Tenable Nessus 10.5.x ユーザーガイド

最終更新日: 11月 27, 2025

Copyright © 2025 Tenable, Inc.All rights reserved.Tenable、Tenable Nessus、Tenable Lumin、Assure、および Tenable のロゴは、Tenable, Inc.またはその関連会社の登録商標です。その他の各製品またはサービスは、それぞれの所有者の商標です。

目次

Tenable Nessus 10.5.x にようこそ 19

システム要件 22

ハードウェア要件 23

Tenable Nessus スキャナーと Tenable Nessus Professional 23

Tenable Nessus Manager 24

ストレージ要件 25

NIC 要件 25

仮想マシン 26

ソフトウェア要件 26

対応ブラウザ 33

PDF レポート 33

SELinux の要件 33

SELinux の強制モードポリシーのカスタマイズ 34

ライセンス要件 35

ポートの要件 37

Tenable Nessus 37

Tenable Nessus Agent 38

デプロイメントに関する考慮事項 38

ホストベースのファイヤーウォール 39

IPv6 のサポート 40

ネットワークアドレス変換 (NAT) の制限 40

ウイルス対策ソフトウェア 40

セキュリティ警告 41

Tenable Nessus を使い始める 42
準備 42
Tenable Nessus をインストールして設定する 42
スキャンを作成して設定する 42
スキャン結果を表示して分析する 43
Tenable Nessus 設定を調整する 43
Tenable Nessus のナビゲーション 43
Tenable Nessus のインストール 44
をダウンロードするTenable Nessus 44
Tenable Nessus のインストール 45
Linux での Tenable Nessus のインストール 45
Windows での Tenable Nessus のインストール 46
Nessus パッケージファイルをダウンロードする 47
Tenable Nessus のインストールを開始する 47
Windows InstallShield ウィザードを完了する 47
macOS での Tenable Nessus のインストール 48
Raspberry Pi での Tenable Nessus のインストール 51
Docker イメージとして Tenable Nessus をデプロイする 51
演算子 53
環境変数 53
Tenable Agents のインストール 57
Tenable Nessus リンクキーの取得 57
Tenable Nessus Manager にエージェントをリンクする 58
Tenable Nessus の設定 60

Tenable Nessus Essentials、Professional、Expert、Manager をインストールする 62
Tenable Nessus Professional または Tenable Nessus Expert の試用版をアクティブにする 65
Tenable Vulnerability Management にリンクする 67
Tenable Nessus Manager にリンクする 72
Tenable Security Center にリンクする 73
アクティベーションコードを管理する 75
Tenable Nessus のライセンシング 75
Tenable Nessus アクティベーションコード 75
Tenable Nessus を Tenable Vulnerability Managementで管理する 76
Tenable Nessus を Tenable Security Centerで管理する 76
アクティベーションコードを表示する 77
アクティベーションコードを更新する 78
アクティベーションコードを転送する 79
Nessus ユーザーインターフェース 79
コマンドラインインターフェース 80
Tenable Nessus プラグインとソフトウェアの更新 81
Tenable Nessus をオフラインで管理する 84
Tenable Nessus をオフラインでインストールする 84
Tenable Nessus のインストール 85
ライセンスを生成する 85
最新のプラグインをダウンロードしてコピーする 86
ライセンステキストのコピーと貼り付け 87
ライセンスをオフラインで更新する 87
プラグインをオフラインで更新する 92

Update Tenable Nessus Manager Plugins on an Offline System 94
監査ウェアハウスを手動で更新する 95
Tenable Nessus と Tenable Agents のアップグレード 96
Nessus をアップグレードする 97
評価版からのアップグレード 97
Tenable Nessus ソフトウェアを更新する 98
Linux で Nessus をアップグレードする 101
Windows で Nessus をアップグレードする 102
macOS で Nessus をアップグレードする 103
Tenable Agent のアップデート 103
Tenable Nessus ソフトウェアのダウングレード 104
Tenable Nessus のバックアップ 106
Tenable Nessus の復元 108
Nessus を削除する 109
Linux での Nessus のアンインストール 110
Windows での Tenable Nessus のアンインストール 111
macOS での Nessus のアンインストール 112
Docker コンテナとして Tenable Nessus を削除する 113
Scan (スキャン) 115
スキャンを作成して管理する 116
スキャンテンプレート 116
スキャナーテンプレート 117
エージェントテンプレート (Tenable Nessus Manager のみ) 123
スキャンポリシー 126

スキャン設定とポリシー設定 129
スキャンの Basic 設定 130
一般 131
スケジュール 133
通知 135
アクセス許可 136
ターゲットのスキャン 136
ポリシーの基本設定 139
一般 140
アクセス許可 140
検出スキャン設定 140
Host Discovery (ホスト検出) 141
ポートスキャン 144
サービス検出 149
ID 151
設定済みのディスカバリースキャン設定 152
アセスメントスキャン設定 177
一般 177
総当たり 179
SCADA 182
ウェブアプリケーション 183
Windows 190
マルウェア 191
データベース 194

設定済みのアセスメントスキャン設定 195
レポートスキャン設定 207
詳細なスキャン設定 209
設定済みの詳細なスキャン設定 218
認証情報 226
クラウドサービスの認証情報 227
データベース認証情報 231
Cassandra 231
Delinea Secret Server 自動検出 232
DB2 233
MongoDB 234
MySQL 235
Oracle 236
PostgreSQL 237
SQL Server 238
Sybase ASE 238
データベース認証情報の認証タイプ 239
Client Certificate (クライアント証明書) 239
Password (パスワード) 240
インポート 241
BeyondTrust 242
CyberArk 243
CyberArk (レガシー) 245
Delinea 249

Delinea 自動検出 249
HashiCorp Vault 251
Lieberman 254
QiAnXin 257
Senhasegura 259
ホスト認証情報 260
SNMPv3 260
SSH 261
Windows 303
認証方法 306
その他の認証情報 339
モバイル認証情報 348
パッチ管理の認証情報 355
プレーンテキスト認証の認証情報 364
HTTP 365
NNTP 367
FTP 367
POP2 367
POP3 368
IMAP 368
IPMI 368
telnet/rsh/rexec 369
SNMPv1/v2c 369
コンプライアンス 369

カスタム監査ファイルのアップロード 373
SCAP 設定 376
プラグイン 378
ダイナミックプラグインを設定する 382
スキャンの作成 383
ホスト検出スキャンを作成する 384
Bit Discovery でアタックサーフェス検出スキャンを作成する 386
エージェントスキャンを作成する 387
スキャンのインポート 388
スキャン設定を変更する 389
vSphere スキャンの設定 390
VMware の認証情報を使用したチェックについて 390
シナリオ 1: vCenter が管理しない ESXi/vSphere スキャン 391
シナリオ 2: vCenter が管理する ESXi/vSphere スキャン 391
シナリオ 3: 仮想マシンのスキャン 393
VMware vCenter サポートマトリクス 393
スキャンのメール通知を設定する 393
監査証跡を設定する 395
スキャンの起動 395
スキャンの一時停止または再開 396
実行中のスキャンの停止 397
スキャンを削除する 398
フォルダーのスキャン 398
スキャン結果 402

Severity (深刻度) 405
CVSS スコアとVPR 406
CVSS 406
CVSS ベースの深刻度 406
CVSS ベースのリスク要因 407
VPR (脆弱性優先度格付け) 407
VPR 主な要因 408
デフォルトの深刻度ベースの設定 409
個別のスキャンの深刻度ベースの設定 411
スキャン結果から新しいスキャンを作成する 412
結果の検索とフィルタリング 413
スキャン結果を比較する 423
Dashboard (ダッシュボード) 424
スキャンサマリーの表示 426
脆弱性 427
ライブ結果 434
ライブ結果を有効または無効にする 435
ライブ結果を削除する 436
スキャンのエクスポートとレポート 436
スキャンをエクスポートする 438
スキャンレポートを作成する 439
カスタマイズされたレポート 441
プラグイン 445
プラグイン情報の例 445

Tenable Nessus プラグインの入手方法 446
Tenable Nessus プラグインの更新方法 446
制限付きプラグインポリシーの作成 447
プラグインを手動でインストールする 451
プラグインルール 452
エラーメッセージ 455
センサー (Tenable Nessus Manager) 471
Agents (エージェント) 471
エージェントグループ 472
エージェントの更新 472
フリーズ期間 472
エージェントのクラスタリング 472
Tenable Agents のインストール 472
Tenable Nessus リンクキーの取得 473
Tenable Nessus Manager にエージェントをリンクする 474
エージェント設定の変更 476
グローバルエージェント設定 477
リモートエージェント設定 478
エージェントの更新 486
エージェントのフィルタリング 489
エージェントのエクスポート 491
リンクされたエージェントログをダウンロードする 492
エージェントを再起動する 494
エージェントのリンク解除 495

エージェントの削除 496
Agent Groups (エージェントグループ) 497
フリーズ期間 502
クラスタリング 507
クラスタリングのシステム要件 509
親ノード (クラスタリングが有効になっている Tenable Nessus Manager) 509
子ノード (Tenable Nessus Manager 親ノードによって管理される Tenable Nessus スキャナー) 510
エージェント 510
クラスタリングを有効にします 510
エージェントをクラスタに移行する 511
エージェントをクラスタにリンクする 513
クラスタのアップグレード 515
ノードを管理する 516
ノードからリンクキーを取得してください。 516
ノードをリンクする 517
ノードを表示または編集する 519
ノードを有効または無効にする 522
ノードのバランスを再調整する 522
ノードを削除する 524
クラスタグループ 525
スキャナー 532
Nessus スキャナーをリンクする 533
Nessus スキャナーのリンクを解除する 534
スキャナーを有効または無効にする 535

スキャナーを削除する ... 536
管理対象スキャナーログをダウンロードする ... 537
設定 ... 539
バージョン情報 ... 539
ログをダウンロードする ... 542
暗号化パスワードの設定 ... 543
Tenable Nessus システムイベントの表示 ... 544
詳細設定 ... 545
ユーザーインターフェース ... 546
Scan (スキャン) ... 549
ログ ... 556
パフォーマンス ... 568
セキュリティ ... 577
エージェントとスキャナー ... 580
クラスタ ... 586
その他 ... 587
Custom (カスタム) ... 597
スキャンエンジン設定 ... 601
Tenable Nessus スキャナー設定 ... 602
最大ホスト数の設定 ... 603
最大同時 TCP セッションの設定 ... 604
最大チェック数の設定 ... 604
Tenable Vulnerability Management および Tenable Security Center のポリシー設定 ... 604
LDAP サーバー (Tenable Nessus Manager) ... 605

プロキシサーバー 608
リモートリンク 610
SMTP サーバー 613
カスタム CA 615
アップグレードアシスタント 616
パスワード管理 616
スキャナーの正常性 619
概要 619
ネットワーク 620
アラート 621
スキャナーの正常性を監視する 621
詳細なデバッグ - パケットキャプチャ 622
通知 625
アカウント 627
マイアカウント 627
ユーザーアカウントを変更する 628
API キーを生成する 629
ユーザーTenable Nessus Manager 630
追加のリソース 634
Amazon Web Service 634
証明書および認証局 634
カスタム SSL サーバー証明書 635
新規サーバー証明書とCA 証明書を作成する 637
新規サーバー証明書とCA 証明書をアップロードします。 639

カスタム CA を信頼する 642
ログイン用の Nessus SSL 証明書を作成する 644
Tenable Nessus Manager 証明書と Tenable Agent 646
コマンドラインの操作 648
Tenable Nessus の開始または停止 649
Windows 649
Linux 649
macOS 650
Tenable Agent の開始または停止 651
Windows 651
Linux 651
macOS 651
Nessus のサービス 652
Nessus のサービス構文 652
Nessusd のコマンド 653
コマンド出力データを抑制する例 654
考慮事項 654
Nessuscli 654
Nessuscli の構文 655
Nessuscli のコマンド 655
Nessuscli Agent 668
Nessuscli の構文 668
Nessuscli のコマンド 668
Tenable Nessus ソフトウェアを更新する (CLI) 685

NIAP に準拠する Tenable Nessus の設定 685
デフォルトのデータディレクトリ 688
暗号強度 688
ファイルとプロセスの許可リスト 689
ログを管理する 691
デフォルトのログの場所 720
大規模デプロイメントのサポート 720
Tenable Nessus 環境変数 721
JSON を使用して Tenable Nessus をデプロイする 722
config.json ファイルの場所 722
Tenable Nessus ファイル形式の例 722
config.json の詳細 723
リンク 723
環境設定 724
ユーザー 724
新しい Linux サーバーに Tenable Nessus を移行する 725
前提条件 725
データを転送する 726
調整 730
ホスト名と IP アドレスを設定する 732
権限のないユーザーとして Tenable Nessus を実行する 733
特権ユーザー以外のユーザーとして、Linux で Systemd を使って Nessus を実行する 734
特権ユーザー以外のユーザーとして、Linux で init.d スクリプトを使って Nessus を実行する 736
特権ユーザー以外のユーザーとして、macOS で Nessus を実行する 738

Tenable Nessus 認証情報を使用したチェック 744
目的 744
アクセスレベル 745
認証情報エラーを検出する 745
Windows での認証チェック 745
前提条件 745
認証スキャン用のアカウントを設定する 746
「Nessus Local Access」セキュリティグループを作成する 747
「Nessus Scan GPO」グループポリシーを作成する 748
「Nessus Local Access」グループを「Nessus Scan GPO」ポリシーに追加する 748
Windows で WMI を許可する 749
GPO をリンクする 749
Windows を設定する 750
Windows ログイン用に Tenable Nessus スキャンを設定する 752
macOS での認証チェック 753
前提条件 753
SSH の公開鍵と秘密鍵の生成 754
ユーザーアカウントの作成 755
macOS のリモートログインの設定 755
SSH 鍵の設定 755
公開鍵システムに戻る 755
SSH 鍵のテスト 756
Linux での認証チェック 756
前提条件 757

SSH ローカルセキュリティチェックを有効にする 757
SSH の公開鍵と秘密鍵の生成 757
ユーザーアカウントを作成し、SSH 鍵を設定する 759
例 759
公開鍵システムに戻る 760
SSH ホストベースのチェック用に Tenable Nessus スキャンを設定する 760

Tenable Nessus 10.5.x へようこそ

ヒント: *Tenable Nessus ユーザーガイド*は、英語と日本語で提供されています。

Tenable Nessus ソリューション

Tenable Nessus Professional

Tenable Nessus Professional は、業界で最も広く導入されている脆弱性評価ソリューションで、企業のアタックサーフェスを減らし、コンプライアンスを確保するのに役立つ製品です。Tenable Nessus は、高速の資産検出、設定監査、ターゲットプロファイリング、マルウェア検出、機密データ検出などの機能を備えています。

Tenable Nessus は、競合ソリューションよりも多くのテクノロジーをサポートしており、オペレーティングシステム、ネットワークデバイス、ハイパーバイザー、データベース、ウェブサーバー、重要なインフラをスキャンして脆弱性、脅威、コンプライアンス違反を検出できます。

絶えず更新される、脆弱性と設定チェックに関する世界最大のライブラリと、Tenable, Inc. の脆弱性調査専門チームによるサポートにより、Tenable Nessus は脆弱性スキャンの速度と精度の標準として認識されています。

Tenable Nessus Professional 製品ページ

Tenable Nessus Expert

Tenable Nessus Expert は、業界で最も広く導入されている脆弱性評価ソリューションと、拡張された DX 時代のアタックサーフェスに対処するために特別に設計された新しい機能を組み合わせています。Nessus Expert を使用すると、企業の IP ベースのアタックサーフェスを縮小してコンプライアンスを確保できるだけでなく、インフラのコード化 (IaC) の脆弱性とポリシー違反を特定し、以前は未知であったインターネットに露呈している資産を特定することもできます。

Tenable Nessus Expert は、競合ソリューションよりも多くのテクノロジーをサポートしており、オペレーティングシステム、ネットワークデバイス、IaC リポジトリ、ハイパーバイザー、データベース、ウェブサーバー、重要インフラをスキャンして、脆弱性、脅威、コンプライアンス違反を検出できます。

絶えず更新される世界最大の脆弱性と設定チェックのライブラリと、Tenable の脆弱性調査専門チームによるサポートにより、Tenable Nessus Expert は脆弱性スキャンの速度と精度の基準を設定しています。これは、DX 時代のアタックサーフェスに対処するために設計された唯一のツールです。

Nessus Expert 製品ページ

Tenable Nessus Manager

> **注意:** Tenable Nessus Manager は、2018 年 2 月 1 日時点で販売を終了しています。既存のスタンドアロンの Tenable Nessus Manager のお客様向けに、Tenable は契約期間が終了するまで引き続きサービスを提供します。Tenable は、エージェント管理のために Tenable Nessus Manager を引き続きサポートし、プロビジョニングします。

Nessus Manager は、Nessus の強力な検出、スキャン、監査機能を組み合わせた、世界で最も広く導入されている脆弱性スキャナーです。広範な管理機能およびコラボレーション機能によってアタックサーフェスを減らします。

Nessus Manager は、Nessus スキャナー、スキャンスケジュール、ポリシー、スキャン結果を複数のユーザーまたはグループ間で共有できるようにします。ユーザーは、同僚、システム所有者、内部監査人、リスクおよびコンプライアンス担当者、IT 管理者、ネットワーク管理者、セキュリティアナリストとリソースと責任を共有して、協働できます。このようなコラボレーション機能により、スキャン、マルウェアと設定ミスの検出と修復が効率化され、セキュリティスキャンとコンプライアンス監査にかかる時間とコストを低減できます。

Nessus Manager は、物理、仮想、モバイル、クラウドの各環境を保護します。Nessus Manager は、オンプレミスデプロイメントで使用することも、Tenable Vulnerability Management のようにクラウドから使用することもできます。Nessus Manager は、非常に広範なシステム、デバイス、資産をサポートし、エージェントレスオプションと Tenable Agent デプロイメントオプションの両方を提供しているので、モバイル環境、一時的な環境、その他のアクセス困難な環境でも容易にカバーできます。

Tenable Agent

Tenable Agent のドキュメントについては、Tenable Agent ユーザーガイドを参照してください。

Tenable Vulnerability Management と Nessus Manager で提供されている Tenable Agents は、継続的なホスト認証情報を必要としない資産やオフラインの資産のスキャンを容易にすることで、スキャンの柔軟性を向上させています。また、ネットワークにほとんど影響を与えずに大規模な同時スキャンが実行できます。

Tenable Agents は、ローカルでホストにインストールできる、軽量でフットプリントの小さいプログラムで、ネットワークベースのスキャンを補完したり、ネットワークスキャンでは見逃されていた部分を可視化したりできます。Tenable Agents は脆弱性、コンプライアンス、システムデータを収集し、分析するために、マネージャーに報告します。Tenable Agents を使用すれば、スキャンの柔軟性と範囲を拡張でき、認証情報を使用せずにホストをスキャンしたり、断続的にインターネットに接続するオフラインの資産やエンドポイントをスキャンしたりできます。さらに、ネットワークにほとんど影響を与えずに大規模な同時スキャンを実行できます。

Tenable Agents は、ネットワークベースのスキャンの課題に取り組むのに役立ちます。特に、組織のセキュリティ態勢に関する情報を一貫して収集するのが不可能またはほぼ不可能な資産がある場合に役立ちます。ネットワークスキャンは通常は選択された間隔で、または指定された時間枠で行われ、スキャンの実行時にシステムにアクセス可能でなければなりません。スキャンの実行時にノートパソコンやその他の一時的デバイスにアクセスできない場合、それらのデバイスはスキャンから除外されるため、脆弱性が見逃されます。Tenable Agents は、スケジュールされた評価時にネットワークに接続されていない、または電源が入っていない資産やその他のスキャン困難な資産をスキャンすることでアタックサーフェスを減らします。

現代の複雑な IT 環境にあるサーバー、ポータブルデバイス、またはその他の資産に Tenable Agents をインストールすると、インストールしたホストの脆弱性、ポリシー違反、設定ミス、マルウェアが検出され、結果が管理製品に報告されるようになります。Tenable Agents は Tenable Nessus Manager または Tenable Vulnerability Management で管理できます。

Tenable Agent 製品ページ

Tenable Vulnerability Management

Tenable Vulnerability Management は、サブスクリプションベースのライセンスで、Tenable Store で購入できます。

Tenable Vulnerability Management を使用すると、セキュリティチームと監査チームは、複数の Tenable Nessus スキャナー、スキャンスケジュール、スキャンポリシー、そして最も重要なスキャン結果を無制限の数のユーザーやグループで共有できます。

Tenable Vulnerability Management は、さまざまなリソースをユーザーとグループで共有することによって、お使いの脆弱性管理プログラムに対応する、高度にカスタマイズされたワークフローを多種多様な形で作成できるようにします。拠点の場所やプログラムの複雑さ、ビジネスを安全に維持するための多数の規制やコンプライアンス要件にかかわらず、無限大の可能性を引き出すことができます。

また、Tenable Vulnerability Management では、複数の Tenable Nessus スキャナーの管理、スキャンのスケジューリング、ポリシーのプッシュ、スキャン結果の表示を、クラウドから一貫して行うことができます。このため、Nessus スキャナーをネットワーク全体、地理的に散在する拠点、さらにはパブリッククラウドやプライベートクラウドにもデプロイできます。

Tenable Vulnerability Management のサブスクリプションには以下が含まれます。

- 境界内のシステムを数に制限なくスキャン
- ウェブアプリケーションの監査
- 現在の PCI 基準に準拠したセキュリティ評価準備の対応
- PCI ASV 検証を受けるための四半期レポートの提出 (Tenable, Inc. 経由で 2 回まで)
- Tenable Nessus ナレッジベースとサポートチケットの作成が可能な Tenable コミュニティサイトへの 24 時間 365 日のアクセス

Tenable Vulnerability Management 製品ページ

Tenable Vulnerability Management ユーザーマニュアル

システム要件

Tenable Nessus は以下の環境で実行できます。

環境			追加情報
Tenable Core	バーチャル	VMware	*Tenable Core ユーザーガイド* の 要件
		Microsoft Hyper-V	
	クラウド	Microsoft Azure	
	ハードウェア		
その他のプラットフォーム	バーチャル	VMware	ハードウェア要件 および ソフトウェア要件
	ハードウェア		ハードウェア要件 および ソフトウェア要件

ライセンス要件については、ライセンス要件 を参照してください。

ハードウェア要件

企業ネットワークでは、そのパフォーマンス、容量、プロトコル、アクティビティが多岐にわたります。Tenable Nessus のデプロイメントにあたり検討すべきリソース要件には、ネットワーク理論速度、ネットワークの規模、Tenable Nessus の設定などがあります。

以下の推奨事項は、最小ハードウェア割り当てのガイドラインです。特定のタイプのスキャンでは、より多くのリソースが使用されます。複雑なスキャン、特に認証情報を使用するスキャンを実行する場合は、さらなるディスク容量、メモリ、処理能力が必要になることがあります。

ヒント: スキャンパフォーマンスの最大化に関する情報やスキャン設定のヒントについては、Tenable Nessus Scan Tuning Guide (スキャン調整ガイド) を参照してください。

注意: Linux 環境では、ディスク容量要件が `/opt` フォルダーに適用されます。

注意: 以下のセクションに記載されている推奨最小ディスク容量に加えて、Tenable Nessus ログファイルを保存するために所属組織で必要な追加のディスク容量を考慮してください。デフォルトでは、`nessusd.dump` と `nessusd.messages` はそれぞれ最大 50 GB のログファイルを保存できますが、所属組織のニーズに応じてこのサイズを増減することができます。詳細については、*Tenable Nessus ユーザーガイド*のログの詳細設定の `dumpfile_max_files`、`dumpfile_max_size`、`logfile_max_files`、`logfile_max_size` の設定を参照してください。

Tenable Nessus スキャナーと Tenable Nessus Professional

次の表は、Tenable Nessus スキャナーと Tenable Nessus Professional のハードウェア要件を示しています。

シナリオ	ハードウェアの最小要件
スキャンあたり最大 50,000 台のホストをスキャンする場合	**CPU** – 2 GHz コア x 4 **メモリ** – 4 GB RAM (8 GB RAM 推奨) **ディスク容量** – 30 GB (ホストオペレーティングシステムで使用する容量は含まれていません) **注意:** 使用状況 (スキャン結果、プラグインアップデート、ログなど) によって必要なディスク容量は次第に増加します。

シナリオ	ハードウェアの最小要件
スキャンあたり 50,000 台以上のホストをスキャンする場合	**CPU** – 2 GHz コア x 8 **メモリ** – 8 GB RAM (16 GB RAM 推奨) **ディスク容量** – 30 GB (ホストオペレーティングシステムで使用する容量は含まれていません) **注意:** 使用状況 (スキャン結果、プラグインアップデート、ログなど) によって必要なディスク容量は次第に増加します。

Tenable Nessus Manager

次の表は、Tenable Nessus Manager のハードウェア要件を示しています。

注意: Nessus Manager クラスタリングのハードウェア要件を表示するには、クラスタリングのシステム要件を参照してください。

シナリオ	ハードウェアの最小要件
0 ~ 10,000 のエージェントがある Tenable Nessus Manager	**CPU** – 2 GHz コア x 4 **メモリ** – 16 GB RAM **ディスク容量** – 同時スキャン 5,000 エージェントあたり 5 GB **注意:** 時の経過とともに、スキャン結果とプラグインアップデートに、より多くのディスク容量が必要になります。
10,001 ~ 20,000 のエージェントがある Tenable Nessus Manager	**CPU** – 2 GHz コア x 8 **メモリ** – 32 GB RAM **ディスク容量** – 同時スキャン 5,000 エージェントあたり 5 GB **注意:** • 時の経過とともに、スキャン結果とプラグインアップデートに、より多くのディスク容量が必要になり

シナリオ	ハードウェアの最小要件
	ます。 • デプロイメントの規模が大きい場合は、Tenable の担当者にご連絡ください。

ストレージ要件

Tenable では、Tenable Nessus スキャナーが正常に動作するために、最低 5,000 MB の一時的なスペースを確保することを推奨しています。

Tenable は、仮想化されていないホストの場合、Tenable Nessus スキャナーと Tenable Nessus Manager をダイレクトアタッチストレージ (DAS) デバイスにインストールすることを推奨しています。仮想ホストの場合、Tenable は、ストレージのレイテンシが 10 ミリ秒以下のストレージエリアネットワーク (SAN) に Tenable Nessus Manager をインストールすることを推奨しています。

Tenable は、NFS などのネットワークファイルシステムを含む、ネットワークアタッチストレージ (NAS) への Tenable Nessus Manager のインストールをサポートしていません。

注意: Tenable Nessus は CPU 負荷の高いアプリケーションです。Tenable Nessus を仮想化されたインフラにデプロイする場合、オーバーサブスクライブ状態のリソース (特に CPU) を利用しようとするような方法で Tenable Nessus を実行しないように注意してください。仮想インフラのリソース割当を最適化するためのガイダンスについては、各ベンダーが提供している仮想インフラに関するドキュメントを参照してください。

NIC 要件

Tenable はネットワークインターフェースコントローラー (NIC) と Tenable Nessus の互換性を確保するために、少なくとも以下の設定を行うことを推奨しています。

- NIC チームを無効にする、または 1 つの NIC を Tenable Nessus に割り当てる
- NIC の IPv6 トンネリングを無効にする
- Tenable Nessus と NIC を共有するパケットキャプチャアプリケーションを無効にする
- 他の Docker コンテナと NIC を共有している Docker コンテナに Tenable Nessus をデプロイしないようにする

他の NIC の設定が Tenable Nessus と互換性があるかどうかを確認したい場合は、Tenable サポートにお問い合わせください。

仮想マシン

Tenable Nessus は、同じ要件を満たしている仮想マシンにもインストールできます。仮想マシンがネットワークアドレス変換 (NAT) を使用してネットワークにアクセスしている場合、Tenable Nessus の脆弱性チェック、ホスト列挙、オペレーティングシステムの識別の大部分が悪影響を受けます。

注意: 任意の物理ホストで実行できる仮想 Tenable Nessus スキャナーは *1* つだけです。Tenable Nessus は、低レベルのネットワーク操作に依存しており、ホストのネットワークインターフェースコントローラー (NIC) へのフルアクセス権を必要とします。仮想環境 (Hyper-V、Docker など) で、複数の仮想化された Tenable Nessus スキャナーが 1 つの物理 NIC を共有しようとすると、スキャナーが不適切に動作したり、ホストが不安定になったりする可能性があります。

注意: Tenable Nessus は CPU 負荷の高いアプリケーションです。Tenable Nessus を仮想化されたインフラにデプロイする場合、オーバーサブスクライブ状態のリソース (特に CPU) を利用しようとするような方法で Tenable Nessus を実行しないように注意してください。仮想インフラのリソース割当を最適化するためのガイダンスについては、各ベンダーが提供している仮想インフラに関するドキュメントを参照してください。

ソフトウェア要件

Tenable Nessus は、次の Linux、Windows、macOS のオペレーティングシステムをサポートしています。

Tenable Nessus 10.10

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9 および 10	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2020	x86_64

	Fedora 41、42	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降、10	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP3 以降	x86_64
	TencentOS	x86_64
	Ubuntu 16.04	x86
	Ubuntu 16.04、18.04、20.04、22.04、24.04	x86_64
	Ubuntu 18.04、20.04、22.04、24.04	AArch64
macOS	macOS 13、14、15、26	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022、2025	x86_64

Tenable Nessus 10.9

オペレーティングシステム	対応バージョン	サポートされるアーキテク

		チャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2020	x86_64
	Fedora 41、42	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降、10	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP3 以降	x86_64
	TencentOS	x86_64
	Ubuntu 16.04	x86
	Ubuntu 16.04、18.04、20.04、22.04、24.04	x86_64
	Ubuntu 18.04、20.04、22.04、24.04	AArch64
macOS	macOS 13、14、15、26	x86_64

		Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022、2025	x86_64

Tenable Nessus 10.8

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2020	x86_64
	Fedora 38 および 39	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64

	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP3 以降	x86_64
	TencentOS	x86_64
	Ubuntu 16.04	x86
	Ubuntu 16.04、18.04、20.04、22.04、24.04	x86_64
	Ubuntu 18.04、20.04、22.04、24.04	AArch64
macOS	macOS 12、13、14、15、26	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022	x86_64

Tenable Nessus 10.7

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 および 12	x86_64

	Kali Linux 2020	x86_64
	Fedora 38 および 39	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP2 以降	x86_64
	TencentOS	x86_64
	Ubuntu 14.04、16.04	x86
	Ubuntu 14.04、16.04、18.04、20.04、22.04	x86_64
	Ubuntu 18.04	AArch64
macOS	macOS 12、13、14	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022	x86_64

Tenable Nessus 10.5

オペレーティン	対応バージョン	サポートされ

グシステム		るアーキテクチャ
Linux	AlmaLinux 9.5	x86_64 AArch64
	Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11	x86_64
	Kali Linux 2020	x86_64
	Fedora 34 および 35	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	Red Hat EL 6.x および 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP1 以降	x86_64
	TencentOS	x86_64
	Ubuntu 14.04、16.04	x86
	Ubuntu 14.04、16.04、18.04、20.04	x86_64
	Ubuntu 18.04	AArch64

macOS	macOS 11、12、13	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022	x86_64

ヒント: Tenable Core + Nessus については、Tenable Core ユーザーガイドのシステム要件を参照してください。

注意: Microsoft Visual C++ 再頒布可能パッケージ 14.22 は、Tenable Nessus と一緒にバンドルされているライセンスパッケージに含まれています。

対応ブラウザ

Tenable Nessus でサポートされるブラウザは次のとおりです。

- Google Chrome (76 以降)
- Apple Safari (10 以降)
- Mozilla Firefox (50 以降)
- Microsoft Edge (102 以降)

PDF レポート

Tenable Nessus の PDF レポート生成機能を使用するには、Oracle Java または OpenJDK の最新バージョンが必要です。

所属組織で PDF レポートが必要な場合は、Tenable Nessus をインストールする前に Oracle Java または OpenJDK をインストールしておく必要があります。Tenable Nessus をインストールした後に Oracle Java または OpenJDK をインストールした場合、PDF レポート機能を適切に機能させるためには、Tenable Nessus を再インストールする必要があります。

SELinux の要件

Tenable Nessus は、無効、許容、強制モードの Security-Enhanced Linux (SELinux) ポリシー設定をサポートしています。

- 無効化されたモードのポリシーと許容モードのポリシーは、通常、Tenable Nessus とのやり取りのためにカスタマイズする必要はありません。
- モードポリシーの実施には、Tenable Nessus とのやり取りのためにカスタマイズする必要があります。詳細については、SELinux の強制モードポリシーのカスタマイズを参照してください。

注意: Tenable では、本番環境のネットワークにデプロイする前に、SELinux の設定をテストすることを推奨しています。

SELinux の強制モードポリシーのカスタマイズ

Security-Enhanced Linux (SELinux) の強制モードポリシーは、Tenable Nessus とやり取りできるようにカスタマイズする必要があります。

Tenable サポート は、SELinux ポリシーのカスタマイズ作業の手助けは行いませんが、Tenable では、SELinux のログを監視して、ポリシー設定のエラーとソリューションを特定することを推奨しています。

始める前に

- SELinux `sealert` ツールを本番環境と同様のテスト環境にインストールします。

SELinux のログを監視して、エラーと解決策を特定する方法

1. `sealert` ツールを実行します。SELinux 監査ログの場所は、`/var/log/audit/audit.log` です。

   ```
   sealert -a /var/log/audit/audit.log
   ```

   このツールが実行されると、エラーのアラートと解決策の概要が生成されます。たとえば、次のようになります。

   ```
   SELinux は、/usr/sbin/sshd による sock_file /dev/log への書き込みアクセスを防止しています。
   SELinux は、/usr/libexec/postfix/pickup がプロセス上で rlimitinh アクセスを使用することを防止しています。
   ```

2. 各エラーアラートに対して推奨される解決策を実行します。
3. Tenable Nessus を再起動します。
4. 再度 `sealert` ツールを実行し、エラーアラートが解消されたことを確認します。

ライセンス要件

このトピックでは、Tenable Nessus のライセンシングの方法を説明し、その機能を一覧表示します。

Tenable Nessus のライセンシング

Tenable Nessus を Tenable Security Center で管理することも、スタンドアロンのサブスクリプション製品として実行することもできます。サブスクリプションを購入するには、Tenable のウェブサイトにアクセスするか、Tenable パートナーにご連絡ください。

Tenable Nessus には次の 2 つのバージョンがあります。

- **Tenable Nessus Professional** – 1 つのサブスクリプション価格。
- **Tenable Nessus Expert** – サブスクリプション価格に、四半期ごとに 5 つ以上のウェブアプリケーションスキャンドメインまたは外部アタックサーフェススキャン (EASM) ドメインを加えたもの。

プラグインフィードアクティベーションコード

Tenable Nessus を管理する場所では、*プラグインフィードアクティベーションコード*が必要になります。このコードは、ライセンスが付与されているバージョンを識別し、該当する場合は、スキャンできる IP アドレスの数、リンクできるリモートスキャナーの数、Tenable Nessus Manager にリンクできる Tenable Agents の数も示します。このコードを入力する場所は、Tenable Nessus をどのように管理しているかによって異なります。

- **Tenable Nessus サブスクリプション** – アクティベーションコードを管理するの説明に従って、Tenable Nessus でアクティベーションコードを管理します。

  > **ヒント**: Tenable Nessus をオフラインで設定するには、Tenable Nessus をオフラインで管理するを参照してください。

- **Tenable Security Center での Tenable Nessus** – アクティベーションコード (およびプラグインの更新) を Tenable Security Center で管理します。Tenable Nessus を登録する場合は、Tenable Security Center の前に起動し、**[Managed by SecurityCenter]** (SecurityCenter による管理) を選択します。詳細については、*Tenable Security Center ユーザーガイド*の新しいライセンスを適用するを参照してください。

Tenable Nessus を Tenable Vulnerability Managementで管理する

Tenable Vulnerability Management を使用して Tenable Nessus スキャナーを管理している場合、プラグインとソフトウェアの更新は Tenable Vulnerability Management から管理します。詳細は、*Tenable Nessus ユーザーガイド*の Tenable Nessus プラグインとソフトウェアの更新を参照してください。

Tenable Vulnerability Management には、無制限の Tenable Nessus スキャナーをデフォルトのコンポーネントとしてリンクする機能があります。

Tenable Vulnerability Management ライセンスの詳細については、*Tenable ライセンスガイド*の Tenable Vulnerability Management ライセンスを参照してください。

Tenable Nessus を Tenable Security Centerで管理する

Tenable Security Center を使用して Tenable Nessus スキャナーを管理している場合、アクティベーションコードとプラグインの更新は Tenable Security Center から管理します。詳細は、*Tenable Nessus ユーザーガイド*の Tenable Nessus プラグインとソフトウェアの更新を参照してください。

Tenable Security Center と通信する前に Tenable Nessus を起動する必要がありますが、通常、有効なアクティベーションコードとプラグインがないと起動しません。この要件を無視して Tenable Nessus を起動させ、Tenable Security Center から情報を取得できるようにするには、スキャナーを登録するときに **[Managed by SecurityCenter]** (SecurityCenterによる管理) を選択します。

Tenable Security Center ライセンスの詳細については、*Tenable ライセンスガイド*の Tenable Security Center ライセンスを参照してください。

Tenable Nessus のバージョン

Tenable Nessus Professional および Tenable Nessus Expert には次の機能があります。

機能	Tenable Nessus Professional	Tenable Nessus Expert
Nessus Live Results	○	○
脆弱性診断	○	○
コンプライアンススキャン	○	○
動的アプリケーションセキュリティテスト (DAST) ウェブアプリケーションスキャン	×	四半期ごとに 5 つのウェブアプリケーション (必要に応じて追加購

		入)
外部アタックサーフェススキャン	×	四半期ごとに5つのドメイン(必要に応じて追加購入)
インフラのコード化のスキャン	×	○

ポートの要件

Tenable Nessus のポート要件には、Tenable Nessus Manager、Tenable Nessus Professional、Tenable Nessus Expert、Tenable Nessus Essentials、Tenable Nessus スキャナー、Tenable Nessus クラスタノード固有の要件、Tenable Agent 固有の要件などがあります。

Tenable Nessus

Tenable Nessus インスタンスは、受信と送信のトラフィック用の特定のポートへのアクセスを必要とします。

受信トラフィック

次のポートへの受信トラフィックを許可する必要があります。

Port (ポート)	トラフィック
TCP 8834	Tenable Nessus インターフェースへのアクセス Tenable Security Center との通信 API とのインタラクション

送信トラフィック

次のポートへの送信トラフィックを許可する必要があります。

Port (ポート)	トラフィック
TCP 25	SMTP メール通知の送信
TCP	Tenable Vulnerability Management との通信 (sensor.cloud.tenable.com または

Port (ポート)	トラフィック
443	sensor.cloud.tenablecloud.cn) プラグイン更新での plugins.nessus.org サーバーとの通信
UDP 53	DNS 解決の実行

Tenable Nessus Agent

Tenable Agents は、送信トラフィック用の特定のポートへのアクセスを必要とします。

送信トラフィック

次のポートへの送信トラフィックを許可する必要があります。

Port (ポート)	トラフィック
TCP 443	Tenable Vulnerability Management との通信
TCP 8834	Tenable Nessus Manager との通信 **注意:** デフォルトの Tenable Nessus Manager ポートは TCP 8834 です。ただし、このポートは設定可能であり、組織によって異なる場合があります。
UDP 53	Tenable Agent がインストールされているホストの外部 DNS サポート。いくつかのプラグインは、その操作に DNS 解決を使用します。

注意: `dnf install` などのオペレーティングシステムのインストールコマンドでは、Tenable Vulnerability Management または Tenable Nessus Manager 以外の接続が必要になる場合があります。詳細については、オペレーティングシステム管理者に問い合わせてください。

デプロイメントに関する考慮事項

Tenable Nessus をデプロイするときは、ルーティング、フィルター、ファイヤーウォールのポリシーに関する知識が役立ちます。NAT デバイスの背後に Nessus をデプロイすることは、内部ネットワークをスキャンするのでない限り、望ましくありません。脆弱性スキャンが NAT デバイスまたは何らかの種類のアプリケーション

プロキシを通過するたびに検査が正確に伝わらず、結果的に誤検出または検出漏れが生じる可能性があります。

また、Tenable Nessus を実行しているシステムにパーソナルまたはデスクトップファイヤーウォールが実装されている場合は、リモート脆弱性スキャンの効果がこのようなツールによって著しく制限される可能性があります。ホストベースのファイヤーウォールは、ネットワーク脆弱性スキャンの妨げになることがあります。ファイヤーウォールの設定によっては、Tenable Nessus スキャンの調査がファイヤーウォールによって阻止、歪曲、非表示にされる可能性があります。

ステートフル検査を実行するネットワークデバイスの一部 (ファイヤーウォール、ロードバランサー、侵入検出/防止システムなど) は、Tenable Nessus がそれらのデバイス経由でスキャンが実行する場合に、悪影響を与えることがあります。Tenable Nessus には、このようなデバイス経由のスキャンの影響を軽減するのに役立つチューニングオプションがいくつか用意されています。ただし、このようなネットワークバイス経由のスキャンに固有の問題を回避する最良の方法は、認証情報を使用したスキャンを実行することです。

Tenable Nessus Manager をエージェント管理用に設定する場合、Tenable Nessus Manager をローカルスキャナーとして使用することはお勧めしません。たとえば、Tenable Security Center のスキャンゾーンに Tenable Nessus Manager を含めるように設定したり、Tenable Nessus Manager からネットワークベースのスキャンを直接実行したりしないでください。このような設定は、エージェントスキャンのパフォーマンスに悪影響を与える可能性があります。

このセクションでは、デプロイメントに関する以下の考慮事項について説明します。

- ポートの要件
- ホストベースのファイヤーウォール
- IPv6 のサポート
- ネットワークアドレス変換 (NAT) の制限
- ウイルス対策ソフトウェア
- セキュリティ警告

ホストベースのファイヤーウォール

ポート 8834

Nessus ユーザーインターフェースでは、ポート **8834** が使用されます。まだポート **8834** を開いていない場合は、ファイヤーウォールベンダーのドキュメントの設定手順を参照してこのポートを開きます。

接続を許可する

ZoneAlarm や Windows ファイヤーウォールなどのサードパーティのファイヤーウォールを使用しているホストに Nessus サーバーを設定した場合は、Nessus を使用するクライアントの IP アドレスからの接続を許可するようにファイヤーウォールを設定する必要があります。

Nessus と FirewallD

Tenable Nessus を FirewallD と連携するように設定できます。`firewalld` を使用して Tenable Nessus をインストールする際に、`firewalld` に Nessus サービスと Nessus ポートを設定できます。

Nessus に必要なポートを開くには、次のコマンドを使用します。

```
>> firewall-cmd --permanent --add-service=nessus
>> firewall-cmd --reload
```

IPv6 のサポート

Nessus では、IPv6 ベースのリソースのスキャンがサポートされます。多くのオペレーティングシステムとデバイスでは、IPv6 のサポートがデフォルトで有効になっています。IPv6 リソースに対してスキャンを実行するには、Nessus がインストールされているホストに IPv6 インターフェースを 1 つ以上設定し、Nessus を IPv6 対応ネットワークに接続する必要があります (IPv4 経由では Nessus は IPv6 リソースをスキャンできません。ただし、IPv4 経由の、認証情報を使用したスキャンで IPv6 インターフェースを列挙することはできます)。スキャンを開始するときには、IPv6 の完全表記と省略表記の両方がサポートされます。

IP を個別に (リスト形式で) 入力する場合を除いて、Nessus は IPv6 グローバルユニキャスト IP アドレス範囲のスキャンをサポートしません。Nessus では、ハイフンでつながれた範囲または CIDR アドレスとして表現された範囲はサポートされません。Nessus では、スキャンターゲットとしての **link6** ディレクティブを含むリンクローカル範囲や **eth0** を含むローカルリンクがサポートされます。

ネットワークアドレス変換 (NAT) の制限

仮想マシンがネットワークアドレス変換 (NAT) を使用してネットワークにアクセスしている場合、Nessus の脆弱性チェック、ホスト列挙、オペレーティングシステムの識別の大部分が悪影響を受けます。

ウイルス対策ソフトウェア

スキャン中に多数のTCP接続が生成されるため、一部のウイルス対策ソフトウェアパッケージでは、Tenable Nessusがワームまたはマルウェアの形態に分類される場合があります。また、ウイルス対策ソフトウェアにより、スキャン処理時間が長くなる可能性があります。

- ウイルス対策ソフトウェアから警告が出た場合は、**[Allow]**(許可)を選択して、Tenable Nessusにスキャンを続行させます。
- ウイルス対策パッケージに、例外リストにプロセスを追加するオプションがある場合は、**`nessusd.exe`**、**`nessus-service.exe`**、**`nessuscli.exe`**を追加します。

セキュリティ製品でのTenable Nessusフォルダー、ファイル、プロセスの許可リスト登録の詳細については、ファイルとプロセスの許可リストを参照してください。

セキュリティ警告

デフォルトでは、Tenable Nessusのインストールと管理には、**HTTPS**および**SSL**のユーザーポート**8834**が使用されます。Tenable Nessusのデフォルトのインストールでは、自己署名SSL証明書が使用されます。

Tenable Nessusインストールのウェブ上の操作では、SSLについて次のようなメッセージが表示されます。

> *SSL証明書が無効であることを示すセキュリティ警告がブラウザに表示される可能性があります。一時的にリスクを受け入れるか、レジストラから有効なSSL証明書を取得することができます。*

これは、Tenable Nessusユーザーインターフェース(https://[サーバーIP]:8834)にアクセスするときに表示されるセキュリティ関連メッセージの情報です。

セキュリティ警告の例

- 接続プライバシーの問題
- 信頼できないサイト
- 安全でない接続

Tenable Nessusは自己署名SSL証明書を提供するので、これは正常な動作です。

SSL警告のバイパス

使用しているブラウザに応じて、次の手順に従ってTenable Nessusログインページに進みます。

ブラウザ	手順
Google Chrome と Microsoft Edge	**[Advanced]** (詳細設定)、**[Proceed to example.com (unsafe)]** (example.com (安全でない) に進む) の順に選択します。 **注意:** Google Chrome と Microsoft Edge の一部のインスタンスでは、続行できません。これが発生する場合、Tenable は、Safari や Mozilla Firefox などの別のブラウザの使用を推奨します。
Mozilla Firefox	**[I Understand the Risks]** (リスクを理解しています)、**[Add Exception]** (例外を追加する) の順に選択します。 次に **[Get Certificate]** (証明書を取得する)、最後に **[Confirm Security Exception]** (セキュリティ例外を確認する) を選択します。

Tenable Nessus を使い始める

準備

1. 設定がシステムの最小要件を満たしていることを確認します。
    - ハードウェア要件
    - ソフトウェア要件
2. Tenable Nessus のアクティベーションコードを取得します。

Tenable Nessus をインストールして設定する

1. お使いの Tenable Nessus ソフトウェアとオペレーティングシステムに応じて、Tenable Nessus のインストールに記載されているインストール手順に従ってください。
2. 初期設定手順を実行します。

スキャンを作成して設定する

1. ホスト検出スキャンを実行し、ネットワーク上の資産を特定します。
2. スキャンを作成します。

3. ニーズに応じたスキャンテンプレートを選択します。

    - Tenable から提供されたスキャナーテンプレートを使用します。
    - (Tenable Nessus Manager のみ)Tenable から提供されたエージェントテンプレートを使用します。
    - ポリシーを作成し、ユーザー定義テンプレートを作成して使用します。

4. スキャンを設定する方法

    - テンプレートで利用できるスキャン設定をします。

      スキャンターゲットについての詳細は、ターゲットのスキャンを参照してください。
    - (オプション) ライブ結果を設定するには、ライブ結果を参照してください。
    - (オプション) 認証情報が必要なスキャンを実行する場合は、認証情報を設定します。
    - (オプション) コンプライアンススキャンを実行する場合は、スキャンに含まれるコンプライアンス監査を選択します。
    - (オプション) 詳細スキャンテンプレートを使用する場合は、スキャンに含まれるプラグインを選択します。

5. スキャンを起動します。

スキャン結果を表示して分析する

- スキャン結果を表示します。
- 脆弱性を表示して管理します。
- スキャンフォルダーを管理します。
- スキャンレポートまたはエクスポートを作成します。

Tenable Nessus 設定を調整する

- 警告メッセージに対処するためにスキャン設定を調整します。
- スキャナーの正常性を監視します。
- Tenable Nessus 詳細設定をします。

Tenable Nessus のナビゲーション

上部のナビゲーションバーには2つの主要ページ **[Scans]** (スキャン) と **[Settings]** (設定) へのリンクが表示されます。Tenable Nessus での主なタスクはすべてこの2つのページから実行できます。ページ名をクリックすると該当ページが開きます。

項目	説明
	[Notifications] (通知) ボックスを切り替えます。通知、成功または失敗したログイン試行、エラー、Tenable Nessus により生成されたシステム情報が一覧表示されます。
Username (ユーザー名)	ドロップダウンボックス形式でオプション **[My Account]** (マイアカウント)、**[What's New]** (最新情報)、**[Documentation]** (ドキュメント)、**[Sign Out]** (サインアウト) が表示されます。

Tenable Nessus のインストール

このセクションには、サポートされているすべてのオペレーティングシステムに Nessus をインストールするために必要な情報と手順が含まれています。

- macOS での Tenable Nessus のインストール
- Linux での Tenable Nessus のインストール
- Windows での Tenable Nessus のインストール
- Raspberry Pi での Tenable Nessus のインストール
- Tenable Core+ Tenable Nessus のデプロイまたはインストール
- Docker イメージとして Tenable Nessus をデプロイする

をダウンロードするTenable Nessus

Tenable Nessus は、Tenable のダウンロードサイトからダウンロードできます。

Tenable Nessus をダウンロードする際は、選択したパッケージがお使いのオペレーティングシステムとプロセッサーに対応していることを確認してください。

オペレーティングシステムとプロセッサーごとに 1 つの Tenable Nessus パッケージがあります。Tenable Nessus Manager、Tenable Nessus Professional、Tenable Nessus Expert のパッケージは分かれていません。インストールされる Tenable Nessus 製品はアクティベーションコードによって決まります。

Tenable Nessus のインストール

Tenable Nessus をインストールするには、Tenable のダウンロードサイトから Tenable Nessus をダウンロードします。

Tenable Nessus をダウンロードする際は、選択したパッケージがお使いのオペレーティングシステムとプロセッサーに対応していることを確認してください。

オペレーティングシステムとプロセッサーごとに 1 つの Tenable Nessus パッケージがあります。Tenable Nessus Manager、Tenable Nessus Professional、Tenable Nessus Expert のパッケージは分かれていません。インストールされる Tenable Nessus 製品はアクティベーションコードによって決まります。

Tenable Nessus のダウンロードが完了したら、ご使用のオペレーティングシステムに応じて、次のいずれかの手順を使用して Tenable Nessus をインストールします。

- Linux
- Windows
- macOS
- Raspberry Pi
- Tenable Core+ Tenable Nessus
- Docker イメージとして Tenable Nessus をデプロイする

Linux での Tenable Nessus のインストール

警告: 既存の Tenable Agent、Tenable Nessus Manager、または Tenable Nessus スキャナーが `nessusd` で実行されているシステムに Tenable Agent、Tenable Nessus Manager、または Tenable Nessus スキャナーをインストールすると、インストールプロセスにより他のすべての `nessusd` プロセスが強制的に終了されます。この結果スキャンデータが失われる場合があります。

注意: Tenable Nessus では、`/opt/nessus/` でのシンボリックリンクの使用はサポートされていません。

始める前に

Nessus を Linux にインストールする方法

1. Tenable Nessus パッケージファイルをダウンロードします。
2. コマンドラインから、ご使用のオペレーティングシステムに固有の Tenable Nessus インストールコマンドを実行します。

   Tenable Nessus インストールコマンドの例:

   Debian/Kali と Ubuntu

   ```
   # dpkg -i Nessus-<version number>-debian6_amd64.deb
   ```

   Red Hat

   ```
   # dnf install Nessus-<version number>-el8.x86_64.rpm
   ```

   SUSE

   ```
   # sudo zypper install Nessus-<version number>-suse12.x86_64.rpm
   ```

3. コマンドラインから nessusd デーモンを再起動します。

   Tenable Nessus デーモン開始コマンドの例:

   CentOS、Debian/Kali、Fedora、Oracle Linux、Red Hat、SUSE、Ubuntu

   ```
   # systemctl start nessusd
   ```

4. ブラウザで Tenable Nessus を開きます。
   - リモートでインストールされた Tenable Nessus インスタンスにアクセスするには、https://<リモート IP アドレス>:8834 (例: https://111.49.7.180:8834) にアクセスします。
   - ローカルにインストールされている Tenable Nessus インスタンスにアクセスするには、https://localhost:8834 にアクセスします。
5. ブラウザで残りの Tenable Nessus インストール手順を実行します。

Windows での Tenable Nessus のインストール

警告: 既存の Tenable Agent、Tenable Nessus Manager、または Tenable Nessus スキャナーが nessusd で実行されているシステムに Tenable Agent、Tenable Nessus Manager、または Tenable Nessus スキャナーをインストールすると、インストールプロセスにより他のすべての nessusd プロセスが強制的に終了されます。この結果スキャンデータが失われる場合があります。

注意: Tenable Nessus では、/opt/nessus/ でのシンボリックリンクの使用はサポートされていません。

注意: インストールを完了するためにコンピューターの再起動を求められる場合があります。

Nessus パッケージファイルをダウンロードする

Tenable Nessus は、Tenable のダウンロードサイトからダウンロードできます。

Tenable Nessus のインストールを開始する

1. Tenable Nessus のインストーラをダウンロードしたフォルダーに移動します。
2. 次に、ファイル名をダブルクリックし、インストールのプロセスを開始します。

Windows InstallShield ウィザードを完了する

1. 最初に、**[Welcome to the InstallShield Wizard for Tenable, Inc. Nessus Agent]** (Tenable Nessus Agent の InstallShield ウィザードへようこそ) 画面が表示されます。**[Next]** (次へ) を選択し継続します。
2. **[License Agreement]** (ライセンス契約) 画面で、Tenable Nessus ソフトウェアライセンスとサブスクリプション契約の利用条件を読みます。
3. **[I accept the terms of the license agreement]** (ライセンス契約の条件に同意します) オプションを選択し、**[Next]** (次へ) をクリックします。
4. **[Destination Folder]** (インストール先フォルダー) 画面で、**[Next]** (次へ) ボタンをクリックし、デフォルトのインストール先フォルダーを承認します。または **[Change]** (変更) ボタンを選択し、Tenable Nessus を別のフォルダーにインストールします。
5. **[Ready to Install the Program]** (プログラムのインストールの準備完了) 画面で、**[Install]** (インストール) ボタンを選択します。

次に、**[Installing Tenable, Inc. Nessus]** (Tenable Nessus のインストール) 画面が表示され、**ステータス**インジケーションバーでインストールの進捗状況が示されます。このプロセスには数分かかる場合があります。

InstallShield ウィザードが完了すると、**[Welcome to Nessus]** (Nessus へようこそ) ページがデフォルトのブラウザに読み込まれます。

ページが読み込まれない場合は、次のいずれかの手順を実行して、ブラウザで Tenable Nessus を開きます。

- リモートでインストールされた Tenable Nessus インスタンスにアクセスするには、https://<リモート IP アドレス>:8834 (例: https://111.49.7.180:8834) にアクセスします。
- ローカルにインストールされている Tenable Nessus インスタンスにアクセスするには、https://localhost:8834 にアクセスします。

Web ブラウザで残りの Tenable Nessus のインストール手順を実行します。

macOS での Tenable Nessus のインストール

警告: 既存の Tenable Agent、Tenable Nessus Manager、または Tenable Nessus スキャナーが `nessusd` で実行されているシステムに Tenable Agent、Tenable Nessus Manager、または Tenable Nessus スキャナーをインストールすると、インストールプロセスにより他のすべての `nessusd` プロセスが強制的に終了されます。この結果スキャンデータが失われる場合があります。

注意: Tenable Nessus では、`/opt/nessus/` でのシンボリックリンクの使用はサポートされていません。

Tenable Nessus パッケージファイルをダウンロードする

Tenable Nessus パッケージファイルをダウンロードします。

GUI インストールパッケージを使用して Nessus をインストールする方法

Nessus ファイルを展開する

`Nessus-<version number>.dmg` ファイルをダブルクリックします。

Nessus のインストールを開始する

Install Nessus.pkg をダブルクリックします。

Tenable, Inc. Nessus サーバーのインストールを完了する

インストールが開始されると、**[Install Tenable, Inc. Nessus Server]** (Tenable Nessus サーバーのインストール) 画面が表示され、インタラクティブなナビゲーションメニューが表示されます。

はじめに

[Welcome to the Tenable, Inc. Nessus Server Installer] (Tenable Nessus サーバーのインストーラへようこそ) ウィンドウに、Nessus のインストールについての一般的な情報が表示されます。

1. インストールの情報をお読みください。
2. **[Continue]** (続行) ボタンを選択して開始します。

ライセンス

1. **[Software License Agreement]** (ソフトウェアライセンス契約) 画面で、**Tenable, Inc.** Nessus ソフトウェアライセンスとサブスクリプション契約の利用条件を読みます。
2. **オプション:** ライセンス契約のコピーを保管するには **[Print]** (印刷) または **[Save]** (保存) を選択します。
3. 次に、**[Continue]** (続行) ボタンを選択します。
4. 同意して Nessus のインストールを継続するには **[Agree]** (同意) ボタンを選択します。あるいは **[Disagree]** (同意しない) ボタンを選択して停止または終了します。

インストールのタイプ

[Standard Install on <DriveName>] (<DriveName> での標準インストール) 画面で、次のオプションのいずれを選択します。

- **[Change Install Location]** (インストール場所を変更) ボタンを選択します。
- デフォルトのインストール場所を使用して続行するには **[Install]** (インストール) ボタンを選択します。

インストール

[Preparing for installation] (インストールのための準備) 画面が表示されると、ユーザー名とパスワードの入力を求められます。

1. 管理者アカウントまたは root のユーザーアカウントの **[Name]** (名前) と **[Password]** (パスワード) を入力します。

2. **[Ready to Install the Program]** (プログラムのインストールの準備完了) 画面で、**[Install]** (インストール) ボタンを選択します。

次に、**[Installing Tenable, Inc. Nessus]** (Tenable Nessus のインストール) 画面が表示され、残りのインストールの進捗状況を表す**ステータス**インジケーションバーが表示されます。このプロセスには数分かかる場合があります。

Summary (サマリー)

1. インストールが完了すると、**[Installation was successful]** (インストールが成功しました) 画面が表示されます。インストールが完了したら **[Close]** (閉じる) を選択します。
2. ブラウザで Tenable Nessus を開きます。
    - リモートでインストールされた Nessus インスタンスにアクセスするには、https://<リモート IP アドレス>:8834 (例: https://111.49.7.180:8834) にアクセスします。
    - ローカルにインストールされている Nessus インスタンスにアクセスするには、https://localhost:8834 にアクセスします。
3. ブラウザで残りの Nessus インストール手順を実行します。

コマンドラインから Nessus をインストールする方法

1. ターミナルを開きます。
2. リスト順に次のコマンドを実行します。
    a. `sudo hdiutil attach <Nessus .dmg package>`
    b. `sudo installer -package /Volumes/Nessus\ Install/Install\ Nessus.pkg -target /`
    c. `sudo hdiutil detach /Volumes/Nessus\ Install`
3. ブラウザで Tenable Nessus を開きます。
    - リモートでインストールされた Nessus インスタンスにアクセスするには、https://<リモート IP アドレス>:8834 (例: https://111.49.7.180:8834) にアクセスします。
    - ローカルにインストールされている Nessus インスタンスにアクセスするには、https://localhost:8834 にアクセスします。

4. ブラウザで残りの Nessus インストール手順を実行します。

Raspberry Pi での Tenable Nessus のインストール

Tenable Nessus 10.0.0 以降では、メモリを最小限の 8 GB に抑えて Raspberry Pi 4 Model B のスキャンをサポートしています。

1. Tenable ダウンロードサイトから Tenable Nessus Raspberry Pi OS パッケージファイルをダウンロードします。
2. コマンドプロンプトまたはターミナルウィンドウから、Tenable Nessus のインストールコマンドを実行します。

   ```
   dpkg -i Nessus-<version>-raspberrypios_armhf.deb
   ```

3. コマンドプロンプトまたはターミナルウィンドウから、次のコマンドを実行することにより nessusd デーモンを開始します。

   ```
   /bin/systemctl start nessusd.service
   ```

4. ブラウザで Tenable Nessus を開きます。
   - リモートでインストールされた Tenable Nessus インスタンスにアクセスするには、https://<リモート IP アドレス>:8834 (例: https://111.49.7.180:8834) にアクセスします。
   - ローカルにインストールされている Tenable Nessus インスタンスにアクセスするには、https://localhost:8834 にアクセスします。
5. ブラウザで残りの Tenable Nessus インストール手順を実行します。

Docker イメージとして Tenable Nessus をデプロイする

管理される Tenable Nessus スキャナーまたは Tenable Nessus Professional のインスタンスを Docker イメージとしてデプロイして、コンテナで実行できます。Tenable は、Oracle Linux 8 (x86_64 および AArch64) と Ubuntu (x86_64 および AArch64) の 2 つのベースとなる Tenable Nessus イメージを提供しています。環境変数を使用して Tenable Nessus インスタンスを設定することで、その設定でイメージを自動的に設定できます。演算子と変数を使用して、Tenable Vulnerability Management または Tenable Security Center にリンクされた Tenable Nessus イメージをデプロイできます。

Tenable は、他の Docker コンテナとネットワークインターフェースコントローラー (NIC) を共有している Docker コンテナへの Tenable Nessus の導入を推奨していません。

> **注意:** Tenable Nessus はストレージボリュームをサポートしていません。したがって、新しい Tenable Nessus イメージをデプロイするとデータが失われ、Tenable Nessus の再設定が必要になります。ただし、新しいイメージをデプロイする際、次の手順のステップ 2 に従って、初期ユーザーとリンク情報を環境変数を使って設定できます。

始める前に

- ご使用のオペレーティングシステム用の Docker をダウンロードして、インストールします。
- https://hub.docker.com/r/tenable/nessus から Tenable Nessus Docker イメージにアクセスします。

Docker イメージとして Tenable Nessus をデプロイするには

1. ターミナルで、`docker pull` コマンドを使用してイメージを取得します。

   ```
   $ docker pull tenable/nessus:<version-OS>
   ```

   <version-OS> タグで、Tenable Nessus バージョンと、Oracle Linux 8 または Ubuntu のどちらを使用するかを指定する必要があります。特定の Tenable Nessus バージョンの代わりに `latest` タグを使用することもできます (例: `latest-ubuntu`)。

2. `docker run` コマンドを使用してイメージを実行します。

   - 演算子の説明に従って、デプロイメントに適切なオプションを指定して演算子を使用します。
   - Tenable Nessus を事前に設定するには、環境変数の説明に従って、`-e` 演算子を使用して環境変数を設定します。

     > **注意:** Tenable では、イメージを実行する際に、環境変数を使用して Tenable Nessus のインスタンスを設定することを推奨しています。アクティベーションコード、ユーザー名、パスワード、リンクキー (管理 Tenable Nessus スキャナーを作成する場合) などの環境変数を含めない場合、これらの項目をあとから設定する必要があります。

3. ブラウザで Tenable Nessus を開きます。

- リモートでインストールされた Tenable Nessus インスタンスにアクセスするには、**https://<remote IP address>:8834** (例: https://111.49.7.180:8834) にアクセスします。
- ローカルにインストールされている Tenable Nessus インスタンスにアクセスするには、**https:/</localhost>:8834** にアクセスします。

4. ブラウザで残りの Tenable のインストール手順を実行します。環境変数を指定しなかった場合は、コマンドラインインターフェースまたは Tenable Nessus 設定ウィザードで残りの設定手順を実行します。

Docker イメージとしての Tenable Nessus を停止および削除する方法

- コンテナを停止および削除するには、Docker コンテナとして Tenable Nessus を削除するを参照してください。

演算子

演算子	説明
`--name`	Docker でコンテナの名前を設定します。
`-d`	コンテナをデタッチモードで起動します。
`-p`	指定されたポートに *host port*:*container port* の形式で公開します。デフォルトでは、ポートは 8834:8834 です。 複数の Tenable Nessus コンテナが実行中の場合は、別のホストポートを使用します。Tenable Nessus がポート 8834 でリッスンしているため、コンテナポートは 8834 である必要があります。
`-e`	環境変数に前置されます。 Tenable Nessus インスタンスの設定の変更を行うために設定できる環境変数の説明については、環境変数を参照してください。

環境変数

必須およびオプションの環境変数は、Tenable Nessus ライセンス、および Tenable Vulnerability Management にリンクしているかどうかによって異なります。次の項目をクリックして、環境変数を確認します。

Tenable Vulnerability Management にリンクされている Tenable Nessus イメージのデプロイ

変数	必須	説明
USERNAME (ユーザー名)	○	Administrator ユーザーを作成します。
PASSWORD	○	ユーザーのパスワードを作成します。
リンクオプション		
LINKING_KEY	○	Manager から取得したリンクキー。
NAME	×	Manager に表示される Tenable Nessus スキャナーの名前。デフォルトでは、名前はコンテナ ID です。
MANAGER_HOST	×	Manager のホスト名または IP アドレスデフォルトでは、ホスト名は cloud.tenable.com です。
MANAGER_PORT	×	Manager のポート。デフォルトでは、ポートは 443 です。
GROUPS	×	スキャナーを追加する単一のグループ、またはコンマ区切りのグループリスト。グループ名は、大文字と小文字が区別されます。
プロキシオプション		
PROXY	×	プロキシサーバーのホスト名または IP アドレス。
PROXY_PORT	×	プロキシサーバーのポート番号。
PROXY_USER	×	プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。
PROXY_PASS	×	プロキシユーザーとして指定したユーザーアカウントのパスワード。
Tenable Nessus 設定		
AUTO_UPDATE	×	Tenable Nessus が自動的に更新を受け取るかどうかを設定します。 有効な値は次のとおりです。

		• all – (デフォルト) プラグインと Tenable Nessus ソフトウェアを自動的に更新します。 • プラグイン – プラグインのみを更新します。 • no – ソフトウェアとプラグインを自動的に更新しません。

例: 管理される Tenable Nessus スキャナーが Tenable Vulnerability Management にリンクされている

```
docker run --name "nessus-managed" -d -p 8834:8834 -e LINKING_KEY=<Tenable
Vulnerability Management linking key> -e USERNAME=admin -e PASSWORD=admin -e MANAGER_
HOST=cloud.tenable.com -e MANAGER_PORT=443 tenable/nessus:<version-OS>
```

Tenable Security Center にリンクされている Tenable Nessus イメージのデプロイ

変数	必須	説明
USERNAME (ユーザー名)	○	Administrator ユーザーを作成します。
PASSWORD	○	ユーザーのパスワードを作成します。
リンクオプション		
SC_MANAGED	○	**yes** に設定した場合、コンテナを Tenable Security Center モードで起動します。イメージを Tenable Security Center 管理スキャナーとしてデプロイするには、この演算子を含める必要があります。
NAME	×	Manager に表示される Tenable Nessus スキャナーの名前。デフォルトでは、名前はコンテナ ID です。
プロキシオプション		
PROXY-HOST	×	プロキシサーバーのホスト名または IP アドレス。
PROXY-PORT	×	プロキシサーバーのポート番号。
PROXY-	×	プロキシサーバーへのアクセスと使用が許可されているユーザー

USERNAME		アカウント名。
PROXY-PASSWORD	×	プロキシユーザーとして指定したユーザーアカウントのパスワード。
PROXY-AGENT	×	ユーザーエージェント名 (プロキシで事前定義されているユーザーエージェントが必要な場合)。

例: 管理される Tenable Nessus スキャナーが Tenable Security Center にリンクされている

```
docker run --name "nessus-managed" -d -p 8834:8834 -e SC_MANAGED=yes -e USERNAME=admin
tenable/nessus:<version-OS>
```

Tenable Nessus Professional イメージのデプロイ

変数	必須	説明
ACTIVATION_CODE	○	Tenable Nessus を登録するためのアクティベーションコード。
USERNAME (ユーザー名)	○	Administrator ユーザーを作成します。
PASSWORD	○	ユーザーのパスワードを作成します。

例: Tenable Nessus Professional

```
docker run --name "nessus-pro" -d -p 8834:8834 -e ACTIVATION_CODE=<activation code> -e
USERNAME=admin -e PASSWORD=admin tenable/nessus:<version-OS>
```

その他の Tenable Nessus イメージのデプロイ

変数	必須	説明
USERNAME (ユーザー名)	×	Administrator ユーザーを作成します。
PASSWORD	×	ユーザーのパスワードを作成します。

Tenable Agents のインストール

Tenable Agents のインストールプロセスを始める前に、Tenable Nessus Manager ユーザーインターフェースからエージェントのリンクキーを取得する必要があります。

リンクキーの取得後、*Tenable Agent ユーザーガイド*で説明されている手順を使用してエージェントをインストールし、Tenable Nessus Manager にリンクします。

エージェントがインストールまたはリンクされると、Tenable Agents は 0 ~ 5 分のランダムな遅延の後に Tenable Nessus Manager にリンクされます。遅延を強制すると、大量のエージェントをデプロイまたは再起動する際のネットワークトラフィックを削減し、Tenable Nessus Manager に対する負荷を軽減できます。リンクされたエージェントは、接続時に、マネージャーからプラグインを自動的にダウンロードします。このプロセスには数分かかる場合があります。これはエージェントがスキャン結果を返すのに必要なプロセスです。

Tenable Nessus リンクキーの取得

を使用する場合に必要なユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Agents のインストールプロセスを始める前に、Tenable Nessus Manager からエージェントのリンクキーを取得する必要があります。

注意: `nessuscli` からエージェントリンクキーを取得することもできます。詳細については、nessuscli Fix コマンドセクションの `nessuscli fix --secure --get agent_linking_key` を参照してください。

エージェントのリンクキーを取得する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. (オプション) **リンクキー**を変更するには、リンクキーの横にある ボタンをクリックします。

   次の場合は、リンクキーを変更してもかまいません。

   - リンクキーを再生成していて、以前のリンクキーに戻したい場合
   - 大規模デプロイメントスクリプトにリンクキーを事前定義したい場合

注意: リンクキーは 64 文字の英数字文字列である必要があります。

3. **リンクキー**を記録するかコピーします。

次の手順

- Tenable Nessus のインストールとリンク。

Tenable Nessus Manager にエージェントをリンクする

Tenable Agent のインストール後、エージェントを Tenable Nessus Manager にリンクします。

始める前に

- Tenable Nessus Manager からリンクキーを取得します。
- Tenable Agent をインストールします。

Tenable Agent を Tenable Nessus Manager にリンクする方法

1. コマンドターミナルから Tenable Agent にログインします。
2. エージェントのコマンドプロンプトで、サポートされている引数を使用して `nessuscli agent link` コマンドを使用します。

   たとえば、次のようになります。

Linux

```
/opt/nessus_agent/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
```

macOS

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
```

Windows

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
```

次の表に、nessuscli agent link でサポートされている引数を示します。

引数	必須	値
--key	○	マネージャーから取得したリンクキー。
--host	○	Tenable Nessus Manager インストール中に設定した静的IPアドレスまたはホスト名。
--port	○	8834 またはカスタムポート。
--name	×	エージェントの名前。エージェントの名前を指定しない場合、名前はエージェントをインストールしているコンピューターの名前にデフォルト設定されます。
--ca-path	×	マネージャーのサーバー証明書の検証に使用するカスタム CA 証明書。
--groups	×	エージェントを追加する 1 つ以上のエージェントグループ。インストール中にエージェントグループを指定しない場合は、リンクされたエージェントを後で Tenable Nessus Manager 内のエージェントグループに追加できます。 コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。 例: --groups="Atlanta,Global Headquarters" **注意:** エージェントグループ名は、大文字と小文字を区別し、正確に一致する必要があります。エージェントグループ名は引用符で囲む必要があります (例: --groups="My Group")。

引数	必須	値
`--offline-install`	×	有効にすると、エージェントはオンラインでない場合でも、定期的に Tenable Nessus Manager へのリンクを試行します。エージェントがコントローラーに接続できない場合、1 時間ごとに再試行します。コントローラーには接続できるがリンクに失敗する場合は、24 時間ごとに再試行します。 このフラグを使用しない場合、エージェントは即座に Tenable Nessus Manager とのリンクを試行します (エージェントは 1 回のみ試行)。
`--proxy-host`	×	プロキシサーバーのホスト名または IP アドレス。
`--proxy-port`	×	プロキシサーバーのポート番号。
`--proxy-password`	×	ユーザー名として指定したユーザーアカウントのパスワード。
`--proxy-username`	×	プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。
`--proxy-agent`	×	ユーザーエージェント名 (プロキシで事前定義されているユーザーエージェントが必要な場合)。

Tenable Nessus の設定

ブラウザで Tenable Nessus にアクセスすると、接続プライバシーの問題、信頼できないサイト、安全でない接続、または関連するセキュリティ証明書の問題に関する警告が表示されます。これは正常な動作です。Tenable Nessus は、自己署名 SSL 証明書を提供します。

SSL 警告のバイパスに必要な手順については、セキュリティ警告セクションを参照してください。

> **注意**：お使いの環境によっては、プラグインの設定と初期化に数分かかる場合があります。

Tenable Core + Tenable Nessus を設定するには、*Tenable Core+ Tenable Nessus ユーザーガイド*のTenable Core のデプロイまたはインストールを参照してください。

始める前に

- Tenable Nessus のインストール.

Tenable Nessus を設定する方法

1. Tenable Nessus のインストールの手順に従って、ブラウザで **[Welcome to Nessus]** (Nessus へようこそ) ページを開きます。
2. **[Welcome to Nessus]** (Nessus へようこそ) ページで、次の操作を行います。
   - (オプション) Tenable Nessus をインターネットに接続してインストールできない場合は、**[Register Offline]** (オフラインで登録する) を選択します。
   - (オプション) **[Settings]** (設定) をクリックし、次の Tenable Nessus 設定を手動で行います。
     - プロキシサーバー - プロキシサーバーを設定します。

       > **注意:** プロキシサーバーを介して Tenable Nessus スキャナーをリンクする場合は、プロキシサーバーを入力する必要があります。後からユーザーインターフェースでプロキシ接続を設定することもできます。詳細は、プロキシサーバーおよびリモートリンクを参照してください。

     - プラグインフィード - Tenable Nessus プラグインフィードのカスタムホストを入力します。Tenable Nessus は、オフラインモードの場合、プラグインフィードとやり取りしません。
     - 暗号化パスワード - Tenable Nessus 暗号化パスワードを入力します。ユーザーインターフェースでユーザーを作成すると、Tenable Nessus で暗号化パスワードの使用が必須になります。

       暗号化パスワードを設定すると、Nessus はすべてのポリシー、スキャンの結果、スキャンの設定を暗号化します。Tenable Nessus の再起動時にパスワードを入力する必要があります。

       > **警告:** 暗号化パスワードを紛失した場合、管理者または Tenable サポート では暗号化パスワードを回復できません。

   > **ヒント:** これらの設定は、後でユーザーインターフェースで行うこともできます。

   完了したら、**[Save]** (保存) をクリックして設定を保存し、**[Welcome to Nessus]** (Nessus へようこそ) ページに戻ります。
3. **[Continue]** (続行) をクリックします。

新しい **[Welcome to Nessus]** (Nessus へようこそ) ページが表示されます。

4. 次のいずれかを行います。

    - Tenable Nessus をオンラインでインストールする場合は、選択した製品の設定手順に従います。

        - Tenable Nessus Essentials、Professional、Expert、Manager をインストールする
        - Tenable Nessus Professional または Tenable Nessus Expert の試用版をアクティブにする
        - Tenable Vulnerability Management にリンクする
        - Tenable Security Center にリンクする
        - Tenable Nessus Manager にリンクする
        - ノードをリンクする (Tenable Nessus Manager クラスタ)

    - Tenable Nessus をオフラインでインストールする場合は、Tenable Nessus をオフラインでインストールするのステップ 1 に進みます。

Tenable Nessus Essentials、Professional、Expert、Manager をインストールする

このオプションでは、スタンドアロンバージョンの Tenable Nessus Essentials、Nessus Professional、Tenable Nessus Expert、または Nessus Manager をインストールします。インストール中、Nessus のアクティベーションコードを入力する必要があります。このアクティベーションコードにより、インストールされる製品が決まります。

Nessus 試用版のアクティベーションの詳細については、Tenable Nessus Professional または Tenable Nessus Expert の試用版をアクティブにするを参照してください。

Tenable Nessus を Tenable Nessus Essentials、Tenable Nessus Professional、Tenable Nessus Expert、または Tenable Nessus Manager として設定するには、以下を実行します。

1. Nessus インストールのブラウザ部分を実行中に、[Welcome to Nessus] (Nessus へようこそ) ページで **[Continue]** (続行) をクリックします。次に、2 番目の **[Welcome to Nessus]** (Nessus へようこそ) 画面で、次のいずれかを行います。

- **[Set up a Nessus purchase]** (Nessus 購入のセットアップ) を選択して、次の Nessus バージョンのいずれかをインストールします。
  - **Nessus Professional** - セキュリティ実践者向けの事実上の業界標準である脆弱性評価ソリューション。
  - **Nessus Expert** - DX 時代のアタックサーフェスに対応した、業界をリードする脆弱性評価ソリューション。
  - **Nessus Manager** - Tenable Agents を大規模に管理するためのエンタープライズソリューション。
- **[Register for Nessus Essentials]** (Nessus Essentials に登録する) を選択して Tenable Nessus Essentials (教育関係者、学生、一般ユーザー向け無料版 Nessus) をインストールします。

2. **[Continue]** (続行) をクリックします。
   - **[Set up a Nessus purchase]** (Nessus 購入のセットアップ) を選択した場合は、**[Login]** (ログイン) ページが表示されます。次のいずれかを行います。
     - アクティベーションコードが必要な場合
       a. **[Login]** (ログイン) ページで、メールとパスワードを入力します。
       b. **[Continue]** (続行) をクリックします。メールアドレスと Tenable カスタマー ID が記載された **[Activate Product]** (製品のアクティベート) ページが表示されます。
       c. ドロップダウンメニューで、アクティベートする製品とアクティベーションコードを選択します。
       d. **[Activate Product]** (製品のアクティベート) をクリックします。**[License Information]** (ライセンス情報) ページが表示されます。
       e. **[Continue]** (続行) をクリックします。**[Create a user account]** (ユーザーアカウントの作成) 画面が表示されます。
       f. 手順 5 でプロセスを続行します。

- すでにアクティベーションコードを入手している場合は、**[Skip]** (スキップ) をクリックします。

- **[Register for Nessus Essentials]** (Nessus Essentials に登録する) を選択した場合は、**[Get an activation code]** (アクティベーションコードの取得) 画面が表示されます。次のいずれかを行います。

  - アクティベーションコードが必要な場合

    a. **[Get an activation code]** (アクティベーションコードの取得) 画面で、名前とメールアドレスを入力します。

    b. **[Email]** (E メール) をクリックします。

    c. メールをチェックして無料のアクティベーションコードを入手します。

  - すでにアクティベーションコードを入手している場合は、**[Skip]** (スキップ) をクリックします。

[Register Nessus] (Nessus の登録) ページが表示されます。

3. **[Register Nessus]** (Nessus の登録) 画面で、**アクティベーションコード**を入力します。

   アクティベーションコードは、アクティベーションメールまたはTenableダウンロードページから入手したコードです。

4. **[Continue]** (続行) をクリックします。

   [Create a user account] (ユーザーアカウントの作成) 画面が表示されます。

5. Tenable Nessus へのログインに使用する Tenable Nessus 管理者のユーザーアカウントを次の手順で作成します。

   a. **[Username]** (ユーザー名) ボックスにユーザー名を入力します。

   b. **[Password]** (パスワード) ボックスにユーザーアカウントのパスワードを入力します。

   > **注意:** パスワードには Unicode 文字は使用できません。

6. **[Submit]** (送信) をクリックします。

   Tenable Nessus が設定プロセスを完了します。これには数分かかる場合があります。

7. 作成した管理者ユーザーアカウントを使用して、Tenable Nessus に**サインイン**します。

注意: 初めて Tenable Nessus にサインインすると、「*Plugins are compiling.Tenable Nessus functionality will be limited until compilation is complete.*」(プラグインはコンパイル中です。コンパイルが完了するまで Tenable.Nessus の機能は限定されます。) というメッセージが表示されます。Tenable Nessus によるプラグインのコンパイル中は、スキャンの作成や起動、ポリシーまたはプラグインルールの表示や作成、アップグレードアシスタントの使用はできません。

Tenable Nessus Professional または Tenable Nessus Expert の試用版をアクティブにする

次のトピックでは、Tenable Nessus Professional または Tenable Nessus Expert の 7 日間の試用版をアクティブにする方法について説明します。

ヒント: アクティベーション時にユーザーアカウントを作成し忘れた場合は、adduser nessuscli コマンドでアカウントを作成できます。

Tenable Nessus Professional または Tenable Nessus Expert の試用版をアクティブにする方法

1. **[Welcome to Nessus]** (Nessus へようこそ) 画面で、アクティブにする Tenable Nessus の試用版を選択します。
   - **Nessus Expert の試用版を開始する**
   - **Nessus Professional の試用版を開始する**
2. **[Continue]** (続行) をクリックします。

   [Get Started] (はじめる) ページが表示されます。
3. 次のいずれかを行います。
   - **Tenable コミュニティアカウントや、試用版のアクティベーションコードをお持ちでない場合:**

     a. Tenable コミュニティアカウントに接続するメールアドレスを入力します。

     b. **[続行]** をクリックします。Tenable により、入力したメールアドレス宛てに確認メールが送信されます。

        - メールアドレスが Tenable Nessus により認識されない場合は、**[Create Account]** (アカウントを作成) ページが表示されます。

i. 新しいアカウントの情報を入力します。

- メールアドレスが Tenable Nessus により認識される場合は、Tenable Nessus がアカウントを検出したことを通知するページが表示されます。

c. **[Start Trial]** (試用版を開始) をクリックします。

[メールの検証] ページが表示されます。

d. 選択したメールアドレスの受信トレイに移動します。

e. **[メールアドレスの確認]** メッセージを開きます。

f. メッセージ内の **[Verify Your Email Address]** リンクをクリックします。

g. Tenable Nessus **[メールの検証]** ページに戻ります。

h. **[検証]** をクリックします。

[Trial License Information] (ライセンス情報) ページが表示され、アクティベーションコードと試用版の終了日が表示されます。Tenable では、アクティベーションコードを安全な場所に記録することを推奨しています。

i. **[続行]** をクリックします。

[Create a user account] (ユーザーアカウントの作成) 画面が表示されます。

j. Tenable Nessus へのログインに使用する Tenable Nessus 管理者のユーザーアカウントを次の手順で作成します。

a. **[Username]** (ユーザー名) ボックスにユーザー名を入力します。

b. **[Password]** (パスワード) ボックスにユーザーアカウントのパスワードを入力します。

> **注意:** パスワードには Unicode 文字は使用できません。

k. **[Submit]** (送信) をクリックします。

Tenable Nessus によって設定プロセスが完了し、ユーザーインターフェースに自動的にサインインします。

> **注意:** 初めて Tenable Nessus にサインインすると、「*Plugins are compiling.Tenable Nessus functionality will be limited until compilation is complete.*」(プラグインはコンパイル中です。コンパイルが完了するまで Tenable.Nessus の機能は限定されます。) というメッセージが表示されます。Tenable Nessus によるプラグインのコンパイル中は、スキャンの作成や起動、ポリシーまたはプラグインルールの表示や作成、アップグレードアシスタントの使用はできません。

- **Tenable コミュニティアカウントと試用版のアクティベーションコードをすでにお持ちの場合:**

  a. **[Skip]**をクリックします。

  b. プロンプトに従ってアカウントにサインインし、アクティベーションコードを送信します。

  Tenable Nessus によって設定プロセスが完了し、ユーザーインターフェースに自動的にサインインします。

  > **注意:** 初めて Tenable Nessus にサインインすると、「*Plugins are compiling.Tenable Nessus functionality will be limited until compilation is complete.*」(プラグインはコンパイル中です。コンパイルが完了するまで Tenable.Nessus の機能は限定されます。) というメッセージが表示されます。Tenable Nessus によるプラグインのコンパイル中は、スキャンの作成や起動、ポリシーまたはプラグインルールの表示や作成、アップグレードアシスタントの使用はできません。

Tenable Vulnerability Management にリンクする

Tenable Nessus は初期インストール時にリモートスキャナーとして Tenable Vulnerability Management にリンクできます。初期インストール時にスキャナーをリンクしない場合は、後で Tenable Nessus スキャナーをリンクできます。Tenable Nessus を Tenable Vulnerability Management にリンクすると、解除するまでリンクしたままになります。

> **注意:** ファイヤーウォールでドメイン許可リストを使用する場合、Tenable では許可リストに *.cloud.tenable.com (ワイルドカード文字入り) を追加することを推奨しています。こうすることで、スキャナーが Tenable Vulnerability Management との通信に使用する sensor.cloud.tenable.com との通信が確実に可能になります。

> **注意:** 中国本土にある Tenable Nessus スキャナー、Tenable Agents、Tenable Web App Scanning スキャナー、または Tenable Network Monitor (NNM) を介して Tenable Vulnerability Management に接続している場合は、sensor.cloud.tenable.com ではなく sensor.cloud.tenablecloud.cn で接続する必要があります。

始める前に

- Tenable Nessus の設定の説明に従って Tenable Nessus を設定します。
- Tenable Nessus スキャナーが Tenable Vulnerability Management、Tenable Security Center、または Tenable Nessus Manager にリンクされているか、または以前にリンクされていた場合は、スキャナーのリンクを解除するか、`nessuscli fix --reset-all` コマンドを実行する必要があります (詳細については、修正コマンドを参照してください)。
- Tenable Nessus スキャナーリンクキーを表示してコピーします。リンクキーは、次のプロセスのステップ 4 で必要になります。Tenable Vulnerability Management のメニューの **[Settings]** (設定) > **[Sensors]** (センサー) > **[Linked Scanners]** (リンクされたスキャナー) > ⊕ **[Add Nessus Scanner]** (Nessus スキャナーを追加する) から表示することができます。

Tenable Nessus ユーザーインターフェースから Tenable Nessus を Tenable Vulnerability Management にリンクする方法

1. **[Welcome to Nessus]** (Nessus へようこそ) 画面で、**[Link Nessus to another Tenable product]** (Nessus を別の Tenable 製品にリンクする) を選択します。
2. **[Continue]** (続行) をクリックします。

   [Managed Scanner] (管理スキャナー) 画面が表示されます。
3. **[Managed by]** (管理者) ドロップダウンボックスから **[Tenable Vulnerability Management]** を選択します。
4. **[Linking Key]** (リンクキー) ボックスに、Tenable Vulnerability Management インスタンスのリンクキーを入力します。

   > **注意**: Tenable Nessus のスキャナーリンクキーは、Tenable Vulnerability Management の **[Add Nessus Scanner]** (Nessus スキャナーを追加する) メニューにあります (**[Settings]** (設定) > **[Sensors]** (センサー) > **[Linked Scanners]** (リンクされたスキャナー) > ⊕ **[Add Nessus Scanner]** (Nessus スキャナーを追加する))。
5. **[続行]** をクリックします。

   [Create a user account] (ユーザーアカウントの作成) 画面が表示されます。
6. Tenable Nessus へのログインに使用する Tenable Nessus 管理者のユーザーアカウントを次の手順で作成します。

a. **[Username]** (ユーザー名) ボックスにユーザー名を入力します。

b. **[Password]** (パスワード) ボックスにユーザーアカウントのパスワードを入力します。

> **注意:** パスワードには Unicode 文字は使用できません。

7. **[Submit]** (送信) をクリックします。

   Tenable Nessus が設定プロセスを完了します。これには数分かかる場合があります。

8. 作成した管理者ユーザーアカウントを使用して、Tenable Nessus に**サインイン**します。

コマンドラインインターフェース (CLI) から Tenable Nessus を Tenable Vulnerability Management にリンクする方法

過去に Tenable Nessus を登録またはリンクした場合は、Tenable Vulnerability Management にリンクする前に Tenable Nessus をリセットする必要があります。

オペレーティングシステムに応じて以下のコマンドを実行して、Tenable Nessus をリセットし、Tenable Vulnerability Management にリンクします。以下のコマンドで必要になるリンクキーを取得するには、*Tenable Vulnerability Management ユーザーガイド*の[センサーをリンクする]を参照してください。

> **注意:** 以下の手順で `--reset-all` コマンドを使用すると、既存のユーザー、データ、設定がすべて削除されます。Tenable ではリセットを行う前に、スキャンデータをエクスポートしてバックアップを作成するようお勧めしています。詳細は、[Tenable Nessus のバックアップ方法]を参照してください。

Linux

> **注意:** リンクコマンドを正常に実行するには、root またはそれ以上のアクセス許可が必要です。

1. Linux CLI を開きます。
2. リスト順に次のコマンドを実行します。

```
# service nessusd stop
```

```
# cd /opt/nessus/sbin
```

```
# ./nessuscli fix --reset-all
```

3. 次のいずれかを行います。

   - Tenable Vulnerability Management FedRAMP サイトにリンクしている場合は、次の link コマンドを実行してください。

     ```
     # /opt/nessus/sbin/nessuscli managed link --key=<key> --
     host=fedcloud.tenable.com --port=443
     ```

   - FedRAMP サイトにリンクしていない場合は、次の link コマンドを実行してください。

     ```
     # ./nessuscli managed link --key=<LINKING KEY> --cloud
     ```

     ヒント: `managed link` コマンドにオプションのパラメーターを追加することで設定できるスキャナーオプションが多数あります (スキャナー名、カスタム CA パス、プロキシサーバー情報など)。詳細は、管理対象スキャナーコマンドを参照してください。

4. 次のリンクコマンドを実行してください。

   ```
   # service nessusd start
   ```

Windows

注意: リンクコマンドを正常に実行するには、管理者レベルのアクセス許可が必要です。

1. Windows CLI を開きます。
2. リスト順に次のコマンドを実行します。

   ```
   net stop "tenable nessus"
   ```

   ```
   cd C:\Program Files\Tenable\Nessus
   ```

   ```
   nessuscli fix --reset-all
   ```

3. 次のいずれかを行います。

   - Tenable Vulnerability Management FedRAMP サイトにリンクしている場合は、次の link コマンドを実行してください。

     ```
     C:\Program Files\Tenable\Nessus\nessuscli.exe managed link --
     key=<key> --host=fedcloud.tenable.com --port=443
     ```

   - FedRAMP サイトにリンクしていない場合は、次の link コマンドを実行してください。

     ```
     nessuscli managed link --key=<LINKING KEY> --cloud
     ```

     ヒント: managed link コマンドにオプションのパラメーターを追加することで設定できるスキャナーオプションが多数あります (スキャナー名、カスタム CA パス、プロキシサーバー情報など)。詳細は、管理対象スキャナーコマンドを参照してください。

4. 次のコマンドを実行します。

   ```
   net start "tenable nessus"
   ```

macOS

注意: リンクコマンドを正常に実行するには、管理者レベルのアクセス許可が必要です。

1. ターミナルを開きます。
2. リスト順に次のコマンドを実行します。

   ```
   # launchctl unload -w
   /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

   ```
   # /Library/Nessus/run/sbin/nessuscli fix --reset-all
   ```

3. 次のいずれかを行います。

- Tenable Vulnerability Management FedRAMP サイトにリンクしている場合は、次の link コマンドを実行してください。

```
# /Library/Nessus/run/sbin/nessuscli managed link --key=<key> --
host=fedcloud.tenable.com --port=443
```

- FedRAMP サイトにリンクしていない場合は、次の link コマンドを実行してください。

```
# /Library/Nessus/run/sbin/nessuscli managed link --key=<LINKING
KEY> --cloud
```

ヒント: `managed link` コマンドにオプションのパラメーターを追加することで設定できるスキャナーオプションが多数あります (スキャナー名、カスタム CA パス、プロキシサーバー情報など)。詳細は、管理対象スキャナーコマンドを参照してください。

4. 次のコマンドを実行してください。

```
# launchctl load -w
/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
```

Tenable Nessus Manager にリンクする

注意: Tenable Security Centerで Tenable Agent 管理用にデプロイされている場合、Tenable Nessus Manager はリンクしている Tenable Nessus スキャナーをサポートしません。

Tenable Nessus は初期インストール時にリモートスキャナーとして Tenable Nessus Manager にリンクできます。初期インストール時にスキャナーをリンクしない場合は、後で Tenable Nessus スキャナーをリンクできます。

注意: Nessus を Tenable Nessus Manager にリンクすると、解除するまでリンクしたままになります。

始める前に

- Tenable Nessus の設定の説明に従って Tenable Nessus を設定します。
- Tenable Nessus スキャナーが Tenable Vulnerability Management、Tenable Security Center、または Tenable Nessus Manager にリンクされているか、または以前にリンクされていた場合は、ス

キャナーのリンクを解除するか、`nessuscli fix --reset-all` コマンドを実行する必要があります (詳細については、修正コマンドを参照してください)。

Tenable Nessus Manager に Nessus をリンクする方法

1. **[Welcome to Nessus]** (Nessus へようこそ) 画面で、**[Link Nessus to another Tenable product]** (Nessus を別の Tenable 製品にリンクする) を選択します。
2. **[Continue]** (続行) をクリックします。

   [Managed Scanner] (管理スキャナー) 画面が表示されます。
3. **[Managed by]** (管理者) ドロップダウンボックスから **[Nessus Manager (Scanner)]** (Nessus Manager (スキャナー)) を選択します。
4. **[Host]** (ホスト) ボックスに、Tenable Nessus Manager のホストを入力します。
5. **[Port]** (ポート) ボックスに、Tenable Nessus Manager のポートを入力します。
6. **[Linking Key]** (リンクキー) ボックスに、Tenable Nessus Manager のリンクキーを入力します。
7. **[Continue]** (続行) をクリックします。

   [Create a user account] (ユーザーアカウントの作成) 画面が表示されます。
8. Tenable Nessus へのログインに使用する Tenable Nessus 管理者のユーザーアカウントを次の手順で作成します。
   a. **[Username]** (ユーザー名) ボックスにユーザー名を入力します。
   b. **[Password]** (パスワード) ボックスにユーザーアカウントのパスワードを入力します。

   > **注意:** パスワードには Unicode 文字は使用できません。
9. **[Submit]** (送信) をクリックします。

   Tenable Nessus が設定プロセスを完了します。これには数分かかる場合があります。
10. 作成した管理者ユーザーアカウントを使用して、Tenable Nessus に**サインイン**します。

Tenable Security Center にリンクする

Tenable Nessus は初期インストール時にリモートスキャナーとして Tenable Security Center にリンクできます。初期インストール時にスキャナーをリンクしない場合は、後で Tenable Nessus スキャナーをリンクできます。

注意： Tenable Nessusを Tenable Security Center にリンクすると、解除するまでリンクしたままになります。

注意: Tenable Security Center は、リンクされた Nessus Manager にプラグインを送信しません。Nessus Manager は、Tenable のプラグインサイトからプラグインを直接プルします。したがって、プラグインセットを更新するには、Nessus Manager がインターネットおよび Tenable のプラグインサイトにアクセスする必要があります (詳細については、Which Tenable sites should I allow? (許可する必要がある Tenable のサイト) というコミュニティ記事を参照してください)。Nessus Manager がインターネットにアクセスできない場合は、そのバージョンとプラグインをオフラインで手動で更新できます (詳細については、Nessus をオフラインで管理するを参照してください)。

始める前に

- Tenable Nessus の設定の説明に従って Tenable Nessus を設定します。
- Tenable Nessus スキャナーが Tenable Vulnerability Management、Tenable Security Center、または Tenable Nessus Manager にリンクされているか、または以前にリンクされていた場合は、スキャナーのリンクを解除するか、`nessuscli fix --reset-all` コマンドを実行する必要があります (詳細については、修正コマンドを参照してください)。

Tenable Security Center に Nessus をリンクする方法

1. **[Welcome to Nessus]** (Nessus へようこそ) で、**[Link Nessus to another Tenable product]** (Nessus を別の Tenable 製品にリンクする) を選択します。
2. **[Continue]** (続行) をクリックします。

   [Managed Scanner] (管理スキャナー) 画面が表示されます。
3. **[Managed by]** ドロップダウンボックスから **[Tenable.sc]** を選択します。
4. **[Continue]** (続行) をクリックします。

   [Create a user account] (ユーザーアカウントの作成) 画面が表示されます。
5. Tenable Nessus へのログインに使用する Tenable Nessus 管理者のユーザーアカウントを次の手順で作成します。

a. **[Username]** (ユーザー名) ボックスにユーザー名を入力します。

b. **[Password]** (パスワード) ボックスにユーザーアカウントのパスワードを入力します。

> **注意:** パスワードには Unicode 文字は使用できません。

6. **[Submit]** (送信) をクリックします。

   Tenable Nessus が設定プロセスを完了します。これには数分かかる場合があります。

7. 作成した管理者ユーザーアカウントを使用して、Tenable Nessus に**サインイン**します。

次の手順

- *Tenable Security Center ユーザーガイド*の Nessus スキャナーを追加するの説明に沿って、Tenable Nessus スキャナーを Tenable Security Center に追加します。

アクティベーションコードを管理する

> **注意:** Tenable Nessus では、インストールプロセス中にアクティベーションコードを生成できます。詳細は、Tenable Nessus Essentials、Professional、Expert、Manager をインストールするを参照してください。

次のトピックでは、Tenable Nessus のライセンス情報を提供します。

Tenable Nessus のライセンシング

Tenable Nessus を Tenable Vulnerability Management または Tenable Security Center で管理することも、スタンドアロンのサブスクリプション製品として実行することもできます。サブスクリプションを購入してアクティベーションコードを受け取るには、Tenable のウェブサイトにアクセスするか、Tenable パートナーにご連絡ください。

Tenable Nessus アクティベーションコード

Tenable Nessus をサブスクリプションモードで使用するには、プラグインフィードのアクティベーションコードが必要です。このコードで、ユーザーがインストールして使用できるように Tenable がライセンス付与した Tenable Nessus のバージョンが特定されます。該当する情報がある場合は、スキャンできる IP アドレスの数、Tenable Nessus にリンクできるリモートスキャナーの数、Tenable Nessus Manager にリンクできる Tenable Agents の数も特定されます。Tenable Nessus Manager のライセンスは、デプロイメントサイズ、特に大規模デプロイメントや多数の Tenable Nessus Manager インスタンスを含むデプロイメントに固有です。担当の Tenable Customer Success Manager と要件について話し合ってください。

アクティベーションコードには、次の特徴があります。

- **ワンタイム**コードです。ただし、ライセンスまたはサブスクリプションが変更された場合は、Tenable が新しいアクティベーションコードを発行します。または、既存のアクティベーションコードを別のシステムに転送することもできます。詳細については、アクティベーションコードを転送するを参照してください。
- 発行後 24 時間以内に、Tenable Nessus のインストールで使用する必要があります。
- 複数のスキャナーで共有することはできません。
- 大文字と小文字が区別されません。
- Tenable Nessus のオフライン管理に必要です。

  注意: Tenable Nessus のオフラインでの管理については、Tenable Nessus をオフラインで管理するを参照してください。

注意: アクティベーションコードの取得方法と使用方法については、アクティベーションコードを取得 のページを参照してください。

Tenable Nessus を Tenable Vulnerability Managementで管理する

Tenable Vulnerability Management を使用して Tenable Nessus スキャナーを管理している場合、プラグインとソフトウェアの更新は Tenable Vulnerability Management から管理します。詳細は、*Tenable Nessus ユーザーガイド*の Tenable Nessus プラグインとソフトウェアの更新を参照してください。

Tenable Vulnerability Management には、無制限の Tenable Nessus スキャナーをデフォルトのコンポーネントとしてリンクする機能があります。

Tenable Vulnerability Management ライセンスの詳細については、*Tenable ライセンスガイド*の Tenable Vulnerability Management ライセンスを参照してください。

Tenable Nessus を Tenable Security Centerで管理する

Tenable Security Center を使用して Tenable Nessus スキャナーを管理している場合、アクティベーションコードとプラグインの更新は Tenable Security Center から管理します。詳細は、*Tenable Nessus ユーザーガイド*の Tenable Nessus プラグインとソフトウェアの更新を参照してください。

Tenable Security Center と通信する前に Tenable Nessus を起動する必要がありますが、通常、有効なアクティベーションコードとプラグインがないと起動しません。この要件を無視して Tenable Nessus を起動させ、Tenable Security Center から情報を取得できるようにするには、スキャナーを登録するときに **[Managed by SecurityCenter]** (SecurityCenterによる管理) を選択します。

Tenable Security Center ライセンスの詳細については、*Tenable ライセンスガイド*の Tenable Security Center ライセンスを参照してください。

アクティベーションコードを管理するには、次のトピックを利用してください。

- アクティベーションコードを表示する
- アクティベーションコードを更新する
- アクティベーションコードを転送する

アクティベーションコードを表示する

Tenable コミュニティで表示する

Tenable Community ガイドの説明に従い、Tenableコミュニティサイトでアクティベーションコードを表示します。

Tenable Nessus で表示する

1. Tenable Nessus にログインします。
2. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。
3. **[Overview]** (概要) タブで、**[Activation Code]** (アクティベーションコード) を表示します。

注意: Tenable Nessus スキャナーを使用している場合、[About] (バージョン情報) ページのライセンスの有効期限とアクティベーションコードの値は **[N/A]** と表示されます。

コマンドラインから表示する

オペレーティングシステム固有の `nessuscli fetch --code-in-use` コマンドを使用する。

Platform	コマンド
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --code-in-use`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --code-in-use`
Linux	`# /opt/nessus/sbin/nessuscli fetch --code-in-use`

アクティベーションコードを更新する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

新しいライセンスを対応するアクティベーションコードとともに受け取った場合、新しいアクティベーションコードを Tenable Nessus に登録する必要があります。

注意: Tenable Nessus をオフラインで使用している場合は、Tenable Nessus をオフラインで管理する を参照してください。

ユーザーインターフェース

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。
2. **[Overview]** (概要) タブで、アクティベーションコードの横にある ボタンをクリックします。
3. アクティベーションコードを入力し、**[Activate]** (アクティブにする) をクリックします。

   これで Tenable Nessus インスタンスのライセンスがアクティブになりました。

注意: Tenable Nessus スキャナーを使用している場合、[About] (バージョン情報) ページのライセンスの有効期限とアクティベーションコードの値は **[N/A]** と表示されます。

コマンドラインインターフェース

1. Tenable Nessus を実行しているシステムで、コマンドプロンプトを開きます。
2. お使いのオペレーティングシステム固有の `nessuscli fetch --register <Activation Code>` コマンドを実行します。

Platform (プラットフォーム)	コマンド
Linux	`# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx`
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register xxxx-xxxx-xxxx-xxxx`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --register`

	`xxxx-xxxx-xxxx-xxxx`

Tenable Nessus は、Tenable Nessus エンジンと最新の Tenable Nessus プラグインをダウンロードおよびインストールした後、再起動します。

> **注意**：最新の更新を自動的にダウンロードまたはインストールせずに Tenable Nessus を登録するには、コマンド `nessuscli fetch --register-only` を使用します。

アクティベーションコードを転送する

> **を使用する場合に必要な [ユーザーロール]Tenable Nessus Manager:** 管理者またはシステム管理者

Tenable Nessus Professional と Tenable Nessus Expert では、1 つのアクティベーションコードを複数のシステムで使用できます。これにより、アクティベーションコードを毎回リセットすることなく、システム間で Tenable Nessus ライセンスを簡単に転送できます。

アクティベーションコードをシステムに転送すると、そのシステムはそのライセンスの Tenable Nessus のアクティブなインスタンスになります。最後にアクティブ化したシステムだけがプラグイン更新を受信できます。そのアクティベーションコードを持つ Tenable Nessus の過去のインスタンスはすべて機能しますが、プラグインの更新は受信できません。非アクティブなインスタンスでは、次のエラーメッセージが表示されます。**ライセンスコードが無効または転送されたため、フィードへのアクセスが拒否されました。**

アクティベーションコードを転送するには、Tenable Nessusのアクティブインスタンスを作成するシステムで、次のいずれかの手順を実行します。

Nessus ユーザーインターフェース

新しい Tenable Nessus インスタンスをアクティブ化

1. お使いのオペレーティングシステムに適した手順に従い、[をインストールします Tenable Nessus] 。
2. ブラウザでシステムにアクセスします。
3. **[Create an account]** (アカウントを作成する) ウィンドウで、ユーザー名とパスワードを入力します。
4. **[Continue]** (続行) をクリックします。
5. **[Register your scanner]** (スキャナーを登録する) ウィンドウの **[Scanner Type]** (スキャナーの種類) ドロップダウンボックスで、**Tenable Nessus Essentials**、**Nessus Professional**、**Nessus**

Manager から選択します。

6. **[Activation Code]** (アクティベーションコード) ボックスに、アクティベーションコードを入力します。
7. **[続行]** をクリックします。

   Tenable Nessus がインストールプロセスを完了します。これには数分かかる場合があります。インストールが完了すると、ライセンスが Tenable Nessusのこのインスタンスでアクティブになります。

既存の Tenable Nessus インスタンスの更新

1. Tenable Nessusをアクティブ化するシステムにアクセスします。
2. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。
3. **[Overview]** (概要) タブで、アクティベーションコードの横にある ボタンをクリックします。
4. アクティベーションコードを入力し、**[Activate]** (アクティブにする) をクリックします。

   これで Tenable Nessus インスタンスのライセンスがアクティブになりました。

注意: Tenable Nessus スキャナーを使用している場合、[About] (バージョン情報) ページのライセンスの有効期限とアクティベーションコードの値は **[N/A]** と表示されます。

コマンドラインインターフェース

root ユーザーで次の手順を実行するか、root 以外のユーザーで sudo を使用します。

1. Tenable Nessusをアクティブ化するシステムで、コマンドプロンプトを開きます。
2. お使いのオペレーティングシステム固有の `nessuscli fetch --register <Activation Code>` コマンドを実行します。

Platform (プラットフォーム)	コマンド
Linux	`# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx`

Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register xxxx-xxxx-xxxx-xxxx`

Tenable Nessus は、Nessus エンジンと最新の Nessus プラグインをダウンロードおよびインストールした後、再起動します。

Tenable Nessus プラグインとソフトウェアの更新

以降のトピックでは、設定とライセンスタイプに基づく、Tenable Nessus のプラグインとソフトウェアの更新の受信方法について説明します。Tenable Nessus プラグインとソフトウェアは、初期セットアップ時の設定に応じて更新方法が異なります。

Tenable Nessus の設定	プラグインのアップデート	ソフトウェアの更新
Tenable Nessus スタンドアロンインストール	スタンドアロンの Tenable Nessus は、デフォルトで plugins.nessus.org からプラグインを毎日自動的に受信するよう設定されています。 **[Settings]** (設定) > **[About]** (製品情報) ページに移動し、**[Last Updated]** (最終更新日) セクションの横にある ↻ をクリックして、手動更新をトリガーすることもできます。同じセクションで、現在インストールされているプラグインセットを確認できます。	Tenable Nessus は、デフォルトで downloads.nessus.org から自動的にソフトウェア更新プログラムを受信します。次の条件が満たされていれば、更新プログラムが利用可能になると、Tenable Nessus ユーザーインターフェースの上部にバナーが表示されます。 • 自動更新が設定されていない • 自動更新は設定されているが、Tenable Nessus がダウンロードしたバージョンは、ダウンロードを完了するためにサービスの再起動が必要 自動更新を設定する方法については、Tenable Nessus ソフトウェアを更新するを参照してください。
Tenable Nessus オフラインインストール	オフラインデバイスの場合、プラグインを手動でインストールする必要があります。詳細は、プラグインをオフラインで更新するを参照	オフラインデバイスの場合、Tenable Nessus がインストールされているオペレーティングシステムに応じたアップグレード方法で、Tenable Nessus ソフトウェアを手

	してください。	動でアップグレードする必要があります。詳細は、Update Tenable Nessus Manager Plugins on an Offline System を参照してください。
Tenable Security Center が管理する Tenable Nessus	Tenable Nessus は Tenable Security Center からプラグインを受信します。Tenable Security Center は 15 分ごとに Tenable Nessus にチェックインし、Tenable Nessus のプラグインセットが Tenable Security Center のセットと一致するかどうかを確認します。一致しない場合は、Tenable Security Center が新しいプラグインセットを提供します。	Tenable Security Center が管理する Tenable Nessus スキャナーのソフトウェアは、自動的に更新されません。唯一の例外は、Tenable Nessus が Tenable Core にインストールされ、自動更新が有効になっている場合です。
Tenable Vulnerability Management にリンクされた Tenable Nessus	Tenable Vulnerability Management にリンクされたデバイスは、cloud.tenable.com からプラグインを受信します。	Tenable Nessus にリンクされた Tenable Vulnerability Management は、cloud.tenable.com から自動的にソフトウェア更新プログラムを受信します。Tenable Nessus は、デフォルトで 24 時間に 1 回 Tenable Vulnerability Management にチェックインして、コアソフトウェアの更新の有無を確認します。
Tenable Nessus Manager が管理する Tenable Agents	Tenable Agents は Tenable Nessus Manager からプラグインを受信します。デプロイ後、エージェントが Tenable Nessus Manager インスタンスからプラグインセット一式をダウンロードします。プラグインセット一式のダウンロード以降は、プラグインセットが	Tenable Agents は Tenable Nessus Manager からソフトウェア更新プログラムを受信します。エージェントは、デプロイされた時間に応じて 24 時間ごとにチェックインし、コアソフトウェアの更新の有無を確認します。エージェントホストがオフになっているなど、通常の更新時間にエージェントがオフラインの場合は、オンラインに戻ったときにソフトウェアの更新をチェック

	5 日以上古くならない限り、エージェントがマネージャーから差分プラグインセットをダウンロードします。	します。以降は、これがエージェントの新しい更新時間となります。
Tenable Vulnerability Management が管理する Tenable Agents	Tenable Agents は Tenable Vulnerability Management からプラグインを受信します。 エージェントは、スキャン用のプラグインセットが必要になるまで、プラグインセットがないままです。エージェントが初めてスキャンする必要がありエージェントにプラグインセットがない場合、エージェントはリクエストされたスキャンタイプに必要なプラグインセット (完全な脆弱性プラグインセットまたはインベントリプラグインセット) をダウンロードします。 最初のスキャンの後、エージェントプラグインセットのいずれかと Tenable Vulnerability Management プラグインセットの差が 15 日以内である場合、エージェントは差分プラグインアップデートを実行します。 また、エージェントプラグインセットのいずれかと Tenable Vulnerability Management プラグインセットの差が 15 日より長い場合、エージェントはフルプラグインアップデートを実行します。 エージェントは、設定可能な時	Tenable Agents は Tenable Vulnerability Management からソフトウェア更新プログラムを受信します。エージェントは、デプロイされた時間に応じて 24 時間ごとにチェックインし、コアソフトウェアの更新の有無を確認します。エージェントホストがオフになっているなど、通常の更新時間にエージェントがオフラインの場合は、オンラインに戻ったときにソフトウェアの更新をチェックします。以降は、これがエージェントの新しい更新時間となります。

	間が経過すると、未使用のプラグインセットを削除します (詳細については、`days_to_keep_unused_plugins` の詳細設定を参照してください)。時間の経過後、エージェントは未使用のプラグインセットを削除します。	

Tenable Nessus をオフラインで管理する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Tenable Nessus をオフラインで管理するには、コンピューターが 2 台必要です。1 台はインターネットに接続されていない Tenable Nessus のサーバー、もう 1 台はインターネットに接続されているコンピューターです。次の手順に従って、オフライン Tenable Nessus サーバーを管理します。

- Tenable Nessus をオフラインでインストールする
- ライセンスをオフラインで更新する
- プラグインをオフラインで更新する
- Update Tenable Nessus Manager Plugins on an Offline System
- 監査ウェアハウスを手動で更新する

Tenable Nessus をオフラインでインストールする

Tenable Nessus **オフライン**登録は、Tenable Nessus を実行しているコンピューターのうち、インターネットに接続されていないものに適しています。

Tenable Nessus のプラグインを最新の状態に保つため、次の手順を使用して、インターネットに接続されていない Tenable Nessus サーバーを登録します。

このプロセスでは、コンピューターを 2 台使用する必要があります。1 台は Tenable Nessus をインストールした、インターネットに接続されていないコンピューターで、もう 1 台はインターネットに接続されているコンピューターです。

以下の説明では、コンピューター **A** (オフライン Tenable Nessus サーバー) と **B** (オンラインコンピューター) を例として使用します。

注意: Tenable Nessus Essentials はオフラインインストールをサポートしていません。

Tenable Nessus のインストール

1. Nessus インストールのブラウザ部分で表示される **[Welcome to Nessus]** (Nessus へようこそ) ページで、**[Register Offline]** (オフラインで登録する) を選択します。
2. **[Continue]** (続行) をクリックします。
3. デプロイする Tenable Nessus タイプを Tenable Nessus Expert、Tenable Nessus Professional、Tenable Nessus Manager、管理スキャナーから選択します。
4. **[Continue]** (続行) をクリックします。
5. (管理スキャナーのみ) 管理スキャナーを選択すると、**[Managed Scanner]** (管理スキャナー) ページが表示されます。
    a. **[Managed by]** (以下による管理) で、Tenable Nessus をリンクする製品を選択します。
    b. **[Linking Key]** (リンクキー) に、リンクキーを入力します。
    c. **[Continue]** (続行) をクリックします。
6. 一意の**チャレンジコード**が表示されます。以下の例のチャレンジコードは、**aaaaaa11b2222cc33d44e5f6666a777b8cc99999** です。

ライセンスを生成する

1. インターネットアクセスのあるシステム (B) で、Nessus オフライン登録ページに移動します。
2. 上部フィールドで、**[Nessus Product Registration]** (Nessus 製品登録) 画面に表示されたチャレンジコードを入力します。

    チャレンジコードの例: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

3. 次に、プロンプトが表示されたら、Tenable Nessus アクティベーションコードを入力します。

   アクティベーションコードの例: AB-CDE-1111-F222-3E4D-55E5-CD6F

4. **[Submit]** (送信) ボタンをクリックします。

   次の要素が含まれるオフライン更新ページが表示されます。

   - **カスタム URL** – 表示されるカスタム URL では、圧縮されたプラグインファイルがダウンロードされます。このファイルは Nessus がプラグイン情報を取得するために使用されます。この URL はお客様の Nessus ライセンスに固有のものです。プラグインの更新が必要なたびに、保存して、使用される必要があります。

     警告: Tenable では、先に進む前に**カスタム URL** を保存することをお勧めします。この URL は登録後に一度しか表示されません。登録ウィンドウを閉じた後に URL を忘れた場合、登録プロセスを再度開始して新しい URL を生成する必要があります。

   - **ライセンス** – 文字列全体が Nessus の製品ライセンス情報になります。文字列は、**-----BEGIN Tenable, Inc. LICENSE-----** で始まり、**-----END Tenable, Inc. LICENSE-----** で終わります。Tenable ではこのテキスト文字列を使用して、製品ライセンスと登録を確認しています。

   - **nessus.license** ファイル – ライセンステキスト文字列が含まれる埋込ファイルがウェブページの最下部にあります。

最新のプラグインをダウンロードしてコピーする

1. インターネットに接続しているコンピューター (**B**) を引き続き使用しながら、**カスタム URL** を選択します。

   圧縮された TAR ファイルがダウンロードされます。

2. TAR 圧縮ファイルを Nessus **オフライン** (**A**) システムにコピーします。

   お使いのオペレーティングシステムに固有のディレクトリを使用します。

Platform (プラットフォーム)	コマンド
Windows	`C:\Program Files\Tenable\Nessus`
macOS	`# /Library/Nessus/run/sbin/`

Platform (プラットフォーム)	コマンド
Linux	`# /opt/nessus/sbin/`

ライセンステキストのコピーと貼り付け

1. インターネットに接続しているコンピューター (B) を引き続き使用し、**-----BEGIN Tenable, Inc. LICENSE-----** で始まり、**-----END Tenable, Inc. LICENSE-----** で終わるテキスト文字列全体をコピーします。
2. Nessus をインストールしているコンピューター (A) で、**[Nessus Product Registration]** (Nessus 製品登録) 画面に、**-----BEGIN Tenable, Inc. LICENSE-----** で始まり、**-----END Tenable, Inc. LICENSE-----** で終わるテキスト文字列全体を貼り付けます。
3. **[Continue]** (続行) を選択します。

   Tenable Nessus がインストールプロセスを終了します。これには数分かかる場合があります。
4. 設定時に作成したシステム管理者アカウントを使用して、Tenable Nessus に**サインイン**します。

ライセンスをオフラインで更新する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

オフラインの既存の Tenable Nessus サーバーが存在し、新しいライセンスで Tenable Nessus を更新する場合は、次の手順を使用します。この手順を使用して、新しいライセンスと既存のライセンスをアップデートできます。

Tenable Nessus をオフラインで管理するには、コンピューターが 2 台必要です。1 台はインターネットに接続されていない Tenable Nessus のサーバー、もう 1 台はインターネットに接続されているコンピューターです。

オフラインの Tenable Nessus サーバーのライセンスを更新する方法

1. Tenable Nessus を実行しているオフラインのシステムで Tenable Nessus チャレンジコードを生成します 。

   オフライン更新操作を実行する前に、Tenable Nessus サーバーで一意のチャレンジコードを生成することが必要になる場合があります。

インターネットに接続した状態で Tenable Nessus 操作を実行するときにはアクティベーションコードが使用されますが、オフライン操作を実行するときにはライセンスが使用されます。生成されたチャレンジコードにより、ライセンスを表示し、オフライン操作に使用することができます。

次のいずれかの手順を使用して、チャレンジコードを生成します。

- **Tenable Nessus ユーザーインターフェースでチャレンジコードを生成する**

  a. Tenable Nessus を実行しているオフラインシステムで、Tenable Nessus にログインします。

  b. **[Settings]** (設定) をクリックします。

  c. アクティベーションコードの横にある鉛筆アイコンをクリックします。

  [Update Activation Code] (アクティベーションコードを更新する) ウィンドウが表示されます。

  d. **[Registration]** (登録) ドロップダウンメニューで、**[Offline]** (オフライン) を選択します。

  e. **[Activate]** (アクティブにする) をクリックします。

  チャレンジコードがウィンドウに表示されます。

  f. 英数字のチャレンジコードをマシンにコピーします。

  チャレンジコードの例: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

- **コマンドラインインターフェースからチャレンジコードを生成する**

  a. Tenable Nessus を実行しているオフラインシステムで、コマンドプロンプトを開きます。

  b. お使いのオペレーティングシステム固有の `nessuscli fetch --challenge` コマンドを使用します。

プラットフォーム	コマンド
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --challenge

macOS	# /Library/Nessus/run/sbin/nessuscli fetch --challenge
Linux	# /opt/nessus/sbin/nessuscli fetch --challenge

c. 英数字のチャレンジコードをマシンにコピーします。

チャレンジコードの例: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

2. Tenable Nessus を実行しているオフラインシステムで Tenable Nessus アクティベーションコードをコピーします。

Tenable Nessus ライセンスを生成するには、アクティベーションコードを入力する必要があります。アクティベーションコードを表示するには、次のいずれかの手順を使用します。

- **Nessus ユーザーインターフェースでアクティベーションコードを表示する**

1. Tenable Nessus にログインします。
2. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。
3. **[Overview]** (概要) タブで、**[Activation Code]** (アクティベーションコード) を表示します。

   アクティベーションコードをマシンにコピーします。

- **コマンドラインインターフェースでアクティベーションコードを表示する**

オペレーティングシステム固有の `nessuscli fetch --code-in-use` コマンドを使用します。

Platform	コマンド
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --code-in-use`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --code-in-use`

Platform	コマンド
Linux	`# /opt/nessus/sbin/nessuscli fetch --code-in-use`

アクティベーションコードをマシンにコピーします。

3. インターネットに*接続しているシステム*の Tenable Nessus ユーザーインターフェースでライセンスを生成します。

   デフォルトでは、Tenable Nessus をインストールすると、ライセンスは非表示になり、自動的に登録されます。このライセンスは表示できません。

   ただし、Tenable Nessus サーバーがインターネットに接続されていない (つまり、オフラインである) 場合は、ライセンスを生成する必要があります。このライセンスはお客様の Tenable Nessus 製品に固有のものであり、共有できません。

   ライセンスは、英数字の文字列を含むテキストベースのファイルです。ライセンスは、一意のチャレンジコードに基づいて作成されます。

   Nessus ユーザーインターフェースでライセンスを生成する

   a. インターネットに*接続しているシステム*で、Tenable Nessus オフライン登録ページに移動します。

   b. プロンプトが表示されたら、チャレンジコードを入力します。

      チャレンジコードの例: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

   c. 次に、プロンプトが表示されたら、Tenable Nessus アクティベーションコードを入力します。

      アクティベーションコードの例: AB-CDE-1111-F222-3E4D-55E5-CD6F

   d. **[Submit]** (送信) を選択します。

      その結果、ウェブページの最下部に、ライセンスのテキスト文字列を含む埋め込みの `nessus.license` ファイルが表示されます。

4. インターネットに*接続しているシステム*で、ライセンスファイル (`nessus.license`) をダウンロードしてコピーします。

   Tenable Nessus ライセンスを生成したら、ライセンスをダウンロードし、Tenable Nessus を実行しているオフラインシステムにコピーする必要があります。

ライセンスファイルをダウンロードしてコピーする

a. Tenable Nessus オフライン登録ページでインターネットに接続しているコンピューターを引き続き使用しながら、画面上の [nessus.license] リンクを選択します。

このリンクをクリックすると、nessus.license ファイルがダウンロードされます。

b. nessus.license ファイルを、Tenable Nessus を実行しているシステムにコピーします。

お使いのオペレーティングシステムに固有のディレクトリを使用します。

Platform (プラットフォーム)	ディレクトリ
Windows	C:\ProgramData\Tenable\Nessus\conf
macOS	# /Library/Nessus/run/etc/nessus
Linux	# /opt/nessus/etc/nessus/

5. Tenable Nessus を実行しているオフラインシステムにライセンスを登録します。

nessus.license ファイルをダウンロードして、Tenable Nessus のオフラインサーバーにコピーしたら、お使いのオペレーティングシステムに対応する nessuscli fetch -- register コマンドを使用します。

ライセンスをオフラインで登録する

a. Tenable Nessus を実行しているオフラインシステムで、コマンドラインインターフェースを開きます。

b. お使いのオペレーティングシステム固有の nessuscli fetch --register-offline コマンドを使用します。

Platform (プラットフォーム)	コマンド
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register-offline "C:\ProgramData\Tenable\Nessus\conf\nessus.license"

macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --register-offline /Library/Nessus/run/etc/nessus/nessus.license`
Linux	`# /opt/nessus/sbin/nessuscli fetch --register-offline /opt/nessus/etc/nessus/nessus.license`

プラグインをオフラインで更新する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

この手順を使用して、既存のオフライン Tenable Nessus サーバーのプラグインを更新します。次の手順では、Tenable Nessus をオフラインでインストールする の手順がすでに完了していることを想定しています。

注意: Tenable は、このプロセスをオフラインの Tenable Nessus インスタンスを更新する場合にのみ使用することを推奨しています。Tenable Nessus のすべてのオンラインインスタンスが、自動プラグイン更新を受け取ります。Tenable Nessus インスタンスがプラグイン更新を受け取る方法については、プラグインや、次の Tenable ナレッジベースの記事を参照してください。

注意: Tenable Nessus がオフラインのときは、Tenable Nessus Expert ウェブアプリケーションスキャンプラグインを更新できません。

オフラインの Tenable Nessus インスタンスにプラグインを更新する方法

1. インターネットに接続しているコンピューターを使用して、最初の Tenable Nessus ライセンス生成プロセスで保存した**カスタム URL** を開きます。

   Tenable Nessus プラグイン TAR ファイルが、お使いのマシンにダウンロードされます。

2. 次のいずれかを行います。

   Tenable Nessus ユーザーインターフェースを介して、プラグイン TAR ファイルをインストールする

   a. オフライン Tenable Nessus システム上の Tenable Nessus ユーザーインターフェースの上部ナビゲーションバーで、**[Settings]** (設定) をクリックします。

      [About] (製品情報) ページが表示されます。

   b. **[Software Update]** (ソフトウェア更新) タブをクリックします。

c. 右上隅にある **[Manual Software Update]** (手動ソフトウェア更新) ボタンをクリックします。

[Manual Software Update] (手動ソフトウェア更新) ダイアログボックスが表示されます。

d. **[Manual Software Update]** (ソフトウェアを手動で更新する) ダイアログボックスで、**[Upload your own plugin archive]** (プラグインのアーカイブからアップロードする) を選択してから、**[Continue]** (続行) を選択します。

e. ダウンロードされた TAR 圧縮ファイルの場所に移動し、選択してから、**[Open]** (開く) をクリックします。

Tenable Nessus がアップロードされたプラグインで更新されます。

コマンドラインインターフェースを介して、プラグイン TAR ファイルをインストールする

a. 圧縮された TAR ファイルを *オフライン* Tenable Nessus システムにコピーします。

お使いのオペレーティングシステムに固有のディレクトリを使用します。

Platform (プラットフォーム)	コマンド
Windows	`C:\Program Files\Tenable\Nessus`
macOS	`# /Library/Nessus/run/sbin/`
Linux	`# /opt/nessus/sbin/`

b. オフライン システムで、コマンドプロンプトを開きます。

c. お使いのオペレーティングシステムに固有の `nessuscli update <tar.gz file name>` コマンドを使用します。

Platform (プラットフォーム)	コマンド
Windows	「`C:\Program Files\Tenable\Nessus\nessuscli.exe`」更新`<tar.gz file name>`
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz file name>`

Platform (プラットフォーム)	コマンド
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz file name>`

Update Tenable Nessus Manager Plugins on an Offline System

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

次の手順を使用して、Tenable Nessus Manager 親ノードがその子ノードに提供するプラグインを更新します。詳細は、クラスタリング を参照してください。

Tenable Nessus Managerでオフラインシステムのプラグインを更新する場合、2 通りの方法があります。

- **オプション 1:**Tenable Nessus Manager ユーザーインターフェースで **Manual Software Update** 機能を使用します。
- **オプション 2:** コマンドラインインターフェースと `nessuscli update` コマンドを使用します。

オプション 1: ユーザーインターフェースを介した手動ソフトウェア更新

1. ファイル `nessus-updates-x.x.x.tar.gz` (x.x.x はバージョン番号) を https://jp.tenable.com/downloads/nessus からダウンロードします。
2. Tenable Nessus Manager (**A**) を実行している **オフライン**システムの上部ナビゲーションバーで、[**Settings] (設定)**を選択します。
3. 左側のナビゲーションメニューから、**[Software Update]** (ソフトウェアの更新) を選択します。
4. **[Manual Software Update] (ソフトウェアの手動更新)**を選択します。
5. **[Manual Software Update]** (ソフトウェアを手動で更新する) ダイアログボックスで、**[Upload your own plugin archive]** (プラグインのアーカイブからアップロードする) を選択してから、**[Continue]** (続行) を選択します。
6. 圧縮された TAR ファイルをダウンロードしたディレクトリに移動します。
7. 圧縮された TAR ファイルを選択し、**[Open]** (開く) を選択します。

   Tenable Nessus Manager がアップロードされたプラグインで更新されます。

オプション 2: コマンドラインから更新する

1. ファイル `nessus-updates-x.x.x.tar.gz` (x.x.x はバージョン番号) を https://jp.tenable.com/downloads/nessus からダウンロードします。
2. Tenable Nessus Manager を実行している**オフライン**システム (A) で、コマンドプロンプトを開きます。
3. お使いのオペレーティングシステムに固有の `nessuscli update <tar.gz file name>` コマンドを使用します。

Platform (プラットフォーム)	コマンド
Windows	`C:\Program Files\Tenable\Nessus\nessuscli.exe update<tar.gz file name>`
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz file name>`
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz file name>`

監査ウェアハウスを手動で更新する

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** System Administrator

現在公開されている監査をすべて含んでいる監査ウェアハウスは、Tenable Nessus の新しいバージョンへのアップグレード時に、自動的に更新されます。Tenable Nessus の新しいバージョンにアップグレードすることなく、監査ウェアハウスを更新するために、オフライン更新を実行することができます。

始める前に

- Tenable監査 ページから監査ウェアハウスのアーカイブファイルをダウンロードします。

Tenable Nessus ユーザーインターフェースを使用して監査ウェアハウスを手動で更新する方法

> **注意:** Tenable Vulnerability Management または Tenable Security Center が管理するスキャナーを更新する場合は、この手順は使用できません。

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. **[Software Update]** (ソフトウェア更新) タブをクリックします。

3. 右上隅にある **[Manual Software Update]** (手動ソフトウェア更新) ボタンをクリックします。

   [Manual Software Update] (手動ソフトウェア更新) ダイアログボックスが表示されます。

4. **[Manual Software Update]** (手動ソフトウェア更新) ダイアログボックスで、**[Upload your own plugin archive]** (プラグインのアーカイブからアップロードする) を選択してから、**[Continue]** (続行) をクリックします。

5. ダウンロードした TAR 圧縮ファイルの場所に移動し、選択して、**[Open]** (開く) をクリックします。

   Tenable Nessus がアップロードされた監査ファイルを使用して更新します。

コマンドラインインターフェースを使用して監査ウェアハウスを手動で更新する方法

1. Tenable Nessus を実行しているシステムで、コマンドプロンプトを開きます。

2. お使いのオペレーティングシステムに固有の `nessuscli update <tar.gz file name>` コマンドを使用します。

Platform (プラットフォーム)	コマンド
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz file name>`
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz file name>`
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz file name>`

   Tenable Nessus がアップロードされた監査ファイルを使用して更新します。

Tenable Nessus と Tenable Agents のアップグレード

このセクションには、サポートされているすべてのオペレーティングシステムで Tenable Nessus と Tenable Agents をアップグレードするための情報が含まれます。

- Nessus をアップグレードする
    - 評価版からのアップグレード
    - Tenable Nessus ソフトウェアを更新する
    - macOS で Nessus をアップグレードする
    - Linux で Nessus をアップグレードする
    - Windows で Nessus をアップグレードする
- Tenable Agent のアップデート
- Tenable Nessus ソフトウェアのダウングレード

Nessus をアップグレードする

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** System Administrator

このセクションでは、Nessus の更新とアップグレードの方法について説明します。

- Tenable Nessus ソフトウェアを更新する
- 評価版からのアップグレード
- Linux で Nessus をアップグレードする
- Windows で Nessus をアップグレードする
- macOS で Nessus をアップグレードする

評価版からのアップグレード

Nessus の評価版から Tenable Nessus のフルライセンスバージョンにアップグレードする場合は、**[About]** (製品情報) タブの **[Settings]** (設定) ページで、フルバージョンのアクティベーションコードを入力します。

> **注意:** Tenable Nessus スキャナーを使用している場合、[About] (バージョン情報) ページのライセンスの有効期限とアクティベーションコードの値は **[N/A]** と表示されます。

アクティベーションコードを更新するには:

1. **[Activation Code]** (アクティベーションコード) の横にある ボタンを選択します。
2. **[Registration]** (登録) ボックスで、お使いの Nessus の種類を選択します。
3. **[Activation Code]** (アクティベーションコード) ボックスに、新しいアクティベーションコードを入力します。
4. **[Activate]** (アクティブにする) をクリックします。

   Nessus は、Nessus エンジンと最新の Nessus プラグインをダウンロードおよびインストールした後、再起動します。

アクティベーションコードの表示、リセット、更新、転送の詳細については、アクティベーションコードを管理するを参照してください。

Tenable Nessus ソフトウェアを更新する

注意: Tenable Nessus スキャナーを管理するオフラインの Tenable Nessus Manager 親ノードのアップグレードに関する詳細は、Update Tenable Nessus Manager Plugins on an Offline Systemを参照してください。

管理者ユーザーは、Tenable Nessus がソフトウェアコンポーネントとプラグインを更新する方法を設定できます。Nessus の更新設定をして Nessus のバージョンとプラグインを自動的に更新することも、Nessus のバージョンとプラグインを手動で更新することもできます。

Tenable Nessus ソフトウェアの更新設定を設定する方法

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。
2. **[Software Update]** (ソフトウェア更新) タブをクリックします。
3. (Tenable Nessus Professional、Tenable Nessus Expert、Tenable Nessus Manager のみ) **[Automatic Updates]** (自動更新) セクションで、次のオプションのいずれかを選択します。

   - **Update all components** (すべてのコンポーネントを更新): Tenable Nessus が自動的にソフトウェアとエンジンを更新し、最新のプラグインセットをダウンロードします。

     Tenable Nessus Professional および管理対象の Tenable Nessus スキャナーでは、Tenable Nessus は **[Nessus Update Plan]** (Nessus 更新プラン) の設定に従ってソフトウェアのバージョンを更新します。

- **Update plugins** (プラグインの更新): Tenable Nessus が自動的に最新のプラグインセットをダウンロードします。
- **Disabled** (無効): Tenable Nessus は自動更新を実行しません。

4. (Tenable Nessus Professional および Tenable Nessus Expert のみ) 自動更新を有効にしている場合は、**[Update Frequency]** (更新頻度) セクションで次のいずれかの操作を行います。
   - 標準の更新間隔を設定するには、ドロップダウンボックスから **[Daily]** (日)、**[Weekly]** (週)、または **[Monthly]** (月) を選択します。
   - カスタムの更新頻度を時間単位で設定するには、ボタンをクリックして、時間数を入力します。
5. (Tenable Nessus Professional、Tenable Nessus Expert、および Tenable Vulnerability Management が管理する Tenable Nessus スキャナーのみ) **[Nessus Update Plan]** (Nessus 更新プラン) を設定して、Tenable Nessus が自動的にアップデートするバージョンを指定します。

   注意: 更新プランを変更して自動更新を有効にすると、選択したプランに相当するバージョンと合わせるために、Tenable Nessus が即座に更新する場合があります。Tenable Nessus はバージョンのアップグレードまたはダウングレードのいずれかを行う場合があります。

オプション	説明
Update to the latest GA release (最新の GA リリースに更新する) (デフォルト)	最新バージョンが一般公開 (GA) され次第、自動的に最新の Tenable Nessus バージョンへと更新されます。 **注意:** この日付はバージョンが一般公開された日と同じ日付です。
Opt in to Early Access releases (早期アクセス用リリースを選択する)	最新バージョンが早期アクセス (EA) 用にリリースされ次第、自動的に最新の Tenable Nessus バージョンへと更新します。通常一般公開よりも数週間早いタイミングです。
Delay updates, staying on an older release (更新を遅ら	自動的に最新の Tenable Nessus バージョンに更新しません。Tenable が設定した旧バージョンの Tenable Nessus の状態を維持します。これは通常、最新の一般公開バージョンよりも 1 リリース

せ、古いリリースを維持する)	前のものとなりますが、8.10.0 よりも前のバージョンにはなりません。Tenable Nessus の新しいバージョンがリリースされると、Tenable Nessus インスタンスのソフトウェアバージョンは更新されますが、最新のリリースよりも前のバージョンに留まります。

6. (オプション) Tenable Support に指示された場合にのみ、**[Update Server]** ボックスに Tenable Nessus がプラグインをダウンロードするサーバーを入力します。
7. **[保存]** ボタンをクリックします。

   Tenable Nessus は、設定に従って入手可能な更新を自動的にダウンロードします。

更新を手動でダウンロードする方法

注意: Tenable Vulnerability Management または Tenable Security Center が管理するスキャナーを更新する場合は、この手順は使用できません。

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。
2. **[Software Update]** (ソフトウェア更新) タブをクリックします。
3. 右上隅にある **[Manual Software Update]** (ソフトウェアを手動で更新する) をクリックします。

   ウィンドウが表示されます。
4. ウィンドウで次のオプションのいずれかを選択します。

   - **Update all components** (すべてのコンポーネントを更新): Tenable Nessus が Nessus のソフトウェアとエンジンを更新し、最新のプラグインセットをダウンロードします。

     Tenable Nessus Professional と Tenable Nessus Expert では、Tenable Nessus は **Nessus 更新プラン**の設定に従ってソフトウェアのバージョンを更新します。

     注意: 更新プランを変更すると、選択したプランに相当するバージョンと合わせるために、Tenable Nessus が即座に更新する場合があります。Nessus は、バージョンのアップグレードとダウングレードのどちらも行う可能性があります。
   - **Update plugins** (プラグインの更新): Tenable Nessus が最新のプラグインセットをダウンロードします。

- **Upload your own plugin archive** (プラグインのアーカイブからアップロードする): ご自身がアップロードしたファイルから Tenable Nessus がプラグインをダウンロードします。

5. **[Continue]** (続行) ボタンをクリックします。
6. **[Upload your own plugin archive]** (プラグインのアーカイブからアップロードする) を選択した場合は、ファイルを参照して選択します。

   Tenable Nessus で入手可能な更新をダウンロードします。

Linux で Nessus をアップグレードする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Nessus をダウンロードする

Tenable ダウンロードページから、Nessus の最新のフルライセンスバージョンをダウンロードします。

ヒント: Tenable Nessusのオフラインインスタンスをアップグレードする場合は、オンラインシステムでパッケージをダウンロードし、所属組織の推奨方法を使用してオフラインインスタンスに転送します。

コマンドを使用して Nessus をアップグレードする

コマンドプロンプトから、Nessus アップグレードコマンドを実行します。

注意: アップグレードコマンドを実行すると、Nessus は自動的に nessusd を停止します。

Red Hat 6 と 7、CentOS 6 と 7、Oracle Linux 6 と 7

```
# yum upgrade Nessus-<version number and OS>.rpm
```

Red Hat 8 以降、CentOS 8 以降、Oracle Linux 8 以降、Fedora

```
# dnf upgrade Nessus-<version number and OS>.rpm
```

SLES/SUSE

```
# zypper in Nessus-<version number and OS>.rpm
```

Debian/Kali と Ubuntu

```
# dpkg -i Nessus-<version number and OS>.deb
```

Nessus デーモンを開始する

コマンドプロンプトから、nessusd デーモンを再起動します。

Red Hat、CentOS、Oracle Linux、Fedora、SUSE

```
# service nessusd start
```

Debian/Kali と Ubuntu

```
# /etc/init.d/nessusd start
```

これで、Linux オペレーティングシステムで Nessus をアップグレードするプロセスが完了しました。

Windows で Nessus をアップグレードする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Nessus をダウンロードする

Tenable ダウンロードページから、Nessus の最新のフルライセンスバージョンをダウンロードします。ダウンロードパッケージは、Nessus ビルドバージョン、お使いのプラットフォーム、プラットフォームバージョン、CPU に固有のものです。

ヒント: Tenable Nessusのオフラインインスタンスをアップグレードする場合は、オンラインシステムでパッケージをダウンロードし、所属組織の推奨方法を使用してオフラインインスタンスに転送します。

Nessus インストーラファイルの例

```
Nessus-<version number>-Win32.msi

Nessus-<version number>-x64.msi
```

Nessus のインストールを開始する

1. Nessus のインストーラをダウンロードしたフォルダーに移動します。
2. 次に、ファイル名をダブルクリックし、インストールのプロセスを開始します。

Windows InstallShield ウィザードを完了する

1. **[Welcome to the InstallShield Wizard for Tenable, Inc. Nessus]** (Tenable Nessus の InstallShield ウィザードへようこそ) 画面で、**[Next]** (次へ) を選択します。
2. **[License Agreement]** (ライセンス契約) 画面で、Tenable, Inc. Nessus ソフトウェアライセンスとサブスクリプション契約の利用条件を読みます。
3. **[I accept the terms of the license agreement]** (ライセンス契約の条件に同意します) オプションを選択し、**[Next]** (次へ) ボタンをクリックします。
4. **[Destination Folder]** (インストール先フォルダー) 画面で、**[Next]** (次へ) ボタンをクリックし、デフォルトのインストール先フォルダーを承認します。または **[Change]** (変更) ボタンを選択し、Nessus を別のフォルダーにインストールします。
5. **[Ready to Install the Program]** (プログラムのインストールの準備完了) 画面で、**[Install]** (インストール) ボタンを選択します。

   [Installing Tenable, Inc. Nessus] (Tenable Nessus のインストール) 画面が表示され、**[Status]** (ステータス) インジケーションバーにアップグレードの進捗状況が示されます。
6. **[Tenable Nessus InstallShield Wizard Completed]** (Tenable Nessus の InstallShield ウィザードの完了) 画面で、**[Finish]** (終了) ボタンを選択します。

   Nessus は、ログインが可能なデフォルトのブラウザで読み込まれます。

macOS で Nessus をアップグレードする

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** System Administrator

Nessus インストール GUI を使用して、masOS で Nessus をアップグレードするプロセスは、新しい Mac インストールと同じです。

> **ヒント:** Tenable Nessusのオフラインインスタンスをアップグレードする場合は、オンラインシステムでパッケージをダウンロードし、所属組織の推奨方法を使用してオフラインインスタンスに転送します。

Tenable Agent のアップデート

エージェントのインストール後、Tenable Nessus Manager はエージェント更新プランに基づいてエージェントソフトウェアを自動的に更新します。エージェント更新プランの設定の詳細については、エージェント更新を参照してください。

注意: エージェント更新プランの使用に加えて、コマンドラインから手動でエージェントを更新できます。詳細については、*Tenable Agent ユーザーガイド*を参照してください。

Tenable Nessus ソフトウェアのダウングレード

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Tenable Nessus は Tenable Nessus を の以前のバージョン Tenable Nessusにダウングレードする機能をサポートしています。

Tenable Nessus ソフトウェアを手動でダウングレードするか、古いリリースに自動的にダウングレードするように **Nessus 更新プラン**を設定できます。

始める前に

- Tenable では、Tenable Nessus バックアップファイルを作成することを推奨しています。
- Tenable Nessus が暗号化パスワードを持っている場合、Tenable Nessus の更新プランを変更してもダウングレードできません。ダウングレードを行う前に Tenable Nessus の暗号化パスワードを削除し、ダウングレード完了後に再び暗号化パスワードを設定します。

  Tenable Nessus 暗号化パスワードを削除するには、ナレッジベースの記事コマンドラインから暗号化パスワード (旧称: マスターパスワード) を削除する方法を参照してください。ダウングレード後に暗号化パスワードの設定 暗号化パスワードを設定するには、Tenable Nessusを参照してください。

Linux または macOS で Tenable Nessus を手動でダウングレードする方法

注意: Windows で Tenable Nessus を手動でダウングレードするには、Tenable サポートに連絡してください。

1. 次のいずれかを実行して、ソフトウェアの自動更新をオフにします。
   - Tenable Nessus ソフトウェアを更新するの説明に従って Tenable Nessus ソフトウェアの更新を変更し、**[Automatic Updates]** (自動更新) を **[Disabled]** (無効) に設定します。
   - 詳細設定の説明に従って、詳細な設定の **[Automatically Update Nessus** (Nessus を自動的にアップデートする) (`auto_update_ui`)] を変更します。
2. ご使用のオペレーティングシステムに応じて、次のいずれかの手順を使用します。

Linux

a. インストールする Tenable Nessus バージョンをダウンロードします。

b. Tenable Nessus バージョンを手動でインストールします。新しい Tenable Nessus `rpm` ファイルを現在の `rpm` ファイルの上に強制的に上書きインストールします。

macOS

a. インストールする Tenable Nessus バージョンをダウンロードします。

b. Tenable Nessus バージョンを手動でインストールします。現在の Tenable Nessus `pkg` ファイルを新しい `pkg` ファイルで置き換えます。

自動ダウングレードするように Tenable Nessus を設定する方法 (Tenable Nessus Professional、Tenable Nessus Expert、および Tenable Vulnerability Management が管理する Tenable Nessus スキャナーのみ)

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. **[Software Update]** (ソフトウェア更新) タブをクリックします。

3. **Nessus 更新プラン**を設定して、Tenable Nessus が自動的にアップデートするバージョンを指定します。自動的にダウングレードするには、**[Delay updates, staying on an older release]** (更新を遅らせ、古いリリースを維持する) を選択します。

   > **注意**：更新プランを変更して自動更新を有効にすると、選択したプランに相当するバージョンと合わせるために、Tenable Nessus が即座に更新する場合があります。Tenable Nessus はバージョンのアップグレードまたはダウングレードのいずれかを行う場合があります。

オプション	説明
Update to the latest GA release (最新の GA リリースに更新する)	最新バージョンが一般公開 (GA) され次第、自動的に最新の Tenable Nessus バージョンへと更新されます。 **注意:** この日付はバージョンが一般公開された日と同じ日付です。

(デフォルト)	
Opt in to Early Access releases (早期アクセス用リリースを選択する)	最新バージョンが早期アクセス (EA) 用にリリースされ次第、自動的に最新の Tenable Nessus バージョンへと更新します。通常一般公開よりも数週間早いタイミングです。
Delay updates, staying on an older release (更新を遅らせ、古いリリースを維持する)	自動的に最新の Tenable Nessus バージョンに更新しません。Tenable が設定した旧バージョンの Tenable Nessus の状態を維持します。これは通常、最新の一般公開バージョンよりも 1 リリース前のものとなりますが、8.10.0 よりも前のバージョンにはなりません。Tenable Nessus の新しいバージョンがリリースされると、Tenable Nessus インスタンスのソフトウェアバージョンは更新されますが、最新のリリースよりも前のバージョンに留まります。

4. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus により、更新プランが保存されます。

Tenable Nessus のバックアップ

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Nessus CLI を使用して Tenable Nessus をバックアップし、後から任意のシステム (異なるオペレーティングシステムでも可) に復元することができます。Tenable Nessus をバックアップするときに、ライセンス情報と設定が保存されされますが、Tenable Nessus はスキャン結果はバックアップしません。

注意: Nessus は 24 時間ごとにバックアップファイルを自動的に作成します。日次バックアップファイルの最大保持数 (Nessus がバックアップファイルを破棄するまでの日数) を設定できます。詳細については、バックアップを保持する日数 のログ設定を参照してください。

注意: Linux システムと Windows システムとの間で、プラットフォームをまたぐバックアップおよび復元を行う場合、Tenable Nessus を復元した後に、スケジュールを使用する Tenable Nessus の設定を再度設定する必要があります。これは、双方のオペレーティングシステムで異なるタイムゾーン名が使用されているため、これらのプラットフォームの間でスケジュールが正しく転送されないためです。

Tenable Nessus をバックアップする方法

1. コマンドターミナルから Tenable Nessus にアクセスします。
2. 次のコマンドを実行して Tenable Nessus バックアップファイルを作成します。

   ```
   > nessuscli backup --create <backup_filename>
   ```

   Tenable Nessus によって次のディレクトリにバックアップファイルが作成されます。

   - Linux : `/opt/nessus/var/nessus`
   - Windows : `C:\ProgramData\Tenable\Nessus\nessus`
   - macOS: `/Library/Nessus/run/var/nessus`

   バックアップファイルには次のファイルが含まれます。

   - /nessus/var/nessus/migrate.db
   - /nessus/var/nessus/tenable-plugins-a-20210201.pem
   - /nessus/var/nessus/log.json
   - /nessus/var/nessus/master.key
   - /nessus/var/nessus/tenable-plugins-b-20210201.pem
   - /nessus/var/nessus/tenable-plugins-20210201.pem
   - /nessus/var/nessus/nessus_org.pem
   - /nessus/var/nessus/users/admin/auth/hash
   - /nessus/var/nessus/users/admin/auth/admin
   - /nessus/var/nessus/users/admin/auth/rules
   - /nessus/var/nessus/users/admin/policies.db
   - /nessus/var/nessus/terrascan.db
   - /nessus/var/nessus/uuid
   - /nessus/var/nessus/backups/

- /nessus/etc/nessus/nessusd.conf.imported
- /nessus/etc/nessus/nessusd.rules
- /nessus/etc/nessus/nessusd.db
- /nessus/etc/nessus/nessus-fetch.db
- /nessus/com/nessus/CA/servercert.pem
- /nessus/com/nessus/CA/cacert.pem
- /nessus/var/nessus/CA/cakey.pem
- /nessus/var/nessus/CA/serverkey.pem
- /nessus/var/nessus/global.db

3. (オプション) Tenable Nessus バックアップファイルを、システム上のバックアップの場所に移動します。

次の手順

- Tenable Nessus の復元

Tenable Nessus の復元

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Nessus CLI を使用し、Tenable Nessus の以前のバックアップを使用して後から任意のシステム (異なるオペレーティングシステムでも可) に復元できます。Tenable Nessus をバックアップするときに、ライセンス情報と設定が保存されされますが、Tenable Nessus はスキャン結果は復元されません。

Tenable Nessus の以前のバージョンで作成されたバックアップであっても復元できます。たとえば Tenable Nessus 10.5.1 を使用している場合、Tenable Nessus 10.4.0 で作成されたバックアップを復元できます。

注意: Linux システムと Windows システムとの間で、プラットフォームをまたぐバックアップおよび復元を行う場合、Tenable Nessus を復元した後に、スケジュールを使用する Tenable Nessus の設定を再度設定する必要があります。これは、双方のオペレーティングシステムで異なるタイムゾーン名が使用されているため、これらのプラットフォームの間でスケジュールが正しく転送されないためです。

注意: 別のデバイスまたは MAC アドレスで Tenable Nessus Manager のバックアップを復元すると、ライセンスは適切に検証されません。

この問題を修正するために Tenable では、`nessuscli fix --reset` コマンドを実行してから、`nessuscli fetch --register` コマンドを実行することで、新しいデバイスまたは MAC アドレスに Tenable Nessus Manager を登録することをお勧めしています。または、ライセンスポータルからライセンスをリセットすることもできます。

この問題は、クラスタリングが有効になっていない場合にのみ Tenable Nessus Manager で発生します。クラスタリングを有効にして Tenable Nessus Manager を復元すると、ライセンスが正常に検証されます。

始める前に

- Tenable Nessus のバックアップ

Tenable Nessus を復元する方法

1. コマンドターミナルから Tenable Nessus にアクセスします。
2. Tenable Nessus サービスを停止します。

   Tenable Nessus によってすべてのプロセスが終了します。
3. 以下のコマンドを実行して、以前に保存したバックアップファイルから Tenable Nessus を復元します。

   ```
   > nessuscli backup --restore path/to/<backup_filename>
   ```

   Tenable Nessus によってバックアップが復元されます。
4. Tenable Nessus サービスを停止して開始します。

   Tenable Nessus が初期化を開始し、バックアップのライセンス情報と設定を使用します。

Nessus を削除する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

このセクションでは、Nessus のアンインストールと削除方法について説明します。

- Linux での Nessus のアンインストール
- Windows での Tenable Nessus のアンインストール
- macOS での Nessus のアンインストール
- Docker コンテナとして Tenable Nessus を削除する

Linux での Nessus のアンインストール

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

次の手順を使用して、Linux で Tenable Nessus をアンインストールします。

始める前に

1. (オプション) スキャンとポリシーをエクスポートします。
2. Tenable Nessus を停止します。
3. 次の手順を使用して Tenable Nessus をアンインストールします。

Tenable Nessus を Linux からアンインストールする方法

1. Tenable Nessus で、実行中のスキャンが完了したことを確認します。
2. コマンドプロンプトから、nessusd デーモンを停止します。

   例: Nessus デーモンの停止コマンド

   Debian/Kali と Ubuntu

   ```
   # /etc/init.d/nessusd stop
   ```

   Red Hat/CentOS/Oracle Linux

   ```
   # /sbin/service nessusd stop
   ```

   SUSE

   ```
   # /etc/rc.d/nessusd stop
   ```

3. ご使用の Linux 系オペレーティングシステム固有の Tenable Nessus の削除コマンドを実行します。

   例: Nessus の削除コマンド

   Debian/Kali と Ubuntu

   ```
   # dpkg -r Nessus
   ```

   Red Hat 6 と 7、CentOS 6 と 7、Oracle Linux 6 と 7

   ```
   # yum remove Nessus
   ```

   Red Hat 8 以降、CentOS 8 以降、Oracle Linux 8 以降、Fedora

   ```
   # dnf remove Nessus
   ```

   SUSE

   ```
   # sudo zypper remove Nessus
   ```

4. お使いの Linux 系オペレーティングシステム固有の削除コマンドを使用して、当初のインストール要素に該当しない残りのファイルを削除します。

   例: Nessus の削除コマンド

   Linux

   ```
   # rm -rf /opt/nessus
   ```

Windows での Tenable Nessus のアンインストール

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** System Administrator

次の手順を使用して、Windows で Tenable Nessus をアンインストールします。

始める前に

1. (オプション) スキャンとポリシーをエクスポートします。
2. Tenable Nessus を停止します。

3. 次の手順を使用して、Windows ユーザーインターフェースまたはコマンドラインから Tenable Nessus をアンインストールします。

Windows ユーザーインターフェースから Tenable Nessus をアンインストールするには

1. Windows で、**プログラムを追加または削除**できる場所、あるいは**プログラムをアンインストールまたは変更**できる場所に移動します。
2. インストール済みプログラムのリストで、**Tenable Nessus** 製品を選択します。
3. **[Uninstall]** (アンインストール) をクリックします。

   Tenable Nessus の削除の選択を確認するダイアログボックスが表示されます。
4. **[Yes]** (はい) をクリックします。

   Windows により Tenable Nessus がアンインストールされます。

Windows CLI から Tenable Nessus をアンインストールするには

1. 管理者権限で PowerShell を開きます。
2. 次のコマンドを実行してください。

   ```
   msiexec.exe /x <path to Nessus installer package>
   ```

   注意: オプションの `msiexec /x` パラメーターの詳細については、Microsoft ドキュメントの msiexec を参照してください。

macOS での Nessus のアンインストール

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

次の手順を使用して、macOS で Tenable Nessus をアンインストールします。

始める前に

1. (オプション) スキャンとポリシーをエクスポートします。
2. Nessus を停止します。
3. 次の手順を使用して、macOS ユーザーインターフェースから Nessus をアンインストールします。

macOS ユーザーインターフェースから Tenable Nessus をアンインストールする方法

1. **[System Preferences]** (システム環境設定) で **[Nessus]** ボタンを選択します。
2. **[Nessus.Preferences]** (Nessus. 環境設定) 画面で、変更を加えるロックを選択します。
3. 次に、ユーザー名とパスワードを入力します。
4. **[Stop Nessus]** (Nessus の停止) ボタンを選択します。

   ステータスが赤色になり、**停止済み**と表示されます。
5. 最後に、**[Nessus.Preferences]** (Nessus. 環境設定) 画面を閉じます。
6. 次の Tenable Nessus ディレクトリ、サブディレクトリ、ファイルを削除します。
   - /Library/Nessus
   - /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   - /Library/PreferencePanes/Nessus Preferences.prefPane
   - /Applications/Nessus
7. macOS がすでに存在しないサービスの開始を試みないように、コマンドプロンプトから次のコマンドを入力して Tenable Nessus サービスを無効にします。

   ```
   $ sudo launchctl remove com.tenablesecurity.nessusd
   ```

   指示されたら、管理者パスワードを入力します。

Docker コンテナとして Tenable Nessus を削除する

> **を使用する場合に必要な [ユーザーロール]Tenable Nessus Manager:** System Administrator

Docker コンテナとして実行中の Tenable Nessus を削除すると、コンテナデータは失われます。

Docker コンテナとして Tenable Nessus を削除する方法

1. ターミナルで、`docker stop` コマンドを使用して、実行中のコンテナを停止します。

   ```
   $ docker stop <container name>
   ```

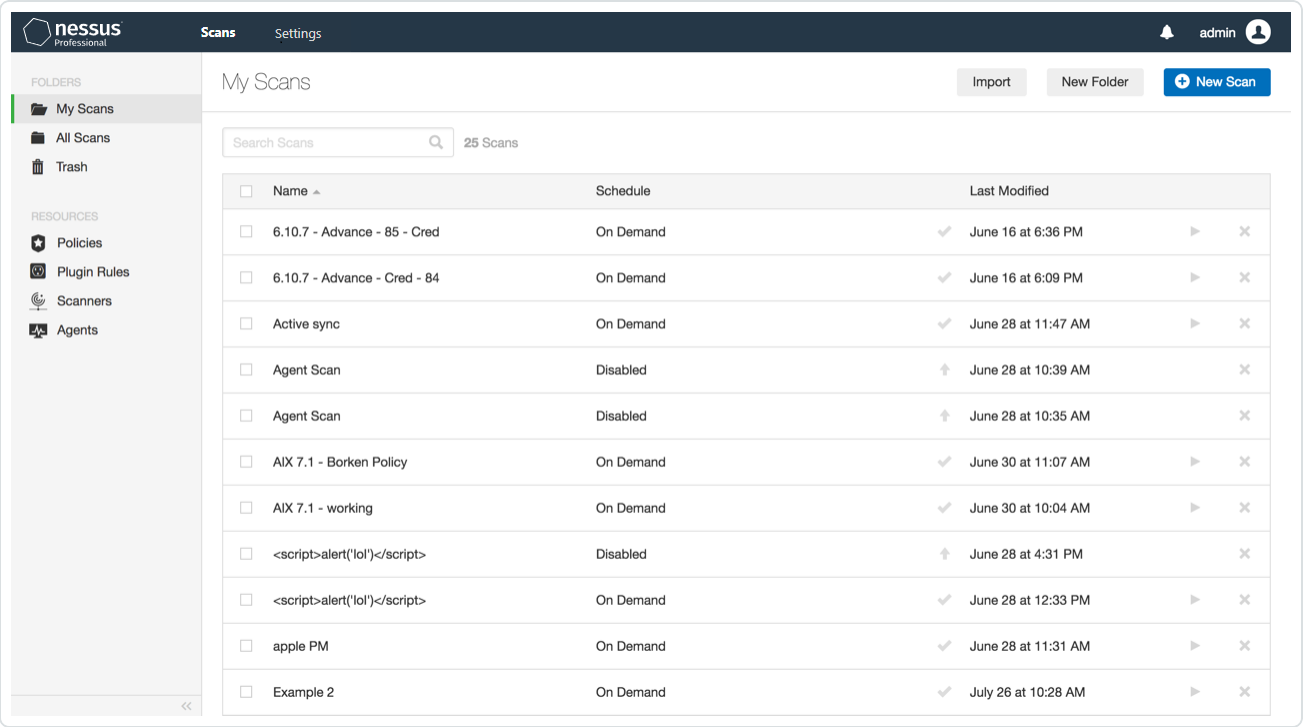
2. docker rm コマンドを使用して、コンテナを削除します。

```
$ docker rm <container name>
```

Scan (スキャン)

注意: Tenable Nessus によるプラグインのコンパイル中は、スキャンの作成および起動、ポリシーまたはプラグインルールの作成や表示、アップグレードアシスタントの使用はできません。

[Scans] (スキャン) ページでは、スキャンとリソースの作成、表示、管理ができます。**[Scans]** (スキャン) ページにアクセスするには、上部のナビゲーションバーで **[Scans]** (スキャン) をクリックします。左側のナビゲーションバーには、**[Folders]** (フォルダー) セクションと **[Resources]** (リソース) セクションが表示されます。



スキャンの詳細については、次のトピックを参照してください。

- スキャンテンプレート
- スキャンを作成して管理する
- スキャン結果
- フォルダーのスキャン
- スキャンポリシー
- プラグイン
- カスタマイズされたレポート

- スキャナー
- Agents (エージェント)

スキャンを作成して管理する

このセクションには、Scan (スキャン) ページで使用できる次のタスクが含まれています。

- スキャンの作成
- スキャンのインポート
- エージェントスキャンを作成する
- スキャン設定を変更する
- 監査証跡を設定する
- スキャンを削除する

スキャンテンプレート

スキャンテンプレートを使用して、所属企業のカスタムポリシーを作成できます。その後、Tenable のスキャンテンプレートまたはカスタムポリシーの設定に基づいてスキャンを実行できます。詳細は、Create a Policyを参照してください。

スキャンまたはポリシーの初回作成時には、**[Scan Templates]**(スキャンテンプレート) セクションまたは **[Policy Templates]** (ポリシーテンプレート) セクションがそれぞれ表示されます。Tenable Nessus は、スキャンに使用するセンサーに応じて、スキャナーとエージェントに個別のテンプレートを用意しています。

- スキャナーテンプレート
- エージェントテンプレート (Tenable Nessus Manager のみ)

カスタムポリシーがある場合は、**[User Defined]** (ユーザー定義) タブに表示されます。

Tenable が提供するスキャンテンプレートを設定する場合、変更できるのはそのスキャンテンプレートタイプに含まれる設定のみです。ユーザー定義スキャンテンプレートを作成すると、スキャン用のカスタム設定セットを変更できます。

スキャナーとエージェントテンプレートのすべての設定の説明については、設定 を参照してください。

注意: プラグインが別のシステムと通信するために認証や設定を必要とする場合、そのプラグインはエージェントで使用できません。これには以下のような例があります。

- パッチ管理
- モバイルデバイス管理
- クラウドインフラ監査
- 認証が必要となるデータベースチェック

スキャナーテンプレート

Tenable Nessus には、3 つのスキャナーテンプレートカテゴリがあります。

- Discovery (検出) – Tenable では、検出スキャンを使用して、ネットワーク上にあるホストを確認し、関連する情報 (IP アドレス、FQDN、オペレーティングシステム、開いているポートなど) がある場合は、それらも確認することを推奨しています。ホストのリストを取得した後、各脆弱性スキャンでターゲットにするホストを選択できます。
- 脆弱性 – Tenable では、所属企業の標準的な日常のスキャンニーズのほとんどで、脆弱性スキャンテンプレートを使用することを推奨しています。Tenable は、特定の脆弱性または脆弱性のグループに対してネットワークをスキャンできる脆弱性スキャンテンプレートも公開しています。Tenable は Tenable Nessus スキャンテンプレートライブラリを頻繁に更新し、Log4Shell などの一般的に関心を集めている最新の脆弱性を検出するテンプレートを追加しています。
- Compliance (コンプライアンス) - Tenable では、設定スキャンテンプレートを使用して、ホスト設定がさまざまな業界標準に準拠しているかどうかをチェックすることを推奨しています。コンプライアンススキャンは、設定スキャンと呼ばれることもあります。コンプライアンススキャンが実行できるチェック事項については、コンプライアンス および SCAP 設定 を参照してください。

次の表では、利用可能なスキャナーテンプレートについて説明します。

ヒント: Tenable Nessus ユーザーインターフェースでは、検索ボックスを使用してテンプレートを素早く見つけることができます。

注意: Tenable Nessus Manager をエージェント管理用に設定する場合、Tenable ではローカルスキャナーとしての Tenable Nessus Manager の使用をお勧めしていません。たとえば、Tenable Security Center のスキャンゾーンに Nessus Manager を含めるように設定したり、Tenable Nessus Manager からネットワークベースのスキャンを直接実行したりしないでください。このような設定は、エージェントスキャンのパフォーマンスに悪影響を与える可

能性があります。ほとんどの場合、Tenable Nessus Manager で作業する際はエージェントスキャンテンプレートを使用します。

テンプレート	説明
Discovery (検出)	
Attack Surface Discovery (アタックサーフェスの検出)	(Tenable Nessus Expert のみ) Bit Discovery を使用して、上位ドメインのリストをスキャンし、サブドメインと DNS 関連のデータを抽出します。詳細は、Bit Discovery でアタックサーフェス検出スキャンを作成するを参照してください。
Host Discovery (ホスト検出)	単純なスキャンを実行して、稼働中のホストと開いているポートを検出します。 このスキャンを起動して、ネットワーク上のホストと該当する関連情報 (IP アドレス、FQDN、オペレーティングシステム、開いているポートなど) を確認します。ホストのリストを取得した後、各脆弱性スキャンでターゲットにするホストを選択できます。 Tenable では、Tenable Network Monitor などのパッシブネットワーク監視のない企業がこのスキャンを毎週実行し、ネットワーク上の新しい資産を検出することを推奨しています。 **注意:** 検出スキャンによって特定された資産は、ライセンスに対してカウントされません。
Ping-Only Discovery (Ping のみの検出)	最小限のネットワークトラフィックでライブホストを検出するためのシンプルなスキャン。
脆弱性	
Basic Network Scan (基本的なネットワークスキャン)	任意のホストで使用できるフルシステムスキャンを実行します。Nessus のプラグインをすべて有効にした資産 (複数可) のスキャンには、このテンプレートを使用します。たとえば、所属する組織のシステムにおける内部脆弱性スキャンを実施することができます。
Credential Validation (認証	Windows および Unix のホスト認証情報のペアがスキャンターゲットに対して正常に認証されることを確認するために使用される軽量スキャンテンプレート。

情報の検証)	このスキャンテンプレートを使用すると、ネットワークの認証情報ペアの問題を素早く診断できます。
Advanced Scan (詳細なスキャン)	最も設定可能なスキャンタイプです。このスキャンテンプレートを、任意のポリシーとマッチするように設定することができます。このテンプレートのデフォルト設定は基本スキャンテンプレートと同じですが、追加の設定オプションを利用できます。 **注意:** 詳細なスキャンテンプレートを使えば、高速チェックや低速チェックなどのカスタム設定をして、より詳細にスキャンすることができますが、設定を誤ると、資産の停止やネットワークの飽和が引き起こされる場合があります。詳細なテンプレートは注意深く使用してください。 **注意:** Tenable は、プラグインがネットワークトラフィックに依存して検出を行う新しくリリースされたプラグインファミリーで、このテンプレートを自動的に更新します。
Advanced Dynamic Scan (詳細な動的スキャン)	プラグインファミリーまたは個別のプラグインを手動で選択する代わりに、動的プラグインフィルターを設定できる、推奨事項のない詳細なスキャンです。Tenable が新しいプラグインをリリースすると、お使いのフィルターに一致するプラグインがスキャンまたはポリシーに自動的に追加されます。これにより、新しいプラグインがリリースされたときにスキャンを最新の状態に維持しながら、特定の脆弱性に合わせてスキャンを調整することが可能になります。
Malware Scan (マルウェアスキャン)	Windows と Linux のシステムで、マルウェアをスキャンします。 Tenable Nessus は、許可リストとブロックリストを組み合わせたアプローチを使用してマルウェアを検出し、既知の良好なプロセスを監視し、既知の不良プロセスに警告を発し、未知のプロセスに「詳細な調査が必要」のフラグを立てることで両者の間のカバレッジギャップを特定します。
Nessus 10.8.0 / 10.8.1 Agent Reset (Nessus 10.8.0 / 10.8.1 Agent のリセット)	Tenable Agents のバージョン 10.8.0 および 10.8.1 をスキャンして検索、リセット、更新します。詳細については、Tenable Agent 10.8.2 リリースノートのアップグレードノートを参照してください。
Mobile Device Scan (モバイルデ	(Tenable Nessus Manager のみ) Microsoft Exchange または MDM を使用してモバイルデバイスを評価します。

バイススキャン)	このテンプレートを使用して、対象のモバイルデバイスにインストールされているものをスキャンし、インストールされているアプリケーションまたはアプリケーションバージョンの脆弱性を報告します。 モバイルデバイススキャンプラグインにより、モバイルデバイス管理 (MDM) に登録されているデバイスから、および Microsoft Exchange Server の情報が保管されている Active Directory サーバーから情報を取得できます。 • 情報のクエリを行うには、Tenable Nessus スキャナーがモバイルデバイス管理サーバーに到達できる必要があります。Nessus スキャナーからこれらのシステムへのトラフィックをブロックするスクリーニングデバイスがないことを確認する必要があります。さらに、Tenable Nessus に Active Directory サーバーへの管理者認証情報 (例:ドメイン管理者) を与える必要があります。 • モバイルデバイスをスキャンするには、管理サーバーとモバイルプラグインの認証情報を Tenable Nessus に設定する必要があります。Tenable Nessus は管理サーバーへの認証を直接受けるので、特定のホストをスキャンするようにスキャンポリシーを設定する必要はありません。 • Microsoft Exchange Server のデータにアクセスする ActiveSync スキャンの場合、Tenable Nessus は過去 365 日以内に更新された携帯電話から情報を取得します。
Credentialed Patch Audit (認証パッチ監査)	ホストを認証し、不足している更新プログラムを列挙します。 このテンプレートを認証情報とともに使用して、Tenable Nessus にホストへの直接アクセスを与え、ターゲットとなるホストをスキャンし、欠落しているパッチ更新を列挙します。
Active Directory Starter Scan (Active Directory 開始スキャン)	Active Directory の設定ミスをスキャンします。 このテンプレートを使用して、Active Directory をチェックし、Kerberoasting 攻撃、脆弱な Kerberos の暗号化、Kerberos 事前認証の検証、有効期限のないアカウントパスワード、制約のない委任、null セッション、Kerberos KRBTGT、危険な信頼関係、プライマリグループ ID の整合性、空白のパスワードがないかを調べます。
Find AI (AI の検	AI、LLM、ML 関連の脆弱性をスキャンします。

出)	
Remote Monitoring and Management (リモートのモニタリングと管理)	リモートのモニタリングと管理に使用されている環境内の資産を特定します。リモートのモニタリングと管理の資産は、リモートコントロールでシステムへのローカルアクセスを取得するためにサイバー攻撃の標的となることがよくあります。 **注意:** このテンプレートではポートスキャンがデフォルトで無効になり、ポートスキャン設定を有効にすることはできません。このテンプレートに含まれるプラグインには、独自のターゲットポート情報が含まれます。 このテンプレートに基づいてスキャンを実行するとき、プラグイン 19506 (Nessus スキャン情報) は次の出力警告を表示します。 警告: スキャン中にポートスキャナーが有効になりませんでした。これにより、結果が不完全になる可能性があります。 この警告は想定されたものであり、エラーを示すものではありません。これは安全に無視できます。
Compliance (コンプライアンス)	
Audit Cloud Infrastructure (クラウドインフラ監査)	サードパーティのクラウドサービスの設定を監査します。 このテンプレートを使用して、監査するサービスの認証情報を提供すると、Amazon Web Service (AWS)、Google Cloud Platform、Microsoft Azure、Rackspace、Salesforce.com、Zoom の設定をスキャンできます。
Internal PCI Network Scan (内部 PCI ネットワークスキャン)	内部 PCI DSS (11.2.1) の脆弱性スキャンを実行します。 このテンプレートでは、PCI コンプライアンス要件を満たす継続的な脆弱性管理プログラム向けの内部 (PCI DSS 11.2.1) スキャン要件に準拠するために使用可能なスキャンが作成されます。これらのスキャンを使用して、継続的に脆弱性を管理したり、結果が合格またはクリーン (問題解消) となるまで再スキャンを実行したりすることができます。不足しているパッチとクライアント側の脆弱性を列挙するために認証情報を提供することができます。 **注意:** PCI DSS では、スキャンの結果が合格または「クリーン」である証拠を少なくとも四半期に 1 度提供することが義務付けられています。また、ネットワークに重大な変更を加えた後にもスキャンを実行する必要があります (PCI DSS 11.2.3)。
MDM Config	モバイルデバイスマネージャーの設定を監査します。

Audit (MDM 設定監査)	MDM 設定監査テンプレートは、パスワード要件、リモートワイプ設定、テザリングや Bluetooth などの安全でない機能の使用など、さまざまな MDM 脆弱性についてレポートします。
Offline Config Audit (オフライン設定監査)	ネットワークデバイスの設定を監査します。 オフライン設定監査により、Tenable Nessus はネットワーク経由のスキャンや認証情報を使用することなく、ホストをスキャンできます。企業のポリシーが、セキュリティ上の理由から、デバイスをスキャンしたり、ネットワーク上のデバイスの認証情報を取得したりすることを許可していない場合があります。オフライン設定監査では、ホストからのホスト設定ファイルを使用してスキャンします。これらのファイルをスキャンすることで、ホストを直接スキャンすることなく、デバイスの設定が監査に準拠しているかを確認できます。 Tenable では、オフライン設定監査を使用して、安全なリモートアクセスをサポートしていないデバイスや、スキャナーがアクセスできないデバイスをスキャンすることを推奨しています。
PCI Quarterly External Scan (PCI 四半期外部スキャン)	PCI で義務付けられている四半期ごとの外部スキャンを実行します。 このテンプレートを使用すると、PCI DSS の四半期スキャンの要件を満たす外部スキャン (PCI DSS 11.2.2) をシミュレーションできます。ただし、このテンプレートのスキャン結果を Tenable に送信して PCI 検証を行うことはできません。Tenable Vulnerability Management のお客様だけが、PCI スキャンの結果を Tenable に送信して、PCI ASV 検証を受けることができます。
Policy Compliance Auditing (ポリシーコンプライアンス監査)	既知の基準値に照らしてシステム設定を監査します。 **注意:** 1 つの**ポリシーコンプライアンス監査**スキャンに含めることができる監査ファイルの最大数は、監査ファイルが必要とする合計実行時間とメモリによって制限されます。この制限を超えると、スキャン結果が不完全になったり失敗したりする可能性があります。Tenable では、想定される影響を限定的なものにするため、スキャンの範囲とコンプライアンス要件を明確にしたうえで、スキャンポリシーで対象となる監査を選択することを推奨しています。 コンプライアンスチェックにより、Windows オペレーティングシステムのパスワードの複雑さ、システム設定、レジストリ値などのカスタムセキュリティポリシーに対して監査を行うことができます。Windows システムの場合、コンプライアンス監査は、Windows ポリシーファイルで記述できるものの大部分をテストできます。

	Unix システムの場合、コンプライアンス監査では、実行中のプロセス、ユーザーセキュリティポリシー、ファイルのコンテンツがテストされます。
SCAP and OVAL Auditing (SCAP および OVAL 監査)	SCAP と OVAL の定義を使用してシステムを監査します。 **注意:SCAP および OVAL 監査** スキャンテンプレートは、後方互換性のために保持されています。このテンプレートは SCAP バージョン 1.2 以前をサポートしています。SCAP バージョン 1.3 以降を必要とする Windows 10 や Windows 11 などの最新のオペレーティングシステムとは互換性がありません。 アメリカ国立標準技術研究所 (NIST) の Security Content Automation Protocol (SCAP) は、政府機関における脆弱性管理とポリシーコンプライアンスのためのポリシーです。OVAL、CVE、CVSS、CPE、FDCCポリシーなど、複数のオープンスタンダードおよびポリシーが使用されています。 • SCAP コンプライアンス監査では、実行可能ファイルをリモートホストに送信することが義務付けられています。 • セキュリティソフトウェア (例: McAfee Host Intrusion Prevention) を実行しているシステムでは、監査に必要な実行可能ファイルがブロックまたは隔離される可能性があります。そのようなシステムでは、ホストまたは送信される実行可能ファイルを例外として設定する必要があります。 • **SCAP および OVAL 監査**テンプレートを使用する場合、NIST の Special Publication 800-126 で指定されているように、Linux および Windows の **SCAP チェック**を実行してコンプライアンス基準をテストできます。

エージェントテンプレート (Tenable Nessus Manager のみ)

Tenable Nessus Manager には、2 つのエージェントテンプレートカテゴリがあります。

- 脆弱性 – Tenable では、所属企業の標準的な日常のスキャンニーズのほとんどで、脆弱性スキャンテンプレートを使用することを推奨しています。
- Compliance (コンプライアンス) - Tenable では、設定スキャンテンプレートを使用して、ホスト設定がさまざまな業界標準に準拠しているかどうかをチェックすることを推奨しています。コンプライアンス

スキャンは、設定スキャンと呼ばれることもあります。コンプライアンススキャンが実行できるチェック事項については、コンプライアンス および SCAP 設定 を参照してください。

次の表では、利用可能なエージェントテンプレートについて説明します。

ヒント: Tenable Nessus ユーザーインターフェースでは、検索ボックスを使用してテンプレートを素早く見つけることができます。

テンプレート	説明
Vulnerabilities (脆弱性)	
Basic Agent Scan (基本のエージェントスキャン)	任意のホストで使用できるフルシステムスキャンを実行します。Nessus のプラグインをすべて有効にした資産 (複数可) のスキャンには、このテンプレートを使用します。たとえば、所属する組織のシステムにおける内部脆弱性スキャンを実施することができます。
Advanced Agent Scan (詳細なエージェントスキャン)	最も設定可能なスキャンタイプです。このスキャンテンプレートを、任意のポリシーとマッチするように設定することができます。このテンプレートのデフォルト設定は基本スキャンテンプレートと同じですが、追加の設定オプションを利用できます。 **注意:** 詳細なスキャンテンプレートを使えば、高速チェックや低速チェックなどのカスタム設定をして、より詳細にスキャンすることができますが、設定を誤ると、資産の停止やネットワークの飽和が引き起こされる場合があります。詳細なテンプレートは注意深く使用してください。
Malware Scan (マルウェアスキャン)	Windows と Linux のシステムで、マルウェアをスキャンします。 Tenable Agent は、許可リストとブロックリストを組み合わせたアプローチを使用して、マルウェアの検出、既知の良好なプロセスの監視、既知の不良プロセスに対するアラートを行い、さらに詳細に検査するために未知のプロセスにフラグを立てることで両者の間のカバレッジギャップを特定します。
エージェント Log4Shell	Apache Log4j の Log4Shell 脆弱性 (CVE-2021-44228) をローカルチェックで検出します。
コンプライアンス	
Policy	既知の基準値に照らしてシステム設定を監査します。

Compliance Auditing (ポリシーコンプライアンス監査)	**注意:** 1 つの**ポリシーコンプライアンス監査**スキャンに含めることができる監査ファイルの最大数は、監査ファイルが必要とする合計実行時間とメモリによって制限されます。この制限を超えると、スキャン結果が不完全になったり失敗したりする可能性があります。Tenable では、想定される影響を限定的なものにするため、スキャンの範囲とコンプライアンス要件を明確にしたうえで、スキャンポリシーで対象となる監査を選択することを推奨しています。 コンプライアンスチェックにより、Windows オペレーティングシステムのパスワードの複雑さ、システム設定、レジストリ値などのカスタムセキュリティポリシーに対して監査を行うことができます。Windows システムの場合、コンプライアンス監査は、Windows ポリシーファイルで記述できるものの大部分をテストできます。Unix システムの場合、コンプライアンス監査では、実行中のプロセス、ユーザーセキュリティポリシー、ファイルのコンテンツがテストされます。
SCAP and OVAL Auditing (SCAP および OVAL 監査)	SCAP と OVAL の定義を使用してシステムを監査します。 **注意:SCAP および OVAL 監査** スキャンテンプレートは、後方互換性のために保持されています。このテンプレートは SCAP バージョン 1.2 以前をサポートしています。SCAP バージョン 1.3 以降を必要とする Windows 10 や Windows 11 などの最新のオペレーティングシステムとは互換性がありません。 アメリカ国立標準技術研究所 (NIST) の Security Content Automation Protocol (SCAP) は、政府機関における脆弱性管理とポリシーコンプライアンスのためのポリシーです。OVAL、CVE、CVSS、CPE、FDCCポリシーなど、複数のオープンスタンダードおよびポリシーが使用されています。 • SCAP コンプライアンス監査では、実行可能ファイルをリモートホストに送信することが義務付けられています。 • セキュリティソフトウェア (例: McAfee Host Intrusion Prevention) を実行しているシステムでは、監査に必要な実行可能ファイルがブロックまたは隔離される可能性があります。そのようなシステムでは、ホストまたは送信される実行可能ファイルを例外として設定する必要があります。 • **SCAP and OVAL Auditing テンプレート**を使用する場合、NIST の Special Publication 800-126 で指定されているように、Linux および Windows の **SCAP チェック**を実行してコンプライアンス基準をテストできます。

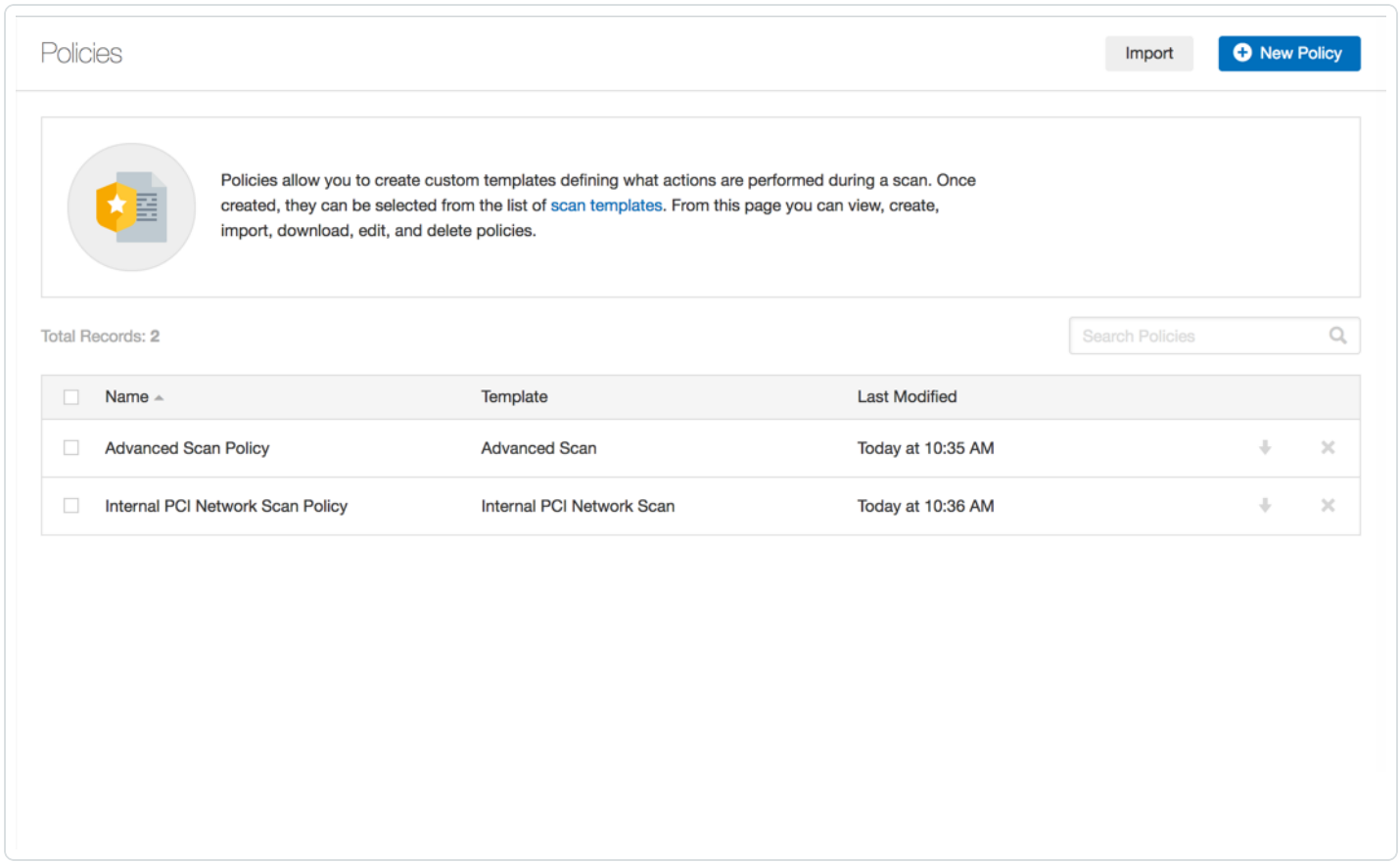
スキャンポリシー

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

ポリシーは、スキャンの実行に関連する定義済み設定オプションのセットです。作成済みのポリシーは、スキャンを作成するときにテンプレートとして選択できます。

注意: Tenable Nessus によるプラグインのコンパイル中は、スキャンの作成および起動、ポリシーまたはプラグインルールの作成や表示、アップグレードアシスタントの使用はできません。

ヒント デフォルト のポリシーテンプレートと設定については、を参照してください スキャンテンプレート



次の手順に従って、ポリシーを管理します。

ポリシーの作成

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Policies]** (ポリシー) をクリックします。

   [Policies] (ポリシー) ページが表示されます。

3. 右上の **[New Policy]** (新しいポリシー) ボタンをクリックします。

   [Policy Templates] (ポリシーテンプレート) ページが表示されます。

4. 使用するポリシーテンプレートをクリックします。

5. ポリシーの設定を行います。

6. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus がポリシーを保存します。

ポリシーを変更する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Policies]** (ポリシー) をクリックします。

3. 設定するポリシーに対応するポリシーテーブルの行のボックスにチェックマークを入れます。

   右上隅に **[More]** (その他) ボタンが表示されます。

4. **[More]** (その他) ボタンをクリックします。

5. **[Configure]** (続行) をクリックします。

   ポリシーの **[Configuration]** (設定) ページが表示されます。

6. 設定を変更します。

7. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus により設定が保存されます。

ポリシーのエクスポート

Tenable Nessus の既存のスキャンポリシーを *.nessus* ファイルとしてエクスポートし、それを別の Tenable Nessus インストールにインポートできます。その後、インポートされたポリシーの設定を表示および変更できます。

ポリシーのエクスポート手順

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Policies]** (ポリシー) をクリックします。

   [Policies] (ポリシー) ページが表示されます。

3. エクスポートするポリシーの行で、↓ をクリックします。

   ポリシーが *.nessus* ファイルとしてマシンにダウンロードされます。ポリシーは、別の Tenable Nessus インストールにインポートすることも、後で使用するために保存することもできます。

ポリシーをインポートする

Tenable Nessus ポリシーを *.nessus* ファイルとしてエクスポートし、それを別の Tenable Nessus インストールにインポートできます。その後、インポートされたポリシーの設定を表示および変更できます。Nessus DB ファイルをポリシーとしてインポートすることはできません。

ポリシーをインポートする方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Policies]** (ポリシー) をクリックします。

   [Policies] (ポリシー) ページが表示されます。

3. 右上隅にある **[Import]** (インポート) をクリックします。

   ブラウザのファイルマネージャーウィンドウが表示されます。

4. インポートするスキャンファイルを参照して選択します。

   > **注意:** サポートされるファイルタイプは、エクスポートされた Nessus (`.nessus`) ファイルです。

   Tenable Nessus によってファイルがポリシーとしてインポートされます。

ポリシーの削除

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Policies]** (ポリシー) をクリックします。

3. ポリシーテーブルの、削除するポリシーに対応する行で、✕ ボタンをクリックします。

   ポリシーを削除してよいかを確認するダイアログボックスが表示されます。

4. **[Delete]** (削除) ボタンをクリックします。

   Tenable Nessus によりポリシーが削除されます。

ポリシーの特徴

- スキャンの技術面を制御するパラメーター。タイムアウト、ホスト数、ポートスキャナーのタイプなどが例として挙げられます。
- ローカルスキャン (Windows、SSH など)、認証された Oracle データベーススキャン、HTTP、FTP、POP、IMAP、または Kerberos ベースの認証用の認証情報。
- ファミリーやプラグインベースのスキャンの詳細な仕様。
- データベースコンプライアンスポリシーチェック、レポート詳細、サービス検出スキャン設定、Unix コンプライアンスチェックなど。
- ネットワークデバイスを対象とするオフラインの設定監査。デバイスを直接スキャンせずに、ネットワークデバイスを安全にチェックできます。
- 既知の無害なファイルと悪意のあるファイル両方のファイルの MD5 チェックサムを比較する Windows マルウェアスキャン。

スキャン設定とポリシー設定

スキャンの設定により、スキャンのパラメーターを各自のネットワークセキュリティのニーズに合うように改良できます。設定可能なスキャン設定は、スキャンやポリシーが基づいている Tenable 提供のテンプレートによって変化します。

これらの設定は、個別のスキャンで、または個別のスキャンの作成に使用するポリシーで設定できます。

Tenable Nessus は、スキャン設定を次のカテゴリに分類します。

- スキャンの Basic 設定
- ポリシーの基本設定
- 検出設定
- 評価設定
- レポート設定
- 詳細設定

ポリシーでの設定

ポリシーの設定を行う場合、次の内容に注意してください。

- ポリシーで設定を行うと、設定はそのポリシーに基づいて作成されたすべてのスキャンに適用されます。
- ポリシーは、Tenable が提供するテンプレートに基づきます。ほとんどの設定は、同じ Tenable 提供のテンプレートを使用する個別のスキャンで設定できるものと同じです。

  しかし、特定の **[Basic]** (基本) 設定はポリシーの作成時に特有のものであり、個別のスキャンの設定時には表示されません。詳細は、ポリシーの基本設定を参照してください。
- 一部の設定はポリシーで設定できますが、ポリシーに基づく個別のスキャンで変更することはできません。このような設定には、**[Discovery]** (検出)、**[Assessment]** (評価)、**[Report]** (レポート)、**[Advanced]** (詳細)、**[Compliance]** (コンプライアンス)、**[SCAP]**、**[Plugins]** (プラグイン) などがあります。こうした設定を個別のスキャンで変更したい場合は、代わりに Tenable 提供のテンプレートに基づいて個別のスキャンを作成してください。
- ポリシーで**認証情報**を構成した場合、他のユーザーがポリシーに基づくスキャンに、スキャン固有の認証情報または管理された認証情報を追加することにより、それらの認証情報を上書きできます。

スキャンの Basic 設定

注意: このトピックでは、スキャンで設定できる **[Basic]** (基本) 設定について記載します。ポリシーの **[Basic]** (基本) 設定については、ポリシーの Basic 設定を参照してください。

基本スキャン設定は、スキャンの名前、ターゲット、スキャンがスケジュールされているかどうか、スキャンにアクセスできるユーザーなどの、組織的およびセキュリティに関連するスキャンの特定の要素を指定するために使用されます。

特定のスキャンに必要な設定項目は、Tenable Nessus インターフェースに示されています。

基本設定には次のセクションが含まれます。

次の表に、使用可能なすべての**基本**設定をセクションごとに示します。

一般

設定	デフォルト値	説明
Name (名前)	なし	スキャンの名前を指定します。この値は Tenable Nessus インターフェースで表示されます。
Description (説明)	なし	(オプション) スキャンの説明を指定します。
Folder (フォルダー)	マイスキャン	保存後にスキャンが表示されるフォルダーを指定します。
Dashboard (ダッシュボード)	Disabled (無効)	(Tenable Nessus Manager のみ) (任意) スキャン結果のページが、デフォルトでインタラクティブなダッシュボードビューになるかどうかを決定します。
Agent Groups (エージェントグループ)	なし	(エージェントスキャンのみ) スキャンの対象にするエージェントグループを指定します。ドロップダウンボックスから既存のエージェントグループを選択するか、新しいエージェントグループを作成します。詳細は、エージェントグループの新規作成を参照してください。
スキャンウィンドウ	1 時間	(エージェントスキャンのみ) (必須) 脆弱性レポートに含めて表示するために、レポートが必要なエージェントの時間枠を指定します。ドロップダウンボックスを使用して時間の間隔を選択するか、✎をクリックしてカスタムスキャン期間を入力します。
Scanner (スキャナー)	自動選択	(Tenable Nessus Manager のみ) スキャンを実行するスキャナーを指定します。

設定	デフォルト値	説明
		このパラメーターに対して選択できるスキャナーは、Tenable Vulnerability Management インスタンス用に設定されたスキャナーおよびスキャナーグループ、およびそれらのスキャナーまたはグループに対するアクセス許可によって決まります。
Policy (ポリシー)	なし	この設定は、スキャンの所有者がポリシーに基づく既存のスキャンを編集する場合にのみ表示されます。 **注意:** スキャンを作成した後、スキャンの元になっている Tenable が提供するテンプレートを変更することはできません。 ドロップダウンボックスで、スキャンの元になるポリシーを選択します。**[Can View]** (閲覧可能) またはそれ以上のアクセス許可があるポリシーを選択できます。 多くの場合、スキャンの作成時にポリシーを設定し、毎回のスキャンの実行時には同じポリシーを適用し続けます。しかし、スキャンのトラブルシューティングやデバッグ時にポリシーを変更することも可能です。たとえば、ポリシーを変更することで、別のプラグインファミリーを有効化または無効化したり、パフォーマンス設定を変更したり、あるいは詳細なログ記録を行うデバッグ専用のポリシーを適用したりすることが容易になります。 スキャンのポリシーを変更した場合、以前割り当てられていたポリシーに従って実行されたスキャンの結果は、スキャン履歴に保持されます。
Target URL (ターゲット URL)	なし	(ウェブアプリテンプレートのみ) Tenable Nessus Web Application Scanning ライセンスに表示されるスキャンするターゲットの URL を指定します。正規表現やワイルドカードは使用できません。ターゲットは、`http://` または `https://` プロトコル識別子で始まる必要があります。 **注意: [Target]** (ターゲット) ボックスに入力した URL の FQDN ホストが、ライセンスに表示されているホストとは異なっていて、スキャンが正常に実行された場合、入力した新しい URL はライセンスに追加される資産としてカウントされます。

設定	デフォルト値	説明
		注意: ユーザー定義スキャンテンプレートを作成する場合、ターゲットの設定はテンプレートに保存されません。新しいスキャンを作成するたびにターゲットを入力します。
Targets (ターゲット)	なし	スキャンする 1 つ以上のターゲットを指定します。ターゲットグループを選択するか、ターゲットファイルをアップロードする場合、追加のターゲットを指定する必要はありません。 さまざまな形式を使用して、ターゲットを指定できます。 **ヒント:** `hostname[ip]` 構文 (例: `www.example.com [192.168.1.1]`) を使用して、スキャン中に Tenable Nessus にサーバーの特定のホスト名を強制的に使用させることができます。
Upload Targets (ターゲットのアップロード)	なし	ターゲットを指定するテキストファイルをアップロードします。 ターゲットファイルは次の形式でなければなりません。 • ASCII ファイル形式 • 1 行につき 1 つのターゲットのみ • 行末に余分なスペースなし • 最終ターゲットの後に余分な行なし **注意:** Unicode/UTF-8 エンコードはサポートされていません。
Show Dashboard (ダッシュボードの表示)	オフ	このチェックボックスをオンにすると、スキャンのデフォルトランディングページとしてスキャンダッシュボードが表示されます。

スケジュール

デフォルトでは、スキャンはスケジュールされていません。**[スケジュール]** セクションへの初回アクセス時に表示される **[スケジュールの有効化]** 設定は、**[オフ]** に設定されています。次の表にリストされている設定を変更するには、**[オフ]** ボタンをクリックします。その他の設定が表示されます。

設定	デフォルト値	説明

Frequency (頻度)	Once (一度)	スキャンを開始する頻度を指定します。
		• **一度**: 特定の時間にスキャンをスケジュールします。
		• **毎日**: 1 ~ 20 日ごとに、特定の時間に行われるようスキャンをスケジュールします。
		• **毎週**: 1 ~ 20 週ごとに、時間と曜日を指定して行われるようにスキャンをスケジュールします。
		• **毎月**: 1 ~ 20 か月単位でスキャンの実行をスケジュールします。
		  • **月の特定の日**: 毎月、特定の日の選択した時間にスキャンが繰り返されます。たとえば、開始日を 10 月 3 日と選択した場合、スキャンは翌月以降、毎月 3 日の選択した時刻に繰り返して実行されます。
		  • **月の特定の週**: 毎月、特定の曜日の選択した時間にスキャンが繰り返されます。たとえば、開始日を月の最初の月曜日と選択した場合、スキャンは翌月以降、毎月最初の月曜日の選択した時刻に実行されます。
		  注意: 毎月スキャンするようスキャンをスケジュールする場合、Tenable は、開始日を 28 日かそれより前の日付にするようお勧めします。いくつかの月に存在しない日付 (例: 29 日) を開始日に選択した場合、Tenable Nessus は、それらの日にはスキャンを実行できません。
		• **年単位**: 時間と曜日ごとに、最大 20 年間、年単位でスキャンの実行をスケジュールします。

Starts (開始)	不定	スキャンを開始する正確な日時を指定します。 デフォルトでは、開始日はスキャンを作成する日付になっています。開始時間は、30 分刻みで最も近い時間になりま

設定	デフォルト値	説明
		す。たとえば、2023 年 9 月 18 日午前 9 時 17 分にスキャンを作成した場合、デフォルトの開始日時は 2023 年 9 月 18 日午前 9 時 30 分に設定されます。
Timezone (タイムゾーン)	America/New York (米国/ニューヨーク)	**[Starts]** (開始) の値セットのタイムゾーンを指定します。
Repeat Every (リピート間隔)	不定	スキャンが再度開始される間隔を指定します。この項目のデフォルト値は、選択した頻度に応じて異なります。
Repeat On (リピートする曜日)	不定	スキャンを繰り返す曜日を指定します。この項目は、**[頻度]** に *[週単位]* を指定した場合にのみ表示されます。 デフォルトでは、**[リピート]** の値はスキャンを作成する曜日になっています。
Repeat By (リピートする日付)	月の特定の日	月単位のスキャンが再度開始される日を指定します。**[頻度]** に *[月単位]* を指定する場合に限り、この項目が表示されます。
Summary (サマリー)	該当なし	利用可能な設定で指定した値に基づいて、スキャンのスケジュール概要が提供されます。

通知

設定	デフォルト値	説明
Email Recipient(s) (Eメールの受信者)	なし	スキャンが完了して結果が利用可能になったときに警告される、0 個または複数のメールアドレスをコンマで区切って指定します。
Attach Report (レポートの添付)	Off (オフ)	(Tenable Nessus Professionalのみ)各メール通知にレポートを添付するかどうかを指定します。このオプションにより、**[Report Type]** (レポートの種類) と **[Max Attachment Size]** (最大添付サイズ) の設定が切り替わります。

Report Type (レポートの種類)	Nessus	(Tenable Nessus Professional のみ) メールに添付するレポートの種類 (CSV、Nessus、PDF)を指定します。
Max Attachment Size (添付ファイルの最大サイズ)	25	(Tenable Nessus Professional のみ) レポートの添付ファイルの最大サイズ (MB) を指定します。レポートが最大サイズを超える場合、メールにレポートは添付されません。Tenable Nessus は、50 MB を超えるレポート添付ファイルをサポートしません。
Result Filters (結果フィルター)	なし	メールで送信する情報の種類を定義します。

アクセス許可

[Permissions] (アクセス許可) セクションの設定を使用すると、グループや個別のユーザーにさまざまなアクセス許可を割り当てることができます。グループにアクセス許可を割り当てると、そのアクセス許可はグループ内のすべてのユーザーに適用されます。次の表には、割り当てられる権限が示されています。

ヒント：個別のユーザーは離職したり入社したりすることがあるので、Tenable では、メンテナンスを最小限に抑えるために個別のユーザーではなくユーザーグループにアクセス許可を割り当てることを推奨します。

アクセス許可	説明
No Access (アクセスなし)	**[No Access]** (アクセスなし) に設定されたグループとユーザーは、スキャンには一切関与できません。デフォルトでは、スキャンの作成者以外のユーザーまたはグループはスキャンにアクセスできません。
Can View (閲覧可能)	**[Can View]** (閲覧可能) に設定されたグループとユーザーは、スキャン結果を閲覧できます。
Can Control (制御可能)	**[Can Control]** (制御可能) に設定されたグループとユーザーは、スキャンの開始、一時停止、停止、結果の閲覧ができます。
Can Configure (設定可能)	**[Can Configure]** (設定可能) に設定されたグループとユーザーは、他のすべてのアクセス許可に加えて、スキャンの設定を変更できます。

ターゲットのスキャン

さまざまな形式を使用して、スキャンのターゲットを指定できます。次の表は、ターゲットの種類、例、およびTenable Nessusがそのターゲットの種類をスキャンしたときに発生する状況についての簡単な説明を示しています。

ターゲットの説明	例	説明
1つのIPv4アドレス	192.168.0.1	Tenable Nessusは、1つのIPv4アドレスをスキャンします。
1つのIPv6アドレス	2001:db8::2120:17ff:fe56:333b	Tenable Nessusは、1つのIPv6アドレスをスキャンします。
スコープ識別子を持つ1つのリンクローカルIPv6アドレス	fe80:0:0:0:216:cbff:fe92:88d0%eth0	Tenable Nessusは、1つのIPv6アドレスをスキャンします。 Tenable Nessusは、Windowsプラットフォームでスコープ識別子のインターフェースインデックスの代わりにインターフェース名を使用することをサポートしていません。
少数のIPv4またはIPv6アドレスのリスト	192.168.0.1, 192.169.1.1	Tenable Nessusはアドレスのリストをスキャンします。各アドレスはコンマまたは改行で区切ります。区切りがないと、Nessusはリストを読み取ることができません。
開始アドレスと終了アドレスを持つIPv4範囲	192.168.0.1-192.168.0.255	Tenable Nessusは、開始アドレスから終了アドレスまでのすべてのIPv4アドレス(両方のアドレスを含む)をスキャンします。
1つまたは複数のオクテットが数値範囲に置き換えら	192.168.0-1.3-5	次のように、オクテット範囲で指定された値のすべての組み合わせに展開されます: 192.168.0.3、192.168.0.4、192.168.0.5、192.168.1.3、192.168.1.4、

ターゲットの説明	例	説明
れたIPv4アドレス		192.168.1.5。
CIDR表記のIPv4サブネット	192.168.0.0/24	Tenable Nessusは、指定されたサブネット内のすべてのアドレスをスキャンします。指定されたアドレスは開始アドレスではありません。同じCIDRでサブネット内の任意のアドレスを指定すると、同じホストのセットをスキャンします。
ネットマスク表記のIPv4サブネット	192.168.0.0/255.255.255.128	Tenable Nessusは、指定されたサブネット内のすべてのアドレスをスキャンします。このアドレスは開始アドレスではありません。同じネットマスクでサブネット内の任意のアドレスを指定すると、同じホストをスキャンします。
IPv4またはIPv6アドレスに解決可能なホスト	www.yourdomain.com	Tenable Nessusは、1つのホストをスキャンします。ホスト名が複数のアドレスに解決される場合、スキャンするアドレスは最初のIPv4アドレスです。または、IPv4アドレスに解決されない場合は、最初のIPv6アドレスです。
CIDR表記でIPv4アドレスに解決可能なホスト	www.yourdomain.com/24	Tenable Nessusは、このホスト名をIPv4アドレスに解決した後に、CIDR表記の他のIPv4アドレスと同様に扱います。
ネットマスク	www.yourdomain.com/255.255.252.0	Tenable Nessusは、ホスト名を

ターゲットの説明	例	説明
表記の IPv4 アドレスに解決できるホスト		IPv4 アドレスに解決した後に、ネットマスク表記の他の IPv4 アドレスと同様に扱います。
IPv6 スコープ識別子がオプションで後に続くテキスト「link6」	link6 または link6%16	Tenable Nessus は、マルチキャスト ICMPv6 エコーリクエストを、スコープ識別子で指定されたインターフェースで ff02::1 アドレスに送信します。Tenable Nessus は、リクエストに応答するすべてのホストをスキャンします。IPv6 スコープ識別子を指定しない場合、Tenable Nessus はすべてのインターフェースにリクエストを送信します。 Tenable Nessus は、Windows プラットフォームでスコープ識別子のインターフェースインデックスの代わりにインターフェース名を使用することをサポートしていません。
角括弧に囲まれた、1 つの IPv4 アドレスまたは IPv6 含む何らかのテキスト	"Test Host 1[10.0.1.1]" または "Test Host 2[2001:db8::abcd]"	Tenable Nessus は、括弧内の IPv4 または IPv6 アドレスを、通常の 1 つのターゲットのようにスキャンします。

ヒント: link6 ターゲット (「link6」のテキストで始まる) または 2 つの IPv6 範囲形式のいずれかに似たホスト名のターゲットを、ターゲットを一重引用符で囲むことにより、ホスト名として処理できます。

ポリシーの基本設定

注意: このトピックでは、ポリシーで設定できる **[Basic]** (基本) 設定について記載します。個別のスキャンでの **[Basic]** (基本) 設定に関しては、スキャンの Basic 設定を参照してください。

[Basic] (基本) 設定を使用することで、誰がポリシーにアクセスできるかを含む、ポリシーの基本的な側面を規定できます。

[Basic] (基本) 設定には、次のセクションが含まれます。

一般

ポリシーの一般的な設定です。

設定	デフォルト値	説明
Name (名前)	なし	ポリシーの名前を指定します。
Description (説明)	なし	(オプション) ポリシーの説明を指定します。

アクセス許可

ユーザーまたはグループにアクセス許可を設定して、他のユーザーにポリシーを共有できます。グループにアクセス許可を割り当てると、そのアクセス許可はグループ内のすべてのユーザーに適用されます。

アクセス許可	説明
No Access (アクセスなし)	(既定のユーザーのみ) このアクセス許可を設定されたグループとユーザーは、ポリシーに関与することはできません。
Can Use (使用可)	このアクセス許可を持つグループとユーザーは、ポリシーの設定の表示と、ポリシーを使用したスキャンの作成が可能です。
Can Edit (編集可)	このアクセス許可をもつグループとユーザーは、ポリシーの表示およびポリシーを使用したスキャンの作成に加えて、ユーザーのアクセス許可を除いたあらゆるポリシーの設定を変更できます。ただし、ポリシーのエクスポートおよび削除はできません。

注意: ポリシーの所有者だけが、ポリシーのエクスポートまたは削除を行えます。

検出スキャン設定

注意: スキャンがポリシーに基づいている場合、スキャンの **[Discovery]** (検出) 設定はできません。これらの設定は、関連するポリシーでのみ変更できます。

注意: Tenable Nessus 特定のスキャンまたはポリシーに必要な設定が示されています。

[検出] 設定では、検出とポートスキャン (ポート範囲や方法など) に関連した設定を行います。

Tenable が提供するスキャナーテンプレートの一部には、設定済みの検出設定が含まれます。

[カスタム] の事前設定オプションを選択した場合、または設定済みの検出設定を含まないスキャナーテンプレートを使用している場合、次のカテゴリに関する **[検出]** 設定を手動で設定できます。

注意: 次のテーブルには、**[Advanced Scan]** (詳細スキャン) テンプレートの設定が含まれます。選択したテンプレートによっては、特定の設定が使用できなかったり、デフォルト値が異なっていたりする場合があります。

Host Discovery (ホスト検出)

Tenable Nessus は、**[Host Discovery]** (ホスト検出) セクションのいくつかの設定をデフォルトで有効にします。**[Host Discovery]** (ホスト検出) セクションに初めてアクセスすると、**[Ping the remote host]** (リモートホストに Ping する) 項目が表示され、**[On]** (オン) に設定されています。

[Host Discovery] (ホスト検出) セクションには次の設定グループがあります。

- 全般設定
- Ping Methods (ping メソッド)
- 脆弱なデバイス
- Wake-on-LAN

設定	デフォルト値	説明
Ping the remote host (リモート ホストに ping)	日付を指定	[オン] に設定すると、ホストがアクティブかどうかを確認するために、スキャナーはリモートホストの複数のポートに ping を送信します。追加のオプション **[全般設定]** と **[ping メソッド]** が表示されます。 [オフ] に設定すると、スキャン時にスキャナーはリモートホストの複数のポートに ping を送信しません。

		注意: VMwareゲストシステムをスキャンするには、**[リモートホストの ping]** を **[オフ]** に設定する必要があります。
Scan unresponsive hosts (応答しないホストのスキャン)	Disabled (無効)	Nessus スキャナーが ping メソッドに応答しないホストをスキャンするかどうかを指定します。このオプションは、PCI 四半期外部スキャンテンプレートを使用するスキャンでのみ使用できます。
全般設定		
Test the local Nessus host (ローカルの Nessus ホストをテストする)	Enabled (有効)	有効になっている場合、ローカルの Nessus ホストをスキャンに含めます。この設定は、Nessus ホストがスキャンのターゲットネットワーク範囲に含まれる場合に使用されます。
Use Fast Network Discovery (高速ネットワーク検出を使用)	Disabled (無効)	無効になっている場合、ホストが ping に応答した際に Tenable Nessus は、誤検出を回避するために追加のテストを実行して、応答がプロキシやロードバランサーからのものでないことを確認します。これらのチェックは、特にリモートホストがファイヤーウォールで保護されている場合には時間が掛かります。 有効になっている場合、Tenable Nessus はこれらのチェックを行いません。
ping メソッド		
ARP	Enabled (有効)	アドレス解決プロトコル (ARP) を介して、ハードウェアアドレスを使ってホストに ping を実行します。これはローカルネットワークでのみ機能します。
TCP	Enabled (有効)	TCP を使用してホストに ping を実行します。
Destination ports (TCP) (デスティネーションポート (TCP))	`built-in` (ビルトイン)	TCP ping に特定のポートを使用するように宛先ポートを設定できます。ここでは、TCP ping でチェックするポートのリストを指定します。 `built-in`、1 つのポート、またはポートのコンマ区切りリス

		トのいずれかを入力します。 `built-in` で指定されるポートに関する詳細は、ナレッジベースの記事を参照してください。
ICMP	Enabled (有効)	Internet Control Message Protocol (ICMP) を使用してホストに ping を実行します。
Assume ICMP unreachable from the gateway means the host is down (ゲートウェイから ICMP に到達できない場合にはホストがダウンしていると見なす)	Disabled (無効)	ゲートウェイからの ICMP 到達不能は、ホストがダウンしていることを意味するものと想定します。ダウンしているホストに ping が送信されると、そのゲートウェイが ICMP 到達不能メッセージを返すことがあります。このオプションが有効になっている場合に ICMP 到達不能メッセージを受信すると、スキャナーはターゲットとなるホストがアクティブでないと見なします。このアプローチは、一部のネットワークで検出を高速化するのに役立ちます。 **注意:** 一部のファイヤーウォールとパケットフィルターは、アクティブになっているものの、フィルタリング対象のポートまたはプロトコルに接続されているホストに対してこれと同じ動作を使用します。そのため、このオプションが有効になっていると、ホストが実際はアクティブであってもダウンしていると見なされることがあります。
Maximum number of retries (最大再試行回数)	2	リモートホストに ping を再試行する回数を指定します。
UDP	Disabled (無効)	User Datagram Protocol (UDP) を使用してホストに ping を実行します。UDPはステートレスプロトコルであるため、通信はハンドシェイクダイアログによって実行されません。UDPベースの通信は、必ずしも信頼できるものではありません。また、UDPサービスとスクリーニングデバイスの性質のため、リモートから検出できるとは限りません。
Fragile Devices		
Scan Network Printers (ネットワーク	Disabled (無効)	有効になっている場合、スキャナーはネットワークプリンターをスキャンします。

プリンターをスキャン)		
Scan Novell Netware hosts (Novell Netware ホストをスキャン)	Disabled (無効)	有効になっている場合、スキャナーは Novell NetWare ホストをスキャンします。
Scan Operational Technology devices (オペレーショナルテクノロジーデバイスをスキャン)	Disabled (無効)	有効になっている場合、スキャナーは、環境要因や機器のアクティビティと状態を監視するオペレーショナルテクノロジー (OT) デバイス (プログラマブルロジックコントローラー (PLC) やリモート端末装置 (RTU) など) のフルスキャンを実行します。 無効になっている場合、スキャナーは ICS/SCADA Smart Scanning を使用して OT デバイスを慎重に識別し、それらのデバイスが検出された場合にはそのデバイスのスキャンを停止します。
ウェイクオン LAN		

List of MAC Addresses (MAC アドレスの一覧)	なし	[Wake-on-LAN (WOL)] メニューでは、スキャンを実行する前にマジックパケットを送信するホストを制御します。
		
		スキャンの前に開始するホストは、1 行ごとに 1 つの MAC が記載されたテキストファイルをアップロードすることによって指定します。
		
		例
		
		`33:24:4C:03:CC:C7`
		`FF:5C:2C:71:57:79`

Boot time wait (in minutes) (起動時の待ち時間 (分))	5	スキャンを実行する前にホストが起動するのを待機する時間。

ポートスキャン

[Port Scanning] (ポートスキャン) セクションには、ポートスキャナーの動作とスキャンするポートを定義する設定があります。

[Port Scanning] (ポートスキャン) セクションには、次の設定のグループが含まれます。

- Ports (ポート)
- ローカルポートの列挙子
- ネットワークポートスキャナー

設定	デフォルト値	説明
Ports (ポート)		
Consider Unscanned Ports as Closed (スキャンされていないポートを閉じていると見なす)	Disabled (無効)	有効にすると、ポートが選択されたポートスキャナーでスキャンされていない場合 (たとえば、ポートが指定された範囲から外れている場合)、スキャナーはそのポートを閉じていると見なします。
Port Scan Range (ポートのスキャン範囲)	デフォルト	スキャンされるポートの範囲を指定します。 サポートされている範囲は次のとおりです。 • `default` (デフォルト) – `nessus-services` ファイルで指定した約 4,790 個のよく使用されるポートをスキャンするようにスキャナーに指示します。`default` キーワードを他のポートおよびポート範囲と組み合わせることもできます。 **注意:** 次の正規表現を使った 4 つの全置換操作を、それをサポートしているテキストエディターで連続で実行すれば、`nessus-services` ファイルをカスタムのポートリストに変換できます。 • `.*\s+(\d+)\/(tcp|udp)(\r\n|\r|\n)` を `$1\/$2` に • `(\d+)\/(tcp|udp)` を `$2:$1` に • `tcp` を `T` に

設定	デフォルト値	説明
		• udp を U に nessus-services ファイルは、オペレーティングシステムに応じた次のディレクトリにあります。 • Linux – /opt/nessus/var/nessus/nessus-services • Windows – C:\ProgramData\Tenable\Nessus\nessus\nessus-services • macOS – /Library/Nessus/run/var/nessus/nessus-services • all (すべて) – ポート 0 を含む 65,536 個のポートをすべてスキャンするようにスキャナーに指示します。all キーワードを他の範囲と組み合わせることはできません。 • コンマ区切りのポートのリスト (例: **21,23,25,80,110**) やポート範囲 (例: **1-1024,9000-9200**、0 を除くすべてのポートをスキャンする場合は **1-65535**、個別の範囲または重複する TCP および UDP ポート範囲をスキャンする場合は **T:1-1024,U:300-500** または **1-1024,T:1024-65535,U:1025**)、またはそれらの組み合わせ。 スキャンポリシーの **[Discovery]** (検出) 設定で UDP、SYN、または TCP ポートスキャナー設定を無効にすると、指定したポートの範囲にかかわらず、それらのポートがスキャンされません。UDP および TCP のポートスキャナー設定は、デフォルトでは無効になっています。SYN ポートスキャナー設定はデフォルトで有効になっています。
ローカルポートの列挙子		
SSH (netstat)	Enabled (有効)	有効にすると、スキャナーはローカルマシンから netstat を使用して開いているポートをチェックします。このオプションを使用するには、

設定	デフォルト値	説明
		ターゲットへのSSH接続を介してnetstatコマンドを実行できる必要があります。このスキャンは、Linuxベースのシステムを対象としており、認証認証情報を必要とします。この設定を使用するには、最初にSSH認証情報を設定する必要があります。
WMI (netstat)	Enabled (有効)	有効にすると、スキャナーはWMIベースのスキャン中にnetstatを使用して開いているポートを特定します。 さらに、スキャナーは次のように動作します。 • **[Port Scan Range]** (ポートのスキャン範囲) 設定で指定されたカスタム範囲を無視します。 • **[Consider unscanned ports as closed]** (スキャンされていないポートを閉じていると見なす) 設定が有効な場合には、スキャンされていないポートを引き続き閉じていると見なします。 ポート列挙子 (netstatまたはSNMP) が正常に機能すると、ポート範囲は *[all]* (すべて) になります。この設定を使用するには、最初にWindows認証情報を設定する必要があります。
SNMP	Enabled (有効)	有効にすると、ユーザーが適切な認証情報を入力した場合に、スキャナーはリモートホストをより効果的にテストし、より詳細な監査結果を生成できます。たとえば、返されたSNMP文字列のバージョンを調べることで、脆弱性が存在するかどうかを判断するCisco ルーターチェックが多数あります。この情報はこのような監査に必要です。
Only run network port scanners if local port enumeration failed (ローカルポートの列挙に	Enabled (有効)	この設定を有効にすると、スキャナーはネットワークポートスキャンの前に、ローカルポート列挙に基づいて判定します。ローカルポート列挙子が実行されると、その資産のすべてのネットワークポートスキャナーが無効になります。 この設定を無効にすると、スキャナーはローカルポート列挙ステータスに関係なく、ネットワークポートスキャンを実行します。

設定	デフォルト値	説明
失敗した場合にのみネットワークポートスキャナーを実行)		
Verify open TCP ports found by local port enumerators (ローカルポートの列挙子が検出した開いている TCP ポートを確認)	Disabled (無効)	有効にすると、ローカルポートエニュメレーター (WMI や netstat など) によってポートが検出された場合、スキャナーはリモートからもそのポートが開いていることを確認します。このアプローチは、何らかの形のアクセス制御 (TCP ラッパー、ファイヤーウォールなど) が使用されているかどうかを確認するのに役立ちます。
ネットワークポートスキャナー		
TCP	Disabled (無効)	内蔵の Tenable Nessus TCP スキャナーを使用して、完全な TCP 3 ウェイハンドシェイクを利用してターゲットの開いている TCP ポートを特定します。このオプションが有効になっている場合、**[ファイヤーウォールの自動検出をオーバーライド]** オプションも設定できます。
SYN	Enabled (有効)	内蔵の Tenable Nessus SYN スキャナーを使用して、ターゲットとなるホストの開いている TCP ポートを特定します。SYN スキャンは、完全な TCP 3 ウェイハンドシェイクを開始しません。スキャナーは、SYN パケットをポートに送信して SYN-ACK 応答を待機し、応答、または応答がないことに基づいてポートの状態を判断します。 このオプションが有効になっている場合、**[ファイヤーウォールの自動検出をオーバーライド]** オプションも設定できます。

設定	デフォルト値	説明
Override automatic firewall detection (ファイヤーウォールの自動検出をオーバーライド)	Disabled (無効)	この設定は、**[TCP]** または **[SYN]** のどちらかのオプションが有効になっている場合に有効化できます。 有効になっている場合、この設定は自動ファイヤーウォール検出をオーバーライドします。 この設定には、次の3つのオプションがあります。 • **積極的な検出を使用**: ポートが閉じているように見える場合でもプラグインの実行を試みます。このオプションは、本番環境のネットワークでは使用しないことをお勧めします。 • **ソフト検出を使用**: リセットが設定される頻度を監視する機能とダウンストリームのネットワークバイスで制限が設定されているかどうかを確認する機能を無効にします。 • **検出機能を無効化**: ファイヤーウォール検出機能を無効にします。
UDP	Disabled (無効)	このオプションは、Tenable Nessus のビルトイン UDP スキャナーを使用して、ターゲットの開いている UDP ポートを特定します。 プロトコルの性質により、ポートスキャナーが開いている UDP ポートとフィルタリングされている UDP ポートの違いを見分けるのは通常は不可能です。UDP ポートスキャナーを有効にすると、スキャン時間が大幅に増加し、信頼できない結果が検出される場合があります。可能な場合は、代わりに netstat または SNMP ポート列挙オプションを使用することを検討してください。

サービス検出

[Service Discovery] (サービス検出) セクションには、開いている各ポートにそのポートで実行されているサービスをマッピングしようとする設定があります。

[Service Discovery] (サービス検出) セクションには次の設定グループがあります。

- 全般設定
- Search for SSL/TLS Services

設定	デフォルト値	説明
全般設定		
Probe all ports to find services (すべてのポートをプローブしてサービスを見つける)	Enabled (有効)	有効にすると、スキャナーは、**[Port scan range]** (ポートのスキャン範囲) オプションで定義されているように、開いている各ポートをそのポートで実行されているサービスにマップしようとします。 **警告:** まれに、調査によって一部のサービスが中断され、予期しない副作用が生じることがあります。
Search for SSL based services (SSL ベースのサービスの検索)	オン	スキャナーが SSL ベースのサービスをテストする方法を制御します。 **警告:** すべてのポートで SSL 機能をテストすると、テスト対象のホストに破壊的な影響を与える可能性があります。
SSL/TLS/DTLS サービスの検索 (有効)		
Search for SSL/TLS on (SSL/TLS を検索)	既知の SSL/TLS ポート	SSL/TLS サービスの検索時に、スキャナーがターゲットとなるホストのどのポートを検索するかを指定します。 この設定には、次の3 つのオプションがあります。 • **なし** **注意:** このオプションを **[なし]** に設定すると、global_settings/disable_test_ssl_based_services KB 項目が有効になります。 • **既知の SSL/TLS ポート** • **すべての TCP ポート**

設定	デフォルト値	説明
Search for DTLS On	なし	DTLS サービスの検索時に、スキャナーがターゲットとなるホストのどのポートを検索するかを指定します。 この設定には、次のオプションがあります。 • **なし** • **既知の DTLS ポート** • **すべての UDP ポート**
Identify Certificates Expiring Within x Days (x 日以内に期限切れになる証明書を特定)	60	有効にすると、スキャナーは、指定した日数内に有効期限が切れる SSL および TLS 証明書を特定します。
Enumerate All SSL Ciphers (SSL 暗号をすべて列挙)	True	有効になっている場合、スキャナーは SSL/TLS サービスによってアドバタイズされた暗号のリストを無視し、すべての可能性のある暗号を使用して接続の確立を試みることで暗号を列挙します。
Enable CRL checking (connects to internet) (CRL チェックを有効化 (インターネットに接続))	False	有効になっている場合、スキャナーは特定されたどの証明書についても失効していないかどうかをチェックします。

ID

ID セクションでは、Active Directory データの収集を有効または無効にできます。

注意: このセクションは、Tenable One Enterprise 環境にのみ適用されます。

設定	デフォルト値	説明
全般設定		
Collect Identity Data from Active Directory (Active Directory から ID	Disabled (無効)	この設定を有効にすると、Tenable Nessus は Active Directory からユーザー、コンピューター、グループのオブジェクトを収集できるようになります。

設定	デフォルト値	説明
データを収集する)		この設定では、スキャン用の Active Directory ユーザーアカウントを指定する必要があります。また、スキャンの対象となっているドメインコントローラーで LDAPS を有効にする必要があります。

設定済みのディスカバリースキャン設定

次の表に記載されている通り、Tenable が提供するスキャナーテンプレートの一部には設定済みの検出設定が含まれます。設定済みの検出設定は、選択したテンプレートおよび **[Scan Type]** (スキャンの種類) の両方によって決定されます。

テンプレート	スキャンタイプ	設定済みの設定
Discovery (検出)		

Host Discovery (ホスト検出)	**Host enumeration** (デフォルト)	• 全般設定
		  ◦ ローカルの Nessus ホストを常にテストする
		  ◦ 高速ネットワーク検出を使用
		• ホストが使用する Ping
		  ◦ TCP
		  ◦ ARP
		  ◦ ICMP (2 回のリトライ)

	OS Identification (OS 識別)	• 全般設定
		  ◦ ローカルの Nessus ホストを常にテストする
		  ◦ 高速ネットワーク検出を使用
		• ホストが使用する Ping

		◦ TCP ◦ ARP ◦ ICMP
	ポートスキャン (共通ポート)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ 共通ポートをスキャンする ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	ポートスキャン (すべてのポート)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定

		◦ すべてのポートをスキャンする (1 ~ 65535) ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	Custom (カスタム)	すべてデフォルト
Vulnerabilities (脆弱性)		
Basic Network Scan (Basic Network スキャン)	**ポートスキャン (共通ポート)** (デフォルト)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ 共通ポートをスキャンする ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping

		◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	ポートスキャン (すべてのポート)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ すべてのポートをスキャンする (1 ~ 65535) ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	高速ネットワーク検出を使用	高速ネットワーク検出を使用
Advanced Scan (詳細なスキャン)	-	すべてデフォルト
Advanced Dynamic Scan (詳細な動的スキャン)	-	すべてデフォルト
Malware Scan (マルウェアスキャン)	**Host enumeration**	• 全般設定

	(デフォルト)	◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	Host enumeration (脆弱なホストを含む)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ) • 次を含むすべてのデバイスをスキャン ◦ プリンター ◦ Novell Netware ホスト
	Custom (カスタム)	すべてデフォルト
Mobile Device Scan (モバイルデバイススキャン)	-	-
Web Application Tests (ウェブアプリケーションテスト)	**ポートスキャン (共通ポート)** (デフォル	• 全般設定

	ト)	◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ 共通ポートをスキャンする ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	ポートスキャン (すべてのポート)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ すべてのポートをスキャンする (1 ~ 65535) ◦ 認証情報が提供されている場合は netstat を使用する

		◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	Custom (カスタム)	すべてデフォルト
Credentialed Patch Audit (認証パッチ監査)	**ポートスキャン (共通ポート)** (デフォルト)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ 共通ポートをスキャンする ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	ポートスキャン (すべてのポート)	• 全般設定 ◦ ローカルの Nessus ホ

		ストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ すべてのポートをスキャンする (1 ~ 65535) ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	Custom (カスタム)	すべてデフォルト
Badlock Detection (Badlock 検出)	**Normal** (デフォルト)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ デフォルトの Nessus のポート範囲をスキャンする

		◦ よく使用されるポート上の SSL/TLS を検出
	Quick (クイック)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ TCP ポート 23、25、80、443 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出
	Thorough	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出
	Custom (カスタム)	すべてデフォルト
Bash Shellshock Detection (Badlock Shellshock 検出)	**Normal** (デフォルト)	• 全般設定:

		◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ デフォルトの Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出 • 次を含むすべてのデバイスをスキャン ◦ プリンター ◦ Novell Netware ホスト
	Quick (クイック)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ TCP ポート 23、25、80、443 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出 • 次を含むすべてのデバイスを

		スキャン ◦ プリンター ◦ Novell Netware ホスト
	Thorough	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出 • 次を含むすべてのデバイスをスキャン ◦ プリンター ◦ Novell Netware ホスト
	Custom (カスタム)	すべてデフォルト
DROWN Detection (DROWN 検出)	**Normal** (デフォルト)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定

		◦ デフォルトの Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出
	Quick (クイック)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ TCP ポート 23、25、80、443 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出
	Thorough	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出

	Custom (カスタム)	すべてデフォルト
Intel AMT Security Bypass (Intel AMT セキュリティバイパス)	**Normal** (デフォルト)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ デフォルトの Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出
	Quick (クイック)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ TCP ポート 16992、16993、623、80、443 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出
	Thorough	• 全般設定: ◦ リモート ホストに ping

		◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出
	Custom (カスタム)	すべてデフォルト
Shadow Brokers Scan (Shadow Brokers スキャン)	**Normal** (デフォルト)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ デフォルトの Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出 • 次を含むすべてのデバイスをスキャン ◦ プリンター ◦ Novell Netware ホスト
	Thorough	• 全般設定:

		◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出 • 次を含むすべてのデバイスをスキャン ◦ プリンター ◦ Novell Netware ホスト
	Custom (カスタム)	すべてデフォルト
Spectre and Meltdown (Spectre および Meltdown)	**Normal** (デフォルト)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ デフォルトの Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出

	Thorough	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出
	Custom (カスタム)	すべてデフォルト
WannaCry Ransomware (WannaCryランサムウェア)	**Normal** (デフォルト)	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ デフォルトの Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出
	Quick (クイック)	• 全般設定: ◦ リモート ホストに ping

		◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ TCP ポート 139、445 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出
	Thorough	• 全般設定: ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定 ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出
	Custom (カスタム)	すべてデフォルト
Log4Shell	**Normal (標準)**	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする

		◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ デフォルトの Tenable Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出 • 脆弱なデバイスをスキャンしません。
	Quick (クイック)	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ TCP ポート 80、443 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出 • 脆弱なデバイスをスキャンしません。
	Thorough (デフォルト)	• 全般設定: ◦ Ping the remote host (リモート ホストに ping)

		◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出 • 脆弱なデバイスをスキャンしません。
	Custom (カスタム)	すべてデフォルト
Log4Shell Remote Checks (Log4Shell リモートチェック)	**Normal** (デフォルト)	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ デフォルトの Tenable Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出 • 脆弱なデバイスをスキャンし

		ません。

	Quick (クイック)	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ TCP ポート 80、443 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出 • 脆弱なデバイスをスキャンしません。
	Thorough	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出

		• 脆弱なデバイスをスキャンしません。
	Custom (カスタム)	すべてデフォルト
Log4Shell Vulnerability Ecosystem (Log4Shell 脆弱性のエコシステム)	**Normal (標準)**	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ デフォルトの Tenable Nessus のポート範囲をスキャンする ◦ よく使用されるポート上の SSL/TLS を検出 • 脆弱なデバイスをスキャンしません。
	Quick (クイック)	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定:

		◦ TCP ポート 80、443 をスキャン ◦ よく使用されるポート上の SSL/TLS を検出 • 脆弱なデバイスをスキャンしません。
	Thorough (デフォルト)	• 全般設定: ◦ Ping the remote host (リモート ホストに ping) ◦ ローカルの Tenable Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • サービス検出設定: ◦ すべての TCP ポートをスキャンする ◦ すべてのオープンなポート上の SSL を検出 • 脆弱なデバイスをスキャンしません。
	Custom (カスタム)	すべてデフォルト
コンプライアンス		
Audit Cloud Infrastructure (クラウドインフラ監査)	-	-
Internal PCI Network Scan (内部 PCI ネットワークスキャン)	**ポートスキャン (共通ポート)** (デフォルト)	• 全般設定 ◦ ローカルの Nessus ホ

		ストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ 共通ポートをスキャンする ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN スキャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	ポートスキャン (すべてのポート)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出を使用 • ポートスキャナーの設定 ◦ すべてのポートをスキャンする (1 ~ 65535) ◦ 認証情報が提供されている場合は netstat を使用する ◦ 必要に応じて SYN ス

		キャナーを使用する • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	Custom (カスタム)	すべてデフォルト
MDM Config Audit (MDM 設定監査)	-	-
Offline Config Audit (オフライン設定監査)	-	-
PCI Quarterly External Scan (PCI 四半期外部スキャン)	-	[Scan unresponsive hosts] (応答しないホストのスキャン) のデフォルト
Policy Compliance Auditing (ポリシーコンプライアンス監査)	**Default** (デフォルト)	• 全般設定 ◦ リモート ホストに ping ◦ ローカルの Nessus ホストを常にテストする • 次を含むすべてのデバイスをスキャン ◦ プリンター ◦ Novell Netware ホスト
	Custom (カスタム)	すべてデフォルト
SCAP and OVAL Auditing (SCAP および OVAL 監査)	**Host enumeration** (デフォルト)	• 全般設定 ◦ ローカルの Nessus ホストを常にテストする ◦ 高速ネットワーク検出

		を使用 • ホストが使用する Ping ◦ TCP ◦ ARP ◦ ICMP (2 回のリトライ)
	Custom (カスタム)	すべてデフォルト

アセスメントスキャン設定

注意: スキャンがポリシーに基づいている場合、スキャンの **[Assessment]** (評価) 設定は設定できません。これらの設定は、関連するポリシーでのみ変更できます。

[評価] 設定では、スキャンが脆弱性を識別する方法と識別される脆弱性を設定できます。これには、マルウェアの識別、総当たり攻撃に対するシステムの脆弱性の評価、ウェブアプリケーションの感染性が含まれます。

Tenable が提供するスキャナーテンプレートの一部には、設定済みの評価設定が含まれます。

[Custom] (カスタム) の事前設定オプションを選択した場合、または設定済みの評価設定を含まないスキャナーテンプレートを使用している場合、次のカテゴリに関する **[Assessment]** (評価) 設定を手動で設定できます。

注意: 次のテーブルには、**[Advanced Scan]** (詳細スキャン) テンプレートの設定が含まれます。選択したテンプレートによっては、特定の設定が使用できなかったり、デフォルト値が異なっていたりする場合があります。

一般

[General] (全般) セクションには、次の設定グループが含まれます。

- 正確性
- アンチウイルス
- SMTP

設定	デフォルト値	説明

正確性		
Override normal Accuracy (通常の冗長性をオーバーライド)	Disabled (無効)	場合によっては、欠陥が存在するかどうかをTenable Nessusがリモートで判断できません。パラノイアレポートが **[Show potential false alarms]** (誤ったアラームの可能性を表示) に設定されている場合、リモートホストに影響があると疑われる場合でも、毎回欠陥が報告されます。反対に、パラノイアの設定が **[Avoid potential false alarms]** (誤ったアラームの可能性を回避) になっていると、リモートホストに関する不確実性の要素があるときには、Tenable Nessusは常に欠陥を報告しません。これら2つの設定の中間の場合は、この設定を無効にします。
Perform thorough tests (may disrupt your network or impact scan speed) (徹底的なテストを実行する (ネットワークの混乱やスキャン速度への影響が生じる可能性あり))	Disabled (無効)	さまざまなプラグインの動作が増加します。たとえば、SMBファイル共有を調べる場合、プラグインは1つではなく3つのディレクトリレベルを深く分析できます。これにより、状況によってはネットワークトラフィックと分析が増加する可能性があります。詳細さを増すことにより、スキャンは介入的になり、ネットワークが中断する可能性が高くなりますが、より良い監査結果が出る見込みがあります。
アンチウイルス		
Antivirus definition grace period (in days) (アンチウイルス定義の猶予期間 (日))	0	日数 (0-7) を設定して、ウイルス対策ソフトウェアチェックの延期を設定します。ウイルス対策ソフトウェアチェックメニューを使用することで、ウイルス対策の署名が期限切れとみなされた場合に、特定の猶予期間を設けて報告するようにTenable Nessusに指示できます。デフォルトでは、署名が1日以上経過している場合、Tenable Nessusは署名を期限切れとみなします。この設定では、期限切れと報告するまでの期間を最大7日間まで設定できます。

SMTP	
Third party domain (サードパーティのドメイン)	Tenable Nessus は、各 SMTP デバイスを介してこのフィールドにリストされているアドレスにスパムを送信しようとします。このサードパーティのドメインアドレスは、Tenable Nessus がスキャンするサイトまたはスキャンが実行されるサイトの範囲外にある必要があります。そうでないと、SMTP サーバーによってテストが中止される場合があります。
From address (送信元アドレス)	SMTP サーバーに送信されたテストメッセージは、このフィールドで指定したアドレスから送信されたかのように表示されます。
To address (送信先アドレス)	Tenable Nessus は、このフィールドにリストされているメール受信者宛てにメッセージの送信を試みます。ほとんどのメールサーバーで有効なアドレスであるため、ポストマスターのアドレスはデフォルト値になっています。

総当たり

[Brute Force] (ブルートフォース) セクションには、次の設定のグループが含まれます。

- 全般設定
- Oracle Database
- Hydra

設定	デフォルト値	説明
全般設定		
Only use credentials provided by the user (ユーザーから提供された認証情報だけを使用します)	Enabled (有効)	状況によっては、Tenable Nessus はデフォルトアカウントと既知のデフォルトパスワードのテストに使用できます。これにより、無効な試行が連続して何度も実行され、オペレーティングシステムまたはアプリケーションでセキュリティプロトコルがトリガーされて、アカウントがロックアウトされることがあります。Tenable Nessus がこのようなテストを実行しないよう、この設定はデフォルトで有効になっています。
Oracle データベース		
Test default	Disabled (無	Oracle ソフトウェアの既知のデフォルトアカウントをテストしま

accounts (slow) (テストのデフォルトアカウント (低速))	効)	す。
Hydra **注意:** Hydra オプションは、スキャンを実行するスキャナーまたはエージェントと同じコンピューターに Hydra がインストールされている場合にのみ表示されます。		
Always enable Hydra (slow) (常に Hydra を有効にする (低速))	Disabled (無効)	Tenable Nessus がスキャンを実行するたびに Hydra を有効にします。

Logins file (ログインファイル)		Hydra がスキャン中に使用するユーザー名が入った .txt ファイルです。
		
		ユーザー名は 1 行に 1 つずつ入力し、ファイルの末尾は空行で終わる必要があります。たとえば、次のようになります。
		
		`<username1>`
		`<username2>`
		`<username3>`

Passwords file (パスワードファイル)		Hydra がスキャン中に使用するユーザーアカウントのパスワードが入った .txt ファイルです。
		
		パスワードは 1 行に 1 つずつ入力し、ファイルの末尾は空行で終わる必要があります。たとえば、次のようになります。
		
		`<password1>`
		`<password2>`
		`<password3>`

Number of parallel tasks (並行タスクの数)	16	同時に実行する Hydra テストの数です。デフォルトでは、この数は 16 になっています。

Timeout (秒単位)	30	ログオン試行 1 回あたりの秒数です。
Try empty passwords (パスワードなしで試行)	Enabled (有効)	有効にすると、Hydra はパスワードを使用せずにユーザー名を試します。
Try login as password (ログイン情報をパスワードとして試行)	Enabled (有効)	有効にすると、Hydra は対応するパスワードとしてユーザー名を試します。
Stop brute forcing after the first success (初回アクセスが成功した後にブルーとフォースを停止)	Disabled (無効)	有効にすると、アカウントへの初回アクセスが成功した後に、Hydra はブルートフォースのユーザーアカウントを停止します。
Add accounts found by other plugins to the login file (他のプラグインを使用して検出したアカウントをログインファイルに追加)	Enabled (有効)	無効にした場合、Tenable Nessus はログインファイルで指定されたユーザー名のみをスキャンに使用します。有効のままの場合、Tenable Nessus は他のプラグインを使用して他のユーザー名を検出し、それらをログインファイルに追加してスキャンに使用します。
PostgreSQL database name (PostgreSQL データベース名)		Hydra でテストを行うデータベースです。
SAP R/3 Client ID (0 ~ 99) (SAP R/3 クライアント ID (0 ~ 99))		Hydra でテストを行う SAP R/3 クライアントの ID です。
Windows	Local	これは *[Local accounts]* (ローカルアカウント)、*[Domain*

accounts to test (テストする Windows アカウント)	accounts (ローカルアカウント)	*Accounts]* (ドメインアカウント)、または *[Either]* (どちらか) に設定できます。
Interpret passwords as NTLM hashes (パスワードを NTLM ハッシュとして解釈)	Disabled (無効)	有効にすると、Hydra はパスワードを NTLM ハッシュとして解釈します。
Cisco login password (Cisco ログインパスワード)		このパスワードを使用して、ブルートフォースでパスワードが使用可能になる前に Cisco システムにログインすることができます。ここにパスワードを入力しない場合、Hydra はスキャンの初期段階でブルートフォースに成功した認証情報を使用してログインを試みます。
Web page to brute force (ブルートフォースするウェブページ)		HTTP 基本認証またはダイジェスト認証によって保護されているウェブページを入力します。ここにウェブページを入力しない場合、Hydra は、Tenable Nessus ウェブクローラによって検出された、HTTP 認証を必要とするページに対してブルートフォースを試みます。
HTTP proxy test website (HTTP プロキシがテストするウェブサイト)		Hydra が HTTP プロキシのブルートフォースに成功すると、ブルートフォースプロキシを介して、ここに入力したウェブサイトへのアクセスを試みます。
LDAP DN		Hydra が認証した LDAP 識別名スコープです。

SCADA

設定	デフォルト値	説明
Modbus/TCP コイルアクセス		Modbus は、1 の機能コードを使用して Modbus サーバーのコイルを読み取ります。コイルはバイナリ出力設定を表し、通常はアクチュエータにマッピングされます。コイルを読み取る機能により、攻撃者がシステムをプロファイルし、書き込みコイルメッセージを介して変更するレジスタの範囲を特定できます。
Start at Register (レジスタで開始)	0	スキャンを開始するレジスタです。
End at Register (レジスタで終了)	16	スキャンを停止するレジスタです。
ICCP/COTP TSAP アドレス指定の脆弱性		ICCP/COTP TSAP アドレス指定メニューは、可能な値を試すことにより、ICCP サーバー上の接続指向トランスポートプロトコル (COTP) トランスポートサービスアクセスポイント (TSAP) の値を決定します。
Start COTP TSAP (開始 COTP TSAP)	8	試行する開始 TSAP 値を指定します。
Stop COTP TSAP (終了 COTP TSAP)	8	試行する終了 TSAP 値を指定します。Tenable Nessus は、**開始値**と**停止値**の間のすべての値を試します。

ウェブアプリケーション

デフォルトでは、Tenable Nessus はウェブアプリケーションをスキャンしません。**[Web Application]** (ウェブアプリケーション) セクションへの初回アクセス時に表示される **[Scan Web Applications]** (ウェブアプリケーションのスキャン) 設定は、**[Off]** (オフ) に設定されています。次の表にリストされているウェブアプリケーションの設定を変更するには、**[Off]** (オフ) ボタンをクリックします。その他の設定が表示されます。

[Web Applications] (ウェブアプリケーション) セクションには、次の設定のグループが含まれます。

- 全般設定
- Web クローラ
- アプリケーションテストの設定

設定	デフォルト値	説明
Use a custom User-Agent (カスタムユーザーエージェントを使用)	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Tenable Nessus がスキャン中に偽装するブラウザの種類を指定します。
ウェブクローラ		
Start crawling from (クロールの開始点)	/	Tenable Nessus がテストする最初のページの URL です。複数のページをテストする必要がある場合は、コロン区切り文字を使用してページを区切ります (例: `/:/php4:/base`)。
除外されたページ (正規表現)	/server_ privileges\.php|logout	クロール対象から除外するウェブサイトの一部を指定します。たとえば、/manual ディレクトリとすべての Perl CGI を除外するには、このフィールドを次のように設定します。(^/manual) <> (\.pl(\?.*)?$) Tenable Nessus は、文字列の照合と処理、および Perl 互換の正規表現 (PCRE) のために POSIX の正規表現をサポートしています。
Maximum pages to crawl (クロールできる最大ページ)	1000	クロールするページの最大数です。
Maximum depth to crawl	6	開始ページごとに Tenable Nessusがたどるリンクの数を制限します。

設定	デフォルト値	説明
(クロールできる最大深度)		
Follow dynamic pages (動的ページに従う)	Disabled (無効)	この設定を有効にすると、Tenable Nessus は動的リンクをたどるので、上記設定のパラメーターを超える場合があります。
アプリケーションテストの設定		
Enable generic web application tests (一般的なウェブアプリケーションテストを有効にする)	Disabled (無効)	次のアプリケーションテスト設定を有効にします。
Abort web application tests if HTTP login fails (HTTP でのログインが失敗した場合にウェブアプリケーションのテストを中止する)	Disabled (無効)	Tenable Nessus が HTTP 経由でターゲットにログインできない場合、すべてのウェブアプリケーションのテストを実行しません。
Try all HTTP methods (すべての HTTP メソッドを試行する)	Disabled (無効)	このオプションは、ウェブフォームのテストを強化するために POST リクエストを使用するように Tenable Nessus に指示します。デフォルトでは、このオプションを有効にしていない限り、ウェブアプリケーションのテストには GET リクエストの

設定	デフォルト値	説明
		みが使用されます。一般的には、ユーザーがアプリケーションにデータを送信する際に、より複雑なアプリケーションで POST メソッドが使用されます。この設定により、より綿密なテストが提供されますが、所要時間が大幅に長くなる可能性があります。選択すると、Tenable Nessus は GET リクエストと POST リクエストの両方で各スクリプトまたは変数をテストします。この設定により、より綿密なテストが提供されますが、所要時間が大幅に長くなる可能性があります。
Attempt HTTP Parameter Pollution (HTTP パラメーター汚染を試行する)	Disabled (無効)	ウェブアプリケーションのテストを実行する場合、変数にコンテンツを挿入すると同時に、同じ変数に有効なコンテンツを提供することにより、フィルタリングメカニズムのバイパスを試みます。たとえば、通常の SQL インジェクションテストは /target.cgi?a='&b=2 のようになります。HTTP パラメーター汚染 (HPP) を有効にすると、リクエストは /target.cgi?a='&a=1&b=2 のようになります。
Test embedded web servers (埋め込みウェブサーバーをテストする)	Disabled (無効)	組み込みウェブサーバーは多くの場合において静的であり、カスタマイズ可能な CGI スクリプトは含まれていません。さらに、組み込みウェブサーバーは、スキャン時に時々クラッシュしたり応答しなかったりする場合もあります。このオプションを使用して、組み込みウェブサーバーを他のウェブサーバーとは別にスキャンすることを Tenable は推奨します。
Test more than one parameter at a	Disabled (無効)	この設定では、HTTP リクエストで使用される引数値の組み合わせを管理します。このオプションにチェックマークを入れないデフォルトで

設定	デフォルト値	説明
time per form (フォームごとに 1 度に複数のパラメーターをテストする)		は、攻撃文字列で 1 つのパラメーターを一度にテストし、追加のパラメーターに対する非攻撃バリエーションを試すことはありません。たとえば Tenable Nessusは、各組み合わせをテストせずに、b と c が他の値を許可する、`/test.php?arg1=XSS&b=1&c=1`を試みます。これは、最小の結果セットを生成してテストする最速の方法です。 この設定には、次の 4 つのオプションがあります。 • **Test random pairs of parameters**: この形式のテストでは、パラメーターのランダムなペアの組み合わせがランダムにチェックされます。これは、複数のパラメーターをテストする最速の方法です。 • **パラメーターのすべてのペアのテスト (低速)**: この形式のテストは、1 つの値のテストよりも若干低速になりますが、より効率的です。複数のパラメーターをテストしながら、攻撃文字列、単一変数の変化の関係をテストし、他のすべての変数に最初の値を使用します。たとえば、Tenable Nessus は `/test.php?a=XSS&b=1&c=1&d=1` を試み、その後、ある変数に攻撃文字列が付与され、ある変数はあらゆる可能な値を循環し (ミラープロセス中に発見されるように)、その他の変数には最初の値が付与されるようにします。この例では、各変数の最初の値が 1 の場合、Tenable Nessusは `/test.php?a=XSS&b=3&c=3&d=3`をテ

設定	デフォルト値	説明
		ストしません。 • **Test random combinations of three or more parameters (slower)**: この形式のテストでは、3つ以上のパラメーターの組み合わせがランダムにチェックされます。ペアのパラメーターのみのテストよりも綿密にチェックされます。組み合わせの数を3つ以上に増やすと、ウェブアプリケーションのテスト時間は長くなります。 • **パラメーターのすべての組み合わせのテスト (最も遅い)**: このテスト方法では、攻撃文字列と変数への有効な入力のあらゆる可能な組み合わせをチェックします。すべてのペアのテストが速度を上げるためにより少ないデータセットを作成しようとするのに対し、すべての組み合わせでは時間を妥協せずにテストの完全なデータセットを使用します。このテスト方法では、完了するまでに長時間かかる場合があります。
Do not stop after first flaw is found per web page (各ウェブページで最初の欠陥が見つかっても停止しないでください)	ウェブサーバーあたり1つのフローが見つかると停止します (最速)	この設定により、新しい欠陥が対象となるタイミングが決まります。これはスクリプトレベルで適用されます。XSSの欠陥を検出しても、SQLインジェクションまたはヘッダーインジェクションの検索は無効になりませんが、特に指定しない限り特定のポートの種類ごとに最大1つのレポートがあります。同じ攻撃によってキャッチされた場合、同じ種類のいくつかの欠陥 (XSS、SQLiなど) が報告される可能性があります。 このオプションが無効になっている場合、スキャンはウェブページ上で欠陥を発見するとすぐ

設定	デフォルト値	説明
		に、次のウェブページに移動します。 このオプションを有効にする場合は、次のいずれかのオプションを選択します。 • **Stop after one flaw is found per web server (fastest)** - (デフォルト) スクリプトによってウェブサーバー上で欠陥が検出されるとすぐに、Tenable Nessus は停止して別のポート上の異なるウェブサーバーに切り替えます。 • **Stop after one flaw is found per parameter (slow)** - CGI のパラメーターで1種類の欠陥 (XSS など) が検出されるとすぐに、Tenable Nessus は同じ CGI の次のパラメーター、次の既知の CGI、または次のポートもしくはサーバーに切り替えます。 • **Look for all flaws (slowest)** - 検出された欠陥にかかわらず、広範なテストを実行します。このオプションは非常に詳細なレポートを生成する可能性があるため、多くの場合において推奨されません。
URL for Remote File Inclusion (リモートファイルインクルード用の URL)	http://rfi.nessus.org/rfi.txt	リモートファイルインクルージョン (RFI) のテスト中、この設定によりテストに使用するリモートホスト上のファイルが指定されます。デフォルトでは、Tenable Nessus は Tenable, Inc. が RFI テスト用にホストする安全なファイルを使用します。スキャナーがインターネットに到達できない場合は、内部でホストされているファイルを使用して、より正確な RFI テストを実行できます。

設定	デフォルト値	説明
Maximum run time (min) (最大ランタイム (分))	5	このオプションでは、ウェブアプリケーションのテストの実行に費やされる時間を分単位で管理します。このオプションのデフォルトは 60 分で、所定のウェブサイトのすべてのポートと CGI に適用されます。通常、小規模なアプリケーションを使用するウェブサイトのローカルネットワークのスキャンは1時間以内に完了しますが、大規模なアプリケーションを使用するウェブサイトにはより大きい値が必要になる場合があります。

Windows

Windows セクションには、次の設定のグループが含まれます。

- 全般設定
- ユーザー列挙メソッド

設定	デフォルト値	説明
全般設定		
Request information about the SMB Domain (SMBドメインに関する情報をリクエストする)	Disabled (無効)	有効にすると、センサーがローカルユーザーの代わりにドメインユーザーをクエリします。この設定を有効にすると、プラグイン 10892 および 10398 を実行できるようになり、プラグイン 72684 および 10907 がドメインユーザーをクエリできるようになります。
ユーザー列挙メソッド		
ユーザー検出に適した数のユーザー列挙メソッドを有効にできます。		
SAM Registry (SAM レジストリ)	Enabled (有効)	Tenable Nessus は、Security Account Manager (SAM) レジストリを介してユーザーを列挙します。
ADSI Query (ADSI クエリ)	Enabled (有効)	Tenable Nessus は、Active Directory Service Interfaces (ADSI) を介してユーザーを列挙します。ADSI を使用する

		には、**[Credentials]** (認証情報) > **[Miscellaneous]** (その他) > **[ADSI]** で認証情報を設定する必要があります。
WMI Query (WMI クエリ)	Enabled (有効)	Tenable Nessus は、Windows Management Interface (WMI) を介してユーザーを列挙します。
RID Brute Forcing (RID ブルートフォース)	Disabled (無効)	Tenable Nessus は、相対識別子 (RID) ブルートフォースを介してユーザーを列挙します。この設定を有効にすると、**[Enumerate Domain Users]** (ドメインユーザーを列挙する) および **[Enumerate Local User]** (ローカルユーザーを列挙する) 設定を有効にします。
ドメインユーザーを列挙する (RID ブルートフォースが有効な場合に利用可能)		
Start UID (開始 UID)	1000	Tenable Nessus がドメインユーザーの列挙を試みる ID 範囲の開始部分です。
End UID (終了 UID)	1200	Tenable Nessus がドメインユーザーの列挙を試みる ID 範囲の終了部分です。
ローカルユーザーを列挙する (RID ブルートフォースが有効な場合に利用可能)		
Start UID (開始 UID)	1000	Tenable Nessus がローカルユーザーの列挙を試みる ID 範囲の開始部分です。
End UID (終了 UID)	1200	Tenable Nessus がローカルユーザーの列挙を試みる ID 範囲の終了部分です。

マルウェア

[Malware] (マルウェア) セクションには、次の設定のグループが含まれます。

- 全般設定
- ハッシュおよび許可リストファイル
- ファイルシステムスキャン

設定	デフォルト値	説明
ハッシュと許可リストファイル		

Custom Netstat IP Threat List (カスタム Netstat IP 脅威リスト)	なし	検出する既知の不良 IP アドレスのリストを含むテキストファイルです。 ファイルの各行は、IPv4 アドレスで始める必要があります。オプションとして、IP アドレスの後にコンマを追加してその後に説明を続けると、説明を追加できます。コンマ区切りのコメントに加えて、ハッシュ区切りのコメント (# など) も使用できます。 **注意:** Tenable は、テキストファイル内のプライベート IP 範囲を検出しません。
Provide your own list of known bad MD5 hashes (既知の不正な MD5 ハッシュのリストを指定する)	なし	追加の不良 MD5 ハッシュをテキストファイル (MD5 ハッシュを 1 行につき 1 つ入力) を介してアップロードすることができます。任意でハッシュの説明を含めることもできます。その場合は、ハッシュの後にコンマを追加し、続けて説明を入力します。ターゲットのスキャン中に一致するものを Tenable Nessus が見つけた場合、スキャン結果に説明が表示されます。コンマ区切りのコメントに加えて、標準のハッシュ区切りのコメント (例: #) も使用できます。
Provide your own list of known good MD5 hashes (既知の正常な MD5 ハッシュのリストを指定する)	なし	追加の正常な MD5 ハッシュをテキストファイル (MD5 ハッシュを 1 行につき 1 つ入力) を介してアップロードすることができます。アップロードされたファイル内に各ハッシュの説明を追加できます (オプション)。ハッシュの後にコンマを追加すると、その後に説明を続けることができます。Tenable Nessus によりターゲットのスキャン中に一致するものが見つかり、ハッシュの説明が提供された場合、スキャン結果に説明が表示されます。コンマ区切りのコメントに加えて、標準のハッシュ区切りのコメント (例: #) も使用できます。
Hosts file allowlist (ホストファイル許可リスト)	なし	Tenable Nessus は、システムホストファイルに侵害の兆候がないかチェックします (例: 侵害された Windows システム (ホストファイルチェック) というタイトルのプラグイン ID 23910)。このオプションを使用すると、スキャン中に Tenable Nessusに無視させる IP とホスト名のリストを含むファイルをアップロードできます。通常のテキストファイルの行ごとに 1 つの IP と 1 つのホスト名 (ターゲット上のホストファイルと同じ形式) を含めます。

Yara Rules (Yara ルール)		
Yara Rules (Yara ルール)	なし	スキャンに適用される YARA ルールを含む .yar ファイルです。1 回のスキャンでアップロードできるファイルは 1 つのみであるため、すべてのルールを 1 つのファイルに含めてください。詳細は、yara.readthedocs.io を参照してください。
ファイルシステムスキャン		
Scan file system (ファイルシステムのスキャン)	Off (オフ)	このオプションを有効にすると、ホストコンピューターのシステムディレクトリとファイルをスキャンできます。 **警告:** 10 台以上のホストを対象としたスキャンでこの設定を有効にすると、パフォーマンスが低下する可能性があります。
Windows ディレクトリ		
Scan %Systemroot% (%Systemroot% スキャン)	Off (オフ)	ファイルシステムのスキャンを有効にして、%Systemroot% をスキャンします。
Scan %ProgramFiles% (%ProgramFiles% スキャン)	Off (オフ)	ファイルシステムのスキャンを有効にして、%ProgramFiles% をスキャンします。
Scan %ProgramFiles (x86)% (%ProgramFiles (x86)% スキャン)	Off (オフ)	ファイルシステムのスキャンを有効にして、%ProgramFiles (x86)% をスキャンします。
Scan %ProgramData% (%ProgramData% スキャン)	Off (オフ)	ファイルシステムのスキャンを有効にして、%ProgramData% をスキャンします。
Scan User Profiles (ユーザープロファイルのスキャン)	Off (オフ)	ファイルシステムのスキャンを有効にして、ユーザープロファイルをスキャンします。

Linux ディレクトリ		
Scan $PATH ($PATH のスキャン)	Off (オフ)	$PATH の場所をスキャンするファイルシステムスキャンを有効にします。
Scan /home (/home のスキャン)	Off (オフ)	/home をスキャンするファイルシステムスキャンを有効にします。
MacOS ディレクトリ		
Scan $PATH ($PATH のスキャン)	Off (オフ)	$PATH の場所をスキャンするファイルシステムスキャンを有効にします。
Scan /Users (/Users のスキャン)	Off (オフ)	/Users をスキャンするファイルシステムスキャンを有効にします。
Scan /Applications (/Applications のスキャン)	Off (オフ)	/Applications をスキャンするファイルシステムスキャンを有効にします。
Scan /Library (/Library のスキャン)	Off (オフ)	/Library をスキャンするファイルシステムスキャンを有効にします。
カスタムディレクトリ		
Custom Filescan Directories (カスタムファイルスキャンディレクトリ)	なし	マルウェアファイルスキャンでスキャンするディレクトリをリストしたカスタムファイルです。ファイル内には、ディレクトリを 1 つずつ改行してリストします。Tenable Nessus では、`C:\` や `/` などのルートディレクトリや、`%Systemroot%` などの変数を使用できません。

データベース

設定	デフォルト値	説明
Oracle データベース		
Use detected SIDs (検出した SID を使用する)	Disabled (無効)	有効にすると、少なくとも 1 つのホスト認証情報と 1 つの Oracle データベース認証情報が設定されている場合、スキャナーはホスト認証情報を使用してターゲットのスキャンを認証してから、ローカルでの Oracle システム ID (SID) の検

		出を試行します。次に、指定されたOracle データベース認証情報と検出されたSID の使用の認証を試行します。 スキャナーがホスト認証情報を使用したターゲットのスキャンを認証できないか、ローカルでSID を検出しない場合、スキャナーはOracle データベース認証情報の手動で指定されたSID を使用してOracle データベースを認証します。

設定済みのアセスメントスキャン設定

次の表に記載されている通り、Tenable が提供するスキャナーテンプレートの一部には設定済みの評価設定が含まれます。設定済みの評価設定は、選択したテンプレートおよび **[Scan Type]** (スキャンの種類) の両方によって決定されます。

テンプレート	スキャンタイプ	設定済みの設定
Discovery (検出)		
Host Discovery (ホスト検出)	-	-
Vulnerabilities (脆弱性)		
Basic Network Scan (Basic Network スキャン)	**Default** (デフォルト)	• 全般設定 ◦ 誤ったアラームの回避 ◦ CGI スキャンの無効化 • ウェブアプリケーション ◦ ウェブアプリケーションスキャンの無効化
	Scan for known web vulnerabilities (既知のウェブの脆弱性をスキャン)	• 全般設定 ◦ 発生する可能性のある誤ったア

		ラームの回避 ◦ CGI スキャンの有効化 • ウェブアプリケーション ◦ "/" からクロールを開始する ◦ (最大) 1,000 ページをクロールする ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションテストが無効化
	Scan for all web vulnerabilities (quick) (すべてのウェブ脆弱性をスキャンする (簡易))	• 全般設定 ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの有効化 • ウェブアプリケーション ◦ "/" からクロールを開始する

		◦ (最大) 1,000 ページをクロールする ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションのテストを各 5 分間 (最大) 行う
	Scan for all web vulnerabilities (complex) (すべてのウェブの脆弱性をスキャン (複合))	• 全般設定: ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの有効化 ◦ 詳細なテストを実行する • ウェブアプリケーション: ◦ "/" からクロールを開始する ◦ (最大) 1,000 ページをクロールする

		◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションのテストを各 10 分間 (最大) 行う ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom (カスタム)	すべてデフォルト
Advanced Scan (詳細なスキャン)	-	-
Advanced Dynamic Scan (詳細な動的スキャン)	-	-
Malware Scan (マルウェアスキャン)	-	[Malware Settings] (マルウェア設定) のデフォルト
Mobile Device Scan (モバイルデバイススキャン)	-	-
Web Application Tests (ウェブアプリケーションテス	**Scan for known web vulnerabilities (既知のウェブの脆**	• 全般設定 ◦ 発生する可能性

ト)	**弱性をスキャン)**	のある誤ったアラームの回避 ◦ CGI スキャンの有効化 • ウェブアプリケーション ◦ "/" からクロールを開始する ◦ (最大) 1,000 ページをクロールする ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションテストが無効化
	Scan for all web vulnerabilities (quick) (すべてのウェブの脆弱性をスキャン (高速)) (デフォルト)	• 全般設定 ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの有効化 • ウェブアプリケーション ◦ "/" からクロールを

		開始する ◦ (最大) 1,000 ページをクロールする ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションのテストを各 5 分間 (最大) 行う
	Scan for all web vulnerabilities (complex) (すべてのウェブの脆弱性をスキャン (複合))	• 全般設定: ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの有効化 ◦ 詳細なテストを実行する • ウェブアプリケーション: ◦ "/" からクロールを開始する ◦ (最大) 1,000 ページをクロール

		する ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションのテストを各 10 分間 (最大) 行う ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom (カスタム)	すべてデフォルト
Credentialed Patch Audit (認証パッチ監査)	-	[Brute Force] (ブルートフォース)、[Windows]、[Malware] (マルウェア) のデフォルト
Badlock Detection (Badlock 検出)	-	-
Bash Shellshock Detection (Badlock Shellshock 検出)		[Web Crawler] (ウェブクローラー) のデフォルト
DROWN Detection (DROWN 検出)	-	-

Intel AMT Security Bypass (Intel AMT セキュリティバイパス)	-	-
Log4Shell	**デフォルト**	• 全般設定 ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの無効化 • Web Applications ◦ ウェブアプリケーションスキャンの無効化
Log4Shell Remote Checks (Log4Shell リモートチェック)	**デフォルト**	• 全般設定 ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの無効化 • Web Applications ◦ ウェブアプリケーションスキャンの無効化
Log4Shell Vulnerability Ecosystem (Log4Shell 脆弱性のエコシステム)	**デフォルト**	• 全般設定 ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの無

		効化 • Web Applications ◦ ウェブアプリケーションスキャンの無効化
Shadow Brokers Scan (Shadow Brokers スキャン)	-	-
Spectre and Meltdown (Spectre および Meltdown)	-	-
WannaCry Ransomware (WannaCryランサムウェア)	-	-
コンプライアンス		
Audit Cloud Infrastructure (クラウドインフラ監査)	-	-
Internal PCI Network Scan (内部 PCI ネットワークスキャン)	デフォルト	• 全般設定 ◦ 誤ったアラームの回避 ◦ CGI スキャンの無効化 • ウェブアプリケーション ◦ ウェブアプリケーションスキャンの無効化

	Scan for known web vulnerabilities (既知のウェブの脆弱性をスキャン)	• 全般設定 ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの有効化 • ウェブアプリケーション ◦ "/" からクロールを開始する ◦ (最大) 1,000 ページをクロールする ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションテストが無効化
	Scan for all web vulnerabilities (quick) (すべてのウェブ脆弱性をスキャンする (簡易))	• 全般設定 ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの有効化

		• ウェブアプリケーション ◦ "/" からクロールを開始する ◦ (最大) 1,000 ページをクロールする ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションのテストを各 5 分間 (最大) 行う
	Scan for all web vulnerabilities (complex) (すべてのウェブの脆弱性をスキャン (複合))	• 全般設定: ◦ 発生する可能性のある誤ったアラームの回避 ◦ CGI スキャンの有効化 ◦ 詳細なテストを実行する • ウェブアプリケーション: ◦ "/" からクロールを開始する

		◦ (最大) 1,000 ページをクロールする ◦ (最大) 6 個のディレクトリを横断する ◦ よく利用されるウェブアプリケーションで既知の脆弱性のためのテストを行う ◦ 一般的なウェブアプリケーションのテストを各 10 分間 (最大) 行う ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom (カスタム)	すべてデフォルト
MDM Config Audit (MDM 設定監査)	-	-
Offline Config Audit (オフライン設定監査)	-	-
PCI Quarterly External Scan (PCI 四半期外部スキャン)	-	-
Policy Compliance	-	-

Auditing (ポリシーコンプライアンス監査)		
SCAP and OVAL Auditing (SCAP および OVAL 監査)	-	-

レポートスキャン設定

レポートスキャン設定には次の設定グループが含まれます。

- 処理
- 出力

設定	デフォルト値	説明
処理中		
Override normal verbosity (通常の冗長性をオーバーライド)	Disabled (無効)	無効になっている場合、レポートには通常レベルのプラグイン活動が掲載されます。出力には、情報プラグイン 56310、64582、58651 の内容は含まれません。 有効になっている場合、この設定には次の2 つのオプションがあります。 • **ディスク容量に限りがあるため、最小限の情報をレポート** - プラグインのアクティビティに関してレポートに掲載する情報量を減らして、ディスクスペースへの影響を最小限に抑えます。 • **最大限の情報をレポート** – プラグインアクティビティに関してレポートに掲載する情報量を増やします。このオプションを選択した場合、出力には情報プラグイン 56310、64582、58651 の内容が含まれます。
Show missing patches that	Enabled (有	有効な場合、スキャンレポートに破棄されたパッチ

設定	デフォルト値	説明
have been superseded (置き換えられたことにより欠落しているパッチを表示する)	効)	の情報が含まれます。
Hide results from plugins initiated as a dependency (依存関係として開始されたプラグインからの結果を非表示)	Enabled (有効)	有効な場合、レポートに依存関係リストは含まれません。レポートに依存関係リストを含める場合は、この設定を無効にします。
Output		
Allow users to edit scan results (ユーザーがスキャン結果を編集できるようにする)	Enabled (有効)	この機能を有効にすると、ユーザーはレポートからアイテム削除できます。コンプライアンスまたはその他の種類の監査のためにスキャンを行う場合、スキャンが改ざんされていないことを示すためこの設定を無効にします。
Designate hosts by their DNS name (DNS 名でホストを指名する)	Disabled (無効)	レポート出力に IP アドレスではなくホスト名を使用します。
ping に応答するホストを表示します	Disabled (無効)	Ping に正常に応答したホストを報告します。
Display unreachable hosts (到達できないホストを表示する)	Disabled (無効)	この機能を有効にすると、ping リクエストに応答しなかったホストが無効としてセキュリティレポートで報告されます。大きな IP ブロックに対してはこのオプションを有効にしないでください。
Display Unicode characters (Unicode 文字を表示する)	Disabled (無効)	この機能を有効にすると、ユーザー名、インストールされているアプリケーション名、SSL 証明書情報などのプラグインの出力が Unicode で表示されます。 **注意:** プラグインの出力では、Unicode の文字列が

設定	デフォルト値	説明
		誤って解析されたり、切り捨てられたりする場合があります。この事象により、プラグインやカスタム監査での正規表現に問題が発生した場合は、この設定を無効にしてスキャンをやり直してください。

詳細なスキャン設定

注意: スキャンがポリシーに基づいている場合、スキャンの **[Advanced]** (詳細) 設定はできません。これらの設定は、関連するポリシーでのみ変更できます。

[詳細] 設定により、スキャン効率とスキャン動作をより詳細に制御でき、プラグインのデバッグも有効にできます。

Tenable が提供するスキャナーテンプレートの一部には、設定済みの詳細設定が含まれます。

[カスタム] の事前設定オプションを選択した場合、または詳細設定が事前設定されていない Nessus スキャナーテンプレートを使用している場合、次のカテゴリの **[詳細]** 設定を手動で設定できます。

- 全般設定
- パフォーマンス
- Unix Find コマンドの除外
- エージェントのパフォーマンス (エージェントスキャンのみ)
- Windows ファイル検索オプション
- デバッグ設定
- スキャン開始のシフト
- コンプライアンスの出力オプション
- 脆弱性オプション

注意: 次のテーブルには、**[Advanced Scan]** (詳細スキャン) テンプレートの設定が含まれます。選択したテンプレートによっては、特定の設定が使用できなかったり、デフォルト値が異なっていたりする場合があります。

設定	デフォルト値	説明
全般設定		
Enable Safe Checks (安全なチェックを有効化)	Enabled (有効)	有効にすると、リモートホストに悪影響を及ぼす可能性のあるすべてのプラグインが無効になります。
Stop scanning hosts that become unresponsive during the scan (スキャン中に反応しなくなるホストのスキャンを停止する)	Disabled (無効)	有効にすると、ホストの無応答状態が検出された場合に Tenable Nessus はスキャンを停止します。この状況は、スキャン中にユーザーがPCをオフにした場合、サービス拒否プラグイン後にホストが応答を停止した場合、またはセキュリティメカニズム (IDS など) がサーバーへのトラフィックのブロックを開始した場合に発生することがあります。通常これらのマシンでスキャンを継続すると、ネットワーク全体に不要なトラフィックが送信され、スキャンが遅延します。
Scan IP addresses in a random order (ランダムに IP アドレスをスキャンする)	Disabled (無効)	デフォルトでは、Tenable Nessus は IP アドレスのリストを順番にスキャンします。有効にすると、Tenable Nessus は IP アドレス範囲内のホストのリストをランダムな順番でスキャンします。通常このアプローチは、大規模なスキャン中にネットワークトラフィックを分散するのに有用です。
Automatically accept detected SSH disclaimer prompts (検出された SSH の免責メッセージを自動的に受け入れる)	Disabled (無効)	有効になっている場合、認証スキャンが免責プロンプトを提示するホストに SSH 経由で接続しようとすると、スキャナーが免責プロンプトを受け入れるのに必要なテキスト入力を行い、スキャンを継続します。 無効にすると、スキャナーがデバイスに接続して免責事項を了承することができないため、免責事項要求のあるホストに対する認証スキャンは失敗します。プラグインの出力にエラーが表示されます。
Scan targets with multiple domain names in parallel (複数のドメイン名	Disabled (無効)	無効になっている場合、Tenable Nessus の 1 つのスキャナーが同時にスキャンしないよう抑止し、こうしてホストの過負荷を防ぎます。代わりに Tenable Nessus スキャナーは、IP アドレスのスキャンの試行を、それがそのスキャナー上の同

設定	デフォルト値	説明
からなるターゲットを並列にスキャンする)		じスキャンタスクや複数のスキャンタスクに一度以上現れた場合でも順番に実行します。スキャン完了までの時間が長くなる可能性があります。 有効になっている場合、Tenable Nessus スキャナーは、1 つの IP アドレスに解決される複数のターゲットを同じスキャンタスク内で、または複数のスキャンタスクにまたがって同時にスキャン可能です。スキャンの完了までの時間は短くなりますが、ホストに負荷が掛かり、タイムアウトおよび不完全な結果が生じる可能性があります。
Trusted CAs (信頼できる CA)	なし	Tenable Nessus がスキャンを許可する認証局 (CA) を指定します。**[Trusted CAs]** (信頼できる CA) ボックスに、1 つまたは複数の CA のテキストを入力します。 **注意:** 開始テキスト `-----BEGIN CERTIFICATE-----` と終了テキスト `-----END CERTIFICATE-----` を含めます。 **ヒント:** 1 つのテキストファイルに証明書を 1 つ以上保存することができます。それぞれについて、開始テキストと終了テキストを含めます。 スキャナーレベルで信頼できる CA を指定することもできます。詳細は、カスタム CA を信頼するを参照してください。
パフォーマンス		
Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)	Disabled (無効)	有効にすると、Tenable は、送信パケットが多すぎてネットワークパイプが限界に近づいていることを検出できます。ネットワーク輻輳を検出すると、スキャンを調整して輻輳に対応し、緩和します。輻輳が緩和されると、Tenable は自動的にネットワークパイプ内の使用可能なスペースを再び使用しようとします。

設定	デフォルト値	説明
Network timeout (in seconds) (ネットワークタイムアウト (秒))	5	プラグイン内で特に指定されていない場合に、Tenable がホストからの応答を待機する時間を指定します。低速接続でスキャンしている場合、この値を高い秒数に設定しても構いません。
Max simultaneous checks per host (ホストごとの同時チェックの最大数)	5	Tenable スキャナーが 1 つのホストに対して同時に実行するチェックの最大数を指定します。
Max simultaneous hosts per scan (スキャンごとの同時ホストの最大数)	30 か、または Tenable Nessus スキャナーの詳細設定 max_hosts のうち小さい方の値。	スキャナーが同時にスキャンするホストの最大数を指定します。 **[Max simultaneous hosts per scan]** (スキャンごとの同時ホストの最大数) に、スキャナーの max_hosts の設定値より大きい値を設定すると、Nessus は **[Max simultaneous hosts per scan]** (スキャンごとの同時ホストの最大数) の値を **max_hosts** の値に制限します。たとえば、**[Max simultaneous hosts per scan]** (スキャンごとの同時ホストの最大数) の値を 150 に設定した場合、スキャナーの **max_hosts** が 100 に設定されているとしたら、この値は 100 ターゲットを超えています。したがって、Nessus が同時にスキャンするホストの最大数は 100 となります。
Max number of concurrent TCP sessions per host (ホストあたりに同時に実行できるの最大 TCP セッション数)	なし	単一ホストに対して確立された TCP セッションの最大数を指定します。 この TCP スロットリングオプションは、SYN スキャナーが送信する 1 秒あたりのパケット数も制御し、その数は TCP セッションの 10 倍になります。たとえば、このオプションが 15 に設定されている場合、SYN スキャナーは最大で毎秒 150 パケットを送信します。
Max number of concurrent TCP	なし	スキャンされるホストの数に関係なく、スキャン全体で確立される TCP セッションの最大数を指定します。

設定	デフォルト値	説明
sessions per scan (スキャンごとの同時 TCP セッションの最大数)		**注意:** [MAX NUMBER OF CONCURRENT TCP SESSIONS PER SCAN] (スキャンあたりの同時 TCP セッションの最大数) 設定は、ディスカバリースキャンでは強制できません。global.max_simult_tcp_sessions Nessus Engine 設定 (各スキャナーで設定) は、1 つのスキャナーで実行されるすべてのスキャンの合計に適用される絶対上限です (たとえば、4 つのスキャナーがあり、それらが同時に生成する TCP セッションの数が合計で 10000 を超えないようにするには、個々のスキャナーのグローバル設定を 2500 に設定します)。
Unix find コマンドのオプション		
Command Timeout (コマンドタイムアウト)	240	Unix システムで find コマンドを実行できる最大秒数です。すべての **Find** コマンドでこのタイムアウトが使用されるわけではありません。 **注意:** プラグインのすべての **Find** コマンドの実行を完了し、プラグインのタイムアウトを回避するには、スキャナーの **[Advanced Settings]** (詳細設定) にある timeout_<plugin ID> でそのプラグインのタイムアウトを調整する必要があります。
Exclude Filepath (除外するファイルパス)	なし	Unix システムで find コマンドを使用して検索する、すべてのプラグインから除外するファイルパスのリストを含むプレーンテキストファイルです。 ファイルでは、Unix の find コマンド -path 引数で許可されているパターンごとにフォーマットされた、1 行ごとに 1 つのファイルパスを入力します。詳細については、find コマンドの man page を参照してください。
Exclude Filesystem (ファイルシステムを除外)	なし	Unix システムで find コマンドを使用して検索するすべてのプラグインから除外するファイルシステムのリストを含むプレーンテキストファイル。 ファイルでは、Unix の find コマンド -fstype 引数でサポートされるファイルシステムの種類を使用して、1 行ごとに 1 つのファイルシステムを入力します。詳細については、find コマンドの man page を参照してください。

設定	デフォルト値	説明
Include Filepath (ファイルパスを含める)	なし	Unix システムで `find` コマンドを使用して検索する、すべてのプラグインから含めるファイルパスのリストを含むプレーンテキストファイルです。 ファイルでは、Unix の `find` コマンド `-path` 引数で許可されているパターンごとにフォーマットされた、1 行ごとに 1 つのファイルパスを入力します。詳細については、`find` コマンドの man page を参照してください。 ファイルパスを含めると、プラグインで検索される場所が増えるため、スキャンの継続時間が延びます。対象ができるだけ固有となるように指定してください。 **ヒント: [Include Filepath]** (ファイルパスを含める) と **[Exclude Filepath]** (ファイルパスを除外する) に同じファイルパスを含めないようにしてください。この競合によって、結果はオペレーティングシステムによって異なる場合がありますが、ファイルパスが検索から除外される可能性があります。
エージェントのパフォーマンスオプション		
Use Tenable supplied binaries for 'find' and 'unzip' (Tenable が提供したバイナリを「find」および「unzip」に使用します)	Disabled (無効)	有効にすると、`find` および `unzip` のオペレーティングシステムのネイティブコマンドを実行する代わりに、プラグインはエージェントベースのスキャン用のプラグインフィード内に含まれるバイナリを使用します。これにより、Tenable Agent `find` コマンドの CPU 消費を制御できます。この設定を有効にするもう 1 つの利点は、`find` または `unzip` がオペレーティングシステムでネイティブに見つからない場合に、フィードからコマンドを使用すると、これらのコマンドでプラグインの完全な実行を続行できることです。 この設定は、エージェントでローカルに設定できる [Scan Performance] (スキャンパフォーマンス) 設定と連携して機能します。この設定を有効にして、**[Scan Performance]** (スキャンパフォーマンス) 設定をデフォルト (**[高]**) 以外の設定に調整した場合、スキャン結果は、同じ設定の以前のスキャン

設定	デフォルト値	説明
		とは異なる場合があります。これは、CPU リソースが減少しているため、スキャンでファイルを見つける際にタイムアウトが発生する可能性があるためです。 **注意:** 詳細で完全な結果が必要なため、監査では Tenable フィードからの `find` や `unzip` バイナリを利用しません。 **注意:** この設定を有効にすると、プラグインが結果のバッチ処理をリクエストした際に、CPU 使用率が急激に上昇するか、100% に近くなる可能性があります。その後、次のバッチ処理がリクエストされるまで、CPU は低いレベルに低下します。
Windows ファイル検索オプション		
Windows Exclude Filepath (Windows で除外するファイルパス)	なし	Tenable の管理されていないソフトウェアのディレクトリスキャンを使用して検索するすべてのプラグインから除外するファイルパスのリストが含まれた、プレーンテキストファイルです。 ファイルに、除外するリテラル文字列としてフォーマットされた絶対または部分ファイルパスを 1 行につき 1 つ入力します。`E:\`、`E:\Testdir\`、`\Testdir\` など、絶対または相対ディレクトリ名を含めることができます。 **ヒント:** この設定を行わない場合、デフォルトの除外パスには `\Windows\WinSxS\` と `\Windows\servicing\` が含まれます。この設定を行う場合、Tenable はこれらの 2 つのパスをファイルに追加することを推奨します。これらのディレクトリは非常に遅く、管理されていないソフトウェアは含まれていません。
Windows Include Filepath (Windows で含めるファイルパス)	なし	Tenable の管理されていないソフトウェアのディレクトリスキャンを使用して検索するすべてのプラグインに含めるファイルパスのリストが含まれる、プレーンテキストファイルです。 ファイルに、含めたいリテラル文字列としてフォーマットされた絶対または部分ファイルパスを 1 行につき 1 つ入力します。`E:\`、`E:\Testdir\`、`C:\` など、絶対または相対ディレクトリ名だけを含めることができます。

設定	デフォルト値	説明
		注意: Windows のインクルードファイルパス は、デフォルトのインクルードディレクトリ (Windows の C: ドライブなど) よりも優先されます。そのため、他のディレクトリに加えてデフォルトのディレクトリを含める場合には、追加のファイルパス行にデフォルトのディレクトリをリストする必要があります。 **警告: Windows Include Filepath** (Windows で含めるファイルパス) と **Windows Exclude Filepath** (Windows で除外するファイルパス) の設定に同じファイルパスを含めないようにしてください。この競合により、ファイルパスは検索から除外されます。
デバッグ設定		
Log scan details (スキャンの詳細を記録する)	Disabled (無効)	nessusd.messages へのスキャン中に使用される各プラグインの開始時間と終了時間を記録します。
Enable plugin debugging (プラグインのデバッグを有効化)	Disabled (無効)	プラグインから利用可能なデバッグログを、このスキャンの脆弱性出力に添付します。
Audit Trail Verbosity (監査証跡の詳細)	Default (デフォルト)	プラグイン監査証跡の詳細度を制御します。**All audit trail data** は、スキャンにプラグインが含まれなかった理由を含みます。 **Default** では、詳細設定 で設定された監査証跡の詳細のグローバル設定を使用します。Tenable Nessus スキャンでは、スキャンは高度な設定の**監査証跡の詳細** (`audit_trail`) を使用します。エージェントスキャンでは、スキャンは詳細な設定の**監査証跡データを含める** (`agent_merge_audit_trail`) を使用します。
Include the KB (KB を含む)	デフォルト	追加のデバッグデータを含むスキャン KB を、スキャン結果に含めるかどうかを制御します。 Tenable Nessus スキャンでは、**デフォルト** で KB が含まれます。エージェントスキャンでは、**Default** (デフォルト) で 詳細設

設定	デフォルト値	説明
		定 で設定されたグローバル設定の **Include KB Data** (KB データを含む) (agent_merge_kb)を使用します。
Enumerate launched plugins (起動されたプラグインを列挙)	Disabled (無効)	スキャン中に Tenable Nessus が起動したプラグインのリストを表示します。プラグイン 112154 のスキャン結果でリストを表示できます。 **注意:** プラグイン 112154 を無効にすると、この設定が正しく機能しません。
スキャン開始のシフト		
Maximum delay (minutes) (最大遅延 (分))	0	(Agents 8.2 以降) 設定されている場合、エージェントグループ内の各エージェントは、指定された時間の値 (分) を最大値とするランダムな時間、スキャンの開始を遅らせます。同時に開始しないようにすることで、仮想マシン CPU などの共有リソースを使用するエージェントの影響を低減できます。 設定した最大遅延時間がスキャンウィンドウを超過する場合、Tenableは、スキャンウィンドウがクローズする最低 30 分前にエージェントがスキャンを開始するよう、最大遅延時間を短縮します。
コンプライアンス出力設定		
Maximum Compliance Output Length in KB (コンプライアンスの最大出力長 (KB))	128,000 KB	ターゲットから返される各コンプライアンスチェック値の最大出力長を制御します。コンプライアンスチェック値がこの設定の値より大きい場合、Tenable Nessus は結果を切り捨てます。 **注意:** コンプライアンススキャン処理が遅い場合、この設定の値を小さくして処理速度を向上させることを推奨します。
Maximum Compliance Check Timeout in Seconds (コンプラ	300 seconds (300 秒)	コンプライアンスチェックの最大タイムアウト期間を制御します。 この設定は、実行時間が長いチェック、特に Windows と Unix の監査の削除対象に対してコマンドを実行するチェック

設定	デフォルト値	説明
イアンスチェックの最大タイムアウト (秒))		において使用されます。このタイムアウト設定が利用可能な場合、他のすべてのタイムアウト設定よりも優先されます。
脆弱性オプション		
Scan for unpatched vulnerabilities (no patches or mitigations available) (パッチ未適用の脆弱性をスキャン (利用可能なパッチまたは軽減策なし))	Disabled (無効)	スキャンでパッチ未適用の脆弱性を検索するかどうかを指定します。これには、関連ベンダーにより**修正されない**ものとしてマークされた CVE が含まれます。 この設定を有効にすると、全体的な検出結果数が増える可能性があります。各プラットフォームとパッケージの組み合わせごとに個別のプラグインが生成されます。プラットフォームとパッケージの組み合わせに影響を与える CVE が他にも見つかった場合、その CVE は既存のプラグインに追加されます。 **注意:** パッチ未適用の脆弱性の検出結果を生成するようにスキャンを設定した後にこの設定をオフにすると、Tenable Nessus は次回のスキャンでパッチ未適用の検出結果を修正します。さらに、複数のスキャンが同じデバイスをターゲットとし、1 つのスキャンではパッチ未適用の脆弱性の検出が有効で、別のスキャンでは有効になっていない場合、検出結果はスキャンごとに異なる可能性があります。
Custom Red Hat Repository Mapping (カスタム Red Hat リポジトリマッピング)	無効の場合は、.json ファイルをアップロードする必要があります。	内部のカスタムリポジトリやミラーリングされたリポジトリを、対応する公式の Red Hat リポジトリにマップするための .json ファイルをアップロードしてください。この動作方法の詳細については、How Red Hat Local Vulnerability Checks Use Repositories To Determine Scope (Red Hat のローカル脆弱性チェックがリポジトリを使用して範囲を決定する方法) を参照してください。

設定済みの詳細なスキャン設定

次の表に記載されている通り、Tenable が提供する Nessus スキャナーテンプレートの一部には設定済みの詳細設定が含まれています。設定済みの詳細設定は、選択したテンプレートおよび **[Scan Type]** (スキャンの種類) の両方によって決定されます。

テンプレート	スキャンタイプ	設定済みの設定
Discovery (検出)		
Host Discovery (ホスト検出)	-	[Performance Options] (パフォーマンスオプション) のデフォルト
Vulnerabilities (脆弱性)		
Basic Network Scan (Basic Network スキャン)	**Default** (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大) ◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト
	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	Custom (カスタム)	すべてデフォルト

Advanced Scan (詳細なスキャン)	-	すべてデフォルト
Advanced Dynamic Scan (詳細な動的スキャン)	-	すべてデフォルト
Malware Scan (マルウェアスキャン)	**Default** (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大) ◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト
	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	Custom (カスタム)	すべてデフォルト
Mobile Device Scan (モバイルデバイススキャン)	-	[Debug Settings] (デバッグ設定) のデフォルト
Web Application Tests (ウェブアプリケーションテスト)	**Default** (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大)

		◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト
	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	Custom (カスタム)	すべてデフォルト
Credentialed Patch Audit (認証パッチ監査)	**Default** (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大) ◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト
	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同

		時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	Custom (カスタム)	すべてデフォルト
Badlock Detection (Badlock 検出)	-	すべてデフォルト
Bash Shellshock Detection (Badlock Shellshock 検出)	-	すべてデフォルト
DROWN Detection (DROWN 検出)	-	すべてデフォルト
Intel AMT Security Bypass (Intel AMT セキュリティバイパス)	-	すべてデフォルト
Log4Shell	-	すべてデフォルト
Log4Shell Remote Checks (Log4Shell リモートチェック)	-	すべてデフォルト
Log4Shell Vulnerability Ecosystem (Log4Shell 脆弱性のエコシステム)	-	すべてデフォルト
Shadow Brokers Scan (Shadow Brokers スキャン)	-	すべてデフォルト
Spectre and Meltdown (Spectre および Meltdown)	-	すべてデフォルト

WannaCry Ransomware (WannaCryランサムウェア)	-	すべてデフォルト
コンプライアンス		
Audit Cloud Infrastructure (クラウドインフラ監査)	-	[Debug Settings] (デバッグ設定) のデフォルト
Internal PCI Network Scan (内部 PCI ネットワークスキャン)	Default (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大) ◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト
	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	Custom (カスタム)	すべてデフォルト
MDM Config Audit (MDM 設定監査)	-	-
Offline Config Audit (オフライン設	-	[Debug Settings] (デバッグ設定)

定監査)		のデフォルト
PCI Quarterly External Scan (PCI 四半期外部スキャン)	**Default** (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大) ◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト
	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	Custom (カスタム)	すべてデフォルト
Policy Compliance Auditing (ポリシーコンプライアンス監査)	**Default** (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大) ◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト

	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	Custom (カスタム)	すべてデフォルト
SCAP and OVAL Auditing (SCAP および OVAL 監査)	**Default** (デフォルト)	• パフォーマンスオプション ◦ 30 の同時ホスト (最大) ◦ ホストごとに 4 件の同時チェック (最大) ◦ 5 秒のネットワーク読み取りタイムアウト
	Scan low bandwidth links (低帯域幅リンクのスキャン)	• パフォーマンスオプション : ◦ 2 個の同時に存在するホスト (最大) ◦ ホストごとに 2 件の同時チェック (最大) ◦ 15 秒のネットワーク読み取りタイムアウト ◦ Slow down the scan

		when network congestion is detected (ネットワーク輻輳の検出時にスキャンを減速させる)
	カスタム	すべてデフォルト

認証情報

スキャンまたはポリシーの**認証情報**を設定すると、ターゲットシステムをスキャンするためのローカルアクセス権を Tenable Nessus スキャナーに付与できるので、エージェントは不要になります。これにより、大規模なネットワークをスキャンしてローカルのエクスポージャーまたはコンプライアンス違反を検出する作業が簡単になります。前述のとおり、ポリシー作成手順の一部は省略可能な場合があります。作成すると、Tenable Nessus は推奨設定を使用してポリシーを保存します。

Tenable Nessus には、セキュアシェル (SSH) を介してリモートの Linux ホストにログインする機能があります。また、Windows ホストでは、Tenable Nessus はさまざまな Microsoft 認証技術を使用します。Tenable Nessus は、簡易ネットワーク管理プロトコル (SNMP) を使用して、ルーターとスイッチにバージョンと情報を照会することもできます。スキャン認証情報は `global.db` に保管されます。

ヒント: Tenable Nessus が認証情報に使用する暗号化の強度については、暗号強度を参照してください。

スキャンまたはポリシーの **[Credentials]** (認証情報) ページでは、スキャン時に認証情報を使用するように Tenable Nessus スキャナーを設定できます。認証情報を設定することで広範囲のチェックを実行でき、Tenable Nessus のスキャン結果はより正確になります。

データベース、SSH、Windows、ネットワークデバイス、パッチ管理サーバー、さまざまなプレーンテキスト認証プロトコル、およびその他を含むさまざまな形式の認証をサポートしています。

Tenable Nessus は、オペレーティングシステムの認証情報に加えて、その他の形式のローカル認証もサポートしています。

スキャンまたはポリシーの **[Credentials]** (認証情報) セクションでは、以下のタイプの認証情報を管理できます。

- クラウドサービス
- データベース (MongoDB、Oracle、MySQL、DB2、PostgreSQL、SQL Server を含む)

- ホスト (Windows ログイン、SSH、SNMPv3 を含む)
- その他のサービス (VMware、Red Hat Enterprise Virtualization (RHEV)、IBM iSeries、Palo Alto Networks PAN-OS、ディレクトリサービス (ADSI および X.509) を含む)
- モバイルデバイスの管理
- パッチ管理サービス
- プレーンテキスト認証メカニズム (FTP、HTTP、POP3、その他のサービスを含む)

認証情報を使用したスキャンでは、ローカルユーザーが実行できる任意の操作を実行できます。スキャンのレベルは、ユーザーアカウントに付与されている権限によって異なります。ログインアカウントを介してスキャナーに与えられる権限 (ルートまたは管理者アクセスなど) が多いほど、スキャン結果はより詳細になります。

注意: Tenable Nessus は、複数の同時認証接続を開きます。監査対象のホストに同時セッションに基づく厳格なアカウントロックアウトポリシーがないことを確認してください。

スキャンに 1 種類の認証情報の複数のインスタンスが含まれている場合、Tenable Nessus はスキャンに認証情報を追加した順に各スキャンターゲットで認証情報を試行します。

注意: Tenable Nessusログインに成功した最初の認証情報を使用して、ターゲット上で認証情報チェックを実行します。ある認証情報でログインが成功した後、Tenable Nessus は、別の認証情報がより大きな権限を持っていても、リスト内の他の認証情報を試すことはありません。

注意: Tenable Nessus スキャンに 1 種類の認証情報の複数のインスタンスが含まれている場合、Tenable Nessus は**スキャンに追加された同じ順序で**各認証情報を順番に使用して有効なターゲットへのログインを試みます。Tenable Nessus は正常にログインできる最初の認証情報を使用して、ターゲットで認証情報チェックを実行します。Tenable Nessus が認証情報セットを使用して正常にログインできるようになると、相対的なアクセスレベルに関係なく、スキャン内の他の認証情報ではログインを試行しません。

クラウドサービスの認証情報

Tenable Nessus は、Amazon Web Services (AWS)、Microsoft Azure、Rackspace、Salesforce.com をサポートしています。

AWS

ユーザーは、[Credentials] (認証情報) メニューから Amazon Web Service (AWS) を選択し、AWS のアカウントのコンプライアンス監査を行う認証情報を入力できます。

オプション	説明
AWS Access Key IDS	AWS アクセスキー ID の文字列です。
AWS Secret Key	AWS アクセスキー ID の認証を提供する AWS シークレットキーです。

AWS グローバル認証情報設定

オプション	デフォルト	説明
Regions to access (アクセスするリージョン)	Rest of the World (世界のその他の地域)	Tenable Nessus で AWS アカウントを監査するには、スキャンするリージョンを定義する必要があります。Amazon のポリシーにより、**中国**リージョンのアカウント設定を監査する場合は、**[Rest of the World]** (世界のその他の地域) の場合とは異なる認証情報が必要です。**[Rest of the World]** (世界のその他の地域) を選択すると、次の選択肢が表示されます。 • us-east-1 • us-east-2 • us-west-1 • us-west-2 • ca-central-1 • eu-west-1 • eu-west-2 • eu-central-1 • ap-northeast-1 • ap-northeast-2 • ap-southeast-1 • ap-southeast-2 • sa-east-1 • us-gov-west-1

HTTPS	Enabled (有効)	HTTPS を使用して AWS にアクセスします。
Verify SSL Certificate (SSL 証明書を検証する)	Enabled (有効)	SSL デジタル証明書の有効性を確認します。

Microsoft Azure

Microsoft Azure には複数の認証方法があります。

認証方法: 鍵

オプション	説明	必須
Tenant ID (テナント ID)	お使いの Azure 環境のテナント ID またはディレクトリ ID。	○
Application ID (アプリケーション ID)	登録したアプリケーションのアプリケーション ID (別称 クライアント ID)。	○
Client Secret (クライアントシークレット)	登録済みアプリケーションの秘密鍵。	○
Subscription IDs (サブスクリプション ID)	コンマで区切られた、スキャン対象のサブスクリプション ID のリスト。このフィールドが空白の場合、すべてのサブスクリプションが監査されます。	×

認証方法: パスワード

オプション	説明	必須
Username (ユーザー名)	Microsoft Azure へのログインに必要なユーザー名。	○

Password (パスワード)	ユーザー名に関連付けられたパスワード。	○
Client ID (クライアント ID)	登録したアプリケーションのアプリケーション ID (別称クライアント ID)。	○
Subscription IDs (サブスクリプション ID)	コンマで区切られた、スキャン対象のサブスクリプション ID のリスト。このフィールドが空白の場合、すべてのサブスクリプションが監査されます。	×

認証方法: 証明書

オプション	説明	必須
Tenant ID (テナント ID)	お使いの Azure 環境のテナント ID またはディレクトリ ID。	○
Application ID (アプリケーション ID)	登録したアプリケーションのアプリケーション ID (別称クライアント ID)。	○
Private Key (プライベートキー)	PEM 形式の 2048 ビット RSA プライベートキーおよび証明書。	○
Config File (設定ファイル)	追加の設定パラメーター。現在、これは SCuBA スキャンにのみ適用されます。	×
Subscription IDs (サブスクリプション ID)	コンマで区切られた、スキャン対象のサブスクリプション ID のリスト。このフィールドが空白の場合、すべてのサブスクリプションが監査されます。	×

Rackspace

オプション	説明
Username (ユーザー名)	ログインに必要なユーザー名です。
Password or API Keys (パスワードま	ユーザー名に関連付けられたパスワードまたは API キーです。

たは API キー)	
Authentication Method (認証方法)	ドロップダウンボックスからパスワードまたは API キーを指定します。
Global Settings (グローバル設定)	Rackspace クラウドインスタンスの場所です。

Salesforce.com

ユーザーは、[Credentials] (認証情報) メニューから Salesforce.com を選択できます。これにより、Tenable Nessus は指定されたユーザーとして Salesforce.com にログインし、コンプライアンス監査を実行できます。

オプション	説明
Username (ユーザー名)	Salesforce.com のログインに必要なユーザー名
Password (パスワード)	Salesforce.com のユーザー名に関連付けられたパスワード

データベース認証情報

次のトピックでは、利用可能な**データベース**認証情報について説明します。

Cassandra

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 • **Password (パスワード)** • **CyberArk** • **Lieberman** • **Hashicorp Vault** 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイ

オプション	説明
	プを参照してください。
Ports (ポート)	データベースがリッスンするポート。デフォルトはポート 9042 です。

Delinea Secret Server 自動検出

オプション	説明	必須
Delinea Host (Delinea ホスト)	Delinea Secret Server ホスト。ここからシークレットをプルします。	○
Delinea ポート	API リクエスト用の Delinea Secret Server ポート。Tenable はデフォルトで 443 を使用します。	○
Delinea Authentication Method (Delinea 認証方式)	認証に、認証情報と API キーのどちらを使用するかを示します。デフォルトでは、**[認証情報]** が選択されています。	○
Delinea Login Name (Delinea ログイン名)	Delinea サーバーに認証されるときに使用するユーザー名。	○
Delinea Password (Delinea パスワード)	Delinea サーバーに認証されるときに使用するパスワード。これは、指定した Delinea ログイン名に関連付けられているものです。	○
Delinea API Key (Delinea API キー)	Secret Server ユーザーインターフェースで生成された API キー。この設定は、API キーの認証方式を選択した場合に必須です。	○
Query Mode (クエリモード)	事前設定されたフィールドを使用するか、URL クエリパラメーターの文字列を構築してアカウントにクエリを実行するかを選択します。デフォルトでは、**[シンプル]** が選択されています。	○
Folder ID (フォル	指定されたフォルダー ID でアカウントにクエリを実行します。このオ	×

オプション	説明	必須
ダー ID)	プションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	
Search Text (検索テキスト)	指定された検索テキストに一致するアカウントにクエリを実行します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Search Field (検索フィールド)	指定された検索テキストを使用して検索するフィールド。指定しない場合、クエリは name フィールドを検索します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Exact Match (完全一致)	検索テキストと完全一致を実行します。デフォルトでは、これは選択されていません。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Query String (クエリ文字列)	URL クエリパラメーターの文字列を指定します。このオプションは、クエリモードが **[高度]** に設定されている場合にのみ使用でき、この場合は必須です。	○
Use Private Key (秘密鍵を使用する)	パスワード認証ではなく鍵ベースの認証を使用して SSH 接続を行います。	×
Use SSL (SSL を使用する)	安全な通信のために SSL を使用します。	○
Verify SSL Certificate (SSL 証明書を検証する)	Delinea Secret Server SSL 証明書を検証します。	×

DB2

次の表は、**IBM DB2** 認証情報に設定する追加オプションを示しています。

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 • Password (パスワード) • インポート • CyberArk • Lieberman • Hashicorp Vault 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイプを参照してください。
Database Port (データベースのポート)	Tenable Nessus Manager からの通信に対して IBM DB2 データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 50000 です。
Database Name (データベース名)	データベースの名前 (インスタンスの名前ではありません)。

Options	Description
Username	The username for a user on the database.
	The password associated with the username you provided.
Port	The TCP port that the Informix/DRDA database instance listens on for communications from Tenable Security Center.The default is port 1526.

MongoDB

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 **注意:** このオプションは、MongoDB 認証方式の非レガシーバージョンでのみ使用できます。

オプション	説明
	• **Password (パスワード)** • **Client certificate (クライアント証明書)** • **CyberArk** • **Lieberman** • **Hashicorp Vault** 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイプを参照してください。
Username (ユーザー名)	(必須) データベースのユーザー名。
Password (パスワード)	(必須) 入力したユーザー名のパスワード。
Database (データベース)	認証先データベースの名前。 **ヒント:** LDAP または saslauthd を使用して認証するには **$external** と入力します。
Ports (ポート)	(必須) Tenable Nessus からの通信に対して MongoDB データベースインスタンスがリッスンする TCP ポート。

MySQL

次の表は、**MySQL** 認証情報に設定する追加オプションを示しています。

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 • **Password (パスワード)** • **インポート** • **CyberArk** • **Lieberman**

オプション	説明
	• Hashicorp Vault 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイプを参照してください。
Username (ユーザー名)	データベースのユーザーのユーザー名。
Password (パスワード)	入力したユーザー名に関連付けられたパスワード。
Database Port (データベースのポート)	Tenable Nessus からの通信に対して MySQL データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 3306 です。

Oracle

次の表は、**Oracle** 認証情報に設定する追加オプションを示しています。

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 • **Password (パスワード)** • **インポート** • **CyberArk** • **Lieberman** • **Hashicorp Vault** 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイプを参照してください。
Database Port (データベースのポート)	Tenable Nessus からの通信に対して Oracle データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 1521 です。
認証の種類	データベースインスタンスにアクセスするために Tenable Nessus が使用するアカウントの種類 • **Normal (標準)**

オプション	説明
	• System Operator • System Database Administrator • SYSDBA • SYSOPER • NORMAL
Service Type (サービスの種類)	データベースインスタンスを指定するために使用する Oracle パラメーター: **SID** または **Service NameSERVICE_NAME**。
Service (サービス)	データベースインスタンスの SID 値または SERVICE_NAME 値。 入力する **[サービス]** 値は、**[サービスタイプ]** オプションのパラメーターとして選択した値と一致する必要があります。

PostgreSQL

次の表は、**PostgreSQL** 認証情報に設定する追加オプションを示しています。

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 • **Password (パスワード)** • **Client certificate (クライアント証明書)** • **CyberArk** • **Lieberman** • **Hashicorp Vault** 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイプを参照してください。
Database Port (データベースのポート)	Tenable Nessus からの通信に対して PostgreSQL データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 5432 です。

オプション	説明
Database Name (データベース名)	データベースインスタンスの名前。

SQL Server

次の表は、**SQL Server** 認証情報に設定する追加オプションを示しています。

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 • **Password (パスワード)** • **インポート** • **CyberArk** • **Lieberman** • **Hashicorp Vault** 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイプを参照してください。
Username (ユーザー名)	データベースのユーザーのユーザー名。
Password (パスワード)	入力したユーザー名に関連付けられたパスワード。
Database Port (データベースのポート)	Tenable Nessus からの通信に対して SQL Server データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 1433 です。
AuthType (認証の種類)	データベースインスタンスにアクセスするために Tenable Nessus が使用するアカウントの種類 (**SQL** または **Windows**)。
Instance Name (インスタンス名)	データベースインスタンスの名前。

Sybase ASE

次の表は、**Sybase ASE** 認証情報に設定する追加オプションを示しています。

オプション	説明
認証の種類	必要な認証情報を提供するための認証方法。 • **Password (パスワード)** • **CyberArk** • **Lieberman** • **Hashicorp Vault** 選択した認証タイプのオプションの説明については、データベース認証情報の認証タイプを参照してください。
Database Port (データベースのポート)	Tenable Nessus からの通信に対して Sybase ASE データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 3638 です。
Auth Type (認証の種類)	Sybase ASE データベースによって使用される認証のタイプ (**RSA** または**プレーンテキスト**)。

データベース認証情報の認証タイプ

データベース認証情報で選択した認証タイプに応じて、このトピックで説明されるオプションを設定する必要があります。

Client Certificate (クライアント証明書)

[クライアント証明書] の認証タイプは **PostgreSQL** データベースのみでサポートしています。

オプション	説明	必須
Username (ユーザー名)	データベースのユーザー名。	○
Client Certificate (クライアント証明書)	データベースの PEM 証明書を含むファイル。	○
Client CA Certificate (クライアント CA 証明書)	データベースの PEM 証明書を含むファイル。	○

オプション	説明	必須
Client Certificate Private Key (クライアント証明書のプライベートキー)	クライアント証明書の PEM プライベートキーを含むファイル。	○
Client Certificate Private Key Passphrase (クライアント証明書のプライベートキーのパスフレーズ)	認証実施時に必要となった場合の秘密鍵のパスフレーズ。	×
Database Port (データベースのポート)	Tenable Nessus とデータベースの通信に使用されるポート。	○
Database Name (データベース名)	データベースの名前。	×

Password (パスワード)

オプション	データベースの種類	説明	必須
Username (ユーザー名)	すべて	データベースのユーザーのユーザー名。	○
Password (パスワード)	すべて	入力したユーザー名のパスワード。	×
Database Port (データベースのポート)	すべて	Tenable Nessus とデータベースの通信に使用されるポート。	○
Database Name (データベース名)	DB2 PostgreSQL	データベースの名前。	×
Auth type (認証の種類)	Oracle SQL Server Sybase ASE	SQL Server の値は以下のとおりです。 • Windows • SQL Oracle の値は以下のとおりです。 • SYSDBA	○

オプション	データベースの種類	説明	必須
		• SYSOPER • NORMAL Sybase ASEの値は以下のとおりです。 • RSA • プレーンテキスト	
Instance Name (インスタンス名)	SQL Server	データベースインスタンスの名前。	×
Service type (サービスの種類)	Oracle	有効な値は以下のとおりです。 • SID • SERVICE_NAME	○
Service (サービス)	Oracle	データベースインスタンスの SID 値または SERVICE_NAME 値です。入力する **[サービス]** 値は、**[サービスタイプ]** オプションのパラメーターとして選択した値と一致する必要があります。	×

インポート

特定のフォーマットに認証情報が入力された .csv ファイルをアップロードします。各アイテムについて使用する有効な値の説明は、そのデータベースの認証情報を参照してください。

Tenable Nessus で認証情報を取得できるようにするためには、CyberArk か HashiCorp のいずれかの認証情報を、同じスキャン内のデータベース認証情報として設定する必要があります。

データベース認証情報	CSV 形式
DB2	`target, port, database_name, username, cred_manager, accountname_or_secretname`

データベース認証情報	CSV 形式
MySQL	`target, port, database_name, username, cred_manager, accountname_or_secretname`
Oracle	`target, port, service_type, service_ID, username, auth_type, cred_manager, accountname_or_secretname`
SQL Server	`target, port, instance_name, username, auth_type, cred_manager, accountname_or_secretname`

注意: 必要なデータを指定された順に入力します。各値はコンマで区切りスペースは入れません。たとえば、CyberArk 付きの Oracle の場合は、`192.0.2.255,1521,SID,service_id,username,SYSDBA,CyberArk,Database-Oracle-SYS` となります。

注意: `cred_manager` の値は、*CyberArk* または *HashiCorp* のどちらかである必要があります。

BeyondTrust

オプション	説明	必須
Username (ユーザー名)	スキャンするホストにログインするためのユーザー名。	○
Domain (ドメイン)	ユーザー名のドメイン。ドメインにリンクされたアカウント (管理対象システムにリンクされたドメインの管理されたアカウント) を使用する場合に推奨されます。	×
BeyondTrust host (BeyondTrust ホスト)	BeyondTrust IP アドレスまたは DNS アドレス。	○
BeyondTrust port (BeyondTrust ポート)	BeyondTrust がリッスンするポート。	○
BeyondTrust API user (BeyondTrust API ユーザー)	BeyondTrust が提供する API ユーザー。	○
BeyondTrust API key	BeyondTrust が提供する API キー。	○

(BeyondTrust API キー)		
Checkout duration (チェックアウト期間)	BeyondTrust で認証情報のチェックアウト状態を保持する時間 (分)。チェックアウト期間は、通常のスキャン期間より長く設定してください。新しいスキャンが開始したときに過去のスキャンのパスワードがまだチェックアウトされている場合、新しいスキャンは失敗します。 **注意:** パスワード変更によってスキャンが中断されないように、BeyondTrust のパスワードの変更間隔を設定してください。スキャン中に BeyondTrust がパスワードを変更すると、スキャンは失敗します。	○
Use SSL (SSL を使用する)	有効にすると、統合では安全な通信のために IIS を介して SSL が使用されます。このオプションを有効にするには、まず BeyondTrust で IIS を介する SSL を設定します。 **警告:** このオプションを有効にしないと、送信されるトラフィックは http となり、Beyond Trust サーバーによって受け入れられません。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、統合では SSL 証明書が検証されます。このオプションを有効にするには、まず BeyondTrust で IIS を介する SSL を設定します。	×

CyberArk

CyberArk は、権限付き認証情報の管理に使用できる一般的なエンタープライズパスワードボールトです。Tenable Nessus は、CyberArk から認証情報を取得してスキャンに使用します。

オプション	説明	必須
CyberArk Host (CyberArk ホスト)	CyberArk AIM Web サービスの IP アドレスまたは FQDN 名。これは、ホスト、または 1 つの文字列にカスタム URL が追加されたホストにすることができます。	○
Ports (ポート)	CyberArk API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○

オプション	説明	必須
AppID	CyberArk API 接続に関連するアプリケーション ID。	○
Client certificate (クライアント証明書)	CyberArk ホストとの通信に使用される PEM 証明書を含むファイル **注意:** Windows Server 2022 以降で CyberArk CCP をセルフホスティングしているお客様は、CyberArk クライアント証明書の認証の問題に関する Tenable のコミュニティの投稿に記載されているガイダンスに従ってください。	×
Client Certificate Private Key (クライアント証明書のプライベートキー)	クライアント証明書の PEM プライベートキーを含むファイル。	○ (秘密鍵が適用されている場合)
Client Certificate Private Key Passphrase (クライアント証明書のプライベートキーのパスフレーズ)	プライベートキーのパスフレーズ (必要な場合)。	○ (秘密鍵が適用されている場合)
Get credential by (認証情報の取得方法)	CyberArk API 認証情報を取得する方法。**[アドレス]**、**[識別子]**、**[パラメーター]**、または **[ユーザー名]** のいずれかです。 **注意: [パラメーター]** オプションの詳細については、**パラメーターオプション**の表を参照してください。 **注意: ユーザー名** のクエリ頻度は、ターゲットごとにクエリ 1 回です。**識別子** のクエリの頻度は、チャンクごとにクエリ 1 回です。この機能では、すべてのターゲットに同じ識別子が必要です。	○
Username (ユーザー名)	([**Get credential by**] が**ユーザー名** に設定されている場	×

オプション	説明	必須
	合) パスワードを要求する CyberArk ユーザーのユーザー名。	
Safe (セーフ)	認証情報を取得するべき CyberArk のセーフ。	×
Account Name (アカウント名)	(**[認証情報の取得]** が **[識別子]** の場合) CyberArk API の認証情報が割り当てられる固有のアカウント名または識別子。	×
Use SSL (SSL を使用する)	有効にすると、スキャナーは安全な通信のために IIS を介して SSL を使用します。CyberArk が IIS を介した SSL をサポートするよう設定されている場合、このオプションを有効にします。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、スキャナーは SSL 証明書を検証します。CyberArk が安全な通信のために IIS によって SSL をサポートするように設定されており、証明書を検証する場合、このオプションを有効にします。	×

CyberArk (レガシー)

CyberArk は、権限付き認証情報の管理に使用できる一般的なエンタープライズパスワードボールトです。Tenable Nessus は、CyberArk から認証情報を取得してスキャンに使用します。

オプション	データベースの種類	説明	必須
Username (ユーザー名)	すべて	ターゲットシステムのユーザー名。	○
Central Credential Provider Host (Central Credential Provider ホスト)	すべて	CyberArk Central Credential Provider の IP/DNS アドレス。	○
Central Credential Provider Port (Central Credential	すべて	CyberArk Central Credential Provider がリッスンするポート。	○

オプション	データベースの種類	説明	必須
Provider ポート)			
CyberArk AIM Service URL (CyberArk AIM サービス URL)	すべて	AIM サービスの URL。デフォルトでは、このフィールドは `/AIMWebservice/v1.1/AIM.asmx` を使用します。	×
Central Credential Provider Username (Central Credential Provider ユーザー名)	すべて	CyberArk Central Credential Provider が基本認証を使用するように設定されている場合は、このフィールドに入力して認証できます。	×
Central Credential Provider Password (Central Credential Provider パスワード)	すべて	CyberArk Central Credential Provider が基本認証を使用するように設定されている場合は、このフィールドに入力して認証できます。	×
CyberArk Safe	すべて	取得する認証情報が格納されていた CyberArk Central Credential Provider サーバー上の金庫。	×
CyberArk Client Certificate (CyberArk クライアント証明書)	すべて	CyberArk ホストとの通信に使用される PEM 証明書を含むファイル。	×
CyberArk Client Certificate Private Key (CyberArk クライアント証明書のプライベートキー)	すべて	クライアント証明書の PEM プライベートキーを含むファイル。	×
CyberArk Client Certificate Private Key Passphrase	すべて	認証実施時に必要となった場合の秘密鍵のパスフレーズです。	×

オプション	データベースの種類	説明	必須
(CyberArk クライアント証明書のプライベートキーパスフレーズ)			
CyberArk AppId	すべて	CyberArk Central Credential Provider でターゲットパスワードを取得するためのアクセス許可を割り当てられた AppId。	○
CyberArk Folder (CyberArk フォルダー)	すべて	取得する認証情報が格納されている CyberArk Central Credential Provider サーバー上のフォルダー。	×
CyberArk Account Details Name (CyberArk アカウント詳細名)	すべて	CyberArk から取得する認証情報の一意の名前。	○
PolicyId (ポリシー ID)	すべて	CyberArk Central Credential Provider から取得する認証情報に割り当てられたポリシー ID。	×
Use SSL (SSL を使用する)	すべて	CyberArk Central Credential Provider が安全な通信のために IIS チェックによって SSL をサポートするように設定されている場合。	×
Verify SSL Certificate (SSL 証明書の検証)	すべて	CyberArk Central Credential Provider が安全な通信のために IIS チェックによって SSL をサポートするように設定されており、証明書を検証する場合、このオプションを選択します。自己署名証明書の使用方法については、custom_CA.inc のマニュアルを参照してください。	×
Database Port (デー	すべて	Tenable Nessus とデータベースの通信に使	○

オプション	データベースの種類	説明	必須
タベースのポート)		用されるポート	
Database Name (データベース名)	DB2 PostgreSQL	データベースの名前。	×
Auth type (認証の種類)	Oracle SQL Server Sybase ASE	SQL Server の値は以下のとおりです。 • Windows • SQL Oracle の値は以下のとおりです。 • **Normal (標準)** • **System Operator** • **System Database Administrator** • **SYSDBA** • **SYSOPER** • **NORMAL** Sybase ASEの値は以下のとおりです。 • RSA • プレーンテキスト	○
Instance Name (インスタンス名)	SQL Server	データベースインスタンスの名前。	×
Service type (サービスの種類)	Oracle	有効な値は以下のとおりです。 • SID • SERVICE_NAME	○
Service (サービス)	Oracle	データベースインスタンスの SID 値または SERVICE_NAME 値です。入力する **[サー**	×

オプション	データベースの種類	説明	必須
		ビス] 値は、[サービスタイプ] オプションのパラメーターとして選択した値と一致する必要があります。	

Delinea

オプション	説明	必須
Delinea Secret Name (Delinea シークレット名)	Delinea サーバーのシークレットの値。シークレットは、Delinea サーバーで Secret Name のラベルが付けられています。	○
Delinea Host (Delinea ホスト)	Delinea シークレット サーバー IP アドレスまたは DNS アドレス。	○
Delinea Port (Delinea ポート)	Delinea シークレット サーバーがリッスンするポート。	○
Delinea 認証方式	認証に、認証情報と API キーのどちらを使用するかを示します。デフォルトでは、認証情報が選択されています。	○
Delinea ログイン名	Delinea サーバーへの認証に使用されるユーザー名。	○
Delinea Password (Delinea パスワード)	Delinea サーバーへの認証に使用されるパスワード。これは、指定した Delinea Login Name に関連付けられているものです。	○
Delinea API key (Delinea API キー)	Delinea シークレット サーバーが提供する API キー。	○
Use SSL (SSL を使用する)	Delinea シークレット サーバーが SSL をサポートするように設定されている場合は有効にします。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Delinea サーバーの SSL 証明書を検証します。	×

Delinea 自動検出

オプション	説明	必須
Delinea Host (Delinea ホスト)	Delinea Secret Server ホスト。ここからシークレットをプルします。	○
Delinea ポート	API リクエスト用の Delinea Secret Server ポート。Tenable はデフォルトで 443 を使用します。	○
Delinea Authentication Method (Delinea 認証方式)	認証に、認証情報と API キーのどちらを使用するかを示します。デフォルトでは、**[認証情報]** が選択されています。	○
Delinea Login Name (Delinea ログイン名)	Delinea サーバーに認証されるときに使用するユーザー名。	○
Delinea Password (Delinea パスワード)	Delinea サーバーに認証されるときに使用するパスワード。これは、指定した Delinea ログイン名に関連付けられているものです。	○
Delinea API Key (Delinea API キー)	Secret Server ユーザーインターフェースで生成された API キー。この設定は、API キーの認証方式を選択した場合に必須です。	○
Query Mode (クエリモード)	事前設定されたフィールドを使用するか、URL クエリパラメーターの文字列を構築してアカウントにクエリを実行するかを選択します。デフォルトでは、**[シンプル]** が選択されています。	○
Folder ID (フォルダー ID)	指定されたフォルダー ID でアカウントにクエリを実行します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Search Text (検索テキスト)	指定された検索テキストに一致するアカウントにクエリを実行します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Search Field (検索フィールド)	指定された検索テキストを使用して検索するフィールド。指定しない場合、クエリは `name` フィールドを検索します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できま	×

オプション	説明	必須
	す。	
Exact Match (完全一致)	検索テキストと完全一致を実行します。デフォルトでは、これは選択されていません。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Query String (クエリ文字列)	URL クエリパラメーターの文字列を指定します。このオプションは、クエリモードが **[高度]** に設定されている場合にのみ使用でき、この場合は必須です。	○
Use Private Key (秘密鍵を使用する)	パスワード認証ではなく鍵ベースの認証を使用して SSH 接続を行います。	×
Use SSL (SSL を使用する)	安全な通信のために SSL を使用します。	○
Verify SSL Certificate (SSL 証明書を検証する)	Delinea Secret Server SSL 証明書を検証します。	×

HashiCorp Vault

HashiCorp Vault は、権限付き認証情報の管理に使用できる一般的なエンタープライズパスワードボールトです。Tenable Nessus では、HashiCorp Vault から認証情報を取得してスキャンに使用できます。

オプション	説明	必須
Hashicorp Vault host (Hashicorp Vault ホスト)	Hashicorp Vault IP アドレスまたは DNS アドレス。 **注意:** Hashicorp Vault インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパス*の形式で入力します。	○
Hashicorp Vault port (Hashicorp Vault ポー	Hashicorp Vault がリッスンするポート。	○

ト)		
Authentication Type (認証タイプ)	インスタンスに接続するための認証タイプとして、**[App Role]** (アプリロール) または **[Certificates]** (証明書) を指定します。 **[証明書]** を選択した場合、**[Hashicorp クライアント証明書]** および **[Hashicorp クライアント証明書の秘密鍵]** の追加オプションが表示されます。クライアント証明書と秘密鍵にそれぞれ適切なファイルを選択してください。	○
Role ID (ロール ID)	App Role を構成したときに Hashicorp Vault によって提供される GUID です。	○
Role Secret ID (ロールシークレット名)	App Role を構成したときに Hashicorp Vault によって生成される GUID です。	○
Authentication URL (認証 URL)	認証エンドポイントへのパス/サブディレクトリ。This is not the full URL. (これは完全な URL ではありません。)例: `/v1/auth/approle/login`	○
Namespace (名前空間)	マルチチーム環境で指定されたチームの名前	×
Vault Type (Vault タイプ)	Tenable Nessus バージョン: KV1、KV2、AD、LDAP。Tenable Nessus バージョンの詳細については、Tenable Nessus のドキュメントを参照してください。	○
KV1 Engine URL (KV1 エンジン URL)	(KV1) Tenable Nessus が KV1 エンジンへのアクセスに使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (KV1 **Vault タイプ**を選択した場合)
KV2 Engine URL (KV2 エンジン URL)	(KV2) Tenable Nessus が KV2 エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (KV2 **Vault タイプ**を選択した場合)

AD Engine URL (AD エンジン URL)	(AD) Tenable Nessus が Active Directory エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (AD **Vault タイプ**を選択した場合)
LDAP Engine URL (LDAP エンジン URL)	(LDAP) Tenable Nessus が LDAP エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (LDAP **Vault タイプ**を選択した場合)
Username Source (ユーザー名 ソース)	(KV1 および KV2) ユーザー名が手動で入力されるか、Hashicorp Vault からプルするかを指定するドロップダウンボックスです。	○
Username Key (ユーザー名 鍵)	(KV1 および KV2) ユーザー名が格納されている Hashicorp Vault での名前です。	○
Password Key (パスワード鍵)	(KV1 および KV2) パスワードが格納されている Hashicorp Vault での鍵です。	○
Secret Name (秘密名)	(KV1、KV2、AD) 値を取得したい鍵秘密です。	○
Use SSL (SSL を使用する)	有効にすると、Tenable Nessus Manager は安全な通信のために SSL を使用します。このオプションを有効にする前に、Hashicorp Vault で SSL を設定してください。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable Nessus Manager は SSL 証明書を検証します。このオプションを有効にするには、Hashicorp Vault で SSL を設定する必要があります。	×
Database Port (データベースのポート)	Tenable Nessus Manager とデータベースの通信に使用されるポート。	○
Auth Type	データベース認証情報の認証方法です。 Oracleの値は以下のとおりです。 • SYSDBA	○

	• SYSOPER • NORMAL	
Service Type (サービスの種類)	(Oracle データベースのみ) 有効な値は以下のとおりです。SID、SERVICE_NAME。	○
Service (サービス)	(Oracle データベースのみ) データベースの構成用の特別なフィールドです。	○

Lieberman

Lieberman は、権限付き認証情報の管理に使用できる一般的なエンタープライズパスワードボールトです。Tenable Vulnerability Management は、Lieberman から認証情報を取得してスキャンに使用します。

オプション	データベースの種類	説明	必須
Username (ユーザー名)	すべて	ターゲットシステムのユーザー名。	○
Lieberman host (Lieberman ホスト)	すべて	Lieberman の IP/DNS アドレス。 **注意:** Lieberman インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパス*の形式で入力します。	○
Lieberman port (Lieberman ポート)	すべて	Lieberman がリッスンするポート。	○
Lieberman API URL	すべて	Tenable Nessus が Lieberman へのアクセスに使用する URL。	×
Lieberman user (Lieberman ユーザー)	すべて	Lieberman API の認証に使用される Lieberman の明示的ユーザー。	○
Lieberman	すべて	Lieberman 明示ユーザーのパスワード。	○

オプション	データベースの種類	説明	必須
password (Lieberman パスワード)			
Lieberman Authenticator (Lieberman 認証)	すべて	Lieberman のオーセンティケーターに使用されるエイリアス。この名前は Lieberman で使用される名前に一致する必要があります。 **注意:** このオプションを使用する場合は、**[Lieberman ユーザー]** オプションにドメインを追加してください (例: *domain\user*)。	×
Lieberman Client Certificate (Lieberman クライアント証明書)	すべて	Lieberman ホストとの通信に使用される PEM 証明書を含むファイル。 **注意:** このオプションを使用する場合は、**[Lieberman ユーザー]**、**[Lieberman パスワード]**、**[Lieberman 認証]** の各フィールドに情報を入力する必要はありません。	×
Lieberman Client Certificate Private Key (Lieberman クライアント証明書のプライベートキー)	すべて	クライアント証明書の PEM プライベートキーを含むファイル。	×
Lieberman Client Certificate Private Key Passphrase (Lieberman クライアント証明書の秘密鍵パスフレーズ)	すべて	プライベートキーのパスフレーズ (必要な場合)。	×
Use SSL (SSL を使用する)	すべて	Lieberman が安全な通信のために IIS チェックによって SSL をサポートするように設	×

オプション	データベースの種類	説明	必須
		定されている場合。	
Verify SSL Certificate (SSL 証明書の検証)	すべて	Lieberman が安全な通信のために IIS チェックによって SSL をサポートするように設定されており、証明書を検証する場合、このオプションにチェックマークを入れます。自己署名証明書の使用方法については、カスタム CA ドキュメントを参照してください。	×
System Name (システム名)	すべて	まれなケースではあるものの、お客様の企業がすべての管理対象システムにデフォルトの Lieberman エントリを 1 つ使用している場合は、デフォルトのエントリ名を入力します。	×
Database Port (データベースのポート)	すべて	Tenable Nessus とデータベースの通信に使用されるポート	○
Database Name (データベース名)	DB2 PostgreSQL	(PostgreSQL と DB2 データベースのみ) データベース名です。	×
Auth type (認証の種類)	Oracle SQL Server Sybase ASE	(SQL Server、Oracle、Sybase ASE データベースのみ) SQL Server の値は以下のとおりです。 • Windows • SQL Oracle の値は以下のとおりです。 • SYSDBA • SYSOPER • NORMAL Sybase ASEの値は以下のとおりです。	○

オプション	データベースの種類	説明	必須
		• RSA • プレーンテキスト	
Instance Name (インスタンス名)	SQL Server	データベースインスタンスの名前。	×
Service type (サービスの種類)	Oracle	有効な値は以下のとおりです。 • SID • SERVICE_NAME	×
Service (サービス)	Oracle	データベースインスタンスの SID 値または SERVICE_NAME 値です。入力する **[サービス]** 値は、**[サービスタイプ]** オプションのパラメーターとして選択した値と一致する必要があります。	○

QiAnXin

QiAnXin は、権限付き認証情報を管理するのに便利な、一般的なエンタープライズパスワードボールトです。Tenable Vulnerability Management は、QiAnXin から認証情報を取得してスキャンに使用することができます。

オプション	説明	必須
QiAnXin Host (QiAnXin ホスト)	QiAnXin ホストの IP アドレスまたは URL。	○
QiAnXin Port (QiAnXin ポート)	QiAnXin API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○
QiAnXin API Client ID (QiAnXin API クライアント ID)	QiAnXin PAM で作成された埋め込みアカウントアプリケーションのクライアント ID。	○
QiAnXin API Secret ID	QiAnXin PAM で作成された埋め込みアカウントアプリ	○

オプション	説明	必須
(QiAnXin API 秘密 ID)	ケーションの秘密 ID。	
Username (ユーザー名)	スキャンするホストにログインするためのユーザー名	○
Host IP (ホスト IP)	使用するアカウントを含む資産のホスト IP を指定します。指定しない場合、スキャンターゲット IP が使用されます。	×
Platform (プラットフォーム)	使用するアカウントを含む資産のプラットフォーム (資産タイプに基づく) を指定します。指定しない場合、認証情報のタイプに基づいてデフォルトのターゲットが使用されます (たとえば、Windows 認証情報の場合、デフォルトは WINDOWS です)。可能な値は次のとおりです。 • **ACTIVE_DIRECTORY** - Windows ドメインアカウント • **WINDOWS** - Windows ローカルアカウント • **LINUX** - Linux アカウント • **SQL_SERVER** - SQL Server データベース • **ORACLE** - Oracle データベース • **MYSQL** - MySQL データベース • **DB2** - DB2 データベース • **HP_UNIX** - HP Unix • **SOLARIS** - Solaris • **OPENLDAP** - OpenLDAP • **POSTGRESQL** - PostgreSQL	×
Region ID (リージョン ID)	使用するアカウントを含む資産のリージョン ID を指定します。	複数のリージョンを使用し

オプション	説明	必須
		ている場合のみ必須
Use SSL (SSL を使用する)	有効にすると、Tenable は安全な通信のために SSL を使用します。このオプションはデフォルトで有効です。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable は、サーバーの SSL 証明書が信頼できる認証局によって署名されたものかどうかを検証します。	×

Senhasegura

オプション	説明	必須
Senhasegura Host (Senhasegura ホスト)	Senhasegura ホストの IP アドレスまたは URL です。	○
Senhasegura Port (Senhasegura ポート)	Senhasegura API が通信に使用するポートです。Tenable はデフォルトで 443 を使用します。	○
Senhasegura API Client ID (Senhasegura API クライアント ID)	Oauth 2.0 API 認証に適用される Senhasegura A2A アプリケーションのクライアント ID です。	○
Senhasegura API Secret ID (Senhasegura API のシークレット ID)	Oauth 2.0 API 認証に適用される Senhasegura A2A アプリケーションのシークレット ID です。	○
Senhasegura Credential ID or Identifier (Senhasegura 認証情報 ID または識別子)	取得をリクエストしている認証情報の認証情報 ID または識別子です。	○

オプション	説明	必須
Private Key File (秘密鍵ファイル)	A2A からの暗号化された機密データを復号するために使用される秘密鍵です。 **注意:** A2A アプリケーション認証で機密データの暗号化を有効にできます。有効にした場合、スキャン認証情報に秘密鍵ファイルを指定する必要があります。これは、Senhasegura の該当する A2A アプリケーションからダウンロードできます。	A2A アプリケーション認証で機密データの暗号化を有効にした場合には必須です。
HTTPS	このオプションはデフォルトで有効です。	○
Verify SSL Certificate (SSL 証明書を検証する)	これはデフォルトでは無効になっています。	×

ホスト認証情報

Tenable Nessus では、次の形式のホスト認証がサポートされます。

SNMPv3

ユーザーは、**[Credentials]** (認証情報) メニューで SNMPv3 設定を選択し、暗号化ネットワーク管理プロトコルを使用してスキャンシステムの認証情報を入力します。

これらの認証情報を使用して、ネットワークデバイスなどのリモートシステムから、パッチ監査やコンプライアンスチェック用のローカル情報を取得します。

ターゲットシステムでチェックを実行するアカウントの SNMPv3 ユーザー名、SNMPv3 ポート、セキュリティレベル、認証アルゴリズムとパスワード、プライバシーアルゴリズムとパスワードを入力するためのフィールドがあります。

Nessus がコミュニティストリングまたはパスワードを判別できない場合、そのサービスの監査を正常に実行できない場合があります。

注意: [Basic Network Scan] (基本ネットワークスキャン) テンプレートでは SNMPv3 設定を変更できません。

オプション	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、SNMPv3 のアカウントのユーザー名	-
Port (ポート)	Tenable Nessus からの通信に対して SNMPv3 がリッスンする TCP ポート	161
Security level (セキュリティレベル)	SNMP のセキュリティレベル: • **認証もプライバシーもなし** • **プライバシーのない認証** • **認証とプライバシー**	認証とプライバシー
Authentication algorithm (認証アルゴリズム)	削除サービスがサポートするアルゴリズム: **SHA1**、**SHA224**、**SHA-256**、**SHA-384**、**SHA-512**、**MD5**。	SHA1
Authentication password (パスワード認証)	(必須) **ユーザー名** に関連付けられたパスワード	-
Privacy algorithm (プライバシーアルゴリズム)	SNMP トラフィックに使用する暗号アルゴリズム: **AES**、**AES-192**、**AES-192C**、**AES-256**、**AES-256C**、または **DES**。	AES-192
Privacy password (プライバシーパスワード)	(必須) 暗号化された SNMP 通信を保護するために使用されるパスワード	-

SSH

Unix システムとサポートされているネットワークデバイスで、ホストベースのチェックに SSH 認証情報を使用します。Tenable Nessus はこれらの認証情報を使用して、パッチ監査やコンプライアンスチェックのために、リモート Unix システムからローカル情報を取得します。Tenable Nessus は、セキュアシェル (SSH) プロトコルバージョン2ベースのプログラム (OpenSSH、Solaris SSH など) をホストベースのチェックに使用します。

Tenable Nessus は、スニファープログラムによる表示から保護するためにデータを暗号化します。

ヒント: サポートされている鍵交換 (KEX) アルゴリズムの詳細については、Linux での認証情報チェックを参照してください。

注意: Linuxシステムにローカルでアクセス可能な特権ユーザー以外のユーザーは、パッチレベルや /etc/passwd ファイルへの入力といった基本的なセキュリティ問題を判断できます。システム設定データやシステム全体のファイルのアクセス許可など、より包括的な情報を得るには、ルート権限を持つアカウントが必要です。

注意: 1 つのスキャンに最大 1,000 個の SSH 認証情報を追加できます。最高のパフォーマンスを得るために、Tenable は追加する SSH 認証情報をスキャンあたりで 10 個以下にすることを推奨しています。

さまざまな SSH 認証方法については、次の設定を参照してください。

グローバル認証情報設定

すべての SSH 認証方法で使用できるSSH認証情報には、4 つの設定があります。

オプション	デフォルト値	説明
known_hosts file (known_hosts ファイル)	なし	SSH の known_hosts ファイルが使用可能で、スキャンポリシーの **Global Credential Settings** の一部として **known_hosts file** フィールドに指定されている場合、Tenable Nessus はこのファイル内のホストにログインを試行します。これにより、既知の SSH サーバーの監査に使用しているものと同じユーザー名とパスワードが、制御できないシステムへのログイン試行に使用されないようにします。
Preferred port (希望のポート)	22	Tenable Nessus が 22 以外のポートで動作している場合、このオプションを設定して Tenable Nessus を SSH に接続するように設定できます。
Client version (Client version (クライアントバージョン))	OpenSSH_5.0	スキャン中に Tenable Nessus が偽装する SSH クライアントの種類を指定します。
Attempt	未選択	動的な権限昇格を有効または無効にします。これを有効に

オプション	デフォルト値	説明
least privilege (Attempt least privilege (最小限の権限を試行))		すると、はオプションでTenable Nessus [Elevate privileges] (権限の昇格) が有効になっている場合でも、より権限の低いアカウントでスキャンを実行しようとします。コマンドが失敗すると、Tenable Nessus は権限を昇格させます。プラグイン 102095 および 102094 では、権限の昇格の有無にかかわらず、実行されたプラグインが報告されます。 **注意:** このオプションを有効にすると、スキャンの実行時間が最長で 30% 長くなる可能性があります。

証明書

オプション	説明
Username (ユーザー名)	ホストシステムで認証に使用されているアカウントのユーザー名です。
User Certificate (ユーザー証明書)	RSA または DSA のユーザー証明書ファイルです。
Private Key (プライベートキー)	ユーザーの RSA、DSA、ECDSA、または ED25519 OpenSSH 秘密鍵。
Private key passphrase (秘密鍵のパスフレーズ)	秘密鍵のパスフレーズです。
Elevate privileges with (権限昇格方法)	認証が完了した後に権限を昇格します。
Targets to	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを

オプション	説明
Prioritize Credentials (認証情報を優先するターゲット)	指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

CyberArk (Tenable Nessus Managerのみ)

ヒント: Cyberark の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

CyberArk は、権限付き認証情報の管理に使用できる一般的なエンタープライズパスワードボールトです。Tenable Nessus Manager は、CyberArk から認証情報を取得してスキャンに使用します。

オプション	説明	必須
CyberArk Host (Delinea ホスト)	CyberArk AIM ウェブサービスの IP アドレスまたは FQDN 名。	○
Ports (ポート)	CyberArk API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○
AppID	CyberArk API 接続に関連付けられているアプリケーション ID。	○
Client certificate (クライアント証明書)	CyberArk ホストとの通信に使用される PEM 証明書を含むファイル。 **注意:** Windows Server 2022 以降で CyberArk CCP をセルフホスティングしているお客様は、CyberArk クライアント証明書の認証の問題に関する Tenable のコミュニティの投稿に記載されているガイダンスに従ってください。	×

オプション	説明	必須
Client Certificate Private Key (クライアント証明書のプライベートキー)	クライアント証明書の PEM プライベートキーを含むファイル。	○ (秘密鍵が適用されている場合)
Client Certificate Private Key Passphrase (クライアント証明書のプライベートキーのパスフレーズ)	プライベートキーのパスフレーズ (必要な場合)。	○ (秘密鍵が適用されている場合)
Kerberos ターゲット認証	有効にすると、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。	×
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストは、ユーザーにセッションチケットを提供します。	○
KDC Port (KDC ポート)	Kerberos 認証 API が通信に使用するポート。デフォルトでは、Tenable は 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。	×
Realm (領域)	(Kerberos ターゲット認証が有効な場合は必須) この領域が、通常ターゲットのドメイン名として表記される、認証ドメインになります	○

オプション	説明	必須
	(例: example.com)。Tenable Nessus はデフォルトで 443 を使用します。	
認証情報の取得方法	CyberArk API 認証情報を取得する方法。**[アドレス]**、**[識別子]**、**[パラメーター]**、または **[ユーザー名]** のいずれかです。 **注意: [パラメーター]** オプションの詳細については、**パラメーターオプション** の表を参照してください。 **注意: ユーザー名** のクエリ頻度は、ターゲットごとにクエリ 1 回です。**識別子** のクエリの頻度は、チャンクごとにクエリ 1 回です。この機能では、すべてのターゲットに同じ識別子が必要です。	○
ユーザー名	(**[認証情報の取得方法]** が **[ユーザー名]** に設定されている場合) パスワードを要求する CyberArk ユーザーのユーザー名。	×
Safe (セーフ)	認証情報の取得元となる CyberArk safe。	×
Address (アドレス)	このオプションは、アドレスの値が単一の CyberArk アカウント認証情報に対して一意である場合にのみ使用します。	×
Account Name (アカウント名)	(**[認証情報の取得方法]** が **[識別子]** の場合) CyberArk API の認証情報に割り当てられている一意のアカウント名または識別子。	×
Use SSL (SSL を使用する)	有効にすると、スキャナーは安全な通信のために IIS を介して SSL を使用します。CyberArk が IIS を通して SSL をサポートするよう設定されている場合、このオプションを有効にします。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、スキャナーは SSL 証明書を検証します。CyberArk が IIS を通して SSL をサポートするように設定されており、証明書を検証する場合、このオプションを有効にします。	×
Targets to Prioritize Credentials (認証情報を優先	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。	×

オプション	説明	必須
するターゲット)	この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	

CyberArk Auto-Discovery (Tenable Nessus Manager のみ)

ヒント: Cyberark の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Tenable と CyberArk との統合による大幅な改善を利用して、複数のターゲットを入力することなく特定のターゲットグループのアカウント情報を一括で収集できるようになりました。

オプション	説明	必須
CyberArk Host (Delinea ホスト)	ユーザーの CyberArk インスタンスの IP アドレスまたは FQDN 名。 **注意:** PVWA と CCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	○
Ports (ポート)	CyberArk API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。 **注意:** PVWA と CCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	○
CCP Host (CCP ホスト)	ユーザーの Cyber Ark CCP コンポーネントの IP アドレスまたは FQDN 名。	×

オプション	説明	必須
	注意: PVWA とCCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	
CCP Port (CCP ポート)	Cyber Ark CCP (AIM ウェブサービス) API が通信するポート。Tenable はデフォルトで 443 を使用します。 **注意:** PVWA とCCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	×
AppID	CyberArk API 接続に関連付けられているアプリケーション ID。	○
Safe (セーフ)	ユーザーは、オプションで Safe ボックスを指定してアカウント情報を収集し、パスワードをリクエストできます。	×
AIM Web Service Authentication Type (AIM ウェブサービス認証のタイプ)	この機能では、2 つの認証方法が確立されています。**IIS 基本認証**と**証明書認証**です。証明書認証は、暗号化することも非暗号化することもできます。	○
CyberArk PVWA ウェブ UI ログイン名	CyberArk ウェブコンソールにログインするためのユーザー名。これは、PVWA REST API に認証したり、アカウント情報を一括収集したりする際に使用されます。	○
CyberArk PVWA ウェブ UI ログインパスワード	CyberArk ウェブコンソールにログインするためのユーザー名のパスワード。これは、PVWA REST API に認証したり、アカウント情報を一括収集したりする際に使用されます。	○
CyberArk プラットフォーム検索文字列	アカウント情報を一括収集するために PVWA REST API クエリパラメーターで使用される文字列。たとえば、`UnixSSH Admin TestSafe` と入力すると、`TestSafe` というセーフにある、ユーザー名 `Admin` を含むすべての UnixSSH プラットフォームのアカウントを収集できます。	○

オプション	説明	必須
	注意: これは完全一致ではないキーワード検索です。精度を向上させるために、CyberArk でカスタムプラットフォーム名を作成し、このフィールドにその値を入力することをお勧めします。	
Elevate Privileges with (権限昇格方法)	現時点では、ユーザーが選択できるのは [なし] か [sudo] だけです。	×
Use SSL (SSL を使用する)	有効にすると、スキャナーは安全な通信のために IIS を介して SSL を使用します。CyberArk が IIS を通して SSL をサポートするよう設定されている場合、このオプションを有効にします。	○
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、スキャナーは SSL 証明書を検証します。CyberArk が IIS を通して SSL をサポートするように設定されており、証明書を検証する場合、このオプションを有効にします。	×
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	×

CyberArk (レガシー) (Tenable Nessus Manager のみ)

ヒント: Cyberark の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

レガシー CyberArk の認証方法は以下の通りです。

オプション	説明
Username (ユーザー名)	ターゲットシステムのユーザー名。
CyberArk AIM Service URL (CyberArk AIM サービス URL)	AIM サービスの URL。デフォルトでは、このフィールドは `/AIMWebservice/v1.1/AIM.asmx` を使用します。
Central Credential Provider Host (Central Credential Provider ホスト)	CyberArk Central Credential Provider の IP/DNS アドレス。
Central Credential Provider Port (Central Credential Provider ポート)	CyberArk Central Credential Provider がリッスンするポート。
Central Credential Provider Username (Central Credential Provider ユーザー名)	CyberArk Central Credential Provider が基本認証を使用するように設定されている場合は、このフィールドに入力して認証できます。
Central Credential Provider Password (Central Credential Provider パスワード)	CyberArk Central Credential Provider が基本認証を使用するように設定されている場合は、このフィールドに入力して認証できます。
Safe (セーフ)	取得する認証情報が格納されていた CyberArk Central Credential Provider サーバー上の金庫。
CyberArk Client Certificate (CyberArk Client 証明書)	CyberArk ホストとの通信に使用される PEM 証明書を含むファイル。
CyberArk Client Certificate Private Key (CyberArk Client Certificate 秘密鍵)	クライアント証明書の PEM 秘密鍵を含むファイル。
CyberArk Client Certificate Private Key Passphrase (CyberArk Client	(オプション) 秘密鍵のパスフレーズ (必要な場合)。

オプション	説明
Certificate 秘密鍵パスフレーズ)	
AppId	CyberArk Central Credential Provider でターゲットパスワードを取得するためのアクセス許可を割り当てられたAppId。
Folder (フォルダー)	取得する認証情報が格納されている CyberArk Central Credential Provider サーバー上のフォルダー。
PolicyId	CyberArk Central Credential Provider から取得する認証情報に割り当てられたポリシー ID です。
Use SSL (SSL を使用する)	IIS で SSL をサポートするように CyberArk Central Credential Provider を設定した場合は、安全な通信のためにこれを選択します。
Verify SSL Certificate (SSL 証明書を検証する)	IIS で SSL をサポートするように CyberArk Central Credential Provider を設定した場合に、証明書を検証するには、これを選択します。自己署名証明書の使用方法については、custom_CA.inc のマニュアルを参照してください。
CyberArk Account Details Name (CyberArk Account Details 名前)	CyberArk から取得する認証情報の一意の名前。
CyberArk Address (CyberArk アドレス)	ユーザーアカウントのドメインです。
CyberArk elevate privileges with (CyberArk 権限昇格方法)	初回認証後にユーザー権限を昇格させるために使用するElevate Privileges with (権限昇格方法)です。この選択によって、設定する必要があるオプションの内容が決まります。

Delinea SSH 認証方法: Delinea

ヒント: Delinea の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグイン を参照してください。

オプション	説明	必須
Delinea 認証方式	認証に、認証情報とAPI キーのどちらを使用するかを示します。デフォルトでは、**[認証情報]** が選択されています。	○
Delinea ログイン名	Delinea サーバーへの認証に使用されるユーザー名。	○
Delinea Password (Delinea パスワード)	Delinea サーバーへの認証に使用されるパスワード。これは、指定した Delinea Login Name に関連付けられているものです。	○
Delinea API キー	Secret Server ユーザーインターフェースで生成された API キー。この設定は、**[API キー]** の認証方法を選択した場合に必須です。	○
Delinea シークレット名	Delinea サーバーのシークレットの値。シークレットには、Delinea サーバーで **シークレット名** のラベルが付けられています。	○
Delinea Host (Delinea ホスト)	この Delinea シークレット サーバー ホストからシークレットをプルします。	○
Delinea Port (Delinea ポート)	API リクエストに使用する Delinea シークレット サーバー ポート。Tenable はデフォルトで 443 を使用します。	○
Use Private Key (秘密鍵を使用する)	有効にすると、パスワード認証ではなく鍵ベースの認証で SSH 接続を行います。	×
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。	×
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストがユーザーにセッションチケットを提供します。	○

KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。Tenable はデフォルトで 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。	×
Realm (領域)	(Kerberos ターゲット認証が有効な場合は必須) この領域は、通常ターゲットのドメイン名として記載されている認証ドメインです。	○
Use SSL (SSL を使用する)	Delinea シークレットサーバーが SSL をサポートするように設定されている場合は有効にします。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Delinea サーバーの SSL 証明書を検証します。	×
Elevate Privileges with (権限昇格方法)	初回認証後にユーザー権限を昇格させる場合に使用する Elevate Privileges with (権限昇格方法)です。su、su+sudo、sudo など、権限昇格の複数のオプションがサポートされています。この選択によって、設定する必要があるオプションの内容が決まります。	×
Custom password prompt (カスタムパスワードプロンプト)	一部のデバイスは、非標準の文字列 (「secret-passcode」など) を使うパスワードのプロンプトを表示します。この設定により、このようなプロンプトを認識できます。ほとんどの標準パスワードプロンプトでは、これを空白のままにしてください。	×
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証	×

	が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	

Delinea Secret Server 自動検出

ヒント: Delinea の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
Delinea Host (Delinea ホスト)	Delinea Secret Server ホスト。ここからシークレットをプルします。	○
Delinea ポート	API リクエスト用の Delinea Secret Server ポート。Tenable はデフォルトで 443 を使用します。	○
Delinea Authentication Method (Delinea 認証方式)	認証に、認証情報と API キーのどちらを使用するかを示します。デフォルトでは、**[認証情報]** が選択されています。	○
Delinea Login Name (Delinea ログイン名)	Delinea サーバーに認証されるときに使用するユーザー名。	○
Delinea Password (Delinea パスワード)	Delinea サーバーに認証されるときに使用するパスワード。これは、指定した Delinea ログイン名に関連付けられているものです。	○
Delinea API Key (Delinea API キー)	Secret Server ユーザーインターフェースで生成された API キー。この設定は、API キーの認証方式を選択した場合に必須です。	○
Query Mode (クエリモード)	事前設定されたフィールドを使用するか、URL クエリパラメーターの文字列を構築してアカウントにクエリを実行するかを選択します。デフォルトでは、**[シンプル]** が選択されています。	○

オプション	説明	必須
Folder ID (フォルダー ID)	指定されたフォルダー ID でアカウントにクエリを実行します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Search Text (検索テキスト)	指定された検索テキストに一致するアカウントにクエリを実行します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Search Field (検索フィールド)	指定された検索テキストを使用して検索するフィールド。指定しない場合、クエリは `name` フィールドを検索します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Exact Match (完全一致)	検索テキストと完全一致を実行します。デフォルトでは、これは選択されていません。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Query String (クエリ文字列)	URL クエリパラメーターの文字列を指定します。このオプションは、クエリモードが **[高度]** に設定されている場合にのみ使用でき、この場合は必須です。	○
Use Private Key (秘密鍵を使用する)	パスワード認証ではなく鍵ベースの認証を使用して SSH 接続を行います。	×
Use SSL (SSL を使用する)	安全な通信のために SSL を使用します。	○
Verify SSL Certificate (SSL 証明書を検証する)	Delinea Secret Server SSL 証明書を検証します。	×
Delinea Elevate Privileges with (Delinea 権限昇	初回認証後にユーザー権限を昇格させる場合に使用する Elevate Privileges with (権限昇格方法)です。su、su+sudo、sudo など、権限昇格の複数のオプションがサポートされています。	○

オプション	説明	必須
格方法)	Elevate Privileges with (権限昇格方法)を選択すると、[クエリモード] とそれに関連するオプションと同様に、昇格クエリを設定するオプションが表示されます。これらのフィールドは、昇格に最初のログインとは別のアカウント (たとえば「su」) を使用する場合にのみ入力必須となります。	

Kerberos

MIT の Athena プロジェクトによって開発された Kerberos は、対称鍵の暗号プロトコルを使用するクライアントサーバーアプリケーションです。対称暗号方式では、データの暗号化に使用されるキーは、データの復号に使用されるキーと同じです。企業は、Kerberos 認証を必要とするすべてのユーザーとサービスを含む KDC (Key Distribution Center) をデプロイします。ユーザーは、TGT (チケット交付用チケット) をリクエストして Kerberos 認証を行います。ユーザーに TGT が付与されると、ユーザーはそれを使用して、他の Kerberos ベースのサービスを利用可能にするサービスチケットを KDC に対してリクエストします。Kerberos は、CBC (Cipher Block Chain) の DES 暗号化プロトコルを使用してすべての通信を暗号化します。

注意: この認証方法を使用するには、Kerberos 環境を既に確立している必要があります。

Tenable Nessus での Linux ベースの SSH 用 Kerberos 認証の実装では、aes-cbc と aes-ctr 暗号アルゴリズムがサポートされます。Tenable Nessus と Kerberos のやり取りの概要を次に示します。

- エンドユーザーが KDC の IP を指定する
- nessusd が sshd で Kerberos 認証がサポートされるかどうかを確認する
- sshd が yes と答える
- nessusd がログインとパスワードとともに Kerberos TGT をリクエストする
- Kerberos が nessusd にチケットを送信する
- nessusd が sshd にチケットを送信する
- nessusd のログインが完了する

Windows と SSH では、リモートシステムの Kerberos キーを使用して認証情報を指定できます。Windows と SSH では設定が異なります。

オプション	説明
Username (ユーザー名)	ターゲットシステムのユーザー名。
Password (パスワード)	指定されたユーザー名のパスワードです。
Key Distribution Center (KDC) (キー配布センター (KDC))	このホストは、ユーザーのセッションチケットを提供します。
KDC Port (KDC ポート)	このオプションを設定すると、88 以外のポートで稼働している KDC に Tenable Nessus を接続させることができます。
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。
Realm (領域)	Realm は、通常標的のドメイン名として記録されている認証ドメインです (例: example.com)。
Elevate privileges with (権限昇格方法)	認証が完了した後に権限を昇格します。
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。

オプション	説明
	[認証情報を優先するターゲット] を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

Kerberos を使用する場合、KDC でチケットを検証するには Kerberos をサポートする sshd を設定する必要があります。これを機能させるには、逆引き DNS ルックアップを適切に設定する必要があります。Kerberos の相互認証方法は、gssapi-with-mi である必要があります。

Password (パスワード)

オプション	説明
Username (ユーザー名)	ターゲットシステムのユーザー名。
Password (パスワード)	指定されたユーザー名のパスワードです。
Elevate privileges with (権限昇格方法)	認証が完了した後に権限を昇格します。
Custom password prompt (カスタムパスワードプロンプト)	ターゲットのホストが使用するパスワードプロンプトこの設定を使用するのは、ターゲットとなるホストのインタラクティブ SSH シェルで、認識されていないパスワードプロンプトを Tenable Vulnerability Management が受け取るために、インタラクティブ SSH セッションが失敗する場合のみです。
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。

オプション	説明
	[認証情報を優先するターゲット] を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

公開鍵

非対称鍵暗号化とも呼ばれる公開鍵暗号化は、公開鍵と秘密鍵のペアを使用することにより、より安全な認証メカニズムを提供します。この非対称暗号化では、Tenable Nessus は公開鍵を使用してデータを暗号化し、Tenable Nessus は秘密鍵を使用してそのデータを復号します。公開鍵と秘密鍵を両方使用すると、より安全でフレキシブルな SSH 認証を行うことができます。Tenable Nessus では DSA 鍵と RSA 鍵の両方式をサポートしています。

Tenable Nessus は、公開鍵暗号化と同様に RSA と DSA の OpenSSH 証明書をサポートしています。Tenable Nessus では、認証局 (CA) の署名付きのユーザー証明書とユーザーの秘密鍵も必要です。

注意: Tenable Nessusは openssh SSH 公開鍵形式 (pre-7.8 OpenSSH) をサポートしています。Tenable Nessus は新たな OPENSSH 形式 (OpenSSH versions 7.8+) をサポートしていません。所有するバージョンを確認するには、秘密鍵の内容を確認してください。openssh では **-----BEGIN RSA PRIVATE KEY-----** または **-----BEGIN DSA PRIVATE KEY-----** と表示され、互換性のない新たな OPENSSH では **-----BEGIN OPENSSH PRIVATE KEY-----** と表示されます。PuTTY や SSH Communications Security などの非 openssh の形式は、openssh 公開鍵形式に変換する必要があります。

認証情報を使用するスキャンでは、root 権限のある認証情報を使用する方法が最も効果的です。多くのサイトは root によるリモートログインを許可していないことから、Tenable Nessus は、su または sudo 権限が設定されたアカウントの別のパスワードを使用して、su、sudo、su+sudo、dzdo、.k5login、pbrun を呼び出すことができます。また Tenable Nessusは、Cisco 'enable' または Kerberos ログイン用の .k5login ファイルを選択することにより、Cisco デバイスにおける権限を昇格できます。

注意: Tenable Nessus は、blowfish-cbc、aes-cbc、aes-ctr 暗号アルゴリズムをサポートしています。商用版の SSH の一部は、おそらく輸出上の制約から blowfish アルゴリズムをサポートしていません。特定の種類の暗号のみを受け入れるように SSH サーバーを設定することもできます。SSH サーバーが適切なアルゴリズムをサポートすることを確認してください。

Tenable Nessus は、ポリシーに保存されているすべてのパスワードを暗号化します。ただし、認証には SSH パスワードではなく SSH 鍵を使用することをお勧めします。これにより、既知の SSH サーバーの監査に使用しているものと同じユーザー名とパスワードが、制御できないシステムへのログイン試行に使用されないようにします。

注意: サポートされているネットワークデバイスでは、Tenable Nessus はそのネットワークデバイスの SSH 接続用のユーザー名とパスワードのみをサポートします。

root 以外のアカウントを使用して権限昇格を行う場合は、昇格アカウントに、そのアカウントと昇格パスワードを指定できます。

オプション	説明
Username (ユーザー名)	ホストシステムで認証に使用されているアカウントのユーザー名です。
Private Key (プライベートキー)	ユーザーの RSA、DSA、ECDSA、または ED25519 OpenSSH 秘密鍵。
Private key passphrase (秘密鍵のパスフレーズ)	秘密鍵のパスフレーズです。
Elevate privileges with (権限昇格方法)	認証が完了した後に権限を昇格します。
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

QiAnXin (Tenable Nessus Manager のみ) SSH 認証方法: QiAnXin

ヒント: QiAnXin の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
QiAnXin Host (QiAnXin ホスト)	QiAnXin ホストの IP アドレスまたは URL。	○
QiAnXin Port (QiAnXin ポート)	QiAnXin API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○
QiAnXin API Client ID (QiAnXin API クライアント ID)	QiAnXin PAM で作成された埋め込みアカウントアプリケーションのクライアント ID。	○
QiAnXin API Secret ID (QiAnXin API 秘密 ID)	QiAnXin PAM で作成された埋め込みアカウントアプリケーションの秘密 ID。	○
Username (ユーザー名)	スキャンするホストにログインするためのユーザー名	○
Host IP (ホスト IP)	使用するアカウントを含む資産のホスト IP を指定します。指定しない場合、スキャンターゲット IP が使用されます。	×
Platform (プラットフォーム)	使用するアカウントを含む資産のプラットフォーム (資産タイプに基づく) を指定します。指定しない場合、認証情報のタイプに基づいてデフォルトのターゲットが使用されます (たとえば、Windows 認証情報の場合、デフォルトは WINDOWS です)。可能な値は次のとおりです。 • **ACTIVE_DIRECTORY** - Windows ドメインアカウント • **WINDOWS** - Windows ローカルアカウント • **LINUX** - Linux アカウント • **SQL_SERVER** - SQL Server データベース	×

オプション	説明	必須
	• **ORACLE** - Oracle データベース • **MYSQL** - MySQL データベース • **DB2** - DB2 データベース • **HP_UNIX** - HP Unix • **SOLARIS** - Solaris • **OPENLDAP** - OpenLDAP • **POSTGRESQL** - PostgreSQL	
Region ID (リージョン ID)	使用するアカウントを含む資産のリージョン ID を指定します。	複数のリージョンを使用している場合のみ必須
Elevate Privileges with (権限昇格方法)	ドロップダウンメニューを使用してElevate Privileges with (権限昇格方法)を選択します。権限昇格をスキップするには [なし] を選択します。 **注意:** Tenable では、権限昇格で su、su+sudo、sudo などの複数のオプションを使用できます。たとえば sudo を選択すると、sudo ユーザー、昇格アカウント名、su と sudo の場所 (ディレクトリ) のフィールドが追加で表示され、これらのフィールドに入力することで QiAnXin による認証と権限昇格をサポートできます。[昇格アカウント名] フィールドは、昇格パスワードが通常のログインパスワードと異なる場合にのみ必要です。 **注意:** サポートされている権限昇格タイプと各タイプに伴うフィールドの詳細については、Nessus ユーザーガイドまたは Tenable Vulnerability Management ユーザーガイドを参照してください。	権限昇格を行う場合は必須です。
Escalation Account	昇格アカウントのユーザー名またはパスワードが最小権限	×

オプション	説明	必須
Username (昇格アカウントのユーザー名)	ユーザーと異なる場合、昇格アカウント認証情報の認証情報 ID または識別子をここに入力します。	
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。	×
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストがユーザーにセッションチケットを提供します。	○
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。Tenable はデフォルトで 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。	×
Realm (領域)	(Kerberos ターゲット認証が有効な場合は必須) この領域は、通常ターゲットのドメイン名として記載されている認証ドメインです。	○
Use SSL (SSL を使用する)	有効にすると、Tenable は安全な通信のために SSL を使用します。このオプションはデフォルトで有効です。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable は、サーバーの SSL 証明書が信頼できる認証局によって署名されたものかどうかを検証します。	×
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。	×

オプション	説明	必須
	この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	

Senhasegura (Tenable Nessus Manager のみ)

ヒント: Senhasegura の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
Senhasegura Host (Senhasegura ホスト)	Senhasegura ホストの IP アドレスまたは URL です。	○
Senhasegura Port (Senhasegura ポート)	Senhasegura API が通信に使用するポートです。Tenable はデフォルトで 443 を使用します。	○
Senhasegura API Client ID (Senhasegura API クライアント ID)	Oauth 2.0 API 認証に適用される Senhasegura A2A アプリケーションのクライアント ID です。	○
Senhasegura API Secret ID (Senhasegura API のシークレット ID)	Oauth 2.0 API 認証に適用される Senhasegura A2A アプリケーションのシークレット ID です。	○
Senhasegura Credential ID or	取得をリクエストしている認証情報の認証情報 ID または識別子です。	○

オプション	説明	必須
Identifier (Senhasegura 認証情報 ID または識別子)		
Use SSH Key for Target Authentication (Use SSH Key for Target Authentication (ターゲット認証に SSH キーを使用する))	設定が Senhasegura に適用可能な場合、ユーザーはこのオプションを選択して、ターゲットへの認証を行うための SSH キーを取得できます。	ターゲットへの認証を SSH キーで行う場合は必須です。
Private Key File (秘密鍵ファイル)	A2A からの暗号化された機密データを復号するために使用される秘密鍵です。 **注意:** A2A アプリケーション認証で機密データの暗号化を有効にできます。有効にした場合、スキャン認証情報に秘密鍵ファイルを指定する必要があります。これは、Senhasegura の該当する A2A アプリケーションからダウンロードできます。	A2A アプリケーション認証で機密データの暗号化を有効にした場合には必須です。
Elevate Privileges with (権限昇格方法)	ドロップダウンメニューを使用してElevate Privileges with (権限昇格方法)を選択します。権限昇格をスキップするには **[Nothing] (なし)** を選択します。 **注意:** Tenable では、権限昇格で su、su+sudo、sudo などの複数のオプションを使用できます。たとえば sudo を選択すると、sudo ユーザー、昇格アカウント名、su と sudo の場所 (ディレクトリ) のフィールドが追加で表示され、これらのフィールドに入力することで Senhasegura による認証と権限昇格をサポートできます。権限昇格を完了するには、[Escalation Account Name] (昇格アカウント名) フィールドに入力する必要があります。 **注意:** サポートされている権限昇格タイプと各タイプに伴う	権限昇格を行う場合は必須です。

オプション	説明	必須
	フィールドの詳細については、Nessus ユーザーガイド、Tenable Vulnerability Management ユーザーガイド、または Tenable Security Center ユーザーガイドを参照してください。	
昇格アカウント認証情報 ID または識別子	昇格アカウントのユーザー名またはパスワードが最小権限ユーザーと異なる場合、昇格アカウント認証情報の認証情報 ID または識別子をここに入力します。	×
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	×
HTTPS	このオプションはデフォルトで有効です。	○
Verify SSL Certificate (SSL 証明書を検証する)	これはデフォルトでは無効になっています。	×

Thycotic Secret Server (Tenable Nessus Manager のみ)

オプション	デフォルト値
ユーザー名 (必須)	ssh 経由のシステム認証に使用されるユーザー名です。

Domain (ドメイン)	Windows 認証情報を使用する場合は、ユーザー名が属するドメインを設定します。
Thycotic シークレット名 (必須)	これは、Thycotic サーバーに保管するシークレットの名前として使用する値です。Thycotic サーバーでは「シークレット名」と呼ばれます。
Thycotic Secret Server URL (必須)	このオプションを使用して、スキャナーの転送方法、ターゲット、ターゲットディレクトリを設定します。この値は、Thycotic サーバーの **[Admin]** (管理) > **[Configuration]** (設定) > **[Application Settings]** (アプリケーション設定) > **[Secret Server URL]** (シークレットサーバー URL) にあります。例として https://pw.mydomain.com/SecretServer/ について検討します。これを解析すると、HTTPS が SSL 接続であること、pw.mydomain.com がターゲットアドレスであること、/SecretServer/ がルートディレクトリであることが分かります。
Thycotic ログイン名 (必須)	Thycotic サーバーを認証するためのユーザー名です。
Thycotic Password (必須)	Thycotic ログイン名に関連付けられたパスワードです。
Thycotic Organization (必須)	この値を Thycotic のクラウドインスタンスで使用して、クエリがヒットする企業を定義します。
Thycotic Domain (オプション)	これは、Thycotic サーバーにドメイン値を設定した場合に設定するオプションの値です。
Private Key (オプション)	SSH 接続には、パスワードではなく鍵ベースの認証を行います。
Verify SSL Certificate (SSL 証明書を検証する)	サーバーの SSL 証明書が信頼できる認証局によって署名されているかどうかを検証。
Thycotic	初回認証後にユーザー権限を昇格させるために使用するElevate Privileges

Elevate privileges with (Thycotic 権限昇格方法)	with (権限昇格方法)です。Tenable Nessus では、権限昇格のために su、su+sudo、sudo などの複数のオプションを使用できます。この選択によって、設定する必要があるオプションの内容が決まります。
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

BeyondTrust (Tenable Nessus のみ)

ヒント: BeyondTrust の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	デフォルト値
Username (ユーザー名)	(必須) スキャンするホストにログインするためのユーザー名です。
BeyondTrust host (BeyondTrust ホスト)	(必須) BeyondTrust IP アドレスまたは DNS アドレスです。
BeyondTrust port (BeyondTrust ポート)	(必須) BeyondTrust がリッスンしているポートです。

BeyondTrust API key (BeyondTrust API キー)	(必須) BeyondTrust が提供する API キーです。
Checkout duration (チェックアウト期間)	(必須) BeyondTrust で認証情報のチェックアウト状態を保持する時間 (分) です。チェックアウトの期間は、Tenable Nessus における通常のスキャン期間を超えるように設定します。新しいスキャンが開始したときに過去のスキャンのパスワードがまだチェックアウトされている場合、新しいスキャンは失敗します。 **注意:** BeyondTrust でパスワードの変更間隔を設定し、パスワード変更によって Tenable Nessusスキャンが中断されないようにします。スキャン中に BeyondTrust がパスワードを変更すると、スキャンは失敗します。
Use SSL (SSL を使用する)	有効にすると、Tenable Nessusは安全な通信のためにIISを介してSSLを使用します。このオプションを有効にするには、BeyondTrust で IIS を使用して SSL を設定する必要があります。
Verify SSL certificate (SSL 証明書の検証)	有効にすると、Tenable Nessus は SSL 証明書を検証します。このオプションを有効にするには、BeyondTrust で IIS を使用して SSL を設定する必要があります。
Use private key (プライベートキーの使用)	有効にすると、Tenable Nessus はパスワード認証ではなく秘密鍵ベースの認証で SSH 接続を行います。失敗した場合、Tenable Nessus はパスワードを要求します。
Use privilege escalation (権限昇格の使用)	有効にすると、BeyondTrust は設定された権限昇格コマンドを使用します。コマンドから何かが返された場合は、それをスキャンに使用します。
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、

	最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

Lieberman (Tenable Nessus Manager のみ)

オプション	説明	必須
Username (ユーザー名)	ターゲットシステムのユーザー名。	○
Lieberman host (Lieberman ホスト)	Lieberman の IP/DNS アドレス。 **注意:** Lieberman インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパス*の形式で入力します。	○
Lieberman port (Lieberman ポート)	Lieberman がリッスンするポート。	○
Lieberman API URL	Tenable Nessus が Lieberman へのアクセスに使用する URL。	×
Lieberman user (Lieberman ユーザー)	Lieberman RED API への認証に使用される Lieberman 明示ユーザーです。	○
Lieberman password (Lieberman パスワード)	Lieberman 明示ユーザーのパスワード。	○
Lieberman Authenticator (Lieberman 認証)	Lieberman のオーセンティケーターに使用されるエイリアス。この名前は Lieberman で使用される名前に一致する必要があります。 **注意:** このオプションを使用する場合は、**[Lieberman ユーザー]** オプションにドメインを追加してください (例: *domain\user*)。	×

オプション	説明	必須
Lieberman Client Certificate (Lieberman クライアント証明書)	Lieberman ホストとの通信に使用される PEM 証明書を含むファイル。 **注意:** このオプションを使用する場合は、**[Lieberman ユーザー]**、**[Lieberman パスワード]**、**[Lieberman 認証]** の各フィールドに情報を入力する必要はありません。	×
Lieberman Client Certificate Private Key (Lieberman クライアント証明書のプライベートキー)	クライアント証明書の PEM プライベートキーを含むファイル。	×
Lieberman Client Certificate Private Key Passphrase (Lieberman クライアント証明書の秘密鍵パスフレーズ)	プライベートキーのパスフレーズ (必要な場合)。	×
Use SSL (SSL を使用する)	Lieberman が安全な通信のために IIS チェックによって SSL をサポートするように設定されている場合。	×
Verify SSL Certificate (SSL 証明書の検証)	Lieberman が安全な通信のために IIS チェックによって SSL をサポートするように設定されており、証明書を検証する場合、このオプションにチェックマークを入れます。自己署名証明書の使用方法については、カスタム CA ドキュメントを参照してください。	×
System Name (システム名)	まれなケースではあるものの、お客様の企業がすべての管理対象システムにデフォルトの Lieberman エントリを 1 つ使用している場合は、デフォルトのエントリ名を入力します。	×

オプション	説明	必須
Custom password prompt (カスタムパスワードプロンプト)	ターゲットのホストが使用するパスワードプロンプトこの設定を使用するのは、ターゲットとなるホストのインタラクティブ SSH シェルで、認識されていないパスワードプロンプトを Tenable Nessus が受け取るために、インタラクティブ SSH セッションが失敗する場合のみです。	×
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	×

Wallix Bastion (Tenable Nessus Manager のみ)

ヒント: Wallix Bastion の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
WALLIX Host (Delinea ホスト)	WALLIX Bastion ホストの IP アドレス。	○
WALLIX ポート	WALLIX Bastion API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○
Authentication Type (認証タイプ)	**[Basic]** (基本) 認証 (WALLIX Bastion ユーザーインターフェースのユーザー名とパスワードが必要) または **[API Key]** (API キー) 認証 (ユーザー名と WALLIX Bastion 生	×

オプション	説明	必須
	成の API キーが必要)。	
WALLIX ユーザー	WALLIX Bastion ユーザーインターフェースのログインユーザー名。	○
WALLIX Password (Delinea パスワード)	WALLIX Bastion ユーザーインターフェースのログインパスワード。API への **[Basic]** (基本) 認証に使用されます。	○
WALLIX API キー	WALLIX Bastion ユーザーインターフェースで生成された API キー。API への **[API Key]** (API キー) 認証に使用されます。	○
Get Credential by Device Account Name (デバイスアカウント名で認証情報を取得する)	ターゲットシステムへのログインに使用する**デバイス**が関連付けられているアカウント名。 **注意:** デバイスに複数のアカウントがある場合、認証情報を取得するアカウントの特定のデバイス名を入力する必要があります。入力しないと、システムから誤ったアカウントの認証情報が返される可能性があります。	複数のアカウントがあるターゲットやデバイスを使用している場合にのみ必要です。
HTTPS	これはデフォルトで有効です。 **注意: HTTPS** を無効にすると、統合が失敗します。	○
Verify SSL Certificate (SSL 証明書を検証する)	これはデフォルトで無効になっており、WALLIX Bastion PAM 統合ではサポートされていません。	×
Elevate Privileges with (権限昇格方法)	これにより、WALLIX Bastion 特権アクセス管理 (PAM) が有効になります。ドロップダウンメニューを使用して、Elevate Privileges with (権限昇格方法)を選択します。この機能をバイパスするには、このフィールドを **[Nothing]** (なし) に設定されたままにします。	権限昇格を行う場合に必要です。

オプション	説明	必須
	警告: PAM を有効にするには、WALLIX Bastion アカウントで、WALLIX Bastion スーパー管理者がアカウントの「認証情報回復」を有効にしている必要があります。有効にしないと、スキャンから結果が返されない可能性があります。詳細は、WALLIX Bastion ドキュメントを参照してください。 **注意:** *su*、*su+sudo*、*sudo* など、複数の権限昇格オプションがサポートされています。たとえば **sudo** を選択すると、**[sudo user]** (sudo ユーザー)、**[Escalation Account Name]** (昇格アカウント名)、**[Location of su and sudo]** (su と sudo の場所) のフィールドが追加で表示され、これらのフィールドに入力することで WALLIX Bastion PAM による認証と権限昇格をサポートできます。権限昇格を完了するには、**[Escalation Account Name]** (エスカレーションアカウント名) フィールドに入力する必要があります。 **注意:** サポートされている権限昇格タイプと各タイプに伴うフィールドの詳細については、Tenable Nessus ユーザーガイドを参照してください。	
Database Port (データベースのポート)	通信に対して Oracle データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 1521 です。	×
Auth Type (認証方法)	データベースインスタンスにアクセスするために Tenable が使用するアカウントの種類。 • **SYSDBA** • **SYSOPER** • **NORMAL**	×
Service Type (サービスの種類)	データベースインスタンスを指定するために使用する Oracle パラメーター: **SID** または **SERVICE_NAME**	×
Service (サービス)	データベースインスタンスの SID 値または SERVICE_NAME 値。	○

オプション	説明	必須
	入力する **[Service]** (サービス) 値は、**[Service Type]** (サービスタイプ) オプションのパラメーターとして選択した値と一致する必要があります。	
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	×

HashiCorp Vault (Tenable Nessus Manager のみ)

ヒント: HashiCorp の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Windows と SSH の認証情報		
オプション	**説明**	**必須**
Hashicorp Vault host (Hashicorp Vault ホスト)	Hashicorp Vault IP アドレスまたは DNS アドレス。 **注意:** Hashicorp Vault インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパス*の形式で入力します。	○
Hashicorp Vault port	Hashicorp Vault がリッスンするポート。	○

(Hashicorp Vault ポート)		
Authentication Type (認証タイプ)	インスタンスに接続するための認証タイプとして、**[App Role]** (アプリロール) または **[Certificates]** (証明書) を指定します。 **[証明書]** を選択すると、**[Hashicorp Client Certificate]** (Hashicorp クライアント証明書) (必須) および **[Hashicorp Client Certificate Private Key]** (Hashicorp クライアント証明書の秘密鍵) (必須) の追加オプションが表示されます。クライアント証明書と秘密鍵にそれぞれ適切なファイルを選択してください。	○
Role ID (ロール ID)	App Role を構成したときに Hashicorp Vault によって提供される GUID です。	○
Role Secret ID (ロールシークレット名)	App Role を構成したときに Hashicorp Vault によって生成される GUID です。	○
Authentication URL (認証 URL)	認証エンドポイントへのパス/サブディレクトリ。This is not the full URL. (これは完全な URL ではありません。)たとえば、 `/v1/auth/approle/login`	○
Namespace (名前空間)	マルチチーム環境で指定されたチームの名前	×
Vault Type (Vault タイプ)	Tenable Nessus バージョン: KV1、KV2、AD、LDAP。Tenable Nessus バージョンの詳細については、Tenable Nessus のドキュメントを参照してください。	○
KV1 Engine URL (KV1 エンジン URL)	(KV1) Tenable Nessus が KV1 エンジンへのアクセスに使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (KV1 **Vault タイプ** を選択した場合)
KV2 Engine URL	(KV2) Tenable Nessus が KV2 エンジンにアクセスするた	○ (KV2

(KV2 エンジン URL)	めに使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	**Vault タイプ**を選択した場合)
AD Engine URL (AD エンジン URL)	(AD) Tenable Nessus が Active Directory エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (AD **Vault タイプ**を選択した場合)
LDAP Engine URL (LDAP エンジン URL)	(LDAP) Tenable Nessus が LDAP エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (LDAP **Vault タイプ**を選択した場合)
Username Source (ユーザー名ソース)	(KV1 および KV2) ユーザー名が手動で入力されるか、Hashicorp Vault からプルするかを指定するドロップダウンボックスです。	○
Username Key (ユーザー名鍵)	(KV1 および KV2) ユーザー名が格納されている Hashicorp Vault での名前です。	○
Password Key (パスワード鍵)	(KV1 および KV2) パスワードが格納されている Hashicorp Vault での鍵です。	○
Domain Key (Windows) (ドメイン鍵 (Windows))	(Kerberos ターゲット認証が有効な場合は必須。) ドメインが保存される秘密鍵の名前です。	○
Secret Name (秘密名)	(KV1、KV2、AD) 値を取得したい鍵秘密です。	○
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。	×
Key Distribution Center (KDC) (キー配	(Kerberos ターゲット認証が有効な場合は必須。) このホストは、ユーザーにセッションチケットを提供します。	○

布センター (KDC))		
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。デフォルトでは、Tenable は 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。	×
Domain (Windows) (ドメイン (Windows))	(Kerberos ターゲット認証が有効な場合は必須。) Kerberos ターゲット認証が属するドメイン (該当する場合)。	○
Realm (SSH) (領域 (SSH))	(Kerberos ターゲット認証が有効な場合は必須。) Realm は、通常標的のドメイン名として記録されている認証ドメインです (例: example.com)。	○
Use SSL (SSL を使用する)	有効にすると、Tenable Nessus Manager は安全な通信のために SSL を使用します。このオプションを有効にする前に、Hashicorp Vault で SSL を設定してください。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable Nessus Manager は SSL 証明書を検証します。このオプションを有効にする前に、Hashicorp Vault で SSL を設定してください。	×
Tenable Nessus に対して有効にする	Tenable Nessus での IBM DataPower Gateway の使用を有効または無効にします。	○
Elevate Privileges with (SSH) (権限昇格方法 (SSH))	スキャンの実行時に追加の権限を使用するには、su や sudo などの権限昇格手法を使用します。 **注意:** Tenable では、権限昇格のために su、su+sudo、sudo などの複数のオプションを使用できます。たとえば sudo を選択すると、sudo ユーザー、昇格アカウントの秘密名、sudo の場所 (ディレクトリ) のフィールドが追加で表示され、これらのフィールドに入力することで Tenable Nessus による認証と権限昇格をサポートできます。	権限昇格を行う場合は必須です。

	注意: サポートされている権限昇格タイプと各タイプに伴うフィールドの詳細については、Nessus ユーザーガイドおよび Tenable Vulnerability Management ユーザーガイドを参照してください。	
Escalation account secret name (SSH) (昇格アカウントシークレット名 (SSH))	昇格アカウントのユーザー名またはパスワードが最小権限ユーザーと異なる場合、昇格アカウント認証情報の認証情報 ID または識別子をここに入力します。	×
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	×

Centrify (Tenable Nessus Manager のみ)

オプション	デフォルト値
Centrify Host (Centrify ホスト)	(必須) Centrify IP アドレスまたは DNS アドレスです。 **注意:** Centrify インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名 / サブディレクトリパスの形式で入力します。*
Centrify Port (Centrify ポート)	Centrify がリッスンするポート。

オプション	デフォルト値
API User (API ユーザー)	(必須) Centrify が提供する API ユーザー
API Key (API キー)	(必須) Centrify が提供する API キー。
Tenant (テナント)	マルチチーム環境で指定されたチームの名前です。
Authentication URL (認証 URL)	Tenable Nessus Manager が Centrify へのアクセスに使用する URL。
Password Engine URL (パスワードエンジン URL)	マルチチーム環境で指定されたチームの名前です。
Username (ユーザー名)	(必須) スキャンするホストにログインするためのユーザー名。
Checkout duration (チェックアウト期間)	Centrify で認証情報のチェックアウト状態を保持する時間 (分)。 **チェックアウトの期間**は、Tenable Nessus Manager における通常のスキャン期間を超えるように設定します。新しいスキャンが開始したときに過去のスキャンのパスワードがまだチェックアウトされている場合、新しいスキャンは失敗します。 **注意**：Centrify でパスワードの変更間隔を設定し、パスワード変更によって Tenable Nessus Manager スキャンが中断されないようにします。スキャン中に Centrify がパスワードを変更すると、スキャンは失敗します。
Use SSL (SSL を使用する)	有効にすると、Tenable Nessus Manager は安全な通信のために IIS を介して SSL を使用します。このオプションを有効にするには、Centrify で IIS を使用して SSL を設定する必要があります。
Verify SSL (SSL を検証する)	有効にすると、Tenable Nessus Manager は SSL 証明書を検証します。このオプションを有効にするには、Centrify で IIS を使用して SSL を設定する必要があります。
Targets to	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロック

オプション	デフォルト値
Prioritize Credentials (認証情報を優先するターゲット)	を指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

Arcon (Tenable Nessus Manager のみ)

ヒント: Arcon の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	デフォルト値
Arcon host (Arcon のホスト)	(必須) Arcon IP アドレスまたは DNS アドレスです。 **注意:** Arcon インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパスの形式で入力します。*
Arcon port (Arcon ポート)	Arcon がリッスンするポート。
API User (API ユーザー)	(必須) Arcon が提供する API ユーザーです。
API Key (API キー)	(必須) Arcon が提供する API キーです。
Authentication URL (認証 URL)	Tenable Nessus Manager が Arcon へのアクセスに使用する URL。
Password Engine	Tenable Nessus Manager が Arcon のパスワードへのアクセスに使用する

オプション	デフォルト値
URL (パスワードエンジン URL)	URL。
Username (ユーザー名)	(必須) スキャンするホストにログインするためのユーザー名。
Arcon Target Type (Arcon ターゲットタイプ)	(オプション) ターゲットタイプの名前。お使いの Arcon PAM のバージョンと SSH 認証情報を作成したシステムのタイプにより異なりますが、デフォルトでは **linux** に設定されます。正しいターゲットタイプ値を知るためのターゲットタイプ/システムタイプのマッピングは、Arcon PAM 仕様ドキュメント (Arcon 提供) を参照してください。
Checkout Duration (チェックアウト期間)	(必須) Arcon で認証情報のチェックアウト状態を保持する時間 (時間)です。 **チェックアウトの期間**は、Tenable Vulnerability Management における通常のスキャン期間を超えるように設定します。新しいスキャンが開始したときに過去のスキャンのパスワードがまだチェックアウトされている場合、新しいスキャンは失敗します。 **注意**: Arcon でパスワードの変更間隔を設定し、パスワード変更によって Tenable Vulnerability Management スキャンが中断されないようにします。スキャン中に Arcon がパスワードを変更すると、スキャンは失敗します。
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストがユーザーにセッションチケットを提供します。
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。Tenable はデフォルトで 88 を使用します。

オプション	デフォルト値
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。
Realm (領域)	(Kerberos ターゲット認証が有効な場合は必須) 領域とは認証ドメインのことです。通常、ターゲットのドメイン名として記載されています。
Use SSL (SSL を使用する)	有効にすると、Tenable Nessus Manager は安全な通信のために IIS を介して SSL を使用します。このオプションを有効にするには、Arcon で IIS を使用して SSL を設定する必要があります。
Verify SSL (SSL を検証する)	有効にすると、Tenable Nessus Manager は SSL 証明書を検証します。このオプションを有効にするには、Arcon で IIS を使用して SSL を設定する必要があります。
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

Windows

Windows 認証情報メニュー項目には、SMB アカウント名、パスワード、ドメイン名などの情報を Nessus に提供する設定があります。デフォルトで、Windows ホストにログインするためのユーザー名、パスワード、ドメインを指定できます。また、Nessus では、Windows ベースのシステム用に複数の異なるタイプの認証方法がサポートされています。

認証方法について

- Lanman 認証の方法は、Windows NT と初期の Windows 2000 サーバーのデプロイメントで普及していました。Lanman 認証方法は、下位互換性用に保持されています。
- Windows NT で導入された NTLM 認証方法は、Lanman 認証よりもセキュリティが向上しています。拡張バージョンである NTLMv2 は、NTLM よりも暗号学的に安全性が高く、Nessus が Windows Server にログインしようとするときに選択するデフォルトの認証方法となっています。NTLMv2 は SMB 署名を使用できます。
- SMB 署名は、Windows Server との間のすべての SMB トラフィックに適用される暗号化チェックサムです。システム管理者の多くは、サーバーで SMB 署名機能を有効化し、リモートユーザーが 100% 認証されており、ドメインの一部であることを確認します。さらに、John the Ripper や L0phtCrack などのツールによる辞書攻撃で簡単に破られることのない強力なパスワードの使用を義務付けるポリシーを実施するようにしてください。SMB 署名は、リモートの Windows Server から求められた場合、Nessus が自動的に使用します。Windows セキュリティに対し、コンピューターからの不正なハッシュの再利用によるサーバーの攻撃など、さまざまな種類の攻撃が行われています。SMB 署名は、これらの中間者攻撃を防ぐためにセキュリティ層を追加します。
- SPNEGO (Simple and Protected Negotiate) プロトコルは、ユーザーの Windows ログイン認証情報を介して、Windows クライアントからさまざまな保護リソースへのシングルサインオン (SSO) 機能を提供します。Nessus は、SPNEGO スキャンとポリシーの使用をサポートします : LMv2 認証付きの NTLMSSP または Kerberos と RC4 暗号化のいずれかで 151 のうち 54 をスキャンします。SPNEGO 認証は、NTLM または Kerberos 認証を通じて行われます。Nessus ポリシーで設定する必要はありません。
- 拡張セキュリティスキーム (Kerberos、SPNEGO など) がサポートされていないか、または失敗した場合、Nessus は NTLMSSP/LMv2 認証を介してログインを試みます。それが失敗した場合、Nessus は NTLM 認証を使用してログインを試行します。
- Nessus は、Windows ドメインでの Kerberos 認証の使用もサポートしています。上記を設定するには、Kerberos ドメインコントローラーの IP アドレス (実際には、Windows Active Directory サーバーの IP アドレス) を提供する必要があります。

サーバーメッセージブロック (SMB) は、コンピューターがネットワーク全体で情報を共有できるようにするファイル共有プロトコルです。この情報を Nessus に提供することで、リモートの Windows ホストからローカル情報を見つけられるようになります。たとえば、認証情報を使用すると、Nessus は重要なセキュリティパッチが適用されているかどうかを判断できます。他の SMB パラメーターをデフォルト設定から変更する必要はありません。

SMB ドメイン設定はオプションであり、Nessus はこの設定がなくてもドメイン認証情報を使用してログオンできます。ユーザー名、パスワード、オプションのドメインは、ターゲットのマシンが認識しているアカウントを参照します。たとえば、*joesmith* というユーザー名と *my4x4mpl3* というパスワードを入力すると、Windows Server は、まずローカルシステムのユーザーリストでこのユーザー名を検索し、それがドメインの一部であるかどうかを判断します。

使用される認証情報に関係なく、Nessus は常に次の組み合わせで Windows Server へのログインを試行します。

- パスワードを持たない管理者
- ゲストアカウントをテストするためのランダムなユーザー名とパスワード
- ユーザー名とパスワードなしで null セッションをテスト

実際のドメイン名は、アカウント名がコンピューター上のアカウント名とドメイン上で異なる場合にのみ必要となります。Windows Server とドメイン内で管理者アカウントを持つことができます。この場合、ローカルサーバーにログオンするために、管理者のユーザー名がそのアカウントのパスワードと共に使用されます。ドメインにログオンするには、管理者のユーザー名をメインパスワードとドメイン名とともに使用します。

複数の SMB アカウントが設定されている場合、Nessus は提供された認証情報で順次ログインを試行します。Nessus は、一連の認証情報で認証できるようになると、提供された次の認証情報を確認しますが、以前のアカウントがユーザーアクセスを提供したときに管理者権限が付与されている場合にのみそれらを使用します。

Windows の一部のバージョンでは、新しいアカウントが作成でき、そのアカウントを管理者として指定できます。これらのアカウントは、認証情報スキャンの実行に必ずしも適しているとは限りません。Tenable は、完全なアクセスが許可されるように、認証情報のスキャンには管理者と名付けられたオリジナルの管理アカウントを使用することを推奨します。Windows の一部のバージョンでは、このアカウントは非表示となっている場合があります。実際の管理者アカウントは、管理者権限で DOS プロンプトを実行し、次のコマンドを入力することで非表示にできます。

```
C:\> net user administrator /active:yes
```

SMB アカウントが制限付き管理者権限で作成されている場合、Nessus は複数のドメインを簡単かつ安全にスキャンできます。Tenable は、ネットワーク管理者がテストを容易にするために特定のドメインアカウントの作成を検討することを推奨しています。Nessus は、ドメインアカウントが提供された場合、Windows 10、11、Windows Server 2012、Server 2012 R2、Server 2016、Server 2019、Server 2022

に対してさまざまなセキュリティチェックをより正確に行えます。アカウントが提供されていない場合でも、Nessus は複数のチェックを試行します。

注意: Windows リモートレジストリサービスを使用すると、認証情報を持つリモートコンピューターが監査対象のコンピューターのレジストリにアクセスできます。サービスが実行されていない場合、認証情報が完全でも、キーと値をレジストリから読み取れません。認証情報を使用してシステムを完全に監査するには、Nessus 認証情報スキャン用にこのサービスを開始する必要があります。

詳細は、Tenableブログ投稿 を参照してください。

Windows システムでの認証情報スキャンでは、完全な管理者レベルのアカウントを使用する必要があります。Microsoft のセキュリティ情報とソフトウェア更新プログラムにより、レジストリが読み取られ、ソフトウェアパッチレベルは管理者権限なしでは信頼できないと判断されましたが、すべてではありません。Nessus プラグインは、提供された認証情報が完全な管理者アクセス権を持っていることを確認し、適切に実行されるようにします。たとえば、ファイルシステムを直接読み取るためには、完全な管理者としてアクセスする必要があります。これにより Nessus をコンピューターにアタッチし、ファイル分析を直接実行して評価対象システムの実際のパッチレベルを判断できます。

認証方法

グローバル認証情報設定

オプション	デフォルト	説明
Never send credentials in the clear (暗号化されていない認証情報を送信しない)	Enabled (有効)	セキュリティ上の理由から、デフォルトで、Windows 認証情報を暗号化されていないテキストで送信することはできません。
Do not use NTLMv1 authentication (NTLMv1 認証を使用しない)	Enabled (有効)	このオプションが無効になっている場合、理論的には、NTLM バージョン 1 プロトコル経由でドメイン認証情報を使用し、Nessus を誘導して Windows Server へのログインを試みることが可能です。これにより、リモートの攻撃者は Nessus から取得したハッシュを使用できます。このハッシュは解読され、ユーザー名またはパスワードが特定される可能性があります。また、その他のサーバーに直接ログインするた

オプション	デフォルト	説明
		めに使用される可能性もあります。スキャン時に[Only use NTLMv2] (NTLMv2 のみ使用) 設定を有効にすると、Nessus は強制的に NTLMv2 を使用します。これにより、悪意のある Windows サーバーが NTLM を使用してハッシュを受信することを防ぎます。NTLMv1 は安全なプロトコルではないため、このオプションはデフォルトで有効となっています。
Start the Remote Registry service during the scan (スキャン中にリモートレジストリサービスを開始する)	Disabled (無効)	このオプションは、スキャン対象のコンピューターでリモートレジストリサービスが実行されていない場合に、開始するよう Nessus に指示します。Nessus が Windows ローカルチェックプラグインを実行するには、このサービスが実行されている必要があります。
Enable administrative shares during the scan (スキャン中に管理共有を有効にする)	Disabled (無効)	このオプションにより、Nessus は ADMIN$ および C$ の管理共有にアクセスできます。これは、管理者権限で読み取ることができます。 **注意:** この設定が適切に機能するようにするには、管理共有を有効にする必要があります。ほとんどのオペレーティングシステムでは、ADMIN$ および C$ がデフォルトで有効になっています。ただし、Windows 10、Windows 11、およびそれ以降の Windows バージョンでは、デフォルトで ADMIN$ が無効になっています。したがって、レジストリエントリへのフルアクセスのためにこの設定を使用することに加えて、Windows 環境の ADMIN$ を手動で有効にする必要があります。詳細については、https://support.microsoft.com/kb/842715/en-us を参照してください。
Start the Server service during the scan (スキャン中にサーバーサービスを開始する)	Disabled (無効)	有効になっている場合、スキャナーによって Windows Server サービスが一時的に有効になります。これによって、コンピューターはネットワーク上のファイルと他のデバイスを共有できます。スキャンが完了すると、サービスは無効になります。 デフォルトでは、Windows システムによって Windows Server

オプション	デフォルト	説明
		サービスは無効になっており、この設定を有効にする必要はありません。ただし、ご利用の環境で Windows Server サービスを無効にし、SMB 認証情報を使用してスキャンする場合は、スキャナーがリモートでファイルにアクセスできるようにこの設定を有効にする必要があります。

CyberArk (Nessus Manager のみ)

ヒント: CyberArk の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

CyberArk は、権限付き認証情報の管理に使用できる一般的なエンタープライズパスワードボールトです。Nessus Manager は、CyberArk から認証情報を取得してスキャンに使用します。

オプション	説明	必須
CyberArk Host (CyberArk ホスト)	CyberArk AIM Web サービスの IP アドレスまたは FQDN 名。これは、ホスト、または 1 つの文字列にカスタム URL が追加されたホストにすることができます。	○
Ports (ポート)	CyberArk API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○
AppID	CyberArk API 接続に関連するアプリケーション ID。	○
Client certificate (クライアント証明書)	CyberArk ホストとの通信に使用される PEM 証明書を含むファイル **注意:** Windows Server 2022 以降で CyberArk CCP をセルフホスティングしているお客様は、CyberArk クライアント証明書の認証の問題に関する Tenable のコミュニティの投稿に記載されているガイダンスに従ってください。	×
Client Certificate Private Key (クライアント証明書のプライ	クライアント証明書の PEM プライベートキーを含むファイル。	○ (秘密鍵が適

オプション	説明	必須
ベートキー)		用されている場合)
Client Certificate Private Key Passphrase (クライアント証明書のプライベートキーのパスフレーズ)	プライベートキーのパスフレーズ (必要な場合)。	○ (秘密鍵が適用されている場合)
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。	×
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストがユーザーにセッションチケットを提供します。	○
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。デフォルトでは、Tenable は 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。	×
Domain (ドメイン)	(Kerberos ターゲット認証が有効な場合は必須) Kerberos ターゲット認証が属するドメイン (該当する場合)。	○
Get credential by (認証情報の取得方法)	CyberArk API 認証情報を取得する方法。**[アドレス]**、**[識別子]**、**[パラメーター]**、または **[ユーザー名]** のいずれかです。 **注意: [パラメーター]** オプションの詳細については、**パラメーターオプ**	○

オプション	説明	必須
	ションの表を参照してください。 **注意: ユーザー名**のクエリ頻度は、ターゲットごとにクエリ1回です。**識別子**のクエリの頻度は、チャンクごとにクエリ1回です。この機能では、すべてのターゲットに同じ識別子が必要です。	
Username (ユーザー名)	([**Get credential by**] が**ユーザー名**に設定されている場合) パスワードを要求する CyberArk ユーザーのユーザー名。	×
Safe (セーフ)	認証情報を取得するべき CyberArk のセーフ。	×
Address (アドレス)	このオプションは、アドレス値が単一の CyberArk アカウント認証情報に対して一意である場合にのみ使用します。	×
Account Name (アカウント名)	(**[認証情報の取得]** が **[識別子]** の場合) CyberArk API の認証情報が割り当てられる固有のアカウント名または識別子。	×
Use SSL (SSL を使用する)	有効にすると、スキャナーは安全な通信のために IIS を介して SSL を使用します。CyberArk が IIS を介した SSL をサポートするよう設定されている場合、このオプションを有効にします。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、スキャナーは SSL 証明書を検証します。CyberArk が安全な通信のために IIS によって SSL をサポートするように設定されており、証明書を検証する場合、このオプションを有効にします。	×

CyberArk Auto-Discovery (Nessus Manager のみ)

ヒント: CyberArk の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Tenable と CyberArk との統合による大幅な改善を利用して、複数のターゲットを入力することなく特定のターゲットグループのアカウント情報を一括で収集できるようになりました。

オプション	説明	必須
CyberArk Host (Delinea ホスト)	ユーザーの CyberArk インスタンスの IP アドレスまたは FQDN 名。 **注意:** PVWA と CCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	○
Ports (ポート)	CyberArk API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。 **注意:** PVWA と CCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	○
CCP Host (CCP ホスト)	ユーザーの Cyber Ark CCP コンポーネントの IP アドレスまたは FQDN 名。 **注意:** PVWA と CCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	×
CCP Port (CCP ポート)	Cyber Ark CCP (AIM ウェブサービス) API が通信するポート。Tenable はデフォルトで 443 を使用します。 **注意:** PVWA と CCP を別々のサーバーでホストしているお客様は、このフィールドを PVWA ホストに対してのみ使用する必要があります。	×
AppID	CyberArk API 接続に関連付けられているアプリケーション ID。	○
Safe (セーフ)	ユーザーは、オプションで Safe ボックスを指定してアカウント情報を収集し、パスワードをリクエストできます。	×
AIM Web Service Authentication Type (AIM ウェブサービス認証のタイプ)	この機能では、2 つの認証方法が確立されています。**IIS 基本認証**と**証明書認証**です。証明書認証は、暗号化することも非暗号化することもできます。	○

オプション	説明	必須
CyberArk PVWA ウェブ UI ログイン名	CyberArk ウェブコンソールにログインするためのユーザー名。これは、PVWA REST API に認証したり、アカウント情報を一括収集したりする際に使用されます。	○
CyberArk PVWA ウェブ UI ログインパスワード	CyberArk ウェブコンソールにログインするためのユーザー名のパスワード。これは、PVWA REST API に認証したり、アカウント情報を一括収集したりする際に使用されます。	○
CyberArk プラットフォーム検索文字列	アカウント情報を一括収集するために PVWA REST API クエリパラメーターで使用される文字列。たとえば、`UnixSSH Admin TestSafe` と入力すると、`TestSafe` というセーフにある、ユーザー名 `Admin` を含むすべての Windows プラットフォームのアカウントを収集できます。 **注意:** これは完全一致ではないキーワード検索です。精度を向上させるために、CyberArk でカスタムプラットフォーム名を作成し、このフィールドにその値を入力することをお勧めします。	○
Use SSL (SSL を使用する)	有効にすると、スキャナーは安全な通信のために IIS を介して SSL を使用します。CyberArk が IIS を通して SSL をサポートするよう設定されている場合、このオプションを有効にします。	○
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、スキャナーは SSL 証明書を検証します。CyberArk が IIS を通して SSL をサポートするように設定されており、証明書を検証する場合、このオプションを有効にします。	×

CyberArk (レガシー) (Nessus Manager のみ)

ヒント: CyberArk の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

CyberArk は、権限付き認証情報の管理に使用できる一般的なエンタープライズパスワードボールトです。Nessus Manager は、CyberArk から認証情報を取得してスキャンに使用します。

オプション	説明
Username (ユーザー名)	ターゲットシステムのユーザー名。
CyberArk AIM Service URL (CyberArk AIM サービス URL)	AIM サービスの URL。デフォルトでは、この設定は `/AIMWebservice/v1.1/AIM.asmx` を使用します。
Central Credential Provider Host (Central Credential Provider ホスト)	CyberArk Central Credential Provider の IP/DNS アドレス。
Central Credential Provider Port (Central Credential Provider ポート)	CyberArk Central Credential Provider がリッスンするポート。
Central Credential Provider Username (Central Credential Provider ユーザー名)	CyberArk Central Credential Provider が基本認証を使用するように設定されている場合は、この設定に入力して認証できます。
Central Credential Provider Password (Central Credential Provider パスワード)	CyberArk Central Credential Provider が基本認証を使用するように設定されている場合は、この設定に入力して認証できます。
Safe (セーフ)	取得する認証情報が格納されていた CyberArk Central Credential Provider サーバー上の金庫。
CyberArk Client Certificate (CyberArk Client 証明書)	CyberArk ホストとの通信に使用される PEM 証明書を含むファイル。
CyberArk Client Certificate Private Key (CyberArk Client Certificate 秘密鍵)	クライアント証明書の PEM 秘密鍵を含むファイル。
CyberArk Client Certificate Private Key Passphrase (CyberArk Client	秘密鍵のパスフレーズ (必要な場合)。

オプション	説明
Certificate 秘密鍵のパスフレーズ)	
AppId	CyberArk Central Credential Provider でターゲットパスワードを取得するためのアクセス許可を割り当てられたAppId。
Folder (フォルダー)	取得する認証情報が格納されている CyberArk Central Credential Provider サーバー上のフォルダー。
PolicyId	CyberArk Central Credential Provider から取得する認証情報に割り当てられたポリシー ID です。
Use SSL (SSL を使用する)	CyberArk Central Credential Provider が安全な通信のために IIS チェックによって SSL をサポートするように設定されている場合。
Verify SSL Certificate (SSL 証明書を検証する)	CyberArk Central Credential Provider が IIS 経由で SSL をサポートするように設定されていて、その証明書を検証する場合は、これを有効にします。自己署名証明書の使用方法については、custom_CA.inc ドキュメントを参照してください。
CyberArk Account Details Name (CyberArk Account Details 名前)	CyberArk から取得する認証情報の一意の名前

ヒント: Delinea の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグイン を参照してください。

オプション	説明	必須
Delinea 認証方式	認証に、認証情報と API キーのどちらを使用するかを示します。デフォルトでは、**[認証情報]** が選択されています。	○
Delinea Login Name (Delinea ログイン名)	Delinea サーバーに認証されるときに使用するユーザー名。	○

Delinea Password (Delinea パスワード)	Delinea サーバーに認証されるときに使用するパスワード。これは、指定した Delinea Login Name に関連付けられているものです。	○
Delinea API キー	Secret Server ユーザーインターフェースで生成された API キー。この設定は、**[API キー]** の認証方法を選択した場合に必須です。	○
Delinea Secret Name (Delinea シークレット名)	Delinea サーバーのシークレットの値。シークレットには、Delinea サーバーで**シークレット名**のラベルが付けられています。	○
Delinea Host (Delinea ホスト)	API リクエストに使用する Delinea シークレットサーバー IP アドレス。	○
Delinea Port (Delinea ポート)	API リクエスト用の Delinea Secret Server ポート。Tenable はデフォルトで 443 を使用します。	○
Checkout Duration (チェックアウト期間)	Tenable が Delinea からパスワードをチェックアウトする期間。期間は時間単位で、スキャン時間より長くしてください。	○
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Windows ターゲットにログインします。	×
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストがユーザーにセッションチケットを提供します。	○
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。Tenable はデフォルトで 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート	×

	88 または 750 を使用するため、ポートも変更する必要があります。	
Domain (ドメイン)	(Kerberos ターゲット認証が有効な場合は必須) この Kerberos ドメインは、通常ターゲットのドメイン名として記載されている認証ドメインです。	○
Use SSL (SSL を使用する)	Delinea Secret Server が SSL をサポートするように設定されている場合は有効にします。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Delinea サーバーで SSL 証明書を検証します。	×

Delinea Secret Server 自動検出

ヒント: Delinea の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
Delinea Host (Delinea ホスト)	Delinea Secret Server ホスト。ここからシークレットをプルします。	○
Delinea ポート	API リクエスト用の Delinea Secret Server ポート。Tenable はデフォルトで 443 を使用します。	○
Delinea Authentication Method (Delinea 認証方式)	認証に、認証情報と API キーのどちらを使用するかを示します。デフォルトでは、**[認証情報]** が選択されています。	○
Delinea Login Name (Delinea ログイン名)	Delinea サーバーに認証されるときに使用するユーザー名。	○
Delinea Password	Delinea サーバーに認証されるときに使用するパスワード。これは、指定した Delinea ログイン名に関連付けられているものです。	○

オプション	説明	必須
(Delinea パスワード)		
Delinea API Key (Delinea API キー)	Secret Server ユーザーインターフェースで生成された API キー。この設定は、API キーの認証方式を選択した場合に必須です。	○
Query Mode (クエリモード)	事前設定されたフィールドを使用するか、URL クエリパラメーターの文字列を構築してアカウントにクエリを実行するかを選択します。デフォルトでは、**[シンプル]** が選択されています。	○
Folder ID (フォルダー ID)	指定されたフォルダー ID でアカウントにクエリを実行します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Search Text (検索テキスト)	指定された検索テキストに一致するアカウントにクエリを実行します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Search Field (検索フィールド)	指定された検索テキストを使用して検索するフィールド。指定しない場合、クエリは `name` フィールドを検索します。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Exact Match (完全一致)	検索テキストと完全一致を実行します。デフォルトでは、これは選択されていません。このオプションは、クエリモードが **[シンプル]** に設定されている場合にのみ使用できます。	×
Query String (クエリ文字列)	URL クエリパラメーターの文字列を指定します。このオプションは、クエリモードが **[高度]** に設定されている場合にのみ使用でき、この場合は必須です。	○
Use Private Key (秘密鍵を使用する)	パスワード認証ではなく鍵ベースの認証を使用して SSH 接続を行います。	×
Use SSL (SSL を使用する)	安全な通信のために SSL を使用します。	○

オプション	説明	必須
Verify SSL Certificate (SSL 証明書を検証する)	Delinea Secret Server SSL 証明書を検証します。	×

Kerberos

オプション	デフォルト	説明
Password (パスワード)	なし	他の認証情報メソッドと同様に、これはターゲットシステムのユーザーパスワードです。これは必須の設定です。
Key Distribution Center (KDC) (キー配布センター (KDC))	なし	このホストは、ユーザーのセッションチケットを提供します。これは必須の設定です。
KDC Port (KDC ポート)	88	この設定を行うと、88 以外のポートで稼働している KDC に Nessus を接続させることができます。
KDC Transport	TCP	KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。
Domain (ドメイン)	なし	KDC が管理する Windows ドメイン。これは必須の設定です。

LM ハッシュ

オプション	説明
Username (ユーザー名)	ターゲットシステムのユーザー名。
Hash (ハッシュ)	使用するハッシュ。
Domain (ドメイン)	指定されたユーザーの名前の Windows ドメイン。

NTLM ハッシュ

オプション	説明
Username (ユーザー名)	ターゲットシステムのユーザー名。
Hash (ハッシュ)	使用するハッシュ。
Domain (ドメイン)	指定されたユーザーの名前の Windows ドメイン。

QiAnXin

ヒント: QiAnXin の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
QiAnXin Host (QiAnXin ホスト)	QiAnXin ホストの IP アドレスまたは URL。	○
QiAnXin Port (QiAnXin ポート)	QiAnXin API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○
QiAnXin API Client ID (QiAnXin API クライアント ID)	QiAnXin PAM で作成された埋め込みアカウントアプリケーションのクライアント ID。	○
QiAnXin API Secret ID (QiAnXin API 秘密 ID)	QiAnXin PAM で作成された埋め込みアカウントアプリケーションの秘密 ID。	○
Domain (ドメイン)	ユーザー名が属するドメイン	×
Username (ユーザー名)	スキャンするホストにログインするためのユーザー名	○
Host IP (ホスト IP)	使用するアカウントを含む資産のホスト IP を指定します。指定しない場合、スキャンターゲット IP が使用されます。	×

オプション	説明	必須
Platform (プラットフォーム)	使用するアカウントを含む資産のプラットフォーム (資産タイプに基づく) を指定します。指定しない場合、認証情報のタイプに基づいてデフォルトのターゲットが使用されます (たとえば、Windows 認証情報の場合、デフォルトは WINDOWS です)。可能な値は次のとおりです。 • **ACTIVE_DIRECTORY** - Windows ドメインアカウント • **WINDOWS** - Windows ローカルアカウント • **LINUX** - Linux アカウント • **SQL_SERVER** - SQL Server データベース • **ORACLE** - Oracle データベース • **MYSQL** - MySQL データベース • **DB2** - DB2 データベース • **HP_UNIX** - HP Unix • **SOLARIS** - Solaris • **OPENLDAP** - OpenLDAP • **POSTGRESQL** - PostgreSQL	×
Region ID (リージョン ID)	使用するアカウントを含む資産のリージョン ID を指定します。	複数のリージョンを使用している場合のみ。
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Windows ターゲットにログインします。	×

オプション	説明	必須
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストがユーザーにセッションチケットを提供します。	○
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。Tenable はデフォルトで 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。	×
Domain (ドメイン)	(Kerberos ターゲット認証が有効な場合は必須) この Kerberos ドメインは、通常ターゲットのドメイン名として記載されている認証ドメインです。	○
Use SSL (SSL を使用する)	有効にすると、Tenable は安全な通信のために SSL を使用します。このオプションはデフォルトで有効です。	×
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable は、サーバーの SSL 証明書が信頼できる認証局によって署名されたものかどうかを検証します。	×

Senhasegura

ヒント: Senhasegura の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
Senhasegura Host (Senhasegura ホスト)	Senhasegura ホストの IP アドレスまたは URL です。	○
Senhasegura Port (Senhasegura ポート)	Senhasegura API が通信に使用するポートです。Tenable はデフォルトで 443 を使用します。	○

オプション	説明	必須
Senhasegura API Client ID (Senhasegura API クライアント ID)	Oauth 2.0 API 認証に適用される Senhasegura A2A アプリケーションのクライアント ID です。	○
Senhasegura API Secret ID (Senhasegura API のシークレット ID)	Oauth 2.0 API 認証に適用される Senhasegura A2A アプリケーションのシークレット ID です。	○
Domain (ドメイン)	ユーザー名が属するドメイン	×
Senhasegura Credential ID or Identifier (Senhasegura 認証情報 ID または識別子)	取得をリクエストしている認証情報の認証情報 ID または識別子です。	○
Private Key File (秘密鍵ファイル)	A2A からの暗号化された機密データを復号するために使用される秘密鍵です。 **注意:** A2A アプリケーション認証で機密データの暗号化を有効にできます。有効にした場合、ユーザーはスキャン認証情報に秘密鍵ファイルを指定する必要があります。これは、Senhasegura の該当する A2A アプリケーションからダウンロードできます。	A2A アプリケーション認証で機密データの暗号化を有効にした場合には必須です。
HTTPS	このオプションはデフォルトで有効です。	○
Verify SSL Certificate (SSL 証明書を検証する)	これはデフォルトでは無効になっています。	×

Thycotic Secret Server (Tenable Nessus Manager のみ)

オプション	デフォルト値
Username (ユーザー名)	(必須) ターゲットシステムのユーザーのユーザー名。
Domain (ドメイン)	Thycotic サーバーで設定されている場合、ユーザー名のドメイン。
Thycotic Secret Name (Thycotic シークレット名)	(必須) Thycoticサーバーのシークレット名の値。
Thycotic Secret Server URL (Thycotic シークレットサーバー URL)	(必須) スキャナーの転送方法、ターゲット、ターゲットディレクトリを設定するときに Tenable Nessus が使用する値。この値は、Thycotic サーバーの **[Admin] (管理者) > [Configuration] (設定) > [Application Settings] (アプリケーション設定) > [Secret Server URL]** (シークレットサーバー URL) にあります。 たとえば、*https://pw.mydomain.com/SecretServer* と入力した場合、Tenable Nessus はこれが SSL 接続であり、*pw.mydomain.com* がターゲットアドレス、*/SecretServer* はルートディレクトリであると判断します。
Thycotic Login Name (Thycotic ログイン名)	(必須) Thycotic サーバーのユーザーのユーザー名。
Thycotic Password (Thycotic パスワード)	(必須) 指定した **Thycotic ログイン名** に関連付けられたパスワード。
Thycotic Organization (Thycotic 企業)	Thycotic のクラウドインスタンスで、Tenable Nessus クエリがターゲットにする必要がある企業を識別する値。
Thycotic Domain (Thycotic ドメイン)	ドメイン (Thycotic サーバーに設定されている場合)。

オプション	デフォルト値
Private Key (プライベートキー)	有効にすると、Tenable Nessus はパスワード認証ではなく鍵ベースの認証で SSH 接続を行います。
Verify SSL Certificate (SSL 証明書を検証する)	有効にすると、Tenable Nessus は Thycotic サーバーの SSL 証明書を検証します。 自己署名証明書の使用の詳細については、カスタム SSL サーバー証明書を参照してください。

Windows LAPS

オプション	説明	必須
LAPS ホストアドレス	Active Directory をホストし、LAPS を管理するドメインコントローラーの IP アドレス。	○
LAPS ホストポート	LAPS ホストとの通信に使用されるポート。デフォルトのポートは 445 です。	×
Username (ユーザー名)	Active Directory から Windows LAPS 認証情報を取得するアクセス許可を持つアカウントのユーザー名。	○
Password (パスワード)	[ユーザー名] フィールドで指定されたアカウントのパスワード。	○
LAPS ドメイン	LAPS 管理対象デバイスが存在するドメイン。	○
LAPS OU	LAPS 管理対象デバイスを含む組織単位 (OU) の識別名 (DN)。	○

BeyondTrust (Tenable Nessus Manager のみ)

ヒント: BeyondTrust の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	デフォルト値
Username (ユー	(必須) スキャンするホストにログインするためのユーザー名です。

オプション	デフォルト値
ザー名)	
Domain (ドメイン)	BeyondTrust で必要な場合、ユーザー名のドメイン。
BeyondTrust host (BeyondTrust ホスト)	(必須) BeyondTrust IP アドレスまたは DNS アドレスです。
BeyondTrust port (BeyondTrust ポート)	(必須) BeyondTrust がリッスンしているポートです。
BeyondTrust API key (BeyondTrust API キー)	(必須) BeyondTrust が提供する API キーです。
Checkout duration (チェックアウト期間)	(必須) BeyondTrust で認証情報のチェックアウト状態を保持する時間 (分) です。チェックアウトの期間は、Nessus における通常のスキャン期間を超えるように設定します。新しいスキャンが開始したときに過去のスキャンのパスワードがまだチェックアウトされている場合、新しいスキャンは失敗します。 **注意**：BeyondTrust でパスワードの変更間隔を設定し、パスワード変更によって Nessus スキャンが中断されないようにします。スキャン中に BeyondTrust がパスワードを変更すると、スキャンは失敗します。
Use SSL (SSL を使用する)	有効にすると、Nessus は安全な通信のために IIS を介して SSL を使用します。このオプションを有効にするには、BeyondTrust で IIS を使用して SSL を設定する必要があります。
Verify SSL certificate (SSL 証明書の検証)	有効にすると、Nessus は SSL 証明書を検証します。このオプションを有効にするには、BeyondTrust で IIS を使用して SSL を設定する必要があります。
Use private key (プライベートキー	有効にすると、Nessus はパスワード認証ではなく秘密鍵ベースの認証で SSH 接続を行います。失敗した場合は、パスワードが要求されます。

オプション	デフォルト値
の使用)	
Use privilege escalation (権限昇格の使用)	有効にすると、BeyondTrust は設定された権限昇格コマンドを使用します。コマンドから何かが返された場合は、それをスキャンに使用します。

Lieberman (Tenable Nessus Manager のみ)

オプション	説明	必須
Username (ユーザー名)	ターゲットシステムのユーザー名。	○
Domain (ドメイン)	ドメイン (ユーザー名がドメインの一部である場合)	×
Lieberman host (Lieberman ホスト)	Lieberman の IP/DNS アドレス。 **注意:** Lieberman インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパス*の形式で入力します。	○
Lieberman port (Lieberman ポート)	Lieberman がリッスンするポート。	○
Lieberman API URL	Tenable Nessus が Lieberman へのアクセスに使用する URL。	×
Lieberman user (Lieberman ユーザー)	Lieberman RED API への認証に使用される Lieberman 明示ユーザーです。	○
Lieberman password (Lieberman パスワード)	Lieberman 明示ユーザーのパスワード。	○
Lieberman Authenticator (Lieberman 認証)	Lieberman のオーセンティケーターに使用されるエイリアス。この名前は Lieberman で使用される名前に一致する必要があります。 **注意:** このオプションを使用する場合は、**[Lieberman ユー**	×

オプション	説明	必須
	ザー] オプションにドメインを追加してください (例: *domain\user*)。	
Lieberman Client Certificate (Lieberman クライアント証明書)	Lieberman ホストとの通信に使用される PEM 証明書を含むファイル。 **注意:** このオプションを使用する場合は、**[Lieberman ユーザー]**、**[Lieberman パスワード]**、**[Lieberman 認証]** の各フィールドに情報を入力する必要はありません。	×
Lieberman Client Certificate Private Key (Lieberman クライアント証明書のプライベートキー)	クライアント証明書の PEM プライベートキーを含むファイル。	×
Lieberman Client Certificate Private Key Passphrase (Lieberman クライアント証明書の秘密鍵パスフレーズ)	プライベートキーのパスフレーズ (必要な場合)。	×
Use SSL (SSL を使用する)	Lieberman が安全な通信のために IIS チェックによって SSL をサポートするように設定されている場合。	×
Verify SSL Certificate (SSL 証明書の検証)	Lieberman が IIS 経由で SSL をサポートするように設定されていて、その証明書を検証する場合は、これを有効にします。自己署名証明書の使用方法については、custom_CA.inc ドキュメントを参照してください。	×
System Name (システム名)	まれなケースではあるものの、お客様の企業がすべての管理対象システムにデフォルトの Lieberman エントリを 1 つ使用している場合は、デフォルトのエントリ名を入力します。	×

Wallix Bastion (Tenable Nessus Manager のみ)

ヒント: Wallix Bastion の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
WALLIX Host (Delinea ホスト)	WALLIX Bastion ホストの IP アドレス。	○
WALLIX ポート	WALLIX Bastion API が通信に使用するポート。Tenable はデフォルトで 443 を使用します。	○
Authentication Type (認証タイプ)	**[Basic]** (基本) 認証 (WALLIX Bastion ユーザーインターフェースのユーザー名とパスワードが必要) または **[API Key]** (API キー) 認証 (ユーザー名と WALLIX Bastion 生成の API キーが必要)。	×
WALLIX ユーザー	WALLIX Bastion ユーザーインターフェースのログインユーザー名。	○
WALLIX Password (Delinea パスワード)	WALLIX Bastion ユーザーインターフェースのログインパスワード。API への **[Basic]** (基本) 認証に使用されます。	○
WALLIX API キー	WALLIX Bastion ユーザーインターフェースで生成された API キー。API への **[API Key]** (API キー) 認証に使用されます。	○
Get Credential by Device Account Name (デバイスアカウント名で認証情報を取得する)	ターゲットシステムへのログインに使用する**デバイス**が関連付けられているアカウント名。 **注意:** デバイスに複数のアカウントがある場合、認証情報を取得するアカウントの特定のデバイス名を入力する必要があります。入力しないと、システムから誤ったアカウントの認証情報が返される可能性があります。	複数のアカウントがあるターゲットやデバイスを使用している場合にのみ必要です。
HTTPS	これはデフォルトで有効です。	○

オプション	説明	必須
	注意: HTTPS を無効にすると、統合が失敗します。	
Verify SSL Certificate (SSL 証明書を検証する)	これはデフォルトで無効になっており、WALLIX Bastion PAM 統合ではサポートされていません。	×
Elevate Privileges with (権限昇格方法)	これにより、WALLIX Bastion 特権アクセス管理 (PAM) が有効になります。ドロップダウンメニューを使用して、Elevate Privileges with (権限昇格方法)を選択します。この機能をバイパスするには、このフィールドを **[Nothing]** (なし) に設定されたままにします。 **警告:** PAM を有効にするには、WALLIX Bastion アカウントで、WALLIX Bastion スーパー管理者がアカウントの「認証情報回復」を有効にしている必要があります。有効にしないと、スキャンから結果が返されない可能性があります。詳細は、WALLIX Bastion ドキュメントを参照してください。 **注意:** *su*、*su+sudo*、*sudo* など、複数の権限昇格オプションがサポートされています。たとえば **sudo** を選択すると、**[sudo user]** (sudo ユーザー)、**[Escalation Account Name]** (昇格アカウント名)、**[Location of su and sudo]** (su と sudo の場所) のフィールドが追加で表示され、これらのフィールドに入力することで WALLIX Bastion PAM による認証と権限昇格をサポートできます。権限昇格を完了するには、**[Escalation Account Name]** (エスカレーションアカウント名) フィールドに入力する必要があります。 **注意:** サポートされている権限昇格タイプと各タイプに伴うフィールドの詳細については、Tenable Nessus ユーザーガイドを参照してください。	権限昇格を行う場合に必要です。
Database Port (データベースのポート)	通信に対して Oracle データベースインスタンスがリッスンする TCP ポート。デフォルトはポート 1521 です。	×

オプション	説明	必須
Auth Type (認証方法)	データベースインスタンスにアクセスするために Tenable が使用するアカウントの種類。 • **SYSDBA** • **SYSOPER** • **NORMAL**	×
Service Type (サービスの種類)	データベースインスタンスを指定するために使用する Oracle パラメーター: **SID** または **SERVICE_NAME**	×
Service (サービス)	データベースインスタンスの SID 値または SERVICE_NAME 値。 入力する **[Service]** (サービス) 値は、**[Service Type]** (サービスタイプ) オプションのパラメーターとして選択した値と一致する必要があります。	○
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	×

HashiCorp Vault (Tenable Nessus Manager のみ)

ヒント: HashiCorp の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Windows と SSH の認証情報		
オプション	**説明**	**必須**
Hashicorp Vault host (Hashicorp Vault ホスト)	Hashicorp Vault IP アドレスまたは DNS アドレス。 **注意:** Hashicorp Vault インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパス*の形式で入力します。	○
Hashicorp Vault port (Hashicorp Vault ポート)	Hashicorp Vault がリッスンするポート。	○
Authentication Type (認証タイプ)	インスタンスに接続するための認証タイプとして、**[App Role]** (アプリロール) または **[Certificates]** (証明書) を指定します。 **[証明書]** を選択すると、**[Hashicorp Client Certificate]** (Hashicorp クライアント証明書) (必須) および **[Hashicorp Client Certificate Private Key]** (Hashicorp クライアント証明書の秘密鍵) (必須) の追加オプションが表示されます。クライアント証明書と秘密鍵にそれぞれ適切なファイルを選択してください。	○
Role ID (ロール ID)	App Role を構成したときに Hashicorp Vault によって提供される GUID です。	○
Role Secret ID (ロールシークレット名)	App Role を構成したときに Hashicorp Vault によって生成される GUID です。	○
Authentication URL (認証 URL)	認証エンドポイントへのパス/サブディレクトリ。This is not the full URL. (これは完全な URL ではありません。)たとえば、	○

	`/v1/auth/approle/login`	
Namespace (名前空間)	マルチチーム環境で指定されたチームの名前	×
Vault Type (Vault タイプ)	Tenable Nessus バージョン: KV1、KV2、AD、LDAP。Tenable Nessus バージョンの詳細については、Tenable Nessus のドキュメントを参照してください。	○
KV1 Engine URL (KV1 エンジン URL)	(KV1) Tenable Nessus が KV1 エンジンへのアクセスに使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (KV1 **Vault タイプ**を選択した場合)
KV2 Engine URL (KV2 エンジン URL)	(KV2) Tenable Nessus が KV2 エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (KV2 **Vault タイプ**を選択した場合)
AD Engine URL (AD エンジン URL)	(AD) Tenable Nessus が Active Directory エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (AD **Vault タイプ**を選択した場合)
LDAP Engine URL (LDAP エンジン URL)	(LDAP) Tenable Nessus が LDAP エンジンにアクセスするために使用する URL です。 例: `/v1/path_to_secret`。末尾の / なし	○ (LDAP **Vault タイプ**を選択した場合)
Username Source (ユーザー名ソース)	(KV1 および KV2) ユーザー名が手動で入力されるか、Hashicorp Vault からプルするかを指定するドロップダウンボックスです。	○
Username Key (ユーザー名鍵)	(KV1 および KV2) ユーザー名が格納されている Hashicorp Vault での名前です。	○
Password Key (パスワード鍵)	(KV1 および KV2) パスワードが格納されている Hashicorp Vault での鍵です。	○

Domain Key (Windows) (ドメイン鍵 (Windows))	(Kerberos ターゲット認証が有効な場合は必須。) ドメインが保存される秘密鍵の名前です。	○
Secret Name (秘密名)	(KV1、KV2、AD) 値を取得したい鍵秘密です。	○
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。	×
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須。) このホストは、ユーザーにセッションチケットを提供します。	○
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。デフォルトでは、Tenable は 88 を使用します。	×
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。	×
Domain (Windows) (ドメイン (Windows))	(Kerberos ターゲット認証が有効な場合は必須。) Kerberos ターゲット認証が属するドメイン (該当する場合)。	○
Realm (SSH) (領域 (SSH))	(Kerberos ターゲット認証が有効な場合は必須。) Realm は、通常標的のドメイン名として記録されている認証ドメインです (例: example.com)。	○
Use SSL (SSL を使用する)	有効にすると、Tenable Nessus Manager は安全な通信のために SSL を使用します。このオプションを有効にする前に、Hashicorp Vault で SSL を設定してください。	×
Verify SSL Certificate	有効にすると、Tenable Nessus Manager は SSL 証明	×

(SSL 証明書の検証)	書を検証します。このオプションを有効にする前に、Hashicorp Vault で SSL を設定してください。	
Tenable Nessus に対して有効にする	Tenable Nessus での IBM DataPower Gateway の使用を有効または無効にします。	○
Elevate Privileges with (SSH) (権限昇格方法 (SSH))	スキャンの実行時に追加の権限を使用するには、su や sudo などの権限昇格手法を使用します。 **注意:** Tenable では、権限昇格のために su、su+sudo、sudo などの複数のオプションを使用できます。たとえば sudo を選択すると、sudo ユーザー、昇格アカウントの秘密名、sudo の場所 (ディレクトリ) のフィールドが追加で表示され、これらのフィールドに入力することで Tenable Nessus による認証と権限昇格をサポートできます。 **注意:** サポートされている権限昇格タイプと各タイプに伴うフィールドの詳細については、Nessus ユーザーガイドおよび Tenable Vulnerability Management ユーザーガイドを参照してください。	権限昇格を行う場合は必須です。
Escalation account secret name (SSH) (昇格アカウントシークレット名 (SSH))	昇格アカウントのユーザー名またはパスワードが最小権限ユーザーと異なる場合、昇格アカウント認証情報の認証情報 ID または識別子をここに入力します。	×
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に	×

	使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。	

Centrify (Tenable Nessus Manager のみ)

オプション	デフォルト値
Centrify Host (Centrify ホスト)	(必須) Centrify IP アドレスまたは DNS アドレスです。 **注意:** Centrify インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名 / サブディレクトリパスの形式で入力します。*
Centrify Port (Centrify ポート)	Centrify がリッスンするポート。
API User (API ユーザー)	(必須) Centrify が提供する API ユーザー
API Key (API キー)	(必須) Centrify が提供する API キー。
Tenant (テナント)	マルチチーム環境で指定されたチームの名前です。
Authentication URL (認証 URL)	Tenable Nessus Manager が Centrify へのアクセスに使用する URL。
Password Engine URL (パスワードエンジン URL)	マルチチーム環境で指定されたチームの名前です。
Username (ユーザー名)	(必須) スキャンするホストにログインするためのユーザー名。
Checkout duration (チェックアウト期間)	Centrify で認証情報のチェックアウト状態を保持する時間 (分)。 **チェックアウトの期間**は、Tenable Nessus Manager における通常のスキャン期間を超えるように設定します。新しいスキャンが開始したときに過去のスキャンのパスワードがまだチェックアウトされている場合、新しいスキャンは失敗

オプション	デフォルト値
	します。 **注意**：Centrify でパスワードの変更間隔を設定し、パスワード変更によって Tenable Nessus Manager スキャンが中断されないようにします。スキャン中に Centrify がパスワードを変更すると、スキャンは失敗します。
Use SSL (SSL を使用する)	有効にすると、Tenable Nessus Manager は安全な通信のために IIS を介して SSL を使用します。このオプションを有効にするには、Centrify で IIS を使用して SSL を設定する必要があります。
Verify SSL (SSL を検証する)	有効にすると、Tenable Nessus Manager は SSL 証明書を検証します。このオプションを有効にするには、Centrify で IIS を使用して SSL を設定する必要があります。
Targets to Prioritize Credentials (認証情報を優先するターゲット)	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。 この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

Arcon (Tenable Nessus Manager のみ)

ヒント：Arcon の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	デフォルト値
Arcon host (Arcon のホスト)	(必須) Arcon IP アドレスまたは DNS アドレスです。

オプション	デフォルト値
	注意: Arcon インストールがサブディレクトリにある場合は、サブディレクトリパスを含める必要があります。たとえば、*IP アドレスまたはホスト名/サブディレクトリパスの形式で入力します。*
Arcon port (Arcon ポート)	Arcon がリッスンするポート。
API User (API ユーザー)	(必須) Arcon が提供するAPIユーザーです。
API Key (API キー)	(必須) Arcon が提供するAPIキーです。
Authentication URL (認証 URL)	Tenable Nessus Manager が Arcon へのアクセスに使用する URL。
Password Engine URL (パスワードエンジン URL)	Tenable Nessus Manager が Arcon のパスワードへのアクセスに使用する URL。
Username (ユーザー名)	(必須) スキャンするホストにログインするためのユーザー名。
Arcon Target Type (Arcon ターゲットタイプ)	(オプション) ターゲットタイプの名前。お使いの Arcon PAM のバージョンと SSH 認証情報を作成したシステムのタイプにより異なりますが、デフォルトでは **linux** に設定されます。正しいターゲットタイプ値を知るためのターゲットタイプ/システムタイプのマッピングは、Arcon PAM 仕様ドキュメント (Arcon 提供) を参照してください。
Checkout Duration (チェックアウト期間)	(必須) Arcon で認証情報のチェックアウト状態を保持する時間 (時間)です。 **チェックアウトの期間** は、Tenable Vulnerability Management における通常のスキャン期間を超えるように設定します。新しいスキャンが開始したときに過去のスキャンのパスワードがまだチェックアウトされている場合、新しいスキャンは失敗します。

オプション	デフォルト値
	注意：Arcon でパスワードの変更間隔を設定し、パスワード変更によって Tenable Vulnerability Management スキャンが中断されないようにします。スキャン中に Arcon がパスワードを変更すると、スキャンは失敗します。
Kerberos Target Authentication (Kerberos ターゲット認証)	有効にした場合、Kerberos 認証を使用して、指定された Linux または Unix ターゲットにログインします。
Key Distribution Center (KDC) (キー配布センター (KDC))	(Kerberos ターゲット認証が有効な場合は必須) このホストがユーザーにセッションチケットを提供します。
KDC Port (KDC ポート)	Kerberos 認証 API が通信するポート。Tenable はデフォルトで 88 を使用します。
KDC Transport	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、このオプションを変更します。KDC Transport の値を変更する必要がある場合、KDC UDP は実装に応じてデフォルトでポート 88 または 750 を使用するため、ポートも変更する必要があります。
Realm (領域)	(Kerberos ターゲット認証が有効な場合は必須) 領域とは認証ドメインのことです。通常、ターゲットのドメイン名として記載されています。
Use SSL (SSL を使用する)	有効にすると、Tenable Nessus Manager は安全な通信のために IIS を介して SSL を使用します。このオプションを有効にするには、Arcon で IIS を使用して SSL を設定する必要があります。
Verify SSL (SSL を検証する)	有効にすると、Tenable Nessus Manager は SSL 証明書を検証します。このオプションを有効にするには、Arcon で IIS を使用して SSL を設定する必要があります。
Targets to Prioritize Credentials (認証	この認証情報を他の認証情報よりも先に試行する IP または CIDR ブロックを指定します。複数の IP または CIDR ブロックを指定する場合は、コンマまたはスペース区切りのリストを使用します。

オプション	デフォルト値
情報を優先するターゲット)	この設定を使用すると、選択したターゲットで成功する認証情報が優先されるため、スキャン時間を短縮できます。たとえば、スキャンで指定された 100 の認証情報のうち、59 番目の認証情報で認証に成功するとします。すると、最初の 58 の認証情報での認証が失敗するまで 59 番目の認証は行われません。**[認証情報を優先するターゲット]** を使用すると、成功した認証情報を最初に使用するようにスキャンを設定するので、スキャンがターゲットにより速くアクセスできます。

その他の認証情報

このセクションでは、**[Miscellaneous]** (その他) セクションで説明される情報と認証情報の設定について説明します。

ADSI

ADSI には、ドメインコントローラー情報、ドメイン、ドメイン管理者とパスワードが必要です。

ADSI を使用すると、Tenable Nessus は ActiveSync サーバーをクエリして、Android ベースまたは iOS ベースのデバイスが接続されているかどうかを判断できます。Tenable Nessus はドメインコントローラー (Exchange サーバーでなく) が直接デバイス情報をクエリできるように、認証情報とサーバー情報を使用してドメインコントローラーへのアクセスを認証します。これらの設定は、モバイルデバイスのスキャンに必要です。

Tenable Nessus は、Exchange Server 2010 および 2013 のみからのモバイル情報の取得をサポートしています。

オプション	説明	デフォルト
Domain Controller (ドメインコントローラー)	(必須) ActiveSync のドメインコントローラーの名前。	-
Domain (ドメイン)	(必須) ActiveSync の NetBIOS ドメインの名前。	-
Domain Admin (ドメイン管理者)	(必須) ドメイン管理者のユーザー名。	-

オプション	説明	デフォルト
Domain Password (ドメインパスワード)	(必須) ドメイン管理者のパスワード。	-

Nessus がモバイル情報を取得できるのは、Exchange Server 2010 と 2013 からのみです。Exchange Server 2007 から情報は読み取れません。

Cisco Meraki

オプション	説明	必須
Cisco Meraki API Host (Cisco Meraki API ホスト)	Cisco Meraki Dashboard API ホストのホスト名または IP アドレス。	○
Cisco Meraki API Port (Cisco Meraki API ポート)	Cisco Meraki Dashboard API のポート (デフォルトは 443)。	○
Cisco Meraki API Key (Cisco Meraki API キー)	Cisco Meraki API への認証に使われる API キー。	○
CIsco Meraki Organization Name (CIsco Meraki 組織名)	認証情報ごとに 1 つの組織を入力します。	○
CIsco Meraki Network Name (CIsco Meraki ネットワーク名)	1 つまたは複数のネットワーク名をコンマ区切りで入力します。	×
Cisco Meraki Product Type	1 つまたは複数の製品タイプをコンマ区切りで入力します。有効な製品タイプは、**appliance**、**camera**、**cellularGateway**、	×

オプション	説明	必須
(Cisco Meraki 製品タイプ)	**secureConnect**、**sensor**、**switch**、**systemManager**、**wireless**、**wirelessController**です。	
Cisco Meraki Tag (Cisco Meraki タグ)	組織内のデバイス検索のフィルターに使用される、1 つ以上のタグをコンマ区切りで入力します。	×
Cisco Meraki Device Name (Cisco Meraki デバイス名)	単一の Cisco Meraki デバイス名を入力します(例: Meraki MS120-8)。	×
Cisco Meraki Device Model (Cisco Meraki デバイスモデル)	1 つ以上の Cisco Meraki デバイスモデルをコンマ区切りで入力します(例:「MS120-8」)。	×
Device Serial Number (デバイスのシリアル番号)	1 つ以上のデバイスシリアル番号をコンマ区切りで入力します。	×
Device MAC Address (デバイス MAC アドレス)	1 つ以上のデバイス MAC アドレスをコンマ区切りで入力します。	×
Discover Devices (デバイスの検出)	検出された Cisco Meraki デバイスをスキャンのターゲットに追加します(デフォルトではオフ)。	×
HTTPS	オンに設定すると、フィールドが拡張し、**[カスタム CA が設定されている場合は SSL クライアント証明書を検証する]** を有効にするオプションが表示されます(デフォルトではオフ)。	×

F5

オプション	説明	デフォルト

Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、スキャン F5 のアカウントのユーザー名。	-
Password (パスワード)	(必須) F5 ユーザーのパスワード。	-
Port (ポート)	(必須) Tenable Nessus からの通信に対して F5 がリッスンする TCP ポート。	443
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable が標準の HTTP を使用して接続します。	有効
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	有効

IBM iSeries

オプション	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、IBM iSeries のアカウントのユーザー名。	-
Password (パスワード)	(必須) IBM iSeries ユーザーのパスワード。	-

NetApp API

オプション	説明	デフォルト
Username	(必須) Tenable Nessus がターゲットシステムのチェックを行うために使	-

(ユーザー名)	用する HTTPS アクセスの Netapp API アカウントのユーザー名。	
Password (パスワード)	(必須) Netapp API ユーザーのパスワード。	-
vFiler	ターゲットシステム上でスキャンする vFiler ノード。 監査を 1 つの vFiler に制限するには、vFiler の名前を入力します。 ターゲットシステム上で検出されたすべての Netapp 仮想ファイラー (vFilers) を監査する場合は、フィールドを空白にします。	-
Port (ポート)	(必須) Tenable Nessus からの通信に対して Netapp API がリッスンする TCP ポート。	443

Nutanix Prism

ヒント: Nutanix Prism の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグイン を参照してください。

オプション	説明	デフォルト
Nutanix Host (Nutanix ホスト)	(必須) Nutanix Prism Central ホストのホスト名または IP アドレス。	-
Nutanix Port (Nutanix ポート)	(必須) Tenable からの通信に対して Nutanix Prism Central ホストがリッスンする TCP ポート。	9440
Nutanix Prism Central Authentication Method (Nutanix Prism Central の認証方法)	(必須) ユーザーは認証方法のリストから選択できます。 • ユーザー名とパスワード (手動入力) • 特権アクセス管理 (PAM) の統合特定の PAM を使用して、利用可能なリストから vCenter API 認証情報を収集します。	ユーザー名とパスワード
Discover Hosts (ホストの検出)	有効にすると、Tenable は検出されたすべての	有効

オプション	説明	デフォルト
	Nutanix ホストをスキャンターゲットのリストに追加します。	
Discover Virtual Machines (仮想マシンの検出)	有効にすると、Tenable は検出されたすべての Nutanix 仮想マシンをスキャンターゲットのリストに追加します。	有効
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable が標準の HTTP を使用して接続します。	有効
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	Disabled (無効)

OpenStack

オプション	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、OpenStack のアカウントのユーザー名。	-
Password (パスワード)	(必須) OpenStack ユーザーのパスワード。	-
認証用のテナント名	(必須) スキャンが認証に使用する特定のテナントの名前。	admin
Port (ポート)	(必須) Tenable Nessus からの通信に対して OpenStack がリッスンする TCP ポート。	443
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。	有効

	無効にすると、Tenable が標準の HTTP を使用して接続します。	
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	有効

Palo Alto Networks PAN-OS

オプション	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、PAN-OS のアカウントのユーザー名。	-
Password (パスワード)	(必須) PAN-OS ユーザーのパスワード。	-
Port (ポート)	(必須) Tenable Nessus からの通信に対して PAN-OS がリッスンする TCP ポート。	443
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable が標準の HTTP を使用して接続します。	有効
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	有効

Red Hat Enterprise Virtualization (RHEV)

オプション	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、RHEV のアカウントのユーザー名。	-
Password (パスワード)	(必須) RHEV ユーザーのパスワード。	-
Port (ポート)	(必須) Tenable Nessus からの通信に対して RHEV サーバーがリッスンする TCP ポート。	443
Verify SSL Certificate (SSL 証明書を検証する)	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	有効

VMware ESX SOAP API

VMware サーバーにはネイティブの SOAP API を通じてアクセスできます。ESX と ESXi サーバーには、VMware ESX SOAP API でユーザー名とパスワードを使用してアクセスできます。また、SSL 証明書の検証を無効にすることも可能です。

VMWare ESX SOAP API の設定についての詳細は、vSphere スキャンの設定 を参照してください。

ヒント: ESXi SOAP API の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Tenable は、ネイティブな VMware SOAP API を通じて VMware サーバーにアクセスすることができます。

オプション	説明	デフォルト
ESX SOAP API Authentication Method (ESX SOAP API 認証方法)	(必須) ユーザーは認証方法のリストから選択できます。 • ユーザー名とパスワード (手動入力) • PAM の統合 (特定の PAM を使用して、利用可能なリストから vCenter API 認証	ユーザー名とパスワード

オプション	説明	デフォルト
	情報を収集します)	
Do not verify SSL Certificate (SSL 証明書を検証しない)	ESXi サーバーの SSL 証明書の有効性を検証しません。	disabled

VMware vCenter

VMWare vCenter SOAP API の設定についての詳細は、vSphere スキャンの設定 を参照してください。

ヒント: VMware vCenter の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Tenable は、ネイティブな VMware vCenter SOAP API を通じて vCenter にアクセスすることができます。利用可能な場合は、TenableはSOAP API に加えて vCenter REST API を使用してデータを収集します。

注意: Tenable は、認証スキャンには VMware vCenter/ESXi バージョン 7.0.3 以降の使用をサポートしています。VMware vCenter/ESXi の脆弱性チェックは認証を必要としないため、この制限による影響はありません。

注意: SOAP API を使用するには、読み取りのアクセス許可と設定権限を持つ vCenter アカウントが必要です。REST API を使用するには、一般的な読み取りのアクセス許可と、VIB を列挙するために必要な Lifecycle Manager 権限を持つ vCenter 管理者アカウントが必要です。

オプション	説明	デフォルト
vCenter Host (vCenter ホスト)	(必須) vCenter ホストの名前。	-
vCenter Port (vCenter ポート)	(必須) Tenable からの通信に対して vCenter がリッスンする TCP ポート。	443
Username (ユーザー名)	(必須) ターゲットシステムのチェックを実行するために Tenable が使用する、管理者の読み取り/書き込みアクセス権を持つ vCenter サーバーアカウントのユーザー名。	-
Password (パスワード)	(必須) vCenver サーバーユーザーのパスワード。	-

オプション	説明	デフォルト
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。無効にすると、Tenable が標準の HTTP を使用して接続します。	有効
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	有効
Auto Discover Managed VMware ESXi Hosts (管理対象の VMware ESXi ホストの自動検出)	このオプションは、検出された VMware ESXi ハイパーバイザーホストを、スキャンに含めるスキャンターゲットに追加します。	Disabled (無効)
Auto Discover Managed VMware ESXi Virtual Machines (管理対象の VMware ESXi 仮想マシンの自動検出)	このオプションは、検出された VMware ESXi ハイパーバイザー仮想ホストを、スキャンに含めるスキャンターゲットに追加します。	Disabled (無効)

X.509

オプション	説明	デフォルト
Client certificate (クライアント証明書)	(必須) クライアント証明書。	-
Client key (クライアントキー)	(必須) クライアントのプライベートキー。	-
Password for key (キーのパスワード)	(必須) クライアント秘密鍵のパスフレーズ。	-
CA certificate to trust (信頼できる CA 証明書)	(必須) 信頼できる認証局 (CA) のデジタル証明書。	-

モバイル認証情報

Tenable Nessus Manager では、パッチ管理システムの認証情報を利用して、認証情報を利用できない可能性のあるシステム上でパッチ監査を実行できます。

注意: パッチ管理統合は、Tenable Nessus Essentials、Tenable Nessus Professional、Tenable Nessus Expert、または管理された Tenable Nessus スキャナーでは利用できません。

ActiveSync

オプション	デフォルト	説明
Domain Controller (ドメインコントローラー)	--	ActiveSync のドメインコントローラー。
Domain (ドメイン)	--	ActiveSync の Windows ドメイン。
Domain Username (ドメインユーザー名)	--	ActiveSync への認証に Tenable Nessus が使用する、ドメイン管理者のアカウントのユーザー名。
Domain Password (ドメインパスワード)	--	ドメイン管理者ユーザーのパスワード。
スキャナー	--	サーバーのスキャン時に Tenable Nessus が使用するスキャナーを指定します。モバイルリポジトリにデータを追加するために Tenable Nessus が使用できるスキャナーは 1 つだけです。
Update Schedule (スケジュールの更新)	毎日 12:30～04:00	Tenable Nessus がサーバーをスキャンしてモバイルリポジトリを更新するタイミングを指定します。Tenable Nessus は、スキャンするたびにリポジトリの現在のデータを削除し、最新のスキャンのデータに置き換えます。

AirWatch

ヒント: AirWatch の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	デフォルト値	説明	必須
AirWatch Environment API URL	-	Workspace ONE API の URL エンドポイントです。(例: https://xxx.awmdm.com/api)	○
Ports (ポート)	443	Tenable からの通信に対して AirWatch がリッスンする TCP ポート。	○
Username (ユーザー名)	-	AirWatch ユーザーアカウントのユーザー名。Tenable は、Workspace One の API に対する認証に使用します。	○
Password (パスワード)	-	AirWatch ユーザーのパスワード。	○
API キー	-	VMware Workspace ONE API の API キー。	○
HTTPS	Enabled (有効)	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Nessus が認証できるようにします。	×
Verify SSL Certificate (SSL 証明書の検証)	Enabled (有効)	サーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを Tenable Nessus が検証できるようにします。	×

Blackberry UEM

ヒント: Blackberry UEM の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明
Hostname (ホスト名)	Blackberry UEM での認証用サーバー URL
Ports (ポート)	Blackberry UEM での認証に使用するポート

Tenant (テナント)	Blackberry UEM の SRP ID **注意:** Blackberry UEM で SRP ID を見つける方法 1. Blackberry UEM の上部ナビゲーションバーで、**[ヘルプ]** ドロップダウンをクリックします。 2. **[Blackberry UEM について]** をクリックします。 SRP ID を含む情報ウィンドウが表示されます。 3. SRP ID をコピーします。
Domain (ドメイン)	Blackberry UEM のドメイン名
Username (ユーザー名)	Blackberry UEM へのアクセスの認証用に Tenable Nessus で使用するアカウントのユーザー名。
Password (パスワード)	Blackberry UEM へのアクセスの認証用に Tenable Nessus で使用するアカウントのパスワード。
HTTPS	有効な場合、Tenable Nessus は Blackberry UEM での認証に暗号化された接続を使用します。
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable Nessus は、サーバーの SSL 証明書が信頼できる認証局によって署名されたものかどうかを検証します。

Intune

ヒント: Intune の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明
Tenant (テナント)	App 登録で表示される Microsoft Azure Directory (tenant) の ID
Client (クライアント)	App 登録中に作成される Microsoft Azure Application (client) の ID
Secret (秘密)	Microsoft Azure でクライアントの秘密鍵を作成した場合に作成される秘密鍵

Username (ユーザー名)	Tenable Nessus が Intune へのアクセスを認証するために使用するアカウントのユーザー名
Password (パスワード)	Intune へのアクセスの認証用に Tenable Nessus で使用するアカウントのパスワード。

Ivanti

(missing or bad snippet)

MaaS360

ヒント: MaaS360 の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
Username (ユーザー名)	認証するユーザー名	○
Password (パスワード)	認証するパスワード	○
Root URL (ルート URL)	MaaS360 での認証用サーバー URL	○
Platform ID (プラットフォーム ID)	MaaS360 用に提供されたプラットフォーム ID	○
Billing ID (請求 ID)	MaaS360 用に提供された請求 ID	○
App ID (アプリ ID)	MaaS360 用に提供されたアプリ ID	○
App Version (アプリのバージョン)	MaaS360 アプリのバージョン	○
App access key (アプリのアクセスキー)	MaaS360 用に提供されたアプリのアクセスキー	○
Collect All Device Data (すべてのデバイスデータの収集)	有効にすると、スキャンがすべてのデータタイプを収集します。 無効にすると、スキャンは 1 つ以上のタイプのデータを収集して、スキャン時間を短縮します。無効にした場	×

	合は、以下の収集オプションから1つ以上を選択してください。 • **Collect Device Summary** • **デバイスアプリケーションの収集** • **デバイスコンプライアンスの収集** • **Collect Device Policies**	

MobileIron

ヒント: MobileIronの認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に`integration_status.nasl`プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	説明	必須
VSP Admin Portal URL (VSP管理者ポータルURL)	Tenable NessusがMobileIron管理者ポータルへの接続認証に使用するサーバーURL。	○
VSP Admin Portal Port (VSP管理者ポータルポート)	Tenable NessusがMobileIron管理者ポータルへの認証に使用するポート (通常、ポート443または8443)。デフォルトではポートは443を想定しています。	×
Port (ポート)	Tenable NessusがMobileIronへの認証に使用するポート (通常、ポート443)。	×
Username (ユーザー名)	Tenable NessusがMobileIronへのアクセスを認証するために使用するアカウントのユーザー名。	○
Password (パスワード)	Tenable NessusがMobileIronへのアクセスを認証するために使用するアカウントのパスワード。	○
HTTPS	有効にすると、Tenable Nessusは暗号化接続を使用して、MobileIronに認証します。	×
Verify SSL Certificate (SSL証明書の検証)	有効にすると、Tenable Nessusは、サーバーのSSL証明書が信頼できる認証局によって署名されたもの	×

	かどうかを検証します。	

Workspace ONE

ヒント: Workspace ONE の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

オプション	デフォルト値	説明	必須
Workspace ONE Environment API URL (Workspace ONE 環境 API の URL)	-	Workspace ONE API の URL エンドポイントです。(例: https://xxx.awmdm.com/api)	○
Ports (ポート)	443	Tenable からの通信を Workspace ONE がリッスンするために使用する TCP ポート。	○
Workspace ONE Username (Workspace ONE ユーザー名)	-	Workspace ONE ユーザーアカウントのユーザー名。Tenable は、Workspace ONE の API に対する認証に使用します。	○
Workspace ONE Password (Workspace ONE パスワード)	-	Workspace ONE ユーザーのパスワード。	○
API キー	-	VMware Workspace ONE API の API キー。	○
HTTPS	Enabled (有効)	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Nessus が認証できるようにします。	×
Verify SSL Certificate (SSL 証明書の検証)	Enabled (有効)	サーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを Tenable Nessus が検証できるようにします。	×

		ヒント: 自己署名証明書を使用している場合は、この設定を無効にします。	
Collect All Device Data (すべてのデバイスデータの収集)	○	プラグインチェックに必要なすべてのデバイスデータを収集します。	×
Collect Device Applications (デバイスアプリケーションの収集)	○	([すべてのデバイスデータの収集] が [いいえ] に設定されている場合に有効) モバイルデバイスにインストールされているアプリケーションを収集します。	×

パッチ管理の認証情報

Tenable Nessus では、パッチ管理システムの認証情報を利用して、認証情報を利用できない可能性のあるシステム上でパッチ監査を実行できます。

注意: パッチ管理統合は、Tenable Nessus Essentials、Tenable Nessus Professional、Tenable Nessus Expert、または管理された Tenable Nessus スキャナーでは利用できません。

Tenable Nessus Manager は次をサポートします。

- Dell KACE K1000
- HCL BigFix
- Microsoft System Center Configuration Manager (SCCM)
- Microsoft Windows Server Update Services (WSUS)
- Red Hat Satellite サーバー
- Symantec Altiris

スキャンの作成で説明したように、スキャンの作成中に **[Credentials]** (認証情報) セクションでパッチ管理オプションを設定できます。

IT 管理者は、パッチ監視ソフトウェアを管理し、パッチ管理システムに必要なエージェントをシステムにインストールする必要があります。

注意: 認証情報チェックでシステムを検出したものの認証できない場合は、パッチ管理システムから取得されたデータを使用してチェックを実行します。Tenable Nessus がターゲットシステムに接続できる場合は、そのシステムに対するチェックを実行し、パッチ管理システムの出力を無視します。

注意: パッチ管理システムが Tenable Nessus に返すデータは、パッチ管理システムがその管理対象ホストから取得できた時点での最新のデータに過ぎません。

複数のパッチマネージャーを使用してスキャンする

Tenable Nessus に対して、パッチ管理ツール用の複数の認証情報セットを指定した場合、Tenable Nessus はそのすべてを使用します。

ホストに加えて 1 つ以上のパッチ管理システムの認証情報を指定した場合、Tenable Nessus はすべての方法による結果を比較したうえで不一致について報告するか、満足のいく結果を提供します。Patch Management Windows Auditing Conflicts プラグインを使用すると、ホストとパッチ管理システムのパッチデータの相違が浮き彫りになります。

Dell KACE K1000

Dell から提供されている KACE K1000 は、Linux、Windows、macOS の各システムの更新プログラムとホットフィックスの配布を管理します。Tenable Nessus は Tenable NessusHCL Bigfix にクエリを実行して、HCL Bigfix が管理しているシステムにパッチがインストールされているかどうかを検証し、そのパッチ情報を表示できます。

Tenable Nessus は KACE K1000 のバージョン 6.x 以前に対応しています。

KACE K1000 のスキャンでは、Tenable プラグインの 76867、76868、76866、76869 を使用します。

オプション	説明	デフォルト
Server (サーバー)	(必須) KACE K1000 の IP アドレスまたはシステム名。	-
Database Port (データベースのポート)	(必須) Tenable Nessus からの通信に対して KACE K1000 がリッスンする TCP ポート。	3306
Organization Database Name (企業のデータベース名)	(必須) KACE K1000 データベース用の企業コンポーネントの名前 (例: ORG1)。	ORG1
Database Username	(必須) ターゲットのシステムでチェックを実行するために	R1

オプション	説明	デフォルト
(データベースのユーザー名)	Tenable Nessus が使用する、KACE K1000 のアカウントのユーザー名。	
K1000 Database Password (K1000 データベースパスワード)	(必須) KACE K1000 ユーザーのパスワード。	-

HCL Tivoli Endpoint Manager (BigFix)

ヒント: HCL BigFix の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

HCL Bigfix は、デスクトップシステムの更新プログラムとホットフィックスの配布を管理するために提供されています。Tenable Nessus は、HCL Bigfix にクエリを実行して、HCL Bigfix が管理しているシステムにパッチがインストールされているかどうかを検証し、そのパッチ情報を表示できます。

パッケージレポーティングは、HCL Bigfix が公式にサポートする RPM ベースと Debian ベースの両方の配布でサポートされています。たとえば、Red Hat 系統の製品 (RHEL、CentOS、Scientific Linux、Oracle Linux)、Debian、Ubuntu が挙げられます。その他の配布でも動作する可能性はありますが、HCL Bigfix がそれらを公式にサポートしていない限り、サポートは提供されていません。

トリガーできるローカルチェックプラグインでサポートされるのは、RHEL、CentOS、Scientific Linux、Oracle Linux、Debian、Ubuntu、Solaris のみです。プラグイン 160250 を有効にする必要があります。

Tenable Nessus は、HCL Bigfix 9.5 とそれ以降、および 10.x とそれ以降をサポートしています。

HCL Bigfix スキャンでは、次の Tenable プラグインが使用されます: 160247、160248、160249、160250、160251。

オプション	説明	デフォルト
Web Reports Server (ウェブレポートサーバー)	(必須) HCL Bigfix ウェブレポートサーバーの名前。	-
Web Reports Port (ウェブレポートポー	(必須) Tenable Nessus からの通信で、HCL Bigfix ウェブレポートのサーバーがリッスンする TCP ポート。	-

オプション	説明	デフォルト
ト)		
Web レポートのユーザー名	(必須) ターゲットシステムに対してチェックを実行するために Tenable Nessus が使用する、HCL Bigfix ウェブレポート管理者アカウントのユーザー名。	-
Web Reports Password (ウェブレポートパスワード)	(必須) HCL Bigfix ウェブレポート管理者ユーザーのパスワード。	-
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable が標準の HTTP を使用して接続します。	Enabled (有効)
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	Enabled (有効)

HCL Bigfix サーバー設定

こうした監査機能を使用するには、HCL Bigfix サーバーに変更を加える必要があります。HCL Bigfix にカスタム分析をインポートし、Tenable Nessus が詳細なパッケージ情報を読み取って利用できるようにしてください。

HCL BigFix コンソールアプリケーションから、次の `.bes` ファイルをインポートします。

BES ファイル:

```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
    <Analysis>
        <Title>Tenable</Title>
        <Description>This analysis provides SecurityCenter with the data it needs for vulnerability
reporting. </Description>
        <Relevance>true</Relevance>
        <Source>Internal</Source>
```

```
        <SourceReleaseDate>2013-01-31</SourceReleaseDate>
        <MIMEField>
            <Name>x-fixlet-modification-time</Name>
            <Value>Thu, 13 May 2021 21:43:29 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <Property Name="Packages - With Versions (Tenable)" ID="74"><![CDATA[if (exists true whose
(if true then (exists object repository) else false)) then unique values of (lpp_name of it & "|" &
version of it as string & "|" & "fileset" & "|" & architecture of operating system) of filesets of
products of object repository else if (exists true whose (if true then (exists debianpackage) else
false)) then unique values of (name of it & "|" & version of it as string & "|" & "deb" & "|" &
architecture of it & "|" & architecture of operating system) of packages whose (exists version of it)
of debianpackages else if (exists true whose (if true then (exists rpm) else false)) then unique
values of (name of it & "|" & version of it as string & "|" & "rpm" & "|" & architecture of it & "|"
& architecture of operating system) of packages of rpm else if (exists true whose (if true then
(exists ips image) else false)) then unique values of (full name of it & "|" & version of it as
string & "|" & "pkg" & "|" & architecture of operating system) of latest installed packages of ips
image else if (exists true whose (if true then (exists pkgdb) else false)) then unique values of
(pkginst of it & "|" & version of it & "|" & "pkg10") of pkginfos of pkgdb else
"<unsupported>"]]></Property>
        <Property Name="Tenable AIX Technology Level" ID="76">current technology level of operating
system</Property>
        <Property Name="Tenable Solaris - Showrev -a" ID="77"><![CDATA[if ((operating system as
string as lowercase contains "SunOS 5.10" as lowercase) AND (exists file "/var/opt/BESClient/showrev_
patches.b64")) then lines of file "/var/opt/BESClient/showrev_patches.b64" else
"<unsupported>"]]></Property>
    </Analysis>
</BES>
```

BES ファイル:

```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
    <Task>
        <Title>Tenable - Solaris 5.10 - showrev -a Capture</Title>
        <Description><![CDATA[&lt;enter a description of the task here&gt; ]]></Description>
        <GroupRelevance JoinByIntersection="false">
            <SearchComponentPropertyReference PropertyName="OS" Comparison="Contains">
                <SearchText>SunOS 5.10</SearchText>
                <Relevance>exists (operating system) whose (it as string as lowercase contains "SunOS
5.10" as lowercase)</Relevance>
            </SearchComponentPropertyReference>
        </GroupRelevance>
        <Category></Category>
        <Source>Internal</Source>
        <SourceID></SourceID>
        <SourceReleaseDate>2021-05-12</SourceReleaseDate>
        <SourceSeverity></SourceSeverity>
        <CVENames></CVENames>
        <SANSID></SANSID>
        <MIMEField>
            <Name>x-fixlet-modification-time</Name>
            <Value>Thu, 13 May 2021 21:50:58 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <DefaultAction ID="Action1">
```

```
            <Description>
                <PreLink>Click </PreLink>
                <Link>here</Link>
                <PostLink> to deploy this action.</PostLink>
            </Description>
            <ActionScript MIMEType="application/x-sh"><![CDATA[#!/bin/sh
/usr/bin/showrev -a > /var/opt/BESClient/showrev_patches
/usr/sfw/bin/openssl base64 -in /var/opt/BESClient/showrev_patches -out /var/opt/BESClient/showrev_
patches.b64

]]></ActionScript>
        </DefaultAction>
    </Task>
</BES>
```

Microsoft System Center Configuration Manager (SCCM)

ヒント: Microsoft SCCM の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に integration_status.nasl プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Microsoft System Center Configuration Manager (SCCM) は、Windows ベースのシステムの大規模グループの管理に使用できます。Tenable Nessus は SCCM サービスにクエリを実行して、SCCM が管理しているシステムにパッチがインストールされているかどうかを検証し、スキャン結果を介してパッチ情報を表示できます。

Tenable Nessus は SCCM サイトを実行しているサーバーに接続します (認証情報が SCCM サービスに対して有効である必要があるため、選択されたユーザーは SCCM MMC のすべてのデータのクエリ権限を持っている必要があります)。このサーバーは SQL データベースも実行している場合があります。あるいは、データベースと SCCM レポジトリが別のサーバーにある場合もあります。この監査を活用する場合、Tenable Nessus が WMI および HTTPS を介して SCCM サーバーに接続される必要があります。

注意: Tenable 製品で SCCM をスキャンするには**[Read-only Analyst]** (読み取り専用アナリスト)、**[Operations Administrator]** (オペレーション管理者)、または**[Full Administrator]** (完全な管理者) のいずれかのロールが必要です。詳しくは、SCCM スキャンポリシーを設定するを参照してください。

SCCM のスキャンでは、Tenable プラグインの 57029、57030、73636、58186 を使用します。

注意: SCCM パッチ管理プラグインは、SCCM 2007 から Configuration Manager 2309 までのバージョンをサポートしています。

認証情報	説明	デフォルト
Server (サーバー)	(必須) SCCM の IP アドレスまたはシステム名。	-
Domain (ドメイン)	(必須) SCCM サーバーのドメインの名前。	-
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、SCCM のユーザーアカウントのユーザー名。このユーザーアカウントには、SCCM MMC のすべてのデータにクエリを実行する権限が必要です。	-
Password (パスワード)	(必須) SCCM MMC のすべてのデータのクエリ権限を持つ SCCM ユーザのパスワード。	-

Windows Server Update Services (WSUS)

ヒント: Microsoft WSUS の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Windows Server Update Services (WSUS) は、Microsoft 製品向けの更新プログラムとホットフィックスの配布を管理できる Microsoft 社の製品です。Tenable Nessus は WSUS にクエリを実行して、WSUS が管理しているシステムにパッチがインストールされているかどうかを検証し、Tenable Nessus のユーザーインターフェースにパッチ情報を表示できます。

WSUS のスキャンでは、Tenable プラグインの 57031、57032、58133 を使用します。

オプション	説明	デフォルト
Server (サーバー)	(必須) WSUS の IP アドレスまたはシステム名。	-
Ports (ポート)	(必須) Tenable Nessus からの通信に対して Microsoft WSUS がリッスンする TCP ポート。	8530
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、WSUS 管理者アカウントのユーザー名。	-

オプション	説明	デフォルト
Password (パスワード)	(必須) WSUS 管理者ユーザーのパスワード。	-
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable が標準の HTTP を使用して接続します。	Enabled (有効)
SSL 証明書の検証	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	Enabled (有効)

Red Hat Satellite 6 サーバー

ヒント: Red Hat Satellite 6 Server の認証情報が正常に認証されたかどうかを確認するには、スキャンの完了後に `integration_status.nasl` プラグインのプラグイン出力を確認します。詳細は、プラグインを参照してください。

Red Hat Satellite 6 は、Linux ベースシステム用のシステム管理プラットフォームです。Tenable Nessus は Satellite にクエリを実行して、Satellite が管理しているシステムにパッチがインストールされているかどうかを検証し、パッチ情報を表示できます。

Tenable によるサポートはありませんが、Red Hat Satellite 6 プラグインは Red Hat Satellite のオープンソースアップストリームバージョンである Spacewalk Server とも連携できます。Spacewalk では、Red Hat をベースとするディストリビューション (RHEL、CentOS、Fedora) と SUSE を管理できます。Tenable は、Red Hat Enterprise Linux 向けの Satellite サーバーをサポートしています。

Red Hat Satellite 6 スキャンでは、Tenable プラグインの 84236、84235、84234、84237、84238、84231、84232、84233 を使用します。

オプション	説明	デフォルト
Satellite server (Satellite サーバー)	(必須) Red Hat Satellite 6 の IP アドレスまたはシステム名。	-

オプション	説明	デフォルト
Ports (ポート)	(必須) Tenable Nessus からの通信に対して Red Hat Satellite 6 がリッスンする TCP ポート。	443
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、Red Hat Satellite 6 のアカウントのユーザー名。	-
Password (パスワード)	(必須) Red Hat Satellite 6 ユーザーのパスワード。	-
HTTPS	有効にすると、Tenable が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable が標準の HTTP を使用して接続します。	Enabled (有効)
SSL 証明書の検証	有効にすると、Tenable がサーバーの SSL 証明書が信頼できる CA によって署名されているかどうかを検証します。 **ヒント:** 自己署名証明書を使用している場合は、この設定を無効にします。	Enabled (有効)

Symantec Altris

Altiris は、Symantec から提供されているパッチ管理システムで、Linux、Windows、macOS の各システムの更新プログラムとホットフィックスの配布を管理します。Tenable Nessus は Altiris API を使用して、Altiris が管理しているシステムにパッチがインストールされているかどうかを検証し、Tenable Nessus のユーザーインターフェースにパッチ情報を表示できます。

Tenable Nessus は、Altiris ホスト上で実行されている Microsoft SQL サーバーに接続します。この監査を活用する際に、MSSQL データベースと Altiris サーバーが別のホストにある場合は、Tenable Nessus を Altiris サーバーではなく、MSSQL データベースに接続する必要があります。

Altiris スキャンでは、Tenable プラグインの 78013、78012、78011、78014 を使用します。

認証情報	説明	デフォルト
Server (サーバー)	(必須) Altiris の IP アドレスまたはシステム名。	-
Database Port (データベースのポート)	(必須) Tenable Nessus からの通信に対して Altiris がリッスンする TCP ポート。	5690
Database Name (データベース名)	(必須) Altiris パッチ情報を管理する MSSQL データベースの名前。	Symantec_CMDB
データベースのユーザー名	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、Altiris MSSQL データベースのアカウントのユーザー名。認証情報は、Altiris MSSQL データベース内のすべてのデータにクエリを実行する権限を持つ MSSQL データベースアカウント用の有効なものでなければなりません。	-
Database Password (データベースパスワード)	(必須) Altiris MSSQL データベースユーザーのパスワード。	-
Use Windows Authentication (Windows認証を使用する)	この機能を有効にすると、古い Windows Server との互換性を確保するために NTLMSSP を使用します。 無効の場合は、Kerberos を使用します。	Disabled (無効)

プレーンテキスト認証の認証情報

警告: Tenable プレーンテキストの認証情報を使用することは推奨されません。可能であれば、暗号化認証を使用してください。

認証情報を用いてチェックをセキュアに実行する方法がない場合、セキュアでないプロトコルを通じたチェックの実行やプレーンテキスト認証オプションの使用を試みるように Nessus に強制できます。

このメニューでは、Nessus スキャナーは HTTP、NNTP、FTP、POP2、POP3、IMAP、IPMI、telnet/rsh/rexec、SNMPv1/v2c をテストする際に認証情報を使用できます。

認証情報を提供することで、Nessus は脆弱性を特定するためのより広範囲なチェックを実行できます。Nessus が、提供された HTTP 認証情報を使用するのは、Basic 認証と Digest 認証のみです。

FTP、IPMI、NNTP、POP2、POP3 用の認証情報としては、ユーザー名とパスワードのみ必要です。

HTTP

HTTP の認証方法には、自動認証、Basic/Digest 認証、HTTP ログインフォーム、HTTP Cookie のインポートの 4 通りあります。

HTTP グローバル設定

オプション	デフォルト	説明
Login method (ログイン方法)	POST	ログインアクションが GET または POST リクエストのどちらを介して実行されるかを指定します。
Re-authenticate delay (seconds) (再認証の遅延 (秒))	0	認証を試みてから次の認証を試みるまでの時間の遅延です。ブルートフォースロックアウトメカニズムのトリガーを回避するのに役立ちます。
Follow 30x redirections (30x 系のリダイレクトに従う) (レベル数)	0	ウェブサーバーから 30 倍のリダイレクトコードを受信した場合、提供されたリンクをフォローするかどうかを Nessus に指示します。
Invert authenticated regex (認証された正規表現の反転)	Disabled (無効)	ログインページで検索対象の正規表現パターンが見つかった場合に、認証が成功しなかったことを Nessus に通知します (例: 認証に失敗しました)。
Use authenticated regex on HTTP headers (認証された正規表現の HTTP ヘッダーでの使用)	Disabled (無効)	認証状態をより正確に判断するために、Nessus は応答の本文ではなく、特定の HTTP 応答ヘッダーで正規表現パターンを検索できます。
Use authenticated regex on HTTP headers (認証された正規表現の HTTP ヘッダーでの使用)	Disabled (無効)	デフォルトでは、正規表現の検索で大文字と小文字が区別されます。このオプションでは、大文字と小文字を区別しないよう Nessus に指示します。

認証方法

自動認証

ユーザー名とパスワードが必要

Basic/Digest 認証

ユーザー名とパスワードが必要

HTTP ログインフォーム

HTTP ログインページの設定を通じて、ウェブベースのカスタムアプリケーションの認証テストを開始する場所を管理します。

オプション	説明
Username (ユーザー名)	ログインユーザーの名前。
Password (パスワード)	指定されたユーザーのパスワードです。
Login page (ログインページ)	アプリケーションのログインページの絶対パス (例: /login.html)。
Login submission page (ログイン送信ページ)	フォーム方法の操作パラメーター。たとえば、<form method="POST" name="auth_form" action="/login.php">のログインフォームは、/login.phpとなります。
Login parameters (ログインパラメーター)	認証パラメーター (例: login=%USER%&password=%PASS%) を指定します。%USER% や %PASS% といったキーワードを使用する場合、それらのキーワードは、ログイン設定ドロップダウンボックスで指定した値に置き換えられます。必要であれば、このフィールドを使用して複数のパラメーターを渡すことができます (認証プロセスでグループ名などの情報が必要な場合など)。
Check authentication on page (ページで認証を検証)	認証ステータスについての Nessus の判断を支援するために、認証を必要とする保護されたウェブページの絶対パス (/admin.html など)。

オプション	説明
Regex to verify successful authentication (正常な認証を検証するための正規表現)	ログインページで検索する正規表現パターン。単に200の応答コードを受け取っただけでは、セッションステータスを判断するのには十分ではない可能性があります。Nessusは「認証に成功しました」などの特定の文字列との照合を試みることができます。

HTTP Cookie のインポート

ウェブアプリケーションのテストを容易にするために、Nessus は HTTP Cookie のインポート設定を使用して、別のソフトウェア (ブラウザ、ウェブプロキシなど) から HTTP Cookie をインポートできます。ウェブアプリケーションへのアクセスを試行するときに Nessus が Cookie を使用するように、Cookie ファイルをアップロードできます。Cookie ファイルは Netscape 形式である必要があります。

NNTP

設定	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、NNTP のアカウントのユーザー名。	-
Password (パスワード)	(必須) NNTP ユーザーのパスワード。	-

FTP

設定	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、FTP のアカウントのユーザー名。	-
Password (パスワード)	(必須) FTP ユーザーのパスワード。	-

POP2

設定	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、POP2 のアカウントのユーザー名。	-
Password (パスワード)	(必須) POP2 ユーザーのパスワード。	-

POP3

設定	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、POP3 のアカウントのユーザー名。	-
Password (パスワード)	(必須) POP3 ユーザーのパスワード。	-

IMAP

設定	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、IMAP のアカウントのユーザー名。	-
Password (パスワード)	(必須) IMAP ユーザーのパスワード。	-

IPMI

設定	説明	デフォルト
Username (ユーザー名)	(必須) ターゲットのシステムでチェックを実行するために Tenable Nessus が使用する、IMPI のアカウントのユーザー名。	-
パスワード (平文で送信)	(必須) IPMI ユーザーのパスワード。	-

telnet/rsh/rexec

telnet/rsh/rexec 認証セクションもユーザー名とパスワードですが、このセクションにはさらにグローバル設定があり、これら 3 つのプロトコルのいずれかを使用してパッチ監査を実行できます。

SNMPv1/v2c

SNMPv1/v2c 設定を使用すると、ネットワークデバイスの認証用コミュニティ文字列を使用できます。SNMP コミュニティ文字列を最大 4 つまで設定できます。

設定	説明	デフォルト
Community string (コミュニティ文字列)	(必須) ホストデバイスでの認証のために Tenable Vulnerability Managementが使用するコミュニティ文字列。	public
グローバル認証情報設定		
UDP Port (UDP ポート)	(必須) Tenable Nessus からの通信に対して SNMPv1/v2c がリッスンする TCP ポート。	161
Additional UDP port #1 (追加の UDP ポート #1)		
Additional UDP port #2 (追加の UDP ポート #2)		
Additional UDP port #3 (追加の UDP ポート #3)		

コンプライアンス

> **注意:** スキャンがユーザー定義ポリシーに基づいている場合、スキャンの **[Compliance]** (コンプライアンス) 設定はできません。これらの設定は、関連するユーザー定義ポリシーでのみ変更できます。

Tenable Nessus は、ネットワークサービスの脆弱性スキャンを実行できるだけでなく、サーバーにログインして不足しているパッチを検出できます。

ただし、脆弱性がないからといって、サーバーが正しく設定されている、または特定の標準に「準拠している」というわけではありません。

Tenable Nessus を使用して、脆弱性のスキャンとコンプライアンスの監査を実行し、すべてのデータを一度に取得できます。サーバーの設定方法、パッチの適用方法、存在する脆弱性の種類を知ることは、リスクを軽減する手段の決定に役立ちます。

より大きな視点から見ると、ネットワーク全体または資産クラスの情報が集約されていれば、セキュリティとリスクをグローバルに分析できます。これにより、監査人とネットワーク管理者は非準拠システムの傾向を見つけ、きめ細かく制御しながら大規模に修正できます。

スキャンまたはポリシーを設定する際に、監査として知られるコンプライアンスチェックを 1 つ以上含めることができます。各コンプライアンスチェックには特定の認証情報が必要です。

一部のコンプライアンスチェックは Tenable によって事前設定されていますが、カスタマイズした監査項目を作成してアップロードすることも可能です。

コンプライアンスチェックや監査項目のカスタマイズの詳細は、Compliance Checks Reference を参照してください。

注意: 1 つの**ポリシーコンプライアンス監査**スキャンに含めることができる監査ファイルの最大数は、監査ファイルが必要とする合計実行時間とメモリによって制限されます。この制限を超えると、スキャン結果が不完全になったり失敗したりする可能性があります。Tenable では、想定される影響を限定的なものにするため、スキャンの範囲とコンプライアンス要件を明確にしたうえで、スキャンポリシーで対象となる監査を選択することを推奨しています。

コンプライアンスチェック	必要な認証情報
Adtran AOS	SSH
Alcatel TiMOS	SSH
Amazon AWS	Amazon AWS
Arista EOS	SSH
ArubaOS	SSH
Blue Coat ProxySG	SSH
Brocade Fabricos	SSH
Check Point GAiA	SSH
Cisco ACI	SSH
Cisco Firepower	SSH

コンプライアンスチェック	必要な認証情報
Cisco IOS	SSH
Cisco Viptela	SSH
Citrix Application Delivery	Citrix NITRO API
データベース	データベース
Extreme ExtremeXOS	SSH
F5	F5
FireEye	SSH
Fortigate FortiOS	SSH
Generic SSH	SSH
Google Cloud Platform	Google Cloud Platform
HP ProCurve	SSH
Huawei VRP	SSH
IBM DB2 DB	データベース
IBM iSeries	IBM iSeries または SSH
Juniper Junos	SSH
Microsoft Azure	Microsoft Azure
モバイルデバイスマネージャー	AirWatch または Mobileiron
MongoDB	MongoDB
Microsoft SQL DB	データベース
MySQL DB	データベース
NetApp API	NetApp API
NetApp Data ONTAP	SSH

コンプライアンスチェック	必要な認証情報
OpenShift Container Platform	OpenShift Container Platform
OpenStack	OpenStack
Oracle DB	データベース
Palo Alto Networks PAN-OS	PAN-OS
PostgreSQL DB	データベース
Rackspace	Rackspace
RHEV	RHEV
Salesforce.com	Salesforce SOAP API
Snowflake	Snowflake API
SonicWALL SonicOS	SSH
Splunk	Splunk API
Sybase DB	データベース
Unix	SSH
Unixファイルコンテンツ	SSH
VMware vCenter/vSphere	VMware vCenter API または VMware ESX SOAP API
WatchGuard	SSH
Windows	Windows
Windowsファイルコンテンツ	Windows
Zoom	Zoom
ZTE ROSNG	SSH

注意: プラグインは、次のいずれかのシナリオに該当するエラーを生成することがあります。

- 懸念事項として通知する必要があるが、大規模なスキャンの結果に影響を与えるリスクはない
- プラグインが問題を報告できない問題が発生した

どちらのシナリオでも、「コンプライアンスプラグインエラー: <プラグイン名>」という名前のコンプライアンス結果が警告として投稿されます。コンプライアンス結果の出力により、検討すべき問題が特定されます。これらの結果は、プラグイン 214001 コンプライアンスステータスによって投稿されます。

カスタム監査ファイルのアップロード

Nessus スキャンのコンプライアンス設定を行うときに、次のカスタム監査ファイルをアップロードできます。

- Tenable が作成した監査ファイル (Tenable ダウンロードページからダウンロードできます)。
- Security Content Automation Protocol (SCAP) データストリームファイル (SCAP リポジトリ (例: https://ncp.nist.gov/repository) からダウンロードできます)。

  このファイルには、完全な SCAP コンテンツ (Open Vulnerability and Assessment Language (OVAL) および Extensible Configuration Checklist Description Format (XCCDF) のコンテンツ) または OVAL スタンドアロンコンテンツが含まれている必要があります。
- 特定の環境用に作成またはカスタマイズされたカスタム監査ファイル。詳細については、Nessus コンプライアンスチェックリファレンスを参照してください。

始める前に

- アップロードするファイルをダウンロードまたは作成します。

  注意: 標準の監査ファイルとは異なり、Tenable Nessus ユーザーインターフェースではカスタム監査ファイルの変数パラメーターを設定できません。これを行うには、Tenable Nessus にアップロードする前に、監査ファイルのパラメーターを直接編集する必要があります。

  たとえば、標準の **[CIS CentOS 6 Server L1 v3.0.0]** 監査ファイルを Tenable Nessus にアップロードする場合、ユーザーインターフェースで **[Network Time]** (ネットワーク時間) という名前のパラメーターを設定できます。

  カスタム監査ファイルで **[Network Time]** (ネットワーク時間) をデフォルト値から変更する場合は、カスタム監査ファイルでそのフィールドを検索します。フィールドの変数名は **[NTP_SERVER]** になります。

  次に、**[@NTP_SERVER@]** を検索します。この検索を実行する際は、変数名を「@」で囲みます。

  次の 4 つの場所が表示されます。

- `regex : "^[\\s]*server[\\s]+@NTP_SERVER@[\\s]*$"`
- `expect: "^[\\s]*server[\\s]+@NTP_SERVER@[\\s]*$"`
- `regex : "^[\\s]*server[\\s]+@NTP_SERVER@"`
- `expect: "^[\\s]*server[\\s]+@NTP_SERVER@"`

監査ファイルで直接変更する値を更新します (この例では **[192.0.2.0]**)。

- `regex : "^[\\s]*server[\\s]+`**`192.0.2.0`**`[\\s]*$"`
- `expect: "^[\\s]*server[\\s]+`**`192.0.2.0`**`[\\s]*$"`
- `regex : "^[\\s]*server[\\s]+`**`192.0.2.0`**`"`
- `expect: "^[\\s]*server[\\s]+`**`192.0.2.0`**`"`

デフォルト値から変更したいすべての変数について、この検索と置換のプロセスを実行します。

カスタム監査ファイルをアップロードする方法

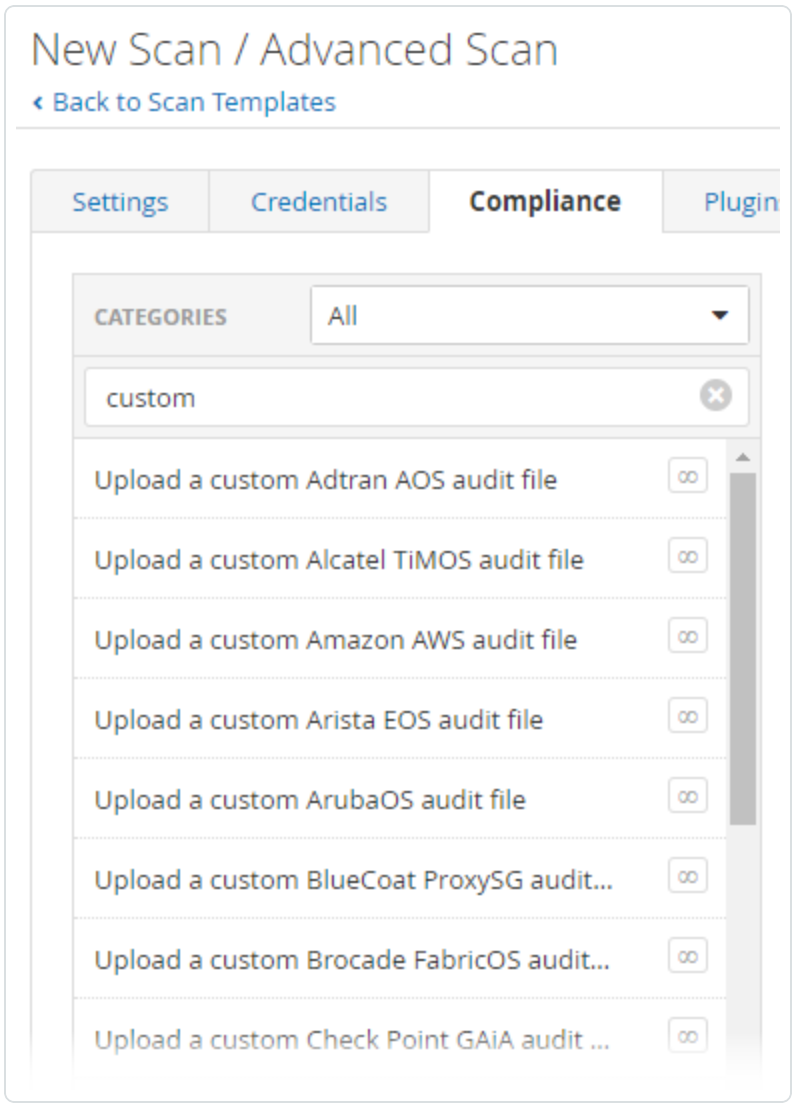
1. Tenable Nessus のユーザーインターフェースにログインします。
2. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。
3. 右上の **[New Scan]** (新しいスキャン) ボタンをクリックします。

   [Scan Templates] (スキャンテンプレート) ページが表示されます。
4. 使用するスキャンテンプレートをクリックします。

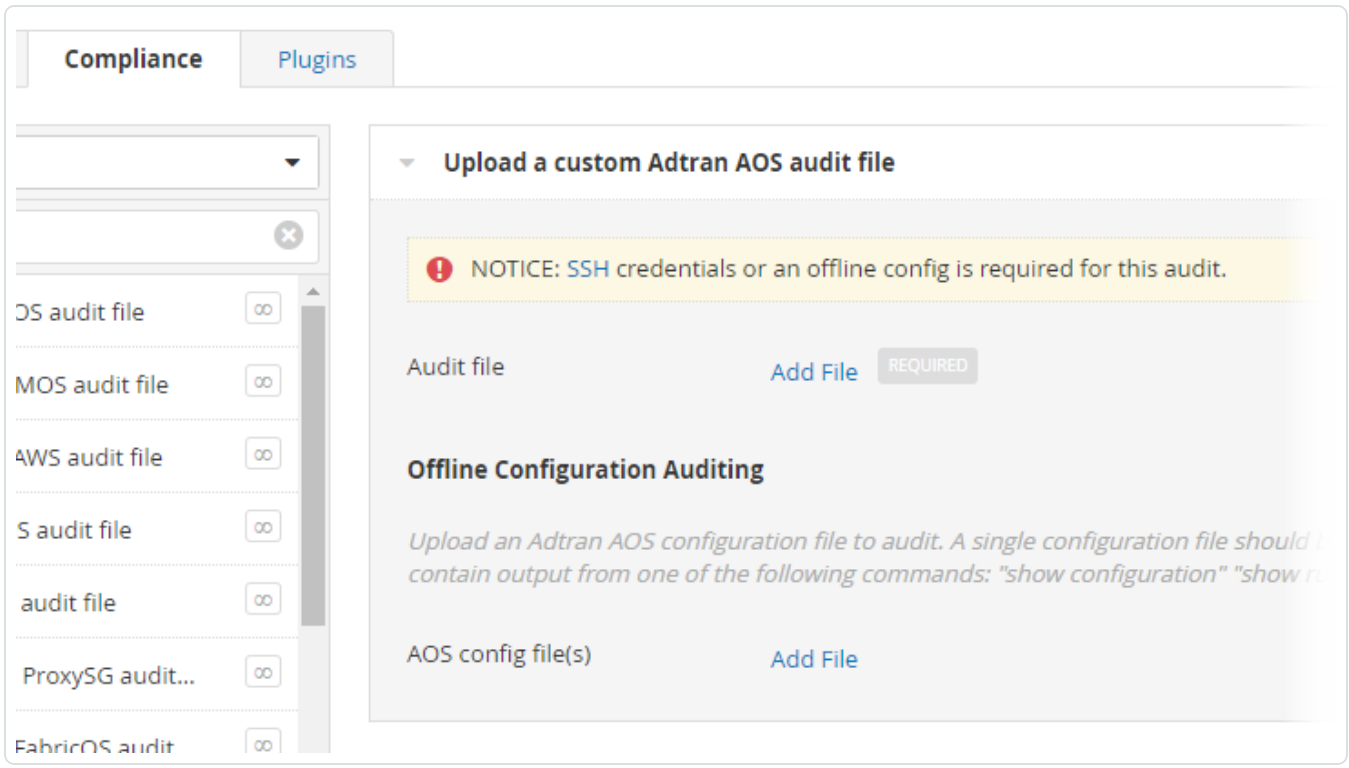
   [scan settings] (スキャンの設定) ページが表示されます。
5. **[Compliance]** (コンプライアンス) タブを開きます。
6. **[Filter Compliance]** (コンプライアンスをフィルタリング) ボックスに、「`custom`」と入力します。

   アップロードできるカスタム監査ファイルの種類のリストが表示されます。



7. アップロードするカスタム監査ファイルの種類を選択します。

   [Upload a custom audit file] (カスタム監査ファイルのアップロード) ペインが表示されます。



8. **[Add File]** (ファイルの追加) をクリックします。マシンからアップロードするカスタム監査ファイルを選択します。

   監査のタイプによっては、カスタム監査をアップロードした後に、追加の設定が必要になる場合があります。

9. 次のいずれかを行います。

   - すぐにスキャンを起動するには、▼ボタンをクリックし、**[Launch]** (起動) をクリックします。

     Tenable Nessus がスキャンを保存して起動します。

   - スキャンを後で起動するには、**[Save]** (保存) ボタンをクリックします。

     Tenable Nessus
     がスキャンを保存します。

SCAP 設定

セキュリティコンテンツ自動化プロトコル (SCAP) は、企業の脆弱性とポリシーのコンプライアンスにおける自動管理を有効にするオープンスタンダードです。OVAL、CVE、CVSS、CPE、FDCC ポリシーなど、複数のオープンスタンダードおよびポリシーが使用されています。

SCAP and OVAL Auditing テンプレートを選択すると、SCAP の設定を変更できます。

注意:SCAP および OVAL 監査 スキャンテンプレートは、後方互換性のために保持されています。このテンプレートは SCAP バージョン 1.2 以前をサポートしています。SCAP バージョン 1.3 以降を必要とする Windows 10 や Windows 11 などの最新のオペレーティングシステムとは互換性がありません。

選択肢は **Linux (SCAP)**、**Linux (OVAL)**、**Windows (SCAP)**、**Windows (OVAL)** です。各オプションの設定について次の表で説明します。

設定	デフォルト値	説明
Linux (SCAP)またはWindows (SCAP)		
SCAP File	なし	SCAP のフルコンテンツ (バージョン 1.0 と 1.1 は XCCDF、OVAL、CPE、バージョン 1.2 は DataStream) を含む有効な zip ファイル。
SCAP Version (SCAP バージョン)	1.2	アップロード済みの SCAP ファイルにあるコンテンツに適した SCAP バージョン。
SCAP Data Stream ID	なし	(SCAP バージョン 1.2 のみ) SCAP XML ファイルからコピーした Data Stream ID。 例: `<data-stream id="scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip">`
SCAP Benchmark ID (SCAP ベンチマーク ID)	なし	SCAP XML ファイルからコピーしたベンチマーク ID。 例: `<xccdf:Benchmark id="xccdf_gov.nist_benchmark_USGCB-Windows-7">`
SCAP Profile ID (SCAP プロファイル ID)	なし	SCAP の XML ファイルからコピーしたプロファイル ID です。 例: `<xccdf:Profile id="xccdf_gov.nist_profile_`

		united_states_government_configuration_baseline_version_1.2.3.1">
OVAL Result Type (OVAL 結果タイプ)	システムの特徴と全結果	結果ファイルに含める情報。 結果ファイルの種類には、システム特性データを含む完全な結果、システム特性データを除外した結果、簡単な結果があります。
Linux (OVAL) または Windows (OVAL)		
OVAL definitions file (OVAL 定義ファイル)	なし	OVAL スタンドアロンコンテンツを含む有効な zip ファイル。

プラグイン

一部の Tenable Nessus テンプレートには **[Plugin]** (プラグイン) オプションが含まれています。

[Plugin] (プラグイン) オプションで、**[Plugin Family]** (プラグインファミリー) または個別のプラグインチェックによるセキュリティチェックを選択できます。

特定のプラグインの詳細については、Tenable プラグインサイトを参照してください。プラグインファミリーの詳細については、Tenable プラグインサイトのプラグインファミリーについてを参照してください。

> **注意:** スキャンまたはポリシーを作成して保存すると、最初に選択したすべてのプラグインが記録されます。Tenable Nessus がプラグインの更新で新しいプラグインを受け取ると、関連付けられているファミリーが有効であれば、Nessus はその新しいプラグインを自動的に有効にします。ファミリーが無効にされているか、一部しか有効でない場合、Nessus はそのファミリーの新しいプラグインも自動的に無効にします。

プラグインファミリー

[Plugin Family] (プラグインファミリー) をクリックすると、ファミリー全体を有効 (**緑色**) または無効 (**灰色**) にできます。ファミリーを選択すると、そのプラグインのリストが表示されます。プラグインを個別に有効または無効にして、特定のスキャンを作成できます。

無効なプラグインが含まれているファミリーは紫色で表示され、一部のプラグインのみ有効であることを示すために **[Mixed]** (混在) と表示されます。プラグインファミリーをクリックすると、プラグインの全リストが読み込まれ、スキャンの環境設定に基づいて詳細な選択ができます。

無効なプラグインが混在するプラグインファミリーには、ロックされた状態またはロック解除された状態の南京錠のアイコンが表示されます。

- ロックされた南京錠 - プラグインフィードの更新を通じてプラグインファミリーに追加された新しいプラグインは、ポリシーで自動的に*無効化*されます。
- ロック解除された南京錠 - プラグインフィードの更新を通じてプラグインファミリーに追加された新しいプラグインは、ポリシーで自動的に*有効化*されます。

南京錠のアイコンをクリックして、プラグインファミリーをロックまたはロック解除します。

警告: [Denial of Service] (サービス拒否) ファミリーには、悪影響のない便利なチェックだけでなく、[Safe Checks] (安全チェック) オプションを有効にしないとネットワークの停止を引き起こす可能性のあるプラグインも含まれています。**サービス拒否**ファミリーを安全チェックと合わせて使用することで、潜在的に危険なプラグインを Tenable Nessus が実行することを防止できます。ただし、Tenable では、保守作業を行っているときかつ問題に対応できるスタッフがいる状態で使用する場合を除き、本番ネットワークでは**サービス拒否**ファミリーを使用しないことを推奨しています。

プラグイン出力の詳細の表示

特定の**プラグイン名**を選択すると、レポートで確認できるプラグイン出力が表示されます。

プラグインの詳細には、次の表に記載されている情報が含まれます。一部のプラグインは、リストされているすべての情報を提供しません。

セクション	説明
概要	プラグインの概要を表示します。
説明	プラグインおよびそれに関連する脆弱性の詳しい説明を表示します。
ソリューション	プラグインの脆弱性の解決策を表示します。
その他の関連項目	プラグインに関連するセキュリティアドバイザリを表示します。
プラグイン情報	次のプラグイン情報を表示します。 • **ID** – プラグインの数値 ID。 • **バージョン** – プラグインの現在のバージョン。

	• **タイプ** – プラグインのタイプ。これにより、スキャナーで実行する際のプラグインの動作を指定します。
	  • **リモート** – プラグインは、ローカルホストへの認証を試みたり、要求したりしません。代わりに、バナーチェック、パッチのテスト、脆弱性の悪用を通じて、リモートで情報を収集します。一部のプラグインはサービスへのサインインを試行しますが、ローカルホストの認証情報を必要としません。
	  • **ローカル** – プラグインはサービス (SMB や SSH など) を通してターゲットに対して認証を行い、情報を抽出します。
	  • **両方** – プラグインは、リモートチェックとローカルチェックを介して情報を収集します。ローカルチェックが利用できない場合でも、プラグインはプラグイン内のリモートチェックからできる範囲で情報を収集します。
	  • **設定** – プラグインは、スキャン中に他のプラグインが使用する 1 つ以上の設定を定義します。
	  • **サマリー** – プラグインは、他のプラグインによって収集されたデータをまとめます。
	  • **サードパーティ** – プラグインはサードパーティアプリケーション (nmap など) を実行します。
	  • **レピュテーション** – サードパーティのレピュテーションサービスを使用します。
	• **公開日** – プラグインが公開された日付。
	• **変更日** – プラグインが変更された直近の日付。

リスク情報	プラグインの次の脆弱性リスク情報を表示します。 • **リスクファクター** – 脆弱性の VPR 深刻度レベル。VPR についての詳細は、CVSS スコアとVPR を参照してください。 • **CVSS v3.0 基本値** – 脆弱性の CVSS v3.0 基本値。脆弱性の基本値は、脆弱性が最初に発見されたときに決定され、時間が経過しても変化しません。 • **CVSS v3.0 区分** – 脆弱性の CVSS v3.0 基本値を決定するために使用される評価基準値のテキスト表示。 • **CVSS v3.0 現状区分** – 脆弱性の CVSS v3.0 現状値を決定するために使用さ

	れる評価基準値のテキスト表示。 • **CVSS v3.0 現状値** – 脆弱性の CVSS v3.0 現状値。現状値は、基本値とは異なり、ソフトウェアベンダーとハッカーの両方が行ったアクティビティに基づいて経時的に更新されます。 • **CVSS v2.0 基本値** – 脆弱性の CVSS v2.0 基本値。脆弱性の基本値は、脆弱性が最初に発見されたときに決定され、時間が経過しても変化しません。 • **CVSS v2.0 区分** – 脆弱性の CVSS v2.0 基本値を決定するために使用される評価基準値のテキスト表示。 • **CVSS v2.0 現状区分** – 脆弱性の CVSS v2.0 現状値を決定するために使用される評価基準値のテキスト表示。 • **CVSS v2.0 現状値** – 脆弱性の CVSS v2.0 現状値。現状値は、基本値とは異なり、ソフトウェアベンダーとハッカーの両方が行ったアクティビティに基づいて経時的に更新されます。 • **IAVM 深刻度** – Information Assurance Vulnerability Management (IAVM) での脆弱性の深刻度レベルです。
脆弱性の情報	プラグインの次の脆弱性情報を表示します。 • **CPE** – プラグインの共通プラットフォーム一覧 (CPE)。 • **エクスプロイトが利用可能** – 現在公開されているエクスプロイトがプラグインに対して利用可能かどうかを示します。 利用可能なエクスプロイトがある場合、Tenable Nessus はエクスプロイトを **[Exploitable With]** (エクスプロイト手段) サブセクションに一覧表示します。 • **悪用の容易さ** – プラグインがどの程度悪用可能かを指定します。 • **パッチ公開日** – プラグイン用のパッチが公開された直近の日付を示します。 • **脆弱性公開日** – プラグインの脆弱性が公表された直近の日付を示します。
参照情報	プラグインに関連する参照資料を表示します (CVE、CWE、CERT、IAVA、BID、SECUNIA、または他の関連情報)。

プラグインに関する詳細情報をさらに表示するには、Tenable プラグインの Web サイトでプラグインを検索してください。

注意: Tenable プラグインの Web サイトでプラグインを表示すると、一部のプラグインには次の注記付きで文書化されています:*「注意: Nessus はこの問題をテストしていませんが、代わりにアプリケーションの自己報告されたバージョン番号にのみ依存しています。」*この注記は、Tenable はプラグインの脆弱性に対する完全な解決策を持っていないため、脆弱性が解決されるかどうかを手動で検証する必要があることを意味します。

ダイナミックプラグインを設定する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

[Advanced Dynamic Scan] (詳細な動的スキャン) テンプレートを使用すると、プラグインファミリーや個別のプラグインを手動で選択する代わりに、ダイナミックプラグインフィルターを使用してスキャンまたはポリシーを作成できます。Tenable が新しいプラグインをリリースすると、お使いのフィルターに一致するプラグインがスキャンまたはポリシーに自動的に追加されます。これにより、新しいプラグインがリリースされたときにスキャンを最新の状態に維持しながら、特定の脆弱性に合わせてスキャンを調整することが可能になります。

特定のプラグインの詳細については、Tenable プラグインサイトを参照してください。プラグインファミリーの詳細については、Tenable プラグインサイトのプラグインファミリーについてを参照してください。

ダイナミックプラグインを設定する方法

1. 次のいずれかを行います。
    - スキャンの作成.
    - Create a Policy.
2. **[Advanced Dynamic Scan]** (詳細な動的スキャン) テンプレートをクリックします。
3. **[Dynamic Plugins]** (ダイナミックプラグイン) タブをクリックします。
4. 次のいずれかのフィルターオプションを指定します。
    - **Match Any or Match All: [All]** (すべて) を選択すると、すべてのフィルターに一致する結果のみが表示されます。**[Any]** (任意) を選択すると、設定されたフィルターのいずれかに一致する結果が表示されます。
    - **プラグイン属性:** プラグイン属性に関する説明は、プラグイン属性 の表を参照してください。

- **Filter argument:** 選択したプラグイン属性のフィルタリング方法を、**[is equal to]** (次の値に等しい)、**[is not equal to]** (次の値に等しくない)、**[contains]** (含む)、**[does not contain]** (含まない)、**[greater than]** (より大きい)、または **[less than]** (より小さい) から指定します。
- **Value :** 選択したプラグイン属性に応じて、値を入力するか、ドロップダウンメニューから値を選択します。

5. (オプション) 別のフィルターを追加するには、⊕ をクリックします。
6. **[Preview Plugins]** (プラグインのプレビュー) をクリックします。

   Tenable Nessus に指定したフィルターに一致するプラグインのリストが表示されます。
7. **[Save]** (保存) をクリックします。

   Tenable Nessus によってスキャンまたはポリシーが作成されます。このスキャンまたはポリシーは、Tenable がダイナミックプラグインフィルターに一致する新しいプラグインを追加したときに自動的に更新されます。

スキャンの作成

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

注意: Tenable Nessus によるプラグインのコンパイル中は、スキャンの作成および起動、ポリシーまたはプラグインルールの作成や表示、アップグレードアシスタントの使用はできません。

注意: Tenable Nessus で Linux マシンをスキャンする場合、Linux マシンのシェル設定ファイルには 4 文字以上の PS1 変数 (例: `PS1='\u@\h:~\$ '`) が必要です。4 文字未満の PS1 変数 (例: `PS1='\$ '`) があると、全体のスキャン時間が大幅に増加する可能性があります。

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。
2. 右上の **[New Scan]** (新しいスキャン) ボタンをクリックします。

   [Scan Templates] (スキャンテンプレート) ページが表示されます。
3. 使用するスキャンテンプレートをクリックします。
4. スキャンの設定を行います。

5. 次のいずれかを行います。

   - すぐにスキャンを起動するには、ボタンをクリックし、**[Launch]** (起動) をクリックします。

     Tenable Nessus がスキャンを保存して起動します。

   - スキャンを後で起動するには、**[Save]** (保存) ボタンをクリックします。

     Tenable Nessus
     がスキャンを保存します。

ホスト検出スキャンを作成する

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** Standard、Administrator、System Administrator

ネットワーク上のホストを把握することが、脆弱性評価の最初のステップです。ホスト検出スキャンを起動して、ネットワーク上のホスト (および IP アドレス、FQDN、オペレーティングシステム、開いているポートなどの該当する関連情報) を確認します。ホストのリストを取得した後、各脆弱性スキャンでターゲットにするホストを選択できます。

以下の概要では、ホスト検出スキャンを作成および起動し、選択した検出済みホストをターゲットとするフォローアップスキャンを作成する標準的なワークフローについて説明しています。

ホスト検出スキャンを作成して起動する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 右上の **[New Scan]** (新しいスキャン) ボタンをクリックします。

   [Scan Templates] (スキャンテンプレート) ページが表示されます。

3. **[Discovery]** (検出) で、**[Host Discovery]** (ホスト検出) テンプレートをクリックします。

4. ホスト検出スキャンを設定します。

   - **[Name]** (名前) に、スキャンの名前を入力します。

- **[Targets]** (ターゲット) に、ターゲットとしてホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。

  > **ヒント:** IP アドレスの場合は、CIDR 表記 (例: 192.168.0.0/24)、範囲 (例: 192.168.0.1-192.168.0.255)、コンマ区切りリスト (例: 192.168.0.0,192.168.0.1) を使用できます。詳細は、ターゲットのスキャンを参照してください。

- (オプション) 残りの設定を行います。

5. すぐにスキャンを起動するには、▾ボタンをクリックし、**[Launch]** (起動) をクリックします。

   Tenable Nessusでホスト検出スキャンが実行され、**[My Scans]** (マイ スキャン) ページが表示されます。

6. スキャンテーブルで、完了したホスト検出スキャンの行をクリックします。

   スキャンの結果ページが表示されます。

7. **[Hosts]** (ホスト) タブで、Tenable Nessus によって検出されたホストと利用できる関連情報 (IP アドレス、FQDN、オペレーティングシステム、開いているポートなど) を表示します。

検出された 1 つ以上のホストに対するスキャンを作成して起動する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] ページが表示されます。

2. スキャンテーブルで、完了したホスト検出スキャンの行をクリックします。

   スキャンの結果ページが表示されます。

3. **[Hosts]** (ホスト) タブをクリックします。

   Tenable Nessusでスキャンされたホストのテーブルが表示されます。

4. 新しいスキャンでスキャンする各ホストの横にあるチェックボックスを選択します。

   ページの上部に **[More]** (その他) ボタンが表示されます。

5. **[More]** (その他) ボタンをクリックします。

   ドロップダウンボックスが表示されます。

6. **[Create Scan]** (スキャンの作成) をクリックします。

   [Scan Templates] (スキャンテンプレート) ページが表示されます。

7. 新しいスキャンのスキャンテンプレートを選択します。

   Tenable Nessusで、事前に選択したホストが **[Targets]** (ターゲット) リストに自動入力されます。

8. 「スキャン設定とポリシー設定」の説明に従い、残りのスキャン設定を行います。

9. すぐにスキャンを起動するには、▼ボタンをクリックし、**[Launch]** (起動) をクリックします。

   Tenable Nessus がスキャンを保存して起動します。

Bit Discovery でアタックサーフェス検出スキャンを作成する

を使用する場合に必要なユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

注意: アタックサーフェス検出スキャンテンプレートは、Tenable Nessus Expert でのみ利用可能です。

Tenable Nessus と Bit Discovery の統合を使用して、アタックサーフェス検出スキャンを作成できます。このスキャンタイプでは、最上位ドメインをスキャンし、スキャン結果に基づいて DNS レコードを生成できます。Tenable Nessus Expert では、ライセンス取得済みのドメインを最大 5 つスキャンできます。

アタックサーフェス検出スキャンを作成する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 右上の **[New Scan]** (新しいスキャン) ボタンをクリックします。

   [Scan Templates] (スキャンテンプレート) ページが表示されます。

3. **[Discovery]** (検出) で、**[Attack Surface Discovery]** (アタックサーフェス検出) テンプレートをクリックします。

4. スキャンを設定します。

   a. **[Basic]** (基本) には、スキャン名、説明、スケジュール、スキャンを保存するフォルダを入力します。

b. **[Discovery]** (検出) には、スキャンする最上位ドメインを入力します。最大 5 つのドメインを入力できます。

> **注意:** 入力できるのは 2 部構成のドメインのみです (たとえば、`tenable.com` は入力できますが、`docs.tenable.com` は入力できません)。複数のドメインをスキャンする必要がある場合は、コンマ区切りリスト (`tenable.com, test.com, example.com` など) で入力してください。

5. 次のいずれかを行います。

   - 後で使用するためにスキャン設定を保存するには、**[Save]** (保存) をクリックします。手順 4 で選択したフォルダーから起動できます。
   - すぐにスキャンを起動するには、▾ボタンをクリックし、**[Launch]** (起動) をクリックします。

     Tenable Nessus でアタックサーフェス検出スキャンが実行され、**[My Scans]** (マイ スキャン) ページが表示されます。

次の手順

- スキャンを起動します。
- スキャン結果を表示します。
- スキャン設定を変更します。
- スキャンレポートを作成します。

  > **注意:** Tenable Nessus は、アタックサーフェス検出スキャン用に用意されているレポートテンプレートは 2 つのみ (**ホスト別の脆弱性一覧** および **ホスト別の脆弱性の詳細**) です。

- スキャン結果をエクスポートします。

  > **注意:** アタックサーフェス検出スキャンで利用できるのは、**Nessus DB** のエクスポート オプションのみです。

エージェント スキャンを作成する

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** Standard、Administrator、System Administrator

エージェント スキャンを作成する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 右上の **[New Scan]** (新規スキャン) ボタンをクリックします。

   [Scan Templates] (スキャンテンプレート) ページが表示されます。

3. **[Agent]** (エージェント) タブをクリックします。

   [Agent] (エージェント) スキャンテンプレートのページが表示されます。

4. 使用するスキャンテンプレートをクリックします。

   > **ヒント:** 上部にあるナビゲーションバーの検索ボックスを使用すると、現在表示されているタブでテンプレートを絞り込めます。

5. スキャンの設定を行います。

6. (オプション)スキャンのコンプライアンスチェックを設定します。

7. (オプション) プラグインファミリーまたは個別のプラグイン別にセキュリティチェックを設定します。

8. 次のいずれかを行います。

   - スキャンを後で起動する場合は、**[Save]** (保存) ボタンをクリックします。

     Tenable Nessus がスキャンを保存します。

   - スキャンをすぐに起動する場合は:

     a. ボタンをクリックしてください。

     b. **[Launch]** (起動) をクリックします。

     Tenable Nessus がスキャンを保存して起動します。

スキャンのインポート

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** Standard、Administrator、System Administrator

エクスポート Tenable Nessusされた (`.nessus`) または Tenable Nessus DB (`.db`) スキャンをインポートできます。インポートされたスキャンを使用すると、スキャン結果を表示したり、スキャンの新しいレポートをエ

クスポートしたり、説明を更新したりできます。インポートされたスキャンを起動したり、ポリシー設定を更新したりすることはできません。

.nessus ファイルをポリシーとしてインポートすることもできます。詳細は、Import a Policyを参照してください。

スキャンをインポートする方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 右上隅にある **[Import]** (インポート) をクリックします。

   ブラウザのファイルマネージャーウィンドウが表示されます。

3. インポートするスキャンファイルを参照して選択します。

   > **注意:** サポートされるファイルタイプは、エクスポートされた Nessus (.nessus) ファイルと Nessus DB (.db) ファイルです。

   [Scan Import] (スキャンのインポート) ウィンドウが表示されます。

4. ファイルが暗号化されている場合は、**パスワード**を入力します。

5. **[Upload]** (アップロード) をクリックします。

   Tenable Nessus によってスキャンとその関連データがインポートされます。

スキャン設定を変更する

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** Standard、Administrator、System Administrator

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 必要に応じて、左のナビゲーションバーで別のフォルダーをクリックします。

3. 設定するスキャンに対応するスキャンテーブルの行のボックスにチェックマークを入れます。

   右上隅に **[More]** (その他) ボタンが表示されます。

4. **[More]** (その他) ボタンをクリックします。

5. **[Configure]** (続行) をクリックします。

   スキャンの **[Configuration]** (設定) ページが表示されます。

6. 設定を変更します。

7. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus により設定が保存されます。

vSphere スキャンの設定

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

次の仮想環境をスキャンするようにスキャンを設定できます。

- vCenter が管理する ESXi/vSphere
- vCenter が管理しない ESXi/vSphere
- 仮想マシン

注意: ESXi ホストをスキャンする場合は、IPv4 アドレスを指定する必要があります。そうしない場合、スキャンは失敗します。

VMware の認証情報を使用したチェックについて

vCenter API または ESXi API の認証情報を設定すると、ESXi サーバーの VMware Installation Bundle (VIB) パッケージの詳細の収集が有効になります。この詳細情報は、ESX Local Security Checks プラグインファミリーで使用されます。これらの認証情報はどちらも ESXi VIB の収集を有効にします。ターゲットの ESXi サーバーへの SSH 認証情報を設定しても、VIB の収集が有効になります。

vCenter 認証情報は、ESXi VIB の収集だけでなく、ESXi サーバーの自動検出と vCenter コンプライアンスチェックも有効にします。vCenter コンプライアンスチェックでは、vCenter サーバーがターゲットとして設定されていなければなりません。

これらの認証情報は、vCenter サーバーに関するホストレベルのデータを収集しません。ホストレベルのデータを収集するには、vCenter サーバーへの追加の認証情報 (例: SSH、Windows) を設定します。

Tenable は、認証情報を使用しないリモートチェックを使用してターゲットホストにあるソフトウェアを検出することで、ESXi と vCenter のバージョン情報も収集します。最新の vCenter および ESXi の脆弱性結果は、このデータに基づいています。

VMware または vCenter の詳細については、VMware 統合ドキュメントを参照してください。

シナリオ 1: vCenter が管理しない ESXi/vSphere スキャン

vCenter が管理しない ESXi/vSphere スキャンを設定する方法

1. スキャンを作成します。
2. **基本**スキャン設定の **[Targets]** (ターゲット) セクションで、ESXi ホストの IP アドレスを入力します。
3. **[Credentials]** (認証情報) タブをクリックします。

   [Credentials] (認証情報) オプションが表示されます。
4. **[Categories]** (カテゴリ) ドロップダウンから **[Miscellaneous]** (その他) を選択します。

   その他の種類の認証情報のリストが表示されます。
5. **[VMware ESX SOAP API]** をクリックします。

   VMware ESX SOAP API のオプションが表示されます。詳細については、VMware ESX SOAP API を参照してください。
6. **[Username]** (ユーザー名) ボックスに、ローカルの ESXi アカウントに関連付けられているユーザー名を入力します。
7. **[Password]** (パスワード) ボックスに、ローカルの ESXi アカウントに関連付けられているパスワードを入力します。
8. vCenter ホストに SSL 証明書 (自己署名証明書でないもの) が含まれている場合 **[Do not verify SSL Certificate]** (SSL 証明書を検証しない) チェックボックスのチェックを外します。含まれていない場合は、このチェックボックスを選択します。
9. **[Save]** (保存) をクリックします。

シナリオ 2: vCenter が管理する ESXi/vSphere スキャン

注意: SOAP API には、読み取りと書き込みのアクセス許可を持つ vCenter 管理者アカウントが必要です。REST API では、読み取りのアクセス許可を持つ vCenter 管理者アカウントと、読み取りのアクセス許可を持つ VMware vSphere Lifecycle マネージャーアカウントが必要です。

vCenter が管理する ESXi/vSphere スキャンを設定する方法

1. スキャンを作成します。
2. **基本**スキャン設定の **[Targets]** (ターゲット) セクションで、次の IP アドレスを入力します。
   - vCenter ホスト
   - ESXi ホスト (複数可)

   注意: vCenter をターゲットとしてリストすると、vCenter バージョンとその脆弱性を収集するスキャンになりますが、オペレーティングシステムレベルの詳細は収集しません。vCenter コンプライアンススキャンでは、vCenter サーバーをターゲットとしてリストする必要もあります。
3. **[Credentials]** (認証情報) タブをクリックします。

   [Credentials] (認証情報) オプションが表示されます。
4. **[Categories]** (カテゴリ) ドロップダウンから **[Miscellaneous]** (その他) を選択します。

   その他の種類の認証情報のリストが表示されます。
5. **[VMware vCenter SOAP API]** をクリックします。

   VMware vCenter SOAP API のオプションが表示されます。詳細については、VMware vCenter SOAP API を参照してください。
6. **[vCenter Host]** (vCenter ホスト) ボックスに vCenter ホストの IP アドレスを入力します。
7. **[vCenter Port]** (vCenter ポート) ボックスに vCenter ホストのポートを入力します。デフォルトでは、この値は 443 です。
8. **[Username]** (ユーザー名) ボックスに、vCenter アカウントに関連付けられているユーザー名を入力します。
9. **[Password]** (パスワード) ボックスに、vCenter アカウントに関連付けられているパスワードを入力します。
10. vCenter ホストで SSL が有効になっている場合は、**[HTTPS]** トグルを有効にします。

11. vCenter ホストに SSL 証明書 (自己署名証明書でないもの) が含まれている場合、**[Verify SSL Certificate]** (SSL 証明書を検証する) チェックボックスを選択します。そうでない場合は、チェックボックスのチェックを外します。
12. **[Save]** (保存) をクリックします。

シナリオ 3: 仮想マシンのスキャン

ネットワーク上のその他のホストと同様に仮想マシンをスキャンすることができます。スキャンターゲットの仮想マシンの IP アドレスを必ず含めてください。仮想マシンは他のホストと同様、スキャンするゲスト OS ごとに認証情報を設定する必要があることに注意してください。詳細は、スキャンの作成を参照してください。

VMware vCenter サポートマトリクス

機能	認証の要否	対応 vCenter バージョン
Vulnerability Management	×	7.x、8.x
自動検出	○	7.0.3+、8.x
監査 / コンプライアンス	○	6.x, 7.x、8.x
VIB 列挙	○	7.0.3+、8.x
アクティブ / 非アクティブな VM	○	7.0.3+, 8.x

スキャンのメール通知を設定する

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** Standard、Administrator、System Administrator

スキャンの完了時に指定された受信者にメール通知を自動的に送信するようにスキャンを設定できます。これにより、自分とステークホルダーは Tenable Nessus でスキャンステータスを手動でチェックすることなく、スキャン結果について常に把握することができます。

始める前に

- または管理者が **Tenable Nessus**で SMTP サーバーを設定したことを確認してください。詳細は、SMTP サーバーを参照してください。

スキャンのメール通知を設定する方法:

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。
2. 次のいずれかを行います。
   - ページの右上にある ⊕ **[New Scan] (新規スキャン)**をクリックします。
   - 既存のスキャンを開きます。次に、**[の設定]**をクリックします。
3. スキャン設定メニューで、**[Basic]** > **[Notifications]**をクリックします。
4. 次の設定を行います。

設定	デフォルト値	説明
Email Recipient(s) (Eメールの受信者)	なし	スキャンが完了して結果が利用可能になったときに警告される、0 個または複数のメールアドレスをコンマで区切って指定します。
Attach Report (レポートの添付)	オフ	(Tenable Nessus Professional および Tenable Nessus Expert のみ) 各メール通知にレポートを添付するかどうかを指定します。このオプションにより、**[Report Type]** (レポートの種類) と**[Max Attachment Size]** (最大添付サイズ) の設定が切り替わります。
Report Type (レポートの種類)	Nessus	(Tenable Nessus Professional および Tenable Nessus Expert のみ) メールに添付するレポートの種類 (CSV、Nessus、PDF) を指定します。
Max Attachment Size (添付ファイルの最大サイズ)	25	(Tenable Nessus Professional および Tenable Nessus Expert のみ) レポートの添付ファイルの最大サイズをメガバイト (MB) で指定します。レポートが最大サイズを超える場合、メールにレポートは添付されません。Tenable Nessus は、50 MB を超えるレポート添付ファイルをサポートしません。
Result Filters (結果フィル	なし	メールで送信する情報の種類を定義します。

ター)		

5. **[保存]** をクリックします。

   Tenable Nessus はスキャンが完了すると、指定された受信者にメール通知を送信します。

監査証跡を設定する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. (オプション) 左のナビゲーションバーで、別のフォルダーをクリックします。

3. スキャンテーブルで、監査証跡を設定するスキャンをクリックします。

   スキャン結果が表示されます。

4. 右上の **[Audit Trail]** (監査証跡) ボタンをクリックします。

   [Audit Trail] (監査証跡) ウィンドウが表示されます。

5. **[Plugin ID]** (プラグイン ID) ボックスに、1 つまたは複数のスキャンで使用されるプラグイン ID を入力します。

   および/または

   [Host] (ホスト) ボックスに、検出されたホストのホスト名を入力します。

6. **[Search]** (検索) ボタンをクリックします。

   リストが表示され、1 つまたは両方のボックスに入力した条件と一致する結果が表示されます。

スキャンの起動

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

スキャンの [Schedule] 設定を設定するだけでなく、スキャンを手動で開始することができます。

注意: Tenable Nessus によるプラグインのコンパイル中は、スキャンの作成および起動、ポリシーまたはプラグインルールの作成や表示、アップグレードアシスタントの使用はできません。

注意: Tenable Nessus で Linux マシンをスキャンする場合、Linux マシンのシェル設定ファイルには 4 文字以上の PS1 変数 (例: `PS1='\u@\h:~\$ '`) が必要です。4 文字未満の PS1 変数 (例: `PS1='\$ '`) があると、全体のスキャン時間が大幅に増加する可能性があります。

スキャンを起動する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. スキャンテーブルで、起動するスキャンの行にある ▶ ボタンをクリックします。

   Tenable Nessus がスキャンを起動します。

次の手順

手動でスキャンを停止する必要がある場合は、実行中のスキャンの停止を参照してください。

スキャンの一時停止または再開

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

スキャンを一時停止することができます。スキャンを一時停止すると、Tenable Nessus はそのスキャンのすべてのアクティブなスキャンタスクを一時停止します。一時停止中のスキャンは、スキャナーリソースを消費しません。

一時停止したスキャンは再開することもできます。スキャンを再開すると、Tenable Nessus はスキャンを一時停止した場所からタスクを再開します。

注意: ウェブアプリケーションのスキャンやアタックサーフェス検出スキャンの一時停止または再開はできません。

スキャンを停止して終了する場合は、実行中のスキャンの停止を参照してください。

スキャンを一時停止または再開する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. スキャンテーブルにある、一時停止または再開するスキャンの行で、次のいずれかを実行します。

   - スキャンを一時停止するには、⏸ ボタンをクリックします。
   - スキャンを再開するには、▷ ボタンをクリックします。

   クリックしたボタンに応じて、Tenable Nessus がスキャンを一時停止または再開します。

実行中のスキャンの停止

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** Standard、Administrator、System Administrator

スキャンを停止すると、Tenable Nessus はそのスキャンに関するすべてのタスクを終了し、スキャンをキャンセル済みに分類します。そのスキャンに関連した Tenable Nessusのスキャン結果は、完了済みのタスクのみを反映します。個別のタスクを停止することはできません。停止できるのは全体としてのスキャンだけです。

ローカルのスキャン (すなわち、Tenable Agent や Tenable Nessus Manager のリンクされたスキャナーで実行されるスキャンではないもの) では、スキャンを強制的に停止することで、スキャンおよび実行中のすべてのプラグインを素早く終了させることができます。Tenable Nessus は、スキャンの強制停止時に実行されていたプラグインからの結果を得ることはできません。

実行中のスキャンを一時的に停止する場合は、スキャンの一時停止または再開を参照してください。

実行中のスキャンを停止する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. スキャンテーブルで、停止するスキャンの行にある ■ ボタンをクリックします。

   [Stop Scan] (スキャンの停止) ダイアログボックスが表示されます。

3. スキャンを停止するには、**[Stop]** (停止) をクリックします。

   Nessus がスキャンプロセスの終了処理を開始します。

4. (オプション) ローカルスキャンの場合、スキャンを強制停止するには ■ ボタンをクリックします。

   Nessus は直ちに、スキャンおよびそのプロセスのすべてを終了します。

スキャンを削除する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

注意: スキャンの移動や削除は、タグベースかつユーザー固有のアクションです。たとえば、あるユーザーがスキャンを削除した場合、そのスキャンはそのユーザーでのみ、ゴミ箱フォルダーに移動します。他のユーザーでは、スキャンは元のフォルダーに残り、ゴミ箱タグが追加されて更新されます。

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 必要に応じて、左のナビゲーションバーで別のフォルダーをクリックします。
3. スキャンテーブルの、削除するスキャンに対応する行で、✕ ボタンをクリックします。

   スキャンが **[Trash]** (ゴミ箱) フォルダーに移動します。

4. スキャンを完全に削除するには、左側のナビゲーションバーの **[Trash]** (ゴミ箱) フォルダーをクリックします。

   [Trash] (ゴミ箱) ページが表示されます。

5. スキャンテーブルで、完全に削除するスキャンに対応する行の ✕ ボタンをクリックします。

   スキャンを削除してよいかを確認するダイアログボックスが表示されます。

6. **[Delete]** (削除) ボタンをクリックします。

   Tenable Nessus によりスキャンが削除されます。

ヒント: [Trash] (ゴミ箱) フォルダー内のすべてのスキャンを完全に削除するには、**[Trash** (ゴミ箱]) ページの右上隅にある **[Empty Trash]** (ゴミ箱を空にする) ボタンをクリックします。

フォルダーのスキャン

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

[Scans] (スキャン) ページの左側のナビゲーションバーは、**[Folders]** (フォルダー) セクションと [Resources] (リソース) セクションに分かれています。**[Folders]** (フォルダー) セクションには、常に次のデフォルトフォルダーがあります。これらのフォルダーは削除できません。

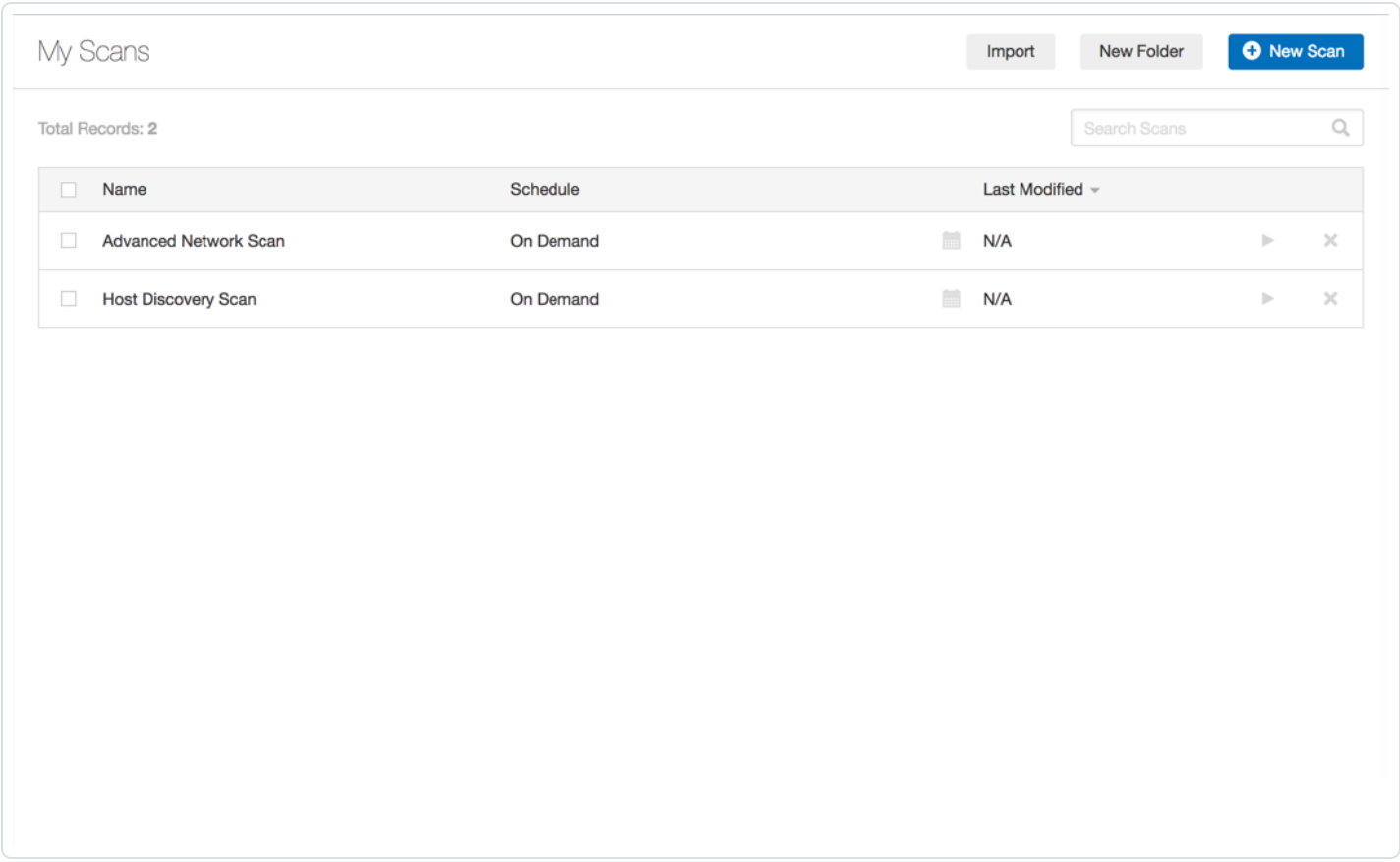
- My Scans (マイスキャン)
- すべてのスキャン
- ゴミ箱

> **注意:** すべてのスキャンフォルダーおよび関連するアクション (例: スキャンの移動や削除) は、ユーザー固有かつタグベースです。たとえば、あるユーザーが、あるスキャンを削除した場合、そのユーザーについてのみ、そのスキャンはゴミ箱フォルダーに移動します。他のユーザーについては、そのスキャンはまだ元のフォルダーにあります。Tenable Nessus はゴミ箱タグを使用してスキャンを更新します。

[Scans] (スキャン) ページにアクセスすると、**[My Scans]** (マイスキャン) フォルダーが表示されます。スキャンを作成すると、そのスキャンはデフォルトで **[My Scans]** (マイスキャン) フォルダーに表示されます。

[All Scans] (すべてのスキャン) フォルダーには、自分が作成したすべてのスキャンと、自分が操作権限を持っているすべてのスキャンが表示されます。フォルダー内のスキャンをクリックすると、スキャン結果が表示されます。

[Trash] (ゴミ箱) フォルダーには、削除したスキャンが表示されます。**[Trash]** (ゴミ箱) では、スキャンを Tenable Nessus インスタンスから完全に削除したり、選択したフォルダーに復元したりできます。スキャンが入ったフォルダーを削除すると、Tenable Nessus がそのフォルダー内のすべてのスキャンを **[Trash]** (ゴミ箱) フォルダーに移動します。Tenable Nessus は、**[Trash]** (ゴミ箱) フォルダーに保存されているスキャンを、30 日後に自動的に削除します。



次の手順を使用してスキャンフォルダーを管理します。

フォルダーを作成する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 右上隅の **[New Folder]** (新規フォルダー) ボタンをクリックします。

   [New Folder] (新規フォルダー) ウィンドウが表示されます。

3. **[Name]** (名前) ボックスに、フォルダーの名前を入力します。

4. **[Create]** (作成) ボタンをクリックします。

   Tenable Nessus により、フォルダーが作成され、左側のナビゲーションバーに表示されます。

スキャンをフォルダーに移動する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 移動するスキャンが **[My Scans]** (マイスキャン) フォルダーにない場合、左側のナビゲーションバーで、移動するスキャンが含まれるフォルダーをクリックします。

3. 設定するスキャンに対応するスキャンテーブルの行のボックスにチェックマークを入れます。

   右上隅に **[More]** (その他) ボタンが表示されます。

4. **[More]** (その他) をクリックします。**[Move To]** (移動先) を示しながら、スキャンを移動するフォルダーをクリックします。

   スキャンがそのフォルダーに移動します。

フォルダーの名前を変更する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで、名前を変更するフォルダーの横にある [▾] ボタン、**[Rename]** (名前を変更) の順にクリックします。

   [Rename Folder] (フォルダーの名前を変更する) ウィンドウが表示されます。

3. **[Name]** (名前) ボックスに新しい名前を入力します。

4. **[Save]** (保存) ボタンをクリックします。

   フォルダー名が変更されます。

フォルダーを削除する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで、削除するフォルダーの横にある [▾] ボタン、**[Delete]** (削除) の順にクリックします。

   [Delete Folder] (フォルダーを削除する) ダイアログボックスが表示されます。

3. **[Delete]** (削除) ボタンをクリックします。

   Tenable Nessus はフォルダーを削除します。フォルダーにスキャンが含まれている場合、Tenable Nessus はそれらのスキャンを **[Trash]** (ゴミ箱) フォルダーに移動します。

スキャン結果

スキャン結果を確認すると、企業のセキュリティ体制と脆弱性を把握できます。スキャンデータの表示方法は、色分けされたインジケータとカスタマイズ可能な表示オプションによってカスタマイズできます。

スキャン結果は、次のいずれかのビューで表示できます。

ページ	説明
Dashboard (ダッシュボード)	Tenable Nessus Manager では、デフォルトのスキャン結果ページには **[Dashboard]** (ダッシュボード) ビューが表示されます。
Scan Summary (スキャンサマリー)	Tenable Nessus Professional、Nessus Expert、または Tenable Nessus Manager の非 Tenable Agent で完了したスキャンのサマリーが表示されます。
Hosts (ホスト)	**[Hosts]** (ホスト) ページには、スキャンされたターゲットがすべて表示されます。
脆弱性	深刻度で分類された、特定された脆弱性の一覧です。 **ヒント:** VPR ごとに脆弱性を表示するには、テーブルヘッダーの ⚙ をクリックし、**[Disable Groups]** (グループを無効にする) をクリックして、**[VPR Score]** (VPR スコア) でテーブルをソートします。
Compliance (コンプライアンス)	スキャンにコンプライアンスチェックが含まれている場合は、このリストに、件数と詳細が脆弱性の深刻度別に表示されます。 コンプライアンススキャンが設定されている場合、⇄ ボタンにより、**[Compliance]** (コンプライアンス) と **[Vulnerability]** (脆弱性) の結果の間を移動できます。
Remediations (修正)	スキャンの結果に **[Remediation]** (修正) 情報が含まれる場合、このリストには、最も多くの脆弱性に対処する推奨された改善策が表示されます。
Notes (注意)	**[Notes]** (注意) ページには、スキャンおよびスキャンの結果に関する追加

ページ	説明
	情報が表示されます。
History (履歴)	**[History]** (履歴) には、スキャンの一覧 (**開始時刻**、**終了時刻**、**スキャンステータス**など) が表示されます。 **注意** • スキャンの履歴を削除できるのは、スキャンの所有者のみです。 • インポートされたスキャンと、Tenable Nessus が実行していない設定済みスキャンでは、スキャン履歴は使用できません。
サマリー (クラスター設定のみ)	スキャン設定内でターゲットとなるすべてのエージェントのスキャンサマリーを、クラスターノード別に整理して表示します。サマリーテーブルには、各クラスターノードの行が以下の詳細とともに表示されます。 • **Node** – ノードの名前。 • **未開始** - スキャンを開始していないエージェントの数。 • **進行中** - 現在スキャン中のエージェント数。 • **完了** - スキャンを完了して Tenable Nessus結果を に送信したエージェントの数 • **中止** - スキャンが中止されたエージェントの数。 エージェントは、スキャンが完了しなかったことを Tenable Nessus に報告するとき、**[中止]** として表示されます。スキャンは起動しない (エージェントがポリシーをダウンロードできない場合など) か、開始するものの早期に停止する (たとえば、スキャンウィンドウの終了またはエージェントが再起動する、または他の状況で完了が妨げられる場合) 可能性があります。 • **Failed** - スキャンが失敗したエージェントの数。 エージェントはスキャンジョブを受信すると**失敗**と表示されますが、Tenable Nessus はエージェントから完了ステータスを受信しません。この状態は通常、エージェントが結果を返す前にホストがオフラインになったり、接続が失われた場合に発生します。

ページ	説明
	• **Total** - スキャンジョブに含まれるエージェントの総数。
Summary (Attack Surface Discovery scan template only) (サマリー (アタックサーフェス検出スキャンテンプレートのみ))	アタックサーフェス検出スキャン設定のサマリーを表示します。サマリーテーブルには、スキャンされた各ドメインの行が以下の詳細とともに表示されます。 • **ドメイン** - スキャンされたドメイン名。 • **最初の完全プル** - スキャンされたドメインデータが利用可能であった、または利用可能になる日時。 • **データ更新** - Tenable Nessus がプルするドメインデータを Bit Discovery が最後に更新した日時。Bit Discovery は、Tenable Nessus が 90 日ごとにプルするデータを更新します。 • **次のデータ更新** - Bit Discovery でこのドメインデータが次に更新される日時。Bit Discovery は、Tenable Nessus が 90 日ごとにプルするデータを更新します。 • **ライセンスの期限切れ** - ドメインが Tenable Nessus ライセンスから期限切れになる日時。 • **レコード数** - 生成されたサブドメインレコードの数。
Records (Attack Surface Discovery scan template only) (レコード (アタックサーフェス検出スキャンテンプレートのみ))	最後のアタックサーフェス検出スキャン中に特定された DNS レコードのリストを表示します。リストには、スキャンされたすべてのドメインのレコードが最大 2,500 件まで表示されます。テーブルをフィルタリングして、特定のレコードタイプまたは特定のドメインのレコードのみを表示できます。Tenable Nessus は、各レコードについて次の情報を提供します。 • **ホスト名** - レコードのホスト名。 • **IP アドレス** - レコードに関連する IP アドレス。 • **ポート** - スキャンされた IP で検出されたオープンポート (該当する場合)。 • **タイプ** - DNS レコードタイプ。最も一般的なレコードタイプは次のとおりです。

ページ	説明
	• A - ホストアドレス • AAAA – IPv6 ホストアドレス • CNAME - エイリアスの正規名 • MX - メール交換 • NS - ネームサーバー • PTR - ポインター • SOA - 権限の開始 • SRV - サービスの場所 • TXT - テキスト • **ターゲットホスト名** - DNS レコードのターゲットとなるホスト名。多くの場合、**ホスト名**と同じです。 **[Records]** (レコード) ページには、最新のアタックサーフェス検出スキャンに関する詳細も表示されます。 • **ポリシー** - スキャンに使用されるスキャンポリシー (**ドメインの検出**)。 • **ステータス** - 現在のスキャンステータス。 • **深刻度ベース** - スキャンで使用される深刻度ベース (例: **CVSS v3.0**)。 • **スキャナー** - スキャンに使用されるスキャナー。 • **開始** - スキャンの開始日時。 • **終了** - スキャンの終了日時。 • **経過** - **開始**時間から**終了**時間までの経過時間。

Severity (深刻度)

深刻度とは、脆弱性のリスクと緊急性を分類したものです。

詳細は、CVSS スコアとVPRを参照してください。

CVSS ベースの深刻度

スキャン結果の脆弱性を表示する際、Tenable Nessus は設定に応じて CVSSv2 スコアまたは CVSSv3 スコアに基づいて深刻度を表示します。

- Tenable NessusがCVSSv2とCVSSv3のどちらのスコアを使って脆弱性の深刻度を計算するかは、デフォルトの深刻度ベースの設定で選ぶことができます。詳細は、デフォルトの深刻度ベースの設定を参照してください。
- また、特定の深刻度ベースを使用するように個別のスキャンを設定することもでき、そのスキャン結果のデフォルトの深刻度ベースは上書きされます。詳細は、個別のスキャンの深刻度ベースの設定を参照してください。

VPR

スキャン結果で脆弱性を表示すると、Tenable Nessus は VPR に基づいて深刻度を表示します。

CVSS スコアとVPR

Tenable は、脆弱性のリスクと緊急性を定量化するために、CVSS スコアと動的な Tenable で計算された VPR (脆弱性優先度格付け) (VPR) を使用しています。

CVSS

Tenable は脆弱性に関連するリスクの説明に、サードパーティーが National Vulnerability Database (NVD) から入手した共通脆弱性評価システム (CVSS) の値を使用・表示しています。CVSS スコアは脆弱性の**深刻度**と**リスクファクター**の値を基に採点されます。

> **注意:** 脆弱性の関連プラグインに CVSS 手法がある場合、**リスクファクター**はその CVSSv2 手法に基づいて計算され、CVSSv2 スコアの**深刻度**に等しくなります。プラグインに CVSS ベクトルがない場合、Tenable は**リスク要因**を単独で計算します。

CVSS ベースの深刻度

Tenable は、すべての脆弱性に静的 CVSS スコア (CVSS のバージョンは設定により異なります) に基づく深刻度 (**[Info]** (情報)、**[Low]** (注意)、**[Medium]** (警告)、**[High]** (重要)、**[Critical]** (緊急)) を割り当てます。詳しくは、深刻度の設定を参照してください。

Tenable Nessus の分析ページには、次のCVSSカテゴリに基づく脆弱性に関する概要情報が表示されます。

深刻度	CVSSv2 の範囲	CVSSv3 の範囲
緊急	プラグインの最も高い脆弱性 CVSSv2 スコアは 10.0 です。	プラグインの最も高い脆弱性 CVSSv3 スコアは 9.0 ~ 10.0 です。
重要	プラグインの最も高い脆弱性 CVSSv2 スコアは 7.0 ~ 9.9 です。	プラグインの最も高い脆弱性 CVSSv3 スコアは 7.0 ~ 8.9 です。
警告	プラグインの最も高い脆弱性 CVSSv2 スコアは 4.0 ~ 6.9 です。	プラグインの最も高い脆弱性 CVSSv3 スコアは 4.0 ~ 6.9 です。
注意	プラグインの最も高い脆弱性 CVSSv2 スコアは 0.1 ~ 3.9 です。	プラグインの最も高い脆弱性 CVSSv3 スコアは 0.1 ~ 3.9 です。
情報	プラグインの最も高い脆弱性 CVSSv2 スコアは 0 です。 -または- プラグインは脆弱性の検索を行いません。	プラグインの最も高い脆弱性 CVSSv3 スコアは 0 です。 -または- プラグインは脆弱性の検索を行いません。

CVSS ベースのリスク要因

各プラグインについて、Tenable はプラグインに関連した脆弱性の CVSS スコアを考慮し、プラグインに対して全体的なリスク要因 (**[Low]** (注意)、**[Medium]** (警告)、**[High]** (重要)、または**[Critical]** (重大)) を割り当てます。**[Vulnerability Details]** (脆弱性の詳細) ページでは、脆弱性が関連付けられているすべてのプラグインについて、最も高いリスク要因の値を表示します。

注意: 検出 (非脆弱性) プラグインおよび一部の自動化された脆弱性プラグインには、CVSS スコアが付きません。このような場合、Tenable はベンダーのアドバイザリに基づいてリスク要因を判断します。

ヒント: **[情報]** プラグインのリスク要因は **なし** になります。CVSS スコアが付いていないその他のプラグインについては、関連するセキュリティアドバイザリで提供される情報に基づいて、カスタマイズされたリスク要因が付与されます。

VPR (脆弱性優先度格付け)

Tenable は、ほとんどの脆弱性について動的な VPR を計算します。Tenable が VPR を更新して現在の脅威の状況を反映させるため、VPR は脆弱性のCVSSスコアが示すデータに、動的に追従します。VPR 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 カテゴリ	VPR 範囲
重大	9.0 ~ 10.0
高	7.0 ~ 8.9
中	4.0 ~ 6.9
低	0.1 ~ 3.9

注意: CVE がない脆弱性 (深刻度が**情報**である多くの脆弱性など) に対しては、VPR は付けられません。Tenable では、CVSS に基づく深刻度に応じてこれらの脆弱性を修復することを推奨します。

注意: VPR 値は編集できません。

注意: Nessus に表示される VPR スコアは静的であり、動的に更新されません。最新の最も正確な VPR スコアを表示するには、再スキャンする必要があります。

Tenable Nessus は、ネットワーク上で最初に脆弱性をスキャンするときに VPR値を提供します。

Tenable では、VPR が最も高い脆弱性から解決することをお勧めします。VPR スコアと概要データは次の場所に表示されます。

- VPR トップの脅威を表示するに記載されている、個別のスキャンの**VPRトップの脅威**です。
- 個別のスキャンの**トップ 10 の脆弱性**レポート。レポートの作成については、スキャンレポートを作成するを参照してください。

VPR 主な要因

脆弱性の VPR を説明する主な要因には、以下が含まれますが、これらに限定されません。

注意: Tenable は、これらの値を特定の企業向けにカスタマイズしません。VPR の主な要因は、脆弱性のグローバルな脅威の状況を反映します。

主な要因	説明

Age of Vuln	National Vulnerability Database (NVD) が脆弱性を公開してからの経過日数です。
CVSSv3 影響スコア	脆弱性に関する NVD 提供の CVSSv3 影響スコア。NVD がスコアを提供しなかった場合、Tenable Nessus では Tenableが予測したスコアが表示されます。
エクスプロイトコード成熟度	内部および外部ソース (Reversinglabs、Exploit-db、Metasploit など) の悪用インテリジェンスの存在、巧妙さ、流行に基づく、実行可能な脆弱性の悪用方法の相対的な成熟度です。可能な値 (**高**、**機能的**、**概念実証**、**未実証**) はそれぞれ、CVSS の攻撃される可能性のカテゴリに相当します。
製品影響範囲	脆弱性の影響を受ける固有の製品の相対的な数 (**注意**、**警告**、**重要**、または **最高**) です。
脅威のソース	この脆弱性に関連する脅威イベントが発生したすべてのソース (ソーシャルメディアチャネル、ダークウェブなど) のリストです。システムが過去 28 日に関連する脅威イベントを確認しなかった場合は、**[イベント記録なし]** が表示されます。
脅威の深刻度	この脆弱性に関連する、最近確認された脅威イベントの数と頻度に基づく相対的な強度 (**最低**、**注意**、**警告**、**重要**、または **最高**) です。
脅威の最新度	脆弱性の脅威イベントが発生してからの経過日数 (0 ~ 180)。

脅威イベントの例

一般的な脅威イベントには次のようなものがあります。

- 脆弱性の悪用
- 公開リポジトリにおける脆弱性の悪用コードの投稿
- メインストリームメディアにおける脆弱性のディスカッション
- 脆弱性に関するセキュリティリサーチ
- ソーシャルメディアチャネルにおける脆弱性のディスカッション
- ダークウェブとアンダーグラウンドにおける脆弱性のディスカッション
- ハッカーフォーラムにおける脆弱性のディスカッション

デフォルトの深刻度ベースの設定

注: この設定は Tenable Nessus Managerには適用されません。Tenable Nessus Manager データの脆弱性スコアは Tenable Security Center 内で **[脆弱性スコアリングシステム]** 設定を通じて管理されます。

注意: デフォルトでは、Tenable Nessus の新規インストールでは、CVSSv3 スコア (利用可能な場合) を使用して脆弱性の深刻度を計算します。既存のアップグレードされたインストールでは、以前のデフォルトの CVSSv2 スコアが維持されます。

Tenable Nessus スキャナーと Tenable Nessus Professional では、デフォルトの深刻度ベースを設定することにより、Tenable Nessus が CVSSv2 と CVSSv3 のどちらのスコア (利用可能な場合) を使って脆弱性の深刻度を計算するかを選ぶことができます。Tenable Nessus スキャナーと Tenable Nessus Professional では、デフォルトの深刻度ベースを設定することにより、Tenable Nessus が CVSSv2、CVSSv3、CVSSv4 のどのスコア (利用可能な場合) を使って脆弱性の深刻度を計算するかを選ぶことができます。デフォルトの深刻度ベースを変更すると、その変更はデフォルトの深刻度ベースで設定されている既存のスキャンすべてに適用されます。今後のスキャンでも、デフォルトの深刻度ベースが使用されます。

個別のスキャンの深刻度ベースの設定 で説明したように、特定の深刻度ベースを使用するように個別のスキャンを設定し、そのスキャンのデフォルトの深刻度ベースは上書きすることがもできます。

CVSS スコアと深刻度の範囲の詳細については、CVSS スコアとVPR を参照してください。

デフォルトの深刻度ベースを設定する方法

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで、**[Advanced]** (アドバンス) をクリックします。

   [Advanced Settings] (詳細設定) ページが表示されます。

3. **[Scanning]** (スキャン中) タブをクリックします。

   スキャンの詳細設定が表示されます。

4. **[System Default Severity Basis]** (システムのデフォルト深刻度ベース) 設定の行をクリックします。

   ヒント: 検索バーを使って、設定名の任意の部分を検索します。

   設定ウィンドウが表示されます。

5. **[Value]** (値) ドロップダウンボックスで、デフォルトの深刻度ベースとして **[CVSS v2.0]** または **[CVSS v3.0]** を選択します。

6. **[Save]** (保存) をクリックします。

   Tenable Nessus は、インスタンスのデフォルトの深刻度ベースを更新します。デフォルトの深刻度ベースの既存のスキャンが更新され、新しいデフォルトを反映します。深刻度ベースが上書きされた個別のスキャンは変更されません。

個別のスキャンの深刻度ベースの設定

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

特定の深刻度ベースを使用するように個別のスキャンを設定し、そのスキャンのデフォルトの深刻度ベースは上書きすることができます。デフォルトの深刻度ベースを変更しても、深刻度ベースが上書きされたスキャンは変更されません。

Tenable Nessus インスタンス全体でデフォルトの深刻度ベースを変更するには、デフォルトの深刻度ベースの設定を参照してください。

CVSS スコアと深刻度の範囲の詳細については、CVSS スコアとVPR を参照してください。

注意：デフォルトでは、Tenable Nessus の新規インストールでは、CVSSv3 スコア (利用可能な場合) を使用して脆弱性の深刻度を計算します。既存のアップグレードされたインストールでは、以前のデフォルトの CVSSv2 スコアが維持されます。

個別のスキャンの深刻度ベースを設定する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. スキャンの表で、深刻度ベースを変更するスキャンをクリックします。

   スキャンページが表示されます。ページの右側には、スキャンの現在の深刻度ベースなどの **[Scan Details]** (スキャンの詳細) が表示されます。

3. **[Scan Details]** (スキャンの詳細) で、現在の **[Severity Base]** (深刻度ベース) の横にある ボタンをクリックします。

   [Change Severity Rating Base] (深刻度評価ベースの変更) ウィンドウが表示されます。

4. **[Severity Rating Base]** (深刻度評価ベース) ドロップダウンボックスから、以下のいずれかを選択します。

   - **CVSS v2.0** – スキャンによって発見された脆弱性の深刻度は、CVSSv2 スコアに基づいています。この設定は、Tenable Nessus インスタンスに設定されているデフォルトの深刻度ベースよりも優先されます。
   - **CVSS v3.0** – スキャンによって発見された脆弱性の深刻度は、CVSSv3 スコアに基づいています。この設定は、Tenable Nessus インスタンスに設定されているデフォルトの深刻度ベースよりも優先されます。
   - **デフォルト** – スキャンで発見された脆弱性の深刻度は、Tenable Nessus デフォルトの深刻度ベースを使用しており、これは括弧内に表示されます。後で[デフォルトの深刻度ベースを変更した]場合、スキャンは自動的に新しいデフォルトの深刻度ベースを使用します。

5. **[Save]** (保存) をクリックします。

   Tenable Nessus は、スキャンの深刻度ベースを更新します。スキャン結果が更新され、更新された深刻度を反映します。

スキャン結果から新しいスキャンを作成する

> **を使用する場合に必要な [ユーザーロール]Tenable Nessus Manager:** Standard、Administrator、System Administrator

スキャン結果を表示し、スキャンされたホストを選択して新しいスキャンのターゲットにできます。新しいスキャンの作成時には、Tenable Nessus が選択したホストをターゲットに自動入力します。

スキャン結果から新しいスキャンを作成する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. スキャンテーブルで、完了したスキャンの行をクリックします。

   スキャンの結果ページが表示されます。

3. **[Hosts]** (ホスト) タブをクリックします。

   Tenable Nessusでスキャンされたホストのテーブルが表示されます。

4. 新しいスキャンでスキャンする各ホストの横にあるチェックボックスを選択します。

   ページの上部に **[More]** (その他) ボタンが表示されます。

5. **[More]** (その他) ボタンをクリックします。

   ドロップダウンボックスが表示されます。

6. **[Create Scan]** (スキャンの作成) をクリックします。

   [Scan Templates] (スキャンテンプレート) ページが表示されます。

7. 新しいスキャンのスキャンテンプレートを選択します。

   Tenable Nessusで、事前に選択したホストが **[Targets]** (ターゲット) リストに自動入力されます。

8. 「スキャン設定とポリシー設定」の説明に従い、残りのスキャン設定を行います。

9. 次のいずれかを行います。

   - すぐにスキャンを起動するには、▾ボタンをクリックし、**[Launch]** (起動) をクリックします。

     Tenable Nessus がスキャンを保存して起動します。

   - スキャンを後で起動するには、**[Save]** (保存) ボタンをクリックします。

     Tenable Nessus
     がスキャンを保存します。

結果の検索とフィルタリング

> **を使用する場合に必要なユーザーロールTenable Nessus Manager:** Basic、Standard、Administrator、System Administrator

検索またはフィルタリングにより特定のスキャン結果を表示できます。ホストや脆弱性をフィルタリングしたり、複数のフィルターを使用して詳細でカスタマイズされたスキャン結果のビューを作成したりできます。

ホストを検索する

1. スキャン結果で、**[Hosts]** (ホスト) タブをクリックします。

   アタックサーフェス検出スキャンを使用している場合は、**[Records]** (レコード) タブをクリックします。

2. ホストテーブルの上部にある **[Search Hosts]** (ホストの検索) ボックスに、ホスト名の一致をフィルタリングするためのテキストを入力します。

   入力テキストに基づいた検索結果が自動でフィルタリングされます。

脆弱性を検索する

1. 次のいずれかを実行します。

   - スキャン結果の **[Hosts]** (ホスト) タブで、特定のホストをクリックするとその脆弱性が表示されます。
   - スキャン結果で **[Vulnerabilities]** (脆弱性) タブをクリックすると、すべての脆弱性が表示されます。

2. 脆弱性一覧の上にある **[Search Vulnerabilities]** (脆弱性の検索) ボックスで、脆弱性のタイトルの検索テキストを入力します。

   入力テキストに基づいた検索結果が自動でフィルタリングされます。

フィルターを作成する

1. 次のいずれかを実行します。

   - スキャン結果で、**[Hosts]** (ホスト) タブをクリックします。
   - スキャン結果の **[Hosts]** (ホスト) タブで、特定のホストをクリックするとその脆弱性が表示されます。
   - スキャン結果で **[Vulnerabilities]** (脆弱性) タブをクリックすると、すべての脆弱性が表示されます。
   - アタックサーフェス検出スキャンの結果で、**[Records]** (レコード) タブをクリックして、すべての DNS レコードを表示します。

2. 検索ボックスの横にある **[Filters]** (フィルター) をクリックします。

   - 保存したフィルターがある場合は、保存したフィルターのリストが表示されます。**[Custom]** (カスタム) をクリックして **[Filters]** (フィルター) ウィンドウを開き、新しいフィルターを作成するか、保存したフィルターをクリックしてテーブルに適用します。
   - 保存したフィルターがない場合、**[Filters]** (フィルター) ウィンドウが表示されます。

3. 次のいずれかのフィルタールールオプションを指定します。

   - **Match Any or Match All: [All]** (すべて) を選択すると、すべてのフィルターに一致する結果のみが表示されます。**[Any]** (任意) を選択すると、設定されたフィルターのいずれかに一致する結果が表示されます。
   - **プラグイン属性:** プラグイン属性に関する説明は、プラグイン属性 の表を参照してください。
   - **Filter argument:** 選択したプラグイン属性のフィルタリング方法を、**[is equal to]** (次の値に等しい)、**[is not equal to]** (次の値に等しくない)、**[contains]** (次を含む)、**[does not contain]** (次を含まない) から指定します。
   - **Value :** 選択したプラグイン属性に応じて、値を入力するか、ドロップダウンメニューから値を選択します。

4. (オプション) 別のフィルタールールを追加するには、⊕ をクリックします。

5. (オプション) 次の手順を実行して、後で使用するためにフィルターを保存します。

   a. **[Save this filter]** (このフィルターを保存する) チェックボックスを選択して、1 つまたは複数のフィルターを保存します。

      [Filter name] (フィルター名) ボックスが表示されます。

   b. フィルターの名前を入力します。

   c. **[Save]** (保存) をクリックします。

      テーブルの **[Filter]** (フィルター) ボタンをクリックして、保存したフィルターを選択できるようになりました。

      > **注意:** フィルターを保存できるのは、**[Hosts]** (ホスト)、**[Vulnerabilities]** (脆弱性)、および **[Records]** (レコード) テーブルのみです。

6. **[Apply]** (適用) をクリックします。

   Tenable Nessus によりフィルターが適用され、フィルターに一致する脆弱性またはレコードがテーブルに表示されます。

保存したフィルターを管理する

1. 次のいずれかを実行します。

   - スキャン結果で、**[Hosts]** (ホスト) タブをクリックします。
   - スキャン結果の **[Hosts]** (ホスト) タブで、特定のホストをクリックするとその脆弱性が表示されます。
   - スキャン結果で **[Vulnerabilities]** (脆弱性) タブをクリックすると、すべての脆弱性が表示されます。

2. 検索ボックスの横にある **[Filter]** (フィルター) をクリックします。

   保存したフィルターのリストが表示されます。

3. 次のいずれかを行います。

   - フィルター名をクリックして、フィルターをテーブルに適用します。
   - ボタンをクリックして、フィルター条件を編集します。

     [Filters] (フィルター) ウィンドウが表示されます。条件を編集し、**[Save]** (保存) をクリックします。

   - ボタンをクリックして、重複する保存済みフィルターを作成します。

     これで、表の **[Filter]** (フィルター) ボタンから、保存したフィルターのコピーを選択して編集できるようになります。

   - ボタンをクリックして、保存したフィルターを削除します。

     [Delete Filter] (フィルターの削除) ウィンドウが表示されます。**[Continue]** (続行) をクリックして、削除を確定します。

適用されているフィルターをクリアする

1. 検索ボックスの横にある **[Filter]** (フィルター) をクリックします。

   [Filter] (フィルター) ウィンドウが表示されます。

2. フィルターを 1 つ解除する場合は、そのフィルター項目の横にある をクリックします。

3. フィルターをすべて解除する場合は、**[Clear Filters]** (フィルターをクリア) をクリックします。

   Tenable Nessus により、テーブルの脆弱性表示からフィルターが解除されます。

プラグイン属性

次の表は、結果のフィルターに使用できるプラグイン属性を示しています。

ヒント: Tenable Nessus プラグインの属性の多くは、深刻度と脆弱性スコアに関連しています。深刻度と脆弱性スコアの詳細については、Severity (深刻度)および CVSS スコアとVPR を参照してください。

オプション	説明
Bugtraq ID	Bugtraq ID を指定された文字列 (例: 51300) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CANVAS Exploit Framework (CANVAS エクスプロイトフレームワーク)	CANVAS エクスプロイトフレームワークにエクスプロイトが存在する (true) か存在しない (false) かの基準で、結果をフィルタリングします。
CANVAS Package (CANVAS パッケージ)	エクスプロイトが存在する CANVAS エクスプロイトフレームワークパッケージに基づいて結果をフィルタリングします。パッケージには CANVAS、D2ExploitPack、White_Phosphorus などがあります。
CERT Advisory ID (CERT アドバイザリ ID)	CERT アドバイザリ ID (現在は「テクニカルサイバーセキュリティアラート」と呼ばれる) を指定された文字列 (例: TA12-010A) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CORE Exploit Framework (CORE エクスプロイトフレームワーク)	CORE エクスプロイトフレームワークにエクスプロイトが存在する (true) か存在しない (false) かの基準で、結果をフィルタリングします。
CPE	Common Platform Enumeration (CPE) を指定された文字列 (例: Solaris) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。

オプション	説明
CVE	CVE v2.0 参照を指定された文字列 (例: 2011-0123) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CVSS Base Score (CVSS ベーススコア)	CVSS v2.0 ベーススコアを文字列 (例: 5) と比較し、より小さい (is less than)、より大きい (is more than)、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。 このフィルターを使用すると、リスクのレベルで選択できます。深刻度のレベルは CVSS スコアと関連付けられており、スコアが 0 は情報、1 ~ 3 は注意、4 ~ 6 は警告、7 ~ 9 は重要、10 は緊急となります。
CVSS Temporal Score (CVSS 一時スコア)	CVSS v2.0 一時スコアを文字列 (例: 3.3) と比較し、より小さい (is less than)、より大きい (is more than)、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CVSS Temporal Vector (CVSS 一時ベクトル)	CVSS v.2.0 一時ベクトルを指定された文字列 (例 : E:F) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CVSS Vector (CVSS ベクトル)	CVSS v.2.0 ベクトルを指定された文字列 (例 : AV:N) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CVSS 3.0 Base Score (CVSS ベーススコア)	CVSS v3.0 ベーススコアを文字列 (例: 5) と比較し、より小さい (is less than)、より大きい (is more than)、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。 このフィルターを使用すると、リスクのレベルで選択できます。深刻度のレベルは CVSS スコアと関連付けられており、スコアが 0 は情報、1 ~ 3 は注意、4 ~ 6 は警告、7 ~ 9 は重要、10 は緊急となります。
CVSS 3.0 Temporal Score	CVSS v3.0 一時スコアを文字列 (例: 3.3) と比較し、より小さい (is less than)、より大きい (is more than)、等しい (is equal to)、等しくない (is not

オプション	説明
(CVSS 3.0 一時スコア)	equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CVSS 3.0 Temporal Vector (CVSS 3.0 一時ベクトル)	CVSS v.3.0 一時ベクトルを指定された文字列 (例 : E:F) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CVSS 3.0 Vector (CVSS 3.0 ベクトル)	CVSS v.3.0 ベクトルを指定された文字列 (例 : AV:N) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
CWE	CVSS ベクトルを CWE 参照番号 (例: 200) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Exploit Available (公開済みのエクスプロイト)	脆弱性に公開済みの既知のエクスプロイトがあるかどうかの基準でフィルタリングします。
Exploit Database ID (エクスプロイトデータベース ID)	エクスプロイトデータベース ID (EDB-ID) を指定された文字列 (例: 18380) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Exploitability Ease (悪用のしやすさ)	悪用のしやすさと次の値を比較し、等しい (is equal to)、等しくない (is not equal to) のいずれかの基準でフィルタリングします。値: 利用可能なエクスプロイトあり、エクスプロイト不要、既知のエクスプロイトなし。
Exploited by Malware (マルウェアによって悪用可能)	脆弱性がマルウェアによって悪用可能である (true) か悪用可能ではない (false) かの基準で、結果をフィルタリングします。
Exploited by	プラグインが実際のエクスプロイトを実行するかどうかという基準でフィルタリング

オプション	説明
Nessus (Nessus によって悪用可能)	します。通常は ACT_ATTACK プラグインです。
Hostname (ホスト名)	ホストを指定された文字列 (例: 192.168 または lab) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。エージェントは、エージェントターゲット名を使用して検索できます。その他のターゲットについては、スキャンの設定内容に応じて、ターゲットの IP アドレスまたは DNS 名で検索できます。
IAVA	IAVA 参照を指定された文字列 (例: 2012-A-0008) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
IAVB	IAVB 参照を指定された文字列 (例: 2012-A-0008) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
IAVM Severity (IAVM 深刻度レベル)	IAVM 深刻度レベル (例: IV) でフィルタリングします。
In The News (ニュース内)	プラグインがカバーする脆弱性がニュースで報道されたかどうかという基準でフィルタリングします。
Malware (マルウェア)	プラグインがマルウェアを検出するかどうかという基準でフィルタリングします。通常は ACT_GATHER_INFO プラグインです。
Metasploit Exploit Framework (Metasploit エクスプロイトフレームワーク)	Metasploit エクスプロイトフレームワークに脆弱性が存在する (true) か存在しない (false) かの基準で、結果をフィルタリングします。
Metasploit Name	Metasploit 名を指定された文字列 (例: xslt_password_reset) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does

オプション	説明
(Metasploit 名)	not contain) のいずれかの基準でフィルタリングします。
Microsoft Bulletin (Microsoft 掲示板)	Microsoft セキュリティ情報の番号で結果をフィルタリングします。この形式は MSXX-XXX で X の部分は数字です (例: MS17-09)。
Microsoft KB	Microsoft ナレッジベースの記事とセキュリティアドバイザリでフィルタリングします。
OSVDB ID	オープンソース脆弱性データベース (OSVDB) を指定された文字列 (例: 78300) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Patch Publication Date (パッチ公開日)	脆弱性パッチ公開日を文字列 (例: 12/01/2011) と比較し、より小さい (is less than)、より大きい (is more than)、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Plugin Description (プラグインの説明)	Plugin Description が指定された文字列 (例: リモート) を含むか (contains) 含まないか (does not contain) で、結果がフィルタリングされます。
Plugin Family (プラグインファミリー)	Plugin Name が、指定された Nessus プラグインファミリーと等しいか (is equal) 等しくないか (is not equal to) で、結果がフィルタリングされます。Tenable Nessus は、一致候補をドロップダウンメニューで表示します。
Plugin ID (プラグイン ID)	プラグイン ID が、指定された文字列 (例: 42111) と等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかで、結果がフィルタリングされます。
Plugin Modification Date (プラグイン修正日)	Nessus プラグイン修正日を文字列 (例: 02/14/2010) と比較し、より小さい (is less than)、より大きい (is more than)、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Plugin Name (プ	プラグイン名を指定された文字列 (例: windows) と比較し、等しい (is equal

オプション	説明
ラグイン名)	to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Plugin Output (プラグイン出力)	プラグインの説明を指定された文字列 (例: PHP) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Plugin Publication Date (プラグイン公開日)	Nessus プラグイン公開日を文字列 (例: 06/03/2011) と比較し、より小さい (is less than)、より大きい (is more than)、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Plugin Type (プラグインタイプ)	プラグインタイプをローカルまたはリモートの 2 種類のプラグインタイプと比較し、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Port (ポート)	ポートを指定された文字列 (例: 80) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Protocol (プロトコル)	プロトコルを指定された文字列 (例: HTTP) と比較し、等しい (is equal to)、等しくない (is not equal to) のいずれかの基準でフィルタリングします。
Risk Factor (リスク要因)	脆弱性のリスク要因 (例: 注意、警告、重要、緊急) の基準でフィルタリングします。
Secunia ID	Secunia ID を指定した文字列 (例: 47650) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
See Also (いずれかの基準)	Nessus プラグインを指定された文字列 (例: seclists.org) と比較し、等しい (is equal to)、等しくない (is not equal to)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
Solution (ソリューション)	プラグイン解決策を指定された文字列 (例: アップグレード) と比較し、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。

オプション	説明
Synopsis	プラグイン解決策を指定された文字列 (例: PHP) と比較し、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。
VPR Score (VPR スコア)	脆弱性 VPR スコアが値と等しい、等しくない、含む、含まない、より小さい、またはより大きい (たとえば、VPR スコアが 8.0 より大きい) かどうかに基づいて結果をフィルタリングします。
Vulnerability Publication Date (脆弱性公開日)	脆弱性公開日を文字列 (例: 01/01/2012) と比較し、以前 (earlier than)、以降 (later than)、一致する (on)、一致しない (not on)、含む (contains)、含まない (does not contain) のいずれかの基準でフィルタリングします。 **注意:** 日付の横にあるボタンを押すとカレンダーのインターフェースが表示され、日付を簡単に選択できます。

スキャン結果を比較する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Basic、Standard、Administrator、System Administrator

2 つのスキャン結果を比較して、その違いを確認できます。この比較は、2 つの結果の真の差分を示していません。古いベースラインスキャンと新しいスキャンの間で Tenable Nessus により検出された新しい脆弱性が表示されます。

スキャン結果を比較すると、特定のシステムまたはネットワークの経時的な変化を確認できます。この情報は、脆弱性がどのように修正されているか、Tenable Nessus により新しい脆弱性が検出されたときにシステムにパッチが適用されているか、または 2 つのスキャンが同じホストをターゲットにしていないかを示すことにより、コンプライアンス分析に役立ちます。

注意: インポートされたスキャンや 3 つ以上のスキャンを比較することはできません。

スキャン結果を比較する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. スキャンをクリックします。

3. **[History]** (履歴) タブをクリックします。

4. 比較する両方のスキャン結果の行で、チェックボックスを選択します。

5. 右上の **[Diff]** (差分) をクリックします。

   [Choose Primary Result] (主要な結果を選択) ウィンドウが表示されます。

6. ドロップダウンボックスで、主要な結果であるスキャン結果を選択します。

   主要な結果は差分ベースラインです。スキャン差分には、Tenable Nessus により非ベースラインスキャンで検出された脆弱性が表示されます。

   > **ヒント:** Tenable では、2 つのスキャン結果の真の差分を表示するために、差分を 2 回生成することを推奨します。古いスキャン結果をベースラインとして使用して 1 回生成し、新しいスキャン結果をベースラインとして使用してもう 1 回生成します。これにより、いずれかのスキャン結果でのみ検出された脆弱性を確認できます。

7. **[Continue]** (続行) をクリックします。

   スキャン差分が表示されます。この差分では、ベースラインスキャン以降に非ベースラインスキャンで脆弱性が検出されたホストが **[Hosts]** (ホスト) タブに表示され、検出された脆弱性が **[Vulnerabilities]** (脆弱性) タブに表示されます。

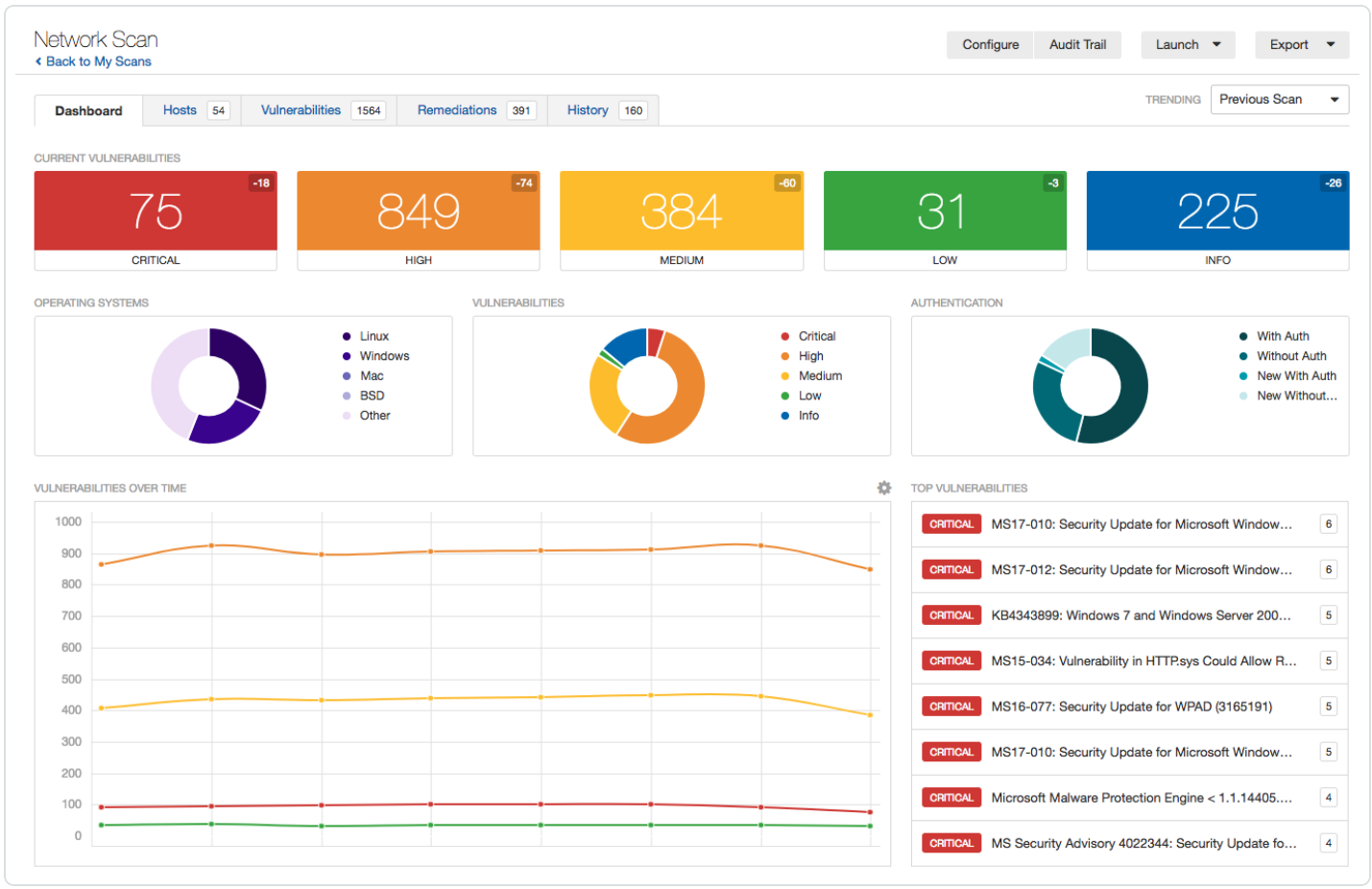
   スキャン差分のレポートを生成できます。詳細は、スキャンレポートを作成するの手順 4 を参照してください。

Dashboard (ダッシュボード)

Tenable Nessus Manager では、スキャンの結果をインタラクティブなダッシュボードビューで表示するようにスキャンを設定できます。

> **注意:** この機能は、非クラスタ化されたマネージャー設定でのみ利用可能です。

実行されたスキャンのタイプと収集されたデータのタイプに基づいて、ダッシュボードにキー値と傾向インジケータが表示されます。



ダッシュボードビュー

実行されたスキャンのタイプと収集されたデータのタイプに基づいて、ダッシュボードにキー値と傾向インジケータが表示されます。

ダッシュボードの詳細

Name (名前)	説明
Current Vulnerabilities (最新の脆弱性)	スキャンによって特定された脆弱性の数 (深刻度別)。
Operating System Comparison (オペレーティングシステムの比較)	スキャンによって特定されたオペレーティングシステムの割合。
Vulnerability	スキャンによって特定されたすべての脆弱性の割合 (深刻度別)。

Comparison (脆弱性の比較)	
Host Count Comparison (ホスト数の比較)	認証情報を使用した認証タイプと認証情報を使用しない認証タイプ (認証なし、認証なしの新規、認証あり、認証ありの新規)によってスキャンされたホストの割合。
Vulnerabilities Over Time (時間の経過に伴う脆弱性)	ある期間に見つかった脆弱性です。このチャートを表示するには、スキャンを少なくとも 2 回実行する必要があります。
Top Hosts (上位のホスト)	スキャンで見つかった脆弱性の数が多い上位 8 つのホスト。
Top Vulnerabilities (上位の脆弱性)	深刻度に基づく上位 8 つの脆弱性。

スキャンサマリーの表示

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Basic、Standard、Administrator、System Administrator

Tenable Nessus Manager の非エージェントスキャン、あるいは Tenable Nessus Professional または Tenable Nessus Expert のスキャンのサマリーを表示できます。スキャンサマリーには、次の情報が表示されます。

サマリーセクション	説明
Scan Details (スキャンの詳細)	スキャン中に検出された重要度高、重要度中、重要度低の脆弱性の数。
Details (詳細)	スキャン名、使用されたスキャンのプラグインセット、スキャンの CVSS スコア (詳細については CVSS スコアとVPR を参照)、スキャンのテンプレート、およびスキャンの開始と終了の時刻。
Authentication/Credential Info (Hosts) (認証/認証情報 (ホスト))	スキャン時に認証に成功/失敗したホストの数。
Scan Durations (スキャンに要した時間)	スキャンに要した時間、ホストごとのスキャン時間の中央値、最大スキャン時間。

Plugin Families Enabled/Disabled (プラグインファミリーの有効/無効)	Tenable Nessus がスキャンを有効または無効にしたプラグインファミリーのリスト。 **注意:** このセクションは、基本的なネットワークスキャンでは表示されません。
Plugin Rules Applied (適用されたプラグインルール)	スキャンに適用されたプラグインルールのリスト。Tenable Nessus がプラグインルールを適用しなかった場合、このセクションは表示されません。
Policy Details (ポリシーの詳細)	スキャンの基本、評価、レポート、詳細、認証情報、ポートスキャナー、脆弱なデバイスの設定。 • 基本、評価、レポート、詳細スキャンの設定の詳細については、スキャン設定とポリシー設定 を参照してください。 • ポートスキャナと脆弱なデバイス設定の詳細については、検出スキャン設定 を参照してください。

注意: スキャンの進行中は、**[Scan Summary]** (スキャンサマリー) タブは表示されません。

スキャンのサマリーを表示する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. サマリーを表示するスキャンをクリックします。

   スキャンの結果ページが表示されます。

3. **[Scan Summary]** (スキャンサマリー) タブをクリックします。

   [Scan Summary] (スキャンサマリー) ページが表示されます。

脆弱性

脆弱性は、プラグインによって発見された潜在的なセキュリティ問題のインスタンスです。スキャン結果では、スキャンで見つかったすべての脆弱性を表示するか、特定のホストで見つかった脆弱性を表示するかを選択できます。

脆弱性ビュー	パス
All vulnerabilities detected by a scan (スキャンによって検出されたすべての脆弱性)	**[Scans]** (スキャン) > *[scan name]* (スキャン名) > **[Vulnerabilities]** (脆弱性)
Vulnerabilities detected by a scan on a specific host (スキャンによって検出された特定のホストの脆弱性)	**[Scans]** (スキャン) > **[Hosts]** (ホスト) > *[scan name]* (スキャン名)

脆弱性を管理するには、次の手順に従います。

脆弱性を表示する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Basic、Standard、Administrator、System Administrator

スキャンで見つかったすべての脆弱性、またはスキャンで見つかった特定のホストの脆弱性を表示できます。脆弱性をドリルダウンすると、プラグインの詳細、説明、ソリューション、出力、リスクの情報、脆弱性情報、参照情報などの情報を表示できます。

ヒント: VPR ごとに脆弱性を表示するには、テーブルヘッダーの ⚙ をクリックし、**[Disable Groups]** (グループを無効にする) をクリックして、**[VPR Score]** (VPR スコア) でテーブルをソートします。

脆弱性を表示する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 脆弱性を表示するスキャンをクリックします。

   スキャンの結果ページが表示されます。

3. 次のいずれかを行います。

   - 特定のホストの脆弱性を表示するには、そのホストをクリックします。
   - すべての脆弱性を表示するには、**[Vulnerabilities]** (脆弱性) タブをクリックします。

     [Vulnerabilities] (脆弱性) タブが表示されます。

4. (オプション) 脆弱性をソートするには、テーブルヘッダー行の属性をクリックして、その属性でソートします。

5. 脆弱性の詳細を表示するには、脆弱性の行をクリックします。

   [Vulnerability Details] (脆弱性の詳細) ページが表示され、ホストの各インスタンスのプラグイン情報と出力が表示されます。

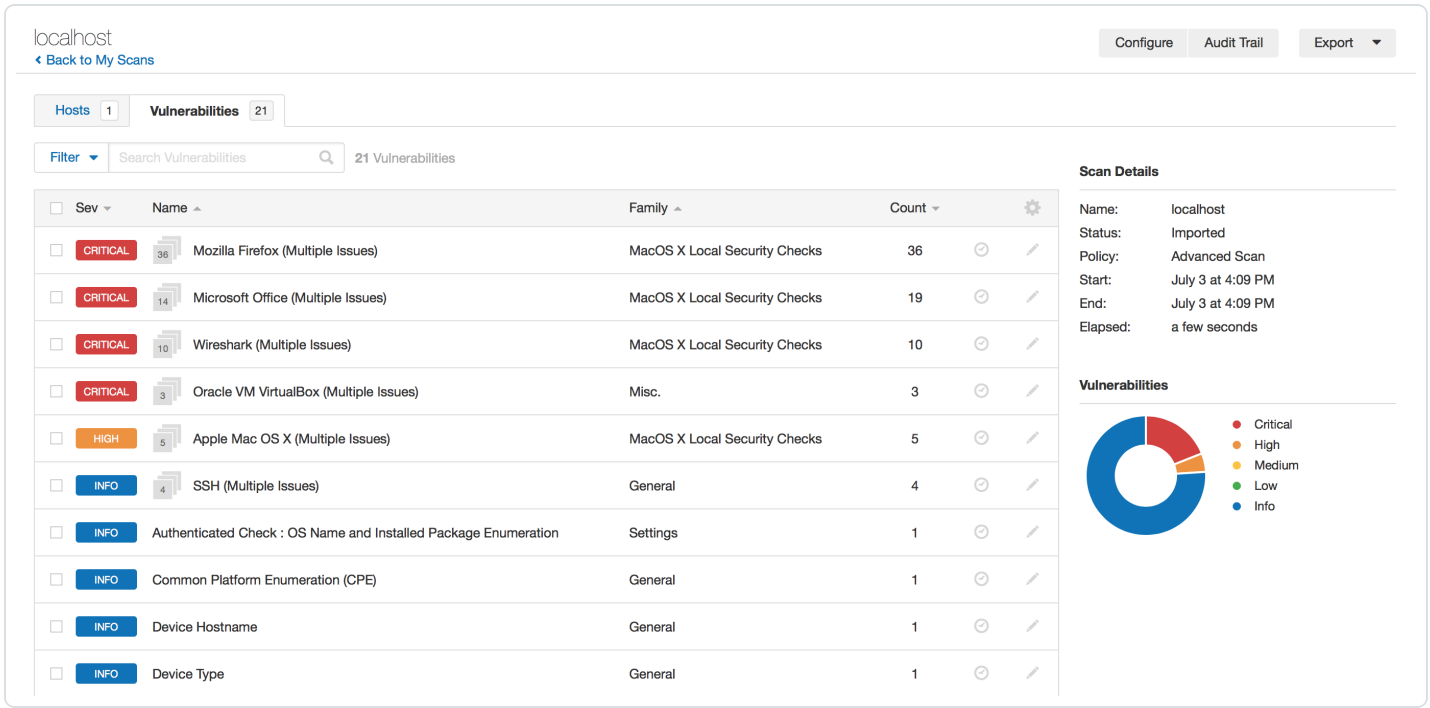
脆弱性をグループ化する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Basic、Standard、Administrator、System Administrator

脆弱性をグループ化すると、Common Platform Enumeration (CPE)、サービス、アプリケーション、プロトコルなどの一般的な属性を持つプラグインがスキャン結果の 1 つの行にまとめられます。脆弱性をグループ化すると、結果のリストが短くなり、関連する脆弱性が一緒に表示されます。

グループが有効になっている場合、グループ内の脆弱性の数が深刻度インジケーターの横に表示され、グループ名に **(Multiple Issues)** と表示されます。

グループの深刻度インジケーターは、グループ内の脆弱性に基づいています。グループ内のすべての脆弱性の深刻度が同じである場合は、Tenable Nessus にその深刻度レベルが表示されます。グループ内の脆弱性の深刻度が異なる場合は、Tenable Nessus の深刻度レベルに **[Mixed]** (混在) と表示されます。



脆弱性をグループ化するには

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 脆弱性を表示するスキャンをクリックします。

   スキャンの結果ページが表示されます。

3. 次のいずれかを行います。

   - 特定のホストをクリックし、そのホストで見つかった脆弱性を表示します。

     -または-

   - **[Vulnerabilities]** (脆弱性) タブをクリックして、すべての脆弱性を表示します。

   [Vulnerabilities] (脆弱性) タブが表示されます。

4. 脆弱性テーブルのヘッダー行で、⚙ をクリックします。

   > **注意:** グループ化できる脆弱性がある場合にのみ、cog アイコン (⚙) が表示されます。

5. **[Enable Groups]** (グループを有効にする) をクリックします。

   Tenable Nessus によって類似した脆弱性が 1 つの行にグループ化されます。

脆弱性のグループ化を解除する方法

1. 脆弱性テーブルのヘッダー行で、⚙ をクリックします。

   > **注意:** グループ化できる脆弱性がある場合にのみ、cog アイコン (⚙) が表示されます。

2. **[Disable Groups]** (グループを無効にする) をクリックします。

   脆弱性がそれぞれの行に表示されます。

グループ内の脆弱性を表示する方法

- 脆弱性テーブルで、脆弱性グループ行をクリックします。

  新しい脆弱性テーブルが開き、グループ内の脆弱性が表示されます。

グループの深刻度タイプを、グループ内で最も高い深刻度に設定するには

- 詳細な設定の scans_vulnerability_groups_mixed を no に設定します。

脆弱性を変更する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

深刻度レベルを変更したり、非表示にしたりして、脆弱性を変更できます。これにより結果の深刻度の優先順位を見直し、企業のセキュリティスタンスと応答計画への適合性を向上することができます。スキャン結果ページから脆弱性を変更すると、その後のすべてのスキャンに変更を適用するように指定しない限り、対象スキャンの脆弱性インスタンスのみに変更が適用されます。すべての脆弱性の深刻度レベルを変更するには、プラグインルールを使用します。

脆弱性を変更する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 脆弱性を表示するスキャンをクリックします。

   スキャンの結果ページが表示されます。

3. 次のいずれかを行います。

   - 特定のホストをクリックし、そのホストで見つかった脆弱性を表示します。
   - **[Vulnerabilities]** (脆弱性) タブをクリックして、すべての脆弱性を表示します。

     [Vulnerabilities] (脆弱性) タブが表示されます。

4. 変更する脆弱性の行で、✎ をクリックします。

   [Modify Vulnerability] (脆弱性を変更する) ウィンドウが表示されます。

5. **[Severity]** (深刻度) ドロップダウンボックスで、深刻度または **[Hide this result]** (この結果を非表示にする) を選択します。

   注意: 脆弱性を非表示にすると元に戻せないため、付随するリスクを受け入れたうえでこの操作を行ってください。脆弱性を一時的に非表示にするには、脆弱性のスヌーズを使用します。

6. (オプション) **[Apply this rule to all future scans]** (このルールを今後のスキャンに適用する) を選択します。

   このオプションを選択すると、Tenable Nessus では今後実行されるすべてのスキャンにこの脆弱性ルールが適用されます。Tenable Nessus が過去のスキャンで検出された脆弱性を変更することはありません。

7. **[Save]** (保存) をクリックします。

   Tenable Nessus により、指定した設定を使用して脆弱性が更新されます。

脆弱性をスヌーズする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Basic、Standard、Administrator、System Administrator

脆弱性をスヌーズすると、スキャン結果のデフォルトビューに表示されなくなります。脆弱性がスヌーズされる期間を選択します。そのスヌーズ期間が終了すると、脆弱性は元のようにスキャン結果のリストに表示されます。また、手動で脆弱性のスヌーズを解除したり、スヌーズされた脆弱性を表示したりすることも可能です。スヌーズは、特定のスキャンにおける脆弱性のすべてのインスタンスに影響するため、特定のホストを指定して脆弱性をスヌーズすることはできません。

脆弱性をスヌーズする場合、作業中のスキャン結果の脆弱性のみをスヌーズします。この脆弱性は、他の既存のスキャン結果や今後のスキャン結果にも表示されます。

脆弱性をスヌーズする方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 脆弱性を表示するスキャンをクリックします。

   スキャンの結果ページが表示されます。

3. 次のいずれかを行います。

   - 特定のホストをクリックし、そのホストで見つかった脆弱性を表示します。

     -または-

- **[Vulnerabilities]** (脆弱性) タブをクリックして、すべての脆弱性を表示します。

  [Vulnerabilities] (脆弱性) タブが表示されます。

4. スヌーズする脆弱性の行で、 をクリックします。

   [Snooze for] (スヌーズする) ドロップダウンボックスが表示されます。

5. 脆弱性をスヌーズする期間を選択します。

   - **[1 Day]** (1 日)、**[1 Week]** (1 週)、**[1 Month]** (1 月) から選択します。

     -または-

   - **[Custom]** (カスタム) をクリックします。

   [Snooze Vulnerability] (脆弱性のスヌーズ) ウィンドウが表示されます。

6. **[Snooze Vulnerability]** (脆弱性のスヌーズ) ウィンドウで

   - 既定のスヌーズ期間を選択する場合は、**[Snooze]** (スヌーズ) をクリックして選択を確定します。
   - スヌーズ期間をカスタマイズする場合は、脆弱性をスヌーズする日付を選択し、**[Snooze]** (スヌーズ) をクリックします。

   Tenable Nessus は、選択した期間の間は脆弱性をスヌーズし、スキャン結果のデフォルトビューに表示しません。

スヌーズされた脆弱性を表示するには

1. 脆弱性テーブルのヘッダー行で、 をクリックします。

   ドロップダウンボックスが表示されます。

2. **[Show Snoozed]** (スヌーズを表示) をクリックします。

   スヌーズされた脆弱性がスキャン結果に表示されます。

スヌーズされた脆弱性を元に戻す方法

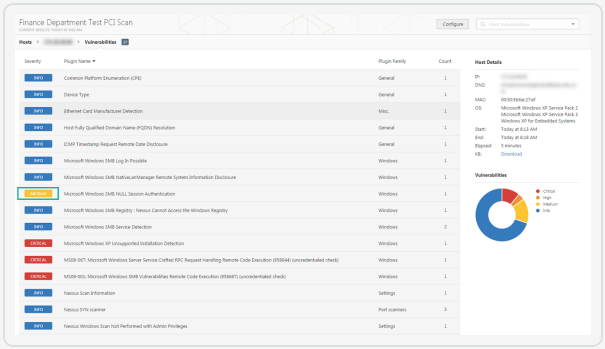
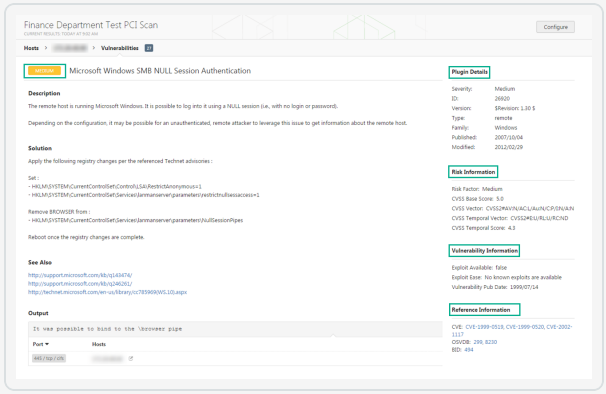
1. スヌーズされた脆弱性の列で、 をクリックします。

   [Wake Vulnerability] (脆弱性の通知) ウィンドウが表示されます。

2. **[Wake]** (通知) をクリックします。

   脆弱性のスヌーズが解除され、スキャン結果のデフォルトリストに表示されます。

脆弱性情報の例

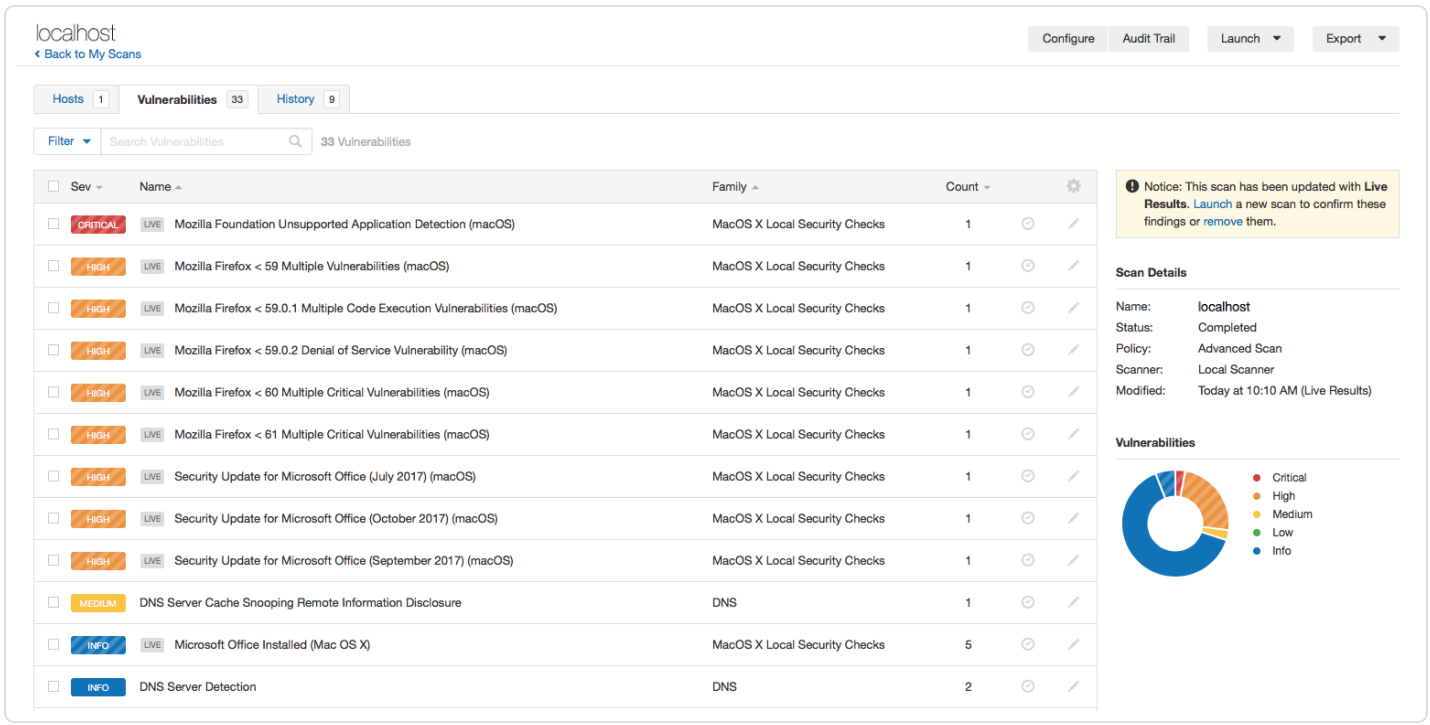
プラグインの深刻度とプラグイン名ごとの単一ホストのスキャン結果リスト	単一ホストのプラグインスキャン結果の詳細
	

ライブ結果

Tenable Nessus は新しいプラグインで自動的に更新され、これにより、新たな脆弱性が資産に存在するかどうかを評価できるようになります。ただし、スキャン日程の間隔が長い場合、プラグインが更新されてから数日経つまでスキャンで新規プラグインが実行されない可能性があります。こうした遅れにより、気付かないうちに資産が脆弱性にさらされる可能性があります。

Nessus Professional と Nessus Expert には、スキャンで収集された最新データを活用して新規プラグインのスキャン結果を閲覧できる *Live Results* 機能が備わっており、新たにスキャンを実行する必要がありません。Live Results により、新たな脅威の兆候を検出し、その調査結果を確認するために手動でスキャンを開始する必要があるかどうかを判断できます。Live Results は、アクティブスキャンの結果とは異なり、すでに収集されたデータに基づく評価です。Live Results では、エクスプロイトなどのアクティブな検出や以前に収集されていないデータを必要とする新しいプラグインの結果は生成されません。

Live Results のスキャン結果には各色のストライプが入っています。**[Vulnerabilities]** (脆弱性) タブの深刻度はストライプ入りで、**[Live]** (ライブ) アイコンがプラグイン名の横に表示されます。



結果ページには、結果にライブ結果が含まれていることを示す注意書きが表示されます。Tenable では、検出項目を確認するために手動スキャンを開始することを推奨しています。各アクティブスキャンの間隔が長いほど、データの鮮度は低下する傾向があり、ライブ結果の効果も低下します。

Live Results を管理するには、次のリンク先を参照してください。

- ライブ結果を有効または無効にする
- ライブ結果を削除する

ライブ結果を有効または無効にする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

スキャンでライブ結果を初めて有効にすると、スキャン結果が更新され、最後のスキャン以降に有効化されたプラグインの検出結果が含められます。それ以降は、新しいプラグインの更新があるたびにスキャンにライブ結果が反映されます。ライブ結果は、アクティブスキャンの結果ではなく、スキャンの最新の収集データに基づく評価です。ライブ結果では、エクスプロイトなどのアクティブな検出や以前に収集されていないデータを必要とする新しいプラグインの結果は生成されません。詳細については、ライブ結果を参照してください。

ライブ結果を有効または無効にする方法

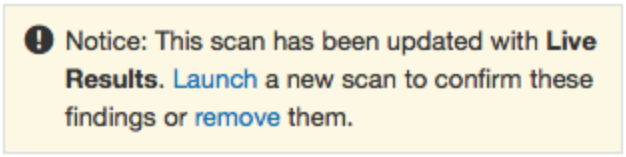
1. Tenable Nessus Professional または Tenable Nessus Expert で、新しいスキャンを作成するか、既存のスキャンを編集します。
2. **[Settings]** (設定) タブに移動します。
3. **[Post-Processing]** (ポスト処理) で、**[Live Results]** (ライブ結果) を有効または無効にします。
    - 有効にするには、**[Live Results]** (ライブ結果) チェックボックスをオンにします。
    - 無効にするには、**[Live Results]** (ライブ結果) チェックボックスをオフにします。
4. **[Save]** (保存) をクリックします。

    Tenable Nessus により、このスキャンに対してライブ結果が有効または無効にされます。

ライブ結果を削除する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

Nessus Professional と Nessus Expert では、スキャンにライブ結果が含まれている場合に、Tenable Nessus のスキャン結果ページに次の通知が表示されます。



ライブ結果を削除すると、スキャン結果ページに表示されなくなります。ただし、Nessus で次にプラグインが更新されたときに、ライブ結果は再び表示されます (スキャンでこの機能を無効にした場合を除く)。

ヒント: スキャンを起動し、ライブ結果の発見事項を確認するには、発見事項を削除する前に、通知で **[Launch]** (起動) をクリックします。

スキャン結果ページからライブ結果の発見事項を削除する方法

- 通知で、**[Remove]** (削除) をクリックします。

スキャンのエクスポートとレポート

スキャンは、で説明しているように、Tenable Nessus ファイルまたは Tenable Nessus DB ファイルスキャンをエクスポートするとしてエクスポートできます。その後、スキャンのインポートとImport a Policyで説明しているように、それらのファイルをスキャンまたはポリシーとしてインポートできます。

また、さまざまな形式でスキャンレポートを作成できます。詳細は、スキャンレポートを作成するを参照してください。

チャプターの選択および順番に基づいて、レポートの内容を定義するためのユーザーレポートテンプレート。カスタムテンプレートを定義したら(詳細についてはCreate a Custom Report Templateを参照)、それらを使用して、スキャン結果のHTMLまたはPDFレポートを生成することができます。カスタムテンプレートに加え、Nessusには事前定義されたシステムテンプレートがいくつか用意されています。カスタムレポートテンプレートおよびシステムレポートテンプレートを表示するには、カスタマイズされたレポートを参照してください。システムテンプレートについての詳細は、https://jp.tenable.com/nessus-reportを参照してください。

形式	説明
エクスポート	
Nessus	.nessusファイルには、ターゲットのリスト、ユーザーが定義したポリシー、スキャン結果が含まれます。Nessusは、XMLにプレーンテキストとしてエクスポートされないようにパスワード認証情報を削除します。.nessusファイルをポリシーとしてインポートする場合は、すべての認証情報にパスワードを再適用する必要があります。
Nessus DB	スキャンによる監査証跡や結果データなどの情報がすべて含まれる、独自の暗号化データベースのフォーマットです。この形式でエクスポートする場合は、スキャン結果を暗号化するためのパスワードを入力する必要があります。
Policy(ポリシー)	スキャンポリシーの詳細が含まれる情報JSONファイル。
Timing Data (タイミングデータ)	スキャンのホスト名、IP、FQDN、スキャンの開始時刻と終了時刻、スキャンに要した時間(秒)が含まれるコンマ区切り値(CSV)の情報ファイル。
Reports	
PDF	PDF形式で生成されたレポートです。レポートのサイズによっては、PDFの生成に数分かかる場合があります。PDFレポートにはOracle JavaまたはOpenJDKのどちらかが必要です。
HTML	通常のHTML出力を使用して生成されたレポートです。このレポートは、ブラウザの新しいタブで開きます。

CSV	データベース、スプレッドシートなどの多くの外部プログラムへのインポートに使用できる CSV エクスポート。

スキャンをエクスポートする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

ある Tenable Nessus スキャナーからスキャンをエクスポートし、別の Tenable Nessus スキャナーにインポートできます。こうすることで、スキャン結果を管理したり、レポートの比較やバックアップを行ったり、企業内のグループ間のコミュニケーションを円滑化したりできるようになります。詳細は、スキャンのインポートを参照してください。

スキャン結果は、Tenable Nessus ファイルまたは Tenable Nessus DB ファイルとしてエクスポートできます。詳細は、スキャンのエクスポートとレポート を参照してください。

注意: Tenable Nessus ファイルについては、プラグインルールを使用して、または脆弱性を変更して (たとえば、プラグインの深刻度を非表示にしたり変更したりすること) スキャン結果を修正した場合、エクスポートされたスキャンにはこれらの変更点は反映されません。

ヒント: 脆弱性と修正の分析のスキャン結果をエクスポートする必要がある場合は、スキャンレポートを作成する を参照してください。

ヒント: Tenable Nessus がエクスポートに使用する暗号化の強度については、暗号強度 を参照してください。

スキャンをエクスポートする方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. スキャンをクリックします。

   スキャンの結果ページが表示されます。

3. 右上隅にある **[Export]** (エクスポート) をクリックします。

4. ドロップダウンボックスから、スキャン結果をエクスポートする形式を選択します。

- **Tenable Nessus** を選択すると、Tenable Nessus は *.nessus* XML ファイルをエクスポートします。
- **[Tenable Nessus DB]** を選択した場合は、**[Export as Tenable Nessus DB]** (Tenable Nessus DB としてエクスポート) ダイアログボックスが表示されます。

  a. ファイルを保護するためのパスワードを入力します。

  Tenable Nessus DB ファイルを別のスキャナーにインポートする際には、このパスワードを入力する必要があります。

  b. **[Export]** (エクスポート) をクリックします。

  Tenable Nessusによって Tenable Nessus Manager DB ファイルがエクスポートされます。
- **[Policy]** (ポリシー) を選択すると、Tenable Nessus はスキャンポリシーの詳細が含まれる情報 JSON ファイルをエクスポートします。
- **[Timing Data]** (タイミングデータ) を選択した場合、Tenable Nessus はスキャンのホスト名、IP、FQDN、スキャンの開始時刻と終了時刻、スキャンに要した時間 (秒) が含まれる情報 CSV ファイルをエクスポートします。

スキャンレポートを作成する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

スキャンレポートを作成して、影響を受けるホストの脆弱性と改善策の分析に利用できます。PDF、HTML、または CSV 形式でスキャンレポートを作成し、特定の情報のみが含まれるようにカスタマイズできます。

スキャンレポートを作成すると、レポートには現在スキャン結果ページに表示されている結果が含まれます。特定のホストまたは脆弱性を選択して、レポートを指定することもできます。

スキャンレポートを作成する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。
2. スキャンをクリックします。

スキャンの結果ページが表示されます。

3. (オプション) 特定のスキャン結果を含むスキャンレポートを作成するには、次の手順を実行します。
   - 検索を使用して、スキャン結果を絞り込みます。
   - フィルターを使用して、スキャン結果を絞り込みます。
   - **[Hosts]** (ホスト) タブで、スキャンレポートに含めるホストの各行のチェックボックスを選択します。
   - **[Vulnerabilities]** (脆弱性) タブで、スキャンレポートに含める各脆弱性または脆弱性グループの各行のチェックボックスを選択します。

   > **注意:** **[Hosts]** (ホスト) または **[Vulnerabilities]** (脆弱性) のいずれかを選択できますが、両方のタブは選択できません。

4. 右上の **[Report]** (レポート) をクリックします。

   [Generate Report] (レポートを生成する) ウィンドウが表示されます。

5. スキャン結果をエクスポートする形式を選択します。
6. 選択した形式のレポートを設定します。

   PDF または HTML

   a. 使用する**レポートテンプレート**をクリックします。

      レポートテンプレートの説明と、テンプレートに適用されているフィルターのリストが表示されます。

      > **ヒント:** **[Hide system templates]** (システムテンプレートを非表示にする) を選択すると、カスタムレポートテンプレートのリストのみが表示されます。

   b. (オプション) 選択したレポートテンプレートで使用可能な場合は、**[脆弱性の結果の間に改ページを含める]** オプションを有効または無効にできます。

   c. (オプション) 選択したレポートテンプレートを (選択したフォーマットに応じて) PDF または HTML レポートのデフォルトとして保存するには、**[Save as default]** (デフォルトとして保存) チェックボックスを選択します。

   d. **[レポートを生成]** をクリックします。

Tenable Nessus がスキャンレポートを作成します。

CSV

a. CSV レポートに表示する列のチェックボックスを選択します。

> **ヒント:** すべての列を選択するには、**[Select All]** (すべて選択) をクリックします。すべての列をクリアするには、**[Clear]** (クリア) をクリックします。列をシステムのデフォルトにリセットするには、**[System]** (システム) をクリックします。

b. (オプション) 現在の設定を CSV レポートのデフォルトとして保存するには、**[Save as default]** (デフォルトとして保存) のチェックボックスを選択します。

c. **[レポートを生成]** をクリックします。

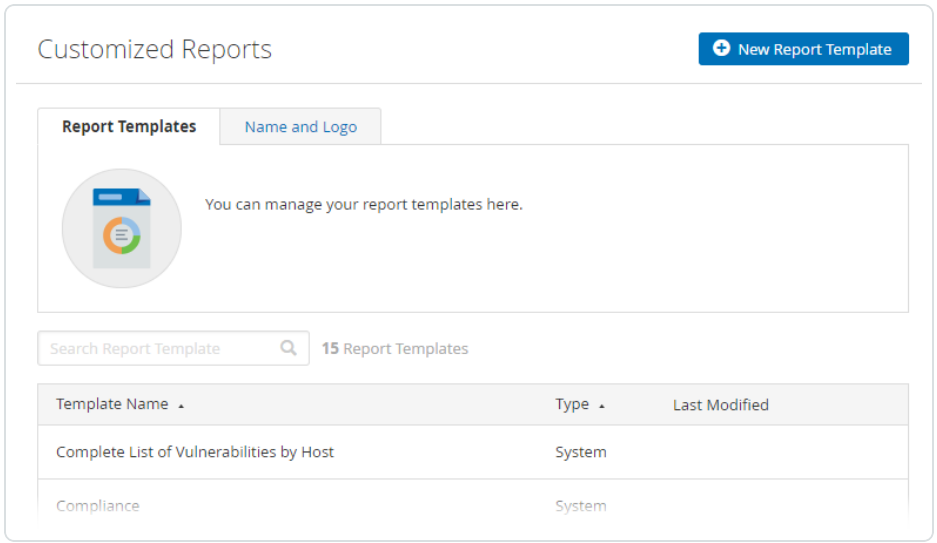
Tenable Nessus がスキャンレポートを作成します。

カスタマイズされたレポート

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** Standard、Administrator、System Administrator

> **注意:** この機能は、Tenable Nessus Manager、Tenable Nessus Professional、および Tenable Nessus Expert でのみ利用できます。

[カスタマイズされたレポート] ページで、各レポートに表示されるタイトルとロゴをカスタマイズし、レポートテンプレートを管理できます。



カスタマイズされたレポートを管理するには、次の手順に従います。

レポートのタイトルとロゴをカスタマイズする

Tenable Nessus では、それぞれのレポートに表示されるタイトルとロゴをカスタマイズできます。これにより、さまざまなステークホルダーのためのレポートを準備することができます。

レポートのタイトルとロゴをカスタマイズする方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Customized Reports]** (カスタマイズされたレポート) をクリックします。

3. **[Name and Logo]** (名称とロゴ) タブをクリックします。

4. **[Custom Name]** (カスタム名) ボックスに、レポートに表示する名前を入力します。

5. カスタムロゴをアップロードするには、**[Upload]** (アップロード) ボタンをクリックします。

   ウィンドウが表示され、アップロードするファイルを選択できます。

6. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus がカスタムタイトルとロゴを保存します。

カスタムレポートテンプレートの作成

Tenable Nessus では、標準のシステムレポートテンプレートに加えて、**[Customized Reports]** (カスタマイズされたレポート) ページでカスタムレポートテンプレートを作成することができます。

カスタムレポートテンプレートを作成する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Customized Reports]** (カスタマイズされたレポート) をクリックします。

   [Report Templates] (レポートテンプレート) ページが表示されます。

3. 右上にある **[New Report Template]** (新規レポートテンプレート) をクリックします。

   当該 **[New Report Template]** (新規レポートテンプレート) ページが表示されます。

4. **[Name]** (名前) テキストボックスで、テンプレート名を入力します。
5. **[Description]** (説明) テキストボックスで、テンプレートの説明を入力します。
6. テンプレートにレポート**チャプター**を追加します。チャプターは、レポートにどのような情報や統計を表示するかを指定します。
    a. **[Add a Chapter]** (チャプターを追加) をクリックします。

    [Add a Report Chapter] (レポートチャプターを追加する) ウィンドウが表示されます。

    b. テンプレートに追加したいチャプターをクリックします。チャプターリストの下には、そのチャプターの説明が表示されます。

    c. **[Add]** (追加) をクリックすると、選択したチャプターがテンプレートに追加されます。

    [Add a Report Chapter] (レポートチャプターの追加) ウィンドウが閉じ、Tenable Nessus が新しいチャプターを **[Chapters]** (チャプター) セクションに追加します。a ~ c の手順を繰り返して、別のチャプターを追加します。
7. 選択したテンプレートのチャプターを編集します。
    - 選択したチャプターに応じて、チャプターの詳細を編集します。これには、チェックボックスの選択やクリア、値の変更などが含まれます。
    - ↑↓ ボタンをクリックすると、チャプターの順番が変わります。
    - ✕ をクリックすると、テンプレートからチャプターが削除されます。
8. **[Save]** (保存) をクリックします。Tenable Nessus により、レポートテンプレートが保存されます。テンプレートの選択と編集は、**[Report Templates] (レポートテンプレート)** タブから行うことができます。

レポートテンプレートをコピーする

Tenable Nessus では、カスタムレポートテンプレートとシステムレポートテンプレートをコピーして、新しいレポートテンプレートを作成できます。

カスタムレポートテンプレートをコピーする方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

    [My Scans] (マイスキャン) ページが表示されます。
2. 左側のナビゲーションバーで **[Customized Reports]** (カスタマイズされたレポート) をクリックします。

[Report Templates] (レポートテンプレート) ページが表示されます。

3. コピーするテンプレートの行の ボタンをクリックします。

   [Copy Report Template] (レポートテンプレートをコピーする) ウィンドウが表示されます。

4. **[Template Name]** (テンプレート名) テキストボックスに新しいテンプレートの名前を入力します。
5. **[Copy]** (コピー) をクリックします。Tenable Nessus により、新しいスキャンテンプレートが保存されます。テンプレートの選択と編集は、**[Report Templates] (レポートテンプレート)** タブから行うことができます。

カスタムレポートテンプレートの編集

注意: カスタムテンプレートの編集のみが可能です。

カスタムレポートテンプレートを編集する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Customized Reports]** (カスタマイズされたレポート) をクリックします。

   [Report Templates] (レポートテンプレート) ページが表示されます。

3. 編集したいカスタムテンプレートの行をクリックします。

   テンプレートの詳細ページが表示されます。

4. 必要に応じて **名前**、**説明**、**チャプター** を編集します。
5. **[保存]** をクリックします。

   Tenable Nessus により、テンプレートの変更が保存されます。

カスタムレポートテンプレートの削除

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Customized Reports]** (カスタマイズされたレポート) をクリックします。

[Report Templates] (レポートテンプレート) ページが表示されます。

3. レポートテンプレートテーブルの削除するカスタムテンプレートの行で、✕ ボタンをクリックします。

   [Delete Report Template] (レポートテンプレートを削除する) ウィンドウが表示されます。

4. **[Delete]** (削除) をクリックします。

   Tenable Nessus によってカスタムテンプレートが削除されます。

プラグイン

新しい脆弱性に関する情報が発見されてパブリックドメインで一般公開されると、Tenable, Inc. の研究スタッフは Tenable Nessus がその脆弱性を検出できるようにプログラムを作成します。

これらのプログラムは、*プラグイン*と呼ばれます。Tenable は、*Tenable Nessus Attack Scripting Language* (NASL) と呼ばれる Tenable Nessus 独自のスクリプト言語でプラグインを作成します。

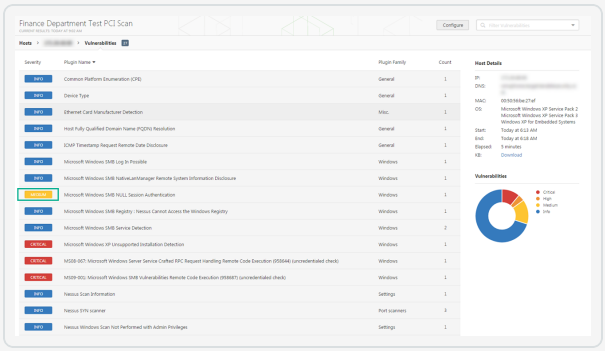
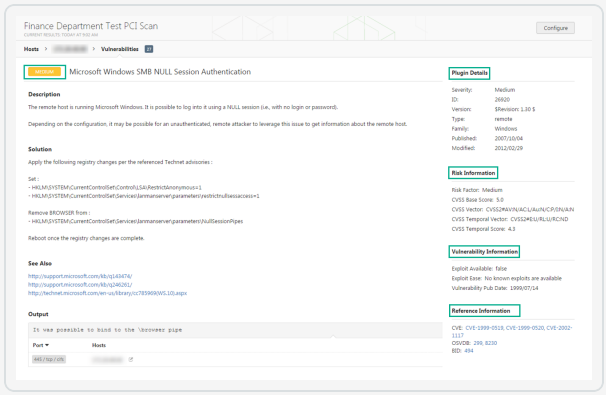
プラグインには、脆弱性情報、一般的な修正処置のセットに加えて、セキュリティ問題が存在しないか検査するアルゴリズムが含まれています。

Tenable Nessus は、CVSS (共通脆弱性評価システム) をサポートしています。v2 と v3 の両方の値を同時にサポートしています。CVSS2 と CVSS3 の両方の属性が存在する場合、Tenable Nessus は両方のスコアを計算します。ただし、リスク要因の属性の判断においては、現在は CVSS2 のスコアが優先されます。

Tenable Nessus はまた、プラグインを使用して、認証されたホストから設定情報を取得します。Tenable Nessus は、この情報をセキュリティのベストプラクティスに対する設定監査の目的で使用します。

プラグイン情報、最新のプラグインリスト、すべての Tenable Nessus プラグインを確認し、特定のプラグインを検索するには、Tenable Nessus プラグインのホームページを参照してください。

プラグイン情報の例

プラグインの重大性とプラグイン名ごとの単一ホストのスキャン結果リスト	単一ホストのプラグインスキャン結果の詳細
	

Tenable Nessus プラグインの入手方法

デフォルトでは、Tenable Nessus はプラグインを自動更新し、コンポーネントとプラグインの更新を 24 時間ごとにチェックします。

Tenable Nessus インストールのブラウザ部分の**製品登録**の実行中、Tenable Nessus はすべてのプラグインをダウンロードし内部データベースにコンパイルします。

`nessuscli fetch –register` コマンドを使用して、手動でプラグインをダウンロードすることもできます。詳細については、本ガイドのコマンドラインセクションを参照してください。

オプションとして、Tenable Nessus インストールのブラウザ部分の**登録**の実行中、**カスタム設定**リンクを選択し、カスタムプラグインフィードをホストするサーバーへホスト名または IP アドレスを渡すこともできます。

Tenable Nessus プラグインの更新方法

デフォルトでは、Tenable Nessus はコンポーネントとプラグインの更新を 24 時間ごとにチェックします。

[**Settings**] (**設定**) > [About] (**製品情報**) ページに移動し、[**Last Updated**] (**最終更新日**) セクションの横にある ↻ をクリックすることで、個別の Tenable Nessus スキャナーで手動更新をトリガーできます。

同じセクションで、現在インストールされているプラグインセットを確認できます。Tenable Nessus Managerでは、リンクされたスキャナーそれぞれの詳細セクションで、リンクされたスキャナーに対してこれらと同じアクションを実行できます。

`nessuscli update --plugins-only` コマンドを使用することでも、手動でプラグインを更新できます。詳細については、Nessusclを参照ください。

ヒント: Tenable Nessus がオフラインであるか、エアギャップされている場合にプラグインをインストールするには、プラグインを手動でインストールするを参照してください。

制限付きプラグインポリシーの作成

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

Tenable Nessus にプリセットされているスキャンテンプレートの使用に加えて、制限付きプラグインポリシーを作成して、カスタム選択したプラグインを使ってスキャンすることができます。

注意: 所属組織に制限付きのプラグインポリシーがある場合、またはそれらを作成する予定の場合、Tenable は、**[Auto Enable Plugin Dependencies]** (プラグイン依存関係の自動有効化) の詳細設定を有効のままにしておくことを強くお勧めします。この設定にしておくと、スキャンデータを収集するために、選択したプラグインが必要とするサポートプラグインが自動的に有効になります。詳しくは、スキャン (詳細設定) を参照してください。

制限付きプラグインポリシーを作成する方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Policies]** (ポリシー) をクリックします。

3. 右上の **[New Policy]** (新しいポリシー) ボタンをクリックします。

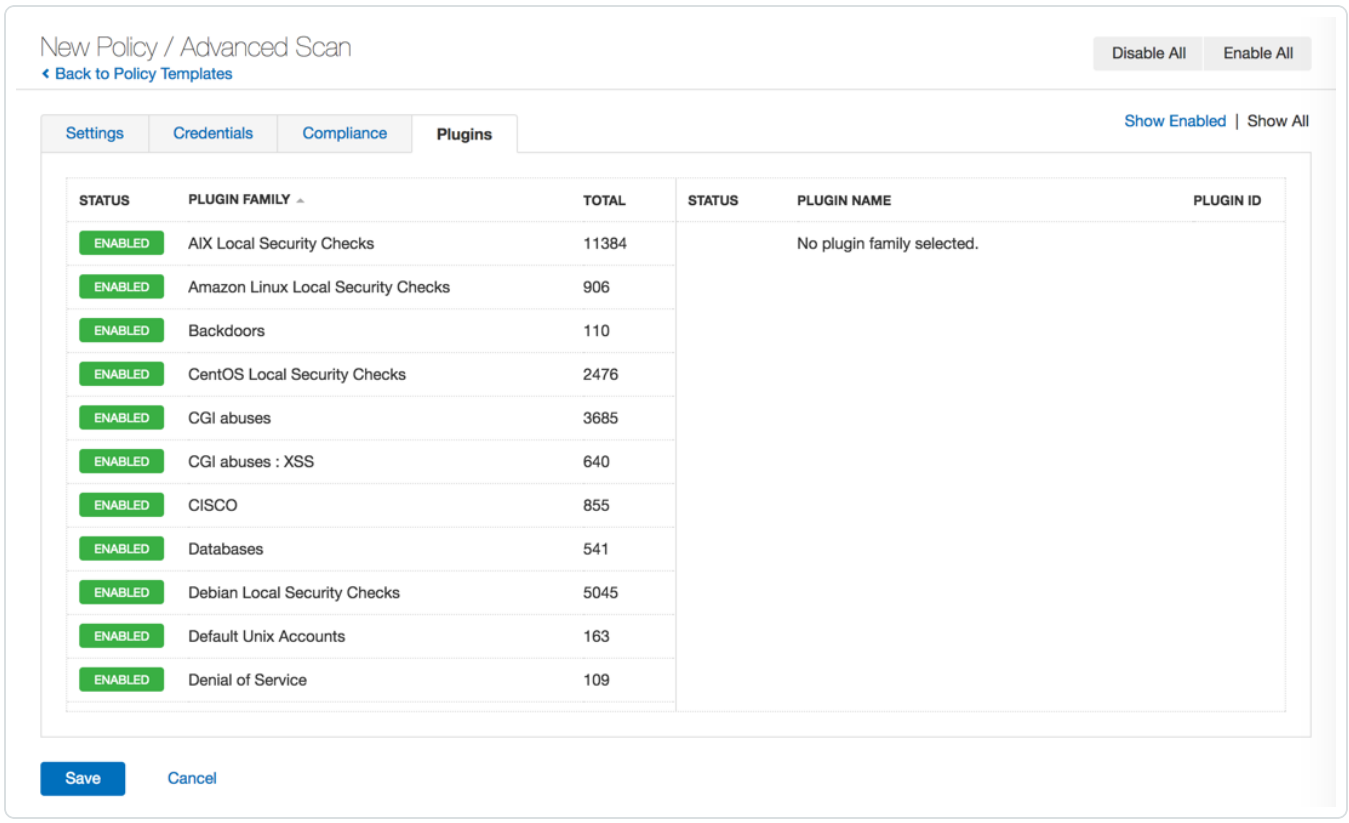
   [Policy Templates] (ポリシーテンプレート) ページが表示されます。

4. **[Advanced Scan]** (詳細なスキャン) テンプレートをクリックします。

   [Advanced Scan] (詳細なスキャン) ページが表示されます。

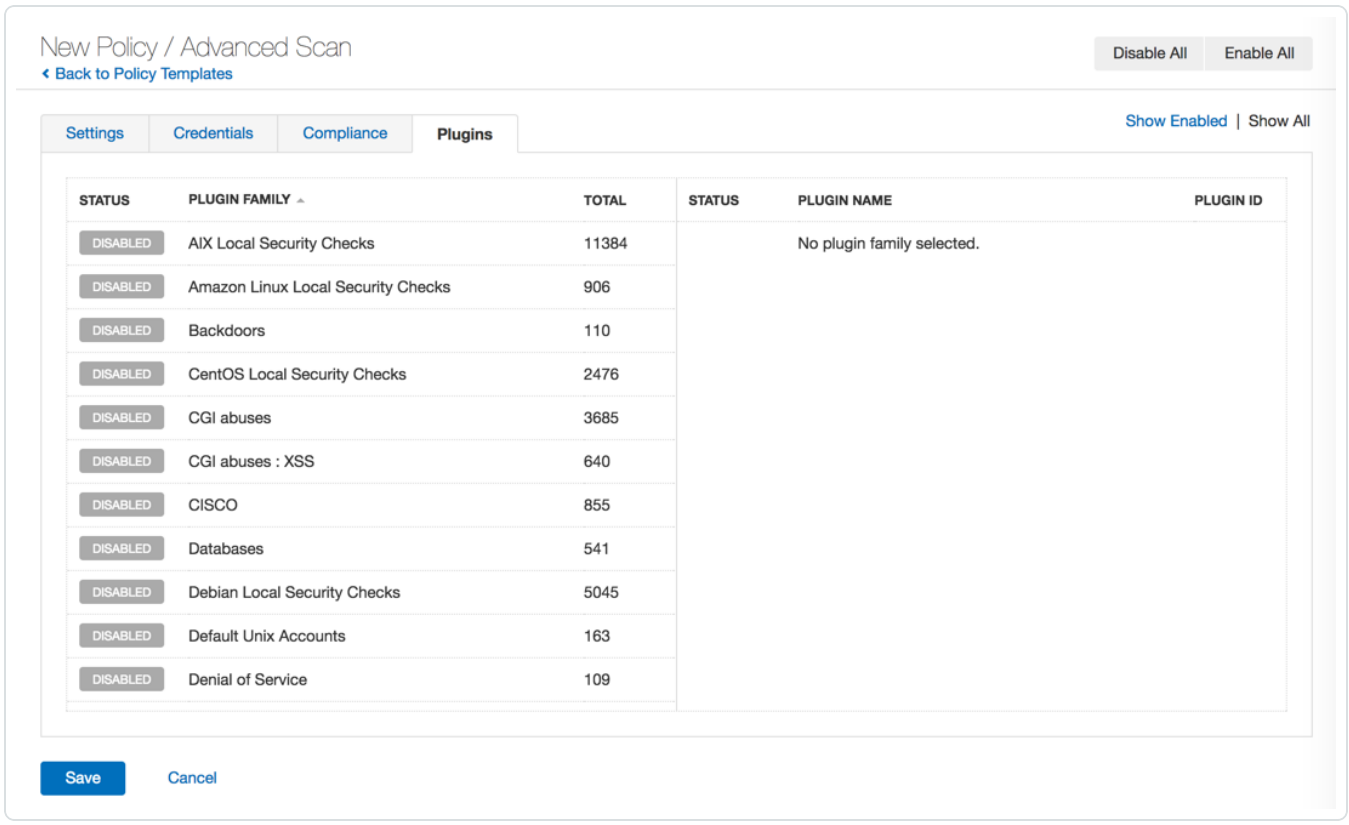
5. **[Plugin]** (プラグイン) タブをクリックします。

   プラグインファミリーのリストが表示されます。デフォルトでは、Tenable Nessus によりすべてのプラグインファミリーが有効になっています。



6. 右上の **[Disable All]** (すべて無効) ボタンをクリックします。

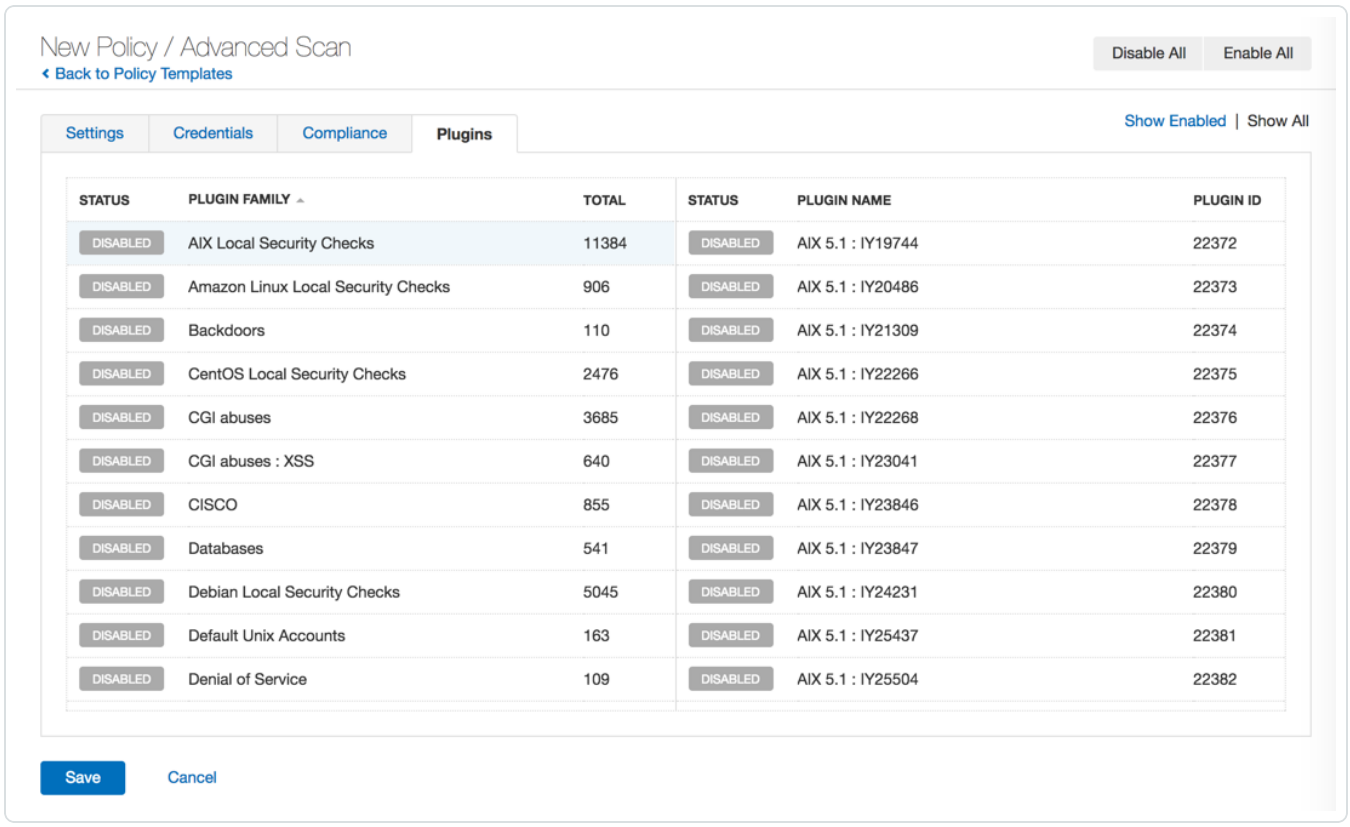
   Tenable Nessus により、すべてのプラグインファミリーが無効になります。



ヒント: すべてのプラグインをすばやく有効または無効にするには、右上にある **[Enable All]** (すべて有効) または **[Disable All]** (すべて無効) ボタンをクリックします。1 つまたはわずかな数のプラグインだけを有効にする必要がある場合には、まずすべてのプラグインを無効にした後、手順 8 の説明に従って個々のプラグインを選択することをお勧めします。

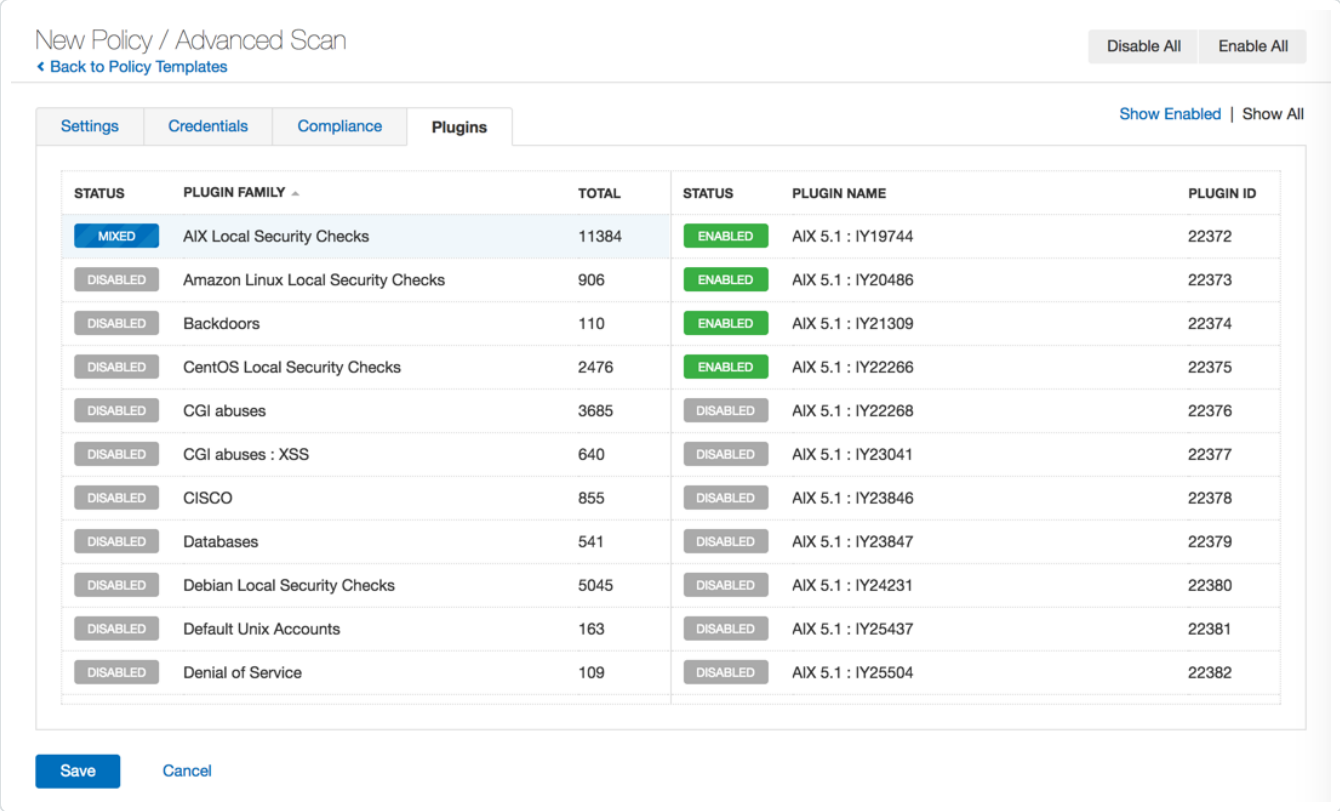
7. 含めるプラグインファミリーをクリックします。

   左側のナビゲーションバーにプラグインのリストが表示されます。



8. 有効にする各プラグインの **[Disabled]** (無効) ボタンをクリックします。

   Tenable Nessus により、各プラグインが有効になります。



ヒント: 右上の **[Filter]** (フィルター) オプションを使用して、プラグインおよびプラグインファミリーを検索できます。これにより、大きなプラグインファミリーに属する個々のプラグインをよりすばやく検索できます。たとえば、個々のプラグインを検索する必要がある場合は、フィルターを `[Match All of the following: Plugin ID is equal to <plugin ID>]` (次のすべてに一致: プラグイン ID は <plugin ID> に等しい) に設定します。詳細は、結果の検索とフィルタリングを参照してください。

9. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus がポリシーを保存します。

プラグインを手動でインストールする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

プラグインは、オフラインの Tenable Nessus システムで、ユーザーインターフェースとコマンドラインインターフェースの 2 通りの方法で手動更新できます。

始める前に

- Nessus プラグインの TAR 圧縮ファイルを ダウンロードして、システムにコピー します。

Tenable Nessus ユーザーインターフェースを使用してプラグインを手動でインストールする方法

注意: Tenable Vulnerability Management または Tenable Security Center が管理するスキャナーを更新する場合は、この手順は使用できません。リンクされたスキャナーのプラグイン更新受信方法の詳細については、Tenable Nessus プラグインとソフトウェアの更新を参照してください。

1. Nessus を実行している**オフライン**システム (A) の上部ナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. **[Software Update]** (ソフトウェア更新) タブをクリックします。

3. 右上隅にある **[Manual Software Update]** (手動ソフトウェア更新) ボタンをクリックします。

   [Manual Software Update] (手動ソフトウェア更新) ダイアログボックスが表示されます。

4. **[Manual Software Update]** (ソフトウェアを手動で更新する) ダイアログボックスで、**[Upload your own plugin archive]** (プラグインのアーカイブからアップロードする) を選択してから、**[Continue]** (続行) を選択します。

5. ダウンロードされた TAR 圧縮ファイルの場所に移動し、選択してから、**[Open]** (開く) をクリックします。

   Nessus がアップロードされたプラグインで更新されます。

コマンドラインインターフェースを使用してプラグインを手動でインストールするには

1. Nessus を実行している**オフライン**システム (A) で、コマンドプロンプトを開きます。

2. お使いのオペレーティングシステム固有の `nessuscli update <tar.gz filename>` コマンドを使用します。

Platform (プラットフォーム)	コマンド
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz filename>`
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz filename>`
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz filename>`

プラグインルール

を使用する場合に必要な ユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

プラグインルールを使ってプラグイン結果の深刻度の優先順位を見直すことで、企業のセキュリティ態勢と対策により適合した評価が可能になります。

[Plugin Rules] (プラグインルール) ページでは、任意のプラグインの深刻度を非表示にしたり変更したりできます。加えて、特定のホストや時間枠に限定したルールが設定できます。このページから、ルールの表示、作成、編集、削除を実行できます。

注意: カスタムプラグインルールを PCI テンプレートに適用することはできません。

プラグインルールに対して次のオプションを設定できます。

オプション	説明
Host (ホスト)	プラグインルールが適用されるホスト。1 つの IP アドレスまたは DNS アドレスを入力するか、またはボックスを空白のままにしてルールをすべてのホストに適用することができます。 **[Host]** (ホスト) オプションは、[Designate hosts by their DNS name] (DNS 名でホストを指名) 設定と同じ形式にする必要があります。つまり、この設定を無効にした場合は **[Host]** (ホスト) には IP アドレスを入力します。この設定を有効にした場合は **[Host]** (ホスト) に DNS アドレスを入力します。 **注意:** プラグインが 2 つのスキャン設定で有効になっていて、[Designate hosts by their DNS name] (DNS 名でホストを指名) の設定が競合している場合には、プラグインに対して 2 つのプラグインルール (IP アドレス用のルールと DNS アドレス用のルール) を作成することを推奨します。
Plugin ID (プラグイン ID)	プラグインルールが適用されるプラグイン。
Expiration Date (有効期限)	(オプション) プラグインルールが期限切れになる日付。
Severity (深刻度)	プラグインルールがアクティブなときに Nessus によりプラグインに割り当てられる深刻度。

プラグインルールを管理するには、次の手順に従います。

プラグインルールの作成

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Plugin Rules]** (プラグインルール) をクリックします。

3. 右上の **[New Rule]** (新しいルール) ボタンをクリックします。

   [New Rule] (新しいルール) ウィンドウが表示されます。

4. 設定を行います。

5. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus がプラグインルールを保存します。

プラグインルールを変更する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Plugin Rules]** (プラグインルール) をクリックします。

3. プラグインルールテーブルで、変更するプラグインルールを選択します。

   [Edit Rule] (ルールを編集する) ウィンドウが表示されます。

4. 必要に応じて設定を変更します。

5. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus により設定が保存されます。

プラグインを削除する

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Plugin Rules]** (プラグインルール) をクリックします。

3. プラグインルールテーブルの、変更するプラグインの行で、✕ ボタンをクリックします。

プラグインルールを削除する選択でよいかを確認するダイアログボックスが表示されます。

4. **[Delete]** (削除) ボタンをクリックします。

   Tenable Nessus がプラグインルールを削除します。

プラグインルールの例

ホスト: 192.168.0.6

プラグイン ID: 79877

有効期限: 2022 年 12 月 31 日

深刻度: 低

このルールの例は、IP アドレス 192.168.0.6 で実行されるスキャンに適用されます。このプラグインルールは、一旦保存されると、2022 年 12 月 31 日までプラグイン ID 79877 (CentOS 8: rpm (CESA-2014:1976)) のデフォルトの深刻度を「低」に変えます。2023 年 1 月 1 日以降、プラグイン ID 79877 の結果は、深刻度が「重大」に戻されます。

エラーメッセージ

次の表は、Tenable Nessus でのスキャン中に表示される可能性があるエラーメッセージと、Tenable が推奨する各エラーの解決方法を示しています。スキャンの作成、変更、起動の詳細については、Scan (スキャン)を参照してください。

警告	説明	推奨アクション
自動構成	この警告は、が JSON デプロイメントプロセス中に発生したことを示します。以下は可能な説明の例です。 • 到達した最大再試行数リンクに失敗しました。 • リンクに失敗しましたは x 秒後に再試行します。	JSON デプロイメントが正しく設定されていることを確認します。その後、再デプロイを試みます。詳細については、Tenable サポート にお問い合わせください。

警告	説明	推奨アクション
	• ユーザーを作成できませんでした禁止されたユーザー名。 • 無効な「アクセス許可」フィールド • ユーザー名が制限を超えています • ユーザー名が重複している • ユーザーの作成に失敗しました。	
No valid targets in list (リストに有効なターゲットがありません)	スキャンのターゲットリストに有効なターゲットがありませんでした。	スキャンのターゲットリストに、有効な Tenable Nessus スキャンターゲット形式のターゲットが 1 つ以上含まれていることを確認してください。 ターゲットルールファイルをチェックして、ターゲットが禁止されているかどうかを判断してください。 スキャンのターゲットリストを調整して、少なくとも 1 つの有効な許可されたターゲットが存在することを確認し、再スキャンしてください。
Can't resolve target [target name] (ターゲット [ターゲット名] を解決できま	Tenable Nessus はターゲット IP アドレスを解決できません	ターゲット名が正しいことを確認してから、DNS

警告	説明	推奨アクション
せん)	でした。	エントリが存在し、ターゲットに対して正しいことを確認してください。ターゲット名とDNSエントリが正しい場合は、再スキャンします。
Unparseable target [target name] (解析できないターゲット [ターゲット名])	名前が有効なターゲット仕様と一致しなかったため、Tenable Nessus はターゲットをスキャンしませんでした。	有効な Tenable Nessus スキャンターゲット形式のいずれかに準拠するようにターゲット名を修正してください。
Restricted target [target name] (制限付きターゲット [ターゲット名])	IP アドレスがスキャンできないものであるため (例: 0.0.0.0)、Tenable Nessus はターゲットをスキャンしませんでした。	スキャンのターゲットリストからターゲットを削除してください。
Rejected attempt to scan [target], as it violates user-defined rules (ユーザー定義のルールに違反したため、[ターゲット] のスキャンの試行が拒否されました)	ユーザー指定のスキャン制限のため、Tenable Nessus はターゲットをスキャンできません。	スキャンのターゲットリストからターゲットを削除するか、ターゲットルールファイルを調整してください。
The allowed number of live hosts scanned with Nessus Essentials has been reached - please contact to upgrade your license. (Nessus Essentials でスキャンされたライブホストが許可されている数に達しました。Tenable に連絡し、ライセンスをアップグレードしてください。)	1 回のスキャンのターゲット数が Tenable Nessus Essentials ライセンス条件で許可されている最大数を超えたため、Tenable Nessus はターゲットをスキャンしませんでした。	スキャンのターゲットの数を減らすか、Tenable Nessus をアップグレードしてください。
The licensed number of live hosts scanned has been reached - please	1 回のスキャンのターゲット数が Tenable Nessus ライセン	スキャンのターゲットの数を減らすか、Tenable

警告	説明	推奨アクション
contact to upgrade your license. (スキャンされたライブホストがライセンスされている数に達しました。Tenable に連絡し、ライセンスをアップグレードしてください。)	ス条件で許可されている最大数を超えたため、Tenable Nessus はターゲットをスキャンしませんでした。	Nessus をアップグレードしてください。
Your current Nessus scanner license limits your scans to [count] live IP addresses. (現在の Nessus スキャナーライセンスでは、スキャンできるライブ IP アドレスの上限は [数] 件です。)You've now scanned over [count] different IP addresses over time, and Nessus will not let you scan any additional hosts. (これまで [数] 件の異なる IP アドレスをスキャンしてきましたが、Nessus ではこれ以上のホストをスキャンできません。)In order to increase this limit, please contact Tenable to upgrade your license. (この上限を引き上げるには、Tenable に連絡してライセンスをアップグレードしてください。)	スキャン全体での一意のターゲットの累計数が Tenable Nessus Essentials ライセンス条件で許可されている最大数を超えたため、Tenable Nessus はターゲットをスキャンしませんでした。	スキャンからターゲットを削除してライセンス条件に準拠するか、Tenable Nessus をアップグレードしてください。
Your current Nessus scanner license limits your scans to [count] live IP addresses. (現在の Nessus スキャナーライセンスでは、スキャンできるライブ IP アドレスの上限は [数] 件です。)You've now scanned over [count] different IP addresses over time, and Nessus will not let you scan any additional hosts. (これまで	スキャン全体での一意のターゲットの累計数が Tenable Nessus 評価版ライセンス条件で許可されている最大数を超えたため、Tenable Nessus はターゲットをスキャンしませんでした。	スキャンからターゲットを削除してライセンス条件に準拠するか、Tenable Nessus をアップグレードしてください。

警告	説明	推奨アクション
[数] 件の異なる IP アドレスをスキャンしてきましたが、Nessus ではこれ以上のホストをスキャンできません。)In order to increase this limit, please contact Tenable to upgrade your license. (この上限を引き上げるには、Tenable に連絡してライセンスをアップグレードしてください。)		
Your current Nessus scanner license limits your scans to [count] live IP addresses. (現在の Nessus スキャナーライセンスでは、スキャンできるライブ IP アドレスの上限は [数] 件です。)You've now scanned over [count] different IP addresses, and Nessus will not let you scan any additional hosts. (これまで [数] 個の異なる IP アドレスをスキャンしてきましたが、Nessus ではこれ以上のホストをスキャンできません。)In order to increase this limit, please contact Tenable. (この上限を引き上げるには、Tenable に連絡してください。)	スキャン全体での一意のターゲットの累計数が Nessus ライセンス条件で許可されている最大数を超えたため、Tenable Nessus はターゲットをスキャンしませんでした。	スキャンからターゲットを削除してライセンス条件に準拠するか、Tenable Nessus をアップグレードしてください。
The network interface [interface] does not support packet forgery This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. (ネットワークインターフェース [インターフェース] はパケットフォージェリをサポートしていません。このため、Nessus は、ターゲットホスト	Tenable Nessus は、生 (raw) IP パケットを送信または受信するためのセッションを確立しようとしましたが、失敗しました。	Tenable では、別のネットワークインターフェースでスキャンすることを推奨しています。 [Ping the remote host] (リモートホストの ping) のスキャン設定を無効にし、Tenable Nessus

警告	説明	推奨アクション
の一部が動作しているかどうか判断できなくなり、それらに対してフルポートスキャンを実行できなくなります。)		にリモートホストへの認証情報を提供してポートスキャンが実行されないようにすることで、この問題を解決できる場合があります。
VMware Fusion does not support packet forgery from the host OS to the target OSs. (VMware Fusion は、ホスト OS からターゲット OS へのパケットフォージェリをサポートしていません。)This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. (そのため、Nessus は、ターゲットホストの一部が動作しているかどうか判断できなくなり、それらに対してフルポートスキャンを実行できなくなります。)If you want to scan your targets within VMware Fusion, either scan them from a different host or install Nessus in a Fusion VM and scan them from there. (VMware Fusion 内でターゲットをスキャンする場合は、別のホストからスキャンするか、Nessus を Fusion VM にインストールしてそこからスキャンしてください。)	Tenable Nessus スキャナーが、サポートされていない VMWare Fusion 設定でインストールされました。	別のホストに Tenable Nessus をインストールします。
The network interface [interface] was not always available for packet forgery, which may lead to	パケットフォージェリは、報告されたインターフェースで少なくとも 1 回は成功しましたが、その後のパケットフォージェリセッ	スキャナーのパフォーマンスに関連する Tenable Nessus 詳細設定の現在の値を確認し、調整

警告	説明	推奨アクション
incomplete results. (ネットワークインターフェース [インターフェース] がパケットフォージェリに常に利用できるとは限らず、結果が不完全になる可能性があります。)This is likely to be a transient error due to a lack of resources on this host. (これは、このホストのリソース不足による一時的なエラーである可能性があります。)To correct this error, reduce the number of scans and/or hosts scanned in parallel. (このエラーを修正するには、並行して行われるスキャンおよび / またはスキャンされるホストの数を減らしてください。)	ションを開く試みは失敗しました。	します。 問題が解決しない場合は、Tenable に問題を報告してください。スキャナーログ nessusd.messages および nessusd.dump の内容全体をレポートに含めてください。
A packet with actual length of [length] bytes was truncated to [truncated length] bytes. (実際の長さが [長さ] バイトのパケットが、[切り捨てる長さ] バイトに切り捨てられました。)The current snapshot length of [snapshot length] for interface [interface name] is too small. (インターフェース [インターフェース名] の現在のスナップショットの長さ [スナップショットの長さ] が短すぎます。)Consider either setting the pcap.snaplen preference to at least [%] or ensuring your network is configured so that packets received by the OS are not greater than the device's MTU (pcap.snaplen 設定を	Tenable Nessus は、スキャン中に生 (raw) IP パケットをキャプチャして分析を試みます。このエラーは、受信したパケットが予想よりも大きく切り捨てられた場合に発生する可能性があります。まれに、これがスキャン結果の精度に影響を与える可能性があります。	スキャンに関連する Tenable Nessus 詳細設定 の現在の値を確認し、調整します。

警告	説明	推奨アクション
少なくとも [%] に設定するか、OS によって受信されるパケットがデバイスの MTU を超えないようにネットワークが設定されていることを確認してください)		
[target] has been turned off, crashed or became unreachable during the audit - scan was interrupted prior to completion (監査中に [ターゲット] がオフになっている、クラッシュした、または到達不能になりました - スキャンが完了する前に中断されました)	Tenable Nessus はターゲットがアクティブであると判断し、スキャンを開始しました。スキャン中にターゲットが応答を停止し、スキャナーはそのターゲットのスキャンのみ終了しました。スキャン結果が不完全になっている可能性があります。 これは、一時的なネットワークの中断、ターゲットで失敗または再起動したサービスの結果であるか、ターゲットがクラッシュしたかネットワークから削除された可能性があります。	ターゲットがアクティブで実行中であることを確認してください。実行中のサービスをチェックし、必要に応じて起動または再起動します。ターゲットがアクティブであことを確認したら、再スキャンしてください。
Some network congestion was detected during the scan. (スキャン中に一部のネットワーク輻輳が検出されました。)This may indicate that one or more of the remote hosts are connected through a connection that does not have enough bandwidth to cope with this scan. (これは、1 つ以上のリモートホストが、このスキャンに対処するのに十分な帯域幅がない接続を介して接続されていることを示	開いていることが判明しているターゲットポートへの接続に、断続的な失敗がありました。	スキャナーのパフォーマンスに関連する Tenable Nessus 詳細設定の現在の値を確認し、調整します。 スキャンポリシーのネットワークタイムアウト設定を増やしてから、再スキャンしてください。

警告	説明	推奨アクション
している可能性があります。)To reduce the risk of congestion: - Reduce 'max hosts' to a lower value - Increase the 'network read timeout' in your policy (輻輳のリスクを減らすには、「最大ホスト」をより低い値に減らし、ポリシーの「ネットワーク読み取りタイムアウト」の値を増やしてください)		
Scan not started for Nessus Agent [agent name] (Nessus Agent [エージェント名] のスキャンが開始されていません)	エージェントのスキャン中に、エージェントがスキャンを開始しませんでした。	エージェントがネットワーク上に存在するかどうかを確認します。エージェントとTenable Nessus Manager/Tenable Vulnerability Management の間のネットワーク接続を確認します。 エージェントがオンラインであることを確認したら、エージェントスキャンを再実行してください。
[count] Nessus Agents didn't start scan: [agent names] ([カウント] 件の Nessus Agent がスキャンを開始しませんでした: [エージェント名])	エージェントのスキャン中に、エージェントがスキャンを開始しませんでした。	各エージェントがネットワーク上に存在するかどうかを確認します。エージェントとTenable Nessus Manager/Tenable Vulnerability Management の間のネットワーク接続を確認します。

警告	説明	推奨アクション
		エージェントがオンラインであることを確認したら、エージェントスキャンを再実行してください。
Scan not completed for Nessus Agent [agent name] at [agent IP] ([エージェント IP] で Nessus Agent [エージェント名] のスキャンが完了していません)	エージェントのスキャン中に、エージェントがスキャン結果を報告しませんでした。	エージェントがネットワーク上に存在するかどうかを確認します。エージェントとTenable Nessus Manager/Tenable Vulnerability Management の間のネットワーク接続を確認します。 エージェントがオンラインであることを確認したら、エージェントスキャンを再実行してください。
[count] Nessus Agents didn't complete scan: [agent names] ([カウント] 件の Nessus Agent がスキャンを完了しませんでした: [エージェント名])	エージェントのスキャン中に、エージェントがスキャン結果を報告しませんでした。	各エージェントがネットワーク上に存在するかどうかを確認します。エージェントとTenable Nessus Manager/Tenable Vulnerability Management の間のネットワーク接続を確認します。 エージェントがオンラインであることを確認したら、エージェントスキャンを再実行してください。

警告	説明	推奨アクション
[count] Nessus Agents aborted scan: [agent names] ([カウント] 件の Nessus Agent がスキャンを中止しました: [エージェント名])	エージェントのスキャン中に、エージェントがスキャンを中止しました。	
Failed to import scan results from remote scanner (リモートスキャナーからスキャン結果をインポートできませんでした)	管理対象の Tenable Nessus スキャナーがスキャン結果を Tenable Nessus Manager にアップロードしましたが、Tenable Nessus Manager がスキャン結果を処理できませんでした。	Tenable Nessus Manager に十分なディスク容量があるか、またはネットワークまたはディスクのエラーが原因でスキャナーによってアップロードされたスキャン結果が破損していないかを確認してください。
Failed to import scan results from remote Nessus Agent [agent name] at [agent IP] - [error] ([エージェント IP] でリモート Nessus Agent [エージェント名] からのスキャン結果をインポートできませんでした - [エラー])	エージェントがスキャン結果をクラスタ子ノードまたは Tenable Nessus Manager のどちらかにアップロードしましたが、スキャン結果を処理できませんでした。	Tenable Nessus Manager に十分なディスク容量があるか、またはネットワークまたはディスクのエラーが原因でスキャナーによってアップロードされたスキャン結果が破損していないかを確認してください。
Failed to import scan results from remote node (リモートノードからスキャン結果をインポートできませんでした)	クラスタスキャンでは、クラスタ「子ノード」はエージェントを管理する Tenable Nessus スキャナーであり、Tenable Nessus Manager によって管理されます。 このエラーは、スキャン結果が子ノードによって Tenable Nessus Manager にアップ	Tenable Nessus Manager に十分なディスク容量があるか、またはネットワークまたはディスクのエラーが原因でスキャナーによってアップロードされたスキャン結果が破損していないかを確認してください。

警告	説明	推奨アクション
	ロードされたものの、結果の処理が失敗した場合に発生します。	
The scan report file was not found (スキャンレポートファイルが見つかりませんでした)	プラグインがスキャン結果にファイルを添付しようとしましたが、ファイルが存在しません。	スキャナーのディスク容量をチェックします。スペースが不十分な場合は、不要なファイルを削除するか、ディスクスペースを追加してスペースを確保してください。
The scan report was [size] which is greater than the [max size] threshold for attaching. (スキャンレポートは [サイズ] で、添付ファイルの [最大サイズ] しきい値を超えています。)	プラグインがスキャン結果にファイルを添付しようとしましたが、ファイルが大きすぎます。	attachment_report_maxum_size の設定を調整してみてください。50MB を超える場合は、レポートの結果をフィルタリングして、サイズを少なくしてください。
This audit has been deprecated and was not executed: [audit file name] (この監査は廃止され、実行されませんでした: [監査ファイル名])	Tenable Nessus コンプライアンス監査スキャンが、すでにサポートされなくなった監査ファイルを指定しました。スキャンは続行されますが、廃止された監査ファイルはスキップされます。	スキャン設定から非推奨の監査を削除してください。
It was not possible to email this scan: [error] (このスキャンをメールで送信できませんでした: [エラー])	Tenable Nessus は、スキャンが完了したときにスキャン結果をメールで送信するように設定されていますが、その送信に失敗しました。	設定された電子メールアドレスとサーバーが正しいこと、およびサーバーがオンラインでありスキャナーから正しく送信できることを確認してください。

警告	説明	推奨アクション
[varies] ([可変])	プラグインがエラーを報告しました。	
Portscanner max ports exceeded (Portscanner の最大ポート数を超えています)	警告: Portscanner が [ターゲット] に対して [ポート数] より多くのポートを開いていることを検出しました。報告されたポートの数が [ポート数] に切り捨てられました (しきい値はスキャナー設定 portscanner.max_ports で制御されています)。通常、これは、ポートスキャンまたはその他の悪意のある可能性のあるアクティビティに対する対策として、接続リクエストを傍受して応答するネットワーク機器が原因です。スキャンの精度とパフォーマンスの両方にマイナスの影響を与えるため、ネットワークセキュリティ設定を調整して、脆弱性スキャンのこの動作を無効にすることが必要な場合があります。	ネットワークセキュリティ設定または portscanner.max_ports の環境設定を調整してください。
Report max ports exceeded (レポートの最大ポート数を超えています)	警告: [ポート] が [ターゲット] に対して開いていることが検出されました - [ポート数] のしきい値 (スキャナー設定 report.max_ports によって制御されます) を超えているため、これらの結果はスキャンレポートから削除されました。	ネットワークセキュリティ設定または report.max_ports の環境設定を調整してください。

警告	説明	推奨アクション
	通常、これは、ポートスキャンまたはその他の悪意のある可能性のあるアクティビティに対する対策として、接続リクエストを傍受して応答するネットワーク機器が原因です。スキャンの精度とパフォーマンスの両方にマイナスの影響を与えるため、ネットワークセキュリティ設定を調整して、脆弱性スキャンのこの動作を無効にすることが必要な場合があります。	
SYN scanner timeout (SYN スキャナーのタイムアウト)	[ターゲット] に対する SYN ポートスキャンが [秒] 後にタイムアウトしました - TCP ポートの結果が不完全な可能性があります。	特定の状況で、SYN ポートスキャナーの実行が遅くなることがあります。最も頻繁に発生する原因は、スキャナーとスキャン対象のホスト間のネットワーク接続の不良、およびファイヤーウォールなどの境界デバイスの設定です。次のいずれかのアクションを実行します。 • 境界デバイス設定を変更する • スキャンするポートの数を減らす • ポートスキャナーのタイムアウトまで

警告	説明	推奨アクション
		の時間を長くする タイムアウトまでの時間を長くする方法については、Tenable サポートに問い合わせてください。
TCP scanner timeout (TCP スキャナーのタイムアウト)	[ターゲット] に対する TCP ポートスキャンが [秒] 後にタイムアウトしました - TCP ポートの結果が不完全な可能性があります。	特定の状況で、TCP ポートスキャナーの実行が遅くなることがあります。最も頻繁に発生する原因は、スキャナーとスキャン対象のホスト間のネットワーク接続の不良、およびファイヤーウォールなどの境界デバイスの設定です。次のいずれかのアクションを実行します。 • 境界デバイス設定を変更する • スキャンするポートの数を減らす • ポートスキャナーのタイムアウトまでの時間を長くする タイムアウトまでの時間を長くする方法については、Tenable サポートに問い合わせてください。
UDP scanner timeout (UDP スキャ	[ターゲット] に対する UDP	UDP ポートスキャナー

警告	説明	推奨アクション
ナーのタイムアウト)	ポートスキャンが [秒] 後にタイムアウトしました - UDP ポートの結果が不完全な可能性があります。	は、特定の状況下では 24 時間を超えて稼働することが知られています。そのため、Tenable では代わりに SYN スキャナーを使用することを推奨しています。ポリシーまたは技術的な理由により SYN スキャナーを使用できない場合は、スキャンするポートの数を減らすか、UDP ポートスキャナーのタイムアウトまでの時間を長くしてください。 タイムアウトまでの時間を長くする方法については、Tenable サポートに問い合わせてください。 **注意:** Tenable クラウドスキャナーで実行されるスキャンでは、UDP ポートのタイムアウトは 8 時間に固定されています。これにより、スキャンがタイムアウトしたり、ほかの望ましくないパフォーマンスの影響が出たりすることを防ぎます。

センサー (Tenable Nessus Manager)

Tenable Nessus Managerの **センサー** ページには、リンクされた Tenable Agents および Tenable Nessus スキャナーすべてを表示および管理するための一元化されたインターフェースがあります。

[Sensors] ページから、いくつかの主な管理タスクを実行できます。

- リンクされたすべてのエージェントとスキャナーの接続ステータス (オンライン、オフライン、無効) をすばやくチェックできます。
- 新しいエージェントまたはスキャナーを Tenable Nessus Managerにリンクするために必要な情報とコントロールへのアクセス。
- 個別のセンサーを選択して、詳細なプロパティを表示したり、グループメンバーシップを管理したり (エージェント用) したり、不要になったセンサーのリンクを解除したりできます。

特定のセンサータイプの管理に関する詳細な手順については、以下のトピックを参照してください。

Agents (エージェント) - のリンク、管理、設定の方法を学習します Tenable Agents

スキャナー – Tenable Nessus スキャナーのリンクと管理方法を説明します。

Agents (エージェント)

エージェントにより、継続的なホスト認証情報がなくても、またはオフラインの資産であっても簡単に資産をスキャンできるようになり、スキャンの柔軟性が高まります。さらに、ネットワークにほとんど影響しない大規模な同時スキャンを可能にします。

リンクし終わったら、スキャンの設定時に、使用するエージェントをエージェントグループに追加する必要があります。リンクされたエージェントは、接続時にマネージャーからプラグインを自動的にダウンロードします。一定時間操作が行われないと、エージェントのリンクは自動的に解除されます。

> **注意:** エージェントは、スキャン結果を返す前にプラグインをダウンロードする必要があります。このプロセスには数分かかる場合があります。

エージェントを管理するには、次を参照してください。

- エージェント設定の変更
- エージェントのフィルタリング

- エージェントのエクスポート
- リンクされたエージェントログをダウンロードする
- エージェントを再起動する
- エージェントのリンク解除
- エージェントの削除

エージェントグループ

エージェントグループを使用すれば、お使いのスキャナーにリンクされたエージェントを整理して管理できます。各エージェントを任意の数のグループに追加し、それらのグループをターゲットとして使用するようにスキャンを設定できます。

注意: エージェントグループ名は、大文字と小文字が区別されます。System Center Configuration Manager (SCCM) またはコマンドラインを使用してエージェントをリンクする場合、大文字と小文字を正しく使用する必要があります。

詳細は、Agent Groups (エージェントグループ)を参照してください。

エージェントの更新

リンクされた Tenable Agents に Tenable Nessus Manager が提供する Tenable Agent バージョンを設定できます。

詳細は、エージェントの更新を参照してください。

フリーズ期間

フリーズ期間を設定すると、リンクされているすべてのエージェントの特定のアクティビティを Tenable Nessus が一時停止する期間をスケジュールできます。

詳細は、フリーズ期間を参照してください。

エージェントのクラスタリング

Tenable Nessus Manager のクラスタリングを使用すると、単一の Tenable Nessus Manager インスタンスから多数のエージェントをデプロイして管理できます。

詳細は、クラスタリングを参照してください。

Tenable Agents のインストール

Tenable Agents のインストールプロセスを始める前に、Tenable Nessus Manager ユーザーインターフェースからエージェントのリンクキーを取得する必要があります。

リンクキーの取得後、*Tenable Agent ユーザーガイド*で説明されている手順を使用してエージェントをインストールし、Tenable Nessus Manager にリンクします。

エージェントがインストールまたはリンクされると、Tenable Agents は 0 ~ 5 分のランダムな遅延の後に Tenable Nessus Manager にリンクされます。遅延を強制すると、大量のエージェントをデプロイまたは再起動する際のネットワークトラフィックを削減し、Tenable Nessus Manager に対する負荷を軽減できます。リンクされたエージェントは、接続時に、マネージャーからプラグインを自動的にダウンロードします。このプロセスには数分かかる場合があります。これはエージェントがスキャン結果を返すのに必要なプロセスです。

Tenable Nessus リンクキーの取得

を使用する場合に必要なユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Agents のインストールプロセスを始める前に、Tenable Nessus Manager からエージェントのリンクキーを取得する必要があります。

注意: `nessuscli` からエージェントリンクキーを取得することもできます。詳細については、nessuscli Fix コマンドセクションの `nessuscli fix --secure --get agent_linking_key` を参照してください。

エージェントのリンクキーを取得する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. (オプション) **リンクキー**を変更するには、リンクキーの横にある ボタンをクリックします。

   次の場合は、リンクキーを変更してもかまいません。

   - リンクキーを再生成していて、以前のリンクキーに戻したい場合
   - 大規模デプロイメントスクリプトにリンクキーを事前定義したい場合

注意: リンクキーは 64 文字の英数字文字列である必要があります。

3. **リンクキー**を記録するかコピーします。

次の手順

- Tenable Nessus のインストールとリンク。

Tenable Nessus Manager にエージェントをリンクする

Tenable Agent のインストール後、エージェントを Tenable Nessus Manager にリンクします。

始める前に

- Tenable Nessus Manager からリンクキーを取得します。
- Tenable Agent をインストールします。

Tenable Agent を Tenable Nessus Manager にリンクする方法

1. コマンドターミナルから Tenable Agent にログインします。
2. エージェントのコマンドプロンプトで、サポートされている引数を使用して `nessuscli agent link` コマンドを使用します。

   たとえば、次のようになります。

   Linux

   ```
   /opt/nessus_agent/sbin/nessuscli agent link
   --key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
   --name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
   ```

   macOS

   ```
   # /Library/NessusAgent/run/sbin/nessuscli agent link
   --key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
   --name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
   ```

   Windows

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
```

次の表に、nessuscli agent link でサポートされている引数を示します。

引数	必須	値
--key	○	マネージャーから取得したリンクキー。
--host	○	Tenable Nessus Manager インストール中に設定した静的IPアドレスまたはホスト名。
--port	○	8834 またはカスタムポート。
--name	×	エージェントの名前。エージェントの名前を指定しない場合、名前はエージェントをインストールしているコンピューターの名前にデフォルト設定されます。
--ca-path	×	マネージャーのサーバー証明書の検証に使用するカスタム CA 証明書。
--groups	×	エージェントを追加する 1 つ以上のエージェントグループ。インストール中にエージェントグループを指定しない場合は、リンクされたエージェントを後で Tenable Nessus Manager 内のエージェントグループに追加できます。 コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。 例: --groups="Atlanta,Global Headquarters" **注意:** エージェントグループ名は、大文字と小文字を区別し、正確に一致する必要があります。エージェントグループ名は引用符で囲む必要があります (例: --groups="My Group")。

引数	必須	値
`--offline-install`	×	有効にすると、エージェントはオンラインでない場合でも、定期的に Tenable Nessus Manager へのリンクを試行します。エージェントがコントローラーに接続できない場合、1 時間ごとに再試行します。コントローラーには接続できるがリンクに失敗する場合は、24 時間ごとに再試行します。 このフラグを使用しない場合、エージェントは即座に Tenable Nessus Manager とのリンクを試行します (エージェントは 1 回のみ試行)。
`--proxy-host`	×	プロキシサーバーのホスト名または IP アドレス。
`--proxy-port`	×	プロキシサーバーのポート番号。
`--proxy-password`	×	ユーザー名として指定したユーザーアカウントのパスワード。
`--proxy-username`	×	プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。
`--proxy-agent`	×	ユーザーエージェント名 (プロキシで事前定義されているユーザーエージェントが必要な場合)。

エージェント設定の変更

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Nessus Manager で、グローバルエージェント設定をして、すべてのリンクされたエージェントのエージェント設定を指定できます。個々のエージェントの詳細設定をリモートで設定できます。エージェントフリーズ期間を設定し、マネージャーのエージェント更新プランを設定することもできます。

Tenable Nessus Manager でエージェント設定を変更するには、次のようにします。

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 次のいずれかを行います。

   - グローバルエージェント設定を変更する方法:

     a. **[Settings]** (設定) タブをクリックします。

     b. グローバルエージェント設定 に記載されているように設定を変更します。

     c. **[Save]** (保存) をクリックします。

   - リモートで個々のエージェント設定を変更するには、リモートエージェント設定を参照してください。

   - マネージャーのエージェント更新プランを変更するには、Configure Agent Update Planを参照してください。

   - エージェントのフリーズ期間設定を変更するには、フリーズ期間のグローバル設定の変更を参照してください。

グローバルエージェント設定

次の表は、Tenable Nessus Manager で変更できるグローバルエージェント設定を示しています。

オプション	説明
エージェントの管理	
Track unlinked agents (リンク解除されたエージェントの追跡)	この設定を有効にすると、手動の介入なしで (非アクティブタイムアウトにより) リンク解除されたエージェントは、対応するエージェントデータと一緒にマネージャーに保存されます。このオプションは、`nessuscli` ユーティリティを使用して設定することもできます。 **注意:** このオプションでは、マネージャーは*削除済み*エージェントを追跡できません。削除されたエージェントは、マネージャーやクラスタにより追跡されたり認識されたりしなくなります。

オプション	説明
Unlink inactive agents after *X* days (X 日後に非アクティブのエージェントのリンクを解除)	マネージャーがエージェントのリンクを解除する基準となる、エージェントが非アクティブである日数を指定します。 Tenable Nessus Manager により自動的にリンクを解除された非アクティブなエージェントは、オンラインに戻った場合に自動的には再リンクできます。 **[Track unlinked agents]** (リンク解除されたエージェントの追跡) が有効になっている必要があります。
Remove agents that have been inactive for *X* days (x 日間非アクティブなエージェントを削除)	マネージャーがエージェントを削除する基準となる、エージェントが非アクティブである日数を指定します。
Remove bad agents (不正なエージェントを削除)	この設定が有効になっている場合、以下の条件のうち 1 つ以上を満たすエージェントが Tenable Nessus Manager から削除されます。 • 過去にエージェントがあるユーザーによって削除された • エージェントが有効なアクセストークンを提供していない • エージェントがブロックリストに登録された **注意:** この設定は、クラスタリングが有効になっている Tenable Nessus 環境にのみ適用されます。
フリーズ期間	
フリーズ期間の設定を変更する の説明に従って、フリーズ期間のグローバル設定を設定してください。	

リモートエージェント設定

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

エージェントのすべての詳細な設定は、*Tenable Agent デプロイメントとユーザーガイド*の詳細設定に説明されているとおり、エージェントのコマンドラインインターフェースを経由して設定できます。ただし、一部の設定は Tenable Nessus Manager を介してリモートで変更できます。

リモートエージェント設定を変更する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 次のいずれかを行います。

   #### 1 つのエージェントを変更する方法

   a. エージェントの表で、設定するエージェントの行をクリックします。

      エージェントの詳細ページが表示されます。デフォルトでは **[Agent Details]** (エージェントの詳細) タブが開きます。

   b. **[Remote Settings]** (リモート設定) タブをクリックします。

      [Remote Settings] (リモート設定) ページが表示されます。

   c. エージェント設定を変更します。

設定	説明	デフォルト	値
Scan Performance (スキャンのパフォーマンス)	CPU 使用率に影響を与える、スキャンのパフォーマンスを設定します。パフォーマンスを low にするとスキャン速度が低下しますが、エージェントの CPU 消費量は減少します。パフォーマンスを medium または high にすると、	`high`	`low`、`medium`、または `high`

	スキャン完了までの時間が短縮されますが、エージェントの CPU 消費量は増加します。詳細については、*Tenable Agentユーザーガイド*のエージェントの CPU リソースコントロールを参照してください。		
Plugin Compilation Performance (プラグインのコンパイルパフォーマンス)	CPU 使用率に影響を与える、プラグインのコンパイルパフォーマンスを設定します。パフォーマンスを low にするとプラグインのコンパイル速度が低下しますが、エージェントの CPU 消費量は減少します。パフォーマンスを medium または high にすると、プラグインのコンパイル完了までの時間が短縮されますが、エージェントの CPU 消費量は増加します。詳細については、*Tenable Agentユーザーガイド*のエージェントの CPU リソースコントロールを参照してください。	Tenable Agent 10.8.3 以降 - `medium` Tenable Agent 10.8.2 以前 - `high`	`low`、`medium`、または `high`

Nessus Agent Log Level (Nessus Agent ログレベル)	backend.log ログファイルのログ記録レベルで、どの情報をログに含めるかを決定する、ログタグのセットで指定されます。 log.json を手動で編集して、ログタグのカスタムセットを backend.log 用に設定している場合、その内容はこの設定によって上書きされます。 詳細は、ログを管理するを参照してください。	normal	• normal - backend.log のログレベルを normal に変更し、ログタグを "log"、"info"、"warn"、"error"、"trace" に設定します。 • debug - backend.log のログレベルを debug に変更し、ログタグを "log"、"info"、"warn"、"error"、"trace"、"debug" に設定します。 • verbose - backend.log のログレベルを verbose に変更し、ログタグを "log"、"info"、

			"warn"、"error"、"trace"、"debug"、"verbose" に設定します。
Maximum Scans Per Day (1 日あたりの最大スキャン数)	エージェントに対して実行する、1 日あたりの最大スキャン数を指定します。	10	整数の 1 以上
Automatic Hostname Update (ホスト名の自動更新)	この機能を有効にすると、エンドポイント上のホスト名が変更されたとき、この新しいホスト名がエージェントのマネージャーで適用されます。カスタムのエージェント名が上書きされないようにするために、この機能はデフォルトで無効になっています。	×	yes または no

複数のエージェントを変更するには

a. 次のいずれかを行います。

- エージェントの表で、編集する各エージェントの横にあるチェックボックスを選択します。
- 表ヘッダーにあるチェックボックスを選択して、ページ全体を選択します。

b. 右上の **[Manage]** (管理) ボタンをクリックします。

ドロップダウンメニューが表示されます。

c. **[Remote Settings]** (リモート設定) ボタンをクリックします。

[Remote Settings] (リモート設定) ページが表示されます。

d. エージェント設定を変更します。

設定	説明	デフォルト	値
Scan Performance (スキャンのパフォーマンス)	CPU 使用率に影響を与える、スキャンのパフォーマンスを設定します。パフォーマンスを low にするとスキャン速度が低下しますが、エージェントの CPU 消費量は減少します。パフォーマンスを medium または high にすると、スキャン完了までの時間が短縮されますが、エージェントの CPU 消費量は増加します。詳細については、*Tenable Agentユーザーガイド*のエージェントの CPU リソースコントロールを参照してください。	`high`	`low`、`medium`、または `high`
Plugin Compilation Performance (プラグインのコンパイルパフォーマンス)	CPU 使用率に影響を与える、プラグインのコンパイルパフォーマンスを設定します。パフォーマンスを low にするとプラグインのコンパイル速度が低下しますが、	Tenable Agent 10.8.3 以降 - `medium` Tenable Agent 10.8.2 以前	`low`、`medium`、または `high`

	エージェントの CPU 消費量は減少します。パフォーマンスを medium または high にすると、プラグインのコンパイル完了までの時間が短縮されますが、エージェントの CPU 消費量は増加します。詳細については、*Tenable Agentユーザーガイド*の エージェントの CPU リソースコントロールを参照してください。	`- high`	
Nessus Agent Log Level (Nessus Agent ログレベル)	`backend.log` ログファイルのログ記録レベルで、どの情報をログに含めるかを決定する、ログタグのセットで指定されます。 `log.json` を手動で編集して、ログタグのカスタムセットを `backend.log` 用に設定している場合、その内容はこの設定によって上書きされます。 詳細は、ログを管理するを参照してください。	`normal`	• `normal` - backend.log のログレベルを `normal` に変更し、ログタグを `"log"`、`"info"`、`"warn"`、`"error"`、`"trace"` に設定します。 • `debug` - backend.log のログレベルを `debug` に変更し、ログタグを

			"log"、"info"、"warn"、"error"、"trace"、"debug" に設定します。 • verbose - backend.log のログレベルを verbose に変更し、ログタグを "log"、"info"、"warn"、"error"、"trace"、"debug"、"verbose" に設定します。
Maximum Scans Per Day (1 日あたりの最大スキャン数)	エージェントに対して実行する、1 日あたりの最大スキャン数を指定します。	10	整数の 1 以上
Automatic Hostname Update (ホスト名の自動更新)	この機能を有効にすると、エンドポイント上のホスト名が変更されたとき、この新しいホスト名がエージェントのマネージャーで適用され	×	yes または no

	ます。カスタムのエージェント名が上書きされないようにするために、この機能はデフォルトで無効になっています。		

3. 次のいずれかを行います。

    - 設定を保存してすぐに適用するには、**[Save and Apply]** (保存して適用) をクリックします。

      注意: 一部の設定では、設定を適用する際にエージェントのソフト (バックエンド) 再起動またはサービスの完全な再起動が求められます。

    - 設定を保存してもまだ適用しない場合は、**[Save]** (保存) ボタンをクリックします。

      注意: 設定がエージェントに対して有効になるには、設定を適用する必要があります。表示されたバナーで、**[Apply all changes now]** (すべての変更を適用) をクリックします。一部の設定では、設定を適用する際にエージェントのソフト (バックエンド) 再起動またはサービスの完全な再起動が求められます。

エージェントの更新

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

リンクされた Tenable Agents に Tenable Nessus Manager が提供する Tenable Agent バージョンを設定して、**[Agent Updates]** (エージェントの更新) ページから更新することができます。

[Agent Updates] (エージェントの更新) ページでは、提供される Tenable Agent バージョンを Tenable Nessus フィードから直接手動で更新することもできます。また、Tenable Nessus Manager が、使用可能な新しいバージョンがないか最後にフィードをチェックしたときの、**GA**、**早期アクセス版**、および **安定版** の更新プランに対応する Tenable Agent バージョン、Tenable Nessus Manager インスタンスが現在提供しているバージョン、および Tenable Nessus Manager がフィードから提供バージョンを最後に更新した時刻が表示されます。

注意: Tenable Nessus が Tenable Security Center や Tenable Nessus Manager によって管理されている場合、**[Agent Updates]** (エージェントの更新) ページは利用できません。

注意: **[Agent Updates]** (エージェントの更新) ページは、Tenable Agent バージョンの更新にのみ影響し、プラグインの更新には影響しません。

エージェント更新の設定を管理するには、次の手順を使用します。

エージェント更新プランの設定

リンクされた Tenable Agents に Tenable Nessus Manager が提供する Tenable Agent バージョンを設定して、**[Agent Updates]** (エージェントの更新) ページから更新することができます。

次の 3 つのエージェント更新プランから 1 つを選択できます。

エージェント更新プラン	説明
GA releases (GA リリース)	(デフォルト) Tenable Nessus Manager により、Tenable Agents が最新の一般提供 (GA) バージョンに自動的に更新されるようになります。
Early Access releases (早期アクセス版のリリース)	最新バージョンが早期アクセス版としてリリースされると (通常は一般提供版よりも数週間早いタイミングでリリースされます)、Tenable Nessus Manager により、Tenable Agents が自動的に最新バージョンへと更新されるようになります。
Stable releases (安定版リリース)	Tenable Agents は最新バージョンに自動更新されず、Tenable により設定された旧バージョンのままです (通常は、最新の一般 提供バージョンよりも 1 つ前のリリース)。

エージェント更新プランの設定

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Updates]** (エージェントの更新) をクリックします。

   [Agent Updates] (エージェントの更新) ページが表示されます。

3. **[Agent Update Plan]** (エージェントの更新プラン) で、Tenable Agents の更新に使用するプランを選択します。

4. **[保存]** をクリックします。

   保存後、Tenable では Tenable Nessus Manager が Tenable Nessus フィードから提供する [Tenable Agent バージョンを更新することが推奨されます。

が提供するエージェントのバージョンを設定する Tenable Nessus Manager

[**Automatic Updates] (自動更新) の** 設定により、Tenable Nessus Manager では、マネージャーの更新プランに基づいて、アップグレードするリンクされたエージェントに提供する Tenable Agent バージョンを自動的に更新できます。あるいは **[Automatic Updates]** (自動更新) をオフにして、提供される Tenable Agent バージョンを手動で設定することもできます。

注意: リンクされたエージェントがソフトウェアの更新をダウンロードしないようにするには、**[Automatic Updates]** (自動更新) を無効にすることに加えて、恒久的なフリーズ期間を作成する必要があります。**[Automatic Updates]** (自動更新) を無効にしても、Tenable Nessus Manager がリンクされたエージェントに提供するバージョンの更新をブロックするだけです。リンクされたエージェントに提供する新しいバージョンのエージェントを Tenable Nessus Manager が既にダウンロードしている場合、リンクされたエージェントはその新しいバージョンにアップグレードまたはダウングレードします。これを回避するには、恒久的なフリーズ期間を作成して、**[Prevent software updates]** (ソフトウェアの更新を防止) 設定をオンにしてください。詳細は、Create a Freeze Windowを参照してください。

[Automatic Updates] (自動更新) の設定を有効または無効にする方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Updates]** (エージェントの更新) をクリックします。

   [Agent Updates] (エージェントの更新) ページが表示されます。

3. **[Automatic Updates]** (自動更新) で、**[Enable Agent Updates]** (エージェントの更新を有効にする) チェックボックスを選択または選択解除します。

4. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus Manager により設定が保存されます。

エージェント更新プランを設定した後や、[Automatic Updates] **(自動更新)**をオフにした後などに、Tenable Nessus Manager が提供する [Tenable Agent バージョンを手動で更新したい場合は次の手順に従います。

提供する Tenable Agent バージョンを手動で更新する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Updates]** (エージェントの更新) をクリックします。

   [Agent Updates] (エージェントの更新) ページが表示されます。

3. ページの右上隅にある **[Manual Software Update]** (手動ソフトウェア更新) ボタンをクリックします。

   [Update Provided Agent Version Now] (提供されたエージェントバージョンを今すぐ更新する) ウィンドウが表示されます。

   > **注意: [Manual Software Update]** (手動ソフトウェア更新) ボタンは、保存されているエージェント更新プランに基づいて、Tenable Agent の提供バージョンを更新します。たとえば、プランを **GA リリース**に設定して保存した場合にこのボタンをクリックすると、Tenable Agent の提供バージョンは最新の GA バージョンに更新されます。**[Disable agent version updates]** (エージェントのバージョン更新を無効にする) を選択した場合、このボタンは表示されません。

4. **[Continue]** (続行) ボタンをクリックします。

   Tenable Nessus Manager が Tenable Nessus フィードから Tenable Agents に提供するバージョンを更新します。

エージェントのフィルタリング

Tenable Nessus Manager でエージェントをフィルタリングするには、この手順を使用します。

エージェントテーブルでエージェントをフィルタリングする方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

[Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. エージェントテーブルの上にある **[Filter]** (フィルター) ボタンをクリックします。

   [Filter] (フィルター) ウィンドウが表示されます。

3. 必要に応じてフィルターを設定します。詳細は、エージェントフィルターを参照してください。

4. **[Apply]** (適用) をクリックします。

   Tenable Nessus Manager により、設定したオプションに一致するエージェントのみが含まれるようにエージェントのリストがフィルタリングされます。

エージェントフィルター

パラメーター	演算子	式
IP Address	次の値に等しい 次の値に等しくない 次の値を含む 次の値を含まない	テキストボックスに、フィルタリングする IPv4 アドレスまたは IPv6 アドレスを入力します。
最終接続 最終プラグイン更新日 最終スキャン	earlier than later than 次の値と等しい not on	テキストボックスに、フィルタリングする日付を入力します。
グループのメンバー	次の値に等しい	ドロップダウンリストから、既存のエージェントグループを選択します。

パラメーター	演算子	式
	次の値に等しくない	
名前	次の値に等しい 次の値に等しくない 次の値を含む 次の値を含まない	テキストボックスに、フィルタリングするエージェント名を入力します。
Platform (プラットフォーム)	次の値を含む 次の値を含まない	テキストボックスに、フィルタリングするプラットフォーム名を入力します。
Status (ステータス)	次の値に等しい 次の値に等しくない	ドロップダウンリストで、エージェントのステータスを選択します。詳細は、*Tenable Agent デプロイメントとユーザーガイド*のエージェントのステータスを参照してください。
Version	次の値に等しい 次の値に等しくない 次の値を含む 次の値を含まない	テキストボックスに、フィルタリングするバージョンを入力します。

エージェントのエクスポート

を使用する場合に必要なユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

でエージェントデータをエクスポートするには Tenable Nessus Manager

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。

2. (オプション) エージェントリストにフィルターを適用するには、**[Filter]** (フィルター) ボタンをクリックします。

3. 右上隅にある **[Export]** (エクスポート) をクリックします。ドロップダウンが表示されたら、**[CSV]** をクリックします。

   ブラウザのダウンロードマネージャーが表示されます。

4. **[OK]** をクリックして `agents.csv` ファイルを保存します。

Tenable Nessus Manager からエクスポートした `agents.csv`ファイルには、次のデータが含まれます。

フィールド	説明
エージェント名	エージェントの名前
Status (ステータス)	エクスポート時のエージェントのステータス。可能な値は `unlinked`、`online`、またはオフラインです。
IP Address (IP アドレス)	エージェントの IPv4 または IPv6 アドレス。
Platform (プラットフォーム)	エージェントがインストールされているプラットフォーム。
Groups (グループ)	エージェントが属しているグループの名前。
Version (バージョン)	エージェントのバージョン。
Last Plugin Update (最後のプラグインの更新)	エージェントのプラグインセットが最後に更新された日付 (ISO-8601 形式)。
Last Scanned (最終スキャン日)	エージェントがホストのスキャンを最後に実行した日付 (ISO-8601 形式)。

リンクされたエージェントログをダウンロードする

を使用する場合に必要なユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Nessus Manager の管理者は、ログとシステム設定データが入ったログファイルを管理スキャナーおよびエージェントに対してリクエストし、ダウンロードすることができます。この情報は、システムの問題をトラブルシューティングするのに役立つとともに、Tenable サポートに提出するデータを簡単に収集する方法を提供します。

Tenable Nessus Manager の各エージェントから最大で 5 つのログファイルを保存できます。上限に達したら、古いログファイルを削除して新しいログファイルをダウンロードする必要があります。

リンクされたエージェントからログをダウンロードするには

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. エージェントテーブルで、ログをダウンロードするエージェントをクリックします。

   そのエージェントの **[Agents]** (エージェント) ページが表示されます。

3. **[Logs]** (ログ) タブをクリックします。

4. 右上にある **[Request Logs]** (ログのリクエスト) をクリックします。

   注意: 上限である 5 つのログファイルに達した場合は、**[リクエストログ]** ボタンは無効になります。新しいログをダウンロードする前に既存のログを削除してください。

   Tenable Nessus Manager は、次回のチェックイン時にエージェントにログをリクエストします。これは数分かかる場合があります。ダウンロードが完了するまで、リクエストのステータスがユーザーインターフェースに表示されます。

5. ログファイルをダウンロードするには、ファイル名をクリックします。

   システムによってログファイルがダウンロードされます。

既存のログを削除する方法

- 削除するログの行で、🗑ボタンをクリックします。

保留中または失敗したログのダウンロードをキャンセルする方法

- キャンセルする保留中または失敗したログダウンロードの行で、⊘ ボタンをクリックします。

エージェントを再起動する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Nessusでは、リンクされたエージェントを **[Linked Agents] (リンクされたエージェント)** ページで再起動できます。

エージェントを再起動する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 次のいずれかを行います。

   1つのエージェントを再起動する方法

   a. エージェントの表で、設定するエージェントの行をクリックします。

      エージェントの詳細ページが表示されます。デフォルトでは **[Agent Details]** (エージェントの詳細) タブが開きます。

   b. **[Remote Settings]** (リモート設定) タブをクリックします。

      [Remote Settings] (リモート設定) ページが表示されます。

   c. 右上の **[Restart Agent]** (エージェントを再起動する) ボタンをクリックします。

      [Restart Agent] (エージェントを再起動する) ウィンドウが表示されます。

   複数のエージェントを再起動する方法

   a. 次のいずれかを行います。

      - エージェントの表で、再起動する各エージェントの横にあるチェックボックスを選択します。

- 表のヘッダーにあるチェックボックスを選択して、ページにリストされているすべてのエージェントを選択します。

b. 右上の **[Manage]** (管理) ボタンをクリックします。

ドロップダウンメニューが表示されます。

c. **[Restart]** (再起動) ボタンをクリックします。

[Restart Agent] (エージェントを再起動する) ウィンドウが表示されます。

> **注意:** 選択したエージェントのいずれもオンラインでない場合、ドロップダウンメニューに **[Restart]** (再起動) ボタンは表示されません。

3. ドロップダウンメニューで、エージェントが実行する再起動タイプを選択します。

- **エージェントサービスのソフト再起動 (サービス再起動なし)** – 次回の Tenable Nessus Manager へのエージェントのチェックイン時にこの再起動が実行されます。
- **エージェントのアイドル時にエージェントサービスを再起動** – 次回の Tenable Nessus Manager へのエージェントのチェックイン時にこの再起動が実行されます。
- **エージェントサービスを直ちに再起動 (実行中のすべてのスキャンを停止)** – この再起動は即時に実行されます。

4. **[Restart]** (再起動) ボタンをクリックします。

ウィンドウが閉じ、選択した再起動タイプを確認するメッセージが表示されます。

エージェントのリンク解除

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** 管理者またはシステム管理者

エージェントを手動でリンク解除すると、そのエージェントは Tenable Nessus **[Agents]** (エージェント) ページから消えますが、関連データはエージェント設定で指定された期間保持されます。エージェントを手動でリンク解除すると、そのエージェントは Tenable Nessus Manager には自動では再リンクしません。

> **ヒント:** エージェントの設定で説明されているように、一定の日数、非アクティブになると、自動的にリンク解除するようにエージェントを設定できます。

Tenable Nessus Manager でエージェントのリンクを手動で解除する方法

Tenable Nessus でエージェントのリンクを解除するには、# nessuscli agent unlink コマンドを実行するか、次の手順を使用します。

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 左側のナビゲーションバーで **[Agents]** (エージェント) をクリックします。

   [Agents] (エージェント) ページが表示されます。

3. 次のいずれかを行います。

   1 つのエージェントのリンクを解除する場合

   a. エージェントの表で、リンク解除するエージェントの行の ボタンをクリックします。

      確認ウィンドウが表示されます。

   1 つまたは複数のエージェントのリンクを解除する方法:

   a. エージェントの表で、リンク解除する各エージェントの行のチェックボタンを選択します。

   b. 右上の **[Manage]** (管理) ボタンをクリックします。

      ドロップダウンメニューが表示されます。

   c. **[Unlink]** (リンク解除) ボタンをクリックします。

      確認ウィンドウが表示されます。

      > **注意:** 選択したエージェントのいずれもリンクされていない場合、ドロップダウンメニューに **[Unlink]** (リンク解除) ボタンは表示されません。

4. **[Unlink]** (リンク解除) ボタンをクリックします。

   Tenable Nessus Manager によりエージェントとのリンクが解除されます。

エージェントの削除

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** 管理者またはシステム管理者

Tenable Nessus Manager の **[Linked Agents]** (リンクされたエージェント) ページで、リンクされたエージェントを削除できます。

Tenable Nessus Manager からエージェントを削除する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 次のいずれかを行います。

   1 つのエージェントを削除する方法

   a. 削除するエージェントの行で ✕ ボタンをクリックします。

      確認ウィンドウが表示されます。

   複数のエージェントを削除する方法

   a. 削除するエージェントのチェックボックスを選択します。

   b. 右上の **[Manage]** (管理) ボタンをクリックします。

      ドロップダウンメニューが表示されます。

   c. **[Delete]** (削除) ボタンをクリックします。

      確認ウィンドウが表示されます。

3. **[Delete]** (削除) ボタンをクリックします。

   Tenable Nessus Manager によりエージェントが削除されます。

Agent Groups (エージェントグループ)

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

エージェントグループを使用して、Tenable Nessus Manager にリンクしたエージェントを編成して管理できます。複数のエージェントグループを追加し、これらのグループをターゲットとして使用するようスキャンを設定できます。そのようになります。

Tenable Nessus Manager でスキャンを管理し、スキャンデータを Tenable Security Center にインポートする場合は特に、Tenable ではエージェントグループのサイズを適切に設定することを推奨します。

Tenable Nessus Manager でエージェントを管理する際に、エージェントグループのサイズを設定できます。

スキャンして単一のエージェントグループに含めるエージェントが増えるほど、マネージャーが 1 つのバッチで処理するデータが増えます。エージェントグループのサイズに応じて、Tenable Security Center にインポートする必要がある .nessus ファイルのサイズが決まります。.nessus ファイルのサイズは、ハードドライブの容量と帯域幅に影響します。

次のプロセスを使用して、エージェントグループを作成および管理します。

エージェントグループの作成

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 新規エージェントグループに追加するエージェントの横にあるチェックボックスを選択します。

3. 右上の **[Manage]** (管理) ボタンをクリックします。

   ドロップダウンメニューが表示されます。

4. ドロップダウンメニューで、**[新しいグループ]**をクリックします。

   [New Agent Group] (新規エージェントグループ) ウィンドウが表示されます。

5. 新規エージェントグループの名前を入力します。

6. **[追加]** をクリックします。

   Tenable Nessus Manager により新規エージェントグループが作成され、選択したエージェントがこの新しいグループに追加されます。

エージェントグループにエージェントを追加する

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. エージェントグループに追加するエージェントの横にあるチェックボックスを選択します。
3. 右上の **[Manage]** (管理) ボタンをクリックします。

   ドロップダウンメニューが表示されます。
4. ドロップダウンメニューで **[Add to Group(s)]** (グループを追加する) をクリックします。

   [Add to Group(s)] (グループを追加する) ウィンドウが表示されます。
5. ウィンドウで、エージェントを追加するグループを選択します。
6. **[追加]** をクリックします。

   Tenable Nessus Manager により、選択したエージェントが 1 つまたは複数のエージェントグループに追加されます。

エージェントグループを変更する

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。
2. 左側のナビゲーションバーで **[Agent Groups]** (エージェントグループ) をクリックします。

   [Agent Groups] (エージェントグループ) ページが表示されます。
3. 次のいずれかを行います。
   - グループ名を変更する
     a. 変更するエージェントグループの行で ボタンをクリックします。

        [Edit Agent Group] (エージェントグループを編集する) ウィンドウが表示されます。
     b. **[Name]** (名前) ボックスで、エージェントグループの名前を入力します。
     c. **[Save]** (保存) をクリックします。

        Nessus Manager が変更を保存します。
   - エージェントグループにエージェントを追加する

a. エージェントグループの表で、変更するエージェントグループをクリックします。

エージェントグループの詳細ページが表示されます。

b. ページの右上にある **[Add Agents] (エージェントの追加)** ボタンをクリックします。

エージェントの追加 ウィンドウが表示されます。このウィンドウには、使用可能なエージェントのテーブルが含まれます。

c. (オプション) **[Search]** (検索) ボックスにエージェントの名前を入力し、**[Enter]** (入力) をクリックします。

エージェントの表が更新され、検索条件と一致するエージェントが表示されます。

d. グループに追加する各エージェントの横にあるチェックボックスをクリックします。

e. **[Add]** (追加) をクリックします。

選択したエージェントはグループに追加されます。

- エージェントグループからエージェントを削除する

a. エージェントグループの表で、変更するエージェントグループをクリックします。

エージェントグループの詳細ページが表示されます。デフォルトでは、[Group Details] **(グループの詳細)** タブがアクティブとなっています。

b. (オプション) テーブルのエージェントグループにフィルターを適用します。

c. (オプション) エージェントの名前で検索します。

d. 削除するエージェントを選択します。

- 個別のエージェントの場合、エージェントの横にある ✕ ボタンをクリックします。

- 複数のエージェントの場合、各エージェントの横にあるチェックボックスを選択し、ページの右上にある **[Remove]** (削除) ボタンをクリックします。

確認ウィンドウが表示されます。

e. 確認ウィンドウで削除を確定します。

- エージェントグループのユーザーのアクセス許可を変更する

1. エージェントグループの表で、アクセス許可を設定するエージェントグループをクリックします。

   エージェントグループの詳細ページが表示されます。

2. **[Permissions]** (アクセス許可) タブをクリックします。

   [Permissions] (アクセス許可]) タブが表示されます。

3. 次のいずれかを行います。

   ヒント：個別のユーザーは離職したり入社したりすることがあるので、Tenable では、メンテナンスを最小限に抑えるために個別のユーザーではなくユーザーグループにアクセス許可を割り当てることを推奨します。

   - 新しいユーザーまたはユーザーグループのアクセス許可を追加する方法

     a. **[Add users or groups]** (ユーザーまたはグループの追加) ボックスに、ユーザーまたはグループの名前を入力します。

        入力すると、ユーザーとグループのフィルタリングされたリストが表示されます。

     b. 検索結果からユーザーまたはグループを選択します。

        Tenable Vulnerability Management によりユーザーがアクセス許可リストに追加され、デフォルトのアクセス許可である **[Can Use]** (使用可能) が割り当てられます。

   - 既存のユーザーまたはユーザーグループのアクセス許可を変更する

     注意: [Default] (デフォルト) ユーザーとは、エージェントグループに特別に追加されていないすべてのユーザーを表します。

a. **[Default]** (デフォルト) ユーザーのアクセス許可ドロップダウンの横にある ▾ ボタンをクリックします。

b. アクセス許可レベルを選択します。

c. **[Save]** (保存) をクリックします。

- ユーザーまたはユーザーグループのアクセス許可を削除する
  - **[Default]** (デフォルト) ユーザーの場合、アクセス許可は **[No access]** (アクセスなし) に設定されます。
  - 他のユーザーまたはユーザーグループについて、アクセス許可を削除するユーザーまたはユーザーグループの横にある ✕ ボタンをクリックします。

4. **[Save]** (保存) をクリックします。

   Tenable Vulnerability Management がエージェントグループの変更を保存します。

エージェントグループを削除する

1. 削除するエージェントグループの行で ✕ ボタンをクリックします。

   確認ウィンドウが表示されます。

2. 確認のため、**[Delete]** (削除) をクリックします。

   マネージャーによりエージェントグループが削除されます。

フリーズ期間

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

フリーズ期間を使用して、Tenable Nessus Manager がすべてのリンクされたエージェントの特定のエージェントアクティビティを一時停止する期間をスケジュールできます。アクティビティには、次のものが含まれます。

- ソフトウェアアップデートの受信と適用
- プラグインアップデートの受信
- エージェントスキャンのインストールまたは実行

フリーズ期間を管理するには、次の手順に従います。

フリーズウィンドウの作成

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Freeze Windows]** (フリーズ期間) をクリックします。

   [Freeze Windows] (フリーズ期間) ページが表示されます。

3. 右上の **[New Window]** (新しいウィンドウ) ボタンをクリックします。

   [New Freeze Window] (新しいフリーズ期間) ページが表示されます。

4. フリーズ期間オプションを必要に応じて設定します。

オプション	説明
Name (名前)	フリーズ期間の名称。
Enabled (有効)	フリーズ期間が有効かどうかを示します。 • このスイッチをオンにすると、フリーズ期間が有効になり、フリーズ期間に割り当てられたエージェントは、そのスケジュールに基づいて特定のアクティビティからブロックされます。 • スイッチをオフにすると、フリーズ期間が無効になり、フリーズ期間に割り当てられたエージェントは、そのスケジュールを無視します。
Frequency (頻度)	フリーズ期間が発生する頻度を示します。可能な値は次のとおりです。 • Once (一度きり) • Daily (日に一度) • Weekly (週に一度) • Monthly (月に一度) • Yearly (年に一度)

Window (期間)	24 時間形式でフリーズ期間の開始時間と終了時間を決めます。時間枠は 30 分間隔で指定できます (例: 9:00 から 17:30)。
Effective (実効)	フリーズ期間が効力を持つ日付範囲を決めます (例: 2025 年 6 月 1 日から 2025 年 7 月 1 日)。**Effective** (実効) の日付範囲を過ぎると、エージェントはフリーズ期間のスケジュールを守らなくなります。
Timezone (タイムゾーン)	**Window** (期間) 範囲のタイムゾーン。

フリーズ期間のスケジュールの概要が **[Summary]** (サマリー) の横に表示されます。

5. **[Save]** (保存) をクリックします。

   フリーズ期間が有効になり、**[Freeze Windows]** (フリーズ期間) タブに表示されます。

フリーズ期間を変更する

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Freeze Windows]** (フリーズ期間) をクリックします。

   [Freeze Windows] (フリーズ期間) ページが表示されます。

3. フリーズ期間テーブルで、変更するフリーズ期間をクリックします。

   フリーズ期間の詳細ページが表示されます。

4. 必要に応じ、オプションを変更します。

オプション	説明
Name (名前)	フリーズ期間の名称。
Enabled (有効)	フリーズ期間が有効かどうかを示します。 • このスイッチをオンにすると、フリーズ期間が有効になり、フリーズ期間に割り当てられたエージェントは、そのスケジュールに基づいて特定の

	アクティビティからブロックされます。 • スイッチをオフにすると、フリーズ期間が無効になり、フリーズ期間に割り当てられたエージェントは、そのスケジュールを無視します。
Frequency (頻度)	フリーズ期間が発生する頻度を示します。可能な値は次のとおりです。 • Once (一度きり) • Daily (日に一度) • Weekly (週に一度) • Monthly (月に一度) • Yearly (年に一度)
Window (期間)	24 時間形式でフリーズ期間の開始時間と終了時間を決めます。時間枠は 30 分間隔で指定できます (例: 9:00 から 17:30)。
Effective (実効)	フリーズ期間が効力を持つ日付範囲を決めます (例: 2025 年 6 月 1 日から 2025 年 7 月 1 日)。**Effective** (実効) の日付範囲を過ぎると、エージェントはフリーズ期間のスケジュールを守らなくなります。
Timezone (タイムゾーン)	**Window** (期間) 範囲のタイムゾーン。

フリーズ期間のスケジュールの概要が **[Summary]** (サマリー) の横に表示されます。

5. **[保存]** をクリックして変更を保存します。

フリーズウィンドウの削除

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Freeze Windows]** (フリーズ期間) をクリックします。

   [Freeze Windows] (フリーズ期間) ページが表示されます。

3. フリーズ期間テーブルの、削除するフリーズ期間の行で、✕ ボタンをクリックします。

   フリーズ期間を削除する選択でよいかを確認するダイアログボックスが表示されます。

4. **[Delete]** (削除) をクリックして、削除を確定します。

   Tenable Nessus Manager は、フリーズ期間を削除します。

フリーズウィンドウのグローバル設定を変更する

Tenable Nessus Manager では、恒久的なフリーズ期間を設定し、フリーズ期間がリンクされたエージェントに対してどのように動作するかを規定するグローバル設定を行うことができます。

フリーズ期間のグローバル設定を変更するには:

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Freeze Windows]** (フリーズ期間) をクリックします。

   [Freeze Windows] (フリーズ期間) ページが表示されます。

3. **[Settings]** (設定) タブをクリックします。

4. 次のいずれかの設定を変更します。

フリーズ期間	
Enforce a permanent freeze window schedule (恒久的なフリーズ期間スケジュールを実施します)	有効にすると、Tenable Nessus Manager では恒久的なフリーズ期間が作成され、エージェントのソフトウェアが更新されないようになります。恒久的なフリーズ期間は、設定を保存した (手順 5) 直後に有効になり、他の既存のフリーズ期間をすべてオーバーライドします。 **注意:** 恒久的なフリーズ期間を終了する唯一の方法は、この設定を無効にすることです。 次のフリーズ期間設定は、恒久的なフリーズ期間の間にも適用さ

	れます。
Prevent software updates (ソフトウェアアップデートを行わない)	有効にすると、スケジュール済みのフリーズ期間中には、エージェントはソフトウェアの更新を受信しません。
Prevent plugin updates (プラグインアップデートを行わない)	有効にすると、スケジュール済みのフリーズ期間中には、エージェントはプラグインの更新を受信しません。
Prevent agent scans (エージェントスキャンの防止)	有効にすると、スケジュール済みのフリーズ期間中には、システムはエージェントスキャンを実行しません。

5. **[Save]** (保存) をクリックします。

   Tenable Nessus Manager により変更が保存されます。

クラスタリング

Tenable Nessus Manager のクラスタリングを使用すると、単一の Tenable Nessus Manager インスタンスから多数のエージェントをデプロイおよび管理できます。10,000 ~ 200,000 のエージェントを持つ Tenable Security Center ユーザーの場合、Tenable Nessus Manager の複数のインスタンスを Tenable Security Center にリンクせずに、単一の Tenable Nessus Manager クラスタからエージェントスキャンを管理できます。

クラスタリングが有効になっている Tenable Nessus Manager インスタンスは*子ノード*の*親ノード*として機能し、それぞれが少数のエージェントを管理します。Tenable Nessus Manager インスタンスが親ノードになると、エージェントを直接管理しなくなります。代わりに、子ノード全体にわたるすべてのエージェントのスキャンポリシーとスケジュールを管理できる単一のアクセスポイントとして機能します。クラスタリングを使用すると、複数の異なる Tenable Nessus Manager インスタンスを個別に管理する場合よりも簡単にデプロイメントサイズを調整できます。

シナリオの例: 100,000 のエージェントをデプロイする

Tenable Security Center ユーザーの担当者が、Tenable Nessus Managerに管理されている 100,000 のエージェントをデプロイするとします。

*クラスタリングを使用しない*場合、それぞれが 10,000 のエージェントをサポートする、10 個の Tenable Nessus Manager インスタンスをデプロイします。エージェントスキャンポリシーとスケジュールの設定、ソフトウェアバージョンの更新など、各 Tenable Nessus Manager インスタンスを個別に手動で管理する必要があります。各 Tenable Nessus Manager インスタンスを、Tenable Security Center に個別にリンクする必要があります。

*クラスタリングを使用する*場合、1 つの Tenable Nessus Manager インスタンスを使用して 100,000 のエージェントを管理します。Tenable Nessus Manager でクラスタリングを有効にすると、それが親ノードとなり、子ノードの管理ポイントに変わります。10 個の子ノードをリンクし、それぞれが約 10,000 のエージェントを管理します。新しいエージェントをリンクするか、クラスタに既存のエージェントを移行できます。子ノードは、親ノードからエージェントスキャンポリシー、スケジュール、プラグイン、ソフトウェアの更新を受け取ります。Tenable Nessus Manager 親ノードのみを Tenable Security Center にリンクできます。

注意: クラスタ内のすべての Tenable Nessus ノードは、同じバージョンである必要があります (たとえば上記のクラスタの例を使用する場合、Tenable Nessus Manager 親ノードと 10 個の子ノードは同じ Tenable Nessus バージョンである必要があります)。バージョンが異なる場合、クラスタのデプロイメントはサポートされません。

定義

Parent node - 子ノードがリンクする、クラスタリングが有効なTenable Nessus Managerインスタンスです。

Child node - Tenable Agentsが接続するノードとして機能するTenable Nessusインスタンスです。

Tenable Nessus Manager cluster - 親ノードとその子ノード、および関連エージェントです。

詳細については、次のトピックを参照してください。

- クラスタリングのシステム要件
- クラスタリングを有効にします
- ノードからリンクキーを取得してください。
- ノードをリンクする
- エージェントをクラスタに移行する
- エージェントをクラスタにリンクする
- ノードを有効または無効にする
- ノードのバランスを再調整する

- ノードを表示または編集する
- ノードを削除する
- クラスタグループ

クラスタリングのシステム要件

次に示すのは、親ノードと子ノードのシステム要件です。これらの推定値は、KB および監査証跡の設定が無効になっていると想定しています。これらの設定を有効にすると、必要なサイズが大幅に増加する可能性があります。Tenable では、このような場合は標準システム要件を少なくとも 50% 増やすことを推奨しています。

注意: クラスタ内のすべての Tenable Nessus ノードは、同じ Tenable Nessus バージョンである必要があります。バージョンが異なる場合、クラスタのデプロイメントはサポートされません。

注意: クラスタリング環境でパフォーマンスが低下した場合、Tenable は、ハードウェア要件 をレビューして親ノードと子ノードが適切に設定されていることを確認するよう強くお勧めします。

警告: Tenable では、Tenable Nessus クラスタリング環境で共有リソースを使用しないことを強く推奨しています。使用すると、重大なパフォーマンスの問題が発生する可能性があります。

親ノード (クラスタリングが有効になっている Tenable Nessus Manager)

Tenable は、1 つの Tenable Nessus Manager 子ノードにつき最大 20,000 のエージェントの接続をサポートします。

注意: 必要なディスク容量は、保持するエージェントのスキャン結果の数と保存期間に応じて異なります。たとえば、5,000 個のエージェントによる単一のスキャンを 1 日に 1 回実行し、スキャン結果を 7 日間保持する場合、使用されるディスク容量は 35 GB と推定されます。スキャン結果ごとに必要なディスク容量は、検出された脆弱性の一貫性、数、種類に応じて異なります。

- **CPU** – すべての実装で最小 8 コア、3 つの子ノードごとに 8 コア追加
- **RAM** – すべての実装で最小 16 GB、子ノードを追加するたびに 4 GB 追加
- **ディスク** – 5,000 のエージェントにつき 5 GB (スキャン 1 回 / 1 日当たりの推定最小容量)

注意: 親ノードには、すべての子ノードで使用されるディスク容量を累積した容量が必要です。たとえば、親ノードに3つの子ノードがあり、それぞれに1 GBのディスク容量が必要な場合、親ノード自体のディスク容量要件に加えて3 GBのディスク容量が必要です。

子ノード (Tenable Nessus Manager 親ノードによって管理される Tenable Nessus スキャナー)

注意: ディスク容量は、結果を親ノードにアップロードする前に、エージェントスキャン結果 (個別と結合の両方) を一時的に保存するために使用されます。

0 ~ 10,000 のエージェントがある子ノード:

- **CPU** – 4 コア
- **RAM** – 16 GB
- **ディスク** – 5,000 のエージェントにつき 5 GB (同時スキャン当たりの推定最小容量)

10,000 ~ 20,000 のエージェントがある子ノード:

子ノードは、最大 20,000 のエージェントをサポートできます。

- **CPU** – 8 コア
- **RAM** – 32 GB
- **ディスク** – 5,000 のエージェントにつき 5 GB (同時スキャン当たりの推定最小容量)

エージェント

リンクするエージェントは、サポートされている Tenable Agent バージョンである必要があります。

クラスタリングを有効にします

を使用する場合に必要なユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Nessus Manager でクラスタリングを有効にすると、それが*親ノード*になります。その後、*子ノード*をリンクでき、各子ノードで Tenable Agents が管理されます。一度親ノードでクラスタリングを有効にすると、操作を取り消すことはできず、Tenable Nessus Manager を通常のスキャナーや Tenable Agent マネージャーに変えることもできません。

注意：Tenable Nessus 8.5.x または 8.6.x で Tenable Nessus Manager のクラスタリングを有効にするには、Tenable の担当者に問い合わせる必要があります。Tenable Nessus Manager 8.7.x 以上では、以下の手順に従ってクラスタリングを有効にできます。

注意: クラスタ内のすべての Tenable Nessus ノードは、同じバージョンである必要があります。バージョンが異なる場合、クラスタのデプロイメントはサポートされません。

Tenable Nessus Manager でクラスタリングを有効にする方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Setup] (クラスタセットアップ) ページが表示され、**[Settings]** (設定) タブ画面となります。

3. **[Enable Cluster]** (クラスタを有効にする) を選択します。

   警告：一度親ノードでクラスタリングを有効にすると、操作を取り消すことはできず、Tenable Nessus Manager を通常のスキャナーや Tenable Agent マネージャーに変えることもできません。

4. **[Save]** (保存) をクリックします。

   Tenable Nessus Manager がクラスタの親ノードになります。

次の手順

- 子ノードを親ノードにリンクします。
- クラスタグループを管理します。

エージェントをクラスタに移行する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

リンクされたエージェントを持つ、クラスタリングされていない Tenable Nessus Manager のインスタンスがある場合、リンクされたエージェントを既存のクラスタに移行できます。クラスタに移行されたエージェントは、元の Tenable Nessus Manager とのリンクが解除されます。移行されなかったエージェントは、引き続き

元の Tenable Nessus Manager にリンクされます。元の Tenable Nessus Manager は Tenable Nessus Manager インスタンスのままで、クラスタには含まれません。

始める前に

- エージェントを移行できる稼働中のクラスタがあることを確認してください。そのクラスタは、Tenable Nessus クラスタリングのシステム要件を満たしている必要があります。稼働中のクラスタがない場合は、クラスタの親ノードにする Tenable Nessus Manager インスタンスでクラスタリングを有効化します。
- エージェントの移行先となるクラスタの Tenable Nessus Manager 親ノードの **[Linked Agents]** (リンク済みエージェント) ページから、リンクキーを取得します。

エージェントをクラスタに移行する方法

1. リンクされたエージェントを持つ、クラスタリングされていない Tenable Nessus Manager インスタンスにアクセスします。
2. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。
3. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Setup] (クラスタセットアップ) ページが表示され、**[Settings]** (設定) タブ画面となります。
4. **[Cluster Migration]** (クラスタの移行) タブをクリックします。
5. **[Cluster Information]** (クラスタ情報) を入力します。
   - **親ノードのホスト名** - 移行するクラスタの Tenable Nessus Manager 親ノードのホスト名または IP アドレスを入力します。
   - **Parent Node Port** - 指定した親ノードホストのポートを入力します。デフォルトは 8834 です。
   - **親ノードのリンクキー** - ノードからリンクキーを取得してください。の説明に従い、Tenable Nessus Manager 親ノードからコピーしたリンクキーを貼り付けるか、入力します。

- **エージェントの移行を有効にする** - このチェックボックスを選択して、エージェントをクラスタに移行します。エージェントの移行中に移行を停止するには、このチェックボックスを無効にします。

6. **[Save]** (保存) をクリックします。

   [Enable Agent Migration] (エージェントの移行を有効にする) を選択しているかどうかに応じて、Tenable Nessus Manager でクラスタへのエージェントの移行が開始または停止されます。

次の手順

Tenable Nessus Manager 親ノードにログインして、リンクされた Tenable Agents を管理します。

エージェントをクラスタにリンクする

> **を使用する場合に必要な [ユーザーロール]Tenable Nessus Manager:** 管理者またはシステム管理者

クラスタグループの設定に応じて、エージェントを親ノードまたは子ノードにリンクできます。一般的に、親ノードにリンクすることが推奨されています。ただし、地理的に分散したクラスタグループがあり、エージェントを特定のクラスタグループに確実にリンクしたい場合は、子ノードにリンクする方が有用かもしれません。

クラスタに関する一般的な情報については、クラスタリングを参照してください。

始める前に

- ノードからリンクキーを取得してください。.エージェントリンクコマンドの **--key** 引数には、ノードのリンクキーが必要です。

エージェントを親ノードにリンクする方法

このシナリオでは、エージェントがクラスタの親ノードにリンクして、子ノードのリストを受け取り、クラスタ内の子ノードへの接続を試みます。

1. コマンドターミナルから Tenable Agent にログインします。
2. エージェントのコマンドプロンプトで、コマンド `nessuscli agent link` とサポートされている引数を使用して親ノードにリンクします。

   たとえば、次のようになります。

   Linux

```
/opt/nessus_agent/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
```

macOS

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
```

Windows

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
```

サポートされているエージェントリンク引数のリストを表示するには、Nessus CLI Agent Commands を参照してください。

エージェントを子ノードにリンクする方法

このシナリオでは、エージェントが特定のクラスタグループ内の子ノードにリンクし、そのクラスタグループ内のすべての子ノードのリストを受け取ります。次に、エージェントがクラスタグループ内の子ノードへの接続を試みます。

1. コマンドターミナルから Tenable Agent にログインします。
2. エージェントのコマンドプロンプトで、コマンド `nessuscli agent link` とサポートされている引数を使用して子ノードにリンクします。

   たとえば、次のようになります。

Linux

```
/opt/nessus_agent/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
```

```
--name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
```

macOS

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
```

Windows

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
```

サポートされているエージェントリンク引数のリストを表示するには、Nessus CLI Agent Commandsを参照してください。

クラスタのアップグレード

> **を使用する場合に必要なユーザーロールTenable Nessus Manager:** System Administrator

クラスタが自動的に更新されるように設定されておらず、新しいTenable Nessusバージョンに更新する必要がある場合は、次の手順を使用してクラスタの親ノードと子ノードを手動で更新します。クラスタノードのバージョンを手動で更新する場合は、記載されている順番にノードを停止、アップグレード、起動することが重要です。こうすることで、子ノードが実行されていれば、子ノードは親ノードにアクセスでき、引き続きスキャン結果やその他のデータを提供できます。

自動的に更新するようにクラスタを設定するには、Tenable Nessusソフトウェアを更新するで説明されているように各ノードの**Nessus更新プラン**を設定します。

Tenable Nessusのクラスタリングの詳細については、クラスタリングおよびクラスタリングのシステム要件を参照してください。

Tenable Nessusクラスタを手動で更新する方法

1. 子ノードで Tenable Nessus を停止します。
2. 親ノードで Tenable Nessus を停止します。
3. 親ノードを目的のバージョンに更新します。
4. 子ノードを目的のバージョンに更新します。
5. 親ノードで Tenable Nessus を起動します。
6. 子ノード Tenable Nessus で起動します。

   新しいバージョンを使用してすべてのノードを起動したら、アップグレードプロセスは完了です。

ノードを管理する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

クラスターノードを管理するには、次のトピックを参照してください。

- ノードからリンクキーを取得してください。
- ノードをリンクする
- ノードを表示または編集する
- ノードを有効または無効にする
- ノードのバランスを再調整する
- ノードを表示または編集する
- ノードを削除する

クラスタグループを管理するには、クラスタグループを参照してください。

ノードからリンクキーを取得してください。

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

子ノードをリンクする、またはエージェントをクラスタに移行するには、クラスタの親ノードからのリンクキーが必要です。同様に、エージェントを子ノードに直接リンクするには、そのクラスタ子ノードからのリンクキーが必要です。

注意: nessuscli から子ノードのリンクキーを取得することもできます。詳細については、nessuscli Fix コマンドセクションの nessuscli fix --secure --get child_node_linking_key を参照してください。

始める前に

- リンク先にするノードでクラスタリングを有効にします。

ノードからのリンクキーを取得する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。

3. **リンクキー**をコピーまたはメモします。

次の手順

- クラスタに子ノードをリンクします。
- クラスタに新しいエージェントをリンクします。
- クラスタに既存のエージェントを移行します。

ノードをリンクする

を使用する場合に必要なユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

子ノードをクラスタにリンクするには、Tenable Nessus のインスタンスをクラスタの子ノードとしてインストールしてから、クラスタの親ノードにリンクするようにノードを設定します。

注意: 始める前に、クラスタの親ノードからリンクキーを取得する必要があります。これは、1 回のセッションで子ノードを親ノードにリンクするプロセスを完了する必要があるためです。プロセスを開始し、そのプロセスが完了する前にユーザーインターフェースから移動すると、子ノードのユーザーインターフェースが早く無効にある可能性があります。

Tenable Nessus を子ノードとしてインストールして設定する

1. お使いのオペレーティングシステムに適した Tenable Nessus のインストール 手順に従い、Tenable Nessus をインストールします。
2. **[Welcome to Nessus]** (Nessus へようこそ) で、**[Link Nessus to another Tenable product]** (Nessus を別の Tenable 製品にリンクする) を選択します。
3. **[Continue]** (続行) をクリックします。

   [Managed Scanner] (管理スキャナー) 画面が表示されます。
4. **[Managed by]** (管理者) ドロップダウンボックスから **[Nessus Manager (Cluster Node)]** (Nessus Manager (クラスタノード)) を選択します。
5. **[Continue]** (続行) をクリックします。

   [Create a user account] (ユーザーアカウントの作成) 画面が表示されます。
6. Tenable Nessus へのログインに使用する Tenable Nessus 管理者のユーザーアカウントを次の手順で作成します。
   a. **[Username]** (ユーザー名) ボックスにユーザー名を入力します。
   b. **[Password]** (パスワード) ボックスにユーザーアカウントのパスワードを入力します。
7. **[Submit]** (送信) をクリックします。

   Tenable Nessus が設定プロセスを完了します。これには数分かかる場合があります。

子ノードを親ノードにリンクする方法

1. Tenable Nessus 子ノードで、初期設定時に作成した管理者ユーザーアカウントを使用して Tenable Nessus にサインインします。

   [Agents] (エージェント) ページが表示されます。デフォルトでは、**[Node Settings]** (ノード設定) タブが表示されます。
2. **[On]** (オン) に切り替えて有効化します。
3. **[General Settings]** (全般設定) を設定します。
   - **ノード名** – 親ノードでこの Tenable Nessus 子ノードを識別する一意の名前を入力します。
   - (オプション) **Node Host** - Tenable Agents が子ノードにアクセスするために使用するホスト名または IP アドレスを入力します。ホストノードを指定しない場合、Tenable Agent はシステ

ムホスト名を使用します。Tenable Agent がホスト名を検出できない場合、リンクは失敗します。

- (オプション) **Node Port** - 指定したホストのポートを入力します。

4. **[Cluster Settings]** (クラスタ設定) を設定します。

   - **Cluster Linking Key** - Tenable Nessus Manager 親ノードからコピーしたリンクキーを貼り付けるか、入力します。
   - **Parent Node Host** - リンクする Tenable Nessus Manager 親ノードのホスト名または IP アドレスを入力します。
   - **Parent Node Port** - 指定したホストのポートを入力します。デフォルトは 8834 です。
   - (オプション) **Use Proxy** - プロキシサーバーに設定されているプロキシ設定を介して親ノードに接続する場合は、このチェックボックスを選択します。

5. **[Save]** (保存) をクリックします。

   確認ウィンドウが表示されます。

6. ノードの親ノードへのリンク実行を確認するために、**[Continue]** (続行) をクリックします。

   Tenable Nessus 子ノードが親ノードにリンクされます。Tenable Nessus によりユーザーインターフェースからログアウトされ、ユーザーインターフェースが無効になります。

   > **注意:** 子ノードのユーザーインターフェースを無効にすると、それ以降、子ノードのユーザーインターフェースにアクセスしようとすると、エラー: リクエストされたファイルが見つかりませんでしたというエラーが発生します。

次の手順

- Tenable Nessus Manager 親ノードにログインして、リンクされた Tenable Agents およびノードを管理します。
- クラスタに新しいエージェントをリンクまたは移行します。
- Tenable Nessus Manager 親ノードで、お使いのネットワークトポロジーに適したグループにノードを整理するために、クラスタグループを管理します。特定のエージェントが特定の子ノードにしかアクセスできない場合は、クラスタグループでネットワークをセグメント化する必要があります。デフォルトでは、Nessus はノードをデフォルトのクラスタグループに割り当てます。

ノードを表示または編集する

を使用する場合に必要なユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

クラスタリングが有効になっている Tenable Nessus Manager では、現在、親ノードにリンクされている子ノードのリストを表示できます。Tenable Nessus は、これらの子ノードをクラスタグループに割り当てます。ステータス、IP アドレス、リンクされたエージェントの数、ソフトウェア情報、プラグインセットなど特定のノードの詳細を表示できます。ノードのエージェントがスキャンを実行中の場合、スキャンの進行状況バーが表示されます。

ノードの名前や子ノードにリンクできるエージェントの最大数を編集できます。

子ノードを表示または編集する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。

3. クラスタグループテーブルで、子ノードを含むクラスタグループの行をクリックします。

   [Cluster Nodes] (クラスタノード) タブが表示されます。**[Cluster Nodes] (クラスタノード)** テーブルには、各クラスタノードに関する次の情報が表示されます。

列	説明
Name (名前)	子ノード名です。
Status (ステータス)	子ノードの現在の状態を示します。 • **アイドル** – ノードは非アクティブであり、スキャンも再調整も実行されていません。 • **アイドル (無効)** – ノードは、 ボタンにより手動で無効にされています。 • **スキャン中** – ノードがスキャン中です。

Scan (スキャン)	子ノードが加わっている進行中のスキャン数です。
Usage (使用)	この列は、最大容量と比較して、現在ノードにリンクされているエージェント数を示します。 **注意:** ノードあたりの最大のエージェント数は、後のステップ 8 で設定できます。
Last Connected (最終接続日)	子ノードが親ノードと通信した最終日時です。
Link (リンク)	をクリックして、クラスタグループ内で子ノードを有効または無効にします。
Delete (削除)	をクリックして、クラスタグループから子ノードを削除します。

4. 表示する子ノードの行をクリックします。

   Tenable Nessus Manager は、**[Node Details]** (ノードの詳細情報) タブを表示します。

5. **[Node Details]** (ノードの詳細情報) タブで、選択したノードの詳細情報を表示します。

6. ノードを別のクラスタグループに移動するには、次を実行します。

   a. **[Cluster Group]** (クラスタグループ) の横にある ボタンをクリックします。

      [Change Cluster Group] (クラスタグループの変更) ダイアログボックスが表示されます。

   b. ドロップダウンメニューで、別のクラスタグループを選択します。

   c. **[Save]** (保存) をクリックします。

      ノードが別のクラスタグループに移動します。

7. ノードの設定を編集するには、**[Settings]** (設定) タブをクリックします。

8. 次のいずれかを編集します。

   - **ノード名** – ノードを識別するための一意の名前を入力します。
   - **Max Agents** – 子ノードにリンクできるエージェントの最大数を入力します。デフォルト値は 10,000 で、最大値は 20,000 です。

9. **[Save]** (保存) をクリックします。

Tenable Nessus Manager がノード設定を更新します。

ノードを有効または無効にする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

子ノードを無効にすると、そのリンクされた Tenable Agents は、同じクラスタグループ内で利用可能な別の子ノードに再リンクされます。子ノードを再度有効にすると、Tenable Agents は不均等に分散される可能性があります。この時点で ノードのバランスを再調整する を選択できます。

子ノードを有効または無効にする方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。

3. クラスタグループテーブルで、子ノードを含むクラスタグループの行をクリックします。

4. 子ノードの行で、次のいずれかを行います。

   - ノードを無効にする方法

     a. ボタンにカーソルを合わせます。 になります。

     b. ボタンをクリックします。

     Tenable Nessus Managerによって子ノードが無効化されます。

   - ノードを有効にする方法

     a. カーソルをボタンに合わせます。 になります。

     b. ボタンをクリックします。

     Tenable Nessus Managerによって子ノードが有効化されます。

ノードのバランスを再調整する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Agents は、さまざまな理由 (1 つまたは複数の子ノードが一時的に利用不能あったり、無効化、削除、最近追加されたりしたなど) により、子ノード間に均等に分散されない場合があります。このようなイベントは、クラスタのパフォーマンスに悪影響を与えます。こうした不均衡が特定のしきい値に達したときに、Tenable Nessus Manager では子ノードのバランスを再調整することを選択できます。次の条件のいずれかまたは両方が満たされると、このしきい値を超えます。

- ノードの理想的なキャパシティに基づいて、エージェントの 10% が理想的に分散されていない
- 1 つのノードに、ノードの理想的なキャパシティよりも 5% 以上多くのエージェントがある

  例

  ユーザーの所属組織では、4 つのノードと 100 のリンクされたエージェントがあります。リンクされたエージェントを 4 つのノードに均等に分散するには、Tenable Nessus Manager が各ノードに、リンクされたエージェント全体の 25% を割り当てる必要があります。この場合、ノードあたりのリンクされたエージェントの数は 25 になります。

  以下のいずれかの場合、Tenable Nessus Manager には子ノードのバランスを再調整できるオプションがあります。

  - *より良い結果を得るために、Tenable Nessus Manager がリンクされたエージェントの 10% 以上 (この例では、10 以上のリンクされたエージェント) を再分散できる。たとえば、2 つのノードのリンクされたエージェントの数が 20 であり、もう 2 つのノードのリンクされたエージェントの数が 30 である場合、Tenable Nessus Manager により、ノードのバランスが再調整され、理想的な 25-25-25-25 に分散されます。*
  - *1 つのノードでそのキャパシティの 30% に達している (この例では約 33 個のリンクされたエージェント)。*

子ノードのバランスを再調整すると、Tenable Agents はクラスタグループ内の子ノード間で、より均等に再配分されます。Tenable Agents は、過剰に読み込まれた子ノードとのリンクを解除し、可用性の高い子ノードに再びリンクします。

子ノードのバランスを再調整する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。

3. クラスタグループテーブルで、クラスタグループの行をクリックします。

4. ページの右上隅で、**[Rebalance Nodes]** (ノードのバランスを再調整する) をクリックします。

   Tenable Nessus Manager が子ノード間における Tenable Agent の配分バランスを再調整します。

ノードを削除する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

子ノードを削除すると、リンクされた Tenable Agents は最終的に、同じクラスタグループ内で利用可能な別の子ノードに再リンクされます。ノードを削除した場合、ノードを無効にした場合と比べて再リンクに長い時間がかかる可能性があります。

削除するノードが、リンクされたエージェントを持つクラスタグループの最後のノードである場合、まずエージェントを別のクラスタグループに移動する必要があります。単に子ノードを一時的に無効にする場合は、ノードを有効または無効にするを参照してください。

子ノードを削除する方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。

3. クラスタグループテーブルで、子ノードを含むクラスタグループの行をクリックします。

4. 削除する子ノードの行で、✕ボタンをクリックします。

   [Delete Agent Node] (エージェントノードの削除) ダイアログボックスが表示されます。

   > **注意:** ノードを削除した場合、操作を取り消すことはできません。

5. 子ノードの削除を確定するには、**[Delete]** (削除) をクリックします。

   Tenable Nessus Manager によって子ノードが削除されます。

クラスタグループ

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** 管理者またはシステム管理者

クラスタをクラスタグループに分割することで、お使いのネットワークトポロジーに適した方法でエージェントをデプロイおよびリンクすることが可能になります。たとえば、ノードやエージェントが物理的に存在する地域別のクラスタグループを作成できます。こうすることで、エージェントの接続が発生する場所のネットワークトラフィックや管理が最小限となります。

クラスタの子ノードはクラスタグループに所属する必要があり、同時に 1 つのクラスタグループにしか所属できません。各クラスタグループ内のエージェントは、同じクラスタグループ内のノードにしかリンクしません。

クラスタグループはエージェントグループとは異なります。エージェントグループは、ターゲットをスキャンするために指定する、エージェントのグループです。クラスタグループを使用して、エージェントがクラスタ内でリンクするノードを管理します。

クラスタグループと、そこに割り当てられたノードおよびエージェントを管理するには、次を参照してください。

クラスターグループを作成する

デフォルトでは、Tenable Nessus は新しいノードとエージェントをデフォルトのクラスタグループに割り当てます。お使いのネットワークトポロジーに適したクラスタグループを作成できます。たとえば、ノードやエージェントが物理的に存在する地域別のクラスタグループを作成できます。こうすることで、エージェントの接続が発生する場所のネットワークトラフィックや管理が最小限となります。

クラスタグループはエージェントグループとは異なります。エージェントグループは、ターゲットをスキャンするために指定する、エージェントのグループです。クラスタグループでは、エージェントがクラスタ内でリンクするノードを管理できます。

注意: クラスタの子ノードの自動ソフトウェアアップデートが無効になっている場合、エージェントクラスタグループを使用するには Nessus 8.12 以降に手動でアップデートする必要があります。クラスタの子ノードの自動ソフトウェアアップデートが有効になっている場合、ノードがアップデートされるのに最大 24 時間かかります。リンクと設定が正しく行われるように、すべての子ノードがサポートされている Nessus バージョンにアップデートされるのを待ってから、カスタムクラスタグループを設定してください。すべての子ノードは、同じ Nessus バージョンおよびオペレーティングシステムである必要があります。

始める前に

- Tenable Nessus Manager 親ノードでクラスタリングを有効にしますを行います。

クラスタグループを作成する方法

1. Tenable Nessus Manager 親ノードにログインします。
2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。
3. 右上の ⊕ **[New Cluster Group]** (新規のクラスタグループ) をクリックします。

   [New Cluster Group] (新規のクラスタグループ) ウィンドウが表示されます。
4. クラスタグループの **[Name]** (名前) を入力します。
5. **[Add]** (追加) をクリックします。

   Tenable Nessus Manager により、新しいクラスタグループが作成されます。

クラスターグループを変更する

クラスタグループの名前を変更したり、クラスタグループをデフォルトのクラスタグループとして設定したりできます。Tenable Nessus は、リンクされた新しいノードをデフォルトのクラスタグループに割り当てます。

クラスタグループを変更する方法

1. Tenable Nessus Manager 親ノードにログインします。
2. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

3. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。

4. クラスタグループテーブルの変更するクラスタグループの行で、✎ ボタンをクリックします。

   [Edit Cluster Group] (クラスタグループを編集する) ウィンドウが表示されます。

5. 次のいずれかの設定を編集します。

   - **名前** – クラスタグループの新しい名前を入力します。
   - **Set as Default** – このクラスタグループを、Tenable Nessus が新しいリンクされたノードを追加するデフォルトのクラスタグループに設定するには、このチェックボックスを選択します。

6. **[Save]** (保存) をクリックします。

   Tenable Nessus Manager により、クラスタグループの設定が更新されます。

ノードをクラスターグループに追加する

デフォルトでは、Tenable Nessus は、リンクされた新しいノードをデフォルトのクラスタグループに割り当てます。ノードを手動で別のクラスタグループに追加することもできます。たとえば、同じような場所に存在する複数のノードを同じクラスタグループに追加できます。ノードは、同時に 1 つのクラスタグループにしか所属できません。

別のクラスタグループに所属していたノードを移動すると、そのノードにリンクされていたエージェントはすべて元のクラスタグループに残り、元のクラスタグループ内の別のノードに再リンクされます。

> **注意:** クラスタの子ノードの自動ソフトウェアアップデートが無効になっている場合、エージェントクラスタグループを使用するには Nessus 8.12 以降に手動でアップデートする必要があります。クラスタの子ノードの自動ソフトウェアアップデートが有効になっている場合、ノードがアップデートされるのに最大 24 時間かかります。リンクと設定が正しく行われるように、すべての子ノードがサポートされている Nessus バージョンにアップデートされるのを待ってから、カスタムクラスタグループを設定してください。すべての子ノードは、同じ Nessus バージョンおよびオペレーティングシステムである必要があります。

始める前に

- ノードをリンクするの説明に従い、クラスタに最低 1 つの子ノードを追加していることを確認します。
- デフォルトのクラスターグループ以外のクラスターグループにノードを追加する場合は、最初にクラスターグループを作成します。

子ノードをクラスタグループに追加する方法

1. Tenable Nessus Manager 親ノードにログインします。
2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。
3. クラスタグループテーブルで、ノードを追加するクラスタグループの行をクリックします。

   クラスタグループの詳細ページが表示され、デフォルトでは **[Cluster Nodes]** (クラスタノード) タブが表示されます。
4. 右上の ⊕ **[Add Nodes]** (ノードを追加) をクリックします。

   [Add Nodes] (ノードを追加) ウィンドウが表示され、追加可能なノードが表示されます。
5. (オプション) 結果をフィルタリングするためにノードの名前で検索します。
6. ノードテーブルで、追加する各ノードの横にあるチェックボックスを選択します。

   > **注意:** ノードは、同時に 1 つのクラスタグループにしか所属できません。別のクラスタグループに所属していたノードを移動すると、そのノードにリンクされていたエージェントはすべて元のクラスタグループに残り、元のクラスタグループ内の別のノードに再リンクされます。
7. **[Add]** (追加) をクリックします。

   Tenable Nessus Managerにより、ノードがクラスタグループに移動します。

エージェントをクラスターグループに追加する

デフォルトでは、Tenable Nessus は新しいエージェントをデフォルトのクラスタグループに割り当てます。エージェントを手動で別のクラスタグループに追加することもできます。たとえば、同じような場所に存在する複数のエージェントを同じクラスタグループに追加できます。エージェントは、同時に 1 つのクラスタグループにしか所属できません。

エージェントをクラスタグループに追加すると、エージェントはそのクラスタグループで利用可能なノードに再リンクされます。

始める前に

- ノードをリンクするの説明に従い、クラスタに最低 1 つの子ノードを追加していることを確認します。
- エージェントを追加するクラスターグループに、最低 1 つのノードがあることを確認します。

エージェントをクラスタグループに追加する方法

1. Tenable Nessus Manager 親ノードにログインします。
2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。
3. クラスタグループテーブルで、エージェントを追加するクラスタグループの行をクリックします。

   クラスタグループの詳細ページが表示され、デフォルトでは **[Cluster Nodes]** (クラスタノード) タブが表示されます。
4. **[Agents]** (エージェント) タブをクリックします。

   クラスタグループに割り当てられたエージェントがテーブルに表示されます。
5. 右上の ⊕ **[Add Agents]** (エージェントを追加) をクリックします。

   [Add Agents] (エージェントを追加) ウィンドウが表示され、追加可能なエージェントが表示されます。
6. (オプション) 結果をフィルタリングするためにエージェントの名前で検索します。
7. エージェントテーブルで、追加する各エージェントの横にあるチェックボックスを選択します。

   > **注意:** エージェントは、同時に 1 つのクラスタグループにしか所属できません。エージェントを別のグループに移動すると、エージェントは新しいクラスタグループで利用可能なノードに再リンクされます。
8. **[Add]** (追加) をクリックします。

   Tenable Nessus Manager により、エージェントがクラスタグループに追加されます。

ノードをクラスターグループに移動する

デフォルトでは、Tenable Nessus は、リンクされた新しいノードをデフォルトのクラスタグループに割り当てます。ノードを手動で別のクラスタグループに追加することも可能です。たとえば、同じような場所に存在する複数のノードを同じクラスタグループに追加できます。ノードは、同時に 1 つのクラスタグループにしか所属できません。

別のクラスタグループに所属していたノードを移動すると、そのノードにリンクされていたエージェントはすべて元のクラスタグループに残り、元のクラスタグループ内の別のノードに再リンクされます。

始める前に

- ノードをリンクするの説明に従い、クラスタに最低 1 つの子ノードを追加していることを確認します。
- デフォルトのクラスターグループ以外のクラスターグループにノードを移動する場合は、最初にクラスターグループを作成します。

子ノードを別のクラスタグループに移動する方法

1. Tenable Nessus Manager 親ノードにログインします。
2. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。
3. クラスタグループテーブルで、移動するエージェントを含むクラスタグループの行をクリックします。

   クラスタグループの詳細ページが表示され、デフォルトでは **[Cluster Nodes]** (クラスタノード) タブが表示されます。
4. クラスタノードテーブルで、別のクラスタグループに移動する各ノードのチェックボックスを選択します。

   > **注意:** クラスタグループに割り当てられているエージェントが存在する場合、クラスタグループに最低 1 つのノードを残す必要があります。
5. 右上の **[Move]** (移動) をクリックします。

   [Move Node] (ノードを移動する) ウィンドウが表示されます。
6. ドロップダウンボックスで、ノードの移動先となるクラスタグループを選択します。

   > **注意:** ノードは、同時に 1 つのクラスタグループにしか所属できません。別のクラスタグループに所属していたノードを移動すると、そのノードにリンクされていたエージェントはすべて元のクラスタグループに残り、元のクラスタグループ内の別のノードに再リンクされます。
7. **[Move]** (移動) をクリックします。

   Tenable Nessus Manager により、選択されたクラスタグループにノードが移動します。

エージェントをクラスターグループに移動する

デフォルトでは、Tenable Nessus は新しいエージェントをデフォルトのクラスタグループに割り当てます。エージェントを手動で別のクラスタグループに追加することも可能です。たとえば、同じような場所に存在

する複数のエージェントを同じクラスタグループに追加できます。エージェントは、同時に1つのクラスタグループにしか所属できません。

エージェントをクラスタグループに移動すると、エージェントはそのクラスタグループで利用可能なノードに再リンクされます。エージェントの移動中または再リンク中は、クラスタグループに一覧表示されるエージェントの数に不整合が生じる可能性があります。

始める前に

- ノードをリンクするの説明に従い、クラスタに最低1つの子ノードを追加していることを確認します。
- エージェントを追加するクラスターグループに、最低1つのノードがあることを確認します。

エージェントを別のクラスタグループに移動する方法

1. Tenable Nessus Manager 親ノードにログインします。
2. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。
3. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。
4. クラスタグループテーブルで、移動するエージェントを含むクラスタグループの行をクリックします。

   クラスタグループの詳細ページが表示され、デフォルトでは **[Cluster Nodes]** (クラスタノード) タブが表示されます。
5. **[Agents]** (エージェント) タブをクリックします。

   クラスタグループに割り当てられたエージェントがテーブルに表示されます。
6. エージェントテーブルで、別のクラスタグループに移動する各エージェントのチェックボックスを選択します。
7. 右上の **[Move]** (移動) をクリックします。

   [Move Agent] (エージェントを移動する) ウィンドウが表示されます。
8. ドロップダウンボックスで、エージェントの移動先となるクラスタグループを選択します。

> **注意**：エージェントは、同時に 1 つのクラスタグループにしか所属できません。エージェントを別のグループに移動すると、エージェントは新しいクラスタグループで利用可能なノードに再リンクされます。

9. **[Move]** (移動) をクリックします。

   Tenable Nessus Manager により、エージェントがクラスタグループに移動します。

クラスターグループを削除する

ノードやエージェントが割り当てられていないクラスタグループは削除できます。デフォルトのクラスタグループは削除できません。

始める前に

- クラスタグループ内のノードを移動または削除します。

クラスタグループを削除する方法

1. Tenable Nessus Manager 親ノードにログインします。
2. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。
3. 左側のナビゲーションバーで **[Agent Clustering]** (エージェントのクラスタリング) をクリックします。

   [Cluster Groups] (クラスタグループ) ページが表示されます。
4. クラスタグループテーブルの削除するクラスタグループの行で、✕ ボタンをクリックします。

   [Delete Cluster Group] (クラスタグループを削除する) ウィンドウが表示されます。
5. クラスタグループの削除を確定するために、**[Delete]** (削除)をクリックします。

   > **注意**：この操作を取り消すことはできません。

   Tenable Nessus Managerによりクラスタグループが削除されます。

スキャナー

Tenable Nessus Manager では、インスタンスのリンクキーと、リンクされているリモート スキャナーの一 覧を表 示 できます。リンク済 みスキャナーをクリックすると、そのスキャナーの詳 細 が表 示 されます。

スキャナーにはスキャナーの種 類 が表 示 され、スキャナーに**共 有** 許 可 があるかどうかが示 されます。

リモート スキャナーは、リンクキーまたは有 効 なアカウント認 証 情 報 を使 用 して Nessus Manager にリンクできます。リンクしたスキャナーは、ローカルで管 理 したり、スキャンの設 定 を行うときに選 択 したりできるようになります。

詳 細 については、次 を参 照 してください。

- Nessus スキャナーをリンクする
- Nessus スキャナーのリンクを解 除 する
- スキャナーを有 効 または無 効 にする
- スキャナーを削 除 する
- 管 理 対 象 スキャナーログをダウンロードする
- Tenable Nessus プラグインとソフト ウェアの更 新

Nessus スキャナーをリンクする

を使 用 する場 合 に必 要 な ユーザーロールTenable Nessus Manager: 管 理 者 またはシステム管 理 者

初 期 インストール時 に Tenable Nessus スキャナーをリンクするには、Nessus を設 定 するを参 照 してください。

初 期 インストール時 にスキャナーをリンクしない場 合 は、後 で Tenable Nessus スキャナーをリンクできます。Tenable Nessus スキャナーは、Tenable Nessus Manager や Tenable Vulnerability Management などのマネージャーにリンクできます。

注 意 : 初 期 インストール後 にユーザーインターフェースから Tenable Security Center にリンクすることはできません。スキャナーがすでに Tenable Security Center にリンクされている場 合 、リンクを解 除 し、そのスキャナーを Tenable Vulnerability Management または Tenable Nessus Manager にリンクできますが、インターフェースから Tenable Security Center に再 びリンクすることはできません。

Tenable Nessus スキャナーをマネージャーにリンクする方 法

1. リンクするマネージャーのユーザーインターフェースで、次のページにある **Linking Key** をコピーします。

   - Tenable Vulnerability Management: **[Settings]** (設定) > **[Sensors]** (センサー) > **[Linked Scanners]** (リンクされたスキャナー) > ⊕**[Add Nessus Scanner]** (Nessus スキャナーを追加する)
   - Tenable Nessus Manager: **[Sensors]** (センサー) > **[Linked Scanners]** (リンクされたスキャナー)

   > **注意:** `nessuscli` からスキャナーリンクキーを取得することもできます。詳細については、nessuscli Fix コマンドセクションの `nessuscli fix --secure --get scanner_linking_key` を参照してください。

2. リンクする Tenable Nessus スキャナーの上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

3. 左側のナビゲーションバーで **[Remote Link]** (リモートリンク) をクリックします。

   [Remote Link] (リモートリンク) ページが表示されます。

4. [Remote Link] (リモートリンク) の説明に従ってマネージャーのリンク設定を入力します。

5. **[Save]** (保存) をクリックします。

   Tenable Nessus がマネージャーにリンクされます。

Nessus スキャナーのリンクを解除する

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** 管理者またはシステム管理者

Tenable Nessus スキャナーのマネージャーへのリンクを解除し、別のマネージャーに再リンクできます。

> **注意：**初期インストール後にユーザーインターフェースから Tenable Security Center にリンクすることはできません。スキャナーがすでに Tenable Security Center にリンクされている場合、リンクを解除し、そのスキャナーを Tenable Vulnerability Management または Tenable Nessus Manager にリンクできますが、インターフェースから Tenable Security Center に再びリンクすることはできません。

Tenable Nessus スキャナーのマネージャーへのリンクを解除する方法

1. リンクを解除する Tenable Nessus スキャナーの上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Remote Link]** (リモートリンク) をクリックします。

   [Remote Link] (リモートリンク) ページが表示されます。

3. トグルを **[Off]** (オフ) に切り替えます。

4. **[Save]** (保存) をクリックします。

   Tenable Nessus でマネージャーへのリンクが解除されます。

次の手順

- Tenable Nessus と Tenable Security Center のリンクを解除した場合、Tenable Security Center からスキャナーを削除します。

スキャナーを有効または無効にする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

リンクされたスキャナーを有効にする方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Linked Scanners]** (リンクされたスキャナー) をクリックします。

3. スキャナーテーブルの、有効にするスキャナーの行で ボタンにカーソルを合わせると、 ボタンに変わります。

4. ボタンをクリックします。

   Tenable Nessus はスキャナーを有効にします。

リンクされたスキャナーを無効にする方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Linked Scanners]** (リンクされたスキャナー) をクリックします。

3. スキャナーテーブルの、無効にするスキャナーの行で ボタンにカーソルを合わせると、 ボタンに変わります。

4. ボタンをクリックします。

   Tenable Nessus はスキャナーを無効にします。

スキャナーを削除する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Linked Scanners]** (リンクされたスキャナー) をクリックします。

3. 次のいずれかを行います。

   - 1 つのスキャナーを削除する方法
     - スキャナーテーブルの、削除するスキャナーの行で、 ボタンをクリックします。

       確認ウィンドウが表示されます。

   - 複数のスキャナーを削除する方法

     a. スキャナーテーブルで、削除する各スキャナーの行にあるチェックボックスをクリックします。

     b. 右上の **[Remove]** (削除) ボタンをクリックします。

        確認ウィンドウが表示されます。

4. 確認ウィンドウで、**[Remove]** (削除) をクリックします。

   Tenable Nessus Managerにより、1 つまたは複数のスキャナーが削除されます。

管理対象スキャナーログをダウンロードする

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

Tenable Nessus Manager の管理者は、ログとシステム設定データを含むログファイルを管理対象スキャナーおよび Tenable Agents にリクエストして、ダウンロードできます。この情報は、システムの問題をトラブルシューティングするのに役立つとともに、Tenable サポート に提出するデータを簡単に収集する方法を提供します。

Tenable Nessus Manager の各管理対象スキャナーから最大で 5 つのログファイルを保存できます。上限に達したら、古いログファイルを削除して新しいログファイルをダウンロードする必要があります。

注意: ログのリクエストは、8.1 以降が動作している Nessus スキャナーに対してのみ行うことができます。

管理対象スキャナーからログをダウンロードする方法

1. 上部のナビゲーションバーで、**[Sensors]** (センサー) をクリックします。

   [Linked Agents] (リンクされたエージェント) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Linked Agents]** (リンクされたエージェント) が選択され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブな状態となっています。

2. 左側のナビゲーションバーで **[Linked Scanners]** (リンクされたスキャナー) をクリックします。

   [Scanners] (スキャナー) ページが表示され、リンクされたスキャナーテーブルが表示されます。

3. リンクされたスキャナーのテーブルで、ログをダウンロードするスキャナーをクリックします。

   そのスキャナーの詳細ページが表示されます。

4. **[Logs]** (ログ) タブをクリックします。

5. 右上にある **[Request Logs]** (ログのリクエスト) をクリックします。

   注意: 上限である 5 つのログファイルに達した場合は、**[リクエストログ]** ボタンは無効になります。新しいログをダウンロードする前に既存のログを削除してください。

Tenable Nessus Manager は、次回のチェックイン時に管理対象スキャナにログをリクエストします。これは数分かかる場合があります。ダウンロードが完了するまで、リクエストのステータスがユーザーインターフェースに表示されます。

6. ログファイルをダウンロードするには、ファイル名をクリックします。

   システムによってログファイルがダウンロードされます。

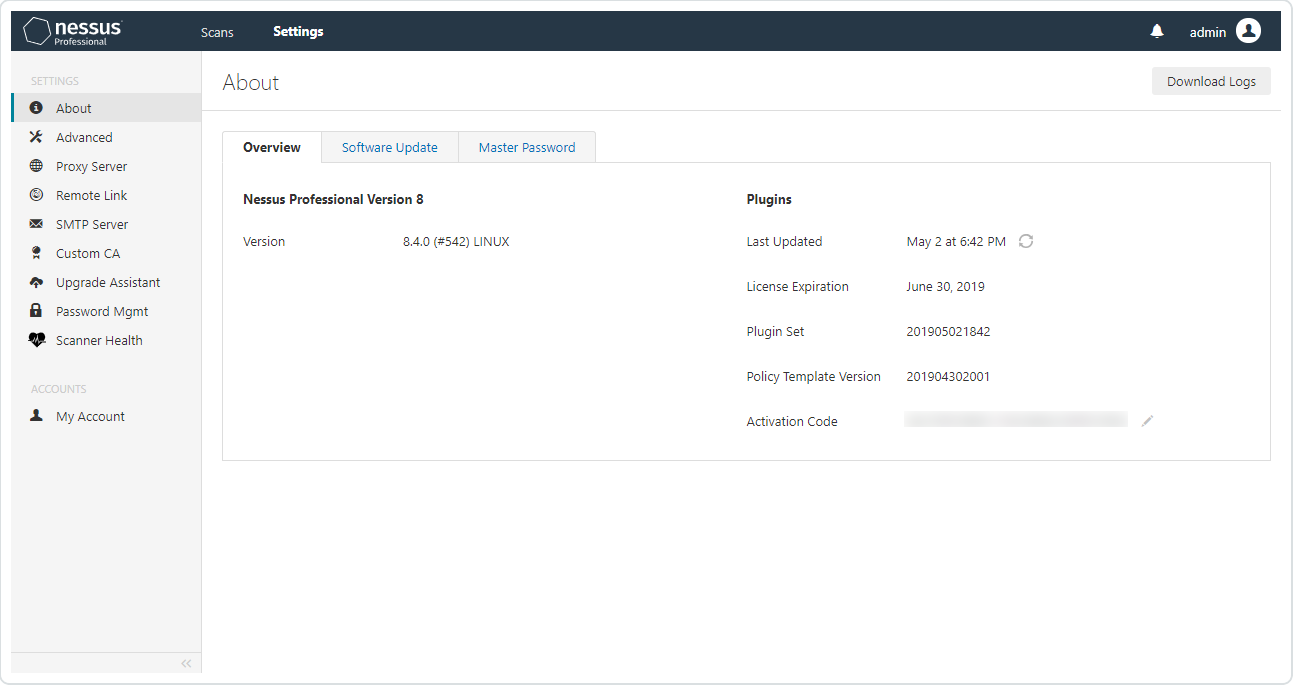
既存のログを削除する方法

- 削除するログの行で、🗑ボタンをクリックします。

保留中または失敗したログのダウンロードをキャンセルする方法

- キャンセルする保留中または失敗したログダウンロードの行で、⊘ ボタンをクリックします。

設定



[Settings] (設定) ページには次のセクションがあります。

- About
- Advanced
- プロキシサーバー
- リモートリンク
- SMTP サーバー
- カスタム CA
- マイアカウント
- ユーザー

バージョン情報

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

[About] (製品情報) ページには、Tenable Nessus のライセンスとプラグインの情報の概要が表示されます。製品設定にアクセスすると、この **[About]** (製品情報) ページが表示されます。デフォルトでは、Tenable Nessus は **[Overview]** (概要) タブを表示します。ここには、[Overview] (概要) 表に記載しているように、Tenable Nessus インスタンスに関する情報が含まれています。

[Software Update] (ソフトウェア更新) タブで、ソフトウェアの自動更新設定を設定したり、手動で Tenable Nessus ソフトウェアを更新したりすることができます。

[Encryption Password] (暗号化パスワード) タブでは、暗号化パスワードを設定することができます。

[Events] (イベント) タブでは、発生した Tenable Nessus システムイベントの履歴を表示できます。

Basic ユーザーは、**[Software Update]** (ソフトウェア更新) と **[Encryption Password]** (暗号化パスワード) タブを表示できません。Standard ユーザーは、製品バージョンと、現在のプラグインセットに関する基本的な情報のみ閲覧できます。

ログをダウンロードするには、ページの右上にある **[Download Logs]** (ログをダウンロードする) ボタンをクリックします。詳細は、ログをダウンロードするを参照してください。

概要

値	説明
Nessus Professional および Nessus Expert	
Version	Nessus インスタンスのバージョンです。
ライセンス済みのドメイン	(Tenable Nessus Expert のみ) 過去 90 日間にアタックサーフェス検出テンプレートでスキャンした一意のドメインの数。Tenable Nessus Expert では、ライセンス取得済みのドメインが 5 つまで許可されています。90 日間スキャンされていないドメインは、Tenable Nessus によって **ライセンス済みドメイン** カウントから削除されます。所属組織でさらにドメインを購入したい場合は、Tenable のCustomer Success Manager (CSM) にお問い合わせください。 詳細は、Bit Discovery でアタックサーフェス検出スキャンを作成するを参照してください。
Licensed URLs	(Tenable Nessus Expert のみ) 過去 90 日間に Tenable Nessus ウェブアプリケーションスキャンでスキャンした一意の URL の数。Tenable Nessus Expert では、最大 5 つのライセンス済み URL を許可します。90 日間 URL をスキャンしていない場合、Tenable Nessus は **ライセンス済みの URL** カウントからその URL を削除し

値	説明
	ます。追加の URL を購入したい場合は、Tenable のCustomer Success Manager (CSM) にお問い合わせください。 詳細は、Tenable Nessus Web Application Scanning Licensing を参照してください。
最終更新日	プラグインセットが最後に更新された日付です。この日付は、がその 自動プラグイン更新サイクル に基づいてプラグインを最後に更新した時、またはプラグインの更新ボタンが最後にクリックされた時を示す可能性があります Tenable Nessus 。
有効期限日	ライセンスが期限切れになる日付。 **注意:** ライセンスの期限が切れた後に、スキャンを実行したり、新しいプラグインをダウンロードしたりすることはできません。有効期限後 30 日間は、システムとスキャンレポートにアクセスできます。
Plugin Set	現在のプラグインセットの ID です。
Policy Template Version	現在設定されているポリシーテンプレートバージョンの ID です。
Activation Code	Nessus インスタンスのアクティベーションコードです。
Nessus Manager	
Version	Nessus インスタンスのバージョンです。
Licensed Hosts	ライセンス数に応じたスキャン可能ホストの数です。
Licensed Scanners	現在使用されているライセンス済みのスキャナーの数です。
Licensed Agents	現在使用されているライセンス済みのエージェントの数です。
Last Updated	プラグインセットが最後に更新された日付です。

値	説明
Expiration	ライセンスが期限切れになる日付。
Plugin Set	現在のプラグインセットの ID です。
Policy Template Version	現在設定されているポリシーテンプレートバージョンの ID です。
Activation Code	Nessus インスタンスのアクティベーションコードです。

ログをダウンロードする

を使用する場合に必要な [ユーザーロール](#)Tenable Nessus Manager: 管理者またはシステム管理者

管理者は、現在ログインしている Tenable Nessus インスタンスに関するローカルのログとシステム設定データが入ったログファイルをダウンロードできます。この情報は、システムの問題をトラブルシューティングするのに役立つとともに、Tenable サポートに提出するデータを簡単に収集する方法を提供します。

ダウンロード可能なログファイルには、**Basic (基本)** と **Extended (拡張)** の 2 種類があります。**Basic (基本)** オプションには、Tenable Nessus の最近のログデータとシステム情報 (オペレーティングシステムのバージョン、CPU 統計情報、使用可能なメモリおよびディスク容量、トラブルシューティングに役立つその他のデータ) が含まれます。**Extended (拡張)** オプションには、Tenable Nessus ウェブサーバーの最近のログレコード、システムログデータ、ネットワーク設定情報も含まれます。

個別の Tenable Nessus ログファイルの管理についての詳細は、[ログを管理する](#)を参照してください。

ログをダウンロードする方法

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 右上隅にある **[Download Logs]** (ログをダウンロードする) をクリックします。

   [Download Logs] (ログをダウンロードする) ウィンドウが表示されます。

3. 次のいずれかの **[Debug Log Type]** (デバッグログタイプ) を選択します。

- **Basic (基本)**: 標準の Tenable Nessus ログデータとシステム設定情報。
- **拡張**: **[Basic]** (基本) オプションのすべての情報、Tenable Nessus ウェブサーバーのログデータ、追加のシステムログ。

4. (オプション) ログの IPv4 アドレスの最初の 2 オクテットを非表示にするには、**[Sanitize IPs]** (IP をサニタイズする) を選択します。
5. **[Download]** (ダウンロード) をクリックします。

   ヒント: ダウンロードをキャンセルするには、**[Cancel]** (キャンセル) をクリックします。

   Tenable Nessus によって *nessus-bug-report-XXXXX.tar.gz* ファイルが生成されます。このファイルがダウンロードされ、ブラウザウィンドウに表示されます。

暗号化パスワードの設定

を使用する場合に必要な [ユーザーロール]Tenable Nessus Manager: System Administrator

暗号化パスワードを設定すると、Nessus はすべてのポリシー、スキャンの結果、スキャンの設定を暗号化します。Tenable Nessus の再起動時にパスワードを入力する必要があります。

警告: 暗号化パスワードを紛失した場合、管理者または Tenable サポート では暗号化パスワードを回復できません。

Tenable Nessus ユーザーインターフェースに暗号化パスワードを設定する方法

1. Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。
2. **[Encryption Password]** (暗号化パスワード) タブをクリックします。
3. **[New Password]** (新しいパスワード) ボックスに暗号化パスワードを入力します。
4. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus は暗号化パスワードを保存します。

コマンドラインインターフェースで暗号化パスワードを設定する方法

1. CLI から Tenable Nessus にアクセスします。
2. オペレーティングシステムに合わせて、以下のコマンドを入力します。

   - Linux

     ```
     /opt/nessus/sbin/nessusd --set-encryption-passwd
     ```

   - Windows

     ```
     C:\Program Files\Tenable\Nessus\nessusd --set-encryption-passwd
     ```

   - macOS

     ```
     /Library/Nessus/run/sbin/nessusd --set-encryption-passwd
     ```

3. プロンプトが表示されたら、新しいパスワードを入力します。

   注意: パスワードは入力中には表示されません。

   ```
   /opt/nessus/sbin/nessusd --set-encryption-passwd
   New password :
   Again :
   New password is set
   ```

   パスワードが有効であれば、成功メッセージが表示されます。

Tenable Nessus システムイベントの表示

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

ユーザーインターフェースの **[About]** (バージョン情報) > **[Events]** (イベント) タブから、Tenable Nessus で発生するバックエンドとシステムレベルのイベント履歴を表示できます。

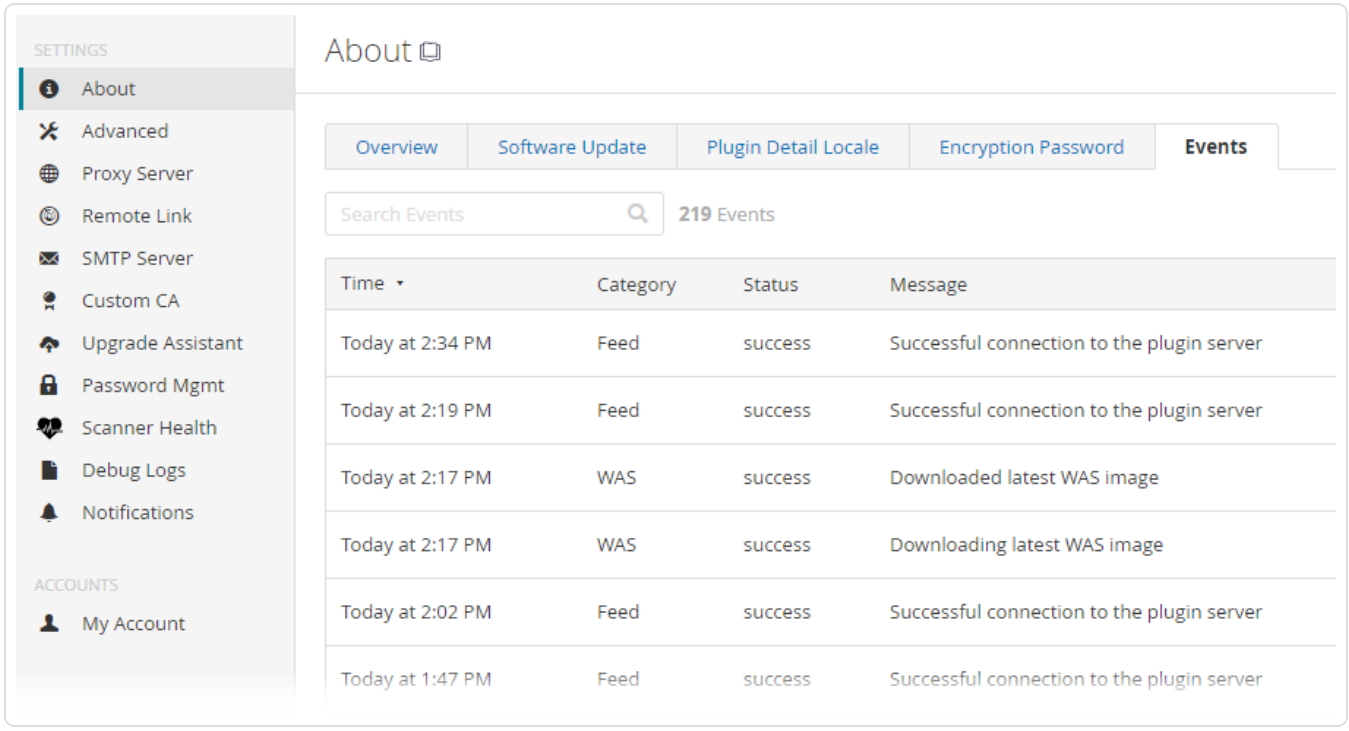
[Events] (イベント) タブを使用してフィードやウェブアプリスキャン (WAS) イベントを表示できます。これらのイベントは、Tenable Nessus がプラグインサーバーに正常に接続したとき、Tenable Nessus がプラグインのダウンロードを開始して終了したとき、Tenable Nessus が最新の WAS イメージをダウンロードしたときに発生します。

Tenable Nessus バックエンドイベントを表示する方法

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. **[Events]** (イベント) タブを選択します。



システムイベントの表が表示されます。表には、各イベントの発生日時、イベントカテゴリ、ステータス、説明メッセージが表示されます。列ヘッダーをクリックして、各列を昇順または降順でフィルタリングしたり、**[Search Events]** (イベント検索) 検索バーで特定のイベントを検索したりできます。

詳細設定

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** System Administrator

[Advanced Settings] (詳細設定) ページでは、Tenable Nessus の設定を手動で変更できます。Tenable Nessus のユーザーインターフェースか、コマンドラインインターフェースから詳細設定を変更できます。Tenable Nessus は、入力値を検証して、有効な設定だけが含まれるようにします。

Tenable Nessus は、詳細設定を次のカテゴリにグループ分けします。

- ユーザーインターフェース
- Scan (スキャン)

- ログ
- パフォーマンス
- セキュリティ
- エージェントとスキャナー
- クラスタ
- その他
- Custom (カスタム)

詳細

- 詳細設定は、お使いのすべての Tenable Nessus インスタンスでグローバルに適用されます。
- 詳細設定を編集するには、Tenable Nessus の管理ユーザーアカウントが必要です。
- Tenable Nessus は、すべての詳細設定を自動更新するわけではありません。
- 変更は反映されるまで数分かかる可能性もあります。
- Tenable Nessus により、変更を適用するために再起動が必要な設定には、ⓘ アイコンが表示されます。
- カスタムポリシー設定は、グローバル詳細設定よりも優先されます。

ユーザーインターフェース

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Allow Post-Scan Editing (allow_post_scan_editing) (スキャン完了後の編集を許可 (allow_	ユーザーにスキャン完了後のスキャン結果の編集を許可します。	○	yes または no	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
post_scan_editing))				
Disable API (disable_api) (API を無効にする (disable_api))	インバウンド HTTP 接続を含む、API を無効にします。ユーザーはユーザーインターフェースや API を介して Tenable Nessus にアクセスできません。	×	yes または no	○
Disable Frontend (disable_frontend) (フロントエンドを無効にする (disable_frontend))	Tenable Nessus のユーザーインターフェースを無効にします。ユーザーは引き続き API を使用できます。	×	yes または no	○
Login Banner (login_banner) (ログインバナー (login_banner))	Tenable Nessus へのログインを試みた後に表示されるテキストバナー。 **注意:** このバナーが表示されるのは、新しいブラウザまたはコンピューターから初めてログインするときのみです。	なし	文字列	×
Maximum Concurrent Web Users (global.max_web_users) (同時接続できる最大ウェブユーザー	同時接続できる最大ウェブユーザー数です。	1024	これは整数で表示されます。 0 に設定した場合、制限はありません。	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
数 (global.max_web_users))				
Nessus Web Server IP (listen_address) (Nessus ウェブサーバー IP (listen_address))	着信接続をリッスンする IPv4 アドレスです。127.0.0.1 に設定された場合、アクセスはローカル接続のみに制限されます。	0.0.0.0	IP アドレス形式の文字列	○
Nessus Web Server Port (xmlrpc_listen_port) (Nessus ウェブサーバーポート (xmlrpc_listen_port))	Tenable Nessus ウェブサーバーがリッスンするポートです。	8834	整数	○
UI Theme (ui_theme) (UI テーマ (ui_theme))	有効になると、ユーザーインターフェースのカラーテーマがダークモードに変更されます。 **注意:** SELinux を有効にしている場合、[UI Theme] (UI テーマ) 設定が適切に機能しない可能性があります。	`Track Os Setting`	`[Light]` (ライト)、`[Dark]` (ダーク)、または `[Track Os Setting]` (Os 設定を記録)	×
Use Mixed Vulnerability Groups (scan_vulnerability_groups_mixed) (混在する脆弱	有効にすると、Tenable Nessus は、グループ内のすべての脆弱性の深刻度が同じでない限り、脆弱性グループの深刻度レベルに **[Mixed]** (混在) と表示します。無効にすると、	○	`yes` または `no`	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
性グループを使用する (scan_vulnerability_groups_mixed))	Tenable Nessus は、グループ内で脆弱性が最も高い深刻度のインジケーターを表示します。			
Use Vulnerability Groups (scan_vulnerability_groups) (脆弱性グループを使用する (scan_vulnerability_groups))	この機能を有効にすると、Tenable Nessus でスキャン結果の脆弱性が共通の属性別にグループ化され、結果リストが短くなります。	○	yes または no	×

Scan (スキャン)

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Audit Trail Verbosity (audit_trail) (監査証跡の詳細度	プラグイン監査証跡の詳細度を制御します。完全な監査証跡には、Tenable Nessus が特定のプラグインをスキャンに含めなかった理由が含まれます。	`full`	`full`、`partial`、`none`	×

(audit_trail))				
Auto Enable Plugin Dependencies (auto_enable_dependencies) (プラグインの依存の自動有効化 (auto_enable_dependencies))	他のプラグインが依存しているプラグインを自動で有効にします。この設定では、スキャンテンプレート設定が依存しているプラグインは有効になりません。 この機能を無効にすると、スキャンポリシーで選択済みであるプラグインの一部が実行されないことがあります。	○	yes または no	×
CGI Paths for Web Scans (cgi_path) (ウェブスキャンの CGI パス (cgi_path))	ウェブサーバースキャンに使用する、コロンで区切られた CGI パスの一覧です。	/cgi-bin:/scripts	文字列	×
Engine Thread Idle Time (engine.idle_wait) (エンジンスレッドアイドル状態時間 (engine.idle_wait))	スキャンエンジンが停止するまでにアイドル状態になる秒数です。	60	0 から 600 までの整数	×
Max Plugin Output Size (plugin_	Tenable Nessus が .nessus 形式でエクスポートするスキャン結果に含めるプラグイン出力の最大サイズ (KB)。出力が最大サイズを超過する場合、Tenable Nessus はレポートの出力を切り捨	1000	これは整数で表示されま	×

output_max_size_kb) (プラグイン出力最大サイズ (plugin_output_max_size_kb))	てます。		す。 0 に設定した場合、制限はありません。	
Maximum Ports in Scan Reports (report.max_ports) (スキャンレポートの最大ポート数 (report.max_ports))	ポートの最大数です。スキャン結果にこの値より多くのポートが報告された場合、Tenable Nessus はポートのスキャン結果を破棄します。この制限は偽のターゲットのポートが大量に報告されるのを回避するためのものですが、スキャン結果データベースから有効な結果が削除されてしまう可能性もあります。このような問題が発生する場合は、デフォルト値を上げることをお勧めします。	1024	整数	×
Maximum Ports Reported by Portscanner Plugins (portscanner.max_ports) (ポートスキャナープラグインによってレポートされるポートの最大数 (portscanner.max_ports))	Tenable Nessus ポートスキャンプラグインがオープンとしてマークできるポートの最大数。これには、適切なポートスキャナーと、NASL 関数 `scanner_add_port()` を呼び出すプラグインが含まれます。	1024	0 から 65535 までの整数	×
Maximum Size for E-	レポートの添付ファイルの最大サイズ (MB) を指定します。レポートが最大サイズを超える場合、メールにレポートは添付されません。Tenable	25	0 から 50 までの整数	×

mailed Reports (attached_ report_ maximum_ size) (メールレポートの最大サイズ (attached_ report_ maximum_ size))	Nessus は、50 MB を超えるレポート添付ファイルをサポートしません。			

Nessus Rules File Location (rules) (Nessus ルールファイルの場所 (rules))	Tenable Nessus ルールファイル (`nessusd.rules`) の場所です。
	各オペレーティングシステムのデフォルトは次のとおりです。
	Linux
	`/opt/nessus/etc/nessus/nessusd.rules`
	macOS
	`/Library/Nessus/run/var/nessus/conf/nessusd.rules`
	Windows
	`C:\ProgramData\Tenable\Nessus\nessus\conf\nessusd.rules`
		お使いのオペレーティングシステムにおける Nessus の config ディレクトリ	文字列	×

Non-Simultaneous Ports (non_ simult_ports) (非同時ポート (non_	2 つのプラグインを同時に実行できないポートを指定します。	139, 445, 3389	文字列	×

simult_ports))				
Paused Scan Timeout (paused_scan_timeout) (スキャンの一時停止状態継続時間 (paused_scan_timeout))	スキャンが一時停止状態のままでいられる時間 (分) です。この時間を過ぎるとTenable Nessusがスキャンを終了させます。	0	0 から 10080 までの整数	×
PCAP Snapshot Length (pcap.snaplen) (PCAP スナップショットの長さ (pcap.snaplen))	パケットキャプチャに使用できるスナップショットの長さ、すなわちキャプチャされたネットワークパケットの最大サイズです。通常、Tenable Nessusは、この値をスキャナーのNICに応じて自動で設定します。しかし、ネットワーク設定によっては、Tenable Nessusがパッケージを切り捨て、スキャンレポートに「インターフェース *X* の現在のスナップショットの長さ *###* が小さすぎます。」というメッセージが表示される可能性があります。この長さを増やすことで、パケットの切り捨てを回避できます。	0	0 から 262144 までの整数	×
Port Range (port_range) (ポートの範囲 (port_range))	スキャナープラグインが検証を行うポートのデフォルトの範囲です。	`default`	`default`、`all`、ポート範囲、ポートおよびポート範囲のコンマ区切り	×

			リスト それぞれの範囲の前に T: または U: を付けて指定された UDP および TCP ポート	
Reverse DNS Lookups (reverse_lookup) (逆引き DNS ルックアップ (reverse_lookup))	これを有効にすると、Tenable Nessus のスキャンレポートには、ターゲットが完全修飾ドメイン名 (FQDN) で表されます。この機能を無効にすると、レポートのターゲットはホスト名または IP アドレスで表されます。	×	yes または no	×
Safe Checks (safe_checks) (安全チェック (safe_checks))	この機能を有効にすると、Tenable Nessus はアクティブな脆弱性テストではなくバナーグラビングを使った安全チェックを使用します。	○	yes または no	×
Silent Plugin Dependencies (silent_dependencie	これを有効にした場合、プラグインの依存関係とその結果のリストは Tenable Nessus のレポートに含められません。ポリシーの一部として、別のプラグインに依存しているプラグインを選択できます。	○	yes または no	×

s) (プラグインの依存関係をサイレントにする (silent_dependencies))	デフォルトでは、Tenable Nessus はこれらのプラグイン依存関係を実行しますが、レポートにはその結果を記載しません。無効にすると、Tenable Nessus は選択されたプラグインとすべてのプラグイン依存関係の両方をレポートに記載します。			
Slice Network Addresses (slice_network_addresses) (ネットワークアドレスを分割する (slice_network_addresses))	このオプションを設定すると、Tenable Nessus はネットワークを順に (10.0.0.1、10.0.0.2、10.0.0.3 など) スキャンせず、ネットワーク全体にワークロードを分割しようとします (たとえば、10.0.0.1、10.0.0.127、10.0.0.2、10.0.0.128 の順にスキャン)。	×	yes または no	×
System Default Severity Basis (severity_basis) (システムのデフォルト深刻度ベース (severity_basis))	Tenable Nessus スキャナーと Tenable Nessus Professional では、デフォルトの深刻度ベースを設定することにより、Tenable Nessus が CVSSv2 と CVSSv3 のどちらのスコア (利用可能な場合) を使って脆弱性の深刻度を計算するかを選ぶことができます。Tenable Nessus スキャナーと Tenable Nessus Professional では、デフォルトの深刻度ベースを設定することにより、Tenable Nessus が CVSSv2、CVSSv3、CVSSv4 のどのスコア (利用可能な場合) を使って脆弱性の深刻度を計算するかを選ぶことができます。 デフォルトの深刻度ベースを変更すると、その変更はデフォルトの深刻度ベースで設定されている既存のスキャンすべてに適用されます。今後のスキャンでも、デフォルトの深刻度ベースが使用されます。	Tenable Nessus の新規インストールの場合：cvss_v3 既存のアップグレードされたインスタンスの場合：cvss_v2	cvss_v2 または cvss_v3	×

	CVSS スコアと深刻度の範囲の詳細については、CVSS スコアとVPR を参照してください。 **注意:** この設定は Tenable Nessus Manager では利用できません。			

ログ

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Log Additional Scan Details (log_details) (追加のスキャンの詳細情報を記録する (log_details))	これを有効にすると、スキャンログには基本情報のほかに、ユーザー名、スキャン名、現在のプラグイン名が記録されます。これらの詳細を表示するには、`log_whole_attack` も有効にする必要があります。	×	yes または no	×
Log Verbose Scan Details (log_whole_attack) (Verbose スキャンの詳細情報を記録	スキャンの詳細情報を記録します。スキャンに関する問題のデバッグに役立ちますが、ディスクの負荷が高くなる可能性があります。詳細をさらに追加するには、`log_details` を有効にします。	×	yes または no	×

設定	説明	デフォルト	有効な値	再起動が必要ですか？
するScan Details (log_whole_attack))				

Nessus Dump File Location (dumpfile) (Nessus Dump ファイルの場所 (dumpfile))	デバッグ出力用ログファイル `nessusd.dump` が生成された場合に保存される場所です。
	
	各オペレーティングシステムのデフォルトは次のとおりです。
	
	Linux
	
	`/opt/nessus/var/nessus/logs/nessusd.dump`
	
	macOS
	
	`/Library/Nessus/run/var/nessus/logs/nessusd.dump`
	
	Windows
	
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump`
		お使いのオペレーティングシステムにおける Nessus のログディレクトリ	文字列	○

Nessus Dump File Log Level	`nessusd.dump` における NASL エンジン出力の種類です。	`normal`	選択肢は `normal`、`none`、	○

設定	説明	デフォルト	有効な値	再起動が必要ですか？
(nasl_log_type) (Nessus Dump ファイルのログのレベル (nasl_log_type))			trace、full です。	
Nessus Dump File Max Files (dumpfile_max_files) (Nessus Dump ファイルの最大数 (dumpfile_max_files))	ディスク上に残される nessusd.dump ファイルの最大数です。ファイル数が指定された値を超えると、Tenable Nessus は最も古いダンプファイルを削除します。	100	1 から 1000 までの整数	○
Nessus Dump File Max Size (dumpfile_max_size) (Nessus	nessusd.dump ファイルの最大サイズ (MB)。ファイルサイズが最大サイズを超えると、Tenable Nessus は新しいダンプファイルを作成します。	512	1 から 2048 までの整数	○

設定	説明	デフォルト	有効な値	再起動が必要ですか？
Dump ファイルの最大サイズ (dumpfile_max_size))				
Nessus Dump File Rotation Time (dumpfile_rotation_time) (Nessus Dump ファイルのローテーション時間 (dumpfile_rotation_time))	Tenable Nessus ダンプファイルのローテーションの頻度を日数で指定します。	1	1 から 365 までの整数	○
Nessus Dump File Rotation (dumpfile_	Tenable Nessus がダンプファイルをローテーションする基準が、サイズまたは時間のどちらの最大ローテーションであるかを決定します。	`size`	`size`: Tenable Nessus は `dumpfil`	○

設定	説明	デフォルト	有効な値	再起動が必要ですか？
rot) (Nessus Dump ファイルのローテーション (dumpfile_rot))			e_max_size で指定されたサイズに基づいてダンプファイルをローテーションします。 time: Tenable Nessus は dumpfile_rotation_time で指定されている時間に基づいてダンプファイルをローテーションします。	

設定	説明	デフォルト	有効な値	再起動が必要ですか？
Nessus Log Level (backend_log_level) (Nessus のログのレベル (backend_log_level))	backend.log ログファイルのログ記録レベルで、どの情報をログに含めるかを決定する、ログタグのセットで指定されます。 log.json を手動で編集して、ログタグのカスタムセットを backend.log 用に設定している場合、その内容はこの設定によって上書きされます。 詳細は、ログを管理するを参照してください。	normal	• normal - ログタグを log、info、warn、error、trace に設定します • debug - ログタグを	○

設定	説明	デフォルト	有効な値	再起動が必要ですか？
			log、info、warn、error、trace、debugに設定します • verbose - ログタグをlog、	

設定	説明	デフォルト	有効な値	再起動が必要ですか？
			`info`、`warn`、`error`、`trace`、`debug`、`verbose` に設定します	
Nessus Scanner Log Location (logfile) (Nessus スキャナーのログの場所 (logfile))	Tenable Nessus がスキャナーのログファイルを保存する場所。 各オペレーティングシステムのデフォルトは次のとおりです。 Linux `/opt/nessus/var/nessus/logs/nessusd.me`	*お使いのオペレーティングシステムにおける*	文字列	○

設定	説明	デフォルト	有効な値	再起動が必要ですか？

	`ssages`
	macOS
	`/Library/Nessus/run/var/nessus/logs/nessusd.messages`
	Windows
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages`
		Nessus のログディレクトリ		

Log File Maximum Files (logfile_max_files) (ログファイルの最大ファイル数 (logfile_max_files))	Tenable Nessus がディスク上に保持する `nessusd.messages` ファイルの最大数を決定します。`nessusd.messages` ログファイル数が指定された値を超えると、Tenable Nessus は最も古いログファイルを削除します。	Tenable Nessus – 100 Tenable Agent – 2	1 から 1000 までの整数	○
Log File Maximum Size (logfile_	`nessusd.messages` ファイルの最大サイズ (MB) を決定します。ファイルサイズが最大サイズを超えると、Tenable Nessus は新しいメッセージログファイルを作成します。	Tenable Nessus –	1 から 2048 までの整数	○

設定	説明	デフォルト	有効な値	再起動が必要ですか？
max_size) (ログファイル最大サイズ (logfile_max_size))		512 Tenable Agent – 10		
Log File Rotation Time (logfile_rotation_time) (ログファイルのローテーション時間 (logfile_rotation_time))	Tenable Nessus メッセージログファイルのローテーションの頻度を日数で指定します。	1	1 から 365 までの整数	○
Log File Rotation (logfile_rot) (ログファイルのローテーション	Tenable Nessus がメッセージログファイルをローテーションする基準が、ローテーションの最大サイズと時間のどちらであるかを決定します。	サイズ	`size` – Tenable Nessus は、`logfile_`	○

設定	説明	デフォルト	有効な値	再起動が必要ですか？
(logfile_rot))			`max_size` で指定されたサイズに基づいてログファイルをローテーションします。 `time` – Tenable Nessus は、`logfile_rotation_time` で指定された時間に基づいてログファイルをローテーションします。	
Scanner	スキャナーパフォーマンスのメトリックデータ収集を	0	0 (オフ)、	×

設定	説明	デフォルト	有効な値	再起動が必要ですか？
Metric Logging (scanner.metrics) (スキャナーメトリックログ (scanner.metrics))	有効にします。		0x3f (プラグインメトリクスを除く全データ)、0x7f (プラグインメトリクスを含む全データ) **注意：** プラグインメトリクスを含めることで、ログファイルのサイズは大幅に増加します。Tenable Nessus では、ログファ	

設定	説明	デフォルト	有効な値	再起動が必要ですか？
			イルが自動的にクリーンアップされません。	
Use Milliseconds in Logs (logfile_msec) (ログでミリ秒を使用する (logfile_msec))	この機能を有効にすると、nessusd.messages および nessusd.dump ログのタイムスタンプがミリ秒単位になります。この機能を無効にすると、ログのタイムスタンプは秒単位になります。	×	yes または no	○

パフォーマンス

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Database Synchronous	データベースの更新が	NORMAL	NORMAL または	○

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Setting (db_synchronous_setting) (データベース同期設定 (db_synchronous_setting))	どのようにディスクに同期されるかを制御します。 NORMAL は高速ですが、予期しないシステムシャットダウン (たとえば停電またはクラッシュ) の時にデータ喪失のリスクがあります。 FULL はより安全ですが、いくらかのパフォーマンスコストを伴います。		FULL	
Engine Logging (global.log.engine_details) (エンジンログ (global.log.engine_details))	これを有効にすると、各ターゲットがスキャン時に割り当てられたスキャンエンジンに関する追加情報が記録されます。	×	yes または no	×
Global Max Hosts Concurrently Scanned (global.max_hosts) (グローバルに同時にスキャンされる最大ホスト数 (global.max_hosts))	Tenable Nessus がすべてのスキャンで同時にスキャンできる最大ホスト数。	ハードウェアにより変わる	整数	×
Global Max Port Scanners (global.max_	ポートスキャナーの最大数。	100	0 から 1024 までの整数	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
portscanners) (グローバルのポートスキャナーの最大数 (global.max_portscanners))				
Global Max TCP Sessions (global.max_simult_tcp_sessions) (グローバルの最大 TCP セッション数 (global.max_simult_tcp_sessions))	すべてのスキャンで同時に実行できる最大 TCP セッション数です。	デスクトップオペレーティングシステム (例: Windows 10) の場合は 50。 その他のオペレーティングシステム (例: Windows Server 2016) の場合は 50000。	整数	×
Max Concurrent Checks Per Host (max_checks) (ホストごとの最大同時実行プラグイン数 (max_checks))	ホストごとに同時に実行できるプラグインの最大数です。	5	整数	×
Max Concurrent Hosts Per Scan (max_hosts) (スキャ	スキャン中に一度にチェックされるホストの	変動あり、最大 100	整数 ゼロに設定さ	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
ンごとの最大同時ホスト数 Max Concurrent Hosts Per Scan (max_hosts))	最大数です。		れた場合、デフォルト値の 100 になります。	
Max Concurrent Scans (global.max_scans) (最大同時スキャン数 (global.max_scans))	スキャナーが同時に実行できるスキャンの最大件数。	0	0 から 1000 までの整数 0 に設定した場合、制限はありません。	×
Max Engine Checks (engine.max_checks) (最大エンジンチェック数 (engine.max_checks))	1 つのスキャンエンジンで同時に実行されるプラグインの最大数です。	64	整数	×
Max Engine Threads (engine.max) (最大エンジンスレッド数 (engine.max))	並行して実行できるスキャンエンジンの最大数です。スキャンエンジンは、1 つ以上のスキャンを同時に実行して複数のターゲットのスキャンを行います (`engine.max_hosts` を参照)。	マシンの CPU コア数の 8 倍	整数	×
Max Hosts Per Engine Thread (engine.max_hosts) (エンジンスレッドごとの最大ホスト数 (engine.max_hosts))	1 つのスキャンエンジンで同時に実行されるターゲットの最大数です。	16	整数	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Max HTTP Connections (max_http_connections) (最大 HTTP 接続数 (max_http_connections))	ウェブサーバーが HTTP コード 503 (サービス利用不可、接続が多すぎます) で応答するまでの同時接続の最大試行回数です。	600	整数	○
Max HTTP Connections Hard (max_http_connections_hard) (厳格な最大 HTTP 接続数 (max_http_connections_hard))	ウェブサーバーが許可する同時接続試行の最大回数です。	3000	整数	○
Max TCP Sessions Per Host (host.max_simult_tcp_sessions) (ホストごとの最大 TCP 接続数 (host.max_simult_tcp_sessions))	ホストごとに同時に実行できる最大 TCP セッション数です。 この TCP スロットリングオプションは、SYN スキャナーが送信する 1 秒あたりのパケット数も制御し、その数は TCP セッションの 10 倍になります。たとえば、このオプションを 15 に設定した場合、SYN スキャナーは最大で毎秒 150 パケットを送信します。	0	これは整数で表示されます。 0 に設定した場合、制限はありません。	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Max TCP Sessions Per Scan (max_simult_tcp_sessions) (スキャンごとの最大 TCP 接続数 (max_simult_tcp_sessions))	スキャンするホストの数に関係なく、スキャン全体で確立される TCP セッションの最大数。	0	0 から 2000 までの整数です。 0 に設定した場合、制限はありません。	×
Minimum Engine Threads (engine.min) (最小エンジンスレッド数 (engine.min))	Tenable Nessus がターゲットをスキャンするときに最初に開始するスキャンエンジン数。エンジンが `engine.optimal_hosts` のターゲット数に達すると、Tenable Nessus はスキャンエンジンを `engine.max` に達するまで追加していきます。	マシンの CPU コア数の 2 倍	整数	×
Optional Hosts Per Engine Thread (engine.optimal_hosts) (エンジンスレッドごとの任意のホスト数 (engine.optimal_hosts))	Tenable Nessus によってエンジンの追加が (最大で `engine.max` まで) 行われる前に、各スキャンエンジンで実行するターゲットの最小数です。	2	整数	×
Optimize Tests (optimize_	テストの手順を最適	○	yes または no	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
test) (テストを最適化する (optimize_test))	化します。この設定を無効にすると、スキャンに通常よりも時間がかかり、誤検出が増える可能性があります。			
Plugin Check Optimization Level (optimization_level) (プラグインチェック最適化レベル (optimization_level))	Tenable Nessus がプラグイン実行前に行うチェックの種類を指定します。 この設定を open_ports に設定した場合、Tenable Nessus は必要なポートが空いているかどうかをチェックします。空いていない場合、プラグインは実行されません。 この設定を required_keys に設定した場合、Tenable Nessus は空いているポートをチェックし、必要なキー (KB エントリ) があるかどうかもチェックします。除外されたキーのチェックは無視	なし	open_ports または required_keys	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
	されます。			
Plugin Timeout (plugins_timeout) (プラグイン タイムアウト (plugins_timeout))	プラグインアクティビティの最長有効期間 (秒) です。	320	0 から 1000 までの整数	×
QDB Memory Usage (qdb_mem_usage) (QDB メモリ使用量 (qdb_mem_usage))	アイドル時に Tenable Nessus のメモリ使用量を調整します。Tenable Nessus が専用サーバーで実行されている場合、この項目を high に設定すると、使用するメモリが増えてパフォーマンスが向上します。Tenable Nessus を共有マシンで実行している場合、これを low に設定すると、使用するメモリは減りますが、パフォーマンスへの影響は中程度になります。	`low`	`low` または `high`	×
Reduce TCP Sessions on Network Congestion (reduce_connections_on_congestion) (ネットワーク混雑時の TCP セッション数を減らす (reduce_	ネットワークが混雑しているときに、並行する TCP セッションの数を減らします。	×	`yes` または `no`	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
connections_on_congestion))				
Remediations Limit (remediations_limit) (修正数の上限 (remediations_limit))	Tenable Nessus が生成し、スキャン結果に表示する修正の数を制限します。	500	ゼロより大きい整数	×
Scan Check Read Timeout (checks_read_timeout) (スキャンチェック読み取りタイムアウト (checks_read_timeout))	テストのソケットの読み取りタイムアウトです。	5	0 から 1000 までの整数	×
Stop Scan on Host Disconnect (stop_scan_on_disconnect) (ホスト接続切断時のスキャン停止 (stop_scan_on_disconnect))	これを有効にすると、Tenable Nessus はスキャン中に切断したホストのスキャンを停止します。	×	yes または no	×
XML Enable Plugin Attributes (xml_enable_plugin_attributes) (XML 有効プラグイン属性 (xml_enable_plugin_attributes))	これを有効にすると、Tenable Nessus は Tenable Security Center にエクスポートされるスキャンにプラグイン属性を含めます。	×	yes または no	×
Webserver Thread Pool Minimum Size (www.thread_pool.min) (ウェブサーバースレッドプー	ウェブサーバーおよびバックエンドのスレッドプールの最小サイズです。	2	0 から 100 までの整数	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
ル最小サイズ (www.thread_pool.min))				
Webserver Thread Pool Maximum Size (www.thread_pool.max) (ウェブサーバースレッドプール最大サイズ (www.thread_pool.max))	ウェブサーバーおよびバックエンドのスレッドプールの最大サイズです。	200	0 から 500 までの整数	×

セキュリティ

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Always Validate SSL Server Certificates (strict_certificate_validation) (常に SSL サーバー証明書を検証する (strict_certificate_validation))	初期リモートリンク中であっても、SSL サーバー証明書を常に検証します (マネージャーが信頼できるルート CA を使用する必要があります)。	×	yes または no	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Cipher Files on Disk (cipher_files_on_disk) (ディスクの暗号ファイル (cipher_files_on_disk))	Tenable Nessus が書き出す暗号ファイルです。	○	yes または no	○
Force Public Key Authentication (force_pubkey_auth) (公開鍵認証を強制する (force_pubkey_auth))	Tenable Nessus のログインで公開鍵認証を使用するように強制します。	×	yes または no	○
Max Concurrent Sessions Per User (max_sessions_per_user) (ユーザーあたりの最大同時セッション数 (max_sessions_per_user))	ユーザーあたりの最大同時セッションです。	0	0 から 2000 までの整数です。 0 に設定した場合、制限はありません。	×
SSL Cipher List (ssl_cipher_list) (SSL 暗号リスト (ssl_cipher_list))	Tenable Nessus のバックエンド接続に使用する暗号リストです。	`compatible`	• `legacy` - 旧式の安全でないブラウザおよび API と統合できる暗号のリスト。 • `compatible` - Internet Explorer 11	○

設定	説明	デフォルト	有効な値	再起動が必要ですか?
	事前設定済みの暗号文字列のリストを使用するか、カスタム暗号リストまたは暗号文字列を入力します。 **注意:** この設定では、TLS 1.2 の暗号のみを設定します。		を含むすべてのブラウザと互換性がある安全な暗号のリスト。最新のすべての暗号が含まれていない場合があります。 • `modern` - 最新の最も安全な暗号のリスト。Internet Explorer 11 などの旧式のブラウザとは互換性がない場合があります。 • `custom` - カスタム OpenSSL 暗号リスト。有効な暗号リストの形式については、OpenSSL のドキュメントを参照してください。 • `niap` - NIAP 基準に準拠する暗号のリスト。 `ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-`	

設定	説明	デフォルト	有効な値	再起動が必要ですか?
			`SHA384:ECDHE-RSA-AES256-GCM-SHA384` **ヒント**: Tenable でサポートされている暗号のリストについては、*Tenable Vulnerability Management ユーザーガイド*のシステム要件を参照してください。	
SSL Mode (ssl_mode) (SSL モード (ssl_mode))	サポートされる TLS の最小バージョンです。	`tls_1_2`	• `compat` - TLS v1.0 以上 • `ssl_3_0` - SSL v3 以上 • `tls_1_1` - TLS v1.1 以上 • `tls_1_2` - TLS v1.2 以上 • `niap` - TLS v1.2	○

エージェントとスキャナー

注意：次の設定項目は、Tenable Nessus Manager でのみ利用可能です。

設定	説明	デフォルト	有効な値	再起動が必要
agent_auto_delete	エージェントが非アクティブになってから agent_auto_delete_threshold で設定されている期間が経過した後、エージェントが自動的に削除されるかどうかを制御します。	×	yes または no	×
agent_auto_delete_threshold	agent_auto_delete が yes に設定されている場合に、非アクティブなエージェントが自動的に削除されるまでの日数です。	60	1 から 365 までの整数	×
agent_auto_unlink	エージェントが非アクティブになってから agent_auto_unlink_threshold で設定されている期間が経過した後、エージェントが自動的にリンク解除されるかどうかを制御します。	×	yes または no	×
agent_auto_unlink_threshold	agent_auto_unlink が yes に設	30	30 から 90 までの整数	×

設定	説明	デフォルト	有効な値	再起動が必要
	定されている場合に、非アクティブなエージェントが自動的にリンク解除されるまでの日数です。 **注意:** この値は、`agent_auto_delete_threshold` の値より少なくする必要があります。			
agents_progress_viewable	エージェント数がこの設定値を超えると、スキャンでエージェントから情報が収集されても、Tenable Nessus Manager はエージェントの詳細情報を表示しません。その代わりに、スキャンが完了したときに、スキャン結果が収集されて閲覧できることを示すメッセージが表示されます。	100	これは整数で表示されます。 ゼロに設定された場合、デフォルト値の 100 に戻ります。	×
agent_updates_from_feed	この機能を有効にすると、Tenable Agent ソフトウェアの新しい更新プログラ	○	yes または no	○

設定	説明	デフォルト	有効な値	再起動が必要
	ムが自動でダウンロードされます。			
cloud.manage.download_max	エージェントの更新プログラムを同時にダウンロードできる最大数です。	10	整数	×
agent_merge_audit_trail	エージェントスキャン結果の監査証跡データをメインのエージェントデータベースに含めるかどうかを決めます。監査証跡データを除外すると、エージェントスキャン結果の処理パフォーマンスが大幅に向上します。 この設定が [false] に設定されていると、個別のスキャンやポリシーの **[Audit Trail Verbosity]** (監査証跡の詳細) 設定がデフォルトで `[No audit trail]` (監査証跡なし) に設定されます。	`false`	`true` または `false`	×
agent_merge_kb	メインのエージェント	`false`	`true` または	×

設定	説明	デフォルト	有効な値	再起動が必要
	データベースにエージェントのスキャン結果のKBデータを含めます。KBデータを除外すると、エージェントスキャン結果の処理パフォーマンスが大幅に向上します。 この設定が[false]に設定されていると、個別のスキャンやポリシーの**[Include the KB]**(KBを含む)設定がデフォルトで`[Exclude KB]`(KBを含まない)に設定されます。		`false`	

agent_merge_journal_mode	エージェントの結果を処理するときに使用するジャーナルモードを設定します。環境によっては、これによって処理パフォーマンスが向上する場合がありますが、クラッシュが発生した場合にスキャン結果が破	`DELETE`	`MEMORY`
			
			`TRUNCATE`
			
			`DELETE`
				×

設定	説明	デフォルト	有効な値	再起動が必要
	損するリスクもあります。詳細は、sqlite3 のドキュメントを参照してください。			
agent_merge_synchronous_setting	エージェントの結果を処理するときに使用するファイルシステムの同期モードを設定します。この設定をオフにすると処理パフォーマンスは大きく向上しますが、クラッシュが発生した場合にスキャン結果が破損するリスクもあります。詳細は、sqlite3 のドキュメントを参照してください。	FULL	OFF NORMAL FULL	×
track_unique_agents	この機能を有効にすると、Tenable Nessus Manager はリンクしようとしているエージェントの MAC アドレスが、同じホスト名、プラットフォーム、ディストリビューションを持つ、リンク済みエージェントの MAC アドレスと	×	yes または no	×

設定	説明	デフォルト	有効な値	再起動が必要
	一致するかどうかをチェックします。Tenable Nessus Manager はエージェントの重複があればそれを削除します。			

クラスタ

注意：次の設定項目は、クラスタリングが有効になっている Tenable Nessus Manager でのみ利用できます。

設定	説明	デフォルト	有効な値
Agent Blacklist Duration Days (agent_blacklist_duration_days) (エージェントブラックリスト日数 (agent_blacklist_duration_days))	エージェントがクラスタノードへの再リンクからブロックされたままとなっている日数です。 たとえば、クラスタ内の既存エージェントに一致する UUID にリンクしようとした場合、Tenable Nessus はエージェントをブロックします。 **注意:** Tenable Nessus 操作がないと、Tenable Nessus がエージェントを完全に削除または削除した後に、エージェントがブロックされます。ただし、管理者が手動でエージェントのリンクを解除して再リンクした場合、Tenable Nessusはそのエージェントを正常な状態に戻します。	7	ゼロより大きい整数
Agent Clustering Scan Cutoff (agent_cluster_scan_cutoff) (エージェントクラスタスキャン中止	子ノードを更新することなくこの設定時間が経過すると、Tenable Nessus はスキャンを中止します。	3600	299 より大きい整数

設定	説明	デフォルト	有効な値
(agent_cluster_scan_cutoff))			
Agent Node Global Maximum Default (agent_node_global_max_default) (最大のデフォルトエージェントノードグローバル (agent_node_global_max_default))	グローバルのクラスタノードあたり最大デフォルトエージェント数です。 子ノードに個別の最大値を設定している場合、そちらの設定値の方がこの設定より優先されます。	10000	0 から 20000 までの整数

その他

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Allow Special Characters in User Names (allow_special_chars_in_username) (ユーザー名の特殊文字を許可する (allow_	Tenable Nessus のユーザー名に括弧 ((および)) を使用できるかどうかを指定します。	`true`	`true` または `false`	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
special_chars_in_username))				
Automatic Update Delay (auto_update_delay) (自動アップデート遅延 (auto_update_delay))	Tenable Nessus が次回自動アップデートまで待機する時間です。	24	ゼロより大きい整数	×
Automatic Updates (auto_update) (自動アップデート (auto_update))	プラグインを自動でアップデートします。この機能を有効にして Tenable Nessus を登録すると、Tenable Nessus は利用可能になった最新プラグインを Tenable から自動的に入手します。スキャナーがインターネットに接続できない独立したネットワーク上にある場合は、この設定を無効にします。 **注意:** この設定は、Tenable Vulnerability Management に接続された Tenable Nessus スキャナーでは機能しません。Tenable Vulnerability Management にリンクされたスキャナーは、cloud.tenable.com から更新を自動的に	○	yes または no	○

設定	説明	デフォルト	有効な値	再起動が必要ですか?
	受信します。詳細は、ナレッジベースの記事を参照してください。			
Automatically Update Nessus (auto_update_ui) (Nessus の自動アップデート (auto_update_ui))	Tenable Nessus の更新プログラムを自動ダウンロードして適用します。 **注意:** この設定は、Tenable Vulnerability Management に接続された Tenable Nessus スキャナーでは機能しません。Tenable Vulnerability Management にリンクされたスキャナーは、cloud.tenable.com から更新を自動的に受信します。詳細は、ナレッジベースの記事を参照してください。	○	yes または no	×
Backups to keep (backup_days_to_keep) (バックアップして保持 (backup_days_to_keep))	Tenable Nessus は、24 時間ごとにバックアップファイルを自動的に作成します。この設定を使用して、Tenable Nessus がバックアップファイルを破棄するまでの日数を指定します。たとえば、この設定をデフォルトの 30 日のままにした場合、Tenable Nessus は過去 30 日間の日次バックアップファイルを保持します。 Tenable Nessus バックアップファイルの詳細については、Tenable Nessus のバックアップを参照してください。	30	ゼロより大きい整数	×
Child Node Port (child_node_	Tenable Nessus 子ノードが別のポートで親ノードと通信できるようにします。	なし	任意の有効なポート値	○

設定	説明	デフォルト	有効な値	再起動が必要ですか?
listen_port) (子ノードポート (child_node_listen_port))				
Initial Sleep Time (ms_agent_sleep) (初期スリープ時間 (ms_agent_sleep))	(Tenable Nessus Manager のみ) 管理スキャナーとエージェントリクエストの間のスリープ時間です。この設定は Tenable Nessus Manager または Tenable Vulnerability Managementでオーバーライドできます。	30	5 から 3300 までの整数	×
Java Heap Size (java_heap_size) (Java ヒープサイズ (java_heap_size))	PDF レポートをエクスポートするときに Tenable Nessus が使用する Java ヒープサイズ (Java 仮想マシンで実行されているアプリケーションによってインスタンス化されたオブジェクトを保存するために使用されるシステムメモリ) を指定します。	auto	auto または 0 より大きい整数	○
Max HTTP Client Requests (max_http_	管理スキャナーおよびエージェントで同時に確立できる HTTP アウトバウンド接続の最大数を指定します。	4	ゼロより大きい整数	○

設定	説明	デフォルト	有効な値	再起動が必要ですか?
client_ requests) (最大 HTTP クライアントリクエスト数 (max_http_ client_ requests))				
Nessus Debug Port (dbg_port) (Nessus デバッグポート (dbg_port))	nessusd が ndbg クライアント接続をリッスンするポートです。空白にすると、Tenable Nessus はデバッグポートを確立しません。	なし	*port*、*localhost:port*、*ip:port*のいずれかの形式の文字列	×

Nessus Preferences Database (config_file) (Nessus 設定データベース (config_ file))	エンジンの環境設定項目を含む設定ファイルの場所です。
	各オペレーティングシステムのデフォルトは次のとおりです。
	Linux
	`/opt/nessus/etc/nessus/nessusd.db`
	macOS
	`/Library/Nessus/run/etc/nessus/conf/`
		お使いのオペレーティングシステムにおける Tenable Nessus のデータベース	文字列	○

設定	説明	デフォルト	有効な値	再起動が必要ですか?

	`nessusd.db`
	Windows
	`C:\ProgramData\Tenable\Nessus\conf\nessusd.db`
		ディレクトリ		

Non-User Scan Result Cleanup Threshold (report_cleanup_threshold_days) (非ユーザースキャン結果クリーンアップしきい値 (report_cleanup_threshold_days))	古いシステムユーザーのスキャンレポートを削除するまでの経過時間のしきい値 (日数) です。	30	ゼロより大きい整数	×
Old User Files Cleanup (old_user_files_	Tenable Nessus が古いユーザーファイルをファイルシステムから削除するまでの経過時間。0 に設定すると、Tenable Nessus はクリーンアップを実行しません。	0	ゼロより大きい整数	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
cleanup_hours) (古いユーザーファイルのクリーンアップ (old_user_files_cleanup_hours))				
Orphaned Scan History Cleanup (orphaned_scan_cleanup_days) (取り残されたスキャンの履歴のクリーンアップ (orphaned_scan_cleanup_days))	Tenable Nessus が取り残された Tenable Security Center のスキャンを削除するまでの経過日数。たとえば、Tenable Security Center 経由で実行されて適切に削除されなかった結果、スキャンが取り残されてしまうことがあります。 0 に設定すると、Tenable Nessus はクリーンアップを実行しません。 **注意:** この設定は、Tenable Security Center から起動されたネットワークスキャンにのみ適用されます。エージェントスキャンまたはウェブアプリケーションスキャンには適用されません。	30	ゼロより大きい整数	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Packet Capture Archive Cleanup (packet_capture_archive_cleanup_days) (パケットキャプチャアーカイブクリーンアップ (packet_capture_archive_cleanup_days))	Tenable Nessus がパケットキャプチャアーカイブをファイルシステムから削除するまでの日数。0 に設定すると、Tenable Nessus はクリーンアップを実行しません。	30	ゼロより大きい整数	×
Plugin Integrity Check Frequency (Minutes) (plugin_healthcheck_frequency)	Tenable Nessus がプラグインの整合性チェックをフルで実行する頻度を分単位で決定します。	10080	1440 から 10080 までの整数	○

設定	説明	デフォルト	有効な値	再起動が必要ですか?
(プラグイン整合性チェック頻度 (分)) (plugin_healthcheck_frequency))				
Remote Scanner Port (remote_listen_port) (リモートスキャナーポート (remote_listen_port))	この設定により、Tenable Nessus は、リモートエージェントおよびスキャナーとの通信専用ポート (通信ポート) と、ユーザーログイン専用のポート (管理ポート) で動作可能になります。この設定を追加することで、`xmlrpc_listen_port` (デフォルトは 8834) で定義されたポートではなく、別のポート (例: 9000) を管理スキャナーとエージェントにリンクできます。	なし	整数	○
Report Crashes to Tenable (report_crashes) (クラッシュを Tenable に報告する (report_crashes))	これを有効にすると、問題を特定するために、Tenable Nessus は Tenable, Inc. にクラッシュ情報を自動送信します。個人情報やシステム識別情報を Tenable Nessus が Tenable, Inc. に送信することはありません。	○	yes または no	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
Scan Source IP (s) (source_ip) (ソース IP をスキャン (source_ip))	マルチホームホストのスキャン実行時に使用するソース IP です。複数の IP がある場合、Tenable Nessus は新しい接続を実行するたびにそれらの IP を繰り返して使用します。	なし	1 つの IP アドレス、またはコンマ区切りの複数の IP アドレスリスト	○
Send Telemetry (send_telemetry) (テレメトリを送信 (send_telemetry))	有効にすると、Tenable Nessus は機密情報ではない製品の使用状況データを、安全な方法で定期的に Tenable に送信します。 使用状況統計データとは、Tenable Nessus インターフェース内でアクセスしたページ、使用したレポートとダッシュボード、Tenable Nessus ライセンス、設定済み機能に関するデータなどを指します。Tenable はこのデータを将来の Tenable Nessus リリースのユーザーエクスペリエンスの改善に活用します。この機能はいつでも無効にすることが可能で、無効にすると使用状況統計データを Tenable と共有することはなくなります。	○	yes または no	○
User Scan Result Deletion Threshold (scan_	Tenable Nessus が完了したスキャンの履歴とデータを完全に削除するまでの日数。 **注意:** この設定は、Tenable Security Center から起動されたすべてのスキャナー、エージェント、ウェブアプリケーションスキャンに影響を与えます。	0	0 または 3 以上の整数です。 0 に設定	×

設定	説明	デフォルト	有効な値	再起動が必要ですか?
history_expiration_days) (ユーザースキャン結果削除しきい値 (scan_history_expiration_days))			すると、Tenable Nessus は履歴を保持します。	
Windows Minidump (windows_minidump) (Windows ミニダンプ (windows_minidump))	Windows 用 Tenable Nessus がクラッシュした場合、Tenable Nessus が Windows ミニダンプファイルをログフォルダーに生成するかどうかを決定します。	×	yes または no	×

Custom (カスタム)

すべての詳細設定が Tenable Nessus ユーザーインターフェースに取り込まれるわけではありませんが、一部の設定はコマンドラインインターフェースで設定できます。作成したカスタム設定項目は、**[Custom]** (カスタム) タブに表示されます。

カスタムの詳細設定を管理するには、次の手順に従います。

新しい設定を作成する

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで、**[Advanced]** (アドバンス) をクリックします。

   [Advanced Settings] (詳細設定) ページが表示されます。

3. 右上の**[New Setting]** (新規設定) ボタンをクリックします。

   [Add Setting] (設定の追加) ウィンドウが表示されます。

4. **[Name]** (名前) ボックスに、新規設定のキーを入力します。

5. **[Value]** (値) ボックスに、対応する値を入力します。

6. **[Add]** (追加) ボタンをクリックします。

   リストに新規設定が表示されます。

設定を変更する

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで、**[Advanced]** (アドバンス) をクリックします。

   [Advanced Settings] (詳細設定) ページが表示されます。

3. 設定テーブルで変更する設定の行をクリックします。

   [Edit Setting] (設定の編集) ボックスが表示されます。

4. 必要に応じて設定を変更します。

5. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus により設定が保存されます。

設定を削除する

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで、**[Advanced]** (アドバンス) をクリックします。

   [Advanced Settings] (詳細設定) ページが表示されます。

3. 設定テーブルの削除する設定の行で、✕ ボタンをクリックします。

   設定を削除する選択でよいかを確認するダイアログボックスが表示されます。

4. **[Delete]** (削除) をクリックします。

   Tenable Nessus が設定を削除します。

次の表は、デフォルトでは Tenable Nessus に表示されないものも含め、設定できる詳細設定を示しています。

識別子	説明	デフォルト	有効な値
acas_classification	Tenable Nessus ユーザーインターフェースの上部と下部に分類バナーを追加し、最後に成功したログインと失敗したログインの通知をオンにします。	なし	• UNCLASSIFIED - 緑のバナー • CLASSIFIED - 紫のバナー • CONFIDENTIAL - 青いバナー • SECRET - 赤いバナー • TOP SECRET - オレンジ色のバナー • TOP SECRET/SCI - 黄色いバナーでフォントは黒色
multi_scan_same_host	無効になっている場合、ホストに負荷を掛けないよう、Tenable Vulnerability Management は単一の IP アド	×	yes または no

識別子	説明	デフォルト	有効な値
	レスに解決される複数のターゲットを 1 つのスキャナーが同時にスキャンしないようにします。代わりに Tenable Vulnerability Management スキャナーは、IP アドレスがスキャナー上の同じスキャンタスクまたは複数のスキャンタスクに複数回現れた場合、IP アドレスのスキャンを順番に実行します。スキャン完了までの時間が長くなる可能性があります。 有効になっている場合、Tenable Vulnerability Management スキャナーは、1 つの IP アドレスに解決される複数のターゲットを同じスキャンタスク内で、または複数のスキャンタスクにまたがって同時にスキャン可能です。スキャンの完了までの時間は短くなりますが、スキャンターゲットに負荷が掛かり、タイムアウトおよび不完全な結果が生じる可能性があります。		
merge_plugin_results	同一ホスト、ポート、プロトコルで複数の結果を生成するプラグインのプラグイン結果の統合をサポートします。Tenable は、Tenable Security Center にリンクされているスキャナーに対してこのオプションを有効にするこ	×	yes または no

識別子	説明	デフォルト	有効な値
	とをお勧めします。		
nessus_syn_scanner.global_throughput.max	Tenable Nessus がポートスキャン中に送信する 1 秒あたりの SYN パケットの最大数 (Tenable Nessus が並行してスキャンするホスト数とは無関係) を設定します。この設定は、大量の SYN パケットに対するリモートデバイスの脆弱性に応じて調整します。	65536	整数
login_banner	Tenable Nessus へのログインを試みた後に表示されるテキストバナー。このバナーが表示されるのは、新しいブラウザまたはコンピューターから初めてログインするときのみです。	なし	文字列
timeout.*<plugin ID>*	*<plugin ID>*にプラグイン ID を入力します。Tenable Nessus がプラグインを停止するまでに、Tenable Nessus がそのプラグイン *<pluginID>* の実行を許可する最大時間 (秒)。このオプションをプラグインに設定すると、この値が `plugins_timeout` よりも優先されます。	なし	0 から 86400 までの整数

スキャンエンジン設定

スタンドアロンの Tenable Nessus Professional または Tenable Nessus Expert であるか、Tenable Vulnerability Management やTenable Security Center によって管理されている Tenable Nessus スキャナーであるかに関わらず、すべての Tenable Nessus デプロイメントで詳細設定を行うことができます。これ

らの設定の一部はスキャンエンジン設定と呼ばれ、Tenable Nessus スキャンエンジンのスキャンパフォーマンスを制御します。スキャンポリシーの **[Settings]** (設定) の **[Performance Options]** (パフォーマンスオプション) セクションで、スキャンエンジン設定を調整できます。

Tenable Nessus スキャナー設定

次の表は、すべての詳細設定を網羅したリストではありません。スキャンエンジンのパフォーマンスに影響する設定のリストです。詳細設定の全一覧については、詳細なスキャン設定を参照してください。

設定	識別子	定義
Global Max Hosts Concurrently Scanned (同時スキャンされたグローバル最大ホスト数)	**global.max_hosts**	実行中のすべてのスキャンでスキャナーが同時に処理するターゲットの総数。この値は、スキャンエンジンで実行されるターゲットの総数を制限します。スキャンエンジンは、**global.max_hosts** に割り当てられた値を超えるターゲットを処理しません。
Max Concurrent Scans (最大同時スキャン)	**global.max_scans**	スキャンエンジンが同時に実行するスキャンの総数。
Global Max TCP Sessions (最大グローバル同時 TCP セッション)	**global.max_simult_tcp_sessions**	すべてのスキャンに許可される同時 TCP セッションの最大数。
Global Max Port Scanners (最大グローバルポートスキャナ)	**global.max_portscanners**	ポートスキャナータスクスレッドプールに割り当てられるスレッドの最大数。この値は、すべてのスキャンでエンジンが同時に実行するポートスキャナーの最大数を表します。
Max Concurrent Hosts Per Scan (スキャンごとの最大同時ホスト数)	**max_hosts**	スキャンエンジンが特定のスキャンで同時に処理するターゲットの最大数。
Max Concurrent Checks Per Host (ホストごとの最大	**max_checks**	特定のターゲットに対して同時に実行できるプラグインの最大数。この設定の値によって、各エンジンスレッドがターゲットに対して実行するプラグインの

同時チェック数)		数が決まります。
Max TCP Sessions Per Scan (スキャンごとの TCP セッションの最大数)	**max_simult_tcp_sessions**	特定のスキャンに許可される同時 TCP セッションの最大数。
Max TCP Sessions Per Host (ホストごとの TCP セッションの最大数)	**host.max_simult_tcp_sessions**	1 つのターゲットに許可される同時 TCP セッションの最大数。
Max Hosts Per Engine Thread (エンジンスレッドごとのホストの最大数)	**engine.max_hosts**	エンジンスレッドが処理するターゲットの最大数。
Optimal Hosts Per Engine Thread (エンジンスレッドごとの最適なホスト数)	**engine.optimal_hosts**	新しいエンジンスレッドを開始する前にスキャンエンジンがエンジンスレッドに割り当てるターゲットの数。
Max Engine Checks (エンジンスチェックの最大数	**engine.max_checks**	エンジンスレッドで実行されているすべてのターゲットにおいて、そのスレッドで実行できるプラグインの総数。
Max Engine Threads (エンジンスレッドの最大数)	**engine.max**	スキャンエンジンが開始するエンジンスレッドの最大数。
Minimum Engine Threads (エンジンスレッドの最小数)	**engine.min**	スキャンエンジンがスキャンの処理を開始するエンジンスレッドの最小数。

以降のセクションでは、優先順位とスキャンエンジンによるターゲットの処理に一部の設定がどのように影響するかに関する注意事項について簡単に説明します。

最大ホスト数の設定

次の設定は、スキャンエンジンのターゲットの処理に影響します。

- global.max_hosts
- max_hosts
- engine.max_hosts
- engine.max

ほとんどのシナリオでは、同時ターゲットの最大数を決定する際に、global.max_hosts がその他の設定よりも優先されますが、そうならないようにすることもできます。たとえば、engine.max_hosts と engine.max を操作することで、スキャナーが同時にスキャンするターゲットの最大数を制限できます。engine.max_hosts および engine.max の値がそのように設定されている場合は、次のようになります。

(engine.max_hosts x engine.max) < global.max_hosts

この場合、スキャナーはより厳しい制限 (engine.max_hosts と engine.max を乗算した値) を適用します。

最大同時 TCP セッションの設定

次の 3 つの詳細設定が、スキャンエンジンの同時 TCP セッションの数に影響を与えます。

- global.max_simult_tcp_sessions
- max_simult_tcp_sessions
- host.max_simult_tcp_sessions

global.max_simult_tcp_sessions 設定は、スキャナーで実行されるすべてのスキャンに適用される絶対上限です。max_simult_tcp_sessions 値は特定のスキャンの同時 TCP セッションを制限し、host.max_simult_tcp_sessions 設定はホストあたりの同時 TCP セッションを制限します。

最大チェック数の設定

スキャンエンジンが同時に実行できるプラグインの数は、次の 2 つの設定で制御します。

- max_checks
- engine.max_checks

engine.max_checks 設定は max_checks の設定よりも優先されるため、エンジンが同時に実行するプラグインの総数が (engine.max_checks x engine.max) を超えることはありません。

Tenable Vulnerability Management および Tenable Security Center のポリシー設定

Tenable Vulnerability Management または Tenable Security Center でスキャンを起動すると、1 つのスキャンが 1 つのスキャナーに割り当てられるわけではありません。代わりに、複数のスキャナーを効果的に利用するために、1 つのスキャンをより小さなチャンク (タスクと呼ばれる) に分割し、タスクを複数のスキャナーに分散します。これにより、複数のスキャナーが 1 つの全体的なスキャンを並行して実行できますが、スキャンエンジン設定の適用方法にも影響します。Tenable Nessus スキャンエンジンは、個々のタスクを 1 つのスキャン全体として解釈します。

たとえば、1,000 の IP をターゲットとする 1 つのスキャンがあるとします。Tenable Vulnerability Management および Tenable Security Center は、次の方法でスキャンを処理します。

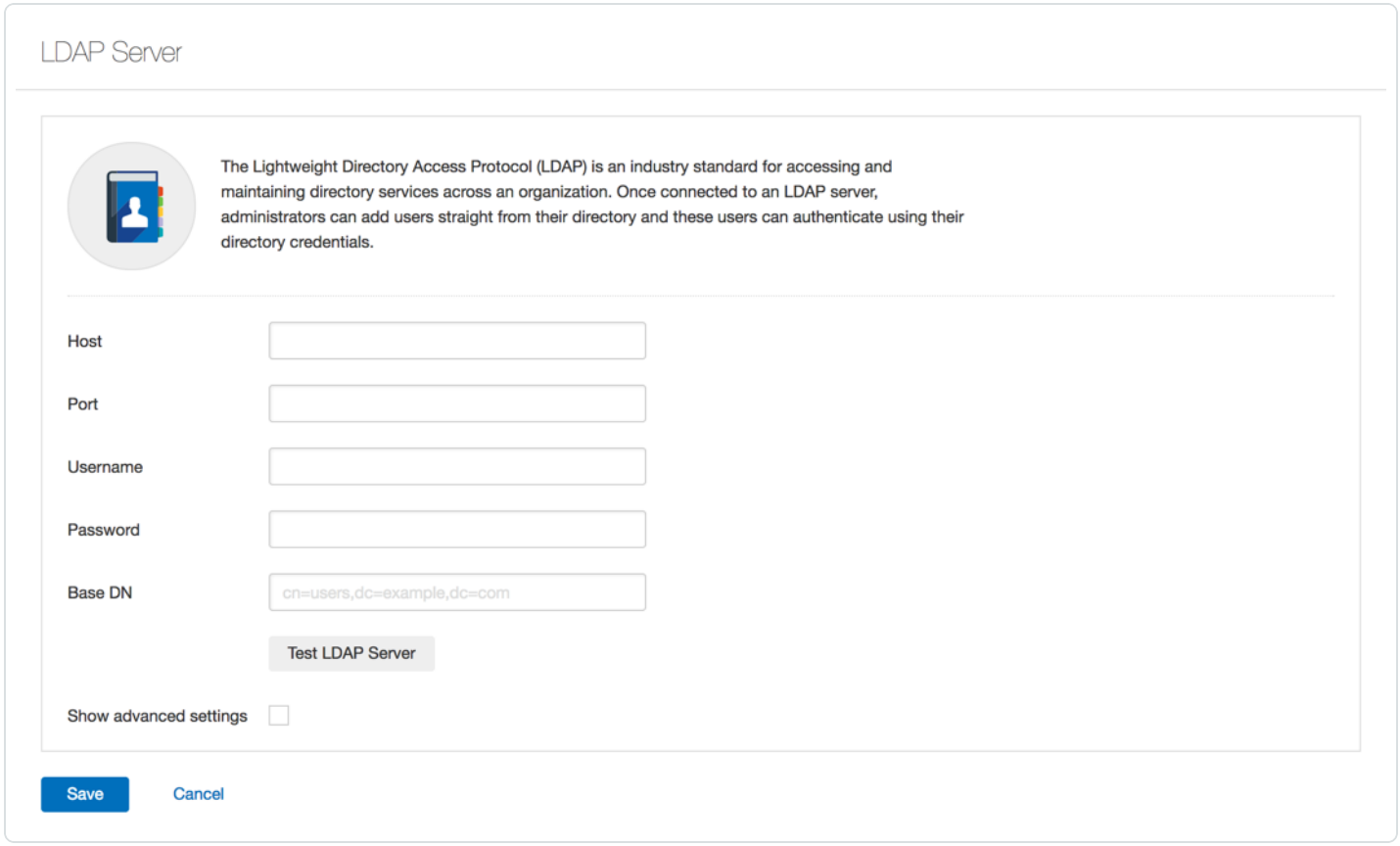
- **Tenable Vulnerability Management** – Tenable Vulnerability Management はスキャンターゲットを、それぞれ 120 IP の 8 個のタスクに分割し、9 個目のタスクに 40 IP を割り当てます。そして、スキャンポリシーの **max_hosts** (ユーザーインターフェースでは **[Max simultaneous hosts per scan]** (スキャンごとの同時ホストの最大数)) が 5 に設定されていると仮定します。このシナリオでは、特定のスキャナーがこれらの 9 個のタスクのうちの 5 個のタスクを取得し、最大 25 ホストを並列実行します (スキャンエンジンの設定に従い、スキャンあたり 5)。最大 5 ホストを並列実行するわけではありません。スキャナーが 5 個のタスクを完了すると、Tenable Vulnerability Management からタスクの新しいバッチを受け取り、スキャンジョブ全体が完了するまでスキャンを続行する場合もあります。
- **Tenable Security Center** – Tenable Security Center はスキャンターゲットを、それぞれ 8 IP の 125 個のタスクに分割します。そして、スキャンポリシーの **max_hosts** (ユーザーインターフェースでは **[Max simultaneous hosts per scan]** (スキャンごとの同時ホストの最大数)) がデフォルト値の 30 に設定されていると仮定します。このシナリオでは、特定のスキャナーが 125 個のタスクのうち 4 個のタスクを取得し、最大 30 ホストを並列実行します (スキャンエンジンの設定に従い、最初の 3 つのタスクで 8、最後のタスクで 6)。スキャナーがタスクを完了すると、Tenable Security Center から新しいタスクを受け取り、スキャンジョブ全体が完了するまでスキャンを続行します。

それぞれの「スキャンごと」の設定は、スキャン全体ではなく、個々の Tenable Vulnerability Management タスクまたは Tenable Security Center タスクに適用されます。これにより、スキャンポリシーでこれらのパフォーマンス調整パラメーターを設定するときに、混乱やスキャナーの予期しない動作が発生することがあります。

LDAP サーバー (Tenable Nessus Manager)

を使用する場合に必要な [ユーザーロール]Tenable Nessus Manager: System Administrator

Tenable Nessus Manager の **[LDAP Server]** (LDAP サーバー) ページに表示されるオプションを使用して、ディレクトリからユーザーをインポートするように Lightweight Directory Access Protocol (LDAP) サーバーを設定できます。



LDAP サーバーを設定するには

1. Tenable Nessus Manager の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[LDAP Server]** (LDAP サーバー) をクリックします。

   [LDAP Server] (LDAP サーバー) のページが表示されます。

3. 必要に応じて設定を行います。

設定	説明
Host (ホスト)	LDAP サーバーホスト。

Port (ポート)	LDAP サーバーポート。選択する値を LDAP サーバー管理者に確認してください。
Username (ユーザー名)	ユーザーデータを検索するための認証情報がある LDAP サーバー上のアカウントのユーザー名。 ユーザー名を、LDAP サーバーが提供する形式で指定します。
Password (パスワード)	ユーザーデータを検索するための認証情報がある LDAP サーバー上のアカウントのパスワード。
Base DN (ベース DN)	ユーザーデータを検索するための開始点として使用される LDAP 検索ベース。
Show advanced settings (詳細設定を表示する)	LDAP の詳細設定を表示または非表示にするには、**[Show advanced settings]** (詳細設定を表示する) チェックボックスをクリックします。
詳細設定 (オプション)	
Username Attribute (ユーザー名属性)	アカウントのユーザー名を含む LDAP サーバーの属性名。これは多くの場合、LDAP により使用される可能性があるサーバーで文字列 `sAMAccountName` で指定されます。 正しい値については、LDAP サーバーの管理者にお問い合わせください。
Email Attribute (メール属性)	アカウントのメールアドレスを含む LDAP サーバーの属性名。これは多くの場合、LDAP により使用される可能性があるサーバーで文字列 `mail` で指定されます。 正しい値については、LDAP サーバーの管理者にお問い合わせください。
Name Attribute (名前属性)	アカウントに関連付けられている名前を含む LDAP サーバーの属性名。これは多くの場合、LDAP により使用される可能性があるサーバーで文字列 `CN` で指定されます。 正しい値については、LDAP サーバーの管理者にお問い合わせくださ

	い。
CA (PEM Format) (CA (PEM 形式))	LDAP サーバーの認証局 (CA) の証明書 (該当する場合)。証明書を PEM 形式で入力します。

4. (オプション) **[Test LDAP Server]** (LDAP サーバーのテスト) ボタンをクリックして、入力した LDAP 設定を検証します。

   ページの右上に、LDAP 設定が有効かどうかを示すメッセージが表示されます。設定が有効でない場合は、設定を確認し、必要に応じて調整してください。

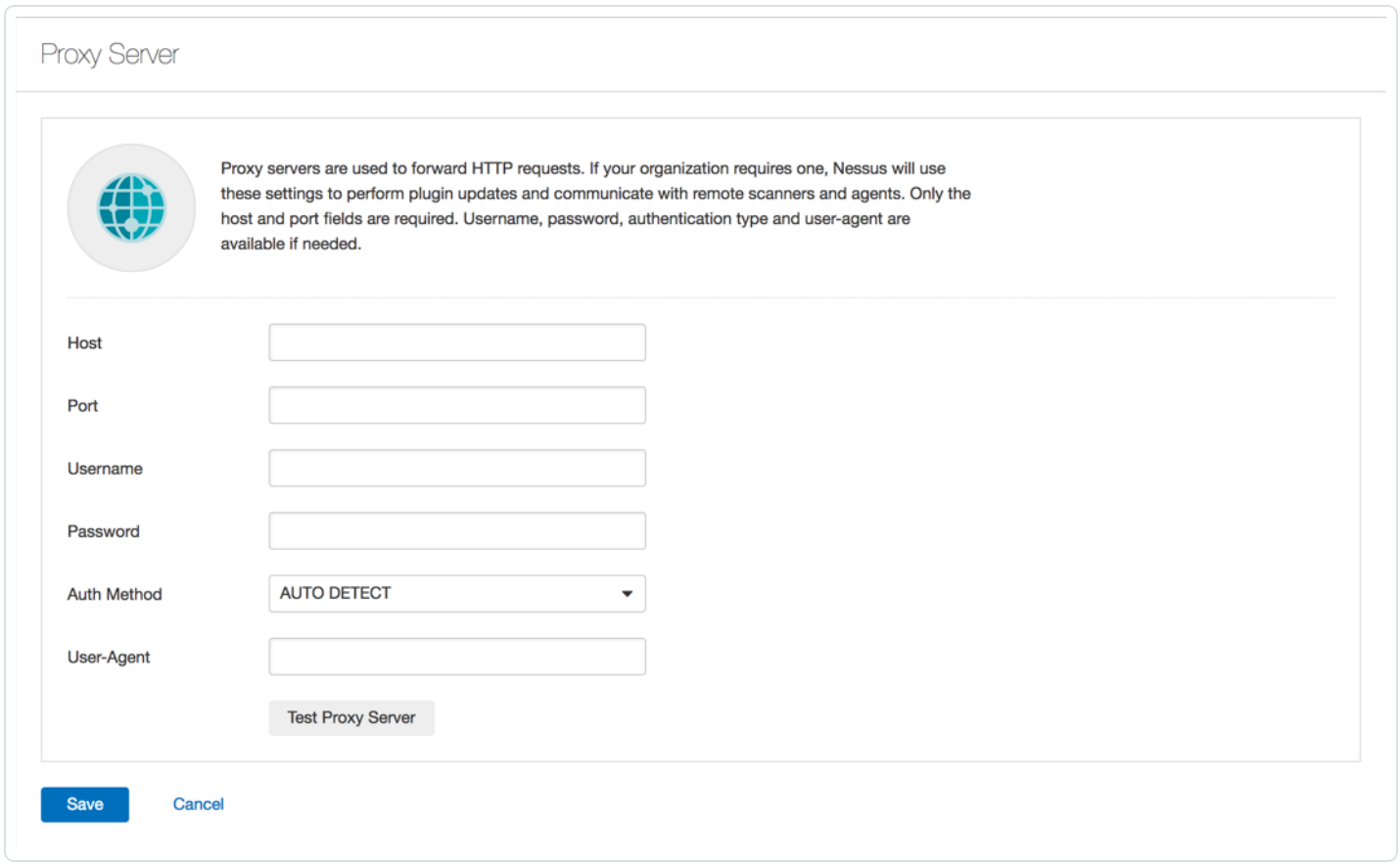
5. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus Manager により LDAP サーバー設定が保存されます。

プロキシサーバー

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

[Proxy Server] (プロキシサーバー) ページでは、プロキシサーバーを設定できます。お使いのプロキシによって特定の HTTP ユーザーエージェントがフィルタリングされる場合は、**[User-Agent]** (ユーザーエージェント) ボックスにカスタムユーザーエージェントの文字列を入力します。



プロキシサーバーを設定するには

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Proxy Server]** (プロキシサーバー) をクリックします。

   [Proxy Server] (プロキシサーバー) のページが表示されます。

3. 必要に応じて設定を行います。

設定	説明
Host (ホスト)	プロキシサーバーホスト。
Port (ポート)	プロキシサーバーポート。
Username (ユーザー名)	ユーザーデータを検索するための認証情報があるプロキシサーバー上のアカウントのユーザー名。

	ユーザー名を、プロキシサーバーが提供する形式で指定します。
Password (パスワード)	ユーザーデータを検索するための認証情報があるプロキシサーバー上のアカウントのパスワード。
Auth Method (認証方法)	Nessus がプロキシサーバーへの接続に使用する認証方法。 • **AUTO DETECT** – Tenable Nessus は以前の設定で入力した内容に基づく認証で接続を保護します。どの方法を選択すべきかわからない場合には、このオプションを選択することを推奨します。 • **NONE** – Tenable Nessus は認証を行いません • **BASIC** – Tenable Nessus は基本認証で接続を保護します。 • **DIGEST** – Tenable Nessus はダイジェスト認証で接続を保護します。 • **NTLM** – Tenable Nessus は NTLM 認証で接続を保護します。 **注意:** Tenable Nessus は NTLMv2 のみに対応しています。
User-Agent (ユーザーエージェント)	プロキシで事前定義されているユーザーエージェントが必要な場合は、プロキシサーバーのユーザーエージェント名。

4. **[Save]** (保存) ボタンをクリックします。

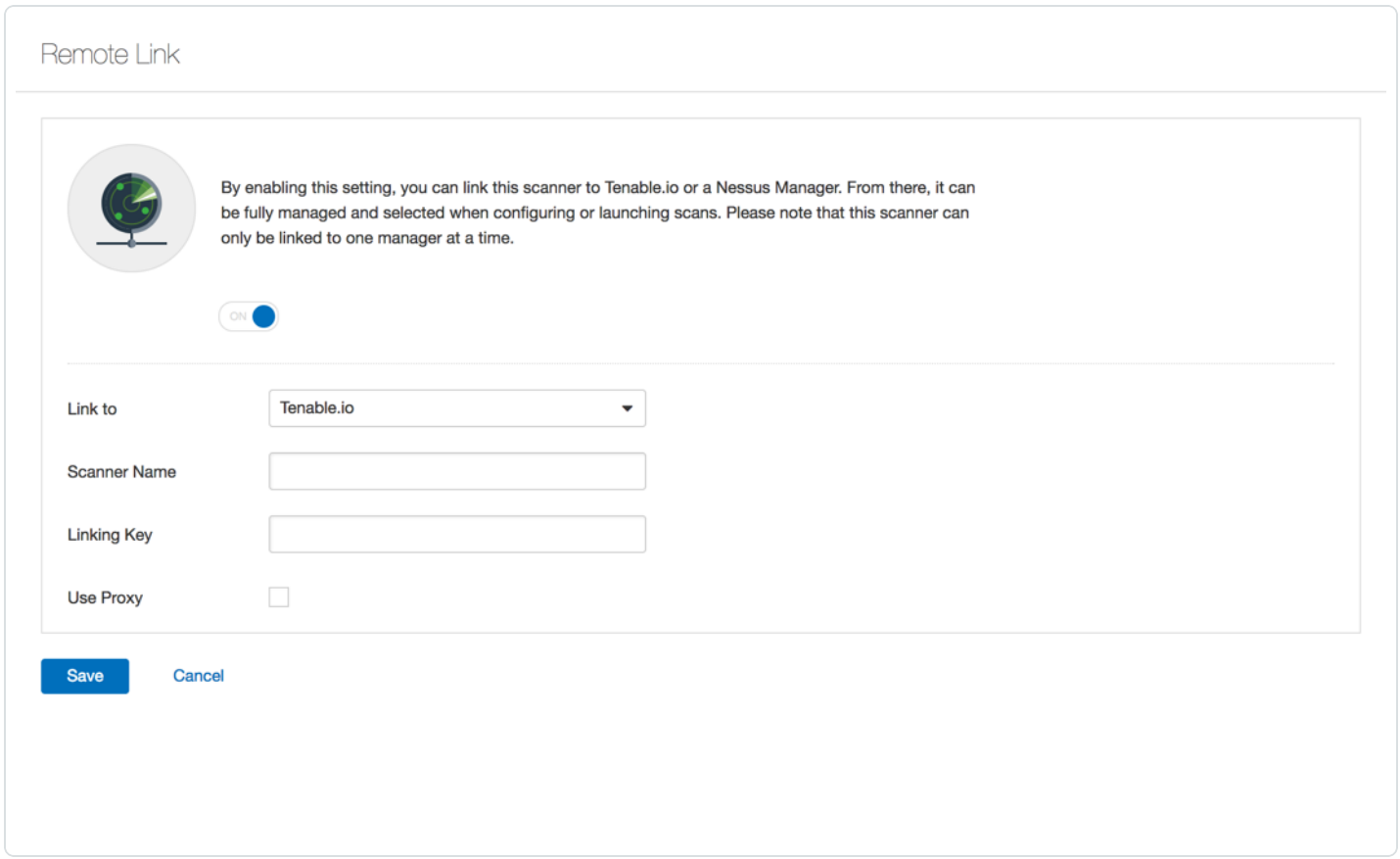
   Tenable Nessus により、プロキシサーバーが保存されます。

リモートリンク

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

[Remote Link] (リモートリンク) ページでは、Tenable Nessus スキャナーをライセンス済み Tenable Nessus Manager または Tenable Vulnerability Management にリンクできます。

注意: 初期インストール後にユーザーインターフェースから Tenable Security Center にリンクすることはできません。スキャナーがすでに Tenable Security Center にリンクされている場合、リンクを解除し、そのスキャナーを Tenable Vulnerability Management または Tenable Nessus Manager にリンクできますが、インターフェースから Tenable Security Center に再びリンクすることはできません。



トグルを有効または無効にしてスキャナーをリンクするか、スキャナーのリンクを解除します。

リモートリンク設定

オプション	設定先
Tenable Nessus を Tenable Nessus Manager にリンク	
Link to (リンク先)	**Nessus Manager**
Scanner Name (スキャナー名)	この Tenable Nessus スキャナーに使用する名前です。
Manager Host (マネージャーホスト)	リンク先となる Tenable Nessus Manager インスタンスの静的IPアドレスまたはホスト名です。

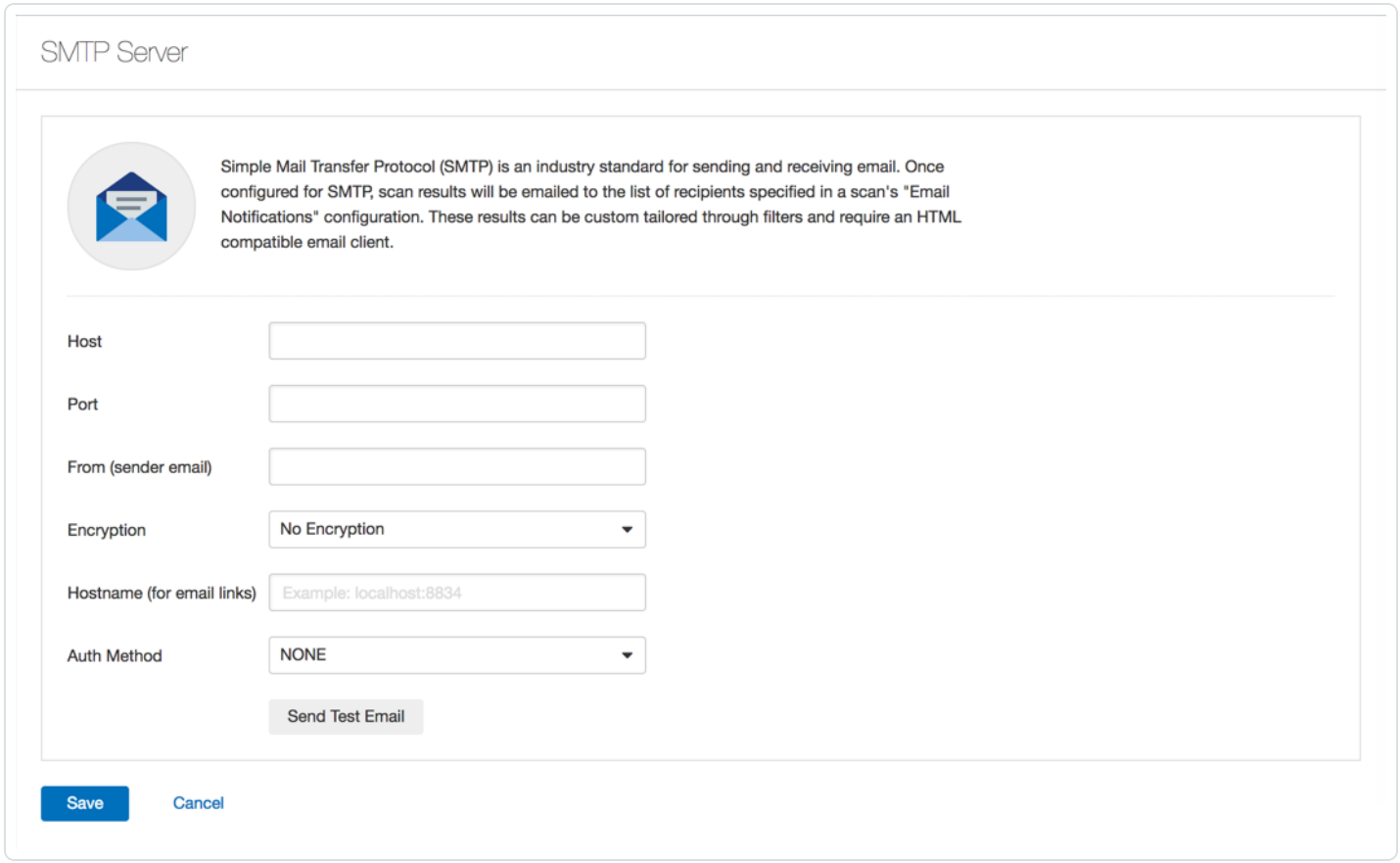
オプション	設定先
Manager Port (マネージャーポート)	お使いの Tenable Nessus Manager のポート、またはデフォルトの 8834 です。
リンクキー	Tenable Nessus Manager インスタンス固有のキーです。
Use Proxy (プロキシを使用)	プロキシ設定に応じて、チェックボックスを選択または選択解除します。**[Use Proxy]** (プロキシを使用する) を選択した場合は、次の設定も必要です。 • **ホスト** – プロキシサーバーのホスト名または IP アドレスです。 • **Port** – プロキシサーバーのポート番号です。 • **ユーザー名** – プロキシサーバーへのアクセスと使用が許可されたアカウントのユーザー名です。 • **Password** – 入力したユーザー名に関連付けられたパスワードです。
Tenable Nessus を Tenable Vulnerability Management にリンク	
Link to (リンク先)	**Tenable.io**
Scanner Name (スキャナー名)	**cloud.tenable.com**
リンクキー	Tenable Vulnerability Management インスタンス固有のキーです。このキーは次のような形式の文字列です。 *2d38435603c5b59a4526d39640655c3288b00324097a08f7a93e5480940d1cae*
Use Proxy (プロキシを使用)	プロキシ設定に応じて、チェックボックスを選択または選択解除します。**[Use Proxy]** (プロキシを使用する) を選択した場合は、次の設定も必要です。 • **ホスト** – プロキシサーバーのホスト名または IP アドレスです。 • **Port** – プロキシサーバーのポート番号です。

オプション	設定先
	• **ユーザー名** – プロキシサーバーへのアクセスと使用が許可されたアカウントのユーザー名です。 • **Password** – 入力したユーザー名に関連付けられたパスワードです。

SMTP サーバー

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

[SMTP Server] (SMTP サーバー) ページでは、Simple Mail Transfer Protocol (SMTP) サーバーを設定できます。SMTP サーバーを設定すると、Nessus はスキャン設定で指定した受信者のリストに HTML スキャン結果を電子メールで送信できます。



注意: Tenable Nessus が Tenable Vulnerability Management にリンクされている場合、**[SMTP Server]** (SMTP サーバー) ページは利用できません。

SMTP サーバーを設定するには

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[SMTP Server]** (SMTP サーバー) をクリックします。

   [SMTP Server] (SMTP サーバー) のページが表示されます。

3. 必要に応じて設定します。

設定	説明
Host (ホスト)	SMTP サーバーホスト。
Port (ポート)	SMTP サーバーポート。
From (sender email)	スキャン結果の電子メールで送信者として表示される電子メールアドレス。
Encryption (暗号化)	メール暗号化タイプ • **暗号化なし** – Tenable Nessus は、メールを暗号化しません。 • **SSL を強制** – Tenable Nessus メールで SSL 暗号化を強制します。 • **TLS を強制** – Tenable Nessus メールで TLS 暗号化を強制します。 • **利用可能な場合は TLS を使用** – 受信サーバーに互換性がある場合、Tenable Nessus は TLS 暗号化を使用します。
ホスト名 (メールリンク用)	メールの送信者ホストおよびポートを示すホスト名。
Auth Method (認証方法)	Nessus が SMTP サーバーへの接続に使用する認証方法。 • **NONE** – Tenable Nessus は接続の認証を行いません。 • **PLAIN** – Tenable Nessus は、プレーン (ユーザー名 / パスワード) 認証で接続を保護します。 • **LOGIN** – Tenable Nessus は、ログイン認証で接続を保護します。

	• **NTLM** – Tenable Nessus は NTLM 認証で接続を保護します。 • **CRAM-MD5** – Tenable Nessus は、CRAM-MD5 認証で接続を保護します。

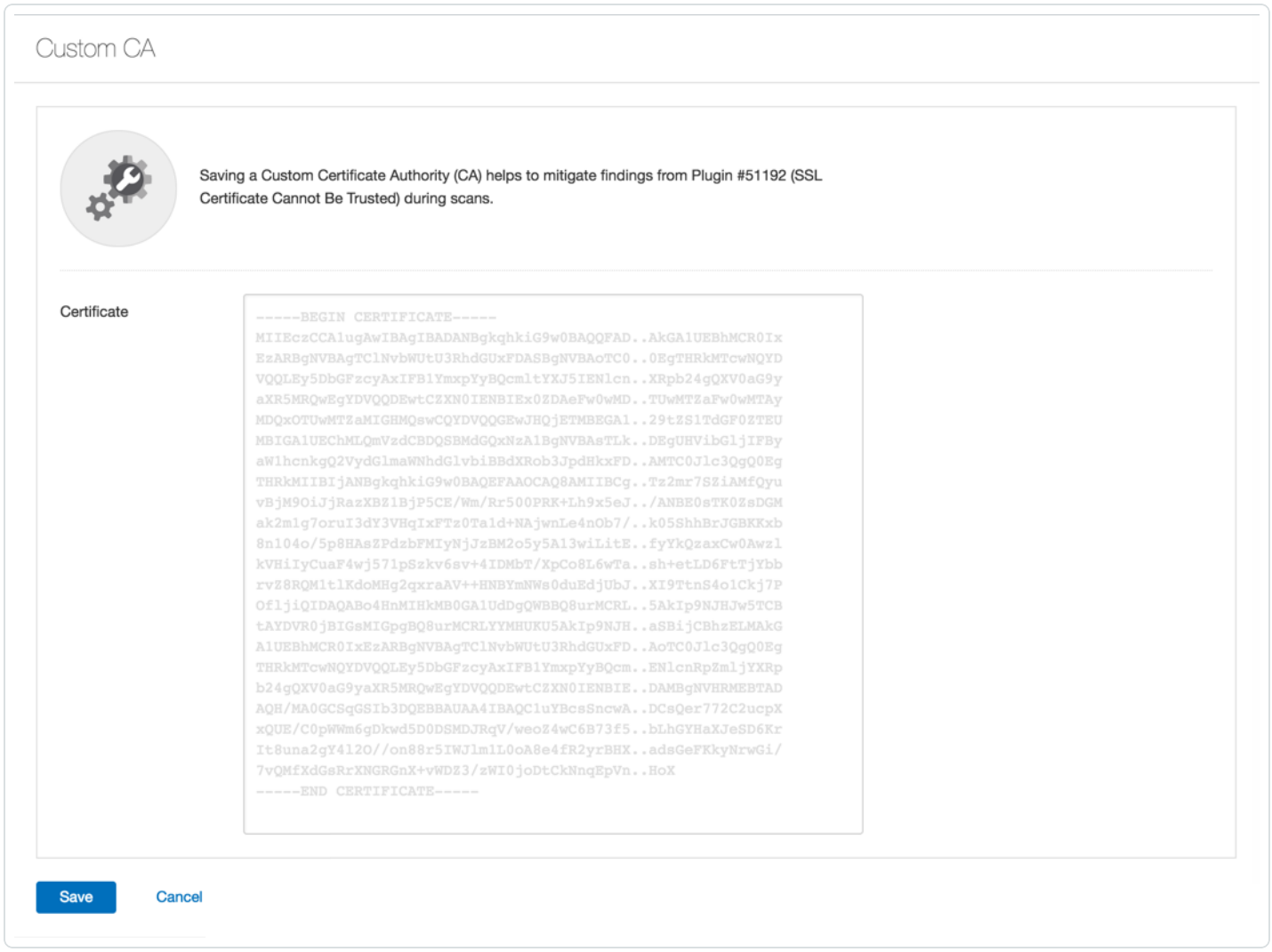
4. **[Save]** (保存) ボタンをクリックします。

   Tenable Nessus により、SMTP サーバーが保存されます。

カスタム CA

を使用する場合に必要な [ユーザーロール](#)Tenable Nessus Manager: System Administrator

[Custom CA] (カスタム CA) ページには、Nessus でカスタム認証局 (CA) をアップロードするために使用するテキストボックスが表示されます。詳細は、[証明書および認証局](#) を参照してください。



注意：開始テキスト `-----BEGIN CERTIFICATE-----` と終了テキスト `-----END CERTIFICATE-----` を含めます。

ヒント：1 つのテキストファイルに証明書を 1 つ以上保存することができます。それぞれについて、開始テキストと終了テキストを含めます。

アップグレードアシスタント

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

以下の機能は、Federal Risk and Authorization Management Program (FedRAMP) 環境ではサポートされていません。詳細については、FedRAMP 製品を参照してください。

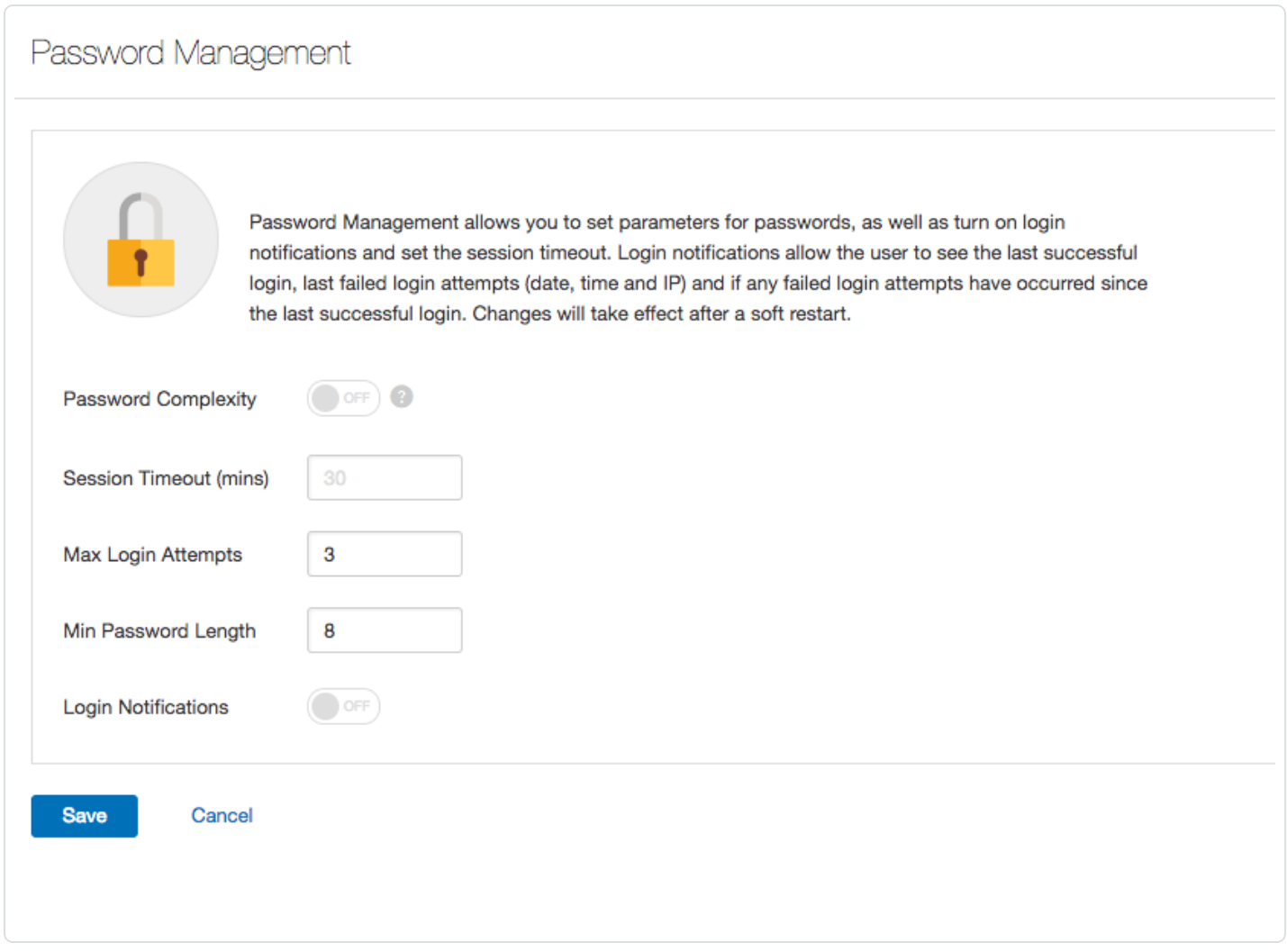
アップグレードアシスタント ツールは、Tenable Nessus のクラスタリング環境では使用できません。

アップグレードアシスタントツールを使って、Tenable Nessus から Tenable Vulnerability Management にデータをアップグレードできます。詳細は、Tenable Nessus から Tenable Vulnerability Management へのアップグレードアシスタントを参照してください。

パスワード管理

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

[Password Management] (パスワード管理) ページでは、パスワード、ログイン通知、セッションタイムアウトのパラメーターを設定できます。



ヒント: nessuscli からパスワード管理設定を行えます。詳細については、Nessuscli トピック内の nessuscli fix --set <password_setting>=<value> をご覧ください。

ヒント: Tenable がパスワードを保存および保護するために使用するセキュリティの詳細については、暗号強度を参照してください。

パスワード管理を設定するには

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Password Mgmt]** (パスワード管理) をクリックします。

   [Password Management] (パスワード管理) ページが表示されます。

3. 必要に応じて設定を行います。

設定	デフォルト	説明
Password Complexity (パスワードの複雑さ)	オフ	Tenable Nessus パスワードが 8 文字以上で、大文字、小文字、特殊文字、数字から 3 種類以上を使用する必要があるかどうかを決定します。
Session Timeout (mins) (セッションタイムアウト (分))	30	ウェブセッションがタイムアウトするまでの時間 (分) を定義します。セッションのアイドル時間がこのタイムアウトの値を超えると、Tenable Nessus はユーザーを自動的にログアウトさせます。
Max Login Attempts (最大ログイン試行回数)	5	アプリケーションがアカウントをロックアウトするまでに Tenable Nessus で許可される、ユーザーの最大ログイン試行回数を定義します。この値をゼロに設定すると、機能は無効になります。
Min Password Length (パスワードの最小文字数)	8	アカウントのパスワードの最小文字数を定義します。
Login Notifications (ログイン通知)	オフ	Tenable Nessus がログイン通知を表示できるかどうかを決定します。 ログイン通知を使用すると、最後に成功したログインと失敗したログイン (日付、時刻、IP)、また最後に成功したログイン以降に失敗したログインがあるかどうかを確認できます。

4. **[保存]** ボタンをクリックします。

   Tenable Nessus は、パスワード設定を保存します。

   注意: [Session Timeout] (セッションタイムアウト) および **[Max Login Attempts]** (最大ログイン試行回数) 設定の変更を有効にするには、再起動する必要があります。

スキャナーの正常性

を使用する場合に必要なユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

[Scanner Health] (スキャナーの正常性) ページには、Tenable Nessus スキャナーのパフォーマンスに関する情報が表示されます。リアルタイムの状態およびパフォーマンスデータを監視して、スキャナーの問題のトラブルシューティングに役立てることができます。スキャナーの警告には、スキャナーの誤動作の原因となるシステムエラーに関する情報が表示されます。

エラーに対処すると、Tenable Nessus によってアラートが削除されます (たとえば、ディスク容量不足に関するアラートを受信した場合、不要なファイルを削除してディスク容量を増やすとアラートが削除されます)。Tenable Nessus は、情報を 30 秒ごとに更新します。

Tenable Nessus では、スキャナーの正常性に関する情報が概要、ネットワーク、アラート の 3 つのカテゴリに分けられます。

概要

ウィジェット	説明	アクション
Current Health (現在の正常性)	Nessus のメモリ使用量 (MB 単位)、CPU 負荷、Tenable Nessus がスキャンしているホストの数を表示するウィジェット。	なし
Scanner Alerts (スキャナーの警告)	Tenable Nessus スキャナーのパフォーマンスが良好ではないエリアにアラートを出します。アラートには、情報、注意、警告、重要の深刻度レベルがあります。	アラートをクリックすると詳細を確認できます。 アラートが 5 件以上ある場合、**[More Alerts]** (アラートをさらに表示) をクリックしてアラート一覧を確認します。
System Memory (システムメモリ)	Tenable Nessus が使用しているシステムメモリ量を示すチャート。	なし
Nessus Data Disk Space	Tenable Nessus のデータディレクトリがインストールされているディスクの空き容量と使用	なし

(Nessus データディスクスペース)	量の割合を示すチャート。	
Memory Usage History (メモリ使用履歴)	Tenable Nessus のメモリ使用量 (MB) の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。
CPU Usage History (CPU 使用履歴)	Tenable Nessus の CPU 使用率の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。
Scanning History (スキャンの履歴)	Tenable Nessus が実行したスキャン回数と Tenable Nessus がスキャンしたアクティブなターゲットの数の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。

ネットワーク

ウィジェット	説明	アクション
Scanning History (スキャンの履歴)	Tenable Nessus が実行したスキャン回数と Tenable Nessus がスキャンしたアクティブなターゲットの数の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。
Network Connections (ネットワーク接続数)	Tenable Nessus がスキャン中に作成した TCP セッション数の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。
Network Traffic (ネットワークトラフィック量)	Tenable Nessus がネットワークを介して送受信するトラフィック量の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。
Number of DNS Lookups (DNS ルックアップ数)	Tenable Nessus が実行する逆引き DNS (rDNS) と DNS ルックアップの数の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。

DNS Lookup Time (DNS ルックアップ時間)	Tenable Nessus の rDNS および DNS ルックアップの実行にかかった平均時間の推移を示すグラフ。	グラフ上の点にカーソルを合わせると詳細データを確認できます。

アラート

ウィジェット	説明	アクション
Scanner Alerts (スキャナーの警告)	Tenable Nessus スキャナーのパフォーマンスが良好ではないエリアについてのアラートの一覧です。アラートには、情報、注意、警告、重要の深刻度レベルがあります。	アラートをクリックすると詳細を確認できます。

詳細は、スキャナーの正常性を監視する を参照してください。

スキャナーの正常性を監視する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: 管理者またはシステム管理者

[Scanner Health] (スキャナーの正常性) ページには、Tenable Nessus スキャナーのパフォーマンスに関する情報が表示されます。パフォーマンスデータに関する詳細は、スキャナーの正常性 を参照してください。

スキャナーの正常性を監視する方法

1. Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Scanner Health]** (スキャナーの正常性) をクリックします。

3. (オプション) グラフの時間の単位を調整するには、**[Overview]** (概要) タブのドロップダウンボックスから期間を選択します。

   [Overview] (概要) と **[Network]** (ネットワーク) の各タブのグラフには選択した期間が反映されています。

4. (オプション) 時間のグラフで項目を非表示にするには、凡例で該当する時間をクリックします。

   ヒント: 項目を非表示にすると、表示可能な項目に合わせてサイズが自動調整され、1 つのデータセットを

一目で確認できるようになります。

5. [**概要**]、[**ネットワーク**]、[**アラート**] タブのいずれかをクリックします。

詳細なデバッグ - パケットキャプチャ

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

スキャン結果を理解するためにTenable Nessusと連携する際は、スキャナーとスキャンされたホスト間の通信について理解する必要が生じる場合があります。その場合、Tenable サポートは、スキャナーとターゲットホスト間のネットワークトラフィックのキャプチャをリクエストします。Tenable Nessus では現在、Tenable Nessus ユーザーインターフェースを使用して、こうしたキャプチャを生成およびダウンロードできるようになっています。

注意: この機能には以下のような制約があります。

- パケットキャプチャは、Tenable Security Center にリンクされている Tenable Nessus スキャナーには適用されません。
- パケットキャプチャは TCP および UDP トラフィックだけに制限されます。ICMP (ping) のようなその他のプロトコルはキャプチャされません。
- **[Target to capture]** (キャプチャするターゲット) フィールドの値は、スキャンのターゲットリストに含まれるホストと一致している必要があります。一致していないと、キャプチャは行われません。
- Tenable Nessusはパケットキャプチャのデータに割り当て可能なディスク容量を制限します。パケットキャプチャサブシステムで使用される可能性があるディスクの総容量は、次の 2 つのパラメーターのうち小さい方となります。Tenable Nessus がインストールされるパーティションサイズの 10% もしくは 20 GB。
- 単一のパケットキャプチャファイルの最大サイズは次の 2 つのパラメーターのうち小さい方となります。パケットキャプチャのディスクの総容量値の 10% もしくは 1 GB。
- キャプチャのセッション中にデータ総量が単一のキャプチャファイルの制限を超えた場合、当該キャプチャは終了し、一部の結果が保存されます。これらの制限は、Tenable Nessus 管理者が `global.network_capture.max_disk_mb` や `global.network_capture.max_file_mb` の詳細な環境設定を使用して調整している可能性があります。
- これらの変更を適用するには、Tenable Nessus を再起動する必要があります。

Tenable Nessus ユーザーインターフェースでパケットキャプチャをスキャンに使用できるようにする方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 右上の **[New Scan]** (新しいスキャン) ボタンをクリックします。

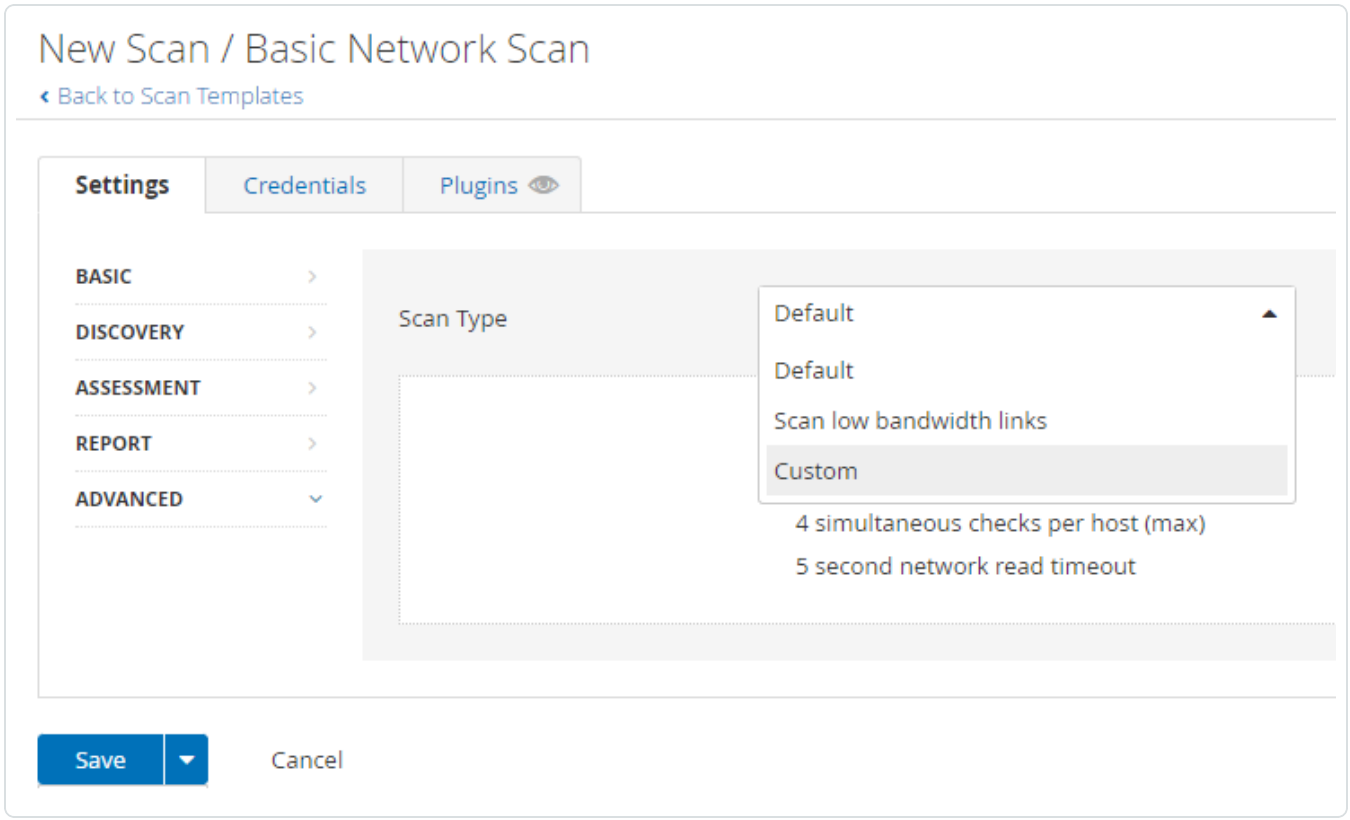
   [Scan Templates] (スキャンテンプレート) ページが表示されます。

3. 使用するスキャンテンプレートをクリックします。

   [New Scan] (新しいスキャン) ページが表示されます。

4. **[Advanced]** (アドバンス) 設定タブをクリックします。

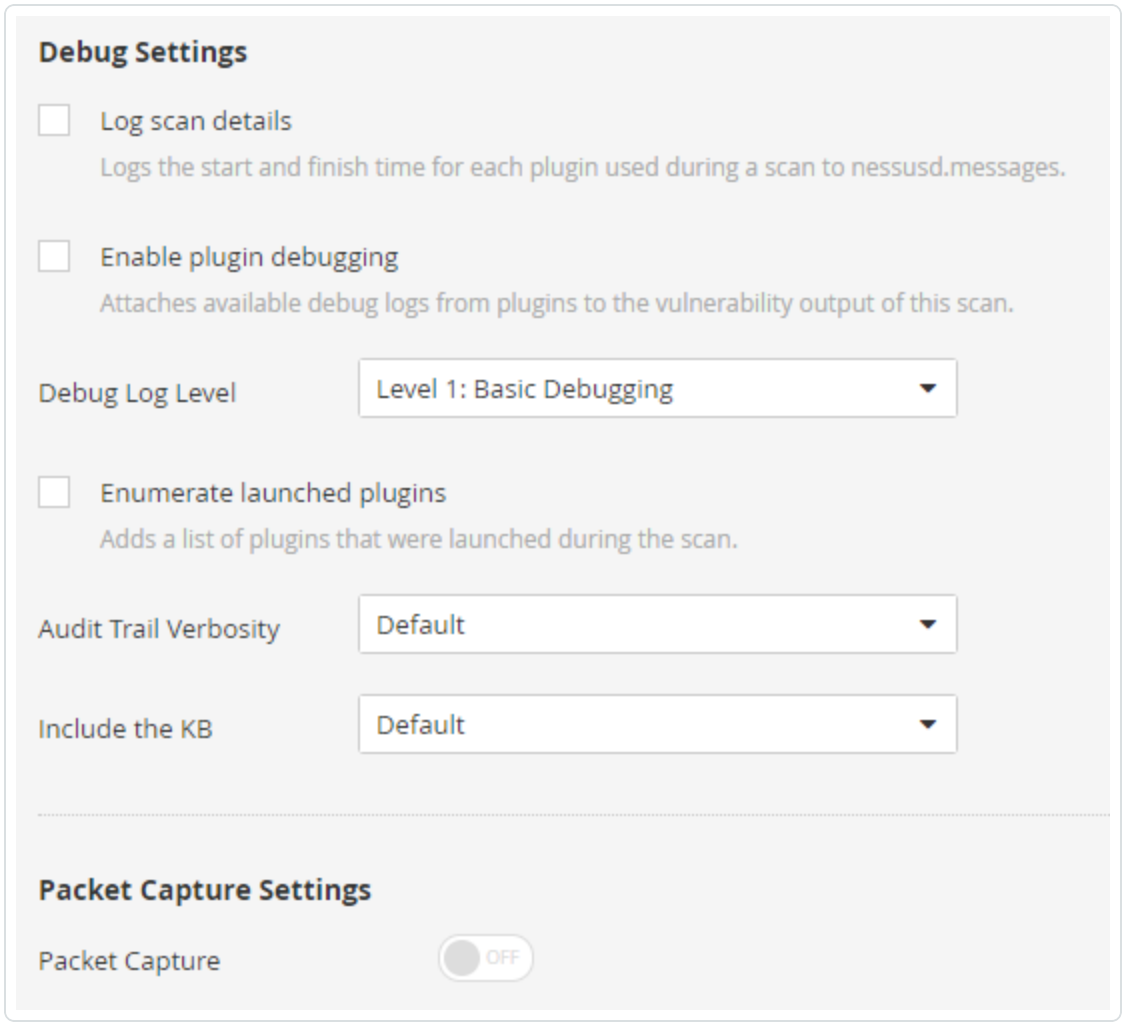
5. **[Scan Type]** (スキャンタイプ) のドロップダウンから **[Custom]** (カスタム) を選択します。



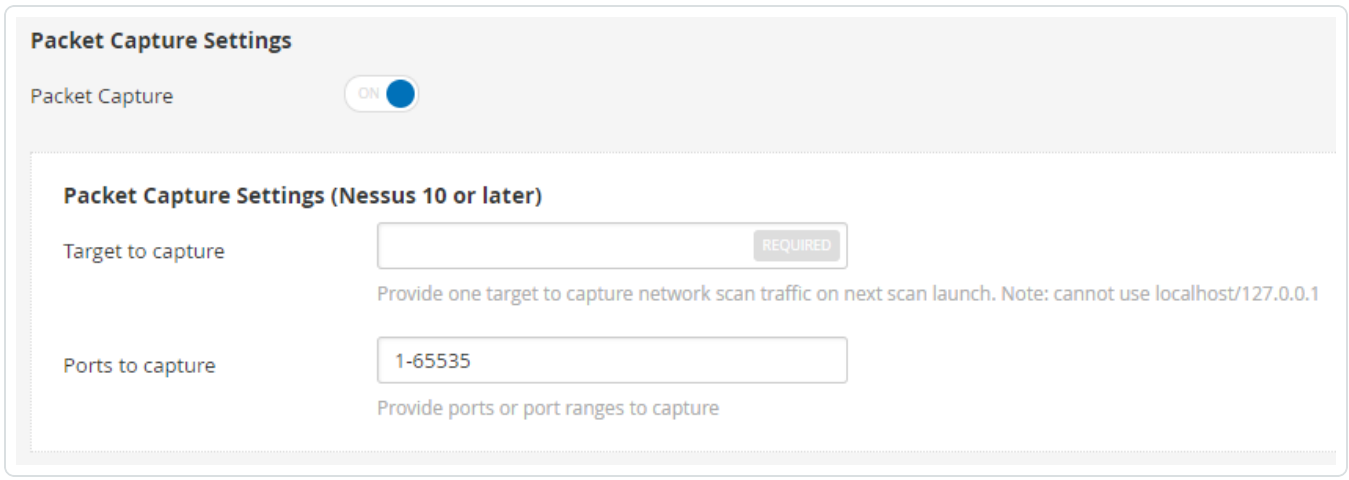
注意: この手順は、基本ネットワークスキャンを設定している場合にのみ必要です。高度なネットワークスキャンを設定している場合は、この手順をスキップしてください。

6. **[General]** (全般) をクリックします。

7. **[General]** (全般) 設定ウィンドウの最下部までスクロールして、**[Packet Capture]** (パケットキャプチャ) を **[ON]** (オン) に設定します。



8. **[Target to capture]** (キャプチャするターゲット) フィールドで、単一ホストの IP アドレスまたはホスト名を入力します。



9. **[Ports to capture]** (キャプチャするポート) フィールドで、ポートまたはポートの範囲を入力します。
10. **[Save]** (保存) ボタンをクリックします。
11. スキャンを起動します。

パケットキャプチャを取得する方法

スキャンの完了後、パケットキャプチャを含む圧縮されたアーカイブは、ダウンロード可能となります。

パケットキャプチャをダウンロードする方法

1. 上部のナビゲーションバーから **[Settings]** (設定) を選択します。
2. 横のナビゲーションバーから **[Debug Logs]** (デバッグログ) を選択します。

   [Debug Logs] (デバッグログ) ウィンドウではパケットキャプチャのリストが表示されます。例としては、`pcap_SCANNAME_SCANID.tar.gz` です。
3. スキャンに一致するアーカイブを選択します。
4. **[Download]** (ダウンロード) ボタンをクリックします。

   スキャナーからローカルのホストにファイルがダウンロードされます。

通知

Tenable Nessus では、ログイン試行、エラー、システム情報、ライセンス期限情報などの通知が定期的に表示されます。これらの通知はログイン後に表示され、通知ごとに受領または拒否することを選択できます。

次の表では通知を表示する 2 つの方法について説明しています。

通知の表示	Location	説明
Current notifications	上部のナビゲーションバーのベルのアイコン ( )	このセッション中に生成された通知が表示されます。 通知を確認すると、その通知は現在の通知セッションに表示されなくなります。ただし、通知履歴には引き続き表示されます。
Notification history	**[Settings]** (設定) > **[Notifications]** (通知)	過去 90 日間のすべての通知が表示されます。 通知表には、各通知と発表日時、受領確認の有無、深刻度、メッセージが表示されます。受領が確認されていない通知は太字で表示されます。通知履歴ビューから通知の受領を確認することはできません。

通知を管理するには、次の手順に従います。

通知を表示する

現在のセッションの未処理の通知を表示できます。また、過去 90 日間の通知履歴も表示できます。

現在の通知を表示する方法

上部のナビゲーションバーで、 をクリックします。

通知履歴を表示する方法

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Notifications]** (通知) をクリックします。

   [Notifications] (通知) ページが表示され、通知テーブルが表示されます。

3. (オプション) 通知テーブルの結果を絞り込むために通知をフィルターまたは検索します。

通知を確認する

通知を確認すると、その通知は現在の通知セッションに表示されなくなります。ただし、通知履歴には引き続き表示されます。通知履歴ビューからは通知を確認できません。

通知を確認しない選択をしている場合、次回のログイン時に表示されます。一部の通知は確認できません。代わりに、推奨するアクションを実行する必要があります。

通知を確認する方法

- 通知ウィンドウで、**[Acknowledge]** (確認)をクリックします。
- 通知バナーで、**[Dismiss]** (拒否) をクリックします。
- 右上の通知で、🗑 をクリックします。

現在の通知を消去する方法

1. 上部のナビゲーションバーで、 をクリックします。
2. **[Clear Notifications]** (通知を消去) をクリックします。

   注意:通知を消去しても、通知の確認は行われません。現在の通知から削除されます。

アカウント

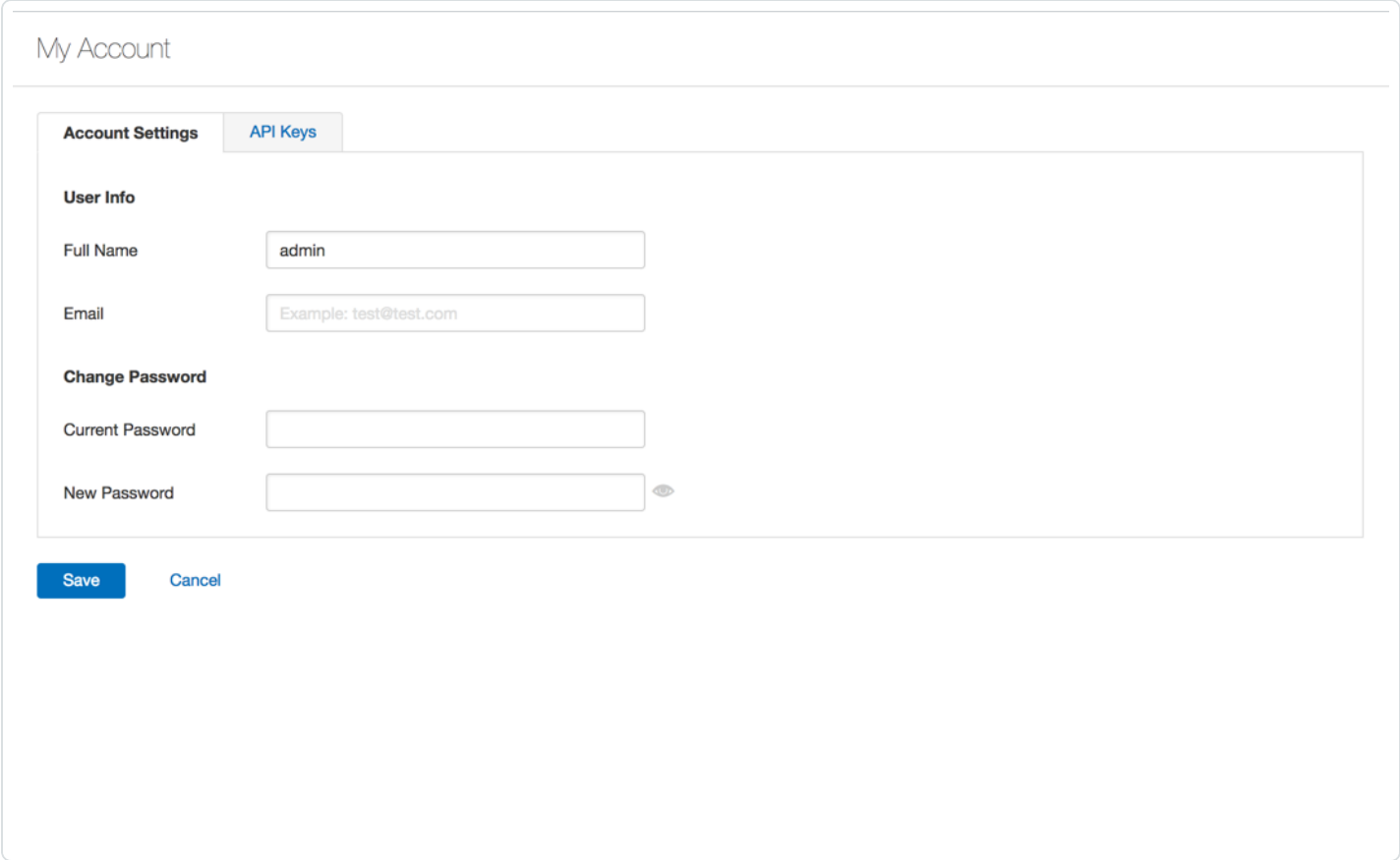
このセクションには、**[Settings]** (設定) ページの **[Accounts]** (アカウント) セクションで使用できる次のタスクが含まれています。

- ユーザーアカウントを変更する
- API キーを生成する
- Create a User Account
- Modify a User Account
- Delete a User Account

マイアカウント

[Account Settings] (アカウント設定) ページには、現在認証されているユーザーの設定が表示されます。

注意: 作成した後にユーザー名を変更することはできません。



API キー

API キーは、アクセスキーとシークレットキーで設定されます。API キーは、**Nessus REST API** によって認証され、`X-ApiKeys` HTTP ヘッダーを使用してリクエストとともに渡されます。

注意:

- Nessus は、API キーを初回生成時にのみ表示します。API キーは安全な場所に保管してください。
- Tenable Nessus で API キーを表示することはできません。API キーをなくした場合、新しい API キーを生成する必要があります。
- API キーを再生成すると、そのキーを現在使用しているアプリケーションは認証されなくなります。

ユーザーアカウントを変更する

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[My Account]** (マイアカウント) をクリックします。

   [My Account] (マイアカウント) ページが表示されます。

3. 必要に応じて、名前、メールアドレス、パスワードを変更します。

   > **注意:** アカウント作成後は、ユーザー名を変更できません。

   > **注意:** パスワードには Unicode 文字は使用できません。

4. **[Save]** (保存) をクリックします。

   Tenable Nessus により、アカウント設定が保存されます。

API キーを生成する

> **を使用する場合に必要な ユーザーロールTenable Nessus Manager:** System Administrator

Tenable Nessus Manager では、Tenable Nessus ユーザーインターフェースの **[API Keys]** (API キー) タブから API キーを生成できます。API キーを生成することで、さまざまなタスクを自動化し、Tenable Nessus を企業内の他のセキュリティツールやシステムと統合できます。新しい API キーを生成するまで、API キーは期限切れになりません。

[API Keys] (API キー) タブは、ライセンスや設定によっては、Tenable Nessus Manager に加えて Tenable Nessus Professional や Tenable Nessus Expert で使用できる場合があります。詳細については、Tenable Customer Success Manager にお問い合わせください。

> **注意:** Tenable Security Center および Tenable Vulnerability Management エンタープライズソリューションの一部として許可されていない限り、Tenable Nessus スキャン API に直接アクセスしてスキャンを設定または起動することはできません。

> **警告:** 新しい API キーを生成すると、既存のキーがすべて置き換えられ、リンクされているアプリケーションの認証がすべて解除されます。

API キーを生成する方法

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[My Account]** (マイアカウント) をクリックします。

   [My Account] (マイアカウント) ページが表示されます。

3. **[API Keys]** (API キー) タブをクリックします。

4. **[Generate]** (生成) をクリックします。

   新しい API キーを生成する選択でよいかを確認するダイアログボックスが表示されます。

5. **[Generate]** (生成) をクリックします。

   新しい API キーが表示されます。

   > **ヒント:** Tenable Nessus API ドキュメントにアクセスするには、***<Tenable Nessushost>:<port>*/api#/overview** に移動します。

ユーザーTenable Nessus Manager

> **を使用する場合に必要な [ユーザーロール]Tenable Nessus Manager:** 管理者またはシステム管理者

> **注意: [Users]** (ユーザー) ページは Tenable Nessus Manager でのみ利用可能です。Tenable Nessus Professional、Tenable Nessus Expert、および Tenable Nessus Essentials の全ユーザーは、システム管理者のアクセス許可を持ちます。

[Users] (ユーザー) ページには、Tenable Nessus Manager のすべてのユーザーアカウントを示す表が表示されます。このドキュメントでは、この表を*ユーザーテーブル*と呼びます。ユーザーテーブルの各行には、ユーザー名、最終ログイン日、アカウントに割り当てられたロールが表示されます。

ユーザーアカウントには、ユーザーが Tenable Nessus Manager で持つアクセスレベルを指定するロールが割り当てられます。ユーザーアカウントのロールは、いつでも無効にしたり、変更したりすることができます。次の表は、ユーザーに割り当てることができるロールを示しています。

Name (名前)	説明
Basic (基本)	基本ユーザーは、スキャン結果を閲覧できます。
Standard	標準ユーザーは、スキャンとポリシーを作成できます。

Name (名前)	説明
	標準ユーザーが作成したスキャンは、スキャン作成者から編集権限を与えられない限り、他の標準ユーザーは編集できません。
Administrator (管理者)	管理者は、標準ユーザーと同じ権限を持ちますが、ユーザー、ユーザーグループ、スキャナーの管理、および他のユーザーが共有するスキャンの表示も可能です。
System Administrator (システム管理者)	システム管理者は、管理者と同じ権限を持ちますが、システム構成設定の管理および変更も行うことができます。
Disabled	無効になったユーザーアカウントは、Tenable Nessus へのログインに使用できません。

ユーザーアカウントを管理するには、次の手順を使用します。

ユーザーアカウントを作成する

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Users]** (ユーザー) をクリックします。

   [Users] (ユーザー) ページが表示されます。

3. 右上の **[New User]** (新しいユーザー) ボタンをクリックします。

   [Account Settings] (アカウント設定) タブが表示されます。

4. 必要に応じて設定を入力し、ユーザーの役割を選択します。

   > **注意:** アカウントを保存した後にユーザー名を変更することはできません。

5. **[Save]** (保存) をクリックします。

   Tenable Nessus がユーザーアカウントを保存します。

ユーザーアカウントを変更する

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Users]** (ユーザー) をクリックします。

   [Users] (ユーザー) ページが表示されます。

3. ユーザーテーブルで、修正するアカウントのユーザーをクリックします。

   <Username> ページが表示されます。<Username> には選択したユーザーの名前が入ります。

4. 必要に応じて、ユーザー名、メールアドレス、ロール、パスワードを変更します。

   > **注意:** アカウント作成後は、ユーザー名を変更できません。

   > **注意:** パスワードには Unicode 文字は使用できません。

5. **[Save]** (保存) をクリックします。

   Tenable Nessus により、アカウント設定が保存されます。

ユーザーアカウントを削除する

1. Tenable Nessus の上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Users]** (ユーザー) をクリックします。

   [Users] (ユーザー) ページが表示されます。

3. ユーザーテーブルの削除するユーザーの行で、✕ ボタンをクリックします。

   ユーザーを削除する選択でよいかを確認するダイアログボックスが表示されます。

4. **[Delete]** (削除) をクリックします。

   Tenable Nessus がユーザーを削除します。

ユーザーデータを転送する

Tenable Nessus Manager ではユーザーデータをシステム管理者に転送できます。ユーザーデータを転送すると、すべてのポリシー、スキャン、スキャン結果、プラグインルールの所有権がシステム管理者アカウント

に転送されます。ユーザーデータの転送は、ユーザーアカウントを削除する必要があり、Tenable Nessus 内の関連データを失いたくない場合に便利です。

ユーザーデータを転送する方法

1. ユーザーデータの転送先となるシステム管理者アカウントで Tenable Nessus にログインします。
2. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。
3. 左側のナビゲーションバーにある **[Accounts]** (アカウント) で **[Users]** (ユーザー) をクリックします。

   [Users] (ユーザー) ページが表示され、ユーザーテーブルを表示します。
4. ユーザーテーブルで、自分のアカウントにデータを転送するユーザーのチェックボックスをオンにします。
5. 右上隅にある **[Transfer Data]** (データを転送する) をクリックします。

   警告ウィンドウが表示されます。

   > **注意:** データを転送した後は、操作を取り消すことはできません。
6. データを転送するには、**[Transfer]** (転送) をクリックします。

   Tenable Nessus は、選択したユーザーのポリシー、スキャン、スキャン結果、プラグインルールの所有権を管理者アカウントに転送します。

追加のリソース

このセクションには、次のリソースが含まれています。

- プラグイン
- Amazon Web Service
- コマンドラインの操作
- NIAP に準拠する Tenable Nessus の設定
- 制限付きプラグインポリシーの作成
- デフォルトのデータディレクトリ
- ログを管理する
- Tenable Nessus 認証情報を使用したチェック
- オフライン更新ページの詳細
- 権限のないユーザーとして Tenable Nessus を実行する
- ターゲットのスキャン

Amazon Web Service

Tenable Nessus と Amazon Web Services の連携については、以下を参照してください。

- Amazon Web Services 上の Tenable Nessus BYOL スキャナー
- BYOL スキャナーを事前承認スキャナー機能でリンクする

証明書および認証局

Tenable Nessus には、以下のデフォルトが含まれます。

- `servercert.pem` および `serverkey.pem` という 2 つのファイルから成るデフォルトの Tenable Nessus SSL 証明書およびキー。
- デフォルトの Tenable Nessus SSL 証明書に署名する Tenable Nessus 認証局 (CA)。CA は `cacert.pem` と `cakey.pem` の 2 つのファイルで構成されます。

デフォルトの証明書ファイルは、ご使用のオペレーティングシステムに応じて、次のディレクトリにあります。

オペレーティングシステム	ディレクトリ
Windows	`C:\ProgramData\Tenable\Nessus\nessus\CA`
macOS	`/Library/Nessus/run/com/nessus/CA`
Linux	`/opt/nessus/com/nessus/CA`

しかし、詳細な設定やスキャンの問題を解決するには、ご自身の証明書または CA をアップロードする必要がある場合があります。詳細については、次を参照してください。

- カスタム SSL サーバー証明書 – Tenable Nessus SSL サーバー証明書の概要を表示し、証明書に関するよくある問題のトラブルシューティングを行います。
    - 新規サーバー証明書と CA 証明書を作成する– お客様固有の CA およびサーバー証明書をお持ちでない場合は、Tenable Nessus を使用して新しいサーバー証明書や CA の証明書を作成することができます。
    - 新規サーバー証明書と CA 証明書をアップロードします。– Tenable Nessus に同梱されているデフォルトの証明書を置き換えます。
- カスタム CA を信頼する – カスタムルート CA を Tenable Nessus が信頼する CA リストに追加します。
- ログイン用の Nessus SSL 証明書を作成する – Tenable Nessus にログインするために、ユーザー名とパスワードの代わりに、SSL クライアント証明書を作成します。
- Tenable Nessus Manager 証明書と Tenable Agent – Tenable Nessus Manager と Tenable Agents の特定の証明書チェーンを理解して、問題のトラブルシューティングを行います。

カスタム SSL サーバー証明書

デフォルトでは、Tenable Nessus は Tenable Nessus の認証局 (CA) である *Nessus Certification Authority* によって署名された SSL 証明書を使用します。Tenable Nessus のインストール時に、証明書を構成する 2 つのファイル (`servercert.pem` と `serverkey.pem`) が作成されます。この証明書によってポート 8834 を介して HTTPS 上から Tenable Nessus にアクセスすることが許可されます。

Nessus の認証局は信頼された有効な認証局ではないため、証明書は信頼されず、そのために以下が生じます。

- ポート 8834 を通じて HTTPS を介して Tenable Nessus にアクセスしようとすると、お使いのブラウザで安全でない接続として警告される可能性があります。
- Tenable Nessus スキャナーホストをスキャンする際に、プラグイン 51192 が脆弱性を報告する場合があります。

この問題を解決するには、企業または信頼できる CA より生成されたカスタム SSL 証明書を使用することができます。

カスタム SSL 証明書を使用するように Tenable Nessus を設定する手順については、以下を参照してください。

- 新規サーバー証明書と CA 証明書を作成する.– 企業より生成されたカスタム SSL 証明書がない場合、内蔵の Tenable Nessus `mkcert` ユティリティーを使用して作成します。
- 新規サーバー証明書と CA 証明書をアップロードします。 – Tenable Nessus に付属しているデフォルトの証明書を置き換えます。
- カスタム CA を信頼する – Tenable Nessus が信頼する CA リストにカスタム CA を追加します。

トラブルシューティング

Tenable Nessus でデフォルトの CA 証明書を使用する際の一般的な問題のトラブルシューティングについては、次の表を参照してください。

問題	ソリューション
ブラウザで Tenable Nessus サーバー証明書が信頼できないと表示される。	次のいずれかを行います。 • 信頼できるルート CA によって署名された Tenable Nessus 自己署名付きの証明書を入手し、その信頼できる CA をブラウザにアップロードします。 • `/getcert` パスを使用してルート CA をお使いのブラウザにインストールします。お使いのブラウザで次のアドレスにアクセスします : `https://[IP address]:8834/getcert` • お客様のカスタム証明書とカスタム CA をブラウザにアップロードします。 a. 新規サーバー証明書と CA 証明書をアップロードします。.

	b. その証明書の CA が Tenable Nessus で信頼されていない場合は、Tenable Nessus を カスタム CA を信頼する に設定します。 **注意:** これらの回避策は、一部のブラウザでは機能しません。Tenable は間もなく Tenable Nessus のアップデートを計画しており、すべてのブラウザが Tenable Nessus サーバー証明書を信頼するようにします。それまでの間、Tenable はサードパーティのカスタムサーバー証明書を使用することを推奨しています。
Plugin 51192 で Tenable Nessus サーバー証明書が信頼できないと表示される。 たとえば、次のようになります。 • 証明書の期限が切れている • 証明書が自己署名されているため信頼されない	次のいずれかを行います。 • Tenable Nessus のサーバー証明書を、既に Tenable Nessus によって信頼されている CA が署名した証明書に置き換えます。 • お客様のカスタム証明書とカスタム CA をブラウザにアップロードします。 a. 新規サーバー証明書と CA 証明書をアップロードします。. b. その証明書の CA が Tenable Nessus で信頼されていない場合は、Tenable Nessus を カスタム CA を信頼する に設定します。
プラグイン 51192 から証明書チェーンの先頭に不明な CA が見つかったと報告される。	カスタム CA を信頼する で説明している手順に従って、Tenable Nessus が信頼する CA のリストにカスタムルート CA を追加します。

新規サーバー証明書と CA 証明書を作成する

お客様固有のカスタム認証局 (CA) およびサーバー証明書 (たとえば、お客様の会社が使用する信頼できる証明書) をお持ちでない場合は、Tenable Nessus を使用して新しいサーバー証明書や CA の証明書を作成することができます。

このサーバー証明書は Tenable Nessus の CA によって署名されます。したがって、お客様のブラウザで信頼できないサーバー証明書として報告される可能性があります。

注意: 新しいカスタム CA とサーバー証明書を作成するには、管理者ユーザーであるか、root 権限を持っている必要があります。

注意: 以下の手順は、Tenable Nessus Manager スキャナーと Tenable Nessus の両方に適用されます。

新規カスタム CA とサーバー証明書を作成する方法

1. Tenable Nessus の CLI に管理者ユーザーまたは root 権限を持つユーザーとしてアクセスします。
2. `nessuscli mkcert` コマンドを実行します。

   Linux

   ```
   # /opt/nessus/sbin/nessuscli mkcert
   ```

   Windows

   ```
   C:\Program Files\Tenable\Nessus\nessuscli.exe mkcert
   ```

   macOS

   ```
   # /Library/Nessus/run/sbin/nessuscli mkcert
   ```

   このコマンドを実行することで、証明書が正しいディレクトリに配置されます。
3. ホスト名の入力を求められたら、ブラウザに https://hostname:8834/ または https://ipaddress:8834/ などの Tenable Nessus サーバーの DNS 名または IP アドレスを入力します。デフォルトの証明書はホスト名を使用しています。

次の手順

- Nessus の認証局は信頼された有効な認証局ではないため、証明書は信頼されず、そのために以下が生じます。
  - ポート 8834 を通じて HTTPS を介して Tenable Nessus にアクセスしようとすると、お使いのブラウザで安全でない接続として警告される可能性があります。

- Tenable Nessus スキャナーホストをスキャンする際に、プラグイン 51192 が脆弱性を報告する場合があります。

これらの問題のいずれも解決するには、カスタム CA を信頼する を行います。Tenable Nessus がカスタム SSL サーバー証明書および CA を使用する方法の詳細は、カスタム SSL サーバー証明書 を参照してください。

新規サーバー証明書と CA 証明書をアップロードします。

こちらの手順では、コマンドラインからカスタムサーバー証明書および認証局 (CA) 証明書を Nessus ウェブサーバーにアップロードする方法について説明します。

`nessuscli import-certs` コマンドを使用してサーバーキー、サーバー証明書、および CA 証明書を検証し、それぞれが一致することを確認し、適切な場所にファイルをコピーします。また、手動でファイルをコピーすることもできます。

始める前に

- 有効なサーバー証明書およびカスタム CA があることを確認します。カスタム CA およびサーバー証明書を内蔵の Tenable Nessus `mkcert` ユーティリティを利用して作成します (まだない場合)。

1 つのコマンドを使用して、カスタム CA 証明書をアップロードする方法

1. CLI から Tenable Nessus にアクセスします。
2. 以下を入力し、各ファイルについて、サーバーキー、サーバー証明書、CA 証明書を適切なパスおよびファイル名に置き換えます。

   ```
   nessuscli import-certs --serverkey=<server key path> --servercert=<server certificate path> --cacert=<CA certificate path>
   ```

   Tenable Nessus はファイルを検証し、一致することを確認し、適切な場所にコピーします。

CLI を使用して、手動でカスタムサーバー証明書と CA 証明書をアップロードする方法

1. Nessus サーバーを停止します。
2. オリジナルの Nessus CA、サーバー証明書、キーをバックアップします。

ヒント使用する オペレーティングシステムのデフォルトの証明書ファイルの場所については、[デフォルトの証明書ファイルは、ご使用のオペレーティングシステムに応じて、次のディレクトリにあります。](#)を参照してください。

Linux の例

```
cp /opt/nessus/com/nessus/CA/cacert.pem /opt/nessus/com/nessus/CA/cacert.pem.orig
cp /opt/nessus/var/nessus/CA/cakey.pem /opt/nessus/var/nessus/CA/cakey.pem.orig
cp /opt/nessus/com/nessus/CA/servercert.pem
/opt/nessus/com/nessus/CA/servercert.pem.orig
cp /opt/nessus/var/nessus/CA/serverkey.pem
/opt/nessus/var/nessus/CA/serverkey.pem.orig
```

Windowsの例

```
copy C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem.orig
copy C:\ProgramData\Tenable\Nessus\nessus\CA\cakey.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\cakey.pem.orig
copy C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem.orig
copy C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem.orig
```

macOS の例

```
cp /Library/NessusAgent/run/com/nessus/CA/cacert.pem
/Library/NessusAgent/run/com/nessus/CA/cacert.pem.orig
cp /Library/NessusAgent/run/var/nessus/CA/cakey.pem
/Library/NessusAgent/run/var/nessus/CA/cakey.pem.orig
cp /Library/NessusAgent/run/com/nessus/CA/servercert.pem
/Library/NessusAgent/run/com/nessus/CA/servercert.pem.orig
cp /Library/NessusAgent/run/var/nessus/CA/serverkey.pem
/Library/NessusAgent/run/var/nessus/CA/serverkey.pem.orig
```

3. オリジナルの証明書を新しいカスタム証明書に置き換えます。

注意: 証明書は復号してから、名前を `servercert.pem` および `serverkey.pem` にする必要があります。

注意: 証明書とルート証明書が直接リンクされていない場合、`serverchain.pem` という名前を付けた中間証明書チェーンを、`servercert.pem` ファイルと同じディレクトリに追加します。このファイルには、Nessus サーバーからその最上位のルート証明書 (ユーザーのブラウザが信頼する証明書) まで完全な証明書チェーンを構築するために必要な 1-n 中間証明書 (連結公開証明書) が含まれています。

Linux の例

```
cp customCA.pem /opt/nessus/com/nessus/CA/cacert.pem
cp cakey.pem /opt/nessus/var/nessus/CA/cakey.pem
cp servercert.pem /opt/nessus/com/nessus/CA/servercert.pem
cp serverkey.pem /opt/nessus/var/nessus/CA/serverkey.pem
```

Windowsの例

```
copy customCA.pem C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem
copy cakey.pem C:\ProgramData\Tenable\Nessus\nessus\CA\cakey.pem
copy servercert.pem C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem
copy serverkey.pem C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem
```

macOS の例

```
cp customCA.pem /Library/NessusAgent/run/com/nessus/CA/cacert.pem
cp cakey.pem /Library/NessusAgent/run/var/nessus/CA/cakey.pem
cp servercert.pem /Library/NessusAgent/run/com/nessus/CA/servercert.pem
cp serverkey.pem /Library/NessusAgent/run/var/nessus/CA/serverkey.pem
```

4. プロンプトされた場合は、既存ファイルを上書きします。
5. Tenable Nessus サーバーを起動します。
6. ブラウザで、Tenable Nessus ユーザーインターフェースに管理者アクセス許可を有するユーザーとしてログインします。

7. プロンプトされた場合は、新しい証明書の詳細を検証します。

   ブラウザが信頼している CA が証明書を生成した場合、それ以降の接続では警告は表示されません。

次の手順

- CA がまだ Tenable Nessus によって信頼されていない場合、Tenable Nessus を カスタム CA を信頼する に設定します。

カスタム CA を信頼する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Tenable Nessus は初期設定で、*Mozilla に含まれる CA 証明書*リストのルート証明書に基づき認証局 (CA) を信頼する設定になっています。Tenable Nessus は、Tenable Nessus ディレクトリにある `known_CA.inc` ファイルにある信頼できる CA を一覧表示します。Tenable はプラグインの更新時に `known_CA.inc` を更新します。

既知の CA に含まれていないカスタムルート CA を持っている場合、Tenable Nessus で証明書認証に使用するカスタム CA を信頼するように設定できます。

Tenable Nessus のユーザーインターフェースまたはコマンドラインインターフェース (CLI) のいずれかを使用できます。

注意: 特定の CA を信頼するように個々のスキャンを設定することもできます。詳細は、Trusted CAs (信頼できる CA)を参照してください。

注意: カスタム SSL 証明書の使用方法については、ログイン用の Nessus SSL 証明書を作成する を参照してください。

注意: `known_CA.inc` および `custom_CA.inc` は、ネットワークの証明書を信頼するために使用され、Nessus SSL 認証には使用されません。

始める前に

- お客様の会社にまだカスタム CA がない場合は、Tenable Nessus を使用して 新規サーバー証明書と CA 証明書を作成する の説明に従って、新しいカスタム CA およびサーバー証明書を作成し

ます。

- CA が PEM (Base64) フォーマットになるようにします。

Tenable Nessus ユーザーインターフェースを使ってカスタム CA を信頼するように Tenable Nessus を設定する方法

1. 上部のナビゲーションバーで、**[Settings]** (設定) をクリックします。

   [About] (製品情報) ページが表示されます。

2. 左側のナビゲーションバーで **[Custom CA]** (カスタム CA) をクリックします。

   [Custom CA] (カスタム CA) のページが表示されます。

3. **[Certificate]** (証明書) ボックスに、カスタム CA のテキストを入力します。

   > **注意:** 開始テキスト `-----BEGIN CERTIFICATE-----` と終了テキスト `-----END CERTIFICATE-----` を含めます。

   > **ヒント:** 1 つのテキストファイルに証明書を 1 つ以上保存することができます。それぞれについて、開始テキストと終了テキストを含めます。

4. **[Save]** (保存) をクリックします。

   これで、CA が Nessus で使用できるようになります。

CLI を使用してカスタム CA を信頼するように Tenable Nessus を設定する方法

1. PEM 形式の CA をテキストファイルとして保存します。

   > **注意:** 開始テキスト `-----BEGIN CERTIFICATE-----` と終了テキスト `-----END CERTIFICATE-----` を含めます。

   > **ヒント:** 1 つのテキストファイルに証明書を 1 つ以上保存することができます。それぞれについて、開始テキストと終了テキストを含めます。

2. ファイル名を `custom_CA.inc` に変更します。

3. ファイルをお使いのプラグインディレクトリに移動します。

   Linux

```
/opt/nessus/lib/nessus/plugins
```

Windows

```
C:\ProgramData\Tenable\Nessus\nessus\plugins
```

macOS

```
/Library/Nessus/run/lib/nessus/plugins
```

これで、CA が Nessus で使用できるようになります。

ログイン用の Nessus SSL 証明書を作成する

ポート 8834 で Tenable Nessus にアクセスする際に、SSL クライアント証明書認証を使用してユーザーが Tenable Nessus にログインできるよう、Tenable Nessus を設定することができます。証明書認証を有効にすると、ユーザー名とパスワードを使用したログインはできなくなります。

警告: SSL クライアント証明書認証を有効にすると、Tenable Nessus でエージェント、リモートスキャナー、または管理スキャナーの接続がサポートされなくなります。リモートエージェントおよびスキャナーのサポートを有効化するには、詳細設定の `remote_listen_port` を使用して代替ポートを設定してください。詳細は、詳細設定を参照してください。

SSL クライアント証明書認証を設定した場合、Tenable Nessus は以下もサポートします。

- スマートカード
- 本人確認 (PIV) カード
- 共通アクセスカード (CAC)

Tenable Nessus ユーザーアカウントの SSL クライアント証明書認証を設定する方法

1. Tenable Nessus の CLI に管理者ユーザーまたは同等の権限を持つユーザーとしてアクセスします。
2. Tenable Nessus に SSL 認証を介してログインする必要のある各ユーザーについて、クライアント証明書を作成します。

a. Tenable Nessus サーバーで、`nessuscli mkcert-client` コマンドを実行します。

Linux

```
# /opt/nessus/sbin/nessuscli mkcert-client
```

macOS

```
# /Library/Nessus/run/sbin/nessuscli mkcert-client
```

Windows

```
C:\Program Files\Tenable\Nessus\nessuscli.exe mkcert-client
```

b. プロンプトに従ってフィールドに入力します。

> **注意:** 同セッション中に、初回プロンプトに入力した回答がその後のクライアント証明書を作成するときのデフォルトとして残ります。作成したそれぞれのクライアント証明書の値は変更が可能です。

Tenable Nessus は、クライアント証明書を作成し、Tenable Nessus の一時ディレクトリに配置します。

- Linux: `/opt/nessus/var/nessus/tmp/`
- macOS: `/Library/Nessus/run/var/nessus/tmp/`
- Windows: `C:\ProgramData\Tenable\Nessus\tmp`

c. 2 つのファイル (証明書およびキー) を統合し、ブラウザにインポートできる形式 (`.pfx` など) でエクスポートします。

前の例では、2 つのファイルは *`key_sylvester`*`.pem` および *`cert_sylvester.pem`* でした。

たとえば 2 つのファイルは、`openssl` プログラムや、次のコマンドを使用して統合することができます。

```
# openssl pkcs12 -export -out combined_sylvester.pfx -inkey key_sylvester.pem
-in cert_sylvester.pem -chain -CAfile /opt/nessus/com/nessus/CA/cacert.pem -
passout 'pass:password' -name 'Nessus User Certificate for: sylvester'
```

Tenable Nessus は、コマンドを起動したディレクトリに、結果の `combined_sylvester.pfx` ファイルを作成します。

3. 証明書をブラウザの個人用証明書ストアにアップロードします。

   お使いのブラウザのドキュメントを参照してください。

4. Tenable Nessus で SSL クライアント証明書認証を許可するよう設定します。

   Linux

   ```
   # /opt/nessus/sbin/nessuscli fix --set force_pubkey_auth=yes
   ```

   Windows

   ```
   C:\Program Files\Tenable\Nessus\nessuscli.exe fix --set force_pubkey_
   auth=yes
   ```

   macOS

   ```
   # /Library/Nessus/run/sbin/nessuscli fix --set force_pubkey_auth=yes
   ```

5. `https://<Tenable Nessus の IP アドレスまたはホスト名>:8834` で Tenable Nessus にログインし、作成したユーザー名を選択します。

次の手順

- カスタム CA を使用している場合、カスタム CA を信頼するの説明に従って、Tenable Nessus プラグインでお客様の CA が発行する証明書を信頼するよう設定します。

Tenable Nessus Manager 証明書と Tenable Agent

エージェントを Tenable Nessus Manager にリンクすると、エージェントが Tenable Nessus Manager にリンクする際に使用するべき証明書をオプションで指定できます。これによってエージェントが Tenable Nessus Manager とリンクする際に、Tenable Nessus Manager からのサーバー証明書を検証することができ、その後のエージェントと Tenable Nessus Manager の間の通信を安全に行うことができます。Tenable Agent へのリンクの詳細については、Nessuscli を参照してください。

リンク時に、認証局 (CA) の証明書を指定しない場合、リンクされた Tenable Nessus Manager から CA 証明書を受け取り、信頼します。これによりその後のエージェントと Tenable Nessus Manager の通信を安全に行うことができます。

注意: Tenable Nessus Manager 証明書に自己署名証明書または信頼できない証明書を使用する場合、その証明書はリンク先のエージェントによって信頼される必要があります。信頼されていない場合、エージェントと Tenable Nessus Manager との接続が失われます。詳細は、カスタム CA を信頼するを参照してください。

リンク時にエージェントが受け取る CA 証明書は次の場所に保存されます。

Linux

```
/opt/nessus_agent/var/nessus/users/nessus_ms_agent/ms_cert.pem
```

Windows

```
C:\ProgramData\Tenable\Nessus Agent\nessus\users\nessus_ms_agent\ms_cert.pem
```

macOS

```
/Library/NessusAgent/run/var/nessus/users/nessus_ms_agent/
```

トラブルシューティング

エージェントが完全な証明チェーンをたどれない場合は、エラーが発生しエージェントはマネージャーとの接続を停止します。このようなイベントの例は、以下のセンサーログに表示されます。

- **nessusd.messages** - 例: Server certificate validation failed: unable to get local issuer certificate
- **backend.log** - 例:[error] [msmanager] SSL error encountered when negotiating with <Manager_IP>:<PORT>.Code 336134278, unable to get local issuer certificate, error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed

シナリオ: 証明書チェーンが壊れているためエージェントがマネージャーと通信できない

証明書チェーンが壊れる原因としてよくあるのは、Tenable Nessus Manager のサーバー証明書を変更したものの、CA 証明書を更新していないことです。この場合、エージェントは、再起動後にマネージャーと通信できなくなります。この問題を解決するには、以下の中から 1 つを実行してください。

- エージェントと Tenable Nessus Manager のリンクを解除して、再度リンクします。そうすることで証明書がリセットされ、エージェントが Tenable Nessus Manager から適切な CA 証明書を受け取る

ようになります。

- また、`cacert.pem` ファイルを Tenable Nessus Manager から手動でアップロードし、エージェントのプラグインディレクトリの `custom_CA.inc` ファイルにロードすることもできます。

  - **Linux**

    `/opt/nessus_agent/lib/nessus/plugins`

  - **Windows**

    `C:\ProgramData\Tenable\Nessus Agent\nessus\plugins`

  - **macOS**

    `/Library/NessusAgent/run/lib/nessus/plugins`

- エージェントがすでに CA 証明書を持っている CA を使用して新しいサーバー証明書を Tenable Nessus Manager 上に生成し、証明書チェーンがまだ有効であるようにします。

コマンドラインの操作

このセクションでは、Tenable Nessus および Tenable Agents でのコマンドラインの操作について説明します。

ヒント: コマンドラインの操作中に表示される、パスワードなどの秘密情報の入力を求めるプロンプトでは、入力した文字が表示されません。ただし、コマンドラインにはデータが記録されており、**[Enter]** (入力) キーを押すとそのデータが受け入れられます。

このセクションは以下のトピックで構成されています。

- Tenable Nessus の開始または停止
- Tenable Agent の開始または停止
- Nessus のサービス
- Nessuscli
- Nessuscli Agent
- Tenable Nessus ソフトウェアを更新する (CLI)

Tenable Nessus の開始または停止

次に、マシンの Nessus サービスの開始と停止の方法を示します。

注意: このトピックでは、ホストマシンで実行される Nessus サービスの開始または停止について取り上げています。個々のスキャンの開始または停止については、スキャンの起動 および 実行中のスキャンの停止 を参照してください。

Windows

1. **[Services]** (サービス) に移動します。
2. **[Name]** (名前) 列で **[Tenable Nessus]** をクリックします。
3. 次のいずれかを行います。
    - **Nessus** のサービスを終了するには、**[Tenable Nessus]** を右クリックしてから **[Stop]** (停止) をクリックします。
    - **Nessus** のサービスを再起動するには、**[Tenable Nessus]** を右クリックしてから **[Start]** (開始) をクリックします。

開始または停止	Windows コマンドライン操作
開始	`C:\Windows\system32>net start "Tenable Nessus"`
停止	`C:\Windows\system32>net stop "Tenable Nessus"`

注意: 開始および停止コマンドを実行するには、root 権限が必要です。

Linux

次のコマンドを使用します。

開始または停止	Linux コマンドライン操作
Red Hat、CentOS、Oracle Linux	
開始	`# systemctl start nessusd`

開始または停止	Linux コマンドライン操作
終了	`# systemctl stop nessusd`
SUSE	
開始	`# systemctl start nessusd`
終了	`# systemctl stop nessusd`
Debian、Kali、Ubuntu	
開始	`# systemctl start nessusd`
終了	`# systemctl stop nessusd`

注意: 開始および停止コマンドを実行するには、root 権限が必要です。

macOS

1. **[System Preferences]** (システム環境設定) に移動します。
2. 🔘 ボタンをクリックします。
3. 🔒 ボタンをクリックします。
4. ユーザー名とパスワードを入力します。
5. 次のいずれかを行います。
    - Nessus のサービスを停止するには、**[Stop Nessus]** (Nessus の停止) ボタンをクリックします。
    - Nessus のサービスを開始するには、**[Start Nessus]** (Nessus の開始) ボタンをクリックします。

開始または停止	macOS コマンドライン操作
開始	`# sudo launchctl start com.tenablesecurity.nessusd`
停止	`# sudo launchctl stop com.tenablesecurity.nessusd`

注意: 開始および停止コマンドを実行するには、root 権限が必要です。

Tenable Agent の開始または停止

以下のセクションで、ホストで Tenable Agent を開始および停止する際のベストプラクティスを説明します。

Windows

1. **[Services]** (サービス) に移動します。
2. **[Name]** (名前) 列で **[Tenable Nessus Agent]** をクリックします。
3. 次のいずれかを実行します。

    - エージェントのサービスを停止するには、**[Tenable Nessus Agent]** を右クリックしてから **[Stop]** (停止) をクリックします。

    - エージェントのサービスを再起動するには、**[Tenable Nessus Agent]** を右クリックしてから **[Start]** (開始) をクリックします。

または、次のコマンドを使用して、コマンドラインからエージェントを開始したり停止したりすることもできます。

開始または停止	Windows コマンドライン操作
開始	`C:\Windows\system32>net start "Tenable Nessus Agent"`
停止	`C:\Windows\system32>net stop "Tenable Nessus Agent"`

Linux

Linux システムでエージェントを開始または停止するには、次のコマンドを使用します。

開始または停止	Linux コマンドライン操作
開始	`# systemctl start nessusagent`
終了	`# systemctl stop nessusagent`

macOS

1. **[System Settings]** (システム設定) に移動します。
2. ボタンをクリックします。
3. ボタンをクリックします。
4. ユーザー名とパスワードを入力します。
5. 次のいずれかを実行します。

    - エージェントのサービスを停止するには、**[Stop Nessus Agent]** (Nessus Agent の停止) ボタンをクリックします。

    - エージェントのサービスを開始するには、**[Start Nessus Agent]** (Nessus Agent の開始) ボタンをクリックします。

または、次のコマンドを使用して、コマンドラインからエージェントを開始したり停止したりすることもできます。

開始または停止	macOS コマンドライン操作
開始	`# sudo launchctl start com.tenablesecurity.nessusagent`
停止	`# sudo launchctl stop com.tenablesecurity.nessusagent`

Nessus のサービス

可能な限り、オペレーティングシステムのインターフェースの Tenable Nessus サービス制御を使用して、Tenable Nessus サービスを開始および停止する必要があります。

ただし、コマンドラインインターフェースで実行できる **nessus-service** 機能も多数あります。

特に記載がない限り、**nessusd** コマンドと **nessus-service** サーバーコマンドは互換可能です。

 # killall nessusd コマンドを使用して、Tenable Nessus のすべてのサービスと実行中のスキャンを停止できます。

> **注意:** 次のコマンドを実行するには、管理者権限が必要です。

Nessus のサービス構文

オペレーティングシステム	コマンド
Linux	# /opt/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
macOS	# /Library/Nessus/run/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]

Nessusd のコマンド

オプション	説明
-c <config-file>	nessusd サーバーを起動するとき、このオプションはサーバー側で使用される nessusd 設定ファイルを指定します。標準 db の代わりに代替設定ファイルの使用が可能です。
-S <ip [,ip2,...]>	nessusd サーバーを起動するとき、このオプションはスキャン中に Tenable Nessus のソース IP を指定します。この設定は、スキャンターゲット IP アドレスではなく、Tenable Nessus をホストするデバイスのソース IP アドレスに関連します。 このオプションは、デフォルトの IP アドレスの代わりに複数のパブリック IP アドレスを使用するマルチホーム型マシンを所有する場合にのみ有用です。この設定が機能するには、nessusd を実行するホストに、これらの IP アドレスが設定された複数の NIC が必要です。
-D	nessusd サーバーを起動するとき、このオプションはサーバーを強制的にバックグラウンドで実行します (daemon モード)。
-v	バージョン番号を表示して終了します。
-l	サードパーティ製ソフトウェアのライセンスリストが表示されます。
-h	コマンドの要約を表示し、終了します。
--ipv4-only	IPv4 ソケットでのみリッスンします。
--ipv6-only	IPv6 ソケットでのみリッスンします。
-q	「quiet」モードで作動し、すべてのメッセージを stdout に抑制します。

オプション	説明
-R	プラグインの再処理を強制します。
-t	開始時に各プラグインのタイムスタンプをチェックして、新たに更新されるプラグインのみをコンパイルします。
-K	スキャナー用の親パスワードを設定します。 親パスワードが設定されている場合、Tenable Nessus ではポリシーに含まれるすべてのポリシーと認証情報が暗号化されます。パスワードが設定されている場合、Tenable Nessus ユーザーインターフェースからパスワードの入力を促されます。 **警告:** 親パスワードを設定して紛失した場合、管理者も Tenable サポートもパスワードを回復することはできません。

コマンド出力データを抑制する例

コマンド出力は **-q** オプションを使用して抑制できます。たとえば、次のようになります。

```
# /opt/nessus/sbin/nessus-service -q -D
```

考慮事項

nessusd をゲートウェイで実行していて、nessusd に外部者が接続しないようにする場合は、listen_address 詳細設定を行います。

この設定を行うには、次のコマンドを実行します。

```
nessuscli fix --set listen_address=<IP address>
```

この設定により、アドレス *<IP address>* (マシン名でなく IP アドレス) での接続のみをリッスンするようにサーバーに指示します。

Nessuscli

Tenable Nessus 機能の一部は、nessuscli ユーティリティを使用して、コマンドラインインターフェース (CLI) で管理できます。

これを使用して、ユーザーアカウントの管理、詳細設定の変更、デジタル証明書の管理、バグの報告、Tenable Nessus の更新、必要なライセンス情報の取得を行うことができます。

> **注意:** コマンドはすべて管理者権限で実行する必要があります。

Nessuscli の構文

オペレーティングシステム	コマンド
Windows	`C:\Program Files\Tenable\Nessus\nessuscli.exe <cmd> <arg1> <arg2>`
macOS	`# /Library/Nessus/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Linux	`# /opt/nessus/sbin/nessuscli <cmd> <arg1> <arg2>`

このトピックでは、次のコマンドタイプについて説明します。

- ヘルプコマンド
- バックアップコマンド
- バグレポートコマンド
- ユーザーコマンド
- Fetch コマンド
- 修正コマンド
- 証明書コマンド
- ソフトウェア更新コマンド
- 管理ツールコマンド
- 管理対象スキャナーコマンド
- Dump Command
- Node Commands

Nessuscli のコマンド

コマンド	説明
ヘルプコマンド	
`nessuscli help`	Tenable Nessus コマンドのリストを表示します。 help の出力は Tenable Nessus ライセンスによって異なる場合があります。
`nessuscli <cmd> help`	nessuscli help の出力結果に表示された特定のコマンドに関する詳細なヘルプ情報を表示します。
バックアップコマンド	
`nessuscli backup --create <backup_filename>`	使用しているライセンスと設定を含む、Tenable Nessus インスタンスのバックアップファイルを作成し、*<Unix epoch timestamp>.tar.gz* に加えます。このコマンドではスキャン結果はバックアップされません。 例: `nessuscli backup --create <december-backup>` を実行すると、Tenable Nessus は次のバックアップファイルを作成します: *december-backup.1671720758.tar.gz*。 詳細は、Tenable Nessus のバックアップ を参照してください。
`nessuscli backup --restore <path/to/backup_filename>`	Tenable Nessus の以前に保存されたバックアップを復元します。 詳細は、Tenable Nessus の復元を参照してください。
バグレポートコマンド バグレポートコマンドは、問題の診断に役立つ Tenable, Inc. を送信できるアーカイブを作成します。スクリプトはデフォルトではインタラクティブモードで実行されます。	
`nessuscli bug-report-generator`	システム診断のアーカイブを作成します。 引数を指定せずにこのコマンドを実行すると、値を求められます。 `--quiet` ：ユーザーにフィードバックを求めることなく、バグレポートジェネレーターが実行されます。

コマンド	説明
	`--scrub` ：quiet モード時に、バグレポートジェネレーターによって IPv4 アドレスの最後の 2 つの 8 ビットがサニタイズされます。 `--full` ：quiet モード時に、バグレポートジェネレーターによって追加データが収集されます。
ユーザーコマンド	
`nessuscli rmuser <username>`	Tenable Nessus ユーザーを削除できます。
`nessuscli chpasswd <username>`	ユーザーのパスワードを変更できます。Tenable Nessus ユーザーの名前を入力するプロンプトが CLI に表示されます。パスワードが CLI の画面にエコー表示されることはありません。
`nessuscli adduser <username>`	Tenable Nessus のユーザーアカウントを追加できます。 CLI から、ユーザー名、パスワードの入力、ユーザーに管理者タイプのアカウントの保有を許可するかどうかの選択を求められます。また、この新しいユーザーアカウントにユーザールールを追加することも求められます。 **注意:** Tenable Nessus Manager インスタンスでこのコマンドを使用して初めてユーザーを作成する場合、Tenable では、ユーザーインターフェースが新しいユーザーの情報で適切に更新されるように、Tenable Nessus を再起動することを推奨しています。
`nessuscli lsuser`	Tenable Nessus ユーザーのリストを表示します。
Fetch コマンド **Tenable Nessus 登録を管理し、更新プログラムを取得する**	
`nessuscli fetch --register <Activation Code>`	アクティベーションコードを使用して Tenable Nessus をオンライン登録します。 例: `# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx-xxxx`

コマンド	説明
`nessuscli fetch --register-only <Activation Code>`	アクティベーションコードを使用して、Tenable Nessus をオンライン登録しますが、プラグインや中核的な更新プログラムは自動的にダウンロードされません。 例: `# /opt/nessus/sbin/nessuscli fetch --register-only xxxx-xxxx-xxxx-xxxx`
`nessuscli fetch --register-offline nessus.license`	https://plugins.nessus.org/v2/offline.php から入手した nessus.license ファイルを使用して Tenable Nessus を登録し、。
`nessuscli fetch --check`	Tenable Nessus が適切に登録されているかどうかと、更新プログラムを入手可能かどうかが表示されます。
`nessuscli fetch --code-in-use`	Tenable Nessus で使用されている Nessus アクティベーションコードが表示されます。
`nessuscli fetch --challenge`	オフライン登録の実行時に使用する必要のあるチャレンジコードが表示されます。 チャレンジコードの例: aaaaaa11b2222cc33d44e5f6666a777b8cc99999
`nessuscli fetch --security-center`	Tenable Security Center に接続されるように Tenable Nessus を準備します。 **警告:** *Tenable Nessus インスタンスを Tenable Security Center に切り替えたくない場合は、このコマンドを使用しないでください。*このコマンドは、Tenable Nessus スキャナーまたは Manager を Tenable Security Center 管理スキャナーに不可逆的に変更します。その結果、ユーザーインターフェースに複数の変更が加えられます (たとえば、サイトのロゴが変更されたり、**[Sensors]** (センサー) ページにアクセスできなくなったりします)。
修正コマンド	

コマンド	説明
`nessuscli fix`	登録のリセット、ネットワークインターフェースの表示、設定されている詳細設定の一覧表示を行います。 `--secure` オプションを選択すると、登録関連情報が含まれる暗号化の環境設定に影響が及びます。 `--list`、`--set`、 `--get`、`--delete` コマンドを使用して、環境設定を変更したり、表示したりできます。
`nessuscli fix [--secure] --list`	
`nessuscli fix [--secure] --set <setting=value>`	
`nessuscli fix [--secure] --get <setting>`	
`nessuscli fix [--secure] --delete <setting>`	
`nessuscli fix --list-interfaces`	使用中のマシンに接続されているネットワークアダプターが一覧表示されます。
`nessuscli fix --set listen_address=<address>`	アドレス `<address>` (マシン名でなくIP) での接続のみをリッスンするように指示するために使用します。このオプションは、nessusd をゲートウェイで実行している場合や nessusd に外部者が接続しないようにする場合に有用です。
`nessuscli fix --show`	すべての詳細設定を、設定していないものも含めて表示します。詳細設定を設定していない場合は、CLI にデフォルト値が表示されます。 **注意:** このコマンドは、すべての Tenable Nessus ライセンスタイプで共有されている設定だけをリストします。つまりこのコマンドは、Tenable Nessus Expert、Tenable Nessus Professional、Tenable Nessus Manager に固有の設定をリストしません。
`nessuscli fix --reset`	このコマンドにより、すべての登録情報と環境設定が削除され、Tenable Nessus は登録されていない状態で実行されます。Tenable Nessus Manager ではリセット後も同じリンクキーが保持されます。 `nesuscli fix --reset` を実行する前に、実行中のスキャンが完了

コマンド	説明
	したことを確認し、Tenable Nessus の開始または停止 で説明したようにessusddaemonまたはservice を停止します。
`nessuscli fix --reset-all`	Tenable Nessus が初期状態にリセットされ、すべての登録情報、設定、データ、ユーザーが削除されます。 **警告**：この操作を取り消すことはできません。完全リセットを実行する前に、Tenable サポート に連絡してください。
`nessuscli fix --set agent_update_channel=<value>`	(Tenable Nessus Manager にリンクされたエージェントのみ) エージェント更新プランを設定して、エージェントが自動的に更新するバージョンを指定します。 値 • **ga** – 最新バージョンが一般公開 (GA) され次第、自動的に最新の Tenable Agent バージョンに更新されます。 • **ea** - 最新バージョンが早期アクセス (EA) 用にリリースされ次第、自動的に最新の Tenable Nessus バージョンへと更新します。通常一般公開よりも数週間早いタイミングです。 • **`stable`** - 自動的に最新の Tenable Nessus バージョンに更新しません。Tenable が設定した旧バージョンの Tenable Nessus の状態を維持します。これは通常、最新の一般公開バージョンよりも 1 リリース前のものとなりますが、8.10.0 よりも前のバージョンにはなりません。Tenable Nessus の新しいバージョンがリリースされると、Tenable Nessus インスタンス のソフトウェアバージョンは更新されますが、最新のリリースよりも前のバージョンに留まります。 **注意**: Tenable Nessus Manager にリンクされているエージェントの場合は、Tenable Nessus Manager `nessuscli` ユーティリティから `agent_update_channel` コマンドを実行する必要があります。Tenable Vulnerability Management にリンクされているエージェントの場合は、エージェントの `nessuscli` ユーティリティから `agent_update_channel` コマンドを実行する必要があります。

コマンド	説明
`nessuscli fix --secure --get agent_linking_key`	一意のエージェントリンクキーを取得します。 **注意:** このリンクキーは、エージェントをリンクする目的でのみ使用できます。スキャナーまたは子ノードとのリンクには使用できません。
`nessuscli fix --secure --get child_node_linking_key`	一意の子ノードリンクキーを取得します。 **注意:** このリンクキーは、子ノードをリンクする目的でのみ使用できます。エージェントまたはスキャナーとのリンクには使用できません。
`nessuscli fix --secure --get scanner_linking_key`	一意のスキャナーリンクキーを取得します。 **注意:** このリンクキーは、スキャナーをリンクする目的でのみ使用できます。エージェントまたは子ノードとのリンクには使用できません。
`nessuscli fix --set niap_mode=enforcing`	Tenable Nessus に NIAP モードを適用します。NIAP モードの詳細については、NIAP に準拠する Tenable Nessus の設定 を参照してください。
`nessuscli fix --set niap_mode=non-enforcing`	Tenable Nessus の NIAP モードを無効にします。NIAP モードの詳細については、NIAP に準拠する Tenable Nessus の設定 を参照してください。
`nessuscli fix --set fips_mode=enforcing`	Tenable Nessus 通信およびデータベース暗号化に対して最新の検証済み FIPS モジュールを適用します。FIPS モジュールはスキャン暗号化に影響しません。 **注意:** NIAP モードを適用すると、Tenable Nessus は FIPS モジュールも適用します。詳細は、NIAP に準拠する Tenable Nessus の設定を参照してください。
`nessuscli fix --set fips_mode=non-enforcing`	Tenable Nessus 通信およびデータベース暗号化に対して FIPS モジュールを無効にします。 **注意:** NIAP モードを無効にすると、Tenable Nessus は FIPS モジュールも無効にします。詳細は、NIAP に準拠する Tenable Nessus の設定を参照してください。

コマンド	説明
`nessuscli fix --set path_to_java=<custom file path>`	PDF エクスポート用の Java へのカスタムファイルパスを設定します。設定しない場合、Tenable Nessus はシステムパスを使います。 Java バイナリを含む絶対ファイルパスを使用する必要があります。たとえば、Tenable Nessus のインストールが `/usr/lib/jvm/java-17-openjdk-amd64` にある場合、カスタムファイルのパスは **`/usr/lib/jvm/java-17-openjdk-amd64/bin`** にする必要があります。
`nessuscli fix --set old_user_files_cleanup_hours=`	Tenable Nessus が古いユーザーファイル (`/nessus/users/<ユーザー>/files` ディレクトリ内) を削除するまでの時間間隔 (1 時間単位) を設定します。この設定は、ユーザーファイルが多すぎることが原因で生じるスキャンエラーに対処する際に活用できます。 この設定のデフォルトおよび最小値は **0** です。この設定に最大値はありません。設定がゼロに設定されている場合、Tenable Nessus はファイルのクリーンアップを実行しません。
`nessuscli fix --set <password_setting>=<value>`	ユーザーパスワードのパラメーターと制限を設定します。このコマンドを使用して、次の設定を編集できます。 • **パスワードの複雑さ** (`passwd_complexity`) - Tenable Nessus パスワードが 8 文字以上で、大文字、小文字、特殊文字、数字から 3 種類以上を使用する必要があるかどうかを決定します。この設定はデフォルトではオフになっています。 • **セッションタイムアウト** (`xmlrpc_idle_session_timeout`) - ウェブセッションのタイムアウトを分単位で定義します。セッションのアイドル時間がこのタイムアウトの値を超えると、Tenable Nessus はユーザーを自動的にログアウトさせます。この設定はデフォルトで 30 に設定されています。 • **最大ログイン試行** (`user_max_login_attempt`) - アプリケーションがアカウントをロックアウトするまでに Tenable Nessus で許可される、ユーザーの最大ログイン試行回数を定義します。この値をゼロに設定すると、機能は無効になります。この設定はデフォルトで 5 に設定されています。

コマンド	説明
	• **最小パスワード長** (`min_password_len`) - この設定は、デフォルトで 8 に設定されています。アカウントのパスワードの最小文字数を定義します。 • **ログイン通知** (`passwd_notifications`) - Tenable Nessus がログイン通知を表示できるかどうかを決定します。ログイン通知を使用すると、最後に成功したログインと失敗したログイン (日付、時刻、IP)、また最後に成功したログイン以降に失敗したログインがあるかどうかを確認できます。この設定はデフォルトではオフになっています。 **注意:** パスワード設定を行うには、システム管理者ロールが必要です。詳細は、ユーザーTenable Nessus Managerを参照してください。 **ヒント:** これらの設定は、**[Password Management]** (パスワード管理) ページで管理することもできます。各パスワード設定のデフォルト値と有効な値を確認するには、パスワード管理をご覧ください。
証明書コマンド	
`nessuscli mkcert-client`	Tenable Nessus サーバー向けの証明書を作成します。
`nessuscli mkcert [-q]`	デフォルトの値で証明書を作成します。 `-q` は静かに作成します。
`nessuscli import-certs --serverkey=<server key path> --servercert=<server certificate path> --cacert=<CA certificate path>`	サーバーキー、サーバー証明書、および CA 証明書を検証し、一致することを確認します。その後、ファイルを正しい場所にコピーします。

コマンド	説明
ソフトウェア更新コマンド	
`nessuscli update`	デフォルトでは、このツールは、Tenable Nessus のユーザーインターフェースで選択されたソフトウェアの更新オプションに基づいて更新を行います。 **注意**: このコマンドは、スタンドアロンの Tenable Nessus スキャナーでのみ機能します。このコマンドは、Tenable Vulnerability Management または Tenable Security Center によって管理されるスキャナーに対しては機能しません。
`nessuscli update --all`	Tenable Nessus の全コンポーネントに更新プログラムを適用します。 **注意**: このコマンドは、スタンドアロンの Tenable Nessus スキャナーでのみ機能します。このコマンドは、Tenable Vulnerability Management または Tenable Security Center によって管理されるスキャナーに対しては機能しません。
`nessuscli update --plugins-only`	Tenable Nessus のプラグインのみに更新プログラムを強制的に適用します。 **注意**: このコマンドは、スタンドアロンの Tenable Nessus スキャナーでのみ機能します。このコマンドは、Tenable Vulnerability Management または Tenable Security Center によって管理されるスキャナーに対しては機能しません。
`nessuscli update <tar.gz filename>`	プラグインフィードから更新プログラムを取得する代わりに、TAR ファイルを使用して Tenable Nessus のプラグインを更新します。TAR ファイルは、Tenable Nessus をオフラインで管理する ~ Download and Copy Pluginsの手順で取得します。
`nessuscli fix --set scanner_update_channel=<value>`	(Tenable Nessus Professional および Tenable Vulnerability Management 管理スキャナーのみ) Tenable Nessusを設定して、Tenable Nessus が自動的にアップデートするバージョンを指定します。 **注意**：更新プランを変更して自動更新を有効にすると、選択したプラン

コマンド	説明
	に相当するバージョンと合わせるために、Tenable Nessus が即座に更新する場合があります。Tenable Nessus はバージョンのアップグレードまたはダウングレードのいずれかを行う場合があります。 値: • **ga** - 最新バージョンが一般公開 (GA) され次第、自動的に最新の Tenable Nessus バージョンへと更新されます。**注意:** この日付はバージョンが一般公開された日と同じ日付です。 • **ea** - 最新バージョンが早期アクセス (EA) 用にリリースされ次第、自動的に最新の Tenable Nessus バージョンへと更新します。通常一般公開よりも数週間早いタイミングです。 • **stable** - 自動的に最新の Tenable Nessus バージョンに更新しません。Tenable が設定した旧バージョンの Tenable Nessus の状態を維持します。これは通常、最新の一般公開バージョンよりも 1 リリース前のものとなりますが、8.10.0 よりも前のバージョンにはなりません。Tenable Nessus の新しいバージョンがリリースされると、Tenable Nessus インスタンスのソフトウェアバージョンは更新されますが、最新のリリースよりも前のバージョンに留まります。
管理ツールコマンド 管理ツールに接続されている管理対象スキャナーとエージェントのプラグイン更新プログラムを生成するために使用されます。	
`nessuscli manager download-core`	リモート管理されるエージェントとスキャナー用コアコンポーネントの更新プログラムがダウンロードされます。
`nessuscli manager generate-plugins`	リモート管理されるエージェントとスキャナー用のプラグインアーカイブが生成されます。
管理対象スキャナーコマンド リモート管理されるスキャナーをリンクする、リンク解除する、ステータスを表示するために使用します。	
`nessuscli managed`	nessuscli-managed コマンドおよび構文を表示します。

コマンド	説明
`help`	
`nessuscli managed link --key=<key> --host=<host> --port=<port> [オプションのパラメーター]`	未登録のスキャナーをマネージャーにリンクします。 **注意:** スキャナーをすでに登録している場合は、CLI を介してスキャナーをリンクできません。ユーザーインターフェースからリンクするか、スキャナーをリセットして登録を解除できます (ただし、スキャナーデータはすべて失われます)。 **オプションのパラメーター** • `--name` – スキャナーの名前。 • `--ca-path` – Manager のサーバー証明書の検証に使用するカスタム CA 証明書。 • `--groups` – スキャナーを追加する、1 つ以上の既存のスキャナーグループ。コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。 例: `--groups="Atlanta,Global Headquarters"` **注意**: スキャナーグループ名は、大文字と小文字を区別し、正確に一致する必要があります。 • `--proxy-host` - プロキシサーバーのホスト名または IP アドレス。 • `--proxy-port` – プロキシサーバーのポート番号。 • `--proxy-username` – プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。 • `--proxy-password` - ユーザー名として指定したユーザーアカウントのパスワード。 • `--proxy-agent` - プロキシに事前定義されたユーザーエージェントが必要とされる場合のユーザーエージェント名。

コマンド	説明
	• `--aws-scanner` - Tenable Nessus スキャナーが事前認証された AWS スキャナー機能とリンクすることを示します。 事前認証 AWS スキャナーが Tenable Nessus スキャナーとは異なる点は、**ターゲット**または**ターゲットのアップロード**のスキャン設定オプションを提供していないことです。代わりに、[Select Targets] (ターゲットの選択) ボタンを提供します。 **[Select Targets]** (ターゲットの選択) をクリックして AWS IMDSv2 にクエリを実行し、表示可能なネットワークターゲットのリストを新しいページに生成します。このページを使用して、スキャンする AWS ターゲットを選択し、**[Confirm]** (確認) をクリックします。 **注意:** このオプションは、Tenable Nessus スキャナーが AWS インスタンスですでに実行されていないと有効になりません。 **注意:** `--aws_scanner` は、Amazon Linux 2023 AMI 環境ではサポートされていません。 **警告:** 事前認証された AWS スキャナー機能と Tenable Nessus をリンクする場合にのみ、`--aws-scanner` パラメーターを含めてください。
`nessuscli managed unlink`	管理対象スキャナーとマネージャーとのリンクを解除します。
`nessuscli managed status`	管理対象スキャナーの状態を特定します。
Dump Command	
`nessuscli dump --plugins`	`sbin` ディレクトリに `plugins.xml` ファイルを追加します。たとえば、Linux で `/opt/nessus/sbin/nessuscli dump --plugins` を実行することにより、`plugins.xml` ファイルが `/opt/nessus/sbin/plugins` ディレクトリに追加されます。
Node Commands	

コマンド	説明
クラスタ環境でノードのリンクを表示および変更するために使用されます。	
`nessuscli node link --key=<key> --host=<host> --port=<port>`	クラスタ環境で子ノードを親ノードにリンクします。 キー、ホスト、およびポートについての詳細は、ノードをリンクするを参照してください。
`nessuscli node unlink`	親ノードと子ノードのリンクを解除します。
`nessuscli node status`	親ノードへの子ノードのリンクの有無、およびリンクするエージェント数について表示されます。

Nessuscli Agent

Tenable Agent の一部の機能をコマンドラインインターフェースを通じて実行するには、Agent `nessuscli` ユーティリティを使用します。

注意: どの Agent `nessuscli` コマンドも、管理者権限を持つユーザーとして実行する必要があります。

Nessuscli の構文

オペレーティングシステム	コマンド
Windows	`C:\Program Files\Tenable\Nessus Agent\nessuscli.exe <cmd> <arg1> <arg2>`
macOS	`# sudo /Library/NessusAgent/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Linux	`# /opt/nessus_agent/sbin/nessuscli <cmd> <arg1> <arg2>`

Nessuscli のコマンド

コマンド	説明
情報のコマンド	
`# nessuscli help`	nessuscli コマンドのリストを表示します。
`# nessuscli -v`	Tenable Agent の現在のバージョンを表示します。
`# nessuscli fix --get <agent setting>`	エージェント設定の現在の値を表示します。
バグレポートコマンド	
`# nessuscli bug-report-generator`	システム診断のアーカイブを作成します。 引数を付けずにこのコマンドを使用すると、ユーティリティによって値を入力するよう促されます。 **オプションの引数** • `--quiet` - ユーザーにフィードバックを求めることなく、バグレポートジェネレーターが実行されます。 • `--scrub` - バグレポートジェネレーターによって IPv4 アドレスの最後の 2 つの 8 ビットがサニタイズされます。 • `--full` - バグレポートジェネレーターによって追加データが収集されます。
画像作成コマンド	
`# nessuscli prepare-image`	以下のように画像処理前のクリーンアップを行います。 • エージェントがリンクされている場合、解除します。 • エージェント上のすべてのホストタグを

コマンド	説明
	削除します。たとえば、Windows ではレジストリキー、Unix では tenable_tag などです。 • エージェント上のすべての UUID ファイルを削除します。例: /opt/nessus/var/nessus/uuid (MacOS/Windows ではこれと同等のもの)。 • プラグイン dbs を削除します。 • global db を削除します。 • master.key を削除します。 • backups ディレクトリを削除します。 **オプションの引数** • --json=<file> - 自動設定用の .json ファイルを検証し、適切なディレクトリに配置します。
ローカルエージェントのコマンド **エージェントステータスのリンク、リンク解除、表示を行うために使用します。**	
# nessuscli agent link --key=<key> --host=<host> --port=<port>	Tenable Agent リンクキーを使用して、エージェントを Tenable Nessus Manager または Tenable Vulnerability Management にリンクします。 **必須の引数** • --key - マネージャーから取得したリンクキー。 • --host - Tenable Nessus Manager のインストール中に設定した静的 IP ア

コマンド	説明
	ドレスまたはホスト名。 **注意:** Tenable Agent 8.1.0 以降では、Tenable Vulnerability Management にリンクされたエージェントは `sensor.cloud.tenable.com` を使用して Tenable Vulnerability Management と通信します。エージェントが `sensor.cloud.tenable.com` に接続できない場合は、代わりに `cloud.tenable.com` を使用します。それより前のバージョンのエージェントは、`cloud.tenable.com` ドメインを使用し続けます。 • `--port` - Tenable Nessus Manager にリンクするには、8834 またはカスタムポートを使用します。Tenable Vulnerability Management にリンクするには 443 を使用します。 **オプションの引数** • `--auto-proxy` – (Windows のみ) 設定した場合、エージェントはプロキシを設定するために、Web Proxy Auto Discovery (WPAD) を使用して Proxy Auto Config (PAC) ファイルを取得します。この設定は、他のすべてのプロキシ設定に優先します。 • `--name` - エージェントの名前。エージェントの名前を指定しない場合、名前はエージェントをインストールしているコンピューターの名前にデフォルトで設定されます。 • `--groups` - エージェントを追加する 1

コマンド	説明
	つ以上のエージェントグループ。インストール中にエージェントグループを指定しない場合は、リンクされたエージェントを後で Tenable Nessus Manager 内のエージェントグループに追加できます。コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。例: `"Atlanta,Global Headquarters"` **注意:** エージェントグループ名は、大文字と小文字を区別し、正確に一致する必要があります。エージェントグループ名は引用符で囲む必要があります (例: `--groups="My Group"`)。 • `--ca-path` - マネージャーのサーバー証明書の検証に使用するカスタム CA 証明書。 • `--offline-install` – 有効にすると、オフラインの状態でも Tenable Agent がシステムにインストールされます。Tenable Agent は定期的にマネージャーへのリンクを試みます。 エージェントがコントローラーに接続できない場合、1 時間ごとに再試行します。コントローラーには接続できるがリンクに失敗する場合は、24 時間ごとに再試行します。 • `--network` - Tenable Vulnerability Management にリンクされたエージェントの場合、エージェントをカスタムネット

コマンド	説明
	ワークに追加します。ネットワークを指定しない場合、エージェントはデフォルトのネットワークに属することになります。 • `--profile-uuid` - エージェントを割り当てるエージェントプロファイルの UUID (例: `12345678-9abc-4ef0-9234-56789abcdef0`)。詳細については、「*Tenable Vulnerability Management ユーザーガイド*」のエージェントプロファイルを参照してください。 • `--proxy-host` - プロキシサーバーのホスト名または IP アドレス。 • `--proxy-port` - プロキシサーバーのポート番号。 • `--proxy-password` - ユーザー名として指定したユーザーアカウントのパスワード。 • `--proxy-username` - プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。 • `--proxy-agent` - プロキシに事前定義されたユーザーエージェントが必要とされる場合のユーザーエージェント名。
`# nessuscli agent relink --host=<new_host> --port=<new_port>`	リンクされたエージェントを Tenable Vulnerability Management から Tenable Sensor Proxy に、またはその逆に再リンクします。 **注意:** このコマンドは、Tenable Nessus

コマンド	説明
	Manager に接続されたエージェントには対応していません。
`# nessuscli agent unlink`	エージェントを Tenable Nessus Manager または Tenable Vulnerability Management からリンク解除します。 **オプションの引数** • `--force` – エージェントがマネージャーと通信できない場合でも、エージェントを Tenable Nessus Manager または Tenable Vulnerability Managementから強制的にリンク解除します。Tenable では、Tenable Nessus Manager または Tenable Vulnerability Management と通信できないエージェントのリンクを解除するため、このフラグを使用することを推奨しています。 `--force` フラグを使用する場合は、Tenable Nessus Manager または Tenable Vulnerability Management でエージェントのリンクを解除する必要が生じる場合もあります。
`# nessuscli scan-triggers --list`	エージェントのルールベーススキャンについての詳細をリストします。 • スキャン名 • ステータス (**uploaded** (アップロード済み) など) • 最後にアクティビティがあった時間 (ステータスの隣に表示されます) • スキャンの説明

コマンド	説明
	• 最新のポリシー変更の時間 • 最終実行時間 • スキャントリガー • スキャン設定テンプレート • スキャンを開始するためのコマンド (`nessuscli scan-triggers --start --UUID=<scan-uuid>`)
`# nessuscli scan-triggers --start --UUID=<scan-uuid>`	(Tenable Vulnerability Management にリンクされたエージェントのみ) UUID に基づくルールベーススキャンを手動で実行します。
`# nessuscli agent status`	エージェントのステータス、ルールベーススキャンの情報、保留中のジョブ、およびエージェントがサーバーにリンクしているかどうかを表示します。 コマンド出力には、次の情報の一部が表示されます。 • Running (実行中) – エージェントが現在ホスト上でアクティブであるかどうかを示します。 • Linked to (リンク先) – エージェントがリンクされているマネージャーを示します。 • Link status (リンクステータス) – エージェントのマネージャーとの現在のリンクステータスを示します。 • Proxy (プロキシ) – エージェントが接続しているプロキシを示します (該当する場合)。

コマンド	説明
	• Plugin set (プラグインセット) – エージェントの現在のプラグインセットを示します。 • Scanning (スキャン中) – エージェントが現在ホストをスキャンしているかどうかを示します。この値は、保留中のスキャンジョブの数と、エージェントに対して設定されたスキャントリガーの数も示します (この値は、出力では **smart scan configs** (スマートスキャン設定) とラベル付けされます)。 • Scans run today (今日実行されたスキャン) – エージェントが今日実行したスキャンの数を示します。 • Last scanned (最終スキャン日) – エージェントが最後にスキャンを実行した日時を示します。 • Last connect (最終接続日) – エージェントがマネージャーに最後に接続した日時を示します。 • Last connection attempt (最終接続試行日) – エージェントがマネージャーに最後に接続を試行した日時を示します。 **オプションの引数** • `--local` – (デフォルトの動作) ステータス、現在のジョブ数、保留中のジョブを示します。このオプションは、エージェントがステータスを取得するためにその管理ソフトウェアに接続しないようにしま

コマンド	説明
	す。代わりに、最後の同期時に取得した最新情報が表示されます。 • `--remote` - (デフォルトの動作) 管理ツールからジョブ数が取得され、ステータスが表示されます。 **注意:** Tenable では、`--remote` オプションによる頻繁なステータスチェックの実行を推奨していません (自動化の利用時など)。 • `--offline` – Tenable Nessus Manager または Tenable Vulnerability Management に接続できない場合、最後にキャッシュされたエージェントステータスを表示します。 • `--show-token` – 管理ツールにより特定および認証に利用された、エージェントのトークンを表示します。 • `--show-uuid` – エージェントの Tenable UUID を表示します。
`# nessuscli plugins --info`	エージェントのフルおよびインベントリプラグインセットの詳細をリストします。 • インストールされているバージョン • 最後にダウンロードされた日時 • 最後に必要とされた日時 • 有効期限 – プラグインセットが期限切れとなる日時 (つまり、プラグインセットが不要になるタイミング)。 • プラグイン – プラグインセット内のプラグ

コマンド	説明
	インの総数。 • 非圧縮時のソースサイズ エージェントのプラグインに関する、以下の詳細および統計情報を一覧表示します。 • 最後にプラグインが更新された日時 • 最後にプラグインの更新を確認した日時 • 圧縮後のプラグインソースの合計サイズ • コンパイル後のプラグインの合計サイズ • プラグイン属性データの合計 • ディスク上のプラグインの合計サイズ
`# nessuscli plugins --reset`	すべてのプラグインとプラグインに関連するデータをディスクから削除します。エージェントは、削除が完了した直後にプラグインをダウンロードできます。 **注意:** このコマンドは、エージェントのディスクにプラグインデータがある場合にのみトリガーされます。
`# nessuscli profile --show`	該当する場合、エージェントに割り当てられている Tenable Vulnerability Management エージェントプロファイルに関する情報を取得します。
`# nessuscli install-relay --linking-key=<Tenable Identity Exposure relay linking`	エージェントに Tenable Identity Exposure セキュアリレーをインストールします。 Tenable Identity Exposure リレーリンクキーを取得するには、*Tenable Identity Exposure*

コマンド	説明
key>	*管理者ガイド*のセキュアリレーを参照してください。 install-relay は、以下の任意のパラメーターをサポートしています。 • proxy_address – プロキシが Tenable ドメインに到達する必要がある場合に使用するプロキシ IP または DNS。proxy_address を入力すると、proxy_port も入力する必要があります。 • proxy_address – プロキシが Tenable ドメインに到達する必要がある場合に使用するプロキシポート。proxy_port を入力すると、proxy_address も入力する必要があります。 • proxy_basic_login – プロキシログインのユーザー名。proxy_basic_login を入力すると、proxy-basic-password も入力する必要があります。 • proxy-basic-password – プロキシのログインパスワード。proxy_basic_login を入力すると、proxy_basic_login も入力する必要があります。 プロキシを指定しない場合は、プロキシパラメーターを一切入力しないでください。認証されていないプロキシを指定するには、proxy_address と proxy_port を入力します。認証されているプロキシを指定するには、proxy_address、proxy_port、proxy_

コマンド	説明
	`basic_login`、および `proxy-basic-password` を入力します。
アップデートコマンド	
`# nessuscli agent update --file=<plugins_set.tgz>`	プラグインセットを手動でインストールします。
修正コマンド	
`# nessuscli fix --list`	エージェントの設定とその値のリストを表示します。
`nessuscli fix --set <setting>=<value>`	エージェント設定を特定の値にセットします。 エージェント設定の一覧は、*Tenable Agent ユーザーガイド*の詳細設定を参照してください。
`# nessuscli fix --set update_hostname="<value>"`	Tenable Vulnerability Management または Tenable Nessus Manager のエージェントホスト名を自動的に更新します。 `update_hostname` パラメーターは、`yes` または `no` に設定できます。デフォルトでは、この環境設定は無効になっています。 **注意:** 変更を Tenable Nessus Manager で有効にするためにエージェントサービスを再起動します。
`# nessuscli fix --set agent_update_channel=<value>`	(Tenable Vulnerability Management にリンクされたエージェントのみ) エージェント更新プランを設定して、エージェントが自動的に更新するバージョンを指定します。 値:

コマンド	説明
	• **ga** - 最新バージョンが一般公開 (GA) され次第、自動的に最新の Tenable Nessus バージョンへと更新されます。**注意:** この日付はバージョンが一般公開された日と同じ日付です。 • **ea** - 最新バージョンが早期アクセス (EA) 用にリリースされ次第、自動的に最新の Tenable Nessus バージョンへと更新します。通常一般公開よりも数週間早いタイミングです。 • **stable** - 自動的に最新の Tenable Nessus バージョンに更新しません。Tenable が設定した旧バージョンの Tenable Nessus の状態を維持します。これは通常、最新の一般公開バージョンよりも 1 リリース前のものとなりますが、8.10.0 よりも前のバージョンにはなりません。Tenable Nessus の新しいバージョンがリリースされると、Tenable Nessus インスタンスのソフトウェアバージョンは更新されますが、最新のリリースよりも前のバージョンに留まります。 **注意:** Tenable Vulnerability Management にリンクされているエージェントの場合は、エージェントの `nessuscli` ユーティリティから `agent_update_channel` コマンドを実行する必要があります。Tenable Nessus Manager にリンクされているエージェントの場合は、Tenable Nessus Manager の `nessuscli` ユーティリティから `agent_update_channel` コマンドを実行する必要があります。

コマンド	説明
`# nessuscli fix --set maximum_scans_per_day=<value>`	(Tenable Vulnerability Management にリンクされたエージェントのみ) エージェントが 1 日につき実行できる最大スキャン数を設定します。最小数量は **1**、最大数量は **48** で、デフォルト数量は **10** となります。
`# nessuscli fix --set max_retries="<value>"`	`agent link`、`agent status`、または `agent unlink` コマンドの実行中に不具合が生じた場合、エージェントが再試行する最大回数が設定されます。コマンドは、試行間隔を `retry_sleep_milliseconds` に設定することで休止時間を徐々に増やしながら、指定回数にわたり、連続して再試行されます。`max_retries` のデフォルト値は 0 です。最小値は 0 で、最大値は 10 です。 たとえば、`max_retries` を 4 に、`retry_sleep_milliseconds` を 1500 (デフォルト) に設定した場合は、エージェントが 1 回目の試行後に 1.5 秒間、2 回目の試行後に 3 秒間、3 回目の試行後に 4.5 秒間休止します。 **注意:** この設定はオフラインの更新やリンク後 24 時間経過してから通常実行されるエージェントのチェックインには影響しません。
`# nessuscli fix --set retry_sleep_milliseconds="<value>"`	`agent link`、`agent status`、または `agent unlink` コマンドの実行中に不具合が生じた場合、エージェントの再試行間隔がミリ秒単位で設定されます。デフォルトは 1500 ミリ秒 (1.5 秒) です。
`# nessuscli fix --set`	Tenable Agent に NIAP モードを適用しま

コマンド	説明
`niap_mode=enforcing`	す。NIAP モードの詳細については、NIAP に準拠する Tenable Agent の設定を参照してください。
`# nessuscli fix --set niap_mode=non-enforcing`	Tenable Agent の NIAP モードを無効にします。NIAP モードの詳細については、NIAP に準拠する Tenable Agent の設定を参照してください。
`# nessuscli fix --set fips_mode=enforcing`	Tenable Agent 通信およびデータベース暗号化に対して最新の検証済み FIPS モジュールを適用します。FIPS モジュールはスキャン暗号化に影響しません。 **注意:** NIAP モードを適用すると、Tenable Agent は FIPS モジュールも適用します。詳細については、NIAP に準拠する Tenable Agent の設定を参照してください。
`# nessuscli fix --set fips_mode=non-enforcing`	Tenable Agent 通信およびデータベース暗号化に対して FIPS モジュールを無効にします。 **注意:** NIAP モードを無効にすると、Tenable Agent は FIPS モジュールも無効にします。詳細については、NIAP に準拠する Tenable Agent の設定を参照してください。
セキュア設定の修正	

コマンド	説明

`nessuscli fix`
 	
`nessuscli fix [--secure] --list`
 	
`nessuscli fix [--secure] --set <setting=value>`
 	
`nessuscli fix [--secure] --get <setting>`
 	
`nessuscli fix [--secure] --delete <setting>`
	`--list`、`--set`、 `--get`、`--delete` コマンドを使用して、詳細なエージェント設定を変更したり表示したりすることができます。
	
	`--secure` オプションを選択すると、登録関連情報が含まれる暗号化の環境設定に影響が及びます。
	
	警告: ドキュメントにない `--secure` 設定の変更は Tenable でサポートされない設定となるため推奨していません。
	
	エージェント設定の一覧は、*Tenable Agent ユーザーガイド*の詳細設定を参照してください。

`# nessuscli fix --secure --get agent_linking_key`	(Tenable Nessus Manager バージョン 10.4.0 以降のみ) 一意のエージェントリンクキーを取得します。 **注意:** このリンクキーは、エージェントをリンクする目的でのみ使用できます。スキャナーまたは子ノードとのリンクには使用できません。
リソース管理コマンド	

`# nessuscli fix --set process_priority="<value>"`
 	
`# nessuscli fix --get process_priority`
 	
`# nessuscli fix --delete process_priority`
	コマンド
	
	`process_priority` 設定をセット、取得、または削除します。
	
	`process_priority` 設定を使用することで、システム上で実行中の他のタスクの優先度に対する Tenable Agent の相対的な優先度を制御できます。
	
	有効な値、およびこの設定の仕組みに関しては、*Tenable Agent デプロイメントとユー*

コマンド	説明
	ザーガイド のエージェント CPU リソースコントロールの <value> 設定オプションを参照してください。

Tenable Nessus ソフトウェアを更新する (CLI)

Tenable Nessus コンポーネントを更新するときには、nessuscli update コマンドを使用できます (コマンドラインセクションにも記載しています)。

注意: Tenable Nessus をオフラインで使用している場合は、Tenable Nessus をオフラインで管理するを参照してください。

注意: 次のコマンドを管理者権限で実行する必要があります。

オペレーティングシステム	コマンド
Linux	`# /opt/nessus/sbin/nessuscli <cmd> <arg1> <arg2>`
Windows	`C:\Program Files\Tenable\Nessus <cmd> <arg1> <arg2>`
macOS	`# /Library/Nessus/run/sbin/nessuscli <cmd> <arg1> <arg2>`
ソフトウェア更新コマンド	
`nessuscli update`	ツールはデフォルトで、Nessus ユーザーインターフェースを通じて選択されたソフトウェアの更新オプションに従います。
`nessuscli update --all`	Nessus の全コンポーネントに更新プログラムを強制的に適用します。
`nessuscli update --plugins-only`	Nessus のプラグインのみに更新プログラムを強制的に適用します。

NIAP に準拠する Tenable Nessus の設定

所属組織が Tenable Nessus のインスタンスを National Information Assurance Partnership (NIAP) 基準に適合させることを要求する場合、関連する設定が NIAP 基準に準拠するように Tenable Nessus を設定できます。

警告: Windows に Tenable Nessus 10.5.8 をインストールする場合、NIAP に準拠し、CVE-2025-36625 の脆弱性を回避するために Tenable Nessus をデフォルトのディレクトリにインストールする必要があります。

始める前に

- Tenable Nessus にログインするために SSL 証明書を使用して SSL 証明書にログインしている場合は、サーバーとクライアントの証明書が NIAP に準拠していることを確認してください。CA が署名した独自の証明書を使用することも、Tenable Nessus を使用して ログイン用の Nessus SSL 証明書を作成する することもできます。
- Tenable Nessus をインストールしたホストのオペレーティングシステムが提供するフルディスク暗号化機能が有効になっていることを確認します。

NIAP に準拠するよう Tenable Nessus を設定するには

1. Tenable Nessus のインスタンスにログインします。
2. コマンドラインインターフェースを使用して NIAP モードを有効にします。
    a. コマンドラインインターフェースから Tenable Nessus にアクセスします。
    b. コマンドラインで、次のコマンドを入力します。

    ```
    nessuscli fix --set niap_mode=enforcing
    ```

    Linux の例

    ```
    /opt/nessus/sbin/nessuscli fix --set niap_mode=enforcing
    ```

    Tenable Nessus は以下を実行します。

    注意: Tenable Nessus が NIAP モードの場合、Tenable Nessus が NIAP モードのままである限り、Tenable Nessus は以下の設定をオーバーライドします。NIAP モードを無効にすると、Tenable Nessus は以前の設定に戻ります。

- **SSL モード** (`ssl_mode_preference`) を **TLS 1.2** (`niap`) オプションでオーバーライドします。
- **SSL 暗号リスト** (`ssl_cipher_list`) の設定を、次の暗号を設定する **NIAP 承認された暗号** (`niap`) 設定でオーバーライドします。
    - ECDHE-RSA-AES128-SHA256
    - ECDHE-RSA-AES128-GCM-SHA256
    - ECDHE-RSA-AES256-SHA384
    - ECDHE-RSA-AES256-GCM-SHA384
- 厳格な証明書検証を使用します。
    - 中間証明書に CA 拡張がない場合、証明書チェーンを許可しません。
    - 署名 CA 証明書を使用して、サーバー証明書を認証します。
    - ログインにクライアント証明書認証を使用する際に、クライアント証明書を認証します。
    - Online Certificate Status Protocol (OCSP) を使用して、CA 証明書の失効ステータスをチェックします。証明書が取り消されると、Tenable Nessus は証明書を無効としてマークします。応答がない場合、Tenable Nessus は証明書を無効としてマークしません。
    - 証明書に、known_CA.inc にある有効で信頼できる CA があることを確認してください。Tenable Vulnerability Management および plugins.nessus.org の CA 証明書は、プラグインディレクトリの known_CA.inc にすでにあります。
    - known_CA.inc にないカスタム CA 証明書を使用する場合は、プラグインディレクトリにある custom_CA.inc にコピーしてください。
- Tenable Nessus 通信およびデータベース暗号化に対して最新の検証済み FIPS モジュールを適用します。FIPS モジュールはスキャン暗号化に影響しません。

    > **注意:** NIAP モードを適用することなく `nessuscli` から FIPS モジュールを適用できます。詳細は、修正コマンドを参照してください。

データベースの暗号化

暗号化されたデータベースをデフォルトの形式 (OFB-128) から NIAP 準拠の暗号化 (XTS-AES-128) に変換できます。

NIAP モードの Tenable Nessus では、デフォルトの形式 (OFB-128) でデータベースを読み取ることができます。

暗号化されたデータベースを NIAP 準拠の暗号化に変換するには

1. Tenable Nessus を停止します。
2. 前の手順で説明されているように、NIAP モードを有効にします。
3. 次のコマンドを入力してください。

   ```
   nessuscli security niapconvert
   ```

   Tenable Nessus は、暗号化されたデータベースを XTS-AES-128 形式に変換します。

デフォルトのデータディレクトリ

デフォルトの Tenable Nessus データディレクトリには、ログ、証明書、一時ファイル、データベースバックアップ、プラグインデータベース、その他の自動生成ファイルが格納されます。

お使いのオペレーティングシステムのデフォルトのデータディレクトリを特定するには、以下の表を参照してください。

オペレーティングシステム	ディレクトリ
Linux	**/opt/nessus/var/nessus**
Windows	**C:\ProgramData\Tenable\Nessus\nessus**
macOS	**/Library/Nessus/run/var/nessus**

注意: Tenable Nessus では、`/opt/nessus/` でのシンボリックリンクの使用はサポートされていません。

暗号強度

Tenable Nessus ではストレージおよび通信時に、次に示すデフォルトの暗号化を使用します。

機能	デフォルトの暗号化
ユーザーアカウントのパスワードの保存	SHA-512 および 512 ビットの鍵を持つ PBKDF2 機能

認証情報に記載されている、スキャンの認証情報のためのユーザーおよびサービスアカウントの保存	AES-128
スキャン結果とスキャンのエクスポート	AES-128
Tenable Nessus とクライアント (GUI/API ユーザー) 間の通信	Tenable Nessus および、お使いのブラウザまたは API プログラムで対応している最も強力な暗号化方法を使用する TLS 1.3 (設定によっては TLS 1.2 以前にフォールバック)
Tenable Nessus と Tenable Agents との間の通信	TLS 1.3 (環境により強制された場合、TLS 1.2 にフォールバック)
Tenable Nessus と Tenable プラグインアップデートサーバー間の通信	ECDHE-RSA-AES256-GCM-SHA384 を使用する TLS 1.2
Tenable Nessus と Tenable 製品登録サーバー間の通信	ECDHE-RSA-AES256-GCM-SHA384 を使用する TLS 1.2

ファイルとプロセスの許可リスト

Tenable は、ファーストパーティ製およびサードパーティ製のエンドポイントセキュリティ製品 (ウイルス対策アプリケーションやホストベースの侵入防止システムなど) で、次の Tenable Nessus フォルダーとプロセスを許可することを推奨しています。

Tenable Agent プロセスの許可リスト登録の詳細については、*Tenable Agent ユーザーガイド*のファイルとプロセスの許可リストを参照してください。

注意: Tenable では、以下にリストされているフォルダーとプロセスに加えて、ファイヤーウォールで特定の Tenable サイトを許可リストに入れることを推奨しています。詳細については、Which Tenable sites should I allow? (許可する必要がある Tenable のサイト)というKB の記事を参照してください。

Windows
フォルダー

注意: Windows インストールで標準以外のドライブまたはフォルダー構造を使用している場合は、%PROGRAMFILES% と %PROGRAMDATA% 環境変数を使用します。
C:\Program Files\Tenable\Nessus*
C:\Program Files (x86)\Tenable\Nessus*
プロセス
C:\ProgramData\Tenable\Nessus\nessus\tmp
C:\Program Files\Tenable\Nessus\nessuscli.exe
C:\Program Files\Tenable\Nessus\nessusd.exe
C:\Program Files\Tenable\Nessus\nasl.exe
C:\Program Files\Tenable\Nessus\nessus-service.exe
C:\Program Files\Tenable\Nessus\openssl.exe
C:\Program Files (x86)\Tenable\Nessus\nasl.exe
C:\Program Files (x86)\Tenable\Nessus\nessuscli.exe
C:\Program Files (x86)\Tenable\Nessus\nessusd.exe
C:\Program Files (x86)\Tenable\Nessus\nessus-service.exe
C:\Program Files (x86)\Tenable\Nessus\openssl.exe
Linux
フォルダー
/opt/nessus/bin/*
/opt/nessus/bin/openssl
/opt/nessus/sbin/*
/opt/nessus/lib/nessus/*
/opt/nessus/etc/nessus

プロセス
/opt/nessus/bin/nasl
/opt/nessus/sbin/nessusd
/opt/nessus/sbin/nessuscli
/opt/nessus/sbin/nessus-service
macOS
フォルダー
/Library/Nessus/run/sbin/*
/Library/Nessus/run/bin/*
プロセス
/Library/Nessus/run/bin/nasl
/Library/Nessus/run/bin/openssl
/Library/Nessus/run/sbin/nessus-service
/Library/Nessus/run/sbin/nessuscli
/Library/Nessus/run/sbin/nessusd
/Library/Nessus/run/sbin/nessusmgt

ログを管理する

Tenable Nessus には、次のデフォルトのログファイルがあります。

- `nessusd.dump` – デバッグ出力に使用される Nessus のダンプログファイル。

  `nessusd.dump` を設定する

  1. `nessuscli` ユーティリティを開きます。
  2. コマンド `# nessuscli fix --set setting=value` を使用して、次の設定を行います。

Name (名前)	説明	デフォルト	有効な値

Nessus Dump File Location (dumpfile) (Nessus ダンプファイルの場所 (dumpfile))	デバッグ出力用ログファイル `nessusd.dump` が生成された場合に保存される場所です。
	
	各オペレーティングシステムのデフォルトは次のとおりです。
	
	Linux
	
	`/opt/nessus/var/nessus/logs/nessusd.dump`
	
	macOS
	
	`/Library/Nessus/run/var/nessus/logs/nessusd.dump`
	
	Windows
	
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump`
		お使いのオペレーティングシステムにおける Nessus のログディレクトリ	文字列

Nessus Dump File Log Level (nasl_log_type) (Nessus ダンプファイルログレベル (nasl_log_type))	`nessusd.dump` における NASL エンジン出力の種類です。	`normal`	選択肢は `normal`、`none`、`trace`、`full` です。

Nessus Dump File Max Files (dumpfile_max_files) (Nessus ダンプファイルの最大ファイル数 (dumpfile_max_files))	ディスク上に残される nessusd.dump ファイルの最大数です。ファイル数が指定された値を超えると、Tenable Nessus は最も古いダンプファイルを削除します。	100	1 から 1000 までの整数
Nessus Dump File Max Size (dumpfile_max_size) (Nessus ダンプファイルの最大サイズ (dumpfile_max_size))	nessusd.dump ファイルの最大サイズ (MB)。ファイルサイズが最大サイズを超えると、Tenable Nessus は新しいダンプファイルを作成します。	512	1 から 2048 までの整数
Nessus	Tenable Nessus ダンプファイルのローテーションの頻度を日数で指定します。	1	1 から 365 まで

Dump File Rotation Time (dumpfile_rotation_time) (Nessus ダンプファイルローテーション時間 (dumpfile_rotation_time))			の整数
Nessus Dump File Rotation (dumpfile_rot) (Nessus ダンプファイルローテーション (dumpfile_rot))	Tenable Nessus がダンプファイルをローテーションする基準が、サイズまたは時間のどちらの最大ローテーションであるかを決定します。	`size`	`size`: Tenable Nessus は `dumpfile_max_size` で指定されたサイズに基づいてダンプファイルをローテーションしま

			す。 time: Tenable Nessus は dumpfile_rotation_time で指定されている時間に基づいてダンプファイルをローテーションします。
Use Milliseconds in Logs (ログでミリ秒を使用する)	この機能を有効にすると、nessusd.messages および nessusd.dump ログのタイムスタンプがミリ秒単位になります。この機能を無効にすると、ログのタイムスタンプは秒単位になります。	×	yes または no

詳細は、詳細設定を参照してください。

または、log.json ファイルを編集して、nessusd.dump のログの場所とローテーション戦略を設定できます。また、新しい reporters[x].reporter セクションを作成してカスタムファイル名を作成することにより、カスタムログを設定することもできます。

log.json を使用してログ設定を変更する方法

1. テキストエディターを使用して、対応するディレクトリにある log.json ファイルを開きます。

オペレーティングシステム	ログの場所
Windows	C:\ProgramData\Tenable\Nessus\nessus\logs\ *<filename>*
macOS	/Library/Nessus/run/var/nessus
Linux	/opt/nessus/var/nessus

2. 各ログファイルの reporters[x].reporter セクションを編集または作成し、次のパラメーターを追加または変更します。

> **注意:** 以下に log.json ファイルのパラメーターと、ユーザーによるそのパラメーターの変更を Tenable が推奨しているかどうかを記載します。一部のパラメーターは詳細なものであり、通常はユーザーが変更する必要はありません。もしユーザーが上級者で、詳細なパラメーターを使用してカスタムログファイルを設定したい場合は、詳細情報としてナレッジベースの記事を参照してください。

パラメーター	デフォルト値	変更可能か?	説明
type	file	非推奨	ログファイルの種類を決定します。
rotation_strategy	サイズ	○	ログがファイルをアーカイブする基準が最大循環サイズ、または循環時間のどちらであるかを指定します。 有効な値: • size – max_size の規定に従い、サイズを基準としてロー

パラメーター	デフォルト値	変更可能か？	説明
			テーションします • daily – rotation_time の規定に従い、時間を基準としてローテーションします
rotation_time	86400 (1 日)	○	循環時間 (秒単位)。 rotation_strategy が daily に設定されている場合にのみ使用します。
max_size	Tenable Nessus:536870912 (512 MB) エージェント：10485760 (10 MB)	○	循環サイズ (バイト単位)。 rotation_strategy が size に設定されている場合にのみ使用します。
max_files	Tenable Nessus: 10 エージェント：2	○	ファイル循環で許容される最大ファイル数。 最大数には、メインファイルが含まれるため、10 の max_files はメインファイル 1 つと

パラメーター	デフォルト値	変更可能か？	説明
			バックアップ 9 つで設定されます。この数を減らすと、古いログは Tenable Nessus によって削除されます。
`file`	オペレーティングシステムとログファイルによる	○	ログファイルの場所と名前。デフォルトのログの場所 を参照してください。 デフォルトの Tenable Nessus ログファイルの名前を変更した場合、一部の詳細設定でログ設定を変更できなくなる可能性があります。

log.json ファイルの例を以下に示します。

Linux の例

```
{
	"reporters": [
	{
	"tags": [
		"response"
	],
	"reporter": {
		"type": "file",
		"rotation_strategy": "daily",
		"rotation_time":"86400",
```

```
            "max_size":"536870912",
            "max_files":"1024",
            "file": "/opt/nessus/var/nessus/logs/www_server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file": "/opt/nessus/var/nessus/logs/backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

Windowsの例

注意: バックスラッシュ (\) は、JSON では特殊文字になります。パス文字列にバックスラッシュを入力するには、最初のバックスラッシュを 2 番目のバックスラッシュでエスケープして、正しくパスが解析されるように工夫する必要があります。

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
```

```
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time":"86400",
            "max_size":"536870912",
            "max_files":"1024",
            "file":"C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\www_
server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file":"C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

macOS の例

```
{
      "reporters": [
      {
      "tags": [
            "response"
```

```
        ],
        "reporter": {
              "type": "file",
              "rotation_strategy": "daily",
              "rotation_time":"86400",
              "max_size":"536870912",
              "max_files":"1024",
              "file": "/Library/Nessus/run/var/nessus/logs/www_server.log"
        },
        "format": "combined"
        },
        {
        "tags": [
              "log",
              "info",
              "warn",
              "error",
              "trace"
        ],
        "reporter": {
        "type": "file",
        "file": /Library/Nessus/run/var/nessus/logs/backend.log"
        },
        "context": true,
        "format": "system"
        }
        ]
}
```

3. log.json ファイルを保存します。
4. Tenable Nessus サービスを再起動します。

   Tenable Nessus により、ログ設定が更新されます。

- nessusd.messages – Nessus スキャナーのログ。

  nessusd.messages を設定する

1. エージェント[コマンドラインインターフェース]を開きます。

2. コマンド `# nessuscli fix --set setting=value` を使用して、次の設定を行います。

Name (名前)	説明	デフォルト	有効な値

Nessus Scanner Log Location (logfile) (Nessus スキャナーログの場所 (logfile))	Tenable Nessus がスキャナーのログファイルを保存する場所。
	
	各オペレーティングシステムのデフォルトは次のとおりです。
	
	Linux
	
	`/opt/nessus/var/nessus/logs/nessusd.messages`
	
	macOS
	
	`/Library/Nessus/run/var/nessus/logs/nessusd.messages`
	
	Windows
	
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages`
		お使いのオペレーティングシステムにおける Nessus のログディレクトリ	文字列

Log File Maximum Files (logfile_max_files) (ログファイルの最大ファイル数	Tenable Nessus がディスク上に保持する `nessusd.messages` ファイルの最大数を決定します。`nessusd.messages` ログファイル数が指定された値を超えると、Tenable Nessus は最も古いログファイルを削除します。	Tenable Nessus – 100 Tenable Agent – 2	1 から 1000 までの整数

(logfile_max_files))			
Log File Maximum Size (logfile_max_size) (ログファイルの最大サイズ (logfile_max_size))	nessusd.messages ファイルの最大サイズ (MB) を決定します。ファイルサイズが最大サイズを超えると、Tenable Nessus は新しいメッセージログファイルを作成します。	Tenable Nessus – 512 Tenable Agent – 10	1 から 2048 までの整数
Log File Rotation Time (logfile_rotation_time) (ログファイルローテーション時間 (logfile_rotation_time))	Tenable Nessus メッセージログファイルのローテーションの頻度を日数で指定します。	1	1 から 365 までの整数
Log File Rotation	Tenable Nessus がメッセージログファイルをローテーションする基準が、ローテーションの最大サイズ	サイズ	size – Tenable

(logfile_rot) (ログファイルのローテーション (logfile_rot))	と時間のどちらであるかを決定します。		Nessusは、`logfile_max_size`で指定されたサイズに基づいてログファイルをローテーションします。 `time` – Tenable Nessusは、`logfile_rotation_time`で指定された時間に基づいてログファイルをローテーションしま

			す。
Use Milliseconds in Logs (logfile_msec) (ログでミリ秒を使用する (logfile_msec))	この機能を有効にすると、nessusd.messages および nessusd.dump ログのタイムスタンプがミリ秒単位になります。この機能を無効にすると、ログのタイムスタンプは秒単位になります。	×	yes または no

詳しくは、詳細設定を参照してください。

- www_server.log – Nessus ウェブサーバーのログ。

www_server.log を設定する

log.json ファイルを編集して、www_server.log に対するログの場所とローテーション戦略を設定できます。また、新しい reporters[x].reporter セクションを作成してカスタムファイル名を作成することにより、カスタムログを設定することもできます。

log.json を使用してログ設定を変更する方法

1. テキストエディターを使用して、対応するディレクトリにある log.json ファイルを開きます。

オペレーティングシステム	ログの場所
Windows	C:\ProgramData\Tenable\Nessus\nessus\logs\ *<filename>*
macOS	/Library/Nessus/run/var/nessus
Linux	/opt/nessus/var/nessus

2. 各ログファイルの reporters[x].reporter セクションを編集または作成し、次のパラメーターを追加または変更します。

> **注意:** 以下に log.json ファイルのパラメーターと、ユーザーによるそのパラメーターの変更を Tenable が推奨しているかどうかを記載します。一部のパラメーターは詳細なものであり、通常はユーザーが変更する必要はありません。もしユーザーが上級者で、詳細なパラメーターを使用してカスタムログファイルを設定したい場合は、詳細情報としてナレッジベースの記事を参照してください。

パラメーター	デフォルト値	変更可能か?	説明
tags	response	×	ログに含めるログ情報を決定します。 • response – ウェブサーバーのアクティビティログ **注意:** response は、www_server.log に対して有効な唯一のタグです。
type	file	非推奨	ログファイルの種類を決

パラメーター	デフォルト値	変更可能か?	説明
			定します。
rotation_strategy	サイズ	○	ログがファイルをアーカイブする基準が最大循環サイズ、または循環時間のどちらであるかを指定します。 有効な値: • size – max_size の規定に従い、サイズを基準としてローテーションします • daily – rotation_time の規定に従い、時間を基準としてローテーションします
rotation_time	86400 (1 日)	○	循環時間 (秒単位)。 rotation_strategy が daily に設定されている場合にのみ使用します。
max_size	Tenable Nessus :536870912 (512 MB)	○	循環サイズ (バイト単位)。 rotation_strategy

パラメーター	デフォルト値	変更可能か?	説明
	Tenable Agent: 10485760 (10 MB)		が `size` に設定されている場合にのみ使用します。
`max_files`	Tenable Nessus: 10 Tenable Agent: 2	○	ファイル循環で許容される最大ファイル数。 最大数には、メインファイルが含まれるため、10 の `max_files` はメインファイル 1 つとバックアップ 9 つで設定されます。この数を減らすと、古いログは Tenable Nessus によって削除されます。
`file`	オペレーティングシステムとログファイルによる	○	ログファイルの場所と名前。デフォルトのログの場所 を参照してください。 デフォルトの Tenable Nessus ログファイルの名前を変更した場合、一部の詳細設定でログ設定を変更できなくなる可能性があります。
`context`	`true`	非推奨	`system` フォーマットのログ (`backend.log` など) で、コンテキスト情報の追加を有効にします。

パラメーター	デフォルト値	変更可能か?	説明
format	combined	非推奨	出力の形式を決定します。 • combined – ウェブサーバーのログに使用される形式で出力を行います • system – デフォルトのオペレーティングシステムのログ形式で出力を行います

log.json ファイルの例を以下に示します。

Linux の例

```
{
	"reporters": [
	{
	"tags": [
		"response"
	],
	"reporter": {
		"type": "file",
		"rotation_strategy": "daily",
		"rotation_time":"86400",
		"max_size":"536870912",
		"max_files":"1024",
		"file": "/opt/nessus/var/nessus/logs/www_server.log"
	},
	"format": "combined"
```

```
        },
        {
        "tags": [
              "log",
              "info",
              "warn",
              "error",
              "trace"
        ],
        "reporter": {
        "type": "file",
        "file": "/opt/nessus/var/nessus/logs/backend.log"
        },
        "context": true,
        "format": "system"
        }
        ]
}
```

Windowsの例

注意: バックスラッシュ (\) は、JSON では特殊文字になります。パス文字列にバックスラッシュを入力するには、最初のバックスラッシュを 2 番目のバックスラッシュでエスケープして、正しくパスが解析されるように工夫する必要があります。

```
{
        "reporters": [
        {
        "tags": [
              "response"
        ],
        "reporter": {
              "type": "file",
              "rotation_strategy": "daily",
              "rotation_time":"86400",
              "max_size":"536870912",
```

```
            "max_files":"1024",
            "file":"C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\www_
server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file":"C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

macOS の例

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time":"86400",
```

```
            "max_size":"536870912",
            "max_files":"1024",
            "file": "/Library/Nessus/run/var/nessus/logs/www_server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file": /Library/Nessus/run/var/nessus/logs/backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

3. log.json ファイルを保存します。
4. Tenable Nessus サービスを再起動します。

   Tenable Nessus により、ログ設定が更新されます。

- backend.log – Nessus バックエンドのログ。

  backend.log を設定する

  log.json ファイルを編集して、backend.log のログの場所とローテーション戦略を設定できます。また、新しい reporters[x].reporter セクションを作成してカスタムファイル名を作成することにより、カスタムログを設定することもできます。

  log.json を使用してログ設定を変更する方法

1. テキストエディターを使用して、対応するディレクトリにある log.json ファイルを開きます。

オペレーティングシステム	ログの場所
Windows	C:\ProgramData\Tenable\Nessus\nessus\logs\ *<filename>*
macOS	/Library/Nessus/run/var/nessus
Linux	/opt/nessus/var/nessus

2. 各ログファイルの reporters[x].reporter セクションを編集または作成し、次のパラメーターを追加または変更します。

> **注意:** 以下に log.json ファイルのパラメーターと、ユーザーによるそのパラメーターの変更を Tenable が推奨しているかどうかを記載します。一部のパラメーターは詳細なものであり、通常はユーザーが変更する必要はありません。もしユーザーが上級者で、詳細なパラメーターを使用してカスタムログファイルを設定したい場合は、詳細情報としてナレッジベースの記事を参照してください。

パラメーター	デフォルト値	変更可能か?	説明
tags	log、info、warn、error、trace	○	ログに含めるログ情報を決定します。 • response – ウェブサーバーのアクティビティログ • info – 特定のタスクの情報ログ • warn – 特定のタスクの警告ログ

パラメーター	デフォルト値	変更可能か？	説明
			• error – 特定のタスクのエラーログ • debug – デバッグ出力 • verbose - debug よりも情報の多いデバッグ出力 • trace – 出力の追跡に使用するログ
type	file	非推奨	ログファイルの種類を決定します。
rotation_strategy	サイズ	○	ログがファイルをアーカイブする基準が最大循環サイズ、または循環時間のどちらであるかを指定します。 有効な値: • size – max_size の規定に従い、サイズを基準としてローテーションします • daily –

パラメーター	デフォルト値	変更可能か？	説明
			rotation_time の規定に従い、時間を基準としてローテーションします
rotation_time	86400 (1 日)	○	循環時間 (秒単位)。 rotation_strategy が daily に設定されている場合にのみ使用します。
max_size	Tenable Nessus:536870912 (512 MB) Tenable Agent: 10485760 (10 MB)	○	循環サイズ (バイト単位)。 rotation_strategy が size に設定されている場合にのみ使用します。
max_files	Tenable Nessus: 10 Tenable Agent: 2	○	ファイル循環で許容される最大ファイル数。 最大数には、メインファイルが含まれるため、10 の max_files はメインファイル 1 つとバックアップ 9 つで設定されます。この数を

パラメーター	デフォルト値	変更可能か？	説明
			減らすと、古いログは Tenable Nessus によって削除されます。
file	オペレーティングシステムとログファイルによる	○	ログファイルの場所と名前。デフォルトのログの場所を参照してください。 デフォルトの Tenable Nessus ログファイルの名前を変更した場合、一部の詳細設定でログ設定を変更できなくなる可能性があります。
context	true	非推奨	system フォーマットのログ (backend.log など) で、コンテキスト情報の追加を有効にします。
format	combined system	非推奨	出力の形式を決定します。 • combined – ウェブサーバーのログに使用される形式で出力を行います • system – デ

パラメーター	デフォルト値	変更可能か？	説明
			フォルトのオペレーティングシステムのログ形式で出力を行います

log.json ファイルの例を以下に示します。

Linux の例

```
{
	"reporters": [
	{
	"tags": [
		"response"
	],
	"reporter": {
		"type": "file",
		"rotation_strategy": "daily",
		"rotation_time":"86400",
		"max_size":"536870912",
		"max_files":"1024",
		"file": "/opt/nessus/var/nessus/logs/www_server.log"
	},
	"format": "combined"
	},
	{
	"tags": [
		"log",
		"info",
		"warn",
		"error",
		"trace"
	],
```

```
        "reporter": {
        "type": "file",
        "file": "/opt/nessus/var/nessus/logs/backend.log"
        },
        "context": true,
        "format": "system"
        }
        ]
}
```

Windowsの例

注意: バックスラッシュ (\) は、JSON では特殊文字になります。パス文字列にバックスラッシュを入力するには、最初のバックスラッシュを 2 番目のバックスラッシュでエスケープして、正しくパスが解析されるように工夫する必要があります。

```
{
        "reporters": [
        {
        "tags": [
                "response"
        ],
        "reporter": {
                "type": "file",
                "rotation_strategy": "daily",
                "rotation_time":"86400",
                "max_size":"536870912",
                "max_files":"1024",
                "file":"C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\www_
server.log"
        },
        "format": "combined"
        },
        {
        "tags": [
                "log",
```

```
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file":"C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

macOS の例

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time":"86400",
            "max_size":"536870912",
            "max_files":"1024",
            "file": "/Library/Nessus/run/var/nessus/logs/www_server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
```

```
            "info",
            "warn",
            "error",
            "trace"
        ],
        "reporter": {
        "type": "file",
        "file": /Library/Nessus/run/var/nessus/logs/backend.log"
        },
        "context": true,
        "format": "system"
        }
        ]
}
```

3. log.json ファイルを保存します。
4. Tenable Nessus サービスを再起動します。

   Tenable Nessus により、ログ設定が更新されます。

- nessuscli.log - Nessuscli のログ。

デフォルトのログの場所

次の表に、各オペレーティングシステムにおけるデフォルトのログファイルの場所を示します。

オペレーティングシステム	ログの場所
Windows	C:\ProgramData\Tenable\Nessus\nessus\logs*<filename>*
macOS	/Library/Nessus/run/var/nessus/logs/*<filename>*
Linux	/opt/nessus/var/nessus/logs/*<filename>*

大規模デプロイメントのサポート

環境変数または設定用の JSON ファイルを使用して、Tenable Nessusスキャナーを自動的に設定してデプロイできます。これにより、大規模なデプロイメントを効率化できます。

インストール後に初めて Tenable Nessus を起動すると、Tenable Nessus は最初に環境変数が存在するかどうかを確認し、次に config.json ファイルを確認します。Tenable Nessus の初回起動時に、

Tenable Nessus はその情報を使用して スキャナーをマネージャーにリンクし、環境設定をセットして、ユーザーを作成します。

> **注意:** 情報が環境変数とconfig.jsonの両方にある場合、Tenable Nessus は両方の情報を使用します。競合する情報がある (たとえば、環境変数とconfig.jsonで異なるリンクキーを持つ) 場合、Tenable Nessus は環境変数からの情報を使用します。

詳細については、次を参照してください。

- Tenable Nessus 環境変数
- JSON を使用して Tenable Nessus をデプロイする

Tenable Nessus 環境変数

環境変数に基づいて Tenable Nessus を設定する場合、Tenable Nessus が動作しているシェル環境に次の環境変数をセットすることができます。

インストール後に初めて Tenable Nessus を起動すると、Tenable Nessus は最初に環境変数が存在するかどうかを確認し、次に config.json ファイルを確認します。Tenable Nessus の初回起動時に、Tenable Nessus はその情報を使用して スキャナーをマネージャーにリンクし、環境設定をセットして、ユーザーを作成します。

ユーザー設定

最初にユーザー設定を行う際は、次の環境変数を使用します。

- NCONF_USER_USERNAME : Tenable Nessus のユーザー名。
- NCONF_USER_PASSWORD : Tenable Nessus ユーザーのパスワード。

  > **注意:** NCONF_USER_PASSWORD の値を空にしてユーザーだけを作成した場合、Tenable Nessus は自動的にパスワードを生成します。そのユーザーでログインするには、nessuscli を使用して初めにユーザーのパスワードを変更してください。

- NCONF_USER_ROLE: Tenable Nessus ユーザーのロール。

リンクの設定

リンクの設定には、次の環境変数を使用します。

- NCONF_LINK_HOST: リンク先となるマネージャーのホスト名またはIPアドレスです。Tenable Vulnerability Managementにリンクするには、cloud.tenable.comを使用します。
- NCONF_LINK_PORT: リンクするマネージャーのポート。
- NCONF_LINK_NAME: リンク時に使用するスキャナーの名前。
- NCONF_LINK_KEY: リンクするマネージャーのリンクキー。
- NCONF_LINK_CERT : (オプション) マネージャーへの接続の検証に使用するCA証明書。
- NCONF_LINK_RETRY : (オプション) Tenable Nessusがリンクを再試行する回数。
- NCONF_LINK_PROFILE_UUID - (オプション) スキャナーを割り当てるスキャナープロファイルのUUID。
- NCONF_LINK_GROUPS: (オプション) スキャナーを追加する、1つ以上の既存のスキャナーグループ。コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。例: `"Atlanta,Global Headquarters"`

JSONを使用してTenable Nessusをデプロイする

JSONファイル`config.json`を使用して、Tenable Nessusスキャナーを自動的に設定してデプロイできます。お使いのオペレーティングシステム上でのこのファイルの場所を確認するには、デフォルトのデータディレクトリを参照してください。

インストール後に初めてTenable Nessusを起動すると、Tenable Nessusは最初に環境変数が存在するかどうかを確認し、次に`config.json`ファイルを確認します。Tenable Nessusの初回起動時に、Tenable Nessusはその情報を使用して スキャナーをマネージャーにリンクし、環境設定をセットして、ユーザーを作成します。

> **注意:** `config.json`はASCII形式である必要があります。PowerShellなどの一部のツールは、デフォルトで他の形式のテストファイルを作成します。

config.jsonファイルの場所

config.jsonファイルは以下の場所に配置してください。

- Linux : `/opt/nessus/var/nessus/config.json`
- Windows: `C:\ProgramData\Tenable\Nessus\nessus\config.json`

Tenable Nessusファイル形式の例

```
{ "link": { "name": "sensor name", "host": "hostname or IP address", "port": 443,
"key": "abcdefghijklmnopqrstuvwxyz", "ms_cert": "CA certificate for linking", "retry":
1, "proxy": { "proxy": "proxyhostname", "proxy_port": 443, "proxy_username":
"proxyusername", "proxy_password": "proxypassword", "user_agent": "proxyagent", "proxy_
auth": "NONE" } }, "preferences": { "global.max_hosts": "500" }, "user": { "username":
"admin", "password": "password", "role": "system_administrator", "type": "local" } }
```

config.json の詳細

config.json の、各セクションの個別設定の書式を以下に記載します。

注意：すべてのセクションは省略可能です。セクションを含めない場合、そのセクションは Tenable Nessus を初めて起動したときには設定されません。その設定は、後で手動で設定できます。

リンク

link セクションでは、Tenable Nessus をマネージャーにリンクするための環境設定をセットします。

設定	説明
名前	(オプション) スキャナーの名前。
host	リンク先となるマネージャーのホスト名または IP アドレスです。
port	リンク先のマネージャーのポート。 Tenable Nessus Managerの場合：8834 またはカスタムポート。
key	Manager から取得したリンクキー。
ms_cert	(オプション) マネージャーのサーバー証明書の検証に使用するカスタム CA 証明書。
proxy	(オプション) プロキシサーバーを使用している場合は、次のように記載します。 proxy：プロキシサーバーのホスト名または IP アドレス。

	proxy_port: プロキシサーバーのポート番号。 proxy_username: プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。 proxy_password: ユーザー名として指定したユーザーアカウントのパスワード。 user_agent: ユーザーエージェント名 (プロキシで事前定義されているユーザーエージェントが必要な場合)。 proxy_auth: プロキシで使用する認証方法。
aws_scanner	(オプション) Tenable Nessus スキャナーを AWS スキャナーとしてリンクするには、aws_scanner を **true** に設定します。 **注意:** このオプションは、Tenable Nessus スキャナーが AWS インスタンスですでに実行されていないと有効になりません。 **警告:** aws_scanner は、Amazon Linux 2023 AMI 環境ではサポートされていません。

環境設定

環境設定セクションでは、詳細な設定を行います。詳しくは、詳細設定を参照してください。

ユーザー

[user] (ユーザー) セクションでは、Tenable Nessus ユーザーを作成します。

設定	説明
username	Tenable Nessus ユーザーのユーザー名。
password	(オプションだが推奨) Tenable Nessus ユーザーのパスワード。 password の値を空にしてユーザーだけを作成した場合、Tenable Nessus は自動的にパスワードを生成します。そのユーザーでログインするには、nessuscli を

	使用して初めにユーザーのパスワードを変更してください。
`role`	ユーザーの役割。`[disabled]` (無効)、`[basic]` (基本)、`[standard]` (標準)、`[administrator]` (管理者)、`[system_administrator]` のいずれかに設定します。詳細については、ユーザーを参照してください。
`type`	`[local]` (ローカル) に設定します。

新しい Linux サーバーに Tenable Nessus を移行する

を使用する場合に必要な ユーザーロールTenable Nessus Manager: System Administrator

Linux にインストールされている Tenable Nessus スキャナーまたは Tenable Nessus Manager のライフサイクル中に、あるサーバーから別のサーバーへの移行が必要になる場合があります。次のトピックでは、同一プラットフォーム間、クロスプラットフォーム、クロスアーキテクチャの移行手順の概要と、いくつかの考慮事項を示します。

前提条件

ターゲットサーバーに Tenable Nessus のターゲットバージョンがサポートしているオペレーティングシステムがあり、他のすべてのシステム要件とハードウェア要件を満たしていることを確認してください。

次に、Tenable Nessus バージョンがソースサーバーとターゲットサーバーで同じであることを確認します。

`/opt/nessus/sbin/nessusd -v` コマンドを実行して、両方のサーバーのバージョンを確認します。ソースバージョンがターゲットバージョンよりも古い場合は、次のいずれかを実行します。

- ソースサーバーの Tenable Nessus をターゲットサーバーと同じバージョンにアップグレードします。
- ターゲットサーバーの Tenable Nessus をソースサーバーと同じバージョンにダウングレードします。
    - Tenable Core で Tenable Nessus をダウングレードするには、ターゲットサーバーで `pkexec /usr/libexec/tenablecore/backup/applicationDowngrade.sh` コマンドを実行し、ダウングレードする Tenable Nessus バージョンを選択してから、**[Enter]** を押します。

      注意: Tenable Core Oracle Linux 8 (OL8) のコックピットの制限により、Tenable Core OL8 のターミナルでこのコマンドを実行することはできません。代わりに Secure Shell (SSH) セッションで実行する必要があります。

- その他のオペレーティングシステムで Tenable Nessus をダウングレードするには、Tenable Nessus をアンインストールしてから、ソースサーバーのバージョンと一致するバージョンをインストールします。

データを転送する

次の 2 つのオプションのいずれかを使用して、ソースサーバーからターゲットサーバーにデータを転送します。どちらのオプションも、移行に必須ではない特定のディレクトリ (バックアップとログを含む) を除外します。それらのディレクトリは必要に応じて個別にバックアップしてください。リモート同期は、バックアップを作成、転送、復元する必要がないため、高速なオプションです。

注意

- すべてのコマンドは root として実行する必要があります。
- 非 root ユーザー (お使いのアカウントで sudo の権限昇格が許可されている) 場合、`sudo -i` コマンドを使用し、非 root ユーザーのパスワードを再度入力することで、root プロンプトに切り替えることができます。
- 一部のオペレーティングシステムでは、tar コマンドをコピーして貼り付けると、「*tar: 無効なオプション -- '▒'*」エラーが表示される場合があります。コマンドを手動で入力することで、この問題を解決できます。

オプション 1: バックアップと復元

1. 開始する前に、バックアップを作成するのに十分なディスク容量がソースサーバーにあることを確認してください。次のコマンドを実行すると、ファイルを作成せずにバックアップに必要な時間とディスク容量の両方を見積もることができます。

   ```
   time tar --exclude=
   {'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
   *','var/nessus/remote*','var/nessus/report-
   engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
   ssus/www*'} -Ppczf - /opt/nessus | wc -c | numfmt --to=iec-i
   ```

   出力の例

```
[root@ness01 ~]# time tar --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} -Ppczf - /opt/nessus | wc -c | numfmt --to=iec-i
43Mi

real 0m7.158s
user 0m7.074s
sys 0m0.362s
```

2. 次のコマンドを実行して、利用可能なマウントポイントのいずれかに、見積もられたサイズのバックアップを保存するのに十分なディスク容量があるかどうかを確認します。

```
df -h
```

3. 十分なディスク容量がある場合は、次のコマンドを実行してソースサーバーに適切なタイミングでバックアップを生成します。/path/to をバックアップを保存するのに十分なディスク容量があることを確認したパスに変更します。

```
service nessusd stop
tar --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} -Ppczf /path/to/nessus_backup.tar.gz /opt/nessus
```

4. 次のコマンドを実行して、十分なディスク容量があるターゲットサーバー上の場所に nessus_backup.tar.gz を転送します。

```
scp /path/to/nessus_backup.tar.gz root@:/path/to
```

出力の例

```
[root@ness01 ~]# scp /tmp/nessus_backup.tar.gz root@ness01_target:/tmp
The authenticity of host 'ness01_target (1.2.3.4)' can't be established.
```

```
ECDSA key fingerprint is SHA256:oarLiSLC4L+z8ts5/qAwhV9JYtqLNy8Eia1IBqh8gso.
ECDSA key fingerprint is MD5:32:3d:4b:3d:4b:e4:78:ce:4b:87:16:ce:f0:ac:f5:82.
Are you sure you want to continue connecting (yes/no)?〇
Warning: Permanently added 'ness01_target' (ECDSA) to the list of known hosts.
root@ness01_target's password:
nessus_backup.tar.gz 100% 3049MB 186.2MB/s 00:16
```

5. ターゲット サーバーで、次 のコマンドを実 行してバックアップを抽 出します。/path/to をターゲット サーバーに転 送されたバックアップパスに変 更します。

```
tar -xvf /path/to/nessus_backup.tar.gz -C /
```

オプション 2: リモート同 期

1. rsync がソースサーバーとターゲット サーバーの両 方 で使 用 可 能 であること、およびソースサーバーからターゲット サーバーに root としてログインできることを確 認します。rsync コマンドがいずれのサーバーでも出 力を返さない場 合 は、Red Hat ベースのオペレーティングシステムでは yum install rsync コマンド、Debian ベースのオペレーティングシステムでは dpkg -i rsync コマンドを実 行してインストールできます。

2. ソースサーバーで次 のコマンドを実 行して、同 期されないディレクトリを除き、Tenable Nessus によって消 費されるディスク容 量を確 認します。

```
du -sh --exclude
{"bin*","lib*","sbin*","var/nessus/backups*","var/nessus/logs*","var/nessus/plugin-
*","var/nessus/remote*","var/nessus/report-
engine*","var/nessus/templates/tmp*","var/nessus/tmp*","var/nessus/tools*","var/ne-
ssus/www*"} /opt/nessus
```

3. ターゲット サーバーに同 量 以 上 の空き容 量 があることを確 認してから、次 のコマンドを実 行してソースとターゲット の両 方 のサーバーでサービスを停 止します。

```
service nessusd stop
```

4. ソースサーバーで次 のコマンドを実 行して、ファイルをターゲット サーバーに同 期します。<target IP address> を実 際 のターゲット IP アドレスに変 更します。

```
rsync -ravz --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} /opt/nessus/* root@<target IP address>:/opt/nessus/
```

出力の例

```
[root@ness01 ~]# rsync -ravz --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} /opt/nessus/* root@1.2.3.4:/opt/nessus/
root@1.2.3.4's password:
sending incremental file list
etc/nessus/
etc/nessus/nessus-fetch.db
etc/nessus/nessus-fetch.db-shm
etc/nessus/nessus-fetch.db-wal
etc/nessus/nessusd.db
etc/nessus/nessusd.db-journal
var/nessus/
var/nessus/.__db_ok
var/nessus/global.db
var/nessus/global.db-shm
var/nessus/global.db-wal
var/nessus/nessus-service.version
var/nessus/nessus.version
var/nessus/tenable_links.json
var/nessus/tenable_rss_feeds.json
var/nessus/upgrades.db
var/nessus/users/
var/nessus/users/admin/
var/nessus/users/admin/policies.db
var/nessus/users/admin/auth/
var/nessus/users/admin/auth/admin
var/nessus/users/admin/auth/hash
var/nessus/users/admin/auth/rules
```

```
var/nessus/users/admin/reports/
var/nessus/users/admin/reports/361da43c-fda9-960c-49e8-
d52d3b60280b1d615196a27e8acb
var/nessus/users/admin/reports/361da43c-fda9-960c-49e8-
d52d3b60280b1d615196a27e8acb.name
var/nessus/users/admin/reports/361da43c-fda9-960c-49e8-
d52d3b60280b1d615196a27e8acb.ts
var/nessus/users/nessus_ms_agent/
var/nessus/users/nessus_ms_agent/tmp/
var/nessus/users/nessus_ms_agent/tmp/e5a9ba0be43e72ab/
var/nessus/users/test/
var/nessus/users/test/policies.db
var/nessus/users/test/auth/
var/nessus/users/test/auth/hash
var/nessus/users/test/auth/rules
var/nessus/users/test/files/
var/nessus/users/test/reports/
sent 2,317,224 bytes received 5,953 bytes 172,087.19 bytes/sec
total size is 335,189,932 speedup is 144.28
```

調整

ターゲットサーバーで次の手順を実行して、データの転送または復元後に一貫した正常な状態になるようにします。

1. nessuscli の実行時に FIPS モジュールエラーが表示されないようにし、正しいプラットフォーム固有のバイナリが配置されるようにするには、Red Hat または Debian ベースのオペレーティングシステム用の適切なコマンドを使用して、強制的な Tenable Nessus アップグレードを実行します。

   Red Hat ベースのオペレーティングシステム

   ```
   rpm -Uvh --force /tmp/Nessus-<version>.x86_64.rpm
   ```

   注意: Tenable Core の Oracle Linx 8 インスタンスで、`yum download Nessus` コマンドを実行して、最新の Tenable Nessus RPM ファイルを現在の作業ディレクトリにダウンロードできます。Tenable Core の古いインスタンスで `yumdownloader Nessus` を実行しても同じ結果が得られます。

   Debian ベースのオペレーティングシステム

```
dpkg --force-all -I /tmp/Nessus-<version>.amd64.deb
```

2. ターゲットサーバーで Tenable Nessus サービスを開始します。

```
service nessusd start
```

3. プラグインのダウンロードを許可し、「*Could not validate this preference file.Have installation files been copied from another system?*」(この環境設定ファイルを検証できませんでした。インストールファイルが別のシステムからコピーされていますか?) のエラーが出ないようにするため、Tenable Nessus にログインし、**[Settings]** (設定) > **[Overview]** (概要) に移動してライセンスを再度適用してください。同じライセンスを再利用するには、まず https://support.tenable.com でリセットしてください。ライセンスの適用後、Tenable Nessus でサインアウトします。

注意

- オンラインで更新するように設定されている場合、Tenable Nessus はその直後に更新を試行し、ログイン画面に「*Plugins are compiling, Nessus functions will limited be limited until compilation is complete*」(プラグインのコンパイル中です。Nessus の機能はコンパイルが完了するまで制限されます) と最大 20 分間表示されます。この間、backend.log には「*<[info] [globaldb] Waiting for Nessus to be ready>*」(<[info] [globaldb] Nessus の準備ができるまで待機します>) と記録されます。ログインしてデータがすべて揃っていることは確認できますが、これが完了するまでスキャンを実行することはできません。完了すると、ユーザーインターフェースには「*Plugins are doned compiling*」(プラグインのコンパイルが完了しました) と表示され、backend.log には「*[info] [globaldb] cleanup is starts*」([info] [globaldb] クリーンアップを開始しています) および他のアクティビティが表示されます。

  `tail -f /opt/nessus/var/nessus/logs/backend.log` コマンドを使用して、backend.log の進行状況を監視できます。

  該当する場合、Tenable Nessus Manager はエージェント DB ファイルの生成も開始します。これにはさらに 10 分かかります。次に、Tenable Nessus Manager により、フィードが新しいエージェントコアバージョンを提供しているかどうかが確認されます。新しいエージェントコアバージョンがある場合、ダウンロードされます。

- エアギャップ環境にある Tenable Nessus のインストールでは、プラグインの手動更新が必要です。プラグインの更新後、次のコマンドを使用して、Tenable Nessus Manager 用のエージェント DB ファイルの生成を強制的に行えます。

```
/opt/nessus/sbin/nessuscli manager generate-plugins -force
```

- Tenable Nessus Manager クラスタノード間の情報交換は、事前共有されたシークレットに依存しています。たとえば、`nessuscli fix --reset` を実行した場合や、新しい証明書が生成されたり、カスタム CA が Tenable Nessus Manager の親にアップロードされたりした場合、「*Invalid certificate signature*」(無効な証明書の署名) エラーが子ノードの backend.log に表示されることがあります。その場合は、Invalid Certificate signature on cluster nodes (クラスタノードでの無効な証明書の署名) に従い、事前共有されたシークレットをリセットし、ノード間の通信を再度有効にしてください。

ホスト名と IP アドレスを設定する

スタンドアロンの Tenable Nessus は、異なるホスト名や IP アドレスを使用する可能性があります。ただし、エージェントはどちらか一方にリンクされるため、Tenable Nessus Manager ターゲットサーバーはソースサーバーと同じ IP アドレスとホスト名を持つ必要があります。データを転送した後、ソースサーバーのホスト名と IP アドレスをメモしておきます。その後、ソースサーバーをシャットダウンして、そのホスト名と IP アドレスをターゲットサーバーに割り当てます。

注意

- Tenable Nessus Manager ターゲットサーバーに異なるホスト名や IP アドレスが使用されている場合、以前のホスト名または IP アドレスにリンクされたエージェントのコンソールではステータスがオフラインになります。これを修正するには、ターゲットサーバーに再リンクされる前に、各エージェントの Tenable タグ (/etc/tenable_tag または HKLM\SOFTWARE\Tenable\TAG) を削除する必要があります。
  - エージェントの再リンクを試みる前に Tenable タグを削除しないと、Tenable Nessus Manager にはすでに同じ Tenable タグの付いたエージェントがあるため 409 エラーが発生します。
  - Tenable タグを削除した後、`service nessusagent restart` を使用してエージェントサービスを再起動し、新しいタグを作成してください。
  - 新しい Tenable タグが付いたエージェントを再リンクすると、Tenable Nessus Manager コンソールのエージェントが更新されます。

次の 2 つのオプションのいずれかを使用して、ホスト名を設定します。

オプション 1: ターゲットサーバーでソースサーバーのホスト名を再利用する

1. ソースサーバーをシャットダウンします。
2. ターゲットサーバーで次のコマンドを root として実行し、ホスト名を変更します。

```
hostname <hostname>
```

> **注意:** ホスト名を変更しても、コマンドプロンプトには即座には反映されません。「exit」と入力してから再度ログインすると、新しいホスト名が表示されます。再起動後に新しいホスト名になっていない場合は、/etc/hostname の名前を直接変更してください。

オプション 2: ターゲットサーバーで新しいホスト名を使用する

1. ターゲットサーバーで root として以下のコマンドを実行し、目的のホスト名を設定します。

```
hostname <new hostname>
```

2. 「exit」と入力してから再度ログインすると、新しいホスト名が表示されます。

ターゲットサーバーの IP アドレスを変更するには、`ip a` 出力で変更する IP アドレスに関連付けられているインターフェース名を特定してから、Red Hat ベースのオペレーティングシステムでは /etc/sysconfig/network-scripts/ifcfg-*<network interface name>*、Debian ベースのオペレーティングシステムでは /etc/network/interfaces で IP アドレスを変更し、サーバーを再起動します。

権限のないユーザーとして Tenable Nessus を実行する

Tenable Nessus は、権限のないユーザーとして実行できます。

制限

- ローカルホストをスキャンする場合、Nessus プラグインは root として実行されていると想定します。したがって、特定タイプのスキャンは失敗する場合があります。たとえば、特権ユーザー以外で Nessus が実行される場合、プラグインがすべてのディレクトリにアクセスできないため、ファイルコンテンツのコンプライアンス監査は失敗するか、間違った結果を返すことがあります。
- `nessuscli` には `--no-root` モードはありません。root で `nessuscli` コマンドを実行すると、root が所有する Nessus インストールディレクトリにファイルが作成され、Nessus が正常にアクセスできなくなる可能性があります。`nessuscli` を実行する場合は注意が必要です。使用後に `chown` でアクセス許可を修正することもできます。

特権ユーザー以外のユーザーとして、Linux で Systemd を使って Nessus を実行する

制限

- ローカルホストをスキャンする場合、Nessus プラグインは root として実行されていると想定します。したがって、特定タイプのスキャンは失敗する場合があります。たとえば、特権ユーザー以外で Nessus が実行される場合、プラグインがすべてのディレクトリにアクセスできないため、ファイルコンテンツのコンプライアンス監査は失敗するか、間違った結果を返すことがあります。
- `nessuscli` には `--no-root` モードはありません。root として `nessuscli` を使用するコマンドを実行すると、root が所有する Nessus インストールディレクトリにファイルが作成され、Nessus がこれらのファイルに正常にアクセスできなくなる可能性があります。`nessuscli` を実行する場合は注意が必要です。使用後に `chown` でアクセス許可を修正することもできます。

手順

1. 次のいずれかを行います。
   - まだ行っていない場合は Nessus をインストールします。
   - Nessus をすでにインストールして実行している場合は、`nessusd` を停止します。
2. Nessus サービスを実行する root 以外のアカウントを作成します。

   ```
   sudo useradd -r -m nonprivuser
   ```

3. `/sbin` ディレクトリ内の Nessus バイナリに対する `world` アクセス許可を削除します。

   ```
   sudo chmod 750 /opt/nessus/sbin/*
   ```

4. `/opt/nessus` の所有権を非 root ユーザーに変更します。

   ```
   sudo chown nonprivuser:nonprivuser -R /opt/nessus
   ```

   注意: Tenable Nessus が更新されるたびに、ステップ 3 と 4 を完了する必要があります。

5. `nessusd` と `nessus-service` の機能を設定します。

ヒント: インターフェースをプロミスキャスモードにするには **cap_net_admin** を使用します。
パケットフォージェリ用の raw ソケットを作成するには、**cap_net_raw** を使用します。
リソース制限を設定するには、**cap_sys_resource** を使用します。

これが管理ツールにすぎず、この Nessus のインスタンスにスキャンを実行させない場合、このインスタンスにリソース制限の変更機能のみを付与する必要があります。

```
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessusd
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessus-service
```

この Nessus インスタンスにスキャンを実行させる場合は、パケットフォージェリを許可し、インターフェース上でプロミスキャスモードを有効にするためにさらにアクセス許可を追加する必要があります。

```
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessusd
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessus-service
```

6. 次の 2 つのコマンドを実行して、オーバーライド設定ファイルを作成します。

```
mkdir -p /etc/systemd/system/nessusd.service.d/
printf '[Service]\nExecStart=\nExecStart=/opt/nessus/sbin/nessus-service -q --no-
root\nUser=nonprivuser\n' > /etc/systemd/system/nessusd.service.d/override.conf
```

このファイルは、権限のない設定で nessusd サービスユニットファイル (/usr/lib/systemd/system/nessusd.service) 内の ExecStart オプションと User オプションをオーバーライドします。

7. 次のコマンドを実行して、systemd マネージャー設定を再読み込みし、オーバーライド設定ファイルを含めます。

```
sudo systemctl daemon-reload
```

8. 次のコマンドを実行して nessusd を開始します。

```
sudo service nessusd start
```

9. 次のコマンドを実行して、権限のないユーザーとして Tenable Nessus が実行されていることを確認します。

```
service nessusd status
```

権限のないユーザーで Tenable Nessus を実行している場合は、`override.conf` が `/etc/systemd/system/nessusd.service.d` の下に生成され、CGroup (コントロールグループ) に、`nessus-service` と `nessusd` の両方が `--no-root` パラメーターで開始されたことが示されます。

特権ユーザー以外のユーザーとして、Linux で init.d スクリプトを使って Nessus を実行する

制限

ローカルホストをスキャンする場合、Nessus プラグインは root として実行されていると想定します。したがって、特定タイプのスキャンは失敗する場合があります。たとえば、特権ユーザー以外で Nessus が実行される場合、プラグインがすべてのディレクトリにアクセスできないため、ファイルコンテンツのコンプライアンス監査は失敗するか、間違った結果を返すことがあります。

`nessuscli` には `--no-root` モードがないため、root として `nessuscli` を使用するコマンドを実行すると、root が所有する Nessus インストールディレクトリにファイルが作成され、Nessus がこれらのファイルに正常にアクセスできなくなる可能性があります。`nessuscli` を実行する場合は注意が必要です。使用後に `chown` でアクセス許可を修正することもできます。

手順

1. まだ行っていない場合は Nessus をインストールします。
2. Nessus サービスを実行する root 以外のアカウントを作成します。

```
sudo useradd -r -m nonprivuser
```

3. /sbin ディレクトリの Nessus バイナリで「world」アクセス許可を削除します。

```
sudo chmod 750 /opt/nessus/sbin/*
```

4. /opt/nessus の所有者を root ユーザー以外に変更します。

```
sudo chown nonprivuser:nonprivuser -R /opt/nessus
```

5. nessusd と nessus サービスの機能を設定します。

> **ヒント:**
>
> **cap_net_admin** を使用してインターフェースをプロミスキャスモードにします。
>
> パケットフォージェリ用の raw ソケットを作成するには、**cap_net_raw** を使用します。
>
> リソース制限を設定するには、**cap_sys_resource** を使用します。

これが管理ツールにすぎず、この Nessus インストールのインスタンスにスキャンを実行させない場合、このインスタンスにリソース制限の変更機能のみを付与する必要があります。

```
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessusd
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessus-service
```

この Nessus のインスタンスにスキャンを実行させる場合は、パケットフォージェリを許可し、インターフェースでプロミスキャスモードを有効にするための権限をさらに追加する必要があります。

```
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessusd
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessus-service
```

6. 次のラインを **/etc/init.d/nessusd** スクリプトに追加します。

CentOS

```
daemon --user=nonprivuser /opt/nessus/sbin/nessus-service -q -D --no-root
```

Debian

```
start-stop-daemon --start --oknodo --user nonprivuser --name nessus --
pidfile --chuid nonprivuser --startas /opt/nessus/sbin/nessus-service -- -q
-D --no-root
```

お使いのオペレーティングシステムに応じて、追加後のスクリプトは次のように表示されます。

CentOS

```
start() {
KIND="$NESSUS_NAME"
echo -n $"Starting $NESSUS_NAME : "
daemon --user=nonprivuser /opt/nessus/sbin/nessus-service -q -D --no-root
echo "."
return 0
}
```

Debian

```
start() {
KIND="$NESSUS_NAME"
echo -n $"Starting $NESSUS_NAME : "
start-stop-daemon --start --oknodo --user nonprivuser --name nessus --pidfile --
chuid nonprivuser --startas /opt/nessus/sbin/nessus-service -- -q -D --no-root
echo "."
return 0
}
```

7. nessusd を開始します。

   このステップで Nessus は root として開始しますが、init.d は Nessus を nonprivuser として開始させます。

   ```
   sudo service nessusd start
   ```

   注意：Debian で Nessus を実行している場合、Nessus の開始後に、chown -R nonprivuser:nonprivuser /opt/nessus コマンドを実行しランタイムに作成されたディレクトリの所有権を再取得します。

特権ユーザー以外のユーザーとして、macOS で Nessus を実行する

制限

- ローカルホストをスキャンする場合、Nessus プラグインは root として実行されていると想定します。したがって、特定タイプのスキャンは失敗する場合があります。たとえば、特権ユーザー以外で Nessus が実行される場合、プラグインがすべてのディレクトリにアクセスできないため、ファイルコンテンツのコンプライアンス監査は失敗するか、間違った結果を返すことがあります。
- nessuscli には --no-root モードはありません。root として nessuscli を使用するコマンドを実行すると、root が所有する Nessus インストールディレクトリにファイルが作成され、Nessus がこれらのファイルに適切にアクセスできなくなる可能性があります。nessuscli を実行する場合は注意が必要です。使用後に chown でアクセス許可を修正することもできます。

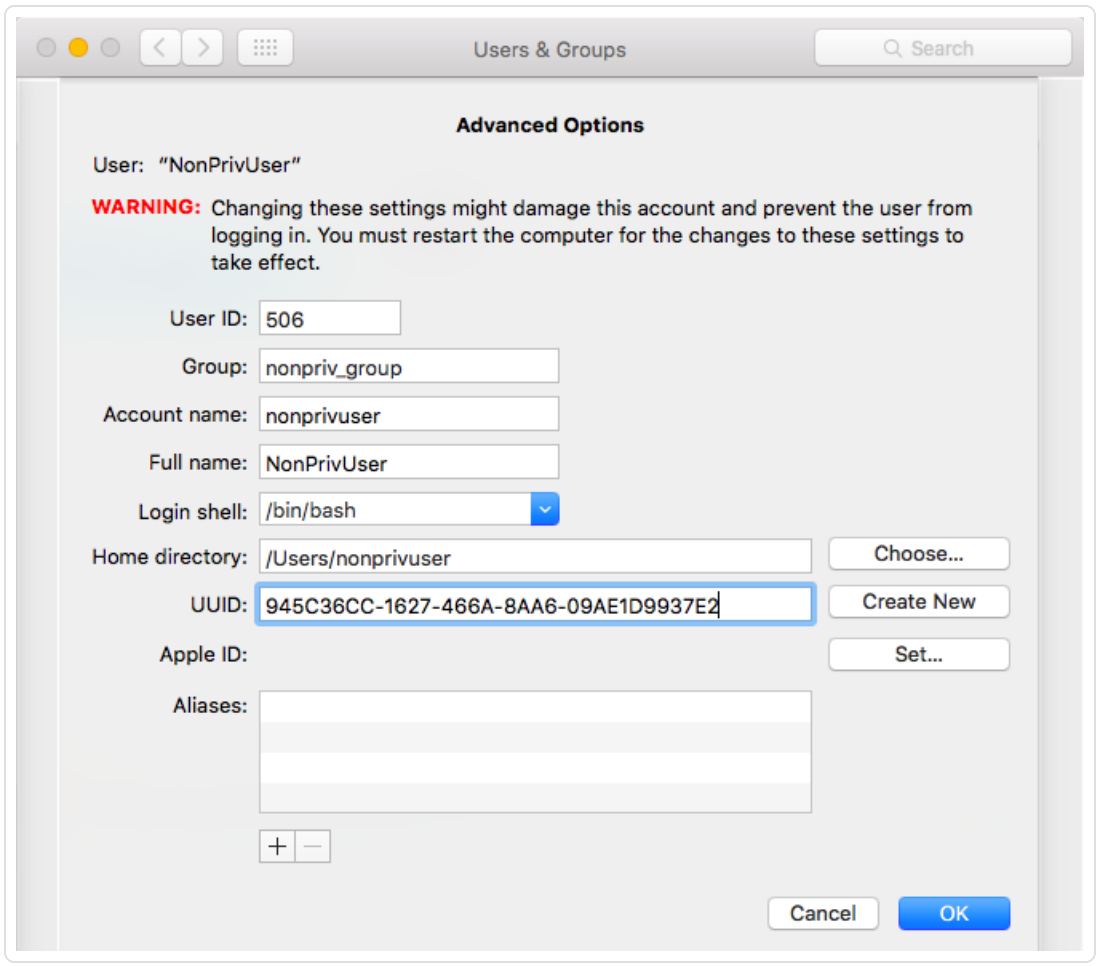
手順

1. まだ行っていない場合は Nessus を MacOSX にインストールします。
2. Nessus のサービスが root で実行されているので、アンロードする必要があります。

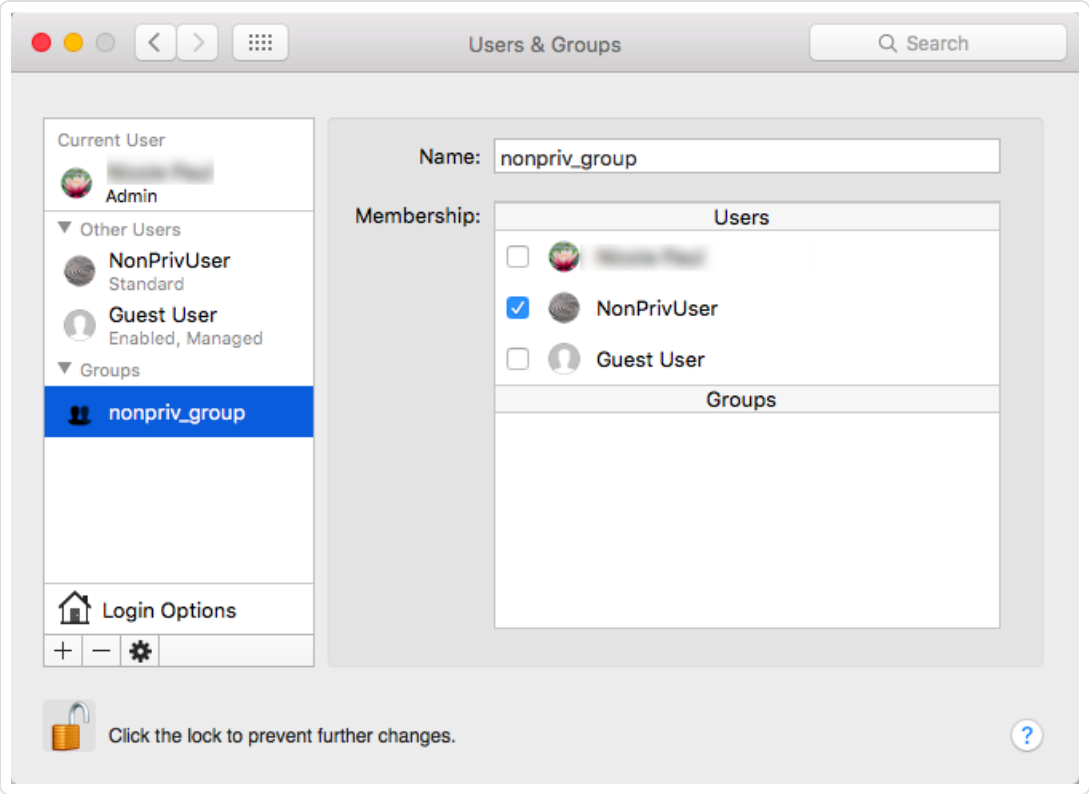
   次のコマンドを使用して、Nessus のサービスをアンロードします。

   ```
   sudo launchctl unload /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

3. Mac で、**[System Preferences] (システム環境設定) > [Users & Groups]** (ユーザーとグループ) の順に移動し、新しい**グループ**を作成します。
4. 次に、**[System Preferences] (システム環境設定) > [Users & Groups]** (ユーザーとグループ) の順に移動し、新しい**標準ユーザー**を作成します。権限のない Nessus アカウントとして実行するようにこのユーザーを設定します。



5. ステップ 1 で作 成したグループにこの新しいユーザーを追 加します。



6. /sbin ディレクトリの Nessus バイナリで「world」アクセス許可を削除します。

```
sudo chmod 750 /Library/Nessus/run/sbin/*
```

7. /Library/Nessus/run ディレクトリの所有者を、ステップ 2 で作成した root 以外 (標準) のユーザーに変更します。

```
sudo chown -R nonprivuser:nonprivuser /Library/Nessus/run
```

8. そのユーザーに /dev/bpf* デバイスへの読み取り/書き込み許可を付与します。これを簡単に実行する方法は、Wireshark のインストールです。これにより、access_bpf と呼ばれるグループと対応する起動デーモンが作成され、/dev/bpf* に適切なアクセス許可が開始時に設定されます。このケースでは、nonpriv ユーザーを access_bpf グループのメンバーに単純に割り当てることができます。この方法以外の場合、起動デーモンを作成して、「nonpriv」ユーザー (またはその一部であるグループ) にすべての /dev/bpf* への読み取り / 書き込み許可を付与する必要があります。

9. ステップ 8 の変更を有効にするために、システムを再起動します。

10. テキストエディターを使用して、Nessus の **/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist** ファイルを変更し、次のラインを追加します。**既存ラインは変更しないでください。**

```
<string>--no-root</string>
<key>UserName</key>
<string>nonprivuser</string>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Disabled</key>
        <true/>
        <key>Label</key>
        <string>com.tenablesecurity.nessusd</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Library/Nessus/run/sbin/nessus-service</string>
                <string>-q</string>
                <string>--no-root</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
      <key>UserName</key>
      <string>nonprivuser</string>
</dict>
</plist>
```

11. **sysctl** を使用して、次のパラメーターが最小値を持つことを確認します。

```
$ sysctl debug.bpf_maxdevices
debug.bpf_maxdevices:16384
$ sysctl kern.maxfiles
kern.maxfiles:12288
$ sysctl kern.maxfilesperproc
kern.maxfilesperproc:12288
$ sysctl kern.maxproc
kern.maxproc:1064
$ sysctl kern.maxprocperuid
kern.maxprocperuid:1064
```

12. ステップ 9 の値が最小要件を満たさない場合、次のステップに沿って値を変更します。

/etc/sysctl.conf ファイルを作成します。
テキストエディターを使用して、ステップ 9 で見つかった適切な値で systctl.conf ファイルを編集します。

例:

```
$ cat /etc/sysctl.conf
kern.maxfilesperproc=12288
kern.maxproc=1064
kern.maxprocperuid=1064
```

13. 次に、launchctl limit コマンドを使用して、お使いの OS のデフォルト値を確認します。

    例: MacOSX 10.10 と 10.11 の値。

```
$ launchctl limit
cpu unlimited unlimited
filesize unlimited unlimited
data unlimited unlimited
stack 8388608 67104768
core 0 unlimited
rss unlimited unlimited
memlock unlimited unlimited
maxproc 709 1064
maxfiles 256 unlimited
```

14. 手順 11 の値を上記の OSX デフォルト値に設定していない場合は、次の手順で値を変更します。

    テキストエディターを使用して、手順 11 に示している適切なデフォルト値を指定して launchd.conf ファイルを編集します。

    例:

```
$ cat /etc/launchd.conf
limit maxproc 709 1064
```

> **注意:** OSX の古いバージョンの中には maxproc の制限が小さいものがあります。お使いの OSX バージョンで /etc/launchctl.conf から制限を引き上げることができる場合、値を増加してください。

15. すべての変更を有効にするために、システムを再起動するか、起動デーモンをリロードします。

```
sudo launchctl load /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
```

Tenable Nessus 認証情報を使用したチェック

Tenable Nessus では、リモートスキャンに加えて、ローカルエクスポージャーをスキャンすることもできます。認証情報を使用したチェックの設定方法については、Windows での認証チェックおよび Linux での認証チェックを参照してください。

目的

外部ネットワークの脆弱性スキャンは、提供されているネットワークサービスとそれらのサービスに潜在する脆弱性の一定時点のスナップショットを取得するには有用です。しかし、これは外部ネットワークのスキャンに過ぎません。実行されているローカルサービスを判別し、ローカル攻撃によるセキュリティエクスポージャーや、外部スキャンで検出できない外部攻撃にシステムをさらす恐れのある設定を特定することが重要です。

一般的なネットワーク脆弱性評価では、外部の接続点に対してリモートスキャンが実行され、オンサイトスキャンはネットワーク内部で実行されます。こうしたスキャンでは、ターゲットシステムのローカルエクスポージャーは特定できません。取得される情報の一部はバナー情報に依存しており、不確定または不正確である場合があります。セキュアな認証情報を使用すると、ターゲットシステムをスキャンするためのローカルアクセス権を Nessus スキャナーに付与できるので、エージェントは不要になります。これにより、大規模なネットワークをスキャンしてローカルのエクスポージャーまたはコンプライアンス違反を検出する作業が簡単になります。

企業内で最も一般的なセキュリティ上の問題は、セキュリティパッチが適時に適用されていないことです。Nessus の認証情報を用いたスキャンでは、パッチのインストール日付が古いシステムを迅速に判断できます。これは、新たな脆弱性が公開され、その企業への影響について経営陣から早急な回答を求められる場合、特に重要です。

企業が懸念するもう 1 つの重要事項は、サイトポリシー、業界基準 (Center for Internet Security (CIS) ベンチマークなど)、または法律 (サーベンス・オクスリー法、グラム・リーチ・ブライリー法、HIPAA など) の順守を判断することです。クレジットカード情報を受け入れる企業は、クレジットカード業界 (PCI) 基準の順守を証明する必要がありますが、こうした顧客情報が数百万規模で漏洩した多数の事例が大きく報道されています。こうした事例では、支払いの補填、高額の罰金、または漏洩したカードの取扱店や決済業者のクレジットカードが受入不能となったことに対する補填責任を負う銀行に多額の金銭的損失が生じます。

アクセスレベル

認証情報を使用したスキャンでは、ローカルユーザーが実行できる任意の操作を実行できます。スキャンのレベルは、Tenable Nessus で使用するように設定したユーザーアカウントに付与する権限によって決まります。

Linux システムにローカルからアクセスする権限のないユーザーは、パッチレベルや /etc/passwd ファイルの入力内容といった基本的なセキュリティ問題のみを特定できます。システム全体のシステム設定データやファイルへのアクセス許可などのより包括的な情報には、「root」権限を持つアカウントが必要です。

Windows システムで認証スキャンを実行するには、Tenable Nessus でローカル管理者アカウントを使用する必要があります。Microsoft の一部の公開情報やソフトウェア更新プログラムでは、ソフトウェアをパッチレベルで判断するためにレジストリを読み取る作業について、管理者権限を信頼性維持の条件としています。ファイルシステムを直接読み取るために、Tenable Nessus にはローカル管理者権限が必要です。これにより、Nessus はコンピューターに接続し、ファイル分析を直接実行して、Tenable Nessus の評価対象システムの実際のパッチレベルを特定することができます。

認証情報エラーを検出する

Nessus を使用して Linux または Windows システムの認証情報監査を実行する場合、結果を分析して適切なパスワードと SSH キーを保有していたかどうかを判断するのは難しい可能性があります。プラグイン 21745 を使用すると、認証情報が機能していないかどうかを見極めることができます。

このプラグインは、SSH または Windows の認証情報によってスキャンがリモートホストにログインできなかった場合を検出します。ログインに成功した場合、結果を生成しません。

Windows での認証チェック

このドキュメントの手順に従って、ローカルセキュリティチェック用に Windows システムを設定します。

> **注意:** 一部のローカルチェックを実行する場合、Tenable Nessus ではホストで PowerShell 5.0 以降が実行されていることを必要とします。

前提条件

この処理を始める前に、次のような Windows での認証チェックをブロックする場所のセキュリティポリシーがないことを確認してください。

- Windows セキュリティポリシー
- ローカルコンピューターポリシー (たとえば、*このコンピューターへのネットワーク経由のアクセスを拒否*、、*ネットワーク経由でのアクセス*など)
- ウイルス対策またはエンドポイントのセキュリティルール
- IPS/IDS

認証スキャン用のアカウントを設定する

Windows 認証情報に関して最も重要なのは、チェックの実行に使用されるアカウントには、必要なすべてのファイルとレジストリエントリにアクセスする権限が必要であるということです。多くの場合、管理権限が必要となります。Tenable Nessus に管理アカウントの認証情報を提供しない場合、Nessus で実行できるのは、レジストリでパッチの有無をチェックすることだけです。これもインストール済みのパッチを確認するための有効な方法ではありますが、ポリシーにキーを設定しないサードパーティ製のパッチ管理ツールとは互換性がありません。Tenable Nessus に管理権限がある場合は、リモートホストのダイナミックリンクライブラリ (`.dll`) のバージョンをチェックできるので、はるかに精度が向上します。

以下のドロップダウンセクションでは、ユースケースに応じて Windows で認証情報を使用したチェックに使用するドメインまたはローカルアカウントを設定する方法について説明します。

> **注意:** ドメインコントローラーのスキャンに使用できるのはドメイン管理者アカウントだけです。

ユースケース 1: ローカル監査用のドメインアカウントを設定する

Windows サーバーのリモートホストベースの監査用のドメインアカウントを作成するには、サーバーがサポートされている Windows のバージョンであり、ドメインの一部である必要があります。ドメインアカウントからのログインを許可するようにサーバーを設定するには、次の手順のように、Classic セキュリティモデルを使用します。

1. **[Start]** (開始) メニューを開き、**[Run]** (実行) を選択します。
2. `gpedit.msc` と入力して **[OK]** をクリックします。
3. **[Computer Configuration]** (コンピューター設定) > **[Windows Settings]** (Windows 設定) > **[Security Settings]** (セキュリティ設定) > **[Local Policies]** (ローカルポリシー) > **[Security Options]** (セキュリティオプション) を選択します。

4. リストで **[Network access: Sharing and security model for local accounts]** (ネットワーク アクセス : ローカル アカウントの共有とセキュリティ モデル) を選択します。

   [Network access: Sharing and security model for local accounts] (ネットワーク アクセス : ローカル アカウントの共有とセキュリティ モデル) ウィンドウが表示されます。

5. [Local Security Setting] (ローカルセキュリティ設定) セクションのドロップダウンボックスで、**[Classic - local users authenticate as themselves]** (クラシック - ローカル ユーザーがローカル ユーザーとして認証する) を選択します。

   これにより、ドメインのローカルユーザーは、特定のサーバーで物理的にローカルでない場合でも、自分自身として認証することができます。この設定を行わない場合、ドメインの実際のユーザーであっても、リモートユーザーはすべてゲストとして認証されるので、リモート監査を実行するための十分な認証情報を持つことにはなりません。

6. **[OK]** をクリックします。

注意: スキャン認証情報の保護の詳細については、Windows ホストのスキャン認証情報を保護する 5 つの方法を参照してください。

ユースケース 2: ローカルアカウントを設定する

スタンドアロンの (つまり、ドメインに属していない) Windows サーバーに、認証情報を使用したチェックで使用するための認証情報を設定するには、管理者として一意のアカウントを作成します。

このアカウントの設定をデフォルトの **[Guest only: local users authenticate as guest]** (Guest のみ - ローカル ユーザーが Guest として認証する) に設定しないでください。代わりに、これを **[Classic: local users authenticate as themselves]** (クラシック - ローカル ユーザーがローカル ユーザーとして認証する) に切り替えます。

注意: 非常によくある間違いとして、リモートでログオンして有用な操作を実行するのに十分な権限がないローカルアカウントを作成してしまうことがあります。デフォルトでは、Windows は新しいローカルアカウントがリモートでログインする場合、ゲスト権限を割り当てます。これにより、リモートの脆弱性監査が正常に実行できなくなります。もう 1 つのよくある間違いは、ゲストユーザーに付与するアクセス権限を増やすことです。これにより、Windows Server のセキュリティが低下します。

「Nessus Local Access」セキュリティグループを作成する

1. Domain Controller にログインして、**[Active Directory Users and Computers]** (Active Directory ユーザーとコンピューター) を開きます。
2. セキュリティグループを作成するには、**[Action]** (アクション) > **[New]** (新規) > **[Group]** (グループ) を選択します。
3. グループに **Nessus Local Access** という名前を付けます。**[Scope]** (範囲) を **[Global]** (グローバル) に、**[Type]** (タイプ) を **[Security]** (セキュリティ) に設定します。
4. Tenable Nessus Windows 認証スキャンを実行するために使用するアカウントを Tenable Nessus Local Access グループに追加します。

「Nessus Scan GPO」グループポリシーを作成する

1. グループポリシー管理コンソールを開きます。
2. **[Group Policy Objects]** (グループポリシーオブジェクト) を右クリックして、**[New]** (新規) を選択します。
3. **Nessus Scan GPO** のポリシー名を入力します。

「Nessus Local Access」グループを「Nessus Scan GPO」ポリシーに追加する

1. **[Nessus Scan GPO Policy]** (Nessus Scan GPO ポリシー) を右クリックして、**[Edit]** (編集) を選択します。
2. **[Computer configuration]** (コンピューターの設定) > **[Policies]** (ポリシー) > **[Windows Settings]** (Windows の設定) > **[Security Settings]** (セキュリティ設定) > **[Restricted Groups]** (制限されたグループ) を展開します。
3. **[Restricted Groups]** (制限されたグループ) の左側のナビゲーションバーで右クリックして、**[Add Group]** (グループの追加) を選択します。
4. **[Add Group]** (グループの追加) ダイアログボックスで **[browse]** (参照) を選択し、**Nessus Local Access** と入力します。
5. **[Check Names]** (名前の確認) を選択します。
6. **[OK]** を 2 回クリックして、ダイアログボックスを閉じます。
7. **[This group is a member of:]** (このグループがメンバーである) で **[Add]** (追加) を選択します。

8. **[Administrators]** (管理者) グループを追加します。
9. **[OK]** を 2 回選択します。

Tenable Nessus は、サーバーメッセージブロック (SMB) と Windows Management Instrumentation (WMI) を使用します。Windows ファイヤーウォールがシステムへのアクセスを許可していることを確認します。

Windows で WMI を許可する

1. **[Nessus Scan GPO Policy]** (Nessus Scan GPO ポリシー) を右クリックして、**[Edit]** (編集) を選択します。
2. **[Computer configuration]** (コンピューターの設定) > **[Policies]** (ポリシー) > **[Windows Settings]** (Windows の設定) > **[Security Settings]** (セキュリティ設定) > **[Windows Firewall with Advanced Security]** (Windows ファイヤーウォールの詳細設定) > **[Windows Firewall with Advanced Security]** (Windows ファイヤーウォールの詳細設定) > **[Inbound Rules]** (インバウンドルール) を展開します。
3. 作業領域を右クリックして、**[New Rule...]** (新しいルール...) を選択します。
4. **[Predefined]** (事前定義) オプションを選択し、ドロップダウンボックスから **[Windows Management Instrumentation (WMI)]** を選択します。
5. **[Next]** (次へ) を選択します。
6. 次のチェックボックスを選択します。
    - Windows Management Instrumentation (ASync-In)
    - Windows Management Instrumentation (WMI-In)
    - Windows Management Instrumentation (DCOM-In)
7. **[Next]** (次へ) を選択します。
8. **[Finish]** (終了) を選択します。

ヒント: 後で作成された定義済みルールを編集し、IP アドレスとドメインユーザーによってポートへの接続を制限することで、WMI を悪用するリスクを減らすことができます。

GPO をリンクする

1. グループポリシー管理コンソールで、ドメインまたは OU を右クリックし、**[Link an Existing GPO]** (既存の GPO をリンクする) を選択します。
2. **[Nessus Scan GPO]** を選択します。

Windows を設定する

認証情報を使用したチェック用の適切なアカウントを作成したら、スキャンする前に、いくつかの Windows オプションを設定する必要があります。

(ローカルアカウントのみ) ユーザーアカウント制御 (UAC)

Windows ユーザーアカウント制御 (UAC) を無効にするか、Tenable Nessus 監査を許可する特定のレジストリ設定を変更する必要があります。UAC を無効にするには、コントロールパネルを開き、**[User Accounts]** (ユーザーアカウント) を選択して、**[Turn User Account Control]** (ユーザーアカウント制御) を **[Off]** (オフ) に設定します。

UAC を無効にする代わりの方法として、Tenable は、**LocalAccountTokenFilterPolicy** という名前の新しいレジストリ DWORD を追加し、その値を **1** に設定することをお勧めします。このキーは、レジストリ `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy` で作成します。このレジストリ設定の詳細については、MSDN 766945 KB を参照してください。

> **ヒント:** UAC を完全にオフにするには、**[Control Panel]** (コントロールパネル) を開き、**[User Accounts]** (ユーザーアカウント) を選択して、[Turn User Account Control to off] (ユーザーアカウント制御) をオフに設定します。または、LocalAccountTokenFilterPolicy という名前の新しいレジストリキーを追加し、その値を 1 に設定します。
>
> このキーは、レジストリの `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy` で作成する必要があります。
>
> このレジストリ設定の詳細については、MSDN 766945 KB を参照してください。Windows 7 および 8 では、UAC を無効にした場合、`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System` の EnableLUA も **0** に設定する必要があります。

ホストファイヤーウォール

- **[Run]** (実行) プロンプトで `gpedit.msc` を実行して、**[Group Policy Object Editor]** (グループポリシーオブジェクトエディター) を有効にします。**[Local Computer Policy]** (ローカルコンピューターポリシー) > **[Administrative Templates]** (管理用テンプレート) > **[Network]** (ネットワーク) >

[Network Connections] (ネットワーク接続) > **[Windows Firewall]** (Windows ファイヤーウォール) > **[Standard Profile]** (標準プロファイル) > **[Windows Firewall: Allow inbound file and printer exception]** (Windows ファイヤーウォール: 着信ファイルとプリンタの共有の例外を許可する) に移動し、これを有効にします。

[Group Policy Object Editor] (グループ ポリシー オブジェクト エディター) で、**[Local Computer Policy]** (ローカル コンピューター ポリシー) > **[Administrative Templates]** (管理用テンプレート) > **[Network]** (ネットワーク) > **[Network Connections]** (ネットワーク接続) > **[Prohibit use of Internet connection firewall on your DNS domain]** (DNS ドメイン ネットワーク上でのインターネット接続ファイヤーウォールの使用を禁止する) に移動します。このオプションを **[Disabled]** (無効) または **[Not Configured]** (未設定) のどちらかに設定します。

- **[Windows Firewall]** (Windows ファイヤーウォール) > **[Windows Firewall Settings]** (Windows ファイヤーウォール設定) で、**[File and Printer Sharing]** (ファイルとプリンターの共有) を有効にします。ホストのファイヤーウォールを開き、TCP ポート **139** および **445** で Tenable Nessus から **[File and Printer Sharing]p** (ファイルとプリンターの共有) への接続を許可します。Tenable Nessus がホスト上で開いている任意のポートやサービスを選べるようにしたい場合は、これらのポートからもスキャナーにアクセスできる必要があります。

リモートレジストリ

[Remote Registry] (リモートレジストリ) を有効にします (デフォルトでは無効)。このサービスは、単発の監査のためにその時だけ有効にすることも、頻繁な監査に対応するために常に有効にすることもできます。

> **注意:** このオプションを有効にすると、スキャンを開始する前にリモートレジストリサービスの開始を試みるように Tenable Nessus が設定されます。
>
> Tenable Nessus スキャンポリシーで指定する Windows 認証情報は、スキャン対象のホストでリモートレジストリサービスを開始するための管理アクセス許可を持つものでなければなりません。

サービスが (*有効*ではなく) *手動*に設定されている場合、プラグイン ID 42897 および 42898 は、スキャンの間だけレジストリを有効にします。

> **注意:** スキャン中にリモートレジストリを有効にする方法については、スキャンポリシーの [Start the Remote Registry service during the scan] (スキャン中にリモートレジストリを有効にする) オプションを有効にする方法を参照してください。

管理共有

AutoShareServer (Windows Server) または **AutoShareWks** (Windows Workstation) のいずれかを使用して、以下のデフォルトの管理共有を有効にします。

- **IPC$**
- **ADMIN$**

  > **注意:** Windows 10 では、**ADMIN$** はデフォルトで無効になっています。他のすべてのオペレーティングシステムでは、3 つの共有はデフォルトで有効になっており、デフォルトで無効にすると別の問題が発生する可能性があります。詳細については、Windows ドキュメントの Overview of problems that may occur when administrative shares are missing (管理共有が見つからない場合に発生する可能性がある問題の概要) を参照してください。

- **C$**

次の手順

- Windows ログイン用に Tenable Nessus スキャンを設定する

Windows ログイン用に Tenable Nessus スキャンを設定する

Tenable Nessus では、Windows ログインに必要な認証情報を使用してスキャン設定を行うことができます。これはスキャンの作成プロセス中に行うことも、既存のスキャン設定に認証情報を追加することもできます。

開始する前に、Windows での認証チェックの説明に従って、認証スキャン用に Windows システムを設定します。

Windows ログイン用に Tenable Nessus スキャン設定を行う方法

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 次のいずれかを行います。

   - **[New Scan]** (新しいスキャン) をクリックして新しいスキャンを作成し、テンプレートを選択します。
   - 左側のナビゲーションバーで **[My Scans]** (マイスキャン) をクリックし、既存のスキャンを選択して、**[Configure]** (設定) ボタンをクリックします。

3. スキャン設定で、**[Credentials]** (認証情報) タブをクリックします。

[Credentials] (認証情報) メニューが開きます。

4. [Categories] (カテゴリ) ドロップダウンメニューで **[Host]** (ホスト) を選択します。
5. [Host] (ホスト) カテゴリで **[Windows]** をクリックします。

   Windows 認証情報ペインが表示されます。
6. 認証方法を選択します。認証方法に応じて、残りの Windows 設定が変更されます。
7. 認証方法に応じて、SMB アカウントのユーザー名、パスワードまたはハッシュ、ドメインを指定します。

   Windows 認証情報設定の説明を表示するには、Windows を参照してください。
8. **[Save]** (保存) をクリックします。Tenable Nessus で新しい Windows 認証情報が保存されます。

macOS での認証チェック

このドキュメントの手順に従って、ローカルセキュリティチェックを実行できるよう macOS システムを設定します。SSH 秘密/公開鍵のペア、またはユーザー認証情報と sudo か su アクセスを使用して、ローカルセキュリティチェックを有効にできます。

このドキュメントでは、サンプルの SSH デーモンとして OpenSSH が使用されています。SSH の商用版を使用している場合、手順が若干異なる場合があります。

前提条件

SSH の設定要件

特定のタイプの暗号を受け入れるように SSH サーバーを設定することができます。ただし、一部の商用 SSH バリアントは、blowfish-cbc をサポートしていません。お持ちの SSH サーバーが、使用するアルゴリズムをサポートしていることを確認してください。

Tenable Nessus は、blowfish-cbc、aesXXX-cbc (aes128、aes192、aes256)、3des-cbc、aes-ctr のアルゴリズムをサポートしています。

ユーザー権限

ユーザー権限の最大の効果を生み出すには、SSH ユーザーはあらゆるコマンドをシステムで実行できる必要があります。macOS システムでは、SSH ユーザーは **Administrator** グループのメンバーであり、フル

ディスクアクセス権を持っている必要があります。特権アクセスでなくても実行できるパッチレベルなどのチェックもありますが、システム設定とファイルアクセス許可を監査する完全なコンプライアンスチェックにはフルディスクアクセス権が必要です。このため、Tenable は、できれば認証情報ではなくSSH 鍵を使用することをお勧めします。

Kerberos の設定要件

Kerberos を使用している場合、Kerberos をサポートして KDC でチケットを検証できるように sshd を設定する必要があります。これを機能させるには、逆引き DNS ルックアップを適切に設定する必要があります。Kerberos のインタラクション方法は、gssapi-with-mic である必要があります。

SSH の公開鍵と秘密鍵の生成

Tenable Nessus スキャナーの秘密鍵/公開鍵ペアを生成します。この鍵ペアは Tenable Nessus スキャナーから生成できます。このドキュメントでは、スキャナーが Linux で実行されていることを前提としていますが、任意のユーザーアカウントを使用して、どの macOS システムでも同じ手順を実行することができます。

注意: 定義済みの Tenable Nessus のユーザーは、この生成された鍵を所有している必要があります。

鍵ペアを生成するには、ssh-keygen を使用し、鍵を安全な場所に保存します。次の例をご覧ください。

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter the file in which to save the key (/Users/test/.ssh/id_dsa):
/home/test/Nessus/ssh_key
Enter the passphrase (empty for no passphrase):
Enter the same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

Tenable Nessus を実行しているシステムサーバー以外のシステムに秘密鍵を移動しないでください。ssh-keygen からパスフレーズの入力を求められたときには、強力なパスフレーズを入力するか、**Return** キーを 2 回押します (つまり、パスフレーズを設定しません)。パスフレーズを指定する場合は、**[Policies]**

(ポリシー) > **[Credentials]** (認証情報) > **[SSH settings]** (SSH 設定) で指定し、お使いの Tenable Nessus スキャン設定で鍵ベースの認証を使用できるようにする必要があります。

ユーザーアカウントの作成

ローカルセキュリティチェックを使用してスキャンするすべてのターゲットシステムで、Tenable Nessus 専用の新しいユーザーアカウントを作成します。このユーザーアカウントの名前は、すべてのシステムで同じ名前にする必要があります。Tenable Nessus がリモート認証スキャンを実行できるよう、このアカウントに **Administrator** 権限と **Remote Login** 権限を付与する必要があります。

macOS のリモートログインの設定

ホストの macOS システムで、**[Remote Login]** (リモートログイン) システム設定の **[Allow full disk access for the remote users]** (リモートユーザーのフルディスクアクセス権を許可する) を有効にします。これにより、以降の手順で必要になる `sshd-keygen-wrapper` へのフルディスクアクセス権が有効になります。

次に、**[Privacy and Security]** (プライバシーとセキュリティ) で、関連するシステムサービスに**フルディスクアクセス権**を付与し、プラグインがファイルシステム全体を検索できるようにします。次のサービスが含まれていることを確認してください。

- `/Library/NessusAgent/run/sbin/nessus-service`
- `/usr/libexec/sshd-keygen-wrapper`

SSH 鍵の設定

次の例に示すように、公開鍵を、鍵が保存されているシステムから、ホストチェックのためにスキャンするシステムに安全にコピーします。このドキュメントでは、このユーザーを `nessus` としますが、任意の名前を使用できます。

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

安全な ftp コマンド **`sftp`** を使用して、Tenable Nessus をインストールしたシステムからこのファイルをコピーすることもできます。その場合は、ターゲットシステムでこのファイル名を `authorized_keys` にする必要があります。

公開鍵システムに戻る

/home/nessus/.ssh ディレクトリと authorized_keys ファイルの両方に対するアクセス許可を設定します。

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

SSH チェックのテストをするすべてのシステムでこのプロセスを繰り返します (ユーザーアカウントの作成 ステップから開始します)。

SSH 鍵のテスト

次に、アカウントとネットワークが正しく設定されていることを確認するためにテストします。Tenable Nessus スキャナーからシンプルなコマンド id を使用して、次のコマンドを実行します。

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

Tenable Nessus スキャナーから Tenable Nessus ユーザーに関する情報が正常に返された場合、設定が成功したことになります。

次の手順

- macOS ログインできるように Tenable Nessus を設定します。

Linux での認証チェック

このドキュメントの手順に従って、ローカルセキュリティチェック用に Linux システムを設定します。以下の例で使用される SSH デーモンは OpenSSH です。SSH の商用版を使用している場合、手順がわずかに異なる場合があります。

SSH 秘密/公開鍵のペアまたはユーザー認証情報と sudo または su アクセスを使用して、ローカルセキュリティチェックを有効にできます。

注意: Tenable Nessus で Linux マシンをスキャンする場合、Linux マシンのシェル設定ファイルには 4 文字以上の PS1 変数 (例: `PS1='\u@\h:~\$ '`) が必要です。4 文字未満の PS1 変数 (例: `PS1='\$ '`) があると、全体のスキャン時間が大幅に増加する可能性があります。

前提条件

SSH の設定要件

Tenable Nessus は、blowfish-cbc、aesXXX-cbc (aes128、aes192、aes256)、3des-cbc、aes-ctr のアルゴリズムをサポートしています。

商用版の SSH の一部は、おそらく輸出上の制約から blowfish cipher をサポートしていません。特定の種類の暗号のみを受け入れるように SSH サーバーを設定することもできます。お使いの SSH サーバーが適切なアルゴリズムをサポートすることを確認してください。

ユーザー権限

ユーザー権限の最大の効果を生み出すには、SSH ユーザーはあらゆるコマンドをシステムで実行できる必要があります。Linux システムでは、SSH ユーザーは `root` 権限を持っている必要があります。権限なしで実行できるチェックもありますが (パッチレベルなど)、監査システム設定とファイル権限の完全なコンプライアンスチェックには root 権限が必要です。そのため、Tenable は、可能な限り認証情報ではなく SSH 鍵を使用することをお勧めします。

Kerberos の設定要件

Kerberos を使用している場合、Kerberos をサポートして KDC でチケットを検証できるように `sshd` を設定する必要があります。これを機能させるには、逆引き DNS ルックアップを適切に設定する必要があります。Kerberos のインタラクション方法は、**`gssapi-with-mic`** である必要があります。

SSH ローカルセキュリティチェックを有効にする

このセクションでは、Tenable Nessus の認証情報チェックに関与するシステム間の SSH を有効にするための大まかな手順を説明します。これは SSH に関する詳細なチュートリアルではなく、Linux システムのコマンドに関する知識をあらかじめ持っているユーザーを対象としています。

SSH の公開鍵と秘密鍵の生成

最初の手順は、Tenable Nessus スキャナーで使用する秘密鍵/公開鍵のペアを生成することです。この鍵のペアは、任意の Linux システムで任意のユーザーアカウントを使用して生成できます。ただし、定義済みの Tenable Nessus ユーザーが鍵を所有することが重要です。

鍵のペアを生成するには、ssh-keygen を使用し、安全な場所に鍵を保管します (次の Red Hat ES 3 インストール環境での例を参照してください)。

```
# ssh-keygen -t ecdsa -b 521
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/test/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/test/.ssh/id_ecdsa
Your public key has been saved in /home/test/.ssh/id_ecdsa.pub
The key fingerprint is:
SHA256:xL27sSSquFGQ2jhemuZGDdtt8lXL3nuUcOVrDIHtfi0 test@ubuntu2204-test
The key's randomart image is:
+---[ECDSA 521]---+
| o |
| . . . . o . |
| o o . . + |
| = . . . o + . |
|+ *.o S o + + o|
|.++= o . o . +E=.|
|.=.+ . o = . o.|
|o.o . . + = . |
|..o....o.o |
+----[SHA256]-----+
#
```

注意: SSH サーバーへの認証時に SSH キーの互換性の問題が発生する場合は、ecdsa の代わりに dsa コマンドを使用してキーを生成できます。

```
ssh-keygen -t dsa
```

Tenable Nessus を実行しているシステムサーバー以外のシステムに秘密鍵を移動しないでください。ssh-keygen からパスフレーズの入力を求められたときには、強力なパスフレーズを入力するか、**Return** キーを 2 回押します (つまり、パスフレーズを設定しません)。パスフレーズを指定する場合は、Tenable Nessus が鍵ベースの認証を使用できるように、**[Policies]** (ポリシー) > **[Credentials]** (認証情報) > **[SSH settings]** (SSH 設定) で指定する必要があります。

ユーザーアカウントを作成し、SSH 鍵を設定する

ローカルセキュリティチェックを使用してスキャンするすべてのターゲットシステムで、Tenable Nessus 専用の新しいユーザーアカウントを作成します。このユーザーアカウントの名前は、すべてのシステムで完全に同じにする必要があります。このドキュメントでは、このユーザーの名前を nessus としますが、任意の名前を使用できます。

ユーザーアカウントを作成したら、アカウントに有効なパスワードが設定されていないことを確認します。Linux システムでは、初期パスワードを明示的に設定した場合を除き、新しいユーザーアカウントはデフォルトではロックされています。パスワードが設定されているアカウントを使用する場合は、passwd -l コマンドを使用してアカウントをロックします。

また、この新しいアカウントのホームディレクトリの下に、公開鍵を保存するディレクトリを作成する必要があります。この演習では、そのディレクトリは /home/nessus/.ssh です。次の Linux システムの例を参照してください。

```
# passwd -l nessus
# cd /home/nessus
# mkdir .ssh
#
```

Solaris 10 システムでは、ロックされているアカウントと非ログインアカウントを区別するために passwd(1) コマンドが強化されています。これは、ロックされているユーザーアカウントがコマンドの実行 (クローンジョブなど) に使用されないようにするためです。非ログインアカウントは、コマンドの実行にのみ使用でき、インタラクティブなログインセッションをサポートしません。このようなアカウントは、/etc/shadow のパスワードフィールドに「NP」トークンがあります。Solaris 10 で非ログインアカウントを設定し、SSH パブリックキーディレクトリを作成するには、次のコマンドを実行します。

```
# passwd -N nessus
# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

これでユーザーアカウントが作成されました。次は、鍵をシステムに移動して適切なディレクトリに配置し、適切なアクセス許可を設定する必要があります。

例

次の例に示すように、鍵が保存されているシステムから、ホストチェックでスキャンするシステムに公開鍵を安全にコピーします。

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

安全な ftp コマンド **sftp** を使用して、Tenable Nessus をインストールしたシステムからこのファイルをコピーすることもできます。その場合は、ターゲットシステムでこのファイル名を authorized_keys にする必要があります。

公開鍵システムに戻る

/home/nessus/.ssh ディレクトリと authorized_keys ファイルの両方に対するアクセス許可を設定します。

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

SSH チェックのテストをするすべてのシステムでこのプロセスを繰り返します (ユーザーアカウントを作成し、SSH 鍵を設定するから開始します)。

アカウントとネットワークが正しく設定されていることをテストして確認します。Tenable Nessus スキャナーからシンプルな Linux コマンド id を使用して、次のコマンドを実行します。

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

Tenable Nessus ユーザーに関する情報が正常に返された場合、キーの交換は成功です。

次の手順

- SSH ホストベースのチェック用に Tenable Nessus を設定する

SSH ホストベースのチェック用に Tenable Nessus スキャンを設定する

を使用する場合に必要なユーザーロールTenable Nessus Manager: Standard、Administrator、System Administrator

Tenable Nessus では、ローカルの macOS または Linux チェックに必要な認証情報を使用してスキャン設定を行うことができます。これはスキャンの作成プロセス中に行うことも、既存のスキャン設定に認証情報を追加することもできます。

まだ実行していない場合は、ホストのオペレーティングシステムに応じて macOS での認証チェック または Linux での認証チェック の手順を実行し、認証スキャン用にホストシステムを設定します。

以下の手順で、Tenable Nessus ユーザーインターフェースで SSH ホストベースのチェックを設定できます。

1. 上部のナビゲーションバーで、**[Scans]** (スキャン) をクリックします。

   [My Scans] (マイスキャン) ページが表示されます。

2. 次のいずれかを行います。

   - **[New Scan]** (新しいスキャン) をクリックして新しいスキャンを作成し、テンプレートを選択します。
   - 左側のナビゲーションバーで **[My Scans]** (マイスキャン) をクリックし、既存のスキャンを選択して、**[Configure]** (設定) ボタンをクリックします。

3. **[Credentials]** (認証情報) タブをクリックします。
4. **[SSH]** を選択します。
5. **[Authentication method]** (認証方法) ドロップダウンボックスで、認証方法を選択します。
6. 残りの設定を行います。
7. **[Save]** (保存) ボタンをクリックします。