Tenable Vulnerability Management ユーザーガイド

最終更新日: 2024 年 4 月 5 日

目次

Tenable Vulnerability Management にようこそ

Tenable Vulnerability Management® (旧 Tenable.io) 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、Tenable Nessus Agent および Tenable Nessus Network Monitor スキャナー、スキャンスケジュール、スキャンポリシーならびにスキャン結果を無制限の数のユーザーやグループの間で共有できます。

注意: Tenable Vulnerability Management は、単独で、または Tenable One パッケージの一部として購入できます。詳細については、Tenable One を参照してください。

ヒント: *Tenable Vulnerability Management ユーザーガイド*は、英語と日本語で提供されています。Tenable Vulnerability Management ユーザーインターフェースは、英語、日本語、フランス語で提供されています。ユーザーインターフェースの言語を切り替えるには、言語 を参照してください。

Tenable Vulnerability Management の詳細は、次の顧客教育資料で確認してください。

- Tenable Vulnerability Management セルフヘルプガイド
- Tenable Vulnerability Management はじめに (Tenable University)

Tenable One サイバーエクスポージャー管理プラットフォーム

Tenable One は、サイバーエクスポージャー管理プラットフォームです。DX 時代のアタックサーフェス全体の可視化、起こり得る攻撃を防ぐための取り組みへのフォーカス、サイバーリスクの正確な伝達を支援することで、最大限のビジネスパフォーマンスを発揮できるようにします。

このプラットフォームは、Tenable Research による高速で広範な脆弱性カバレッジを基盤として構築されており、IT 資産、クラウドリソース、コンテナ、ウェブアプリケーション、ID システムを含む、業界で最大の網羅性を誇る脆弱性カバレッジを提供します。また、包括的な分析機能が作業の優先順位付けを可能にし、サイバーリスクを伝達します。Tenable One を利用する組織は、以下のことが行えます。

- DX 時代のアタックサーフェス全体を包括的に可視化
- 起こり得る脅威に先駆けた攻撃防止対策の優先順位付け
- より適切な判断を可能にするサイバーリスクの伝達

Tenable Vulnerability Management はスタンドアロン製品として存在しますが、Tenable One サイバーエクスポージャー管理プラットフォームの一部としても購入できます。

ヒント: Tenable One 製品の使用開始の詳細については、「Tenable Oneデプロイメントガイド」を参照してください。

Tenable Vulnerability Management

動画: Tenable Vulnerability Management の紹介

Tenable Vulnerability Management を使い始める

Tenable Vulnerability Management はさまざまなリソースをユーザーおよびグループ内で共有することによって、個別のニーズに応じた脆弱性管理プログラムのワークフローを無制限に作成でき、ビジネスの安全性を保つための多くの規則やコンプライアンス要件に対応します。

Tenable Vulnerability Management ではクラウドを通じて、スキャンのスケジュール化、ポリシーの推進、スキャン結果の表示、および複数の Tenable Nessus スキャナーの管理ができます。これにより、パブリッククラウド、プライベートクラウド、複数の物理ロケーションにわたるネットワークへの Tenable Nessus スキャナーのデプロイメントが可能になります。

Tenable Lumin

Tenable Lumin を使い始める

Tenable Lumin の機能は Tenable Vulnerability Management のデータを強化します。Tenable Lumin を使用すると、エクスポージャーリスクを素早く正確に評価でき、企業の正常性や修正状況を Salesforce 業界および全体の他の Tenable ユーザーと比較できます。

Tenable Lumin は、未加工の脆弱性データを資産のビジネス上の重要度や脅威の文脈データと関連付けることで、従来の脆弱性管理ツールよりも高速かつターゲットを絞った分析ワークフローをサポートします。

Tenable Web App Scanning

Tenable Web App Scanning は、Tenable Nessus スキャナーが提供する既存の**ウェブアプリケーションテスト**ポリシーのテンプレートを大幅に改善します。今までのテンプレートでは、Javascript に依存した、HTML5 で構築されている最新のウェブアプリケーションに対応できず、お使いのウェブアプリケーションのセキュリティ態勢が充分に理解できない状態でした。

Tenable Web App Scanning は、最新のウェブアプリケーションに対応した、包括的な脆弱性スキャンを提供します。Tenable Web App Scanning の正確な脆弱性カバレッジによって誤検出や検出漏れが最

小限に抑えられ、セキュリティチームはウェブアプリケーションの真のセキュリティリスクを把握できます。本製品は、HTML5 や AJAX のフレームワークを使用して構築されたウェブアプリケーションにも対応し、本番環境で中断したり遅延したりすることがないよう、安全で確実な外部スキャンを実行します。

Tenable Container Security

> **動画：** の紹介 Tenable Container Security

Tenable コンテナのセキュリティは、本番稼働前のコンテナイメージがビルドされたときに、そのイメージを保管してスキャンします。脆弱性とマルウェアの検出、およびコンテナイメージの継続的な監視を行います。コンテナイメージをビルドする CI/CD（継続的統合および継続的デプロイメント）システムに Tenable Container Security を統合することで、本番環境にデプロイするすべてのコンテナの安全性と企業ポリシーへの準拠を確実なものにします。

Tenable Container Security の概要に関するデモについては、次の動画をご覧ください。

Tenable Vulnerability Management API

API 参照

Tenable Vulnerability Management API を利用すると、スキャン、ポリシー作成、ユーザー管理など、Tenable Vulnerability Management プラットフォームのさまざまな機能を使用して、独自のアプリケーションを開発できます。

Tenable Vulnerability Management を使い始める

次の開始手順に従って、Tenable Vulnerability Management のデプロイメントの設定を完成させてください。

1. デプロイメント計画の準備
2. スキャナーのインストールとリンク
3. スキャンの設定
4. 追加の Tenable Vulnerability Management 設定
5. レビューと分析
6. 拡張

ヒント: Tenable Vulnerability Management の詳細は、次の顧客教育資料で確認してください。

- Tenable Vulnerability Management Self Help Guide
- Tenable Vulnerability Management Introduction (Tenable University)

デプロイメント計画の準備

デプロイメント計画と分析ワークフローを作成する方法

1. TCP/IP インターネットプロトコルスイートの原理を確認します。Tenable Vulnerability Management のドキュメントは、基本的なネットワークの概念と原理に関する知識があることを前提としています。
2. Tenable の担当者から、Tenable Vulnerability Management のアクセス権に関する情報と開始時のアカウント資格情報を入手します。
3. 必要に応じて、Tenable サポートや、Professional Services のスキャン戦略ガイドなどの Tenable Vulnerability Management トレーニングリソースにアクセスします。
4. 企業の目的を特定するとともにネットワークトポロジーの分析を行って、デプロイメント計画を設計します。Tenable 推奨のベストプラクティスをご利用の環境に適用することを検討してください。

環境要件についての詳細は、一般要件ガイドにある、お使いのスキャナー用のガイドラインを参照してください。Tenable Vulnerability Management に対応したブラウザについての詳細は、Tenable Vulnerability Management システム要件を参照してください。

5. 内部スキャンと外部スキャン計画を設計します。実行するスキャンを指定し、十分なネットワーク容量があることを確認してください。
6. 分析ワークフローを設計します。管理グループと作業グループ内のステークホルダーを、各ステークホルダーと共有するデータを考慮のうえ指定します。

スキャナーのインストールとリンク

スキャナーをインストールして Tenable Vulnerability Management にリンクする方法

1. Tenable Vulnerability Management のユーザーインターフェースにログインします。
2. リンクされたスキャナーを設定します。
    - デプロイメント計画に Tenable Nessus スキャナーがある場合、*Tenable Nessus ユーザーガイド*の Tenable Nessus のインストールの説明に従って、Tenable Nessus をインストールします。
    - デプロイメント計画に Tenable Nessus Agents がある場合、*Tenable Nessus Agent デプロイメントとユーザーガイド*の Tenable Nessus Agents のインストールの説明に従って、エージェントをインストールします。
    - デプロイメント計画に Tenable Nessus Network Monitor がある場合、*Tenable Nessus Network Monitor ユーザーガイド*の NNM のインストールの説明に従って、Tenable Nessus Network Monitor をインストールします。
        - 次に*Tenable Nessus Network Monitor ユーザーガイド*の NNM を設定するの説明に従って、Tenable Nessus Network Monitor を Tenable Vulnerability Management と通信するように設定します。
    - デプロイメント計画に Tenable Web App Scanning がある場合、*Tenable Core ユーザーガイド*の Tenable Core + Tenable Web App Scanning のデプロイメントとインストールの説明に従って、ウェブアプリケーションをインストールします。

    次にセンサーのリンクの説明に従って、最初のスキャナーを Tenable Vulnerability Management にリンクします。

スキャンの設定

基本スキャンを設定して実行し、デプロイメント計画と分析ワークフローの有効性の評価を開始します。

注意: 環境とビジネスのニーズに基づいてスキャンを設定する方法については、Tenable Vulnerability Management スキャンの調整ガイドを参照してください。

1. **[基本的なネットワークスキャン]** テンプレートを使用して最初のアクティブスキャンを設定します。
    a. スキャナーグループを作成するの説明に従い、スキャナーグループを作成します。
    b. スキャンの作成の説明に従い、**[基本的なネットワークスキャン]** テンプレートを使用してスキャンを作成します。
2. 次に、**[基本的なエージェントスキャン]** テンプレートを使用して最初のエージェントスキャンを設定します。
    a. エージェントグループの作成の説明に従い、エージェントグループを作成します。
    b. スキャンを作成するの説明に従い、**基本エージェントスキャン**テンプレートを使用してエージェントスキャンを作成します。
3. スキャンの起動の説明に従い、最初の Tenable Nessus スキャンとエージェントスキャンを起動します。
4. ネットワークのすべてのターゲット領域にアクセスした状態で、Tenable Nessus スキャンとエージェントスキャンが完了したことを確認します。検出された資産を確認し、お使いのネットワークの知識を評価します。

追加の Tenable Vulnerability Management 設定

必要に応じて他の機能を設定し、既存の設定を調整します。

1. Tenable Vulnerability Management コンテナ内にユーザーアカウントを作成し、ユーザーグループを作成します。
2. 資産とターゲットの閲覧およびスキャンのアクセス許可を管理するアクセスグループを作成します。
3. タグを設定して、資産へのアクセスを整理、グループ化、制御します。

4. 資産検出をコネクタや Professional Services 統合、統合製品を使用して設定します。詳細は、コネクタ、カスタム統合サービスページ、Tenable Vulnerability Management のドキュメントページの**統合ガイド**セクションを参照してください。

5. 認証情報の説明に従って、管理された認証情報、スキャン固有の認証情報、ポリシー固有の認証情報を Tenable Nessus スキャン用に設定します。認証されたスキャンの設定とトラブルシューティングについての詳細は、Tenable Nessus 認証情報チェックを参照してください。

    a. スキャンの起動の説明に従って、認証された Tenable Nessus スキャンと認証されたエージェントスキャンを起動します。

    b. 認証スキャンが完了し、お使いのネットワークのすべてのターゲット領域にアクセスしていることを確認します。

6. エクスポージャーを評価する場合は、Tenable Lumin のライセンスを取得します。

7. ウェブアプリケーションのスキャンを実行する場合、Tenable Web App Scanning ライセンスを取得します。

8. お使いのコンテナのリスクを評価する場合は、Tenable Container Security ライセンスを取得します。

9. Tenable Vulnerability Management でユーザーが表示および操作できるオブジェクトとできないオブジェクトを制御するには、ユーザーの アクセス制御 を設定します。

レビューと分析

ヒント: Tenable では、スキャン結果とスキャンの範囲を頻繁に確認することを推奨しています。企業の目的に合わせ、ネットワークのすべての領域をスキャンするよう、スキャン設定を変更する必要がある場合があります。

データをさらにレビューして分析するには、次を行います。

1. スキャンと個別のスキャンの詳細を表示する。

2. [検出結果]と[資産]のページを使用して、脆弱性と資産の検出結果の表示と分析を行う。

3. ダッシュボードを作成して、ネットワークの脆弱性に関するインサイトを即座に取得し、迅速に分析する。インタラクティブなウィジェットとカスタマイズ可能な表を使用して、データを調査する。

4. ダッシュボードと資産、検出結果をフィルター処理して、データを掘り下げ、進捗状況を調査する。

5. 変更または許容ルールを作成して、スキャンで検出された脆弱性の変更や許容を行う。
6. レポートを作成して、スキャンや脆弱性の情報を企業内の他のユーザーと共有する。

拡張

Tenable は、デプロイメント計画と分析ワークフローを常に把握するためのベストプラクティスとして以下を推奨しています。

- 特定された脆弱性に対する企業の対応を確認するために、ミーティングを毎週開催します。チームが分析ワークフローを実行するのを監督するため、管理ミーティングを毎週開催します。
- スキャン結果とスキャン範囲を見直します。企業の目的に合わせ、ネットワークのすべての領域をスキャンするよう、スキャン設定を変更する必要がある場合があります。
- Tenable Vulnerability Management API ドキュメントの説明に従って、API の統合を検討してください。

Tenable Vulnerability Management のライセンス

このトピックでは、スタンドアロン製品の Tenable Vulnerability Management のライセンス付与プロセスを説明します。また、資産のカウント方法を説明し、購入できるアドオンコンポーネントをリストし、ライセンスがどのように流用されるか、および出力がライセンスカウントから除外されるプラグインについて説明します。Tenable Vulnerability Management の使用方法については、Tenable Vulnerability Management ユーザーガイドを参照してください。

Tenable Vulnerability Management のライセンシング

Tenable Vulnerability Management を使用する際は、所属する組織のニーズと環境に基づいてライセンスを購入してください。Tenable Vulnerability Management はその後、ライセンスを*資産*に割り当てます。それには、スキャンで特定されたか、脆弱性があるとしてインポートされたかのいずれかにより、過去 90 日間に評価されたリソース(サーバー、ストレージデバイス、ネットワークデバイス、仮想マシン、コンテナなど)が含まれます。

環境が拡張すると資産数も増えるため、その変化に合わせてライセンスを追加購入する必要があります。Tenable のライセンスは、累進的な価格設定であるため、多く購入するほど単価は安くなります。価格については、Tenable の担当者までお問い合わせください。

ヒント: 現在のライセンス数と利用可能な資産を表示するには、Tenable の上部ナビゲーションバーで  、**[ライセンス情報]** の順にクリックします。詳細については、ライセンス情報ページを参照してください。

注意: Tenable は、マネージドセキュリティサービスプロバイダー(MSSP)にシンプルな価格設定を提供しています。詳細については、Tenable の担当者にお問い合わせください。

資産のカウント方法

Tenable Vulnerability Management は資産をスキャンする際に、以前に検出された資産と比較します。通常、新しい資産が以前に検出された資産と一致せず、脆弱性の有無について評価されている場合、ライセンスとしてカウントされます。

Tenable Vulnerability Management は、複雑なアルゴリズムを使用して、重複を作成することなく新しい資産を特定します。このアルゴリズムは、資産の BIOS UUID、MAC アドレス、NetBIOS 名、完全修飾ドメイン名 (FQDN) などを調べます。また、認証されたスキャナーまたはエージェントは、各資産に Tenable UUID を割り当てて、資産を一意としてマークします。詳細は、Tenable Vulnerability Management FAQ を参照してください。

次の表は、どの場合に資産がライセンスにカウントされるかを示しています。

ライセンスにカウントされる	ライセンスにカウントされない
• アクティブスキャンによって特定された資産 • エージェントスキャンによって特定された資産 • 脆弱性を含む資産インポート (Tenable Nessus Professional のスキャン結果など) • ホストおよび Tenable Web App Scanning 資産タイプ (直近のライセンスのあるスキャンが過去 90 日以内に実行された場合)	• ホスト検出テンプレートで設定されたスキャン、または検出プラグインのみを使用するよう設定されたスキャン • 脆弱性を含まない資産インポート (ServiceNow データなど) • 検出モードで実行中の Tenable Nessus Network Monitor のリンクされたインスタンス • 検出専用コネクタ (資産の脆弱性がスキャンされるまで、およびスキャンされない場合) スキャンされたモバイルデバイス管理資産 • 除外されるプラグイン出力で説明されている一部のプラグイン出力

Tenable Vulnerability Management コンポーネント

コンポーネントを追加することで、それぞれのユースケースに合わせて Tenable Vulnerability Management をカスタマイズできます。一部のコンポーネントは有料のアドオンです。

購入に含まれるもの	アドオンコンポーネント
• 無制限の Tenable Nessus スキャナー • 無制限の Tenable Nessus Agent • 脆弱性検出機能ありの無制限の Tenable Nessus Network Monitor • Tenable Vulnerability Management API へのアクセス権	• Tenable PCI ASV. • Tenable Attack Surface Management.

ライセンスの流用

ライセンスを購入しても、追加のライセンスを購入しない限り、ライセンスの総数は契約期間中ずっと同じです。ただし、一部の条件下で Tenable Vulnerability Management はライセンスを回収し、ライセンスを新しい資産に再割り当てすることで、ライセンスが不足しないようにします。

次の表は、Tenable Vulnerability Management がライセンスを流用する方法を示しています。

資産タイプ	ライセンス流用プロセス
削除された資産	Tenable Vulnerability Management は、削除された資産を **[資産]** ワークベンチから削除し、24 時間以内にそのライセンスを流用します。
期限切れの資産	**[設定]** > **[センサー]** > **[ネットワーク]** で、**[期限切れの資産]** を有効にした場合、Tenable Vulnerability Management は指定された期間スキャンされなかった資産のライセンスを流用します。
コネクタの資産	Tenable Vulnerability Management は、終了した翌日にコネクタから資産を回収して流用します。このイベントは各コネクタで発生します。
その他のすべての資産	Tenable Vulnerability Management は、90 日間スキャンされなかったその他のすべての資産 (他の製品からインポートされたものや、期限切れ設定なしの資産など) のライセンスを流用します。

ライセンス制限の超過

ハードウェアの更新、急激な環境の拡張、予期しない脅威などによる、使用率の急増に対応できるよう、Tenable ライセンスは柔軟に提供されます。ただし、ライセンスされている以上の資産をスキャンすると、Tenable はその超過について明確に伝達し、その後 3 段階で機能を削減します。

シナリオ	結果
3 日間連続して、ライセンスされている以上の資産をスキャンした。	Tenable Vulnerability Management にメッセージが表示されます。
15 日間以上、ライセンスされている以上の資産をスキャンした。	Tenable Vulnerability Management には、機能の制限に関するメッセージと警告が表示されます。

45 日間以上、ライセンスされている以上の資産をスキャンした。	Tenable Vulnerability Management にメッセージが表示されます。スキャンおよびエクスポート機能が無効になります。

ヒント: 不適切なスキャンや製品の設定ミスにより、スキャンが過剰になり、資産数が増加する可能性があります。詳細については、スキャンのベストプラクティスを参照してください。

期限切れのライセンス

購入した Tenable Vulnerability Management ライセンスは契約期間中ずっと有効です。ライセンスの有効期限が切れる 30 日前になると、ユーザーインターフェースに警告が表示されます。この更新期間中に、Tenable の担当者と連携して、製品の追加や削除、ライセンス数の変更を行ってください。

ライセンスの有効期限が切れると、Tenable プラットフォームにサインインできなくなります。

除外されるプラグイン出力

このセクションにリストされているプラグインは、ライセンス制限にはカウントされません。

注意: プラグイン ID は静的ですが、プラグイン名は Tenable 製品によって時折変更される場合があります。プラグインの最新情報は、Tenable プラグインを参照してください。

検出設定の Tenable Nessus プラグイン

[検出設定] で次の プラグインを設定します。これらのプラグインは、ライセンスにはカウントされません。

Tenable Nessus プラグイン ID	プラグイン名
10180	リモート ホストに ping
10335	Nessus TCP スキャナー
11219	Nessus SYN スキャナー
14274	Nessus SNMP スキャナー
14272	Netstat Portscanner (SSH)
34220	Netstat Portscanner (WMI)
34277	Nessus UDP スキャナー

プラグインページの Tenable Nessus プラグイン

次の プラグインを [プラグイン] ページで設定します。これらのプラグインは、ライセンスにはカウントされません。

Tenable Nessus プラグイン ID	プラグイン名
45590	共通プラットフォーム一覧 (CPE)
54615	デバイスタイプ
12053	ホスト完全修飾ドメイン名 (FQDN)
11936	OS 識別
10287	トレースルート情報
22964	サービスの検出
11933	プリンタをスキャンしない
87413	ホストタギング
19506	Nessus スキャン情報
33812	ポートスキャナーの設定
33813	ポートスキャナーの依存関係

Tenable Nessus Network Monitor プラグイン

次の プラグインは、ライセンスにはカウントされません。

Tenable Nessus Network Monitor プラグイン ID	プラグイン名
0	開いているポート
12	検出されたホスト TTL
18	汎用プロトコル検出
19	VLAN ID 検出

20	汎用 IPv6 トンネルトラフィック検出
113	VXLAN ID 検出
132	ホストの属性列挙

Tenable Vulnerability Management システム要件

ディスプレイ設定

最小画面解像度: 1440 x 1024

対応ブラウザ

Tenable Vulnerability Management は、以下のブラウザの最新バージョンをサポートしています。

注意: Tenable Vulnerability Management に関する問題を報告する前に、ブラウザが最新であることを確認してください。

- Google Chrome
- Apple Safari
- Mozilla Firefox
- Microsoft Edge

注意: Tenable Vulnerability Management は、モバイルブラウザではサポートされていません。

Tenable Vulnerability Management にログインする

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: ブラウザで Tenable Vulnerability Management ページをブックマークする場合でも、ブックマーク済みページにアクセスする前にログインする必要があります。
場合によっては、ブックマークされたページにアクセスする前に、[ワークスペース] ページや Tenable Vulnerability Management アプリケーションに移動する必要が生じることがあります。

始める前に

- Tenable Vulnerability Management ユーザーアカウントの認証情報を取得します。

  注意: 管理者として Tenable Vulnerability Management インスタンスに初めてログインする場合には、Tenable がセットアップ中に初回認証情報を提供します。新しいパスワードは初回ログイン後に設定できます。初回セットアップの後に Tenable Vulnerability Management にログインする場合には、Tenable Vulnerability Management アカウントの登録に使用したメールアドレスがユーザー名になります。

- *一般要件ユーザーガイド*のシステム要件をレビューして、ご利用のコンピューターとブラウザが要件を満たしていることを確認します。

注意: SAML を使用するようにアカウントが構成されている場合は、SAML プロバイダーから直接、Tenable Vulnerability Management にログインできます。詳細は、SAML を参照してください。

Tenable Vulnerability Management にログインする方法

1. サポートされているブラウザで、https://cloud.tenable.com に移動します。

   Tenable Vulnerability Management のログインページが表示されます。

2. [ユーザー名] ボックスで、Tenable Vulnerability Management のユーザー名を入力します。

3. [パスワード] ボックスで、登録時に作成した Tenable Vulnerability Management のパスワードを入力します。

4. (オプション) 後のセッションのためにユーザー名を保存するには、**[ログイン情報を記憶しますか?]** チェックボックスを選択します。

5. **[サインイン]** をクリックします。

   Tenable Vulnerability Management [ワークスペース] ページが表示されます。

注意: Tenable Vulnerability Management 一定の時間 (通常は 30 分) 使用しない場合、ログアウトします。

CVSS 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 Vulnerability Priority Rating (VPR) を使用しています。

注意: これらのメトリクスをプラグイン別に整理された分析ページ (たとえば、**[プラグイン別脆弱性]** ページ) で表示するとき、メトリクスは、プラグインに関連付けられた脆弱性に割り当てられた、または計算された最高値を表します。

VPR およびその他の Tenable Lumin のメトリクスに関する、Tenable Lumin 特有の情報については、Tenable Lumin のメトリクスを参照してください。

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 攻撃区分がある場合、**リスクファクター**はその CVSSv2 攻撃区分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 攻撃元区分がない場合、Tenable は独自で**リスクファクター**を計算します。

Tenable Vulnerability Management は、スキャンで脆弱性が検出されるたびに CVSS スコアをインポートします。

CVSS ベースの深刻度

Tenable は、すべての脆弱性に、CVSSv2 または CVSSv3 の静的なスコアに基づく深刻度 (**情報**、**低**、**中**、**高**、**緊急**) を割り当てます。詳しくは、深刻度メトリクスの設定を参照してください。

Tenable Vulnerability Management 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。各深刻度に使用されるアイコンの詳細については、Vulnerability Severity Indicators を参照してください。

深刻度	CVSSv2 の範囲	CVSSv3 の範囲
緊急	プラグインの最高脆弱性 CVSSv2 スコアは 10.0 です。	プラグインの最高脆弱性 CVSSv3 スコアは 9.0 ~ 10.0 です。
重要	プラグインの最高脆弱性 CVSSv2 スコアは 7.0 ~ 9.9 です。	プラグインの最高脆弱性 CVSSv3 スコアは 7.0 ~ 8.9 です。
警告	プラグインの最高脆弱性 CVSSv2 スコアは 4.0 ~ 6.9 です。	プラグインの最高脆弱性 CVSSv3 スコアは 4.0 ~ 6.9 です。
注意	プラグインの最高脆弱性 CVSSv2 スコアは 0.1 ~ 3.9 です。	プラグインの最高脆弱性 CVSSv3 スコアは 0.1 ~ 3.9 です。
なし	プラグインの最高脆弱性 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。	プラグインの最高脆弱性 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 ベースのリスクファクター

各プラグインについて、Tenable はそのプラグインに関連付けられている脆弱性の CVSSv2 または CVSSv3 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 (**低**、**中**、**高**、**緊急**) を割り当てます。**[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。

Vulnerability Priority Rating

動画: Tenable Vulnerability Management の Vulnerability Priority Rating

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
緊急	9.0 ~ 10.0
高	7.0 ~ 8.9
中	4.0 ~ 6.9
低	0.1 ~ 3.9

注意: National Vulnerability Database (NVD) にある 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。

Tenable Vulnerability Management 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。その後 Tenable Vulnerability Management は、毎日自動的に新規または更新された 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。

- Tenable が提供する [脆弱性管理の概要] ダッシュボード
- [プラグイン別脆弱性] プレーン
- [プラグイン別脆弱性 (従来)] ページ

VPR 主な要因

脆弱性の VPR を説明する、次の主な要因を表示することができます。

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 Vulnerability Management 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**、**動作可能**、**PoC**、または **未実証**) は CVSS エクスプロイトコード成熟度と同等です。
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 (**低**、**中**、**高**、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**、**低**、**中**、**高**、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

脆弱性の深刻度インジケーター

Tenable は、すべての脆弱性に、CVSSv2 または CVSSv3 の静的なスコアに基づく深刻度 (**情報**、**低**、**中**、**高**、**緊急**) を割り当てます。詳しくは、深刻度メトリクスの設定を参照してください。

Tenable Vulnerability Management インターフェースでは、深刻度カテゴリ、許容済みステータス、変更済みステータスごとに異なるアイコンを使用します。

アイコン	カテゴリ	詳細
	緊急	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[重大]** に変更しました。
	高	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[高]** に変更しました。
	中	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[中]** に変更しました。
	低	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[低]** に変更しました。
	情報	リスクを許容していない、またはリスクの深刻度を変更していません。
		リスクを許容しました。
		深刻度を **[Info]** に変更しました。

脆弱性の軽減

Tenable Vulnerability Management の脆弱性は**アクティブ**または**修正済み**の 2 つのカテゴリのいずれかに分類されます。Tenable Vulnerability Management が資産の脆弱性を検出すると、その脆弱性は、軽減または修正されるまで**アクティブ**カテゴリに含められます。軽減または修正された脆弱性は、**修正済み**カテゴリに移動します。

アクティブな脆弱性

アクティブな脆弱性とは、状態が**[新規]**、**[アクティブ]**、または**[再表面化]**である脆弱性です。詳細は、脆弱性の状態を参照してください。

修正済みの脆弱性

修正済みカテゴリには、スキャン定義、スキャンの結果、および認証情報に基づいて脆弱ではないと Tenable Vulnerability Management により判断された脆弱性が含まれています。軽減の対象となるには、脆弱性がアクティブであり、正常に認証されている必要があります。

以下の条件に該当する場合に脆弱性が軽減されます。

- 脆弱性の IP アドレスまたは他の識別属性 (IA) の組み合わせが、スキャンのターゲットリストに含まれている。IA の詳細については、Tenable Communityをご覧ください。
- 脆弱性のプラグイン ID がスキャン結果にリストされている。

  > スキャン済みホストからソフトウェアを削除し、それによりプラグインとその依存関係が起動しなくなる場合、脆弱性の状態をそのまま変えずに、リスクを許容することが必要になるかもしれません。

- 脆弱性のポートが、スキャン済みポートのリストに含まれている。
- IP アドレス、ポート、プロトコル、プラグイン ID の組み合わせの脆弱性が、スキャン結果にリストされていない。

軽減の例外

脆弱性の軽減には、次のような例外があります。

- **thorough_tests** 属性を持つプラグインによる完全スキャン中に特定された脆弱性は、別の完全スキャンでのみ軽減可能です。
- **requires_paranoid_scanning** 属性を持つプラグインによる綿密なスキャン中に特定された脆弱性は、別の綿密なスキャンでのみ緩和可能です。
- 認証情報スキャンで、ポート 0 または 445 で報告されたローカルプラグインまたは結合プラグインによって検出された脆弱性は、別の認証スキャンでのみ緩和可能です。
- プラグイン 14272 (SSH netstat)、34220 (WMI netstat)、14274 (SNMP) のいずれかがホストをトリガーした場合に、スキャン済みポートのリストを「すべての」ポートに展開できます。
- エージェントスキャンは、リモートポート (0/445 以外) で報告された結合型プラグインによって検出された脆弱性を軽減できません。

脆弱性の状態

Tenable は、ネットワークで検出された脆弱性に対して、*状態*を割り当てます。脆弱性の状態別に追跡、フィルタリングすることで、脆弱性の検出、解決、再発の推移を確認できます。状態で脆弱性をフィルタリングするには、**[検出結果]**ワークベンチを使用します。

脆弱性の状態	説明
新規	Tenable Vulnerability Management が脆弱性を 1 回検出したことを示します。
アクティブ	Tenable Vulnerability Management が脆弱性を複数回検出したことを示します。 **注意: アクティブ**な脆弱性でフィルタリングする場合、Tenable Vulnerability Management は **[新規]** の脆弱性も返します。フィルタリングにおいては、**[新規]** は **[アクティブ]** のサブカテゴリになります。
修正済み	Tenable Vulnerability Management がホストで脆弱性を 1 回検出したものの、今後は検出されないことを示します。 **注意**: **[修正済み]** の脆弱性を日付範囲別に表示するには、**[最終修正日]** フィルターを使用します。
再表面化	Tenable Vulnerability Management が以前に脆弱性を **[修正済み]** としてマークしたものの、再検出されたことを示します。脆弱性が **[再表面化]** である場合、スキャンがその脆弱性を修正済みとして識別するまで、この状態のままになります。その後、脆弱性は **[修正済み]** に戻ります。

注意: API では、脆弱性の状態に関して、ユーザーインターフェースとは異なる用語を使用します。API では、新規とアクティブのどちらの状態も [オープン] とラベル付けされます。再表面化した状態は、[再オープン済み] としてラベル付けされます。修正済みの状態は同じです。

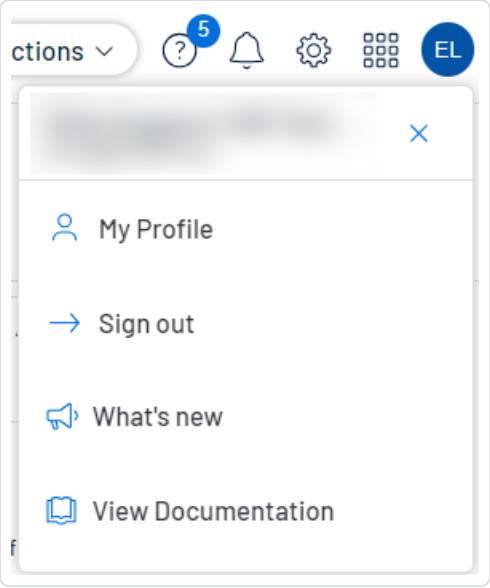
Tenable Vulnerability Management をログアウトする

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management をログアウトする方法

1. 右上の青いユーザー円をクリックします。

   ユーザーアカウントメニューが表示されます。



2. **[サインアウト]** をクリックします。

Tenable Vulnerability Management のナビゲーション

Tenable Vulnerability Management には、重要な情報を強調し、ユーザーインターフェースをより効率的に操作するのに役立つ、便利なショートカットやツールが含まれています。

クイックアクションメニュー

クイックアクションメニューは、最もよく利用されるアクションをリスト表示します。

クイックアクションメニューにアクセスする方法

1. 右上にある ☆ **クイックアクション** ボタンをクリックします。

   クイックアクションメニューが表示されます。

2. リンクをクリックして、一覧にあるいずれかのアクションを開始します。

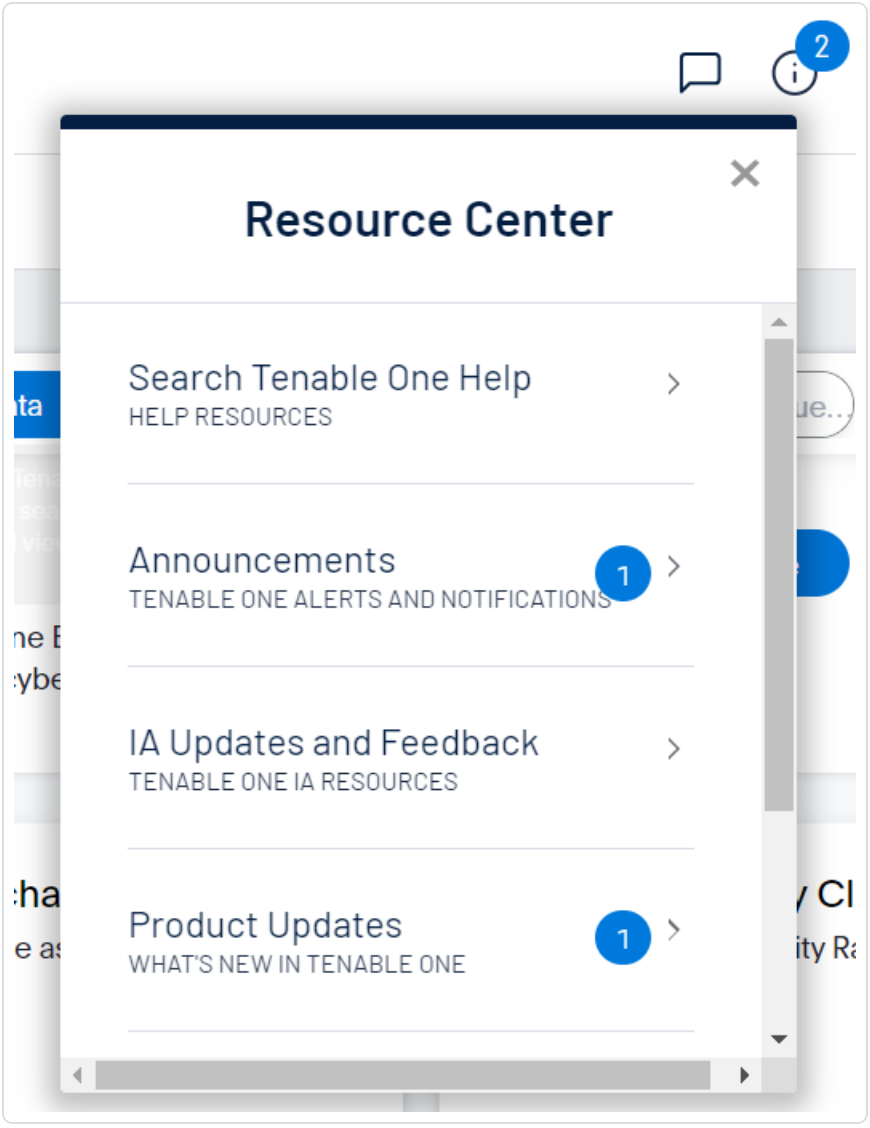
リソースセンター

リソースセンターには、製品発表、Tenable ブログ投稿、ユーザーガイドドキュメントなどの情報リソースのリストが表示されます。

リソースセンターにアクセスする方法

1. 右上の ⓘ ボタンをクリックします。

   [リソースセンター] メニューが表示されます。



2. リソースのリンクをクリックすると、そのリソースに移動します。

通知

Tenable Vulnerability Management の **[通知]** パネルにはシステム通知のリストが表示されます。🔔 ボタンは、現時点で確認されていない通知の数を示しています。**[通知]** パネルを開くと、これらの通知は Tenable Vulnerability Management によって確認済みとしてマーキングされます。通知を確認したら、消去して **[通知]** パネルから削除できます。

> **注意:** Tenable Vulnerability Management は類似の通知をグループ化してまとめます。

通知を表示するには:

- 右上の 🔔 ボタンをクリックします。

  [通知] パネルが表示され、システムの通知のリストが表示されます。

  [通知] パネルでは、以下の操作を実行できます。

  - 1つの通知を消去するには、通知の隣の ✕ ボタンをクリックします。
  - 通知のグループを展開するには、グループ化された通知の下部にある **[追加の通知]** をクリックします。
  - 展開された通知のグループを折りたたむには、展開された通知の上部にある **[表示数を減らす]** をクリックします。
  - 展開された通知のグループを消去するには、展開された通知の上部にある **[グループのクリア]** をクリックします。
  - すべての通知を消去するには、パネルの下部にある **[すべてクリア]** をクリックします。

設定アイコン

⚙ ボタンをクリックして [設定] ページに直接移動し、システム設定を設定します。

ワークスペース

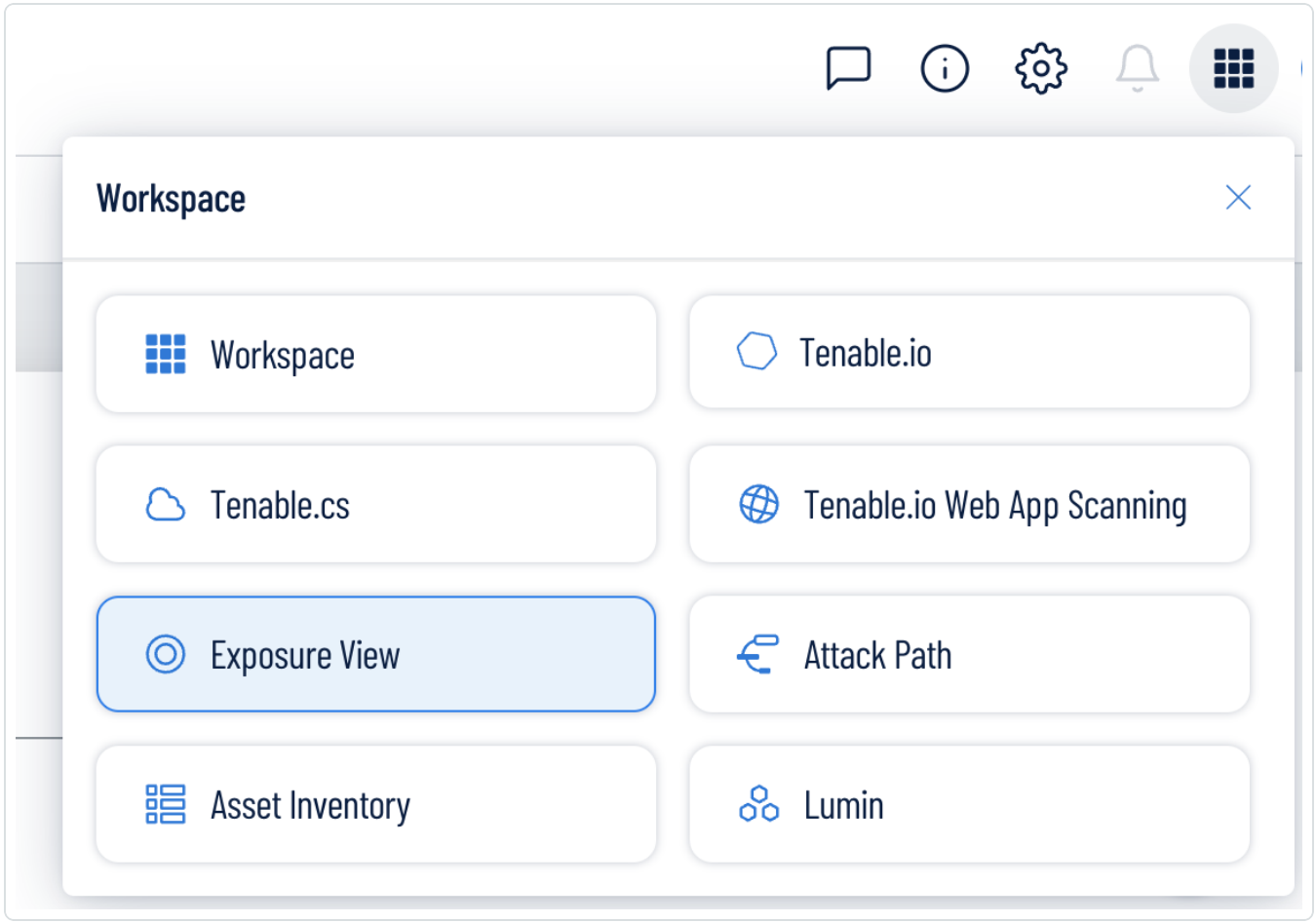
Tenable にログインすると、デフォルトで **[ワークスペース]** ページが表示されます。**[ワークスペース]** ページで、Tenable アプリケーションを切り替えたり、デフォルトのアプリケーションを設定して今後 **[ワークスペース]** ページをスキップするようにしたりできます。上部のナビゲーションバーに表示される **[ワークスペース]** メニューから、アプリケーションを切り替えることもできます。

ワークスペースメニューを開く

[ワークスペース] メニューを開く方法

1. いずれかの Tenable アプリケーションの右上隅にある ボタンをクリックします。

   [ワークスペース] メニューが表示されます。



2. アプリケーションタイルをクリックして開きます。

ワークスペースページを表示する

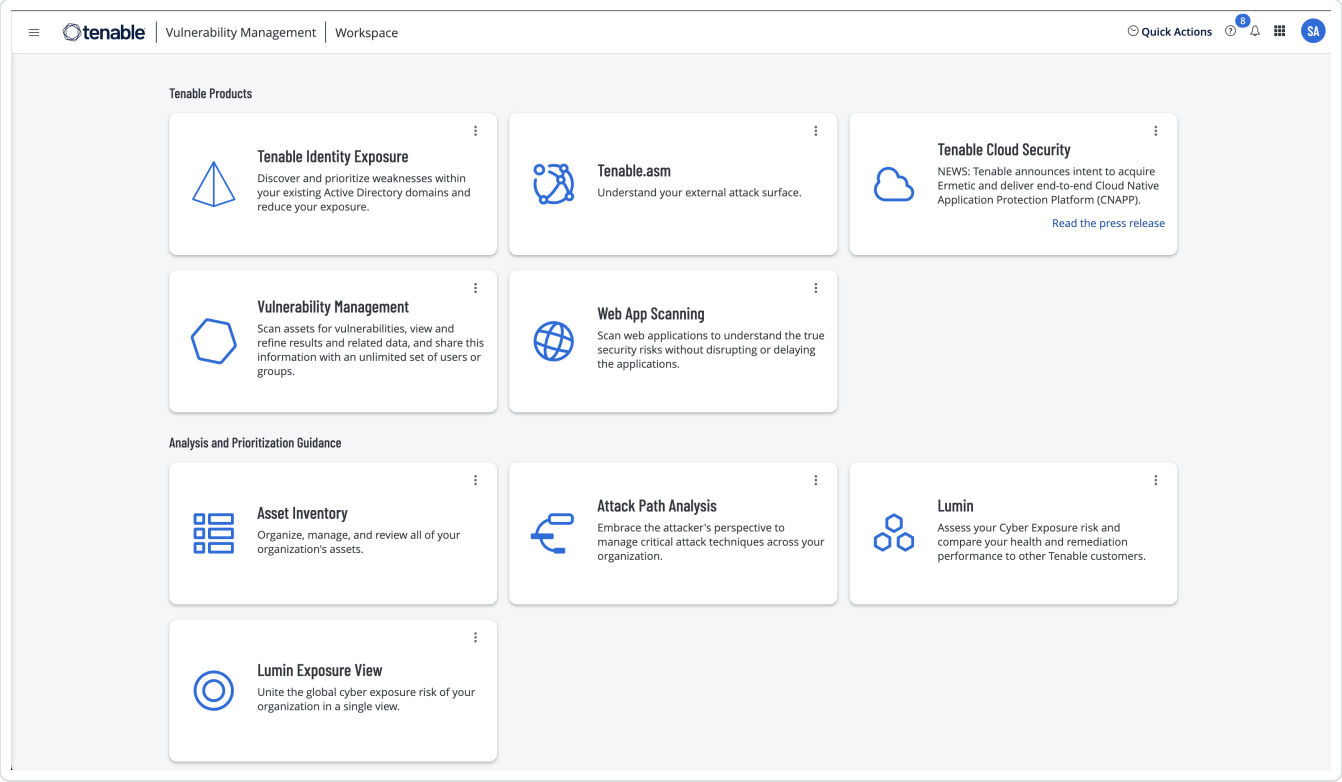
[ワークスペース] ページを表示する方法

1. いずれかの Tenable アプリケーションの右上隅にある ボタンをクリックします。

   [ワークスペース] メニューが表示されます。

2. **[ワークスペース]** メニューの **[ワークスペース]** をクリックします。

[ワークスペース] ページが表示されます。



デフォルトのアプリケーションを設定する

Tenable にログインすると、デフォルトで **[ワークスペース]** ページが表示されます。ただし、今後 **[ワークスペース]** ページをスキップするように、デフォルトアプリケーションを設定することもできます。

> デフォルトでは、**管理者**、**スキャンマネージャー**、**スキャンオペレーター**、**標準**、**基本**のロールを持つユーザーは、デフォルトのアプリケーションを設定できます。別のロールをお持ちの場合は、管理者に連絡して、**[マイアカウント]** から **[管理]** アクセス許可をリクエストしてください。詳細については、カスタムロールを参照してください。

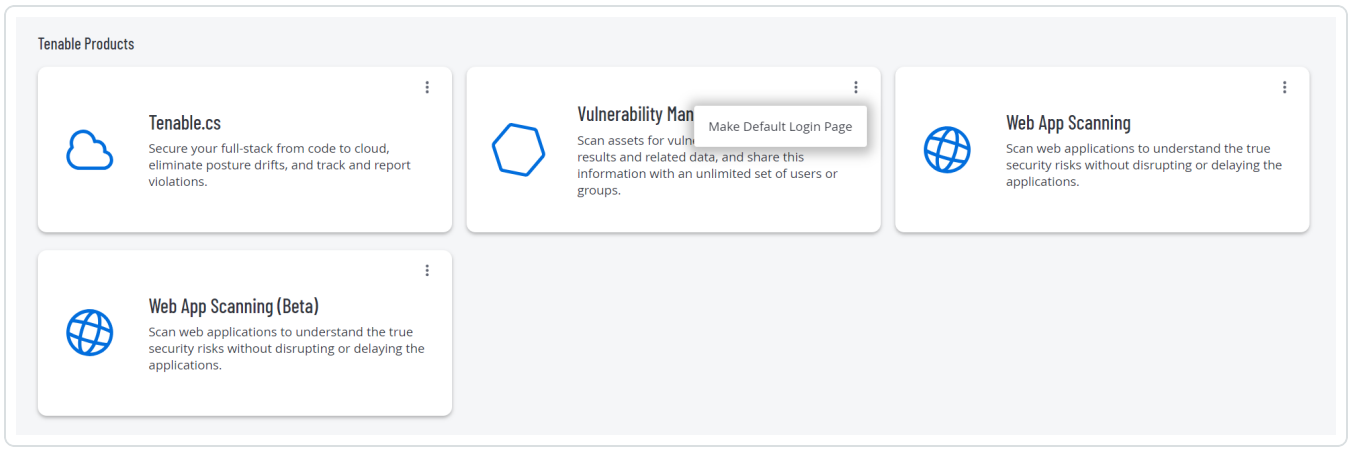
デフォルトのログインアプリケーションを設定する方法

1. Tenable にログインします。

   [ワークスペース] ページが表示されます。

2. 選択するアプリケーションの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。



3. メニューで、**[デフォルトログインページの作成]** をクリックします。

   ログインするとこのアプリケーションが表示されるようになります。

デフォルトのアプリケーションを削除する

デフォルトのアプリケーションを削除する方法

1. Tenable にログインします。

   [ワークスペース] ページが表示されます。

2. 削除するアプリケーションの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。

3. **[デフォルトログインページの削除]** をクリックします。

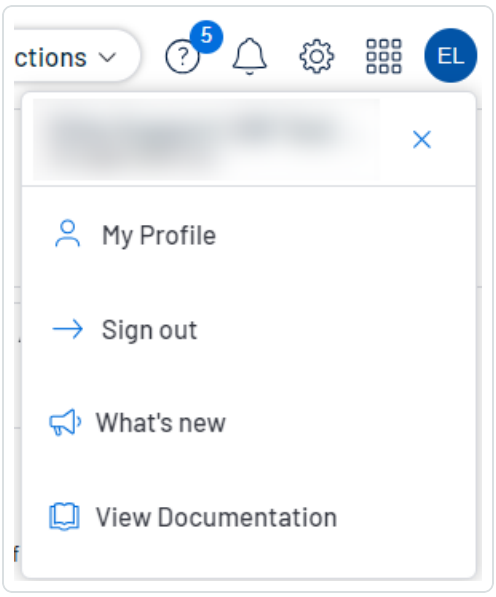
   ログインすると **[ワークスペース]** ページが表示されるようになります。

ユーザーアカウントメニュー

ユーザーアカウントメニューには、ユーザーアカウントのいくつかのクイックアクションがあります。

1. 右上の青いユーザー円をクリックします。

   ユーザーアカウントメニューが表示されます。



2. 次のいずれかを行います。

   - **[マイプロファイル]** をクリックして、自身のユーザーアカウントを設定します。**[マイアカウント]** 設定ページに直接移動します。詳細はマイアカウントを参照してください。
   - Tenable Vulnerability Management からサインアウトするには、**[サインアウト]** をクリックします。
   - **[新機能]** をクリックして、Tenable Vulnerability Management リリースノートに直接移動します。
   - **[ドキュメントの表示]** をクリックし、Tenable Vulnerability Management ユーザーガイドのドキュメントに直接移動します。

Tenable Vulnerability Management インターフェースのナビゲーション方法の詳細については、次のトピックを参照してください。

ブレッドクラムのナビゲーション

プレーンのナビゲーション

Tenable Vulnerability Management の表

ブレッドクラムのナビゲーション

Tenable Vulnerability Management インターフェースでは、特定のページの上部のナビゲーションバーにブレッドクラムが表示されます。ブレッドクラムには、現在のページに到達するまでにアクセスしたページの経路が左から右に向かって表示されます。

ブレッドクラムのナビゲーション方法

- 上部のナビゲーションバーで、ブレッドクラムのリンクをクリックし、前のページに戻ります。

プレーンのナビゲーション

Tenable Vulnerability Management では、固定されたページとオーバーラップするプレーンが組み合わされています。

新しいインターフェースのプレーンのナビゲーション方法

1. 次のいずれかの方法を使用してプレーンにアクセスします。

   - ダッシュボード上のウィジェットをクリックします。
   - 左側のナビゲーションプレーンを次のように使用します。

     a. 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     b. 左側のナビゲーションプレーンで、メニューオプションをクリックします。

   左側のナビゲーションプレーンを除き、プレーンは画面の右側から開きます。

2. プレーンの左端にある次のボタンを使用してプレーンを操作します。

ボタン	短縮名	アクション
⤡	展開	プレーンを展開します。一部のプレーンは全画面に展開できます。
⤢	戻す	展開したプレーンをデフォルトのサイズに戻します。
×	閉じる	プレーンを閉じます。
←	プレビューを展開する	プレビュープレーンを展開します。
→	プレビューを元に戻す	展開したプレーンをプレビュープレーンに戻します。

3. 前のプレーンをクリックして、前のプレーンまたはページに戻ります (新しいプレーンは閉じます)。

Tenable Vulnerability Management の表

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management ワークベンチの表

Tenable Vulnerability Management **ワークベンチの表** とは、Tenable Vulnerability Management のインターフェースで **[調査]** セクション外にあるすべての表です。これらの表には検索機能とナビゲーション機能があります。列をドラッグアンドドロップして任意の順番に配置できる機能や、列幅の変更、複数列のデータを一度に並べ替える機能も備えています。詳細は、Tenable Vulnerability Management ワークベンチの表 を参照してください。

調査の表

調査 の表とは、Tenable Vulnerability Management のユーザーインターフェースの **[調査]** セクションにあるすべての表です。これらの表には Tenable Vulnerability Management ワークベンチの表にある多くの機能が含まれていますが、追加のカスタマイズ機能とフィルタリング機能も含まれています。詳細は、検出結果または資産のフィルタリング を参照してください。

Tenable Vulnerability Management ワークベンチの表

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: カスタマイズ可能な表では、表の行を右クリックすることでアクションボタンにアクセスすることもできます。ブラウザメニューにアクセスするには、Ctrl キーを押しながら右クリックします。

Tenable Vulnerability Management ワークベンチの表とは、Tenable Vulnerability Management のインターフェースで **[調査]** セクション外にあるすべての表です。

Tenable Vulnerability Management ワークベンチの表を操作する方法

1. ワークベンチの表を表示します。
2. 次のいずれかを行います。
    - 表内を移動する場合
        - ソート順を調整するには、列のタイトルをクリックします。

          選択した列のデータを基準に、Tenable Vulnerability Management は表のすべてのページをソートします。
        - Tenable Vulnerability Management で、各ページに表示される行数を増減するには、**[ページ当たりの件数]** をクリックして、数字を選択します。

          Tenable Vulnerability Management によって表が更新されます。
        - 表の行で利用可能なすべてのアクションボタンを表示するには、⋮ ボタンをクリックします。

          このボタンは、行に対して 5 つ以上のアクションが可能な場合に、個別のアクションボタンの代わりに表示されます。
        - 表の別のページに移動するには、矢印をクリックします。

ボタン	アクション
|<	表の最初のページに移動します。

< >	表の前のページまたは次のページに移動します。
>|	表の最後のページに移動します。

注意: 制限により、検出結果の合計数が 1000 の制限を超えていることがわからないことがあります。この場合、表のインターフェースが変わったり、ページ割のラベリングが変わったり、最終ページへのナビゲーションボタンが無効になったりする可能性があります。

- 表内を検索する場合

  新しいインターフェースでは、さまざまなページやプレーンの各表の上に検索ボックスが表示されます。いくつかのケースでは、検索ボックスは **[フィルター]** ボックスの横に表示されます。

  a. **[検索]** ボックスに検索条件を入力します。

     検索条件は、検索する表内のデータの種類によって異なります。

  b. 🔎 ボタンをクリックします。

     Tenable Vulnerability Management は検索条件に従って表にフィルターを適用します。

- 列順を変更するには、列のヘッダーをドラッグアンドドロップして表内の別の場所に移動させます。

- 列を削除または追加する場合

  a. 任意の列にカーソルを合わせます。

     ヘッダーに ☰ ボタンが表示されます。

  b. ☰ ボタンをクリックします。

     列の選択ボックスが表示されます。

  c. 表で表示または非表示にする列のチェックボックスを、それぞれ選択または選択解除します。

     ヒント: 検索ボックスを使用すると列名を素早く見つけることができます。

     選択された内容に応じて表が更新されます。

- 列幅を調整する場合

  a. サイズ調整カーソルが表示されるまで、2 つの列の間のヘッダーにカーソルを合わせます。

     列幅をクリックしたままドラッグして、好みの幅に調整します。

     > **ヒント:** 内容に合わせて列幅を自動調整するには、列のヘッダーの右側をダブルクリックします。

- 表のデータをソートするには、列のヘッダーをクリックします。

  選択した列のデータを基準に、Tenable Vulnerability Management は表のすべてのページをソートします。

- 複数の列を使用して表のデータをソートするには、**Shift** を押しながら 1 つ以上の列のヘッダーをクリックします。

  > **注意:** すべての表や列で複数の列によるソートができるわけではありません。

  Tenable Vulnerability Management は、列を選択した順序で表のすべてのページをソートします。

表のフィルタリング

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management では、さまざまなページやプレーンの各表の上に**[フィルター]**ボックスが表示されます。

表をフィルタリングする方法

1. **[フィルター]**の横にある ⌄ ボタンをクリックします。

   フィルター設定が表示されます。

2. (オプション) Tenable Vulnerability Management でフィルターを素早く選択するには、☆**[フィルターの選択]**をクリックします。

   ドロップダウンリストが表示されます。

   a. ドロップダウンリストで、適用するフィルターを検索します。

      検索条件に基づいて、リストが更新されます。

   b. 適用するフィルターの横にあるチェックボックスを選択します。

      選択したフィルターがフィルターセクションに表示されます。

3. **[カテゴリの選択]**ドロップダウンボックスで、属性を選択します。

   たとえば、検出結果をフィルタリングする場合には**[深刻度]**を、資産をフィルタリングする場合には**[資産 ID]**を選択できます。

4. **[演算子の選択]**ドロップダウンボックスで、演算子を選択します。

   注意: **[次の値を含む]**または**[次の値を含まない]**演算子を使用するには、次のベストプラクティスに従ってください。

   - 最も正確で完全な検索結果を生成するには、検索値に単語全体を入力します。
   - 検索値には終止符を含めません。

- 資産をフィルタリングする際は、検索値は大文字と小文字が区別されます。
- 可能であれば、Tenable は**[次の値に等しい]**または**[次の値に等しくない]**演算子の代わりに**[次の値を含む]**または**[次の値を含まない]**演算子を使用することを推奨しています。

5. **[値を選択する]**ボックスで、次のいずれかを行います。

値の種類	アクション
テキスト	フィルタリングしたい値を入力します。 入力を開始するまで、ボックスには予測入力の例が表示されます。入力内容が属性として無効な場合は、テキストボックスの周囲に赤い枠線が表示されます。
単一の有効な値	属性にデフォルトの値が関連付けられている場合、Tenable Vulnerability Management は自動的にそのデフォルトの値を選択します。 デフォルトの値を変更する、またはデフォルトの値が関連付けられていない場合は、次を行います。 a. ボックスをクリックしてドロップダウンリストを表示します。 b. リストから値を探して、選択します。
複数の有効な値	1つ以上の値を選択するには、次を行います。 a. ボックスをクリックしてドロップダウンリストを表示します。 b. 値を探して、選択します。 選択した値がボックスに表示されます。 c. すべての該当する値が選択されるまで、繰り返します。

	d. ドロップダウンリストの外側をクリックして、リストを閉じます。 値を選択解除するには、次を行います。 a. 削除する値にカーソルを合わせます。 値の上に ✕ ボタンが表示されます。 b. ✕ ボタンをクリックします。 値がボックスから消えます。

6. (オプション) フィルターセクションの左下で、次を行います。
   - 別のフィルターを追加するには、**[追加]** ボタンをクリックします。
   - すべてのフィルターを消去するには、**[フィルターのリセット]** ボタンをクリックします。
7. **[適用]** をクリックします。

   Tenable Vulnerability Management が 1 つまたは複数のフィルターを表に適用します。
8. (オプション) 1 つまたは複数のフィルターを後で使用するために保存します。
9. (オプション) 適用したフィルターを消去します。
   a. 表のヘッダーで、**[すべてのフィルターのクリア]** をクリックします。

      Tenable Vulnerability Managementにより、保存された検索条件を含むすべてのフィルターが表から消去されます。

      > **注意:** フィルターを消去しても、ページの右上で選択された日付範囲は変更されません。詳細は、Tenable Vulnerability Management の表 を参照してください。

Tenable Lumin を使い始める

Tenable Lumin を使用すると、リスクを素早く正確に評価でき、企業の正常性や修正状況を Salesforce 業界および全体の他の Tenable ユーザーと比較できます。Tenable Lumin は、未加工の脆弱性データを資産のビジネス上の重要度や脅威の文脈データと関連付けることで、従来の脆弱性管理ツールよりも高速かつターゲットを絞った分析ワークフローをサポートします。

Tenable では、Tenable Lumin のデータと機能の使用を開始するために、次の手順を推奨します。

ライセンスおよび有効化

Tenable Lumin ライセンスを取得し、Tenable Vulnerability Management を Tenable Lumin で有効化します。

1. Tenable Lumin を Tenable Vulnerability Management ライセンスに追加するには、Tenable 担当者にお問い合わせください。
2. ブラウザで、Tenable Lumin の有効化の妨げになりそうな機能を無効にします。
    - 広告ブロッカー拡張機能
    - トラッキング拒否機能 (Mozilla Firefox、Google Chrome、Apple Safari、Microsoft Internet Explorer のいずれか)
    - 保護モード (Microsoft Internet Explorer)

    ヒント: Tenable Lumin を完全に有効化した後で、これらの機能を再び有効にすることができます。
3. Tenable Lumin へのログインの説明に従って、Tenable Vulnerability Management にログインします。

    Tenable Lumin のウェルカムウィンドウが表示されます。
4. ウィザードに従って、Tenable Lumin を有効化します。

    Lumin ダッシュボードが表示されます。

準備

データを作成し、Tenable Lumin の用語を理解するようにします。

Tenable Vulnerability Management のみ	Tenable Security Center + Tenable Vulnerability Management Tenable Lumin
1. Tenable Vulnerability Management で認証済みの評価スキャンを実行して、脆弱性データを生成します。 **注意：** Tenable Lumin ビューでデータを表示するにはスキャンを実行する必要があります。Tenable Lumin では、Tenable Lumin がライセンスされた後に生成されたスキャン結果データが表示されます。詳細は、Tenable Lumin のデータのタイミング を参照してください。 **注意：** Tenable Lumin サードパーティの統合データには対応していません。 2. 資産に事業の文脈を追加するために、Tenable Vulnerability Management でタグを作成します。 3. メトリクスの用語をレビューして、Vulnerability Priority Rating (VPR) および ACR (資産重大度の格付け) (ACR) の値について、またそれらがどのように資産のエクスポージャースコア (AES)、評価成熟度グレード、および Cyber Exposure Score (CES) に影響を与えるかについて理解します。 4. メトリクス計算のための時間を十分に確保します。詳細は、Tenable Lumin のデータのタイミング を参照してください。	1. レポジトリを Tenable Security Center から Tenable Lumin に同期します。すべての脆弱性データはすぐに同期されます。 **注意：** Tenable Lumin サードパーティの統合データには対応していません。 2. 資産に事業の文脈を追加するために、Tenable Security Center で資産を作成します。 3. Tenable Security Center から Tenable Lumin への同期を設定します。 同期が完了するのに十分な時間を取ります。詳細は、Tenable Lumin のデータのタイミング を参照してください。 4. 資産を事業の文脈タグに従って Tenable Vulnerability Management で表示します。詳細は、Manage Asset Tags を参照してください。 5. メトリクスの用語をレビューして、Vulnerability Priority Rating (VPR) および ACR (資産重大度の格付け) (ACR) の値について、またそれらがどのように資産のエクスポージャースコア (AES)、評価成熟度グレード、および Cyber Exposure Score (CES) に影響を与えるかについて理解します。 6. メトリクス計算のための時間を十分に確保します。詳細は、Tenable Lumin のデータのタイミング を参照してください。

Exposure を評価する

注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

CES を確認し、脆弱性管理分析を実行します。

1. Tenable Lumin ダッシュボードを使用して、CES を理解し、詳細ページにアクセスします。
    - **[Cyber Exposure Score]** ウィジェット - 他の Tenable のお客様 (Salesforce 業界および全体)と比較して、全体的なリスクはどの程度ですか?
    - **[Cyber Exposure Score Trend]** ウィジェット - 企業全体の総合的なリスクは、時間とともにどう変化していますか?
    - **[評価成熟度]** ウィジェット - どのくらいの頻度でどれだけ徹底的に資産をスキャンしていますか?
    - **[修正成熟度]** ウィジェット - 資産の脆弱性をどれだけ迅速かつ徹底的に修正していますか?
    - **[Cyber Exposure Score の低減]** ウィジェット - 上位 20 の推奨アクションのすべてを実行した場合、どのような影響があるでしょうか?
    - **[資産重大度の格付けの内訳]** ウィジェット - 対象となる資産はどのような程度の重要度のものですか?
    - **[資産のスキャンの分類]** ウィジェット - 資産上でどの種類のスキャンが実行されましたか?
    - **[緩和]** ウィジェット - どのような エンドポイント保護エージェント が資産で実行されていますか?
    - **[事業の文脈タグによる Cyber Exposure Score]** ウィジェット - 異なるタグ(固有のビジネス文脈)別に資産を比較するとどうですか?
2. ネットワークで最も重大な脆弱性を表示するには、脆弱性を VPR で並べ替えます。
3. ネットワークで最も重要な資産を表示するには、資産を ACR で並べ替えます。

ACR 値をカスタマイズする

Tenable が提供する ACR 値を確認してそれをカスタマイズすることで、企業固有のインフラや懸念事項を反映させます。

1. 資産ページを使用して、お持ちの資産に対する Tenable が提供した ACR 値を確認します。
    - その資産の相対的な重要性に比較して、ACR 値が高すぎると思われる資産がありますか？
    - その資産の相対的な重要性に比較して、ACR 値が低すぎると思われる資産がありますか？
2. 必要に応じて、資産の ACR 値を手動でカスタマイズします。

CES および AES を低減させる

CES および AESを下げるには、ネットワークの脆弱性に対処することが必要です。

重要: 非公開の検出結果は、Tenable Lumin 内のすべてのスコアから除外されます。詳細は、検出結果 を参照してください。

1. Tenable 推奨のアクションアイテムリストを表示します。
    - ネットワーク上のすべての資産に対する上位の推奨アクション。

      必要に応じて、上位の推奨アクションをエクスポートします。
    - ネットワーク上のすべてのソリューション。

      必要に応じて、ソリューションをエクスポートします。
2. 推奨事項を手順を実行して、ネットワークの脆弱性に対処します。

成熟させる

脆弱性管理戦略を成熟させます。

- CES および AES を下げるために、脆弱性の監視と対処を継続します。
- 企業内の他の人に推奨アクション(ソリューション)データを継続してエクスポートおよび共有し、脆弱性管理戦略を改善します。

エラーメッセージ

Tenable Vulnerability Management の API ステータスコードについては、Tenable 開発者ポータルを参照してください。

スキャン中

次の表は、Tenable Vulnerability Management で表示される可能性のあるスキャンエラーメッセージを説明しています。

一部のスキャンエラーは、次の Tenable Vulnerability Management スキャン制限事項を超えた場合に発生します。

スキャン制限事項

次の表は Tenable Vulnerability Management のスキャンの制限事項を示しています。

制限	説明
評価スキャンごとのターゲット IP アドレスまたはホスト名	Tenable Vulnerability Management は、1 回の評価スキャンでターゲットとする IP アドレスまたはホスト名の数を制限します (詳しくは、検出スキャンと評価スキャンを参照してください)。ホストターゲットの制限は、組織でライセンス付与されている資産数の 10 倍です。 たとえば、組織でライセンス付与されている資産数が 1,000 の場合、Tenable Vulnerability Management では 1 回の評価スキャンで 10,000 を超えるホスト名または IP アドレスをターゲットにできません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。
検出スキャンごとのターゲット IP アドレスまたはホスト名	Tenable Vulnerability Management は、1 回の検出スキャンでターゲットとする IP アドレスまたはホスト名の数を制限します (詳しくは、検出スキャンと評価スキャンを参照してください)。ホストターゲットの制限は、組織でライセンス付与されている資産数の 1,000 倍です。 たとえば、組織でライセンス付与されている資産数が 1,000 の場合、Tenable Vulnerability Management では 1 回の検出スキャンで 1,000,000 を超えるホスト名または IP アドレスをターゲットにできません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。

スキャンあたりのホストスキャン結果数	Tenable Vulnerability Management は、1 回のスキャンで生成できるライブホストの数を制限しています。ライブホストスキャン結果の制限は、所属組織のライセンスのある資産数の 1.1 倍です。 たとえば、所属組織のライセンスのある資産カウントが 1,000 の場合、Tenable Vulnerability Management では 1 回のスキャンで 1,100 を超えるライブホストのスキャン結果を生成できません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。Tenable Vulnerability Management は、検出スキャンにはライブホストスキャン結果の上限を適用しません。 Tenable Vulnerability Management1 回のスキャンで生成できるスキャン結果のデッドホストの数も制限しています。デッドホストスキャン結果の上限は、所属組織のライセンスのある資産カウントの 100 倍です。 たとえば、所属組織のライセンスのある資産カウントが 1,000 の場合、Tenable Vulnerability Management では 1 回のスキャンで 100,000 を超えるデッドホストのスキャン結果を生成できません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。
スキャンごとのターゲット IP アドレスまたは範囲	スキャンのターゲットを設定する際に、300,000 個を超えるコンマ区切りの IP アドレスまたは範囲を指定することはできません。
アクティブスキャン	コンテナで 25 を超えるスキャンを同時に実行することはできません。
チャンクのスキャン	Tenable Vulnerability Management は、スキャンチャンクを 10,000 個のホストまたは 150,000 件の検出結果に制限します。スキャンチャンクがいずれかの値を超えると、Tenable Vulnerability Management はスキャンを処理せず、最終的に中止します。
スキャンの設定	Tenable Vulnerability Management で作成できるスキャン設定の数は 10,000 スキャンに制限されています。Tenable では、新しいスキャンを作成する代わりに、スケジュールされたスキャンを再利用することを推奨しています。このアプローチにより、ユーザーインターフェースの待ち時間が短縮できます。

スキャンの作成、変更、起動の詳細については、スキャンを管理するを参照してください。スキャンステータスの値に関する詳細は、スキャンステータスを参照してください。

警告	メッセージ	推奨アクション
アカウントターゲットの上限	ターゲット数がこのアカウントの制限を超えています。カスタマーサポートに連絡して、ライセンスをアップグレードしてください。	スキャンターゲット数の上限に達しました。ライセンスをアップグレードしてスキャンターゲット数の上限を引き上げるには、Tenable サポート にご連絡ください。
エージェントグループエラー	エージェントグループの取得中に予期せぬエラーが発生しました。	
エージェントグループのアクセス許可	所有者が、設定された一部のエージェントグループに対するアクセス権を持っていません。	このスキャンに対して選択された一部のエージェントグループにアクセスできません。適切なグループを選択します。詳細は、エージェントグループを参照してください。
すべて非アクティブなスキャナー	すべてのターゲットが、アクティブなスキャナーのないスキャナーグループにルーティングされました。	
すべてのスキャンの中止	すべてのアクティブなスキャンが中止されました。	Tenable Vulnerability Management は、システムの中止リクエストにより、スキャンを中止しました。スキャンを再実行してください。
自動ルーティングのカスタムターゲット	自動ルーティングのスキャンでは、カスタムのスキャンターゲットは現在サポートされていません。	カスタムターゲットに対してスキャンを実行するには、特定のスキャナーを選択します。
自動ルーティングが無効	スキャンは自動ルーティングするように設定されていますが、自動ルーティングが有効になっていません。	
同時ス	このアカウントの同時スキャン数の上限	同時スキャンの上限に達しました。後でス

警告	メッセージ	推奨アクション
キャンの上限	に達したため、スキャンを完了できませんでした。カスタマーサポートに連絡して、ライセンスをアップグレードしてください。	キャンを再実行してください。
同時スキャン数の上限に到達	このアカウントの同時スキャン数の上限に達したため、スキャンを完了できませんでした。カスタマーサポートに連絡して、ライセンスをアップグレードしてください。	同時スキャンの上限に達しました。後でスキャンを再実行してください。
競合	インデックス作成から一時停止への移行はサポートされていません。	スキャンが完了し、現在インデックス作成中です。インデックス作成が完了するまでお待ちください。
空のスキャナーグループ	スキャンが、スキャナーが割り当てられていないスキャナーグループを使用するように設定されています。	スキャナーグループに機能しているスキャナーが含まれていることを確認してから、スキャンを再実行してください。詳細は、スキャナーグループを参照してください。
空のターゲット	スキャンに対してターゲットが設定されていません。	スキャン設定に有効なターゲット範囲が1つ以上含まれていることを確認してから、スキャンを再実行してください。
非アクティブなスキャナー	スキャンが、アクティブなスキャナーのないスキャナーグループを使用するように設定されています。	スキャナーグループに機能しているスキャナーが含まれていることを確認してから、スキャンを再実行してください。詳細は、スキャナーグループを参照してください。
インデックス作成エラー	タスクの処理中に予期せぬエラーが発生しました。次のターゲットを再スキャンする必要があるかもしれません。[スキャンターゲット]	未スキャンのターゲットまたは再スキャンが必要なターゲットのスキャンを再実行してください。
初期化エラー	初期化中に予期せぬエラーが発生しました。	Tenable Vulnerability Management がスキャンを中止しました。スキャンを再実行

警告	メッセージ	推奨アクション
		してください。
無効な AWS ターゲット	スキャンに対して有効な AWS ターゲットが設定されていません。	スキャンに有効な AWS スキャンターゲットが含まれていることを確認し、スキャンを再実行してください。詳細は、ターゲット を参照してください。
無効な PCI スキャナー	PCI スキャンは、Tenable Cloud Scanners を使用する場合のみ起動できます。	Tenable クラウドセンサーを使用して Tenable PCI ASV スキャンを実行します。詳細は、クラウドセンサー を参照してください。
無効なタグターゲット	設定されたタグの資産からターゲット FQDN または IP を解決できませんでした。	スキャンに対して設定されたタグの 1 つ以上の資産にスキャンターゲットを関連付ける必要があります。タグの設定を確定してから、スキャンを再実行してください。詳細は、タグ を参照してください。
Invalid Target (無効なターゲット)	ターゲットを解決できません。	スキャンに有効なスキャンターゲットが含まれていることを確認してから、スキャンを再実行してください。詳細は、ターゲット を参照してください。
無効なターゲット範囲	スキャンに対して無効なターゲット範囲が設定されています。*[スキャンターゲット]*	無効なスキャンターゲット範囲を修正または削除してから、スキャンを再実行してください。詳細は、ターゲット を参照してください。
無効なターゲット	スキャンに対して有効なターゲットが設定されていません。	スキャンターゲットが次の基準を満たしていることを確認してください。 • IP アドレスに有効な形式を使用している • IP アドレスのリストを区切るためにコンマを使用している

警告	メッセージ	推奨アクション
		• ターゲットグループ内の IP アドレスに有効な形式を使用している 詳細は、ターゲットとターゲットグループを参照してください。 トラブルシューティングでさらにサポートが必要な場合は、ナレッジベースの記事を参照してください。
ジョブ初期化エラー	初期化中に予期せぬエラーが発生しました。スキャンターゲットと設定に異常がないか確認し、問題が解決しない場合はサポートに連絡してください。	スキャンを再実行してください。
Log4j DNS リクエストの失敗	DNS [スキャンターゲット] を解決できないため、Log4j 脆弱性をチェックできません。	未スキャンのターゲットまたは再スキャンが必要なターゲットのスキャンを再実行してください。
最大検出結果エラー	検出結果が最大数に達しました。	Tenable Vulnerability Management のスキャン制限事項を確認し、スキャン設定を調整して許可された検出結果の数を生成するようにします。
ホスト最大数到達エラー	スキャンが、許可されたホストの最大数を超えました。	Tenable Vulnerability Management のスキャン制限事項を確認し、スキャン設定を調整して許可されたホストの数をスキャンするようにします。
ネットワークの輻輳の検出	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。これは、1 つ以上のリモートホストが、スキャン中に発生したネットワークトラフィックの輻輳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している可	輻輳のリスクを軽減する方法 • **最大ホスト数**の値を下げる • ポリシーで**ネットワーク読み取りタイムアウト**の値を引き上げる

警告	メッセージ	推奨アクション
	能性があります。	
使用可能なスキャナーなし	スキャンを実行できるスキャナーが見つかりません。	適切なスキャナーを選択していることを確認してから、スキャンを再実行してください。
設定されたエージェントグループなし	スキャンには設定されたエージェントグループがありません。	少なくとも 1 つのエージェントグループをスキャンに追加してください。
スキャンポリシーなし	スキャンポリシーを使用してスキャンを設定する必要があります。	スキャンにスキャンポリシーが必要です。スキャンポリシーを設定してから、スキャンを再実行してください。
タグターゲットなし	設定されたタグから有効なターゲットが見つかりませんでした。	
通知エラー	このスキャンの通知が送信されなかった可能性があります。	スキャンは完了しましたが、通知の送信に失敗しました。
所有者が無効	スキャンの所有者が無効になっています。	スキャンの所有者を有効にするか、有効なユーザーに所有権を譲渡してください。詳細は、権限 を参照してください。
一時停止スキャンのタイムアウト	一時停止中のスキャンが *[最大許容一時停止]* 日数のタイムアウトを超えたため一部のタスクが中止されました。ターゲットを再スキャンする必要があるかもしれません。	一時停止中のスキャンが、最大一時停止期間を超えました。スキャンが終わっていないすべてのスキャンターゲットに対してスキャンを再実行します。
保留中のスキャンのタイムアウト	想定タイムアウトが過ぎる前に、スキャンの実行に移行できませんでした。	選択したスキャナーグループに十分なキャパシティがあることを確認してから、スキャンを再実行してください。詳細は、スキャナーグループ を参照してください。
ポリシーの	スキャンの所有者が、設定されたポリ	このスキャンのスキャンポリシーに対するア

警告	メッセージ	推奨アクション
アクセス許可	シーに対してアクセス権を持っていません。	クセス権がありません。適切なアクセス許可でスキャンを再実行してください。詳細は、権限を参照してください。
ポートスキャナの最大ポート数超過	ポートスキャナがターゲット *[ターゲット名]* に対して *[数]* より多くのポートを開いていることを検出し、報告されたポートの数が *[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悪影響を与えるため、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したいと思われるかもしれません。
処理エラー	処理中に予期せぬエラーが発生しました。	Tenable Vulnerability Management がスキャンを中止しました。スキャンを再実行してください。
非アクティブなスキャナーにルーティング	次のターゲットは、アクティブなスキャナーのないスキャナーグループにルーティングされました。*[スキャンターゲット]*	スキャナーグループに機能しているスキャナーが含まれていることを確認してから、スキャンを再実行してください。詳細は、スキャナーグループを参照してください。
実行中のスキャンのタイムアウト	スキャンが最大許容ランタイムを超過しました。	一部のスキャンターゲットのスキャンに時間がかかりすぎている可能性があります。スキャンを再実行してください。
スキャンが中止されました	スキャンが初期化中に停止したため中止されました。	Tenable Vulnerability Management がスキャンを中止しました。スキャンを再実行してください。
スキャンが中止され	スキャンの初期化中にエラーが発生しました。	Tenable Vulnerability Management は、スキャンの初期化に失敗しました。スキャ

警告	メッセージ	推奨アクション
ました		ンを再実行してください。
スキャンが中止されました	Tenable Nessus からのプラグインセット情報の取得に失敗しました。	Tenable Vulnerability Management は、プラグインセットのダウンロードに失敗しました。スキャンを再実行してください。
スキャンが中止されました	割り当てられたスキャナーが見つかりませんでした。	Tenable Vulnerability Management は、選択されたスキャナーを見つけることができませんでした。別のスキャナーを選択して、スキャンを再実行してください。
スキャン抽出エラー	スキャンの抽出中にエラーが発生しました。	
スキャン抽出タイムアウトエラー	スキャンの抽出がタイムアウトしました。	
スキャン禁止	ユーザー定義のルールに違反したため、*[スキャンターゲット]*のスキャンの試行が拒否されました。	このスキャンターゲットは、スキャンから除外されています。このターゲットをスキャンする場合は、除外から削除して、スキャンを再実行してください。詳細は、除外 を参照してください。 あるいは、スキャンを実行するための適切なユーザーアクセス許可がないのかもしれません。ユーザーアクセス許可をチェックし、スキャンを再実行してください。詳細は、権限 を参照してください。
スキャンジョブ初期化エラー	スキャンを初期化できませんでした。スキャンターゲット設定に異常がないか確認し、問題が解決しない場合はサポートに連絡してください。	Tenable Vulnerability Management がスキャンの起動に失敗しました。正しいスキャンターゲットを使用してスキャンを再実行してください。詳細は、ターゲット を参照してください。
スキャナー	割り当てられたスキャナーが無効になっ	ユーザーが選択されたスキャナーを無効に

警告	メッセージ	推奨アクション
が無効	ています。	しました。別のスキャナーを選択して、スキャンを再実行してください。
スキャナーエラー	割り当てられたスキャナーの取得中に予期せぬエラーが発生しました。	
スキャナーグループエラー	スキャナー *[スキャナー ID]* のスキャナーグループを読み込めません。	スキャン設定に有効なターゲット範囲が1つ以上含まれていることを確認してから、スキャンを再実行してください。
スキャナー中断	スキャン中にスキャナーの中断が検出されたため、このスキャンは想定より長く実行された可能性があります。	このエラーは、Tenable Nessus スキャナーがスキャンタスクを完了できず、Tenable Vulnerability Management がそのスキャンタスクを別のスキャナーに再割り当てした場合に発生します。これは通常、元のスキャナーが意図的にオフラインになった(ユーザーがスキャナーを停止、電源を切った、リンクを解除したなど)か、スキャンタスクの実行中に予期しないエラー(電源やネットワークの損失など)が発生した場合に発生します。 中断を防ぐために必要に応じて Tenable Nessus スキャナーを調整します。
スキャナーが見つからない	割り当てられたスキャナーが見つかりませんでした。	Tenable Vulnerability Management は、選択されたスキャナーを見つけることができませんでした。有効なスキャナーを選択して、スキャンを再実行してください。
スキャナーのアクセス許可	スキャンの所有者が、割り当てられたスキャナーへのアクセス権を持っていません。	選択されたスキャナーに対するアクセス権がありません。別のスキャナーを選択して、スキャンを再実行してください。詳細は、権限を参照してください。
タスクのス	スキャナーでのストール後にタスクは自	スキャナーが適切に機能しており、スキャ

警告	メッセージ	推奨アクション
トール	動的に中断されました。次のターゲットを再スキャンする必要があるかもしれません。*[スキャンターゲット]*	ンに十分な容量があることを確認してから、スキャンされていないターゲットまたは再スキャンが必要なターゲットに対してスキャンを再実行してください。
タグターゲットエラー	スキャンに関連付けられたタグターゲットの取得に失敗しました。	Tenable Vulnerability Management は、スキャンターゲットを取得できませんでした。ターゲットを検証して、スキャンを再実行してください。詳細は、ターゲット を参照してください。
ターゲットアクセスエラー	スキャンの所有者が設定されたターゲットへのアクセス権を持っていません。	スキャンを実行するための適切なユーザーアクセス許可がありません。ユーザーアクセス許可をチェックし、スキャンを再実行してください。詳細は、権限 を参照してください。
ターゲットグループのアクセス許可	スキャンの所有者が、設定された一部のターゲットグループへのアクセス権を持っていません。	スキャン所有者のアクセス許可を確認してから、スキャンを再実行してください。詳細は、ターゲットグループ を参照してください。
ターゲット上限	ターゲットが Tenable Vulnerability Management で許容されている最大値を超えました。	スキャンターゲットの範囲が広すぎます。スキャン設定に有効なターゲット範囲が含まれていることを確認してから、スキャンを再実行してください。詳細は、ターゲット を参照してください。
ターゲット範囲の上限	ターゲット範囲が最大許容ターゲットを超えています。*[スキャンターゲット]*	設定されたスキャンターゲットの範囲を確認または縮小して、スキャンを再実行してください。詳細は、ターゲット を参照してください。
ターゲットを完了できません	次のターゲットは、許可されたスキャン時間でスキャンを完了できず、再スキャンする必要があります。*[スキャンター*	未スキャンのターゲットまたは再スキャンが必要なターゲットのスキャンを再実行します。

警告	メッセージ	推奨アクション
	ゲット]	
タスク初期化エラー	初期化中に予期せぬエラーが発生しました。次のターゲットを再スキャンする必要があるかもしれません。[*スキャンターゲット*]	未スキャンのターゲットまたは再スキャンが必要なターゲットのスキャンを再実行してください。
タスク処理エラー	処理中に予期せぬエラーが発生しました。次のターゲットを再スキャンする必要があるかもしれません。[*スキャンターゲット*]	未スキャンのターゲットまたは再スキャンが必要なターゲットのスキャンを再実行してください。
移行タイムアウト	一部のタスクが[*再開、一時停止、または停止*]中に停止し、中止されました。ターゲットを再スキャンする必要があるかもしれません。	一部のスキャンターゲットでスキャンを完了できませんでした。すべての未スキャンのスキャンターゲットに対してスキャンを再実行します。
ターゲットをルーティングできない	次のターゲットで一致するスキャナールートが見つかりません。[*スキャンターゲット*]	Tenable Vulnerability Management は、スキャン設定で指定された1つ以上のスキャンターゲットを見つけることができませんでした。以下を実行してから、スキャンを再実行してください。 • スキャン設定が正しいネットワークを指定していることを確認します • そのネットワークのスキャナーグループのスキャンルーティング設定を確認します

ダッシュボード

ダッシュボードは対話式のグラフィカルなインターフェースで、特定の目標や業務プロセスに関連する重要業績評価指標 (KPI) を一目で表示するためによく使用されます。

この **[ダッシュボード]** ページには、以下を表すタイルが含まれています。

- Tenable 提供のダッシュボード。Tenable が提供するダッシュボードテンプレートの完全なインデックスについては、Tenable Vulnerability Management ダッシュボードを参照してください。

  > **注意:** ライセンスによっては、その他のダッシュボードが含まれます。たとえば Tenable Lumin ダッシュボードなどです。

- 自分が作成したダッシュボードテンプレートベースのダッシュボードまたはカスタムダッシュボードを Tenable が提供するウィジェットやカスタムウィジェットで作成するには、ダッシュボードの作成 を参照してください。

- 他のユーザーが共有しているダッシュボード **[共有されているダッシュボード]** タブをクリックして、他のユーザーから共有されているダッシュボードを表示します。

脆弱性管理ダッシュボード

この Tenable が提供するダッシュボードは、ご利用中の脆弱性管理プログラムに関する実用的なインサイトをビジュアル化して表示します。スキャンが実行されるたびに、Tenable Vulnerability Management はダッシュボードデータを更新します。

注意: Tenable Vulnerability Management がデータのインデックスを作成している間は、スキャンが完了してからダッシュボードのデータが更新されるまでに時間がかかる場合があります。

[脆弱性管理の概要] ダッシュボードにアクセスする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[脆弱性管理]** をクリックします。

   [脆弱性管理の概要] ダッシュボードが表示されます。

個別の項目にカーソルを合わせて追加情報を表示したり、項目をクリックしてデータの詳細にドリルダウンしたりできます。

ヒント: [脆弱性管理の概要] のすべてのチャートには、**[新規]**、**[アクティブ]**、**[再表面化]** の脆弱性データが表示されます。ただし、各グラフに表示されるカウント数やデータは別の理由で異なる場合があります。たとえば、**[脆弱性優先度の格付け (VPR)]** ウィジェットは VPR カテゴリ別に脆弱性を整理しますが、**[脆弱性の傾向分析]** ウィジェットは CVSS に基づいた深刻度カテゴリ別に脆弱性をグラフ化します。深刻度と VPR のメトリクスの比較方法に関する詳細は、CVSS と VPR を参照してください。

[脆弱性管理の概要] では、次のウィジェットに対してアクションを実行できます。

ウィジェット	アクション
Cyber Exposure ニュースフィード	このウィジェットでは、セキュリティインシデントに関連する最新の Tenable ブログ投稿を紹介します。 • タイルをクリックして、Tenable ブログ投稿に移動します。 • ⌄ または ⌃ ボタンをクリックすると、フィードを折りたたんだり展開したりできます。 • ❮ または ❯ ボタンをクリックすると、タイルをスクロールできます。

統計	このウィジェットには、過去 30 日間で、ネットワークで検出された深刻度が最も高い脆弱性をまとめられています。 • 過去 30 日間で検出された脆弱性の総数と、深刻度が高い脆弱性(**重大**および**高**)の数を表示します。 • 脆弱性のリストを表示するには、いずれかのカウントをクリックします。 **[重大]**または**[高]**のカウントを選択した場合、**[脆弱性]**ページは深刻度でフィルタリングされた状態で表示されます。詳細は、View Vulnerabilities by Plugin を参照してください。 • ライセンスのある資産の総数、過去 7 日間で検出された資産の数、および過去 30 日間で検出された資産の数を表示します。 必要に応じて、新たに検出された資産を登録します。 • 資産のリストを表示するには、いずれかのカウントをクリックします。 **[7 日]**または**[30 日]**のカウントを選択した場合は、時間範囲でフィルタリングされた**[資産]**ページが表示されます。詳細は、View Asset Details in the Assets Plane を参照してください。 • 過去 90 日間で実行したスキャンの数と、成功した割合と失敗した割合を表示します。 失敗したスキャンを調査するには、ステータスが**[中止]**または**[キャンセル]**のスキャンを確認します。詳細は、View Scans を参照してください。 • ウィジェット内のデータをエクスポートするには、⋮ボタンをクリックして形式を選択します。
CISA アラート AA22-011A および AA22-047A	このウィジェットは、特定または緩和された CISA アラート AA22-011A および AA22-047A の脆弱性に関連付けられたリスクの脆弱性数を提供します。 • プラグインごとに関連する脆弱性のリストを表示するには、**[脆弱性]**列でいずれかのタイルをクリックします。 脆弱性の状態ごとにフィルタリングされた結果が、**[脆弱性]**ページに表示されます。詳細については、プラグイン別の脆弱性の表示を参照してください。

	• 資産ごとに関連する脆弱性のリストを表示するには、**[資産]** 列でいずれかのタイルをクリックします。 脆弱性の状態でフィルタリングされた **[脆弱性]** ページが表示されます。詳細については、資産別の脆弱性の表示 を参照してください。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
Vulnerability Priority Rating (VPR)	このウィジェットは、VPR 別に整理された、ネットワーク上の脆弱性の数をまとめたものです。詳細は、CVSS と VPR を参照してください。 • VPR 範囲でフィルタリングされた脆弱性のリストを表示するには、いずれかのタイルをクリックします。 **[脆弱性]** ページが、選択した範囲でフィルタリングされた状態で表示されます。詳細は、View Vulnerabilities by Plugin を参照してください。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
SLA 進捗状況: 脆弱性の経過日数	このウィジェットでは、深刻度とサービスレベル契約 (SLA) への遵守度別で脆弱性の数をビジュアル化します。Tenable Vulnerability Management による SLA 深刻度の計算方法を変更するには、全般設定を参照してください。 • 脆弱性のリストを表示するには、いずれかのタイルをクリックします。 **[脆弱性]** ページが、深刻度でフィルタリングされた状態で表示されます。詳細は、View Vulnerabilities by Plugin を参照してください。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
脆弱性の傾向分析	このウィジェットには、ネットワーク上の一定期間における、深刻度が **[重大]**、**[高]**、**[中]**、**[低]** の脆弱性の累積数が表示されます。詳細は、CVSS と VPR を参照してください。 • 特定の深刻度のデータを表示または非表示にするには、グラフ凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示に

	します。 • 過去の脆弱性カウントと深刻度データを表示するには、グラフ上のポイントにカーソルを合わせます。 • 最新の脆弱性リストを表示するには、グラフのポイントをクリックします。 **[脆弱性]** ページが、選択した深刻度と、**[新規]**、**[アクティブ]**、**[再表面化]** の状態別にフィルタリングされた状態で表示されます。詳細は、View Vulnerabilities by Plugin を参照してください。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
悪用されうる脆弱性 (重大と高)	このウィジェットは、ネットワーク上に存在する脆弱性の深刻度が **[重大]** および **[高]** の数を、悪用される可能性の特性カテゴリ別に整理してまとめたものです。1 つの脆弱性には悪用される可能性がある特性が複数あり、複数のカテゴリにカウントされる場合があります。 • 降順の優先順位で脆弱性の数を見るには、カテゴリとカウントを左から右に見ます。 • 脆弱性のリストを表示するには、グラフにあるいずれかのバーをクリックします。 **[脆弱性]** ページが、**[重大]** と **[高]** の深刻度と、選択した悪用される可能性の特性でフィルタリングされた状態で表示されます。詳細は、View Vulnerabilities by Plugin を参照してください。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
将来の脅威: まだ悪用されていない脆弱性	このウィジェットでは、**[エクスプロイトコード成熟度]** と **[脆弱性公開日]** で判断された、まだ悪用されていない脆弱性をまとめています。 • 降順の優先順位で脆弱性の数を見るには、カテゴリとカウントを左上から右下に見ます。Tenable は、既知のエクスプロイトが現れる前から、概念実証を使用して脆弱性に対処することをお勧めします。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式

	を選択します。
脆弱性の経過日数	このウィジェットには、SLA の管理に役立つように、脆弱性の経過日数 (**[初めて確認された脆弱性]** の日付が基準) を深刻度別にまとめています。深刻度の詳細については、CVSS と VPRを参照してください。 • 脆弱性のリストを表示するには、いずれかの脆弱性カウントをクリックします。 **[脆弱性]** ページが、選択した **[初めて確認された脆弱性]** の日付順に、深刻度別でフィルタリングされた状態で表示されます。詳細は、View Vulnerabilities by Plugin を参照してください。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。

脆弱性管理の概要 (調査)

[脆弱性管理の概要 (調査)] ダッシュボードでは、経営陣向けにリスク情報の概要が一目でわかるように表示できます。一方、セキュリティアナリストがウィジェットをクリックして技術的な詳細をドリルダウンすることもできます。Tenable Vulnerability Management はスキャンを実行するたびにダッシュボードデータを更新します。

注意: Tenable Vulnerability Management がデータのインデックスを作成している間、スキャンが完了してからダッシュボードのデータが更新されるまでに時間がかかる場合があります。

個別の項目にカーソルを合わせるとデータの概要が表示され、クリックするとドリルダウンして詳細を表示できます。

[脆弱性管理の概要 (調査)] では、次のウィジェットを使用できます。

ウィジェット	アクション
Cyber Exposure ニュースフィード	このウィジェットでは、セキュリティインシデントに関連する最新の Tenable ブログ投稿を紹介します。 • タイルをクリックして、Tenable ブログ投稿に移動します。 • ﹀ または ﹀ ボタンをクリックすると、フィードを折りたたんだり展開したりできます。 • 〈 または 〉 ボタンをクリックすると、タイルをスクロールできます。
ソース別の深刻度統計	このウィジェットは、複数のソース (Tenable Nessus スキャン、Tenable Nessus Agents、Frictionless Assessment) から収集された脆弱性の数を示します。このウィジェットに表示される深刻度の数に基づいて、軽減する脆弱性の優先順位を決定します。 • 特定のカテゴリの資産のリストを表示するには、関連するカテゴリの概要情報をクリックします。 **[検出結果]** ページが表示され、そのカテゴリで検出された資産の詳細が表示されます。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。

Tenable Research アドバイザリ	このウィジェットは、Tenable Research によって検出された現在の主要な脅威の 2 つのインジケーターを提供します。赤のインジケーターは関連する脆弱性が存在することを示し、これらの脆弱性にパッチが適用されるとインジケーターは緑になります。 • タイルをクリックすると、**[検出結果]** ページが表示され、**欠落したパッチ**と**適用されたパッチ**で検出された資産の詳細が表示されます。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
Vulnerability Priority Rating (VPR)	このウィジェットには、Vulnerability Priority Rating (VPR) 別にグループ化された脆弱性が表示されます。VPR は、Tenable の予測に基づいた優先順位付けプロセスによって出力され、進化する脅威の状況に対応するために継続的に更新されます。 Tenable は、ネットワーク上の資産の初期スキャンの後、機械学習アルゴリズムを使用して初期 VPR を計算します。このアルゴリズムは、各脆弱性の 150 以上の異なる側面を分析してリスクレベルを判断します。一覧表示される脆弱性は、左にあるものが最も VPR が高く、右にあるものが最も低くなります。詳細は、CVSS と VPR を参照してください。 • 特定の範囲で検出された資産の詳細を表示するには、VPR の範囲をクリックします。 **[検出結果]** ページが表示され、選択した範囲で検出された資産の詳細が表示されます。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
SLA の進捗: 脆弱性の経過日数	このウィジェットは、Vulnerability Priority Rating (VPR) スコアと脆弱性の経過日数で分類された脆弱性ビューを提供し、企業がサービスレベルアグリーメント (SLA) を管理するのに役立ちます。 Tenable は、過去 X 日以内の日付フィルターを使用して SLA を満たしていない脆弱性を計算します。SLA を満たす脆弱性は、X 日より古い日付フィルターを使用します。

	デフォルトの SLA 設定を適用する場合 • **重大**: 行は 9.0 を超える VPR を使用します。 • **高**: 行は 7.0 ~ 8.9 の VPR を使用します。 • **中**: 行は 4.0 ~ 6.9 の VPR を使用します。 • **低**: 行は 0 ~ 3.9 の VPR を使用します。 Tenable Vulnerability Management による SLA 深刻度の計算方法については、全般設定 を参照してください。 • 特定のカテゴリについて検出された資産のリストを表示するには、SLA カテゴリの下の [概要情報] をクリックします。 **[検出結果]** ページに資産の詳細が表示されます。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
悪用されうる脆弱性 (重大と高)	修正に優先順位を付けられるように、このウィジェットは、最も深刻な現在の脅威、悪用されうる脆弱性 (重大と高) に焦点を当てています。各バーは、悪用される可能性の特性ごとにグループ化された脆弱性を表しています。 • **マルウェアによる悪用**: ウイルス、ワーム、スパイウェア、アドウェア、ランサムウェアなどの悪意のあるソフトウェアによって悪用される可能性のある脆弱性。 • **リモートで悪用可能 (複雑度が低い)**: リモートで簡単に悪用でき、悪用するためのスキルや情報収集をほとんど必要としない脆弱性。 • **ローカルで悪用可能 (複雑度が低い)**: ローカルアクセスで簡単に悪用でき、悪用するためのスキルや情報収集をほとんど必要としない脆弱性。 • **フレームワークにより悪用可能 (Metasploit)**: Metasploit などのさまざまなエクスプロイトフレームワークにインポートされた一般に公開されている悪用コードを含み、リスクのある脆弱性。これらの一般的なエクスプロイトフレームワークは簡単にアクセス可能で、セキュリティ研究者と悪意のある攻撃者の両者が使用しています。 • **リモートで悪用可能 (複雑度が高い)**: リモートで悪用できるものの、悪

	用するには高度なスキルと情報収集が必要な脆弱性。 **注意**: 1 つの脆弱性が複数の悪用される可能性のカテゴリに該当する可能性があるため、これらのグループは相互に排他的ではありません。Tenable では、一番左の列の **[マルウェアによる悪用]** の脆弱性から優先的に修正を始めることを推奨しています。 • 特定のカテゴリの資産の詳細を表示するには、グラフ上のバーのいずれかをクリックします。 **[検出結果]** ページが表示され、そのカテゴリで検出された資産の詳細が表示されます。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
将来の脅威: まだ悪用されていない脆弱性	このウィジェットは、エクスプロイトコードの成熟度と脆弱性の公開日に基づく脆弱性のビューを提供します。列には、指定された期間内に公開された、企業内に存在する脆弱性の数が表示されます。行には、エクスプロイトコードの成熟度が表示されます。**概念実証 (PoC)** は**未実証のエクスプロイト**よりも深刻です。 • 特定のカテゴリの資産のリストを表示するには、**[公開済み]** カテゴリの下の数をクリックします。 **[検出結果]** ページが表示され、そのカテゴリで検出された資産の詳細が表示されます。 **ヒント**: Tenable は、既知のエクスプロイトが発生する前から、概念実証を使用して脆弱性に対処することをお勧めします。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
スキャンの状態	このウィジェットは、認証の成功と失敗に関連したスキャンの状態に関するサマリーを示します。5 つの列には、以下に関連する資産数が表示されます。 • **認証成功** - スキャンは完全な管理者や root 権限で正常に認証されます。スキャン結果は最も包括的なものです。

	• **成功するがアクセスが不十分** - スキャンは正常に認証されるものの、特権アクセスがありません。スキャン結果は、権限のないローカルユーザーの範囲に限定されます。 • **成功するが断続的に失敗する** - スキャンの認証情報は断続的に失敗します。セッションレート制限、セッションの同時実行制限、または一貫した認証の成功を妨げるその他の問題が原因で発生します。 • **認証の失敗 (認証情報)** - 入力された認証情報が正しくありません。 • 特定のカテゴリに分類される資産のリストを表示するには、目的のカテゴリをクリックします。 **[検出結果]** ページが表示され、そのカテゴリで検出された資産の詳細が表示されます。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。
脆弱性の経過日数: SLA の管理	このウィジェットは、深刻度と経過日数に基づく脆弱性のビューを提供します。列には、指定された期間内に公開された、企業内に存在する脆弱性の数が表示されます。行には、脆弱性の深刻度レベルが表示されます。 • 特定のカテゴリの資産の詳細を表示するには、目的のカテゴリの脆弱性数をクリックします。 **[検出結果]** ページが表示され、そのカテゴリで検出された資産の詳細が表示されます。 • ウィジェット内のデータをエクスポートするには、⋮ ボタンをクリックして形式を選択します。

Tenable Web App Scanning ダッシュボード

デフォルトの **Web Applications Scanning** ダッシュボードには Tenable Web App Scanning が収集したデータが表示されます。

下の表では、**Web Applications Scanning** ダッシュボードに表示されるセクションとウィジェットについて説明します。ウィジェットをクリックすると、データに関する詳細をウィジェットに表示できます。

Tenable Web App Scanning 統計

下の表では、**ウェブアプリケーションのスキャン** ダッシュボードの [Statistics] セクションに表示されるウィジェットについて説明します。ウィジェットをクリックすると、データに関する詳細をウィジェットに表示できます。

ウィジェット	説明
検出結果	Tenable Web App Scanning が検出した検出結果の数。結果は、深刻度 (**重大**、**高**) で分類されます。 Tenable でリスク分析に使用する脆弱性の格付けと深刻度のメトリクスについては、*Tenable Vulnerability Management ユーザーガイド*の深刻度と VPR を参照してください。
スキャンされたウェブ資産	経時的にスキャンされた資産の数。
不完全なスキャン	過去 90 日間の不完全なスキャンの数。
認証されていないスキャン	過去 90 日間の認証されていないスキャンの数。

OWASP Top 10

このチャートには、最新の OWASP (Open Web Application Security Project) の Top 10 Most Critical Web Application Security Risks (上位 10 個の最も重大なウェブアプリケーションセキュリティリスク) ドキュメントに記載されている Tenable Web App Scanning によって検出された脆弱性が表示されます。

ダッシュボードページの表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ダッシュボードに対してカスタムウィジェットを作成するを追加すると、Tenable Vulnerability Management は適用される日付フィルターに基づいてダッシュボードデータを更新します。

[ダッシュボード] ページを表示する方法

1. 次のいずれかの方法で **[ダッシュボード]** ページにアクセスします。
   - 任意の Tenable 提供ダッシュボードページで、**[ダッシュボード]** ボタンをクリックします。
   - 任意の他のページで、次を実行します。
     a. 左上にある ☰ ボタンをクリックします。

        左側にナビゲーションプレーンが表示されます。

     b. 左側のナビゲーションプレーンで **[ダッシュボード]** をクリックします。

   [ダッシュボード] ページが表示されます。このページには、以下を表すタイルが含まれています。
   - Tenable 提供のダッシュボード
   - 作成したダッシュボード
   - 他のユーザーが共有しているダッシュボード
2. 次のいずれかを行います。
   - 左上にある **[検索]** バーを使用して、特定のダッシュボードを検索します。
   - 左上にあるドロップダウンを使用して、**[ダッシュボード]** ページに表示されるダッシュボードの順序を変更します。
   - **[グループ]** セクションで、次のいずれかを行います。
     - **[検索グループ]** バーを使用して、特定のダッシュボードグループを検索します。
     - **[共有されているダッシュボード]** タブをクリックして、共有されているダッシュボードを表示します。

    - **[利用可能な更新]**タブをクリックして、自動更新の対象となるダッシュボードを表示します。

- 個別のダッシュボードタイルにカーソルを合わせて、追加情報を表示します。
- グリッド表示とリスト表示を切り替えます。
- デフォルトのダッシュボードを設定します。
- ダッシュボードを編集します。
- ダッシュボードを共有します。
- ダッシュボードをエクスポートします。
- ダッシュボードを複製します。
- ダッシュボードを削除します。
- ダッシュボードのタイルをクリックして、個別のダッシュボードを表示します。

Tenable 提供のダッシュボード

[ダッシュボード] ページ上で、Tenable Vulnerability Management はダッシュボードを次の順序で表示します。

1. Tenable 提供のダッシュボード。Tenable が提供するダッシュボードテンプレートの完全なインデックスについては、Tenable Vulnerability Management ダッシュボードを参照してください。
2. 作成したダッシュボードと共有されたダッシュボード

注意: **[ダッシュボード]** ページの右上にあるドロップダウンを使用して、ダッシュボードが表示される順序を変更できます。

表示される Tenable 提供のダッシュボードは、お持ちのライセンスによって異なりますが、次が含まれます。

Dashboard	ライセンス
脆弱性管理の概要	Tenable Vulnerability Management
Lumin	Tenable Lumin
コンテナのセキュリティ	Tenable Container Security
ウェブアプリケーションスキャン	Tenable Web App Scanning

注意: **[脆弱性管理の概要]** および **[資産ビュー]** ダッシュボードのランディングページや、ダッシュボードに含まれる個別のウィジェットはエクスポートが可能です。詳細は、「ダッシュボード全体をエクスポートする」および「個別のダッシュボードのウィジェットをエクスポートする」を参照してください。

注意: ダッシュボードにデータが表示されない場合は、ダッシュボードをフィルタリングしているターゲットグループのターゲットが多すぎる可能性があります。Tenable では、1 つのターゲットグループ内にあるターゲット数を制限することをお勧めします。

ダッシュボードのランディングページ全体をエクスポートする

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management で、次のダッシュボードランディングページをエクスポートすることができます。

- 脆弱性管理の概要
- 資産ビュー
- Tenable Lumin
- Tenable Web App Scanning

ダッシュボードのランディングページ全体をエクスポートする方法

1. エクスポートするダッシュボードページを表示します。
2. 右上にある **[エクスポート]** 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。
3. ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - **[PDF]** をクリックして、ダッシュボードを PDF 形式でエクスポートします。
   - **[PNG]** をクリックして、ダッシュボードを PNG 形式でエクスポートします。
   - **[JPG]** をクリックして、ダッシュボードを JPG 形式でエクスポートします。

   [進行中] メッセージが表示されます。

   エクスポートが完了したら、**[成功]** メッセージが表示され、Tenable Vulnerability Management によりお使いのコンピューターにエクスポートファイルがダウンロードされます。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

個別のダッシュボードのウィジェットをエクスポートする

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management で、次のダッシュボードランディングページから個別のウィジェットをエクスポートすることができます。

- 脆弱性管理の概要
- 資産ビュー
- Tenable Lumin
- Tenable Web App Scanning

個別のダッシュボードのウィジェットをエクスポートする方法

1. エクスポートするウィジェットを含むダッシュボードページを表示します。
2. エクスポートするウィジェットのヘッダーで、••• 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。
3. ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - **[PDF]** をクリックして、ダッシュボードを PDF 形式でエクスポートします。
   - **[PNG]** をクリックして、ダッシュボードを PNG 形式でエクスポートします。
   - **[JPG]** をクリックして、ダッシュボードを JPG 形式でエクスポートします。

   [進行中] メッセージが表示されます。

   エクスポートが完了したら、**[成功]** メッセージが表示され、Tenable Vulnerability Management によりお使いのコンピューターにエクスポートファイルがダウンロードされます。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

個別のダッシュボードを表示する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

スキャンが実行されるたびに、Tenable Vulnerability Management はダッシュボードデータを更新します。

個別のダッシュボードを表示する方法

1. **[ダッシュボード]** ページを表示します。
2. 次のいずれかを行います。
   - グリッド表示の場合、表示するダッシュボードのタイルにカーソルを合わせます。

     ダッシュボードの情報とオプションが、ダッシュボードタイルの上にオーバーレイ表示されます。
   - リスト表示の場合、表示するダッシュボードのサムネイル画像にカーソルを合わせます。

     ダッシュボードのオプションが、ダッシュボードのサムネイル画像の上にオーバーレイ表示されます。
3. **[表示]** をクリックします。

   そのダッシュボードのページが表示されます。
4. 次のいずれかを行います。
   - 表示しているダッシュボードを変更する方法

     a. 右上にある **[ダッシュボードへジャンプ]** 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。

     b. 表示したいダッシュボードを選択します。

     > **ヒント:** [調査] ダッシュボードのレガシーバージョンを表示するには、このオプションを使用します。詳細は、[調査] ダッシュボードを有効化を参照してください。
   - 個別のウィジェットにカーソルを合わせて、追加情報を表示します。
   - ウィジェット要素をクリックして、データの詳細を掘り下げます。
   - ダッシュボードを共有します。

- ダッシュボードをエクスポートします。
- ダッシュボードを編集します。
- ダッシュボードをデフォルトとして設定します。
- ダッシュボードを複製します。
- 新しいダッシュボードを作成します。
- ダッシュボードを削除します。

ダッシュボードテンプレートライブラリの表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable が提供する一連のダッシュボードを**テンプレートライブラリ**からご利用いただけます。

ヒント: Tenable Vulnerability Management のダッシュボードテンプレートの詳細は、Dashboards のブログ記事を参照してください。

ダッシュボードテンプレートライブラリを表示する方法

1. **[ダッシュボード]** ページを表示します。
2. ⊕ **[新しいダッシュボード]** をクリックします。

   オプションのリストが表示されます。
3. **[テンプレートライブラリ]** をクリックします。

   [テンプレートライブラリ] ページが表示されます。

   [テンプレートライブラリ] ページでは以下が可能です。

   - **[テンプレートライブラリ]** ページの並べ替え:
     a. ページの右上で、ドロップダウンボックスの ⌄ ボタンをクリックします。
     b. ページを並べ替える条件を選択します。
   - 左上にある **[検索]** バーを使用して、特定のダッシュボードを検索します。
   - **[新規および更新済み]** タブをクリックして、自動更新の対象となるダッシュボードを表示します。
   - グリッド表示とリスト表示を切り替えます。
   - ダッシュボードをプレビューします。
   - ダッシュボードを作成します。

ダッシュボードの作成

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

カスタムダッシュボードを作成するか、**テンプレートライブラリ**を使用して、利用可能なテンプレートからコピーを作成できます。ダッシュボードを使用すると、各ウィジェットの詳細を表示することができます。

重要: Tenable Vulnerability Management の**テンプレートライブラリ**には、**[探索する]** ダッシュボードテンプレートが含まれています。**[調査]** ダッシュボードテンプレートは、テンプレート名の末尾に**(調査)** が付いています。例: **脆弱性管理 (調査)**。これらのテンプレートを使用して作成したダッシュボードから、**[検出結果]** ページまたは **[資産]** ページにドリルダウンできます。**[調査]** ダッシュボードを追加するには、[調査] ダッシュボードを有効化 を参照してください。

ダッシュボードを作成する方法

1. **[ダッシュボード]** ページを表示します。
2. ⊕ **[新しいダッシュボード]** をクリックします。

   オプションのリストが表示されます。
3. 次のいずれかを行います。

テンプレートからダッシュボードを作成する方法

a. **[テンプレートライブラリ]** をクリックします。

   [テンプレートライブラリ] ページが表示されます。

b. ライブラリで、使用するテンプレートを見つけます。

c. テンプレートにカーソルを合わせます。

   テンプレート情報とオプションがオーバーレイ表示されます。

d. (オプション) ダッシュボードテンプレートをプレビュー表示するには、**[プレビュー]** をクリックします。詳細は、ダッシュボードをプレビュー表示する を参照してください。

e. ⊕ **[追加]** をクリックします。

   [ダッシュボードにダッシュボードを追加しました] という確認メッセージが表示されます。

新しいダッシュボードが、**[ダッシュボード]** ページに「***選択したダッシュボードのコピー***」という名で表示されます。

カスタムダッシュボードを作成する方法

a. **[カスタムダッシュボード]** をクリックします。

[ダッシュボードの編集] ページが表示されます。

b. ダッシュボードに名前を付けます。

a. ダッシュボードの名前をクリックします。

名前は編集可能なテキストボックスになります。

b. ダッシュボードの名前を入力します。

c. ✓ ボタンをクリックして名前の変更を確認します。

Tenable Vulnerability Management は更新された名前を保存します。

c. ダッシュボードの説明を追加するには

a. ダッシュボードの説明をクリックします。

説明は編集可能なテキストボックスになります。

b. ダッシュボードの説明を入力します。

d. ダッシュボードにウィジェットを追加します。

a. ページ右上にある ⊕ **[ウィジェットの追加]** をクリックします。

メニューが表示されます。

b. 次のいずれかを行います。

- テンプレートからウィジェットを追加するには、**[テンプレートウィジェット]** をクリックします。

[ウィジェット] ページが表示されます。

- ダッシュボードにウィジェットを追加するの説明に従って、ウィジェットを選択します。

- カスタムウィジェットを追加するには、**[カスタムウィジェット]**をクリックします。

  [ウィジェットの作成]ページが表示されます。

  - カスタムウィジェットを作成するの説明に従って、カスタムウィジェットを設定します。

e. ダッシュボードのフィルターを追加するには

a. ページ右上にある **[フィルターの編集]**をクリックします。

[フィルター]プレーンが表示されます。

> **注意:** ダッシュボードにウィジェットが追加されていない場合、**[フィルターの編集]**オプションは表示されません。

b. ダッシュボードにフィルターを適用するの説明に従って、ダッシュボードフィルターを設定します。

f. (オプション) ダッシュボードのウィジェットを並び替える場合

a. 移動させるウィジェットにカーソルを合わせます。

b. マウスボタンを押したままにして、ウィジェットをハイライトします。

ウィジェットの端がくっきりして、浮き上がって表示されます。

c. マウスを使用して、ウィジェットを新しい場所にドラッグします。

d. マウスボタンを放して、ウィジェットを新しい場所にドロップします。

g. (オプション) ダッシュボードを削除する場合

- ページの左下にある **[ダッシュボードを削除]**をクリックします。

Tenable Vulnerability Managementは、新しく作成されたダッシュボードを破棄します。

次の手順：

- ダッシュボードの管理

ダッシュボードをプレビュー表示する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

テンプレートから新しいダッシュボードを作成する際に、**[ダッシュボード]** ページに追加する前にダッシュボードをプレビュー表示することができます。

ダッシュボードをプレビュー表示する方法

1. ダッシュボードを作成します。
2. **[テンプレートライブラリ]** で、プレビュー表示するテンプレートにカーソルを合わせます。

   テンプレート情報とオプションがオーバーレイ表示されます。
3. **[プレビュー]** をクリックします。

   ダッシュボードがプレビュー表示されます。
4. プレビュー表示を終了するには、上部のナビゲーションバーでブレッドクラムのリンクをクリックして、**[テンプレートライブラリ]** または **[ダッシュボード]** ページに戻ります。
5. **[ダッシュボード]** ページにテンプレートを追加するには、⊕ **[ダッシュボードに追加]** をクリックします。

   [ダッシュボードにダッシュボードを追加しました] 確認メッセージが表示され、新しいダッシュボードが **[ダッシュボード]** ページに ***[選択したダッシュボードのコピー]*** の名前で表示されます。

[調査] ダッシュボードを有効化

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management 内で **[調査]** ダッシュボードを使用するには、最初に**テンプレートライブラリ**を介してインターフェースに追加する必要があります。

注意: [探索する] ダッシュボードに表示される数値データは、レガシー Tenable Web App Scanning または VM ダッシュボードのデータと一致しない場合があります。

注意: [探索する] Tenable Web App Scanning および [VM] ダッシュボードのデータは、完全なスキャン履歴を反映しています。これは、過去 30 日間のデータのみを表示する Tenable Web App Scanning および VM ダッシュボードとは異なります。

[調査] ダッシュボードを有効化する方法

1. **[ダッシュボード]** ページを表示します。
2. ⊕ **[新しいダッシュボード]** をクリックします。

   オプションのリストが表示されます。
3. **[テンプレートライブラリ]** をクリックします。

   [テンプレートライブラリ] ページが表示されます。
4. 左上の **[検索]** バーで、「(調査)」と入力します。

   利用可能なすべての **[調査]** ダッシュボードが表示されます。

   [調査] ダッシュボードが表示されない場合は、コンテナが有効化されていない可能性があります。Customer Success Manager に連絡してください。
5. インターフェースに追加する **[調査]** ダッシュボードごとに、以下を実行します。

   a. [調査] ダッシュボードテンプレートにカーソルを合わせます。

      テンプレート情報とオプションがオーバーレイ表示されます。

b. ⊕ **[追加]** をクリックします。

[ダッシュボードにダッシュボードを追加しました] 確認メッセージが表示され、**[調査]** ダッシュボードが **[ダッシュボード]** ページに表示されます。

注意: Tenable Web App Scanning または VM ダッシュボードを再度有効にするには、対応するワークベンチを有効にしてください。

ダッシュボードの管理

このセクションには、Tenable Vulnerability Management ダッシュボードの管理に役立つ関連する次のトピックが含まれます。

ダッシュボードグループ

Tenable Vulnerability Management では、ダッシュボードの **[グループ]** パネルを使用してダッシュボードをグループにまとめることができます。これにより、さまざまな種類のダッシュボードだけでなく、他のユーザーから共有されているダッシュボードも追跡できます。ダッシュボードグループを 1 人以上のユーザーまたはユーザーグループと共有することもできます。

[ダッシュボード] ページを表示させると、**[グループ]** パネルが自動的に展開されます。このパネルは、Tenable 提供のダッシュボードグループとユーザー作成のダッシュボードグループで区切られています。

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ダッシュボードグループを追加する

ダッシュボードグループは、**[ダッシュボード]** ページの **[グループ]** パネルから追加できます。

ダッシュボードグループを追加する方法

1. **[ダッシュボード]** ページを表示します。

   デフォルトでは、**[グループ]** パネルが展開されます。

2. **[グループ]** パネルで、⊕ **[追加]** をクリックします。

   [グループを編集] ペインが表示されます。

3. **[グループ名]** ボックスで、ダッシュボードグループの名前を入力します。

4. **[含めるダッシュボード]** セクションで、ダッシュボードグループに追加するダッシュボードの横にあるチェックボックスを選択します。

5. **[保存]** をクリックします。

   Tenable Vulnerability Management は、ダッシュボードグループを、**[グループ]** パネルのユーザー作成ダッシュボードリストに追加します。

ダッシュボードグループを共有する

Tenable Vulnerability Management では、**[グループ]** パネルを使用して、ユーザー作成のダッシュボードグループを他のユーザーまたはユーザーグループと共有できます。

注意: ダッシュボードグループが更新された場合、他のユーザーに自動的に再共有されません。例: ユーザー A はユーザー B とダッシュボードグループを共有しており、ユーザー A がそのダッシュボードグループに変更を加えた場合、更新内容を表示するには、ユーザー A がそのダッシュボードグループをユーザー B と再共有する必要があります。

注意: 共有コンテンツは、そのコンテンツが属しているアクセスグループに基づいて共有されるユーザーに対して異なって表示される場合があります。

ダッシュボードグループを共有する方法

1. **[ダッシュボード]** ページを表示します。

   デフォルトでは、**[グループ]** パネルが展開されます。

2. **[グループ]** パネルで、共有するユーザー作成のダッシュボードグループをクリックします。

   グループとそれに含まれるダッシュボードが表示されます。

3. **[グループを共有]** をクリックします。

   [グループを共有] ペインが表示されます。

4. 次のいずれかを行います。

   - ダッシュボードグループを全ユーザーと共有するには、**[すべてのユーザー]** チェックボックスをオンにします。
   - ダッシュボードグループを特定のユーザーまたはユーザーグループと共有するには、ドロップダウンボックスからダッシュボードグループを共有するユーザーまたはユーザーグループを選択します。

     ヒント: 複数のユーザーまたはユーザーグループと共有できます。

5. **[共有]** をクリックします。

[グループを共有しました] というメッセージが表示されます。Tenable Vulnerability Management は、指定されたユーザーまたはユーザーグループとダッシュボードグループを共有し、ダッシュボードが共有されたことを伝える E メールを送信します。

ダッシュボードグループを編集する

Tenable Vulnerability Management では、**[グループ]** パネルからユーザー作成のダッシュボードグループを編集できます。

ダッシュボードグループを編集する方法

1. **[ダッシュボード]** ページを表示します。

   デフォルトでは、**[グループ]** パネルが展開されます。

2. **[グループ]** パネルで、編集するユーザー作成のダッシュボードグループをクリックします。

   グループとそれに含まれるダッシュボードが表示されます。

3. **[グループを編集]** をクリックします。

   [グループを編集] ペインが表示されます。

4. (オプション) **[グループ名]** ボックスで、ダッシュボードグループの名前を編集します。

5. (オプション) **[含めるダッシュボード]** セクションで、ダッシュボードグループに表示されるダッシュボードを選択または選択解除します。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management によって変更内容がダッシュボードグループに保存されます。

ダッシュボードグループを削除する

Tenable Vulnerability Management では、**[グループ]** パネルからユーザー作成のダッシュボードグループを削除できます。

ダッシュボードグループを削除する方法

1. **[ダッシュボード]** ページを表示します。

   デフォルトでは、**[グループ]** パネルが展開されます。

2. **[グループ]** パネルで、削除するユーザー作成のダッシュボードグループをクリックします。

   グループとそれに含まれるダッシュボードが表示されます。

3. **[グループの削除]** をクリックします。

   確認のメッセージが表示されます。

4. **[削除]** をクリックします。

   Tenable Vulnerability Management がダッシュボードグループを削除します。

   注意: ダッシュボードグループを削除しても、グループ内のダッシュボードは削除されません。

ダッシュボード上のウィジェットの自動更新

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable は最新の脆弱性情報を提供するために、たとえば、新しい脆弱性の脅威が発見された場合、または Tenable Vulnerability Management が新しい脆弱性フィルターを追加した場合、ダッシュボードのウィジェットを更新したり追加したりします。Tenable がこれらのウィジェットを更新したら、次のいずれかの方法でウィジェットを表示して自動的に更新できます。

- **[ダッシュボード]** ページ - **[ダッシュボード]** ページでは、ダッシュボード上にあるすべての更新済みウィジェットを一度に更新できます。
- ダッシュボードの **[テンプレートライブラリ]** - **[テンプレートライブラリ]** でカスタムダッシュボードを作成する場合、新しいウィジェットまたは更新されたウィジェットを表示すると、それらをカスタムダッシュボードに追加できます。

  注意: 事前定義されたダッシュボードテンプレートの場合、Tenable Vulnerability Management は常に最新バージョンのウィジェットを表示します。

- **[ウィジェットライブラリ]** - **[ウィジェットライブラリ]** では、新規ウィジェットまたは更新済みウィジェットを表示して、最大 10 個のダッシュボードにそれらのウィジェットを追加できます。

[ダッシュボード] ページからウィジェットを自動更新する方法

1. **[ダッシュボード]** ページを表示します。
2. **[グループ]** セクションで、**[利用可能な更新]** タブをクリックします。

   ウィジェットが更新されたダッシュボードのリストが表示されます。

   注意: **[すべて]** タブで新規ウィジェットや更新されたウィジェットを含むダッシュボードを表示することもできます。これらのダッシュボードは、ダッシュボード名の横に青い点が点滅した状態で表示されます。

3. ウィジェットを更新するダッシュボードにカーソルを合わせます。

   オプションのオーバーレイが表示されます。

4. **[適用]** をクリックします。

   ダッシュボードのウィジェットの更新を説明する **[利用可能な更新]** メッセージが表示されます。

5. **[更新]**をクリックします。

   [更新が正常に適用されました]メッセージが表示され、Tenable Vulnerability Management がダッシュボードのウィジェットを更新します。

ダッシュボードの**[テンプレートライブラリ]**からウィジェットを自動更新する方法

1. ダッシュボードの**[テンプレートライブラリ]**を表示します。
2. **[新規および更新済み]**タブをクリックします。

   新規ウィジェットと更新済みウィジェットを含むダッシュボードテンプレートのリストが表示されます。
3. 追加するダッシュボードテンプレートにカーソルを合わせます。

   オプションのオーバーレイが表示されます。
4. **[追加]**をクリックします。

   [ダッシュボードテンプレートをダッシュボードに追加しました]メッセージが表示され、新規ウィジェットと更新済みウィジェットを含むダッシュボードテンプレートが**[ダッシュボード]**ページに表示されます。

[ウィジェットライブラリ]からウィジェットを自動更新する方法

1. **ウィジェットライブラリ**を表示します。
2. **[新規および更新済み]**タブをクリックします。

   新規ウィジェットと更新済みウィジェットのリストが表示されます。
3. ダッシュボードに追加するウィジェットにカーソルを合わせます。
4. **[ダッシュボードに追加]**をクリックします。

   [ダッシュボードに追加]プレーンが表示されます。
5. **[ダッシュボード]**ドロップダウンで、新規または更新済みウィジェットを追加するダッシュボード(複数選択可)を選択します。
6. **[保存]**をクリックします。

   選択したすべてのダッシュボードに正常に追加されましたメッセージが表示され、Tenable Vulnerability Management は新規または更新されたウィジェットを選択したダッシュボードに追加します。

ダッシュボードの編集

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ダッシュボードを編集する方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページから **[ダッシュボードを編集]** ページにアクセスします。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。

     c. **[編集]** をクリックします。

   - 個別のダッシュボードから **[ダッシュボードの編集]** ページにアクセスします。
     編集するダッシュボードを

     a. 表示します。

     b. ダッシュボードヘッダーで、**[さらに表示]** ⌄ ボタンをクリックします。

     > **注意:** **[さらに表示]** ボタンは、Tenable 提供のダッシュボードでは使用できません。

     ドロップダウンが表示されます。

     c. ✎ **[ダッシュボードの編集]** をクリックします。

   [ダッシュボードの編集] ページが表示されます。

2. **[ダッシュボードの編集]** ページで、次のいずれかの操作を行います。

- ダッシュボードの名前を変更する場合

  a. ダッシュボードの名前をクリックします。

     名前は編集可能なテキストボックスになります。

  b. 新しいダッシュボード名を入力します。

  c. ✓ ボタンをクリックして名前の変更を確認します。

     Tenable Vulnerability Management が名前を保存します。

- ダッシュボードの説明を編集する場合

  a. ダッシュボードの説明をクリックします。

     説明は編集可能なテキストボックスになります。

  b. ダッシュボードの新しい説明を入力します。

- ダッシュボードのフィルターを編集する場合

  a. ページ右上にある **[フィルターの編集]** をクリックします。

     [フィルター] プレーンが表示されます。

  b. ダッシュボードにフィルターを適用するの説明に従って、ダッシュボードフィルターを設定します。

- ダッシュボードにウィジェットを追加する場合

  a. ページ右上にある ⊕ **[ウィジェットの追加]** をクリックします。

     メニューが表示されます。

  b. 次のいずれかを行います。

     - テンプレートからウィジェットを追加するには、**[テンプレートウィジェット]** をクリックします。

       [ウィジェット] ページが表示されます。

- ダッシュボードにウィジェットを追加するの説明に従って、ウィジェットを選択します。

- カスタムウィジェットを追加するには、**[カスタムウィジェット]**をクリックします。

  [ウィジェットの作成]ページが表示されます。

  - カスタムウィジェットを作成するの説明に従って、カスタムウィジェットを設定します。

- ダッシュボードのウィジェットを並び替える場合

  a. 移動カーソルが表示されるまで、ウィジェットの上部にカーソルを合わせます。

  b. ウィジェットをクリックして移動したい場所までドラッグします。

- ダッシュボードのウィジェットをサイズ調整する場合

  a. サイズ調整カーソルが表示されるまで、ウィジェットの右下にカーソルを合わせます。

  b. ウィジェットをクリックして、希望するサイズになるまでドラッグします。

  新しいウィジェットのサイズが適用されます。

- ダッシュボードを削除する場合

  - ページの左下にある **[ダッシュボードを削除]**をクリックします。

    Tenable Vulnerability Managementは、**[ダッシュボード]**ページからダッシュボードを削除します。

3. **[編集を完了]**をクリックします。

選択したダッシュボードに戻ると、Tenable Vulnerability Management が変更を適用します。

デフォルトのダッシュボードの設定

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

任意のダッシュボードをデフォルトのダッシュボードとして設定して、ランディングページにすることができます。デフォルトのダッシュボードを設定しない場合、Tenable Vulnerability Management は Tenable が提供する **[脆弱性管理の概要]** ダッシュボードをデフォルトとして使用します。

ダッシュボードをデフォルトとして設定すると、**[ダッシュボード]** ページで、ダッシュボードタイルのヘッダーに **[デフォルト]** ラベルが表示されます。

注意: デフォルトとして設定されたダッシュボードを削除すると、製品の Tenable 提供ダッシュボードがデフォルトになります。

デフォルトのダッシュボードを設定する方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページでデフォルトのダッシュボードを設定します。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードタイルヘッダーで、⋮ ボタンをクリックします。

   - 個別のダッシュボードを介してデフォルトのダッシュボードを設定します。

     a. デフォルトにするダッシュボードを表示します。

     b. ダッシュボードヘッダーで、**[さらに表示]** ⌄ ボタンをクリックします。

   ドロップダウンリストが表示されます。

2. **[デフォルトにする]** を選択します。

   確認メッセージ「**デフォルトのダッシュボードとして正常に設定されました**」が表示され、Tenable Vulnerability Management によってダッシュボードがデフォルトとして設定されます。

   注意: 更新されたデフォルトのダッシュボードを表示するには、ログアウトして再びログインする必要があります。

ダッシュボード名の変更

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ダッシュボードの名前を変更する方法

1. 名前を変更するダッシュボードを表示します。
2. ダッシュボードページで、ダッシュボード名にカーソルを合わせます。

   名前が強調表示され、✎ ボタンが表示されます。
3. ✎ ボタンをクリックするか、名前をダブルクリックします。

   名前フィールドは、テキストボックスになります。
4. 新しいダッシュボード名を入力します。
5. ✓ ボタンをクリックして名前の変更を確認します。

   ページ上部に確認が表示されます。

   新しい名前が表示されます。

ダッシュボードの複製

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

ダッシュボードを複製する方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページを介してダッシュボードを複製します。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。

   - 個別のダッシュボードを介してダッシュボードを複製します。
     複製するダッシュボードを

     a. 表示します。

     b. ダッシュボードヘッダーで、**[さらに表示]** ⌄ ボタンをクリックします。

     ドロップダウンリストが表示されます。

2. **[複製]** をクリックします。

   [ダッシュボードが正常にコピーされました] 確認メッセージが表示され、Tenable Vulnerability Management によってダッシュボードが **[ダッシュボード]** ページ上でコピーされます。

ダッシュボードへのフィルターの適用

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ダッシュボード内のすべてのウィジェットにダッシュボードレベルでフィルターを適用できます。

注意: 個別のウィジェットに対して設定を適用できます。ウィジェットレベルの設定は、ダッシュボードレベルの設定よりも優先されます。

新しいインターフェースでダッシュボードをフィルタリングする方法

1. フィルタリングするダッシュボードを表示します。
2. ダッシュボードヘッダーで、**[さらに表示]** ボタンをクリックします。

   注意: [さらに表示] ボタンは、Tenable 提供のダッシュボードでは使用できません。

   ドロップダウンが表示されます。
3. **[フィルター]** をクリックします。

   [フィルター] プレーンが表示されます。
4. **[フィルタータイプを選択]** ドロップダウンで、ダッシュボードが分析する資産を選択します。次の表でオプションと要件を確認します。

オプション	説明	要件
すべての資産	(デフォルト) このオプションは、ダッシュボードのすべての資産を含めます。	これはデフォルトのオプションで、ダッシュボードのすべての資産を含めます。このオプションに要件はありません。
ターゲットグループ	このオプションは、特定のターゲットグループの資産のみを含めます。	このオプションを選択すると、**[ターゲットグループの選択]** 用の追加フィールドが表示されます。ドロップダウンリストから目的のターゲットグループを選択します。

カスタム	このオプションは、特定のホスト名、IP アドレス、FQDN、または CIDR を持つ資産のみを含めます。	このオプションを選択すると、テキストボックスが表示されます。1 つまたは複数のカスタムオプション形式 (ホスト名、IP アドレス、FQDN、または CIDR) を入力します。複数の項目はコンマで区切ります。 **重要**: 検索フィルターの IP アドレスの数は必ず 25 個以下にしてください。 **重要**: 検索フィルターのホスト名の数は必ず 300 個以下にしてください。

5. **[適用]** をクリックします。

   すべてのダッシュボードウィジェットのヘッダーに、▽ アイコンが表示されます。

6. ウィジェットセクションで、▽ アイコンにカーソルを合わせて追加したフィルターを表示します。

注意: 以下は、**[調査]** ウィジェットのフィルタリング制限です。

- **[調査]** ウィジェットは、**ターゲットグループ**をサポートしていません。
- **[クラウド設定ミス]** ウィジェットは、IP またはホスト名によるフィルタリングをサポートしていません。
- **[クラウド設定ミス]** と **[ウェブアプリケーションの検出結果]** ウィジェットは、タグをサポートしていません。

注意: フィルタリングできるのは、アクセスできるタグのみです。アクセスできないタグは適用できません。

時間に基づくフィルターをダッシュボードに適用する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

特定の時間枠(時間、日、月、年)の脆弱性のみを表示するようにダッシュボードをフィルタリングできます。フィルターは、カスタムダッシュボード、またはテンプレートライブラリを使用して作成されたダッシュボードでのみ使用できます。

注意:時間に基づくフィルターのオプションは、調査ダッシュボードおよび調査ウィジェットでのみ使用できます。

特定の時間枠でダッシュボードをフィルタリングする方法

1. フィルタリングするダッシュボードを表示します。
2. 特定の時間枠でダッシュボードデータをフィルタリングするには、次のいずれかを実行します。
   - **[すべて]**ドロップダウンボックスで、必要な時間枠を選択します(**[すべて]**、**[7 日前]**、**[14 日前]**、**[30 日前]**、**[60 日前]**、**[90 日前]**)。
   - カスタムの時間枠の場合は、**[最終確認日]**ボックスに、表示するデータの時間枠の値(直近の日数、時間数、年数、月数)を入力します。

   Tenable Vulnerability Management で、選択された時間枠の脆弱性がダッシュボードに表示されます。

ダッシュボードを共有する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management ユーザーは、1 人以上のユーザー、または 1 つ以上のユーザーグループとダッシュボードを共有できます。共有ダッシュボードは、共有されているユーザーまたはグループに対して自動的に表示されます。

注意: 共有されているダッシュボードは編集できません。ただし、共有されているダッシュボードの複製または削除は可能です。

注意: ダッシュボードが更新された場合、他のユーザーとは自動的に再共有されません。たとえば、ユーザー A はユーザー B とダッシュボードを共有しており、ユーザー A がそのダッシュボードに変更を加えた場合、更新内容を表示するには、ユーザー A がそのダッシュボードをユーザー B と再共有する必要があります。

注意: 共有コンテンツは、そのコンテンツが属しているアクセスグループに基づいて共有されるユーザーに対して異なって表示される場合があります。

ダッシュボードを共有する方法

1. 次のいずれかを行います。

    - **[ダッシュボード]** ページを介してダッシュボードを共有します。

        a. **[ダッシュボード]** ページを表示します。

        b. ダッシュボードタイルヘッダーで、⋮ ボタンをクリックします。

        ドロップダウンリストが表示されます。

        c. **[共有]** をクリックします。

    - 個別のダッシュボードを介してダッシュボードを共有します。

        a. 共有するダッシュボードを表示します。

        b. 右上の **[共有]** をクリックします。

    [共有] パネルが表示されます。

2. 次のいずれかを行います。

- 全ユーザーとダッシュボードを共有するには、**[すべてのユーザー]** チェックボックスを選択します。
- ダッシュボードを特定のユーザーまたはユーザーグループと共有するには、ドロップダウンボックスからダッシュボードを共有するユーザーまたはグループを選択します。

  ヒント: 複数のユーザーまたはユーザーグループと共有できます。

3. **[共有]** をクリックします。

   [ダッシュボードが正常に共有されました] というメッセージが表示されます。Tenable Vulnerability Management は、指定されたユーザーまたはユーザーグループとダッシュボードを共有し、ダッシュボードが共有されたことを伝える E メールを送信します。

ダッシュボードのエクスポートの管理

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

エクスポート機能を使用すると、ダッシュボードのデータを CSV、PDF、および詳細な PDF 形式でエクスポートできます。ダッシュボードのエクスポートをオンデマンドで作成できます。または、指定した受信者に対する自動エクスポートをスケジュール化することもできます。

さらに、ダッシュボードのエクスポートを管理できます。ダッシュボードエクスポートのダウンロード、エクスポート履歴の表示、エクスポートの削除、設定の削除を行うことができます。

注意: **[脆弱性管理の概要]** および **[資産ビュー]** ダッシュボードをエクスポートすることはできませんが、関連するランディングページや、ダッシュボードに含まれる個別のウィジェットはエクスポートできます。詳細は、ダッシュボードのランディングページ全体をエクスポートするおよび個別のダッシュボードのウィジェットをエクスポートするを参照してください。

ダッシュボードのエクスポート

ダッシュボードを CSV 形式でエクスポートする方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページを介してダッシュボードをエクスポートします。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。

     c. **[CSV にエクスポート]** をクリックします。

   - 個別のダッシュボードを表示した状態でダッシュボードをエクスポートします。
     エクスポートするダッシュボードを

     a. 表示します。

     b. 右上にある **[エクスポート]** をクリックします。

     ドロップダウンリストが表示されます。

     c. **[CSV]** をクリックします。

   [エクスポート中] 確認メッセージが表示されます。

   エクスポートのリクエストとステータスは、**[エクスポート]** プレーンの **[ダウンロード]** セクションに表示されます。

   エクスポートが完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

ダッシュボードを PDF 形式でエクスポートする方法

[PDF にエクスポート]機能を使用すると、カスタマイズされたダッシュボードを外部と共有できます。エクスポートされる PDFは、選択したダッシュボードから生成されたレポートです。

PDF をエクスポートする方法

1. 次のいずれかを行います。

- **[ダッシュボード]** ページを介してダッシュボードをエクスポートします。
  a. **[ダッシュボード]** ページを表示します。
  b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。
  c. **[PDF にエクスポート]** をクリックするか、利用可能な場合は **[PDF にエクスポート - 詳細]** をクリックします。

     注意: デフォルトでは、次のダッシュボードで **[PDF - 詳細]** エクスポートがサポートされています。

     - エグゼクティブサマリー
     - マルウェアにより悪用可能
     - 悪用可能なフレームワークの分析
     - 脆弱性管理の測定
     - 緩和状況サマリー
     - 未解決の修正のトラッキング
     - 資産の優先順位付け
     - 一般ポート別の脆弱性
     - Vulnerability Management
     - ウェブサービス

- 個別のダッシュボードを介してダッシュボードをエクスポートします。
  エクスポートするダッシュボードを

  a. 表示します。

  b. 右上にある [→] **[エクスポート]** をクリックします。

     ドロップダウンリストが表示されます。

  c. **[PDF]** をクリックするか、利用可能な場合は **[PDF - 詳細]** をクリックします。

> **注意:** PDF レポートには、選択したダッシュボードに表示される情報が含まれています。画面に表示されている情報が、レポートに含まれる情報です。
>
> **[PDF - 詳細]** レポートには、脆弱性の詳細など、表示される項目の範囲を超えた詳細情報が含まれます。

> **注意:** **[PDF - 詳細]** を選択し、ダッシュボードにある 1 つ以上のウィジェットにユーザーが作成したフィルターが適用されている場合、Tenable Vulnerability Management がユーザー作成のフィルターを追加のチャプターに適用していないことを示す **エクスポートの確認** メッセージが表示されます。**[確認]** をクリックして、エクスポートを続行します。

[エクスポート中] 確認メッセージが表示されます。

エクスポートのリクエストとステータスは、**[エクスポート]** プレーンの **[ダウンロード]** セクションに表示されます。

エクスポートが完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

ダッシュボードのエクスポートをスケジュールする方法

[エクスポートのスケジュール] オプションを使用すると、指定した時刻にダッシュボードをエクスポートできます。

エクスポートをスケジュールする方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページから **[定期エクスポート]** プレーンにアクセスします。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。

     c. **[エクスポートのスケジュール]** をクリックします。

   - 個別のダッシュボードから **[エクスポートのスケジュール]** 画面にアクセスします。
     エクスポートするダッシュボードを

     a. 表示します。

     b. 右上にある [→ **[エクスポート]** をクリックします。

     ドロップダウンリストが表示されます。

     c. ドロップダウンリストから、**[スケジュール]** をクリックします。

   [エクスポートのスケジュール] プレーンが表示されます。

2. 次のいずれかを行います。

   - ダッシュボードのエクスポートや、スケジュールを設定したことがない場合は、**[スケジュール]** オプションが自動的に表示されます。
   - ダッシュボードを既にエクスポートしている場合は、**[スケジュール]** セクションで ⊕ **[新しく追加]** をクリックします。

     [スケジュール] オプションが表示されます。

- ダッシュボードのエクスポートを既にスケジュールしている場合、別のエクスポートは作成できません。最初に、スケジュールしたダッシュボードエクスポートをキャンセルする必要があります。

3. **[CSV]** または **[PDF]** を選択するか、利用可能な場合は **[PDF - 詳細]** を選択します。

   注意: PDF レポートには、選択したダッシュボードに表示される情報が含まれています。画面に表示されている情報が、レポートに含まれる情報です。

   [PDF - 詳細] レポートには、脆弱性の詳細など、表示される項目の範囲を超えた詳細情報が含まれます。

   注意: [PDF - 詳細] を選択し、ダッシュボードにある 1 つ以上のウィジェットにユーザーが作成したフィルターが適用されている場合、Tenable Vulnerability Management がユーザー作成のフィルターを追加のチャプターに適用していないことを示す **エクスポートの確認** メッセージが表示されます。**[確認]** をクリックして、エクスポートを続行します。

4. **[スケジュール]** セクションで、次のパラメーターを設定します。

オプション	説明
名前	スケジュールしたエクスポートの名前
開始日時	エクスポートを開始する日時
繰り返し	Tenable Vulnerability Management にエクスポートを送信させる頻度: • **日単位** - エクスポートは、指定された時刻に毎日行われます。 • **週単位** - エクスポートは、毎週同じ曜日に指定された時刻で行われます (毎週火曜日など)。 • **月単位** - エクスポートは、月に 1 回、指定した曜日と時刻に行われます (毎月の最終火曜日など) • **カスタム** - エクスポートはカスタム間隔で行われます。**[カスタム]** を選択すると、さらにオプションが表示されます。 a. **[リピート間隔]** セクションのドロップダウンで、エクスポート

	を繰り返す頻度を選択します。たとえば、エクスポートを2日ごとに繰り返す場合は、最初のドロップダウンボックスで、**[2]** を選択し、2番目のドロップダウンボックスで **[日]** を選択します。 • **繰り返さない** – エクスポートは繰り返されません。
パスワード保護	エクスポートの暗号化の有無を指定します。 このオプションをオンにすると、**[暗号化パスワード]** ボックスが表示されます。エクスポートファイルの暗号化に使用するパスワードを入力します。 **注意:** 定期エクスポートを保存すると、**[暗号化パスワード]** の編集ができなくなります。編集したい場合は、ダッシュボードのコピーを作成し、定期エクスポートを作成した後に、希望するパスワードを選択する必要があります。
受信者を追加する	(オプション) レポートの受信者のメールアドレス。複数のメールアドレスをコンマ区切りのリストとして指定できます。

5. **[スケジュール]** をクリックします。

   [エクスポートのスケジュール] プレーンにスケジュールしたエクスポートが表示されます。

ダッシュボードのエクスポートをダウンロードする

ダッシュボードのエクスポートをダウンロードする方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページから **[定期エクスポート]** プレーンにアクセスします。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。

     c. **[エクスポート]** をクリックします。

   - 個別のダッシュボードから **[エクスポートのスケジュール]** 画面にアクセスします。

     a. ダウンロードするエクスポートがあるダウンロードを表示します。

     b. 右上にある **[エクスポート]** をクリックします。

     ドロップダウンリストが表示されます。

     c. ドロップダウンリストから、**[スケジュール]** をクリックします。

   [エクスポートのスケジュール] プレーンが表示されます。

2. **[ダウンロード]** セクションで、ダウンロードするエクスポートダウンロードの横にある ⭳ ボタンをクリックします。

   Tenable Vulnerability Management でエクスポートファイルがコンピューターにダウンロードされます。

ダッシュボードのエクスポート履歴の表示

ダッシュボードのエクスポート履歴を表示する方法

1. エクスポート履歴を表示するダッシュボードを表示します。
2. 右上にある [→ **[エクスポート]** をクリックします。

   ドロップダウンリストが表示されます。
3. ドロップダウンリストで、**[履歴]** をクリックします。

   [エクスポート履歴] プレーンが表示されます。
   [エクスポート履歴] プレーンでは、次の内容を確認できます。

   - ダッシュボードのエクスポートのスケジュール
   - 過去のダッシュボードエクスポートから利用可能なダウンロード

   > ダッシュボードがまだエクスポートされていない場合は、**[エクスポート履歴]** プレーンにアクセスできません。

ダッシュボードのエクスポートダウンロードを削除する

ダッシュボードのエクスポートダウンロードを削除する方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページから **[定期エクスポート]** プレーンにアクセスします。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。

     c. **[エクスポート]** をクリックします。

   - 個別のダッシュボードから **[エクスポートのスケジュール]** 画面にアクセスします。
     削除するダッシュボードを

     a. 表示します。

     b. 右上にある **[エクスポート]** をクリックします。

     ドロップダウンリストが表示されます。

     c. ドロップダウンリストから、**[スケジュール]** をクリックします。

   [エクスポートのスケジュール] プレーンが表示されます。

2. **[ダウンロード]** セクションで、削除するエクスポートダウンロードにカーソルを合わせます。
3. 🗑 ボタンをクリックします。

   削除の確認 メッセージが表示されます。

4. **[削除]** をクリックします。

[ダウンロードは正常に削除されました] メッセージが表示され、Tenable Vulnerability Management が **[エクスポートのスケジュール]** プレーンからエクスポートダウンロードを削除します。

ダッシュボードエクスポート設定の削除

ダッシュボードエクスポート設定を削除する方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページから **[定期エクスポート]** プレーンにアクセスします。

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードヘッダーで、⋮ ボタンをクリックします。

     ドロップダウンリストが表示されます。

     c. **[エクスポート]** をクリックします。

   - 個別のダッシュボードから **[エクスポートのスケジュール]** 画面にアクセスします。

     a. スケジュールしたエクスポートを削除するダッシュボードを表示します。

     b. 右上にある **[エクスポート]** をクリックします。

     ドロップダウンリストが表示されます。

     c. ドロップダウンリストから、**[スケジュール]** をクリックします。

   [エクスポートのスケジュール] プレーンが表示されます。

2. **[スケジュール]** セクションで、削除するスケジュールしたエクスポート設定にカーソルを合わせます。
3. 🗑 ボタンをクリックします。

   削除の確認 メッセージが表示されます。

4. **[確認]** をクリックします。

[**Successfully deleted export configuration**] というメッセージが表示され、Tenable Vulnerability Management は [**Schedule Export**] プレーンの [**Schedule**] セクションからエクスポート構成を削除します。

ダッシュボードを削除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: Tenable Vulnerability Management では、カスタムダッシュボードのみを削除できます。Tenable 提供のダッシュボードは削除できません。

ダッシュボードを削除する方法

1. 次のいずれかを行います。

   - **[ダッシュボード]** ページからダッシュボードを削除するには

     a. **[ダッシュボード]** ページを表示します。

     b. ダッシュボードタイルヘッダーで、⋮ ボタンをクリックします。

   - 個別のダッシュボードからダッシュボードを削除するには

     a. 削除するダッシュボードページを表示します。

     b. ダッシュボードヘッダーで、**[さらに表示]** ⌄ ボタンをクリックします。

   ドロップダウンリストが表示されます。

2. **[削除]** をクリックします。

   [削除の確認] の確認のメッセージが表示されます。

3. **[削除]** をクリックします。

   [ダッシュボードが正常に削除されました] 確認メッセージが表示され、Tenable Vulnerability Management によってダッシュボードが **[ダッシュボード]** ページから削除されます。

ウィジェットの管理

ウィジェットライブラリを使用すると、ダッシュボード全体で使用するウィジェットの作成と編集ができます。

ウィジェットライブラリでウィジェットを管理する方法

- ウィジェットライブラリの表示
- カスタムウィジェットを作成する
- カスタムウィジェットを編集する
- ダッシュボードにウィジェットを追加する

ダッシュボードでは、ウィジェットをさらに設定してダッシュボードを変更できます。

ダッシュボードでウィジェットを管理する方法

- ウィジェットの設定
- ウィジェットの複製
- ウィジェットの名前変更
- ダッシュボードからのウィジェットの削除

ウィジェットライブラリの表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ウィジェットライブラリから Tenable が提供する一連のウィジェットを入手し、テンプレートベースまたはカスタムのダッシュボードに追加できます。

注意: ウィジェットライブラリでは、Tenable が提供する **[脆弱性の傾向分析]** ウィジェットは使用できません。Tenable が提供する他のすべてのウィジェットは、ウィジェットライブラリに表示されます。

ウィジェットライブラリを表示する方法

1. **[ダッシュボード]** ページを表示します。
2. ページの右上にある **[ウィジェットライブラリ]** ボタンをクリックします。

   [ウィジェット] ページが表示されます。
3. (オプション) ページの右上で、表示するダッシュボードウィジェットのタブをクリックします。たとえば、Tenable Vulnerability Management に関連付けられたウィジェットのみを表示するには、**[脆弱性管理]** タブをクリックします。

   注意: **[ウィジェット]** ページに表示されるタブは、Tenable Vulnerability Management で有効にしたライセンス (たとえば、Tenable Lumin、Tenable Web App Scanning) によって異なります。

   [ウィジェット] ページでは、次の操作を実行できます。

   - **[ウィジェット]** ページを並べ替えます。
     a. ページの右上で、ドロップダウンボックスの ⌄ ボタンをクリックします。
     b. ウィジェットページを並べ替える条件を選択します。
   - 左上にある **[検索]** バーを使用して、特定のウィジェットを検索します。
   - **[新規および更新済み]** タブをクリックして、自動更新の対象となるダッシュボードウィジェットを表示します。
     ダッシュボードにウィジェットを
   - 追加します。

- ウィジェット ライブラリからウィジェットを削除します。

ウィジェットライブラリからウィジェットを削除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: 削除できるのはカスタムウィジェットのみです。事前設定されている Tenable Vulnerability Management ウィジェットは削除できません。

カスタムウィジェットを削除する方法

1. ウィジェットライブラリを表示します。
2. **[マイウィジェット]** タブをクリックします。

   ユーザーが作成したすべてのウィジェットが表示されます。
3. 削除するウィジェットのヘッダーで、⋮ 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. **[削除]** をクリックします。

   確認ウィンドウが表示されます。
5. **[削除]** をクリックします。

   Tenable Vulnerability Management はウィジェットプレーンからウィジェットを削除し、プレーンの上部に削除の確認メッセージが表示されます。

カスタムウィジェットを作成する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

カスタムウィジェットオプションを使用すると、一意に定義したウィジェットを作成し、それをユーザー定義のダッシュボードに追加できます。

カスタムウィジェットを作成する方法

1. 次のいずれかを行います。

   - ウィジェットライブラリからカスタムウィジェットを作成します。

     a. ウィジェットライブラリを表示します。

     b. ページの右上にある ⊕ **[カスタムウィジェット]** ボタンをクリックします。

     [カスタムウィジェットの作成] ページが表示されます。

   - ダッシュボードの編集中にカスタムウィジェットを作成します。

     a. ダッシュボードを編集します。

     b. ページ右上にある ⊕ **[ウィジェットの追加]** をクリックします。

     メニューが表示されます。

     c. **[カスタムウィジェット]** をクリックします。

   [カスタムウィジェットの作成] ページが表示されます。

2. ページ右上にある ⊕ **[ウィジェットの追加]** をクリックします。

   メニューが表示されます。

3. **[カスタムウィジェット]** をクリックします。

   [ウィジェット] ページが表示されます。

4. グラフセクションで、カスタムウィジェットのグラフタイプを選択します。

- 表
- リングチャート (**脆弱性**データセットのみ)
- 棒グラフ(**脆弱性**データセットのみ)

5. **[データセット]**ドロップダウンボックスで、Tenable Vulnerability Management でウィジェットの更新に使用される情報のタイプを選択します。
   - **脆弱性**
   - **資産**

     > **注意:** グラフセクションでリングチャートまたは棒グラフを選択した場合、**資産**データセットを選択すると、グラフの選択が表にリセットされます。

   グラフの種類、**データのグループ化**、および**表示フィード**のオプションは、ユーザーの選択内容に基づいて更新されます。
6. **[データのグループ化]**ドロップダウンボックスで、データをグループ化する方法を選択します。
   - **プラグインごと**(**脆弱性**データセットのみ)
   - **資産ごと**(**脆弱性**データセットのみ)
   - **CVE ごと**(**脆弱性**データセットのみ)
   - **資産リスト** (**資産**データセットのみ)
7. (オプション) フィルターを使用してウィジェットデータをフィルタリングする方法
   a. ⌄ ボタンをクリックして、フィルターオプションを展開します。
   b. ドロップダウンボックスで、カテゴリ、演算子、値のタイプを選択します。
   c. (オプション) その他のフィルターを指定するには、⊕ **[追加]**ボタンをクリックします。

> **注意:** 以前にタグを作成している場合は、カスタムウィジェットのフィルターのリストに表示されます。

> **注意:** 現在の資産クエリ制限である 5,000 を超えている場合、インターフェースにメッセージが表示されます。クエリをより小さい資産タグのセットに調整します。

> **注意:** Tenable Vulnerability Management 現在、エクスポートのタグフィルターはサポートされていません。

8. (オプション) 既存の保存済み検索を使用してウィジェットデータをフィルタリングするには、[**保存された検索条件**]ドロップダウンボックスで、ウィジェットデータのフィルタリングに使用する保存済みの検索を選択します。

   注意: 保存された検索条件がない場合、このオプションは表示されません。新しく検索条件を保存するには、Saved Search を参照してください。

9. **[名前]** ボックスにカスタムウィジェットの名前を入力します。

   [ウィジェットプレビュー] では、タイトルが自動的に更新されます。

10. (オプション) **[説明]** ボックスに、カスタムウィジェットの説明を入力します。

    [ウィジェットプレビュー] では、ⓘ アイコンが表示され、説明のホバーテキストが自動的に更新されます。

11. **[プレビューの更新]** をクリックして、ウィジェットプレビューを更新します。

    注意: **[名前]**、**[説明]**、およびグラフの種類はすべてウィジェットプレビューで自動的に更新されますが、**[プレビューの更新]** をクリックすると、その他すべての設定オプションが更新されます。

12. **[保存して終了]** をクリックします。

    Tenable Vulnerability Management はカスタムウィジェットをウィジェットライブラリに保存するので、ウィジェットをユーザー定義のダッシュボードに追加できます。

調査ダッシュボードのカスタムウィジェットの作成

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

カスタムウィジェットオプションを使用すると、一意に定義したウィジェットを作成し、それをユーザー定義の[調査]ダッシュボードに追加できます。脆弱性データと資産データを含むカスタムウィジェットを作成できます。脆弱性には、ホストの脆弱性、Tenable Web App Scanning 脆弱性、および Tenable Cloud Security の脆弱性が含まれます。これらのカスタムウィジェットの組み合わせをダッシュボードに追加すると、脆弱性環境の全体像を把握できます。

カスタムウィジェットから[検出結果]ページと[資産]ページにドリルダウンできます。

カスタムウィジェットを作成する方法

1. 次のいずれかを行います。

   - ウィジェットライブラリからカスタムウィジェットを作成します。

     a. ウィジェットライブラリを表示します。

     b. ページの右上にある ⊕ **[新しいカスタムウィジェット]** ボタンをクリックします。

     [カスタムウィジェットの作成] ページが表示されます。

   - ダッシュボードの編集中にカスタムウィジェットを作成します。

     a. ダッシュボードを編集します。

     b. ページ右上にある ⊕ **[ウィジェットの追加]** をクリックします。

     メニューが表示されます。

     c. **[カスタムウィジェット]** をクリックします。

   [カスタムウィジェットの作成] ページが表示されます。

2. **[チャートタイプ]** セクションで、カスタムウィジェットのチャートタイプを選択します。

- 脆弱性のチャートタイプ
    - **横棒**
    - **列**
    - **ドーナツ**
    - **マトリックス**
    - **複数系列の横棒**
    - **複数系列の縦棒**
    - **積み上げ横棒**
    - **積み上げ縦棒**
    - **テーブル**
- 資産のチャートタイプ
    - **縦棒**
    - **横棒**
    - **ドーナツ**
    - **表**

3. **[名前]** ボックスにカスタムウィジェットの名前を入力します。

   [ウィジェットプレビュー] では、タイトルが自動的に更新されます。

4. (オプション) **[説明]** ボックスに、カスタムウィジェットの説明を入力します。

   [ウィジェットプレビュー] では、ⓘ アイコンが表示され、文脈の説明が自動的に更新されます。

5. **[データセット]** ドロップダウンボックスで、Tenable Vulnerability Management でウィジェットの更新に使用される情報のタイプを選択します。
    - **検出結果**
    - **資産**

[チャートタイプ]、**[グループ化基準]**、**[ソートフィールド]** のオプションは、選択内容に基づいて更新されます。

選択内容	オプション
検出結果	次の詳細を指定します。 a. **[エンティティ]** ドロップダウンボックスで、作成するウィジェットの対象となる脆弱性タイプを選択します。次の中から選択できます。 • **脆弱性** – 検出結果のリストが含まれます。 • **ウェブアプリケーションの検出結果** - Tenable Web App Scanning が検出した脆弱性が含まれます。 • **クラウド設定ミス** - Tenable Cloud Security が検出した脆弱性が含まれます。 b. **[制限]** ドロップダウンボックスで、ウィジェットに表示するレコードの数を選択します。デフォルト値は 5 で、最大値は 20 です。 c. **[グループ化基準]** ドロップダウンボックスで、データをグループ化する方法を選択します。**[グループ化]** ドロップダウンの値は、選択した**エンティティ**に応じて変化します。 **注意**: **[横棒]**、**[縦棒]**、**[ドーナツ]**、**[テーブル]** チャートタイプでは、脆弱性をグループ化するオプションを 1 つのみ選択できます。**[マトリックス]**、**[マルチシリーズバー]**、**[複数系列の縦棒]**、**[積み重ね棒]**、**[積み上げ縦棒]** チャートタイプでは、脆弱性をグループ化するために 2 つのオプションを選択する必要があります。 すべてのフィルターの詳細については、検出結果フィルターを参照してください。 d. **[統計]** ドロップダウンボックスで、ウィジェットに表示する統計情報を選択します。 **[テーブル]** を除くすべてのチャートタイプで、[カウント] はデフォルトの統計オプションです。**[テーブル]** チャートタイプでは、複数のオプションから選択できま

	す。 e. **[並び替えフィールド]**ドロップダウンボックスで、ウィジェットでデータを並べ替える方法を選択します。次のいずれかのオプションで並べ替えることができます。 • **カウント** • **[グループ化]**の値 f. **[ソート順序]**ドロップダウンボックスで、並び替えを昇順または降順のどちらにするかを選択します。
資産	次の詳細を指定します。 a. **[制限]**ドロップダウンボックスで、ウィジェットに表示するレコードの数を選択します。デフォルト値は 5 で、最大値は 20 です。 b. **[グループ化]**ドロップダウンボックスで、データをグループ化する方法を選択します。 • **システムタイプ** • **名前** • **オペレーティングシステム** • **SSH フィンガープリント** • **完全修飾ドメイン** • **Mac アドレス** • **資産タイプ** **注意**: **[横棒]**、**[縦棒]**、**[ドーナツ]**、および **[テーブル]** チャートタイプでは、資産をグループ化するオプションを 1 つのみ選択できます。**[マトリックス]**、**[複数系列の横棒]**、**[複数系列の縦棒]**、**[積み上げ横棒]**、**[積み上げ縦棒]** チャートタイプでは、資産をグループ化するために 2 つのオプションを選択する必要があります。 c. **[統計]**ドロップダウンボックスで、ウィジェットに表示する統計情報を選択します。

	[テーブル] を除くすべてのチャートタイプで、[カウント] はデフォルトの統計オプションです。**[テーブル]** チャートタイプでは、複数のオプションから選択できます。

6. 使用するフィルターごとに、次の操作を行います。

   注意: Tenable では、カスタムウィジェットを作成する際に、複雑なクエリではなく単純なクエリ、または 1 レベルのネスト化フィルターを使用することを推奨しています。ウィジェットがダッシュボードに追加されるときに追加のコンテキストフィルターが適用されない場合、ウィジェットは最大 1 レベルのネスト化フィルターのみを持つことができます。ネストレベルが 1 のクエリの例:
   (CVSSv3 基本値が 8.9 を超えている、または VPR が 8.9 を超えている) かつ、状態が修正済みと等しくない

   a. **[フィルターの選択]** をクリックします。

      [フィルターの選択] ドロップダウンボックスが表示されます。

   b. 適用するフィルターをクリックします。

      フィルターがボックスに表示されます。

   c. フィルターで、v ボタンをクリックします。

      フィルター値と演算子オプションのリストが表示されます。

   d. 1 つ目のドロップダウンボックスで、フィルターに適用する演算子を選択します。

   e. 2 つ目のドロップダウンボックスで、フィルターに適用する値を 1 つ以上選択します。

   f. ドロップダウンボックスで **[すべてに一致]** を選択します。デフォルトでは、Tenable Vulnerability Management はフィルターを **[すべてに一致]** に設定します。

7. **[プレビューの更新]** をクリックして、ウィジェットプレビューを更新します。

   注意: [名前]、**[説明]**、およびグラフの種類はすべてウィジェットプレビューで自動的に更新されますが、**[プレビューの更新]** をクリックすると、その他すべての設定オプションが更新されます。

8. **[保存して終了]** をクリックします。

   Tenable Vulnerability Management はカスタムウィジェットをウィジェットライブラリに保存するので、ウィジェットをユーザー定義のダッシュボードに追加できます。

カスタムウィジェットを編集する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: Tenable が提供するウィジェットは編集できません。

カスタムウィジェットを編集する方法

1. ウィジェットライブラリを表示します。
2. **[マイウィジェット]** タブをクリックします。

   ユーザーが作成したすべてのウィジェットが表示されます。
3. 編集するウィジェットの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。
4. **[編集]** をクリックします。

   ウィジェットオプションが表示されます。
5. ウィジェットオプションを編集します。
6. **[保存して終了]** をクリックします。

   確認が表示されます。

注意: ウィジェットを編集する前からダッシュボードに含まれていたカスタムウィジェットは、編集を反映するように更新されません。編集したウィジェットを含めるには、ダッシュボードにウィジェットを追加するの説明に従って、ウィジェットを再度ダッシュボードに追加する必要があります。

ダッシュボードにウィジェットを追加する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

次の手順に従い、テンプレートベースのダッシュボードやカスタムダッシュボードにウィジェットを追加します。

カスタムウィジェット、Tenable 提供のダッシュボードからのウィジェット、その他の汎用ウィジェット (Tenable 提供のウィジェット) を追加できます。

ウィジェットをダッシュボードに追加する方法

注意: この手順では、ダッシュボードにテンプレートウィジェットを追加する方法を説明しています。カスタムウィジェットを作成してダッシュボードに追加する方法については、「カスタムウィジェット」を参照してください。

1. ウィジェットライブラリを表示します。
2. 追加したい各ウィジェットについて
   a. 次のいずれかを行います。
      - ウィジェットのリストをスクロールします。
      - **[検索]** ボックスを使用して、特定のウィジェットを見つけます。

      ヒント: ウィジェットタイルの上にカーソルを置くと、各ウィジェットの簡単な説明を見ることができます。Tenable 提供のダッシュボードから作成されたウィジェットの詳細については、Tenable 提供のダッシュボードを参照してください。

   b. 追加するウィジェットにカーソルを合わせます。

      ⊕ **[ダッシュボードに追加]** ボタンが表示されます。

   c. ⊕ **[ダッシュボードに追加]** をクリックします。

      [ダッシュボードに追加] プレーンが表示されます。

   d. **[ダッシュボード]** のドロップダウンボックスで、ウィジェットを追加したいダッシュボード (複数選択可) を選択します。

   e. **[保存]** をクリックします。

Tenable Vulnerability Management で適切なダッシュボード (複数選択可) の下部にウィジェットが追加されます。

f. ⊕ **[追加]** をクリックします。

Tenable Vulnerability Management が適切なダッシュボードの下部にウィジェットを追加します。

3. **[完了]** をクリックします。

[ダッシュボード] ページに戻ります。

ウィジェットの設定

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ウィジェットを設定する方法

1. 設定するウィジェットを含むダッシュボードページを表示します。
2. 変更するウィジェットの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。
3. **[設定]** をクリックします。

   ウィジェットの概要プレーンが表示されます。
4. ウィジェットのサマリープレーンで、次のいずれかを行います。

   - ウィジェットの名前を変更する場合

     a. 次のいずれかを行います。

     - ウィジェットの名前をクリックします。
     - ウィジェットのサマリープレーンでウィジェット名にカーソルを合わせて、✎ ボタンをクリックします。

     名前フィールドは、編集可能なテキストボックスになります。

     b. 新しいウィジェット名を入力します。

     c. ✓ ボタンをクリックして名前の変更を確認します。

     ページ上部に確認メッセージが表示され、ウィジェットのヘッダーに新しい名前が表示されます。

   - ウィジェットの説明を編集する場合

a. 次のいずれかを行います。

- ウィジェットの説明をクリックします。
- ウィジェットのサマリープレーンでウィジェットの説明にカーソルを合わせて、✎ ボタンをクリックします。

説明フィールドは、編集可能なテキストボックスになります。

b. 新しいウィジェットの説明を入力します。

c. ✓ ボタンをクリックして変更を確認します。

ページ上部に確認メッセージが表示され、ウィジェットのヘッダーに新しい説明が表示されます。

- ウィジェットを複製する場合
  - **[アクション]** 行で、⧉ ボタンをクリックします。

    確認メッセージが表示され、Tenable Vulnerability Management は複製したウィジェットをダッシュボードに追加します。

- ダッシュボードからウィジェットを削除する場合

a. **[アクション]** 行で、🗑 ボタンをクリックします。

削除の確認メッセージが表示されます。

b. **[削除]** をクリックします。

確認メッセージが表示され、Tenable Vulnerability Management は **[ダッシュボード]** ページからダッシュボードを削除します。

- ウィジェットにフィルターを適用する場合

オプション	説明	要件
すべての資	(デフォルト) このオプションは、	これはデフォルトのオプションで、ダッ

産	ダッシュボードのすべての資産を含めます。	シュボードのすべての資産を含めます。このオプションに要件はありません。
カスタム	このオプションは、特定のホスト名、IP アドレス、FQDN、または CIDR を持つ資産のみを含めます。	このオプションを選択すると、テキストボックスが表示されます。1 つまたは複数のカスタムオプション形式 (ホスト名、IP アドレス、FQDN、または CIDR) を入力します。複数の項目はコンマで区切る必要があります。
タグ	このオプションでは、タグを使用して資産の結果または脆弱性の結果をフィルター処理します。 **注意:** ACR ウィジェットは Tenable Lumin データを使用するため、このウィジェットはタグによるフィルタリングはサポートしていません。	このオプションを選択すると、ドロップダウンボックスが表示されます。結果のフィルター処理をするタグ名を選択または入力します。Tenable Vulnerability Management は、選択したタグで結果をフィルター処理します。 **注意:** Tenable Vulnerability Management は最大 100 個のフィルターをサポートしています。

注意: ウィジェットにフィルターを適用すると、ウィジェットのヘッダーに ▽ アイコンが表示されます。適用されたフィルターを表示するには、▽ アイコンにカーソルを合わせます。

5. **[適用]** をクリックします。

   確認メッセージが表示され、Tenable Vulnerability Management はウィジェットに変更を適用します。

ウィジェットの複製

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ウィジェットを複製する方法

1. 複製するウィジェットを含むダッシュボードページを表示します。
2. 複製するウィジェットの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。
3. **[複製]** をクリックします。

   複製されたウィジェットがページ下部に表示されます。
4. (オプション) ウィジェットの名前を変更します。
5. (オプション) ウィジェットのセクションを並べ替える。

ウィジェットの名前変更

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ウィジェットの名前を変更する方法

1. 変更するウィジェットを含むダッシュボードページを表示します。
2. 名前を変更するウィジェットの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。
3. **[設定]** をクリックします。

   ウィジェットの概要プレーンが表示されます。
4. ウィジェットサマリープレーンで、ウィジェット名にカーソルを合わせます。

   ✎ ボタンが名前の横に表示されます。
5. ✎ ボタンをクリックするか、名前をダブルクリックします。

   名前フィールドは、編集可能なテキストボックスになります。
6. 新しいウィジェット名を入力します。
7. ✓ ボタンをクリックして名前の変更を確認します。

   ページ上部に確認メッセージが表示されます。

   新しい名前がウィジェットヘッダーに表示されます。

ダッシュボードからのウィジェットの削除

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

ダッシュボードからウィジェットを削除する方法

1. 削除するウィジェットを含むダッシュボードページを表示します。
2. 削除するウィジェットの右上にある ⋮ ボタンをクリックします。

   メニューが表示されます。
3. 🗑 **[削除]** をクリックします。

   🗑により削除の確認を促すメッセージが表示されます。
4. **[削除]** をクリックします。

   ページ上部に確認メッセージが表示されます。

   Tenable Vulnerability Management はダッシュボードからウィジェットを削除します。その他のウィジェットは新規スペースを埋めるよう再配置されます。

Tenable Lumin にようこそ

Tenable Lumin を使用すると、リスクを素早く正確に評価でき、企業の正常性や修正状況を Salesforce 業界および全体の他の Tenable ユーザーと比較できます。Tenable Lumin は、未加工の脆弱性データを資産のビジネス上の重要度や脅威の文脈データと関連付けることで、従来の脆弱性管理ツールよりも高速かつターゲットを絞った分析ワークフローをサポートします。

Tenable が提供するメトリクスはリスクを定量化し、情報に基づく修正と戦略的なセキュリティ判断を行う手助けとなります。Tenable Lumin の分析で使用されるメトリクスについての詳細は、Tenable Lumin のメトリクスを参照してください。

Tenable Lumin の準備、インストール、設定の方法については、Tenable Lumin を使い始めるを参照してください。

重要!Tenable One のユーザーは、[ワークスペース] ページから直接 Tenable Lumin にアクセスできます。

Tenable Lumin のメトリクス

TenableTenable Lumin では、リスクの評価に役立つ複数のメトリクスを使用します。

- Cyber Exposure Score (CES)
- Vulnerability Priority Rating (VPR)
- ACR (資産重大度の格付け) (ACR)
- 資産のエクスポージャースコア (AES)
- 評価成熟度グレード
- 修正成熟度 グレード

Tenable Lumin のメトリクスの精度を改善して脆弱性管理全体の健全性を向上させる方法に関する詳細は、Tenable Lumin メトリクスを改善する を参照してください。

重要: 非公開の検出結果は、Tenable Lumin 内のすべてのスコアから除外されます。詳細は、検出結果 を参照してください。

Cyber Exposure Score (CES)

Tenable は、直近の 90 日間にスキャンされた資産の AES (資産のエクスポージャースコア) に基づいて、リスクを 0 から 1000 の整数として表す、動的な CES を計算します。CES 値が高いほど、リスクは高くなります。

次のような異なる資産のグループに対しての CESを表示できます。

- 企業全体の総合的な CES (**[Cyber Exposure Score]** ウィジェットに表示される CES など)
- 特定の事業の文脈の資産のタグレベルの CES (**[事業の文脈タグによる Cyber Exposure Score]** ウィジェットで表示される CES など)。

CES カテゴリ	CES 範囲
高	650 ~ 1000
中	350 ~ 649
低	0 ~ 349

企業全体の、または資産グループのCESを表示するには、「Tenable Luminダッシュボードを表示する」でウィジェットを表示します。

Tenable Vulnerability ManagementがCESを計算または再計算するのにかかる時間の詳細は、「Tenable Lumin のデータのタイミング」を参照してください。

Vulnerability Priority Rating (VPR)

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
緊急	9.0 ~ 10.0
高	7.0 ~ 8.9
中	4.0 ~ 6.9
低	0.1 ~ 3.9

注意: National Vulnerability Database (NVD) にある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。

Tenable Vulnerability Management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。その後 Tenable Vulnerability Managementは、毎日自動的に新規または更新されたVPR値を提供します。

Tenableでは、ACR値が最大の資産上にある、VPRが最大の脆弱性を優先するよう推奨します。

特定の脆弱性のVPRを表示するには、「View Vulnerabilities by Plugin」の説明に従って脆弱性を表示します。

VPR主な要因

Tenableは脆弱性のVPRの計算に、次の主な要因を使用します。

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 Vulnerability Management 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**、**動作可能**、**PoC**、または **未実証**) は CVSS エクスプロイトコード成熟度と同等です。
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 (**低**、**中**、**高**、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**、**低**、**中**、**高**、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

ACR(資産重大度の格付け)(ACR)

Tenable は、ACR をネットワーク上の各資産に割り当て、資産の相対重要度を 1 ~ 10 の整数として表します。ACR が高いほど重要度も高くなります。

ACR カテゴリ	ACR 範囲
緊急	9 ~ 10
高	7 ~ 8
中	4 ~ 6
低	1 ~ 3

Tenable Vulnerability Management は 24 時間ごとに ACR 値を計算するため、ネットワーク上の資産をスキャンした後に ACR を表示するには最大 24 時間待つ必要があります。

注意: Tenable では必要に応じて、Tenable が提供する ACR 値を確認して上書きすることを推奨しています。ACR を編集するまたはの説明のように、ACR 値をカスタマイズして、企業固有のインフラやニーズを反映させることができます。

資産が複数の ACR 値を持つ場合、Tenable Vulnerability Management は次の順番で値に優先順位を付けます。

1. 設定されている場合は、手動でオーバーライドされた ACR 値。
2. Tenable が提供する ACR 値。

特定の資産の ACRを確認するには、「View Asset Details」の説明に従って資産の詳細を表示します。

ACR 主な要因

Tenable は次の主な要因を使用して、資産の Tenable標準提供の ACR を計算します。

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。ACR の主な要因は、資産の特性に関連するグローバルな脅威の状況を反映したものです。

注意: 非認証スキャンを実行すると、ACR の主な要因が限定的あるいは不完全になる可能性があります。

主な要因のタイプ

主な要因	説明
device_type	デバイスのタイプ例 • **hypervisor** - デバイスは、仮想マシンをホストするタイプ1のハイパーバイザーです。(Microsoft Hyper-V、VMware ESX/ESXi、Xen など) • **printer** - デバイスは、ネットワークに接続されたプリンターまたは印刷サーバーです。
device_capability	デバイスのビジネス目的例 • **file_server** - デバイスは、ファイル共有サービスを提供するサーバーです。(FTP、SMB、NFS、NAS サーバーなど) • **mail_server** - デバイスは、メールの送受信用に指定されたサーバーです。
internet_exposure	デバイスのネットワーク上の場所とインターネットとの近接度例 • **internal** - デバイスは、ローカルエリアネットワーク(LAN) 内にあり、おそらくはファイヤーウォールの背後にあります。 • **external** - デバイスは、LAN 外にあり、ファイヤーウォールの背後にありません。

ACR デバイス機能

ACR デバイス機能の一部は、ターゲットホストにインストールされているソフトウェアによって決まります。

機能	説明	ソフトウェアまたはサービス
accounting_system	会計ソリューションがターゲット資産にインストールされています。	Intuit Quickbooks

backup_agent	バックアップソリューションエージェントがターゲット資産にインストールされています。	Amanda バックアップ (エージェント)
analytics_system	データ分析とレポート作成のためのソフトウェアソリューションがターゲットホストにインストールされています。	QlikView
		TIBCO Spotfire
		IBM SPSS
		SharePoint 2013
		SOLR
		Elasticsearch
		Enterprise Search
		Google Search Appliance
		Lucene
		SQL Server Reporting Services
		Oracle BI Publisher
		SAP Business Object

backup_server	エンタープライズバックアップソリューションがターゲットホストにインストールされているか、実行されています。	Acronis Backup
		Quest NetVault
		Unitrends Enterprise Backup
		Veritas Backup Exec
		Spectrum Protect (旧 Tivoli Storage Manager)
crm_system	顧客関係管理 (CRM) ソリューションが、ターゲットホストにインストールされているか、実行されています。	SugarCRM
		Bitrix24 CRM
		Siebel CRM

database_server	ターゲット ホストにデータベースシステムがインストールされているか、ターゲット ホストでデータベースサーバーが実行されています。	PostgreSQL
		Microsoft SQL Server
		MongoDB
		Oracle Database
		Db2 Hosted
		Percona XtraDB Cluster
		IBM Informix
		PostgreSQL
		Percona Server
		MariaDB Cluster
		MySQL
		Microsoft SQL Server
		SAP Adaptive Server Enterprise (ASE)
		MariaDB Server
		SQLite
		Apache Derby Network Server
		SAP DB
		Cogent Datahub Server

directory_server	ターゲット資産は認証サーバーです。	McAfee Stonegate Authentication Server
		Kerberos Ticketing Server
		LDAP プロトコル
		IBM Tivoli
		Stonegate Auth Server
dns_server	DNS サーバーがターゲット資産で実行されています。	ポート 53 の DNS サービス
erp_system	Enterprise Resource Planning Suite サーバーがターゲット資産で実行されているかインストールされています。	Microsoft Dynamics AX
		Oracle E-Business Suite
		SAP ERP
		Microsoft Dynamics GP
		SAP DB
		SAPControl
		SAP RMI-P4 プロトコルサービス
		SAP Host Control
		Apache OFBiz
erp_system_client	ERP システムにアクセスするためのクライアントソフトウェアが、ターゲット資産にインストールされています。	SAP GUI

file_server	ターゲット資産は、ファイル共有の目的で使用されています。ここでのファイル共有は狭義です。SMB サーバーは、この分類ではファイルサーバーとは見なされません。	WebCenter
		ownCloud
		Sharepoint
		Oracle WebCenter Content
		Sharepoint
		FTP サービス
		Apple File Protocol (AFP) サービス
		Network File System (NFS) Server Detection
helpdesk_system	ヘルプデスクチケットサーバーが、ターゲットの資産にインストールされているか実行されています。	SugarCRM
		Track-It!
		ServiceDesk Plus
		OTRS
		ManageEngine Service Desk
it_management_system	ターゲット資産は、ある種の IT 管理機能を実行しています。IT インフラ管理 (単一またはグループのデバイスやサービスの管理など)、または IT サービス管理 (ソフトウェアプロビジョニング、デバイス、ソフトウェアリポジトリ管理など) である可能性があります。	Application Insight
		Solarwinds Server & Application Monitor
		ManageEngine Application

		Performance Monitoring
		System Center Operations Manager
		Applications Manager - ManageEngine
		ManageEngine Desktop Central
		Ghost Solution Suite
		ZENworks - Configuration Management
		IBM BigFix
		System Center Configuration Manager
		CA Unified Infrastructure Management
		Centreon
		VMware vRealize Operations
		OpManager
		Nagios XI

		SCOM

		PRTG Network Monitor
		Zabbix
		SolarWinds Storage Resource Monitor
		GroundWork Monitor
		Pandora FMS
		Tivoli Monitoring
		OP5 Monitor
		NetFlow Traffic Analyzer
		PRTG Network Monitor
		Cisco Prime Infrastructure
		H3C Intelligent Management Center
		ZENworks Asset Management
		ManageEngine Desktop Central
		Unified Endpoint Manager

		Google Analytics
		Cisco Prime Infrastructure
		H3C Intelligent Management Center
		HP 3PAR Management Server
		Ghost Solution Suite
		Fortigate Firewall Management Console
		Barracuda Spam & Virus Firewall Management Web Console
mail_server	ターゲット資産はメールサーバーです。	IBM Domino
		IMAP Service Detection
		CCProxy SMTP Server Detection
		SMTP Service Detection
		POP Service Detection

PCI	ターゲット資産には PCI の機密情報があります。	PCI Plugin Fired
pci-target	ターゲット資産は PCI スキャンのターゲットです。	スキャン名に「pci」キーワードが見つかりました
proxy_server	ターゲット資産はプロキシサーバーです。	Oracle iPlanet Web Proxy Server
		HTTP proxy Detected in Service Banner
		McAfee Email Gateway
reverse_proxy_server	ターゲット資産は、外部クライアントのリクエストを内部サーバーに転送するリバースプロキシです。リバースプロキシは、ADC またはロードバランサーである可能性があります。	NetApp SANtricity Web Services Proxy
		Foreman Smart-Proxy TFTP
rnd_software	ターゲット資産には製品開発ソフトウェアがインストールされているため、開発目的です。	Red Hat Mobile Application Platform
		Application Testing Suite
		Windows Visual Studio
		AutoCAD
		MAC OS Xcode IDE
		Autodesk DWG TrueView Detection

SCADA	ターゲット資産に、産業プロセスの管理に使用されるソフトウェアシステムがインストールされているか実行されています。	AVEVA InduSoft Web Studio / InTouch Edge HMI TCP/IP Server
		Trihedral VTScada Detection
upnp	ターゲット資産は UPnP をサポートしています。アプライアンスである可能性が高いです。	UPnP service detection

web_application_server	ターゲット資産で実行中またはインストールされているウェブアプリケーションサーバーがあります。ターゲット資産でウェブアプリケーションサーバーが実行されていても、必ずしもその重大度を示唆するわけではありません。ただし、一部のプロパティと併用されている場合、重大度を示唆している可能性があります(例:ウェブアプリケーションサーバー + 外部 + サーバーデバイスタイプ = 重大度高)。	Geronimo
		Resin
		Tuxedo
		Tomcat
		Jetty
		Red Hat OpenShift
		Microsoft .NET Platform
		Red Hat Jboss EAP
		WebLogic Server
		Magento
		WebSphere Commerce
		Cobalt
		DNN Platform
		Umbraco
		Oracle WebCenter Sites
		Glassfish
		nginx
		Microsoft IIS

資産のエクスポージャースコア(AES)

Tenable は、ネットワーク上の各資産について、資産の相対的暴露を表す動的な AESを 0 ~ 1000 の整数として計算します。AES が高くなるほど、高いサイバーエクスポージャーを示しています。

Tenable は、現在の ACR(Tenable が提供する、またはカスタム) と、資産に関連付けられている VPR に基づいて AES を計算します。

AES カテゴリ	AES 範囲
高	650 ~ 1000
中	350 ~ 649
低	0 ~ 349

特定の資産の AES を表示するには、「View Assets」を参照してください。

評価成熟度グレード

重要: Tenable Lumin 内のデータ移行およびアルゴリズムの変更により、最近評価成熟度および修正成熟度のスコアが変更された可能性があります。これは想定された動作です。詳細については、Tenable の担当者までお問い合わせください。

評価成熟度 は、ライセンスのある資産の脆弱性をどれだけ効果的にスキャンしているかについて大まかなまとめを提供します。Tenable では、評価スキャンの健全性を **A** から **F** までの文字グレードで表す、動的な 評価成熟度 グレードを計算します。**A** グレードは、資産を高い頻度で徹底的に評価していることを示します。

Tenable は、初めてスキャンしたときに評価成熟度グレードを提示します。その後、Tenable Vulnerability Management は毎日自動的に更新された評価成熟度グレードを提供します。

評価成熟度文字グレード	数値の範囲
A	75 ~ 100
B	55 ~ 74
C	30 ~ 54
D	15 ~ 29
F	0 ~ 14

評価成熟度の計算方法

- 資産スコアの場合
  - **スキャン頻度**スコア - 過去 90 日間に資産がスキャンされた頻度
  - **スキャンの深度**スコア - 資産が過去 90 日間に認証スキャンされたかどうか
  - **評価成熟度**スコア - (スキャン頻度スコア + スキャンの深度スコア)/2 の計算
- コンテナ/事業の文脈スコアの場合
  - **スキャン頻度**スコア - 資産のスキャン頻度スコアの平均
  - **スキャンの深度**スコア - 資産のスキャン深度スコアの平均
  - **評価成熟度**スコア - 資産の評価成熟度スコアの平均

スキャンの深度スコア

深度が高いグレードは、これらの資産で認証スキャンを実行していることを示します。

深度グレードの文字グレード	数値の範囲
A	75 ~ 100
B	55 ~ 74
C	30 ~ 54
D	15 ~ 29
F	0 ~ 14

スキャン頻度スコア

Tenable は、どのくらい頻繁にネットワーク上の資産をスキャンしているかに基づいて、頻度グレードを計算します。頻度グレードが高い場合、資産を頻繁にスキャンしていることを示します。

頻度グレードの文字グレード	数値の範囲
A	75 ~ 100
B	55 ~ 74
C	30 ~ 54

D	15 ~ 29
F	0 ~ 14

評価成熟度 グレード、深度グレード、および頻度グレードを表示するには、評価成熟度詳細を表示するを参照してください。

Tenable Vulnerability Management が評価成熟度 グレードを計算または再計算するのにかかる時間の詳細は、Tenable Lumin のデータのタイミング を参照してください。

修正成熟度 グレード

重要: Tenable Lumin 内のデータ移行およびアルゴリズムの変更により、最近評価成熟度および修正成熟度のスコアが変更された可能性があります。これは想定された動作です。詳細については、Tenable の担当者までお問い合わせください。

修正成熟度 は、ライセンスのある資産の脆弱性をどれだけ効果的に修正しているかについて大まかなまとめを提供します。Tenable では、修正の健全性を **A** から **F** までの文字グレードで表す、動的な 修正成熟度 グレードを計算します。**A** グレードは、資産の脆弱性を迅速かつ徹底的に修正していることを表します。

修正成熟度 文字グレード	数値の範囲
A	75 ~ 100
B	55 ~ 74
C	30 ~ 54
D	15 ~ 29
F	0 ~ 14

修正成熟度 グレードは、修正成熟度 *修正応答性グレード*と、修正成熟度 *修正範囲グレード*を結合したものです。

Tenable は、最初に脆弱性を修正したタイミングで 修正成熟度 グレードを提示します。その後、Tenable Luminは毎日自動的に更新された 修正成熟度 グレードを提供します。

修正応答性グレード

Tenable は、脆弱性が最初に検出された日 (**初回確認**日) から修正までに要した時間に基づいて、修正応答性グレードを計算します。

修正応答性グレードが高い場合、資産の脆弱性を迅速に修正していることを表します。

修正応答性の文字グレード	数値の範囲
A	75 ~ 100
B	55 ~ 74
C	30 ~ 54
D	15 ~ 29
F	0 ~ 14

修正範囲グレード

Tenable は、資産の脆弱性の修正割合に基づいて修正範囲グレードを計算します。

修正範囲グレードが高い場合、資産の脆弱性の修正割合が高いことを表します。

修正範囲の文字グレード	数値の範囲
A	75 ~ 100
B	55 ~ 74
C	30 ~ 54
D	15 ~ 29
F	0 ~ 14

修正成熟度 グレード、修正応答性グレード、修正範囲グレードを表示するには、修正成熟度 詳細を表示するを参照してください。

Tenable Lumin が修正成熟度 グレードを計算または再計算するのにかかる時間の詳細は、Tenable Lumin のデータのタイミングを参照してください。

Tenable Lumin メトリクスを改善する

Tenable Lumin メトリクスの精度を改善して脆弱性管理全体の健全性を向上させたい場合は、Tenable が提供する値およびスキャン戦略の評価を行います。

重要: 非公開の検出結果は、Tenable Lumin 内のすべてのスコアから除外されます。詳細は、検出結果 を参照してください。

Tenable Lumin メトリクスの精度を改善する方法

1. [評価成熟度の詳細] ページで、評価成熟度 グレードをレビューしてスキャン全体の健全性を評価します。

   表示されるデータによって、次のいずれかを行います。

   - **[推奨アクション]** ウィジェットに記載されている任意のアクションを実行します。
   - **[深度グレード]** ウィジェットで、評価成熟度 深度グレードの詳細を表示します。必要に応じて、ユーザー定義テンプレートまたはスキャンで有効となっているプラグインの数を増やすか、認証スキャンまたはエージェントスキャンの数を増やして、深度グレードを改善します。詳細は、Tenable Vulnerability Management スキャンでのプラグインの設定、Tenable Vulnerability Management スキャンの認証情報、またはスキャンテンプレートを参照してください。

   スキャン全体の健全性が向上すると、評価成熟度 スコアも上昇します。

   評価成熟度 スコアが改善すると、Tenable が提供する ACR および VPR の値の精度が向上します。そして、ACR および VPR の値の精度が向上すると、AES と CES の値の精度も向上します。

2. 資産の表で、Tenable が提供する ACR の値をレビューして、ネットワーク上の資産の特性を評価します。ACR の値が企業独自のインフラやニーズを反映していない場合、それをオーバーライドすることができます。詳細については、ACR を手動で編集するを参照してください。

   ACR の値の精度が向上すると、AES と CES の値の精度も向上します。

3. [修正成熟度の詳細] ページで、修正成熟度 グレードをレビューして脆弱性修正全体の健全性を評価します。

   表示されるデータによって、次のいずれかを行います。

- **[推奨アクション]** ウィジェットに記載されている任意のアクションを実行します。
- **[修正応答性グレード]** ウィジェットで、修正成熟度 修正応答性グレードの詳細を表示します。必要に応じて、最も重大な(VPR が最大の)脆弱性を速やかに修正して、修正応答性グレードを改善します。詳細は、推奨アクションを表示する を参照してください。
- **[修正範囲グレード]** ウィジェットで、修正成熟度 修正範囲グレードの詳細を表示します。必要に応じて、修正する脆弱性の数を増やすことで修正範囲グレードを改善します。最も重大な脆弱性のある資産に関する詳細は、「脆弱性管理ダッシュボード」に従って **[脆弱性優先度の格付け]** ウィジェットを参照してください。

修正全体の健全性が向上すると、修正成熟度 スコアも上昇します。

ACR を手動で編集する

必要な追加ライセンス: Tenable Lumin

必要なユーザーロール: 管理者

資産の Asset Criticality Rating (ACR) 値をカスタマイズして、企業固有のインフラストラクチャやニーズを反映させることができます。1 つの資産の ACR を個別に編集することも、複数の資産の ACR を同時に編集することもできます。

ヒント: ACR値の変更内容 (および AESとCES値の再計算結果) は、24 時間以内に有効となります。

ヒント: 手動で上書きされた ACR 値に対して Tenable Vulnerability Management が優先度を付ける方法についての詳細は、ACR (資産重大度の格付け) (ACR)を参照してください。

注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

1 つの資産の ACRを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 次のいずれかを行います。

場所	アクション
[資産の詳細] ページ	a. 左側のナビゲーションプレーンの **[資産ビュー]** セクションで、**[資産]** をクリックします。 **[資産]** ページが表示されます。 b. 資産の行をクリックします。 **[資産の詳細]** ページが表示されます。 c. **[資産重大度の格付け]** セクションで、✎ ボタンをクリックします。

	Tenable Lumin **[資産重大度の格付けの編集]** プレーンが表示されます。
[資産] ページ	a. 左側のナビゲーションプレーンの **[資産ビュー]** セクションで、**[資産]** をクリックします。 **[資産]** ページが表示されます。 b. 資産の表で、編集する資産にカーソルを合わせます。 c. ⋮ ボタンをクリックします。 d. ✎ **[ACR の編集]** ボタンをクリックします。 **[資産重大度の格付けの編集]** プレーンが表示されます。

3. 次のいずれかを行います。

   - ACR 値を変更するには、**[資産重大度の格付け]** スライダーをクリックまたはドラッグして、ACR を増加または減少させます。

   - 既存の ACR 値を Tenable 提供の ACR 値にリセットするには、**[Tenable の ACR にリセットする]** をクリックします。

4. (オプション) ACRの変更に正当性を持たせる場合、**[上書きの理由]** セクションで 1 つ以上の理由を選択します。

   たとえば、開発ラボ環境にある資産に対して、より公共性の高い資産に適した Tenable 割り当ての ACR が与えられた場合、上書きの理由として **[開発環境のみ]** を選択できます。

5. (オプション) ACRの変更に注記を含める場合、**[注記]** セクションで注記を記入します。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management がカスタムの ACRを保存します。

複数の資産の ACRを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[Lumin]** をクリックします。

   Lumin ダッシュボードが表示されます。

3. **[事業の文脈タグによる Cyber Exposure Score]** ウィジェットで、資産の詳細を表示するタグをクリックします。

   Tenable Lumin **[事業の文脈とタグ資産の詳細]** ページ が、選択したタグでフィルタリングされた状態で表示されます。

4. 「事業の文脈/タグ資産の詳細を表示する」で説明されているとおり、**[資産重大度の格付け]** ウィジェット、**[資産のスキャンの分類]** ウィジェット、または **[資産スキャン頻度]** ウィジェットを通じて、**[資産]** ページにアクセスします。

   ウィジェットの選択によりフィルタリングされた状態で、**[資産]** ページが表示されます。

5. 表で、編集する資産の横にあるチェックボックスを選択します。

   ページの下部またはに、アクションバーが表示されます。

6. アクションバーで、✎ ボタンをクリックします。

   Tenable Lumin **[資産重大度の格付けの編集]** プレーンが表示されます。

7. **[資産重大度の格付け]** スライダーをクリックおよびドラッグして、ACR を設定します。

8. (オプション) ACRの変更に正当性を持たせる場合、**[上書きの理由]** セクションで 1 つ以上の理由を選択します。

9. (オプション) ACRの変更に注記を含める場合、**[注記]** セクションで注記を記入します。

10. **[保存]** をクリックします。

    Tenable Vulnerability Management は選択したすべての資産のカスタム ACRを保存します。

Tenable Lumin のデータのタイミング

スキャンを実行して、Tenable Lumin のビューで使用する脆弱性データを生成します。

- Tenable Vulnerability Management のスキャン結果データを表示する時間
- 次からのデータが同期されるタイミング Tenable Security Center
- CES、評価成熟度、または修正成熟度 グレードの計算または再計算のタイミング

Tenable Vulnerability Management のスキャン結果データを表示する時間

Tenable Vulnerability Management スキャンにより生成される脆弱性データは、スキャンが完了すると即座に Tenable Lumin ビューに表示されます。

新たに生成されたデータは、Tenable Lumin のメトリクス (たとえば CES) に直ちに影響するわけではありません。Tenable は、メトリクスの再計算のためにより多くの時間を必要とします。詳細は、CES、評価成熟度、または修正成熟度 グレードの計算または再計算のタイミング を参照してください。

次からのデータが同期されるタイミング Tenable Security Center

脆弱性および資産のデータは、異なる方法で Tenable Vulnerability Managementと同期されます。

データ	同期方法	タイミング
脆弱性データ	• 手動による最初の同期 • 同期されたリポジトリへの新しいスキャン結果データのインポート時に、自動的に継続して行われる同期。	同期を開始すると、Tenable Security Center は即座に Tenable Vulnerability Management へのデータ転送を開始します。10 ~ 15 分後、データが Tenable Vulnerability Managementに現れ始めます。 新たに転送されたデータは、Tenable Lumin メトリクス (たとえば CES) に直ちに影響するわけではありません。Tenable はメトリクスの再計算に、最長 48 時間を必要とします。 すべてのデータおよび再計算された Tenable Lumin メトリクスは、48 時間以内に Tenable Vulnerability Management に表示されます。
資産データ (Tenable Vulnerability Management 内のタグ)	手動 (オンデマンド) による同期のみ。	

Tenable Security Center の同期についての詳細は、*Tenable Security Center ユーザーガイド*の Tenable One の同期を参照してください。

CES、評価成熟度、または修正成熟度 グレードの計算または再計算のタイミング

Tenable Lumin は次のいずれかのイベントの後、メトリクスの計算または再計算に最大 24 時間を必要とします。

- Tenable Lumin ライセンス付与の後、Tenable Vulnerability Management が設定した最初のスキャンを実行した。
- Tenable Lumin ライセンス付与の後、最初の Tenable Security Center の同期を開始した。
- Tenable Vulnerability Management がスキャンを実行した。
- Tenable Security Center が、同期されたリポジトリに新しいデータをインポートするスキャンを実行した。

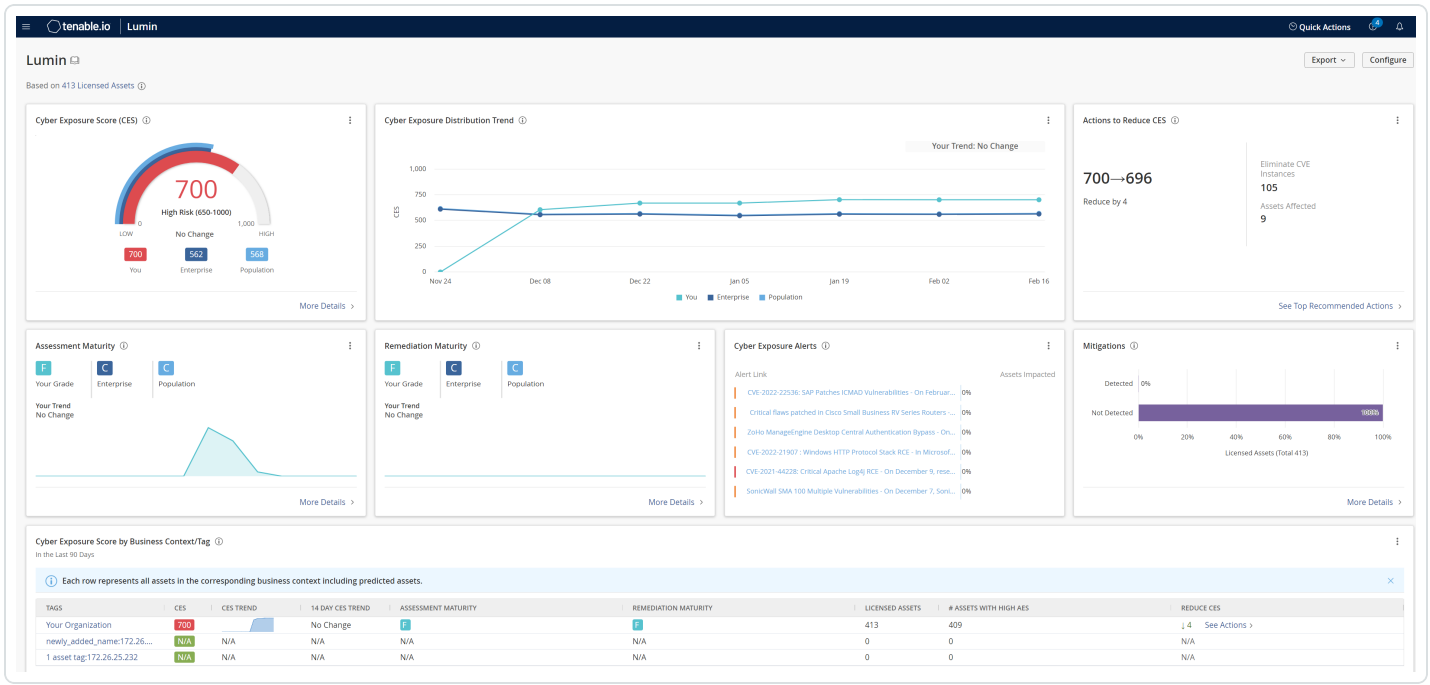
ヒント: Tenable Vulnerability Management は直近 90 日間のライセンスのある資産に基づいて、メトリクスを Tenable Luminします。スキャン設定を変更した場合 (例: 評価成熟度 グレードを向上させるために推奨アクションを行った場合)、変更は次回のスケジュールされた再計算に影響を与えますが、メトリクスに有意に影響を与えて一新させるまでには、さらに 90 日以上が必要となります。

Tenable Luminダッシュボードを表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable 提供の Tenable Lumin ダッシュボードは、企業のエクスポージャーデータを可視化します。この Tenable 提供のダッシュボードのウィジェットは、カスタマイズできません。



重要!Tenable One のユーザーは、[ワークスペース] ページから直接 Tenable Lumin にアクセスできます。

Tenable Lumin ダッシュボードで概要データを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[Lumin]** をクリックします。

   Lumin ダッシュボードが表示されます。

注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

Tenable Lumin ダッシュボードのランディングページをエクスポートする

必要な追加ライセンス: Tenable Lumin

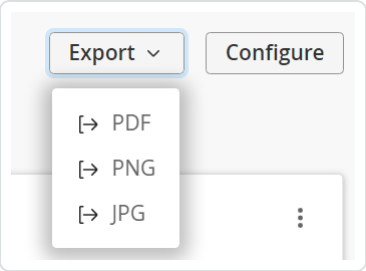
必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management で、[Tenable Lumin] ダッシュボードランディングページをエクスポートすることができます。

Tenable Lumin ダッシュボードランディングページをエクスポートする方法

1. Tenable Lumin ダッシュボードを表示します。
2. 右上にある **[エクスポート]** 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。

3. ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - **[PDF]** をクリックして、ダッシュボードを PDF 形式でエクスポートします。
   - **[PNG]** をクリックして、ダッシュボードを PNG 形式でエクスポートします。
   - **[JPG]** をクリックして、ダッシュボードを JPG 形式でエクスポートします。

   [進行中] メッセージが表示されます。

   エクスポートが完了したら、**[成功]** メッセージが表示され、Tenable Vulnerability Management によりお使いのコンピューターにエクスポートファイルがダウンロードされます。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

Tenable Lumin ダッシュボードからウィジェットをエクスポートする

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management で、Tenable Lumin ダッシュボードから個別のウィジェットをエクスポートすることができます。

注意: **[事業の文脈別の Cyber Exposure Score]** ウィジェットのエクスポートはできません。

Tenable Lumin ダッシュボードからウィジェットをエクスポートする方法

1. Tenable Lumin ダッシュボードを表示します。
2. エクスポートするウィジェットのヘッダーで、••• 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。

3. ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - **[PDF]** をクリックして、ダッシュボードを PDF 形式でエクスポートします。
   - **[PNG]** をクリックして、ダッシュボードを PNG 形式でエクスポートします。
   - **[JPG]** をクリックして、ダッシュボードを JPG 形式でエクスポートします。

   [進行中] メッセージが表示されます。

   エクスポートが完了したら、**[成功]** メッセージが表示され、Tenable Vulnerability Management によりお使いのコンピューターにエクスポートファイルがダウンロードされます。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

Tenable Lumin 業界ベンチマークを更新する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

大規模な企業では、複数の業界にまたがる事業部や、1 つの業界に分類しにくい事業部が存在する場合があります。Tenable Lumin で最適な業界ベンチマークを選択すると、データの関連性が最大化され、Tenable Lumin 適用される指標をほかの類似した業界の指標と比較してより正確に追跡できます。

Tenable Lumin 業界ベンチマークを更新する方法

1. 左上にある ☰ ボタンをクリックします。

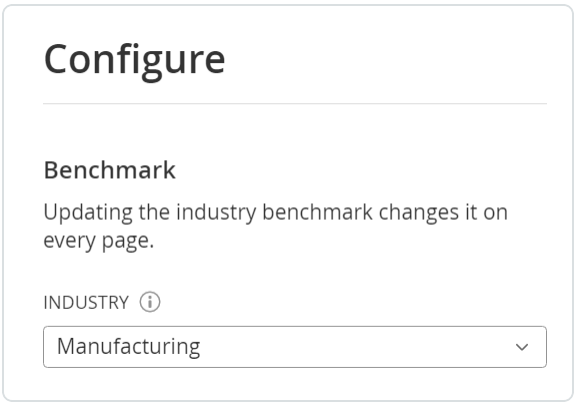
   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[Lumin]** をクリックします。

   Lumin ダッシュボードが表示されます。

3. 右上の **[設定]** をクリックします。

   [設定] プレーンが表示されます。



4. **[ベンチマーク]** セクションの **[業界]** ドロップダウンから、Tenable Lumin ダッシュボードで使用する業界ベンチマークを選択します。

5. **[保存]** をクリックします。

   [業界が更新されました] という確認メッセージが表示され、Tenable Vulnerability Management は Tenable Lumin ダッシュボードに新しい業界を適用します。

(オプション) Tenable Lumin 業界ベンチマークをリセットする方法

1. **[Configure Industry]** プレーンで、**[Reset to Default]** をクリックします。

   確認のメッセージが表示されます。

2. **[確認]** をクリックします。

   [Industry Updated] という確認メッセージが表示され、Tenable Vulnerability Management は業界を、アカウント作成時に選択した業界にリセットします。

Tenable Lumin ダッシュボードウィジェット

Tenable Lumin ダッシュボードは、次のウィジェットで構成されます。

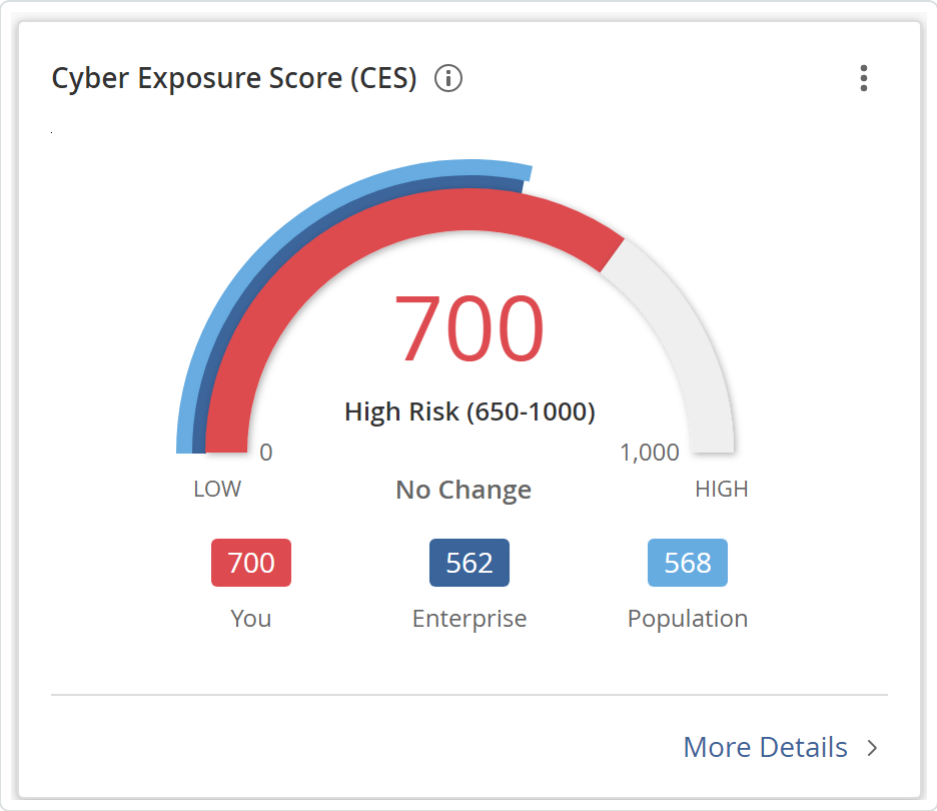
- Cyber Exposure Score
- Cyber Exposure Score Trend
- CES を減らすためのアクション
- 評価成熟度
- 修正成熟度
- Cyber Exposure アラート
- 軽減策
- 事業の文脈/タグ別の Cyber Exposure Score

注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

Cyber Exposure Score

他の Tenable のお客様 (Salesforce 業界および全体)と比較して、全体的なリスクはどの程度ですか?

タイムフレーム	資産
過去 90 日	企業全体のライセンスのある資産



このウィジェットは、企業全体の CESを Tenable のお客様 (Salesforce 業界および全体)と比較してまとめたものです。

このウィジェットでは、次のアクションを実行できます。

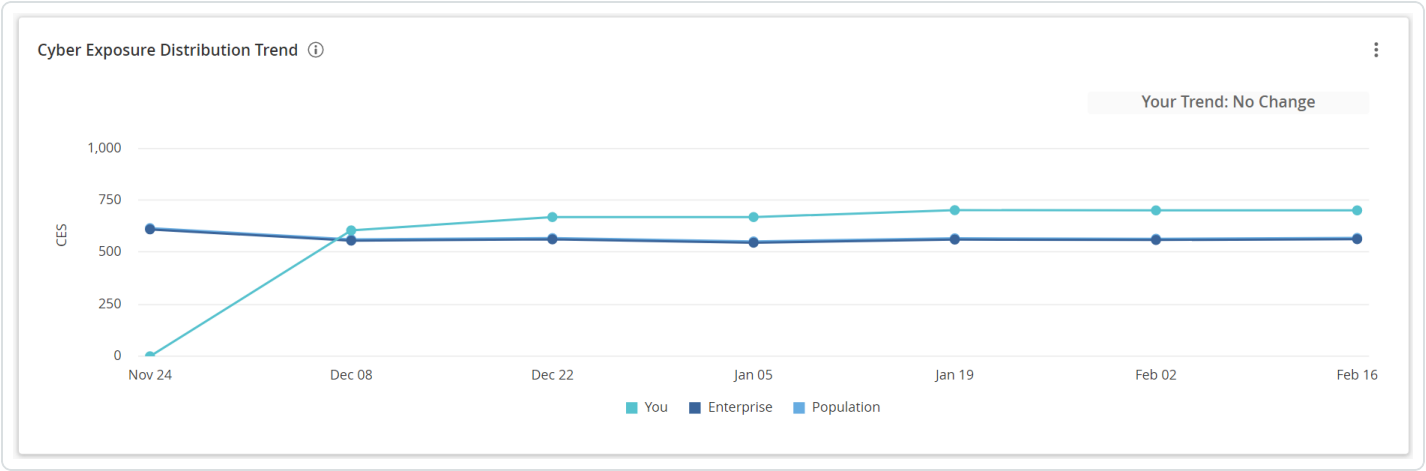
- 自分の CESと、Tenable のお客様 (Salesforce 業界および全体)の CESの平均を比較して視覚的に表示します。
- 最近 CESが増加しているのか減少しているのかについての概要を表示します。
- CES の詳細を表示するには、CES の値をクリックします。

  Tenable Lumin **Cyber Exposure Score** の詳細のプレーンが表示されます。詳細は、CESDetailsを参照してください。
- ダッシュボードウィジェットをエクスポートします。

Cyber Exposure Score Trend

企業全体の総合的なリスクは、時間とともにどう変化していますか?

タイムフレーム	資産
過去 90 日間のグラフ上の各ポイント、日ごとに再計算	企業全体のライセンスのある資産



このウィジェットは、自分の CESと、Tenable のお客様 (Salesforce 業界および全体) の CESの平均の増減をグラフ化します。

このウィジェットでは、次のアクションを実行できます。

- 特定の日付の、業界または全体の CESの値の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。

  CES の履歴データが表示されます。

- 特定の日付の、自分の CESの値の詳細を表示するには、**You** の線上のポイントをクリックします。

  Tenable Lumin[Cyber Exposure Score] の詳細のプレーンが表示されます。詳細は、CES の詳細を参照してください。

- 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。

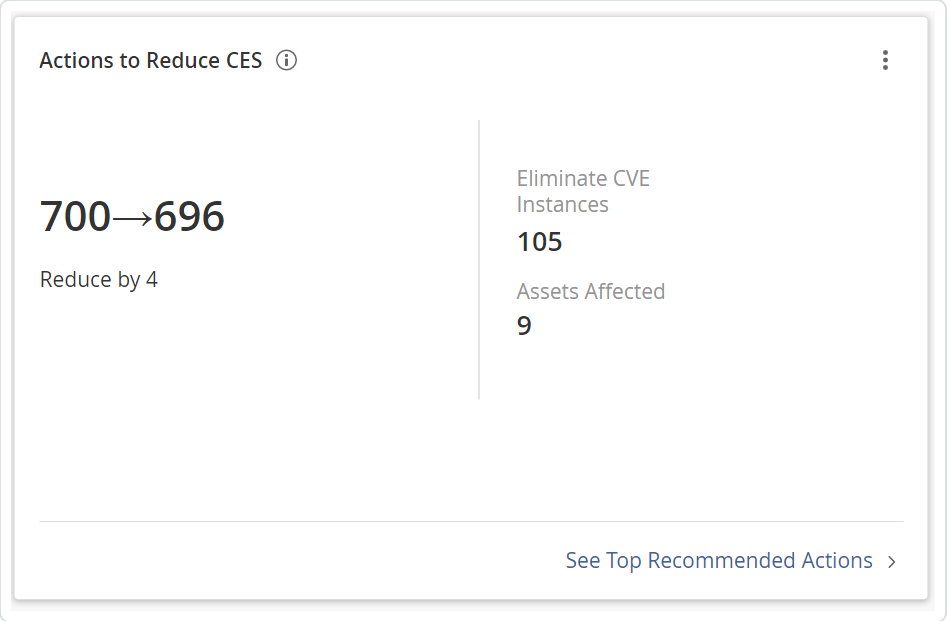
  システムはウィジェットを更新して、選択したデータを表示または非表示にします。

- ダッシュボードウィジェットをエクスポートします。

CES を減らすためのアクション

上位 20 の推奨アクションのすべてを実行した場合、どのような影響があるでしょうか?

タイムフレーム	資産
過去 90 日	企業全体のライセンスのある資産



このウィジェットは、上位 20 の推奨アクションが与える影響についてまとめたものです。

このウィジェットでは、次のアクションを実行できます。

- 上位 20 の推奨アクションのすべてを実行した場合に予想される CES の減少量を表示します。
- 上位 20 の推奨アクションのすべてを実行した場合に除去できる脆弱性インスタンスの数を表示します。

  ヒント：脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。

- 上位 20 の推奨アクションにより影響を受けている資産の数を表示します。
- 上位 20 の推奨アクションに関する詳細を表示するには、**[上位の推奨アクションを参照]** をクリックします。

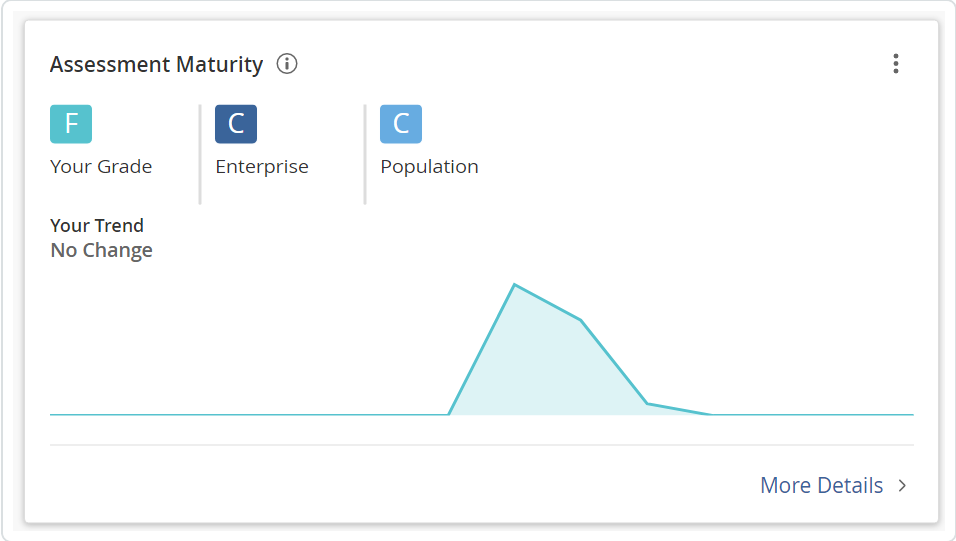
  Tenable Lumin **[推奨アクション]** ページが表示されます。詳細は、推奨アクションを表示する を参照してください。

- ダッシュボードウィジェットをエクスポートします。

評価成熟度

どのくらいの頻度でどれだけ徹底的に資産をスキャンしていますか?

タイムフレーム	資産
過去 90 日	企業全体のライセンスのある資産



このウィジェットは、企業全体の評価成熟度 グレードを Tenable のお客様 (Salesforce 業界および全体) と比較してまとめたものです。

重要: Tenable Lumin 内のデータ移行およびアルゴリズムの変更により、最近評価成熟度および修正成熟度のスコアが変更された可能性があります。これは想定された動作です。詳細については、Tenable の担当者までお問い合わせください。

このウィジェットでは、次のアクションを実行できます。

- 自分の評価成熟度 グレードと、Tenable のお客様 (Salesforce 業界および全体) の評価成熟度 グレードの平均を比較して表示します。
- 最近、評価成熟度 グレードが増加しているのか減少しているのかについての概要を表示します。
- 評価成熟度 グレードの過去の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。

  評価成熟度 グレードの履歴データが表示されます。
- 評価成熟度 グレードについての詳細を表示するには、**[詳細]** をクリックします。

  Tenable Lumin **[評価成熟度]** ページ が表示されます。詳細は、評価成熟度詳細を表示する を

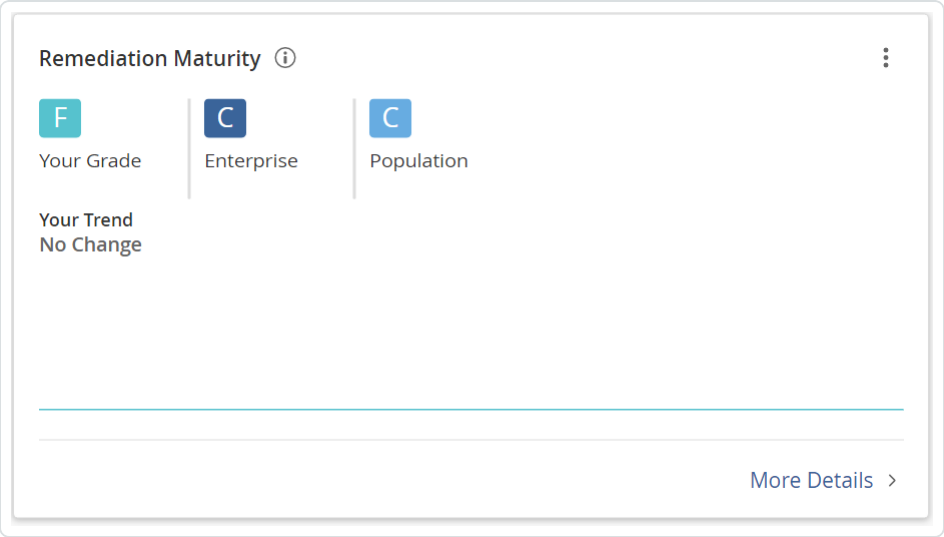
参照してください。

- ダッシュボードウィジェットをエクスポートします。

修正成熟度

資産の脆弱性をどれだけ迅速かつ徹底的に修正していますか?

タイムフレーム	資産
過去 90 日	企業全体のライセンスのある資産



重要: Tenable Lumin 内のデータ移行およびアルゴリズムの変更により、最近評価成熟度および修正成熟度のスコアが変更された可能性があります。これは想定された動作です。詳細については、Tenable の担当者までお問い合わせください。

このウィジェットは、企業全体の修正成熟度グレードを Tenable のお客様 (Salesforce 業界および全体) と比較してまとめたものです。

このウィジェットでは、次のアクションを実行できます。

- 自分の修正成熟度 グレードと、Tenable のお客様 (Salesforce 業界および全体) の修正成熟度グレードの平均を比較して表示します。
- 最近、修正成熟度 グレードが増加しているのか減少しているのかについての概要を表示します。
- 修正成熟度 グレードの過去の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。

修正成熟度 グレードの履歴データが表示されます。

- 修正成熟度 グレードについての詳細を表示するには、**[詳細]** をクリックします。

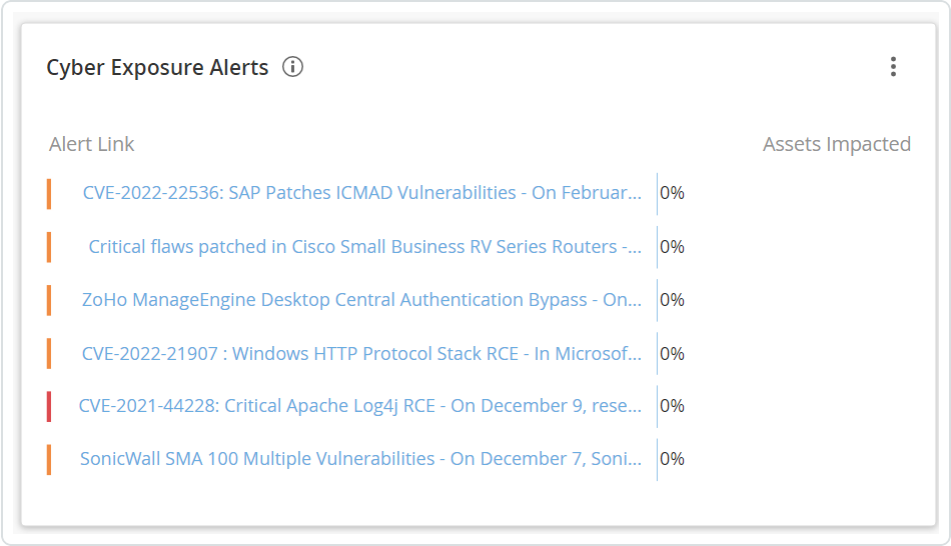
  Tenable Lumin [**Remediation Maturity**] ページ が表示されます。詳細は、修正成熟度 詳細を表示する を参照してください。

- ダッシュボード ウィジェット をエクスポートします。

Cyber Exposure アラート

Tenable Research のサイバーセキュリティアラート で知っておくべきアラート

タイムフレーム	資産
直近のアラート 6 件	企業全体のライセンスのある資産



このウィジェット には、Tenable Researchチームが提供する直近のサイバーセキュリティアラート が 6 つ表示されます。Tenable Lumin では、影響を受けている可能性のある資産の数に関する詳細と、アラートに関する Tenable ブログ投稿 へのリンクを提供します。このブログ投稿でさらに詳しい情報と必要な対応を確認できます。

注意: 正確な CVE カウントを維持するために Tenable Lumin では、Patch Tuesday や Oracle CPU などからのエントリを **[サイバーエクスポージャーアラート]** ウィジェット 内にアラートとして含めません。

[サイバーエクスポージャーアラート] ウィジェット 内のノイズを低減させるために Tenable Lumin は、特定の (つまり、Patch Tuesday/Oracle CPU からの) CVE をターゲットとしていません。

このウィジェットでは、次のアクションを実行できます。

- サイバー空間に露呈されたリスクのアラートを次のいずれかの深刻度で表示します。
    - **情報**(低) - このアラートには、関心があるかもしれない情報が含まれていますが、即座に対応する必要はありません。
    - **アドバイザリ**(中) - このアラートには警告情報が含まれており、対応が必要な場合があります。
    - **応答**(重大) - このアラートには即座の対応が必要です。
- アラートの深刻度、簡単な説明、およびアラートが公開された日付を表示するには、ウィジェットにあるアラートのいずれかにカーソルを合わせます。
- アラートによって影響を受けている資産(アラートに関連付けられているCVEのいずれかが資産の脆弱性として存在している資産)の割合を表示するには、**[影響を受ける資産]**列にある行の1つにカーソルを合わせます。

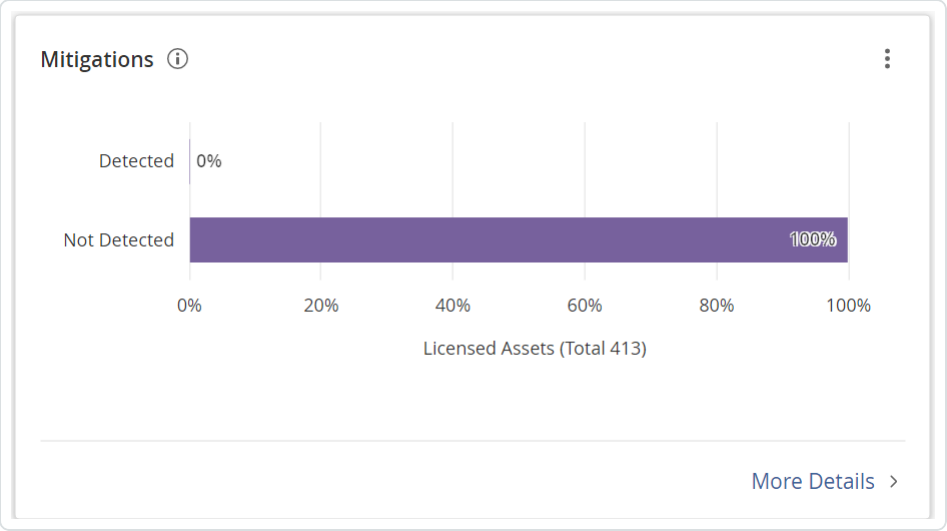
  アラートにCVEがあるものの影響を受けている資産が存在しない場合、あるいは資産の脆弱性スキャンを実施していない場合、**[影響を受けた資産]**列には0%の値が表示されます。現在、アラートに割り当てられているCVEが存在しない場合、**[影響を受けた資産]**列には**[保留中]**の値が表示されます。Tenable Vulnerability Managementがアラートの CVEを計算すると、Tenable Luminは適切な値で列を更新します。
- アラートに関連付けられているCVEで自動的にフィルタリングされた資産別の脆弱性を表示するには、ウィジェットにあるパーセンテージのいずれかをクリックします。
- サイバー空間に露呈されたリスクのアラートに関するTenableのブログ投稿を表示するには、ウィジェット内にアラートのいずれかをクリックします。
- アラートの**[流行している脅威]**ページを表示するには、ウィジェット内のアラートの1つをクリックします。
- ダッシュボードウィジェットをエクスポートします。

軽減策

エンドポイント保護エージェント は資産にどのように分布されていますか?

タイムフレーム	資産

過去 90 日	企業全体のライセンスのある資産



このウィジェットでは、資産のエンドポイント保護エージェント の分布がまとめられています。

[基本的なネットワークスキャン] テンプレートまたは **[高度なネットワークスキャン]** テンプレートに基づく認証スキャンを実行する場合、もしくは **[基本的なエージェントスキャン]** または **[高度なエージェントスキャン]** テンプレートに基づくエージェントスキャンを実行する場合、Tenable は資産に存在する緩和策の検出に必要なプラグインを自動的に有効にします。Tenable Lumin は、緩和策をエンドポイント保護エージェント、これにはアンチウイルスソフトウェア、エンドポイント保護プラットフォーム (EPP)、またはエンドポイント検知・対応 (EDR) ソリューションが含まれます。として定義します。

このウィジェットでは、次のアクションを実行できます。

- 軽減策 カテゴリ内の資産のリストを表示するには、ウィジェットの割合の中の 1 つをクリックします。

  ライセンスのある資産、選択した緩和策カテゴリ、および過去 90 日間でフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。

  > **注意: 軽減策** ウィジェットから **[資産]** ページにアクセスすると、ページの上部に資産カウントの通知が表示される場合があります。この通知は、ユーザーが属しているアクセスグループを基にして表示するアクセス許可を持っている資産の数を示しています。

- 資産で検出されたエンドポイント保護エージェント についての詳細を表示するには、**[詳細]** をクリックします。

  Tenable Lumin **[緩和]** ページ が表示されます。詳細は、Tenable Lumin で 軽減策 の詳細を表

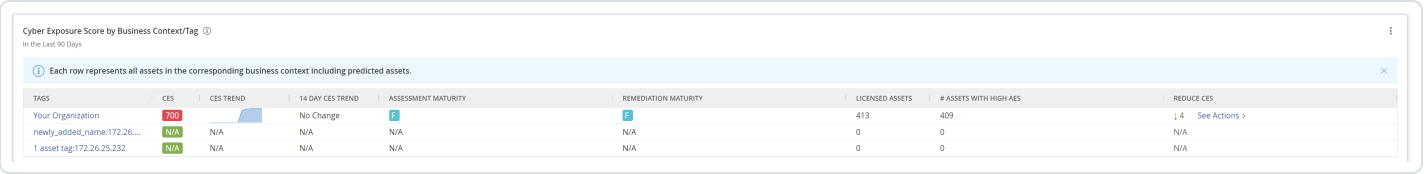
示する を参照してください。

- ダッシュボードウィジェットをエクスポートします。

事業の文脈/タグ別の Cyber Exposure Score

異なるタグ(固有のビジネス文脈)別に資産を比較するとどうですか?

タイムフレーム	資産
過去 90 日	選択したタグが適用された、すべてのライセンスのある資産



このウィジェットには、企業全体に対して、および特定の事業の文脈タグによりタグ付けされた資産に対して計算された CES に関するデータがまとめられています。

このウィジェットでは、次のアクションを実行できます。

- 各タグの資産のデータを表示します。

  - **CES** - タグ付けされた資産の CES の平均。値が **[N/A]** の場合、Tenable が CES を計算中であることを示します。

  - **CES Trend** - 過去 180 日間での CES の変化の視覚的な表示。値が **[N/A]** の場合、Tenable が CES データを処理中であるか、このタグが付いた資産の数が 0 であることを示します。
  - **14 Day Trend** - 過去 14 日間で CES がどう増加 (↑) あるいは減少 (↓) したかのサマリー。値が **[N/A]** の場合、Tenable が CES データを処理中であるか、このタグが付いた資産の数が 0 であることを示します。

  - **評価成熟度** - タグ付けされた資産の 評価成熟度 グレード。値が **[N/A]** の場合、タグ付けされた、ライセンスのある資産の数が 0 であることを示します。

特定のタグが付いた資産に対する評価成熟度グレードに関する詳細を表示するには、**[評価成熟度]**列でグレードをクリックします。

Tenable Lumin **[評価成熟度]**ページが、選択したタグでフィルタリングされた状態で表示されます。

- **修正成熟度** - タグ付けされた資産の修正成熟度グレード。

  特定のタグが付いた資産に対する修正成熟度グレードに関する詳細を表示するには、**[修正成熟度]**列でグレードをクリックします。

  Tenable Lumin [**Remediation Maturity**] ページが、選択したタグでフィルタリングされた状態で表示されます。詳細は、修正成熟度 詳細を表示する を参照してください。

- **ライセンス資産** - タグ付けされた、ライセンスのある資産の数。
- **「高」AES を持つ資産の数** - AESの高いタグ付けされた資産の数。

- **Reduce Tag CES** - この特定のタグを付けられた資産に対するすべてのソリューションを実行した場合に想定される、タグレベルでの CES の減少量。値が**[N/A]**の場合、想定される減少量が 5 以下であることを示します。一般的に、多くの資産が認証なしでスキャンされている場合や、資産が健全でリスクが既に低い場合には、CES を大きく低減させることはできません。

  特定のタグが付いた資産に対する推奨アクションを表示するには、**[タグの CES の削減]**列で**[アクションを見る]**をクリックします。

  ライセンスのある資産と選択したタグでフィルタリングされた状態で、Tenable Lumin **[推奨アクション]**ページが表示されます。

- 特定のタグが付いた資産の詳細を表示するには、表の行をクリックします。

  Tenable Lumin **[事業の文脈とタグ資産の詳細]**ページが表示されます。詳細は、事業の文脈/タグ資産の詳細を表示する を参照してください。

- ウィジェットに表示されるタグを変更する方法

1. ⋮ ボタンをクリックします。
2. ⚙ **[設定]** ボタンをクリックします。

   ウィジェットの編集プレーンが表示されます。
3. 次のいずれかを行います。
   - ウィジェットの順番を変える方法
     a. 移動したいタグの隣にある ⠿ ボタンを押しつづけます。
     b. 移動したい場所までタグをドラッグします。
     c. マウスボタンを放して、タグを新しい場所にドロップします。
   - ウィジェットからタグを削除するには、🗑 ボタンをクリックします。
   - ウィジェットにタグを追加するには、⊕ **[タグを追加]** ボタンをクリックし、追加するタグを指定します。

     このウィジェットでは、25 個までのタグのデータを表示できます。
4. **[保存]** をクリックします。

   Tenable Vulnerability Management によってウィジェットが更新されます。

- 表の並べ替えについては、Tenable Vulnerability Management の表を参照してください。

CES の詳細パネルを表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

このページを使用して、自社、または特定の事業の文脈タグを持つ資産の CES 詳細を参照します。

CES の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[Lumin]** をクリックします。

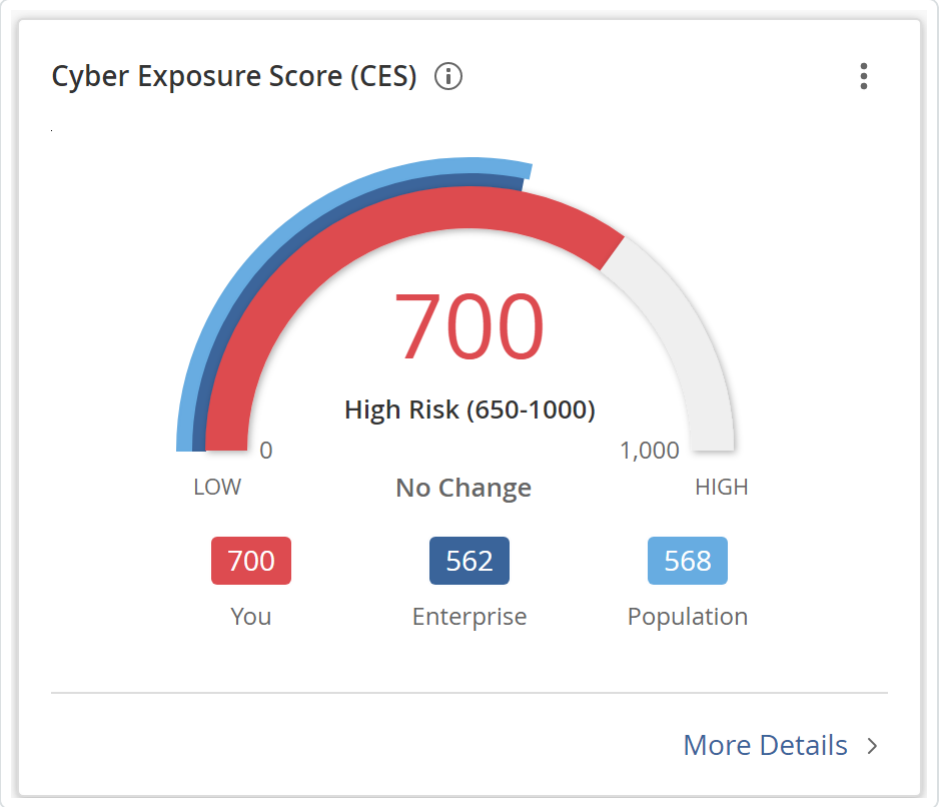
   Lumin ダッシュボードが表示されます。

3. 次のいずれかを行います。

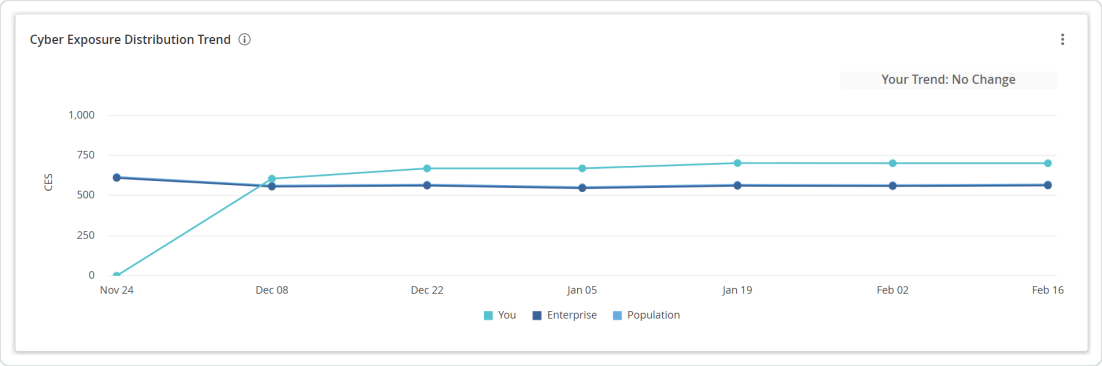
   - 企業全体の CES の詳細を表示する方法

     a. 次のいずれかを行います。

     - 現在の CES の詳細を表示するには、**[Cyber Exposure Score]** ウィジェットで CES の値をクリックします。



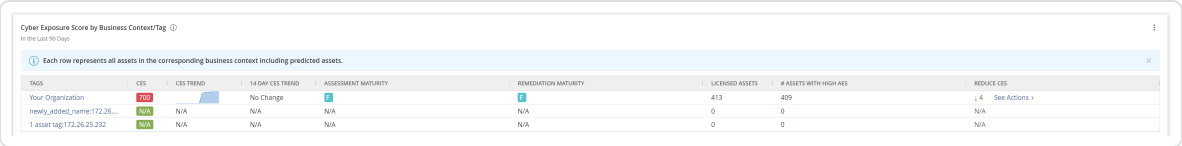
- 過去の CES の詳細を表示するには、**[Cyber Exposure Score トレンド]** ウィジェットでグラフ上の過去のポイントをクリックします。



- 特定の事業の文脈タグの付いた資産の CES の詳細を表示する方法

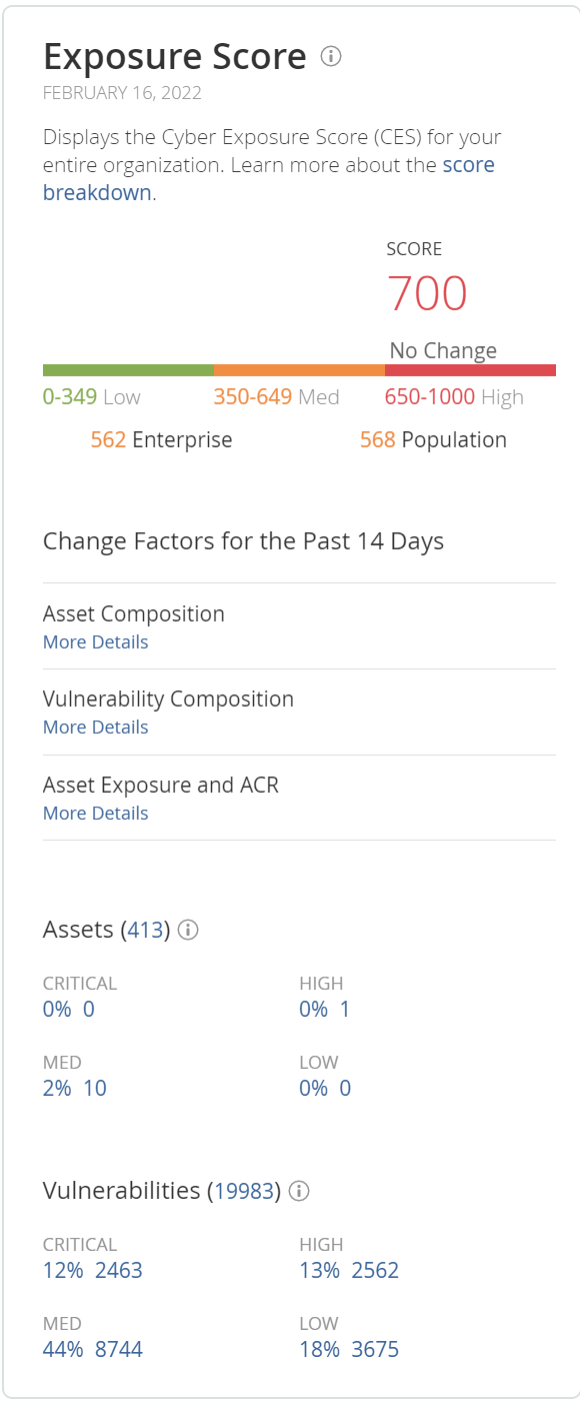
  a. **[事業の文脈タグによる Cyber Exposure Score]** ウィジェットで、資産の詳細を表示するタグをクリックします。

  Tenable Lumin **[事業の文脈とタグ資産の詳細]** ページが、選択したタグでフィルタリングされた状態で表示されます。



b. **[Cyber Exposure Score トレンド]** ウィジェットで、CES の値をクリックします。

Tenable Lumin[Cyber Exposure Score] の詳細のプレーンが表示されます。



注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

セクション	タイムフレーム	資産	アクション

Score	過去 90 日	ライセンスのある資産	• 企業全体の CES と、他の Tenable のお客様 (Salesforce 業界および全体) の CES の平均を表示します。 • 企業全体のスコアが過去 14 日間のうちに増加したか (↑)、または減少したか (↓) を表示します。
Change Factors for the Past 14 Days	過去 14 日	ライセンスのある資産	• スコア変更の一因となった主なイベントを表示します。Tenable Vulnerability Management は、変更タイプごとに因子をグループ化します。 ◦ **CES Algorithm** - CES のアルゴリズムのアップデートに関連するすべての変更点詳細は、Lumin FAQ を参照してください。 **注意:** このセクションはアルゴリズムの更新によって CES のスコアに影響が出た場合のみ表示されます。 ◦ **[資産構成の変更]** - 資産ライセンスの変更、資産の深度変更など ◦ **[脆弱性構成の変更]** - 脆弱位の修正、新しい脆弱性の検出など ◦ **[資産エクスポージャーおよび ACR]** - AES または ACR への変更 • 変更内容に関する具体的な詳細を表示するには、変更要因グループで、**[詳**

			細] をクリックします。 Tenable Lumin は、過去 14 日間で増加 (↑) または減少 (↓) した要因の数を特定の原因ごとに表示します。
資産 (#) (現在の CES の詳細を表示しているときのみ表示)	常時	ライセンスのある資産とライセンスのない資産	• 資産の合計数を表示します。 • 各 ACR カテゴリごとに、次の情報を表示します。 ◦ 重大、高、中、低の ACR 値を持つ資産割合 **ヒント:** スコア化されていない資産がある場合、割合の合計は 100% にはなりません。 ◦ 重大、高、中、低の ACR 値を持つ資産の総数 ◦ 重大、高、中、低の ACR 値を持つ資産の数が過去 14 日間で増減した場合、対象期間における資産の割合と資産の総数が増加 (↑) または減少した (↓) 数。 • ACR カテゴリ内の資産のリストを表示するには、割合をクリックします。 ライセンスのある資産、および選択した ACR カテゴリでフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。
Vulnerabilities (#) (現在の CES の詳	常時	ライセンスのある	• 資産に存在する脆弱性の合計数を表示します。

細を表示しているときのみ表示)		資産とライセンスのない資産	• 各 VPR カテゴリごとに、次の情報を表示します。 ◦ 重大、高、中、低の VPR 値を持つ脆弱性の割合 **ヒント:** スコア化されていない資産がある場合、割合の合計は 100% にはなりません。 ◦ 重大、高、中、低の VPR 値を持つ脆弱性の総数 ◦ 重大、高、中、低の VPR 値を持つ脆弱性の数が過去 14 日間で増減した場合、対象期間における脆弱性の割合と脆弱性の総数が増加 (↑) または減少した (↓) 数。 • VPR カテゴリ内の脆弱性リストを表示するには、割合をクリックします。 ライセンスのある資産、および選択した VPR カテゴリでフィルタリングされた状態で、**[脆弱性]** ページが表示されます。詳細は、View Vulnerabilities by Plugin を参照してください。

評価成熟度詳細を表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable は、総合的なスキャンの深度と頻度を表す、動的な 評価成熟度 グレードを計算します。詳細については、評価成熟度 を参照してください。

重要: Tenable Lumin 内のデータ移行およびアルゴリズムの変更により、最近評価成熟度および修正成熟度のスコアが変更された可能性があります。これは想定された動作です。詳細については、Tenable の担当者までお問い合わせください。

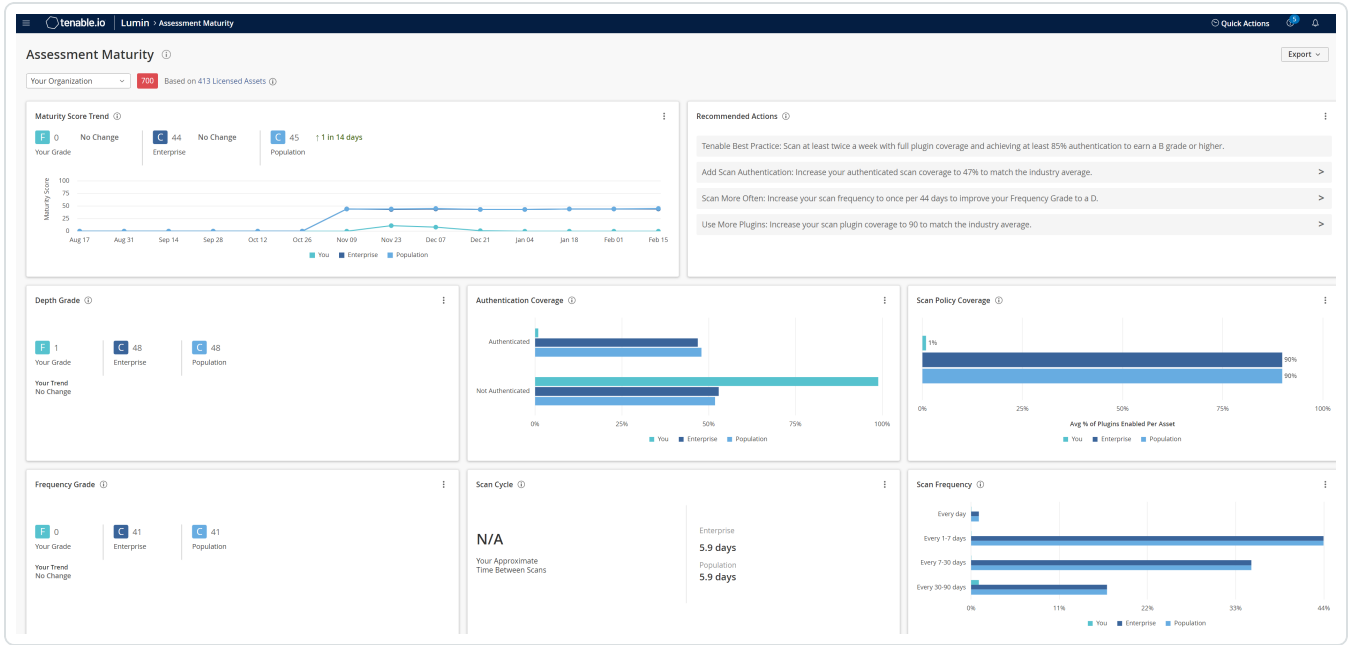
すべての資産に対する 評価成熟度 の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[評価成熟度]** をクリックします。

   [評価成熟度] ページが表示され、デフォルトでは、企業全体の詳細が表示されます。



3. (オプション) ページに適用されるタグフィルターを変更するには、左上にあるドロップダウンリストからタグを選択します。

   Tenable Lumin は、ユーザーが選択したタグでページをフィルタリングします。

注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

セクションまたはウィジェット	タイムフレーム	資産	アクション
サマリー	過去 90 日	ライセンスのある資産	このセクションは、自分の評価成熟度 グレードを Tenable のお客様 (Salesforce 業界および全体) と比較してまとめたものです。 • 自分の評価成熟度と、Tenable のお客様 (Salesforce 業界および全体)の評価成熟度の平均を比較して視覚的に表示します。 • 評価成熟度 に影響を与えるライセンスのある資産のリストを表示するには、**[<count> ライセンス資産]** をクリックします。 過去 90 日間のライセンスのある資産がフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。 • 評価成熟度 に影響を与えない、ライセンスのない資産のリストを表示するには、**[<count> ライセンスなし]** をクリックします。 過去 90 日間のライセンスのない資産がフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。
Maturity Score Trend	過去 90 日間の	ライセンスの	このウィジェットは、自分の評価成熟度 グレードと、Tenable のお客様 (Salesforce 業界および全体) の

評価成熟度 グレードは時間とともにどう変化していますか?	グラフ上の各ポイント、日ごとに再計算	ある資産	評価成熟度 グレードの平均の増減をグラフ化します。 • 特定の日付の評価成熟度 グレードの詳細を表示するには、グラフ上のポイントにカーソルを合わせます。 評価成熟度 グレードの履歴データが表示されます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。
推奨アクション スキャンの健全性を向上させるために、どんな一般的なアクションをとることができますか?	過去 90 日	ライセンスのある資産	このウィジェットでは、Tenable 推奨のベストプラクティスを提供して、スキャンの健全性を向上させます。 • 推奨されるベストプラクティスを確認します。 • アクションを行うには、説明の横のリンクをクリックします。
Depth Grade 資産は十分徹底的にスキャンされていますか?	過去 90 日	ライセンスのある資産	このウィジェットは、企業全体の評価成熟度 の深度グレードを Tenable のお客様 (Salesforce 業界および全体) と比較してまとめたものです。 • 自分の深度グレードと、Tenable のお客様 (Salesforce 業界および全体) の深度グレードの平均を比較して視覚的に表示します。 • 最近、深度グレードが増加しているのか減少しているのかについての概要を表示します。
Authentication Coverage	過去 90 日	ライセンスのある	このウィジェットでは、認証スキャンおよび非認証スキャンされた資産の割合を、Tenable のお客様 (Salesforce 業界および全体) と比較してグラフ化し

どのくらいの頻度で認証スキャンを実行していますか?		資産	ます。資産上ですべてのプラグインが動作するように正常な認証状態で確実にスキャンを行うことで、認証の範囲を最適化できます。 • 自分の認証範囲と、Tenable のお客様 (Salesforce 業界および全体) の深度グレードの平均を比較して視覚的に表示します。 • 詳細を表示するには、グラフ上のスキャンタイプクラスターにカーソルを合わせます。 スキャンタイプに関するデータが表示されます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。
頻度グレード 資産は十分な頻度でスキャンされていますか?	過去 90 日	ライセンスのある資産	このウィジェットは、企業全体の評価成熟度 の頻度グレードを Tenable のお客様 (Salesforce 業界および全体) と比較してまとめたものです。 **ヒント:** Tenable は、どのくらい頻繁にネットワーク上の資産をスキャンしているかに基づいて、頻度グレードを計算します。 • 自分の頻度グレードと、Tenable のお客様 (Salesforce 業界および全体) の頻度グレードの平均を比較して視覚的に表示します。 • 最近、頻度グレードが増加しているのか減少しているのかについての概要を表示します。
スキャンサイクル スキャン実行の間隔はどのくらいです	過去 90 日	ライセンスのある資産	このウィジェットは、自分のスキャン頻度の日数の平均を Tenable のお客様 (Salesforce 業界および全体) と比較してまとめたものです。スキャンサイクルは、資産に対する各スキャンの間の日数の平均です。

か?			
資産スキャン頻度 どのくらいの頻度で、資産をスキャンしていますか?	過去 90 日	ライセンスのある資産	このウィジェットは、日単位、週単位、月単位、四半期単位で Tenable Vulnerability Management がスキャンする資産の割合を Tenable のお客様 (Salesforce 業界および全体) と比較してグラフ化します。 • 特定の期間のスキャン頻度の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。 スキャン頻度のデータが表示されます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。

修正成熟度 詳細を表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable は、総合的な脆弱性の修正応答性と修正範囲を表す、動的な 修正成熟度 グレードを計算します。詳細は、修正成熟度を参照してください。

重要: Tenable Lumin 内のデータ移行およびアルゴリズムの変更により、最近評価成熟度および修正成熟度のスコアが変更された可能性があります。これは想定された動作です。詳細については、Tenable の担当者までお問い合わせください。

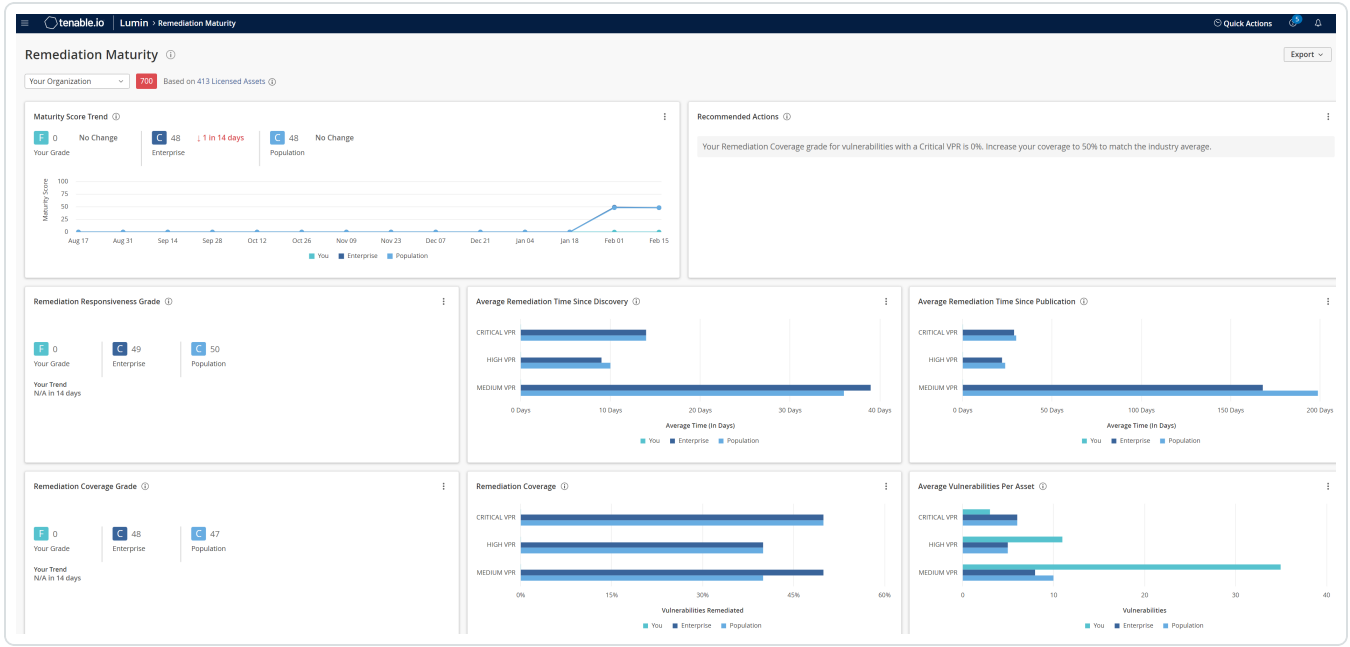
すべての資産に対する 修正成熟度 の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[修正成熟度]** をクリックします。

   [修正成熟度] ページが表示されます。



3. (オプション) ページに適用されるタグフィルターを変更するには、左上にあるドロップダウンリストからタグを選択します。

   Tenable Lumin は、ユーザーが選択したタグでページをフィルタリングします。

注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

セクションまたはウィジェット	タイムフレーム	資産	アクション
サマリー	過去 90 日	ライセンスのある資産	このセクションは、自分の修正成熟度グレードを、Tenable のお客様 (Salesforce 業界および全体)と比較してまとめたものです。 • 自分の修正成熟度と、Tenable のお客様 (Salesforce 業界および全体)の修正成熟度の平均を比較して視覚的に表示します。 • 修正成熟度 グレードに影響を与えるライセンスのある資産のリストを表示するには、**[*<count>* ライセンス資産]** をクリックします。 過去 90 日間のライセンスのある資産がフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。 • 修正成熟度 グレードに影響を与えない、ライセンスのない資産のリストを表示するには、**[*<count>* ライセンスなし]** をクリックします。 過去 90 日間のライセンスのない資産がフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。

Maturity Score Trend 修正成熟度 グレードは時間とともにどう変化していますか？	過去 90 日間のグラフ上の各ポイント、日ごとに再計算	ライセンスのある資産	このウィジェットは、自分の修正成熟度グレードと、Tenable のお客様 (Salesforce 業界および全体)の修正成熟度 グレードの平均の増減をグラフで表示します。 • 特定の日付の修正成熟度 グレードの詳細を表示するには、グラフ上のポイントにカーソルを合わせます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。
推奨アクション 修正の健全性を向上させるために、どんな一般的なアクションをとることができますか？	過去 90 日	ライセンスのある資産	このウィジェットは、Tenable 推奨のベストプラクティスを提供して、修正の健全性を向上させます。 • 推奨されるベストプラクティスを確認します。 • アクションを行うには、説明内のリンクをクリックします。
修正応答性グレード どれだけ迅速に脆弱性を修正していますか?	過去 90 日	ライセンスのある資産	このウィジェットは、企業全体の修正成熟度修正応答性グレードを、Tenable のお客様 (Salesforce 業界および全体)と比較してまとめたものです。 • 自分の修正応答性グレードと、Tenable のお客様 (Salesforce 業界および全体)の修正応答性グレードの平均を比較して視覚的に表示します。 • 最近、修正応答性グレードが増加して

			いるのか減少しているのかについての概要を表示します。
Average Remediation Time Since Discovery 脆弱性が最初に検出された日 (**[初回確認]** 日) から、修正までにどのくらいの時間を要していますか?	過去 90 日	ライセンスのある資産	このウィジェットは、各 VPR カテゴリの脆弱性が最初に検出されてから修正されるまでにかかった平均時間 (日数) を、Tenable のお客様 (Salesforce 業界および全体) と比較してグラフで表示します。 • 特定の VPR カテゴリの平均時間の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。
Average Remediation Time Since Publication プラグインが最初に利用可能となった日 (**[プラグイン公開]** 日) から、脆弱性の修正までにどのくらいの時間を要していますか?	過去 90 日	ライセンスのある資産	このウィジェットは、プラグインが最初に利用可能となってから、各 VPR カテゴリの脆弱性が修正されるまでにかかった平均時間 (日数) を、Tenable のお客様 (Salesforce 業界および全体) と比較してグラフで表示します。 • 特定の VPR カテゴリの平均時間の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。

修正範囲グレード どれだけ徹底的に脆弱性を修正していますか?	過去 90 日	ライセンスのある資産	このウィジェットは、企業全体の修正成熟度修正範囲グレードを、Tenable のお客様 (Salesforce 業界および全体)と比較してまとめたものです。 • 自分の修正範囲グレードと、Tenable のお客様 (Salesforce 業界および全体)の修正範囲グレードの平均を比較して視覚的に表示します。 • 最近、修正範囲グレードが増加しているのか減少しているのかについての概要を表示します。
Remediation Coverage どのくらいの割合の脆弱性が修正されていますか?	過去 90 日	ライセンスのある資産	このウィジェットは、各 VPR カテゴリの修正済み (Fixed) の脆弱性の割合を、Tenable のお客様 (Salesforce 業界および全体)と比較してグラフで表示します。 • 特定の VPR カテゴリの割合の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。
Average Vulnerabilities Per Asset 資産に平均でいくつの脆弱性が存在していますか?	過去 90 日	ライセンスのある資産	このウィジェットは、資産に存在する各 VPR カテゴリの脆弱性の数 (Active、Fixed、または Resurfaced) を、Tenable のお客様 (Salesforce 業界および全体)と比較してグラフで表示します。 • 特定の VPR カテゴリでの数の詳細を表

			示するには、グラフ上のポイントにカーソルを合わせます。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。

事業の文脈/タグ資産の詳細を表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

このページを使用して、特定の事業の文脈 tag の付いた資産の詳細を表示できます。

始める前に

- タグの資産への追加の説明に従って、資産にタグを追加します。

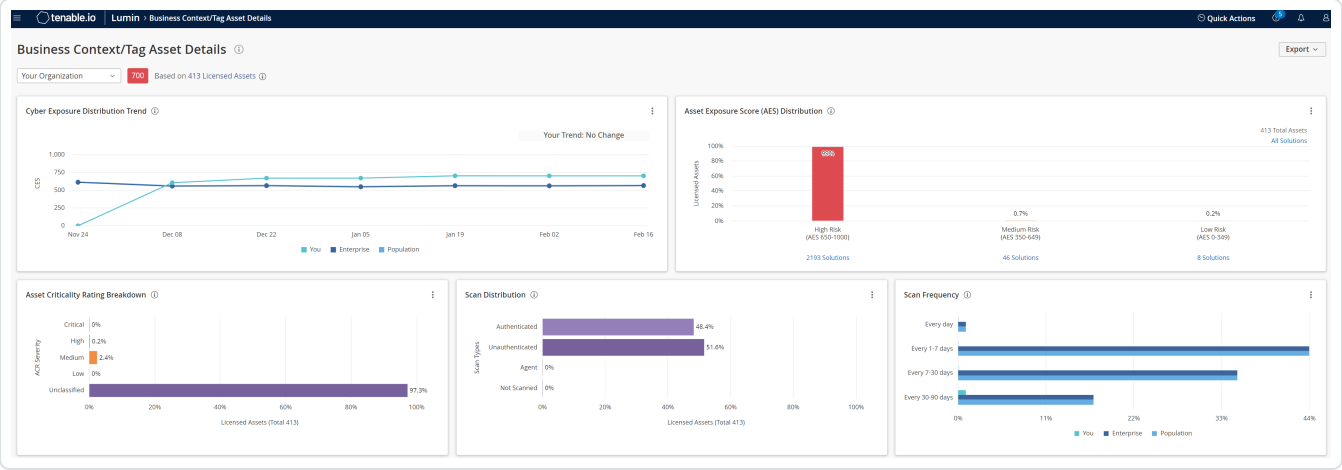
事業の文脈タグ資産の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで、**[事業の文脈]** をクリックします。

   [事業の文脈とタグ資産の詳細] ページが表示されます。



3. (オプション) ページに適用されるタグフィルターを変更するには、左上にあるドロップダウンリストからタグを選択します。

   Tenable Lumin は、ユーザーが選択したタグでページをフィルタリングします。

注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

セクションまたはウィジェット	タイムフレーム	資産	アクション
Tag summary	常時	タグが適用された、ライセンスのある資産とライセンスのない資産	• タグの名前を表示します。 • タグが付いた資産に対して計算した CES を表示します。
Cyber Exposure Score Trend このビジネス文脈の総合的なリスクは、時間とともにどう変化していますか?	過去 90 日間のグラフ上の各ポイント、日ごとに再計算	タグが適用された、ライセンスのある資産	このウィジェットは、自分のタグ別の CES と、Tenable のお客様 (Salesforce 業界および全体)の企業レベルでの CES の平均の増減をグラフで表示します。 **注意:** 新たに追加されたタグが、CES トレンド情報を表示するまでに最大 14 日かかる場合があります。 • 特定の日付の、業界または全体の企業レベルでの CES の値の詳細を表示するには、グラフ上のポイントにカーソルを合わせます。 CES の履歴データが表示されます。 • 特定の日付の、自分のタグ別の CES の値の詳細を表示するには、**You** の線上のポイントをクリックします。 **Tenable Lumin[Cyber Exposure Score]** の詳細のプレーンが表示されます。詳細は、CES の詳細を参照してください。

			• 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボックスをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。
Asset Distribution by Asset Exposure Score (AES) 資産はどのくらい脅威にさらされていますか?	過去 90 日	タグが適用され、アクセスグループを通じて自分のユーザーアカウントに共有された、ライセンスのある資産	このウィジェットには、各 AES カテゴリ毎の脆弱性数がまとめられています。 • AES カテゴリの推奨ソリューションを表示するには、**[<*Category*> AES のソリューション]** リンクの 1 つをクリックします。 タグ、ライセンスのある資産、および選択した AES カテゴリでフィルタリングされた状態で、**[ソリューション]** ページが表示されます。詳細は、ソリューションを表示する を参照してください。 • すべての資産に対する推奨ソリューションを表示するには、**[すべてのソリューション]** リンクをクリックしてください。 タグおよびライセンスのある資産でフィルタリングされた状態で、**[ソリューション]** ページが表示されます。詳細は、ソリューションを表示する を参照してください。
Asset Criticality Rating Breakdown	過去 90 日	タグが適用された、ライセンスの	このウィジェットでは、各 ACRカテゴリにおける資産の割合が表示されます。

資産はどれだけ重要ですか?		ある資産とライセンスのない資産	• ネットワークのスキャンされた資産の合計数を表示します。 • 資産の割合は次のカテゴリ別に表示されます。**Critical**、**High**、**Medium**、**Low**、**Unclassified** • 資産のリストを表示するには、グラフでカテゴリをクリックします。 タグ、過去 90 日間のライセンスのある資産、および選択した ACR カテゴリでフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。
資産のスキャンの分類 どのくらいの割合の資産が、異なる方法でスキャンされましたか?	過去 90 日	タグが適用された、ライセンスのある資産とライセンスのない資産	このウィジェットでは、過去 90 日間の資産スキャン分布がまとめられています。 **[認証スキャン]** は認証スキャンが設定された非エージェントスキャナーによって実行されます。**[エージェントスキャン]** はエージェントスキャナーによって実行されます。他のすべてのスキャンは **[非認証スキャン]** です。 • 過去 90 日間にネットワークでスキャンされた資産の合計数を表示します。 • システムが過去 90 日間に、認証スキャン、非認証スキャン、エージェントスキャンを実行した資産の割合を表示します。 • 過去 90 日間にシステムがスキャンしなかった資産の割合を表示し

			ます。 • ウィジェットに表示されているデータにフィルターを適用するには、ウィジェットにカーソルを合わせて ▽ ボタンをクリックします。必要なフィルターをクリックします。 Tenable Vulnerability Management によってウィジェットが更新されます。 • 資産リストを表示するには、スキャンカテゴリをクリックします。 タグ、過去90日間のライセンスされた資産、選択したスキャンタイプ、そしてウィジェットに適用された ACR カテゴリフィルターでフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。
資産スキャン頻度 どのくらいの頻度で、資産をスキャンしていますか?	過去 90 日	タグが適用された、ライセンスのある資産とライセンスのない資産	このウィジェットでは、過去 90 日間にネットワークでスキャンされた資産の割合が、Salesforce 業界の他のユーザーや一般ユーザーと比較して表示されます。 • **[日単位]**、**[週単位]**、**[月単位]**、または **[四半期]** の間隔でスキャンされたネットワーク上の資産の割合を表示します。 • 企業、業界、一般ユーザーのデータを表示したり非表示にしたりするには、グラフの凡例のボック

			スをクリックします。 システムはウィジェットを更新して、選択したデータを表示または非表示にします。 • ウィジェットに表示されているデータにフィルターを適用するには、ウィジェットにカーソルを合わせて ▽ ボタンをクリックします。必要なフィルターをクリックします。 Tenable Vulnerability Management によってウィジェットが更新されます。 • 資産リストを表示するには、グラフのバーをクリックします。 タグ、ライセンスされた資産、選択した期間、およびウィジェットに適用された ACR カテゴリフィルターによってフィルタリングされた状態で、**[資産]** ページが表示されます。詳細は、View Assets を参照してください。

Tenable Lumin で軽減策 の詳細を表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[基本的なネットワークスキャン] テンプレートまたは **[高度なネットワークスキャン]** テンプレートに基づく認証スキャンを実行する場合、もしくは **[基本的なエージェントスキャン]** または **[高度なエージェントスキャン]** テンプレートに基づくエージェントスキャンを実行する場合、Tenable は資産に存在する緩和策の検出に必要なプラグインを自動的に有効にします。Tenable Lumin は、緩和策をエンドポイント保護エージェント、これにはアンチウイルスソフトウェア、エンドポイント保護プラットフォーム (EPP)、またはエンドポイント検知・対応 (EDR) ソリューションが含まれます。として定義します。

次に、Tenable Lumin 軽減策 データを使用して、資産がエンドポイント保護エージェントソフトウェアで適切にカバーされているかどうかを評価することができます。

資産で エンドポイント保護エージェント を検出するには、認証スキャンやエージェントスキャンで特定のプラグインを有効にする必要があります。詳細は、資産検出のためのプラグイン を参照してください。

始める前に

- スキャンで必要なプラグインを有効にします。
- [**軽減策**] ページをチェックする前にスキャンを実行します。

資産のエンドポイント保護エージェントのリストを表示する方法

1. 左上にある ☰ ボタンをクリックします。

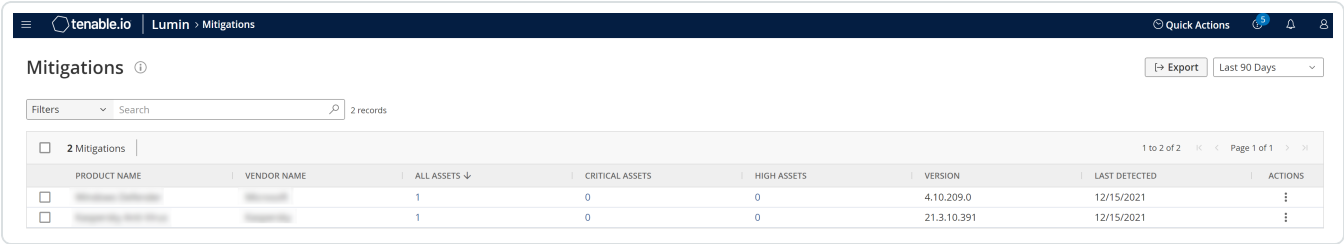
   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[Lumin]** をクリックします。

   Lumin ダッシュボードが表示されます。

3. **[緩和]** ウィジェットで、**[詳細]** をクリックします。

Tenable Lumin **[緩和]** ページ が表 示されます。



注意: すべての Tenable Lumin データは、企 業の Tenable Vulnerability Management インスタンス内のすべての資 産を反 映します。

セクション	アクション
Exports button	以 前に生 成したエクスポートファイルをダウンロードします。
Date range selector	緩 和策の表の日 付範囲を変 更します。詳 細は、Tenable Vulnerability Management の表 を参 照してください。
[フィルター] ボックス	緩 和策の表に表 示されるデータをフィルタリングします。
[検 索] ボックス	緩 和策の表を製 品名で検 索します。詳 細は、Tenable Vulnerability Management の表 を参 照してください。
Mitigations table	この表で次の操 作を行うことができます。 • 各エンドポイント保 護エージェントについての情 報を表 示します。 ◦ **[製 品名]** - エンドポイント保 護エージェント の名 前 ◦ **[ベンダー名]** - エンドポイント保 護エージェント を保 守しているベンダーの名 前 ◦ **[すべての資 産]** - エンドポイント保 護エージェント が存 在する資 産の総 数 ◦ **[重 大な資 産]** - エンドポイント保 護エージェント が存 在する**重 要** ACR の資 産の総 数

	◦ **[高の資産]** - エンドポイント保護エージェント が存在する**高** ACR の資産の総数 ◦ **[バージョン]** - エンドポイント保護エージェント のバージョン ◦ **[最終検出]** - スキャンが資産上で最後にエンドポイント保護エージェント を検出した日付 • 並べ替え、ページ当たりの行数の増減、または表の別のページへ移動します。詳細は、Tenable Vulnerability Management の表 を参照してください。 • 緩和策をエクスポートします。 • 特定のエンドポイント保護エージェントが存在する資産のリストを表示するには、次の適切な列で資産カウントをクリックします。 • **[すべての資産]** は資産の ACR に関係なくすべての資産を表示します。 • **[重大な資産]** は ACR が**[重大]** の資産を表示します。 • **[高の資産]** は、ACR が**[高]** の資産を表示します。 **[資産]** ページが表示され、ライセンスのある資産、ACR 深刻度、緩和策製品名、緩和策ベンダー名、緩和策のバージョン、過去 90 日間でフィルタリングされます。詳細は、View Assets を参照してください。

資産検出のためのプラグイン

緩和策を検出するには、スキャンで次のプラグインを有効にする必要があります。

ヒント: Tenable Vulnerability Management により、これらのプラグインは次の Tenable が提供するスキャンテンプレートを自動的に有効にします。**[高度なネットワークスキャン]**、**[基本的なネットワークスキャン]**、**[高度なエージェントスキャン]**、**[基本的なエージェントスキャン]**。

ID	名前
12107	McAfee Antivirus Detection and Status
16192	Trend Micro Antivirus Detection and Status
20283	Panda Antivirus Detection and Status
20284	Kaspersky Anti-Virus Detection and Status
21162	Spybot Search & Destroy Detection
21608	NOD32 Antivirus Detection and Status
21725	Symantec Antivirus Software Detection and Status
21726	Webroot SpySweeper Enterprise Detection
24232	BitDefender Antivirus Detection and Status
52668	F-Secure Anti-Virus Detection and Status
54845	Sophos Anti-Virus for Mac OS X Detection
54846	Sophos Anti-Virus Detection and Status (Mac OS X)
56567	Mac OS X XProtect Detection
56568	Mac OS X XProtect Installed
58580	Trend Micro ServerProtect Detection and Status (credentialed check)
67119	McAfee ePolicy Orchestrator Installed (credentialed check)
68997	Check Point ZoneAlarm Detection and Status

74038	McAfee VirusScan Enterprise for Linux Detection and Status
84432	AVG Internet Security Detection
87777	Avast Antivirus Detection and Status
87923	McAfee Application Control / Change Control Installed
87955	McAfee Agent Detection
87989	McAfee Agent Detection (Linux/MacOS)
88598	Symantec Endpoint Protection Installed (Unix Credentialed Check)
95470	McAfee Host Intrusion Prevention Installed
100131	McAfee Security Scan Plus Detection
106757	CylancePROTECT Detection
106758	CylancePROTECT Detection (Mac OS X)
112279	Windows Defender Advanced Threat Protection Installed (Windows)
124366	McAfee Endpoint Security and Module Detection
131023	Windows Defender Installed
131725	Sophos Anti-Virus Installed (Windows)
133843	VMware Carbon Black Cloud Endpoint Standard Installed (Windows)
133962	Sophos Anti-Virus Installed (Linux)
134216	VMware Carbon Black Cloud Endpoint Standard Installed (macOS)
134871	Trend Micro Apex One Server Installed (Windows)
135408	Trend Micro Deep Security Agent Installed (Linux)
135409	Trend Micro Deep Security Agent Installed (Windows)
136760	BitDefender Endpoint Security Tools Status (Windows)
136761	BitDefender Endpoint Security Tools Detection (Windows)

138209	Symantec Critical System Protection/Data Center Security Agent (Windows)
138853	F-Secure PSB Computer Protection (Windows)
139913	Check Point Endpoint Security SandBlast Agent Installed (Windows)
139918	ClamAV Installed (Linux)
140633	CrowdStrike Falcon Sensor Installed (Windows)
152356	Cybereason Endpoint Agent Installed (Windows)

Export 軽減策

必要な追加ライセンス: Tenable Lumin

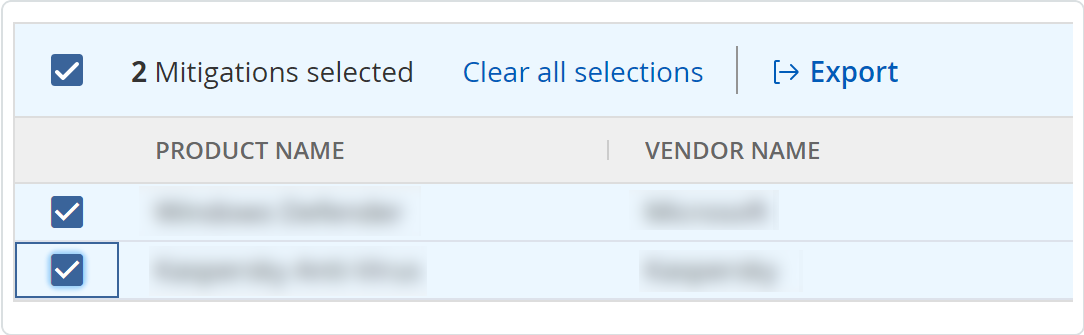
必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要に応じて、緩和策と影響を受けている資産をエクスポートして、企業内の他の人とデータを共有できます。

緩和策と影響を受けている資産をエクスポートする方法

1. 企業の緩和策の詳細を表示します。
2. 緩和策の表で、エクスポートファイルに含める緩和策の横にあるチェックボックスを選択します。

   表の上部にアクションバーが表示されます。



3. アクションバーで、[→ **[エクスポート]** をクリックします。

   Tenable Lumin 緩和策の **[エクスポート]** プレーンが表示されます。
4. **[種類]** セクションで、実行するエクスポートのタイプをクリックします。
   - **CSV - 軽減策** - 選択した緩和策を含む 1 つの .csv ファイル。
   - **CSV - 軽減策 & Assets Affected** - 選択した緩和策とその緩和策が存在する場所で影響を受けている資産を含む、2 つの .csv ファイル。

   エクスポートが開始され、Tenable Vulnerability Management がエクスポートファイルを tar.gz パッケージでダウンロードします。エクスポートファイルのデータに関する詳細は、「緩和策エクスポートファイルの内容」を参照してください。

次の手順

- 過去にエクスポートした緩和策データをダウンロードするには、エクスポートされた緩和策を表示およびダウンロードするを参照してください。

緩和策エクスポートファイルの内容

[軽減策]ページから緩和索をエクスポートすることができます。エクスポートファイルには次のデータが含まれています。

エクスポートフィールド	説明
`mitigations_summary.csv` - **[緩和]**ファイル	
product_name	エンドポイント保護エージェント の名前
vendor_name	エンドポイント保護エージェント を保守しているベンダーの名前
all_assets	エンドポイント保護エージェント が存在する資産の総数
critical_assets	エンドポイント保護エージェント が存在する**重要** ACR の資産の総数
high_assets	エンドポイント保護エージェント が存在する**高** ACR の資産の総数
version	エンドポイント保護エージェント のバージョン
last_detected	スキャンが資産上で最後にエンドポイント保護エージェント を検出した日付
`mitigations_detail.csv` - **[影響を受けた資産]**ファイル	
product_name	エンドポイント保護エージェント の名前
vendor_name	エンドポイント保護エージェント を保守しているベンダーの名前
version	エンドポイント保護エージェント のバージョン
last_detected	スキャンが資産上で最後にエンドポイント保護エージェント を検出した日付
asset_uuid	資産の UUID。
hostname	資産のホスト名。
ipv4	資産の IPv4 アドレス。
operating_system	資産のオペレーティングシステム
acr_score	資産の ACR。

acr_severity	資産に対して計算された ACR の ACR カテゴリ。
aes_score	資産の AES です。
aes_severity	資産に対して計算された AES の AES カテゴリ。

エクスポートされた緩和策を表示およびダウンロードする

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

緩和策や影響を受けた資産のファイルをエクスポートすると、それらの表示やダウンロードが可能になります。他のユーザーが作成したエクスポートファイルは、表示もダウンロードもできません。

始める前に

- 緩和策や影響を受けている資産のファイルをエクスポートします。

緩和策や影響を受けている資産のエクスポートファイルを表示してダウンロードする方法

1. 企業の緩和策の詳細を表示します。
2. ページ右上にある [→ **[エクスポート]** をクリックします。

   Tenable Lumin 緩和策の **[エクスポート]** プレーンが表示されます。
3. エクスポートの表で、ダウンロードするエクスポートの行をクリックします。

   Tenable Vulnerability Management では、エクスポートファイルを `tar.gz` パッケージでダウンロードします。エクスポートファイルのデータに関する詳細は、緩和策エクスポートファイルの内容を参照してください。

推奨アクションを表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable は、アクセスグループのアクセス許可に関わらず、ネットワーク上の資産に対する上位の推奨アクション(ソリューション)のリストを提供します。ソリューションを特定し、その詳細を掘り下げてネットワークの脆弱性に対処する手順を理解することができます。

推奨される上位のアクションを生成する目的で、Tenable Lumin は、すべてのライセンス資産を修正した場合に CES に特に大きな影響を与えるプラグインを検索します。プラグインに関連性がある場合、1 つの修正が他のプラグインに影響を与えることがあります。

ネットワークの脆弱性に対処することで、CES メトリクスおよび AESメトリクスを下げることができます。

ネットワーク上のすべての資産に対する上位の推奨ソリューションを表示する方法

1. 左上にある ☰ ボタンをクリックします。

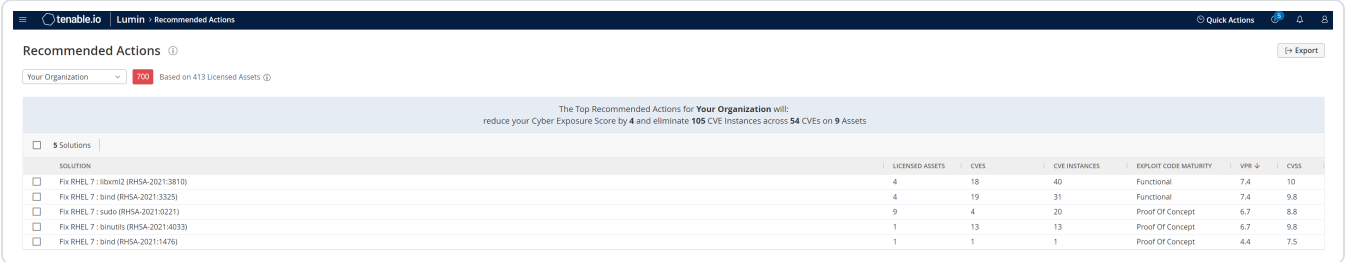
   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[Lumin]** をクリックします。

   Lumin ダッシュボードが表示されます。

3. **[CES を削減するためのアクション]** ウィジェットで、**[上位の推奨アクションを参照]** をクリックします。

   Tenable Lumin **[推奨アクション]** ページが表示されます。表には上位のソリューション(最大 20 位)が、まず VPR カテゴリ順 (**[Critical]** から **[Low]**) で、次に **[影響を受ける資産]** の降順で並べられます。



4. (オプション) ページに適用されるタグフィルターを変更するには、左上にあるドロップダウンリストからタグを選択します。

   Tenable Lumin は、ユーザーが選択したタグでページをフィルタリングします。

セクション	アクション
Summary bar	**[推奨されるアクション]** 表内のすべてのソリューションを解決した場合の、予想される影響に関する統計情報の概要を表示します。 • 上位のソリューションをすべて解決した場合に予想される CES の減少量。 • 上位のソリューションにより除去される脆弱性インスタンスの数 **ヒント：**脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。 • 上位のソリューションにより影響を受ける資産の数。

推奨アクションの表	• 各ソリューションの情報を表示します。
	  • **Solution** - ソリューションの説明
	  • **ライセンスのある資産** - ソリューションによって対処される脆弱性により影響を受けている資産の総数。
	  • **CVE** - ソリューションによって対処された個別の Common Vulnerabilities and Exposures (CVE) の数。
	  • **CVE インスタンス** - ソリューションによって対処された、重複を含む Common Vulnerabilities and Exposures (CVE) の総数。
	  • **Exploit Code Maturity** - ソリューションが対処する脆弱性の最大の VPR に対する、主な要因値
	  • **VPR** - ソリューションが対応している脆弱性の最大の VPR
	  • **CVSS** - ソリューションが対応している脆弱性の最大 CVSSv2 スコア (または使用可能な場合は CVSSv3 スコア)。
	• ソリューションの詳細を表示するには、ソリューションの行をクリックします。
	[ソリューションの詳細] ページが表示されます。詳細は、ソリューションの詳細を表示する を参照してください。

	• ソリューションのデータをエクスポートするには、推奨アクションをエクスポートするを参照してください。

推奨アクションをエクスポートする

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要に応じて、推奨されるアクション(ソリューション)と影響を受けている資産をエクスポートして、企業内の他の人とデータを共有できます。

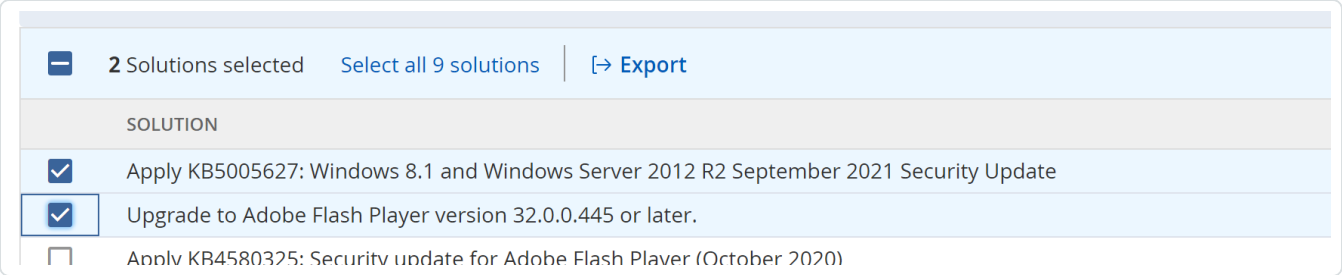
推奨アクションや影響を受けている資産をエクスポートする方法

1. 推奨アクションを表示するの記載内容に従って、Tenable Lumin **[推奨アクション]** ページに移動します。

   Tenable Lumin **[推奨アクション]** ページ が表示されます。

2. 表で、エクスポートファイルに含める推奨アクションの横にあるチェックボックスを選択します。

   表の上部にアクションバーが表示されます。



3. アクションバーで、[→ **[エクスポート]** をクリックします。

   [エクスポート] プレーンが表示されます。

4. **[CSV]** セクションで、エクスポートする推奨アクションデータのチェックボックスを選択します。

   - **ソリューション** - 選択した推奨アクションを含む .csv ファイル。このチェックボックスはデフォルトで選択されています。
   - **詳細** - 選択した推奨アクションとそれらのソリューションに関する追加の詳細を含む .csv ファイル。

エクスポートが開始され、Tenable Vulnerability Management がエクスポートファイルを tar.gz パッケージでダウンロードします。エクスポートファイルのデータに関する詳細は、推奨アクションのエクスポートファイルの内容を参照してください。

推奨アクションのエクスポートファイルの内容

推奨アクション(ソリューション)は、2 種類の推奨アクションのページからエクスポートすることができます。各ページからエクスポートされる内容は、そのページ固有のものになります。

資産グループに対する推奨アクションのエクスポート

資産グループに対する **[推奨されるアクション]** ページから、推奨アクションと影響を受けている資産のファイルをエクスポートする場合、エクスポートファイルには次のデータが含まれます。

エクスポートフィールド	説明
`detail.csv` - **Assets Affected** ファイル	
solution_id	ソリューションの UUID
solution_title	ソリューションの説明
asset_uuid	資産の UUID。
hostname	資産のホスト名。
ipv4	資産の IPv4 アドレス。
operating_system	資産のオペレーティングシステム
cve_count	ソリューションによって対処される、この資産の脆弱性の数
cve_instance_count	ソリューションによって対処される、この資産の脆弱性インスタンスの総数。 **ヒント**:脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。
`solution.csv` - **選択されたアクション** ファイル	
solution_id	ソリューションの UUID
solution_title	ソリューションの説明
assets_	ソリューションによって対処される脆弱性により影響を受けている資産の総数。

affected	
cve_count	ソリューションた対応している脆弱性の総数
vpr	ソリューションが対応している脆弱性の最大の VPR
cvss	ソリューションが対応している脆弱性の最大 CVSSv2 スコア(または使用可能な場合は CVSSv3 スコア)。

すべての資産に対する推奨アクションのエクスポート

すべての資産に対する **[推奨アクション]** ページから、推奨アクションと影響を受けている資産のファイルをエクスポートする場合、エクスポートファイルには次のデータが含まれます。

エクスポートフィールド	説明
`detail.csv` - **Assets Affected** ファイル	
solution_id	ソリューションの UUID
solution_title	ソリューションの説明
asset_uuid	資産の UUID。
hostname	資産のホスト名。
ipv4	資産の IPv4 アドレス。
operating_system	資産のオペレーティングシステム
acr_score	資産の ACR。
acr_severity	資産に対して計算された ACR の ACR カテゴリ。
aes_score	資産の AES です。
aes_severity	資産に対して計算された AES の AES カテゴリ。
vuln_count	ソリューションによって対処される、この資産の脆弱性の数
vuln_instance_	ソリューションによって対処される、この資産の脆弱性インスタンスの総数。

count	**ヒント：**脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。
summary.csv - 選択されたアクション ファイル	
solution	ソリューションの UUID
summary	ソリューションの説明
assets_affected	ソリューションによって対処される脆弱性により影響を受けている資産の総数。
vulnerabilities	ソリューションた対応している脆弱性の総数
exploit_code_maturity	ソリューションが対応している脆弱性の最大の VPR に対する、主な要因値
vpr	ソリューションが対応している脆弱性の最大の VPR
cvss	ソリューションが対応している脆弱性の最大 CVSSv2 スコア(または使用可能な場合は CVSSv3 スコア)。

スキャン

Tenable Vulnerability Management では、スキャンを作成、設定、管理できます。

セクション	説明
スキャンを管理する	スキャンを作成、インポート、起動します。スキャンとスキャン結果を表示、管理します。
スキャン (統一設定) の概要	Tenable Vulnerability Management の統一されたユーザーインターフェースで Tenable Vulnerability Management および Tenable Web App Scanning のスキャンを作成、起動、管理します。
スキャンテンプレートと設定	Tenable が提供するスキャナーテンプレート、エージェントテンプレート、およびユーザー定義のテンプレートを使用して、スキャン設定を設定します。
センサー	Tenable Nessus スキャナー、Tenable Nessus Agents、および Tenable Nessus Network Monitor などのセンサーを Tenable Vulnerability Management にリンクします。

注意: Tenable Web App Scanning でのスキャンの詳細については、Tenable Web App Scanning スタートアップガイドを参照してください。

注意: Tenable Container Security でのスキャンの詳細については、Tenable Container Security Scanner スキャンの概要を参照してください。

スキャンを管理する

統一された **[スキャン]** ユーザーインターフェースで Tenable Vulnerability Management および Tenable Web App Scanning のスキャンを管理するには、スキャンの概要を参照してください。

Tenable Web App Scanning で Tenable Web App Scanning スキャンを管理するには、Tenable Web App Scanning スタートガイド参照してください。

スキャンの概要

[スキャン] ページでは Tenable Vulnerability Management スキャンと Tenable Web App Scanning スキャンを作成、起動、および設定できます。

[スキャン] のワークフローと手順の多くは、レガシーの **[脆弱性管理]** > **[スキャン]** ページおよび **[Web App Scanning]** > **[スキャン]** ページの手順と似ていますが、ここでは新しいスキャンユーザーインターフェースに合わせてヘルプトピックを更新しました。

スキャンの作成

Tenable Vulnerability Management で、スキャンテンプレートを使用してスキャンを作成できます。テンプレートに関する一般的な情報については、Scan Templates and Settingsを参照してください。

スキャンを作成すると、Tenable Vulnerability Management はあなたにそのスキャンに対する所有者のアクセス許可を割り当てます。

ヒント: 以前のスキャン時に資産で識別された特定の脆弱性を素早くターゲットにするには、Tenable Vulnerability Management 修正スキャンを作成します。

注意: Tenable Vulnerability Management のダッシュボード、レポート、ワークベンチから、**PCI 四半期外部**スキャンデータが意図的に除外されています。これは、スキャンが事細かく検出する設定になっているためです。この設定の場合、Tenable Vulnerability Management が本来検出しないはずのものを誤検出してしまいます。詳細は、Tenable PCI ASV Scans を参照してください。

始める前に

- (オプション) Tenable Vulnerability Management のスキャン制限事項を確認します。
- ユーザー定義テンプレートからスキャンを作成する場合は、Create a User-Defined Template の説明に従ってユーザー定義テンプレートを作成します。
- スキャンで使用する任意のターゲットのアクセスグループを作成し、適切なユーザーに**[スキャン可]**アクセス許可を割り当てます。

スキャンを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]**で、**[脆弱性管理スキャン]**か**[ウェブアプリケーションスキャン]**の表示を選択します。

   またこれにより、Tenable Vulnerability Management スキャンと Tenable Web App Scanning スキャンのどちらを作成するかが決定されます。

4. ページの右上にある [→] **[スキャンを作成する]** ボタンをクリックします。

   [スキャンテンプレートの選択] ページが表示されます。

5. 次のいずれかを行います。

   - Tenable Vulnerability Management スキャンを作成する場合は、次の手順を使用します。

     a. **[Nessus スキャナー]**、**[Nessus Agent]**、**[ユーザー定義]** タブのいずれかをクリックし、スキャンに使用できるテンプレートを表示します。

     タブが表示されます。

     > **注意:** [スキャンオペレーター] のアクセス許可を持つユーザーは、自分のアカウントと共有されているユーザー定義テンプレートのみを表示および使用できます。

     b. スキャンに使用するテンプレートのタイルをクリックします。

     [スキャンの作成] ページが表示されます。

     c. スキャンを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定を行います。 • 基本設定 - スキャンテンプレートの組織的な要素とセキュリティ関連の要素を指定できます。これには、スキャンの名前、ターゲット、スキャンをスケジュールするかどうか、スキャンのアクセス許可を持つユーザーの指定が含まれます。 • Discovery 設定 - スキャンが検出とポートスキャンを実行する方法を指定します。 • 評価設定 - 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指定します。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。

	• Report 設定 - スキャンがレポートを生成するかどうかを指定します。 • 詳細設定 - スキャン効率のための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
Compliance/SCAP	監査する必要のあるプラットフォームを指定します。Tenable, Inc. は各プラットフォームの監査のベストプラクティスを提供しています。また、カスタムの監査ファイルをアップロードすることもできます。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

d. 次のいずれかを行います。

- スキャンを起動せずに保存する場合は、**[保存]** をクリックします。

  Tenable Vulnerability Management がスキャンを保存します。

- 今すぐスキャンを保存して起動する場合は、**[保存して起動]** をクリックします。

  > **注意:** スキャンを後で実行するようにスケジュールした場合は、**[保存して起動]** オプションは利用できません。

  Tenable Vulnerability Management がスキャンを保存して起動します。

- Tenable Web App Scanning スキャンを作成する場合は、次の手順を使用します。

a. **[ウェブアプリケーション]** タブまたは **[ユーザー定義]** タブをクリックし、スキャンに使用できるテンプレートを表示します。

タブが表示されます。

> **注意:** [スキャンオペレーター] のアクセス許可を持つユーザーは、自分のアカウントと共有されているユーザー定義テンプレートのみを表示および使用できます。

b. スキャンに使用するテンプレートのタイルをクリックします。

[スキャンの作成] ページが表示されます。

c. スキャンを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定をします。詳細は、Tenable Web App Scanning スキャンの基本設定 を参照してください。
範囲	スキャンに含めるまたはスキャンから除外する URL とファイルタイプを指定します。詳細は、Tenable Web App Scanning スキャンの範囲設定 を参照してください。
資産	スキャンによる脆弱性の識別方法と、識別対象の脆弱性を指定します。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。詳細は、Tenable Web App Scanning スキャンの評価設定 を参照してください。
詳細	スキャン効率を高めるための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

d. 次のいずれかを行います。

- スキャンを起動せずに保存する場合は、**[保存]** をクリックします。

  Tenable Vulnerability Management がスキャンを保存します。

- 今すぐスキャンを保存して起動する場合は、**[保存して起動]** をクリックします。

  > **注意:** スキャンを後で実行するようにスケジュールした場合は、**[保存して起動]** オプションは利用できません。

  Tenable Vulnerability Management がスキャンを保存して起動します。

スキャンの表示

必要なスキャンのアクセス許可: 表示可

Tenable Vulnerability Management は、35 日間が経過したそれぞれのスキャン結果を **Archived** と定義します。35 日以内のスキャン結果については、Tenable Vulnerability Management で結果を表示してエクスポートすることができます。アーカイブされたスキャン結果については、結果をエクスポートすることは可能ですが、Tenable Vulnerability Management で表示することはできません。この制限は、インポートされたスキャン結果、および Tenable Vulnerability Management がスキャナーから直接集めたスキャン結果の両方に適用されます。15 か月を経過すると、Tenable Vulnerability Management はスキャンデータを完全に消去します。

設定されたスキャンとインポートされたスキャンを表示することができます。適切なアクセス許可があれば、スキャンの管理も実行できます。

始める前に

- 1 つ以上のスキャンを作成またはインポートします。

[スキャン] セクションでスキャンを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

   スキャンフォルダーについての詳細は、Scan Folders を参照してください。

5. 次のうちのいずれかを行います。

セクション	アクション
検索ボック	スキャン名またはステータスで表を検索します。詳細は、Tenable Vulnerability

ス	Management の表 を参照してください。
[フィルター]	Tenable 提供のスキャンフィルターで表をフィルタリングします。
[スキャンの作成] ボタン	右上の ⊕ **[スキャンの作成]** ボタンをクリックして、新しいスキャンを作成します。
[ツール] ボタン	右上にある **[ツール]** ボタンをクリックします。以下のオプションを含むメニューが表示されます。 • スキャンのインポート (Tenable Vulnerability Management スキャンのみ) • センサーの管理 • 認証情報の管理 • 除外の管理

スキャンの表	• 各スキャンについての概要情報を表示します。
	  • **Name** - スキャン名
	  他のユーザーに割り当てられたスキャンのアクセス許可がある場合は、スキャン名の横に **[共有]** ラベルが表示されます。
	  • **スケジュール** - スキャンのスケジュール
	  • **最終変更日** - (Tenable Web App Scanning スキャンのみ) スキャンが最後に変更された日時。
	  • **最終実行日** - スキャンが最後に実行された日時。
	  • **ステータス** - スキャンのステータス
	• 並べ替え、ページ当たりの行数の増減、または表の別のページへ移動します。詳細は、Tenable Vulnerability Management の表 を参照してください。
	• スキャンの詳細を表示します。
	• スキャンを起動します。

	スキャンの確認ステータスを • 変更します。 スキャン結果を • エクスポートします。 スキャンをゴミ箱に • 移動します。 スキャンを完全に • 削除します。 • スキャンを別のフォルダーに移動します。

スキャンの詳細の表示

必要なスキャンのアクセス許可: 表示可

所有しているスキャンと共有されているスキャンのスキャン結果を表示できます。スキャン結果を表示するときは、次のことを考慮してください。

- 個別のスキャンの詳細は、スキャンに対して設定されたアクセス許可に基づいて表示することができます。ただし、集計したスキャン結果をダッシュボードなどの分析ビュー(**脆弱性**や**資産**の表など)で表示する場合、ユーザーのアクセスは、所属するアクセスグループに基づきます。
- Tenable Vulnerability Management は、35 日間が経過したそれぞれのスキャン結果を **Archived** と定義します。35 日以内のスキャン結果については、Tenable Vulnerability Management で結果を表示してエクスポートすることができます。アーカイブされたスキャン結果については、結果をエクスポートすることは可能ですが、Tenable Vulnerability Management で表示することはできません。この制限は、インポートされたスキャン結果、および Tenable Vulnerability Management がスキャナーから直接集めたスキャン結果の両方に適用されます。15 か月を経過すると、Tenable Vulnerability Management はスキャンデータを完全に消去します。
- 最後に実行したスキャンの結果を表示すると、Tenable Vulnerability Management はそのスキャンを **[読み取り]** に分類します。**[読み取り]** のステータスは、ユーザーアカウント固有のものです。[読み取り] ステータスを手動で変更することも可能です。
- Tenable Vulnerability Management はスキャンデータを 15 か月間保持します。スキャンデータを 15 か月以上保存する場合は、そのスキャンデータを Tenable Vulnerability Management 以外にエクスポートすると保存できます。

個別のスキャンのスキャン詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

5. スキャンの表で、詳細を表示するスキャンをクリックします。

   スキャンの表の下に、スキャンの詳細プレーンが表示されます。デフォルトで、このプレーンにはスキャンの直近の実行に関する詳細が表示されます。

6. 次のいずれかを行えます。

セクション	アクション
[**Scan Actions**] メニュー	• スキャンを起動します。 スキャンの設定を • 編集します。 スキャン結果を • エクスポートします。 スキャンを別のフォルダーに • 移動します。 スキャンの確認ステータスを • 変更します。 スキャンを完全に • 削除します。 スキャンを • コピーします。 スキャンをゴミ箱に • 移動します。
[すべての詳細の表示] ボタン	**[すべての詳細の表示]** ボタンをクリックして、**[スキャンの詳細]** ページを開き、スキャンの脆弱性と影響を受けている資産、ターゲット情報、スキャン履歴を表示します。**[スキャンの詳細]** ページを使用して、スキャンをエクスポートしたり、スキャン設定を編集したり、スキャンをゴミ箱フォルダーに移動したり、PCI 検証のためにスキャンを送信したりすることもできます。

	スキャンの詳細ページには、次の機能と情報が含まれています。 ### 表のヘッダー - (ロールオーバースキャンのみ) ロールオーバースキャンの残りのターゲットのリストをダウンロードします。 - 現在表示されているスキャン結果をエクスポートします。 - スキャン設定を編集する。 - スキャンを [ゴミ箱] フォルダーに移動します。 ### 深刻度の概要 スキャン結果の深刻度が **Critical**、**High**、**Medium**、**Low** の脆弱性の数。 ### [Scan Details] セクション スキャン実行の詳細を表示します。 - **Status** - スキャンのステータス - **Start Time** - スキャンの開始日時 - **Template** - スキャン設定の基盤となる、Tenable が提供するテンプレート - **スキャナー** - スキャンを実行するスキャナー - **スキャナーグループ** - Tenable Vulnerability Management がスキャンを割り当てたスキャナーグループ (1 つまたは複数) この詳細は、スキャンに対してスキャンのルーティングが有効になっている場合のみ表示されます。 - **Targets** - スキャンが評価するターゲット

[プラグイン別の脆弱性] タブ

スキャン結果の脆弱性をプラグイン別に表示します。

> **注意:** 35 日より前のスキャン結果では、このタブは表示されません。

- 各脆弱性に関する情報を表示します。
  - Severity アイコン - 脆弱性の深刻度
  - **Name** - 脆弱性を特定したプラグインの名前。
  - **ファミリー** - 脆弱性を特定したプラグインのファミリー。
  - **インスタンス** - 脆弱性インスタンスの数。

    > **ヒント:** 脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。
- 表に表示されるデータをフィルタリングするには、表のフィルタリングを参照してください。
- 並べ替え、ページ当たりの行数の増減、または表の別のページへの移動を行うには、Tenable Vulnerability Management の表を参照してください。
- 脆弱性の詳細を表示するには、表の行をクリックします。

  [脆弱性の詳細] ページが表示されます。詳細は、脆弱性の詳細を参照してください。

[監査] タブ

	コンプライアンス監査チェックの結果を表示します。コンプライアンス監査チェックのデータがスキャン結果に含まれる場合のみ、このタブが表示されます。 **ヒント:** 35 日以上経過しているスキャン結果にこのタブは表示されません。 このタブでは、次を表示することができます。 • 最後のスキャン完了時に特定された監査チェックの数を表すタイルを、深刻度レベル別に整理して表示します。 • スキャン中に検出された監査の表を表示します。各行は特定の監査を表しており、次の情報が含まれています。 ◦ **Status** - 監査のステータス (**Passed**、**Warning**、または **Failed** など) ◦ **Name** - コンプライアンスチェックの名前 ◦ **Family** - 対象の監査が属しているコンプライアンスチェックファミリー ◦ **カウント** - 監査が特定された回数 • 特定の監査チェックについての追加情報を表示するには、監査の表の行をクリックします。 **[監査の詳細]** ページが表示されます。 • **概要** - チェックの説明およびチェックに使用された監査ファイルを含む、監査チェックについての情報です。 • **資産** - スキャンで監査チェックが行われた資産のリストです。

[サマリー] タブ

	(ルールベースのスキャンのみ) スキャンの説明、トリガー、ルールベーススキャンの説明、脆弱性ワークベンチへのリンクを表示します。
	
	[資産別の脆弱性]タブ
	
	スキャン結果の脆弱性を資産別に表示します。デフォルトでは、表内にある資産は、脆弱性件数の降順、次に脆弱性深刻度の降順の優先度で並べ替えられています。
	
	ヒント: 35 日以上経過しているスキャン結果にこのタブは表示されません。
	
	• 各脆弱性に関する情報を表示します。
	  • **資産** - 資産の識別子 Tenable Vulnerability Management はこの識別子に、特定の資産属性が存在するかに応じて、次の優先順位に基づいて資産属性を割り当てます。
	  ◦ エージェント名 (エージェントスキャンの場合)
	  ◦ NetBIOS 名
	  ◦ FQDN
	  ◦ IPv4 アドレス
	  たとえば、スキャンによって、ある資産に対して NetBIOS 名と IPv4 アドレスが特定された場合、NetBIOS 名が資産名として表示されます。
	  • **脆弱性** - 資産の脆弱性に関する視覚的な要約。深刻度別に整理されて表示されます。
	  • **脆弱性数** - 資産の脆弱性の合計数。

	• **重大** - 深刻度が重大な資産の脆弱性の総数 • **高** - 深刻度が高の資産の脆弱性の総数 • **監査** - 脆弱性に関する監査の視覚的な要約。深刻度別に整理されて表示されます。 • **監査数** - 資産に対する監査の総数 • 表に表示されるデータをフィルタリングするには、表のフィルタリングを参照してください。 • 並べ替え、ページ当たりの行数の増減、または表の別のページへの移動を行うには、Tenable Vulnerability Management の表を参照してください。 • 資産の詳細を表示するには、表の行をクリックします。 **[資産の詳細]** ページが表示されます。詳細は、View Legacy Workbench Asset Details を参照してください。 **[警告]** タブ スキャン実行中に発生した Tenable Vulnerability Management またはスキャナーの問題に関する警告を表示します。このタブは、スキャン実行中に Tenable Vulnerability Management またはスキャナーで問題が発生した場合にのみ表示されます。 スキャンの警告を確認して、スキャンの問題を解決する方法を決定します。たとえば、**[無効なターゲット]** の注記がある場合は、スキャンの設定のターゲットパラメーターを確認します。

ヒント: 35 日以上経過しているスキャン結果にこのタブは表示されません。

[修正] タブ

修正についての詳細を表示します。

注意: **[修正]** タブは、そのスキャンでの既知の修正策がある場合のみ表示されます。

このタブには修正のためのアクションを一覧表示した表が含まれます。このタブでは、次を表示することができます。

- **脆弱性** - 推薦された修正方法で解決された脆弱性の数
- **資産** - スキャンされた資産数

[履歴] タブ

スキャンの履歴を表示します。

このタブには、毎回の実行されたスキャンが記載された表が含まれます。現在 **[スキャンの詳細]** ページに表示されているスキャンの実行に対して、Tenable Vulnerability Management により **[最新]** というラベルが追加されます。デフォルトで、最も最近実行されたスキャンに **[最新]** ラベルが追加されます。

注意: スキャンの履歴は、インポートされたスキャン、まだ実行されていない設定済みスキャン、およびトリガーされたスキャンでは利用できません。

注意: トリガーされたスキャン履歴については、Tenable Vulnerability Management では過去 7 日間の 12 時間ごとのスキャン履歴エントリが表示されます。Tenable Vulnerability Management は各スキャンで一度に最大 15 件のトリガーされたスキャン履歴のみを保持します。

	このタブでは、次のことを実行できます。 • 実行されたスキャンの各回についての概要情報を表示します。 • **Start Time** - スキャンの開始日時 • **End Time** - スキャンの終了日時 • **Duration** - スキャンの継続時間 • **Status** - スキャンのステータス 表に表示されるデータを • フィルタリングします。 • 並べ替え、ページ当たりの行数の増減、または表の別のページへ移動します。詳細は、Tenable Vulnerability Management の表 を参照してください。 • 表の行をクリックすることで、過去のスキャンの詳細を表示します。 Tenable Vulnerability Managementは選択された実行に**[最新]**とマーキングし、**[スキャンの詳細]**セクションを更新して選択された実行のデータを表示します。 過去のスキャン結果が35日以内のものであれば、Tenable Vulnerability Management は**[スキャンの詳細]**ページのタブも更新します。 過去のスキャン結果が35日より以前のものであれば、**[スキャンの詳細]**ページから追加のタブは無くなります。代わりにエクスポートを使用して、結果を入手してください。
[アクティビティ] セクション	スキャンのアクティビティの履歴。

	このセクションでは、スキャンが**開始**、**完了**した日時と、スキャンが**変更**、**キャンセル**、または手動で**中止**された日時を表示できます。
[深刻度別の脆弱性/VPR の内訳] セクション	スキャン結果にある **[重大]**、**[高]**、**[中]**、**[低]** の深刻度の脆弱性の数。
[スキャン時間] セクション	スキャンの開始と終了の間の経過時間。
[ターゲット] セクション	スキャンされたターゲットの数。
[タイプ] セクション	スキャンのタイプ。
[テンプレート] セクション	使用されたスキャンテンプレート。
[スケジュール] セクション	スキャンのスケジュール

スキャン脆弱性の詳細の表示

[スキャン] セクションから、プラグイン別または資産別 (Tenable Vulnerability Management スキャンのみ) にスキャン結果の脆弱性の詳細を表示できます。

[スキャン] セクションからスキャン結果の脆弱性の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** の下で、**[脆弱性管理スキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

5. スキャンの表で、詳細を表示するスキャンをクリックします。

   スキャンの表の下に、スキャンの詳細プレーンが表示されます。デフォルトで、このプレーンにはスキャンの最後の実行に関する詳細が表示されます。

6. スキャンの詳細プレーンで、**[詳細をすべて表示]** ボタンをクリックします。

   [スキャンの詳細] ページが表示されます。デフォルトで、**[プラグイン別の脆弱性]** タブが表示されます。

7. 影響を受けた資産別に脆弱性を表示する場合は、**[プラグイン別の脆弱性]** タブをクリックします。

   資産別の脆弱性の表が表示されます。

8. **[プラグイン別の脆弱性]** タブまたは **[資産別の脆弱性]** タブで、次のいずれかを実行します。

   - プラグインの表を脆弱性の属性でフィルタリングします。
   - プラグインの表を検索します。
   - **[検索]** ボックスの横にある、プラグインの検索結果の数を表示します。

- **[プラグイン別の脆弱性]**タブで、脆弱性をクリックしてその詳細を表示します。詳細は、View Vulnerability Details を参照してください。
- **[資産別の脆弱性]**タブで、資産行をクリックして脆弱性の詳細を表示します。詳細は、View Legacy Workbench Asset Details を参照してください。

スキャンフィルター

[スキャン] ページでは、Tenable が提供するフィルターを使ってスキャンをフィルタリングすることができます。Tenable Vulnerability Managementスキャンのビューでは、スキャンステータス別にフィルタリングできます。また、Tenable Web App Scanning スキャンのビューでは複数の値を基準にフィルタリングできます。

フィルター	説明
ステータス	スキャンのステータスです。スキャンステータスに関する詳細は、スキャンステータス を参照してください。
作成日 (Tenable Web App Scanning スキャンのみ)	スキャン設定が作成された日付です。
説明 (Tenable Web App Scanning スキャンのみ)	スキャン設定の説明です。
完了日 (Tenable Web App Scanning スキャンのみ)	スキャンが最後に完了した日付です。
最終変更日 (Tenable Web App Scanning スキャンのみ)	スキャン設定が最後に変更された日付です。
最終実行日 (Tenable Web App Scanning スキャンのみ)	スキャンが最後に実行された日付です。
名前 (Tenable Web App Scanning スキャンのみ)	スキャン設定の名前です。
スケジュール(Tenable Web App Scanning スキャンのみ)	スキャンスケジュールが有効かオンデマンドかでフィルタリングします。
ターゲット (Tenable Web App Scanning スキャンのみ)	スキャンの起動に使用されるターゲット URL です。
テンプレート (Tenable Web App Scanning スキャンのみ)	スキャン設定のベースとなった Tenable 提供のスキャンテンプレートです。
ユーザーテンプレート (Tenable Web App Scanning スキャンのみ)	スキャン設定のベースとなったユーザー定義スキャンテンプレートです。

Tenable Vulnerability Management スキャンの起動

スケジュールした時間に起動するようにスキャンの[スケジュール]を設定するほか、手動でスキャンを起動することもできます。新しいスキャンを起動できるのは、前回のスキャンのステータスが**[完了]**、**[中止]**、または**[キャンセル]**である場合のみです(詳細は、スキャンステータスを参照してください)。

標準スキャンを手動で起動するには、スキャンの起動を参照してください。または、*ロールオーバースキャン*を起動して、途中で終了した前回のスキャンの残りのターゲットをスキャンすることもできます(詳細は、ロールオーバースキャンを起動するを参照してください)。最後に、*修正スキャン*を起動して、既存のスキャン結果に対してフォローアップスキャンを実行します(詳細は、修正スキャンの起動を参照してください)。

注意: Tenable Vulnerability Management のスキャンの制限については、スキャン制限事項を参照してください。

スキャンの起動

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なスキャンのアクセス許可: 制御可

次の手順を使用して、スキャンを手動で起動します。スキャンに設定されているターゲットを使用してスキャンを開始できます。または、設定されたターゲットをオーバーライドするカスタムターゲットを使用してスキャンを開始することもできます。

スキャンを起動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

   スキャンフォルダーについての詳細は、Scan Foldersを参照してください。

5. スキャンの表で、起動するスキャンにカーソルを合わせます。

   アクションボタンが行に表示されます。

6. 次のいずれかを行います。

   - スキャン内で設定されたターゲットを使用してスキャンを開始するには、行の上で ▷ ボタンをクリックします。
   - 以前にスキャンを起動し、設定されたターゲットにオーバーライドされるカスタムターゲットを使用したい場合には、次を行います。

a. 行の上で ボタンをクリックします。

[カスタム起動スキャン] プレーンが開きます。

b. **[ターゲット]** ボックスに、ターゲットのコンマ区切り文字列を入力します。

c. **[起動]** をクリックします。

Tenable Vulnerability Management がスキャンを起動します。

[スキャン] ページでスキャンステータスをチェックすることにより、スキャンの進行状況を確認できます。

ロールオーバースキャンを起動する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なスキャンのアクセス許可: 制御可

ロールオーバースキャンを起動すると、以前に Tenable Vulnerability Management でスキャンされなかったターゲットとホストに対してのみスキャンが実行されます。これは、割り当てられたすべてのターゲットを調べる前にスキャンが終了したときに発生します。次のような場合です。

- ユーザーがスキャンを手動で停止した時
- スキャン期間の設定により、スキャンがタイムアウトした時
- スキャナーがスキャンタスクを中止するか、適切に初期化しなかった時

場合によっては、ロールオーバースキャンを実行できる対象として **完了済み**スキャンが表示されることがあります。これは、割り当てられたすべてのターゲットがスキャンされたものの、一部のスキャンタスクが失敗した可能性があることを示しています。

繰り越しスキャンにより、すべての資産を完全にカバーするスキャンを達成でき、ネットワークに影響を与える大規模なスキャンを、ロールオーバー機能を使用して分割実行できます。**[スキャン]** ページからロールオーバースキャンを起動できます。Tenable Vulnerability Management は、スキャン表にあるロールオーバースキャンを起動できるスキャンの **[名前]** 列に **[ロールオーバー]** タグでマークを付けます。

ロールオーバースキャンが実行される残りのターゲットを表示するには、Download Rollover Targetsを参照してください。スキャンを再起動してすべてのターゲットを再スキャンする場合は、スキャンの起動を参照してください。

注意: ロールオーバーウェブアプリケーションスキャンを起動することはできません。

ロールオーバースキャンを起動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。
4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

   スキャンフォルダーについての詳細は、Scan Foldersを参照してください。
5. スキャンの表で、起動するスキャンにカーソルを合わせます。
6. 行にある ⋮ ボタンをクリックします。

   メニューが表示されます。
7. **[ロールオーバーを起動]** オプションをクリックします。

   Tenable Vulnerability Management がロールオーバースキャンを起動します。

   [スキャン] ページでスキャンステータスをチェックすることにより、スキャンの進行状況を確認できます。

修正スキャンの起動

必要な Tenable Vulnerability Management ユーザーロール: 標準、スキャンマネージャー、または管理者

必要なアクセスグループのアクセス許可: スキャン可

既存のスキャン結果に対するフォローアップスキャンを実行するための修正スキャンを作成することができます。修正スキャンは、以前のアクティブなスキャンで脆弱性が存在した特定のスキャンターゲットに対して特定のプラグインを評価します。

修正スキャンを使用して、スキャンターゲット上の脆弱性の修正アクションが成功したかどうかを検証することができます。以前に脆弱性が特定されたターゲット上の脆弱性を修正スキャンで特定できない場合、システムはその脆弱性のステータスを **[修正済み]** に変更します。

スキャン結果の修正スキャンは、次の特定のセンサーからのみ実行できます。

センサータイプ	サポート対象
Tenable Vulnerability Management クラウドセンサー	○
オンプレミス Tenable Nessus	○
Amazon Web Services (AWS) 向け Tenable Nessus スキャナー	○
Tenable Web App Scanning	×
Tenable Nessus Network Monitor	×
Tenable Nessus Agent	×

注意: Tenable Vulnerability Management のスキャンの制限については、スキャン制限事項を参照してください。

修正スキャンを起動する方法

1. 修正スキャンの範囲を設定します。

修正スキャンの範囲	アクション
脆弱性を有するすべての資産で検出	この範囲はサポートされていません。
脆弱性を有する個別の資産で検出	この範囲を設定する方法 a. 資産の詳細を表示します。 b. **[資産の詳細]** ページで、**[脆弱性]** タブをクリックします。 **[脆弱性]** タブが表示されます。 c. 右上の **[アクション]** ボタンをクリックします。 アクションメニューが表示されます。 d. アクションメニューで、**[修正スキャンの起動]** をクリックします。
複数の資産のすべての脆弱性	この範囲はサポートされていません。
影響を受ける上位 500 の資産の個別の脆弱性	この範囲を設定する方法 a. 脆弱性の詳細を表示します。 b. **[影響を受ける資産]** タブをクリックします。 資産の表が表示されます。 c. 右上の **[アクション]** ボタンをクリックします。 アクションメニューが表示されます。 d. **[修正スキャンの起動]** をクリックします。
個別の資産の個別の脆弱性	この範囲を設定する方法 a. 脆弱性の詳細を表示します。

	b. **[影響を受ける資産]** タブをクリックします。 資産の表が表示されます。 c. 資産の表で、選択する資産のチェックボックスを選択します。 ページの下部またはに、アクションバーが表示されます。 d. アクションバーで、 **[修正スキャンの起動]** をクリックします。
複数の資産の個別の脆弱性	この範囲を設定する方法 a. 脆弱性の詳細を表示します。 b. **[影響を受ける資産]** タブをクリックします。 資産の表が表示されます。 c. 資産の表で、選択する各資産の横にあるチェックボックスを選択します。 ページの下部またはに、アクションバーが表示されます。 d. アクションバーで、 **[修正スキャンの起動]** をクリックします。
影響を受けるすべての資産の複数の脆弱性	この範囲はサポートされていません。
個別の資産の複数の脆弱性	この範囲を設定する方法 a. 資産の詳細を表示します。 b. **[資産の詳細]** ページで、**[脆弱性]** タブをクリックします。 **[脆弱性]** タブが表示されます。 c. 脆弱性の表で、選択する各脆弱性の横にあるチェックボックスを選択します。

	ページの下部またはに、アクションバーが表示されます。 d. アクションバーで、**[修正スキャンの起動]**をクリックします。
複数の脆弱性を複数の資産で検出	この範囲はサポートされていません。
個別の検出結果	この範囲を設定する方法 a. ホストの脆弱性の検出結果またはウェブアプリケーションの脆弱性の検出結果の詳細を表示します。 b. **[検出結果の詳細]**ページの右上にある**[アクション]**ボタンをクリックします。 アクションメニューが表示されます。 c. アクションメニューで、**[修正スキャンの起動]**をクリックします。

[スキャンの作成 - 修正スキャン]が表示されます。

Tenable Vulnerability Management は、Tenable 提供の[高度なネットワークスキャン]テンプレートから自動的に修正スキャンを作成し、選択された資産と脆弱性を基にして特定の設定を入力します。

2. **[スキャンの作成]**ページで次の操作を実行します。

   a. 選択した脆弱性と資産を基にして Tenable Vulnerability Management によって入力された設定を確認します。

   b. スキャンの追加の設定を設定します。

   実行する必要がある手動による変更の数は、修正スキャンに含まれているプラグインによって異なります。

次の表に、修正スキャンの設定の継承される値とデフォルト値の定義を示します。

設定カテゴリ	設定	修正スキャンの値

基本	名前	「Remediation scan of plugin # *number*」の形式で修正可能なスキャン名を指定します。「*number*」は、脆弱性を特定したプラグインの番号です。
	フォルダー	設定できません。修正スキャンは、**[修正スキャン]** フォルダーにのみ表示されます。
	スキャナー	スキャンを実行するスキャナーを指定します。 選択するスキャナーは、修正スキャンに含まれているターゲットの場所に応じて異なります。例 • デフォルトでは、この値は地域のクラウドスキャナーになります(たとえば、**US クラウドスキャナー**)。ただし、クラウドスキャナーは、ルーティングできない IP アドレスをスキャンできません。スキャンターゲットにルーティングできない IP アドレスが含まれている場合は、代わりに[リンクされたスキャナー]を選択してください。 • 次の場合は、スキャナーグループを選択してください。 ◦ 複数のスキャナーの間でスキャンの負荷を分散し、スキャンスピードを上げる場合 ◦ スキャン設定でスキャナーの指定を更新する必要なしに、将来スキャナーを再構築して新しいスキャナーをリンクする場合
	ネットワーク	(スキャナーが **[自動選択]** に設定されている場合に必要)次のいずれかの操作を実行します。 • スキャンが重複する IP 範囲を持つ別々の環境に関係する場合、スキャンのルーティング用に設定したスキャナーグループを含むネットワークを選択します。 • スキャンが重複する IP 範囲を持つ別々の環境に関係しない

		場合は、**[デフォルト]** ネットワークのままにします。
	ターゲット	修正スキャンで選択した資産を基にしてスキャンターゲットを指定します。
	ユーザーアクセス許可	[高度なネットワークスキャン] テンプレートのデフォルト設定を指定します。 デフォルトでは、修正スキャンの個別のスキャン結果にのみアクセスできます。**[デフォルト]** ユーザーアクセス許可は **[アクセスなし]** に設定されます。修正スキャンを他のユーザーと共有する場合は、[ユーザーアクセス許可] を設定します。
	スケジュール	設定できません。修正スキャンを作成した時に起動しない場合は、スキャンを後で手動で起動することができます。
	その他すべての設定	[高度なネットワークスキャン] テンプレートのデフォルト設定を指定します。
検出	すべて	[高度なネットワークスキャン] テンプレートのデフォルト設定を指定します。 **注意:** デフォルトの **[ポートスキャン範囲]** は、共通ポートのみをスキャンします。修正スキャンで使用されているプラグインに特定のポートが必要な場合は、それらのポートが含まれる範囲に対してこの設定をします。
資産	すべて	[高度なネットワークスキャン] テンプレートのデフォルト設定を指定します。
レポート	すべて	[高度なネットワークスキャン] テンプレートのデフォルト設定を指定します。
詳細	すべて	[高度なネットワークスキャン] テンプレートのデフォルト設定を指定します。
認証情報	すべて	デフォルトでは、認証情報は設定されません。修正スキャンのプラグインに認証情報が必要な場合は、修正スキャンでそれらを設定しま

		す。 **注意:** 修正スキャンは認証情報のないネットワークスキャン結果に対して最適に動作します。スキャン認証情報を必要とするプラグインに対して修正スキャンを実行するときには注意してください。特定のプラグインに必要なスキャン認証情報を追加し忘れた場合、または認証情報を誤って入力した場合、システムは関連する脆弱性を修正済みとして特定する場合があります。事実、システムは認証スキャンを完了できないため、脆弱性はスキャン結果に表示されません。
コンプライアンス	すべて	デフォルトでは、コンプライアンス監査は設定されません。認証スキャンのプラグインにコンプライアンス監査の設定が必要な場合は、適切な設定を設定してください。
プラグイン	制限あり	以下に制限されるプラグインを指定します。 • 修正スキャン用に選択されたプラグイン • 選択したプラグインが依存している任意のプラグイン

3. 次のいずれかを行います。

   - スキャンを起動せずに保存する場合は、**[保存]** をクリックします。

     Tenable Vulnerability Management がスキャンを保存します。

   - 今すぐスキャンを保存して起動する場合は、**[保存して起動]** をクリックします。

     注意: スキャンを後で実行するようにスケジュールした場合は、**[保存して起動]** オプションは利用できません。

     Tenable Vulnerability Management がスキャンを保存して起動します。

次の手順

- **[スキャン]** ページの **[修正スキャン]** フォルダーで次の操作を実行します。
  スキャンステータスを

  ◦ 表示して、スキャンが完了したタイミングを特定します。

- スキャン設定を編集する。
  スキャン結果の読み取りステータスを
- 変更します。
- スキャンを起動します。

- スキャンが完了したら次の操作を実行します

  a. **[脆弱性]** ページで、プラグインを検索します。

  b. 修正スキャンのターゲットとなった資産上で選択した脆弱性のステータスが **[修正済み]** になったことを確認します。

実行中のスキャンの停止

必要なスキャンのアクセス許可: 制御可

スキャンを停止すると、Tenable Vulnerability Management 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。停止したスキャンに関連するスキャン結果には、完了済みのタスクのみが反映されます。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。

実行中のスキャンを停止する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. スキャンの表で、停止するスキャンにカーソルを合わせます。

4. 行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

5. **[停止]** をクリックします。

   確認ウィンドウが表示されます。

6. 確認ウィンドウで、**[停止]** をクリックします。

   Tenable Vulnerability Management によりスキャンが停止されます。**[ステータス]** 列が更新され、スキャンのステータスが反映されます。

スキャンの一時停止または再開

必要なスキャンのアクセス許可: 制御可

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 Vulnerability Management はそのスキャンのすべてのアクティブなタスクを一時停止し、スキャナーのローカルスキャンタスクを終了します。一時停止されたスキャンではスキャナーリソースは消費されず、一時停止したスキャンが存在する間は他のスキャンを実行することができます。Tenable Vulnerability Management により一時停止されたスキャンジョブから新規タスクがディスパッチされることはありません。スキャンが 14 日を超えて一時停止状態になると、スキャンはタイムアウトします。Tenable Vulnerability Management はスキャナー上の関連タスクを終了させ、スキャンを中断済みに分類します。

一時停止したスキャンは再開できます。スキャンを再開すると、Tenable Vulnerability Management はスキャンが一時停止した場所からタスクを開始するようスキャナーに指示します。スキャンの再開時に Tenable Vulnerability Managementが問題を発見した場合には、スキャンは失敗し、Tenable Vulnerability Management はスキャンを中断済みに分類します。Tenable Vulnerability Management により一時停止されたスキャンジョブから新規タスクがディスパッチされることはありません。スキャンが 14 日を超えて一時停止状態になると、スキャンはタイムアウトします。Tenable Vulnerability Management はスキャナー上の関連タスクを終了させ、スキャンを中断済みに分類します。

注意: 一時停止して再開できるのは、Tenable Vulnerability Management スキャンのみです。

スキャンを一時停止または再開する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. スキャンの表で、スキャンにカーソルを合わせます。

4. 次のいずれかを行います。

   - スキャンを一時停止するには、行の上の ⏸ ボタンをクリックします。
   - スキャンを再開するには、行の上の ▷ 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。

5. 確認ウィンドウで、それぞれの場合に応じて**[一時停止]**または**[再開]**をクリックします。

   Tenable Vulnerability Management により、スキャンが一時停止または再開されます。

スキャンの所有権の変更

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要なスキャンのアクセス許可: 所有者

始める前に

- スキャンがユーザー定義テンプレートに基づいている場合、そのテンプレートで新しい所有者に最低でも**[表示可]**アクセス許可を割り当ててください。そうしないと、新しい所有者はスキャン設定を表示できません。

注意: スキャンの所有者のみがスキャンの所有権を変更できます。従って、管理者が別のユーザーのスキャン所有者を変更する必要がある場合は、まずそのユーザーのアカウントについて適切に対応してから、適切なユーザーに所有権を割り当てる必要があります。

新しいインターフェースでスキャンの所有権を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]**で、**[脆弱性管理スキャン]**か**[ウェブアプリケーションスキャン]**の表示を選択します。

4. **[フォルダー]**セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

5. (オプション) 編集するスキャンを検索します。詳細は、Tenable Vulnerability Management の表を参照してください。

6. スキャンの表で、編集するスキャンをクリックします。

   スキャンの詳細が表示されます。

7. スキャン名の横にある ボタンをクリックします。

   [スキャンの編集] ページが表示されます。

8. 左側のナビゲーションメニューの **[設定]** セクションで、**[基本]** をクリックします。

   [基本] 設定が表示されます。

9. **[ユーザーアクセス許可]** セクションの、**[所有者]** 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。

   利用可能なユーザーアカウントのリストが表示されます。

10. リストからユーザーを選択します。

    Tenable Vulnerability Management により自動的にユーザーのリストに追加され、自分のユーザーアカウントに **[表示可]** アクセス許可が付与されます。

11. (オプション) ユーザーアカウントのすべてのアクセス許可を削除するには

    a. ユーザーリストで、自分のユーザーアカウントにカーソルを合わせます。

       リストの最後に ボタンが表示されます。

    b. ボタンをクリックします。

       Tenable Vulnerability Management により、ユーザーのリストからアカウントが削除されます。

12. (オプション) ユーザーアカウントの Tenable Vulnerability Management アクセス許可を編集する方法

    a. ユーザーアカウント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. アクセス許可を選択します。

13. **[保存]** をクリックします。

    Tenable Vulnerability Management により選択されたユーザーに所有権が割り当てられ、自分のユーザーアカウントに選択したアクセス許可が割り当てられます。スキャンから自分のユーザーアカウントのすべてのアクセス許可を削除すると、そのスキャンは自分のスキャンフォルダーのいずれにも表示されなくなります。

スキャンの確認ステータスの変更

必要なスキャンのアクセス許可: 表示可

[スキャン] ページでは、直近のスキャンの実行結果が未表示 (確認) なスキャンは、スキャンの表内に太字で表示されます。

スキャンの結果を表示すると、Tenable Vulnerability Management はスキャンを「確認済み」に分類し、スキャンの表内でそのスキャンの太字フォーマットを削除します。

スキャンの確認ステータスを手動で変更することも可能です。

スキャンの確認ステータスを変更する方法

1. スキャンを表示します。
2. スキャンの表で、変更するスキャンにカーソルを合わせます。
3. ⋮ ボタンをクリックします。

   メニューが表示されます。
4. 次のいずれかを行います。
   - スキャンを既に確認している場合は、✉ **[未確認にする]** をクリックします。
   - スキャンを確認していない場合は、✉ **[確認済みにする]** をクリックします。

   Tenable Vulnerability Management がスキャンの確認ステータスを変更します。

スキャン設定を編集する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なスキャンのアクセス許可: 設定可

スキャン設定を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

5. (オプション) 編集するスキャンを検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

6. スキャンの表で、編集するスキャンをクリックします。

   スキャンの詳細が表示されます。

7. スキャン名の横にある ✎ ボタンをクリックします。

   [スキャンの編集] ページが表示されます。

8. スキャンの設定を変更します。スキャン設定の詳細については、スキャンの設定 を参照してください。

9. 次のいずれかを行います。

   - スキャンを起動せずに保存する場合は、**[保存]** をクリックします。

     Tenable Vulnerability Management がスキャンを保存します。

- 今すぐスキャンを保存して起動する場合は、**[保存して起動]**をクリックします。

  注意: スキャンを後で実行するようにスケジュールした場合は、**[保存して起動]**オプションは利用できません。

  Tenable Vulnerability Management がスキャンを保存して起動します。

vSphere スキャンの設定

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

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

シナリオ 1: vCenter が管理しない ESXi/vSphere のスキャン

vCenter が管理しない ESXi/vSphere スキャンを設定する方法

1. 高度なネットワーク Tenable Vulnerability Management スキャンを作成します。
2. 左側のナビゲーションメニューの **[設定]** セクションで、**[基本]** をクリックします。

   [基本] 設定が表示されます。
3. **[ターゲット]** セクションに ESXi ホストの IP アドレスを入力します。
4. 左側のナビゲーションメニューで、**[認証情報]** タブをクリックします。

   [認証情報] ページが表示されます。このページには、スキャン用に設定されている認証情報の表が含まれます。
5. **[認証情報の追加]** の横にある ⊕ ボタンをクリックします。

   [認証情報タイプの選択] プレーンが表示されます。
6. **[その他]** セクションで **[VMware ESX SOAP API]** を選択します。
7. **[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。
8. **[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。
9. vCenter ホストに SSL 証明書 (自己署名証明書ではない) が含まれている場合は、**[SSL 証明書を検証しない]** トグルを無効にします。それ以外の場合は、トグルを有効のままにします。

10. **[保存]**をクリックします。
11. 次のいずれかを行います。
    - スキャンを起動せずに保存する場合は、**[保存]**をクリックします。

      Tenable Vulnerability Management がスキャンを保存します。
    - 今すぐスキャンを保存して起動する場合は、**[保存して起動]**をクリックします。

      > **注意:** スキャンを後で実行するようにスケジュールした場合は、**[保存して起動]**オプションは利用できません。

      Tenable Vulnerability Management がスキャンを保存して起動します。

> **注意:** vCenter が管理する ESXi で認証情報を使用してスキャンする場合、Nessus スキャン情報プラグインは、vCenter のスキャン結果に必ず [Credentialed Checks: No] (認証チェック: なし) と表示します。認証が成功したことを確認するには、Nessus スキャン情報プラグインの ESXi のスキャン結果に [認証情報を使用したチェック: はい] と表示されていることを確認します。

シナリオ 2 : vCenter が管理する ESXI/vSphere のスキャン

vCenter が管理する ESXi/vSphere スキャンを設定する方法

1. 高度なネットワーク Tenable Vulnerability Management スキャンを作成します。
2. 左側のナビゲーションメニューの**[設定]**セクションで、**[基本]**をクリックします。

   [基本]設定が表示されます。
3. **[ターゲット]**セクションに以下の IP アドレスを入力します。
   - vCenter ホスト
   - ESXi ホスト
4. 左側のナビゲーションメニューで、**[認証情報]**タブをクリックします。

   [認証情報]ページが表示されます。このページには、スキャン用に設定されている認証情報の表が含まれます。
5. **[認証情報の追加]**の横にある ⊕ ボタンをクリックします。

   [認証情報タイプの選択]プレーンが表示されます。

6. **[その他]** セクションで **[VMware vCenter SOAP API]** を選択します。
7. **[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。
8. **[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。
9. **[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。
10. **[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。
11. 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。
12. vCenter ホストに SSL 証明書 (自己署名証明書ではない) が含まれている場合は、**[SSL 証明書を検証する]** トグルを無効にします。それ以外の場合は、トグルを無効のままにします。
13. **[保存]** をクリックします。
14. 次のいずれかを行います。
    - スキャンを起動せずに保存する場合は、**[保存]** をクリックします。

      Tenable Vulnerability Management がスキャンを保存します。
    - 今すぐスキャンを保存して起動する場合は、**[保存して起動]** をクリックします。

      > **注意:** スキャンを後で実行するようにスケジュールした場合は、**[保存して起動]** オプションは利用できません。

      Tenable Vulnerability Management がスキャンを保存して起動します。

セクション 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。**[ターゲット]** テキストボックスに仮想マシンの IP アドレスが必ず含まれるようにしてください。詳細は、スキャンの作成を参照してください。

スキャン設定のコピー

必要なスキャンのアクセス許可: 所有者

スキャン設定をコピーすると、Tenable Vulnerability Management は、コピーの作成者に所有者としてのアクセス許可を割り当て、コピーには元のスキャンのスキャンアクセス許可を割り当てます。

注意: [修正スキャン] フォルダーからスキャンをコピーすることはできません。

スキャン設定をコピーする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

5. スキャンの表で、コピーするスキャンにカーソルを合わせます。

6. 行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

7. **[コピー]** をクリックします。

   [フォルダへのコピー] プレーンが表示されます。ここにはスキャンフォルダーのリストが含まれます。

8. コピーを保存するフォルダーをクリックします。

9. **[コピー]** をクリックします。

   Tenable Vulnerability Management は、スキャンのコピーを作成し、その名前の先頭に*コピー*を付けます。そして、そのコピーの作成者に所有者のアクセス許可を与えます。選択したフォルダーのコピーがスキャンの表に表示されます。

スキャン結果のエクスポート

必要なスキャンのアクセス許可: 表示可

インポートされたスキャン結果、および Tenable Vulnerability Management がスキャナーから直接集めた結果の両方をエクスポートすることができます。

Tenable Vulnerability Management は、個別のスキャン結果を 15 か月が経過するまで保持します。

注意: フィルターは Tenable Web App Scanning のエクスポートには適用できません。すべての結果がエクスポートされます。

注意: アーカイブされたスキャン結果 (すなわち、45 日よりも前の結果) の場合、Tenable Vulnerability Management により、エクスポートタイプが `.nessus` ファイルと `.csv` ファイルに制限されます。

注意: スキャンがアクティブに実行中の場合、Tenable Vulnerability Management インターフェースに **[エクスポート]** ボタンは表示されません。スキャンが完了するのを待ってから、スキャン結果をエクスポートしてください。

個別のスキャン結果をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

5. 次のいずれかを行います。

場所	エクスポートの範囲
スキャンの表	a. スキャンの表で、エクスポートするスキャンにカーソルを合わせます。 b. ⋮ ボタンをクリックします。 メニューが表示されます。 c. ↦**[エクスポート]**をクリックします。 **[エクスポート]**プレーンが表示されます。 **注意:** スキャンに複数のターゲットがある場合、スキャンの表からスキャン結果をエクスポートできません。複数のターゲットがあるスキャンの場合、**[スキャンの詳細]**ページから各ターゲットのスキャン結果をエクスポートできます。
スキャンの詳細	a. スキャンの表で、エクスポートするスキャンをクリックします。 スキャンの表の下に、スキャンの詳細プレーンが表示されます。 b. **[スキャンアクション]**ボタンをクリックします。 メニューが表示されます。 c. ↦**[エクスポート]**をクリックします。 **[エクスポート]**プレーンが表示されます。

6. エクスポート形式を選択します。

形式	説明	アーカイブされたスキャン結果に対応
Tenable Vulnerability Management スキャン		
PDF - カスタム	Adobe `.pdf` ファイルです。	×

	注意: Tenable Vulnerability Management では、40 万件を超える個別のスキャン結果を含む PDF ファイルはエクスポートできません。	
PDF - Executive Summary	Adobe `.pdf` ファイルです。 **注意:** Tenable Vulnerability Management では、40 万件を超える個別のスキャン結果を含む PDF ファイルはエクスポートできません。	×
HTML - カスタム	Web ベースの `.html` ファイルです。	×
HTML - Executive Summary	Web ベースの `.html` ファイルです。	×
Nessus	XML フォーマットの `.nessus` ファイル。ターゲットのリスト、ユーザーが定義したスキャンの設定、およびスキャン結果が含まれます。Tenable Vulnerability Management がパスワード認証情報を除去するので、パスワードが XML にプレーンテキストとしてエクスポートされることはありません。`.nessus` ファイルをユーザー定義のスキャンテンプレート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。	○
CSV	スキャン結果のみを含む `.csv` テキストファイル **注意:** スキャン結果を `.csv` ファイルとしてエクスポートする場合、深刻度はユーザーが設定した深刻度メトリクスにかかわらず、常に CVSSv2 スコアで表示されます。コンプライアンススキャン結果を `.csv` ファイルとしてエクスポートする場合、**[リスク]** 列の結果は次の値に置き換えられます。 • `PASSED` の結果が [なし] と表示される • `WARNING` の結果が [中] と表示される • `FAILED` の結果が [高] と表示される	○
Tenable Web App Scanning スキャン		

HTML	ターゲット、スキャン結果、スキャンの注記のリストを含むウェブベースの `.html` ファイル。	該当なし
PDF	ターゲット、スキャン結果、スキャンの注記のリストを含む Adobe `.pdf` ファイル。 **注意:** Tenable Vulnerability Management では、40 万件を超える個別のスキャン結果を含む PDF ファイルはエクスポートできません。	該当なし
Nessus	XML フォーマットの `.nessus` ファイル。ターゲットのリスト、ユーザーが定義したスキャンの設定、およびスキャン結果が含まれます。Tenable Vulnerability Management がパスワード認証情報を除去するので、パスワードが XML にプレーンテキストとしてエクスポートされることはありません。	該当なし
CSV	スキャン結果のみを含む `.csv` テキストファイル。	該当なし
JSON	ターゲットのリスト、ユーザーが定義したスキャンの設定、スキャン結果が含まれる、`.json` ファイル。Tenable Vulnerability Management がパスワード認証情報を除去するので、パスワードが JSON にプレーンテキストとしてエクスポートされることはありません。	該当なし

7. Tenable Vulnerability Management スキャンでは、**[PDF - カスタム]** または **[HTML - カスタム]** 形式を選択した場合、

   - 既定の **[データ]** 設定を維持します (**[脆弱性]** が選択されています)。
   - エクスポートファイルでスキャン結果をグループ化する方法に応じて、**[グループ化]** リストから **[資産]** または **[プラグイン]** のいずれかを選択します。

8. **[エクスポート]** をクリックします。

   Tenable Vulnerability Management によりエクスポートファイルが作成されます。ブラウザの設定によっては、ブラウザがエクスポートファイルを自動的にコンピューターにダウンロードするか、続行する前にダウンロードの確認を促すメッセージを表示されます。

スキャンのインポート

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

スキャン結果を Tenable Vulnerability Management にインポートできます。15 か月より前に実行したスキャンの結果はインポートできません。

インポートされたスキャンは、常にデフォルトネットワークに属します。詳細は、ネットワークを参照してください。

注意: インポートできるのは、Tenable Vulnerability Management スキャンのみです。

注意: Tenable Vulnerability Management では、4 GB までの大きさのスキャンをインポートできます。

新しいインターフェイスでスキャンをインポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. ページの右上で、**[ツール]** ボタンをクリックします。

   メニューが表示されます。

4. **[スキャンのインポート]** をクリックします。

   ファイルディレクトリが表示されます。

5. 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。

   スキャンファイルが .nessus または .db ファイルの場合、**[インポート]** プレーンが表示されます。

   注意: .nessus ファイル形式については、Nessus File Format (Nessus ファイル形式) を参照してください。

   スキャンファイルが他の種類のファイルの場合、**[スキャンのインポート]** ウィンドウが表示されます。

6. 次のいずれかを行います。

   - スキャンファイルが .nessus または .db ファイルの場合、次を行います。

     a. **[パスワード]** ボックスにパスワードを入力して、Tenable Vulnerability Management がスキャンを表示できるようにします。

     b. (オプション) スキャン結果をダッシュボードに表示するには、**[ダッシュボードに表示しますか?]** チェックボックスを選択します。

     c. **[インポート]** をクリックします。

   - スキャンファイルが他の種類のファイルの場合は、スキャン結果をダッシュボードに表示するかどうかを指定します。

     ◦ ダッシュボードにスキャン結果を表示するには、**[はい]** をクリックします。

     ◦ ダッシュボードにスキャン結果を表示しないようにするには、**[いいえ]** をクリックします。

   注意: **[キャンセル]** をクリックすると、インポートをキャンセルします。

   [スキャン] ページが表示され、インポートしたスキャンが表に表示されます。

   Tenable Vulnerability Managementは、インポートされたスキャン結果の処理を開始します。処理が完了すると、インポートされたデータは個別のスキャン詳細および集計されたデータビュー (ダッシュボードなど) に表示されます。インポートされたファイルのサイズによっては、このプロセスに最大 30 分かかる可能性があります。

   ヒント: 十分と思われる処理時間が経過しても、インポートされたデータが個別のスキャン結果や集計されたデータビューに表示されない場合は、アクセスグループ内でインポートされたターゲットに対する適切なアクセス許可が割り当てられていることを確認してください。

カスタムスキャンフォルダーを作成する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

カスタムスキャンフォルダーは作成者に対してのみ表示され、他のユーザーには共有できません。作成者のみが、スキャンフォルダーの表示、名前の変更、または削除を行うことができます。

スキャンフォルダーを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** の横にある ⊕ ボタンをクリックします。

   フォルダーリストの下部に **[新しいフォルダー]** ボックスが表示されます。

5. **[新しいフォルダー]** ボックスに、フォルダーの名前を入力します。

6. ✓ ボタンをクリックします。

   [フォルダーの追加に成功しました] というメッセージが表示され、新しいフォルダーが **[フォルダー]** セクションに表示されます。

カスタムスキャンフォルダーの名前を変更する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

名前の変更が可能なのは、カスタムスキャンフォルダーのみです。デフォルトのスキャンフォルダーの名前を変更することはできません。

カスタムフォルダーは作成者に対してのみ表示され、他のユーザーには共有できないため、スキャンフォルダーの名前の変更は作成者のユーザーアカウントにのみ影響します。

スキャンフォルダーの名前を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、名前を変更するフォルダーにカーソルを合わせます。

   アクションボタンが行に表示されます。

5. 行にある ✎ ボタンをクリックします。

   編集可能なボックスがフォルダー名を置き換えます。

6. ボックスに、フォルダーの新しい名前を入力します。

7. ✓ ボタンをクリックします。

   Tenable Vulnerability Managementによりフォルダー名が更新され、**[フォルダーの更新に成功しました]** というメッセージが表示されます。

カスタムスキャンフォルダーを削除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

削除できるのは、カスタムスキャンフォルダーのみです。Tenable Vulnerability Management が提供するデフォルトのスキャンフォルダー(**[すべてのスキャン]**、**[マイスキャン]**、および **[ゴミ箱]**) は削除できません。

カスタムフォルダーは作成者に対してのみ表示され、他のユーザーには共有できないため、スキャンフォルダーの削除は作成者のユーザーアカウントにのみ影響します。

スキャンを含むフォルダーを削除すると、そのスキャンは **[ゴミ箱]** フォルダーへと Tenable Vulnerability Management により移動されます。

スキャンフォルダーを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、削除するフォルダーにカーソルを合わせます。

   アクションボタンが行に表示されます。

5. 行にある ✕ 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。

6. **[削除]** をクリックして、アクションを確定します。

   [フォルダーの削除に成功しました] というメッセージが表示され、Tenable Vulnerability Management によりフォルダーが削除されます。

スキャンフォルダーへのスキャンの移動

必要なスキャンのアクセス許可: 表示可

スキャンをデフォルトフォルダーから**[マイスキャン]**デフォルトフォルダー、またはカスタムスキャンフォルダーに移動できます。またスキャンを、カスタムフォルダーから**[マイスキャン]**デフォルトフォルダーに、または別のカスタムフォルダーに移動することもできます。

スキャンを**[すべてのスキャン]**デフォルトフォルダーから移動すると、そのスキャンは選択したフォルダーと**[すべてのスキャン]**フォルダーの両方に表示されます。

スキャンを**[マイスキャン]**デフォルトフォルダーから移動すると、そのスキャンはカスタムフォルダーにのみ表示されます。

スキャンをゴミ箱に移動する方法に関する詳細は、ゴミ箱フォルダーへのスキャンの移動を参照してください。

注意:[修正スキャン]フォルダー内に、およびこのフォルダーの外にスキャンを移動することはできません。

スキャンをスキャンフォルダーに移動する方法

1. 左上にある☰ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]**で、**[脆弱性管理スキャン]**か**[ウェブアプリケーションスキャン]**の表示を選択します。

4. **[フォルダー]**セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

5. スキャンの表で、移動するスキャンにカーソルを合わせます。

6. 行にある⋮ボタンをクリックします。

   メニューが表示されます。

7. メニューで**[移動]**をクリックします。

[フォルダーに移動] プレーンが表示されます。このプレーンにはスキャンフォルダーのリストが含まれます。

8. フォルダーを検索します。

   a. 検索ボックスにフォルダー名を入力します。

   b. 🔍 ボタンをクリックします。

      Tenable Vulnerability Management がリストを制限して、検索に合致するフォルダーのみを表示します。

9. フォルダーのリストで、スキャンを移動するフォルダーをクリックします。

10. **[移動]** をクリックします。

    Tenable Vulnerability Management は選択したフォルダーにスキャンを移動します。

ゴミ箱フォルダーへのスキャンの移動

必要なスキャンのアクセス許可: 表示可

あるユーザーが共有されたスキャンを **[ゴミ箱]** フォルダーに移動すると、Tenable Vulnerability Management はそのユーザーのアカウントのスキャンのみを移動します。そのスキャンへの **[表示可]** またはそれ以上のアクセス許可を持つ他のすべてのユーザーに対しては、スキャンは元のフォルダーに残ります。

[ゴミ箱] フォルダーに移動されたスキャンは、**[ゴミ箱]** のラベルが付いた状態で **[すべてのスキャン]** フォルダーにも表示されます。

注意: スキャンを **[ゴミ箱]** フォルダーに移動した後、**[編集可]** アクセス許可を持つユーザーがスキャンを完全に削除するまで、スキャンは **[ゴミ箱]** フォルダーに残ります。

注意: スケジュールしたスキャンがスキャン所有者の **[ゴミ箱]** フォルダーにある場合は実行されません。

- Tenable Vulnerability Management スキャンのスケジュールの詳細については、スケジュールを参照してください。
- Tenable Web App Scanning スキャンのスケジュールの詳細については、スケジュールを参照してください。

注意: **[修正スキャン]** フォルダーから **[ゴミ箱]** フォルダーにスキャンを移動することはできません。代わりにフォルダー内で、直接修正スキャンを削除します。

1 つまたは複数のスキャンを **[ゴミ箱]** フォルダーに移動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、移動するスキャンを含むフォルダーをクリックします。

   スキャンの表に、選択したフォルダーのスキャンが一覧表示されます。

5. 次のいずれかを行います。

   - 1 つのスキャンを選択する場合

     a. スキャンの表で、移動するスキャンにカーソルを合わせます。

     b. ⋮ ボタンをクリックします。

        メニューが表示されます。

     c. **[ゴミ箱]** をクリックします。

   - 複数のスキャンを選択する場合

     a. スキャンの表で、移動する各スキャンの横にあるチェックボックスを選択します。

        表の上部にアクションバーが表示されます。

     b. アクションバーで、**[ゴミ箱]** をクリックします。

   Tenable Vulnerability Management が 1 つまたは複数の選択したスキャンを **[ゴミ箱]** フォルダーに移動します。

スキャンの削除を削除する

必要なスキャンのアクセス許可: 設定可

スキャンを完全に削除すると、そのスキャンの共有相手であるすべてのユーザーでスキャン設定およびスキャン結果が削除されます。

修正スキャンを削除するためのワークフローは、この手順で説明しているワークフローとは異なります。詳細については、このトピックの最後にある 修正スキャンの削除 の手順を参照してください。

警告: スキャンを削除した後で、スキャンまたはそのスキャンに関連付けられているスキャンデータを元に戻すことはできません。表示または実行する必要がなくなったことを確信できるスキャンのみを削除してください。

始める前に

- スキャンを **[ゴミ箱]** フォルダーに移動します。

スキャンを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. **[フォルダー]** セクションで、**[ゴミ箱]** フォルダーをクリックします。

   スキャンの表が更新され、ゴミ箱フォルダーのスキャンが表示されます。

5. 次のいずれかを行います。

   - 1つのスキャンを選択する場合

     a. スキャンの表で、削除するスキャンにカーソルを合わせます。

     b. 行にある ⋮ ボタンをクリックします。

        メニューが表示されます。

c. **[削除]** をクリックします。

確認ウィンドウが表示されます。

- 複数のスキャンを選択する場合

a. スキャンの表で、削除するスキャンの横にあるチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで、**[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。

6. 確認ウィンドウで、**[削除]** をクリックします。

Tenable Vulnerability Management により選択したスキャンが削除されます。

修正スキャンの削除

必要なスキャンのアクセス許可: 設定可

修正スキャンを削除する場合、そのスキャンが共有されているすべてのユーザーに対して、スキャン設定およびスキャン結果を削除します。

注意: Tenable Vulnerability Management は 90 日以上経過しているスキャン結果を削除します。

修正スキャンを削除する方法

1. 左上にある ☰ ボタンをクリックします。

左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[フォルダー]** セクションで、**[修正スキャン]** フォルダーをクリックします。

注意: **[修正スキャン]** フォルダーは、Tenable Vulnerability Management スキャンの場合にのみ表示されます。

スキャンの表が更新され、所有しているかまたは他のユーザーから共有された修正スキャンが表示されます。デフォルトでは、行が**[作成日]**で並べ替えられます。

4. 次のいずれかを行います。

   - 1つのスキャンを選択する場合

     a. スキャンの表で、削除するスキャンにカーソルを合わせます。

     b. 行にある ⋮ ボタンをクリックします。

     メニューが表示されます。

     c. **[削除]**をクリックします。

     確認ウィンドウが表示されます。

   - 複数のスキャンを選択する場合

     a. スキャンの表で、削除するスキャンの横にあるチェックボックスを選択します。

     表の上部にアクションバーが表示されます。

     b. アクションバーで、**[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。

5. 確認ウィンドウで、**[削除]**をクリックします。

   Tenable Vulnerability Managementにより選択したスキャンが削除されます。

> **注意:** Tenable Vulnerability Managementは、最大1万件の修正スキャン結果を保持します。10,000以上の修正スキャン結果がある場合は、Tenable Vulnerability Managementは最も古い結果から順番にスキャン結果を削除します。

検出スキャンと評価スキャン

Tenable の製品を使用して、*検出スキャン*と*評価スキャン*の 2 種類のスキャンを実行できます。Tenable は、ネットワーク上の資産の全容を正確に掴むためにディスカバリースキャンを行い、資産の脆弱性を把握するためにアセスメントスキャンを行うことを推奨します。

検出および評価された資産がどのようにライセンスに対してカウントされるかについての詳細は、Tenable Vulnerability Management ライセンスを参照してください。

タイプ	説明	ライセンス
検出スキャン	ネットワーク上の資産を見つけます。 例 • **ホスト検出**テンプレートにより設定されたスキャン • 検出プラグインのみを使用するように設定されたスキャン • Tenable Nessus Network Monitor を検出モードで使用するように設定されたスキャン	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。
評価スキャン	資産の脆弱性を見つけます。 たとえば、Tenable Nessus スキャナーまたは Tenable Nessus Agentを使用する、*認証*スキャンまたは*非認証*スキャンの実行 **認証スキャン** 評価スキャンの設定にアクセス認証情報を追加することで、認証 (Authenticated) スキャン (*Credentialed* スキャンとも呼ばれます) を設定します。 認証されたスキャンを設定することで、認証されていないスキャンよりも広範なチェックを実行できるようになり、スキャン結果がより正	一般的には、評価スキャンにより評価されたスキャンは、ライセンスに対してカウントされます。

	確になります。これにより、非常に大規模なネットワークのスキャンが容易になり、ローカルのエクスポージャーやコンプライアンス違反を特定できます。 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付与される権限が多いほど(root アクセスや管理者アクセスなど)、スキャン結果は詳細になります。 詳細は、Tenable Vulnerability Management スキャンの認証情報 を参照してください。 **非認証スキャン** 評価スキャンの設定にアクセス認証情報を追加しない場合、Tenable Vulnerability Management は資産のスキャン時に制限された数のチェックを行います。	

評価されたことのない資産の特定

Tenable Vulnerability Management は、資産の脆弱性を評価することなしに資産を検出、または*参照*できます。(たとえばホスト検出スキャン、Tenable Nessus Network Monitor の検出モードでの実行、またはコネクタ経由)資産のうち、過去に参照されたが評価されていないものは、資産のライセンス制限に対してカウントされません。資産が評価の対象になる条件の一覧は、資産のカウント方法を参照してください。ただし一度評価されたら、仮にライセンスカウントが期限切れとなったとしても、その資産は常に評価済みとして分類されます。

このライセンス付与の特例により、ライセンス制限に対して大量の資産をカウントすることなく、ネットワーク上の資産を検出することが可能です。資産を検出した後で、どの資産がまだ脆弱性に関して評価されたことがないかを特定し、それらの中でどの資産をスキャンおよび管理していくかを選ぶことができます。

評価されたことのない資産を特定する方法

1. 次のいずれかの方法を使用して資産を検出します。

   - Tenable Vulnerability Management でホスト検出スキャンを作成して起動する。
   - 検出モードを有効にして Tenable Nessus Network Monitorを設定し、Tenable Vulnerability Managementにリンクする。
   - コネクタを設定します。

   これらの方法で検出された資産は、脆弱性に関して評価されるまでは資産のライセンス制限に対してカウントされません。

2. 評価されたことのない資産をフィルタリングします。

   a. 資産の表で、以下の設定でフィルターを作成します。

      - **[カテゴリ]** ボックスで、**[評価済み資産]** を選択します。
      - **[演算子]** ボックスで、**[次の値に等しい]** を選択します。
      - **[値]** ボックスで、**[False]** を選択します。

   a. **[適用]** をクリックします。

      Tenable Vulnerability Managementは、脆弱性に関してまだ評価されたことのない資産をフィルタリングします。

> **注意:** 未評価の資産 (**[評価済み資産]** が **[False]** の値に等しい資産) は、ライセンスのない資産 (**[ライセンス済み (VM)]** が **[False]** の値に等しい資産) とは異なる場合があります。一度資産の脆弱性をスキャンすると、Tenable Vulnerability Management はその時以降、資産を評価済みに分類します。しかし、資産のライセンスの状態は、資産の削除や企業のライセンスカウントの期限切れに伴い、時間とともに変化する可能性があります。

b. (オプション) 後で使用するために検索条件を保存します。

3. (オプション) 資産にタグ付けを行い、評価されたことのない資産を特定します。

   a. 評価されたことのない資産を特定するタグを作成します。

      たとえば、Assets:NotYetAssessed

   b. 手動で資産にタグを適用するか、評価されたことのない資産を自動的にフィルタリングするタグルールを作成します。

      たとえば、まだ評価されたことのない資産に対する動的なタグを作成するには、**[評価済み資産]** を **[False] の値に等しい**ようにフィルタリングするタグルールを設定します。

4. (オプション) スキャンを作成し、作成したタグを使用して資産をターゲットします。

スキャンのフェイルオーバー

Tenable Vulnerability Management がスキャナーにスキャンジョブを割り当て、スキャン中にスキャナーがオフラインになると、次のことが起こります。

1. 割り当てられたスキャナーが 2 時間後に Tenable Vulnerability Management に応答しない場合、スキャンジョブがタイムアウトします。
2. Tenable Vulnerability Management はスキャナーからスキャンジョブを削除し、同じスキャナーグループ内の別のスキャナーでスキャンを試行します。オンラインに戻った場合は、同じスキャナーで試行します。
3. Tenable Vulnerability Management は、手順 1 と 2 を 3 回試行します。3 回試行してもスキャンジョブが完了しない場合、Tenable Vulnerability Management はスキャンジョブを中止します。

スキャンステータス

Tenable Vulnerability Management は、設定された各スキャンのスキャンステータスを提供します。

スキャンが進行中の場合、Tenable Vulnerability Management は完了したスキャンタスクの数の割合を示します。

たとえば、1 回のスキャンで 120 個未満の IP アドレスをスキャンする場合、Tenable Vulnerability Management は 1 つのスキャンタスクを作成し、完了時には進行状況パーセンテージが 0% から 100% に変わります。

ただし、120 個を超える IP アドレスをターゲットにした場合、Tenable Vulnerability Management は複数のスキャンタスクを作成します。各タスクが完了すると、完了したタスクの数に応じて割合が変化します。たとえば、300 個の IP アドレスをターゲットとするスキャンが 3 つのスキャンタスクに分割され、各タスクが完了すると、進捗バーのパーセンテージが更新され、タスクが完了と表示されます。

注意: スキャンを一時停止すると、Tenable Vulnerability Management は完了した結果を処理に回します。スキャンを再開すると、Tenable Vulnerability Management は未完了の結果を生成するために 1 つまたは複数の新しいスキャンタスクを作成します。したがって、スキャンを一時停止すると、進行状況のパーセンテージが更新される場合があります。

ヒント: Tenable Vulnerability Management スキャンでは、スキャンステータスにカーソルを合わせるとポップアップウィンドウが表示され、スキャンされたターゲットの数や経過時間または最終スキャン時間など、より多くのステータス情報が示されます。ウィンドウには、スキャンの現在のステータスに基づいて異なる情報が表示されます。

Tenable Vulnerability Management スキャンでは、次のステータスの値を持つことができます。

ステータス	説明
Tenable Vulnerability Management スキャン **ヒント:** 一般的な Tenable Vulnerability Management スキャンのステータスフローは、**初期化中**、**実行中**、**結果の公開中**、**完了済み**です。	
中止	実行中に Tenable Vulnerability Management またはスキャナーで問題が発生したために、直近のスキャン実行が不完全、あるいはスキャンが 4 時間以上実行されずにキューに残っていた場合。実行中に発見した問題の詳細については、スキャンの警告を表示してください。
キャンセル	ユーザーのリクエストにより、Tenable Vulnerability Management がこのスキャンの直

ステータス	説明
	近の実行を正常に停止しています。
完了	スキャンの最新の実行が完了しています。
Empty	スキャンが、空であるか(新規もしくは実行前)、保留中 (Tenable Vulnerability Management がスキャンの実行リクエストを処理中)のどちらかです。
Imported	このスキャンはユーザーがインポートしたものです。インポートしたスキャンは実行できません。スキャン履歴は、インポートされたスキャンでは利用できません。
Pausing	ユーザーがこのスキャンを一時停止したため、Tenable Vulnerability Management が処理中です。
Paused	ユーザーの要求により、Tenable Vulnerability Management がスキャンに関連するアクティブなタスクを正常に一時停止しました。一時停止されたタスクは、タスクに割り当てられたスキャナーのタスク容量を消費し続けます。Tenable Vulnerability Management により一時停止されたスキャンジョブから新規タスクがディスパッチされることはありません。スキャンが 14 日を超えて一時停止状態になると、スキャンはタイムアウトします。Tenable Vulnerability Management はスキャナー上の関連タスクを中止させ、スキャンを中断済みに分類します。
Pending	Tenable Vulnerability Management がスキャンを開始するためにキューに入れ、割り当てられたセンサーにスキャンタスクを割り当てています。 **注意:** Tenable Vulnerability Management は、4 時間以上 **保留中** ステータスになったままのスキャンを中止します。Tenable Vulnerability Management によってスキャンが中止された場合は、重複するスキャンの数が減るようにスキャンのスケジュールを変更してください。問題が解決しない場合は、Tenable サポートにお問い合わせください。
結果の公開中	Tenable Vulnerability Management は、Tenable Vulnerability Management ユーザーインターフェースで表示および使用する目的でスキャン結果データを処理して保存します。**結果の公開中** ステータスは、**実行中** ステータスが 100% に達すると開始します。
再開中	Tenable Vulnerability Management はユーザーがスキャンを再開した後の、タスクの再開処理中です。Tenable Vulnerability Management はスキャンが一時停止した

ステータス	説明
	場所からタスクを開始するようスキャナーに指示します。スキャンの再開時に Tenable Vulnerability Management またはスキャナーが問題を発見した場合、スキャンは失敗し、Tenable Vulnerability Management はスキャンのステータスを中断済みへと更新します。
実行中	スキャンは現在実行中です。このステータスが表示されている間に、スキャンのセンサーは割り当てられたスキャンタスクを完了し、Tenable Vulnerability Management はスキャン結果を処理します。スキャンの実行中は、ステータスの横に進行状況バーが表示されます。進行状況バーには、完了したタスクの割合が表示されます。
停止中	ユーザーがスキャンを停止した、スキャンがタイムアウトした、または Tenable Vulnerability Management が関連するすべてのスキャンタスクの完了後にスキャンを停止しています。

スキャンテンプレート

スキャンテンプレートには、スキャンの詳細な設定が含まれています。Tenable のスキャンテンプレートを使用して、組織のカスタムスキャン設定を作成できます。その後、Tenable のスキャンテンプレートまたはカスタム設定に基づいてスキャンを実行できます。

スキャン設定を作成すると、**[スキャンテンプレートの選択]** ページが表示されます。Tenable Vulnerability Management では Tenable Vulnerability Management 用と Tenable Web App Scanning 用の個別のテンプレートが用意されています。Tenable Vulnerability Management スキャンでは、スキャンに使用するセンサーに応じてスキャナー用とエージェント用の別個のテンプレートが Tenable Vulnerability Management にあります。

カスタム設定がある場合は、**[ユーザー定義]** タブに表示されます。ユーザー定義テンプレートの詳細については、ユーザー定義テンプレートを参照してください。

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。

すべてのスキャンテンプレート設定の説明については、スキャンの設定を参照してください。

ヒント： Tenable Vulnerability Management スキャン設定を最適化するための情報とヒントについては、Tenable Vulnerability Managementスキャンの調整ガイドを参照してください。

Tenable が提供する Tenable Nessus スキャナーテンプレート

Tenable Vulnerability Management 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。

- 脆弱性スキャン(共通) - Tenable では、所属する組織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。
- 設定スキャン - 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。設定スキャンは、コンプライアンス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、Tenable Vulnerability Management スキャンにおけるコンプライアンス および Tenable Vulnerability Management スキャンでの SCAP 設定 を参照してください。
- 戦術スキャン - Tenable では、戦術スキャンテンプレートを使用して、特定の脆弱性または脆弱性グループについてネットワークをスキャンすることを推奨しています。戦術スキャンは軽量でタイムリーなスキャンテンプレートであり、特定の脆弱性に対して資産をスキャンするために使用できます。Tenable では、Tenable Vulnerability Management 戦術スキャンライブラリを頻繁に更新し、Log4Shell など一般的に関心の高い最新の脆弱性を検出するテンプレートを随時追加しています。

次の表では、利用可能な Tenable Nessus スキャナーテンプレートについて説明します。

テンプレート	説明
脆弱性スキャン(共通)	
高度なネットワークスキャン	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:** 高度なスキャンテンプレートを使うと、Tenable Vulnerability Management のエキスパートは、高速または低速チェックといったカスタム設定によって詳細なスキャンを行えますが、設定を誤ると、資産の停止やネットワークの過負荷が引き起こされる場合があります。高度なテンプレートは注意深く使用してください。
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。
資格認定されたパッチ監査	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 Vulnerability Management 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。
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 Nessus 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。
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)。
従来のウェブアプリケーションスキャン	Tenable Nessus スキャナーを使用してウェブアプリケーションをスキャンします。

	注意： Tenable Web App Scanning スキャナーとは異なり、Tenable Nessus スキャナーはウェブアプリケーションのスキャンにブラウザを使用しません。したがって、**従来のウェブアプリケーションスキャン**は Tenable Web App Scanning ほど包括的ではありません。
モバイルデバイススキャン	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。
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。 **注意：** PCI ASV はその性質上スキャンの検出レベルが非常に高く、データに誤検出が含まれる可能性があるため、Tenable Vulnerability Management の集計データからは除外されます。これは意図的な設計です。
設定スキャン	
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。 監査するサービスの認証情報を提供した場合、このテンプレートを使用して 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。
MDM 設定監査	モバイルデバイスマネージャーの設定を監査します。 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 Vulnerability Management 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。
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。 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 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。 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。
戦術スキャン	
2022 年の脅威状況レポート (TLR)	Tenable の脅威状況レポート (2022 年) に掲載されている脆弱性を検出します。
Active Directory ID	ドメインユーザーアカウントを使用して、AD ID 情報をクエリします。このポリシーは、LDAPS を介して Active Directory ID 情報を列挙します。これには、

	ドメインユーザーの認証情報、LDAPS 設定、およびスキャンターゲットとしての Active Directory ドメインコントローラーが必要です。
Active Directory Starter Scan	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。
CISA Alerts AA22-011A および AA22-047A	最近の CISA アラートからの脆弱性に対するリモートチェックとローカルチェックを実行します。
ContiLeaks	ContiLeaks の脆弱性に対するリモートチェックとローカルチェックを実行します。
GHOST (glibc) 検出	CVE-2015-0235 のリモートチェックとローカルチェックを実行します。
Intel AMT セキュリティバイパス	CVE-2017-5689 のリモートチェックとローカルチェックを実行します。
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。
Log4Shell Remote Checks (Log4Shell リモートチェック)	Apache Log4j の Log4Shell 脆弱性 (CVE-2021-44228) をリモートチェックで検出します。
Log4Shell Vulnerability Ecosystem	Apache Log4j の Log4Shell 脆弱性 (CVE-2021-44228) をローカルおよびリモートチェックで検出します。このテンプレートは動的で、サードパーティベンダーがソフトウェアにパッチを適用すると、新しいプラグインで定期的に更新されます。
マルウェアのスキャン	Windows と Linux のシステムで、マルウェアをスキャンします。
PrintNightmare	Windows Print Spooler の脆弱性 (PrintNightmare) である CVE-2021-34527 のローカルチェックを行います。
ProxyLogon: MS	リモートおよびローカルでチェックを行い、CVE-2021-26855、CVE-2021-

Exchange	26857、CVE-2021-26858、CVE-2021-27065 に関連する Microsoft Exchange Server の脆弱性を検出します。
ランサムウェアのエコシステム	一般的なランサムウェアの脆弱性に対するリモートチェックとローカルチェックを実行します。
Ripple20 Remote Scan	Ripple20 脆弱性の影響を受ける可能性のある、Treck 製のスタックをネットワーク内で実行しているホストを検出します。
Solarigate	リモートチェックとローカルチェックを使用して SolarWinds Solorigate 脆弱性を検出します。
Spectre and Meltdown	CVE-2017-5753、CVE-2017-5715、CVE-2017-5754 のリモートチェックとローカルチェックを実行します。
WannaCry Ransomware	WannaCry ランサムウェア (MS17-010) のスキャンを行います。
Zerologon リモートスキャン	Microsoft Netlogon の権限昇格の脆弱性 (Zerologon) を検出します。

Tenable が提供する Tenable Nessus Agent テンプレート

Tenable Vulnerability Management 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。

- 脆弱性スキャン - Tenable では、所属する組織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。
- インベントリコレクション - 標準の Tenable Nessus Agent 脆弱性スキャンとは異なり、インベントリ収集テンプレートは Tenable の Frictionless Assessment テクノロジーを使用して、より高速なスキャン結果を提供し、スキャンのシステムフットプリントを削減します。エージェントベースのインベントリスキャンは、ホストから基本情報を収集し、それを Tenable Vulnerability Management にアップロードします。その後、Tenable Vulnerability Management は、Tenable がカバレッジをリリースする際に、不足しているパッチおよび脆弱性に対して情報を分析します。これにより、ターゲットとなるホストのパフォーマンスへの影響が軽減されると同時に、アナリストが最新パッチの影響を確認する時間を減らすことができます。

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

次の表では、利用可能な Tenable Nessus Agentテンプレートについて説明します。

テンプレート	説明
脆弱性スキャン	
高度なエージェントスキャン	推奨のないエージェントスキャン。スキャン設定は完全にカスタマイズできます。Tenable Vulnerability Management では、[高度なエージェントスキャン] テンプレートで 2 つのスキャン方法が許可されています。 • スキャンウィンドウ - エージェントが脆弱性レポートに含めて表示するように報告する時間枠を指定します。 • トリガーされたスキャン - スキャンを起動するタイミングを示す特定の基準を

テンプレート	説明
	エージェントに提供します。基準の1つ(または複数)が満たされると、エージェントはスキャンを起動します。詳細は、*Tenable Vulnerability Management ユーザーガイド*の基本設定を参照してください。 **注意:** 高度なエージェントスキャンのテンプレートを使用してエージェントスキャンを作成する際は、スキャンに使用するプラグインも選択する必要があります。
エージェント Log4Shell	Apache Log4j CVE-2021-44228 のエージェント検出。
基本的なエージェントスキャン	Tenable Nessus Agents を介して接続されたシステムをスキャンします。
マルウェアのスキャン	Tenable Nessus Agents を介して接続されたシステムでマルウェアをスキャンします。 Tenable Nessus 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。
ポリシーコンプライアンス監査	Tenable Nessus Agents を介して接続されたシステムの既知の基準値と照らしてシステム設定を監査します。 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 および OVAL エージェント監査	Tenable Nessus Agents を介して接続されたシステムの SCAP および OVAL 定義を使用してシステムを監査します。 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

テンプレート	説明
	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。
インベントリコレクション	
インベントリ収集	Frictionless Assessment Tenable Nessus Agents を介して、コンパイル済みインベントリをスキャンします。 インベントリ収集テンプレートは Frictionless Assessment を使用して、より速くスキャン結果を出し、システムフットプリントを削減します。これは、脆弱性チェックを Frictionless Assessment を介して実行することで行われますが、エージェントは資産情報(インストールされているソフトウェアや IP アドレスなど)を収集するチェックのみを実行します。このスキャン方法は、Tenable Vulnerability Management ユーザーインターフェースおよびドキュメントでは、*インベントリスキャン*と呼ばれることがあります。 Collect Inventory スキャンは、以下をカバーします。 • RedHat ローカルセキュリティチェック • CentOS ローカルセキュリティチェック • Amazon Linux ローカルセキュリティチェック • Debian ローカルセキュリティチェック • Fedora ローカルセキュリティチェック

テンプレート	説明
	• SuSE ローカルセキュリティチェック • Ubuntu ローカルセキュリティチェック • Windows/Microsoft の更新プログラムチェック (2017 年以降のすべての Windows ロールアップチェック) Collect Inventory スキャンは、現在、以下をカバーしていません。 • マルウェアおよびコンプライアンスチェック • dpkg や rpm でインストールされていない、インスタンス上のサードパーティ Linux アプリケーションの検出 (Apache HTTP や Postgres など) • サードパーティ Windows アプリケーション (Google Chrome や Mozilla Firefox など) • Microsoft 製品のパッチ火曜日の更新 (Exchange や Sharepoint など) **注意:** MacOS で実行されている Tenable Nessus Agents とバージョン 10.1.0 以前の Tenable Nessus Agents では、インベントリスキャンが実行されず、スキャン結果から除外されます。

Tenable が提供する Tenable Web App Scanning テンプレート

次の表では、利用可能な Tenable Web App Scanning スキャンテンプレートについて説明します。

テンプレート	説明
API	API 内で脆弱性の有無をチェックするスキャン。このスキャンは、OpenAPI (Swagger) 仕様ファイルで記述された RESTful API を分析します。添付ファイルのサイズは 1 MB に制限されています。 **ヒント:** API のスキャンに認証用のキーやトークンが必要な場合、**[HTTP 設定]** セクションの [詳細] 設定で必要になるカスタムヘッダーを追加することができます。 **注意:** API スキャンテンプレートは、パブリックベータ版として提供されています。この機能は、ベータ期間中の継続的な改善に伴い、変更される可能性があります。 **注意:** API スキャンは一度に 1 つのターゲットのみをサポートします。
設定監査	ウェブアプリケーションの HTTP セキュリティヘッダーおよび他の外部向けの設定を分析し、アプリケーションが一般的なセキュリティ業界標準に準拠しているかどうかを確認する高レベルのスキャン。 **[設定監査]** スキャンテンプレートを使用してスキャンを作成する場合、Tenable Web App Scanning はセキュリティ業界標準のコンプライアンスに関連するプラグインについてのみウェブアプリケーションを分析します。
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。
概要	ウェブアプリケーション内のどの URL をデフォルトで Tenable Web App Scanning がスキャンするかを決定する高レベルの予備的なスキャン。 **[概要]** スキャンテンプレートは、ウェブアプリケーション内のアクティブな脆弱性を分析するものではありません。そのため、このスキャンテンプレートは **[スキャン]** テンプレートほど多くのプラグインファミリーオプションを提供していません。 **注意:** このスキャンテンプレートは、従来の Tenable Web App Scanning インターフェースの **[ウェブアプリケーションの概要]** テンプレートに相当します。

PCI	Tenable PCI ASV 用にウェブアプリケーションのクレジットカード業界データセキュリティ標準 (PCI DSS) のコンプライアンスを分析するスキャン
クイックスキャン	ウェブアプリケーションの HTTP セキュリティヘッダーおよび他の外部向けの設定を分析し、アプリケーションが一般的なセキュリティ業界標準に準拠しているかどうかを確認する**設定監査**スキャンに似た高レベルのスキャン。スケジュール設定はありません。 **[クイックスキャン]** スキャンテンプレートを使用してスキャンを作成する場合、Tenable Vulnerability Management はセキュリティ業界標準のコンプライアンスに関連するプラグインについてのみウェブアプリケーションを分析します。
スキャン	ウェブアプリケーションの広範囲の脆弱性を評価する包括的なスキャン。 **[スキャン]** テンプレートは、すべてのアクティブなウェブアプリケーションプラグイン用のプラグインファミリーオプションを提供します。 **[スキャン]** テンプレートを使用してスキャンを作成すると、Tenable Web App Scanning は、**[設定監査]**、**[概要]**、**[SSL TLS]** テンプレートを使用して作成されたスキャンがチェックするすべてのプラグイン、および特定の脆弱性検出のための追加のプラグインについてウェブアプリケーションを分析します。 このスキャンテンプレートを使用してスキャンを実行すると、ウェブアプリケーションのより詳細な評価が提供されますが、他の Tenable Web App Scanning スキャンよりも時間がかかります。 **注意:** このスキャンテンプレートは、従来の Tenable Web App Scanning インターフェースの **[ウェブアプリケーションスキャン]** テンプレートに相当します。
SSL TLS	ウェブアプリケーションが SSL/TLS 公開鍵暗号化を使用しているかどうかを確認し、使用している場合には、暗号化がどのように設定されているかを確認するためのスキャン。 **[SSL TLS]** テンプレートを使用してスキャンを作成する場合、Tenable Web App Scanning は、SSL/TLS の実装に関連するプラグインについてのみウェブアプリケーションを分析します。スキャナーは、URL をクロールしたり、個別のページの脆弱性を評価したりしません。

ユーザー定義テンプレート

必要なテンプレートのアクセス許可: 所有者

Tenable は、特定のスキャン目的のために使用できるさまざまなスキャンテンプレートを用意しています。Tenable 提供のスキャンテンプレートをカスタマイズして他のユーザーと共有したい場合は、ユーザー定義スキャンテンプレートを作成できます。

さまざまなスキャン設定についての詳細は、スキャンの設定を参照してください。

[スキャン] ページから、ユーザー定義の Tenable Vulnerability Management および Tenable Web App Scanning スキャンテンプレートを作成、編集、コピー、エクスポート、削除できます。Tenable Vulnerability Management スキャンテンプレートをインポートおよびエクスポートすることもできます。

ユーザー定義のスキャンテンプレートを管理する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. ページの右上で、**[ツール]** ボタンをクリックします。

   メニューが表示されます。

4. **[スキャンテンプレートの管理]** を選択します。

   [スキャンテンプレート] ページが表示されます。

5. **[スキャンテンプレート]** で、**[脆弱性管理のスキャンテンプレート]** か **[ウェブアプリケーションスキャンテンプレート]** の表示を選択します。

   選択された内容に応じてスキャンテンプレートの表が更新されます。

テンプレートをクリックしてその設定とパラメーターを表示または編集するか、次の手順に従ってユーザー定義のテンプレートを細かく管理します。

ユーザー定義テンプレートの作成

ユーザー定義スキャンテンプレートを作成することで、カスタムスキャン設定を保存して、他の Tenable Vulnerability Management ユーザーと共有できます。

スキャンテンプレートを定義すると、Tenable Vulnerability Management は定義した人物にそのスキャンテンプレートに対する所有者のアクセス許可を割り当てます。他のユーザーにテンプレートのアクセス許可を割り当てることでスキャンテンプレートを共有できますが、テンプレートを削除できるのは所有者だけです。

ユーザー定義スキャンテンプレートを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. ページの右上にある [⊕ **Create Template**] ボタンをクリックします。

   [テンプレートの選択] ページが表示されます。

5. ユーザー定義スキャンテンプレートのベースとして使用するテンプレートのタイルをクリックします。

   [テンプレートの作成] ページが表示されます。

6. 次のいずれかを行います。

   - Tenable Vulnerability Management スキャンテンプレートを作成する場合は、次の手順を使用します。

a. スキャンテンプレートを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定を行います。 • 基本設定 - スキャンテンプレートの組織的な要素とセキュリティ関連の要素を指定できます。これには、スキャンの名前、ターゲット、スキャンをスケジュールするかどうか、スキャンのアクセス許可を持つユーザーの指定が含まれます。 • Discovery 設定 - スキャンが検出とポートスキャンを実行する方法を指定します。 • 評価設定 - 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指定します。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。 • Report 設定 - スキャンがレポートを生成するかどうかを指定します。 • 詳細設定 - スキャン効率のための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
Compliance/SCAP	監査する必要のあるプラットフォームを指定します。Tenable, Inc. は各プラットフォームの監査のベストプラクティスを提供しています。また、カスタムの監査ファイルをアップロードすることもできます。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

- Tenable Web App Scanning スキャンを作成する場合は、次の手順を使用します。

a. スキャンを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定をします。詳細は、Tenable Web App Scanning スキャンの基本設定 を参照してください。
範囲	スキャンに含めるまたはスキャンから除外する URL とファイルタイプを指定します。詳細は、Tenable Web App Scanning スキャンの範囲設定 を参照してください。
資産	スキャンによる脆弱性の識別方法と、識別対象の脆弱性を指定します。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。詳細は、Tenable Web App Scanning スキャンの評価設定 を参照してください。
詳細	スキャン効率を高めるための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management はユーザー定義スキャンテンプレートを保存し、それを **[スキャンテンプレート]** ページのスキャンテンプレートリストに追加します。

ユーザー定義テンプレートの編集

必要なテンプレートのアクセス許可: 設定可

ユーザー定義スキャンテンプレートを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。
4. ページの右上で、**[ツール]** ボタンをクリックします。

   メニューが表示されます。
5. **[スキャンテンプレートの管理]** を選択します。

   [スキャンテンプレート] ページが表示されます。
6. スキャンテンプレートの表で、編集するスキャンテンプレートをクリックします。

   [スキャンテンプレートの編集] ページが表示されます。
7. 次のいずれかを行います。

- Tenable Vulnerability Management スキャンテンプレートを編集する場合は、次の手順を使用します。

a. スキャンテンプレートのオプションを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定を行います。 • 基本設定 - スキャンテンプレートの組織的な要素とセキュリティ関連の要素を指定できます。これには、スキャンの名前、ターゲット、スキャンをスケジュールするかどうか、スキャンのアクセス許可を持つユーザーの指定が含まれます。 • Discovery 設定 - スキャンが検出とポートスキャンを実行する方法を指定します。 • 評価設定 - 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指定します。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。 • Report 設定 - スキャンがレポートを生成するかどうかを指定します。 • 詳細設定 - スキャン効率のための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
Compliance/SCAP	監査する必要のあるプラットフォームを指定します。Tenable, Inc. は各プラットフォームの監査のベストプラクティスを提供しています。また、カスタムの監査ファイルをアップロードすることもできます。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

- Tenable Web App Scanning スキャンテンプレートを編集する場合は、次の手順を使用します。

  a. スキャンテンプレートのオプションを設定します。

タブ	アクション
設定	スキャンテンプレートで利用できる設定をします。詳細は、Tenable Web App Scanning スキャンの基本設定 を参照してください。
範囲	スキャンに含めるまたはスキャンから除外する URL とファイルタイプを指定します。詳細は、Tenable Web App Scanning スキャンの範囲設定 を参照してください。
資産	スキャンによる脆弱性の識別方法と、識別対象の脆弱性を指定します。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。詳細は、Tenable Web App Scanning スキャンの評価設定 を参照してください。
詳細	スキャン効率を高めるための高度な制御を指定します。
認証情報	認証スキャンを実行するために Tenable Vulnerability Management が使用する認証情報を指定します。
プラグイン	プラグインファミリーまたは個別のプラグインによるセキュリティチェックを選択します。

8. **[保存]** をクリックします。

   Tenable Vulnerability Management はユーザー定義スキャンテンプレートを保存し、それを **[スキャンテンプレート]** ページのテンプレートリストに追加します。

ユーザー定義テンプレートのコピー

ユーザー定義スキャンテンプレートをコピーすると、Tenable Vulnerability Management はコピーの作成者にそのコピーに対する所有者アクセス許可を割り当てます。他のユーザーにテンプレートのアクセス許可を割り当てることでコピーを共有できますが、コピーされたテンプレートを削除できるのは所有者だけです。

ユーザー定義スキャンテンプレートをコピーする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. ページの右上で、**[ツール]** ボタンをクリックします。

   メニューが表示されます。

5. **[スキャンテンプレートの管理]** を選択します。

   [スキャンテンプレート] ページが表示されます。

6. スキャンの表で、起動するスキャンにカーソルを合わせます。

7. 行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

8. メニューにある ⧉ ボタンをクリックします。

   [テンプレートをコピーしました] というメッセージが表示されます。Tenable Vulnerability Management は、スキャンテンプレートのコピーを作成し、その名前の末尾に*「- コピー」*を付けます。そして、そのコピーの作成者に所有者のアクセス許可を与えます。コピーがスキャンテンプレートの表に表示されます。

ユーザー定義テンプレートをエクスポートする(Tenable Vulnerability Management のみ)

ユーザー定義スキャンテンプレートをエクスポートして、後でインポートできます。

> **注意:** Tenable Vulnerability Management では、ユーザー定義スキャンテンプレートのパスワード、認証情報、ファイルベースの設定 (`.audit` ファイルや SSH **known_hosts ファイル**など) はエクスポートされません。

ユーザー定義スキャンテンプレートをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** の表示を選択します。

4. ページの右上で、**[ツール]** ボタンをクリックします。

   メニューが表示されます。

5. **[スキャンテンプレートの管理]** を選択します。

   [スキャンテンプレート] ページが表示されます。

6. スキャンの表で、エクスポートするスキャンテンプレートにカーソルを合わせます。

7. 行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

8. 行にある [→ ボタンをクリックします。

   Tenable Vulnerability Management は、ユーザー定義のスキャンテンプレートを .nessus ファイルとしてエクスポートします。

   > **注意:** .nessus ファイル形式については、Nessus File Format (Nessus ファイル形式) を参照してください。

ユーザー定義テンプレートをインポートする(Tenable Vulnerability Management のみ)

スキャンテンプレートをインポートすると、Tenable Vulnerability Management はそのスキャンテンプレートの所有者アクセス許可を割り当てます。他のユーザーにテンプレートのアクセス許可を割り当てるとスキャンテンプレートを共有できますが、テンプレートを削除できるのは所有者だけです。

Tenable Vulnerability Management でエクスポートされたユーザー定義スキャンテンプレートには、パスワードやコンプライアンス監査ファイルは含まれません。スキャンテンプレートをインポートした後に、これらの設定を手動で追加する必要があります。

ユーザー定義スキャンテンプレートをインポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** の下で、**[脆弱性管理スキャン]** の表示を選択します。
4. ページの右上で、**[ツール]** ボタンをクリックします。

   メニューが表示されます。
5. **[スキャンテンプレートの管理]** を選択します。

   [スキャンテンプレート] ページが表示されます。
6. ページの右上の **[インポート]** ボタンをクリックします。

   ファイルマネージャーが表示されます。
7. インポートするスキャンテンプレートを選択します。
8. **[開く]** をクリックします。

   [テンプレートがアップロードされました] というメッセージが表示され、スキャンテンプレートが **[スキャンテンプレート]** ページに表示されます。

次の手順

- 必要に応じて、インポートされたテンプレートにパスワードとコンプライアンス監査ファイルを追加します。

ユーザー定義テンプレートの削除

ユーザー定義スキャンテンプレートを削除すると、Tenable Vulnerability Management によりすべてのユーザーアカウントから削除されます。

始める前に

- 削除するテンプレートを使用している、すべてのスキャンを削除します。スキャンによって現在使用中のスキャンテンプレートは削除できません。

1つまたは複数のユーザー定義スキャンテンプレートを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、**[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。

3. **[スキャン]** で、**[脆弱性管理スキャン]** か **[ウェブアプリケーションスキャン]** の表示を選択します。

4. ページの右上で、**[ツール]** ボタンをクリックします。

   メニューが表示されます。

5. **[スキャンテンプレートの管理]** を選択します。

   [スキャンテンプレート] ページが表示されます。

6. 1つまたは複数の削除するユーザー定義スキャンテンプレートを選択します。

   - 1つのスキャンテンプレートを選択する場合:

     a. スキャンの表で、起動するスキャンにカーソルを合わせます。

     b. 行にある ⋮ ボタンをクリックします。

        メニューが表示されます。

     c. メニューにある 🗑 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。

   - 複数のスキャンテンプレートを選択する場合:

     a. スキャンテンプレートの表で、削除する各スキャンテンプレートのチェックボックスを選択します。

        ページの下部またはに、アクションバーが表示されます。

     b. アクションバーで、🗑 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。

7. 確認ウィンドウで、**[削除]** をクリックします。

   Tenable Vulnerability Management により、選択した1つまたは複数のユーザー定義スキャンテンプレートが削除されます。

ユーザー定義テンプレート所有権の変更

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要なテンプレートのアクセス許可: 所有者

新しいインターフェースでユーザー定義スキャンテンプレートの所有権を変更する方法

1. ユーザー定義テンプレートの編集.
2. 左側のナビゲーションメニューの **[設定]** セクションで、**[基本]** をクリックします。

   [基本] 設定が表示されます。
3. **[ユーザーアクセス許可]** セクションの、**[所有者]** 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。

   利用可能なユーザーアカウントのリストが表示されます。
4. リストからユーザーを選択します。

   Tenable Vulnerability Management により自動的にユーザーのリストに追加され、自分のユーザーアカウントに **[表示可]** アクセス許可が付与されます。
5. (オプション) ユーザーアカウントのすべてのアクセス許可を削除するには

   a. ユーザーリストで、自分のユーザーアカウントにカーソルを合わせます。

   リストの最後に ✕ ボタンが表示されます。

   b. ✕ ボタンをクリックします。

   Tenable Vulnerability Management により、ユーザーのリストからアカウントが削除されます。
6. (オプション) ユーザーアカウントのアクセス許可を編集するには

   a. ユーザーアカウント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. アクセス許可を選択します。
7. **[保存]** をクリックします。

Tenable により選択されたユーザーに所有権が割り当てられ、自分のユーザーアカウントに選択したアクセス許可が割り当てられます。テンプレートから自分のユーザーアカウントのすべてのアクセス許可を削除すると、そのテンプレートはテンプレートの表に表示されなくなります。

スキャンの設定

スキャンの設定により、スキャンのパラメーターを独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、スキャンやユーザー定義テンプレートのベースになっている Tenable 提供のテンプレートによって変わります。

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ユーザー定義テンプレートで設定できます。

スキャン設定は、次のカテゴリに分類されます。

Tenable Vulnerability Management スキャン	Tenable Web App Scanning スキャン
• ユーザー定義テンプレートの基本設定 • Tenable Vulnerability Management スキャンの基本設定 • Tenable Vulnerability Management スキャンの検出設定 • Tenable Vulnerability Management スキャンの評価設定 • Tenable Vulnerability Management スキャンのレポート設定 • Tenable Vulnerability Management スキャンの詳細設定 • Tenable Vulnerability Management スキャンの認証情報 • Tenable Vulnerability Management スキャンにおけるコンプライアンス • Tenable Vulnerability Management スキャンでの SCAP 設定 • Tenable Vulnerability Management スキャンでのプラグインの設定	• ユーザー定義テンプレートの基本設定 • Tenable Web App Scanning スキャンの基本設定 • Tenable Web App Scanning スキャンの範囲設定 • Tenable Web App Scanning スキャンのレポート設定 • Tenable Web App Scanning スキャンの評価設定 • Tenable Web App Scanning スキャンの詳細設定 • Tenable Web App Scanning スキャンの認証情報 • Tenable Web App Scanning スキャンのプラグイン設定

ユーザー定義テンプレートの設定

ユーザー定義テンプレートを設定する際は、次のことに注意してください。

- ユーザー定義テンプレートを設定すると、その設定はそのユーザー定義テンプレート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。
- ユーザー定義テンプレートは、Tenable 提供のテンプレートをベースにして作成します。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。

  ただし、一部の**[基本]**設定はユーザー定義テンプレートの作成にだけ使用でき、個別のスキャンの設定時には表示されません。詳細は、ユーザー定義テンプレートの基本設定を参照してください。
- ユーザー定義テンプレートで設定できても、ユーザー定義テンプレートに基づく個別のスキャンで変更することができない設定があります。このような設定には、**[検出]**、**[評価]**、**[レポート]**、**[詳細]**、**[コンプライアンス]**、**[SCAP]**、**[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。
- ユーザー定義テンプレートで**認証情報**を設定した場合、他のユーザーがテンプレート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オーバーライドできます。

Tenable Vulnerability Management スキャンの設定

スキャンの設定により、スキャンのパラメーターを独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、スキャンやユーザー定義テンプレートのベースになっている Tenable 提供のテンプレートによって変わります。

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ユーザー定義テンプレートで設定できます。

Tenable Vulnerability Management のスキャン設定は、次のカテゴリに分類されます。

- ユーザー定義テンプレートの基本設定
- Tenable Vulnerability Management スキャンの基本設定
- Tenable Vulnerability Management スキャンの検出設定
- Tenable Vulnerability Management スキャンの評価設定
- Tenable Vulnerability Management スキャンのレポート設定
- Tenable Vulnerability Management スキャンの詳細設定
- Tenable Vulnerability Management スキャンの認証情報
- Tenable Vulnerability Management スキャンにおけるコンプライアンス
- Tenable Vulnerability Management スキャンでの SCAP 設定
- Tenable Vulnerability Management スキャンでのプラグインの設定

ユーザー定義テンプレートの設定

ユーザー定義テンプレートを設定する際は、次のことに注意してください。

- ユーザー定義テンプレートを設定すると、その設定はそのユーザー定義テンプレート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。
- ユーザー定義テンプレートは、Tenable 提供のテンプレートをベースにして作成します。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。

ただし、一部の**[基本]**設定はユーザー定義テンプレートの作成にだけ使用でき、個別のスキャンの設定時には表示されません。詳細は、ユーザー定義テンプレートの基本設定を参照してください。

- ユーザー定義テンプレートで設定できても、ユーザー定義テンプレートに基づく個別のスキャンで変更することができない設定があります。このような設定には、**[検出]**、**[評価]**、**[レポート]**、**[詳細]**、**[コンプライアンス]**、**[SCAP]**、**[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。
- ユーザー定義テンプレートで**認証情報**を設定した場合、他のユーザーがテンプレート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オーバーライドできます。

Tenable Vulnerability Management スキャンの基本設定

注意: このトピックでは、個別のスキャンで設定できる **[基本]** 設定について記載します。ユーザー定義テンプレートでの **[基本]** 設定に関しては、ユーザー定義テンプレートの基本設定を参照してください。

基本設定を使用すると、スキャン設定の組織的な要素とセキュリティ関連の要素を指定できます。これには、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の指定が含まれます。

注意: Tenable Vulnerability Management のスキャンの制限については、スキャン制限事項を参照してください。

[基本] 設定には、次のセクションが含まれます。

- 一般
- スケジュール
- 通知
- ユーザーアクセス許可

一般

スキャンの一般的な設定

設定	デフォルト値	説明
名前	None (なし)	スキャンの名前を指定します。
説明	None (なし)	(オプション) スキャンの説明を指定します。
スキャン結果	ダッシュボードに表示	スキャン結果を、ワークベンチ、ダッシュボード、レポートに表示するか非公開にするかを指定します。 **[プライベート表示]** に設定されている場合、スキャン結果の **[最終確認日]** の日付は更新されず、結果を表示するにはスキャンに直接アクセスする必要があります。 プライベートスキャン結果には、ワークベンチ、ダッシュボード、レポートに新しい**アクティブな**検出結果は表示されません。また、以前に検出された検出結果の脆弱性ステータスが **[修正済み]** または **[再表面**

		化] に移行することもありません。 **注意 : [ダッシュボードに表示]** はトリガーされたスキャンに対して常に有効です。
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。 修正スキャンを起動するときにフォルダーを指定することはできません。すべての修正スキャンは、**[修正スキャン]** フォルダーにのみ表示されます。
エージェントグループ	なし	(Tenable Nessus Agent テンプレートのみ) スキャンの対象にする 1 つまたは複数の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で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。
スキャナータイプ	内部スキャナー	ローカルの内部スキャナーとクラウド管理対象スキャナーのどちらがスキャンを実行するかを指定し、**[スキャナー]** フィールドの選択肢として、ローカルスキャナーとクラウド管理対象スキャナーのどちらを一覧表示するかを決めます。
スキャナー	自動選択	スキャンを実行するスキャナーを指定します。 スキャンするターゲットの場所に応じて、スキャナーを選択します。例 • リンクされたスキャナーを選択して、ルーティング不可能な IP アドレスをスキャンします。 **注意 :** クラウドスキャナーの場合、自動選択は使用できません。 • 次の場合は、スキャナーグループを選択してください。 ◦ 複数のスキャナーの間でスキャンの負荷を分散し、スキャンスピードを上げる場合 ◦ スキャン設定でスキャナーの指定を更新する必要なしに、将来スキャナーを再構築して新しいスキャナーをリンクする場合 • ターゲットに対してスキャンのルーティングを有効にするには、**[自**

		動選択]を選択してください。
タグ	なし	指定されたタグのいずれかが適用されているすべての資産をスキャンするには、1 つまたは複数のタグを選択します。指定されたタグで識別される資産のリストを表示するには、**[資産の表示]**をクリックします。
IP の選択	内部	(必須) **内部**または**外部** のどちらの IP アドレスのタグベースのスキャンを実行するかを選択します。 • **内部** – RFC 1918 (プライベート) IP アドレス。 • **外部** – RFC 1918 以外の (パブリック) IP アドレス。 **注意:** 組織のクラウド以外のスキャナーを使用して、**内部**と**外部**の両方のターゲットをスキャンできます。クラウドスキャナーは、**外部**ターゲットのスキャンにのみ使用できます。 **ヒント:** **外部**ターゲットと**内部**ターゲットの両方を同じタグでスキャンする必要がある場合は、2 つのスキャン設定を作成してください。**外部** IP をターゲットとするスキャンを 1 つ、**内部** IP をターゲットとするスキャンを 1 つ設定します。 Tenable Vulnerability Management は識別子を評価して、次の順序で 1 つのターゲットを決定します。 1. 最終スキャンターゲット 2. 直近の IPv4 3. 直近の IPv6 4. 直近で追加された FQDN **注意:** スキャンのルーティングは、リンクされたスキャナーでのみ利用可能です。
タグルールをターゲットとして使用する	既存のタグ付けされた資産のみ	(必須) Tenable Vulnerability Management がタグ付けされた資産のみをスキャンするか、選択したタグのルールが適用されている資産をスキャンするかを指定します。 • **既存のタグ付けされた資産のみ** - Tenable Vulnerability

		Management は、指定されたタグのいずれかが適用されている既存の資産をすべてスキャンします。 • **タグで定義されたターゲット** - Tenable Vulnerability Management は、IP アドレスまたは DNS が指定されたタグのルールに一致するすべての資産をスキャンします。**[タグで定義されたターゲット]** オプションは、IPv4、IPv6、DNS のタグルールに対してのみ機能します。 **注意:** **[すべてに一致]** フィルターを選択した場合、設定できるタグルールは 1 つのみです。それ以外の設定では、タグは空のターゲットに解決されます。 **[いずれかに一致]** フィルターを選択した場合は、複数のタグルールを持つことができます。ルールが IPv4、IPv6、DNS に対するものである限り、すべてのタグルールはターゲットとして解決されます。 たとえば、特定の IPv4 範囲を指定するタグルールでタグをスキャンするスキャンポリシーを作成します。タグ名の例は *My IPv4s* です。 • **[既存のタグ付けされた資産のみ]** を選択した場合、Tenable Vulnerability Management は *My IPv4s* タグで既にタグ付けされている資産のみをスキャンします。 • **[タグで定義されたターゲット]** を選択した場合、Tenable Vulnerability Management は IPv4 アドレスが *My IPv4s* タグルールで指定された範囲内にある資産をスキャンします。 タグとタグルールの詳細については、タグおよびタグルールを参照してください。
スキャンウィンドウ	無効	(Tenable Nessus スキャナーテンプレートのみ) スキャンが自動的に停止するまで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。 **注意:** スキャン期間の時間枠はスキャンジョブにのみ適用されます。スキャンジョブが時間枠内で完了した後、またはスキャン期間の終了により

		スキャンジョブが停止した後も、Tenable Vulnerability Management はスキャンジョブのインデックス作成をする必要があるかもしれません。このため、スキャン期間が過ぎても、スキャンが**[完了]**と表示されない場合があります。Tenable Vulnerability Management がスキャンにインデックスを付けると、**[完了]**と表示されます。
スキャンタイプ	スキャンウィンドウ	(Tenable Nessus Agent テンプレートのみ)(必須)スキャン期間とトリガーのどちらに基づいてエージェントスキャンを実行するかを指定します。 • **スキャン期間** - 脆弱性レポートに含めて表示するために必要になる、エージェントの報告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。 ウィンドウスキャンは明示的に起動するか、特定の時間に起動するようにスケジュールする必要があります。 • **Triggered Scan** - エージェントが報告するトリガーを指定します。ドロップダウンボックスを使用して、次のトリガータイプから選択します。 • **Interval** - 各スキャン間の時間間隔(時間)(たとえば、**12** 時間ごと) • **File Name** - エージェントスキャンをトリガーするファイル名[トリガーディレクトリ](#)でファイル名が検出されると、スキャンがトリガーされます。 **ヒント:** 1 回のスキャンに複数のトリガーを設定すると、スキャンはリストされた順序でトリガーを検索します(つまり、スキャンが 1 番目のトリガーでトリガーされない場合は、2 番目のトリガーを検索します)。 トリガーされたエージェントスキャンの詳細については、[トリガーされたエージェントスキャン](#)を参照してください。
情報レベルの	[トリガーされたエージェントス](#)	(Tenable Nessus Agent 脆弱性テンプレートのみ)(必須)エージェントスキャンが、深刻度が[情報](#)レベルで変更のない脆弱性検出結果を

レポート	キャン - 10 回のスキャン後 スキャンウィンドウのエージェントスキャン - 10 日後以降 **注意:** Tenable では、デフォルト値の使用を強く推奨しています。所属組織でそうする必要がある場合にのみ、この値を下げてください。	報告する頻度を指定します。この設定の詳細については、情報レベルのレポート を参照してください。 次のいずれかの間隔で新しいベースラインスキャンを起動することで、すべての深刻度の検出結果を報告するようにエージェントスキャンを設定できます。 • **数回のスキャン後** – エージェントスキャンは *x* 回のスキャンごとにすべての検出結果を報告します。7、10、15、20 回のスキャン増分から選択します。 • **数日後** – エージェントスキャンがすべての検出結果を最後に報告した前日から、設定した日数が経過した後に、エージェントスキャンがすべての検出結果を報告します。7、10、20、30、60、90 日のスキャン増分から選択します。 トリガーされたエージェントスキャンは、**[数回のスキャン後]** にのみ設定できます。スキャンウィンドウのスキャンは、**[数回のスキャン後]** または **[数日後]** のいずれかに設定できます。
ターゲットグループ	なし	スキャンを適用する新しいターゲットグループを選択または追加できます。ターゲットグループの資産は、スキャンターゲットとして使用されます。 **注意:** Tenable では、近い将来にターゲットグループを廃止する予定です。現在はまだ、ターゲットグループを作成および管理できます。ただし、Tenable は、代わりにタグを使用して Tenable Vulnerability Management インスタンス上の資産をグループ化してスキャンすることを推奨しています。
ターゲット	None (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。 指定するターゲットは、そのスキャンに選択したスキャナーに適切なものでなければなりません。たとえば、クラウドスキャナーはルーティングで

		きない IP アドレスをスキャンできません。代わりに内部スキャナーを選択してください。 **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 Vulnerability Management 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。ただし、スキャンに対してスキャンのルーティングを有効にしている場合は、この手法は取れません。 **注意:** 1 つのスキャンに 300,000 IP アドレスを超えるターゲットを適用することはできません。Tenable Vulnerability Management でのスキャン制限事項の詳細については、スキャン制限事項を参照してください。 **注意:** アクセス許可がターゲットに与える影響の詳細については、権限を参照してください。
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。
ポリシー	なし	この設定は、スキャンの所有者がユーザー定義のスキャンテンプレートに基づく既存のスキャンを編集する場合にのみ使用されます。 **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 が提供するスキャン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ユーザー定義スキャンテンプレートを選択します。**[表示可]** またはそれ以上のアクセス許可があるユーザー定義スキャンテンプレートをを選択できます。

		多くの場合、スキャン作成時にユーザー定義スキャンテンプレートを設定し、毎回のスキャンの実行時には同じテンプレートを適用し続けます。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ユーザー定義スキャンテンプレートを変更することも可能です。たとえば、テンプレートを変更すると、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テンプレートを適用したりすることが容易になります。 スキャン用にユーザー定義スキャンテンプレートを変更した場合、以前割り当てられていたテンプレート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。

スケジュール

スキャンスケジュール設定

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。

注意: スケジュールしたスキャンがスキャン所有者の **[ゴミ箱]** フォルダーにある場合は実行されません。

設定	デフォルト値	説明
頻度	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、同じ日時でスキャンするようスケジュールする場合、Tenable では、開始日を 28 日以前に設定することを推奨します。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 Vulnerability Management は、それらの日にはスキャンを実行できません。 • **年単位**: 時間と日付ごとに、1 ~ 20 年単位でスキャンの実行をスケジュールします。
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す。たとえば、2023 年 9 月 8 日午前 9 時 16 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 8 日 9 時 30 分*に設定されます。
タイムゾーン	Zulu	**[開始]** に設定された値のタイムゾーンを指定します。
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。
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。
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。
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

スキャンの通知設定

設定	デフォルト値	説明
E メールの受信者	なし	スキャンが完了して結果が参照可能になったときにアラートを受け取る、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。
結果フィルター	None (なし)	メールで送信する情報の種類を定義します。

ユーザーアクセス許可

ユーザーまたはグループにアクセス許可を設定して、他のユーザーにスキャンを共有できます。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。

ヒント: 個別のユーザーは企業を離れたり企業に加わったりすることがあるので、Tenable では、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
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、スキャンに関与することはできません。
表示可	このアクセス許可を持つグループとユーザーは、スキャン結果の表示、スキャン結果のエ

	クスポート、およびスキャンの**[ゴミ箱]**フォルダーへの移動を行うことが可能です。スキャンの設定を表示したり、スキャンを完全に削除したりすることはできません。
実行可	このアクセス許可を持つグループとユーザーは、**[表示可]**で許可されているタスクに加えて、スキャンの起動、一時停止、および停止が可能です。スキャンの設定を表示したり、スキャンを完全に削除したりすることはできません。 **注意:** スキャンを実行するユーザーは、スキャンに対する**[実行可]**アクセス許可に加えて、指定されたターゲット用のアクセスグループ内で**[スキャン可]**アクセス許可を持っている必要があります。そうでない場合、スキャナーはターゲットをスキャンしません。
編集可	このアクセス許可を持っているグループとユーザーは、**[実行可]**で許可されるタスクに加えて、スキャン設定を表示し、スキャンの所有権以外のスキャン設定を変更することができます。スキャンを削除することも可能です。 **注意:** スキャンの所有者のみがスキャンの所有権を変更できます。 **注意:** 次の場合では、スキャンのアクセス許可よりもユーザーロールが優先されます。 • 基本ユーザーが、個別のスキャンで割り当てられたアクセス許可にかかわらず、スキャンを実行および設定することができない場合 • 管理者は、個別のスキャンの管理者アカウントに設定されたアクセス許可にかかわらず、常に**[編集可]**に相当するアクセス許可を有します。これは、ユーザー定義のスキャンテンプレートには適用されません。

ユーザー定義テンプレートの基本設定

注意: このトピックでは、ユーザー定義テンプレートで設定できる**[基本]**設定について記載します。個別のスキャンでの**[基本]**設定に関しては、Tenable Vulnerability Management スキャンの基本設定を参照してください。

[基本]設定を使用することで、誰がユーザー定義テンプレートにアクセスできるかを含む、ユーザー定義テンプレートの基本的な側面を規定できます。

[基本]設定には、次のセクションが含まれます。

- 一般
- アクセス許可

一般

ユーザー定義テンプレートの一般的な設定です。

設定	デフォルト値	説明
名前	なし	ユーザー定義テンプレートの名前を指定します。
説明	なし	(オプション) ユーザー定義テンプレート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、他のユーザーにユーザー定義テンプレートを共有できます。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。

ヒント: 個別のユーザーは企業を離れたり企業に加わったりすることがあるので、Tenable では、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
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、スキャンに関与することはできません。
表示可	このアクセス許可を持つグループとユーザーは、スキャン結果の表示、スキャン結果のエ

	クスポート、およびスキャンの **[ゴミ箱]** フォルダーへの移動を行うことが可能です。スキャンの設定を表示したり、スキャンを完全に削除したりすることはできません。
実行可	このアクセス許可を持つグループとユーザーは、**[表示可]** で許可されているタスクに加えて、スキャンの起動、一時停止、および停止が可能です。スキャンの設定を表示したり、スキャンを完全に削除したりすることはできません。 **注意:** スキャンを実行するユーザーは、スキャンに対する **[実行可]** アクセス許可に加えて、指定されたターゲット用のアクセスグループ内で **[スキャン可]** アクセス許可を持っている必要があります。そうでない場合、スキャナーはターゲットをスキャンしません。
編集可	このアクセス許可を持っているグループとユーザーは、**[実行可]** で許可されるタスクに加えて、スキャン設定を表示し、スキャンの所有権以外のスキャン設定を変更することができます。スキャンを削除することも可能です。 **注意:** スキャンの所有者のみがスキャンの所有権を変更できます。 **注意:** 次の場合では、スキャンのアクセス許可よりもユーザーロールが優先されます。 • 基本ユーザーが、個別のスキャンで割り当てられたアクセス許可にかかわらず、スキャンを実行および設定することができない場合 • 管理者は、個別のスキャンの管理者アカウントに設定されたアクセス許可にかかわらず、常に **[編集可]** に相当するアクセス許可を有します。これは、ユーザー定義のスキャンテンプレートには適用されません。

認証

ユーザー定義テンプレートでは、**[認証]** 設定を使用して、専用認証スキャン時に Tenable Vulnerability Management が実行する認証を設定できます。

ヒント: **[認証]** 設定は、Tenable 提供のスキャンテンプレートにおける **[スキャン全体の認証情報タイプの設定]** と同等です。

設定	デフォルト値	説明
SNMPv1/v2c		

[スキャン] > [認証情報] > [プレーンテキスト認証] > [SNMPv1/v2c] と同等		
UDP ポート	161	Tenable Vulnerability Management がホストデバイスで認証を試みるポートです。
追加の UDP ポート #1	161	
追加の UDP ポート #2	161	
追加の UDP ポート #3	161	
HTTP		
[スキャン] > [認証情報] > [プレーンテキスト認証] > [HTTP] と同等		
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。
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。時間遅延を設定すると、ブルートフォースロックアウトメカニズムのトリガーの回避に利用できます。
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 30x 系のリダイレクトコードを受信した場合に、提供されたリンクに従うかどうかを、この設定で Tenable Vulnerability Management に指示します。
認証された正規表現の反転	無効	ログインページで検索する正規表現パターン。パターンが見つかった場合、認証が成功しなかったことが Tenable Vulnerability Management に通知されます。(例: 認証に失敗しました。)
認証された正規表現の HTTP ヘッダーで	無効	認証状態をより適切に判断するために、Tenable Vulnerability Management が与えられた正規表現パターンで、レスポンスの本文ではなく HTTP レスポンスヘッダーを検索することを許可します。

の使用		
大文字と小文字を区別しない認証された正規表現	無効	regex 検索は、デフォルトで大文字と小文字を区別します。このオプションでは、大文字と小文字を区別しないよう Tenable Vulnerability Management に指示します。
telnet/rsh/rexec		
[スキャン] > [認証情報] > [プレーンテキスト認証] > [telnet/ssh/rexec] と同等		
telnet を使用してパッチ監査を実行	無効	Tenable Vulnerability Management は、パッチ監査のために telnet を使用してホストデバイスに接続します。
rsh を使用してパッチ監査を実行	無効	Tenable Vulnerability Management は、パッチ監査のために rsh を使用してホストデバイスに接続します。
rexec を使用してパッチ監査を実行	無効	Tenable Vulnerability Management は、パッチ監査のために rexec を使用してホストデバイスに接続します。
Windows		
[スキャン] > [認証情報] > [ホスト] > [Windows] と同等		
暗号化されていない認証情報を送信しない	有効	デフォルトでは、セキュリティ上の理由からこのオプションは有効になっています。
NTLMv1 認証を使用し	有効	**[NTLMv1 認証を使用しない]** 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

ない		証情報を使用し、Tenable Vulnerability Management 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 Tenable Vulnerability Management 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めに使用される可能性もあります。スキャン時に **[NTLMv2 のみ使用]** 設定を有効にすると、Tenable Vulnerability Management 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 は安全でないプロトコルであるため、このオプションはデフォルトで有効になっています。
スキャン中にリモートレジストリを有効にする	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、それを開始するよう Tenable Vulnerability Management に指示します。Tenable Vulnerability Management 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。 **注意:** デフォルトのスキャンパフォーマンスを向上させるために、このオプションはデフォルトでは無効になっています。また、このオプションを有効にすることで、ネットワークセキュリティの実装によっては影響が生じる可能性があります。たとえば、ネットワークファイヤーウォールの特定のアクセス制御設定は、サーバーメッセージブロックプロトコル (SMB プロトコル) 接続のネゴシエートを試みるスキャナーをブラックリストに登録する場合があります。
スキャン中に管理共有を有効にする	無効	このオプションにより、Tenable Vulnerability Management は管理者権限で読み取り可能な特定のレジストリエントリにアクセスできます。 **注意:** デフォルトのスキャンパフォーマンスを向上させるために、このオプションはデフォルトでは無効になっています。また、このオプションを有効にすることで、ネットワークセキュリティの実装によっては影響が生じる可能性があります。たとえば、ネットワークファイヤーウォールの特定のアクセス制御設定は、サーバーメッセージブロックプロトコル (SMB プロトコル) 接続のネゴシエートを試みるスキャナーをブラックリス

		トに登録する場合があります。
SSH		
[スキャン] > [認証情報] > [ホスト] > [SSH] と同等		
known_hosts ファイル	なし	SSH known_hosts ファイルをアップロードすると、Tenable Vulnerability Management はこのファイルのホストに対してのみ、ログインを試みます。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。
優先ポート	22	ターゲットのシステムで SSH が実行されているポートです。
クライアントバージョン	OpenSSH_5.0	スキャン中に Tenable Vulnerability Management が偽装する SSH クライアントの種類を指定します。
最小限の権限を試行	未選択	動的な権限昇格を有効または無効にします。この機能を有効にすると、Tenable Vulnerability Management は、**[権限昇格方法]** オプション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 Vulnerability Management は権限を昇格させます。プラグイン 101975 および 101976 では、権限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。
Amazon AWS		
[スキャン] > [認証情報] > [クラウドサービス] > [Amazon AWS] と同等		
アクセスするリージョン	世界のその他の地域	Tenable Vulnerability Management が Amazon AWS アカウントを監査するには、スキャンする地域を定義する必要があります。Amazon のポリシーにより、中国地域のアカウント設定を監査するには、世界のその他の地域とは異なる認証情報が必要です。 可能性がある地域には次が含まれます。

		• **GovCloud** - この地域を選択すると、政府のクラウドが自動的に選択されます (例: us-gov-west-1)
		• **世界のその他の地域** - この地域を選択すると、次の追加オプションが表示されます。
		  • 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
		• **中国** - この地域を選択すると、次の追加オプションが表示されます。
		  • cn-north-1
		  • cn-northwest-1

HTTPS	有効	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management が認証するかどうかを設定します。
SSL 証明書を検証する	有効	Tenable Vulnerability Management が SSL デジタル証明書の有効性を確認するかどうかを設定します。

Rackspace		
[スキャン] > [認証情報] > [クラウドサービス] > [Rackspace] と同等		
場所	–	Rackspace クラウドインスタンスの場所です。可能性がある場所には次が含まれます。 • ダラスフォートワース (DFW) • シカゴ (ORD) • 北バージニア (IAD) • ロンドン (LON) • シドニー (SYD) • 香港 (HKG)
Microsoft Azure		
[スキャン] > [認証情報] > [クラウドサービス] > [Amazon AWS] と同等		
サブスクリプション ID	–	スキャンするサブスクリプション ID をコンマで区切ってリストします。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。
Apple プロファイルマネージャ		
[スキャン] > [認証情報] > [モバイル] > [Apple プロファイルマネージャ] と同等		
デバイスを強制的に更新	有効	Apple プロファイルマネージャを使用して直ちに、デバイスを強制的に更新します。
デバイス更新のタイムアウト (分)	5	デバイスが Apple プロファイルマネージャーに再接続するまでに待機する分数です。

トリガーされたエージェントスキャン

Tenable Vulnerability Management で Tenable Nessus Agent スキャンを設定するとき、Tenable Vulnerability Management には 2 つのエージェントスキャンタイプ (**スキャンウィンドウとトリガーされたスキャン**) があります。

ウィンドウスキャンの場合、Tenable Vulnerability Management は時間枠 (デフォルトでは 3 時間) を作成します。スキャン結果に含まれるには、エージェントグループがこの時間内にレポートする必要があります。スケジュールされた時間にウィンドウスキャンが起動するように Tenable Vulnerability Management をスケジュールするか、または Tenable Vulnerability Management のユーザーインターフェースから手動でスキャンを起動する必要があります (たとえば、毎週月曜日に 3 時間のエージェントウィンドウスキャンをスケジュールした場合、Tenable Vulnerability Management は毎週月曜日に 3 時間、データの更新内容をエージェントグループからプルします)。

トリガーされたスキャンがウィンドウエージェントスキャンと異なる点は、Tenable Vulnerability Management またはユーザーの介入なしでエージェントまたはエージェントグループがスキャンを起動することです。エージェントはトリガーされたスキャンを次の 3 種類の方法で起動できます。

- 間隔トリガー - 特定の時間間隔 (例: 12 時間ごとまたは 24 時間ごと) にスキャンを実行するようにエージェントを設定します。
- ファイル名トリガー - 特定の名前のファイルがエージェントトリガーディレクトリに追加されるたびにスキャンを実行するように、エージェントを設定します。トリガーファイルはスキャン開始後に消去されます。エージェントトリガーディレクトリの場所は、オペレーティングシステムによって異なります。

オペレーティングシステム	場所
Windows	`C:\ProgramData\Tenable\Nessus Agent\nessus\triggers`
macOS	`/Library/NessusAgent/run/var/nessus/triggers`
Linux	`/opt/nessus_agent/var/nessus/triggers`

- Nessuscli トリガー - Tenable Nessus Agent `-nessuscli` ユーティリティで次のコマンドを実行して、既存のトリガーされるスキャンを手動で起動します。

  ```
  # nessuscli scan-triggers --start --UUID=<scan-uuid>
  ```

また、1 回のスキャンに複数のトリガーを設定すると、スキャンではリストされた順序でトリガーを検索します(つまり、スキャンが 1 番目のトリガーでトリガーされない場合は、2 番目のトリガーを検索します)。

トリガーされたスキャンとウィンドウスキャン

Tenable では、多くの場合、ウィンドウエージェントスキャンよりもトリガーされたエージェントスキャンを使用することを推奨しています。Tenable Vulnerability Management からのスキャンの独立性、またはユーザー介入や複数のトリガーオプションの観点から、トリガーされたスキャンには、特に複数のタイムゾーンにモバイルワーカーがいる場合にワークフローのニーズに対応できる高い柔軟性があるためです。

トリガーされたスキャンは、ウィンドウスキャンよりも一貫性の高いカバレッジを提供し、Tenable Vulnerability Management とリンクされたエージェントの間の接続の問題を克服するのに役立ちます。ウィンドウスキャンでは、応答しないエージェントやオフラインエージェントが原因でデータカバレッジにギャップが生じる可能性がありますが、トリガーされたスキャンでは、トリガーが発生するたびにエージェントがデータをスキャンして Tenable Vulnerability Management に送信できます。Tenable Vulnerability Management は、トリガーされたスキャンからのデータをいつでも受け入れて処理します。

トリガーされたスキャンのデータをエクスポートするには、脆弱性一括エクスポート API を使うのが唯一の手段であるため、個別のスキャン結果をエクスポートする必要がある場合は、Tenable はスキャンウィンドウを使用することを推奨します。

トリガーされたスキャンの詳細の確認

トリガーされたスキャンの結果を表示するには、View Tenable Vulnerability Management Scan Detailsを参照してください。

注意: トリガーされたスキャン履歴については、Tenable Vulnerability Management では過去 7 日間の 12 時間ごとのスキャン履歴エントリが表示されます。Tenable Vulnerability Management は各スキャンで一度に最大 15 件のトリガーされたスキャン履歴のみを保持します。

トリガーされたスキャンを Tenable Vulnerability Management から管理できる他に、Tenable Nessus Agent `nessuscli` ユーティリティで次のコマンドを実行することで、トリガーされたスキャンの詳細を確認できます。

```
# nessuscli scan-triggers --list
```

`--list` コマンドは、エージェントでトリガーされたスキャンに関する詳細を返します。詳細には、以下が含まれます。

- スキャン名
- ステータス (**uploaded** 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
- 最新のポリシー変更の時間
- 最後に実行された時間
- スキャントリガーの説明
- スキャン設定テンプレート

  Tenable Nessus Agent `nessuscli` ユーティリティの詳細については、*Tenable Nessus ユーザーガイド*の Nessuscli Agent を参照してください。

また、エージェントトリガーディレクトリでエージェントトリガー情報を確認することもできます。

オペレーティングシステム	場所
Windows	`C:\ProgramData\Tenable\Nessus Agent\nessus\triggers`

macOS	`/Library/NessusAgent/run/var/nessus/triggers`
Linux	`/opt/nessus_agent/var/nessus/triggers`

ターゲットのスキャン

Tenable Vulnerability Management では、スキャンのターゲットを指定する際にさまざまな形式を使用できます。次の表に、ターゲットの形式、例、および Tenable Vulnerability Management がそのターゲットの種類をスキャンしたときに起こることについての簡単な説明を示します。

注意: Tenable では 1 回のスキャンでスキャンできるターゲットの数を制限しています。詳細は、スキャン制限事項 を参照してください。

注意: 過去にスキャンした資産に関しては、IP アドレスのようなホストの識別子の代わりに、オペレーティングシステムやインストールされたソフトウェアなどのホストの属性に基づいてスキャンターゲットを設定できます。

ヒント: ホスト名のターゲットが link6 ターゲット (「link6」のテキストで始まる) か、または 2 種類の IPv6 範囲形式のうちの 1 つのように見える場合は、ターゲットを一重引用符で囲むことで、Tenable Vulnerability Management によってホスト名として確実に処理されるようにしてください。

ターゲットの説明	例	説明
1 つの IPv4 アドレス	192.168.0.1	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	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	1 つの IPv6 アドレスをスキャンします。Windows プラットフォームでは、スコープ識別子にインターフェース名ではなくインターフェースインデックスを使用する必要があります。
IPv4 アドレスのリスト	192.168.0.1, 192.168.0.32, 192.168.0.200, 192.168.0.255	異なる IPv4 アドレスのリストをスキャンします。
開始アドレスと終了アドレスで指	192.168.0.1-192.168.0.255	開始アドレスと終了アドレスの間のすべての IPv4 アドレス (開始アドレスと終了アドレスを含む) をスキャンします。

ターゲットの説明	例	説明
定した IPv4 範囲		
最後のオクテット範囲が数値範囲に置き換えられた IPv4 アドレス	192.168.0-1.3-5	オクテット範囲で指定された値のすべての組み合わせをスキャンします。この例では、次の組み合わせをスキャンします。192.168.0.3、192.168.0.4、192.168.0.5、192.168.1.3、192.168.1.4、192.168.1.5
CIDR 表記の IPv4 サブネット	192.168.0.0/24	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	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。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	1 つのホストをスキャンします。 Tenable Vulnerability Management によりホスト名が複数のアドレスに解決できる場合は、Tenable Vulnerability Management は解決された最初の IPv4 アドレスをスキャンします。Tenable Vulnerability Management が IPv4 アドレスに解決

ターゲットの説明	例	説明
		できない場合は、解決された最初の IPv6 アドレスをスキャンします。
CIDR 表記で IPv4 アドレスに解決可能なホスト	www.yourdomain.com/24	ホスト名を IPv4 アドレスに解決した後、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。 Tenable Vulnerability Management はこの形式を、他の CIDR 表記の IPv4 アドレスと同じように扱います。
ネットマスク表記の IPv4 アドレスに解決できるホスト	www.yourdomain.com/255.255.252.0	ホスト名を IPv4 アドレスに解決した後、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。 Tenable Vulnerability Management はこの形式を、他のネットマスク表記の IPv4 アドレスと同じように扱います。
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	スコープ識別子で指定されたインターフェースで ff02::1 アドレスに送信されるマルチキャスト ICMPv6 エコー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 スコープ識別子が指定されていない場合、リクエストはすべてのインターフェースに送信されます。Windows プラットフォームでは、スコープ識別子にインターフェース名ではなくインターフェースインデックスを使用する必要があります。
角括弧に囲まれた、1 つの IPv4 アドレスま	"Test Host 1[10.0.1.1]" または "Test Host 2 [2001:db8::abcd]"	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。

ターゲットの説明	例	説明
たは IPv6 含む何らかのテキスト		

ターゲットグループ

ターゲットグループを使用して、スキャンターゲットを管理することもできます。ただし Tenable では、可能であれば、代わりにタグを使用して資産をグループ化してスキャンすることを推奨しています。将来的に、タグ付け機能とオプションがターゲットグループで現在使用可能なものと一致する場合は、Tenable がターゲットグループをタグに変換し、既存のターゲットグループを廃止する予定です。ユーザー側のアクションは必要ありません。Tenable は、ターゲットグループを変換して廃止する 60 暦日前に通知を行います。詳細については、Tenable の担当者までお問い合わせください。

ターゲットグループにより、FQDN、CIDR 表記、または IP アドレス範囲でスキャンターゲットのリストを設定することができます。そしてそのターゲットグループを、企業のどのユーザーがスキャンの設定や(ワークベンチを含む)ダッシュボードのフィルタリングに使用できるのかを指定できます。

注意: Tenable では、1 つのターゲットグループ内にあるターゲット数を制限することをお勧めします。ターゲット数が多すぎるターゲットグループでダッシュボードをフィルタリングすると、Tenable Vulnerability Management はデータを表示できない場合があります。

注意: CIDR 表記でリストされたスキャンターゲットは、次のいずれかの形式である必要があります。

- xx.xx.0.0/16
- xx.xx.xx.0/24

ユーザーにターゲットグループのアクセス許可を付与すると、そのユーザーはスキャン設定の **[ターゲットグループ]** オプションで、そのターゲットグループを使用できるようになります。しかし、そのユーザーには、アクセスグループ内でそのターゲットに対する **[スキャン可]** アクセス許可も付与しなければなりません。そうしないと、Tenable Vulnerability Management はそのターゲットをスキャン結果から除外します。詳細は、権限を参照してください。

ターゲットグループを管理するには、次の手順を使用します。

ターゲットグループの作成

システムターゲットグループ

必要なユーザーロール: 管理者

ユーザーターゲットグループ

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

新しいインターフェースでターゲットグループを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[ターゲットグループ]** タイルをクリックします。

   [ターゲットグループ] ページが表示されます。デフォルトでは、**[システム]** タブがアクティブとなっています。このタブには、システムターゲットグループの表が含まれます。

4. ユーザーターゲットグループを編集する場合は、**[ユーザー]** をクリックします。編集しない場合は、**[システム]** ターゲットグループタブにとどまります。

5. ページの右上にある ⊕ **[ターゲットグループの作成]** ボタンをクリックします。

   [ターゲットグループの作成] ページが表示されます。

6. **[一般]** 設定を行います。

設定	説明
名前	ターゲットグループの名前
ターゲット	FQDN、CIDR 表記、または IP アドレスのコンマ区切りのリスト **注意:** CIDR 表記でリストされたスキャンターゲットは、次のいずれかの形式である必要があります。 • xx.xx.0.0/16 • xx.xx.xx.0/24 **注意**: IP アドレス範囲の形式 (例: 192.168.0.1-192.168.0.255) では、Tenable Vulnerability Management は「-」から 1023 までの最大数をサポートします。
ターゲットのアップロード	スキャンする FQDN または IP アドレス範囲のコンマ区切りのリストを含むテキストファイル

設定	説明
	システムは、ターゲットグループが保存された後、アップロードされたターゲットを **[ターゲット]** ボックスに追加します。

7. グループのユーザーアクセス許可を設定します。

   注意: ユーザーにターゲットグループのアクセス許可を付与すると、そのユーザーはスキャン設定の **[ターゲットグループ]** オプションで、そのターゲットグループを使用できるようになります。しかし、そのユーザーには、アクセスグループ内でそのターゲットに対する **[スキャン可]** アクセス許可も付与しなければなりません。そうしないと、Tenable Vulnerability Management はそのターゲットをスキャン結果から除外します。詳細については、アクセスグループを参照してください。

8. **[保存]** をクリックします。

   次のうちのいずれかが起こります。

   - ターゲットグループのユーザーアクセス許可を設定した場合、Tenable Vulnerability Management はターゲットグループを作成し、それを **[ターゲットグループ]** ページ上の表に追加します。
   - ターゲットグループに対してデフォルトの **[アクセスなし]** アクセス許可を維持した場合、確認ウィンドウが表示されます。

     これに対し、次のうちのどちらかを選択します。

     - そのターゲットグループに対してデフォルトの設定が適切な場合は、**[続行]** をクリックしてアクションを確定します。
     - そのターゲットグループに対してデフォルトの設定が適切ではない場合は、**[キャンセル]** をクリックしてターゲットグループのユーザーアクセス許可の設定に戻ります。

ターゲットグループのユーザーアクセス許可の設定

システムターゲットグループ

必要なユーザーロール: 管理者

必要なターゲットグループのアクセス許可: Any

ユーザーターゲットグループ

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なターゲットグループのアクセス許可: 変更可

注意: クラウドインフラを監査するために、Tenable Vulnerability Management では、**[スキャン可]** アクセス許可を持つターゲットグループが 127.0.0.1 上に存在する必要があります。

注意: ユーザーがスキャン設定の **[ターゲットグループ]** オプションでターゲットグループを使用できるようにするには、ターゲットのアクセスグループでそのユーザーに **[スキャン可]** アクセス許可を付与する必要もあります。付与しなかった場合は、Tenable Vulnerability Management によりスキャン結果からそのターゲットが除外されます。詳細については、アクセスグループを参照してください。

ターゲットグループのアクセス許可を設定する方法

1. ターゲットグループを作成または編集します。
2. **[ユーザーのアクセス許可]** セクションで、次のいずれかを行います。

   - **[デフォルト]** ユーザーのアクセス許可を変更する

     注意: **[デフォルト]** ユーザーとは、ターゲッ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. **[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. **[保存]** をクリックします。

   - アクセス許可を追加する

     a. **[ユーザーアクセス許可]** の横にある ⊕ ボタンをクリックします。

     [ユーザーアクセス許可の追加] プレーンが表示されます。

     b. **[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。

c. 検索結果からユーザーまたはグループを選択します。

選択したユーザーまたはグループが、ユーザーとグループのリストに表示されます。

デフォルトでは、Tenable Vulnerability Management は**[使用可]**アクセス許可を新しいユーザーまたはグループに割り当てます。

d. ユーザーまたはグループ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。

e. アクセス許可レベルを選択します。

f. **[保存]**をクリックします。

- アクセス許可を編集する

a. ユーザーまたはグループ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. **[保存]**をクリックします。

- アクセス許可を削除する

a. ユーザーのリストで、削除するユーザーまたはグループにカーソルを合わせます。

b. その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。

ユーザーまたはグループがアクセス許可リストから削除されます。

c. **[保存]**をクリックします。

ターゲットグループの編集

システムターゲットグループ

必要なユーザーロール: 管理者

必要なターゲットグループのアクセス許可: Any

ユーザーターゲットグループ

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なターゲットグループのアクセス許可: 変更可

注意: システムターゲットグループ、および関連する機能である資産分離は廃止されました。スキャンのアクセス許可を制御するには、代わりにアクセスグループを使用します。

システムターゲットグループを作成したり、スキャン設定やダッシュボードフィルターでシステムターゲットグループを使用したりすることは現在でも可能です。しかし、Tenable では代わりにユーザーターゲットグループを使用することを推奨します。

新しいインターフェースでターゲットグループを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[ターゲットグループ]** タイルをクリックします。

   [ターゲットグループ] ページが表示されます。デフォルトでは、**[システム]** タブがアクティブとなっています。このタブには、システムターゲットグループの表が含まれます。

4. ユーザーターゲットグループを編集する場合は、**[ユーザー]** をクリックします。そうでない場合は、**[システム]** ターゲットグループタブにとどまります。

5. ターゲットグループの表で、編集するターゲットグループをクリックします。

   [ターゲットグループの更新] ページが表示されます。

6. ターゲットグループの **[一般]** 設定を編集します。

設定	説明
名前	ターゲットグループの名前
Targets	スキャンする FQDN、CIDR 表記、または IP アドレス範囲のコンマ区切りのリスト

設定	説明
Upload Targets	スキャンする FQDN または IP アドレス範囲のコンマ区切りのリストを含むテキストファイル システムは、ターゲットグループが保存された後、アップロードされたターゲットを **[ターゲット]** ボックスに追加します。

7. ターゲットグループのユーザーのアクセス許可を設定します。
8. **[保存]** をクリックします。

   確認ウィンドウが表示されます。
9. 確認ウィンドウで、**[続行]** をクリックします。

   Tenable Vulnerability Management により変更内容がターゲットグループに保存されます。

ターゲットグループのインポート

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

ターゲットグループを .csv ファイルによりインポートすることができます。

ヒント: .csv ファイルの作成または変更に際して、Tenable では Microsoft Excel などの堅牢なエディターの使用を推奨します。

始める前に

- 指定された形式で .csv ファイルを作成します。

ターゲットグループをインポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。
2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。
3. **[ターゲットグループ]** タイルをクリックします。

[ターゲットグループ] ページが表示されます。デフォルトでは、**[システム]** タブがアクティブとなっています。このタブには、システムターゲットグループの表が含まれます。

4. ユーザーターゲットグループをインポートする場合は、**[ユーザー]** をクリックします。編集しない場合は、**[システム]** ターゲットグループページにとどまります。

   > **注意:** システムターゲットグループ、および関連する機能である資産分離は廃止されました。スキャンのアクセス許可を制御するには、代わりにアクセスグループを使用します。
   >
   > システムターゲットグループを作成したり、スキャン設定やダッシュボードフィルターでシステムターゲットグループを使用したりすることは現在でも可能です。しかし、Tenable では代わりにユーザーターゲットグループを使用することを推奨します。

5. ページの右上の **[インポート]** ボタンをクリックします。

   オペレーティングシステムのファイルマネージャーが表示されます。

6. インポートする `.csv` ファイルを選択します。

   Tenable Vulnerability Management によりファイルがインポートされ、ターゲットグループがターゲットグループボックスに追加されます。

ターゲットグループのインポートファイル形式

ターゲットグループのインポートファイルの各行には、次のフィールドがある必要があります。

フィールド名	説明
`id`	ターゲットグループの識別に使用される数値フィールド
`name`	ターゲットグループ名の識別に使用されるフィールド **name** フィールドでは英数字またはシンボルを任意に組み合わせて使用できます。
`members`	ターゲットグループに含まれるホストアドレスの識別に使用されるフィールド。
`creation_date`	UNIX タイムスタンプ形式の数値フィールド
`last_modification_date`	UNIX タイムスタンプ形式の数値フィールド

ターゲットグループのエクスポート

必要な Tenable Vulnerability Management ユーザーロール: 標準、スキャンマネージャー、または管理者

必要なターゲットグループのアクセス許可: 使用可

ターゲットグループを .csv ファイルとしてエクスポートできます。使用するブラウザによっては、ターゲットグループが自動的にダウンロードされる場合があります。

新しいインターフェースで 1 つまたは複数のターゲットグループをエクスポートする場合、

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[ターゲットグループ]** タイルをクリックします。

   [ターゲットグループ] ページが表示されます。デフォルトでは、**[システム]** タブがアクティブとなっています。このタブには、システムターゲットグループの表が含まれます。

4. ユーザーターゲットグループをエクスポートするには、**[ユーザー]** をクリックします。そうでない場合は、**[システム]** ターゲットグループタブにとどまります。

   注意: システムターゲットグループ、および関連する機能である資産分離は廃止されました。スキャンのアクセス許可を制御するには、代わりにアクセスグループを使用します。

   システムターゲットグループを作成したり、スキャン設定やダッシュボードフィルターでシステムターゲットグループを使用したりすることは現在でも可能です。しかし、Tenable では代わりにユーザーターゲットグループを使用することを推奨します。

5. エクスポートする 1 つまたは複数のターゲットグループを選択します。

   - 1 つのターゲットグループを選択します。

     a. ターゲットグループの表で、エクスポートするターゲットグループにカーソルを合わせます。

        アクションボタンが行に表示されます。

     b. 行にある [→ ボタンをクリックします。

Tenable Vulnerability Management は選択された 1 つまたは複数のターゲットグループを、1 つの .csv ファイルとして自動的にエクスポートします。

- 複数のターゲットグループを選択します。

  a. ターゲットグループの表で、エクスポートする各ターゲットグループのチェックボックスを選択します。

  ページの下部またはに、アクションバーが表示されます。

  b. **[ターゲットグループ]** の横にある [→ ボタンをクリックします。

ターゲットグループエクスポートファイルのヘッダーフィールド

次の表は、除外のエクスポートファイルに表示されるヘッダーについて説明しています。

フィールド名	説明
id	ターゲットグループの数値識別子
名前	英数字によるターゲットグループの名前
メンバー	ターゲットグループに含まれる 1 つ以上のホストアドレス
creation_date	ターゲットグループの作成日 (UNIXタイムスタンプ形式)
last_modification_date	ターゲットグループの最終変更日 (UNIX タイムスタンプ形式)

ターゲットグループの削除

システムターゲットグループ

必要なユーザーロール: 管理者

必要なターゲットグループのアクセス許可: Any

ユーザーターゲットグループ

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なターゲットグループのアクセス許可: 変更可

新しいインターフェースでターゲットグループを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[ターゲットグループ]** タイルをクリックします。

   [ターゲットグループ] ページが表示されます。デフォルトでは、**[システム]** タブがアクティブとなっています。このタブには、システムターゲットグループの表が含まれます。

4. ユーザーターゲットグループを削除する場合は、**[ユーザー]** をクリックします。そうでない場合は、**[システム]** ターゲットグループタブにとどまります。

5. 削除する 1 つまたは複数のターゲットグループを選択します。

   - 1 つのターゲットグループを選択します。

     a. ターゲットグループの表で、削除するターゲットグループにカーソルを合わせます。

        アクションボタンが行に表示されます。

     b. 行にある 🗑 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。

   - 複数のターゲットグループを選択します。

     a. ターゲットグループの表で、削除する各ターゲットグループのチェックボックスを選択します。

        ページの下部またはに、アクションバーが表示されます。

     b. アクションバーで、🗑 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。

6. 確認ウィンドウで、**[削除]** をクリックします。

Tenable Vulnerability Management により、選択した 1 つまたは複数のターゲットグループが削除されます。

ターゲットグループのアクセス許可

次の表では、システムターゲットグループとユーザーターゲットグループの両方に対して、ユーザーのアクセス許可について説明します。

アクセス許可	説明
システムターゲットグループ	
アクセスなし	(デフォルトユーザーのみ) このアクセス許可を割り当てられたユーザーは、システムターゲットグループを使用してダッシュボードをフィルタリングすることはできません。
使用可	**注意:** システムターゲットグループは廃止されます。Tenable では代わりにユーザーターゲットグループの使用を推奨しています。 このアクセス許可を割り当てられたユーザーは、ユーザーターゲットグループのホストを使用してダッシュボードをフィルタリングしたり、スキャンを設定したりできます。 **注意:** ユーザーがスキャン設定の **[ターゲットグループ]** オプションでターゲットグループを使用できるようにするには、ターゲットのアクセスグループでそのユーザーに **[スキャン可]** アクセス許可を付与する必要もあります。付与しなかった場合は、Tenable Vulnerability Management によりスキャン結果からそのターゲットが除外されます。詳細については、アクセスグループを参照してください。
ユーザーターゲットグループ	
アクセスなし	(デフォルトユーザーのみ) このアクセス許可を割り当てられたユーザーは、ユーザーターゲットグループのホストのスキャンを設定することや、ユーザーターゲットグループのホストを使用してダッシュボードをフィルタリングすることはできません。
使用可	このアクセス許可を割り当てられたユーザーは、ユーザーターゲットグループのホストを使用してダッシュボードをフィルタリングしたり、スキャンを設定したりできます。 **注意:** ユーザーがスキャン設定の **[ターゲットグループ]** オプションでターゲットグループを使用できるようにするには、ターゲットのアクセスグループでそのユーザーに **[スキャン可]** アクセス

	許可を付与する必要もあります。付与しなかった場合は、Tenable Vulnerability Management によりスキャン結果からそのターゲットが除外されます。詳細については、アクセスグループを参照してください。
Can Change	このアクセス許可を割り当てられたユーザーは、スキャンの設定時やダッシュボードのフィルタリング時にユーザーターゲットグループのホストを使用することに加えて、ターゲットグループのアクセス許可以外のあらゆる設定を変更することが可能です。

情報レベルのレポート

情報レベルのレポートは、Nessus Agent 脆弱性スキャンテンプレートに使用できるスキャン設定です。この設定によって、深刻度が情報レベルで変更のない脆弱性検出結果を報告する頻度を指定します。

説明

深刻度が情報レベルの検出結果は、エージェントスキャンの検出結果の最大 90% を占める可能性があります。ほとんどの情報レベルの検出結果は、スキャンを重ねても変わらず、ネットワークのサイバーエクスポージャー全体への影響は非常に限られています。**[情報レベルのレポート]** を設定することで、毎回のエージェントスキャンで Tenable Vulnerability Management が処理する、深刻度が情報レベルで変更のない検出結果の数を減らし、スキャン処理時間を最小限に抑えることができます。

エージェントスキャンの設定後、そのスキャンを最初に実行したときには、深刻度レベルに関係なく、検出されたすべての結果が常にレポートされます。これはベースラインスキャンと呼ばれます。2 回目以降のスキャンでは、深刻度が [低] 以上のすべての脆弱性検出結果と、新規または変更ありの情報レベルの検出結果が返されます。エージェントは、新しいベースラインスキャンが実行されるまで、変更のない既出の情報レベルの検出結果を Tenable Vulnerability Management に再報告しません。

エージェント脆弱性スキャン結果を Tenable Vulnerability Management ユーザーインターフェースで表示すると、ベースラインスキャンはベースラインアイコン () で次のように示されます。

注意: スキャンがベースラインスキャンであったかどうかにかかわらず、トリガーされたスキャンにはベースラインアイコンは表示されません。

スキャン設定に**[情報レベルのレポート]**設定がないスキャンには、ベースラインアイコンが常に表示されます。そのようなスキャンでは毎回すべての検出結果が含められ、結果的にベースラインスキャンになるためです。

その設定に**[情報レベルのレポート]**設定があるものの、**[情報レベルのレポート]**機能がリリースされる前に実行されたスキャンには、ベースラインアイコンは表示されません。

設定

次のいずれかの間隔で新しいベースラインスキャンを起動することで、すべての深刻度の検出結果を報告するようにエージェントスキャンを設定できます。

- **数回のスキャン後** – エージェントスキャンは *x* 回のスキャンごとにすべての検出結果を報告します。7、10、15、20 回のスキャン増分から選択します。

  たとえば、この値をデフォルトの 10 に設定した場合、エージェントスキャンは次のスキャンですべての検出結果を報告し、それから 10 回目のスキャンごとに再びすべての検出結果を報告します。その間のすべてのスキャンでは、深刻度が [低] 以上の検出結果と、新規または変更ありの情報レベルの検出結果のみが返されます。

- **数日後** – エージェントスキャンがすべての検出結果を最後に報告した前日から、設定した日数が経過した後に、エージェントスキャンがすべての検出結果を報告します。7、10、20、30、60、90 日のスキャン増分から選択します。

  たとえば、この値をデフォルトの 10 に設定した場合、エージェントスキャンは次のスキャンですべての検出結果を報告します。10 日の間のすべてのスキャンでは、深刻度が [低] 以上の検出結果と、新規または変更ありの [情報] レベルの検出結果が返されます。10 日が経過すると、エージェントスキャンは次のスキャンですべての検出結果を再び報告します。

  トリガーされたエージェントスキャンは、**[数回のスキャン後]** にのみ設定できます。スキャンウィンドウのスキャンは、**[数回のスキャン後]** または **[数日後]** のいずれかに設定できます。

  トリガーされたエージェントスキャンのデフォルト値は **10 回のスキャン後** で、スキャンウィンドウのエージェントスキャンのデフォルト値は **10 日後** です。Tenable では、デフォルト値の使用を推奨しています。所属組織でそうする必要がある場合にのみ、この値を下げてください。

[情報レベルのレポート] に加えて、**[次のスキャン時にすべての情報深刻度の脆弱性を強制的に更新します]** を有効にして、次のスキャンですべての検出結果をエージェントスキャンでレポートするように強制できます。次のスキャンが完了してすべての検出結果を報告した後に深刻度が情報レベルの検出結果をスキャンが報告する頻度は、**[情報レベルのレポート]** 設定によって決まります。

> **注意:** 深刻度が [低] 以上、または深刻度が情報レベルでも新規または変更ありの脆弱性については、すべての脆弱性検出結果が毎回のスキャン後に常に報告されます。

制限と考慮事項

- **[情報レベルのレポート]** 設定を使用できるのは、エージェントのバージョン 10.5.0 以降のみです。これより以前のバージョンのエージェントは、常にベースラインスキャンを実行します。
- Tenable Vulnerability Management が Tenable Security Center に接続されている場合、**[情報レベルのレポート]** 設定はサポートされません。
- [コンプライアンス] が設定されているエージェントスキャンでは、**[情報レベルのレポート]** 設定はサポートされません。[コンプライアンス] が設定されているエージェントスキャンはすべてベースラインスキャンになります。
- 情報レベルのプラグインをより高い深刻度レベル (例: [低] または [中]) に変更した場合、そのプラグインは引き続き **[情報レベルのレポート]** の影響を受け、プラグイン出力に変更がない場合は非ベースラインスキャンから除外されます。
- 各エージェントは、**[数回のスキャン後]** の値を個別に計算します。したがって、トリガーされたスキャンは、ベースラインと非ベースラインの結果を組み合わせたものを返す場合があります。
- 各スキャンでは常に、プラグイン 19506 (Nessus スキャン情報) および 42980 (SSL 証明書の有効期限) のフルレポートが生成されます。

Tenable Vulnerability Management スキャンの検出設定

注意: スキャンがユーザー定義テンプレートに基づいている場合、スキャンの **[検出]** 設定は設定できません。これらの設定は、関連するユーザー定義テンプレートでのみ変更できます。

[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。

- ホスト検出
- ポートスキャン
- サービス検出

ホスト検出

[ホスト検出] セクションのいくつかの設定は、デフォルトで有効です。最初に **[ホスト検出]** セクションにアクセスすると、**[リモートホストに ping を実行]** オプションが **[オン]** に設定された状態で表示されます。

設定	デフォルト値	説明
Ping the Remote Host	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。
応答しないホストのスキャン	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		
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 Vulnerability Management 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ようとします。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 Vulnerability Management 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	有効	TCP を使用してホストに ping を実行します。
Destination Ports (TCP)	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	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	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。
UDP	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。
Maximum Number of Retries	2	リモートホストに ping を再試行する回数を指定します。
脆弱なデバイス		
ネットワークプリンターをスキャン	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。
Scan Novell Netware Hosts	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	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		

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)	5 分	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

[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含まれています。

設定	デフォルト値	説明
ポート		
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。
ポートのスキャン範囲	Default (デフォルト)	スキャンされるポートの範囲を指定します。 サポートするキーワードの値は以下のとおりです。 • [デフォルト] は、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。 • [すべて] は、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。 また、コンマ区切りのポートリストまたはポート範囲を使用して、カ

設定	デフォルト値	説明
		スタムリストを指定することもできます。たとえば、「21,23,25,80,110」または「1-1024,8080,9000-9200」と入力します。ポート 0 以外のすべてのポートをスキャンする場合は、「1-65535」と入力します。 ポートスキャンに指定したカスタム範囲は、**[Network Port Scanners]**(ネットワークポートスキャナー)設定グループで選択したプロトコルに適用されます。 TCP と UDP の両方をスキャンする場合は、各プロトコルに固有の分割範囲を指定できます。たとえば、同じポリシーで TCP と UDP の異なる範囲のポートをスキャンする場合は、「T:1-1024,U:300-500」と入力します。 両方のプロトコルでスキャンするポートのセットを指定したり、プロトコルごとに個別の範囲を指定したりすることもできます。たとえば、「1-1024,T:1024-65535,U:1025」と入力します。
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、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。
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

設定	デフォルト値	説明
		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。
SNMP	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。
ローカルポートの列挙が失敗した場合にのみネットワークポートスキャンを実行	有効	ローカルポート列挙子が実行されると、その資産に対して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。
ローカルポートエニュメレーターによって検出された開いている TCP ポートを確認	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。

設定	デフォルト値	説明
SYN	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。
ファイヤーウォールの自動検出をオーバーライド	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

[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。

設定	デフォルト値	説明
全般設定		
すべてのポートをプローブしてサービスを見つける	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/TLS Based Services	日付を指定	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)		
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2 つのオプションがあります。 • **既知の SSL/TLS ポート** • **すべての TCP ポート**
Search for DTLS On	None (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。 • **None (なし)** • **既知の SSL/TLS ポート**

設定	デフォルト値	説明
		• **すべての TCP ポート**
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。
SSL/TLS 暗号をすべて列挙	真	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 the Internet)	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。

設定済みの Discovery 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
脆弱性スキャン（共通）		
高度なネットワークスキャン	–	すべてデフォルト
基本的な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
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)
	カスタム	すべてデフォルト
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 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)
	カスタム	すべてデフォルト
内部 PCI ネットワークスキャン	**ポートスキャン (共通**	• 全般設定

	ポート)(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 • 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)
	カスタム	すべてデフォルト
従来のウェブアプリケーションスキャン	**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)
	カスタム	すべてデフォルト
モバイルデバイススキャン	–	–
PCI 四半期毎外部スキャン	–	**[応答しないホストのスキャン]** のデフォルト
設定スキャン		
クラウドインフラ監査	–	–
内部 PCI ネットワークスキャン	–	–
オフライン設定監査	–	–
ポリシーコンプライアンス監査	**Default** (デフォルト)	• 全般設定 : ◦ Ping the remote host

		◦ ローカルの Tenable 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
	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)
	カスタム	すべてデフォルト
戦術スキャン		
Badlock 検出	**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 • 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
	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 • 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 • 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 検出	**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

		• 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
	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 • 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 • 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 検出	**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 • 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
	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 • 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 • 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
	カスタム	すべてデフォルト
Intel AMT セキュリティバイパス	**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 • 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
	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 • 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 • 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
	カスタム	すべてデフォルト
マルウェアのスキャン	**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)
	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
	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 • 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 • 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
	カスタム	すべてデフォルト
Spectre および Meltdown 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 • 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 • 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
	カスタム	すべてデフォルト
WannaCry Ransomware Detection	**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 • 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
	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 • 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 • 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
	カスタム	すべてデフォルト

Tenable Vulnerability Management スキャンの評価設定

注意: スキャンがユーザー定義テンプレートに基づいている場合、スキャンの **[評価]** 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テンプレート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。

- 一般
- 総当たり
- SCADA
- ウェブアプリケーション
- Windows
- マルウェア
- データベース

注意: 次の表には、**[高度なネットワークスキャン]** 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		
通常の冗長性をオーバーライド	無効	場合によっては、欠陥が存在するかどうかをTenable Vulnerability Management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 Vulnerability Management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します。そのため、状況によってはネットワークトラフィックと分析の負荷が増加する可能性があります。より詳細にすることにより、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	0	日数(0-7)を設定して、ウィルス対策ソフトウェアチェックの延期を設定します。ウィ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、ウィ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 Vulnerability Managementに指示できます。Tenable

義の猶予期間 (日))		Vulnerability Management のデフォルト設定では、署名の期限切れは、更新ソフトが利用可能になった時期 (数時間前など) を考慮しません。このオプションでは、期限切れと報告され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 Vulnerability Management 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、スキャンされるサイトまたはスキャンを実行するサイトの範囲外にある必要があります。それ以外の場合は、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。	
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されたアドレスから発信されたように表示されます。	
送信先アドレス	Tenable Vulnerability Management 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 データベース

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	Enabled (有効)	状況によっては、Tenable Vulnerability Management 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。そのような場合、試行が連続して無効になる回数が多すぎると、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、アカウントがロックアウトされる可能性があります。デフォルトでは、Tenable Vulnerability Management がこれらのテストを実行できないよう、この設定は

す)		有効になっています。
Oracle データベース		
Test default accounts (slow) (テストのデフォルトアカウント (低速))	Disabled (無効)	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す。

SCADA

設定	デフォルト値	説明
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。

ウェブアプリケーション

[ウェブアプリケーション] セクションには、次の設定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
ウェブアプリケーションのスキャン	無効	デフォルトでは、Tenable Vulnerability Management はウェブアプリケーションをスキャンしません。次の設定を編集するには、この設定を有効にします。
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 Vulnerability Management がスキャン中に偽装するウェブブラウザの種類を指定します。

設定	デフォルト値	説明
Web クローラ		
クロールの開始点	/	テストされる最初のページの URL です。複数のページが必要な場合は、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 Vulnerability Management は文字列の照合と処理のため、Perl 互換の正規表現 (PCRE) と同様に POSIX の正規表現をサポートしています。
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 (クロールできる最大深度)	6	開始ページごとに Tenable Vulnerability Managementがたどるリンクの数を制限します。
動的に生成されたページに従う	無効	選択すると、Tenable Vulnerability Management は動的リンクをたどり、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	無効	次の設定を有効にします。

設定	デフォルト値	説明
ケーションテストを有効にする)		
Abort web application tests if HTTP login fails	Disabled (無効)	Tenable Vulnerability Management 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)	無効	このオプションは、Web フォームのテストを強化する目的で POST リクエストも使用するよう Tenable Vulnerability Management 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。有効にすると、Tenable Vulnerability Management 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。

設定	デフォルト値	説明
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 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)	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 Vulnerability Management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

設定	デフォルト値	説明
		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 Vulnerability Management 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 Vulnerability Managementは /test.php?a=XSS&b=3&c=3&d=3をテストしません。 • **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

設定	デフォルト値	説明
		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。
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	Stop after one flaw is found per web server (fastest)	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 Vulnerability Management 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

設定	デフォルト値	説明
		るとすぐに、Tenable Vulnerability Management 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。
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 Vulnerability Management は Tenable 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。
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		
SMBドメインに関する情報をリクエストする	有効	有効にすると、ローカルユーザーの代わりにドメインユーザーが照会されます。
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 Vulnerability Management 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 Vulnerability Management 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、**[認証情報]** > **[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 Vulnerability Management は、Windows Management Interface (WMI) を介してユーザーを列挙します。
RID Brute Forcing	有効	Tenable Vulnerability Management 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。
Enumerate Domain Users (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 Vulnerability Management 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	1200	Tenable Vulnerability Management がドメインユーザーの列挙

UID)		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 Vulnerability Management 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 Vulnerability Management 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
- ハッシュおよびホワイトリストファイル
- Yara Rules (Yara ルール)
- ファイルシステムスキャン

設定	デフォルト値	説明
全般設定		
Disable DNS resolution (DNS 解決を無効にする)	Disabled (無効)	このオプションをオンにすると、Tenable Vulnerability Management はクラウドを使用してスキャン結果を既知のマルウェアと比較することができなくなります。
ハッシュおよび許可リストファイル		
カスタム Netstat IP 脅威リスト	None (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	追加の既知の不良な MD5 ハッシュを指定する、1 行に 1 つの MD5 ハッシュを含むテキストファイル オプションとして、ハッシュの後にコンマを追加してその後に説明を続けると、ハッシュの説明を含めることができます。ターゲットのスキャン中に一致するものが見つかった場合、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、ハッシュ区切りのコメント (fop など) も使用できます。
既知の正しい MD5 ハッシュのリストを指定する	なし	追加の既知の良好な MD5 ハッシュを指定する、1 行に 1 つの MD5 ハッシュを含むテキストファイル オプションとして、ハッシュの後にコンマを追加してその後に説明を続けると、各ハッシュの説明を含めることができます。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、ハッシュ区切りのコメント (# など) も使用できます。
ホストファイル許可リスト	なし	Tenable Vulnerability Management 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 Vulnerability Management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)	None (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		
ファイルシステムのスキャン	無効	有効にすると、Tenable Vulnerability Management は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 のディレクトリ([ファイルシステムのスキャン] が有効な場合に利用可能)		
%Systemroot% のスキャン	無効	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。
%ProgramFiles% スキャン	無効	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。
%ProgramFiles (x86)% スキャン	無効	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。
%ProgramData% スキャン	無効	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。
ユーザープロファイルのスキャン	無効	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。
カスタムファイルスキャンディレクトリ	None (なし)	マルウェアファイルスキャンによってスキャンされるディレクトリをリストするカスタムファイルです。各ディレクトリを 1 行にリストします。
Linux ディレクトリ		
$PATH をスキャンする	無効	ファイルシステムスキャンを有効にして、$PATH をスキャンします。
スキャン/ホーム	無効	スキャン/ホームをスキャンするファイルシステムを有効にする。

MacOS ディレクトリ		
$PATH をスキャンする	無効	ファイルシステムスキャンを有効にして、$PATH をスキャンします。
スキャン/ユーザー	無効	スキャン/ユーザーをスキャンするファイルシステムを有効にする。
スキャン/アプリケーション	無効	スキャン/アプリケーションをスキャンするファイルシステムを有効にする。
スキャン/ライブラリ	無効	スキャン/ライブラリをスキャンするファイルシステムを有効にする。

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)	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。

設定済みの評価設定

次の表に記載されている通り、Tenable が提供するTenable Nessus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 **[モード]** の両方によって決定されます。

テンプレート	モード	設定済みの設定
脆弱性スキャン(共通)		
高度なネットワークスキャン	–	すべてデフォルト
基本的な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
資格認定されたパッチ監査	–	すべてデフォルト
ホスト検出	–	–
内部 PCI ネットワークスキャン	**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
	カスタム	すべてデフォルト
従来のウェブアプリケーションスキャン	**既知の Web 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
	カスタム	すべてデフォルト
モバイルデバイススキャン	–	–
PCI 四半期毎外部スキャン	–	–
設定スキャン		
クラウドインフラ監査	–	–
内部 PCI ネットワークスキャン	–	–
オフライン設定監査	–	–
ポリシーコンプライアンス監査	–	–
SCAP および OVAL 監査	–	–
タクティカルスキャン		

Badlock 検出	–	**[ウェブクローラー]** のデフォルト
Bash Shellshock 検出	–	**[Web Crawler]** (ウェブクローラー) のデフォルト
DROWN 検出	–	–
Intel AMT セキュリティバイパス	–	–
マルウェアのスキャン	–	**[マルウェア]** のデフォルト
Shadow Brokers のスキャン	–	–
Spectre および Meltdown 検出	–	
	–	–
WannaCry Ransomware Detection	–	–

Tenable Vulnerability Management スキャンのレポート設定

注意: スキャンがユーザー定義テンプレートに基づいている場合、スキャンの **[レポート]** 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テンプレートでのみ変更できます。

[レポート] 設定には、以下の設定グループが含まれます。

- 処理中
- 出力

設定	デフォルト値	説明
処理		
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 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)	Enabled (有効)	有効な場合、スキャンレポートに破棄されたパッチの情報が含まれます。
Hide results from plugins	Enabled (有	有効な場合、レポートに依存関係リストは含まれま

設定	デフォルト値	説明
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)	効)	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。
出力		
DNS 名でホストを指名します	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。
Display hosts that respond to ping (ping に応答するホストを表示する)	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)	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。 **警告**: この設定を有効にすると、応答があるかどうかに関わらず、当該スキャンのすべてのターゲットに関する検出結果を作成します。このため、返されるホストの数がライセンスの上限を超えると、スキャンが中止される場合があります。詳細は、スキャン制限事項 を参照してください。
ユニコード文字を表示します	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。

Tenable Vulnerability Management スキャンの詳細設定

注意: スキャンがユーザー定義テンプレートに基づいている場合、スキャンの **[詳細]** 設定は設定できません。これらの設定は、関連するユーザー定義テンプレートでのみ変更できます。

[Advanced] (詳細) 設定により、スキャン効率とスキャン動作の管理能力が向上し、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
- パフォーマンスオプション
- Unix find コマンドのオプション
- 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 (エージェントスキャンのみ)

注意: 次の表には、**[高度なネットワークスキャン]** 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	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 Vulnerability Management 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

設定	デフォルト値	説明
(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)		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)	無効	デフォルトでは、Tenable Vulnerability Management 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 Vulnerability Management 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。
SSH の免責メッセージを自動的に受け入れる	無効	有効にすると、認証スキャンが免責事項要求のある FortiOS ホストに SSH 経由で接続を試みる場合に、スキャナーが免責事項要求の了承に必要なテキスト入力を行い、スキャンを継続します。 スキャンは、サポートされている認証方法を取得するために、最初に不良 ssh リクエストをターゲットに送信します。これにより、ターゲットへの接続方法を決定できます。この方法は、カスタム ssh バナーを設定してから、ホストへの接続方法を決定する際に便利です。 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 (複数のドメイン名からなるターゲットを並列にスキャンする)	無効	無効になっている場合、Tenable Vulnerability Management は、単一の IP アドレスに解決される複数のターゲットを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 Vulnerability Management 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

設定	デフォルト値	説明
		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、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。
認証スキャンを実行したホストに一意的な識別子を作成して付与する	有効	有効にすると、スキャナーは認証スキャンに使用する一意の識別子を作成します。
Trusted CAs	なし	スキャンで信頼できると見なされる CA 証明書を指定します。これにより、Tenable Vulnerability Management 環境の脆弱性であるプラグイン 51192 をトリガーすることなく、SSL 認証に自己署名証明書を使用することができます。 **注意:** この設定に加えて、個別のスキャナーレベルで信頼できる CA を設定できます (詳細については、*Tenable Nessus ユーザーガイド*のカスタム CA を信頼するを参照してください)。Tenable Vulnerability Management スキャン設定で設定された信頼できる CA と、Tenable Nessus スキャナーで設定された信頼できる CA の間には、優先順位や階層はありません。Tenable Vulnerability Management は、どの製品で設定されているかにかかわらず、スキャンを完了するために必要な適切な証明書を使用し、無関係の証明書を無視します。
パフォーマンスオプション		
ネットワーク輻輳の検出時にスキャンを減速させる	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

設定	デフォルト値	説明
		す。
Linux カーネル輻輳検出を使用する	無効	この設定を有効にすると、Tenable Vulnerability Management は Linux カーネルを使用して、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します。検出すると、Tenable Vulnerability Management はスキャンにスロットルをかけて輻輳状態を緩和します。輻輳状態が緩和すると、Tenable Vulnerability Management 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の再使用を試みます。
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。
スキャンごとの同時ホストの最大数	スキャンに使用される Tenable 提供のテンプレートに依存	Tenable Vulnerability Management が個別のスキャンタスクでの同時スキャンの対象として送信するホストの最大数を指定します。 ホスト制限を使用してスキャンパフォーマンスをさらに改善するために、Tenable は、個々のスキャナーの**詳細**設定 (たとえば、**max_hosts**、**global.max_hosts**、**global.max_scans**) を調整することを推奨しています。詳細は、*Tenable Nessus ユーザーガイド* の詳細設定を参照してください。 **[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** 設定より大きな値を設定すると、Tenable Vulnerability Management は **[スキャンごとの同時ホストの最大数]** を **max_hosts** の値に制限します。たとえば、**[スキャンごとの同**

設定	デフォルト値	説明
		時ホストの最大数] 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、ターゲット数が 100 を超えるときに Tenable Vulnerability Management は 100 個のホストを同時にスキャンします。 **注意:** 所属している企業が管理しているスキャナーの個別のスキャナー設定のみを調整できます。Tenable でホストされているスキャナーの設定は変更できません。
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。
スキャンごとの同時 TCP セッションの最大数	なし	スキャンされるホストの数に関係なく、各スキャンタスクで確立される TCP セッションの最大数を指定します。 Windows ホストにインストールされたスキャナーの場合、正確な結果を得るには、この値を 19 以下に設定する必要があります。
Unix find コマンドのオプション		
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。
除外するファイル	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

設定	デフォルト値	説明
システム		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。
含めるファイルパス	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。
Windows ファイル検索オプション		
Windows で除外するファイルパス	なし	Windows システムでの検索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。 ファイルには、1 行に 1 つのファイルパスを入力します。この設定で、デフォルトの除外をオーバーライドしたり、デフォルトの除外を削除したりします。 **注意：** Windows のファイルの除外は、そのオペレーティングシステ

設定	デフォルト値	説明
		ムによって管理されているプラグインには適用されません。
Windows インクルードファイルパス	なし	Windows システムでの再帰的な検索に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。 ファイルには、1 行に 1 つのファイルパスを入力します。この設定により、デフォルトが完全に置き換えられます。
デバッグ設定		
プラグインのデバッグ処理を有効にする	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	デフォルト	プラグイン監査証跡の詳細度を制御します。 次のオプションがあります。 • **監査証跡なし** - (デフォルト) Tenable Vulnerability Management はプラグイン監査証跡を生成しません。 • **すべての監査証跡データ** - スキャンにプラグインが含まれなかった理由を監査証跡に含めます。 • **スキャンエラーのみ** - スキャン時に発生したエラーのみを監査証跡に含めます。
スキャン開始のシフト		
Maximum delay (minutes)	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。

設定済みの詳細設定

次の表に記載されている通り、特定の Tenable 提供の Nessus スキャナーテンプレートでは、詳細設定が事前設定されています。事前設定される詳細設定は、選択したテンプレートおよび **モード** の両方によって決まります。

テンプレート	スキャンタイプ	設定済みの設定
脆弱性スキャン(共通)		
高度なネットワークスキャン	-	すべてデフォルト
基本的な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 • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する • 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 • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与す

		る
	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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	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 • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する

	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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	カスタム	すべてデフォルト
ホスト検出	–	–
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 • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する

	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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	カスタム	すべてデフォルト
従来のウェブアプリケーションスキャン	**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 • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	Scan low bandwidth links (低帯域幅リン	• パフォーマンスオプション :

	クのスキャン)	◦ 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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	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)	–	**[デバッグ設定]** 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 : ◦ 20 個の同時に存在するホスト (最大) ◦ 4 回のホスト毎の同時チェック (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
	低帯域幅リンクのス	• パフォーマンスオプション :

	キャン	◦ 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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	カスタム	• パフォーマンスオプション (デフォルトのオプション) • Unix Find コマンドの除外 (デフォルトのオプション)
設定スキャン		
クラウドインフラ監査	–	**[デバッグ設定]** のデフォルト
MDM 設定監査	–	–
Offline Config Audit (オフライン設定監査)	–	**[デバッグ設定]** のデフォルト
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 • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	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

		• 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	カスタム	すべてデフォルト
戦術スキャン		
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 セキュリティ	–	すべてデフォルト

バイパス		
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 • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	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) • 資産特定のオプション ◦ 認証スキャンを実行したホストに一意的な識別子を作成して付与する
	カスタム	すべてデフォルト

Shadow Brokers のスキャン	–	すべてデフォルト
Spectre および Meltdown 検出	–	すべてデフォルト
WannaCry Ransomware Detection	–	すべてデフォルト

Tenable Vulnerability Management スキャンの認証情報

認証情報を使用して Tenable Vulnerability Management スキャナーにローカルのアクセス権を付与し、エージェントを必要とすることなく対象システムをスキャンできます。認証されたスキャンを設定することで、認証されていないスキャンよりも広範なチェックを実行できるようになり、スキャン結果がより正確になります。このアプローチにより、非常に大規模なネットワークのスキャンが容易になり、ローカルの漏えいやコンプライアンス違反を特定できます。

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。

Tenable Vulnerability Management では、次の方法でスキャンに使用する認証情報を作成できます。

カテゴリ	説明	アクセス許可
スキャン固有	• 個別のスキャンでこの認証情報を設定し保存できます。 • スキャンを削除する場合、認証情報も削除されます。 • 別のスキャンで認証情報を使用する場合は、スキャン固有認証情報を管理された認証情報に変換するか、別のスキャンでスキャン固有認証情報の設定を再作成します。	スキャンの **[基本]** 設定の **[ユーザーアクセス許可]**
Template-specific	• この認証情報は [ユーザー定義テンプレート] で設定し保存できます。その後、テンプレートを使用して個別のスキャンを作成できます。 • 認証情報をユーザー定義テンプレートに追加した場合、他のユーザーがテンプレートから作成された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で、それらの認証情報をオーバーライドできます。Tenable では、認証情報をユーザー定義テンプレートに追加するのではなく、管理された認証情報をスキャンに追加することを推奨しています。	テンプレートの **[基本]** 設定の **[ユーザーアクセス許可]**

	• テンプレートを削除する場合、テンプレート固有認証情報も削除されます。ただし Tenable Vulnerability Management は、削除前にそのユーザー定義テンプレートを使用して作成したスキャンの認証情報は保持します。 • 別のテンプレートの認証情報を使用する場合は、別のテンプレートにテンプレート固有の認証情報を再作成する必要があります。	
管理	• Tenable Vulnerability Management は、管理された認証情報を認証情報マネージャーで一元的に保存しています。新しい管理された認証情報は、認証情報マネージャーで直接作成するか、スキャン設定中に作成できます。または、スキャン設定中に、スキャン固有の認証情報を管理された認証情報に変換することもできます。 • 管理された認証情報は複数のスキャンで使用できます。別のユーザーに、管理された認証情報をスキャンで使用するアクセス許可を付与することもできます。 • テンプレートでは、管理された認証情報は使用できません。	認証情報のユーザーアクセス許可を設定する

認証情報の設定は、認証情報の種類によって異なります。認証情報の種類は次の通りです。

- クラウドサービス
- データベース
- ホスト
- その他
- モバイルデバイス管理
- パッチ管理
- プレーンテキスト認証

詳細については、次を参照してください。

- スキャン認証情報の追加
- スキャンの認証情報の編集

- スキャン固有の認証情報の管理された認証情報への変換
- 認証情報をユーザー定義のテンプレートに追加する
- ユーザー定義のテンプレートの認証情報の編集

注意: Tenable Vulnerability Management 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。

注意: デフォルトでは、認証スキャンまたはユーザー定義テンプレートを作成するときに、ホストは **Tenable Asset Identifier (TAI)** で識別され、マークされます。このグローバルな一意の識別子はホストのレジストリまたはファイルシステムに書き込まれ、以降のスキャンでは **TAI** を取得して使用できます。

このオプションは、スキャン設定またはテンプレートの **[詳細] -> [全般設定]** の **[認証スキャンを実行したホストに一意的な識別子を作成して付与する]** で有効（デフォルト）または無効になっています。

スキャン認証情報の追加

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なスキャンのアクセス許可: 制御可

スキャンに1つの種類の認証情報 (SSH ログイン、SMB ログインなど) が複数インスタンス含まれている場合、Tenable Vulnerability Management はそれらをスキャン設定に追加された順番で、有効なターゲットに対して使用するよう試みます。

注意: ターゲット上での認証情報チェックには、ログインに成功した最初の認証情報が使用されます。ある認証情報で Tenable Vulnerability Management がログインに成功した後は、たとえリストの後方にある認証情報がより大きなアクセス権や権限を持っているとしても、リスト内の他の認証情報を試すことはありません。

認証情報をスキャンに追加する方法

1. スキャンを作成または編集します。
2. 左側のナビゲーションメニューで、**[認証情報]** タブをクリックします。

   [認証情報] ページが表示されます。このページには、スキャン用に設定されている認証情報の表が含まれます。
3. **[認証情報の追加]** の横にある ⊕ ボタンをクリックします。

   [認証情報タイプの選択] プレーンが表示されます。
4. 次のいずれかを行います。

   ### 既存の管理された認証情報を追加します。

   [認証情報タイプの選択] の **[管理された認証情報]** プレーンには、**[使用可]** または **[編集可]** のアクセス許可を持つ認証情報が含まれています。

   a. (オプション) リストで管理された認証情報を検索するには、テキストボックスに検索条件を入力し、🔍 ボタンをクリックします。

b. **[管理された認証情報]** セクションで ⌄ ボタンをクリックして、すべての管理された認証情報を表示します。

c. 追加する管理された認証情報をそれぞれクリックします。

[認証情報タイプの選択] プレーンは開いたままになります。

d. **[認証情報タイプの選択]** プレーンを閉じるには、プレーンの右上にある ✕ ボタンをクリックします。

スキャン固有の認証情報を追加します。

a. **[認証情報タイプの選択]** プレーンの **[管理された認証情報]** 以外のセクションで、⌄ ボタンをクリックして、そのタイプの認証情報を表示します。

b. 追加する認証情報をそれぞれクリックします。

該当する認証情報のタイプの設定プレーンが表示されます。

c. 個別の認証情報設定の設定をします。

新しい管理された認証情報を追加します。

a. **[認証情報タイプの選択]** プレーンの **[管理された認証情報]** 以外のセクションで、⌄ ボタンをクリックして、そのタイプの認証情報を表示します。

b. 追加する認証情報をそれぞれクリックします。

該当する認証情報のタイプの設定プレーンが表示されます。

c. 新しい管理された認証情報の設定をします。

d. **[管理された認証情報に保存]**トグルをクリックします。

管理された認証情報の設定が表示されます。

e. 1つ目のテキストボックスに、管理された認証情報の名前を入力します。

f. (オプション) 2番目のテキストボックスに、管理された認証情報の簡単な説明を入力します。

g. 管理された認証情報のユーザーアクセス許可を設定します。

5. **[保存]**をクリックして、認証情報の変更を保存します。

Tenable Vulnerability Managementにより設定プレーンが閉じられ、認証情報がスキャンの認証情報の表に追加されます。

> **注意:** 保存する際、Tenable Vulnerability Management は自動的に ID の昇順で認証情報を並べ替え、タイプ別に認証情報をグループ化します。

6. 次のいずれかを行います。

- スキャンを起動せずに保存する場合は、**[保存]**をクリックします。

  Tenable Vulnerability Management がスキャンを保存します。

- 今すぐスキャンを保存して起動する場合は、**[保存して起動]**をクリックします。

  > **注意:** スキャンを後で実行するようにスケジュールした場合は、**[保存して起動]**オプションは利用できません。

  Tenable Vulnerability Management がスキャンを保存して起動します。

スキャンの認証情報の編集

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なスキャンのアクセス許可: 設定可

スキャンの認証情報を編集する方法

1. スキャンを編集します。
2. 左側のナビゲーションメニューで、**[認証情報]** タブをクリックします。

   スキャン用に設定されている認証情報の表が表示されます。
3. 認証情報の表で、編集する認証情報をクリックします。

   [認証情報設定] プレーンが表示されます。
4. 次のいずれかを行います。
   - スキャン固有の認証情報の場合は、認証情報の設定を設定します。
   - 管理された認証情報の場合には
     a. 名前または説明を編集します。
     b. 認証情報の設定を設定します。
     c. 管理された認証情報のユーザーアクセス許可を設定します。
   - **注意:** **[編集可]** アクセス許可を持っている、管理された認証情報の設定のみを表示または編集できます。
5. **[保存]** をクリックして認証情報の変更を保存します。

   管理された認証情報を編集した場合は、Tenable Vulnerability Management によってその他のスキャンが管理された認証情報を使用しているかどうかが確認され、変更の確認を求めるメッセージが表示されます。
6. (管理された認証情報のみ) **[はい]** をクリックして管理された認証情報への変更を保存します。
7. **[保存]** をクリックして、スキャンの変更を保存します。

認証情報をユーザー定義のテンプレートに追加する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なテンプレートのアクセス許可: 設定可

認証情報をユーザー定義のテンプレートに追加する前に、次の事項を検討します。

- 他のユーザーは、テンプレートから作成された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で、テンプレート固有の認証情報をオーバーライドできます。Tenable では、認証情報をユーザー定義テンプレートに追加するのではなく、管理された認証情報をスキャンに追加することを推奨しています。
- ユーザー定義テンプレートでは、管理された認証情報は使用できません。複数のスキャンで 1 式の認証情報を使用するには、認証情報をユーザー定義のテンプレートに追加するのではなく、管理された認証情報をスキャンに追加します。

注意: スキャン設定では、**スキャン全体の認証情報タイプ**の設定は、個別の認証情報内に置かれます。ユーザー定義テンプレートでは、これらの設定は、テンプレートの **[基本]** 設定の **[認証]** セクションにあります。

テンプレート固有の認証情報を追加する方法

1. テンプレートを作成または編集します。
2. 左側のナビゲーションメニューで、**[認証情報]** タブをクリックします。

   [認証情報] ページが表示されます。このページには、テンプレート用に設定されている認証情報の表が含まれます。
3. **[認証情報の追加]** の横にある ⊕ ボタンをクリックします。

   [認証情報タイプの選択] プレーンが表示されます。
4. **[認証情報タイプの選択]** プレーンで、認証情報のタイプをクリックします。

   該当する認証情報のタイプの設定プレーンが表示されます。
5. 個別の認証情報設定の設定をします。

6. **[保存]**をクリックして、認証情報の変更を保存します。

   Tenable Vulnerability Management により設定プレーンが閉じられ、認証情報がテンプレートの認証情報の表に追加されます。

7. **[保存]**をクリックして、テンプレートの変更を保存します。

   Tenable Vulnerability Management により、認証情報がテンプレートの認証情報の表に追加されます。

ユーザー定義のテンプレートの認証情報の編集

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なテンプレートのアクセス許可: 設定可

ユーザー定義のテンプレートの認証情報を編集する方法

1. ユーザー定義テンプレートを編集します。
2. 左側のナビゲーションメニューで、**[認証情報]** タブをクリックします。

   テンプレート用に設定されている認証情報の表が表示されます。
3. 認証情報の表で、編集する認証情報をクリックします。

   [認証情報設定] プレーンが表示されます。
4. 認証情報の設定を設定します。
5. **[保存]** をクリックして認証情報の変更を保存します。
6. **[保存]** をクリックしてテンプレートの変更を保存します。

スキャン固有の認証情報の管理された認証情報への変換

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なスキャンのアクセス許可: 所有者

スキャン固有の認証情報は、1 回のスキャンでのみ使用できます。複数のスキャンでスキャン固有の認証情報を再使用するには、管理された認証情報に変換します。

スキャン固有の認証情報を変換する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[脆弱性管理]** セクションで、**[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。

3. **[フォルダー]** セクションで、表示するスキャンを読み込むフォルダーをクリックします。

   選択したフォルダーでスキャンを表示するようスキャンテーブルが更新されます。

4. スキャンの表で、編集するスキャンをクリックします。

   [スキャンの詳細] ページが表示されます。

5. スキャン名の横にある ✎ ボタンをクリックします。

   [スキャンの更新] ページが表示されます。

6. 左側のナビゲーションメニューで、**[認証情報]** タブをクリックします。

   スキャン用に設定されている認証情報の表が表示されます。

7. 認証情報の表で、変換するスキャン固有の認証情報をクリックします。

   [認証情報設定] プレーンが表示されます。

8. **[管理された認証情報に保存]** トグルをクリックします。

   管理された認証情報の設定が表示されます。

9. 1 つ目のテキストボックスに、管理された認証情報の名前を入力します。

10. (オプション) 2番目のテキストボックスに、管理された認証情報の簡単な説明を入力します。
11. 管理された認証情報のユーザーアクセス許可を設定します。
12. **[保存]** をクリックして、認証情報の変更を保存します。

    Tenable Vulnerability Managementにより設定プレーンが閉じられ、認証情報がスキャンの認証情報の表に追加されます。
13. [**Save**] をクリックして、スキャンの変更を保存します。

クラウド サービス

Tenable Vulnerability Management では、以下に一覧するクラウド サービスのアカウントを使用して、スキャンを認証できます。

注意: 選択したスキャンテンプレートによっては、一部の認証情報タイプが設定に利用できない場合があります。

AWS

オプション	デフォルト値	説明	必須
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。	○
スキャン全体の認証情報タイプの設定			

アクセスするリージョン	世界のその他の地域	Tenable Vulnerability Management が Amazon AWS アカウントを監査するには、スキャンする地域を定義する必要があります。Amazon のポリシーにより、中国地域のアカウント設定を監査するには、世界のその他の地域とは異なる認証情報が必要です。
		
		可能性がある地域には次が含まれます。
		
		• **GovCloud** - この地域を選択すると、政府のクラウドが自動的に選択されます (例: us-gov-west-1)
		
		• **世界のその他の地域** - この地域を選択すると、次の追加オプションが表示されます。
		
		  • 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
		• **中国** - この地域を選択すると、次の追加オプションが表示されます。
		  • cn-north-1
		  • cn-northwest-1	

HTTPS	有効	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management が認証するかどうかを設定します。	×
Verify SSL Certificate (SSL 証明書の検証)	有効	Tenable Vulnerability Management が SSL デジタル証明書の有効性を確認するかどうかを設定します。	×

Microsoft Azure

オプション	デフォルト値	説明	必須
ユーザー名	–	Microsoft Azure へのログインに必要なユーザー名	○
パスワード	–	ユーザー名に関連するパスワード	○
Client 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)	
スキャン全体の認証情報タイプの設定			
サブスクリプション ID	–	スキャンするサブスクリプション ID をコンマで区切ってリストします。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	デフォルト値	説明	必須
ユーザー名	–	ログインユーザー名	○
Password or API Key	–	ユーザー名に関連するパスワードまたは API キー	○
認証方法	API-Key	ドロップダウンボックスから、**[パスワード]** または **[API キー]** を選択します。	○
スキャン全体の認証情報タイプの設定	選択済みのすべての場所	Rackspace クラウドインスタンスの場所です。可能性がある場所には次が含まれます。 • ダラスフォートワース (DFW) • シカゴ (ORD) • 北バージニア (IAD) • ロンドン (LON) • シドニー (SYD) • 香港 (HKG)	×

Salesforce.com

オプション	デフォルト値	説明	必須
ユーザー名	–	Salesforce.com のログインに必要なユーザー名です。	○
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

注意: 選択したスキャンテンプレートによっては、一部の認証情報タイプが設定に利用できない場合があります。

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。

DB2

次の表は、**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。
データベースのポート	Tenable Vulnerability Management 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)。

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** • **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。
データベースのポート	Tenable Vulnerability Management 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。
データベースのポート	Tenable Vulnerability Management 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 Vulnerability Management が使用するアカウントの種類。 • **SYSDBA** • **SYSOPER** • **NORMAL**
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**)。
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)** • **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。
データベースのポート	Tenable Vulnerability Management 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。
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。
データベースのポート	Tenable Vulnerability Management 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。
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 Vulnerability Management が使用するアカウントの種類 (**SQL** または **Windows**)。
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	必要な認証情報を提供するための認証方法。

オプション	説明
種類	• **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。
データベースのポート	Tenable Vulnerability Management 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。
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**)。

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プを参照してください。
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。

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。 • **Password (パスワード)** • **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。
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。
ポート	(必須) Tenable Vulnerability Management 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。

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。

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。	○
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。	○
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。	○
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。	○
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 Vulnerability Management 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 Vulnerability Management 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 • SYSOPER • NORMAL Sybase ASEの値は以下のとおりです。 • RSA • プレーンテキスト	○
インスタンス名	SQL Server	データベースインスタンスの名前。	×
サービスの種	Oracle	有効な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
類		• 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。各アイテムに対して使用できる有効な値の説明については、データベースの認証情報を参照してください。

Tenable Vulnerability Management 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`
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 host ポート)	BeyondTrust がリッスンするポート。	○
BeyondTrust API user	BeyondTrust が提供する API ユーザー。	○
BeyondTrust API key (BeyondTrust API キー)	BeyondTrust が提供する 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 の使用)	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。	×
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 Vulnerability Management 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 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。	○
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。	○
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。	×
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）
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）
認証情報の取得方法	CyberArk API 認証情報を取得する方法。**[ユーザー名]**、**[識別子]**、または **[アドレス]** のいずれかです。	○

オプション	説明	必須
	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。 **注意：[ユーザー名]**オプションを使用すると、API クエリの**[アドレス]**パラメーターも追加され、解決されたホストのターゲット IP がこの**[アドレス]**パラメーターに割り当てられます。これにより、[アカウントの詳細**アドレス**]フィールドにターゲット IP アドレス以外の値が含まれている場合、認証情報のフェッチに失敗する可能性があります。	
Username (ユーザー名)	(**[認証情報の取得]**が**[ユーザー名]**の場合) パスワードを要求する CyberArk ユーザーのユーザー名。	×
Safe	認証情報を取得するべき CyberArk のセーフ。	×
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 の使用)	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 Vulnerability Management 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 ホスト	すべて	CyberArk Central Credential Provider の IP/DNS アドレス。	○
Central Credential Provider ポート	すべて	CyberArk Central Credential Provider がリッスンするポート。	○
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 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 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 クラ	すべて	CyberArk ホストとの通信に使用される PEM 証明	×

オプション	データベースの種類	説明	必須
イアント証明書		書を含むファイル。	
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 クライアント証明書のプライベートキーパスフレーズ	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。	×
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 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 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。	○
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 の使用)	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	×

オプション	データベースの種類	説明	必須
		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 (データベースのポート)	すべて	Tenable Vulnerability Management 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** • **SYSOPER** • **NORMAL** Sybase ASEの値は以下のとおりです。 • RSA • プレーンテキスト	○
インスタンス名	SQL Server	データベースインスタンスの名前。	×
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	×

オプション	データベースの種類	説明	必須
		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 Authentication Method (Delinea 認証方法)	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 Delinea Login Name (Delinea 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 の使用)	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。	×

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 Vulnerability Management 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。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 Vulnerability Management バージョン: KV1、KV2、AD、LDAP。Tenable Vulnerability Management バージョンの詳細については、Tenable Vulnerability Management 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 Vulnerability Management 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 エンジン URL	(KV2) Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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 の使用)	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、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)	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 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 ポート	すべて	Lieberman がリッスンするポート。	○
Lieberman API URL	すべて	Tenable Vulnerability Management が Lieberman へのアクセスに使用する URL。	×
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 パスワード	すべて	Lieberman 明示ユーザーのパスワード。	○
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 ク	すべて	Lieberman ホストとの通信に使用される PEM 証	×

オプション	データベースの種類	説明	必須
クライアント証明書		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 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 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 の使用)	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。	×
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	すべて	Tenable Vulnerability Management とデータベースの通信に使用されるポート	○

オプション	データベースの種類	説明	必須
のポート)			
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。 • RSA • プレーンテキスト	○
インスタンス名	SQL Server	データベースインスタンスの名前。	×
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 ホスト	QiAnXin ホストの IP アドレスまたは URL。	○
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 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 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	○
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。	×
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	×

オプション	説明	必須
	• **DB2** - DB2 データベース • **HP_UNIX** - HP Unix • **SOLARIS** - Solaris • **OPENLDAP** - OpenLDAP • **POSTGRESQL** - PostgreSQL	
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
Use SSL (SSL の使用)	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。	×

Host (ホスト)

Tenable Vulnerability Management では、次の形式のホスト認証がサポートされます。

- SNMPv3
- セキュアシェル(SSH)
- Windows

注意: 選択したスキャンテンプレートによっては、一部の認証情報タイプが設定に利用できない場合があります。

SNMPv3

SNMPv3 認証情報を使用して、暗号化されたネットワーク管理プロトコルを使用するリモートシステムをスキャンします。(ネットワークデバイスを含む。)Tenable Vulnerability Management 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をスキャンします。

注意: SNMPv3 オプションは、高度なネットワークのスキャンテンプレートでのみ使用できます。

[認証情報] リストの **[SNMPv3]** をクリックして、次の項目を設定します。

オプション	説明	デフォルト	必須
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 Vulnerability Management が使用する、SNMPv3 のアカウントのユーザー名	-	○
ポート	Tenable Vulnerability Management からの通信に対して SNMPv3 がリッスンする TCP ポート	161	×
Security level	SNMP のセキュリティレベル: • **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	○
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-**	SHA1	○ (認証を選択する場

オプション	説明	デフォルト	必須
	512、または **MD5**。		合)
Authentication password	(必須) **ユーザー名** に関連付けられたパスワード	-	○ (認証を選択する場合)
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	○ (プライバシーのある認証を選択する場合)
Privacy password	(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	-	○ (プライバシーのある認証を選択する場合)

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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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。

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 1000 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。

[認証情報] リストで **[SSH]** を選択して、次の SSH 認証方法の設定を行います。

SSH 認証方法: 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、データの暗号化に公開鍵を、復号に秘密鍵を使用します。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 Vulnerability Management では DSA 鍵と RSA 鍵の両方式をサポートしています。

Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management は OpenSSH SSH 公開鍵形式をサポートしています。PuTTY や SSH Communications Security などの他の SSH アプリケーションの形式は、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 としてのリモートログインを許可していないため、Tenable Vulnerability Management 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、または pbrun を呼び出します。また Tenable Vulnerability Management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 Vulnerability Management 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 サーバーをチェックして、正しいアルゴリズムがサポートされていることを確認してください。

Tenable Vulnerability Management 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 キーの使用を推奨します。これにより、既知の SSH サーバーの監査に使用しているユーザー名とパスワードが、管理下にないシステムへのログイン試行に使われないようにすることができます。

注意: サポートされているネットワークデバイスでは、Tenable Vulnerability Management 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。

ルート以外のアカウントを権限昇格に使用する必要がある場合は、エスカレーションパスワードを使用してエスカレーションアカウントで指定できます。

オプション	説明	必須
ユーザー名	ホストに認証するユーザー名	○
プライベートキー	ユーザーの RSA または DSA Open SSH キーファイル	○
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です。	×
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。詳細は、権限昇格を参照してください。	×
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。	×

SSH 認証方法: 証明書

オプション	説明	必須
ユーザー名	ホストに認証するユーザー名	○

オプション	説明	必須
User Certificate	ユーザーの RSA または DSA Open SSH 証明書ファイル	○
プライベートキー	ユーザーの RSA または DSA Open SSH キーファイル	○
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です。	×
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。詳細は、権限昇格を参照してください。	×
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。	×

SSH 認証方法: CyberArk Vault

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 Vulnerability Management は、CyberArk から認証情報を取得してスキャンに使用します。

CyberArk

オプション	説明	必須
CyberArk Host	CyberArk AIM ウェブサービスの IP アドレスまたは FQDN 名。	○

オプション	説明	必須
(Delinea ホスト)		
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。	○
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。	×
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)
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。	×
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 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	KDC は、Linux 実装ではデフォルトで TCP を使用します。UDP では、	×

オプション	説明	必須
Transport	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。	
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(例: example.com)。Tenable Vulnerability Management 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。**[ユーザー名]**、**[識別子]**、または**[アドレス]**のいずれかです。 **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。 **注意: [ユーザー名]**オプションを使用すると、API クエリの**[アドレス]**パラメーターも追加され、解決されたホストのターゲット IP がこの**[アドレス]**パラメーターに割り当てられます。このため、CyberArk アカウント詳細の**[アドレス]**フィールドにターゲット IP アドレス以外の値が含まれていると、認証情報のフェッチに失敗する可能性があります。	○
Username (ユーザー名)	(**[認証情報の取得方法]**が**[ユーザー名]**の場合)パスワードを要求する CyberArk ユーザーのユーザー名。	×
Safe	認証情報の取得元となる CyberArk safe。	×
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。	×
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 の使用)	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。	×

オプション	説明	必須
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 Auto-Discovery

Tenable の CyberArk Integration に対す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。詳細は、*Tenable CyberArk 統合ガイド*の CyberArk Dynamic Scanning (CyberArk 動的スキャン) を参照してください。

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。	○
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。	○
Safe	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 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	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	○

オプション	説明	必須
UI ログインパスワード	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。」 **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。	○
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 の使用)	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)

オプション	説明	必須
ユーザー名	ターゲットシステムのユーザー名	○
CyberArk AIM サービス URL	CyberArk AIM ウェブサービスの URL です。デフォルトでは、Tenable Vulnerability Management は `/AIMWebservice/v1.1/AIM.asmx` を使用します。	×
Central	CyberArk Central Credential Provider の IP/DNS アドレス。	○

オプション	説明	必須
Credential Provider ホスト		
Central Credential Provider ポート	CyberArk Central Credential Provider がリッスンするポート	○
Central Credential Provider ユーザー名	ボールト 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に基本情報を使用します。	×
Central Credential Provider パスワード	ボールト 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に基本情報を使用します。	×
Safe	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 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	×
CyberArk 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	×
CyberArk クライアント証明書のプライ	プライベート キーのパスフレーズ (必要な場合)	×

オプション	説明	必須
ベートキーパスフレーズ		
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	○
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	○
ポリシー ID	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	×
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	×
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。	×
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 アカウント詳細名	CyberArk から取得する認証情報の一意の名前	×

オプション	説明	必須
CyberArk Address	ユーザーアカウントのドメイン	×
CyberArk elevate privileges with	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。	×
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。	×

Delinea SSH 認証方法: Delinea

オプション	説明	必須
Delinea Authentication Method (Delinea 認証方法)	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	シークレットサーバー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	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	○

(Delinea ホスト)	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	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。	×
Use SSL (SSL の使用)	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。	×
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。	×
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。	×
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。	×

SSH 認証方法: 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 Vulnerability Management 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。

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。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 Vulnerability Management バージョン: KV1、KV2、AD、LDAP。Tenable Vulnerability Management バージョンの詳細については、Tenable Vulnerability Management 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 Vulnerability Management 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 エンジン URL	(KV2) Tenable Vulnerability Management 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/kv_mount_name`。末尾の / なし **注意:** 追加の文字列/セグメントである `data` が KV v2 ストアの Vault に対して行われた読み取りリクエストに挿入されるため、KV2 エンジン URL の秘密へのパスを使用することはできません。**[エンジン URL]** フィールドには、秘密へのパスではなく、KV マウントの名前のみを入力します。 **注意:** `data` セグメントを自分で含める必要はありません。秘密名/パスに含めると、Vault への読み取り呼び出しに無効な `/data/data` が含められます。	○ (KV2 **Vault タイプ**を選択した場合)
AD Engine URL (AD エンジン URL)	(AD) Tenable Vulnerability Management 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 Vulnerability Management 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。	○
ドメイン鍵	(KV1 および KV2) ドメインが格納されている Hashicorp Vault での名前です。	×
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。	○
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)	(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 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。	×
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)。	
レルム(SSH)	(Kerberos ターゲット認証が有効な場合は必須。)このレルムは、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(例: example.com)。	○
Use SSL (SSL の使用)	有効にすると、Tenable Vulnerability Management 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。	×
SSL 証明書を検証する	有効にすると、Tenable Vulnerability Management 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には、Hashicorp Vault で SSL を使用する必要があります。	×
Tenable Vulnerability Management に対して有効にする	Tenable Vulnerability Management での IBM DataPower Gateway の使用を有効または無効にします。	○
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 および 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 Vulnerability Management 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、[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。

昇格アカウント認証情報 ID または識別子 (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。	×

SSH 認証方法: Kerberos

MIT の Athena プロジェクトによって開発された Kerberos は、対称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、その TGT を使用して KDC にサービスチケットをリクエストし、他の Kerberos ベースのサービスを利用できるようになります。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 Vulnerability Management での Unix 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 Vulnerability Management と Kerberos のやり取りの概要を次に示します。

1. エンドユーザーが KDC の IP を指定する
2. nessusd が sshd で Kerberos 認証がサポートされるかどうかを確認する
3. sshd が「yes」と答える
4. nessusd がログインとパスワードと共に Kerberos TGT をリクエストする
5. Kerberos が nessusd にチケットを送信する
6. nessusd が sshd にチケットを送信する
7. 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	必須
ユーザー名	ターゲットシステムのユーザー名	○
パスワード	指定されたユーザー名のパスワード	○
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 ポート	KDC がポート 88 以外で動作している場合に、Tenable Vulnerability Management に KDC への接続先を指定します。	×
KDC Transport	KDC サーバーにアクセスする方法 **注意:** [KDC Transport] を **[UDP]** に設定した場合は、ポート番号も変更する必要があります。実装に応じて、KDC UDP プロトコルはデフォルトでポート 88 または 750 を使用するためです。	×
領域	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 (example.com など。)	○
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。詳細は、権限昇格を参照してください。	×
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。	×

Kerberos を使用する場合、KDC でチケットを検証するには Keberos サポートを使って sshd を設定する必要があります。設定が正常に機能するには、DNS 逆引きが適切に設定されることが条件となります。Kerberos の相互認証方法は、gssapi-with-mi である必要があります。

SSH 認証方法: パスワード

オプション	説明	必須
ユーザー名	ターゲットシステムのユーザー名	○
パスワード	指定されたユーザー名のパスワード	○
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。詳細は、権限昇格を参照してください。	×
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。	×
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。	×

SSH 認証方法: Lieberman RED

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	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 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 ポート	Lieberman がリッスンするポート。	○
Lieberman API URL	Tenable Vulnerability Management が Lieberman へのアクセスに使用する URL。	×
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 パスワード	Lieberman 明示ユーザーのパスワード。	○
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*)。	×
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	×

オプション	説明	必須
	力する必要はありません。	
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 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 の使用)	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。	×
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。	×
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	×

オプション	説明	必須
	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。	
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。	×

SSH 認証方法: QiAnXin

オプション	説明	必須
QiAnXin ホスト	QiAnXin ホストの IP アドレスまたは URL。	○
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 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 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	○
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。	×
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	×

オプション	説明	必須
	• **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	
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
権限昇格方法	ドロップダウンメニューを使用して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	権限昇格を行う場合は必須です。

オプション	説明	必須
	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。	
昇格アカウントのユーザー名	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。	×
Use SSL (SSL の使用)	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。	×

SSH 認証方法: Thycotic Secret Server

オプション	説明	必須
ユーザー名	SSH 経由のシステム認証に使用されるユーザー名	○
Thycotic シークレット名	Thycotic サーバーのシークレットの値。シークレットには、Thycotic 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。	○
Thycotic Secret Server URL	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。この値は、Thycotic サーバーの**[管理者]** > **[設定]** > **[アプリケーションの設定]** > **[シークレットサーバー URL]** にあります。 たとえば、次のアドレスがあるとします。 **`https://pw.mydomain.com/SecretServer/`** • 転送方法: **`https`** はSSL 接続を示します。 • ターゲット: **`pw.mydomain.com`** はターゲットアドレスです。	○

	• ターゲット ディレクトリ: **/SecretServer/** はルート ディレクトリです。	
Thycotic ログイン名	Thycotic サーバーを認証するためのユーザー名	○
Thycotic パスワード	Thycotic サーバーを認証するためのパスワード	○
Thycotic Organization	クエリする企業この値を Thycotic のクラウド インスタンスに使用できます。	×
Thycotic Domain	Thycotic サーバーのドメイン	×
Use Private Key	パスワードを使用しない場合、SSH 接続の鍵を使用します。	×
SSL 証明書を検証する	Tenable.io でサーバーの SSL 証明書が信頼できる CA によって署名されたかどうかを確認します。	×
Thycotic elevate privileges with	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。詳細は、権限昇格を参照してください。	×
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。	×
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。	

SSH 認証方式: BeyondTrust

オプション	説明	必須
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	○
BeyondTrust host	BeyondTrust IP アドレスまたは DNS アドレス	○
BeyondTrust port	BeyondTrust がリッスンするポート。	○
BeyondTrust API user	BeyondTrust が提供する API ユーザー	○
BeyondTrust API key	BeyondTrust が提供する API キー	○
Checkout duration	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:** 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 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 BeyondTrust がパスワードを変更すると、スキャンは失敗します。	○
SSL を使用する	有効にすると、Tenable Vulnerability Management 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。	
SSL 証明書を検証する	有効にすると、Tenable Vulnerability Management 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	有効にすると、Tenable Vulnerability Management はパスワード認証ではなく秘密鍵ベースの認証で SSH 認証を行います。失敗した場合は、パスワードが要求されます。	×
Use privilege escalation	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。何かが返された場合は、それをスキャンに使用します。	×
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。	×
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。	×

SSH のスキャン全体の認証情報タイプの設定

これらの設定は、現在のスキャンのすべての SSH タイプの認証情報に適用されます。これらの設定は、現在のスキャンの認証情報のインスタンスで編集できます。変更内容は、スキャン中のそのタイプの他の

認証情報に自動的に適用されます。

オプション	デフォルト値	説明
known_hosts ファイル	なし	SSH known_hosts ファイルをアップロードすると、Tenable Vulnerability Management はこのファイルのホストに対してのみ、ログインを試みます。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。
優先ポート	22	ターゲットのシステムで SSH が実行されているポートです。
クライアントバージョン	OpenSSH_5.0	スキャン中に Tenable Vulnerability Management が偽装する SSH クライアントの種類を指定します。
最小限の権限を試行	未選択	動的な権限昇格を有効または無効にします。この機能を有効にすると、Tenable Vulnerability Management は、**[昇格した権限がある]** オプション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 Vulnerability Management は権限を昇格させます。プラグイン 101975 および 101976 では、権限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。

SSH 認証方法: Centrify

オプション	説明
Centrify ホスト	(必須) Centrify IP アドレスまたは DNS アドレス **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 ポート	(必須) Centrify がリッスンするポート Tenable Vulnerability Management は初期設定でポート 443 を使用します。
API ユー	(必須) Centrify が提供するAPIユーザーです。

ザー	
API キー	(必須) Centrify が提供する API キー。
テナント	(必須) API に関連付けられた Centrify テナント Tenable Vulnerability Management は初期設定で *centrify* を使用します。
認証 URL	(必須) Tenable Vulnerability Management が Centrify にアクセスするために使用する URLTenable Vulnerability Management は初期設定で */Security* を使用します。
パスワードクエリ URL	(必須) Tenable Vulnerability Management が Centrify 内のパスワードをクエリするために使用する URLTenable Security Center は初期設定で */RedRock* を使用します。
パスワードエンジン URL	(必須) Tenable Vulnerability Management が Centrify 内のパスワードにアクセスするために使用する URLTenable Vulnerability Management は初期設定で */ServerManage* を使用します。
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。
チェックアウト期間	(必須) 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 Security Center における通常のスキャン期間を超えるように設定し、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 Centrify がパスワードを変更すると、スキャンは失敗します。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。
SSL を使用する	有効にすると、Tenable Vulnerability Management 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。
SSL 証明書の検証	有効にすると、Tenable Vulnerability Management 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。

SSH 認証方法: Arcon

オプション	説明

Arcon ホスト	(必須) Arcon IP アドレスまたは DNS アドレス **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 ポート	(必須) Arcon がリッスンするポート Tenable Security Center はデフォルトでポート 444 を使用します。
API ユーザー	(必須) Arcon が提供するAPIユーザーです。
API キー	(必須) Arcon が提供するAPIキーです。
認証 URL	(必須) Tenable Security Center が Arcon にアクセスするために使用する URL
パスワードエンジン URL	(必須) Tenable Security Center が Arcon 内のパスワードにアクセスするために使用する URL
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 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。
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 Security Center 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。 **ヒント:** 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 Security Center 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。
Use SSL (SSL の使用)	有効にすると、Tenable Security Center 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。

SSL 証明書の検証	有効にすると、Tenable Security Center 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。
権限昇格	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権限昇格方法です。**[権限昇格]** 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。詳細は、権限昇格を参照してください。

注意: Unix システムのローカルアクセス権を持つ特権ユーザー以外は、パッチレベルや **/etc/passwd** ファイルのエントリなど、基本的なセキュリティ問題を特定できます。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。

Windows

[認証情報] リストの **[Windows]** をクリックして、以下の Windows ベースの認証方法の設定を行います。

Windows 認証方法: CyberArk Vault

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 Vulnerability Management は、CyberArk から認証情報を取得してスキャンに使用します。

CyberArk

オプション	説明	必須
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。	○
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。	○
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。	×
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

オプション	説明	必須
ベートキー		が適用されている場合)
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。	×
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 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。	×
認証情報の取得方法	CyberArk API 認証情報を取得する方法。**[ユーザー名]**、**[識別子]**、または **[アドレス]** のいずれかです。 **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。 **注意: [ユーザー名]** オプションを使用すると、API クエリの **[アドレス]** パラメーターも追加され、解決されたホストのターゲット IP がこの **[アドレス]** パラメーターに割り当てられます。これにより、[アカウントの詳細 **アドレス**]	○

オプション	説明	必須
	フィールドにターゲット IP アドレス以外の値が含まれている場合、認証情報のフェッチに失敗する可能性があります。	
Username (ユーザー名)	(**[認証情報の取得]** が **[ユーザー名]** の場合) パスワードを要求する CyberArk ユーザーのユーザー名。	×
Safe	認証情報を取得するべき CyberArk のセーフ。	×
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。	×
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 の使用)	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

Tenable の CyberArk Integration に対す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。詳細は、*Tenable CyberArk 統合ガイド*の CyberArk Dynamic Scanning (CyberArk 動的スキャン) を参照してください。

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。	○
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 接続に関連付けられているアプリケーション ID。	○
Safe	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 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 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 の使用)	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)

オプション	説明	必須
ユーザー名	ターゲットシステムのユーザー名	○
CyberArk AIM サービス URL	CyberArk AIM ウェブサービスの URL です。デフォルトでは、Tenable Vulnerability Management は `/AIMWebservice/v1.1/AIM.asmx` を使用します。	×
ドメイン	ユーザー名が属するドメイン	×
Central Credential Provider ホスト	CyberArk Central Credential Provider の IP/DNS アドレス。	○
Central Credential Provider ポート	CyberArk Central Credential Provider がリッスンするポート	○
Central Credential Provider ユーザー名	ボールトユーザー名。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に基本情報を使用します。	×
Central Credential Provider パスワード	ボールトパスワード。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に基本情報を使用します。	×
Safe	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 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	×
CyberArk クライアント証明書のプライベー	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	×

オプション	説明	必須
トキー		
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	プライベートキーのパスフレーズ(必要な場合)	×
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	○
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	○
ポリシー ID	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	×
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	×
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 アカウント詳細名	CyberArk から取得する認証情報の一意の名前	×

Windows 認証方法: Delinea

オプション	説明	必須
Delinea Authentication Method (Delinea 認証方法)	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 サーバーに入る際の認証に使用されるユーザー名。	○

Delinea Password	Delinea サーバーに入る際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	シークレット サーバー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 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	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 Password	Delinea サーバーに入る際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。	○
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。	○
Use SSL (SSL の使用)	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。	×

Windows 認証方法: 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 Vulnerability Management 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。

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。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 Vulnerability Management バージョン: KV1、KV2、AD、LDAP。Tenable Vulnerability Management バージョンの詳細については、Tenable Vulnerability	○

	Management 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 Vulnerability Management 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 エンジン URL	(KV2) Tenable Vulnerability Management 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/kv_mount_name`。末尾の / なし **注意:** 追加の文字列/セグメントである `data` が KV v2 ストアの Vault に対して行われた読み取りリクエストに挿入されるため、KV2 エンジン URL の秘密へのパスを使用することはできません。**[エンジン URL]** フィールドには、秘密へのパスではなく、KV マウントの名前のみを入力します。 **注意:** `data` セグメントを自分で含める必要はありません。秘密名/パスに含めると、Vault への読み取り呼び出しに無効な `/data/data` が含められます。	○ (KV2 **Vault タイプ**を選択した場合)
AD Engine URL (AD エンジン URL)	(AD) Tenable Vulnerability Management 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 Vulnerability Management 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。	○

ドメイン鍵	(KV1 および KV2) ドメインが格納されている Hashicorp Vault での名前です。	×
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。	○
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)	(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 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。	×
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)。	○
レルム (SSH)	(Kerberos ターゲット認証が有効な場合は必須。) このレルムは、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 (例: example.com)。	○
Use SSL (SSL の使用)	有効にすると、Tenable Vulnerability Management 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。	×
SSL 証明書を検証する	有効にすると、Tenable Vulnerability Management 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	×

	効にするには、Hashicorp Vault で SSL を使用する必要があります。	
Tenable Vulnerability Management に対して有効にする	Tenable Vulnerability Management での IBM DataPower Gateway の使用を有効または無効にします。	○
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 および 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 Vulnerability Management 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、[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。
昇格アカウント認証情報 ID または識別子 (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。	×

Windows 認証方法: Kerberos

オプション	Default (デフォルト)	説明	必須
ユーザー名	なし	ターゲットシステムのユーザー名	○
パスワード	なし	ターゲットシステムのパスワード	○
キー配布センター (KDC)	なし	ユーザーにセッションチケットを提供するホスト	○

オプション	Default (デフォルト)	説明	必須
KDC ポート	88	KDC がポート 88 以外で動作している場合に、Tenable Vulnerability Management に KDC への接続先を指定します。	×
KDC Transport	TCP	KDC サーバーにアクセスする方法 **注意:** [KDC Transport] を **[UDP]** に設定した場合は、ポート番号も変更する必要があります。実装に応じて、KDC UDP プロトコルはデフォルトでポート 88 または 750 を使用するためです。	×
ドメイン	なし	KDC が管理する Windows ドメイン。	○

Windows 認証方法: Lieberman RED

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	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 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 ポート	Lieberman がリッスンするポート。	○
Lieberman API	Tenable Vulnerability Management が Lieberman へのアクセスに使	×

オプション	説明	必須
URL	用する URL。	
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 パスワード	Lieberman 明示ユーザーのパスワード。	○
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*)。	×
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 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 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 の使用)	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。	×

オプション	説明	必須
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。	×

Windows 認証方法: LM Hash

Lanman 認証方法は、Windows NT および初期 Windows 2000 サーバーの展開において一般的でした。これは下位互換性のために保持されます。

オプション	説明	必須
ユーザー名	ターゲットシステムのユーザー名	○
Hash	使用するハッシュ	○
ドメイン	ユーザー名が属する Windows ドメイン	×

Windows 認証方法: NTLM Hash

Windows NT で導入された NTLM 認証方法は、Lanman 認証よりも向上したセキュリティを提供しました。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、Tenable Vulnerability Management 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。

オプション	説明	必須
ユーザー名	ターゲットシステムのユーザー名	○
Hash	使用するハッシュ	○
ドメイン	ユーザー名が属する Windows ドメイン	×

Windows 認証方式: パスワード

オプション	説明	必須
ユーザー名	ターゲットシステムのユーザー名	○
パスワード	ターゲットシステムのパスワード	○
ドメイン	ユーザー名が属する Windows ドメイン	×

Windows 認証方法: QiAnXin

オプション	説明	必須
QiAnXin ホスト	QiAnXin ホストの IP アドレスまたは URL。	○
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 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 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	○
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。	×
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	×

オプション	説明	必須
	• **HP_UNIX** - HP Unix • **SOLARIS** - Solaris • **OPENLDAP** - OpenLDAP • **POSTGRESQL** - PostgreSQL	
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。
Use SSL (SSL の使用)	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。	×

Windows 認証方法: Thycotic Secret Server

オプション	説明	必須
ユーザー名	SSH 経由のシステム認証に使用されるユーザー名	○
Domain (ドメイン)	ユーザー名が属するドメイン	×
Thycotic シークレット名	Thycotic サーバーのシークレットの値。シークレットには、Thycotic 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。	○
Thycotic Secret Server URL	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。この値は、Thycotic サーバーの **[管理者]** > **[設定]** > **[アプリケーションの設定]** > **[シークレットサーバー URL]** にあります。 たとえば、次のアドレスがあるとします。 `https://pw.mydomain.com/SecretServer/`	○

	• **`https`** は SSL 接続を示します。 • **`pw.mydomain.com`** はターゲットアドレスです。 • **`/SecretServer/`** はルートディレクトリです。	
Thycotic ログイン名	Thycotic サーバーを認証するためのユーザー名	○
Thycotic パスワード	Thycotic サーバーを認証するためのパスワード	○
Thycotic Organization	クエリする企業この値を Thycotic のクラウドインスタンスに使用できます。	×
Thycotic Domain	Thycotic サーバーのドメイン	×
SSL 証明書を検証する	Tenable.io でサーバーの SSL 証明書が信頼できる CA によって署名されたかどうかを確認します。	×

Windows 認証方法: BeyondTrust

オプション	説明	必須
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 IP アドレスまたは DNS アドレス	○
BeyondTrust port	BeyondTrust がリッスンするポート。	○
BeyondTrust API user	BeyondTrust が提供する API ユーザー	○
BeyondTrust API key	BeyondTrust が提供する API キー	○

Checkout duration	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：** 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 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 BeyondTrust がパスワードを変更すると、スキャンは失敗します。	○
SSL を使用する	有効にすると、Tenable Vulnerability Management 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。	×
SSL 証明書を検証する	有効にすると、Tenable Vulnerability Management 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。	×

Windows のスキャン全体の認証情報タイプの設定

これらの設定は、現在のスキャンのすべての Windows タイプの認証情報に適用されます。これらの設定は、現在のスキャンの認証情報のインスタンスで編集できます。変更内容は、スキャン中のそのタイプの他の認証情報に自動的に適用されます。

オプション	Default（デフォルト）	説明
暗号化されていない認証情報を送信しない	有効	デフォルトでは、セキュリティ上の理由からこのオプションは有効になっています。
NTLMv1 認証を使用しない	有効	**[NTLMv1 認証を使用しない]** 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

オプション	Default (デフォルト)	説明
		使用し、Tenable Vulnerability Management 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 Tenable Vulnerability Management 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めに使用される可能性もあります。スキャン時に **[NTLMv2 のみ使用]** 設定を有効にすると、Tenable Vulnerability Management 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 は安全でないプロトコルであるため、このオプションはデフォルトで有効になっています。
スキャン中にリモートレジストリを有効にする	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、それを開始するよう Tenable Vulnerability Management に指示します。Tenable Vulnerability Management 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。
スキャン中に管理共有を有効にする	無効	このオプションにより、Tenable Vulnerability Management は管理者権限で読み取り可能な特定のレジストリエントリにアクセスできます。
Start the Server service during the scan	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 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。

Windows 認証方法: Centrify

オプション	説明
Centrify ホスト	(必須) Centrify IP アドレスまたは DNS アドレス **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 ポート	(必須) Centrify がリッスンするポート Tenable Vulnerability Management は初期設定でポート 443 を使用します。
API ユーザー	(必須) Centrify が提供するAPIユーザーです。
API キー	(必須) Centrify が提供する API キー。
テナント	(必須) API に関連付けられた Centrify テナント Tenable Vulnerability Management は初期設定で *centrify* を使用します。
認証 URL	(必須) Tenable Vulnerability Management が Centrify にアクセスするために使用する URLTenable Vulnerability Management は初期設定で */Security* を使用します。
パスワードクエリ URL	(必須) Tenable Vulnerability Management が Centrify 内のパスワードをクエリするために使用する URLTenable Security Center は初期設定で */RedRock* を使用します。
パスワードエンジン URL	(必須) Tenable Vulnerability Management が Centrify 内のパスワードにアクセスするために使用する URLTenable Vulnerability Management は初期設定で */ServerManage* を使用します。
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。
チェックアウト期間	(必須) 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 Security Center における通常のスキャン期間を超えるように設定し、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 Centrify がパスワードを変更すると、スキャンは失敗します。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。

SSL を使用する	有効にすると、Tenable Vulnerability Management 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。
SSL 証明書の検証	有効にすると、Tenable Vulnerability Management 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。

Windows 認証方法: Arcon

オプション	説明
Arcon ホスト	(必須) Arcon IP アドレスまたは DNS アドレス **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 ポート	(必須) Arcon がリッスンするポート Tenable Security Center はデフォルトでポート 444 を使用します。
API ユーザー	(必須) Arcon が提供するAPIユーザーです。
API キー	(必須) Arcon が提供するAPIキーです。
認証 URL	(必須) Tenable Security Center が Arcon にアクセスするために使用する URL
パスワードエンジン URL	(必須) Tenable Security Center が Arcon 内のパスワードにアクセスするために使用する URL
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 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。
チェックア	(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**

ウト期間	**ウトの期間**は、Tenable Security Center 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。 **ヒント:** 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 Security Center 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。
Use SSL (SSL の使用)	有効にすると、Tenable Security Center 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。
SSL 証明書の検証	有効にすると、Tenable Security Center 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。
権限昇格	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権限昇格方法です。**[権限昇格]** 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。詳細は、権限昇格を参照してください。

Windows 認証の考慮事項

認証方法について:

- Tenable Vulnerability Management は、リモート Windows Server で必要とされる場合、SMB 署名を自動的に使用します。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 LOphtCrack 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。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。Tenable Vulnerability Management は、SPNEGO スキャンとポリシーの使用をサポートします。すなわち、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 認証または Kerberos 認証を通じて行われるため、Tenable Vulnerability Management スキャン設定では何も設定する必要がありません。

- 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、Tenable Vulnerability Management はNTLMSSP/LMv2 認証を介してログインを試みます。上記が失敗した場合、Tenable Vulnerability Management は NTLM 認証を使用してログインを試行します。

- Tenable Vulnerability Management は、Windows ドメインでの Kerberos 認証の使用もサポートしています。これを設定するには、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)を指定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 Tenable Vulnerability Management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、Tenable Vulnerability Management 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 ドメインフィールドはオプションであり、Tenable Vulnerability Management はこのフィールド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が何であろうと、Tenable Vulnerability Management 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には、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際にも管理者のユーザー名が使用されますが、ドメインパスワードとドメイン名が共に使用されます。

複数の SMB アカウントが設定されている場合、Tenable Vulnerability Management は指定された認証情報を使用して順番にログインを試みます。Tenable Vulnerability Management 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を表示するには、管理者権限で DOS プロンプトを開いて、次のコマンドを実行します。

```
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、Tenable Vulnerability Management 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 では、テストを容易にするために、ネットワーク管理者が特定のドメインアカウントを作成することを推奨しています。Tenable Vulnerability Management は、ドメインアカウントが提供された場合、Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2 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。Tenable Vulnerability Management はアカウントが提供されていなくても、大抵の場合に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。Tenable Vulnerability Management 認証スキャンで認証情報を使用してシステムを完全に監査するには、このサービスが開始される必要があります。

詳細は、Tenable のブログ記事 Dynamic Remote Registry Auditing - Now you see it, now you don't! を参照してください。

Windows システム上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。Tenable Vulnerability Management プラグインは、プラグインが適切に実行されるように、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 Tenable Vulnerability Management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。

権限昇格

選択した**認証方法**の**[設定]**タブの**[特権の昇格方法]**部分にある次の認証方法をスキャンで使用する場合は、認証スキャンの作成時に権限昇格を追加できます。

昇格に対応する認証方法	対応している昇格方法
Arcon 証明書 CyberArk Kerberos パスワード 公開鍵 Thycotic シークレットサーバー	.k5login Cisco 'enable' dzdo pbrun su su+sudo sudo

下の表には、権限昇格の設定が必要な追加の認証情報オプションが記載されています。

注意: BeyondTrust の PowerBroker (pbrun) と Centrify の DirectAuthorize (dzdo) は、Unix システムと Linux システム用の独自のルートタスク委任方法です。

ヒント: su+sudo を使用して実行されるスキャンでは、ユーザーが権限のないアカウントでスキャンしてから、リモートホストで sudo 権限を持つユーザーに切り替えることができます。これは、リモート権限によるログインが禁止されている場所で重要になります。

注意: sudo を使用して実行されるスキャンと、root ユーザーを使用して実行されるスキャンでは、必ずしも同じ結果が返されません。これは、sudo ユーザーには異なる環境変数が適用されることと、その他の微妙な違いによるものです。詳細については、https://www.sudo.ws/docs/man/sudo.man/を参照してください。

Arcon の権限昇格オプション

オプション	昇格タイプ	説明	必須
昇格アカウント名	.k5login dzdo pbrun su su+sudo sudo	昇格した権限があるアカウントのユーザー名	○

昇格ユーザー名	.k5login Cisco 'enable' dzdo pbrun su su+sudo sudo Checkpoint Gaia 'エキスパート'	昇格した権限があるアカウントのユーザー名	○
Escalation password	dzdo su su+sudo	昇格した権限があるアカウントのパスワード	○
Location of dzdo (ディレクトリ)	dzdo	dzdo コマンドのディレクトリパス	×
Location of pbrun (ディレクトリ)	pbrun	pbrun コマンドのディレクトリパス	×
Location of su (ディレクトリ)	su	su コマンドのディレクトリパス	×
Location of su and sudo (ディレクトリ)	su+sudo	su コマンドと sudo コマンドのディレクトリパス	×
Location sudo (ディレクトリ)	sudo	sudo コマンドのディレクトリパス	×
SSH user password	pbrun	昇格した権	○

		限があるアカウントのパスワード	
su login	su	su 権限があるアカウントのユーザー名	○
su user	su+sudo	su 権限があるアカウントのユーザー名	○
sudo password	sudo	sudo 権限があるアカウントのパスワード	○
sudo user	su+sudo sudo	sudo 権限があるアカウントのユーザー名	○

証明書、Kerberos、パスワード、公開鍵の権限昇格オプション

オプション	昇格タイプ	説明	必須
Enable password	Cisco 'enable'	Cisco デバイスで 'enable' ユーティリティを実行するためのパスワード	○
Escalation account	.k5login pbrun dzdo	昇格した権限があるアカウントのユーザー名	○
Escalation password	dzdo pbrun su	昇格した権限があるアカウントのパスワード	○

	su+sudo		
Location of dzdo (ディレクトリ)	dzdo	dzdo コマンドのディレクトリパス	×
Location of pbrun (ディレクトリ)	pbrun	pbrun コマンドのディレクトリパス	×
Location of su (ディレクトリ)	su	su コマンドのディレクトリパス	×
Location of su and sudo (ディレクトリ)	su+sudo	su コマンドと sudo コマンドのディレクトリパス	×
Location sudo (ディレクトリ)	sudo	sudo コマンドのディレクトリパス	×
SSH user password	pbrun	昇格した権限があるアカウントのパスワード	○
su login	su	su 権限があるアカウントのユーザー名	○
su user	su+sudo	su 権限があるアカウントのユーザー名	○
sudo password	sudo	sudo 権限があるアカウントのパスワード	○
sudo user	su+sudo sudo	sudo 権限があるアカウントのユーザー名	○

CyberArk の権限昇格オプション

オプション	昇格タイプ	説明	必須
CyberArk アカウント詳細名	.k5login Cisco 'enable' dzdo pbrun su su+sudo sudo	昇格した権限がある CyberArk アカウントの名前パラメーター	○

Escalation account	dzdo	昇格した権限があるアカウントのユーザー名	○
Location of dzdo (ディレクトリ)	dzdo	dzdo コマンドのディレクトリパス	×
Location of pbrun (ディレクトリ)	pbrun	pbrun コマンドのディレクトリパス	×
Location of su (ディレクトリ)	su	su コマンドのディレクトリパス	×
Location of su and sudo (ディレクトリ)	su+sudo	su コマンドと sudo コマンドのディレクトリパス	×
Location sudo (ディレクトリ)	sudo	sudo コマンドのディレクトリパス	×
su login	su	su 権限があるアカウントのユーザー名	○
su user	su+sudo	su 権限があるアカウントのユーザー名	○
sudo user	su+sudo sudo	sudo 権限があるアカウントのユーザー名	○

Thycotic シークレットサーバーの権限昇格オプション

オプション	昇格タイプ	説明	必須
Thycotic Escalation Account	.k5login Cisco 'enable' dzdo pbrun su su+sudo sudo	昇格した権限がある Thycotic アカウントの名前パラメーター	○
Location of dzdo (ディレクトリ)	dzdo	dzdo コマンドのディレクトリパス	×

Location of pbrun (ディレクトリ)	pbrun	pbrun コマンドのディレクトリパス	×
Location of su (ディレクトリ)	su	su コマンドのディレクトリパス	×
Location of su and sudo (ディレクトリ)	su+sudo	su コマンドと sudo コマンドのディレクトリパス	×
Location sudo (ディレクトリ)	sudo	sudo コマンドのディレクトリパス	×
su user	su+sudo	su 権限があるアカウントのユーザー名	○

その他

Tenable Vulnerability Management は、次に説明する追加の認証方法をサポートしています。

注意: 選択したスキャンテンプレートによっては、一部の認証情報タイプが設定に利用できない場合があります。

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 Vulnerability Management 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 Vulnerability Management 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。この操作のためにスキャン設定でポートを指定する必要はありません。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。

オプション	説明
Domain Controller	(必須) ActiveSync のドメインコントローラーの名前
ドメイン	(必須) ActiveSync の Windows ドメインの名前
Domain Admin	(必須) ドメイン管理者のユーザー名
Domain Password	(必須) ドメイン管理者のパスワード

Tenable Vulnerability Management 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。Tenable Vulnerability Management は、Exchange Server 2007 から情報を取得できません。

F5

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明
ユーザー名	(必須) F5 ターゲットのスキャンアカウントのユーザー名
パスワード	(必須) スキャンアカウントに関連付けられるパスワード

ポート	F5 ターゲットに接続するときに使用するポート
HTTPS	有効にすると、安全な通信 (HTTPS) を使用して接続されます。無効にすると、標準的な HTTP を使用して接続されます。
SSL 証明書を検証する	SSL 証明書の有効性を検証します。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。

IBM iSeries

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明
ユーザー名	(必須) iSeries ユーザー名
パスワード	(必須) iSeries のパスワード。

NetApp API

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明
ユーザー名	(必須) HTTPS アクセスを持つ NetApp システムのアカウントのユーザー名
パスワード	(必須) アカウントに関連付けられるパスワード
vFiler	この設定が空白の場合、スキャンはターゲットシステムで検出されたすべての NetApp 仮想ファイラー (vFiler) を監査します。監査を 1 つの vFiler に制限するには、vFiler の名前を入力します。
ポート	ターゲットシステムでスキャンするポートポート番号のコンマ区切りリストを入力します。

Nutanix Prism

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明	Default (デフォルト)
Nutanix Host	(必須) Nutanix Prism Central ホストのホスト名または IP アドレス。	-
Nutanix Port	(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
Username (ユーザー名)	(必須) Nutanix Prism Central ホストへの認証に使用されるユーザー名。	-
Password (パスワード)	(必須) Nutanix Prism Central ホストへの認証に使用されるパスワード。	-
Discover Host	このオプションは、検出された Nutanix Prism Central ホストをスキャン対象のスキャンターゲットに追加します。	-
Discover Virtual Machines	このオプションは、検出された Nutanix Prism Central 仮想マシンをスキャン対象のスキャンターゲットに追加します。	-
HTTPS	有効にすると、Tenable Vulnerability Management が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable Vulnerability Management 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 Vulnerability Management 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

OpenStack

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明

ユーザー名	(必須) OpenStack デプロイメントのアカウントのユーザー名
パスワード	(必須) アカウントに関連付けられるパスワード
Tenant Name for Authentication	(必須) スキャンが認証に使用する特定のテナントの名前テナント (別名プロジェクト) は、テナント内のユーザーが制御できるリソースのグループです。
ポート	(必須) スキャナーが OpenStack への接続に使用するポート
HTTPS	有効にすると、安全な通信 (HTTPS) を使用して接続されます。無効にすると、標準的な HTTP を使用して接続されます。
SSL 証明書を検証する	SSL 証明書の有効性を検証します。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。

Palo Alto Networks PAN-OS

オプション	説明
ユーザー名	(必須) PAN-OS ユーザー名
パスワード	(必須) PAN-OS パスワード
ポート	(必須) 管理ポート番号。
HTTPS	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management が認証するかどうかを設定します。
SSL 証明書を検証する	SSL 証明書の有効性を検証します。ターゲットが自己署名証明書を使用している場合は、この設定を無効化します。

Red Hat Enterprise Virtualization (RHEV)

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明
ユーザー名	(必須) RHEVサーバーにログインするためのユーザー名
パスワード	(必須) RHEVサーバーにログインするためのパスワードに対するユーザー名

オプション	説明
ポート	RHEV サーバーへの接続用ポート
SSL 証明書を検証する	RHEV サーバーの SSL 証明書の有効性を検証

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。さらに、SSL 証明書の検証を有効にしないオプションがあります。

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明
ユーザー名	(必須) ESXi サーバーにログインするためのユーザー名
パスワード	(必須) ESXi サーバーにログインするためのパスワードに対するユーザー名
Do not verify SSL Certificate	ESXi サーバーの SSL 証明書の有効性を検証しません。

VMware vCenter SOAP API

VMware vCenter SOAP API を通じて vCenter にアクセスできます。利用可能な場合は、SOAP API に加えて vCenter REST API を使用してデータを収集します。

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。

注意: 読み取りと書き込みのアクセス許可を持つ vCenter 管理者アカウントを使用する必要があります。

オプション	説明
vCenter Host	(必須) vCenter ホストの名前
vCenter Port	vCenter ホストにアクセスするためのポート
ユーザー名	(必須) vCenter サーバーへのログイン用ユーザー名

オプション	説明
パスワード	(必須) vCenter サーバーへのログイン用ユーザー名のパスワード
HTTPS	SSL 経由で vCenter に接続
SSL 証明書を検証する	ESXi サーバーの SSL 証明書の有効性を検証

VMware vCenter の自動検出

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

Tenable Vulnerability Management 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 Vulnerability Management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 を使用するには、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 Manager アカウントが必要です。

オプション	説明	Default (デフォルト)
vCenter Host	(必須) vCenter ホストの名前。	-
vCenter Port	(必須) Tenable Vulnerability Management 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 Vulnerability Management 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。	-
HTTPS	有効にすると、Tenable Vulnerability Management が安全な通信 (HTTPS) を使用して接続します。無	有効

オプション	説明	Default (デフォルト)
	効にすると、Tenable Vulnerability Management 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 Vulnerability Management 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
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。	有効になっていません
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。	有効になっていません

X.509

注意: この認証情報タイプは、[高度なネットワークスキャン] テンプレートでのみ使用できます。

オプション	説明
Client certificate	(必須) クライアント証明書。
Client key	(必須) クライアントのプライベートキー。
Password for key	(必須) キーのパスフレーズ
CA certificate to trust	(必須) 信頼できる認証局 (CA) のデジタル証明書

モバイル

注意: 選択したスキャンテンプレートによっては、一部の認証情報タイプが設定に利用できない場合があります。

ActiveSync

オプション	Default (デフォルト)	説明
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。
ドメインユーザー名	--	ActiveSync への認証に Tenable Vulnerability Management が使用する、ドメイン管理者のアカウントのユーザー名。
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 Vulnerability Management 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 Vulnerability Management が使用できるスキャナーは 1 つだけです。
スケジュールの更新	毎日 12:30 ~ 04:00	Tenable Vulnerability Management 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 Vulnerability Management 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

設定	デフォルト値	説明	必須
AirWatch 環境 API URL	-	Workspace ONE API の URL エンドポイントです。(例: https://xxx.awmdm.com/api)	○

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。	yes
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。	yes
Password (パスワード)	–	AirWatch ユーザーのパスワード。	yes
API キー	–	VMware Workspace ONE API の API キー。	yes
HTTPS	Enabled (有効)	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management 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 Vulnerability Management が検証できるようにします。	×

Apple プロファイルマネージャー

設定	デフォルト値	説明	必須
サーバー	–	Apple プロファイルマネージャでの認証用サーバー URL	○
ポート	443	Tenable Vulnerability Management が Apple プロファイルマネージャでの認証に使用するポート	○
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	○
HTTPS	有効	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management が認証するかどうかを設定します。	×

Verify SSL Certificate (SSL 証明書の検証)	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ことを Tenable Vulnerability Management が検証するかどうか。	×
スキャン全体の認証情報タイプの設定			
デバイスを強制的に更新	有効	Apple プロファイルマネージャーを使用して直ちに、デバイスを強制的に更新します。	×
デバイス更新のタイムアウト (分)	5	デバイスが Apple プロファイルマネージャーに再接続するまでに待機する分数です。この設定を省略すると、Tenable Vulnerability Management はデフォルトのタイムアウト (5 分) を使用します。	×

Blackberry UEM

オプション	説明
ホスト名	Blackberry UEM での認証用サーバー URL
ポート	Blackberry UEM での認証に使用するポート
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 Vulnerability Management 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 Vulnerability

	Management で使用するアカウントのパスワード。
HTTPS	有効な場合、Tenable Vulnerability Management 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)	Tenable Vulnerability Managementは有効時に、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します。

Good MDM

注意: 1 万件を超える資産をスキャンしている場合、Good MDM の認証スキャンが失敗する可能性があります。

設定	デフォルト値	説明	必須
サーバー	-	(必須) Good MDM で認証するサーバー URL	○
ポート	-	(必須) Good MDM で認証するために使用するポートの設定	○
ドメイン	-	(必須) Good MDM のドメイン名	○
ユーザー名	-	(必須) 認証するユーザー名	○
パスワード	-	(必須) 認証するパスワード	○
HTTPS	有効	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management が認証するかどうかを設定します。	×
Verify SSL Certificate (SSL 証明書の検証)	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ことを Tenable Vulnerability Managementが検証するかどうか。	×

> Intune

オプション	説明
テナント	App 登録で表示される Microsoft Azure Directory (tenant) の ID

Client	App 登録中に作成される Microsoft Azure Application (client) の ID
Secret	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 Vulnerability Management 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 Vulnerability Management で使用するアカウントのパスワード。

MaaS360

設定	デフォルト値	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	–	MaaS360 での認証用サーバー URL	○
Platform ID	–	MaaS360 用に提供されたプラットフォーム ID	○
Billing ID	–	MaaS360 用に提供された請求 ID	○
App ID	–	MaaS360 用に提供されたアプリ ID	○
App Version	–	MaaS360 アプリのバージョン	○
App access key	–	MaaS360 用に提供されたアプリのアクセスキー	○
すべてのデバイスデータの収集	日付を指定	有効にすると、スキャンは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

設定	デフォルト値	説明	必須
VSP Admin Portal URL	–	Tenable Vulnerability Management が MobileIron 管理ポータルでの認証に使用するサーバー URL	○
VSP Admin Portal Port	443	Tenable Vulnerability Management が MobileIron 管理ポータルでの認証に使用するポート	×
ポート	443	Tenable Vulnerability Management が MobileIron システムマネージャーでの認証に使用するポート	○
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	○
HTTPS	有効	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management が認証するかどうかを設定します。	×
Verify SSL Certificate (SSL 証明書の検証)	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ことを Tenable Vulnerability Managementが検証するかどうか。	×

Workspace ONE

注意: Workspace ONE 統合が適切に機能するには、自分のロールで使用できるすべての**読み取り専用**アクセス許可が割り当てられていなければなりません。詳細は、VMware ドキュメントを参照してください。

設定	デフォルト値	説明	必須
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)	○
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。	yes
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。	yes
Workspace ONE パスワード	–	Workspace ONE ユーザーのパスワード。	yes
API キー	–	VMware Workspace ONE API の API キー。	yes
HTTPS	Enabled (有効)	暗号化 (HTTPS) 接続または非暗号化 (HTTP) 接続で Tenable Vulnerability Management 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 Vulnerability Management が検証できるようにします。	×
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。	×
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

注意: 選択したスキャンテンプレートによっては、一部の認証情報タイプが設定に利用できない場合があります。

Tenable Vulnerability Management では、パッチ管理システムの認証情報を利用して、Nessus Professional または管理対象スキャナーが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。

Tenable Vulnerability Management は次をサポートしています。

- 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

Vulnerability Management スキャンを作成するで説明したように、スキャンの作成中に**[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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management は Tenable Vulnerability ManagementHCL 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 Vulnerability Management 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	Default (デフォルト)
Server	(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 Vulnerability Management からの通信に対して KACE K1000 がリッスンする TCP ポート。	3306
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
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 Vulnerability Management が使用する、KACE K1000 のアカウントのユーザー名。	R1
K1000 Database Password	(必須) KACE K1000 ユーザーのパスワード。	-

HCL Tivoli Endpoint Manager (BigFix)

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 Vulnerability Management 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 Vulnerability Management 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	Default (デフォルト)
Web Reports Server	(必須) HCL Bigfix ウェブレポートサーバーの名前。	-
Web Reports Port	(必須) Tenable Vulnerability Management 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。	-
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 Vulnerability Management 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	(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 Vulnerability Management が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable Vulnerability Management 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 Vulnerability Management 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。	Enabled (有効)

オプション	説明	Default (デフォルト)
	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。	

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 Vulnerability Management 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. <
        <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
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 tr
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 debianp
(exists true whose (if true then (exists rpm) else false)) then unique values of (name of it & "|" & version of
"|" & "rpm" & "|" & architecture of it & "|" & architecture of operating system) of packages of rpm else if (exi
(if true then (exists ips image) else false)) then unique values of (full name of it & "|" & version of it as st
"pkg" & "|" & architecture of operating system) of latest installed packages of ips image else if (exists true w
then (exists pkgdb) else false)) then unique values of(pkginst of it & "|" & version of it & "|" & "pkg10") of p
pkgdb else "<unsupported>"]]></Property>
        <Property Name="Tenable AIX Technology Level" ID="76">current technology level of operating system</Prop
        <Property Name="Tenable Solaris - Showrev -a" ID="77"><![CDATA[if ((operating system as string as lowerc
"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)

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 Vulnerability Management 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 Vulnerability Management 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)。このサーバーでは SQL データベースや別のサーバーに配置されている可能性がある SCCM リポジトリも実行される場合があります。この監査を活用する場合、構成

済みのセンサー Tenable Vulnerability Management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**読み取り専用アナリスト**、**オペレーション管理者**、または**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	Default (デフォルト)
Server	(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 Vulnerability Management 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。	-

Microsoft Windows Server Update Services (WSUS)

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 Vulnerability Management 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 Vulnerability Management 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	Default (デフォルト)
Server	(必須) WSUS の IP アドレスまたはシステム名。	-

オプション	説明	Default (デフォルト)
ポート	(必須) Tenable Vulnerability Management 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 Vulnerability Management が使用する、WSUS 管理者アカウントのユーザー名。	-
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 Vulnerability Management が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable Vulnerability Management 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 Vulnerability Management 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 5 サーバー

Red Hat Satellite 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 Vulnerability Management 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 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。

Satellite スキャンでは、Tenable プラグインの 84236、84235、84234、84237、84238 を使用します。

オプション	説明	デフォルト
Satellite サーバー	(必須) Red Hat Satellite の IP アドレスまたはシステム名	-
ポート	(必須) Tenable Vulnerability Management からの通信に対して Red Hat Satellite 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 Vulnerability Management が使用する、Red Hat Satellite のアカウントのユーザー名。	-
Password (パスワード)	(必須) Red Hat Satellite ユーザーのパスワード。	-
Verify SSL Certificate (SSL 証明書の検証)	有効にすると、Tenable Vulnerability Management 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

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 Vulnerability Management 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 サー	(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
バー		
ポート	(必須) Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management が安全な通信 (HTTPS) を使用して接続します。 無効にすると、Tenable Vulnerability Management 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 Vulnerability Management 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 Altiris

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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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	Default (デフォルト)
Server	(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 Vulnerability Management 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 Vulnerability Management 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	(必須) Altiris MSSQL データベースユーザーのパスワード。	-
Use Windows Authentication	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。	無効

プレーンテキスト認証

警告: プレーンテキストの認識情報の使用は推奨しません。可能であれば、暗号化認証を使用してください。

認証情報チェックを安全に行う方法が使用できない場合、**[プレーンテキスト認証]** 設定を使用することで、安全ではないプロトコルを介してチェックを実行するように Tenable Vulnerability Management を設定できます。

注意: 選択したスキャンテンプレートによっては、一部の認証情報タイプが設定に利用できない場合があります。

FTP

設定	デフォルト値	説明	必須
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○

HTTP

設定	Default (デフォルト)	説明	必須
認証方法	HTTP Login Form	認証方法。 サポートする値は以下のとおりです。 • Automatic Authentication • Basic/Digest Authentication • HTTP login form - 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制御します。 • HTTP cookies import - ウェブアプリケーションにアクセスを試みる際、別のソフトウェア (ウェブブラウザ、ウェブプロキシなど) からインポートした Cookie を使用して、ウェブアプリケーショ	○

設定	Default (デフォルト)	説明	必須
		ンのテストを簡略化します。	
メソッド: Automatic Authentication			
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○
メソッド: Basic/Digest Authentication			
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○
メソッド: HTTP login form			
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○
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 (/login.html など)	○
ログイン送信ページ	-	フォーム方法の操作パラメーター。<form method="POST" name="auth_form" action="/login.php"> のログインフォームは /login.php など。	○
ログインパラメーター	-	認証パラメーター (login=%USER%&password=%PASS% など) を指定します。キーワード %USER% や %PASS% 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メニューで提供される値に置き換えられます。必要な場合、このフィールドを使用して複数のパラメーターを提供できます。(認証プロセスでグループ名と他の情報が必要な場合など)	○
ページで認証を検	-	認証が必要な保護された Web ページへの絶対パ	○

設定	Default (デフォルト)	説明	必須
証		ス (/admin.html など) で、Tenable Vulnerability Management が認証ステータスを判断しやすくします。	
Regex to verify successful authentication	–	ログインページで検索する正規表現パターン200 件の応答コードを受信してもセッションステータスを判断するためには十分ではない場合があります。Tenable Vulnerability Management は「認証に成功しました」などの所与の文字列との照合を試みることができます。	○
メソッド: HTTP cookies import			
Cookies ファイル	–	Cookie ファイルをアップロードします。ファイルは Netscape 形式である必要があります。	○
すべてのメソッド: Scan-wide Credential Type Settings			
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。	○
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。時間遅延を設定すると、ブルートフォースロックアウトメカニズムのトリガーの回避に利用できます。	○
Follow 30x redirections (レベル数)	0	ウェブサーバーから 30x 系のリダイレクトコードを受信した場合に、提供されたリンクに従うかどうかを、この設定で Tenable Vulnerability Management に指示します。	○
認証された正規表現の反転	無効	ログインページで検索する正規表現パターン。パターンが見つかった場合、認証が成功しなかったことが Tenable Vulnerability Management に通知されます。(例: 認証に失敗しました。)	×

設定	Default (デフォルト)	説明	必須
認証された正規表現の HTTP ヘッダーでの使用	無効	認証状態をより適切に判断するために、Tenable Vulnerability Management が与えられた正規表現パターンで、レスポンスの本文ではなく HTTP レスポンスヘッダーを検索することを許可します。	×
大文字と小文字を区別しない認証された正規表現	無効	regex 検索は、デフォルトで大文字と小文字を区別します。このオプションでは、大文字と小文字を区別しないよう Tenable Vulnerability Management に指示します。	×

IMAP

設定	デフォルト値	説明	必須
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○

IPMI

設定	デフォルト値	説明	必須
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○

NNTP

設定	デフォルト値	説明	必須
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○

POP2

設定	デフォルト値	説明	必須
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○

POP3

設定	デフォルト値	説明	必須
ユーザー名	-	ログインユーザーの名前	○
パスワード	-	指定されたユーザーのパスワード	○

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	デフォルト値	説明	必須
Community string	public	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	○
スキャン全体の認証情報タイプの設定			
UDP ポート	161	Tenable Vulnerability Management がホストデバイスで認証を試みるポートです。	×
追加の UDP ポート #1	161		×
追加の UDP ポート #2	161		×
追加の UDP ポート #3	161		×

telnet/rsh/rexec

Tenable Vulnerability Management は Windows 以外のターゲットのみパッチ監査を行います。

設定	デフォルト値	説明	必須
ユーザー名	–	ログインユーザーの名前	○
パスワード	–	指定されたユーザーのパスワード	○
スキャン全体の認証情報タイプの設定			
telnet を使用してパッチ監査を実行	無効	Tenable Vulnerability Management は、パッチ監査のために telnet を使用してホストデバイスに接続します。	×
rsh を使用してパッチ監査を実行	無効	Tenable Vulnerability Management は、パッチ監査のために rsh を使用してホストデバイスに接続します。	×
rexec を使用してパッチ監査を実行	無効	Tenable Vulnerability Management は、パッチ監査のために rexec を使用してホストデバイスに接続します。	×

Tenable Vulnerability Management スキャンにおけるコンプライアンス

注意: スキャンがユーザー定義テンプレートに基づいている場合、スキャンの **[コンプライアンス]** 設定は行えません。これらの設定は、関連するユーザー定義テンプレートでのみ変更できます。

Tenable Vulnerability Management 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 Vulnerability Management 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。

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

コンプライアンスチェック	必要な認証情報
Brocade Fabricos	SSH
Check Point GAiA	SSH
Cisco ACI	SSH
Cisco Firepower	SSH
Cisco IOS	SSH
Cisco Viptela	SSH
Citrix Application Delivery	SSH
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	SSH
HP ProCurve	SSH
Huawei VRP	SSH
IBM DB2 DB	**データベース**
IBM iSeries	IBM iSeries
Juniper Junos	SSH
Microsoft Azure	Microsoft Azure
モバイルデバイスマネージャー	AirWatch、Apple Profile Manager、または Mobileiron
MongoDB	MongoDB

コンプライアンスチェック	必要な認証情報
Microsoft SQL Server DB	データベース
MySQL DB	データベース
NetApp API	NetApp API
NetApp Data ONTAP	SSH
OpenShift	OpenShift Container Platform
OpenStack	OpenStack
Oracle DB	データベース
NetApp Data ONTAP	SSH
Palo Alto Networks PAN-OS	PAN-OS
Rackspace	Rackspace
RHEV	RHEV
Salesforce.com	Salesforce SOAP 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 ESX SOAP APIまたはVMware vCenter SOAP API
WatchGuard	SSH
Windows	Windows
Windowsファイルコンテンツ	Windows
Zoom	Zoom
ZTE ROSNG	SSH

Tenable Vulnerability Management スキャンでの 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。SCAP では、OVAL、CVE、CVSS、CPE、FDCC のポリシーなど、複数のオープンスタンダードとポリシーが基準として使用されています。

Tenable Vulnerability Management では、SCAP(および OVAL)コンプライアンスチェックをスキャンに追加できます。**SCAP** 設定をできるのは、**SCAP and OVAL Auditing**スキャンテンプレートを使用している場合のみです。

警告: Tenable Vulnerability Management での SCAP スキャンは検証されていません。

選択肢は **Linux (SCAP)**、**Linux (OVAL)**、**Windows (SCAP)**、**Windows (OVAL)** です。次の表に、各オプションの設定を示します。

設定	デフォルト値	説明
Linux (SCAP)または**Windows (SCAP)**		
SCAP File	なし	すべての SCAP コンテンツを含む有効な zip ファイル。このファイルには、XCCDF、OVAL、CPE バージョン 1.0 と 1.1、DataStream バージョン 1.2 が含まれています。
SCAP Version	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-10-1.2.3.1.zip">`
SCAP Benchmark ID	なし	SCAP XML ファイルからコピーした `Benchmark id`。 例:

		`<xccdf:Benchmark id="xccdf_gov.nist_benchmark_USGCB-Windows-7">`
SCAP Profile ID	なし	SCAP XML ファイルからコピーした `Profile id`。 例: `<xccdf:Profile id="xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1">`
OVAL Result Type	システムの特徴と全結果	結果ファイルに含める情報。 結果ファイルのタイプは、**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**のいずれかになります。
Linux (OVAL) または Windows (OVAL)		
OVAL definitions file	None (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。

Tenable Vulnerability Management スキャンでのプラグインの設定

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なスキャンのアクセス許可: 設定可

必要なテンプレートのアクセス許可: 設定可

注意: スキャンがユーザー定義テンプレートに基づいている場合、スキャンの **[プラグイン]** 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テンプレートでのみ変更できます。

注意: Tenable が新しいプラグインを Tenable Vulnerability Management に追加したときに、そのプラグインが属するプラグインファミリー全体がスキャンポリシーテンプレートで有効になっている場合、その新しいプラグインは自動的に有効になります。ファミリーから一部のプラグインのみを有効にした場合は、新しいプラグインを手動で有効にしてスキャンポリシーに含める必要があります。

Tenable 提供の **[高度なスキャン]** テンプレートを使用してスキャンまたはユーザー定義テンプレートを作成する場合、個別またはプラグインファミリー別にプラグインを有効にする、もしくは無効にすることで、スキャンがどのセキュリティチェックを実施するかを設定できます。

スキャンまたはユーザー定義テンプレートを作成して保存すると、最初に選択されたすべてのプラグインが記録されます。プラグインの更新により新しいプラグインを受領したときに、プラグインが関連付けられているファミリーが有効な場合、このプラグインも自動的に有効になります。ファミリーが無効にされるか、一部のみ有効な場合、そのファミリーの新しいプラグインも自動的に無効になります。

警告: **サービス拒否** ファミリーには、障害を引き起こさない便利なチェックが含まれていますが、その他に、**安全チェック** オプションが有効になっていない場合に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が実行されないようにできます。ただし、Tenable は、保守作業のための時間中で問題に対応できるスタッフがいる場合を除き、本番環境のネットワークでは **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。

スキャンまたはユーザー定義テンプレートのプラグインを設定する方法

1. 次のいずれかを行います。

スキャンを

a. 作成または編集します。

b. ユーザー定義テンプレートを作成または編集します。

2. スキャン設定ページの左側のメニューで、**[プラグイン]** をクリックします。

   [プラグイン] ページが表示されます。このページにはプラグインファミリーの表が含まれます。

3. 次のいずれかを行います。各種の属性を使用して、プラグインファミリーの表を

   - フィルタリングします。
   - プラグインファミリー名を使用して、プラグインファミリーを検索します。検索についての詳細は、Tenable Vulnerability Management の表を参照してください。

4. プラグインファミリーのすべてのプラグインを有効または無効にするには、プラグインファミリーの行にある **[ステータス]** トグルをクリックします。

   - **On** - プラグインファミリーに関連するセキュリティチェックをスキャンに含めます。
   - **Off** - プラグインファミリーに関連するセキュリティチェックをスキャンから除外します。

5. 個別のプラグインファミリーの特定のプラグインを有効または無効にします。

   a. プラグインファミリーの表で、プラグインを編集するプラグインファミリーをクリックします。プラグインファミリープレーンが表示されます。

   b. (オプション) 個別のプラグインをクリックして、プラグインの詳細 (**[概要]**、**[説明]**、および **[ソリューション]**) をレビューします。

   c. 有効または無効にしたいそれぞれのプラグインで、**[ステータス]** チェックボックスを選択または選択解除します。

   d. **[保存]** をクリックします。

      [プラグイン] ページが表示されます。プラグインファミリーの表で、Tenable Vulnerability Management はプラグインファミリーのステータスを次のように更新します。

      - **On** - プラグインファミリーのすべてのプラグインが有効となっている場合、そのプラグインファミリーに関連するセキュリティチェックはスキャンに含まれます。

- **Off** - プラグインファミリーのすべてのプラグインが無効となっている場合、そのプラグインファミリーに関連するセキュリティチェックはスキャンから除外されます。
- **Mixed** - プラグインファミリーの一部のプラグインのみが有効となっている場合、有効となっているプラグインのみがスキャンに含まれます。

e. **[保存]** をクリックして、プラグインファミリーの変更を保存します。

6. **[保存]** をクリックして、スキャンまたはユーザー定義テンプレートの変更を保存します。

Tenable Web App Scanning スキャンの設定

スキャンの設定により、スキャンのパラメーターを独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、スキャンやユーザー定義テンプレートのベースになっている Tenable 提供のテンプレートによって変わります。

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ユーザー定義テンプレートで設定できます。

Tenable Web App Scanning のスキャン設定は、次のカテゴリに分類されます。

- ユーザー定義テンプレートの基本設定
- Tenable Web App Scanning スキャンの基本設定
- Tenable Web App Scanning スキャンの範囲設定
- Tenable Web App Scanning スキャンのレポート設定
- Tenable Web App Scanning スキャンの評価設定
- Tenable Web App Scanning スキャンの詳細設定
- Tenable Web App Scanning スキャンの認証情報
- Tenable Web App Scanning スキャンのプラグイン設定

ユーザー定義テンプレートの設定

ユーザー定義テンプレートを設定する際は、次のことに注意してください。

- ユーザー定義テンプレートを設定すると、その設定はそのユーザー定義テンプレート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。
- ユーザー定義テンプレートは、Tenable 提供のテンプレートをベースにして作成します。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。

  ただし、一部の **[基本]** 設定はユーザー定義テンプレートの作成にだけ使用でき、個別のスキャンの設定時には表示されません。詳細は、ユーザー定義テンプレートの基本設定を参照してください。

- ユーザー定義テンプレートで設定できても、ユーザー定義テンプレートに基づく個別のスキャンで変更することができない設定があります。このような設定には、**[検出]**、**[評価]**、**[レポート]**、**[詳細]**、**[コンプライアンス]**、**[SCAP]**、**[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。
- ユーザー定義テンプレートで**認証情報**を設定した場合、他のユーザーがテンプレート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オーバーライドできます。

Tenable Web App Scanning スキャンの基本設定

設定によって、スキャン設定における組織的およびセキュリティ関連の基本要素を指定します。これには、スキャンの名前、1つまたは複数のターゲット、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の指定が含まれます。

スキャンまたはユーザー定義スキャンテンプレートを作成したときに**設定**できます。任意のスキャンタイプを選択できます。詳細は、スキャンテンプレート を参照してください。

ヒント: 設定を保存して他のスキャンに適用したい場合は、ユーザー定義スキャンテンプレートを作成して設定できます。

[基本] 設定には、次のセクションが含まれます。

- 一般
- スケジュール
- 通知
- ユーザーアクセス許可
- データ共有

一般

スキャンの一般的な設定

設定	デフォルト値	説明	必須
名前	なし	スキャンまたはテンプレートの名前を指定します。	○
説明	なし	スキャンまたはテンプレートの説明を指定します。	×
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。	○
スキャナータイプ	内部スキャナー	ローカルの内部スキャナーとクラウド管理対象スキャナーのどちらがスキャンを実行するかを指定し、**[スキャナー]** フィールドの選択肢として、ローカルスキャナーとクラウド管理対象スキャナーのどちらをリストするかを決めます。	○

設定	デフォルト値	説明	必須
スキャナー	不定	スキャンを実行するスキャナーを指定します。	○
ターゲット	なし	Tenable Web App 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。 **[ファイルからインポート]** リンクをクリックすると、ファイルマネージャーウィンドウが開きます。ターゲットリストは、1 行に 1 つのターゲットが入った TXT 形式でインポートできます。ファイルは 1 MB 以下で、各行は 4096 文字より短くする必要があります。ターゲットを追加した後、リストからターゲットを検索して削除できます。ターゲットをインラインで変更することはできません。 **ヒント:** 新しいターゲットリストをアップロードすると、スキャン内にある既存のターゲットが置き換えられます。複数のターゲットリストがある場合は、Tenable Web App Scanning にアップロードする前にそれらを 1 つのファイルに統合します。 スキャンには、API ターゲットを含むスキャンを除き、最大 1000 個のターゲットを追加できます。API スキャンは一度に 1 つのターゲットのみをサポートします。 **注意:** **[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。 **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。	○

スケジュール

スキャンのスケジュール設定

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、スケジュールの設定はスキャン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スケジュールを設定してください。

設定	Default (デフォルト)	説明
スケジュール	off	スキャンが指定されているかどうかを指定するトグルデフォルトでは、スキャンはスケジュールされていません。 **[スケジュール]** トグルが無効になっている場合、他のスケジュール設定は非表示のままになります。 トグルをクリックする等、スケジュールが有効になり、残りの **[スケジュール]** 設定が表示されます。

頻度	一度	スキャンを開始する頻度を指定します。
		
		注意 : ターゲットをスキャンできる頻度は、いくつかの要因 (ウェブアプリケーションの更新頻度、ウェブアプリケーションに含まれるコンテンツなど) によって異なります。ほとんどのウェブアプリケーションについて、Tenable では少なくとも 1 か月に 1 回スキャンを実行することを推奨しています。
		
		• **一度**: 特定の時間にスキャンをスケジュールします。
		• **日単位**: 特定の時間、または最大 20 日で、日単位でスキャンの実行をスケジュールします。
		• **週単位**: 時間と曜日ごとに、最大 20 週間、継続的にスキャンの実行をスケジュールします。
		• **月単位**: 1 ~ 20 か月単位でスキャンの実行をスケジュールします。
		  • **Day of Month**: 月の特定の曜日で選択した時間にスキャンが繰り返されます。
		  • **Week of Month**: スキャンを開始する週にスキャンが毎月繰り返されます。たとえば、開始日を 10 月 3 日と選択し、それが月の第 1 週に当たる場合、スキャンは翌月以降、毎月第 1 週の選択した時刻に繰り返します。

設定	Default (デフォルト)	説明
		注意: 毎月、同じ日時でスキャンするようスケジュールする場合、Tenable では、開始日を 28 日以前に設定することを推奨します。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 Vulnerability Management は、それらの日にはスキャンを実行できません。 • **毎年**: 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。
開始	不定	スキャンを開始する正確な日時を指定します。 **注意:** 過剰な数のスキャンを同時に実行されるようにスケジュールした場合、Tenable Web App Scanning のスキャン能力が枯渇する場合があります。必要な場合は、一貫したスキャンのパフォーマンスを確保するために、Tenable Web App Scanning が同時スキャンをシフトします。 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 1 時間刻みで、24 時間形式で表示されます。たとえば、2019 年 10 月 31 日の午後 9 時 12 分にスキャンを作成する場合、デフォルトの開始日時は *10/31/2019* および *22:00* になります。
タイムゾーン	不定	**[開始]** に設定した値のタイムゾーン

通知

スキャンの通知設定

設定	デフォルト値	説明
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通知される、0 個または複数のメールアドレスをコンマ、スペース、または改行で区切って指定します。

ユーザーアクセス許可

ユーザーにアクセス許可を設定して、他のユーザーにスキャンまたはユーザー定義スキャンテンプレートを共有します。ユーザーのアクセス許可の追加または編集についての詳細は、Set Scan Permissions を参照してください。

アクセス許可	説明
アクセスなし	(既定)このアクセス許可を設定されたユーザーは、スキャンに関与することはできません。
表示可	このアクセス許可を設定されたユーザーは、スキャンの結果を表示することができます。
Can Control	このアクセス許可を持つユーザーは、**[表示可]**で許可されているタスクに加えて、スキャンの起動および停止が可能です。スキャンの設定を表示または編集したり、スキャンを削除したりすることはできません。
設定可	このアクセス許可を持つユーザーは、**[制御可]**で許可されているタスクに加えて、スキャンの設定の表示と、スキャンの所有権以外のスキャンの設定の変更が可能です。スキャンを削除することも可能です。

データ共有

設定	デフォルト値	説明
スキャン結果	ダッシュボードに表示	スキャン結果を非公開にするか**[ダッシュボード]**ページと**[検出結果]**ページに表示するかを指定します。**[プライベート表示]**に設定されている場合、スキャン結果の**[最終確認日]**の日付は更新されず、結果を表示するにはスキャンに直接アクセスする必要があります。

Tenable Web App Scanning スキャンの範囲設定

[範囲] を設定し、スキャンに含めるまた除外する URL およびファイルタイプを指定します。

スキャンまたはユーザー定義スキャンテンプレートを作成し、**[概要]** または **[スキャン]** テンプレートタイプを選択したときに、**[範囲]** の項目を設定できます。詳細は、スキャンテンプレート を参照してください。

ヒント: 設定を保存して他のスキャンに適用したい場合は、ユーザー定義スキャンテンプレートを作成して設定できます。

[範囲] 設定には、次のセクションが含まれます。

- クロールスクリプト
- OpenAPI (Swagger) 仕様
- スキャンの包含
- スキャンの除外

クロールスクリプト

複雑なアクセスロジックを使用するページをスキャナーが分析できるようにするためにスキャンに追加する必要がある Selenium スクリプト。

注意: スキャンに複数のターゲットを追加すると、これらの設定は無効になります。

設定	説明
ファイルの追加	1 つ以上の記録されている Selenium スクリプトファイルをスキャンに追加できるようにするハイパーリンク。 スクリプトは `.side` ファイルとして追加される必要があります。

OpenAPI (Swagger) 仕様

スキャンしたい RESTful API の仕様ファイルです。ファイルは OpenAPI 仕様 (v2 または v3) に準拠し、JSON または YAML 形式が使われています。

設定	説明

ファイルの追加	1 つまたは複数の OpenAPI (v2 または v3) 仕様ファイルを追加するためのハイパーリンクです。仕様ファイルには、JSON または YAML のいずれかの形式が使われています。

スキャンの包含

スキャナーで含める URL およびスキャナーでそれらの URL をクロールする方法。

注意: スキャンに複数のターゲットを追加すると、これらの設定は無効になります。

設定	Default (デフォルト)	説明
URL の一覧	なし	[基本] 設定で指定したターゲット URL 以外の、スキャンで確実に分析したい URL。 各 URL を絶対 URL として入力します。 各 URL を別々の行に入力します。 **注意:** すべての URL は同じドメインでなければならず、ワイルドカードは使用できません。
アプリケーションのクロール中に見つかった URL をスキャナーが処理する方法を指定します。	Crawl all URLs detected (検出されたすべての URL をクロール)	スキャナーが URL をクロールするときに従う制限を指定します。 次のいずれかを選択します。 • **Crawl all URLs detected** (検出されたすべての URL をクロール) - スキャナーはターゲット URL のドメインホスト上で検出したすべての URL と子パスをクロールします。 • **Limit crawling to specified URLs and child paths** (指定された URL と子パスにクロールを制限) - スキャナーはターゲット URL と子パスのみをクロールします。 • **Limit crawling to specified URLs** (指定さ

設定	Default (デフォルト)	説明
		れた URL にクロールを制限) - スキャナーはターゲット URL のみをクロールします。ターゲット URL の子パスはクロールしません。

スキャンの除外

スキャナーでスキャンから除外する URL の属性。

設定	デフォルト値	説明
Regex for Excluded URLs	logout	スキャナーが URL で検索できるスキャンから除外する正規表現パターンを指定できるテキストボックスオプション。改行することで、複数の正規表現を指定できます。 **注意:** 除外する正規表現値は、URL に含まれる値である必要があります。たとえば、`http://www.example.com/blog/today.htm` という URL では、有効な正規表現値は `blog` または `today` となります (URL 全体ではありません)。また、正規表現の値には大文字と小文字の区別があります。
File Extensions to Exclude	js、css、png、jpeg、gif、pdf、csv、svn-base、svg、jpg、ico、woff、woff2、exe、msi、zip	スキャナーでスキャンから除外するファイルタイプを指定できるテキストボックスオプション 各ファイルタイプはコンマで区切ります。 **注意**: 特定のファイル拡張子を除外すると役立つ場合があります。スキャナーはスキャン対象がウェブページではなくてもそれを認識せず、ウェブページであるかのようにスキャンを試みることがあるためです。これは時間の無駄になり、スキャン速度を低下させます。使用することがわかっており、スキャンする必要がないことが確実な場合は、追加のファイル拡張子を追加できます。たとえば、Tenable にはデフォルトで .png や .jpeg などのさまざまな画像拡張子が含まれています。
パスの分解	未選択	このチェックボックスオプションを使用して、スキャン中に識別された各 URL を、ディレクトリパスレベルを基にして追加の URL にブレー

設定	デフォルト値	説明
		クダウンするかどうかを指定できます。 たとえば、ターゲットとして *www.example.com/dir1/dir2/dir3* を指定し、**[パスの分解]** を選択した場合、スキャナーは、以下のそれぞれをターゲットの個別の URL として分析します。 • www.example.com/dir1/dir2/dir3 • www.example.com/dir1/dir2 • www.example.com/dir1 ウェブアプリケーションスキャンの対象範囲を拡大するには、このオプションを選択します。 **注意:** パスの分解を含むスキャンは、パスの分解のないスキャンよりも完了に時間がかかることがあります。
バイナリを除外	選択済み	スキャナーで応答の URL をバイナリ形式で監査するかどうかを指定できるチェックボックスオプション。 ウェブアプリケーションスキャンの対象範囲を拡大するには、このオプションを選択します。 **注意:** バイナリを含むスキャンは、スキャナーがバイナリ応答を読み取ることができないので、完了するまでに時間がかかる場合があります。

その他

設定	説明
類似したページを重複除外	類似ページが既に監査されているページをスキャナーに無視させるかどうかを指定できるチェックボックスオプション。

Tenable Web App Scanning スキャンの評価設定

[評価] 設定では、スキャナーが URL をクロールするときにどのウェブアプリケーション要素を監査するかを指定します。**評価** 設定は、スキャンやユーザー定義スキャンテンプレートを作成する際に設定できます。詳細は、スキャンテンプレート を参照してください。

評価 設定には、次のセクションが含まれます。

- スキャンタイプ
- 共通ページとバックアップページ
- 認証情報ブルートフォース攻撃
- 監査する要素
- オプション
- DOM 要素の除外

スキャンタイプ

これらの設定では、スキャナーで実行する評価の強度を指定します。

設定	デフォルト値	説明	必須
評価	推奨	以下のオプションから選択してスキャナーで実行するスキャンタイプを指定できるドロップダウンボックス。 • **推奨** - Tenable の推奨に基づくスキャナーの監査要素。 • **なし** - スキャナーはどの要素も監査しません。 • **高速** - スキャナーはリストに表示されている最も一般的な要素を監査します。 • **広範囲** - スキャナーはリストに表示されているすべての要素を監査します。 • **カスタム** - スキャナーは選択した要素だけを監査します。 **注意:** **[推奨]**、**[高速]**、または **[広範囲]** を選択してからこのセクション	○

設定	デフォルト値	説明	必須
		の設定を変更すると、**[スキャンタイプ]** 設定が自動的に**[カスタム]**に変更されます。	

共通ページとバックアップページ

設定	デフォルト値	説明
Detection Level (検出レベル)	最も検出されたページ	以下のオプションから選択してスキャナーでクロールするページを指定できるドロップダウンボックスです。 • **最も検出されたページ** - スキャナーは最も多く検出されたページのみをクロールします。 • **拡張辞書** - スキャナーは、非表示のページを検出するためにより多くのパスバリエーションをテストします。全体的なスキャン時間は長くなります。 **注意:** **[検出レベル]**ドロップダウンボックスは、**[スキャンタイプ]** 設定で**[カスタム]**を選択した場合にのみ使用できます。

認証情報ブルートフォース攻撃

[認証情報ブルートフォース攻撃] 設定は**[スキャン]**テンプレートでのみ使用できます。

設定	Default (デフォルト)	説明
認証情報ブルートフォース攻撃	無効	有効の場合、**[プラグイン]** 設定に含まれるブルートフォース攻撃を実行するプラグインが実行されます。 無効の場合、**[プラグイン]** 設定に含まれている場合でもブルートフォース攻撃プラグインは実行されません。

設定	Default (デフォルト)	説明
		注意: [認証情報ブルートフォース] の設定は、**[スキャンタイプ]** 設定で **[カスタム]** を選択した場合にのみ使用できます。

監査する要素

この設定では、スキャナーで脆弱性を分析するウェブアプリケーション内の要素を指定します。

設定	スキャナーのアクション
Cookies	Cookie ベースの脆弱性をチェックします。
ヘッダー	ヘッダーの脆弱性と安全ではない設定 (X-Frame-Options の消失など) をチェックします。
フォーム	フォームベースの脆弱性をチェックします。
リンクおよびクエリ文字列パラメーター	リンクおよびそれらのパラメーターの脆弱性をチェックします。
パラメーター名	パラメーター名の広範囲のファジングを実行します。
パラメーター値	パラメーター値の広範囲のファジングを実行します。
パスパラメーター	パスのパラメーターを評価します。パスパラメーターは、URL リライトにおいて、URL 内のアクションのオブジェクトを特定するために使用されます。たとえば、**scanId** は次の URL のパスパラメーターで、結果を表示するスキャンを特定するために使用されます。 `http://example.com/scan/scanId/results`
JSON 要素 / リクエスト本文	JSON リクエストデータを監査します。

設定	スキャナーのアクション
(JSON)	
XML 要素 / リクエスト本文 (XML)	XML リクエストデータを監査します。
UI フォーム	JavaScript コードに関連付けられている入力およびボタングループをチェックします。 **注意**: UI フォームでは、Tenable Web App Scanning はページとボタンで入力を受け取り、フォームのような要素 (UI フォーム) を作成します。Tenable Web App Scanning は各ボタンに、ページ上のすべての入力を含む `UIForm` 要素を作成します。
UI 入力	関連付けられたドキュメントオブジェクトモデル (DOM) イベントに対して孤立している入力要素をチェックします。 **注意**: UI 入力は、イベントに応答する入力がある場合です。たとえば、検索バーに入力した後、検索バーは「onEnter」イベントに応答して次のページを読み込みます。そのため、Tenable Web App Scanning はこのベクトルも監査するために `UIInput` 要素を作成します。

オプション

設定	Default (デフォルト)	説明
リモートファイルインクルード用の URL	None (なし)	Tenable Web App Scanning がリモートファイルインクルージョン (RFI) の脆弱性をテストするために使用できるリモートホスト上のファイルを指定します。 スキャナーがインターネットに到達できない場合は、スキャナーはこの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 テストを実行します。 **注意:** ファイルを指定しない場合、Tenable Web App Scanning は安全な Tenable でホストされたファイルを使用して RFI テストを実行します。

DOM 要素の除外

DOM 要素の除外は、スキャンが特定のページ要素やその子を対象にして動作しないようにします。この設定は、スキャン、概要、および PCI スキャンテンプレートで使用できます。

注意: スキャナーが属性値に基づいて要素を除外するかどうかを決定する際に、等価性チェックが実行されます。したがって、css `class foo` のある要素を除外する場合、スキャナーは `class="foo"` の要素を除外しますが、`class="foo bar"` の要素は除外しません。

⊕ ボタンをクリックして、**[テキストコンテンツ]** または **[CSS 属性]** を選択すると、除外項目を追加できます。

設定	Default (デフォルト)	説明
Text Contents	なし	テキストの内容に基づいて要素を除外します。 たとえば、スキャナーが Log Out という名前のログアウトボタンをクリックすることを防ぎたい場合は、`Log Out` というテキストをマッチさせます。
CSS Attribute	なし	CSS 属性のキーと値のペアに基づいて、要素を除外します。 たとえば、CSS 属性のキーと値のペア `id="logout"` を含むフォームとスキャナーが連動しないようにするには、キーに `id`、値に `logout` と入力します。

Tenable Web App Scanning スキャンのレポート設定

レポート設定では、スキャンレポートに含める追加の項目を指定します。たとえば Tenable PCI ASV スキャンに関するスキャンレポートでは、該当する場合、ロードバランサーの使用の詳細が必要です。

Tenable が提供するスキャンテンプレート **[PCI]** を使用してスキャンまたはユーザー定義スキャンテンプレートを作成するときに、**レポート**設定を行えます。詳細は、スキャンテンプレート を参照してください。

レポート設定には、次のセクションが含まれます。

- (Tenable PCI ASV 6.1) ロードバランサーの使用

(Tenable PCI ASV 6.1) ロードバランサーの使用

この設定では、スキャンレポートに含めるロードバランサーの使用状況を指定します。

設定	デフォルト値	説明	必須
(Tenable PCI ASV 6.1) ロードバランサーの使用	なし	テキストボックスを使用して、Tenable PCI ASV に必要なロードバランサーとそれらの設定のリストを入力できます (該当する場合)。	×

Tenable Web App Scanning スキャンの詳細設定

詳細設定では、ウェブアプリケーションスキャンで実装する必要がある追加のコントロールを指定します。

詳細設定は、Tenable 提供のスキャンテンプレートを使用してスキャンまたはユーザー定義スキャンテンプレートを作成するときに設定できます。ただし、**[概要]**と**[スキャン]**テンプレートタイプでは、**[設定監査]**や**[SSL TLS]**テンプレートタイプよりも多くの**詳細**設定が可能です。詳細は、スキャンテンプレート を参照してください。

[詳細設定]オプションを使用して、スキャンの効率とパフォーマンスを制御することができます 。

- 一般
- HTTP 設定
- 画面設定
- 制限
- Selenium の設定
- パフォーマンス設定
- セッションの設定

一般

[一般]オプションは、**[概要]**および**[スキャン]**テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明
Target Scan Max Time (HH:MM:SS)(対象資産スキャン最大時間 (HH:MM:SS))	08:00:00	スキャンジョブが停止するまでの実行最長時間を指定します。時間、分、秒で表示されます。 **注意:** 設定できる最大期間は 99:59:59 (時間:分:秒) です。
最大キュー時間 (HH:MM:SS)	08:00:00	スキャンが Queued 状態を続ける最大期間を指定します。時間、分、秒で表示されます。

		注意: 設定できる最大期間は 48:00:00 (時間:分:秒) です。
このスキャンのデバッグログを有効にする	無効	プラグインから利用可能なデバッグログを、スキャナーがこのスキャンの脆弱性出力に添付するかどうかを指定します。
Debug Flags (デバッグフラグ)	無効	(**[このスキャンのデバッグログを有効にします]** を有効にしたときのみ表示) デバッグ用に、サポートから提供されるキーと値のペアを指定できます。

HTTP 設定

これらの設定では、スキャナーで識別するユーザーエージェント、およびスキャナーでウェブアプリケーションに対するリクエストに含める必要がある HTTP レスポンスヘッダーを指定します。

Tenable 提供のスキャンテンプレートをベースにしたスキャンおよびユーザー定義スキャンテンプレートで **[クロールの設定]** オプションを設定することができます。

設定	Default (デフォルト)	説明
Use a different User Agent to identify scanner (異なるユーザーエージェントを使用してスキャナを特定する)	無効	スキャナーで HTTP リクエストを送信するときに Chrome 以外のユーザーエージェントヘッダーを使用するかどうかを指定します。
User Agent (ユーザーエージェント)	Chrome's user-agent (Chrome のユーザーエージェント)	スキャナーが HTTP リクエストを送信するときに使用するユーザーエージェントヘッダーの名前を指定します。 このオプションは、**[異なるユーザーエージェントを使用してスキャナーを特定する]** チェックボックスを選択した後にのみ設定できます。 デフォルトでは、Tenable Web App Scanning は、使用中の

		マシンのオペレーティングシステムとプラットフォームに対応するオペレーティングシステムとプラットフォーム用の Chrome が使用するユーザーエージェントを使用します。Chrome のユーザーエージェントの詳細については、*Google Chrome* のドキュメントを参照してください。 **注意:** 現在の Tenable Web App Scanning ユーザーエージェントヘッダーは次のとおりです。 `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36` **注意:** スキャナーからのすべてのリクエストが、ユーザーエージェントによって送信されるわけではありません。
スキャン ID HTTP ヘッダーの追加	無効	スキャナーがターゲットに送信するすべての HTTP リクエストにもう 1 つ `X-Tenable-Was-Scan-Id` ヘッダー (スキャン ID で設定されている) を追加するかどうかを指定します。これにより、ウェブサーバーのログでスキャンジョブを特定し、スキャン設定を変更してサイトを保護することができます。
Custom Headers (カスタムヘッダー)	なし	リクエストおよびレスポンスの形式の各 HTTP リクエストに挿入するカスタムヘッダーを指定します。 ⊕ ボタンをクリックし、各追加のヘッダーの値を入力することで、カスタムヘッダーを追加することができます。 **注意:** ユーザーエージェントのカスタムヘッダーを入力した場合、その値は **[ユーザーエージェント]** 設定ボックスに入力された値をオーバーライドします。

画面設定

[画面設定] オプションは、**[概要]** および **[スキャン]** テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明

Screen Width (画面の幅)	1600	スキャナーに埋め込まれたブラウザの画面の幅 (ピクセル単位) を指定します。
Screen Height (画面の高さ)	1200	スキャナーに埋め込まれたブラウザの画面の高さ (ピクセル単位) を指定します。
Ignore Images (画像を無視する)	無効	埋め込まれたブラウザがターゲットのウェブページ上の画像をクロールするか無視するかを指定します。

制限

[制限] オプションは、**[概要]** および **[スキャン]** テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明
Number of URLS to Crawl and Browse (クロールおよびブラウズする URL の数)	10000	スキャナーでクロールを試行する URL の最大数を指定します。
Path Directory Depth (パスディレクトリの深さ)	10	スキャナーでクロールするサブディレクトリの最大数を指定します。 たとえば、ターゲットが `www.example.com` で、スキャナーで `www.example.com/users/myname` をクロールしたい場合、テキストボックスに「2」と入力します。
Path Directory Depth (ページ DOM 要素の深さ)	5	スキャナーでクロールする HTML にネストされた要素のレベルの最大数を指定します。
Max Response Size (最大レスポンスサイズ)	500000	スキャナーで分析するページの最大読み込みサイズ (バイト単位) を指定します。 スキャナーで URL をクロールし、応答がこの上限を超えた場合、スキャナーはそのページの脆弱

		性を分析しません。
リダイレクト制限のリクエスト	3	スキャナーでページのクロールの試行を停止するまでに、スキャナーが従うリダイレクトの数を指定します。

Selenium の設定

この設定では、記録されている Selenium 認証情報を使用してウェブアプリケーションに対する認証を試行するときのスキャナーの動作を指定します。

これらのオプションは、Selenium 認証情報を使用してウェブアプリケーションに認証されるようにスキャンを設定している場合に設定します。詳細は、Tenable Web App Scanning スキャンの認証情報 を参照してください。

[Selenium の設定] オプションは、**[概要]** および **[スキャン]** テンプレートをベースにしたスキャンとユーザー定義スキャンテンプレートでのみ設定できます。

設定	Default (デフォルト)	説明
Page Rendering Delay (ページレンダリング遅延)	30000	スキャナーがページの表示を待機する時間 (ミリ秒単位) を指定します。
Command Execution Delay (コマンド実行遅延)	500	スキャナーがコマンドを処理してから次のコマンドを実行する前に待機する時間 (ミリ秒単位) を指定します。
Script Completion Delay (スクリプト完了遅延)	5000	スキャナーがすべてのコマンドが新しいコンテンツを表示して処理を終了するのを待機する時間 (ミリ秒単位) を指定します。

パフォーマンス設定

設定	Default (デフォルト)	説明
Max Number of Concurrent HTTP	10	単一ホストに許可される確立された HTTP

Connections (同時 HTTP 接続の最大数)		セッションの最大数を指定します。
Max Number of HTTP Requests Per Second (1 秒当たりの最大 HTTP リクエスト数)	25	スキャンの期間中に単一ホストに許可される HTTP リクエストの最大数を指定します。
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)	無効	ネットワークの混雑が発生した場合にスキャナーでスキャンを調整するかどうかを指定します。
Network Timeout (In Seconds) (ネットワークタイムアウト (秒))	5	スキャナーがスキャンを中止する前にホストからの応答を待機する時間 (秒単位) を指定します。プラグイン内で特に指定されていない場合に有効になります。 インターネット接続の速度が遅い場合、Tenable は長い待機時間を指定することを推奨します。
Browser Timeout (In Seconds) (ブラウザータイムアウト (秒))	30	スキャナーがスキャンを中止する前にブラウザからの応答を待機する時間 (秒単位) を指定します。プラグイン内で特に指定されていない場合に有効になります。 インターネット接続の速度が遅い場合、Tenable では長い待機時間を指定することを推奨します。
Timeout Threshold (タイムアウトしきい値)	100	スキャナーがスキャンを中止するまでに許可される連続タイムアウト数を指定します。

セッションの設定

これらのトークンを指定すると、スキャナーでトークン検証をスキップできるようになり、スキャンにかかる時間が短縮されます。セッション設定は、既存のスキャンを編集している場合にのみ使用できます。

トークンタイプ	デフォルト	説明
クッキー	なし	スキャナーが使用するアプリケーションの認証クッキーの名前。
ヘッダー	なし	スキャナーが使用するアプリケーションの認証ヘッダーの名前。

Tenable Web App Scanning スキャンの認証情報

注意: このセクションのトピックでは、新しいインターフェースでの認証情報についてのみ説明します。新しいインターフェースをアクティブにした場合、従来のインターフェースで設定した過去の認証情報のスナップショットを表示できますが、それらの認証情報を変更することはできません。

注意: 認証情報の設定は、単一ターゲットのスキャンに対してのみ設定できます。複数のターゲットでスキャンを作成する場合、これらの設定は使用できません。

Tenable Web App Scanning スキャンでは、Tenable Web App Scanning でウェブアプリケーションの認証スキャンを実行できるように認証情報を設定することができます。認証されたスキャンを設定することで、認証されていないスキャンよりも広範なチェックを実行できるようになり、スキャン結果がより正確になります。

Tenable Web App Scanning のスキャンは管理された認証情報を使用します。管理された認証情報によって、認証情報の設定を認証マネージャーで一元的に保存できます。その後、これらの認証情報設定を、スキャンごとに認証情報を設定する代わりに、複数のスキャン設定に追加できます。

Tenable Web App Scanning スキャンでは、次の認証タイプの認証情報がサポートされています。

- HTTP サーバー認証
- ウェブアプリケーション認証

ヒント: API スキャンテンプレートを使用して API をスキャンするときに、API 認証にキーまたはトークンが必要な場合は、**[HTTP設定]** セクションの [詳細] 設定で、必要になるカスタムヘッダーを追加することができます。

次の方法を使用して Tenable Web App Scanning スキャンで認証情報を設定することができます。

認証情報のカテゴリ	認証タイプ	設定方法
HTTP サーバー認証	-	Tenable Web App Scanning のユーザーインターフェースを使用して、スキャンの認証情報を手動で設定します。
ウェブアプリケーション認証	ログインフォーム	
	Cookie 認証	

	Selenium 認証	次のいずれかを行います。 ◦ Chrome の Selenium IDE (Integrated Development Environment) 拡張機能を使用して、認証情報を記録し、Tenable Web App Scanning ユーザーインターフェースを使用して認証情報をスキャンに手動で追加します。 **注意:** Chrome の Selenium IDE 拡張機能の詳細については、Google Chrome のドキュメントを参照してください。 ◦ Tenable Web App Scanning Chrome 拡張機能 を使用して認証情報を記録し、スキャン設定に認証情報を自動的に追加します。 **ヒント:** Tenable Web App Scanning で使用する Selenium スクリプトの詳細については、Tenable Web App Scanning の Selenium コマンドを参照してください。
	API キー ベアラー認証	Tenable Web App Scanning のユーザーインターフェースを使用して、スキャンの認証情報を手動で設定します。

Selenium 認証情報の設定を自動的に設定する

必要な追加ライセンス: Tenable Web App Scanning

Tenable Web App Scanning Chrome 拡張機能 を使用して、Selenium 認証情報を記録し、それらの認証情報を新しいスキャンまたは既存のスキャンに自動的に追加することができます。

注意: Tenable Web App Scanning Chrome 拡張機能 は、ウェブアプリケーションスキャンの Selenium 認証情報の設定のみを更新します。その他のスキャンオプションは、Tenable Web App Scanning Chrome 拡張機能 インターフェースを使用して設定する必要があります。

始める前に

- Chrome ウェブストアから Tenable Web App Scanning Chrome 拡張機能 をダウンロードします。
- Tenable Vulnerability Management にログインするの説明に従って、Tenable Vulnerability Management にログインします。

Tenable Web App Scanning Chrome 拡張機能 を使用して Selenium 認証情報を記録する方法

1. ブラウザの右上の Tenable Vulnerability Management ロゴをクリックします。

   Tenable Web App Scanning Chrome 拡張機能の **[スキャンを作成する]** ウィンドウが表示されます。

2. 次のいずれかを行います。

タスク	アクション
Selenium 認証情報を既存のスキャンに記録および追加する	• **[既存のスキャンに追加する]** をクリックします。 **[既存のスキャンに追加する]** ウィンドウが表示され、既存のスキャンのリストが表示されます。 • 検索ボックスに、Selenium 認証情報を追加するスキャンの名前を入力します。 • 🔎ボタンをクリックします。

	Tenable Web App Scanning Chrome 拡張機能 によって、入力した名前でリストがフィルタリングされます。 • Selenium 認証情報を追加するスキャンをクリックします。
Selenium 認証情報を新しいスキャンに記録および追加する	• **[新規のスキャンを作成する]** をクリックします。 **[新規スキャン]** ウィンドウが表示されます。 • **[名前]** ボックスにスキャンの名前を入力します。 • **[URL]** ボックスに、スキャンするウェブアプリケーションのターゲットを URL 形式で入力します。

3. **[次へ]** をクリックします。

   スキャンターゲットとして指定したリンクが拡張機能によって開かれます。

4. **[記録]** をクリックします。

   Tenable Web App Scanning Chrome 拡張機能 によってセッションの記録が開始されます。

   記録が開始されたことを示すメッセージが表示されます。

5. ウェブアプリケーションを認証するために使用するログイン手順を実行します。

6. システムに正常に認証した後で、正常に認証されたときにのみ表示されるウェブページ上のテキスト (たとえば [**Welcome,** [ユーザー名]**!**]) をハイライトします。

7. 右下の **[完了]** をクリックします。

8. (オプション) 記録したログイン手順を再生するには、**[再生]** をクリックします。

9. 認証ログイン手順を正常に記録した後で、**[保存]** をクリックします。

   Tenable Web App Scanning Chrome 拡張機能 が認証を保存してスキャンにインポートします。

次の手順

- Tenable Web App Scanning Chrome 拡張機能 を使用して新しいスキャンを作成した場合は、Tenable Web App Scanning Chrome 拡張機能 インターフェースで他のオプションを設定する必要があります。

Tenable Web App Scanning の Selenium コマンド

Tenable Web App Scanning の Selenium コマンドは、認証およびクロールのスクリプトを記録するために使用されます。これにより、ユーザーは特定のシナリオで何を実行するかをスキャナーに正確に指示できるようになります。これらのコマンドは、Selenium IDE 拡張機能と Tenable Web App Scanning Chrome 拡張機能 の両方で実行できます。どちらも Chrome ウェブストアでダウンロードできます。

Tenable Web App Scanning の Selenium コマンドのサポートについては、以下に詳述します。

サポートされているコマンド	サポートされていないコマンド
• addSelection • answerOnNextPrompt • assert • assertAlert • assertChecked • assertConfirmation • assertEditable • assertElementNotPresent • assertElementPresent • assertNotChecked • assertNotEditable • assertNotSelectedValue • assertNotText • assertPrompt • assertSelectedLabel • assertSelectedValue • assertText • assertTitle	• close • debugger • do • else • else if • end • execute async script • execute script • for each • if • repeat if • run • select window • store • store attribute • store json • store text • store title

- assertValue
- check
- chooseCancelOnNextConfirmation
- chooseCancelOnNextPrompt
- chooseOkOnNextConfirmation
- click
- clickAt
- doubleClick
- doubleClickAt
- echo
- editContent
- mouseDown
- mouseDownAt
- mouseMoveAt
- mouseOut
- mouseOver
- mouseUp
- mouseUpAt
- open
- pause
- removeSelection
- runScript
- select
- selectFrame

- store value
- store window handle
- store xpath count
- times
- while

- sendKeys

  > **注意：** sendKeys コマンドは、任意のテキストに加えて以下のエスケープシーケンスのみをサポートします。
  >
  > - `${KEY_ENTER}`
  > - `${KEY_DELETE}`
  > - `${KEY_BACKSPACE}`

- setSpeed
- setWindowSize
- submit
- type
- uncheck
- verify
- verifyChecked
- verifyEditable
- verifyElementNotPresent
- verifyElementPresent
- verifyNotChecked
- verifyNotEditable
- verifyNotSelectedValue
- verifyNotText
- verifySelectedLabel
- verifySelectedValue
- verifyText
- verifyTitle

• verifyValue • waitForElementEditable • waitForElementNotEditable • waitForElementNotPresent • waitForElementNotVisible • waitForElementPresent • waitForElementVisible • webdriverAnswerOnNextPrompt • webdriverAnswerOnVisiblePrompt • webdriverChooseCancelOnNextConfirmation • webdriverChooseCancelOnNextPrompt • webdriverChooseCancelOnVisibleConfirmation • webdriverChooseCancelOnVisiblePrompt • webdriverChooseOkOnNextConfirmation • webdriverChooseOkOnVisibleConfirmation	

Tenable Web App Scanning スキャンでの HTTP サーバー認証設定

Tenable Web App Scanning スキャンでは、HTTP サーバーベースの認証の認証情報に関する次の項目を設定できます。

オプション	アクション
ユーザー名	Tenable Web App Scanning で HTTP ベースのサーバーを認証するために使用するユーザー名を入力します。
パスワード	Tenable Web App Scanning で HTTP ベースのサーバーを認証するために使用するパスワードを入力します。
認証タイプ	ドロップダウンリストで、次の認証タイプのいずれかを選択します。 • **Basic/Digest** • **NTLM** • **Kerberos**
Kerberos ドメイン	(Kerberos 認証タイプを有効にする場合に必要) Kerberos ターゲット認証が属する領域 (該当する場合)。
キー配布センター (KDC)	(Kerberos 認証タイプを有効にする場合に必要) このホストが、ユーザーのセッションチケットを提供します。

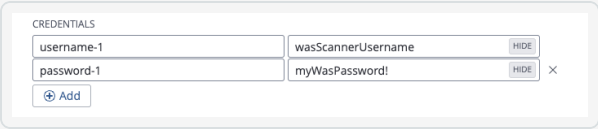
注意: Tenable Web App Scanning は、単一のターゲットに対する複数の HTTP 認証タイプをサポートしていません。

ウェブアプリケーション認証

Tenable Web App Scanning スキャンで、次のいずれかのタイプの**ウェブアプリケーション認証**の認証情報を設定できます。

- ログインフォーム認証
- Cookie 認証
- Selenium 認証
- API キー認証
- ベアラー認証

ログインフォーム認証

オプション	アクション
Authentication Method (認証方法)	ドロップダウンボックスで、**[ログインフォーム]** を選択します。
ログインページ	スキャンするウェブアプリケーションのログインページの URL を入力します。
認証情報	ターゲットのログインフォームの各フィールド (ユーザー名、パスワード、ドメインなど) について、次のように認証情報エントリに入力します。 a. 左側のテキストボックスに、ログインフィールドの名前または ID HTML DOM 属性の値を入力します。 b. 行の右側のテキストボックスに、ログイン時にそのテキストフィールドに挿入するリテラル値を入力します。 典型的な設定の例 

	ヒント: テキストフィールドの名前または ID HTML DOM 属性を表示するには、テキストフィールドを右クリックし、Firefox または Chrome ブラウザで [検査] を選択します。 **ヒント:** 認証情報なしの **[概要]** スキャンを実行する場合、プラグイン 98033 (**[ログインフォームが検出されました]**) が、必要なログインボックスを自動的に検出してプラグインの出力にそれを表示することがあります。
正常な認証を検証するためのパターン	認証が成功した場合にのみウェブサイトに表示される単語、語句、または正規表現を入力します (たとえば、**ようこそ**、*[ユーザー名]* さん!)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。
アクティブなセッションを確認するためのページ	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します (たとえば、**こんにちは**、*[ユーザー名]* さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

Cookie 認証

オプション	アクション
Authentication Method (認証方法)	ドロップダウンボックスで、**[Cookie 認証]** を選択します。
セッション Cookie	次を実行します。 a. 最初のテキストボックスで、Cookie 認証の認証情報の名前を入力します。 b. 2 番目のテキストボックスに、Cookie 認証の認証情報の値を入力します。
アクティブなセッションを確認するため	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。

のページ	
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します(たとえば、**こんにちは**、*[ユーザー名]*さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に **.*** は必要ありません。

Selenium 認証

オプション	アクション
Authentication Method(認証方法)	**[Selenium 認証]**を選択します。
Selenium Script (.side)	次を実行します。 a. Selenium IDE 拡張機能で、認証の認証情報を Selenium IDE 拡張機能に記録します。 b. **[ファイルの追加]**をクリックします。 お使いのオペレーティングシステムのファイルマネージャーが表示されます。 c. Selenium 認証情報 `.side` ファイルに移動して選択します。 Tenable Web App Scanning によって認証情報ファイルがインポートされます。
アクティブなセッションを確認するためのページ	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します(たとえば、**こんにちは**、*[ユーザー名]*さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に **.*** は必要ありません。

API キー認証

オプション	アクション
認証方法	**API キー**を選択します。
ヘッダー	次を実行します。 a. 最初のテキストボックスに、HTTP ヘッダーの名前を入力します。 b. 2 番目のテキストボックスに、HTTP ヘッダーの値を入力します。 c. (オプション) ⊕ ボタンをクリックしてヘッダーを追加します。
アクティブなセッションを確認するためのページ	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します (たとえば、**こんにちは**、*[ユーザー名]* さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

ベアラー認証

オプション	アクション
認証方法	**[ベアラー認証]** を選択します。
ベアラートークン	ベアラートークンの値を入力します。 **注意**: ベアラートークンは OAuth の一部です。Tenable Web App Scanning が OAuth をサポートするのは、OAuth が OpenIDConnect に含まれ、selenium スクリプトを介して記録可能な場合です。OpenIDConnect に含まれない OAuth の実装は、トークンが動的であるか、または認証目的で特別な静的 (非動的) トークンを作成した場合にのみサポートされます。
アクティブなセッションを確認するため	Tenable Web App Scanning が認証されたセッションを検証するために継続的にアクセスできる URL を入力します。

のページ	
アクティブなセッションを確認するためのパターン	セッションが引き続きアクティブな場合のみウェブサイトに表示される単語、語句、または正規表現を入力します (たとえば、**こんにちは**、*[ユーザー名]* さんなど)。なお、先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

クライアント証明書認証

Tenable Web App Scanning スキャンで、**クライアント証明書認証**の認証情報を設定できるようになりました。

オプション	アクション
クライアント証明書	ホストとの通信に使用される PEM 形式の証明書を含むファイル。
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 形式のプライベートキーを含むファイル。
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)。
正常な認証を検証するためのページ	Tenable Web App Scanning が認証されたセッションを検証するためにアクセスできる URL を入力します。
正常な認証を検証するためのパターン	認証が成功した場合にのみウェブサイトに表示される単語、語句、または正規表現を入力します(たとえば、ようこそ、[ユーザー名]さん!)。先頭のスラッシュはエスケープされ、パターンの最初と最後に .* は必要ありません。

Tenable Web App Scanning スキャンのプラグイン設定

必要な Tenable Web App Scanning ユーザーロール: スキャンマネージャーまたは管理者

[プラグイン] を設定して、スキャナーでウェブアプリケーションをスキャンするときに使用するプラグインおよびプラグインファミリーを指定します。

スキャンが作成され起動されると、Tenable Web App Scanning はさまざまなプラグインファミリーのプラグインを使用します。それぞれが特定のタイプの検出結果または脆弱性を特定して、ウェブアプリケーションを分析するように設計されています。Tenable Web App Scanning では、98000 ~ 98999 と 112290 ~ 117290 のプラグイン ID 範囲をスキャンに使用します。Tenable Web App Scanning プラグインファミリーの詳細については、Tenable Web App ScanningTenable Web App Scanning プラグインファミリーサイトを参照してください。

注意：Tenable Web App Scanning には、スキャンごとに各プラグインの最初に検出された 25 のインスタンスのみがスキャン結果に表示されます。スキャン結果に 1 つのプラグインの 25 のインスタンスが表示された場合は、修正ステップを実行して対応する脆弱性を解決してから、ターゲットを再スキャンすることをお勧めします。

スキャンまたはユーザー定義スキャンテンプレートを作成し、**[API]**、**[概要]**、**[(基本) スキャン]**、**[標準スキャン]**、**[カスタム]** のテンプレートまたはスキャンタイプを選択するときに、**[プラグイン]** の項目を設定できます。詳細については、スキャンプラグインの表示を参照してください。

ヒント: 設定を保存して他のスキャンに適用したい場合は、ユーザー定義スキャンテンプレートを作成して設定できます。

プラグインの設定には次のセクションがあります。

- すべて有効
- プラグインの表

すべて有効

クリックしてすべてのプラグインの有効または無効を同時に切り替えます。

プラグインの表

列	説明	アクション
名前	グループ化されたプラグインが属するプラグインファミリーを指定します。	• 各プラグインファミリーの名前を表示します。 • 列を選択して、表をアルファベット順またはファミリー名ごとにソートします。
合計	プラグインファミリーのプラグインの数を指定します。	• ファミリー内のプラグインの数を表示します。 • 列を選択して、各ファミリーのプラグインの数で表をソートします。
ステータス	ターゲット分析するためにプラグインファミリーのプラグインをスキャナーで使用するかどうかを指定するトグルです。	• **[ステータス]**トグルをクリックし、プラグインファミリーのプラグインを無効にします。 • (オプション) 無効になったプラグインファミリーを有効にするには、**[ステータス]**トグルをクリックします。

プラグインの表で、個別のプラグインの詳細を表示したり無効にしたりすることができます。

個別のプラグインに関する詳細を表示する方法

1. 表で、表示するプラグインが含まれているファミリーの行をクリックします。

   プラグインファミリーの詳細ペインが表示され、ファミリー内の各プラグインの名前、ID、およびステータスがページ分割されたリストが表示されます。

2. (オプション) 特定のプラグインを見つけるには、**[検索]**ボックスに名前または ID を入力します。
3. 詳細を表示するプラグインをクリックします。

個別のプラグインを無効にする方法

1. 表で、無効にするプラグインが含まれているファミリーの行をクリックします。

   プラグインファミリーの詳細ペインが表示され、ファミリー内の各プラグインの名前、ID、およびステータスがページ分割されたリストが表示されます。

2. (オプション) 特定のプラグインを見つけるには、**[検索]** ボックスに名前または ID を入力します。

3. **[ステータス]** 列で、無効にするプラグインの横にあるチェックボックスを選択します。

4. (オプション) 無効になったプラグインを有効にするには、このチェックボックスを選択します。

5. **[保存]** をクリックします。

   詳細プレーンが消去されます。

   Tenable Web App Scanning によってプラグインの選択が更新されます。

スキャンの分散

概要

スキャン分散機能により、企業のスキャナーだけでなく、Tenable Vulnerability Management が提供するクラウドスキャナーのスキャン効率がプラットフォーム全体で向上します。企業に属するスキャナーの場合、Tenable Vulnerability Management は個別のスキャナーに完全なスキャンジョブを割り当てるのではなく、スキャンに割り当てられたスキャナーグループ内の複数のスキャナーに対して、スキャンをタスクとして分散します。同様に、Tenable Vulnerability Management は Tenable が提供するクラウドスキャナーを使用して、スキャナーグループの間にまたがるジョブとしてスキャンを分散します。Tenable Vulnerability Management はジョブをタスクに分割し、グループ内のスキャナーに送ります。

いずれの場合も、複数のスキャンを同時に効果的に実行でき、個別のスキャナーでスキャンを 1 回ずつ行う場合のボトルネックを解消できます。企業による需要が拡大すればするほど、パフォーマンスは低下しがちです。スキャンが特定のスキャナーに割り当てられている場合でも、それらのスキャンは同時に実行できるタスクに分割されるため、スキャナーはスキャンジョブをより効率的に完了できます。

スキャナーがタスクを完了すると、Tenable Vulnerability Management はすぐに結果を反映します。スキャンをキャンセルしても、既に取得された結果は保持されます。スキャン中にスキャナーがクラッシュした場合や、ターゲットで問題が発生した場合も、他のタスクは通常どおり実行されます。

各スキャンタスクは、120 の IP アドレスをスキャンします。スキャンジョブの最後のスキャンタスクでは、IP アドレスが 120 未満になる場合があります (たとえば、Tenable Vulnerability Management は 300 の IP アドレスのスキャンジョブを 2 つの 120 IP アドレスタスクと 1 つの 60 IP アドレスタスクに分割します)。

スキャン分散機能の仕組み

スキャンジョブが作成されると、ジョブは時スキャナーのジョブキューのディレクトリ (スキャンでスキャナーが指定されている場合) またはスキャナーグループのジョブキューに入れられます。

スキャン操作

スキャン分散機能によるスキャンのタスクへの分割は非同期的に行われるため、スキャンを操作できる方法には若干の差異があります。

スキャナーグループ

スキャングループを作成すると、企業のスキャナーでスキャン分散機能を使用できます。スキャナーグループを使用すると、1台のスキャナーで全体のジョブを完了するのではなく、グループに割り当てた個別のスキャナー間にタスクを分配することによって、スキャン効率を最大化できます。

スキャン結果

スキャナーがタスクを完了すると、スキャン結果をリアルタイムで表示できます。タスクが完了するたびに、Tenable Vulnerability Management はスキャン結果を新規データで更新します。スキャンが失敗または中断された場合、プロセスが完了しなかったことがスキャンに反映されますが、既に完了した結果は Tenable Vulnerability Management により保持されます。

ジョブが複数のスキャナーに割り当てられており、それらのスキャナーの1つが失敗した場合、他のスキャナーにディスパッチされたタスクは引き続き実行されます。

スキャナー容量

Tenable Vulnerability Management は、スキャナーが処理できるタスクの数を効率的に判断するために、スキャンを分散するときに次の 3 種類のスキャナー容量を考慮します。

- ターゲット容量: スキャナーが同時にスキャンできる資産数この値のデフォルトは、プロセッサ数や利用可能なメモリ量などのスキャナーのハードウェアリソースに基づきます。
- タスク容量: スキャナーが同時に実行できるタスク(スキャンの一部)の数スキャナーのタスク容量は、ターゲット容量に基づいて決まります。
- ジョブ容量: スキャナーが一度にタスクを含めることができる異なるジョブの数これにより、スキャンを非同期的に行うことができ、空き容量のあるスキャナーが異なるスキャンから派生したタスクでも複数のタスクを完了できるようになります。スキャナーのジョブ容量がフルの場合でも、すべてのジョブのタスクを完了できるよう、ジョブ容量は常にタスク容量を下回るようになっています。

スキャナーグループ容量

Tenable Vulnerability Management では、スキャンの分散時にスキャナーグループのジョブ容量も考慮します。利用可能な容量がある場合、スキャナーグループレベルのジョブはタスクに分割されます。これらのジョブからのタスクは、グループ内のスキャナー間に分配されます。

ジョブキュー

Tenable Vulnerability Management は、スキャンを分散するためにスキャンジョブをタスクに分割する前に、それらをキューに入れます。

スキャナーグループのジョブキュー

Tenable Vulnerability Management はジョブを受け取った順に、ジョブをスキャナーグループのキューに入れます。スキャナーグループにジョブの空き容量がある場合、Tenable Vulnerability Management はキューの 1 つ目のジョブをタスクに分割し、グループ内の各スキャナーに順に割り当てます。(ラウンドロビン方式。)Tenable Vulnerability Management は、ジョブに割り当てられたスキャナーにタスクをディスパッチします。

スキャナージョブキュー

Tenable Vulnerability Management はスキャンジョブの出所に関係なく、ジョブを受け取った順に、ジョブを 1 つのスキャナーのキューにも入れます。

たとえば、スキャナーのジョブキューには、スキャナーに直接割り当てられたスキャンジョブやスキャナーが属するグループ単位でスキャナーに配信されるスキャンジョブが含まれる場合があります。

ディスパッチタスク

スキャナーにタスクに対応できる能力がある場合、スキャナーのジョブ能力を消費したジョブからの追加タスクのポーリングが行われ、それらのタスクがスキャナーに割り当てられます。ジョブがグループ内のスキャナーに割り当てられる方法と同じように、ラウンドロビン方式で順次、各ジョブからタスクが割り当てられます。これはテストとなります。

タスクがスキャナーにディスパッチされる方法は、シナリオによって異なります。

シナリオの例：1つのジョブに1つのスキャナー

この例では、キューされたジョブが1つとスキャナーが1個あると仮定します。このスキャナーはスキャナーグループの一部ではなく、ジョブがキューされた順番で、1つずつスキャンジョブを処理します。このスキャナーのタスク能力は6件です。ジョブがタスクに分けられると、そのタスクのうちの6つがスキャナーに割り当てられ、同時に実行されるようにします。スキャンジョブが完了するまで、タスクはスキャナーのタスク能力を消費し続けます。

シナリオの例：複数ジョブを処理する1つのスキャナー

この例では、キューされた複数のジョブと1個のスキャナーがあると仮定します。スキャナーは2つのスキャナーグループ、SG1とSG2に属しています。3つのスキャンジョブが作成されました。最初のスキャンはスキャナーを直接使用するように設定されています。他の2つのスキャンはそれぞれSG1とSG2を使用するように設定されています。

最初のスキャンジョブは特定のスキャナーを使用するように設定されているため、スキャナーのジョブキューに追加されます。SG1とSG2では、このスキャナーは両方のグループで次にジョブを受領する順番になっています。それらのグループからのジョブもスキャナーのジョブキューに追加されます。

このスキャナーのジョブ能力は3件のため、スキャナーには3つすべてのジョブからのタスクを割り当てを受けることができます。

このスキャナーのタスク能力は5件です。タスクは、各ジョブから1つずつ連続してスキャナーに割り当てられます。この場合、タスクは次の順番で割り当てられます。ジョブ1、ジョブ2、ジョブ3、ジョブ1、ジョブ2と、タスク能力を満たしていきます。この「ラウンドロビン」方式を使用し、スキャナーは最初のジョブからの2つのタスクの作業を開始し、2番目のジョブの2つのタスク、3番目のジョブの1つのタスクと続けます。タスクの1つが完了すると、3番目のジョブから次のタスクがディスパッチされます。

シナリオの例：複数ジョブに複数のスキャナー

この例では、2 つのスキャナー (スキャナー 1 とスキャナー 2) があると仮定します。スキャナーは両方ともスキャナーグループ SG1 に割り当てられています。スキャナー 1 とスキャナー 2 のジョブ能力は、それぞれ 3 件です。

2 つのスキャンジョブが作成されました。ジョブ 1 はスキャナー 1 に直接割り当てられました。ジョブ 2 は SG1 に割り当てられました。ジョブは両方ともタスクに分解されます。ジョブ 1 はスキャナー 1 によってのみ処理されますジョブ 2 はスキャナー 1 とスキャナー 2 の両方で処理される可能性があります。

スキャナー 1 とスキャナー 2 のタスク能力は、それぞれ 6 件です。スキャナー 1 には、各ジョブから 1 つずつ連続してタスクが割り当てられます。(ジョブ 1 から 3 件、ジョブ 2 から 3 件。)スキャナー 2 には、ジョブ 2 から 6 件のタスクが割り当てられます。

各スキャナーがタスクに対応できるようになると、ジョブ 2 のタスクは SG1 からスキャナー 1 とスキャナー 2 にディスパッチされます。この処理は両方のジョブが完了するまで続きます。

スキャンのルーティングの設定

スキャンのルーティングを使用すると、各スキャナーグループがアクセス可能なネットワーク領域に従って、複数のスキャナーグループ間でスキャンを自動的に割り振ることができます。スキャンのルーティングにより、個別のスキャンそれぞれに対して特定のスキャナーを設定する必要がなくなり、スキャン設定および管理のオーバーヘッドが削減されます。この機能は、大規模デプロイメントで大きな利点をもたらします。運用効率を高めるために、高い権限を持つチームメンバーがスキャナープールを管理し、低い権限のチームメンバーがスキャンの設定時にそのスキャナープールを使用することができます。

注意: スキャンのルーティングは、リンクされたスキャナーでのみ利用可能です。

あるスキャンに対してスキャンのルーティングを設定した場合、そのスキャンの実行時に Tenable Vulnerability Management は自動的に次を実行します。

- 一致するターゲット範囲が最も狭く設定されたスキャナーグループにスキャンターゲットを割り当てます。
- そのスキャナーグループ内で、スキャナーの容量とまだ利用可能なターゲットに応じて、スキャナーが登録されると同時にスキャナーにターゲットを割り当てます。

詳細は、設定のガイドラインを参照してください。

注意: Tenable では、ネットワークの別個の領域を効果的にターゲットできるように、スキャンのルーティング戦略を事前に計画することを推奨しています。設定が不適切な場合、スキャンのルーティングによってスキャナーのターゲットへの到達が妨げられる可能性があります。

スキャンのルーティングを設定する方法

1. スキャンのルーティングに関する設定ガイドラインを確認します。
2. スキャンのルーティング用のスキャナーグループを設定します。
    a. スキャナーグループを作成または編集します。
    b. **[スキャンルーティングのターゲット]** ボックスで、スキャンのルーティングのターゲットをコンマ区切りのリスト形式で入力します。

    リスト内のターゲットは、対応する形式に従う必要があります。

> **注意:** 個別のスキャナーグループに対して、最大 10,000 の個別のスキャンのルーティングターゲットを指定できます。たとえば、`192.168.0.1, example.com, *.example.net, 192.168.0.0/24` では、4 つのスキャンのルーティングターゲットを指定しています。スキャンのルーティングのターゲットのリストを集約するために、Tenable では個別の IP アドレスの代わりに、ワイルドカードや範囲指定形式の使用を推奨しています。

c. **[保存]** をクリックします。

Tenable Vulnerability Management により、スキャナーグループへの変更が保存されます。

3. スキャンのルーティング用のスキャンを設定します。

a. スキャン設定を作成または編集します。

b. **[基本]** 設定セクションで、次のオプションを設定します。

オプション	アクション
スキャナー	**[自動選択]** オプションを選択します。 このオプションを選択すると、**[ネットワーク]** ボックスが表示されます。
Network	次のいずれかを行います。 • スキャンが重複する IP 範囲を持つ別々の環境に関係する場合、スキャンのルーティング用に設定したスキャナーグループを含むネットワークを選択します。 • スキャンが重複する IP 範囲を持つ別々の環境に関係しない場合は、**[デフォルト]** ネットワークのままにします。
Targets / Upload Targets / Tags	次のいずれかのオプションを使用して、スキャンのターゲットを指定します。 • **[ターゲット]** ボックスで、ターゲットの一覧を入力します。 • **[ターゲットのアップロード]** ボックスで、ターゲットのファイルをアップロードします。 • **[タグ]** ボックスで、ターゲットをタグで指定します。 スキャンターゲットを指定する際は、次に注意してください。

	• スキャンターゲットが、スキャナーグループで指定したスキャンのルーティングのターゲットと一致するようにしてください。 スキャンターゲットをスキャナーグループのターゲットの範囲外に指定した場合、Tenable Vulnerability Management はスキャナーグループの範囲内のホストのみをスキャンし、スキャンされなかったホストを警告する一覧とともに、不完全な結果を返します。 • スキャンのルーティングのターゲットとスキャンターゲットを照合する際、Tenable Vulnerability Management は FQDN を IP アドレスに解決*しません*。 たとえば、`*.example.com` をスキャンのルーティングのターゲットとして指定した場合、Tenable Vulnerability Management はスキャンターゲットが `www.example.com` として設定されているスキャンを、そのスキャナーグループに割り当てることができます。しかし、たとえ `www.example.com` が `192.168.0.1` に解決される可能性があったとしても、ターゲットが `192.168.0.1` として設定されているスキャンを、Tenable Vulnerability Management がそのスキャナーグループに割り当てることはありません。

c. **[保存]** をクリックします。

Tenable Vulnerability Management によりスキャン設定に対する変更が保存されます。

設定のガイドライン

- Tenable では、スキャンのルートを設定する場合に可能であれば、個別の IP アドレスではなく IP 範囲および CIDR 範囲を使用することを推奨しています。このアプローチは、より狭いターゲット値が推奨されるスキャンターゲットに対する推奨アプローチとは異なります。
- Tenable Vulnerability Management では、IPv6 アドレスの数値範囲形式はサポートされていません。代わりに、IPv6 アドレス範囲の CIDR 形式を使用してください。
- 通常、Tenable では個別のスキャナーを 1 つのスキャナーグループのみに追加することを推奨しています。しかし一部のケースでは、スキャン範囲や冗長性を確保するために、重複するスキャナーグループを設定したい場合もあります。2 つまたはそれ以上のスキャングループが企業のネットワークの同じ領域をターゲットとしている場合、それらは冗長なグループとなります。Tenable Vulnerability

Management が冗長なスキャナーグループを使用してスキャンを実行する場合、最も狭く、最も特定的なスキャナーグループを排他的に使用してスキャンを試みます。

たとえば、2 つのスキャナーグループが次に記載するスキャンのルーティングのターゲットを指定しているとします。

- スキャナーグループ #1 - `192.168.0.1-192.168.0.200`
- スキャナーグループ #2 - `192.168.0.10-192.168.0.20`

スキャンで指定されているスキャンターゲットが `192.168.0.15-192.168.0.19` の場合、Tenable Vulnerability Management はそのスキャンをスキャナーグループ #2 に割り当てます。なぜならそのグループのスキャンのルーティングのターゲット範囲は、スキャナーグループ #1 で指定されている範囲よりも狭いためです。

- スキャナーグループ内のスキャナーの利用可能性の定義については、スキャナーグループを参照してください。

サポートされるスキャンのルーティングのターゲット形式

Tenable Vulnerability Management では、スキャンのルーティングのターゲットとして次の形式がサポートされています。

ターゲットの形式	例
1 つの IPv4 アドレス	192.168.0.1
1 つの IPv6 アドレス	2001:db8::2120:17ff:fe56:333b
開始アドレスと終了アドレスで指定した IPv4 範囲	192.168.0.1-192.168.0.255
CIDR 表記の IPv4 サブネット	192.168.0.0/24
CIDR 表記の IPv6 サブネット	2001:db8::/32
IPv4 または IPv6 アドレスに解決可能なホスト	www.yourdomain.com
サブドメインとしてワイルドカードを含む、IPv4 アドレスまたは IPv6 アドレスに解決可能なホスト	*.yourdomain.com

スキャンのベストプラクティス

はじめに

脆弱性管理プログラムのニーズは企業ごとに異なります。使用するスキャナー(クラウドまたはオンプレミス)、センサーの配置場所、環境内のテクノロジー、脆弱性管理プログラムのその他の条件によって、要件は異なる場合があります。本書の情報は、すべての企業に適用できるデプロイメントのベストプラクティスであり、継続的な資産数の超過が発生した場合にも役立つ内容です。

一般的なベストプラクティス

ロールベースのアクセス制御 (RBAC)

アクセス制御 とRBAC を使用して、資産のスキャンと表示に関するアクセス許可を管理することができます。アクセス制御やユーザーグループの設定を誤ると、スキャンに失敗したり、ダッシュボードやレポートで資産や脆弱性の欠陥が生じたりする恐れがあります。

認証スキャン

Tenable は、可能な限り認証スキャンを実行することを推奨しています。認証スキャンにより、企業は現在の環境のより正確なスナップショットを手に入れ、ネットワークやシステムに関する情報を迅速かつ安全に収集することができます。この情報を利用して、セキュリティアーキテクチャのギャップを埋め、より良い判断を下して情報セキュリティプログラムを改善することができます。

また、認証スキャンは非認証スキャンよりも広範なチェックを実行でき、より正確なスキャン結果を提供します。これにより、ネットワークの広範なスキャンを確実に行うことができ、ローカルレベルでのエクスポージャーやコンプライアンス違反を特定できます。認証スキャンのメリットの詳細については、*Tenable Nessus Agent ユーザーガイド*にある認証スキャンをご覧ください。

資産の適切なインベントリ

ネットワーク内の既存の資産を正確に把握することは、効果的な脆弱性管理の第一歩です。詳細については、資産インベントリのベストプラクティスと資産インベントリの分析とレビューを参照してください。

資産の削除

ユーザーインターフェースを介して資産を削除できますが、その資産のライセンスはその後 90 日間または資産期限切れまで有効です。90 日以内または期限切れ前に資産が再度検出された場合には、新たなライセンス資産としてカウントされます。そのため、再検出されることが想定される資産は、ライセンスの問題を避けるためにグローバル除外リストに追加するか、削除された資産を削除後 7 日以内にパージするために資産エイジアウトを有効にすることをお勧めします。詳細は、Delete Legacy Workbench Assets を参照してください。

削除するすべての資産にタグを付け、API を利用してそれらの資産を一括削除することもできます。たとえば、資産に「削除」タグを付け、自動化されたスクリプトを使ってカスタム設定の時間間隔で削除することができます。再検出されることが想定される資産 (ハニースポットネットワークなど) は、ライセンスの問題を避けるためにグローバル除外リストに追加するか、スキャン対象範囲を縮小して除外することをお勧めします。

- 一括削除 API のドキュメント
- 除外 API のドキュメント
- 資産エイジアウト API のドキュメント

エージェントスキャン

エージェント は、可動性のある資産や機密性の高い資産の脆弱性データを取得する上で最適です。エージェントスキャンでは、TLS の脆弱性など、外部エクスポージャーの可能性を調べることはできないことを理解しておく必要があります。このようなタイプの資産にある外部エクスポージャーに関連する脆弱性が企業のプログラムにとって重要である場合は、ネットワークベースのスキャンと組み合わせる必要があります。脆弱性の認証スキャンを実行できない場合は、非認証スキャンを使用することができます。ただし、エージェントに対する非認証スキャンによって新たなライセンス付与資産が生じる可能性があることに注意してください。詳細については、次のセクションを参照してください。

スキャンの健全性

スキャンする前に、Tenable は *Tenable Vulnerability Management スキャンの調整ガイド*を確認することをお勧めします。Tenable Vulnerability Management では、スキャンスケジュールの総数を 10,000 件に制限しています。スキャンスケジュールには、スキャンテンプレート (検出および評価の設定を含む)、スキャンターゲットのリスト、および (オプションで) 認証情報およびコンプライアンス監査が含まれます。スキャンスケジュールは再利用することができ、スキャンスケジュールの [履歴] タブにスキャン結果がグループ化されます。

「オンデマンド」のスキャンスケジュールを再利用してスキャンスケジュールを探す手間を減らし、スキャンの健全性を良好に保つことがベストプラクティスです。新しい資産のセットをスキャンするたびに新しい「オンデマンド」のスキャンスケジュールを作成することには、ほとんどメリットはありません。その代わり、既存のスキャンスケジュールを使って、単に対象を変えたり、履歴を使って古いデータを確認したりすることが推奨されます。なお、ワークベンチにデータを送信することを避けた場合を除いて、スキャン中に見つかった変更点はすべてワークベンチに反映されるので、古いスキャン結果を再確認する必要性はあまりありません。

大抵、「前回のスキャンと今回では何が変わったのか」と考えるかもしれませんが、そうすると前回のスキャンに注意が向いてしまうことがあります。ただし、スキャンするたびに資産が最新の情報で更新されることに留意してください。[資産アクティビティ] タブでは、Tenable のセンサーが資産を検出したタイミングを確認することができます。さらに、各脆弱性には、その脆弱性やプラグインがいつ「最初に検出」され、いつ「最後に検出」されたかが表示されます。通常、この 2 つの日付の間で見られる違いは、前回のスキャン以降に変更された内容を特定するのに役立ちます。

最後に、事前に定義されたスキャンサイクル以外で資産を再スキャンするために、修正スキャンを使用することをベストプラクティスとして推奨します。脆弱性の [詳細] ページにある [アクション] ボタンから、修正スキャンを開始することができます。これは、修正スキャンを管理する最も便利な方法であり、スキャンの健全性を保つ上で役立ちます。

API スキャン作成のベストプラクティス

API を利用してスキャン作成を自動化したとしても、スキャンの健全性を維持することは依然として重要です。ワークロードに同じスキャンスケジュールを再利用できない場合は、Tenable は、スキャン削除を自動スキャン手順の一部にすることをお勧めします。新しいスキャンのたびに新しいスキャンポリシーを作成するのではなく、API ドキュメントで説明されているように、新しいスキャンを開始する際に `alt_targets` パラメーターを使用することを検討してください。

スキャンの健全性を維持することで、`/scans` エンドポイントへのリクエストごとに送り返されるスキャンの数を減らし、エンドポイントの速度の向上に役立ちます。

重複の課題と救済策

非認証スキャンは、資産を一意に特定するための十分なデータをスキャン中に取得できない可能性があります。よくある例として、複数のインターフェースを持つ資産の場合があります。続くセクションでは、この点のいくつかの例と考えられる解決策が示されています。

複数の NIC を持つサーバー

非認証スキャンでは、スキャン中に見つかった 2 つのネットワークインターフェースをマージするのに十分なデータを収集できない可能性があります。

解決策

- 認証情報を使って資産をスキャンして一意に特定し、複数の NIC の重複を排除します。
- 資産の追加の IP アドレスがレポート値を提供しない場合は、除外します。ネットワークスキャンを使用して資産を「ペネトレーションテスト」を行い、異なるネットワークインターフェース上のさまざまな脆弱性やオープンポートの可視化によって、インサイトや値が得られることもあります。レポートの精度の問題を修正するには、ユーザーインターフェースまたは API を使用して資産を削除してください。
- 削除された重複を削除するには、資産エイジアウトを有効にして、スキャンスケジュールをミラーリングします。

ファイヤーウォールとレイヤー 3 スイッチ

非認証スキャンでは、複数のインターフェースがスキャンされた場合、ファイヤーウォールやレイヤー 3 スイッチを一意に特定するのに必要なデータを十分収集できません。十分なデータを収集するには、Tenable Vulnerability Management はデバイスのシステム設定をクロールして、インターフェースの IP を確認しなければなりません。しかし、たとえ認証スキャンであっても、Tenable Vulnerability Management は設定ファイルをクロールしてこのようなデータを収集することはしません。

解決策

- スキャンで複数のインターフェースが見つかった場合、どのインターフェースの値が重複しているかを特定し、除外リストに追加します。
    - 例: 3 つのインターフェースを持つファイヤーウォールの場合、3 つの IP アドレスが存在し、そのうち 2 つの IP アドレスを除外し、ユーザーインターフェースまたは API を使って削除します。
- 削除された重複を削除するには、資産エイジアウトを有効にして、スキャンスケジュールをミラーリングします。

エージェントスキャンと非認証スキャン

非認証スキャンでは、2 つの検出結果 (エージェントスキャンと非認証スキャン) をマージするのに十分なデータを収集できない可能性があります。十分に堅牢化されたサーバーは、資産を一意に特定するのに十分なデータを提供しません。しかし、Tenable のアルゴリズムは、データがもっと多くある場合はライセンス数を減らして資産の重複を排除します。

解決策

- 充分に堅牢化されている資産や、Tenable のアルゴリズムが確信を持って資産をマージするのに必要なデータを提供しない資産については、認証情報を追加してください。そうすることによって、Tenable はマージに必要なデータを十分収集できるようになります。

一過性の資産

一時的な資産や、90 日の期限が切れる前に終了して再構築された資産は、再構築またはデプロイされるたびに新しい資産として作成されます。多くの場合、資産が終了した後に資産の属性が変更され、資産を以前のバージョンとマージすることが困難になることがあります。

解決策

- クラウドコネクタを使用します。クラウドコネクタは、クラウド上の一過性の資産を特定するだけでなく、その終了を検出して対応するライセンスを削除します。
- クラウドコネクタを利用できない場合は、資産エイジアウト機能を利用する必要があります。資産エイジアウト機能は、設定された期間内に資産が見つからない場合、自動的に資産をパージします。

スキャン制限事項

次の表は Tenable Vulnerability Management のスキャンの制限事項を示しています。

制限	説明
評価スキャンごとのターゲット IP アドレスまたはホスト名	Tenable Vulnerability Management は、1 回の評価スキャンでターゲットとする IP アドレスまたはホスト名の数を制限します (詳しくは、検出スキャンと評価スキャンを参照してください)。ホストターゲットの制限は、組織でライセンス付与されている資産数の 10 倍です。 たとえば、組織でライセンス付与されている資産数が 1,000 の場合、Tenable Vulnerability Management では 1 回の評価スキャンで 10,000 を超えるホスト名または IP アドレスをターゲットにできません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。
検出スキャンごとのターゲット IP アドレスまたはホスト名	Tenable Vulnerability Management は、1 回の検出スキャンでターゲットとする IP アドレスまたはホスト名の数を制限します (詳しくは、検出スキャンと評価スキャンを参照してください)。ホストターゲットの制限は、組織でライセンス付与されている資産数の 1,000 倍です。 たとえば、組織でライセンス付与されている資産数が 1,000 の場合、Tenable Vulnerability Management では 1 回の検出スキャンで 1,000,000 を超えるホスト名または IP アドレスをターゲットにできません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。
スキャンあたりのホストスキャン結果数	Tenable Vulnerability Management は、1 回のスキャンで生成できるライブホストの数を制限しています。ライブホストスキャン結果の制限は、所属組織のライセンスのある資産数の 1.1 倍です。 たとえば、所属組織のライセンスのある資産カウントが 1,000 の場合、Tenable Vulnerability Management では 1 回のスキャンで 1,100 を超えるライブホストのスキャン結果を生成できません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。Tenable Vulnerability Management は、検出スキャンにはライブホストスキャン結果の上限を適用しません。 Tenable Vulnerability Management1 回のスキャンで生成できるスキャン結果のデッドホストの数も制限しています。デッドホストスキャン結果の上限は、所属組織のライセンスのある資産カウントの 100 倍です。

	たとえば、所属組織のライセンスのある資産カウントが 1,000 の場合、Tenable Vulnerability Management では 1 回のスキャンで 100,000 を超えるデッドホストのスキャン結果を生成できません。この上限を超えると、Tenable Vulnerability Management はスキャンを中止します。
スキャンごとのターゲット IP アドレスまたは範囲	スキャンのターゲットを設定する際に、300,000 個を超えるコンマ区切りの IP アドレスまたは範囲を指定することはできません。
アクティブスキャン	コンテナで 25 を超えるスキャンを同時に実行することはできません。
チャンクのスキャン	Tenable Vulnerability Management は、スキャンチャンクを 10,000 個のホストまたは 150,000 件の検出結果に制限します。スキャンチャンクがいずれかの値を超えると、Tenable Vulnerability Management はスキャンを処理せず、最終的に中止します。
スキャンの設定	Tenable Vulnerability Management で作成できるスキャン設定の数は 10,000 スキャンに制限されています。Tenable では、新しいスキャンを作成する代わりに、スケジュールされたスキャンを再利用することを推奨しています。このアプローチにより、ユーザーインターフェースの待ち時間が短縮できます。

調査

Tenable Vulnerability Management の **[調査]** セクションには、所属組織の検出結果と資産が、カスタマイズ可能なダッシュボードやワークベンチに表示されます。このデータは、スキャンから取得されたものです。Tenable Vulnerability Management は、複雑なアルゴリズムを使用して、受信したスキャンデータを既存のリソースと照合するか、新しいリソースを作成します。

トレンドを特定できるビジュアル化された概要、特定のリソースを返すフィルター、豊富なエクスポート機能など、さまざまな方法でデータを表示して分析できます。さらに、これらすべてを 1 つのインターフェースで実行できます。

[調査] セクションには、**[調査の概要]** ページ、**[検出結果]** ワークベンチ、および **[資産]** ワークベンチの 3 つのコンポーネントがあります。

> **ヒント**: レガシーワークベンチから移行する場合の機能の比較については、調査 ワークベンチとレガシーワークベンチ を参照してください。

調査の概要

検出結果

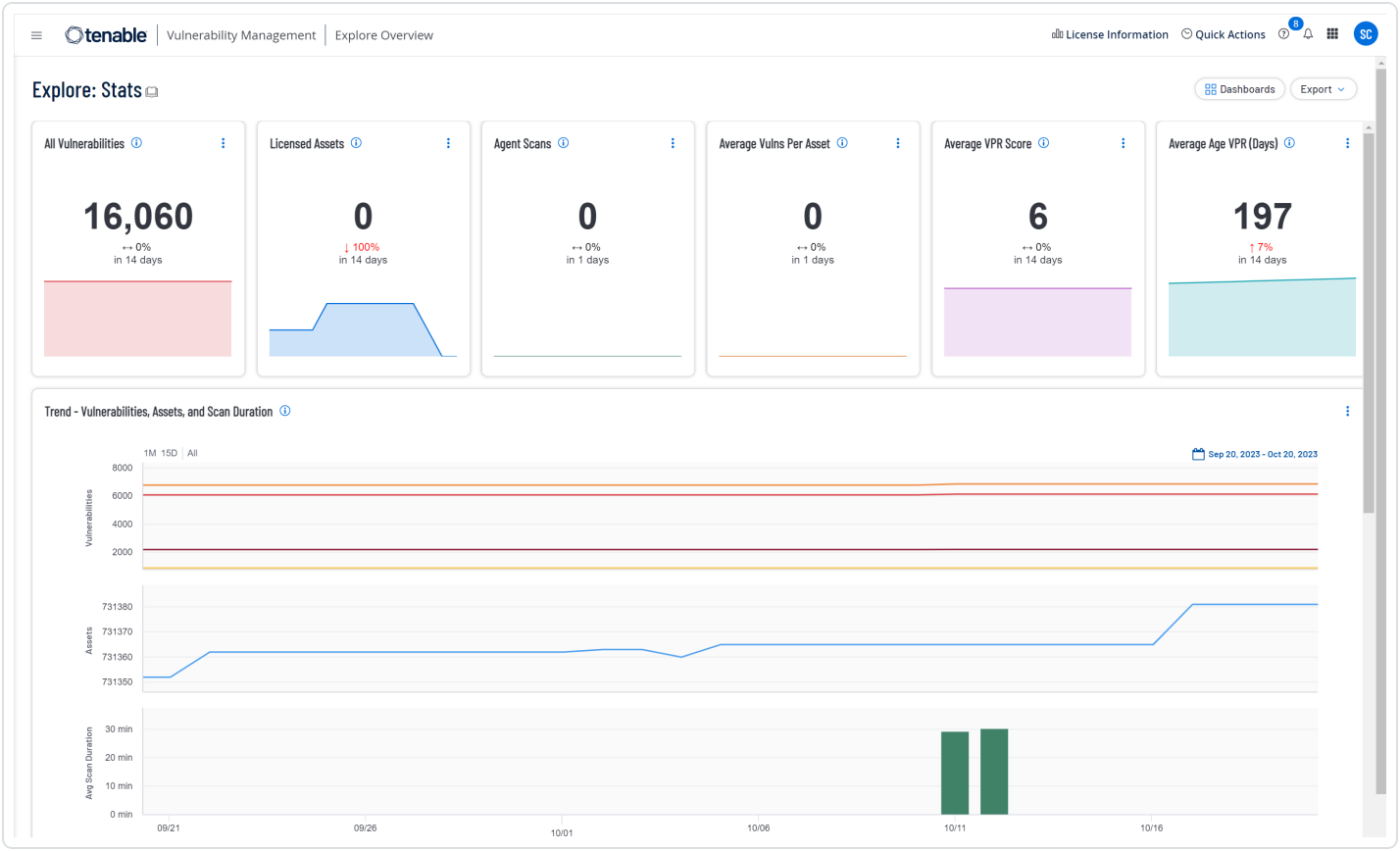
資産

調査 ワークベンチとレガシーワークベンチ

調査の概要

[調査の概要] ページでは、カスタマイズ可能なダッシュボードに所属組織の検出結果と資産の概要がビジュアル化されて表示され、トレンドを特定することができます。たとえば、ソース別の資産、一定期間の平均スキャン時間、一定期間の資産あたりの平均脆弱性を表示できます。また、個別の項目にカーソルを合わせて追加情報を表示したり、項目をクリックして詳細情報にドリルダウンしたり、データをエクスポートしたりもできます。Tenable Vulnerability Management はスキャンを実行するたびにダッシュボードをアップデートします。

注意: Tenable Vulnerability Management はダッシュボードをアップデートする前にスキャンデータをインデックス化します。そのため、アップデートはすぐには反映されません。Tenable Vulnerability Management は、ダッシュボードのアップデート前に、キャッシュデータを最大 30 分間表示する場合があります。



[調査の概要] ページを表示する

[調査の概要] ページを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

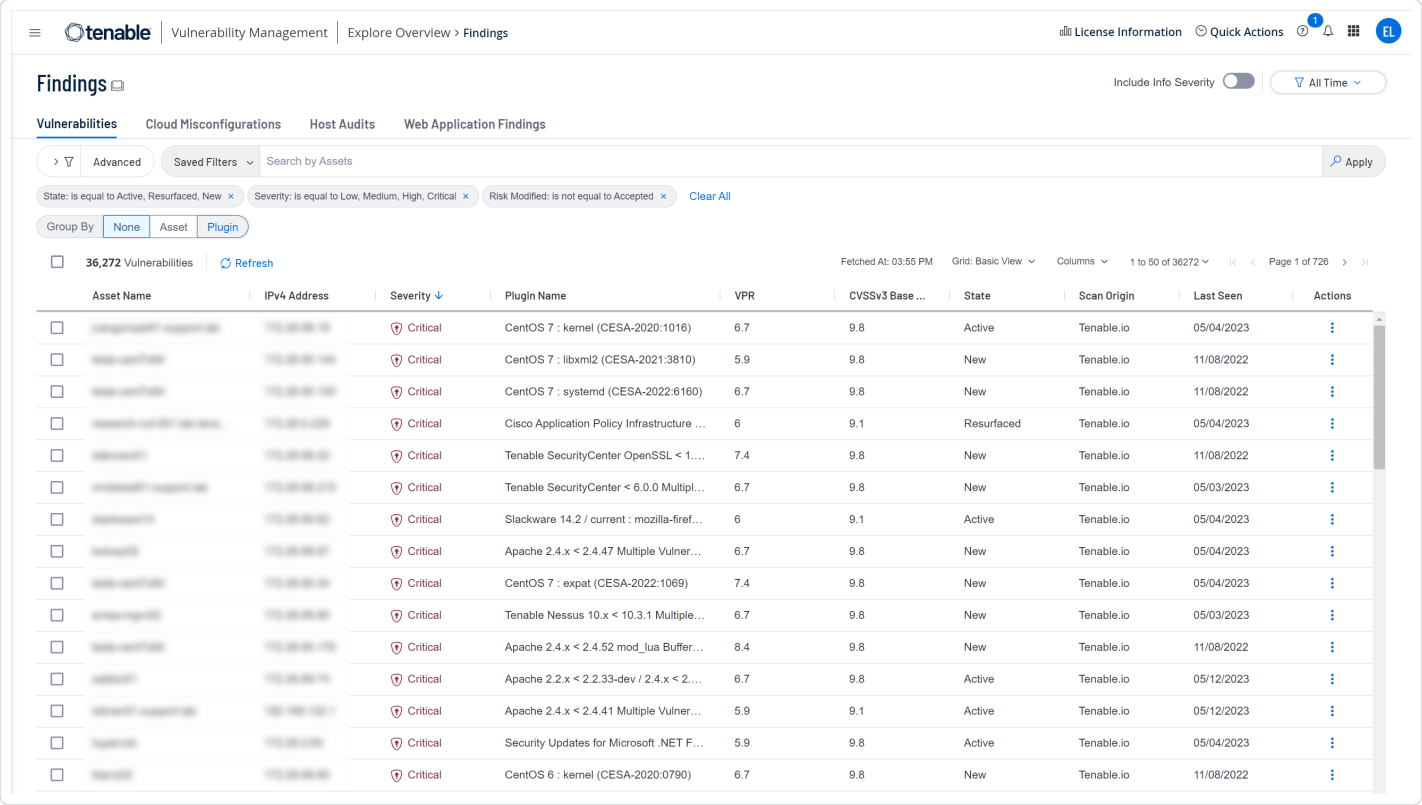
2. 左側のナビゲーションプレーンで **[調査]** をクリックします。

   [調査の概要] ページが表示されます。ページには次のウィジェットが含まれています。

ウィジェット	説明
すべての脆弱性	過去 14 日間のすべてのホスト脆弱性の傾向を表示します。
ライセンスのある資産	過去 14 日間のすべてのライセンスのある資産の傾向を表示します。
エージェントスキャン	過去 14 日間のエージェントスキャンの傾向を表示します。
資産ごとの平均脆弱性	過去 14 日間のホスト資産別の脆弱性の傾向を表示します。
平均 VPR スコア	過去 14 日間のホストタイプの Vulnerability Priority Rating (VPR) スコアの傾向を表示します。
平均 VPR (日数)	過去 14 日間のホストの脆弱性の平均 VPR 日数の傾向を表示します。
トレンド - 脆弱性、資産、スキャン期間	スキャン結果の傾向を表示します。これには、ホストの脆弱性、経時的な資産数、スキャン期間が含まれます。右上で、日付の範囲でフィルタリングします。
ソース別資産	資産の推移をソースごとに色付きの線で示し、各ソースの傾向を時系列で表示します。右上で、日付の範囲でフィルタリングします。このウィジェットの資産数は、過去 7 日間のスキャンに基づいています。

検出結果

[検出結果] ワークベンチでは、所属組織の検出結果に関するインサイトを得ることができます。これには、脆弱性、クラウド設定ミス、ホスト監査、ウェブアプリケーションの検出結果が含まれます。



注意: Tenable Vulnerability Management は検出結果データを 15 か月間保持します。

それぞれの検出結果は、資産上に表示される脆弱性の 1 つのインスタンスであり、プラグイン ID、ポート、プロトコルによって一意に識別されます。検出結果についての包括的な情報を提供することで、Tenable Vulnerability Management はセキュリティリスクの可能性を低減し、十分に活用されていないリソースを特定し、コンプライアンスの取り組みをサポートします。

Tenable Vulnerability Management はスキャンが完了したとき、またはスキャン結果がインポートされたときに、検出結果を自動的に作成または更新します。

詳細については、次のトピックを参照してください。

検出結果ワークベンチの表示

[検出結果] ワークベンチですべての検出結果を表示できます。

検出結果を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[調査]** > **[検出結果]** をクリックします。

   [検出結果] ワークベンチが **[脆弱性]** タブがアクティブな状態で表示されます。

3. (オプション) 次のいずれかの操作を実行します。

   - 1つの検出結果タイプを表示するには、次のいずれかのタブをクリックします。
     - 脆弱性
     - クラウドの設定ミス
     - ホスト監査
     - ウェブアプリケーションの検出
   - [検索] ボックスで、資産名で検出結果を検索します。

     注意: Tenable Vulnerability Management は、ワイルドカード (*) を使用しない限り、完全一致を検索します。たとえば、「1」で終わるすべての値を見つけるには、*1* と入力します。

   - 検出結果または資産のフィルタリング の説明に従って、表示された検出結果をフィルタリングし、ビューをカスタマイズします。

     ヒント: すべての検出結果フィルターの定義を確認するには、検出結果フィルターを参照してください。

   - 検出結果または資産の保存されたフィルター で説明されているように、フィルターをカスタム検索として保存します。
   - 検出結果のグループ化 の説明に従って、資産やプラグインなどで検出結果をグループ化します。

- 右上にある**[情報の深刻度を含める]**をクリックすると、これらの検出結果も含めることができます。このオプションは、脆弱性とウェブアプリケーションの検出結果にのみ適用されます。脆弱性の深刻度インジケーターの説明を参照してください。
- 右上にあるドロップダウンを使用して、表示された検出結果を期間でフィルタリングします。
- 検出結果または資産のエクスポート で説明されているように、検出結果を CSV または JSON 形式にエクスポートします。
- 検出結果の詳細の表示の説明に従って、検出結果の詳細を表示します。

脆弱性

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[検出結果] ワークベンチで **[脆弱性]** タブをクリックすると、資産の脆弱性が表示されます。一般的な脆弱性には、システムの設定ミス、パッチが適用されていないソフトウェア、貧弱なデータ暗号化、脆弱な認証情報などがあります。

[脆弱性] タブには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズを参照してください。

列	説明
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
資産名	資産の名前。この値は Tenable Vulnerability Management に対して一意です。
資産タグ	資産に適用されるタグです。
IPv4 アドレス	影響を受けている資産の IPv4 アドレス。
IPv6 アドレス	影響を受けている資産の IPv6 アドレス。
最終修正日	以前に検出された脆弱性が最後にスキャンされ、資産にもう存在しないと記録された時間。
深刻度	CVSS に基づく脆弱性の深刻度。詳細は、CVSS と VPR を参照してください。
プラグイン名	検出結果で検出された脆弱性を特定したプラグインの名前です。
プラグイン ID	脆弱性を特定したプラグインの ID。
プラグインファミリー	脆弱性を特定したプラグインのファミリー。
ポート	スキャンで脆弱性が検出された資産にスキャナーが接続するために使用したポート。
Protocol	スキャンで脆弱性が検出された資産との通信で、スキャナーが使用

	したプロトコル。
修正にかかった時間	スキャンで特定された脆弱性の修正に所属組織がかけた時間 (時間数または日数) です。修正済みの脆弱性に関してのみ表示されます。より正確な結果を得るには、このフィルターと、**[修正済み]** に設定した **[状態]** フィルターを併用します。
VPR	脆弱性の VPR を示す説明アイコン。詳細は、CVSS と VPR を参照してください。
CVSSv2 基本値	CVSSv2 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。Tenable Vulnerability Management では、**[脆弱性の深刻度メトリクス]** の設定に応じて **CVSSv2** または **CVSSv3** の列が表示されます。
状態	脆弱性の状態。
CVSSv3 基本値	CVSSv3 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。Tenable Vulnerability Management では、**[脆弱性の深刻度メトリクス]** の設定に応じて **CVSSv2** または **CVSSv3** の列が表示されます。
検出元	検出結果を検出したスキャナー。また、スキャンがワークロードスキャンであるかどうかを示します。この列で使用できる値は、Tenable Vulnerability Management、Tenable Security Center、および [エージェントなしの評価] です。
リージョン	資産が実行されるクラウドリージョン。
アカウント ID	資産をホストするクラウドサービスの資産リソースに割り当てられた一意の識別子。
Live Result	スキャン結果が Live Results に基づいているかどうかを示します。Agentless Assessment の Live Results 機能を使えば、新しいスキャンを実行しなくても、直近で収集されたスナップショットデータに基づく新しいプラグインのスキャン結果を見ることができます。可能な値は、**Yes** または **No**です。詳細については、Agentless Assessment の Live Results を参照してください。

初回確認日	スキャンが資産上で初めて脆弱性を検出した日付。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
アクション	この列の⋮ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **レポートを生成** - レポートで説明されているように、テンプレートからレポートを生成します。 • **変更** – 検出結果の変更ルールまたは許容ルールの追加で説明されているように、検出結果の深刻度を変更または承認します。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。 • **すべての詳細を表示** – 検出結果の詳細の表示で説明されているように、検出結果の詳細をすべて表示します。 • **修正プロジェクトの作成** - 修正プロジェクトで説明されているように、資産に対して新しい修正プロジェクトを開始します。 • **修正スキャンの起動** - 修正スキャンの起動で説明されているように、修正スキャンを開始して既存のスキャン結果をフォローアップします。

クラウドの設定ミス

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[検出結果] ワークベンチで **[クラウドの設定ミス]** タブをクリックし、クラウドの設定ミスを表示します。クラウドでよくある設定ミスには、無制限のインバウンドポートやアウトバウンドポート、認証情報の管理と暗号化、監視とログの無効化、安全でない自動バックアップ、ストレージアクセスなどがあります。

[クラウドの設定ミス] タブには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズ を参照してください。

列	説明
リソース ID	リソースタイプと資産名からなる一意の識別子。
ポリシー名	影響を受けている資産を管理するセキュリティポリシー。
ポリシーグループ名	影響を受けている資産を管理するセキュリティポリシーに関連付けられているグループ。
深刻度	CVSS に基づく脆弱性の深刻度。詳細は、CVSS と VPR を参照してください。
結果	脆弱性スキャンの結果。
ソース	影響を受けている資産が実行されている環境。
初回確認日	スキャンが資産上で初めて脆弱性を検出した日付。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
クラウドプロバイ	資産をホストするクラウドプロバイダーの名前。

ダー	
IaC リソースタイプ	資産のインフラのコード化 (IAC) リソースタイプ。
リソース名	スキャナーで脆弱性が検出された資産の名前。Tenable Vulnerability Management はこの識別子に、特定の資産属性が存在するかに応じて、次の優先順位に基づいて資産属性を割り当てます。 1. エージェント名 (エージェントスキャンの場合) 2. NetBIOS 名 3. FQDN 4. IPv6 アドレス 5. IPv4 アドレス たとえばスキャンによって、ある資産の NetBIOS 名と IPv4 アドレスが特定された場合、NetBIOS 名がリソース名として表示されます。
リージョン	資産が実行されるクラウドリージョン。
VPC	資産が AWS でホストされている仮想プライベートクラウド。
ARN	AWS にある資産を示す一意の Amazon リソース名。
リソースタイプ	プラグインデータによって判別された、影響を受けている資産のタイプ。
ベンチマーク	検出結果に関連付けられているベンチマーク。
アカウント ID	資産をホストするクラウドサービスの資産リソースに割り当てられた一意の識別子。
リポジトリ	資産に関連付けられているコードリポジトリ。

リソースタイプ	プラグインデータによって判別された、影響を受けている資産のタイプ。
ポリシーカテゴリ	影響を受けている資産を管理するセキュリティポリシーに関連付けられているカテゴリ。
最終スキャン時間	Tenable Vulnerability Management が資産を最後にスキャンした日時。
更新時間	ユーザーが資産を最後に更新した日時。
アクション	この列の ⋮ ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **レポートを生成** - レポートで説明されているように、テンプレートからレポートを生成します。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。

ホスト監査

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[検出結果] ワークベンチで **[ホスト監査]** タブをクリックすると、ホスト監査の検出結果が表示されます。ホスト監査は、ターゲットに適用されている設定、堅牢化、セキュリティコントロールを評価するために、ワークステーション、サービス、ネットワークデバイスを評価します。特定のホスト監査結果を表示して、修正すべき問題を特定します。

[ホスト監査] タブには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズを参照してください。

列	説明
監査チェック名	影響を受けている資産に対してスキャナーが実行したコンプラインスチェックの名前です。
監査ファイル	スキャナーがコンプライアンスチェックの実行に使用した監査ファイルの名前です。
結果	コンプライアンスチェックの結果です。
プラグイン名	コンプライアンスチェックの検出結果を特定したプラグインの名前。
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
資産名	資産の名前。この値は Tenable Vulnerability Management に対して一意です。
資産タグ	資産に適用されるタグです。
状態	コンプライアンスチェックの検出結果の状態。
最終監査日	スキャンによって資産のコンプライアンスチェックが最後に実行された日時です。
コントロール ID	影響を受けている資産をホストするシステムに適用されるコントロールインスタンスの UUID です。この値は Tenable Vulnerability Management に対して一意です。

アクション	この列の⋮ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。 • **すべての詳細を表示** – 検出結果の詳細の表示で説明されているように、検出結果の詳細をすべて表示します。

ウェブアプリケーションの検出

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[検出結果] ワークベンチの **[ウェブアプリケーションの検出]** タブをクリックすると、ウェブアプリケーションの検出結果が表示されます。一般的なウェブアプリケーションの検出結果には、SQL インジェクション、クロスサイトスクリプティング、ローカルファイルインクルージョン、セキュリティ設定ミス、XML 外部エンティティ処理などがあります。

[ウェブアプリケーションの検出] タブには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズを参照してください。

列	説明
資産 ID	スキャンで脆弱性が検出された資産の UUID。この値は Tenable Vulnerability Management に対して一意です。
資産名	スキャナーで脆弱性が検出された資産の名前。この値は Tenable Vulnerability Management に対して一意です。
IPv4 アドレス	資産レコードに関連付けられた IPv4 アドレスです。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します (例: hostname_example, example.com, 192.168.0.0)。IP アドレスには、個別のアドレス、CIDR 表記 (例: 192.168.0.0/24)、または範囲 (例: 192.168.0.1-192.168.0.255) を指定できます。 **注意:** このパラメーターで CIDR マスク /0 を指定するとすべての IP アドレスに適合するので、Tenable Vulnerability Management ではこの値がサポートされていません。このパラメーターに値 /0 を指定すると、Tenable Vulnerability Management は 400 Bad Request エラーメッセージを返します。
深刻度	CVSS に基づく脆弱性の深刻度。詳細は、CVSS と VPR を参照してください。
プラグイン名	脆弱性を特定したプラグインの名前。
プラグイン ID	脆弱性を特定したプラグインの ID。

プラグインファミリー	脆弱性を特定したプラグインのファミリー。
CVSSv2 基本値	CVSSv2 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。 Tenable Vulnerability Management では、**[脆弱性の深刻度メトリクス]** の設定に応じて **CVSSv2** または **CVSSv3** の列が表示されます。
CVSSv3 基本値	CVSSv3 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。 Tenable Vulnerability Management では、**[脆弱性の深刻度メトリクス]** の設定に応じて **CVSSv2** または **CVSSv3** の列が表示されます。
状態	脆弱性の状態。
初回確認日	スキャンが資産上で初めて脆弱性を検出した日付。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
アクション	この列の ⋮ ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **変更** – 検出結果の変更ルールまたは許容ルールの追加で説明されているように、検出結果の深刻度を変更または承認します。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。 • **すべての詳細を表示** – 検出結果の詳細の表示で説明されているように、検出結果の詳細をすべて表示します。

検出結果の詳細の表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[検出結果] ワークベンチから、1 つの資産をドリルダウンすると、**[検出結果の詳細]** ページに資産が表示されます。Tenable Vulnerability Management は検出結果のタイプ別にこのページをカスタマイズします。

検出結果の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[調査]** > **[検出結果]** をクリックします。

   [検出結果] ワークベンチが **[脆弱性]** タブがアクティブな状態で表示されます。

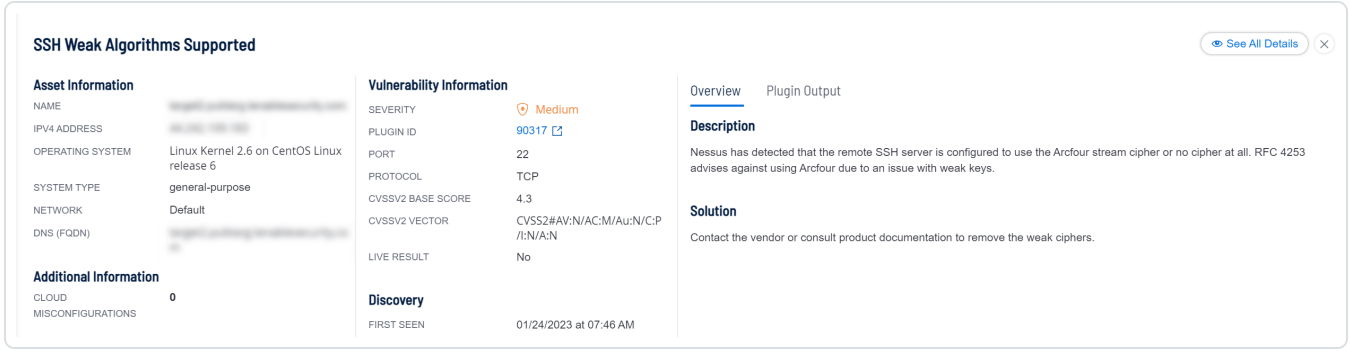
3. (オプション) 別の検出結果タイプを表示するには、別のタブをクリックします。

   そのタイプの検出結果が表示されます。タイプによって表示されるデフォルト列は異なります。

4. 検出結果または資産のフィルタリング の説明に従って、表示された検出結果をフィルタリングし、ビューをカスタマイズします。

5. 検出結果を表示する行をクリックします。

   プレビューがページの下部に表示されます。



6. プレビューで、**[すべての詳細を表示]**をクリックします。

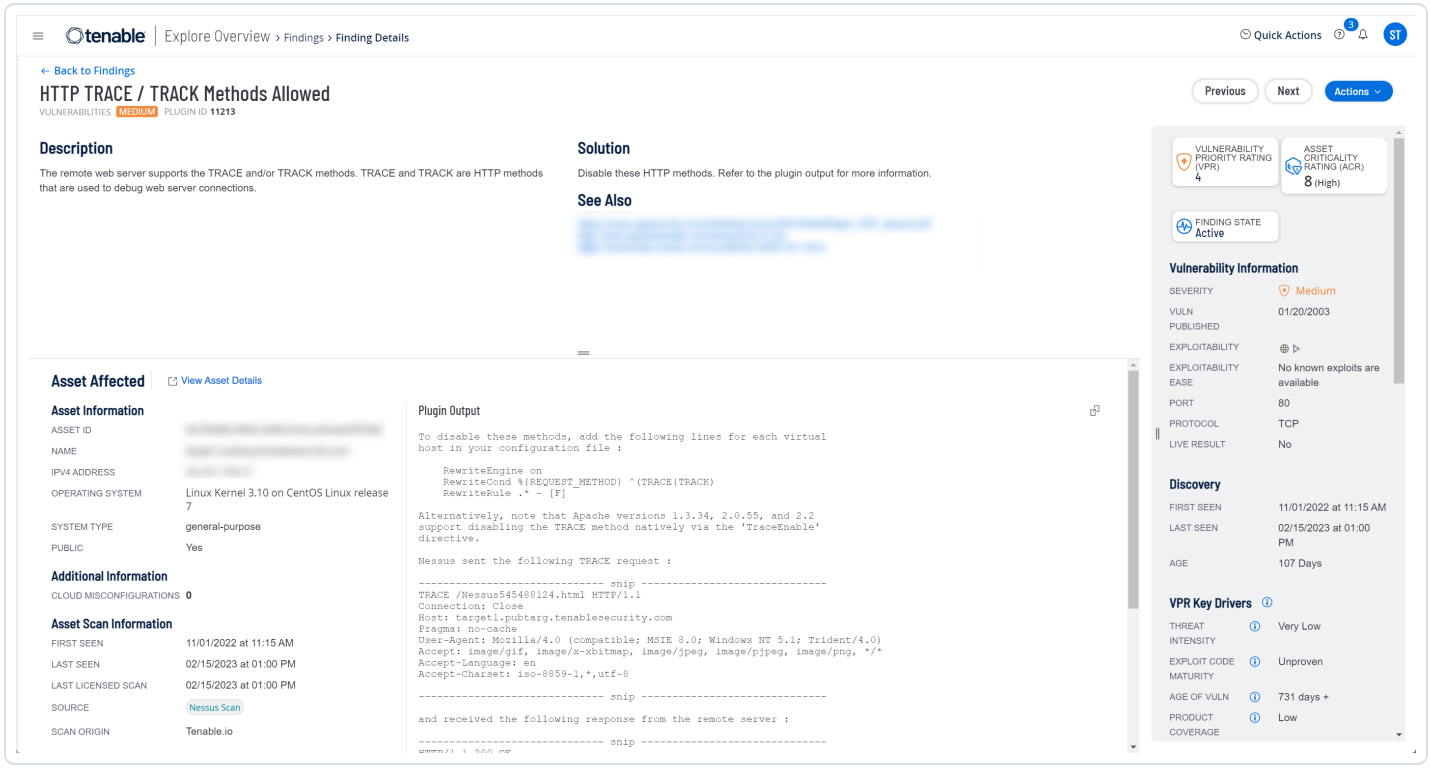
   [検出結果の詳細]ページが表示されます。ページのレイアウトは検出結果のタイプによって異なります。

   - 脆弱性の詳細
   - クラウド設定ミスの詳細
   - ホスト監査の詳細
   - ウェブアプリケーションの検出結果の詳細

脆弱性の詳細

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

検出結果の詳細の表示 を行う際の **[検出結果の詳細]** ページは、検出結果タイプによって異なります。脆弱性の検出結果の場合、説明、推奨されるソリューション、プラグインの出力が含まれます。



脆弱性の **[検出結果の詳細]** ページには、次のセクションがあります。

注意: Tenable Vulnerability Management は空のセクションを非表示にするため、これらのセクションは表示されない場合があります。

セクション	説明
説明	検出結果で検出された脆弱性を特定した Tenable プラグインの説明です。
ソリューション	検出結果で検出された脆弱性を修正する方法に関する概要です。公式のソリューションが使用可能な場合にのみ表示されます。

その他の関連項目	検出結果で検出された脆弱性についての役立つ情報を含むウェブサイトへのリンクです。
資産情報	影響を受けている資産に関する情報で、次のものが含まれます。 • **資産 ID** - スキャンで脆弱性が検出された資産の UUID。 • **Name** - スキャンで脆弱性が検出された資産の名前。この値は Tenable Vulnerability Management に対して一意です。 • **IPV4 アドレス** - 影響を受けている資産の IPv4 アドレス。 • **IPV6 アドレス** - 影響を受けている資産の IPv6 アドレス。 • **オペレーティングシステム** - 影響を受けている資産にインストールされているとスキャンによって識別されたオペレーティングシステム。 • **システムタイプ** - 影響を受けている資産にインストールされているとスキャンによって識別されたオペレーティングシステムのタイプ。 • **ネットワーク** - 資産を特定したスキャナーに関連付けられているネットワークオブジェクトの名前。デフォルトの名前は **Default** です。詳細は、ネットワークを参照してください。 • **パブリック** - 資産がパブリックネットワークで使用可能かどうかを指定します。パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Management クエリ名前空間の `is_public` 属性によって識別されます。
クラウドの設定ミス	設定されたポリシーに準拠していないリソースの数。この数字をクリックして **[クラウドの設定ミス]** タイルに移動し、影響を受けているリソースを表示します。
資産スキャン情報	脆弱性を検出したスキャンに関する情報。次の情報が含まれます。 • **初回確認日** - スキャンが資産上で初めて脆弱性を検出した日付。 • **最終確認日** - スキャンが資産上で脆弱性を検出した直近の日付。 • **最終ライセンススキャン日** - 資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ラ

	イセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]**フィールドは更新されますが、**[最終認証スキャン日]**フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。 • **最終認証スキャン日** - 資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]**フィールドは更新されますが、**[最終ライセンススキャン日]**フィールドは更新されません。 • **ソース** - 影響を受けている資産の脆弱性を検出したスキャンのソース。 • **検出元** - 結果を検出したスキャナー。また、スキャンがワークロードスキャンであるかどうかを識別するのにも役立ちます。使用できる値は、Tenable Vulnerability Management、Tenable Security Center、およびエージェントなしの評価です。
追加情報	脆弱性の検出結果に関する追加情報で、次のものが含まれます。 • **ネットワーク** - 検出結果を特定したスキャナーに関連付けられたネットワークオブジェクトの名前。デフォルトのネットワーク名は**[Default]**です。詳細は、ネットワークを参照してください。 • **DNS (FQDN)** - 検出結果で特定された脆弱性が検出されたホストの完全修飾ドメイン名。 • **MAC アドレス** - 影響を受けている資産の静的メディアアクセス制御 (MAC) アドレス。 • **Tenable ID** - 影響を受けている資産に関連付けられている Tenable アカウントの一意の識別子。 • **インストール済みソフトウェア** - 影響を受けている資産でスキャンによって識別されたソフトウェア。 • **SSH フィンガープリント** - スキャンによって資産レコードに関連付けられた SSH キーのフィンガープリント。

Vulnerability Priority Rating (VPR)	(Tenable Lumin ライセンスが必要) 脆弱性の VPR を示す説明アイコンです。詳細は、CVSS と VPR を参照してください。
資産重大度の格付け (ACR)	(Tenable Lumin ライセンスが必要) 企業にとっての資産の重大度を 1 ～ 10 の範囲で評価します。値が高いほど、ビジネスにおけるその資産の重大度が高くなります。詳細は、Tenable Lumin のメトリクス を参照してください。
検出結果の状態	脆弱性の状態を示す説明アイコンです。詳細は、脆弱性の状態 を参照してください。
脆弱性の情報	プラグインが特定した脆弱性に関する情報です。次のものが含まれます。 • **深刻度** - 検出結果に関する脆弱性の深刻度。 • **元の深刻度** - スキャンが最初に検出結果を検出した際の、脆弱性に関する CVSS ベースの深刻度。 • **公開日** - 脆弱性がアドバイザリで文書化されたか、または National Vulnerability Database (NVD) で公開された最も古い日付。 • **悪用される可能性** - 脆弱性の潜在的な悪用可能性において考慮される、脆弱性の特性。 • **悪用の容易さ** - 脆弱性をどれほど容易に悪用できるかに関する説明。 • **悪用される経路** - 脆弱性が悪用される可能性のある特に一般的な方法。 • **マルウェアによる悪用** - 脆弱性がマルウェアによって悪用されたことが知られているかどうかを示します。 • **Nessus による悪用** - 特定プロセス中に Tenable Nessus がその脆弱性をエクスプロイトしたかどうかを示します。 • **報道の有無** - このプラグインが、メディア (たとえば ShellShock や Meltdown) の注目を受けたかどうかを示します。 • **最終修正日** - 以前に検出された脆弱性が最後にスキャンされ、資産にもう存在しないと記録された時間。

	• **マルウェア** - その脆弱性を特定したプラグインでマルウェアが検査されるかどうかを示します。 • **修正にかかった時間** - スキャンで特定された脆弱性の修正に所属組織がかけた時間 (時間数または日数) です。修正済みの脆弱性に関してのみ表示されます。より正確な結果を得るには、このフィルターと、**[修正済み]** に設定した **[状態]** フィルターを併用します。 • **ベンダーのサポートなし** - このプラグインにより検出されたソフトウェアは、ソフトウェアベンダーによってサポートされていません (たとえば、Windows 95 や Firefox 3)。 • **パッチ公開日** - 脆弱性に対するパッチが公開された日付を表示します。 • **ポート** - スキャンで脆弱性が検出された資産に接続するためにスキャナーが使用したポート。 • **プロトコル** - スキャンで脆弱性が検出された資産との通信で、スキャナーが使用したプロトコル。 • **Live Result** - スキャン結果がライブ結果に基づいているかどうかを示します。Agentless Assessment の Live Results 機能を使えば、新しいスキャンを実行しなくても、直近で収集されたスナップショットデータに基づく新しいプラグインのスキャン結果を見ることができます。可能な値は、**Yes** または **No**です。詳細については、Agentless Assessment の Live Results を参照してください。 • **CPE** - プラグインが特定する脆弱性の共通プラットフォーム一覧 (CPE) 番号。 • **資産インベントリ** - このプラグインは Asset Inventoryのプラグインです。 • **デフォルトアカウント** - デフォルトの認証情報またはアカウント。
検出	Tenable Vulnerability Management が脆弱性を最初に検出した時に関する情報。次の情報が含まれます。 • **初回確認日** - スキャンが資産上で初めて脆弱性を検出した日付。

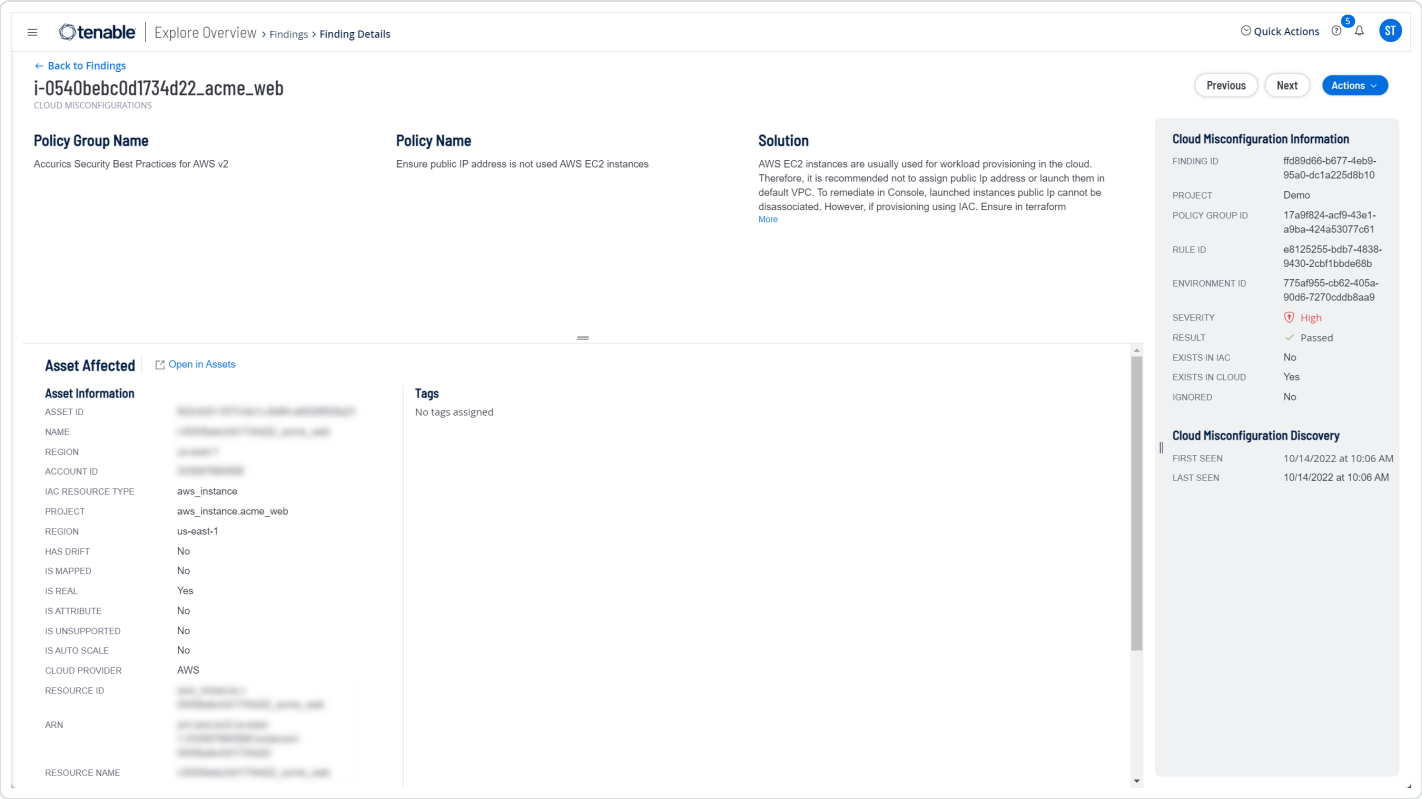
	• **最終確認日** - スキャンが資産上で脆弱性を検出した直近の日付。 • **経過日数** - ネットワーク内の資産上で、スキャンによってその脆弱性が最初に検出されてから経過した日数。
VPR の主要推進要因	Tenable がこの脆弱性の VPR の計算に使用する主な要因に関する情報で、次のものが含まれます。 • **脅威の最新度** - 脆弱性の脅威イベントが発生してからの経過日数 (0 ~ 730)。 • **脅威度** - この脆弱性に関連して直近で検出された脅威イベントの数と頻度に基づく相対強度 (**最低**、**低**、**中**、**高**、**最高**)。 • **エクスプロイトコード成熟度** - 内部および外部のソース (Reversinglabs、Exploit-db、Metasploit など) のエクスプロイトインテリジェンスの存在、巧妙さ、流行に基づく、脆弱性の可能性があるエクスプロイトの相対的な成熟度。可能な値 (**高**、**動作可能**、**PoC**、または **未実証**) は CVSS エクスプロイトコード成熟度と同等です。 • **脆弱性の経過日数** - National Vulnerability Database (NVD) が脆弱性を公開してからの経過日数。 • **製品の対象範囲** - 脆弱性の影響を受けている固有の製品の相対的な数 (**低**、**中**、**高**、**最高**)。 • **CVSS3 影響スコア** - 脆弱性に関して NVD が提供する CVSSv3 影響スコア。NVD がスコアを提供しなかった場合、Tenable Vulnerability Management では Tenable が予測したスコアが表示されます。 • **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。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。
プラグインの詳細	脆弱性を検出したプラグインに関する情報で、次のものが含まれます。 • **公開日** - 脆弱性を特定した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。

	• **ファミリー** - 脆弱性を特定したプラグインのファミリー。 • **タイプ** - プラグインチェックの一般的なタイプ (たとえば、ローカルまたはリモート)。 • **バージョン** - 脆弱性を特定したプラグインのバージョン。 • **プラグイン ID** - 脆弱性を特定したプラグインの ID。
リスク情報	影響を受けている資産に脆弱性が与える相対リスクに関する情報で、次のものが含まれます。 • **リスクファクター** - プラグインに関連する CVSS に基づくリスク要因。 • **CVSSv3 基本スコア** - 時間の経過やユーザー環境によらず一定である、本質的かつ基本的な脆弱性の特性です。 • **CVSSv3 現状値** - 時間の経過とともに変化する脆弱性の特性です。 • **CVSSV3 手法** - 脆弱性に関する追加の CVSSv3 メトリクス。 • **CVSSv2 基本スコア** - 時間の経過やユーザー環境によらず一定である、本質的かつ基本的な脆弱性の特性です。 • **CVSSv2 現状値** - 時間の経過とともに変化するがユーザー環境間では不変の、脆弱性の特性を示すスコアです。 • **CVSSV2 手法** - 脆弱性に関する追加の CVSSv2 メトリクス。 • **STIG 深刻度** - 米国国防総省のセキュリティ技術実装ガイド (STIG) に基づく脆弱性の深刻度評価です。
参照情報	脆弱性に関する追加情報を提供する業界リソースです。
アクション	右上の **[アクション]** ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **レポートを生成** - レポートで説明されているように、テンプレートからレポートを生成します。

	• **変更** – 検出結果の変更ルールまたは許容ルールの追加で説明されているように、検出結果の深刻度を変更または承認します。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。 • **すべての詳細を表示** – 検出結果の詳細の表示で説明されているように、検出結果の詳細をすべて表示します。 • **新しいタブですべての詳細を表示** – 資産の完全な詳細をブラウザの新しいタブに表示します。 • **修正プロジェクトの作成** - 修正プロジェクトで説明されているように、資産に対して新しい修正プロジェクトを開始します。 • **修正スキャンの起動** - 修正スキャンの起動で説明されているように、修正スキャンを開始して既存のスキャン結果をフォローアップします。

クラウド設定ミスの詳細

検出結果の詳細の表示 を行う際の **[検出結果の詳細]** ページは、検出結果タイプによって異なります。クラウド設定ミスの検出結果には、ポリシー情報、推奨されるソリューション、影響を受ける資産の詳細が含まれます。



クラウド設定ミスの **[検出結果の詳細]** ページには、次のセクションがあります。

注意: Tenable Vulnerability Management は空のセクションを非表示にするため、これらのセクションは表示されない場合があります。

セクション	説明
ポリシーグループ名	影響を受けている検出結果に関連付けられているクラウドポリシーグループの名前。
ポリシー名	影響を受けている検出結果に関連付けられているクラウドポリシーの名前。
ソリューション	脆弱性を修正する方法に関する簡単な概要。このセクションは、公式のソリューションが使用可能な場合にのみ表示されます。

資産情報	影響を受けている資産に関する情報で、次のものが含まれます。 • **資産 ID** - スキャンで脆弱性が検出された資産の UUID。この値は Tenable Vulnerability Management に対して一意です。 • **Name** - スキャンで脆弱性が検出された資産の名前。この値は Tenable Vulnerability Management に対して一意です。 • **プロジェクト** - 検出結果と影響を受けている資産に関連付けられたクラウドプロジェクト。 • **リージョン** - 資産が存在するクラウドリージョン。 • **VPC** AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。「virtual private cloud (仮想プライベートクラウド)」の略です。 • **アカウント ID** - スキャンで結果が検出された資産に割り当てられている一意の識別子。 • **リソース名** - 資産の識別子。 • **タイプ** - プラグインデータによって決定される、影響を受けている資産のタイプ。 • **IaC リソースタイプ** - 資産のインフラのコード化 (IAC) リソースタイプ。 • **リソースタイプ** - プラグインデータによって決定される、影響を受けているリソースのタイプ。 • **ドリフトあり** - 資産にドリフトがあるかどうかを示します。詳細については、*Tenable Cloud Security ユーザーガイド*のドリフト分析の設定を参照してください。 • **マッピング済み** - 資産がマッピングされているかを示します。詳細については、*Tenable Cloud Security ユーザーガイド*のクラウドスキャンワークフローを参照してください。 • **リアル** - 影響を受けている資産がクラウド環境に存在するかどうかを示します。

	• **クラウドプロバイダー** - リソースをホストしているクラウドプロバイダーの名前。
	• **リソース ID** - リソースのリソース ID。
	• **リソース名** - スキャナーにより脆弱性が検出された資産の名前。Tenable Vulnerability Management はこの識別子に、特定の資産属性が存在するかに応じて、次の優先順位に基づいて資産属性を割り当てます。
	  • エージェント名 (エージェントスキャンの場合)
	  • NetBIOS 名
	  • FQDN
	  • IPv6 アドレス
	  • IPv4 アドレス
	  たとえばスキャンによって、ある資産の NetBIOS 名と IPv4 アドレスが特定された場合、リソース名として NetBIOS 名が表示されます。
	• **ARN** - AWS にある資産の一意の Amazon リソース名。
	• **リソースの重要度** - 直近のスキャンに基づく、コンテナのセキュリティによる資産の重大度評価

追加情報	ポリシーがスキャン中に検出した脆弱性の数。
資産スキャン情報	脆弱性を検出したスキャンに関する情報。次の情報が含まれます。 • **初回確認日** - スキャンが資産上で初めて脆弱性を検出した日付。 • **最終確認日** - スキャンが資産上で脆弱性を検出した直近の日付。 • **最終ライセンススキャン日** - 資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャン

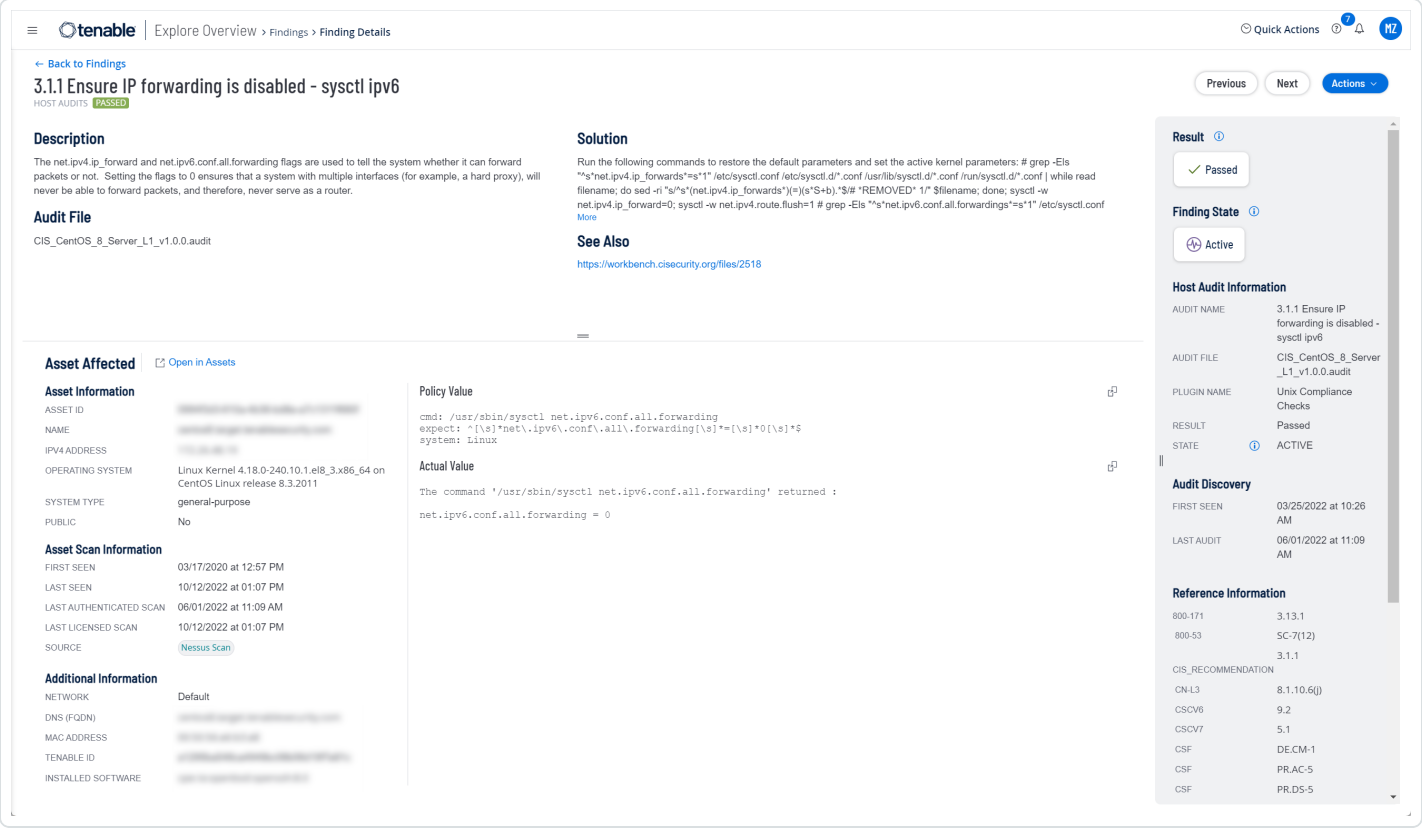
	では、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。 • **最終認証スキャン日** - 資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。 • **ソース** - 影響を受けている資産の脆弱性を検出したスキャンのソース。
タグ	影響を受けている資産に割り当てられたタグ。
クラウド設定ミスの情報	脆弱性の検出結果に関する情報。次の情報が含まれます。 • **検出結果 ID** - 個別の検出結果の一意の ID。検出結果の **[検出結果の詳細]** ページにアクセスしてページの URL を確認すると、検出結果の ID を表示できます。検出結果 ID は、*詳細と資産* の間にあるパスに表示される英数字のテキストです。 • **プロジェクト** - 検出結果と影響を受けている資産に関連付けられたクラウドプロジェクト。 • **ポリシーグループ ID** - 検出結果に関連するポリシーグループ ID のタイプ。 • **ポリシー ID** - 影響を受けている資産に関連付けられているクラウドポリシーの一意の ID。 • **ルール ID** - 検出結果に関連するルール ID。 • **環境 ID** - 検出結果に関連する環境 ID。 • **深刻度** - 脆弱性に関する CVSS ベースの深刻度を示す説明アイコン。詳細は、CVSS と VPR を参照してください。 • **結果** - 検出結果。 • **ベンチマーク** - 検出結果に関連するベンチマーク。

	• **ポリシーカテゴリ** - 検出結果に関連するポリシーカテゴリ。 • **IaC タイプ** - 資産のインフラのコード化 (IAC) リソースタイプ。 • **管理者** - 影響を受けている資産を管理する個人、グループ、または会社の名前。 • **ポリシータイプ** - 検出結果に関連するクラウドポリシーのタイプ。 • **ルール参照 ID** - スキャナーが違反を検出したセキュリティルールの参照 ID。 • **バージョン** - 検出結果に関連するバージョン。 • **IAC に存在** - 影響を受けている資産がインフラのコード化 (IaC) で作成されたかどうかを示します。 • **クラウドに存在** - 影響を受けている資産がクラウド環境に存在するかどうかを示します。 • **無視** – 検出結果の深刻度を判断するときに、Tenable Cloud Security がポリシー違反を無視したかどうかを示します。
クラウド設定ミスの検出	Tenable Vulnerability Management が脆弱性を最初に検出した時に関する情報。次の情報が含まれます。 • **初回確認日** - Tenable Vulnerability Management が影響を受けている資産を最初にスキャンした日付 • **最終確認日** - 影響を受けている資産を Tenable Vulnerability Management が最後にスキャンした日付
アクション	右上の **[アクション]** ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **レポートを生成** - レポートで説明されているように、テンプレートからレポートを生成します。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。

ホスト監査の詳細

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

検出結果の詳細の表示 を行う際の **[検出結果の詳細]** ページは、検出結果タイプによって異なります。ホスト監査の検出結果の場合、ホスト監査の検出結果の説明、推奨されるソリューション、対応する資産のサマリーが含まれます。



ホスト資産の **[検出結果の詳細]** ページには、次のセクションがあります。

注意: Tenable Vulnerability Management は空のセクションを非表示にするため、これらのセクションは表示されない場合があります。

セクション	説明
説明	コンプライアンスチェック中に検出結果を識別したプラグインの概要です。
ソリューション	コンプライアンスチェックの結果に対処する方法の概要です。

監査ファイル	スキャナーがコンプライアンスチェックの実行に使用した監査ファイルの名前です。
その他の関連項目	コンプライアンスチェックに関する役立つ情報を含む外部ウェブサイトへのリンクです。
資産情報	影響を受けている資産に関する情報で、次のものが含まれます。 • **資産 ID** - スキャンで脆弱性が検出された資産の UUID。 • **名前** - スキャナーがコンプラインスチェックを実行した資産の名前。 • **オペレーティングシステム** - 影響を受けている資産にインストールされているとスキャンによって識別されたオペレーティングシステム。 • **IPv4 アドレス** - 影響を受けている資産の IPv4 アドレス。 • **システムタイプ** - 影響を受けている資産が実行されているシステムのタイプ。 • **パブリック** - 資産がパブリックネットワークで使用可能かどうかを指定します。パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Management クエリ名前空間の `is_public` 属性によって識別されます。
資産スキャン情報	脆弱性を検出したスキャンに関する情報。次の情報が含まれます。 • **初回確認日** - スキャンが資産上で初めて脆弱性を検出した日付。 • **最終確認日** - スキャンが資産上で脆弱性を検出した直近の日付。 • **最終認証スキャン日** - 資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。 • **最終ライセンススキャン日** - 資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してくださ

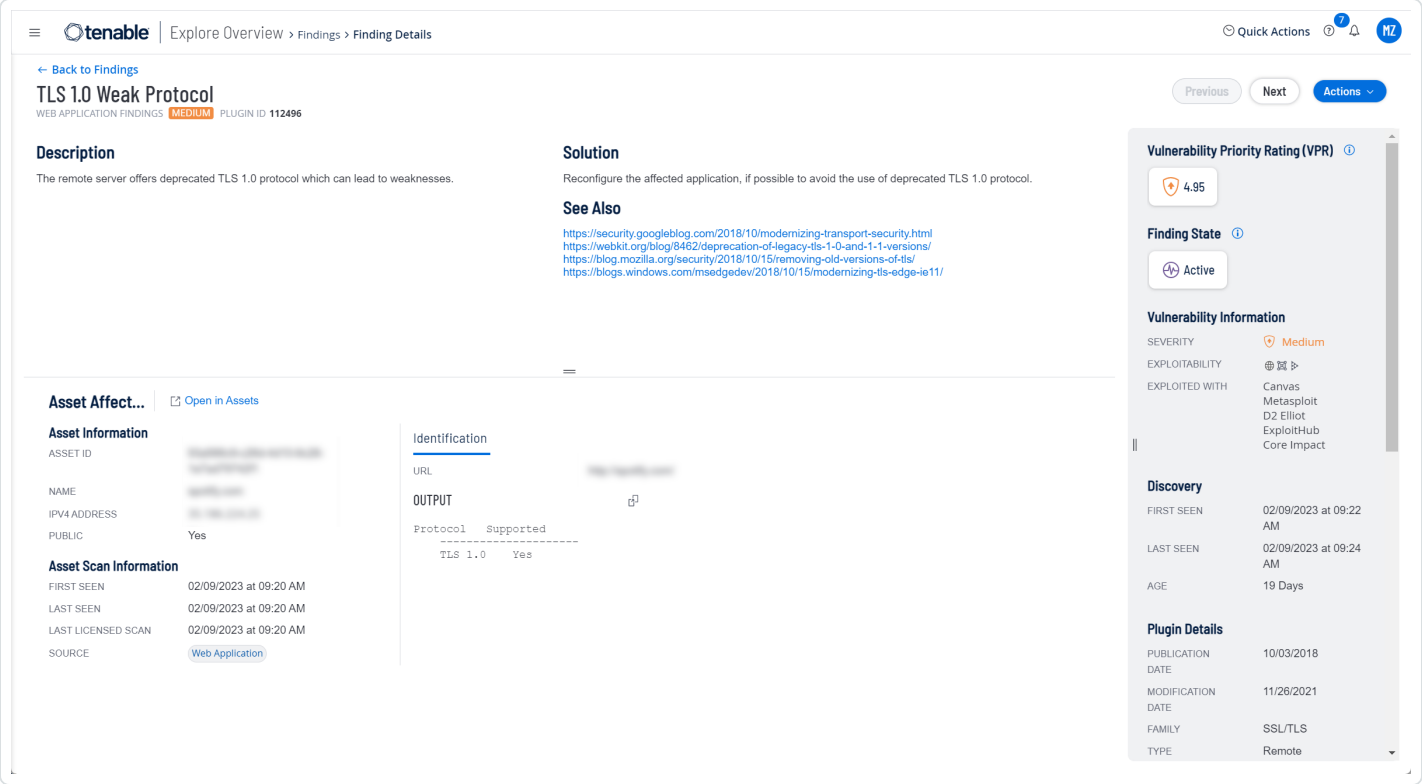
	い。 • **ソース** - 影響を受けている資産の脆弱性を検出したスキャンのソース。
追加情報	影響を受けている資産に関する追加情報で、次のものが含まれます。 • **ネットワーク** - 結果を検出したスキャナーに関連付けられたネットワークオブジェクトの名前。デフォルトのネットワーク名は **[Default]** です。詳細は、ネットワークを参照してください。 • **ネットワーク (FQDN)** - 検出結果で特定された脆弱性が見つかったホストの完全修飾ドメイン名。 • **MAC アドレス** - 影響を受けている資産の静的メディアアクセス制御 (MAC) アドレス。 • **Tenable ID** - 影響を受けている資産に関連付けられている Tenable アカウントの一意の識別子。 • **インストール済みソフトウェア** - 影響を受けている資産でスキャンによって識別されたソフトウェア。
ポリシー値	影響を受けている資産が監査ポリシーに準拠しているかどうかの結果に表示されるプラグイン出力です。
実際の値	検出結果に実際に表示されるプラグイン出力です。
ホスト監査情報	コンプライアンスチェックに関する情報で、次のものが含まれます。 • **監査名** - 影響を受けている資産に対してスキャナーが実行したコンプライアンスチェックの名前。 • **監査ファイル** - スキャナーがコンプライアンスチェックの実行に使用した監査ファイルの名前。 • **プラグイン名** - コンプライアンスチェックを識別したプラグインの名前。 • **結果** - 設定監査の各項目の結果です。結果は **[合格]**、**[警告]**、**[不合格]** のいずれかです。 • **状態** - 影響を受けている資産に対して監査結果が現在アクティブであるかどうか

	の表示。状態は、**[アクティブ]**、**[修正済み]**、**[再表面化]** のいずれかです。
監査検出	• **最初の監査** - スキャンによって資産のコンプライアンスチェックが最初に実行された日時。 • **最後の監査** - スキャンによって資産のコンプライアンスチェックが最後に実行された日時。
参照情報	コンプライアンスチェックに関する追加情報を提供する業界リソースのリストです。
アクション	右上の **[アクション]** ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **レポートを生成** - レポートで説明されているように、テンプレートからレポートを生成します。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。 • **すべての詳細を表示** – 検出結果の詳細の表示で説明されているように、検出結果の詳細をすべて表示します。 • **新しいタブですべての詳細を表示** – 資産の完全な詳細をブラウザの新しいタブに表示します。

ウェブアプリケーションの検出結果の詳細

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

検出結果の詳細の表示 を行う際の **[検出結果の詳細]** ページは、検出結果タイプによって異なります。ウェブアプリケーションの検出結果の場合、説明、推奨されるソリューション、影響を受けている資産の詳細が含まれます。



ウェブアプリケーションの検出結果の **[検出結果の詳細]** ページには、次のセクションがあります。

注意: Tenable Vulnerability Management は空のセクションを非表示にするため、これらのセクションは表示されない場合があります。

セクション	説明
説明	検出結果で検出された脆弱性を特定した Tenable プラグインの説明です。
ソリューション	検出結果で検出された脆弱性を修正する方法に関する概要です。このセクションは、公式のソリューションが使用可能な場合にのみ表示されます。

その他の関連項目	検出結果で検出された脆弱性についての役立つ情報を含む外部ウェブサイトへのリンクです。
資産情報	影響を受けている資産に関する情報で、次のものが含まれます。 • **資産 ID** - スキャンで脆弱性が検出された資産の UUID。この値は Tenable Vulnerability Management に対して一意です。 • **Name** - 影響を受けている資産の名前。名前のリンクをクリックすると、影響を受けている資産の詳細がウェブアプリケーションの詳細ページに表示されます。 • **IPV4 アドレス** - 資産の IPv4 アドレス • **パブリック** - 資産がパブリックであるかどうかを示します。
資産スキャン情報	脆弱性を検出したスキャンに関する情報。次の情報が含まれます。 • **初回確認日** - スキャンが最初に資産を特定した日時。 • **最終確認日** - スキャンの際に資産が最後に確認された日時。 • **最終ライセンススキャン日** - 資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。 • **最終認証スキャン日** - 資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。 • **ソース** - 影響を受けている資産の脆弱性を検出したスキャンのソース。
識別	検出結果で検出された脆弱性のプラグインの識別方法に関する情報で、次のものが含まれます。 • **URL** - スキャナーによって脆弱性が検出された対象 URL

	• **Proof** - 影響を受けている資産で脆弱性が悪用されることを証明する脆弱性を検証しようとするスキャナーからの出力 • **Input Type** - 攻撃者が悪意のあるコード (フォームやセッション Cookie など) を挿入する可能性のある資産のコンポーネントこのセクションは、資産がインジェクション攻撃に対して脆弱である場合にのみ表示されます。 • **Input Name** - 攻撃者が悪意のあるコードを挿入する可能性のある資産コンポーネントの名前このセクションは、資産がインジェクション攻撃に対して脆弱である場合にのみ表示されます。 • **Output** - スキャン中に検出された脆弱性に関するプラグインからのより詳細な情報
HTTP 情報	スキャナーとウェブアプリケーション間の HTTP メッセージに関する情報で、次のものが含まれます。 • **HTTP リクエスト** - 脆弱性を特定したスキャナーがウェブアプリケーションに対して行った HTTP 要求。 • **HTTP 応答** - 脆弱性を特定したスキャナーにウェブアプリケーションが送信した HTTP 応答
添付ファイル	検出結果で検出された脆弱性に関する詳細を含むプラグインの添付ファイルです。このセクションは、添付ファイルが使用可能な場合にのみ表示されます。
Vulnerability Priority Rating (VPR)	Tenable によって計算された脆弱性の Vulnerability Priority Rating です。
検出結果の状態	検出結果で検出された脆弱性の状態。詳細は、脆弱性の状態 を参照してください。
脆弱性の情報	プラグインが特定した脆弱性に関する情報です。次のものが含まれます。 • **深刻度** - 脆弱性の深刻度を示すアイコン。 • **悪用される可能性** - 脆弱性の潜在的な悪用可能性において考慮される、脆弱性の特性 • **悪用される** - 脆弱性が悪用される可能性のある特に一般的な方法。

検出	Tenable Vulnerability Management が検出結果で検出された脆弱性を最初に検出した時に関する情報。次のものが含まれます。 • **初回確認日** - スキャンが資産上で初めて脆弱性を検出した日付。 • **最終確認日** - スキャンが資産上で脆弱性を検出した直近の日付。 • **経過日数** - ネットワーク内の資産上で、スキャンによってその脆弱性が最初に検出されてから経過した日数。
プラグインの詳細	検出結果で検出された脆弱性を検出したプラグインに関する情報で、次のものが含まれます。 • **公開日** - 脆弱性を特定した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。 • **ファミリー** - 脆弱性を特定したプラグインのファミリー。 • **リスクファクター** - プラグインに関連する CVSS に基づくリスク要因 • **プラグイン ID** - 脆弱性を特定したプラグインの ID。
リスク情報	影響を受けている資産に脆弱性が与える相対リスクに関する情報で、次のものが含まれます。 • **リスクファクター** - プラグインに関連する CVSS に基づくリスク要因。 • **CVSSV3 基本スコア** - CVSSv3 基本スコア(時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。 • **CVSSV3 手法** - 脆弱性に関する追加の CVSSv3 メトリクス。 • **CVSSV2 ベーススコア** - CVSSv2 ベーススコア(時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。 • **CVSS2 攻撃元区分** - 脆弱性に関する追加の CVSSv2 メトリクス。
参照情報	Tenable Vulnerability Management によって検出結果で検出された脆弱性に関する追加情報を提供する業界リソースには、次のようなものが含まれます。 • **OWASP** - 脆弱性の存在について OWASP (Open Web Application Security Project) が提供するトップ 10 リストへの 1 つまたは複数のリンク

	• **OWASP API** - 脆弱性の存在に関する OWASP API トップ 10 リストへの 1 つまたは複数のリンク • **WASC** - 脆弱性の脅威分類に関して WASC (Web Application Security Consortium) が提供する説明へのリンク • **CWE** - 脆弱性の CWE スコアが分かる共通脆弱性タイプ一覧 (CWE: Common Weakness Enumeration) の説明へのリンク
アクション	右上の **[アクション]** ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **レポートを生成** - レポートで説明されているように、テンプレートからレポートを生成します。 • **変更** – 検出結果の変更ルールまたは許容ルールの追加で説明されているように、検出結果の深刻度を変更または承認します。 • **変更** – 検出結果の変更ルールまたは許容ルールの追加で説明されているように、検出結果の深刻度を変更または承認します。 • **すべての検出結果を表示** – 資産の詳細の表示で説明されているように、資産のすべての検出結果を表示します。 • **すべての詳細を表示** – 検出結果の詳細の表示で説明されているように、検出結果の詳細をすべて表示します。 • **新しいタブですべての詳細を表示** – 資産の完全な詳細をブラウザの新しいタブに表示します。

検出結果フィルター

[検出結果] ページでは、次の検出結果タイプに関する分析のフィルタリングと表示が可能です。

- **脆弱性**
- **クラウドの検出結果**
- **ホスト監査の結果**
- **ウェブアプリケーションの脆弱性**

よく使用するフィルターのセットを保存済みフィルターとして保存し、後でアクセスしたり、チームの他のメンバーと共有したりできます。

注意: パフォーマンスを最適化するために、Tenable では、**[調査]** > **[検出結果]** ビューまたは **[資産]** ビュー (**[グループ化基準]** 表を含む) に適用できるフィルターの数を 18 個に制限しています。

注意: Tenable Vulnerability Management が複数のスキャンで同じ検出結果を識別する場合、最新の結果のみを保存します。たとえば、エージェントスキャンがある検出結果を識別し、その後 Tenable Nessus スキャンが同じ検出結果を識別した場合、その検出結果は Tenable Nessus スキャンに関連付けられます。**[ソース]** などのフィルターを使って既知の結果を見つけられない場合は、その結果を直接検索してください。

脆弱性フィルター

オプション	説明
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
資産名	スキャンで脆弱性が検出された資産の名前です。この値は Tenable Vulnerability Management に対して一意です。このフィルターでは大文字と小文字が区別されますが、ワイルドカード文字を使用してこれをオフにできます。
資産タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。

	詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。
Bugtraq ID	脆弱性を特定したプラグインの Bugtraq ID。
Canvas Exploit	脆弱性を含む CANVAS エクスプロイトパックの名前です。
CERT Advisory ID	脆弱性に関する CERT アドバイザリの ID です。
CERT Vulnerability ID	CERT Vulnerability Notes Database における脆弱性の ID です。
CISA KEV 対処期限日	Binding Operational Directive 22-01 に基づく、Cybersecurity and Infrastructure Security Agency (CISA) の Known Exploitable Vulnerability (KEV) 修正の期日。プラグインに関連付けられている KEV の最も早い対処期限日で検索されます。詳細は、既知の悪用された脆弱性カタログを参照してください。
CORE エクスプロイトフレームワーク	脆弱性向けのエクスプロイトが、CORE Impact フレームワークに存在するかどうかを示します。
CPE	プラグインが特定する脆弱性の共通プラットフォーム一覧 (CPE) 番号。 (200 の値制限)。
CVE	プラグインが特定する脆弱性の共通脆弱性識別子 (CVE) ID。 (200 の値制限)。
CVSSv2 基本値	CVSSv2 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。
CVSSv2 Temporal Score	CVSSv2 現状値 (時間の経過とともに変化するがユーザー環境間では変化しない、脆弱性の特性です。)
CVSSv2 Temporal Vector	脆弱性の CVSSv2 現状のメトリクスです。
CVSSv2 攻撃元区	脆弱性に対する、加工していない CVSSv2 メトリクス。詳細は、CVSSv2 の

分	ドキュメントを参照してください。
CVSSv3 基本値	CVSSv3 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。
CVSSv3 Temporal Score	CVSSv3 現状値 (時間の経過とともに変化するがユーザー環境間では変化しない、脆弱性の特性)です。
CVSSv3 Temporal Vector	脆弱性の CVSSv3 現状のメトリクスです。
CVSSv3 攻撃元区分	脆弱性に関する、その他の CVSSv3 メトリクス。
CWE	脆弱性の共通脆弱性タイプ一覧 (CWE)。
Default/Known Account	その脆弱性を特定したプラグインが、デフォルトのアカウントをチェックするかどうかを示します。
Elliot Exploit	D2 Elliot Web Exploitation フレームワークにある、その脆弱性向けのエクスプロイトの名前です。
Exploit Database ID	Exploit Database における脆弱性の ID です。
悪用の容易さ	脆弱性の悪用がどの程度容易かに関する説明。
マルウェアによる悪用	脆弱性がマルウェアによって悪用されたことが知られているかどうかを示します。
Exploited By Nessus	特定プロセスで Tenable Nessus がその脆弱性をエクスプロイトしたかどうかを示します。
Exploit Hub	その脆弱性向けのエクスプロイトが、ExploitHub フレームワークに存在するかどうかを示します。
検出結果 ID	個別の検出結果の一意の ID です。 **注意:** 検出結果の **[検出結果の詳細]** ページにアクセスしてページの URL を確認すると、検出結果の ID を表示できます。検出結果 ID は、*詳細*と*資産*の間にあるパスに表示される英数字のテキストです。

初回確認日	スキャンが資産上で初めて脆弱性を検出した日付。
IAVA ID	脆弱性の情報保証脆弱性アラート (IAVA) の ID です。
IAVB ID	脆弱性の情報保証脆弱性速報 (IAVB) の ID です。
IAVM Severity	Information Assurance Vulnerability Management (IAVM) での脆弱性の深刻度です。
IAVT ID	脆弱性の情報保証脆弱性技術速報 (IAVT) の ID です。
In The News	このプラグインが、メディア (たとえば ShellShock や Meltdown) の注目を受けたかどうかを示します。
IPv4 アドレス	影響を受けている資産の IPv4 アドレス。このフィルターには最大 256 個の IP アドレスを追加できます。
IPv6 アドレス	影響を受けている資産の IPv6 アドレス。
最終修正日	以前に検出された脆弱性が最後にスキャンされ、資産にもう存在しないと記録された時間。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
マルウェア	その脆弱性を特定したプラグインが、マルウェアをチェックするかどうかを示します。
Metasploit Exploit	Metasploit フレームワークにある、関連するエクスプロイトの名前です。
Microsoft 掲示板	脆弱性を特定したプラグインがカバーする、Microsoft のセキュリティ速報。
元の深刻度	スキャンが検出結果を最初に検出した際の脆弱性の CVSS ベースの深刻度。詳細は、CVSS と VPR を参照してください。
OSVDB ID	Open Sourced Vulnerability Database (OSVDB) における脆弱性の ID です。
パッチ公開済み	ベンダーがその脆弱性に対してのパッチを公開した日付。
プラグインの説明	脆弱性を特定した Tenable プラグインの説明。
プラグインファミリー	脆弱性を特定したプラグインのファミリー。 (200 の値制限)。

プラグイン ID	脆弱性を特定したプラグインの ID。 (200 の値制限)。
プラグイン変更日	脆弱性を特定したプラグインが最後に変更された日付。
プラグイン名	脆弱性を特定したプラグインの名前。

プラグイン出力	このフィルターを使用して、指定したプラグイン出力のある検出結果を返します。フィルターの使用で説明されているように、値を含む、または含まないプラグイン出力を検索できます。
	
	たとえば、「Kernel」という語を含むプラグイン出力を検索するには、詳細モードで次のように入力します。
	
	`Plugin Output contains Kernel`
	
	注意:[設定]>[全般検索]>[プラグイン出力検索を有効にする]で、このフィルターを手動で有効にしてください。このフィルターは、35 日間使用しないと再び無効になります。
	
	プラグイン出力検索のベストプラクティス
	
	プラグイン出力は大きくなることがあり、検索範囲が広すぎると、**[検出結果]**ワークベンチがフリーズする可能性があります。最良の結果を得るために、**[プラグイン出力]**フィルターと**[プラグイン ID]**フィルターを使用して結果を絞り込んでください。同時に検索するプラグイン ID の数を制限して、システムのタイムアウトを回避します。
	
	プラグイン ID を指定して、特定のプラグインを検索するか、除外します。こうしたアプローチは、別のユースケースにも当てはまります。たとえば、オペレーティングシステムごとのソフトウェアリストを検索するときには、プラグインを含めます。上位プラグインに何度も表示されるプラグインは、探索的検索から除外します。
	
	• **1 つのプラグインの出力を検索する場合**
	
	`Plugin Output contains Kernel AND Plugin ID is equal to 110483`

	• **複数のプラグインの出力を検索する場合**
	`Plugin Output contains Chrome AND Plugin ID is equal to 45590, 10456`
	• **リストしたプラグインを除外したプラグインの出力を検索する場合**
	`Plugin Output contains Chrome AND Plugin ID is not equal to 45590, 10456`

公開されたプラグイン	脆弱性を特定したプラグインが公開された日付です。
プラグインタイプ	プラグインチェックの一般的なタイプです。可能なオプションは次のとおりです。 • **Local** • **リモート** • **Local & Remote**
ポート	スキャンで脆弱性が検出された資産への接続に、スキャナーが使用したポートの情報です。 (200 の値制限)。
プロトコル	スキャンで脆弱性が検出された資産との通信で、スキャナーが使用したプロトコルです。
修正されたリスク	脆弱性の深刻度に適用されるリスクの変更。可能なオプションは次のとおりです。 • **変更済** • **許容済み** • **なし** 詳細は、変更ルールと許容ルールを参照してください。
検出元	検出結果を検出したスキャナー。
Secunia ID	脆弱性に関する Secunia Explore アドバイザリの ID です。

その他の関連項目	脆弱性についての役立つ情報を含む、外部ウェブサイトへのリンクです。
深刻度	CVSS に基づく脆弱性の深刻度。詳細は、CVSS と VPR を参照してください。 このフィルターは、デフォルトで **[重大]**、**[高]**、**[中]**、**[低]** が選択された状態でフィルタープレーンに表示されます。
ソリューション	脆弱性を修正する方法に関する概要。
ソース	資産を特定したスキャンのソース。可能な値は次のとおりです。 • エージェント (Tenable Nessus Agent) • Nessus (Tenable Nessus スキャン) • PVS/NNM (Tenable Nessus Network Monitor) • WAS (Tenable Web App Scanning) • AWS コネクタ • Azure コネクタ • GCP コネクタ • Qualys コネクタ
状態	脆弱性の状態。デフォルトでは、**アクティブ**、**再表面化**、**新規** が選択された状態でフィルタープレーンに表示されます。詳細は、脆弱性の状態を参照してください。
Stig の深刻度	検出結果に関連する STIG の深刻度。
概要	プラグインまたは脆弱性の概略の説明。
ターゲットグループ	脆弱性を特定したスキャンに関連するターゲットグループ詳細は、ターゲットグループを参照してください。
修正にかかった時間	スキャンで特定された脆弱性の修正に所属組織がかけた時間 (時間数または日数) です。修正済みの脆弱性に関してのみ表示されます。より正確な結果を得るには、このフィルターと、**[修正済み]** に設定した **[状態]** フィルターを併用します。

ベンダー非対応	このプラグインにより検出されたソフトウェアが、ソフトウェアベンダーにサポートされていません (たとえば、Windows 95 や Firefox 3)
VPR	Tenable によって計算された脆弱性の Vulnerability Priority Rating。
公開された脆弱性	脆弱性の定義が最初に公開された日付 (たとえば、CVE が公開された日付)。

クラウド

クラウドの設定ミスのフィルター

オプション	説明	
フィルター		
アカウント ID	スキャンで結果が検出された資産をホストするクラウドサービスの資産リソースに割り当てられた一意の識別子。	
ARN	スキャンで結果が検出された資産の Amazon リソース名 (ARN)。	
資産 ID	スキャンで結果が検出された資産の UUID。この値は Tenable Vulnerability Management に対して一意です。	
ベンチマーク	検出結果に関連付けられているベンチマーク。	
クラスター	検出結果に関連するクラスター。	
作成時刻	スキャンで検出結果が検出された資産レコードを Tenable Vulnerability Management が作成した日時。	
重大度	脆弱性の検出結果の重大度。	
クラウドに存在	影響を受けているクラウドリソースがクラウド環境に存在するかどうかを示します。	
IAC に	影響を受けている資産がインフラのコード化 (Infrastructure as Code: IaC) で作	

存在	成されたかどうかを示します。	
検出結果 ID	個別の検出結果の一意の ID です。 **注意:** 検出結果の**[検出結果の詳細]**ページにアクセスしてページの URL を確認すると、検出結果の ID を表示できます。検出結果 ID は、*詳細と資産*の間にあるパスに表示される英数字のテキストです。	
初回確認日	Tenable Vulnerability Management が影響を受けている資産を最初にスキャンした日付。	
TF 状態で発見	検出結果が TF 状態で発見されたかどうかを示します。	
初回確認日	Tenable Vulnerability Management が影響を受けている資産を最初にスキャンした日付。	
IaC リソースタイプ	資産のインフラのコード化 (IAC) リソースタイプ。	
IaC タイプ	資産のインフラのコード化 (IAC) タイプ。	
無視	検出結果の深刻度を計算するときに、Tenable Vulnerability Management がポリシー違反を無視したかどうかを示します。	
不変のドリフト	資産に不変のドリフトがあるかどうかを示します。詳細については、*Tenable Cloud Security ユーザーガイド*のドリフト分析の設定を参照してください。	
属性	資産が属性であるかどうかを指定します。	
最終修正日	検出結果が最後に修正された日付。	
最終スキャン時間	検出結果に対してスキャンが最後に実行された日付。	
最終確	Tenable Vulnerability Management が影響を受けている資産を最後にスキャン	

認日	した日付。	
管理者	影響を受けている資産を管理する個人、グループ、または会社の名前。	
ポリシーカテゴリ	検出結果に関連するポリシーカテゴリ。	
ポリシーID	影響を受けている資産に関連付けられているクラウドポリシーの一意の ID。	
ポリシー名	影響を受けている資産に関連付けられているクラウドポリシーの一意の ID。	
ポリシーの種類	影響を受けている資産に関連付けられているクラウドポリシーの一意の ID。	
プロジェクト	検出結果に関連するプロジェクト。	
プロバイダー	検出結果に関連するサードパーティプロバイダー。	
リージョン	影響を受けている資産が実行されるクラウドリージョン。	
リポジトリ	影響を受けている資産に関連付けられているコードリポジトリ。	
リソースカテゴリ	影響を受けている資産をホストするクラウドサービスの資産リソースのカテゴリ。	
リソースID	影響を受けている資産をホストするクラウドサービスの資産リソースの ID。	
リソース名	影響を受けている資産をホストするクラウドサービスの資産リソースの名前。	
リソースタイプ	影響を受けている資産をホストするクラウドサービスの資産リソースのタイプ。	
結果	スキャンの結果です。可能なオプションは次のとおりです。	

	• **Failed** • **Passed** • **不明**	
ルール ID	スキャナーが違反を検出したセキュリティルールの一意の ID です。	
ルール参照 ID	スキャナーが違反を検出したセキュリティルールの参照 ID。	
深刻度	CVSS に基づく脆弱性の深刻度。詳細は、CVSS と VPR を参照してください。 このフィルターは、デフォルトで **[重大]**、**[高]**、**[中]**、**[低]** が選択された状態でフィルタープレーンに表示されます。	
ソース行	検出結果に関連するソース行。	
更新時間	資産レコードが最後に更新された日時。	
バージョン	検出結果に関連するバージョン。	
VPC	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、Amazon Virtual Private Cloud ユーザーガイドを参照してください。	

ホスト監査フィルター

オプション	説明
フィルター	
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
資産名	スキャナーが監査チェックを実行した資産の名前です。この値は Tenable Vulnerability Management に対して一意です。
資産タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロ

	ン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。
監査ファイル	スキャナーが監査の実行に使用した監査ファイルの名前です。監査ファイルは、特定の設定、ファイルアクセス許可、実行するアクセス制御テストが含まれている、XML ベースのテキストファイルです。
監査チェック名	Tenable が監査に割り当てた名前です。場合によっては、コンプライアンスコントロールが名前のプレフィックスとしてリストされることがあります。
コントロール ID	結果を、特定のベンチマーク推奨事項を満たす他の結果と関連付けることができる ID。このフィルターを使用して、監査ポータルでチェックを特定できます。
初回監査日	資産に対して監査チェックが初めて実行された日付を示します。
FQDN	資産の完全修飾ドメイン名 (FQDN)。
IPv4 アドレス	影響を受けている資産の IPv4 アドレス。このフィルターには最大 256 個の IP アドレスを追加できます。
IPv6 アドレス	影響を受けている資産の IPv6 アドレス。
最終監査日	資産に対して実行された最新の監査チェックの日付を示します。
最終修正日	検出結果が最後に修正された日付。
最終確認日	スキャンで最後に調査結果が確認された日付。
元の結	初回監査の結果。

果	
プラグイン ID	監査チェックの実行に使用された Nessus プラグイン ID。
プラグイン名	監査チェックの実行に使用された Nessus プラグイン名。
プラグイン名	この監査検出結果を識別したプラグインの名前。
結果	監査チェックの現在の結果または修正後の結果です。
修正後の結果	ルールを作成して、監査チェックの結果を承認または修正できます。このフィルターを使用すると、修正後の結果をレポートできます。
深刻度	CVSS に基づく脆弱性の深刻度。詳細は、CVSS と VPR を参照してください。 このフィルターは、デフォルトで **[重大]**、**[高]**、**[中]**、**[低]** が選択された状態でフィルタープレーンに表示されます。
状態	検出結果で検出された脆弱性の状態。デフォルトでは、**アクティブ**、**再表面化**、**新規** が選択された状態でフィルタープレーンに表示されます。詳細は、脆弱性の状態を参照してください。

ウェブアプリケーションの脆弱性のフィルター

オプション	説明
資産 ID	スキャンで脆弱性が検出された資産の UUID。この値は Tenable Vulnerability Management に対して一意です。
資産名	スキャナーで脆弱性が検出された資産の名前。この値は Tenable Vulnerability Management に対して一意です。 このフィルターは、デフォルトでフィルタープレーンに表示されます。
Bugtraq ID	脆弱性を特定したプラグインの Bugtraq ID。
CPE	プラグインが特定する脆弱性の共通プラットフォーム一覧 (CPE) 番号。 (200 の値制限)。

CVE	プラグインが特定する脆弱性の共通脆弱性識別子 (CVE) ID。 (200 の値制限)。
CVSSv2 基本値	CVSSv2 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。
CVSSv2 攻撃元区分	脆弱性に対する、加工していない CVSSv2 メトリクス。詳細は、CVSSv2 のドキュメントを参照してください。
CVSSv3 基本値	CVSSv3 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。
CVSSv3 攻撃元区分	脆弱性に関する、その他の CVSSv3 メトリクス。
CWE	脆弱性の共通脆弱性タイプ一覧 (CWE)。
初回確認日	スキャンが資産上で初めて脆弱性を検出した日付。
入力名	脆弱性によって悪用される特定のウェブアプリケーションコンポーネントの名前。
入力タイプ	脆弱性によって悪用されるウェブアプリケーションコンポーネントのタイプ (フォーム、Cookie、ヘッダーなど)。
IPv4 アドレス	影響を受けている資産の IPv4 アドレス。このフィルターには最大 256 個の IP アドレスを追加できます。
最終修正日	検出結果が最後に修正された日付。
最終確認日	スキャンで最後に調査結果が確認された日付。
元の深刻度	スキャンが検出結果を最初に検出した際の脆弱性の CVSS ベースの深刻度。詳細は、CVSS と VPR を参照してください。
OWASP 2010	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2010 年のカテゴリ。

OWASP 2013	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2013 年のカテゴリ。
OWASP 2017	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2017 年のカテゴリ。
OWASP 2021	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2021 年のカテゴリ。
OWASP API 2019	プラグインが対象としている脆弱性の Open Web Application Security Project (OWASP) 2019 年のカテゴリ。可能なオプションは次のとおりです。 • **API1:2019 破られたオブジェクトレベルの承認** • **API2:2019 破られたユーザー認証** • **API3:2019 過剰なデータ漏洩** • **API4:2019 リソースとレート制限の不足** • **API5:2019 破られた関数レベルの承認** • **API6:2019 一括割り当て** • **API7:2019 セキュリティの不適切な設定** • **API8:2019 インジェクション** • **API9:2019 不適切な資産管理** • **API10:2019 不十分なロギングとモニタリング**
プラグインの説明	脆弱性を特定した Tenable プラグインの説明。
プラグインファミリー	脆弱性を特定したプラグインのファミリー。 (200 の値制限)。
プラグイン ID	脆弱性を特定したプラグインの ID。 (200 の値制限)。
プラグイン変	プラグインが最後に変更された日付。

更日	
プラグイン名	この監査検出結果を識別したプラグインの名前。
公開されたプラグイン	脆弱性を特定したプラグインが公開された日付です。
修正されたリスク	脆弱性の深刻度に適用されるリスクの変更。可能なオプションは次のとおりです。 • **変更** • **許容済み** • **なし** 詳細は、変更ルールと許容ルールを参照してください。
その他の関連項目	脆弱性についての役立つ情報を含む、外部ウェブサイトへのリンクです。
深刻度	CVSS スコアベースの深刻度詳細については、Tenable Vulnerability Management ユーザーガイドの CVSS スコアと VPR を参照してください。 このフィルターは、デフォルトで **[重大]**、**[高]**、**[中]**、**[低]** が選択された状態でフィルタープレーンに表示されます。
ソリューション	脆弱性を修正する方法に関する概要。
状態	検出結果で検出された脆弱性の状態。デフォルトでは、**アクティブ**、**再表面化**、**新規** が選択された状態でフィルタープレーンに表示されます。詳細は、脆弱性の状態を参照してください。
Url	スキャナーで脆弱性が検出された完全な URL。 このフィルターは、デフォルトでフィルタープレーンに表示されます。
WASC	プラグインが対象とする脆弱性に関連付けられている Web Application Security Consortium (WASC) のカテゴリ。

検出結果のグループ化

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[検出結果] ワークベンチでは、検出結果を特定の属性でグループ化できます。ホスト脆弱性、クラウド設定ミス、ウェブアプリケーションの検出結果をグループ化できますが、ホスト監査検出結果はグループ化できません。

脆弱性の検出結果をグループ化する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[検出結果]** をクリックします。

   [検出結果] ページが表示され、検出結果を示す表が表示されます。**[脆弱性]** タブはデフォルトでアクティブになっています。

3. 次のいずれかを行います。

ホストの脆弱性の検出結果をグループ化する方法

a. 検出結果の表の上部の **[グループ化]** の横にある、次の属性のいずれかをクリックします。

- **資産** - スキャンで脆弱性が特定された資産の名前です。
- **プラグイン** - 脆弱性を特定したプラグインの名前です。

検出結果の表に、選択された属性でグループ化された検出結果が表示されます。

b. グループ化された検出結果に関する次の詳細を表示します。これらは、選択する属性によって異なります。

列	説明
資産	
資産名	スキャンで脆弱性が検出された資産の名前です。この値は Tenable Vulnerability Management に対して一意です。
資産タグ	影響を受けている資産の資産タグ。最初のタグにカーソルを

	合わせると、他のタグが表示されます。
最終確認日	スキャンが資産上でこの脆弱性を検出した直近の日時。
資産 IP	資産レコードに関連付けられた IPv4 または IPv6 アドレスです。
脆弱性	グループ化された検出結果の各セットについて、脆弱性の CVSS ベースの深刻度別の割合を示す説明画像。詳細は、CVSS と VPR を参照してください。
脆弱性カウント	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した脆弱性の数。
緊急	グループ化された検出結果の各セットにおいて、CVSS ベースの深刻度評価で緊急とされた脆弱性の数。詳細は、CVSS と VPR を参照してください。
高	グループ化された検出結果の各セットにおいて、CVSS ベースの深刻度評価で重要とされた脆弱性の数。詳細は、CVSS と VPR を参照してください。
プラグイン	
深刻度	グループ化された検出結果の各セットで特定された CVSS ベースの深刻度スコア詳細は、CVSS と VPR を参照してください。
名前	脆弱性を特定したプラグインの名前。
ファミリー	脆弱性を特定したプラグインのファミリー。
プラグイン ID	脆弱性を特定したプラグインの ID。
脆弱性カウント	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した脆弱性の数。

クラウド設定ミスに関する検出結果をグループ化する方法

a. 検出結果の表の上部の**[グループ化]**の横にある、次の属性のいずれかをクリックします。

- **ポリシー** - 影響を受けている資産に関連付けられているクラウドポリシーです。

  ポリシーグループ - 影響を受けている資産に関連付けられているクラウドポリシーの一意の ID。

- **リソースタイプ** - クラウドリソースタイプの名前 (リソースグループや仮想マシンなど)。

検出結果の表に、選択された属性でグループ化された検出結果が表示されます。

b. グループ化された検出結果に関する次の詳細を表示します。これらは、選択する属性によって異なります。

列	説明
ポリシー	
ポリシー名	影響を受けている資産に関連付けられているポリシーの名前です。
深刻度	CVSS に基づく脆弱性の深刻度詳細は、CVSS と VPR を参照してください。
ソース	ポリシーのソースです。可能な値は次のとおりです。 • クラウド • IaC (インフラのコード化)
最終確認日	スキャンで脆弱性が特定された最後の日付です。
影響を受けるリソースの数	脆弱性が影響を与えるクラウドリソースの数。
ポリシーグループ	
ポリシー ID	影響を受けている資産に関連付けられているクラウドポリシーの一意の ID。
深刻度	CVSS に基づく脆弱性の深刻度詳細は、CVSS と VPR を参照してください。

ポリシーグループ	影響を受けている資産を管理するセキュリティポリシーに関連付けられているグループ。
クラウドに存在	影響を受けているクラウドリソースがクラウド環境に存在するかどうかを示します。
IAC に存在	影響を受けている資産がインフラのコード化 (Infrastructure as Code: IaC) で作成されたかどうかを示します。
影響を受けるリソースの数	脆弱性が影響を与えるクラウドリソースの数。
設定ミスの数	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した設定ミスの数。
リソースタイプ	
リソースタイプ	グループ化された検出結果の各セットで特定された CVSS ベースの深刻度スコア詳細は、CVSS と VPR を参照してください。
影響を受けるリソースの数	脆弱性が影響を与えるクラウドリソースの数
不変のドリフトのカウント	影響を受けているリソースが稼働しているクラウド環境と、それをデプロイするために使用されたインフラのコード化 (Infrastructure as Code: IaC) との間の不一致の数。
設定ミスの数	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した設定ミスの数。

ウェブアプリケーションの検出結果をグループ化する方法

a. 検出結果の表の上部の **[グループ化]** の横にある、次の属性のいずれかをクリックします。

- **資産** - 影響を受けている資産に関連付けられているウェブアプリケーションの一意の名前。

- **プラグイン** - ウェブアプリケーションリソースタイプの ID (リソースグループや仮想マシンなど)。

ウェブアプリケーションの検出結果の表が表示され、選択した属性でグループ化された検出結果が表示されます。

b. グループ化された検出結果に関する次の詳細を表示します。これらは、選択する属性によって異なります。

列	説明
資産	
資産名	スキャンで脆弱性が検出された資産の名前。この値は Tenable Vulnerability Management に対して一意です。
脆弱性	グループ化された検出結果の各セットについて、脆弱性の CVSS ベースの深刻度別の割合を示す説明画像。詳細は、CVSS と VPR を参照してください。
緊急	グループ化された検出結果の各セットにおいて、CVSS ベースの深刻度評価で緊急とされた脆弱性の数。詳細は、CVSS と VPR を参照してください。
高	グループ化された検出結果の各セットにおいて、CVSS ベースの深刻度評価で重要とされた脆弱性の数。詳細は、CVSS と VPR を参照してください。
脆弱性カウント	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した脆弱性の数。
最終確認日	スキャンが資産上でこの脆弱性を検出した直近の日時。
アクション	グループ化された検出結果の各セットで実行できるアクション。
プラグイン	
深刻度	グループ化された検出結果の各セットで特定された CVSS

	ベースの深刻度スコア詳細は、CVSS と VPR を参照してください。
名前	脆弱性を特定したプラグインの名前。
ファミリー	脆弱性を特定したプラグインのファミリー。
CVSSv2 基本値	CVSSv2 基本値 (時間の経過やユーザー環境によらず一定である、本質的で基本的な脆弱性の特性)。 **注意:** 深刻度メトリクス設定に基づいて、このパラメーターは CVSSv3 ベーススコアを表示する可能性があります。詳細は、全般設定 を参照してください。
プラグイン ID	脆弱性を特定したプラグインの ID。
資産数	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した資産の数。
脆弱性カウント	グループ化された検出結果の各セットで Tenable Vulnerability Management が特定した脆弱性の数。
アクション	グループ化された検出結果の各セットで実行できるアクション。

検出結果の変更ルールまたは許容ルールの追加

Tenable Vulnerability Management では、脆弱性の検出結果に対するルールを作成して、リスクが表示される方法をカスタマイズできます。*変更*ルールは検出結果の深刻度を変更し、*許容*ルールは深刻度を変更せずにそのリスクを許容します。

ヒント: このトピックでは、**[検出結果]** ワークベンチからルールを作成する方法を説明しますが、Tenable Vulnerability Management **[設定]** からルールを作成することもできます。ルールを作成するべきケースなど、詳しい情報は、変更/許容ルールを参照してください。

注意: ルールが IP アドレスによって指定される場合、各ネットワーク上で見つかった指定の IP に対してそのルールが適用されます。詳細は、ネットワークを参照してください。

検出結果で変更ルールを作成する

[検出結果] ワークベンチから変更ルールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[検出結果]** をクリックします。

   [検出結果] ページが表示され、**[脆弱性]** タブがアクティブになり、検出結果がテーブルビューで表示されます。

3. (オプション) **[ウェブアプリケーションの検出]** をクリックします。

   [ウェブアプリケーションの検出] タブが表示されます。

4. ルールを作成する検出結果の行で ⋮ 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。

5. **[変更]** をクリックします。

   [ルールの追加] プレーンが表示されます。

6. **[ルール情報]** セクションで以下のオプションを設定します。

a. **脆弱性プラグイン ID** - 変更するプラグインの ID が事前選択されているものと異なる場合は、その ID を入力します(たとえば 51192)。

> **注意:** プラグイン ID が Tenable Nessus プラグインに対応する場合は、**元の深刻度**インジケーターが脆弱性のデフォルトの深刻度に一致するよう変更されます。

b. **新しい深刻度** - 脆弱性に関する適切な深刻度レベルを選択します。

c. **ターゲット** - **[すべて]** を選択してすべての資産をターゲットにするか、**[カスタム]** を選択してルールを実行するターゲットを指定します。

> **注意:** **[ターゲット]** ドロップダウンを **[すべて]** に設定した場合、このオプションにより既存のルールがオーバーライドされる可能性があることを知らせる警告が表示されます。

d. **ターゲットとなるホスト** - 必要に応じて、ルールの 1 つ以上のカスタムターゲットを入力します。IP アドレス、IP 範囲、CIDR、ホスト名の任意の組み合わせを含むコンマ区切りリストを入力できます。

> **注意**: 指定できるコンマ区切りカスタムエントリは 1000 個までとなっています。これよりも多くのカスタムエントリをターゲットにする場合は、複数のルールを作成してください。

e. (オプション) **有効期限日** - ルールが期限切れになる日付を選択します。

f. (オプション) **コメント** - ルールの説明を入力します。このオプションは、ルールが変更された場合にのみ表示されます。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management が既存の検出結果にルールを適用し始めます。システムの負荷と一致する検出結果の数によっては、このプロセスに時間がかかる場合があります。Tenable Vulnerability Management はダッシュボードを更新し、影響を受けている検出結果のインスタンスがいくつ変更されたかを示すラベルが表示されます。

   > **注意:** 変更ルールによって、スキャンの履歴結果に影響が出ることはありません。

検出結果で許容ルールを作成する

[検出結果] ワークベンチから許容ルールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[検出結果]** をクリックします。

   [検出結果] ページが表示され、**[脆弱性]** タブがアクティブになり、検出結果がテーブルビューで表示されます。

3. (オプション) **[ウェブアプリケーションの検出]** をクリックします。

   [ウェブアプリケーションの検出] タブが表示されます。

4. ルールを作成する検出結果の行で ⋮ 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。

5. **[変更]** をクリックします。

   [変更ルールの追加] プレーンが表示されます。

6. **[変更ルールの追加]** プレーンの **[アクション]** セクションで、**[許容]** をクリックします。

7. **[ルール情報]** セクションで以下のオプションを設定します。

   a. **脆弱性プラグイン ID** - 許容するプラグインの ID が事前選択されているものと異なる場合は、その ID を入力します(たとえば 51192)。

   > **注意:** プラグイン ID が Tenable Nessus プラグインに対応する場合は、**元の深刻度** インジケーターが脆弱性のデフォルトの深刻度に一致するよう変更されます。

   b. **ターゲット** - **[すべて]** を選択してすべての資産をターゲットにするか、**[カスタム]** を選択してルールを実行するターゲットを指定します。

   c. **ターゲットとなるホスト** - 必要に応じて、ルールの 1 つ以上のカスタムターゲットを入力します。IP アドレス、IP 範囲、CIDR、ホスト名の任意の組み合わせを含むコンマ区切りリストを入力できます。

   > **注意**: 指定できるコンマ区切りカスタムエントリは 1000 個までとなっています。これよりも多くのカスタムエントリをターゲットにする場合は、複数のルールを作成してください。

   d. (オプション) **有効期限日** - ルールが期限切れになる日付を選択します。

e. (オプション) **コメント** - ルールの説明を入力します。このオプションは、ルールが変更された場合にのみ表示されます。

8. (オプション) 脆弱性を誤検出として報告する方法

   a. **[誤検出として報告する]** トグルを有効にします。

      [Tenable へのメッセージ] ボックスが表示されます。

   b. **[Tenable へのメッセージ]** ボックスに、誤検出の説明を入力します。

9. **[保存]** をクリックします。

   Tenable Vulnerability Management が既存の検出結果にルールを適用し始めます。システムの負荷と一致する検出結果の数によっては、このプロセスに時間がかかる場合があります。

検出結果レポートを生成する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management では、**[検出結果]** ワークベンチで、テンプレートからレポートを PDF に生成できます。このレポートをスケジュールして、メールで送信できます。

注意: 10,000 件を超える検出結果についてレポートを生成することはできません。この数を超える検出結果を選択してレポートを生成すると、エラーが表示されます。

注意: 脆弱性の検出結果のレポートのみを生成できます。他のタイプの検出結果のレポートは生成できません。

レポートを生成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** で **[検出結果]** をクリックします。

   [検出結果] ワークベンチが **[脆弱性]** タブと共に表示されます。

3. (オプション) フィルターの使用 の説明に従って、検出結果のリストを選別します。

   注意: レポートには最大 5 つのフィルターを適用できます。

4. レポートを作成する検出結果の横にあるチェックボックスを 1 つまたは複数選択します。

   ヒント: リストの一番上にあるチェックボックスを選択すると、すべての検出結果を選択できます。

   アクションバーが表示されます。

5. アクションバーで、**[レポートの生成]** をクリックします。

   [レポートを生成] プレーンが表示されます。次のオプションが含まれています。

オプション	説明
名前	(オプション) レポートのカスタム名を入力します。

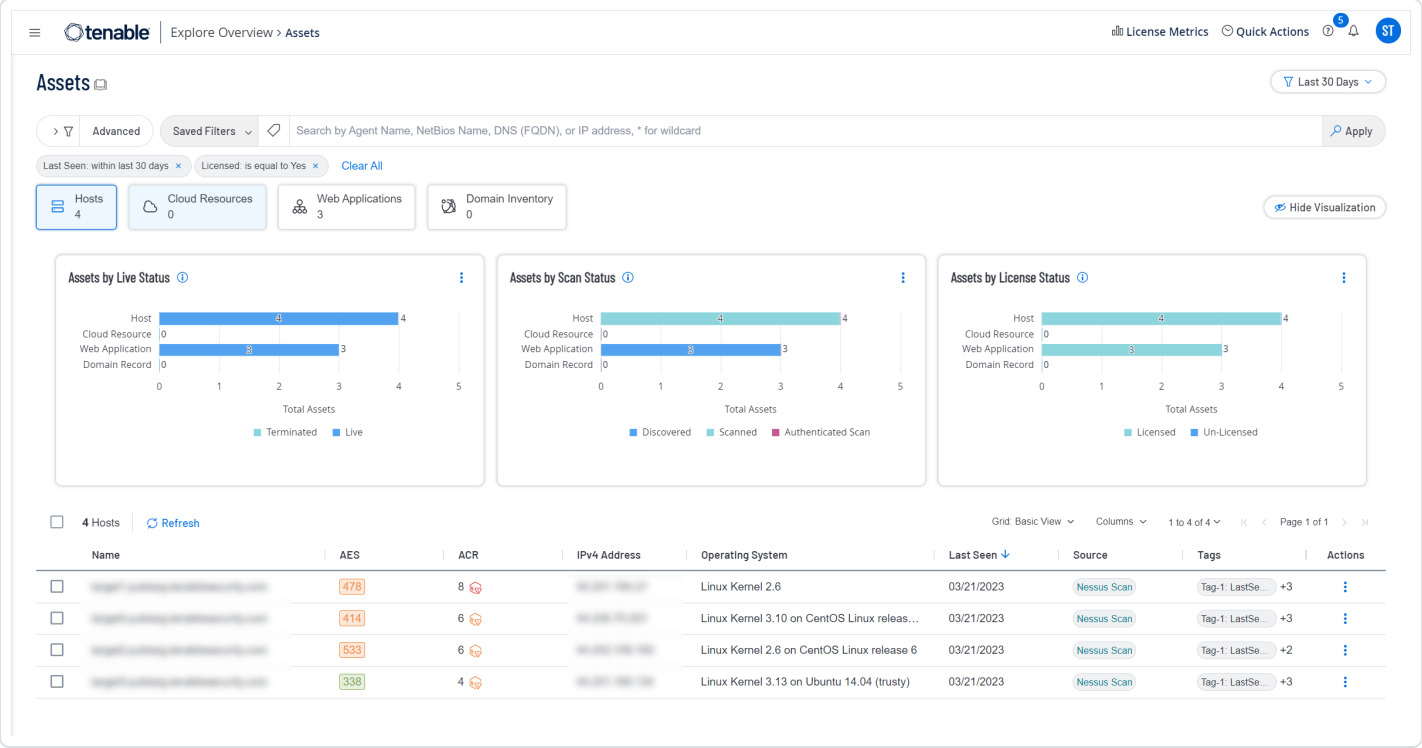
テンプレート	レポートのテンプレートを選択します。次のテンプレートから選択します。 • **ホスト検出結果エグゼクティブサマリーレポート** - 報告対象の脆弱性の深刻度レベルと、関連する資産の深刻度、最終スキャン時間、ポート数をまとめたものです。 • **ホスト検出結果の脆弱性詳細 (プラグイン別)** - レポートを作成している脆弱性の詳細をプラグイン別に示します。 • **ホスト検出結果の脆弱性詳細 (資産別)** - レポートを作成している脆弱性に関連する資産の詳細を示します。
スケジュール	**[スケジュール]** トグルをオンにして、レポートのスケジュールを設定します。 a. **[開始日時]** セクションで、レポートを実行する日時を選択します。 b. **[タイムゾーン]** ドロップダウンで、タイムゾーンを選択します。 c. **[繰り返し]** ドロップダウンで、レポートを繰り返す頻度を選択します (例: 毎日)。 d. **[繰り返し終了]** ドロップダウンで、レポートの実行を終了する日付を選択します。
受信者を追加する	(オプション) 完成したレポートを Tenable Vulnerability Management が送信するメールを入力します。
パスワード保護	(オプション) AES 128 ビット暗号化でレポートをパスワード保護するには、このトグルを有効にします。**[暗号化パスワード]** フィールドに、受信者に提供するパスワードを入力します。

6. **[レポートを生成]** をクリックします。

確認メッセージが表示され、Tenable Vulnerability Management がレポートの作成を開始します。メッセージ内のリンクをクリックして、レポートを表示します。または、**[アクション]** > **[レポート]** > **[レポートの結果]** ページに移動します。

資産

[資産] ワークベンチで、所属組織の資産に関するインサイトを得られます。これらには、ホスト資産、クラウドリソース、ウェブアプリケーション、ドメインインベントリが含まれます。



資産はネットワーク上の価値を持つエンティティであり、悪用される可能性があります。これには、ラップトップ、デスクトップ、サーバー、ルーター、携帯電話、仮想マシン、ソフトウェアコンテナ、クラウドインスタンスなどがあります。Tenable Vulnerability Management は資産についての包括的な情報を提供することで、セキュリティリスクの可能性を排除し、十分に活用されていないリソースを特定し、コンプライアンスの取り組みをサポートします。

Tenable Vulnerability Management はスキャンが完了したとき、またはスキャン結果がインポートされたときに、資産を自動的に作成または更新します。Tenable Vulnerability Management は、ホスト属性を調べ、可能な限り最適なマッチを選択するヒューリスティックを採用している複雑なアルゴリズムを通じて、受信するスキャンデータと既存の資産のマッチングを試行します。Tenable Vulnerability Management がマッチを見つけられない場合、資産をそのとき初めて発見したものと仮定して、新しいレコードを作成します。Tenable Vulnerability Management がマッチする資産を見つけた場合、新しく変更されたプロパティがあればそれを更新します。

可能な場合には、Tenable Vulnerability Management は他の資産情報を収集します。

- インターフェース (IP アドレスと MAC アドレス)
- DNS 名
- NetBIOS 名
- オペレーティングシステム
- インストール済みのソフトウェア
- UUIDS (Tenable、ePO、BIOS)
- エージェントの有無

詳細については、次のトピックを参照してください。

資産ワークベンチの表示

[資産] ワークベンチですべての資産を表示できます。

資産を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[調査]** > **[資産]** をクリックします。

   [資産] ワークベンチが表示され、**[ホスト]** タイルがアクティブになります。

3. (オプション) 次のいずれかの操作を実行します。

   - 表示される資産タイプをカスタマイズするには、タイルを選択または選択解除します。
     - ホスト資産
     - クラウドリソース
     - ウェブアプリケーション
     - ドメインインベントリ
   - 検索ボックスで、エージェント名、NetBios 名、DNS (FQDN)、または IP アドレスで検索します。(*) をワイルドカードとして使用します。
   - 検出結果または資産のフィルタリング の説明に従って、表示された資産をフィルタリングし、ビューをカスタマイズします。

     > **ヒント**: すべての資産フィルターの定義は、資産フィルターで確認できます。

   - 検出結果または資産の保存されたフィルターで説明されているように、フィルターをカスタム検索として保存します。
   - 検出結果または資産のエクスポート で説明されているように、資産を CSV または JSON 形式にエクスポートします。
   - 右上にあるドロップダウンを使用して、表示された資産を期間でフィルタリングします。
   - 資産の詳細の表示で説明されているように、資産に関する詳細を表示します。

- 資産ビジュアライゼーションの表示で説明されているように、表示された資産をビジュアル化して表示します。

ホスト資産

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[資産] ワークベンチでホスト資産のみを表示するには、**[ホスト]** タイルを選択し、他のタイルの選択を解除します。一般的なホスト資産には、ワークステーション、サーバー、仮想マシン、プリンター、ネットワークスイッチ、ルーター、ワイヤレスアクセスポイントなどがあります。

[ホスト] タイルには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズを参照してください。

列	説明
資産 ID	資産の UUID。この値は Tenable Vulnerability Management に対して一意です。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。

AES	資産の資産のエクスポージャースコア。
ACR	資産の ACR (資産重大度の格付け)。
IPV4 アドレス	影響を受けている資産の IPv4 アドレス。
IPV6 アドレス	影響を受けている資産の IPv6 アドレス。
オペレーティングシステム	スキャンにより資産にインストールされていると特定されたオペレーティングシステム。
ライセンス済み	資産が Tenable Vulnerability Management 内でライセンスされるかどうかを示します。詳細は、Tenable Vulnerability Management のライセンス を参照してください。
初回確認日	スキャンが最初に資産を特定した日時。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
最終ライセンススキャン日	資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。
最終認証スキャン日	資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。
ソース	資産を特定したスキャンのソース。
タグ	資産に適用されるタグです。
システムの種類	資産にインストールされているオペレーティングシステム。
NetBIOS 名	資産の NetBIOS 名。
DNS (FQDN)	資産ホストの完全修飾ドメイン名。 **注意:** ホスト資産の完全修飾ドメイン名 (FQDN) を処理するとき、Tenable Vulnerability Management はすべての FQDN を小文字に正規化してから、重複を

	マージします。
MAC アドレス	スキャンにより資産レコードと関連付けられた MAC アドレス。
ServiceNow Sys ID	該当する場合、ServiceNow での資産の固有レコード識別子。詳細は、ServiceNow のドキュメントを参照してください。
エージェント名	資産をスキャンして特定した、Tenable Nessus エージェントの名前。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
更新日	Tenable Vulnerability Management が資産レコードを最後に更新した日時。
プラグインの結果有り	資産が関連付けられたプラグイン結果を持つかどうかを指定します。
パブリック	資産がパブリックネットワークで使用可能かどうかを指定します。 **注意:** パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Management クエリ名前空間の `is_public` 属性によって識別されます。
AWS 可用性ゾーン	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS 可用性ゾーン(該当する場合)。
AWS EC2 AMI ID	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS EC2 AMI ID (該当する場合)。
AWS EC2 インスタンス ID	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS EC2 インスタンス ID (該当する場合)。
AWS セキュリティグループ	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS セキュリティグループ(該当する場合)。
AWS インスタンスの状態	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS インスタンスの状態 (該当する場合)。
AWS インスタンスタイプ	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS インスタンスタイプ(該当する場合)。
AWS EC2 名	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS EC2 名 (該当する場合)。

AWS EC2 製品コード	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS EC2 製品コード (該当する場合)。
AWS 所有者 ID	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS 所有者 ID (該当する場合)。
AWS リージョン	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS リージョン (該当する場合)。
AWS サブネット ID	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS サブネット ID (該当する場合)。
AWS VPC ID	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS VPC ID (該当する場合)。
Azure リソース ID	Tenable Vulnerability Management AWSドキュメントで説明されている、資産の AWS リソース ID (該当する場合)。
Azure VM ID	Tenable Vulnerability Management Microsoft Azureドキュメントで説明されている、資産の Azure VM ID (該当する場合)。
Google Cloud インスタンス ID	Tenable Vulnerability Management Google Cloud Platformドキュメントで説明されている、資産の Google Cloud インスタンス ID (該当する場合)。
Google Cloud プロジェクト ID	Tenable Vulnerability Management Google Cloud Platformドキュメントで説明されている、資産の Google Cloud プロジェクト ID (該当する場合)。
Google Cloud ゾーン	Tenable Vulnerability Management Google Cloud Platformドキュメントで説明されている、資産の Google Cloud ゾーン (該当する場合)。
リソースタグ	クラウドプロバイダーからインポートするタグまたはラベルを指定します。このフィールドは、ソースが**クラウド検出コネクタ**である資産に対して表示されます。 **注意:** Tenable Vulnerability Management は、次の事項を考慮してタグとラベルをインポートします。 • AWS および Azure の制限は、リソースあたり 50 タグです。 • GCP の制限は、リソースあたり 64 ラベルです。 • Tenable Vulnerability Management は、Azure タグの JSON 文字列のインポートをサポートしていません。

クラウドプロバイダー	資産が AWS、Azure、GCP のどれからのものであるかを示します。
アクション	この列の ⋮ ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **タグの追加** - 新しいタグを追加します。表示されたダイアログで、タグで説明されているように、*[カテゴリ]* と *[値]* を選択します。 • **タグの削除** - 既存のタグを削除します。表示されたダイアログでタグをクリックし、**[削除]** をクリックします。 • **ACR の編集** – (Tenable Lumin のみ)。ホスト資産の ACR の編集 で説明されているように、ACR (資産重大度の格付け)を編集します。 • **移動** - 資産を別のネットワークに移動するで説明されているように、資産を別のネットワークに移動します。 • **すべての詳細を表示** – 資産の詳細の表示で説明されているように、資産の詳細をすべて表示します。 • **新しいタブですべての詳細を表示** – 資産の完全な詳細をブラウザの新しいタブに表示します。 • **すべてのソリューションを表示** – ソリューションで説明されているように、資産の脆弱性に対して利用可能なソリューションを表示します。 • **削除** - 資産の削除で説明されているように、資産を完全に削除します。

クラウドリソース

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[資産] ワークベンチでクラウドリソースのみを表示するには、**[クラウドリソース]** タイルを選択し、他のタイルの選択を解除します。クラウドリソースとは、クラウドプラットフォーム内で作成または設定できるコンピューティングインスタンス、ストレージオブジェクト、ネットワークデバイス、またはオブジェクトです。クラウドリソースの例としては、仮想サーバー、バケット、データベース、ディスク、コンテナーなどの資産が挙げられます。他にも、リソースグループ、ポリシー、ユーザー、ロールなどの設定可能なアイテムがあります。

[クラウドリソース] タイルには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズを参照してください。

列	説明
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名

	上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。
リソースタイプ	クラウドリソースタイプの名前 (リソースグループや仮想マシンなど)。
リソースカテゴリ	クラウドリソースタイプが属するカテゴリの名前 (オブジェクトストレージや仮想ネットワークなど)。
リソースタグ	Amazon Web Services (AWS) などのクラウドソースから同期されたタグ。最初のタグのみが表示されます。表示されているタグにカーソルを合わせると、完全なリストが表示されます。
クラウドプロバイダー	資産をホストするクラウドプロバイダーの名前。
リージョン	資産が実行されるクラウドリージョン。
ライセンス済み	資産が Tenable Vulnerability Management 内でライセンスされるかどうかを示します。詳細は、Tenable Vulnerability Management のライセンス を参照してください。
初回確認日	スキャンが最初に資産を特定した日時。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
ソース	資産を特定したスキャンのソース。
タグ	資産に適用されている任意の Tenable Vulnerability Management タグ。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
更新日	Tenable Vulnerability Management が資産レコードを最後に更新した日時。
アクション	この列の ⋮ ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポート で説明されているように、CSV または JSON にエクスポートします。 • **タグの追加** - 新しいタグを追加します。表示されたダイアログで、タグ で説明されて

	いるように、*[カテゴリ]*と*[値]*を選択します。 • **タグの削除** - 既存のタグを削除します。表示されたダイアログでタグをクリックし、**[削除]**をクリックします。

ウェブアプリケーション

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[資産] ワークベンチでウェブアプリケーション資産のみを表示するには、**[ウェブアプリケーション]** タイルを選択し、他のタイルの選択を解除します。ウェブアプリケーションとは、ブラウザで実行されるソフトウェアのことです。ウェブアプリケーションの例としては、ワークプレースコラボレーションアプリ、e コマースアプリ、メールアプリ、バンキングアプリなどがあります。

[ウェブアプリケーション] タイルには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズを参照してください。

列	説明
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されま

	す。
AES	資産の資産のエクスポージャースコア。
ACR	資産の ACR (資産重大度の格付け)。
ライセンス済み	資産が Tenable Vulnerability Management 内でライセンスされるかどうかを示します。詳細は、Tenable Vulnerability Management のライセンス を参照してください。
SSL/TLS	資産がホストされているアプリケーションが SSL/TLS 公開鍵暗号化を使用するかどうかを指定します。
IPV4 アドレス	影響を受けている資産の IPv4 アドレス。
オペレーティングシステム	資産にインストールされているオペレーティングシステム。
初回確認日	スキャンが最初に資産を特定した日時。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
最終ライセンススキャン日	資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。
最終認証スキャン日	資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。
パブリック	資産がパブリックネットワークで使用可能かどうかを指定します。 **注意:** パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Management クエリ名前空間の `is_public` 属性によって識別されます。
ソース	資産を特定したスキャンのソース。
タグ	資産に適用されるタグです。

作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
更新日	Tenable Vulnerability Management が資産レコードを最後に更新した日時。
アクション	この列の ⋮ ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **タグの追加** - 新しいタグを追加します。表示されたダイアログで、タグで説明されているように、*[カテゴリ]* と *[値]* を選択します。 • **タグの削除** - 既存のタグを削除します。表示されたダイアログでタグをクリックし、**[削除]** をクリックします。 • **すべての詳細を表示** – 検出結果の詳細の表示で説明されているように、検出結果の詳細をすべて表示します。 • **削除** - 資産の削除で説明されているように、資産を完全に削除します。

ドメインインベントリ

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[資産] ワークベンチでドメインインベントリ資産のみを表示するには、**[ドメインインベントリ]** タイルを選択し、他のタイルの選択を解除します。ドメインインベントリは、所属組織が所有するすべてのドメインの完全なアカウントです。ドメインは、データベース、アプリケーション、ディレクトリサービス、ID またはアクセス管理プラットフォームなど、幅広い資産に関連付けられています。

[ドメインインベントリ] タイルには、以下の列がある表が表示されます。列を表示または非表示にするには、調査の表のカスタマイズを参照してください。

列	説明
資産 ID	スキャンで検出結果が検出された資産の UUID です。この値は Tenable Vulnerability Management に対して一意です。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。

ホスト名	資産のホスト名。
レコードタイプ	資産のタイプ。
レコード値	資産のレコード値。
ドメイン	資産が属するドメイン
DNS (FQDN) (ASM)	資産ホストの完全修飾ドメイン名。
IPv4 アドレス (ASM)	資産の IPv4 アドレス。
IPv4 アドレス (ASM)	資産の IPv6 アドレス。
ホスティングプロバイダー	資産をホストするプロバイダー。
ASN	資産の自律システム番号 (ASN)。
ライセンス済み	資産が Tenable Vulnerability Management 内でライセンスされるかどうかを示します。詳細は、Tenable Vulnerability Management のライセンス を参照してください。
初回確認日	スキャンが最初に資産を特定した日時。
最終確認日	スキャンが資産上で脆弱性を検出した直近の日付。
ソース	資産を特定したスキャンのソース。
タグ	資産に適用されるタグです。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
更新日	Tenable Vulnerability Management が資産レコードを最後に更新した日時。

ポート	資産に関連付けられているポート。
アクション	この列の ⋮ ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **タグの追加** - 新しいタグを追加します。表示されたダイアログで、タグで説明されているように、*[カテゴリ]* と *[値]* を選択します。 • **タグの削除** - 既存のタグを削除します。表示されたダイアログでタグをクリックし、**[削除]** をクリックします。 • **高度なネットワークスキャンを作成** - スキャンの作成で説明されているように、高度なネットワークスキャンを作成します。 • **ウェブアプリケーションスキャンを作成** – スキャンの作成で説明されているように、ウェブアプリケーションスキャンを作成します。 • **削除** - 資産の削除で説明されているように、資産を完全に削除します。

資産の詳細の表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Vulnerability Managementアクセス許可: 該当する資産に対する Can View アクセス許可

[資産] ワークベンチから、1 つの資産をドリルダウンすると、**[資産の詳細]** ページに資産が表示されます。Tenable Vulnerability Management は資産のタイプ別にこのページをカスタマイズします。

注意: ドメインインベントリ資産には **[資産の詳細]** ページはありませんが、ドメインインベントリのプレビューで説明されているように、プレビューで表示できます。

資産の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンで **[調査]** > **[資産]** をクリックします。

   [資産] ワークベンチが表示され、**[ホスト]** タイルがアクティブになります。

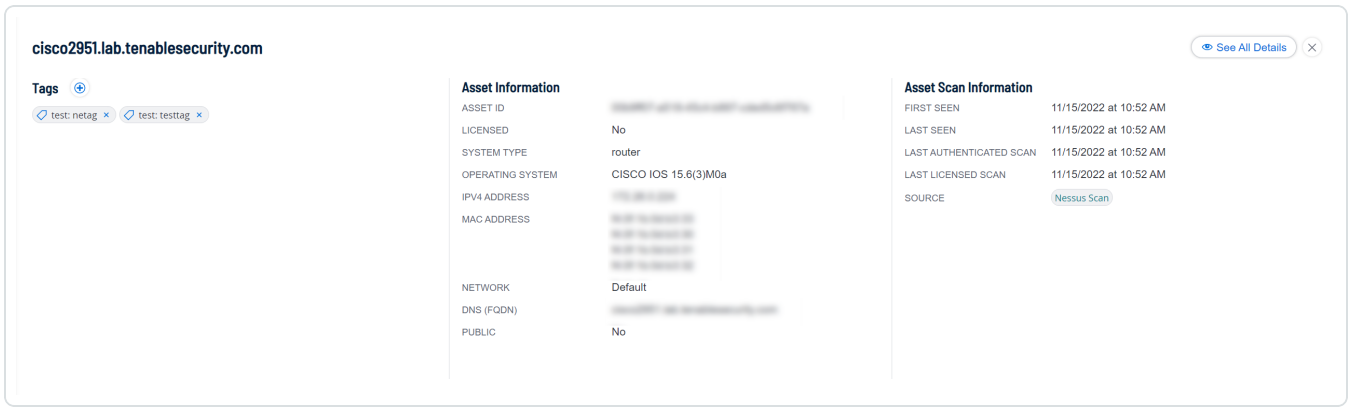
3. (オプション) 別のタイルをクリックして、結果を展開します。

   そのタイルの資産が表示されます。各資産タイプでデフォルト列は異なります。

4. 検出結果または資産のフィルタリング の説明に従って、表示された資産をフィルタリングし、ビューをカスタマイズします。

5. 表示する資産の行をクリックします。

   プレビューがページの下部に表示されます。



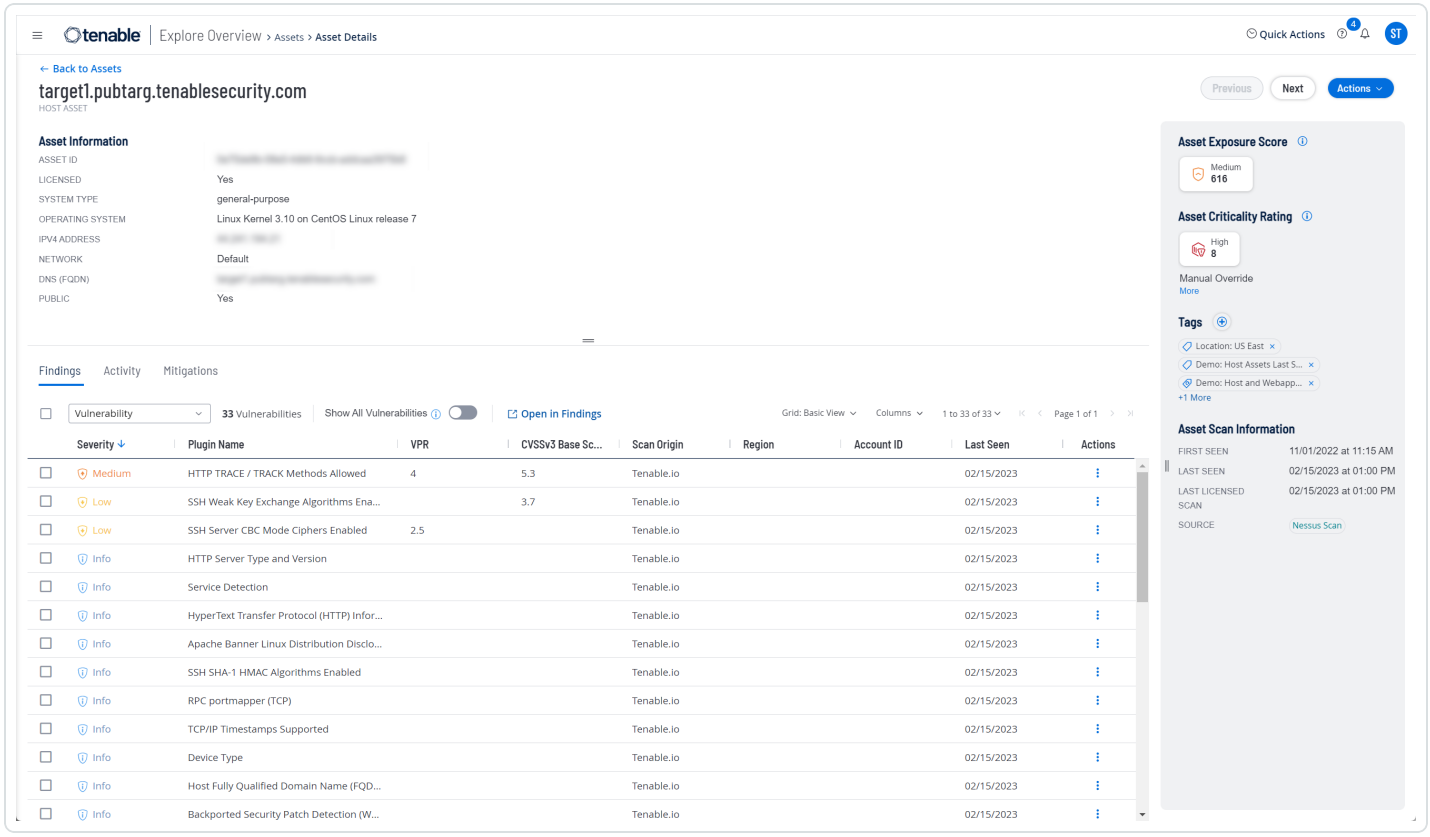
6. プレビューで、**[すべての詳細を表示]**をクリックします。

   [資産の詳細]ページが表示されます。ページのレイアウトは、次のように資産タイプによって異なります。

   - ホスト資産の詳細
   - クラウドリソースの詳細
   - ウェブアプリケーションの詳細

ホスト資産の詳細

資産の詳細の表示 で表示される**[資産の詳細]**ページは、資産のタイプによって異なります。ホスト資産の場合、資産情報、関連する検出結果のリスト、AES、および ACR が含まれます。



ホスト資産の**[資産の詳細]**ページには、次のセクションがあります。

注意: Tenable Vulnerability Management は空のセクションを非表示にするため、これらのセクションは表示されない場合があります。

セクション	説明
ヘッダー	資産ヘッダー。特定の属性の存在に基づいて次の論理順序で表示されます。 1. エージェント名 2. NetBIOS 名 3. ローカルホスト名 4. ホスト完全修飾ドメイン名 (FQDN)

	5. IPv4 アドレス 6. IPv6 アドレス
資産情報	ホスト資産に関する情報で、次のものが含まれます。 • **資産 ID** - 資産の UUID。 • **ライセンス済み** - 資産がライセンスされているかどうかを示します。 • **システムタイプ** - プラグイン ID 54615 によって報告されるシステムタイプ。詳細は、Tenableプラグインを参照してください。 • **オペレーティングシステム** - スキャンによって資産にインストールされていると識別されたオペレーティングシステム。 • **IPv4 Address** - 資産の IPv4 アドレス • **IPV6 アドレス** - 資産の IPv6 アドレス。 • **MAC アドレス** - 資産の MAC アドレス。 • **ネットワーク** - 資産を識別したスキャナーに関連付けられたネットワークオブジェクトの名前。デフォルトのネットワーク名は **[Default]** です。ネットワークに関する詳細は、ネットワークを参照してください。 • **エージェント名** - 資産をスキャンして特定した Tenable Nessus Agentの名前。 • **DNS (FQDN)** - 資産ホストの完全修飾ドメイン名。 • **SSH フィンガープリント** - スキャンによって資産レコードに関連付けられた SSH キーのフィンガープリント。 • **Tenable ID** - Tenable Vulnerability Management での資産の UUID。 • **パブリック** - 資産がパブリックネットワークで使用可能かどうかを指定します。パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Managementクエリ名前空間の `is_public` 属性によって識別されます。 • **BIOS ID** - 資産の BIOS UUID。 • **ServiceNow Sys ID** - 該当する場合、ServiceNow での資産の固有レコード識別子。

	• **カスタム属性** - 資産に追加されたカスタム属性。詳細は、Tenable 開発者ポータルを参照してください。
検出結果	**[検出結果]** タブをクリックすると、資産に関連付けられているすべての検出結果を表示できます。 • ドロップダウンで、**[脆弱性]** と **[ホスト監査]** の検出結果を切り替えます。 • **[すべての脆弱性を表示]** トグルをクリックして、[修正済み] と [許容済み] の脆弱性やホスト監査を非表示にします。 • **[検出結果で開く]** をクリックして、**[検出結果]** ワークベンチにすべての検出結果を表示します。 • 検出結果の行で ⋮ をクリックするとメニューが表示され、検出結果の詳細を表示したり、検出結果をエクスポートしたり、修正スキャンを起動したりできます。 • 調査の表のカスタマイズで説明されているように、列を表示または非表示にします。
開いているポート	**[開いているポート]** タブをクリックして、資産の開いているポートを表示します。 • **開いているポート** - 資産の開いているポートに関する情報を表示します。 • **プロトコル** - TCP や UDP などの開いているポートに情報を転送する際に使用するプロトコルを指定します。 • **最初に検出されたオープン** - ポートが開いていると最初に検出された日時 • **最後に検出されたオープン** - ポートが開いていると最後に検出された日時 • **サービス** - そのオープンポートで実行されているサービス (HTTPS、SSH、FTP など) 使用できるサービスの詳細については、*Internet Assigned Numbers Authority* の Web サイトの Service Name and Transport Protocol を参照してください。
アクティビティ	**[アクティビティ]** タブをクリックすると、資産のアクティビティが表示されます。 • **イベント** – Tenable Vulnerability Management によってログ記録されたすべての資産イベントを指定します (例: 検出された資産)。 • **日付** – イベントの日付を指定します。 • **ソース** – Nessus スキャンなどのイベントソースを指定します。

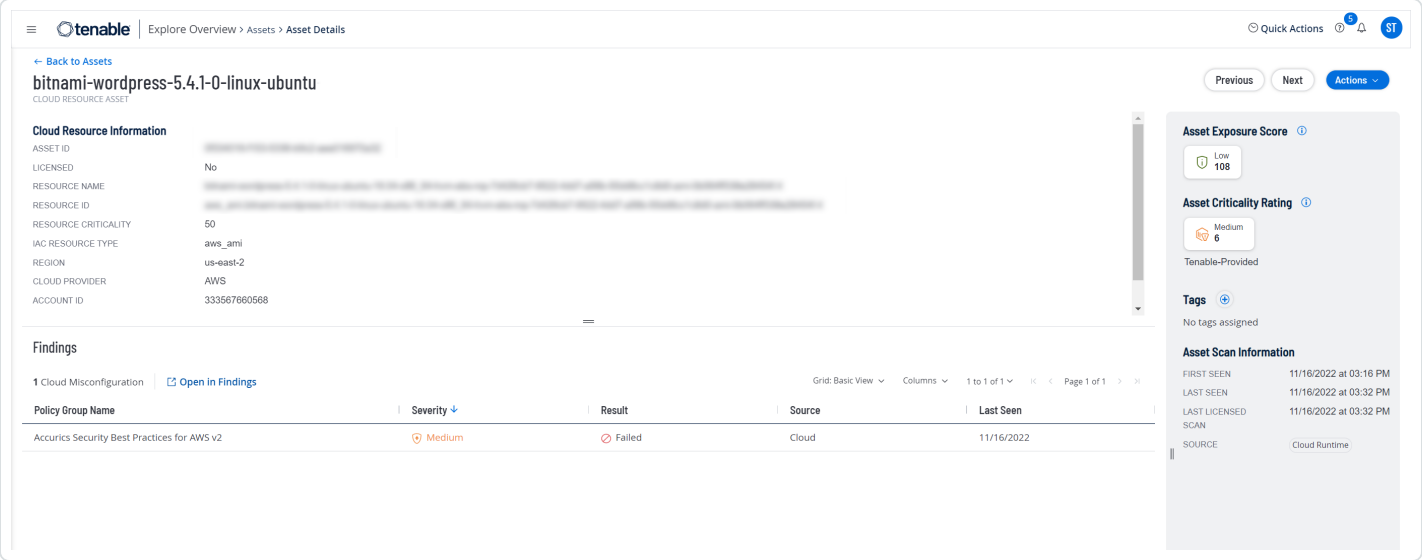
緩和	**[緩和]** タブをクリックすると、スキャンによって資産で特定された軽減ソフトウェアに関する情報が表示されます。
資産のエクスポージャースコア	(Tenable Lumin ライセンスが必要) 資産に対して計算された 資産のエクスポージャースコア (AES) を示す説明アイコン。
ACR (資産重大度の格付け)	(Tenable Lumin ライセンスが必要) 資産の ACR (資産重大度の格付け) を示す説明アイコン。
クラウドリソース情報	クラウドリソース情報には次のものが含まれます。 • **AWS 可用性ゾーン** - 資産の AWS EC2 AMI ID。詳細については、Tenable Vulnerability ManagementAWS ドキュメントを参照してください。 • **AWS EC2 AMI ID** - 資産の AWS EC2 インスタンス ID。 • **AWS EC2 インスタンス ID** - 資産の AWS EC2 インスタンス ID。 • **AWS セキュリティグループ** - 資産の AWS セキュリティグループ。 • **AWS インスタンスの状態** - 資産の AWS インスタンスの状態。 • **AWS インスタンスタイプ** - 資産の AWS インスタンスタイプ。 • **AWS EC2 名** - 資産の AWS EC2 名。 • **AWS EC2 製品コード** - 資産の AWS EC2 製品コード。 • **AWS 所有者 ID** - 資産の AWS 所有者 ID。 • **AWS リージョン** - 資産の AWS リージョン。 • **AWS サブネット ID** - 資産の AWS サブネット ID。 • **AWS VPC ID** - 資産の AWS VPC ID。 • **Google Cloud インスタンス ID** - 資産の Google Cloud インスタンス ID。詳細は、Tenable Vulnerability ManagementGoogle Cloud Platform ドキュメントを参照してください。

	• **Google Cloud プロジェクト ID** - 資産の Google Cloud プロジェクト ID。 • **Google Cloud ゾーン** - 資産の Google Cloud ゾーン。
タグ	資産に適用されるタグです。タグを追加するには、⊕ ボタンをクリックします。タグを削除するには、タグラベルの ✕ ボタンをクリックします。詳細は、タグ を参照してください。
資産スキャン情報	資産のスキャン履歴に関する情報です。次の情報が含まれます。 • **First Seen** - スキャンが最初に資産を特定した日時 • **最終確認日** - スキャンが資産を最後に特定した日時。 • **最終認証スキャン日** - 資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。 • **最終ライセンススキャン日** - 資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。 • **ソース** - 資産を特定したスキャンのソースです。
アクション	右上の **[アクション]** ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポート で説明されているように、CSV または JSON にエクスポートします。 • **タグの追加** - 新しいタグを追加します。表示されたダイアログで、タグで説明されているように、*[カテゴリ]* と *[値]* を選択します。 • **タグの削除** - 既存のタグを削除します。表示されたダイアログでタグをクリックし、**[削除]** をクリックします。 • **ACR の編集** – (Tenable Lumin のみ)。ホスト資産の ACR の編集 で説明されて

	いるように、ACR (資産重大度の格付け)を編集します。 • **移動** - 資産を別のネットワークに移動するで説明されているように、資産を別のネットワークに移動します。 • **すべてのソリューションを表示** – ソリューションで説明されているように、資産の脆弱性に対して利用可能なソリューションを表示します。 • **削除** - 資産の削除で説明されているように、資産を完全に削除します。

クラウドリソースの詳細

資産の詳細の表示 で表示される**[資産の詳細]**ページは、資産のタイプによって異なります。クラウドリソース資産の場合、サマリー、関連する検出結果のリスト、AES、および ACR が含まれます。



クラウドリソースの**[資産の詳細]**ページには、次のセクションがあります。

注意: Tenable Vulnerability Management は空のセクションを非表示にするため、これらのセクションは表示されない場合があります。

セクション	説明
ヘッダー	資産ヘッダー。特定の属性の存在に基づいて次の論理順序で表示されます。 1. エージェント名 2. NetBIOS 名 3. ローカルホスト名 4. ホスト完全修飾ドメイン名 (FQDN) 5. IPv4 アドレス 6. IPv6 アドレス
クラウドリソース情	クラウドリソースに関する情報で、次のものが含まれます。 • **資産 ID** - リソースの UUID。

報	• **ライセンス済み** - リソースがライセンスされているかどうか。 • **リソース名** - リソースの名前。 • **リソース ID** - リソースをホストするクラウドサービスのリソースに割り当てられた一意の識別子。 • **リソースの重要度** - 直近のスキャンに基づく、Tenable Container Security によるリソースの重大度評価。 • **リージョン** - リソースが実行されるクラウドリージョン。 • **クラウドプロバイダー** - 資産をホストしているクラウドプロバイダーの名前。 • **アカウント ID** - リソースに関連付けられている Tenable Cloud Security アカウントの ID。 • **VPC** - 仮想プライベートクラウド。AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。 • **リソースタイプ** - 資産のクラウドリソースの種類 (ネットワーク、仮想マシンなど) • **リソースカテゴリ** - クラウドリソースタイプが属するカテゴリの名前 (オブジェクトストレージや仮想ネットワークなど) • **リソースタグ** - クラウドプロバイダーによってリソースに関連付けられたラベル。 • **IaC リソースタイプ** - インフラのコード化 (IaC) クラウドリソース資産に関連付けられた Terraform リソースタイプ。 • **リポジトリ** - 資産のソースディレクトリへのパス。 • **ドリフトあり** - 資産にドリフトがあるかどうかを示します。詳細については、*Tenable Cloud Security ユーザーガイド*のドリフト分析の設定を参照してください。 • **マッピング済み** - 資産がマッピングされているかを示します。詳細については、*Tenable Cloud Security ユーザーガイド*のクラウドスキャンワークフローを参照してください。 • **プロジェクト** - 資産に関連付けられているクラウドプロジェクト。 • **Network** - 資産をスキャンするスキャナーが属するネットワークの名前詳細は、ネットワークを参照してください。

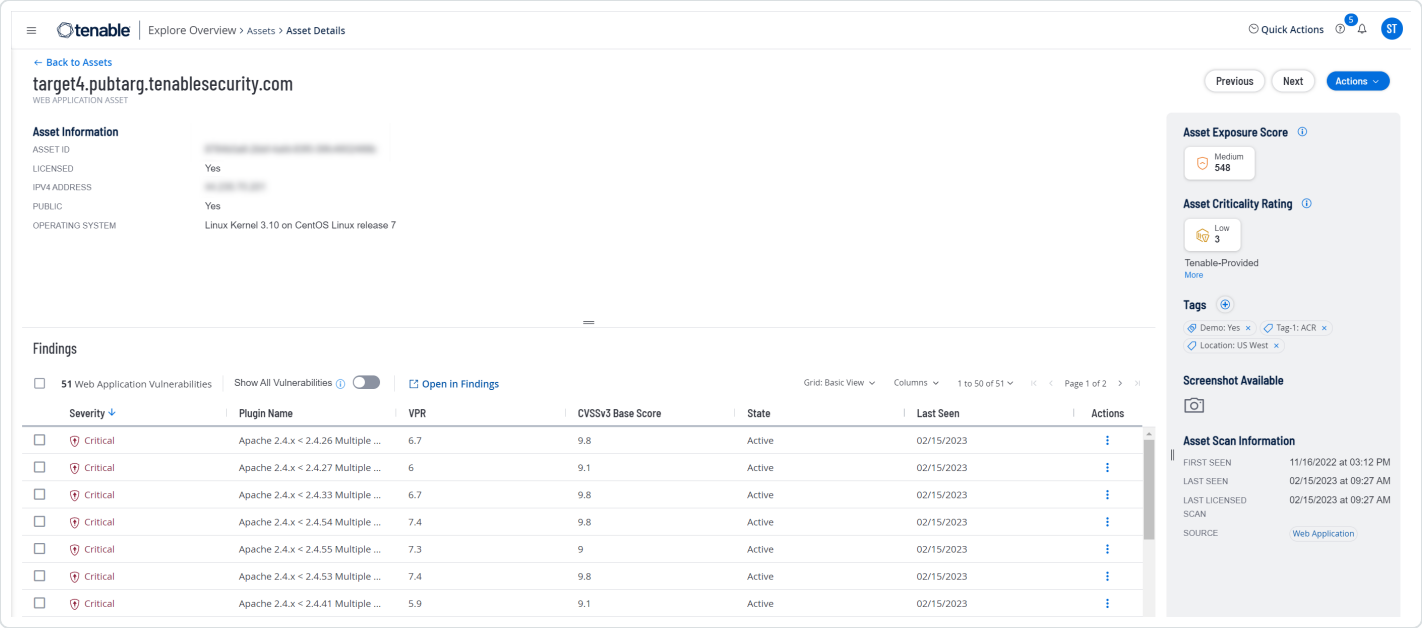
	• **可用性ゾーン** - 仮想マシンインスタンスがホストされている可用性ゾーンの名前。
検出結果	リソースに関連付けられたすべての検出結果を一覧表示する表。**[検出結果で開く]** をクリックすると、[脆弱性] ページが表示されます。
資産のエクスポージャースコア	(Tenable Lumin ライセンスが必要) 資産に関して計算された資産のエクスポージャースコアを示す説明アイコン。
ACR (資産重大度の格付け)	(Tenable Lumin ライセンスが必要) 資産の ACR (資産重大度の格付け) を示す説明アイコン。
タグ	資産に適用されるタグです。タグを追加するには、⊕ ボタンをクリックします。タグを削除するには、タグラベルの ✕ ボタンをクリックします。詳細は、タグ を参照してください。
資産スキャン情報	• **First Seen** - スキャンが最初に資産を特定した日時 • **最終確認日** - スキャンが資産を最後に特定した日時。 • **最終ライセンススキャン日** - 資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。 • **最終認証スキャン日** - 資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。 • **ソース** - 資産を特定したスキャンのソースです。
アクション	右上の **[アクション]** ボタンをクリックしてドロップダウンを表示し、次の操作を実行できま

	す。 • **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 • **タグの追加** - 新しいタグを追加します。表示されたダイアログで、タグで説明されているように、*[カテゴリ]* と *[値]* を選択します。 • **タグの削除** - 既存のタグを削除します。表示されたダイアログでタグをクリックし、**[削除]** をクリックします。 • **すべての詳細を表示** – 資産の詳細の表示で説明されているように、資産の詳細をすべて表示します。 • **新しいタブですべての詳細を表示** – 資産の完全な詳細をブラウザの新しいタブに表示します。

ウェブアプリケーションの詳細

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

資産の詳細の表示 で表示される**[資産の詳細]**ページは、資産のタイプによって異なります。ウェブアプリケーション資産の場合、資産情報、関連する検出結果のリスト、AES、および ACR が含まれます。



ウェブアプリケーション資産の**[資産の詳細]**ページには、次のセクションがあります。

注意: Tenable Vulnerability Management は空のセクションを非表示にするため、これらのセクションは表示されない場合があります。

セクション	説明
ヘッダー	資産ヘッダー。特定の属性の存在に基づいて次の論理順序で表示されます。 1. エージェント名 2. NetBIOS 名 3. ローカルホスト名 4. ホスト完全修飾ドメイン名 (FQDN) 5. IPv4 アドレス

	6. IPv6 アドレス
資産情報	資産に関する情報です。次のものが含まれます。 • **資産 ID** - 資産の UUID。 • **ライセンス済み** - 資産がライセンスされているかどうかを示します。 • **システムタイプ** - プラグイン ID 54615 によって報告されるシステムタイプ。詳細は、Tenableプラグインを参照してください。 • **IPv4 アドレス** - 資産の IPv4 アドレス。IPv4 アドレスがない場合は、資産の最初の IPv6。 • **パブリック** - 資産がパブリックネットワークで使用可能かどうかを指定します。パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Management クエリ名前空間の `is_public` 属性によって識別されます。 • **DNS** - 資産ホストの完全修飾ドメイン名。 • **オペレーティングシステム** - スキャンによって資産にインストールされていると識別されたオペレーティングシステム。 • **ネットワーク** - 資産を識別したスキャナーに関連付けられたネットワークオブジェクトの名前。デフォルトのネットワーク名は **[Default]** です。詳細は、ネットワークを参照してください。 • **MAC アドレス** - 資産の静的メディアアクセス制御 (MAC) アドレス。 • **SSH フィンガープリント** - スキャンによって資産レコードに関連付けられた SSH キーのフィンガープリント。 • **Tenable UUID** - 資産に関連付けられている Tenable アカウントの一意の識別子。 • **カスタム属性** - 資産に追加されたカスタム属性。詳細は、Tenable 開発者ポータルを参照してください。
検出結果	資産に関連付けられたすべての検出結果を一覧表示する表。このセクションでは、次のアクションを実行できます。 • 選択された検出結果をエクスポートします。

	• **[検出結果で開く]** をクリックすると、資産の [脆弱性] ページが表示されます。
資産のエクスポージャースコア	(Tenable Lumin ライセンスが必要) 資産の資産のエクスポージャースコアを示す説明アイコン。
ACR (資産重大度の格付け)	(Tenable Lumin ライセンスが必要) 資産の ACR (資産重大度の格付け) を示す説明アイコン。
利用可能なスクリーンショット	スクリーンショットが使用可能かどうかを示すインタラクティブなボタンです。スクリーンショットを表示するには、📷 ボタンをクリックします。
タグ	資産に適用されるタグです。タグを追加するには、⊕ ボタンをクリックします。タグを削除するには、タグラベルの ✕ ボタンをクリックします。詳細は、タグ を参照してください。
スキャンの情報	資産のスキャン履歴に関する情報です。次の情報が含まれます。 • **初回確認日** - スキャンが最初に資産を特定した日時。 • **最終確認日** - スキャンの際に資産が最後に確認された日時。 • **ソース** - 資産を特定したスキャンのソースです。
アクション	右上の **[アクション]** ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 • **エクスポート** - 調査の表からのエクスポート で説明されているように、CSV または JSON にエクスポートします。 • **タグの追加** - 新しいタグを追加します。表示されたダイアログで、タグ で説明されているように、*[カテゴリ]* と *[値]* を選択します。 • **タグの削除** - 既存のタグを削除します。表示されたダイアログでタグをクリックし、**[削除]** をクリックします。 • **すべての詳細を表示** – 資産の詳細の表示 で説明されているように、資産の詳

	細をすべて表示します。 • **新しいタブですべての詳細を表示** – 資産の完全な詳細をブラウザの新しいタブに表示します。 • **削除** - 資産の削除で説明されているように、資産を完全に削除します。

ドメインインベントリのプレビュー

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[資産] ワークベンチでドメインインベントリ資産をクリックすると、その詳細をプレビューできます。

プレビューには次のセクションが含まれています。

セクション	説明
ヘッダー	資産ヘッダー。特定の属性の存在に基づいて次の論理順序で表示されます。 1. エージェント名 2. NetBIOS 名 3. ローカルホスト名 4. ホスト完全修飾ドメイン名 (FQDN) 5. IPv4 アドレス 6. IPv6 アドレス
タグ	資産に適用されるタグです。タグを追加するには、⊕ ボタンをクリックします。タグを削除するには、タグラベルの × ボタンをクリックします。詳細は、タグ を参照してください。
資産情報	資産に関する情報です。次のものが含まれます。 • **資産 ID** - 資産の UUID。 • **ライセンス済み** - 資産がライセンスされているかどうかを示します。 • **IPv4 アドレス** - 資産の IPv4 アドレス。 • **IPV6 アドレス** - 資産の IPv6 アドレス。
資産スキャン情報	資産のスキャン履歴に関する情報です。次の情報が含まれます。 • **初回確認日** - スキャンが最初に資産を特定した日時。 • **最終確認日** - スキャンの際に資産が最後に確認された日時。

	• **更新日付** - 資産レコードが最後に更新された日時です。 • **ソース** - 資産を特定したスキャンのソースです。
関連資産	フィルターされた資産のリストへのリンク。Tenable Vulnerability Management スキャンが資産を識別した別の機会の結果を表示します。

資産フィルター

注意: このトピックでは、調査 セクション内の資産で利用可能なフィルターについて説明します。レガシーワークベンチの資産に利用できるフィルターを表示するには、Legacy Workbench Asset Filtersを参照してください。

[資産] ページで、すべての資産に適用される標準フィルターを使って、または、資産固有のフィルターを使って、資産をフィルタリングできます。

よく使用するフィルターのセットを保存済みフィルターとして保存し、後でアクセスしたり、チームの他のメンバーと共有したりできます。

注意: パフォーマンスを最適化するために、Tenable では **[調査]** > **[資産]** ビュー (**[グループ化]** 表を含む) に適用できるフィルターの数を 35 個に制限しています。

注意: 表のセル内の値を右クリックして、**[フィルター]** オプションを使用することができます。詳細については、右クリックでフィルターを参照してください。

次のフィルタータイプの中から選択できます。

すべて

次の表で、すべての資産に適用されるフィルターについて説明します。

フィルター	説明
アカウント ID	資産をホストするクラウドサービスの資産リソースに割り当てられた一意の識別子。
ACR	(Tenable Lumin のライセンスが必要) 資産の ACR。
ACR の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された ACR の ACR カテゴリ。
AES	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES (資産のエクスポージャースコア)。
AES の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES の AES カテゴリ。
エージェント名	資産をスキャンして特定した、Tenable Nessus エージェントの名前。

ARN	資産の Amazon リソース名 (ARN)。
ASN	資産の自律システム番号 (ASN)。
[評価済み]と[検出済み]	Tenable Vulnerability Management が資産の脆弱性をスキャンしたかどうか、または Tenable Vulnerability Management が検出スキャンで資産を検出しただけかどうかを指定します。可能な値は次のとおりです。 • **評価済み** • **検出済みのみ** **注意:** このフィルターはデフォルトで選択されています。
資産 ID	資産の UUID。
AWS 可用性ゾーン	AWS が仮想マシンインスタンスをホストしているアベイラビリティゾーンの名前。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS EC2 AMI ID	Amazon Elastic Compute Cloud (Amazon EC2) での、Linux AMI イメージの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 インスタンス ID	Amazon EC2 での Linux インスタンスの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 名	Amazon EC2 での仮想マシンインスタンスの名前。
AWS EC2 製品コード	Amazon EC2 での仮想マシンインスタンスの立ち上げに使用された AMI に関連付けられた製品コード。
AWS インスタンスの状態	AWS での仮想マシンインスタンスのスキャン時の状態。可能な値については、Amazon Elastic Compute Cloud ドキュメントの API インスタンスの状態を参照してください。
AWS インスタンスタイプ	Amazon EC2 での仮想マシンインスタンスのタイプ。Amazon EC2 のインスタンスタイプは、インスタンスの仕様を決定します (たとえば、どのくらいの RAM を持つか)。可能な値の一覧は、AWS ドキュメントの Amazon EC2 インスタンスタイプを参照してください。

AWS 所有者 ID	仮想マシンインスタンスを作成した Amazon AWS アカウントの UUID。詳細は、AWS ドキュメントの AWS アカウント ID を参照してください。 この属性は、Amazon EC2 インスタンスのみに対して値を持ちます。他の資産タイプに対しては、この属性は空となります。
AWS リージョン	たとえば `us-east-1` などの、AWS が仮想マシンインスタンスをホストするリージョン。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS セキュリティグループ	Amazon EC2 インスタンスに関連付けられた AWS セキュリティグループ (SG)。
AWS サブネット ID	スキャン時に仮想マシンインスタンスが動作していた、AWS サブネットの固有識別子。
AWS VPC ID	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、Amazon Virtual Private Cloud ユーザーガイドを参照してください。
Azure ロケーション	Azure Resource Manager でのリソースの場所。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソースグループ	Azure Resource Manager でのリソースグループの名前。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソース ID	Azure Resource Manager での、リソースの固有識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソースタイプ	Azure Resource Manager でのリソースのリソースタイプ。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure サブスクリプション ID	Azure Resource Manager でのリソースの固有サブスクリプション識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure VM ID	Microsoft Azure 仮想マシンインスタンスの固有識別子。詳細は、Microsoft Azure ドキュメントの Azure VM Unique ID のアクセスと使用を参照してください。
BIOS ID	資産の NetBIOS 名。
クラウドプロバイ	資産をホストするクラウドプロバイダーの名前。

ダー	
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
カスタム属性	カテゴリと値のペアを使用してカスタム属性を検索するフィルター。カスタム属性の詳細については、Tenable 開発者ポータルを参照してください。
DNS	脆弱性が検出されたホストの完全修飾ドメイン名。
ドメイン	資産が属するドメイン
初回確認日	スキャンが最初に資産を特定した日時。
Google Cloud Instance	Google Cloud Platform (GCP) での、仮想マシンインスタンスの固有識別子。
Google Cloud プロジェクト ID	GCP で、仮想マシンインスタンスが所属するプロジェクトのカスタマイズされた名前。詳細は、GCP ドキュメントのプロジェクトの作成と管理を参照してください。
Google Cloud ゾーン	GCP で、仮想マシンインスタンスが動作しているゾーン。詳細は、GCP ドキュメントのリージョンとゾーンを参照してください。
プラグインの結果有り	資産が関連付けられたプラグイン結果を持つかどうかを指定します。
ホスト名 (ドメインインベントリ)	アタックサーフェス管理スキャン中に検出された資産のホスト名。ドメインインベントリ資産でのみ使用されます。
ホスティングプロバイダー	資産のホスティングプロバイダー。
IaC リソースタイプ	資産のインフラのコード化 (IAC) リソースタイプ。
インストール済みのソフトウェア	スキャンにより資産上に存在が確認されたソフトウェアアプリケーションを表す、共通プラットフォーム一覧 (CPE) の値。このフィールドは CPE 2.2 形式に対応します。詳細は、CPE 仕様書バージョン 2.2 の Component Syntax セクションを参照してください。Tenable スキャンで特定された資産に関して、このフィールドは、Tenable Nessus プラグイン ID 45590 を使用するスキャンが資産を評価した場合にのみ値を持ちます。

	注意：アプリケーションが検出された最初のスキャンから 30 日の間に、そのアプリケーションを検出するスキャンがなかった場合、Tenable Vulnerability Management はそのアプリケーションの検出を期限切れとみなします。その結果、次にその資産をスキャンで評価する際、Tenable Vulnerability Management は期限切れとなったアプリケーションを **[インストール済みソフトウェア]** 属性から削除します。このアクティビティは、削除の種類の属性変更として資産アクティビティログに記録されます。
IPV4 アドレス	資産レコードに関連付けられた IPv4 アドレス。
IPV6 アドレス	資産レコードに関連付けられた IPv6 アドレス。
属性	資産が属性であるかどうかを指定します。
自動スケール	資産を自動的にスケーリングするかどうかを指定します。
サポートなし	Tenable Vulnerability Management で資産がサポートされていないかどうかを指定します。
最終監査日	資産が最後に監査された日時。
最終認証スキャン日	資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。
最終ライセンススキャン日	資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。
最終スキャン時間	資産に対してスキャンが最後に実行された日付。
最終確認日	スキャンの際に資産が最後に確認された日時。
ライセンス済み	資産が Tenable Vulnerability Management インスタンスの資産カウントに含まれるかどうかを規定します。
MAC アドレス	スキャンにより資産レコードと関連付けられた MAC アドレス。

緩和済み	スキャンによって資産の軽減ソフトウェアが識別されたかどうかを指定します。
Mitigation Last Detection	資産の軽減ソフトウェアを最後に識別したスキャンの日時です。
緩和製品名	資産で識別された軽減ソフトウェアの名前Tenable Lumin は、エンドポイント資産上で実行されるセキュリティエージェントソフトウェアとして緩和策を定義します。これには、アンチウイルスソフトウェア、エンドポイント保護プラットフォーム (EPP)、またはエンドポイント検知・対応 (EDR) ソリューションが含まれます。
緩和ベンダー名	スキャンが資産で識別した緩和策のベンダーの名前です。
緩和バージョン	スキャンが資産で識別した緩和策のバージョンです。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。 **注意:** このフィルターはデフォルトで選択されています。

NetBIOS 名	資産の NetBIOS 名。
ネットワーク	資産を特定したスキャナーに関連付けられているネットワークオブジェクトの名前。デフォルトの名前は **Default** です。詳細は、ネットワークを参照してください。
開いているポート	資産で、値または範囲と等しい(または等しくない)開いているポートが検出されました。
オペレーティングシステム	スキャンにより資産にインストールされていると特定されたオペレーティングシステム。 **注意:** このフィルターはデフォルトで選択されています。
オペレーティングシステム(WAS)	資産にインストールされているとスキャンで特定された Tenable Web App Scanning (Tenable Web App Scanning) オペレーティングシステム。
パブリック	資産がパブリックネットワークで使用可能かどうかを指定します。パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Managementクエリ名前空間の `is_public` 属性によって識別されます。
レコードタイプ	資産タイプ。
リージョン	資産が実行されるクラウドリージョン。
リポジトリ	資産に関連付けられているコードリポジトリ。
リソースタイプ	資産のクラウドリソースタイプ(ネットワーク、仮想マシンなど)。 **注意:** このフィルターはデフォルトで選択されています。
スキャン頻度	過去 90 日間で、資産がスキャンされた回数。
ServiceNow Sys ID	該当する場合、ServiceNow での資産の固有レコード識別子。詳細は、ServiceNow のドキュメントを参照してください。
ソース	資産を特定したスキャンのソース。可能な値は次のとおりです。 • AWS • AWS FA

	• Azure • AZURE FA • Cloud Connector • Cloud IAC • クラウドランタイム • GCP • Nessus Agent • Nessus Scan • NNM • ServiceNow • WAS **注意:** このフィルターはデフォルトで選択されています。
SSL/TLS	資産がホストされているアプリケーションが SSL/TLS 公開鍵暗号化を使用するかどうかを指定します。
システムの種類	プラグイン ID 54615 によりレポートされたシステムの種類。詳細は、Tenableプラグインを参照してください。
タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。

	注意: このフィルターはデフォルトで選択されています。
ターゲットグループ	資産が所属するターゲットグループ。資産がターゲットグループに所属していない場合、この属性は空になります。詳細は、ターゲットグループを参照してください。
Tenable ID	Tenable Vulnerability Management での資産の UUID。
終了	資産が終了しているかどうかを指定します。
タイプ	資産が管理されているシステムのタイプ。可能なオプションは次のとおりです。 • **クラウドリソース** • **コンテナ** • **ホスト** • **クラウド** **注意:** このフィルターはデフォルトで選択されています。

ホスト資産

次の表では、ホスト資産のフィルターについて説明します。

フィルター	説明
ACR	(Tenable Lumin のライセンスが必要) 資産の ACR。
ACR の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された ACR の ACR カテゴリ。
AES	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES (資産のエクスポージャースコア)。
AES の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES の AES カテゴリ。
エージェント名	資産をスキャンして特定した、Tenable Nessus エージェントの名前。

資産 ID	資産の UUID。
AWS 可用性ゾーン	AWS が仮想マシンインスタンスをホストしているアベイラビリティゾーンの名前。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS EC2 AMI ID	Amazon Elastic Compute Cloud (Amazon EC2) での、Linux AMI イメージの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 インスタンス ID	Amazon EC2 での Linux インスタンスの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 名	Amazon EC2 での仮想マシンインスタンスの名前。
AWS EC2 製品コード	Amazon EC2 での仮想マシンインスタンスの立ち上げに使用された AMI に関連付けられた製品コード。
AWS インスタンスの状態	AWS での仮想マシンインスタンスのスキャン時の状態。可能な値については、Amazon Elastic Compute Cloud ドキュメントの API インスタンスの状態を参照してください。
AWS インスタンスタイプ	Amazon EC2 での仮想マシンインスタンスのタイプ。Amazon EC2 のインスタンスタイプは、インスタンスの仕様を決定します (たとえば、どのくらいの RAM を持つか)。可能な値の一覧は、AWS ドキュメントの Amazon EC2 インスタンスタイプを参照してください。
AWS 所有者 ID	仮想マシンインスタンスを作成した Amazon AWS アカウントの UUID。詳細は、AWS ドキュメントの AWS アカウント ID を参照してください。 この属性は、Amazon EC2 インスタンスのみに対して値を持ちます。他の資産タイプに対しては、この属性は空となります。
AWS リージョン	たとえば `us-east-1` などの、AWS が仮想マシンインスタンスをホストするリージョン。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS セキュリティグループ	Amazon EC2 インスタンスに関連付けられた AWS セキュリティグループ (SG)。

AWS サブネット ID	スキャン時に仮想マシンインスタンスが動作していた、AWS サブネットの固有識別子。
AWS VPC ID	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、Amazon Virtual Private Cloud ユーザーガイドを参照してください。
Azure ロケーション	Azure Resource Manager でのリソースの場所。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソースグループ	Azure Resource Manager でのリソースグループの名前。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソース ID	Azure Resource Manager での、リソースの固有識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソースタイプ	Azure Resource Manager でのリソースのリソースタイプ。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure サブスクリプション ID	Azure Resource Manager でのリソースの固有サブスクリプション識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure VM ID	Microsoft Azure 仮想マシンインスタンスの固有識別子。詳細は、Microsoft Azure ドキュメントの Azure VM Unique ID のアクセスと使用を参照してください。
BIOS ID	資産の NetBIOS 名。
クラウドプロバイダー	資産のクラウドプロバイダー(AWS、Azure、または GCP)。 **注意:** インポートされたタグでリソースを検索するには、**[ソース]** の代わりに **[クラウドプロバイダー]** でフィルタリングします。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
カスタム属性	カテゴリと値のペアを使用してカスタム属性を検索するフィルター。カスタム属性の詳細については、Tenable 開発者ポータルを参照してください。
DNS	脆弱性が検出されたホストの完全修飾ドメイン名。
ドメイン	資産が属するドメイン

初回確認日	スキャンが最初に資産を特定した日時。
Google Cloud Instance	Google Cloud Platform (GCP) での、仮想マシンインスタンスの固有識別子。
Google Cloud プロジェクト ID	GCP で、仮想マシンインスタンスが所属するプロジェクトのカスタマイズされた名前。詳細は、GCP ドキュメントのプロジェクトの作成と管理を参照してください。
Google Cloud ゾーン	GCP で、仮想マシンインスタンスが動作しているゾーン。詳細は、GCP ドキュメントのリージョンとゾーンを参照してください。
プラグインの結果有り	資産が関連付けられたプラグイン結果を持つかどうかを指定します。
インストール済みのソフトウェア	スキャンにより資産上に存在が確認されたソフトウェアアプリケーションを表す、共通プラットフォーム一覧 (CPE) の値。このフィールドは CPE 2.2 形式に対応します。詳細は、CPE 仕様書バージョン 2.2 の Component Syntax セクションを参照してください。Tenable スキャンで特定された資産に関して、このフィールドは、Tenable Nessus プラグイン ID 45590 を使用するスキャンが資産を評価した場合にのみ値を持ちます。 **注意:** アプリケーションが検出された最初のスキャンから 30 日の間に、そのアプリケーションを検出するスキャンがなかった場合、Tenable Vulnerability Management はそのアプリケーションの検出を期限切れとみなします。その結果、次にその資産をスキャンで評価する際、Tenable Vulnerability Management は期限切れとなったアプリケーションを **[インストール済みソフトウェア]** 属性から削除します。このアクティビティは、削除の種類の属性変更として資産アクティビティログに記録されます。
IPv4 アドレス	資産レコードに関連付けられた IPv4 アドレスです。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します (例: hostname_example, example.com, 192.168.0.0)。IP アドレスには、個別のアドレス、CIDR 表記 (例: 192.168.0.0/24)、または範囲 (例: 192.168.0.1-192.168.0.255) を指定できます。 **注意:** このパラメーターで CIDR マスク /0 を指定するとすべての IP アドレスに適合するので、Tenable Vulnerability Management ではこの値がサポートされていません。このパラメーターに値 /0 を指定すると、Tenable Vulnerability

	Management は 400 Bad Request エラーメッセージを返します。 **注意:** フィルター値の最後にピリオド「.」は付けないでください。
IPv6 アドレス	スキャンにより資産レコードと関連付けられた IPv6 アドレス。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します。IPV6 アドレスは完全に一致する必要があります (例: 0:0:0:0:0:ffff:c0a8:0)。 **注意:** フィルター値の最後にピリオド「.」は付けないでください。
最終認証スキャン日	資産で直近で実行された認証スキャンの日時です。
最終ライセンススキャン日	資産がライセンスされていると識別された最後のスキャン日時ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。
最終確認日	スキャンの際に資産が最後に確認された日時。 **注意:** このフィルターはデフォルトで選択されています。
ライセンス済み	資産が Tenable Vulnerability Management インスタンスの資産カウントに含まれるかどうかを規定します。 **注意:** このフィルターはデフォルトで選択されています。
MAC アドレス	スキャンにより資産レコードと関連付けられた MAC アドレス。
緩和済み	スキャンによって資産の軽減ソフトウェアが識別されたかどうかを指定します。
Mitigation Last Detection	資産の軽減ソフトウェアを最後に識別したスキャンの日時です。
緩和製品名	資産で識別された軽減ソフトウェアの名前Tenable Lumin は、エンドポイント資産上で実行されるセキュリティエージェントソフトウェアとして緩和策を定義します。これには、アンチウイルスソフトウェア、エンドポイント保護プラッ

	トフォーム (EPP)、またはエンドポイント検知・対応 (EDR) ソリューションが含まれます。
緩和ベンダー名	スキャンが資産で識別した緩和策のベンダーの名前です。
緩和バージョン	スキャンが資産で識別した緩和策のバージョンです。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。 **注意:** このフィルターはデフォルトで選択されています。
NetBIOS 名	資産の NetBIOS 名。
ネットワーク	資産を特定したスキャナーに関連付けられているネットワークオブジェクトの名前。デフォルトの名前は **Default** です。詳細は、ネットワークを参照してください。

オペレーティングシステム	スキャンにより資産にインストールされていると特定されたオペレーティングシステム。
パブリック	資産がパブリックネットワークで使用可能かどうかを指定します。パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Managementクエリ名前空間の `is_public` 属性によって識別されます。
リソースタグ(キー別	クラウドプロバイダーからインポートするタグまたはラベルの、キーと値のペアのキー。
リソースタグ(値別	クラウドプロバイダーからインポートするタグまたはラベルの、キーと値のペアの値。
スキャン頻度	過去 90 日間で、資産がスキャンされた回数。
ServiceNow Sys ID	該当する場合、ServiceNow での資産の固有レコード識別子。詳細は、ServiceNow のドキュメントを参照してください。
ソース	資産を特定したスキャンのソース。可能な値は次のとおりです。 • AWS • AWS FA • Azure • Azure FA • クラウド検出コネクタ **注意:** Tenable Vulnerability Management は、インポートされたリソースタグを持つコンピューティング資産についてこのソースを表示します。 • 既存の資産の場合、**[ソース]** 列には既存のソース(AWS、Azure、または GCP)とともに**クラウド検出コネクタ**が表示されます。 • 新しい資産の場合、**[ソース]** 列には**クラウド検出コネクタ**が表示されます。 資産のインポート元は、**[クラウドプロバイダー]** 列で確認できます。 **警告**: 現在、AWS、GCP、または Azure をソースとして利用しているクエリがある場合は、これらのクエリを更新する必要があります。**クラウド検出コ**

	ネクタのソースは、AWS、GCP、および Azure のソースに取って代わりました。さらに、資産のソースの場合は、**[クラウドプロバイダー]** パラメーターを使用して AWS、Azure、または GCP を示します。 • クラウド IaC • クラウドランタイム • GCP • Nessus Agent • Nessus Scan • NNM • ServiceNow • WAS **注意:** このフィルターはデフォルトで選択されています。
システムの種類	プラグイン ID 54615 によりレポートされたシステムの種類。詳細は、Tenable プラグインを参照してください。
タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。 **注意:** このフィルターはデフォルトで選択されています。
ターゲットグループ	資産が所属するターゲットグループ。資産がターゲットグループに所属していない場合、この属性は空になります。詳細は、ターゲットグループを参照

	してください。
Tenable ID	資産に存在するエージェントの UUID。
終了	資産が終了しているかどうかを指定します。
更新日	資産レコードが最後に更新された日時。

クラウドリソース資産

次の表では、クラウドリソースのフィルターについて説明します。

オプション	説明
アカウント ID	資産に関連付けられているアカウント ID。
ARN	資産の Amazon リソース名 (ARN)。
資産 ID	資産の UUID。
クラウドプロバイダー	資産をホストするクラウドプロバイダーの名前。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
初回確認日	スキャンが最初に資産を特定した日時。
IaC リソースタイプ	資産のインフラのコード化 (IAC) リソースタイプ。
属性	資産が属性であるかどうかを指定します。
自動スケール	資産を自動的にスケーリングするかどうかを指定します。
サポートなし	Tenable Vulnerability Management で資産がサポートされていないかどうかを指定します。

最終監査日	Tenable Vulnerability Management が資産を最後に審査した日時です。
最終ライセンススキャン日	資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。
最終確認日	スキャンの際に資産が最後に確認された日時。
ライセンス済み	資産が Tenable Vulnerability Management インスタンスの資産カウントに含まれるかどうかを規定します。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。

	注意: このフィルターはデフォルトで選択されています。
リージョン	資産が実行されるクラウドリージョン。
リポジトリ	資産に関連付けられているコードリポジトリ。
リソースカテゴリ	資産をホストするクラウドサービスの資産リソースのカテゴリ。
リソースタグ(キー別)	Amazon Web Services (AWS) などのクラウドソースから同期され、タグキー (Name など) と一致するタグ。個々の検索項目をコンマで区切ります。ワイルドカード (*) を使用して、文字列に等しい、文字列で始まる/終わる、または文字列の一部を含むキーを検索します。または、タグ付きまたはタグなしの資産を検索します。
リソースタグ(値別)	Amazon Web Services (AWS) などのクラウドソースから同期され、タグ値と一致するタグ。個々の検索項目をコンマで区切ります。ワイルドカード (*) を使用して、文字列に等しい、文字列で始まる/終わる、または文字列の一部を含む値を検索します。または、タグ付きまたはタグなしの資産を検索します。
リソースタイプ	資産のクラウドリソースタイプ (ネットワーク、仮想マシンなど)。 **注意:** このフィルターはデフォルトで選択されています。
ソース	資産を特定したスキャンのソース。可能な値は次のとおりです。 • **Cloud IaC** • **クラウドランタイム** **注意:** このフィルターはデフォルトで選択されています。
タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。

	注意: タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。 **注意:** このフィルターはデフォルトで選択されています。

ウェブアプリケーション資産

次の表では、ウェブアプリケーション資産のフィルターについて説明します。

フィルター	説明
ACR	(Tenable Lumin のライセンスが必要) 資産の ACR。
ACR の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された ACR の ACR カテゴリ。
AES	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES の AES カテゴリ。
AES の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES の AES カテゴリ。
資産 ID	資産の UUID。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
カスタム属性	カテゴリと値のペアを使用してカスタム属性を検索するフィルター。カスタム属性の詳細については、Tenable 開発者ポータルを参照してください。
初回確認日	スキャンが最初に資産を特定した日時。
最終認証スキャン日	資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。
最終ライセンススキャン日	資産にライセンスがあると識別された直近のスキャン日時。ライセンスのある資産に関する詳細は、ライセンス情報 を参照してください。
最終確認日	スキャンの際に資産が最後に確認された日時。

	注意: このフィルターはデフォルトで選択されています。
ライセンス済み	資産が Tenable Web App Scanning インスタンスの資産カウントに含まれるかどうかを規定します。 資産は以下の条件を満たす場合にライセンス付与されます。 • 資産のスキャン結果に検出プラグインの結果が含まれていない • 資産のスキャン結果に Tenable Web App Scanning のソース (Tenable Nessus スキャナー、エージェント、Tenable Nessus Network Monitor の結果など) が含まれていない • 資産が終了していない
緩和済み	スキャンによって資産の軽減ソフトウェアが識別されたかどうかを指定します。
最後に検出された緩和策	資産の軽減ソフトウェアを識別した直近のスキャン日時。
緩和製品名	資産で識別された軽減ソフトウェアの名前Tenable Lumin は、エンドポイント資産上で実行されるセキュリティエージェントソフトウェアとして緩和策を定義します。これには、アンチウィルスソフトウェア、エンドポイント保護プラットフォーム (EPP)、またはエンドポイント検知・対応 (EDR) ソリューションが含まれます。
緩和バージョン	スキャンが資産で識別した軽減ソフトウェアのバージョン。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名

	7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名 10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。 **注意:** このフィルターはデフォルトで選択されています。
オペレーティングシステム (WAS)	スキャンにより資産にインストールされていると特定されたオペレーティングシステム。
パブリック	資産がパブリックネットワークで使用可能かどうかを指定します。 **注意:** パブリック資産はパブリック IP 空間内にあり、Tenable Vulnerability Management クエリ名前空間の `is_public` 属性によって識別されます。
ソース	資産を特定したスキャンのソース。可能な値は次のとおりです。 • **ASM** • **AWS** • **AWS FA** • **Azure** • **Azure FA** • **Cloud IAC** **注意:** このフィルターはデフォルトで選択されています。
SSL/TLS	資産がホストされているアプリケーションが SSL/TLS 公開鍵暗号化を使用するかどうかを指定します。

タグ	タグのペア(カテゴリ: 値)を検索する一意のフィルター。タグの値を入力するときは、コロン(:)の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ(,)を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ(\)を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。 **注意:** このフィルターはデフォルトで選択されています。
更新日	資産レコードが最後に更新された日時。

ドメインインベントリ資産

次の表では、ドメインインベントリ資産のフィルターについて説明します。

フィルター	説明
ASN	資産の自律システム番号 (ASN)。
資産 ID	資産の UUID。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
DNS (FQDN)	脆弱性が検出されたホストの完全修飾ドメイン名。
ドメイン	資産のドメイン名。
ホスト名	資産のホスト名。この文字列は、ターゲットのプラグインによって報告される情報によって決定され、ユーザーの環境と設定に依存します。
ホスティングプロバイダー	資産のホスティングプロバイダー。
IPv4 アドレス	資産レコードに関連付けられた IPv4 アドレスです。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します (例: hostname_example, example.com, 192.168.0.0)。IP アドレスには、個別のアドレ

	ス、CIDR 表記 (例: 192.168.0.0/24)、または範囲 (例: 192.168.0.1-192.168.0.255) を指定できます。 **注意:** このパラメーターで CIDR マスク /0 を指定するとすべての IP アドレスに適合するので、Tenable Vulnerability Management ではこの値がサポートされていません。このパラメーターに値 /0 を指定すると、Tenable Vulnerability Management は 400 Bad Request エラーメッセージを返します。 **注意:** フィルター値の最後にピリオド「.」は付けないでください。
IPv6 アドレス	スキャンにより資産レコードと関連付けられた IPv6 アドレス。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します。IPV6 アドレスは完全に一致する必要があります (例: 0:0:0:0:0:ffff:c0a8:0)。 **注意:** フィルター値の最後にピリオド「.」は付けないでください。
最終確認日	スキャンの際に資産が最後に確認された日時。
ライセンス済み	資産が Tenable Vulnerability Management インスタンスの資産カウントに含まれるかどうかを規定します。
名前	特定の属性の存在に基づき次の論理順序で割り当てられる資産 ID です。 1. Nessus Agent 名 2. ホスト名 3. ウェブアプリのホスト名 4. コンテナセキュリティ画像名 5. コンテナランタイムのホスト名 6. クラウド共通リソース名 7. クラウド共通リソース識別子 8. クラウドランタイム名 9. クラウド IAC 名

	10. Active Directory 資産名 11. ドメインレコードのホスト名 上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。 **注意:** このフィルターはデフォルトで選択されています。
ポート	資産に関連付けられたポート (開いているか閉じているか)。ドメインインベントリ資産にのみ適用されます。
レコードタイプ	資産のタイプ。
ソース	資産を特定したスキャンのソース。可能な値は次のとおりです。 • **ASM** • **AWS** • **AWS FA** • **Azure** • **Azure FA** • **Cloud IAC** **注意:** このフィルターはデフォルトで選択されています。
タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。
更新日	資産レコードが最後に更新された日時。

オープンポートと資産ワークベンチ

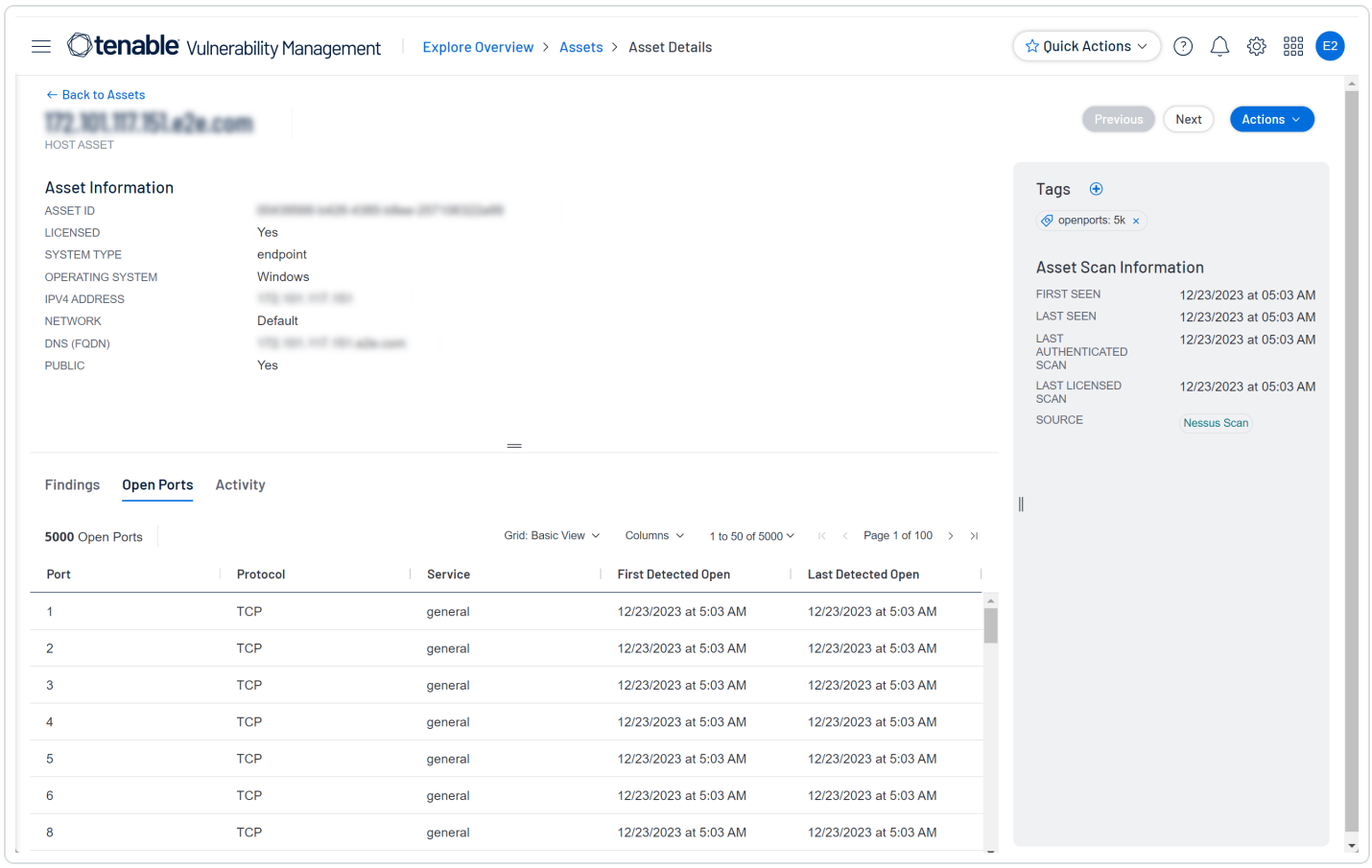
注意: 所属する組織で **[開いているポートの検出結果を再配置する]** をまだ有効にしていない場合、これらの機能は表示されません。ただし、今後数週間のうちにこれらがシステムのデフォルトになります。

注意: **[開いているポートの検出結果を再配置する]** を有効にすると、開いているポートが個別の検出結果として保存されなくなるため、サードパーティ統合で開いているポートの検出結果を受け取ることができなくなります。

注意: **[資産の詳細]** ページに移動する前に実行されたスキャンによる開いているポートの検出結果は、**[検出結果]** ワークベンチに一時的に表示される場合があります。開いているポートの新しい検出結果は、そこには表示されません。

ヒント: オープンポートと Tenable Vulnerability Management API の詳細については、*Tenable 開発者ポータル*の API 変更ログを参照してください。詳細については、Tenable カスタマーサポートにお問い合わせください。

Tenable Vulnerability Management は、開いているポートの検出結果を **[資産の詳細]** ページに表示します。このページは、**[資産]** ワークベンチでホスト資産をクリックし、**[すべての詳細の表示]** をクリックすると表示されます。**[資産の詳細]** ページの **[オープンポート]** タブには、資産で開いているポートが表示され、ポートプロトコル、ポートが開いていることが最初と最後に検出された日時、ポートで実行中のサービスの情報も表示されます。


tenable Vulnerability Management
Explore Overview > Assets > Asset Details
Quick Actions
E2
← Back to Assets
172.101.117.151.e2e.com
HOST ASSET
Previous
Next
Actions
Asset Information
ASSET ID
LICENSED Yes
SYSTEM TYPE endpoint
OPERATING SYSTEM Windows
IPV4 ADDRESS
NETWORK Default
DNS (FQDN)
PUBLIC Yes
Tags
openports: 5k
Asset Scan Information
FIRST SEEN 12/23/2023 at 05:03 AM
LAST SEEN 12/23/2023 at 05:03 AM
LAST AUTHENTICATED SCAN 12/23/2023 at 05:03 AM
LAST LICENSED SCAN 12/23/2023 at 05:03 AM
SOURCE Nessus Scan
Findings
Open Ports
Activity
5000 Open Ports
Grid: Basic View
Columns
1 to 50 of 5000
Page 1 of 100
Port
Protocol
Service
First Detected Open
Last Detected Open
1 TCP general 12/23/2023 at 5:03 AM 12/23/2023 at 5:03 AM
2 TCP general 12/23/2023 at 5:03 AM 12/23/2023 at 5:03 AM
3 TCP general 12/23/2023 at 5:03 AM 12/23/2023 at 5:03 AM
4 TCP general 12/23/2023 at 5:03 AM 12/23/2023 at 5:03 AM
5 TCP general 12/23/2023 at 5:03 AM 12/23/2023 at 5:03 AM
6 TCP general 12/23/2023 at 5:03 AM 12/23/2023 at 5:03 AM
8 TCP general 12/23/2023 at 5:03 AM 12/23/2023 at 5:03 AM

オープンポートの操作

以下の機能を使用して、オープンポートデータの検索、管理、エクスポートを行います。

- **[オープンポート] フィルター** - **[資産]** ワークベンチで、ホスト資産で開いているポートを検索します。
- **[オープンポート] タグルール** - **[資産]** ワークベンチで、開いているポートにタグを追加します。
- **[オープンポート] エクスポートフィールド** - カスタムフィールドを使用して、**[資産]** ワークベンチから開いているポートのデータをエクスポートします。

サポートされているプラグイン

[オープンポート] タブには、次の高トラフィックプラグインからの出力が表示されます。

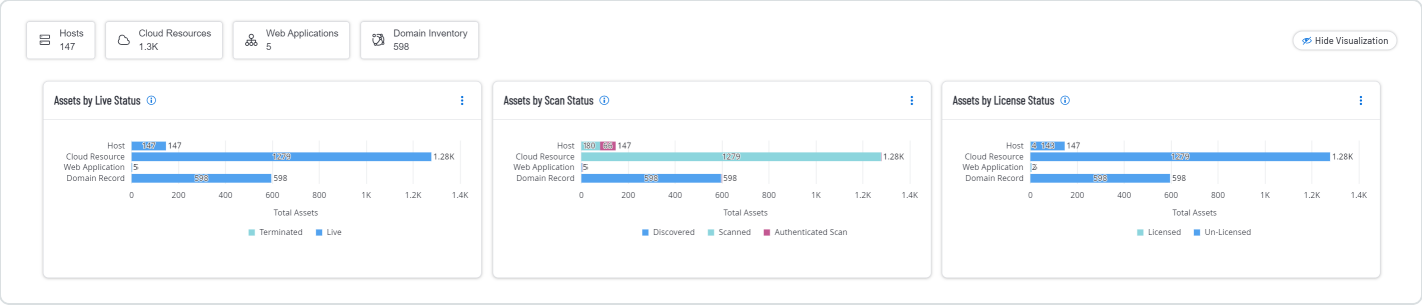
- 34220 - Netstat Portscanner (WMI)
- 34252 - Microsoft Windows リモートリスナーの列挙 (WMI)
- 11219 - Nessus SYN スキャナー
- 14272 - Netstat Portscanner (SSH)
- 25221 - リモートリスナーの列挙 (Linux / AIX)
- 10736 - DCE サービスの列挙
- 99265 - macOS リモートリスナーの列挙
- 10335 - Nessus TCP スキャナー
- 14274 - Nessus SNMP スキャナー
- 34277 - Nessus UDP スキャナー

資産ビジュアライゼーションの表示

[資産] ページではインタラクティブなビジュアライゼーションを表示できます。その際、資産を複数のメトリクスで分類し、フィルターを適用して自動的に更新することができます。またビジュアライゼーションを PDF、JPG、または PNG にエクスポートすることもできます。

- 資産ビジュアライゼーションを表示するには、**[資産]** ページの右側にある **[ビジュアライゼーションを表示]** をクリックします。

- 資産ビジュアライゼーションを非表示にするには、**[資産]** ページの右側にある **[ビジュアライゼーションを非表示]** をクリックします。



ビジュアライゼーションのタイプ

次の表では、**[資産]** ページのビジュアライゼーションについて説明します。

ウィジェット	説明
ライブステータス別の資産	資産をタイプ別にグループ化し、資産が**[ライブ]**と**[終了]**のいずれであるかを示します。このメトリクスは、特にクラウド資産に関連しています。
スキャンステータス別の資産	資産をタイプ別にグループ化し、資産が**検出済み**であるがスキャンされていないか、**スキャン済み**であるが認証されていないか、あるいは**認証スキャン**を受信済みであるかを示します。
ライセンスステータス別の資産	資産をタイプ別にグループ化し、資産が**ライセンス済み**であるか**ライセンスなし**であるかを示します。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。

ビジュアライゼーションのエクスポート

ビジュアライゼーションを PDF、JPG、または PNG にエクスポートできます。

ビジュアライゼーションをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある**[調査]**セクションで、**[資産]**をクリックします。

   [資産]ページが表示されます。

3. ページの右側にある**[ビジュアライゼーションを表示]**をクリックします。

   資産のビジュアライゼーションが表示されます。

4. エクスポートするビジュアライゼーションの右上で、3 つのドットのボタンをクリックします。

   メニューが表示されます。

5. 使用するエクスポートのタイプを選択します。

   ファイルがコンピューターにダウンロードされます。

ホスト資産の ACR の編集

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management の **[調査]** セクションで、ホスト資産の ACR (資産重大度の格付け) (ACR) を手動でオーバーライドすると、所属組織に固有のインフラやニーズをより適切に反映できます。

調査の資産の ACR を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

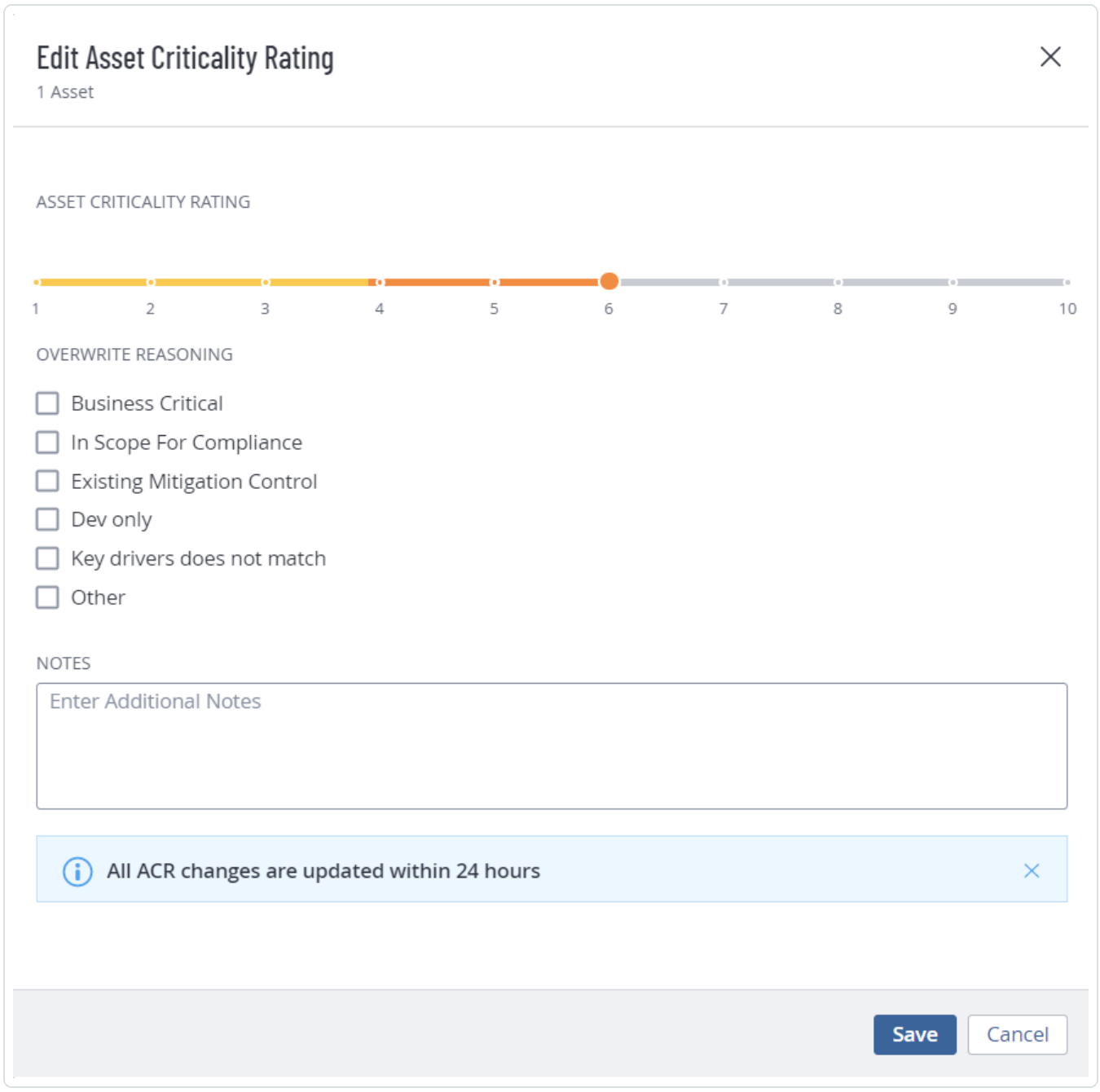
   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

3. ホスト資産の表の **[アクション]** 列で、編集対象の ACR のホスト資産の行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

4. ✎ **[ACR の編集]** をクリックします。

   [ACR の編集] ウィンドウが表示されます。



5. **ACR** スライダーで、変更後の ACR のスコア数をクリックします。
6. **[理由の上書き]** セクションで、ACR を編集する理由に最もよく合致する理由の横にあるチェックボックスをオンにします。
7. (オプション) **[注記]** セクションで、追加のコメントを入力します。
8. **[保存]** をクリックします。

Tenable Vulnerability Management が新しい ACR を資産に適用するのに最大で 24 時間かかります。更新の処理中、ホスト資産の表に ACR が **[処理中]** であると表示される場合があります。

資産を別のネットワークに移動する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Vulnerability Management は、スキャンされた資産をスキャナーのネットワーク ID に基づいてネットワークに自動的に割り当てます。ただし、手動で資産を別のネットワークに移動する必要が生じることもあります。たとえば、同一 IP アドレスを持つ複数の資産がさまざまなサブネットに属していて、それらを個別のエンティティとして識別できるような場合です。

[資産] ワークベンチから別のネットワークに資産を移動できます。最初に資産の移動先のネットワークを作成する必要がある場合は、ネットワークを作成するを参照してください。

ヒント: **[設定]** セクションから資産をネットワークに移動することもできます。

資産を移動するときには、資産とともにスキャナーも必ず移動してください。そうしないと、スキャナーによって同じ資産が再作成されます。詳細は、ネットワークにスキャナーを追加する を参照してください。

注意: 新しいネットワークでスキャンを実行する前に、資産を移動してください。既にスキャンを実行したことのあるネットワークに資産を移動した場合、Tenable Vulnerability Management で重複レコードが作成されてそれがライセンスとしてカウントされる可能性があります。

ヒント: **[資産]** ワークベンチでは、ホスト資産、クラウドリソース、またはウェブアプリケーションを別のネットワークに移動できます。ドメインインベントリ資産は移動できません。

別のネットワークに資産を移動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

   [資産] ワークベンチが表示され、**[ホスト]** タイルがアクティブになり、資産がテーブルビューで表示されます。

3. (オプション) 表データを選別します。詳細は、検出結果または資産のフィルタリングを参照してください。

4. 移動する資産のチェックボックスを選択します。

表の上部にアクションバーが表示されます。

5. アクションバーで、**[移動]** を選択します。

   ダイアログが表示されます。

6. ダイアログの **[新しい宛先ネットワークを選択してください]** で、資産の移動先のネットワークを選択します。

7. **[移動]** をクリックします。

   資産が宛先ネットワークに移動します。選択した資産の数によっては、Tenable Vulnerability Management で移動が完了するまでに時間がかかることがあります。

重複資産の削除と防止

Tenable Vulnerability Management では、認証スキャンまたはエージェントスキャンでスキャンすると、資産に一意の ID が割り当てられます。Tenable Vulnerability Management は、スキャンを実行するたびにこの一意の ID をチェックします。これにより、既存の資産レコードを新規の検出結果、解決済みの検出結果、または再表面化した検出結果で更新できます。その後、同じ資産に対して認証なしのスキャンを実行すると、スキャンは資産にログインできず、一意の ID を取得できません。この場合、Tenable Vulnerability Management はその資産を新規と見なし、新しいレコードを作成します (この例では資産の複製)。

重複資産の削除

Tenable Vulnerability Management の重複資産を削除する方法

1. **[調査]** セクションで、資産リストを表示します。
2. 重複する資産を削除します。

   資産が削除されると、Tenable Vulnerability Management はすぐにライセンスを使用可能なライセンス数に戻します。

重複資産の防止

重複資産が Tenable Vulnerability Management に表示されないようにするには、通常、上記の原因を避けるだけで済みます。ベストプラクティスとして、また重複の問題を解決するために、認証なしのスキャンを認証スキャンまたはエージェントスキャンと組み合わせて資産をスキャンしないようにしてください。代わりに、どちらか一方を選択してください。

各スキャンタイプでそれぞれ異なるユースケースがありますが、Tenable が一般的に推奨するスキャンタイプの優先順位は、次の順番になります。

1. Tenable Nessus スキャナーから行う認証スキャン
2. Tenable Nessus Agent スキャン
3. 認証なしのスキャン
4. Tenable Nessus Network Monitor

詳細は、Create a Tenable Vulnerability Management Scanを参照してください。

インベントリデバッグデータのダウンロード

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Vulnerability Management アクセス許可: 編集可、該当する資産タグに対する使用可アクセス許可

必要なアクセスグループのアクセス許可: 表示可

Tenable Vulnerability Management 管理の資産に関連するサポートケースを開くと、資産のインベントリデータ(資産のスキャンデータを含む .zip ファイル)をダウンロードして、それをサポートチケットに添付できます。

資産データは、次のいずれかの場所でダウンロードできます。

- **[調査]** > **[資産]**
- **[調査]** > **[資産]** > **[資産の詳細]** > **[アクション]** ドロップダウンメニュー

注意: .zip ファイルに含まれているスキャンデータは、サポートケース専用であり、予告なく変更されることがあります。

注意: **[インベントリデバッグデータのダウンロード]** アクションは、Tenable Vulnerability Management が過去 90 日間にスキャンし、ソースタイプが **SSM**、**AZURE_FA**、または **NESSUS_AGENT** スキャン(インベントリコレクションプラグインが有効なもの(ハイブリッドエージェント))のいずれかである資産にのみ使用できます。

[調査] > **[資産]** ページから資産スキャンデータをダウンロードする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

3. (オプション) 検出結果または資産のフィルタリングの説明に従って、表示されたデータを選別します。

4. 次のいずれかを行います。

- 資産の表で、ダウンロードするスキャンデータの資産の行を右クリックします。
- 資産の表の**[アクション]**列で、ダウンロードするスキャンデータの資産の行にある⋮ボタンをクリックします。

  アクションボタンが行に表示されます。

5. 資産データをダウンロードするには、**[インベントリデバッグデータのダウンロード]**をクリックします。

   資産のスキャンデータが .zip ファイルとしてダウンロードされます。

資産の削除

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

[資産]ワークベンチでは、ホスト資産、ウェブアプリケーション資産、またはドメインインベントリ資産を削除できます。資産を削除すると、Tenable Vulnerability Management は**[資産]**ワークベンチから資産を削除し、関連するすべての検出結果を削除し、スキャン結果と資産のマッチングを停止します。また、24 時間以内に、Tenable Vulnerability Management は資産をライセンスカウントから削除します。

注意: **[資産エイジアウト]**が有効になっているネットワークでは、資産はスケジュールに従って期限切れになります。詳細は、ネットワークを表示または編集するとネットワークを作成するを参照してください。

警告: 資産を削除すると、廃止されたホストやその他の無関係の資産が、ライセンスカウントとレポートから恒久的に削除されます。この機能に注意してください。

注意: **[資産 ID]**フィルターの使用時に削除された資産が表示されている場合、これは一時的なものです。削除された資産はライセンスに対してカウントされず、関連する検出結果もありません。削除された資産は**[削除済み]**としてラベル付けされます。

資産を削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある**[調査]**で**[資産]**をクリックします。

   [資産]ワークベンチが表示されます。

3. **[資産]**ワークベンチで、次のいずれかを実行します。

   - **⋮ ボタンを使用して 1 つの資産を削除する**

     a. 削除する資産の行で、⋮ ボタンをクリックします。

     メニューが表示されます。

     b. メニューで、🗑**[削除]**をクリックします。

c. 表示される確認ウィンドウで、もう一度 **[削除]** をクリックします。

> **ヒント**: **[資産の詳細]** ページから 1 つの資産を削除することもできます。

- **アクションバーから複数の資産を削除する**

a. 削除する資産の横にあるチェックボックスを選択します。

アクションバーが表示されます。

> **ヒント**: すべての資産を削除するには、**[すべて選択]** をクリックします。一度に削除できる資産は 1,000 個までです。

b. アクションバーで **[その他]** をクリックします。

c. 表示されるメニューで、**[削除]** をクリックします。

d. 表示される確認ウィンドウで、もう一度 **[削除]** をクリックします。

検出結果または資産のフィルタリング

> **必要な Tenable Vulnerability Management ユーザーロール:** 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[検出結果] と **[資産]** ワークベンチでは、*[調査]* の表を使用して所属組織のデータを表示します。これらの表をフィルタリングして、特定の資産や検出結果を表示できます。

フィルターの使用

[検出結果] ワークベンチと **[資産]** ワークベンチの [調査] の表で、フィルターを使用して特定の検出結果または資産を表示できます。

注意: パフォーマンスを最適化するために、Tenable では、適用できる検出結果フィルターの数を 18 に、適用できる資産フィルターの数を 35 に制限しています。

ヒント: 使用できるフィルターの一覧については、検出結果フィルター または 資産フィルター を参照してください。

注意: 検出結果をフィルタリングして検出結果レポートを生成する場合、各レポートに最大 5 つのフィルターを適用できます。

[調査] の表でフィルターを使用する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** で **[検出結果]** または **[資産]** をクリックします。

3. 次のいずれかを行います。

   基本モードで表をフィルタリングする

   a. 左上にある ▽ ボタンをクリックします。

      フィルタープレーンが展開され、選択されたデフォルトフィルターのリストが表示されます。

   b. **[フィルターの選択]** をクリックします。

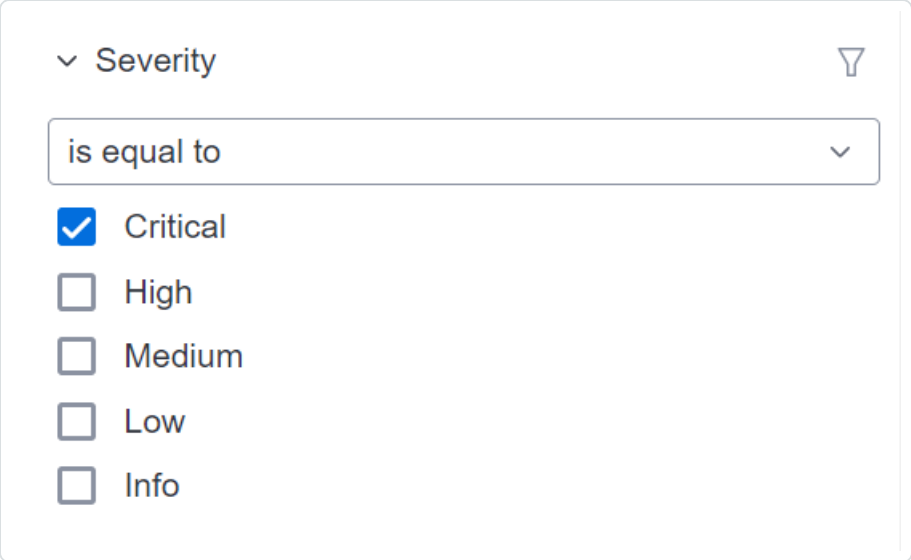
      使用可能なすべてのフィルターを示す **[フィルターの選択]** ボックスが表示されます。

   c. 適用するフィルターを選択します。

   d. **[フィルターの選択]** ボックスの外側をクリックします。

      [フィルターの選択] ボックスが閉じます。

e. フィルターごとに、適切な *演算子とオプション*を選択します。たとえば、深刻度が「重大」の脆弱性を返すには、次の画像に示すように、演算子 **[次の値に等しい]** と **[重大]** オプションを選択します。



検索演算子は、選択したフィルターに応じて異なります。詳細なリファレンスについては、次の表を参照してください。

演算子	説明
存在する	選択されたフィルターが存在するアイテムを表示します。
存在しない	選択されたフィルターが存在しないアイテムを表示します。
次の値に等しい	フィルター値に一致するアイテムを表示します。
次の値に等しくない	フィルター値を含まないアイテムを表示します。

演算子	説明
次の値より大きい **次の値以上**	指定されたフィルター値より大きい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以上]** 演算子を使用します。
次の値より小さい **次の値以下**	指定されたフィルター値より小さい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以下]** 演算子を使用します。
直近	今日より前の数時間、数日、数か月、または数年以内の日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
後	指定されたフィルター値より後の日付のアイテムを表示します。
前	指定されたフィルター値より前の日付のアイテムを表示します。
経過	今日より前の数時間、数日、数か月、または数年が経過した日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
日付	指定された日付のアイテムを表示します。
期間	指定された 2 つの日付間のアイテムを表示します。
次の値を含む:	指定されたフィルター値を含むアイテムを表示します。
次の値を含まない:	指定されたフィルター値を含まないアイテムを表示します。
ワイルド	次のように、ワイルドカード (*) でアイテムを絞り込みます。

演算子	説明
カード	• **次で始まるまたは終わる** - 指定したテキストで始まるまたは終わる値を表示します。たとえば、「1」で始まるすべての値を見つけるには、*1** と入力します。「1」で終わるすべての値を見つけるには、**1* と入力します。 • **次の値を含む** - 指定したテキストを含む値を表示します。たとえば、最初と最後の文字の間のどこかに「1」があるすべての値を見つける場合は、**1** と入力します。 • **大文字と小文字の区別をオフにする** - 大文字と小文字を区別せずに値を表示します。たとえば、**プラグイン名** が「TLS バージョン 1.2 プロトコル検出」*または*「tls バージョン 1.2 プロトコル検出」である検出結果を検索するには、**tls バージョン 1.2 プロトコル検出* と入力します。

f. (オプション) フィルターを削除またはリセットするには、次のいずれかを実行します。

- フィルターの値をクリアするには、フィルターの右側にカーソルを合わせ、**[クリア]** をクリックします。
- フィルターを削除するには、フィルターの右側にカーソルを合わせ、**[削除]** をクリックします。
- **[検出結果]** ワークベンチでフィルターをデフォルトの設定にリセットするには、フィルタープレーンの上部にある **[リセット]** をクリックします。
- **[資産]** ワークベンチのすべてのフィルターを削除するには、フィルタープレーンの上部にある **[すべてクリア]** をクリックします。

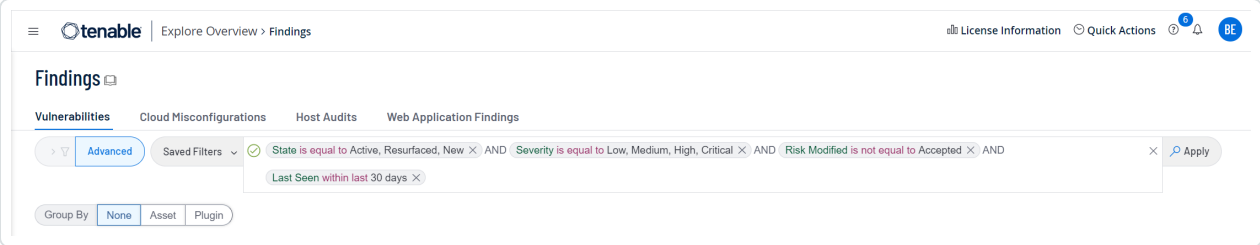
g. **[適用]** をクリックします。

Tenable Vulnerability Management がデータをフィルタリングします。

詳細モードで表をフィルタリングする

a. 左上にある **[詳細]** をクリックします。

ボックスが表示され、現在のフィルターが表示されます。



b. ボックス内をクリックします。

ドロップダウンが表示されます。

c. ドロップダウンで、**AND** または **OR** 条件を選択するか、またはボックスに条件を入力します。

d. ドロップダウンで、フィルターを選択するか、またはボックスにフィルター名を入力します。

e. ドロップダウンで、次の演算子のいずれかを選択するか、またはボックスに演算子を入力します。

> **注意:** (') または (") で始まる値や (*) または (,) を含む値でフィルタリングする場合は、値を引用符 (") で囲む必要があります。

> **注意**: フィルターは、最大で 2 つのネストレベルを持つことができます。

演算子	説明
存在する	選択されたフィルターが存在するアイテムを表示します。
存在しない	選択されたフィルターが存在しないアイテムを表示します。
次の値に等しい	フィルター値に一致するアイテムを表示します。
次の値に等しくない	フィルター値を含まないアイテムを表示します。

演算子	説明
次の値より大きい **次の値以上**	指定されたフィルター値より大きい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以上]** 演算子を使用します。
次の値より小さい **次の値以下**	指定されたフィルター値より小さい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以下]** 演算子を使用します。
直近	今日より前の数時間、数日、数か月、または数年以内の日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
後	指定されたフィルター値より後の日付のアイテムを表示します。
前	指定されたフィルター値より前の日付のアイテムを表示します。
経過	今日より前の数時間、数日、数か月、または数年が経過した日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
日付	指定された日付のアイテムを表示します。
期間	指定された 2 つの日付間のアイテムを表示します。
次の値を含む:	指定されたフィルター値を含むアイテムを表示します。
次の値を含まない:	指定されたフィルター値を含まないアイテムを表示します。
ワイルドカード	次のように、ワイルドカード (*) でアイテムを絞り込みます。

演算子	説明
	• **次で始まるまたは終わる** - 指定したテキストで始まるまたは終わる値を表示します。たとえば、「1」で始まるすべての値を見つけるには、*1** と入力します。「1」で終わるすべての値を見つけるには、**1* と入力します。 • **次の値を含む** - 指定したテキストを含む値を表示します。たとえば、最初と最後の文字の間のどこかに「1」があるすべての値を見つける場合は、**1** と入力します。 • **大文字と小文字の区別をオフにする** - 大文字と小文字を区別せずに値を表示します。たとえば、**プラグイン名** が「TLS バージョン 1.2 プロトコル検出」*または*「tls バージョン 1.2 プロトコル検出」である検出結果を検索するには、**tls バージョン 1.2 プロトコル検出* と入力します。

f. ドロップダウンで、フィルター値を選択するか、またはボックスにフィルター値を入力します。

g. (オプション) フィルターを追加または削除するには、次のいずれかを実行します。

- 複数のフィルターを追加するには、**Space** キーを押してから、別の条件、演算子、フィルター、値を選択します。
- 1 つのフィルターを削除するには、フィルターの右側にある ✕ ボタンをクリックします。
- すべてのフィルターを削除するには、テキストボックスの右隅にある ✕ ボタンをクリックします。

h. **[適用]** をクリックします。

Tenable Vulnerability Management がデータをフィルタリングします。

4. (オプション) フィルターを保存して、後でアクセスしたり、チームの他のメンバーと共有したりします。

ヒント: Tenable Vulnerability Management では検出結果の検索がバックグラウンドで実行されるので、ユーザーは **[検出結果]** ページから他のページに移動し、複雑な検索の完了後にページに戻ってくることができます。検索を**キャンセル**することもできます。さらに、Tenable Vulnerability Management は、直近検索の 30 分間のキャッシュ、トップツールバーへの日時表記、次回のアクセス用に **[検出結果]** ページの状態保存も行います。

コンテキストメニューの使用

[検出結果]と**[資産]**の各ワークベンチにある調査の表で、任意の行を右クリックすると、検出結果と資産の両方に関するコンテキストメニューのオプションが表示されます。メニューには、次のオプションが常に表示されます。

オプション	説明
すべての詳細を表示	検出結果または資産の詳細ページを開きます。
新しいタブですべての詳細を表示	新しいブラウザタブで検出結果または資産の詳細ページを開きます。
クリップボードにコピー	調査の表の任意の値を取得します。たとえば、タグを作成するときに**[資産]**ワークベンチのフィールドからオペレーティングシステムの値をコピーして、タグにペーストします。
値でフィルター	調査の表を任意の値でフィルタリングします。たとえば、**[検出結果]**ワークベンチでIPv4アドレスを右クリックし、このオプションをクリックすると、そのIPv4アドレスを持つすべての検出結果が表示されます。
除外値	調査の表から特定の値を持つすべてのエントリを除外します。たとえば、**[資産]**ワークベンチでオペレーティングシステムタイプを右クリックすると、そのオペレーティングシステムのすべての資産が除外されます。

調査の表のカスタマイズ

[調査] セクションの **[検出結果]** または **[資産]** ワークベンチで、表の列をカスタマイズできます。

調査の表をカスタマイズする方法

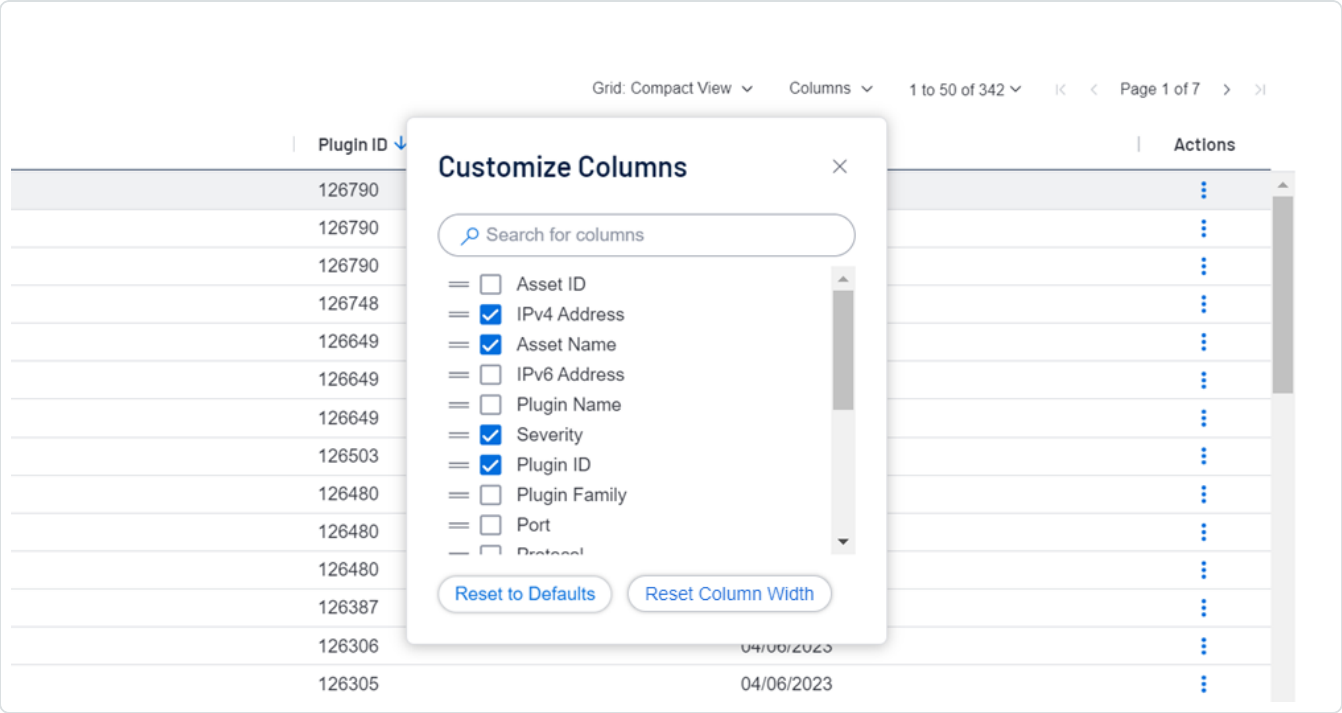
1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** で **[検出結果]** または **[資産]** をクリックします。

3. 右側で、表の上にある **[列]** をクリックします。

   [列のカスタマイズ] ダイアログが表示されます。



4. 次のいずれかを行います。

アクション	説明
列の追加または削除	**[列のカスタマイズ]** ダイアログで、列の横のチェックボックスを選択または選択解除します。

追加する列の検索	**[列のカスタマイズ]** ダイアログで列を探し、そのチェックボックスを選択します。
列の並べ替え	**[列のカスタマイズ]** ダイアログで、列をクリックして上から下にドラッグします。
列幅の変更	**資産**または**検出結果**の表で、列見出しの間のセパレーターにカーソルを合わせ、左右にドラッグします。
列幅をデフォルトにリセットする	**[列のカスタマイズ]** ダイアログで **[列の幅のリセット]** をクリックします。
すべての列のカスタマイズをデフォルトにリセットする	**[列のカスタマイズ]** ダイアログで **[デフォルトにリセット]** をクリックします。

検出結果または資産のエクスポート

[検出結果] および **[資産]** ワークベンチからデータを CSV または JSON にエクスポートできます。エクスポートのカスタマイズ、スケジュール、メール送信、パスワード保護、および期限切れの設定が可能です。これらのワークベンチにはさまざまなデータが含まれていますが、基本的なエクスポートプロセスは同じです。

検出結果または資産をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. **[検索]**の下にある右のナビゲーションプレーンで、次のいずれかを行います。

   - 所属組織でスキャンした脆弱性の検出結果をエクスポートするには、**[検出結果]** をクリックします。

     [検出結果] ワークベンチが表示されます。

   - 所属組織でスキャンした資産をエクスポートするには、**[資産]** をクリックします。

     [資産] ワークベンチが表示されます。

3. (オプション) フィルターの使用 の説明に従って、両ワークベンチで表示されたデータを絞り込みます。

   > **注意:** **[検出結果]** ワークベンチで検出結果をグループ化するために **[グループ化基準]** フィルターを使用する場合、一度にエクスポートできる検出結果は 5 つのみです。

4. エクスポートする検出結果または資産の横にあるチェックボックスを 1 つ以上選択します。

   > **注意**: 手動で選択できる検出結果または資産は最大 200 個です。それ以上の場合は、すべてを選択する必要があります。

   > **ヒント**: リストの一番上にあるチェックボックスを選択すると、すべての検出結果または資産を選択できます。

5. アクションバーで、[→ **[エクスポート]** をクリックします。

   [エクスポート] プレーンが表示されます。次のオプションが含まれています。

オプション	説明
名前	エクスポートのカスタム名を入力します。
形式	エクスポート形式を選択します。 • **CSV** – Microsoft Excel などのスプレッドシートアプリケーションで開くことができる CSV ファイル。 **注意**: 検出結果のエクスポートでは、Tenable Vulnerability Management により 32,000 文字を超えるセルが自動的にトリミングされ、Microsoft Excel に正しく表示されるようにします。これを無効にするには、**[切り捨てられないデータ]** を選択します。 **注意:** エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を追加します。詳細は、ナレッジベースを参照してください。 • **JSON** – 空のフィールドなしでネストされた検出結果のリストを含む JSON ファイル。
設定	含めるフィールドを選択します。 • **[フィールドセットの選択]** で、エクスポートに追加するフィールドを検索または選択します。 • 選択されたフィールドのみを表示するには、**[選択したフィールドを表示]** をクリックします。 • **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。
スケジュール	**[スケジュール]** トグルをオンにして、エクスポートのスケジュールを設定します。 a. **[開始日時]** セクションで、エクスポートの日時を選択します。 b. **[タイムゾーン]** ドロップダウンで、タイムゾーンを選択します。 c. **[繰り返し]** ドロップダウンで、エクスポートを繰り返す頻度を選択します (例: 毎日)。

	d. **[繰り返し終了]**ドロップダウンで、エクスポートを終了する日付を選択します。**[なし]**を選択した場合は、スケジュールを変更または削除するまで、エクスポートが繰り返されます。
Eメール通知	メール通知を送信するには、**[Eメール通知]**トグルをオンにします。 a. **[受信者の追加]**ボックスに、通知するメールアドレスを入力します。 b. **[パスワード]**ボックスに、エクスポートファイルのパスワードを入力します。受信者がエクスポートファイルをダウンロードできるようにするために、このパスワードを受信者と共有します。

6. **[エクスポート]**をクリックします。

   エクスポートファイルのサイズによっては、処理に数分かかる場合があります。処理が完了すると、Tenable Vulnerability Managementはコンピューターにファイルをダウンロードします。

   ヒント: ダウンロードが完了する前に**[エクスポート]**プレーンを閉じた場合は、**[設定]**>**[エクスポート]**でエクスポートファイルにアクセスできます。

検出結果または資産の保存されたフィルター

[検出結果]または**[資産]**ワークベンチで、フィルターを適用し、それらのフィルターの完全な組み合わせを保存して、後から使用することができます。保存したフィルターをチームと共有することもできます。

注意: 保存されたフィルターは、検出結果または資産タイプに固有です。たとえば、ホスト脆弱性検出結果で作成された保存済みフィルターを、ホスト監査検出結果に使用することはできません。

ヒント: 使用できるフィルターの一覧については、検出結果フィルターまたは資産フィルターを参照してください。

保存されたフィルターの作成

保存済みフィルターを作成する方法

1. **[検出結果]**または**[資産]**ワークベンチで、フィルターを追加してカスタム検索を作成します。
2. 検索バーの左側で、**[保存済みフィルター]**ドロップダウ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。
3. ドロップダウンボックスで、 **[保存]**をクリックします。
4. ドロップダウンボックスで、フィルター名を入力します。

   Tenable Vulnerability Management は ASCII 文字のみを受け入れます。
5. ✓ ボタンをクリックします。

   Tenable Vulnerability Management によりフィルターが保存されます。

保存されたフィルターの使用

保存されたフィルターを使用する方法

1. **[検出結果]**または**[資産]**ワークベンチの検索バーの左側で、**[保存済みフィルター]**ドロップダウ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。

2. ドロップダウンボックスから、適用するフィルターを選択します。

   検索結果が表示されます。

保存されたフィルターの編集

フィルターは編集できます。変更後、既存のフィルターを更新するか、変更を新しいフィルターとして保存できます。

保存したフィルターを編集する方法

1. **[検出結果]**または**[資産]**ワークベンチの検索バーの左側で、**[保存済みフィルター]**ドロップダウンをクリックします。

   保存したフィルターを含むドロップダウンボックスが表示されます。

2. 保存したフィルターをクリックして編集します。
3. フィルターを追加または削除します。詳細は、検出結果または資産のフィルタリングを参照してください。

   フィルター名の横に*[編集済み]*バッジが表示されます。

4. **[保存済みフィルター]**ドロップダウンで、オプションを選択します。
   a. フィルターを更新するには、🔄 **[更新]**をクリックします。
   b. フィルターを新しいバージョンとして保存するには、💾 **[新しく保存]**をクリックします。

ヒント: 変更を破棄するには、フィルター名の右側にある ✕ ボタンをクリックします。

保存されたフィルターの名前変更

保存されたフィルターの名前を変更する方法

1. **[検出結果]**または**[資産]**ワークベンチの検索バーの左側で、**[保存済みフィルター]**ドロップダウンをクリックします。

   保存したフィルターを含むドロップダウンボックスが表示されます。

2. 名前を変更するフィルターの右側にある⋮ボタンをクリックします。

   ドロップダウンが表示されます。

3. ドロップダウンで、**[名前の編集]**をクリックします。

4. 表示されるボックスに新しいフィルター名を入力します。

   ✓ ボタンをクリックします。

   Tenable Vulnerability Management がフィルターの名前を変更します。

保存されたフィルターの共有

リンクを使用して、保存したフィルターをチームに共有できます。

注意: チームメンバーが Tenable Vulnerability Management で異なるアクセスレベルを持っている場合、同じ検出結果や資産を表示できません。詳細は、権限 を参照してください。

保存したフィルターを共有する方法

1. **[検出結果]** または **[資産]** ワークベンチの検索バーの左側で、**[保存済みフィルター]** ドロップダウ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。

2. 保存済みフィルターの右側にある ⋮ ボタンをクリックします。

   ドロップダウンが表示されます。

3. ドロップダウンで、🔗 **[リンクをコピー]** をクリックします。

   Tenable Vulnerability Management がリンクをクリップボードにコピーします。

保存されたフィルターの削除

保存したフィルターを削除できます。保存されたフィルターは、完全に削除されます。検出結果または資産に現在適用されている保存済みフィルターを削除すると、Tenable Vulnerability Management は現在のビューをリセットします。

保存したフィルターを削除する方法

1. **[検出結果]** または **[資産]** ワークベンチの検索バーの左側で、**[保存済みフィルター]** ドロップダウ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。

2. 削除する保存済みフィルターの右側にある ⋮ ボタンをクリックします。

   ドロップダウンが表示されます。

3. **[削除]** をクリックします。

4. 保存したフィルターの削除を確定するには、**[削除]** をもう一度クリックします。

   Tenable Vulnerability Management が保存済みフィルターを削除します。

調査ワークベンチとレガシーワークベンチ

Tenable Vulnerability Management の調査ワークベンチでは、Tenable が廃止されたレガシーワークベンチを置き換える合理化されたユーザーインターフェースで、すべての検出結果と資産を表示、分析、エクスポートできます。

Tenable Vulnerability Management の左側のナビゲーションプレーンの **[調査]** セクションに次の 2 つのワークベンチが表示されます。

- **検出結果ワークベンチ** – 脆弱性、クラウド設定ミス、ホスト監査、ウェブアプリケーションの検出結果を 1 か所で管理
- **資産ワークベンチ** – 脆弱性、クラウド設定ミス、ホスト監査、ウェブアプリケーションの検出結果を組み合わせて表示

次の表は、調査ワークベンチとレガシーワークベンチおよび関連ドキュメントへのリンクを比較したものです。

機能	レガシーワークベンチ	調査ワークベンチ	詳細情報
資産ワークベンチ	ホスト資産は表示専用	• ホスト資産、クラウドリソース、ウェブアプリケーション、ドメインインベントリを 1 か所で表示 • 列を追加して**資産**ワークベンチをカスタマイズ • 資産のビジュアライゼーションを表示	• 資産 • 資産ワークベンチの表示 • 調査の表のカスタマイズ • 資産ビジュアライゼーションの表示
[資産の詳	資産タイプのカスタ	• 資産タイプ別に追加詳細を表示	• 資産の

細] ページ	マイズはサポート対象外	• [脆弱性] タブの名前が **[検出結果]** に変更 • **[オープンポート]** タブに、高トラフィックプラグインのオープンポート検出結果を追加	詳細の表示 • オープンポートと資産 ワークベンチ
検出結果 ワークベンチ	• 脆弱性のみが表示 • 検出結果は、プラグインまたは資産別にのみグループ化 • 検出結果のビジュアライゼーションのサポート	• 脆弱性、クラウド設定ミス、ホスト監査、ウェブアプリケーションの検出結果が1か所に表示 • プラグインまたは資産別にグループ化するか、グループ化せずにすべてのリソースを表示 • 列を追加して**検出結果**ワークベンチをカスタマイズ • 検出結果のビジュアライゼーションはサポート対象外	• 検出結果 • 検出結果ワークベンチの表示 • 検出結果のグループ化 • 検出結果または資産のフィルタリング
検出結果および資産 フィルター	• 高度なフィルターモードなし • ネストされたフィルターはサポート対象外	• 高度なフィルターモードで複雑なクエリを構築 • ネストされたフィルターのサポート	• 検出結果フィルター • 資産 • 検出結果または資産のフィル

			タリング
調査結果および資産のエクスポート	HTML、PDF、CSV、またはJSONにエクスポート	• JSONまたはCSVにエクスポート • PDFの場合は、**検出結果**ワークベンチの各行の右側にあるメニューの**[レポートの生成]**をクリック • **検出結果**ワークベンチと**資産**ワークベンチの両方から、新しいフィールドを使用して追加のデータをエクスポート	検出結果または資産のエクスポート
サイドバーナビゲーション	• 資産と脆弱性は2つの別々のセクションに表示 • [脆弱性]セクションにスキャンは表示	• 検出結果と資産は、左側のナビゲーションプレーンの**[調査]**セクションに表示 • スキャンは、左側のナビゲーションプレーンの**[スキャン]**セクションに表示	プレーンのナビゲーション

アクション

[アクション] セクションでは、以下を表示および管理できます。

- コンテナ内のレポート
- 修正作業

[アクション] メニューとオプションにアクセスする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで、次のいずれかを行います。

   - **[レポート]** をクリックします。

     [レポート] ページが表示されます。詳細は、レポートを参照してください。

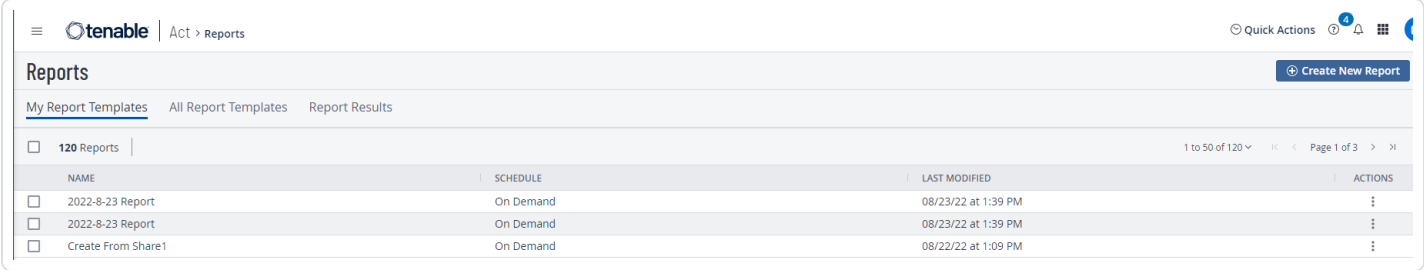
     > **ヒント:** **[アクション]** をクリックして、**[レポート]** ページに直接移動することもできます。

   - **[修正]** をクリックします。

     [修正] ページが表示されます。詳細は、修正を参照してください。

レポート

レポートは、レポートとレポート結果の 2 つの部分で構成されます。**[レポート]** ページでは、テンプレートからのレポート作成、既存レポートの実行、これらのレポートの結果の表示を行うことができます。



注意: レポートには、過去 30 日間のデータが表示されます。Tenable では、セキュリティ衛生を維持し、レポートデータを最新の状態に保つために、少なくとも月 1 回はスキャンすることを推奨しています。

[レポート] ページには、次のフォルダーがあります。

- **[マイレポートテンプレート]** フォルダーは、**[レポート]** ページにアクセスした場合に表示されるデフォルトのフォルダーです。作成したレポートはこのフォルダーに表示されます。
- **[すべてのレポートテンプレート]** フォルダーには、操作するアクセス許可があるすべてのレポートが表示されます。すべてのレポートはユーザー固有です。
- **[レポート結果]** フォルダーには、表示するアクセス許可があるレポートのすべての結果が表示されます。結果は、レポートが実行された時期に基づき時系列順に表示されます。**[レポート結果]** にあるレポートのすべての結果は、ユーザー固有です。

Tenable Vulnerability Management を使用することで、テーマに沿った情報豊富なレポートを作成でき、見過ごしがちな情報を見つけることができます。たとえば、[認証情報スキャンエラー] レポートは、失敗した認証スキャンのわかりやすく整理されたリストを提供するため、アナリストはスキャンの問題に手早く対処でき、認証スキャンに関する問題のトラブルシューティングが容易になります。Tenable Vulnerability Management に含まれているレポートテンプレートの完全なリストについては、Tenable Vulnerability Management レポートテンプレートを参照してください。

注意: **[PCI 四半期外部]** スキャンデータは、ダッシュボード、レポート、ワークベンチから故意に除外されています。これは、このスキャンは細かいものを検出する性質があり、本来検出しないはずのものを誤検出してしまう可能性があるからです。詳細は、Tenable PCI ASV スキャンを参照してください。

[レポート] ページを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

レポートテンプレート

Tenable Vulnerability Management では、レポートテンプレートおよびカスタマイズ可能なレポート形式から選択できます。Tenable が提供するレポートテンプレートを設定することも、利用可能な形式の 1 つから完全にカスタマイズされたレポートを作成することもできます。

Tenable が提供するレポートテンプレートの完全なインデックスについては、Tenable Vulnerability Management レポートテンプレートを参照してください。

ヒント: 各レポートに含まれる特定のデータの詳細については、レポートの詳細の表示 を参照してください。

注意: **サイバー保険レポート**には、次の注意事項が含まれています。

- レポートはいかなる方法でも編集できません。これにより、引受会社はメトリクスが 100% 正確であることを確認できます。
- このレポートには、過去 180 日間の調査データのみが含まれます。
- このレポートを利用できるのは、コンテナで調査レポートが有効になっているお客様のみです。
- レポート名は、レポートの後続の生成で変更されません。たとえば、レポート名の日付/タイムスタンプは、次回レポートを実行するときに更新されませんが、レポートデータ自体には、レポートが最後に実行された日付が含まれます。
- 深刻度は、CVSSv3 ベーススコアのみを使用して報告されます。

詳細は、**サイバー保険レポート**のブログ投稿を参照してください。

レポート設定

新規レポートを作成するか、既存のレポートを編集する場合は、次のオプションを使用できます。

オプション	説明
一般	
名前	このテキストボックスには、選択したレポートテンプレートの名前が表示されます。このテキストボックスを編集してレポートの名前を変更できます。
説明	このテキストボックスには、選択したレポートテンプレートに基づくデフォルトの説明が表示されます。このテキストボックスを編集してレポートの説明を変更できます。
ロゴを更新	**[ロゴを更新]** をクリックして、レポートに新しいロゴを追加するか、最近アップロードされたロゴのリストから選択します。 **[すべてのレポートのデフォルトとして設定]** チェックボックスを選択して、ロゴをデフォルトとして設定します。
エグゼクティブサマリー	
[ウィジェットライブラリ] をクリックして、レポートの結果に含める Tenable 提供のウィジェットのリストから選択します。	
追加のチャプター	
[チャプターライブラリ] をクリックして、レポートの結果に含める段落とコンポーネントのリストから選択します。	

レポートの作成

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

新規レポートを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. 右上の **[新しいレポートを作成]** をクリックします。

   [レポートテンプレート] ページが表示され、レポートがカテゴリ別に整理されます。

カテゴリ	説明
脆弱性管理	Tenable Vulnerability Management は、組織をリアルタイムで継続的に評価することにより、最も包括的な脆弱性カバレッジを提供します。これらのビルトインレポートにより、企業は優先順位付け、脅威インテリジェンス、リアルタイムのインサイトに基づいてリスクを伝達し、プロアクティブに修正アクションに優先順位を付けることができます。これらのレポートは、Tenable Nessus などの Tenable Vulnerability Management アプリケーションを使用して収集されたデータに関する概要と詳細情報を提供します。
Web App Scanning	ウェブアプリケーションのセキュリティは、ウェブアプリケーションの機密性、整合性、可用性を損なう可能性のある脅威や脆弱性を検出して軽減する機能

	を提供します。これらのレポートでは、最新のウェブアプリケーション向けの包括的で自動化された脆弱性スキャンツールである Tenable Web App Scanning からのデータを流用しています。

4. 表示されるリストで、テンプレートを選択します。
5. **[レポートを生成]** をクリックします。

   [レポートの詳細] ページが表示されます。
6. **[レポートの詳細]** ページで、次の操作を行います。
   - **[名前]** ボックスにレポートの名前を入力します。
   - (オプション) **[説明]** ボックスに説明を入力します。
   - **[エグゼクティブサマリー]** セクションで、利用可能なウィジェットから選択するか、**[新しいウィジェットを追加]** をクリックして**ウィジェットライブラリ**からウィジェットを選択します。
   - **[追加のチャプター]** セクションで、利用可能なチャプターから選択するか、**[新しいチャプターを追加]** をクリックして**チャプターライブラリ**からチャプターを 1 つ選択します。
   - (オプション) レポートにフィルターを追加します。詳細は、レポートのフィルター を参照してください。
   - (オプション) レポートのロゴをアップデートします。詳細は、レポート設定 を参照してください。
7. **[保存]** をクリックします。

   Tenable Vulnerability Management により新しいレポートが作成され、**[マイレポートテンプレート]** ページに表示されます。

ヒント: 作成されたら、最初のレポートを生成したり、コピーをダウンロードしたりできます。詳細は次をを参照してください: レポートの生成。

レポートの生成

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

重要: ユーザーアカウントを無効にしても、そのユーザーに対してスケジュールされたレポートは無効になりません。さらに、無効なユーザーが他のユーザーとレポートを共有した場合、これらの他のユーザーはそのレポートを生成できます。詳細は、ユーザーアカウントの無効化 を参照してください。

レポートを生成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. 実行するレポートを選択します。

範囲	アクション
単一のレポートを生成	単一のレポートを生成する方法 a. **[レポート結果]** タブで、生成するレポートの行を右クリックします。 -または- 生成するレポートの横にあるチェックボックスを選択します。 Tenable Vulnerability Management のアクションバーが有効になります。

	-または- **[レポート結果]** タブの **[アクション]** 列で、生成するレポート結果の行の ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. ▷ **[レポートを生成]** をクリックします。

Tenable Vulnerability Management はレポートの生成を開始します。レポートの状態は、**[レポート結果]** タブで追跡できます。

レポートの詳細の表示

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: 管理者以外のユーザーが表示できるのは、自分が作成したレポート、または他のユーザーから共有されたレポートの詳細のみです。

[レポートの詳細] ページを表示するには、次の操作を行います。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. **[マイレポートテンプレート]** タブで、詳細を表示するレポートの行をクリックします。

   [レポートの詳細] ページが表示されます。

[レポートの詳細] ページには、レポートに関する次の詳細が表示されます。

セクション	説明
説明	これは、レポートの簡単な説明です。
ターゲット	このセクションは、レポートに含まれるすべての資産を示します。
レポートのロゴ	レポートのロゴです。
History	このセクションには、レポートが生成された時刻、レポートの完了時刻、レポートの現

	在のステータスが表示されます。 a. レポートの表で、レポートをダウンロードまたは削除するには、次のいずれかを実行します。 • ダウンロードまたは削除するレポートの横にあるチェックボックスを選択します。Tenable Vulnerability Management は、アクションバーの **[ダウンロード]** および **[削除]** オプションを有効にします。 • **[アクション]** 列で、⋮ ボタンをクリックします。アクションオプションから、次のいずれかを選択します。 • **ダウンロード** - このオプションをクリックして、レポートをダウンロードします。レポートは PDF 形式でダウンロードされます。 • **削除** - このオプションをクリックすると、レポートが削除されます。
レポートの詳細	レポートの詳細には、レポートの簡単な要約が含まれます。 • **ステータス** - レポートのステータス。 • **タイプ** - レポートのタイプ(例: PDF)。 • **作成日** - レポートが作成された日付。 • **開始時間** - レポート生成が開始された時間。 • **終了時間** - レポート生成が完了した時間。 • **作成者** - レポートを作成したユーザー。

レポートテンプレートの共有

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

レポートテンプレートを組織内の他のユーザーと共有できます。

レポートテンプレートを共有する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

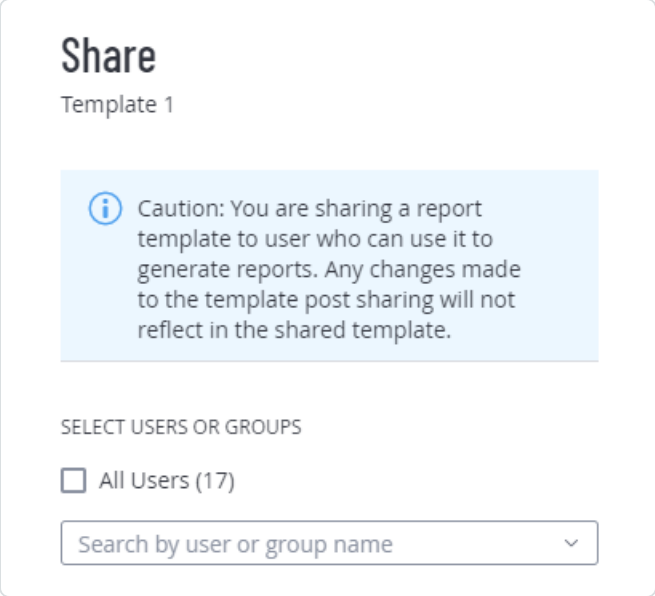
   [レポート] ページが表示されます。デフォルトでは、**[マイレポートテンプレート]** タブが表示されます。

3. 共有するレポートテンプレートを選択します。

範囲	アクション
単一レポートの共有	**[レポート]** ページからレポートテンプレートを共有する方法 a. **[マイレポートテンプレート]** タブで、共有するレポートテンプレートの行を右クリックします。 -または- **[マイレポートテンプレート]** の **[アクション]** 列で、共有するレポートテンプレートの行の ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 -または-

	[マイレポートテンプレート] タブで、共有するレポートテンプレートの横にあるチェックボックスをオンにします。 アクションバーで、Tenable Vulnerability Management は **[その他]** > **[共有]** を有効にします。 b. **[共有]** をクリックします。

[共有] プレーンが表示されます。



4. **[ユーザーまたはグループの選択]** セクションで、**[すべてのユーザー]** を選択するか、特定のユーザーまたはグループを検索します。

5. **[共有]** をクリックします。

   Tenable Vulnerability Management はレポートテンプレートを、**[共有レポートテンプレート]** タブでレポートテンプレートを表示できるユーザーと共有します。各ユーザーは、共有レポートの詳細、送信者のメールアドレス、共有レポートへのリンクが記載されたメール通知を受け取ります。

既存のレポートを編集する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

始める前に

所有者、管理者アカウントを保有するユーザー、そのレポートに対して **[設定可]** のアクセス許可を保有するユーザーのみ、レポートを変更できます。

レポートを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

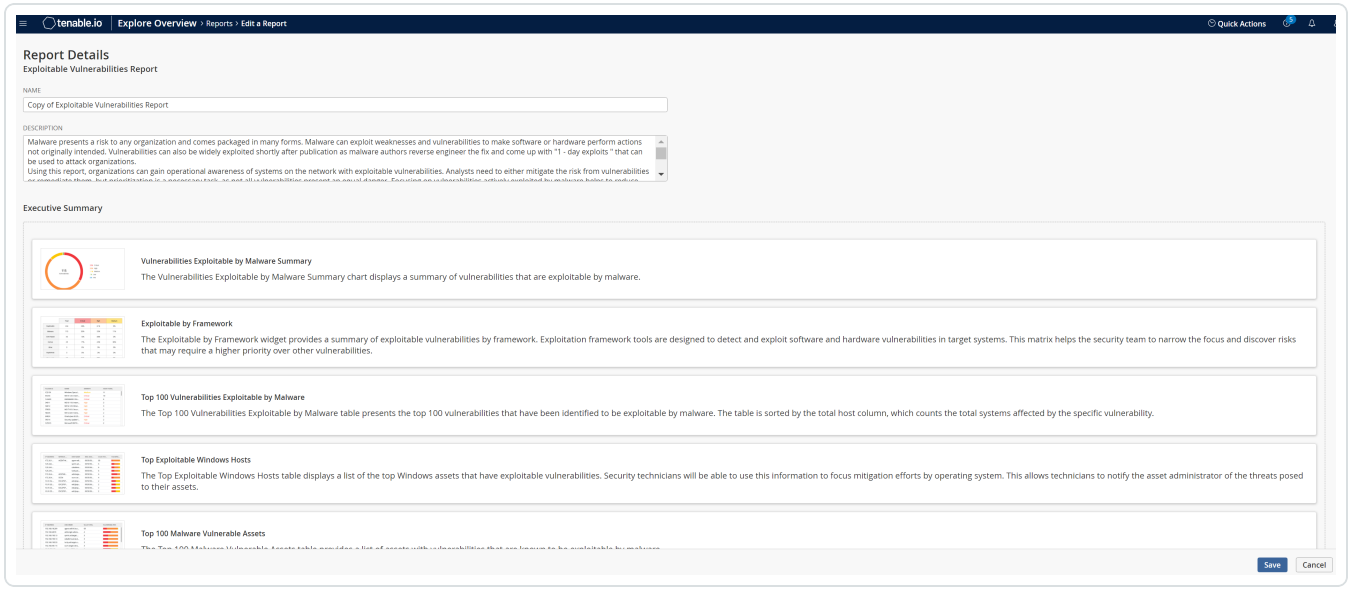
   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. 編集するレポートを選択します。

範囲	アクション
1つのレポートを編集する	**[レポート]** ページからレポートを編集する方法 a. **[マイレポートテンプレート]** または **[すべてのレポートテンプレート]** タブで、編集するレポートの行を右クリックします。 -または- **[マイレポートテンプレート]** または **[すべてのレポートテンプレート]** タブの **[アクション]** 列で、編集するレポートの行の ⋮ ボタンをクリックします。

	アクションボタンが行に表示されます。 b. **[編集]** をクリックします。

[レポートの詳細] ページが表示されます。



4. レポート設定を変更します。
5. 必要に応じて[フィルターを適用]します。
6. **[保存]** をクリックします。

   Tenable Vulnerability Management はレポートを保存し、**[レポート]** ページが表示されます。

レポートのフィルター

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

レポートを作成または編集するときに、ウィジェットにフィルターを追加できます。フィルターを使用すると、フィルタリングされた資産固有の詳細をレポートに表示できます。すべての資産、タグ別の資産、カスタム資産でフィルターできます。

注意: レポートのフィルタリングは現在、VM および調査 VM ウィジェットでのみ利用可能です。

注意: Tenable Web App Scanning は、タグによる脆弱性のフィルタリングをサポートしていません。

新しいレポートまたは既存のレポートのフィルターを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. 新しいレポートを作成するか、既存のレポートを編集します。
4. **[レポートの詳細]** ページで、✎ **[フィルターの編集]** をクリックします。

   [フィルター] プレーンが表示されます。

5. **[フィルタータイプを選択]** ドロップダウンボックスから、次のいずれかのフィルターを選択します。

- **すべての資産** - これを選択すると、すべての資産のデータがレポートに含められます。**[すべての資産]** フィルターはデフォルトで選択されています。
- **タグ** - 複数のタグを選択して、レポートをフィルタリングします。
- **カスタム資産** - IP アドレスを入力して、カスタム資産でデータをフィルタリングします。

  注意: **[カスタム資産]** フィルターを使用する場合、100 個以下の個別の IP アドレスでフィルタリングできます。

6. **[確認]** をクリックします。

   Tenable Vulnerability Management は、すべてのウィジェットにフィルターを適用します。▽ フィルターアイコンにカーソルを合わせると、適用されているフィルターを表示できます。

   注意: 関連するフィルターがない場合、Tenable Vulnerability Management は ▽ フィルターアイコンを無効にします。

7. (オプション) ウィジェットのフィルターを編集するには、ウィジェットの ⋮ アイコンをクリックし、**[設定]** をクリックして **[フィルター]** プレーンを開きます。
8. (オプション) ウィジェットのフィルターを削除する方法
   a. フィルターを削除するウィジェットで、⋮ アイコンをクリックし、**[削除]** をクリックします。
   b. 確認ウィンドウで、**[削除]** をクリックして削除します。
9. **[保存]** をクリックします。

   Tenable Vulnerability Management はフィルターをレポートテンプレートに適用します。

レポートをスケジュールする

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

始める前に

レポートをスケジュールできるのは、所有者、管理者アカウントを保有するユーザー、またはそのレポートに対して **[設定可]** のアクセス許可を保有するユーザーのみです。

重要: ユーザーアカウントを無効にしても、そのユーザーに対してスケジュールされたレポートは無効になりません。さらに、無効なユーザーが他のユーザーとレポートを共有した場合、これらの他のユーザーはそのレポートを生成できます。詳細は、ユーザーアカウントの無効化 を参照してください。

レポートをスケジュールする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

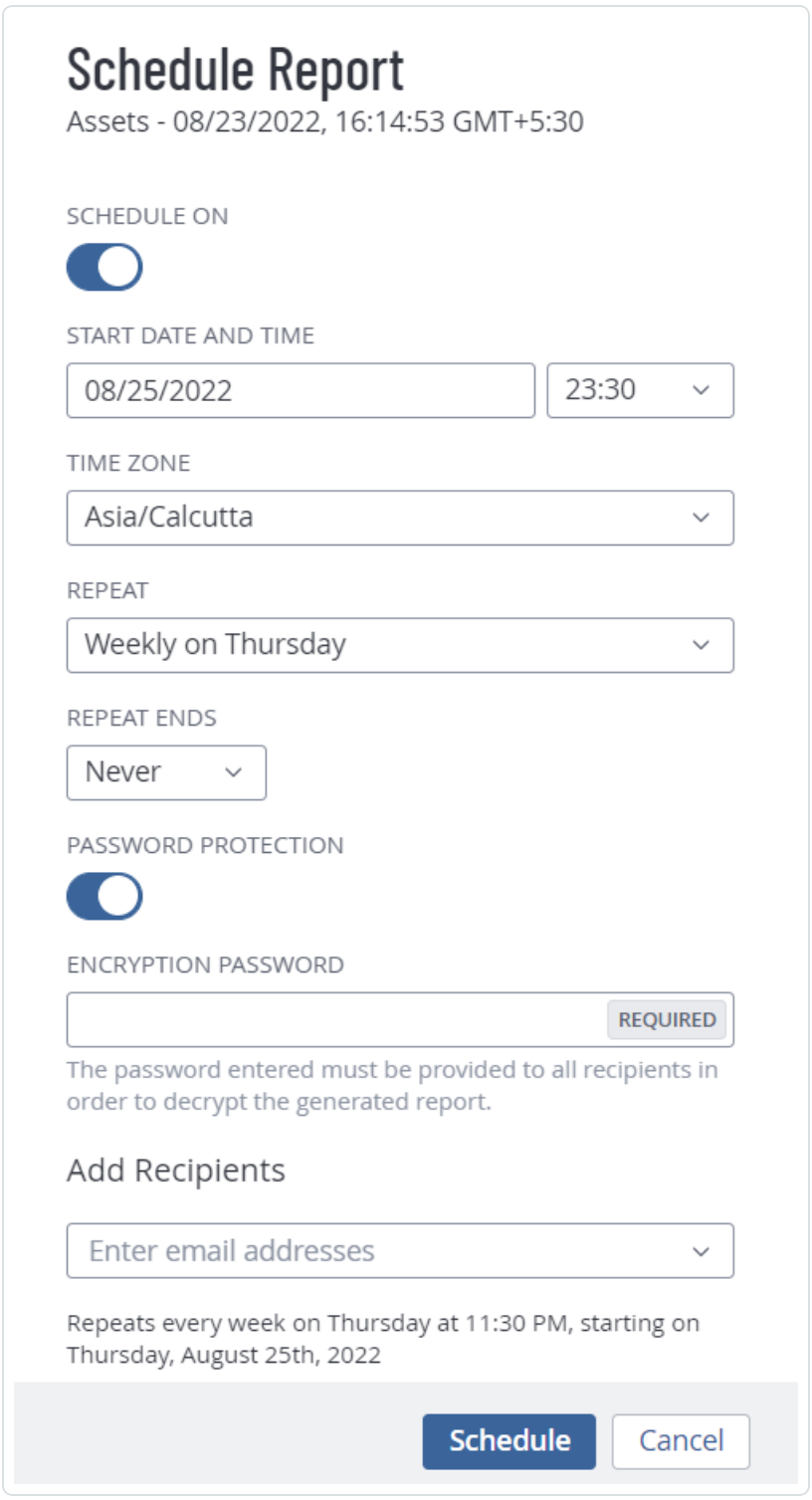
   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. スケジュールするレポートを選択します。

範囲	アクション
単一レポートのスケジュール	**[レポート]** ページからレポートをスケジュールする方法 a. **[マイレポートテンプレート]** または **[すべてのレポートテンプレート]** タブで、スケジュールするレポートの行を右クリックします。

	-または- **[マイレポートテンプレート]** または **[すべてのレポートテンプレート]** タブの **[アクション]** 列で、スケジュールするレポートの行の ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[スケジュール]** をクリックします。

[レポートをスケジュール] プレーンが表示されます。



4. レポートのスケジュール設定を変更します。

設定	Default (デ	説明

	フォルト)	
Schedule On	オフ	レポートがスケジュールされているかどうかを指定するトグルです。デフォルトでは、レポートはスケジュールされていません。 **[スケジュール]**トグルが無効になっている場合、他のスケジュール設定は非表示のままになります。 トグルをクリックする等、スケジュールが有効になり、残りの**[スケジュール]**設定が表示されます。
開始日時	不定	Tenable Vulnerability Management がレポートを開始する正確な日時を指定します。 デフォルトでは、開始日はスケジュール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す。たとえば、2022 年 9 月 31 日の午前 9 時 12 分にレポートスケジュールを作成した場合、Tenable Vulnerability Management はデフォルトの開始日時を 2022 年 9 月 31 日の 9 時 30 分に設定します。
タイムゾーン	不定	**[開始日時]**に設定した値のタイムゾーンです。
繰り返し	一度	Tenable Vulnerability Management がレポートを開始する頻度を指定します。レポートは**[開始日時]**で指定した時刻に実行されます。 • **Once**: レポートを 1 回実行するようにスケジュールします。 • **日単位**: レポートを毎日実行するようにスケジュールします。 • **週単位**: レポートを毎週実行するようにスケジュールします。 **注意:** レポートは、スケジュールが開始する曜日に実行されます。たとえば、レポートの初回実行日を 2021 年 2

		月 14 日月曜日にスケジュールした場合、レポートは毎週月曜日に実行されます。 • **月単位**: レポートを毎月実行するようにスケジュールします。 **注意:** レポートは、スケジュールが開始する曜日に実行されます。たとえば、レポートの初回実行日を 2021 年 2 月 14 日月曜日にスケジュールした場合、レポートは毎月第 2 月曜日に実行されます。 • **カスタム**: 特定の日数、週数、または月数に基づいて、カスタム間隔でレポートを実行するようにスケジュールします。 • **年単位**: レポートを毎年実行するようにスケジュールします。
終了日なし	Never	• **オン:** このオプションを選択すると**[終了日]**設定が表示され、レポートスケジュールを終了する日付を選択できます。 • **Never:** レポートのスケジュールを変更するまで、レポートはスケジュールに従って実行されます。
パスワード保護	オフ	レポートのスケジュールをパスワードで保護するかどうかを指定するトグルです。 レポートのパスワードを設定する方法 a. **[パスワード保護]**トグルをクリックして、レポートのパスワード保護を有効にします。 b. **[暗号化パスワード]**ボックスに、レポートのパスワードを入力します。 **注意:** レポートを開けるように、必ずこのパスワードを受信者に提供してください。

受信者を追加する		このボックスに、レポートのスケジュールを設定する 1 つ以上のメールアドレスを入力します。

5. **[スケジュール]** をクリックします。

   Tenable Vulnerability Management はレポートをスケジュールし、受信者はレポートを E メールとして受信します。パスワード保護トグルを有効にしている場合、受信者はプロンプトが表示されたときにパスワードを入力する必要があります。

レポート結果のメール送信

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

レポート結果を共有する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

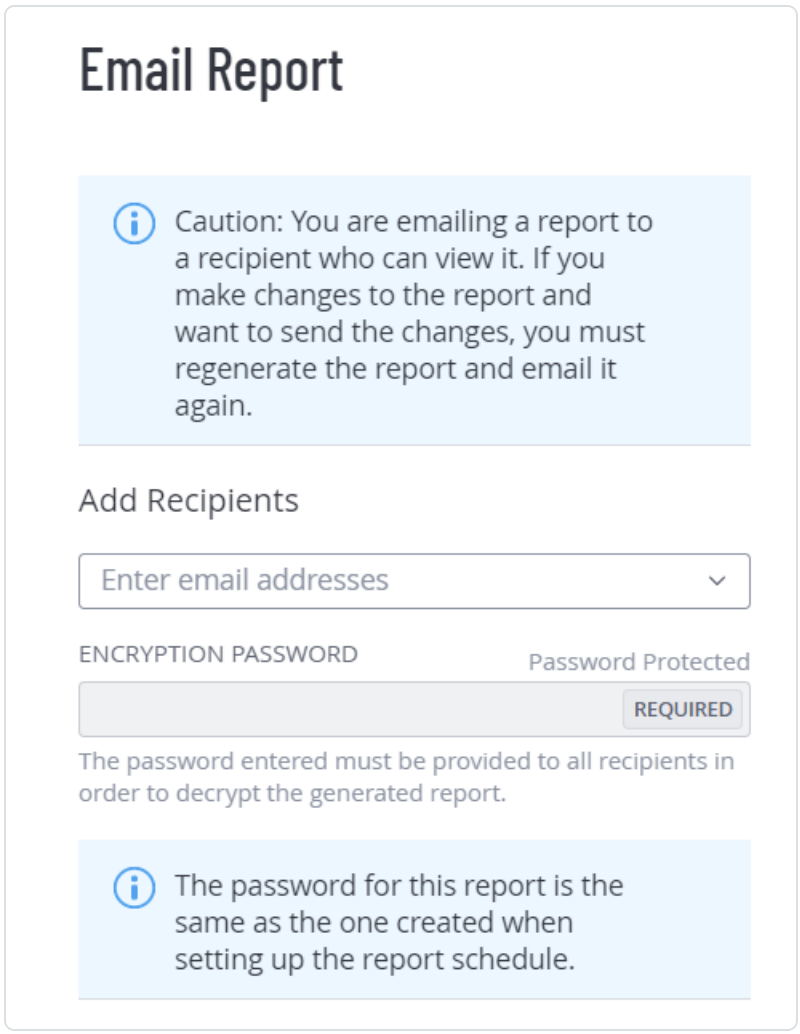
2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. 共有するレポート結果を選択します。

範囲	アクション
単一レポートの共有	**[レポート]** ページからレポート結果を共有する方法 a. **[レポート結果]** タブで、共有するレポート結果の行を右クリックします。 -または- **[レポート結果]** タブの **[アクション]** 列で、共有するレポート結果の行の ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[Eメール]** をクリックします。

[レポート結果] プレーンが表示されます。



4. **[受信者を追加する]** ボックスで、既存のメールアドレスのリストから選択するか、レポート結果の1人以上のメール受信者を入力します。

   選択した受信者が、レポート結果の PDF が添付された E メールを受信します。

5. **[暗号化パスワード]** ボックスに、生成されたレポートのパスワードを入力します。

   重要: レポートを開けるように、必ずこのパスワードを受信者に提供してください。

   注意: レポートのスケジュール時にパスワードを指定すると、Tenable Vulnerability Management はレポートを E メールで送信するときに同じパスワードを適用します。スケジュール時にパスワードが適用されるレポートでは、**[暗号化パスワード]** ボックスが無効になり、パスワードがスケジュールプロセス中に作成されたものと同じであることを示すメッセージが下部に表示されます。

6. **[E メール]** をクリックします。

レポート結果がＥメールとして共有され、**[レポート]**ページが表示されます。レポートにパスワードを追加している場合、受信者はプロンプトが表示されたときにパスワードを入力する必要があります。

レポートスケジュールの編集

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

始める前に

レポートスケジュールを編集できるのは、所有者、管理者アカウントを保有するユーザー、またはそのレポートに対して **[設定可]** のアクセス許可を保有するユーザーのみです。

レポートスケジュールを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

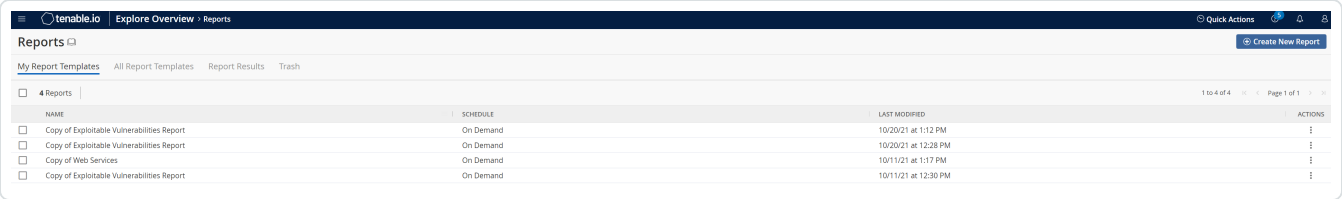
   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. スケジュールを編集するレポートを選択します。

範囲	アクション
1つのレポートスケジュールを編集する	**[レポート]** ページからレポートスケジュールを編集する方法 a. **[マイレポートテンプレート]** または **[すべてのレポートテンプレート]** タブで、編集するレポートの行を右クリックします。 -または- **[マイレポートテンプレート]** または **[すべてのレポートテンプレート]** タブの **[アクション]** 列で、編集するレポートの行の ⋮ ボタンをクリッ

	クします。 アクションボタンが行に表示されます。 b. **[スケジュール]** をクリックします。

[レポートをスケジュール] ペインが表示されます。



4. レポートのスケジュール設定を変更します。
5. **[スケジュール]** をクリックします。

   Tenable Vulnerability Management はレポートスケジュールを保存し、**[レポート]** ページが表示されます。

レポートの削除

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

レポートを削除できるのは、所有者または管理者アカウントのユーザーのみです。

レポートを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[アクション]** セクションで、**[レポート]** をクリックします。

   [マイレポートテンプレート] タブが選択された状態で **[レポート]** ページが表示されます。

3. 削除するレポートを選択します。

   注意: この手順は、**レポートの結果**と**レポートテンプレート**の両方に適用されます。

範囲	アクション
複数のレポートの削除	レポートを削除する方法 a. 削除する各レポートのチェックボックスを選択します。 リストの上部にアクションバーが表示されます。 b. アクションバーで、🗑 **[削除]** をクリックします。
1つのレポートの削除	1つのレポートを削除する方法

	a. 削除するレポートの行を右クリックします。 -または- 削除するレポートの横にあるチェックボックスを選択します。 Tenable Vulnerability Management は、アクションバーで **[さらに表示]** を有効にします。 -または- **[アクション]** 列で、削除するレポートの行の ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[削除]** をクリックします。

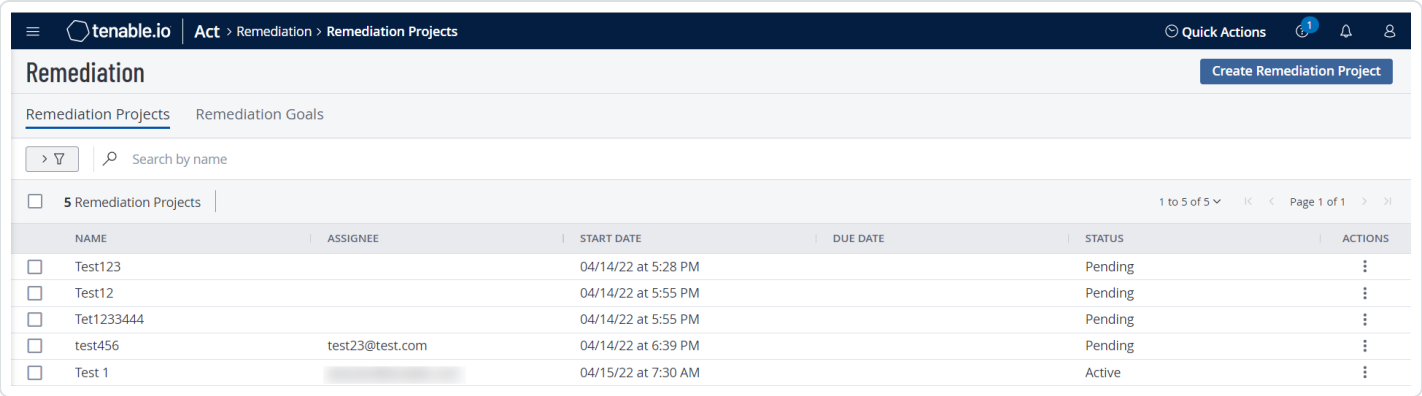
[レポートを削除] ダイアログボックスが表示されます。

4. **[削除]** をクリックします。

Tenable Vulnerability Management はレポートを完全に削除します。

修正

修正が必要なアイテムをすべて追跡するには、大きな労力を必要とします。**[修正]**ページで、環境内の脆弱性タスクに優先順位を付け、配信し、追跡する 2 つの異なる方法を作成すると、修正する項目の追跡が簡単になります。



修正の表示

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正 ページで、修正プロジェクトまたは修正目標を表示できます。

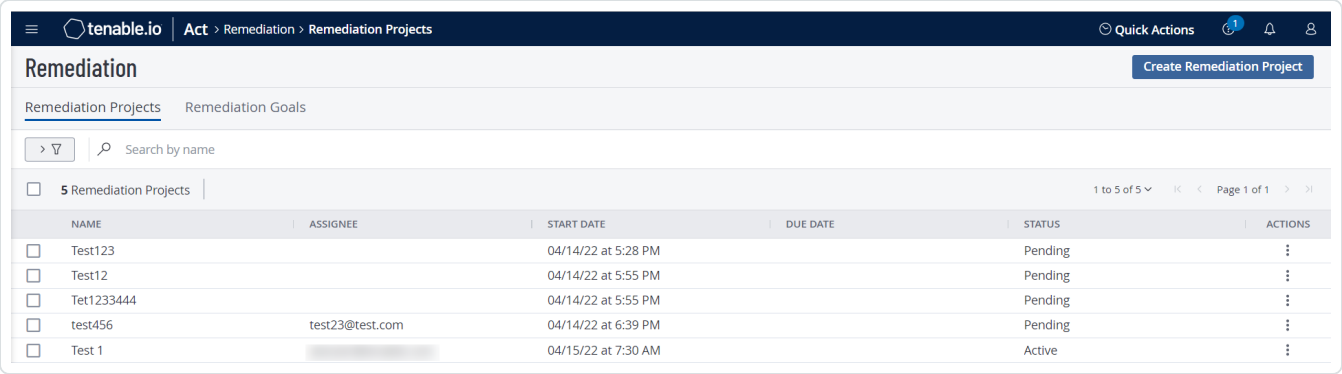
修正プロジェクトまたは目標を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. 次のいずれかを行います。

   - 修正プロジェクトを表示します。

     デフォルトでは、**[修正プロジェクト]** タブが表示されます。次の表では、各列を定義しています。

列	説明
名前	修正プロジェクトの名前。
担当者	修正プロジェクトに割り当てられているユーザーのユーザー名

資産タグ	プロジェクト作成時に追加される、修正プロジェクトに関連付けられた資産タグ。
開始日	割り当てられたユーザーが修正プロジェクトを開始した日時
期限	割り当てられたユーザーが修正プロジェクトを完了する予定の日時
ステータス	修正プロジェクトの状態。
アクション	修正プロジェクトで実行できるアクション

- 修正目標を表示します。

  修正目標を表示するには、**[修正目標]**タブをクリックします。次の表では、各列を定義しています。

列	説明
名前	修正目標の名前。
タイプ	目標が静的か動的かを示します。目標のタイプは、修正目標を作成したときに設定した期限日のオプションによって異なります。
開始日	修正目標が開始された日時
期限	修正目標を達成しなければならない期限の日時
ステータス	修正目標のステータス
資産タグ	プロジェクト作成時に追加される、修正プロジェクトに関連付けられた資産タグ。
アクション	修正目標で実行できるアクション

4. (オプション) 修正フィルターで説明したように、フィルターでビューを絞り込みます。

修正フィルター

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正 ページで、フィルターを使用して、表示される修正プロジェクトの目標を絞り込めます。

修正プロジェクト

次の表は、修正プロジェクトのフィルターを定義したものです。

フィルター	説明
資産タグ	プロジェクト作成時に追加される、プロジェクトに関連付けられた資産タグ。Tenable Vulnerability Management が「資産タグが次のオペレーティングシステムに等しい: Windows」などの肯定一致があるタグのみを返します。
担当者	修正プロジェクトに割り当てられているユーザー。
プロジェクト名	修正プロジェクトの名前。
プロジェクトの状態	修正プロジェクトの状態。

修正目標

次の表は、修正目標のフィルターを定義したものです。

フィルター	説明
資産タグ	プロジェクト作成時に追加される、プロジェクトに関連付けられた資産タグ。Tenable Vulnerability Management が「資産タグが次のオペレーティングシステムに等しい: Windows」などの肯定一致があるタグのみを返します。

目標名	修正目標の名前。
目標ステータス	修正目標のステータス。
目標タイプ	目標が静的か動的かを示します。目標のタイプは、修正目標を作成したときに設定した期限日のオプションによって異なります。

修正プロジェクト

修正プロジェクトは、修正プログラムの作成と管理に役立ちます。修正プロジェクトでは、作業の範囲を定義し、検出結果に優先順位を付け、プロジェクトを所有者に割り当て、修正タスクの進捗状況を追跡できます。修正プロジェクトのステータスにより、進行中または終了したすべての修正アクティビティを素早く視覚化できます。

次のタイプの修正プロジェクトを作成できます。

- **By fixed date** - 指定された日付までに完了する必要がある固定スコープの修正プロジェクト。
- **Within number of days** - 特定の期間内に完了する必要があるオープンスコープまたは進行中の修正プロジェクト。このタイプの修正プロジェクトにより、特定のタイプの重大な脆弱性を常に割り当てて追跡することができます。

詳細は、固定スコープの修正目標と進行中の修正目標 を参照してください。

[修正プロジェクト] ページで、以下のタスクを実行できます。

- 新しい修正プロジェクトの作成
- Findings から新しい修正プロジェクトを作成する
- 修正プロジェクトの詳細表示
- 修正プロジェクトをアクティブ化する
- 修正プロジェクトの編集
- 修正プロジェクトの一時停止
- 修正プロジェクトのクローズ
- 修正プロジェクトのエクスポート
- 修正プロジェクトの削除

新しい修正プロジェクトの作成

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: **[調査]** > **[検出結果]** から修正プロジェクトを作成することもできます。詳細については、検出結果から修正プロジェクトを作成するを参照してください。

修正プロジェクトを作成して、作業の範囲を定義し、検出結果に優先順位を付け、プロジェクトを所有者に割り当て、修正タスクの進捗状況を追跡できます。

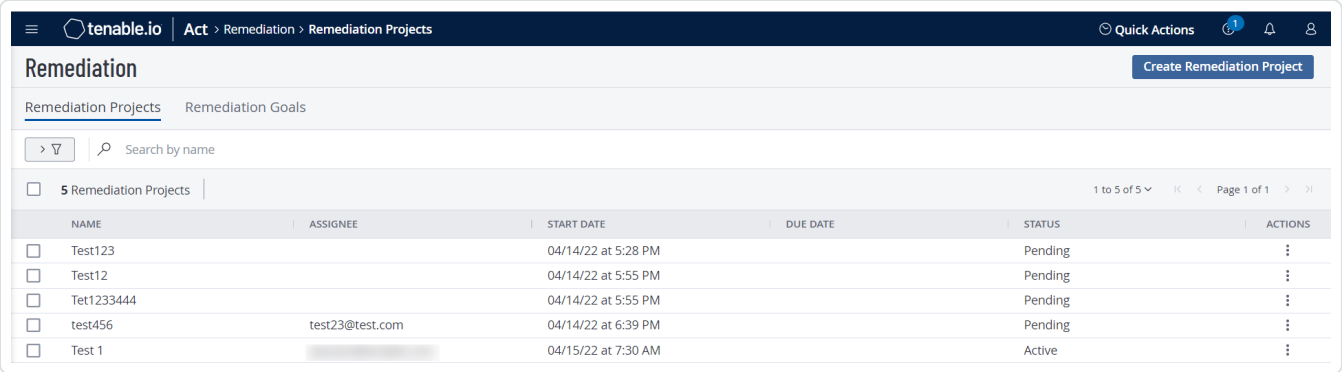
新しい修正プロジェクトを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. 右上の **[修正プロジェクトを作成する]** をクリックします。

   [修正プロジェクトの作成] ページが表示されます。

   ページの左側で、以下の選択肢から選択してから、**[次へ]** をクリックします。

オプション	アクション
名前	• **[プロジェクト名]** ボックスに、プロジェクトの名前を入力します。

	• (オプション) **[説明]** ボックスに、修正プロジェクトの説明を入力します。
範囲	**[検出結果フィルター]** セクションには、次のフィルターがデフォルトで選択されています。 • **変更されたリスクが承認済みになっていません** • **深刻度: 情報ではありません** • **ステータス: 修正済みではありません** **注意: [ステータス: 修正済みではありません]** フィルターが適用されると、プログレスバーに 0% と表示されます。修正プロジェクトの進捗率を表示するには、このフィルターを削除してください。 **注意:** 最大 5 つのフィルターを選択できます。 既存のフィルターを変更するか、**AND** および **OR** オプションでリストに新しいフィルターを追加できます。 **ヒント**: Tenable Vulnerability Management は、**範囲** のフィルターに基づいた検出数を示しています。 プロジェクトの範囲を指定するために使用する各フィルターについて、以下を実行します。 1. **[検出結果フィルター]** で、**[フィルターの選択]** をクリックします。 **[フィルターの選択]** ドロップダウンボックスが表示されます。 2. 適用するフィルターをクリックします。 フィルターが **[検出結果フィルター]** ボックスに表示されます。 3. フィルターで、v ボタンをクリックします。 フィルター値と演算子オプションのリストが表示されます。 4. 1 つ目のドロップダウンボックスで、フィルターに適用する演算子を選択します。

	5. 2 つ目のドロップダウンボックスで、フィルターに適用する値を 1 つ以上選択します。 6. ドロップダウンボックスで **[すべてに一致]** を選択します。デフォルトでは、Tenable Vulnerability Management はフィルターを **[すべてに一致]** に設定します。
割り当て	**[ユーザーまたはユーザーグループの選択]** ドロップダウンボックスで、修正プロジェクトを割り当てるユーザーまたはグループを選択します。
スケジュール	• **[開始日]** ボックスで、割り当てられたユーザーおよびグループを修正プロジェクトに含める日付を選択します。 • **[期限]** セクションで、次のいずれかを選択します。 • **日数以内** - プロジェクトの完了期限までの日数 **注意**: このオプションが選択された修正プロジェクトでは、**[プロジェクトの詳細]** ページの右側のプログレスバーは表示されません。 • **確定日順** - プロジェクトの完了期限の日付 詳細は、固定スコープの修正目標と進行中の修正目標 を参照してください。

4. **[保存]** をクリックします。

Tenable Vulnerability Management が修正プロジェクトを作成します。

注意: すべてのタスクが完了した場合や、プロジェクトが期日に達した場合でも、修正プロジェクトは自動的にクローズしません。完了後、プロジェクトのステータスを **[クローズ]** に変更して、プロジェクトを手動でクローズする必要があります。

Findings から新しい修正プロジェクトを作成する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

新しい修正プロジェクトを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[検出結果]** をクリックします。

   [検出結果] ページが表示され、検出結果を示す表が表示されます。**[脆弱性]** タブはデフォルトでアクティブになっています。

3. 修正プロジェクトを作成するには、次のいずれかを実行します。

   注意: [修正プロジェクトを作成する] オプションは、選択したフィルターが 3 つ以下の場合に利用できます。3 つを超えるフィルターを選択した場合、Tenable Vulnerability Management には **[修正プロジェクトを作成する]** オプションが表示されません。

作成	アクション
単一の検出結果に対する修正プロジェクト	a. 次のいずれかを行います。 • 修正プロジェクトを作成する結果の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 • 修正プロジェクトを作成する結果のチェックボックスを選択します。 アクションバーで、Tenable Vulnerability Management は **[さらに表示]** > ⊕ **[修正プロジェクトを作成する]** を有効にします。 • **[アクション]** 列で、作成する修正プロジェクトの行にある ⋮ ボタンをクリックします。

	アクションボタンが行に表示されます。 b. **[修正プロジェクトを作成する]** をクリックします。
複数の検出結果に対する修正プロジェクト	a. 修正プロジェクトを作成する結果のチェックボックスを選択します。 アクションバーで、Tenable Vulnerability Management は⊕ **[修正プロジェクトを作成する]** を有効にします。 b. ⊕ **[修正プロジェクトを作成する]** をクリックします。

4. **[修正プロジェクトの作成]** ページが表示されます。

   ページの左側で、以下の選択肢から選択してから、**[次へ]** をクリックします。

オプション	アクション
名前	• **[プロジェクト名]** ボックスに、プロジェクトの名前を入力します。 • (オプション) **[説明]** ボックスに、修正プロジェクトの説明を入力します。
範囲	**[検出結果フィルター]** セクションには、次のフィルターがデフォルトで選択されています。既存のフィルターを変更するか、**AND** および **OR** オプションでリストに新しいフィルターを追加できます。 • **資産 ID: <asset ID> と等しい** • **プラグイン ID: <plugin ID> と等しい** • **[検出結果]** ページで選択されたフィルター **ヒント**: Tenable Vulnerability Management は、**範囲** のフィルターに基づいた検出数を示しています。 プロジェクトの範囲を指定するために使用する各フィルターについて、以下を実行します。 1. **[検出結果フィルター]** で、**[フィルターの選択]** をクリックします。 **[フィルターの選択]** ドロップダウンボックスが表示されます。

	2. 適用するフィルターをクリックします。 フィルターが **[検出結果フィルター]** ボックスに表示されます。 3. フィルターで、v ボタンをクリックします。 フィルター値と演算子オプションのリストが表示されます。 4. 1 つ目のドロップダウンボックスで、フィルターに適用する演算子を選択します。 5. 2 つ目のドロップダウンボックスで、フィルターに適用する値を 1 つ以上選択します。 6. ドロップダウンボックスで **[すべてにー致]** を選択します。デフォルトでは、Tenable Vulnerability Management はフィルターを **[すべてにー致]** に設定します。
割り当て	**[ユーザーまたはユーザーグループの選択]** ドロップダウンボックスで、修正プロジェクトを割り当てるユーザーまたはグループを選択します。

スケジュール	• **[開始日]** ボックスで、割り当てられたユーザーおよびグループを修正プロジェクトに含める日付を選択します。
	
	• **[期限]** セクションで、次のいずれかを選択します。
	
	  • **日数以内** - プロジェクトの完了期限までの日数
	
	  • **確定日順** - プロジェクトの完了期限の日付

5. **[保存]** をクリックします。

Tenable Vulnerability Management が修正プロジェクトを作成します。

注意: すべてのタスクが完了した場合や、プロジェクトが期日に達した場合でも、修正プロジェクトは自動的にクローズしません。完了後、プロジェクトのステータスを **[クローズ]** に変更して、プロジェクトを手動でクローズする必要があります。

修正プロジェクトの詳細表示

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

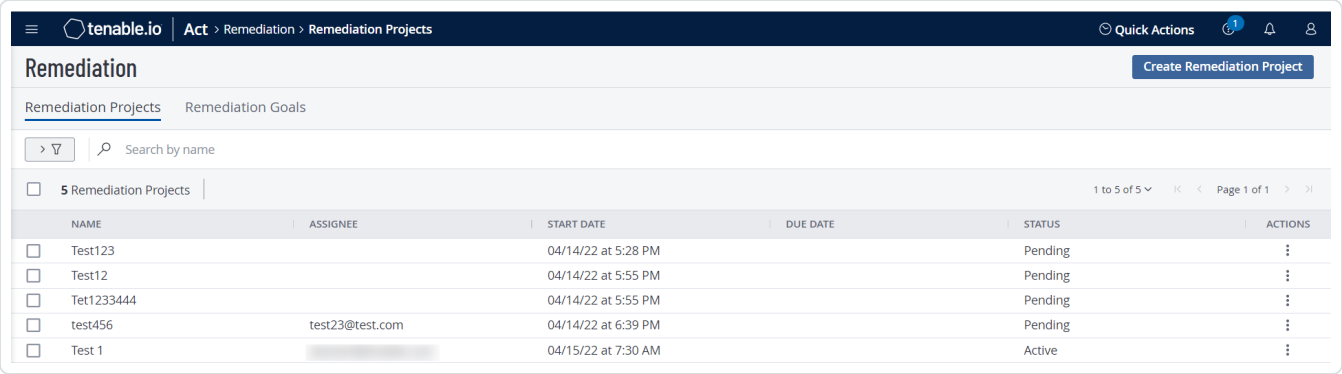
修正プロジェクトの詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。

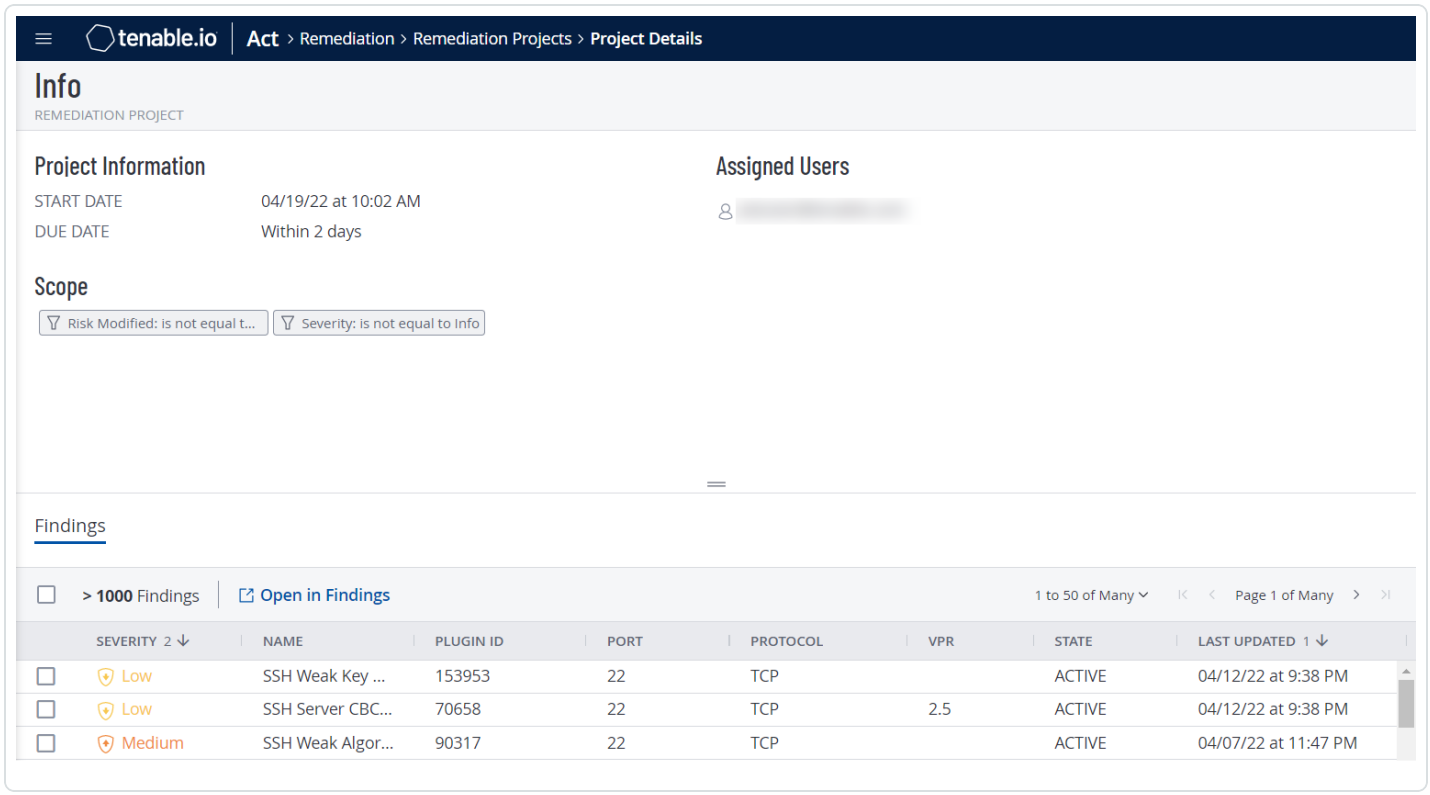


3. **修正プロジェクト** の表で、詳細を表示する修復プロジェクトの行をクリックします。

   修正プロジェクトの詳細 ページが表示されます。

修正プロジェクトの詳細

修正の**[プロジェクトの詳細]**ページには、修正プロジェクトの概要ビュー、修正プロジェクトの設定で指定されている脆弱性の検出結果に関する詳細、各修正プロジェクトの現在の進捗状況が表示されます。



注意:[プロジェクトの詳細]ページのデータは、ページから移動したり、ページを更新したりすると更新されます。

プロジェクトの詳細

[プロジェクトの詳細]ページには、修正プロジェクトに関する次の詳細が表示されます。

セクション	説明
プロジェクト情報	このセクションには、プロジェクトの**開始日**や**期限**など、修正プロジェクトに関する基本情報が表示されます。
範囲	このセクションには、修正プロジェクトに適用されているアクティブなフィルターが表示されます。詳細は、修正フィルターを参照してください。

割り当てられたユーザー	修正プロジェクトに割り当てられているユーザーの一覧。
検出結果	このセクションの表には、修正プロジェクトに関連するすべての検出結果が一覧表示されます。この表で次の情報を確認できます。 • **深刻度** - CVSS に基づく脆弱性の深刻度。詳細は、CVSS と VPR を参照してください。 • **名前** - 修正の検出結果の名前。 • **プラグイン ID** - 脆弱性を特定したプラグインの ID。 • **ポート** - スキャンで脆弱性が検出された資産に接続するためにスキャナーが使用したポート。 • **プロトコル** - スキャンで脆弱性が検出された資産との通信で、スキャナーが使用したプロトコル。 • **VPR** – Tenable が脆弱性に対して計算した VPR です。 • **状態** – 脆弱性の状態。 • **最終更新日** – スキャンが資産上で脆弱性を検出した直近の日付。 • **資産名** - スキャンで脆弱性が検出された資産の名前。この値は Tenable Vulnerability Management に対して一意です。 • **アクション** - この列の ⋮ ボタンをクリックしてドロップダウンを表示し、次の操作を実行できます。 ◦ **エクスポート** - 調査の表からのエクスポートで説明されているように、CSV または JSON にエクスポートします。 検出結果の表では、次の操作も実行できます。 • 表データを選別する • **[検出結果で開く]** をクリックして、[検出結果] ページで脆弱性の詳細を表示する • 1 つ以上の検出結果をエクスポートする

	1. エクスポートする検出結果の横にあるチェックボックスを選択します。 表の上部にアクションバーが表示されます。 2. アクションバーで、[→ **[エクスポート]** をクリックします。エクスポートの設定については、修正プロジェクトのエクスポートを参照してください。

修正プロジェクトの編集

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

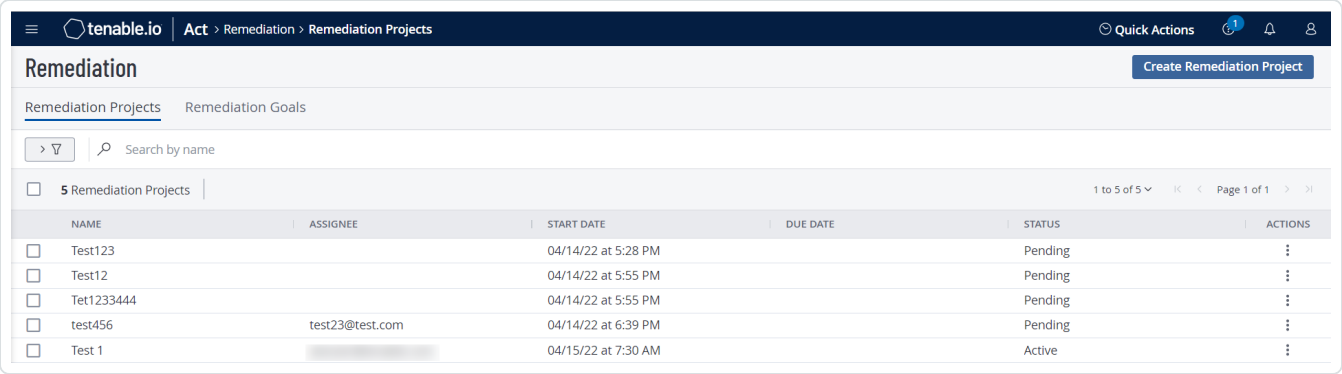
修正プロジェクトを編集します。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. 修正プロジェクトを編集します。

   a. **[修正プロジェクト]** のページで、次のいずれかを実行します。

      - **修正プロジェクト** の表で、編集する修正プロジェクトの行を右クリックします。

        アクションオプションがカーソルの横に表示されます。

      - **修正プロジェクト** の表で、編集する修正プロジェクトのチェックボックスを選択します。

        表の上部にアクションバーが表示されます。

      - **修正プロジェクト** の表の **[アクション]** 列で、編集するプロジェクトの行にある ⋮ ボタンをクリックします。

        アクションボタンが行に表示されます。

4. ✎ **[編集]** をクリックします。

[プロジェクトの編集] ページが表示されます。

5. 修正プロジェクトの設定を変更します。
6. **[保存]** をクリックします。

   Tenable Vulnerability Management が修正プロジェクトを保存し、**[修正プロジェクト]** ページが表示されます。

修正プロジェクトをアクティブ化する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正プロジェクトを作成すると、プロジェクトは **[保留中]** のステータスになります。修正プロジェクトの進捗状況の追跡を開始するには、プロジェクトをアクティブ化する必要があります。

注意: プロジェクトをアクティブ化するには、スコープと担当者を定義する必要があります。

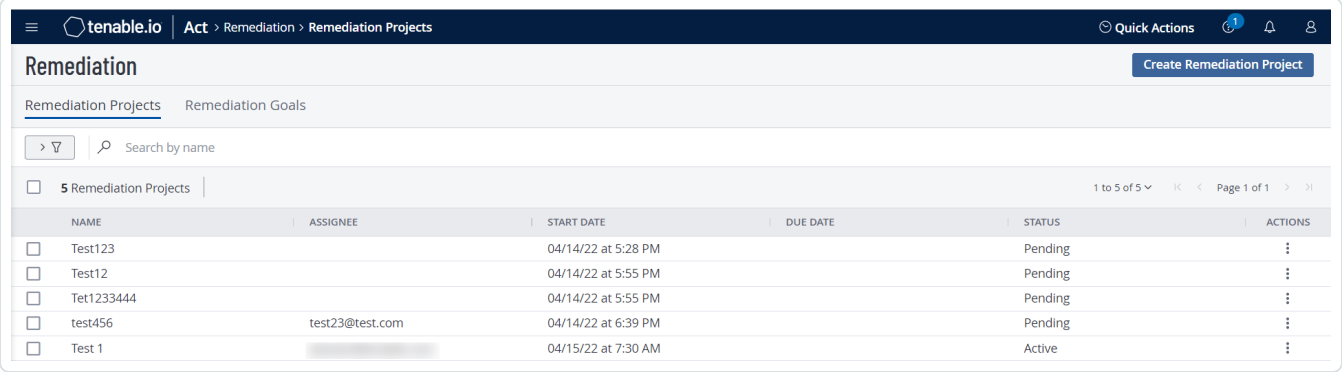
修正プロジェクトをアクティブ化する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正プロジェクト]** の表で、次のいずれかを実行します。

   - **修復プロジェクト** の表で、アクティブ化する修正プロジェクトの行を右クリックします。

     アクションオプションがカーソルの横に表示されます。

   - **修復プロジェクト** の表で、アクティブ化する修正プロジェクトのチェックボックスを選択します。

     表の上部にアクションバーが表示されます。

   - **修正プロジェクト** の表の **[アクション]** 列で、アクティブ化するプロジェクトの行にある ⋮ ボタンを

クリックします。

アクションボタンが行に表示されます。

4. **[アクティブ]** をクリックします。

   Tenable Vulnerability Management が修正プロジェクトをアクティブ化します。

   [修正プロジェクト] ページが表示され、**[ステータス]** 列にプロジェクトが **[アクティブ]** と表示されます。

修正プロジェクトの一時停止

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正プロジェクトを一時停止すると、プロジェクトの進行状況の追跡が一時的に停止します。プロジェクトを中断しても、プロジェクトがアクティブ化されるまで、プロジェクトのステータスは変わりません。

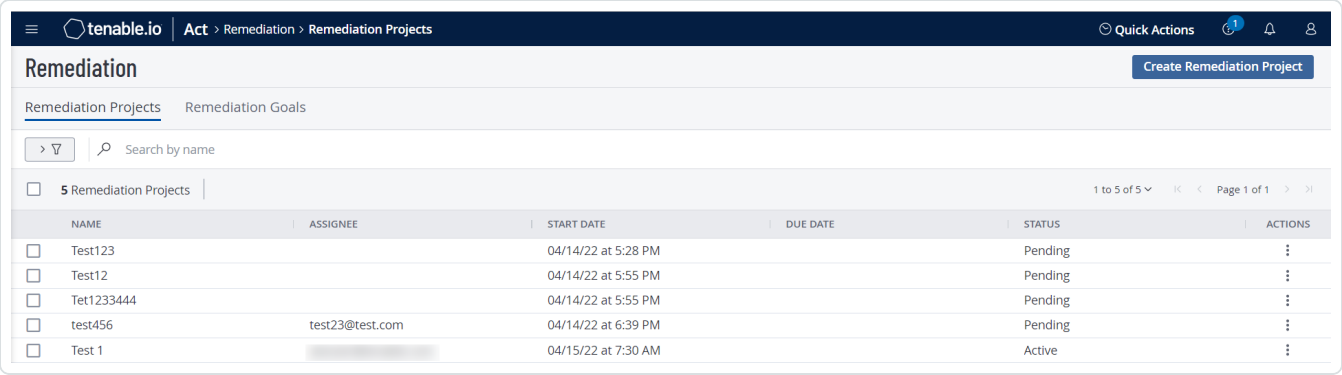
修正プロジェクトを一時停止する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. 次のいずれかを行います。

   - **修正プロジェクト** の表で、一時停止する修正プロジェクトの行を右クリックします。

     アクションオプションがカーソルの横に表示されます。

   - **修正プロジェクト** の表で、一時停止する修正プロジェクトのチェックボックスを選択します。

     アクションバーで、Tenable Vulnerability Management は **[その他]** > **[一時停止]** を有効にします。

- **修正プロジェクト**の表の**[アクション]**列で、一時停止するプロジェクトの行にある ⋮ ボタンをクリックします。

  アクションボタンが行に表示されます。

4. **[一時停止]**をクリックします。

   Tenable Vulnerability Management が修正プロジェクトを一時停止します。

   [修正プロジェクト]ページが表示され、**[ステータス]**列にプロジェクトが**[一時停止済み]**と表示されます。

修正プロジェクトのクローズ

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正プロジェクトはクローズされると終了したことになります。ただし、必要に応じて、クローズされたプロジェクトをアクティブ化できます。すべてのタスクが完了した場合や、プロジェクトが期日に達した場合でも、プロジェクトは自動的にクローズされません。完了後、プロジェクトのステータスを **[クローズ]** に変更して、プロジェクトを手動でクローズする必要があります。

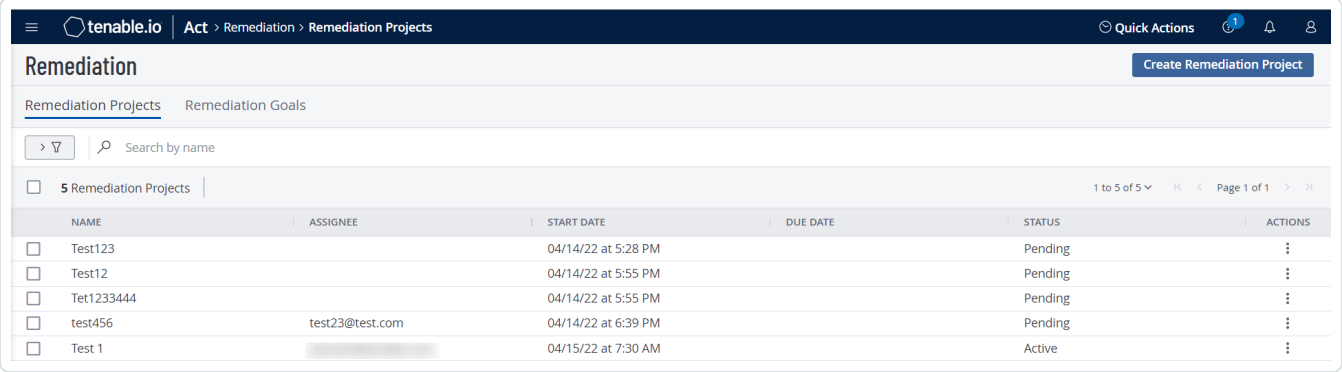
修正プロジェクトをクローズする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. 次のいずれかを行います。

   - **修復プロジェクト** の表で、クローズする修正プロジェクトの行を右クリックします。

     アクションオプションがカーソルの横に表示されます。

   - **修復プロジェクト** の表で、クローズする修正プロジェクトのチェックボックスを選択します。

     アクションバーで、Tenable Vulnerability Management は **[さらに表示]** > **[クローズ]** を有効にします。

- **修正プロジェクト**の表の**[アクション]**列で、クローズするプロジェクトの行にある ⋮ ボタンをクリックします。

  アクションボタンが行に表示されます。

4. **[閉じる]**をクリックします。

   Tenable Vulnerability Management が修正プロジェクトをクローズします。

   [修正プロジェクト]ページが表示され、**[ステータス]**列にプロジェクトが**[クローズ済み]**と表示されます。

修正プロジェクトのエクスポート

[修正] ページで、修正プロジェクトを CSV 形式でエクスポートできます。

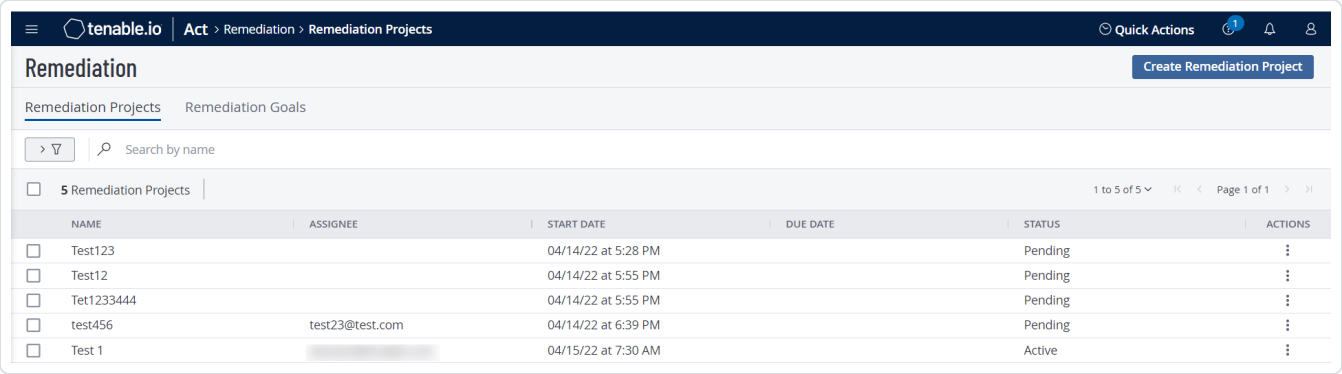
修正プロジェクトをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

4. 次のいずれかを行います。

単一の修正プロジェクトをエクスポートする場合

a. 修正プロジェクトの表で、エクスポートする修正プロジェクトの行を右クリックします。

   アクションオプションがカーソルの横に表示されます。

   -または-

   修正プロジェクトの表の **[アクション]** 列で、エクスポートする修正プロジェクトの行にある ⋮ ボタンをクリックします。

   アクションボタンが行に表示されます。

b. **[エクスポート]** をクリックします。

複数の修正プロジェクトをエクスポートする場合

a. 修正プロジェクトの表で、エクスポートする各修正プロジェクトのチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで、[→ **[エクスポート]** をクリックします。

> **注意:** 個別に選択してエクスポートできる修正プロジェクトは最大 200 個です。200 件以上の修正プロジェクトをエクスポートする場合は、**[プロジェクト]** の表の一番上にあるチェックボックスを選択して、Tenable Vulnerability Management インスタンスのすべての修正プロジェクトを選択してから、[→**[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。

5. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
6. 使用するエクスポート形式をクリックします。

形式	説明
CSV	タグのカテゴリまたは値のリストを含む CSV テキストファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	タグのカテゴリまたは値がネストされたリストを含む JSON ファイル。 Tenable Vulnerability Management は JSON ファイルに空のフィールドを含めません。

7. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
8. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

> **注意**: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

9. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

- **[スケジュール]**トグルをクリックします。

  [スケジュール] セクションが表示されます。

- **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
- **[タイムゾーン]**ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
- **[繰り返し]**ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
- **[繰り返し終了]**ドロップダウンで、スケジュールが終了する日付を選択します。

  注意: [無し]を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

10. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]**トグルをクリックします。

      [メール通知] セクションが表示されます。

    - **[受信者の追加]**ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須) **[パスワード]**ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      注意: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

11. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

12. ブラウザのダウンロード ディレクトリを介して、エクスポート ファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]** でエクスポート ファイルにアクセスできます。

修正プロジェクトの削除

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

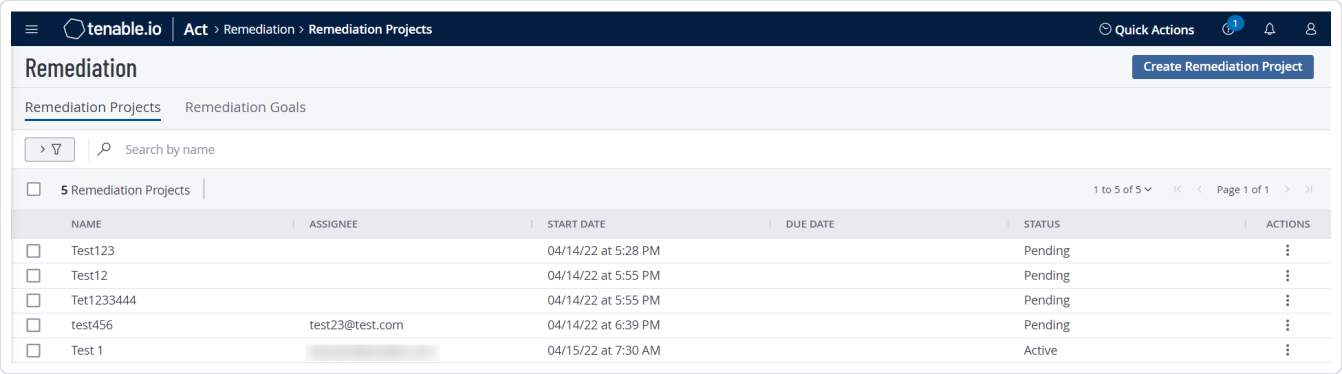
修正プロジェクトを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. 次の方法で、単一または複数の修正プロジェクトを削除します。

削除	アクション
単一の修正プロジェクト	a. 次の方法で単一の修正プロジェクトを削除します。 • **修正プロジェクト**の表の **[アクション]** 列で、削除するプロジェクトの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 • **修復プロジェクト**の表で、削除する修正プロジェクトの横にあるチェックボックスを選択します。 アクションバーで、Tenable Vulnerability Management は **[さらに表示]** > **[削除]** を有効にします。 • **修正プロジェクト**の表で、削除するプロジェクトの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 b. **[削除]** をクリックします。
複数の修正プロジェクト	a. **修正プロジェクト**の表で、削除する 1 つ以上の修正プロジェクトを選択します。 Tenable Vulnerability Management では、アクションバーの **[削除]** ボタンが有効になります。 b. **[削除]** をクリックします。

Tenable Vulnerability Management は、選択した修正プロジェクトを削除します。

修正目標

修正目標により、修正プログラムの有効性を測定できます。修正目標を設定することで、修正プロジェクトによって特定の期間内の重大な検出結果が適切に追跡され、クローズされているかどうかを追跡できます。

次のタイプの修正目標を作成できます。

- **By fixed date** - 指定された期日までに達成しなければならない修正目標。達成できなかった場合、目標は失敗します。
- **Within the number of days** - 特定の日数以内に達成しなければならない修正目標。Tenable Vulnerability Management は、このタイプの目標を動的目標または継続的目標として分類します。
- **Ongoing** - 特定の範囲のすべての結果が修正されるまで未解決のままである、継続的または動的な目標

[修正目標] ページで、以下のタスクを実行できます。

- 新しい修正目標の作成
- 修正目標の詳細表示
- 修正目標のアクティブ化
- 修正目標の編集
- 修正目標の一時停止
- 修正目標のクローズ
- 修正目標のエクスポート
- 修正目標の削除

固定スコープの修正目標と進行中の修正目標

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正目標を作成するときに、スコープを固定にするか進行中にするかを設定できます。

固定スコープの目標 - これは、脆弱性のグループまたは1つの脆弱性を一定期間内に修正する必要があるシナリオに該当します。

進行中 (オープンスコープ) の目標 - これは、特定のタイプの脆弱性を追跡するための所有者が常に割り当てられている必要のあるシナリオに該当します。たとえば、修正が必要なすべての重大な Tenable PCI ASV 脆弱性を所有者に割り当てる場合です。

修正目標を作成するには、新しい修正目標の作成を参照してください。

新しい修正目標の作成

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正目標は、静的または動的にすることができます。静的修正目標には固定の期限があります。一方、動的目標には固定の期限はありませんが、指定期間内に目標を達成するか、進行中のステータスにする必要があります。

たとえば、動的修正目標を設定して、Log4J の結果がシステムに存在しないようにします。この修正目標を**Ongoing**として設定できます。Log4J の結果のカウントがゼロより大きくなると、目標は失敗します。

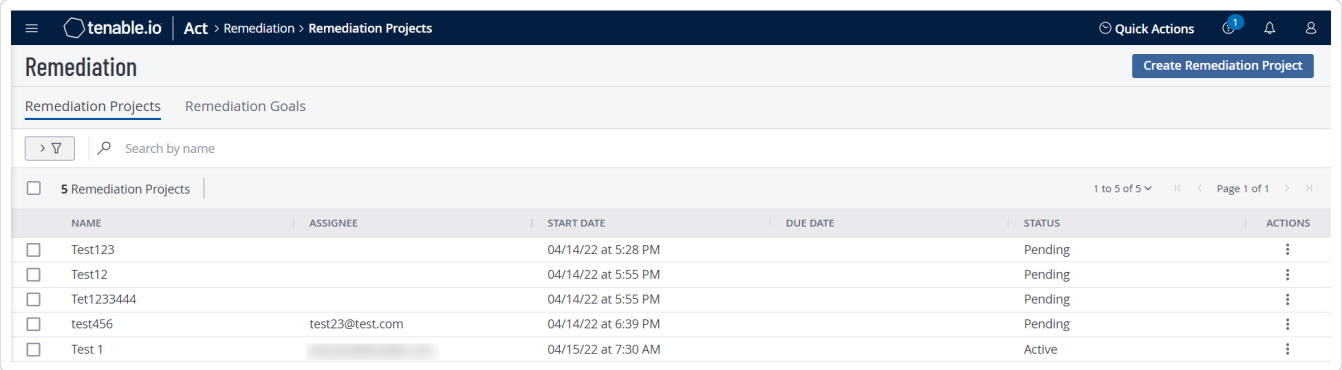
新しい修正目標を作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

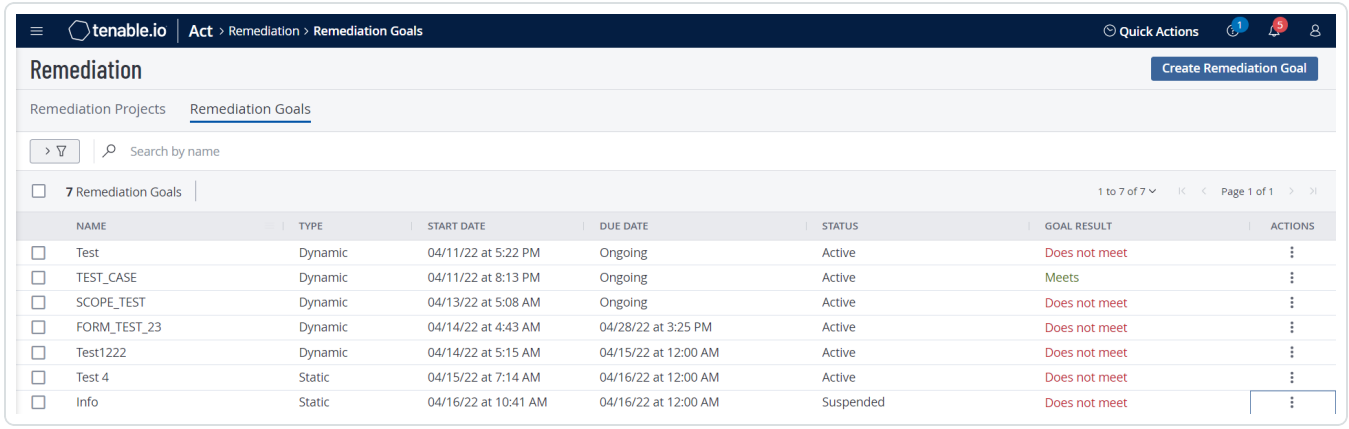
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. 右上の**[修正目標を作成する]**をクリックします。

   [修正目標の作成]ページが表示されます。

   ページの左側で、以下の選択肢から選択してから、**[次へ]**をクリックします。

オプション	アクション
名前	• **[目標名]**ボックスに、修正目標の名前を入力します。 • **[説明]**ボックスに、修正目標の説明を入力します。
条件	**[検出結果フィルター]**セクションには、次のフィルターがデフォルトで選択されています。 • **深刻度は情報ではありません** • **ステータスが修正済みではありません** **注意:** 最大 5 つのフィルターを選択できます。 既存のフィルターを変更するか、**AND** および **OR** オプションでリストに新しいフィルターを追加できます。 **ヒント**: Tenable Vulnerability Management は、**範囲** のフィルターに基づいた検出数を示しています。 1. **[検出結果フィルター]**で、**[フィルターの選択]**をクリックします。

	[フィルターの選択]ドロップダウンボックスが表示されます。 2. 適用するフィルターをクリックします。 フィルターが**[検出結果フィルター]**ボックスに表示されます。 3. フィルターで、 ボタンをクリックします。 フィルター値と演算子オプションのリストが表示されます。 4. 1つ目のドロップダウンボックスで、フィルターに適用する演算子を選択します。 5. 2つ目のドロップダウンボックスで、フィルターに適用する値を1つ以上選択します。 6. ドロップダウンボックスで**[すべてに一致]**を選択します。デフォルトでは、Tenable Vulnerability Managementはフィルターを**[すべてに一致]**に設定します。
目標期限	次のいずれかのオプションを選択して設定します。 **注意:** Tenable Vulnerability Managementは、設定した期限オプションに基づいて、修正目標タイプを決定します。**[日数以内]**または**[継続中]**のオプションを設定する場合、Tenable Vulnerability Managementは動的目標として目標を作成します。**[確定日順]**を選択した場合、Tenable Vulnerability Managementは目標を静的タイプとして作成します。 • **日数以内** - 目標の完了期限までの日数 • **確定日順** - 目標の完了期限の日付 • **継続中** - 進行中の目標は、常に進行中の修正目標であり、常に達成する必要があります。このオプションはデフォルトで選択されています。 詳細は、固定スコープの修正目標と進行中の修正目標を参照してください。

5. **[保存]**をクリックします。

Tenable Vulnerability Managementが修正目標を保存します。

修正目標の詳細表示

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

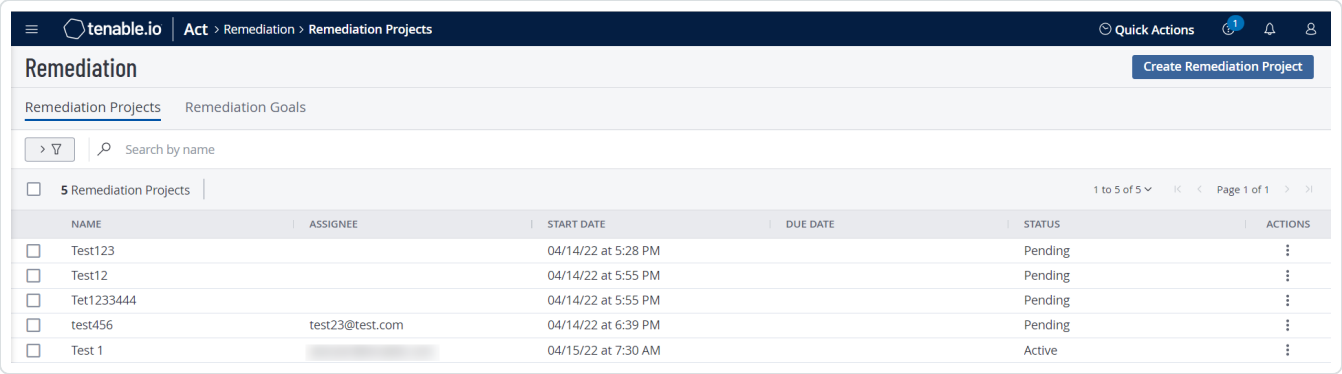
修正目標の詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

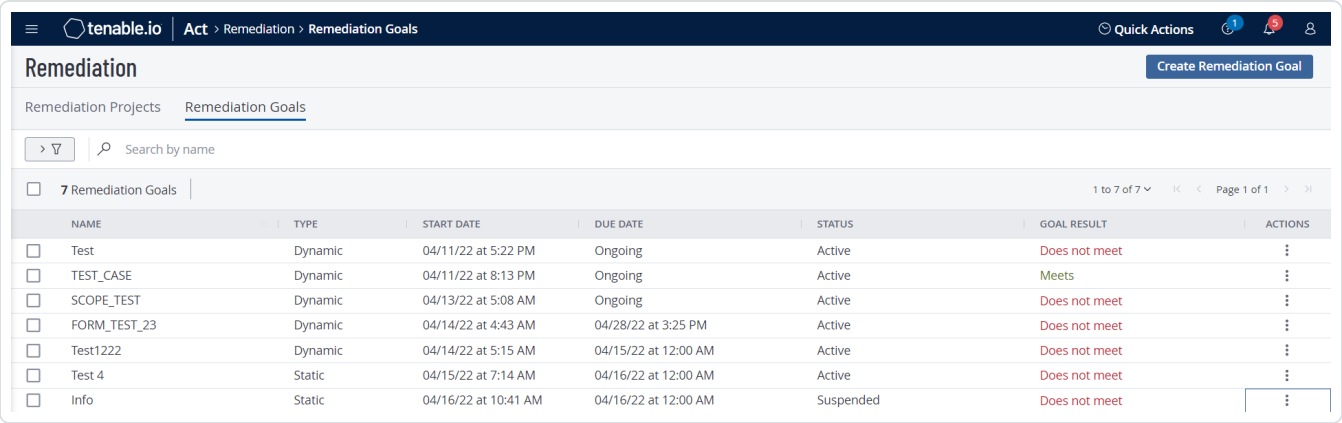
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. **[修正目標]** の表で、詳細を表示する任意の行をクリックします。

   [目標の詳細] ページが表示されます。

[目標の詳細] ページには、修正目標に関する次の詳細が表示されます。

セクション	説明
目標情報	修正目標のタイプ、開始日、期限
成功の基準	検出結果に割り当てられたフィルターフィルターに一致するインスタンスの数がゼロの場合は、修正目標が成功であることを示しています。
検出結果	• 表データを選別します。 • ホスト脆弱性の検出結果をエクスポートします。 • **[検出結果で開く]** をクリックして、[検出結果] ページで脆弱性の詳細を表示します。
進捗状況	修正目標の全体的な進行状況このセクションには、以下の情報が表示されます。 **注意:** これらのパラメーターは、期日が固定されている目標 (静的目標) にのみ適用されます。動的修正目標の場合、Tenable Vulnerability Management は進捗状況バーを表示しません。 • **作成日** - 修正プロジェクトが作成された日時。 • **修正済み** - 修正済みの結果の数。 • **再表面化** - 修正後に再出現した検出結果の数。

修正目標の編集

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

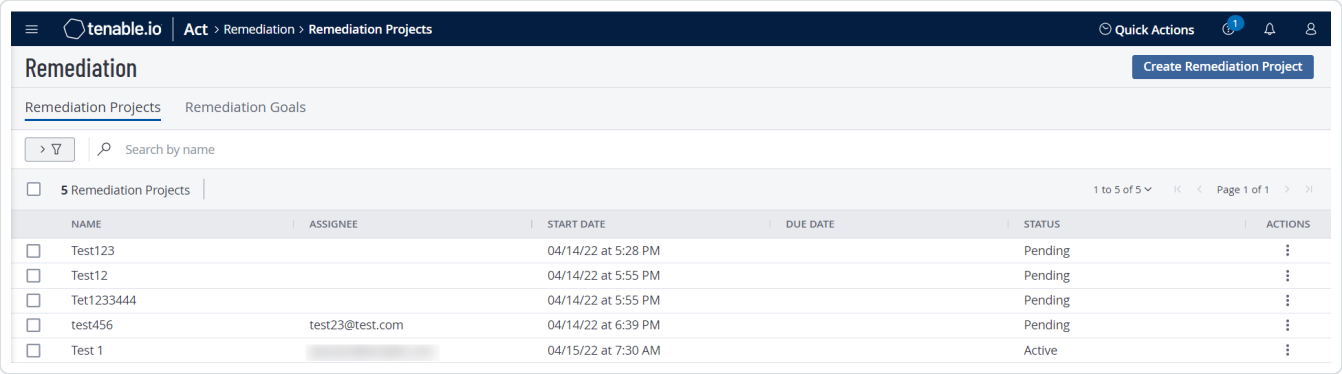
修正目標を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

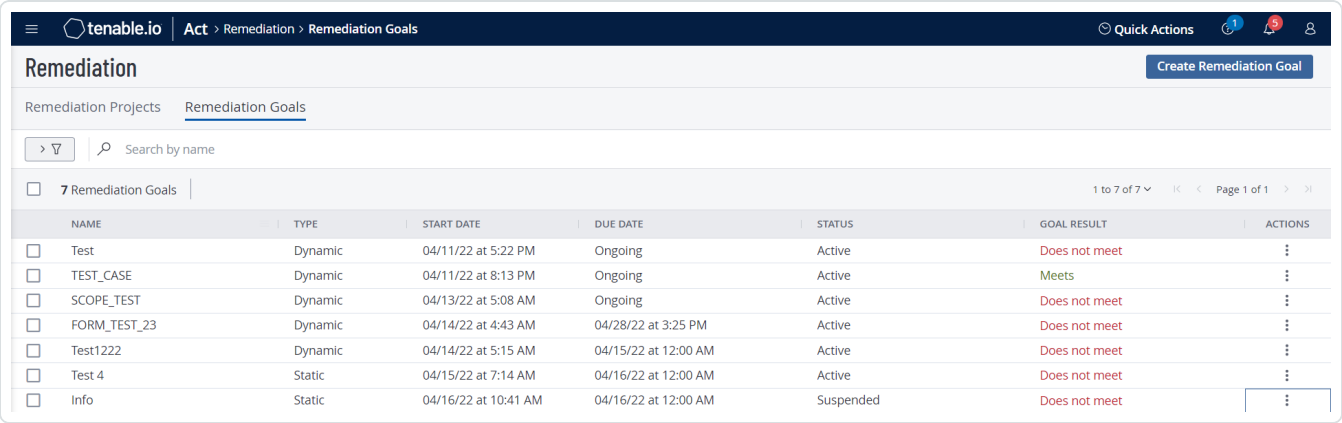
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. 次のいずれかを行います。

- **修復目標**の表で、編集する修正目標の行を右クリックします。

  アクションオプションがカーソルの横に表示されます。

- **修復目標**の表で、編集する修正目標のチェックボックスを選択します。

  表の上部にアクションバーが表示されます。

- **修正目標**の表の**[アクション]**列で、編集する目標の行にある ⋮ ボタンをクリックします。

  アクションボタンが行に表示されます。

5. ✎ **[編集]**をクリックします。

   [目標の修正]ページが表示されます。

6. 修正目標の設定を変更します。

7. **[保存]**をクリックします。

   Tenable Vulnerability Management が修正目標を保存します。

   [修正目標]ページが表示されます。

修正目標のアクティブ化

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

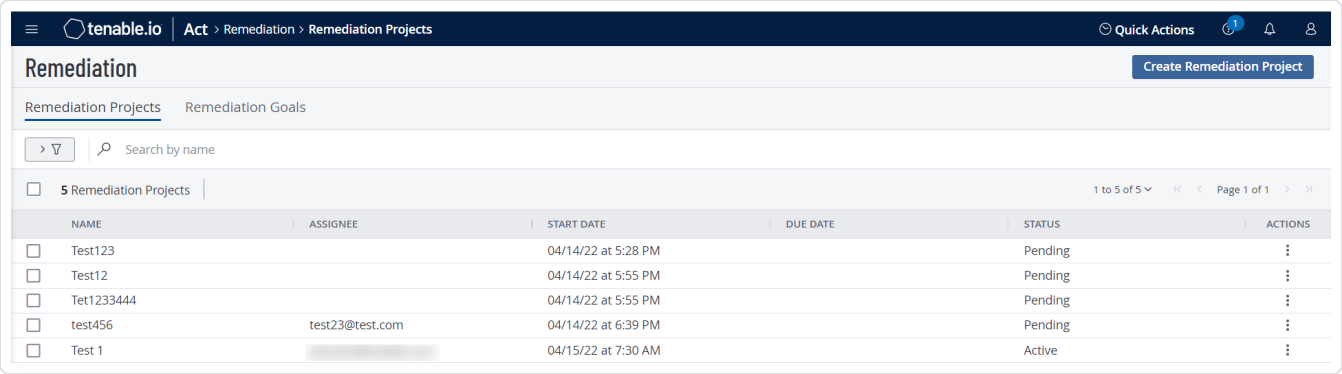
修正目標をアクティブ化する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

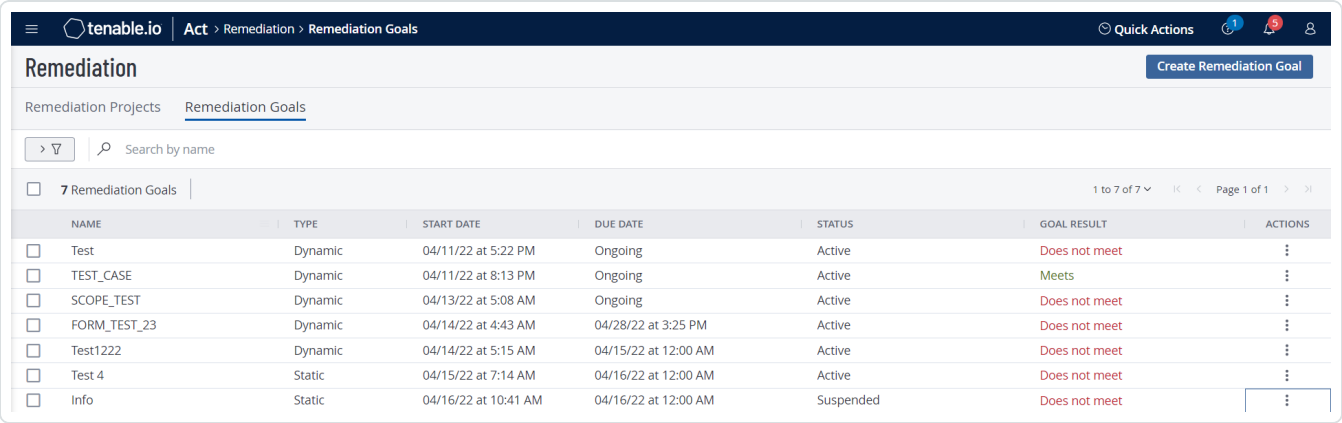
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. 次のいずれかを行います。

    - **修復目標**の表で、アクティブ化する修正目標の行を右クリックします。

      アクションオプションがカーソルの横に表示されます。

    - **修復目標**の表で、アクティブ化する修正目標のチェックボックスを選択します。

      表の上部にアクションバーが表示されます。

    - **修正目標**の表の**[アクション]**列で、アクティブ化する目標の行にある ⋮ ボタンをクリックします。

      アクションボタンが行に表示されます。

5. **[アクティブ]**をクリックします。

Tenable Vulnerability Management が修正目標をアクティブ化します。

[**修正目標**] ページが表示され、[**ステータス**] 列にプロジェクトが [**アクティブ**] と表示されます。

修正目標の一時停止

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

目標を一時的に中断し、いつでも再アクティブ化できます。

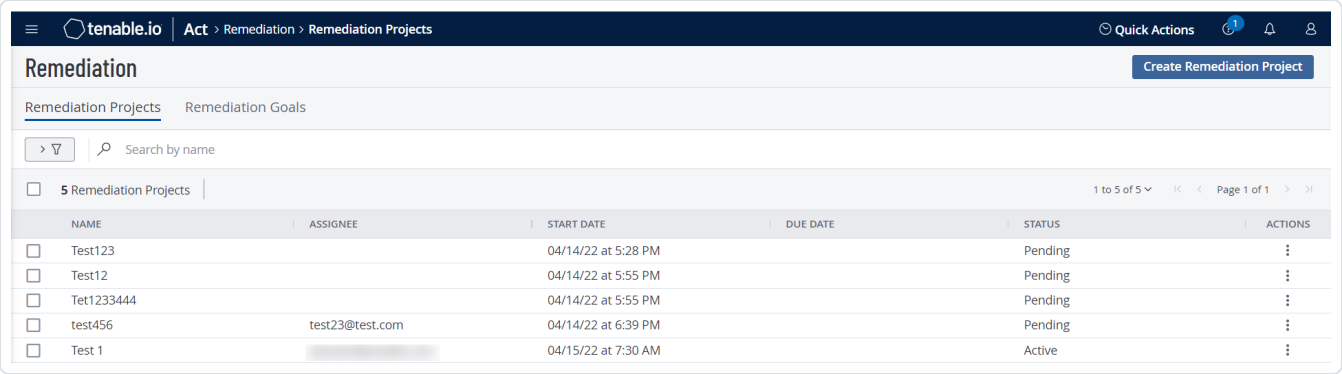
修正目標を一時停止する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

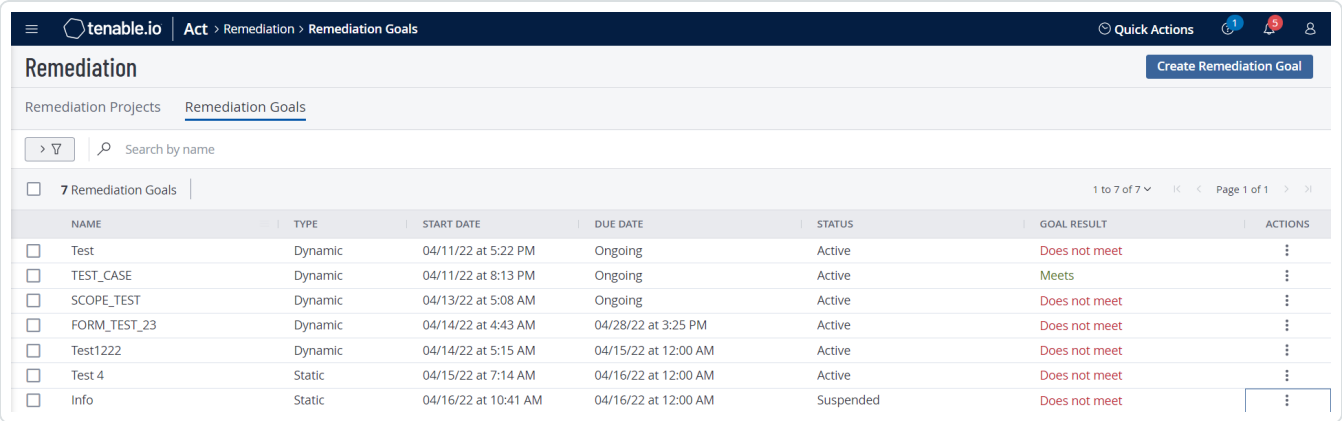
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. 次のいずれかを行います。

   - **修復目標**の表で、一時停止する修正目標の行を右クリックします。

     アクションオプションがカーソルの横に表示されます。

   - **[修正目標]**の表で、一時停止する修正目標のチェックボックスを選択します。

     アクションバーで、Tenable Vulnerability Management は**[その他]** > **[一時停止]**を有効にします。

   - **修正目標**の表の**[アクション]**列で、一時停止する目標の行にある ⋮ ボタンをクリックします。

     アクションボタンが行に表示されます。

5. **[一時停止]**をクリックします。

   Tenable Vulnerability Management が修正目標を一時停止します。

   [修正目標]ページが表示され、**[ステータス]**列に目標が**[一時停止済み]**と表示されます。

修正目標のクローズ

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

修正目標はクローズされると終了したことになります。ただし、必要に応じて、クローズされた目標をアクティブ化できます。

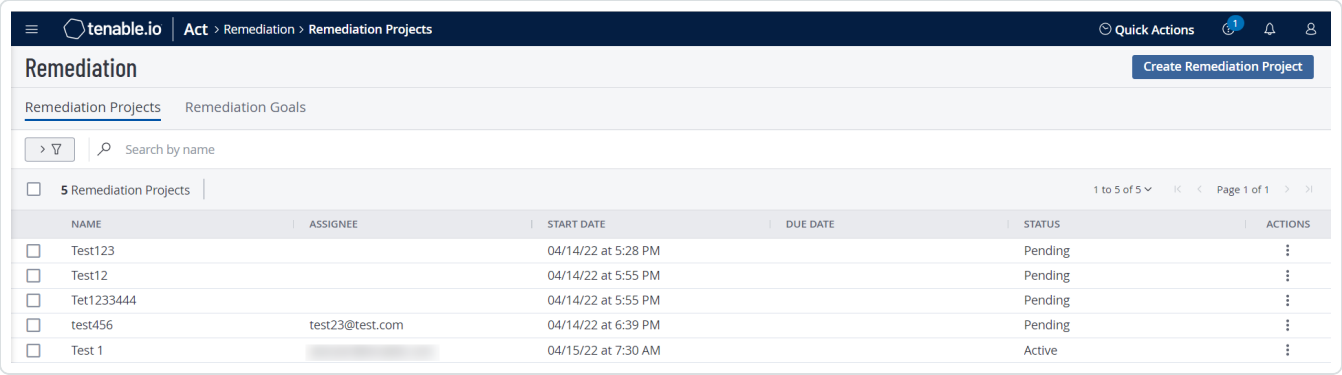
修正目標をクローズする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

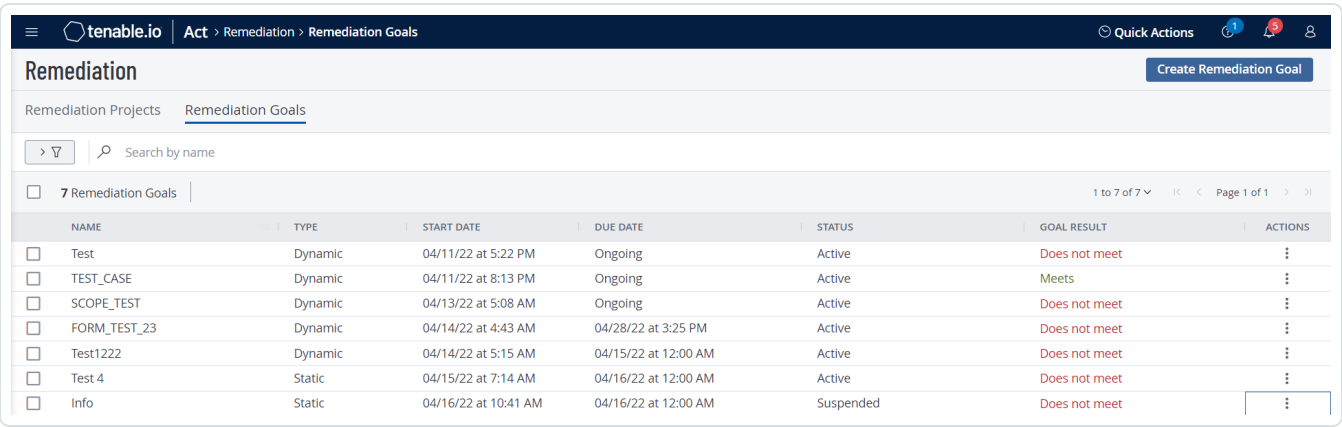
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. 次のいずれかを行います。

   - **修復目標**の表で、クローズする修正目標の行を右クリックします。

     アクションオプションがカーソルの横に表示されます。

   - **修復目標**の表で、クローズする修正目標のチェックボックスを選択します。

     アクションバーで、Tenable Vulnerability Management は**[さらに表示]** > **[クローズ]**を有効にします。

   - **修正目標**の表の**[アクション]**列で、クローズする目標の行にある ⋮ ボタンをクリックします。

     アクションボタンが行に表示されます。

5. **[閉じる]**をクリックします。

   Tenable Vulnerability Management が修正目標をクローズします。

   [修正目標]ページが表示され、**[ステータス]**列にプロジェクトが**[クローズ済み]**と表示されます。

修正目標のエクスポート

[修正] ページで、修正目標を CSV 形式でエクスポートできます。

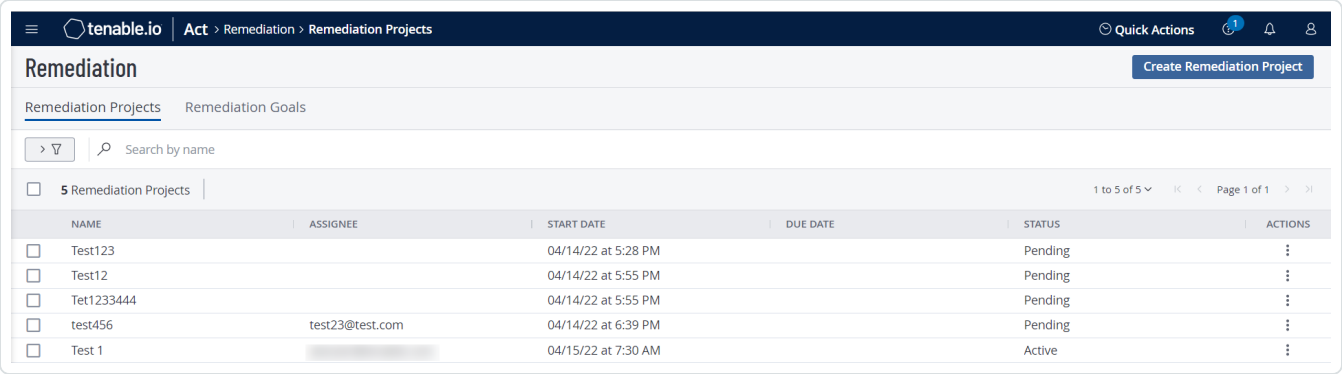
修正目標をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

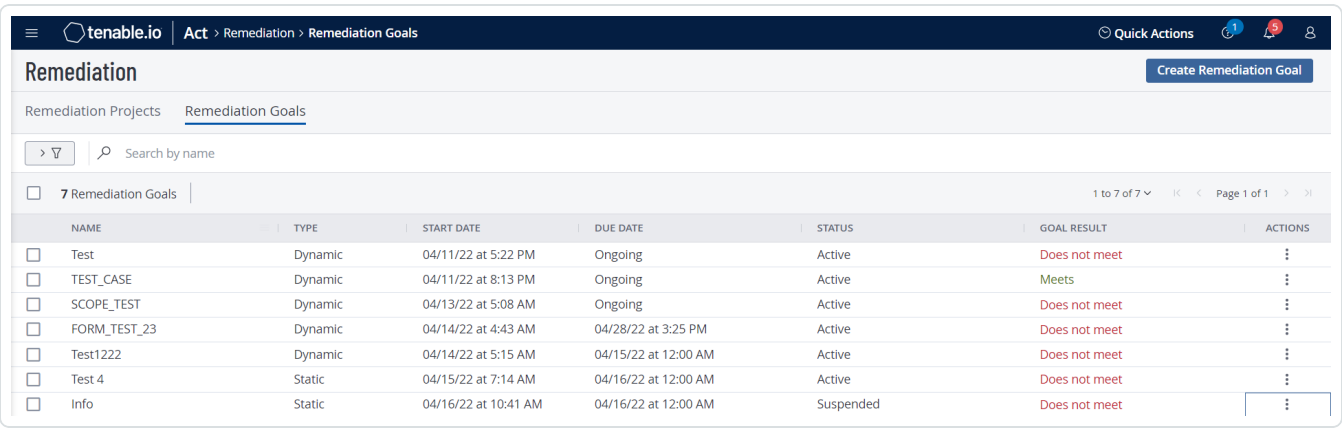
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. 次のいずれかを行います。

単一の修正目標をエクスポートする場合

a. 修復目標の表で、エクスポートする修正目標の行を右クリックします。

アクションオプションがカーソルの横に表示されます。

-または-

修正目標の表の**[アクション]**列で、エクスポートする修正目標の行にある ⋮ ボタンをクリックします。

アクションボタンが行に表示されます。

b. **[エクスポート]**をクリックします。

複数の修正目標をエクスポートする場合

a. 修復目標の表で、エクスポートする各修正目標のチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで、[→ **[エクスポート]**をクリックします。

> **注意:** 個別に選択してエクスポートできる修正目標は最大 200 個です。200 個以上の修正目標をエクスポートする場合は、**目標**の表の上部にあるチェックボックスを選択して、Tenable Vulnerability Management インスタンス上のすべての修正目標を選択してから、[→**[エクスポート]**をクリックする必要があります。

[エクスポート]プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、Tenable Vulnerability Management はすべてのフィールドを選択します。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス。
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]**ボックスに、エクスポートファイルの名前を入力します。

7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	タグのカテゴリまたは値のリストを含む CSV テキストファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]** でエクスポートファイルにアクセスできます。

修正目標の削除

必要な Tenable Vulnerability Management ユーザーロール: 基本ユーザー、スキャンオペレーター、標準、スキャンマネージャー、または管理者

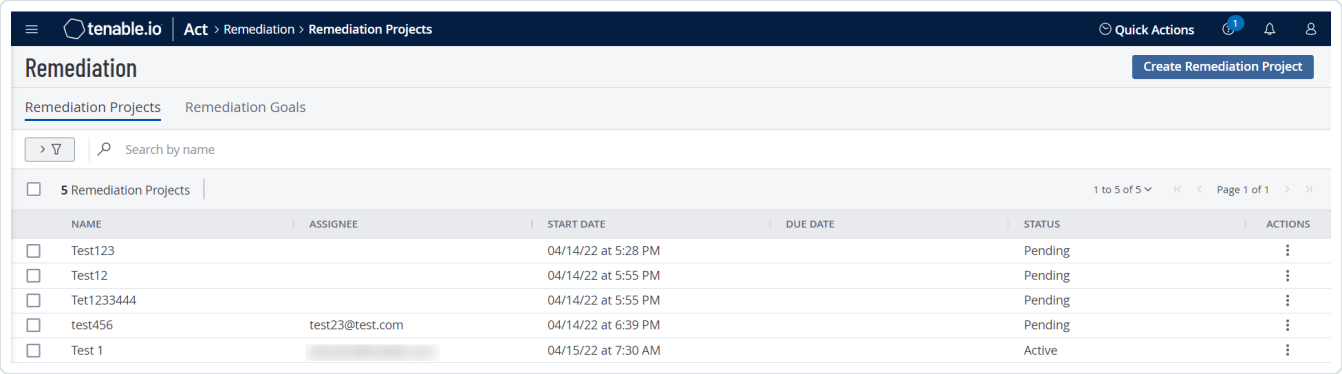
修正目標を削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

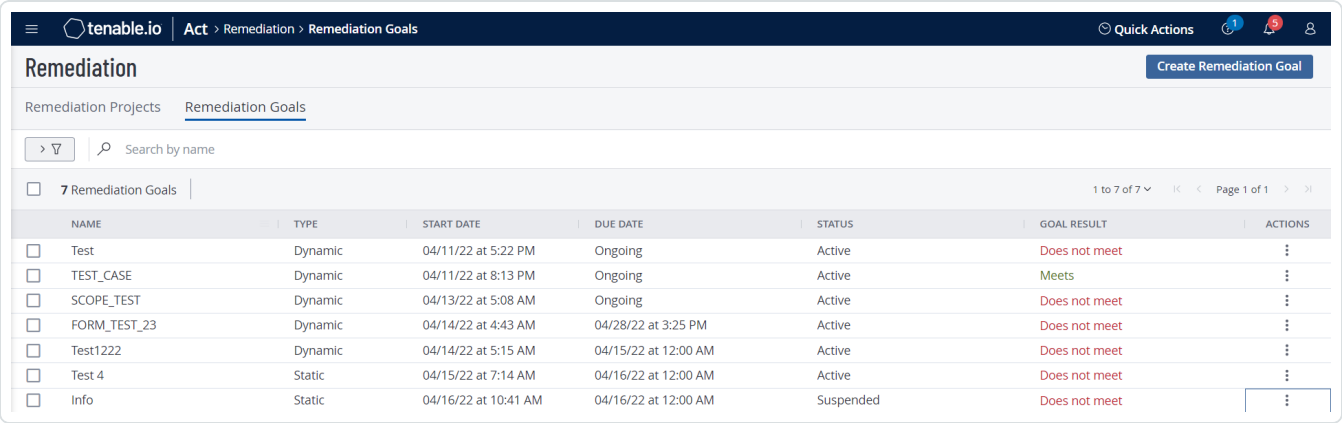
2. 左のナビゲーションプレーンの **[Act]** セクションで、**[修正]** をクリックします

   [修正] ページが表示されます。デフォルトでは、**[修正プロジェクト]** タブが有効になっています。



3. **[修正目標]** タブをクリックします。

   [修正目標] ページが表示されます。



4. 次の方法で、単一または複数の修正目標を削除します。

削除	アクション
単一の修正目標	a. 次のいずれかを行います。 • 修正目標の表の **[アクション]** 列で、削除する目標の行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 • 修復目標の表で、削除する修正目標の横にあるチェックボックスを選択します。 アクションバーで、Tenable Vulnerability Management は **[さらに表示]** > **[削除]** を有効にします。 • 修復目標の表で、削除する修正目標の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 b. **[削除]** をクリックします。
複数の修正目標	a. **修復目標** の表で、削除する 1 つ以上の修正目を選択します。 Tenable Vulnerability Management では、アクションバーの **[削除]** ボタンが有効になります。 b. **[削除]** をクリックします。

Tenable Vulnerability Management は、選択した修正目標を削除します。

ソリューション

Tenable は、企業のネットワーク上のすべての脆弱性に対する推奨ソリューションを提供しています。推奨ソリューションを VPR で並べ替えることで最も優先すべきソリューションを特定し、その詳細を掘り下げてネットワークの脆弱性に対処する手順を理解することができます。

注意: Tenable Lumin ライセンスがない場合は、ソリューションの詳細を表示することはできません。詳細は、Tenable Lumin にようこそ を参照してください。

ソリューションを表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable は、企業のネットワーク上のすべての脆弱性に対する推奨ソリューションを提供しています。推奨ソリューションを Vulnerability Priority Rating (VPR) で並べ替えることで最も優先すべきソリューションを特定し、その詳細を掘り下げてネットワークの脆弱性に対処する手順を理解することができます。

脆弱性インスタンスに対処することで、CES メトリクスおよび AESメトリクスを下げることができます。

ヒント: 脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。

新しいインターフェースでソリューションを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[脆弱性管理]** セクションで、**[ソリューション]** をクリックします。

   [ソリューション] ページが表示されます。

   注意: すべての Tenable Lumin データは、企業の Tenable Vulnerability Management インスタンス内のすべての資産を反映します。

   このページでは、次の操作を実行できます。

セクション	アクション
フィルター	表に表示されるデータをフィルタリングします。
[保存された検索条件] ドロップダウンボックス	• 既存の保存された検索条件を読み込む、または編集します。 • 新しく検索条件を保存します。
エクスポート	ソリューションを .csv ファイルとしてエクスポートします。

Solutions table	• 各ソリューションの情報を表示します。
	  • **Solution** - ソリューションの説明
	  • **影響を受ける資産** - ソリューションによって対処される脆弱性により影響を受けている資産の総数。
	  • **CVE Count** - そのソリューションに含まれる CVE
	  • **VPR** - ソリューションが対処する脆弱性の最大 VPR
	  • **CVSS** - ソリューションが対応している脆弱性の最大 CVSSv2 スコア(または使用可能な場合は CVSSv3 スコア)。
	• ソリューションの詳細を表示するには、ソリューションの行をクリックします。
	  [ソリューションの詳細] ページが表示されます。詳細は、ソリューションの詳細を参照してください。
	• 並べ替え、ページ当たりの行数の増減、または表の別のページへの移動を行うには、Tenable Vulnerability Management の表を参照してください。

ソリューションフィルター

必要な追加ライセンス: Tenable Lumin

[ソリューション] ページでは、Tenable が提供するフィルターと資産タグに基づくフィルターを使用して、脆弱性をフィルタリングできます。

Tenable が提供するフィルター

Tenable Vulnerability Management には、次のソリューションフィルターがあります。

フィルター	説明
ACR スコア	ソリューションに関連する資産の ACR。
ACR の深刻度	ソリューションに関連する資産の ACR 深刻度。
AES の深刻度	ソリューションに関連する資産の AES 深刻度。
資産数	ソリューションの影響を受けている資産の数。
資産 ID	ソリューションに関連する資産の UUID。この値は Tenable Vulnerability Management に対して一意です。
CVE カウント	ソリューションに関連する共通脆弱性識別子 (CVE) カウント。
CVSS	ソリューションに関連する脆弱性の共通脆弱性評価システム (CVSS) スコア。
CVSS の深刻度	ソリューションに関連する脆弱性の共通脆弱性評価システム (CVSS) の深刻度。
ファミリー	ソリューションに関連する資産のプラグインファミリー。
ホスト名	ソリューションに関連する資産のホスト名。 **注意:** 検索クエリの末尾に終止符が使われていないことを確認してください。
ライセンスの状態	ソリューションに関連する資産のライセンスの状態。

ソリューション	脆弱性を修正する方法に関する概要。
VPR	ソリューションに関連する脆弱性の Vulnerability Priority Rating (VPR)。
VPR の深刻度	ソリューションに関連する脆弱性の Vulnerability Priority Rating (VPR) の深刻度。

タグフィルター

Tenable Vulnerability Management では、タグにより資産に説明メタデータを追加することで、資産を事業の文脈別にグループに分けることができます。詳細は、タグを参照してください。

フィルターの **[カテゴリ]** ドロップダウンボックスでは、リストの下部の Tenable が提供するフィルターの後に、所属する企業のタグが表示されます。

ソリューションをエクスポートする

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

新しいインターフェースでは、エクスポート機能によりソリューションデータを .csv ファイル形式でエクスポートすることができます。

ソリューションを .csv ファイルとしてエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[脆弱性管理]** セクションで、**[ソリューション]** をクリックします。

   [ソリューション] ページが表示されます。

3. 右上にある [→ **[エクスポート]** をクリックします。

   [エクスポート] プレーンが表示されます。

4. エクスポート用に選択されたフォーマット、CSVを確認します。

5. エクスポートファイルに含める **[データ]** オプションの横にあるチェックボックスをクリックします。

データ	説明
ソリューション	ソリューションデータを含めます。
Details	ソリューションデータ、および Tenable が推奨するソリューションのデータにより影響を受けている資産のデータを含めます。

6. **[エクスポート]** をクリックします。

   Tenable Vulnerability Management がレポートの処理を開始します。エクスポートされたデータのサイズに応じて、Tenable Vulnerability Management によるレポートの処理に数分かかる場合があります。

処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

7. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。

ソリューションの詳細を表示する

必要な追加ライセンス: Tenable Lumin

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

このページを利用して、資産と脆弱性の情報などのソリューションの詳細を表示できます。

新しいインターフェースでソリューションの詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[脆弱性管理]** セクションで、**[ソリューション]** をクリックします。

   [ソリューション] ページが表示されます。

3. ソリューションの行をクリックします。

   [ソリューションの詳細] ページが表示されます。

   このページでは、次の操作を実行できます。

セクション	アクション
[概要] パネル	
Metrics summary	推奨ソリューションの統計情報の概要を表示します。 • **影響を受ける資産** - ソリューションによって対処される脆弱性により影響を受けている資産の総数。 • **CVE Count** - そのソリューションに含まれる CVE の総数 • **CVE Instances** - ソリューションた対応している脆弱性の総数 • **VPR** - ソリューションに含まれる脆弱性の最大 VPR。 • **CVSS V2/V3 Base Score** - ソリューションが対応している脆弱性の最大 CVSSv2 スコア(または使用可能な場合は CVSSv3 スコア)。

Vulnerabilities Included (#) 表	• ソリューションによって対処されるすべての脆弱性を表示します。
	  • **Identifier** - 脆弱性の識別子: CVE (使用可能な場合)、TVI、またはプラグイン ID
	  • **VPR** - 脆弱性の VPR
	  • **CVSS** - 脆弱性の CVSSv2 スコア (または使用可能な場合は CVSSv3 スコア)
	  • **影響を受ける資産** - 脆弱性によって影響を受けている資産の総数
	• 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。
	  脆弱性の詳細プレーンが表示されます。このプレーンでは、次の操作を実行できます。
	  • 脆弱性の概要を表示します。
	  • この脆弱性の VPRの計算に使用された主な要因 Tenable に関する情報を表示します。
	  • 過去 30 日間の VPRの調整状況を、静的な CVSSv2 スコア (または使用可能な場合は CVSSv3) と比較して示すグラフを表示します。
	  • TVI を含む、脆弱性に関する追加情報を表示します。
	• 表の別のページに移動するには、「 Tenable Vulnerability Management の表 」を参照してください。

[影響を受ける資産] タブ	
ACR タイル	影響を受けている資産の数を**低**、**中**、**高**、もしくは**重要**、または**未分類** ACRのカテゴリでまとめた、ACR 重要度タイルを表示します。

影響を受ける資産 表	• 資産情報を表示します。
	  • **Asset** -
	  特定の属性の存在に基づき次の論理順序で割り当てら

れる資産 ID です。

1. Nessus Agent 名
2. ホスト名
3. ウェブアプリのホスト名
4. コンテナセキュリティ画像名
5. コンテナランタイムのホスト名
6. クラウド共通リソース名
7. クラウド共通リソース識別子
8. クラウドランタイム名
9. クラウド IAC 名
10. Active Directory 資産名
11. ドメインレコードのホスト名

上記の属性がいずれも存在しない場合、**FQDN** が資産の名前として選択されます。

- **IP** - 資産の IP アドレス
- **ACR** - 資産の ACR。
- **CVE Count** - その資産上の CVE の総数
- **OS** - 資産のオペレーティングシステム
- **Detection Source** - 資産を最初にスキャンしたスキャナーの種類

- 資産の詳細を表示するには、資産の行をクリックします。

  [資産の詳細] ページが表示されます。詳細は、View Legacy Workbench Asset Details を参照してください。

- 表に表示される資産を絞り込むには、表のフィルタリングを参照し

	てください。 Tenable Vulnerability Management によって表が更新されます。 • 並べ替え、ページ当たりの行数の増減、または表の別のページへの移動を行うには、Tenable Vulnerability Management の表を参照してください。

Tenable Container Security ダッシュボード

重要: Tenable は、レガシー コンテナのセキュリティ のライフサイクル終 了を発 表しました。2024 年 9 月 30 日までは、引き続きアプリケーションにアクセスし、サポートを受 けることができます。Tenable は、すぐに コンテナのセキュリティ の現 行 バージョンに移 行 することを推 奨しています (新しい [クラウド セキュリティ] タイルから入 手 可 能)。詳 細については、ライフサイクル終 了 のお知らせをご覧ください。

[コンテナのセキュリティ] ダッシュボード は、Tenable Container Security のランディングページとして機 能します。このダッシュボード に含 まれるウィジェット には、コンテナ、イメージとイメージリポジトリ、ポリシーに関する大 まかな情 報 が表 示されます。ダッシュボード 上 のウィジェット をクリックすると、項 目 の種 類 に関する詳 細を表 示したり、データ項 目 (イメージなど) を Tenable Container Security にインポートしたりできます。

注 意 : Tenable Container Security による資 産 のリスク評 価 の方 法 に関しては、Tenable Container Security でのリスクメトリクスを参 照してください。

[コンテナのセキュリティ] ダッシュボード からは、以 下 を実 行 できます。

Tenable Container Security Scanner スキャンの概要

必要な追加ライセンス: Tenable Container Security

分析のためにコンテナに関するデータを収集するように Tenable Container Security スキャンを設定します。企業によっては、1 人ですべての手順を行うことも、複数人で手順をシェアして行うこともできます。

Tenable Container Security スキャンを設定する方法

1. コンテナイメージをインポートしてスキャンします。

    - 特定のイメージを Tenable Container Security にアップロードしてスキャンしたい場合は、外部のレジストリから対象のイメージをダウンロードして、Tenable Container Security にプッシュします。
    - レジストリからすべてのイメージを Tenable Container Security にインポートしてスキャンしたい場合は、イメージをレジストリからインポートするためのコネクタを設定します。

      注意: コネクタを使用してイメージをインポートしてスキャンすると、Tenable Container Security のダッシュボードにイメージが表示されるまでに最大で数時間かかる場合があります。

      インポートを開始してから 24 時間経ってもイメージがダッシュボードに表示されない場合は、Tenable サポート にお問い合わせください。
    - 自社のローカルレジストリまたはお使いのマシンからイメージを直接スキャンしたい場合は、Tenable Container Security Scanner をダウンロードして実行します。

    Tenable Container Security がレジストリ内のイメージをスキャンして結果を表示するのにかかる時間は、スキャンするイメージの大きさと数によって異なります。

    注意: イメージをインポートしたときに Tenable Container Security が保持するデータは、使用したインポート方法によって異なります。

    - Docker コマンドまたはコネクタ - Tenable Container Security はイメージ自体と、イメージに関連付けられているすべてのメタデータ (たとえばイメージレイヤー、イメージ上のソフトウェアパッケージなど) を保持します。
    - Container Security Scanner- Tenable Container Security はイメージに関連付けられているメタデータのみを保持します。

> イメージを削除すると、Tenable Container Security はイメージ全体とイメージのメタデータのすべてを削除します。

2. Tenable Container Security ダッシュボードに移動し、スキャンデータを表示して管理します。

注意: イメージを最初にインポートしてスキャンした後は、そのイメージは Tenable Container Security によって定期的にインポートされて再スキャンされるようになります。

Docker CLI を介して Tenable Container Security にログインする

必要な追加ライセンス: Tenable Container Security

Docker コマンドを使用して Tenable Container Security Scanner にログインし、Docker コマンドラインインターフェース (CLI) を介してイメージをプッシュできます。

インターフェースを操作して他の機能を使用するには、Tenable Vulnerability Management インターフェースを介してログインします。詳細は、Tenable Vulnerability Management にログインする を参照してください。

始める前に

- Tenable Vulnerability Management ユーザーアカウントの認証情報を取得します。

  注意: 管理者として Tenable Vulnerability Management インスタンスに初めてログインする場合には、Tenable がセットアップ中に初回認証情報を提供します。新しいパスワードは初回ログイン後に設定できます。初回セットアップの後に Tenable Vulnerability Management にログインする場合には、Tenable Vulnerability Management アカウントの登録に使用したメールアドレスがユーザー名になります。

- *一般要件ユーザーガイド*のシステム要件をレビューして、ご利用のコンピューターとブラウザが要件を満たしていることを確認します。

Docker コマンドを介して Tenable Container Security にログインする方法

1. API アクセスキーと秘密鍵を生成します。
2. Docker CLI で、次のコマンドを実行します。

   ```
   docker login registry.cloud.tenable.com
   ```

   CLI により、ユーザー名の入力を求めるメッセージが表示されます
   。
3. API アクセスキーを入力します。
4. **Enter** を押します。

   CLI により、パスワードの入力を求めるメッセージが表示されます。
5. API 秘密鍵を入力します。

6. **Enter** を押します。

   Docker CLI により、Tenable Container Security レジストリにログインできます。

Tenable Container Security へのコンテナイメージのプッシュ

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Docker コマンドを使用して外部レジストリに存在しているイメージをダウンロードし、Tenable Container Security にインポートします。

Tenable Container Security がレジストリ内のイメージをスキャンして結果を表示するのにかかる時間は、スキャンするイメージの大きさと数によって異なります。

始める前に

- Docker コマンドを介して Tenable Vulnerability Management Container Security にログインします。

コンテナイメージを Tenable Container Security にプッシュする方法

1. CLI で次のコマンドを実行して、外部レジストリからイメージをダウンロードします。

   ```
   docker pull alpine:latest
   ```

2. CLI で次のコマンドを実行して、`registry.cloud.tenable.com` タグを追加します。

   ```
   docker tag alpine:latest registry.cloud.tenable.com/alpine:latest
   ```

   注意: `registry.cloud.tenable.com` タグは、Docker に対してイメージを Tenable Container Security にプッシュするように指示します。`registry.cloud.tenable.com` タグを追加しないと、Docker は自動的にイメージを Docker 中央リポジトリにプッシュします。

3. CLI で次のコマンドを実行して、タグが追加されたイメージを Tenable Container Security にプッシュします。

   ```
   docker push registry.cloud.tenable.com/alpine:latest
   ```

Docker により、イメージが Tenable Container Security にプッシュされます。Tenable Container Security はイメージの脆弱性をスキャンします。

> **注意:** コンテナイメージをインポートしてスキャンして、そのスキャンの実行時間が 60 分に達した場合、Tenable Container Security はスキャンを中止する場合があります。この状況が発生すると、**[イメージ]** ページの **[脆弱性]** と **[マルウェア]** 列の中止されたイメージに *[スキャン失敗]* が表示されます。
>
> Tenable Container Security によってスキャンが中止された場合は、*Docker* のドキュメントの説明に従って、イメージをインポートする前にイメージを簡略化してみてください。別な方法として、Tenable Container Security Scanner を使用すると、イメージを Tenable Container Security にインポートせずにスキャンできます。
>
> Tenable Container Security がスキャンを中止し続ける場合は、Tenable サポート にお問い合わせください。

次の手順

- コンテナイメージのスキャン結果を表示するの説明に従って、スキャン結果を表示します。

Bamboo から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Bamboo から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Bamboo の利用に習熟していて、現在も Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Bamboo を使用しているものの、Docker コンテナイメージをまだビルドした経験がない場合は、Bamboo のドキュメント「Configuring the Docker task in Bamboo」(Bamboo での Docker タスクの設定)を参照し、習熟してください。

手順

1. 関連するジョブ向けの新しい Docker タスクを作成します。
2. **[タスク]** ボックスで、タスクの説明を入力します。
3. タスクを実行するかどうかに応じて、**[タスクの無効化]** チェックボックスを選択または解除します。
4. **[Docker イメージを Docker レジストリコマンドにプッシュ]** を選択し、設定を完了させます。

   Tenable Vulnerability Management は Bamboo のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

CircleCI から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、CircleCI から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは CircleCI の利用に習熟していて、現在も Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。CircleCI を使用しているものの、Docker コンテナイメージをまだビルドした経験がない場合は、CircleCI のドキュメント「Continuous Integration and Delivery with Docker」(Docker を使用した継続的インテグレーションと継続的デリバリ) を参照し、習熟してください。

`circle.yml` ファイルに関する情報は、こちらをクリックしてください。

CircleCI を使用して Docker コンテナイメージをビルドしている場合、プロジェクトのソースコントロールリポジトリに以下の例のような内容の `circle.yml` ファイルを含める必要があります。

```
machine:
services:
- docker

dependencies:
override:
- docker info
- docker build -t circleci/elasticsearch .

test:
override:
- docker run -d -p 9200:9200 circleci/elasticsearch; sleep 10
- curl --retry 10 --retry-delay 5 -v http://localhost:9200

deployment:
hub:
branch: master
commands:
- docker push circleci/elasticsearch
```

circle.yml 内の以下の行は、CircleCI に対してビルドプロセスに Docker を使用するように指示しています。

```
machine:
services:
- docker
```

circle.yml 内の以下の行は、CircleCI に対して elasticsearch イメージを circleci/ リポジトリ内にビルドするように指示しています。

```
dependencies:
override:
- docker info
- docker build -t circleci/elasticsearch .
```

以下の行は、CircleCI 環境に Tenable Container Security 統合を追加する、最も重要な行です。これらの行は CircleCI に対して、Docker を使用してレジストリ(今回のケースではプライベートレジストリが指定されていないため Docker Hub) にログインし、cicleci/elasticsearch をレジストリにプッシュするように指示しています。

```
deployment:
hub:
branch: master
commands:
- docker login -u $DOCKER_USER -p $DOCKER_PASS
- docker push circleci/elasticsearch
```

手順

1. CircleCI コンソールでプロジェクトに環境変数を追加するには、プロジェクトを開き、**[プロジェクトの設定]** をクリックした後に **[環境変数]** をクリックします。
2. 以下の変数を定義します。

変数	説明
TENABLE_IO_	Tenable Container Security へのログインに使用するメールアドレ

変数	説明
CONTAINER_SECURITY_EMAIL	スです。
TENABLE_IO_CONTAINER_SECURITY_USER	Tenable Container Security へのログインに使用するユーザー名。Tenable Container Security の **[設定]** ページに表示されています。
TENABLE_IO_CONTAINER_SECURITY_ENDPOINT	Tenable Container Security のホストされたクラウドのユーザの場合、この値は `registry.cloud.tenable.com` です。

3. Tenable Container Security のサポートを追加するために、`circle.yml` ファイルを以下のように更新します。

```
machine:
environment:
VERSION: 2.1.1
TAG: ${VERSION}
services:
- docker

dependencies:
override:
- docker info
- docker version
- docker build -t $TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch .

test:
override:
- docker run -d -p 9200:9200 $TENABLE_IO_CONTAINER_SECURITY_
ENDPOINT/circleci/elasticsearch; sleep 10
- curl --retry 10 --retry-delay 5 -v registry.cloud.tenable.com

deployment:
hub:
branch: master
commands:
```

```
- docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY
- docker tag $TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch
$TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch:${TAG}
- docker push $TENABLE_IO_CONTAINER_SECURITY_
ENDPOINT/circleci/elasticsearch:${TAG}
- docker logout
```

Tenable Vulnerability Management は CircleCI のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Codeship から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Codeship から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Codeship の利用に習熟していて、現在 Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Codeship を使用しているものの、Docker コンテナイメージをまだビルドした経験がない場合は、Codeship のドキュメント「Pushing to a remote registry」(リモートレジストリへのプッシュ) を参照し、習熟してください。

手順

1. **codeship-services.yml** ファイルを編集して、Tenable Container Security で指定されているリポジトリ名とイメージ名を使用するようにします。

   ```
   app:
   build:
   image: repository_name/image_name
   dockerfile_path: Dockerfile
   ```

   注意: 今回初めてリポジトリにイメージをプッシュする場合、事前設定されたイメージ名はありません。イメージ名は、Codeship からプッシュされた後に自動的に追加されます。

2. **codeship-steps.yml** ファイルのサービスのセクションを編集して、以下の例のようにします。

   ```
   service:
   app type: push
   image_name: repository_name/image_name
   registry: registry.cloud.tenable.com
   encrypted_dockercfg_path: dockercfg.encrypted
   ```

   Tenable Vulnerability Management は Codeship のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Distelli から Tenable Container Security へのプッシュ

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Distelli から Tenable Container Security に Distelli WebUI Manifest を使用して Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Distelli の利用に習熟していて、現在も Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Distelli を使用しているものの、Docker コンテナイメージをまだビルドした経験がない場合は、Distelli Manifest に関する Distelli のドキュメントを参照し、習熟してください。Distelli マニフェストファイルは、Distelli WebUI Manifest を使用するか、**distelli-manifest.yml** ファイルを直接編集するかのいずれかの方法で使用できます。

手順

1. Distelli にログインし、アプリケーションに移動します。
2. **[マニフェスト]** タブをクリックします。

   [ビルド] セクションに、以下の例に似た内容が表示されます。

   ```
   docker build --quiet=false -t $DOCKER_REPO:$DISTELLI_BUILDNUM .
   docker login -u $DOCKER_USERNAME -p $DOCKER_PW
   docker push $DOCKER_REPO:$DISTELLI_BUILDNUM
   ```

3. Tenable Container Security のサポートを追加するには、**[ビルド]** セクションを以下の例のように変更します。

   ```
   bash docker build --quiet=false -t $TENABLE_IO_CONTAINER_SECURITY_REPO:$DISTELLI_
   BUILDNUM . docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY
   registry.cloud.tenable.com docker push $TENABLE_IO_CONTAINER_SECURITY_
   REPO:$DISTELLI_BUILDNUM
   ```

   この変更により、Tenable Container Security URI が docker login に追加されます。

Tenable Vulnerability Management は Distelli のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Drone.io から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Drone.io から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Drone.io の利用に習熟していて、既に Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Drone.io に関する詳細については、Drone.io のドキュメントを参照してください。

Docker コンテナイメージのビルドに Drone.io を使用している場合、以下のようなビルドスクリプト (通常は **build.sh** ファイル) を既にお持ちのはずです。

```
$ docker build -t docker-registry/image-name .
$ docker push docker-registry/image-name
```

手順

1. **build.sh** ファイルを開きます。
2. 以下の例のように、スクリプト内の docker push 指示の前に docker login 指示を追加します。

   ```
   $ docker build -t docker-registry/image-name .
   $ docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY
   registry.cloud.tenable.com
   $ docker push docker-registry/image-name
   ```

   Tenable Vulnerability Management はこのプロジェクト用の Drone.io のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンが行います。

Jenkins から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Jenkins から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Jenkins の利用に習熟していて、現在も Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Jenkins を使用しているものの、Docker コンテナイメージをまだビルドした経験がない場合は、Jenkins の CloudBees Docker Build and Publish プラグインに関するドキュメントを参照し、習熟してください。

CloudBees Docker Build and Publish プラグインをインストールする手順については、こちらをクリックしてください。

1. Jenkins にログインします。
2. **[Jenkins の管理]** をクリックし、次に **[プラグインの管理]** をクリックします。
3. **[インストール済み]** をクリックします。

   インストールされているプラグインのリストが表示されます。
4. **[使用可能]** をクリックします。
5. **[フィルター]** ボックスに、「**CloudBees Docker Build and Publish plugin**」と入力します。
6. 該当するプラグインのチェックボックスを選択します。
7. プラグインをインストールします。

   CloudBees Docker Build and Publish プラグインがインストールされ、Jenkins ジョブで使用する準備ができました。

手順

1. Jenkins のダッシュボードで、変更するジョブを選択します。
2. **[設定]** をクリックします。

3. **[ビルド]** セクションで、**[ビルド手順を追加]** をクリックします。
4. ドロップダウンボックスで、**[Docker ビルドと公開]** を選択します。
5. 以下の設定パラメーターについて、詳細情報を入力します。
    - **Repository Name**: リポジトリ名とイメージ名です。たとえば、rabbitmq のコンテナイメージをビルドする場合、リポジトリに rabbitmq、イメージに rabbitmq という名前を付けることができます。この例では、**[リポジトリ名]** ボックスに「*rabbitmq/rabbitmq*」と入力します。
    - **Tag**: タグ名です。最も簡単に使用できるタグ名は *latest* です。
    - **Docker Host URI**: Docker Host への Jenkins のパスです。Docker Host がローカルホストで実行されている場合は、**[Docker ホスト URI]** ボックスに「*tcp://127.0.0.1:4243*」と入力します。
    - **[Docker レジストリ URL]**: Tenable Container Security API のエンドポイントです。今回の例では *registry.cloud.tenable.com* です。
    - **[レジストリの認証情報]**: ボックスから選択する、レジストリの認証情報です。

      ### レジストリの認証情報を追加する

      1. **[追加]** をクリックします。
      2. **[ユーザー名とパスワード]** をクリックします。
      3. **[ユーザー名]** ボックスで、Tenable Container Security のユーザー名を入力します。
      4. **[パスワード]** ボックスに Tenable Container Security のパスワードを入力します。
      5. **[追加]** をクリックします。

         認証情報が追加されます。
6. **[保存]** をクリックします。

   Tenable Vulnerability Management は Jenkins のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Shippable から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Shippable から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Shippable の利用に慣れていて、すでに Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Shippable を使用しているものの、Docker コンテナイメージをまだビルドしたことがない場合は、Shippable のドキュメントを参照し、習熟してください。

手順

1. Shippable にログインします。
2. 画面の右上にある **[アカウント設定]** ボタンをクリックします。
3. **[統合]** をクリックし、次に **[統合を追加]** をクリックします。
4. **[マスター統合]** セクションで、**[プライベート Docker レジストリ]** をクリックします。
5. **[名前]** ボックスに「**Tenable Container Security**」と入力します。
6. **[URL]** ボックスに「**registry.cloud.tenable.com**」と入力します。
7. **[ユーザー名]** ボックスで、Tenable Container Security のユーザー名を入力します。
8. **[パスワード]** ボックスに Tenable Container Security のパスワードを入力します。
9. **[E メール]** ボックスに、Tenable Container Security アカウントと関連付けられたメールアドレスを入力します。
10. **[保存]** をクリックします。

    これで、Shippable でビルドされたコンテナイメージをお使いの Tenable Container Security アカウントでホストする準備ができました。
11. プロジェクトページにアクセスして、**[設定]** をクリックします。

12. **[ハブ]** をクリックして、作成した Tenable Container Security 統合を選択します。
13. **[ビルドをプッシュ]** フィールドで **[はい]** をクリックします。
14. **[イメージのプッシュ先]** ボックスに、Tenable Container Security でのリポジトリとイメージの名前を入力します (例 : `testrepo/nodejs`)。
15. **[プッシュイメージタグ]** ボックスで、**default**、**commitsha**、**latest** の中から選択します。
16. **[保存]** をクリックします。

    Tenable Vulnerability Management は Shippable のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Solano Labs から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Solano Labs から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Solano Labs の利用に習熟していて、現在も Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Solano Labs を使用しているものの、Docker コンテナイメージをまだビルドした経験がない場合は、Solano Labs のドキュメントを参照し、習熟してください。

注意: Solano Labs での Docker コンテナイメージのビルドのサポートは、プライベートベータ状態です。Solano Labs では参加したい顧客に対し、Solano Labs サポートまで連絡するよう推奨しています。

手順

1. **solano.yml** ファイルを開きます。以下の例に似た内容のはずです。

```
# Use docker-enabled workers (currently private beta - contact
support@solanolabs.com)
system:
docker: true
python:
python_version: 2.7
hooks:
pre_setup: |
set -ex
sudo apt-get update -qq
sudo docker pull jenkins
sudo docker build -t myrepo/jenkins-dsl-ready:my .
tests:
- python -m doctest build/resolve_jenkins_plugins_dependencies.py
```

2. Tenable Container Security のユーザー名を使用して post_build フェーズを追加します。

```
# Use docker-enabled workers (currently private beta - contact
support@solanolabs.com)
system:
docker: true
python:
python_version: 2.7
hooks:
pre_setup: |
set -ex
sudo apt-get update -qq
sudo docker pull jenkins
sudo docker build -t myrepo/jenkins-dsl-ready .
post_build: |
docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY
registry.cloud.tenable.com
docker push myrepo/jenkins-dsl-ready
tests:
- python -m doctest build/resolve_jenkins_plugins_dependencies.py
```

Tenable Vulnerability Management は Solano Labs のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Travis CI から Tenable Container Security にプッシュする

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Travis CI から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Travis CI の利用に習熟していて、現在も Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Travis CI を使用しているものの、Docker コンテナイメージをまだビルドした経験がない場合は、Travis CI のドキュメント「Using Docker in Builds」(ビルドで Docker を使用する) を参照し、習熟してください。

`travis.yml` ファイルに関する情報は、こちらをクリックしてください。

Travis CI を使用して Docker コンテナイメージをビルドしている場合、プロジェクトのソースコントロールリポジトリに以下のような内容の **`travis.yml`** ファイルを含める必要があります。

```
sudo: required
language: ruby
services:
  - docker
before_install:
  - docker build -t carlad/sinatra .
  - docker run -d -p 127.0.0.1:80:4567 carlad/sinatra /bin/sh -c "cd /root/sinatra; bundle exec
foreman start;"
  - docker ps -a
  - docker run carlad/sinatra /bin/sh -c "cd /root/sinatra; bundle exec rake test"
script:
  - bundle exec rake test
```

`travis.yml` 内の以下の行は、Travis CI に対してビルドプロセスに Docker を使用するように指示しています。

```
sudo: required
services:
  - docker
```

`travis.yml` 内の以下の行は、Travis CI に対して `carlad/` リポジトリ内に sinatra イメージをビルドするように指示しています。

```
before_install:
  - docker build -t carlad/sinatra .
```

手順

1. **travis.yml** ファイルを開きます。
2. Tenable Container Security の認証情報を追加します。

   ```
   $ travis encrypt TENABLE_IO_CONTAINER_SECURITY_EMAIL=email@organization.com
   $ travis encrypt TENABLE_IO_CONTAINER_SECURITY_USER=username
   $ travis encrypt TENABLE_IO_CONTAINER_SECURITY_PASSWORD=password
   ```

3. 環境変数を追加します。

   ```
   env:
     global:
     - secure: "UkF2CHX0lUZ...VI/LE=" # TENABLE_IO_CONTAINER_SECURITY_EMAIL
     - secure: "Z3fdBNPt5hR...VI/LE=" # TENABLE_IO_CONTAINER_SECURITY_USER
     - secure: "F4XbD6WybHC...VI/LE=" # TENABLE_IO_CONTAINER_SECURITY_PASSWORD
     - COMMIT=${TRAVIS_COMMIT::8}
   ```

4. 接続情報を追加します。

   ```
   after_success:
     - docker login -u $TENABLE_IO_CONTAINER_SECURITY_EMAIL -p $TENABLE_IO_CONTAINER_SECURITY_
   PASSWORD registry.cloud.tenable.com
     - export REPO=web-login-site/web-login-site
     - export TAG=`if [ "$TRAVIS_BRANCH" == "master" ]; then echo "latest"; else echo $TRAVIS_
   BRANCH; fi`
     - docker build -f Dockerfile -t $REPO:$COMMIT .
     - docker tag $REPO:$COMMIT registry.cloud.tenable.com/$REPO:$TAG
     - docker tag $REPO:$COMMIT registry.cloud.tenable.com/$REPO:travis-$TRAVIS_BUILD_NUMBER
     - docker push registry.cloud.tenable.com/$REPO:travis-$TRAVIS_BUILD_NUMBER
     - docker push registry.cloud.tenable.com/$REPO:$TAG
   ```

   Tenable Vulnerability Management は Travis CI のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Wercker から Tenable Container Security へのプッシュ

必要な追加ライセンス: Tenable Container Security

始める前に

以下では、Wercker から Tenable Container Security に Docker イメージをプッシュする方法について説明しています。

以下の手順では、ユーザーは Wercker の利用に慣れていて、既に Docker イメージをパブリックまたはプライベートレジストリにプッシュしていることを前提としています。Wercker を使用しているものの、Docker コンテナイメージをまだビルドしたことがない場合は、Wercker のドキュメントを参照して習熟してください。

手順

1. プロジェクトのソースコントロールリポジトリで、**wercker.yml** ファイルを開きます。
2. deploy 指示を以下のように変更して、Tenable Container Security のサポートを追加します。

```
deploy:
steps:
- internal/docker-push:
username: $USERNAME
password: $PASSWORD
tag: my-amazing-tag
repository: turing/bar
registry: registry.cloud.tenable.com
```

Tenable Vulnerability Management は Wercker のビルドを Tenable Container Security に送信し、保管、配信、脆弱性スキャン、不正なコードのスキャンを行います。

Tenable Container Security Scanner を Kubernetes で使用する

Kubernetes を使用して Tenable Container Security Scanner を実行すると、コンテナイメージを自社ネットワークの外に送信することなく、安全にスキャンできます。詳細は、Tenable Container Security Scanner を参照してください。

- Kubernetes 向け Tenable Container Security Scanner のシステム要件
- Tenable Container Security Scanner を設定して実行するための Kubernetes オブジェクトを準備する
- Kubernetes で Tenable Container Security Scanner を設定して実行する

Kubernetes 向け Tenable Container Security Scanner のシステム要件

Kubernetes を使用して Tenable Container Security Scanner を実行するマシンは、次の要件を満たす必要があります。

ソフトウェアおよびハードウェア要件

Software Requirements	RAM	Temporary Storage	CPU
Linux コンテナが実行可能	2 GiB	15 GB	1.5 GHz

インターネット

Container Security Scanner を実行するマシンは、スキャナーをダウンロードして実行する際にインターネットにアクセスできる必要があります。

SSL 証明書の要件

イメージをホストしているレジストリに HTTPS プロトコルが必要な場合、信頼できる認証局 (CA) によって署名された SSL 証明書をレジストリにインストールする必要があります。お使いのレジストリでの SSL 証明書のインストールに関するドキュメントを参照してください。

注意: Mozilla の CA 証明書ストアは、Tenable Container Security Scanner の信頼できる認証局です。

注意: 信頼できる CA によって署名された証明書であることを検証せずに Container Security Scanner でレジストリをスキャンしたい場合は、スキャナーの実行時に `ALLOW_INSECURE_SSL_REGISTRY` 変数を含める必要があります。詳細は、環境変数 を参照してください。

Tenable Container Security Scanner を設定して実行するための Kubernetes オブジェクトを準備する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Kubernetes で Container Security Scanner を設定して実行できるようにするためには、Kubernetes 名前空間とシークレットオブジェクトを準備する必要があります。Container Security Scanner は Kubernetes 内のイメージをスキャンするときに、これらのオブジェクトを参照します。

シークレットは、環境変数で説明されている TENABLE_ACCESS_KEY、TENABLE_SECRET_KEY、REGISTRY_USERNAME、REGISTRY_PASSWORD 環境変数に関連する機密情報を含みます。Kubernetes で Container Security Scanner を実行するには、これらのシークレットを設定して、スキャンするイメージが保管されているレジストリにシークレットをデプロイする必要があります。

Kubernetes でオブジェクトを作成する方法に関する詳細については、kubernetes.io にある Kubernetes ドキュメントを参照してください。

始める前に

- CS Scanner をダウンロードするの説明に従って、Container Security Scanner をダウンロードします。

Container Security Scanner を設定して実行するための Google Kubernetes Engine (GKE) を準備する方法

1. Container Security Scanner を設定して実行するマシンの CLI にログインします。
2. テキストエディターで、CS Scanner 用の名前空間ファイル (`tiocsscanner-namespace.yaml`) を作成します (次の `tiocsscanner-namespace.yaml` ファイルを参照)。

tiocsscanner-namespace.yaml

```
apiVersion: v1
kind: Namespace
metadata:
```

```
  name: tiocsscanner
  labels:
    name: tiocsscanner
```

3. ファイルを保存して閉じます。

4. CLI で次のコマンドを実行して、`tiocsscanner-namespace.yaml` ファイルを GKE にデプロイします。

```
kubectl apply -f tiocsscanner-namespace.yaml
```

   Tenable Vulnerability Management は、名前空間を設定およびデプロイします。

   注意: 上記のコマンドは、ファイルが現在の作業ディレクトリに保存されている場合にのみ動作します。ファイルが作業ディレクトリ以外に保存されている場合は、コマンドにディレクトリのフルパスを含めます。例

   `kubectl apply -f /home/jsmith/images/tiocsscanner-namespace.yaml`

5. Tenable Vulnerability Management アクセスキーおよび秘密鍵のシークレットを設定します。例

```
kubectl create secret generic tio \
--from-literal=username=<Your Tenable Vulnerabiltiy Management access key> \
--from-literal=password=<Your Tenable Vulnerability Management secret key> \
--namespace=tiocsscanner
```

6. スキャナーがプルするイメージ用の、Google Container Registry (GCR) レジストリのユーザー名とパスワード (GCP GCR を準備するの手順 3 と 4 で取得) のシークレットを設定します。例

```
kubectl create secret generic gcr-registry \
--from-literal=username=<Your gcr registry username> \
--from-literal=password=<Your gcr registry password> \
--namespace=tiocsscanner
```

7. スキャン対象のイメージが保管されているレジストリにシークレットをデプロイします。例

   Tenable Container Security スキャナーイメージが保管されているレジストリのシークレットを設定します。例

```
kubectl create secret docker-registry jfrog-tio \
--docker-server=https://tenableio-docker-consec-local.jfrog.io \
--docker-username=<tenable jfrog userrname obtained from the Tenable Container Security
console> \
--docker-password=<tenable jfrog password obtained from the Tenable Container Security console>
\
--docker-email=<Your email address> \
--namespace=tiocsscanner
```

シークレットがレジストリにデプロイされました。

次の手順

- Kubernetes で CS Scanner を設定して実行するの説明に従って、Kubernetes で Container Security Scanner を設定して実行します。

Kubernetes で Tenable Container Security Scanner を設定して実行する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Kubernetes で Container Security Scanner を使用してイメージをスキャンするには、Kubernetes デプロイメントファイルを作成し、CLI を介してスキャンを実行するマシンにファイルを展開する必要があります。

始める前に

- お使いのマシンが、Tenable Container Security Scanner システム要件に記載されているシステム要件を満たしていることを確認します。
- Tenable Container Security Scanner をダウンロードするの説明に従って Container Security Scanner をダウンロードします。
- Tenable Container Security Scanner を設定して実行するための Kubernetes オブジェクトを準備するの説明に従って、Kubernetes で Container Security Scanner を設定して実行する準備をします。

Container Security Scanner を Google Kubernetes Engine (GKE) に展開する方法

1. テキストエディターで新規ファイルを開きます。
2. ファイルを `tiocsscanner-deployment.yaml` として保存します。
3. `tiocsscanner-deployment.yaml` ファイルに以下のテキストをコピー & ペーストして、該当箇所に特定の変数を入力します。以下の変数に関する詳細は、「環境変数」を参照してください。

   注意: 下記の `tiocsscanner-deployment.yaml` サンプルファイルは、Google Cloud Registry (GCR) と Google Kubernetes Engine (GKE) の組み合わせで通常動作します。お使いの Kubernetes のバージョンに応じて、`apiVersion` の値の変更が必要になる場合があります。

tiocsscanner-deployment.yaml

```
apiVersion: v1
kind: Service
metadata:
  name: tiocsscanner
  namespace: tiocsscanner
  labels:
    app: tiocsscanner
spec:
  selector:
    app: tiocsscanner
  type: ClusterIP
  ports:
  - name: http
    protocol: TCP
    port: 5000
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  labels:
    app: tiocsscanner
  name: tiocsscanner
  namespace: tiocsscanner
spec:
  minReadySeconds: 10
  replicas: 1
  selector:
    matchLabels:
      app: tiocsscanner
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 1
    type: RollingUpdate
  template:
    metadata:
      labels:
        app: tiocsscanner
    spec:
      imagePullSecrets:
        - name: jfrog-tio
      containers:
        - image: "tenableio-docker-consec-local.jfrog.io/cs-scanner:latest"
          name: tiocsscanner
          resources:
            limits:
              cpu: "3"
            requests:
              cpu: "1.5"
              memory: "2Gi"
          args:
           - import-registry
          env:
            - name: TENABLE_ACCESS_KEY
```

```
            valueFrom:
              secretKeyRef:
                name: tio
                key: username
          - name: TENABLE_SECRET_KEY
            valueFrom:
              secretKeyRef:
                name: tio
                key: password
          - name: REGISTRY_USERNAME
            valueFrom:
              secretKeyRef:
                name: gcr-registry
                key: username
          - name: REGISTRY_PASSWORD
            valueFrom:
              secretKeyRef:
                name: gcr-registry
                key: password
          - name: IMPORT_REPO_NAME
            value: "<variable>"
          - name: REGISTRY_URI
            value: "https://[gcr-domain]/[project]"
          - name: IMPORT_INTERVAL_MINUTES
            value: "<variable>"
```

注意: GCP でのプロジェクト名が myapigw で、レジストリが gcr.io ドメインにある場合、REGISTRY_URI の値は「https://gcr.io/myapigw」となります。

4. ファイルを保存して閉じます。
5. スキャンを実行するマシンのコマンドラインインターフェースで、次のコマンドを実行してファイルをデプロイします。

```
kubectl apply -f tiocsscanner-deployment.yaml
```

注意: 上記のコマンドは、ファイルが現在の作業ディレクトリに保存されている場合にのみ動作します。ファイルが作業ディレクトリ以外に保存されている場合は、コマンドにディレクトリのフルパスを含めます。例

/home/jsmith/images/tiocsscanner-namespace.yaml

6. **Enter** を押します。

   Kubernetes 上で Container Security Scanner が実行されます。

7. コマンドラインインターフェースで次のコマンドを実行し、スキャンが正しく実行されることを確認します。

```
kubectl get pods --namespace=tiocsscanner
```

スキャンステータスのログが表示されます。

> **注意:** スキャンデータ内でエラーメッセージが表示された場合は、エラーメッセージに従って問題を修正します。

次の手順

- コンテナイメージのスキャン結果を表示するの説明に従って、スキャンの結果を表示します。

Tenable Container Security Scanner

Tenable Container Security Scanner (Container Security Scanner) により、コンテナイメージを自社ネットワークの外に送信することなく、安全にスキャンできます。Container Security Scanner はスキャンするイメージの最初のインベントリ(別名スナップショット)を受け取り、そのインベントリを分析のために Tenable Vulnerability Management に送信します。その後、イメージのスキャンデータを、通常通り Tenable Vulnerability Management にインポートされたイメージのデータと並べて表示できます。Container Security Scanner では、以下をスキャンできます。

- レジストリからエクスポートされ、スキャナーをインストールしたマシン上にローカルに保存された特定のイメージ。
- 特定のレジストリ(たとえば Docker レジストリ)でホストされたすべてのイメージ。

システム要件を満たしていれば、どのマシン上でも Container Security Scanner を設定して実行できます。

まず、お使いのマシンに Container Security Scanner をダウンロードします。次に、Container Security Scanner を設定して実行します。スキャンが完了したら、Tenable Container Security ダッシュボードでスキャン結果を表示できます。

Tenable Container Security Scanner システム要件

Tenable Container Security Scanner を実行するマシンでは次の要件を満たす必要があります。

ソフトウェアおよびハードウェア要件

Deployment Type	Software Requirements	RAM	Temporary Storage	CPU
Local	Linux コンテナが実行可能	2 GB	15 GB	64-bit multi-core, x86 compatible

インターネット

Container Security Scanner を実行するマシンは、スキャナーをダウンロードして実行する際にインターネットにアクセスできる必要があります。マシンでは、*cloud.tenable.com* サーバーとの通信用に送信 HTTPS トラフィックを許可する必要があります。

SSL 証明書の要件

イメージをホストしているレジストリに HTTPS プロトコルが必要な場合、信頼できる認証局 (CA) によって署名された SSL 証明書をレジストリにインストールする必要があります。お使いのレジストリでの SSL 証明書のインストールに関するドキュメントを参照してください。

注意: Mozilla の CA 証明書ストアは、Tenable Container Security Scanner の信頼できる認証局です。

注意: 信頼できる CA によって署名された証明書であることを検証せずに Container Security Scanner でレジストリをスキャンしたい場合は、スキャナーの実行時に `ALLOW_INSECURE_SSL_REGISTRY` 変数を含める必要があります。詳細は、環境変数 を参照してください。

サポートされているコンテナイメージの形式

Container Security Scanner では、次のイメージ形式をサポートしています。

- Docker イメージ
- Open Containers Initiative (OCI) イメージ

Tenable Container Security Scanner をダウンロードする

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Container Security Scanner を設定して実行するマシンに Container Security Scanner Docker イメージをダウンロードします。

始める前に

- お使いのマシンが、CS スキャナーのシステム要件に記載されているシステム要件を満たしていることを確認します。

CS スキャナーをダウンロードする方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[コネクタ]** セクションで、**[作成]** をクリックします。

   [コネクタの選択] プレーンが表示されます。

2. **[コンテナのセキュリティ]** の下にある **[CS スキャナー]** をクリックします。

   [CS スキャナー] プレーンがログイン認証情報とともに表示されます。

3. 後ほどダウンロードの際に使用するために、認証情報をコピーするか、スクリーンショットを撮ります。

4. Container Security Scanner をダウンロードするマシンのコマンドラインインターフェース (CLI) で、次のコマンドを実行します。

   ```
   docker login tenableio-docker-consec-local.jfrog.io
   ```

5. **Enter** を押します。

   CLI により、ユーザー名とパスワードの入力を求めるメッセージが表示されます。

6. **[CS スキャナー]** プレーンに表示された認証情報を使用して、フィールドを更新します。

7. **Enter** を押します。

   Tenable Vulnerability Management は Container Security Scanner にログインします。

8. 次のコマンドを入力して、最新バージョンの Container Security Scanner イメージをプルします。

```
docker pull tenableio-docker-consec-local.jfrog.io/cs-scanner:latest
```

9. **Enter** を押します。

次の手順

- Tenable Container Security Scanner を設定して実行するの説明に従って、Container Security Scanner を設定して実行します。

Tenable Container Security Scanner 環境変数

環境変数を設定して Container Security Scanner を実行するためには、お使いのコンピューター上で CLI を使用する必要があります。

レジストリとレジストリソースの任意の組み合わせを使用して、Container Security Scanner を必要な回数だけ設定して実行できます。

環境変数

変数	説明	タイプ	必須	サポートされたモード
TENABLE_ACCESS_KEY	Tenable Vulnerability Management API のアクセスキーです。	文字列	○	Image Inspect または Registry Import
TENABLE_SECRET_KEY	Tenable Vulnerability Management API の秘密鍵です。	文字列	○	Image Inspect または Registry Import
IMPORT_REPO_NAME	イメージをインポートする Container Security Scanner リポジトリの名前です。この名前にはスペースを含めることができません。 リポジトリ名は以下の要件を満たす必要があります。 • 64 文字以下であること • 英数字、ダッシュ(-)、アンダースコア	文字列	○	Image Inspect または Registry Import

	(_)、または終止符 (.) のみを含むこと • 英数字で始まること • 英大文字を含まないこと			
REGISTRY_URI	イメージのインポート元となるレジストリの URI です。	文字列	×	Registry Import
REGISTRY_USERNAME	スキャンするレジストリを認証するためのユーザー名です。 レジストリの認証が必要な場合に、この変数を設定してください。 ユーザー名の変数は、スキャンするレジストリに応じて異なります。 • Amazon Web Services (AWS) Elastic Container Registry (ECR) - ユーザー名として AWS アクセスキー ID を入力します。アクセスキー ID を取得する方法については、*AWS のドキュメント*を参照してください。 • Azure レジストリ - レジストリのサービスプリンシパル ID を入力します。サービスプリンシパルを作成する方法の詳細については、*Azure のドキュメント*を参照してください。 • Google Cloud Platform (GCP) Google Container Registry (GCR) - サービスアカウントプライベートキー JSON ファイルの `client_email` フィールドに表示される、GCR アカウントのクライアントメールアドレスを入力します。サービスアカウントプライベートキーを作成してダウン	文字列	×	Registry Import

	ロードする方法については、*Google Container Registry のドキュメント*を参照してください。 • 他のすべてのレジストリ - レジストリの認証に使用するユーザー名を入力します。			
REGISTRY_PASSWORD	イメージのインポート元となるレジストリの認証用パスワード レジストリの認証が必要な場合に、この変数を設定してください。 パスワードは、スキャンするレジストリに応じて異なります。 • Amazon Web Services (AWS) Elastic Container Registry (ECR) - パスワードとして AWS アクセス秘密鍵を入力します。アクセス秘密鍵を取得する方法については、*AWS のドキュメント*を参照してください。 • Azure レジストリ - レジストリのサービスプリンシパルパスワードを入力します。サービスプリンシパルを作成する方法の詳細については、*Azure のドキュメント*を参照してください。 • Google Cloud Platform (GCP) Google Container Registry (GCR) - サービスアカウントプライベートキー JSON ファイルの `private_key` フィールドに表示される、GCR サービスアカウントの秘密鍵を入力します。サービスアカウントプライベートキーを作成してダウンロードする	文字列	×	Registry Import

	方法については、*Google Container Registry* のドキュメントを参照してください。 • 他のすべてのレジストリ - レジストリの認証に使用するパスワードを入力します。			
TENABLE_PROXY	Container Security Scanner が Tenable Vulnerability Management に接続するために使用する HTTP プロキシの URL です。 Container Security Scanner をデプロイしたマシンが Tenable Vulnerability Management に接続するためにプロキシサーバーを必要とする場合に、この変数を設定してください。 **注意:** Container Security Scanner をデプロイしたマシンが、レジストリと Tenable Vulnerability Management の両方にプロキシ接続を必要とする場合は、設定に REGISTRY_PROXY 変数と TENABLE_PROXY 変数の両方を適用できます。両方の変数を適用する場合は、Container Security Scanner を [Registry Import] モードで実行してください。 TENABLE_PROXY 変数は、プロキシがユーザー名とパスワードの認証を必要とするかどうかによって異なります。 • 認証が必要な場合 - プロキシ URL を以下の形式で入力します。 <ユーザー名>:<パスワード>@<ホスト>:<ポート> • 認証が不要な場合 - プロキシ URL を以下の形式で入力します。	文字列	×	Image Inspect または Registry Import

	<ホスト>:<ポート> **注意:** ホストはホスト名 (例: example.com) または IP アドレス (例: 192.0.2.202) を使用して指定できます。			
REGISTRY_PROXY	Container Security Scanner がレジストリに接続するために使用する HTTP プロキシの URL です。 Container Security Scanner をデプロイしたマシンがスキャン対象のレジストリに接続するためにプロキシサーバーを必要とする場合に、この変数を設定してください。 **注意:** Container Security Scanner をデプロイしたマシンが、レジストリと Tenable Vulnerability Management の両方にプロキシ接続を必要とする場合は、設定に REGISTRY_PROXY 変数と TENABLE_PROXY 変数の両方を適用できます。 REGISTRY_PROXY 変数は、プロキシがユーザー名とパスワードの認証を必要とするかどうかによって異なります。 • 認証が必要な場合 - プロキシ URL を以下の形式で入力します。 <ユーザー名>:<パスワード>@<ホスト>:<ポート> • 認証が不要な場合 - プロキシ URL を以下の形式で入力します。 <ホスト>:<ポート>	文字列	×	Registry Import

	注意: ホストはホスト名 (例: `example.com`) または IP アドレス (例: `192.0.2.202`) を使用して指定できます。			
IMAGE_NAME_WHITELIST	Tenable Container Security Scanner が行うレジストリスキャンに含めたいイメージ名またはイメージに割り当てられたタグです。 Tenable Container Security Scanner を [Registry Import] モードで実行し、特定の名前またはタグを持つイメージのみをスキャナーのスキャン対象としたい場合に、この変数を含めてください。 この変数を設定しない場合、Tenable Container Security Scanner はレジストリ内のすべてのイメージをスキャンします。 **注意:** 同じスキャン設定内に、IMAGE_NAME_WHITELIST 変数と IMAGE_NAME_BLACKLIST 変数を含めることはできません。 許可リスト変数は、何に基づいてイメージを含めるか (名前、タグ、またはその両方) によって異なります。 • 名前 - スキャンに含めるイメージに割り当てられた名前を入力します。 たとえば「`-e IMAGE_NAME_WHITELIST=alpine`」と入力すると、Tenable Container Security Scanner は alpine という名前のイメージのみをスキャンします。 • タグ - 含めるイメージに割り当てられたタグを `*:<tag>` の形式で入力します。	文字列	×	Registry Import

	たとえば「`-e IMAGE_NAME_WHITELIST=*:latest`」と入力すると、Tenable Container Security Scanner は latest のタグが付いたイメージのみをスキャンします。 • 両方 - 含めるイメージに割り当てられた名前とタグのセットを `<image>:<name>` の形式で入力します。 たとえば「`-e IMAGE_NAME_WHITELIST=alpine:latest`」と入力すると、alpine という名前で latest タグが付いたイメージのみをスキャンに含めます。 **ヒント**: イメージ名とタグの値を指定する際には、アスタリスク (*) ワイルドカード文字を使用できます。 **ヒント**: 各変数をコンマで区切ることにより、複数の許可リスト変数を指定できます (例: `-e IMAGE_NAME_WHITELIST=alpine1,alpine2,alpine3,*:latest`)。			
IMAGE_NAME_BLACKLIST	Tenable Container Security Scanner によるレジストリスキャンから除外するイメージ名またはイメージに割り当てられたタグです。 Tenable Container Security Scanner を [Registry Import] モードで実行するとき、特定のイメージをスキャン対象から除外したい場合には、この変数を含めてください。この変数を設定しない場合、Tenable Container Security Scanner はレジストリ内のすべてのイメージをスキャンします。	image_name_	×	Registry Import

	この変数を設定しない場合、Tenable Container Security Scanner はレジストリ内のすべてのイメージをスキャンします。 **注意:** 同じスキャン設定内に、IMAGE_NAME_BLACKLIST 変数と IMAGE_NAME_WHITELIST 変数を含めることはできません。 ブロックリスト変数は、何に基づいてイメージを除外するか(名前、タグ、またはその両方)によって異なります。 • 名前 - スキャンから除外するイメージに割り当てられた名前を入力します。 たとえば「`-e IMAGE_NAME_BLACKLIST=alpine`」と入力すると、Tenable Container Security Scanner は alpine という名前のイメージのみをスキャンから除外します。 • タグ - スキャンから除外するイメージに割り当てられたタグを `*:<tag>` の形式で入力します。 たとえば「`-e IMAGE_NAME_BLACKLIST=*:latest`」と入力すると、Tenable Container Security Scanner は latest のタグが付いたイメージのみをスキャンから除外します。 • 両方 - 除外するイメージに割り当てられた名前とタグのセットを `<image>:<name>` の形式で入力します。 たとえば「`-e IMAGE_NAME_BLACKLIST=alpine:latest`」と入力			

	すると、alpine という名前で latest タグが付いたイメージのみをスキャンから除外します。 **ヒント**: イメージ名とタグの値を指定する際には、アスタリスク (*) ワイルドカード文字を使用できます。 **ヒント**: 各セットをコンマで区切ることにより、複数のブロックリスト変数のセットを指定できます (例: `-e IMAGE_NAME_BLACKLIST=alpine1,alpine2,alpine3,*:latest`)。			
CHECK_POLICY	真の場合、Tenable Container Security Scanner は Tenable Vulnerability Management に対して、スキャン結果に 1 つ以上のコンプライアンスポリシー違反が含まれているかどうかを検証するよう要求します。 Tenable Container Security Scanner が出力ログに出力するメッセージは、ポリシーチェックの結果に応じて異なります。 • ポリシー違反が検出された場合 - Tenable Container Security Scanner は次のメッセージを出力します: [この画像はコンプライアンスポリシーに準拠していません]。 • ポリシー違反が検出されなかった場合 - Tenable Container Security Scanner は次のメッセージを出力します: [画像はポリシーコンプライアンスに準拠しています]。 • ポリシーチェックがタイムアウトした場合 -	Boolean	×	Image Inspect

	Tenable Container Security Scanner は次のメッセージを出力します: [致命的なエラー: レポートを取得しようとしてタイムアウトしました]。 ポリシーチェックが、ポリシー違反やポリシーチェックのタイムアウト以外の何らかの理由で失敗した場合、Container Security Scanner は失敗の原因となったエラーごとに固有のメッセージを出力します。 **ヒント**: Container Security Scanner を介したイメージのスキャンを自動化するためのカスタムコードを記述した場合、以下の終了コードを参照することにより、イメージがポリシーチェックに合格したかどうかを判定できます。 • 0 - イメージはポリシーチェックに合格しました。 • 1 - タイムアウトまたはその他のエラーにより、ポリシーチェックは失敗しました。 • 2 - イメージのポリシーチェックは失敗しました。1 つ以上のコンプライアンスポリシー違反があります。 Tenable Container Security Scanner のポリシーに関する詳細については、Tenable Container Security ポリシーを管理するを参照してください。			
CHECK_POLICY_TIMEOUT	Tenable Vulnerability Management がイメージのスキャンを終えて、脆弱性検出分析を完了するのを Tenable Container Security Scanner が待機する時間 (秒) です。 デフォルトでは、Container Security Scanner は 600 秒経っても応答のないポリシーの要求をタイムアウトとします。	整数	×	Image Inspect

	注意: Container Security Scanner は、ポリシーのタイムアウトの上限値を設定しません。			
IMPORT_INTERVAL_MINUTES	Container Security Scanner が選択したレジストリからイメージをインポートしてスキャンする間隔 (分) です。 設定した時間間隔でスキャナーを繰り返し実行したい場合に、この変数を設定してください。 この変数を設定しない場合、Container Security Scanner はユーザーがレジストリのスキャンを実行した最初の 1 回のみ、選択したレジストリからイメージをインポートしてスキャンします。 この変数を設定しない場合、Container Security Scanner は選択したレジストリからイメージを 1 回のみインポートしてスキャンし、スキャン完了後に終了します。 **注意:** レジストリをスキャンする場合にのみ、設定した時間間隔でスキャナーを実行するようにスケジュール設定できます。スキャナーを [Image Inspect] モードに設定して実行する場合には、スケジュールを設定することはできません。	整数	×	Registry Import
DEBUG_MODE	真の場合、Container Security Scanner はデバッグに追加情報をスキャンのログに追加します。 **注意:** Tenable では、Tenable サポート から要求があった場合にのみ、この変数を含めることを推奨しています。	Boolean	×	Image Inspect または Registry Import
ALLOW_	真の場合、Container Security Scanner はレ	Boolean	×	Registry

INSECURE_SSL_REGISTRY	ジストリの SSL 証明書が信頼できる認証局 (CA) によって発行されていることを検証せずに、証明書を受け入れます。 **警告**: 信頼できる認証局 (CA) によって発行された SSL 証明書であることを検証せずに Tenable が証明書を受け入れると、証明書は有効ではなく、接続は安全ではない可能性があります。したがって、Tenable ではテストまたはデバッグ作業中にのみこの変数を含めることを推奨しています。			Import
HTTP_CONNECTION_TIMEOUT_SECONDS	Container Security Scanner がレジストリに接続要求を送信した後、応答が来るのを待機する時間 (秒) です。レジストリがこの時間内に接続要求を受け入れない場合、Container Security Scanner は要求をキャンセル (タイムアウト) します。 デフォルトでは、Container Security Scanner は 10 秒経っても応答のない接続要求をタイムアウトとします。	整数	×	Image Inspect または Registry Import
HTTP_IDLE_TIMEOUT_SECONDS	Container Security Scanner がレジストリにイメージデータの要求を送信した後、応答が来るのを待機する時間 (秒) です。レジストリがこの制限時間内に応答しない場合、Container Security Scanner は要求をキャンセル (タイムアウト) します。 デフォルトでは、Container Security Scanner は 60 秒経っても応答のない要求をタイムアウトとします。	整数	×	Image Inspect または Registry Import
HTTP_REQUEST_TIMEOUT_	要求をアクティブな状態にしておくことを Container Security Scanner が許可する時間 (秒) (すなわち、レジストリが接続要求を	整数	×	Image Inspect または

SECONDS	受け入れて、イメージデータの要求に応答するのを Container Security Scanner が待機する時間)。この制限時間の経過後に要求がアクティブな場合、Container Security Scanner は要求をキャンセル(タイムアウト)します。 デフォルトでは、Container Security Scanner はアクティブな要求を 60 秒後にタイムアウトとします。			Registry Import

Tenable Container Security Scanner を設定して実行する

Tenable Container Security Scanner を実行する際、1 つのイメージをスキャンするか、リポジトリでホストされたすべてのイメージをスキャンするかを設定できます。

- 1 つのイメージをスキャンするには、Container Security Scanner を [Image Inspect] モードに設定して実行します。
- レジストリ内のすべてのイメージをスキャンするには、Container Security Scanner を [Registry Import] モードに設定して実行します。

Tenable Container Security Scanner を介してイメージをスキャンする

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Container Security Scanner を [Image Inspect] モードで実行し、1 つのイメージをスキャンします。

始める前に

- スキャンするイメージをローカルマシンにダウンロードします。
- お使いのローカルマシンが、CS Scanner のシステム要件に記載されているシステム要件を満たしていることを確認します。
- CS Scanner をダウンロードするの説明に従って、Container Security Scanner をダウンロードします。
- 環境変数の説明に従って、環境変数の値を設定します。

Container Security Scanner を [Image Inspect] モードで実行する方法

1. スキャナーを実行するマシンのコマンドラインインターフェースで、次のパラメーターを使用して、デプロイメントタイプにあわせてカスタマイズされた設定とコマンドを実行します。

   注意: 以下の変数の一部は、スキャナーの実行に必須ではありません。これらの変数とその定義に関する詳細については、環境変数を参照してください。

   ```
   docker save <your image name as it appears in the repository> | docker run \
   -e TENABLE_ACCESS_KEY=<variable> \
   -e TENABLE_SECRET_KEY=<variable> \
   -e IMPORT_REPO_NAME=<variable> \
   -i tenableio-docker-consec-local.jfrog.io/cs-scanner:latest inspect-image <Image name as you
   want it to appear in Tenable Vulnerability Management
   ```

2. **Enter** を押します。

   Container Security Scanner によってイメージがスキャンされます。

次の手順

- コンテナイメージのスキャン結果を表示するの説明に従って、スキャン結果を表示します。

Tenable Container Security Scanner を介してレジストリをスキャンする

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Container Security Scanner を [Registry Import] モードで実行し、レジストリ内のすべてのイメージをスキャンします。

始める前に

- お使いのマシンが、Tenable Container Security Scanner システム要件に記載されているシステム要件を満たしていることを確認します。
- 「CS Scanner をダウンロードする」の説明に従って、Container Security Scanner をダウンロードします。
- 「環境変数」の説明に従って、環境変数の値を設定します。
- (オプション) Amazon Web Services (AWS) Elastic Container Registry (ECR)、Azure レジストリ、Google Container Registry (GCR) のいずれかでホストされたイメージをスキャンする場合は、レジストリを準備するの説明に従ってレジストリを準備します。

Container Security Scanner を [Registry Import] モードで実行する方法

1. スキャナーを実行するマシンのコマンドラインインターフェースで、次のパラメーターを使用して、デプロイメントタイプにあわせてカスタマイズされた設定とコマンドを実行します。

   注意: 以下の変数の一部は、スキャナーの実行に必須ではありません。これらの変数とその定義に関する詳細については、環境変数を参照してください。

   ```
   docker run \
   -e TENABLE_ACCESS_KEY=<variable> \
   -e TENABLE_SECRET_KEY=<variable> \
   -e IMPORT_REPO_NAME=<variable> \
   ```

```
-e REGISTRY_URI=<variable> \
-e REGISTRY_USERNAME=<variable> \
-e REGISTRY_PASSWORD=<variable> \
-e IMPORT_INTERVAL_MINUTES=<variable> \
-i tenableio-docker-consec-local.jfrog.io/cs-scanner:latest import-registry
```

2. **Enter** を押します。

   Container Security Scanner によってレジストリ内のすべてのイメージがスキャンされます。

次の手順

- コンテナイメージのスキャン結果を表示するの説明に従って、スキャン結果を表示します。

レジストリを準備する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

Container Security Scanner を介して以下のレジストリをスキャンする前に、これらのレジストリを準備する必要があります。

- Amazon Web Service (AWS) Elastic Container Registry (ECR)
- Azure Registry
- Google Cloud Platform (GCP) Google Container Registry (GCR)

他の種類のレジストリは、スキャン前の準備は不要です。

Amazon Web Service (AWS) Elastic Container Registry (ECR)

お使いの AWS ECR に固有の設定を行う方法については、*AWS のドキュメント*を参照してください。

AWS ECR を準備する方法

1. AWS アクセスキーを取得します。

   注意: AWS アクセスキーは、アクセスキー ID とアクセス秘密鍵の 2 つで構成されます。アクセスキー ID はレジストリのユーザー名変数で、アクセス秘密鍵はレジストリのパスワード変数です。詳細は、Tenable Container Security Scanner 環境変数 を参照してください。

次の手順

- Tenable Container Security Scanner を介してレジストリをスキャンするの説明に従って、リポジトリをスキャンします。

Azure Registry

お使いの Azure レジストリに固有の設定を行う方法については、*Azure のドキュメント*を参照してください。

Azure レジストリを準備する方法

1. お使いの Azure レジストリ用のサービスプリンシパルを作成し、サービスプリンシパルに AcrPull ロールを割り当てます。

次の手順

- Tenable Container Security Scanner を介してレジストリをスキャンするの説明に従って、リポジトリをスキャンします。

Google Cloud Platform (GCP) Google Container Registry (GCR)

お使いの GCP GCR に固有の設定を行う方法については、*Google Container Registry* のドキュメントを参照してください。

GCP GCR を準備する方法

1. GCR で、Project Viewer ロールが付与されたサービスアカウントを作成します。
2. サービスアカウントキーを JSON ファイルとして作成してダウンロードすることにより、レジストリを認証します (次の例を参照)。

```
{
  "type": "service_account",
  "project_id": "my-gcp-lab",
  "private_key_id": "d21bbxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvAAAAAAAA\nBBBBBBBB\nCCCCCCCC\nDDDDDDDD\nEEEEEEEE\nFFFFFFFF\nGGGGGGGG==\n-----END PRIVATE
KEY-----\n",
  "client_email": "cs-scanner@my-gcp-lab.iam.gserviceaccount.com",
  "client_id": "111111111111111111111",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/cs-scanner%40dh-
lab.iam.gserviceaccount.com"
}
```

3. サービスアカウント JSON ファイルを、docker -v フラグを使用してパス /serviceAccount.json にマウントします。

```
docker run -e TENABLE_ACCESS_KEY=<redacted> \
  -e TENABLE_SECRET_KEY=<redacted> \
  -e IMPORT_REPO_NAME=<repo-name>
  -e REGISTRY_URI=https://gcr.io/<gcp-project-name> \
  -v <path-to-file>:/serviceAccount.json \
  -it tenableio-docker-consec-local.jfrog.io/cs-scanner:latest import-registry
```

次の手順

- Tenable Container Security Scanner を介してレジストリをスキャンするの説明に従って、リポジトリをスキャンします。

Tenable Container Security 用語集

Tenable Container Security の製品ドキュメントでは、以下の用語が使用されています。

用語	説明
CD System (CD システム)	継続的デプロイメントシステムです。通常、テストにパスした成功したビルドを監視し、それらのビルドを受け取って本番環境にプッシュすることにより、成功したビルドのデプロイメントを自動化するために使用されます。
CI System (CI システム)	継続的インテグレーションシステムです。通常、GitHub におけるマージされたプルリクエストなどのソースコントロールのコミットを監視して、ソースコントロール内の変更が検出されたときにビルドをトリガーする (テストする) 目的で使用されます。
CI/CD System (CI/CD システム)	継続的インテグレーションおよび継続的デプロイメントシステムです。通常、GitHub におけるマージされたプルリクエストなどのソースコントロールのコミットを監視して、ソースコントロール内の変更が検出されたときにビルドをトリガー (テストする) 目的で使用されます。ビルドとテストの段階が問題なく完了したら、それらのビルドを受け取って本番環境にプッシュすることにより、成功したビルドのデプロイメントを自動化します。
コンテナ	コンテナイメージの実行時インスタンスです。開始された、または何らかの方法で実行されたコンテナイメージです。
Container Image (コンテナイメージ)	コンテナイメージファイルの内部でホストされているアプリケーション (例: ubuntu:14.04)。
Container Image Tag (コンテナイメージタグ)	コンテナの内部でホストされているアプリケーションの特定のリリースまたはバージョン (例: 14.04)。
Container Registry (コンテナレジストリ)	コンテナイメージの保管場所です。開発者と継続的インテグレーションシステムが、プッシュされたコンテナを保管できるようにします。
Continuous Deployment (継	正常にテストされたビルドをオペレーション (または DevOps) が自動的に本番環境にプッシュし、即座に利用可能にする開発プラクティスです。

用語	説明
続的デプロイメント)	
Continuous Integration (継続的インテグレーション)	開発者がコードを変更したときに定期的に、共有ソースコントロールリポジトリにコードを統合する開発プラクティスです。
Image (イメージ)	コンテナイメージファイルの内部でホストされているアプリケーション (例: ubuntu:14.04)。
Image Tag (イメージタグ)	コンテナの内部でホストされているアプリケーションの特定のリリースまたはバージョン (例: 14.04)。
Organization Admin (企業の管理者)	Tenable Container Security に最初に登録したユーザーに割り当てられるロールで、割り当て時に Organization が作成されます。招待なしで登録したユーザーには Organization Admin のロールが自動的に割り当てられ、そのアカウント用に新しい Organization が作成されます。
Registry (レジストリ)	コンテナイメージの保管場所です。開発者と継続的インテグレーションシステムが、プッシュされたコンテナを保管できるようにします。
Repository (リポジトリ)	レジストリ内の、イメージの保管場所または名前空間です。(たとえば /org/tenable_io_container_security/approved/)
Tag (タグ)	コンテナの内部でホストされているアプリケーションの特定のリリースまたはバージョン (例: 14.04)。
ユーザー	招待されて、Tenable Container Security の既存の Organization に登録したユーザーに割り当てられるロールです。招待を介して登録したユーザーには、User のロールが自動的に割り当てられ、招待者のユーザーと同じ Organization に追加されます。

イメージをインポートしてスキャンするための Tenable Container Security コネクタの設定

コネクタは、ローカルまたはサードパーティのレジストリへのリンクとして機能します。コネクタを使用してこれらのレジストリにアクセスし、そこからイメージデータを Tenable Container Security にインポートできます。

コンテナイメージをインポートして分析するには、レジストリに、または一部のケースではレジストリ独自のコネクタに接続するコネクタを設定する必要があります。

利用するコネクタを作成した後は、Tenable Vulnerability Management の **[設定]** ページからコネクタを表示して管理できます。コネクタに関する詳細については、*Tenable Vulnerability Management ユーザーガイド*のコネクタを参照してください。

Tenable Container Security がレジストリ内のイメージをスキャンして結果を表示するのにかかる時間は、スキャンするイメージの大きさと数によって異なります。

注意: コネクタを使用してイメージをインポートしてスキャンすると、Tenable Container Security のダッシュボードにイメージが表示されるまでに最大で数時間かかる場合があります。

インポートを開始してから 24 時間経ってもイメージがダッシュボードに表示されない場合は、Tenable サポート にお問い合わせください。

Tenable Container Security コネクタ

注意: Tenable Container Security では、Azure Container Registries (ACR) 用のコネクタ設定はサポートされていません。ACR レジストリからイメージをインポートするには、Tenable Container Security Scanner を使用してください。

Tenable Container Security では、以下のコネクタを介したイメージのインポートがサポートされています。

Connector	説明
Tenable Container Security Scanner	イメージを Tenable Container Security にインポートせずにスキャンすることを可能にする、コマンドラインで操作するオンプレミスのスキャンツールです。Tenable Container Security Scanner を設定するには、Tenable Container Security Scannerを参照してください。
Amazon Web Service (AWS)	AWS Elastic Container Registry 内にホストされている資産用のコネクタです。AWS ECR コネクタを設定して資産をインポートするには、イメージを Tenable

Elastic Container Registry (ECR)	Container Security にインポートするための AWS ECR コネクタを設定するを参照してください。 **注意:** AWS ECR から資産をインポートするために、Tenable Container Security はお使いの AWS アカウントへの読み取り専用アクセス権を必要とします。
Docker	Docker 互換レジストリ内にホストされている資産用のコネクタです。Docker EE レジストリ用のコネクタを設定するには、イメージを Tenable Container Security にインポートするためのローカルコネクタを設定するを参照してください。 **注意:** お使いのレジストリがリストに記載されていなくても、Docker Registry API バージョン 2.0 と互換性がある場合には、このコネクタを選択してください。Docker 互換コネクタに関する詳細については、*Docker のドキュメント*を参照してください。
Docker EE	Docker Enterprise Edition (EE) レジストリ内にホストされている資産用のコネクタです。Docker EE レジストリ用のコネクタを設定するには、イメージを Tenable Container Security にインポートするためのローカルコネクタを設定するを参照してください。
JFrog Artifactory	JFrog Artifactory レジストリ内にホストされている資産用のコネクタです。JFrog Artifactory レジストリ用のコネクタを設定するには、イメージを Tenable Container Security にインポートするためのローカルコネクタを設定するを参照してください。

イメージを Tenable Container Security にインポートするための AWS ECR コネクタを設定する

必要な追加ライセンス: Tenable Container Security

必要なユーザーロール: 管理者

Amazon Web Service (AWS) Elastic Container Registry (ECR) でホストされているイメージをインポートして分析するには、AWS ECR コネクタを設定する必要があります。その後、Tenable Container Security がレジストリからイメージをインポートし、イメージの脆弱性をスキャンします。

Tenable Container Security がレジストリ内のイメージをスキャンして結果を表示するのにかかる時間は、スキャンするイメージの大きさと数によって異なります。

注意: コネクタを使用してイメージをインポートしてスキャンすると、Tenable Container Security のダッシュボードにイメージが表示されるまでに最大で数時間かかる場合があります。

インポートを開始してから 24 時間経ってもイメージがダッシュボードに表示されない場合は、Tenable サポート にお問い合わせください。

始める前に

- Docker CLI を介して Tenable Container Security にログインするの説明に従って、アカウントをアクティブ化して Tenable Container Security にログインします。
- インポートするイメージが、自社のコンテナレジストリに保存されていることを確認します。

AWS Elastic Container Registry に接続するコネクタを設定する方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[コネクタ]** セクションで、**[作成]** をクリックします。

   Tenable Vulnerability Management で **[クラウド コネクタ]** ページが開き、**[クラウドコネクタ]** プレーンが表示されます。

2. **[コンテナのセキュリティ]** セクションで、**[AWS Elastic コンテナレジストリ]** をクリックします。

3. **[URL]** ボックスに、ECR デプロイメントの完全修飾ドメイン名を入力します (例: **`https://579133718396.dkr.ecr.us-east-2.amazonaws.com`**)。

4. **[ユーザー名]** ボックスに*[AWS]* と入力します。

5. **[パスワード]** ボックスに、AWS CLI で生成された **`docker login`** コマンドで使用された、Base 64 エンコードのパスワードを入力します。

   ヒント: お使いの ECR が us-east-2 リージョンにある場合は、**`aws ecr get-login-password --region us-east-2`** コマンドを実行して **`docker login`** コマンドを取得できます。

6. 次のいずれかを行います。

   - コネクタを保存するには、**[保存]** をクリックします。

     注意: [保存] をクリックした場合、Tenable Container Security は設定済みのコネクタを保存しますが、資産のインポートは行いません。コネクタの手動インポートを起動するには、コネクタインポートの手動起動を参照してください。

   - コネクタを保存してレジストリから資産をインポートするには、**[保存してインポート]** をクリックします。

     注意: コンテナイメージをインポートしてスキャンして、そのスキャンの実行時間が 60 分に達した場合、Tenable Container Security はスキャンを中止する場合があります。この状況が発生すると、**[イメージ]** ページの **[脆弱性]** と **[マルウェア]** 列の中止されたイメージに *[スキャン失敗]* が表示されます。

     Tenable Container Security によってスキャンが中止された場合は、*Docker* のドキュメントの説明に従って、イメージをインポートする前にイメージを簡略化してみてください。別な方法として、Tenable Container Security Scanner を使用すると、イメージを Tenable Container Security にインポートせずにスキャンできます。

     Tenable Container Security がスキャンを中止し続ける場合は、Tenable サポート にお問い合わせください。

7. (オプション) **[戻る]** をクリックして、別のコネクタを設定します。

次の手順

- コンテナイメージのスキャン結果を表示するの説明に従って、スキャン結果を表示します。

イメージを Tenable Container Security にインポートするためのローカルコネクタを設定する

必要な追加ライセンス: Tenable Container Security

必要なユーザーロール: 管理者

ローカルレジストリ内にホストされたイメージをインポートして分析するには、レジストリのコネクタを設定する必要があります。その後、Tenable Container Security がレジストリからイメージをインポートし、イメージの脆弱性をスキャンします。

Tenable Container Security がレジストリ内のイメージをスキャンして結果を表示するのにかかる時間は、スキャンするイメージの大きさと数によって異なります。

注意: コネクタを使用してイメージをインポートしてスキャンすると、Tenable Container Security のダッシュボードにイメージが表示されるまでに最大で数時間かかる場合があります。

インポートを開始してから 24 時間経ってもイメージがダッシュボードに表示されない場合は、Tenable サポート にお問い合わせください。

始める前に

- Docker CLI を介して Tenable Container Security にログインするの説明に従って、アカウントをアクティブ化してウェブポータルにログインします。
- インポートするイメージが、自社のコンテナレジストリに保存されていることを確認します。

ローカルのコンテナレジストリに接続するコネクタを設定する方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[コネクタ]** セクションで、**[作成]** をクリックします。

   Tenable Vulnerability Management で **[クラウド コネクタ]** ページが開き、**[クラウドコネクタ]** プレーンが表示されます。

2. **[コンテナのセキュリティ]** セクションで、使用するコンテナレジストリの種類をクリックし、**コンテナ名** を入力します。または、検索ボックスにレジストリの名前を入力します。

   注意: リストに表示されていないレジストリに接続したい場合は、Tenable サポート に連絡をとり、お使いのコンテナレジストリの正式なサポートを希望する旨を伝えてください。レジストリがリストに記載されていな

いが Docker に対応している場合は、**[Docker]** を選択してください。Docker 対応コネクタに関する詳細については、*Docker のドキュメント*を参照してください。

3. **[URL]** ボックスにレジストリの URL を入力します。
4. **[ポート]** ボックスにレジストリのポート ID を入力します。
5. **[ユーザー名]** ボックスに、レジストリのユーザー名を入力します。
6. **[パスワード]** ボックスに、レジストリのパスワードを入力します。
7. **[インポートのスケジュール]** トグルを使用して、スケジュールしたインポートを有効または無効にします。

   注意: デフォルトでは、Tenable Container Security は 12 時間ごとに新規の資産と更新された資産のレコードをリクエストします。

   有効な場合は、[インポート] ドロップダウンボックスで、Tenable Container Security からレジストリにデータリクエストを送信する頻度として **[日]** または **[週]** を選択します。

8. 次のいずれかを行います。

   - コネクタを保存するには、**[保存]** をクリックします。

     注意: **[保存]** をクリックした場合、Tenable Container Security は設定済みのコネクタを保存しますが、資産のインポートは行いません。コネクタの手動インポートを起動するには、*Tenable Vulnerability Management ユーザーガイド*のコネクタのインポートを手動で起動するを参照してください。

   - コネクタを保存してレジストリから資産をインポートするには、**[保存してインポート]** をクリックします。

     注意: コンテナイメージをインポートしてスキャンして、そのスキャンの実行時間が 60 分に達した場合、Tenable Container Security はスキャンを中止する場合があります。この状況が発生すると、**[イメージ]** ページの **[脆弱性]** と **[マルウェア]** 列の中止されたイメージに *[スキャン失敗]* が表示されます。

     Tenable Container Security によってスキャンが中止された場合は、*Docker のドキュメント*の説明に従って、イメージをインポートする前にイメージを簡略化してみてください。別な方法として、Tenable Container Security Scanner を使用すると、イメージを Tenable Container Security にインポートせずにスキャンできます。

> Tenable Container Security がスキャンを中止し続ける場合は、Tenable サポート にお問い合わせください。

9. (オプション) **[戻る]** をクリックして、別のコネクタを設定します。

次の手順

- コンテナイメージのスキャン結果を表示するの説明に従って、スキャン結果を表示します。

コンテナの詳細を表示する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

コンテナはイメージの実行インスタンスです。アプリケーション上でイメージを実行するときは毎回、イメージからコンテナを作成します。1 つのイメージから複数のコンテナを作成することができ、作成元のイメージに影響を与えずにこれらのコンテナを変更することができます。

システム上で認証 Tenable Nessus スキャンを実行すると、Tenable Container Security はスキャン結果を使用してイメージとコンテナを特定し、各コンテナのリスクを分析します。

その後、Tenable Container Security は直近のスキャン結果に基づいて、Tenable Container Security ダッシュボードの **[識別されたコンテナ]** ウィジェットに、スキャンステータスとリスクレベル別にコンテナを表示します。

注意: Tenable Container Security は、認証 Tenable Nessus スキャンを介して見つかったイメージとコンテナのみを特定して分析します。

注意: イメージを最初にインポートしてスキャンした後は、そのイメージは Tenable Container Security によって定期的にインポートされて再スキャンされるようになります。

始める前に

- 分析するコンテナの作成に使用されたソースイメージが Tenable Container Security によってまだスキャンされていない場合、次のいずれかの方法を使用してイメージをスキャンのためにインポートします。
    - 個別のイメージを Tenable Container Security にプッシュする。
    - 自社のローカルレジストリに保管されたイメージをインポートしてスキャンするための Tenable Container Security コネクタの設定。
    - Tenable Container Security Scanner を使用して、自社のローカルレジストリまたはお使いのマシンからイメージを直接スキャンする。

- コンテナを実行するネットワーク上で Tenable Nessus スキャンを実行します。その際 **[基本的なネットワークスキャン]** テンプレートを選択し、ネットワーク認証の認証情報を指定します。Tenable Nessus スキャンのテンプレートに関する詳細については、*Tenable Nessus ユーザーガイド*のスキャンテンプレートとポリシーテンプレートを参照してください。

  注意: Tenable Container Security は Tenable Nessus からのデータをインポートして、コンテナ内のファイルに何らかの変更が加えられたかどうかを判定します。Tenable Nessus がファイルの変更を検出した場合、Tenable ではイメージとリポジトリをチェックして、認可されていないユーザーによるアクセスがなかったことを確認するよう推奨しています。

  ヒント: 別な方法として、コンテナを実行するネットワーク上で Tenable Nessus Agent スキャンを実行することもできます。詳細については、Tenable Nessus Agentユーザーガイドを参照してください。

コンテナの詳細を表示する方法

1. **[コンテナのセキュリティ]** ダッシュボードで、**[識別されたコンテナ]** ウィジェットを見つけます。このウィジェットは、コンテナをリスクとスキャンステータス別に分類します。

   注意: Tenable Container Security によるコンテナのリスクの計算方法については、コンテナのリスクを参照してください。

2. **[識別されたコンテナ]** ウィジェットをクリックします。
   [識別されたコンテナ] ページが表示されます。特定されたコンテナの表には、Tenable Container Security によってスキャンされたイメージから作成されたすべてのコンテナが一覧表示されます。

3. 特定されたコンテナの表では、以下が可能です。

   - 特定されたコンテナの表をフィルタリングします。
   - 特定されたコンテナの表を検索します。
   - 特定されたコンテナの表内の特定されたコンテナに関する概要を表示します。

列	説明
Container ID	コンテナを実行するソフトウェアがコンテナに割り当てた ID です。
Repository/Image:Tag	リポジトリ名、イメージ名、イメージタグ (例: latest)。

Risk Score	リスクスコアを 1 ~ 10 の段階で表したものです。
スキャンステータス	Tenable Container Security によってコンテナのソースイメージがスキャンされているかどうかを示します。 • ✓ - Tenable Container Security によってソースイメージがスキャンされています。 • ⓘ - Tenable Container Security によってソースイメージが一度もスキャンされていません。 **注意:** イメージのインポートを開始すると、Tenable Container Security は即座にイメージをスキャン予定のキューに入れます。しかし、Tenable Container Security はスキャンを即座に完了させない場合もあります。脆弱性の検出漏れを防ぐために Tenable では、未スキャンと表示されているイメージがある場合には、スキャンのためにインポートされていることを確認するよう推奨しています。
File Changed	コンテナファイルに対する何らかの変更が Tenable Nessus スキャンによって検出されたかどうかを示します。 **注意:** Tenable Vulnerability Management がファイルの変更を検出した場合、Tenable ではイメージとリポジトリをチェックして、認可されていないユーザーによるアクセスがなかったことを確認するよう推奨しています。 • ✓ - Tenable Nessus はスキャン中にファイルの変更を検出しませんでした。 • ⓘ - Tenable Nessus はスキャン中にファイルの変更を検出しました。
脆弱性	コンテナ内で検出された脆弱性の数です。
マルウェア	コンテナ内で検出されたマルウェアアイテムの数です。
Host IP	コンテナが実行されるサーバーの IP アドレスです。

- 特定のコンテナの詳細情報を表示します。

  a. 特定されたコンテナの表で、表示したいコンテナの行をクリックします。
  特定されたコンテナの詳細ページが表示されます。

  b. 特定されたコンテナの詳細ページでは、以下が可能です。

タブ	アクション
Vulnerabilities	• 特定されたコンテナがリンクしているイメージ内で特定された、各脆弱性の詳細情報を表示します。 • **[深刻度]** 列では、Tenable Container Security がイメージに割り当てた深刻度評価を表示します。 **注意:** Tenable Container Security によるイメージのリスクの判定方法については、イメージのリスクを参照してください。 • **[エクスポージャー ID]** 列では、脆弱性の ID を表示します。 **注意:** 各脆弱性を特定した機関が、脆弱性の ID の形式を決定します。 • **[リスクスコア]** 列では、CVSSv2 スコアを表示します。 • **[リリース日]** 列では、コンテナを実行しているソフトウェアの脆弱性の公開日を表示します。

	• 脆弱性の表の行をクリックします。 脆弱性の詳細プレーンが表示され、その中に脆弱性の詳細情報と推奨される修正が表示されます。
Malware	• 特定されたコンテナで検出されたマルウェアに関する詳細を表示します。 • **[感染したファイル]** 列では、コンテナに出現した各感染ファイルのファイル名を表示します。 • **[リスクスコア]** 列では、それぞれの感染したファイルの CVSSv2 スコアを表示します。
Images	• コンテナがリンクしているイメージに関する詳細情報を表示します。 • **[イメージ ID]** 列では、イメージ ID を表示します。 **注意:** イメージをホストするソフトウェア (Docker など) がイメージを作成すると、イメージ ID は自動的に生成されます。 • **[リポジトリ]** 列では、イメージが存在するローカルリポジトリを表示します。 • **[イメージ名]** 列では、リポジトリに表示されるイメージ名を表示します。 • **[タグ]** 列では、イメージに関連付けられたタグ

	を表示します (例 : latest)。 • イメージの表の行をクリックします。 特定されたコンテナがリンクしているイメージの詳細ページが表示されます。イメージの詳細に関しては、「コンテナイメージのスキャン結果を表示する」を参照してください。
Package Inventory	特定されたコンテナがリンクしているイメージ内のパッケージに関する詳細情報を表示します。パッケージ名、バージョン、ライセンス、種類が含まれます。

コンテナイメージのスキャン結果を表示する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Container Security によるコンテナイメージのスキャンが完了したら、Tenable Container Security ダッシュボードでスキャン結果の詳細を表示できます。

始める前に

- 次のいずれかの方法を使用して、分析するコンテナイメージをスキャンします。
  - 個別のイメージを Tenable Container Security にプッシュする。
  - 自社のローカルレジストリに保管されたイメージをインポートしてスキャンするためのコネクタを設定する。
  - Tenable Container Security Scanner を使用して、自社のローカルレジストリまたはお使いのマシンからイメージを直接スキャンする。

コンテナイメージのスキャン結果を表示する方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[統計]** セクションで、**[イメージ]** ウィジェットをクリックします。

   [イメージ] ページが表示されます。

2. イメージの表では、次の操作を実行できます。
   - イメージの表にフィルターを適用します。
   - イメージの表内を検索します。
   - イメージの詳細情報を表示します。
     a. イメージの表で、イメージの行をクリックします。

        [イメージの詳細] ページが表示されます。

     b. **[イメージの詳細]** ページでは、以下が可能です。

タブ	アクション
Vulnerabilities	• イメージ内で特定された各脆弱性に関する脆弱性の詳細を表示します。 • **[深刻度]** 列では、Tenable Container Security がイメージに割り当てた深刻度評価を表示します。 **注意:** Tenable Container Security によるイメージのリスクの判定方法については、イメージのリスクを参照してください。 • **[脆弱性]** 列では、脆弱性 ID を表示します。 **注意:** 各脆弱性を特定した機関が、脆弱性の ID の形式を決定します。 • **[リスクスコア]** 列では、CVSSv2 スコアを表示します。 • **[リリース日]** 列では、イメージをホストしているソフトウェアの脆弱性の公開日を表示します。 • 脆弱性の表の行をクリックします。 脆弱性の詳細プレーンが表示され、その中に脆弱性の詳細情報と推奨される修正が表示されます。
Malware	イメージ内で特定されたマルウェアに関する詳細情報を表示します。感染したファイルのリスト、ファイルの種類、ファイルの MD5 と SHA256 ダイジェストが含まれます。
Package Inventory	特定されたコンテナがリンクしているイメージ内のパッケージに関する詳細情報を表示します。パッケージ名、バージョン、ライセンス、種類が含まれます。
Layer Digest	イメージ内の各レイヤーのダイジェスト ID を表示します。

Identified Containers	• **[コンテナ ID]** 列では、コンテナを実行するソフトウェアが各コンテナに割り当てた ID を表示します。 • **[ホスト名]** 列では、各コンテナが実行されるネットワークの名前を表示します。 **注意:** すべてのネットワークがホスト名を持つわけではなく、IP アドレスしか持たないものもあります。 • **[ホスト IP]** 列では、各コンテナが実行されるネットワークの IP アドレスを表示します。 • **[開始日]** 列では、コンテナが起動された直近の日付を表示します。

Tenable Container Security イメージリポジトリを管理する

必要な追加ライセンス: Tenable Container Security

レジストリにイメージをプッシュすると、自動的にイメージリポジトリが作成されます。

Tenable Container Security のイメージリポジトリを管理する方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[統計]** セクションで、**[リポジトリ]** ウィジェットをクリックします。

   [リポジトリ] ページが表示され、リポジトリの概略の説明が表示されます。

2. リポジトリの表では、以下が可能です。

   - 表内を検索します。

     必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

     a. テキストボックスに検索する語句を入力します。

     b. 🔎 ボタンをクリックします。

     Tenable Vulnerability Management は検索条件に従って表にフィルターを適用します。

     ヒント: 上部のナビゲーションバーでブレッドクラムのリンクをクリックすると、前のページに戻ります。

   - リポジトリ内のイメージの詳細を表示します。

     必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

     a. リポジトリの表で、表示するイメージを含んでいるリポジトリの行をクリックします。

     [リポジトリの詳細] ページが表示され、リポジトリの概略の説明が表示されます。**[リポジトリの詳細]** ページ上に **[コンテナイメージ]** 表が表示され、リポジトリに保管されている各イメージが一覧表示されます。

b. **[コンテナイメージ]** 表でイメージの行をクリックすると、詳細情報が表示されます。

[タグ] ページが表示されます。

c. **[コンテナタグ]** 表で行をクリックすると、そのタグの **[アクティビティログ]** 詳細プレーンが展開されます。

> **ヒント**: 上部のナビゲーションバーでブレッドクラムのリンクをクリックすると、前のページに戻ります。

- イメージリポジトリを削除します。

> **必要な Tenable Vulnerability Management ユーザーロール:** スキャンオペレーター、標準、スキャンマネージャー、または管理者

a. リポジトリの表で、削除するリポジトリの行をクリックします。

[リポジトリの詳細] ページが表示されます。

b. 詳細セクションで、**[アクション]** の横にある × 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。

c. **[削除]** をクリックして確認します。

> **ヒント**: 上部のナビゲーションバーでブレッドクラムのリンクをクリックすると、前のページに戻ります。

Tenable Container Security イメージの削除

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

注意: イメージをインポートしたときに Tenable Container Security が保持するデータは、使用したインポート方法によって異なります。

- Docker コマンドまたはコネクタ - Tenable Container Security はイメージ自体と、イメージに関連付けられているすべてのメタデータ (たとえばイメージレイヤー、イメージ上のソフトウェアパッケージなど) を保持します。
- Container Security Scanner- Tenable Container Security はイメージに関連付けられているメタデータのみを保持します。
  イメージを削除すると、Tenable Container Security はイメージ全体とイメージのメタデータのすべてを削除します。

イメージを削除する方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[統計]** セクションで、**[イメージ]** ウィジェットをクリックします。

   [イメージ] ページが表示されます。このページの表には、Tenable Container Security がインポートしてスキャンしたイメージが一覧表示されます。

2. イメージの表で、削除するイメージの横にある × ボタンをクリックします。

   [削除の確認] ウィンドウが表示されます。

3. **[削除]** をクリックして、削除を確定します。

   Tenable Container Security によってイメージと、そのイメージに関連する脆弱性がすべて削除されます。

Tenable Container Security ポリシーを管理する

Tenable Container Security ポリシーを使用すると、コンテナイメージ内の脆弱性の深刻度を特定する際に Tenable Container Security が参照するルールを設定できます。

Tenable Container Security でポリシーを設定すると、スキャナーはポリシーで設定した条件に一致するすべてのイメージを検出し、それらのイメージに false というラベルを付けます。

Tenable Container Security のポリシーを追加する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Container Security にポリシーを追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[コンテナのセキュリティ]** セクションで、**[ポリシー]** をクリックします。

   [ポリシー] ページにポリシーの表が表示されます。

   注意: ポリシーの表には、Tenable Container Security によって決定された優先順位の順番でポリシーが表示されます。

3. 右上の **[ポリシーの作成]** をクリックします。

   [新しいポリシー] プレーンが表示されます。

4. ポリシー名のテキストボックスに、意味のあるポリシー名を入力します。

5. **[リポジトリ]** セクションで、Tenable Container Security がポリシーを適用するリポジトリを選択します。

   - すべてのリポジトリにポリシーを適用するには、**[すべてのリポジトリ]** を選択します。
   - 1 つのリポジトリにポリシーを適用するには、以下の手順を行います。

     a. **[特定のリポジトリ]** を選択します。

     b. ドロップダウンボックスに、ポリシーを適用するリポジトリの名前を入力します。

     c. リポジトリを選択します。

6. **[条件]** セクションで、ポリシーをトリガーする条件を設定します。

7. **[ポリシーの作成]** をクリックします。

   [ポリシー] ページのポリシーの表に、新しいポリシーが表示されます。

注意： デフォルトでは、システムはポリシーに最高の優先順位 (1) を割り当てます。優先順位の設定を変更する場合は、ポリシーを編集します。

ヒント：上部のナビゲーションバーでブレッドクラムのリンクをクリックすると、前のページに戻ります。

Tenable Container Security ポリシーを編集する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Container Security でポリシーを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[コンテナのセキュリティ]** セクションで、**[ポリシー]** をクリックします。

   [ポリシー] ページにポリシーの表が表示されます。

   注意: ポリシーの表には、Tenable Container Security によって決定された優先順位の順番でポリシーが表示されます。

3. 編集するポリシーをクリックします。

   [ポリシーの編集] プレーンが表示されます。

4. **[プライオリティ]** ボックスに、ポリシーの優先順位を表す数字を入力します。

   Tenable Container Security は、コンテナイメージを指定した優先順位でポリシーに照らして評価します。

   既に別のポリシーに関連付けられている優先順位の数字を入力した場合、システムは新しい優先順位を受け入れ、それより下のすべてのポリシーの優先順位を引き下げます。

5. **[リポジトリ]** セクションで、Tenable Container Security がポリシーを適用するリポジトリを選択します。

   - すべてのリポジトリにポリシーを適用するには、**[すべてのリポジトリ]** を選択します。
   - 1 つのリポジトリにポリシーを適用するには、以下の手順を行います。

a. **[特定のリポジトリ]** を選択します。

b. ドロップダウンボックスに、ポリシーを適用するリポジトリの名前を入力します。

c. リポジトリを選択します。

6. **[条件]** セクションで、ポリシーをトリガーする条件を設定します。

7. **[保存]** をクリックします。

Tenable Container Security によって変更が保存され、**[ポリシー]** ページに更新された情報が表示されます。

ヒント: 上部のナビゲーションバーでブレッドクラムのリンクをクリックすると、前のページに戻ります。

Tenable Container Security ポリシーの削除

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

ポリシーの表からポリシーを削除する方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[統計]** セクションで、**[ポリシー]** ウィジェットをクリックします。

   [ポリシー] ページが表示されます。このページの表には、Tenable Container Security がコンテナイメージの評価に使用するポリシーが一覧表示されます。

   表のポリシーは、Tenable Container Security によって決定された優先順位の順番で表示されます。

2. ポリシーの表で、削除するポリシーの横にある × ボタンをクリックします。

   ヒント: ポリシーの行にカーソルを合わせると、そのポリシーの × ボタンが表示されます。

3. **[削除]** をクリックして、削除を確定します。

ポリシーの設定を表示した状態でポリシーを削除する方法

1. **[コンテナのセキュリティ]** ダッシュボードの **[統計]** セクションで、**[ポリシー]** ウィジェットをクリックします。

   [ポリシー] ページが表示されます。このページの表には、Tenable Container Security がコンテナイメージの評価に使用するポリシーが一覧表示されます。

   表のポリシーは、Tenable Container Security によって決定された優先順位の順番で表示されます。

2. ポリシーの表で、削除するポリシーの行をクリックします。

   [ポリシーの編集] プレーンが表示されます。

3. **[アクション]** セクションで、× ボタンをクリックします。

4. **[削除]** をクリックして、削除を確定します。

ヒント：上部のナビゲーションバーでブレッドクラムのリンクをクリックすると、前のページに戻ります。

Tenable Container Security ポリシーの条件設定

必要な追加ライセンス: Tenable Container Security

以下の条件のうちのいずれかを設定して、Tenable Container Security でポリシーをトリガーできます。

オプション	説明
CVSS	ポリシーをトリガーする CVSS の最大値を設定する方法 1. **[CVSS の最大値]** をクリックします。 2. ドロップダウンボックスから、演算子を選択します。 3. CVSS トリガー値を入力します。
CVE	ポリシーをトリガーする 1 つまたは複数の CVE を設定する方法 1. **[CVE]** をクリックします。 2. テキストボックスに、1 つまたは複数の CVE 値を小数形式 (0.0) で、コンマ区切りのリスト形式で入力します。
マルウェア	マルウェアに対してトリガーするポリシーを設定する方法 1. **[Malware]** をクリックします。 2. ドロップダウンボックスから **[True]** を選択します。

Tenable Container Security でのリスクメトリクス

Tenable Container Security は次のトピックに記載されるメトリクスを使用して、イメージとコンテナを Tenable Container Security ダッシュボード上で分類します。

イメージのリスク

Tenable Container Security では、脆弱性の CVSSv2 スコアに基づいて、イメージ内のすべての脆弱性に静的な深刻度カテゴリが割り当てられます。

深刻度	説明
緊急	脆弱性の CVSSv2 スコアは 9.0 ~ 10.0 の間です。
高	脆弱性の CVSSv2 スコアは 7.0 ~ 8.9 の間です。
中	脆弱性の CVSSv2 スコアは 4.0 ~ 6.9 の間です。
低	脆弱性の CVSSv2 スコアは 0.1 ~ 3.9 の間です。
Unscored	脆弱性のリスクスコアが Tenable Container Security によってまだ判定されていません。

コンテナのリスク

Tenable Container Security は、コンテナ内で最大の CVSSv2 スコアを持つ脆弱性を決定することによってコンテナの総合的なリスクスコアを計算し、そのスコアを最も近い整数に丸めます。

たとえば、コンテナ内の脆弱性の最大リスクスコアが 9.2 の場合、Tenable Container Security はコンテナ全体にリスクスコアとして 9 を割り当てます。

カテゴリ	説明
Unscanned	イメージからコンテナが作成されましたが、Tenable Container Security によって一度も脆弱性スキャンが行われていません。
Low/Medium Risk	Tenable Container Security がイメージとコンテナをスキャンし、0 ~ 7 のリスクスコアを割り当てました。
High Risk	Tenable Container Security がイメージとコンテナをスキャンし、8 ~ 10 のリスクスコアを割り当てました。

Tenable Container Security のデータ使用量を表示する

必要な追加ライセンス: Tenable Container Security

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

Tenable Container Security は、[コンテナのセキュリティ] ダッシュボードの **[使用率]** ウィジェットの使用済みデータと利用可能なデータにより、データ容量を表示します。

注意: Tenable Cloud Security のライセンスがある場合、**使用率** ウィジェットは使用できません。ライセンスの使用率を表示するには、**[設定] > [ライセンス]** ページに移動し、クラウドセキュリティリソースに **コンテナイメージ** を表示します。詳細については、ライセンス情報を表示するを参照してください。

[使用率] ウィジェットでは、お使いのライセンスで指定されている計測方法に応じて、ライセンスされたコンテナイメージ数またはギガバイト (GB) 単位でデータを分類します。ライセンスの計測方法に関する詳細については、Tenable の担当者までご連絡ください。

データ使用量を表示する方法

1. [コンテナのセキュリティ] ダッシュボードから **[使用率]** ウィジェットを見つけます。
2. データ使用量に関する以下の詳細情報を確認します。

ウィジェットのセクション	説明
[ライセンスされたスペース] または **[ライセンスイメージ]** (ライセンス体系による)	お使いのアカウントにライセンスされたデータ量です。
[ライセンスされたスペース制限] または **[ライセンスイメージの制限]** (ライセンス体系による)	現在利用可能なライセンスされたデータ量です。
[使用済みスペース] または **[使用済みライセンスイメージ]** (ライセンス体系による)	既に使用中のライセンスされたデータ量が、ライセンスされたデータ量の上限に対する割合 (パーセント) で表示されます。

	使用中のデータを計算するために、Tenable Container Security は以下を行います。 • コンテナ名、イメージレジストリ、バージョンタグの組み合わせによって各イメージを特定します。 • イメージのタグのうち最新の 3 つのみを、ライセンスされた使用量に含めます。 結果として、**[イメージ] ウィジェット**に表示されるイメージのカウント数が、**[使用率]** ウィジェットに表示される使用中のライセンスされたデータ量と一致しない場合があります。 たとえば、ライセンスされたイメージ数の上限が 20 で、既に 10 のイメージを使用している場合、**[使用済みライセンスイメージ]** の割合は 50% になります。

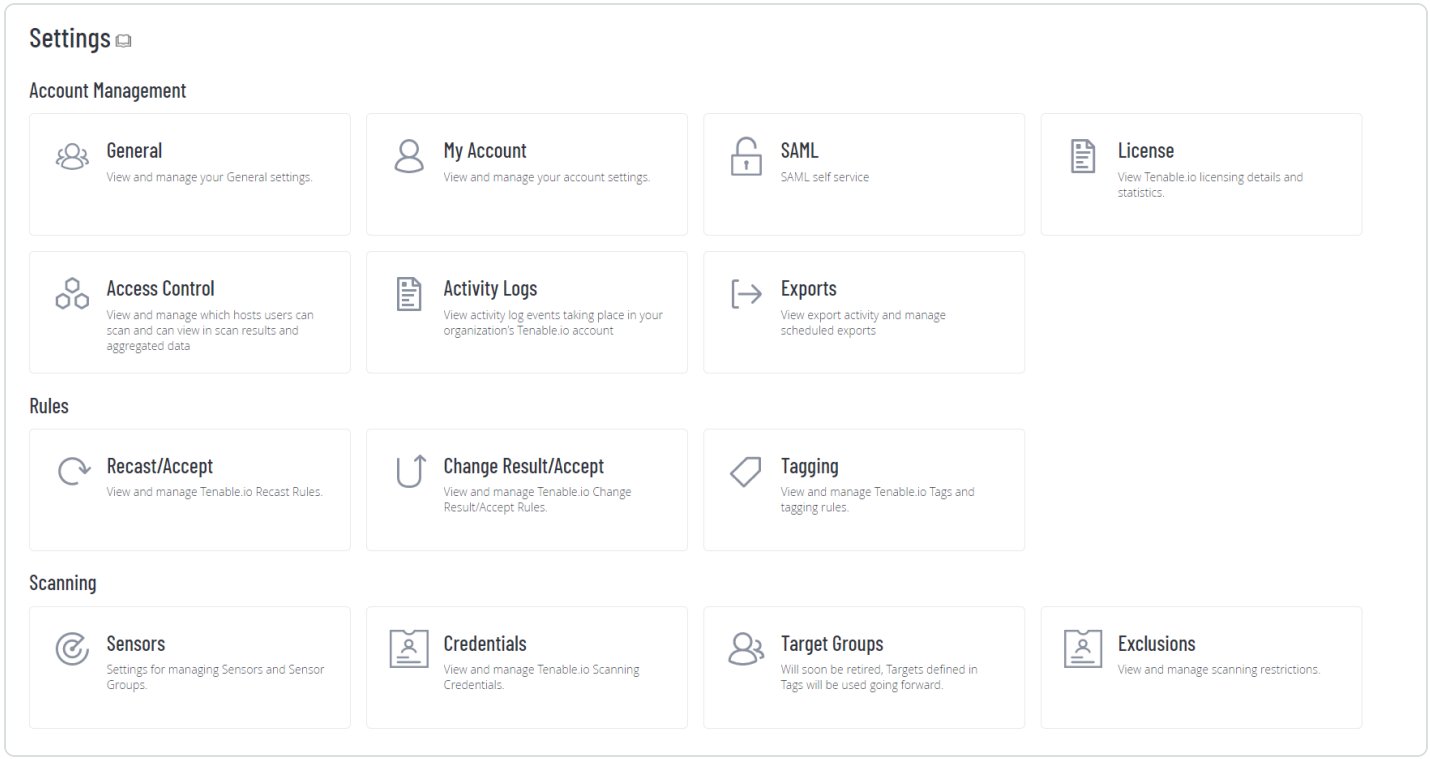
Tenable PCI ASV

Tenable PCI ASV は、独立したアプリケーションとして **[ワークスペース]** ページで利用可能になりました。Tenable PCI ASV はネットワークを包括的にスキャンすることができます。これにより、脆弱性を特定して対処し、所属組織がクレジットカード業界データセキュリティ標準 (PCI DSS) に準拠していることを確認できます。Tenable PCI ASV の詳細については、Tenable PCI ASVユーザーガイドを参照してください。

設定

[設定] ページで、さまざまなカテゴリの Tenable Vulnerability Management エクスペリエンスに影響する設定を管理できます。

たとえば、**[マイアカウント]** で、二要素認証を有効にしたり、企業のユーザーグループとアクセス許可を変更したりできます。**[タグ]** で、Tenable Vulnerability Management タグやタグ付けルールの表示と編集を行うことができます。最後に、**[クラウドコネクタ]** で、Tenable Vulnerability Management を他のプラットフォームと統合するサードパーティデータコネクタを管理できます。



このセクションには **[設定]** ページの完全なドキュメントが含まれており、Tenable Vulnerability Management インターフェースに合わせて編成されています。扱われているトピックは以下のとおりです。

- 全般設定
- マイアカウント
- SAML
- ライセンス情報
- アクセス制御
- アクティビティログ

アクセスグループ

言語

エクスポート

変更/許容ルール

タグ

センサー

認証情報

除外

コネクタ

全般設定

必要なユーザーロール: 管理者

[一般] ページで、Tenable Vulnerability Management インスタンスの全般設定を設定できます。

全般設定にアクセスする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

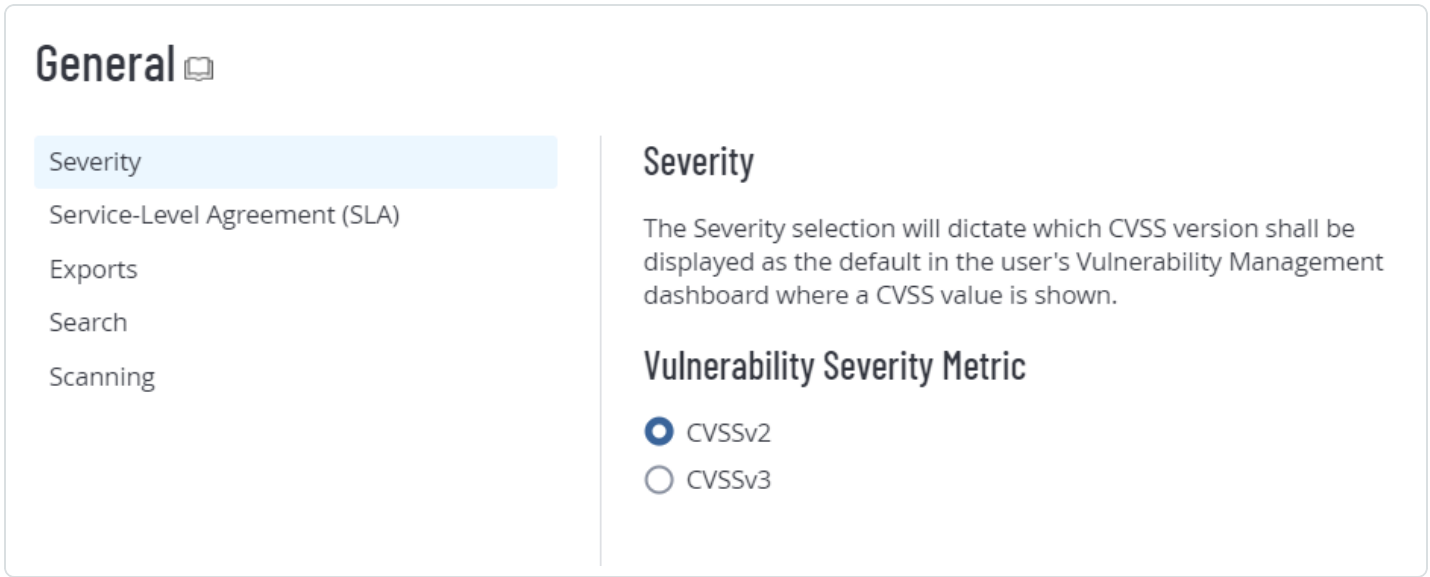
3. **[一般]** タイルをクリックします。

   [一般] ページが表示されます。デフォルトでは、**[深刻度]** タブがアクティブになっています。

ここでは、以下のオプションを設定できます。

深刻度

Tenable Vulnerability Management はデフォルトで個別の脆弱性インスタンスの深刻度の計算に CVSSv2 スコアを使用します。Tenable Vulnerability Management での脆弱性の深刻度の計算に CVSSv3 スコア(利用できる場合)を使用する場合は、深刻度メトリクス設定で設定できます。



ヒント：脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。

CVSSv2 と CVSSv3 の深刻度や範囲の詳細は、CVSS と VPRを参照してください。

注意：この設定は、以下には影響しません。

- Tenable Web App Scanning 脆弱性。
- Tenable Container Security脆弱性
- **[SLA の進捗：脆弱性の経過日数]** ウィジェットに表示される計算。SLA の深刻度を変更するには、**[一般]** ページの **[サービスレベルアグリーメント (SLA)]** タブに移動します。

注意：CVSS 深刻度メトリクス設定を変更した場合、新しい設定は、システムに入ってくる新しい検出結果にのみ反映されます。既存の検出結果は、以前の深刻度設定のみを反映します (別の方法で変更しない限り)。変更ルールの詳細については、変更/許容ルールを参照してください。

深刻度設定を行う方法

1. **[深刻度]** タブで、Tenable Vulnerability Management での深刻度の計算に使用するメトリクスを選択します。
   - **CVSSv2** - すべての深刻度の計算に CVSSv2 スコアを使用します。
   - **CVSSv3** - すべての深刻度の計算に CVSSv3 スコアを使用します。CVSSv3 スコアを利用できない場合に限り CVSSv2 スコアを使用します。
2. **[保存]** をクリックします。
3. システムで変更が保存され、選択された内容に基づき深刻度が計算されるようになります。

   変更前に検出された脆弱性は、すべて検出された時点での深刻度が維持されます。変更後は、スキャンで検出された脆弱性の深刻度は、すべて新たに選択された内容に基づいて設定されます。そのため、1 つの脆弱性について異なる CVSS スコアや深刻度が表示される場合があります。

   ヒント：脆弱性インスタンスは、資産上に表示されている脆弱性の単一インスタンスで、プラグイン ID、ポート、プロトコルによって一意に識別されます。

サービスレベルアグリーメント (SLA)

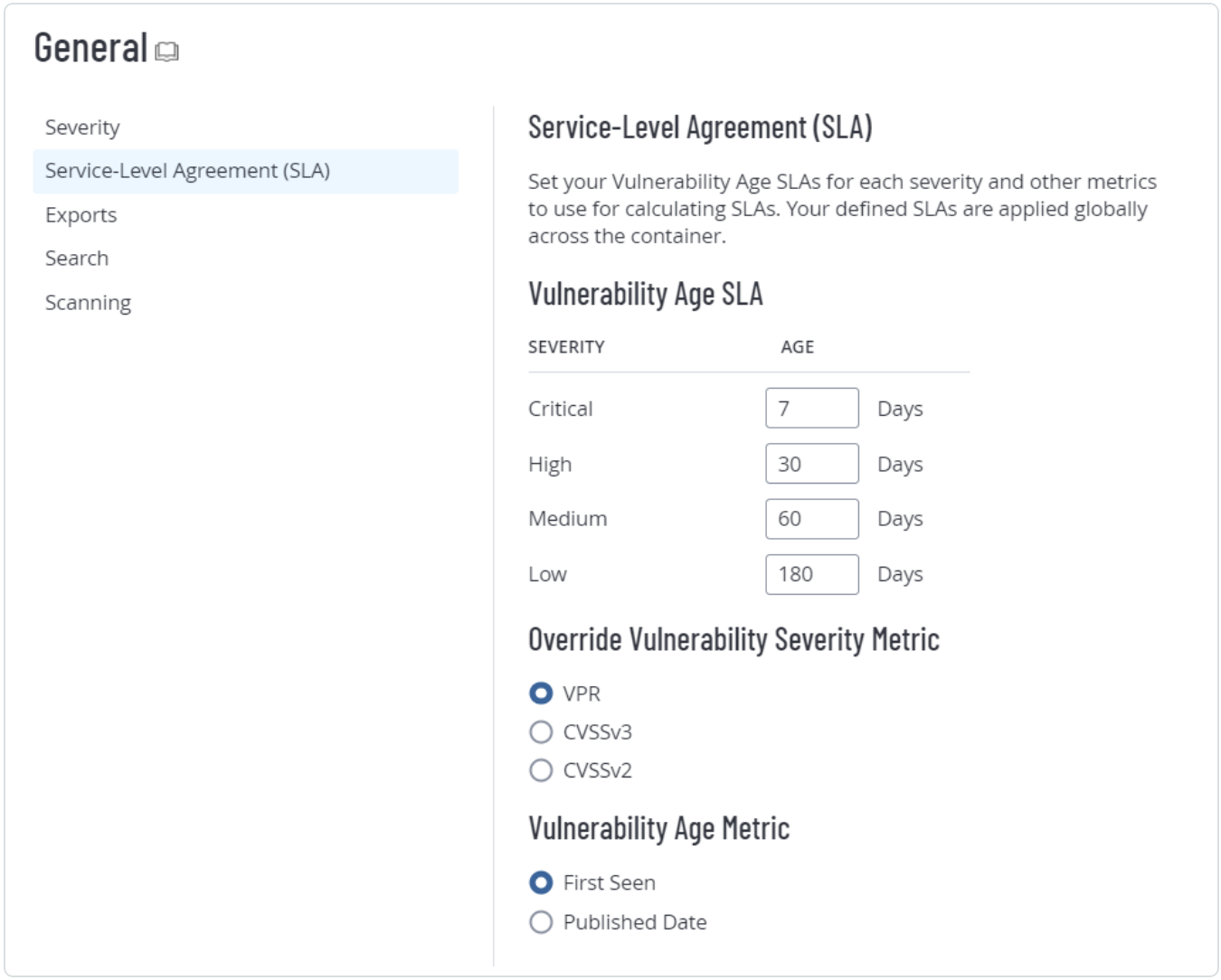
サービスレベルアグリーメント (SLA) 設定を行うと、Tenable による SLA データの計算方法を変更できます。

このデータは **[脆弱性管理の概要]** ダッシュボードの **[SLA 進捗状況: 脆弱性の経過日数]** ウィジェットで表示できます。詳細は、脆弱性管理ダッシュボード を参照してください。

SLA 設定を行う方法

1. **[サービスレベルアグリーメント (SLA)]** タブをクリックします。

   SLA オプションが表示されます。



2. 次のオプションを設定します。

オプション	デフォルト	説明/アクション
Vulnerability Age SLA	• **Critical** 7 日 • **High** 30 日 • **Medium** 60 日 • **Low** 180 日	各深刻度に含まれている日数を変更するには、**[重大]**、**[高]**、**[中]**、または **[低]** の横にあるボックスに整数を入力します。
Override Vulnerability Severity Metric	VPR	Tenable が SLA データの計算に VPR 深刻度、CVSSv2 深刻度、または CVSSv3 深刻度のいずれを使用するかを指定します。 これらのメトリクスについては、CVSS と VPRを参照してください。 **注意:** このオプションは、**[SLA の進捗: 脆弱性の経過日数]** ウィジェットに表示される計算にのみ反映されます。製品の他のすべての領域に対し、深刻度メトリクスの変更を反映させるには、**[一般]** ページの **[深刻度]** タブに移動します。
脆弱性の経過日数メトリクス	初回確認日	Tenable が SLA データの計算に **First Seen** または **Published Date** のいずれを使用するかを指定します。

3. **[保存]** をクリックします。

   Tenable Vulnerability Management によって SLA 設定が保存されます。

言語

[一般] ページで、Tenable Vulnerability Management コンテナ内のプラグイン言語を、英語、日本語、簡体字中国語、繁体字中国語に変更できます。この設定は、コンテナ内のすべてのユーザーに影響します。

プラグイン言語を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[一般]** タイルをクリックします。

   [一般] タイルが表示されます。デフォルトでは、**[深刻度]** タブがアクティブになっています。

4. **[言語]** タブをクリックします。

   [言語] タブが表示されます。

5. **[言語]** で、新しい言語を選択します。

   Tenable Vulnerability Management によって、コンテナのプラグイン言語が更新されます。

エクスポート

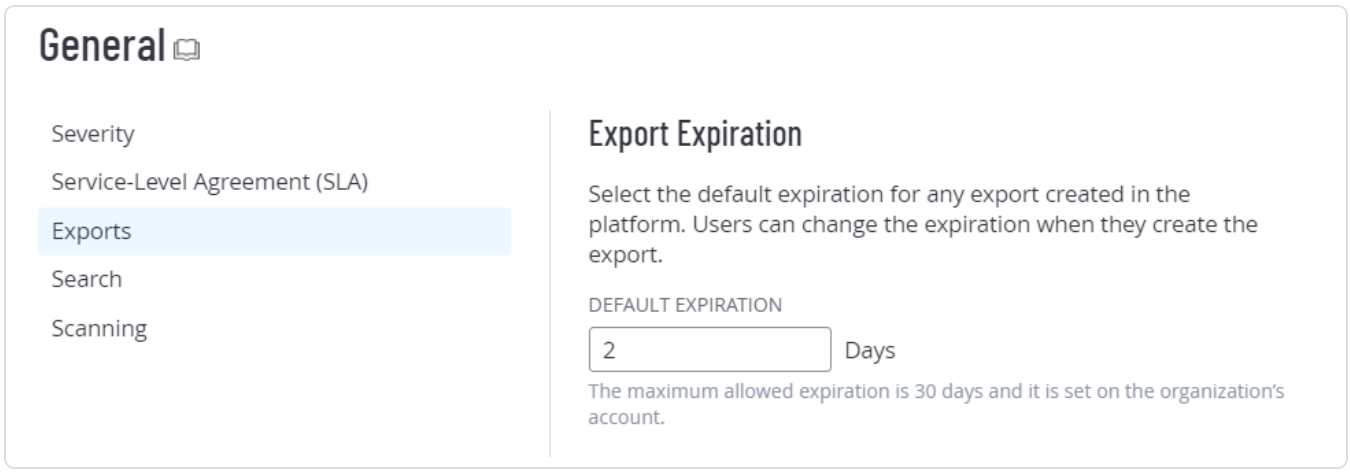
デフォルトのエクスポート有効期限を設定する方法

エクスポートを作成する場合、エクスポートファイルの有効期限を最大 30 暦日 (Tenable Vulnerability Management が許可する最大日数) まで設定できます。

デフォルトでは、Tenable Vulnerability Management で作成するエクスポートの有効期限は 30 日です。Tenable Vulnerability Management が許可するエクスポートファイルの有効期限の日数を減らしたい場合は、デフォルトのエクスポート有効期限日数を設定できます。

1. **[エクスポート]** タブをクリックします。

   [エクスポートの有効期限] オプションが表示されます。



2. **[デフォルトの有効期限]** ボックスに、Tenable Vulnerability Management が許可するエクスポート有効期限までの日数を入力します。

   注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

   注意: 日数は 1 から 30 の整数で入力する必要があります。

3. **[保存]** をクリックします。

   Tenable Vulnerability Management によって設定が保存され、エクスポートの有効期限が切れるまでの許容日数が更新されます。

検索

プラグイン出力データ保持を有効にすると、スキャンを起動するたびに Tenable Vulnerability Management でプラグイン出力データを保存できるようになります。その後、プラグイン出力で脆弱性の検出結果をフィルターできます。詳細は、検出結果フィルターを参照してください。

注意: この設定が 35 日間使用されないと、Tenable がこの設定を自動的に無効にします。その後のすべてのスキャンでプラグイン出力の検索を実行するには、この設定を再度有効にします。この設定は、**調査** ユーザーインターフェース内で通常の検索を実行する必要がある場合にのみ使用します。

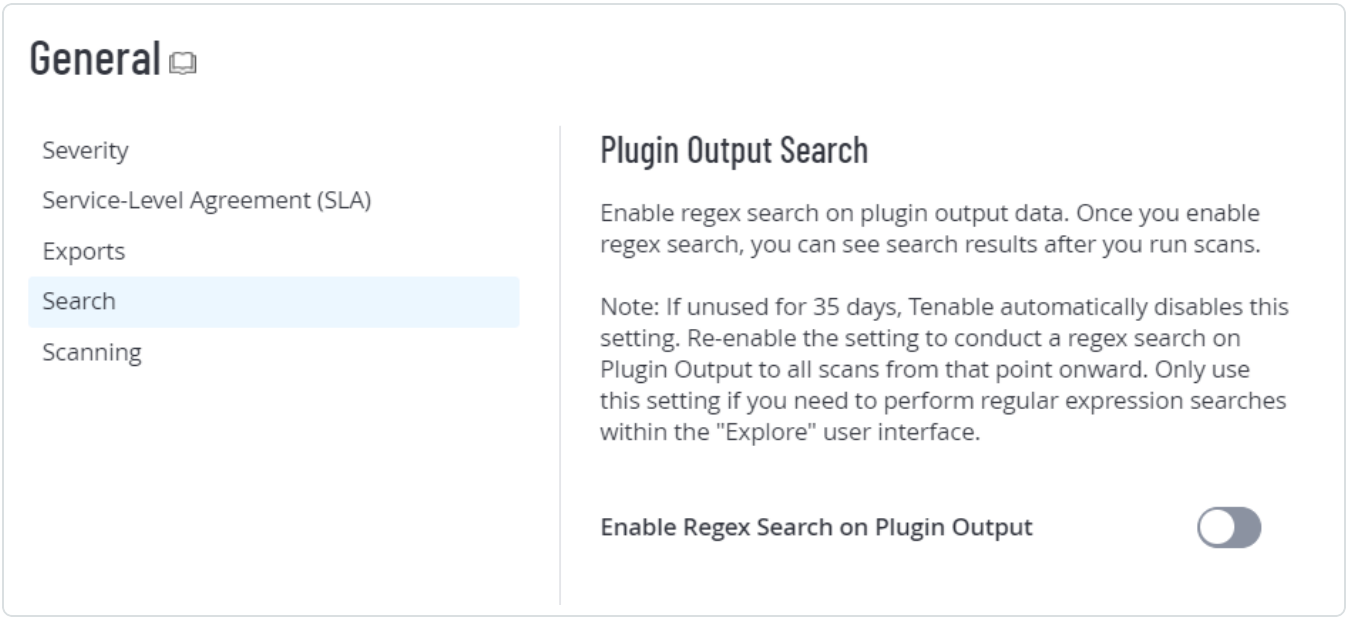
プラグイン出力データ保持を有効にしたら、スキャンを起動して、Tenable Vulnerability Management がプラグイン出力データを識別して保存できるようにする必要があります。

注意: 有効にしたプラグイン出力データ保持を無効にすることはできません。

プラグイン出力データ保持を有効にする方法

1. 左側のナビゲーションプレーンで、**[検索]** タブをクリックします。

   検索オプションが表示されます。



2. **[プラグイン出力で正規表現検索を有効にします]** トグルをクリックします。
3. **[保存]** をクリックします。

   Tenable Vulnerability Management で、ご使用のアカウントのプラグイン出力データ保持が有効になります。

次の手順

- ホスト資産のスキャンを起動します。

スキャン中

[スキャン] セクションでは、2 つの設定を使用して Tenable Vulnerability Management が情報レベルのプラグインを処理する方法を変更できます。

警告: Tenable は今後数週間のうちにすべてのお客様のこれらの設定を削除します。詳細については、Tenable の担当者までお問い合わせください。

高容量トラフィック情報のプラグインの処理

この設定を無効にすると、Tenable Vulnerability Management がスキャンされたすべてのホストのすべてのオープンポートに関して個別の検出結果を生成しなくなります。この設定を無効にすると、スキャン時間とスキャン結果のエクスポート時間が短縮され、有効にすると時間が非常に長くなる場合があります。詳細については、Platform Performance Improvement FAQ - Info Plugins (プラットフォームパフォーマンスの向上に関する FAQ - 情報プラグイン) を参照してください。

影響を受けるプラグイン ID

- 34220 - Netstat Portscanner (WMI)
- 34252 - Microsoft Windows リモートリスナーの列挙 (WMI)
- 11219 - Nessus SYN スキャナー
- 14272 - Netstat Portscanner (SSH)
- 25221 - リモートリスナーの列挙 (Linux / AIX)
- 10736 - DCE サービスの列挙
- 99265 - macOS リモートリスナーの列挙
- 10335 - Nessus TCP スキャナー
- 14274 - Nessus SNMP スキャナー
- 34277 - Nessus UDP スキャナー

ヒント: これら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。

開いているポートの検出結果を再配置する

開いているポートの検出結果を **[検出結果]** ワークベンチではなく **[資産の詳細]** ページに表示して、Tenable Vulnerability Management が検出結果を処理する方法を変更するには、この設定を有効にします。この変更が所属組織に与える可能性のある影響については、Tenable Vulnerability Management New Data Format: Relocate Open Port Findings (Tenable Vulnerability Management の新しいデータ形式: 開いているポートの検索結果を再配置する) を参照してください。

注意: **[開いているポートの検出結果を再配置する]** を有効にすると、開いているポートが個別の検出結果として保存されなくなるため、サードパーティ統合で開いているポートの検出結果データを受け取ることができなります。

この設定では、以下を実行できます。

- 開いているポートの検出結果を**[検出結果]**ワークベンチから**[資産の詳細]**ページに*移動*します。**[資産の詳細]**ページは、**[資産]**ワークベンチでホスト資産をクリックすると表示されます。

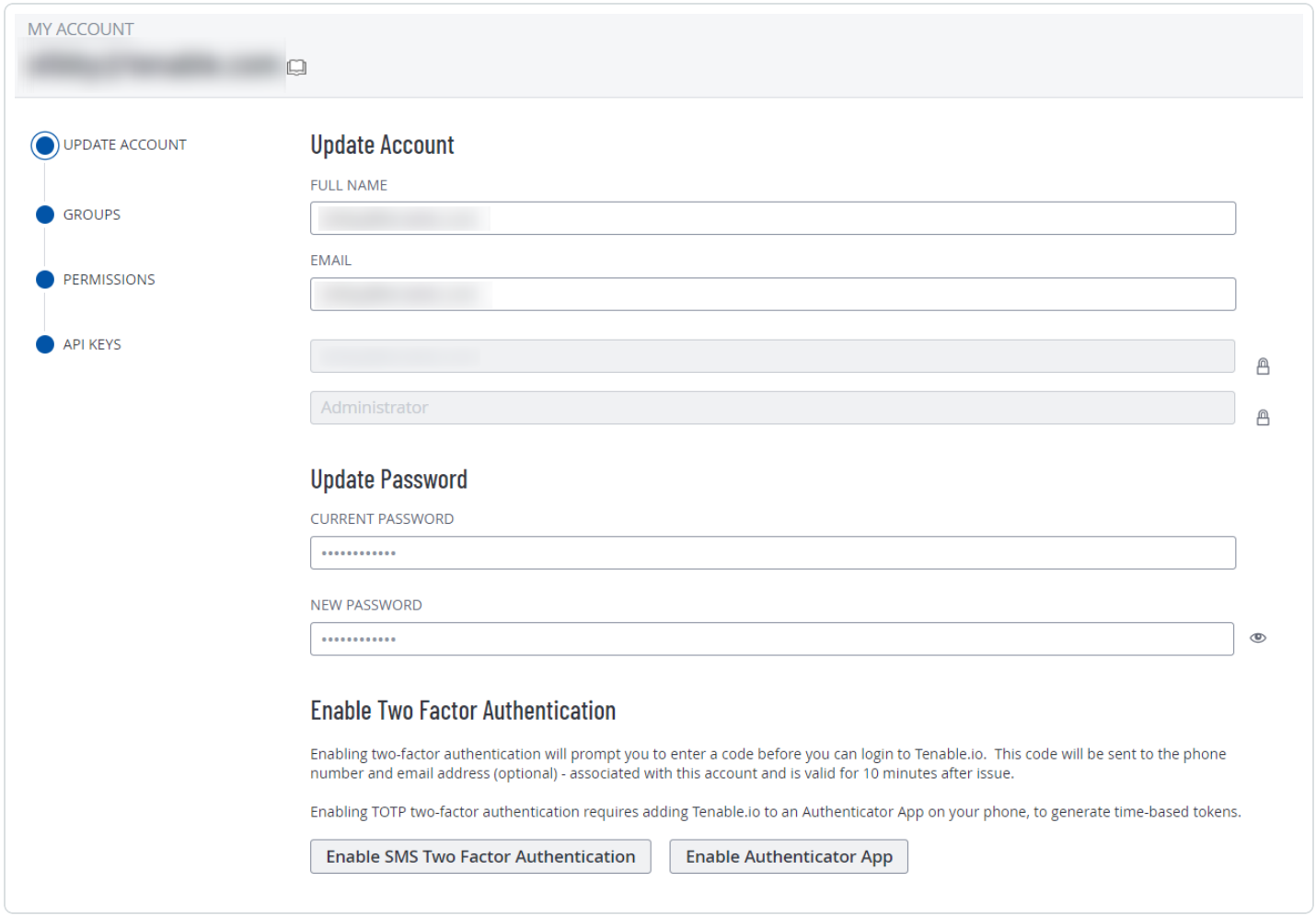
  次の高トラフィックプラグインの開いているポートの検出結果が[資産の詳細]ページに移動

  - 34220 - Netstat Portscanner (WMI)
  - 34252 - Microsoft Windows リモートリスナーの列挙 (WMI)
  - 11219 - Nessus SYN スキャナー
  - 14272 - Netstat Portscanner (SSH)
  - 25221 - リモートリスナーの列挙 (Linux / AIX)
  - 10736 - DCE サービスの列挙
  - 99265 - macOS リモートリスナーの列挙
  - 10335 - Nessus TCP スキャナー
  - 14274 - Nessus SNMP スキャナー
  - 34277 - Nessus UDP スキャナー

- **[資産の詳細]**ページの**[オープンポート]**タブを有効にします。このタブに、開いているポートの検出結果が表示されるようになります。
- **[資産]**ワークベンチで**[オープンポート]**フィルターを有効にし、ホスト資産の開いているポートを検索できます。
- **[タグ]**ページで**[オープンポート]**ルールを有効にし、開いているポートにタグを付けることができます。
- **[資産]**ワークベンチに[オープンポート]フィールドを追加し、開いているポートのデータをエクスポートできるようにします。
- (オプション) 開いているポートの検出結果を一括資産エクスポート API に追加します。詳細については、*Tenable 開発者ポータル*の API 変更ログを参照してください。この機能をリクエストするには、Tenable の Customer Success Manager までご連絡ください。

マイアカウント

[**My Account**] ページから、独自のユーザーアカウントを変更できます。



次のいずれかの方法で マイアカウント ページに移動できます。

- **[設定]** ページから **[マイアカウント]** ページにアクセスする方法

  a. 左上にある ☰ ボタンをクリックします。

  左側にナビゲーションプレーンが表示されます。

  b. 左のナビゲーションプレーンで **[設定]** をクリックします。

  [設定] ページが表示されます。

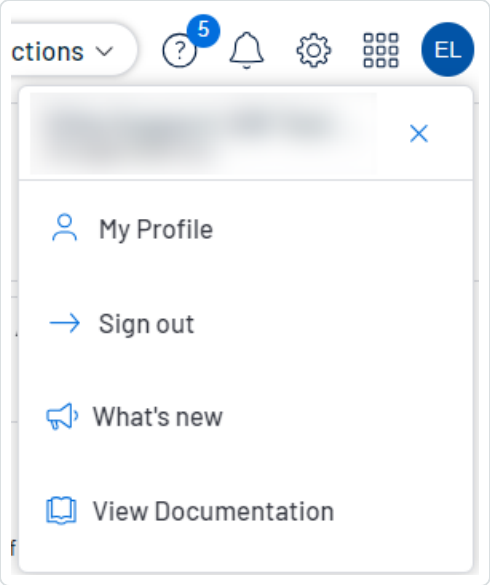
c. **[マイアカウント]** タイルをクリックします。

[マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

- 任意のページの上部ナビゲーションメニューから **[マイアカウント]** ページにアクセスする方法

a. 右上の青いユーザー円をクリックします。

ユーザーアカウントメニューが表示されます。



b. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

アカウントの詳細の表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[マイアカウント] ページでは、ログインの詳細、ユーザーロール、割り当てられているグループとアクセス許可など、アカウントに関する詳細を表示できます。

アカウントの詳細を表示する方法

1. 次のいずれかを行います。

   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

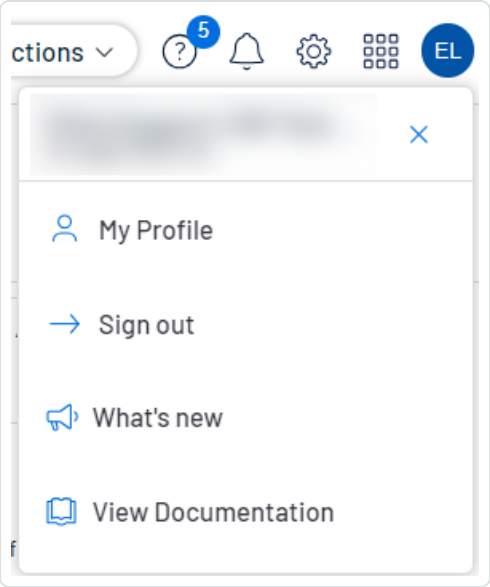
        [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

        [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

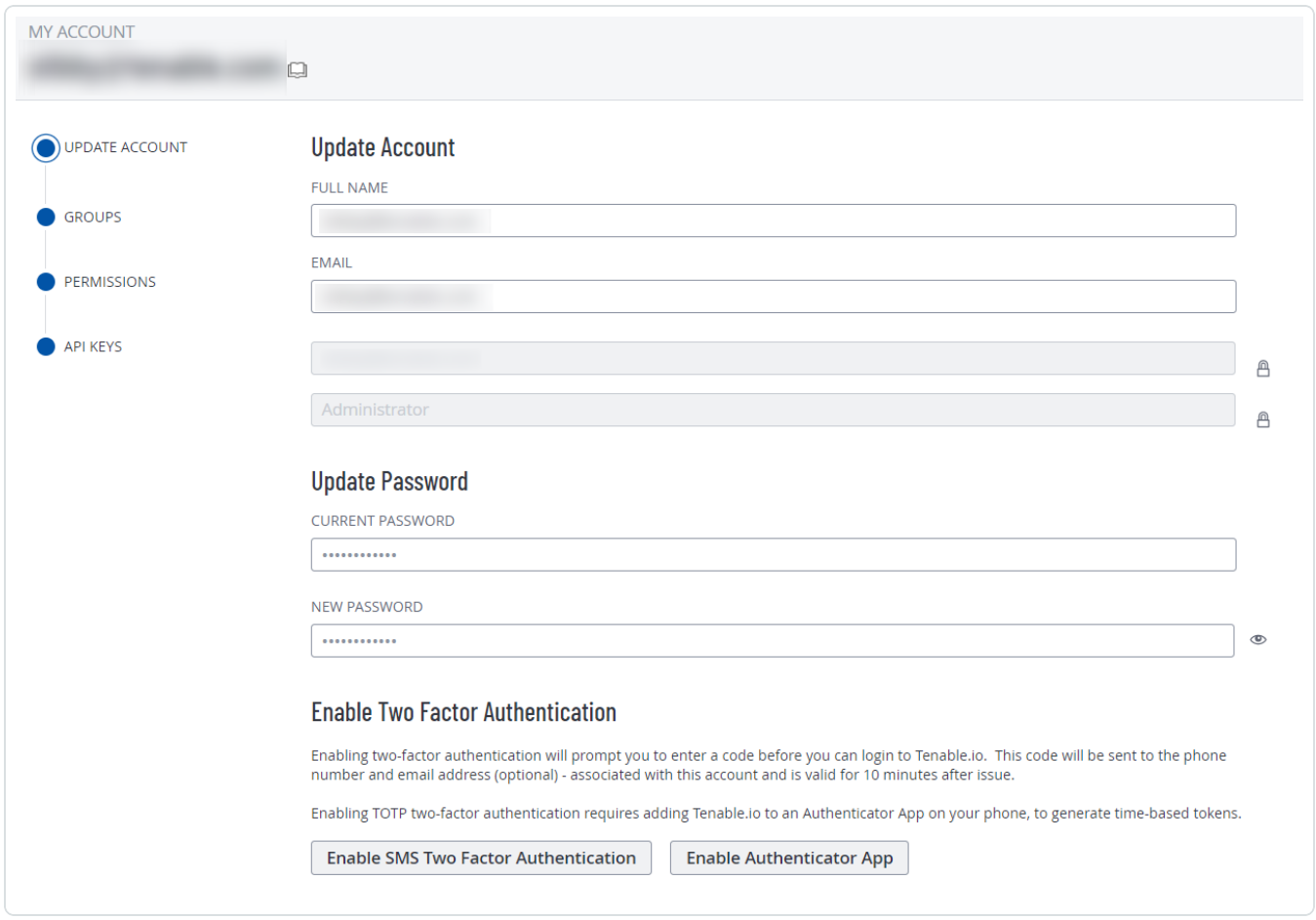
   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。



2. ページの左側で、以下の選択肢から選択します。

オプション	アクション
アカウントの更新	• **[アカウントのアップデート]** をクリックします。 **[アカウントのアップデート]** セクションが表示され、アカウントに関する以下の項目の詳細が表示されます。 ◦ **氏名** ◦ **Eメール** ◦ **ユーザー名** ◦ **ロール**

	• (オプション) 基本的なアカウント情報 (名前やメールアドレスなど) を更新します。 **注意:** ユーザー名やロールを変更することはできません。 • (オプション) パスワードを変更します。 • (オプション) アカウントで二要素認証を設定または無効にします。 • (オプション) アカウントでベータ版機能の探索機能を有効または無効にします。
グループ	• **[グループ]** をクリックします。 **注意:** **[マイアカウント]** ページでグループ設定を変更することはできません。詳細は、ユーザーグループを参照してください。 • **[グループ]** 表には以下の内容が表示されます。 ◦ 割り当てられているユーザーグループ ◦ 各ユーザーグループのメンバー数
アクセス許可	• **[アクセス許可]** をクリックします。 **注意:** アクセス許可をユーザーに適用すると、指定された資産タグ (つまり、オブジェクト)、およびそれらのオブジェクトに該当する資産に対して特定のアクションが実行できるようになります。アクセス許可は、個別のユーザーまたはユーザーグループのすべてのメンバーに適用できます。詳細は、権限を参照してください。 **注意:** **[マイアカウント]** ページでアクセス許可設定を変更することはできません。 • **[アクセス許可]** 表には以下の内容が表示されます。 ◦ アカウントに割り当てられているアクセス許可の名前 ◦ それらのアクセス許可によって実行できるアクション ◦ 各アクセス許可が適用されるオブジェクト
API	• **[API キー]** をクリックします。

キー	• API キーの説明が表示されます。 • API キーを生成する. **警告:** **[生成]** ボタンをクリックすると、既存の API キーはすべて置き換えられます。以前の API キーを使用していたアプリケーションを更新する必要があります。 **警告**: **[API キー]** タブを閉じる前に、アクセスキーと秘密鍵を必ずコピーしてください。このタブを閉じてしまうと、Tenable Vulnerability Management からキーを取得することはできなくなります。

注意: ユーザーアカウントの有効期限は、そのアカウントが属する Tenable Vulnerability Management コンテナの作成日に基づいて設定されます。Tenable は、この設定を直接制御します。詳細については、Tenable サポートにお問い合わせください。

アカウントを更新する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

アカウントを更新する方法

1. 次のいずれかを行います。

   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

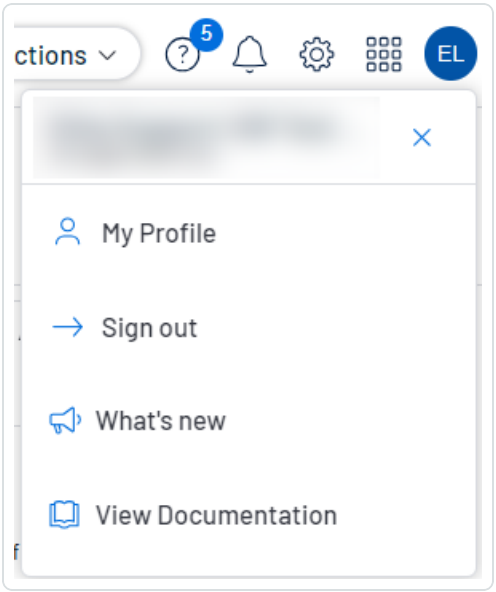
     [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

     [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. (オプション) **[名前]** を編集します。

3. (オプション) **[Eメール]** を編集します。

有効なメールアドレスは、

name@domein

の形式である必要があります。ここで、*domain* はお使いの Tenable Vulnerability Management インスタンス用に承認されたドメインに対応します。

このメールアドレスは、**[ユーザー名]** として設定されたメールアドレスをオーバーライドします。このオプションを空のままにすると、Tenable Vulnerability Management は **[ユーザー名]** の値をメールアドレスとして使用します。

> **注意:** 初期設定の間に、Tenable は Tenable Vulnerability Management インスタンス用に承認されたドメインを設定します。お使いのインスタンスにドメインを追加する方法については、Tenable サポート にお問い合わせください。

4. **[保存]** をクリックします。

Tenable Vulnerability Management はアカウントへの変更を保存します。

5. (オプション) パスワードを変更します。

6. (オプション) 二要素認証を設定します。

7. (オプション) API キーを生成します。

パスワードを変更する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

いずれの種類のユーザーアカウントのパスワードも変更できます。パスワードを変更する方法は、ユーザーアカウントに割り当てられたロールによって若干異なります。

別のユーザーのパスワードを変更するには、別のユーザーのパスワードの変更を参照してください。

パスワードを変更するには

1. 次のいずれかを行います。
   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

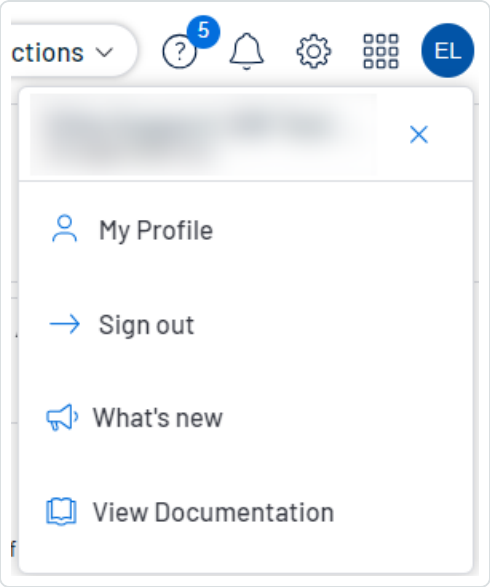
     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

     [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

     [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。
   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. **[現在のパスワード]** ボックスに現在のパスワードを入力します。
3. **[新しいパスワード]** ボックスに新しいパスワードを入力します。詳細は、Tenable Vulnerability Management のパスワード要件を参照してください。
4. **[保存]** ボタンをクリックします。

   Tenable Vulnerability Management により新しいパスワードが保存され、お使いのアカウントで現在アクティブなセッションが終了します。Tenable Vulnerability Management によりその後、再認証を求めるメッセージが表示されます。
5. 新しいパスワードを使用して、Tenable Vulnerability Management にログインします。

二要素認証を設定する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[マイアカウント] ページで、自分のアカウントに二要素認証を設定できます。

ヒント: 管理者は、ユーザーアカウントを作成または編集するときに、他のアカウントに対して二要素認証を強制することもできます。

注意: 二要素認証を設定する前に、International Phone Availability リストを確認して、Tenable Vulnerability Management からテキストメッセージを受信できることを確認してください。

二要素認証を追加または変更する方法

1. 次のいずれかを行います。

   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

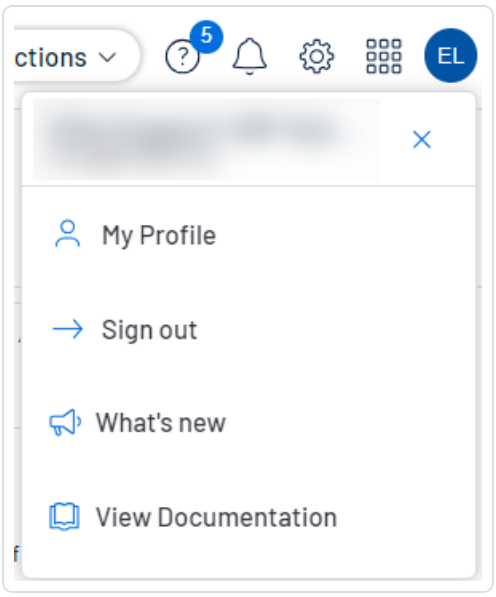
        [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

        [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. **[二要素認証を有効にする]** セクションで、以下のいずれかを行います。

- SMS の二要素認証を有効にします。

a. **[SMS 二要素認証を有効にする]** をクリックします。

[二要素認証] プレーンが表示されます。

b. **[現在のパスワード]** ボックスに現在の Tenable Vulnerability Management のパスワードを入力します。

c. **[電話番号]** ボックスに自分の携帯電話番号を入力します。

> **注意:** Tenable Vulnerability Management はデフォルトで携帯電話の番号を米国内の番号として扱い、国コードの +1 を前に付けるよう設定されています。お使いの携帯電話が米国内の番号でない場合、適切な国コードを前に付けてください。

d. **[次へ]** をクリックします。

[検証コード] プレーンが表示され、Tenable Vulnerability Management より検証コードが記載されたテキストメッセージが電話番号宛てに送信されます。

e. **[検証コード]** ボックスに、受け取った検証コードを入力します。

f. **[次へ]** をクリックします。

[二要素認証が正常にセットアップされました] メッセージが表示され、Tenable Vulnerability Management によって設定が Tenable Vulnerability Management アカウントに適用されます。

g. (オプション) Tenable Vulnerability Management が、ユーザーアカウントに関連付けられたメールアドレス宛てに検証コードを送信するかどうかを設定する方法

a. **[バックアップの E メールを送信する]** チェックボックスを選択するかクリアします。

b. **[更新]** をクリックします。

Tenable Vulnerability Managementはバックアップメールの設定を更新します。

注意: この設定の電話番号を保存すると、電話番号の編集や変更はできなくなります。使用する追加の電話番号がある場合は、新しい認証セットアップを設定する必要があります。

- 次のように、認証アプリケーションベースの認証を有効にします。

a. **[Authenticator アプリを有効にする]** をクリックします。

[二要素認証] プレーンが表示されます。

b. **[現在のパスワード]** ボックスに現在の Tenable Vulnerability Management のパスワードを入力します。

c. **[次へ]** をクリックします。

[時間ベースのワンタイムパスワード] プレーンが表示されます。

d. お好みの認証アプリケーションで、QR コードをスキャンします。

認証アプリケーションに Tenable Vulnerability Management の検証コードが表示されます。

e. **[検証コード]** ボックスに、認証アプリケーションに表示されたコードを入力します。

注意: 正しい検証コードが入力されない場合、Tenable Vulnerability Management によって QR コードがロックされます。認証アプリケーションからの設定を削除して、新しい QR をスキャンしてください。

f. **[次へ]** をクリックします。

[二要素認証が正常にセットアップされました] メッセージが表示され、Tenable Vulnerability Management によって設定が Tenable Vulnerability Management アカウントに適用されます。

新しいインターフェースで二要素認証を無効にする方法

1. 次のいずれかを行います。

   - 左上にある ☰ ボタンをクリックします。

     左側にナビゲーションプレーンが表示されます。

     a. 左のナビゲーションプレーンで **[設定]** をクリックします。

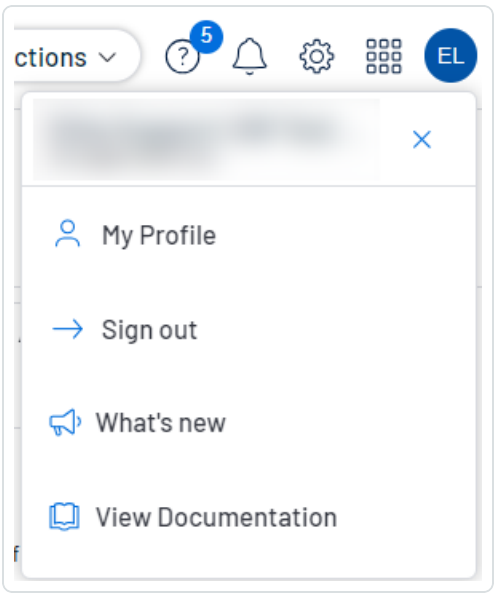
     [設定] ページが表示されます。

     b. **[マイアカウント]** タイルをクリックします。

     [マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

   - 右上の青いユーザー円をクリックします。

     ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. **[パスワードの変更]** セクションの **[現在のパスワード]** ボックスに、現在のパスワードを入力します。
3. **[二要素認証を有効にする]** セクションで、**[無効化]** をクリックします。

[二要素認証を無効化する] の確認メッセージが表示されます。

4. 警告メッセージを読み、**[続行]** をクリックします。

Tenable Vulnerability Management でお使いのアカウントの二要素認証が無効化されます。

API キーを生成する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

お使いのユーザーアカウントに関連付けられた API キーにより、お客様の企業にライセンスされた、すべての Tenable Vulnerability Management 製品の API にアクセスすることが可能になります。

注意: **Tenable Vulnerability Management API を認証するには** Tenable Vulnerability Management API のアクセスキーと秘密鍵が必要です。

注意: お使いのユーザーアカウントに関連付けられた API キーを使って、お客様の会社にライセンス付与されているすべての Tenable Vulnerability Management 製品の API にアクセスすることができます。個別の製品に別々のキーを設定することはできません。たとえば、Tenable Vulnerability Management で API キーを生成した場合、この操作により Tenable Web App Scanning および Tenable Container Security の API キーも変更されます。

注意: アプリケーションごとに、同一の API キーを使用してください。以下は例ですが、これらに限定されません。

- Tenable Vulnerability Management の統合
- サードパーティの統合
- その他のカスタムアプリケーション (Tenable Professional Services からのものを含む)

API キーを生成する方法は、ユーザーアカウントに割り当てられたロールによって異なります。管理者は、任意のアカウントの API キーを生成できます。詳細は、別のユーザーの API キーの生成 を参照してください。他のロールは自分のアカウントの API キーを生成できます。

自分のアカウントの API キーを生成する方法

1. 次のいずれかを行います。

    - 左上にある ☰ ボタンをクリックします。

      左側にナビゲーションプレーンが表示されます。

a. 左のナビゲーションプレーンで **[設定]** をクリックします。

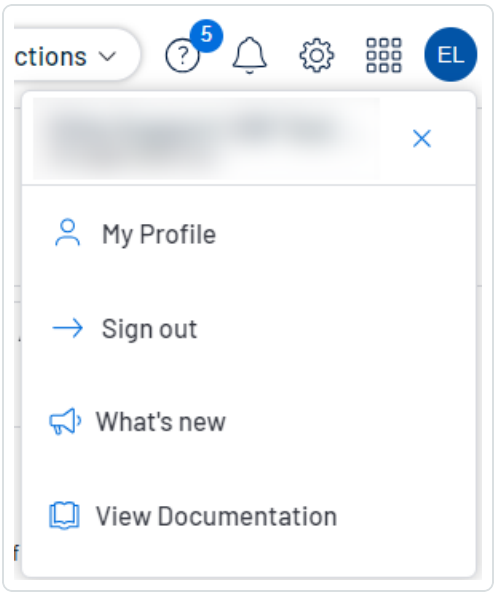
[設定] ページが表示されます。

b. **[マイアカウント]** タイルをクリックします。

[マイアカウント] ページが表示され、アカウントの詳細を表示および更新できます。

- 右上の青いユーザー円をクリックします。

ユーザーアカウントメニューが表示されます。



a. **[マイプロファイル]** をクリックします。

[マイアカウント] ページが表示されます。

2. **[API キー]** タブをクリックします。

[API キー] セクションが表示されます。

3. **[生成]** をクリックします。

[API キーを生成する] ウィンドウが警告とともに表示されます。

> **警告:** **[生成]** ボタンをクリックすると、既存の API キーはすべて置き換えられます。以前の API キーを使用していたアプリケーションを更新する必要があります。

4. 警告を確認し、**[生成]** をクリックします。

Tenable Vulnerability Management により新しいアクセスキーと秘密鍵が生成され、ページの **[カスタム API キー]** セクションに新しいキーが表示されます。

> **ヒント:** **[生成]** ボタンが無効になっている場合は、管理者に連絡して、アカウントの API アクセスが有効になっていることを確認してください。詳細は、ユーザーアカウントの編集を参照してください。

5. 新しいアクセスキーと秘密鍵を安全な場所にコピーします。

> **警告:** **[API キー]** タブを閉じる前に、アクセスキーと秘密鍵を必ずコピーしてください。このタブを閉じてしまうと、Tenable Vulnerability Management からキーを取得することはできなくなります。

自分のアカウントのロックを解除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

Tenable Vulnerability Management でログインを試みて 5 回連続して失敗すると、アカウントがロックされます。

注意: アカウントで指定されたメールアドレスにアクセスできない場合、Tenable Vulnerability Management インスタンスの管理者が代わりにパスワードをリセットできます。

注意: ユーザーは、ユーザーインターフェースからロックアウトされる可能性がありますが、適切な認証 (api_permit) が割り当てられている場合は API リクエストを送信できます。詳細は、Tenable 開発者ポータルを参照してください。

自分のアカウントのロックを解除する方法

1. Tenable Vulnerability Management ログインページで、**[パスワードをお忘れですか?]** をクリックします。リンクをクリックします。

   パスワードリセットのページが表示されます。

2. **[ユーザー名]** ボックスに、Tenable Vulnerability Management のユーザー名を入力します。
3. CAPTCHA ボックスに、質問に対する自分の答えを入力します。
4. **[送信]** をクリックします。

   Tenable Vulnerability Management により、ユーザーアカウントで指定されたメールアドレス宛てにパスワード復旧の手順が送信されます。

5. メールに記載された手順に従い、パスワードをリセットします。詳細については、パスワード要件を参照してください。

SAML

SAML ID プロバイダーからの認証情報を受け入れるように Tenable Vulnerability Management を設定できます (例: Okta)。これによりセキュリティの層がさらに厚くなり、SAML 認証情報が Tenable Vulnerability Management 内での使用のために認定されます。ユーザーの SAML を有効にすると、そのユーザーは ID プロバイダーを通じて Tenable Vulnerability Management に直接ログインできるようになり、自動的にサインインして Tenable Vulnerability Management ランディングページにリダイレクトされます。

[SAML] ページで、SAML 認証情報を表示して管理できます。また Tenable Vulnerability Management インスタンス内のユーザーに対して新しい設定を有効化、無効化、追加することもできます。

ヒント: Tenable Vulnerability Management で使用するために SAML を設定する方法については、Tenable SAML 設定クイックリファレンスガイドにある手順を確認してください。

注意: Tenable Vulnerability Management は SAML 2.0 設定をサポートしています。

注意: ユーザーの SAML が設定されたら、ユーザーが IdP タイルまたは SP メタデータファイルで提供されている URL (cloud.tenable.com/SAML/XXXXXX など) を使用してログインし、ログアウトしてから、Tenable Vulnerability Management ログインページの **[SSO 経由のサインイン]** リンクにアクセスできるようになります。

SAML の詳細

[SAML] ページでは、SAML 設定に関する次の詳細を含む表を表示できます。

列	説明
UUID	新しい SAML 設定を作成すると、Tenable Vulnerability Management によって自動的に生成される UUID
説明	SAML 設定の説明
前回のログイン	インスタンス上のユーザーが SAML 設定を使って最後に正常にログインした日時 **注**: Tenable Vulnerability Management に SAML アイデンティティプロバイダーのログインデータがある場合にのみ、**[最終ログイン]** 列に値が表示されます。
前回のログイン試行	インスタンス上のユーザーが最後に SAML 設定を介してログインを試行した日時 **注**: Tenable Vulnerability Management に SAML アイデンティティプロバイダーの試行ログイ

	ンデータがある場合にのみ、**[最終試行ログイン]** 列に値が表示されます。
証明書	SAML 設定の証明書 証明書の列で、次のタスクを実行できます。 • ボタンをクリックすると、証明書がクリップボードにコピーされます。 • ボタンにカーソルを合わせると、証明書の有効期限日が表示されます。 **注意:** アイデンティティプロバイダーが証明書の有効期限を決定します。
アクション	当該設定の 1 つ以上のセキュリティ証明書を含む metadata.xml ファイルをダウンロードできる、インタラクティブな列 metadata.xml ファイルをダウンロードする方法 a. metadata.xml ファイルをダウンロードする設定の **[アクション]** 列で、⋮ ボタンをクリックします。 オプションメニューが表示されます。 b. メニューで、⭳ **[SP メタデータのダウンロード]** をクリックします。 Tenable Vulnerability Management で metadata.xml ファイルがコンピューターにダウンロードされます。

SAML 設定の表示

必要なユーザーロール: 管理者

SAML 設定を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

   [SAML] ページが表示されます。

   ヒント: Tenable Vulnerability Management で使用するために SAML を設定する方法については、Tenable SAML 設定クイックリファレンスガイドにある手順を確認してください。

4. (オプション) 表データを選別します。詳細については、テーブルを参照してください。

   [SAML] 表には次の列が含まれています。

列	説明
UUID	新しい SAML 設定を作成すると、Tenable Vulnerability Management によって自動的に生成される UUID
説明	SAML 設定の説明
前回のログイン	インスタンス上のユーザーが SAML 設定を使って最後に正常にログインした日時 **注意:** Tenable Vulnerability Management に SAML アイデンティティプロバイダーのログインデータがある場合にのみ、[**Last Login**] 列に値が表示されます。
前回のログイン試行	インスタンス上のユーザーが最後に SAML 設定を介してログインを試行した日時 **注意:** Tenable Vulnerability Management に SAML アイデンティティプロバイダーの試行ログインデータがある場合にのみ、[**前回のログイン試行**] 列に値が表示されます。

証明書	SAML 設定の証明書 証明書の列で、次のタスクを実行できます。 • ボタンをクリックすると、証明書がクリップボードにコピーされます。 • ボタンにカーソルを合わせると、証明書の有効期限日が表示されます。 **注意:** アイデンティティプロバイダーが証明書の有効期限を決定します。
アクション	当該設定の 1 つ以上のセキュリティ証明書を含む metadata.xml ファイルをダウンロードできる、インタラクティブな列 metadata.xml ファイルをダウンロードする方法 1. metadata.xml ファイルをダウンロードする設定の **[アクション]** 列で、⋮ ボタンをクリックします。 オプションメニューが表示されます。 2. メニューで、⭳ **[SP メタデータのダウンロード]** をクリックします。 Tenable Vulnerability Management で metadata.xml ファイルがコンピューターにダウンロードされます。

SAML 設定の追加

必要なユーザーロール: 管理者

SAML 設定の詳細を手動で入力するか、ID プロバイダー (IdP) からダウンロードした metadata.xml ファイルをアップロードできます。

注意: ユーザーの SAML が設定されたら、ユーザーが IdP タイルまたは SP メタデータファイルで提供されている URL (cloud.tenable.com/SAML/XXXXXX など) を使用してログインし、ログアウトしてから、Tenable Vulnerability Management ログインページの **[SSO 経由のサインイン]** リンクにアクセスできるようになります。

始める前に

Tenable Vulnerability Management で使用するために SAML を設定する方法については、Tenable SAML 設定クイックリファレンスガイドにある手順を確認してください。この大まかな手順は、次のとおりです。

- IdP のドキュメントで説明されている手順に従って、IdP アカウントで Tenable Vulnerability Management 用に SAML アプリケーションを設定します。SAML アプリケーションを設定するには、IdP で Tenable Vulnerability Management 用にエンティティ ID と応答 URL が必要です。
  - エンティティ ID/オーディエンス URI - `TENABLE_IO_PLACEHOLDER`
  - ACS/SSO URL/ログイン URL/応答 URL— `https://cloud.tenable.com/SAML/login/placeholder.com`。
- IdP アカウントで、metadata.xml ファイルをダウンロードします。

注意: Tenable は現在、SP が開始する SAML フローをサポートしていません。アイデンティティサービスプロバイダー側から起動する必要があるため、https://cloud.tenable.com に直接移動しても SSO は許可されません。

重要! すべてのユーザーは SSO ログインに一致するアカウントを Tenable Vulnerability Management に設定しておく必要があります。SSO ログインが完全な Tenable アカウント名 (例: user@tenable.com) と一致することを確認する必要があります。

新しい SAML 設定を追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

   [SAML] ページが表示されます。

4. アクションバーで、⊕ **[作成]** をクリックします。

   [SAML 設定] ページが表示されます。

5. 次のいずれかを行います。

IdP の metadata.xml ファイルをアップロードして設定の詳細を入力する方法

a. 最初のドロップダウンボックスで、**[XML のインポート]** を選択します。

> **注意:** デフォルトでは、**[XML のインポート]** が選択されています。

b. **タイプ**ドロップダウンボックスは、使用しているアイデンティティプロバイダーのタイプを指定します。Tenable Vulnerability Management は SAML 2.0 をサポートしています (例: Okta、OneLogin など)。
このオプションは読み取り専用です。

c. **[インポート]** で、**[ファイルの追加]** をクリックします。

   ファイルマネージャーウィンドウが表示されます。

d. metadata.xml ファイルを選択します。

   metadata.xml ファイルがアップロードされます。

IdP の metadata.xml ファイルのデータを使用して SAML 設定を手動で作成する方法

a. 最初のドロップダウンボックスで、**[手動入力]** を選択します。

   SAML 設定フォームが表示されます。

b. 次の表にある設定を設定します。

設定	説明
[有効化]トグル	SAML 設定が有効か無効かを示す、右上にあるトグル。 デフォルトでは、**[有効化]**設定は**[有効]**に設定されています。トグルをクリックして、SAML 設定を無効にします。
タイプ	使用しているアイデンティティプロバイダーのタイプを指定します。Tenable Vulnerability Management は SAML 2.0 をサポートしています(例:Okta、OneLogin など)。 このオプションは読み取り専用です。
説明	SAML 設定の説明。
IdP エンティティ ID	IdP が提供する一意のエンティティ ID です。 **注意:** ユーザーアカウントに複数の IdP を設定する場合は、アイデンティティプロバイダーごとに新しい設定を作成します。つまり、アイデンティティプロバイダーの URL、エンティティ ID、署名証明書を個別に設定します。
IdP URL	IdP の SAML URL です。
証明書	IdP セキュリティ証明書です。 **注意:** セキュリティ証明書は、アイデンティティプロバイダーが提供する metadata.xml ファイルにあります。ファイルの内容をコピーして、**[証明書]**ボックスに貼り付けることができます。
ユーザー自動プロビジョニングが有効にされています	ユーザーアカウントの自動作成が有効か無効かを示すトグル。
IdP はプロビ	プロビジョニング中にユーザーロールを割り当てるには、このトグルを有効化します。SAML ID プロバイダーで、属性名に **userRoleUuid** を、属性

ジョニング時にユーザーロールを割り当てる	値にユーザーロール UUID を指定した属性ステートメントを追加します。 ユーザーロールの UUID を取得するには、**[設定]** > **[アクセス制御]** > **[ロール]** に移動します。
IdP はログインごとにユーザーロールをリセットする	ユーザーがログインするたびにロールを割り当て、現在のロールを IdP で選択したロールで上書きするには、このトグルを有効化します。SAML ID プロバイダーで、属性名に **userRoleUuid** を、属性値にユーザーロール UUID を指定した属性ステートメントを追加します。 ユーザーロールの UUID を取得するには、**[設定]** > **[アクセス制御]** > **[ロール]** に移動します。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management で SAML 設定が保存されます。

次の手順

- [SAML 設定] 表の ⭳ **[SP メタデータのダウンロード]** オプションを使用して、Tenable Vulnerability Management から metadata.xml をダウンロードします。
- SAML プロバイダーで Tenable Vulnerability Management 用に作成した SAML アプリケーションにこのファイルをアップロードします。

ヒント: SAML 設定中に問題が発生した場合、Tenable は、オンラインで入手できるさまざまなサードパーティ製 SAML デバッグツールのいずれかを試すことをお勧めします。トラブルシューティングのサポートについては、Tenable サポート にお問い合わせいただくこともできます。

SAML 設定の編集

必要なユーザーロール: 管理者

SAML 設定は **[SAML]** ページで編集できます。

SAML 設定を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

   [SAML] ページが表示されます。

4. SAML 表で、編集する SAML 設定をクリックします。

   [SAML 設定] ページが表示されます。

5. (オプション) 最初のドロップダウンボックスで、基本的な設定の詳細を提供する別の方法を選択します。

   - **XML をインポート** - 新しい SAML 設定の追加で説明されているように、IdP から提供されたメタデータファイルをアップロードして、SAML 認証を設定します。
   - **手動入力** - 新しい SAML 設定の追加で説明されているように、IdP から提供された metadata.xml ファイルのデータを使用して SAML オプションを手動で設定し、SAML 認証を設定します。

     Tenable Vulnerability Management は選択されたソースに基づいて設定オプションを更新します。

6. 次の表に示す設定可能な SAML 設定のいずれかを更新します。

   注意: 一部の設定は読み取り専用になっており、変更できません。

   注意: 更新できる設定オプションは、最初のドロップダウンボックスで選択したソースによって異なります。

設定	ソース	説明
[有効化] トグル	**手動入力**	SAML 設定が有効か無効かを示します。 デフォルトでは、**[有効化]** 設定は **[有効]** に設定されています。右上のトグルをクリックして、SAML 設定を無効にします。
タイプ	**手動入力**、**XML のインポート**	使用しているアイデンティティプロバイダーのタイプを指定します。Tenable Vulnerability Management は SAML 2.0 をサポートしています。(例: Okta、OneLogin など)
UUID	**入力**、**XML のインポート**	新しい SAML 設定を作成すると、Tenable Vulnerability Management によって自動的に生成されるアイデンティティの一意の識別子 このボックスは読み取り専用です。
URL	**手動入力**、**XML のインポート**	設定を作成すると、Tenable Vulnerability Management によって生成されるログイン URL このボックスは読み取り専用です。
Entity ID	**手動入力**、**XML のインポート**	設定を作成すると、Tenable Vulnerability Management によって生成される一意の識別子 このボックスは読み取り専用です。
作成日	**手動入力**、**XML のインポート**	管理者ユーザーが設定を作成した日時 このボックスは読み取り専用です。

最終更新日	**手動入力、XML のインポート**	管理者ユーザーが最後に設定を更新した日時 このボックスは読み取り専用です。
説明	**手動入力**	SAML 設定の説明
IdP エンティティ ID	**手動入力**	ID プロバイダーの一意のエンティティ ID **注意:** ユーザーアカウントに複数の IdP を設定する場合は、アイデンティティプロバイダーごとに新しい設定を作成します。つまり、アイデンティティプロバイダーの URL、エンティティ ID、署名証明書を個別に設定します。
IdP URL	**手動入力**	ID プロバイダーの SAML URL
証明書	**手動入力**	1 つまたは複数のアイデンティティプロバイダーのセキュリティ証明書 **注意:** セキュリティ証明書は、アイデンティティプロバイダーが提供する metadata.xml ファイルにあります。ファイルの内容をコピーして、**[証明書]** ボックスに貼り付けることができます。
ユーザー自動プロビジョニングの有効化	**手動入力**	アカウントユーザーの自動作成が有効か無効かを示すトグル
IdP はプロビジョニング時にユーザーロールを割り当てる	**手動入力**	プロビジョニング中にユーザーロールを割り当てるには、このトグルを有効化します。SAML ID プロバイダーで、属性名に **userRoleUuid** を、属性値にユーザーロール UUID を指定した属性ステートメントを追加します。 ユーザーロールの UUID を取得するには、**[設定]** > **[アクセス制御]** > **[ロール]** に移動します。

IdP はログインごとにユーザーロールをリセットする	**手動入力**	ユーザーがログインするたびにロールを割り当て、現在のロールを IdP で選択したロールで上書きするには、このトグルを有効化します。SAML ID プロバイダーで、属性名に **userRoleUuid** を、属性値にユーザーロール UUID を指定した属性ステートメントを追加します。 ユーザーロールの UUID を取得するには、**[設定]** > **[アクセス制御]** > **[ロール]** に移動します。
インポート	**XML のインポート**	1 つ以上の SAML 証明書を含む、アイデンティティプロバイダーからの metadata.xml ファイルです。 アイデンティティプロバイダーから新しい metadata.xml ファイルをインポートする方法 a. **[インポート]** で、**[ファイルの追加]** をクリックします。 ファイルエクスプローラーウィンドウが表示されます。 b. metadata.xml ファイルを選択します。 metadata.xml ファイルがアップロードされます。 **注意:** metadata.xml ファイルに複数の証明書が含まれている場合、**[SAML]** ページの設定の **[証明書]** 列には最初の証明書のみが表示されます。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management が設定を保存します。

   [SAML] ページが、更新された設定で表示されます。

SAML 設定の無効化

必要なユーザーロール: 管理者

SAML 設定を無効にすると、インスタンス上のユーザーがその設定の SAML 認証情報を使用して Tenable Vulnerability Management にログインできなくなります。SAML 設定の有効化の説明に従って、無効になっている SAML 設定を有効にできます。

注意: SAML 設定を無効にすると、ユーザーは SAML 認証情報を使用して Tenable Vulnerability Management にログインできなくなります。SAML 設定を無効にする前に、インスタンス上のすべてのユーザーが別の方法で Tenable Vulnerability Management にログインできることを確認してください。

SAML 設定を無効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

   [SAML] ページが表示されます。

4. SAML 表で、無効にする SAML 設定をクリックします。

   [SAML 設定] ページが表示されます。

5. ページの下部で、**[SAML の有効化]** トグルをクリックして設定を無効にします。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management が SAML 設定を無効にします。**[SAML]** ページで、無効になっている設定が薄いグレーで表示されます。

SAML 設定の有効化

必要なユーザーロール: 管理者

無効になっている SAML 設定を有効にできます。Tenable Vulnerability Management での SAML 認証の詳細については、SAML を参照してください。

ヒント: Tenable Vulnerability Management で使用するために SAML を設定する方法については、Tenable SAML 設定クイックリファレンスガイドにある手順を確認してください。

注意: ユーザーの SAML が設定されたら、ユーザーが IdP タイルまたは SP メタデータファイルで提供されている URL (cloud.tenable.com/SAML/XXXXXX など) を使用してログインし、ログアウトしてから、Tenable Vulnerability Management ログインページの **[SSO 経由のサインイン]** リンクにアクセスできるようになります。

始める前に:

Tenable Vulnerability Management で認証するように IdP を設定します。詳細は、Tenable SAML 設定クイックリファレンスガイドを参照してください。

SAML 設定を有効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

   [SAML] ページが表示されます。

4. SAML 表で、有効にする SAML 設定をクリックします。

   ヒント: 無効になっている設定は薄いグレーで表示されます。

   [SAML 設定] ページが表示されます。

5. ページの下部で、**[SAML の有効化]** トグルをクリックして設定を有効にします。

6. **[保存]** をクリックします。

Tenable Vulnerability Management が SAML 設定を有効にします。**[SAML]** ページで、有効になっている設定が黒色で表示されます。

自動アカウントプロビジョニングを有効にする

必要なユーザーロール: 管理者

SAML 設定を手動で設定または編集する場合、ユーザーアカウントの自動プロビジョニングを有効にできます。自動アカウントプロビジョニングを使用すると、SAML 設定で名前が付けられた IdP の認証情報を持つユーザーは、IdP 経由で初めてログインする際に Tenable Vulnerability Management アカウントを作成できます。

ヒント: Tenable Vulnerability Management で使用するために SAML を設定する方法については、Tenable SAML 設定クイックリファレンスガイドにある手順を確認してください。

Tenable Vulnerability Management は、次のデフォルト設定を使用して、自動的にプロビジョニングされるアカウントを作成します。

- **氏名** - NameID
- **ユーザー名** - NameID
- **E メール** - NameID
- **ユーザーロール** - 基本

現在、Tenable Vulnerability Management ではその他の要求の種類はサポートされていません。

始める前に:

Tenable Vulnerability Management で認証するように IdP を設定します。詳細は、Tenable SAML 設定クイックリファレンスガイドを参照してください。

ユーザーアカウントの自動プロビジョニングを有効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

[SAML] ページが表示されます。

4. SAML 表で、自動アカウントプロビジョニングを有効にする SAML 設定をクリックします。

   [SAML 設定] ページが表示されます。

5. ページの下部で、**[ユーザー自動プロビジョニングの有効化]** トグルをクリックして、自動アカウントプロビジョニングを有効にします。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management は、SAML 設定で自動アカウントプロビジョニングを有効にします。

自動アカウントプロビジョニングを無効にする

必要なユーザーロール: 管理者

自動アカウントプロビジョニングを無効にすると、ユーザーが IdP 経由で最初にプラットフォームにアクセスしたときに Tenable Vulnerability Management アカウントが自動作成されません。自動アカウントプロビジョニングを有効にするの説明に従って、SAML 設定で自動アカウントプロビジョニングを有効にすることができます。

ユーザーアカウントの自動プロビジョニングを無効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

   [SAML] ページが表示されます。

4. SAML 表で、自動アカウントプロビジョニングを無効にする SAML 設定をクリックします。

5. **[SAML 設定]** ページが表示されます。

6. ページの下部で、**[ユーザー自動プロビジョニングの有効化]** トグルをクリックして、自動アカウントプロビジョニングを無効にします。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management は、SAML 設定で自動アカウントプロビジョニングを無効にします。

SAML 設定の削除

必要なユーザーロール: 管理者

SAML 設定は[**SAML**]ページで削除できます。Tenable Vulnerability Management での SAML 認証の詳細については、SAML を参照してください。

SAML 設定を有効にする方法

始める前に

- 削除する SAML 設定を無効にします。

SAML 設定を削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[SAML]** タイルをクリックします。

   [SAML] ページが表示されます。

4. SAML 表で、削除する SAML 設定のチェックボックスをオンにします。

5. アクションバーで、🗑 **[削除]** ボタンをクリックします。

   Tenable Vulnerability Management で SAML 設定が削除されます。

   注意： SAML 設定を削除する際は、IdP の関連する設定も必ず削除してください。

次の手順

- アイデンティティプロバイダーのアプリケーションから関連する設定を削除します。

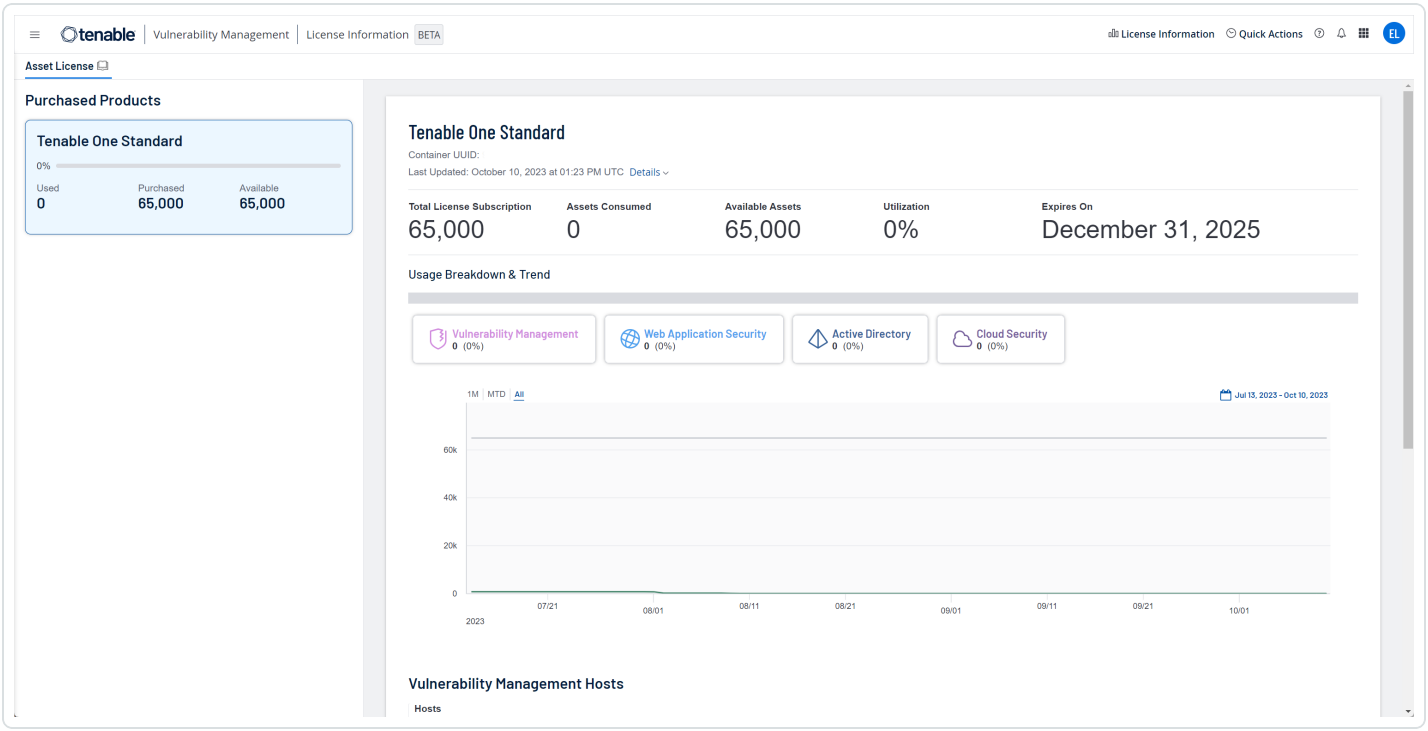
ライセンス情報

[ライセンス情報] ページでは、Tenable 製品とそのライセンスの使用状況の内訳を確認することができます。この情報は、製品別または期間別にビジュアル化された概要など、複数の方法で表示することができます。これにより、一時的な使用量の急増や製品の設定ミスなどの傾向を特定することができます。

ヒント: **[ライセンス情報]** ページに表示される各製品の Tenable ライセンスの仕組みについては、Tenable 製品のライセンスを参照してください。ライセンス超過についての詳細は、Tenable Cloud Overage Process (Tenable クラウドライセンス超過プロセス) を参照してください。

[ライセンス情報] ページの表示

[ライセンス情報] ページを表示するには、上部のナビゲーションバーから **[ライセンス情報]** をクリックします。



[ライセンス情報] ページには、現在の Tenable コンテナにある全製品のライセンス使用状況が表示され、次のセクションがあります。

セクション	説明
購入済みの製	左側で、製品タイルをクリックして詳細を表示します。製品が評価中または期

品	限切れの場合は、ラベルが表示されます。 • **使用中** - 製品サブスクリプションで使用または評価されたライセンスの総数。 • **購入済み** - その製品で購入したライセンスの数。 • **使用可能** - サブスクリプションで利用可能な、まだ評価されていない残りのライセンスの数。
製品のサマリー	ページの上部に、選択した製品のサマリーを表示します。 • **製品名** - 製品の名前。 • **コンテナ UUID** - コンテナの一意の ID。 • **最終更新日** - 製品が最後に更新された日時。 • **サイト名** - Tenable のクラウドにインストールされている製品を含むクラスター。 • **リージョン** - クラスターが配置されている地域。 • **プラグインセット** - 製品の Nessus プラグインセットのバージョン。 • **プラグインの更新** - Nessus プラグインセットが最後に更新された日時。 • **合計ライセンスサブスクリプション** - 製品サブスクリプションの一部として購入したライセンスの総数。 • **消費された資産** - 製品サブスクリプションで使用または評価されたライセンスの総数。 • **利用可能な資産** - サブスクリプションで利用可能な、まだ評価されていない残りのライセンスの数。 • **使用率** - 使用済みのライセンスの割合。この値は、消費されたライセンス数を合計ライセンスサブスクリプション数で割って計算されます。 • **有効期限日** - Tenable サブスクリプションが期限切れとなる日付。
使用率の内訳と傾向	資産の使用率の内訳を視覚的に表示します。 • **棒グラフ** - (Tenable One のみ) Tenable One コンポーネント別の合計ライ

	センス使用量を棒グラフで表示します。 **注意**: Tenable Cloud Security の新しいバージョンがある場合、ライセンスのある資産の数は、**計算**、**サーバーレス**、**コンテナリポジトリ**の資産に比率を乗算し、**コンテナイメージ** (Tenable Container Security がある場合) を加算して算出されます。所属組織に比率がある場合は、**[クラウドセキュリティ]** セクションの **[ライセンス比率]** フィールドに表示されます。ご利用のクラウドリソースに Tenable が適用する場合がある比率については、Tenable の担当者にお問い合わせください。 • **使用量の推移** - ライセンスの使用量の推移を折れ線グラフで表示します。X 軸は期間、Y 軸は使用された資産の数です。グラフの上部にあるフィルターを使用して、左側で期間を切り替えるか、右側でカスタムの日付範囲を指定します。 **ヒント**: (Tenable One のみ) グラフの上のタイルをクリックして、製品を選択または選択解除できます。
脆弱性管理ホスト	ライセンスとしてカウントされる Tenable Vulnerability Management 資産の数を表示します。 • **ホスト** - ライセンスとしてカウントされるホストの数。
クラウドセキュリティリソース	Tenable Cloud Security によって特定された環境内のクラウドリソースの数を表示します。 **注意**: Tenable Cloud Security には 2 つのバージョンがあります。最新バージョンの場合、ライセンスのあるクラウド資産の数は、**[計算]**、**[サーバーレス]**、**[コンテナリポジトリ]** の各フィールドに表示され、Tenable Container Security の場合には **[コンテナイメージ]** フィールドにも表示されます。ライセンスのあるクラウド資産の*合計*を表示するには、**使用率の内訳と傾向** セクションを参照してください。 • **ライセンス比率** – (新規バージョンのみ) **コンピューティング**、**サーバーレス**、および**コンテナリポジトリ**のリソースに適用される任意の比率。たとえば、企業の比率が 3 である場合、10 コンピューティングリソースは 30 の *ライセンス取得済みの* Tenable 資産に等しくなります。クラウドリソースに適用される比率 Tenable に関する詳細については、Tenable の担当者にお問い合わせください。

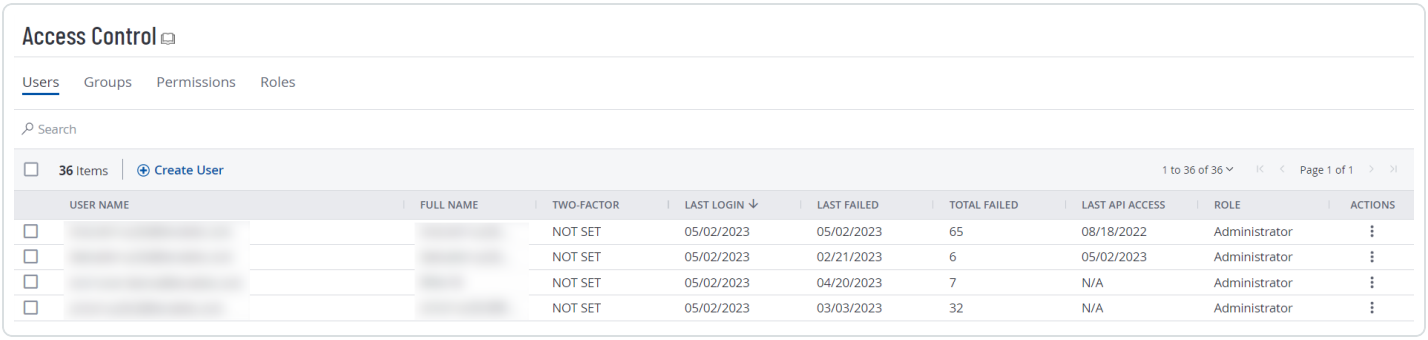
	• **コンピューティング** – (新規バージョンのみ) AWS EC2 インスタンスや Azure 仮想マシンなどのクラウドコンピューティングリソース。このフィールドにカーソルを合わせると、*請求可能な*リソース、または比率が適用される前のリソースの合計数が表示されます。 • **サーバーレス** – (新規バージョンのみ) AWS Lambda や Azure Functions などのクラウドサーバーレスリソース。このフィールドにカーソルを合わせると、*請求可能な*リソース、または比率が適用される前のリソースの合計数が表示されます。 • **コンテナリポジトリ** – (新規バージョンのみ) Tenable Cloud Security によってスキャンされたクラウドコンテナリポジトリ。このフィールドにカーソルを合わせると、*請求可能な*リソース、または比率が適用される前のリソースの合計数が表示されます。 • **コンテナイメージ (レガシーのコンテナセキュリティ)** – ライセンスとしてカウントされるパッケージ化されたアプリケーションの数。Tenable Container Security をお持ちの場合にのみ使用されます。 • **請求可能** - (レガシーのみ) ライセンスがあると見なされるクラウド資産のサブセット。通常は過去 90 日間にスキャンされたクラウドコンピューティング、ストレージ、ネットワークリソースです。 **ヒント:** Tenable Cloud Security の新しいバージョンを使用している場合、これらの資産はライセンスに対してカウントされません。 • **請求不可能** - (レガシーのみ) リポジトリまたはパイプライン内でローカルにスキャンされた、インフラのコード化 (IaC) 資産。これらは、ライセンスがあるとは見なされません。
Web App Scanning FQDN	ライセンスとしてカウントされる Tenable Web App Scanning リソースの数を表示します。 • **FQDN** - ライセンスとしてカウントされる完全修飾ドメイン名の数。 **注意**: Tenable Web App Scanning は、ユーザーアカウントでスキャンされる*完全修飾ドメイン名* (FQDN) の数によって資産カウントを決定します。脆弱性のスキャンが正常に終わるまで、資産はライセンスの制限数に対してカウントされません。

Attack Surface Management 資産	Tenable Attack Surface Management リソースを表示します。 • **観察可能オブジェクト** - Tenable Attack Surface Management で検出され、インベントリに追加された資産の数。 **注意**: Tenable One Standard のお客様の場合、これらのリソースは資産ライセンスとしてカウントされません。
Active Directory ユーザー	ライセンスとしてカウントされる Tenable Identity Exposure リソースの数を表示します。 • **ユーザー** - 有効なアクティブユーザーの数。

アクセス制御

必要なユーザーロール: 管理者

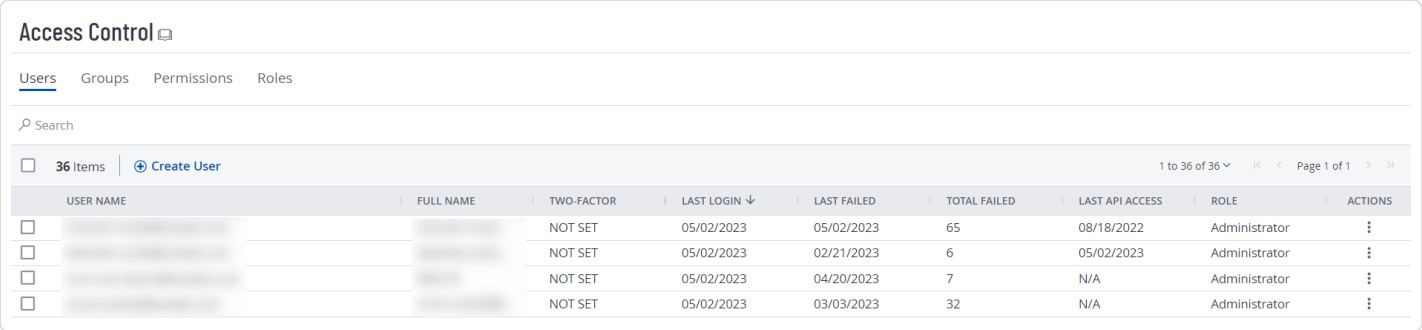
[アクセス制御] ページから、アカウントのユーザーとグループのリスト、およびそれらに割り当てられたアクセス許可を表示および設定できます。



ユーザー

このセクション内のトピックは、Tenable Vulnerability Management の主な機能強化の機能更新を反映するように変更されています。詳細は、Tenable Vulnerability Management Key Enhancements を参照してください。

アクセス制御 ページの **[ユーザー]** タブで、管理者ユーザーは Tenable Vulnerability Management の組織のリソース用のユーザーアカウントを作成して管理できます。



ユーザーの表

列	説明
名前	アカウントのユーザー名
氏名	ユーザーのフルネーム
前回のログイン	ユーザーが最後に Tenable Vulnerability Management インターフェースに正常にログインした日付
Last Failed	ユーザーが最後に Tenable Vulnerability Management インターフェースへのログインに失敗した日付
Total Failed	ユーザーがログイン試行に失敗した合計回数 この数字は、管理者またはユーザーがユーザーアカウントのパスワードをリセットしたときにリセットされます。
Last API Access	ユーザーが最後に API キーを生成した日付
ロール	ユーザーに割り当てられたロール詳細は、ロールを参照してください。

アクション	管理者ユーザーがユーザーに対して実行できるアクション(ユーザーのエクスポートなど)

[ユーザー] ページでは、次のアクションを実行できます。

- ユーザーアカウントの作成
- ユーザーリストの表示
- ユーザーアカウントの編集
- 別のユーザーのパスワードの変更
- 各自のアカウントでユーザーをサポートする
- 別のユーザーの API キーを生成する
- ユーザーアカウントのロックの解除
- ユーザーアカウントの無効化
- ユーザーアカウントの有効化
- ユーザーアクセス認証情報の管理
- ユーザーアクティビティの監査
- ユーザーをエクスポートする
- Delete a User Account

ユーザーアカウントを作成する

必要なユーザーロール: 管理者

[ユーザー] ページで、新しいユーザーのアカウントを作成できます。

ヒント: SAML IdP によるアカウントの作成については、SAML のドキュメントを参照してください。

注意: ユーザーアカウントの有効期限は、そのアカウントが属する Tenable Vulnerability Management コンテナの作成日に基づいて設定されます。Tenable は、この設定を直接制御します。詳細については、Tenable サポートにお問い合わせください。

ユーザーアカウントを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

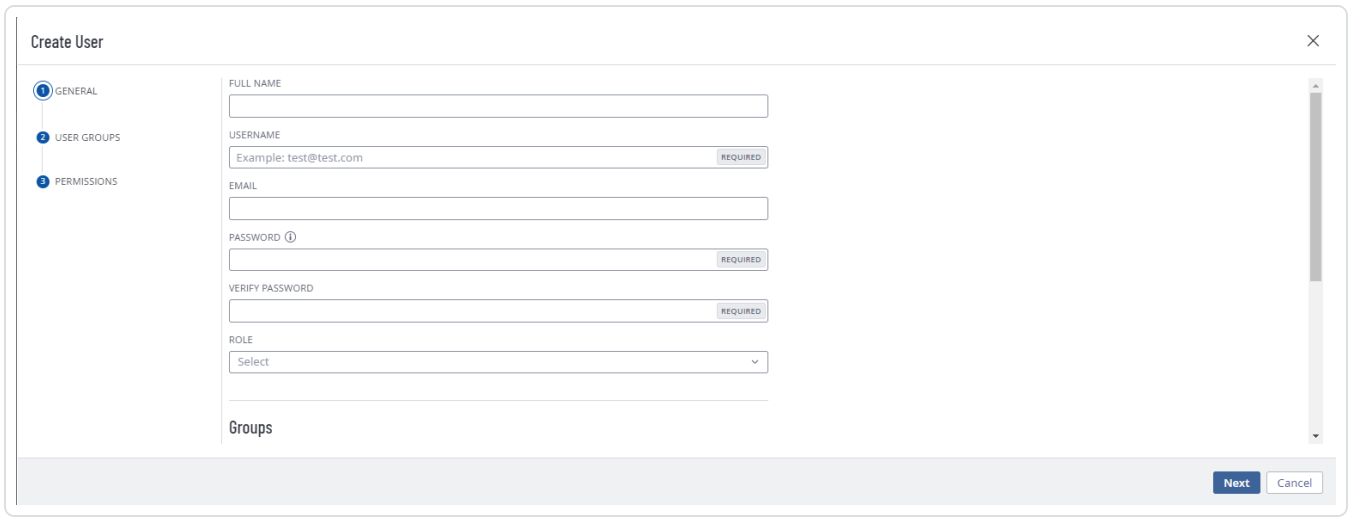
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ⊕ **[ユーザーの作成]** ボタンをクリックします。

   [ユーザーの作成] ページが表示されます。



5. 次のオプションを設定します。

注意: 各セクションのオプションを表示して設定するには、左側のメニューでセクションを選択する必要があります。

オプション	アクション
[一般] セクション	
氏名	ユーザーの氏名を入力します。
ユーザー名	有効なユーザー名を入力します。 有効なユーザー名は、次の形式である必要があります。 *name@domain* ここで、*domain* はお使いの Tenable Vulnerability Management インスタンス用に承認されたドメインに対応します。 **注意:** 初期設定の間に、Tenable は Tenable Vulnerability Management インスタンス用に承認されたドメインを設定します。インスタンスにドメインを追加する方法については、Tenable の担当者にお問い合わせください。 **注意:** Tenable Vulnerability Management のユーザー名に

	次の文字を含めることはできません: '、！ 、# 、$、%、^、&、*、(、)、/、\、|、{、}、[、]、"、:、;、 ~、`、<、>、,
メール	有効なメールアドレスを *name@domein* の形式で入力します。この *domain* は、お使いの Tenable Vulnerability Management インスタンスで承認されたドメインになります。 このメールアドレスは、**[ユーザー名]** ボックスに設定されたメールアドレスをオーバーライドします。このオプションを空のままにすると、Tenable Vulnerability Management は **[ユーザー名]** の値を、ユーザーのメールアドレスとして使用します。 **注意:** 管理者は、承認されていないドメインのメールアドレスでユーザーアカウントを作成できます。ユーザーアカウントの作成後は、メールアドレスを別の承認されたドメインにのみ変更できます。
パスワード	有効なパスワードを入力します。詳細については、パスワード要件を参照してください。 Tenable Web App Scanning では、パスワードは最低 12 文字の長さで、次のものを含む必要があります。 • 大文字 • 小文字 • 数字 • 特殊文字
パスワードの確認	パスワードをもう一度入力します。
ロール	ドロップダウンボックスで、ユーザーに割り当てるロールを選択します。

認証	利用可能なセキュリティ設定オプションを選択または選択解除します。選択する場合、以下の設定があります。 **注意:** カスタムロールのあるユーザーに対して**パスワードアクセス**または**SAML**オプションを有効にすると、そのユーザーは自動的にダッシュボードおよびウィジェットへの基本的なアクセス権を持ちます。 • **API キー** - ユーザーがAPIキーを生成することを許可します。 **ヒント:** この設定だけを選択して、APIのみのユーザーアカウントを作成できます。 • **SAML** - ユーザーがSAMLシングルサインオン(SSO)を使用してアカウントにログインできるようにします。詳細は、SAMLを参照してください。 • **ユーザー名 / パスワード** - ユーザーがパスワードを使用してアカウントにログインできるようにします。 **注意:** このオプションの選択を解除すると、MFAオプションを選択できません。 • **二要素が必要です** - ユーザーが自分のアカウントにログインするには二要素認証の入力が必要です。 **ヒント:** マイアカウントページで、自分のアカウントに二要素認証を設定できます。
[ユーザーグループ] セクション	
ユーザーグループ	ユーザーの割当先となる1つまたは複数のユーザーグループを選択します。 デフォルトでは、新しいユーザーはシステム生成の**[すべて**

	のユーザー] ユーザーグループに属し、これによって **[基本]** ロールが割り当てられます。 次の手順でユーザーグループを追加します。 • **[ユーザーグループ]** ボックスの任意の場所をクリックします。 検索ボックスとロールのドロップダウンリストが表示されます。 • (オプション) **[検索]** ボックスに、ユーザーグループ名を入力します。 入力すると、検索条件に一致するユーザーグループのリストが表示されます。 • 追加するユーザーグループをクリックします。 **[ユーザーグループ]** ボックスに、Tenable Vulnerability Management によってユーザーグループを表すラベルが追加されます。 • これらの手順を繰り返して、別のユーザーグループにユーザーを追加します。
[アクセス許可] セクション	
アクセス許可	**[アクセス許可]** の表で、ユーザーに割り当てるアクセス許可設定を選択します。

6. **[保存]** をクリックします。

> **注意:** ユーザーにアクセス許可を割り当てると、ボタンは **[追加して保存]** と表示されます。

Tenable Vulnerability Management によって新しいユーザーアカウントが一覧表示されます。

ユーザーアカウントの編集

必要なユーザーロール: 管理者

ユーザーアカウントを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、編集するユーザーの名前をクリックします。

   [ユーザーの編集] ページが表示されます。

5. 次のオプションを設定します。

オプション	アクション
アカウント設定	
Full Name	ユーザーの氏名を編集します。
ユーザー名	このオプションは編集できません。
メール	有効なメールアドレスを *name@domein* の形式で入力します。この *domain* は、お使いの Tenable Vulnerability Management インスタンスで承認されたドメインになります。 このメールアドレスは、**[ユーザー名]** ボックスに設定されたメールアドレスをオーバーライドします。このオプションを空のままにすると、Tenable Vulnerability Management は **[ユーザー名]** の値を、ユーザーのメールアドレスとして使用します。

	注意: 管理者は、承認されていないドメインのメールアドレスでユーザーアカウントを作成できます。ユーザーアカウントの作成後は、メールアドレスを別の承認されたドメインにのみ変更できます。
新しいパスワード	有効なパスワードを入力します。詳細については、パスワード要件を参照してください。 Tenable Web App Scanning では、パスワードは最低 12 文字の長さで、次のものを含む必要があります。 • 大文字 • 小文字 • 数字 • 特殊文字
ロール	ドロップダウンボックスから、ユーザーに割り当てるロールを選択します。
グループ	
User Groups	ユーザーを割り当てる 1 つまたは複数のユーザーグループを選択します。ユーザーは、そのユーザーグループに関連付けられているロールとアクセス許可を継承します。
セキュリティ設定	利用可能なセキュリティ設定オプションを選択または選択解除します。選択する場合、以下の設定があります。 • **API** - ユーザーが API キーを生成することを許可します。 **ヒント:** この設定だけを選択して、API のみのユーザーアカウントを作成できます。 • **SAML** - ユーザーが SAML シングルサインオン (SSO) を使用してアカウントにログインできるようにします。詳細は、SAML を参照してください。 • **Password Access** - ユーザーがパスワードを使用してアカウントにログインできるようにします。

	注意: このオプションの選択を解除すると、MFA オプションを選択できません。 • **MFA** - ユーザーが自分のアカウントにログインするためには二要素認証の入力が必要です。 **ヒント:** My Accountページで、自分のアカウントに二要素認証を設定できます。

6. (オプション) ユーザーの API キーを生成します
7. **[保存]** をクリックします。

   Tenable Vulnerability Management はアカウントへの変更を保存します。

ユーザーリストの表示

必要なユーザーロール: 管理者

アクセス制御ページの **[ユーザー]** タブで、Tenable Vulnerability Management インスタンス上のすべてのユーザーのリストを表示できます。

Tenable Vulnerability Management インスタンスのユーザーとユーザーデータを表示する方法

1. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

2. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

3. **[ユーザー]** タブをクリックします。

   [ユーザー] タブが開き、Tenable Vulnerability Management インスタンス上のすべての Tenable Vulnerability Management ユーザーアカウントの表が表示されます。このドキュメントでは、この表を *ユーザー表* と呼びます。

ユーザー表

ユーザー表で、Tenable Vulnerability Management インスタンス上のユーザーに関する以下の情報を表示できます。

列	説明
名前	アカウントのユーザー名
前回のログイン	ユーザーが最後に Tenable Vulnerability Management インターフェースに正常にログインした日付
Last Failed	ユーザーが最後に Tenable Vulnerability Management インターフェースへのログインに失敗した日付
Total Failed	ユーザーがログイン試行に失敗した合計回数 この数字は、管理者またはユーザーがユーザーアカウントのパスワードをリセットした

	ときにリセットされます。
Last API Access	ユーザーが最後に API キーを生成した日付
ロール	ユーザーに割り当てられたロール詳細は、ロールを参照してください。
アクション	管理者ユーザーがユーザーに関して実行できるアクション (ユーザーのエクスポートなど)

Tenable Vulnerability Management のパスワード要件

Tenable Vulnerability Management はすべてのアカウントに対し、次のパスワード要件を適用します。

パスワード基準

パスワードは最低 12 文字の長さで、次のものを含む必要があります。

- 大文字
- 小文字
- 数字
- 特殊文字

パスワードの有効期限

Tenable Vulnerability Management のパスワードに有効期限はありません。

アカウントのロックアウト

デフォルトでは、ログイン試行が 5 回失敗すると、Tenable Vulnerability Management はユーザーをアカウントからロックアウトします。ユーザーが自分のアカウントからロックアウトされた場合、ユーザー自身が自分のアカウントのロックを解除するか、管理者がパスワードをリセットします。

パスワード履歴

現在のパスワードや以前のパスワードを再利用することはできません。

別のユーザーのパスワードの変更

必要なユーザーロール: 管理者

別のユーザーアカウントのパスワードを変更するには、管理者の権限が必要です。自分自身のパスワードを変更するには、パスワードを変更するを参照してください。

別のユーザーのパスワードを変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、編集するユーザーの名前をクリックします。

   [ユーザーの編集] ページが表示されます。

5. **[新しいパスワード]** ボックスに新しいパスワードを入力します。詳細については、「パスワード要件」を参照してください。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management は、ユーザーアカウントの新しいパスワードを保存します。

各自のアカウントでユーザーをサポートする

必要なユーザーロール: 管理者

管理者として、ユーザーサポート機能を使用し、別のアカウントとしてログインをシミュレートできます。ユーザーアカウントをサポートする間、そのユーザーのパスワードを取得したり、管理者アカウントからログアウトしたりすることなく、そのユーザーとして Tenable Vulnerability Management で操作できます。

注意: **ユーザーアシスト**は、次の認証設定のいずれかまたは両方が有効になっているユーザーアカウントでのみ使用できます。

- **ユーザー名 / パスワード**
- **SAML**

これらのセキュリティ設定を有効にするには、ユーザーアカウントの編集を参照してください。

各自のアカウントでユーザーをサポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、サポートするユーザーアカウントのチェックボックスをクリックします。

   表の上部にアクションバーが表示されます。

   注意: 一度に選択できるユーザーは 1 人だけです。

5. アクションバーで、👤 ボタンをクリックします。

   Tenable Vulnerability Management により、サポートしているユーザー用のデフォルトのダッシュボードが更新されて表示されます。ユーザーをサポートしている間、Tenable Vulnerability Management の各ページの上部にはサポートしているユーザーのロールを記載したオーバーレイが表示されます。

各自のアカウントでユーザーのサポートを停止する方法

- 任意のページの上部にある、サポート中のユーザーのロールが表示されているオーバーレイで ✕ ボタンをクリックします。

別のユーザーの API キーの生成

必要なユーザーロール: 管理者

お使いのユーザーアカウントに関連付けられた API キーにより、お客様の企業にライセンスされた、すべての Tenable Vulnerability Management 製品の API にアクセスすることが可能になります。これらのキーは、Tenable Vulnerability Management REST API での認証に使用する必要があります。

管理者は、任意のアカウントの API キーを生成できます。他のロールは、自分自身のアカウントの API キーを生成できます。詳細は、Generate API Keysを参照してください。

注意: お使いのユーザーアカウントに関連付けられた API キーを使って、お客様の会社にライセンス付与されているすべての Tenable Vulnerability Management 製品の API にアクセスすることができます。個別の製品に別々のキーを設定することはできません。たとえば、Tenable Vulnerability Management で API キーを生成した場合、この操作により Tenable Web App Scanning および Tenable Container Security の API キーも変更されます。

別のユーザーの API キーを生成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、編集するユーザーの名前をクリックします。

   [ユーザーの編集] ページが表示されます。

5. **[API キー]** セクションで、**[API キーの生成]** をクリックします。

   警告: 新しい API キーを生成すると、既存の API キーはすべて置き換えられます。以前の API キーを使用していたアプリケーションを更新する必要があります。

   警告メッセージが表示されます。

6. 警告を確認し、**[置き換えと生成]**をクリックします。

   [API キーの生成]テキストボックスが表示されます。

   アカウントの新しいアクセスキーと秘密鍵がテキストボックスに表示されます。

7. (オプション)**[API キーの再生成]**をクリックします。

8. 新しいアクセスキーと秘密鍵を安全な場所にコピーします。

   警告:[ユーザーの編集]ページから移動する前に、アクセスキーと秘密鍵を必ずコピーしてください。このページを閉じてしまうと、Tenable Vulnerability Management からキーを取得することはできなくなります。

ユーザーアカウントのロックの解除

Tenable Vulnerability Management でログインを試みて 5 回連続して失敗すると、アカウントがロックされます。

注意: ユーザーは、ユーザーインターフェースからロックアウトされる可能性がありますが、適切な認証 (api_permit) が割り当てられている場合は API リクエストを送信できます。詳細は、Tenable 開発者ポータルを参照してください。

次のいずれかの方法で、ユーザーアカウントのロックを解除できます。

- ユーザーがユーザーアカウントで指定されたメールアドレスにアクセスできる場合、ユーザーは自分のアカウントのロックを解除できます。
- ユーザーが上記メールアドレスにアクセスできない場合、管理者権限を持つ別のユーザーがそのユーザーのパスワードをリセットできます。

ユーザーアカウントの無効化

必要なユーザーロール: 管理者

ユーザーアカウントを無効にすると、ユーザーがログインできなくなり、そのユーザーのスキャンが実行されなくなります。無効のユーザーアカウントを有効にする方法については、ユーザーアカウントの有効化を参照してください。

重要: ユーザーアカウントを無効にしても、そのユーザーに対してスケジュールされたレポートは無効になりません。さらに、無効なユーザーが他のユーザーとレポートを共有した場合、これらの他のユーザーはそのレポートを生成できます。詳細は、レポートを参照してください。

ユーザーアカウントを無効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. 無効にする1人または複数人のユーザーを選択します。

   - 1人のユーザーを選択する場合

     a. で、無効にするユーザーアカウントの行にある ⋮ ボタンをクリックします。

        アクションボタンが行に表示されます。

     b. 行にある ⊘ 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。

   - 複数のユーザーを選択する場合

a. で、無効にする各ユーザーのチェックボックスをクリックします。

ページの下部またはに、アクションバーが表示されます。

b. アクションバーで、⊘ 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。

5. 確認ウィンドウで、**[無効化]** をクリックします。

成功したことを示すメッセージが表示され、

Tenable Vulnerability Management により、選択した 1 人または複数のユーザーが無効になります。で、無効になったユーザーは薄いグレーで表示されます。

> **注意:** 無効にされたユーザーに進行中のセッションがある場合は、引き続き制限付きのアクセス権が付与される場合があります。ただし、ログアウト後は再度ログインできません。

ユーザーアカウントの有効化

必要なユーザーロール: 管理者

ユーザーアカウントを無効にした場合は、アカウントを再度有効にしてユーザーのアクセスを復元できます。

ユーザーアカウントを有効にするには:

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. 有効にする 1 人または複数のユーザーを選択します。

   ### 1 人のユーザーを選択します。

   a. で、有効にするユーザーアカウントの行にある ⋮ ボタンをクリックします。

      アクションボタンが行に表示されます。

      注意: ユーザーが無効になっている場合はグレー表示されます。

   b. 行にある ✓ 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。

   ### 複数のユーザーを選択します。

   a. で、有効にする各ユーザーのチェックボックスをクリックします。

      ページの下部またはに、アクションバーが表示されます。

b. アクションバーで、✓ 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。

5. 確認ウィンドウで、**[有効]** をクリックします。

成功したことを示すメッセージが表示され、

Tenable Vulnerability Management により、選択した 1 人または複数のユーザーが有効になります。ユーザーテーブルで、有効になったユーザーは黒で表示されます。

ユーザーアクセス認証情報の管理

ユーザーは、次の方法を使用して Tenable Vulnerability Managementにアクセスできます。

- ユーザー名とパスワードログイン
- シングルサインオン(SSO)詳細は、SAML を参照してください。
- Tenable Vulnerability Management REST API(API キー使用)詳細は、別のユーザーの API キーの生成 を参照してください。

新規ユーザーを作成すると、すべてのアクセス権がデフォルトで認証されます。企業のセキュリティポリシーに応じて、SSO を強化するためにユーザ名およびパスワードログインを無効化するなど、特定のアクセス方法を無効化できます。

Tenable Vulnerability Management Platform API を使用して、ユーザーのアクセス認証の表示、付与、失効ができます。詳細については、Tenable 開発者ポータルのユーザー認証を取得するおよびユーザー認証を更新するを参照してください。

ユーザーアクティビティの監査

必要なユーザーロール: 管理者

Tenable Vulnerability Management では、監査ログによって企業の Tenable Vulnerability Management アカウントで実行されるユーザーイベントが記録されます。各イベントで、ログには次に関する情報が含まれます。

- 実行されたアクション
- アクションが実施された時期
- ユーザー ID
- ターゲットのエンティティ ID

監査ログは、企業内のユーザーが Tenable Vulnerability Management で行ったアクションに対する可視性をもたらし、セキュリティ上の課題や他の潜在的な問題を特定するのに役立ちます。

企業の Tenable Vulnerability Management アカウントの監査ログを表示する方法

- Tenable 開発者ポータルでの記載内容に従い、**[監査ログ]** エンドポイントを使用します。

ログに記録されるイベント

監査ログイベントには以下が含まれます。

アクション	説明
audit.log.view	システムが監査ログリクエストを受け取り、処理しました。
session.create	システムが、ユーザーに対するセッションを作成しました。このイベントは、ユーザーのログインによってトリガーされます。
session.delete	セッションが期限切れとなったか、またはユーザーがセッションを終了しました。
session.impersonation.end	管理者が、別のユーザーになりすますセッションを終了しました。
session.impersonation.start	管理者が、別のユーザーになりすますセッションを開始しました。

user.authenticate.mfa	二要素認証が成功し、ログインが許可されました。
user.authenticate.password	ユーザーがパスワードを使用してセッションの開始を認証しました。
user.create	管理者が新しいユーザーアカウントを作成しました。
user.delete	管理者がユーザーアカウントを削除しました。
user.impersonation.end	管理者が、他のユーザーへのなりすましを停止しました。
user.impersonation.start	管理者が、他のユーザーへのなりすましを開始しました。
user.logout	ユーザーがセッションからログアウトしました。
user.update	管理者またはユーザーのどちらかが、ユーザーアカウントを更新しました。

ユーザーをエクスポートする

必要なユーザーロール: 管理者

[ユーザー] ページでは、1 人以上のユーザーを CSV または JSON 形式でエクスポートできます。

ユーザーをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ユーザー]** タブをクリックします。

   [ユーザー] ページが表示されます。このページの表には、Tenable Vulnerability Management インスタンスのすべてのユーザーが一覧表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. エクスポートするユーザーを選択します。

エクスポート範囲	アクション
選択したユーザー	選択したユーザーをエクスポートする方法 a. で、エクスポートする各ユーザーのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。

	注意： [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。 200 人以上のユーザーをエクスポートする場合は、リスト内のすべてのユーザーを選択して、[→ **[エクスポート]** をクリックします。
1 人のユーザー	1 人のユーザーをエクスポートする方法 a. で、エクスポートするユーザーの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- ユーザーの表の **[アクション]** 列で、エクスポートするユーザーの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意： デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	ユーザーのリストを含む CSV テキストファイル

	注意: .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたユーザーのリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

ユーザーアカウントを削除する

必要なユーザーロール: 管理者

ユーザーアカウントを削除する前に、ユーザーアカウントを無効にする必要があります。

警告: ユーザーアカウントを削除すると、アカウントを復元することも、操作を元に戻すこともできません。

警告: Tenable Web App Scanning はオブジェクトの移行をサポートしていません。Tenable Web App Scanning ユーザーを削除すると、アプリケーションは削除されたユーザーに属するオブジェクトを再割り当てしません。所有者が削除された場合、Tenable Web App Scanning スキャンを新しい所有者に再割り当てすることはできません。

警告: ユーザーアカウントを削除する前に、関連する修正プロジェクトを割り当て直してください。これらは自動的には再割り当てされません。

次の表に、ユーザーを削除したときにどのオブジェクトが移行、保持、または完全に削除されるかを示します。

オブジェクトタイプ	削除	注記
スキャンの監査ファイル	○	完全に削除
スキャンのスケジュール	×	新しいオブジェクト所有者に移行 **注意:** 移行されたスキャンスケジュールは、完全に削除された他のオブジェクト (監査ファイル、ターゲットグループ、管理されていない認証情報など) に依存している場合は無効になることがあります。
過去のスキャン結果	×	新しいオブジェクト所有者に移行
スキャンテンプレート	×	新しいオブジェクト所有者に移行
スキャンの管理されていな	○	完全に削除

オブジェクトタイプ	削除	注記
い認証情報		
カスタムダッシュボード/ウィジェット	○	完全に削除
認証情報の管理	×	保持 (**[作成者]** 値に **[null]** が表示)
タグ	×	保持 (**[作成者]** 値に **[null]** が表示)
変更/許容ルール	×	保持 (**[所有者]** 値に **[不明なユーザー]** が表示)
除外	×	保持
システムターゲットグループ	×	保持
User Target Groups	×	新しいオブジェクト所有者に移行
保存された検索条件	○	完全に削除
コネクタ	×	保持
センサー	×	保持

ユーザーアカウントの削除手順

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

[アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. で、削除するユーザーアカウントの行にある ⋮ ボタンをクリックします。

   メニューが表示されます。

5. メニューにある 🗑 ボタンをクリックします。

   注意: ユーザーが無効になっていない場合は、🗑 ボタンは表示されません。ユーザーを削除する前にユーザーを無効にします。

   注意: デフォルトの管理者アカウントを削除することはできません。デフォルトの管理者アカウントを削除する場合は、Tenable サポート に連絡する必要があります。

   ユーザー画面が表示されます。

6. **[新しいオブジェクト所有者の選択]** ドロップダウンリストボックスから、ユーザーのオブジェクト (スキャン結果、ユーザー定義スキャンテンプレートなど) の転送先のユーザーを選択します。

7. 🗑 **[削除]** をクリックします。

   確認のメッセージが表示されます。

8. **[削除]** をクリックします。

   Tenable Vulnerability Managementユーザーを削除し、ユーザーオブジェクトを指定されたユーザーに転送します。

ユーザーグループ

このセクション内のトピックは、Tenable Vulnerability Management の主な機能強化の機能更新を反映するように変更されています。詳細は、Tenable Vulnerability Management Key Enhancements を参照してください。

ユーザーグループを使用して、Tenable Vulnerability Management のさまざまなリソースのユーザーのアクセス許可を管理することができます。ユーザーをグループに割り当てると、ユーザーはグループに割り当てられたアクセス許可を継承します。企業では、グループを使用して、ユーザーのロールや企業のセキュリティ方針に基づいてユーザーにアクセス許可を割り当てることができます。

注意: ユーザーグループがユーザーアカウントおよびアクセスグループとやり取りする方法の例については、例: アクセスグループを参照してください。

ユーザーグループを表示するには、次の手順を使用します。

1. 左のナビゲーションプレーンで **[設定]** をクリックします。

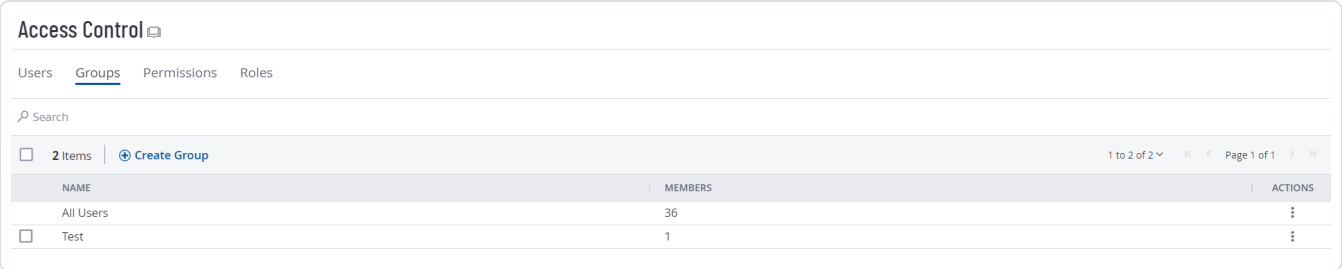
   [設定] ページが表示されます。

2. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

3. **[グループ]** タブをクリックします。

   [グループ] ページが表示されます。



[ユーザーグループ] ページに、Tenable Vulnerability Management インスタンス内のすべてのユーザーグループの表が表示されます。このドキュメントでは、この表をユーザーグループの表と呼びます。

ユーザーグループの表には次の列が含まれています。

列	説明
名前	グループ名。Tenable によって提供されている **[すべてのユーザー]** グループと **[管理者]** グループを除くすべてのユーザーグループにこの名前を定義することができます。
Members	ユーザーグループに割り当てられているユーザーの数
アクション	グループで実行できるアクション

[グループ] タブでは、次のアクションを実行できます。

- グループを作成する
- グループを編集する
- グループのエクスポート
- グループを削除する

ユーザーグループを作成する

必要なユーザーロール: 管理者

ユーザーグループを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

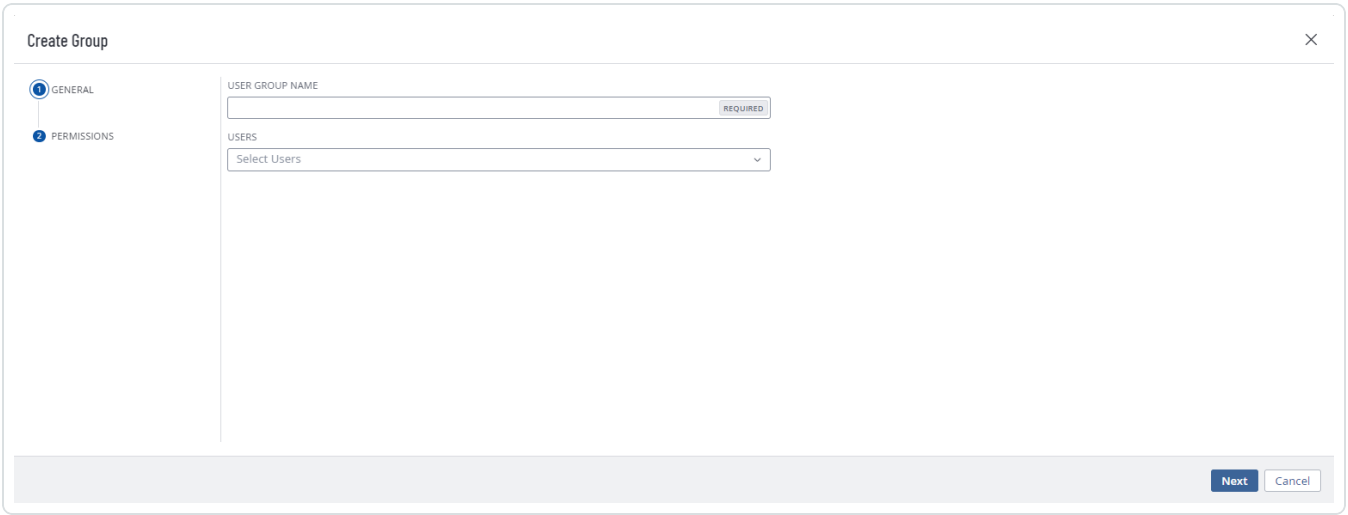
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ユーザーグループの表の上部にある ⊕ **[ユーザーグループの作成]** ボタンをクリックします。

   [グループの作成] ページが表示されます。



5. **[ユーザーグループ名]** ボックスで、新規グループの名前を入力します。

6. ユーザーをグループに追加します。

a. 追加するユーザーごとに、[ユーザー]ドロップダウンボックスをクリックして、ユーザー名の入力を始めます。

入力に伴い、Tenable Vulnerability Management は検索に一致するよう、ドロップダウンボックスのユーザーリストを絞り込みます。

b. ドロップダウンボックスでユーザーを選択します。

Tenable Vulnerability Management は、ユーザーグループに追加するユーザーのリストにそのユーザーを追加します。

> **ヒント:** 追加するユーザーリストからユーザーを削除するには、そのユーザーにカーソルを合わせて ✕ ボタンをクリックします。

7. **[保存]**をクリックします。

Tenable Vulnerability Management はユーザーグループを作成し、リスト化されたユーザーをメンバーとして追加します。

[**Groups**] ページが表示され、ユーザーグループの表にリストされている新しいグループを確認できます。

ユーザーグループを編集する

必要なユーザーロール: 管理者

グループを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ユーザーグループの表で、編集するユーザーグループをクリックします。

   [ユーザーグループの編集] ページが表示されます。

5. 次のいずれかを行います。

   - **[ユーザーグループ名]** ボックスに新しいグループ名を入力します。
   - ユーザーをグループに追加する場合

     a. 追加するユーザーごとに、**[ユーザー]** ドロップダウンボックスをクリックして、ユーザー名の入力を始めます。

     入力に伴い、Tenable Vulnerability Management は検索に一致するよう、ドロップダウンボックスのユーザーリストを絞り込みます。

     b. ドロップダウンボックスでユーザーを選択します。

     Tenable Vulnerability Management は、ユーザーグループに追加するユーザーのリストにそのユーザーを追加します。

   - ユーザーをグループから削除する場合

a. **[ユーザー]** リストで、削除するユーザーアカウントの横にある × ボタンをクリックします。

Tenable Vulnerability Management により、そのユーザーが **[ユーザー]** リストから削除されます。

- グループのアクセス許可を追加または削除します。

6. **[保存]** をクリックします。

Tenable Vulnerability Management により、変更したユーザーグループが保存されます。

[**Groups**] ページが表示され、ユーザーグループの表にリストされている新しいグループを確認できます。

グループのエクスポート

必要なユーザーロール: 管理者

アクセス制御ページの **[グループ]** タブでは、1 つ以上のユーザーグループを CSV または JSON 形式でエクスポートできます。

ユーザーグループをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[グループ]** タブをクリックします。

   [グループ] タブが開き、Tenable Vulnerability Management インスタンス内のすべてのユーザーグループを一覧にした表が表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. 次のいずれかを行います。

   #### 1 つのグループをエクスポートする場合

   a. グループの表で、エクスポートするグループの行を右クリックします。

      アクションオプションがカーソルの横に表示されます。

      -または-

      グループの表の **[アクション]** 列で、エクスポートするグループの行にある ⋮ ボタンをクリックします。

アクションボタンが行に表示されます。

b. **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス

複数のグループをエクスポートする場合

a. グループの表で、エクスポートする各グループのチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで、[→ **[エクスポート]** をクリックします。

> **注意:** 個別に選択してエクスポートできるグループは最大 200 個です。200 個以上のグループをエクスポートする場合は、グループの表の上部にあるチェックボックスを選択して、Tenable Vulnerability Management インスタンス上のすべてのグループを選択してから、[→**[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  > **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	グループのリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたグループのリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    > **注意**: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

- **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
- **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
- **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
- **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

  > **注意:** [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    > **注意**: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。
    - **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]** でエクスポートファイルにアクセスできます。

グループを削除する

必要なユーザーロール: 管理者

注意: Tenable 提供の**[管理者]**または**[すべてのユーザー]**のユーザーグループを削除することはできません。

始める前に

- すべてのユーザーをユーザーグループから削除します。ユーザーが含まれているユーザーグループを削除することはできません。

1 つ以上のユーザーグループを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで**[設定]**をクリックします。

   [設定]ページが表示されます。

3. **[アクセス制御I]**タイルをクリックします。

   [アクセス制御]ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[グループ]**タブをクリックします。

   [グループ]ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのユーザーグループがリストされます。

5. 次のいずれかを行います。

   - 1 つのユーザーグループを削除する方法

     a. ユーザーグループの表で、削除するユーザーグループの ⋮ ボタンをクリックします。

     メニューが表示されます。

     b. 🗑 **[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。

- 複数のユーザーグループを削除する方法

    a. ユーザーグループの表で、削除する各ユーザーグループのチェックボックスを選択します。

    表の上部にアクションバーが表示されます。

    b. アクションバーで、**[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。

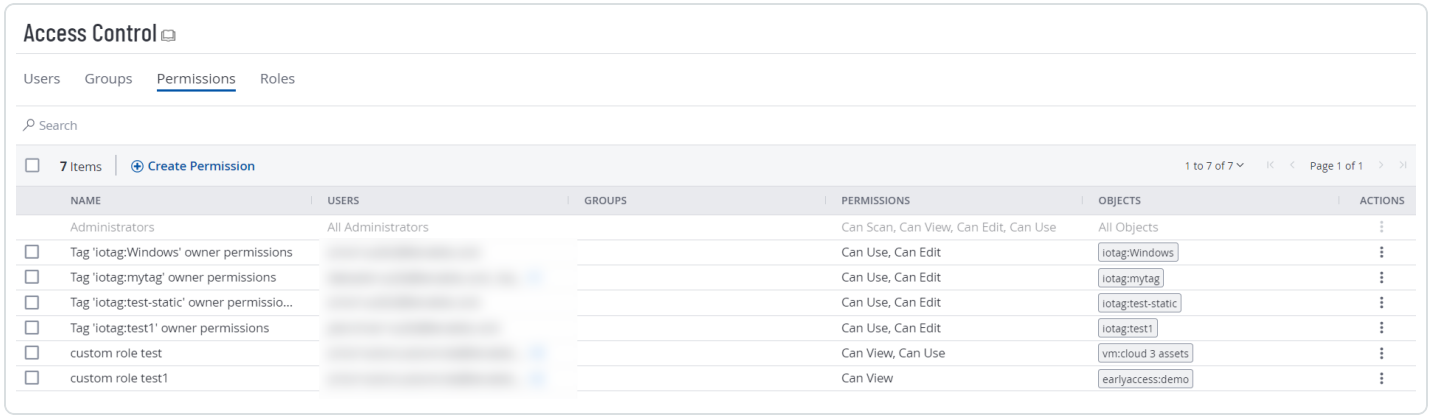
6. 確認ウィンドウで、**[削除]** をクリックします。

Tenable Vulnerability Managementにより、選択した1つまたは複数のユーザーグループが削除されます。削除されたグループは、ユーザーグループの表に表示されなくなります。

権限

Tenable Vulnerability Management では、企業のアカウントで企業のリソースとデータに対して特定のアクションを実行できるユーザーを決定する設定を作成および管理できます。このドキュメントでは、これらの設定を***アクセス許可設定***[1]と呼びます。

[マイアカウント] ページで、各ユーザーは自分に割り当てられたアクセス許可設定を表示できます。ただし、他のユーザーのアクセス許可設定を表示または管理できるのは、管理者ユーザーのみです。詳細は、Tenable 提供のロールと権限 を参照してください。



ユーザーまたはユーザーグループを作成する場合、過去に作成したタグで指定された条件を満たす資産に対して、既存のアクセス許可設定をそれらに割り当てることができます。Tenable Vulnerability Management では、これらの資産とそれらを定義するタグを***オブジェクト***[2]と言います。

ロールとアクセス許可の違いは何ですか?

- ロール - ロールにより、Tenable Vulnerability Management の主要機能の権限を管理し、ユーザーがアクセスできる Tenable Vulnerability Management モジュールや機能を制御できます。
- アクセス許可 - アクセス許可により、タグ、資産、その検出結果など、自分のデータへのアクセスを管理できます。

アクセス許可設定を作成する場合は、以下にある定義済みのアクセス許可を 1 つ以上選択する必要があります。これらのアクセス許可は、アクセス許可設定で定義された 1 つまたは複数のオブジェクトに対してユーザーが実行できるアクションを決定します。

---

[1]特定のユーザーおよびグループが特定のリソースセットで実行できるアクションを決定するために、管理者が作成できる設定です。
[2]アクセス許可設定において、アクセス許可を定義する資産とタグのことです。

アクセス許可	説明
閲覧可	ユーザーまたはグループがオブジェクトによって定義された資産を表示できるようにします。
スキャン可	ユーザーまたはグループがオブジェクトによって定義された資産をスキャンできるようにします。 **注意:** 手動で入力されたターゲットが有効と見なされるには、次の基準を満たす必要があります。 • ユーザーが管理者である、 または • ユーザーに少なくともスキャンオペレーターロール権限があり、かつ • ターゲットが Tenable Vulnerability Management システム内に存在しない場合、ユーザーは IPv4、IPV6 または FQDN を介してターゲットを明示的に参照するオブジェクトに対する**スキャン可能**アクセス許可を持っている必要があります。オブジェクトに複数のルールがある場合、それらのルールは「いずれかに一致」フィルターで結合される必要があります。または • ターゲットが Tenable Vulnerability Management システム内に既に存在する場合、ユーザーが**スキャン可能**アクセス許可を持つオブジェクトによってターゲットがタグ付けされる必要があります。
編集可	ユーザーまたはグループがオブジェクトを定義するタグを編集できるようにします。
使用可	ユーザーまたはグループがオブジェクトを定義するタグを使用できるようにします。

Tenable Vulnerability Management でアクセス許可設定を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

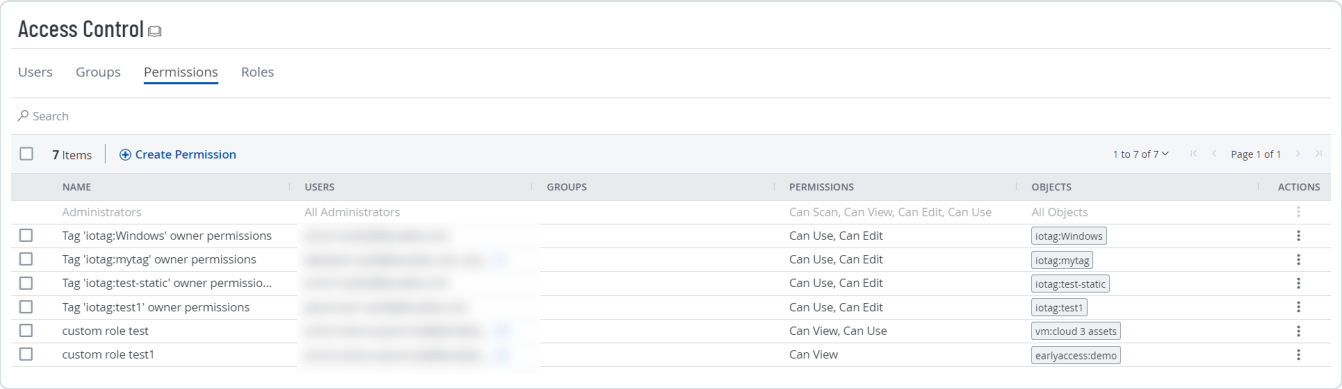
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定が一覧表示されます。



> **注意:** アクセス許可の表の最初の行には、管理者の読み取り専用エントリが含まれています。このエントリは、管理者がアカウントのすべてのリソースに対するすべてのアクセス許可を持っていることを示すために存在します。詳細は、ロールを参照してください。

[アクセス許可] タブでは、次のアクションを実行できます。

- アクセス許可設定の作成および追加
- ユーザーまたはグループへのアクセス許可設定の追加
- アクセス許可設定の編集
- アクセス許可設定のエクスポート
- ユーザーまたはユーザーグループからアクセス許可設定を削除する
- アクセス許可設定の削除

アクセス許可設定の作成および追加

必要なユーザーロール: 管理者

Tenable Vulnerability Management でアクセス許可設定を作成すると、その設定を 1 人以上のユーザーまたはグループに適用できます。

始める前に

- Tenable Vulnerability Management アカウントのユーザーまたはグループを作成します。
- アクセス許可を作成するオブジェクトのタグを作成します。

ユーザーまたはグループにアクセス許可設定を作成および追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

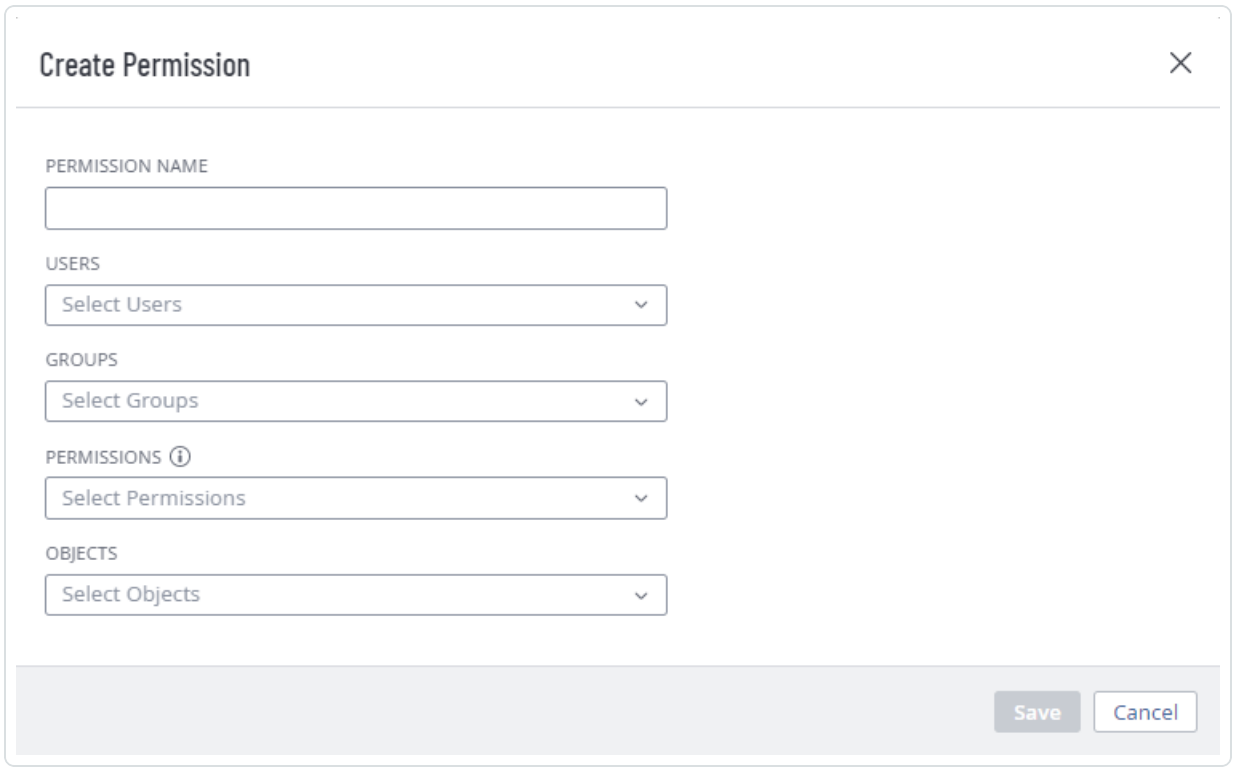
   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定が一覧表示されます。

5. 表の上部にある **[アクセス許可を作成]** をクリックします。

   [アクセス許可を作成] ウィンドウが表示されます。



6. **[アクセス許可名]**ボックスに、アクセス許可設定の名前を入力します。
7. (オプション)**[ユーザー]**ドロップダウンボックスで、1 人以上のユーザーを選択します。

   注意:[ユーザー]ボックスはオプションですが、少なくとも 1 人のユーザーまたはユーザーグループが選択されていない限り、アクセス許可設定を保存することはできません。

8. (オプション)**[グループ]**ドロップダウンボックスで、1 つ以上のユーザーグループを選択します。

   注意:[グループ]ボックスはオプションですが、少なくとも 1 人のユーザーまたはユーザーグループが選択されていない限り、アクセス許可設定を保存することはできません。

   注意:[グループ]ドロップダウンボックスで**[すべてのユーザー]**を選択して、Tenable Vulnerability Management インスタンス上のすべてのユーザーにアクセス許可設定を割り当てることができます。ただし、アクセス許可設定をすべてのユーザーに割り当てることはセキュリティのベストプラクティスに反するため、Tenable は慎重に行うことを推奨しています。

9. **[アクセス許可]**ドロップダウンボックスで、1 つ以上のアクセス許可を選択します。

注意: **[編集可]** アクセス許可を **[表示可]** または **[スキャン可]** アクセス許可とともにアクセス許可設定に追加すると、割り当てられたユーザーは、表示およびスキャンできる資産の範囲を変更することができるようになります。Tenable は、**[編集可]** アクセス許可に **[表示可]** または **[スキャン可]** を組み合わせるのは、管理者ユーザーにのみ行うことを推奨しています。

注意: **[編集可]** アクセス許可を選択すると、Tenable Vulnerability Management によって **[使用可]** アクセス許可が自動的に追加されます。

10. **[オブジェクト]** ドロップダウンボックスで、アクセス許可設定を適用するオブジェクトを 1 つ以上選択します。

注意: ドロップダウンボックス内のオブジェクトは、資産を識別および定義する前に作成されたタグです。詳細については、アクセス許可を参照してください。

ヒント: **[すべての資産]** を選択すると、資産が既存のオブジェクトに一致するかどうかに関係なく、ユーザーとグループがインスタンス上のすべての資産を表示またはスキャンできるようになります。また、**[すべてのタグ]** を選択すると、ユーザーとグループがインスタンス上のすべてのオブジェクトを編集または使用できるようにもなります。オブジェクトの詳細については、アクセス許可を参照してください。

11. **[保存]** をクリックします。

確認のメッセージが表示されます。

Tenable Vulnerability Management により変更が保存されます。アクセス許可設定が [**Permissions**] タブに表示されます。

ユーザーまたはグループへのアクセス許可設定の追加

必要なユーザーロール: 管理者

始める前に

- Tenable Vulnerability Management アカウントのユーザーまたはグループを作成します。
- アクセス許可設定を作成します。

ユーザーまたはグループにアクセス許可設定を追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. 次のいずれかを行います。

   - ユーザーにアクセス許可設定を追加する場合

     a. **[ユーザー]** タブをクリックします。

     [ユーザー] タブが表示されます。このタブには、Tenable Vulnerability Management インスタンスのすべてのユーザーのリストが含まれています。

     b. ユーザーの表で、アクセス許可設定を追加するユーザーをクリックします。

     [ユーザーの編集] ページが表示されます。

     c. 表の上部にある **[アクセス許可]** セクションで、**[アクセス許可の追加]** をクリックします。

     [アクセス許可の追加] ウィンドウが表示されます。

     d. 1つ以上のアクセス許可設定の横にあるチェックボックスを選択します。

e. **[追加]** をクリックします。

アクセス許可設定は、**[ユーザーの編集]** ページの **[アクセス許可]** 表に表示されます。

- ユーザーグループにアクセス許可設定を追加する場合

a. **[グループ]** タブをクリックします。

[グループ] タブが表示されます。このタブには、Tenable Vulnerability Management インスタンスのすべてのユーザーグループのリストが含まれています。

b. グループの表で、アクセス許可設定を追加するグループをクリックします。

[ユーザーグループの編集] ページが表示されます。

c. 表の上部にある **[アクセス許可]** セクションで、**[アクセス許可の追加]** をクリックします。

[アクセス許可の追加] ウィンドウが表示されます。

d. 1 つ以上のアクセス許可設定の横にあるチェックボックスを選択します。

e. **[追加]** をクリックします。

アクセス許可設定は、**[ユーザーグループの編集]** ページの **[アクセス許可]** 表に表示されます。

5. **[保存]** をクリックします。

Tenable Vulnerability Management によって変更が保存され、ユーザーまたはグループにアクセス許可設定が追加されます。

アクセス許可設定の編集

必要なユーザーロール: 管理者

アクセス許可設定を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブには、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定のリストが含まれています。

5. 表で、編集するアクセス許可設定をクリックします。

   [アクセス許可の詳細] ページが表示されます。

6. (オプション) **[アクセス許可名]** ボックスに、アクセス許可設定の新しい名前を入力します。

7. (オプション) ユーザーまたはユーザーグループを追加または削除します。

8. (オプション) アクセス許可を追加または削除します。

   注意: *[編集可]* アクセス許可を *[表示可]* または *[スキャン可]* アクセス許可とともにアクセス許可設定に追加すると、そのアクセス許可設定で選択されたユーザーは、表示およびスキャンできる資産の範囲を変更できます。Tenable は、*[編集可]* アクセス許可に *[閲覧可]* または *[スキャン可]* を組み合わせるのは、管理者ユーザーにのみ行うことを推奨しています。

   注意: **[編集可]** アクセス許可を選択すると、Tenable Vulnerability Management によって **[使用可]** アクセス許可が自動的に追加されます。

注意: 別のアクセス許可設定を使用して割り当てられたアクセス許可と重複する特定のオブジェクトのユーザーまたはグループにアクセス許可を割り当てることはできません。たとえば、オブジェクトに*[編集可]*アクセス許可を選択したものの、**[ユーザー]**にリストされているユーザーが既存のアクセス許可設定に基づいてそのオブジェクトを編集することが既にできる場合、Tenable Vulnerability Management によってエラーメッセージが生成され、選択を変更して冗長性を削除するまで現在のアクセス許可設定が保存できなくなります。

a. アクセス許可を追加するには、**[アクセス許可]**ドロップダウンボックスで、1 つ以上のアクセス許可を選択します。

b. アクセス許可を削除するには、**[アクセス許可]**ドロップダウンボックスで、削除する各アクセス許可の横にある ✕ ボタンをクリックします。

9. (オプション) オブジェクトを追加または削除します。

a. オブジェクトを追加するには、**[オブジェクト]**ドロップダウンボックスからオブジェクトを 1 つ以上選択します。

b. オブジェクトを削除するには、**[オブジェクト]**ドロップダウンボックスで、削除する各オブジェクトの横にある ✕ ボタンをクリックします。

10. **[保存]**をクリックします。

Tenable Vulnerability Management により変更が保存されます。更新されたアクセス許可設定が[**Permissions**]タブに表示されます。

アクセス許可設定のエクスポート

必要なユーザーロール: 管理者

[アクセス許可] ページでは、1 つ以上のアクセス許可を CSV または JSON 形式でエクスポートできます。

アクセス許可設定をエクスポートする場合

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定が一覧表示されます。

   注意: アクセス許可の表の最初の行には、管理者の読み取り専用エントリが含まれています。このエントリは、管理者がアカウントのすべてのリソースに対するすべてのアクセス許可を持っていることを示すために存在します。詳細は、ロールを参照してください。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. 次のいずれかを行います。

   ### 1 つのアクセス許可設定をエクスポートする場合

   a. アクセス許可設定の表で、エクスポートするアクセス許可設定の行を右クリックします。

      アクションオプションがカーソルの横に表示されます。

      -または-

アクセス許可設定の表の **[アクション]** 列で、エクスポートするアクセス許可設定の行にある ⋮ ボタンをクリックします。

アクションボタンが行に表示されます。

b. **[エクスポート]** をクリックします。

複数のアクセス許可設定をエクスポートする場合

a. アクセス許可設定の表で、エクスポートする各アクセス許可設定のチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで ⋮ **[その他]** をクリックします。

メニューが表示されます。

c. [→ **[エクスポート]** をクリックします。

> **注意:** 個別に選択してエクスポートできるアクセス許可設定は最大 200 個です。200 個以上のアクセス許可設定をエクスポートする場合は、アクセス許可設定の表の上部にあるチェックボックスを選択して、Tenable Vulnerability Management インスタンス上のすべてのアクセス許可設定を選択してから、[→ **[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。このプレーンには以下が含まれています。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	アクセス許可設定のリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたアクセス許可設定のリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  注意: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

ユーザーまたはユーザーグループからアクセス許可設定を削除する

必要なユーザーロール: 管理者

注意: Tenable 提供の **[管理者]** または **[すべてのユーザー]** のユーザーグループからアクセス許可設定を削除することはできません。

ユーザーまたはユーザーグループからアクセス許可設定を削除するには、次の手順に従います。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. ユーザーからアクセス許可設定を削除する方法

   - 次のいずれかを行います。

     - **[ユーザー]** タブからアクセス許可設定を削除する場合

       a. **[ユーザー]** タブをクリックします。

       [ユーザー] タブが表示されます。このタブには、Tenable Vulnerability Management インスタンスのすべてのユーザーのリストが含まれています。

       b. で、アクセス許可設定を削除するユーザーをクリックします。

       [ユーザーの編集] ページが表示されます。

       c. **[アクセス許可]** 表の **[アクション]** 列で、削除するアクセス許可設定の横にある ⋮ ボタンをクリックします。

       d. **[削除]** 🗑 ボタンをクリックします。

Tenable Vulnerability Management によってユーザーのアクセス許可設定が削除されます。

e. (オプション) アクセス許可設定を削除するユーザーごとにこの手順を繰り返します。

- **[アクセス許可]** タブからアクセス許可を削除する場合

a. **[アクセス許可]** タブをクリックします。

[アクセス許可] タブが表示されます。このタブの表には、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定が一覧表示されます。

b. 表で、削除するアクセス許可設定をクリックします。

[アクセス許可の詳細] ページが表示されます。

c. **[ユーザー]** で、アクセス許可設定を削除する各ユーザーの横にある ✕ ボタンをクリックします。

Tenable Vulnerability Management によって、**[ユーザー]** リストからアクセス許可設定が削除されます。

5. ユーザーグループからアクセス許可設定を削除する方法

- 次のいずれかを行います。

- **[グループ]** タブからアクセス許可設定を削除する場合

a. **[グループ]** タブをクリックします。

[グループ] タブが表示されます。このタブには、Tenable Vulnerability Management インスタンスのすべてのユーザーグループのリストが含まれています。

b. ユーザーグループの表で、アクセス許可設定を削除するグループをクリックします。

[ユーザーグループの編集] ページが表示されます。

c. **[アクセス許可]** 表の **[アクション]** 列で、削除するアクセス許可設定の横にある ⋮ ボタンをクリックします。

d. **[削除]** 🗑 ボタンをクリックします。

Tenable Vulnerability Management によってユーザーグループからアクセス許可設定が削除されます。

e. (オプション) アクセス許可設定を削除するユーザーグループごとにこの手順を繰り返します。

- **[アクセス許可]** タブからアクセス許可設定を削除する場合

a. **[アクセス許可]** タブをクリックします。

[アクセス許可] タブが表示されます。このタブの表には、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定が一覧表示されます。

b. 表で、削除するアクセス許可をクリックします。

[アクセス許可の詳細] ページが表示されます。

c. **[グループ]** で、アクセス許可設定を削除する各ユーザーグループの横にある ✕ ボタンをクリックします。

Tenable Vulnerability Management によって、**[グループ]** リストからアクセス許可設定が削除されます。

6. **[保存]** をクリックします。

Tenable Vulnerability Management によって変更が保存され、ユーザーまたはグループからアクセス許可が削除されます。

アクセス許可設定の削除

必要なユーザーロール: 管理者

注意: デフォルトのアクセス許可設定を削除することはできません。

ユーザーまたはユーザーグループからアクセス許可設定を削除するには、次の手順に従います。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[アクセス許可]** タブをクリックします。

   [アクセス許可] タブが表示されます。このタブの表には、Tenable Vulnerability Management インスタンスのすべてのアクセス許可設定が一覧表示されます。

5. 表の **[アクション]** 列で、削除するアクセス許可設定の横にある ⋮ ボタンをクリックします。

6. **[削除]** 🗑 ボタンをクリックします。

   Tenable Vulnerability Management がアクセス許可設定を削除します。

ロール

ロールにより、Tenable Vulnerability Management の主要機能の権限を管理し、Tenable Vulnerability Management でユーザーがアクセスできる Tenable Vulnerability Management リソースを制御できます。

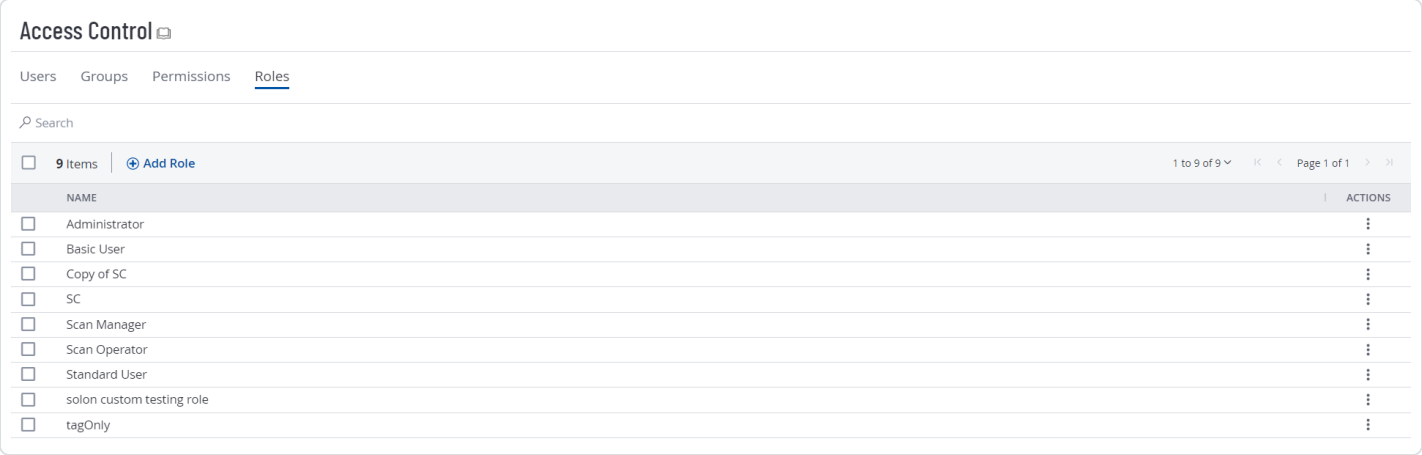
ユーザーを作成するときには、そのユーザーが実行できる操作にだいたい該当するロールを選択する必要があります。

注意: 個別のユーザーまたはグループにアクセス許可を割り当てることにより、特定のリソースへのユーザーアクセスをさらに絞り込むことができます。詳細は、権限を参照してください。

ロールとアクセス許可の違いは何ですか?

- ロール - ロールにより、Tenable Vulnerability Management の主要機能の権限を管理し、ユーザーがアクセスできる Tenable Vulnerability Management モジュールや機能を制御できます。
- アクセス許可 - アクセス許可により、タグ、資産、その検出結果など、自分のデータへのアクセスを管理できます。

[ロール] ページでは、Tenable 提供のすべてのロールと、Tenable Vulnerability Management インスタンスで作成されたカスタムロールを表示できます。



以下のロールのいずれか種類をユーザーに割り当てることができます。

ロールの種類	説明
Tenable 提供のロール	アカウントのライセンスで指定された Tenable Vulnerability Management 製品によって断定される、事前定義された一連の権限が含まれています。各ロールには下位

と権限	ロールの権限が含まれ、新しい権限が追加されます。管理者が最も多くの権限を持っています。ただのユーザーには最小限のアクセス許可があります。
カスタムロール	Tenable Vulnerability Management インスタンス上のユーザー権限とリソースへのアクセス権を調整できる、権限のカスタムセットが含まれています。

ユーザーロールを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

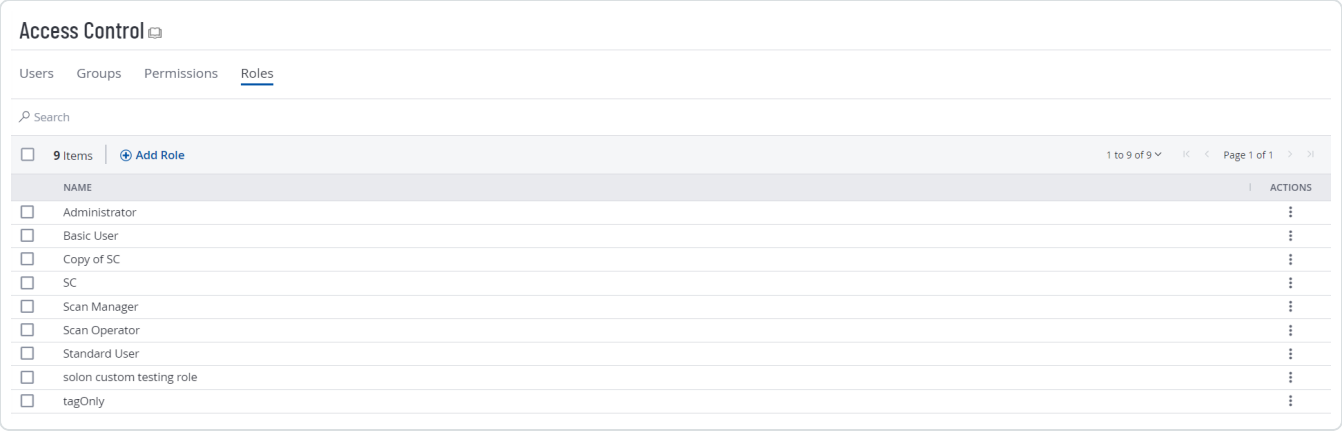
   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Vulnerability Management インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。



[**Roles**] ページでは、次のアクションを実行できます。

- カスタムロールの作成
- ロールを複製する

- カスタムロールの編集
- ロールのエクスポート
- カスタムロールを削除する

Tenable 提供のロールと権限

以下の表は、Tenable 提供の各ユーザーロールに関連付けられた権限を各製品の機能別にまとめたものです。

注意: 個別のユーザーまたはグループにアクセス許可を割り当てることにより、特定のリソースへのユーザーアクセスをさらに絞り込むことができます。詳細は、権限を参照してください。

領域	Tenable Vulnerability Management で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
Activity Logs	表示、エクスポート	-	-	-	-
API キー	表示、修正	表示、修正	表示、修正	表示、修正	表示、修正
アカウント設定	表示、修正	表示、修正	表示、修正	表示、修正	表示、修正
エージェント	表示、削除	表示、削除	-	-	-
エージェントフリーズ期間	表示、作成、修正、削除	表示、作成、修正、削除	-	-	-
エージェントグループ	表示、作成、修正、削除	表示、作成、修正、削除	-	-	-
エージェント設定	表示、修正	表示、修正	-	-	-
資産	表示、修正、エクスポート、削除	表示、修正、エクスポート、削除	表示、修正、エクスポート、削除	表示、修正、エクスポート、削除	表示、エクスポート
コネクタ	表示、作成、修正、	-	-	-	-

領域	Tenable Vulnerability Management で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	削除				
ダッシュボード	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除	表示、作成、修正、エクスポート、削除
除外	表示、インポート、エクスポート、削除	表示、インポート、エクスポート、削除	-	-	-
Exports	表示、修正、エクスポート、削除	-	-	-	-
全般設定	表示、修正	-	-	-	-
正常性とステータス	表示	-	-	-	-
認証情報の管理	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除
PCI 管理	表示、インポート、エクスポート、修正、削除	-	-	-	-
変更ルール	表示、作成、修正、削除	-	-	-	-
レポート	表示、実	表示、実	表示、実	表示、実	表示

領域	Tenable Vulnerability Management で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	行、作成、修正、削除	行、作成、修正、削除	行、作成、修正、削除	行、作成、修正、削除	
レポート結果	表示、削除	表示、削除	表示、削除	表示、削除	表示
スキャン[1]	表示、インポート、実行、作成、修正、削除	表示、インポート、実行、作成、修正、削除	表示、インポート、実行、作成、修正、削除	表示、インポート、実行、作成[2]、修正、削除	表示[3]、インポート
スキャン結果	表示、エクスポート、削除	表示、エクスポート、削除	表示、エクスポート、削除	表示、エクスポート、削除	表示、エクスポート、削除
センサー	表示、追加、修正、削除	表示、追加、修正、削除	-	-	-
スキャナーグループ	表示、作成、修正、削除	表示、作成、修正、削除	-	-	-
タグ[4]	表示、タグカテゴリの作成、タグ値の	表示、タグ値の作成、削除、割り当	表示、削除、割り当て、割り当て	表示、削除、割り当て、割り当て	表示、割り当て、割り当て解除

[1]ユーザーができることはユーザーロールによって決まりますが、特定のスキャンに対してユーザーが持つアクセス許可はスキャンアクセス許可によって決まります。
[2]ユーザーが共有する既存のユーザー定義ポリシーを使用してスキャンを作成できます。
[3]スキャンの一覧を表示できますが、スキャンの詳細設定は表示できません。
[4]タグの割り当ておよび割り当て解除は、[資産の詳細]ページから実行できます。

領域	Tenable Vulnerability Management で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	作成、削除、エクスポート、割り当て、割り当て解除	て、割り当て解除	解除[1]	解除	
ユーザーグループ	表示、作成、修正、削除、エクスポート	-	-	-	-
ユーザー定義のスキャンテンプレート	表示、インポート、エクスポート、修正、削除	表示、インポート、エクスポート、修正、削除	表示、インポート、エクスポート、修正、削除	-	-
ユーザー	表示、作成、修正、削除	-	-	-	-
脆弱性	表示、エクスポート	表示、エクスポート	表示、エクスポート	表示、エクスポート	表示、エクスポート

領域	Tenable Web App Scanning で提供されるロールと権限					
	管理者	スキャンマネージャー	標準	スキャンオペレーター		基本
ダッシュボード	表示、作成、	表示、作成、修正、	表示、作成、修	表示、作成、	表示	表示

[1]標準ユーザーがタグを表示、削除、割り当て、割り当て解除するには、**[使用可]** アクセス許可が必要です。

領域	Tenable Web App Scanning で提供されるロールと権限					
	管理者	スキャンマネージャー	標準	スキャンオペレーター		基本
	修正、削除	削除	正、削除	修正、削除		
Tenable 提供スキャンテンプレート	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示	-	-
User-Defined Templates	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	-	-
スキャン (スキャンアクセス許可も必要です)	表示、インポート、作成、修正、実行、削除	表示、インポート、作成、修正、実行、削除	表示、作成、修正、実行、削除	表示、作成[1]、修正、実行、削除、ゴミ箱に移動	表示	表示
認証情報の管理	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除	表示、作成、修正、削除

[1]ユーザーが共有する既存のユーザー定義ポリシーを使用してスキャンを作成できます。

領域	Tenable Web App Scanning で提供されるロールと権限					
	管理者	スキャンマネージャー	標準	スキャンオペレーター		基本
スキャンアクセス許可	表示、作成、修正、削除[1]	表示、作成、修正、削除[2]	表示、作成、修正、削除[3]	表示、作成、修正、削除[4]	-	-
スキャン結果 (スキャンアクセス許可も必要です)	表示、削除	表示、削除	表示、削除	表示、削除	表示、削除	表示、削除

領域	Lumin Exposure View で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
設定	管理、読み取り	読み取り	読み取り	読み取り	読み取り
アクセスできる資産タイプ	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、	コンピューティングリソース(ホスト)、クラウドリソース、

[1]管理者は、アカウントの任意のユーザーが所有するスキャンのアクセス許可を作成、変更、削除することができます。
[2]スキャンマネージャーユーザーは、自分が所有するスキャンのアクセス許可のみを作成、変更、削除することができます。
[3]Standard ユーザーは、自分が所有するスキャンのアクセス許可のみを作成、変更、削除することができます。
[4]Scan Operator ユーザーは、自分が所有するスキャンのアクセス許可のみを作成、変更、削除することができます。

領域	Lumin Exposure View で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
	ウェブアプリケーション、ID	ウェブアプリケーション、ID	ウェブアプリケーション、ID	ウェブアプリケーション、ID	ウェブアプリケーション、ID
エクスポート	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理
エクスポージャーカード	作成、共有、読み取り	作成、共有、読み取り	作成、共有、読み取り	共有、読み取り	読み取り

領域	Asset Inventory で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
アクセスできる資産タイプ	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID	コンピューティングリソース(ホスト)、クラウドリソース、ウェブアプリケーション、ID
エクスポート	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理
タグ	作成、編集	作成、編集	-	-	-

領域	Attack Path Analysis で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
エクスポート	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理	自分のもののみ管理

領域	Attack Path Analysis で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
検出結果	管理、読み取り	管理、読み取り	読み取り	読み取り	読み取り
クエリ	検索、保存	検索、保存	検索、保存	検索	検索

領域	Tenable Attack Surface Management で提供されるロールと権限		
	ビジネス管理者	アクティブユーザー	閲覧専用ユーザー
インベントリ	管理、追加、修正、削除	追加、修正、放置	閲覧
提案	管理、追加、修正、削除	管理、追加、修正、削除	閲覧
サブスクリプション	管理、追加、修正、削除	管理、追加、修正、削除	閲覧
レポート	管理、追加、修正、削除	管理、追加、修正、削除	閲覧
テキストレコード	管理、修正、削除	管理、修正、削除	閲覧
ユーザーアカウント	管理、修正、削除	-	-
ビジネス	管理、修正	-	-

注意: デフォルトでは、Tenable One 内で作成された Tenable Attack Surface Management ユーザーには**アクティブユーザー**の役割が付与されます。

領域	Tenable Container Security で提供されるロールと権限				
	管理者	スキャンマネージャー	標準	スキャンオペレーター	基本
ダッシュ	表示	表示	表示	表示	表示

ボード					
データ使用量	表示[1]	表示	表示	表示	表示
イメージ	表示、Tenable Vulnerability Management にプッシュ、削除[2]	表示、Tenable Vulnerability Management にプッシュ、削除	表示、Tenable Vulnerability Management にプッシュ、削除	表示、Tenable Vulnerability Management にプッシュ、削除	-
イメージリポジトリ	表示、検索、削除	表示、検索、削除	表示、検索、削除	表示、検索、削除	表示、検索
コンテナ	表示	表示	表示	表示	表示
ポリシー	作成、表示、編集、アクセス許可の設定、削除	作成、表示、編集、アクセス許可の設定、削除	表示	表示	表示
コネクタ	作成、設定、表示、削除	-	-	-	-
CS スキャナー	ダウンロード、表示、設定、実行	ダウンロード、表示、設定、実行	ダウンロード、表示、設定、実行	ダウンロード、表示、設定、実行	ダウンロード
スキャン結果	表示、検索	表示、検索	表示、検索	表示、検索	表示、検索

[1]管理者ロールを持つユーザーは、その他のロールでは表示できないライセンス情報を表示できます。
[2]管理者ロールを持つユーザー以外のユーザーは、自分がインポートしたイメージのみを削除できます。管理者ユーザーは、アカウント上のすべてのユーザーのイメージを削除できます。

カスタムロール

Tenable Vulnerability Management インスタンスでユーザーのカスタムロールを作成して、自社のニーズに固有の権限をそれらのユーザーに付与できます。

カスタムロールを作成する場合は、以下の権限の一部またはすべてを追加できます。カスタムロールを編集して権限を削除することもできます。ロールに追加またはロールから削除できる権限は、各権限が適用される Tenable Vulnerability Management の領域によって異なります。

注意: アカウント上のリソースへのユーザーのアクセスは、ユーザーのロールに関係なく、ユーザーのアクセス許可によって制限される場合があります。

- **作成** - ユーザーはエクスポージャーカードまたはタグを作成できます。この権限は、それぞれ Lumin Exposure View および Asset Inventory に固有のものです。
- **管理** - 権限が適用される領域でユーザーが作成、変更、削除を行えるようにします。

  注意: 管理権限をカスタムロールに追加すると、Tenable Vulnerability Management は自動的に**読み取り**権限も追加します。最初に**管理**権限を無効にしない限り、**読み取り**権限は無効にできません。

- **すべて管理** - ユーザーは、他のユーザーが作成したエクスポートを含め、エクスポートを表示、変更、削除できます。
- **自分のもののみ管理** - ユーザーは、自分が作成したエクスポートのみを表示、変更、削除できます。
- **共有** - ユーザーは、他のユーザーまたはグループとオブジェクトを共有できます。

  注意: カスタムロールで **[読み取り]** アクセス許可も有効になっていない場合、そのカスタムロールは、オブジェクトの共有相手となる他のユーザーのリストにアクセスできません。

- **読み取り** - ユーザーは、権限が適用される領域のアイテムを閲覧できます。
- **使用** - ユーザーは、Tenable Vulnerability Management スキャンの作成中に Tenable 提供のスキャンテンプレートを使用できます。
- **PCI の提出** - ユーザーは、PCI 検証のためにスキャンを送信できるようになります。詳細については、*Tenable PCI ASV ユーザーガイド*を参照してください。
- **検索** - ユーザーは、権限が適用される範囲でクエリを検索できます。この権限は、Attack Path Analysis に固有です。

- **保存** - ユーザーは、権限が適用されるクエリを保存できます。この権限は、Attack Path Analysis に固有です。
- **クラウドリソース** - ユーザーは、**クラウドリソース**データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。
- **コンピューティングリソース** - ユーザーは、**コンピューティングリソース**データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。
- **ID** - ユーザーは、**ID** データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。
- **ウェブアプリケーション** - ユーザーは、**ウェブアプリケーション**データソースの資産にアクセスできます。この権限は Lumin Exposure View および Asset Inventory に固有です。

次の表に、Tenable Vulnerability Management の各セクションでカスタムロールに使用できる権限オプションを示します。

注意: カスタムロールを作成するときは、**[一般設定]**、**[ライセンス]**、および **[マイアカウント]** セクションの**読み取り**権限を含める必要があります。これらのセクションの**読み取り**権限を含めないと、ロールに割り当てられたユーザーは Tenable Vulnerability Management にログインできません。

セクション	権限オプション
Asset Inventory	
アクセスできる資産タイプ	**クラウドリソース、コンピューティングリソース、ID、ウェブアプリケーション**
インベントリ	**読み取り**
エクスポート	**自分のもののみ管理**
タグ	**作成、編集**
Attack Path Analysis	
エクスポート	**自分のもののみ管理**
検出結果	**読み取り、管理**
クエリ	**保存、検索**

Lumin Exposure View	
アクセスできる資産タイプ	**クラウドリソース、コンピューティングリソース、ID、ウェブアプリケーション**
エクスポート	**自分のもののみ管理**
エクスポージャーカード	**読み取り、作成、共有**
設定	**読み取り、管理**
プラットフォーム設定	
資産	**読み取り**
検出結果	**読み取り**
マイアカウント	**読み取り、管理**
アクセス制御	**読み取り、管理** **注意:** アクセス制御 で**管理**権限を追加すると、そのカスタムロールを持つユーザーはだれでも、管理者ユーザーを作成し、そのユーザーとしてログインし、そのユーザー自身のインスタンスを含め、Tenable Vulnerability Management インスタンスの任意のユーザーの権限やアクセス許可を変更することができます。アクセス制御 設定を管理できるユーザーアカウントを作成する場合、Tenable はそのユーザーに管理者ロールを割り当てることを推奨します。詳細は、Tenable 提供のロールと権限を参照してください。
Activity Log	**読み取り**
全般設定	**読み取り、管理**
ライセンス情報	**読み取り**
ワークスペース	
資産	**読み取り**
検出結果	**読み取り**
Vulnerability Management	

Dashboard	**管理、共有** **注意:** ダッシュボード セクションのカスタムロール権限には、ダッシュボードをエクスポートする機能が含まれていません。ユーザーがダッシュボードをエクスポートできるようにするには、Tenable が提供するロールをユーザーに割り当てます。 **注意:**すべてのユーザーは、自分に割り当てられた権限に関係なく、自分が作成したダッシュボード、または他のユーザーが共有してくれたダッシュボードを表示できます。
エクスポート	**すべて管理、自身を管理**
変更/許容ルール	**読み取り、管理**
スキャン	
Nessus/Nessus Agent スキャン	**読み取り、管理、PCI の提出**
スキャンの除外	**読み取り、管理**
Tenable 提供のスキャンテンプレート	**使用**
ユーザー定義スキャンテンプレート	**読み取り、管理**
管理された認証情報	**読み取り、管理**
ターゲットグループ	**読み取り、管理**

カスタムロールの作成

必要なユーザーロール: 管理者

注意: Tenable アプリケーションは現在、カスタムロールによるスキャンとセンサーの管理をサポートしていません。

カスタムロールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

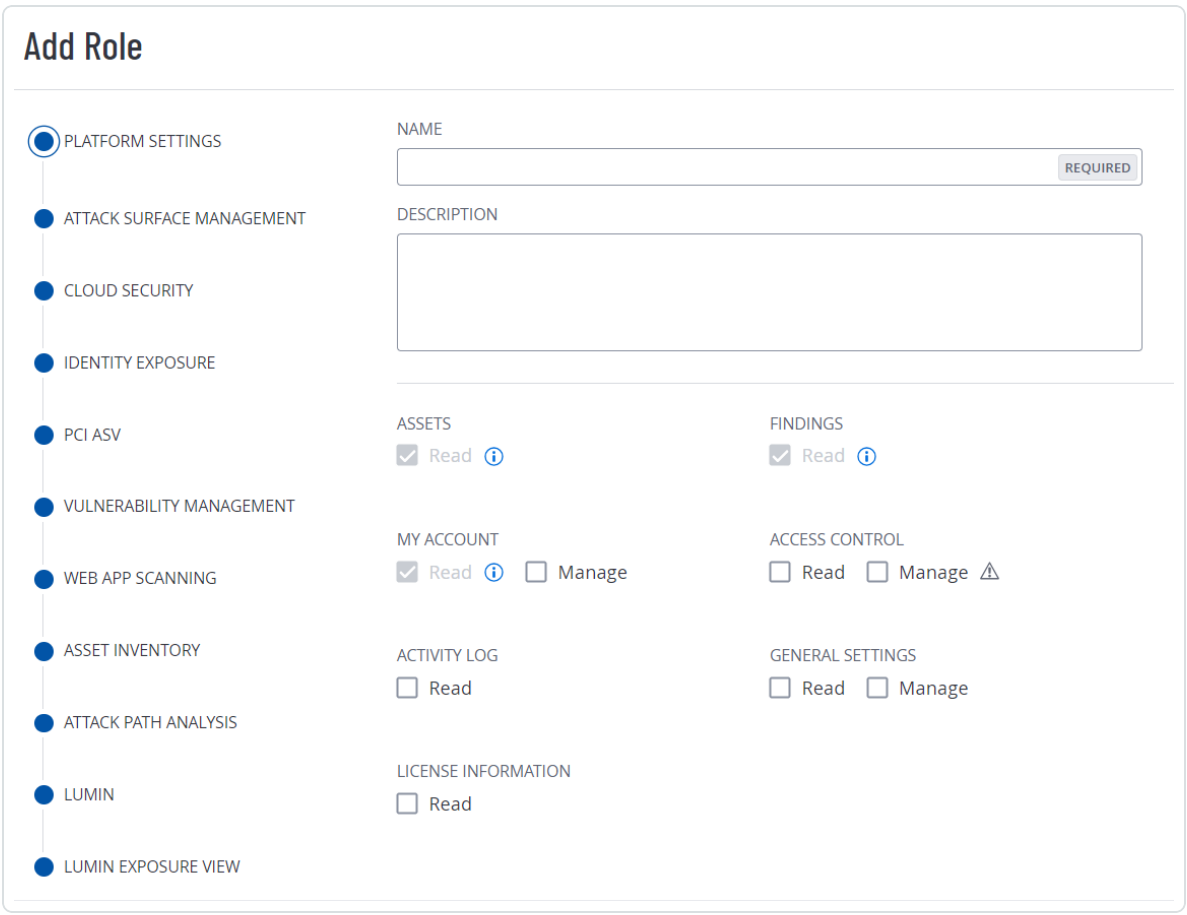
   [ロール] ページが表示されます。このページの表に、Tenable Vulnerability Management インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. 次のいずれかを行います。

   - 既存のロールを複製して変更します。
   - 新しいロールを追加する

     a. 表の上部にある **[ロールの追加]** をクリックします。

        [ロールの追加] ページが表示されます。



b. **[名前]**ボックスにカスタムロールの名前を入力します。

c. (オプション)**[説明]**ボックスに、カスタムロールの説明を入力します。

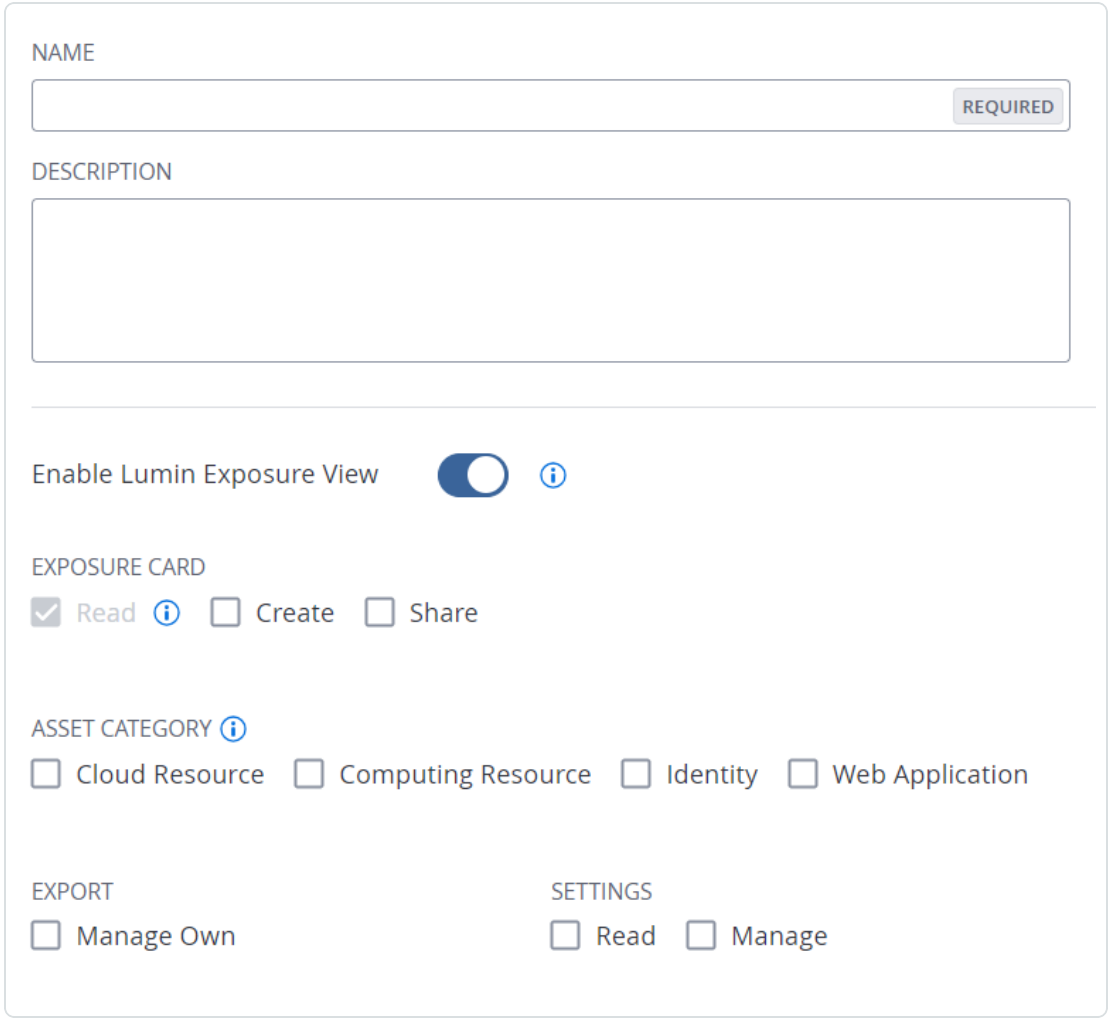
d. カスタムロールがアクセスできるアプリケーションを決定します。

   i. 左側のパネルで、[アプリケーション名]をクリックします。

      [有効化]トグルが表示されます。

   ii. **[有効化]**トグルをクリックして、作成しているカスタムロールについて、このアプリケーションへのアクセスを有効または無効にします。

      一部のアプリケーションでは、アプリケーションに関連付けられた権限が表示されます。



iii. カスタムロールに追加する各権限のチェックボックスを選択します。

e. **[保存]**をクリックします。

Tenable Vulnerability Management によってロールが保存され、ロールの表に追加されます。

ロールを複製する

必要なユーザーロール: 管理者

カスタムロールを作成するには、既存のカスタムロールを複製し、必要に応じて新しいロールの設定を変更します。

注意: Tenable 提供のロールは複製できません。

複製を使用してカスタムロールを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Vulnerability Management インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. ロールの表で、複製するロールの横にあるチェックボックスを選択します。

   表の上部にアクションバーが表示されます。

6. アクションバーで ⋮ **[その他]** をクリックします。

   メニューが表示されます。

7. **[複製]** をクリックします。

   ロールのコピーが表に表示され、「[ロール名] のコピー」がプレフィックスとして付きます。

8. 複製されたロールをクリックします。

[ロールの詳細] ページが表示されます。複製するロールの名前、説明、および選択した権限は、元のロールからコピーされます。

9. 次の設定から1つ以上を更新します。

    - 名前 - **[名前]** ボックスにロールの新しい名前を入力します。
    - 説明 - **[説明]** ボックスに、ロールの説明を入力します。
    - Privileges - Tenable Vulnerability Management の各領域で、ロールに追加またはロールから削除する各権限の横にあるチェックボックスを選択または選択解除します。

10. **[保存]** をクリックします。

    Tenable Vulnerability Management によって変更が複製ロールに保存されます。

カスタムロールの編集

必要なユーザーロール: 管理者

注意: Tenable アプリケーションは現在、カスタムロールによるスキャンとセンサーの管理をサポートしていません。

カスタムロールを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Vulnerability Management インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. ロールの表で、編集するロールをクリックします。

   [ロールの詳細] ページが表示されます。

6. 次の設定から 1 つ以上を更新します。

   - 名前 - **[名前]** ボックスにロールの新しい名前を入力します。
   - 説明 - **[説明]** ボックスに、ロールの説明を入力します。
   - Privileges - Tenable Vulnerability Management の各領域で、ロールに追加またはロールから削除する各権限の横にあるチェックボックスを選択または選択解除します。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management により変更が保存されます。

カスタムロールを削除する

必要なユーザーロール: 管理者

注意: 削除できるのはカスタムロールのみです。Tenable 提供のロールと権限は削除できません。

カスタムロールを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表に、Tenable Vulnerability Management インスタンスで使用可能なすべてのユーザーロールが一覧表示されます。

5. 表の **[アクション]** 列で、削除するロールの横にある ⋮ ボタンをクリックします。

6. **[削除]** 🗑 ボタンをクリックします。

   Tenable Vulnerability Management によってロールが削除され、ロールの表からそのロールが削除されます。

ロールのエクスポート

必要なユーザーロール: 管理者

[ロール] ページでは、1 つ以上のユーザーグループを CSV または JSON 形式でエクスポートできます。

ユーザーロールをエクスポートする場合

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセス制御I]** タイルをクリックします。

   [アクセス制御] ページが表示されます。このページで、Tenable Vulnerability Management アカウントのリソースへのユーザーアクセスとグループアクセスを制御できます。

4. **[ロール]** タブをクリックします。

   [ロール] ページが表示されます。このページの表には、Tenable Vulnerability Management インスタンス上のすべての Tenable 提供ロールとカスタムロールが一覧表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. 次のいずれかを行います。

   ### 1 つのロールをエクスポートする場合

   a. ロールの表で、エクスポートするロールの行を右クリックします。

      アクションオプションがカーソルの横に表示されます。

      -または-

      ロールの表の **[アクション]** 列で、エクスポートするロールの行にある ⋮ ボタンをクリックします。

      アクションボタンが行に表示されます。

   b. **[エクスポート]** をクリックします。

複数のロールをエクスポートする場合

a. ロールの表で、エクスポートする各ロールのチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. アクションバーで、[→ **[エクスポート]** をクリックします。

> **注意:** 個別に選択してエクスポートできるロールは最大 200 個です。200 個以上のロールをエクスポートする場合は、ロールの表の上部にあるチェックボックスを選択して、Tenable Vulnerability Management インスタンス上のすべてのロールを選択してから、[→ **[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

> **注意:** デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	ロールのリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたロールのリストを含む JSON ファイル

	空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

    - **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

> **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

アクティビティログ

必要なユーザーロール: 管理者

[アクティビティログ] ページでは、企業の Tenable Vulnerability Management アカウント内のすべてのユーザーに対するイベントのリストを表示できます。各アクティビティが行われたタイミング、アクション、アクター、その他アクティビティに関連する情報を確認できます。

重要: Tenable では現在アクティビティログデータは 3 年保持され、その後 Tenable のデータベースから削除されます。

アクティビティログを表示する方法

1. 左上にある ☰ ボタンをクリックします。

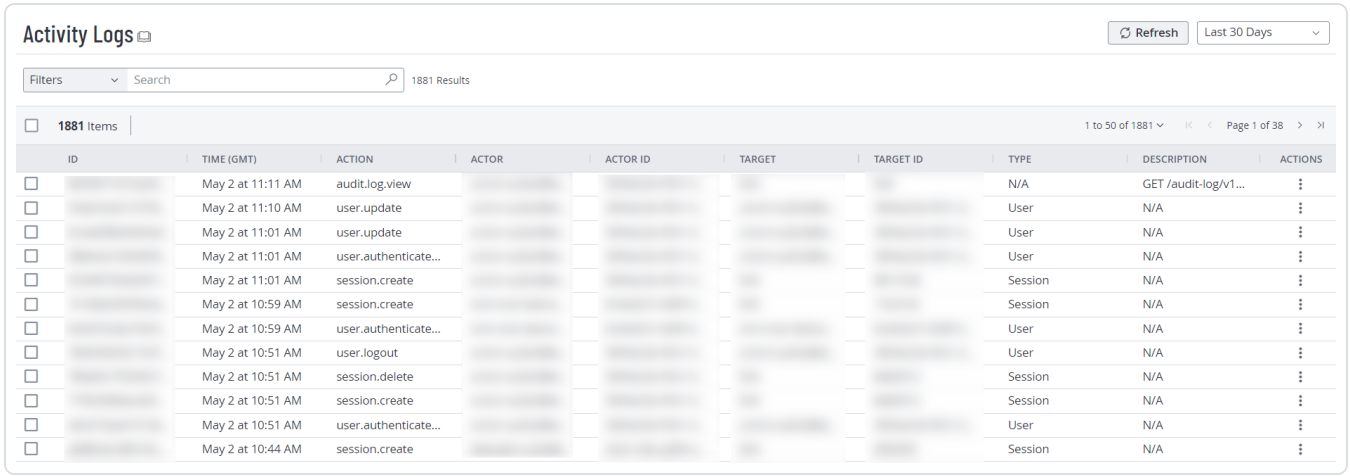
   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクティビティログ]** タイルをクリックします。

   [アクティビティログ] ページが表示されます。このページには、企業の Tenable Vulnerability Management アカウントに関連するアクティビティのリストが表示されます。



4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management の表 を参照してください。

5. (オプション) 表にフィルターを適用します。

フィルター	説明
アクター ID	アクションを実行したアカウントの ID
ターゲット ID	アクションの影響を受けたアカウントの ID (存在する場合)
アクション	アクションの種類
日付	アクションが実行された日付

6. (オプション) アクティビティログの表を更新するには、右上にある **[更新]** ボタンをクリックします。
7. (オプション) 表を特定の期間でフィルタリングします。
    - **過去 7 日間**
    - **過去 14 日間**
    - **過去 30 日間**
    - **過去 90 日間**
    - **すべて**

次の手順

- (オプション) 1 つ以上のアクティビティログをエクスポートします。

アクティビティログのエクスポート

必要なユーザーロール: 管理者

[アクティビティログ] ページでは、1 つ以上のアクティビティログを CSV または JSON 形式でエクスポートできます。

アクティビティログをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクティビティログ]** タイルをクリックします。

   [アクティビティログ] ページが表示されます。このページには、企業の Tenable Vulnerability Management アカウントに関連するアクティビティのリストが表示されます。

4. (オプション) 表データを選別します。詳細は、表のフィルタリング を参照してください。

5. エクスポートするアクティビティログを選択します。

エクスポート範囲	アクション
選択したアクティビティログ	選択したアクティビティログをエクスポートする方法 a. アクティビティログの表で、エクスポートする各アクティビティログのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→**[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のアクティビティログをエクスポートする場合は、リスト内のすべてのア

	クティビティログを選択してから、[→**[エクスポート]**をクリックします。
1つのアクティビティログ	1つのアクティビティログをエクスポートする方法 a. アクティビティログの表で、エクスポートするアクティビティログの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- アクティビティログの表の**[アクション]**列で、エクスポートするアクティビティログの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. [→ **[エクスポート]**をクリックします。

[エクスポート]プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス。
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]**ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	アクティビティログのリストを含むCSVテキストファイル。

	注意: .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたアクティビティログのリストを含む JSON ファイル。 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。
    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。
11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポートプレーンを閉じた場合は、エクスポートページからエクスポートファイルにアクセスできます。

アクセスグループ

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

注意: スキャン結果の表示、および特定のターゲットのスキャンを制御していたシステムターゲットグループのアクセス許可は、アクセスグループに移行しました。詳細は、スキャンのアクセス許可の移行 を参照してください。

アクセスグループを使用することで、次を実行できる組織のユーザーまたはグループを制御できます。

- 特定の資産および関連する脆弱性を、集約されたスキャン結果のビュー(新しいインターフェースのダッシュボード、および従来のインターフェースのワークベンチ)で表示する。
- 特定のターゲットに対してスキャンを実行し、ターゲットの個別のスキャン結果を表示する。

アクセスグループに含まれる資産またはターゲットは、設定したルールにより規定されます。アクセスグループのルールでは、資産またはターゲットをグループに関連付けるために Tenable Vulnerability Management が使用する、固有の属性を指定します。(たとえば、AWS Account ID、FQDN、IP アドレスなど)アクセスグループでユーザーまたはユーザーグループにアクセス許可を割り当てることで、そのアクセスグループに関連付けられた資産またはターゲットに対する、表示またはスキャンのアクセス許可をユーザーに付与できます。

注意: アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのにある程度の時間を要する場合があります。

[アクセスグループ] ページにあるアクセスグループの表の **[ステータス]** 列で、この割り当てプロセスのステータスを確認できます。

アクセスグループを表示、作成、編集できるのは管理者のみです。他のロールを割り当てられているユーザーは、自分が所属するアクセスグループおよびそれに関連するルールを表示できますが、アクセスグループのその他のユーザーを表示することはできません。

注意: **アクセスグループ**タイルは、1 つ以上のアクセスグループが割り当てられている場合や、自分が管理者であり、Tenable Vulnerability Management のユーザーがアクセスグループに割り当てられている場合にのみ表示されます。すべてのアクセスグループを権限設定に変換すると、**アクセスグループ**タイルはアカウントに表示されなくなります。

デフォルトでは、すべてのユーザーがTenable Vulnerability Managementインスタンスのすべての資産に**アクセスできない**ようになっています。したがって、資産にアクセス権を割り当てる場合は、アクセスグループを作成し、そのグループのユーザー権限を設定する必要があります。

> **注意:** Tenable Vulnerability Management はアクセスグループの範囲にかかわらず、動的タグをあらゆる資産に適用します。結果として、自分が作成したタグが、自分の所属するアクセスグループ外にある資産に適用される場合があります。

企業当たり5,000個までアクセスグループが作成できます。

アクセス許可設定への移行

必要なユーザーロール: 管理者

Tenable は、すべてのアクセスグループを、アクセス許可設定に変換しています。この変換の実行中に、既存のアクセスグループが変更中であることに気づく場合があります。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

Tenable Vulnerability Management は、ユーザーとグループの管理を統合して**アクセス制御**ページに移動し、アクセス管理をより直感的で効率的なものにしました。

その一環として、Tenable Vulnerability Management はアクセスグループを権限に置き換えます。この機能により、アクセス許可設定を作成できます。これらのアクセス許可設定では、タグを使用して、Tenable Vulnerability Management インスタンス上のどのユーザーとグループが、組織のリソースを使用して特定のタスクを実行できるかを決定します。

以前は、アクセスグループを作成して、インスタンス上のユーザーのアクセス設定をカスタマイズする必要がありました。アクセス許可設定を作成すると、ユーザーとグループを管理する **[アクセス制御]** ページで、ユーザーとグループのアクセス設定を表示して管理できます。

Tenable Vulnerability Management では、既存のすべてのアクセスグループがアクセス許可設定に変換され次第、アクセスグループを廃止する予定です。Tenable Vulnerability Management では、アクセス許可設定を使用して、リソースへのユーザーアクセスを管理することを推奨しています。

新しい設定方法について

Tenable Vulnerability Management はアクセスグループデータをアクセス許可設定に変換しますが、それに伴って以下の変更が生じていますのでご注意ください。

- Tenable Vulnerability Management は、複数のアクセスグループタイプがあるアクセスグループを分割して、タイプ別のグループとして再編成します。アクセスグループタイプの詳細については、アクセスグループの種類を参照してください。
- Tenable Vulnerability Management は、すべての **[ターゲットのスキャン]** タイプのアクセスグループを、**[資産の管理]** タイプのアクセスグループに変換します。

- Tenable Vulnerability Management は、タグルールのフィルターと演算子に一致するようにアクセスグループルールフィルターをアップデートします。
- タグではなくルールに基づく、お使いのインスタンス上のアクセスグループについては、Tenable Vulnerability Management は、アクセスグループルールに基づいてタグを作成し、新しいタグを参照するように各グループをアップデートしています。タグルールの詳細については、タグルールを参照してください。
- インストール環境のアクセスグループごとに、Tenable Vulnerability Management は、そのアクセスグループで定義されたルールとユーザーアクセス許可に基づいてアクセス許可設定を作成しています。

同等タスク

次の表に、**[アクセスグループ]** ページで実行可能な一般的なタスクと、**[アクセス許可]** ページ上の同等のタスクを示します。

アクセスグループ	アクセス許可
アクセスグループを作成する	アクセス許可設定の作成および追加
割り当てられたアクセスグループを表示する	アカウントの詳細の表示
アクセスグループを編集する	アクセス許可設定の編集
アクセスグループのユーザーのアクセス許可を設定する	• ユーザーまたはグループへのアクセス許可設定の追加 • ユーザーまたはユーザーグループからアクセス許可設定を削除する
アクセスグループを削除する	アクセス許可設定の削除

アクセスグループをアクセス許可設定に変換する

必要なユーザーロール: 管理者

Tenable は、すべてのアクセスグループを、アクセス許可設定に変換しています。この変換の実行中に、既存のアクセスグループが変更中であることに気づく場合があります。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

[アクセスグループ] ページで、既存のアクセスグループをアクセス許可設定に変換できます。

注意: アクセスグループをアクセス許可設定に変換した場合、変換したアクセス許可設定をアクセスグループに戻すことはできません。

注意: **アクセスグループ**タイルは、1 つ以上のアクセスグループが割り当てられている場合や、自分が管理者であり、Tenable Vulnerability Management のユーザーがアクセスグループに割り当てられている場合にのみ表示されます。すべてのアクセスグループをアクセス許可設定に変換すると、**アクセスグループ**タイルはアカウントに表示されなくなります。

アクセスグループをアクセス許可設定に変換する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルをクリックします。

   [アクセスグループ] ページが表示されます。このページには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. アクセスグループの表で、変換するアクセスグループのチェックボックスを選択します。

   表の上部にアクションバーが表示されます。

5. **[権限へ移行]** をクリックします。

   確認のメッセージが表示されます。

6. 確認ウィンドウで、[→ **[権限へ移行]** をクリックします。

   Tenable Vulnerability Management は、アクセスグループのアクセス許可設定への変換を開始します。

   Tenable Vulnerability Management は、アクセスグループの **[ステータス]** 列を更新して、現在の移行ステータスを表示します。

アクセスグループの種類

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

次の種類のアクセスグループを作成できます。スキャンするターゲットの識別子に基づいて、アクセスグループの種類を選択してください。

タイプ	説明
資産の管理	ユーザーは、以前のスキャン時に作成された資産レコードを表示して、それらの資産に関連するターゲットをスキャンできます。 表示またはスキャンしたいターゲットを過去にスキャンしたことがあり、資産の属性 (たとえばオペレーティングシステムや AWS Account ID など) に基づいたタグによってターゲットを最もよく識別できる場合に、この種類のアクセスグループを使用します。
ターゲットのスキャン	ユーザーは、このアクセスグループに関連付けられたターゲットをスキャンし、そのスキャン結果を表示できます。 表示またはスキャンしたいターゲットを過去にスキャンしたことがなく、特定の資産識別子 (特に FQDN、IPv4 アドレス、または IPv6 アドレス) を使用することでのみターゲットの識別が可能な場合に、この種類のアクセスグループを使用します。

注意: アクセスグループの種類名は、指定されたターゲットに対してユーザーが取ることのできる、各グループが管理するアクションの制限を示すものではありません。**[資産の管理]** と **[ターゲットのスキャン]** グループの両方で、指定されたターゲットの分析結果をダッシュボードに表示するため、または指定されたターゲットをスキャンするため、あるいはその両方を行うためのアクセス許可をユーザーに付与することができます。ユーザーのアクセス許可についての詳細は、アクセスグループのユーザーのアクセス許可を設定するを参照してください。

ヒント: ユーザーに両タイプのスキャンターゲットのスキャンを許可するには、そのユーザーを両方のアクセスグループタイプに追加します。

[すべての資産]グループのユーザーを制限する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

[すべての資産] グループは、システムによって生成されるデフォルトのアクセスグループで、すべての資産が属します。

デフォルトでは、次の条件が真となります。

- **[すべての資産]** グループには、企業内のすべてのユーザーを含む **[すべてのユーザー]** ユーザーグループが割り当てられます。
- **[すべてのユーザー]** グループのアクセス許可として、**[閲覧可]** および **[スキャン可]** が設定されます。

すべてのユーザーがすべての資産をスキャンしたり、個別および集約された結果を表示したりできないようにしたい場合は、**[すべてのユーザー]** グループのアクセス許可を **[アクセスなし]** にする必要があります。その後で特定のユーザーまたはを任意で追加して、すべての資産へのアクセス権を個別に付与することができます。

注意: アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのにある程度の時間を要する場合があります。

[アクセスグループ] ページにあるアクセスグループの表の **[ステータス]** 列で、この割り当てプロセスのステータスを確認できます。

[すべての資産]グループのユーザーのアクセス許可を制限する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルをクリックします。

   [アクセスグループ] ページが表示されます。このページには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. アクセスグループの表で、**[すべての資産]** グループをクリックします。

   [すべての資産アクセスグループを編集] ページが表示されます。

5. **[ユーザーとグループ]** セクションで、**[すべてのユーザー]** グループが表示されている箇所を見つけます。

6. **[すべてのユーザー]** グループの表示から、**[編集可]** と **[スキャン可]** の両方のラベルを削除します。

   a. ラベルにカーソルを合わせます。

      ラベル上に ✕ ボタンが表示されます。

   b. ✕ ボタンをクリックします。

      Tenable Vulnerability Management によりラベルが削除されます。

   注意：[すべてのユーザー] ユーザーグループを設定する際、Tenable では以下に留意するよう推奨しています。

   - **[すべての資産]** のアクセス許可を **[閲覧可]** のままにした場合、すべてのユーザーが企業のすべての資産またはターゲットに対するスキャン結果を表示できます。
   - **[すべての資産]** のアクセス許可を **[スキャン可]** に設定した場合、すべてのユーザーが企業のすべての資産またはターゲットをスキャンし、関連するスキャン結果を表示することができます。

7. (オプション) **[すべての資産]** グループに追加するユーザーまたはグループのそれぞれに対して、ユーザーアクセス許可を設定します。

8. **[保存]** をクリックします。

   [アクセスグループ] ページが表示されます。**[すべての資産]** グループへのアクセスは、追加したユーザーまたはグループに制限されます。

アクセスグループを作成する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

AWS アカウント ID、FQDN、IP アドレス、およびその他の固有の属性を使用し、ルールに基づいてグループ資産へのアクセスグループを作成できます。その後ユーザーまたはユーザーグループにアクセス許可を割り当て、そのアクセスグループで資産を表示またはスキャンすることができます。

アクセスグループを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルをクリックします。

   [アクセスグループ] ページが表示されます。このページには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. ページの右上にある ⊕ **[アクセスグループの作成]** ボタンをクリックします。

   [アクセスグループの作成] ページが表示されます。

5. **[一般]** セクションの **[名前]** ボックスで、アクセスグループの名前を入力します。

   注意: 名前は企業内で一意である必要があります。

6. **[種類]** セクションで、スキャンするターゲットの種類に基づいて、適切なアクセスグループの種類を選択します。

ある種類のアクセスグループを作成した後で、設定の最中にその種類を変更すると、Tenable Vulnerability Management は操作の確認を促すメッセージを表示します。確認すると、Tenable Vulnerability Management はそれまでに追加されたルールのフィルターを消去します。

7. **[ルール]** セクションで、アクセスグループにルールを追加します。

   アクセスグループのルールでは、資産またはターゲットをアクセスグループに含めるかどうかを判断する際に Tenable Vulnerability Management が評価する条件を規定します。

   注意: 1 つのアクセスグループにつき最大 1,000 個のルールを追加できます。

   a. **[カテゴリ]** ドロップダウンボックスで、資産またはターゲットを絞り込むために属性を選択します。

   b. **[演算子]** ドロップダウンボックスで、演算子を選択します。

      たとえば次の演算子があります。

      • **is equal to**: Tenable Vulnerability Management は、指定された語句との完全一致に基づいてルールを資産またはターゲットと照合します。

      注意: Tenable Vulnerability Management では、1 つの IPv4 アドレスを指定するルールに対してはこの演算子を「等しい」と解釈しますが、IPv4 範囲または CIDR 範囲を指定するルールに対しては演算子を「含む」と解釈します。

      • **contains**: Tenable Vulnerability Management は、指定された語句との部分一致に基づいてルールを資産またはターゲットと照合します。

      • **starts with**: Tenable Vulnerability Management は、ルールを指定された語句で始まる資産またはターゲットと照合します。

      • **ends with**: Tenable Vulnerability Management は、ルールを指定された語句で終了する資産またはターゲットと照合します。

   c. テキストボックスで、選択したカテゴリに有効な値を入力します。

      ヒント: 複数の値をコンマで区切って入力できます。**IPV4 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。

d. (オプション) 別のルールを追加するには、⊕ **[追加]** ボタンをクリックします。

> **注意:** アクセスグループに複数のルールを設定した場合、アクセスグループにはいずれかのルールに適合する資産またはターゲットが含まれます。たとえば、**[ネットワーク名]** 属性に適合するルールと、**[IPv4 アドレス]** に適合するルールの 2 つを設定した場合、アクセスグループには指定されたネットワーク内のすべての資産に加えて、指定されたネットワークに属するかどうかに関わらず、指定された IPv4 アドレスを持つすべての資産が含まれます。

8. **[ユーザーとグループ]** セクションで、アクセスグループのユーザーのアクセス許可を設定します。
9. **[保存]** をクリックします。

   Tenable Vulnerability Management によりアクセスグループが作成されます。[**アクセスグループ**] ページが表示されます。

> **注意:** アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのにある程度の時間を要する場合があります。
>
> **[アクセスグループ]** ページにあるアクセスグループの表の **[ステータス]** 列で、この割り当てプロセスのステータスを確認できます。

アクセスグループのユーザーのアクセス許可を設定する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

個別のユーザーまたはユーザーグループに対して、アクセスグループのアクセス許可を設定できます。グループに対してアクセスグループのアクセス許可を設定する場合、グループ内のすべてのユーザーに同じアクセス許可を割り当てます。詳細は、ユーザーグループ を参照してください。

ユーザーまたはユーザーグループに対して、次のアクセスグループのアクセス許可を割り当てることができます。

- **アクセスなし** - (**[すべてのユーザー]** ユーザーグループのみ) (特別にアクセス許可を割り当てたユーザーやグループを除く) すべてのユーザーは、アクセスグループで指定された資産またはターゲットをスキャンできません。またすべてのユーザーは、指定された資産やターゲットに関連する、個別の、または集約されたスキャン結果を表示することもできません。
- **閲覧可** - ユーザーが表示できる、集約されたスキャン結果のビュー (ワークベンチ/ダッシュボード) には、このアクセスグループで指定された資産やターゲットのスキャンデータが含まれます。このアクセス許可をアクセスグループの **[すべてのユーザー]** グループに割り当てた場合、このアクセスグループの資産やターゲットに対する集約されたスキャン結果を、すべてのユーザーが表示できます。
- **スキャン可** - ユーザーは、アクセスグループで指定された資産やターゲットをスキャンしたり、資産やターゲットの個別のスキャン結果を表示したりできます。このアクセス許可がない場合、Tenable Vulnerability Management がこのアクセスグループで指定された資産やターゲットを使用するスキャンの設定を妨げることはありませんが、スキャナーはその資産やターゲットをスキャンしません。このアクセス許可をアクセスグループの **[すべてのユーザー]** グループに割り当てた場合、すべてのユーザーはアクセスグループの資産やターゲットをスキャンしたり、関連する個別のスキャン結果を表示したりできます。

アクセスグループにおけるユーザーのアクセス許可は、階層的ではなく累積的です。ユーザーに対して資産またはターゲットのスキャンを許可し、かつその資産またはターゲットに対する集約された結果の表示も許可するには、アクセスグループでそのユーザーのアクセス許可を、**[閲覧可]** と **[スキャン可]** の両方に設定する必要があります。

ヒント: クラウドインフラを監査するスキャンを実行するには、127.0.0.1 をターゲットとして含む **[ターゲットのスキャン]** アクセスグループを設定し、ユーザーのアクセス許可を **[スキャン可]** に設定します。

アクセスグループのユーザーのアクセス許可を設定する方法

1. アクセスグループを作成または編集します。
2. **[ユーザーとグループ]** セクションで、次のいずれかを行います。

   - **[すべてのユーザー]** ユーザーグループのアクセス許可を編集する。

     [すべてのユーザー] ユーザーグループのデフォルトの値は、アクセスグループに依存します。

     - **[すべてのユーザー]** アクセスグループの場合、Tenable Vulnerability Management は **[すべてのユーザー]** グループに対してデフォルトでは **[閲覧可]** および **[スキャン可]** アクセス許可を割り当てます。Tenable では、初期設定時にこれらのアクセス許可を制限することをお勧めします。
     - 他のすべてのアクセスグループの場合、Tenable Vulnerability Management は **[すべてのユーザー]** グループに対してデフォルトでは **[アクセスなし]** アクセス許可を割り当てます。これらのアクセスグループに対しては、次のように **[すべてのユーザー]** グループのアクセス許可を設定します。

       a. **[すべてのユーザー]** グループ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. **[閲覧可]** をクリックします。

       c. アクセス許可ドロップダウンの横にある ⌄ ボタンをもう一度クリックします。

       d. **[スキャン可]** をクリックします。

       e. **[保存]** をクリックします。

       Tenable Vulnerability Management がすべてのユーザーに対して、グループ内の資産やターゲットの表示やスキャンを許可します。

   - ユーザーをアクセスグループに追加する

     a. 検索ボックスで、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、デフォルトでは**[閲覧可]**アクセス許可が付与された状態でユーザーがアクセスグループに追加され、関連するラベルが表示されているユーザーに追加されます。

c. (オプション) ユーザーに**[スキャン可]**アクセス許可を追加します。

i. ユーザーまたはグループ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。

ii. **[スキャン可]**をクリックします。

Tenable Vulnerability Management により、表示されているユーザーに**[スキャン可]**ラベルが追加されます。

d. **[保存]**をクリックします。

Tenable Vulnerability Management によりユーザーがアクセスグループに追加されます。

- 既存のユーザーにアクセス許可を追加する。

a. 編集するユーザーまたはグループを見つけます。

b. ユーザーまたはグループ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。

c. **[閲覧可]**または**[スキャン可]**を適宜クリックします。

Tenable Vulnerability Management により、表示されているユーザーに新しいアクセス許可を示すラベルが追加されます。

d. **[保存]**をクリックします。

Tenable Vulnerability Management により変更内容がアクセスグループに保存されます。

- 既存のユーザーからアクセス許可を削除する。

a. 編集するユーザーまたはグループを見つけます。

b. 削除する権限を示すラベルの╳ボタン

Tenable Vulnerability Managementをクリックします。により、表示されているユーザーからアクセス許可ラベルが削除されます。

[すべてのユーザー] グループから最後のアクセス許可を削除した場合、Tenable Vulnerability Management はそのグループのアクセス許可を **[アクセスなし]** に設定します。

個別のユーザーまたはグループから最後のアクセス許可を削除した場合、Tenable Vulnerability Management によりそのユーザーをアクセスグループから削除する旨の確認メッセージが表示されます。

- ユーザーをアクセスグループから削除する。

a. 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。

ユーザーまたはグループが **[ユーザーとグループ]** リストから消えます。

b. **[保存]** をクリックします。

Tenable Vulnerability Management により変更内容がアクセスグループに保存されます。

アクセスグループを編集する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

既存のアクセスグループのルールを編集したり、アクセスグループに割り当てられているユーザーとユーザーグループを追加または削除したりできます。

注意: システムによって生成された **[すべての資産]** アクセスグループの名前またはルールを編集することはできません。

アクセスグループを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルをクリックします。

   [アクセスグループ] ページが表示されます。このページには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. アクセスグループの表で、編集するアクセスグループをクリックします。

   [アクセスグループの編集] ページが表示されます。

5. **[一般]** セクションの **[名前]** ボックスで、アクセスグループの新しい名前を入力します。

6. **[種類]** セクションで、アクセスグループの種類を編集します。

   a. 変更後のアクセスグループの種類を選択します。

      Tenable Vulnerability Managementにより操作の確認を促すメッセージが表示されます。

   b. **[確認]** をクリックします。

Tenable Vulnerability Management により、それまでに追加されたルールのフィルターが消去されます。

7. **[ルール]** セクションで、アクセスグループのルールを編集します。

   アクセスグループのルールでは、資産またはターゲットをアクセスグループに含めるかどうかを判断する際に Tenable Vulnerability Management が評価する条件を規定します。

   - 既存のルールを編集するには、必要に応じてカテゴリ、演算子、値を変更します。
   - 既存のルールを削除するには、ルールの横にある ✕ ボタンをクリックします。
   - 新しいルールを追加するには、⊕ **[追加]** をクリックして新しいルールを作成します。

8. **[ユーザーとグループ]** セクションで、アクセスグループのユーザーのアクセス許可を設定します。

9. **[保存]** をクリックします。

   Tenable Vulnerability Management が変更内容をアクセスグループに反映します。**[アクセスグループ]** ページが表示されます。

   > **注意:** アクセスグループを作成または編集するとき、システムの負荷、照合資産の数、脆弱性の数に応じて、Tenable Vulnerability Management が資産をアクセスグループに割り当てるのにある程度の時間を要する場合があります。
   >
   > **[アクセスグループ]** ページにあるアクセスグループの表の **[ステータス]** 列で、この割り当てプロセスのステータスを確認できます。

アクセスグループに割り当てられていない資産を表示する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

資産がどのアクセスグループのルールとも一致しない場合、Tenable Vulnerability Management はその資産をどのアクセスグループにも割り当てません。これらの割り当てられていない資産は、**[すべての資産]** グループのユーザーにのみ表示されます。所属する企業で **[すべての資産]** グループのメンバーシップを制限している場合、**[すべての資産]** グループのメンバーではないユーザーは、これらの割り当てられていない資産を閲覧できません。またユーザーは、このように閲覧が制限されていることをすぐに理解するとは限りません。**[すべての資産]** グループのメンバーであるユーザーは、フィルターを使用してこれらの割り当てられていない資産を特定できます。

アクセスグループに割り当てられていない資産を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンの **[資産ビュー]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。

3. 以下の手順でフィルターを作成します。

   - カテゴリ: **アクセスグループに属する**
   - 演算子: **is equal to**
   - 値: **false**

4. **[適用]** をクリックします。

   資産テーブルが更新され、アクセスグループに割り当てられていないすべての資産が表示されます。

割り当てられたアクセスグループを表示する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

管理者は、すべてのアクセスグループについて、ルールおよびアクセスグループに割り当てられたユーザーとユーザーグループを表示できます。アクセスグループのパラメーターを編集することもできます。

他のすべてのロールのユーザーは、自分に割り当てられたアクセスグループしか表示できません。表示には、各アクセスグループに関連付けられたルールが含まれますが、アクセスグループに割り当てられた他のユーザーまたはユーザーグループは除外されます。アクセスグループの設定を編集することはできません。

注意: **アクセスグループ**タイルは、1 つ以上のアクセスグループが割り当てられている場合や、自分が管理者であり、Tenable Vulnerability Management のユーザーがアクセスグループに割り当てられている場合にのみ表示されます。すべてのアクセスグループを権限設定に変換すると、**アクセスグループ**タイルはアカウントに表示されなくなります。

ユーザーが自分に割り当てられたアクセスグループを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルをクリックします。

   [アクセスグループ] ページが表示されます。このページには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. **[アクセスグループ]** ページには、以下の情報を含む表が含まれています。

- **名前** - アクセスグループ名
- **所有者** - アクセスグループの所有者
- **権限タイプ** - アクセスグループのタイプ
- **最終変更日** - 組織のユーザーがアクセスグループ設定を最後に変更した日付
- **最終変更者** - アクセスグループ設定を最後に変更した組織のユーザー
- **ステータス** - 資産をアクセスグループに一致させる Tenable Vulnerability Management プロセスのステータス可能な値は**進行中**または**完了**です。進行中のプロセスの完了率を表示するには、[進行中] ステータスにカーソルを合わせます。

5. (オプション) 詳細を表示するには、アクセスグループをクリックします。

   [アクセスグループの編集] ページが表示されます。

   管理者の場合、このページにはルールおよび割り当てられたユーザーとユーザーグループが含まれ、すべてのアクセスグループのパラメーターを編集できます。

   他のロールに割り当てられたユーザーの場合、このページにはルールのみが含まれ、ルールの編集はできません。

アクセスグループを削除する

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行 を参照してください。

必要なユーザーロール: 管理者

注意: システム生成の **[すべての資産]** グループは削除できません。

1 つ以上のアクセスグループを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[アクセスグループ]** タイルをクリックします。

   [アクセスグループ] ページが表示されます。このページには、アクセス権を持つアクセスグループを一覧にした表が含まれます。

4. 削除するアクセスグループを選択します。

   - 1 つのアクセスグループを選択します。

     a. アクセスグループの表で、削除するアクセスグループにカーソルを合わせます。

        アクションボタンが行に表示されます。

     b. 🗑 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。

   - 複数のアクセスグループを選択します。

a. アクセスグループの表で、削除するアクセスグループの横にあるチェックボックスを選択します。

   ページの下部またはに、アクションバーが表示されます。

b. アクションバーで、 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。

5. 確認ウィンドウで、**[削除]** ボタンをクリックします。

   Tenable Vulnerability Management により選択されたアクセスグループが削除され、アクセスグループ表が更新されます。

アクセスグループルールのフィルター

Tenable は、アクセスグループを廃止しています。今後も、Tenable では、アクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することや、既存のアクセスグループをアクセス許可設定に変換することを推奨しています。詳細は、アクセス許可設定への移行を参照してください。

アクセスグループのルールを作成するために、次のセクションで説明されているフィルターを使用できます。詳細については、次を参照してください。

- Tenable が提供するフィルター
- Tenable が提供するフィルターのガイドライン
- タグフィルター

Tenable が提供するフィルター

次の表の右端の 2 列は、**[資産の管理]** または **[ターゲットのスキャン]** のグループタイプにフィルターを使用できるかどうかを示します。

フィルター	説明	資産の管理	ターゲットのスキャン
AWS Account ID	資産に関連付けられた Amazon Web Services (AWS) アカウントの正規ユーザー識別子です。詳細は、AWS ドキュメントの「AWS アカウントの識別子」を参照してください。	○	×
AWS 可用性ゾーン	AWS が仮想マシンインスタンスをホストしているアベイラビリティゾーンの名前。詳細は、AWS ドキュメントの「リージョンとアベイラビリティゾーン」を参照してください。	○	×
AWS EC2 AMI ID	Amazon Elastic Compute Cloud (Amazon EC2) での、Linux AMI イメージの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。	○	×

AWS EC2 インスタンス ID	Amazon EC2 での Linux インスタンスの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。	○	×
AWS EC2 名	Amazon EC2 での仮想マシンインスタンスの名前。	○	×
AWS EC2 製品コード	Amazon EC2 での仮想マシンインスタンスの立ち上げに使用された AMI に関連付けられた製品コード。	○	×
AWS リージョン	たとえば 'us-east-1' などの、AWS が仮想マシンインスタンスをホストするリージョン。詳細は、AWS ドキュメントの「リージョンとアベイラビリティゾーン」を参照してください。	○	×
AWS セキュリティグループ	Amazon EC2 で、仮想マシンインスタンスを割り当てたセキュリティグループ。詳細は、Amazon Virtual Private Cloud ユーザーガイドの「セキュリティグループ」を参照してください。	○	×
AWS サブネット ID	スキャン時に仮想マシンインスタンスが動作していた、AWS サブネットの固有識別子。	○	×
AWS VPC ID	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、「Amazon Virtual Private Cloud ユーザーガイド」を参照してください。	○	×
Azure リソース ID	Azure Resource Manager での、リソースの固有識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。	○	×
Azure VM ID	Microsoft Azure 仮想マシンインスタンスの固有識別子。詳細は、Microsoft Azure ドキュメントの「Azure VM Unique ID のアクセスと使用」を参照してください。	○	×
FQDN/Hostname	次のうちのいずれかです。 • 資産の完全修飾ドメイン名 • 資産のホスト名。	○	○

Google Cloud インスタンス ID	Google Cloud Platform (GCP) での、仮想マシンインスタンスの固有識別子。	○	×
Google Cloud プロジェクト ID	GCP で、仮想マシンインスタンスが所属するプロジェクトのカスタマイズされた名前。詳細は、GCP ドキュメントの「プロジェクトの作成と管理」を参照してください。	○	×
Google Cloud ゾーン	GCP で、仮想マシンインスタンスが動作しているゾーン。詳細は、GCP ドキュメントの「リージョンとゾーン」を参照してください。	○	×
IPv4 アドレス	資産の IPv4 アドレス。このフィルターでは、CIDR 表記 (例: 192.168.0.0/24)、範囲 (例: 192.168.0.1-192.168.0.255)、コンマ区切りのリスト (例: 192.168.0.0, 192.168.0.1) を使用できます。	○	○
IPv6 アドレス	資産の IPv6 アドレス。	×	○
MAC アドレス	資産の MAC アドレスです。	○	×
NetBIOS 名	資産の NetBIOS 名。	○	×
ネットワーク名	資産が所属するネットワークの名前です。	○	×
オペレーティングシステム	資産にインストールされているオペレーティングシステム。	○	×
Qualys 資産 ID	Qualys の資産の資産 ID。詳細は、Qualys のドキュメントを参照してください。	○	×
Qualys ホスト ID	Qualys での資産のホスト ID。詳細は、Qualys のドキュメントを参照してください。	○	×
ServiceNow Sys ID	ServiceNow での、資産の固有レコード識別子です。詳細は、ServiceNow のドキュメントを参照してください。	○	×

Tenable が提供するフィルターのガイドライン

- **[ターゲットのスキャン]** アクセスグループのルールを設定する際、資産の属性タイプは、関連するスキャンに使用されるターゲットの形式と一致する必要があります。たとえば、**[ターゲットのスキャン]** アクセスグループのルールが **[FQDN/ホスト名]** 属性でフィルタリングする場合、スキャンターゲットが FQDN またはホスト名の形式で指定されている場合には関連するスキャンは成功しますが、スキャンターゲットが IPv4 形式で指定されている場合には失敗します。

タグフィルター

Tenable Vulnerability Management では、タグにより資産に説明メタデータを追加することで、資産を事業の文脈別にグループに分けることができます。詳細は、タグを参照してください。

作成したタグを使用して、資産を **[資産の管理]** アクセスグループに割り当てることができます。

ルールにタグフィルターを追加する方法

1. **[カテゴリ]** ドロップダウンボックスで、**[タグ]** を選択します。
2. **[演算子]** ドロップダウンボックスで、**[含む]** を選択します。
3. テキストボックスで、検索するタグカテゴリと値を次の形式で入力します。

   ```
   Category Name:Value Name
   ```

4. ルールの作成を続行するか、アクセスグループを作成するの説明に従って、アクセスグループを保存します。

注意: 関連付けられている値が 100,000 以上あるタグカテゴリは、ルールとしてアクセスグループに追加できません。

スキャンのアクセス許可の移行

ユーザーが特定のターゲットをスキャンできるかどうかを制御していた、システムターゲットグループのアクセス許可は、アクセスグループに移行しました。

注意: Tenable は、近い将来にアクセスグループを非推奨にする予定です。現在はまだ、アクセスグループを作成および管理できます。ただし、Tenable では、代わりにアクセス許可を使用して、Tenable Vulnerability Management インスタンス上のリソースへのユーザーアクセスとグループアクセスを管理することを推奨しています。

この移行により、次に示す既存の Tenable Vulnerability Management の設定が影響を受けます。

要素	アクション
既存のアクセスグループ	Tenable Vulnerability Management: • 既存のアクセスグループはすべて、**[資産の管理]** の種類のアクセスグループへと更新されます。 • **[すべてのユーザー]** トグルは、デフォルトの **[すべてのユーザー]** グループで置き換えられます。 • 現在表示のアクセス権を持つ既存のユーザーまたはユーザーグループには、**[閲覧可]** アクセス許可が割り当てられます。
既存のシステムターゲットグループ	既存の各システムターゲットグループに対して、Tenable Vulnerability Management は次を実行します。 • 新たに **[ターゲットのスキャン]** の種類のアクセスグループを作成します。このアクセスグループは、既存のシステムターゲットグループと同じスキャンターゲットを指定します。Tenable Vulnerability Management は移行されたアクセスグループの所有者として、[移行] を表示します。 • システムターゲットグループで **[スキャン可]** アクセス許可を持つすべてのユーザーを新しいアクセスグループに移動し、そのユーザーにそのアクセスグループでの **[スキャン可]** アクセス許可を割り当てます。そのターゲットでの結果をユーザーが表示できるようにするには、そのアクセスグループでユーザーに **[閲覧可]** アクセス許可を設定してください。 **注意:** この移行では、既存のシステムターゲットグループは削除されません。移行により、システムターゲットグループから **[スキャン可]** アクセス許可のみが削除されます。

	注意：移行時に既存のターゲットグループにスキャンのアクセス許可が含まれている場合、新しい Tenable Vulnerability Management ユーザーインターフェースでターゲットグループの表の **[アクセス許可]** 列のグループに **[スキャン]** ラベルが表示される場合があります。このラベルは、過去のスキャンのアクセス許可のみを表します。現在のスキャンのアクセス許可は、アクセスグループで指定されます。
既存のスキャン設定、ダッシュボードフィルター、および保存した検索	既存のスキャン設定は、システムターゲットグループのターゲット設定として維持されます。既存のダッシュボードフィルターおよび保存した検索は、システムターゲットグループのフィルター設定として維持されます。システムターゲットグループの **[アクセス許可]** がある場合、スキャン設定でターゲットグループを指定するために、あるいはダッシュボードおよび検索のフィルターで、そのシステムターゲットグループを使用し続けることができます。ただし、そのターゲットでのスキャン結果を表示できるユーザーを指定するには、適切なアクセスグループで **[Can View]** アクセス許可を設定してください。

言語

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[言語] ページで、Tenable Vulnerability Management コンテナのユーザーインターフェース言語を英語、フランス語、または日本語に変更できます。この設定は、自分のユーザーアカウントにのみ影響します。

ユーザーインターフェース言語を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[言語]** タイルをクリックします。

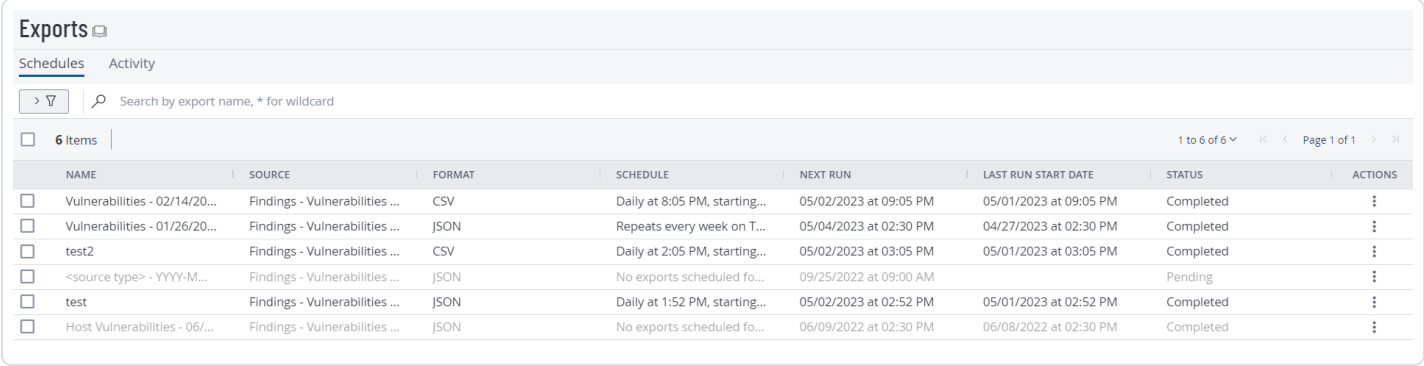
   [言語] タイルが表示されます。

4. **[ユーザーインターフェース言語]** で、設定する言語を選択します。

   Tenable Vulnerability Management は、アカウントのユーザーインターフェースの言語を更新します。

エクスポート

[エクスポート] ページで、[定期エクスポート] および [エクスポートアクティビティ] を表示および設定できます。



このページのエクスポート情報は、次のソースから取得されます。

- **資産** - Tenable Vulnerability Management ライセンス上に含まれるすべての資産に関する情報。詳細は、検出結果または資産のエクスポート を参照してください。
- **資産のホスト** - スキャン中にホスト上で Tenable Vulnerability Management によって特定された資産に関する情報。詳細は、ホスト資産および検出結果または資産のエクスポートを参照してください。
- **検出結果 - 脆弱性 - ホスト** - スキャン中にホスト上で Tenable Vulnerability Management が特定した脆弱性の検出結果に関する情報。詳細は、検出結果または資産のエクスポート を参照してください。
- **ユーザー** - アカウントに割り当てられたユーザーに関する情報。詳細は、ユーザーをエクスポートする を参照してください。

詳細については、以下のトピックを参照してください。

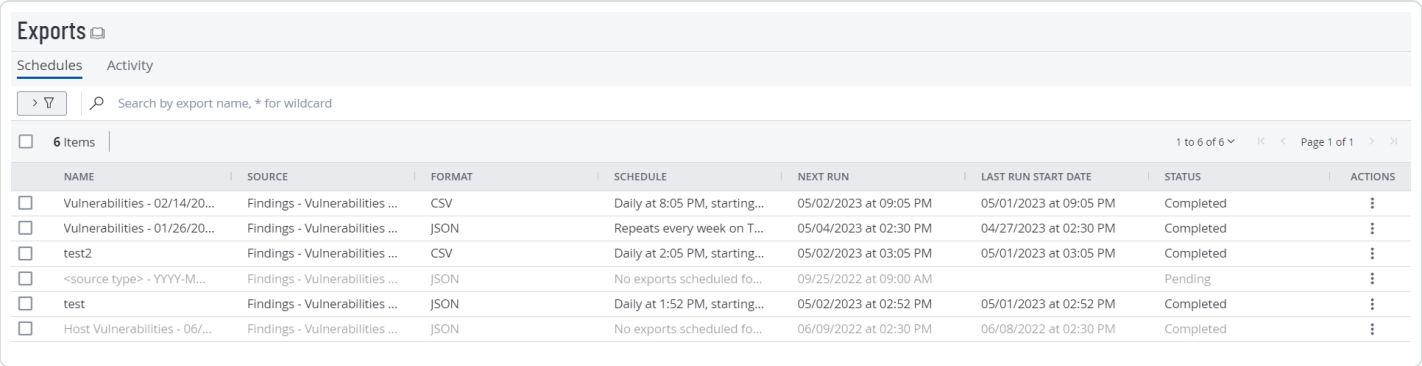
定期エクスポート

[スケジュールされたエクスポート] ページに、スケジュールを含む、アカウント上のエクスポートに関する詳細が表示されます。

> **注意:** Tenable Vulnerability Management インスタンスに保持できるエクスポートスケジュールは、最大 1000 件です。

このページのエクスポート情報は、次のソースから取得されます。

- **資産** - Tenable Vulnerability Management ライセンス上に含まれるすべての資産に関する情報。詳細は、検出結果または資産のエクスポート を参照してください。
- **資産のホスト** - スキャン中にホスト上で Tenable Vulnerability Management によって特定された資産に関する情報。詳細は、ホスト資産および検出結果または資産のエクスポートを参照してください。
- **検出結果 - 脆弱性 - ホスト** - スキャン中にホスト上で Tenable Vulnerability Management が特定した脆弱性の検出結果に関する情報。詳細は、検出結果または資産のエクスポート を参照してください。
- **ユーザー** - アカウントに割り当てられたユーザーに関する情報。詳細は、ユーザーをエクスポートする を参照してください。



[定期エクスポート] ページで、次の操作を実行できます。

- 定期エクスポートを表示する
- 定期エクスポートの無効化

- 無効になっている定期エクスポートの有効化
- 定期エクスポートの削除

注意: エクスポートの有効期限は**[設定]**セクションで設定します。詳細は、全般設定を参照してください。

定期エクスポートを表示する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[エクスポート] ページで、アカウント上のすべての定期エクスポートを表示できます。

注意: Tenable Vulnerability Management インスタンスには、最大 1000 件のエクスポートスケジュールを保持できます。

定期エクスポートを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

スケジュール表

[スケジュール] 表には、定期エクスポートに関する以下の情報が含まれています。

列	説明
名前	定期エクスポートファイルの名前
ソース	Tenable Vulnerability Management の定期エクスポートのデータソース考えられるソースは次のとおりです。 • **資産** - Tenable Vulnerability Management ライセンス上に含まれるすべての資産に関する情報。

	• **資産のホスト** - スキャン中にホスト上で Tenable Vulnerability Management によって特定された資産に関する情報。 • **Findings - Vulnerabilities - Host** - スキャン中にホスト上で Tenable Vulnerability Management が特定した脆弱性の検出結果に関する情報 • **Users** - アカウントに割り当てられたユーザーに関する情報
形式	エクスポートファイルの形式 (CSV または JSON)
スケジュール	エクスポートを実行する日付、時刻、および頻度
Next Run	次にエクスポートを実行するようにスケジュールされている日時
Last Run Start Date	Tenable Vulnerability Management が最後にエクスポートを開始した日時
ステータス	スケジュールされた直近のエクスポートのステータス
アクション	以下のアクションを含む、定期エクスポートで実行できるアクション • 1 つ以上の定期エクスポートを無効にする • 1 つ以上の無効な定期エクスポートを有効にする • 1 つ以上の定期エクスポートを削除する

定期エクスポートの無効化

必要なユーザーロール: 管理者

定期エクスポートを無効にすると、Tenable Vulnerability Management はそのエクスポートスケジュールに基づいてエクスポートを自動的に作成しなくなります。無効になっている定期エクスポートの有効化の説明に従って、無効になっている定期エクスポートを有効にできます。

注意: 定期エクスポートを無効にしても、**[スケジュール]** 表や 1000 件の定期エクスポート制限に対してカウントされるエクスポートのリストからは定期エクスポートが削除されません。アカウントから定期エクスポートを削除するには、定期エクスポートを削除する必要があります。

定期エクスポートを無効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. 次のいずれかを行います。

1 つの定期エクスポートを無効にする場合

a. **[スケジュール]** 表で、無効にする定期エクスポートの行の ⋮ ボタンをクリックします。

   アクションボタンが行に表示されます。

b. その行の ⊘ **[無効化]** ボタンをクリックします。

複数の定期エクスポートを無効にする場合

a. **[スケジュール]** 表で、無効にする各定期エクスポートのチェックボックスを選択します。

> **注意:** 同時に無効にできるエクスポートスケジュールは最大 10 件です。

表の上部にアクションバーが表示されます。

b. アクションバーで、⊘ **[無効化]** ボタンをクリックします。

成功したことを示すメッセージが表示され、

1 つまたは複数の選択済みの定期エクスポートが Tenable Vulnerability Management で無効になります。

[**Schedules**] 表で、無効になっている定期エクスポートがグレーで表示されます。

無効になっている定期エクスポートの有効化

必要なユーザーロール: 管理者

定期エクスポートを無効にしているとき、その定期エクスポートを再度有効にすると、スケジュールで指定されたエクスポート頻度を再開できます。

無効になっている定期エクスポートを有効にするその定期エクスポートを再度有効にすると、スケジュールで指定されたエクスポート頻度を再開できます。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. 次のいずれかを行います。

   ### 1つの定期エクスポートを有効にする場合

   a. **[スケジュール]** 表で、有効にする定期エクスポートの行の ⋮ ボタンをクリックします。

      アクションボタンが行に表示されます。

   b. その行の ✓ **[有効化]** ボタンをクリックします。

   ### 複数の定期エクスポートを有効にする場合

   a. **[スケジュール]** 表で、有効にする無効になっている各定期エクスポートのチェックボックスを選択します。

      注意: 同時に有効にできるエクスポートスケジュールは最大 10 個です。

表の上部にアクションバーが表示されます。

b. アクションバーで、 ✓ **[有効化]** ボタンをクリックします。

成功したことを示すメッセージが表示され、

Tenable Vulnerability Management が、1 つまたは複数の選択済みの定期エクスポートを有効にします。

[**Schedules**] 表で、有効になっている定期エクスポートが黒色で表示されます。

定期エクスポートの削除

必要なユーザーロール: 管理者

[エクスポート] ページで、Tenable Vulnerability Management インスタンスから 1 つ以上の定期エクスポートを削除できます。

注意: 定期エクスポートを削除すると、Tenable Vulnerability Management インスタンスからスケジュールが完全に削除されます。定期エクスポートを一時停止する場合は、スケジュールを無効にします。

定期エクスポートを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. 次のいずれかを行います。

   ### 1 つの定期エクスポートを削除する場合

   a. **[スケジュール]** 表で、削除する定期エクスポートの行の ⋮ ボタンをクリックします。

      メニューが表示されます。

   b. 🗑 **[削除]** ボタンをクリックします。

   ### 複数の定期エクスポートを削除する場合

   a. **[スケジュール]** 表で、削除する各定期エクスポートのチェックボックスを選択します。

      注意: 同時に削除できるエクスポートスケジュールは最大 10 件です。

表の上部にアクションバーが表示されます。

b. アクションバーで、 **[削除]** ボタンをクリックします。

Tenable Vulnerability Management で、1 つまたは複数の選択済みの定期エクスポートが削除されます。削除された定期エクスポートは、[**Schedules**] 表に表示されなくなります。

アクティビティのエクスポート

[アクティビティのエクスポート] タブで、アカウントで作成されたすべてのエクスポートを表示できます。各エクスポートのソース、タイプ、形式、状態、サイズ、作成日、および作成者を確認できます。

注意: エクスポートの有効期限は **[設定]** セクションで設定します。詳細は、全般設定 を参照してください。

注意: デフォルトでは、Tenable Vulnerability Management で保存できるエクスポートデータは一度に最大 500 MB です。この上限に達すると、既存のエクスポートデータの一部を削除するまで、新しいエクスポートを作成できません。エクスポートストレージの上限を引き上げるには、Tenable 担当者に連絡してください。

エクスポートアクティビティを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

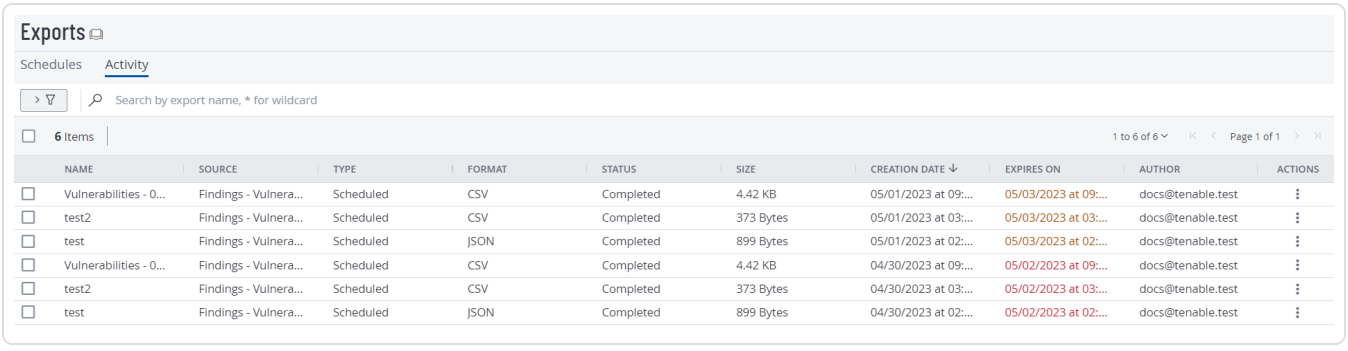
   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. **[アクティビティ]** タブをクリックします。

   [アクティビティ] ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのエクスポートが表示されます。



アクティビティの表

[アクティビティ] の表には、エクスポートに関する以下の情報が含まれています。

列	説明
名前	エクスポートファイルの名前
ソース	Tenable Vulnerability Management のエクスポートのデータソース次のソースが考えられます。 • **Asset** - Tenable Vulnerability Management ライセンスで持っているすべての資産に関する情報。 • **資産のホスト** - スキャン中にホスト上で Tenable Vulnerability Management によって特定された資産に関する情報。 • **Findings - Vulnerabilities - Host** - スキャン中にホスト上で Tenable Vulnerability Management が特定した脆弱性の検出結果に関する情報 • **Users** - アカウントに割り当てられたユーザーに関する情報
タイプ	エクスポートのタイプ (手動または定期エクスポート)
形式	エクスポートファイルの形式 (CSV または JSON)
ステータス	エクスポートのステータス次のステータスが考えられます。 • **Pending** - Tenable Vulnerability Management がエクスポートプロセスを開始しています。 • **Running** - Tenable Vulnerability Management が要求されたファイルを準備しています。 • **Completed** - Tenable Vulnerability Management がエクスポートプロセスを正常に完了しました。エクスポートファイルをダウンロードできます。 • **キャンセル** - Tenable Vulnerability Management がエクスポートプロセスをキャンセルしました。ユーザーが保留中または実行中のエクスポートを停止すると、**[キャンセル]** ステータスになります。 • **Failed** - エクスポートプロセスが失敗しました。
理由	エクスポートの試行が失敗した理由 デフォルトでは、**[理由]** 列は非表示です。列を表に追加する方法については、

	カスタマイズ可能な表を操作するを参照してください。 理由の値は、エクスポートステータスが**[失敗]**の場合にのみ表示されます。
Size	エクスポートファイルのサイズ サイズの値は、エクスポートの状態が**[完了]**の場合にのみ表示されます。
Creation Date	ユーザーがエクスポートを開始した日時
Completion Date	エクスポートプロセスが完了した日時
File Name	CSV または JSON エクスポートファイルの名前
Expires On	エクスポートの有効期限が切れる日時 **注意:** エクスポートの有効期限は**[設定]**セクションで設定します。詳細は、 を参照してください。
作者	エクスポートを開始したユーザー
アクション	以下のアクションを含む、エクスポートで実行できるアクション • エクスポートファイルのダウンロード • 1つ以上のエクスポートの有効期限の更新 • 1つ以上のエクスポートファイルの削除 • エクスポートアクティビティのエクスポート

[アクティビティのエクスポート]ページでは、次のアクションを実行できます。

- エクスポートのフィルタリング
- エクスポートの有効期限の更新
- エクスポートの停止
- エクスポートアクティビティのダウンロード
- エクスポートアクティビティのエクスポート
- エクスポートの削除

注意：エクスポートの有効期限は**[設定]**セクションで設定します。詳細は、を参照してください。

エクスポートのフィルタリング

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

[エクスポート] ページで、Tenable Vulnerability Management インスタンスのエクスポートデータをフィルタリングできます。

エクスポートをフィルタリングする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. (オプション) エクスポートアクティビティのデータをフィルタリングするには、**[アクティビティ]** タブをクリックします。

   [アクティビティ] ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのエクスポートが表示されます。

5. 左上にある ▽ ボタンをクリックします。

   フィルター画面が展開されます。画面には、デフォルトのフィルターオプションのリストが表示されます。

6. **[フィルターの編集]** をクリックします。

   ドロップダウンボックスが表示され、すべてのフィルターオプションが一覧表示されます。

7. 追加または削除するフィルターを選択または選択解除します。使用可能なフィルターの詳細なリストについては、フィルターをエクスポートするを参照してください。

8. フィルターのドロップダウンボックスの外側をクリックします。

ドロップダウンボックスが閉じられます。

9. 選択したフィルターごとに、最初のテキストボックスで演算子を選択します。
10. 2番目のテキストボックスで、フィルターの値を選択または入力します。

    注意: エクスポートに適用するフィルターごとに最大 5 つの異なる値を選択できます。

    注意: 選択したフィルターに汎用的なオプションがある場合、それらのオプションはフィルターの下に表示されます。フィルターに特定の一意の値が必要な場合は、値を入力する必要があります。

    ヒント: フィルターの値を入力する場合、ワイルドカード文字 (*) を使用して、値の任意の場所でテキストのセクションにすることができます。たとえば、フィルターして 1 で終わるすべての値を表示する場合は、*1 と入力します。フィルターして 1 で始まるすべての値を表示する場合は、1* と入力します。最初と最後の文字の間のどこかに 1 があるすべての値をフィルターに含める場合は、*1* と入力します。

11. (オプション) フィルターの値をクリアする方法

    a. クリアするフィルターにカーソルを合わせます。

       フィルターの上にインタラクティブウィンドウが表示されます。

    b. ウィンドウで **[クリア]** をクリックして、フィルターボックスに表示された値を削除します。

       Tenable Vulnerability Management がフィルター値を消去します。

12. (オプション) フィルターを削除する方法

    a. 削除するフィルターにカーソルを合わせます。

       フィルターの上にインタラクティブウィンドウが表示されます。

    b. ウィンドウで **[削除]** をクリックしてフィルターを削除します。

       Tenable Vulnerability Management がフィルターを削除します。

13. **[適用]** をクリックします。

    Tenable Vulnerability Management はエクスポートデータをフィルタリングします。

フィルターをエクスポートする

[エクスポート] ページでは、以下のフィルターを使用してエクスポートデータをフィルタリングできます。

注意: 使用できるフィルターは、エクスポートするデータのタイプによって異なります。

フィルター	データタイプのエクスポート	説明
名前	定期エクスポート、エクスポートアクティビティ	Tenable Vulnerability Management でエクスポートに割り当てた名前。 このフィルターはデフォルトで選択されています。
Size	エクスポートアクティビティ	エクスポートファイルのサイズ(バイト単位) このフィルターはデフォルトで選択されています。
ソース	定期エクスポート、エクスポートアクティビティ	エクスポートが適用される Tenable Vulnerability Management の領域 このフィルターはデフォルトで選択されています。
ステータス	定期エクスポート、エクスポートアクティビティ	エクスポートの現在の状態可能なオプションは次のとおりです。 • **Pending** • **実行中** • **キャンセル** • **Failed** • **完了** このフィルターはデフォルトで選択されています。
作者	エクスポートアクティビティ	エクスポートを作成したユーザー
Completion	エクスポートア	Tenable Vulnerability Management がエクスポートを完了した

Date	クティビティ	日付このフィルターは、ステータスが **[完了]** のエクスポートにのみ適用されます。
Creation Date	定期エクスポート、エクスポートアクティビティ	インスタンスのユーザーがエクスポートを作成した日付
Expires On	エクスポートアクティビティ	エクスポートファイルが期限切れになる時期を示します。フィルター値には、日付、日付範囲、またはエクスポートファイルの有効期限が切れるまでの日数を指定できます。
File Name	エクスポートアクティビティ	エクスポートファイルの名前
形式	定期エクスポート、エクスポートアクティビティ	エクスポートファイルの種類可能なオプションは次のとおりです。 • **CSV** • **JSON**
理由	エクスポートアクティビティ	エクスポートが失敗した理由このフィルターは、状態が **Failed** のエクスポートにのみ適用されます。
Next Run	定期エクスポート	次のエクスポートがスケジュールされている日時。
Last Run Start Date	定期エクスポート	Tenable Vulnerability Management が最後にエクスポートを開始した日時。
最終実行完了日	定期エクスポート	Tenable Vulnerability Management が最後にエクスポートを完了した日時。
作成者	定期エクスポート	エクスポートを作成したユーザー
更新日	定期エクスポート	ユーザーが最後にエクスポートを更新した日時。
Updated By	定期エクス	エクスポートを最後に更新したユーザー。

	ポート	

エクスポートの有効期限の更新

必要なユーザーロール: 管理者

[エクスポート] ページで、Tenable Vulnerability Management インスタンス上のエクスポートの有効期限日を再設定できます。

注意: 一度に有効期限を再設定できるのは 1 つのエクスポートのみです。

ヒント: [全般設定] ページで、デフォルトのエクスポート有効期限を設定することもできます。

エクスポートの有効期限日を再設定する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. **[アクティビティ]** タブをクリックします。

   [アクティビティ] ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのエクスポートが表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. 次のいずれかを行います。

   - エクスポートの表で、有効期限をリセットするエクスポートの行を右クリックします。

     アクションオプションがカーソルの横に表示されます。

- エクスポートの表の **[アクション]** 列で、有効期限をリセットするエクスポートの行にある ⋮ ボタンをクリックします。

  アクションボタンが行に表示されます。

7. **[更新]** をクリックします。

   Tenable Vulnerability Management によって、エクスポートの有効期限が現在の日付から 30 日間に再設定されます。

エクスポートの停止

必要なユーザーロール: 管理者

[エクスポート] ページで、Tenable Vulnerability Management インスタンス上の保留中または実行中の 1 つ以上のエクスポートを停止できます。

注意: 既に完了、キャンセル、または失敗したエクスポートを停止することはできません。

保留中または実行中のエクスポートを停止する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. **[アクティビティ]** タブをクリックします。

   [アクティビティ] ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのエクスポートが表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. 停止するエクスポートを選択します。

停止範囲	アクション
選択したエクスポート	選択したエクスポートを停止する方法 **ヒント:** 最大 10 個のエクスポートを同時に停止できます。 a. エクスポートの表で、停止する各エクスポートのチェックボックスを選択

	します。 表の上部にアクションバーが表示されます。 b. アクションバーで、**[停止]**をクリックします。
1つのエクスポート	1つのエクスポートを停止する方法 a. エクスポートの表で、停止するエクスポートの行を右クリックします。 -または- エクスポートの表の**[アクション]**列で、停止するエクスポートの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[停止]**をクリックします。

エクスポートアクティビティのダウンロード

必要なユーザーロール: 管理者

[エクスポート] ページで、Tenable Vulnerability Management インスタンス上のエクスポートファイルをダウンロードできます。

注意: 一度にダウンロードできるエクスポートファイルは 1 つだけです。

注意: エクスポートファイルをダウンロードできるのは、エクスポートの状態が **Completed** の場合のみです。

エクスポートファイルをダウンロードする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. **[アクティビティ]** タブをクリックします。

   [アクティビティ] ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのエクスポートが表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. 次のいずれかを行います。

   - エクスポートの表で、ダウンロードするエクスポートファイルの行を右クリックします。

     アクションオプションがカーソルの横に表示されます。

- エクスポートの表の **[アクション]** 列で、ダウンロードするエクスポートファイルの行にある ⋮ ボタンをクリックします。

  アクションボタンが行に表示されます。

7. **[ダウンロード]** をクリックします。

   Tenable Vulnerability Management でエクスポートファイルがコンピューターにダウンロードされます。

エクスポートアクティビティのエクスポート

必要なユーザーロール: 管理者

[エクスポート] ページで、Tenable Vulnerability Management インスタンス上のエクスポートアクティビティのデータをエクスポートできます。

エクスポートアクティビティのデータをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。

4. **[アクティビティ]** タブをクリックします。

   [アクティビティ] ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのエクスポートが表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. エクスポートするエクスポートを選択します。

エクスポート範囲	アクション
選択したエクスポート	選択したエクスポートをエクスポートする方法 a. エクスポートの表で、エクスポートする各エクスポートのチェックボックスを選択します。 表の上部にアクションバーが表示されます。

	b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→**[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のエクスポートをエクスポートする場合は、リストにあるすべてのエクスポートを選択して、[→**[エクスポート]** をクリックします。
1 つのエクスポート	1 つのエクスポートをエクスポートする方法 a. エクスポートの表で、エクスポートするエクスポートの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- エクスポートの表の **[アクション]** 列で、エクスポートするエクスポートの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. [→**[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	エクスポートのリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたエクスポートのリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. **[設定]** セクションで、任意のフィールドの横にあるチェックボックスを選択して、エクスポートファイルに含めるフィールドを選択します。テキストボックスを使用してフィールドを検索します。

   選択されたフィールドのみを表示するには、**[選択したフィールドを表示]** をクリックします。

10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  注意: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]** でエクスポートファイルにアクセスできます。

エクスポートの削除

必要なユーザーロール: 管理者

[エクスポート] ページでは、Tenable Vulnerability Management インスタンスから 1 つ以上のエクスポートを削除できます。

注意: エクスポートファイルを削除できるのは、エクスポートの状態が **完了**、**キャンセル**、**失敗** の場合のみです。

エクスポートを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

   左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。
2. 詳細は、Tenable Vulnerability Management ワークベンチの表 を参照してください。
3. **[エクスポート]** タイルをクリックします。

   [エクスポート] ページが表示されます。デフォルトでは、**[スケジュール]** タブがアクティブとなっています。
4. **[アクティビティ]** タブをクリックします。

   [アクティビティ] ページが表示されます。このページの表に、Tenable Vulnerability Management アカウントのすべてのエクスポートが表示されます。
5. (オプション) 表データを選別します。

6. 削除するエクスポートを選択します。

削除範囲	アクション
選択したエクスポート	選択したエクスポートを削除する方法 **ヒント:** 最大 10 個のエクスポートを同時に削除できます。 a. エクスポートの表で、削除する各エクスポートのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、**[削除]** をクリックします。
1 つのエクスポート	1 つのエクスポートを削除する方法 a. エクスポートの表で、削除するエクスポートの行を右クリックします。 -または- エクスポートの表の **[アクション]** 列で、削除するエクスポートの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[削除]** をクリックします。

Tenable Vulnerability Management がアカウントからエクスポートを削除します。

変更/許容ルール

注意: ルールが IP アドレスによって指定される場合、各ネットワーク上で見つかった指定の IP に対してそのルールが適用されます。詳細は、ネットワークを参照してください。

変更ルール

変更ルールを使用して、脆弱性の深刻度を変更できます。ルールが変更された脆弱性は、[検出結果の詳細] ページでそのように識別されます。変更ルールに有効期限を指定した場合、期限切れると、Tenable Vulnerability Management は既存のダッシュボードを元の深刻度に戻します。ただし、過去のスキャン結果は変更されずに残ります。

Tenable Vulnerability Management スタンドアロンをご利用のお客様の場合、変更された深刻度は VPR、CES、AES などのスコアには影響しません。ただし、Tenable One および Tenable Lumin をご利用の場合、変更された深刻度がスコア計算に含まれている場合は、スコアが更新される場合があります。

注意: カスタムスキャンターゲットを変更する場合、Tenable Vulnerability Management は次の資産値のみをサポートします。

- IPv4
- IPv6
- Hostname
- FQDN

たとえば、1 組の内部サーバーを定期的にスキャンする場合があります。これらの内部サーバーは、自己署名された証明書を SSL 接続に対し使用します。証明書が自己署名されているため、スキャンはプラグイン 51192 (「SSL 認証は信頼できません」) の脆弱性を報告します。これは深刻度「中」です。サーバーは自己署名された証明書を使用していることがわかっているため、変更ルールを作成してプラグイン 51192 の深刻度レベルを「中」から「情報」に変更し、その対象を内部サーバーに設定することができます。

ダッシュボードでは変更ルールの影響が反映されます。タグが表示され脆弱性が変更されたことを示します。ルールは、ルールのパラメーターに応じてすべての資産または特定の資産に適用されます。ルールが有効である限り、そのルールは対応するデータとスキャン結果に適用されます。

注意: Tenable Nessus Network Monitor プラグインのルールが変更されている間、元の深刻度は不明になります。

重要:

- **[PCI 四半期外部スキャン]** テンプレートを使用する Tenable PCI ASV スキャンには独自のルールセットがあるため、スキャン結果にはいかなる変更ルールも適用されません。
- Frictionless Assessment コネクタは変更ルールをサポートしていません。

許容ルール

許容ルールを使用すると、プラグインの深刻度レベルを変更せずに脆弱性のリスクを許容することができます。許容した脆弱性は依然としてスキャンによって識別されますが、スキャン結果には表示されません。許容した脆弱性を表示するには、**[変更 / 許容ルール]** フィルターを使用します。許容ルールの有効期限を指定した場合、期限切れと同時に Tenable Vulnerability Management はその脆弱性のリスクを許容しなくなります。ただし、過去のスキャン結果は変更されずに残ります。許容された深刻度は VPR、AES、CES などのスコアには影響しません。

先述の例を考えてみましょう。深刻度レベルを「Medium」から「Information」に変更する代わりに、自己署名証明書の使用に関連するリスクがあることを認め、しかしその脆弱性がサーバーに表示されないようにしたいとします。プラグイン 51192 のリスクを受け入れるよう許容ルールを作成すれば、脆弱性は指定した対象に表示されなくなります。同じ脆弱性がスキャンで別の資産で識別された場合は、その脆弱性は依然としてスキャン結果に表示されます。

Tenable Vulnerability Management により許容ルールの影響が反映されます。許容された脆弱性は非表示となり、[変更 / 許容済み] フィルターを使用して表示できます。

誤検出

さらに、許容ルールを使用して、誤検出をレポートできます。Tenable はプラグインの潜在的な問題を特定するため、報告された誤検出の確認を行っています。

先述の例を再度検討してみます。この場合、対象のサーバーは実際には適切な証明機関の証明書を使用しています。しかし、プラグイン 51192 は引き続きこれらのサーバーの脆弱性を報告します。この誤検出を非表示にし、問題を報告するためには、脆弱性を誤検出として受け入れる許容ルールを作成します。

スキャン履歴の完全性

ルールを変更する場合も許容する場合も、スキャン結果の履歴は変更されません。スキャンを全時間範囲にわたって正確に表示するために、また、スキャン履歴の変更によって内部的または外部的な監査問題が発生することを防ぐために、スキャン履歴は変更不可能になっています。

変更ルールと許容ルールを表示する

必要なユーザーロール: 管理者

[変更/許容ルール] ページには、Tenable Vulnerability Management インスタンスにある設定された変更ルールおよび許容ルールのすべてが表示されます。

[Recast/Accept Rules] ページを表示する方法

1. 左上にある ☰ ボタンをクリックします。

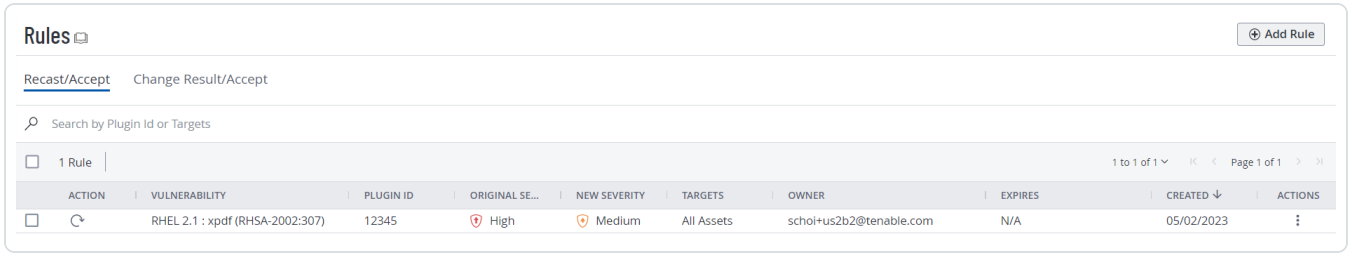
   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[変更]** タイルをクリックします。

   [許容 / 変更ルール] ページが表示されます。このページには、変更ルールをすべて一覧表示する表が含まれています。



変更ルールを作成する

必要なユーザーロール: 管理者

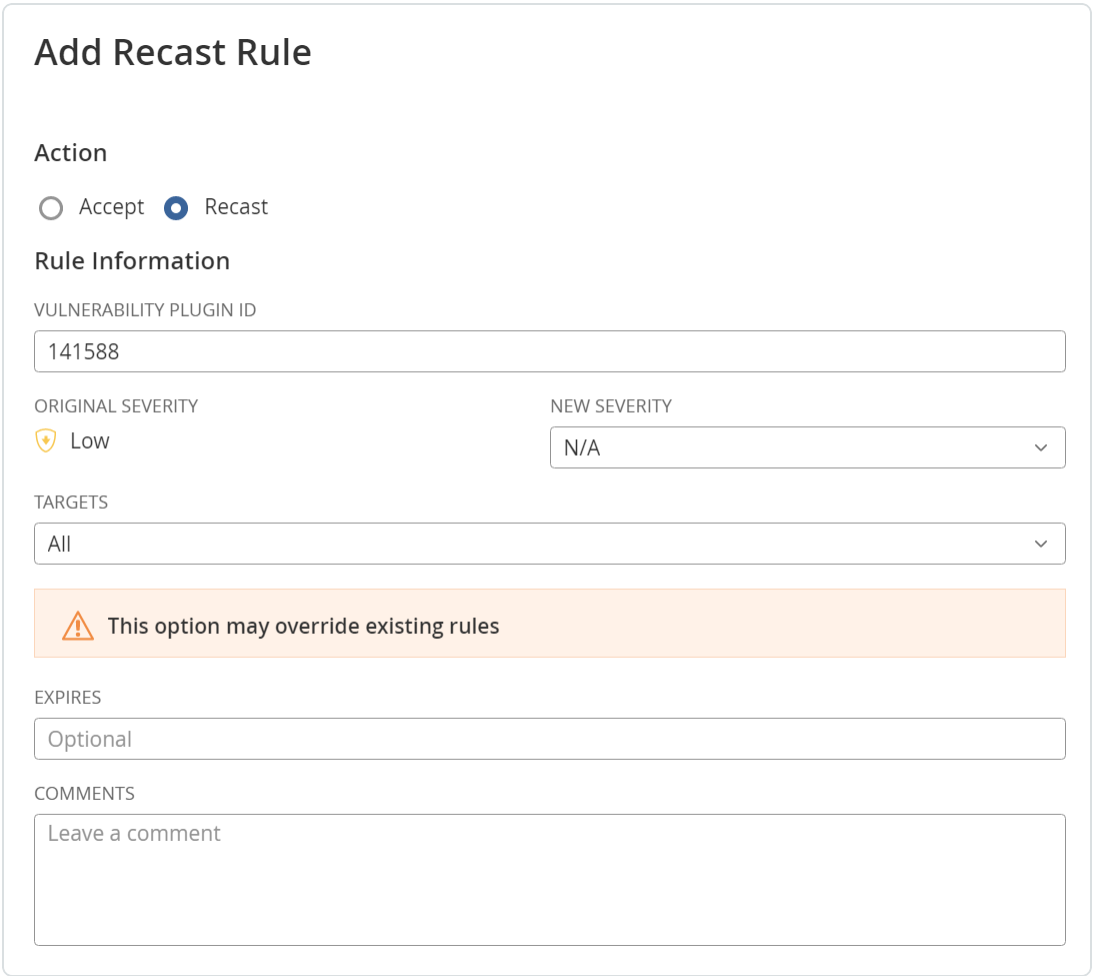
ヒント: 変更ルールを **[脆弱性の詳細]** ページから直接作成することもできます。

重要: 変更/許容ルールの適用にかかる時間は、システムの負荷と一致する脆弱性の数によって異なります。

変更ルールを作成する方法

1. **[変更/許容ルール]** ページを表示します。
2. 左上の ⊕ **[ルールの追加]** ボタンをクリックします。

   [ルールの追加] プレーンが表示されます。



注意: フォームは、ユーザーが **[新しい重大度]** ドロップダウンの **[N/A]** の値を他の値に変更した後にのみ送信できます。

3. **[アクション]** セクションで、**[変更]** を選択します。
4. **[脆弱性]** ボックスに、変更するプラグインの ID を入力します。(たとえば 51192)。

   注意: プラグイン ID が Tenable Nessus プラグインに対応する場合は、**元の深刻度** インジケーターが脆弱性のデフォルトの深刻度に一致するよう変更されます。他のタイプのプラグインを使用する場合、**元の深刻度** インジケーターは変更されません。

5. **[新しい深刻度]** ドロップダウンボックスで、脆弱性の深刻度レベルを選択します。
6. **[ターゲット]** ドロップダウンボックスで、次のいずれかを実行します。

   - すべての資産をターゲットとする場合は、**[すべて]** を選択します。これは既定のターゲットです。

     注意: **[ターゲット]** ドロップダウンが **[すべて]** に設定された場合、このオプションにより既存のルールがオーバーライドされる可能性があることを知らせる警告が表示されます。

   - カスタムの資産のセットをターゲットとする方法

     a. **[カスタム]** を選択します。

     [ターゲットのホスト] ボックスが表示されます。

     b. **[ターゲットのホスト]** ボックスに、このルールの 1 つまたは複数のターゲットを入力します。IP アドレス、IP 範囲、CIDR、ホスト名の任意の組み合わせを含むコンマ区切りリストを入力できます。

     注意: 指定できるコンマ区切りカスタムエントリは 1000 個までとなっています。これよりも多くのカスタムエントリをターゲットにする場合は、複数のルールを作成してください。

7. (オプション) **[有効期限]** ボックスで、ルールの有効期限を設定します。このアクションは、ルールに有効期限を設ける場合のみ必須となります。デフォルトでは、ルールに有効期限はありません。
8. (オプション) **[コメント]** ボックスに、ルールの説明を入力します。このボックスに入力したテキストは、ルールが変更されて機能しない場合にのみ表示されます。
9. **[保存]** をクリックします。

Tenable Vulnerability Management は既存の脆弱性へのルールの適用を開始します。システムの負荷と一致する脆弱性の数によっては、このプロセスに時間がかかる場合があります。変更はダッシュボードに反映され、影響を受けている脆弱性のインスタンスがいくつ変更されたかを示すラベルが表示されます。

注意: 変更ルールによって、スキャンの履歴結果に影響が出ることはありません。

プラグインに対する許容ルールを作成する

必要なユーザーロール: 管理者

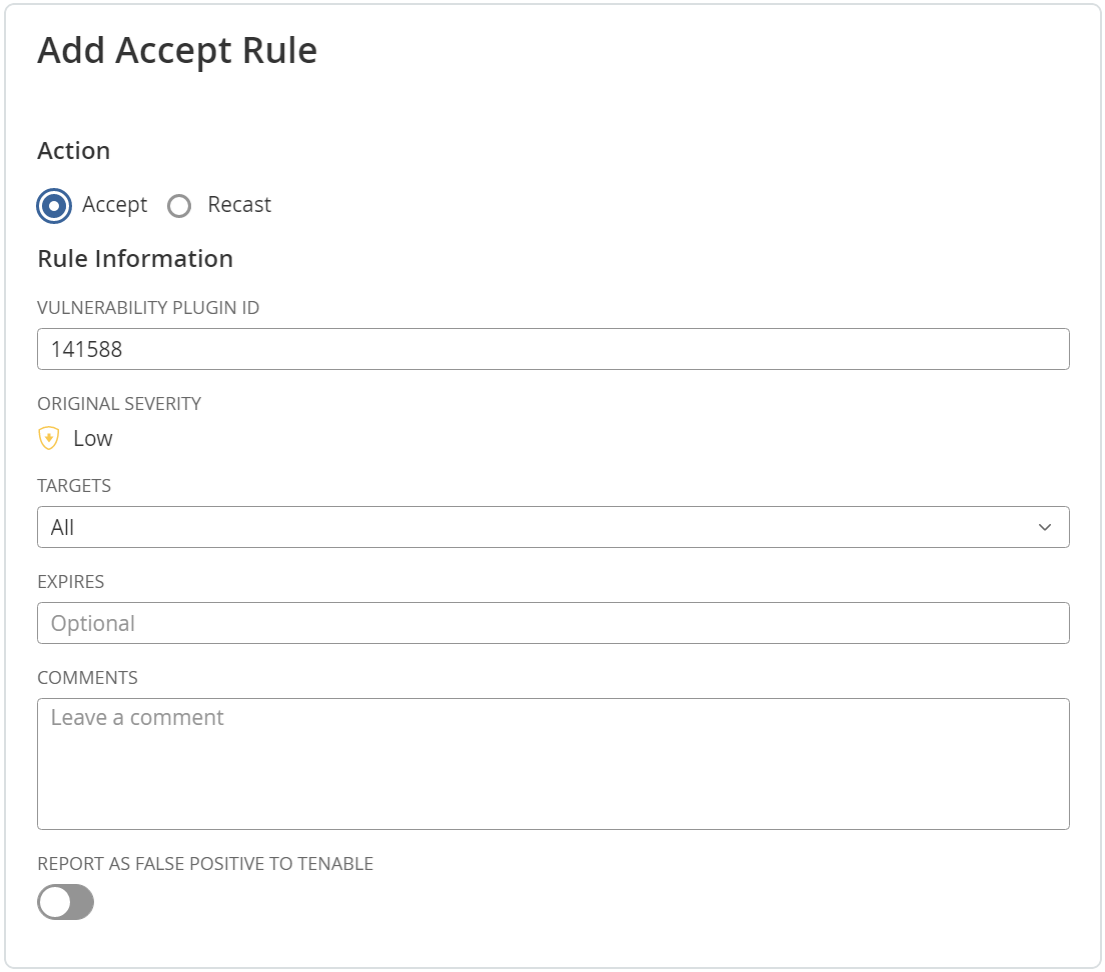
ヒント: 許容ルールを **[脆弱性の詳細]** ページから直接作成することもできます。

重要: 変更/許容ルールの適用にかかる時間は、システムの負荷と一致する脆弱性の数によって異なります。

許容ルールを作成する方法

1. **[変更/許容ルール]** ページを表示します。
2. 左上の ⊕ **[ルールの追加]** ボタンをクリックします。

   [ルールの追加] プレーンが表示されます。



3. **[アクション]** セクションで、**[許容]** を選択します。

4. **[脆弱性]** ボックスに、変更するプラグインの ID を入力します。(たとえば 51192)。

   注意: プラグイン ID が Tenable Nessus プラグインに対応する場合は、**元の深刻度** インジケーターが脆弱性のデフォルトの深刻度に一致するよう変更されます。他のタイプのプラグインを使用する場合、**元の深刻度** インジケーターは変更されません。

5. **[ターゲット]** ドロップダウンボックスで、次のいずれかを実行します。

   - すべての資産をターゲットとする場合は、**[すべて]** を選択します。これは既定のターゲットです。
   - カスタムの資産のセットをターゲットとする方法

     a. **[カスタム]** を選択します。

     [ターゲットのホスト] ボックスが表示されます。

     b. **[ターゲットのホスト]** ボックスに、このルールの 1 つまたは複数のターゲットを入力します。IP アドレス、IP 範囲、CIDR、ホスト名の任意の組み合わせを含むコンマ区切りリストを入力できます。

     注意: 指定できるコンマ区切りカスタムエントリは 1000 個までとなっています。これよりも多くのカスタムエントリをターゲットにする場合は、複数のルールを作成してください。

6. (オプション) **[有効期限]** ボックスで、ルールの有効期限を設定します。このアクションは、ルールに有効期限を設ける場合のみ必須となります。デフォルトでは、ルールに有効期限はありません。

7. (オプション) **[コメント]** ボックスに、ルールの説明を入力します。このボックスに入力したテキストは、ルールが変更されて機能しない場合にのみ表示されます。

8. (オプション) 脆弱性を誤検出として報告する方法

   a. **[誤検出として報告する]** トグルを有効にします。

   [Tenable へのメッセージ] ボックスが表示されます。

   b. **[Tenable へのメッセージ]** ボックスに、Tenable に送信する誤検出の説明を入力します。

9. **[保存]** をクリックします。

   Tenable Vulnerability Management は既存の脆弱性へのルールの適用を開始します。システムの負荷と一致する脆弱性の数によっては、このプロセスに時間がかかる場合があります。影響を受けている脆弱性はワークベンチで非表示になります。

注意: ワークベンチで非表示の脆弱性を表示するには、**[変更 / 許容]** の高度なフィルターを使用します。

変更ルールまたは許容ルールの編集

必要なユーザーロール: 管理者

変更ルールまたは許容ルールを編集する方法

1. **[変更/許容ルール]** ページを表示します。
2. **[変更/許容ルール]** の表で、編集するルールの行をクリックします。

   [ルール] プレーンが表示されます。
3. 必要な変更を行います。

   設定のオプションについての詳細は、変更ルールを作成するまたはプラグインに対する許容ルールを作成するを参照してください。
4. **[保存]** をクリックします。

   Tenable Vulnerability Management が変更をルールに適用します。システムの負荷と対象となる脆弱性の数によって、このプロセスには時間がかかる場合があります。

変更ルールをエクスポートする

必要なユーザーロール: 管理者

[変更/許容ルール] ページでは、1 つ以上の変更ルールを CSV または JSON 形式でエクスポートできます。

変更ルールをエクスポートする場合

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[変更]** タイルをクリックします。

   [許容 / 変更ルール] ページが表示されます。このページには、変更ルールをすべて一覧表示する表が含まれています。

4. (オプション) 表データを選別します。詳細は、表のフィルタリング を参照してください。

5. エクスポートする変更ルールを選択します。

エクスポート範囲	アクション
選択した変更ルール	選択した変更ルールをエクスポートする場合 a. 変更ルールの表で、エクスポートする各変更ルールのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上の変更ルールをエクスポートする場合は、リスト内のすべての変更

	ルールを選択してから、[→**[エクスポート]**をクリックします。
1つの変更ルール	1つの変更ルールをエクスポートする場合 a. 変更ルールの表で、エクスポートする変更ルールの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 変更ルールの表の**[アクション]**列で、エクスポートする変更ルールの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. [→ **[エクスポート]**をクリックします。

[エクスポート]プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]**ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	変更ルールのリストを含むCSVテキストファイル **注意:** .csvエクスポートファイルに=、+、-、@のいずれかの文字で始まるセルが含まれ

	ている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされた変更ルールのリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]** でエクスポートファイルにアクセスできます。

変更ルールまたは許容ルールを削除する

必要なユーザーロール: 管理者

変更ルールまたは許容ルールを削除する方法

1. **[変更/許容ルール]** ページを表示します。
2. 削除するルールを選択します。
   - 1つのルールを選択する場合
     a. **[変更/許容ルール]** の表で、削除するルールの行にカーソルを合わせます。
     b. 行の右側にある 🗑 ボタンをクリックします。

     [変更ルールを削除する] の確認メッセージが表示されます。
   - 複数のルールを選択する場合
     a. **[変更/許容ルール]** の表で、削除するルールの横にあるチェックボックスを選択します。

     ページの下部またはに、アクションバーが表示されます。
     b. アクションバーで、🗑 ボタンをクリックします。

     [変更ルールを削除する] の確認メッセージが表示されます。
3. **[削除]** をクリックします。

   Tenable Vulnerability Managementは選択したルールを削除します。Tenable Vulnerability Management では、システムの負荷と一致する脆弱性の数によって、既存の脆弱性からルールを削除するのに時間を要する場合があります。

タグ

Tenable Vulnerability Management で記述メタデータを資産にタグ付けすることで、資産に独自の事業の文脈を追加できます。資産タグは、主に *カテゴリ:値* のペアで設定されます。たとえば、資産を場所ごとにグループ化する場合は、*[場所]* というカテゴリを作成し、その値を *Headquarters* にできます。その後、個々の資産に手動でタグを適用するか、ルールをタグに追加して Tenable Vulnerability Management が一致する資産に自動的にタグを適用するようにできます。

タグ構造の詳細については、タグの形式と適用を参照してください。

注意: 個別のカテゴリを使用せずにタグを作成する場合、Tenable では、すべてのタグに使用できる汎用カテゴリの *[カテゴリ]* を追加することを推奨しています。

タグを利用して資産に独自の事業の文脈を付加することで、分析ビューをタグでフィルタリングすることが可能になります。

タグを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

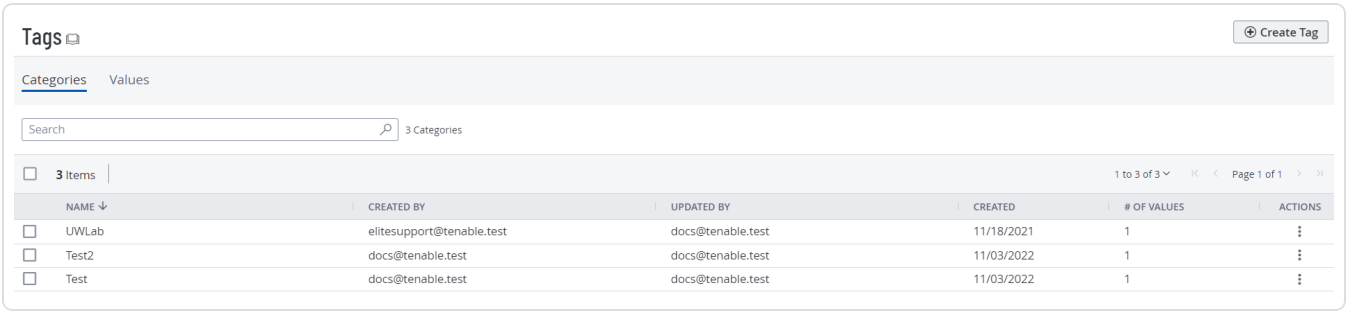
2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。



4. 次のいずれかを行います。

Tenable Vulnerability Management インスタンス上のすべてのタグに割り当てられたカテゴリを表示する方法

a. **[カテゴリ]** 表で、タグカテゴリとそれに関連するデータを確認できます。

列	説明
名前	タグの名前
作成者	タグを作成したユーザーのユーザー名
最終使用者	タグの値またはカテゴリを最後に作成または編集したユーザーのユーザー名
作成日	タグが作成された日付
値の数	当該タグカテゴリに関連付けられているタグ値の数
アクション	タグで実行できるアクション

Tenable Vulnerability Management インスタンス上のすべてのタグを表示する方法

a. **[値]** タブをクリックします。

[値] ページが開き、Tenable Vulnerability Management インスタンス上のすべてのタグの表が表示されます。

b. **[値]** 表で、タグとそれらに関連するデータを確認できます。

列	説明
名前	タグの名前
作成者	タグを作成したユーザーのユーザー名
更新者	タグのカテゴリまたは値を最後に更新したユーザーのユーザー名
作成日	タグが作成された日付
適用方法	タグの適用が**手動**または**自動**で行われるかを示します

最終処理日時	Tenable Vulnerability Management によって最後にスキャン処理が行われ、関連するすべての資産に適用した日時
評価	Tenable Vulnerability Management が特定を終了し、一致するすべての資産にタグを適用したかどうかを示します
アクション	タグで実行できるアクション

例: 資産のタグ付け

一般的なユースケースとして、次の資産のタグ付けの設定例を確認してください。タグについての一般的な情報は、タグを参照してください。

- 例: インストール済みソフトウェア別に自動でタグ付けする
- 例: 優先度によって手動でタグ付けする

例: インストール済みソフトウェア別に自動でタグ付けする

あなたの会社では、Oracle と Wireshark の、2 種類のソフトウェア上で動作する資産を管理しています。会社はソフトウェアの種類に基づいて、資産の所有者のアクセス許可を従業員に割り当てます。従業員は、自身が管理するソフトウェアの種類の資産上に認められた、脆弱性を解決する義務があります。

管理者ユーザーであるあなたは、両方のソフトウェアの種類に対する動的タグを作成できます。そうすることで、従業員は**[インストール済みのソフトウェア]**タグを使用して資産を検索し、自身が管理するソフトウェアの種類によって Tenable Vulnerability Management 資産をフィルタリングできます。

> **注意:** より厳密な結果を得るためには、タグの値を該当する NVD 共通プラットフォーム一覧 (CPE) に合わせて設定します。例: `cpe:/a:microsoft:office`

インストール済みソフトウェア別に自動で資産にタグ付けする方法

1. 次の設定を使用して、Oracle 資産のタグを作成して自動的に適用します。

オプション	値
カテゴリ	*インストール済みのソフトウェア*
値	*Oracle*
ルール	以下のルールを指定して有効にします。 • **すべてに一致** • **カテゴリ**: *インストール済みのソフトウェア* • **演算子**: *次の値に等しい*: • **値**: *Oracle*

2. 次の設定を使用して、Wireshark 資産のタグを作成して自動的に適用します。

オプション	値
カテゴリ	*インストール済みのソフトウェア*
値	*Wireshark*
ルール	以下のルールを指定して有効にします。 • **すべてに一致** • **カテゴリ**: *インストール済みのソフトウェア* • **演算子**: *次の値に等しい*: • **値**: *Wireshark*

3. 従業員に、新しいタグを使用して資産の表で資産をフィルタリングするか、タグの表から資産を検索するように指示します。

例: 優先度によって手動でタグ付けする

あなたの会社には機密性の高い資産があり、従業員にはそれらの資産の脆弱性を、資産の他の属性(たとえば資産の VPR)に関わらず最優先で対処してほしいとします。

従業員がそれらの機密性の高い資産を最初に表示し、対応することを確実にするため、**[高優先度]**タグを作成して、従業員に優先してほしい資産に手動で追加できます。そうすることで、従業員は**[高優先度]**タグを使用して、自身が管理する最優先の資産でフィルタリングし、資産を検索できます。

優先度によって資産に手動でタグ付けする方法

1. 次の設定を使用して、最優先の資産のタグを作成します。

オプション	値
カテゴリ	*優先度*
値	*高優先度*
値の説明	このタグを持つ資産の脆弱性修復の緊急度に関するカスタムの説明です。

2. 最優先の資産に、タグを手動で適用します。
3. 従業員に、新しいタグを使用して資産の表で資産をフィルタリングするか、タグの表から資産を検索するように指示します。

タグの形式と適用

資産タグは、主に *カテゴリ:値* のペアで設定されます。たとえば、資産を場所ごとにグループ化する場合は、*[場所]* というカテゴリを作成し、その値を *Headquarters* にできます。

> **注意:** 個別のカテゴリを使用せずにタグを作成する場合、Tenable では、すべてのタグに使用できる汎用カテゴリの *[カテゴリ]* を追加することを推奨しています。

次の場合に、タグメンバーシップが再評価されます。

- タグを更新または作成する場合
- Tenable Vulnerability Management がデータをインポートする場合
- 12 時間ごと

手動タグと自動タグ

タグを作成すると、Tenable Vulnerability Management により、タグルールに一致するインスタンス上の資産に、そのタグが自動的に適用されます。これらの自動的に適用されるタグは、*動的タグ*と呼ばれることもあります。自動タグを作成すると、Tenable Vulnerability Management が、現在のすべての資産と、企業のアカウントに新しく追加された資産にそのタグを適用します。Tenable Vulnerability Management はまた、資産の属性に変更がないか定期的に確認し、その結果に応じて自動タグを追加または削除します。

> **注意:** 自動タグを作成または編集する場合、システムの負荷や対象資産の数によっては、Tenable Vulnerability Management がタグを既存の資産に適用するのに時間を要する場合があります。

ルールなしでタグを作成し、個別の資産に手動で適用することもできます。または、自動タグを、そのタグのルール基準を満たさない可能性のある他の資産に手動で適用することもできます。これらの手動で適用されるタグは、*静的タグ*と呼ばれることもあります。

手動タグは アイコンで表示され、自動タグは アイコンで表示されます。

説明については、以下の例を参照してください。

シナリオ	タグのタイプ	タグアイコン
カテゴリ:値 ペアに *Location:Headquarters* を指定してタグを作成しますが、タグ	手動	

ルールは追加しません。後で、そのタグを本社 (headquraters) にある資産に追加します。		
カテゴリ: *値* ペアを *Location*: *Headquarters* にしてタグを作成し、タグルールで IP アドレス範囲を指定します。これにより Tenable Vulnerability Management によって、その IP アドレス範囲内にあるすべての既存の資産または新規の資産に、このタグが自動的に適用されます。	自動	

手動タグまたは自動タグの作成

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

注意: **[タグ付け]** ページでタグを作成する場合は、汎用資産フィルターのリストから選択してタグルールを作成できます。特定の資産タイプに固有のフィルターに基づいてタグを作成する場合、Tenable は、**[資産]** ページでタグを作成することを推奨しています。[資産] ページでは、各資産タイプに固有の追加のフィルターを選択できます。

タグを適用できない場合、タグルールから返される資産が多過ぎて Tenable Vulnerability Management で処理できない可能性があります。たとえば、ワイルドカードを含む完全修飾ドメイン名 (FQDN) の長いリストには、多数の資産が含まれます。この状況が発生した場合、Tenable では、より厳密なタグルールを使用して資産の数を減らすことを推奨しています。必要に応じて、追加のタグを使用して各リストを結合できます。

[タグを作成] ページで、手動タグを作成して資産に個別に適用できます。Tenable Vulnerability Management が一致する資産を識別してタグ付けする際に使用するタグルールを作成することで、自動タグを作成することもできます。

注意: 最大 100 個のタグカテゴリを作成でき、各カテゴリには最大 100,000 個のタグを含めることができます。

[タグ] ページで自動タグを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

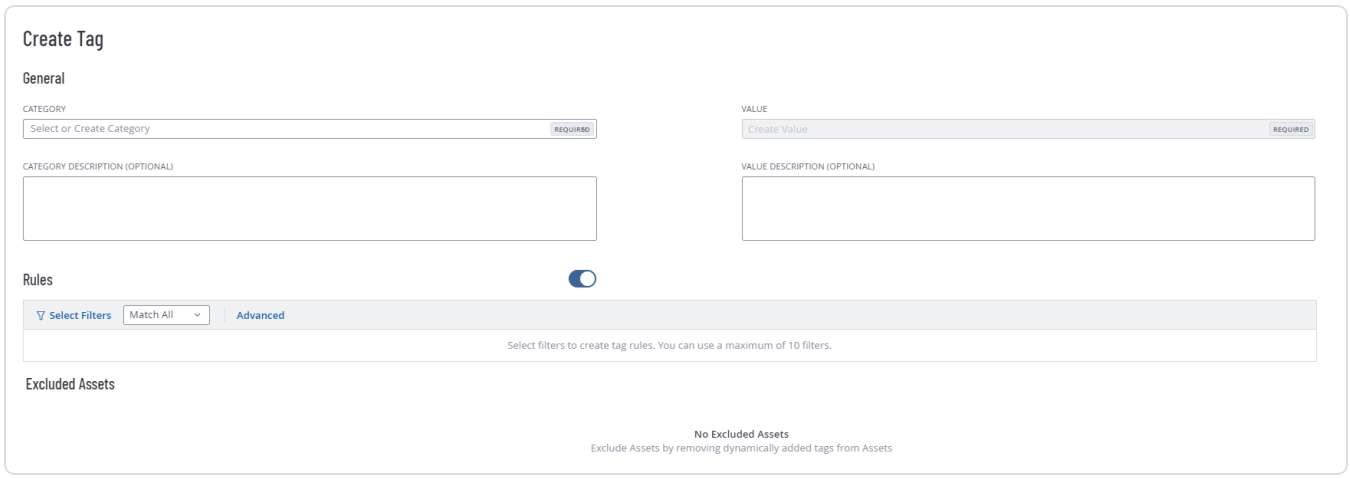
3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. ページの右上にある ⊕ **[タグの作成]** ボタンをクリックします。

   [タグの作成] ページが表示されます。



5. **[カテゴリ]** ドロップダウンボックスをクリックします。

6. **[新しいカテゴリの追加]** ボックスにカテゴリを入力します。

   入力に伴って、リストでは一致が絞り込まれます。

7. ドロップダウンボックスから既存のカテゴリを選択するか、新しいカテゴリの場合は **["*カテゴリ名*"の作成]** をクリックします。

   注意: Tenable Vulnerability Management インスタンスでは最大 100 個のカテゴリを作成できます。

8. (オプション) **[カテゴリの説明]** ボックスに、タグカテゴリの説明を入力します。

9. **[値]** ボックスに、タグの名前を入力します。

   注意: タグ名は、コンマを含めず 50 文字以内にしてください。

   ヒント: Tenable では、タグカテゴリに直接対応するタグ名を指定することを推奨しています。たとえば、カテゴリが *[場所]* の場合は、「*Headquarters*」が適切な値になります。

10. (オプション) **[値の説明]** ボックスに、新しいタグの説明を入力します。

11. 次のいずれかを行います。

    タグを手動タグとして保存する方法

    a. **[保存]** をクリックします。

       Tenable Vulnerability Management によって、タグがタグの表に保存されます。

    b. (オプション) 1 つ以上の資産に手動でタグを追加します。

タグを保存して自動的に適用する方法

a. タグルールを作成します。

b. **[保存]**をクリックします。

Tenable Vulnerability Management は、タグを作成して、既存の資産を評価し、タグルールに一致する資産にタグを自動的に適用します。

> **注意:** 自動タグを作成する場合、システムの負荷や資産の数によっては、Tenable Vulnerability Management がタグを適用し、除外された資産を更新するのに数分かかる場合があります。

ルール付きのタグに関する考慮事項

自動での適用

Tenable Vulnerability Management は次の状況のとき、タグルールに照らして資産を評価します。

- 新しい資産が(スキャン経由、コネクタによるインポート、または Tenable Vulnerability Management API を活用して)追加されると、Tenable Vulnerability Management は資産をタグルールに照らして評価します。
- タグルールが作成または更新されると、Tenable Vulnerability Management はそのタグルールに照らして資産を評価します。

  > **注意:** タグルールを作成または編集すると、システムの負荷や対象資産の数によっては、Tenable Vulnerability Management がタグを既存の資産に適用するのに時間を要する場合があります。

- 既存の資産が更新されると、Tenable Vulnerability Management は資産を再評価し、資産の属性がタグルールに一致していない場合は、そのタグを削除します。

手動による適用

ルール付きで設定されたタグを手動で適用すると、Tenable Vulnerability Management は以後、そのルールに基づく評価からその資産を除外します。

タグルール

タグルールを使用すると、Tenable Vulnerability Management は作成されたタグを、タグルールに一致するインスタンス上の資産に自動的に適用します。これらの自動的に適用されるタグは、*動的タグ*または*自動タグ*と呼ばれています。

タグルールは、資産属性に基づく 1 つ以上のフィルターと値のペアで設定されます。ルールを作成してタグに追加すると、Tenable Vulnerability Management が、タグルールに一致するインスタンス上のすべての資産にそのタグを適用します。

> **注意:** Tenable Vulnerability Management は、タグごとに最大 1,000 のルールをサポートします。この制限は、1 つのタグ値に対して最大 1,000 個の **and** または **or** 条件を指定できることを意味します。さらに、Tenable Vulnerability Management は、個別のタグルールごとに最大 1,024 個の値をサポートします。

自動タグに関する詳細は、タグの形式と適用を参照してください。

[タグ] セクションで、タグルールを使用して次のタスクを実行できます。

- タグルールの作成
- タグルールの編集
- タグルールの削除

タグルールの作成

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

タグを作成または編集して自動的に適用する場合は、ルールを作成し、タグルールフィルターを通してタグに適用する必要があります。タグルールは、**[基本]** モードまたは **[詳細]** モードのいずれかで作成できます。

注意: タグルールを **[基本]** モードで作成してから **[詳細]** モードに切り替えると、作成したルールは **[詳細]** モードの形式で表示されます。ただし、**[詳細]** モードから **[基本]** モードに切り替えた場合は、Tenable Vulnerability Management によりルールセクションからすべてのルールが削除されます。

注意: **[タグ付け]** ページでタグを作成する場合は、汎用資産フィルターのリストから選択してタグルールを作成できます。特定の資産タイプに固有のフィルターに基づいてタグを作成する場合、Tenable は、**[資産]** ページでタグを作成することを推奨しています。[資産] ページでは、各資産タイプに固有の追加のフィルターを選択できます。

タグの自動適用に関する詳細は、ルール付きのタグに関する考慮事項を参照してください。

始める前に

- タグを作成または編集します。

ルールを作成してタグに追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[値]** タブをクリックします。

[値] ページが開き、Tenable Vulnerability Management インスタンス上のすべてのタグの表が表示されます。

5. ルールの設定を有効にするには、**[ルール]** トグルをクリックします。

   [ルール] セクションが表示されます。

6. 作成するタグルールごとに、次のいずれかを実行します。

   注意: デフォルトでは **[基本]** モードがアクティブになっています。

   ## [基本] モードでタグルールを作成する方法

   a. **[ルール]** セクションで、**[フィルターの選択]** をクリックします。

      ドロップダウンボックスが開き、タグルールフィルターオプションが一覧表示されます。

      注意: タグルールフィルターによって、1 つのフィルターに適用可能な値の数の上限が異なります。これらの制限の詳細については、タグルールフィルターを参照してください。

   b. フィルターを選択します。

      選択したフィルターが **[ルール]** セクションに表示されます。

   c. ドロップダウンボックスの外側をクリックします。

      ドロップダウンボックスが閉じられます。

   d. フィルターで、 ボタンをクリックします。

      フィルターが展開されます。

   e. 1 つ目のドロップダウンボックスで、フィルターに適用する演算子を選択します。

   f. 2 つ目のドロップダウンボックスで、フィルターの値を 1 つ以上選択または入力します。

   g. (オプション) 別のルールを作成するには、**[基本]** モードでタグを作成する手順を繰り返します。

   h. (オプション) 別のルールを作成する方法

i. **[基本]** モードでタグルールを作成する手順を繰り返します。

ii. **[ルール]** セクションの **[いずれかに一致]** ドロップダウンボックスで、次のいずれかを実行します。

- いずれかのルールに一致する資産にタグを適用するには、**[いずれかに一致]** を選択します。

  OR 演算子が各ルールの間に表示され、Tenable Vulnerability Management はそのタグに指定されたルールのいずれかを満たす資産にタグを適用します。

- すべてのルールに一致する資産のみにタグを適用するには、**[すべてに一致]** を選択します。

  各ルールの間に **AND** 演算子が表示されます。

  Tenable Vulnerability Management は、そのタグに指定されたすべてのルールを満たす資産にのみタグを適用します。

[詳細] モードでタグルールを作成する方法

a. **[ルール]** セクションで、**[詳細]** をクリックします。

テキストボックスが表示されます。

b. テキストボックス内にカーソルを置きます。

ドロップダウンボックスが開き、タグルールフィルターオプションが一覧表示されます。

> **注意:** タグルールフィルターによって、1 つのフィルターに適用可能な値の数の上限が異なります。これらの制限の詳細については、タグルールフィルターを参照してください。

> **注意:** タグルールに誤字が含まれていた場合は、問題の説明を含むエラーが **[ルール]** ボックスに表示されます。

c. 適用するフィルターを選択または入力します。

> **ヒント:** 矢印キーを使用してフィルタードロップダウンボックス内を移動し、**Enter** キーを押してオプションを選択できます。

フィルターがテキストボックスに表示されます。

フィルターの右側に演算子のドロップダウンボックスが表示されます。

d. 次の演算子のいずれかを選択します。選択できる演算子は、選択したフィルターに応じて異なります。

> **注意:** (') または (") で始まる値や (*) または (,) を含む値でフィルタリングする場合は、値を引用符 (") で囲む必要があります。

演算子	説明
存在する	選択されたフィルターが存在するアイテムを表示します。
存在しない	選択されたフィルターが存在しないアイテムを表示します。
次の値に等しい	フィルター値に一致するアイテムを表示します。
次の値に等しくない	フィルター値を含まないアイテムを表示します。
次の値より大きい **次の値以上**	指定されたフィルター値より大きい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以上]** 演算子を使用します。
次の値より小さい **次の値以下**	指定されたフィルター値より小さい値のアイテムを表示します。フィルターで指定した値を含める場合は、**[次の値以下]** 演算子を使用します。

演算子	説明
直近	今日より前の数時間、数日、数か月、または数年以内の日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
後	指定されたフィルター値より後の日付のアイテムを表示します。
前	指定されたフィルター値より前の日付のアイテムを表示します。
経過	今日より前の数時間、数日、数か月、または数年が経過した日付のアイテムを表示します。数値を入力してから、時間の単位を選択します。
日付	指定された日付のアイテムを表示します。
期間	指定された 2 つの日付間のアイテムを表示します。
次の値を含む:	指定されたフィルター値を含むアイテムを表示します。
次の値を含まない:	指定されたフィルター値を含まないアイテムを表示します。
ワイルドカード	次のように、ワイルドカード (*) でアイテムを絞り込みます。 • **次で始まるまたは終わる** - 指定したテキストで始まるまたは終わる値を表示します。たとえば、「1」で始まるすべての値を見つけるには、*1** と入力します。「1」で終わるすべての値を見つけるには、**1* と入力します。 • **次の値を含む** - 指定したテキストを含む値を表示します。たとえば、最初と最後の文字の間のどこかに「1」があるすべての値を見つける場合は、**1** と入力します。 • **大文字と小文字の区別をオフにする** - 大文字と小文字を区別せずに値を表示します。たとえば、**プラグイン名** が「TLS バージョン 1.2 プロトコル検出」*または*「tls バージョン 1.2 プロトコル検出」である検出結果を検索するには、**tls バージョン 1.2 プロトコル検出*と入力します。

演算子の右側にフィルターの値を選択または入力します。

> **ヒント:** 一部のテキストフィルターは、フィルター値内のテキストのセクションを表すワイルドカードとして文字 (*) をサポートしています。たとえば、フィルターして 1 で終わるすべての値を表示する場合は、*1 と入力します。フィルターして 1 で始まるすべての値を表示する場合は、1* と入力します。
>
> ワイルドカード演算子を使用して、特定のテキストを含む値を表示することができます。たとえば、最初と最後の文字の間のどこかに 1 があるすべての値を表示するようにフィルターを掛ける場合は、*1* と入力します。

e. (オプション) 複数のタグのルールを作成する方法

i. **Space** キーを押します。

修飾子ドロップダウンボックスが開き、**AND And** と **OR Or** がオプションとして表示されます。

ii. 修飾子を選択します。

iii. **Space** キーを押します。

ドロップダウンボックスが開き、タグルールフィルターオプションが一覧表示されます。

iv. **[詳細]** モードでタグルールを作成する手順を繰り返します。

7. **[保存]** をクリックします。

Tenable Vulnerability Management が、ルールを作成してタグに適用します。

タグルールの編集

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

自動タグを作成した後、**[値の編集]** ページでタグに適用するルールを編集できます。

注意: [タグ付け] ページでルールを編集する場合は、汎用資産フィルターのリストから選択してタグルールを作成できます。ただし、特定の資産タイプ (ウェブアプリケーション資産など) に固有のフィルターを追加する場合、Tenable では、**[資産]** ページでタグを編集することを推奨しています。[資産] ページでは、各資産タイプに固有のフィルターを選択できます。

始める前に

- 自動タグを作成します。

タグルールを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[値]** タブをクリックします。

   [値] ページが開き、Tenable Vulnerability Management インスタンス上のすべてのタグの表が表示されます。

5. タグの表で、タグルールを編集するタグをクリックします。

   [値の編集] ページが表示されます。

ヒント: **[値]** 表で確認するタグをクリックすれば、**[カテゴリの編集]** ページから **[値の編集]** ページに移動することもできます。

6. ルールの設定を有効にするには、**[ルール]** トグルをクリックします。

   [ルール] セクションが表示されます。

7. **[ルール]** セクションで、編集するルール[フィルター]にある ⌄ 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、そのフィルターに対して以前に選択したルール値の一覧が表示されます。

   注意: 1 つのタグルールに適用できるフィルターは最大 10 個です。

8. (オプション) 1 つ目のドロップダウンボックスで、新しい演算子を選択します。

9. (オプション) 2 つ目のボックスで、ルール値を追加または削除します。

   注意: ルールフィルターに選択可能なオプション (日付範囲など) がある場合は、それらのオプションがフィルターの下に表示されます。そうでない場合は、値を入力する必要があります。

10. ルールドロップダウンボックスの外側をクリックします。

    ドロップダウンボックスが閉じられます。

11. **[保存]** をクリックします。

    Tenable Vulnerability Management が、変更内容を保存して、既存の資産を評価し、更新されたタグルールに一致する資産にタグを自動的に適用します。

    注意: システムの負荷や資産の数によっては、Tenable Vulnerability Management が資産にタグを適用し、のに時間を要する場合があります。

タグルールの削除

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

自動タグから 1 つのルールが削除されると、Tenable Vulnerability Management はそのタグルールに一致するすべての資産からそのタグを削除します。自動タグからすべてのルールを削除すると、そのタグは手動タグになります。

タグルールを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[タグ]** ページで、**[値]** タブをクリックします。

   [値] ページが開き、Tenable Vulnerability Management インスタンス上のすべてのタグを含む表が表示されます。

5. タグの表で、タグルールを削除するタグをクリックします。

   [値の編集] ページが表示されます。

   > **ヒント:** **[値]** 表で確認するタグをクリックすれば、**[カテゴリの編集]** ページから **[値の編集]** ページに移動することもできます。

6. **[ルール]** セクションで、削除するルールの ✕ ボタンをクリックします。

   ルールが **[ルール]** セクションに表示されなくなります。

7. **[保存]**をクリックします。

   Tenable Vulnerability Management が変更を保存して適用します。

タグルールフィルター

注意: タグルールに誤字が含まれていた場合は、問題について説明したエラーが **[ルール]** ボックスに表示されます。

注意: Tenable Vulnerability Management は、タグごとに最大 1,000 のルールをサポートします。この制限は、1 つのタグ値に対して最大 1,000 個の **and** または **or** 条件を指定できることを意味します。さらに、Tenable Vulnerability Management は、個別のタグルールごとに最大 1,024 個の値をサポートします。

[タグ] ページで、以下のフィルターから選択して自動タグのルールを作成できます。

フィルター	説明
アカウント ID	資産をホストするクラウドサービスの資産リソースに割り当てられた一意の識別子。
ACR	(Tenable Lumin ライセンスが必要) 資産の ACR (資産重大度の格付け) です。
ACR 深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された ACR の ACR カテゴリ。
AES	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES (資産のエクスポージャースコア)。
AES の深刻度	(Tenable Lumin のライセンスが必要) 資産に対して計算された AES の AES カテゴリ。
エージェント名	資産をスキャンして特定した、Tenable Nessus エージェントの名前。
ARN	資産の Amazon リソース名 (ARN)。
ASN	資産の自律システム番号 (ASN)。
[評価済み] と [検出済み]	Tenable Vulnerability Management が資産の脆弱性をスキャンしたかどうか、または Tenable Vulnerability Management が検出スキャンで資産を検出しただけかどうかを指定します。可能な値は次のとおりです。 • **評価済み** • **検出済みのみ**

資産 ID	資産の UUID。
AWS 可用性ゾーン	AWS が仮想マシンインスタンスをホストしているアベイラビリティゾーンの名前。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS EC2 AMI ID	Amazon Elastic Compute Cloud (Amazon EC2) での、Linux AMI イメージの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 インスタンス ID	Amazon EC2 での Linux インスタンスの固有識別子。詳細は、Amazon Elastic Compute Cloud ドキュメントを参照してください。
AWS EC2 名	Amazon EC2 での仮想マシンインスタンスの名前。
AWS EC2 製品コード	Amazon EC2 での仮想マシンインスタンスの立ち上げに使用された AMI に関連付けられた製品コード。
AWS インスタンスの状態	AWS での仮想マシンインスタンスのスキャン時の状態。可能な値については、Amazon Elastic Compute Cloud ドキュメントの API インスタンスの状態を参照してください。
AWS インスタンスタイプ	Amazon EC2 での仮想マシンインスタンスのタイプ。Amazon EC2 のインスタンスタイプは、インスタンスの仕様を決定します (たとえば、どのくらいの RAM を持つか)。可能な値の一覧は、AWS ドキュメントの Amazon EC2 インスタンスタイプを参照してください。
AWS 所有者 ID	仮想マシンインスタンスを作成した Amazon AWS アカウントの UUID。詳細は、AWS ドキュメントの AWS アカウント ID を参照してください。 この属性は、Amazon EC2 インスタンスのみに対して値を持ちます。他の資産タイプに対しては、この属性は空となります。
AWS リージョン	たとえば `us-east-1` などの、AWS が仮想マシンインスタンスをホストするリージョン。詳細は、AWS ドキュメントのリージョンとアベイラビリティゾーンを参照してください。
AWS セキュリティグループ	Amazon EC2 インスタンスに関連付けられた AWS セキュリティグループ (SG)。

AWS サブネット ID	スキャン時に仮想マシンインスタンスが動作していた、AWS サブネットの固有識別子。
AWS VPC ID	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、Amazon Virtual Private Cloud ユーザーガイドを参照してください。
Azure リソースグループ	Azure Resource Manager でのリソースグループの名前。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソース ID	Azure Resource Manager での、リソースの固有識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure リソースタイプ	Azure Resource Manager でのリソースのリソースタイプ。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure サブスクリプション ID	Azure Resource Manager でのリソースの固有サブスクリプション識別子。詳細は、Azure Resource Manager のドキュメントを参照してください。
Azure VM ID	Microsoft Azure 仮想マシンインスタンスの固有識別子。詳細は、Microsoft Azure ドキュメントの Azure VM Unique ID のアクセスと使用を参照してください。
BIOS ID	資産の NetBIOS 名。
クラウドプロバイダー	資産をホストするクラウドプロバイダーの名前。
作成日	Tenable Vulnerability Management が資産レコードを作成した日時。
カスタム属性	カテゴリと値のペアを使用してカスタム属性を検索するフィルター。カスタム属性の詳細については、Tenable 開発者ポータルを参照してください。
削除	資産が削除済みかどうかを指定します。
Deleted Date	ユーザーが資産レコードを削除した日付、またはユーザーが資産を削除してからの日数。ユーザーが資産レコードを削除した場合、Tenable Vulnerability Management は資産のライセンスカウントが期限切れとなるまで、そのレコードを保持します。
DNS (FQDN)	資産ホストの完全修飾ドメイン名。 **注意:** これは、**[名前]** フィルターを使用する必要があるウェブアプリケーション資

	産には適用されません。
ドメイン	ソースとして追加されたドメイン、またはアタックサーフェス管理によってユーザーに属するものとして検出されたドメイン。
初回確認日	スキャンが最初に資産を特定した日時。
Google Cloud インスタンス ID	Google Cloud Platform (GCP) での、仮想マシンインスタンスの固有識別子。
Google Cloud プロジェクト ID	GCP で、仮想マシンインスタンスが所属するプロジェクトのカスタマイズされた名前。詳細は、GCP ドキュメントのプロジェクトの作成と管理を参照してください。
Google Cloud ゾーン	GCP で、仮想マシンインスタンスが動作しているゾーン。詳細は、GCP ドキュメントのリージョンとゾーンを参照してください。
プラグインの結果有り	資産が関連付けられたプラグイン結果を持つかどうかを指定します。
ホスト名 (ドメインインベントリ)	アタックサーフェス管理スキャン中に検出された資産のホスト名。ドメインインベントリ資産でのみ使用されます。
ホスティングプロバイダー	資産のホスティングプロバイダー。
IaC リソースタイプ	資産のインフラのコード化 (IAC) リソースタイプ。
インストール済みのソフトウェア	スキャンにより資産上に存在が確認されたソフトウェアアプリケーションを表す、共通プラットフォーム一覧 (CPE) の値。このフィールドは CPE 2.2 形式に対応します。詳細は、CPE 仕様書バージョン 2.2 の Component Syntax セクションを参照してください。Tenable スキャンで特定された資産に関して、このフィールドは、Tenable Nessus プラグイン ID 45590 を使用するスキャンが資産を評価した場合にのみ値を持ちます。 **注意:** アプリケーションが検出された最初のスキャンから 30 日の間に、そのアプリケーションを検出するスキャンがなかった場合、Tenable Vulnerability Management はそのアプリケーションの検出を期限切れとみなします。その結果、次にその資産をスキャンで評価する際、Tenable Vulnerability Management は期限切れとなったアプリケーションを **[インストール済みソフトウェア]** 属性から削除します。このアクティビティは、削除の種類の属性変更として

	資産アクティビティログに記録されます。
IPv4 アドレス	資産レコードに関連付けられた IPv4 アドレスです。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します (例: hostname_example, example.com, 192.168.0.0)。IP アドレスには、個別のアドレス、CIDR 表記 (例: 192.168.0.0/24)、または範囲 (例: 192.168.0.1-192.168.0.255) を指定できます。 **注意:** CIDR マスクの /0 はすべての IP アドレスに適合するため、このパラメーターではサポートされていません。このパラメーターに値 /0 を指定すると、Tenable Vulnerability Management は 400 Bad Request エラーメッセージを返します。 **注意:** タグフィルターの値が終止符 (.) で終わらないようにしてください。
IPv6 アドレス	スキャンにより資産レコードと関連付けられた IPv6 アドレス。 このフィルターは、コンマ区切りのリストによる複数の資産識別子に対応します。IPV6 アドレスは完全に一致する必要があります (例: 0:0:0:0:0:ffff:c0a8:0)。 **注意:** タグフィルターの値が終止符 (.) で終わらないようにしてください。
属性	資産が属性であるかどうかを指定します。
自動スケール	資産を自動的にスケーリングするかどうかを指定します。
サポートなし	Tenable Vulnerability Management で資産がサポートされていないかどうかを指定します。
最終監査日	資産が最後に監査された日時。
最終認証スキャン日	資産に対する認証スキャンが実行された直近の日時。検出プラグインのみを使用する認証スキャンでは、**[最終認証スキャン日]** フィールドは更新されますが、**[最終ライセンススキャン日]** フィールドは更新されません。
最終ライセンススキャン日	資産が「ライセンス済み」と見なされ、Tenable のライセンス制限にカウントされた最後のスキャンの日時。ライセンススキャンでは、非検出プラグインが使

	用され、脆弱性を特定できます。非検出プラグインを実行する非認証スキャンでは、**[最終ライセンススキャン日]** フィールドは更新されますが、**[最終認証スキャン日]** フィールドは更新されません。ライセンスのある資産に関する詳細は、Tenable Vulnerability Management のライセンスを参照してください。
最終確認日	資産を特定した直近のスキャンの日時。
ライセンス済み	資産が Tenable Vulnerability Management インスタンスの資産カウントに含まれるかどうかを規定します。
MAC アドレス	スキャンにより資産レコードと関連付けられた MAC アドレス。
最後に検出された緩和策	資産の軽減ソフトウェアを識別した直近のスキャン日時。
名前	特定の資産属性の存在に基づいて Tenable Vulnerability Management によって次の順序で割り当てられる資産識別子です。 1. エージェント名 (エージェントスキャンの場合) 2. NetBIOS 名 3. FQDN 4. IPv6 アドレス 5. IPv4 アドレス たとえばスキャンによって、ある資産に対して NetBIOS 名と IPv4 アドレスが特定された場合、NetBIOS 名が資産名として表示されます。
NetBIOS 名	資産の NetBIOS 名。
ネットワーク	資産を特定したスキャナーに関連付けられているネットワークオブジェクトの名前。デフォルトの名前は **Default** です。詳細は、ネットワークを参照してください。
開いているポート	資産のポートを開きます。
オペレーティングシステム	スキャンにより資産にインストールされていると特定されたオペレーティングシステム。

ポート	資産に関連付けられているポート。
パブリック	資産がパブリックネットワークで使用可能かどうかを指定します。
レコードタイプ	資産タイプ。
リージョン	資産が実行されるクラウドリージョン。
リポジトリ	資産に関連付けられているコードリポジトリ。
リソースカテゴリ	クラウドリソースタイプが属するカテゴリの名前 (オブジェクトストレージや仮想ネットワークなど)。
リソースタグ (キー別)	Amazon Web Services (AWS) などのクラウドソースから同期された、タグキー (Name など) と一致するタグ。
リソースタグ (値別)	Amazon Web Services (AWS) などのクラウドソースから同期された、タグ値と一致するタグ。
リソースタイプ	資産のクラウドリソースタイプ (ネットワーク、仮想マシンなど)。
ServiceNow Sys ID	該当する場合、ServiceNow での資産の固有レコード識別子。詳細は、ServiceNow のドキュメントを参照してください。
ソース	資産を特定したスキャンのソース。可能なフィルター値は次のとおりです。 • AWS • AWS FA • Azure • AZURE FA • Cloud Connector • Cloud IAC • クラウドランタイム • GCP • Nessus Agent • Nessus Scan

	• NNM • ServiceNow • WAS
SSL/TLS	資産がホストされているアプリケーションが SSL/TLS 公開鍵暗号化を使用するかどうかを指定します。
システムの種類	プラグイン ID 54615 によりレポートされたシステムの種類。詳細は、Tenable プラグインを参照してください。
タグ	タグのペア (カテゴリ: 値) を検索する一意のフィルター。タグの値を入力するときは、コロン (:) の後にスペースを入れて、「*カテゴリ: 値*」という構文を使用する必要があります。値を区切るためにコンマ (,) を使用できます。タグ名にコンマが含まれている場合は、コンマの前にバックスラッシュ (\) を挿入します。最大 100 個のタグを追加できます。 詳細については、タグを参照してください。 **注意:** タグ名に二重引用符 (" ") が含まれている場合は、代わりに UUID を使用する必要があります。
ターゲットグループ	資産が所属するターゲットグループ。資産がターゲットグループに所属していない場合、この属性は空になります。詳細は、ターゲットグループを参照してください。
Tenable ID	資産に存在するエージェントの UUID。
終了	資産が終了しているかどうかを指定します。
タイプ	資産が管理されているシステムのタイプ。可能なフィルター値は次のとおりです。 • **クラウドリソース** • **コンテナ** • **ホスト** • **クラウド**

更新日	ユーザーが資産を最後に更新した日時。
VPC	AWS 仮想マシンインスタンスをホストするパブリッククラウドの固有識別子。詳細は、Amazon Virtual Private Cloud ユーザーガイドを参照してください。

資産フィルターを使用したタグの作成

必要なユーザーロール: 管理者

資産をフィルタリングする時に、フィルターをタグルールとして使用して、新しい自動タグを作成できます。

タグを作成すると、Tenable Vulnerability Management はそれらのフィルターで特定された資産にタグを自動的に適用します。

[タグ付け] ページから資産の手動タグまたは自動タグを作成することもできます。

資産フィルターを使用してタグを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

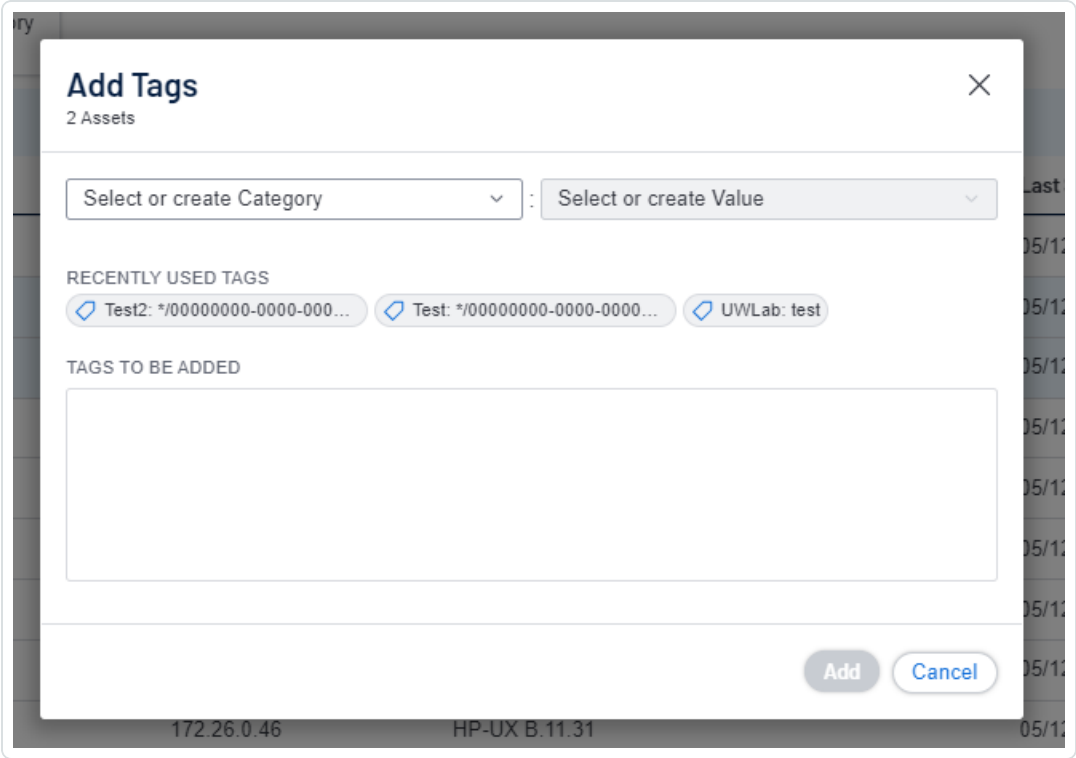
   [資産] ページが表示されます。

3. 表をフィルタリングします。この時、タグに追加またはタグから削除するルールに応じて、フィルターを選択および選択解除します。

   選択したフィルターは、フィルター画面の上にあるヘッダーに表示されます。

4. ヘッダーで、最初のフィルターの左側にある 🏷 **[タグの追加]** ボタンをクリックします。

   [タグの追加] ウィンドウが表示されます。



5. **[タグの作成 / 選択]** の最初のドロップダウンボックスにカテゴリを入力します。

   入力に伴って、リストでは一致が絞り込まれます。

6. ドロップダウンボックスから既存のカテゴリを選択するか、カテゴリを新規作成する場合は [***"カテゴリ"*** **の作成**] をクリックします。

   ヒント: 汎用タグカテゴリを作成してさまざまなタグ値に適用すると、タグをグループ化できます。たとえば、*[場所]* カテゴリを作成し、*Headquarters* や *Offshore* などの複数の値に適用すると、場所タグのグループを作成できます。

7. **[タグの作成 / 選択]** の 2 番目のドロップダウンボックスに新しいタグの値を入力します。

8. ドロップダウンボックスで、**[*"値"* の作成]** をクリックします。

9. **[保存]** をクリックします。

   Tenable Vulnerability Management によってタグが保存され、アカウントの該当する資産に適用されます。

   注意: Tenable Vulnerability Management が対象の資産にタグを適用するには最大で数分かかる場合があります。

タグまたはタグカテゴリの編集

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

[タグ付け] セクションで、タグの 1 つ以上の設定要素を編集できます。これには、タグが属しているカテゴリ、タグの名前と説明、およびタグに適用されているルールが含まれます。

タグまたはタグカテゴリを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. 個別のタグを編集する方法

   a. **[タグ]** ページで、**[値]** タブをクリックします。

      [値] ページが開き、Tenable Vulnerability Management インスタンス上のすべてのタグを含む表が表示されます。

   b. **[値]** 表で、編集するタグをクリックします。

      [値の編集] ページが表示されます。

      > **ヒント:** **[値]** 表で確認するタグをクリックすれば、**[カテゴリの編集]** ページから **[値の編集]** ページに移動することもできます。

   c. (オプション) **[値]** ボックスで、タグ名を編集します。

   d. (オプション) **[値の説明 (オプション)]** ボックスで、タグの説明を編集します。

e. (オプション) タグルールを設定します。

5. タグカテゴリを編集する方法

注意: タグカテゴリを編集すると、Tenable Vulnerability Management はそのタグカテゴリ内のすべてのタグのカテゴリを変更します。

a. タグカテゴリの表で、編集するカテゴリをクリックします。

[カテゴリの編集] ページが表示されます。

b. タグカテゴリの表で、編集するカテゴリをクリックします。

[カテゴリの編集] ページが表示されます。

c. (オプション) 名前を編集するには、**[カテゴリ]** ボックスに新しい名前を入力します。

d. (オプション) 説明を編集するには、**[カテゴリの説明]** ボックスに新しい説明を入力します。

6. **[保存]** をクリックします。

Tenable Vulnerability Management が変更を保存して適用します。

資産フィルターを使用したタグの編集

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

[資産] ページでは、資産フィルターを使用してタグのルール、カテゴリ、値を編集できます。

資産フィルターを使用してタグを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

3. 表をフィルタリングします。この時、タグに追加またはタグから削除するルールに応じて、フィルターを選択および選択解除します。

   適用したフィルターは、フィルター画面の上にあるヘッダーに表示されます。

4. ヘッダーで、最初のフィルターの左側にある 🏷 ボタンをクリックします。

   [資産と一致するタグ] ウィンドウが表示されます。

5. 次のいずれかを行います。

   - 最後に使用したタグを編集する場合

     a. **[最近使用したタグ]** で、編集するタグをクリックします。

     タグカテゴリが **[カテゴリを選択または作成する]** ドロップダウンボックスに表示されます。

     タグの値が **[値を選択または作成する]** ドロップダウンボックスに表示されます。

   - 他のタグを編集する場合

a. **[カテゴリを選択または作成する]**ドロップダウンボックスにカテゴリ名を入力します。

入力に伴って、リストでは一致が絞り込まれます。

b. 編集するタグのカテゴリを選択します。

c. **[値を選択または作成する]**ドロップダウンボックスに値名を入力します。

入力に伴って、リストでは一致が絞り込まれます。

d. ドロップダウンボックスから編集するタグの値を選択します。

6. (オプション) タグカテゴリを編集する方法

a. **[カテゴリを選択または作成する]**ドロップダウンボックスにカテゴリの新しい名前を入力します。ドロップダウンボックスに

["*カテゴリ*" の作成] が表示されます。

b. ドロップダウンボックスから **["*カテゴリ*" の作成]** を選択します。

ドロップダウンボックスに新しいカテゴリ名が選択された状態で表示されます。

7. (オプション) タグの値を編集する方法

a. **[値を選択または作成する]**ドロップダウンボックスにタグの新しい値を入力します。ドロップダウンボックスに

["*値*" の作成] が表示されます。

b. ドロップダウンボックスから **["*値*" の作成]** を選択します。

ドロップダウンボックスに新しい値名が選択された状態で表示されます。

8. (オプション) **[タグ用の選択した検索フィルター]** ボックスで、タグから削除するフィルター内にある ✕ をクリックします。

9. **[保存]** をクリックします。

Tenable Vulnerability Management で編集が保存されます。

タグの資産への追加

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する使用可アクセス許可

タグを作成すると、Tenable Vulnerability Management インスタンスの 1 つ以上の資産に手動で適用できます。

タグを資産に追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

3. 資産リストを表示します。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. 次のいずれかを行います。

   ### 1 つの資産にタグを追加する方法

a. タグを追加するページを選択します。

場所	アクション
[資産] ページ	**[資産]** ページからタグを追加する方法 a. 資産の表で、タグを追加する資産の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 資産の表の **[アクション]** 列で、タグを追加する資産の ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[タグの追加]** をクリックします。
[資産の詳細] ページプレビュー画面	**[資産の詳細]** ページからタグを追加する方法 a. 資産の表で、タグを追加する資産の行をクリックします。 資産の **[資産の詳細]** ページのプレビュー画面が表示されます。 b. プレビュー画面の左側の **[タグ]** の横にある ⊕ ボタンをクリックします。
[資産の詳細] ページ	**[資産の詳細]** ページからタグを追加する方法 a. タグを削除する資産の **[資産の詳細]** ページを表示します。 **[資産の詳細]** ページが表示されます。 b. 右上の **[アクション]** ボタンをクリックします。

	アクションメニューが表示されます。 c. アクションメニューで、[**タグの追加**] をクリックします。 -または- ページの左側の **[タグ]** の横にある ⊕ ボタンをクリックします。

[タグの追加] ウィンドウが表示されます。

b. **[追加]** をクリックします。

資産の表が表示されます。確認のメッセージが表示されます。Tenable Vulnerability Management は、資産に **[追加予定のタグ]** で指定されたタグを追加します。

複数の資産にタグを追加する場合

a. 資産の表で、タグを追加する各資産のチェックボックスを選択します。

表の上部にアクションバーが表示されます。

b. **[タグの追加]** をクリックします。

資産の表が表示されます。確認のメッセージが表示されます。Tenable Vulnerability Management は、資産に **[追加予定のタグ]** で指定されたタグを追加します。

6. 次のいずれかを行います。

最後に使用したタグを追加する場合

- **[最近使用したタグ]** で、追加するタグを選択します。

タグが **[追加予定のタグ]** ボックスに表示されます。

> **ヒント: [追加予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせて ✕ ボタンをクリックします。

新しいタグまたは既存のタグを追加する場合

a. **[カテゴリ]** ボックスに、カテゴリを入力します。

入力に伴って、リストでは一致が絞り込まれます。

b. ドロップダウンボックスから既存のカテゴリを選択するか、新しいカテゴリの場合は **["*カテゴリ名*" の作成]** をクリックします。

> **ヒント:** 汎用タグカテゴリを作成してさまざまなタグ値に適用すると、タグをグループ化できます。たとえば、*[場所]* カテゴリを作成し、*Headquarters* や *Offshore* などの複数の値に適用すると、場所タグのグループを作成できます。

c. **[値]** ボックスに値を入力します。

入力に伴って、リストでは一致が絞り込まれます。

d. ドロップダウンボックスから既存の値を選択するか、値を新規作成する場合は **["*値*" の作成]** をクリックします。

> **注意:** この方法で新しいタグを作成した場合、その新しいタグは資産に追加するまで保存されません。

タグが **[追加予定のタグ]** ボックスに表示されます。

> **ヒント:** **[追加予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせて ✕ ボタンをクリックします。

7. **[追加]** をクリックします。

資産の表が表示されます。確認のメッセージが表示されます。Tenable Vulnerability Management は、資産に **[追加予定のタグ]** で指定されたタグを追加します。

資産からのタグの削除

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要なアクセスグループのアクセス許可: 表示可、編集可

資産に手動でタグを追加するとき、またはタグのルールに基づいて Tenable Vulnerability Management がその資産に自動適用するタグを作成するときに、タグの範囲から資産を除外する場合は、資産から手動で削除できます。

資産からタグを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションプレーンにある **[調査]** セクションで、**[資産]** をクリックします。

   [資産] ページが表示されます。デフォルトでは、**[ホスト]** タブが表示されます。

3. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

4. 次のいずれかを行います。

   ### 1 つの資産からタグを削除する場合

   資産からタグを削除するページを選択します。

場所	アクション
[資産] ページ	**[資産]** ページで資産からタグを削除する方法 a. 資産の表で、タグを削除する資産の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 資産の表の **[アクション]** 列で、タグを削除する資産の ⋮ ボタンをク

	リックします。 アクションボタンが行に表示されます。 b. **[タグの削除]** をクリックします。 **[タグの削除]** ウィンドウが表示されます。 c. **[現在のタグ]** で、削除するタグにカーソルを合わせて ✕ ボタンをクリックします。 タグが **[削除予定のタグ]** ボックスに表示されます。 **ヒント: [削除予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせ、✕ ボタンをクリックします。
[資産の詳細] ページ	**[資産の詳細]** ページで資産からタグを削除する方法 a. タグを削除する資産の **[資産の詳細]** ページを表示します。 b. 次のいずれかを行います。 • ページ左側の **[タグ]** セクションで、削除するタグにカーソルを合わせて ✕ ボタンをクリックします。 • **[アクション]** メニューからタグを削除する方法 i. 右上の **[アクション]** ボタンをクリックします。 アクションメニューが表示されます。 ii. アクションメニューで、**[タグの削除]** をクリックします。 **[タグの削除]** ウィンドウが表示されます。 iii. **[現在のタグ]** で、削除するタグにカーソルを合わせて ✕ ボタンをクリックします。 タグが **[削除予定のタグ]** ボックスに表示されます。

	ヒント: **[削除予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせ、× ボタンをクリックします。

複数の資産からタグを削除する場合

a. 削除するタグで資産を検索します。

b. 次のいずれかを行います。

- 選択した資産からタグを削除するには、資産の表で、タグを削除する各資産の横にあるチェックボックスを選択します。
- すべての資産からタグを削除する方法

i. 資産の表のヘッダー行で、資産の総数の横にあるチェックボックスを選択します。

表の上部にアクションバーが表示されます。

ページ上にあるすべての資産が選択されています。

ii. **[***"タグ付けされた資産の合計数"* **の資産すべてを選択]** をクリックします。

> **注意:** タグ付けされた資産をすべて選択しない場合、Tenable Vulnerability Management は現在のページにある資産からのみタグを削除します。

c. アクションバーで、⋮ **[さらに表示]** ボタンをクリックします。

メニューが表示されます。

d. アクションメニューで、**[タグの削除]** をクリックします。

[タグの削除] ウィンドウが表示されます。

e. **[現在のタグ]** で、削除するタグにカーソルを合わせて × ボタンをクリックします。

タグが **[削除予定のタグ]** ボックスに表示されます。

> **ヒント:** **[削除予定のタグ]** からタグを削除するには、そのタグにカーソルを合わせ、× ボタンをクリックします。

5. **[削除]** をクリックします。

Tenable Vulnerability Management で、選択したタグが資産から削除されます。

タグのエクスポート

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

[タグ] ページでは、タグのカテゴリと値を CSV または JSON 形式でエクスポートできます。

タグのカテゴリや値をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

   > 注意: **[タグ]** ページの表をフィルタリングすることはできません。

5. 次のいずれかを行います。

   タグカテゴリをエクスポートする場合

a. エクスポートするタグカテゴリを選択します。

エクスポート範囲	アクション
選択したタグカテゴリ	選択したタグカテゴリをエクスポートする方法 a. カテゴリの表で、エクスポートする各タグカテゴリのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のタグカテゴリをエクスポートする場合は、リストにあるすべてのタグカテゴリを選択して、[→ **[エクスポート]** をクリックします。
1 つのタグカテゴリ	1 つのタグカテゴリをエクスポートする方法 a. カテゴリの表で、エクスポートするタグカテゴリの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- カテゴリの表の **[アクション]** 列で、エクスポートするタグカテゴリの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[エクスポート]** をクリックします。

タグ値をエクスポートする場合

a. **[値]** タブをクリックします。

[値] タブが表示されます。このタブは、すべてのタグ値を含む表があります。

b. エクスポートするタグ値を選択します。

エクスポート範囲	アクション
選択したタグ値	選択したタグ値をエクスポートする方法 a. 値の表で、エクスポートする各タグ値のチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のタグ値をエクスポートする場合は、リストにあるすべてのタグ値を選択して、[→**[エクスポート]** をクリックします。
1 つのタグ値	1 つのタグ値をエクスポートする方法 a. カテゴリの表で、エクスポートするタグ値の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 値の表の **[アクション]** 列で、エクスポートするタグ値の行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

注意: デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	タグのカテゴリまたは値のリストを含む CSV テキストファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	タグのカテゴリまたは値がネストされたリストを含む JSON ファイル。 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。
    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。

- **[繰り返し終了]**ドロップダウンで、スケジュールが終了する日付を選択します。

  注意: [無し]を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]**トグルをクリックします。

      [メール通知]セクションが表示されます。

    - **[受信者の追加]**ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須)**[パスワード]**ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      注意: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]**をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、**[エクスポート管理の表示]**でエクスポートファイルにアクセスできます。

タグカテゴリの削除

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

タグカテゴリを削除すると、Tenable Vulnerability Management によりそのカテゴリ下に作成されたタグがすべて削除され、それらのタグが適用されたすべての資産からもそれらのタグが削除されます。

注意: タグカテゴリを削除すると、関連するすべての値と割り当ても削除されます。特定のタグを削除する場合は、タグの削除を参照してください。

タグカテゴリを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[カテゴリ]** タブをクリックします。

   タグカテゴリの表が表示されます。

5. 1 つのタグカテゴリを削除する場合

   a. タグの表の **[アクション]** 列で、⋮ ボタンをクリックします。

      メニューが表示されます。

b. **[削除]** ボタンをクリックします。

確認ウィンドウが開き、カテゴリと関連するすべてのタグと割り当てを削除するかどうかを確認するメッセージが表示されます。

複数のタグカテゴリを削除する場合

a. タグカテゴリの表で、削除する各カテゴリのチェックボックスを選択します。

ページの下部またはに、アクションバーが表示されます。

b. アクションバーで、**[削除]** ボタンをクリックします。

確認ウィンドウが開き、カテゴリと関連するすべてのタグと割り当てを削除するかどうかを確認するメッセージが表示されます。

6. **[削除]** をクリックします。

Tenable Vulnerability Management によりタグカテゴリとそれに関連するすべてのタグが削除され、それらのタグを適用したすべての資産からも削除されます。

タグの削除

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Vulnerability Management アクセス許可: 該当する資産タグに対する編集可および使用可アクセス許可

タグを削除すると、Tenable Vulnerability Management はそのタグを適用したすべての資産から、その特定のタグを削除します。

1 つ以上のタグを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. 1 つ以上のタグを削除します。

削除の範囲	アクション
1 つのタグ	1 つのタグを削除する場合 a. **[値]** タブをクリックします。 **[値]** タブが開き、Tenable Vulnerability Management インスタンスのすべてのタグを含む表が、*カテゴリ: 値* の形式で表示されます。 b. タグの表で、削除するタグの行を右クリックします。 アクションオプションがカーソルの横に表示されます。

	-または- タグの表の **[アクション]** 列で、削除するタグの ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 c. 🗑 **[削除]** をクリックします。
複数のタグ	複数のタグを削除する場合 a. **[値]** タブをクリックします。 **[値]** タブが開き、Tenable Vulnerability Management インスタンスのすべてのタグを含む表が、*カテゴリ: 値* の形式で表示されます。 b. タグの表で、削除する各タグのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 c. アクションバーで、🗑 **[削除]** をクリックします。 -または- タグカテゴリを削除して、カテゴリ内にあるすべてのタグを削除します。

5. **[値]** タブをクリックします。
6. 1つのタグを削除する場合
   a. タグの表で、削除するタグにカーソルを合わせます。
   アクションボタンが行に表示されます。
   b. 🗑 **[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。

   複数のタグを削除する場合
   a. タグの表で、削除する各タグのチェックボックスを選択します。
   ページの下部またはに、アクションバーが表示されます。
   b. アクションバーで、🗑 **[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。

7. **[確認]**をクリックします。

   Tenable Vulnerability Management はそのタグを削除し、そのタグを適用したすべての資産からもそのタグを削除します。

タグの表からタグで資産を検索する

必要な Tenable Vulnerability Management ユーザーロール: スキャンオペレーター、標準、スキャンマネージャー、または管理者

タグで資産を検索すると、特定のタグが適用されている資産を確認できます。

タグの表からタグで資産を検索する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[タグ付け]** タイルをクリックします。

   [タグ] ページが表示されます。このページでは、資産タグのカテゴリと値を表示できます。

   [カテゴリ] タブはアクティブです。

4. **[値]** タブをクリックします。

5. 表にある ⋮ ボタンをクリックします。

   アクションメニューが表示されます。

6. **[タグ別に検索]** をクリックします。

   [**資産**] ページが表示され、選択したタグでフィルタリングされた資産の表が表示されます。

センサー

Tenable Vulnerability Management では、次のセンサータイプがサポートされます。

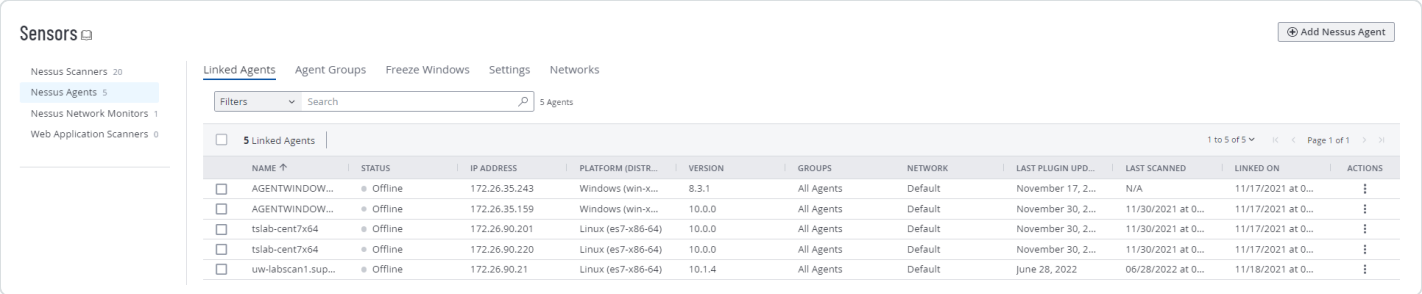
- Tenable が提供する*地域のクラウドセンサー*。詳細は、クラウドセンサーを参照してください。
- 手動で設定した、*リンクされたセンサー*(Tenable Nessus スキャナー、Tenable Nessus Network Monitor インスタンス、Tenable Web App Scanning センサー、Tenable Nessus Agents)。詳細は、リンクされたセンサーを参照してください。

ヒント: データを Tenable Vulnerability Management に取り込む他の方法については、Tenable Vulnerability Management でのデータ取り込みクイックリファレンスガイドを参照してください。

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。エージェントは、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可能にします。

ホスト上に Tenable Nessus Agent をインストールしてエージェントを Tenable Vulnerability Management にリンクすると、Tenable Vulnerability Management **[リンクされたエージェント]** ページにエージェントが表示されます。



注意: 1 つ以上のエージェントを 1 つのネットワークに割り当てたときに、その中のいずれかのエージェントが既に別のカスタムネットワークに割り当てられていた場合、「このネットワークにエージェントを追加することで、エージェントは以前のネットワークから割り当て換えされる」ことを示す確認メッセージが表示されます。

エージェントによって次の情報が Tenable Vulnerability Management に送信されます。

- バージョン情報 (エージェントのバージョン、ホストのアーキテクチャ)
- インストールされている Tenable プラグインのバージョン
- OS 情報 (例: `Microsoft Windows Server 2008 R2 Enterprise Service Pack 1`)
- Tenable 資産 ID (例: Unix の場合は `/etc/tenable_tag`、Windows の場合は `HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\TAG`)
- ネットワークインターフェース情報 (ネットワークインターフェース名、MAC アドレス、IPv4 アドレス、IPv6 アドレス、ホスト名、および情報が存在する場合は DNS 情報)
- `update_hostname` が `yes` に設定されている場合はホスト名 (詳細については、Tenable Nessus Agent の詳細設定を参照してください)
- (Agents 10.0.x 以降) AWS EC2 インスタンスメタデータ (存在する場合)

注意: Tenable Nessus Agent は 169.254.169.254 に接続して、AWS メタデータを Tenable Vulnerability Management に提供します。Tenable Nessus Agent と 169.254.169.254 の間のトラフィックは正常で予期された動作です。

- privateIp
- accountId
- imageId
- region
- instanceType
- availabilityZone
- architecture
- instanceId
- local-hostname
- public-hostname
- public-ipv4
- mac
- iam/security-credentials/
- public-keys/0/openssh-key
- security-groups

注意: エージェントのバージョンが 8.3.1 以前の場合、エージェントは起動時と再起動後にチェックインします。

エージェントのバージョンが 10.0.0 以降の場合、エージェントは起動時、再起動後、およびメタデータが更新されるたびに(10 分ごとに) チェックインします。

ヒント: データを Tenable Vulnerability Management に取り込む他の方法については、Tenable Tenable Vulnerability Management でのデータ取り込みクイックリファレンスガイドを参照してください。

Tenable Nessus Agent リンクキーの取得

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Nessus Agents のインストールプロセスを始める前に、Tenable Vulnerability Management 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。

エージェントのリンクキーを取得する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ⊕ **[Nessus Agent の追加]** をクリックします。

   [エージェントを追加する] プレーンが表示されます。

6. **[コピー]** ボタンをクリックし、**リンクキー**をコピーします。

   [リンクキーをクリップボードにコピー] のメッセージが表示され、リンクキーがクリップボードにコピーされます。

次の手順

- Tenable Nessus Agent のインストール

リンクされたエージェントログをダウンロードする

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management では、ログとシステム設定データを含むログファイルを、任意のリンクされたエージェント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 に簡単にデータを提供することができます。

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。エージェントログファイルをリクエストした後、Tenable Vulnerability Management はログファイルを 7 日間保持します。

Tenable Vulnerability Management で、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方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. エージェントの表で、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詳細ページが表示されます。

6. **[ログ]** タブをクリックします。

   表には、以前にダウンロードされたログが表示されます。

7. 右上にある **[リクエストログ]** 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 Vulnerability Management 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。

エージェントログをリクエストすると、Tenable Vulnerability Management はログを 7 日間保持します。

8. ログファイルをダウンロードするには、⬇ ボタンをクリックします。

   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

1. 削除するログの行で、🗑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. 確認ウィンドウで、**[削除]** をクリックします。

   Tenable Vulnerability Management によってログが削除され、表からそのログが削除されます。

保留中または失敗したログのリクエストをキャンセルする方法

- キャンセルする保留中のログまたは失敗したログのリクエスト行で、⏸ ボタンをクリックします。

  Tenable Vulnerability Management によってログのリクエストが削除され、表から削除されます。

エージェントを再起動する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management では、リンクされたエージェント (バージョン 7.6 以降) を **[リンクされたエージェント]** タブで再起動できます。

エージェントを再起動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. (オプション) 特定のエージェントを検索するか、表のエージェントにフィルターを適用します。

6. 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、再起動するエージェントの行の 🔄 ボタンをクリックします。

      [エージェントの再起動] ウィンドウが表示されます。

   b. 次の **[再起動タイプ]** からいずれかを選択します。

Restart Type	説明
Soft	エージェントのバックエンドを再起動しますが、サービスは再起動しませ

	ん。
Hard	エージェントのバックエンドとサービスを再起動します。
Idle	エージェントがスキャンを実行していないときに、エージェントのバックエンドとサービスを再起動します。

c. **[保存]** をクリックします。

Tenable Vulnerability Management によって設定が保存され、エージェントが次回チェックインしたときに変更が有効になります。オンラインエージェントの場合、この作業には最大で 45 分かかります。

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。

ページの下部またはに、アクションバーが表示されます。

> **ヒント:** アクションバーで **[すべてのページを選択]** を選択して、リンクされているすべてのエージェントを選択します。

b. アクションバーで、↻ ボタンをクリックします。

[エージェントの再起動] ウィンドウが表示されます。

c. 次の **[再起動タイプ]** からいずれかを選択します。

Restart Type	説明
Soft	エージェントのバックエンドを再起動しますが、サービスは再起動しません。
Hard	エージェントのバックエンドとサービスを再起動します。

Idle	エージェントがスキャンを実行していないときに、エージェントのバックエンドとサービスを再起動します。

d. **[保存]** をクリックします。

Tenable Vulnerability Management によって設定が保存され、エージェントが次回チェックインしたときに変更が有効になります。オンラインエージェントの場合、この作業には最大で 45 分かかります。

エージェントのリンク解除

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

エージェントとのリンクを手動で解除すると、そのエージェントは **[エージェント]** ページから削除されますが、システムにはエージェント設定で指定した期間、関連データが保持されます。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自動では Tenable Vulnerability Managementに再リンクしません。

ヒント：エージェントの設定で説明されているように、エージェントが一定の日数非アクティブな場合、それをリンク解除するよう設定できます。

Tenable Vulnerability Management でエージェントのリンクを解除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. (オプション) 特定のエージェントを検索するか、表のエージェントにフィルターを適用します。フィルターの詳細については、エージェントフィルターを参照してください。

6. リンクを解除するエージェントを選択してください。

範囲	アクション
1つのエージェントのリンクを解除する	**[Nessus Agent]** タブからエージェントのリンクを解除する方法 a. エージェント表で、リンクを解除するエージェントの行を右クリックします。 -または- リンクを解除するエージェントの行の **[アクション]** 列で、⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 -または- リンクを解除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。 アクションバーで、Tenable Vulnerability Management は **[その他]** > **[選択したもののリンク解除]** を有効にします。 b. 必要に応じて、**[選択解除]** または **[選択したもののリンク解除]** をクリックします。
複数のエージェントのリンクを解除する	**[Nessus Agent]** タブから複数のエージェントのリンクを解除する方法 a. リンクを解除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。 アクションバーで、Tenable Vulnerability Management は **[その他]** > **[選択したもののリンク解除]** を有効にします。 b. **[選択したもののリンク解除]** をクリックします。

Tenable Vulnerability Management によりエージェントとのリンクが解除されます。

エージェントの名前変更

リンクされたエージェントの名前は、**[センサー]** メニューから変更できます。名前を変えることで、他のユーザーが容易に識別できるようになります。

エージェントの名前を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. 名前を変更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。

6. エージェント名の横にある ✎ ボタンをクリックします。

7. エージェント名を編集します。

8. エージェント名の横にある ✓ ボタンをクリックします。

   Tenable Vulnerability Management で、新しいエージェント名が保存され、関連する表が新しい名前で更新されます。

エージェント設定

エージェントマネージャー上でグローバルエージェント設定を変更することで、リンクされたすべてのエージェントに対してエージェントおよびフリーズ期間設定を指定できます。フリーズ期間の作成、変更、および削除の詳細については、フリーズウィンドウを参照してください。

また、個別のエージェントに対してログレベル、パフォーマンスレベル、ホスト名の自動更新、バージョンの自動更新の設定を調整できます。詳細は、リモートエージェント設定を変更するを参照してください。

リモートエージェント設定を変更する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management では、個々のエージェント (バージョン 7.6 以降) の設定を **[リンクされたエージェント]** タブで変更できます。同様の設定をコマンドラインインターフェースで編集する方法については、*Tenable Nessus Agent ユーザーガイド*の詳細設定を参照してください。

注意: 以下の手順に加えて、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 Nessus Agent ユーザーガイド*を参照してください。

Tenable Vulnerability Management のリモートエージェント設定を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. (オプション) 特定のエージェントを検索するか、*Tenable Nessus Agent デプロイメントとユーザーガイド*のエージェントをフィルタリングするの説明に従って、表のエージェントにフィルターを適用します。

6. 次のいずれかを行います。

   ### 1 つのエージェントを編集する場合

   a. エージェントの表で、編集するエージェントの行の ✎ ボタンをクリックします。

      [エージェントの編集] ウィンドウが表示されます。

   b. エージェント設定を編集します。

設定	説明	Default (デフォルト)	値
Nessus Agent 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。 詳細については、*Tenable Nessus ユーザーガイド*の log.json の書式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。
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 Nessus Agent デプロイメントとユーザーガイド* 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
スキャンパフォーマンス	CPU 使用率に影響を	high	low、medium、または high

	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 Nessus Agent デプロイメントとユーザーガイド* 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。		
Nessus Agent Update Plan	エージェントの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。 **注意:** エージェントに エージェントプロファイルを割り当てる場合、エージェントプロファイルのバージョンは、**Nessus Agent 更新プラン**をオーバーライドします。	`Keep up to date with GA releases`	`Keep up to date with GA releases`、`Opt in to Early Access releases`、または `Delay updates, staying on the last stable release`

	エージェントにフリーズ期間を割り当てると、フリーズ期間は **Nessus Agent 更新プラン** とエージェントプロファイルの両方をオーバーライドします。この場合、エージェントは現在のバージョンのままで、エージェントがフリーズ期間に割り当てられている限り、そのエージェントのソフトウェア更新は発生しません。		
Automatic Hostname Update	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
Offline Agent Scan Trigger Execution Threshold	ルールベースのスキャンが実行を停止するまでにエージェントをオフラインにできる日数を指定します。	14	整数の 1 ～ 48

1 日あたりの最大スキャン	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

c. **[保存]** をクリックします。

Tenable Vulnerability Management によって設定が保存され、エージェントが次回チェックインしたときに変更が有効になります。オンラインエージェントの場合、この作業には最大で 45 分かかります。

設定が変更される必要がある場合、エージェントは次回アイドル状態になったときに再起動します。

複数のエージェントを編集する場合

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。

ページの下部またはに、アクションバーが表示されます。

> **ヒント:** アクションバーで **[すべてのページを選択]** を選択して、リンクされているすべてのエージェントを選択します。

b. アクションバーで、 ボタンをクリックします。

[エージェントの編集] ウィンドウが表示されます。

c. エージェント設定を編集します。

設定	説明	Default (デフォルト)	値
Nessus Agent 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	normal	• normal - ログタグを "log"、"info"、"warn"、

	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。 詳細については、*Tenable Nessus ユーザーガイド*の log.json の書式を参照してください。		"error"、"trace" に設定します • debug - ログタグを "log"、"info"、"warn"、"error"、"trace"、"debug" に設定します • verbose - ログタグを "log"、"info"、"warn"、"error"、"trace"、"debug"、"verbose" に設定します
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	high	low、medium、または high

	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 Nessus Agent デプロイメントとユーザーガイド* 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。		
スキャンパフォーマンス	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 Nessus Agent デプロイメントとユーザーガイド* 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`
Automatic	この機能を有効にする	×	`yes` または `no`

Hostname Update	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。		
Nessus Agent Update Plan	エージェントの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。 **注意:** エージェントにエージェントプロファイルを割り当てる場合、エージェントプロファイルのバージョンは、**Nessus Agent 更新プラン**をオーバーライドします。 エージェントにフリーズ期間を割り当てると、フリーズ期間は **Nessus Agent 更新プラン** とエージェントプロファイルの両方をオーバーライドします。この場合、エージェントは現在のバージョンのままで、エージェントがフリー	`Keep up to date with GA releases`	`Keep up to date with GA releases`、`Opt in to Early Access releases`、または `Delay updates, staying on the last stable release`

	ズ期間に割り当てられている限り、そのエージェントのソフトウェア更新は発生しません。		
Offline Agent Scan Trigger Execution Threshold	ルールベースのスキャンが実行を停止するまでにエージェントをオフラインにできる日数を指定します。	14	整数の1～48
1日あたりの最大スキャン	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

d. **[保存]**をクリックします。

Tenable Vulnerability Management によって設定が保存され、エージェントが次回チェックインしたときに変更が有効になります。オンラインエージェントの場合、この作業には最大で 45 分かかります。

設定が変更される必要がある場合、エージェントは次回アイドル状態になったときに再起動します。

グローバルエージェント設定を変更する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

この手順を使用して、Tenable Vulnerability Management のエージェント設定を編集します。

Tenable Vulnerability Management で、グローバルエージェント設定を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで **[設定]** を選択します。

   [設定] ページが表示されます。

6. 必要に応じて設定を編集します。

オプション	説明
非アクティブなエージェント	
次の期間、アクティブでないエージェントのリンクを解除します: X 日	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。指定された日数が経過するとエージェントはリンクを解除されますが、対応するエージェントデータは管理ツールから削除されません。 Tenable Vulnerability Management は、このオプションで指定された日

オプション	説明
	数の間、リンク解除されたエージェントと関連データを自動的に追跡します。この追跡をオフにすることはできません。 **注意:** Tenable Vulnerability Management 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でも自動的には再リンクしません。
フリーズ期間のオーバーライド	
すべてのエージェントをソフトウェアアップデートから除外する	このオプションを有効にすると、リンクされたすべてのエージェントがソフトウェアアップデートを受け取らなくなります。このオプションは、既存のフリーズ期間よりも優先されます。 この設定を有効にすると、エージェントは引き続きプラグインのアップデートを受け取り、スケジュールされたスキャンを実行します。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management により変更が保存されます。

エージェントプロファイル

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

エージェントプロファイルを使用して、リンクされたエージェントに特定のバージョンを適用できます。これは、テストに役立ちます。たとえば、すべてのエージェントを新しいバージョンにアップグレードする前に、エージェントのサブセットのテスト期間をスケジュールできます。

エージェントプロファイルを使用すると、期間限定でエージェントのサブセットに新しいバージョンを適用できます。さらに広い意味では、エージェントを簡単に異なるバージョンにアップグレードしたり、ダウングレードしたりできます。1 つのエージェントを 1 つのプロファイルにのみ割り当てることができます。

注意: エージェントプロファイルを 10.4.1 より前のバージョンに設定することはできません。エージェントプロファイルは、10.4.1 より前のバージョンのエージェントには影響しません。

注意: エージェントプロファイルのバージョンは、エージェントの Nessus Agent アップデートプランの設定をオーバーライドします。エージェントにフリーズ期間を割り当てると、フリーズ期間は Nessus Agent のアップデートプランとエージェントプロファイルの両方をオーバーライドします。この場合、エージェントは現在のバージョンのままで、エージェントがフリーズ期間に割り当てられている限り、そのエージェントのソフトウェア更新は発生しません。

エージェントプロファイルを管理する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. リンクされたエージェントの表の上にある**[プロファイル]**をクリックします。

   [プロファイル]ページが表示されます。

エージェントプロファイルを管理するには、次の手順を使用します。

エージェントプロファイルの作成

注意: サポートが終了した(EOL) Tenable Nessus Agent バージョンのエージェントプロファイルを作成することはできません。

エージェントプロファイルを作成する方法

1. **[プロファイル]**ページで、⊕ **[エージェントプロファイルの追加]**をクリックします。

   [エージェントプロファイルの作成]ページが表示されます。

2. エージェントプロファイルの**名前**を入力します。

3. (オプション) エージェントプロファイルの**説明**を入力します。

4. エージェントプロファイルの**センサーのバージョン**を選択します。これは、プロファイルに割り当てられたエージェントがアップグレードまたはダウングレードされた後のバージョンです。

   最新のメジャーバージョンリリース(例: 10.x)または最新のマイナーバージョンリリース(例: 10.4.x)を維持するようにエージェントプロファイルを設定したり、特定のパッチリリース(例: 10.4.1)に設定したりできます。

5. **[エージェントの割り当て]**で、割り当て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。

6. **[作成]**をクリックします。

エージェントプロファイル ID の表示

nessuscli エージェントリンクコマンドを実行し、オプションの `--profile-uuid` 引数を指定することで、エージェントをプロファイルにリンクできます。*config.json ファイル*で `profile-uuid` を指定することで、デプロイメント中にエージェントをプロファイルにリンクすることもできます。プロファイルの `--profile-uuid` を表示するには、次の手順を使用します。

エージェントプロファイル ID を表示する方法

1. **[プロファイル]** ページで、ID を表示するエージェントプロファイルをダブルクリックします。

   [センサープロファイルの詳細] ページが表示されます。

2. **[詳細]** タブで、**[エージェントプロファイル ID]** の下に `--profile-uuid` が表示されます。 をクリックすると、ID をクリップボードにコピーできます。

エージェントプロファイルの編集

エージェントプロファイルを編集する方法

1. **[プロファイル]** ページで、編集するプロファイルをダブルクリックします。

   [センサープロファイルの詳細] ページが表示されます。

2. 必要に応じてエージェントプロファイルを編集します。

   - エージェントプロファイル名を編集するには、エージェント名の横にある をクリックします。
   - **[詳細]** タブで、プロファイルの説明と、そのプロファイルで設定されている、リンクされたエージェントのエージェントバージョンを編集できます。
   - **[エージェント]** タブでは、リンクされたエージェントをエージェントプロファイルに追加または削除できます。

3. **[保存]** をクリックします。

   Tenable Vulnerability Management により変更が保存されます。プロファイルにエージェントを追加または削除した場合、編集から 24 時間以内にエージェントのバージョンが更新されます。

エージェントプロファイルのコピー

エージェントプロファイルをコピーして、既存のエージェントプロファイルの複製を作成します。その複製を使用して新しいエージェントプロファイルを設定できます。

エージェントプロファイルをコピーする方法

1. **[プロファイル]** ページのコピーするプロファイルの行で をクリックします。

   メニューが表示されます。

2. **[コピー]** をクリックします。

Tenable Vulnerability Management は、プロファイル名 に「 のコピー」を付 けた新しいプロファイルを作成します。

エージェント プロファイルの削 除

エージェント プロファイルが不 要 になった場 合 は、エージェント プロファイルを削 除します。エージェント プロファイルの削 除 を取 り消 すことはできません。

エージェント プロファイルを削 除 する方 法

1. **[プロファイル]** ページで、削 除 するプロファイルの行 で ⋮ をクリックします。

   メニューが表 示 されます。

2. 🗑 **[削 除]** をクリックします。

   [エージェント プロファイルの削 除] ウィンドウが表 示 されます。

3. **[削 除]** をクリックして、削 除 を確 定 します。

   Tenable Vulnerability Management のエージェント プロファイルが削 除 され、リンクされたすべてのエージェント がプロファイルから削 除 されます。

次 の手 順

- エージェント プロファイルにエージェント を追 加 または削 除 する

エージェントプロファイルにエージェントを追加または削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

次の手順を使用して、Tenable Vulnerability Management 内のエージェントプロファイルにエージェントを追加したり、エージェントプロファイルからエージェントを削除したりします。**[センサープロファイルの詳細]** ページで、プロファイルにエージェントを追加したり、プロファイルからエージェントを削除したりすることもできます。詳細については、エージェントプロファイルの編集を参照してください。

Tenable Vulnerability Management ユーザーインターフェースの使用に加えて、`nessuscli agent link`コマンドを実行し、オプションの `--profile-uuid` 引数を指定することで、エージェントをプロファイルにリンクできます。*config.json ファイル*で `profile-uuid` を指定することで、デプロイメント中にエージェントをプロファイルにリンクできます。プロファイルの `profile-uuid` を確認するには、エージェントプロファイル ID の表示を参照してください。

注意: エージェントプロファイルのバージョンは、エージェントの Nessus Agent アップデートプランの設定をオーバーライドします。エージェントにフリーズ期間を割り当てると、フリーズ期間は Nessus Agent のアップデートプランとエージェントプロファイルの両方をオーバーライドします。この場合、エージェントは現在のバージョンのままで、エージェントがフリーズ期間に割り当てられている限り、そのエージェントのソフトウェア更新は発生しません。

エージェントにエージェントプロファイルを適用する

エージェントにエージェントプロファイルを適用する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. 次のいずれかを行います。

- エージェントプロファイルに1つのエージェントを割り当てる方法

  a. プロファイルに割り当てるエージェントの行で、⋮をクリックします。

  アクションボタンが行に表示されます。

  b. **[エージェントプロファイルの適用]**をクリックします。

  [エージェントプロファイルの選択]ウィンドウが表示されます。

  c. 表で、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チェックボックスを選択します。

  d. **[適用]**をクリックします。

  Tenable Vulnerability Managementがエージェントをエージェントプロファイルに割り当てます。

- 複数のエージェントをエージェントプロファイルに追加する場合は、次のいずれかを行います。

  - エージェントの表で、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。
  - 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。

  ページの下部またはに、アクションバーが表示されます。

  > **ヒント:** アクションバーで**[すべてのページを選択]**を選択して、リンクされているすべてのエージェントを選択します。

  a. アクションバーで、**[エージェントプロファイルを適用]**をクリックします。

  [エージェントプロファイルの選択]ウィンドウが表示されます。

  b. 表で、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チェックボックスを選択します。

  c. **[適用]**をクリックします。

  Tenable Vulnerability Managementがエージェントをエージェントプロファイルに割り当てます。エージェントのバージョンは、プロファイルが適用されてから24時間以内に更新されます。

エージェントからエージェントプロファイルを削除する

エージェントからエージェントプロファイルを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. 次のいずれかを行います。

   - エージェントプロファイルから 1 つのエージェントを削除するには次を行います。

     a. プロファイルに割り当てるエージェントの行で、⋮ をクリックします。

        アクションボタンが行に表示されます。

     b. **[エージェントプロファイルの削除]** をクリックします。

        [エージェントプロファイルの削除] ウィンドウが表示されます。

     c. **[削除]** をクリックして確定します。

        Tenable Vulnerability Management により、エージェントプロファイルからエージェントが削除されます。

   - エージェントグループから複数のエージェントを削除する場合は、次のいずれかを行います。

     - エージェントの表で、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。
     - 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。

     ページの下部またはに、アクションバーが表示されます。

ヒント : アクションバーで **[すべてのページを選択]** を選択して、リンクされているすべてのエージェントを選択します。

a. アクションバーで、**[エージェントプロファイルの削除]** をクリックします。

[エージェントプロファイルの削除] ウィンドウが表示されます。

b. **[削除]** をクリックして確定します。

Tenable Vulnerability Management により、エージェントが 1 つまたは複数のプロファイルから削除されます。エージェントのバージョンは、プロファイルが削除されてから 24 時間以内に更新されます。

次の手順

- エージェントプロファイルの管理

エージェントのステータス

Tenable Nessus Agents は、次のいずれかのステータスとなります。

ステータス	説明
Online	Tenable Nessus Agent を含むホストは現在接続済みで、Tenable Vulnerability Management と通信しています。
Offline	Tenable Nessus Agent を含むホストは現在停止中か、ネットワークに接続されていません。
Initializing	Tenable Nessus Agent は、Tenable Vulnerability Management でのチェックインの処理中です。

エージェントのエクスポート

Tenable Vulnerability Management でエージェントデータをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. 各エージェントのチェックボックスをクリックして、エクスポートするエージェントを選択します。

6. エージェントの表の上部にある [→ **[エクスポート]** ボタンをクリックします。

   [エクスポート] プレーンが表示され、エクスポートされるエージェントの数が表示されます。

7. **[フォーマット]** セクションで、**[CSV]** フォーマットを選択します。

   > **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。

8. エージェントデータを `.csv` 形式でエクスポートするには、**[エクスポート]** 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。

9. **[OK]** をクリックして `agents.csv` ファイルを保存します。

Tenable Vulnerability Management 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
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 アドレス	エージェントの IPv4 または IPv6 アドレス。
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。
プロファイル名	エージェントに割り当てられたエージェントプロファイルの名前。
プロファイル UUID	エージェントに割り当てられたエージェントプロファイルの UUID。
グループ	エージェントが属しているグループの名前
グループ ID	エージェントが属しているグループの ID
バージョン	エージェントのバージョン。
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)
エージェントの ID	エージェントの ID
エージェント UUID	エージェント UUID
リンク日	エージェントが Tenable Vulnerability Management にリンクされた日付 (ISO-8601 形式)
最終接続日	エージェントが前回チェックインした日付 (ISO-8601 形式)
最終スキャン日	エージェントが最後にスキャンされた日付 (ISO-8601 形式)

リンクされたエージェントをエクスポートする

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

[センサー管理] ページでは、1 つ以上のリンクされたエージェントを CSV または JSON 形式でエクスポートできます。

リンクされたエージェントをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[フリーズ期間]** を選択します。

6. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

7. エクスポートするリンクされたエージェントを選択します。

エクスポート範囲	アクション
1 つのリンクされたエージェ	1 つのリンクされたエージェントを選択してエクスポートする方法 a. リンクされたエージェントの表で、エクスポートするリンクされたエージェントの行を右クリックします。

ント	アクションオプションが行に表示されます。 -または- リンクされたエージェントの表にある **[アクション]** 列で、エクスポートするリンクされたエージェントの行にある ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。 -または- リンクされたエージェントの表で、エクスポートするエージェントのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. [→ **[エクスポート]** をクリックします。
複数のリンクされたエージェント	複数のリンクされたエージェントを選択してエクスポートする方法 a. リンクされたエージェントの表で、エクスポートする各リンクされたエージェントのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のリンクされたエージェントをエクスポートする場合は、リストにあるすべてのリンクされたエージェントを選択して、[→ **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

注意: デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- メール通知を設定するためのトグル

8. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
9. 使用するエクスポート形式をクリックします。

形式	説明
CSV	リンクされたエージェントのリストを含む CSV テキストファイル
JSON	リンクされたエージェントがネストされたリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

10. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
11. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

> **注意**: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

> **注意**: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。
- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

リンクされたエージェントの詳細をエクスポートする

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

リンクされたエージェントの **[詳細]** ページでは、リンクされたエージェントに関する詳細を CSV または JSON 形式でエクスポートできます。

リンクされたエージェントに関する詳細をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. リンクされたエージェントの表で、詳細をエクスポートするリンクされたエージェントをクリックします。

   [詳細] ページが表示されます。

7. 右上にある [→ **[エクスポート]** をクリックします。

   [エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

   - エクスポートファイル名を設定するテキストボックス
   - 利用可能なエクスポート形式のリスト
   - エクスポートされたファイルに含めるフィールドの設定オプションの表

注意: デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

8. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
9. 使用するエクスポート形式をクリックします。

形式	説明
CSV	リンクされたエージェントに関する詳細の一覧をフィールド別に整理した CSV テキストファイル。
JSON	リンクされたエージェントに関する詳細をネストした一覧をフィールド別に整理した JSON ファイル。 空のフィールドは JSON ファイルに含まれません。

10. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
11. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

> **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

エージェントのフィルタリング

Tenable Vulnerability Management のエージェントの表でエージェントをフィルタリングする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 左のナビゲーションメニューで、**[Nessus Agent]** をクリックします。

   [リンクされたエージェント] ページが表示されます。

5. エージェントの表の上にある **[フィルター]** ボタンをクリックします。

   [フィルター] ペインが表示されます。

6. 必要に応じてオプションを設定します。選択したパラメーターに応じて異なるオプションが表示されます。

カテゴリ	演算子	値
Distro	contains 次の値を含まない:	テキストボックスに、フィルターを適用するディストリビューション名を入力します。
IP Address	次の値に等しい 次の値に等しくない 次の値を含む:	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。

カテゴリ	演算子	値
	次の値を含まない:	
Last Connection 最終プラグイン更新日 最終スキャン日	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 次の値に等しくない	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。
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。
プラットフォーム	contains 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。
ステータス	次の値に等しい 次の値に等	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。

カテゴリ	演算子	値
	しくない	
バージョン	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。

7. **[適用]**をクリックします。

   マネージャーにより、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

Tenable Vulnerability Management は、次のカテゴリによるエージェントのフィルタリングをサポートしています。

カテゴリ	演算子	値
Distro	contains 次の値を含まない:	テキストボックスに、フィルターを適用するディストリビューション名を入力します。
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。
Last Connection 最終プラグイン更新日 最終スキャン日	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 次の値に等しくない	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。
名前	次の値に等しい 次の値に等	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。

カテゴリ	演算子	値
	しくない 次の値を含む: 次の値を含まない:	
プラットフォーム	contains 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。
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。
UUID	次の値に等しい 次の値に等しくない	テキストボックスに、フィルタリングするエージェント UUID を入力します。 次のエージェント UUID 形式のいずれかを使用できます。 • xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (例: 885c5f3e-aca3-42bf-9355-ace1c71bfe9a) • xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx (例: 885c5f3eaca342bf9355ace1c71bfe9a) エージェントの UUID を見つけるには、Tenable Vulnerability Management ユーザーインターフェースでエージェントの詳細を表示するか、`# nessuscli agent status --show-uuid` コマンドを実行することができます。
バージョン	次の値に等しい 次の値に等しくない	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。

カテゴリ	演算子	値
	次の値を含む: 次の値を含まない:	

エージェントグループ

エージェントグループを使用して、Tenable Vulnerability Management にリンクしたエージェントを編成して管理できます。エージェントを複数のグループに追加し、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。

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
- エージェントグループにエージェントを追加する
- エージェントグループを編集する
- エージェントグループを削除する
- エージェントグループからエージェントを削除する
- エージェントグループでエージェントを表示する
- エージェントグループのフィルター

エージェントグループの作成

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

エージェントグループを使用して、お使いのアカウントにリンクしたエージェントを組織化し管理できます。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。

この手順を使用して、Tenable Vulnerability Management のエージェントグループを作成します。

新規エージェントグループを作成するには:

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[エージェントグループ]** を選択します。

   エージェントグループのリストが表示されます。

6. ⊕**[エージェントグループを追加する]** をクリックします。

   エージェントグループ設定プレーンが表示されます。

7. **[グループ名]** ボックスで、新規エージェントグループの名前を入力します。

8. エージェントグループのユーザーのアクセス許可を設定する

9. **[保存]** をクリックします。

   新規エージェントグループが表に表示されます。

次の手順

- エージェントスキャン設定のユーザーグループを使用します。

エージェントグループにエージェントを追加する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

この手順を使用して、Tenable Vulnerability Management のエージェントグループにエージェントを追加します。エージェントグループを変更している場合も、グループにエージェントを追加できます。

エージェントグループにエージェントを追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[エージェントグループ]** を選択します。

   エージェントグループのリストが表示されます。

6. (オプション) 特定のエージェントを検索するか、表のエージェントにフィルターを適用します。フィルターの詳細については、エージェントフィルターを参照してください。

7. 次のいずれかを行います。

   - 1 つのエージェントをエージェントグループに追加する場合

     a. エージェントの表で、追加するエージェントにカーソルを合わせます。

        アクションボタンが行に表示されます。

b. 🗁 ボタンをクリックします。

[グループに追加する] プレーンが表示されます。

- 複数のエージェントをエージェントグループに追加する場合は、次のいずれかを行います。
  - エージェントの表で、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。
  - 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。

ページの下部またはに、アクションバーが表示されます。

> **ヒント:** アクションバーで **[すべてのページを選択]** を選択して、リンクされているすべてのエージェントを選択します。

a. アクションバーで、🗁 ボタンをクリックします。

[グループに追加する] プレーンが表示されます。

8. 次のいずれかを実行してください。

- 既存のエージェントグループがある場合は、その中の1つを選択します。
  a. 検索ボックスで、エージェントグループ名で検索します。

  b. 選択するエージェントグループをクリックします。

- 既存のエージェントグループがない場合は作成します。
  a. **[新しいグループに追加する]** をクリックします。

  エージェントグループ設定プレーンが表示されます。

  b. テキストボックスに、新しいグループの名前を入力します。

  c. **[ユーザーとグループ]** セクションで、新しいグループのユーザーアクセス許可を設定します。

d. **[保存]**をクリックします。

[グループに追加する]プレーンが再表示されます。新しいグループが選択リストに表示されます。

9. **[保存]**をクリックして変更を保存します。

Tenable Vulnerability Managementにより、選択した1つまたは複数のグループにエージェントが追加されます。

エージェントグループを編集する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management でエージェントグループを変更するには、この手順を使用します

エージェントグループを変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[エージェントグループ]** を選択します。

   エージェントグループのリストが表示されます。

6. (オプション) 特定のエージェントグループを検索するか、表のエージェントグループにフィルターを適用します。フィルターの詳細については、エージェントグループフィルターを参照してください。

7. エージェントグループ設定を編集します。

   a. エージェントの表で、次のいずれかを行います。

   - **[アクション]** 列で、編集するエージェントの ⋮ アイコンをクリックします。

     アクションオプションが行に表示されます。

   - 編集するエージェントを右クリックします。

アクションオプションがカーソルの横に表示されます。

- 編集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。

  表の上部にアクションバーが表示されます。

b. **[編集]** ボタンをクリックします。

   [エージェントグループの編集] プレーンが表示されます。

c. 🗁 ボックスに、エージェントグループの新しい名前を入力します。

d. エージェントグループのユーザーのアクセス許可を設定します。

e. **[保存]** をクリックして変更を保存します。

   Tenable Vulnerability Management により変更が保存されます。

8. エージェントグループにエージェントを割り当てます。

   a. エージェントを追加するエージェントグループの行をクリックします。

      エージェントグループの詳細ページが表示されます。

   b. 右上の ⊕**[エージェントの割り当て]** をクリックします。

      エージェントの割り当てページが表示されます。

   c. (オプション) 特定のエージェントを検索するか、表のエージェントにフィルターを適用します。フィルターの詳細については、エージェントフィルターを参照してください。

   d. エージェントの表で、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。

   e. **[割り当て]** をクリックします。

      Tenable Vulnerability Managementによりエージェントグループにエージェントが追加され、詳細ページが表示されます。

エージェントグループを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Managementでエージェントグループを削除するには、この手順を使用します。

エージェントグループを削除するには:

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[エージェントグループ]** を選択します。

   エージェントグループのリストが表示されます。

6. (オプション) 特定のエージェントグループを検索するか、表のエージェントグループにフィルターを適用します。フィルターの詳細については、エージェントグループフィルターを参照してください。

7. エージェントの表で、次のいずれかを行います。

   - 削除するエージェントグループの行の [アクション] 列で、⋮ ボタンをクリックします。

     アクションオプションが行に表示されます。

   - 削除するエージェントを右クリックします。

     アクションオプションがカーソルの横に表示されます。

- 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。

  上部にアクションバーが表示されます。

8. **[削除]** をクリックします。

   確認ウィンドウが表示されます。

9. **[削除]** をクリックします。

   Tenable Vulnerability Management によりエージェントグループが削除されます。

エージェントグループからエージェントを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management でエージェントグループから 1 つまたは複数のエージェントを削除するには、この手順を使用します。

エージェントグループからエージェントを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[エージェントグループ]** を選択します。

   エージェントグループのリストが表示されます。

6. (オプション) 特定のエージェントグループを検索するか、表のエージェントグループにフィルターを適用します。フィルターの詳細については、エージェントグループフィルターを参照してください。

7. 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。

   [グループの詳細] ページが表示されます。

8. 選択したエージェントグループを削除します。

削除する方法	アクション
単一のエージェントグループ	a. 次のいずれかを行います。 • エージェントの表で、削除するエージェントグループを右クリックします。 アクションボタンが行に表示されます。 • 削除するエージェントグループの行の **[アクション]** 列で、⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 • 削除するエージェントグループの横にあるチェックボックスを選択します。 Tenable Vulnerability Management により、**[その他]** > **[グループから削除する]** が有効になります。 b. **[グループから削除する]** をクリックします。
複数のエージェントグループ	a. 次のいずれかを行います。 • エージェントの表で、削除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。 Tenable Vulnerability Management により、**[その他]** > **[グループから削除する]** が有効になります。 b. **[グループから削除する]** をクリックします。

Tenable Vulnerability Management により、エージェントがグループから削除されます。

エージェントグループでエージェントを表示する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management でエージェントグループのエージェントを表示するには、この手順を使用します。

新しいインターフェースのエージェントグループでエージェントを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[エージェントグループ]** を選択します。

   エージェントグループのリストが表示されます。

6. (オプション) 特定のエージェントを検索するか、表のエージェントにフィルターを適用します。フィルターの詳細については、エージェントフィルターを参照してください。

7. エージェントグループの表で、表示するエージェントグループをクリックします。

   [グループの詳細] ページが表示されます。このページには、グループに割り当てたエージェントを記載した表が含まれます。

エージェントグループのフィルター

以下にリストされているフィルターを使用して、**[エージェントグループ]** タブのエージェントグループを絞り込むことができます。

カテゴリ	演算子	値
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、エージェントグループの名前を入力します。
Creation Date	earlier than later than 次の値と等しい not on	テキストボックスに、エージェントグループの作成日を入力します。
最終変更日	earlier than later than 次の値と等しい not on	テキストボックスに、エージェントグループの最終変更日を入力します。 変更には次のものがあります。 • エージェントの名前または説明の変更 • グループへのエージェントの追加 • グループからのエージェントの削除

フリーズウィンドウ

フリーズ期間を使用すると、リンクされているすべてのエージェントに対して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

フリーズ期間を使用すると、リンクされているエージェントは次の動作を行うことはできません。

- 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

> **注意:** フリーズ期間は、エージェントプロファイルとNessus Agent更新プランの両方をオーバーライドします。エージェントをフリーズ期間に割り当て、フリーズ期間を有効にした場合、エージェントのエージェントプロファイルやエージェントの更新プランによって通常発生するすべてのバージョンの更新がブロックされます。

フリーズ期間の作成と管理を行う方法

- フリーズ期間の作成
- フリーズ期間の変更
- フリーズ期間を有効または無効にする
- フリーズ期間の削除

フリーズ期間の作成

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

フリーズ期間を作成するには、次の手順を使用します。

フリーズ期間はリンクされているすべてのエージェントに適用され、スケジュールされた期間中、エージェントはソフトウェア更新プログラムを取得および適用できなくなります。エージェントはこれらのウィンドウ内でもプラグイン更新プログラムは取得でき、スケジュールされたスキャンを引き続き実行できます。

リンクされたエージェントのフリーズウィンドウを作成するには:

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[フリーズ期間]** を選択します。

6. ⊕**[新しいフリーズ期間]** をクリックします。

   [新しいフリーズ期間] プレーンが表示されます。

7. 必要に応じてオプションを設定します。

8. **[保存]** をクリックします。

   フリーズ期間が保存され、**[フリーズ期間]** ページに表示されます。

フリーズ期間を編集する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

この手順を使用して、Tenable Vulnerability Management のエージェントスキャン用のフリーズ期間を管理します。

フリーズ期間を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[フリーズ期間]** を選択します。

   フリーズ期間のリストが表示されます。

6. フリーズ期間の表で、変更するフリーズ期間をクリックします。

   [フリーズ期間の更新] ページが表示されます。

7. 必要に応じてオプションを編集します。

8. **[保存]** をクリックして変更を保存します。

   Tenable Vulnerability Management によりフリーズ期間に対する変更が保存されます。

フリーズ期間を有効または無効にする

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management でリンクされているエージェントのフリーズ期間を有効または無効にするには、この手順を使用します。

新しいインターフェースでリンクされたエージェントに対してフリーズ期間を有効または無効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[フリーズ期間]** を選択します。

6. 有効または無効にするフリーズ期間を検索します。

7. 有効または無効にするフリーズ期間の行で、**[ステータス]** トグルをクリックします。

   フリーズ期間が有効または無効になり、確認ウィンドウが表示されます。

フリーズ期間のエクスポート

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

[センサー] ページでは、1 つ以上のフリーズ期間を CSV または JSON 形式でエクスポートできます。

フリーズ期間をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[フリーズ期間]** を選択します。

   フリーズ期間のリストが表示されます。

6. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

7. 選択したフリーズ期間をエクスポートします。

範囲	アクション
1 つのフリーズ期間をエクスポート	a. フリーズ期間表で、次のいずれかを実行します。 • エクスポートするフリーズ期間の行を右クリックします。 アクションオプションが行に表示されます。

する場合	• **[アクション]** 列で、エクスポートするフリーズ期間の行にある ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。 • エクスポートするフリーズ期間のチェックボックスを選択します アクションバーが表の上部に表示されます。 b. [→ **[エクスポート]** をクリックします。
複数のフリーズ期間をエクスポートする場合	a. フリーズ期間の表で、エクスポートする各フリーズ期間のチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** 個別に選択してエクスポートできるフリーズ期間は最大 200 個です。200 個以上のフリーズ期間をエクスポートする場合は、フリーズ期間の表の上部にあるチェックボックスを選択して、Tenable Vulnerability Management インスタンス上のすべてのフリーズ期間を選択してから、[→**[エクスポート]** をクリックする必要があります。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- メール通知を設定するためのトグル

8. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
9. 使用するエクスポート形式をクリックします。

形式	説明
CSV	フリーズ期間のリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたフリーズ期間のリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

10. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
11. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

    - **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      注意: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

フリーズ期間の削除

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

この手順を使用して、Tenable Vulnerability Management でエージェントスキャン用のフリーズ期間を削除します。

エージェントスキャン用のフリーズウィンドウを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

   エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

5. ドロップダウンボックスで、**[フリーズ期間]** を選択します。

   フリーズ期間のリストが表示されます。

6. 選択したフリーズ期間を削除します。

範囲	アクション
単一のフリーズ期間を削除する	a. フリーズ期間表で、次のいずれかを実行します。 • 削除するウィンドウを右クリックします。 アクションオプションが行に表示されます。 • **[アクション]** 列で、削除するフリーズ期間の行にある ⋮ ボタンをクリックします。

	アクションオプションが行に表示されます。 • 削除するフリーズ期間のチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. **[削除]** をクリックします。 確認ウィンドウが表示されます。
複数のフリーズ期間を削除する	a. フリーズ期間の表で、削除する各ウィンドウの横にあるチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. **[削除]** をクリックします。 確認ウィンドウが表示されます。

7. **[削除]** をクリックして、削除を確定します。

   Tenable Vulnerability Management により、選択した 1 つまたは複数のフリーズ期間が削除されます。

プラグインのアップデート

次の表は、Tenable Vulnerability Management にリンクされているエージェントの差分プラグイン更新の動作を示しています。

リンク先	差分アップデート	完全な更新
Tenable Vulnerability Management	エージェントは、24 時間に一度、Tenable Vulnerability Management に差分更新をリクエストします。	エージェントは、特定のスキャンポリシーに対してすべてのプラグインセットを必要とする場合には、スキャン時にプラグインの完全な更新を実行します。 エージェントは、設定可能な時間が経過すると、未使用のプラグインセットも削除します。時間の経過後、エージェントは完全な更新を実行し、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。

ネットワーク

大企業では、同じ内部 IP アドレスの環境をデプロイすることで、場所の設定とメンテナンスにかかる時間とコストを節約できます。複数の環境で内部 IP アドレスが同じである資産の曖昧さをなくすには、Tenable Vulnerability Management のネットワークを使用します。ネットワークを使用して、レポート、ロールベースのアクセス制御 (RBAC)、タグ付けのために資産を理論上分離することもできます。

同じ内部 IP アドレスの環境をデプロイする場合は、各環境に対してネットワークを作成し、各ネットワークにスキャナーとスキャナーグループを割り当てます。スキャナーで資産がスキャンされると、関連するネットワークが資産の詳細に追加されます。ネットワークによって資産にフィルターを適用するか、ネットワークに基づいて動的タグを作成できます。変更ルールとアクセスグループは、ネットワークに対応していません。

スキャナーやスキャナーグループは、一度に 1 つのネットワークのみに属します。

ネットワークには次の 2 種類があります。

- **デフォルトのネットワーク** - カスタムネットワークに割り当てられていないスキャナーやスキャナーグループが属するネットワーク。

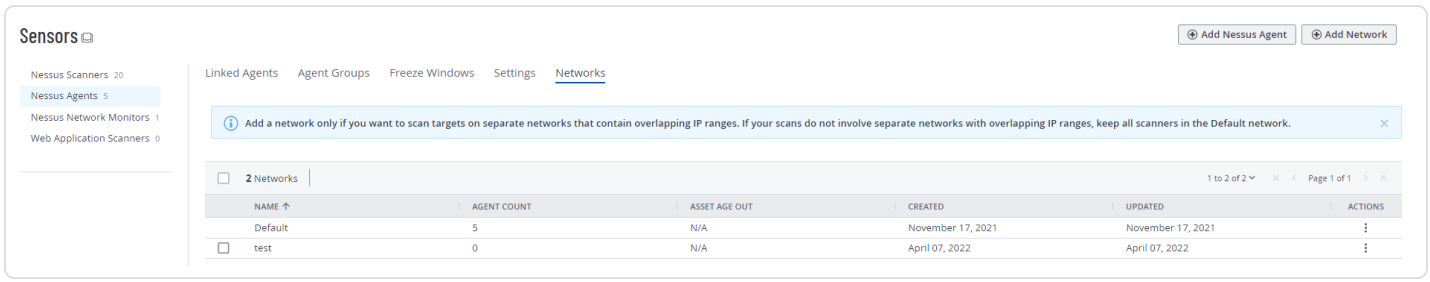
  デフォルトネットワークのスキャナーは表示できますが、追加や削除はできません。カスタムネットワークからスキャナーやスキャナーグループを削除するか、またはカスタムネットワークを削除すると、Tenable Vulnerability Management はスキャナーやスキャナーグループをデフォルトネットワークに戻します。インポートされたスキャンは、常にデフォルトネットワークに属します。

  > **注意:** AWS 事前認証スキャナーからの資産は、*デフォルト*ネットワークにのみ表示可能です。

  > **注意:** エージェントをカスタムネットワークから**デフォルト**ネットワークに移動した場合は、エージェントの関連資産を**デフォルト**ネットワークに手動で移動する必要があります。資産が自動的に**デフォルト**ネットワークに戻ることはありません。詳細は、ネットワークへのエージェントの追加と[設定]で資産をネットワークに移動するを参照してください。

- **カスタムのネットワーク** - ユーザーが作成するカスタムネットワーク。カスタムネットワークを使用すると、ビジネスニーズに基づいてさまざまなスキャナーや資産をグループ化して分類できます。たとえば、異なるサブ組織、外部スキャンと内部スキャン、一時的スキャンと静的スキャンのネットワークを作成できます。

  > **警告:** スキャナーと同じネットワーク内にない資産をスキャナーがスキャンすると、重複した資産レコードが作成されます。したがって、スキャンの開始前に、新しいスキャナーまたはスキャナーグループが正しいネットワークに含まれていることを確認する必要があります。


Sensors
Add Nessus Agent
Add Network
Nessus Scanners 20
Nessus Agents 5
Nessus Network Monitors 1
Web Application Scanners 0
Linked Agents
Agent Groups
Freeze Windows
Settings
Networks
Add a network only if you want to scan targets on separate networks that contain overlapping IP ranges. If your scans do not involve separate networks with overlapping IP ranges, keep all scanners in the Default network.
2 Networks
1 to 2 of 2
Page 1 of 1
NAME
AGENT COUNT
ASSET AGE OUT
CREATED
UPDATED
ACTIONS
Default 5 N/A November 17, 2021 November 17, 2021
test 0 N/A April 07, 2022 April 07, 2022

ネットワークを作成する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

IP 範囲が重複する別々の環境にあるターゲットをスキャンする場合にのみ、カスタムネットワークを作成します。スキャンが重複する IP 範囲を持つ別々の環境に関係しない場合は、すべてのスキャナーを **[デフォルト]** ネットワークに保持します。

新規ネットワークを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[ネットワーク]** タブをクリックします。

   ネットワークのリストが表示されます。

5. ⊕ **[ネットワークを追加する]** をクリックします。

   [設定] ページが表示されます。

6. ネットワークの名前を入力します。

7. (オプション) ネットワークの説明を入力します。

8. (オプション) **[資産エイジアウト]** を設定します。

   注意: デフォルトでは、**[資産エイジアウト]** トグルは有効になっており、値は 180 日に設定されています。この日数が経過した時点で、Tenable Vulnerability Management はすべての資産レコードと関連する脆弱性を削除します。これらは復元することはできず、削除された資産はライセンスにカウントされなくなります。

- 検出されない資産を Tenable Vulnerability Management が削除するまでの日数を変更するには、**[日表示されていない資産の削除]** テキストボックスに日数を入力します。
- **[資産エイジアウト]** トグルを無効にするには、トグルをクリックします。

9. 右下の **[作成]** をクリックします。

   Tenable Vulnerability Management により新しいネットワークが作成されます。**[スキャナーの管理]** ページが表示されます。

ネットワークを表示または編集する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

既存のネットワークの設定を表示または編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[ネットワーク]** タブをクリックします。

   ネットワークのリストが表示されます。

5. **ネットワーク**の表で、編集するネットワークをクリックします。

   [ネットワークの詳細] ページが表示され、**[設定]** タブがアクティブになります。

6. ネットワークの詳細を変更します。

   a. ネットワークの**名前**または**説明**を編集します。名前には、任意の英数字、および < と > 以外の特殊文字を使用できます。

   b. **[資産の期限切れ]** をオンにして、特定の日数の間にスキャンで確認されなかったネットワーク資産を完全に削除します。

   c. 表示されたテキストボックスに日数を入力します。最小値は 14 で、最大値は 450 です。

   警告: このオプションを有効にして保存すると、Tenable Vulnerability Management は資産を即座に削除します。すべての資産レコードおよび関連付けられた脆弱性が削除され、復元することはできません。削除された資産は、ライセンスにカウントされなくなります。

> **注意**: 15 か月 (456 日) より前の資産を期限切れにすることはできません。これらの資産を削除するには、**[資産]** ワークベンチでフィルターを掛けて表示してから手動で削除します。詳細は、資産の削除を参照してください。

7. **[保存]** をクリックします。

   Tenable Vulnerability Management により変更が保存されます。

ネットワークにスキャナーを追加する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

スキャナーやスキャナーグループは、カスタムネットワークに追加しない限り、デフォルトネットワークに属します。スキャナーやスキャナーグループは、同時に 1 つのネットワークにのみ属することができます。

スキャナーグループをカスタムネットワークに追加できるのは、そのグループ内のすべてのスキャナーがデフォルトネットワークまたは同じカスタムネットワークに属している場合のみです。別のカスタムネットワークに既に割り当てられているスキャナーを含むスキャナーグループを追加しようとすると、Tenable Vulnerability Managementは、競合を解決するまでそのスキャナーグループをネットワークに追加できないようにします。

AWS 事前認証スキャナーをネットワークに追加することはできません。

始める前に

- 新しいネットワークを作成します。

  注意: 不要な資産の統合を防ぐため、Tenable では既存のネットワークではなく新しいネットワークにスキャナーを移動することを推奨しています。スキャナーを移動するネットワークに資産のレコードが既にあり、移動されたスキャナーに由来する資産の識別子がネットワークに既に存在する識別子と一致する場合、Tenable Vulnerability Management はそれらの資産を自動的に統合します。

- ある既存のネットワークから、別の既存のネットワークにスキャナーを移動する場合は:
  - 移動するスキャナーにより識別された資産の IP アドレスをメモします。
  - その IP アドレスを使用して、資産を最初のネットワークから 2 番目のネットワークに移動します。
  - 最初のネットワークから2番目のネットワークへと、スキャナーを追加します。次の手順を使用してスキャナーを追加します。

スキャナーやスキャナーグループをネットワークに追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[ネットワーク]** タブをクリックします。

   ネットワークのリストが表示されます。

5. ネットワークの表で、スキャナーまたはスキャナーグループを追加するネットワークをクリックします。

   [設定] ページが表示されます。

6. 左側のナビゲーションリストで、**[スキャナーの管理]** をクリックします。

   [追加可能なスキャナー] と **[ネットワークのメンバースキャナー]** のリストが表示されます。

7. ネットワークに追加するスキャナーまたはスキャナーグループの行で、⊕ ボタンをクリックします。

   Tenable Vulnerability Management は、スキャナーグループの競合があるかどうかを判断します。

   競合がない場合、Tenable Vulnerability Management はスキャナーまたはスキャナーグループをネットワークに追加し、それを [メンバースキャナー] 表に移動します。

   競合がある場合、Tenable Vulnerability Management はメッセージを表示します。スキャナーグループからあるスキャナーを削除して、競合を解消する必要があります。スキャナーグループからスキャナーを削除する方法の詳細は、スキャナーグループを編集するを参照してください。

   スキャナーまたはスキャナーグループが **[ネットワークのメンバースキャナー]** に表示されます。

ネットワークからスキャナーを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

カスタムネットワークからスキャナーまたはスキャナーグループを削除すると、Tenable Vulnerability Management はそれをデフォルトネットワークに再割り当てします。

ヒント: スキャナーグループを削除する場合、またはスキャナーグループからセンサーを削除する場合は、スキャナーグループを削除するとスキャナーグループからセンサーを削除するを参照してください。

ネットワークからスキャナーまたはスキャナーグループを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[ネットワーク]** タブをクリックします。

   ネットワークのリストが表示されます。

5. ネットワークの表で、スキャナーまたはスキャナーグループを削除するネットワークをクリックします。

   [設定] ページが表示されます。

6. 左側のナビゲーションプレーンで、**[スキャナーの管理]** をクリックします。

   [追加可能なスキャナー] と **[ネットワークのメンバースキャナー]** のリストが表示されます。

7. ネットワークから削除するスキャナーまたはスキャナーグループの行で、✕ ボタンをクリックします。

   Tenable Vulnerability Management は、スキャナーまたはスキャナーグループをデフォルトネットワークに移動します。スキャナーまたはスキャナーグループは **[使用可能なスキャナー]** リストに表示されます。

ネットワークへのエージェントの追加

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

エージェントは、カスタムネットワークに追加しない限り *Default* ネットワークに属します。エージェントは同時に 1 つのネットワークにしか所属できません。

注意: 1 つ以上のエージェントを 1 つのネットワークに割り当てたときに、その中のいずれかのエージェントが既に別のカスタムネットワークに割り当てられていた場合、「このネットワークにエージェントを追加することで、エージェントは以前のネットワークから割り当て換えされる」ことを示す確認メッセージが表示されます。

始める前に

- 新しいネットワークを作成します。

  注意: 不要な資産の統合を防ぐため、Tenable では既存のネットワークではなく新しいネットワークにエージェントを移動することを推奨しています。エージェントを移動するネットワークに資産のレコードが既にあり、移動されたエージェントに由来する資産の識別子がネットワークに既に存在する識別子と一致した場合、Tenable Vulnerability Management はそれらの資産を自動的に統合します。

- ある既存のネットワークから、別の既存のネットワークにエージェントを移動する場合は、次を行います。

  - 移動するエージェントによって識別された資産の IP アドレスをメモします。
  - その IP アドレスを使用して、資産を最初のネットワークから 2 番目のネットワークに移動します。
  - 最初のネットワークから 2 番目のネットワークに、エージェントを追加します。

エージェントをネットワークに追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

[センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 次のいずれかを行います。

   - **[リンクされたエージェント]** タブからエージェントを追加する方法

     a. **[Nessus エージェント]** タブをクリックします。

     エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

     b. 次のいずれかの方法で、1 つまたは複数のエージェントを選択します。

     - エージェントの表で、追加するエージェントの行を右クリックします。

       アクションボタンが行に表示されます。

     - **[アクション]** 列で、削除するフリーズ期間の行にある ⋮ ボタンをクリックします。

       アクションボタンが行に表示されます。

     - エージェントの表で、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。

       表の上部にアクションバーが表示されます。

     - 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。

     ページの下部またはに、アクションバーが表示されます。

     c. 必要に応じて、**[ネットワークに追加]** または **[選択したものをネットワークに追加]** をクリックします。

     [ネットワークに追加] プレーンが表示されます。

     d. ドロップダウンリストで、1 つまたは複数のエージェントを追加するネットワークを選択します。

     e. **[割り当て]** をクリックします。

     Tenable Vulnerability Management により、選択したネットワークにエージェントが追加されます。

- **[ネットワーク]** ページからエージェントを追加する方法

  a. **[ネットワーク]** タブをクリックします。

     ネットワークのリストが表示されます。

  b. ネットワークの表で、エージェントを追加するネットワークをクリックします。

     [設定] ページが表示されます。

  c. 左側のナビゲーションリストで、**[エージェントの管理]** をクリックします。

     [追加できるエージェント] と **[ネットワークのメンバーエージェント]** の 2 つのリストが表示されます。

  d. ネットワークに追加するエージェントの行で、⊕ ボタンをクリックします。

     Tenable Vulnerability Management は、エージェントグループの競合があるかどうかを判断します。手作業で競合を解消したら、上記の手順を繰り返します。

     グループの競合がなければ、Tenable Vulnerability Management はエージェントをネットワークに追加します。

エージェントをカスタムネットワークから **デフォルト** ネットワークに移動した場合は、エージェントの関連資産を **デフォルト** ネットワークに手動で移動する必要があります。資産が自動的に **デフォルト** ネットワークに戻ることはありません。詳細は、[設定]で資産をネットワークに移動するを参照してください。

エージェントグループをネットワークに追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[Nessus エージェント]** タブをクリックします。

エージェントのリストが表示され、ドロップダウンボックスで**[リンクされたエージェント]**が選択されます。

5. エージェントの表をフィルタリングして、ネットワークに追加するエージェントグループを表示します。

   a. **[フィルター]**をクリックします。

   b. **[カテゴリ]**ドロップダウンリストから**[グループのメンバー]**を選択します。

   c. **[値]**ドロップダウンリストで、追加するエージェントグループを選択します。

   d. **[適用]**をクリックします。

6. エージェントの表のヘッダーにあるチェックボックスを選択して、ページ全体を選択します。

   ページの下部またはに、アクションバーが表示されます。

7. アクションバーで、**[選択したものをネットワークに追加]**をクリックします。

   [ネットワークに追加]プレーンが表示されます。

8. ドロップダウンで、1つまたは複数のエージェントを追加するネットワークを選択します。

9. **[割り当て]**をクリックします。

   Tenable Vulnerability Managementにより、選択したネットワークにエージェントが追加されます。

   エージェントをカスタムネットワークから**デフォルト**ネットワークに移動した場合は、エージェントの関連資産を**デフォルト**ネットワークに手動で移動する必要があります。資産が自動的に**デフォルト**ネットワークに戻ることはありません。詳細は、[設定]で資産をネットワークに移動するを参照してください。

ネットワークからのエージェントの削除

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

始める前に

- ある既存のネットワークから、別の既存のネットワークにエージェントを移動する場合は、次を行います。
    - 移動するエージェントによって識別された資産の IP アドレスをメモします。
    - その IP アドレスを使用して、資産を最初のネットワークから 2 番目のネットワークに移動します。
    - 最初のネットワークから 2 番目のネットワークに、エージェントを追加します。

ネットワークからエージェントを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 次のいずれかを行います。

    - **[リンクされたエージェント]** タブからエージェントを削除します。

        a. **[Nessus エージェント]** タブをクリックします。

        エージェントのリストが表示され、ドロップダウンボックスで **[リンクされたエージェント]** が選択されます。

        b. 次のいずれかの方法で、1 つまたは複数のエージェントを選択します。

- エージェントの表で、削除するエージェントの行を右クリックします。

  アクションボタンが行に表示されます。

- エージェントの表で、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。

  Tenable Vulnerability Management により、アクションバーの **[ネットワークから選択したものを削除]** が有効になります。

- 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。

  ページの下部またはに、アクションバーが表示されます。

c. 必要に応じて、**[ネットワークからの削除]** または **[ネットワークから選択したものを削除]** をクリックします。

   Tenable Vulnerability Management によってエージェントがネットワークから削除され、*Default* ネットワークに追加されます。

- **[ネットワーク]** タブからエージェントを削除します。

a. **[ネットワーク]** タブをクリックします。

   ネットワークのリストが表示されます。

b. ネットワークの表で、1 つまたは複数のエージェントを削除するネットワークを選択します。

   [設定] ページが表示されます。

c. 左側のナビゲーションメニューで **[エージェントの管理]** をクリックします。

   [追加できるエージェント] と **[ネットワークのメンバーエージェント]** の 2 つのリストが表示されます。

d. ネットワークから削除するエージェントの行で、× ボタンをクリックします。

   Tenable Vulnerability Management によってエージェントがネットワークから削除され、*Default* ネットワークに追加されます。<<スキャナーグループの競合と同様の場合は、SME に問い合わせてください。その場合は同じドキュメントを参照してください。>>

[設定] で資産をネットワークに移動する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

スキャナーは資産のスキャン時に、自身が属しているネットワークをスキャンした資産の識別情報に自動的に追加します。ただし、資産が割り当てられているネットワークを変更する場合は、資産を手動でネットワークに移動することもできます。

新しいネットワークに資産を移動するときは、その新しいネットワークでスキャンを実行する前に資産を移動してください。既にスキャンを実行したことのあるネットワークに資産を移動した場合、Tenable Vulnerability Management はライセンスに対してカウントされる重複した資産レコードを作成する可能性があります。

ヒント: **[調査]** > **[資産]** ワークベンチを使用して、資産をネットワークに移動することもできます。

注意: エージェントまたはエージェントグループをカスタムネットワークから**デフォルト**ネットワークに移動した場合は、エージェントの関連資産を**デフォルト**ネットワークに手動で移動する必要があります。資産が自動的に**デフォルト**ネットワークに戻ることはありません。

1 つまたは複数の資産を、[ネットワーク] ページからネットワークに移動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[ネットワーク]** タブをクリックします。

   ネットワークのリストが表示されます。

5. ネットワーク表で、次のいずれかを実行します。

- 資産の移動元や移動先のネットワークを右クリックします。

  アクションボタンが行に表示されます。

- **[アクション]** 列で、削除するフリーズ期間の行にある ⋮ ボタンをクリックします。

  アクションボタンが行に表示されます。

6. **[資産の移動]** をクリックします。

   [資産の移動] ページが表示されます。

7. **[ソースネットワーク]** ドロップダウンボックスで、資産の移動先となるネットワークを選択します。

8. テキストボックスで、次のいずれかを行います。

   - 1つの資産を検索するには、1つのIPアドレスを入力します。
   - 複数の資産を検索するには、CIDR範囲またはコンマで区切られた個別のIPアドレスを入力します。

   Tenable Vulnerability Managementにより、検索条件に一致する1つまたは複数の資産が表示されます。

9. 次のいずれかを行います。

   - 1つの資産を移動する場合

     a. 資産表で、次のいずれかを行います。

        - 移動する資産を右クリックします。アクションボタンが行に表示されます。
        - **[アクション]** 列で、移動する資産の行にある ⋮ ボタンをクリックします。アクションボタンが行に表示されます。

     a. [資産の移動] をクリックします。

        Tenable Vulnerability Managementにより、選択したネットワークに資産が移動します。

   - 選択した複数の資産を移動する場合

     a. 選択する各資産に対して、アイコンにカーソルを合わせます。

        資産のチェックボックスが表示されます。

b. チェックボックスをクリックします。

ページの下部またはに、アクションバーが表示されます。

c. アクションバーで、 ボタンをクリックします。

Tenable Vulnerability Management により、選択された 1 つまたは複数の資産が移動元のネットワークから移動先のネットワークに移動します。

- 現在のページにあるすべての資産を移動する場合

a. 資産の表のヘッダーで、チェックボックスをクリックします。

Tenable Vulnerability Management により、現在のページにあるすべての資産が選択されます。ページの下部またはに、アクションバーが表示されます。

b. アクションバーで、 ボタンをクリックします。

Tenable Vulnerability Management が、選択された資産を移動元のネットワークから移動先のネットワークに移動します。

- 移動元のネットワークにあるすべての資産を移動する場合

a. 資産の アイコンにカーソルを合わせます。

ページの下部またはに、アクションバーが表示されます。

b. アクションバーで、**[すべての資産を選択]** をクリックします。

Tenable Vulnerability Management により、移動元のネットワークにあるすべての資産が選択されます。

c. アクションバーで、 ボタンをクリックします。

Tenable Vulnerability Management により、移動元のネットワークのすべての資産が、移動先のネットワークに移動します。

1 つまたは複数の資産を、資産の表からネットワークに移動する方法

1. 左上にある ボタンをクリックします。

左側にナビゲーションプレーンが表示されます。

2. 左側のナビゲーションバーで **[資産]** をクリックします。

[資産] ダッシュボードが開き、資産の表が表示されます。

3. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management の表 を参照してください。
4. (オプション) 保存された検索フィルターを適用します。
5. 次のいずれかを行います。

- 1つの資産を移動する場合

  a. 移動する資産にカーソルを合わせます。

  アクションボタンが行に表示されます。

  b. → ボタンをクリックします。

  c. **[移動]** プレーンが表示されます。

  d. **[デフォルト]** ドロップダウンボックスで、資産の移動先となるネットワークを選択します。

  e. **[移動]** ボタンをクリックします。

  f. Tenable Vulnerability Management により、選択したネットワークに資産が移動します。

- 選択した複数の資産を移動する場合

  a. 移動する各資産に対して、資産の行にあるチェックボックスをクリックします。

  ページの下部またはに、アクションバーが表示されます。

  b. アクションバーで、→ ボタンをクリックします。

  [移動] プレーンが表示されます。

  c. **[デフォルト]** ドロップダウンボックスで、資産の移動先となるネットワークを選択します。

  d. **[移動]** ボタンをクリックします。

  Tenable Vulnerability Management により、選択したネットワークに資産が移動します。

- 現在のページにあるすべての資産を移動する場合

a. 表のヘッダーにあるチェックボックスをクリックします。

ページの下部または上に、アクションバーが表示されます。

b. アクションバーで、→ ボタンをクリックします。

[移動] プレーンが表示されます。

c. **[デフォルト]** ドロップダウンボックスで、資産の移動先となるネットワークを選択します。

d. **[移動]** ボタンをクリックします。

Tenable Vulnerability Management により、選択したネットワークに資産が移動します。

- すべての資産を移動する場合

a. 表のヘッダーにあるチェックボックスをクリックします。

b. ページの下部または上に、アクションバーが表示されます。

c. アクションバーで、**[すべての資産を選択]** をクリックします。

> **注意：[すべての資産を選択]** をクリックすると、現在のページおよび他のページにあるすべての資産が選択されます。

d. アクションバーで、**[移動]** をクリックします。

e. **[移動]** プレーンが表示されます。

f. **[デフォルト]** ドロップダウンボックスで、資産の移動先となるネットワークを選択します。

g. **[移動]** ボタンをクリックします。

h. Tenable Vulnerability Management により、選択したネットワークに資産が移動します。

> **注意：**適用されたフィルターや選択された資産の数によっては、Tenable Vulnerability Management がすべての資産を移動先のネットワークに移動するのに時間がかかる場合があります。

ネットワーク内の資産を削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

ヒント: 資産を削除せずに、ネットワークから削除するには、[設定]で資産をネットワークに移動するを参照してください。

資産を手動で削除する

資産を手動で削除すると、Tenable Vulnerability Management は資産の表のデフォルトビューに資産を表示しなくなり、資産に関連付けられた脆弱性データを削除し、スキャン結果と資産のマッチングを停止します。手動で削除された資産は、資産の期間が 14 日間経過するまでTenable Vulnerability Managementライセンスにカウントされます。

手動で削除した資産を表示するには、削除した資産を表示するを参照してください。

資産を手動で削除する方法

- 1 つの資産を削除します。詳細は、資産を削除するを参照してください。
- 従来のインターフェースで、ネットワーク内の複数の資産を削除します。詳細は、ネットワークから資産を削除する (従来のインターフェース) を参照してください。
- Tenable Vulnerability Management API を使用して複数の資産を削除します。詳細は、Tenable 開発者ポータルを参照してください。

資産を自動的に削除する

ネットワーク内の資産を自動的に削除した場合、Tenable Vulnerability Management は、指定された日数が経過した後に資産およびすべての関連付けられている脆弱性データを完全に削除します。自動的に削除された資産は、Tenable Vulnerability Managementライセンスに対してカウントされません。

資産を自動的に削除するには、ネットワークを作成または編集するときに、**[資産エイジアウト]** 機能を有効にします。

ネットワークのエクスポート

必要なユーザーロール: 管理者

[センサー] ページで、1 つ以上のネットワークをエクスポートできます。

ネットワークをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[ネットワーク]** タブをクリックします。

   ネットワークのリストが表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

6. エクスポートするネットワークを選択します。

エクスポート範囲	アクション
選択されたネットワーク	選択されたネットワークをエクスポートする方法: a. エクスポートする各ネットワークのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. [→ **[エクスポート]** をクリックします。

	注意: [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のネットワークをエクスポートする場合は、リスト内のすべてのネットワークを選択してから、[→ **[エクスポート]** をクリックします。
1 つのネットワーク	1 つのネットワークをエクスポートする方法 a. ネットワークの表で、エクスポートするネットワークの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- ネットワークの表の **[アクション]** 列で、エクスポートするネットワークの行にある ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。 -または- エクスポートするネットワークのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 アクションボタンが行に表示されます。 b. [→ **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。

8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	ネットワークのリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされたネットワークのリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。

10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

    注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

12. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

13. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

14. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポートプレーンを閉じた場合は、エクスポートページからエクスポートファイルにアクセスできます。

ネットワークを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

- ネットワークを削除しても、削除したネットワークにあった資産は依然としてそのネットワーク属性を保持します。
- Tenable Vulnerability Management では、ライセンスのある資産が期限切れになるまで、削除したネットワークの資産レコードを保持します。削除したネットワークを使用する資産にはフィルターを適用できます。
- 削除したネットワークと同じ名前の新しいネットワークは作成できません。

始める前に

ネットワークを削除する前に、次を考慮してください。

- 資産は、ネットワークを削除する前に別のネットワークに移動させることを検討してください。削除したネットワークから別のネットワークに資産を移動するには、Tenable Vulnerability Management API を使用する必要があります。
- Tenable Vulnerability Management は、削除されたネットワークにあるスキャナーまたはスキャナーグループを、デフォルトのネットワークに再び割り当てます。スキャナーまたはスキャナーグループを削除する場合は、スキャナーグループからセンサーを削除する と スキャナーグループを削除する を参照してください。

ネットワークを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[ネットワーク]** タブをクリックします。

ネットワークのリストが表示されます。

5. 選択したネットワークを削除します。

削除範囲	アクション
単一のネットワークを削除する方法	単一のネットワークを削除する方法: a. ネットワークの表で、削除するネットワークの行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- ネットワークの表の**[アクション]**列で、削除するネットワークの行にある ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。 -または- 削除するネットワークのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. 🗑 **[削除]**をクリックします。
複数のネットワークを削除する方法	複数のネットワークを削除する方法: a. ネットワークの表で、削除するネットワークのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. 🗑 **[削除]**をクリックします。

Tenable Vulnerability Management はネットワークを削除します。

リンクされたスキャナー

Tenable Nessus スキャナー、Tenable Nessus Network Monitor インスタンス、Tenable Web App Scanning センサー、または Tenable Nessus Agent センサーをインストールした後、それらを Tenable Vulnerability Management にリンクできます。

リンクされたスキャナーを Tenable Vulnerability Management のスキャンで使用する前に、以下を行う必要があります。

1. 該当する Tenable 製品をセンサーまたはスキャンするホストにインストールします。

センサータイプ	詳細
Tenable Nessus Agent	• 環境 • *Tenable Nessus Agent デプロイメントとユーザーガイド*
Tenable Nessus Network Monitor	の Tenable Nessus Agent のインストール • 環境 • Tenable Nessus Network Monitorを*Tenable Nessus Network Monitor ユーザーガイド* にインストールする • *Tenable Core ユーザーガイド*のTenable Container Security + Tenable Nessus Network Monitor のデプロイまたはインストール
Tenable Nessus	• 環境 • Tenable Nessusを*Tenable Nessus ユーザーガイド* にインストールする • *Tenable Core ユーザーガイド*のTenable Core + Tenable Nessus のデプロイまたはインストール **注意:** Tenable Nessus スキャナーが複数の NIC / インターフェースを持っている場合、スキャナーに対して複数の IPv4/IPv6 アドレスが表示される場合があります。
Tenable Web App Scanning	• 環境 • *Tenable Core ユーザーガイド*の Tenable Core + Tenable Web App Scanning のデプロイまたはインストール

2. センサーを Tenable Vulnerability Management にリンクします。

リンクされたスキャナーを表示する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

リンクされたスキャナーを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

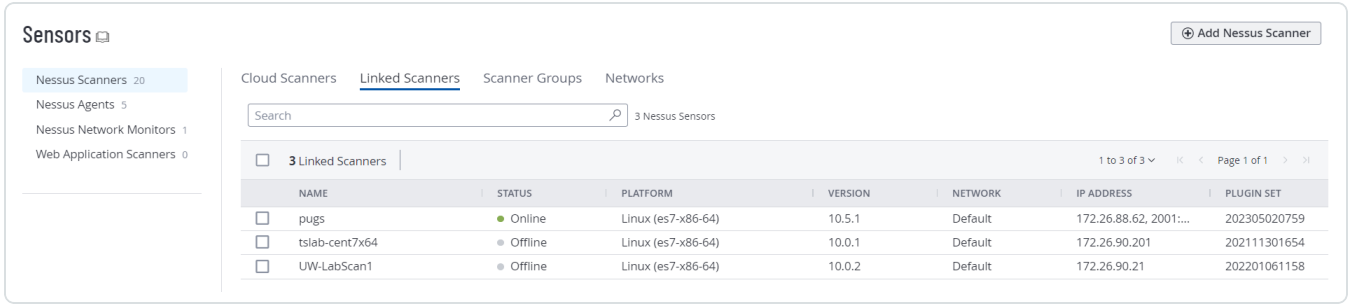
   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 別の種類のリンクされたスキャナーを表示するには、上部のナビゲーションバーで、表示したいリンクされたスキャナーの種類をクリックします。

   Tenable Vulnerability Management により、選択した種類のリンクされたスキャナーが表示されます。



リンクされたスキャナーの名前変更

リンクされたスキャナーの名前は、**[センサー]** メニューから変更できます。名前を変えることで、他のユーザーが容易に識別できるようになります。

注意: クラウドスキャナーの名前を変更することはできません。クラウドスキャナー名は、Tenable が管理しています。

リンクされたスキャナーの名前を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 名前を変更するスキャナーの行をクリックします。

   スキャナーの **[詳細]** ページが表示されます。

5. スキャナー名の横にある ✎ ボタンをクリックします。

6. スキャナー名を編集します。

7. スキャナー名の横にある ✓ ボタンをクリックします。

   Tenable Vulnerability Management で、新しいスキャナー名が保存され、関連する表が新しい名前で更新されます。

リンクされたスキャナーログのダウンロード

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

Tenable Vulnerability Management では、ログとシステム設定データを含むログファイルを、任意のリンクされたスキャナー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 に簡単にデータを提供することができます。

各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。

Tenable Vulnerability Management でリンクされたスキャナーからログをダウンロードする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. リンクされたスキャナーの表で、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。

5. **[ログ]** タブをクリックします。

   表には、以前にダウンロードされたログが表示されます。

6. 右上にある **[リクエストログ]** 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。

   保留中のログはログの表に行として表示されます。Tenable Vulnerability Management は、次回のチェックイン時にスキャナーにログをリクエストします。これには数分かかる場合があります。

7. 利用可能なログのファイルの行で、 ボタンをクリックします。

   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

1. 削除するログの行で、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. 確認ウィンドウで、**[削除]** をクリックします。

   Tenable Vulnerability Management によってログが削除され、表からそのログが削除されます。

保留中または失敗したログのリクエストをキャンセルする方法

- キャンセルする保留中のログまたは失敗したログのリクエスト行で、 ボタンをクリックします。

  Tenable Vulnerability Management によってログのリクエストが削除され、表から削除されます。

リンクされたスキャナーのエクスポート

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

[センサー] ページでは、1 つ以上のリンクされたスキャナーを CSV または JSON 形式でエクスポートできます。

リンクされたスキャナーをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 次のいずれかを行います。

   - Tenable Nessus のリンクされたスキャナーをエクスポートするには、ドロップダウンボックスで **[リンクされたスキャナー]** タブを選択します。

     [リンクされたスキャナー] ページが開き、すべての Tenable Nessus のリンクされたスキャナーを含む表が表示されます。

   - Tenable Nessus Network Monitor のリンクされたスキャナーをエクスポートするには、**[Nessus Network Monitors]** タブをクリックします。

     Tenable Nessus Network Monitor のリンクされたすべてのスキャナーの表が表示されます。

   - Tenable Web App Scanning のリンクされたスキャナーをエクスポートするには、**[Web App Scanners]** タブをクリックします。

     Tenable Web App Scanning にリンクされたスキャナーの表が表示されます。

5. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表

を参照してください。

6. エクスポートするリンクされたスキャナーを選択します。

エクスポート範囲	アクション
1つのリンクされたスキャナー	**[リンクされたスキャナー]** ページから1つのリンクされたスキャナーをエクスポートする方法: a. リンクされたスキャナーの表で、エクスポートするリンクされたスキャナーの行を右クリックします。 -または- リンクされたスキャナーの表にある **[アクション]** 列で、エクスポートするリンクされたスキャナーの行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 -または- エクスポートするリンクされたスキャナーのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. [→ **[エクスポート]** をクリックします。 **[詳細]** ページからエクスポートする方法 a. リンクされたスキャナーの表で、エクスポートするリンクされたスキャナーの行をクリックします。 **[詳細]** ページが表示されます。 b. 右上の [→ **[エクスポート]** ボタンをクリックします。
複数のリンクされたスキャナー	リンクされたスキャナーを複数選択してエクスポートする方法 a. スキャナーの表で、エクスポートする各リンクされたスキャナーのチェックボックスを選択します。 表の上部にアクションバーが表示されます。

	b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→**[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上のスキャナーをエクスポートする場合は、リストにあるすべてのスキャナーを選択して、[→ **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	リンクされたスキャナーのリストを含む CSV テキストファイル **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	リンクされたスキャナーがネストされたリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法

    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。

    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。

11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

    - **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

      注意: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

リンクされたスキャナーの詳細のエクスポート

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

リンクされたスキャナーの **[詳細]** ページでは、リンクされたスキャナーに関する詳細を CSV または JSON 形式でエクスポートできます。

リンクされたスキャナーの詳細をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. リンクされたスキャナーの表で、詳細をエクスポートするリンクされたスキャナーをクリックします。

   [詳細] ページが表示されます。

6. 右上にある [→ **[エクスポート]** をクリックします。

   [エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

   - エクスポートファイル名を設定するテキストボックス
   - 利用可能なエクスポート形式のリスト
   - エクスポートされたファイルに含めるフィールドの設定オプションの表

     注意: デフォルトでは、すべてのフィールドが選択されています。

   - エクスポートの有効期限が切れるまでの日数を設定するテキストボックス

- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

7. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
8. 使用するエクスポート形式をクリックします。

形式	説明
CSV	リンクされたスキャナーに関する詳細の一覧をフィールド別に整理した CSV テキストファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	リンクされたスキャナーに関する詳細をネストした一覧をフィールド別に整理した JSON ファイル。 空のフィールドは JSON ファイルに含まれません。

9. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
10. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

11. (オプション) エクスポートの完了時にメール通知を送信する方法

注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

- **[メール通知]** トグルをクリックします。

  [メール通知] セクションが表示されます。
- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

> **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポート画面を閉じた場合は、[**Export Management View**] でエクスポートファイルにアクセスできます。

差分プラグイン更新

次の表は、Tenable Vulnerability Management にリンクされている Tenable Nessus スキャナーの差分プラグイン更新の動作を示しています。

リンク先	差分更新	完全な更新
Tenable Vulnerability Management	スキャナーは、24 時間ごとに一度、Tenable Vulnerability Management に差分更新をリクエストします。	プラグインがない場合、スキャナーは完全なプラグイン更新を実行します (たとえば、スキャナーを Tenable Vulnerability Management にリンクした直後)。

スキャナーグループ

スキャナグループを使用して、Tenable Vulnerability Management インスタンスにリンクされたスキャナを組織化および管理できます。たとえば、特定の地理的な場所に関連するすべてのセンサーを、「東海岸スキャナー」などの名前のグループに追加できます。

スキャナーは、1 つまたは複数のスキャナーグループに追加できます。

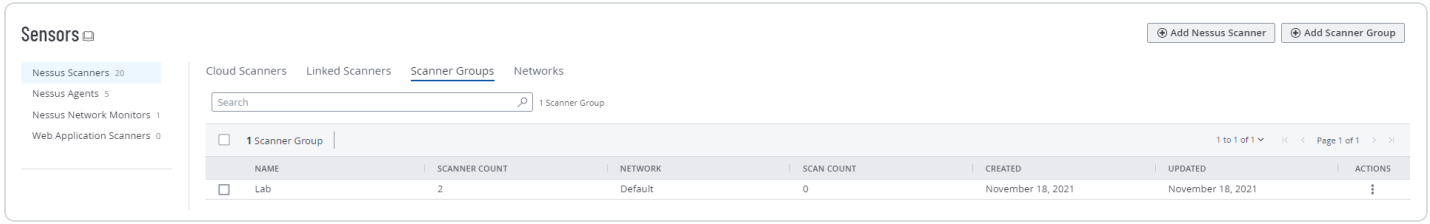
スキャンを作成するときに、スキャンの起動に使用するスキャナーグループを選択できます。もう一つの方法として、**[自動選択]**を選択することにより、そのスキャンに対してスキャンのルーティングを有効にできます。この機能では、スキャナーグループで設定されたターゲットに基づいて、スキャンをスキャナーに割り当てます。

Tenable Vulnerability Management は、スキャナーグループ内で使用するスキャナーを次の基準に基づいて決定します。

- アクティブなスキャナーで、ここ 5 分以内に Tenable Vulnerability Managementと通信している。
- スキャナーは最小限の数のアクティブスキャンを実行しており、最小限の数のホストをスキャンしている。

注意: 企業でスキャンネットワークを利用している場合、同じネットワークに属しているスキャナーのみをスキャナーグループに追加できます。詳細は、ネットワークを参照してください。

注意: リモートスキャナーが**スキャナーグループ**に含まれていて、そのスキャナーの動作中にリンクが解除された場合、スキャン動作は完了しますが、Tenable Vulnerability Management はリンク解除されたスキャナーを今後の使用には含めません。



スキャナーグループを作成する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

新しいインターフェースでスキャナーグループを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. ドロップダウンボックスで、**[スキャナーグループ]** を選択します。

   使用または管理するためのアクセス許可を持つ既存のスキャナーグループのリストが表示されます。

5. ⊕ **[スキャナーグループを追加する]** をクリックします。

   [スキャナーグループを追加] プレーンが表示されます。

6. **[グループ名]** フィールドに、グループの名前を入力します。

7. (オプション) **[スキャンルーティングのターゲット]** ボックスで、スキャンのルーティングのターゲットをコンマ区切りのリスト形式で入力します。

   リスト内のターゲットは、対応する形式に従う必要があります。

   このリストでは、スキャンが **[自動選択]** スキャナーを使用するように設定されている場合に、このスキャナーグループ内のスキャナーによってスキャン可能となるターゲットを指定します。詳細については、例: スキャンのルーティングを参照してください。

   注意: 個別のスキャナーグループに対して、最大 10,000 の個別のスキャンのルーティングターゲットを指定できます。たとえば、`192.168.0.1, example.com, *.example.net, 192.168.0.0/24` では、4 つのスキャンのルーティングターゲットを指定しています。スキャンのルーティングのターゲットのリストを集約するために、Tenable では個別の IP アドレスの代わりに、ワイルドカードや範囲指定形式の使用を推奨しています。

8. (オプション) スキャナーグループのユーザーのアクセス許可を設定します。

   デフォルトでは、新しいスキャナーグループでは、Tenable Vulnerability Management がシステム生成の **[すべてのユーザー]** グループに **[使用可]** アクセス許可を割り当てます。

9. **[保存]** をクリックします。

   [スキャンルーティングのターゲット] で最大数を超えるターゲットが指定されている場合、エラーメッセージが表示されます。個別の IP アドレスの代わりにワイルドカードや範囲指定の形式を使用して、スキャンのルーティングターゲットを集約した後で、スキャナーグループの保存を再試行してください。

   そうでない場合には、新しいグループが **[スキャナーグループ]** リストに表示されます。

スキャナーグループの変更

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

スキャナーグループを変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. ドロップダウンボックスで、**[スキャナーグループ]** を選択します。

   使用または管理するためのアクセス許可を持つ既存のスキャナーグループのリストが表示されます。

5. (オプション) 変更するグループの表を検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

6. スキャナーグループ表で、次のいずれかを実行します。

   変更するスキャナーグループの

   - **[アクション]** 列で、⋮ ボタンをクリックします。

     アクションオプションが行に表示されます。

   - 変更するスキャナーグループを右クリックします。

     アクションオプションがカーソルの横に表示されます。

7. **[編集]** をクリックします。

   [スキャナーグループの編集] プレーンが表示されます。

8. 次のいずれかの設定を変更します。

設定	アクション
名前	新しい名前を入力します。
ユーザーおよびグループのアクセス許可	スキャナーグループのユーザーアクセス許可を設定します。

9. (オプション) **[スキャンルーティングのターゲット]** ボックスで、スキャンのルーティングのターゲットをコンマ区切りのリスト形式で入力します。

   リスト内のターゲットは、対応する形式に従う必要があります。

   このリストでは、スキャンが **[自動選択]** スキャナーを使用するように設定されている場合に、このスキャナーグループ内のスキャナーによってスキャン可能となるターゲットを指定します。詳細については、例：スキャンのルーティングを参照してください。

   > **注意：** 個別のスキャナーグループに対して、最大 10,000 の個別のスキャンのルーティングターゲットを指定できます。たとえば、`192.168.0.1, example.com, *.example.net, 192.168.0.0/24` では、4 つのスキャンのルーティングターゲットを指定しています。スキャンのルーティングのターゲットのリストを集約するために、Tenable では個別の IP アドレスの代わりに、ワイルドカードや範囲指定形式の使用を推奨しています。

10. **[保存]** をクリックします。

    [スキャンルーティングのターゲット] で最大数を超えるターゲットが指定されている場合、エラーメッセージが表示されます。個別の IP アドレスの代わりにワイルドカードや範囲指定の形式を使用して、スキャンのルーティングターゲットを集約した後で、スキャナーグループの保存を再試行してください。

    それ以外の場合には、Tenable Vulnerability Management は変更を反映してスキャナーグループを更新します。

スキャナーグループにスキャナーを割り当てる方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. (オプション) Tenable Web App Scanning については、**[Web App Scanners]** タブをクリックします。

   [Web App Scanners] タブが表示され、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されます。

5. ドロップダウンボックスで、**[スキャナーグループ]** を選択します。

   使用または管理するためのアクセス許可を持つ既存のスキャナーグループのリストが表示されます。

6. スキャナーグループの表で、スキャナーを追加するスキャナーグループの行をクリックします。

   [グループの詳細] ページが表示されます。

7. ⊕ **[スキャナーの割り当て]** をクリックします。

   [スキャナーの割り当て] ページが表示されます。

8. (オプション) テーブルで割り当てるスキャナーを検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

9. スキャナーテーブルで、スキャナーグループに追加する1つまたは複数のスキャナーの横にあるチェックボックスを選択します。

10. **[割り当て]** をクリックします。

    割り当てが成功すると、Tenable Vulnerability Management によってスキャナーがスキャナーグループに追加され、**[グループの詳細]** ページが表示されます。
    Tenable Vulnerability Management の処理中に何らかの問題が発生した場合、**[スキャナーの割り当て]** ページがアクティブなままとなり、影響を受けているスキャナーの **[割り当て]** 列に次のいずれかのメッセージが表示されます。

表示される可能性があるエラーメッセージ	アクション
このセンサーは既にスキャナーグループに存在しています。	**[キャンセル]** をクリックして、ページを閉じます。
このセンサーをスキャナーグループに追加する	**[割り当て]** を再度クリックします。処理が継続

際にエラーが発生しました。	して失敗する場合は、Tenable サポート に連絡してください。

スキャナーグループのユーザーのアクセス許可を設定する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

個別のユーザーまたはユーザーグループに対して、スキャナーグループのアクセス許可を設定できます。ユーザーグループに対してスキャナーグループのアクセス許可を設定する場合、グループ内のすべてのユーザーに同じアクセス許可を割り当てます。詳細については、ユーザーグループを参照してください。

ユーザーまたはユーザーグループに対して、次のスキャナーグループのアクセス許可を割り当てることができます。

- **アクセスなし** - (**[すべてのユーザー]** ユーザーグループのみ) (特別にアクセス許可を割り当てたユーザーやグループを除く) すべてのユーザーは、スキャン設定でスキャナーグループを使用できません。
- **使用可** - ユーザーまたはユーザーグループは、スキャン設定でスキャナーグループを使用できます。ユーザーまたはグループはスキャナーグループの設定を表示することはできますが編集することはできません。
- **管理可** - ユーザーまたはグループはスキャン設定でスキャナーグループを使用できます。ユーザーまたはグループはスキャナーグループの設定を表示および編集することはできます。

スキャナーグループのユーザーのアクセス許可を設定する方法

1. スキャナーグループを作成または編集します。
2. スキャナーグループの設定中に、**[ユーザーとグループ]** セクションで、次のいずれかを行います。

    - **[すべてのユーザー]** ユーザーグループのアクセス許可を編集する。

        a. **[すべてのユーザー]** グループ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。

    - ユーザーまたはユーザーグループをスキャナーグループに追加する。

a. **[ユーザーとグループ]** 見出しで、⊕ ボタンをクリックします。

[ユーザーとグループを追加する] プレーンが表示されます。

b. **[検索]** フィールドで、入力するかドロップダウンをクリックして検索し、ユーザーまたはグループを追加します。

> **ヒント**: 個別のユーザーは企業を離れたり企業に加わったりすることがあるので、Tenable では、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。

追加したユーザーとグループが **[検索]** フィールドの下に表示されます。

c. **[追加]** ボタンをクリックします。

スキャナーグループプレーンが表示されます。

デフォルトでは、Tenable Vulnerability Management は、**[使用可]** アクセス許可を追加されたユーザーまたはユーザーグループに割り当てます。

- 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編集する。

a. 編集するユーザーまたはグループ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。

- ユーザーまたはユーザーグループをスキャナーグループから削除する。

a. 削除するユーザーまたはグループにカーソルを合わせます。

b. その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。

ユーザーまたはグループが **[ユーザーとグループ]** リストから消えます。

3. **[保存]** をクリックします。

Tenable Vulnerability Managementにより、スキャナーグループへの変更が保存されます。

次の手順

- スキャン設定のスキャナーグループを使用します。

スキャナーグループを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

1 つ以上のスキャナーグループを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. ドロップダウンボックスで、**[スキャナーグループ]** を選択します。

   使用または管理するためのアクセス許可を持つ既存のスキャナーグループのリストが表示されます。

5. スキャナーグループの表で、削除する 1 つ以上のスキャナーグループを選択します。

範囲	アクション
1 つのスキャナーグループを削除する方法	a. スキャナーグループ表で、次のいずれかを実行します。 • 削除するスキャナーグループのチェックボックスを選択します。 表の上部にアクションバーが表示されます。 • 削除するスキャナーグループを右クリックします。 アクションオプションがカーソルの横に表示されます。 • **[アクション]** 列で、削除するスキャナーグループの ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。

	b. **[削除]** をクリックします。 確認ウィンドウが表示されます。
複数のスキャナーグループを削除する方法	a. スキャナーグループの表で、削除するスキャナーグループの横にあるチェックボックスを選択します。 ページの下部またはに、アクションバーが表示されます。 b. アクションバーで、**[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。

6. 確認ウィンドウで、**[削除]** ボタンをクリックします。

   Tenable Vulnerability Management により、選択した 1 つまたは複数のグループが削除されます。

センサーのスキャナーグループへの追加

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

次のタイプのセンサーをスキャナーグループに追加できます。

センサータイプ	導入環境
オンプレミス Tenable Nessus	○
オンプレミス Tenable Web App Scanning	○
Tenable Vulnerability Management クラウド	×
Amazon Web Services (AWS) 向け Tenable Nessus センサー	×
Tenable Nessus Network Monitor (NNM)	×
Tenable Nessus Agent	× (エージェントグループ参照)

新しいインターフェースで、センサーを 1 つまたは複数のスキャナーグループに追加する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. (オプション) スキャナーグループに追加するスキャナーを検索します。

5. 追加するスキャナーと、スキャナーの追加先となるグループを選択します。

範囲	アクション
1 つのスキャナーを 1 つまたは複	a. スキャナーグループ表で、次のいずれかを実行します。

数のグループに追加する	• スキャナーグループに追加するセンサーを右クリックします。 アクションオプションがカーソルの横に表示されます。 • **[アクション]** 列で、スキャナーグループに追加するセンサーの ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。 • スキャナーグループに追加するセンサーのチェックボックスを選択します。 Tenable Vulnerability Management は、アクションバーの **[選択したものをグループに追加]** を有効にします。 b. 🗁 **[グループに追加する]** をクリックします。 **[グループに追加する]** プレーンが表示されます。 c. 検索ボックスに、スキャナーを追加するスキャナーグループの名前を入力します。 d. 一致グループのドロップダウンボックスでグループをクリックします。 e. (オプション) 手順 c と d を繰り返して他のスキャナーグループを追加します。
複数のスキャナーを 1 つまたは複数のグループに追加する	a. スキャナーの表で、スキャナーグループに追加するスキャナーの横にあるチェックボックスを選択します。 ページの下部またはに、アクションバーが表示されます。 b. 🗁 **[選択したものをグループに追加]** ボタンをクリックします。

	[グループに追加する] プレーンが表示されます。 c. 検索ボックスに、スキャナーを追加するスキャナーグループの名前を入力します。 d. 一致グループのドロップダウンリストでグループをクリックします。 e. (オプション) 手順 c と d を繰り返して他のスキャナーグループを追加します。

6. **[保存]** をクリックして変更を保存します。

   Tenable Vulnerability Managementによって、選択したグループに 1 つまたは複数のスキャナーが追加され、**[グループに追加する]** プレーンが閉じます。

スキャナーグループからセンサーを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Web App Scanning ユーザーロール: スキャンマネージャーまたは管理者

新規のインターフェースのスキャナーグループからセンサーを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. ドロップダウンボックスで、**[スキャナーグループ]** を選択します。

   使用または管理するためのアクセス許可を持つ既存のスキャナーグループのリストが表示されます。

5. (オプション) 変更するグループの表を検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

6. スキャナーグループの表で、変更するスキャナーグループをクリックします。

   [グループの詳細] ページが表示されます。このページには、グループに割り当てたセンサーをリストした表が含まれます。

7. (オプション) 削除するセンサーを検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

8. 削除する 1 つまたは複数のセンサーを選択します。

9. 削除するセンサーを選択します。

範囲	アクション

単一センサーの削除	a. センサー表で、次のいずれかを実行します。 • 削除するセンサーを右クリックします。 アクションオプションがカーソルの横に表示されます。 • **[アクション]** 列で、削除するセンサーの ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。 • 削除するセンサーのチェックボックスを選択します。 表の上部にアクションボタンが表示されます。 b. **[グループから削除する]** 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。
複数のセンサーを削除	a. センサーの表で、グループから削除する各センサーのチェックボックスを選択します。 ページの下部またはに、アクションバーが表示されます。 b. アクションバーで、**[グループから削除する]** 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。

10. 確認ウィンドウで、**[削除]** をクリックします。

Tenable Vulnerability Managementにより、1つまたは複数のセンサーがスキャナーグループから削除されます。

スキャナーグループのセンサーを管理する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

新しいインターフェースのスキャナーグループに割り当てられたセンサーを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. ドロップダウンボックスで、**[スキャナーグループ]** を選択します。

   使用または管理するためのアクセス許可を持つ既存のスキャナーグループのリストが表示されます。

5. (オプション) 表示するグループの表を検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

6. スキャナーグループの表で、表示するスキャナーグループをクリックします。

   [グループの詳細] ページが表示されます。このページには、グループに割り当てたセンサーを記載した表が含まれます。

センサーのすべての実行中のスキャンの表示

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

注意: Tenable Nessus スキャナーグループのセンサーについてのみ、すべてのスキャンを表示できます。

センサーのすべての実行中のスキャンを表示する方法

1. 適切なスキャナーグループのセンサーを表示します。
2. センサーの表で、すべてのスキャンを表示するセンサーをクリックします。

   スキャナーの **[詳細]** ページが表示されます。
3. **[スキャンの管理]** タブをクリックします。

   Tenable Vulnerability Management は、センサーが現在実行しているすべてのスキャンを一覧表示します。

OT コネクタ

所属組織に OT Security と Tenable Vulnerability Management がある場合、OT コネクタを設定して、OT Security が資産と検出結果のデータを Tenable Vulnerability Management に送信することを許可することができます。Tenable Vulnerability Management の **[センサー]** ページから OT コネクタを管理することができます。

Tenable Vulnerability Management で **[OT コネクタ]** メニューを開く方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. **[OT コネクタ]** タブをクリックします。

   リンクされた OT コネクタのリストが表示されます。

5. OT コネクタを管理するには、次の手順を使用します。

OT コネクタを追加する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

OT コネクタを追加する方法

1. ⊕ **[OT コネクタの追加]** をクリックします。

   [OT コネクタの追加] ウィンドウが表示されます。

2. **[生成]** をクリックします。

   Tenable Vulnerability Management は、OT コネクタをリンクする適切なクラウドサイトを表示し、OT リンクキーを生成します。

> **注意:** リンクキーを使用して *1* つの OT コネクタをリンクできます。リンクキーは生成後 2 時間以内に使用する必要があります。さらに OT コネクタをリンクするには、コネクタごとに新しいリンクキーを生成して使用します。

3. OT Security ユーザーインターフェースから、クラウドサイトとリンクキーを使用してコネクタを Tenable Vulnerability Management にリンクします。詳細については、*OT Security ユーザーガイド*を参照してください。

OT コネクタの名前またはタイプを変更する

> **必要な Tenable Vulnerability Management ユーザーロール:** スキャンマネージャーまたは管理者

お使いの OT コネクタが、認識可能になり、正しいタイプとして表示されるように、Tenable Vulnerability Management 内の OT コネクタの名前とタイプの変更が必要な場合があります。**ICP** と **EM** (Enterprise Manager) の 2 つのタイプから選択できます。タイプの詳細については、*OT Security ユーザーガイド*を参照してください。

> **注意:** Tenable Vulnerability Management で OT コネクタの名前やタイプを更新しても、OT Security では変更されません。

OT コネクタの名前またはタイプを変更する方法

1. **OT コネクタ**の表で、**[名前]** または **[タイプ]** セルをダブルクリックして編集します。
2. 新しい名前を入力するか、新しいタイプ (**ICP** または **EM**) を選択します。
3. セルの外側をクリックします。

   Tenable Vulnerability Management が変更を保存します。

OT コネクタを有効または無効にする

> **必要な Tenable Vulnerability Management ユーザーロール:** スキャンマネージャーまたは管理者

OT コネクタを一時的に無効にし、後で有効にしたい場合があるかもしれません。たとえば、OT Security が不要なネットワークから Tenable Vulnerability Management へのデータ送信を開始した場合、OT コネクタを無効にする必要があるかもしれません。問題が解決した後に、コネクタを再度有効にすることができます。

OT コネクタを有効または無効する方法

1. OT コネクタの表で、有効または無効にするコネクタの列の ⋮ 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。

2. 現在、コネクタが有効になっている場合は、 **[無効化]** をクリックします。現在、コネクタが無効になっている場合は、 **[有効化]** をクリックします。

   コネクタを有効にしている場合、Tenable Vulnerability Management によりコネクタ行のテキストが太字になり、**[有効]** 列が **[はい]** に更新されます。コネクタを無効にしている場合、Tenable Vulnerability Management によりコネクタ行のテキストがグレー表示になり、**[有効]** 列が **[いいえ]** に更新されます。

OT コネクタを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

OT コネクタから Tenable Vulnerability Management にデータを送信させない場合は、Tenable Vulnerability Management から OT コネクタを削除してください。たとえば、OT Security を再デプロイする必要がある場合、古いデプロイメントに関連付けられているコネクタを削除する必要があります。

Tenable では、Tenable Vulnerability Management から OT コネクタを削除するときは必ず OT Security で関連するコネクタも削除することを推奨しています。これにより、Tenable Vulnerability Management と OT Security の整合性が保たれます。

注意: OT コネクタの削除を取り消すことはできません。OT コネクタを再リンクする場合は、OT コネクタの追加プロセスを繰り返す必要があります。

OT コネクタを Tenable Vulnerability Management から削除する方法

1. OT コネクタの表で、削除するコネクタの列の ⋮ 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。

2. **[削除]** をクリックします。

   [OT コネクタの削除] ウィンドウが表示されます。

3. **[削除]** をクリックします。

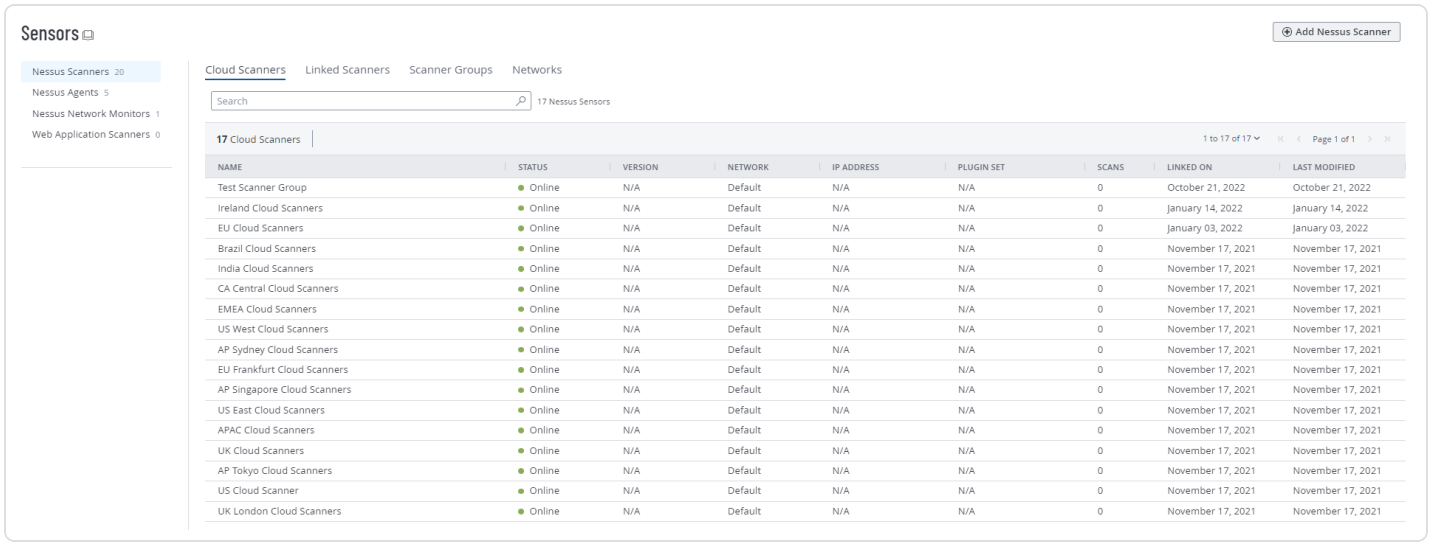
   Tenable Vulnerability Management により、表からコネクタが削除されます。

クラウドセンサー

デフォルトで、Tenable は Tenable Vulnerability Management で使用する地域のクラウドセンサーを提供しています。スキャンを作成して起動するときに、これらのセンサーを選択できます。

次の表は、各地域のクラウドセンサーとその IP アドレス範囲 (許可リスト登録用) を示しています。これらの IP アドレス範囲は Tenable専用です。

Tenable Vulnerability Management



注意: クラウドコネクタを使用する場合、Tenable はサイトが拠点を置く地域の IP アドレスを許可リストに登録することをお勧めします。

注意: これらの IP アドレスは送信リクエスト用ですが、着信 cloud.tenable.com リクエストにも使用されます。

ヒント: データをプログラムで解析するユーザーのために、下の表のクラウドセンサーと IP アドレスの情報は JSON 形式でも提供されます。

Tenable Attack Surface Management に関連付けられたクラウド IP については、*Tenable Attack Surface Management ユーザーガイド*の Cloud Sensors を参照してください。

センサー地域	IPv4 範囲	IPv6 範囲
ap-northeast-1	13.115.104.128/25 35.73.219.128/25	2406:da14:e76:5b00::/56
ap-southeast-1	13.213.79.0/24	2406:da18:844:7100::/56

センサー地域	IPv4 範囲	IPv6 範囲
	18.139.204.0/25 54.255.254.0/26	
ap-southeast-2	13.210.1.64/26 3.106.118.128/25 3.26.100.0/24	2406:da1c:20f:2f00::/56
ap-south-1	3.108.37.0/24	2406:da1a:5b2:8500::/56
ca-central-1	3.98.92.0/25 35.182.14.64/26	2600:1f11:622:3000::/56
eu-west-1	3.251.224.0/24	2a05:d018:f53:4100::/56
eu-west-2	18.168.180.128/25 18.168.224.128/25 3.9.159.128/25 35.177.219.0/26	2a05:d01c:da5:e800::/56
eu-central-1	18.194.95.64/26 3.124.123.128/25 3.67.7.128/25 54.93.254.128/26	2a05:d014:532:b00::/56
me-central-1	51.112.93.0/24	2406:da17:524:dd00::/56
us-east-1	34.201.223.128/25 44.192.244.0/24 54.175.125.192/26	2600:1f18:614c:8000::/56
us-east-2	13.59.252.0/25 18.116.198.0/24 3.132.217.0/25	2600:1f16:8ca:e900::/56
us-west-1	13.56.21.128/25 3.101.175.0/25 54.219.188.128/26	2600:1f1c:13e:9e00::/56

センサー地域	IPv4 範囲	IPv6 範囲
us-west-2	34.223.64.0/25 35.82.51.128/25 35.86.126.0/24 44.242.181.128/25 35.93.174.0/24	2600:1f14:141:7b00::/56
sa-east-1	15.228.125.0/24	2600:1f1e:9a:ba00::/56
静的	162.159.129.83/32 162.159.130.83/32	2606:4700:7::a29f:8153 2606:4700:7::a29f:8253

ヒント: 内部スキャナーまたはエージェント通信には、以下を追加します。

- 162.159.129.83/32
- 162.159.130.83/32
- 162.159.140.26/32
- 172.66.0.26/32
- 2606:4700:7::1a
- 2a06:98c1:58::1a
- 2606:4700:7::a29f:8153
- 2606:4700:7::a29f:8253
- ワイルドカード文字 (*) 付きの *.cloud.tenable.com として、cloud.tenable.com およびすべてのサブドメイン (sensor.cloud.tenable.com など) を許可してください。

注意: Tenable サポートによる Tenable Web App Scanning に関する問題のトラブルシューティングを行う場合、次の IP 範囲を許可リストに追加するよう求められる場合があります。

- 13.59.250.76/32

地域のクラウドセンサーが以下のグループに分かれて表示されます。

- **US East Cloud Scanners**: us-east-1 (バージニア州) または us-east-2 (オハイオ州) 範囲のスキャナーグループ

- **US West Cloud Scanners**: us-west-1 (カリフォルニア州) または us-west-2 (オレゴン州) 範囲のスキャナーグループ
- **AP Singapore Cloud Scanners**: ap-southeast-1 (シンガポール) 範囲のスキャナーグループ
- **AP Sydney Cloud Scanners**: ap-southeast-2 (シドニー) 範囲のスキャナーグループ
- **AP Tokyo Cloud Scanners**: ap-northeast-1 (東京) 範囲のスキャナーグループ
- **CA Central Cloud Scanners**: ca-central-1 (カナダ) 範囲のスキャナーグループ
- **EU Frankfurt Cloud Scanners**: eu-central-1 (フランクフルト) 範囲のスキャナーグループ
- **UK Cloud Scanners**: eu-west-2 (ロンドン) 範囲のスキャナーグループ
- **Brazil Cloud Scanners**: sa-east-1 (サンパウロ) 範囲のスキャナーグループ
- **India Cloud Scanners**: ap-south-1 (ムンバイ) 範囲のスキャナーグループ
- **Amazon GOV-CLOUD**: Federal Risk and Authorization Management Program (FedRAMP) 環境で利用可能なスキャナーグループ
- **US Cloud Scanner**: 次の AWS 範囲のスキャナーグループ
    - us-east-1 (バージニア州)
    - us-east-2 (オハイオ州)
    - us-west-1 (カリフォルニア州)
    - us-west-2 (オレゴン州)
- **APAC Cloud Scanners**: 次の AWS 範囲のスキャナーグループ
    - ap-northeast-1 (東京)
    - ap-southeast-1 (シンガポール)
    - ap-southeast-2 (シドニー)
    - ap-south-1 (ムンバイ)
- **EMEA Cloud Scanners**: 次の AWS 範囲のスキャナーグループ

- eu-west-1 (アイルランド)
- eu-west-2 (ロンドン)
- eu-central-1 (フランクフルト)

注意: 中国本土にある Tenable Nessus スキャナー、Tenable Nessus Agents、Tenable Web App Scanning スキャナー、または Tenable Nessus 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。

センサーのセキュリティ

Tenable Vulnerability Management プラットフォームを使用する際のセンサーのセキュリティと暗号化の詳細については、以下のセクションを参照してください。

- センサーの概要
- リンクキー
- データの暗号化

センサーの概要

センサーは、次のサイトから Tenable Vulnerability Management にアクセスします: `<port> - sensor.cloud.tenable.com:443`。すべてのセンサー(Tenable Nessus スキャナー、Tenable Nessus Agents、Tenable Nessus Network Monitor)には `cloud.tenable.com:443` へのアクセス権が必要です。

> **注意:** 中国本土にある Tenable Nessus スキャナー、Tenable Nessus Agents、Tenable Web App Scanning スキャナー、または Tenable Nessus 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。

Tenable Nessus スキャナーと Tenable Nessus Network Monitor をどのようにデプロイしてい設定するかに応じて、それぞれのユーザーインターフェースにアクセスし初期設定する必要があります。

- Tenable Nessus — `<IP>:8834`
- Tenable Nessus Network Monitor — `<IP>:8835`

  > **注意:** Tenable Core で Tenable Nessus または Tenable Nessus Network Monitor をデプロイする場合は、基盤となる仮想アプライアンスインターフェース(`<IP>:8000`)へのアクセス権も必要です。

Tenable Vulnerability Management は、Tenable のお客様向けの API により動作するユーザーインターフェースをすべての操作に使用します。Tenable Vulnerability Management に接続するセンサーは、脆弱性と資産情報を収集して、セキュリティにおいて重要な役割を果たします。このデータを保護し、通信パスの安全性を確保することは、Tenable Vulnerability Management のコア機能です。

Nessus センサーは、Tenable Vulnerability Management に対して安全に認証され、リンクした後に、Tenable Vulnerability Management プラットフォームに接続します(詳細については、次のセクションのリンクキーを参照)。リンクが完了すると、Tenable Vulnerability Management はすべての更新を管理して、センサーを常に最新の状態に保ちます。

センサーは常にセンサーと Tenable Vulnerability Management の間のトラフィックを開始します。トラフィックはポート 443 を介したアウトバウンド専用です。トラフィックは、TLS 1.2+ (NIAP モードの場合はバージョン 1.2) と 4096 ビットキーを使用し、SSL 通信によって暗号化されます。これにより、ファイヤーウォールを変更する必要がなくなり、ファイヤーウォールルールを介して接続を制御できるようになります。

注意: NIAP モードの詳細については、各製品のユーザーガイドで以下のトピックを参照してください。

- NIAP に準拠する Tenable Nessus の設定
- NIAP に準拠する Tenable Nessus Agent の設定
- NIAP に準拠する Tenable Nessus Network Monitor の設定

リンクキー

Tenable Vulnerability Management は、センサーの初期認証トークンとしてリンクキーを使用します。リンクキーを使用すると、センサー (Nessus スキャナー、Nessus Agent、または Tenable Nessus Network Monitor) と Tenable Vulnerability Management の間に初期リンクを作成できます。

Tenable Vulnerability Management プラットフォームはセンサーからリンクリクエストを受信すると、有効なリンクキーで提示されたリンクキーを検証します。Tenable Vulnerability Management は、リンクキーが有効なリンクキーと一致した場合は、センサーのリンクを許可します。

リンク時に、Tenable Vulnerability Management は 256 ビット長のキーをランダムに生成して、保存し、センサーに送信します。このキーはセンサーに対して一意です。

リンクプロセスが完了すると、センサーではリンクキーが不要になり、使用されません。それ以降の認証は、以下の方法で行われます。

- **センサーからプラットフォームへの認証**

  最初のリンクプロセス以降は、センサーは 256 ビットのキーを提供して、リクエストを識別し、認証します。これらのリクエストには、ジョブ、スキャンポリシー、プラグインの更新、スキャナーバイナリの更新のリクエストや、スキャン結果やセンサーの正常性データといった情報の Tenable Vulnerability Management への提供が含まれますが、これらに限定されません。

- **センサーからプラットフォームへのジョブ通信**

  センサーは Tenable Vulnerability Management に頻繁にチェックインします (センサーのタイプによってチェックイン頻度が異なります)。スキャンジョブが起動されると、Tenable Vulnerability Management はポリシーを生成し、ランダムに生成された 128 ビットキーでポリシーを暗号化します。センサーは、プラットフォームからポリシーをリクエストします。ポリシーはディスクに保存されますが、

キーはメモリ内にのみ存在します。コントローラーはキーを使用して、スキャン認証情報を含むポリシーを暗号化します。

データの暗号化

Tenable Vulnerability Management は AES-256 以上を使用して、少なくとも 1 つのレベルですべての状態のすべてのデータを暗号化します。

- **保存データ** - Tenable Vulnerability Management は、少なくとも 1 つのレベルの AES-256 暗号化を使用して、暗号化メディアにデータを保存します。一部のデータクラスには、第 2 レベルのファイルごとの暗号化が含まれています。
- **転送中データ** - Tenable Vulnerability Management は TLS バージョン 1.2+ と 4096 ビットキーを使用して、転送中 (内部転送を含む) のデータを暗号化します。
- **バックアップまたは複製されたデータ** - Tenable Vulnerability Management は、ソースと同じレベル (AES-256 以上) の暗号化を使用して、ボリュームスナップショットとデータレプリカを保存します。すべての複製は AWS 内で行われます。Tenable は、物理的なオフサイトのメディアおよび物理システムにはデータをバックアップしません。
- **インデックスデータ** - Tenable Vulnerability Management は、少なくとも 1 つのレベルの AES-256 暗号化を使用して、暗号化メディアにインデックスデータを保存します。

Tenable は、保存されているすべての暗号化データを新しいキーにローテーションできます。新しいサイトに切り替えて新しいキーを使用することもできます (つまり、Tenable は新しいサイトをプロビジョニングするときにキーを再利用しません)。Tenable は、AWS Key Management Service を使用してキーを管理します。

センサーのリンク

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

必要な Tenable Web App Scanning ユーザーロール: スキャンマネージャーまたは管理者

この手順では、Tenable Vulnerability Management にセンサーをリンクする方法を説明します。

センサーを削除しない限り、Tenable Vulnerability Management にセンサーをリンクさせるのはセンサーを管理する上で 1 度限りとなります。センサーをリンクした後、センサーは一意の認証情報を使用して Tenable Vulnerability Managementに接続します。

Tenable Vulnerability Management でリンクキーをコピーしたら、そのリンクキーをセンサーユーザーインターフェースの適切な場所 (たとえば、Tenable Nessus Agent CLI、または Tenable Nessus Network Monitor の **[クラウド設定]** セクション) にペーストする必要があります。具体的な詳細は、次のセクションを展開してください。

注意: ファイヤーウォールでドメイン許可リストを使用している場合、Tenable は、その許可リストに *.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。中国本土にある Tenable Nessus スキャナー、Tenable Nessus Agents、Tenable Web App Scanning スキャナー、または Tenable Nessus 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。

注意: 特定の状況では、リンクキーの再生成が必要になる場合があります。詳細は、リンクキーを再生成するを参照してください。センサーのセキュリティとリンクキーの詳細については、センサーのセキュリティを参照してください。

センサーをリンクする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

[センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 続けて、次のようにします。

   Tenable Nessus Agent センサーをリンクするには、**[Nessus Agent]** タブをクリックします。

   a. ⊕ **[エージェントを追加する]** をクリックします。

      [エージェントを追加する] プレーンが表示されます。

   b. 次のいずれかを行います。

      - Tenable Nessus Agent を手動でインストールしリンクする方法

        a. **[リンクキー]** セクションで **[コピー]** をクリックします。

           [リンクキーをクリップボードにコピー] のメッセージが表示され、リンクキーがクリップボードにコピーされます。

        b. Tenable Vulnerability Management にリンクさせる Tenable Nessus Agentインスタンスにアクセスします。

        c. コピーしたリンクキーを Tenable Nessus Agent CLI で使用し、センサーをリンクします。詳細については、*Tenable Nessus Agent デプロイメントとユーザーガイド* のインストール Tenable Nessus Agentを参照してください。

      - (Windows のみ) 1 つのコマンドで Tenable Nessus Agent をインストールしリンクする方法

        a. **[Windows プラットフォームへのエージェントのインストール]** ヘッダーにあるコマンドをコピーします。

           このコマンドには、エージェントをインストールして Tenable Vulnerability Management にリンクさせ、エージェント名を変更し、エージェントグループに追加するために必要なリンクキーと構文が含まれています。例:

           ```
           Invoke-WebRequest -Uri “https://cloud.tenable.com/install/
           {sensorType}/installer/ms-install-script.ps1” -OutFile “./ms-
           installscript.
           ```

```
ps1"; & “./ms-install-script.ps1” -key “{linkingKey}” -type
“{sensorType}” -name “<agent name> ” -groups “<list of groups> “;
Remove-Item -Path “./ms-install-script.ps1”
```

b. コマンドの *<agent name>* 部分を実際のエージェント名に置き換えます。

ヒント: エージェント名をカスタマイズしない場合は、`-name "<agent name>"` を削除します。名前をカスタマイズしない場合、エージェントがインストールされているマシンのホスト名を使用して、Tenable によりエージェントに名前が付けられます。

c. コマンドの `<list of groups>` 部分を実際のエージェントグループ名に置き換えます。

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"`)。

ヒント: エージェントをエージェントグループに追加しない場合は、`-groups "<list of groups>"` を削除します。

d. 管理者権限を持つユーザーとして、エージェントをインストールしたい Windows マシンの CLI にアクセスします。

e. コマンドを実行します。

Tenable Nessus Agent が Windows マシンにインストールされ、Tenable Vulnerability Management のインスタンスにリンクされます。また必要に応じて、エージェント名とエージェントグループが更新されます。

- (Linux のみ) 1 つのコマンドで Tenable Nessus Agent をインストールしリンクする方法

a. **[Linux プラットフォームへのエージェントのインストール]** ヘッダーで、コマンドをコピーします。

このコマンドには、エージェントをインストールして Tenable Vulnerability Management にリンクさせ、エージェント名を変更し、エージェントグループに追加するために必要なリンクキーと構文が含まれています。例

```
curl -H 'X-Key:
abcd1234efgh5678ijkl9012mnop3456qrst7890uvwx1234yz5678abcd1234ef'
'https://cloud.tenable.com/install/agent?name=agent-
name&groups=agent-group' | bash
```

b. コマンドの *agent-name* 部分をエージェント名に置き換えます。

ヒント: エージェント名をカスタマイズしない場合は、name=agent-name を削除します。名前をカスタマイズしない場合、エージェントがインストールされているマシンのホスト名を使用して、Tenable によりエージェントに名前が付けられます。

c. コマンドの *agent-group* 部分をエージェントグループ名に置き換えます。

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"`)。

ヒント: エージェントをエージェントグループに追加しない場合は、`groups=agent-group` を削除します。

d. 管理者権限を持つユーザーとして、エージェントをインストールしたい Linux マシンの CLI にアクセスします。

e. コマンドを実行します。

Tenable Nessus Agent が Linux マシンにインストールされ、Tenable Vulnerability Management のインスタンスにリンクされます。また必要に応じて、エージェント名とエージェントグループが更新されます。

Tenable Nessus Network Monitor インスタンスをリンクするには、**[Nessus Network Monitor]** タブをクリックします。

a. ⊕ **[Nessus Network Monitor を追加する]** をクリックします。

[Nessus Network Monitor を追加する] プレーンが表示されます。

b. **[リンクキー]** セクションで **[コピー]** をクリックします。

[リンクキーをクリップボードにコピー] のメッセージが表示され、リンクキーがクリップボードにコピーされます。

c. Tenable Vulnerability Management にリンクさせる Tenable Nessus Network Monitorインスタンスにアクセスします。

d. コピーしたリンクキーを Tenable Nessus Network Monitor ユーザーインターフェースで使用し、センサーをリンクします。詳細は、NNM ユーザーガイドを参照してください。

Tenable Nessus センサーをリンクするには、**[Nessus スキャナー]** タブをクリックします。

a. ⊕ **[Nessus スキャナーの追加]** をクリックします。

[Nessus の追加] プレーンが表示されます。

b. 次のいずれかを行います。

- Tenable Nessus を手動でインストールしリンクする方法

  a. **[リンクキー]** セクションで **[コピー]** をクリックします。

  [リンクキーをクリップボードにコピー] のメッセージが表示され、リンクキーがクリップボードにコピーされます。

  b. Tenable Vulnerability Management にリンクさせる Tenable Nessusインスタンスにアクセスします。

  c. コピーしたリンクキーを Tenable Nessus ユーザーインターフェースで使用し、センサーをリンクします。詳細は、*Tenable Nessus ユーザーガイド*の Link to Tenable Vulnerability Management を参照してください。

- (Windows のみ) 1 つのコマンドで Tenable Nessus スキャナーをインストールしリンクするには:

a. **[ワンラインインストール]** のインストラクションにあるコマンドをコピーします。

コマンドには、スキャナーをインストールして Tenable Vulnerability Management にリンクし、スキャナー名を変更し、スキャナーグループに追加するために必要な、リンクキーと構文が含まれます。例:

```
Invoke-WebRequest -Uri
"https://cloud.tenable.com/install/scanner/installer/ms-install-
script.ps1" -OutFile "./ms-install-script.ps1"; & "./ms-install-
script.ps1" -key
"51cc161bfa7c62dd7fc90a63561a256306cda982e3edba9d7ebadc05f6a2118c"
-type "scanner" -name "<scanner name>" -groups "<list of groups>";
Remove-Item -Path "./ms-install-script.ps1"
```

b. コマンドの `<scanner-name>` 部分を実際のスキャナー名に置き換えます。

> **ヒント:** スキャナー名をカスタマイズしない場合は、`-name "<scanner-name>"` を削除します。名前をカスタマイズしない場合、スキャナーがインストールされているマシンのホスト名を使用して、Tenable によりスキャナーに名前が付けられます。

c. コマンドの `<list of groups>` 部分を実際のスキャナーグループ名に置き換えます。

> **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。

> **ヒント:** スキャナーをスキャナーグループに追加しない場合は、`-groups "<list of groups>"` を削除してください。

d. 管理者権限を持つユーザーとして、スキャナーをインストールしたい Windows マシンの CLI にアクセスします。

e. コマンドを実行します。

Tenable Nessus が Windows マシンにインストールされ、Tenable Vulnerability Management のインスタンスにリンクされます。また必要に応じて、スキャナー名とスキャナーグループが更新されます。

- (Linux のみ) 1 つのコマンドで Tenable Nessus スキャナーをインストールおよびリンクする方法

  a. **[ワンラインインストール]** のインストラクションにあるコマンドをコピーします。

  コマンドには、スキャナーをインストールして Tenable Vulnerability Management にリンクし、スキャナー名を変更し、スキャナーグループに追加するために必要な、リンクキーと構文が含まれます。例

  ```
  curl -H 'X-Key:
  abcd1234efgh5678ijkl9012mnop3456qrst7890uvwx1234yz5678abcd1234ef'
  'https://cloud.tenable.com/install/scanner?name=scanner-
  name&groups=scanner-group'| bash
  ```

  b. コマンドの *scanner-name* 部分をスキャナー名に置き換えます。

  ヒント: スキャナー名をカスタマイズしない場合は、name=scanner-name を削除します。名前をカスタマイズしない場合、スキャナーがインストールされているマシンのホスト名を使用して、Tenable によりスキャナーに名前が付けられます。

  c. コマンドの *scanner-group* 部分をスキャナーグループ名に置き換えます。

  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。

  ヒント: スキャナーをスキャナーグループに追加しない場合は、groups=scanner-group を削除してください。

  d. 管理者権限を持つユーザーとして、スキャナーをインストールする Linux マシンの CLI にアクセスします。

  e. コマンドを実行します。

Tenable Nessus が Linux マシンにインストールされ、Tenable Vulnerability Management のインスタンスにリンクされます。また必要に応じて、スキャナー名とスキャナーグループが更新されます。

Tenable Core + Tenable Web App Scanning インスタンスをリンクするには、左側のナビゲーションメニューで **[Web App Scanners]** をクリックします。

a. ⊕ **[ウェブアプリケーションスキャナーの追加]** をクリックします。

[ウェブアプリケーションスキャナーの追加] プレーンが表示されます。

b. **[リンクキー]** セクションで **[コピー]** をクリックします。

[リンクキーをクリップボードにコピー] のメッセージが表示され、リンクキーがクリップボードにコピーされます。

c. Tenable Vulnerability Management にリンクさせる Tenable Core + Tenable Web App Scanning インスタンスにアクセスします。

d. コピーしたリンクキーを Tenable Core + Tenable Web App Scanning ユーザーインターフェースで使用し、センサーをリンクします。詳細については、Tenable Core + Tenable Web App Scanning ユーザーガイドを参照してください。

次の手順

- Tenable Vulnerability Management でセンサーを管理します。(センサーのリンクの無効化または再有効化を含む。)
- Tenable Vulnerability Management スキャンの設定時にセンサーを選択します。

リンクキーを再生成する

必要なユーザーロール: 管理者

特定の状況では、Tenable Vulnerability Management インスタンスのリンクキーの再生成が必要になる場合があります。たとえば、リンクキーに関する知識を持つ従業員が退社した場合は、セキュリティ上の理由でリンクキーの再生成が必要になることがあります。

リンクキーは最初のリンクを確立するためだけに使用されるため、リンクキーの再生成は現在 Tenable Vulnerability Managementにリンクされているセンサーに影響しません。センサーをリンクした後、センサーは一意の認証情報を使用して Tenable Vulnerability Managementに接続します。

企業がリンクキーを実装スクリプトにハードコードしている場合は、次の点に注意してください。

- スクリプトエラーを防ぐため、必ず元のキーを再生成したキーに置き換えてください。
- 各 Tenable Vulnerability Management インスタンスは、すべてのタイプのセンサーに対して 1 つのリンクキーを使用します。あるタイプのセンサー (Tenable Nessus スキャナーなど) を使用しているときにリンクキーを再生成すると、それは他のセンサータイプにも対応するリンクキーとなります。リンクキーを再生成したら、必ずすべてのタイプのセンサーに関連するスクリプトの実装を更新してください。

注意: Tenable Vulnerability Management リンクキーの詳細については、センサーのセキュリティを参照してください。

Tenable Vulnerability Management インスタンスのリンクキーを再生成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 任意のセンサータイプタブ (**NNM** など) をクリックします。

   該当するセンサーページが表示されます。

5. ⊕ **[[センサータイプ] を追加する]** ボタン (**[NNM を追加する]** など) をクリックします。

   該当するセンサープレーンが表示されます。(**[NNM を追加する]** など)

6. **[[センサータイプ] を追加する]** プレーンで、**[再生成]** 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。

7. 確認ウィンドウで、**[再生成]** をクリックします。

   リンクキーが再生成されると [**Regenerated Linking Key**] というメッセージが表示され、[**Add [センサータイプ]**] プレーンで元のリンクキーが新しいリンクキーに置き換えられます。

次の手順

- センサーをリンクする。

センサーおよびセンサーグループの表示

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

[センサー] ページでは、リンクされたセンサー(Tenable Vulnerability Management クラウドセンサー、Tenable Nessus スキャナー、Tenable Nessus Agents、Tenable Nessus Network Monitor、Tenable Web App Scanning スキャナー)を確認できます。またスキャナーグループとエージェントグループを表示することもできます。

センサーおよびセンサーグループを表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

   左側のナビゲーションペインを使用して、表示するセンサーを選択します。

   - **Nessus スキャナー** - クラウドスキャナー、リンクされたスキャナー、スキャナーグループ
   - **Nessus Agent** - リンクされたエージェント、エージェントグループ
   - **Nessus Network Monitor**
   - **ウェブアプリケーションスキャナー** - リンクされた Tenable Web App Scanning スキャナー、Tenable Web App Scanning スキャナーグループ

   各センサーページにはリンクされているセンサーまたはグループのリストが表示され、次の表に示す基本情報も表示されます。表示しているセンサーによっては、説明されている列がすべて表示されない場合もあります。

列	説明
名前	センサーの名前。
作成日	センサーグループが作成された日付。
IP アドレス	センサーの IP アドレス。
最終変更日	センサーが変更された直近の日付。
リンク日	センサーが Tenable Vulnerability Management にリンクされた日付。
ネットワーク	センサーまたはセンサーグループに関連付けられたネットワーク。
プラットフォーム	センサーに関連付けられたプラットフォーム。
プラグインセット	センサーのプラグインセット。
スキャン数	センサーまたはセンサーグループが現在実行しているスキャンの数。
スキャナー数	グループ内のスキャナーの数。
ステータス	センサーのステータス(オンラインまたはオフライン)。
更新日	センサーグループが最後に更新された日付。
バージョン	センサーのバージョン。
アクション	各センサーに対して実行できるアクション。

センサーの詳細の表示

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

クラウドセンサーとリンクされたセンサーの両方の詳細を表示できます。

センサーの詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 表示するセンサータイプのタブをクリックします。

   センサーの表が表示されます。

5. **[Nessus スキャナー]** の場合は、次のいずれかを行います。

   - ドロップダウンボックスで、**[クラウドスキャナー]** タブを選択して、Tenable Vulnerability Management に接続されたクラウドスキャナーを表示します。詳細は、クラウドセンサー を参照してください。
   - ドロップダウンボックスで、**[リンクされたスキャナー]** タブをクリックして、Tenable Vulnerability Management にリンクされたオンプレミススキャナーを表示します。詳細は、リンクされたスキャナーを参照してください。

6. センサーの表で、詳細を表示するセンサーをクリックします。

   [詳細] ページが表示されます。

   センサーの種類に応じて、**[詳細]** ページで次の操作を実行できます。

   - **[設定]** タブをクリックして、センサー設定を変更します。
   - **[アクセス許可]** タブをクリックして、センサーのアクセス許可を変更します。

センサー設定を編集する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

リンクされた以下の種類のセンサーに関する設定を編集できます。

- Tenable Nessus Network Monitor
- Tenable Nessus Amazon Web Service (AWS) 向け

新しいインターフェースでセンサー設定を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 適切なセンサータイプタブをクリックします。

   センサーの表が表示されます。

5. センサーが **[Nessus スキャナー]** の場合は、次のいずれかを行います。

   - ドロップダウンボックスで、**[クラウドスキャナー]** タブを選択して、Tenable Vulnerability Management に接続されたクラウドスキャナーを表示します。詳細は、クラウドセンサーを参照してください。
   - ドロップダウンボックスで、**[リンクされたスキャナー]** タブを選択して、Tenable Vulnerability Management に接続されたスキャナーを表示します。詳細は、リンクされたスキャナーを参照してください。

6. リンクされたセンサーの表で、設定を編集するセンサーをクリックします。

   センサーの詳細が表示されます。デフォルトでは、**[概要]** タブが有効です。

7. **[設定]** タブをクリックします。

センサー設定が表示されます。

8. センサー設定を編集します。

設定	センサータイプ	説明
レポート頻度	NNM	センサーから Tenable Vulnerability Managementに情報を報告する頻度を分単位で指定します。
ソフトウェア更新の種類	NNM (5.6.1 以降のみ)	Tenable Nessus Network Monitor によって自動的に更新するコンポーネントがある場合、それを指定します。 **[すべてのコンポーネント]** には、Web サーバー、HTML クライアント、プラグイン、エンジンが含まれます。
インスタンスの更新間隔 (分)	AWS	アクセス権のあるインスタンスに関する情報を、AWS センサーから Tenable Vulnerability Management に報告する頻度を分単位で指定します。

9. ページ右下の **[保存]** をクリックします。

センサーのアクセス許可を編集する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

センサー設定で、次の Tenable Vulnerability Management ユーザーアクセス許可レベルを設定できます。

- **アクセスなし** - ユーザーまたはグループはスキャン設定内のスキャナーを使用できず、スキャナー設定の編集もできません。
- **使用可** - ユーザーまたはグループはスキャン設定内のスキャナーを使用できますが、スキャナー設定を編集することはできません。
- **管理可** - ユーザーまたはグループはスキャン設定内のスキャナーの使用、およびスキャナー設定の編集ができます。

注意: クラウドスキャナーには、設定方法に関わらず、常に **[使用可]** アクセス許可が付与されます。

センサーのアクセス許可を変更する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 適切なセンサータイプタブをクリックします。

   センサーの表が表示されます。

5. センサーが **[Nessus スキャナー]** の場合は、**[リンクされたスキャナー]** タブをクリックして Tenable Vulnerability Management にリンクされたオンプレミススキャナーを表示します。詳細は、リンクされたスキャナーを参照してください。

6. リンクされたセンサーの表で、アクセス許可を設定するセンサーをクリックします。

[詳細] ページが表示されます。エージェントを除くすべてのセンサーで、**[概要]** タブがデフォルトでアクティブになっています。

7. **[アクセス許可]** タブをクリックします。

   注意: デフォルトでは、Tenable Vulnerability Management インスタンスのすべてのユーザーがスキャナーを使用できます。

8. 次のいずれかを行います。

   - ドロップダウンボックスから**デフォルト**ユーザーのアクセス許可レベルを選択する場合
   - 個別のユーザーまたはユーザーグループのアクセス許可を指定する場合

     a. **[ユーザーまたはユーザーグループを追加する]** テキストボックスに、ユーザーまたはユーザーグループの名前を入力します。

     入力すると、Tenable Vulnerability Management は既存のユーザーまたはユーザーグループとの一致を検索します。

     b. 検索結果で、ユーザーまたはユーザーグループを選択します。

     c. アクセス許可ドロップダウンで、追加したユーザーまたはユーザーグループのアクセス許可レベルを選択します。

9. ページ右下の **[保存]** をクリックします。

センサーを有効または無効にする

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

センサーを有効または無効にする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 適切なセンサータイプタブをクリックします。

   センサーの表が表示されます。

5. (オプション) センサーが **[Nessus スキャナー]** の場合は、ドロップダウンボックスの **[リンクされたスキャナー]** を選択して、Tenable Vulnerability Management にリンクされたオンプレミススキャナーを表示します。詳細は、リンクされたスキャナー を参照してください。

6. リンクされているセンサーの表で、次のいずれかを実行します。

   - 有効または無効にするセンサーを右クリックします。

     アクションオプションがカーソルの横に表示されます。

   - **[アクション]** 列で、有効または無効にする ⋮ ボタンをクリックします。

     アクションオプションが行に表示されます。

7. 次のいずれかを行います。

   - センサーを有効にするには、🔗 **[有効化]** ボタンをクリックします。
   - センサーを無効にするには、⛓ **[無効化]** ボタンをクリックします。

   Tenable Vulnerability Management はセンサーを有効または無効にします。

センサーを削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

注意: クラウドセンサーを削除することはできません。

センサーを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[センサー]** タイルをクリックします。

   [センサー] ページが表示されます。デフォルトでは、**[Nessus スキャナー]** タブがアクティブで、ドロップダウンボックスで **[リンクされたスキャナー]** が選択されています。

4. 適切なセンサータイプタブをクリックします。

   センサーの表が表示されます。

5. **[Nessus スキャナー]** の場合は、ドロップダウンボックスで **[リンクされたスキャナー]** を選択して、Tenable Vulnerability Management にリンクされたオンプレミススキャナーを表示します。詳細は、リンクされたスキャナー を参照してください。

6. リンクされたセンサーの表で、削除するセンサーに次のいずれかのロールオーバーを実行します。

範囲	アクション
センサーの削除	a. センサー表で、次のいずれかを実行します。 • 削除するセンサーを右クリックします。 アクションオプションがカーソルの横に表示されます。 • **[アクション]** 列で、削除するセンサーの ⋮ ボタンをクリックします。 アクションオプションが行に表示されます。

	• 削除するセンサーの横にあるチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. **[削除]** をクリックします。 確認ウィンドウが表示されます。
複数のセンサーを削除	a. センサー表で、削除するセンサーのチェックボックスを選択します。表の上部にアクションバーが表示されます。 b. **[削除]** をクリックします。 確認ウィンドウが表示されます。

7. **[削除]** をクリックして、削除を確定します。

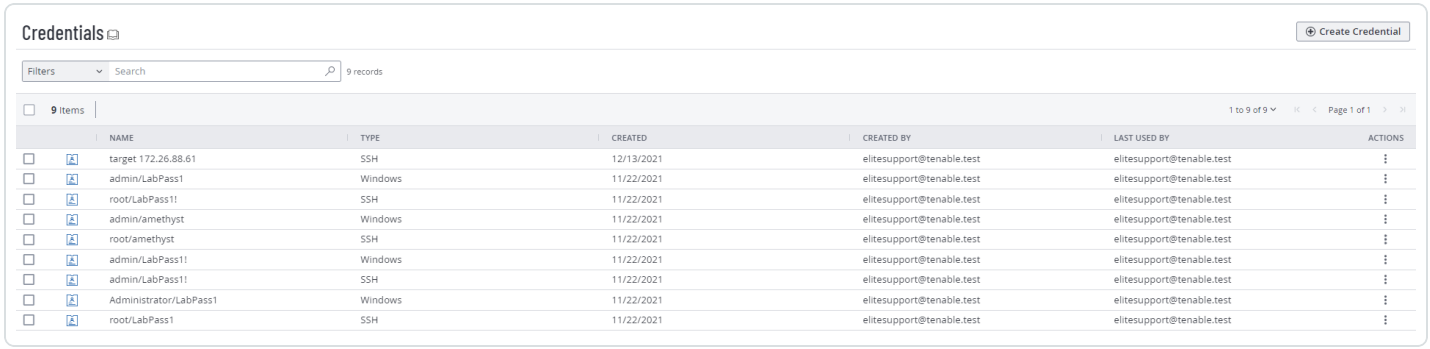
   Tenable Vulnerability Management により、そのセンサーがリストから削除されます。

認証情報

注意: このセクションでは、管理された認証情報を作成し維持する方法を説明します。スキャン固有またはポリシー固有の認証情報の詳細は、Tenable Vulnerability Management スキャンの認証情報 またはTenable Web App Scanning スキャンの認証情報を参照してください。

管理された認証情報によって、認証情報の設定を認証マネージャーで一元的に保存できます。その後、これらの認証情報設定を、スキャンごとに認証情報を設定する代わりに、複数のスキャン設定に追加できます。

アクセス許可が付与されたユーザーは、管理された認証情報をスキャンで使用できます。認証情報のユーザーアクセス許可によって、どのユーザーが管理された認証情報を使用し編集できるかが管理されます。



管理された認証情報の作成

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

このトピックでは、管理された認証情報を Tenable Vulnerability Management認証マネージャーで作成する方法を説明します。

スキャン固有の認証情報を管理された認証情報に変換するだけでなく、管理された認証情報をスキャン設定中に作成することもできます。詳細については、スキャン認証情報の追加または Tenable Web App Scanning で認証情報を設定するを参照してください。

管理された認証情報を作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

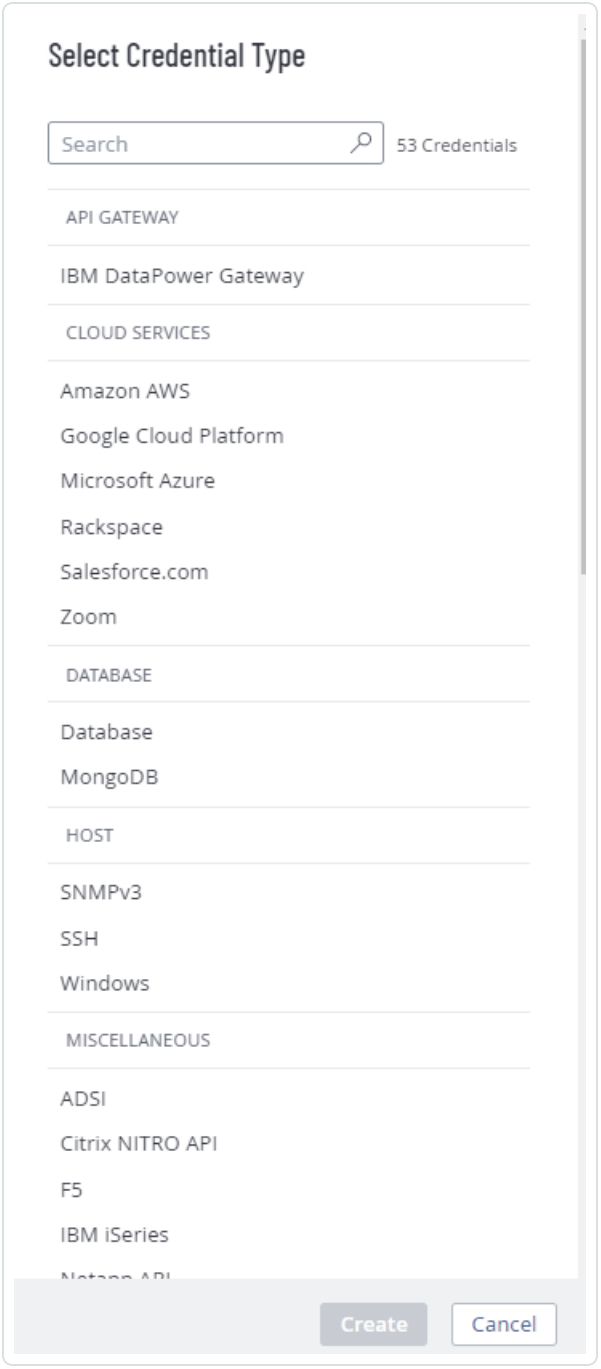
   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. ページの右上にある ⊕ **[認証情報の作成]** ボタンをクリックします。

   [認証情報タイプの選択] プレーンが表示されます。



5. 次のいずれかを行います。

   - 使用できる認証情報タイプのうちいずれかを選択します。
   - カテゴリセクションで認証情報タイプをクリックします。

   認証情報が表示されます。

6. **[タイトル]** ボックスに、認証情報の名前を入力します。

7. (オプション) **[説明]** ボックスに、認証情報の説明を入力します。
8. 選択した認証情報タイプを設定します。

   認証情報設定の詳細については、認証情報 (Tenable Vulnerability Management) または認証情報 (Tenable Web App Scanning) を参照してください。
9. ユーザーアクセス許可を追加します。
10. **[保存]** をクリックします。

    Tenable Vulnerability Management は [**Credentials**] ページの認証情報の表に認証情報を追加します。

管理された認証情報を編集する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

このトピックでは、認証情報を Tenable Vulnerability Management認証マネージャーで編集する方法を説明します。

スキャン設定中に管理された認証情報を編集することもできます。詳細については、Tenable Vulnerability Management の場合は認証情報をスキャンに追加する、Tenable Web App Scanning の場合は Tenable Web App Scanning スキャンで認証情報を設定するを参照してください。

編集可 アクセス許可を持つ認証情報を編集できます。

管理された認証情報を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. 編集したい認証情報について、認証情報の表をフィルタリングまたは検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

5. 認証情報の表で、編集する認証情報の名前をクリックします。

   [認証情報設定] プレーンが表示されます。

6. 次のいずれかを行います。

   - 認証情報の名前または説明を編集します。

     a. 名前または説明ボックスの上にカーソルを合わせます。

     b. ボックスの横に表示される ✎ ボタンをクリックします。

     c. 変更を行います。

     d. ボックスの右下にある ✓ ボタンをクリックして、変更内容を保存します。

   - 認証情報タイプの設定を編集します。これらの設定の詳細については、認証情報 (Tenable Vulnerability Management) または認証情報 (Tenable Web App Scanning) を参照してください。

   - 認証情報のユーザーアクセス許可を設定します。

7. **[保存]** をクリックします。

管理された認証情報のユーザーアクセス許可を設定する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

認証情報を使用するスキャンのために設定するアクセス許可とは別に、管理された認証情報のユーザーアクセス許可を設定します。

個別のユーザーまたはユーザーグループに対して認証情報のアクセス許可を設定できます。グループに対して認証情報のアクセス許可を設定する場合、グループ内のすべてのユーザーに同じアクセス許可を割り当てます。認証情報を管理するユーザーのグループを作成することで、認証情報のマネージャーロールと同等のアクセス許可を作成することもできます。詳細は、ユーザーグループを参照してください。

管理された認証情報を作成する場合、Tenable Vulnerability Management は自動的に**[編集可]**アクセス許可を割り当てます。

管理された認証情報のユーザーアクセス許可を設定する方法

1. 管理された認証情報を作成または編集します。

場所	アクション
認証マネージャー内	作成または編集
スキャン設定内	作成または編集

2. 次のいずれかを行います。

- ユーザーまたはユーザーグループのアクセス許可を追加する

    a. [認証情報設定]プレーンで、**[ユーザーのアクセス許可]**タイトルの横にある ⊕ ボタンをクリックします。

    [ユーザーアクセス許可の追加]設定が表示されます。

b. 検索ボックスで、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。

c. 検索結果からユーザーまたはグループを選択します。

d. ユーザーまたはグループ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。

e. アクセス許可レベルを選択します。

- **使用可** - ユーザーは、管理された認証情報の表の認証情報の表示と、スキャンでの認証情報の使用が可能です。
- **編集可** - ユーザーは、認証情報設定の表示と編集、認証情報の削除、スキャンでの認証情報の使用が可能です。

f. **[追加]** をクリックします。

g. **[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編集する

a. [認証情報設定] プレーンの **[ユーザーのアクセス許可]** セクションで、ユーザーまたはグループ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。

- **使用可** - ユーザーは、管理された認証情報の表の認証情報の表示と、スキャンでの認証情報の使用が可能です。

- **編集可** - ユーザーは、認証情報設定の表示と編集、認証情報の削除、スキャンでの認証情報の使用が可能です。

c. **[保存]** をクリックします。

- ユーザーグループのアクセス許可を削除する

a. [認証情報設定] プレーンの **[ユーザーのアクセス許可]** セクションで、削除するユーザーまたはグループにカーソルを合わせます。

b. その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。

そのユーザーまたはグループは、**[ユーザーのアクセス許可]** リストから削除されます。

c. **[保存]** をクリックします。

認証情報のエクスポート

必要なユーザーロール: 管理者

[認証情報] ページでは、1 つ以上の管理されている認証情報データをエクスポートできます。

注意: 認証情報データをエクスポートしても、ユーザー名、パスワード、キーなどの認証の詳細はエクスポートに含まれません。

認証情報データをエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. エクスポートする認証情報を選択します。

エクスポート範囲	アクション
選択した認証情報	選択した認証情報をエクスポートする方法 a. 認証情報の表で、エクスポートする各認証情報のチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。

	注意: [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。 200 個以上の認証情報をエクスポートする場合は、リスト内のすべての認証情報を選択してから、[→ **[エクスポート]** をクリックします。
1 つの認証情報	1 つの認証情報をエクスポートする方法 a. 認証情報の表で、エクスポートする認証情報の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 認証情報の表の **[アクション]** 列で、エクスポートする認証情報の行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. [→ **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。
- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	認証情報のリストを含む CSV テキストファイル

	注意: .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。
JSON	ネストされた認証情報のリストを含む JSON ファイル 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。
    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。
11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。

- **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
- (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

  > **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポートプレーンを閉じた場合は、エクスポートページからエクスポートファイルにアクセスできます。

管理された認証情報を削除する

必要な Tenable Vulnerability Management ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、または管理者

必要な Tenable Web App Scanning ユーザーロール: 基本、スキャンオペレーター、標準、スキャンマネージャー、管理者のいずれか

編集可 アクセス許可を持つ認証情報を削除できます。

管理された認証情報を削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[認証情報]** タイルをクリックします。

   [認証情報] ページが表示されます。認証情報の表では、表示するアクセス許可がある管理された認証情報が一覧表示されます。

4. 削除したい認証情報について、認証情報の表をフィルタリングまたは検索します。詳細は、Tenable Vulnerability Management の表 を参照してください。

5. 表で、削除する認証情報にカーソルを合わせます。

   アクションボタンが行に表示されます。

6. 🗑 ボタンをクリックします。

   [Confirm Deletion] ウィンドウが表示されます。

7. 次のいずれかを行います。

   - スキャンで認証情報を使用しない場合は、**[削除]** をクリックします。
   - スキャンで認証情報を使用する場合には

a. **[スキャンの表示]** をクリックします。

[スキャン] プレーンが表示されます。

b. 認証情報を使用するスキャンをフィルタリングまたは検索します。

c. 次のいずれかを行います。

- **[キャンセル]** をクリックして、削除をキャンセルします。
- **[削除]** をクリックして、削除を確定します。

除外

除外を使用して、選択したスケジュールに基づいて特定のホストのスキャンを制限できます。

注意: 除外はエージェントスキャンには適用されません。

除外の詳細は、以下のトピックを参照してください。

除外を作成する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

注意: 除外はエージェントスキャンには適用されません。

除外を作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

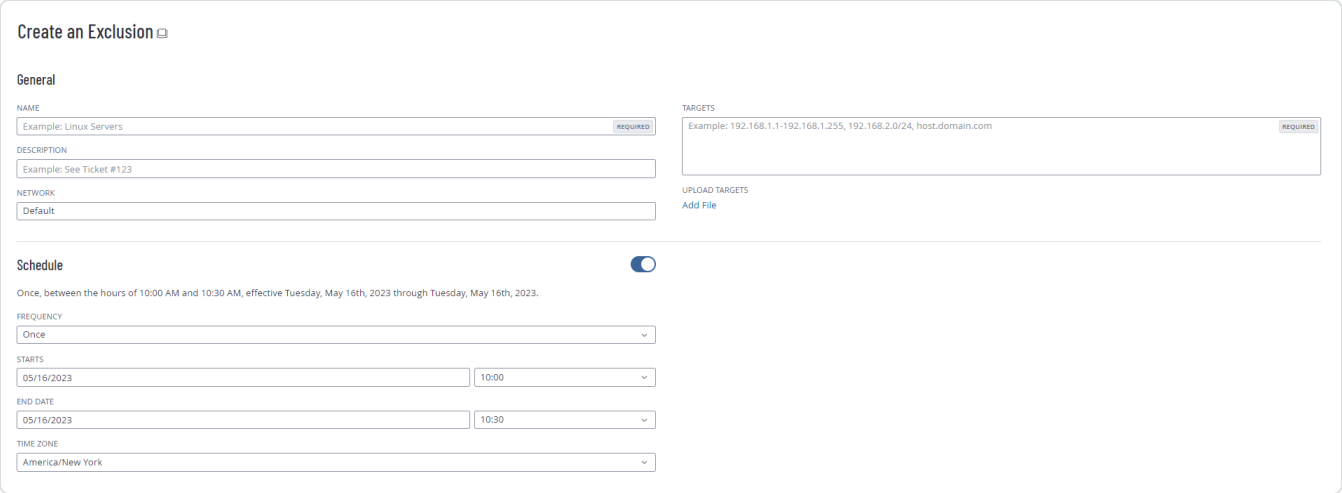
   [設定] ページが表示されます。

3. **[除外]** タイルをクリックします。

   [除外] ページが表示されます。

4. ページの右上にある ⊕ **[除外を作成]** ボタンをクリックします。

   [除外を作成] ページが表示されます。



5. 除外の設定を行います。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management で除外が保存され、選択されたスキャンターゲットに適用されます。

除外の編集

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

除外を編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[除外]** タイルをクリックします。

   [除外] ページが表示されます。

4. 除外の表で、編集する除外をクリックします。

   [除外を作成] ページが表示されます。

5. [除外の設定] を編集します。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management により除外が保存され、[**除外**] ページが表示されます。

除外をインポートする

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

除外を .csv ファイルによりインポートすることができます。

注意：除外をインポートすると、Tenable Vulnerability Management が自動的にそれをデフォルトのネットワークに割り当てます。インポート後、カスタムネットワークに除外を移動できます。

始める前に

- 指定された形式で .csv ファイルを作成します。

除外をインポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[除外]** タイルをクリックします。

   [除外] ページが表示されます。

4. ページの右上の **[インポート]** ボタンをクリックします。

   オペレーティングシステムのファイルマネージャーが表示されます。

5. インポートする .csv ファイルを選択します。

   Tenable Vulnerability Management によりファイルがインポートされ、除外が除外の表に追加されます。

除外インポートファイル

1 つまたは複数の除外を .csv ファイルとしてインポートできます。

注意: Tenable では .csv ファイルを Microsoft Excel で開くことは推奨していません。Excel で開くと、Tenable Vulnerability Management が識別できない文字がファイルに追加される場合があります。

このファイルは、ヘッダーと 1 つ以上のデータ行で設定されます。ファイルの各行は、改行で区切られている必要があります。

ヘッダー (オプション)

ファイルのヘッダー行はオプションです。ヘッダーを含める場合は、次のような形式でファイルの最初の行に配置する必要があります。

```
id,name,description,members,creation_date,last_modification_date
```

注意: コンマの後にスペースはありません。

データ (必須)

ファイルの各データ行は 1 つの除外設定を表します。データ行は、改行で相互に区切られている必要があります。ファイルには 1 つ以上のデータ行が含まれている必要があります。

各データ行は、次の表に示すフィールドのコンマ区切りの文字列です。

注意: オプションのフィールドは空白にできますが、関連付けられているコンマ区切り文字はデータ行に存在する必要があります。

フィールド	説明	必須
id	除外を一意に識別する整数。	×
名前	除外の名前。英数字またはシンボルの任意の組み合わせを使用できます。	○
説明	除外の説明。	○
メンバー	スキャンの除外を適用するターゲット。	○

	この値は次の形式で指定できます。 • ホスト名 (example.com) • IP アドレス (192.0.2.57) • IP 範囲 (192.0.2.57-192.0.2.67) • 引用符で囲まれた、複数のホスト名、IP アドレス、または IP 範囲のコンマ区切りのリスト ("192.0.2.57,192.0.2.177,192.0.2.8")	
creation_date	インポートされた除外の作成日として Tenable Vulnerability Management が使用する Unix タイムスタンプ。	×
last_modification_date	除外の最終変更日として Tenable Vulnerability Management が使用する Unix タイムスタンプ。	×

例

```
id,name,description,members,creation_date,last_modification_date
1,Exclusion Rule 1,routers,"192.0.2.57,192.0.21.177,192.0.28",1561643735,1561643785,Exclusion Rule
2,workstations,192.0.257-192.0.267,,
```

除外をエクスポートする

必要なユーザーロール: 管理者

[除外] ページで、1 つ以上のスキャン除外をエクスポートできます。

除外をエクスポートする方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[除外]** タイルをクリックします。

   [除外] ページが表示されます。このページには、Tenable Vulnerability Management アカウント上で設定された除外のリストが表示されます。

4. (オプション) 表データを選別します。詳細は、Tenable Vulnerability Management ワークベンチの表を参照してください。

5. エクスポートする除外を選択します。

エクスポート範囲	アクション
選択した除外	選択した除外をエクスポートする方法 a. 除外の表で、エクスポートする各除外のチェックボックスを選択します。 表の上部にアクションバーが表示されます。 b. アクションバーで、[→ **[エクスポート]** をクリックします。 **注意:** [→ **[エクスポート]** リンクで選択できるネットワークは最大 200 個です。200 個以上の除外をエクスポートする場合は、リスト内のすべての除外を選択してから、[→ **[エクスポート]** をクリックします。

1 つの除外	1 つの除外をエクスポートする方法 a. 除外の表で、エクスポートする除外の行を右クリックします。 アクションオプションがカーソルの横に表示されます。 -または- 除外の表の **[アクション]** 列で、エクスポートする除外の行にある ⋮ ボタンをクリックします。 アクションボタンが行に表示されます。 b. [→ **[エクスポート]** をクリックします。

[エクスポート] プレーンが表示されます。このプレーンには、次のものが含まれます。

- エクスポートファイル名を設定するテキストボックス
- 利用可能なエクスポート形式のリスト
- エクスポートされたファイルに含めるフィールドの設定オプションの表

  注意: デフォルトでは、すべてのフィールドが選択されています。

- エクスポートの有効期限が切れるまでの日数を設定するテキストボックス
- エクスポートスケジュールを設定するためのトグル
- メール通知を設定するためのトグル

6. **[名前]** ボックスに、エクスポートファイルの名前を入力します。
7. 使用するエクスポート形式をクリックします。

形式	説明
CSV	除外のリストを含む CSV テキストファイル。 **注意:** .csv エクスポートファイルに =、+、-、@ のいずれかの文字で始まるセルが含まれている場合、Tenable Vulnerability Management はセルの先頭に単一引用符 (') を自動的に入力します。詳細は、関連するナレッジベースの記事を参照してください。

JSON	ネストされた除外のリストを含む JSON ファイル。 空のフィールドは JSON ファイルに含まれません。

8. (オプション) エクスポートファイルに表示したくないフィールドがあれば、それらの選択を解除します。
9. **[有効期限]** ボックスに、エクスポートファイルの有効期限が切れるまでの日数を入力します。

   注意: Tenable Vulnerability Management では、エクスポート有効期限に最大 30 暦日を設定できます。

10. (オプション) 繰り返すエクスポートのスケジュールを設定する方法
    - **[スケジュール]** トグルをクリックします。

      [スケジュール] セクションが表示されます。
    - **[開始日時]** セクションで、エクスポートスケジュールを開始する日時を選択します。
    - **[タイムゾーン]** ドロップダウンボックスで、そのスケジュールで使用されるタイムゾーンを選択します。
    - **[繰り返し]** ドロップダウンボックスで、エクスポートを繰り返す頻度を選択します。
    - **[繰り返し終了]** ドロップダウンで、スケジュールが終了する日付を選択します。

      注意: [無し] を選択した場合は、エクスポートスケジュールを変更または削除するまで、スケジュールが繰り返されます。
11. (オプション) エクスポートの完了時にメール通知を送信する方法

    注意: エクスポートのスケジュールを設定する場合もしない場合も、メール通知を有効にできます。

    - **[メール通知]** トグルをクリックします。

      [メール通知] セクションが表示されます。
    - **[受信者の追加]** ボックスに、エクスポート通知を送信するメールアドレスを入力します。
    - (必須) **[パスワード]** ボックスに、エクスポートファイルのパスワードを入力します。受信者がファイルをダウンロードできるようにするには、このパスワードを受信者と共有する必要があります。

> **注意**: Tenable Vulnerability Management がリンク付きのメールを受信者に送信します。受信者は正しいパスワードをそのリンク先で入力することでファイルをダウンロードできます。

12. **[エクスポート]** をクリックします。

    Tenable Vulnerability Management がエクスポートの処理を開始します。エクスポートされるデータのサイズによっては、Tenable Vulnerability Management によるエクスポートの処理に数分かかる場合があります。

    処理が完了すると、Tenable Vulnerability Management はコンピューターにエクスポートファイルをダウンロードします。ブラウザーの設定によっては、ダウンロードの完了が通知される場合があります。

13. ブラウザのダウンロードディレクトリを介して、エクスポートファイルにアクセスします。ダウンロードが完了する前にエクスポートプレーンを閉じた場合は、エクスポートページからエクスポートファイルにアクセスできます。

除外を削除する

必要な Tenable Vulnerability Management ユーザーロール: スキャンマネージャーまたは管理者

除外を削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[除外]** タイルをクリックします。

   [除外] ページが表示されます。

4. 削除する 1 つまたは複数の除外を選択します。

   - 1 つの除外を選択する場合

     a. 除外の表で、削除する除外にカーソルを合わせます。

     アクションボタンが行に表示されます。

     b. 行にある 🗑 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。

   - 複数の除外を選択する場合

     a. 除外の表で、削除する各除外のチェックボックスを選択します。

     ページの下部またはに、アクションバーが表示されます。

     b. アクションバーで、🗑 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。

5. 確認ウィンドウで、**[削除]** をクリックします。

   Tenable Vulnerability Management により、選択した 1 つまたは複数の除外が削除されます。

除外の設定

注意: 除外はエージェントスキャンには適用されません。

設定	説明
設定	
名前	除外の名前を指定します。
説明	除外の説明を指定します。
ターゲット	スキャンから除外するターゲットを指定します。ターゲットは、コンマで区切られたホスト名または IP 範囲として追加します。 **[ターゲットのアップロード]** 設定ですでにターゲットを指定している場合は、**[ターゲット]** 設定を使用できません。 **ヒント: [ターゲット]** 設定では、「IP:Port」エントリの入力で、IP アドレスごとに特定のポートを除外できます。
ネットワーク	ターゲットが **[デフォルト]** またはカスタムネットワークのいずれかに属するネットワークを指定します。
ターゲットのアップロード	スキャンから除外する、コンマで区切られたホスト名または IP 範囲を含むテキストファイルをアップロードします。 **[ターゲット]** 設定ですでにターゲットを指定している場合は、**[ターゲットのアップロード]** 設定を使用できません。
スケジュール	
有効	除外が有効になっているときのスケジュールを有効または無効にします。無効にする場合、除外は **[常に有効]** に設定されます。有効にする場合、除外が有効な場合の頻度とスケジュールを設定する、次の項目を設定できます。
サマリー	**[頻度]**、**[開始]**、**[終了]** 設定の選択内容に関する概要。
頻度	**[1 度]**、**[日単位]**、**[週単位]**、**[月単位]**、**[年単位]** のオプションを含むドロップダウンボックスです。

設定	説明
開始	除外を開始する日付と時刻を選択できる 2 つのドロップダウンボックスです。 **ヒント:** より細かい開始時刻を選択するには、ボックスに目的の時刻を手動で入力して **[作成]** をクリックします。 **注意:** Tenable Vulnerability Management は、00:00 ~ 00:00 に開始および終了する除外をサポートしていません。
終了	除外を終了する日付と時刻を選択できる 2 つのドロップダウンボックスです。 **ヒント:** より細かい終了時刻を選択するには、ボックスに目的の時刻を手動で入力して **[作成]** をクリックします。 **注意:** Tenable Vulnerability Management は、00:00 ~ 00:00 に開始および終了する除外をサポートしていません。
タイムゾーン	選択した日付と時刻のタイムゾーンを選択できる検索バー付きのドロップダウンボックスです。

コネクタ

Tenable Vulnerability Management では、他のプラットフォームから資産をインポートするために、サードパーティのデータコネクタを含むコネクタを使用しています。Tenable Vulnerability Management は Tenable Vulnerability Management および Tenable Container Security のコネクタをサポートします。

Tenable Vulnerability Management コネクタ

Vulnerability Management には、AWS、GCP、および Microsoft Azure 用のコネクタが含まれています。Tenable Vulnerability Management コネクタを使用して資産をするには、プラットフォームに該当するセクションでセクションで説明しているとおり、最初にコネクタが統合されるプラットフォームを設定してから、コネクタを作成する必要があります。

- Amazon Web Service (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

プラットフォームを設定してコネクタを作成した後は、Tenable Vulnerability Management の [設定] ページからコネクタを管理できます。

> **注意:** クラウドコネクタ使用時、Tenable は、Tenable Vulnerability Management が拠点を置く地域の IP アドレスを許可リストに登録することをおすすめします。

ライセンス付与の意味は次のとおりです。

- 資産が脆弱性のスキャンをされるまで、および脆弱性のスキャンをされない限り、コネクタを介して検出された資産は、ライセンスに不利に作用することはありません。コネクタによる検出には制約がありません。
- コネクタを介して検出された資産のうち、ライセンス付与の対象になったものは、資産が停止した翌日にライセンス対象から外されます。このイベントはコネクタを介して監視できます。
- 資産が終了されると、Tenable Vulnerability Management はスキャン結果と資産のマッチングを停止します。資産は、資産の表のデフォルトビューからも削除されます。
- 資産が削除されると、Tenable Vulnerability Management は資産およびエクスプローラー内の関連するすべての検出結果をパージし、資産のライセンスをリリースします。詳細は、資産を削除するを参照してください。

ヒント: データを Tenable Vulnerability Management に取り込む他の方法については、Tenable Vulnerability Management でのデータ取り込みクイックリファレンスガイドを参照してください。

Container Security コネクタ

Tenable Container Security のコネクタに関しては、イメージをインポートしてスキャンするための Tenable Container Security コネクタの設定を参照してください。

サポートされているプラグイン

AWS および Azure でサポートされているプラグインを表示するには、Tenable プラグインのページを参照してください。Frictionless Assessment プラグインを表示するには、**サポートされているセンサー**のフィルターを使用してください。

Amazon Web Services コネクタ

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

Amazon Web Services (AWS) コネクタは、AWS アカウントにおける EC2 インスタンスのリアルタイム可視性とインベントリを備えています。

AWS における EC2 インスタンスに関する情報をインポートして分析するには、最初に AWS をコネクタ設定に対応する設定にしてから、Tenable Vulnerability Management で AWS コネクタを作成する必要があります。

AWS コネクタを作成すると、AWS 資産を検出して Tenable Vulnerability Management にインポートできます。資産が脆弱性のスキャンをされるまで、および脆弱性のスキャンをされない限り、コネクタを介して検出された資産は、ライセンスに不利に作用することはありません。

AWS 資産の脆弱性を評価する場合、Tenable では、Frictionless Assessment を使用してクラウドの脆弱性を評価することをお勧めします。または、ホスト上でプラグインをローカルに実行する Tenable Nessus スキャナーまたはエージェントスキャンを実行することもできます。

注意: AWS コネクタは、2 種類のインポートを実行します。

- **完全同期**: AWS コネクタがアカウント内のすべての EC2 インスタンスを記述し、それらを Tenable Vulnerability Management にインポートする場合。
- **部分同期**: AWS コネクタがすべてのクラウドトレイルイベントを読み取り、前回の同期以降に作成または終了された EC2 インスタンスをインポートする場合。

AWS コネクタは、24 時間で最大 47 回の部分同期と 1 回の完全同期を実行します。新しいスケジュールを設定すると、AWS はリセットし、もう一度完全同期をトリガーします。

目標	コネクタタイプ
Frictionless Assessment を使用して AWS 資産を検出し、脆弱性を評価する クラウドコネクタは AWS 資産を検出し、AWS EC2 インスタンス上のデータ	• Frictionless Assessment を有効にしたキーレス認証

ポイントにあるインベントリを収集してから、ホスト上でプラグインをローカルで実行するのではなく、クラウド内でホストの脆弱性を評価します。 詳細は、AWS 用の Frictionless Assessment を参照してください。	
AWS 資産を検出する クラウドコネクタは、脆弱性を評価しなくても AWS 資産を検出します。オプションで、Tenable Nessus スキャナーまたはエージェントスキャンを使用すると、検出された資産を後でスキャンできます。 詳細は、AWS クラウドコネクタ (検出のみ) を参照してください。	• キーレス認証 (推奨) • キーベースの認証

既存の AWS コネクタを管理するには、コネクタの管理を参照してください。

ヒント : よくあるコネクタエラーに関する詳細については、Tenable 開発者ポータルのコネクタを参照してください。

AWS 用の Frictionless Assessment

Frictionless Assessment のプロビジョニングは終了し (2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

Frictionless Assessment を使用すると、Tenable Vulnerability Management は Amazon Web Services (AWS) EC2 インスタンス上にあるデータポイントのインベントリを検出して収集します。次に、Frictionless Assessment に指定した AWS タグを持つ EC2 インスタンスの場合、Tenable Vulnerability Management はホスト上ローカルにプラグインを実行するのではなく、クラウド内でホストの脆弱性を評価します。

注意 : Frictionless Assessment は、「停止」状態であっても資産情報を報告します。ホストからデータを収集し AWS EC2 インスタンス上にデータポイントのインベントリを作成するために Frictionless Assessment が利用する AWS Systems Manager エージェント (SSM エージェント) は、「停止」状態であってもデータを収集します。

Frictionless Assessment は、AWS Systems Manager Inventory と AWS Systems Manager Agent (SSM エージェント) を使用して必要なデータを収集します。AWS の設定要件に関する詳細については、Frictionless Assessment 用の AWS を設定するを参照してください。

Frictionless Assessment でホストを評価するためにスキャナー、Tenable Nessus Agents、スキャン、スキャンのスケジュールを設定する必要はありません。

オペレーティングシステムのカバレッジ

Frictionless Assessment は、以下の Amazon Machine イメージから作成された EC2 インスタンスの脆弱性カバレッジを持っています。

- Amazon Linux 1 / 2
- CentOS 6 / 7 / 8
- Red Hat 6 / 7 / 8
- SUSE Linux Enterprise Server (SLES) 11.4-15.2
- SUSE Linux Enterprise Desktop (SLED) 12-15.2
- Ubuntu 16.04 / 18.04 / 20.04
- Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022
- Windows 7、Windows 8、Windows 10、Windows 11

ライセンスの考慮事項

一般に、Tenable Vulnerability Management の資産は脆弱性が評価されるとライセンスに対してカウントされます。そのため、Frictionless Assessment によって評価された EC2 ホストは、ライセンスに対してカウントされます。詳細は、Tenable Vulnerability Management のライセンス を参照してください。

Frictionless Assessment によって評価されるホストの AWS タグを選択するときには、そのタグのいずれかを持つホストがすべてライセンスにカウントされることに注意してください。コネクタによって検出されただけで、Frictionless Assessment によって評価されないホスト (たとえば、Frictionless Assessment に選択したタグを持っていないホスト) は、ライセンスの数としてカウントされません。

サポートされているリージョン

AWS Frictionless Assessment は次のリージョンでサポートされています。

- us-east-1、アメリカ東部 (バージニア州北部)
- us-east-2、アメリカ東部 (オハイオ)
- us-west-1、アメリカ西部 (カリフォルニア州北部)
- us-west-2、アメリカ西部 (オレゴン)
- ca-central-1、カナダ (中央)
- ap-south-1、アジア太平洋 (ムンバイ)
- ap-northeast-1、アジア太平洋 (東京)
- ap-northeast-2、アジア太平洋 (ソウル)
- ap-southeast-1、アジア太平洋 (シンガポール)
- ap-southeast-2、アジア太平洋 (シドニー)
- eu-central-1、EU (フランクフルト)
- eu-west-1、EU (アイルランド)
- eu-west-2、EU (ロンドン)
- eu-west-3、EU (パリ)
- sa-east-1、南アメリカ (サンパウロ)

制限

- Frictionless Assessment は、情報プラグインの実行、リモート脆弱性プラグインの実行、コンプライアンスデータの収集を行いません。
- Frictionless Assessment を使用して設定されたコネクタは、1 つの AWS アカウントしかサポートしません。複数の AWS アカウントのホストを評価する場合は、AWS アカウントごとに個別のコネクタを設定する必要があります。
- Frictionless Assessment で評価する資産を識別するには、1 つの AWS タグキーを使用する必要があります。
- Tenable Vulnerability Management は Frictionless Assessment のインベントリを収集するために、インスタンスに AWS Systems Manager のインベントリ関連を作成します。しかし、AWS ドキュメントに記述されているとおり、AWS Systems Manager ではインベントリのインスタンスへの関連付けは一度に 1 つまでに制限されています。既存のインベントリがインスタンスに関連付けられている場合、Frictionless Assessment を設定する前に解除するようにしてください。詳細は、AWS のドキュメントを参照してください
- Frictionless Assessment スキャンの制限は 1 日あたり 1 回ですが、2023 年 5 月 1 日より前に作成された既存の Frictionless Assessment コネクタは、インベントリデータをより頻繁に送信します。Frictionless Assessment では、この頻度制限を超えるデータはドロップされ、スキャンされません。

  > **注意**: この制限は、Tenable Container Security、エージェントなしの評価、および Tenable Nessus エージェントベースのインベントリスキャンには適用されません。

はじめる

1. 企業内のどのユーザーが、AWS コンソールにアクセスできる適切な AWS 認証情報を持っているかを判断します。
2. AWS 認証情報を持っているユーザーに応じて、次のいずれかを実行します。
    - Tenable Vulnerability Management クラウドコネクタを設定していて、さらに適切な企業の AWS 認証情報を持っている場合
        a. AWS 設定が、Frictionless Assessmentに記載されている Frictionless Assessment の要件を満たしていることを確認してください。
        b. Frictionless Assessment 用の AWS コネクタを作成する の説明に従って AWS コネクタを作成します。
    - Tenable Vulnerability Management クラウドコネクタを設定しているが、企業で*自分以外*のユーザーが必要な AWS 認証情報を持っている場合
        a. AWS 認証情報を持っているユーザーは、Frictionless Assessment 用の AWS を設定するで説明しているように、AWS 設定が Frictionless Assessment の要件を満たしていることを確認する必要があります。
        b. AWS 認証情報を持っているユーザーは、Frictionless Assessment 用の AWS ロールとポリシーを手動で設定する必要があります。
        c. Frictionless Assessment 用にキーレス認証を使用して AWS コネクタを作成するの説明に従って AWS コネクタを作成します。
3. AWS クラウドコネクタを削除するには、コネクタを削除するを参照してください。
4. コネクタを削除したら、AWS でコネクタアーティファクトの手動削除の説明に従って、AWS で CloudFormation スタックを手動で削除します。

Frictionless Assessment 用の AWS を設定する

> Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

Frictionless Assessment は、AWS Systems Manager Inventory と AWS Systems Manager Agent (SSM Agent) を使用してホストからデータを収集し、AWS EC2 インスタンスにデータポイントのインベントリを作成します。Frictionless Assessment でホストを評価するためにスキャナー、Tenable Nessus Agents、スキャン、スキャンのスケジュールを設定する必要はありません。

企業の AWS コンソールへのアクセス権を持っている場合は、Tenable Vulnerability Management クラウドコネクタを作成する前に、AWS の設定が次の要件を満たしていることを確認してください。

他のユーザーが企業の AWS コンソールへのアクセス許可を持っている場合は、そのユーザーが次の要件を満たしていることを確認してから Tenable Vulnerability Management クラウドコネクタを作成してください。

Frictionless Assessment とともに使用するように AWS 環境を設定する方法

1. AWS Systems Manager のドキュメントの説明に従ってアカウント用の AWS Systems Manager をセットアップします。
2. AWS Systems Manager Inventory にアクセスできることを確認します。詳細については、AWS Systems Manager のドキュメントにある *AWS Systems Manager Inventory* (AWS Systems Manager インベントリ) を参照してください。
3. EC2 インスタンスに SSM エージェントがインストールされていることを確認します。
    - ほとんどの EC2 インスタンスのディストリビューションには SSM エージェントがプリインストールされています。詳細については、AWS Systems Manager のドキュメントの *About SSM Agent* (SSM エージェントについて) を参照してください。
    - 使用中のディストリビューションに SSM がインストールされていない場合、AWS Systems Manager のドキュメントの説明に従って SSM エージェントを手動でインストールしてください。
4. Frictionless Assessment で評価する対象の EC2 インスタンスが、1 つの AWS タグキーでタグ付けされていることを確認します。たとえば、タグキー *Tenable* を使用できます。

後でこの AWS タグキーを選択すると、Frictionless Assessment で評価するインスタンスを特定できます。

5. Tenable Vulnerability Management は Frictionless Assessment のインベントリを収集するために、インスタンスに AWS Systems Manager のインベントリ関連を作成します。しかし、AWS ドキュメントに記述されているとおり、AWS Systems Manager ではインベントリのインスタンスへの関連付けは一度に 1 つまでに制限されています。既存のインベントリがインスタンスに関連付けられている場合、Frictionless Assessment を設定する前に解除するようにしてください。詳細は、AWS のドキュメントを参照してください

次の手順

- 所属の組織の AWS 認証情報を持っているユーザーに応じて、次のことを実行します。
    - Tenable Vulnerability Management クラウドコネクタを設定していて、さらに所属組織の適切な AWS 認証情報を持っている場合
        - Frictionless Assessment 用の AWS コネクタを作成する の説明に従って AWS コネクタを作成します

Frictionless Assessment 用の AWS コネクタを作成する

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

Frictionless Assessment 用のキーレス認証を使用して Amazon Web Services (AWS) クラウドコネクタを設定した場合、Tenable Vulnerability Management は Cloud Formation テンプレート (CFT) を使用して、ユーザーの AWS アカウントに必要なロールとポリシーを自動的に設定します。この設定は、通常のクラウドコネクタと Frictionless Assessment をセットアップします。

AWS コネクタを Frictionless Assessment で使用するには、AWS タグキーを入力して、Frictionless Assessment が評価するホストを特定する必要があります。タグキーを入力しない場合、コネクタは検出のみとして機能し、資産の脆弱性は評価されません。

注意: Frictionless Assessment について評価するホストを所有する AWS アカウントごとに個別のクラウドコネクタを作成します。

始める前に

- AWS 設定が、Frictionless Assessment に記載されている Frictionless Assessment の要件を満たしていることを確認してください。
- 最善の結果を得るには、これが新しい AWS クラウドコネクタのセットアップであることを確認してください。既存の AWS クラウドコネクタが設定済みの場合は、新しい AWS クラウドコネクタを作成する前に既存の *[tenableio-connector]* IAM ロールを削除します。

  注意: Tenable Cloud Security プレビューまたは Tenable Cloud Security を使用するには、Tenable Cloud Security をサポートする新しいロールを更新または作成する必要があります。Tenable Vulnerability Management クラウドコネクタロールでは、Agentless Assessment をサポートしていません。

- Tenable Vulnerability Management へのアクセスに使用している同じブラウザの別のウィンドウまたはタブで、Frictionless Assessment でターゲットにする AWS アカウントを使用して AWS コンソールにログインします。

AWS Frictionless Assessment コネクタと CFT を作成

1. Tenable Vulnerability Management のユーザーインターフェースにログインし、**[設定]** > **[クラウドコネクタ]** の順に移動します。
2. **[クラウドコネクタの作成]** をクリックします。

   [クラウドコネクタの選択] パネルが表示されます。
3. **[クラウドコネクタ]** リストで、**[Frictionless Assessment]** を選択します。

   [コネクタのセットアップ] ポップアップが表示されます。
4. **[クラウドプロバイダー]** の手順で、**[AWS]** を選択して **[コネクタ名]** を入力します。

   [次へ] をクリックします。
5. **[機能の有効化]** の手順で、**[Frictionless Assessment を使用して脆弱性を特定する]** チェックボックスがオンになっていることを確認します。

   [次へ] をクリックします。
6. **[設定]** の手順で、ターゲットパラメーターを選択します。
   a. ターゲットにする**アカウント ID** を入力します。
   b. **タグ**キーと値を入力してタグを選択します。
      i. **[タグキー]** ボックスに AWS タグキーを入力します。

         たとえば、AWS タグの場合は *Tenable:FA* で、タグ値は *Tenable* です。
      ii. **[タグ値]** ボックスで次のいずれかを実行します。

         たとえば、AWS タグの場合は *Tenable:FA* で、タグ値は *FA* です。

> **ヒント:** AWS Frictionless Assessment に対して指定できるタグは 1 つだけです。

> **注意:** タグのキーと値では大文字と小文字が区別され、AWS にあるものと正確に一致する必要があります。

> **注意:** AWS コネクタを Frictionless Assessment で使用するには、AWS タグキーを入力して、Frictionless Assessment が評価するホストを特定する必要があります。タグキーを入力しない場合、コネクタは検出のみとして機能し、資産の脆弱性は評価されません。

c. ターゲットにする **[ネットワーク]** を選択します。**[ネットワーク]** ドロップダウンメニューを使用して、既存のネットワークを選択するか、新しいネットワークを作成できます。ネットワークを指定しない場合、デフォルトのネットワークが選択されます。

[次へ] をクリックします。

7. **[選択を適用]** の手順で、**[ダウンロードして終了]** をクリックします。

CFT が .yml 形式でダウンロードされ、新しいコネクタが **[クラウドコネクタ]** ページに表示されます。

CFT を使用してコネクタをデプロイメント

前のセクションでダウンロードした CFT を AWS アカウントにデプロイします。(詳細については、AWS のドキュメントを参照してください。)

複数のリージョンにデプロイする必要がある場合は、テンプレートをスタックセットとしてデプロイすることをお勧めします。(詳細については、AWS スタックセットのドキュメントを参照してください。)

次の手順

- AWS アカウントをお持ちでない場合は、検出専用のキーレス認証を使用した AWS コネクタの作成を使用してください。資産のステータスと資産の終了を追跡するには、AWS アカウントに Tenable Vulnerability Management のキーレスコネクタが必要です。

  > **注意:** キーレスコネクタは、AWS Frictionless Assessment が設定されているのと同じアカウントに設定する必要があります。

- 必要に応じて、AWS Frictionless Assessment コネクタのタグを編集します。詳細は、AWS Frictionless Assessment コネクタの編集 を参照してください。
- View assets はコネクタによって検出されたホストを表示します。AWS コネクタが Frictionless Assessment を使用して検出したホストがソースの **SSM** とともに表示されます。
- 脆弱性を表示し、Frictionless Assessment によって特定された脆弱性を表示します。

AWS Frictionless Assessment コネクタの編集

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

Amazon Web Services (AWS) Frictionless Assessment コネクタの名前、タグ、およびネットワークを編集できます。

注意: AWS Frictionless Assessment コネクタのタグを編集する場合、AWS アカウントにコネクタを再デプロイして、AWS のタグ情報を更新する必要があります。

AWS Frictionless Assessment コネクタを編集する方法

1. Tenable Vulnerability Management のユーザーインターフェースにログインし、**[設定]** > **[クラウドコネクタ]** の順に移動します。
2. クラウドコネクタの表で、タグを編集する **AWS_FA** コネクタをクリックします。

   コネクタの **[編集]** ページが表示されます。
3. コネクタを編集します。
   - コネクタ名を編集するには、**[コネクタ名]** フィールドをクリックし、新しい名前を入力します。
   - コネクタタグを編集するには、次のようにします。
     a. **[タグキー]** ボックスに AWS タグキーを入力します。

        たとえば、AWS タグの場合は *Tenable:FA* で、タグ値は *Tenable* です。

     b. **[タグ値]** ボックスで次のいずれかを実行します。

        たとえば、AWS タグの場合は *Tenable:FA* で、タグ値は *FA* です。

   ヒント: AWS Frictionless Assessment に対して指定できるタグは 1 つだけです。

   注意: タグのキーと値では大文字と小文字が区別され、AWS にあるものと正確に一致する必要があります。

> **注意：** AWS コネクタを Frictionless Assessment で使用するには、AWS タグキーを入力して、Frictionless Assessment が評価するホストを特定する必要があります。タグキーを入力しない場合、コネクタは検出のみとして機能し、資産の脆弱性は評価されません。

- コネクタがリンクされているネットワークの変更を編集するには、**[ネットワーク]** ドロップダウンメニューを使用して、既存のネットワークを選択するか、新しいネットワークを作成します。ネットワークを指定しない場合、Tenable Vulnerability Management はデフォルトのネットワークを選択します。

4. **[CFT のダウンロード]** ボタンをクリックします。

   > **注意：** コネクタタグを編集した場合、ボタンには **[CFT をダウンロードして保存する]** と表示されます。

   CFT が .yml 形式でダウンロードされ、更新されたコネクタ情報が **[クラウドコネクタ]** ページに表示されます。

5. コネクタタグを編集した場合は、CFT を AWS アカウントに再デプロイします（詳細については、AWS のドキュメントを参照してください）。

   複数のリージョンにデプロイする必要がある場合は、テンプレートをスタックセットとしてデプロイすることをお勧めします（詳細については、AWS スタックセットのドキュメントを参照してください）。

AWS でコネクタアーティファクトの手動削除

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

最後の AWS コネクタを削除すると、Tenable Vulnerability Management によって、コネクタと Frictionless Assessment 設定に関連付けられているほとんどの AWS のアーティファクトの自動削除がトリガーされます。

ただし、CloudFormation スタックまたはスタックセットは自動的には削除されません。CloudFormation スタックまたはスタックセットは、AWS CloudFormation コンソールで手動で削除する必要があります。

始める前に

- コネクタを削除するの説明に従って、AWS コネクタを削除します。

AWS コネクタからアーティファクトを削除する方法

- AWS CloudFormation ユーザーガイドの *AWS CloudFormation コンソールでのスタックの削除*の説明に従って、Tenable によって作成された CloudFormation スタックまたはスタックセットを削除します。スタックは、`.yml` ファイルで、関連するコネクタと同じ名前です。

AWS の Frictionless Assessment コネクタを更新して Log4j を検出します。

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

AWS Frictionless Assessment コネクタで Log4j の脆弱性を検出できるようにするには、**TenableInventoryCollection** スクリプトがインストールされている各 AWS リージョンでそのスクリプトを更新します。

注意: AWS アカウントが複数ある場合は、各アカウント内で関連するすべてのリージョンで以下の手順を完了する必要があります。

AWS Frictionless Assessment コネクタを更新して Log4j を検出する方法

1. [Tenable の摩擦のないダウンロード] ページに移動して、`TenableInventoryCollection-document-v2.json` ファイルをダウンロードします。
2. AWS コンソールにログインします。
3. **[システム管理]** を開きます。
4. **[ドキュメント]** > **[所有]** の順にクリックします。
5. **TenableInventoryCollection** ドキュメントを開きます。

   `TenableInventoryCollection` の **[説明]** ページが開きます。
6. 右上の **[アクション]** をクリックします。
7. **[新しいバージョンの作成]** をクリックします。

   新しいバージョンの **[コンテンツ]** ペインが表示されます。
8. **[JSON]** ラジオボタンを選択します。
9. **[JSON]** の下にあるボックス内の内容を削除します。

10. `TenableInventoryCollection-document-v2.json` の内容をコピーして、**JSON** の下にあるボックスに貼り付けます。
11. コンテンツボックスの下にある **[新しいバージョンの作成]** をクリックします。

    [ドキュメント] > **[Amazon 所有]** ページが開きます。
12. **[ドキュメント]** > **[所有]** ページに移動します。
13. **TenableInventoryCollection** ドキュメントを開きます。
14. 右上の **[アクション]** をクリックします。
15. **[デフォルトバージョンの設定]** をクリックします。

    [デフォルトバージョンの設定] ページが表示されます。
16. ドロップダウンリストを使用して、**[バージョン]** の値を **2** に設定します。
17. **[デフォルトバージョンの設定]** をクリックします。

    > **注意:** AWS のリージョンが更新されて Log4j が検出されているかを確認するには、**TenableInventoryCollection** ドキュメントを開いて **[コンテンツ]** タブに移動し、**Ctrl + F** で「log4j」を検索します。コードに「log4j」が含まれている場合は更新されています。

AWS クラウドコネクタ (検出のみ)

Amazon Web Services (AWS) クラウドコネクタは、AWS アカウントにおけるリアルタイムの可視性と EC2 資産のインベントリを備えています。

AWS コネクタを作成すると、AWS 資産を検出して Tenable Vulnerability Management にインポートできます。資産が脆弱性のスキャンをされるまで、および脆弱性のスキャンをされない限り、コネクタを介して検出された資産は、ライセンスに不利に作用することはありません。

> **ヒント:** エージェントやスキャンを設定せずに EC2 インスタンスの脆弱性を評価できる Frictionless Assessment を使用して AWS コネクタを設定するには、AWS 用の Frictionless Assessmentを参照してください。

次のいずれかの設定をしようすると、検出用の AWS コネクタを作成できます。

- 推奨: キーレス認証を使用した AWS コネクタ (検出のみ)
- キーによる認証を使用する AWS コネクタ

サポートされているリージョン

AWS 検出コネクタは次のリージョンでサポートされています。

- us-east-1、アメリカ東部 (バージニア州北部)
- us-east-2、アメリカ東部 (オハイオ)
- us-west-1、アメリカ西部 (カリフォルニア州北部)
- us-west-2、アメリカ西部 (オレゴン)
- ca-central-1、カナダ (中央)
- ap-south-1、アジア太平洋 (ムンバイ)
- ap-northeast-1、アジア太平洋 (東京)
- ap-northeast-2、アジア太平洋 (ソウル)
- ap-southeast-1、アジア太平洋 (シンガポール)
- ap-southeast-2、アジア太平洋 (シドニー)
- ap-southeast-3、アジア太平洋 (ジャカルタ)
- eu-central-1、EU (フランクフルト)

- eu-west-1、EU（アイルランド）
- eu-west-2、EU（ロンドン）
- eu-west-3、EU（パリ）
- me-south-1、中近東（バーレーン）
- ap-east-1、アジアパシフィック（香港）
- af-south-1、アフリカ（ケープタウン）
- eu-south-1、ヨーロッパ（ミラノ）
- sa-east-1、南アメリカ（サンパウロ）

キーレス認証を使用したAWSコネクタ(検出のみ)

Amazon Web Services (AWS) コネクタは、AWS アカウントにおけるリアルタイムの可視性とEC2 資産のインベントリを備えています。

AWS コネクタを作成すると、AWS 資産を検出して Tenable Vulnerability Management にインポートできます。資産が脆弱性のスキャンをされるまで、および脆弱性のスキャンをされない限り、コネクタを介して検出された資産は、ライセンスに不利に作用することはありません。

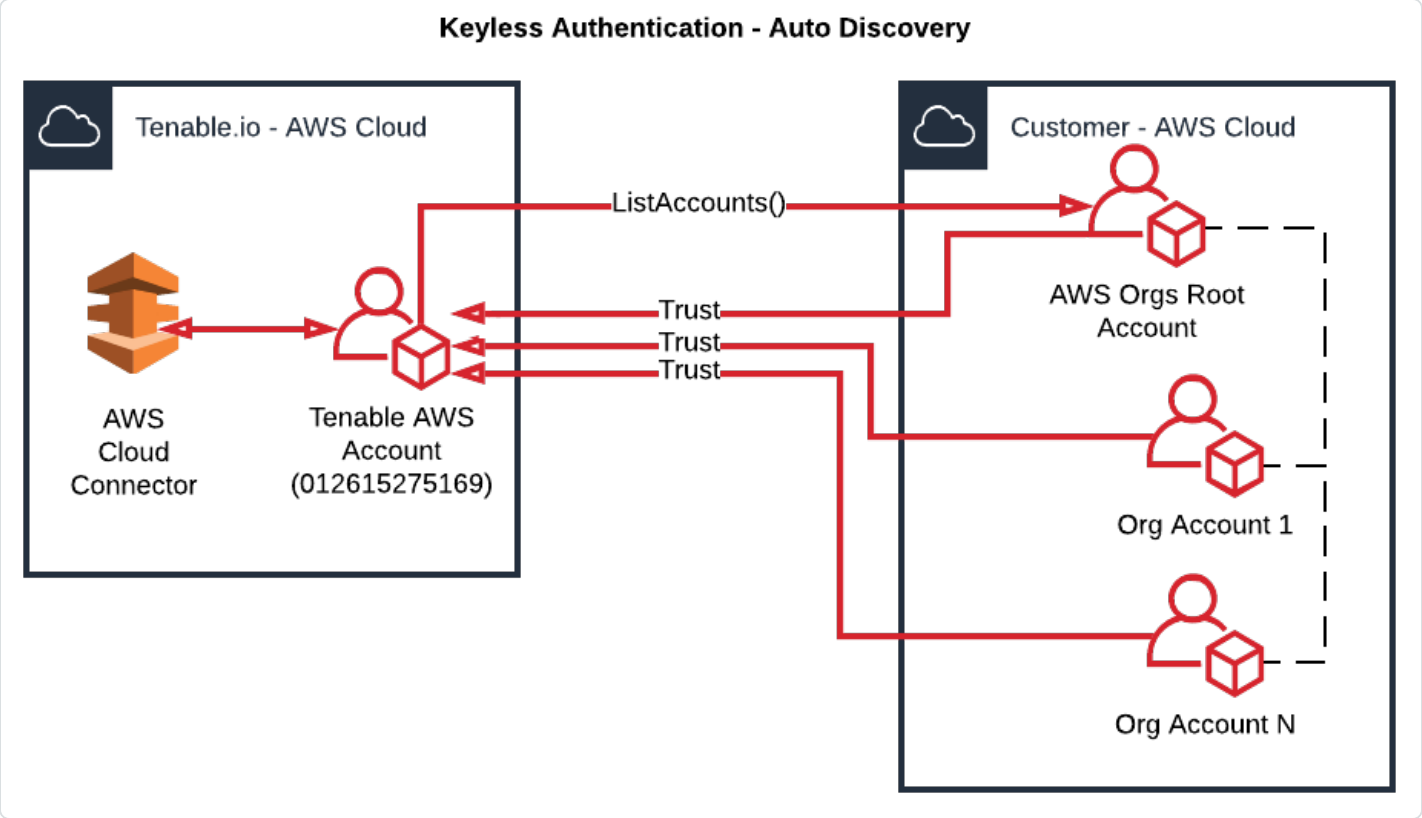
ヒント: エージェントやスキャンを設定せずに EC2 インスタンスの脆弱性を評価できる Frictionless Assessment を使用して AWS コネクタを設定するには、AWS 用の Frictionless Assessmentを参照してください。

キーレス認証

Tenable Vulnerability Management AWS コネクタは、AWS のロール委任によるキーレス認証に対応しています。AWS ロール委任によるキーレス認証により、AWS 資産の自動検出が可能になります。キーレス認証を使用するには、AWS アカウントと Tenable AWS アカウントの間に信頼関係を確立する必要があります。このシナリオでは、ご利用の AWS アカウントが信頼関係のある AWS アカウントと通信し、AWS アカウントがご利用の AWS コネクタと通信します。

AWS アカウントの自動検出

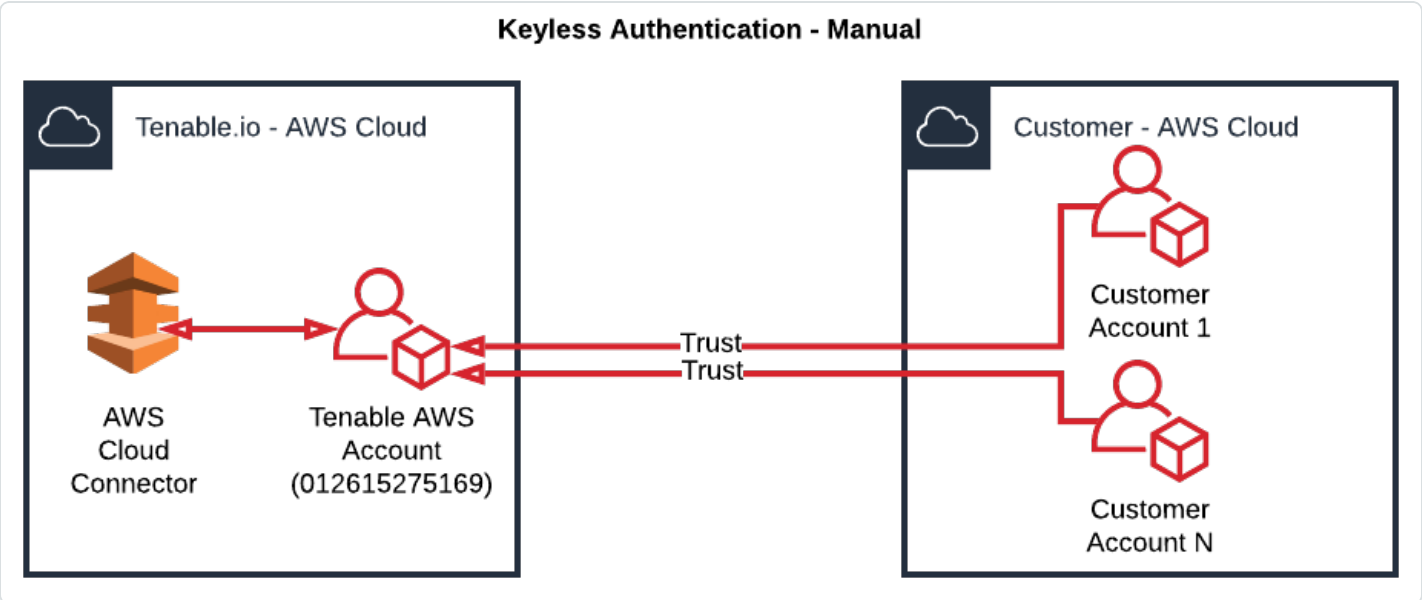
Tenable AWS アカウントが組織内に存在する他の AWS アカウントを自動で検出できるようにするには、自動アカウント検出でキーレス認証を使用します。AWS Organizations を有効にして、`ListAccounts` ポリシーを割り当てる必要があります。これにより、他の AWS アカウントが検出され、次の図に示すように、信頼関係が確立されます。



AWS Organizations をセットアップする方法の詳細は、AWS のドキュメントを参照してください。

AWS アカウントの手動リンク

自動アカウント検出を使用しない場合、または AWS 企業を使用しない場合は、以下の図のようにリンクされた AWS アカウントを手動で設定できます。



キーレス認証を使用して AWS コネクタを設定および作成する方法

1. キーレス認証用の AWS の設定 (検出のみ)
2. 検出専用のキーレス認証を使用した AWS コネクタの作成

キーレス認証用の AWS の設定 (検出のみ)

必要なユーザーロール: 管理者

キーレス認証を使用して検出専用コネクタを作成する前に、まず AWS を設定する必要があります。AWS アカウントのリンクと信頼関係の構築に関する詳細については、「キーレス認証を使用した AWS コネクタ (検出のみ)」を参照してください。

始める前に

1. AWS アカウントで、CloudTrail を有効にします。
2. CloudTrail がまだない場合は、証跡を作成します。
3. 証跡で、**[すべて]** または **[書き込みのみ]** の管理イベントとログをオンにします。

   注意: 資産のインポートに AWS コネクタを使用する場合、Tenable はそのコネクタに関してすべての CloudTrails を照会し、CloudTrails がイベントを受け取るすべてのリージョンを確認します。確認された一連のリージョンは、EC2 および CloudTrail API のコールの際に使用されます。

キーレス認証を使用して検出専用コネクタ用に AWS を手動で設定する方法

1. ライセンス情報の説明に従って、Tenable Vulnerability Management コンテナ ID を取得します。
2. AWS アカウントでは、*tenableio-connector*というロールを作成して、IAM ユーザーにアクセス許可を委任します。

   ヒント: 詳細については、Amazon AWS ドキュメントを参照してください。

   a. AWS コンソールのナビゲーションペインで、**[ロール]** > **[ロールの作成]** の順にクリックします。

   b. ロールの種類については、**[別の AWS アカウント]** をクリックします。

   c. **[アカウント ID]** には ID `012615275169` を入力します。

      注意: `012615275169` は、AWS ロール委任をサポートするために信頼関係を構築する Tenable AWS アカウントのアカウント ID です。

   d. **[外部 ID の要求]** チェックボックスを選択して、ステップ 1 で取得した Tenable Vulnerability Management コンテナ ID を入力します。

   e. **[次へ: アクセス許可の追加]** をクリックします。

f. 次のアクセス許可を持つポリシーを作成または再使用します。

AWS サービス	アクセス許可
Amazon EC2	• DescribeInstances
AWS CloudTrail	• DescribeTrails • GetEventSelectors • GetTrailStatus • ListTags • LookupEvents
AWS Organizations	• ListAccounts **注意:** Tenable Vulnerability Management が AWS アカウントを自動検出するには、`ListAccounts` のアクセス許可が必要です。自動アカウント検出を使用しない場合、このアクセス許可は不要です。

注意: Tenable では、各 AWS サービスの **Amazon リソースネーム** を *(すべてのリソース)に設定することをお勧めします。

a. **[次へ: タグ]** をクリックします。

b. (オプション) 必要なタグを追加します。

c. **ポリシー**を作成します。

g. **[次へ: レビュー]** をクリックします。

h. **[ロール名]** ボックスに *tenableio-connector* と入力します。

警告: ロールには、コネクタが動作するよう *tenableio-connector* と名前を付ける必要があります。

i. ロール名が *tenableio-connector* であることを確認し、**[ロールの作成]** をクリックします。

j. 新しい *tenableio-connector* ロールを表示して、**[信頼関係]** タブをクリックします。

k. **[信頼関係の編集]** をクリックします。

ポリシードキュメントがテキストボックスに表示されます。

l. テキストボックスの **AWS** 行で、`arn:aws:iam::012615275169:root` を `arn:aws:iam::012615275169:role/keyless_connector_role` に置き換えます。

m. **[信頼ポリシーの更新]** をクリックします。

次の手順

- 検出専用のキーレス認証を使用した AWS コネクタの作成

検出専用のキーレス認証を使用したAWSコネクタの作成

必要なユーザーロール: 管理者

AWSコネクタを作成すると、AWS資産を検出してTenable Vulnerability Managementにインポートできます。資産が脆弱性のスキャンをされるまで、および脆弱性のスキャンをされない限り、コネクタを介して検出された資産は、ライセンスに不利に作用することはありません。

始める前に

- キーレス認証用のAWSの設定 (検出のみ)

注意: Tenable Cloud Securityプレビューまたは Tenable Cloud Securityを使用するには、Tenable Cloud Securityをサポートする新しいロールを更新または作成する必要があります。Tenable Vulnerability Managementクラウドコネクタロールでは、Agentless Assessmentをサポートしていません。

検出専用のキーレス認証を使用してAWSコネクタを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. ページの右上にある **[クラウドコネクタの作成]** ボタンをクリックします。

   クラウドコネクタ選択プレーンが表示されます。

5. **[クラウドコネクタ]** セクションで、**[Amazon Web Services]** をクリックします。

   コネクタ作成プレーンが表示されます。

6. **[コネクタ名]** ボックスに、コネクタを識別する名前を入力します。

7. **[アカウント ID]** ボックスにプライマリAWSアカウントIDを入力します。

8. (オプション) **[スタックの作成]** をクリックして、クラウド形成テンプレート (CFT) をAWSアカウントにデプロイします。

注意: 検出専用コネクタの場合、AWS アカウントで手動で *Tenableio-Connector* ロールを設定した場合に限り、ユーザーインターフェースのスタック作成手順をスキップしてください。スタックは、Tenable Vulnerability Management コネクタの使用に必要なパラメーター、ポリシー、およびロールを設定します。

9. (オプション) クラウドコネクタ設定をさらに展開するには、**[クラウドコネクタの詳細設定]** をクリックします。

    a. (オプション) **[アカウントの自動検出]** トグルを使用して、リンク済みアカウントと CloudTrails の自動検出を有効または無効にします。

    注意: リンクされたアカウントごとに、手動または CFT を介して、*tenableio-connector* のロールを必ず作成してください。

    b. (オプション) **[自動アカウント検出]** を無効にした場合は、次のいずれかの操作を実行します。

    - AWS アカウントを手動で追加するには、**[クラウド評価用のアカウント]** の横にある ⊕ をクリックします。
    - AWS CloudTrails を手動で追加するには、**[クラウド評価用の AWS CloudTrails]** の横にある ⊕ をクリックします。

    c. (オプション) **[ネットワークの選択または作成]** ドロップダウンボックスで、コネクタを追加する既存のネットワークを選択します。

    コネクタが資産を検出すると、関連するネットワークが資産の詳細に追加されます。詳細は、ネットワークを参照してください。

    d. (オプション) **[クラウドコネクタスケジュール]** トグルを使用してスケジュールしたインポートを有効または無効にします。

    デフォルトでは、Tenable Vulnerability Management は 1 日ごとに新規および更新された資産レコードをリクエストします。

    有効にした場合には

    i. テキストボックスに、Tenable Vulnerability Management が AWS サーバーにデータリクエストを送信する頻度を入力します。

ii. ドロップダウンボックスで、**[分]**、**[時]**、**[日]** のいずれかを選択します。

> **注意:** コネクタ設定を 30 分ごとに同期するようにスケジュールすると、検出ジョブが 30 分ごとにキューに配置されます。コネクタサービスのワークロードに応じて、検出ジョブの結果が Tenable Vulnerability Management インターフェースとログで参照できるようになります。したがって、キューによっては、検出ジョブの結果が出るのに 30 分以上かかる場合があります。

10. 次のいずれかを行います。

    - コネクタを保存するには、**[保存]** をクリックします。
    - コネクタを保存して、AWS から資産をインポートするには、**[保存してインポート]** をクリックします。

    Tenable Vulnerability Managementによって、AWS から資産をインポートします。資産が表示されるまで多少時間がかかる場合があります。

次の手順

- View assets、コネクタが検出した資産を表示します。

キーによる認証を使用する AWS コネクタ

Amazon Web Services (AWS) コネクタは、AWS アカウントにおけるリアルタイムの可視性と EC2 資産のインベントリを備えています。

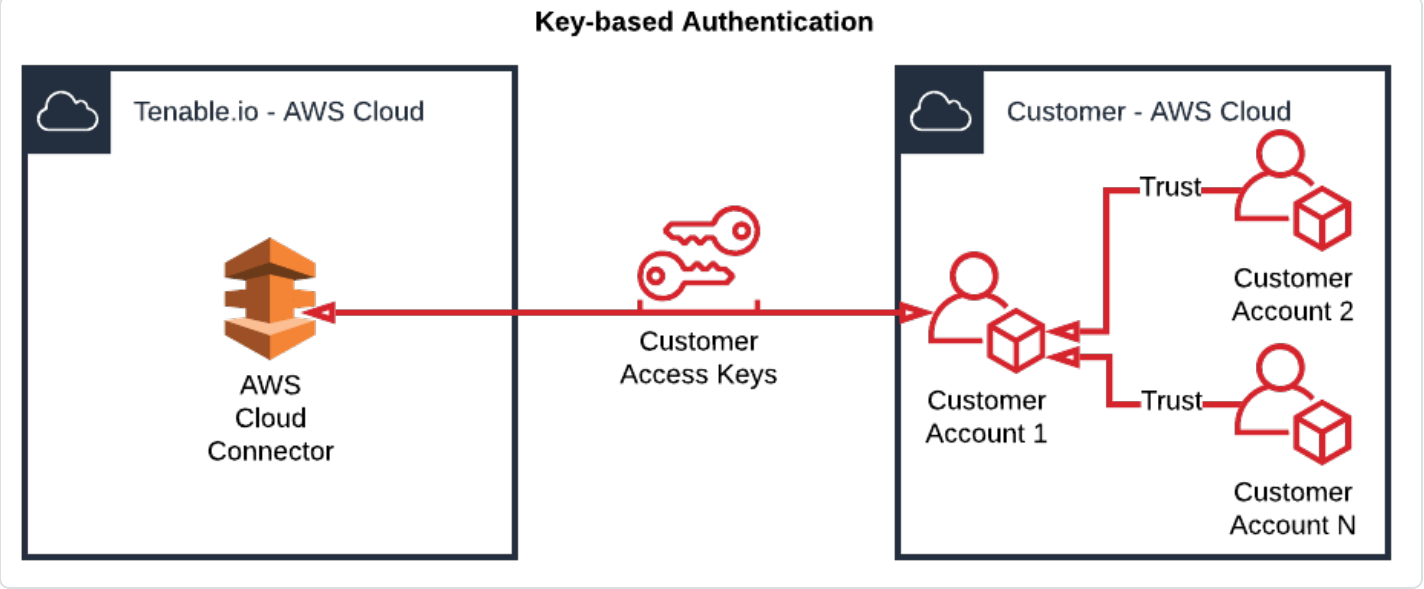
AWS コネクタを作成すると、AWS 資産を検出して Tenable Vulnerability Management にインポートできます。資産が脆弱性のスキャンをされるまで、および脆弱性のスキャンをされない限り、コネクタを介して検出された資産は、ライセンスに不利に作用することはありません。

キーによる認証

Tenable Vulnerability Management AWS コネクタは、アクセス許可を持つ IAM ユーザーおよび秘密鍵とアクセスキーを使用する、鍵ベースの認証をサポートします。このシナリオでは、Tenable Vulnerability Management AWS コネクタは、秘密鍵とアクセスキーを使用してプライマリ AWS アカウントと認証します。さらに、次の図に示すように、プライマリ AWS アカウントとの信頼関係を持つリンクされたセカンダリ AWS アカウントを手動で設定できます。

その他の AWS 認証オプションについて詳しくは、Amazon Web Services コネクタを参照してください。

> **注意:** 鍵ベースの認証が設定された AWS コネクタでは、AWS アカウントの自動検出はサポートされません。また、鍵ベースの認証は推奨されません。



Tenable Vulnerability Management との、AWS の鍵ベースの認証を完全に設定する方法

1. 鍵ベース認証にAWSを設定するで説明されているように、AWSで、コネクタの鍵ベース認証をサポートするようにプライマリAWSアカウントを設定します。
2. (オプション) AWSでは、リンクされたAWSアカウントを設定する(鍵ベース)で説明されるとおりにリンクされたAWSアカウントを手動で設定します。
3. Tenable Vulnerability Managementで、鍵ベース認証を使用してAWSコネクタを作成するの説明に従ってAWSコネクタを作成します。

AWS にキーによる認証を設定する

必要なユーザーロール: 管理者

始める前に

- CloudTrail を有効にし、trail がまだない場合は trail を作成します。

  注意: **[すべて]** または **[書き込みのみ]** の管理イベントと、証跡ログをオンにする必要があります。

アクセス許可を持つ IAM ユーザーを介して Tenable Vulnerability Managementコネクタに対応するよう AWS を設定する方法 (キーベースの認証):

1. Tenable Vulnerability Management と統合するために、Policy Generator を使用して IAM アクセス許可ポリシーを作成します。
2. 次のアクセス許可をポリシーに追加します。

AWS Service	アクセス許可
EC2	• DescribeInstances
CloudTrail	• DescribeTrails • GetEventSelectors • GetTrailStatus • ListTags • LookupEvents

   各 AWS サービスに対して、**Amazon Resource Name** には* (すべてのリソース) の設定をお勧めします。
3. programmatic access (プログラムによるアクセス) で IAM ユーザーを作成します。
4. 手順 2 で作成したポリシーを IAM ユーザーに割り当てます。
5. アクセスとシークレットキーを入手します。

(オプション) リンクされた AWS アカウントを設定する方法

- AWS アカウントをリンク

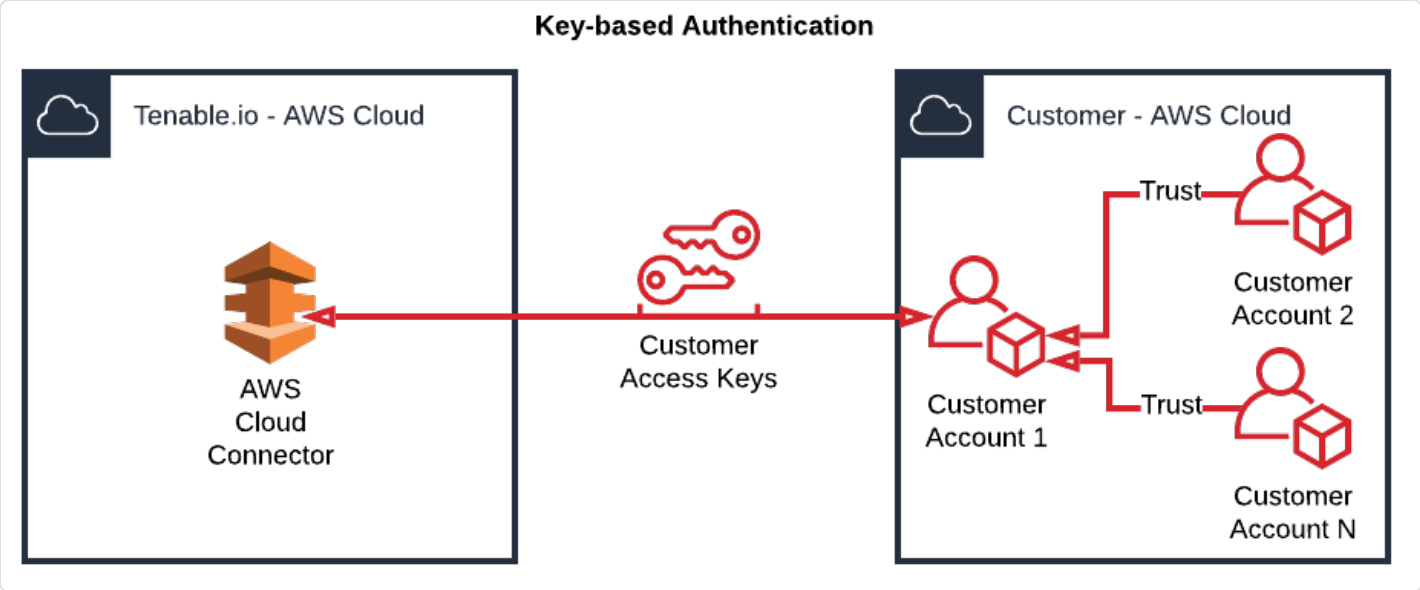
次の手順

- キー付き認証を使用して AWS コネクタを作成します

キーによる認証用にリンクされた AWS アカウントの設定

必要なユーザーロール: 管理者

このセクションでは、プライマリーアカウントでアクセスキーが既に生成されているものとし、以下の図で示すように、AWS 連結アカウントの設定方法を説明します。



始める前に

- AWS プライマリーアカウントを設定します。
- プライマリ AWS アカウントのアカウント ID を記録します。

リンクされた AWS アカウントを設定する方法

1. ライセンス情報の説明に従って、Tenable Vulnerability Management コンテナ ID を取得します。
2. AWS アカウントでは、Amazon AWS ドキュメントに記載のとおり、「**tenableio-connector**」というロールを作成し、IAM ユーザーへのアクセス許可を割り当てます。
    a. コンソールのナビゲーションペインで、**[ロール] > [ロールの作成]** の順にクリックします。
    b. ロールの種類については、**[別の AWS アカウント]** をクリックします。
    c. **[アカウント ID]** では、AWS プライマリアカウントの AWS アカウント ID を入力します。

d. **[外部 ID の要求]** チェックボックスを選択して、ステップ 1 で取得した Tenable コンテナ ID を入力します。

e. **[次へ: アクセス許可]** をクリックします。

f. 次のアクセス許可を持つポリシーを作成または再使用します。

AWS サービス	アクセス許可
Amazon EC2	• DescribeInstances
AWS CloudTrail	• DescribeTrails • GetEventSelectors • GetTrailStatus • ListTags • LookupEvents

各 AWS サービスに対して、**Amazon Resource Name** には * (すべてのリソース) の設定をお勧めします。

g. **[次へ: タグ付け]** をクリックします。

h. (オプション) 必要なタグを追加します。

i. **[次へ: レビュー]** をクリックします。

j. **[ロール名]** ボックスに **tenableio-connector** と入力します。

> **警告:** ロールには、コネクタが動作するよう「**tenableio-connector**」と名前を付ける*必要があります*。

k. ロール名が **tenableio-connector** であることを確認し、**[ロールの作成]** をクリックします。

l. 作成したロールに**ロール ARN** を登録します。次のセクションの設定でロール ARN が必要となります。

AWS プライマリーアカウントを設定する方法

> **注意:** 手順の詳細については、Amazon ドキュメントの所属組織のメンバーアカウントへのアクセスと管理を参照してください。

1. AWS Security Token Service (AWS STS) の AssumeRole API (*sts:AssumeRole*) のアクションを使用するため、アクセス許可のあるポリシーを作成します。
    a. **[ポリシー]** に移動し、**[ポリシーの作成]** をクリックします。
    b. **[サービス]** に、**[STS]** を選択します。
    c. **[アクション]** に、**[フィルター]** ボックスで **AssumeRole** と入力し、横に表示されるチェックボックスを選択します。
    d. **[ロールのリソースタイプを必要とするアクションを選択しました]** をクリックします。
    e. **[ARN の追加]** をクリックします。
    f. **[ロール用の ARN の指定]** フィールドに、リンクされたアカウントで作成したロールに対し登録した ARN を貼り付けます。
    g. **[追加]** をクリックします。
    h. **[ポリシーのレビュー]** をクリックします。
    i. **[名前]** フィールドで、ポリシー固有の名前を入力します。
    j. **[ポリシーの作成]** をクリックします。
2. ステップ 1 で作成したポリシーを、コネクタを作成した際に使用するアクセスキーと関連づけるユーザーまたはグループに追加します。
    a. **[アクセス許可の追加]** ボタンをクリックします。
    b. **[既存のポリシーを直接添付]** チェックボックスを選択します。
    c. ステップ 1 で作成した `sts:AssumeRole` を持つポリシーを検索します。
    d. **[次へ: レビュー]** をクリックします。
    e. **[アクセス許可の追加]** をクリックします。

鍵ベース認証を使用して AWS コネクタを作成する

必要なユーザーロール: 管理者

始める前に

- 鍵ベースの認証のために必要な AWS 設定手順を完了します。

AWS コネクタを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. ページの右上にある **[クラウドコネクタの作成]** ボタンをクリックします。

   クラウドコネクタ選択プレーンが表示されます。

5. **[クラウドコネクタ]** セクションで、**[AWS - Keyed セットアップ]** をクリックします。

   クラウドコネクタ作成プレーンが表示されます。

6. **[コネクタ名]** ボックスに、コネクタを識別する名前を入力します。

7. **[アクセスキー]** ボックスに、AWS の設定の際に取得したアクセスキーを入力します。

8. **[秘密鍵]** ボックスに、使用したアクセスキーに対応する秘密鍵を入力します。

9. **[ネットワークを選択または作成する]** ドロップダウンボックスで、コネクタの既存のネットワークを選択するか、⊕ ボタンをクリックして新しいネットワークを作成します。

   注意: ネットワークは、クラウド資産と Nessus によって検出された資産の間での IP アドレスの衝突を回避するのに役立ちます。Tenable では、異なるクラウド環境の資産レコードが相互に上書きされないように、使用するコネクタタイプごとにネットワークを作成することをお勧めします。ネットワーク機能の詳細については、ネットワークを参照してください。

10. **[クラウドコネクタスケジュール]**トグルを使用してスケジュールしたインポートを有効または無効にします。

    > **注意:** デフォルトでは、Tenable Vulnerability Management は 1 時間ごとに新規および更新された資産レコードをリクエストします。

    有効にした場合

    - **[インポート]**テキストボックスに、Tenable Vulnerability Management が AWS サーバーにデータリクエストを送信する頻度を入力します。
    - ドロップダウンボックスで、*[分]*、*[時間]*、*[日]*のいずれかを選択します。

      > **注意:** コネクタ設定を 30 分ごとに同期するようにスケジュールすると、検出ジョブが 30 分ごとにキューに配置されます。コネクタサービスのワークロードに応じて、検出ジョブの結果が Tenable Vulnerability Management インターフェースとログで参照できるようになります。したがって、キューによっては、検出ジョブの結果が出るのに 30 分以上かかる場合があります。

11. 次のいずれかを行います。

    - コネクタを保存するには、**[保存]**をクリックします。
    - コネクタを保存して、AWS から資産をインポートするには、**[保存してインポート]**をクリックします。

> **注意:** 資産が Tenable Vulnerability Managementに表示されるまでに時間がかかる場合があります。

Microsoft Azure コネクタ

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

Microsoft Azure コネクタは、Microsoft Azure アカウントにおけるリアルタイムの可視性と資産のインベントリを備えています。

Microsoft Azure の資産についての情報をインポートおよび分析するには、Azure がコネクタに対応するよう設定し、Tenable Vulnerability Management で Azure コネクタを作成する必要があります。

注意: お使いの Azure デプロイメントが、Azure China または Azure Government リージョンの Azure インスタンスを含む場合、Tenable Vulnerability Management ではそれらのインスタンスに接続することはできません。

Azure 資産の脆弱性を評価する場合、Tenable では、Frictionless Assessment を使用してクラウドの脆弱性を評価することをお勧めします。または、Nessus スキャナーまたはエージェントスキャンを実行することもできます。どちらも、ホスト上でプラグインをローカルに実行します。

目標	コネクタタイプ
Frictionless Assessment を使用して Microsoft Azure 資産を検出し、脆弱性を評価する クラウドコネクタは Azure 資産を検出し、ホスト上でプラグインをローカルで実行するのではなく、クラウド内でホストの脆弱性を評価します。 詳細については、Azure の Frictionless Assessmentを参照してください。	Frictionless Assessment
Microsoft Azure 資産の検出 クラウドコネクタは、脆弱性を評価しなくても Azure 資産を検出します。オプションで、Nessus スキャナーまたはエージェントスキャンを使用すると、検出された資産を後でスキャンできます。 Microsoft Azure コネクタを介して資産を分析する方法 1. Microsoft Azure の設定 (検出のみ) の説明に従って Azure アカウントがコ	検出コネクタ

ネクタに対応するように設定します。 2. Microsoft Azure コネクタの作成 の説明に従って Azure コネクタを作成します。	

注意： 既存の Microsoft Azure コネクタを管理するには、コネクタの管理についてTenable Vulnerability Management ユーザーガイドで参照してください。

ヒント： よくあるコネクタのエラーに関しては、Tenable 開発者ポータルのコネクタを参照してください。

Azure 用の Frictionless Assessment

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

Frictionless Assessment を使用すると、Tenable Vulnerability Management は、Azure 仮想マシン(VM)インスタンスと VM スケールセットのインスタンス上にあるデータポイントのインベントリを検出して収集します。次に、Frictionless Assessment に指定したインスタンスに関して、Tenable Vulnerability Management はホスト上でローカルにプラグインを実行するのではなく、クラウド上でホストの脆弱性を評価します。

Frictionless Assessment は、カスタムのオートメーションランブックを使用して、選択されたリソースグループの VM および VM スケールセットから必要なデータを収集します。Frictionless Assessment でホストを評価するために、Microsoft Azure 検出コネクタ、スキャナー、Tenable Nessus Agents、スキャン、またはスキャンのスケジュールを設定する必要はありません。

Azure のFrictionless Assessment ランブックは、基本的なコマンドで各 VM からデータを収集し、インストールされているパッケージや特定のファイルの存在などの情報を収集します。この情報は、Azure の Public Blob Resource API を使用して安全に Tenable に送信されます。この接続は、定期的に循環する顧客固有の共有アクセス署名 (SAS)トークンを使用して行われます。ランブックが VM から収集するデータの詳細については、Azure ランブック情報 を参照してください。

注意: Azure Frictionless Assessment によってスキャンされた仮想マシンは、情報を Azure の Public Blob Resource API にプッシュするために送信ネットワークアクセス権を必要とします。これは、「Storage」サービスタグを使用して送信セキュリティルールを追加することで実現できます。このアクセス権がない場合は、Runbook コレクションの結果が Tenable によって受信されず、資産や脆弱性が評価されません。

オペレーティングシステムのカバレッジ

Frictionless Assessment には、以下の脆弱性カバレッジがあります。

- Amazon Linux 1 / 2
- CentOS 6 / 7 / 8
- Red Hat 6 / 7 / 8

- SUSE Linux Enterprise Server (SLES) 11.4-15.2
- SUSE Linux Enterprise Desktop (SLED) 12-15.2
- Ubuntu 16.04./ 18.04 / 20.04 / 20.10
- Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022
- Windows 7、Windows 8、Windows 10、Windows 11

ライセンスの考慮事項

一般に、Tenable Vulnerability Management の資産は脆弱性が評価されるとライセンスに対してカウントされます。そのため、Frictionless Assessment によって評価されたホストは、ライセンスに対してカウントされます。詳細は、Tenable Vulnerability Management のライセンス を参照してください。

Frictionless Assessment によって評価されるホストの Azure タグを選択するときには、そのタグのいずれかを持つホストがすべてライセンスにカウントされることに注意してください。コネクタによって検出されただけで、Frictionless Assessment によって評価されないホスト (たとえば、Frictionless Assessment に選択したタグを持っていないホスト) は、ライセンスの数としてカウントされません。

制限

- Frictionless Assessment は、情報プラグインの実行、リモート脆弱性プラグインの実行、コンプライアンスデータの収集を行いません。
- Azure の Frictionless Assessment は、カスタムの暗号化ディスクをサポートしていません。
- Frictionless Assessment で設定されたコネクタは、1 つの Azure サブスクリプションだけをサポートします。複数の Azure サブスクリプションのホストを評価する場合は、サブスクリプションごとに個別のコネクタを設定する必要があります。
- ARM テンプレートのデプロイ先となる Azure サブスクリプションごとに、**Microsoft.ContainerInstance** リソースプロバイダーを登録する必要があります。
- Frictionless Assessment スキャンの制限は 1 日あたり 1 回ですが、2023 年 5 月 1 日より前に作成された既存の Frictionless Assessment コネクタは、インベントリデータをより頻繁に送信します。Frictionless Assessment では、この頻度制限を超えるデータはドロップされ、スキャンされません。

  > **注意**: この制限は、Tenable Container Security、エージェントなしの評価、および Tenable Nessus エージェントベースのインベントリスキャンには適用されません。

はじめる

1. Frictionless Assessment 用の Azure コネクタを作成する.

   > **注意:** Frictionless Assessment Azure コネクタを削除する場合は、Azure 用の Frictionless Assessment からコネクタアーティファクトを手動で削除するの説明に従って残りの Azure Artifacts を手動で削除します。

2. Frictionless Assessment Azure に使用される自動アカウントの Runbook が正常に完了したかどうかを確認します。正常に完了していない場合は、Azure 管理者またはサポート担当者に連絡して問題を解決してください。

   ランブックは、[Microsoft Azure] > **[自動化アカウント]** > **[Tenable FA 自動化アカウント]** > **[プロセスの自動化]** > **[ランブック/ジョブ]** にあります。

Frictionless Assessment 用の Azure コネクタを作成する

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

Frictionless Assessment 用に Azure クラウドコネクタを設定するときに、Tenable Vulnerability Management は Azure Resource Manager (ARM) テンプレートを使用します。ARM は、Azure のリソースグループまたはサブスクリプション内にあるリソースを整理、更新、プロビジョニングするための Azure の方法です。これを使用すると、ユーザーはアプリケーションまたはユースケースのリソース、依存関係、およびネットワークを定義できます。

Tenable Vulnerability Management で Microsoft Azure Frictionless Assessment コネクタを作成するには、次の手順に従います。このプロセスでは、Frictionless Assessment で評価する各 Azure サブスクリプションにデプロイする必要がある ARM テンプレートも作成します。

始める前に

- Tenable Vulnerability Management へのアクセスに使用している同じブラウザの別のウィンドウまたはタブで、Frictionless Assessment でターゲットにする Azure アカウントを使用して Azure コンソールにログインします。

注意: Tenable Cloud Security プレビューまたは Tenable Cloud Security を使用するには、Tenable Cloud Security をサポートする新しいロールを更新または作成する必要があります。Tenable Vulnerability Management クラウドコネクタロールでは、Agentless Assessment をサポートしていません。

Microsoft Azure Frictionless Assessment コネクタと ARM テンプレートを作成します。

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. **[クラウドコネクタの作成]** をクリックします。

   [クラウドコネクタの選択] パネルが表示されます。

Select a Cloud Connector

Import data from various sources to further enrich Tenable.io

Search

CLOUD CONNECTORS

AWS - Keyed setup

AWS - Keyless setup

Microsoft Azure

Microsoft Azure Frictionless Assessment

Google Cloud Platform

CONTAINER SECURITY

Container Security Scanner

Docker

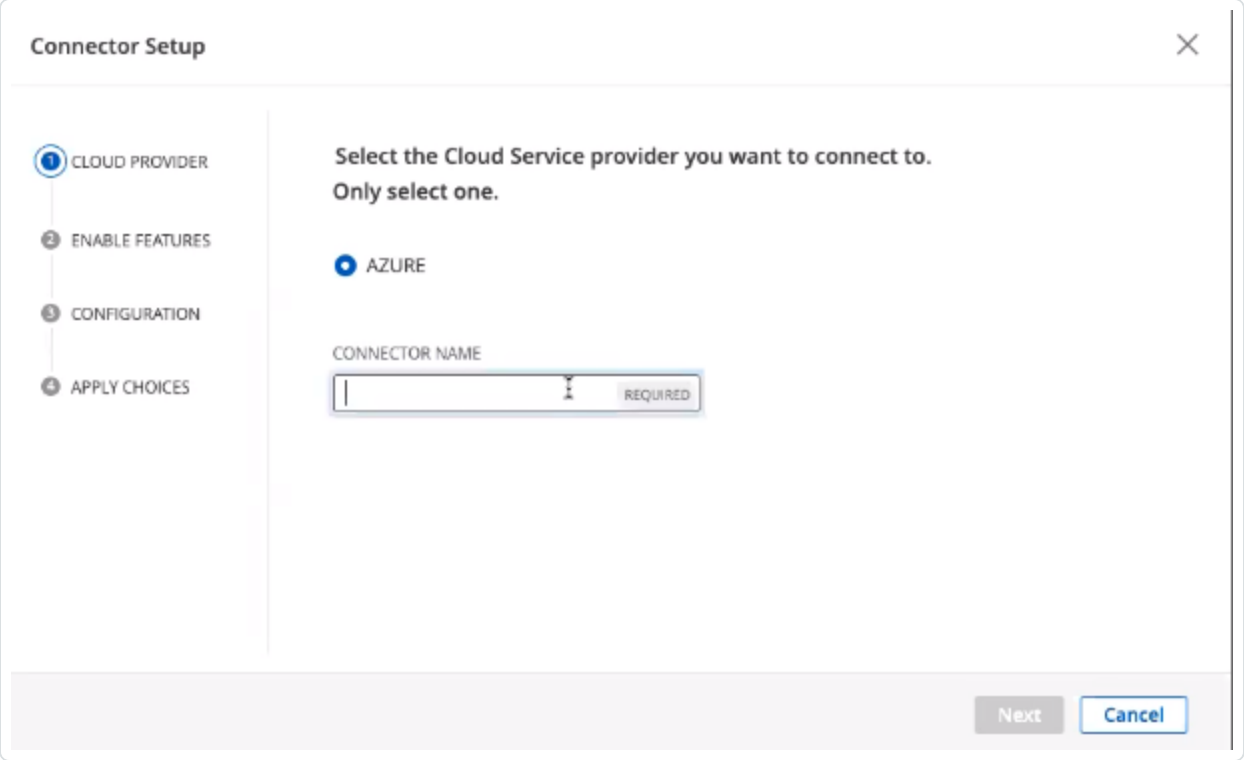
Docker EE

AWS Elastic Container Registry

JFrog Artifactory

5. **[クラウドコネクタ]** リストで、**[Microsoft Azure 用の Frictionless Assessment]** を選択します。

   [コネクタのセットアップ] ポップアップが表示されます。



6. **[クラウドプロバイダー]** の手順で、**コネクタ名** を入力します。

   [次へ] をクリックします。

7. **[機能の有効化]** の手順で、**[Frictionless Assessment を使用して脆弱性を特定する]** チェックボックスがオンになっていることを確認します。

   [次へ] をクリックします。

8. **[設定]** の手順で、**[すべてスキャン]** チェックボックスをオンにするか、特定の対象パラメーターを選択します。

   注意: より具体的なリソースのサブセットを対象にするには、特定のリソースグループ、特定のタグキー、特定のタグ値、またはこれら 3 つをすべて組み合わせてコネクタを対象にすることができます。

   注意: ドロップダウンの **ANY** 入力をワイルドカードとして使用して、リソースグループ、タグキー、またはタグ値のすべての値を対象にします。

> **注意:** 特定のパラメーターを持つ複数の対象を選択できます。

[次へ] をクリックします。

9. **[選択を適用]** の手順で、**[ダウンロードして終了]** をクリックします。

   新しい ARM テンプレートが .json 形式でダウンロードされ、新しいコネクタが **[クラウドコネクタ]** ページに表示されます。

ARM テンプレートを使用してコネクタをデプロイする

前のセクションでダウンロードした ARM テンプレートを Azure サブスクリプションにデプロイします。

デプロイメントのガイダンスについては、Microsoft Azure のドキュメントを参照してください。

> **注意:** ARM テンプレートのデプロイ先となる Azure サブスクリプションごとに、**Microsoft.ContainerInstance** リソースプロバイダーを登録する必要があります。

> **注意:** Azure CLI を介して Azure 用の Frictionless Assessment をデプロイする場合は、上記の手順で作成された ARM テンプレートを使用してサブスクリプションをデプロイしてください。
>
> 例
>
> ```
> az deployment sub create --location eastus --template-file /path/to/arm-template.json
> ```
>
> コマンドに --debug を追加すると、デプロイ中に詳細ログを生成できます。
>
> ```
> az deployment sub create --location eastus --template-file /path/to/arm-template.json --debug
> ```

Azure 用の Frictionless Assessment からコネクタアーティファクトを手動で削除する

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

始める前に

- コネクタを削除するの説明に従って、Azure 用の Frictionless Assessment コネクタを削除します。

Azure ポータルで以下の Azure 用の Frictionless Assessment アーティファクトを削除します。

- カスタムロール定義に関連する Automation アカウントのロール割り当て(例: **Tenable-FA-Automation-Account**)
- カスタムロール定義 (例: **Tenable FA ロール(サブスクリプション: [UUID] | コネクタ: [UUID])**)
- Frictionless Assessment リソースグループ(例: **TenableFA-Connector- {UUID}**)

  注意: Azure クライアントに **Contributor** 以上のアクセス許可がある場合は、以下のコマンドを使用してリソースグループを Azure CLI から削除することもできます。

  ```
  az group list --tag Tenable=AzureFa --query "[].name" -o tsv | xargs -ot az group delete --no-wait -n
  ```

記載されている Azure Artifacts の詳細については、Microsoft Azure のドキュメントを参照してください。

Azure ランブック情報

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

Frictionless Assessment は、カスタムのオートメーションランブックを使用して、選択したリソースグループの VM および VM スケールセットから以下のデータを収集します。

ARM テンプレートのデプロイの数分後に、いくつかの中間リソースが表示されます。これらのリソースは、次のリソースをデプロイするために Tenable Vulnerability Management が使用するデプロイメントスクリプトです。Tenable Vulnerability Management は、デプロイメントが完了すると、スクリプトを削除します。

- リソースグループ:
    - 名前: `Tenable-FA-Connector` で始まります
    - Azure Frictionless Assessment リソースを含みます。
- 自動化アカウント:
    - 名前: `Tenable-FA-Automation-Account` で始まります
- ランブック:
    - 名前: `TenableFATerminateInstances`
    - 説明: 終了したインスタンスの Tenable Frictionless Assessment ランブック。
    - 名前: `TenableFACollector`
    - 説明: Tenable Frictionless Assessment コレクションランブック
- ストレージアカウント:
    - 名前: スクリプトで始まります。
    - 説明: 資産に対して実行する shell/powershell スクリプト化チェックが含まれています。

- ロールの定義:
  - 名前: `Tenable FA Role` または `Tenable-FA-Custom-Role-Def` で始まります。
  - 説明: ランブックが資産をスキャンできるようにするために必要なロール
  - アクション:

```
"Microsoft.ClassicCompute/operatingSystems/read",
"Microsoft.ClassicCompute/operatingSystemFamilies/read",
"Microsoft.ClassicCompute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachines/runCommand/action",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/runCommand/action"
```

Microsoft Azure の設定 (検出のみ)

Tenable Vulnerability Management Azure コネクタを使用する前に、Microsoft Azure でいくつかの手順を実行する必要があります。

> **注意:** お使いの Azure デプロイメントが、Azure China または Azure Government リージョンの Azure インスタンスを含む場合、Tenable Vulnerability Management ではそれらのインスタンスに接続することはできません。

Microsoft Azure を設定する方法

1. Azure アプリケーションがまだない場合、Azure アプリケーションの作成をします。

   > **注意:** Azure アプリケーション ID とクライアントシークレットはこの手順の中で入手します。

2. Azure テナント ID (ディレクトリ ID) を入手します。
3. Azure サブスクリプション ID を入手します。
4. Azure アプリケーションの閲覧者ロールのアクセス許可を付与します。
5. (オプション) Azure アプリケーションに追加の Azure サブスクリプションをリンクします。

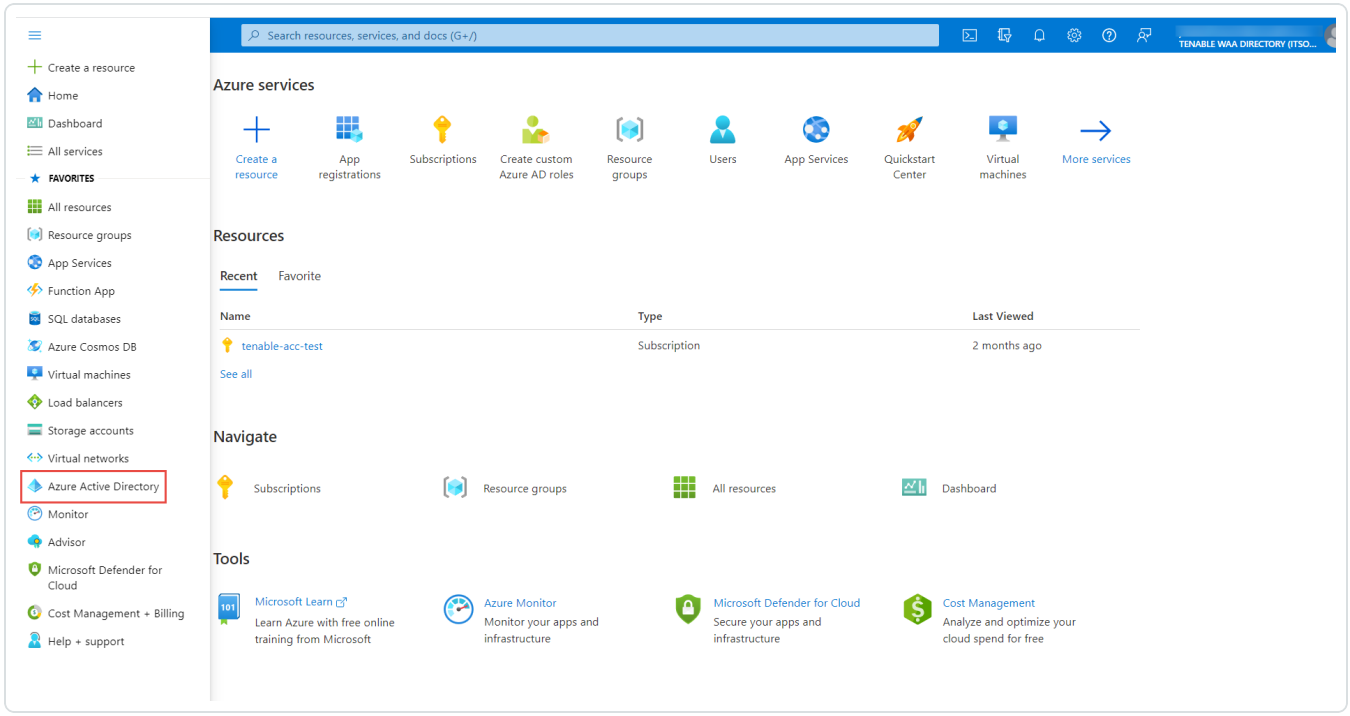
次の手順

- Azure コネクタを作成します。

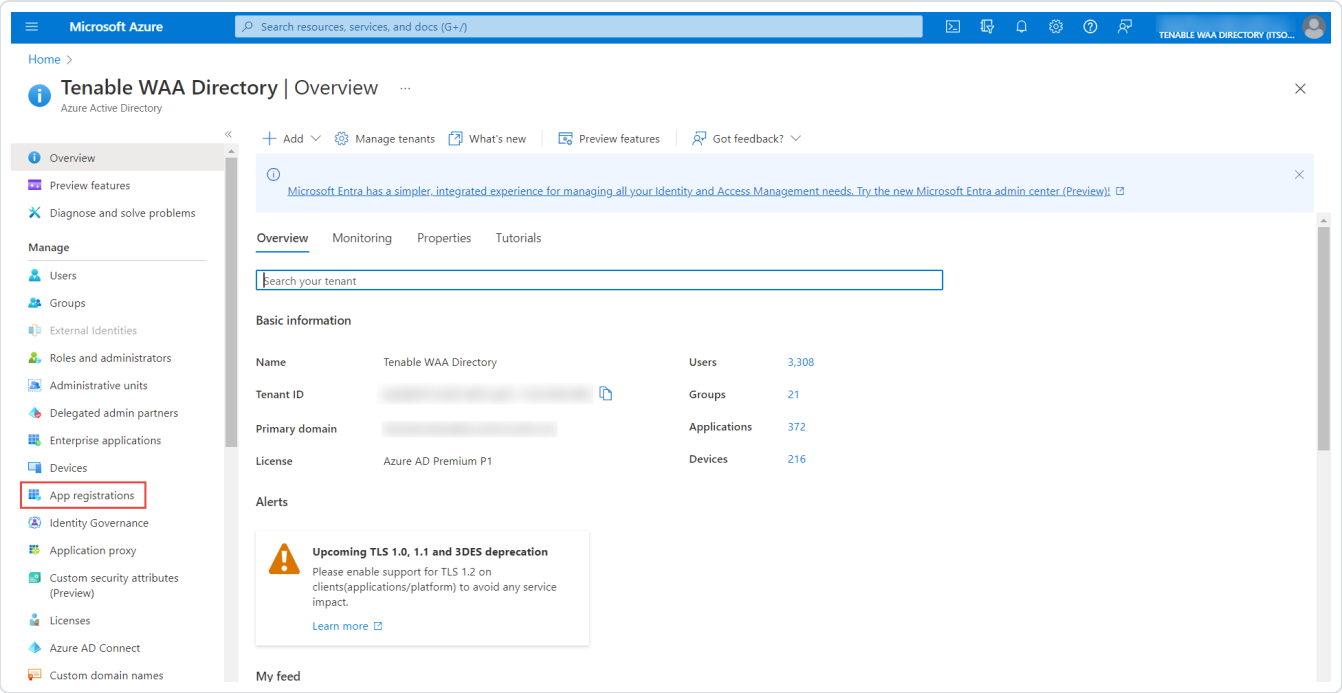
Azure アプリケーションを作成する

Azure Tenable Vulnerability Managementコネクタ用の Azure アプリケーションを作成する方法

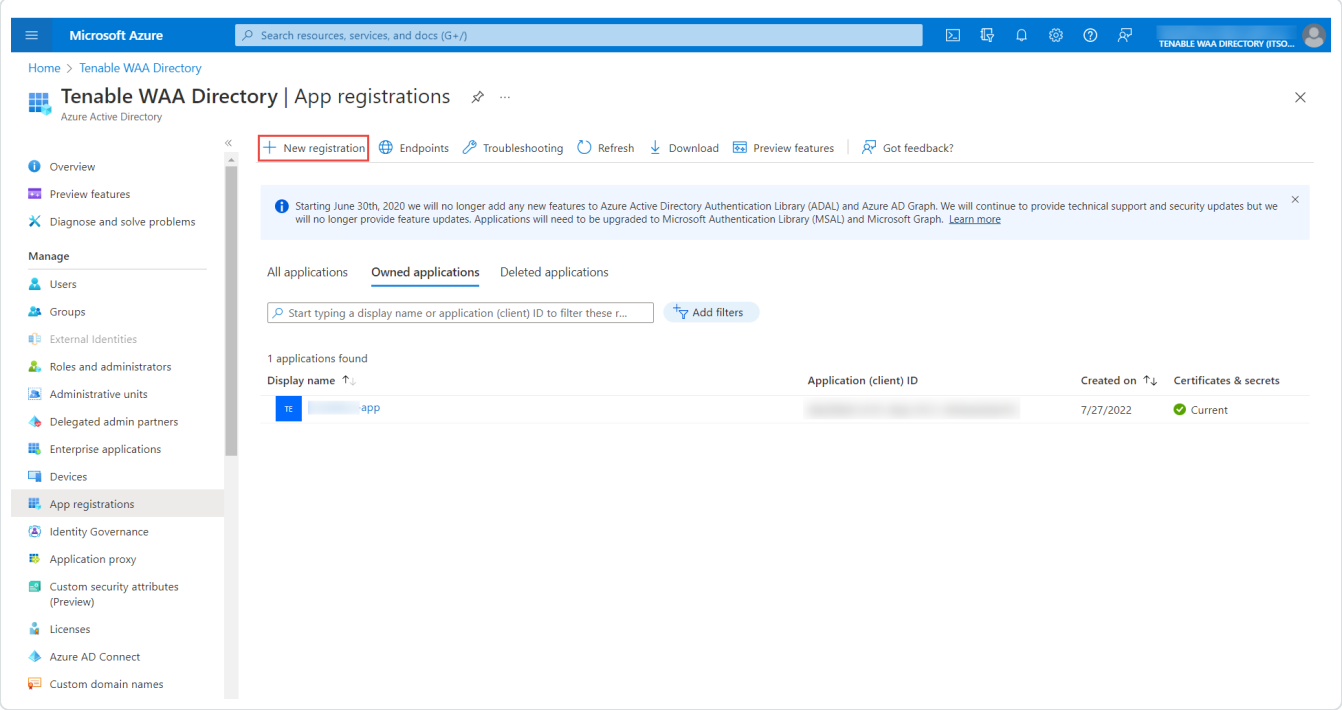
1. Microsoft Azure ポータルにログインします。
2. 左側のメニューで、**[Microsoft Entra ID]** をクリックします



3. **[App 登録]** をクリックします。



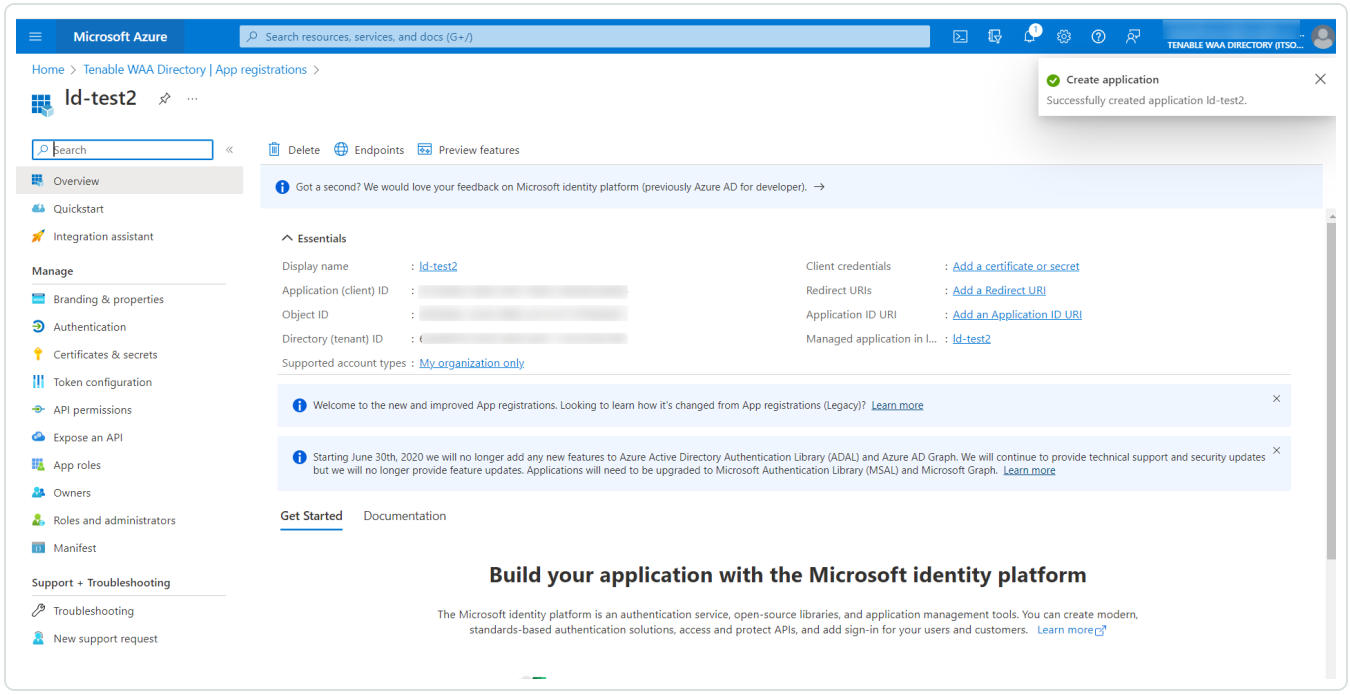
4. 新しいアプリケーションを追加するには、**[新規登録]** をクリックします。



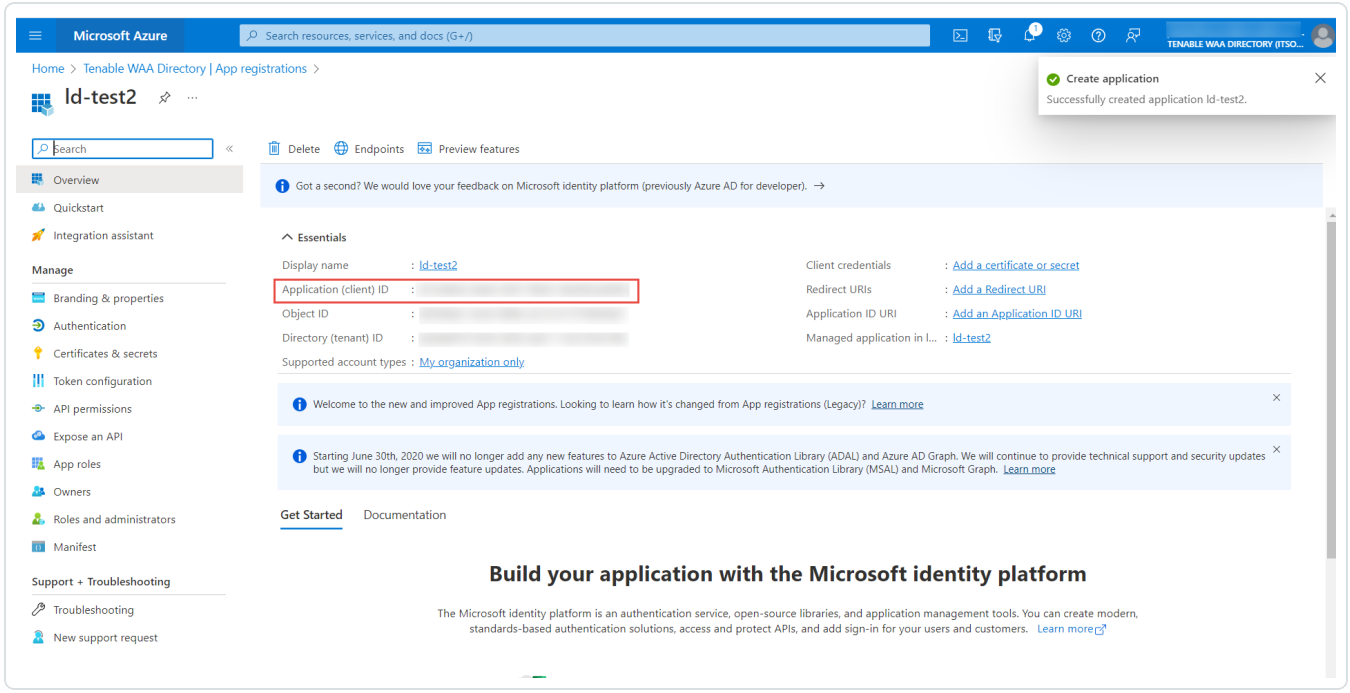
5. **[名前]** ボックスに、アプリケーションのわかりやすい名前を入力します。

6. **[サポートされているアカウントタイプ]** セクションで、3 つのオプションのいずれかを選択して、API にアクセスできるアカウントのタイプを指定します。
7. (オプション) **[リダイレクト URI]** セクションで、ドロップダウンから **[ウェブ]** または **[パブリッククライアント (モバイル & デスクトップ)]** を選択し、テキストボックスに URI を入力します。
8. **[登録]** をクリックして設定を確定し、アプリケーションを作成します。

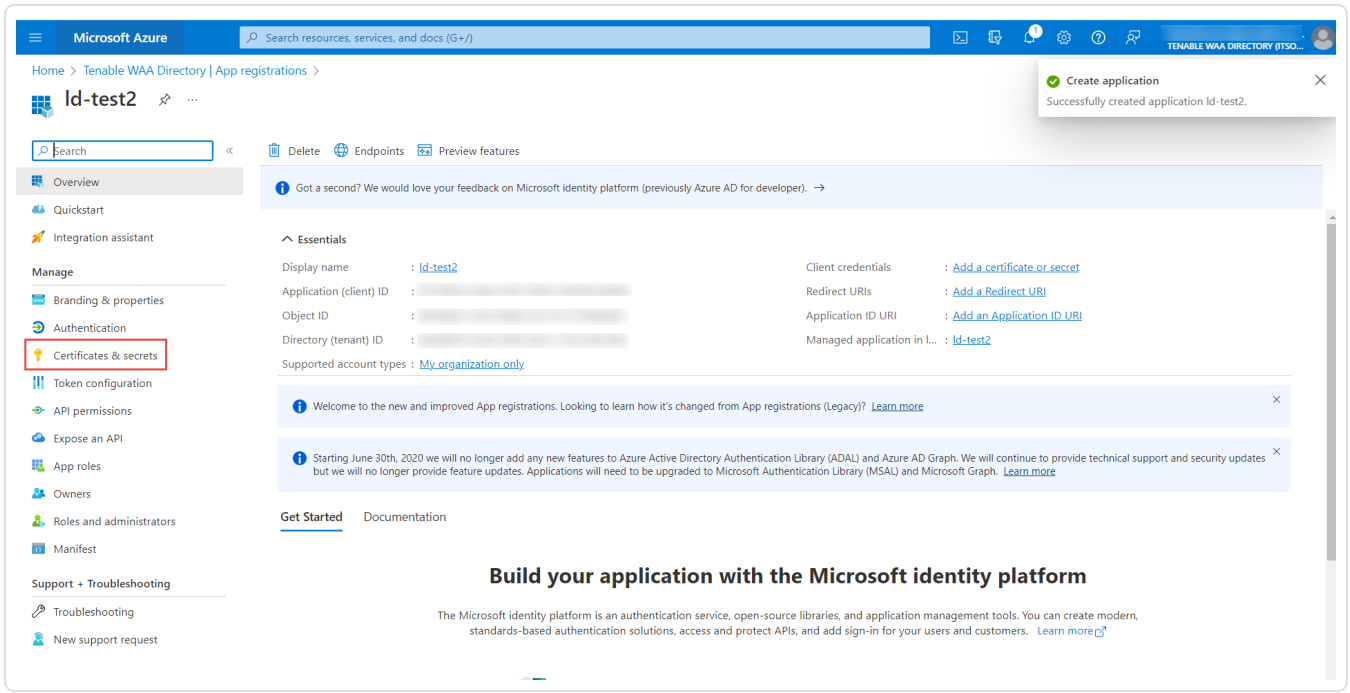
   新しいアプリケーションが作成されたことを示す成功メッセージがページの上部に表示され、ページがアプリケーションの **[概要]** ページにリダイレクトされます。



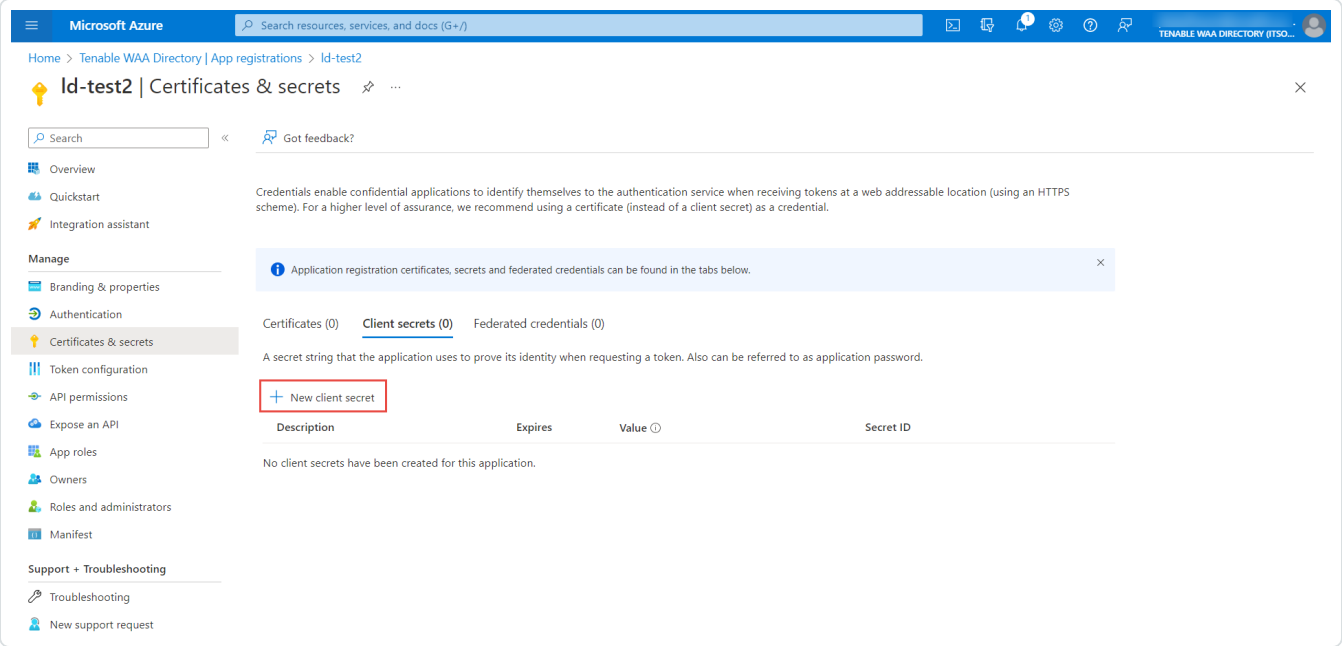
9. **Application (client) ID** をコピーします。この情報は、Tenable Vulnerability Management でコネクタを設定する際に使用されます。



10. アプリケーションの **[管理]** セクションで、**[証明書 & シークレット]** をクリックします。

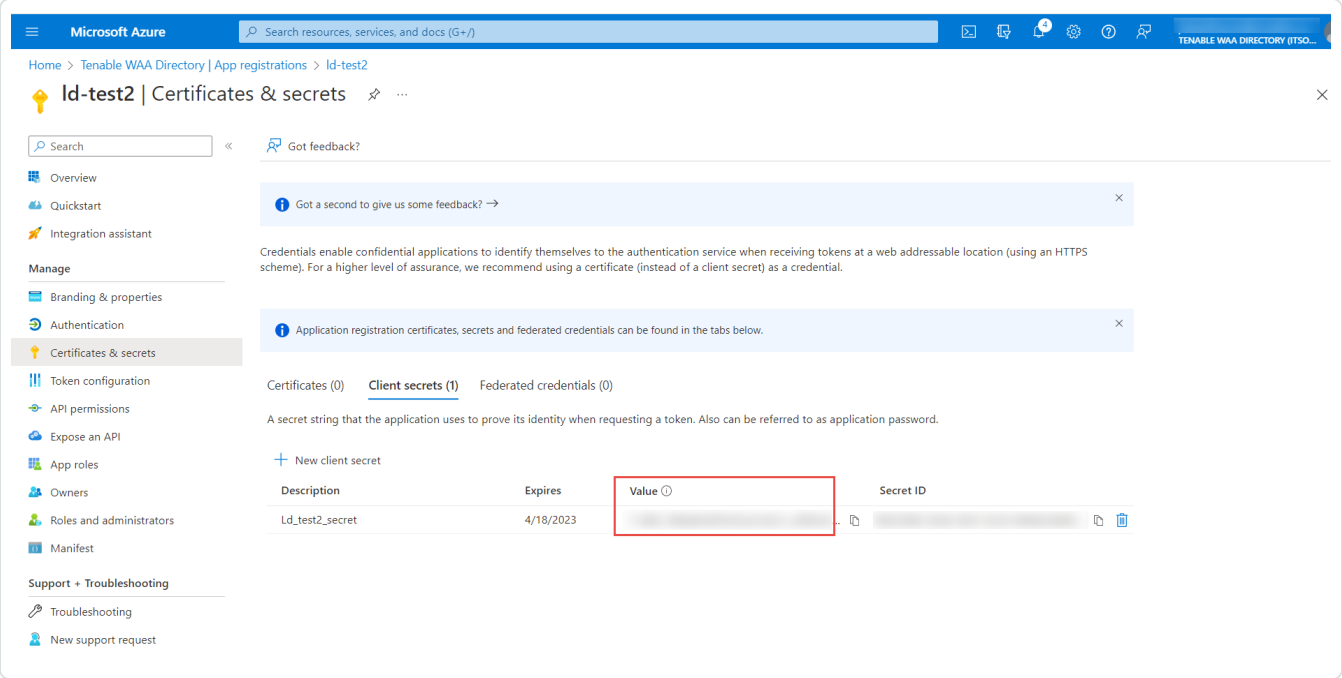


11. **[クライアントシークレット]** セクションで、**[+新しいクライアントシークレット]** をクリックします。



12. **[説明]** ボックスに、クライアントシークレットの説明を入力します。
13. **[有効期限]** オプションで、有効期限を選択します。
14. **[追加]** ボタンをクリックします。

    新しいクライアントシークレットが追加されます。
15. クライアントシークレットの値をコピーまたは書き留めます。



後で Tenable Vulnerability Management を使用してコネクタを設定するには、このクライアントシークレットが必要になります。

次の手順

- Azure テナント ID (ディレクトリ ID) を入手する

Azure テナント ID (ディレクトリ ID) を入手

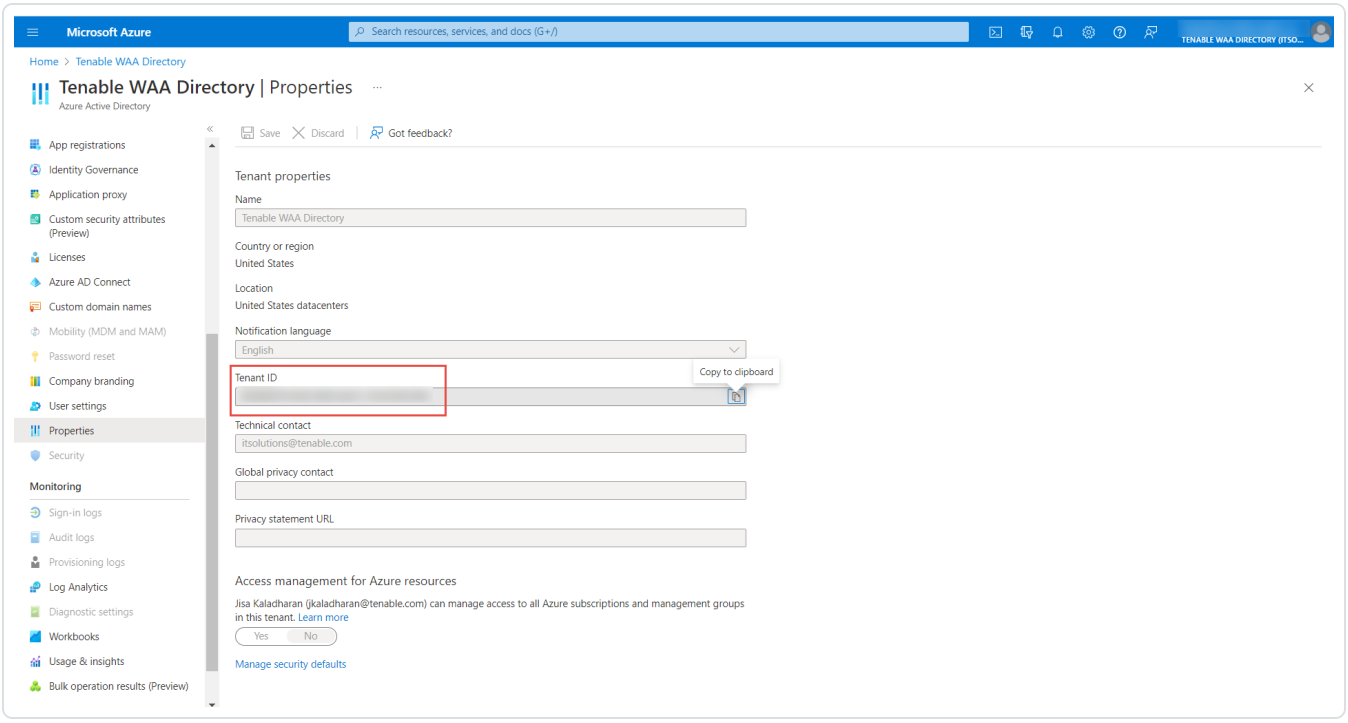
Azure Tenable Vulnerability Managementコネクタのためのテナント ID を取得する方法

1. Microsoft Azure ポータルにログインします。
2. 左側のメニューで、**[Microsoft Entra ID]** をクリックします。

   [ディレクトリの概要] ページが表示されます。
3. **[管理]** セクションで、**[プロパティ]** をクリックします。

   [ディレクトリプロパティ] ページが表示されます。
4. **Directory ID** をコピーします。

   > **注意：**テナント ID とディレクトリ ID は同じです。



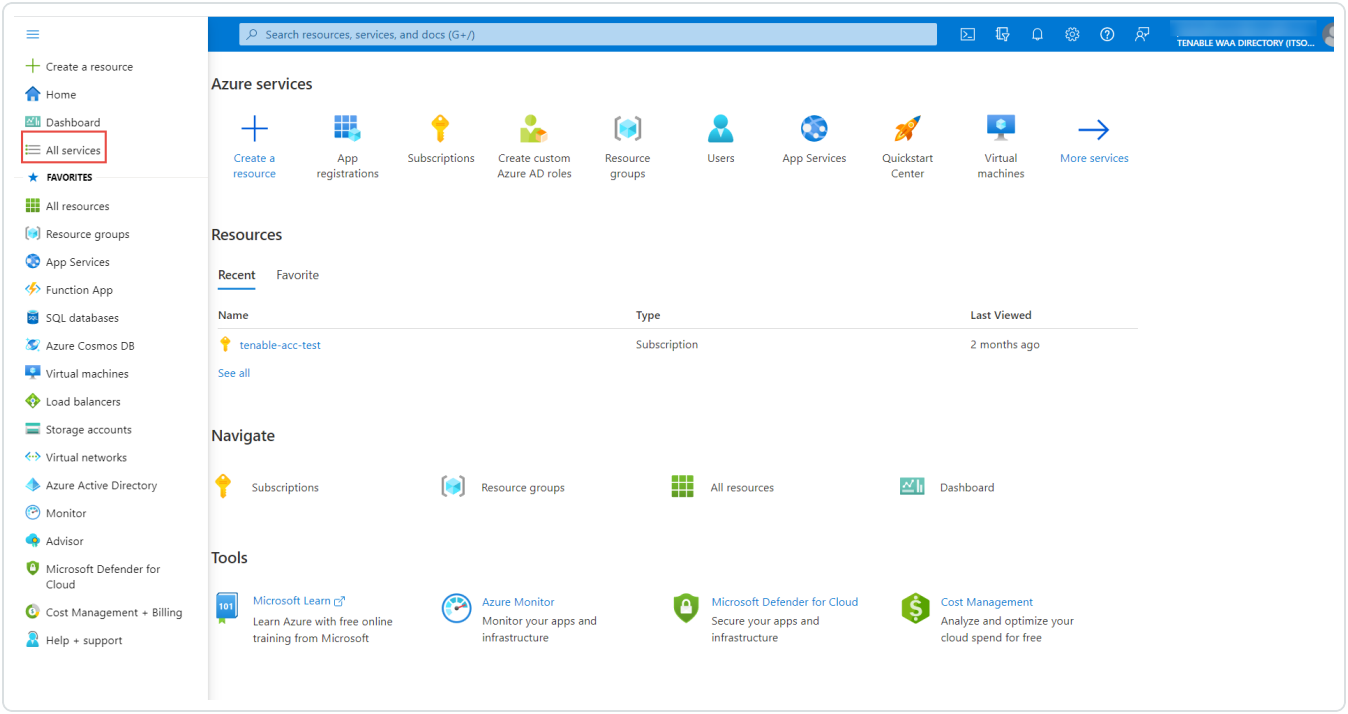
次の手順

- Azure サブスクリプション ID を入手します。

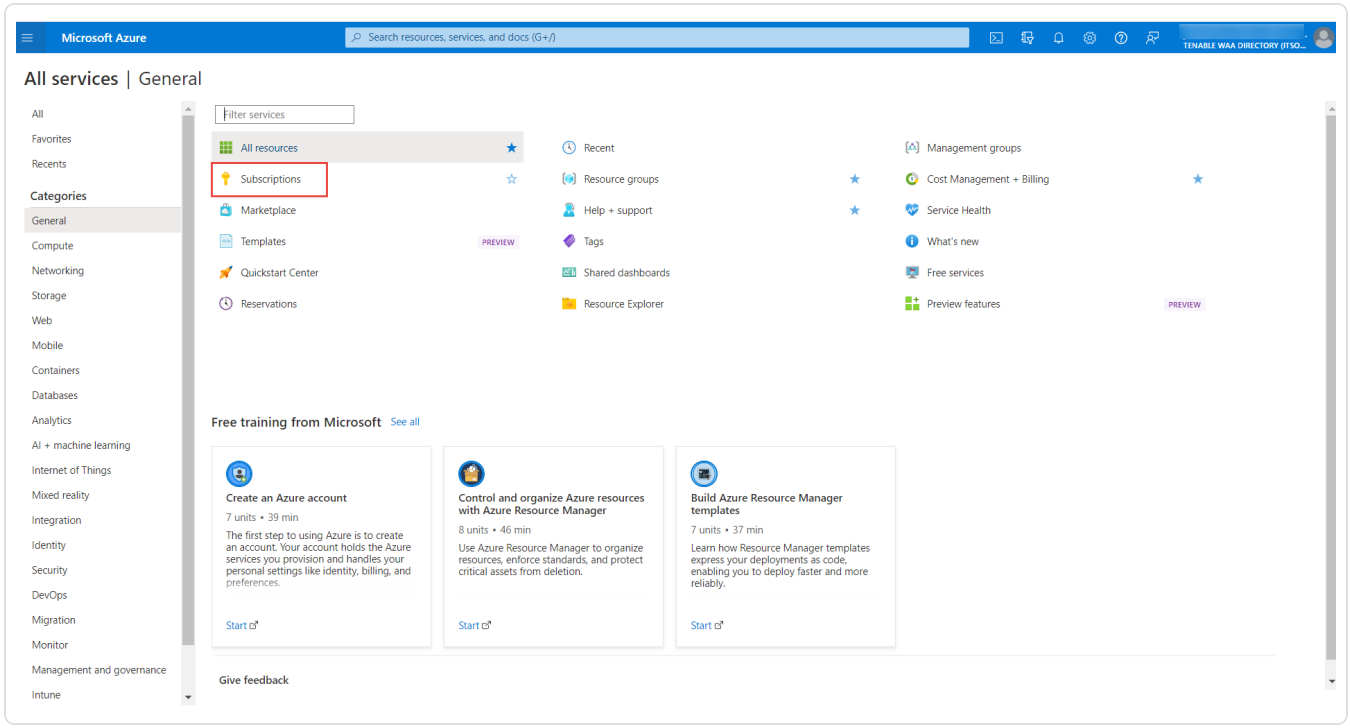
Azure サブスクリプション ID を取得

Azure Tenable Vulnerability Managementコネクタのためのサブスクリプション ID を取得する方法

1. Microsoft Azure ポータルにログインします。
2. 左側のメニューで、**[すべてのサービス]** をクリックします。



3. **[一般]** セクションで、**[サブスクリプション]** をクリックします。



4. 該当するサブスクリプションの**サブスクリプション ID** をコピーします。

次の手順

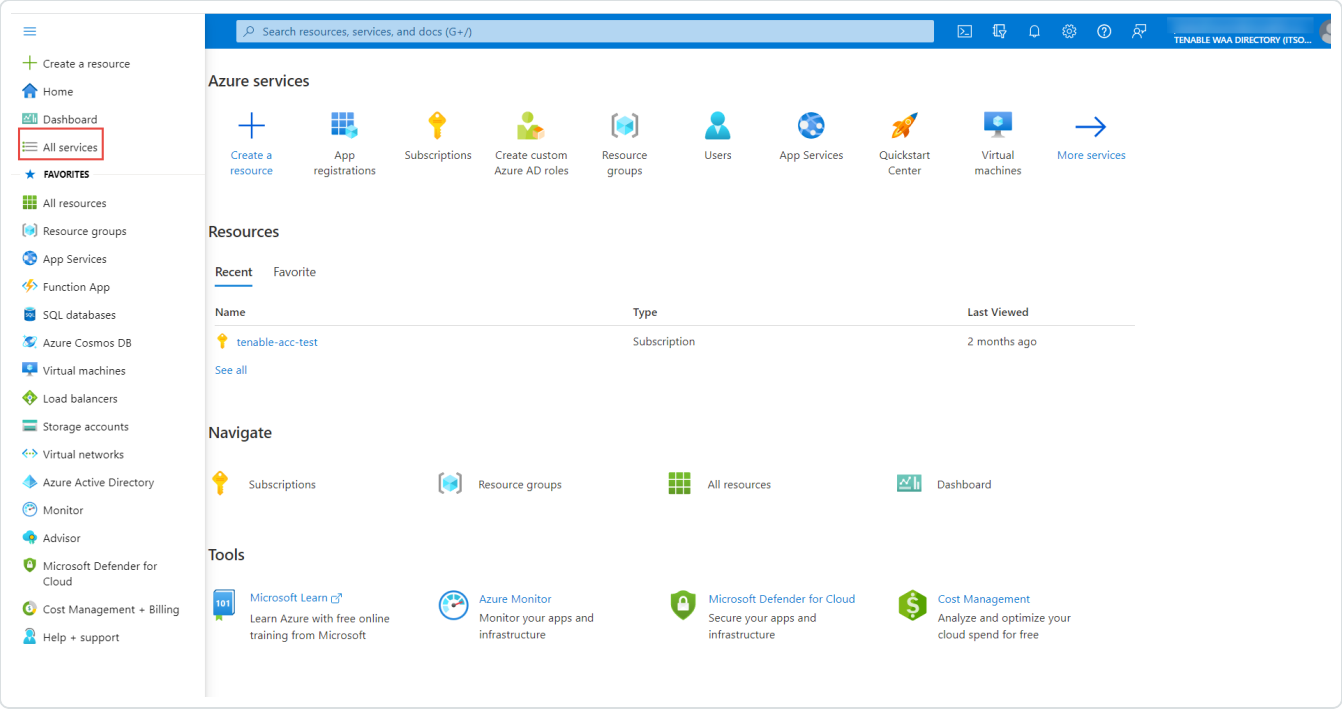
- Azure アプリケーションのリーダーロールのアクセス許可を付与します。

Azure アプリケーションのリーダーロールのアクセス許可を付与する

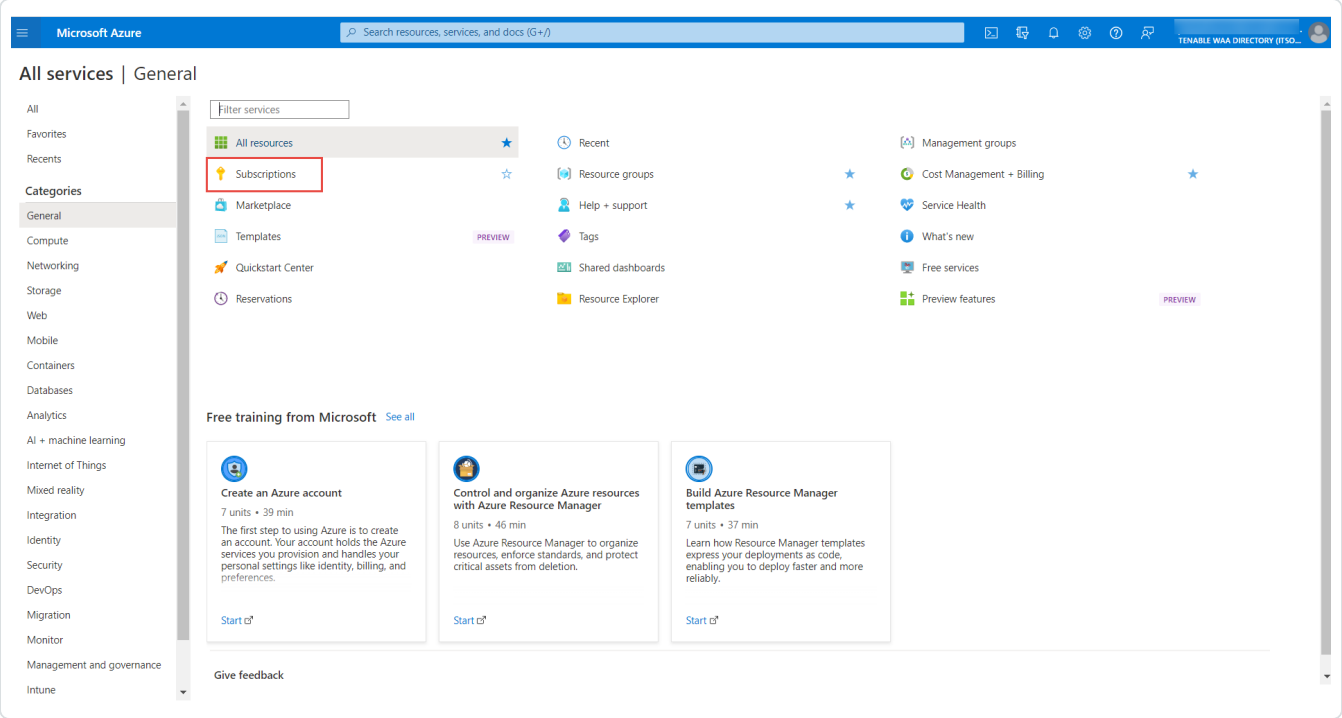
Azure Tenable Vulnerability Managementコネクタのための Azure アプリケーションのリーダーロールのアクセス許可を付与する方法

注意: 詳細については、Microsoft Azure のドキュメントを参照してください。RBAC と Azure ポータルを使用して Azure リソースへのアクセスを管理します。

1. Microsoft Azure ポータルにログインします。
2. 左側のメニューで、**[すべてのサービス]** をクリックします。



3. **[一般]** セクションで、**[サブスクリプション]** をクリックします。



4. サブスクリプションの表で、該当するサブスクリプションをクリックします。

   サブスクリプションの **[概要]** ページが表示されます。

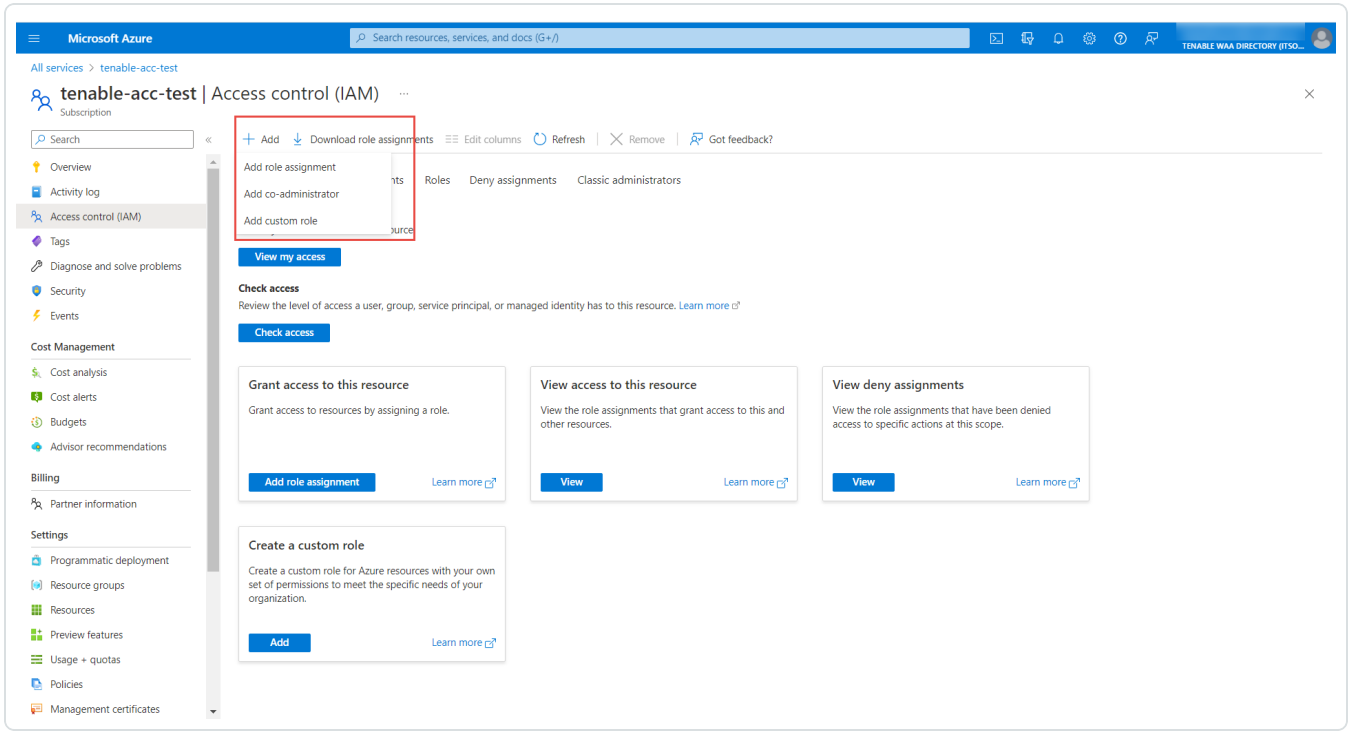
5. サブスクリプションのメニューで、**[アクセス制御 (IAM)]** をクリックします。

   [アクセス制御 (IAM)] ページが表示されます。

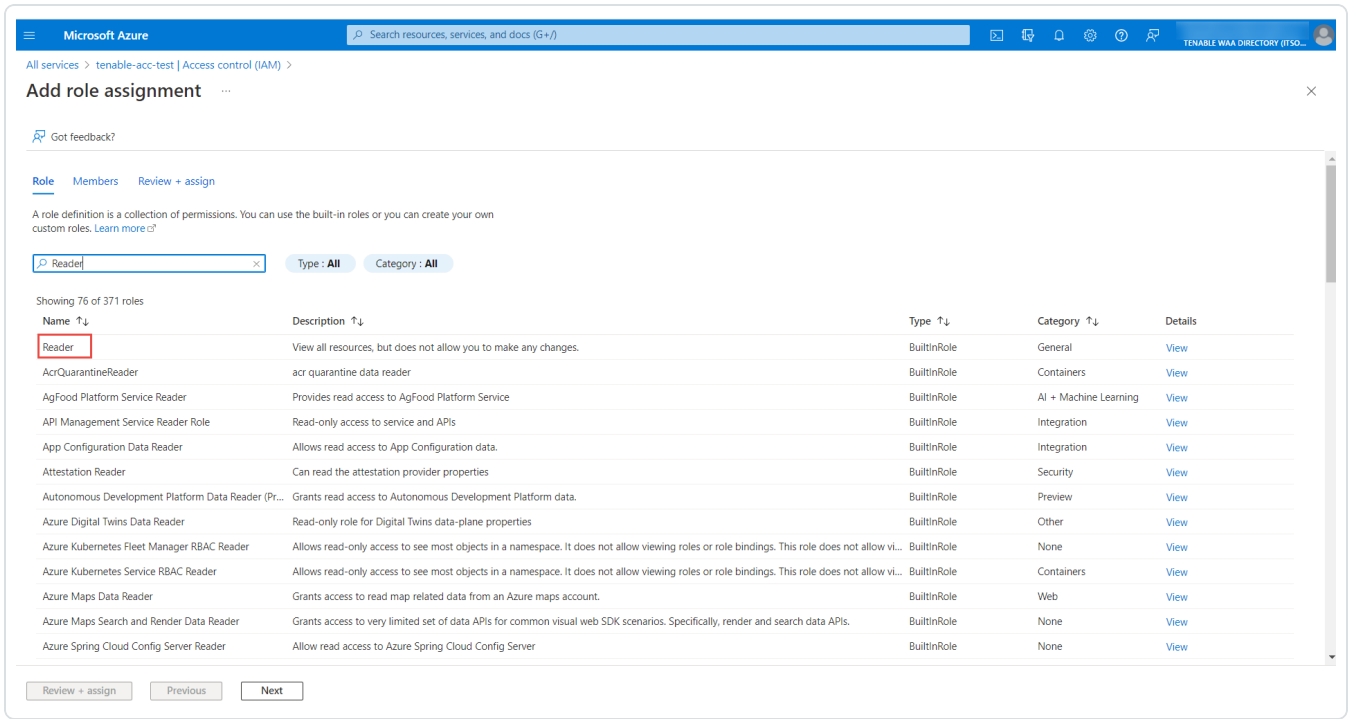
6. **[+ 追加]** ボタンをクリックします。

   ポップアップメニューが表示されます。

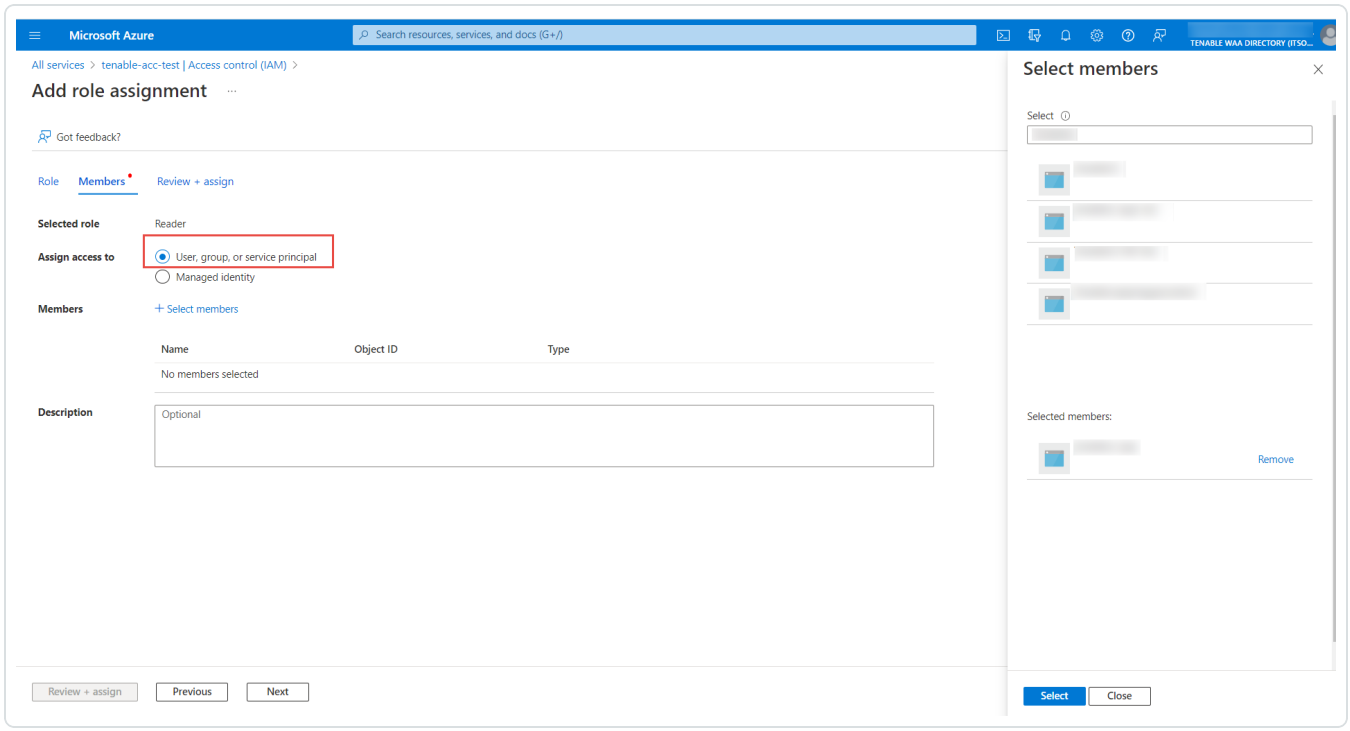
7. **[ロールの割り当てを追加]** をクリックします。



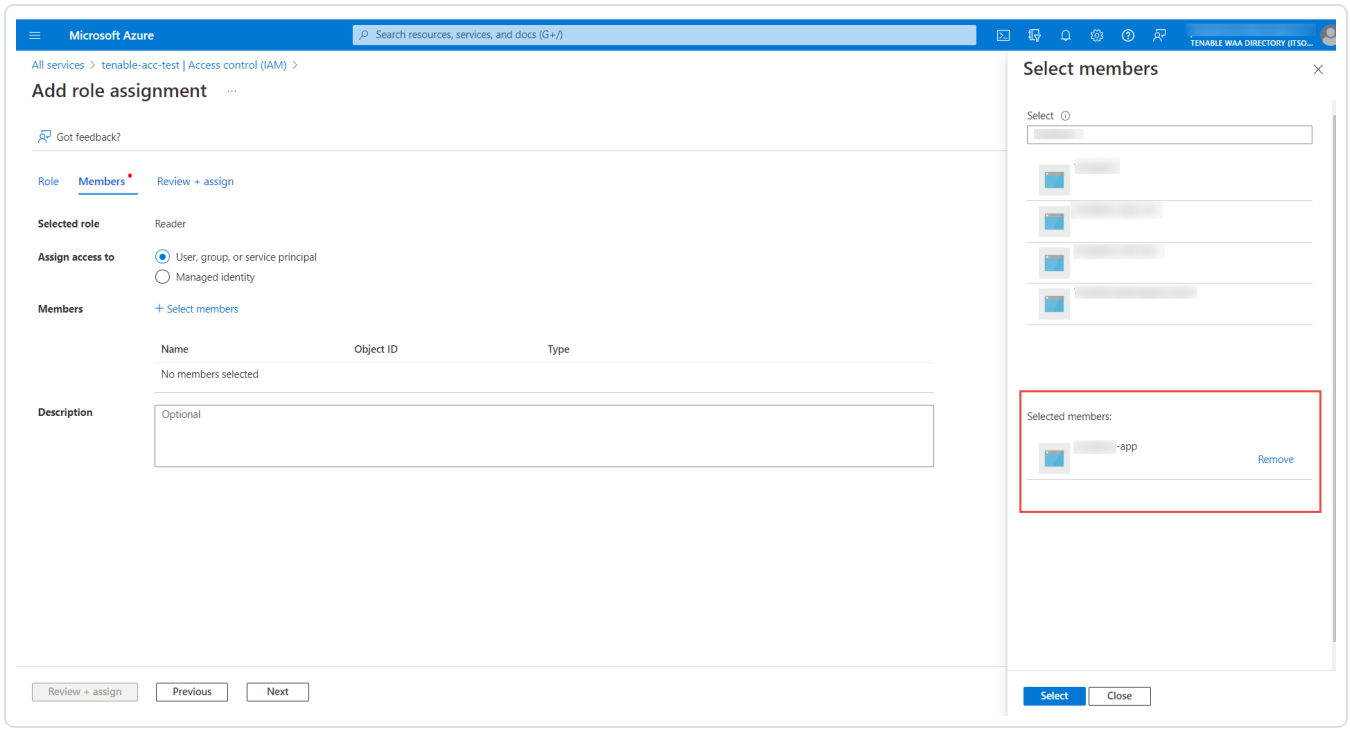
8. **[ロールの割り当てを追加]** ウィンドウの **[ロール]** タブで、**[リーダー]** を検索して選択します。



9. **[メンバー]** タブの **[アクセス権の割り当て]** セクションで、**[ユーザー、グループ、サービスプリンシパル]** を選択します。

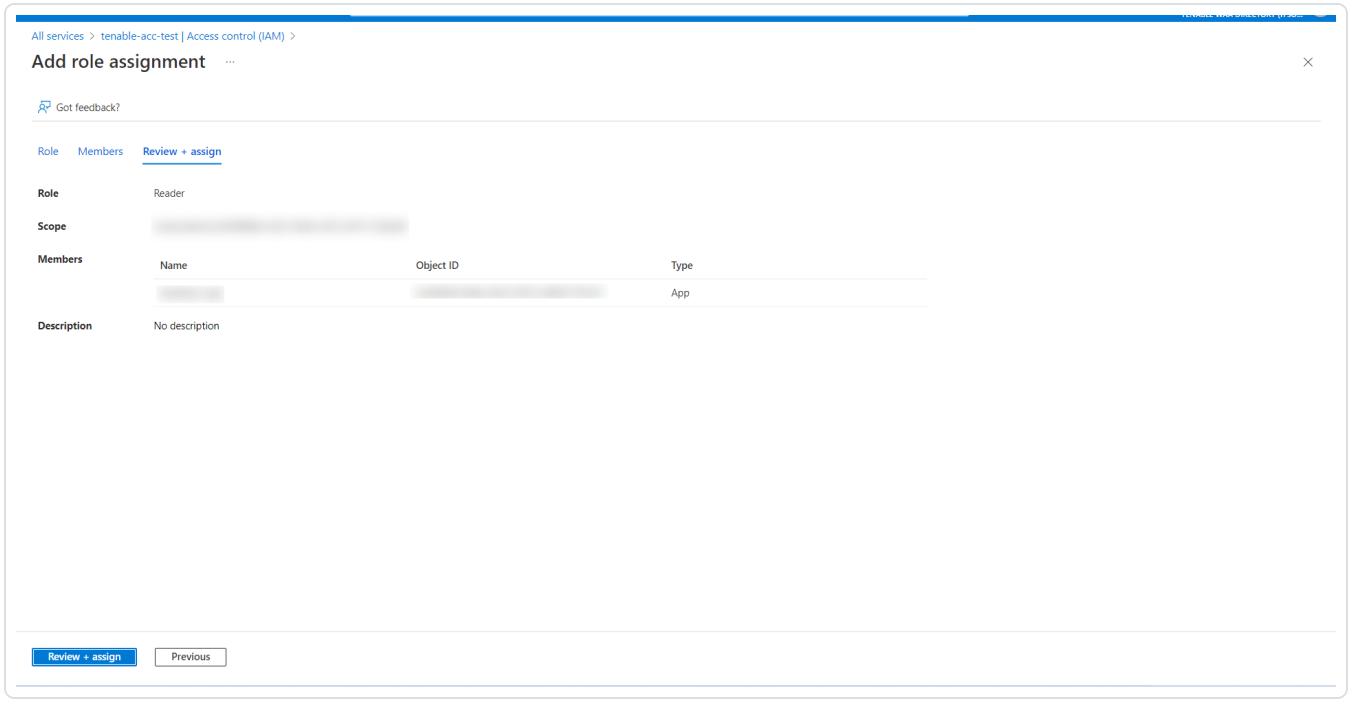


10. Azure アプリケーションを選択するには、**[+ メンバーを選択]** をクリックします。



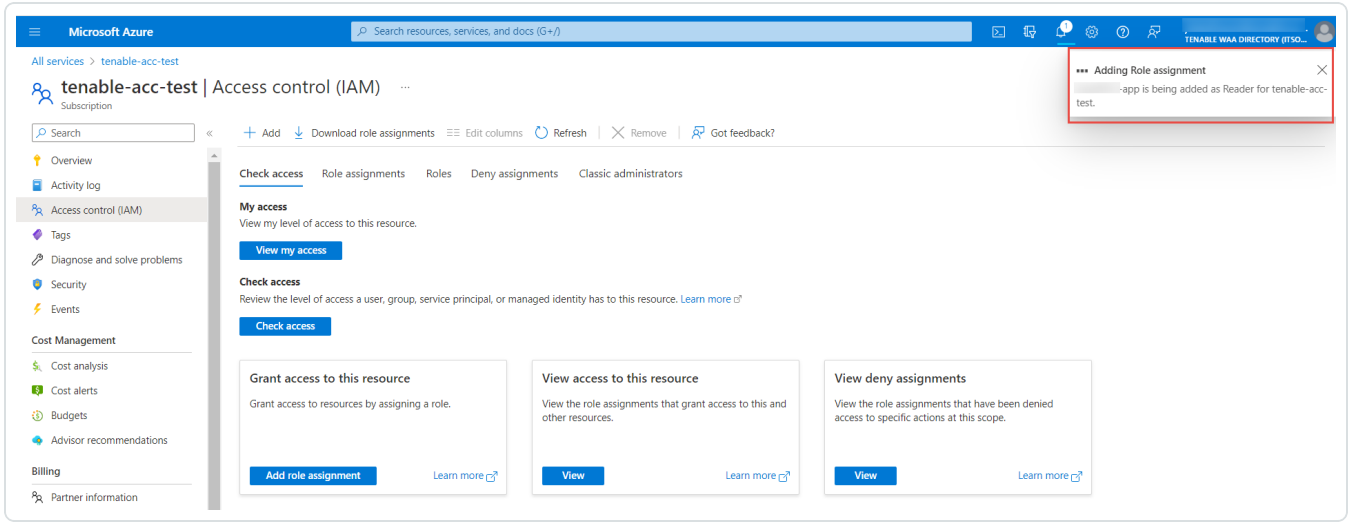
[メンバーを選択] プレーンが表示されます。

11. Azure アプリケーションを検索し、リストから必要なアプリケーションを選択します。
12. **[確認 + 割り当て]** タブで、選択したロールとメンバーを確認します。



13. **[確認 + 割り当て]** をクリックします。

選択したアプリケーションが、サブスクリプションの**リーダー**として追加されます。



次の手順

次のいずれかを行います。

- (オプション) Azure アプリケーションに追加の Azure サブスクリプションをリンクします。
- Azure コネクタを作成します。

Azure サブスクリプションをリンクする

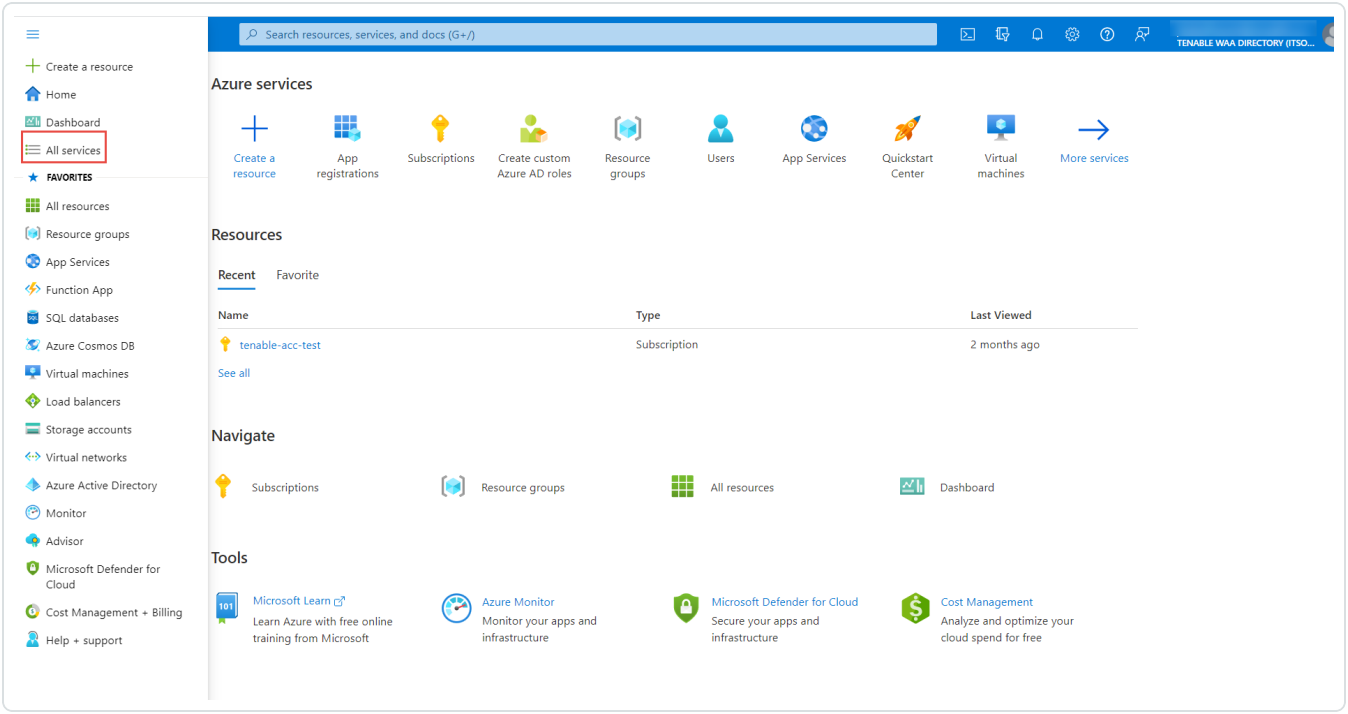
始める前に

- プライマリ Azure サブスクリプション向けに作成したアプリケーション名を記録します。

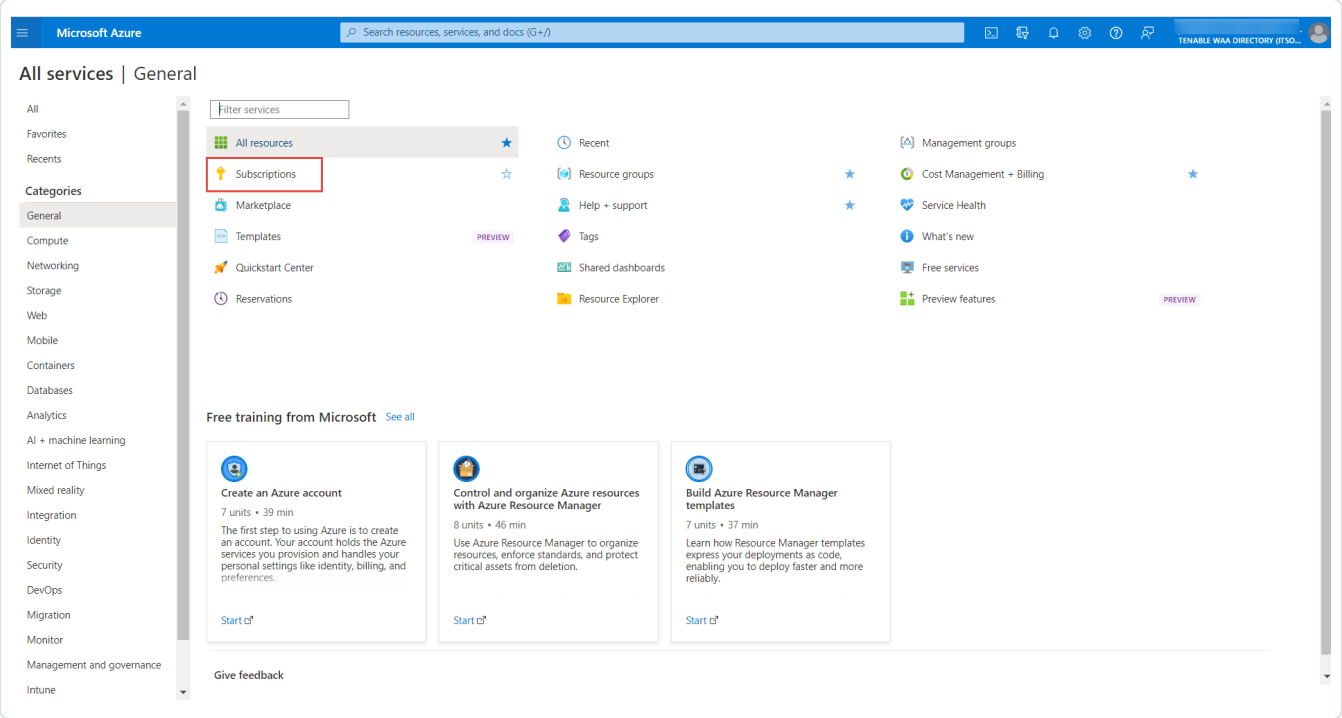
リンクされた Azure サブスクリプションを設定する方法

プライマリ Azure サブスクリプション向けに作成したアプリケーションに対し、セカンダリサブスクリプションリーダーロールのアクセス許可を付与します。

1. Microsoft Azure ポータルにログインします。
2. 左側のメニューで、**[すべてのサービス]** をクリックします。



3. **[一般]** セクションで、**[サブスクリプション]** をクリックします。



4. サブスクリプションの表で、該当するサブスクリプションをクリックします。

   サブスクリプションの **[概要]** ページが表示されます。

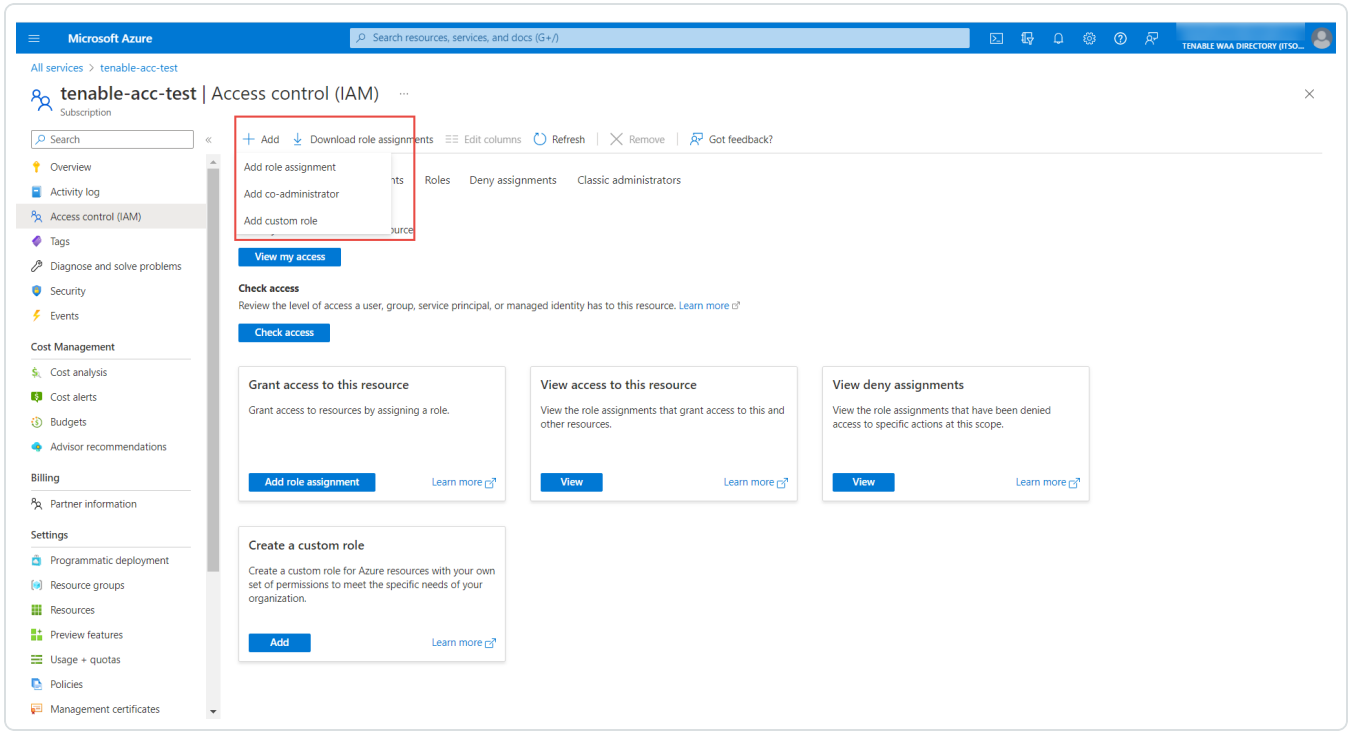
5. サブスクリプションのメニューで、**[アクセス制御 (IAM)]** をクリックします。

   [アクセス制御 (IAM)] ページが表示されます。

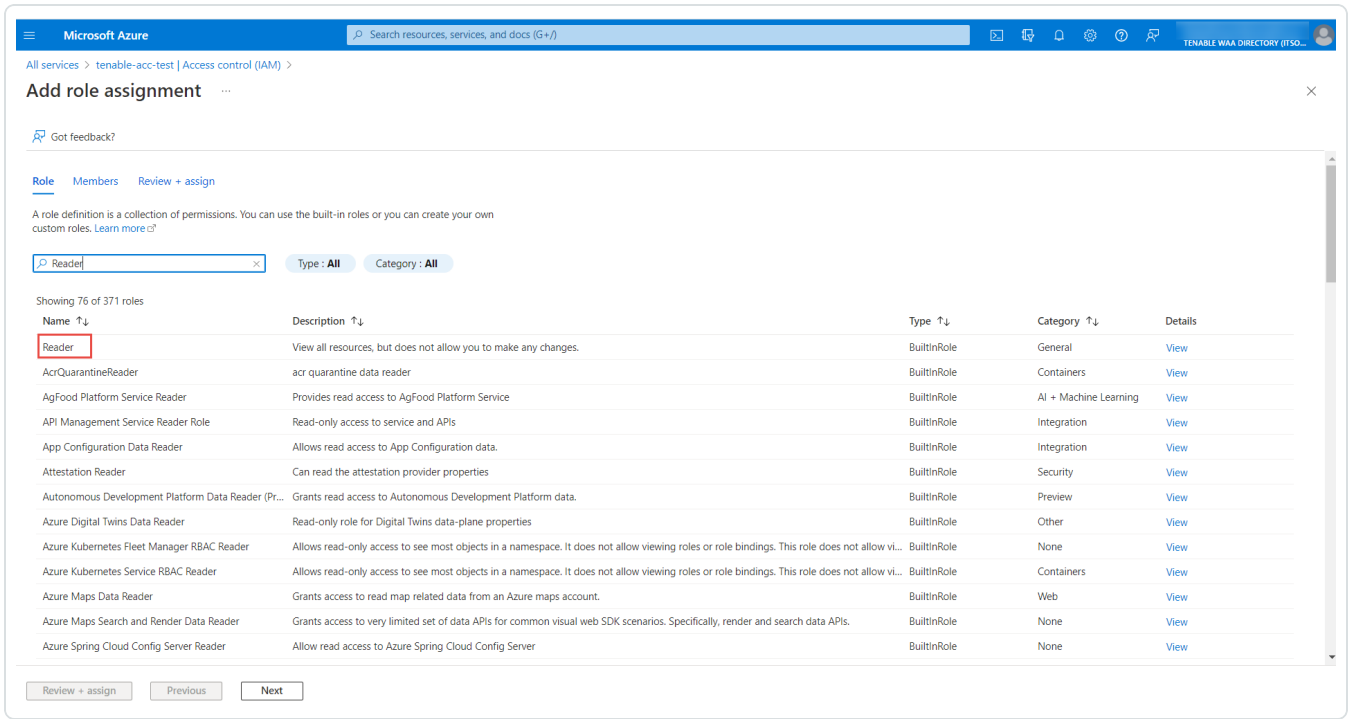
6. **[+ 追加]** ボタンをクリックします。

   ポップアップメニューが表示されます。

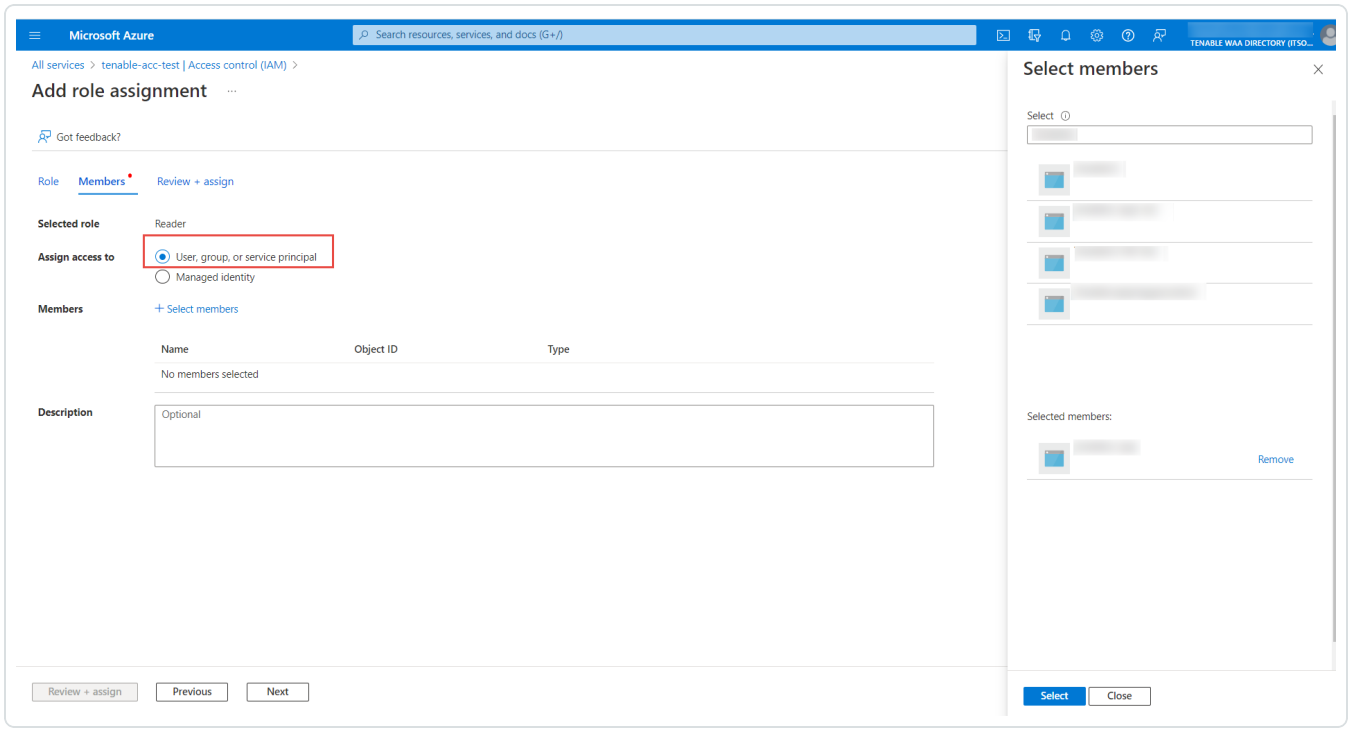
7. **[ロールの割り当てを追加]** をクリックします。



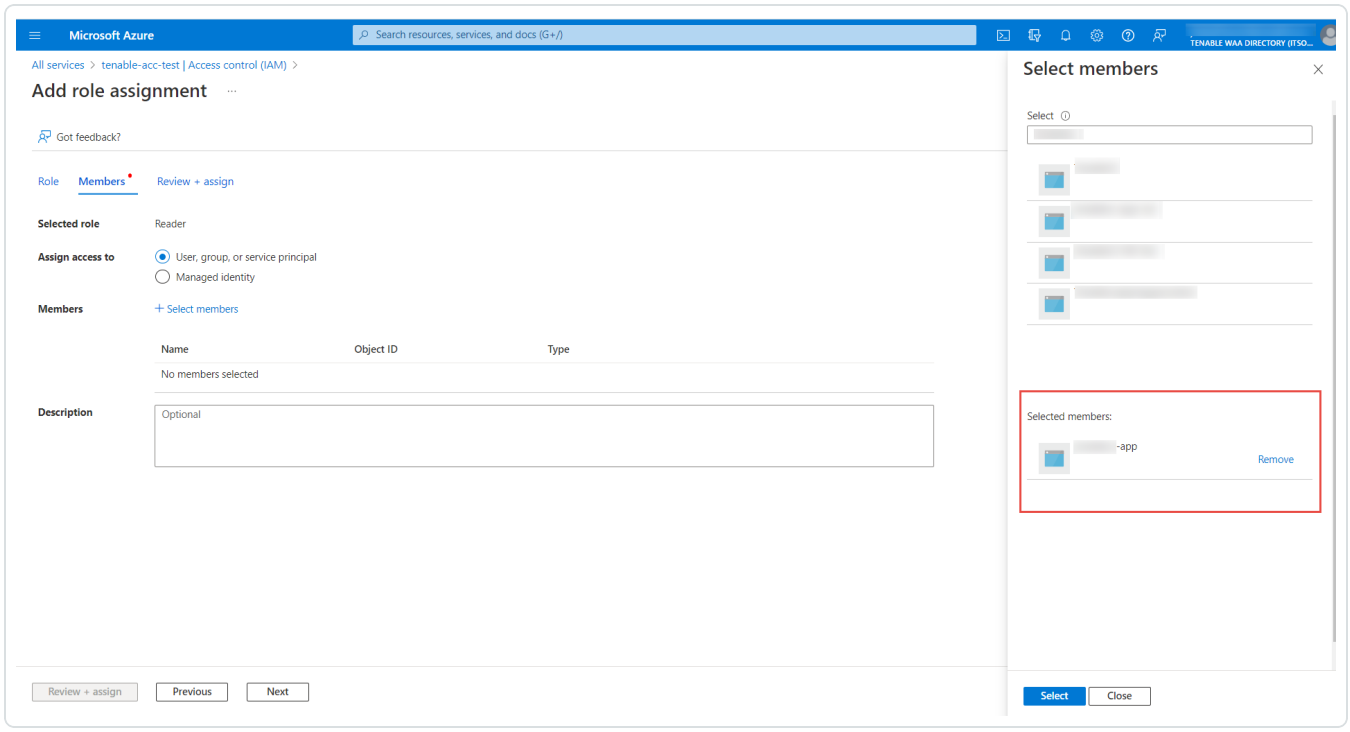
8. **[ロールの割り当てを追加]** ウィンドウの **[ロール]** タブで、**[リーダー]** を検索して選択します。



9. **[メンバー]** タブの **[アクセス権の割り当て]** セクションで、**[ユーザー、グループ、サービスプリンシパル]** を選択します。

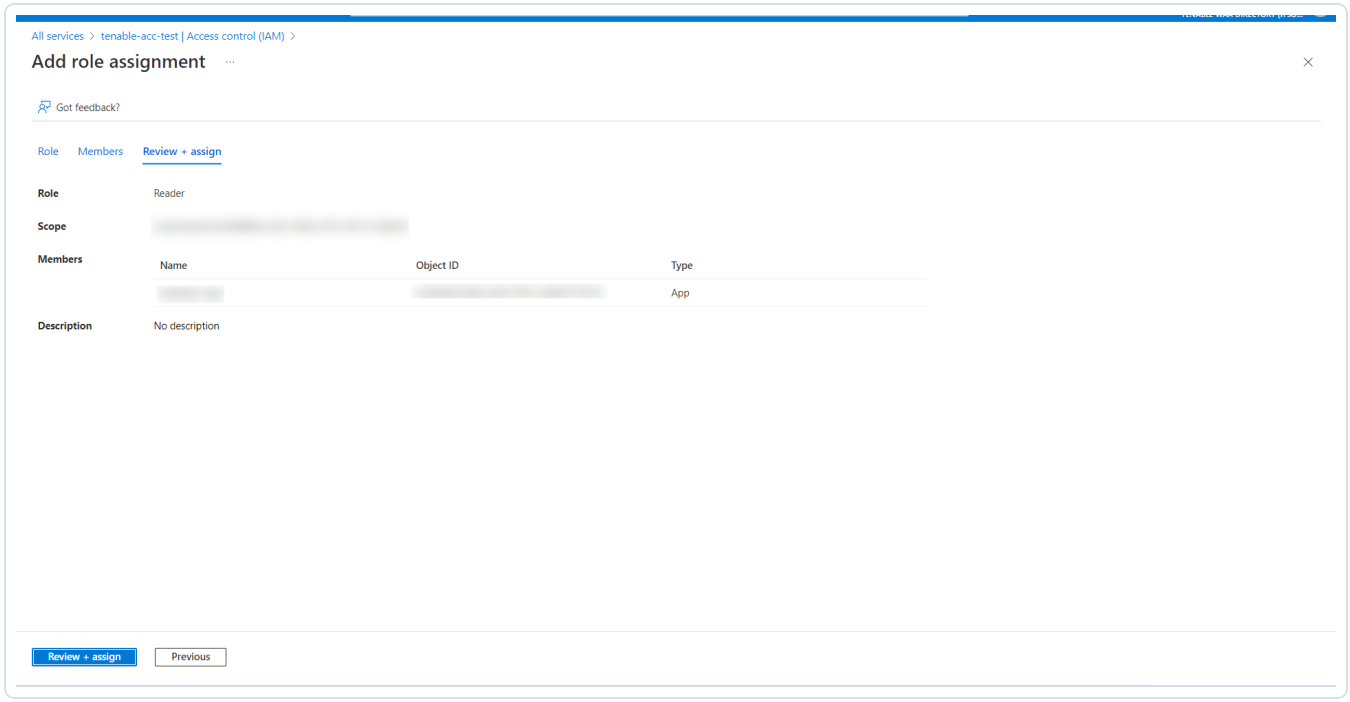


10. Azure アプリケーションを選択するには、**[+ メンバーを選択]** をクリックします。



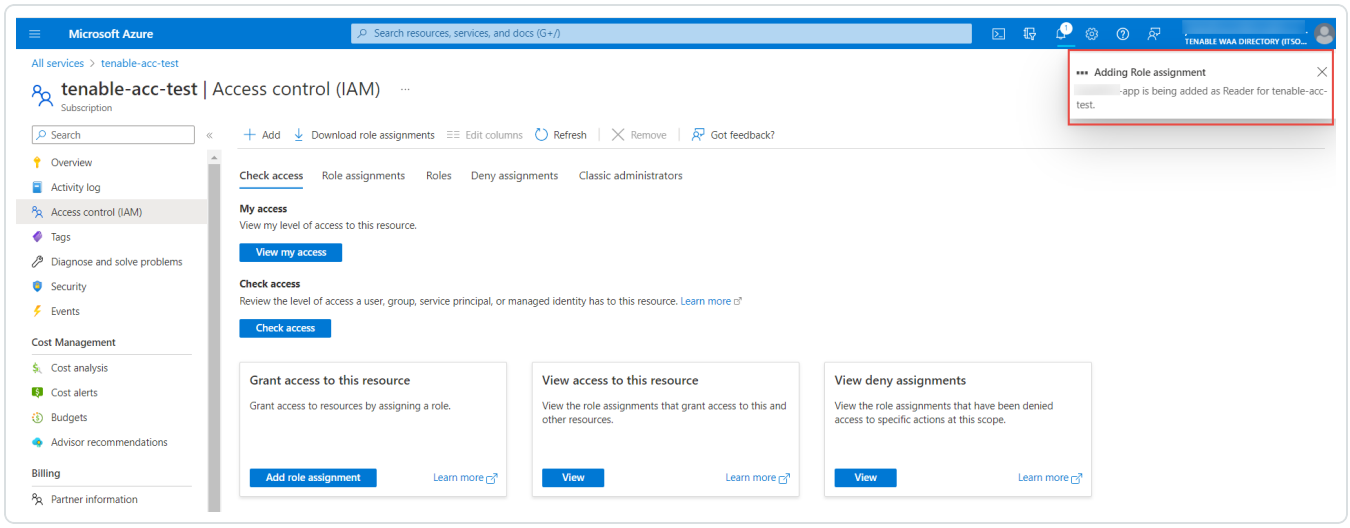
[メンバーを選択] プレーンが表示されます。

11. Azure アプリケーションを検索し、リストから必要なアプリケーションを選択します。
12. **[確認 + 割り当て]** タブで、選択したロールとメンバーを確認します。



13. **[確認 + 割り当て]** をクリックします。

選択したアプリケーションが、サブスクリプションの**リーダー**として追加されます。



次の手順

- Azure コネクタを作成します。

Microsoft Azure コネクタの作成

必要なユーザーロール: 管理者

始める前に

- 必要な Microsoft Azure の設定手順を完了します。
- プラグインの設定を 2018 年 12 月 19 日以降に更新します。

Microsoft Azure コネクタを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. ページの右上にある **[クラウドコネクタの作成]** ボタンをクリックします。

   [クラウドコネクタ] プレーンが表示されます。

5. **[クラウドコネクタ]** セクションで、**[Microsoft Azure]** をクリックします。

   [Microsoft Azure] 設定プレーンが表示されます。

6. **[コネクタ名]** ボックスに、コネクタを識別する名前を入力します。

7. **[アプリケーション ID]** ボックスに、Microsoft Azure を設定する際に取得した Azure アプリケーション ID を入力します。

8. **[テナント ID]** ボックスに、Microsoft Azure を設定する際に取得した Azure テナント ID を入力します。

9. **[クライアントシークレット]** ボックスに、Microsoft Azure を設定する際に取得したクライアントシークレットを入力します。

10. **[自動アカウント検出]**トグルを使用して、Azure サブスクリプション ID の自動検出を有効または無効にします。

    > **注意:** 自動アカウント検出はデフォルトで有効になっています。Azure コネクタはサブスクリプション ID とリンクされたあらゆるサブスクリプション ID を自動的に検出します。

11. (オプション)**[自動アカウント検出]**が無効になっている場合は、1 つまたは複数のサブスクリプション ID を手動で追加します。

    a. **[サブスクリプション ID]**セクションで、**[サブスクリプション ID]**の横にある ⊕ ボタンをクリックします。

       [サブスクリプション ID を追加]プレーンが表示されます。

    b. **[サブスクリプション ID]**ボックスに、Microsoft Azure を設定する際に取得したサブスクリプション ID を入力します。

    c. (オプション)**[別のサブスクリプション ID を追加]**の横にある ⊕ ボタンをクリックし、リンクされた別の Azure アカウントを追加します。

    d. **[サブスクリプション ID]**ボックスで、リンクする Azure アカウントのサブスクリプション ID を入力します。リンクされたサブスクリプションについての情報は、Azure サブスクリプションをリンクするを参照してください。

    e. サブスクリプション ID を追加するには、**[追加]**をクリックします。

       Tenable Vulnerability Management に**[Microsoft Azure]**設定プレーンが表示され、リンクしたサブスクリプション ID は**[サブスクリプション ID]**に一覧表示されます。

12. **[ネットワークを選択または作成する]**ドロップダウンボックスで、コネクタの既存のネットワークを選択するか、⊕ ボタンをクリックして新しいネットワークを作成します。

    > **注意:** ネットワークは、クラウド資産と Nessus によって検出された資産の間での IP アドレスの衝突を回避するのに役立ちます。Tenable では、異なるクラウド環境の資産レコードが相互に上書きされないように、使用するコネクタタイプごとにネットワークを作成することをお勧めします。ネットワーク機能の詳細については、ネットワークを参照してください。

13. **[インポートのスケジュール]**トグルを使用して、スケジュールしたインポートを有効または無効にします。

注意: デフォルトでは、Tenable Vulnerability Management は 1 日ごとに新規および更新された資産レコードをリクエストします。

有効な場合

- **[インポート]** テキストボックスに、Tenable Vulnerability Management が Azure サーバーにデータリクエストを送信する頻度を入力します。
- ドロップダウンボックスから、**[分]**、**[時]**、**[日]** のいずれかを選択します。

  注意: コネクタ設定を 30 分ごとに同期するようにスケジュールすると、検出ジョブが 30 分ごとにキューに配置されます。コネクタサービスのワークロードに応じて、検出ジョブの結果が Tenable Vulnerability Management インターフェースとログで参照できるようになります。したがって、キューによっては、検出ジョブの結果が出るのに 30 分以上かかる場合があります。

14. 次のいずれかを行います。
    - コネクタを保存するには、**[保存]** をクリックします。
    - コネクタを保存して、Azure から資産をインポートするには、**[保存してインポート]** をクリックします。

注意: 資産が Tenable Vulnerability Managementに表示されるまでに時間がかかる場合があります。

Google Cloud Platform コネクタ

Google Cloud Platform (GCP) コネクタは、Google Cloud Platform にある資産と在庫をリアルタイムで表示します。GCP コネクタは、ユーザーが設定したスケジュールに従って更新されます。

Google Cloud Platform の資産についての情報をインポートおよび分析するには、GCP がコネクタに対応するよう設定し、Tenable Vulnerability Management で GCP コネクタを作成する必要があります。

GCP コネクタを介して資産を分析する方法

1. Google Cloud Platform (GCP) を設定するの説明に従って GCP アカウントがコネクタに対応するように設定します。
2. Google Cloud Platform コネクタを作成する (検出のみ)の説明に従って GCP コネクタを作成します。

注意: 既存の GCP コネクタを管理するには、コネクタの管理を参照してください。

ヒント: よくあるコネクタエラーについては、Tenable 開発者ポータルのコネクタを参照してください。

Google Cloud Platform (GCP) を設定する

必要なユーザーロール: 管理者

Tenable Vulnerability Management GCP コネクタを使用する前に、コネクタに対応するよう GCP を設定する必要があります。

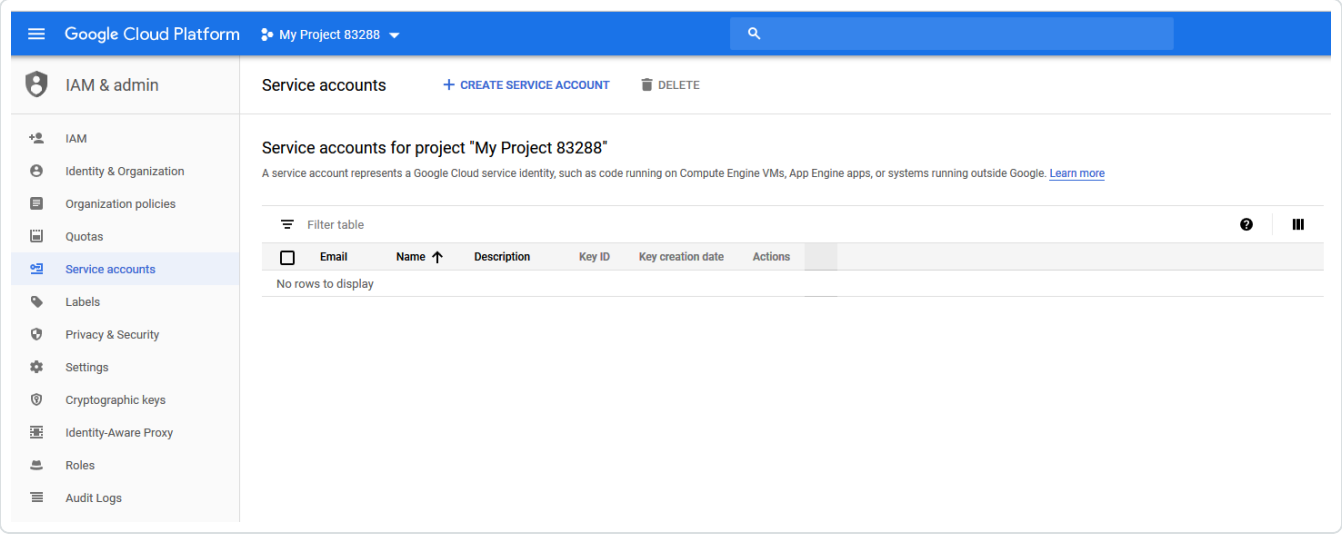
注意: 設定の前に、スキャンする各プロジェクトに対して Google Cloud Platform 内からコンピュートエンジン API を有効にする必要があります。詳細は、Google API のドキュメントを参照してください。

GCP を Tenable Vulnerability Managementコネクタに対応するよう設定する方法

1. Google Cloud Platform にログインします。
2. 左側のナビゲーションバーで **[IAM & admin]** をクリックします。

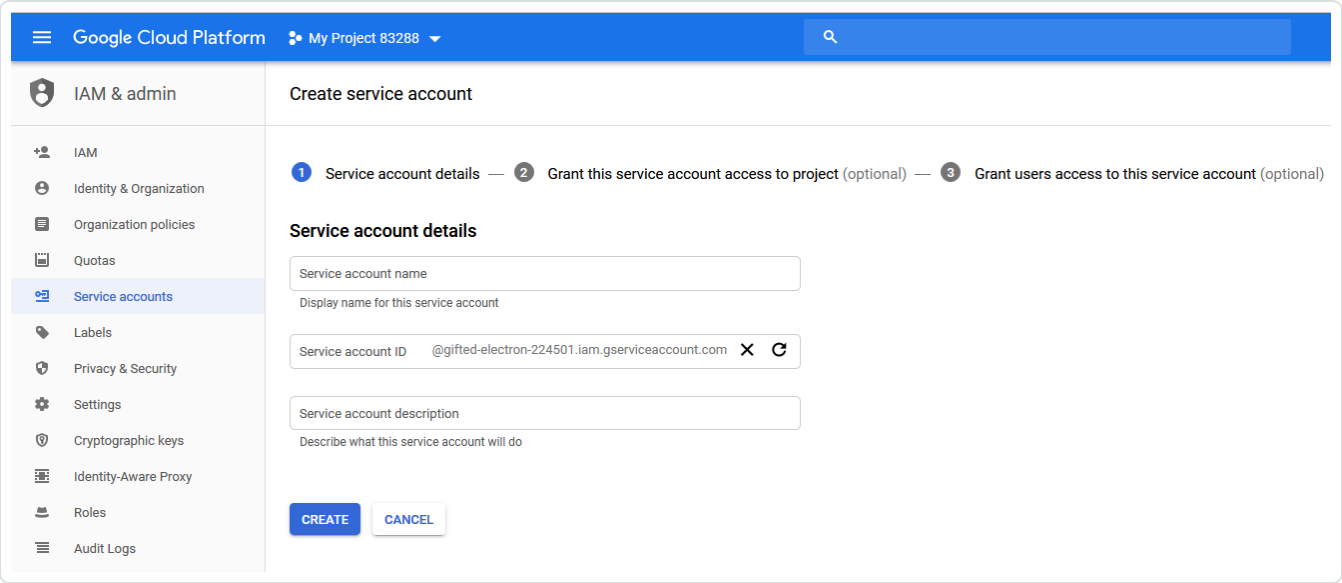
   [IAM & admin] ページが表示されます。
3. 左上の **[プロジェクトの選択]** ドロップダウンボックスで、適用可能な GCP プロジェクトを選択します。
4. 左側のナビゲーションバーで **[サービスアカウント]** をクリックします。

   GCP プロジェクトの **[サービスアカウント]** ページが表示されます。



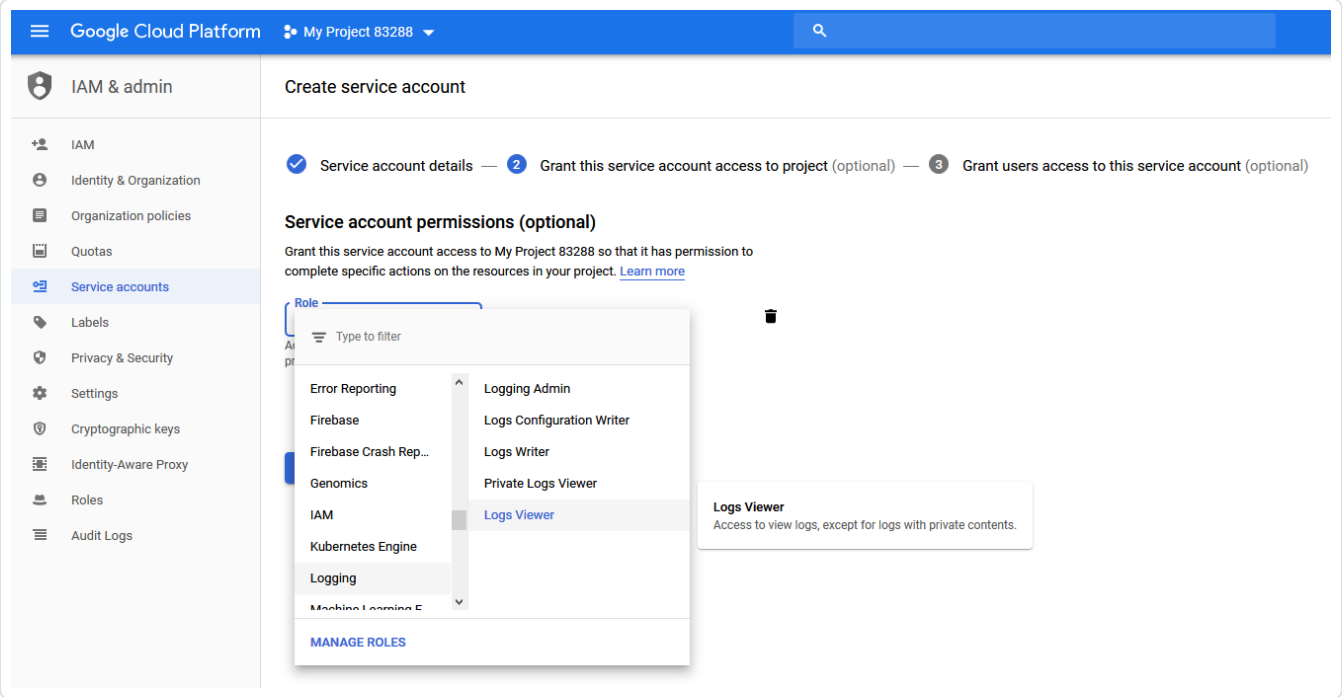
5. **[+ サービスアカウントの作成]** をクリックします。

   [サービスアカウントの作成] ページが表示されます。



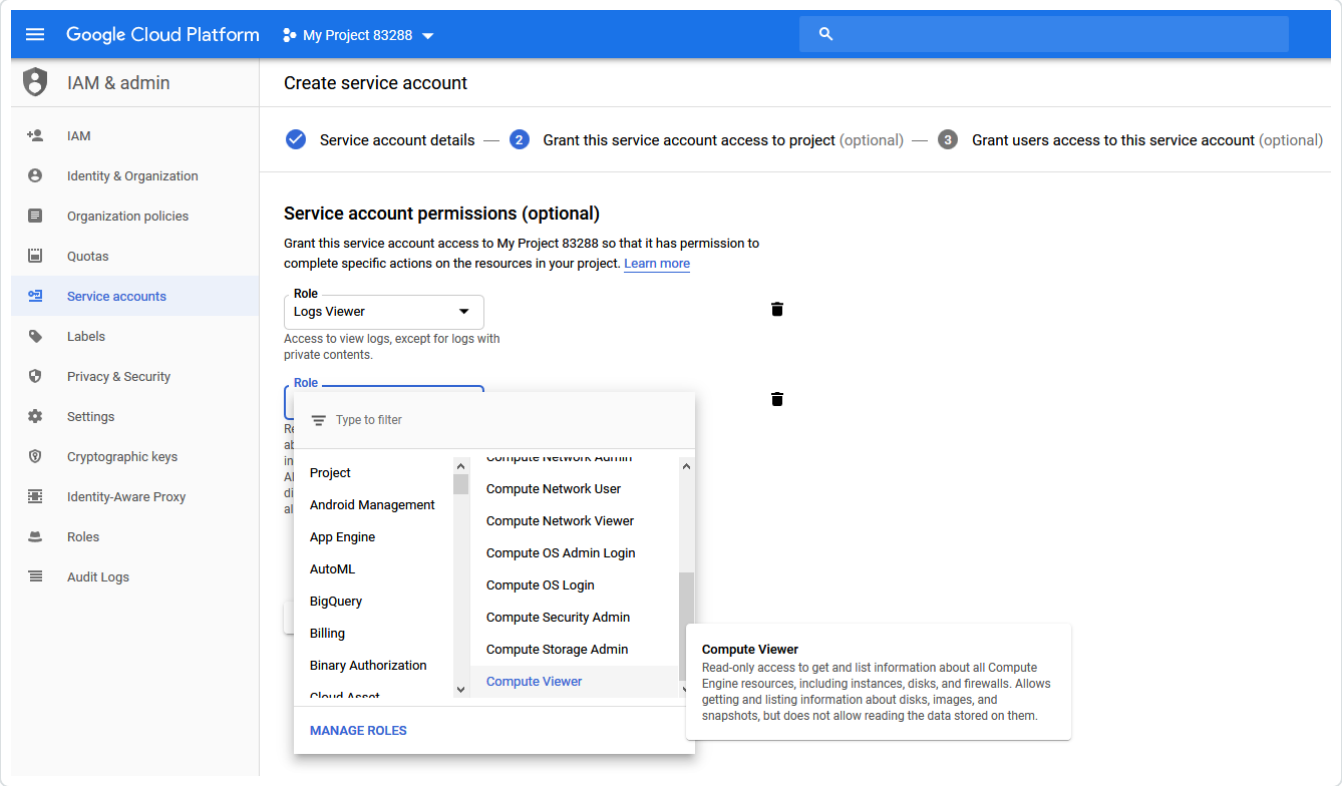
6. **[サービスアカウント名]** ボックスにサービスアカウントの名前を入力します。
7. **[サービスアカウント ID]** ボックスに固有のサービスアカウント ID を入力します。
8. **[サービスアカウントの説明]** ボックスにサービスアカウントの実行内容を説明します。
9. **[作成]** ボタンをクリックします。

   [このサービスアカウントにプロジェクトへのアクセス権を与える] ページが表示されます。
10. **[サービスアカウントのアクセス許可 (オプション)]** ページのドロップダウンボックスで、[ログ] > [ログ閲覧者] のロールを追加します。



注意：サービスアカウントには、検出同期（最初のフル同期後の差分同期）用に［ログ］>［ログ閲覧者］のロールがある必要があります。

11. **［サービスアカウントのアクセス許可（オプション）］**ページで、**［+ 別のロールを追加する］**をクリックします。
12. **［Compute Engine］**->**［Compute 閲覧者］**のロールを追加します。



13. **[続行]** ボタンをクリックします。

    [ユーザーにこのサービスアカウントへのアクセス権を与える] ページが表示されます。

14. **[キーの作成 (オプション)]** セクションで、**[+ キーの作成]** をクリックします。

    [キーの作成 (オプション)] ペインが表示されます。

15. **[キータイプ]** で、**[JSON]** を選択して JSON フォーマットでキーを作成します。

16. **[作成]** ボタンをクリックします。

17. ブラウザが JSON フォーマットでキーをダウンロードします。

(オプション) 複数のプロジェクトにアクセス可能な GCP サービスアカウントを設定する方法

多くの GCP アカウントが定期的に追加・削除されます。各 GCP アカウントを異なるコネクタとして追加するのではなく、最上位のサービスアカウントを複数のプロジェクトにアクセスするよう設定できます。GCP コネクタはリンクされたプロジェクトをすべて自動で検出し、それらのプロジェクトから資産を抽出します。

> **注意:** 最上位のサービスアカウントでは、複数のプロジェクトにアクセスするため、Cloud Resource Manager API が有効になっています。

警告: GCP コネクタは、最上位のサービスアカウントへのアクセスで設定された、いずれのプロジェクトからも資産を抽出します。GCP コネクタにデータを抽出させるプロジェクトを追加するだけで済みます。

1. Google Cloud Platform にログインします。
2. 左側のナビゲーションバーで **[IAM & admin]** をクリックします。

   [IAM & admin] ページが表示されます。
3. 左上のドロップダウンメニューで、2 番目の GCP プロジェクトを選択します。
4. IAM メニューバーで、**[+ 追加]** をクリックします。

   [メンバーをプロジェクトに追加] ペインが表示されます。
5. **[新しいメンバー]** ボックスで、最初のセクションの手順 6 で作成した最上位サービスアカウントの名前を入力します。
6. **[ロールの選択]** ドロップダウンボックスで、**[ログ]** > **[ログ閲覧者]** のロールを選択します。
7. **[+ 別のロールを追加する]** ボタンをクリックします。
8. **[ロールの選択]** ドロップダウンボックスで、**[Compute Engine]** > **[Compute 閲覧者]** のロールを選択します。
9. (オプション) 追加のロールを追加するには、**[+ 別のロールを追加する]** ボタンをクリックします。
10. 追加のプロジェクトを追加するには、手順 3 から 9 までを繰り返します。

次の手順

- Google Cloud Platform コネクタを作成する (検出のみ)の説明に従って GCP コネクタを作成します。

Google Cloud Platform コネクタを作成する(検出のみ)

必要なユーザーロール: 管理者

始める前に

- 必要な GCP の設定手順を完了します。

GCP コネクタを作成する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. ページの右上にある **[コネクタの作成]** ボタンをクリックします。

   [コネクタの選択] ペインが表示されます。

5. **[コネクタ]** セクションで、**[Google Cloud Platform]** をクリックします。

   [Google Cloud Platform] ペインが表示されます。

6. **[コネクタ名:]** ボックスに、コネクタを識別する名前を入力します。

7. **[サービスアカウントキー]** セクションで、**[ファイルの追加]** をクリックして、GCP の設定時に取得したサービスアカウントキーをアップロードします。

8. **[自動アカウント検出]** トグルは常に有効で、無効にすることはできません。提供したサービスアカウントに関連するすべてのプロジェクト ID は自動検出され、これらのプロジェクトから資産が抽出されます。

9. **[ネットワークを選択または作成する]** ドロップダウンボックスで、コネクタの既存のネットワークを選択するか、⊕ ボタンをクリックして新しいネットワークを作成します。

注意: ネットワークは、クラウド資産とNessusによって検出された資産の間でのIPアドレスの衝突を回避するのに役立ちます。Tenableでは、異なるクラウド環境の資産レコードが相互に上書きされないように、使用するコネクタタイプごとにネットワークを作成することをお勧めします。ネットワーク機能の詳細については、ネットワークを参照してください。

10. **[インポートのスケジュール:]** トグルを使用してスケジュールしたインポートを有効または無効にします。

    注意: デフォルトでは、Tenable Vulnerability Managementは1日ごとに新規および更新された資産レコードをリクエストします。

    有効にした場合

    - Tenable Vulnerability Managementが GCP サーバーにデータリクエストを送信する頻度を、**[インポート]** テキストボックスに入力します。
    - ドロップダウンボックスで、*[分]*、*[時間]*、*[日]* のいずれかを選択します。

      注意: コネクタ設定を30分ごとに同期するようにスケジュールすると、検出ジョブが30分ごとにキューに配置されます。コネクタサービスのワークロードに応じて、検出ジョブの結果がTenable Vulnerability Management インターフェースとログで参照できるようになります。したがって、キューによっては、検出ジョブの結果が出るのに30分以上かかる場合があります。

11. 次のいずれかを行います。

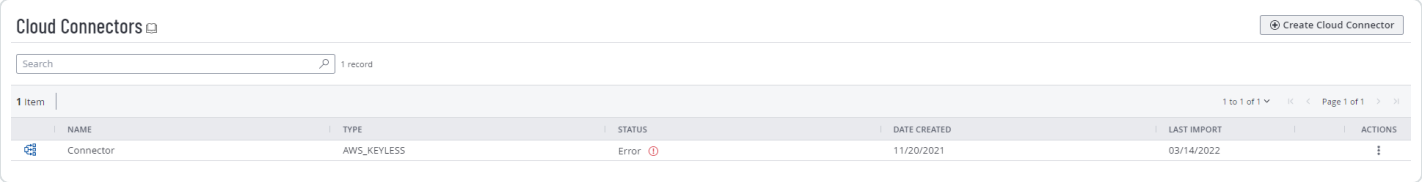
    - コネクタを保存するには、**[保存]** をクリックします。
    - コネクタを保存して、GCPから資産をインポートするには、**[保存してインポート]** をクリックします。

注意: 資産がTenable Vulnerability Managementに表示されるまでに時間がかかる場合があります。

既存コネクタの管理

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

[クラウドコネクタ] ページには、すべての設定済みコネクタが一覧表示された [コネクタ] の表が表示されます。



コネクタインポートの手動起動

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

コネクタの手動インポートを起動する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. 手動インポートを起動するコネクタの行の **[アクション]** 列で、[⋮] > ⇤ **[インポート]** をクリックします。

   Tenable Vulnerability Management はソースにデータのリクエストを送信します。リクエスト処理中、インポートボタンはチェックマークとして表示されます。リクエスト処理が完了するまで、同じコネクタに対して別の手動インポートは起動できません。

コネクタの詳細を表示する

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

[コネクタ] ページでは、コネクタとインポートに関する詳細を表示できます。

注意: 手動でのインポートの開始、コネクタの編集、コネクタの削除などのコネクタ管理タスクは、**[コネクタ]** ページから実行することもできます。詳細は、既存コネクタの管理 を参照してください。

始める前に

- コネクタの説明に従って、コネクタがアクセスする必要があるプラットフォームを設定し、コネクタを作成します。

コネクタとインポートの詳細を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. **[コネクタ]** 表では、次のことができます。

   a. **[コネクタ]** 表を検索する

   b. コネクタとインポートに関する詳細を表示する

列	アクション
Name	コネクタの名前が表示されます。
Type	コネクタが資産を取得するプラットフォームまたはレジストリタイプが表示されます。
Status	直近の資産インポートのステータスが表示されます。 **注意:** コネクタが Tenable Container Security コネクタである場合は、**[ステータス]** 列のコネクタ行の上にカーソルを合わせると、失敗したインポートのエラーの詳細が表示されます。
Date Created	• コネクタが作成された日付が MM/DD/YYYY 形式で表示されます。 • 列見出しをクリックすると、コネクタが作成日で並べ替えられます。
Last Import	直近の資産インポートの日付が表示されます。 **注意:** コネクタが Tenable Container Security コネクタである場合は、インポートの開始後に日付の横に緑色の ⟳ アイコンが表示されます。このアイコンの上にカーソルを合わせると、コネクタがインポートする各資産の詳細が表示されます。インポートが進行するにつれて、詳細がリアルタイムで更新されます。

コネクタのイベント履歴を表示する

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

キーレス認証により設定された Microsoft Azure コネクタおよび AWS コネクタでは、問題のトラブルシューティングに役立つコネクタのイベント履歴を表示できます。Tenable Vulnerability Management がコネクタとの同期、資産のインポート、終了した資産の確認などを行った際のイベントを表示できます。

始める前に

- コネクタの説明に従って、コネクタがアクセスする必要があるプラットフォームを設定し、コネクタを作成します。

コネクタのイベント履歴を表示する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. コネクタの表で、イベント履歴を表示するコネクタをクリックします。

   > **注意:** イベント履歴は、キーレス認証により設定された Microsoft Azure コネクタおよび AWS コネクタの場合に表示できます。

   コネクタ設定プレーンが表示されます。

5. **[イベント履歴を表示]** をクリックします。

コネクタプレーンが展開し、**[コネクタのイベント履歴]** の表が表示されます。表には、コネクタから Tenable Vulnerability Management に送信された、Tenable Vulnerability Management がコネクタとの同期、資産のインポート、終了した資産の確認などを行った際のイベントが表示されます。コネクタのエラーに関する詳細は、Tenable 開発者ポータルに文書化されているコネクタを参照してください。

コネクタの編集

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

[設定] ページでは、資産のインポートスケジュールなど、コネクタの詳細を編集できます。コネクタを編集する手順は、プラットフォームによって異なります。

始める前に

- コネクタの説明に従ってコネクタを設定、作成します。
- Tenable Vulnerability Management にログインします。

Microsoft Azure コネクタを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. コネクタの表で、編集するコネクタをクリックします。

   [コネクタの編集] ペインが表示されます。

5. 以下のコネクタ設定を変更します。

   - **[ネットワークの選択または作成]** ドロップダウンボックスで、コネクタの既存のネットワークを変更するか、⊕ ボタンをクリックして新しいネットワークを作成します。
   - **[コネクタ名]** ボックスで、コネクタの名前を変更します。

- **[アプリケーション ID]** ボックスで、アプリケーション ID を変更します。
- **[テナント ID]** ボックスで、テナント ID を変更します。
- **[クライアントシークレット]** ボックスで、クライアントシークレットを変更します。
- **[自動アカウント検出]** トグルを使用して、サブスクリプション ID の自動検出を有効または無効にします。
- **[自動アカウント検出]** が無効になっている場合は、サブスクリプション ID を追加または削除します。
- **[インポートのスケジュール]** オプションで、スケジュールされたインポートの頻度を変更します。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management がコネクタを保存します。資産が Tenable Vulnerability Managementに表示されるまで多少時間がかかる場合があります。

Amazon Web Service (AWS) コネクタを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. コネクタの表で、編集するコネクタをクリックします。

   [コネクタの編集] ペインが表示されます。

5. コネクタを変更します。

   ### AWS ロール委任 (キーレス認証) を使用する場合

   - **[ネットワークを選択または作成する]** ドロップダウンボックスで、コネクタの既存のネットワークを変更するか、⊕ ボタンをクリックして新しいネットワークを作成します。
   - **[コネクタ名]** ボックスで、コネクタの名前を変更します。

- **[自動アカウント検出]**トグルを使用して、リンク済みアカウントとCloudTrail の自動検出を有効または無効にします。
- **[インポートのスケジュール]** オプションで、スケジュールされたインポートの頻度を変更します。

キーによる認証を使用する場合

- **[ネットワークを選択または作成する]**ドロップダウンボックスで、コネクタの既存のネットワークを変更するか、⊕ ボタンをクリックして新しいネットワークを作成します。
- **[コネクタ名]** ボックスで、コネクタの名前を変更します。
- **[アクセスキー]** ボックスで、アクセスキーを変更します。
- **[秘密鍵]** ボックスで、アクセスキーに対応する秘密鍵を変更します。
- **[追加のアカウント]** セクションで、リンクされたアカウントを追加または削除します。
- **[AWS CloudTrails]** セクションで、CloudTrails を追加または削除します。
- **[CloudTrails の更新]** をクリックして AWS 地域にクエリを実行し、**[AWS CloudTrails]** 表を更新します。
- **[インポートのスケジュール]** オプションで、スケジュールされたインポートの頻度を変更します。

6. (オプション) 別の証跡を選択した場合は、**[資産の検索]** をクリックします。

   Tenable Vulnerability Management にインポートされる資産の数は、**[資産の検索]** ボタンの隣に表示されます。この数には、過去にインポートされた資産が含まれる場合があります。資産が過去にインポート済みの場合、重複して作成されません。

7. **[保存]** をクリックします。

   コネクタが保存されます。別の Trails を選択した場合、AWS からインポートされた資産が表示されます。資産が Tenable Vulnerability Managementに表示されるまで多少時間がかかる場合があります。

Google Cloud Platform (GCP) コネクタを編集する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. コネクタの表で、編集するコネクタをクリックします。

   [コネクタの編集] ペインが表示されます。

5. 以下のコネクタ設定を変更します。

   - **[ネットワークの選択または作成]** ドロップダウンボックスで、コネクタの既存のネットワークを変更するか、⊕ ボタンをクリックして新しいネットワークを作成します。
   - **[コネクタ名]** ボックスで、コネクタの名前を変更します。
   - **[サービスアカウントキー]** で、**[ファイルの追加]** をクリックして、サービスアカウントキーを変更します。
   - **[インポートのスケジュール]** オプションで、スケジュールされたインポートの頻度を変更します。

6. **[保存]** をクリックします。

   Tenable Vulnerability Management がコネクタを保存します。資産が Tenable Vulnerability Managementに表示されるまで多少時間がかかる場合があります。

Tenable Container Security コネクタを編集する方法

1. Tenable Container Security にログインします。ログインの方法については、*Tenable Container Security ユーザーガイド*のログインTenable Container Securityを参照してください。
2. [コンテナのセキュリティ] ダッシュボードの **[コネクタ]** セクションで、**[コネクタの表示]** をクリックします。

   [コネクタ] ページが表示されます。

3. コネクタの表で、編集するコネクタをクリックします。

   [コネクタの詳細の入力] ペインが表示されます。

4. 次の 1 つ以上のコネクタの詳細を変更します。

   - **[URL]** ボックスで、URL を変更します。
   - **[ポート]** ボックスで、ポート ID を変更します。

- **[ユーザー名]** ボックスで、ユーザー名 を変 更します。
- **[パスワード]** ボックスで、パスワードを変 更します。

5. **[保 存]** をクリックします。

   コネクタが保 存されます。資 産 が Tenable Vulnerability Managementに表 示されるまで多 少 時 間 がかかる場 合 があります。

注 意 : Tenable Container Security のコネクタに関 する詳 細 は、*Tenable Vulnerability Management Container Security ユーザーガイド*のイメージをインポートするためのコネクタの設 定を参 照してください。

コネクタを削除する

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

コネクタを削除する方法

1. 左上にある ☰ ボタンをクリックします。

   左側にナビゲーションプレーンが表示されます。

2. 左のナビゲーションプレーンで **[設定]** をクリックします。

   [設定] ページが表示されます。

3. **[クラウドコネクタ]** タイルをクリックします。

   [クラウドコネクタ] ページが表示され、設定済みのコネクタの表が表示されます。

4. コネクタの表で、削除するコネクタの横にある ✕ ボタンをクリックします。

   [削除の確認] ウィンドウが表示されます。

5. **[削除]** をクリックします。

   Tenable Vulnerability Management はコネクタを削除します。

次の手順

- キーレス認証を使用している AWS コネクタを削除する場合は、AWS でコネクタアーティファクトの手動削除を参照してください。

Frictionless Assessment の削除

Frictionless Assessment のプロビジョニングは終了し(2023 年 5 月 15 日以降)、新しいユーザーは Frictionless Assessment コネクタをデプロイできなくなります。2023 年 12 月 31 日に Frictionless Assessment はサポート終了となり、サポートを受けたり更新を受け取ったりできなくなります。ただし、既存の Frictionless Assessment コネクタは、2024 年 12 月 31 日にサポートが終了するまで引き続きお使いいただけます。Tenable では、クラウドリソースのスキャン用に、エージェントなしの評価を含む Tenable Cloud Security に移行することを推奨しています。詳細については、Tenable Vulnerability Management リリースノートを参照してください。

必要なユーザーロール: 管理者

エージェントなしの評価にアップグレードする際に、既存の AWS および Azure コネクタを Tenable コンテナから削除またはオフボードできます。

- AWS Frictionless Assessment の削除
- Azure Frictionless Assessment の削除

重要: Frictionless Assessment コネクタは変更/許容ルールをサポートしていません。

AWS Frictionless Assessment の削除

コネクタには次の 2 つのタイプがあります。

- キーレス認証を使用した AWS Frictionless Assessment コネクタ
- AWS Frictionless Assessment コネクタ

キーレス認証を使用した AWS Frictionless Assessment コネクタ

キーレス認証を使用した AWS Frictionless Assessment コネクタを削除する前の考慮事項

- このコネクタには、検出機能と Frictionless Assessment 機能の両方が含まれています。
- 削除後に検出機能を引き続き利用するには、別の検出コネクタを作成する必要があります。
- 作成プロセス中にコネクタが以下のいずれかの CloudFormation テンプレートをデプロイしたかどうかを確認してください。
  - AWS キーレス Frictionless Assessment シングルタグ CloudFormation テンプレート
  - AWS キーレス Frictionless Assessment CloudFormation テンプレート

キーレス認証を使用した AWS Frictionless Assessment コネクタを削除する方法

1. AWS コネクタを削除します。詳細については、コネクタを削除するを参照してください。

   Tenable は、アカウントから次の AWS Systems Manager リソースを削除します。

   - `TenableInventoryAssociation` - AWS Systems Manager アソシエーション名
   - `TenableInventoryCollection` - AWS Systems Manager ドキュメント名
   - `tenb-inv-upload-<customerRegionName>-<clusterName>-sync` — ResourceDataSync

2. AWS で、AWS Systems Manager のリソースがアカウントから削除されているかどうかを確認します。
3. AWS で、`tenableio-connector-aws-keyless-fa-single-tag-cft` または `tenableio-connector-aws-keyless-fa-cft` という名前のスタックインスタンスを削除します。

   これにより、Tenable で Frictionless Assessment インベントリスキャンと検出を実行するのに必要と

されたアクセス許可が削除されます。

4. (オプション) Frictionless Assessment に使用される AWS EC2 インスタンスのタグを削除します。

AWS Frictionless Assessment コネクタ

AWS Frictionless Assessment コネクタを削除する前の考慮事項

- このコネクタには Frictionless Assessment 機能のみが含まれています。
- CloudFormation StackSet により、このコネクタの AWS Systems Manager リソースがデプロイされています。したがって、スタックインスタンスと StackSet を AWS アカウントから削除すると、AWS Systems Manager リソースが削除されます。
- Frictionless Assessment コネクタと同じアカウントに別の検出コネクタを設定済みであるかどうか確認してください。この検出コネクタは、終了した資産を検出します。この検出コネクタは引き続き AWS アカウントから資産を検出してインポートするため、この検出コネクタを削除する必要はありません。

AWS Frictionless Assessment コネクタを削除する方法

1. Tenable Vulnerability Management で AWS Frictionless Assessment コネクタを削除します。詳細については、コネクタを削除するを参照してください。

   アカウントのインベントリが今後処理されないようにする目的で、Tenable はコネクタのバックエンド設定を削除します。

2. AWS で、この CloudFormation テンプレート を使用してデプロイした StackSet を AWS アカウントから削除します。

   これにより、アカウントから AWS Systems Manager アソシエーション、AWS Systems Manager ドキュメント、および ResourceDataSync が削除されます。この手順が完了すると、これ以降 Tenable はスキャン対象のインベントリを受け取りません

3. (オプション) Frictionless Assessment によりスキャンされる EC2 インスタンスのタグを削除します。

Azure Frictionless Assessment の削除

Azure Frictionless Assessment は AWS Frictionless Assessment コネクタに似ています。

Azure Frictionless Assessment コネクタを削除する方法

1. Tenable Vulnerability Management で Azure Frictionless Assessment コネクタを削除します。詳細については、コネクタを削除するを参照してください。
2. Azure ポータルで `Tenable-FA-Connector-*` リソースグループを見つけて削除します。

   これは、Azure Frictionless Assessment コネクタを作成したときに ARM テンプレートによってデプロイされたリソースグループです。
3. (オプション) Frictionless Assessment に使用されるタグを削除します。