーク例外ではなく論理エラーを明らかにします。

ログエラー:

```
Failure { ... httpResponseMessageContent="TenantNotExist" ... }
```

原因: Helm コマンドで指定された `accountId` が正しくないか、インストールを実行する前にターゲットのクラウドアカウントが Tenable One Cloud Exposure にオンボーディング (接続) されていません。

解決策

- **オンボーディングファースト** クラウドアカウント (AWS/Azure/GCP) が Tenable コンソールで完全に接続されていることを確認します。

- **ID の検証:** オンプレミスクラスタにインストールする場合は、**[Kubernetes クラスタ (エージェント)]** ウィザードでアカウント ID を検証し、明示的に渡します。`--set accountId=<ID>`。

helm のインストールは成功するが、何か問題がある

これらのエラーは、`helm install` が正常に完了した後に表示されます。クラスタが間違ったアカウント範囲に関連付けられているか、リソースがダッシュボードに入力されていません。

間違ったアカウントに関連付けられたクラスタ

症状: Helm チャートは正常にインストールされますが、クラスタは特定のクラウドアカウント範囲 (AWS/Azure など) ではなく、**オンプレミスのデフォルトアカウント** の下に表示されます。

原因: Tenable がクラウドプロバイダーを自動的に検出します。Helm をインストールする前にクラウドアカウントが Tenable と統合されていない場合、システムはデフォルトでオンプレミスの範囲になります。「クラスタアカウントの場所を参照してください。

解決策: アカウント間でライブクラスタを移動することはできません。再インストールが必要です。

1. `helm uninstall tenable-cloud-security-kubernetes-cluster -n <namespace>`を実行してください。
2. クラウドアカウントが Tenable ユーザーインターフェースで接続されていることを確認します。
3. `helm install`を再実行してください。

リソース同期のハングアップ

症状: インストールは成功しますが、ダッシュボードにリソースは表示されません。ログに「リージョンのクエリに失敗しました」と表示される場合があります。

原因: ターゲットテナントまたはアカウントが Tenable バックエンドで無効になっているため、リージョンのクエリができません。

解決策: Tenable プラットフォーム設定でアカウントステータスを確認し、テナントが有効になっていることを確認します。

デプロイ後にポッドが失敗する、または接続が切断される

これらの問題は、インストールコマンドが成功した後に発生します。Helm が「デプロイ済み」と報告されていても、コンポーネントが接続に失敗したり、クラッシュしたりする可能性があります。

コネクタ Pod のエラーとリバーストンネルの障害

症状: Tenable コンソールの状態が **[接続失敗]** です。

診断: Helm が成功した場合でも、コネクタポッドが実行されていることを確認し、そのログを確認してください。

1. ステータスの確認:

```
kubectl get pods -l app.kubernetes.io/name=kubernetes-cluster-connector -n <namespace>
```

2. ログのチェック

```
kubectl logs -l app.kubernetes.io/name=kubernetes-cluster-connector -n <namespace>
```

特定のチェック (トンネル): ポッドがトンネルエンドポイントに到達できないことを示すエラー (例: `us1-tunnel.internal.app.tenable.com` や `connect to server error`) を探します。コネクタには、API (`app.tenable.com`) と専用トンネルエンドポイントの両方にアクセスする必要があります。

原因:

- **ゾンビトンネル:** バックエンドは、Kubernetes API へのリバーストンネルを確立できませんでした。
- **Duplicate Install:** コネクタの 2 つの同時インストール (たとえば異なる名前空間) により、競合が発生しています。

解決策

- **ポッドを再起動:** コネクタポッドを削除して強制的に再起動し、トンネルハンドシェイクを再開します。

```
kubectl delete pod -l app.kubernetes.io/name=kubernetes-cluster-connector -n <namespace>
```

注意: 通常これにより、同期ステータスがすぐに解決されます。

- **複数のインストールのチェック:** 次のコマンドを使用して、異なる名前空間に同一のデプロイがないかチェックします。

```
kubectl get pod -l app.kubernetes.io/name=kubernetes-cluster-connector -A
```

センサーのアクセス許可拒否 (PSS)

症状: センサーポッド (DaemonSet) が起動に失敗する、クラッシュする、またはログにアクセス許可エラーが表示される。

原因: センサーには、ノードをスキャンするために特権アクセス (`hostPID: true`、`privileged: true`、`hostPath` マウント) が必要です。クラスタの Pod Security Standards (PSS) がこれらのアクセス許可をブロックしています。

解決策: 制限ポリシーから Tenable 名前空間を除外します。

```
kubectl label namespace <namespace> pod-security.kubernetes.io/enforce=privileged
```

注意: コネクタ (リソース同期) とアドミッションコントローラーは、特権ステータスを必要としません。センサーのみが知ることができます。

循環的再起動 (オンプレミス)

症状: オンプレミスクラスタ内のノードは、センサーのインストール後に再起動ループに入ります。

原因: Tenable センサー (eBPF プローブ) と特定の OS/カーネルバージョン間の非互換性。

解決策: センサーを直ちに無効にし、カーネルログを Tenable サポートに連絡してください。

```
helm upgrade tenable-cloud-security-kubernetes-cluster tenable/tenable-cloud-security-kubernetes-cluster --
--set sensor.enabled=false
```

プライベートレジストリを持つクラスタ

Tenable は、新規インストールやアップグレードにプライベートレジストリを使用する Kubernetes 環境をサポートしています。この設定を使用するには、以下の手順に従って Tenable リポジトリをミラーし、内部レジストリを使用して Helm チャートをインストールします。

プライベートレジストリを使用するクラスタを追加するには

1. **レジストリ認証情報の取得**: レジストリ設定パラメーターを取得します。「Tenable コンポーネントリポジトリへのアクセスを参照してください。
2. **Tenableリポジトリにアクセスする:** 取得したパラメーターを使用して、`containers.tenable.com` でコンポーネントリポジトリにアクセスします。
3. **ミラーリングの設定**: プライベートレジストリを、ミラーリングするか、Tenable リポジトリからプルスルーするように設定します。
4. **セキュリティデータの同期**: 最新のイメージをプライベートレジストリに取り込みます。

ミラーリングまたはプルスルーを設定した後、デフォルトのレジストリ設定を独自のレジストリ値でオーバーライドします。これらは values.yaml ファイルで更新するか、次のパラメーターを使用して `helm install` または `helm upgrade` コマンド中に明示的に指定できます。

- `--set containerImage.registry`
- `--set containerImage.registryUsername`
- `--set containerImage.registryPassword`

Tenable コンポーネントリポジトリへのアクセス

Tenable レジストリ設定パラメーター

パラメーター	デフォルト値	注記
containerImage.registry	`containers.tenable.com`	
containerImage.registryUsername		アップグレードウィザードの 2 つ目のステップに表示される

パラメーター	デフォルト値	注記
		`helm upgrade` コマンドで提供されます。
containerImage.registryPassword		アップグレードウィザードの 2 つ目のステップに表示される `helm upgrade` コマンドで提供されます。

新しい Chart バージョンにアップグレードする

Tenable が新しい Helm チャートバージョンをリリースしても、プライベートレジストリ環境は自動的に更新されません。アップグレードするには:

1. `containers.tenable.com`からミラーリングするかプルスルーを設定して、プライベートレジストリで最新の Tenable [エージェント] イメージを利用できるようにします。「Tenable コンポーネントリポジトリへのアクセスを参照してください。
2. 最新の Helm チャートを `https://charts.tenable.com` から内部リポジトリに取り込み、デプロイするチャートバージョンを固定します。
3. レジストリオーバーライド値 `containerImage.registry`、`containerImage.registryUsername`、`containerImage.registryPassword` を使用して `helm upgrade`を実行します。

> **注意:** パブリックリポジトリ (`https://charts.tenable.com`) に対して `helm repo update tenable` を実行しないでください。プライベートレジストリ環境では、内部リポジトリからチャートをインストールします。

GitOps ツールによる Helm チャートのデプロイメント

GitOps フレームワークを使用して Kubernetes クラスタを管理している場合は、手動の`helm install`コマンドを実行する代わりに、業界標準のツールを使用して Tenable One Cloud Exposure Helm チャートを簡単にデプロイおよび管理できます。

Git リポジトリを信頼できる唯一の情報源として確立することで、GitOps ツールはクラスタを希望する設定と自動的に同期し、手動による設定のドリフトを防ぎ、Git バージョン管理履歴を使用して Helm チャートのバージョン管理とパラメーターを簡単に追跡できるようにします。

Tenable は、Helm チャートのデプロイメントを管理するために Flux と Argo CD セットアップ の両方をサポートしています。

フラックスセットアップ

Fluxは、カスタムKubernetesリソース(`HelmRepository`、`HelmRelease`、`Kustomization`)に基づくモジュラー構成スタイルを利用して、Gitリポジトリから直接更新プログラムをプルします。

フラックスの初期化

Helm チャートをデプロイする前に、Flux がインストールされ、クラスタ環境に対して適切に設定されていることを確認してください。Flux 入門ガイドの公式実装手順に従うことができます。

リポジトリのレイアウトを設定する

クラウドサイバーエクスポージャー Helm チャートをデプロイするには、次のディレクトリレイアウトを使用して Git リポジトリ内のファイルを整理します。

```
./clusters/my-cluster/
  tenable-sync.yaml        # Flux Kustomization (The entry point)
./apps/tenable/
  kustomization.yaml       # Grouping all the files together
  tenable-repo.yaml        # HelmRepository source definition
  tenable-release.yaml     # HelmRelease deployment configuration
  tenable-secrets.yaml     # Kubernetes Secret for sensitive tokens
```

設定マニフェストの追加

Git リポジトリで、次の YAML ファイルをアプリケーションディレクトリ (`./apps/tenable/`) 内に追加します。

tenable-repo.yaml

このマニフェストは、Flux が公式 クラウド サイバーエクスポージャー Helm チャートをどこでフェッチするかを定義します。

YAML

```
apiVersion: source.toolkit.fluxcd.io/v1
kind: HelmRepository
metadata:
  name: tenable
  namespace: tenable-cloud-security-kubernetes-cluster
spec:
  interval: 1h
  url: https://charts.tenable.com/
```

tenable-release.yaml

これには、デプロイメントの手順が含まれています。クラウド サイバーエクスポージャー チャート バージョンがリンクされ、カスタムパブリック値がマッピングされ、プライベート認証値がシークレット ファイルから Helm チャートにバインドされます。

YAML

```
apiVersion: helm.toolkit.fluxcd.io/v2
kind: HelmRelease
metadata:
  name: tenable-cloud-security-kubernetes-cluster
  namespace: tenable-cloud-security-kubernetes-cluster
spec:
  interval: 1h
  install:
    createNamespace: true
  chart:
    spec:
      chart: cloud-security-kubernetes-cluster
      version: '>=1.0.0'
```

```
      sourceRef:
        kind: HelmRepository
        name: tenable
        namespace: flux-system
  values:
    apiUrl: "{}"
    containerImage:
      registryUsername: "{}"
  valuesFrom:
    - kind: Secret
      name: tenable-cloud-security-secrets
      valuesKey: apiKeyToken
      targetPath: apiKeyToken
    - kind: Secret
      name: tenable-cloud-security-secrets
      valuesKey: registryPassword
      targetPath: containerImage.registryPassword
```

tenable-secrets.yaml

このマニフェストには、Helm チャートの機密トークンと認証データが格納されています。これらの値を適用する前に、必ず Base64 でエンコードしてください。

YAML

```
apiVersion: v1
kind: Secret
metadata:
  name: tenable-cloud-security-secrets
  namespace: tenable-cloud-security-kubernetes-cluster
type: Opaque
data:
  apiKeyToken: {}
  registryPassword: {}
```

kustomization.yaml

このファイルは、Kubernetes マニフェストをバンドルするために同じ `./apps/tenable/` ディレクトリに存在する必要があります。

YAML

```yaml
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
resources:
  - tenable-repo.yaml
  - tenable-secrets.yaml
  - tenable-release.yaml
```

エントリポイントの作成

クラスタ設定パス (`./clusters/my-cluster/tenable-sync.yaml`) でエントリポイントマニフェストを作成します。これにより、Helm チャートを実行するためにどのフォルダーをモニタリングおよび同期するべきかが Flux に通知されます。

YAML

```yaml
apiVersion: kustomize.toolkit.fluxcd.io/v1
kind: Kustomization
metadata:
  name: tenable-app
  namespace: flux-system
spec:
  interval: 10m
  path: ./apps/tenable
  prune: true
  sourceRef:
    kind: GitRepository
    name: flux-system
```

Argo CD セットアップ

Argo CD は、統一されたアプリケーションカスタムリソース定義 (CRD) を介して Helm チャートの管理を直接処理し、Helm チャートのデプロイの状態を追跡するための一元化された Web ダッシュボードを提供します。

Argo CD のインストール

Argo CD をクラスタにインストールするには、公式の Helm リポジトリコマンドを使用できます。

Bash

```
# Add the official Argo Helm repository
helm repo add argo https://argoproj.github.io/argo-helm

# Install Argo CD into its own namespace
helm install argo-cd argo/argo-cd --namespace argocd --create-namespace

# Make sure all platform pods are running successfully
kubectl get pods -n argocd
```

便利な Argo CD アクション

以下で概説するアクションを使用して、コマンドラインからクラウドサイバーエクスポージャー Helm チャートの状態を追跡、監視、維持できます。

Argo CD アプリケーションマニフェスト

Helm チャートをデプロイするには、`Application` マニフェストと呼ばれる YAML 形式の設定ファイルを作成する必要があります。このマニフェストは、Argo CD に対して Tenable Helm リポジトリをモニタリングし、特定のクラスタパラメーターに基づいてそのコンポーネントをデプロイするように指示します。

この YAML 設定ファイルを保存し、追跡対象の Git リポジトリに直接コミットする必要があります。

次の設定を`Application.yaml`として保存します。

YAML

```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: tenable-cloud-security
  namespace: argocd
spec:
  project: default
  source:
    repoURL: https://charts.tenable.com
    chart: cloud-security-kubernetes-cluster
    targetRevision: "1.1.0" # The CHART VERSION you need to run (fetch via: helm search repo tenable)
    helm:
      parameters:
```

```
        - name: apiKeyToken
          value: ""
        - name: apiUrl
          value: ""
        - name: containerImage.registryUsername
          value: ""
        - name: containerImage.registryPassword
          value: ""
        - name: name
          value: "cluster"
        - name: containerImage.registry
          value: ""
  destination:
    server: https://kubernetes.default.svc
    namespace:       # The target deployment namespace for the Tenable sensor
  syncPolicy:
    automated:
      selfHeal: true # Automatically reverts manual cluster modifications back to the Git state
      prune: true    # Automatically removes resources deleted from your config
```

アプリケーションマニフェストの適用

次のコマンドを実行してアプリケーションマニフェストを登録し、Argo CD内のアプリケーショントラッキングを初期化します。

Bash

```
kubectl apply -f Application.yaml
```

> **注意:** Helm チャートのデプロイメントのライフサイクルは、Argo CD によってアクティブに管理され、内部的にレンダリングされます。結果として、`helm list -A` などのローカルターミナルコマンドを実行する場合、リストされたデプロイメントは表示されません。

アプリケーションステータスの確認

このコマンドを実行して、管理対象アプリケーションの大まかな動作ステータス (実行中、保留中、デグレード状態など) をチェックします。

Bash

```
kubectl get applications -n argocd
```

Helm チャートオーケストレーションの詳細を表示する

次のコマンドを実行すると、ライブ同期イベント、ターゲットリビジョンステータス、Helm チャートの詳細ログ設定が表示されます。

```
Bash

kubectl アプリケーションを説明します tenable-cloud-security -n argocd
```

アプリケーションを削除する

次のコマンドを実行してアプリケーション設定を削除し、実行中の Helm チャートリソースをターゲットクラスタから引き出します。

```
Bash

kubectl delete application tenable-cloud-security -n argocd
```

複数のクラウドマネージド Kubernetes クラスタの接続

Tenable では、クラウドプロバイダー API ワークフローを使用して、クラウドマネージドの Kubernetes クラスタをすばやく接続できます。個々のクラスタ内で専用のスクリプトを実行する必要がある Helm ベースのインストールとは異なり、クラウドマネージド方式では、クラウドアカウントごとに 1 つの統一されたスクリプトを生成し、その範囲内で選択したすべてのクラスタに適用されることで、オンボーディングを効率化します。

この方法を使用すると、クラスタコントロールプレーン内にセンサーをインストールせずに、リソース同期とクラウドネイティブの可視性を確立できます。

> **注意:** この接続方法は、現在 OCI クラスタではサポートされていません。

要件

生成された設定スクリプトを実行する前に、環境が次の要件を満たしていることを確認してください。

- **Cloud CLI ツール**: 関連するクラウドプロバイダー CLI がインストールされ、アクティブなプロファイルで認証されているか、プロバイダーのウェブベースのクラウドシェルにアクセスできます。
- **Kubectl**:`kubectl` コマンドラインツールは、ローカルマシンまたはスクリプトを実行するターミナル環境にインストールする必要があります。
- **パーミッション**: スクリプトの実行に使用する認証済みクラウドプロファイルまたはユーザーアカウントには、対象の Kubernetes クラスタへの明示的な書き込みアクセス許可が必要です。
  - **AWS EKS**: 組織の範囲でのリソース作成アクセス許可が必要です。
  - **Azure AKS**: スクリプトに含まれるすべてのクラスタに対する書き込みアクセス許可が必要です。

    詳細については、「Amazon EKS クラスタの接続」および「Azure AKS クラスタの接続を参照してください。

クラスターを追加する

クラウドマネージドクラスタを追加する方法

1. Tenable One Cloud Exposure コンソールで、**[Explore > Kubernetes Clusters]** に移動します。
2. *(オプション)* 組織ツリーで、アカウントの範囲を選択します。デフォルトでは、コンソールは組織全体 (すべてのアカウント) を選択します。
3. 接続方法のオプションから **[エージェントレス]** を選択します。これにより、クラスタ選択画面が開き、オンボーディングできる検出されたクラスタのみが表示されます。
4. **[Select Clusters] (クラスタの選択)** 画面で、インベントリテーブルでターゲットクラスタを見つけます。

   > **注意**: [名前] または [アカウント] フィルターを使用すると、リストを素早く絞り込むことができます。

5. 接続する各クラスタの横にあるチェックボックスを選択します。
6. **[次へ]** をクリックして、[スクリプト] 画面に進 ***みます*** 。
7. スクリプトウィンドウの上部で、関連するクラウドアカウントタブを選択します。Tenable は、その特定のアカウント内で選択されたすべてのクラスタの設定を含む、単一の bash スクリプトを作成します。

> **注意:** 複数の異なるクラウドアカウントでクラスタを選択した場合は、各アカウントタブを選択し、対応するスクリプトを個別に実行する必要があります。

8. コンソールウィンドウに表示されている動的に生成されたbashスクリプトをコピーします。
9. ターミナルまたは Cloud Shell インターフェースを開き、コピーしたスクリプトを実行します。

このスクリプトは、必要な安全なクラウドアクセスエントリを設定し、Tenable そのクラウドアカウント内の指定されたすべてのクラスタ間で自動リソース同期を確立できるようにします。

> **注意:** スクリプトが正常に実行されると、クラウドサイバーエクスポージャーコンソールで接続ステータスが **[接続済み]** に更新されるまでに最大 10 分かかることがあります。

チケッティングと ITSM

Azure Boards

Azure Boards 組織を Tenable One Cloud Exposure と統合して、Tenable の特定の検出結果に関連する作業項目の作成をサポートします。

次の手順

- 検出結果のワークアイテムの作成を開始するには、自動化を設定するか、ツールと統合した後検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

始める前に

Tenable は、Microsoft Entra ID アプリケーション、**クラウドサイバーエクスポージャー Azure Boards コネクタを介して Azure Boards** に対して認証を行います。すでに Tenable に接続した Microsoft Entra ID 統合を再利用することも、セットアップ中に新しい統合接続することもできます。

ウィザードを開始する前に、次のことを確認してください。

- **既存の Microsoft Entra ID 統合 (推奨)、または統合を追加できること。** Tenable は、既存の統合がある場合は再利用することを推奨しています。
- **Microsoft Entra ID のグローバル管理者またはアプリケーション管理者のロール。** コネクタアプリケーションのサービスプリンシパルを作成するデプロイメントスクリプトを実行するには、これらのロールのいずれかが必要です。
- **Azure DevOps 組織にユーザーを追加するアクセス許可。** これは、後ほどウィザードでコネクタのサービスプリンシパルに組織へのアクセス権を付与するために必要になります。

組織の追加

前提条件を完了したら、クラウドサイバーエクスポージャーコンソールから Azure Boards 組織を追加します。

新しい組織を追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. (オプション)[Organization] (組織) ドロップダウンで、アカウント範囲を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで、**[Azure Boards]** をクリックします。[Azure Boards の追加] ウィザードが開きます。
5. Microsoft Entra ID の設定 (ウィザードのステップ 1):
    1. **[Microsoft Entra ID]** で、**[既存の Microsoft Entra ID 統合を使用する]** を選択し、ドロップダウンから統合を選択するか、**+ 追加** をクリックして新しい統合を接続します。または、**[Microsoft Entra ID 統合を使用しない** (非推奨)] を選択します。
    2. **[アクセスの検証]** で、**[確認]** をクリックして Microsoft Entra ID にサインインし、アクセスを確認します。
    3. **[デプロイ]** で、提供された PowerShell スクリプトをコピーします。
    4. [使用している Azure 環境]Azure 環境で PowerShell スクリプトを実行します。このスクリプトは、**クラウドサイバーエクスポージャー Azure Boards コネクタ** アプリケーションのサービスプリンシパルを作成します (まだ存在しない場合)。

> **必要なクラウドサイバーエクスポージャーユーザーロール:** スクリプトを実行するには、Microsoft Entra ID で **グローバル管理者** または **アプリケーション管理者** のロールが必要です。

5. **[次へ]** をクリックします。

6. Azure DevOps ポータルで組織のアクセス許可を付与します (ウィザードのステップ 2)。
7. **[次へ]** をクリックします。
8. ドロップダウン (ウィザードのステップ 3) から Azure DevOps 組織を選択し、**[完了]** をクリックします。統合プロファイルが開き、**[プロジェクト]** タブがアクティブになります。

組織が正常に追加されると、Settings > 統合 > Azure Boards のテーブルに表示されます。

> **重要:** 検出結果のワークアイテムの作成を開始するには、自動化を設定するか、ツールと統合した後 検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

組織アクセス許可を付与

組織にアクセス許可を付与するには:

1. Azure DevOps にログインし、追加する組織を選択して、左下の **[組織の設定]** をクリックします。
2. **[一般 > ユーザー]** に移動し、**[ユーザーの追加]** をクリックします。
3. 次のユーザーの詳細を入力します。
    1. ユーザーまたはサービスプリンシパル: **クラウドサイバーエクスポージャー Azure Boards コネクタ** を選択し、オブジェクト ID が含まれているサービスプリンシパルを必ずクリックします。
    2. アクセスレベル: **[基本]** を選択します。
    3. プロジェクトに追加: Tenableで使用するプロジェクトを選択します。
    4. Azure DevOps グループ: **[プロジェクト共同作成者]** を選択します。
    5. **[Add]** (追加) をクリックします。

プロジェクトの追加

Azure Boards プロジェクトを追加する前に、まず Azure Boards 組織を追加する必要があります。

Azure Boards プロジェクトを追加するには:

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > 統合]** に移動し、追加した関連する Azure Boards 組織を見つけます。
2. 組織名の横にある三点リーダーをクリックし、**[プロジェクトの追加]** をクリックします。[プロジェクトを追加] ウィザードが開きます。

   > **注意: [プロジェクト]** ドロップダウンには、**クラウドサイバーエクスポージャー Azure Boards コネクタ** アプリがすでにメンバーである Azure DevOps プロジェクトのみが一覧表示されます。目的のプロジェクトがリストにない場合は、**[プロジェクトに追加]** の 組織の追加 に追加します。

3. プロジェクトをアクティブ化します (ウィザードのステップ 1):
   1. ドロップダウンから追加するAzure Boardsプロジェクトを選択します。

      > **注意:** プロジェクトがドロップダウンに表示されない場合は、組織アクセス許可を付与して Azure DevOps に追加します。

   2. **[次へ]** をクリックします。
4. 作業項目の優先度を同期して、Tenable の検出結果の深刻度を Azure Boards の対応する優先度と一致させます (ウィザードの手順 2)。Tenable 経由で作成された Azure Boards 作業項目には、選択した優先順位が割り当てられます。作業項目の種類 (バグ、タスク、ストーリー、組織で定義されているカスタムの種類) ごとに、**検出結果の深刻度** を Azure Boards の既定の優先順位フィールドである **[優先度]** フィールドの値に割り当てます。完了したら、**[次へ]** をクリックします。
5. 作業項目の状態を同期して、Tenable の検出結果の状態を Azure Boards の対応する状態に合わせます (ウィザードの手順 3)。Tenable 経由で作成された Azure Boards 作業項目には、選択した状態が割り当てられます。作業項目の種類ごとに、Azure Boardsの必須フィールドである **[状態]** フィールドの値に**検出結果の状態**を割り当てます。**[終了]** をクリックします。

プロジェクトが正常に追加されると、Azure Boards Settings > 統合の表>表示されます。

検出結果のAzure Boards作業項目の詳細

検出結果を Azure Boards 作業項目にリンクした後、検出結果テーブルのチケット アイコンにカーソルを合わせると、**プロジェクト**、**作業項目の種類**、**ID**、および作業項目へのリンクが表示されます。

作業項目の更新を同期する

Tenable 検出結果の変更に応じて、リンクされた Azure Boards 作業項目を最新の状態に保ちます。

- **状態と深刻度は、**プロジェクトの追加 で構成したマッピングに基づいて、Tenable から Azure Boards に自動的に更新されます。
- **担当者は**、Tenable と Azure Boards の間で双方向に同期します。Tenable は、Azure Boards で行われた他のフィールドの変更を検出結果に同期しません。

たとえば、構成が無効なために、統合で作業項目を更新できない場合、Tenable は、Jira の場合と同じ方法で、失敗の表示と理由でプロジェクトの状態にフラグを立てます。

サポートされている作業項目の種類とフィールド

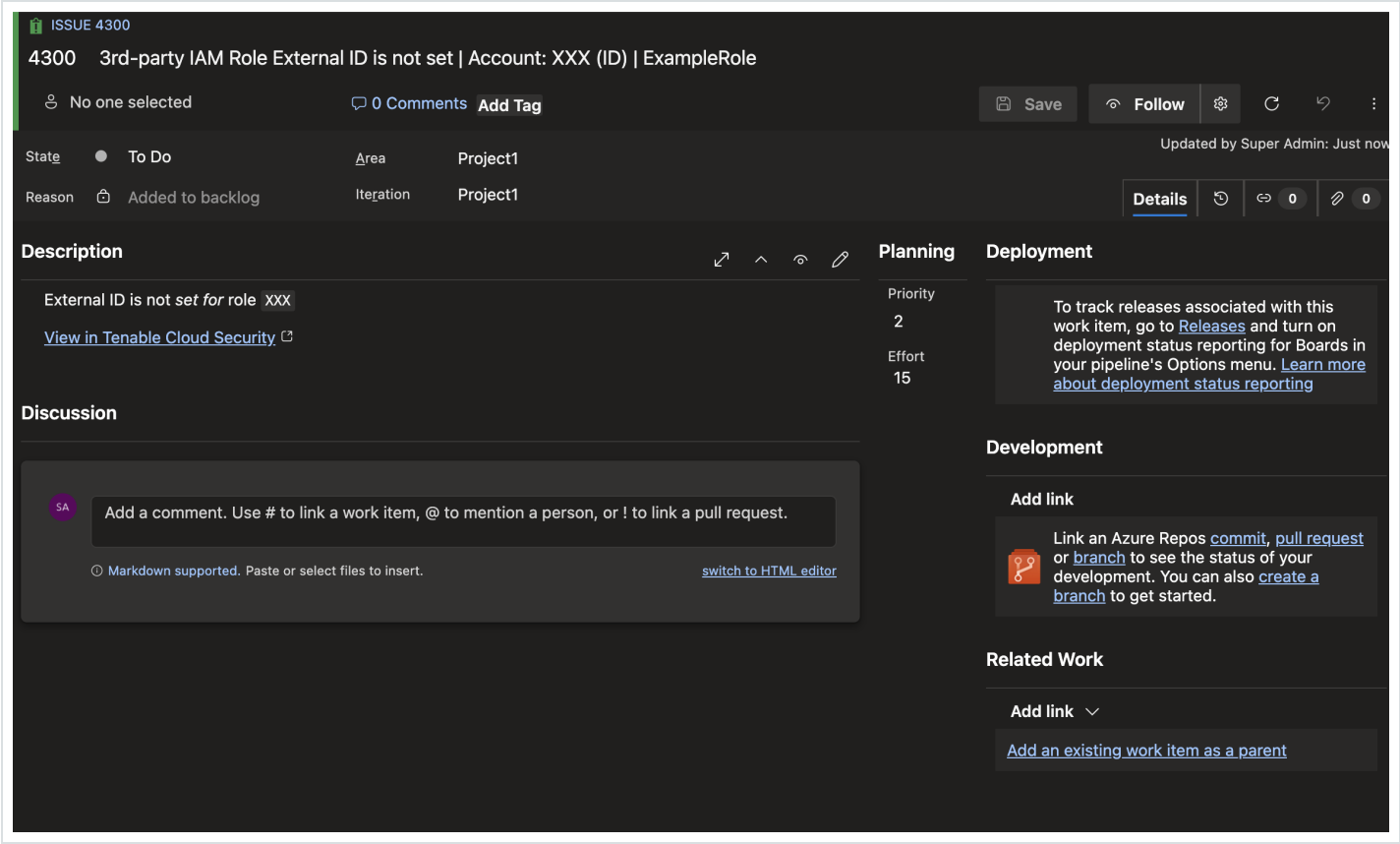
Tenable は、作業項目を作成および同期するときに、次の Azure Boards 作業項目の種類とフィールドをサポートします。

- **作業項目の種類。** すべての組み込みの種類 (ユーザーストーリー、バグ、タスク、エピックなど) と、組織で定義されているカスタム作業項目の種類。
- **標準フィールド。** タイトル、説明、イテレーション、エリア、優先度、担当者、工数、タグ (タグの作成を含む)。
- **カスタムフィールド。** サポートされているフィールドタイプにマッピングされるカスタムフィールド。
- **フィールドタイプ。** 文字列、整数、double、ブーリアン値、日付と時刻、および選択リスト (1 つの選択した値)。

以下はサポートされていません。

- **作業項目のリンク。** 親子リンクおよび関連するリンク。
- **コラボレーションと歴史。** コメント、ディスカッションスレッド、改訂履歴。
- **専門分野。** 担当者以外のアイデンティティ**フィールド**、**依存**フィールド、サードパーティ拡張機能によって生成されたフィールド。

Azure Boards 作業項目のサンプル



Jira

Jiraプロジェクトを Tenable One Cloud Exposure と統合し、Tenableの特定の検出結果に関連する課題を作成できるようにします。Tenable は、Jira Software (オンプレミス、バージョン 8.5.3 以降) および Jira Software Cloud の両方との統合をサポートしています。

プロジェクトを Tenable と統合するには、以下のことを行う必要があります。

1. Jira インスタンスの追加 - OAuth、パスワードまたは API トークン、またはパーソナルアクセストークンを使用して、Jiraインスタンスを Tenable に接続します。管理者ユーザーである必要があります。
2. Jira スペースの追加 - 専任 Tenable ユーザーにプロジェクトへのアクセス許可を付与して、1 つ以上のJiraプロジェクトを Tenable と統合します。

次の手順

- 検出結果の課題の作成を開始するには、自動化を設定するか、ツールと統合した後 検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

始める前に

Jira インスタンスを クラウド サイバーエクスポージャー に追加するには、専用の Jira ID と、次の 3 つの認証方法のいずれかが必要です。

- OAuth 2.0
- パスワードまたは API トークン
- 個人アクセストークン (PAT)

Tenable は OAuth を推奨しています。既存のJiraユーザーを使用することもできますが、監査証跡アクティビティを簡素化するために、Tenable では専用ユーザーまたはサービスアカウントを作成することを推奨しています。後日必要に応じて、Jira アイデンティティを削除して統合を終了できます。

ウィザードを開始する前に、Jira で選択した認証方法の設定を完了します。

OAuth 2.0 認証情報の設定

Jira サービスアカウントの OAuth 2.0 認証情報を作成します。統合はそのサービスアカウントとして実行され、認証情報を付与した範囲を継承します。サービスアカウントをまだお持ちでない場合は、まず作成してください。詳細は、Atlassian のドキュメントを参照してください。

OAuth 2.0 認証情報を作成する方法

1. Atlassian Administration で、組織を選択します (複数の組織がある場合)。
2. **[ディレクトリ > サービスアカウント]** に移動します。
3. 認証情報を作成するサービスアカウントを選択します。
4. **[認証情報の作成]** をクリックします。
5. **[OAuth 2.0]** を選択し、**[次へ]** をクリックします。

6. 以下の範囲を選択して、認証情報がJiraでできることを決定します。
    - `write:jira-work`
    - `read:jira-work`
    - `read:jira-user`
    - `read:priority:jira`
7. **[次へ]** をクリックします。
8. OAuth情報を確認し、**[作成]** をクリックします。
9. **クライアント ID** と**クライアントシークレット**をコピーします。

> **重要:** 認証情報を作成した後に、クライアント ID およびクライアントシークレットを回復することはできません。Tenable では、それらをパスワードマネージャーに保存することをお勧めします。

Jira ユーザーのセットアップ

パスワードまたは API トークンまたは**パーソナルアクセストークン**認証の場合は、次を使用して専用の Jira ユーザーを作成します。

- プロジェクトが属する Jira 製品への**製品アクセス** (例: Jira Software)。製品を特定するには、Jiraコンソール(管理者ページではない)で、**[プロジェクト]** > **[すべてのプロジェクトを表示]** に移動し、ドロップダウンフィルターを使用します。
- ユーザーのプロジェクトに対してアクセス許可スキーム経由で付与される、以下のプロジェクトアクセス許可
    - 課題の割り当て
    - プロジェクトを参照する
    - 添付ファイルを作成する
    - 課題の作成
    - 問題を編集

次に、メソッドの認証情報を作成します。

- **(パスワードまたはAPIトークン)APIトークンを作成します。** Jiraユーザーの APIトークンを作成します。APIトークンを作成する手順については、Atlassian のドキュメントを参照してください。
- **(個人アクセストークン)個人用アクセストークンを作成します。** Jiraユーザーのパーソナルアクセストークン (PAT) を作成します。個人用アクセストークンを作成する手順については、Atlassianドキュメントを参照してください。

Jira インスタンスの追加

前提条件を満たしたら、クラウドサイバーエクスポージャーコンソールからJiraインスタンスを追加します。

Jira インスタンスを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. (オプション) [組織] ドロップダウンからアカウント 範囲 を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで **[Jira]** をクリックします。Jira ウィザードが開きます。
5. Jira インスタンスをアクティブ化します。
    1. Jira **インスタンスの URL** を入力します。

        > **注意:** Jira URL は、Atlassian 管理コンソールのアカウントプロファイル領域の **製品** ページで確認できます。

    2. **[認証]** で、次のいずれかを実行します。
        - OAuth を使用するには、**OAuth (推奨)** を選択し、Jira で作成した OAuth 2.0 認証情報の **クライアント ID** と **クライアントシークレット** を入力します。
        - パスワードまたは API トークンを使用するには、**[パスワードまたは API トークン]** を選択し、作成した Jira ユーザーの **ユーザー名** (メールアドレス) と **ユーザーパスワードまたは API トークン** を入力します。
        - 個人用アクセストークンを使用するには、**個人用アクセストークン (PAT)** を選択し、作成したトークンを入力します。
    3. **[終了]** をクリックします。

インスタンスが正常に追加されると、クラウドサイバーエクスポージャーコンソールの > 統合 Settings>Jira のテーブルに表示されます。

Jira スペースの追加

Jira スペースを追加する前に、まず Jira インスタンスの追加する必要があります。

Jira スペースを追加するには:

> **注意:** ウィザードの実行中、クラウドサイバーエクスポージャーコンソールとお使いの Jira Software インスタンスの両方を操作します。

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Integrations]** に移動し、作成した関連 Jira インスタンスの追加を見つけます。
2. インスタンス名の横にある三点リーダーをクリックし、**[スペースの追加]** をクリックします。[スペースの追加 Jira] ウィザードが開きます。
3. **スペースを設定します** (ウィザードのステップ 1)。Jira インスタンスの追加 Jira プロジェクトに追加したときに作成したTenableサービスアカウントまたはユーザーにアクセス許可を付与し、スペースのキーを入力します。
    1. Jira Software インスタンスで、**[Projects]** ページに移動し、追加するプロジェクトを選択します。
    2. プロジェクトを見つけ、次のいずれかの方法で **[プロジェクト設定]** に移動します。
        - プロジェクトの横にある三点リーダーをクリックし、**[プロジェクトの設定]** をクリックします。
        - プロジェクトをクリックし、**[プロジェクト設定]** に移動します。
    3. **[ユーザー]** に移動し、**[ユーザーの追加]** をクリックします。
    4. Jira インスタンスの追加したときに作成したサービスアカウントまたはユーザーのメールアドレスを入力し、**ロール**を選択して、**[追加]** をクリックします。
    5. クラウドサイバーエクスポージャーコンソールで、**スペースキー**を入力します。プロジェクトキーは、Jira Software インスタンスの [Projects] (プロジェクト) ページにあります。
    6. **[次へ]** をクリックします。

4. **作業項目の優先度を同期**して、Tenableの検出結果の深刻度をJiraの対応する優先度と一致させます(ウィザードのステップ2)。Tenable経由で作成されたJiraチケットには、選択された優先度が割り当てられます。完了したら、**[次へ]**をクリックします。

    - **同期しない**
    - **カスタムマッピングを使用して同期します**。Tenableの**検出結果の深刻度**ごとに、**Jira問題の優先度**を割り当てます。

5. **作業項目のステータスを同期**して、Tenableの検出結果のステータスをJiraの対応するステータスと一致させます(ウィザードのステップ3)。Tenable経由で作成されたJiraチケットには、選択されたステータスが割り当てられます。完了したら、**[次へ]**をクリックします。

    > **注意:** この機能には、Jiraでの追加のアクセス許可と設定が必要です。詳細については、「Jira課題のトランジションを許可する」を参照してください。

    - **同期しない**
    - **カスタムマッピングを使用する際の同期問題。**
        1. Tenable内の**課題タイプ**ごとに、**カスタムマッピングを使用して同期**するかどうかを選択します。
        2. Tenableの**検出結果ステータス**ごとに、**Jira課題ステータス**を割り当てます。

6. **[終了]**をクリックします。

スペースが正常に追加されると、そのスペースは> 統合>Jiraのテーブル Settingsに表示されます。

> **重要:** 検出結果の課題の作成を開始するには、自動化を設定するか、Jiraと統合した後検出結果に基づくアクションのトリガーする必要があります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Jira課題のトランジションを許可する

ステータス間でJira課題を移行するには、プロジェクト ワークフローで許可されていることを確認する必要があります。ワークフローとは、課題がライフサイクル中に通過する一連のステータスとトランジションであり、通常は組織内のプロセスを表します。ワークフローでトランジションが許可されていない場合は、Tenableが課題を移動できるようにする追加のトランジションを設定する必要があります。

例:

ワークフローによっては、ステータスが [To Do] (要対応)の課題は、最初に [In Progress] (進行中)に移動しないと [Done] (完了)にトランジションできない場合があります。ただし、クラウドサイバーエクスポージャーでオープンの検出結果が [クローズ] になった場合、ワークフローは最初に [進行中] に移動されなかったため、ステータストランジションは許可されません。クラウドサイバーエクスポージャー がそのようなトランジション制限をバイパスできるようにするには、Jira で追加のトランジションを設定する必要があります。

検出結果のステータス	Jira ステータス
オープン	To Do
-	進行中
クローズ	完了

注意: 追加のJiraトランジションを設定する前に、まずJira スペースの追加で、Tenable検出結果のステータスとJira課題ステータスの間のカスタムマッピングを定義します。

Tenable 用に Jira トランジションを設定するには:

1. **プロジェクトロールを追加する**
    1. 関連するプロジェクトで、**[Settings > System]** に移動します。
    2. [セキュリティ] で、**[プロジェクトロール]** をクリックします。[Project Role Browser] (プロジェクトロールブラウザ) に Jira サイトの全プロジェクトロールのリストが表示されます。
    3. ページ下部にあるAdd Project Role で、理解しやすい名前と説明を入力します。以下に例を挙げます。
        - 名前: **クラウドサイバーエクスポージャー プロジェクトロール**
        - 説明: **移行アクセス許可を設定するためにプロジェクトのワークフローで使用**されます。
    4. **[Add Project Role]** をクリックします。

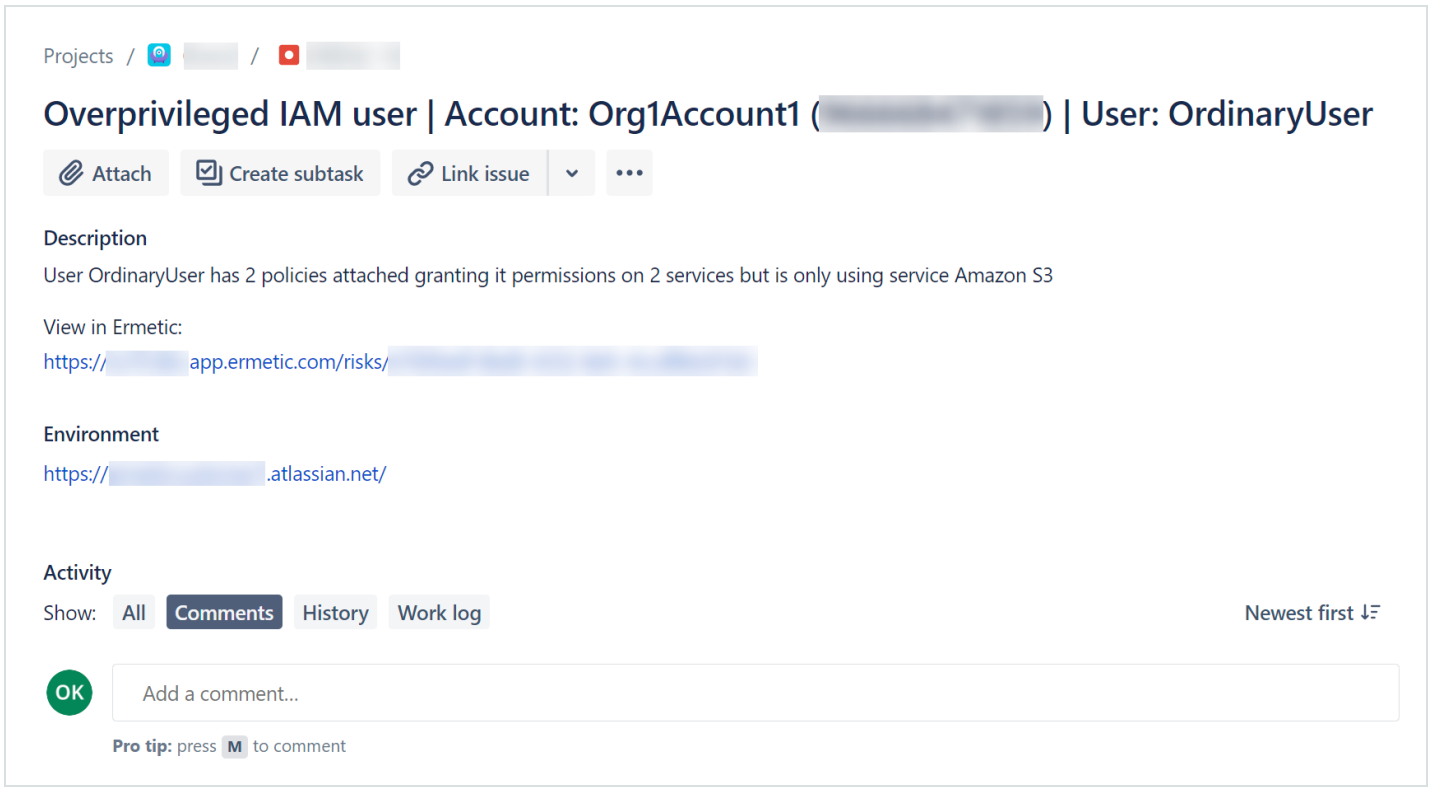
2. **ユーザーまたはグループをプロジェクトロールに割り当てます。**
    1. 同じプロジェクトに戻り、「**プロジェクトに戻る**」、「**プロジェクト設定**」の順にクリックします。
    2. **[ユーザー]** をクリックします。
    3. 右上にある **[ユーザーを追加]** をクリックします。
    4. クラウドサイバーエクスポージャーにJiraインスタンスを追加したときに作成したユーザー**の名前**を選択します。

        > **注意:** 関連するユーザーのメールアドレスではなくユーザー名を選択します。

    5. 前に作成した **ロール** (クラウドサイバーエクスポージャー プロジェクトロール) を選択します。
    6. **[1人を追加]** をクリックします。
3. **ワークフロートランジションを追加します。**
    1. 「**プロジェクトに戻る**」をクリックし、「**プロジェクト設定**」をクリックします。
    2. **[ワークフロー]** をクリックします。
    3. 関連するワークフローを選択し、**[編集]** をクリックします。
    4. 「**ダイアグラム**」ビューで、「**トランジションの追加**」をクリックします。
    5. ダイアログで、次のフィールドに入力します。
        - 開始ステータス: **任意のステータス**
        - ステータスへ: **完了**
        - 名前: **Any to Done**
    6. **[追加]** をクリックします。
    7. 図の [完了] ステータスの横にある **[すべて]** をクリックします。
    8. **[条件]** をクリックします。
    9. 開いたページの下部にある **[条件の追加]** をクリックします。
    10. 「**ユーザーはプロジェクト・ロールに属しています**」オプションを選択し、「**追加**」をクリックします。
    11. 前のステップで作成した **プロジェクトロール** を選択し、「**追加**」をクリックします。

12. 上記の手順を繰り返して、[Any Status] から [To Do]へ別の移行を追加します。
13. 準備ができたら、[ワークフロー] ページの上部にある **[ドラフトの公開]** をクリックします。

サンプル Jira 課題



ServiceNow

ServiceNow インスタンスを Tenable One Cloud Exposure と統合し、Tenable の特定の検出結果に関連するインシデントを作成できるようにします。

次の手順

- 検出結果の問題/インシデントの作成を開始するには、自動化を設定するか、ツールと統合した後 検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

始める前に

OAuth 2.0 または基本認証を使用して統合を認証できます。Tenable は OAuth を推奨しています。どちらの方法でも、専用の ServiceNow ユーザーが必要です。OAuth には、そのユーザーとして実行する OAuth アプリケーションを登録するという、もう 1 つの追加ステップが必要です。

Tenable では、監査証跡アクティビティを簡素化するために、専任のユーザーを推奨しています。統合が不要になった場合は、そのユーザーを削除して終了させることができます。

ウィザードを開始する前に、ServiceNow インスタンスで次の作業を行います。

- **ServiceNow ユーザーを作成します。両方の認証方法に必要です。専用ユーザーを作成し、[Web サービスアクセスのみ]** オプションを選択します。Tenable では、すべてのデータが表示されるように **グローバルユーザーを** 推奨しています。使用する認証方法に応じてロールを付与します。
    1. 基本認証の場合は、`itil` ロールを付与します。
    2. OAuth の場合、`itil`、`sn_incident_read`、`sn_incident_write` ロールを付与します。

    ヒント: Tenable では、すべてのデータを表示できるように **グローバル** ユーザーを推奨します。ユーザーは、インシデントを作成して更新し、ユーザーとグループを表示できる必要があります。

- **(OAuth のみ)OAuth アプリケーションを登録します。** OAuth で認証するには、クライアント認証情報付与を使用する OAuth アプリケーションを ServiceNow に登録します。アプリケーションは上記で作成したユーザーとして実行され、そのユーザーのアクセス許可のみを継承します。
    1. ServiceNow インスタンスで、**[System OAuth]** > **[Inbound Integrations]** に移動します。
    2. **[新しい統合]** をクリックし、**[OAuth - クライアント認証情報の付与]** を選択します。
    3. **[OAuthアプリケーションユーザー]** で、作成した専用ユーザーを選択します。
    4. アプリケーションがそのユーザーのアクセス許可のみを継承するように、**[認証スコープ]** を **[制限付き]** に設定します。
    5. **[次の API に承認を制限する]** で、**[添付ファイル API]** と **[テーブル API]** を選択します
    6. 生成された **クライアント ID** と **クライアントシークレット** をコピーします。

    注意: アクセストークンの最小有効期間は 5 分 (300 秒) です。

インスタンスの追加

前提条件を満たしたら、クラウドサイバーエクスポージャーコンソールからServiceNowインスタンスを追加します。

新しいインスタンスを追加するには

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. (オプション)[Organization] (組織)ドロップダウンで、アカウント範囲を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで、**[ServiceNow]** をクリックします。ServiceNowウィザードが開きます。
5. インスタンスをアクティブ化します (ウィザードのステップ1)。
    1. Tenableに**インスタンスのインスタンス**名を入力します。
    2. ServiceNowインスタンスの **インスタンスURL** を入力します。
    3. **[認証]** で、次のいずれかを実行します。
        - OAuthを使用するには、**OAuth** を選択し、ServiceNowに登録したOAuthアプリケーションの **クライアントID** と **クライアントシークレット** を入力します。
        - 基本認証を使用するには、**[基本]** を選択し、作成したServiceNowユーザーの **ユーザー名** (ID) と **パスワード** を入力します。

        詳細については、「始める前に」を参照してください。
    4. **[次へ]** をクリックします。
6. インシデントの優先度を同期して、Tenable内の検出結果の深刻度と、対応するServiceNowのインシデントの影響/緊急性を一致させます (ウィザードのステップ2)。Tenable経由で作成されたServiceNowインシデントには、選択した優先度が割り当てられます。完了したら、**[次へ]** をクリックします。
    - **同期しない**
    - **カスタムマッピングを使用して同期します**。Tenableの**検出結果の深刻度**ごとに、**ServiceNowインシデントの影響**と**ServiceNowインシデントの緊急度**を割り当てます。
7. **インシデントの状態を同期** して、Tenableの検出結果のステータスをServiceNowの対応する状態と一致させます (ウィザードのステップ3)。Tenable経由で作成されたServiceNowインシデントには、選択した状態が割り当てられます。完了したら、**[完了]** をクリックします。

> **注意:** この機能には、ServiceNow での追加のアクセス許可と設定が必要です。詳細については、インシデントの状態と検出結果のステータスの同期 を参照してください。

- **同期しない**
- **カスタムマッピングを使用して同期します**。
  - Tenable の**検出結果ステータス**ごとに、**ServiceNow インシデント状態**を割り当てます。
  - **[検出結果が再オープンされたときに新しいインシデントを作成する]** かどうかを選択します。

  ServiceNow の [Closed] (クローズ) および [Canceled] (キャンセル) の状態は最終的なものと見なされ、アクティブ状態に戻すことはできません。インシデントがこれらの状態のいずれかに達すると、事実上インシデントライフサイクルから廃止されます。その結果、検出結果のステータスをこれらの状態のいずれかにマッピングすると、検出結果が再オープンされたときに新しいインシデントを作成することを選択できません。検出結果を確実に再オープンして追跡できるようにするには、検出結果を最終ではない ServiceNow 状態にマッピングすることを検討してください。

インスタンスが正常に追加されると、そのインスタンスは Settings > 統合 > ServiceNow のテーブルに表示されます。

> **重要:** 検出結果の問題/インシデントの作成を開始するには、自動化 を設定するか、ツールと統合した後 検出結果に基づくアクションのトリガー する必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

インシデントの状態と検出結果のステータスの同期

Tenableに別のレベルのアクセス許可を付与することで、ServiceNow インシデントの状態をクラウドサイバーエクスポージャー 検出結果のステータスと同期できます。これを行うには、Tenable によって作成されたカスタム更新セットをインポートします。

インシデントの状態を検出結果のステータスと同期する方法

1. ServiceNow インスタンスで、**[Retrieved Update Sets] (取得された更新セット)** に移動します ([System Update Sets] (システム更新セット) の下にあります)。
2. [関連リンク] で、**[XML から更新セットのインポート]** をクリックします。
3. 次の XML ファイルを選択して **アップロード** します。

   ServiceNowSyncIncidentStates.xml
4. クリックすると、新しく作成された **Tenable ロール更新セット - インシデント状態** が開きます。
5. **[プレビュー更新セット]** をクリックします。[Update Set Preview] (更新セットのプレビュー) ダイアログが表示されます。完了したら、**[閉じる]** をクリックします。
6. 競合 (衝突) が存在しないことを確認します。
7. 変更 (顧客の更新) を確認し、**[更新セットのコミット]** をクリックします。[Update Set Commit] (更新セットの反映) ダイアログが表示されます。完了したら、**[閉じる]** をクリックします。これで、更新セットの状態は [コミット済み] になっているはずです。
8. **[ユーザー] と [グループ] > [ユーザー]** に移動します。
9. ServiceNow インスタンスを追加した際に作成したTenableユーザーの**ユーザー ID** を見つけてクリックします。
10. ページ下部にある **[ロール]** セクションに移動し、**[編集...]** をクリックします。
11. Tenable ロールをロールリストに追加します。
    - 左側のコレクション領域から、**tenable_state_readonly_role**を検索して選択します。
    - 追加ボタン (>) をクリックして、ロールを右側のロールリストに移動します。

    > **重要: itil** ロールが右側のロールリストにも含まれていることを確認します。このロールは ServiceNow インスタンスを追加したときに付与されたもので、統合が機能するために必要です。
12. **[保存]** をクリックします。

インシデントの追加フィールドの使用

デフォルトでは、Tenable は、クラウド サイバーエクスポージャー アクションを介して ServiceNow インシデントを作成する際に、関連フィールドの基本セットのカスタマイズをサポートしています。これらには、[担当者]、[割り当てグループ]、[カテゴリ]、[影響]、[緊急度]、[サマリー]、[説明] のフィールドが含まれます。

- ServiceNow と統合したときに付与されたアクセス許可を超えるレベルのアクセス許可をTenableに付与することで、追加のフィールドをカスタマイズできます。これを行うには、Tenable によって作成されたカスタム更新セットをインポートします。
- 使用できる追加フィールドについては、「サポートされているフィールド を参照してください。

インシデントの追加フィールドを使用するには

1. ServiceNow インスタンスで、**[Retrieved Update Sets] (取得された更新セット)** に移動します ([System Update Sets] (システム更新セット) の下にあります)。
2. [関連リンク] で、**[XML から更新セットのインポート]** をクリックします。
3. 次の XML ファイルを選択して **アップロード** します。

   ServiceNowAdditionalFields.xml
4. クリックすると、新しく作成された **[Tenable ロール更新セット - 追加フィールド]** が開きます。
5. **[プレビュー更新セット]** をクリックします。[Update Set Preview] (更新セットのプレビュー) ダイアログが表示されます。完了したら、**[閉じる]** をクリックします。
6. 競合 (衝突) が存在しないことを確認します。
7. 変更 (顧客の更新) を確認し、**[更新セットのコミット]** をクリックします。[Update Set Commit] (更新セットの反映) ダイアログが表示されます。完了したら、**[閉じる]** をクリックします。これで、更新セットの状態は [コミット済み] になっているはずです。
8. **[ユーザー] と [グループ] > [ユーザー]** に移動します。
9. ServiceNow インスタンスを追加した際に作成したTenableユーザーの**ユーザー ID** を見つけてクリックします。
10. ページ下部にある **[ロール]** セクションに移動し、**[編集...]** をクリックします。
11. Tenable ロールをロールリストに追加します。
    - 左側のコレクション領域から、**tenable_fields_readonly_role**を検索して選択します。
    - 追加ボタン (>) をクリックして、ロールを右側のロールリストに移動します。

    重要: itil ロールが右側のロールリストにも含まれていることを確認します。このロールは ServiceNow

> インスタンスを追加したときに付与されたもので、統合が機能するために必要です。

12. **[保存]** をクリックします。

サポートされているフィールド

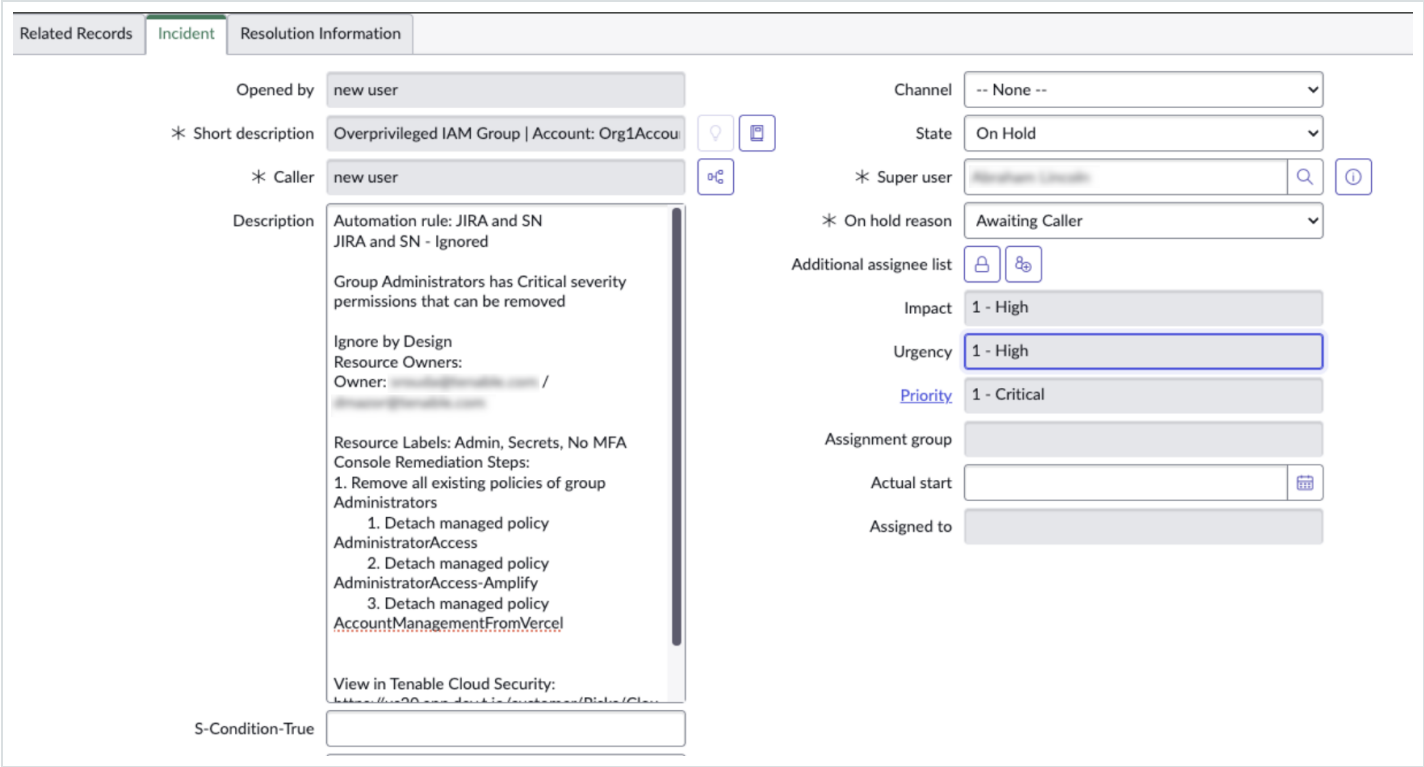
Tenable は、次の **基準をすべて** 満たすフィールドのカスタマイズのみをサポートします。

- フィールドは別のフィールドの値に依存しません。
- フィールドが表示されます (無条件に適用される UI ポリシーによって非表示になりません)。
- フィールドは書き込み可能です。ディクショナリ、ディクショナリオーバーライド、または無条件に適用される UI ポリシーによってフィールドが読み取り専用とマークされている場合、フィールドは除外されます。
- フィールドタイプがサポートされています (文字列、choice、整数、参照)。
- UI ポリシーによって条件付きで制限されたフィールドは、引き続き完全に利用できます (表示、オプション、書き込み可能)。Tenable は条件が存在することを検出できますが、それらを評価することはできないため、これらのフィールドには「(UI-Policy)」ラベルとツールチップでフラグが立てられます。

次のフィールドは表示されません:

- `number` (ServiceNow により自動生成)
- `state` (別売り)

ServiceNow インシデントのサンプル



コラボレーション

Slack

Slack ワークスペースを Tenable One Cloud Exposure と統合し、以下をサポートします。

- Tenable で特定の検出結果が作成された場合に Slack チャンネルに通知を送信します。
- セルフサービスのジャストインタイムアクセスワークフローの一部として Slack を使用することで、ユーザーはアクセスのリクエストや承認を簡単に行えるようになります。設定方法の詳細については、「Slack と JIT の統合」を参照してください。

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Workspace の追加

Slack ワークプレイスを追加するには、Slack で所有者ロールまたは管理者ロールが必要です。すべてのユーザーが Slack チャンネルを追加できます。

ワークスペースを統合すると、Tenable は、Slack の Tenable 統合ページに表示されない個別のチャンネルを含む、ワークスペース内のすべてのチャンネルを自動的に識別し、使用できるようにします。ワークスペースを統合した後に Slack に新しいチャンネルを追加した場合、そのチャンネルが Tenable 内で使用できるようになるまでに数分かかる場合があります。

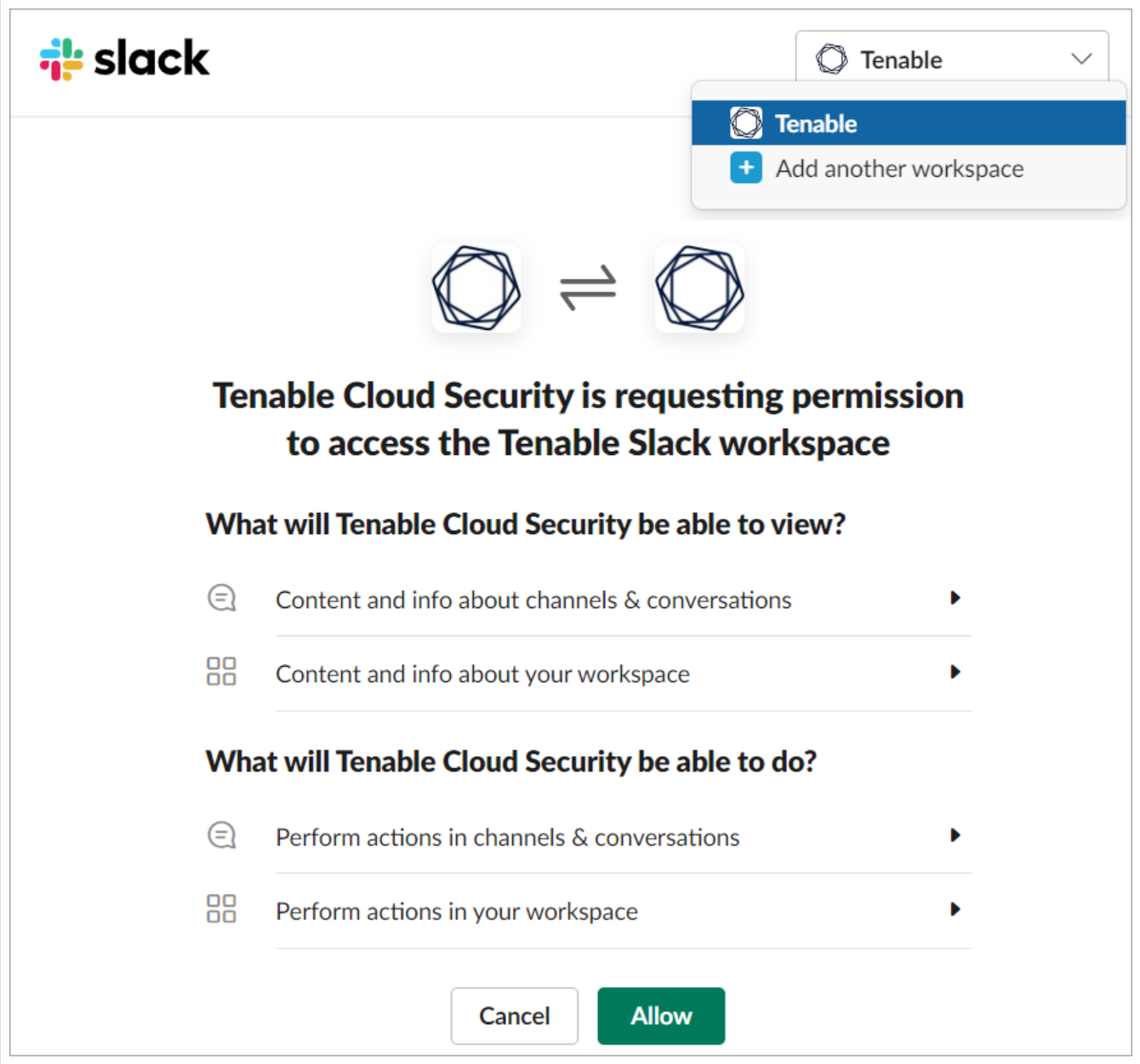
注意:

- Slack の要件により、関連するワークスペースに属するユーザーのみがクラウドサイバーエクスポージャーコンソールで関連するチャンネルを閲覧できます。つまり、Slack で使用されるメールは、コンソールへのログインに使用されるメールと同一である必要があります。
- 1 つの自動化に関して 1 日に送信するのに十分な数の通知がある場合、それらは個別に送信されるのではなく、1 つの Slack メッセージまたはメールに集約されます。

重要: (JIT のみ)バージョン 1.51 以前に追加された Slack ワークスペースの操作に関する重要な情報については、「ワークスペースの再認証」を参照してください。

Slack ワークスペースとチャンネルを追加するには

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** に移動します。
2. (オプション)[組織]ドロップダウンでアカウント範囲を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで、**[Slack**ワークスペース**]** をクリックします。



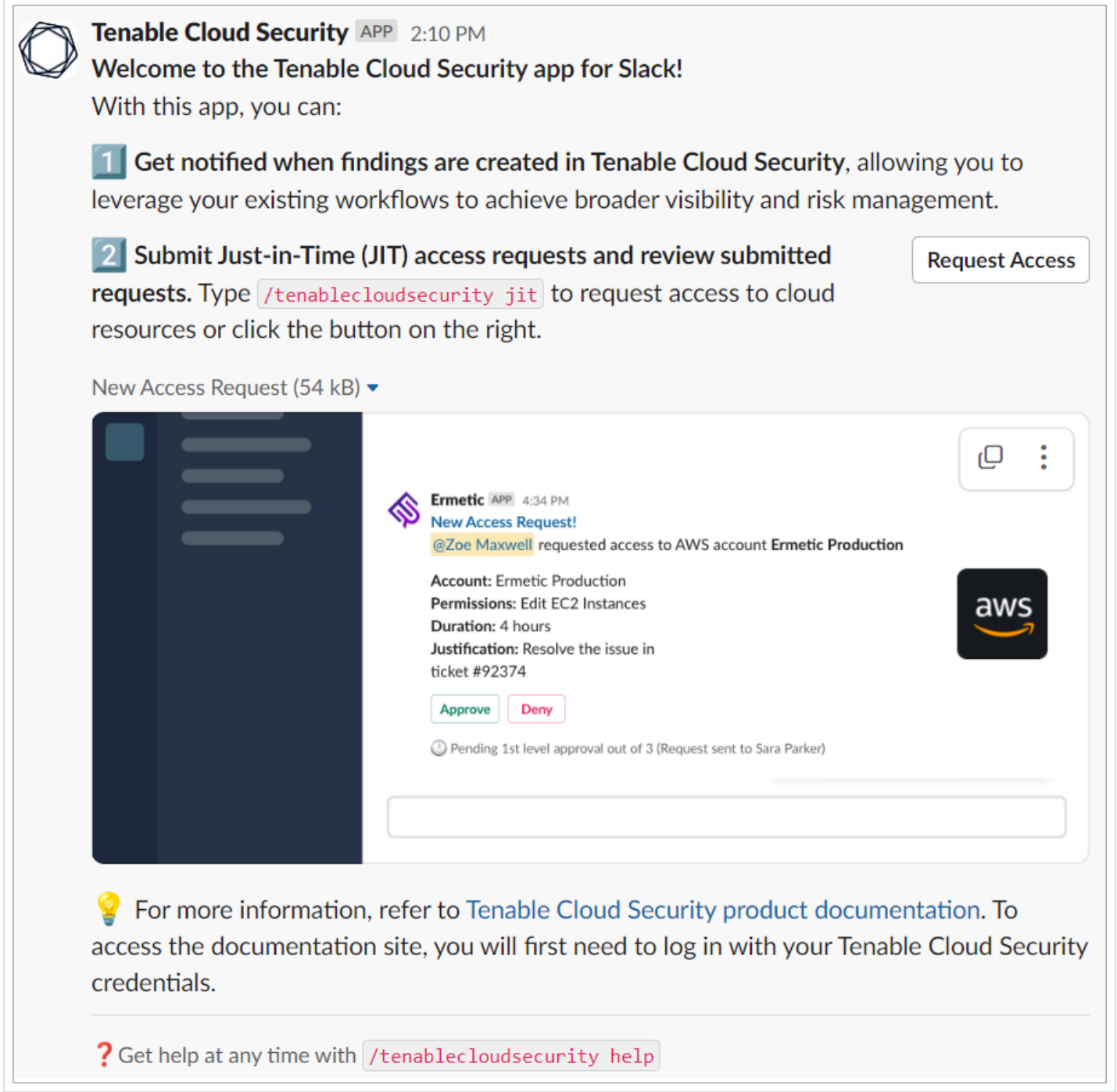
5. 複数のワークスペースがある場合は、ページの右上にあるドロップダウンから対象のワークスペースを選択できます。
6. **[許可]** をクリックして、Tenable 会社のワークスペースへのアクセス権を付与します。ワークスペースが正常に追加されると、そのワークスペースは > 統合 Settings Slack >テーブルに表示されます。
7. チャンネルを追加するには、関連するチャンネルで次のコマンドを入力して送信します。

   ```
   /invite @tenablecloudsecurity
   ```

2023 年 12 月に、アプリの名前が Ermetic から *クラウド サイバーエクスポージャー* に変更されました。

- 名前変更の前にアプリを追加した場合は、引き続き前の `/invite @ermetic` コマンドを使用してチャンネルを追加してください。
- 必要に応じて、Slack でアプリのボット名を編集し、名前を手動で クラウド サイバーエクスポージャー に更新できます。チャンネルの追加に使用するコマンドは、それに応じて変更されます。これを行うには、ワークスペースの所有者ロールまたは管理者ロールが必要です。

アプリが正常にインストールされると、Slack にウェルカムメッセージが表示されます。



重要: 検出結果の通知の送信を開始するには、Slack と統合した後に自動化を設定する必要があります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

JIT 用のワークスペースを再認証する

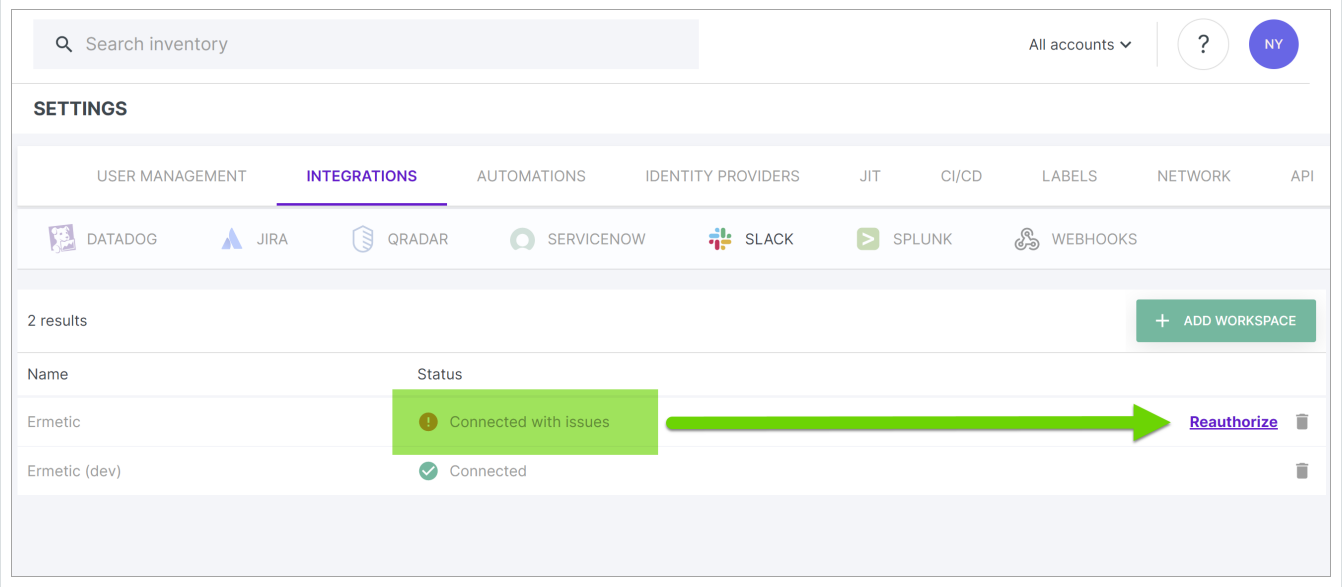
JIT ワークフローの一部として Slack を使用している場合は、次の重要な情報に注意して、ワークスペースが JIT で動作する資格があることを確認します。

- JIT で Slack の使用をサポートするには、2022 年 12 月 11 日 (バージョン 1.51) **より前**に追加したワークスペースを再**認証**する必要があります。
- この日付より後に追加した新しいワークスペースには、必要なアクセス許可がすでに付与されているため、アクションは必要ありません。

ワークスペースを再認証する方法(

> **必要なクラウドサイバーエクスポージャーユーザーロール:** ワークスペースの所有者ロールまたは管理者

1. **[Settings > INTEGRATIONS > SLACK]** に移動します。
2. ステータスが [接続に問題あり] (Connected with issues) で、[再認証] (Reauthorize) ボタンがあるワークスペースを見つけます。
3. **[再認証]** をクリックしてワークスペースを更新します。



Slack で検出結果を表示する

Slack でクラウドサイバーエクスポージャー検出結果を表示する方法

1. Slack ワークスペースで、自動化ルールまたは手動アクションの設定内容に応じて、検出結果が送信されたチャンネルに移動します。
2. チャンネルで、クラウドサイバーエクスポージャー アプリから送信されたメッセージを表示します。

Microsoft Teams

Microsoft Teams と統合して、特定の検出結果が Tenable One Cloud Exposure で作成されたときに Teams のチャネルに通知を送信します。

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Teams 組織の追加

統合を使用するには、クラウドサイバーエクスポージャーコンソールに Teams 組織を追加し、関連する各チーム/チャネルの クラウドサイバーエクスポージャー Teams アプリをインストールする必要があります。

Microsoft Teams と統合するには:

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** に移動します。
2. (オプション)[組織]ドロップダウンで 範囲 を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで、**[チーム組織]** をクリックします。
5. Microsoft アカウントのサインインページで、Tenable と統合させるテナントが属する管理アカウントを選択します。
6. **[承認]** をクリックして Microsoft の クラウドサイバーエクスポージャー Teams アプリを承認し、Tenableに必要なアクセス許可を付与します。同意が承認されると、Tenable にリダイレクトされます。
7. Microsoft Teams に移動します。

8. **[アプリ]** をクリックし、**クラウドサイバーエクスポージャー** アプリを検索します。
9. **[追加]** > **[チームに追加]** をクリックします。

重要: 検出結果の通知の送信を開始するには、Teams と統合した後に自動化を設定する必要があります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

SIEM (セキュリティ情報イベント管理)

データドッグ

Datadog と統合して、Tenable One Cloud Exposure 検出結果を Datadog 組織に送信します。

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Datadog 組織の追加

Datadog 組織を追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. (オプション)[組織]ドロップダウンで範囲を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで、**[Datadog]** をクリックします。Datadog ウィザードが開きます。
5. Datadog 組織の **組織名** を入力します。
6. ドロップダウンから Datadog **サイト** を選択します。どのサイトにいるかは、Datadog Web サイトの URL を Datadog ドキュメントに記載されているサイトの URL と照合することで特定できます。
7. Datadog **API キー**を入力します。Datadog ユーザーインターフェースで新しい API キーを追加します:

1. Datadog ユーザーインターフェースにログインし、(ユーザー名 の横 にある) [Organization settings] に移 動して、**[API keys]** タブをクリックします。
2. **[新しいキー]** ボタンをクリックします。
3. キーまたはトークンの名 前を入 力します。
4. **[API キーの作 成]** をクリックします。

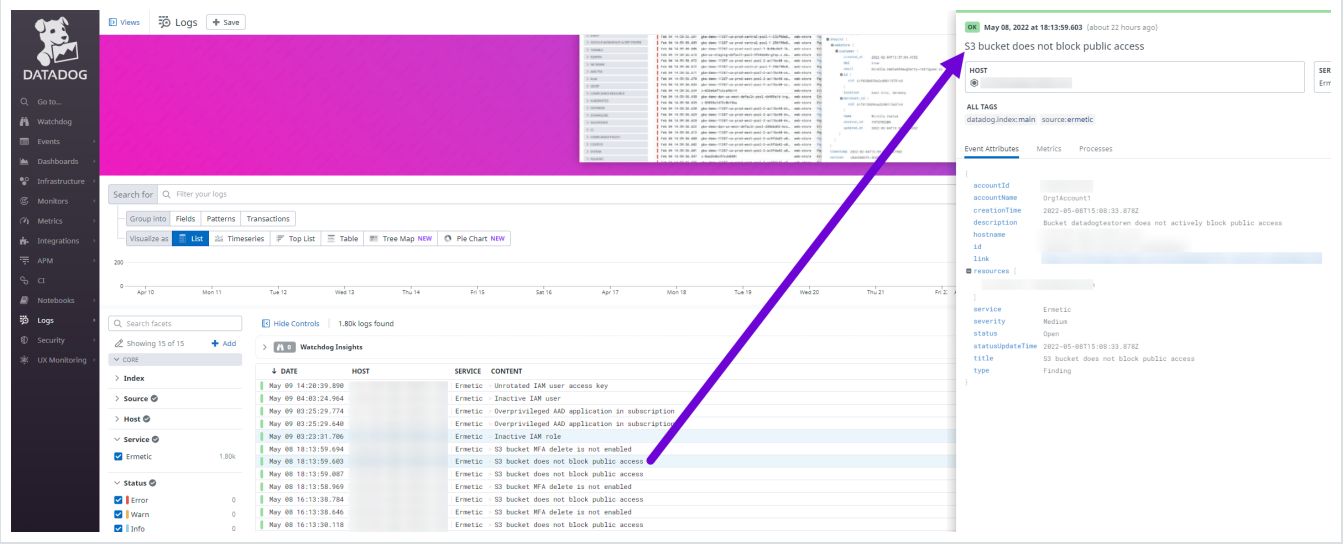
8. **[保 存]** をクリックします。

重 要: 検 出 結 果 の通 知 の送 信 を開 始 するには、Datadog と統 合 した後 に 自 動 化 を設 定 する必 要 があります。すべての統 合 ステップを正 常 に完 了 しても、それ自 体 ではデータ送 信 はトリガーされません。

Datadog で Tenable の検 出 結 果 を表 示 する

Datadog で検 出 結 果 を表 示 する方 法

1. Datadog 組 織 にログインします。
2. **[ログ]** に移 動 し、Ermetic がサービスとしてリストされているログを検 索 します。



JSON のサンプル

JSON

```
{
    "id": "***",
```

```
"content": {
    "timestamp": "2022-05-08T12:31:25.909Z",
    "tags": [
        "source:ermetic"
    ],
    "host": "***",
    "service": "Ermetic",
    "attributes": {
        "status": "Open",
        "hostname": "***",
        "description": "***",
        "service": "Ermetic",
        "labels": [
            "Admin"
        ],
        "creationTime": "2022-05-08T12:15:16.164Z",
        "accountName": "Org1Subscription1",
        "link": "***",
        "statusUpdateTime": "2022-05-08T12:15:16.164Z",
        "accountId": "***",
        "type": "Finding",
        "id": "***",
        "resource": [
            "azure-cli-2021-01-19-07-49-00"
        ],
        "severity": "Critical",
        "policyName": "Inactive AAD application in subscription",
        "ticketLinks": [
            "https://tenablecustomer1.atlassian.net/browse/DAV-24140",
            "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
            "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
            "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
        ],
        "comments": [
            {
                "message": "created a ServiceNow incident for this threat story",
                "time": "2026-07-29T09:00:13.124307Z",
                "userName": "Tenable"
            },
            {
                "message": "created a Jira ticket for this threat story",
                "time": "2026-07-29T09:00:05.609867Z",
                "userName": "Tenable"
            }
        ]
    }
```

```
    }
}
```

QRadar

IBM QRadar (バージョン 7.3.2 以降) と統合して、Tenable One Cloud Exposure 検出結果を QRadar サーバーに送信します。

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

QRadar サーバーの追加

この統合は、インターネット向けサーバーとネットワーク分離されたサーバーの両方をサポートしています。ネットワーク分離サーバーの操作の詳細については、「ネットワーク分離されたサーバーの接続を参照してください。

> **注意:** QRadar との統合に使用される Tenable QRadar 拡張 XML は静的です。つまり、新しいバージョンのクラウドサイバーエクスポージャーがリリースされると、Tenable がリリースした新しい検出結果タイプは、QRadar で不明なイベントとして表示されます。このようなイベントを適切に表示するには、QRadar コンソールで Tenable 拡張を再アップロードする必要があります。

QRadar サーバーを追加する方法:

> **注意:** ウィザードの実行中は、クラウドサイバーエクスポージャーコンソールとIBM QRadar コンソールの両方を操作する必要があります。このタスクの手順の大半は、別段の指示がない限り IBM QRadar コンソールで実行します。

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** に移動します。
2. (オプション)[組織]ドロップダウンで範囲を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリーで、**QRadar** をクリックします。QRadar ウィザードが開きます。

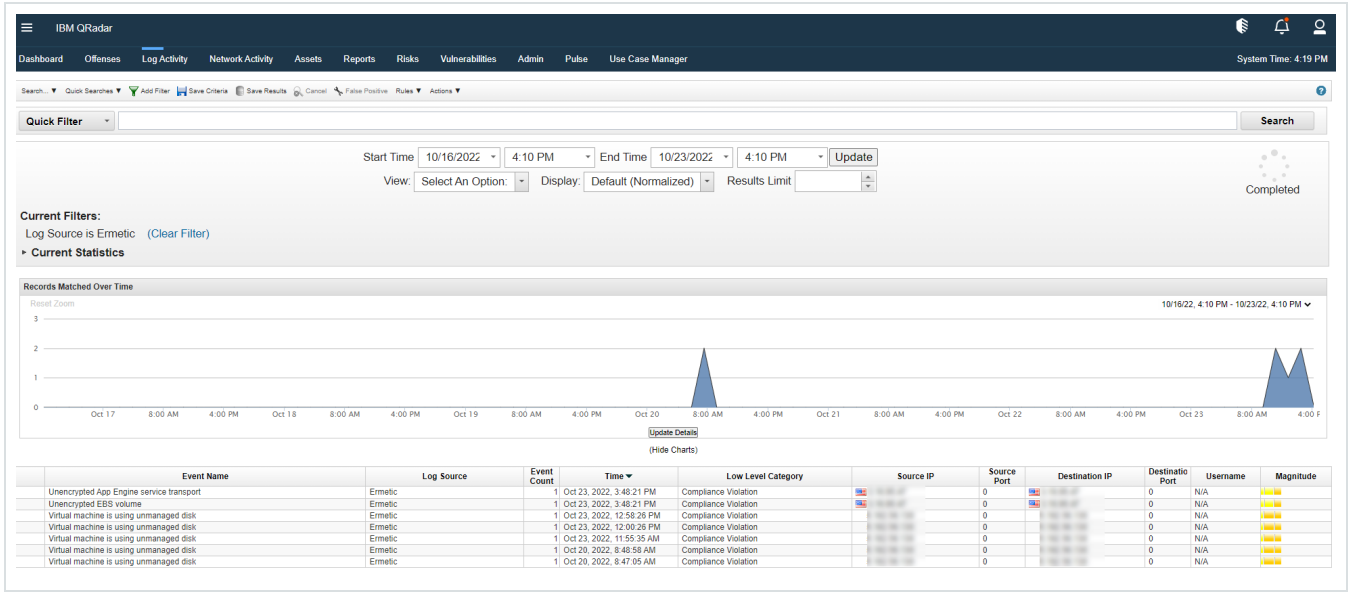
5. QRadar にTenable 拡張を追加します (ウィザードのステップ 1):
    1. ウィザードのリンクを使用してTenableQRadar 拡張をダウンロードします。
    2. IBM QRadar コンソールで、「**管理者**」ページに移動し、「**拡張管理**」をクリックします。
    3. 「**追加**」をクリックし、Tenable QRadar 拡張を保存した場所を参照します。
    4. **[追加]** をクリックします。
6. Tenableログソースを追加します (ウィザードのステップ 2):
    1. 「QRadar **管理**」ページで、「**ログ・ソース**」(「データ・ソース」>「イベント」セクション内) をクリックします。新しいウィンドウが表示され、QRadar Log Source Management アプリを使用するように要求されます。
    2. **[Launch]** (起動) をクリックします。
    3. 「IBM QRadar Log Source Management」ページで、「**ログ・ソース]** をクリックします。
    4. **[+ New Log Source]** をクリックします。追加するログソースの数を確認するページが表示されます。
    5. **[単一のログソース]** をクリックします。
    6. ログソースとして **Ermetic** を検索して選択し、**ステップ 2: プロトコルタイプを選択します**。
    7. **[TLS Syslog]** を選択し、**[ステップ 3: ログソースパラメーターの設定]** をクリックします。
7. 次のようにログソースパラメーターを設定することにより、Tenable ログソースを追加します (ウィザードのステップ 3):
    1. ログ**ソースの名前として**「Ermetic」と入力します。
    2. **[拡張機能]** で、**ErmeticCustom_ext** を選択します。
    3. **[Coalescing Events]** ラジオボタンをオフにします。
    4. **[ステップ 4: プロトコルパラメーターの設定]** をクリックします。
    5. **ログ・ソース識別子**として「**Ermetic**」と入力します。
    6. (オプション) 必要に応じて、TLS リッスンポートまたは証明書タイプを変更します。
    7. **ペイロードの最大長**として「**30000**」と入力します。
    8. **[ステップ 5: プロトコルパラメーターのテスト]** をクリックします。
    9. (オプション)**[テストの開始]** をクリックして、プロトコルパラメーターをテストします。

8. クラウドサイバーエクスポージャーに以下のQRadarサーバーパラメーターを入力します(ウィザードのステップ4)。
    - **表示名**。クラウドサイバーエクスポージャーでのQRadar統合の表示名。
    - Tenableのサーバーへの接続方法を選択します。サーバーがネットワークから分離されている場合、Tenableエンドポイントコネクタを使用して接続を確立します。
        - **エンドポイント(インターネット向け):**
            - IBM QRadarコンソールの**ホスト名またはIPアドレス**を、`https://`プロトコル接頭部を除いて入力します。
            - **QRadar TLSポート**を入力します。変更しない限り、デフォルトは6514です。
        - **エンドポイントコネクタ(ネットワーク分離)**。ドロップダウンから関連するコネクタを選択します。このオプションが無効になっている場合は、まだコネクタを追加していないということです。追加方法については、「ネットワーク分離されたサーバーの接続」を参照してください。
    - サーバーでSSLが有効になっている場合は、**すべてのサーバーSSL証明書を受け入れる**にチェックを入れます。
9. **[終了]**をクリックします。

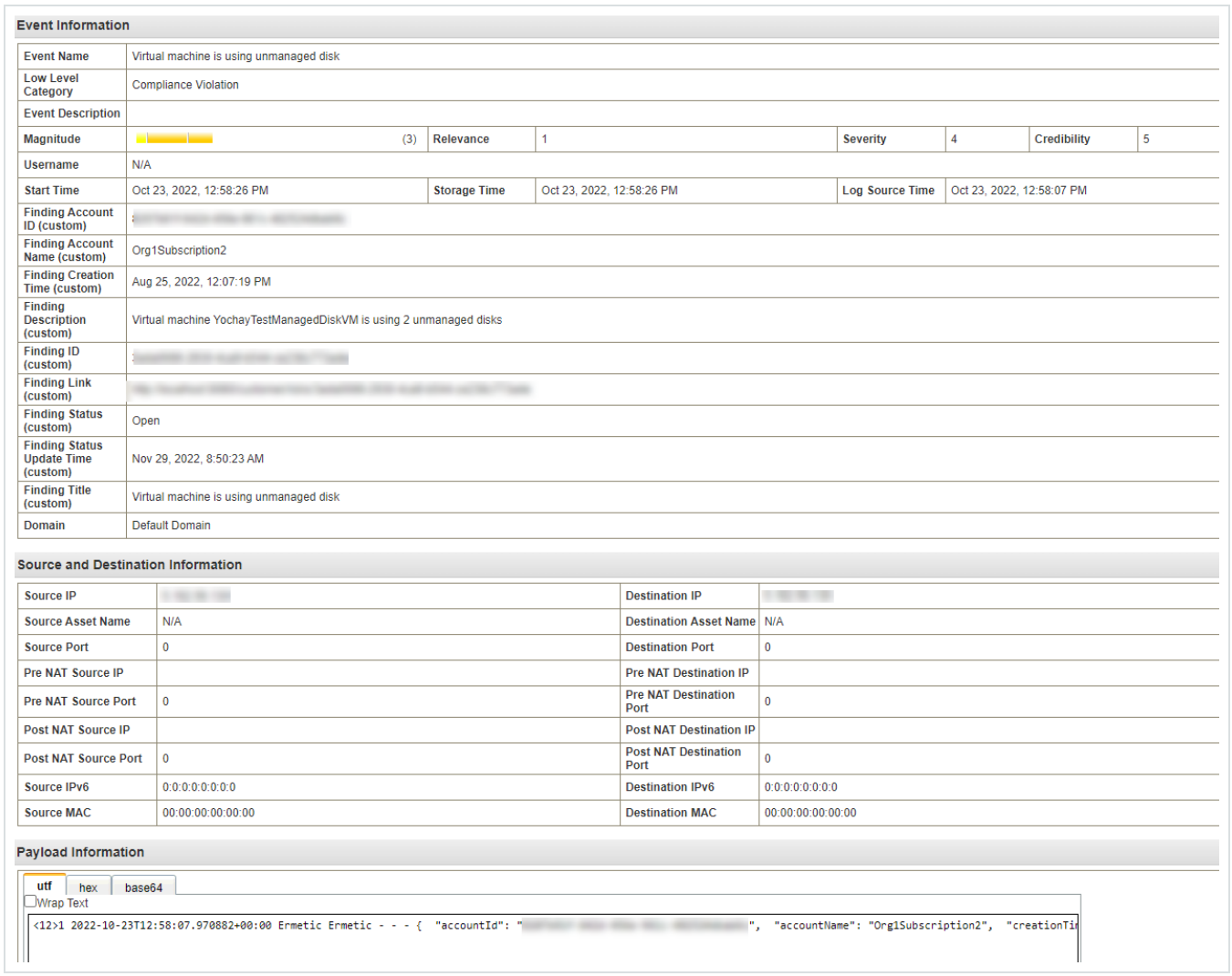
重要: 検出結果の通知の送信を開始するには、QRadarと統合した後に自動化を設定する必要があります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

QRadarでのTenable検出結果の表示

1. IBM QRadarコンソールで、「**ログ・アクティビティー**」ページに移動します。
2. **[フィルターの追加]**をクリックし、フィルターを次のように定義します。
    - パラメーター: **ログソース[インデックス済み]**
    - 演算子: **Equals**
    - ログソースフィルター: **Ermetic**
3. **[フィルターの追加]**をクリックします。



4. イベントをダブルクリックして、イベントの詳細ビューを表示します。



Event Information

Event Name	Virtual machine is using unmanaged disk						
Low Level Category	Compliance Violation						
Event Description							
Magnitude	(3)	Relevance	1	Severity	4	Credibility	5
Username	N/A						
Start Time	Oct 23, 2022, 12:58:26 PM	Storage Time	Oct 23, 2022, 12:58:26 PM	Log Source Time	Oct 23, 2022, 12:58:07 PM		
Finding Account ID (custom)							
Finding Account Name (custom)	Org1Subscription2						
Finding Creation Time (custom)	Aug 25, 2022, 12:07:19 PM						
Finding Description (custom)	Virtual machine YochayTestManagedDiskVM is using 2 unmanaged disks						
Finding ID (custom)							
Finding Link (custom)							
Finding Status (custom)	Open						
Finding Status Update Time (custom)	Nov 29, 2022, 8:50:23 AM						
Finding Title (custom)	Virtual machine is using unmanaged disk						
Domain	Default Domain						

Source and Destination Information

Source IP		Destination IP	
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf hex base64

Wrap Text

<12>1 2022-10-23T12:58:07.970882+00:00 Ermetic Ermetic - - - { "accountId": "", "accountName": "Org1Subscription2", "creationTi

JSON のサンプル

JSON

```
{
  "accountId": "*****project",
  "accountName": "*****Project",
  "creationTime": "2022-10-23T10:31:54.446Z",
  "description": "App Engine Service default has 1 version not enforcing HTTPS connections",
  "id": "********-****-****-****-************",
  "link": "https://****.***.app.ermetic.com/customer/risks/ca6978eb-****-****-****-68241bedc38f",
  "labels": [
  ],
  "resource": [
    "apps/*****project/services/default"
```

```
  ],
  "severity": "Medium",
  "status": "Open",
  "statusUpdateTime": "2022-10-23T18:50:23.321Z",
  "policyName": "Unencrypted App Engine service transport",
  "type": "Finding",
  "ticketLinks": [
    "https://tenableccustomer1.atlassian.net/browse/DAV-24140",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
  ],
  "comments": [
    {
      "message": "created a ServiceNow incident for this threat story",
      "time": "2026-07-29T09:00:13.124307Z",
      "userName": "Tenable"
    },
    {
      "message": "created a Jira ticket for this threat story",
      "time": "2026-07-29T09:00:05.609867Z",
      "userName": "Tenable"
    }
  ]
}
```


Splunk

Splunk Enterprise または Splunk Cloud Platform と統合して、Tenable One Cloud Exposure 検出結果をお使いの Splunk インスタンスに送信します。

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Splunk インスタンスの追加

Splunk での通知を有効にするには、まず HTTP イベントコレクタ (HEC) と HEC トークンを作成する必要があります。これらは、Tenable が送信する検出結果を Splunk が受信できるようにするために使用されます。

Splunk と統合するには

1. Splunk で HEC を有効にし、HEC トークンを設定します。Splunk Enterprise または Splunk Cloud Platform でこれを行う方法については、Splunk のドキュメント を参照してください。これらの手順を実行しながら、次の情報を記録してください。
    - HEC に対して SSL が有効になっているかどうか。
    - HEC が使用する HTTP ポート番号。
    - 設定するトークンの値。

    > **注意:** Splunk Cloud Platform では、HEC はデフォルトで有効であり、SSL/HTTP ポート番号は自動的に設定され、変更できません。SSL が有効で、ポートは 8088 です。Splunk Enterprise では HEC を積極的に有効にする必要があります。また、SSL/HTTP ポート番号の設定を変更できます。

2. クラウドサイバーエクスポージャー コンソールで、**[設定] > [統合]** に移動します。
3. (オプション)[組織] ドロップダウンで 範囲 を選択します。
4. **[統合の追加]** をクリックします。
5. 統合ライブラリで **[Splunk]** をクリックし、**[Next]** をクリックしてステップ 2 (Splunk HTTP イベントコレクター情報の提供) に進みます。
6. クラウドサイバーエクスポージャー での Splunk 統合の **[表示名]** を入力します。
7. イベント **コレクターの URL** を入力します。これは、Splunk プラットフォームのインスタンスアドレスと、HEC が使用する HTTP ポート番号を合わせたものです。たとえば、https://splunkcloud.com:8088
8. HEC に対して SSL が有効になっている場合は、**[Accept any server SSL certificates]** にチェックを入れます。
9. Splunk で設定した HEC **トークン** 値を入力します。
10. **[終了]** をクリックします。

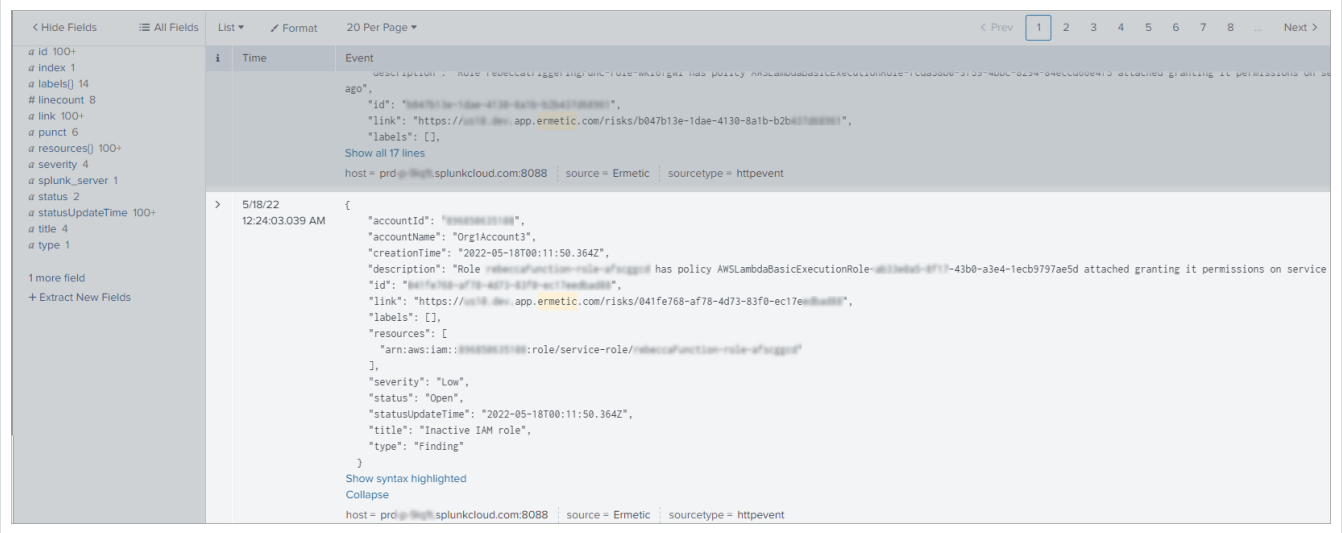
統合が正常に追加されたら、**[完了]** をクリックして [統合] ページに戻り、新しく追加された統合が表示されます。

重要: 検出結果の通知の送信を開始するには、Splunk と統合した後に自動化を設定する必要があります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Splunk で Tenable の検出結果を表示する

Splunk で検出結果を表示する方法

1. Splunk Cloud または Enterprise インスタンスにログインします。
2. クラウドサイバーエクスポージャー検出結果に関連する検索語を使用してイベントを検索します。



JSON のサンプル

JSON


```
{
  "preview": false,
  "lastrow": true,
  "result": {
    "_raw": "{\n    \"accountId\": \"***\",\n    \"accountName\": \"***\",\n    \"creationTime\": \"2022-
05-18T00:11:50.364Z\",\n    \"description\": \"Role Function-role-afscggcd has policy
AWSLambdaBasicExecutionRole-********************************** attached granting it permissions on
service Amazon CloudWatch Logs, but it has not used it and was last active one month ago\",\n    \"id\":
\"**********************************\",\n    \"link\":
```

```
\"https://****.***.app.ermetic.com/risks/**********************************\",\n    \"labels\": [],\n
\"resources\": [\n      \"arn:aws:iam::"
    ************
    ",:role/service-role/Function-role-afscggcd\"\n    ],\n    \"severity\": \"Low\",\n    \"status\":
\"Open\",\n    \"statusUpdateTime\": \"2022-05-18T00:11:50.364Z\",\n    \"title\": \"Inactive IAM
role\",\n    \"type\": \"Finding\"\n  }",
    "_time": "2022-05-18T00:24:03.039+0000",
    "accountId": "************",
    "accountName": "Org1Account3",
    "creationTime": "2022-05-18T00:11:50.364Z",
    "description": "Role rebeccaFunction-role-afscggcd has policy AWSLambdaBasicExecutionRole-
********************************** attached granting it permissions on service Amazon CloudWatch Logs,
but it has not used it and was last active one month ago",
    "host": "********.splunkcloud.com:8088",
    "id": "**********************************",
    "index": "main",
    "linecount": "17",
    "link": "https://******.app.ermetic.com/risks/**********************************",
    "punct": "{____\"\":_\"\",____\"\":_\"\",____\"\":_\"--::.\",____\"\":_\"_-",
    "resource{}": "arn:aws:iam::************:role/service-role/Function-role-afscggcd",
    "severity": "Low",
    "source": "Ermetic",
    "sourcetype": "httpevent",
    "splunk_server": "si-i-*****************.*****.splunkcloud.com",
    "status": "Open",
    "statusUpdateTime": "2022-05-18T00:11:50.364Z",
    "policyName": "Inactive IAM role",
    "type": "Finding",
    "ticketLinks": [
      "https://tenablecustomer1.atlassian.net/browse/DAV-24140",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
    ],
    "comments": [
      {
        "message": "created a ServiceNow incident for this threat story",
        "time": "2026-07-29T09:00:13.124307Z",
        "userName": "Tenable"
      },
      {
        "message": "created a Jira ticket for this threat story",
        "time": "2026-07-29T09:00:05.609867Z",
        "userName": "Tenable"
      }
    ]
  }
}
```

SQS キュー

SQS と統合して、Tenable One Cloud Exposure 検出結果を SQS キューに送信します。

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

SQS キューの追加

SQS キューを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** に移動します。
2. (オプション)[組織]ドロップダウンで範囲を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで、**[SQS]** をクリックします。SQS ウィザードが開きます。
5. クラウドサイバーエクスポージャーに表示する**統合の名前を入力します**。
6. キューの **URL** を入力します。この URL は、AWS コンソールのキューのDetails セクションで確認できます。有効な形式 - https://sqs{region}.amazonaws.com/{account id}/{queue name}
7. **Tenableアクセス許可を付与します**。Tenable は IAM ロールを使用して、メッセージを SQS キューにプッシュします。AWS 環境を Tenable にオンボーディングしたときと同じロールを使用する (デフォルト) か、カスタムロールを作成します (オンボーディングされていないアカウントにキューがある場合など)。
    - **デフォルトのIAMロールを使用する:**
        1. AWS 管理コンソールで、**[IAM > Roles]** に移動します。
        2. AWS の概要した際に作成したロールを検索してクリッククラウドサイバーエクスポージャーします。
        3. ポリシーを編集するには、[アクセス許可] > [アクセス許可ポリシー] で、オンボーディング時に作成したモニタリング (読み取り専用) ポリシー名をクリックします。

4. JSON エディターで、次のアクセス許可を追加します:

   "SQS:SendMessage"

5. **[次へ]** をクリックします。
6. 変更を確認し、**[変更の保存]** をクリックします。
7. (**キューが KMS で暗号化されている場合**):
   1. AWS 管理コンソールで、**[KMS] > [カスタマーマネージドキー]** に移動します。
   2. 関連するキーをクリックし、[キーポリシー] セクションで **[編集]** をクリックします。
   3. JSON エディターで、次のステートメントをポリシーに追加し、**[変更の保存]** をクリックします。

```
JSON

 {
    "Sid": "Allow Read Access to Key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "<IAM Role ARN>"
    },
    "Action": [
     "kms:GenerateDataKey",
     "kms:Decrypt"
    ],
    "Resource": "*"
 }
```

- **カスタムIAMロールを使用する**:
  1. AWS マネジメントコンソールで、**[IAM] > [ロール]** の順に移動し、**[ロールを作成]** をクリックします。
  2. [信頼できるエンティティタイプ] については、**[AWS アカウント]** を選択します。
  3. AWS アカウントについては、**[別の AWS アカウント]** を選択し、お使いの AWS 環境タイプに応じて以下のいずれかの数字をアカウント ID として入力します。
     - パブリッククラウド: **081802104111**
     - US Gov クラウド: **757023926892**

> **注意:** これは Tenable のアカウント ID です。この ID は 12 桁です。余分なスペースが含まれないようにしてください。

4. [オプション] で、**[外部 ID が必要]** にチェックを入れます。
5. [Add SQS Queue] (SQS キューの追加) ウィザードで提供された**ロールの外部 ID** を入力します (Tenable コンソール)。

> **注意:** ロールの外部 ID は、クラウドサイバーエクスポージャーが顧客アカウントに割り当てる一意の識別子です。この ID は組織用に作成する各アカウントの ID と同一になります。詳細は、AWS IAM ドキュメントを参照してください。

6. **[次へ]** をクリックします。
7. [アクセス許可の追加] ページで、**[次へ]** をクリックします。
8. 意味のある **ロール名** と **説明** を入力し、**[ロールの作成]** をクリックします。
9. 新しく作成したロールを開き、[アクセス許可] で **[アクセス許可の追加] > [インラインポリシーの作成]** をクリックします。
10. 次のポリシーをコピーして **[JSON]** タブに貼り付け、既存のテキストを置き換えます。ここで、`{SQS_ARN}` は SQS キューの ARN です。

> **注意:** 以下のスニペットの `{SQS_ARN}` を SQS キューの ARN に置き換えます。この ARN は、AWS コンソールのキューの [Details] (詳細) セクションで確認できます。

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Effect": "Allow",
         "Action": [
             "sqs:SendMessage"
         ],
         "Resource": "{SQS_ARN}"
     }
 ]
}
```

11. **[次へ]** をクリックします。
12. 意味のある **ポリシー名** を入力し、**[ポリシーの作成]** をクリックします。
13. 作成したカスタムロールの **ARN** をコピーします。
14. (クラウドサイバーエクスポージャーコンソール) **IAM ロール ARN** を貼り付け、**完了** をクリックします
15. (**キューが KMS で暗号化されている場合**)
    1. AWS 管理コンソールで、**[KMS] > [カスタマーマネージドキー]** に移動します。
    2. 関連するキーをクリックし、[キーポリシー] セクションで **[編集]** をクリックします。
    3. JSON エディターで、次のステートメントをポリシーに追加し、**[変更の保存]** をクリックします。

```
JSON

 {
    "Sid": "Allow Read Access to Key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "<IAM Role ARN>"
    },
    "Action": [
     "kms:GenerateDataKey",
     "kms:Decrypt"
    ],
    "Resource": "*"
 }
```

JSON のサンプル

```
JSON

{
  "source": "Tenable",
  "action": "Create JIT eligibility",
  "details": {},
  "result": "Success",
  "scope": "Organization\\Azure AD",
  "time": "2024-06-25T10:21:23.7023655Z",
  "approvalRequired": true,
  "approvers": [
```

```
      "006"
    ],
    "requesters": [
      "003"
    ],
    "maxDurationHours": 21,
    "name": "More eligibilities for testing",
    "user": "***@customer1.onmicrosoft.com",
    "ticketLinks": [
      "https://tenablecustomer1.atlassian.net/browse/DAV-24140",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
    ],
    "comments": [
      {
        "message": "created a ServiceNow incident for this threat story",
        "time": "2026-07-29T09:00:13.124307Z",
        "userName": "Tenable"
      },
      {
        "message": "created a Jira ticket for this threat story",
        "time": "2026-07-29T09:00:05.609867Z",
        "userName": "Tenable"
      }
    ]
  }
```


Webhook

Webhook

イベントによってトリガーされたデータを HTTP Webhook を使って共有する場合、Webhook を使用する任意の宛先に Tenable One Cloud Exposure の検出結果を送信できます。たとえば、Webhook 接続を使用して、Tenable 検出結果を次の URL に送信できます。

- Microsoft センチネル
- Sumo Logic
- テレグラム

- ページャーデューティ
- 着信 Webhook をサポートするその他すべてのサービス

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Webhook の追加

Webhook を追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Integrations]** に移動し、**[Webhook]** をクリックします。
2. (オプション)[組織]ドロップダウンでアカウント範囲を選択します。
3. **[Add Webhook]** をクリックします。
4. クラウドサイバーエクスポージャーに Webhook **の名前を入力します**。
5. 宛先アプリケーションに属する **Webhook URL** を入力します。たとえば Sumo Logic では、これはコレクター API URL です。
6. コレクターで SSL が有効になっている場合は、**[すべてのサーバー SSL 証明書を受け入れる]** にチェックを入れます。
7. 追加の関連情報を含む HTTP ヘッダー **Name** と **Value** を Webhook が受信すると予想される場合は、追加します。
8. **[保存]** をクリックします。

Microsoft Sentinel (Webhook 経由)

イベントによってトリガーされたデータを HTTP Webhook を使って共有する場合、Webhook を使用する任意の宛先に Tenable One Cloud Exposure の検出結果を送信できます。

クラウドサイバーエクスポージャーデータを Microsoft Sentinel に送信するには、次の手順に従います。

1. Log Analytics ワークスペースを作成します。
2. ロジック アプリを作成する
3. Tenable で Sentinel Webhook 統合を作成する
4. 次のいずれかの方法で Webhook にデータを送信します。
    - 自動化
    - 検出結果に基づくアクションのトリガー
5. Microsoft Sentinel でデータを表示する

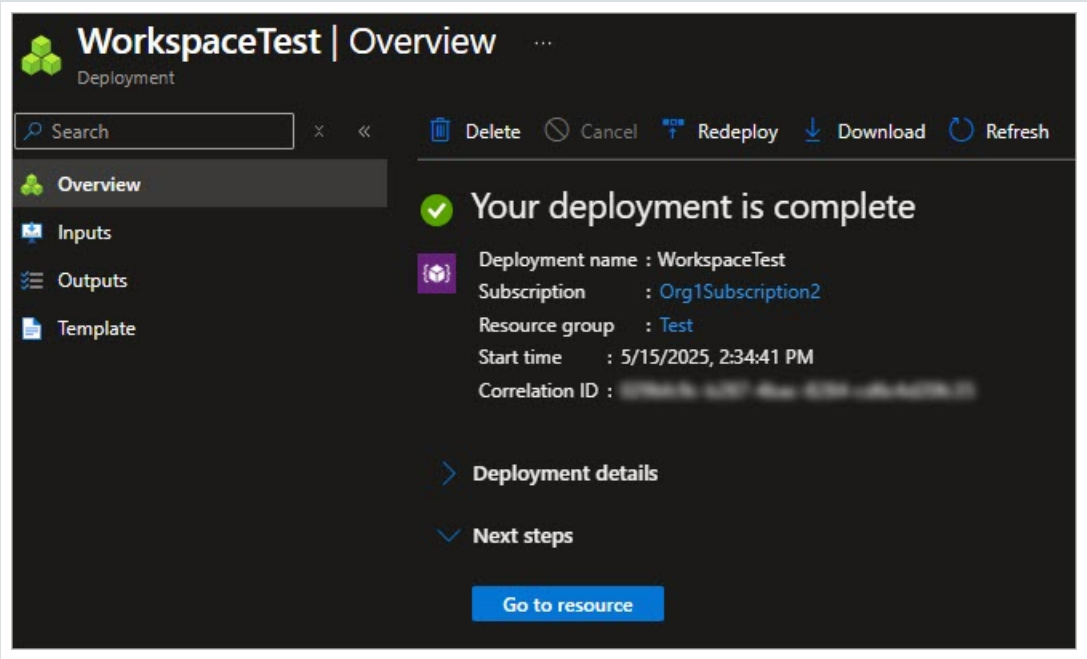
次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

ログ分析ワークスペースを作成する

Microsoft Sentinel でログアナリティクス ワークスペースを作成して、クラウド サイバーエクスポージャー データの保存先として使用します。

1. Azure ポータルにログインし、**Microsoft Sentinel** サービスに移動します。
2. **[作成]** をクリックします。
3. **[新しいワークスペースの作成]** をクリックします。
4. [プロジェクトの詳細] で、関連する **サブスクリプション** と **リソースグループ** を選択します。
5. [インスタンスの詳細] で、**[名前]** を入力し、**[リージョン]** を選択します。
6. **[レビュー + 作成]** をクリックし、**[作成]** をクリックします。
7. 新しいデプロイの [概要] ページで、**[リソースに移動]** をクリックします。



8. ワークスペースページで、**[Settings > Agents]** に移動します。
9. **[Log Analytics エージェントの指示]** セクションを展開し、後で必要になる次の値をコピーします。
    1. **ワークスペース ID**
    2. **プライマリキー**

ロジック アプリを作成する

仲介者として機能するように Azure Logic App を構成し、Tenable からデータを受け取り、それを Log Analytics ワークスペースに転送します。

1. Azure portal で、**ロジック アプリ** サービスに移動します。
2. **[追加]** をクリックします。
3. [ホスティング オプション] で、**[消費]** を選択します。
4. [プロジェクトの詳細] で、関連する **サブスクリプション** と **リソースグループ** を選択します。
5. [インスタンスの詳細] で、**[名前]** を入力し、**[リージョン]** を選択します。
6. **ログ分析を有効にするかどうか** を選択します。
7. 有効にした場合は、前に作成した **ログ アナリティクス ワークスペース** を選択します。
8. **[レビュー + 作成]** をクリックし、**[作成]** をクリックします。

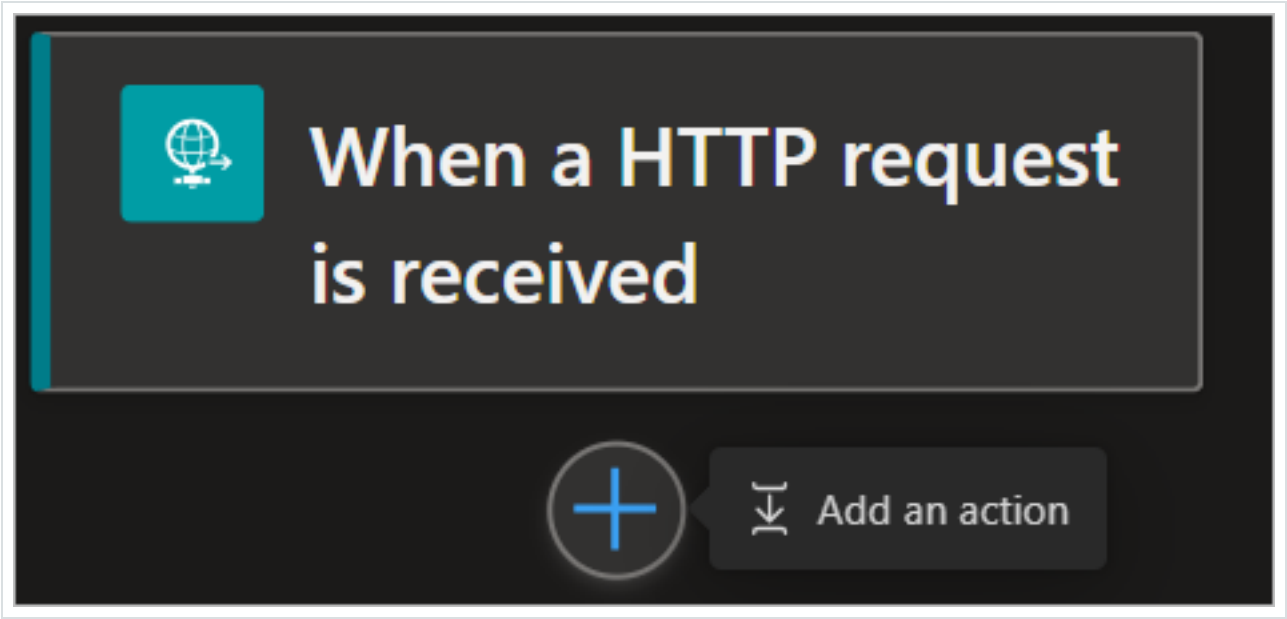
9. 作成したら、[デプロイの詳細] にある **[リソース]** リンクをクリックします。
10. ロジック アプリ リソース ページで、**開発ツール** > **ロジック アプリ デザイナー**に移動します。
11. **[トリガーの追加]** をクリックします。
12. **[HTTP リクエストを受信したとき]** アクションを検索して選択します。
13. 「リクエスト本文 JSON スキーマ」セクションで、「**サンプル・ペイロードを使用してスキーマを生成**」をクリックし、次のサンプル JSON をコピーして貼り付けて、「**完了**」をクリックします。

> JSON Schema

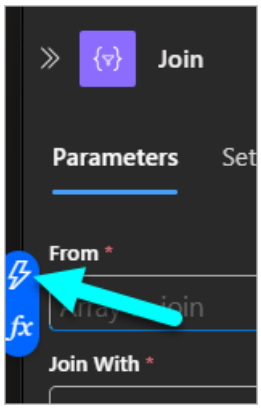
JSON

```
{
"accountId": "",
"accountName": "Org2Account2",
"creationTime": "2022-01-12T01:10:24.868Z",
"description": "User FindingsFixer には、2 つのサービスに対するアクセス許可を付与する 2 つのポリシーがアタッチされていますが、いずれも 68 週間使用されませんでした",
"findingType": "AwsExcessivePermissionUserFinding",
"id": "",
"link": "https://us.app.ermetic.com/risks/*",
"labels": [
"Admin",
"Access Keys",
"No MFA"
],
"resources": [
"arn:aws:iam:::user/FindingsFixer"
],
"severity": "High",
"source": "Ermetic",
"status": "Open",
"statusUpdateTime": "2022-05-21T22:16:44.785Z",
"title": "過剰な権限を持つ IAM ユーザー",
"type": "Finding"
}
```

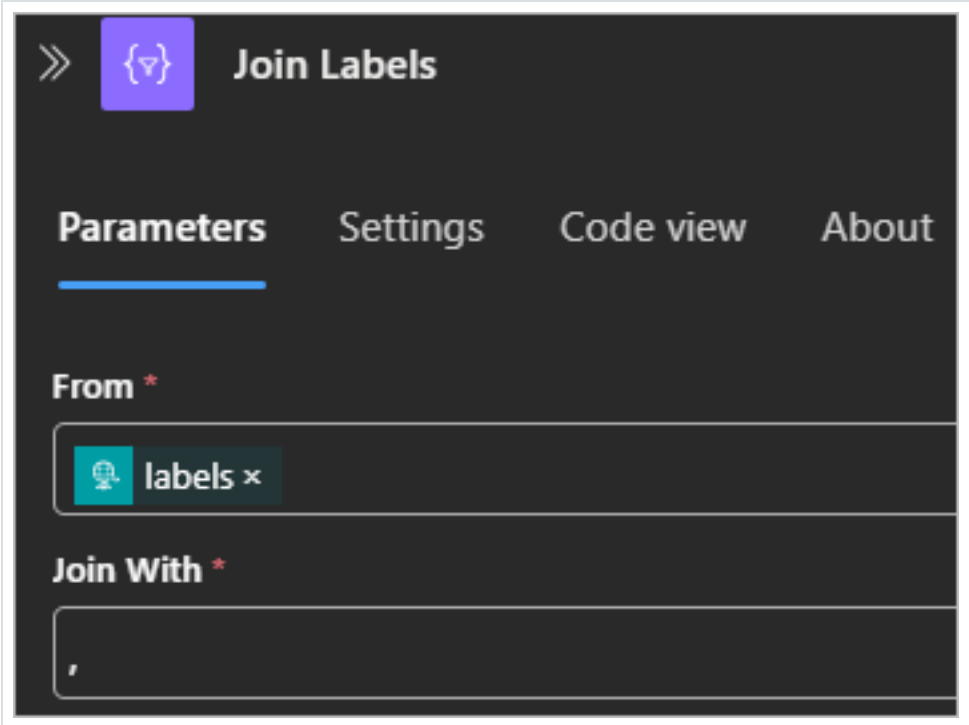
14. **[+]** をクリックし、**[アクションの追加]** をクリックして、デザイナーに新しいステップを挿入します。



15. 「**結合** (データ操作)」アクションを検索して選択します。
16. **[送信元]** フィールド内をクリックし、稲妻アイコンをクリックして、**ラベル**を選択します。



17. **[Join with]** フィールドにコンマ (,) を入力し、アクションの名前を **[Join Labels] に変更します**。



18. **[+]** をクリックし、**[アクションの追加]** をクリックして、デザイナーの [ラベルの結合] の後に新しいステップを挿入します。
19. 「**結合** (データ操作)」アクションを検索して選択します。
20. **[送信元]** フィールド内をクリックし、稲妻アイコンをクリックして、**リソース**を選択します。
21. 「**参加」フィールドにコンマ(,)**を入力し、アクションの名前を**「リソースの結合」**に変更します
22. 「**+**」をクリックし、「**アクションを追加」**をクリックして、「リソースの結合」の後にデザイナに新しいステップを挿入します。

23. **[データの送信** (Azure Log Analytics データコレクター)] アクションを検索して選択します。
24. 接続に関する次の詳細を入力し、**[新規作成]** をクリックします。
    - **接続名**。
    - **ワークスペース ID**。この手順で先ほどコピーした値を入力します。
    - **ワークスペースキー**。この手順の前半でコピーした値を入力します。

    > **注意:** 関連する Log Analytics ワークスペースの **[Settings > エージェント] > [Log Analytics エージェントの手順]** で利用できます。

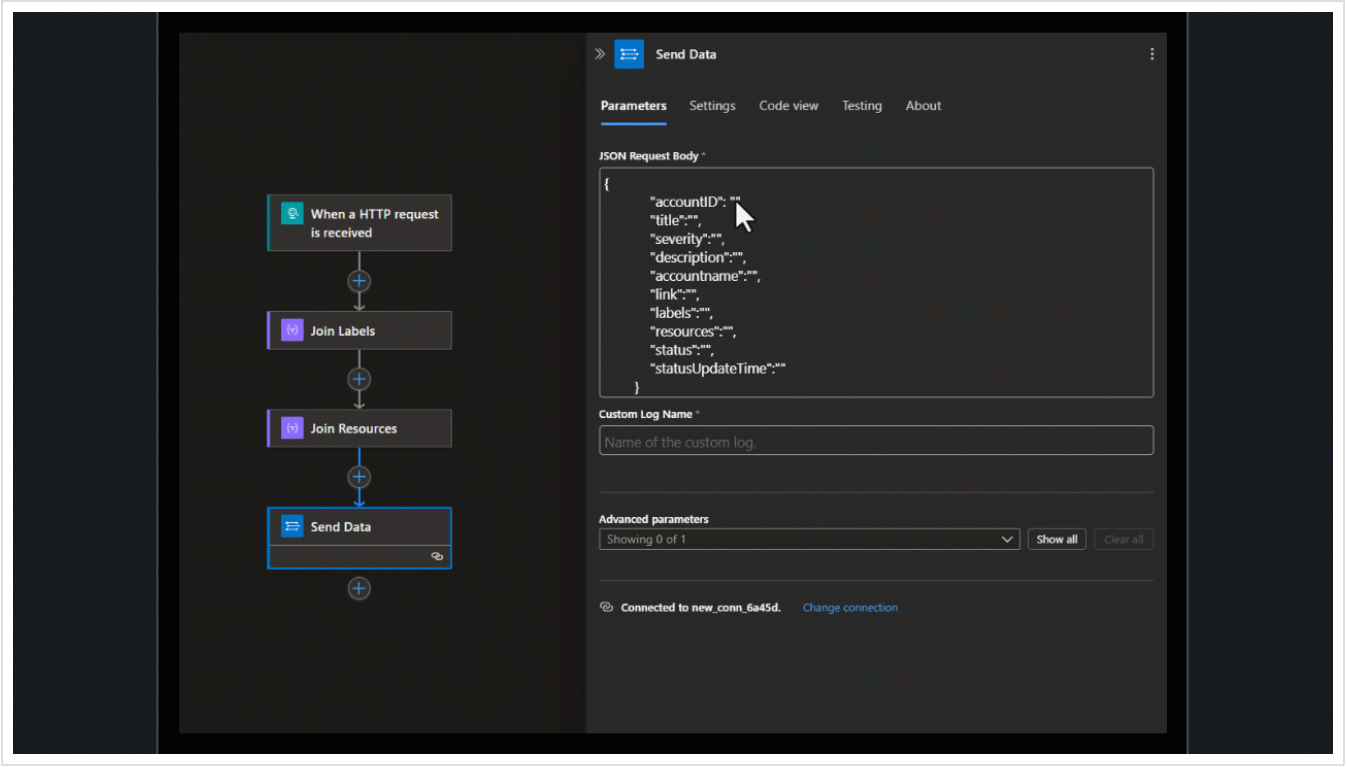
25. **[JSON リクエスト本文]** フィールドに、次の JSON コードスニペットを入力します。

    > JSON リクエスト本文

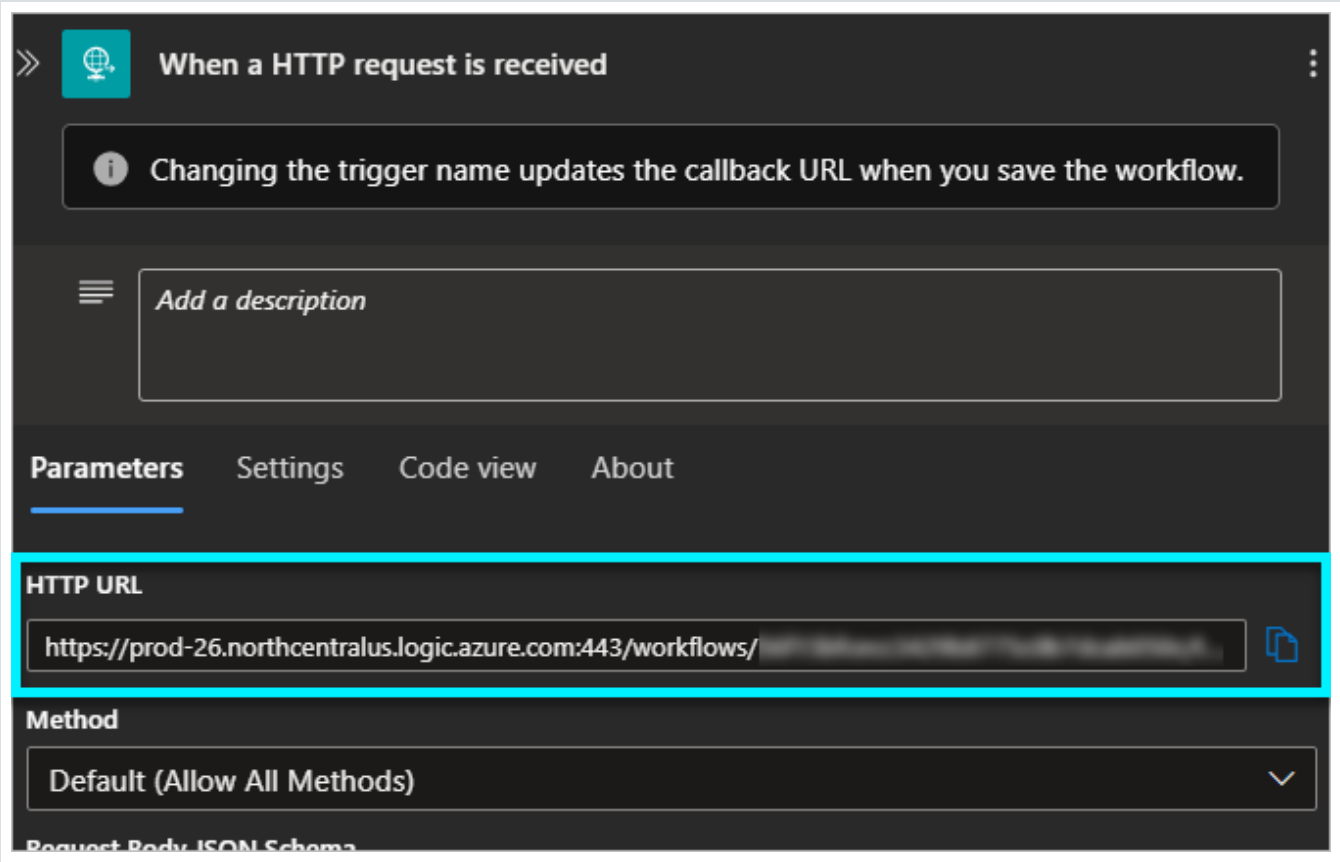
    JSON

```
{
"accountID": "",
"title":"",
"severity":"",
"description":"",
"accountname":"",
"link":"",
"labels":"",
"resources":"",
"status":"",
"statusUpdateTime":""
}
```

26. **JSON リクエスト本文** 内に、次に示すように、稲妻を使用してデータを引用符で囲み、前のステップの関連データを入力します。



27. 意味のある **カスタムログ名** を入力し、**[保存]** をクリックしてワークフローを保存します。
28. クリックして **[HTTP リクエスト受信時]** アクションを開き、**HTTP URL** をコピーします。



Tenable で Sentinel Webhook 統合を作成する

接続を確立するには、クラウドサイバーエクスポージャー内で Webhook 統合を作成し、セキュリティデータをロジックアプリに配信します。

Webhook 統合を作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Integrations]** に移動し、**[Webhook]** をクリックします。
2. **[Add Webhook]** をクリックします。
3. Tenable に Webhook **の名前を入力します**。たとえば、Sentinel Webhook です。
4. **[Webhook URL]** フィールドに、ロジックアプリの作成の最後の手順でコピーした HTTP URL を貼り付けます。

5. (オプション)コレクターで SSL が有効になっている場合は、**[すべてのサーバー SSL 証明書を受け入れる]** にチェックを入れます。
6. (オプション)追加の関連情報を含む Webhook がそのようなヘッダーを受信することを想定する場合は、**[名前]** と **[値]** (**HTTP ヘッダー**) に入力します。
7. **[保存]** をクリックします。

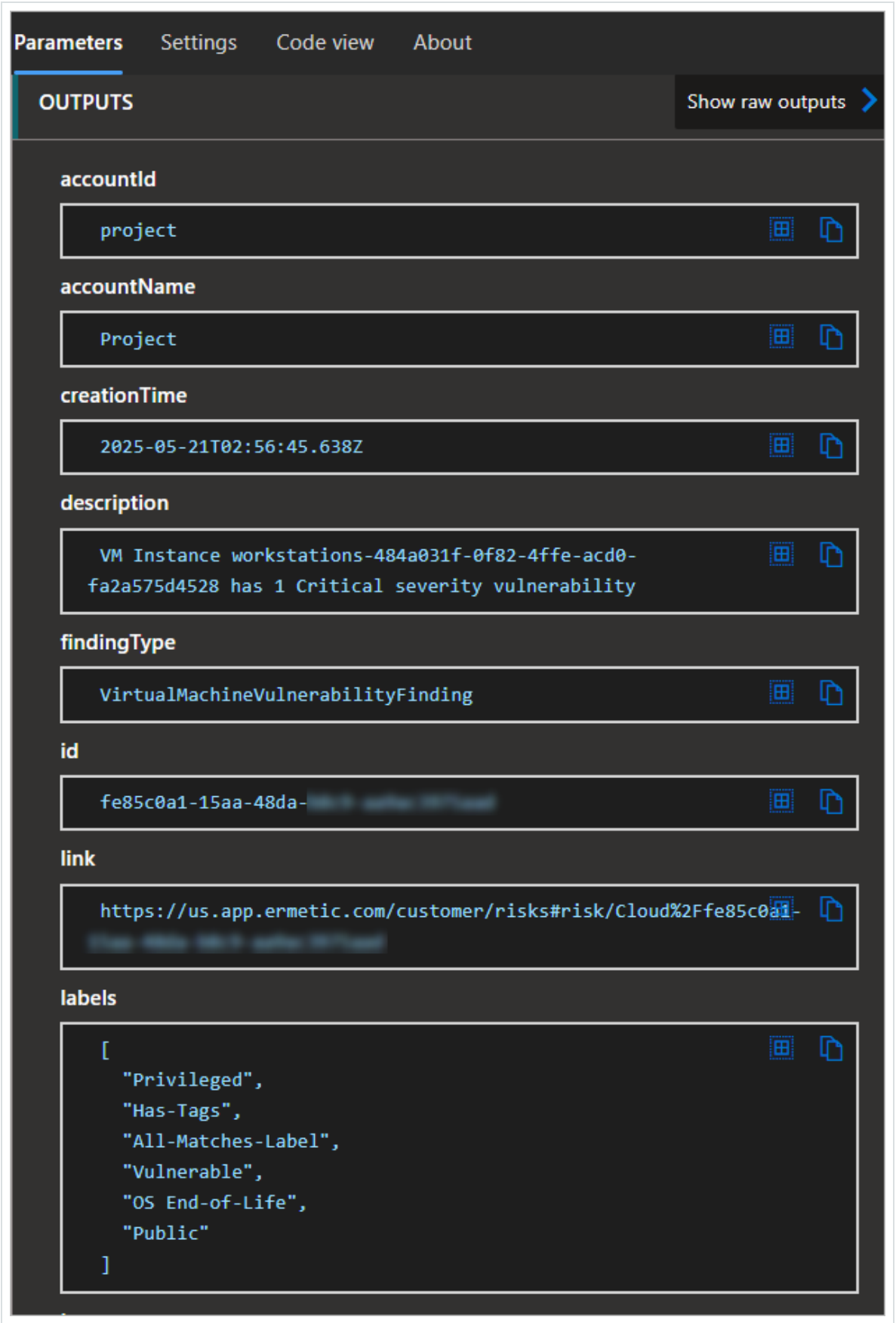
Microsoft Sentinel でデータを表示する

統合が成功したことを確認し、Microsoft Sentinel 内で直接 クラウド サイバーエクスポージャー データの分析を開始します。

Azure でデータを表示する方法

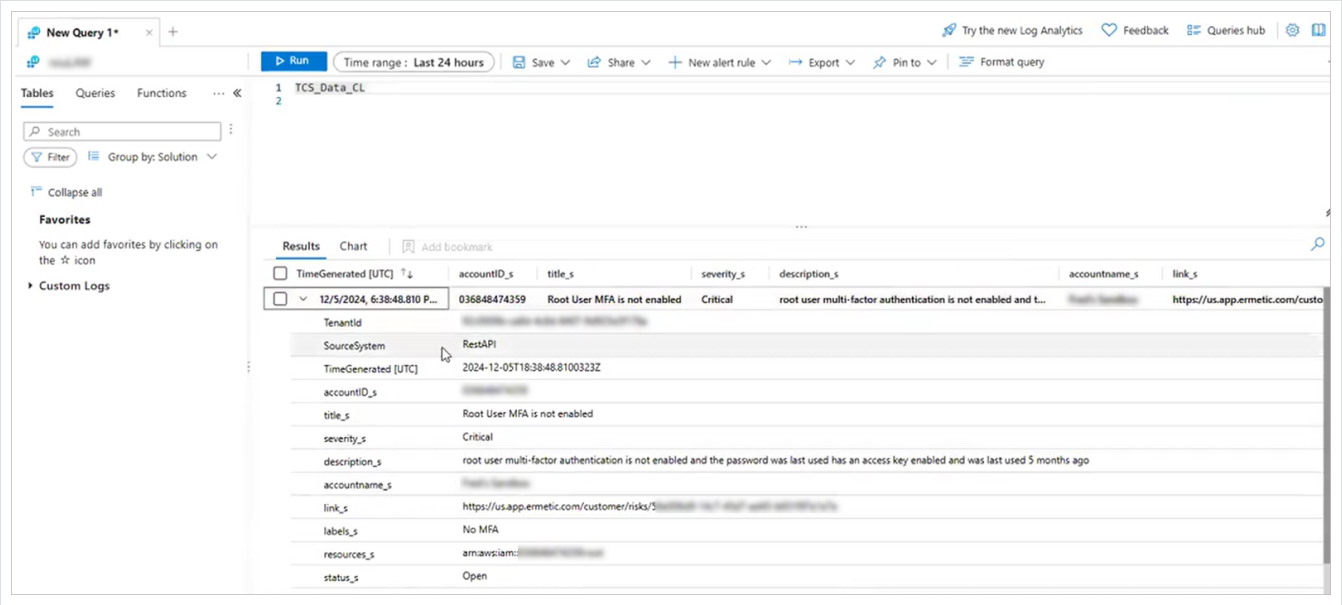
1. ロジックアプリでデータを確認します。
    1. Azure portal で、**ロジック アプリ** サービスに移動し、作成したロジック アプリを開きます。
    2. [概要] ページで、**[実行履歴]** タブに移動します。
    3. 実行 **識別子** をクリックします。
    4. 表示される実行 ワークフローで以下を行います。

- **[HTTPリクエストの受信時]** をクリックし、[パラメーター] タブで **[出力]** セクションまで下にスクロールすると、解析された出力が表示されます。


Parameters
Settings
Code view
About
OUTPUTS
Show raw outputs
accountId
project
accountName
Project
creationTime
2025-05-21T02:56:45.638Z
description
VM Instance workstations-484a031f-0f82-4ffe-acd0-fa2a575d4528 has 1 Critical severity vulnerability
findingType
VirtualMachineVulnerabilityFinding
id
fe85c0a1-15aa-48da-
link
https://us.app.ermetic.com/customer/risks#risk/Cloud%2Ffe85c0a1-
labels
[
"Privileged",
"Has-Tags",
"All-Matches-Label",
"Vulnerable",
"OS End-of-Life",
"Public"
]

- **[データの送信]** をクリックし、[パラメーター] タブで **[入力]** セクションまで下にスクロールすると、**JSON リクエスト本文** に出力全体が表示されます。

2. Microsoft Sentinel でデータを表示する:
    1. Azure portal で、**Microsoft Sentinel** サービスに移動します。
    2. 前に作成したワークスペースに移動し、**[ログ]** をクリックします。
    3. 新しいクエリ (KQL モード) で、ロジック アプリを作成したときに使用した**カスタム ログ名** を入力し、**[実行]** をクリックします。



Sumo Logic (Webhook 経由)

イベントによってトリガーされたデータを HTTP Webhook を使って共有する場合、Webhook を使用する任意の宛先に Tenable One Cloud Exposure の検出結果を送信できます。

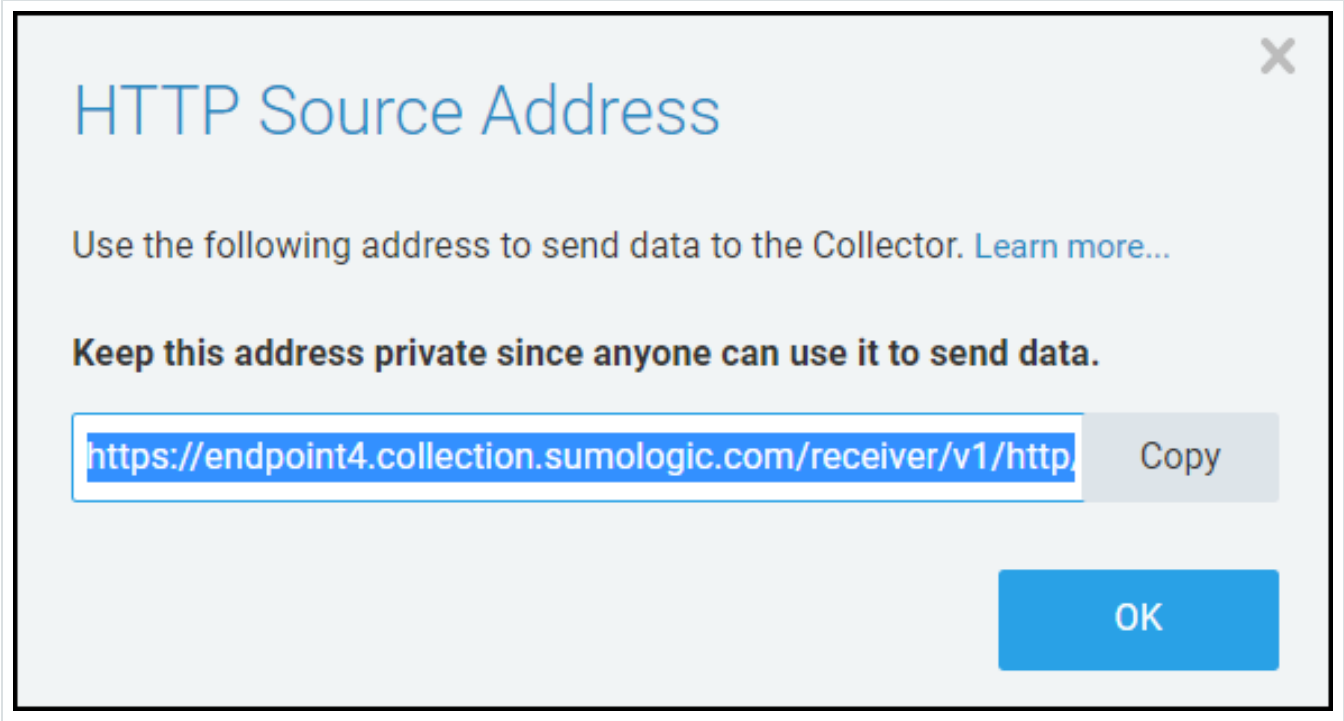
次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

Sumo Logic へのデータ送信

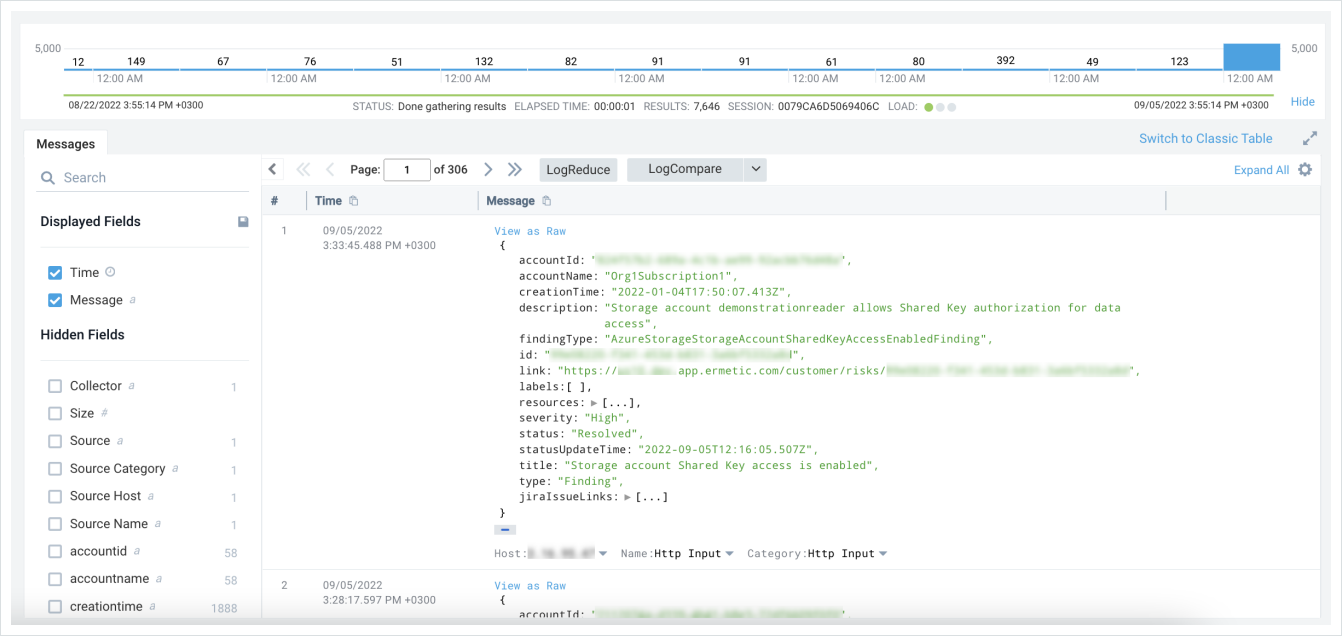
Sumo Logic にデータを送信する方法

1. Sumo Logic コンソールで、[データ>**コレクションの管理**] に移動します。
2. ホスト型コレクター用に **HTTP ログとメトリクス** ソースを設定します。詳細は、Sumo Logic のドキュメント を参照してください。
    - [メッセージ処理] 領域内の [ログの詳細オプション] セクションで、**[要求ごとに 1 つのメッセージ]** を選択します。これにより、クラウドサイバーエクスポージャー からの各メッセージは、1 つのメッセージが複数の行に分割 (マルチライン処理) されるのではなく、それぞれの行に表示されます。
3. すべての情報の入力が完了したら **[保存]** をクリックし、ダイアログボックスに表示される URL をコピーします。



4. クラウドサイバーエクスポージャー コンソールで、**[Settings > Integration > Webhooks]** に移動し、**[Lets Start]** をクリックします。
5. Tenable で Webhook の**表示名**を入力します。
6. 前の手順で Sumo Logic からコピーした **Webhook URL** を入力します。

7. コレクターで SSL が有効になっている場合は、**[すべてのサーバー SSL 証明書を受け入れる]** にチェックを入れます。
8. 追加の関連情報を含む HTTP ヘッダー **Name** と **Value** を Webhook が受信すると予想される場合は、追加します。
9. **[保存]** をクリックします。
10. Tenable データを Sumo Logic で表示するには、Sumo Logic コンソールに移動して、上記で定義したソース名とコレクター名を検索します。



JSON のサンプル

JSON


```
{
  "accountId": "************",
  "accountName": "Org2Account2",
  "creationTime": "2022-01-12T01:10:24.868Z",
  "description": "User FindingsFixer has 2 policies attached granting it permissions on 2 services, but none of them were used for 68 weeks",
  "findingType": "AwsExcessivePermissionUserFinding",
  "id": "**********************************",
  "link": "https://us.app.ermetic.com/risks/**********************************",
  "labels": [
    "Admin",
```

```
    "Access Keys",
    "No MFA"
  ],
  "resources": [
    "arn:aws:iam::***********:user/FindingsFixer"
  ],
  "severity": "High",
  "source": "Ermetic",
  "status": "Open",
  "statusUpdateTime": "2022-05-21T22:16:44.785Z",
  "title": "Overprivileged IAM user",
  "type": "Finding"
}
```


Telegram (Webhook 経由)

Telegram と統合して、Tenable One Cloud Exposure 検出結果を Webhook 経由で Telegram に送信します。次の手順を実行して統合を完了します。AWS を仲介として使用して、Teams で読み取れるように Tenable データを変換します。

次の手順

- 検出結果のデータ送信を開始するには、自動化を設定するか、統合を追加した後に検出結果に基づくアクションのトリガーする必要もあります。すべての統合ステップを正常に完了しても、それ自体ではデータ送信はトリガーされません。

BotFather で新しい Telegram ボットを作成する

ボットを Telegram に接続する前に、BotFather で Telegram ボットを作成します。

> **注意:** これらの手順のほとんどは Telegram アプリで実行できますが、最後の手順では Telegram Web を使用する必要があります。

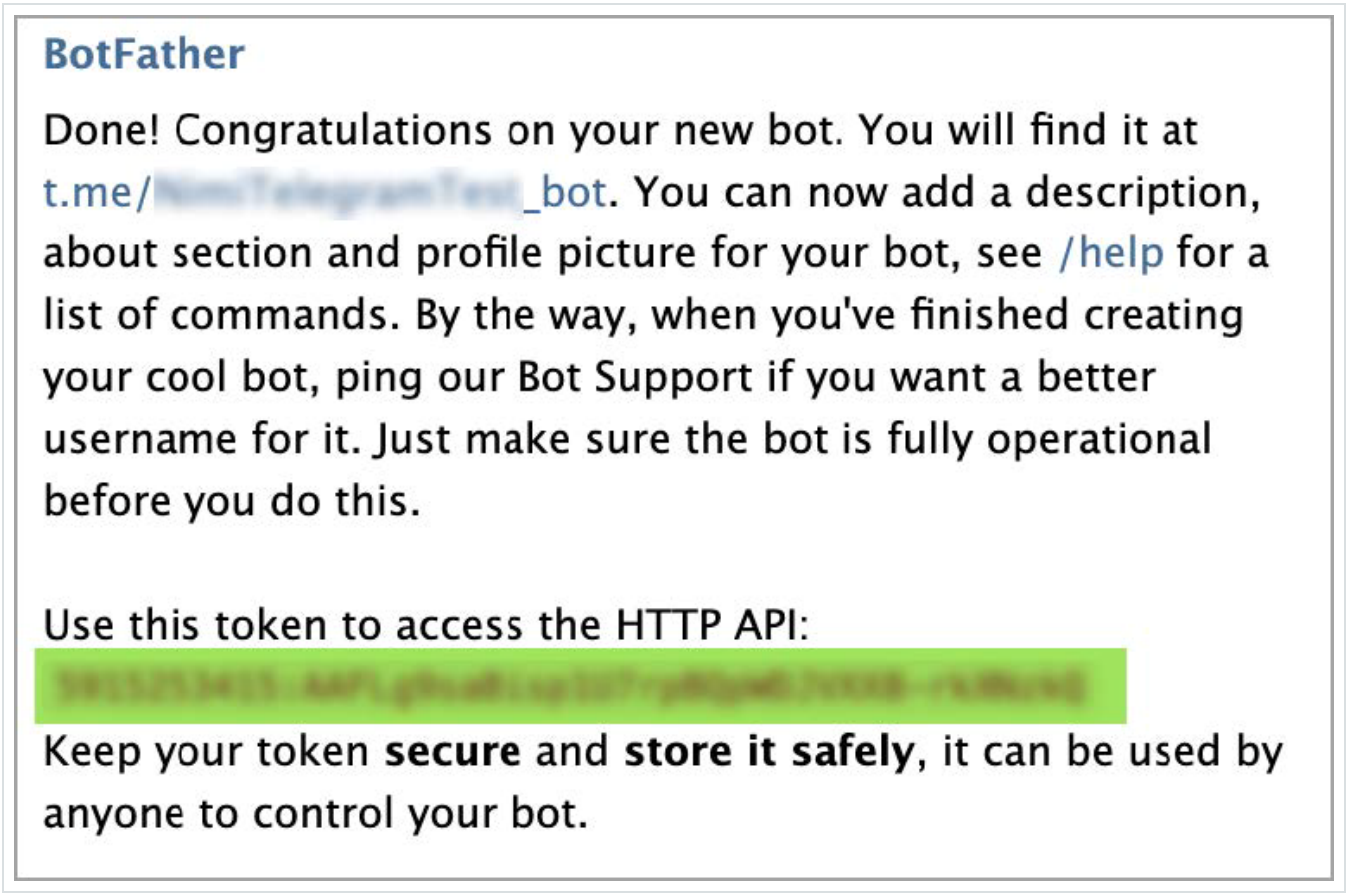
1. Telegram で、BotFather との新しい会話を開始します。
2. 次のメッセージを送信して、新しい Telegram ボットを作成します。

   ```
   /newbot
   ```

3. プロンプトが表示されたら、ボットの名前を入力します。Telegram ボットに一意のユーザー名を付けます。

   > **注意:** ボット名は「bot」という単語で終わる必要があります (大文字と小文字は区別しません)。

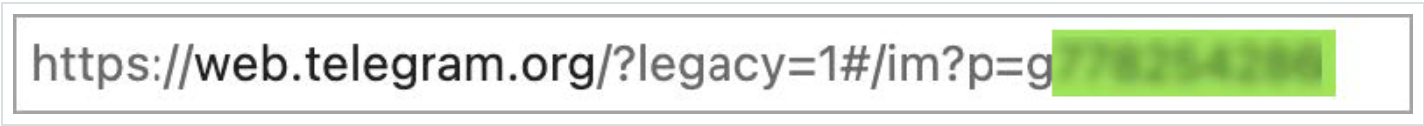
4. 後の手順で使用するため、Telegram ボットのアクセストークンをコピーして保存します。



5. (オプション)ボットのプロファイル画像を設定します (たとえば、Tenable ロゴを使用するなど)。
   - `/setuserpic`のメッセージを BotFather に送信します。
   - Tenable用に作成したボットを選択します。
   - プロファイル画像を送信します。
6. Telegram で新しいグループを作成します。
7. 前に作成したボットを選択し、関連するユーザーを追加します。
8. (オプション)グループに名前を付けて画像を追加し、**[作成]** をクリックします。

9. Telegram Web で、新たに作成したグループをクリックします。ブラウザの URL で、チャット ID (文字「g」の後に表示される数字) を特定して保存します。後で使用するため、この値を保存します。

> **注意:** ここまでの手順は Telegram アプリで実行できますが、この手順では Telegram Web を使用する必要があります。



AWS を使用した CloudFormation スタックの作成

次の手順を実行して、AWS を使用して検出結果ペイロードを Tenable から Telegram 通知に適した形式に解析します。

- SSM パラメーターを設定する
- CloudFormation スタックの作成

SSM パラメーターを設定する

SSM パラメーターを設定する方法

1. AWS コンソールで、**Systems Manager** > **パラメーターストア**に移動します。
2. **[パラメーターの作成]** をクリックし、次の詳細を入力します。
    - 名前: **TelegramErmeticToken**

      > **重要:** 統合を機能させるには、名前を正確に入力する必要があります。

    - 階層: **Standard**
    - 入力: **SecureString**
    - KMS キーソース: デフォルト値のままにします
    - データタイプ: **テキスト**
    - 値: 前に設定した Telegram **ボットアクセストークン**を入力します
3. **[パラメーターの作成]** をクリックします。

4. **[パラメーターの作成]** をクリックして別のパラメーターを追加し、次の詳細を入力します。
    - 名前: **TelegramErmeticChatID**

      > **重要:** 統合を機能させるには、名前を正確に入力する必要があります。

    - 階層: **Standard**
    - 入力: **SecureString**
    - KMS キーソース: デフォルト値のままにします
    - データタイプ: **テキスト**
    - 値: 前に設定した Telegram **チャット ID** を入力します
5. **[パラメーターの作成]** をクリックします。

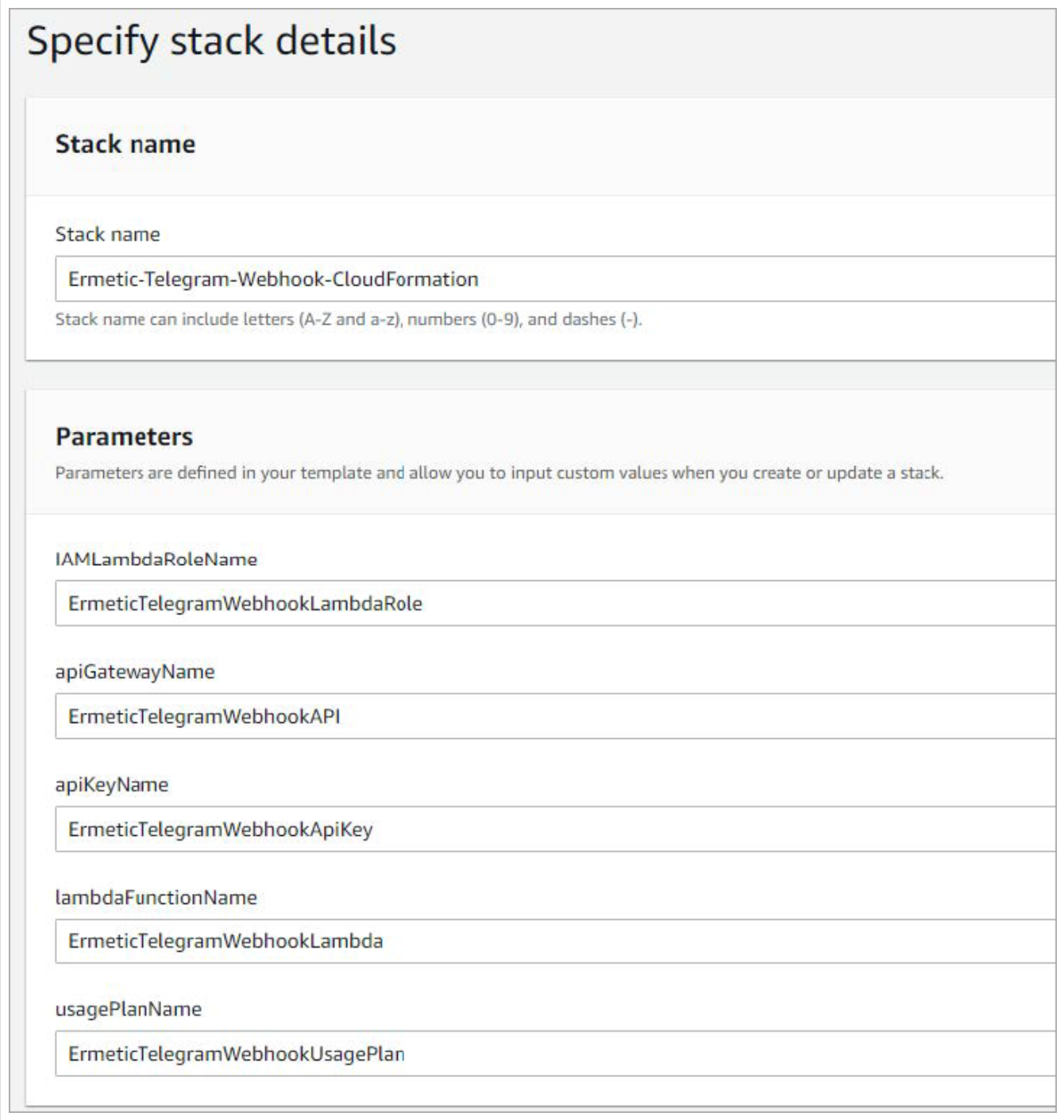
CloudFormation スタックの作成

サポートへの問い合わせ。この手順で必要となる次のファイルを取得します。

- CloudFormation テンプレートファイル
- lambda 関数用の .zip ファイルデプロイメントパッケージ

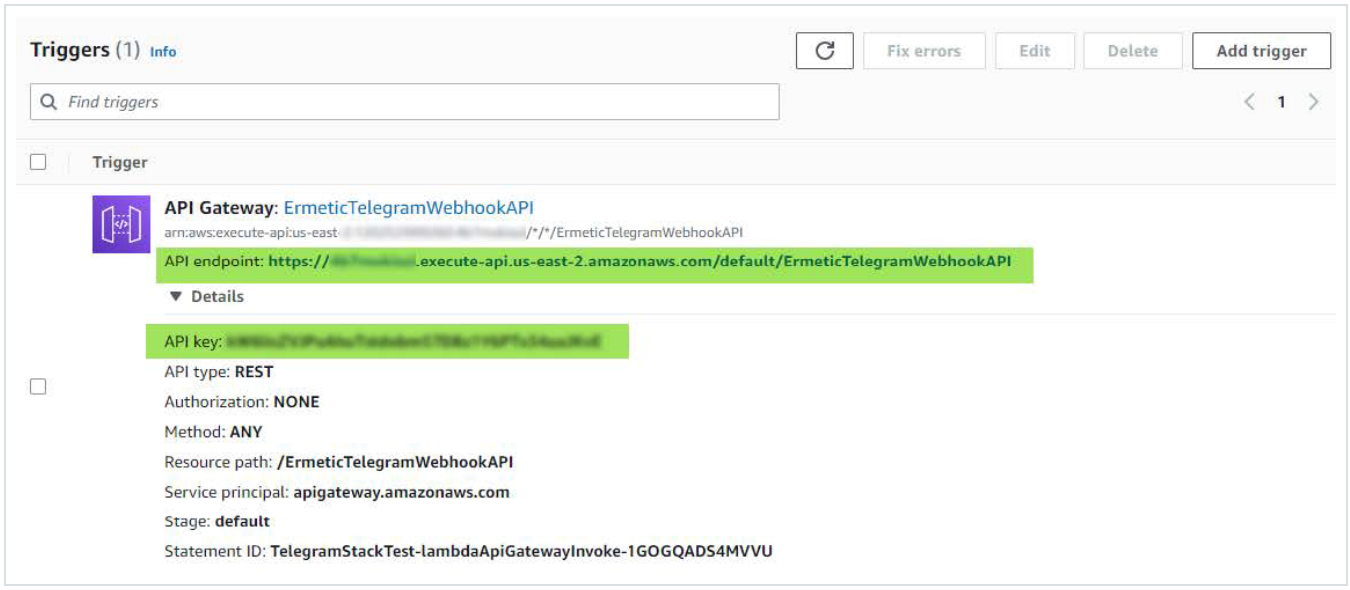
CloudFormation スタックを作成する方法

1. AWS コンソールで、**[CloudFormation]** > **[スタック]** に移動し、**[スタックの作成 (新しいリソースを使用可能 - 標準)]** をクリックします。[Create stack] (スタックの作成) ウィザードが開きます。
2. 前提条件 - テンプレートの準備 セクションで、**テンプレートの準備ができています** を選択します。
3. [テンプレートの指定] セクションで、**[テンプレート ファイルのアップロード]** を選択し、**[ファイルの選択]** をクリックして、テクニカル サポートから提供されたテンプレート ファイルをアップロードします。
4. **[次へ]** をクリックします。
5. クラウド形成スタックの **スタック名** を入力します。例: Tenable-Telegram-Webhook-CloudFormation。
6. (オプション) スタックはいくつかのリソース (Lambda 関数、API ゲートウェイ、IAM ロール、API キー) を作成します。リソースの名前を変更するか、デフォルト名を使用できます。**[次へ]** をクリックします。



7. [スタック オプションの構 成] ページで、**[次 へ]** をクリックします (このページには、当 面 のタスクを完 了するために必 須 のフィールド はありません)。
8. [Review] (レビュー) ページで、ページ下 部 のチェックボックス (AWS CloudFormation がカスタム名 で IAM リソースを作 成 する場 合 があることを承 認します) を確 認し、[Submit] (**送 信**) をクリックします。

9. スタックの作成が完了したら **[Resources]** タブに移動し、Lambda関数の **物理ID** リンクをクリックします。
10. **[コード]** タブに移動し、[コード ソース] セクション **> [.zip ファイルからアップロード]** をクリックし、テクニカル サポートから提供されたErmetic_Telegram_lambda_code .zip ファイルをアップロードします。
11. [Configuration] (**構成**) タブに移動します。次のステップのこのタブから、Lambdaトリガー情報を入力する必要があります。
12. APIゲートウェイトリガーを見つけ、**[詳細]** をクリックして追加情報を表示します。次のステップのTenable で Webhook 統合を作成するときに必要になるため、API エンドポイントとAPI キーをコピーして保存します。

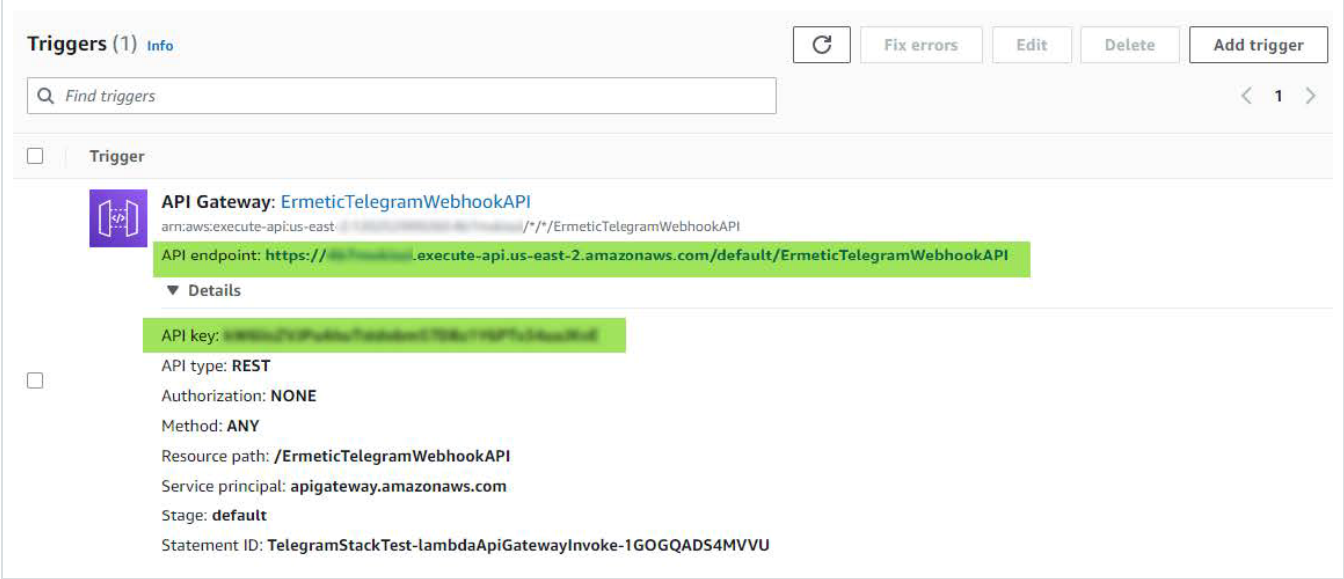


Tenable で Telegram Webhook 統合を作成する

Webhook 統合を作成する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Integrations]** に移動し、**[Webhook]** をクリックします。
2. **[開始]** をクリックします。
3. Tenable で Webhook の**表示名**を入力します。例: Telegram Webhook。

4. **Webhook URL** には、CloudFormation スタックの作成ときに作成されたラムダトリガーの API ゲートウェイの API エンドポイント URL を入力します。
5. **[HTTP ヘッダー]** で、次の詳細を入力します。
    - 名前: **x-api-key**
    - 値: CloudFormation スタックの作成ときに作成された、Lambda トリガーの API ゲートウェイの API キーを入力します。



6. **[保存]** をクリックします。

    自動化を作成したり、手動でアクションを検出結果に基づくアクションのトリガーしたりして、クラウドサイバーエクスポージャー検出結果データを Webhook 経由で Telegram に送信できるようになりました。

データリソースの接続

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

所定のアカウントでデータ保護を有効にするには、アカウントを Tenable One Cloud Exposure に接続し、そのアカウントのアクセス許可を Tenable データ保護に付与する必要があります。この機能は、次のクラウドプロバイダーに対して有効にできます。

- AWS: データ保護アクセス許可の付与
- Azure: データ保護アクセス許可の付与
- GCP: データ保護アクセス許可の付与
- OCI: データ保護アクセス許可の付与
- Snowflake: データ保護アクセス許可の付与

AWS: データ保護アクセス許可の付与

> **必要なライセンス:** このプロバイダーのデータスキャンは **Standard** と **Enterprise** ライセンスで利用できます。詳細については、ライセンスを参照してください。

Tenable IAM ロールに追加されたカスタムのインラインポリシーを通じてデータリソースをスキャンするため、クラウドサイバーエクスポージャーにアクセス許可を付与します。これらのアクセス許可は、Tenable ウィザードでの AWS 統合プロセスの一環として、データリソーススキャンのアクセス許可を通じて付与されていますが、アカウントを接続した時期によっては、まだ付与されていない場合もあります。

- 機密データのスキャンを行う AWS アカウントをすでに接続しているものの、データリソーススキャンのアクセス許可がまだ追加されていない場合は、以下の手順を実行します。
- 機密データのスキャンを行う AWS アカウントをまだ接続していない場合は、AWS の概要に記載されている手順を実行します。

データリソーススキャンのアクセス許可がすでに追加されているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **[設定] > [AWS]** の順に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [接続に問題あり] で、ツールチップにデータ保護のアクセス許可が付与されていないことが示されている場合は、以下の手順を実行します。

データ保護アクセス許可を付与する方法

1. クラウドサイバーエクスポージャーコンソールで **[設定] > [アカウント] > [AWS]** の順に移動します。
2. 関連するアカウントを見つけて、**[編集]** をクリックします。

3. ウィザードのステップ 2 (アクセス許可) に移動し、**データリソーススキャン (データ保護)** のアクセス許可を有効にして、**[次へ]** をクリックします。
4. ステップ 3 (IAM ロール) で、**データリソーススキャンのアクセス許可ポリシー (データ保護)** のインラインポリシーをコピーします。
5. 関連するアカウントの AWS マネジメントコンソールで、**[IAM] > [ロール]** に移動し、Tenable 用にアカウント統合の際に作成したロールを開きます。
6. [アクセス許可] タブで、**[アクセス許可の追加] > [インラインポリシーの作成]** の順にクリックします。
7. 先ほどコピーしたポリシーを [JSON] タブに貼り付けて、既存のテキストを置き換えます。JSON 形式でポリシーを表示するには、AWS データ保護ポリシー 参照してください。
8. **[ポリシーのレビュー]** をクリックします。
9. ポリシーの名前 (例: TenableDataProtection) を入力して、**[ポリシーを作成]** をクリックします。
10. クラウドサイバーエクスポージャーコンソールで、**[アカウント] > [AWS]** の順に移動し、アカウントのステータスが [接続済み] であることを確認します。

注意: ステータスが [接続済み] に変わるまで数分かかる場合があります。またブラウザでハードリフレッシュの実行が必要になる場合もあります。

AWS データ保護ポリシー

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:Scan",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBSnapshot",
        "rds:CreateDBClusterSnapshot",
```

```
        "rds:CreateDBSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBSnapshotAttribute",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "rds:AddTagsToResource",
      "Resource": [
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:cluster-snapshot:*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/TenableContext": "DataAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "rds:DeleteDBSnapshot",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:snapshot-tag/TenableContext": "DataAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "rds:DeleteDBClusterSnapshot",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rds:cluster-snapshot-tag/TenableContext": "DataAnalysis"
        }
      }
    }
  ]
}
```

Azure: データ保護アクセス許可の付与

必要なライセンス: このプロバイダーのデータスキャンは **Standard** と **Enterprise** ライセンスで利用できます。詳細については、ライセンスを参照してください。

以下のロールを通じてストレージアカウント Blob コンテナ内の機密データをスキャンするため、クラウド サイバーエクスポージャー にアクセス許可を付与します。

- ストレージ Blob データ閲覧者の組み込みロール
- Tenable データスキャンのカスタムロール
    - ネットワーク制限のあるストレージアカウント Blob コンテナの場合、Tenable はプライベートエンドポイントを使用して、保存されたオブジェクトにアクセスします。このアクセス許可は、Tenable によって開始された保留中のプライベートエンドポイント接続リクエストを承認するために必要です。このアクセス許可は、[設定] ページでデータが有効になっている場合にのみ使用されます。
    - Azure 承認ロックが設定されている場合、そのようなネットワーク制限を持つストレージアカウントのデータスキャンはサポートされません。ロックは、ストレージアカウント、リソースグループ、サブスクリプションの各レベルで適用が可能です。このような場合、Tenable はスキャン後に接続を削除できません。スキャンを有効にするには、ロックを解除します。

これらのアクセス許可は、Tenable ウィザードでの Azure 統合プロセスの一環として付与されていますが、組織またはプロジェクトを接続した時期によっては、まだ付与されていない場合もあります。

- 機密データのスキャンを行う Azure サブスクリプションをすでに接続しているものの、データ保護スキャンのアクセス許可がまだ追加されていない場合は、以下の手順を実行します。
- 機密データのスキャンを行う Azure サブスクリプションをまだ接続していない場合は、Azure の概要に記載されている手順を実行します。

データ保護のアクセス許可がすでに追加されているかどうかを確認するには、クラウド サイバーエクスポージャー コンソールで **[アカウント] > [Azure]** の順に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [データ保護のアクセス許可が付与されていません] の場合は、以下の手順に従って不足しているアクセス許可を追加します。

データ保護アクセス許可を付与する方法

1. Azure ポータルで、接続するものに応じて次のいずれかに移動します。
    - **組織**: 組織のルート **[管理グループ]** ページ。
    - **サブスクリプション**: **[サブスクリプション]** ページで、該当のサブスクリプションをクリックします。
2. カスタムロールの作成
    1. **[アクセス制御 (IAM)]** をクリックして、**[追加] > [カスタムロールの追加]** の順にクリックします。
    2. [カスタムロール名] には、**Tenable データスキャン**を入力します。
    3. [ベースラインのアクセス許可] では、**[最初から始める]** を選択して **[次へ]** をクリックします。
    4. **[アクセス許可の追加]** をクリックし、以下のアクセス許可を検索して選択します。
        - `Microsoft.Storage/storageAccounts/privateEndpointConnections/write`
        - `Microsoft.Sql/servers/databases/write`
    5. [アクション] で `Write : Put Private Endpoint Connection` を選択し、**[追加]** をクリックします。
    6. カスタムロールの作成を終了します。
3. ロールの割り当てを追加します。**各ロールに対して**以下の手順を実行して、`Storage Blob Data Reader` ビルトインロールと `Tenable Data Scanning` カスタムロールの両方を クラウド サイバーエクスポージャー Connector アプリに割り当てます。
    1. **[アクセス制御 (IAM)]** をクリックして、**[追加] > [ロールの割り当ての追加]** の順にクリックします。
    2. [ロールの割り当ての追加] ページで、以下のいずれかのロールを検索して選択し、**[次へ]** をクリックします。
        - `Storage Blob Data Reader` 組み込みロール
        - `Tenable Data Scanning` カスタムロール
    3. [アクセスの割り当て先] は、デフォルトの選択 **[ユーザー、グループ、またはサービスプリンシパル]** のままにします。
    4. [メンバー] で、**[+ メンバーを選択する]** をクリックします。
    5. **クラウド サイバーエクスポージャー コネクタアプリ**を検索して選択し、**[選択]** をクリックします。

6. **[次へ]** をクリックし、新しいロールを確認して **[レビューと割り当て]** をクリックします。
7. 他のロールに対してもこの手順を繰り返します。

4. クラウドサイバーエクスポージャーコンソールで、**[アカウント] > [Azure]** の順に移動し、アカウントのステータスが [接続済み] であることを確認します。

GCP: データ保護アクセス許可の付与

> **必要なライセンス:** このプロバイダーのデータスキャンは **Standard** と **Enterprise** ライセンスで利用できます。詳細については、ライセンスを参照してください。

機密データについて、カスタムポリシーを通じてストレージバケット内のオブジェクトをスキャンするためのアクセス許可をクラウドサイバーエクスポージャーに付与します。これらのアクセス許可は、Tenable ウィザードでの GCP 統合プロセスの一環として付与されていますが、組織またはプロジェクトを接続した時期によっては、まだ付与されていない場合もあります。

- 機密データのスキャンを行う GCP の組織またはプロジェクトをすでに接続しているものの、データ保護のアクセス許可がまだ追加されていない場合は、以下の手順を実行します。
- 機密データのスキャンを行う GCP の組織またはプロジェクトをまだ接続していない場合は、GCP の概要に記載されている手順を実行します。

データ保護のアクセス許可がすでに追加されているかどうかを確認するには、クラウドサイバーエクスポージャーコンソールで **[アカウント] > [GCP]** の順に移動し、アカウントのステータスを確認します。

- ステータスが [接続済み] の場合、必要なアクセス許可はすでに付与されています。
- ステータスが [データ保護のアクセス許可がありません] の場合は、以下の手順に従って不足しているアクセス許可を追加します。

データ保護アクセス許可を付与する方法

1. 関連する環境の GCP コンソールで、**[組織]** スコープに移動します。
2. 左上にある三本線メニューをクリックして、**[IAM と管理] > [ロール]** の順にクリックします。
3. テーブルフィルターに、最初の GCP 統合の際に使用したサービスアカウントのメールアドレスを入力します。

4. **[ロールを作成]** をクリックします
5. **[タイトル]** を「Tenable データスキャン」に変更します。
6. **[ID]** を「tenabledatascanning」に変更します。
7. **[アクセス許可を追加する]** をクリックします。
8. 以下の各アクセス許可について、フィルターを使用してアクセス許可を検索して選択し、**[追加]** をクリックします。
    - bigquery.datasets.get
    - bigquery.datasets.getIamPolicy
    - bigquery.models.export
    - bigquery.models.getData
    - bigquery.models.getMetadata
    - bigquery.models.list
    - bigquery.routines.get
    - bigquery.routines.list
    - bigquery.tables.createSnapshot
    - bigquery.tables.export
    - bigquery.tables.get
    - bigquery.tables.getData
    - bigquery.tables.getIamPolicy
    - bigquery.tables.list
    - bigquery.tables.replicateData
    - cloudsql.backupRuns.create
    - cloudsql.backupRuns.delete
    - cloudsql.backupRuns.get
    - cloudsql.backupRuns.list
    - cloudsql.instances.get

- dataplex.projects.search
- resourcemanager.projects.get
- resourcemanager.projects.list
- storage.folders.get
- storage.folders.list
- storage.managedFolders.get
- storage.managedFolders.list
- storage.objects.get
- storage.objects.list

9. 完了したら、**[作成]** をクリックします
10. サービスアカウント名をクラウドサイバーエクスポージャーコンソールから取得します：
    1. クラウドサイバーエクスポージャーコンソールで **[設定] > [統合] > [GCP 組織]** の順に移動し、関連する組織を見つけて、三点リーダーメニューで **[編集]** をクリックします。
    2. 表示されたウィザードで、**[次へ]** をクリックして、ステップ 4 (ロールの割り当て) に移動します。
    3. **[手動 (Google Clou d Console)]** タブをクリックします。
    4. 表示されたサービスアカウントの値をコピーします。
11. GCP コンソールで、左側のメニューにある **[IAM]** をクリックします。
12. **[+アクセスを許可]** をクリックします。
13. **[プリンシパルの追加]** セクションで、コピーしたサービスアカウントの値を貼り付けます。
14. [ロールの割り当て] セクションで、先ほど作成したカスタムロールをフィルタリングして選択します。
15. **[保存]** をクリックします。

OCI: データ保護アクセス許可の付与

> **必要なライセンス:** このプロバイダーのデータスキャンは **Standard** と **Enterprise** ライセンスで利用できます。詳細については、ライセンスを参照してください。

オブジェクトストレージリソースの機密データをスキャンするためにクラウドサイバーエクスポージャーにアクセス許可を付与するには、標準のOCIテナンシの接続プロセスを完了します。統合の後に、追加のロール、ポリシー、またはアクセス許可の付与は必要ありません。

統合後、必要なアクセス許可が付与されていることを確認します。クラウドサイバーエクスポージャーコンソールで、**[設定] > [アカウント] > [OCI]** の順に移動し、アカウントのステータスが [接続済み] であることを確認します。これは、必要なアクセス許可がすべて正常に適用されたことを示します。これ以上のアクションは必要ありません。

Snowflake: データ保護アクセス許可の付与

> **必要なライセンス:** このプロバイダーのデータスキャンは **Enterprise** ライセンスで利用できます。詳細については、ライセンスを参照してください。

Snowflake でデータをスキャンするためのアクセス許可をクラウドサイバーエクスポージャーに付与するには、標準のSnowflake の接続プロセスを完了します。必要なすべてのアクセス許可は統合プロセス中に付与され、追加の設定は必要ありません。

統合後、必要なアクセス許可が付与されたことを確認します。クラウドサイバーエクスポージャーコンソールで、**[設定] > [アカウント] > [Snowflake]** の順に移動し、アカウントのステータスが [接続済み] であることを確認します。これは、必要なアクセス許可がすべて正常に適用されたことを示します。これ以上のアクションは必要ありません。

Snowflake で必要なアクセス許可

データ保護をサポートするために、Tenable には Snowflake の次の読み取り専用アクセス許可が必要です。

- **`MONITOR USAGE` (アカウント)**: アカウントレベルの使用量情報を Tenable で表示できるようになります。
- **`MONITOR` (アカウント)**: アカウントリソースの稼働ステータスとメタデータを Tenable で表示できるようになります。

- **USAGE (Tenable 専用ウェアハウス)**: スキャンに使用されるコンピューティングリソースへのアクセスを許可します。
- **IMPORT SHARE (アカウント)**: 統合を許可し、アカウントレベルで共有データをインポートできます。このアクセス許可は、DSPM オンボーディング時に自動的に付与されます。
- **IMPORTED PRIVILEGES(データベース)**: アカウントレベルの IMPORT SHARE アクセス許可が付与された後に、共有データベースへのアクセスを有効にします。
- **USAGE (データベースおよび現在および将来のすべてのスキーマ)**: データベース構造の可視化を許可します。
- **SELECT (データベースの現在および将来のすべてのテーブル)**: 分類のためにデータ値を読み取る必要があります。
- **SNOWFLAKE.GOVERNANCE_VIEWER (データベース)**: 適用されたオブジェクトタグ、マスキングポリシー、および行アクセスポリシーを検査する場合に必要です。
- **SNOWFLAKE.OBJECT_VIEWER (データベース)**: 包括的な資産検出とインベントリのために、オブジェクトのメタデータに対するアカウント全体の可視化を許可します。
- **SNOWFLAKE.SECURITY_VIEWER (データベース)**: セキュリティリスクを特定するために、ユーザーロール、権限、ネットワーク設定の分析を有効にします。

これらのアクセス許可は、統合時に自動的に付与されます。統合プロセスが不完全な場合を除き、追加の設定は必要ありません。

Okta 組織の接続

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

Okta 組織を Tenable One Cloud Exposure と統合すると、環境内の Okta グループとユーザーの完全なインベントリが明らかになります。

> **注意:** このセクションで取り上げているのは、SSO 経由でのクラウドサイバーエクスポージャーコンソールのログインを目的にした IdP の統合ではありません。コンソールにアクセスする必要があるユーザーに対して SSO 経由のログインを有効にする方法の詳細については、シングルサインオンを参照してください。

ダッシュボードで Okta 認証データを活用するには、以下で説明されている手順に従って、スーパー管理者として Okta Admin Console にログインし、関連するアカウント情報を収集して、Tenable に Okta アカウントへのアクセスを付与するアクセストークンを作成します。Tenable では、この目的のために専用ユーザーを作成することをお勧めします。これにより、監査証跡アクティビティが簡素化され、後日統合が不要になった場合、ユーザーを削除することで統合をより簡単に終了できるようになります。

Okta 組織を追加する方法

> **注意:** ウィザードの実行中、クラウドサイバーエクスポージャーコンソールと Okta Admin Console の両方を操作する必要があります。このタスクの手順の大半は、別段の指示がない限り Okta Admin Console で実行します。

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** に移動します。
2. **[統合の追加]** をクリックします。
3. 統合ライブラリで、**[Okta]** をクリックします。[Okta] ウィザードが開きます。
4. 新規 Okta ユーザーを作成します (ウィザードのステップ 1)。
    1. スーパー管理者として Okta Admin Console にログインし、**[ディレクトリ] > [ユーザー]** の順に移動します。
    2. **[ユーザーの追加]** をクリックします。
    3. すべての関連フィールドに入力し、**[保存]** をクリックします。

        > **注意:** ユーザーの目的を識別できる名と姓を使用することをお勧めします。たとえば、名: Tenable、姓: 読み取り専用。

    4. クラウドサイバーエクスポージャーコンソールで、**[次へ]** をクリックして、ウィザードの次のステップに移動します。
5. Tenable にアクセス許可を付与します (ウィザードのステップ 2)。
    1. **[セキュリティ] > [管理者]** に移動します。
    2. **[+ 管理者の追加]** をクリックします。
    3. [管理者] フィールドで、前のステップで作成したユーザーを選択します。
    4. [ロール] フィールドで、**[読み取り専用管理者]** ロールを選択し、**[変更を保存]** をクリックします。

5. クラウド サイバーエクスポージャー コンソールで、**[次 へ]** をクリックして、ウィザード の次 のステップ に移 動します。

6. アクセスト ークンを作 成します (ウィザード のステップ 3)。

    1. Okta Admin Console からサインアウトし、ここまでの手 順 で作 成した新しいユーザーを使 用し てサインインします。

        > **注 意:** 新しいユーザーアカウント のアクティブ化 がまだの場 合 はここでアクティブ化し、セキュリ ティメソッド を設 定してください。

    2. **[セキュリティ] > [API]** に移 動します。
    3. [トークン] タブに移 動し、**[トークンの作 成]** をクリックします。
    4. トークンに意 味 のある名 前 を入 力し (「Tenable」など)、**[トークンの作 成]** をクリックします。
    5. **[トークン値]** をコピーして保 存します。

        > **重 要:** トークン値 は安 全 な場 所 に保 存してください。この値 は、次 のステップで入 力する必 要 があります。

    6. クラウド サイバーエクスポージャー コンソールで、**[次 へ]** をクリックして、ウィザード の次 のステップ に移 動します。

7. Okta 組 織 を Tenable に接 続します (ウィザード のステップ 4)。

    1. クラウド サイバーエクスポージャー コンソールに、Tenable の組 織 の表 示 名 を入 力します。
    2. **Okta 組 織 URL** を入 力します。これは、Okta ポータルにアクセスするためにブラウザで使 用 するウェブアドレス (ルートドメインのみ) です。これは、Okta からのウェルカムメールやアクティベー ションメールにも記 載されています。

        例: https://example.okta.com/

    3. ここまでの手 順 でコピーした**ユーザートークン**を入 力し、**[終 了]** をクリックします。

OneLogin アカウント の接 続

> **注 意:** この機 能 は、Cloud Vulnerability Management ライセンスでは使 用 できません。

OneLogin アカウントを Tenable One Cloud Exposure と統合すると、環境内の OneLogin グループとユーザーの完全なインベントリが明らかになります。

> **注意:** このセクションで取り上げているのは、SSO 経由でのクラウドサイバーエクスポージャーコンソールのログインを目的にした IdP の統合ではありません。コンソールにアクセスする必要があるユーザーに対して SSO 経由のログインを有効にする方法の詳細については、シングルサインオンを参照してください。

OneLogin アカウントを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** に移動します。
2. **[統合の追加]** をクリックします。
3. 統合ライブラリで、**[OneLogin]** をクリックします。[OneLogin] ウィザードが開きます。
4. API 認証情報を作成します (ウィザードのステップ 1)。
    1. OneLogin 管理ポータルにログインし、**[開発者] > [API 認証情報]** の順に移動します。
    2. **[新しい認証情報]** をクリックします。
    3. 意味のある**名前**を入力し、**[すべて読み取り]** を選択して、**[保存]** をクリックします。
    4. **クライアント ID** と**クライアントシークレット**をコピーして保存し、**[完了]** をクリックします。

        > **重要:** これらの値は安全な場所に保存してください。この値は、次のステップで入力する必要があります。

    5. クラウドサイバーエクスポージャーコンソールで、**[次へ]** をクリックして、ウィザードの次のステップに移動します。
5. OneLogin アカウントを Tenable に接続します(ウィザードのステップ 2)。
    1. クラウドサイバーエクスポージャーコンソールで、OneLogin アカウントの**名前**を入力します。
    2. ここまでの手順でコピーした**クライアント ID** と**クライアントシークレット**を入力します。
    3. **[リージョン]** を選択し、**[終了]** をクリックします。

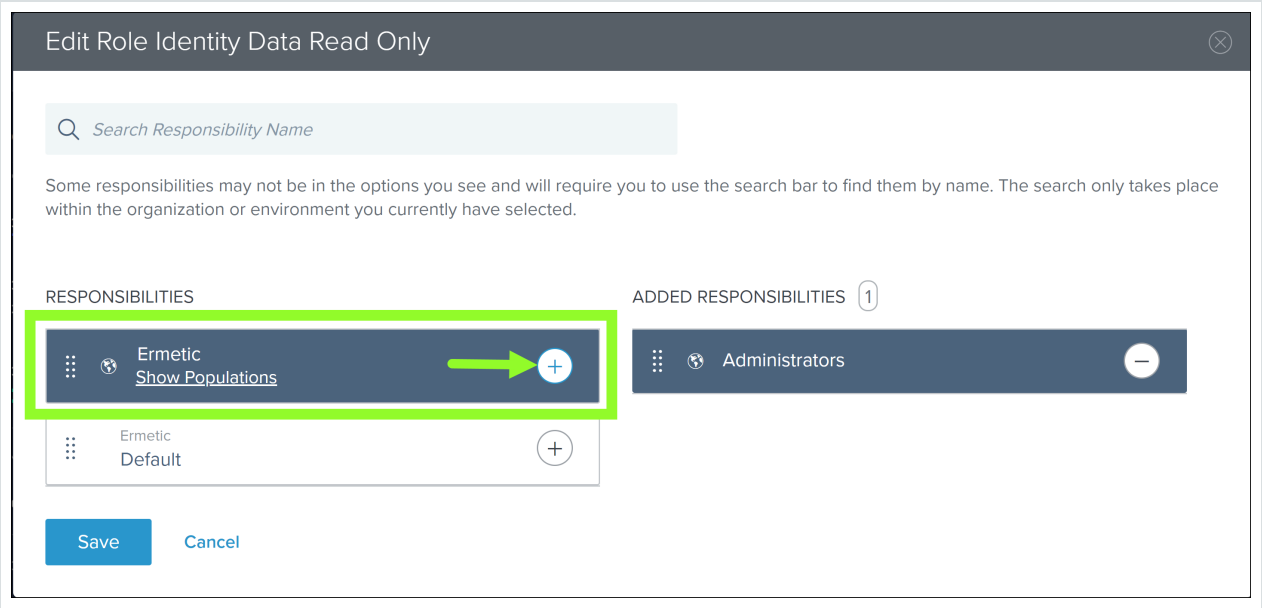
Ping Identity 環境の接続

Ping Identity 環境を Tenable One Cloud Exposure と統合すると、環境内の Ping Identity グループとユーザーの完全なインベントリが明らかになります。

> **注意:** このセクションで取り上げているのは、SSO 経由でのクラウドサイバーエクスポージャーコンソールのログインを目的にした IdP の統合ではありません。コンソールにアクセスする必要があるユーザーに対して SSO 経由のログインを有効にする方法の詳細については、シングルサインオンを参照してください。

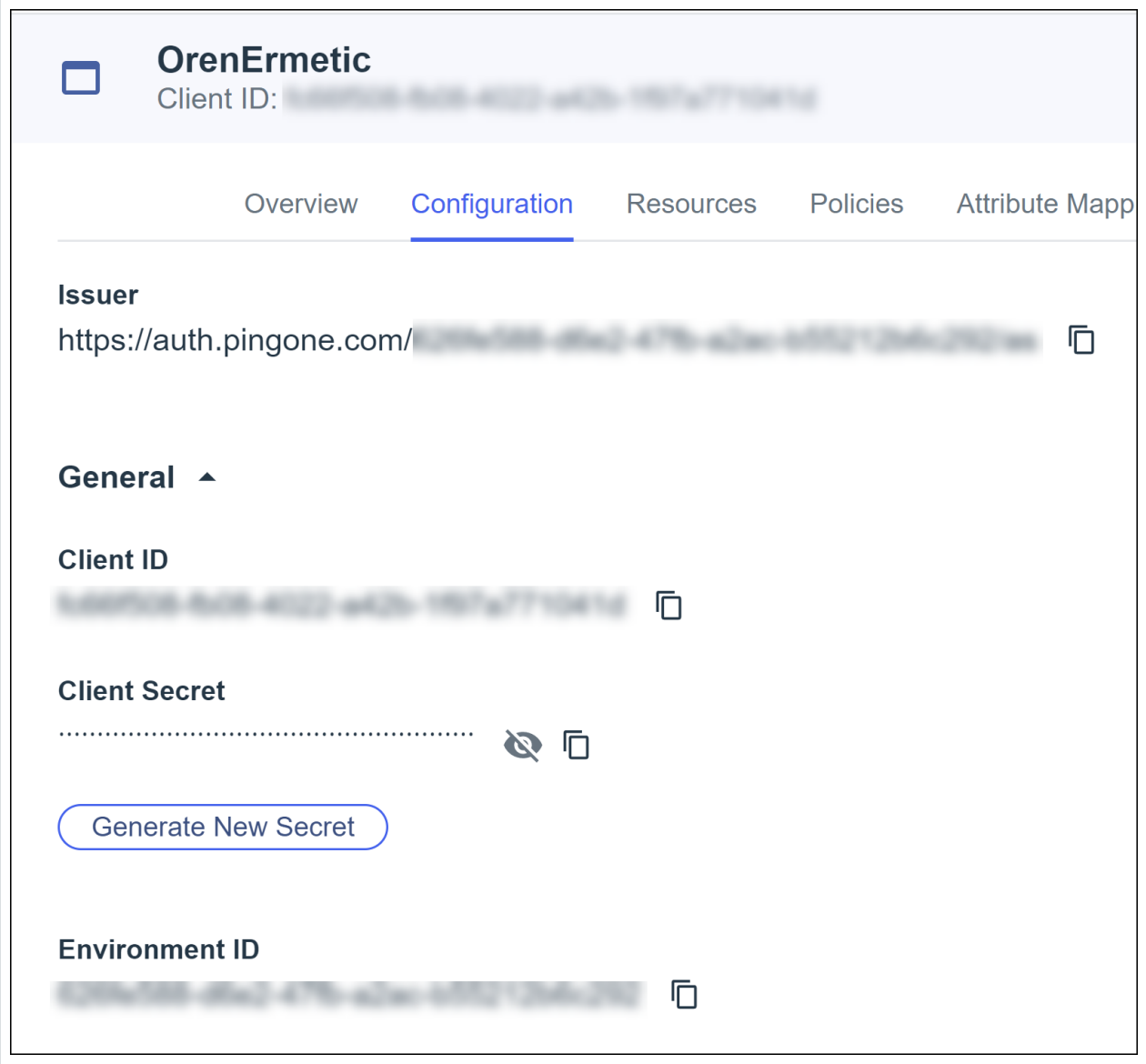
Ping Identity 環境を追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定] > [統合]** に移動します。
2. **[統合の追加]** をクリックします。
3. 統合ライブラリで、**[Ping Identity]** をクリックします。[Ping Identity] ウィザードが開きます。
4. 新しいアプリケーションを作成します (ウィザードのステップ 1)。
    1. Ping Identity コンソールにログインし、**[接続] > [アプリケーション]** の順に移動します。
    2. プラス記号 (+) をクリックして新しいアプリケーションを追加します。
    3. アプリケーションに**名前を付け**、アプリケーションタイプとして **[Worker]** (従業員) を選択して、**[保存]** をクリックします。
    4. 表示されたアプリケーションページの **[ロール]** タブに移動します。
    5. 以下のロールを除くすべてのロールを削除します。
        - 設定 (読み取り専用)
        - アイデンティティデータ (読み取り専用)
    6. [編集] ボタンをクリックしてロールを編集し、**[アイデンティティデータ (読み取り専用)]** ロールの横にある [編集] ボタンをクリックします。
    7. [RESPONSIBILITIES] (責任)リストから、[ADDED RESPONSIBILITIES] (追加した責任) のリストに環境を追加します。



8. アプリケーションページでトグルボタンをクリックし、アプリケーションへのユーザーアクセスを有効にします。
9. クラウドサイバーエクスポージャーコンソールで、**[次へ]** をクリックして、ウィザードの次のステップに移動します。

5. 以下の詳細を指定して、環境を Tenable に接続します (ウィザードのステップ 2)。
    1. Ping Identity コンソールのアプリケーションページで、**[設定]** タブに移動し、**[General]** (一般) セクションを展開します。この情報は、クラウドサイバーエクスポージャーコンソールに入力する必要があります。



2. クラウド サイバーエクスポージャー コンソールで、以下の詳細を入力します。
   - アプリケーションの**名前**
   - **環境 ID**
   - **クライアント ID** と**クライアント シークレット**
   - 環境の**リージョン**

     注意: [環境] > [プロパティ] の順に移動すると、Ping Identity コンソールでリージョンを確認できます。

3. クラウド サイバーエクスポージャー コンソールで、**[終了]** をクリックします。

クラウド アカウントのオフボーディング

次のいずれかの状況では、Tenable One Cloud Exposure からアカウントをオフボーディングする必要がある場合があります。

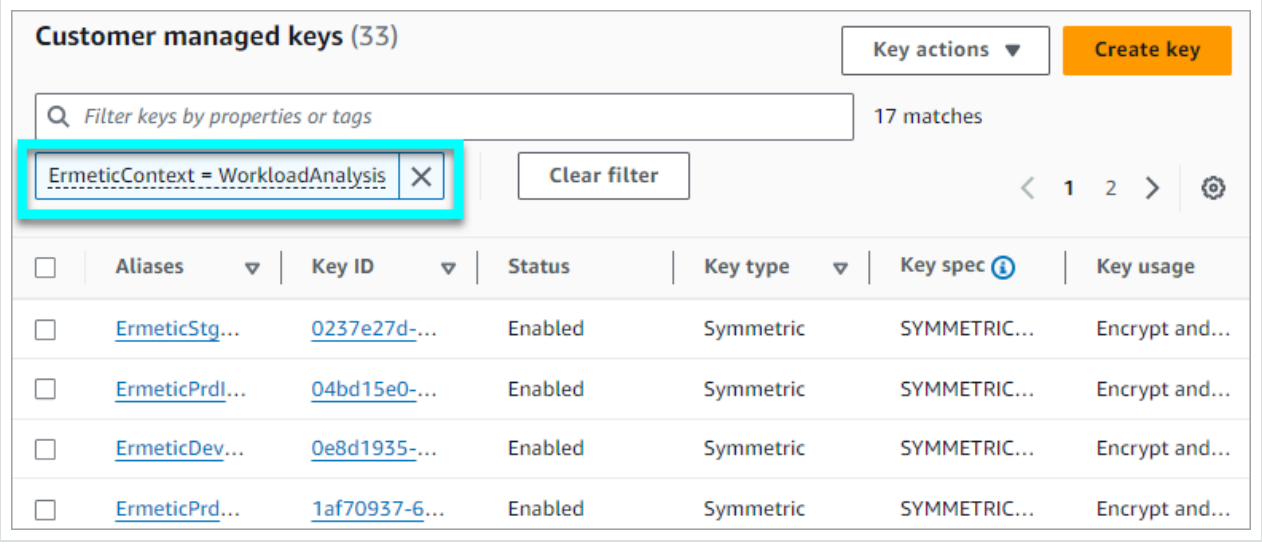
- アカウントのグループに対して監査を実行し、監査を完了した場合
- アカウントを閉鎖する場合

> **注意:** Tenable は、お客様が契約を終了してから 30 日以内にお客様のデータを削除します。

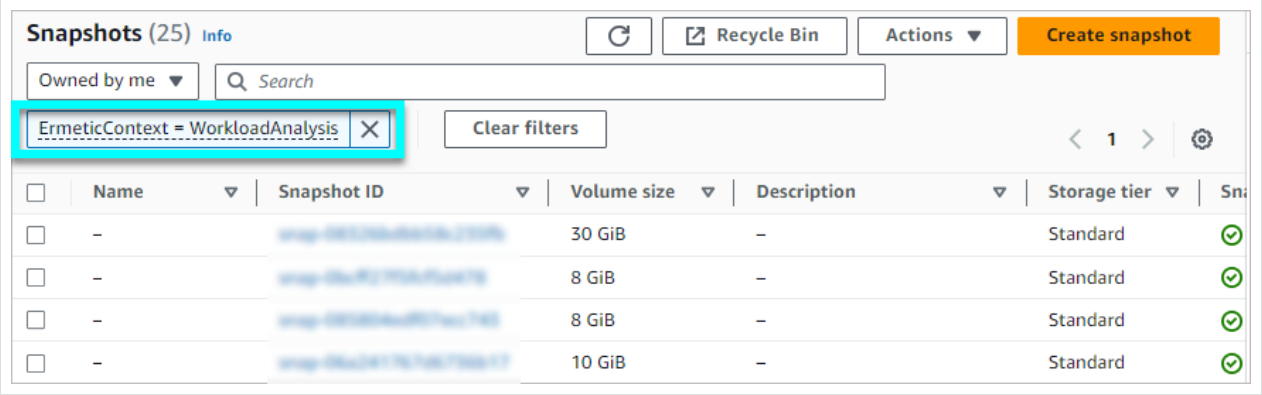
AWS アカウントのオフボーディング

AWS アカウントや AWS 組織をオフボーディングする手順は次のとおりです。

1. オンボーディング中に作成した IAM ロールを削除します。
2. (ワークロード保護) 作成されたすべての KMS キーやスナップショットを削除します。
    1. AWS コンソールで、**[KMS] > [カスタマーマネージド キー]** の順に移動し、`ErmeticContext = WorkloadAnalysis` のタグキーや値を持つキーを検索します。



2. 関連するキーを選択して削除します。
3. **[EC2] > [Elastic Block Store] > [スナップショット]** の順に移動し、`ErmeticContext = WorkloadAnalysis` のタグキーや値を持つスナップショットを検索します。



4. 関連するキーを選択し、**[アクション] > [スナップショットの削除]** をクリックします。

3. CloudFormation を使用して IAM ロールを作成した場合は、作成されたスタックインスタンスと StackSets を以下の手順で削除します。
   1. AWS コンソールで、**[CloudFormation] > [StackSets]** の順に移動し、オンボーディング中に作成した StackSets を検索します。
   2. StackSets を選択し、**[アクション] > [StackSet からスタックを削除]** をクリックします。
   3. 必要な詳細を入力し、スタックの削除を進めます。
   4. スタックを削除後、もう一度 StackSets を選択し、**[アクション] > [StackSet の削除]** をクリックします。
   5. **[削除]** をクリックして確認します。
4. クラウドサイバーエクスポージャーコンソールから組織またはアカウントを削除します。-
   - **組織**: **[設定] > [統合] > [AWS 組織]** の順に移動し、関連する組織の横にある **[削除]** をクリックします。組織を削除すると、その下にあるすべての関連フォルダーとアカウントが自動的に削除されます。
   - **[アカウント] > [AWS]** の順に移動し、関連するアカウントの横にある **[削除]** をクリックします。

     > **注意:**

- アカウントが、オンボーディングされた組織に属している場合は、その組織からアカウントを除外する必要があります。
- または、**[設定]** > **[アカウント]** > **[AWS]** からアカウントを削除します。

Azure サブスクリプションのオフボーディング

Azure サブスクリプションや組織をオフボーディングする手順は次のとおりです。

1. オンボーディング中にクラウドサイバーエクスポージャーアプリに追加したロールの割り当てを削除します。
2. Microsoft Entra ID からクラウドサイバーエクスポージャーアプリを削除します。
3. クラウドサイバーエクスポージャーコンソールから組織またはサブスクリプションを削除します。
    - **組織**: **[設定]** > **[統合]** > **[Azure 組織]** の順に移動し、関連する組織の横にある **[削除]** をクリックします。
    - **サブスクリプション**: **[アカウント]** > **[Azure]** の順に移動し、関連するサブスクリプションの横にある **[削除]** をクリックします。

      注意:
      - サブスクリプションが、オンボーディングされた組織に属している場合は、フォルダーまたはサブスクリプションを組織から除外する必要があります。
      - または、**[設定]** > **[アカウント]** > **[Azure]** からサブスクリプションを削除します。

GCP プロジェクトのオフボーディング

GCP プロジェクトや組織をオフボーディングする手順は次のとおりです。

1. オンボーディング中に Tenable サービスアカウントに付与したアクセス許可を削除します。
2. Google Workspace の接続ときに作成した Tenable サービスアカウントを削除します。
3. クラウドサイバーエクスポージャーコンソールから組織またはプロジェクトを削除します。
    - **組織**: **[設定]** > **[統合]** > **[GCP 組織]** の順に移動し、関連する組織の横にある **[削除]** をクリックします。

- **プロジェクト**: **[アカウント] > [GCP]** の順に移動し、関連するアカウントの横にある **[削除]** をクリックします。

  > **注意:**
  > - プロジェクトが、オンボーディングされた組織に属している場合は、フォルダーまたはプロジェクトを組織から除外する必要があります。
  > - または、**[設定] > [アカウント] > [GCP]** からプロジェクトを削除します。

OCI テナンシのオフボーディング

OCI テナンシをオフボーディングする手順は次のとおりです。

1. Oracle Cloud テナンシをオンボーディングしたときに作成したグループ、ユーザー、キーの認証情報を削除します。
2. クラウドサイバーエクスポージャー コンソールからテナンシを削除します。**[設定] > [統合] > [OCI テナンシ]** の順に移動し、関連するテナンシの横にある **[削除]** をクリックします。

アカウント内スキャンの設定

アカウント内スキャンを設定するには、専用アカウントを作成して接続してから、ターゲットアカウントでリージョンごとにプロビジョニングされるリソースためのアクセス許可を Tenable One Cloud Exposure に付与します。

アカウント内スキャンを設定する方法

1. スキャン用に 1 つ以上の専用アカウントを作成します。

   > **注意:**
   > - クラウドサイバーエクスポージャーでアカウント階層とフォルダーごとに定義できるスキャンアカウントは 1 つのみです。スキャンアカウントは、1 つの範囲にのみマッピングできます。
   > - 当該アカウントに関連するコンピューティングコスト (1 リージョンあたり推定約 300 ドル) は、お客様の負担となります。詳細については、リージョンごとにプロビジョニングされるリソースを参照してください。

2. クラウドサイバーエクスポージャー のアカウントを接続します。

3. クラウドプロバイダーに応じて、以下をアカウントに追加して、コンピューティングリソースを管理するために必要なアクセス許可を Tenable に付与します。
    - **AWS** はすべての必要なアクセス許可を追加します。
    - **Azure** はすべての必要なアクセス許可を クラウド サイバーエクスポージャー コネクタアプリに割り当てます。
    - **GCP** はすべての必要なアクセス許可を追加します。
    - **OCI** はすべての必要なアクセス許可を追加します。
4. プロセスを完了するうえでご不明な点がある場合は、サポートにお問い合わせください。この時点で、以下が実行されます。
    - Tenable は、仮想マシンがある各リージョンに必要なコンピューティングリソースをプロビジョニングします。詳細については、リージョンごとにプロビジョニングされるリソースを参照してください。
    - Tenable は、定期的にスキャンをオーケストレーションします。

必要な AWS アクセス許可

必要な AWS アクセス許可は、AWS 管理ポリシーとカスタムインラインポリシーで構成されます。

- 次の AWS 管理ポリシーをアタッチします。AmazonVPCFullAccess。
- 以下のカスタムのインラインポリシーを、統合時に作成した IAM ロールに追加します。

これらのアクセス許可は、お客様の環境でワークロードをデプロイ、管理、スキャンするために必要です。これには、コンピューティングリソースのプロビジョニングと変更 (EC2、Auto Scaling、EKS)、認証とアクセス制御のための IAM ロールとポリシーの管理、安全なデータアクセスのための暗号化キーの処理 (KMS)、リソースの効率的な編成 (リソースグループ) が含まれます。これらのアクセス許可により、セキュリティとコンプライアンスを維持しながら、ワークロードスキャンに必要なインフラを確保できます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "autoscaling:UpdateAutoScalingGroup"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DetachVolume"
              ],
            "Resource": "*",
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVolume",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Context": "WorkloadAnalysis"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVolume",
            "Resource": "arn:aws:ec2:*:*:snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVolume",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Context": "WorkloadAnalysis"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateLaunchTemplate",
                "ec2:CreateLaunchTemplateVersion",
                "ec2:DeleteLaunchTemplate",
                "ec2:ModifyLaunchTemplate",
                "ec2:RunInstances"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "eks:AssociateEncryptionConfig",
                "eks:CreateAddon",
                "eks:CreateCluster",
                "eks:CreateNodegroup",
                "eks:CreatePodIdentityAssociation",
                "eks:DeleteCluster",
                "eks:DeleteNodegroup",
                "eks:TagResource",
                "eks:UpdateAddon",
                "eks:UpdateClusterVersion",
                "eks:UpdateNodegroupConfig",
                "eks:UpdateNodegroupVersion"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:CreateServiceLinkedRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:List*Tags",
                "iam:PassRole",
                "iam:PutRolePolicy",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:Tag*",
                "iam:UpdateAssumeRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateAlias",
                "kms:CreateGrant",
                "kms:CreateKey",
                "kms:Decrypt",
                "kms:DeleteAlias",
```

```
                "kms:DescribeKey",
                "kms:EnableKeyRotation",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ListAliases",
                "kms:ListKeys",
                "kms:ListResourceTags",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:ScheduleKeyDeletion",
                "kms:TagResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "license-manager:ListReceivedLicenses",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:AddTagsToResource",
                "rds:CreateDBSubnetGroup",
                "rds:DeleteDBSubnetGroup"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:DeleteGroup",
                "resource-groups:Get*",
                "resource-groups:Tag"
            ],
            "Resource": "*"
        }
    ]
}
```

必要な Azure アクセス許可

専用のアカウント内サブスクリプションで、クラウドサイバーエクスポージャーコネクタアプリに次の**カスタムロール**を割り当てます。このロールにより、Tenable で以下が可能になります。

- ディスクの作成や削除を含む、マネージドディスクのモニタリング
- Kubernetes クラスタがディスクをスキャンジョブにアタッチできるようにするロール定義 (TenableRoleDefinitionWorkloadAnalysisScanning) の作成

JSON

```
{
    "properties": {
        "assignableScopes": [
            "/subscriptions/<SubscriptionId>"
        ],
        "description": "",
        "permissions": [
            {
                "actions": [
                    "Microsoft.Authorization/roleAssignments/delete",
                    "Microsoft.Authorization/roleAssignments/write",
                    "Microsoft.Authorization/roleDefinitions/delete",
                    "Microsoft.Authorization/roleDefinitions/write",
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/register/action",
                    "Microsoft.Compute/skus/read",
                    "Microsoft.Compute/virtualMachines/attachDetachDataDisks/action",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachineScaleSets/write",
                    "Microsoft.ContainerService/managedClusters/agentPools/abort/action",
                    "Microsoft.ContainerService/managedClusters/agentPools/deleteMachines/action",
                    "Microsoft.ContainerService/managedClusters/agentPools/machines/read",
                    "Microsoft.ContainerService/managedClusters/agentPools/machines/write",
                    "Microsoft.ContainerService/managedClusters/agentPools/read",
                    "Microsoft.ContainerService/managedClusters/agentPools/upgradeNodeImageVersion/action"
,
                    "Microsoft.ContainerService/managedClusters/agentPools/write",
                    "Microsoft.ContainerService/managedClusters/delete",
                    "Microsoft.ContainerService/managedClusters/listClusterUserCredential/action",
                    "Microsoft.ContainerService/managedClusters/write",
                    "Microsoft.ContainerService/register/action",
                    "Microsoft.Features/providers/features/register/action",
                    "Microsoft.KeyVault/*",
                    "Microsoft.ManagedIdentity/register/action",
                    "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.ManagedIdentity/userAssignedIdentities/delete",
                    "Microsoft.ManagedIdentity/userAssignedIdentities/federatedIdentityCredentials/delete"
,
```

```
                "Microsoft.ManagedIdentity/userAssignedIdentities/federatedIdentityCredentials/write",
                "Microsoft.ManagedIdentity/userAssignedIdentities/write",
                "Microsoft.Network/natGateways/delete",
                "Microsoft.Network/natGateways/write",
                "Microsoft.Network/networkSecurityGroups/delete",
                "Microsoft.Network/networkSecurityGroups/join/action",
                "Microsoft.Network/networkSecurityGroups/securityRules/delete",
                "Microsoft.Network/networkSecurityGroups/securityRules/write",
                "Microsoft.Network/networkSecurityGroups/write",
                "Microsoft.Network/publicIPAddresses/delete",
                "Microsoft.Network/publicIPAddresses/write",
                "Microsoft.Network/register/action",
                "Microsoft.Network/routeTables/delete",
                "Microsoft.Network/routeTables/join/action",
                "Microsoft.Network/routeTables/write",
                "Microsoft.Network/virtualNetworks/delete",
                "Microsoft.Network/virtualNetworks/subnets/delete",
                "Microsoft.Network/virtualNetworks/subnets/join/action",
                "Microsoft.Network/virtualNetworks/subnets/write",
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Resources/subscriptions/providers/read",
                "Microsoft.Resources/subscriptions/resourceGroups/delete",
                "Microsoft.Resources/subscriptions/resourceGroups/write",
                "Microsoft.Resources/tags/write",
                "Microsoft.Storage/register/action",
                "Microsoft.Storage/storageAccounts/blobServices/containers/delete",
                "Microsoft.Storage/storageAccounts/blobServices/containers/write",
                "Microsoft.Storage/storageAccounts/delete",
                "Microsoft.Storage/storageAccounts/listkeys/action",
                "Microsoft.Storage/storageAccounts/managementPolicies/delete",
                "Microsoft.Storage/storageAccounts/managementPolicies/write",
                "Microsoft.Storage/storageAccounts/write"
            ],
            "dataActions": [
                "Microsoft.ContainerService/managedClusters/*",
                "Microsoft.KeyVault/vaults/keyrotationpolicies/*",
                "Microsoft.KeyVault/vaults/keys/*",
                "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete",
                "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read",
                "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"
            ],
            "notActions": [],
            "notDataActions": []
        }
    ],
    "roleName": "InAccountCustomRole"
```

```
    }
}
```

必要な GCP アクセス許可

以下の事前定義されたロールを統合中に作成したクラウドサイバーエクスポージャー サービスアカウントに追加します。

GCP ロール	説明
Cloud KMS Admin	保存時に暗号化されたワークロードの復号化とスキャンに使用される暗号化キーを管理するために必要です。
Editor	リソースの読み取りと変更を行うアクセス許可を付与し、さまざまな GCP サービスのワークロードをスキャンできるようにします。
Kubernetes Engine Admin	Google Kubernetes Engine (GKE) クラスタで実行されているワークロードを検査し、セキュリティコンプライアンスを確保するために必要です。
Project IAM Admin	IAM ポリシーを管理して、プロジェクト全体のワークロードにアクセスして検査するために必要なアクセス許可がスキャナーにあることを確認するために必要です。
Service Account Admin	認証とスキャン操作に必要なサービスアカウントの作成と管理を可能にします。

必要な OCI アクセス許可

統合時に作成した OCI ポリシーに以下のステートメントを追加することで、OCI アカウント内ワークロードをスキャンするアクセス許可をクラウドサイバーエクスポージャーに付与します。

- グループTenableCSがコンパートメント内のすべてのリソースを管理できるようにします<InAccount コンパートメントOCID>
- `グループ TenableCS が tenancy</codetext のボリュームを使用できるようにする>

カスタマーマネージドキーで暗号化されたボリュームをスキャンするには、次のステートメントを OCI ポリシーに追加します。

- `グループ TenableCS が tenancy</codetext で key-delegate を使用できるようにします>

リージョンごとにプロビジョニングされるリソース

このセクションでは、それぞれの異なる地理的**クラウドリージョン**内で Tenable がデプロイおよび使用する**特定のクラウドインフラコンポーネント** (リソース) と、各コンポーネントの**特定の技術要件および文脈**の詳細に重点を置いています。

- AWS
- Azure
- GCP
- OCI

AWS

リソース	要件	文脈情報
コンピュート	• EKSクラスター • オンデマンド管理型仮想マシン 2 台、vCPU 4 個、RAM 16 GB • 仮想マシンのスキャン	• **EKSクラスター**: スキャン操作とオーケストレーションを管理します • **仮想マシンの管理**: EKSクラスターによって開始されたスキャンプロセスをオーケストレーションする • **仮想マシンのスキャン**: スキャン処理を実行します。オンデマンドで拡張可能で、最大32 vCPU、64 GB RAMまで対応しています。 **注**: 必要に応じて増やすことも可能です

リソース	要件	文脈情報
		プロビジョニングされるノードの数とサイズは Tenable によって自動的に管理され、スキャンの要求に対応しながらコストを最小限に抑えます
アイデンティティ	5 個の IAM ロール	• EKS クラスター(コントロールプレーン) で使用されます • Kublet 管理ノードで使用されます • KarpenterノードのKubletが、VMの起動およびスキャンに使用する • EBS CSI ドライバーが、スキャンを行うために EC2 インスタンスにディスクを接続する際に使用されます • 管理ポッドで使用される
ストレージ	該当なし	該当なし
ネットワーク	• 2つのエラスティックIP • 1 インターネットゲートウェイ • 2つのNATゲートウェイ • 6 ルーティングテーブル • 4 セキュリティグループ • 6つのサブネット • 1 VPC	• **サブネット** : 外部との通信用のアウトバウンドサブネット 2 つ、内部通信用のプライベートサブネット 2 つ • **インターネットゲートウェイ**: 送信トラフィックに使用されます • **NATゲートウェイ**: NATで使用される • **VPC**: ネットワークコンテナ サブネットは、プライベートサブネット 、EKS (コントロールプレーンおよびワーカー)、VPC に使用されます
セキュリ	KMS キー	Kubernetes シークレットの暗号化と復号化に使用

リソース	要件	文脈情報
ティ		
推定最小コスト(月ごと)	$300	インフラに対する最小コスト (スキャンコストを除く)スナップショットスキャン費用計算ツールとデータスキャンコスト保護のスキャンコストの詳細をご確認ください。

Azure

リソース	要件	文脈情報
コンピュート	• AKSクラスター • オンデマンド管理型仮想マシン2台、vCPU 4個、RAM 16 GB • 仮想マシンのスキャン • 内部ロードバランサー	• **AKS クラスター**: スキャン操作とオーケストレーションを管理します • **仮想マシンの管理**: AKS クラスター内のスキャンプロセスを調整します • **仮想マシンのスキャン**: スキャン処理を実行します。オンデマンドで拡張可能で、最大32 vCPU、64 GB RAMまで対応しています。 **注**: 必要に応じて増やすことも可能です • **ロードバランサー**: ASK API サーバーへの着信および発信トラフィックを管理するために使用されます
アイデンティティ	3個のユーザー管理アイデンティティ	• AKS クラスター(コントロールプレーン) では、以下の目的で使用されます: • スキャン用にディスクをVMに接続する • Kubernetesのシークレットの暗号化と復号化 • Kublet によって使用されます(AKS の作成時に Azure によって自動的に作成されます) • KarpenterがVMの起動およびスキャンに使用する

リソース	要件	文脈情報
ストレージ	• 1 個のストレージアカウント • 1つのBlobコンテナ	スキャン対象サブスクリプションからスキャン用サブスクリプションへマネージドディスクをコピー

ネットワーク	• 3つのサブネット
	  • 3 ネットワークセキュリティグループ
	• 1 プライベートエンドポイント
	• 1 NATゲートウェイ
	• 1つのパブリックIPアドレス
	• 1 仮想ネットワーク
	• 3 ルーティングテーブル
		• **サブネット**：外部との通信用のエグレス・サブネット 1 つ、内部通信用のプライベート・サブネット 1 つ、ASK API サーバーの VNet 統合用のサブネット 1 つ
		  • **セキュリティグループ**：ネットワークのサブネットごとに使用されます
		• **プライベートエンドポイント**：AKS 仮想ネットワークのプライベート IP を Azure Key Vault にマッピングし、API トラフィックをインターネットから隔離します。
		• **NATゲートウェイ**：送信トラフィックに使用されます
		• **パブリックIP**：NATで使用される
		• **仮想ネットワーク**：ネットワークコンテナ
		• **ルーティングテーブル**：サブネットによって使用される

セキュリティ	Key Vault キー	Kubernetes シークレットの暗号化と復号化に使用
推定最小コスト (月ごと)	$325	インフラに対する最小コスト (スキャンコストを除く)スナップショットスキャン費用計算ツールとデータスキャンコスト保護のスキャンコストの詳細をご確認ください。

GCP

リソース	要件	文脈情報
コンピュート	• 1つのGKEクラスター • 1 個のスポットマシン - e2-standard-2 (2vCPU および 8GB RAM)	• **GKE クラスター**: スキャン操作とオーケストレーションを管理します プロビジョニングされるノードの数とサイズは Tenable によって自動的に管理され、スキャンの要求に対応しながらコストを最小限に抑えます
アイデンティティ	1 個のサービスアカウント (プロジェクトごと)	GKE クラスタノードが使用 Kubelet (コントロールプレーン)
ストレージ	該当なし	該当なし
ネットワーク	• 1 出口サブネット • 1 プライベートサブネット • 1つのIPアドレス • 1 ルーター • 1 NATゲートウェイ • 1 VPC(プロジェクトごとに)	• **サブネット**: 外部との通信用のアウトバウンドサブネット 1 つ、内部通信用のプライベートサブネット 1 つ • **ルーター + NAT**: 送信トラフィックに使用されます • **IP**: NATで使用される • **VPC**(ネットワークコンテナ) : プライベートサブネットと GKE(コントロールプレーンおよびノード) のネットワーク分離を実現します
セキュリティ	クラウドキーリングキー	Kubernetes シークレットの暗号化と復号化に使用
推定最小コスト (月ごと)	$300	インフラに対する最小コスト (スキャンコストを除く)スナップショットスキャン費用計算ツールとデータスキャンコスト保護のスキャンコストの詳細をご確認ください。

OCI

リソース	要件	文脈情報
コンピュート	• 1 OKEクラスター • ノード	• **ノード**：アベイラビリティ・ドメインごとに1つのノード Tenable はプロビジョニングされたノードの数とサイズを自動的に管理し、スキャンの要求に対応しながらコストを最小限に抑えます
アイデンティティ	該当なし	該当なし
ストレージ	該当なし	該当なし
ネットワーク	• 3つのサブネット • 3 ルーティングテーブル • VCN • 3 セキュリティリスト • 1 インターネットゲートウェイ • 1 予約済みIPアドレス	• **サブネット**：外部との通信用のアウトバウンドサブネット 2 つ、内部通信用のプライベートサブネット 1 つ • **NATゲートウェイ**：送信トラフィックに使用されます • **IP**：NATで使用される • **VCN**(ネットワークコンテナ) ：プライベートサブネットおよびOKE (コントロールプレーンおよびノード) に対してネットワークの分離を実現します

リソース	要件	文脈情報
	• 1 NAT ゲートウェイ • 1 サービスゲートウェイ	
セキュリティ	• Vault • キー	Kubernetes シークレットの暗号化と復号化に使用
推定最小コスト (月ごと)	$300	インフラに対する最小コスト (スキャンコストを除く)スナップショットスキャン費用計算ツールとデータスキャンコスト保護のスキャンコストの詳細をご確認ください。

ネットワーク分離されたサーバーの接続

次の統合のために、ネットワーク分離されたサーバーを Tenable One Cloud Exposure に接続できます。

- IaC セキュリティ
    - **GitHub Enterprise Server**
    - **GitLab セルフマネージドサーバー**
- SIEM (セキュリティ情報イベント管理)
    - **QRadar**
- ワークロード保護
    - **コンテナイメージレジストリ (サードパーティ)**

このようなサーバーを接続するには、まず統合する各サーバーにTenableエンドポイントコネクタを追加し、次に統合の追加を行います。統合と同じネットワークにあり、統合に接続されている専用のKubernetesクラスタでHelmチャートを介してクラスタを接続するを介してコネクタを追加します。

Tenableのサーバーへの接続方法

以下の手順は、Helmチャートを介してクラスタを接続するを使用して、専用のKubernetesクラスタにコネクタをインストールする場合の、クラウドサイバーエクスポージャーのサーバーへの接続方法です。

1. コネクタの追加と、ワークロード(デプロイメント)が作成され、クラスタ内で実行されます。このワークロードには次の特徴があります。
    - ポートを外部に公開せず、インターネットからアクセスできません。
    - クラウドサイバーエクスポージャープラットフォームのみを信頼するように設定されています。
2. ワークロードは、リバースプロキシを使用してクラウドサイバーエクスポージャーとの安全な専用接続を開始します。
3. ワークロードは、安全な接続とネットワーク分離されたサーバーとの間でトラフィックをルーティングします。
4. その後、Tenableは安全な接続を使用して、ネットワーク分離されたサーバーに定期的にアクセスします。

重要: このプロセスは、ネットワーク分離サーバーをインターネットに公開しません。すべての外部通信は、作成されたワークロードを経由してのみ実行されます。

コネクタの追加

クラウドサイバーエクスポージャーと統合するネットワーク分離サーバーごとにコネクタを追加します。現在、以下の統合がサポートされています。

- GitHub Enterprise Serverの追加
- GitLabグループの追加

- QRadar
- サードパーティレジストリの追加

Tenable Endpoint コネクタを追加する方法

1. クラウドサイバーエクスポージャーコンソールで、**[設定]** > **[統合]** に移動します。
2. (オプション) [組織] ドロップダウンからアカウント 範囲 を選択します。
3. **[統合の追加]** をクリックします。
4. 統合ライブラリで、**[エンドポイントコネクタ]** をクリックします。[エンドポイントコネクタ] ウィザードが開きます。
5. 以下の統合の詳細 (ウィザードのステップ 1) を入力して、**[次へ]** をクリックします。
    1. **名前**。クラウドサイバーエクスポージャーコンソールに表示されるコネクタ名。
    2. **エンドポイント**。統合のホスト名または IP アドレス。たとえば、github.tenable.com や 192.82.156.1 などです。
    3. **ポート**。統合で使用するポート番号。
6. **Kubernetes クラスタにデプロイ** します (ウィザードのステップ 2)。統合と同じネットワークにあり、統合に接続されている専用の Kubernetes クラスタにコネクタをデプロイします。
    1. Kubernetes のパッケージマネージャーとして Helm をインストールします。使用を開始するには、Helm のドキュメント を参照してください。
    2. Kubernetes クラスタに接続するように kubectl を設定します。
    3. 次のコマンドを実行して、Tenable リポジトリを追加します。
       ```
       helm repo add tenable https://charts.tenable.com
       ```
    4. Tenable に接続してデータを送信するには、ウィザードに表示されるコマンドを実行します。このコマンドにより、Kubernetes クラスタにエンドポイントコネクタがインストールされます。
7. **[終了]** をクリックします。

高度なコネクタ設定

values.yaml ファイルを使用すると、高度なユースケースのためのコネクタ設定をカスタマイズできます。Helm コマンドを使用してこのファイルを取得し、必要に応じてその値を設定してから、helm install コマンドを実行する際にこのファイルを含めます。

> **注意:** 一部のファイル値は helm install コマンド内で引数として指定できます。

values.yaml ファイルを使用してコネクタを設定する方法

1. 以下のコマンドを実行して、values.yaml を取得します。

   ```
   helm show values tenable/tenable-cloud-security-endpoint-connector
   ```

2. 必要に応じて values.yaml ファイルを設定し、ファイルを保存します。
3. 以下のように、実行する Helm install コマンドの末尾にファイルを追加します。

   ```
   helm install {...} -f custom-values.yaml
   ```

   ここで {...} は、[クラスタを追加] ダイアログに表示される、動的に生成されるコマンドです。

values.yaml の内容

values.yaml ファイルには次の共通するパラメーターが含まれています。

パラメーター	説明	デフォルト
apiKeyTokenSecretName	Tenable API キーを含む Kubernetes シークレットの名前。これは apiKeyToken が直接提供されない場合にのみ必須です。	

パラメーター	説明	デフォルト
resources	CPU やメモリなど、Pod のコンピューティングリソースの要件と制限を指定します。	
tolerations	taint のあるノードに Pod をスケジュールできる条件を指定します。	
proxyUrl	プロキシサーバーを使用して接続します。	• **認証なし:** `proxyUrl: "http://your-proxy:<port>"` • **認証がある場合** `proxyUrl: "http://<username>:<password>@your-proxy:<port>"`

プレイブックとチュートリアル

クイックスタートガイド

このセクションでは、Tenable One Cloud Exposure でクラウド環境の保護を開始するにあたり、すぐに実行できる基本的な最初の手順の概要を説明します。これらの手順は、クラウドサイバーエクスポージャーを使用するためのクラウド環境のセットアップと重大な問題の対処に焦点を当てており、将来モニタリングや修正に取り組むための土台を構築するのに役立ちます。これらの手順をすべて完了するには、環境の規模や複雑さに応じて数週間またはそれ以上かかる場合があります。

- ステップ 1: 環境のセットアップ
- ステップ 2: 関連するセキュリティ領域の所有者の特定
- 検出結果への対処の開始
    - ステップ 3: 重大な検出結果への対処
    - ステップ 4:「容易に解決できる問題」への対処
- ステップ 5: 検出結果のレビュー
- ステップ 6: 検出結果の修正

ステップ 1: 環境のセットアップ

以下の手順に従ってクラウドサイバーエクスポージャー環境をセットアップします。

1. リージョンに基づいて提供された URL を使用して、クラウドサイバーエクスポージャーにログインします。

   詳しくは、リージョン別の Tenable コンソール URL を参照してください。

   > **リージョン:** URL に反映されるリージョンによって、Tenable APIにアクセスする際に使用される API エンドポイントが決まります。

2. クラウドアカウントを クラウドサイバーエクスポージャーに接続します。

3. アイデンティティプロバイダー (IdP) を クラウド サイバーエクスポージャー と統 合します。
4. SSO 経 由 での Tenable コンソールへのログインを有 効 化します。
5. アカウント階 層 とフォルダーを クラウド サイバーエクスポージャー で行います。
6. 必 要 に応じて、ユーザーとグループを追 加 設 定します。
7. オプションのインバウンドとアウト バウンドの統 合 を設 定します。
8. 機 密 度 の高いリソースをマークする。一 部 のリソースは機 密 性 が高いか、機 密 データを含んでいる可 能 性 があります。以 下 を行うためには、これらのリソースを クラウド サイバーエクスポージャー 内 で機 密 としてマークすることが重 要 です。
    - クラウド サイバーエクスポージャー がそのようなリソースに関 連 付 けられた検 出 結 果 のリスクを正 確 に評 価 できるようにする。
    - そのような検 出 結 果 、またはそのリソースにアクセス権 を持 つアイデンティティの優 先 度 を上 げる。

環 境 をセット アップし、データの同 期 と更 新 の頻 度 と、コンソールに環 境 の実 際 のデータが表 示 され始 めます。あと少しで、クラウド サイバーエクスポージャー コンソールを使 用 してクラウド 環 境 を保 護 するための作業 を開 始 できます。

コンソールにもう少 し慣 れたい場 合 は、コンソールの操 作 方 法 、ダッシュボードを管 理 する方 法 、データのフィルタリング方 法 (クラウド サイバーエクスポージャー 全 体 が対 象) をご確 認 ください。

> **重 要 :** クラウド サイバーエクスポージャー では、選 択 されたデータオブジェクト グループのデータを指 定 された期 間 保 持 します。詳 細 については、データ保 持 期 間 と学 習 期 間 を参 照 してください。

ステップ 2: 関 連 するセキュリティ領 域 の所 有 者 の特 定

セキュリティチームを構 成 するユーザーやロール (IAM 担 当 者 、DevSecOps など) について考 えてみましょう。クラウド サイバーエクスポージャー で検 出 されたさまざまなセキュリティの検 出 結 果 に対 して、チーム全 体 でどのように所 有 権 を割 り当 てますか? たとえば、以 下 を割 り当 てることができます。

- 特 定 のクラウド アカウント またはアカウント グループの所 有 者
- 特 定 の検 出 結 果 のタイプまたはカテゴリの所 有 者 (IAM 関 連 の検 出 結 果 すべての所 有 者 など)

- 特定のプロジェクトに属するリソースすべての所有者。この目的のためにタグキーや、値、パターンに基づいてリソースに自動的にラベルを付けるインベントリ(プロパティとラベル)できます。

責任の分担が決まったら、関連する問題について各所有者に通知する方法を考えます。たとえば、次の方法で所有者に通知できます。

- 自動化ルールによって検出結果を所有者に割り当てる
- 所有者に送信するために、レポートの作成をスケジュール化する
- 特定の問題についてクラウドサイバーエクスポージャーコンソールを積極的に検索するよう求める。コンソールユーザーのアクセスを、そのユーザーが担当するフォルダーやアカウントに制限するために、特定の関連範囲を持つユーザーとグループ。

自動化ルールによって検出結果を所有者に割り当てる

自動化ルールを使用して、特定の所有権カテゴリに関連するすべての検出結果を適切なユーザーまたはグループに割り当てることができます。割り当てられたユーザーまたはグループは検出結果を詳しく調査し、必要に応じて修正できます。

検出結果を割り当てる方法

1. サードパーティのチケッティング、通知、またはSIEMツールをクラウドサイバーエクスポージャーに統合します。
2. 自動化を作成して、特定の検出結果がクラウドサイバーエクスポージャーで作成された際、サードパーティツールにプッシュ通知を送信します。
3. 自動化ルールに加え、メールやWebhookで検出結果をクラウドの検出結果送信することや、Jira課題やServiceNowインシデントを作成することもできます。

所有者に送信するために、レポートの作成をスケジュール化する

セキュリティ問題について関連するステークホルダーに連絡するために、スケジュールされたレポートを作成します。たとえば、経営幹部に送信するマネジメントレポートをスケジュールします。このレポートには、アカウントと全体的なセキュリティポスチャーのスナップショットが提示され、クラウド環境の包括的な概要が含まれます。

クラウド サイバーエクスポージャー でのレポート 作 成 に関 する詳 細 については、レポートを参 照 してくださ い。

スケジュールされたレポート の作 成 方 法

1. クラウド サイバーエクスポージャー コンソールで、**[ポリシー]** をクリックします。
2. **アカウント 階 層 とフォルダー** を選 択 します。選 択 された範 囲 内 でアクセス許 可 を持 つユーザーがレ ポート にアクセスできるようになります。
3. **[新 規 レポート]** をクリックします。
4. ドロップダウンからレポート の **レポート** を選 択 します。
5. レポート に**名 前** を付 けます。
6. 配 信 時 間 を設 定 するため **[スケジュール]** を選 択 して、特 定 の日 時 にレポート を生 成 するよう、日 次 、週 次 、月 次 といった頻 度 を定 義 します。
7. 任 意 で **その他 の配 信 方 法** を選 択 して、レポート のコピーを特 定 の受 信 者 にメールまたは Slack チャンネルで送 信 します。
8. **[生 成]** をクリックします。

ステップ 3: 重 大 な検 出 結 果 への対 処

環 境 をセット アップし、セキュリティチームのロールや責 任 を特 定 したら、クラウド サイバーエクスポージャー が検 出 した重 大 な検 出 結 果 に対 処 し、最 も重 要 なセキュリティ問 題 への取 り組 みを始 めることができま す。重 大 な検 出 結 果 には、広 範 囲 のさまざまなセキュリティ違 反 が存 含 まれる可 能 性 があります。 Tenable では、次 の問 題 の確 認 から始 めることを推 奨 しています。

> **注 意 :** これらの問 題 タイプには、お使 いの環 境 に関 連 しないものもあります。所 属 組 織 のニーズに応 じて、 どの問 題 を対 処 するか、または優 先 するか調 整 してください。必 要 に応 じて、クラウド サイバーエクスポー ジャー Customer Success チームにお問 い合 わせください。

- サード パーティアクセス
- MFA を使 用 しないルート アカウント
- 一 般 に公 開 されているリソース

- 本番環境で露出しているシークレット
- 次のステップ: 本番環境で「高」と「重大」の検出結果

サードパーティアクセス

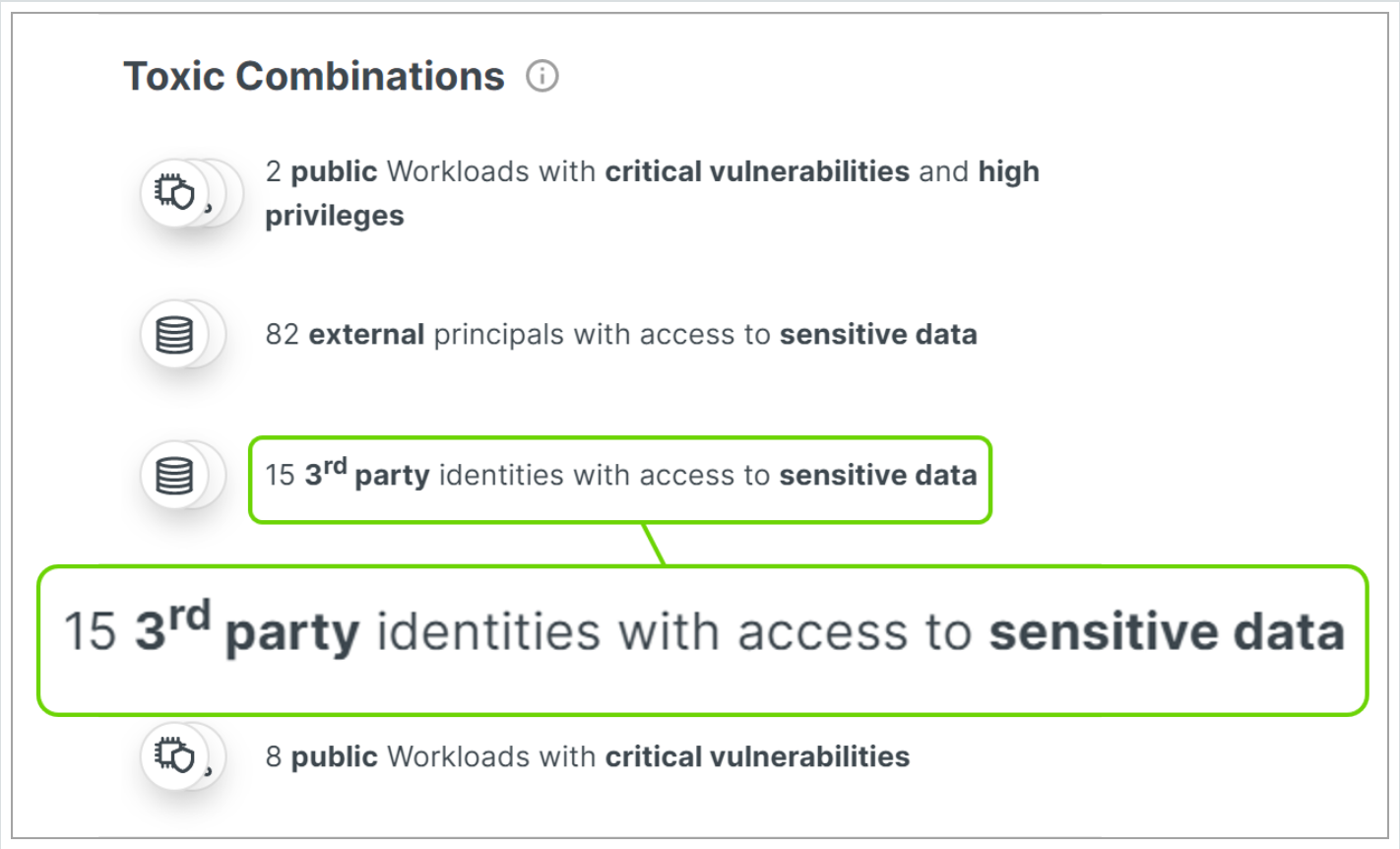
組織はさまざまなサードパーティのツールを利用してサービスを運用しており、専用のクラウドアイデンティティを介してそのようなツールにインフラリソースへのアクセスを許可しています。そのため、どのサードパーティが環境にアクセスでき、どのようなアクセス許可を持っているのか、そしてどのようなリスクがあるのかについて可視化することが大切です。

クラウドサイバーエクスポージャーには、サードパーティアクセスに関連する違反を特定してレビューする方法が複数あります。よくある例をいくつか示します。

- 機密データへのアクセス権を持つサードパーティアイデンティティの検索
- 過剰な権限を持つサードパーティアイデンティティの検索

機密データへのアクセス権を持つサードパーティアイデンティティの検索

1. [概要] ダッシュボードに移動します (**[ダッシュボード]** > **[概要]**)。
2. **[危険な組み合わせ]** ウィジェットまで下にスクロールします。
3. **[機密データにアクセスできるサードパーティアイデンティティ]** のエントリがある場合は、それをクリックします。
4. 検出結果のレビューを行います。
5. 検出結果の修正を行います。



詳細については、ダッシュボードを管理すると危険な組み合わせを参照してください。

過剰な権限を持つサードパーティアイデンティティの検索

1. **[検出結果]** に移動します。
2. [深刻度] フィルターで **[重大]** を選択し、提示されたリスクに対して早急なアクションが必要な検出結果を表示します。
3. [ポリシー] フィルターで**過剰な権限**という単語を検索して、**[一致を選択]** をクリックします。
4. [ラベル] フィルターで **[サードパーティ]** を選択し、サードパーティアプリケーションに関連する検出結果をすべて表示します。
5. 検出結果をクリックして詳細を確認します。
6. 検出結果のレビューを行います。
7. 検出結果の修正を行います。

検出結果の使用方法の詳細については、検出結果の詳細の表示を参照してください。

MFA を使用しないルートアカウント

ルートアカウントはクラウドアカウントで最高の特権ユーザーです。MFA により攻撃者は機密リソースにアクセスすることが困難になるため、ルートアカウントユーザーの MFA を有効にすることは非常に重要です。

クラウドサイバーエクスポージャーで MFA を使用しない AWS ルートアカウントを見つける方法は複数ありますが、ここでは一般的な例を 1 つ示します。

- [検出結果] ページを使用して、MFA を使用しないルートアカウントを特定する

[検出結果] ページを使用して、MFA を使用しないルートアカウントを特定する

1. **[検出結果]** に移動します。
2. [ポリシー] フィルターで、**ルートユーザーの MFA が有効になっていない**というポリシーを検索して選択します。
3. 検出結果をクリックして詳細を確認します。
4. 検出結果のレビューを行います。
5. 検出結果の修正を行います。

検出結果の使用方法の詳細については、検出結果の詳細の表示を参照してください。

一般に公開されているリソース

一般に公開されているリソースは、直ちに攻撃のターゲットになります。クラウドサイバーエクスポージャーを使用して、ネットワークまたは IAM 設定を経由して公開されているリソースを特定します。

クラウドサイバーエクスポージャーで一般に公開されているコンピューティングインスタンスを見つける方法は複数ありますが、ここでは 1 つの一般的な例を示します。

- ダッシュボードの [パブリックリソース] ウィジェットを使用してパブリックリソースを素早く表示する

ダッシュボードの [パブリックリソース] ウィジェットを使用してパブリックリソースを素早く表示する

1. **[ダッシュボード]** に移動します。
2. コンソールの上部にある範囲フィルターを使用して、本番アカウントでフィルタリングします。

3. **[パブリックリソース]** ウィジェットまで下にスクロールします。
4. 次のいずれかを行います。
    - ウィジェットの右上にある **[さらに表示]** をクリックして、パブリックリソースに関連付けられた検出結果をすべて表示する。
    - 関連するリソースタイプのタイルを選択して、そのリソースに関連付けられた検出結果のリストを表示する。
5. [深刻度] フィルターで **[重大]** を選択し、提示されたリスクに対して早急なアクションが必要な検出結果を表示します。
6. 検出結果をクリックして詳細を確認します。以下に例を挙げます。
    - リソースを一般に公開するリソース **ACL** や **ポリシー** を表示する。
    - S3 バケットによって公開されている特定のアクセス許可 (`DeleteBucket` アクセス許可など) など、関連するコンテキスト情報を表示する。
7. 検出結果のレビューを行います。
8. 検出結果の修正を行います。

ダッシュボードとそのウィジェットの詳細については、ダッシュボードを管理するを参照してください。

本番環境で露出しているシークレット

本番環境のリソースでは、パスワードやアクセストークンのような機密データを AWS Secrets Manager や Azure Key Vault などのツールに保存する必要があります。

1. **[ダッシュボード]** に移動します。
2. コンソールの上部にある範囲フィルターを使用して、本番アカウントでフィルタリングします。
3. **[シークレットを露出するリソース]** ウィジェットまで下にスクロールします。
4. 次のいずれかを行います。
    - ウィジェットの右上にある **[さらに表示]** をクリックして、シークレットを露出しているリソースに関連する検出結果をすべて表示する。
    - ウィジェット内の特定のエントリをクリックして、シークレットを公開している特定のリソースタイプに関連する検出結果を表示する。

5. 検出結果のレビューを行います。
6. 検出結果の修正を行います。

本番環境で「高」と「重大」の検出結果

組織の本番環境に持ち込まれる「高」または「重大」のセキュリティ問題の数が増え続けています。上記以外の重大な検出結果や問題に対処したら、Tenable では、本番環境に高深刻度または重大深刻度の検出結果がないか一般的な検索を実行することを推奨しています。重大深刻度の検出結果は、通常、問題に対して早急のアクションが必要であることを示しています。一方、高深刻度の検出結果は、通常、重大ではないものの、できるだけ早く対処する必要がある問題を表しています。

1. **[検出結果]** に移動します。
2. [アカウント] フィルターで関連する各クラウドの本番アカウントを選択します。
3. [深刻度] フィルターで **[高]** と **[重大]** を選択します。
4. 検出結果のレビューを行います。
5. 検出結果の修正を行います。

ステップ 4:「容易に解決できる問題」への対処

環境内で最も重大な検出結果に対処したら、次は「容易に解決できる問題」に対処することを Tenable は推奨しています。この文脈で「容易に解決できる問題」とは、容易に修正ができ、不要なリソースを排除して環境をクリーンに保つことができ、解決すれば、組織にとって価値のある成果を迅速にもたらす問題のことを指します。Tenable では、次の問題の確認から始めることを推奨しています。

- 非アクティブなアイデンティティ
- 未使用の認証情報
- 未使用のセキュリティグループ

非アクティブなアイデンティティ

長期間非アクティブになっているユーザー、Microsoft Entra ID アプリケーション、およびサービスアカウントをモニタリングし、修正します。

1. **[検出結果]** に移動します。

   > **注意:** 以下の各クエリについて、表示される検出結果の数は環境の仕様が大きく影響します。結果の数やチームが持っているリソースによっては、**深刻度**フィルター (**例: [高] または [重大]** の検出結果) を使用してクエリをさらに制限する必要がある場合があります。

2. MFA が設定されていない非アクティブな IAM ユーザーに関連する検出結果を特定します。
   1. [ポリシー] フィルターで**非アクティブな IAM ユーザー**のポリシーを検索して選択します。
   2. [ラベル] フィルターで **[MFA なし]** フィルターを選択します。
3. アクティブなアクセスキーを持つ非アクティブな IAM ユーザーに関連する検出結果を特定します。
   1. [ポリシー] フィルターで**非アクティブな IAM ユーザー**のポリシーを検索して選択します。
   2. [ラベル] フィルターで **[アクセスキー]** フィルターを選択します。
4. 管理者権限を持つ非アクティブな Azure AD アプリケーションに関連する検出結果を特定します。
   1. [ポリシー] フィルターで、**非アクティブな Microsoft Entra ID アプリケーション**というポリシーを検索して選択します。
   2. [ラベル] フィルターで **[管理者]** フィルターを選択します。
5. アクティブなアクセスキーを持つ非アクティブなサービスアカウントに関連する検出結果を特定します。
   1. [ポリシー] フィルターで、**非アクティブなサービスアカウント**というポリシーを検索して選択します。
   2. [ラベル] フィルターで **[アクセスキー]** フィルターを選択します。
6. 前の手順で検出された各検出結果について、次を実行します。
   1. 検出結果のレビューを行います。
   2. 検出結果の修正を行います。

未使用の認証情報

45 日以上使用されていない認証情報はすべて削除または無効化することが推奨されます。不要な認証情報を無効化または削除すると、攻撃者や内部関係者の脅威アクターが機密リソースにアクセスできる機会を減らします。

1. **[検出結果]** に移動します。
2. [ポリシー] フィルターで **IAM ユーザーの未使用パスワード** や **IAM ユーザーの未使用アクセスキー** というポリシーを検索して選択します。
3. 必要に応じて、テーブルを **[高]** または **[重大]** 深刻度でフィルタリングします。
4. 検出結果のレビューを行います。
5. 検出結果の修正を行います。

未使用のセキュリティグループ

使用されていないセキュリティグループは削除する必要があります。これは、リソースが誤ってグループにアタッチされ、意図しないネットワークエクスポージャーにつながる可能性があるためです。

1. **[検出結果]** に移動します。
2. [ポリシー] フィルターで**未使用のセキュリティグループ**というポリシーを検索して選択します。
3. 必要に応じて、テーブルを **[高]** または **[重大]** 深刻度でフィルタリングします。
4. 検出結果のレビューを行います。
5. 検出結果の修正を行います。

ステップ 5: 検出結果のレビュー

検出結果の修正に進む前に検出結果をしっかりとレビューして、特定のクラウド環境内での検出結果の全体の文脈を理解することが重要です。ほとんどの場合、クラウドサイバーエクスポージャーによって提案された修正手順は、ユーザー側で調整することなくそのまま実装可能であり、一部の検出結果で調整が必要な場合もわずかな調整で済みます。また場合によっては、特定のビジネス面の文脈により、特定のリソースがクラウドサイバーエクスポージャーによって潜在的なリスクとしてフラグを立てられていても、修正する必要がないと判断されることがあります。修正したくない状況の例については、クラウドの検出結果を参照してください。

検出結果のレビュー方法

1. 関連する検出結果をクリックしてドリルダウンし、検出結果のすべての分析を表示します。
2. 検出結果の詳細とその他の関連情報を確認して、次の点について理解を深めます。
    - 検出結果の根本的な原因
    - 検出結果の範囲
    - 環境にもたらされる潜在的なリスク
    - 検出結果の深刻度の説明
3. **[修正ステップ]** エリアに移動して、記載されている手順をよく確認します。
4. 検出結果を今すぐ修正しない正当な理由がある場合、以下を行うことができます。
    - 検出検出結果を無視するして後の日付に延期し、その日付になったらリマインダーを受け取ります。
    - 推奨事項を無視し、無視された検出結果からのパターンベースの除外の作成 かどうかを決定して、同様の検出結果が作成されないようにします。

ステップ 6: 検出結果の修正

先行的に軽減手順を適用して、組織のセキュリティリスクを修正します。クラウドサイバーエクスポージャーの修正に関する推奨事項は、実際のサイバーエクスポージャー、設定ミス、過剰でリスクの高い権限、流出した秘密情報、脆弱性などのリスク要因を考慮した、マルチクラウド環境全体の継続的な分析に基づいています。

関連要件を含め、クラウドサイバーエクスポージャーによる修正に関する詳細については、検出結果の修正を参照してください。

検出結果の手動修正

検出結果によっては、関連する問題をクラウドサイバーエクスポージャー以外で修正する方が、検出結果を Tenable で自動的に修正するよりも適切な場合があります。これは特に、Tenable によって自動的に実行された修正が開発者のコードで上書きされる可能性がある、インフラのコード化 (IaC) ワークフローで役立ちます。修正されたポリシーの提案をアタッチすることで、Tenable の推奨事項をコーディング環境に合わせて直接実装できるようになります。

1. 関連する検出結果をクリックしてドリルダウンします。
2. 検出結果の詳細ビューで **[修正ステップ]** エリアに移動し、手順に従って 1 つずつ実行します。
3. 修正ステップにポリシー変更の提案が含まれている場合、ステップの横に以下のボタンの一部またはすべてが表示され、修正されたポリシーをさまざまな形式で表示およびダウンロードしたり、古いポリシーと新しいポリシーを並べて差分表示したりできます。

   - JSON
   - Diff
   - Terraform
   - CloudFormation

   開発者が手動でコードに適用できるように、これらの提案のコピーを開発者に送信することができます。
4. 検出結果を修正した後、そのクラウドの検出結果して、[検出結果] ページから削除します。

検出結果の自動修正

クラウドサイバーエクスポージャー では、検出結果を自動的に修正してワンクリック修正が可能になり、リスク緩和のプロセスを効率化できます。Tenable クラウド環境内で関連する修正手順をプロアクティブに実行することで、時間と労力を節約できます。

関連要件を含め、自動修正に関する詳細については、検出結果の自動修正を参照してください。

検出結果を自動修正する方法

1. 関連する検出結果をクリックしてドリルダウンします。
2. 検出結果の [修正] タブで、**[修正]** ボタンをクリックします。

3. さまざまなステップをクリックして以下を行います。
    - 問題のリソースに関する詳細情報を表示する。
    - 提案されたポリシー変更の表示と編集を行う。
    - 提案されたポリシー変更を編集する場合は、**[編集]** をクリックし、関連する変更を加えてから **[保存]** をクリックする。
    - アクセスキーを無効にするか削除するかを選択する (**IAM ユーザーの未使用の認証情報** ポリシーによってトリガーされる検出結果の場合など)。
4. **[次へ]** をクリックします。
5. アカウントのオンボーディング中に Tenable に読み取り専用のアクセス許可のみを付与した場合、ワンタイム認証情報を Tenable に付与する必要があります。
6. 適用される手順を確認して、**[適用]** をクリックします。

AI リスクを検出する方法

これは Tenable One Cloud Exposure コンソールから AI リスクを検出する方法に関するガイドです。Tenableの AI-SPM 機能の概念概要については、AI-SPMを参照してください。

目的

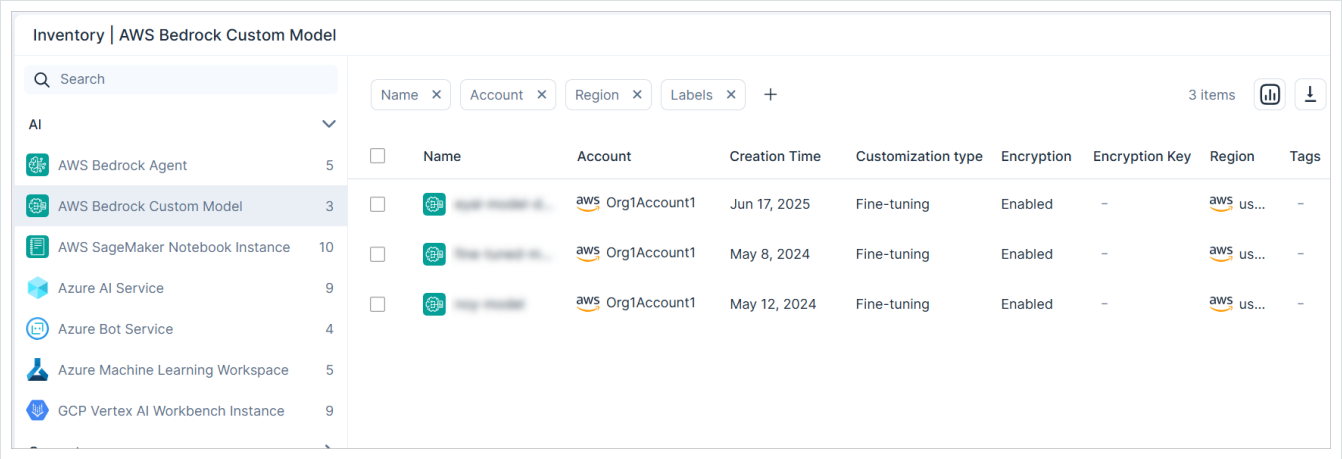
クラウドサイバーエクスポージャー AI-SPM 機能を利用して、AI/ML 環境の可視性を確保し、固有の AI 関連のリスク (データポイズニング、特権の過剰なエージェントなど) を管理します。

ステップ 1: インベントリで AI 資産を検出する

インベントリを使用して、環境内で実行されているすべての AI リソース (PaaS サービス、ソフトウェア、データリポジトリ) を検出します。

1. **[調査]** > **[インベントリ]** に移動します。
2. **AI** カテゴリを展開します。

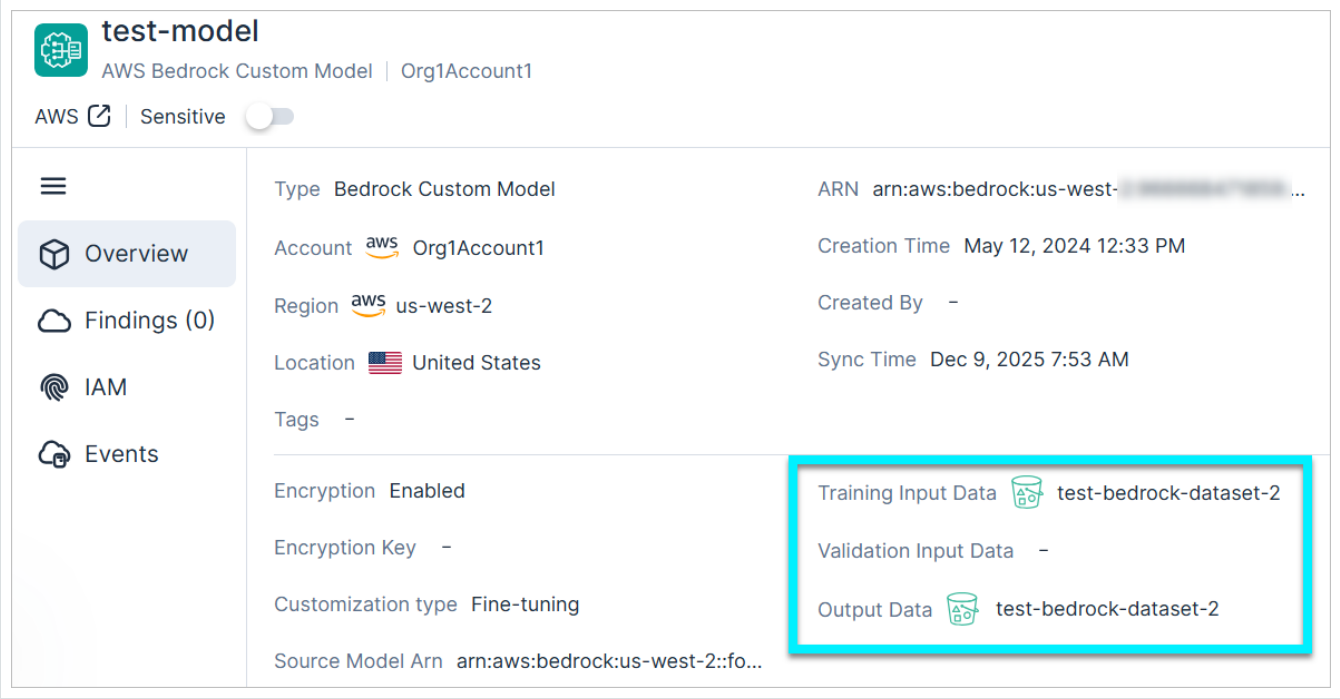
3. クロスクラウド AI リソースタイプを検索します。



ステップ 2: AI リソースとトレーニングデータを関連付ける

AI-SPM で最も重要な手順の 1 つは、AI モデルと、AI モデルがトレーニングされた機密データの間の関係を確立することです。この相関は、データポイズニングや知的財産の盗難から保護するための鍵です。

1. **AI モデルを検出する**: インベントリで開始し、コア AI 資産を見つけます。たとえば、AWSbedrock カスタムモデルなどです。
2. **リソースの詳細の表示**: 特定の Basedrock Custom Model 名をクリックして、リソースプロファイルページを開きます。
3. **相関データの特定**: リソースプロファイルの [概要] タブには、モデルとソースデータをリンクさせるプロパティが表示されます。以下に例を挙げます。
    - **トレーニング入力データ**: モデルの微調整に使用された特定の S3 バケットまたはリポジトリが表示されます。
    - **出力データ**: モデルで生成された出力を保存するために使用されるバケットを表示します。



4. **データの機密性を評価する**: **[トレーニング入力データ]** リンクをクリックします。リンクすると、リンクされている S3 バケットリソースページに直接移動します。
5. バケットのリソースページから、**[データ]** タブに移動し、トレーニングデータセット内の機密情報または機密情報 (PII、PCI など) の存在を確認します。

脆弱性のある特権 VM を保護する

目的

深刻度の高い脆弱性が高い権限に対応している仮想マシン (VM) を特定し、監視する。これにより、エクスプロイトがプロジェクトの完全なコントロールやラテラルムーブメントにつながる可能性のある資産に優先順位を付けることが可能になります。

> **注意:** プレイブックは、プラットフォーム内でセキュリティワークフローを運用するための設計資産として機能します。概説されている手順は、技術的な可視性を一貫性のある実用的な結果に変えるための繰り返し可能な方法を示しています。**このガイドでは特定のユースケースに焦点を当てていますが、これらの原則は他のリソースタイプやセキュリティシナリオに適用されることで、環境全体の包括的なリスク管理を確実にすることができます。**

ステップ 1: リスクの表面化 (ビルトインクエリ)

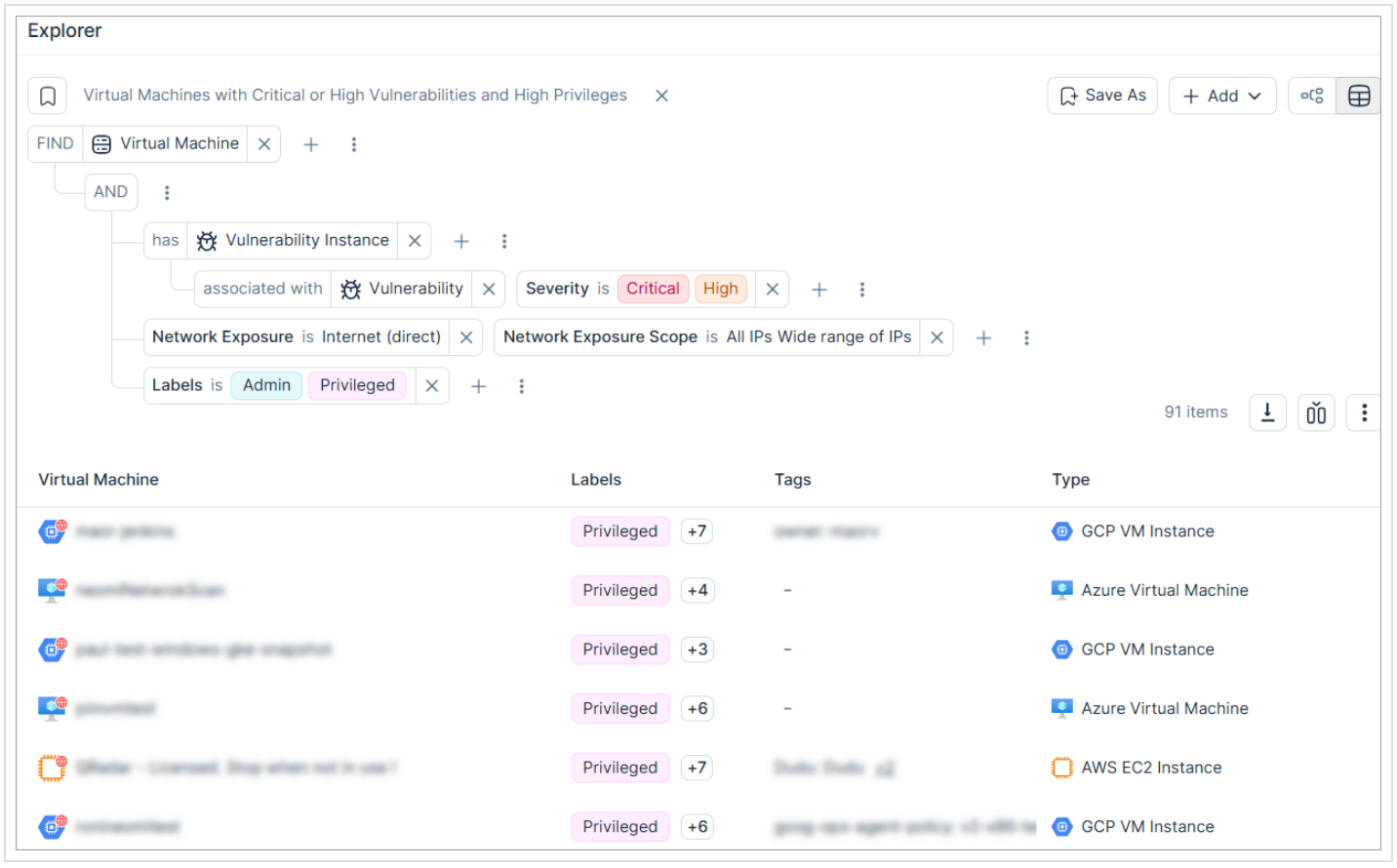
ビルトインクエリを使用して、直近の脅威を検出します。

1. **[調査]** > **[エクスプローラー]** に移動します。
2. **[クエリの選択]** をクリックして、次のクエリを選択します。

    - `Virtual Machines with Critical or High Vulnerabilities and High Privileges`

注意: フィルターの理解 悪用されるとプロジェクトの完全なコントロールにつながる可能性のある、危険な組み合わせの VM のインベントリをフィルター処理します。

- **脆弱性の深刻度 (重大/高)**: 最も影響の大きなエクスプロイトに結果を制限します。
- **ネットワーク漏洩 (インターネットダイレクト)**: 資産が外部の攻撃者によって到達可能かどうかを特定します。
- **ラベル (管理者 / 特権)**: 高レベルの ID アクセス許可で脆弱性を関連付けます。



ステップ 2: 検出を運用可能にする

継続的なガバナンスを確保するには、このクエリを自動 カスタムポリシーの作成 とレポートの作成に変換します。

カスタムポリシーの作成

これらのリスクを継続的に監視するには、クエリをカスタムポリシーに変換します。

1. ビルトインクエリページで、**[追加]** > **[カスタムポリシー]** をクリックします。[カスタムポリシーの作成] ウィザードが開きます。
2. 意味のある **名前** と **説明** を入力します (オプション)。
3. ポリシータイプは **[Query]** のままにしておきます。
4. **[既存のクエリにリンクする]** オプションを有効のままにします。

   > **注意:** これにより、ポリシーがソースクエリに対する将来の更新と同期されたままになります。

5. ポリシーに、ポリシーによってトリガーされた検出結果の深刻度レベルを決定する、**深刻度** を割り当てます。
6. (オプション) カスタムの **修正** 手順を入力して、セキュリティチームに明確なガイダンスを提供します。
7. 完了したら、**[を作成]** をクリックします。

レポートの作成

CSV レポートを作成し、関連するステークホルダー向けにこれらの高リスク VM の週次サマリーをスケジュールします。

1. ビルトインクエリページで、**[追加]** > **[レポート]** をクリックします。[レポートの作成] ウィザードが開きます。
2. 意味のある **名前** を入力します。
3. レポートタイプを **[Query] (クエリ)** のままにします。
4. **[既存のクエリにリンクする]** オプションを有効のままにします。

> **注意:** これにより、ポリシーがソースクエリに対する将来の更新と同期されたままになります。

5. **[お届け時期]** を選択します。たとえば、毎週月曜日午前に行う配信をスケジュールするには、次のようにします。
    1. **[スケジュール]** を選択します。
    2. **[M 午前10時]** で **[1 週間**ごとに繰り返し] を選択します。
6. **配信方法** を追加して、レポートのコピーを特定の受信者に送信します。
7. **[スケジュール]** をクリックします。

無視された検出結果からのパターンベースの除外の作成

目的

無視された検出結果は、多くの場合、一度に1つずつ抑制されます。手動による各無視は、共有スコープ、記録上の正当性、有効期限のない判断呼び出しです。それらのほとんどが再訪されます。このプレイブックでは、パターンについて累積された決定を監査し、文書化されたビジネスコンテキストを使用して、繰り返される決定を適切な範囲の除外に変換する方法を示します。

> **注意:** プレイブックは、プラットフォーム内でセキュリティワークフローを運用可能にするためのブループリントです。概説されている手順は、個別に無視された検出結果の管理されていないリストを、明確なビジネス上の正当性のある一連の管理された除外に変える、反復可能な方法を示しています。

ステップ 1: 無視された検出結果のパターンを監査する

除外を作成する前に、すでに無視されているものとその理由を理解しておく必要があります。[無視されたもの] タブには、個別の決定が記録されます。ポリシー別にグループ化すると、ノイズパターンが表示されます。

無視した検出結果を監査する方法

1. **[リスク > クラウドの検出結果]** に移動します。
2. **[無視]** をクリックします。

3. **[ポリシー別>グループ化]** をクリックします。

> **カウントが多いと教えてくれること:** 無視された検出結果が20件以上あるポリシーは、既存の除外が機能しているか、検出結果が一度に1つずつ手動で抑制されていることを意味します。どちらもレビューする価値があります。

4. 無視されたカウントが多いポリシーグループごとに、次のフィルターを一度に1つずつ適用します。
   a. **[アカウント]** でフィルタリングして、ノイズがDevアカウントやQAアカウントなどの1つの環境に集中しているかどうかをチェックします
   b.**[サブステータス]** でフィルタリングすると、[設計別]、[例外]、[誤検知] の理由の内訳が表示されます
   c. **[リソース]** でフィルタリングして、名前が `lab-`、`test-`、`qa-`、`sprint-` で始まるリソースなど、命名パターンを探します。
5. 表の右上にある **[エクスポート]** ボタンをクリックして、フィルタリングされたビューをCSVに保存します。

> **強力な除外候補となる理由:** フィルタリングされた結果から次のシグナルを探します。
>
> - 同じポリシーが複数のリソースにまたがって繰り返し表示されます。
> - リソースは一貫した命名パターンに従うか、`env:dev` などのタグを共有します。
> - 検出結果は1つのアカウントまたはフォルダーに集中され、本番環境全体に分散されることはありません。
>
> 1つのDevアカウントで50件の無視された検出結果を含むポリシーが、すべて `lab-*` という名前のリソースに関するものである場合、それは1つの除外を構築する価値があります。

ステップ2: パターンベースの除外を構築する

繰り返しパターンを特定したら、それを [除外] ページから除外に変換します。[除外] ページでは、範囲、リソースパターンの一致、有効期限、およびビジネス上の正当性を完全に制御できます。[検出結果] ページから直接作成された除外は高速になりますが、設定オプションが少なくて1回限りの抑制に最適です。

> **注意:** 新しい除外を作成する前に、既存の除外が検出結果をすでにカバーできるかどうかを確認してください。検出結果の表で、検出結果の横にある三点リーダーアイコンをクリックし、**[無視]** を選択して、**[既存**

の除外に追加] オプションを探します。互換性のある除外が表示された場合、検出結果を追加します。これにより、除外カウントが不必要に増加するのを防ぐことができます。

パターンベースの除外を作成する方法

1. **[ポリシー]** > **[除外]** に移動します。
2. [組織] ドロップダウンボックスで、パターンが発生する特定のアカウントまたはフォルダーを選択します。パターンが本当にあらゆる場所に当てはまる場合を除き、組織全体に範囲を限定しないでください。
3. **[除外の追加]** をクリックします。アカウントの範囲は、開始後は変更できません。
4. **[名前]** ボックスに、検出結果のタイプではなく、ビジネスの文脈を説明する名前を入力します。例: Dev1 のパブリックにアクセス可能な EC2 インスタンス – QA テスト
5. **[説明]** ボックスに、理由を入力します。例: 開発アカウントがロードテスト用に EC2 インスタンスを意図的に公開しています。レビューの結果、実稼働には適用できないことを確認しました。オーナー: QA チーム。
6. **[アクション]** で、**[検出結果を無視]** を選択し、**[理由]** を選択します。
   - 設計上: 構成は意図的なものであり、機能のために必要です。
   - 例外: 修正の進行中は、検出結果が一時的に受け入れられます。
   - 誤検出: 検出結果が不正確または無関係であることが確認されました。

   理由は、この除外がカバーする各検出結果に表示されるサブステータスになります。
7. **[ターゲットの検出結果]** で、**[タイプ]** を [クラウド] に設定します。
8. **[ポリシー]** で、**[特定のポリシー]** を選択し、関連するポリシーを選択します。

   > **注意:** 各除外のスコープを 1 つのポリシーに設定してください。無関係のポリシーを1つの除外に混在させると、対象範囲の重複が生じ、監査が難しく、ステークホルダーに正当化することが難しくなります。

9. **[ターゲット リソース]** で、**[特定のリソース]** を選択し、ワイルドカードを使用して **名前** のパターンを入力します。

- アスタリスク * は、0 文字以上と一致します。
- クエスチョンマーク ? 1 文字に一致します。

たとえば、`lab-*` は、名前が `lab-` で始まるすべてのリソースを対象とします。規則に従わない手動で名前が付けられたインスタンスもキャッチするには、2 番目の条件 OR リソース名が `JohnD` と等しい。

> **重要:** 保存する前に、**[検出結果のプレビュー]** パネルでパターンをテストします。広範囲の除外の `prod-*` のようなパターンでは、同じ名前プレフィックスを共有する新しく作成された本番リソースが自動的に除外されます。プレビューパネルには、現在ターゲットになっている未解決の検出結果がすべて表示されます。

10. **[有効期限]** で、恒久的な設定の場合は [なし] を選択し、既知の終了日がある許容リスクの場合は [有効期限] を選択します。
11. **[検出結果のプレビュー]** パネルを確認して、範囲が意図と一致していることを確認します。
12. **[Save]** (保存) をクリックします。

保存後、除外は次のスキャンサイクルに有効になります。対象となる検出結果は、サブステータスとして選択した理由とともに、オープンから無視に移動します。

除外を監査して維持する

目的

除外が低下します。リソースの名前が変更され、環境が廃止され、かつて有効な例外だったものが、実際の検出結果を隠して静かにデッドカバレッジになります。このプレイブックでは、アクティブな除外の正確性を確認し、スコープのドリフトが複合化する前にキャッチし、有効なビジネスケースを反映していないカバレッジを削除する方法を示します。

> **注意:** このレビューを毎月実行してください。所要時間は約 15 分で、未解決の検出結果の精度が徐々に失われるのを防ぎます。

ステップ 1: 警告サインがないか各除外を確認する

アクティブな除外を確認する方法

1. **[ポリシー]** > **[除外]** に移動します。
2. 表内の除外ごとに、次の4つをすべてチェックします。
    1. **検出結果カウントはゼロです。** 検出結果をカバーしない除外は、ターゲットとなるリソースがもはや存在しないか、名前のパターンがずれていることを意味する可能性があります。すぐには削除しないでください。最初に除外を無効にし、1つのスキャンサイクル待機します。検出結果が再オープンされない場合、除外は安全に削除できます。
    2. **有効期限が過ぎているか、7日以内です。** 新しい正当な理由で更新するか、有効期限を切れさせて、検出結果が再オープンされるかどうかを確認します。現在の検出結果カウントを最初に確認せずに更新しないでください。
    3. **範囲が元のビジネスケースよりも広い**抑止するつもりはなかったアカウントまたはリソース全体の検出結果が除外に含まれるようになった場合は、範囲を絞り込むか、別々の除外に分割します。
    4. **検出結果の数は、作成以来大幅に増加しています。** 大幅に増加すると、環境が拡張され、除外が元の正当理由でサポートされる範囲を超える範囲をカバーすることを意味します。同じ範囲で更新する前に、追加の検出結果の範囲とリスクが同等であるかどうかを確認してください。

ステップ2: 削除する前に無効にする

除外を削除する前に、除外がカバーする検出結果が実際の問題であり、有効な抑制ではないことを確認してください。

除外を安全に削除する方法

1. 除外の横にある三点リーダーアイコンをクリックし、**[無効化]** を選択します。除外は無効になりますが、表には残ります。
2. 次のスキャンサイクルを待ちます。以前は非表示だった検出結果は、オープンに戻ります。
3. 再オープンされた検出結果を確認します。次のいずれかを行います。
    - 再オープンされた検出結果が修正が必要な実際の問題である場合は、除外を削除します。ライブリスクを隠していたのです。

- 再オープンされた検出結果が確認された誤検出または許容リスクである場合は、除外を復元するか、より狭い範囲で再構築します。

重要: 再オープンされた検出結果を最初に確認せずに除外を削除すると、予期しない大量の検出結果が一度に表面化する可能性があります。常に最初に無効にしてから、決定します。

ステップ 3: 除外の所有権を確認する

自分で作成していない除外の場合は、更新または変更する前に正当性を検証してください。

除外の所有権を確認する方法

1. [除外] テーブルで、各除外の **[作成者]** 列と **[作成時刻]** 列を確認します。
2. 明確な説明がない除外については、**[説明]** フィールドを確認します。正当な理由がないか曖昧な場合は、除外を更新する前に作成者に連絡してください。
3. 除外を作成または変更したユーザーの完全な履歴を表示するには、**[Settings > Audit]** に移動し、関連する除外アクションでフィルタリングします。たとえば、「`Create risk exclusion`」と入力します。

   注意: 監査ログには、ユーザー、アクション、タイムスタンプが表示されます。作成者がチームを去ったとき、または除外のビジネス上の文脈が不明確な場合に、所有権を追跡するために使用します。

独自の機密データの管理

目的

安全でない場所にデータが漏洩するのを防ぐために、ビジネスに固有のデータを特定、監視、保護します。カスタムデータタイプを作成してカスタムポリシーに追加することで、固有のデータパターンを追跡し、承認された境界外でデータが検出されたときにアラートを受け取ることができます。

内部アカウント ID やプロジェクトコードなど、ビジネスに固有の情報がある場合、それは Tenable One Cloud Exposure スキャン対象データタイプ対象にはならない場合があります。このプレイブックでは、機密

情報が安全な環境に残されるようにするためのワークフローを提供しており、機密情報が認証されていない場所に移動された場合にアラートをトリガーします。

> 例: Global-Logistics ID シナリオ

所属組織が、**Global-Logistics ID** という独自の内部識別子を使用して、世界の出荷を追跡します。これらの ID は特定の形式 (例:「GL-12345678」) に従い、機密のビジネス情報と見なされます。

目標は、このプレイブックを使用して以下を行うことです。

- **マルチクラウド環境全体でこれらの ID が保存されている場所を特定します**。
- **これらの ID が公開ストレージバケットや開発アカウントなどの認証されていない場所で見つかった場合、通知を受け取る**。

関連記事

- カスタムデータ型の作成
  - データリソース
- クラウドポリシー: カスタム
  - クラウドの検出結果

> **注意:** プレイブックは、プラットフォーム内でセキュリティワークフローを運用するためのブループリントとして機能します。概説されている手順は、技術的な可視性を一貫性のある実用的な結果に変換するために繰り返し利用できる手法です。このガイドでは特定のユースケースに焦点を当てていますが、これらの原則は他のリソースタイプやセキュリティシナリオにも適用できるため、環境全体の包括的なリスク管理が可能になります。

ステップ 1: ビジネス固有のデータを定義する (カスタムデータタイプ)

自社に固有のデータを管理するには、クラウドサイバーエクスポージャー がそれを認識できるように、まずその構造を カスタムデータ型の作成 として定義する必要があります。特定の従業員 ID の形式にかかわらず、正確な定義は高精度のスキャンの基盤となり、信頼できる検出の基盤となります。

カスタムデータタイプを作成する方法

1. **[設定]** > **[クラウドサイバーエクスポージャー]** > **[Data]** > **[Data Types]** に移動し、**[Add Custom Data Type]** をクリックします。
2. **名前**、**カテゴリ**、**機密性**などのデータタイプのパラメーターを定義します。
    - 初回スキャンでは、**[機密性]** を [パブリック] または [プライベート] に設定することをお勧めします。これにより、深刻度の高いアラートを即座にトリガーしたり、リソースのリスクスコアに影響を与えたりすることなく、検出結果を観察し、検出の精度を検証できます。
3. RE2 形式を使用して、**[含める] の正規表現** フィールドでデータの一意の構造を定義します。
    - パターンが正確であることを確認するために、regex101.com などのツールを使用することをお勧めします。
    - たとえば、プレフィックス「GL-」の後に 8 桁の数字「GL-12345678」が続く **Global-Logistics ID** には、式 `\bGL-\d{8}\b`が必要です。
4. **コンテキスト** キーワードを追加して、検出の精度を高めることができます。これらのキーワードはクラウドサイバーエクスポージャー、正規表現が構造化されていないファイルで関連する語句に近接して表示される場合、または構造化されたデータの特定の列名および JSON キーでのみ一致にフラグを立てるようにします。

> 例: カスタムデータタイプの作成

出荷識別子のカスタムデータタイプ (「`GL-12345678`」など、プレフィックス「GL-」の後に 8 桁の数字で構成されます) を作成するには、次のパラメーターを**カスタムデータタイプ** ウィザードの追加

- **名前**: グローバルログイン ID
- **説明**: 「GL-」プレフィックスで始まる独自の出荷識別子
- **カテゴリ**: PII
- **秘密性** プライベートリスクスコアに影響を与えないように、最初のスキャンでプライベートに設定。検証されたら、Proprietary に更新してください

値とコンテキストの構成

- **インクルード正規表現** `\bGL-\d{8}\b`
- **コンテキスト正規表現** `ShipmentID`, `LogisticsKey`, `Logistics`

コンテキスト正規表現 条件を追加することで、関連するロジスティクスキーワードの近くで表示されない限り、8 桁のランダムな文字列にフラグが立てられないようにします。

ステップ 2: 検出と正確性を検証する

ポリシーは、その背後にある検出ロジックと同程度に効率的です。ポリシーを作成する前に、検出ロジックが意図したとおりに動作することを確認する必要があります。このフェーズにより、正規表現やコンテキストキーワードが正しい情報を特定できるようになります。

検出を検証する方法

1. クラウドサイバーエクスポージャーでスキャンサイクルを完了させます。通常、新しいデータタイプを作成するか既存のデータタイプを更新した後、検出結果がコンソールに入力されるまでに2448時間必要です。
2. **[調査]** > **データリソース** に移動し、新しい **データタイプ** でインベントリをフィルタリングし、一致をトリガーした特定のリソースを隔離します。

   > **重要:** 結果がゼロの場合、またはデータタイプが予期しないリソースにある場合は、正規表現がより正確であることを示している可能性があります。ステップ 1: ビジネス固有のデータを定義する (カスタムデータタイプ) に戻って、**含める** または **コンテキストの** 正規表現を調整することを検討してください。

3. リソースで、**[データ]** > **[分類されたデータ]** に移動し、そのデータタイプを含むオブジェクトまたはテーブルを見つけます。[サンプル] ツールチップを使用して、オブジェクトまたはテーブル内の機密データの場所を検証します。
4. サンプルが想定するデータ形式と一致する場合、検出署名はポリシー適用の準備ができました。

> **注意:** 最初のスキャンが完了して結果を検証した後、データタイプの機密性レベルをプロプライエーターに更新します。

> 例: 検出結果を検証する

スキャンサイクルが完了するのを待ってから、Global-Logistics ID の新しい検出署名の精度を検証します。

- **検出結果**: **データリソース** ページに移動し、Global-Logistics ID データタイプでフィルタリングします。結果には、このデータタイプを含むリソースが表示されます。データタイプが予期しないリソースにある場合、正規表現をより正確にする必要があることを示している可能性があります。**Include regex** の微調整を検討してください。
- **分類されたデータの場所を確認します**: リソースプロファイルで、**データ** > **分類されたデータ** に移動し、Global-Logistics ID データタイプを含むオブジェクトまたはテーブルを見つけます。。その行で、サンプルツールチップを調べて、オブジェクトまたはテーブル内の機密データの場所を確認します。

ステップ 3: ガバナンスを実施する (カスタムクラウドポリシー)

検出ロジックを検証したら、クラウドポリシー: カスタムことで、検出からアクティブガバナンスに移行できます。この手順により、独自のデータの存在が許可されている場所を特定し、その境界の外に移動したときにアラートをトリガーすることで、データの拡散を監視できます。

カスタムポリシーの作成手順

1. **[ポリシー]** > **[クラウドポリシー]** に移動し、**[カスタムポリシーの作成]** をクリックします。
2. **[名前と説明]** を入力します。
3. **[Type]** ドロップダウンで、[Template] を選択します。
4. **[テンプレートの選択]** をクリックします。
    1. **機密データの監視** テンプレートを選択し、関連するプロバイダーの要件に適合するガバナンス戦略を選択します。
        - **この機密データはこれらのリソースに存在するべきではありません**: 公開ストレージや開発環境などの認証されていない場所に機密データが表示されたときに、検出結果が生成されます。
        - **この機密データは以下のリソースにのみ存在する必要があります**。機密データは承認されたリソース内にのみ存在するようにしてください。定義された境界の外でデータが発見されたときに、検出結果が生成されます。
    2. **[秘密データ]** ドロップダウンで、監視する秘密データを選択します。具体的には、[これらの

データタイプの機密データ] オプションから関連するデータタイプを選択します。

3. **[リソース]** ドロップダウンで、ポリシー境界を定義する関連リソーススコープを選択します。

5. このポリシーから生成された検出結果の **深刻度** レベルを設定します。これにより、これらの検出結果を環境内でどのように優先順位を付け、内部リスク管理基準に基づいて表示するかが決まります。
6. **[修正]** ボックスに、このポリシーによってトリガーされた検出結果の処理方法を説明する、企業のワークフローまたは手順を書き込みます。

> 例: カスタムポリシーの作成

Global-Logistics ID の検出が正確であることを検証しました。次は、このデータが [パブリック] のラベルが付いたパブリック AWS バケットに表示されないようにポリシーを作成します。

- カスタムポリシー設定:
  - **名称**: Global-Logistics ID データの拡散監視
  - **説明**: パブリック・バケット内での Global-Logistics ID の使用は許可されていません
- **テンプレート**: Monitor Sensitive Data > AWS > この機密データは、これらのリソースに存在するべきではありません
- **秘密データ > これらのデータタイプの秘密データ**: Global-Logistics IDを選択データ型を発見しました。
- **リソース > これらのラベルのデータリソース**: パブリック。
- **重要度**: 高 (公開バケットにある独自のロジスティクス ID は会社のポリシーに直接違反するため、[高] を選択します)。
- **修正**:

```
1 . オブジェクトへの公開アクセスをブロックします
2. Jira チケットを開いて InfoSec に割り当てます
```

保存されると、システムは Global-Logistics ID が Public というラベルの付いた AWS 公開バケットで検出された瞬間に検出結果を生成するようになりました。

ライセンス数の増加または超過に対処

目的

Tenable One Cloud Exposure のライセンス数は、必ずしも明らかではないいくつかの理由で増加することがあります。このプレイブックでは、ライセンスを消費しているものを確認し、増加の原因を特定し、消費を減らす方法や超過に対処する方法を示します。

ステップ 1: ライセンスの使用状況を確認する

1. **[Settings] › [Licensing] に移動します**。
2. 権利に対する現在の消費量と、増加に最初に気付いた日付を書き留めます。
3. ライセンスのある各リソースタイプをクリックして **[Inventory] (インベントリ)** ページを開き、請求されるリソースのリストを表示します。

> **注意:** ライセンス数は、リアルタイムではなく定期的に更新されます。

ステップ 2: 一般的な原因を除外する

原因不明な増加のほとんどは、次のことが原因です。

- **仮想マシンのデータディスクスキャン仮想マシンデータディスクのスキャン**が有効になっている場合、データディスクは請求対象のリソースとしてカウントされるため、カウントが著しく増加する可能性があります。データディスクのスキャンを無効にするには、**[Settings] › [Security] › [Workload] › [Virtual Machine]** に移動します。ディスクが請求対象としてカウントされなくなるまでに最大 1 週間かかります。
- **コンテナホスト (レガシーライセンスのみ)。** レガシーライセンスモデルでは、コンテナをホストする仮想マシンは、ホストとして 1 回、コンテナホストとして 2 回カウントされる可能性があります。現在のライセンスモデルでは、コンテナをホストしている場合でも、仮想マシンは 1 回のみカウントされます。
- **データセキュリティスキャンプライベートバケットスキャンとデータベーススキャン**が有効になっている場合、消費量が増加する可能性があります。データセキュリティスキャンを無効にするには、**セキュリティ>データ>Settings**に移動します。

- **イメージスキャン仮想マシンイメージのデータスキャンを有効にすると、**請求対象の資産が追加されます。イメージスキャンを無効にするには、**Settings** › **[セキュリティ]** › **[仮想マシン>ワークロード]** に移動します

ステップ 3: 増加を追跡する

1. **[Settings]** › **[Licensing]** に移動し、請求使用量が増加したリソースタイプを選択します。
2. **[Explore > Explorer]** に移動し、**[Billing Usage]** (次の **値より大きい)** `0` のクラウドリソースをクエリして、請求対象の資産を一覧表示します。
    1. 増加の前後の作成 **時間** でフィルタリングします。
    2. 新しくオンボーディングされたアカウント、有効な機能、大規模なデプロイメントなど、最近の変更とクロスチェックします。

ステップ 4: 消費を減らすか、超過に対処する

- **不要なスキャンを停止します。**適切な範囲で関連機能を無効にしてください。
- 古い仮想マシンまたは非アクティブな仮想マシンを削除します。**[Explore > Explorer の探索]** に移動して、可能性のある仮想マシンを特定します。
    - 請求対象のリソースから始めます。**[Billing Usage]** のクエリ: **[Greater than** `0` **]** は、ライセンスを消費する仮想マシンのみを確認します。
    - ステータスのフィルタリング **が停止されています**。
    - **アカウント**、**リージョン**、**タイプ**でフィルタリングまたはグループ化して、停止または終了した仮想マシンや廃止されたアカウントのリソースなどのクラスタを露出します。
    - リストをエクスポートして、仮想マシンが非アクティブであることをリソースの所有者に確認した後、クラウドプロバイダー内で仮想マシンを停止または削除します。
- **一時的な増額をリクエストします。**使用量をライセンス制限に合わせて調整している間に期限切れが生じた場合は、一時的な調整について Tenable サポートに連絡してください。

警告: 設定を変更したり、リソースを停止/削除したりした後、カウントはすぐには更新されません。カウントに変化が反映されるまでに最大 1 週間かかります。上記の原因で増加を説明できない場合は、コンテナ ID と、インベントリビューとライセンスビューのエクスポートを Tenable サポートに連絡してください。

クラウドオンボーディングのアクセス許可とロールのエラーを解決する (AWS、Azure、GCP)

目的

クラウドオンボーディングの失敗の多くは、アクセス許可に起因します。Tenable One Cloud Exposure が使用するロールまたはサービスアカウントにアクションがない、組織のポリシーによってブロックされている、または間違った範囲で作成されたなどです。アカウントまたは組織がオンボーディングを完了しなかった場合、ステータスが `Connected with Issues` または `Failed` を示した場合、またはセットアップスクリプトが正常に完了したように見えたにも関わらず `Missing permissions` エラーを返した場合に、このプレイブックを使用します。

> **注意:** セットアップスクリプトがエラーなしで終了しても、接続のアクセス許可が満たされていないままになることがあります (たとえば、Tenable が必要とするものをすべて付与する権限を持たないアイデンティティで実行されている場合)。完了 **ステップで** アクセス許可がないことが報告された場合、エラーなしで完了したスクリプトではアクセス許可の完了は確認されません。

ステップ 1: ロールとサービスアカウントの設定を検証する

> **注意:** これらのチェックは、CSP に関係なく適用されます。

ロールまたはサービスアカウントが正しいことを確認するには

1. 提供されたオンボーディングスクリプトまたは Terraform モジュールを使用して、ロールまたはサービスアカウントをデプロイします。手動でトリミングされたアクセス許可セットは、`Missing permissions` エラーの最も一般的な原因です。
2. 個別のアカウントではなく組織全体のオンボーディング組織レベルで接続することで、アカウントを一度に 1 つずつオンボーディングする必要がなくなり、新しいアカウントとそのリソースが追加されても、クラウドサイバーエクスポージャーは継続的に可視化を確保できます。組織で設定を実行して、メンバーアカウントが自動的に検出され接続されるようにします。

3. アクセス許可を変更した後、次の方法で修正を確認します。
    - オンボーディングウィザードを再度開き、**[完了]** をクリックします。
    - 次のオーケストレーションサイクルまで待ってから、問題が解決したかどうかを確認します。

ステップ 2: クラウド固有のブロッカーを確認する

AWS

- **サービス制御ポリシー (SCP)。** 組織レベルの SCP は、ロールと CloudFormation スタックが正しいと思われる場合でも、クラウドサイバーエクスポージャー ロールを密かにブロックできます。クラウドサイバーエクスポージャー が必要とするアクションを拒否する SCP がないことを確認します。これは、メンバーアカウントが `Connected with Issues` ステータスでスタックする原因として頻繁に発生します。
- **組織全体の StackSets** AWS 組織の場合は、CloudFormation StackSet がすべてのメンバーアカウントにロールをデプロイしたことを確認します。ロールのないアカウントは、管理アカウントに問題がなければ見える場合でも、ステータスが `Connected with Issues` または `Failed` 表示されます。
- **クロスアカウントの CloudTrail と KMS。** CloudTrail バケットが別のログアーカイブアカウントにある場合、または別のアカウントの AWS Key Management Service (KMS) キーで暗号化されている場合、クラウドサイバーエクスポージャー ロールにはクロスアカウント読み取りアクセス権と KMS 復号化アクセス許可が必要です。

Azure

- **ビルトインロールとカスタムロール**クラウドサイバーエクスポージャー は、特定の組み込みロールの割り当てをチェックします。同等に見えるカスタムロールでも、チェックに失敗する可能性があります。Tenable によって指定された組み込みロールを割り当てます。
- **ディレクトリのアクセス許可。** Microsoft Entra ID テナントまたは組織のオンボーディングには、十分なディレクトリ権限 (同意を付与するためのグローバル管理者ロールなど) が必要です。通常、最後のステップの `Missing permissions to retrieve organization data` エラーは、この原因を示しています。

- **セカンドテナントまたはシングルサインオン (SSO) 認証ループ。** プライマリコンテナが企業ドメイン SSO を強制する場合、2 つ目の Microsoft Entra ID テナントをオンボーディングすると認証ループが発生する可能性があります。この問題を解決するには、ターゲットテナントの管理者認証情報を使用してプライベートまたはシークレットのブラウザウィンドウを使用するか、アプリケーションをサービスプリンシパルとして手動で登録して、テナント ID、クライアント ID、シークレットを直接入力します。

GCP

- **組織の範囲とプロジェクトの範囲。** 個別のプロジェクトをオンボーディングする場合、プロジェクト所有者ロールだけでは十分ではありません。組織レベルで必要なロールを割り当てます。

ステップ 3: 接続を確認する

接続ステータスを確認する方法

1. オンボーディングウィザードを再度開き、**[完了]** をクリックしてキーのアクセス許可を検証します。ここでは、主要なアクセス許可のみがチェックされ、フルセットはチェックされません。
2. 次のオーケストレーションサイクルを待ちます。
3. 管理アカウントだけでなく、各メンバーアカウント、サブスクリプション、またはプロジェクトに `Connected` ステータスが表示され、データが入力され始めることを確認します。
4. 最初の完全な分析が完了するまで待ちます。大規模な企業の場合、検出結果のデータが入力されるまでに数時間かかることがあります。

重要: それでもアカウントが接続されない場合や、ロール、SCP、StackSets が正しいにも関わらず次のオーケストレーションサイクル後にアカウントがスタックした場合は、Tenable サポートにお問い合わせください。コンテナ ID、クラウドプロバイダー、および正確なエラーテキストを入力します。

常設管理者アクセスをジャストインタイムアクセスに変換する

必要なライセンス: このプレイブックには、JIT とオンデマンドの最小権限の推奨事項の両方を含むライセンス別機能比較 が必要です。JIT ライセンスだけでは、最小権限の推奨は含まれていません。

目的

常時の管理者アクセス権を持つユーザーは、恒久的なターゲットです。認証情報が漏洩すると、攻撃者はいつでも管理者になります。このプレイブックでは、ユーザーがそのアクセスで実際に何をするかを測定し、リクエストに応じて正確にそれを付与する JIT 使用資格を構築し、スタンディング割り当てを削除する方法を示します。

一度に 1 人のユーザーに対して実行します。**[過剰なアクセス許可]** ページで、管理者アクセスがアクセス許可の深刻度が [重大] と表示されているユーザーから開始します。

前提条件

始める前に

- Tenable One Cloud Exposure で**管理者**ロールがあることを確認します。最小権限ポリシーの生成には、**コラボレータ**または**管理者**が必要です。使用資格の追加には、**管理者**または**JIT 管理者**が必要です。
- 関連するクラウドプロバイダーに対して Tenable JIT アクセス許可を付与する されていることを確認してください。
- ユーザーが SSO 経由で JIT ポータルにログインできることを確認します。
    - AWS: JIT for AWS は Identity Center ユーザーおよびグループにのみアクセス権を付与するため、ユーザーが IAM Identity Center ユーザーであることを確認してください。常任管理者が IAM ユーザーの場合は、開始する前にユーザーを Identity Center に移動します。

> **警告:** JIT の使用資格が機能することを確認するまで、スタンディングアサインメントを削除しないでください。最初に取り消すと、ユーザーはまだ行う必要がある作業からロックされます。

ステップ 1: 使用状況の決定

クラウドサイバーエクスポージャーは、アクセス許可使用のラーニング期間 (デフォルトでは 90 日) 中使用されなかった場合、過剰なアクセス許可としてマークします。その計算の背後にある使用状況データは、JIT アクセス許可の基礎となります。

ユーザーの使用状況を確認する方法

1. クラウドサイバーエクスポージャーコンソールで、**[過剰なアクセス許可のリスク>]** に移動します。
2. 関連するユーザーについてテーブルをフィルタリングし、[Services] (**サービス**) と **[Resources] (リソース)** 列を確認します。これらは、ユーザーがアクセスできるもののまだ使用していないサービスとリソースの数を示します。
3. ユーザーをドリルダウンして、使用済みと未使用のアクセス許可、およびアクセス許可のマッピングを確認します。
4. ユーザーが学習期間よりも頻度が低いタスク (たとえば四半期決算や年次キーローテーションなど) を書き留めます。使用状況データはこれらをキャプチャしないため、アクセス許可セットを生成するときに手動で追加する必要があります。

ステップ 2: 最小権限のアクセス許可セットを生成する

ユーザーの実際のアクティビティから最小権限ポリシーの生成とロールポリシーまたはカスタムロールを生成します。これは、ユーザーが JIT を通じてリクエストするアクセス許可になります。

アクセス許可セットを生成する方法

1. クラウドサイバーエクスポージャーで、**[IAM > Identity Intelligence >調査]** に移動します。
2. 関連するアイデンティティを見つけて、次のいずれかを実行します。
    - **AWS**: 三点リーダーメニューをクリックし、**[最小権限ポリシーの生成]** を選択します。ワイルドカードではなく特定のリソースを使用する (サポートされている AWS サービスのみ) をクリアします。特定のリソースによりポリシーは大きくなり、ポリシーは資格のインラインポリシー制限に収まる必要があります。
    - **Azure**: Microsoft Entra ID ユーザーの **[カスタムロールの生成]** をクリックします。ユーザーがアクセスを必要とする場所に一致する **範囲レベル** (管理グループ、サブスクリプション、またはリソースグループ) を選択します。
    - **GCP**: [Google Workspace ユーザーの **カスタムロールの生成]** をクリックします。ユーザーがアクセスする必要がある場所に一致する **範囲レベル** (組織、フォルダー、またはプロジェクト) を選択します。

3. ユーザーの作業サイクル全体をカバーする学習期間 (Azure と GCP の場合は**タイムフレーム**) を設定します。少なくとも 90 日間のデフォルトを使用します。
4. ユーザーがグループを介して管理者アクセス権を取得した場合は、**[グループ メンバーシップ経由で付与されたアクセス許可を含める]** を選択します。
5. **[生成]** をクリックし、結果をコピーします。
6. 以前に書き留めた頻度の低いタスクを追加します。
7. (Azure および GCP のみ): 生成された定義からクラウドプロバイダーのカスタムロールを作成します。JIT の使用資格には、すべてのビルトインロールとカスタムロールがリストされるため、資格が作成される前にロールが存在している必要があります。

> **注意: AWS**: 生成されたポリシーがAWSの最大ポリシーサイズを超える場合、クラウド サイバーエクスポージャー はポリシーを複数のポリシーに分割します。数字は JSON ポリシーアイコンの横の括弧内に表示されます。

ステップ 3: アクセス許可セットの JIT 使用資格の作成

資格は、誰が、どのアカウントに対して、どのくらいの期間、誰の承認を得て、アクセス許可セットをリクエストできるかを定義します。

使用資格を作成するには:

1. JIT ポータルで、ユーザーが必要とするアカウントを含む範囲を選択します。
2. **[資格]** に移動し、**[資格の追加]** をクリックします。
3. タスクを説明する **[名前]** (Name `Prod DB Admin`など) を入力します。リクエスト者にはこの名前が表示されます。
4. **[ユーザーとグループ]** で、ユーザーを選択します。
5. **[アクセス許可]** で、先ほど生成したアクセス許可セットを追加します。
    - **AWS**: 生成されたポリシーを **[インラインポリシーの追加]** に貼り付けます。インラインポリシーは 7,680 文字を超えることはできません。
    - **Azure**: カスタムロールを選択します。サブスクリプション以下のアクセスを制限するには、**[リ**

ソース グループのみ] を選択し、リソース グループを選択します。

- GCP: カスタムロールを選択します。

6. **[アカウント]** で、ユーザーが常時の管理者アクセス権を持っているアカウントのみを選択します。各リクエストをさらに制限するには、**[リクエストごとのアカウント選択を制限する]** を有効にします。
7. **[最大期間] は**、一般的なタスクをカバーする最短の期間に設定します。範囲は1～24時間です。
8. 承認 **ワークフロー** で、**承認が必要** を選択し、1人以上の**承認者**を選択します。管理者レベルのアクセスの場合、第2承認レベルの追加を検討してください。
9. **正当性と判断を有効にします**。
10. **[反復アクセス]** で **[無効]** を選択するか、低く**[反復日数の最大日数]** の値を設定します。反復アクセスはデフォルトで最大 364 日間有効になっており、1年間のスケジュールされた再付与はスタンディングアクセスとよく似ています。
11. **[Add]** (追加) をクリックします。

ステップ 4: 資格が機能することを確認する

スタンディングアクセスが有効な状態でユーザーに使用資格をテストしてもらいます。

資格を確認するには:

1. ユーザーに、JIT ポータル、Slack、または Teams を通じて アクセスをリクエストする し、付与されたアクセス許可で実際のタスクを1つ実行するように依頼します。テストを意味のあるものにするには、ユーザーはスタンディングアクセスではなく、JIT で付与された割り当てを通じてサインインする必要があります。
2. タスクが失敗した場合は、不足しているアクセス許可を資格に追加してテストを繰り返します。
3. JIT ポータルで、[Audit > **Access Requests] (アクセスリクエストの監査**) に移動し、リクエスト、承認、期間が想定どおりに表示されることを確認します。

ステップ 5: スタンディング アクセスを取り外す

クラウドプロバイダーのスタンディング割り当てを削除します。ユーザーに適した終了状態を選択します。

- **オプションA:スタンディングアクセスはゼロです。** すべてのスタンディング割り当てを削除します。JIT リクエストが承認されるまで、ユーザーはアカウントにアクセスできません。
- **オプション B: 読み取り専用ベースライン。** 管理者の割り当てを、読み取り専用ロール(`ReadOnlyAccess`、Azure **Reader**、GCP **Viewer** などAWS) に置き換えます。ユーザーは日常業務の可視性を維持し、変更があれば JIT にリクエストします。

注意: [過剰なアクセス許可] ページからのワンクリック修正は、どちらの終了状態にも達しません。ユーザーのポリシーを、使用済みのアクセス許可から構築された最小権限ポリシーに置き換えるため、ユーザーが実行した管理者アクションは維持されます。

スタンディングアクセスを削除するには:

- **AWS**: IAM Identity Center で、管理者アクセス許可セットに対するユーザーのアカウント割り当てを削除します。ユーザーがグループを通じてアクセス許可セットを取得した場合は、そのユーザーをグループから削除します。グループの割り当てを変更しないでください (他のメンバーは引き続きその割り当てに依存しています)。オプション B では、読み取り専用のアクセス許可セットを割り当てます。
- **Azure**: サブスクリプションまたはリソースグループでのユーザーのロール割り当てを削除します。オプション B では、同じスコープで **Reader** を割り当てます。
- **GCP**: 組織、フォルダー、またはプロジェクトにおけるユーザーの IAM バインディングを削除します。オプション B では、同じレベルの **Viewer** を付与します。

警告: Azure: Azure では、すべてのサブスクリプションに少なくとも 1 人のアクティブな所有者を保持する必要があります。ユーザーが最後の恒久的な所有者である場合は、ユーザーを削除する前に (JIT 外部の) 恒久的な所有者を割り当てます。それ以外の場合、唯一の所有者になる JIT で付与された所有者の割り当ては期限切れになりません。詳細については、「FAQ: JIT」を参照してください。

ステップ 6: 結果を確認する

結果を確認する方法

1. クラウドサイバーエクスポージャーコンソールで、**[Risks > Excessive Permissions] (過剰なアクセス許可**のリスク) に移動し、ユーザーが管理者レベルの過剰なアクセス許可で表示されなくなったことを確認します。ユーザーの過剰な権限の検出結果は、次の同期後にクローズされます。

2. JIT ポータルで、2 週間後のユーザーの **>アクセスリクエストの監査** を確認します。最大期間に達する要求が頻繁に発生する場合は、期間が短すぎるか、ユーザーの作業に別の資格が必要であることを意味します。リクエストが発生しない場合、そのユーザーはそのアクセス権がまったく必要ない場合があり、ユーザーはその資格を削除できます。

サンプル修正ワークフロー

検出結果を分析して修正するには、以下の手順にある一般的なガイドラインに従ってください。

検出結果を修正する方法

1. Tenable One Cloud Exposure コンソールで、**[検出結果]** をクリックします。
2. 関連するフィルターを適用して、表示される検出結果の範囲を絞り込みます。詳細については、検出結果ページの操作参照してください。
3. 関連する検出結果をクリックしてドリルダウンし、検出結果のすべての分析を表示します。
4. 以下のような検出結果の詳細情報とその他の関連情報を確認して、理解を深めます。
    - 検出結果の主な原因は何ですか
    - 検出結果の範囲
    - が環境にもたらす潜在的なリスク
    - 検出結果の深刻度の説明
5. **修正** 領域に移動し、一覧表示されている手順をよく確認します。

    > **注意:** IaC Securityを使用する場合、この領域には検出結果に応じて **IaC** と **Console** の 2 つのタブが表示される場合があります。[IaC] タブではプルリクエストによるコードベースの修正が提供され、[コンソール] タブではクラウドベースの修正が提供されます。

6. 現時点で検出結果を修正できない正当な理由がある場合は、検出結果を無視するできます。
7. 検出結果に修正アクションが必要であると判断した場合は、次のいずれかを行います。
    - リストされている手順に従って、検出結果を手動で修正する。これには、検出結果に対する検出結果に基づくアクションのトリガーも含まれます (たとえば、Jira 問題を作成して、開発者の 1 人が検出結果を修正できるようにするなど)。

- 検出結果で使用可能な場合、**修正** Remediate ボタンを使用して検出結果の自動修正

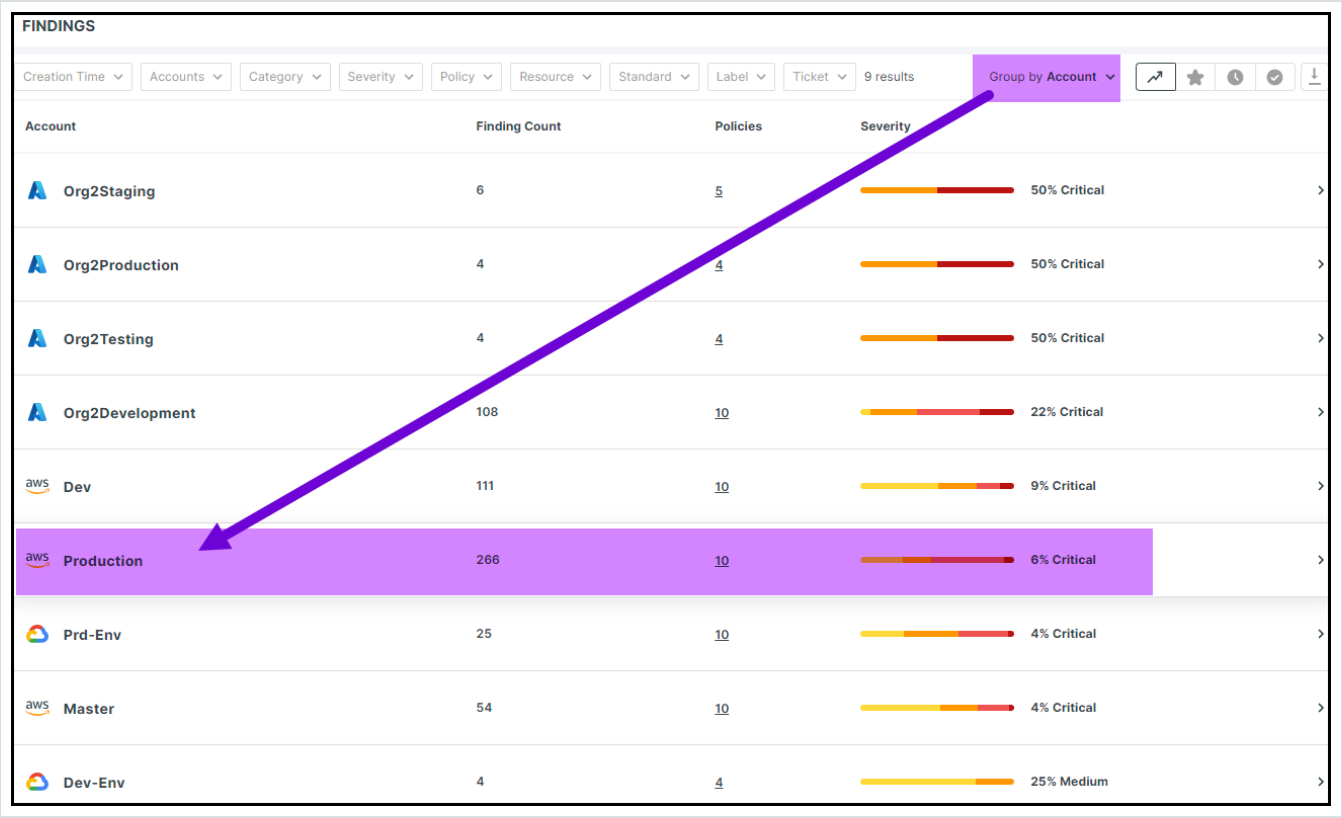
> **注意:** 検出結果を自動的に修正するには、次のいずれかを行う必要があります。1) Tenable オンボーディング [[中に、関連クラウドアカウントに] 管理権限を付与するか、または、2) Tenable ワンタイム認証情報を提供する 必要な修正を実行する発見しました。

8. 検出結果を手動で修正した場合、修正後に検出結果を手動でクローズする [オープンな検出結果] ページから削除できます。問題が修正されると、Tenable がその問題を自動的に検出して解決します。この自動識別には時間がかかる場合があるため、手動でクローズしすると、より早く [Open Findings] (オープンの検出結果) ページから削除することができます。

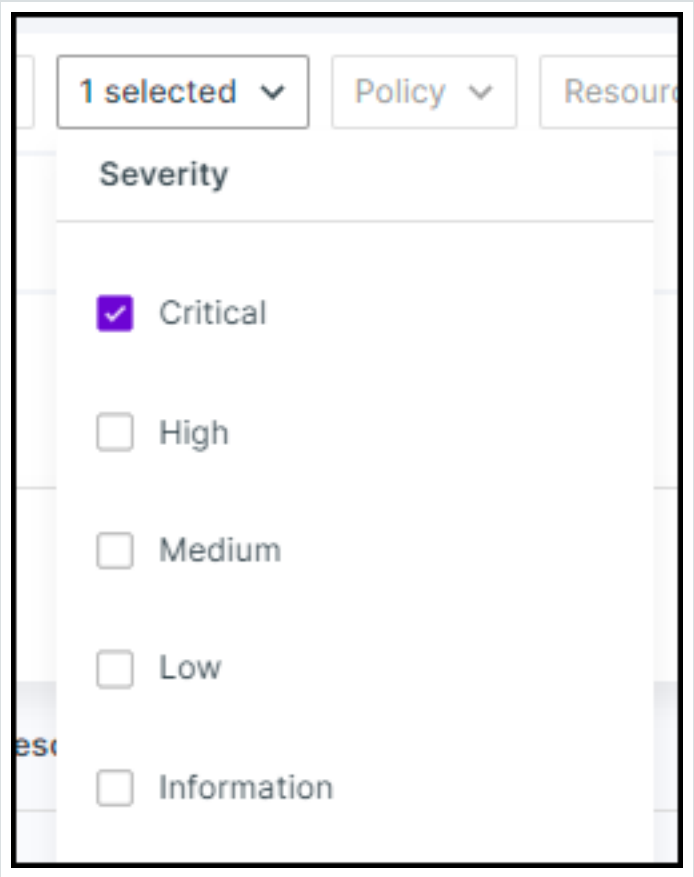
エンドツーエンドの検出結果ワークフローのサンプル

以下のサンプルワークフローは、環境内の検出結果を分析して修正するために実行できるアプローチの一例を示しています。この例を使い、検出結果のライフサイクルを順番に説明します。このケースでは、**AWS 本番** 環境で深刻度が「重大」である **権限昇格 IAM***DemoMaker* の検出結果に焦点を当てます。これらの手順は調整され、他の検出結果タイプ / シナリオに拡張される可能性があります。

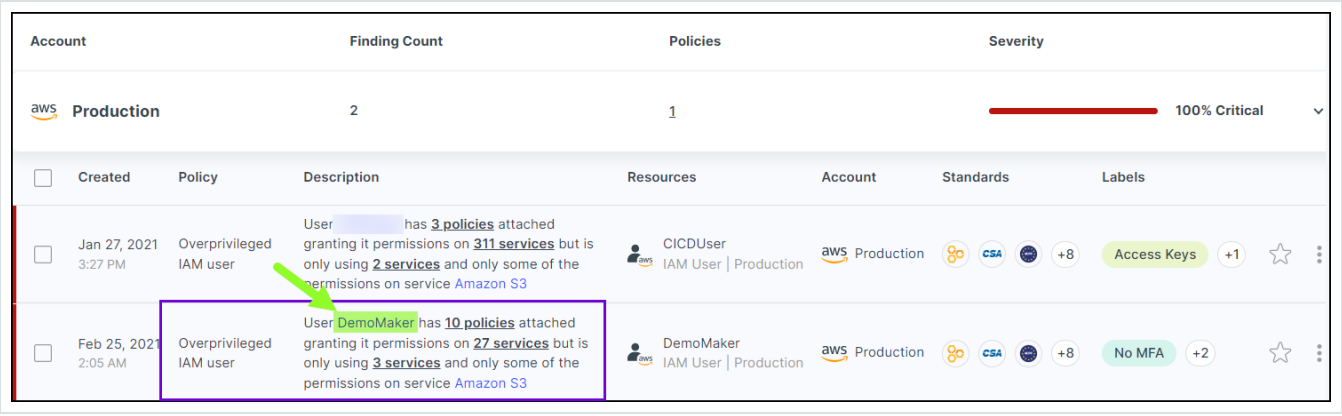
1. Tenable One Cloud Exposure コンソールで、**[リスク]** > **[クラウドの検出結果]** をクリックして、環境内のすべてのクラウド検出結果のリストを表示します。デフォルトのビューでは、検出結果が深刻度レベル順に並べられています。
2. AWS 本番環境でリソースを探しているため、アカウント別に検出結果の内訳を確認できるように検出結果を表示できます。**[グループ化]** ドロップダウンをクリックし、**[アカウント]** をクリックします。
3. このビューから、[AWS 本番] アカウントを簡単に見つけることができます。ただし、このアカウントに関連付けられている検出結果は 200 件を超えており、実際に探している検出結果を特定するのは簡単ではありません。



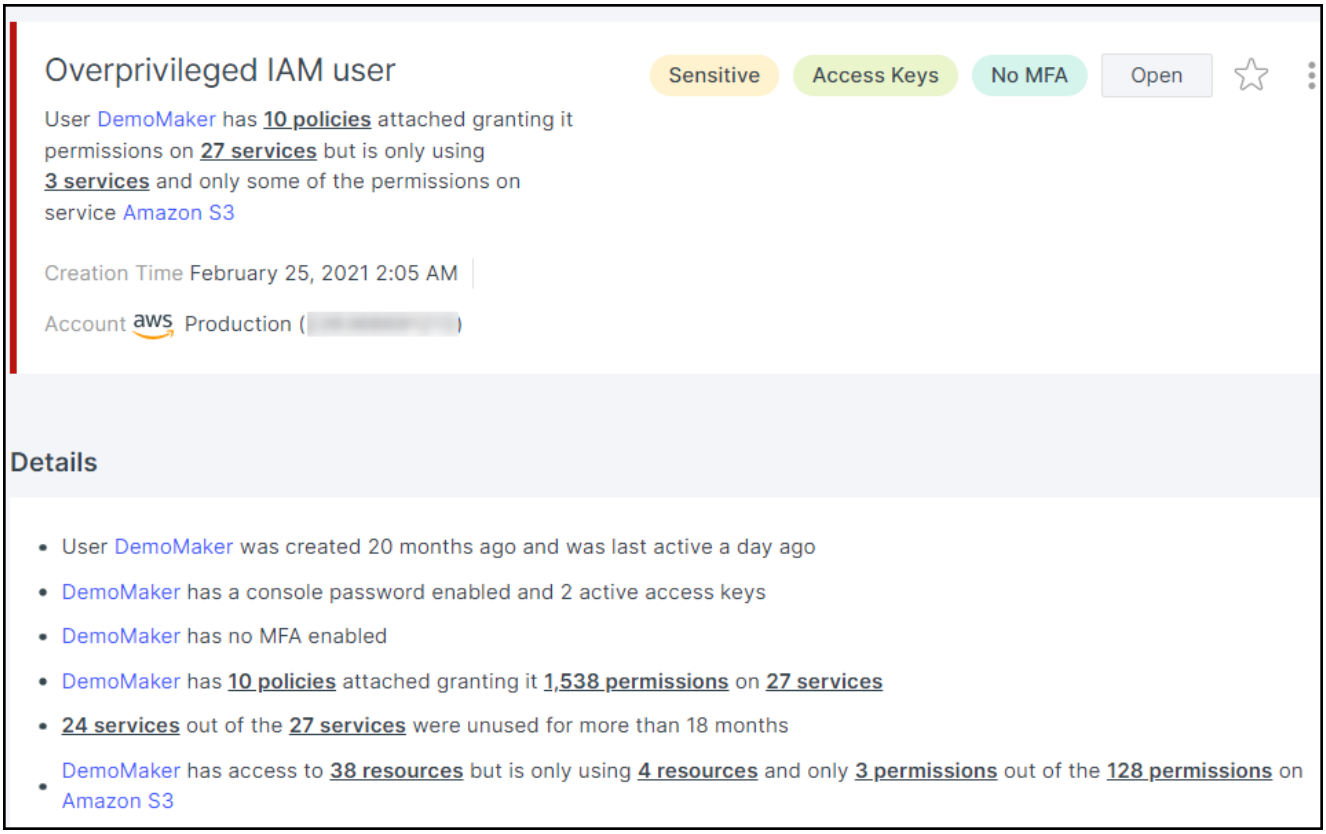
4. 深刻度が「重大」の検出結果を検索するので、テーブルの上部にある **[深刻度]** フィルターを使用して結果を **[重大]** のみに絞り込むことができます。これにより、検出結果の数が大幅に減少します。



5. その後、**ポリシー**フィルターを使用して、探している検出結果のタイプに従って結果をさらに絞り込むことができます (**権限過剰な IAM ユーザー**)。これを行うと、数件の結果のみが確認されます。そのうちの 1 つは、探している *DemoMaker* ユーザーです。

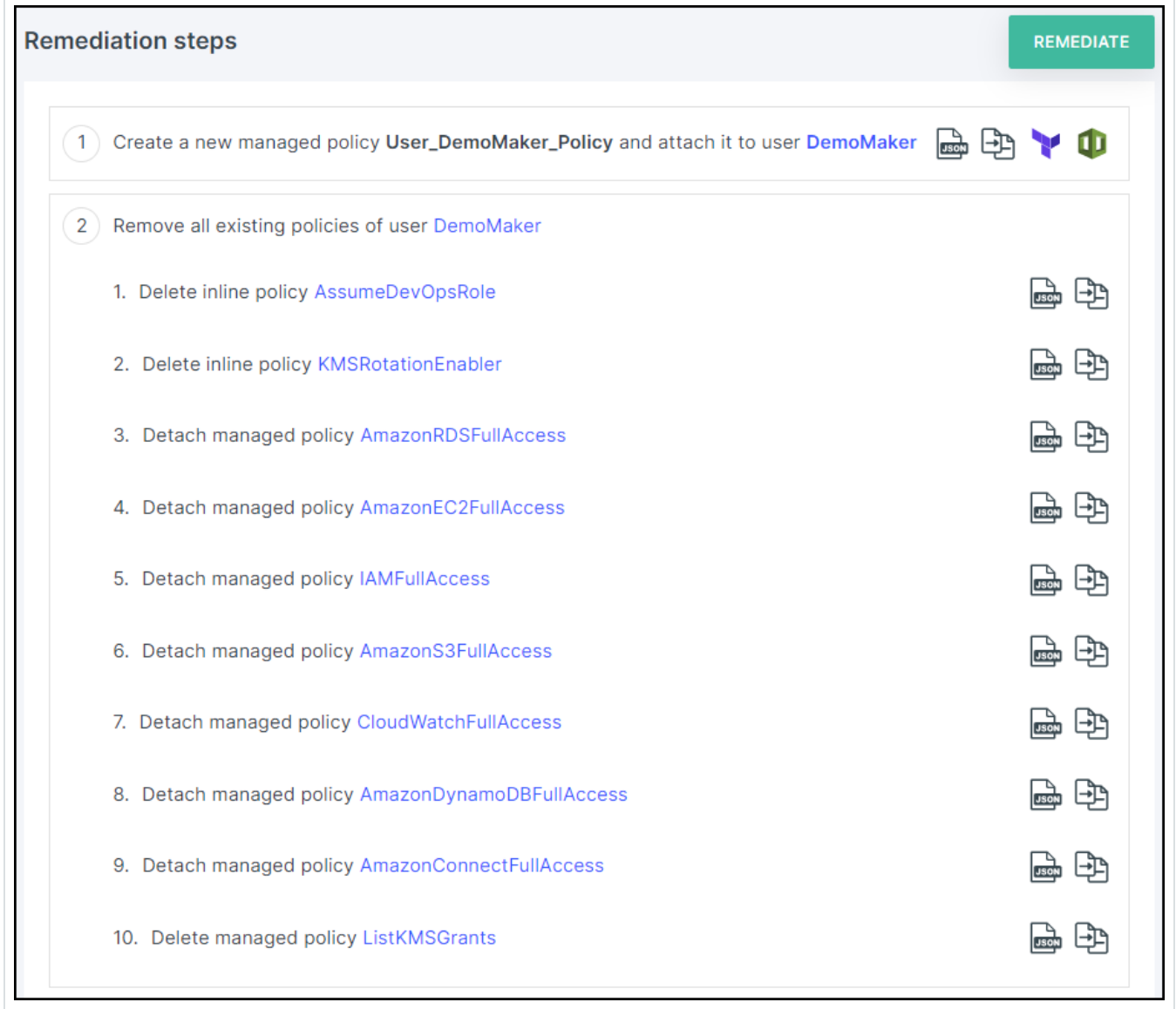


6. 検出結果をクリックすると、専用の検出結果ビューにその詳細情報が表示されます。



- このIAM IDは、ポリシーがアクセス許可を付与する27サービスのうち3つだけを使用していることが判明します。これらのサービス(使用済みと未使用の両方)またはポリシーをクリックすると完全なリストが表示され、過剰となっている特定の権限を詳しく把握することができます。
- **[詳細]**セクションで、IAM IDのMFAが有効化されていないことが(および[No MFA]ラベル経由で)確認でき、検出結果にさらにリスクのレイヤーが追加されます。

7. **[アクセス許可と使用]**セクションで、このIAM IDのアクセス許可マッピングを視覚化し、アイデンティティが環境内のロールを引き受けて他のリソースにアクセスする方法をより詳しく把握できます。たとえば、マップをフィルタリングして、重大の深刻度を持つ過剰なアクセス許可を表示することができます。この機能の詳細については、アクセス許可マッピングの視覚化 参照してください。
8. 次に、**[修正手順]**セクションに移動し、推奨されるアクション項目を確認します。



- クラウドサイバーエクスポージャーでは、単一の管理ポリシーを作成して、現在添付されている 10 個のポリシーを置き換えることを推奨していることがわかりました。
- クラウドサイバーエクスポージャーが過剰なポリシーを削除またはデタッチすることを推奨していることが判明しました。インラインポリシーは簡単に削除できますが、他のアイデンティティに適用されている可能性がある管理ポリシーはデタッチする必要があるでしょう。管理ポリシーが他の場所で使用されていない場合、Tenable はそれを削除するよう提案しますが、関連する手順詳細ページの **[デタッチのみ]** ラジオボタンを選択することで、これをオーバーライドできます。

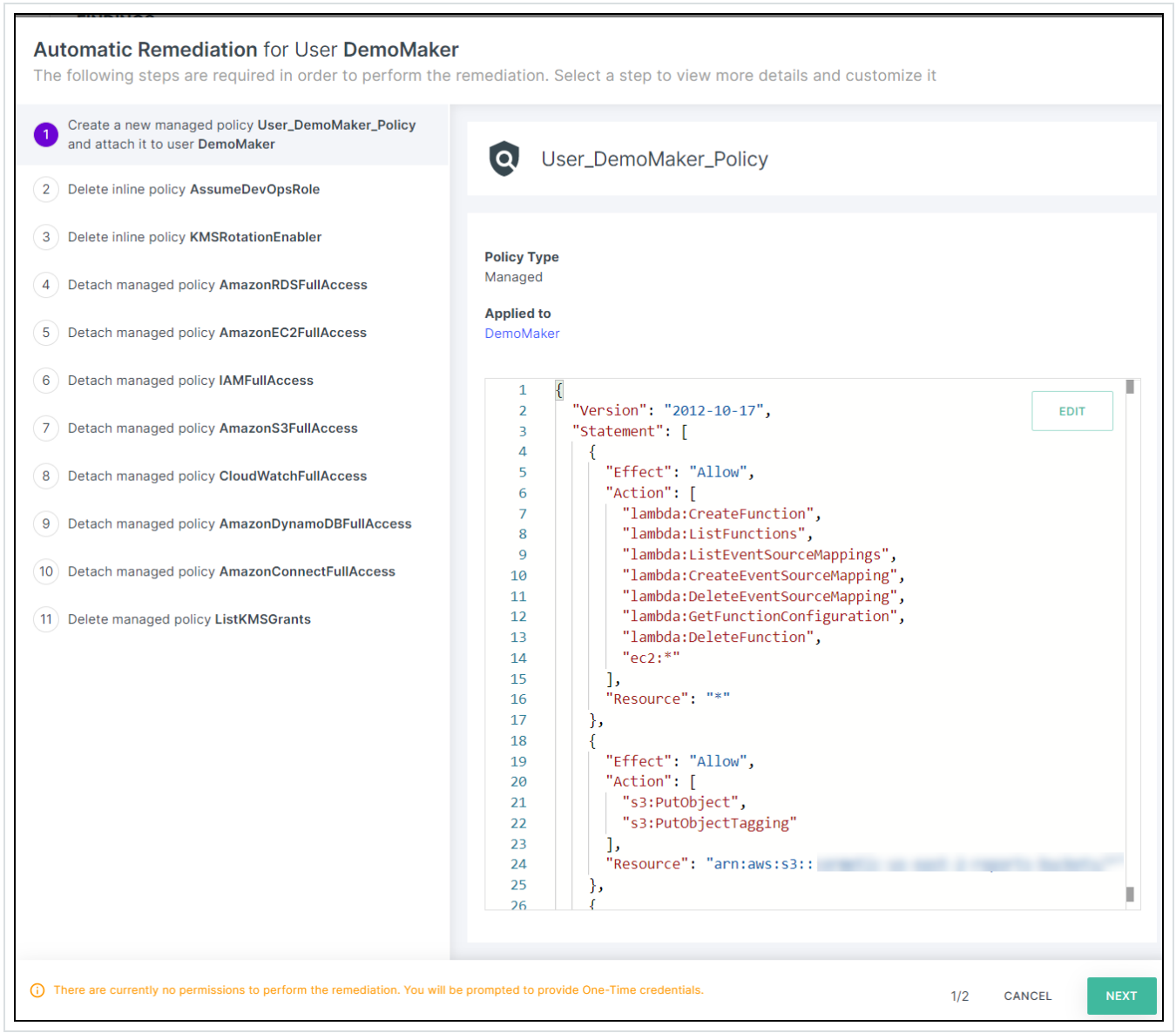
9. 最初の修正手順の横にある [Diff] ボタンをクリックすると、古いポリシーと新しいポリシーの並べ替えが表示されます。[古いポリシー] 領域で、ドロップダウンをクリックして表示する特定のポリシーを選択します。



クラウドサイバーエクスポージャー、標準の手順に従って新しいポリシーを構築し、ユーザーが実際に必要とするすべてのアクセス許可を収集して、それらを 1 つのポリシーにまとめます。

10. 手順を慎重に確認した後、この発見事項を検出結果の自動修正 意味があると判断しました。手動修正もオプションとしてあり、状況によっては手動の方が妥当ですが、この特定の検出結果タイプのプロセスを自動化すると、軽減プロセスが大幅に簡素化され、関連するクラウドプロバイダーコンソールで多様な (そして多くの場合、複雑な) アクションを実行する必要がなくなります。

11. **是正措置** REMEDIATE ボタンをクリックして、自動修正プロセスを開始します。



> **注意:** アカウントのオンボーディング中にTenable読み取り専用アクセス許可のみを付与した場合は、修正を完了するために ワンタイム認証情報による修正 ように求められることを示す注意がページの下部に表示されます。

12. ページ左側にあるさまざまな手順をクリックすると、対象のリソースに関する詳細情報が表示されます。

13. 新しい管理ポリシーを作成する最初のステップでは、ポリシーを確認し、必要に応じて編集できます (**[編集]** をクリックし、関連する変更を行ってから **[保存]** をクリックします)。たとえば、順序を変更したり、特定のアクセス許可を削除したりすることができます。
14. 手順を確認したら、**[次へ]** をクリックします。
15. [アクションの概要] ページで、もう一度アクションを確認し、準備ができたら **[応募する]** をクリックします。

アイデンティティの影響範囲を視覚化

目的

1 つの設定ミスまたはアイデンティティがクラウド資産にどのように影響するかを視覚化します。ラテラルムーブメントの可能性への影響に基づいて、修正に優先順位を付けます。

> **注意:** プレイブックは、プラットフォーム内でセキュリティワークフローを運用するための設計資産として機能します。概説されている手順は、技術的な可視性を一貫性のある実用的な結果に変えるための繰り返し可能な方法を示しています。**このガイドでは特定のユースケースに焦点を当てていますが、これらの原則は他のリソースタイプやセキュリティシナリオに適用されることで、環境全体の包括的なリスク管理を確実にすることができます。**

ステップ 1: エクスポージャーの範囲の定義 (カスタムクエリ)

Explorer を使用して、異なるデータタイプを結合します。たとえば、プリンシパルをクラウドの検出結果とその管理ポリシーに参加させることができます。

1. **[調査]** > **[エクスプローラー]** に移動します。
2. 非アクティブで権限のある IAM プリンシパルを見つけます。
    1. **[リソース]** ドロップダウンをクリックし、**[プリンシパル]** を選択します。
    2. 次のフィルターをプリンシパルリソースに追加します。
        - **非アクティブがTrue** に等しい
        - **ラベル** は **管理者** および **特権** です

3. 重要度が高い/重大なクラウド検出結果を検索に含める
    1. **[参加する]** をクリックし、**[クラウド・ファインディングとは]** を選択します。
    2. **深刻度** が**「重大」**で**「高」**のフィルターを追加
4. 関連する特権ポリシーを検索に結合します。
    1. **[参加する]** をクリックし、**[ポリシーに基づいて生成]** を選択します。
    2. **システムID**のフィルターを追加し、関連する**オーバー権限** ポリシーを追加します。

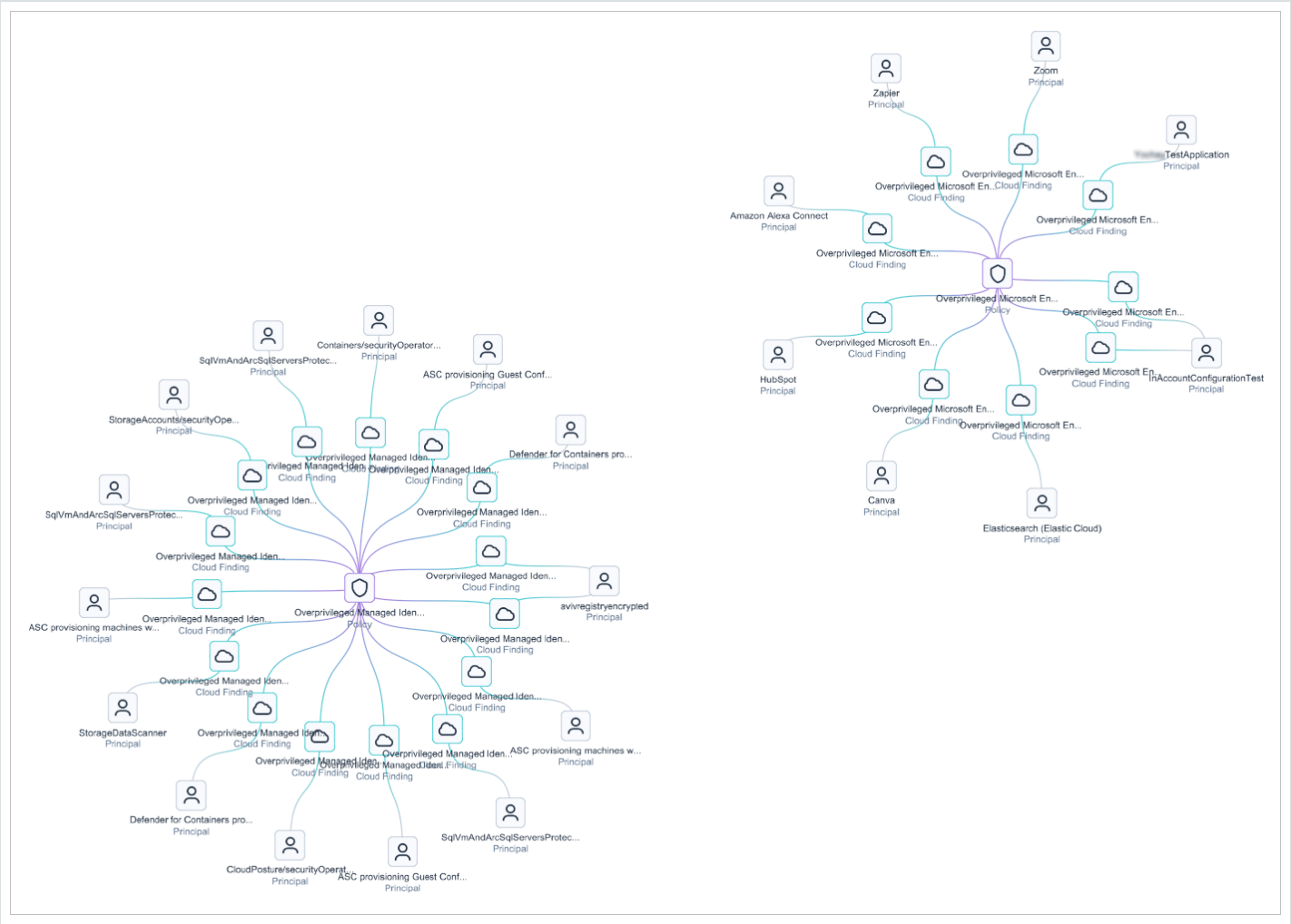
ステップ2: エクスポージャーマップを表示する (Organic Graph)

グラフビューに切り替えて、リスク間の関係を表示します。

1. [エクスプローラー] ページの右上で、**[グラフ]トグル**をクリックします です。
2. グラフの下部で、**[レイアウトを変更**] をクリックしてから、**[組織]** をクリックします。

ステップ 3: 値が高いターゲットを特定する

アイデンティティの集約については、グラフを確認します。ここでは、単一のプリンシパルが複数のリスクポイントに関連しています。プリンシパルアイコンが複数の異なるクラウド検出結果にリンクされている場合、そのアイデンティティは高リスクのエントリポイントです。この視覚化により、特定のアカウントを速やかに修正する必要がある理由が特定されます。



製品のユースケース

次の Tenable One Cloud Exposure のコア機能を使用すると、クラウドセキュリティの広範なユースケースで課題を解決できます。

マルチクラウドの可視化

- 資産 **インベントリ**を通じたクラウド資産の管理
- クラウドイベント ログを介してクラウドアクティビティを監視および監査する

最小権限の適用

- アイデンティティインテリジェンスとアクセス許可マッピングの視覚化「アクセスグラフ」により、有効な権限を視覚化
- 重要な問題をすばやく表面化するための、アイデンティティ間のアクセス許可クエリ
- [過剰なアクセス許可 許可] ページおよびクラウドの検出結果経由で過剰なアクセス許可を取り消す
- 最小権限ポリシーの生成とロール

リスクの評価と優先順位付け

- クラウドポリシーおよびクラウドポリシー: カスタムポリシーでクラウドポスチャーを保護します
- クラウドの検出結果によってリスクを評価し、優先順位を付ける

リスクの高い権限と不具合のある設定の軽減

- 検出結果を通じて検出結果の修正
- 検出結果の自動修正

クラウドコンプライアンスのモニタリング

- アカウントのコンプライアンスを監視する
- コンプライアンスを追跡するレポートを作成する

クラウド検出と対応

- クラウドイベント経由でクラウドアクティビティを監視および監査する
- クラウドの検出結果経由で異常を検出して対応する

セルフサービスのジャストインタイムアクセス

- JIT アクセスを管理する
- アクセスをリクエストする
- アクセスの確認

JIT アクセス

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

必要に応じて、あらかじめ決められた期間、ユーザーにクラウドアカウントへのアクセスを許可します。セルフサービスのジャストインタイム (JIT) アクセスを実装することで、安全な特権アクセスをプロビジョニングでき、以下が可能になります。

- ユーザーがタスクを完了するために必要な最短時間でのアクセスを許可することで、潜在的な攻撃者に過剰な権限を悪用されるリスクを最小限に抑えます。
- アクセスのリクエストプロセスとレビューまたは承認プロセスの両方が簡素化され、時間を節約できます。
- 一般的なリクエストの承認プロセスを自動化して、作業負担を軽減します。
- 付与されたすべての資格とアクセスリクエストに対する完全な監査証跡を通じて、ユーザーのアクセス動作を把握します。

ユーザーは、それぞれのクラウドコンソールから、またはプログラムを使用して、AWS、Azure、GCP のクラウド環境にアクセスできます。

Tenable JIT ユーザーインターフェース

JIT アクセスは、次の場所にある Tenable One Cloud Exposure で管理されます。

- 独立したセルフサービスの クラウド サイバーエクスポージャー **JIT ポータル** 。組織の関連するステークホルダーは、次のことが実行できます。

- 有効なアクセスリクエストのパラメーターを定義する資格を管理します。
- アクセスをリクエストします。
- アクセスリクエストを確認し、承認または拒否します。
- アクセスリクエスト、資格の変更、JIT アクセス許可を持つユーザーがクラウドで実行したアクティビティなど、JIT 関連のアクティビティに関する監査証跡情報を表示します。

> **注意:** クラウド サイバーエクスポージャー コンソールと JIT ポータルの両方にアクセスできる場合は、「切り替える...」ユーザープロファイル

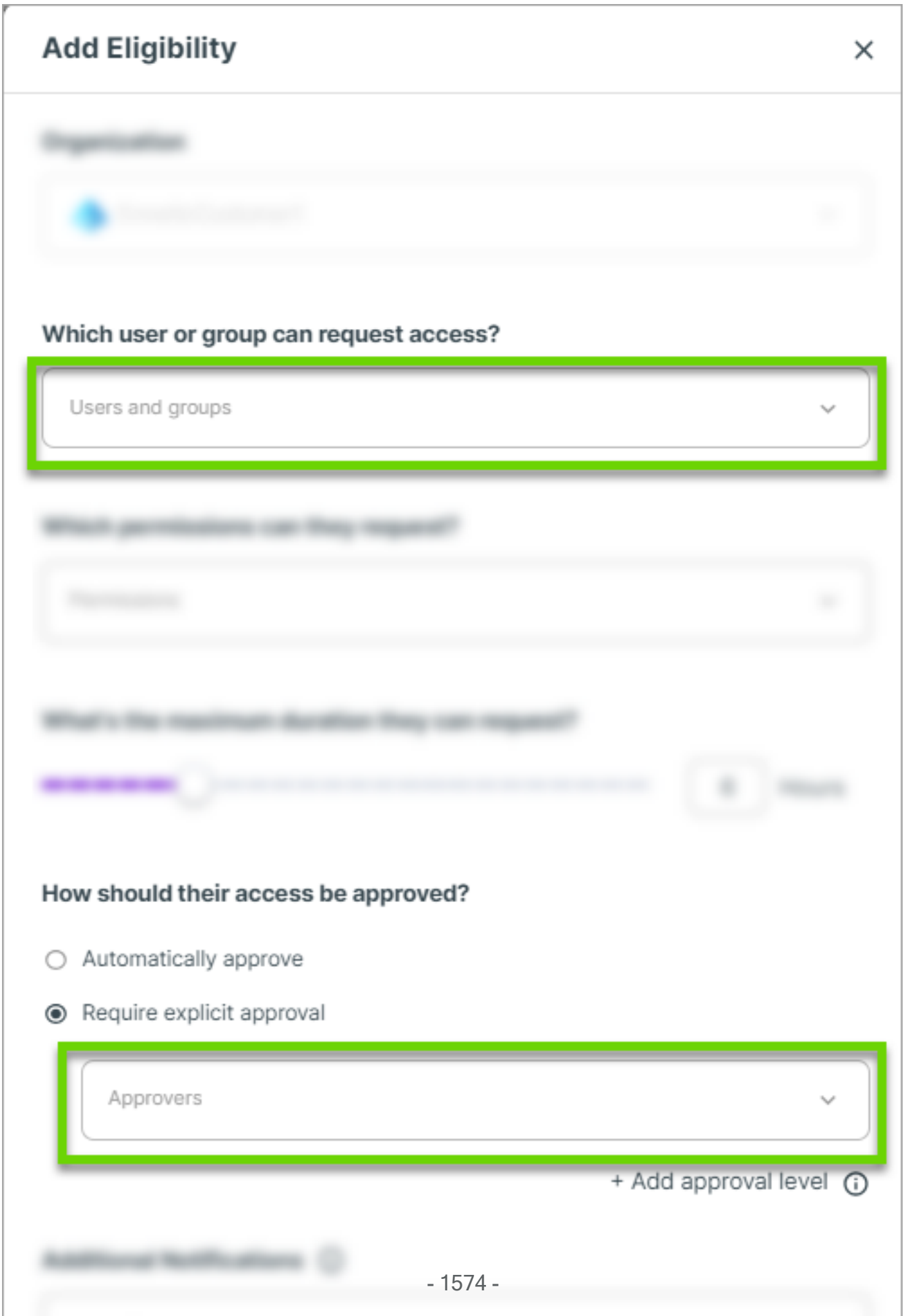
- Slack メッセージとチャンネル。組織の関連するステークホルダーは次のことを実行できます。
  - アクセスをリクエストします。
  - アクセスリクエストを確認し、承認または拒否します。

  JIT と連動するように Slack を設定するには、「Slack と JIT の統合を参照してください。
- Teams メッセージ/チャネル。関連する組織の利害関係者が次のことを行うことができます。
  - アクセスをリクエストします。
  - アクセスリクエストを確認し、承認または拒否します。

  JIT と連携するように Teams を構成するには、「Teams と JIT の統合を参照してください。

JIT ポータルにアクセスできるユーザー

- クラウド サイバーエクスポージャー コンソールで構成された**管理者**または **JIT 管理者**のユーザー。
- 資格においてリクエスト者と定義されたユーザー。
- 資格において承認者と定義されたユーザー。


Add Eligibility
Which user or group can request access?
Users and groups
How should their access be approved?
Automatically approve
Require explicit approval
Approvers
+ Add approval level

JIT を使い始める

JIT を開始するには、次のことを行う必要があります。

- クラウドアカウントがに接続されクラウドサイバーエクスポージャーていることを確認します。
- 付与Tenable関連するクラウドプロバイダーが機能の使用を開始するための JIT アクセス許可。

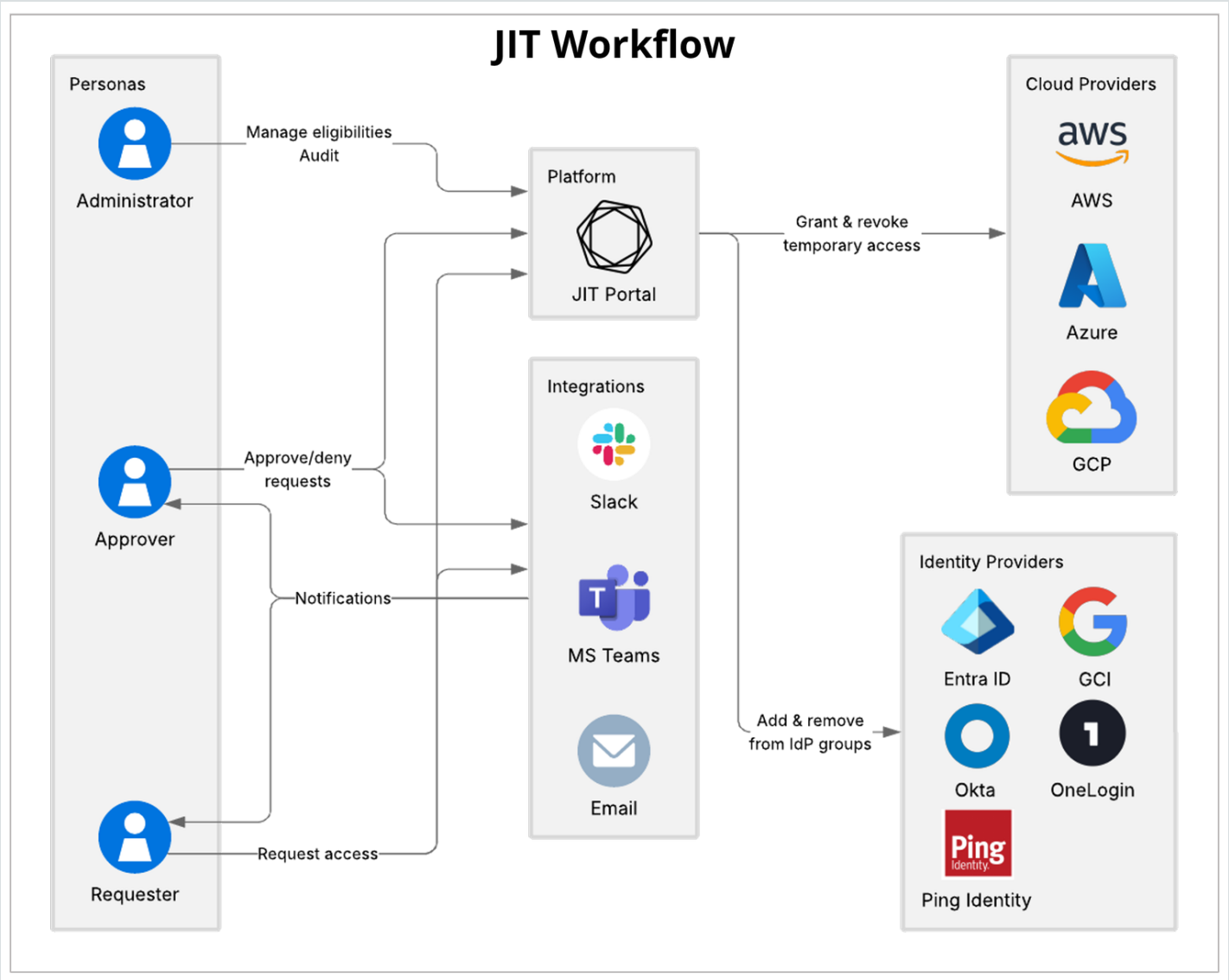
JIT ペルソナとワークフロー

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

JIT アクセスワークフローには、次のペルソナの参加が含まれます。

- **管理者。** JIT ポータル経由で資格の追加し、JIT 関連のアクティビティを監査できるTenable One Cloud Exposureユーザー (**管理者**または **JIT 管理者**ロール)。
- **リクエスト者**。クラウド環境でアカウントにアクセスしたいユーザーまたはグループメンバーで、JIT ポータル経由でのアクセスのリクエスト、Slack 経由でアクセスをリクエストするTeams 経由でアクセスをリクエストする由でリクエストを送信します。
- **承認者**。JITポータルからアクセスを確認する、Slack 経由でアクセスを確認するTeams 経由のアクセスの確認 を介してリクエストを手動でレビューまたは承認する資格があると指定されたクラウド環境のユーザーまたはグループメンバー。

JIT ワークフロー



1. 管理者が資格を追加します。資格は、アクセスをリクエストできるユーザーとリクエストできる内容(アカウントの範囲、アクセス許可、期間)を指定する事前定義されたポリシーです。このポリシーでは、アクセスを自動的に承認して付与するか、または明示的な承認を待つ必要があるかについても定義します。
2. 資格に含まれているリクエスト者が、アカウントへのアクセスをリクエストできます。ユーザーがアクセス権をリクエストできるかどうかは、管理者によって定義された資格基準に基づきます。
3. 資格基準に自動承認が規定されている場合、アクセスリクエストは即座に承認され、付与されます。

4. 資格基準が明示的な承認を必要とする場合、リクエストは保留となり、メール通知やSlack、Teamsメッセージ(有効な場合)が承認者に送信されます。オプションで、追加のメールアドレスまたはSlackチャンネルやTeamsチャネルを定義して通知を受信することもできます。
5. 承認者がリクエストをレビューし、承認するか拒否するかを決定します。
6. 承認者がリクエストを承認した場合
    - リクエスト者には、定義されたアクセス許可レベルを使用して、特定の期間、アカウントにアクセスできます。承認ワークフローの同じレベルに複数の承認者がいる場合、承認を付与する必要があるのはそのうちの1人のみです。
    - 複数レベルの承認ワークフローを構成した場合、レビューのために第2レベルまたは第3レベルの承認者に通知が送信されます。資格で定義された最終承認者がリクエストを承認した後にのみ、リクエスト者にアクセスが許可されます。
7. 権限の期間が終了すると、リクエスト者のアクセス権は自動的に取り消されます。

Tenable JIT アクセス許可を付与する

> **注意:** この機能は、Cloud Vulnerability Managementライセンスでは使用できません。

必要なアクセス許可 Tenable 付与することで、以下のクラウドサービスプロバイダー / アイデンティティプロバイダー(IdP)をJITに接続できます。

- AWS (アイデンティティセンター)
- Azure
- GCP
- Microsoft Entra ID
- Google Workspace
- Okta
- OneLogin
- Ping Identity

注意: Slack を JIT ワークフローの一部として使用して、ユーザーが Slack 経由でアクセスをリクエストまたは承認できるようにするには、JIT 用に Slack を設定する必要があります。

JIT 用に AWS Identity Center に接続する

Tenable One Cloud Exposure AWS の JIT アクセスは、IAM Identity Center (AWS シングルサインオンの後継) に基づいています。次のガイドラインに従って、JIT 用の AWS Identity Center を接続します。

- IdP を IAM Identity Center に接続します。
- IAM Identity Center のユーザーとグループのみが JIT ワークフローに参加できます。ユーザーは SSO を経由してクラウドサイバーエクスポージャーにログインするよう構成されたユーザーと一致する必要があります。
- Tenable が IAM Identity Center 内で関連するすべての IdP データを確実に収集するには、AWS 管理アカウントが Tenable に接続されていることを確認してください。
- Tenable は、JIT での AWS 委任管理者アカウントの使用をサポートしています。委任されたアカウントを使用する場合は、そのアカウントも統合する必要があります。委任されたアカウントの詳細については、AWS のドキュメント を参照してください。
- に JIT 関連のアクセス許可を付与する Tenable

  注意: 委任された管理者アカウントを使用している場合は、必ず管理アカウントではなく委任されたアカウントにアクセス許可を付与してください。

- 外部アイデンティティプロバイダー (IdP) と Tenableの間に信頼を確立します。
  - SSO 経由でのコンソールへのログインの有効化
  - SSO 経由の JIT ポータルログインを有効化

注意: IAM Identity Center を使用して外部 IdP から AWS 環境へのアイデンティティを認証する場合は、外部 IdP をクラウドサイバーエクスポージャーと個別に統合する必要はありません。AWS は、ユーザーとグループを自動的に IdP から IAM Identity Center にプロビジョニングします。このデータは、AWS管理アカウントを接続する際に Tenable 取り込まれます。

警告: Tenable は、複数のアクセス許可セットを使用して JIT ユーザーのアクセスを定義します。これらは、組織ですでに使用されている既存の許可セットに追加されるものです。IAM Identity Center のアクセス許

可セットに関連するAWSアカウントのクォータに注意してください。また、これらのクォータの一部は増加可能であることに注意してください。

にJIT関連のアクセス許可を付与するTenable

注意: 委任された管理者アカウントを使用している場合は、管理アカウントではなく委任されたアカウントにアクセス許可を付与してください。**両方の**アカウントにアクセス許可を付与すると、委任されたアカウントからアクセス許可がTenable受け継ぎます。JIT内で委任されたアカウントを操作することの影響については、資格の追加を参照してください。

TenableにJITアクセスのアクセス許可を付与するには

1. AWS管理アカウントが接続されていることを確認します。AWSの委任された管理者アカウントを使用している場合は、そのアカウントも接続する必要があります。
2. AWS管理コンソールで、**[IAM > Roles] (IAMロール)**に移動し、関連するアカウントを接続したときに作成したロールを開きます。
    - 委任された管理者アカウントを使用している場合は、委任されたアカウントを接続したときに作成したロールを開きます。
    - または、管理アカウントを接続した際に作成したロールを開きます。
3. [アクセス許可]タブで、**[アクセス許可の追加] > [インラインポリシーの作成]**の順にクリックします。
4. [JSON]タブで、以下のセクションにある関連するJITポリシーを貼り付けて、既存のテキストを置き換えます。
    - **AWSアカウントアクセスの場合**: 設定(管理アカウントまたは委任された管理者アカウント)に一致する[AWSアカウントアクセス用のJITポリシー]のポリシーを使用します。
    - **アプリケーションアクセスの場合**: 設定(管理アカウントまたは委任された管理者アカウント)に一致するアプリケーションアクセスのJITポリシーのポリシーを使用します。
5. **[ポリシーのレビュー]**をクリックします。
6. ポリシーの名前(例: TenableJIT)を入力し、**[ポリシーの作成]**をクリックします。

AWSアカウントアクセスのJITポリシー

これらのポリシーを使用すると、AWS Identity Center を介した AWS アカウントとアクセス許可セットへの JIT アクセスを Tenable One Cloud Exposure で管理できるようになります。

AWS Identity Center がアカウントアクセス用の管理アカウントから直接管理されているか、アカウントアクセス用の委任された管理者アカウントを介して管理されているかに応じて、環境ごとに 1 つのポリシーのみを使用します。

アカウントアクセス用の管理アカウント

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider",
                "iam:UpdateSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO__DO_NOT_DELETE"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "identitystore:Describe*",
                "identitystore:List*",
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeletePermissionSet",
                "sso:Describe*",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:Get*",
                "sso:List*",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso-directory:List*",
                "sso-directory:Search*"
            ],
            "Resource": "*"
        }
    ]
}
```

アカウントアクセス用の委任された管理者アカウント

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet"
            ],
            "Resource": "*"
        }
    ]
}
```

アプリケーションアクセスの JIT ポリシー

これらのポリシーを使用すると、AWS Identity Center によって管理されるアプリケーションへの JIT アクセスを Tenable One Cloud Exposure で管理できるようになります。

AWS Identity Center がアプリケーションアクセス用の管理アカウントから直接管理されているか、アプリケーションアクセス用の委任された管理者アカウントを介して管理されているかに応じて、環境ごとに 1 つのポリシーのみを使用します。

アプリケーションアクセス用の管理アカウント

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "identitystore:Describe*",
        "identitystore:List*",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso-directory:List*",
        "sso-directory:Search*"
      ],
      "Resource": "*"
    }
  ]
}
```

アプリケーションアクセス用の委任された管理者アカウント

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
      ],
      "Resource": "*"
    }
  ]
}
```

JIT 用に Azure を接続する

Azure でロールの割り当てを追加して、クラウド サイバーエクスポージャー アプリにルート管理グループへのアクセス権を付与します。

> **注意:**
>
> - Azure の概要 中に、すでにルート管理グループにTenable管理アクセス許可を付与してある場合は、この手順をスキップできます。
> - JIT を使用するには、Microsoft Entra ID テナントの接続も必要です。

Tenable に JIT アクセスのアクセス許可を付与するには

1. Azure ポータルで、組織のルート管理グループを開きます。デフォルトでは、ルート管理グループの表示名は **[テナント ルート グループ]** です。
2. **[アクセス制御 (IAM)]** に移動します
3. **[追加] > [ロールの割り当てを追加]** をクリックします。
4. [特権管理者ロール] で、**[ユーザー アクセス管理者]** を検索して選択し、**[次へ]** をクリックします。
5. **[+メンバーを選択]** をクリックし、**クラウド サイバーエクスポージャー コネクタ**を検索して選択します。
6. **[選択]** をクリックし、**[確認 + 割り当て]** をクリックして新しいロールの割り当てを確認します。
7. もう一度 **[確認 + 割り当て]** をクリックして、ロールの割り当てを追加します。

JIT 用に GCP を接続する

クラウド サイバーエクスポージャーサービスアカウントに、組織レベルでのセキュリティ管理者のアクセス権を付与します。

> **注意:**
>
> - GCP の概要時に、すでに組織レベルでのTenable管理アクセス許可を付与してある場合は、この手順をスキップできます。
> - JIT を使用するには、Google Workspace の接続 の接続も必要です。

Tenable に JIT アクセスのアクセス許可を付与するには

1. Google Cloud コンソールで、追加する組織ノードに移動します。
2. **[IAM と管理] > [IAM]** の順に移動します。
3. **[+アクセス権を付与]** をクリックします。
4. [新しいプリンシパル] フィールドに、対象の Google Workspace サービスアカウントのメールを入力します。この値は、次の場合に確認できます。
   - Google Cloud コンソールの **[IAM と管理] > [サービスアカウント]** の [メール] フィールド。
   - クラウド サイバーエクスポージャー コンソールの **[設定] > [アイデンティティプロバイダー] > [GOOGLE WORKSPACE]** の [サービスアカウントのメール] フィールド。
5. [ロール] フィールドで、**セキュリティ管理者** ロールを検索して選択します。

   このロールの詳細については、Google Cloud のドキュメントを参照してください。
6. **[保存]** をクリックします。

JIT 用に Microsoft Entra ID を接続する

Azure で **クラウド サイバーエクスポージャー JIT コネクタ** アプリを承認する管理者の同意を許可します。

前提条件

- Microsoft Entra テナントの追加

JIT アクセス権を付与するには

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > JIT]** に移動します。組織の範囲内にいることを確認します。
2. [Microsoft Entra ID group memberships] (Microsoft Entra ID グループメンバーシップ) で関連するテナントを見つけ、**[Grant Permissions] (アクセス許可の付与)** をクリックします。
3. Azure で **クラウドサイバーエクスポージャー JIT コネクタ** アプリを承認する管理者の同意を許可し、必要なアクセス許可を Tenable に付与します。同意が承認されると Tenable にリダイレクトされ、設定が完了します。

    1. **アカウントを選択します**。Microsoft アカウントのサインインページで、Tenable と統合させるテナントが属する管理アカウントを選択します。担当するユーザーは、組織を代表して同意することを認められている必要があります。これを実行するために必要な特定のロールの詳細については、ドキュメント Microsoftを参照してください。
    2. [リクエストされたアクセス許可] ページで **[同意]** をクリックし、Azure のクラウドサイバーエクスポージャー JIT コネクタアプリを承認します。

    必要な Microsoft Entra テナント情報が表示され、アクセス許可が正常に付与された状態で Tenable に戻ります。

Tenable JIT アプリに必要なアクセス許可

クラウドサイバーエクスポージャー JIT Connector アプリを承認すると、Tenable には次のアクセス許可が付与されます。

- **サインインしてユーザープロファイルを読みます**。ユーザーのアプリへのサインインを許可します。アプリはサインインしたユーザーのプロファイルを読み取ることができます。また、アプリはサインインしているユーザーの基本的な会社情報も読み取ることができます。
- **すべてのグループメンバーシップの読み取りと書き込み**。サインインしているユーザーがいなくても、アプリがグループを一覧表示し、基本的なプロパティを読み取り、アプリがアクセスできるグループのメンバーシップを読み取ったり更新したりできます。グループのプロパティと所有者を更新することはできません。グループを削除することもできません。

注意: Azure のアプリを承認すると、テナントのサービスプリンシパルが作成されます。これはアプリの統治メカニズムとして機能し、ディレクトリ内でアプリのインスタンスと見なされることがあります。Microsoft Entra の

アプリケーションおよびサービスプリンシパルオブジェクトの詳細については、ドキュメントMicrosoftを参照してください。

JIT用にGoogle Workspaceを接続する

JIT用にGoogle Workspaceを接続できます。

- クラウドサイバーエクスポージャーへの初期Googleワークスペース統合中に、Googleワークスペースを追加するとき。
- 最初の統合後に、次の手順に従います。

前提条件

- Google Workspaceの接続

JITアクセス権を付与するには

次のいずれかの方法を選択して、Tenableにアクセス許可を付与します。

注意:

- **カスタムロール**: ジャストインタイムアクセスを含むクラウドサイバーエクスポージャー内のすべてのコア機能をサポートします。このオプションは、ほとんどの組織に推奨されます。
- **ドメイン全体の委任**: 高度なIAM機能を必要とする組織に適しています。また、ジャストインタイムアクセスをサポートしています。詳細については、「ドメイン全体の委任 (アドバンス)を参照してください。

これらのアクセス許可が必要な理由についての詳細は、必要なアクセス許可を参照してください。

カスタムロール

1. Google管理コンソールで**アカウント** > **管理者ロール**に移動し、Googleワークスペースに接続したときにTenable用に作成したロールを見つけます。

2. *権限 > 管理 API 権限*で、次の権限を選択します。
    - グループ > **更新**

        このアクセス許可により、ジャストインタイムアクセスを活用して、Google Workspace グループにユーザーを一時的に
        できます。

3. **[保存]** をクリックします。

ドメイン全体の委任

1. Google Cloud コンソールで、Google Workspace を接続したときに作成したサービスアカウントに移動し、*[詳細]* タブで、[**詳細設定** セクションをクリックして展開します。
2. [**Workspace 管理コンソールGoogle表示** をクリックします。
3. 管理コンソールで、**[セキュリティ]** > **[アクセスとデータ管理]** > **[API の制御]** に移動します。
4. **[ドメイン全体の委任の管理]** をクリックし、**[新しく追加]** をクリックします。
5. Google ワークスペースを接続したときに使用した **クライアント ID** を見つけます。
6. 次の **OAuth スコープをコピーして貼り付けます**:
   `https://www.googleapis.com/auth/admin.directory.group.member`

    このアクセス許可により、ジャストインタイムアクセスを活用して、Google ワークスペースグループにユーザーを一時的に追加できます。

7. **[承認] をクリックします。**

JIT 用に Okta を接続

JIT 用に Okta を接続できます。

- Okta を クラウド サイバーエクスポージャー に初めて統合する際に、Okta 組織の接続 とき。
- 最初の Okta 統合後に、次の手順に従います。

前提条件

- Okta 組織の接続

JIT アクセス権を付与するには

1. スーパー管理者として Okta 管理コンソールにログインします。
2. **[セキュリティ>管理者]** に移動し、**[管理者]** タブをクリックします。
3. Okta 組織を クラウド サイバーエクスポージャー に追加したときに使用した管理者を検索します (読み取り専用管理者ロールを持つ管理者)。
4. **[編集] > [割り当ての編集]** をクリックします。
5. **[+ 割り当ての追加]** をクリックし、**[グループ メンバーシップ管理者]** を検索して選択します。

   > **注意:** 管理ロールを持つグループがある場合、そのようなグループを管理できるのはスーパー管理者のみであるため、代わりに **スーパー管理者** ロールを割り当てる必要があります。

6. 終了したら、**[Save Changes]** をクリックします。

JIT 用に OneLogin を接続する

JIT 用に OneLogin を接続できます。

- OneLogin を クラウド サイバーエクスポージャー に初めて統合する際に、OneLogin アカウントの接続とき。
- 最初の OneLogin 統合後に、次の手順に従います。

前提条件

- OneLogin アカウントの接続

JIT アクセス権を付与するには

1. OneLogin **管理** ページに移動します。
2. トップメニューで、**[開発者> API 認証情報]** をクリックします。

3. **[新しい認証情報]** をクリックし、**[名前]** を入力して **[ユーザーの管理]** を選択して、ディレクトリデータへのクラウドサイバーエクスポージャー読み取り/書き込みアクセスを許可します。**[保存]** をクリックします。
4. **クライアント ID** と**クライアントシークレット**をコピーします。このコピーは後の手順で入力します。
5. クラウドサイバーエクスポージャーコンソールで、**[Settings > Integrations] > OneLogin**に移動します。
6. 対象の OneLogin アカウントを見つけて三点リーダーアイコンをクリックし、**[編集]** をクリックします。
7. [Edit OneLogin Account] (OneLogin アカウントの編集) ウィザードで、**[Next]** をクリックしてステップ 3 [Grant JIT Access (Optional)*] に移動します。
8. ステップ 3b で、先ほどコピーした **クライアント ID** と **クライアントシークレット** を入力し、**[完了]** をクリックします。

JIT 用に Ping Identity を接続する

JIT 用に Ping Identity を接続できます。

- Ping Identity を クラウドサイバーエクスポージャー に初めて統合する際に、Ping Identity 環境の接続とき。
- 最初の Ping Identity 統合後に、次の手順に従います。

前提条件

- Ping Identity 環境の接続

JIT アクセス権を付与するには

1. Ping Identity コンソールにログインし、**[アプリケーション] > [アプリケーション]** の順に移動します。
2. Ping Identity 環境を クラウドサイバーエクスポージャー に追加した際に作成したアプリケーションをクリックします。
3. 表示されたアプリケーションページで、**[ロール]** タブに移動し、**[ロールの付与]** をクリックします。
4. **[アイデンティティデータ管理者]** ロールを展開し、ロールを付与する関連環境を選択します。

5. **[保存]** をクリックしてロールの割り当てを更新し、上部のトグルボタンが選択されていることを確認して、アプリケーションを有効にします。

SSO 経由の JIT ポータルログインを有効化

外部アイデンティティプロバイダー (IdP) と Tenable One Cloud Exposure の間に信頼を確立することで、ユーザーが SSO 経由で JIT ポータルにログインできるようにします。これにより、ユーザーの既存の企業アイデンティティを利用してユーザーのプロビジョニングを実行できます。

AWS Identity Center 経由でのログインの有効化 (SAML 2.0)

AWS Identity Center をアイデンティティプロバイダー (IdP) として使用して、SAML 2.0 経由での JIT ポータルへのログインを有効にします。

始める前に

- **前提条件: 認証ドメイン** AWS Identity Center ユーザーが使用する email ドメインを、クラウドサイバーエクスポージャー で認証ドメインとして追加する必要があります。ドメインが設定されていない場合、SSO のセットアップ中に SAML メタデータのアップロードが失敗します。

AWS Identity Center (SAML 2.0) を使用した JIT ポータルへのログインを有効にする方法

1. AWS で、**AWS Identity Center** を開きます。
2. **[アプリケーション]** に移動し、**[アプリケーションの追加]** をクリックします。
3. **[セットアップするアプリケーションがあります]**、**[SAML 2.0]** を選択して、**[次へ]** をクリックします。
4. [アプリケーションの設定] で、**[表示名]** と **[説明]** を入力します (例: クラウドサイバーエクスポージャー) の SSO 経由での JIT ポータルアクセスの有効化)。
5. [アプリケーションのプロパティ] で、**アプリケーションの開始 URL** のリージョン固有の値を入力します。
    - **グローバル (すべてのリージョン)**: `app.tenable.com/user`
    - **米国ガバメントクラウド**: `app.tenable.us/user`

6. [Application metadata] で以下を行います。
    1. **アプリケーション ACS URL** の値を入力します。

        https://{URL}/api/console/authentication/saml2/user/acs

        {URL} の場合

        - **グローバル (すべてのリージョン)**: app.tenable.com
        - **米国ガバメントクラウド**: app.tenable.us

    2. **[Application SAML audience] (アプリケーション SAML オーディエンス)** に、次のように入力します。

        urn:user.app.ermetic.com

        > **注意:** アプリケーション SAML オーディエンス (エンティティ ID とも呼ばれます) は、JIT ポータルをサービスプロバイダーとして一意に識別します。この値はリージョン固有ではありません。

7. 「**送信**」をクリックしてアプリケーションを作成します。
8. **[ユーザーとグループの割り当て]** をクリックして、JIT ポータルにアクセスする必要があるユーザーまたはグループを割り当てます。
    1. 検索バーから、関連するユーザーまたはグループを追加します。
    2. **[割り当て]** をクリックします。

9. アプリケーションが作成されたら、それを開き、**[アクション] > [属性マッピングの編集]** を選択します。
    1. 次の属性マッピングを確認または追加します*

アプリケーションのユーザー属性	この文字列の値またはユーザーにマップされます IAM Identity Center の属性	フォーマット
サブジェクト (NameID)	`${user:email}`	電子メールアドレス
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	`${user:email}`	指定なし
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	`${user:givenName}`	指定なし
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	`${user:familyName}`	指定なし
グループ (オプション)	`${user:groups}`	指定なし

    *__グループ__属性では大文字と小文字が区別されます。AWS グループを使用する場合は、表示されているとおりに入力してください。

    2. **[変更を保存]** をクリックします。
10. アプリケーションページで、**[アクション] > [設定の編集]** を選択し、**IAM Identity Center SAML メタデータファイル**をダウンロードします。

11. クラウドサイバーエクスポージャーコンソールで、**[Settings > Single Sign-On]** に移動します。
12. **[アイデンティティプロバイダーの追加]** をクリックし、**[SAML]** を選択します。
13. **[アプリケーションの選択]** ドロップダウンで、**[JIT]** を選択します。
14. **[ファイル]** を選択し、AWS Identity Center からダウンロードしたメタデータファイルをアップロードして、**[追加]** をクリックします。

Google 経由でのログインを有効化

次のいずれかのアイデンティティ仕様を使用して、Google 経由で JIT ポータルへのログインを有効にします。

- OpenID Connect (OIDC)
- SAML

OIDC を使用した Google 経由でのログインの有効化

OIDC を使用したログインを有効にするには

1. クラウドサイバーエクスポージャーコンソールで、**[Settings > Single Sign-On]** に移動します。
2. **[アイデンティティプロバイダーの追加]**、**[Google]** の順にクリックします。
3. [Add Identity Provider] ダイアログで、**[Add]** をクリックします。

> **注意:** この方法で Google を IdP として追加すると、クラウドサイバーエクスポージャーコンソールと JIT ポータルの両方へのログインが有効になります。

SAML を使用した Google 経由でのログインの有効化

SAML を使用したログインを有効にする方法

1. Google管理コンソールで、**[アプリ] > [ウェブアプリとモバイルアプリ]** に移動します。
2. **[アプリの追加] > [カスタム SAML アプリの追加]** をクリックします。
3. **[アプリ名]** を入力し、**[続行]** をクリックします。
4. [Google ID プロバイダの詳細] ページで、**[メタデータをダウンロード]** をクリックします。

5. クラウド サイバーエクスポージャー コンソールで、**[Settings > Single Sign-On]** に移 動します。
6. **[アイデンティティプロバイダーの追 加]**、**[SAML]** の順にクリックします。
7. [アイデンティティプロバイダーの追 加] ダイアログで、ドロップダウンから **[JIT]** を選 択します。
8. **[ファイル]** を選 択し、Google からダウンロードしたメタデータをアップロードして、**[追 加]** をクリックします。
9. Google 管 理コンソールの [サービス プロバイダの詳 細] ページで、それぞれのフィールドに次 の値 を入 力します。
   - ACS URL: **https://{region}.app.ermetic.com/api/authentication/saml2/user/acs**

   region に入 力する値 は、Tenable One Cloud Exposure コンソールにログインする際に使 用する URL の値 に依 存します。リージョン別 の Tenable コンソール URL を参 照してください。
   - エンティティ ID: **urn:user.app.ermetic.com**
   - 名 前 ID の形 式 : **メール**
   - 名 前 ID: **基 本 情 報>プライマリメール**
10. **[続 行]** をクリックします。
11. [属 性 マッピング] ページで **[マッピングの追 加]** をクリックし、次 の属 性を追 加します。

    Google マッピングに対 するディレクトリ属 性 (アプリ属 性):
    - **名 :** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
    - **姓 :** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
    - **プライマリメール:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
12. (オプション) Google グループのサポートを追 加します。
13. **[終 了]** をクリックします。

Microsoft Entra ID 経 由 でのログインの有 効 化

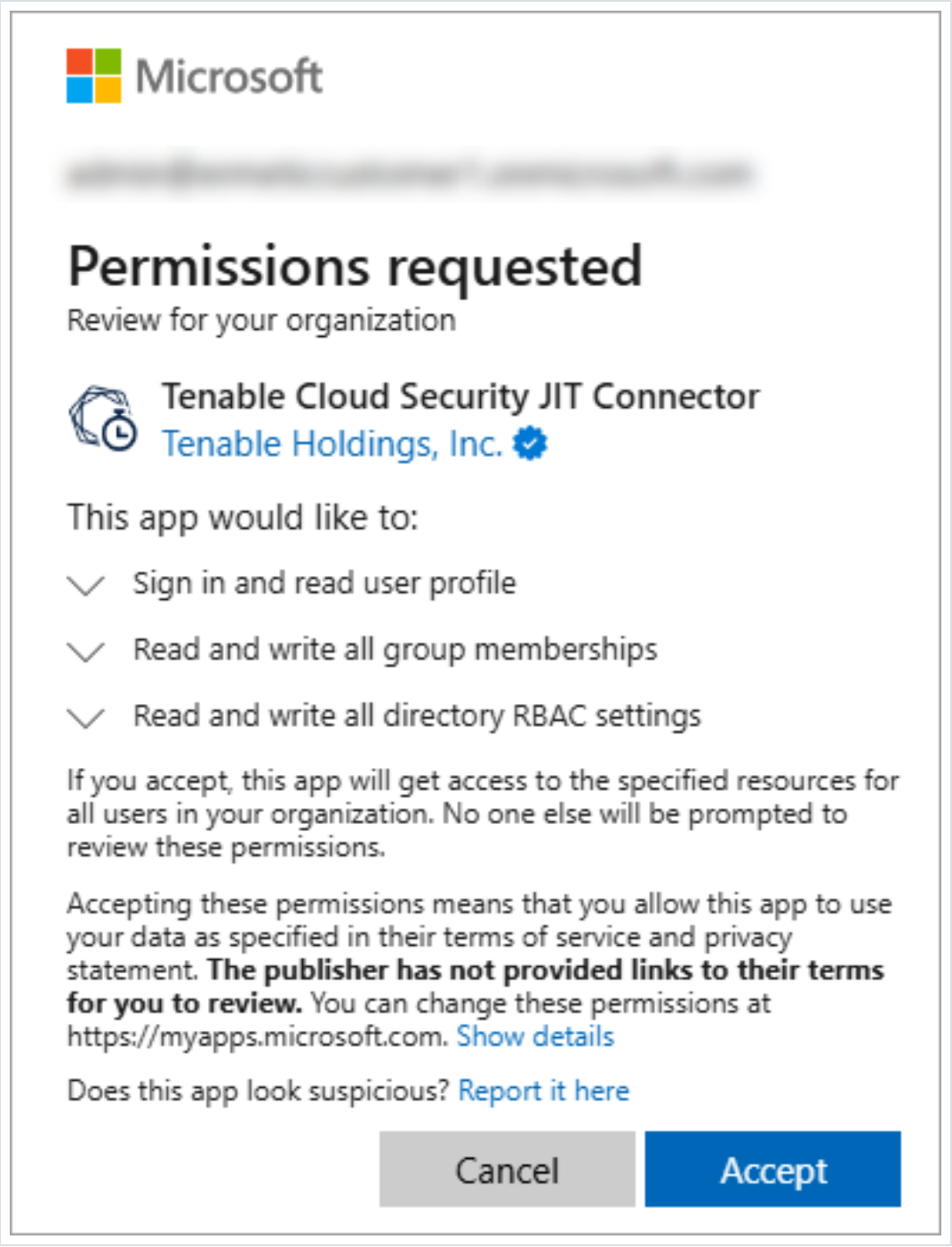
次 のいずれかのアイデンティティ仕 様を使 用して、Microsoft Entra ID 経 由 での JIT ポータルへのログインを有 効にします。

- OpenID Connect (OIDC)
- SAML

OIDC を使用した Microsoft Entra ID 経由でのログインの有効化

OIDC を使用したログインを有効にするには

1. クラウド サイバーエクスポージャー コンソールで、**[Settings > Single Sign-On]** に移動します。
2. **[アイデンティティ プロバイダーの追加]** をクリックし、**[Microsoft]** をクリックします。
3. [Add Identity Provider] (アイデンティティプロバイダーの追加) ダイアログで、**JIT** のリンクをクリックしてアクセス権を付与します。
4. 組織で クラウド サイバーエクスポージャー 管理者に関連付けられているアカウントを選択します。
5. リクエストされたアクセス許可を**受け入れ**ます。

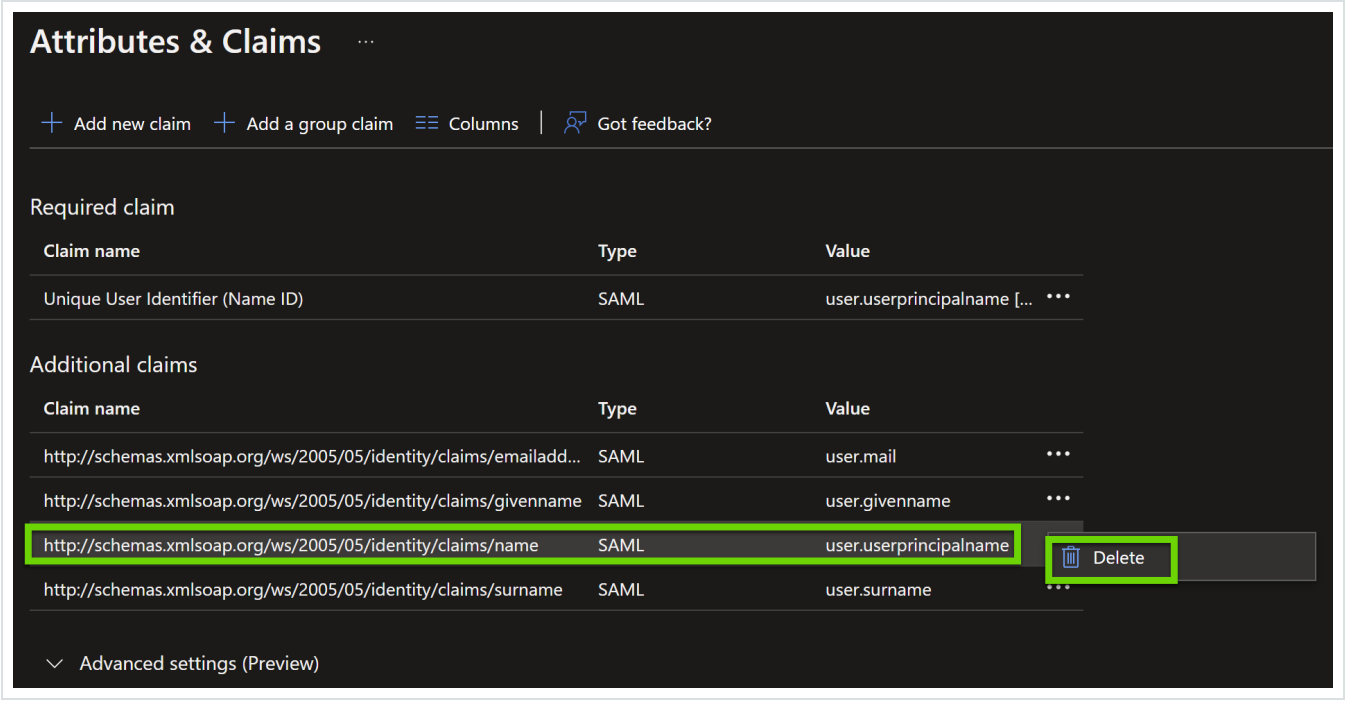


6. **[アクセス権を許可したことを確認する]** が選択されていることを確認し、**[追加]** をクリックします。

SAML を使用した Microsoft Entra ID 経由でのログインの有効化

SAML を使用したログインを有効にする方法

1. Azure portal で、**[エンタープライズ アプリケーション]** に移動し、**[新しいアプリケーション]** を追加します。
2. **[独自のアプリケーションの作成]** をクリックし、アプリの名前を入力します。
3. **[ギャラリーに見つからない他のアプリケーションを統合する (ギャラリー以外)]** の既定値を選択し、**[作成]** をクリックします。
4. 表示されるアプリの [概要] ページの [シングル サインオンの設定] ステップで、**[開始]** をクリックします。
5. SSO 方法として **[SAML]** を選択します。
6. [基本的な SAML 構成] で、**[編集]** をクリックし、それぞれのフィールドに以下の値を入力します。
    - 識別子 (エンティティ ID): **urn:user.app.ermetic.com**
    - 応答 URL (アサーションコンシューマサービス URL): **https://app.tenable.com/api/authentication/saml2/user/acs**
7. **[Save]** (保存) をクリックします。
8. [属性と要求] で **[編集]** をクリックし、[追加の要求] で **user.userprincipalname** 要求を削除します。



9. [SAML 証明書] で、**フェデレーションメタデータ XML** をクリックしてダウンロードします。

10. クラウド サイバーエクスポージャー コンソールで、**[Settings > Single Sign-On]** に移 動します。
11. **[アイデンティティプロバイダーの追 加]**、**[SAML]** の順にクリックします。
12. [アイデンティティプロバイダーの追 加] ダイアログで、ドロップダウンから **[JIT]** を選 択します。
13. **[ファイル]** を選 択し、Azure からダウンロードしたメタデータをアップロードして、**[追 加]** をクリックしま す。

Okta 経 由 でのログインの有 効 化

SAML 2.0 のアイデンティティ仕 様を利 用して、Okta 経 由 での JIT ポータルへのログインを有 効にします。

Okta 経 由 での JIT ポータルへのログインを有 効にする方 法

1. Okta 管 理コンソールで、**[アプリケーション] > [アプリケーション]** の順に移 動します。
2. **[アプリカタログを参 照]** をクリックします。
3. [検 索] フィールドに「 **クラウド サイバーエクスポージャー JIT** 」と入 力し、アプリケーションタイルをクリッ クして、**[追 加]** をクリックします。
4. アプリの **[サインオン]** タブを選 択し、**[編 集]** をクリックします。
5. [高 度 なサインオン] Settingsまでスクロールし、**[リージョン]** を入 力します。ここで入 力 する値 は、JIT ポータルへのログインに使 用 する URL (**https://{region}.app.ermetic.com/user/**) の値 によって異 なります。

   詳しくは、リージョン別 の Tenable コンソール URL を参 照してください。
6. [SAML セットアップ] セクションで、**[SAML セットアップ手 順 の表 示]** をクリックします。
7. [Configuration Steps] (構 成 ステップ) で、ステップ 2 にリストされている URL の値 をコピーします。
8. クラウド サイバーエクスポージャー コンソールで、**[Settings > Single Sign-On]** に移 動します。
9. **[アイデンティティプロバイダーの追 加]**、**[SAML]** の順にクリックします。
10. [アイデンティティプロバイダーの追 加] ダイアログで、ドロップダウンから **[JIT]** を選 択します。
11. **URL** を選 択し、Okta の URL 値 を貼り付 けて、**[追 加]** をクリックします。

OneLogin 経 由 でのログインを有 効にする

SAML 2.0 のアイデンティティ仕様を利用して、OneLogin 経由での JIT ポータルへのログインを有効にします。

OneLogin 経由での JIT ポータルへのログインを有効にする方法

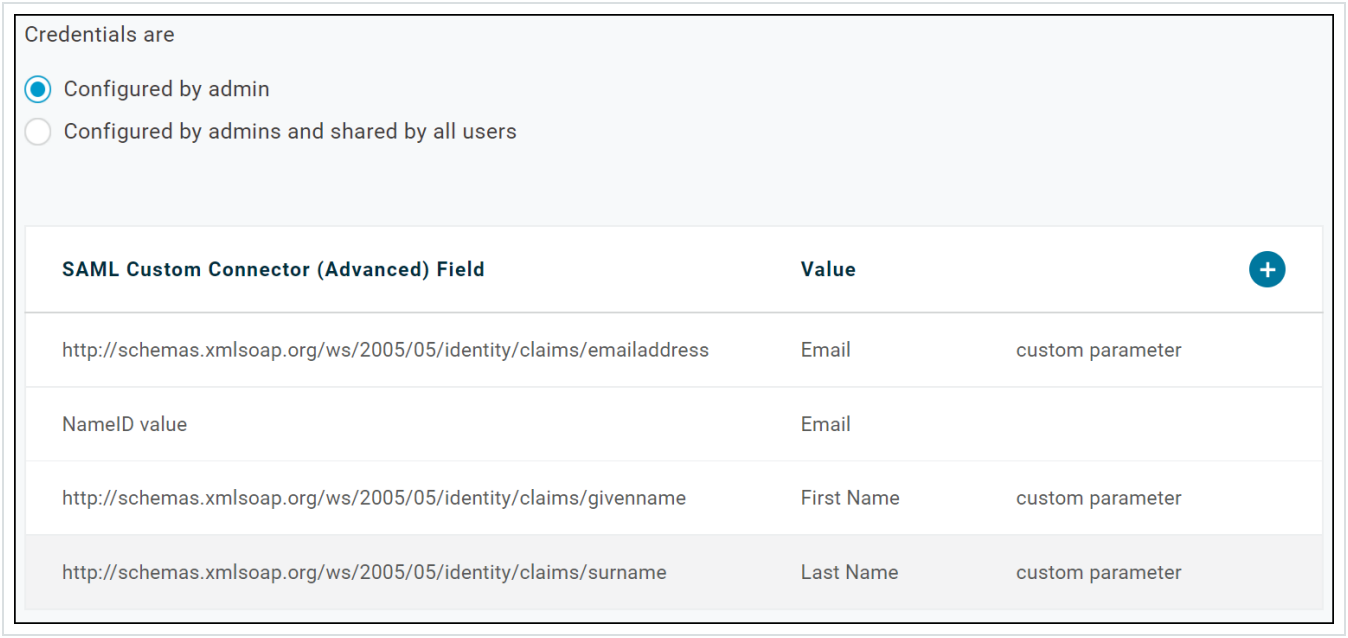
1. OneLogin 管理コンソールで、**[アプリケーション] > [アプリケーション]** の順に移動します。
2. **[アプリの追加]** をクリックします。
3. **[SAML Custom Connector (Advanced)]** を検索して選択します。
4. [設定] ページで、**[表示名]** (「クラウドサイバーエクスポージャー」など) を入力し、**[保存]** をクリックします。
5. [Configuration] (**構成**) タブに移動し、これらのアプリケーションの詳細に次の値を入力します。
   - オーディエンス (エンティティ ID): **urn:user.app.ermetic.com**
   - ACS (コンシューマー) URL Validator/ACS (コンシューマー) URL: **https://{region}.app.ermetic.com/api/authentication/saml2/user/acs**

   `region` に入力する値は、Tenable One Cloud Exposure コンソールにログインする際に使用する URL の値に依存します。リージョン別の Tenable コンソール URL を参照してください。
6. **[パラメーター]** タブに移動し、⊕ をクリックして、次の新しいフィールド/値を追加します。

   フィールド名を値に追加します。
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress:** E メール
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname:** 名
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname:** 姓

   重要: 各フィールド/値で **[Include in SAML assertion] (SAML アサーションに含める**) フラグが有効になっていることを確認します。

   注意: [NameID value] (NameID の値) フィールドは、OneLogin に標準装備で表示されます。このフィールドはそのままにしておくことができます。



7. [SSO] タブに移動し、**SAML 署名アルゴリズム** を **SHA-256** に設定します。
8. [その他のアクション] ドロップダウンをクリックし、**[SAML メタデータ]** を選択します。メタデータをコピーします。
9. クラウド サイバーエクスポージャー コンソールで、**[Settings > Single Sign-On]** に移動します。
10. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
11. [アイデンティティプロバイダーの追加] ダイアログで、ドロップダウンから **[JIT]** を選択します。
12. **[ファイル]** を選択し、OneLogin からコピーしたメタデータをアップロードして、**[追加]** をクリックします。

Ping Identity 経由でのログインの有効化

SAML 2.0 のアイデンティティ仕様を利用して、Ping Identity 経由での JIT ポータルへのログインを有効にします。

Ping Identity 経由での JIT ポータルへのログインを有効にする方法

1. Ping Identity 管理コンソールで、**[接続] > [アプリケーション]** に移動します。
2. [⊕] をクリックしてアプリケーションを追加します。
3. **アプリケーション名** を入力します。たとえば、「クラウド サイバーエクスポージャー」と入力します。

4. [アプリケーションタイプ] として **[SAML アプリケーション]** を選択し、**[構成]** をクリックします。
5. [SAML Configuration] (SAML 構成) で、**[Manually Enter] (手動入力)** を選択し、次の詳細を入力します。
    - **ACS の URL**:https://{region}.app.ermetic.com/api/authentication/saml2/user/acs

      `region` に入力する値は、Tenable One Cloud Exposure コンソールにログインする際に使用する URL の値に依存します。リージョン別の Tenable コンソール URL を参照してください。
    - **エンティティ ID**: urn:user.app.ermetic.com
6. **[保存]** をクリックします。
7. [Attribute Mappings] タブに移動し、[Edit] をクリックして、次の属性を追加します。

    PingOne マッピングの属性:

    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress:** メールアドレス
    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname:** 名
    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname:** 姓
8. ラジオボタンをクリックして、



9. [構成] タブに移動し、**[メタデータのダウンロード]** をクリックします。
10. クラウドサイバーエクスポージャーコンソールで、**[Settings > Single Sign-On]** に移動します。
11. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
12. [アイデンティティプロバイダーの追加] ダイアログで、ドロップダウンから **[JIT]** を選択します。
13. **[ファイル]** を選択し、OneLogin からコピーしたメタデータをアップロードして、**[追加]** をクリックします。

カスタム SAML 2.0 プロバイダー経由でのログインの有効化

上記のセクションで説明されていないプロバイダーを使用する場合は、SAML 2.0 のアイデンティティ仕様を利用することで、そのプロバイダー経由での JIT ポータルへのログインを有効にすることができます。

注意: 各プロバイダーでは、以下にリストされている詳細、パラメーター、属性を参照する際に、若干異なる名前や用語が使用される場合があります。以下の値が正しいパラメーターに構成されていることを確認してください。

カスタム SAML プロバイダー経由での JIT ポータルへのログインを有効にする方法

1. 対象プロバイダーごとに概説しているステップに従って、クラウドサイバーエクスポージャー専用のアプリケーションを追加します。必要に応じて、関連するドキュメントを参照してください。
2. アプリケーションで、以下の SAML の詳細を設定します。
    - エンティティ ID: **urn:user.app.ermetic.com**
    - ACS (リダイレクト URL): **https://{region}.app.ermetic.com/api/authentication/saml2/user/acs**

      `region` に入力する値は、Tenable One Cloud Exposure コンソールにログインする際に使用する URL の値に依存します。リージョン別の Tenable コンソール URL を参照してください。
    - 暗号化: **SHA-256**
    - SAML NameID の形式: **メール**
3. 以下の SAML 属性を追加し、必要に応じてそれらを指定されたプロバイダーにマッピングします:

    マッピングする属性:
    - メールアドレス: **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress**
    - 名: **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname**
    - 姓: **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname**

    注意: 名前の形式 = 指定なし
4. メタデータをダウンロードします。
5. クラウドサイバーエクスポージャーコンソールで、**[Settings > Single Sign-On]** に移動します。
6. **[アイデンティティプロバイダーの追加]**、**[SAML]** の順にクリックします。
7. [アイデンティティプロバイダーの追加] ダイアログで、ドロップダウンから **[JIT]** を選択します。
8. **[ファイル]** を選択し、前にダウンロードしたメタデータをアップロードして、**[追加]** をクリックします。

Slack と JIT の統合

注意: この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

Slack を JIT ワークフローの一部として使用して、ユーザーが簡単に以下のことを実行できるようにすることができます。

- Slack 経由でアクセスをリクエストする
- Slack 経由でアクセスを確認する

Slack と JIT を統合すると、ユーザーは Slack コマンドを通じてアクセス権をリクエストでき、承認リクエストが指定されたすべての承認者にプライベートメッセージ経由で自動的に送信されるため (設定されたワークスペースに Slack アカウントを持っている場合)、Slack でリクエストをネイティブにレビューできるようになります。プライベートな承認リクエストは Tenable One Cloud Exposure Slack アプリを通じて送信されます。承認リクエストを特定の Slack チャネルに送信することもできます。

JIT 用に Slack が有効になっている場合、関連する通知がメールと Slack のプライベートメッセージの両方で送信されます。リクエスト者と承認者は、リクエストや承認を JIT ポータル経由で行うか、Slack 経由で行うかを選択できます。そのどちらかで実行されたアクションは、もう一方でも更新されます。

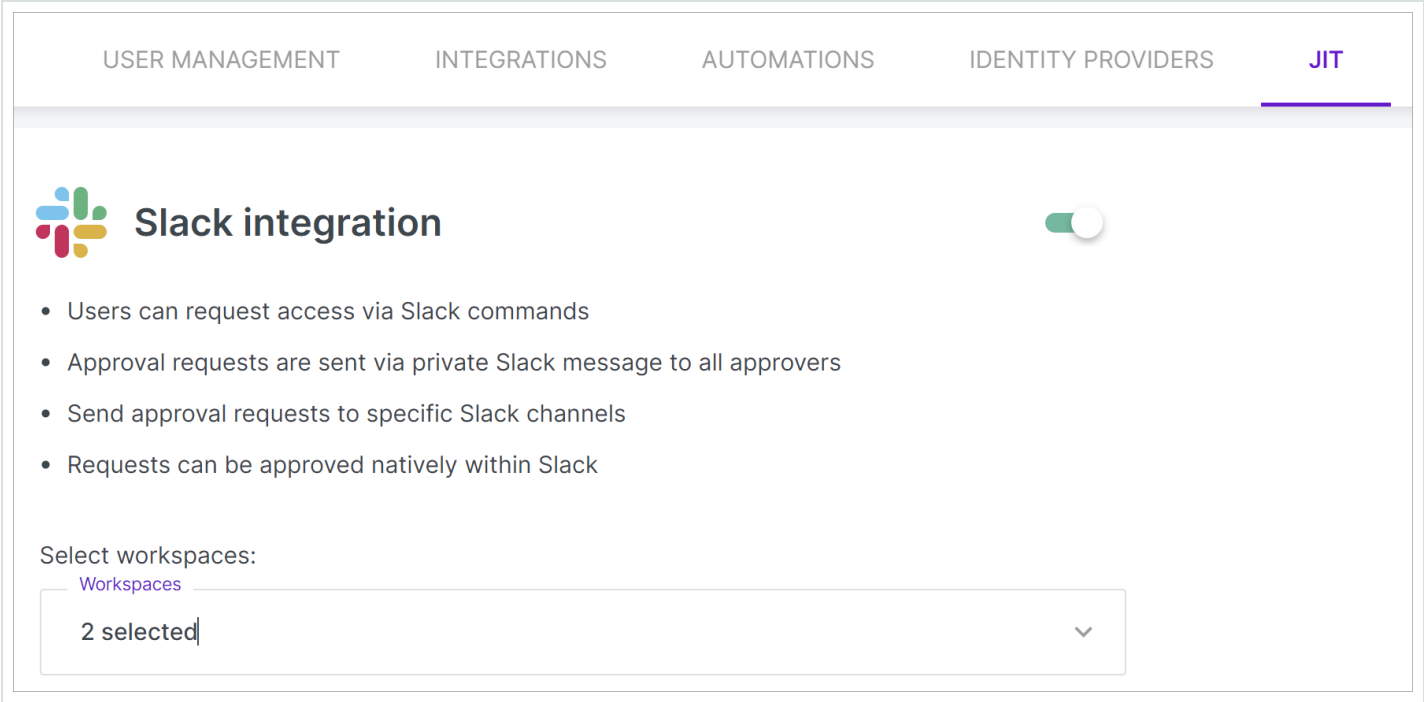
JIT アクセス用に Slack を有効にする前に、Slack ワークスペースを と統合する クラウド サイバーエクスポージャー必要があります。

JIT アクセス用に Slack を有効化

Slack for JIT を有効化するには

1. Slack ワークスペースとチャネルを またはと統合し クラウド サイバーエクスポージャー 、必要に応じてが 再認証されていることを確認します。
2. **[設定] > [JIT]** に移動します。
3. トグルボタンを使用して JIT 用の Slack を有効にし、JIT ワークフローの一部として使用する **ワークスペースを選択します** 。選択したワークスペースに存在するユーザーのみが Slack メッセージを受信します。複数のワークスペースを選択した場合、複数のワークスペースに存在するユーザーは、両方の場所でメッセージを受信します。

[Slack] トグルの画像を表示



重要: バージョン 1.51 以降にクラウドサイバーエクスポージャーコンソールに追加したワークスペース、またはクラウドサイバーエクスポージャーコンソールで再認証されたワークスペースのみが、ここにリストされ、JIT と連携する資格があります。

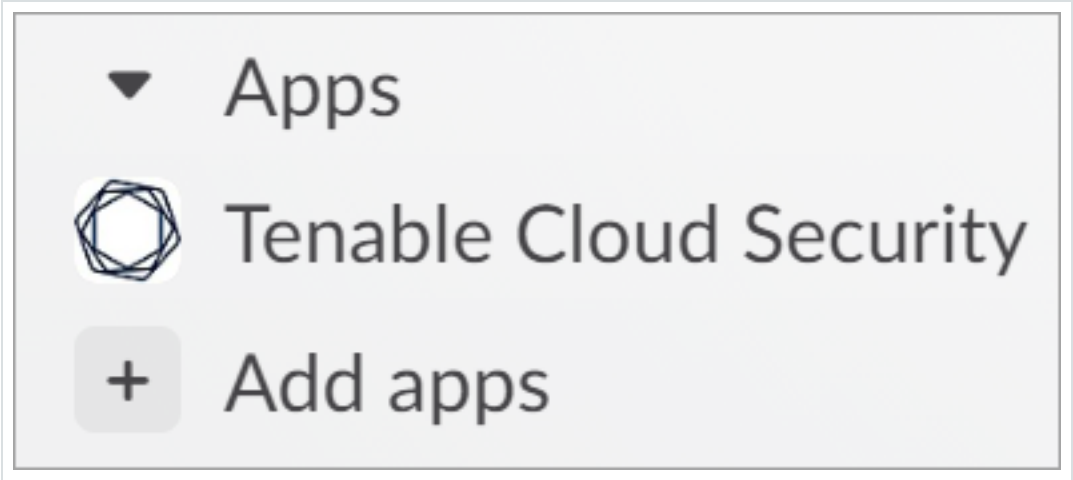
JIT 用の Slack を使用できるユーザー

Slack for JIT を使用するには、Slack for JIT を有効にした際に構成したワークスペースにユーザーが存在する必要があります。さらに、ユーザーは次の条件を満たす必要があります。

- **Slack 経由でアクセスをリクエストするには**: ユーザーは、アクセスをリクエストできるユーザー / グループのメンバーとして、資格情報で指定されている必要があります。
- **Slack 経由のアクセスをレビュー (承認または拒否) するには** Slack チャンネルに送信されたリクエストはさまざまなユーザーに表示される可能性がありますが、実際にリクエストの承認や拒否ができるのは「承認者」のみです。

メッセージの送信先

- プライベート承認リクエストは、アプリ領域にあるクラウドサイバーエクスポージャー Slack アプリを通じて、指定されたすべての承認者 (資格の追加で定義) に送信されます。



- 承認リクエストは、資格の追加の [追加の通知] セクションで定義されているチャネルにも送信されます。

Teams と JIT の統合

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

Teams を JIT ワークフローの一部として使用して、ユーザーが簡単に以下のことを実行できるようにすることができます。

- Teams 経由でアクセスをリクエストする
- Teams 経由でアクセスを確認 / 承認する

Teams を JIT と統合すると、ユーザーは JIT Portal の埋め込みバージョンを介して、Teams 内で直接アクセスをリクエストできます。JIT 用に Teams が有効になっている場合、関連する通知がメールアドレスと Teams の両方に送信されます。リクエスト者と承認者は、リクエストや承認を JIT ポータル経由で行うか、Teams 経由で行うかを選択できます。そのどちらかで実行されたアクションは、もう一方でも更新されます。

JIT アクセス用に Teams を有効にする前に、Teams 組織を と統合する Tenable One Cloud Exposure 必要があります。

JIT アクセス用に Teams を有効にする

Teams for JIT を有効化するには

1. Teams 組織を と統合します クラウド サイバーエクスポージャー。
2. クラウド サイバーエクスポージャー コンソールで、**[設定] > [JIT]** に移動します。
3. トグルボタンを使用して、Teams の JIT を有効にします。
4. Microsoft Teams に移動します。
5. **[アプリ]** をクリックし、**クラウド サイバーエクスポージャー Teams** アプリを検索して **[追加]** をクリックします。
    - チーム / チャネルの JIT アクセスを有効にするには、**[チームへの追加]** をクリックしてチーム / チャネル名を入力します。使用するチームとチャネルそれぞれに対してこれを行います。
    - 簡単にアクセスできるように左側のメニューにアプリを固定するには、**[チームに追加]** ボタンの横にあるドロップダウンをクリックし、**[追加]** をクリックします。

追加したチーム/チャネルは、クラウド サイバーエクスポージャー コンソールの **[設定] > [統合] > [チーム]** に表示されます。

Tenable Teams 用のアプリに必要なアクセス許可

クラウド サイバーエクスポージャー アプリを承認すると、Tenable に次のアクセス許可を付与します。

- **サインインして、ユーザープロファイルを読みます**。ユーザーのアプリへのサインインを許可します。アプリはサインインしたユーザーのプロファイルを読み取ることができます。また、アプリはサインインしているユーザーの基本的な会社情報も読み取ることができます。
- **組織の情報 を読み取ります**。サインインしているユーザーがいなくても、アプリが組織と関連リソースを読み取ることができます。関連するリソースには、サブスクリプションの skus やテナント ブランディング情報などがあります。

- **すべてのユーザーの完全なプロファイルの読み取り**。サインインしているユーザーなしで、アプリがユーザープロファイルを読み取ることができるようにします。
- **すべてのチームのリストを取得** サインインユーザーなしで、すべてのチームのリストを取得
- **すべてのチャネルの名前と説明を確認します**。サインインしていないユーザーなしで、すべてのチャネル名とチャネル説明を読み取ることができます。
- **すべてのチームにインストールされている Teams アプリを読み取る**。サインインしているユーザーがいなくても、アプリがチームにインストールされている Teams アプリを読み取ることができます。アプリケーション固有の設定を読み取る機能を提供しません。
- **すべての ユーザー に対してアプリの自身を管理できるようにします**。資格で定義された、すべての対象リクエスト者や承認者に対し、アプリが自身をインストールできます。

JIT アクセスを管理する

Tenable One Cloud Exposure ユーザー (「管理者」または「JIT 管理者」のロールを持つユーザー) は、アクセスに関する使用資格を管理して、有効なアクセスリクエストのパラメーターを定義し、JIT アクティビティ履歴の監査証跡を表示できます。

> **注意:** これらの機能に関するチュートリアルビデオを見ることもできます。
>
> - 使用資格の管理
> - JIT 監査ビデオ

資格の追加

資格を追加して、有効なアクセスリクエストのパラメーターを定義 JIT を利用して特定のクラウドプロバイダーにアクセス権を付与する方法の例については、一般的な JIT のユースケース。

選択されている場合、[資格] ページには次の 2 つのタブがあります。

- アカウントの使用資格: アカウントへのアクセスを許可する資格を表示します。
- AWS SSO アプリケーション利用資格: AWS Identity Center によって管理されるアプリケーションへのアクセスを許可する利用資格を表示します。このタブは AWS でのみ使用できます。

前提条件

- クラウドサイバーエクスポージャーで使用資格を追加するには、「管理者」または「JIT 管理者」のロールが必要です。
- 付与 Tenableクラウドサービスプロバイダーの関連組織に対する JIT アクセス許可。

注意: IAM Identity Center の委任された管理者アカウント (詳細については AWS のドキュメント を参照) を使用している場合、管理アカウントの範囲に使用資格を追加することはできません。管理アカウントの範囲で以前に追加された資格は、委任されたアカウントの使用に切り替えると無効になり、編集できなくなります。そのような使用資格は、範囲内にある他のアカウントでは引き続き有効です。

使用資格を追加する方法

1. 左側 アカウント階層とフォルダー ツリーで資格の範囲 (アカウントフォルダー) を選択します。これは、*リクエスト者*が依頼できるアカウントを定義します。
2. クラウドサイバーエクスポージャー JIT ポータルで、**[資格]** に移動します。
3. 選択した範囲が AWS アカウントにある場合は、関連するタブを選択します。
    - **アカウントの使用資格**: アカウントへのアクセスを許可する資格。
    - **AWS SSO アプリケーション利用資格**: AWS Identity Center が管理するアプリケーションへのアクセスを許可する資格。
4. **[使用資格の追加]** をクリックします。
5. 使用資格/アクセス **許可の名前を入力します** 。この名前はユーザーがアクセスをリクエストしたときに表示されます。
6. (AWS アカウントのアクセス許可)資格やアクセス許可の **ID** を入力します。これは一意の識別子として機能し、クラウドプロバイダーコンソールに表示されます。自動生成された ID を使用するか、独自に作成します。ID は小文字で 18 文字以内にする必要があります。
7. (オプション)リクエスト者がアクセス許可の性質を理解できるように、わかりやすい **説明** を入力します。説明は、リクエスト者が JIT ポータル経由でのアクセスのリクエストする際に、アクセス許可の横にツールチップとしてリクエスト者に表示されます。
8. リクエスト者が属する **組織** を選択します (JIT に複数の組織が構成されている場合)。

9. アクセスをリクエストできる **ユーザーとグループ** (*リクエスト者*) を選択します。複数のユーザーやグループを選択できます。
10. (AWS/Azure/GCP)ユーザーまたはグループがリクエストできる 1 つ以上の **アクセス許可** を選択します。
    - **AWS アカウントのアクセス許可: 管理ポリシー** を手動で選択するか、カスタマーマネージドポリシーを持つもの、またはアクセス許可の境界があるものを除く既存の IAM Identity Center **アクセス許可セット** を選択します。
      マネージドポリシーを使用する場合は、**インラインポリシー** (カスタム JSON) を追加し、ユーザーが上記で選択したアクセス許可に加えて組織固有のアクセス許可を使用してアクセスをリクエストできるようにします。JSON ポリシーは、関連するサイズ制限とともに、標準の AWS IAM ポリシー言語に従う必要があります。

      > **注意:** アクセス許可セットのインラインポリシーは 7,680 文字を超えることはできません。

    - **Azure**: すべての組み込みロールとカスタムロールはここで利用できます。複数のロールを選択した場合、リクエスト者は、リクエストを送信するときに、定義済みロールのうちどのアクセスをリクエストするかを選択できます。

      > **注意:** サブスクリプションに所有者ロールを付与するアクティブなアクセスリクエストが 1 つしかない場合、このアクセスが期限切れになることはなく、取り消すことはできません。

    - **GCP**: すべての組み込みロールとカスタムロールはここで利用できます。複数のロールを選択した場合、リクエスト者は、リクエストを送信するときに、定義済みロールのうちどのアクセスをリクエストするかを選択できます。
11. (アイデンティティプロバイダー)選択したユーザーとグループが参加をリクエストできる **グループ** を選択します。これにより、ユーザーやグループは、そのようなグループを介して付与された必要なアクセス許可を使用できます。

    > **注意:**
    > - **OneLogin**: ロール (グループの代わり)
    > - **Microsoft Entra ID**: ロール割り当て可能なグループと動的グループはリストされません。

12. ユーザーがアクセスをリクエストできる **アカウント** (または **アプリケーション**) を選択します。
    [リクエストごとにアカウント選択を制限する] を有効にすることもできます。これにより、アクセスリクエ

ストを送信する際にリクエスト者が選択できるアカウントの数を制限できます。たとえば、使用資格で 5 つのアカウントを選択した場合、ユーザーはリクエストごとに最大 3 つまで選択できます。

13. (Azure)使用資格を**リソースグループ**に制限するかどうかを選択します。
    1. アクセスをサブスクリプション全体ではなく特定のリソースグループに制限するには、**[リソースグループのみ]** にチェックを入れます。
    2. 選択すると、**[リソースグループ]** ドロップダウンがアクティブになります。ユーザーがこの使用資格をリクエストしたときにアクセスできる 1 つ以上の Azure リソースグループを選択します。**[リクエストごとにアカウントとリソースグループの選択を制限する]** を有効にすることもできます。これにより、リクエスト者が 1 つのリクエストで選択できるアカウントとリソースグループの数が制限されます。

    - **[リソースグループのみ]** が選択されていない場合は、次の点に注意してください。
        - ドロップダウンは無効になっていますが、以前に選択したグループは記憶されます。
        - リクエスト者は引き続きリソースグループへのアクセスをリクエストできますが、リソースグループに限定されるものではありません。
14. ユーザーまたはグループがリクエストできる **最大期間** (時間単位) (1～24) を選択します。期間は、アクセスが許可された時間から計算されます。
15. **承認ワークフロー**では、次のいずれかを選択します。
    - **承認は必要ありません**。リクエストが行われた後すぐにアクセス権を付与します。
    - **承認が必要です**。
16. 承認を必要とする場合は、プロンプトに従います。
    - リクエストをレビューする **承認者** を 1 人以上選択します。承認リクエストはすべての承認者にメールで送信されます。
        - JIT 用の Slack を有効にしている場合、リクエストは Slack のプライベートメッセージを介して、定義したワークスペースに存在するすべての承認者にも送信されます。
        - JIT 用の Team を有効にしている場合、リクエストは関連する Teams チャネル内にも送信されます。
    - (オプション)承認 **レベルを追加** して 複数レベルの承認ワークフローを作成し、アクセスを許可する前に別のユーザーがリクエストを承認する必要があります。

- (オプション) **追加の通知を送信します**。コラボレーションを進めるため、ここに他のユーザーを追加しておくと、メールまたはSlackチャンネルやTeamsチャネル(構成されている場合)でそうしたユーザーに通知することもできます。承認者のみがリクエストを承認または拒否できます。追加したクラウドサイバーエクスポージャーSlackチャンネルや、JIT用のSlackを有効化したときに選択したワークスペースにあるチャンネルはすべて、ここで利用できます。

17. ユーザーがアクセスをリクエストしたときに**正当性**の入力を要求するかどうかを設定します。
18. 反**復アクセス**を有効にするかどうかを選択します。これにより、リクエスト者はスケジュールされた間隔で自動的に再付与されるアクセスをリクエストできます。
    有効にした場合、**[最大反復日数]**を設定して、リクエスト者がアクセスをスケジュールできる期間を制限することもできます。これは、反復アクセスリクエストの開始日と終了日の間の最大日数を定義します。たとえば、制限が30日で、アクセスリクエストの開始日が1月1日の場合、リクエスト者は1月31日までのみ反復アクセスをスケジュールできます。なお、最大日数は364日を超えることはできません。
    デフォルトでは、すべての使用資格の**反復アクセス**が有効になり、**[反復の最大日数]**が364に設定されているため、リクエスト者は追加設定を行わなくても反復アクセスを利用できます。
19. **[追加]**をクリックします。

Azure所有者の使用資格

ユーザーがAzureで所有者ロールをリクエストできるようにする資格を追加できます。ただし、Azureでは、すべてのサブスクリプションに常に少なくとも1つのアクティブな所有者ロールの割り当てがあることを要求します。そのため、JITリクエストがサブスクリプションの唯一のアクティブな所有者割り当てである場合、スケジュールされた期間が終了した後でも、割り当てが期限切れになったり取り消されたりすることはありません。このキーは、別の所有者が割り当てられるまで有効です。

> 例を見る

たとえば、3人のユーザー(A、B、C)に3時間の間、所有者ロールに割り当てられる資格があるとします。必要な承認はありません。各ユーザーが所有者ロールに割り当てられるタイミングと、アクセス許可が期限切れになるタイミングの内訳を次に示します。

時間	アクション	オーナー
8:00	ユーザー A が所有者ロールに割り当てられます。	A
9:00	ユーザー B が所有者ロールに割り当てられます。	A、B
11:00	ユーザー A のアクセス許可の有効期限が切れます。	B
12:00	ユーザー B のアクセス許可は期限切れになりません。他の所有者がいないこと。	B
13:00	ユーザー C が所有者ロールに割り当てられます。ユーザー B のアクセス許可の有効期限が切れます。	C

JIT 経由で付与された所有者ロールのアクセス許可が想定どおりに期限切れになるように、サブスクリプションごとに少なくとも 1 つの恒久的な所有者割り当て (JIT 外部) を持つことをお勧めします。

> **注意:** JIT を介してすべての所有者割り当てをクラウド サイバーエクスポージャー削除する場合は、テナントの Tenable にグローバル管理者 ロールを割り当てることができます。これにより、サブスクリプションの最後の所有者割り当てを削除するために必要なアクセス許可がクラウド サイバーエクスポージャー 付与されます。

使用資格の管理

[資格] ページですべての使用資格を確認して管理できます。

- **テーブルをフィルタリングして** 、必要な情報をすばやく見つけます。たとえば、**[アカウント]** フィルターを使用して、特定のアカウント、フォルダー、またはアカウント ID の使用資格を表示できます。アカウント名、アカウント ID、フォルダー名でフィルタリングすることで、大きなリストを絞り込み、関連する使用資格を素早く見つけることができます。
- **テーブルの列は、** 選択した範囲内のプロバイダーまたは IdP の統合に基づいて変更されます。
- 列ピッカーを使用して**表をカスタマイズ**し、必要に応じて列を表示または非表示にします。

資格テーブルの列

縦棒	説明
名前	使用資格の名前。
範囲	定義されている場所を簡単に識別するための、資格の完全な組織パス。
組織	資格にリンクされている組織。
プリンシパル	アクセスをリクエストできるユーザーまたはグループ
アクセス許可	使用資格によって付与されるアクセス許可。(クラウドプロバイダーのみ)
インラインポリシー	資格に関連付けられているインラインポリシー。*(AWS のみ)*
アカウント	使用資格の範囲 (アカウントやフォルダーなど)*(クラウドプロバイダーのみ)*
リソースグループ	資格に含まれる Azure リソースグループ。(Azure のみ)
グループ	資格に含まれる IdP グループ。*(IdP のみ)*
最大期間	1 回のリクエストに対してアクセスを付与できる最大時間。
承認が必要	その資格に明示的な承認が必要かどうか。(デフォルトでは非表示)
承認者	アクセスリクエストを承認するために割り当てられているユーザー
第 2 レベル/第 3 レベルの承認者	複数レベルの承認ワークフローの追加承認者 (設定されている場合)。*(クラウドプロバイダーのみ)*
ステータス	使用資格の現在のステータス (アクティブ、非アクティブなど)。
正当性	リクエストを送信する際にリクエスト者が提供した説明。
反復アクセス	反復アクセスを通じて、アクセスを自動的に付与できる最大日数。反復アクセス

縦棒	説明
制限 (日数)	が無効になっている場合、このフィールドにはダッシュ (-) が表示されます。
アカウント/リソースグループの制限	資格で定義されている場合、リクエストごとに選択できるアカウント (または Azure ではアカウントとリソースグループを組み合わせたもの) の最大数。*(クラウドプロバイダーのみ)*

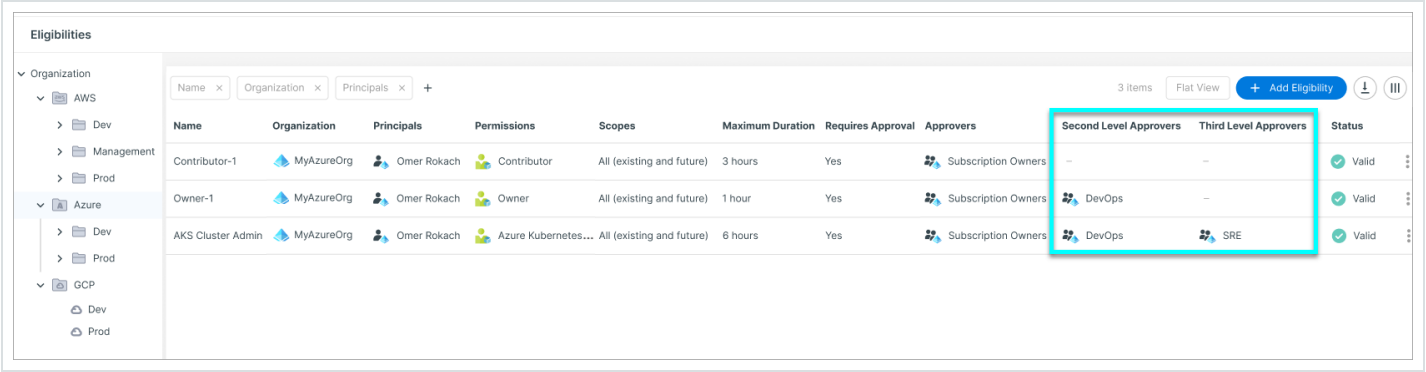
使用資格を管理するには

1. クラウドサイバーエクスポージャー JIT ポータルで、**[資格]** に移動します。
2. 対象の資格に移動し、三点リーダーをクリックして次のいずれかを選択します。
    - **編集**します。1 つ以上の資格パラメーターを更新します。
    - **削除**します。システムから資格を削除します。
    - **複製します**。既存の資格を複製して新しい資格を作成し、そのパラメーターを再利用または変更できるようにします。

複数レベルの承認ワークフロー

アクセスを許可する前に追加の承認段階を必要とする複数レベルの承認ワークフローを作成できます。

資格を追加する際に、アクセスリクエストに対して明示的な承認を必須とすることを選択した場合は、第 2 レベルまたは第 3 レベルの承認者を追加することもできます。最初の承認者 (第 1 レベル) がリクエストを承認すると、第 2 レベルの承認者に通知が送信されます。第 2 承認者はその後リクエストをレビューし、承認や拒否を行うことができます。資格で定義された最終承認者がリクエストを承認した後にのみ、リクエスト者にアクセスが許可されます。



- 最大 3 つの承認レベルを追加できます。
- 任意の承認レベル内で、1 人以上のユーザーやグループメンバーを承認者として選択できます。1 つのレベルに複数の承認者がいる場合、リクエストを次の承認レベルに進めるには、承認者のうちの 1 人の承認のみ必要です。
- リクエストが作成されてから 12 時間以内に承認者がリクエストをレビューしなかった場合、そのリクエストは期限切れとなります。複数レベルのワークフローを構成する場合、第 1 レベルの承認者によって承認されたリクエストは、第 2 レベルの承認者によって 12 時間以内にレビューされなければ有効期限が切れます。第 3 レベルの承認者が設定されている場合も、同じロジックが適用されます。

Slack での複数レベルの承認

Slack で JIT が有効になっている場合、複数レベルのワークフローのリクエストや承認は、JIT ポータルに加えて Slack 内でも実行できます。

> **注意:** Slack での複数レベルの承認ワークフローでは、承認者の **承認 / 拒否** ボタンは、(クラウドサイバーエクスポージャー アプリ内の) プライベートメッセージでのみ表示され、追加の通知の送信先として構成した Slack チャンネルには表示されません。

Ermetic1 APP 1 minute ago

Hi @[redacted], your access request was submitted successfully

Account: Org1Account3
Permissions: Reader
Duration: 4 hours
Justification: Deploying changes to dev environment. Ticket #7745

Connect

✅ @[redacted] and @[redacted] approved the request

3 replies

Ermetic1 APP 1 minute ago

Sent to review by [redacted]

Ermetic1 APP < 1 minute ago

Approved by @[redacted] and sent to review by [redacted]

Ermetic1 APP < 1 minute ago

✅ Access granted

Connect to your cloud environment

JIT アクティビティの監査

JIT 関連のアクティビティに関する監査証跡情報を、専用の監査ビューで表示します。このビューには、資格の追加、アクセスをリクエストする、JIT アクセス許可を持つユーザーがクラウドで実行したアクティビティに関する情報が含まれます。さらに、資格のアクティビティも一般 クラウド サイバーエクスポージャー 監査に送信されます。

現在フィルタリングされている監査証跡の結果を CSV ファイルにエクスポートできます。アクセス許可資格監査イベントテーブルとアクセス許可リクエスト監査イベントテーブルでは、列セレクターを使用して列の可視性をカスタマイズできます。列の設定は、セッション間で保存されます。

アクセス許可資格監査イベントテーブル

列	説明
時刻	アクションが実行された日時。
ユーザー	アクションを実行したユーザー (アクセスをリクエストした人やリクエストを承認した人など)。
アクション	実行されたアクション (アクセスのリクエスト、リクエストの承認など)。
リクエスト者	アクセスリクエストを送信したユーザー。
資格	使用されている資格の名前。
アカウント	各資格イベントに関連付けられたアカウント (表示参照とパスなど)。
Azure リソースグループ	イベントに関連する Azure リソースグループ。*(Azure アカウントのみ)*
リソースグループ	リクエストで選択された Azure リソースグループ。
アカウントの制限	資格で定義されている場合、リクエストごとに選択できるアカウント (または Azure ではアカウントとリソースグループを組み合わせたもの) の最大数。

列	説明
アクセス許可 *(クラウドプロバイダー)*	資格条件で付与されたアクセス許可、またはリクエスト者から要求されたアクセス許可。
[新規]	**グループ** *(IdP、デフォルトでは非表示)*
期間	アクセスが許可された時間の長さ。
反復アクセス制限 (日数) *(デフォルトでは非表示)*	反復アクセスを通じて、アクセスを自動的に付与できる最大日数。反復アクセスが無効になっている場合、このフィールドにはダッシュ (-) が表示されます。
正当性	リクエストを送信する際にリクエスト者が提供した説明。
承認が必要 *(デフォルトでは非表示)*	資格が明示的な承認を必要とするか、リクエストが行われた直後に自動的に承認されるか。
承認者	リクエストの承認に割り当てられたユーザーの一覧
スケジュール時間	アクセス許可リクエストのスケジュールされたアクティブ化時刻。

アクセス許可リクエスト監査イベントテーブル

列	説明
時刻	アクションが実行された日時。
ユーザー	アクションを実行したユーザー (アクセスをリクエストした人やリクエストを承認した人など)。
アクション	実行されたアクション (アクセスのリクエスト、リクエストの承認など)。
リクエスト者	アクセスリクエストを送信したユーザー。

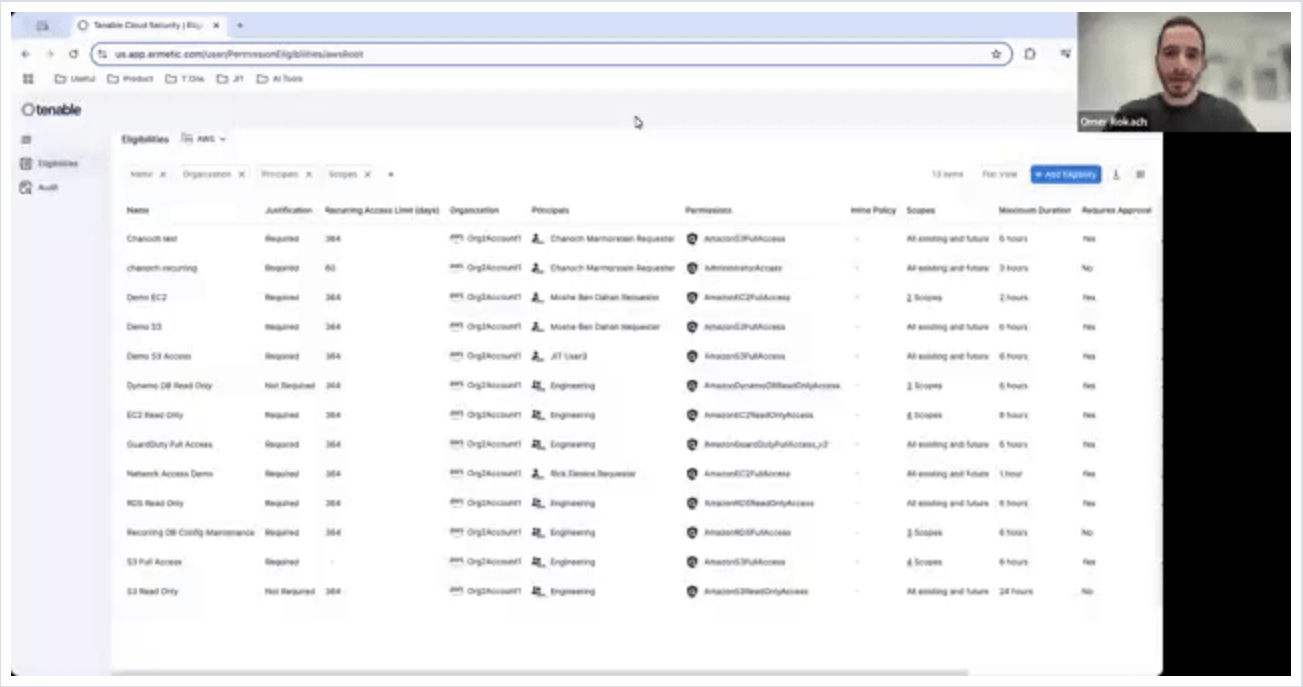
列	説明
資格	使用されている資格の名前。
アカウント	各リクエスト監査イベントに関連付けられているアカウント。
リソースグループ	リクエストで選択された Azure リソースグループ。
アカウントの制限	資格で定義されている場合、リクエストごとに選択できるアカウント (または Azure ではアカウントとリソースグループを組み合わせたもの) の最大数。
アクセス許可 *(クラウドプロバイダー)*	資格条件で付与されたアクセス許可、またはリクエスト者から要求されたアクセス許可。
グループ *(IdP、デフォルトでは非表示)*	資格で付与された、またはリクエスト者によって要求された IdP グループ。
期間	アクセスが許可された時間の長さ。
反復アクセス制限 (日数)	反復アクセスを通じて、アクセスを自動的に付与できる最大日数。反復アクセスが無効になっている場合、このフィールドにはダッシュ (-) が表示されます。
正当性	リクエストを送信する際にリクエスト者が提供した説明。
承認が必要	資格が明示的な承認を必要とするか、リクエストが行われた直後に自動的に承認されるか。
承認者	リクエストの承認に割り当てられたユーザーの一覧
スケジュール時間	アクセス許可リクエストのスケジュールされたアクティブ化時刻。

JIT アクティビティを監査する方法

1. クラウドサイバーエクスポージャー JIT ポータルで、**[監査]** に移動します。
2. 目的の監査データに応じて、次のいずれかのタブに移動します。
    - **アクセスリクエスト**
    - **資格**
3. 関連するパラメーターに従ってテーブルをフィルタリングします。

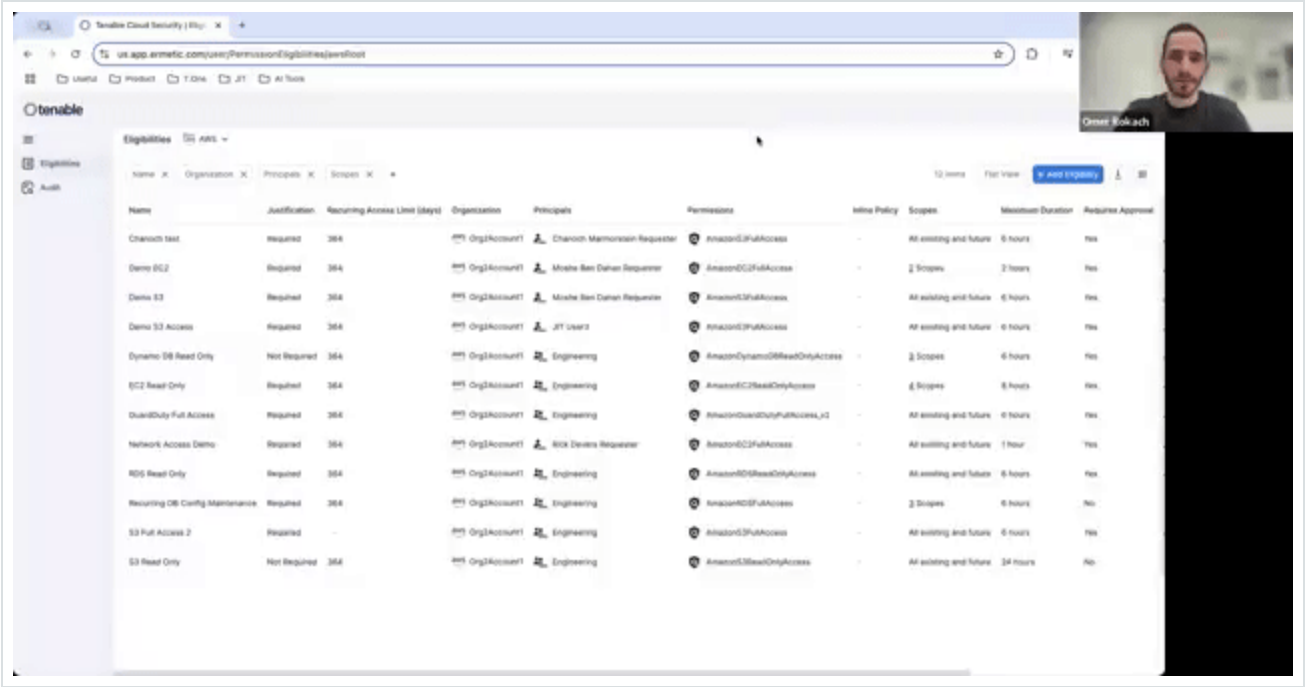
JIT 監査ビデオ

このビデオでは、JIT アクティビティの監査証跡の表示など、JIT アクセスの監査ページの使い方を学習できます。



資格管理 JIT ビデオ

このビデオでは、JIT アクセスで使用資格を追加および管理する方法を説明できます。



アクセスをリクエストする

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

定義されたアクセス許可を使用して、特定の期間に関連するアカウントへのアクセス (1 回限りの付与、反復スケジュールのいずれか) をリクエストします。リクエストを送信する場合、最初に資格 (管理ユーザーによって作成) を選択します。リクエストフォームに想定した資格がない場合は、そのユーザーがリクエスト者として設定されていないということです。

次の方法でアクセスをリクエストできます。

- Tenable One Cloud Exposure JIT ポータル
- Slack 経由でアクセスをリクエストする (有効な場合)
- Microsoft Teams (有効な場合)

リクエストに承認が必要な場合は、リクエストが承認または拒否されるとメールで通知されます。承認者が 12 時間以内にリクエストをレビューしなければ、そのリクエストは期限切れになります。リクエストが自動的に承認された場合、JIT ポータル、Slack、クラウドプロバイダー、またはアイデンティティプロバイダー

(IdP) のいずれかを介して、アクセス許可が即座に付与されます。JIT を介してアクセスが付与されると、クラウドプロバイダーのコンソールやポータルから、またはプログラムを使用してクラウドアカウントにアクセスできるようになります。また、アイデンティティプロバイダー (IdP) グループに追加されることでアクセス権が付与されることもあります。グループに参加すると、そのグループに関連付けられたアクセス許可が自動的に付与されます。

> **注意:** アクセスのリクエスト ビデオも視聴できます。

JIT ポータル経由でのアクセスのリクエスト

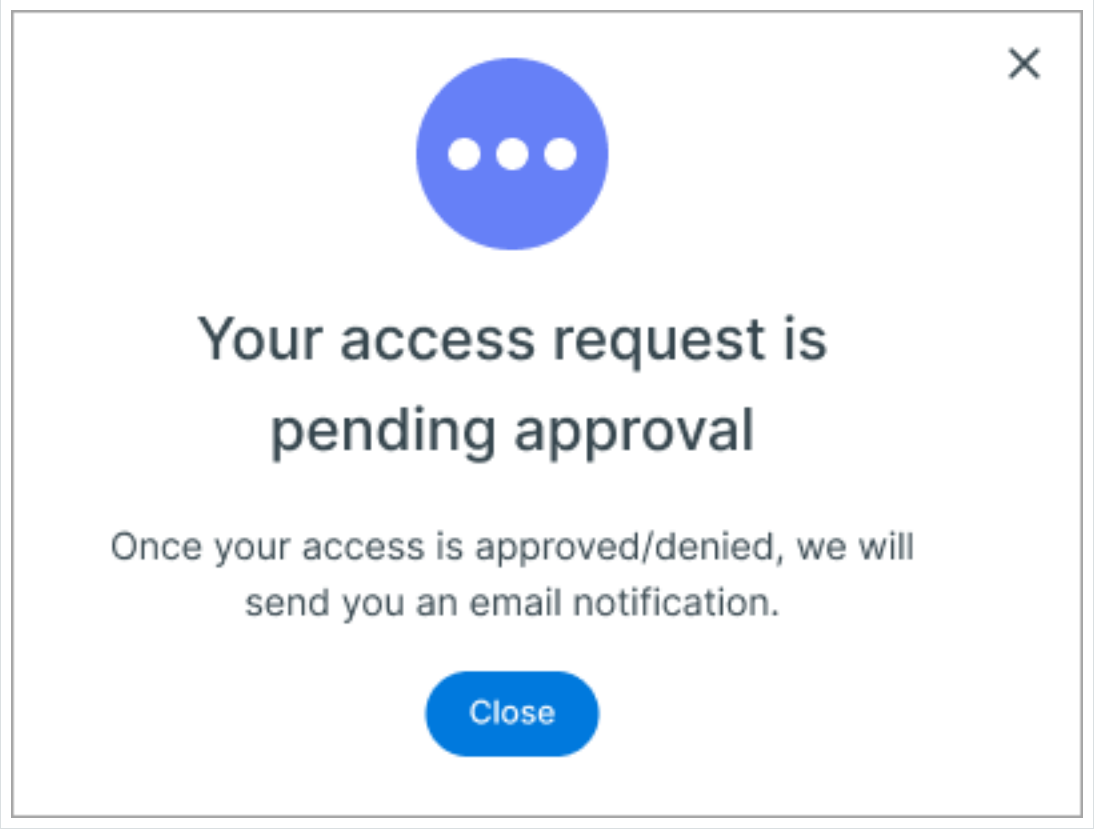
アクセスをリクエストするには

1. 次のいずれかの URL を使用して、クラウド サイバーエクスポージャー JIT ポータルにログインします。
   - **グローバル (すべてのリージョン)**: `app.tenable.com/user`
   - **米国ガバメントクラウド**: `app.tenable.us/user`
2. 左側のナビゲーションメニューから **[リクエスト]** に移動します。
3. **[アクセスのリクエスト]** をクリックします。
4. タスクの実行に必要な **資格** を選択します。利用可能なアクセス許可の詳細については、「資格の追加」を参照してください。
5. クラウドプロバイダーへのアクセスをリクエストする場合は、アクセスする **アカウント** を選択します。資格設定によっては、リクエストごとに選択できるアカウントの数 (Azure ではアカウントとリソースグループの数) に制限がある場合があります。
6. (Azure)選択したサブスクリプション内の **リソースグループ** を選択します。リソースグループの選択がオプションである場合は、この手順をスキップして、サブスクリプションレベルでアクセスをリクエストできます。
7. (Azure および GCP)資格により複数のロールへのアクセスを許可できる場合は、アクセスをリクエストする **ロール** を選択します。このリストには、資格で定義されているロールのみが含まれます。タスクに必要なものに応じて、1 つ以上のロールを選択できます。

8. 希望の**アクセス時刻**を選択します。アクセスをリクエストできます。
    - **即時** および期間: アクセス許可は、必要な承認後すぐに付与されます。期間は、リクエストが承認された時点から計算されます。
    - スケジュール**済み**: アクセス許可が付与される日時を指定し、必要な承認を保留にします。期間は、承認後、選択した開始時間から計算されます。
    - 反**復**: 開始日時、反復頻度 (毎日、毎週月曜、毎月 1 日など)、反復アクセスの終了日を指定します。アクセスはスケジュールに従って複数回にわたって付与されても、反復リクエストの承認は一度だけです。各インスタンスの期間は、最初の承認後にスケジュールされた開始時刻から計算されます。承認されると、追加の承認なしで、スケジュールされた時間にアクセス権が自動的に付与されます。

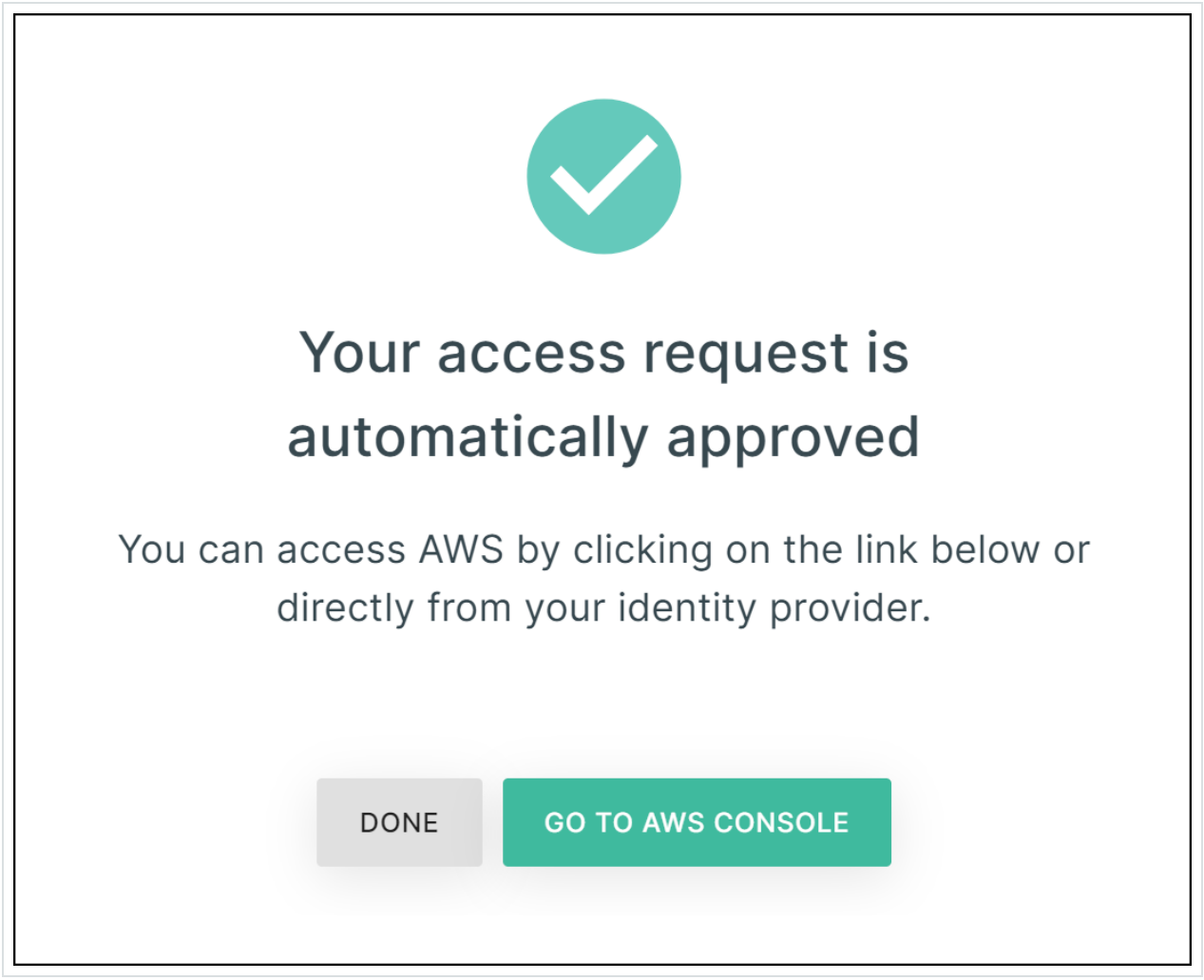
      次の点に注意してください。
    - 管理者の設定によっては、反復アクセスをリクエストできない場合があります。
    - 各資格には、反復する最大日数の制限があります。反復リクエストの終了日は、開始日から許容された日数内に収まる必要があります。たとえば、最大期間が 30 日で、開始日が 1 月 1 日の場合、アクセスをリクエストできるのは 1 月 31 日までです。
    - スケジュールされた開始時刻または最初の反復の開始時刻までにリクエストが承認されなければ、その時点で (または 12 時間後のいずれか早い方で) 期限切れになります。たとえば、ユーザーが、毎週月曜日の午後 3 時に開始して 4 時間継続するアクセスを 1 か月間反復するというリクエストを午前 9 時に送信したとします。承認者が最初の月曜日の午後 3 時までに承認しなかった場合、この反復リクエスト全体が期限切れになります。
9. 必要に応じて、**理由** を入力し、このアクセスが必要な理由について詳細を提供します。
10. **[リクエスト]** をクリックします。

- リクエストに承認が必要な場合は、リクエストが承認または拒否されるとメールで通知されます。



リクエストは [Access Requests] (アクセスリクエスト) ページの [Pending] (保留中) セクションに表示されます。

- リクエストが自動的に承認される場合は、承認の関連リンクをクリックすることでクラウドアカウントにアクセスできます。



> **注意:** AzureとGCPの場合、サーバープロバイダー側のキャッシングの問題により、承認からアクセスが可能になるまでに1分から10分かかる場合があります。

リクエストは [Access Requests] (アクセスリクエスト) ページの [Active] (アクティブ) セクションに表示されます。

クラウドまたはIdPアカウントに接続する

[接続] オプションを使用して接続し、関連するクラウドプロバイダーまたはアイデンティティプロバイダーにアクセスします。

1. JIT ポータルで、左側のナビゲーションメニューから **[アクセスリクエスト]** に移動します。
2. [Active] (アクティブ) セクションで、関連するリクエストに移動します。
3. 三点リーダーアイコンをクリックし、**[接続]** をクリックします。

アクセスの再リクエスト

[再度リクエスト] を使用して、前のリクエストと同じパラメーターで新しいアクセスリクエストを開始します。リクエストフォームには以前の詳細が自動入力されており、それを編集して送信できます。

1. JIT ポータルで、左側のナビゲーションメニューから **[アクセスリクエスト]** に移動します。
2. [Active] (アクティブ) セクションで、関連するリクエストに移動します。
3. 三点リーダーアイコンをクリックし、**[再リクエスト]** をクリックします。

Slack 経由でアクセスをリクエストする

Slack コマンドを使用すると、必要なアカウントへのアクセスをリクエストできます。

[アクセスのリクエスト] ダイアログボックスで、**[再度リクエスト]** をクリックすると、以前のリクエストと同じパラメータで新しいアクセスリクエストを開始できます

Slack コマンドの使用に加えて、クラウドサイバーエクスポージャー Slack アプリの [ホーム] タブで最近のアクセスリクエストの最新ステータスを確認できます。リクエストが承認されたら、すぐにクラウドアカウントに接続するか、Slack から直接アクセスを取り消すことができます。

前提条件

- Slack ワークスペースを クラウドサイバーエクスポージャー と統合する
- JIT アクセス用に Slack を有効にする
- アクセスをリクエストする 資格 が必要です。Slack 経由でアクセス権をリクエストできない場合は、リクエストする資格があるかどうかを クラウドサイバーエクスポージャー 管理者に確認してください。

アクセスをリクエストするには

1. クラウド サイバーエクスポージャー Slack アプリまたは任 意 の Slack チャンネル/メッセージから、次 のように入 力します。

   ```
   /tenable jit
   ```

2. [アクセスのリクエスト] ダイアログボックスで、次を選 択します。

   - アクセスする **クラウドプロバイダー** 。
   - タスクを実 行するために必 要な **資 格** 。利 用 可 能なアクセス許 可 の詳 細については、「 資 格の追 加 」を参 照してください。
   - アクセスする**アカウント** 。(資 格に選 択 肢 制 限 が定 められている場 合 は、その数まで選 択できます)。
   - **(Azure)** 選 択したサブスクリプション内 のリソースグループ (該 当する場 合)。
   - **(Azure および GCP)** リクエストするロール (資 格で定 義されたロールのみ)。
   - アクセスが必 要な **期 間** (時 間 単 位)。期 間は、リクエストが承 認された時 点から計 算されます。
   - 承 認 後 の希 望する**アクセス時 間**

     - **即 時** および期 間 : アクセス許 可 は、必 要な承 認 後すぐに付 与されます。期 間は、リクエストが承 認された時 点から計 算されます。
     - スケジュール**済 み** : アクセス許 可 が付 与される日 時を指 定し、必 要な承 認を保 留にします。期 間は、承 認 後 、選 択した開 始 時 間から計 算されます。
     - 反 **復** : 開 始 日 時 、反 復 頻 度 (毎 日 、毎 週 月 曜 、毎 月 1 日など)、反 復アクセスの終 了 日を指 定します。アクセスはスケジュールに従って複 数 回にわたって付 与されますが、反 復リクエストの承 認は一 度だけです。反 復アクセスの各 インスタンスの期 間は、最 初 の承 認 後 に、そのインスタンスのスケジュールされた開 始 時 刻から計 算されます。反 復リクエストが承 認されると、ユーザーはスケジュールされた時 間に自 動 的にアクセス権を受 け取り、その都 度 インスタンスの承 認を受 ける必 要はありません。

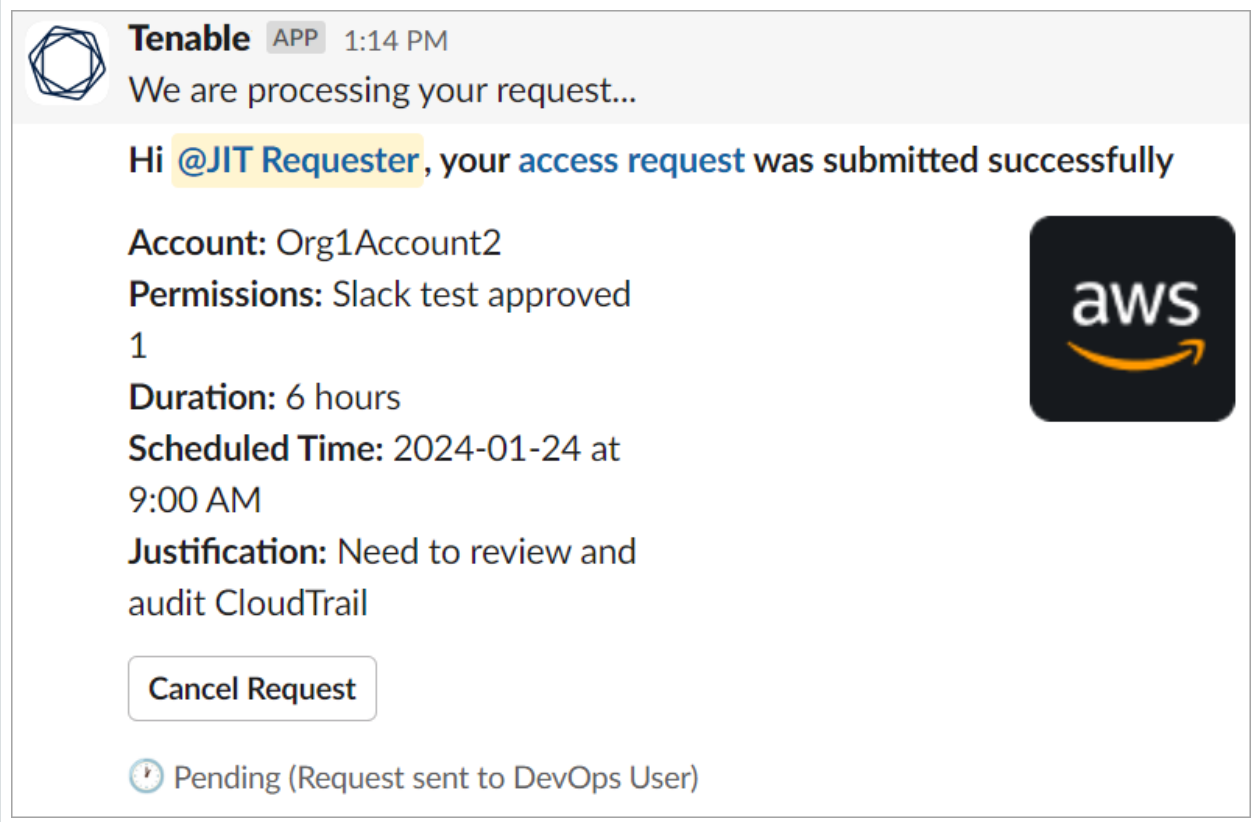
     > スケジュールされた開 始 時 刻または最 初 の反 復の開 始 時 刻までにリクエストが承 認されなければ、その時 点で (または 12 時 間 後 のいずれか早 い方で) 期 限 切 れになります。たとえば、ユーザーが、毎 週 月 曜 日の午 後 3 時に開 始して 4 時 間 継 続するアクセスを 1 か月 間 反 復するというリクエストを午 前 9 時に送 信したとします。承 認 者 が最 初 の月 曜 日の午 後 3 時までに承 認しなかった場 合 、この反 復リクエスト全 体が期 限 切 れになります。

- 理由を入力し、このアクセスが必要な理由について**詳細を提供します。**このフィールドは必須です。

3. **[Submit]** (送信) をクリックします。リクエストについて通知する Slack のレスポンスを受け取ります。Slack のレスポンスは、非公開で送信されます。公開メッセージまたはチャネルでコマンドを入力した場合、応答はその公開メッセージまたはチャネルには送信されません (チャネルが通知の受信 資格の追加 ている場合を除きます)。

   Slack の対応:

   - **リクエストには承認が必要です**: リクエストが承認または拒否されると通知が届きます。Slack メッセージ内の **アクセスリクエスト** リンクをクリックすると、クラウドサイバーエクスポージャー JIT ポータルの [アクセスリクエスト] ページ ([保留中] セクション) にリクエストが表示されます。リクエストをキャンセルするには、**[リクエストをキャンセル]** をクリックします。



   - リクエスト **承認済み**: クラウドアカウントがアクティブになっている間はいつでも、**[接続]** またはアクセス**の取り消し**をクリックすることでアクセスできます。

> **注意:** AzureとGCPについては、サーバープロバイダー側のキャッシングの問題により、承認からアクセスが可能になるまでに最大で10分かかる場合があります。

Teams経由でアクセスをリクエストする

埋め込みバージョンのJITポータルから、Teamsで直接アクセスをリクエストできます。

前提条件

- Microsoft Teams
- JITアクセス用にTeamsを有効にする

アクセスをリクエストするには

1. Microsoft Teamsに移動します。
2. [アクセスリクエスト] ページで、**[アクセスのリクエスト]** をクリックします。
3. [アクセスのリクエスト] ダイアログボックスで、次を選択します。
    - タスクを実行するために必要な **アクセス許可** 。利用可能なアクセス許可の詳細については、「資格の追加」を参照してください。
    - クラウドプロバイダーへのアクセスをリクエストする場合は、アクセスする **アカウント** を選択します。
    - アクセスが必要な **期間** (時間単位)。期間は、リクエストが承認された時点から計算されます。
    - 承認後にアクセスを開始する開始 **時刻**
        - **すぐに**。アクセス許可は、必要な承認が行われた後すぐに付与されます。期間は、リクエストが承認された時点から計算されます。
        - **開始時刻を選択します**。アクセス許可が付与される日時を指定し、必要な承認をそれまで保留にします。期間は、承認後、選択した開始時間から計算されます。

    スケジュールされた開始時間までにリクエストが承認されない場合、その時点で (または12時間後のいずれか早い方で) 期限切れになります。たとえば、ユーザーが午前9時に、同日の午後3時から4時間のアクセスをリクエストしたとします。

- 承認者が午後 3 時までにリクエストを承認または拒否しなかった場合、リクエストはその時点で期限切れとなります (スケジュールされた時間を過ぎたため)。
- 承認者が午後 3 時より前の任意の時点でリクエストを承認した場合、リクエスト者は午後 3 時から午後 7 時までのアクセス権を付与されます。

4. 理由を入力し、このアクセスが必要な理由について**詳細を提供します。**このフィールドは必須です。
5. **[リクエスト]** をクリックします。
    - リクエストに承認が必要な場合は、リクエストが承認または拒否されるとメールで通知されます。

    リクエストは [Access Requests] (アクセスリクエスト) ページの [Pending] (保留中) セクションに表示されます。
    - リクエストが自動的に承認される場合は、承認の関連リンクをクリックすることでクラウドアカウントにアクセスできます。

> **注意:** Azure と GCP については、サーバープロバイダー側のキャッシングの問題により、承認からアクセスが可能になるまでに 1 分から 10 分かかる場合があります。

リクエストの表示と管理

アクセスアクティビティは、JIT ポータルの 2 つのページ (**アクセスリクエストとアクセスレビュー**) から表示および管理できます。

アクセスリクエスト

[アクセスリクエスト] ページでは、リクエスト者が作成したアクセスリクエストを追跡および管理できます。

[**Active]** タブでは、すべてのアクティブなリクエストと保留中のリクエストを表示できます。

- 保留中のリクエストについては、たとえば、実際にはアクセス権が必要ないことが判明した場合や、誤ってリクエストを送信していた場合に、リクエストをキャンセルできます。
- アクティブなリクエストの場合、関連するクラウドアカウントにアクセスしたり、アクセス権を取り消したり、同じ設定でアクセスを再度リクエストすることができます。

[Active] タブのステータスリスト:

ステータス	記
アクティブ	リクエストが承認されてアクティブ化され、ユーザーがアクセス権を持っています。
アクティブ化待ち	リクエストは承認されましたが、アクセスはまだアクティブ化されていません
承認待ち	リクエストが送信され、承認者による承認を待っています

[履歴] タブでは、過去のすべてのリクエストを表示できます。

[履歴] タブのステータスリスト

ステータス	記
アクセスの期限切れ	承認されたアクセス期間が終了し、アクセスの有効期限が切れています
アクセスの取り消し	承認されたリクエストの期間が終了し、アクセスが取り消されました
アクティベーションの失敗	承認後にアクセスのアクティブ化中にエラーが発生しました
リクエストのキャンセル	リクエストはリクエスト者によってキャンセルされました
リクエストの拒否	リクエストが承認者により拒否されました
リクエストがタイムアウトしました	12 時間以内、またはリクエストのスケジュール時刻までに、リクエストが承認者によってレビューされなかった

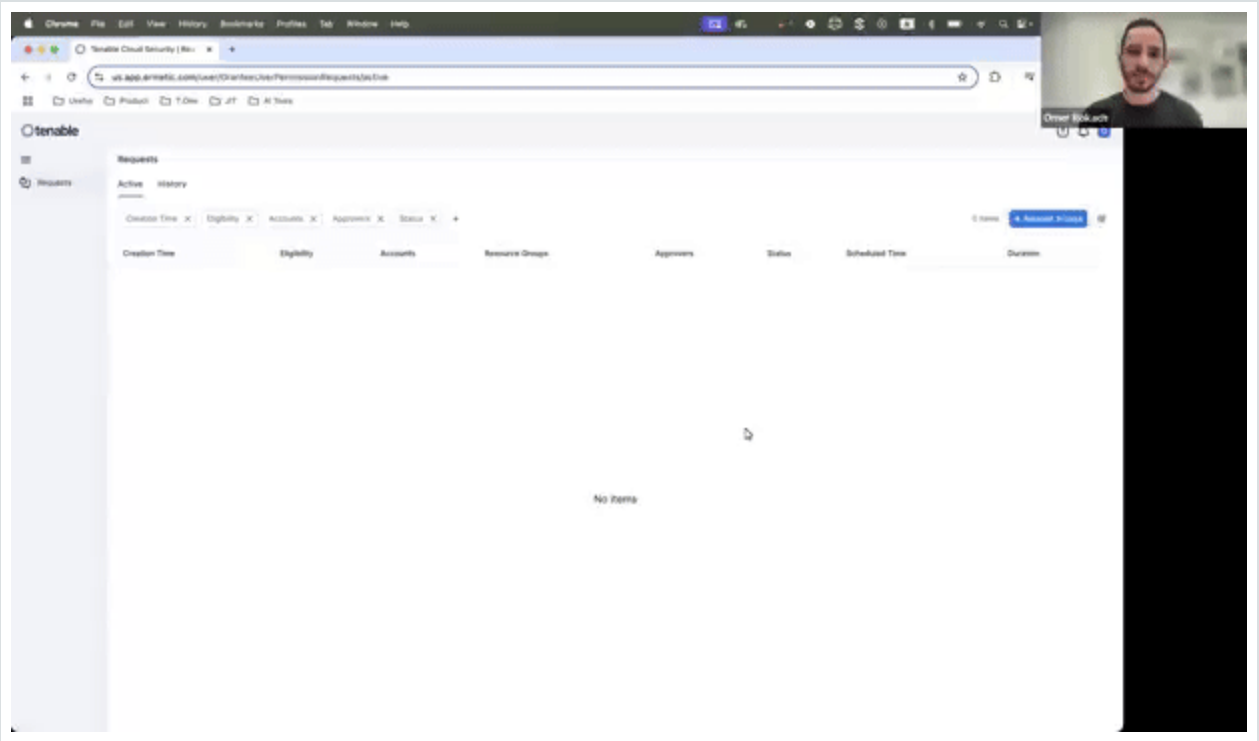
アクセスレビュー

[Access Reviews] ページには、すでに付与されているアクセスに関する情報が表示されます。これは、追跡や監査の目的に役立ちます。このページは、少なくとも 1 つの資格で承認者ロールが割り当てられている場合に表示されます。

[Active] タブでは、現在アクティブなアクセスセッションをすべて表示できます。**[履歴]** タブでは、アクティブでなくなった過去のすべてのアクセスセッションを表示できます。

アクセスのリクエスト ビデオ

このビデオでは、アカウント、ロール、グループの選択方法、必要な詳細の入力方法など、JIT アクセスリクエストを送信する方法を説明します。



アクセスの確認

> **注意:** この機能は、Cloud Vulnerability Management ライセンスでは使用できません。

Tenable One Cloud Exposure [] 管理者は権限を追加するとき、その権限に関連するアクセスリクエストを手動でレビューするように承認者を指定できます。リクエストが行われると、承認者はメールおよびSlackを介して(有効な場合)、保留中のリクエストがあることが通知されます。

次の方法でアクセスを確認および承認できます。

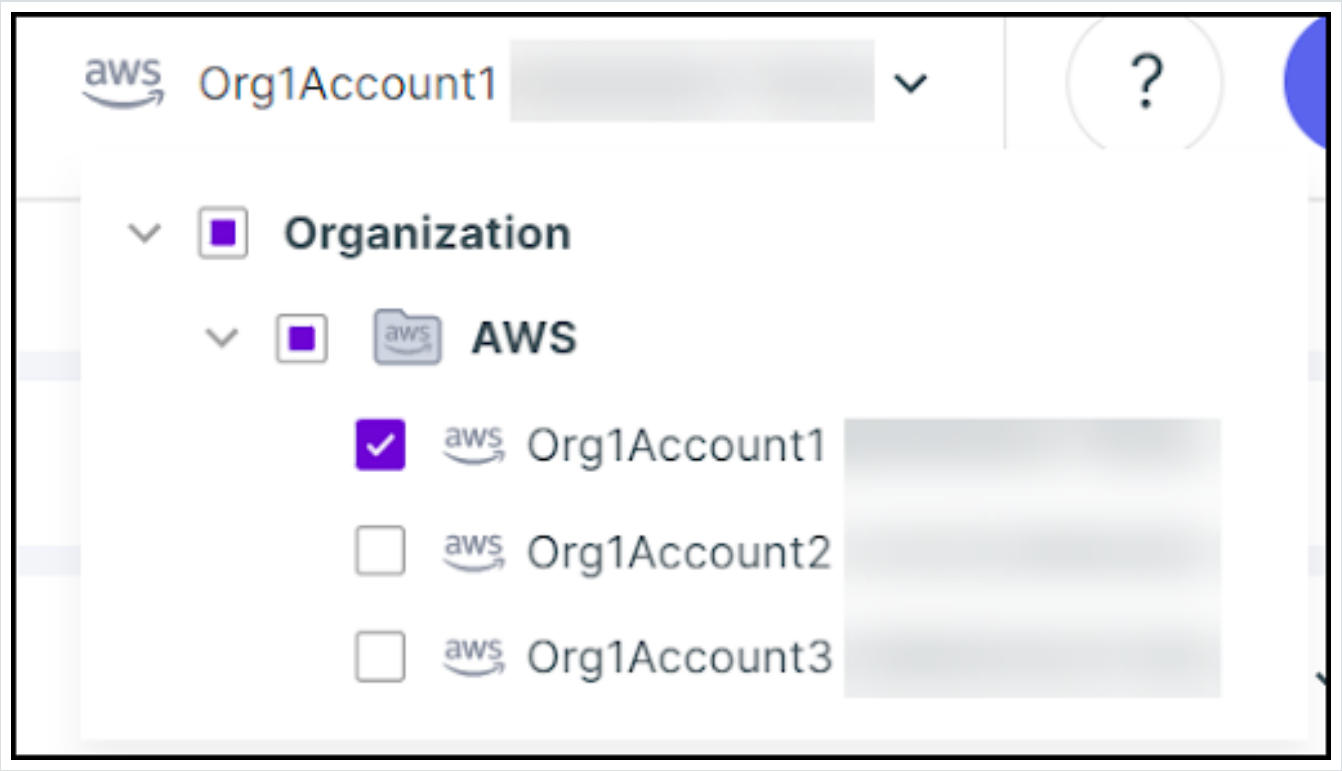
- JIT Portal
- Slack経由でアクセスを確認する(有効な場合)
- Microsoft Teams(有効な場合)

> **注意:** アクセスビデオの確認も見ることができます。

JITポータルからアクセスを確認する

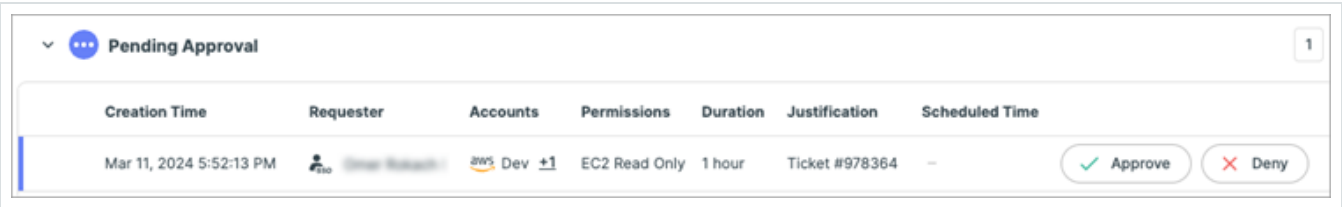
アクセスリクエストを確認する方法

1. 次のいずれかのURLを使用してクラウドサイバーエクスポージャーJIT Portalにログインします。
    - **グローバル(すべてのリージョン)**: `app.tenable.com/user`
    - **米国ガバメントクラウド**: `app.tenable.us/user`
2. 左側のナビゲーションメニューから**[アクセスレビュー]**に移動します。
3. 特定のアカウントのアクセスリクエストを確認する場合は、ページ右上のドロップダウンからアカウントを選択します。



4. **[保留中]** セクションに移動し、リクエストを確認します。

> **注意:** 上部にあるフィルターを使用して、結果を絞り込みます。

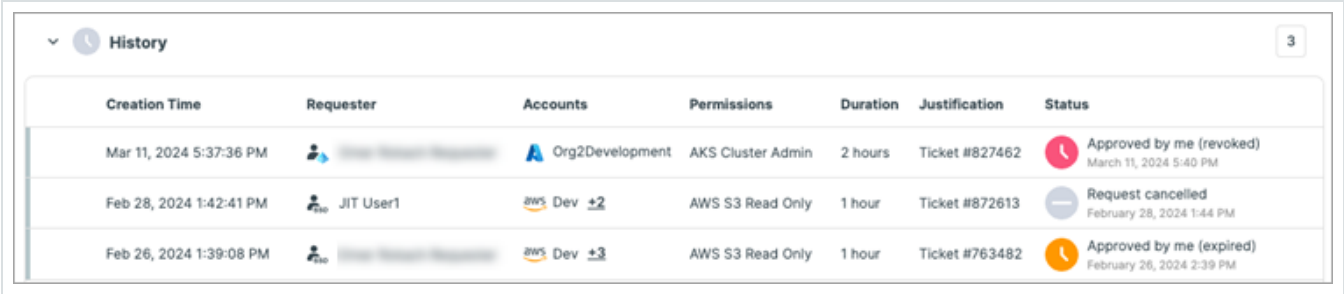


5. リクエスト **を承認** または **拒否します** 。

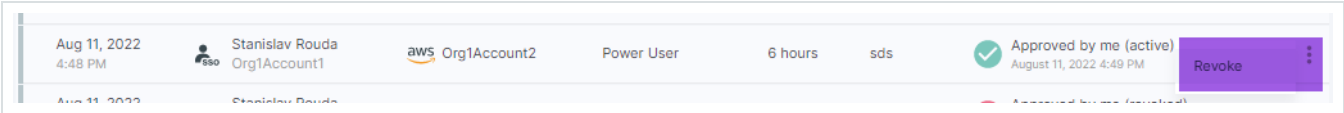
リクエストを確認した後、[履歴] セクションでリクエストの詳細をステータスとともに確認できます。

- *リクエストのキャンセル* - リクエストはリクエスタによってキャンセルされました。
- *拒否* - リクエストがアプローブによって拒否されました。
- *承認者* - リクエストは承認者によって承認されました。その期間はまだ **アクティブ**な か、の **いずれ**かです。

- *リクエストの期限切れ* - リクエストは 12 時間以内に承認者によってレビューされませんでした。



6. (オプション) 必要に応じて、承認者として指定されたリクエストのアクティブなセッションへのユーザーアクセス **を取り消す** ことができます。これにより、関連するリクエストに対するユーザーのアクセス許可が即座に削除されます。定期アクセスを取り消す場合、将来すべてのインスタンスを取り消すか、現在のインスタンス (アクティブな場合) または今後のインスタンス (保留中の場合) のみを取り消すかを選択できます。



> **注意:** 自動的に承認された (かつ明示的な承認を必要としない) リクエストを取り消すには、管理者が権限を削除する必要があります。

Slack 経由でアクセスを確認する

Slack を使用して、クラウドサイバーエクスポージャー JIT Portal にログインすることなくアクセスリクエストを確認および管理できます。

前提条件

- Slack ワークスペースを と統合するクラウドサイバーエクスポージャー
- JIT アクセス用に Slack を有効にします
- アクセスを確認または承認する資格が必要です。Slack 経由でアクセスを確認できない場合は、クラウドサイバーエクスポージャー管理者に確認してください。

クラウドサイバーエクスポージャー Slack アプリには、**[ホーム]** および **[メッセージ]** の2 つのタブがあります。

Slack の [ホーム] タブ

[ホーム] タブには、アクセス要求とアクションの概要が表示されます。

- **保留中のリクエスト**: 詳細を確認し、**[承認]** または **[拒否]** を選択します。
- **承認したアクティブなアクセス**: 必要に応じてアクセスを確認し、取り消します。

> **注意:** ホームタブが自動的に更新されません。最新の情報を表示するには、タブを閉じて再オープンしてください。

Slack の [メッセージ] タブ

[メッセージ] タブにはすべての JIT アクセス通知が一覧表示され、Slack から直接アクションを実行できます。

- **保留中のリクエスト**: リクエストの詳細を確認し、[承認] または [拒否] を選択します。
- **ご自身で承認されたアクティブなアクセス**: 必要に応じてアクセスを取り消します。
- **クローズされたリクエスト**: 取り消されたリクエストおよび期限切れのリクエストの履歴を表示します。

Teams 経由のアクセスの確認

クラウド サイバーエクスポージャー JIT Portal の埋め込みバージョンを介して、Teams で直接アクセスリクエストを確認できます。

前提条件

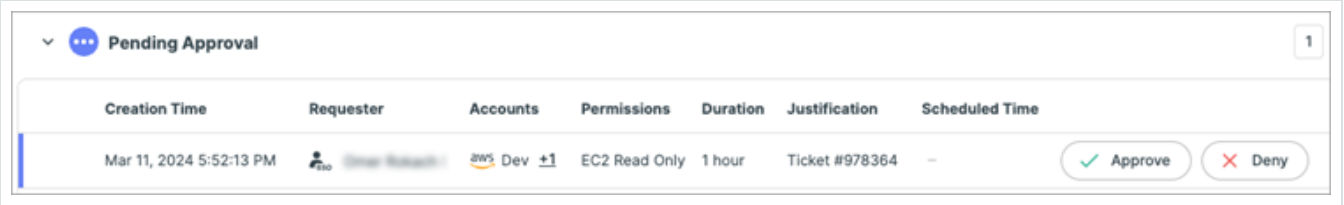
- Microsoft Teams
- JIT アクセス用に Teams を有効にする

アクセスリクエストを確認する方法

1. Microsoft Teams に移動します。
2. [レビューを見る] ページに移動します。

3. **[保留中]** セクションに移動し、リクエストを確認します。

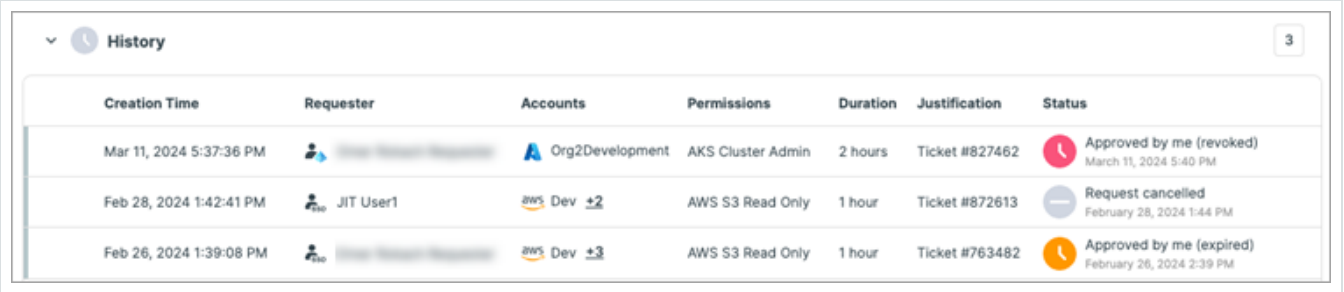
> **注意:** 上部にあるフィルターを使用して、結果を絞り込みます。



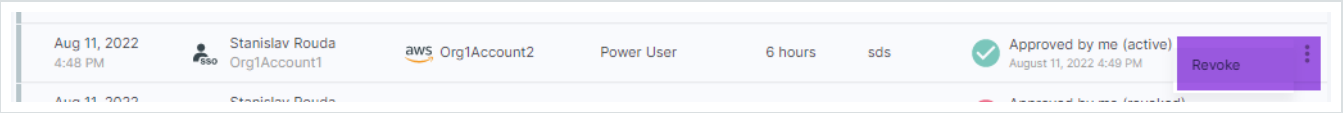
4. リクエスト **を承認** または **拒否します** 。

   リクエストを確認した後、[履歴] セクションでリクエストの詳細をステータスとともに確認できます。

   - *リクエストのキャンセル* - リクエストはリクエスタによってキャンセルされました。
   - 拒否 - リクエストがアプローブによって拒否されました。
   - 承認者 - リクエストは承認者によって承認されました。その期間はまだ **アクティブ**な か、の **いずれ**かです。
   - リクエストの期限切れ - リクエストは 12 時間以内に承認者 によってレビューされませんでした。



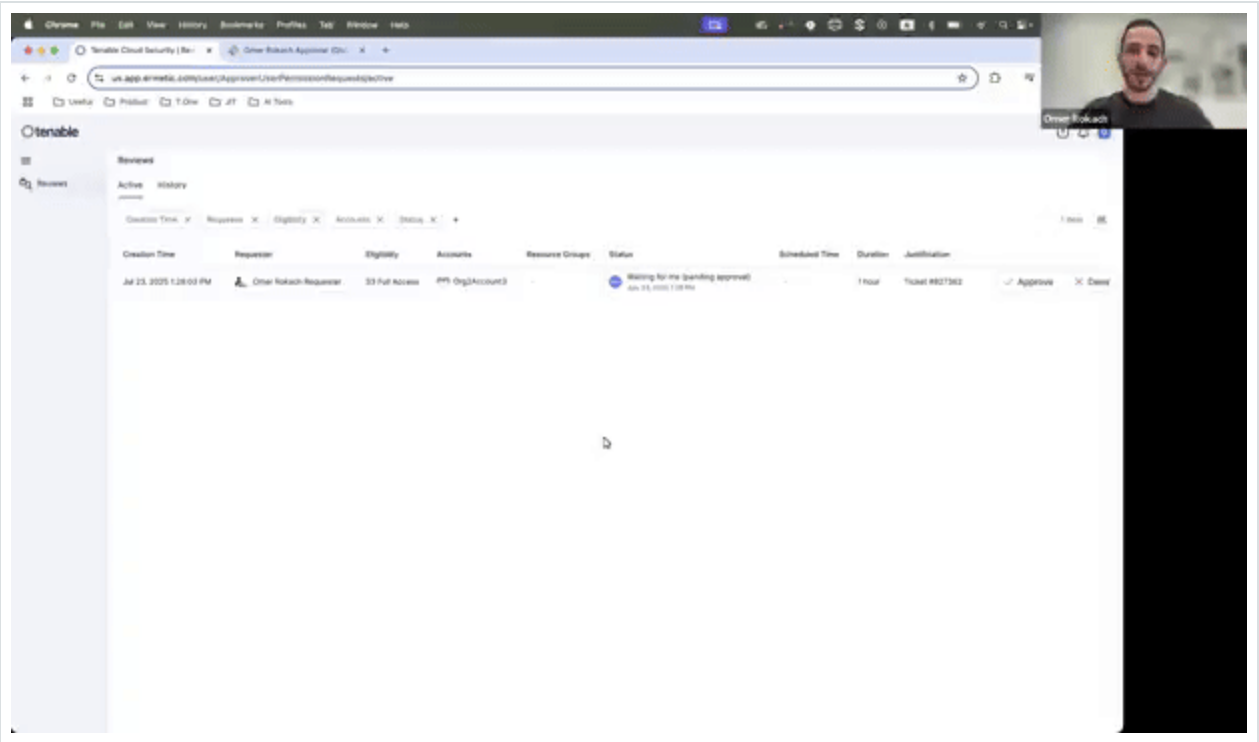
5. (オプション) 必要に応じて、承認者として指定されたリクエストのアクティブなセッションへのユーザーアクセス **を取り消す** ことができます。これにより、関連するリクエストに対するユーザーのアクセス許可が即座に削除されます。



> **注意:** 自動的に承認された (かつ明示的な承認を必要としない) リクエストを取り消すには、管理者が権限を削除する必要があります。

アクセスビデオの確認

このビデオでは、JIT アクセスリクエストを確認し、アクションを実行する方法を学習できます。



一般的な JIT のユースケース

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

このセクションでは Tenable One Cloud Exposure 、JIT Access で解決できる一般的なユースケースについて概説します。

AWS アカウントへのアクセスのリクエスト

JIT for AWS を利用して、組織へのアクセス権をユーザーに付与できます。たとえば、エンジニアリングチームに次のいずれかのアクセス許可を動的に付与する 2 つの別々の権限を作成し、組織の S3 バケットにアクセスすることができます。

- **読み取りアクセス**自動承認 (最大 24 時間)。
- **フルアクセス権**。SRE チームによる手動承認、最大 6 時間。

前提条件

- 権限を追加するには、クラウドサイバーエクスポージャーで管理者または JIT 管理者ロールが必要です。
- JIT 用のオンボード AWS。

AWS アカウントの権限を構成するには:

1. 資格の追加、特定のユースケースに合わせて必要に応じてカスタマイズします。
2. たとえば、次のことが可能です。
    1. 次のサンプル値をガイドラインとして使用し、S3 **読み取り専用** アクセスの資格情報を作成します。
        - **名前**: S3 読み取り専用
        - **説明**: この権限は、S3 バケットに読み取り専用のアクセス許可を付与します
        - **どのユーザーまたはグループがアクセスを要求できるか**: 組織の SSOの設計 グループ
        - **どのアクセス許可がリクエストできるか**: AmazonS3ReadOnlyAccess、AWS 管理コンソールを介してすべてのバケットへの読み取り専用アクセスを提供する AWS 管理ポリシー。
        - **リクエストできる最大期間は何ですか?**: 24 時間
        - **そのアクセスはどのように承認されるべきですか**: 自動的に承認
    2. 次のサンプル値をガイドラインとして使用して、S3 **フル** アクセスの資格情報を作成します。
        - **名前**: S3 フルアクセス
        - **説明**: この権限は、S3 バケットへのフルアクセス許可を付与します
        - **どのユーザーまたはグループがアクセスを要求できるか**: 組織の SSOの設計 グループ
        - **どのアクセス許可がリクエストできるか**: AmazonS3FullAccess、AWS 管理コンソールを介してすべてのバケットへのフルアクセスを提供する AWS 管理ポリシー。
        - **リクエストできる最大期間は何ですか?**: 6 時間

- **そのアクセスはどのように承認されるべきですか**明示的な承認が必要
- **承認者**: 所属組織のSRE SSOグループ

Add Eligibility

Name

S3 Read Only

Id

S3-Read-Only

Description

This eligibility grants read only permissions to S3 buckets

Organization

aws Org2Account1

Which user or group can request access?

Engineering
SSO Group | Org2Account1

Which permissions can they request?

- (•) Choose policies manually
- ( ) Choose a permission set

AmazonS3ReadOnlyAccess
IAM Managed Policy | AWS

- [ ] Include an inline policy (JSON)

Which accounts can they access?

Azure アカウントへのアクセスをリクエストする

JIT for Azure を利用して、所属組織へのアクセス権をユーザーに付与できます。たとえば、2 つの別々の権限を作成し、エンジニアリングチームに次のいずれかのアクセス許可を動的に付与し、組織のブロブデータにアクセスすることができます。

- **読み取りアクセス**自動承認 (最大 24 時間)。
- **フルアクセス権**。最大 6 時間の SRE チームによる手動承認。

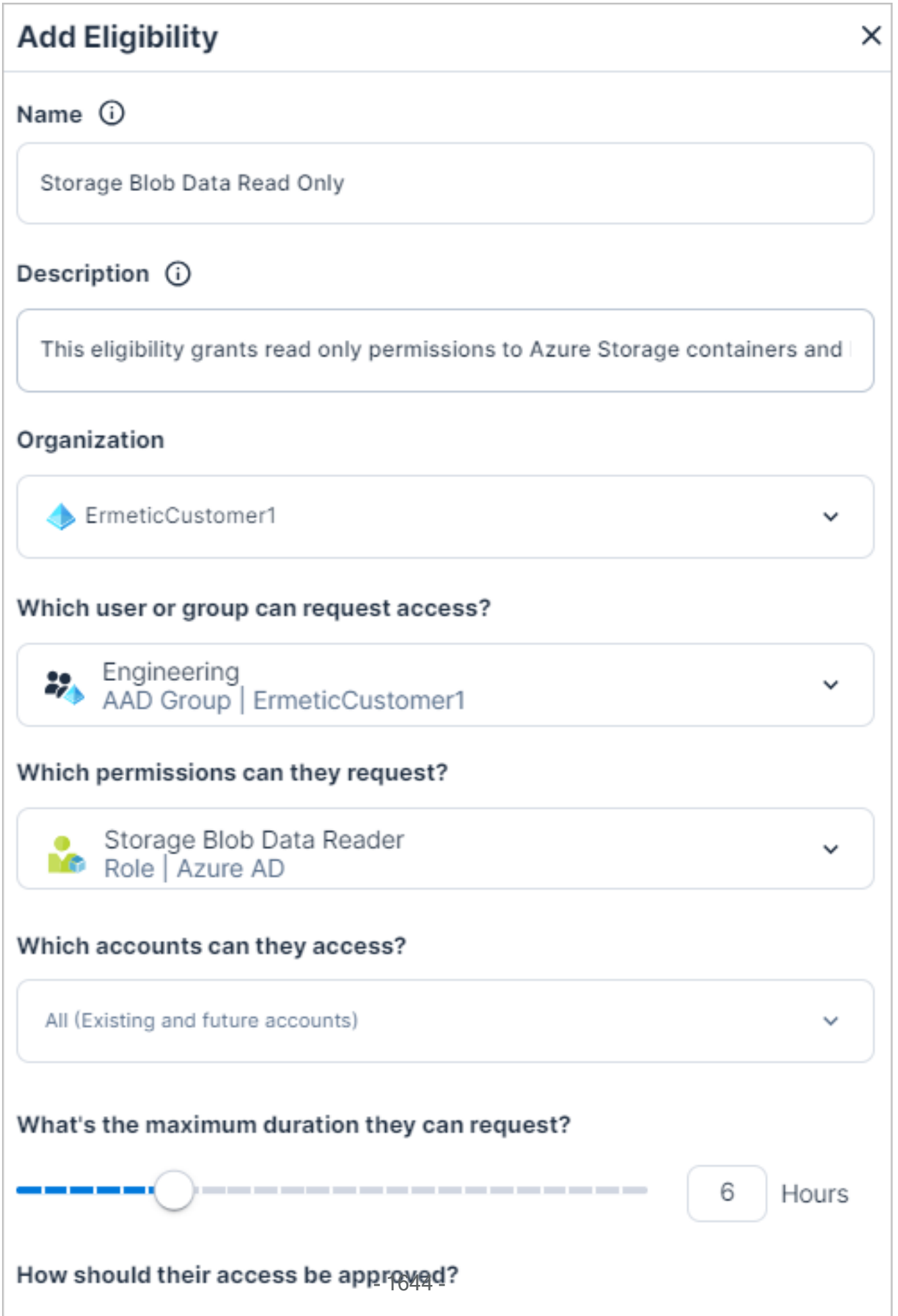
前提条件

- 権限を追加するには、クラウドサイバーエクスポージャーで管理者または JIT 管理者ロールが必要です。
- JIT 用のオンボード Azure

Azure アカウントの権限を設定するには

1. 資格の追加、特定のユースケースに合わせて必要に応じてカスタマイズします。
2. たとえば、次のことが可能です。
    1. 次のサンプル値をガイドラインとして使用し、blob データの **読み取り専用** アクセスの資格情報を作成します。
        - **名前**: ストレージ Blob データの読み取り専用
        - **説明**この権限は、Azure ストレージのコンテナおよび blob に対する読み取り専用のアクセス許可を付与します
        - ***どのユーザーまたはグループがアクセスを要求できるか***: 組織の SSOの設計 グループ
        - ***どのアクセス許可がリクエストできるか***ストレージ Blob データリーダー: ユーザーが Azure Storage コンテナと blob を読み取ってリストできるようにする Azure ビルトインロール。
        - **リクエストできる最大期間は何ですか?**: 24 時間
        - ***そのアクセスはどのように承認されるべきですか***: 自動的に承認
    2. 次のサンプル値をガイドラインとして使用し、ブロブデータの **フル** アクセスの資格情報を作成します。

- **名前**: ストレージブロブデータのフルアクセス
- **説明**: この権限により、Azure Storage のコンテナと blob へのフルアクセス許可が付与されます
- **どのユーザーまたはグループがアクセスを要求できるか**: 組織の Engineering SSO グループ
- **どのアクセス許可がリクエストできるか**ストレージ Blob データの所有者。Azure Storage Blob コンテナおよびデータへのフルアクセスを提供する Azure ビルトインロールです。
- **リクエストできる最大期間は何ですか?**: 6 時間
- **そのアクセスはどのように承認されるべきですか**明示的な承認が必要
- **承認者**: 所属組織の SRE SSO グループ


Add Eligibility
Name
Storage Blob Data Read Only
Description
This eligibility grants read only permissions to Azure Storage containers and
Organization
ErmeticCustomer1
Which user or group can request access?
Engineering
AAD Group | ErmeticCustomer1
Which permissions can they request?
Storage Blob Data Reader
Role | Azure AD
Which accounts can they access?
All (Existing and future accounts)
What's the maximum duration they can request?
6
Hours
How should their access be approved?

GCP アカウントへのアクセスをリクエストする

JIT for GCP を利用して、ユーザーに組織へのアクセスを付与できます。たとえば、2 つの別々の権限を作成し、エンジニアリングチームに次のいずれかのアクセス許可を動的に付与し、組織のブロブデータにアクセスすることができます。

- **読み取りアクセス**自動承認、最大 24 時間。
- **フルアクセス権**。最大 6 時間の SRE チームによる手動承認。

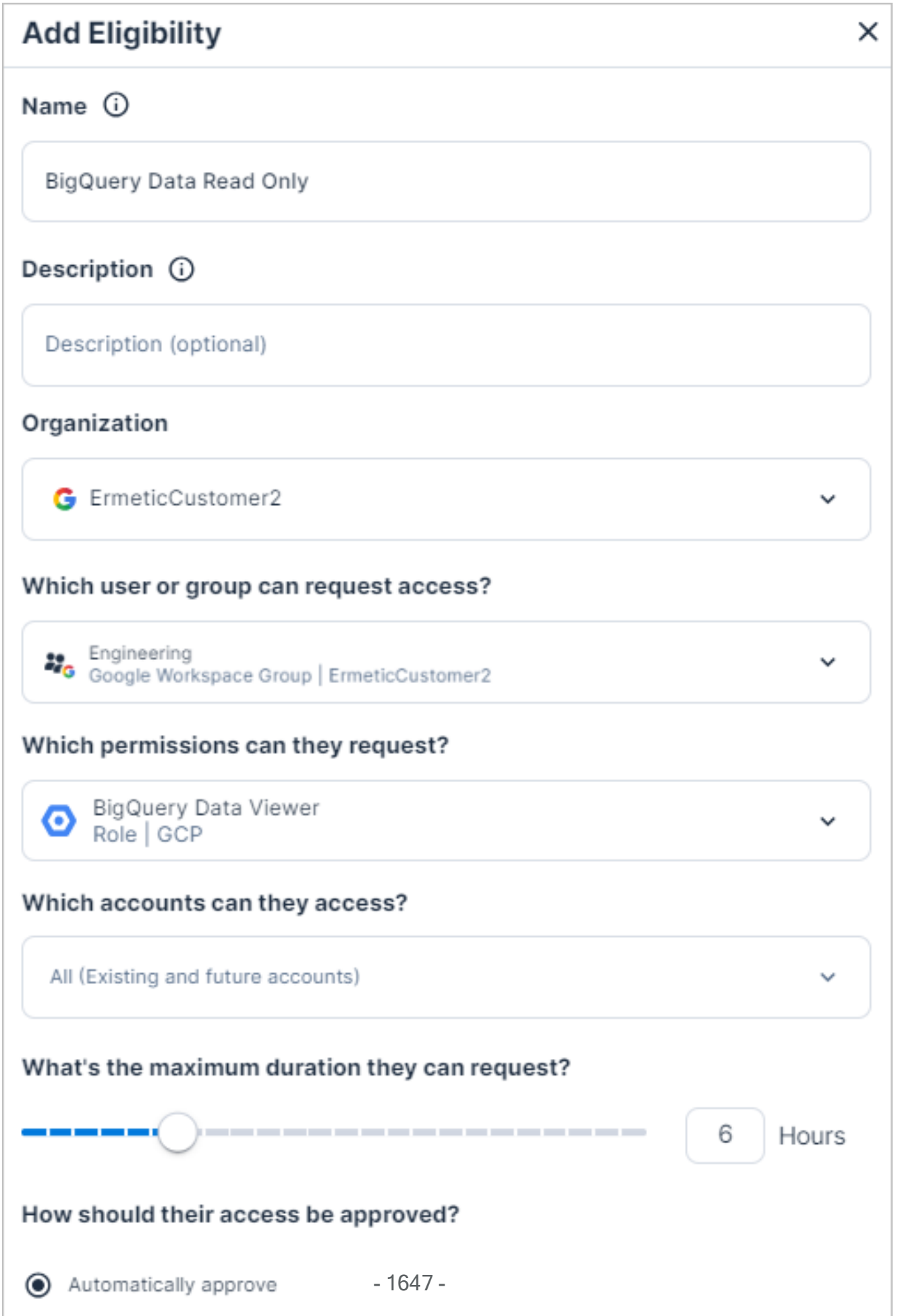
前提条件

- 権限を追加するには、クラウドサイバーエクスポージャーで管理者または JIT 管理者ロールが必要です。
- JIT向けのオンボードGCP。

GCP アカウントの権限を設定するには

1. 資格の追加、特定のユースケースに合わせて必要に応じてカスタマイズします。
2. たとえば、次のことが可能です。
    1. 次のサンプル値をガイドラインとして使用し、BigQuery データの **読み取り専用** アクセスの資格情報を作成します。
        - **名前**: BigQuery データの読み取り専用
        - **説明**: この権限は、BigQuery データに対する読み取り専用のアクセス許可を付与します。
        - ***どのユーザーまたはグループがアクセスを要求できるか***: 組織の SSOの設計 グループ
        - ***どのアクセス許可がリクエストできるか***GCP の事前定義されたロールである BigQuery データビューア。
        - **リクエストできる最大期間は何ですか?**: 24 時間
        - ***そのアクセスはどのように承認されるべきですか***: 自動的に承認
    2. 次のサンプル値をガイドラインとして使用し、BigQuery データに**フル**アクセスできる資格情報を作成します。

- **名前**: BigQuery データ所有者
- **説明**: この資格は、BigQuery データへの完全なアクセス許可を付与します。
- **どのユーザーまたはグループがアクセスを要求できるか**: 組織の SSOの設計 グループ
- **どのアクセス許可がリクエストできるか**BigQuery Data 所有者。GCP で事前定義されたロールであり、ユーザーは BigQuery テーブル/ビューを読み、共有、削除できます。
- **リクエストできる最大期間は何ですか?**: 6 時間
- **そのアクセスはどのように承認されるべきですか**明示的な承認が必要
- **承認者**: 所属組織の SRE SSO グループ


Add Eligibility
Name
BigQuery Data Read Only
Description
Description (optional)
Organization
ErmeticCustomer2
Which user or group can request access?
Engineering
Google Workspace Group | ErmeticCustomer2
Which permissions can they request?
BigQuery Data Viewer
Role | GCP
Which accounts can they access?
All (Existing and future accounts)
What's the maximum duration they can request?
6
Hours
How should their access be approved?
Automatically approve

SaaS アプリケーションへのアクセスのリクエスト

JIT を利用して、ユーザーに IdP グループ経由で SaaS アプリケーションへのアクセスを許可できます。たとえば、Okta グループを使用して、グループを Salesforce.com アプリに割り当てることで、Salesforce へのアクセスを許可できます。Salesforce へのアクセス権が必要なユーザーは、Okta グループへの参加をアクセスをリクエストする できます。これにより、Salesforce へのアクセス権が付与されます。

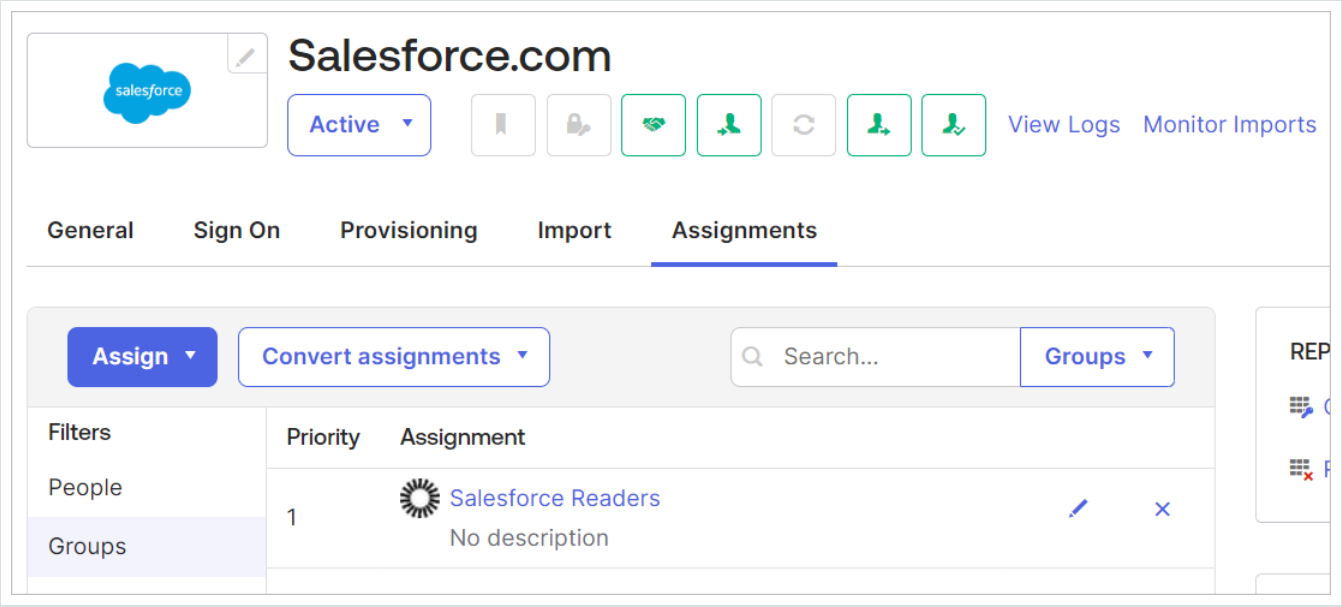
> **注意:** 次の手順は Okta の使用資格を構成する方法を示していますが、他の IdP に対しても同様の手順を実行できます。

前提条件

- 権限を追加するには、クラウドサイバーエクスポージャー で管理者または JIT 管理者ロールが必要です。
- JIT 用の Onboard Okta。

SaaS アカウントの権限を設定するには

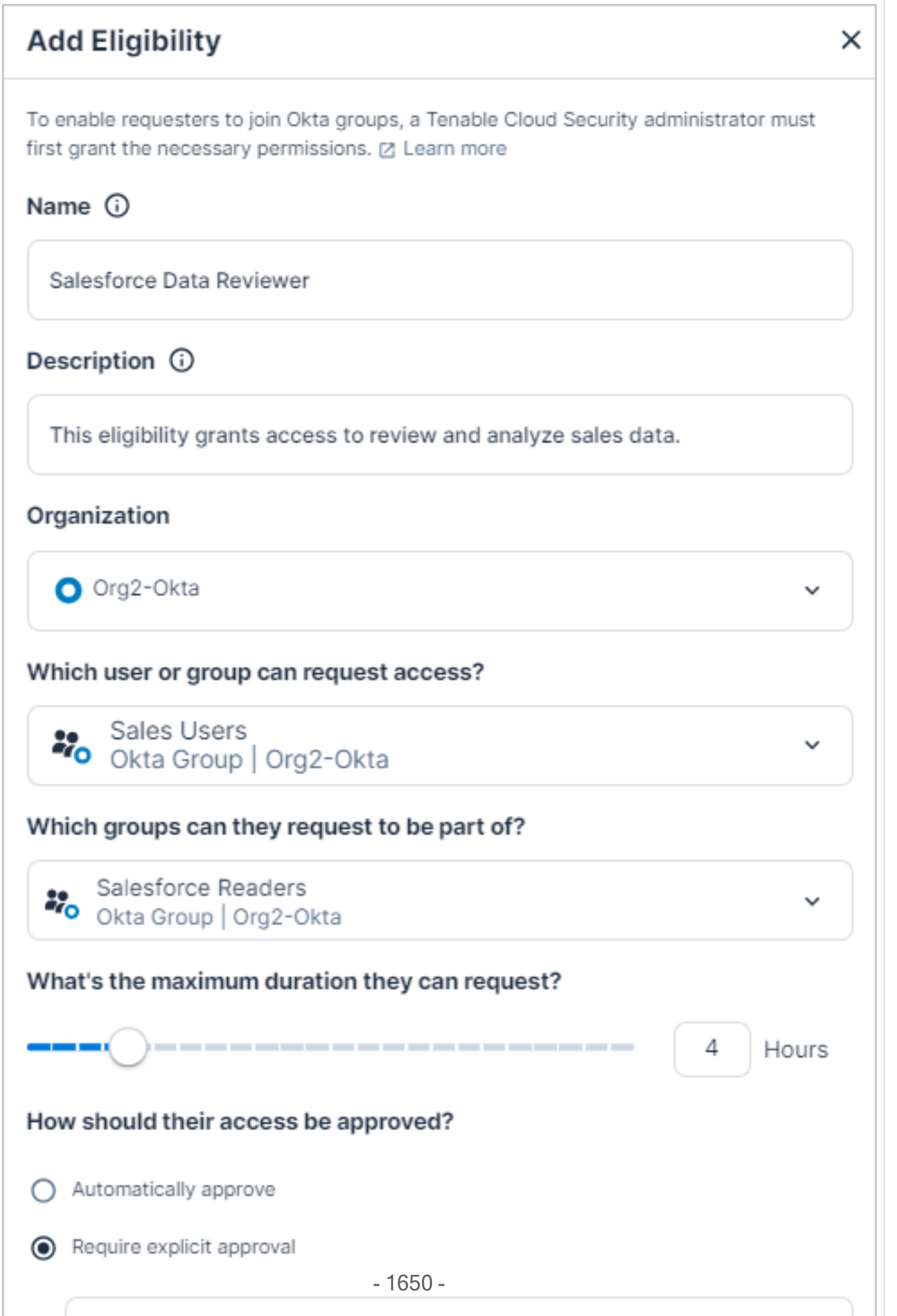
1. Okta 管理コンソールで、Salesforce.com アプリケーションへのグループアクセスを割り当てます。



2. 資格の追加、特定のユースケースに合わせて必要に応じてカスタマイズします。たとえば、次のサンプル値をガイドラインとして使用し、Okta グループ (Salesforce.com アプリに割り当てられている) へ

のアクセス権を作成できます。

- **名前**: Salesforce データレビューア
- **説明**: この資格は、販売データを確認および分析するためのアクセス権を付与します。
- **どのユーザーまたはグループがアクセスを要求できるか**: 組織の営業担当者のSSO グループ。
- **リクエストできるグループはどれですか?** Salesforce Reader
- **リクエストできる最大期間は何ですか?**: 4 時間
- **そのアクセスはどのように承認されるべきですか**オクタ セールスディレクター グループのメンバーによる明示的な承認が必要です。


Add Eligibility
To enable requesters to join Okta groups, a Tenable Cloud Security administrator must first grant the necessary permissions. Learn more
Name
Salesforce Data Reviewer
Description
This eligibility grants access to review and analyze sales data.
Organization
Org2-Okta
Which user or group can request access?
Sales Users
Okta Group | Org2-Okta
Which groups can they request to be part of?
Salesforce Readers
Okta Group | Org2-Okta
What's the maximum duration they can request?
4
Hours
How should their access be approved?
Automatically approve
Require explicit approval



EKS クラスターへのアクセスのリクエスト

AWS アクセスエントリと IdP グループを利用して、IAM ユーザーに EKS クラスターへの JIT アクセスを付与することで、このようなクラスターへのユーザーアクセスの付与に存在する一般的な問題を解決できます。アクセスエントリを作成すると、クラスタ外から IAM ユーザーの Kubernetes アクセス許可を管理できるようになります。アクセスエントリの詳細については、関連する AWS ドキュメント を参照してください。

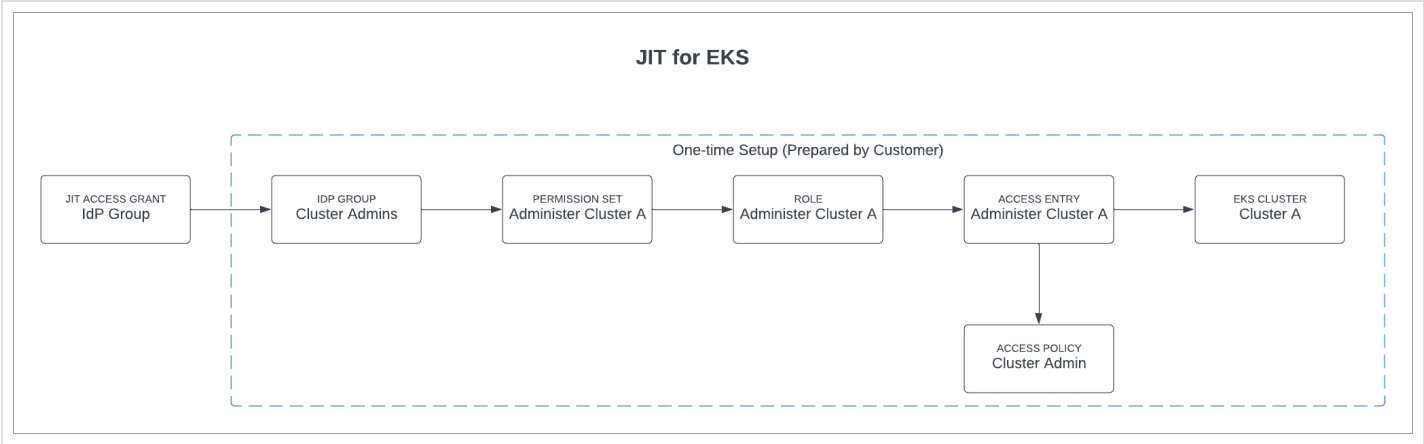
ユーザーがアクセス権をリクエストできるようにするには

1. (AWS) 指定された IdP グループを介して EKS クラスターアクセスを許可するための AWS IAM を設定する (クラスターごとに 1 回限りのセットアップ)。
2. (JIT) JIT 資格情報を追加します (管理者または JIT 管理者ロールが必要です)。
    - 設定時に使用される IdP グループを含む IdP アカウントの範囲内に権限を追加します。
    - IdP グループをリクエスタとして設定します。
3. (JIT) IdP グループへの アクセスをリクエストする 。承認されると、リクエスタには関連する EKS クラスターで Kubernetes のアクセス許可が与えられます。

EKS クラスターアクセスを許可するための AWS IAM を設定する

一般的には、JIT ユーザーに EKS クラスターへのアクセスを許可するには、次の手順に従います (手順の詳細手順)。

- IAM アイデンティティ・センター で空のアクセス許可セットを作成します。
- IdP グループと新しいアクセス許可セットをクラスターのアカウントに割り当てます。
- Elastic Kubernetes Service にアクセスエントリを作成し、アイデンティティをアクセスポリシーにマッピングできるようにします (事前定義された AWS が管理する Kubernetes アクセス許可)。



前提条件

- **アイデンティティプロバイダーIdP**。
  - と統合され クラウドサイバーエクスポージャー 、JIT 向けにオンボードされたIdP。
  - 関連する EKS クラスターで選択されたアクセス許可がユーザーに付与される IdP グループ。このグループは、IAM Identity Center で利用できる必要があります。
- **EKSクラスター**
  - Kubernetesバージョン1.23以降
  - 最新の EKS プラットフォームバージョン (Kubernetes のバージョンによって異なります)。

  サポートされているバージョンの完全なリストを含む、クラスタの前提条件の詳細については、AWS の関連ドキュメントを参照してください。

EKS クラスターアクセスを許可する AWS IAM を設定する方法

1. **空のアクセス許可セットを作成します。**
    1. AWS コンソールにログインします。
    2. **IAM アイデンティティ・センター**に移動します。
    3. **[アクセス許可セット]** をクリックし、**[アクセス許可セットを作成]** をクリックします。
    4. タイプとして、**[カスタム] アクセス許可セット**を選択し、**[次へ]** をクリックします。
    5. [ポリシーとアクセス許可の境界] ページで、**[次へ]** をクリックします。

        > **注意:** 権限セットは空である必要があります。ポリシーを選択する必要はありません。

    6. [アクセス許可セットの詳細] で、**アクセス許可セット名**を入力します。
    7. **[次へ]** をクリックし、アクセス許可設定を確認して **[作成]** をクリックします。
2. **IdP グループと許可セットをクラスタのアカウントに割り当てます:**
    1. **[複数アカウントの権限] > [AWSアカウント]** に移動します。
    2. アクセス許可を付与するクラスターを含むアカウントを選択し、**[ユーザーまたはグループを割り当てる]** をクリックします。
    3. [グループ] で、関連する IdP グループを選択し、**[次へ]** をクリックします。詳細については上記の前提条件を参照してください。
    4. [アクセス許可セット] で、前に作成したアクセス許可セットを選択し、**[次へ]** をクリックします。
    5. 割り当てを確認し、**[送信]** をクリックします。

        > **注意:** この割り当てを作成すると、「AWSReservedSSO_」の先頭で新しいロールが自動的に作成されます。この手順の後のステップで、このロールを使用する必要があります。

3. **クラスタのアクセスエントリを作成します:**
    1. AWS コンソールで、**Elastic Kubernetes Service** (EKS) に移動します。
    2. 対象のクラスタをクリックします。
    3. **[アクセス]** タブをクリックし、[IAM アクセスエントリ] で **[アクセスエントリの作成]** をクリックします。
    4. [IAM プリンシパル] で、先に自動作成されたロールを選択します。このロールは、以下の先頭で始まります。`AWSReservedSSO_`

5. [アクセスポリシー] で以下を行います。
    - 選択したクラスターに付与する必要な Kubernetes アクセス許可を含む **ポリシー名** を選択します。
    - これらのアクセス許可の **アクセス範囲が** クラスター全体であるか、名前空間レベルであるかを選択します。
    - **[ポリシーの追加]** をクリックして、必要に応じてポリシーを追加します。
6. **[次へ]** をクリックし、アクセスエントリを確認して **[作成]** をクリックします。

よくある質問 JIT

> **注意:** この機能は、**Cloud Vulnerability Management** ライセンスでは使用できません。

以下は、Tenable One Cloud Exposure 内の JIT に関連するよくある質問です。

AWS アクセス割り当て

> クラウドサイバーエクスポージャー はどのようにして AWS JIT リクエストのアクセスを付与および取り消しますか?

回答: AWS では、クラウドサイバーエクスポージャー がAWS IAM Identity Center を使用してアクセス権を付与します。ユーザーが JIT 経由でアクセスをリクエストするとき、Tenable

1. 資格情報で定義されたポリシー (アクセス許可) を含む **アクセス許可セット** を作成します。
2. 選択したアカウントのリクエストユーザーにアクセス許可セットを割り当てます。

リクエストが期限切れになるか取り消されると、Tenable はアクセス許可セットとアカウント割り当ての両方を自動的に削除し、ユーザーのアクセスを完全に取り消します。

Azure アクセス割り当て

> クラウドサイバーエクスポージャー はどのようにして Azure JIT リクエスト へのアクセスを許可および取り消しますか?

回答: Azure では、ユーザー (ID)、ロール (ビューアーなど)、ターゲットリソース (サブスクリプションやリソースグループなど) を接続するロール割り当てを使用してアクセスが許可されます。

ユーザーが JIT 経由でアクセスをリクエストするとき、クラウドサイバーエクスポージャー はターゲットとロールの組み合わせごとに **個別のロール割り当て** を作成します。たとえば、権限が 10 のサブスクリプションで 5 つのロールを付与する場合、50 のロールが割り当てられます。

アクセスリクエストの有効期限が切れた、または取り消された場合、Tenable は作成したロール割り当てを削除します。これは想定された動作であり、リクエストが終了したときにアクセスが完全に取り消されるようになります。

定期的なアクセスリクエスト

> 継続的なアクセスリクエストは無効にできますか?

回答: はい。継続的なアクセスはすべての 資格の追加 でデフォルトで有効になっていますが、任意の権限で無効にできます。これにより、自動再付与なしで、リクエスト者は毎回新しいアクセスリクエストを送信する必要があります。

定期アクセスを無効にする方法

1. クラウドサイバーエクスポージャー JIT Portal で、**[応募資格]** に移動します。
2. 資格情報を見つけて、**[編集]** をクリックします。
3. **[定期的なアクセス]** で、**[無効]** を選択します。
4. **[保存]** をクリックします。

> 継続的なリクエストが送信できる直近のリクエストの詳細を制限できますか?

はい。デフォルトでは、継続的なリクエストは開始日から最大 **1 年 (365 日)** です。

有効性を作成する場合、**[最大継続日数]** の値を定義して、ユーザーが継続アクセスをスケジュールできるようになるまでの **日数 (1 ~ 364 日** の任意の値) を制限できます。

たとえば、制限が 60 日に設定されており、ユーザーが 7 月 1 日からアクセスをリクエストする場合、8 月 30 日までしか継続的なアクセスをスケジュールできません。

Azure 所有者ロール

> クラウド サイバーエクスポージャー は、Azure JIT で所有者ロールの割り当てをどのように処理しますか?

回答: Azure では、すべてのサブスクリプションに常に、少なくとも 1 つのアクティブな所有者ロールが割り当てられている必要があります。

JIT アクセス要求が、サブスクリプションにおけるアクティブな所有者の割り当てのみである場合、スケジュールされた期間が終了した場合でも、その割り当ては期限切れになったり、取り消されたりすることはできません。別の所有者が割り当てられるまで、アクティブなままになります。

> 例を参照

3 人のユーザー (A、B、C) は、3 時間にわたり所有者ロールに割り当てられる資格情報です。必要な承認はありません。各ユーザーが所有者ロールに割り当てられるタイミングと権限が期限切れになるタイミングの内訳を示します

時間	アクション	所有者
8:00	ユーザー A は所有者ロールに割り当てられています。	権限昇格
9:00	ユーザー B は、所有者ロールに割り当てられています。	A、B

時間	アクション	所有者
11:00	ユーザー A のアクセス許可が期限切れになりました。	B
12:00	ユーザー B のアクセス許可は期限切れになりません。その他の所有者なし	B
13:00	ユーザー C は、所有者ロールに割り当てられています。ユーザー B のアクセス許可が期限切れになります。	C

では
、**これが原因で**、Azure はサブスクリプションが孤立-アクセスを管理できる者なしで放置されるのを防ぐことができます。これを防ぐため、アクションがグローバル管理者によって実行されない限り、サブスクリプションレベルで最後の所有者またはユーザーアクセス管理者ロール割り当ては削除されません。

の回避策

- テナントで **[グローバル管理者]**(https://learn.microsoft.com/ja-jp/azure/role-based-access-control/rbac-and-directory-admin-roles#microsoft-entra-roles){target="_blank"} ロールを割り当てます Tenable 。これにより、クラウドサイバーエクスポージャー は最後の Owner 割り当てを削除できます。
- または、**すべてのサブスクリプションで**Tenable 所有者ロールを割り当てます。これにより、クラウドサイバーエクスポージャー が最後の所有者になることがなくなり、他の JIT 付与の所有者ロールを想定通りに取り消すことができます。

ベストプラクティス
JIT を通じて付与された所有者権限を確実に有効期限切れにできるように、各サブスクリプションで恒久的な所有者ロール (JIT 外部) を割り当てることを推奨します。

大規模環境で Jit Access を管理する

> 多数のアカウントやユーザーの JIT 特権をどのように管理すべきですか?

回答: 多数のアカウント (および Azure のリソースグループ) とアクセス許可やロールがある大規模な環境では、アカウントとロールのセットを含む広範な資格情報を作成できます。そうすることで、リクエスタがリクエストごとに選択できる数を制限できます。

たとえば、50 個のアカウントで権限を作成すると、各リクエスト者はリクエストごとに 3 つのみ選択できます。

Azure と GCP では、リクエスタはアクセスが必要な特定のロールのみを選択できます。

このアプローチにより、環境全体で最小限の権限を確保しながら、維持する必要がある権限の数を減らすことができます。

JIT Source IPs (JIT ソース IP)

> どの IP アドレスから JIT トラフィックが発生するのですか?

回答: eu-central-1 (ヨーロッパ) 地域のテナントの場合、JIT トラフィックは次の静的 IP アドレスから発生します。

- `18.192.163.94`
- `3.67.105.194`