Tenable Security Center 大規模エンタープライズデプロイメントガイド

最終更新日: 2024 年 4 月 5 日

目次

Tenable Security Center の大規模エンタープライズデプロイメントガイドにようこそ

Tenable Security Center の大規模エンタープライズデプロイメントを計画するにあたり、考慮すべき数多くの固有の技術上・ビジネス上の要件があるかもしれません。100,000 以上の IP アドレスをスキャンしている企業では、Tenable Security Center デプロイメントの計画、実行、運用の際に、このガイドの情報を考慮してください。

本ガイドは、お客様のデプロイメントの計画に役立ちますが、すべてのデプロイメントのシナリオやネットワークアーキテクチャをカバーするものではありません。詳細については、Tenable サポート または Tenable Professional Services にお問い合わせください。Tenable では、本ガイドをTenable Security Center ユーザーガイドの手引きとして使用されることをお勧めしています。

- デプロイメントを計画する
- スキャン戦略を計画する
- 構築済みのデプロイメントを運用可能にする

ヒント: *Tenable Security Center「大規模エンタープライズデプロイメントガイド」* は、英語版と日本語版があります。

デプロイメントを計画する

Tenable Security Center デプロイメントを計画する際は、次の点について考慮してください。

- エアギャップ環境
- 階層化されたデプロイメント
- アクセス制御
- 統合
- API の使用方法

エアギャップ環境

関連記事: *Tenable Security Center ユーザーガイド* のオフラインリポジトリ

Tenable Security Center をエアギャップ (オフライン) 環境に展開する場合は、次のことに留意してください。

アーキテクチャ

Tenable Security Center およびスキャナーのセットを、それぞれのエアギャップネットワーク内に展開する必要があります。

他のネットワークからのデータを、エアギャップされたネットワークで生成されたデータと統合する場合、オフラインリポジトリを使用して、エアギャップされた Tenable Security Center から他の Tenable Security Center インスタンスへとデータをエクスポートできます。これは、統合されたレポート構造と連結されたレポート構造の両方に対応します。

アップグレードと更新

Tenable では、Tenable Security Center のアップグレードを少なくとも年 1 回 (四半期ごとが望ましい)、プラグインやフィードの更新を少なくとも月 1 回行うことを推奨しています。プラグインの更新を実施した後は、包括的なスキャンを実行し、新しい脆弱性データを活用して最新のスキャン結果を生成してください。

注意: いくつかのプラグインはインターネットアクセスを必要とし、エアギャップ環境では実行できません。たとえば Tenable Nessus プラグイン 52669 は、ホストがボットネットの一部かどうかをチェックするものです。

プラグインの更新またはフィードの更新を実施した後は、ナレッジベースの記事に記載されている通り、ファイルを検証してください。

Tenable Security Center のアップグレード、プラグインの更新、フィードの更新をオフラインで実行するには

ヒント: API を使用することで、Tenable Security Center のアップグレードおよびプラグインの更新プロセスの一部を自動化できます。

1. ブラウザ内または API 経由でファイルをダウンロードします。
2. ファイルの完全性を検証します。
    - Tenable Security Center アップグレードの場合は、ダウンロードしたチェックサムと Tenable のダウンロードページのチェックサムを比較します。
    - プラグイン更新とフィード更新の場合はチェックサムをダウンロードして比較します。
3. ファイルを Tenable Security Center インスタンスに移動します。
4. ファイルを Tenable Security Center にアップロードします。
    - Tenable Security Center のアップグレードは CLI 経由で行います。
    - プラグイン更新とフィード更新は ブラウザー内または API 経由で行います。

Tenable Nessus Agents

エアギャップで Tenable Nessus Agent を管理するために Tenable Nessus Manager を導入している場合、Tenable Nessus Manager でオフラインのソフトウェアアップデート (Tenable ダウンロードサイトの `nessus-agent-updates-X.X.X.tar.gz`) を実行してください。Tenable Nessus Manager により、管理対象の Tenable Nessus Agent にアップデートが展開されます。

詳細は、ナレッジベースの記事を参照してください。

階層化されたデプロイメント

関連記事: *Tenable Security Center ユーザーガイド*の階層型リモートリポジトリと*一般要件ガイド*のハードウェア要件

*階層化されたリモートリポジトリ*設定では、リモートリポジトリを使用して複数の Tenable Security Center インスタンス間でデータを共有します。

- 100,000 個 ~ 249,999 個のホストに対応する場合、Tenable では階層化されたリモートリポジトリ設定を推奨しています。
- 250,000 個以上のホストに対応する場合は、Tenable では階層化されたリモートリポジトリ設定が**必要**です。

階層化された Tenable Security Center インスタンスは、Tenable Security Center デプロイメント全体の中で非公式な役割を果たします。Tenable では、最低 1 つの指定されたレポート用の Tenable Security Center と、ネットワーク上のホスト 100,000 個 ~ 150,000 個ごとに 1 つの追加 Tenable Security Center インスタンスを推奨しています。

- *スキャン層*の Tenable Security Center は、接続されたスキャナー全体に渡ってスキャンジョブを管理することで、スキャンを最適化します。スキャン層の Tenable Security Center インスタンスは、スキャンデータの効率的な収集を優先します。
- *レポート層*の Tenable Security Center は、スキャン層の Tenable Security Center インスタンスにより収集されたデータを集約することで、ダッシュボードとレポートを最適化します。

注意: スキャン層およびレポート層の Tenable Security Center インスタンスは、同一の Tenable Security Center バージョンが動作している必要があります。

階層化されたリモートリポジトリ設定がない場合、エンタープライズ規模のスキャンおよび分析によって、単一の Tenable Security Center 上でパフォーマンスの問題が発生する可能性があります。リモートリポジトリを階層化することで、スキャンのパフォーマンスに悪影響を及ぼすことなく、分析とレポートの生成を最適化します。

ヒント: 2 つの Tenable Security Center インスタンスをオフラインリポジトリとして接続することは可能ですが、オフラインリポジトリはインスタンス間の真の接続を確立しません。すべてのデータは、オフラインリポジトリ間で手動で転送される必要があります。

リポジトリを使用して階層を接続する

スキャン層を、レポート層の Tenable Security Center デプロイメントの読み取り専用リポジトリとしてレポート層に接続します。

階層化されたリモートリポジトリのデプロイメントを設定するには

1. スキャン層の Tenable Security Center インスタンスで、スキャン結果データを保存するための 1 つ以上のリポジトリを作成します。

   注意: レポート層の Tenable Security Center インスタンスで、スキャン階層の Tenable Security Center インスタンスのトレンドデータを表示するには、スキャン階層の Tenable Security Center インスタンスの各リポジトリの**トレンドデータを生成する**オプションを有効にします。詳細は、エージェントリポジトリおよび IPv4/IPv6 リポジトリを参照してください。

2. スキャン層の Tenable Security Center インスタンスで、スキャンを実行してリポジトリにデータを埋め込みます。

3. レポート層の Tenable Security Center インスタンスで、スキャン層の Tenable Security Center インスタンス上の各リポジトリにリモートリポジトリを作成します。

   レポート層の Tenable Security Center が、スキャン層の Tenable Security Center リポジトリからスキャン結果データを同期します。

デフォルトでは、リモートリポジトリは毎日同期されます。Tenable Security Center API を使用することで、より頻繁にデータの更新を行うことができます。

バージョンとアップグレードの考慮事項

スキャン層およびレポート層の Tenable Security Center インスタンスは、同一の Tenable Security Center バージョンが動作している必要があります。新しいバージョンの Tenable Security Center へとアップグレードする場合、スキャン層インスタンスの前に、レポート層インスタンスを更新してください。

ハードウェアの考慮事項

最良のパフォーマンスを得るために、スキャン層およびレポート層インスタンスのハードウェアをカスタマイズします。

スキャン層インスタンス	レポート層インスタンス
スキャン層インスタンスは、次の恩恵を受けます。	レポート層インスタンスは、次の恩恵を受けます。

スキャン層 インスタンス	レポート層 インスタンス
• 高速な CPU • 高速なディスク I/O スピード アクティブスキャンとセンサーの管理を支援するために、CPU とディスク I/O のリソースの追加を検討してください。	• 大容量で高速な RAM • 大容量のディスクスペース レポート、ユーザー管理、およびデータのクエリを支援するために、RAM とディスクスペースの追加を検討してください。 Tenable では、100,000 個のアクティブな IP アドレス毎に 128 GB の RAM (たとえば、150,000 個の IP アドレスの場合は 192 GB の RAM の割り当て) を推奨しています。

詳細は、パフォーマンスを参照してください。

ユーザーアクセス制御を計画する

ユーザーに、スキャン層およびレポート層インスタンスの目的に合わせたアクセス権を付与します。

スキャン層 インスタンス	レポート層 インスタンス
次のユーザーのためのアカウントを作成します。 • インスタンスの管理上の設定を変更する必要のある技術ユーザー • スキャンを設定し、実行する必要のある技術ユーザー • 組織全体の分析レポートを作成する必要のある技術ユーザー	次のユーザーのためのアカウントを作成します。 • リポジトリや階層設定を管理する必要のあるテクニカルユーザー • 脆弱性分析のための累積データやトレンドデータを一元的に把握する必要があるビジネスユーザー

アクセス制御

関連記事: *Tenable Security Center ユーザーガイド* のユーザーアクセス

Tenable Security Center のユーザーアクセスモデルは、ロールベースのアクセス制御 (RBAC) の基本方針に対応しています。各ユーザーに対して、*グループメンバーシップ* (データアクセス用) および*ロール* (アプリケーションアクセス用) が規定されます。これは同じチームに所属するユーザーが (共有グループ内で) 同じデータにアクセスしながら、異なる機能を実行するために (ロール毎に) 異なるレベルのアクセス権を持つためのものです。グループとユーザーのセットを含む、*組織*を構成できます。組織では、独自のリソースが割り当てられたユーザーとグループの個別のセットを考慮できます。この機能を使用して、会社の組織構造を Tenable Security Center の中に複製することができます。

たとえば、次のことが可能です。

- 脆弱性管理シニアエンジニアに、完全なセキュリティマネージャーのアクセス権を付与する
- 役員にはアクセス権を付与しないが、ARC をエクスポートして共有するようセキュリティマネージャーに指示する
- セキュリティエンジニアに API エクスポートのアクセス権を付与する
- セキュリティエンジニアに API 統合のアクセス権を付与する

アクセス制御と API

Tenable Security Center API へのアクセスはユーザーベースです。これにより、事前に構築された統合とカスタム統合の両方で、RBAC ユーザーモデルを利用することができます。詳細は、API の使用方法を参照してください。

アクセス制御とリポジトリ

スキャン結果データを Tenable Security Center に格納するには、*リポジトリ*を設定します。Tenable は、大規模なデータセット (数万の IP アドレス) を複数のリポジトリに分割することを推奨しています。

- 素早いデータのインポートおよびクエリの実行
- ユーザーアクセスのコントロールと柔軟性の向上
- 報告のコントロールと柔軟性の向上
- 最大リポジトリサイズ (32 GB) に関連する潜在的な問題への対応

リポジトリの組織化

ニーズに応じて、いろいろな方法でリポジトリを組織化できます。例:

- 企業内の部門や部署ごとに、企業構造を超えた報告を簡素化
- 論理的なネットワーク定義により、集中管理された IT 部門や非連合企業の特定のニーズに対応

リポジトリの容量

1 つのリポジトリには 32 GB のデータを保存することができますが、これは資産の種類や認証スキャンを実行しているかどうかに応じて、約 30,000 から 100,000 の IP アドレスに相当します。

リポジトリの組織化を計画している場合は、各リポジトリに格納される IP アドレスの数を概算してください。もし概算結果が上限に近づいているリポジトリがあれば、そのリポジトリを 2 つ以上のリポジトリに分割してください。データのインポート後に、そのデータを別のリポジトリに移動することはできないため、Tenable では、リポジトリのサイズに余裕を持たせることをお勧めします。

統合

Tenable Security Center は、お客様のネットワーク内で最大限の機能を発揮するために、さまざまなサードパーティ製品との統合をサポートします。Tenable がサポートする統合機能については、https://jp.tenable.com/partners/technology またはドキュメントを参照してください。

Tenable Security Center 内のデータを強化して、企業で使用する他のプラットフォームに Tenable Security Center のデータを共有するために、ほとんどの統合で Tenable Security Center API が使用されます。

統合を Tenable Security Center の大規模デプロイメントで使用する場合は、次のベストプラクティスを考慮してください。

- Tenable が対応する統合であることを確認してください。Tenable サポートは、サードパーティのベンダーが管理する Tenable Security Center 統合機能についてはサポートしません。
- お使いの Tenable Security Center が環境要件に適合することを確認してください。
- サードパーティ製品の構成が、Tenable Security Center デプロイメントの規模や想定されるデータフローに対応できるかを確認してください。
- Tenable Security Center とサードパーティ製品のテストインスタンスを維持し、アップグレードのリスクを最小限に抑えます。変更を実稼働環境に展開する前に、アップグレードと構成変更をテストインスタンス上で試験してください。

社内のプラットフォームやツールのカスタム統合については、Tenable Professional Services にお問い合わせください。

API の使用方法

Tenable Security Center API は、JSON 形式でデータを提供する Tenable Security Center 機能への RESTful インターフェースです。開発者は多くの場合 REST API を使用して、Tenable Security Center を他のスタンドアロンまたはウェブアプリケーションと統合します。管理者は、Tenable Security Center サーバーとのやり取りをスクリプト化するために REST API をよく使用します。

詳細については、次を参照してください。

- Tenable Security Center API ガイド
- Tenable Security Center API ベストプラクティスガイド
- 共通機能に関する Python SDK ガイド

API を Tenable Security Center の大規模デプロイメントで使用する場合は、次のベストプラクティスを考慮してください。

- 処理の観点から見ると、ユーザーインターフェース経由で開始されたタスクと、API 経由で開始されたものでは、完了までにかかる時間は同じです。
- Tenable Security Center は、ユーザーの API アクセスとユーザーインターフェースのアクセスに同じ RBAC システムを使用しています。
- Tenable では、アクセス高速化のためのマルチスレッドの API 呼び出しは推奨していません。
- Tenable では、`/scanResult` エンドポイントから個別の結果を解析するのではなく、`/analysis` エンドポイントからデータを引き出すことを推奨しています。
- Tenable Security Center からデータを送信または要求する API コールの頻度を設定する際には、データが変更される可能性が高いことを考慮してください。たとえば、スキャンを週次でしか行っていない場合は、データを 1 時間おきに引き出す必要はありません。

注意： Tenable は、プロトコルまたは実装を拡張する際に後方互換性を維持しない場合があります。結果として、一部の API で構造または機能が変更される可能性があります。**API は、将来の互換性の保証なしで提供されます。**

Tenable サポート では、API を使用したカスタム実装に関しては支援していません。カスタムデザインや実装のサポートについては、Tenable Professional Services にお問い合わせください。

スキャン戦略を計画する

Tenable Security Center デプロイメントのスキャン戦略を計画する際は、次の点について考慮してください。

- ネットワークスキャンのカバレッジ
- アセスメントスキャンの方法
- スキャン時間に影響を及ぼす変動要素
- データフロー

ネットワークスキャンのカバレッジ

関連記事: *一般要件ガイド*のTenable Security Center のハードウェア要件とライセンス要件

ほとんどの企業では、ネットワーク上に数多くのテクノロジーがあるため、ネットワークにある資産の全容 (および総数) を掴むことが難しくなっています。お客様のネットワークにも、多様なハードウェア、オペレーティングシステム、ソフトウェア、およびインフラ用途の資産が含まれているかもしれません。

Tenable Security Center は主として IP アドレスベースのツールです。Tenable Security Center のデータ、スキャン、クエリ、およびレポートの多くは、資産の IP アドレスに基づいています。ネットワーク上の資産の IP アドレス数は、ネットワークサイズとライセンス付与を議論する際の主要なデータの尺度となっています。

Tenable Security Center を初めてご使用になる場合は、現在ネットワーク上で追跡している資産よりも多くの資産に対応できるように、Tenable Security Center を展開することを検討してください。別の製品からの資産インベントリがある場合、これまでに確認されていない資産 (たとえば未知のシステム、追跡されていないシステム、複数の IP アドレスを使用中のシステム) を考慮するために、Tenable では通常、合計の資産数を 20% ~ 30% 増加させることを推奨しています。正確な増加率はさまざまですが、ネットワークサイズを見積もる上で、まずは 20 ~ 30% とするのが良いでしょう。

ヒント: 検出スキャン (たとえば、ホスト検出テンプレートで設定されたスキャンや、検出モードの Tenable Nessus Network Monitor インスタンス) を実行して、実際の IP アドレス数をより正確に推定することもできます。

Tenable Security Center インスタンスの設定

ネットワークサイズを概算した後、Tenable Security Center の単一のインスタンスは適切に展開およびスケーリングされた場合に、150,000 個 ~ 200,000 個の IP アドレスに対応できることに留意してください。

*階層化されたリモートリポジトリ*設定では、リモートリポジトリを使用して複数の Tenable Security Center インスタンス間でデータを共有します。

- 100,000 個 ~ 249,999 個のホストに対応する場合、Tenable では階層化されたリモートリポジトリ設定を推奨しています。
- 250,000 個以上のホストに対応する場合は、Tenable では階層化されたリモートリポジトリ設定が**必要**です。

階層化された Tenable Security Center インスタンスは、Tenable Security Center デプロイメント全体の中で非公式な役割を果たします。Tenable では、最低 1 つの指定されたレポート用の Tenable Security

Center と、ネットワーク上のホスト 100,000 個 ~ 150,000 個ごとに 1 つの追加 Tenable Security Center インスタンスを推奨しています。

詳細は、階層化されたデプロイメントを参照してください。

アクティブスキャン

アクティブスキャンを実行する場合、Tenable Nessus スキャナーのデプロイメントは、お客様のネットワークアーキテクチャ独自のニーズに応えられるよう、柔軟性を持った設計となっていることに留意してください。さまざまな方法で、Tenable Nessus のカバレッジを最適化することができます。たとえば、以下の設定が可能です。

- IP アドレス 50 個を含む遠隔地の低帯域ネットワークエリアに対応する 1 つのスキャンゾーン専用の 1 つのスキャナー
- IP アドレス 50,000 個を含むフラットなネットワークエリアに対応する多数のスキャンゾーン専用の 10 個のスキャナー

Tenable では、お客様のネットワークアーキテクチャ独自のニーズに適合するよう、Tenable Nessus スキャナーのデプロイメントをカスタマイズすることを推奨しています。詳細は、*Tenable Nessus ユーザーガイド* のデプロイメント時の注意点を参照してください。

スキャナーの配置に関する詳細は、アセスメントスキャンの方法を参照してください。

アセスメントスキャンの方法

関連記事: *Tenable Security Center ユーザーガイド*のスキャンの概要

資産の評価には主に、*アクティブネットワークスキャン*と*エージェントスキャン*の 2 つの方法があります。

- アクティブ – Tenable Nessus または Tenable Vulnerability Management スキャナーを使用して、定義されたネットワークとターゲットを評価し、スキャンデータを Tenable Security Center に送信します
- エージェント – エンドポイントにインストールされた軽量エージェントを使用して、Tenable Nessus Manager または Tenable Vulnerability Management にスキャンデータを送信します

各タイプの利点と制限については、*Tenable Nessus Agent デプロイメントとユーザーガイド* の利点と制限を参照してください。

ターゲットに応じて、アセスメントスキャンの方法を選択します。完全に対応し、企業のリスクを適切に評価するためには、必要に応じて両方の方法 (異なるターゲットタイプを異なる方法でスキャン) を実行します。

例

エージェントスキャンは、ネットワーク上に稀にしか存在しない (あるいは複数のネットワークの間を移ってゆく) システムに適しています。Tenable Nessus Agents はどこからでもレポートすることができ、想定されるネットワーク内に留まる必要はありません。

アクティブネットワークスキャンは、データセンターに接続されているシステムを評価するために、ほとんどの環境に適しています。これらのシステムには通常、多くのリッスンしているネットワークサービスがあり、常に実行中です。ネットワークベースのアセスメントスキャンは、各サービスを個別に評価し、システムが高負荷で利用されていない特定の時間にスケジュールすることが可能です。

ヒント: その他のニーズ向けに、Tenable Security Center Continuous View は Tenable Nessus Network Monitor を介したパッシブスキャンおよび LCE を使用したイベントログ記録にも対応しています。

アクティブスキャンでのスキャンゾーン

関連記事: *Tenable Security Center ユーザーガイド* のスキャンゾーン

完全なアクティブスキャンの設定には、スキャンゾーンが含まれます。これは 1 つ以上のスキャナーを、ネットワークの特定の領域へと関連付けます。あるゾーン内にある IP アドレスのスキャンでは、そのゾーンに割り当てられたスキャナー間で、負荷が分散されます。これをカスタマイズすることで、お客様独自のネットワークトポロジーに対応できます。たとえば、次のことが可能です。

- 事業部ごとに 1 つのゾーンを作成し、各ゾーンに 1 つのスキャナーを追加する
- 1 つの大きなゾーンを作成し、そのゾーンに複数のスキャナーを追加する
- 分離されたネットワーク (低帯域幅または高レイテンシ接続によって分離されたネットワーク) 用のゾーンを作成し、そのゾーンに 1 つのスキャナーを追加し、そのスキャナーを分離されたネットワーク内へと展開する

スキャンゾーンは、企業における Tenable Security Center のデプロイメントの成功に極めて重要です。スキャナーをスキャンゾーンへ割り当てることで、許可されたネットワークの範囲をスキャンするようにスキャナーを制限し、ファイヤーウォール経由で、または WAN リンクを超えてスキャンを行うことで発生する問題を回避します。

デプロイメントの例

スキャンゾーンの IP アドレスは、単一の IP アドレス、IP アドレスの範囲、または CIDR 表記のサブネットとして指定できるので、論理グループ、物理的な場所、または IP アドレスの範囲によってネットワーク上のスキャンをセグメント化することができます。

一般に、大規模かつフラットなネットワークでは、Tenable Security Center がスキャン負荷を自動的にスキャナー全体に分散できるため、複数のスキャナーが最も効率的です。大規模な企業では通常、中核となるネットワークにいくつかのスキャナーを展開し、より区分されたネットワーク、またはリモートのネットワークに追加のスキャナーを展開します。また、お客様独自のネットワークインフラに適した、アーキテクチャの組み合わせを設計することもできます。

最適なデプロイメントは、ネットワークおよび企業のニーズによって左右されます。あらゆる状況に対応できるデプロイメント手法は存在しません。

たとえば、30 の物理的な拠点を有する 2 つの地方銀行で、最適なデプロイメントは異なるかもしれません。

- 銀行 A: 5 つのスキャナーをデータセンター内部で展開し、ネットワークリンク経由でのみスキャンを行う
- 銀行 B: 物理的な拠点のそれぞれに 1 つのスキャナーを展開する

さらに、ネットワークサイズに基づく最適な推奨もありません。

- お客様 A: 40 個の Tenable Nessus スキャナーを導入し、合計 300,000 個の IP アドレスをスキャン
- お客様 B: 300 の物理的な拠点に 300 個の Tenable Nessus スキャナーを導入し、ローカルスキャナーの要件を満たすことで、合計 37,000 個の IP アドレスをスキャン

大規模エンタープライズデプロイメントに関する推奨事項

大規模エンタープライズデプロイメントでは、Tenable は次のことを推奨します。

- 最低でも、ゾーン内のアクティブな IP アドレス 5,000 個ごとに 1 つのスキャナーを追加する。
- 1 つのスキャナーを 1 つのゾーンに追加する。Tenable では、1 つのスキャナーを複数のゾーンに追加することは推奨していません。
- スキャンゾーンに重複する IP アドレスがある場合、自動スキャンディストリビューションを無効化する。
- 任意の IP アドレスを、お客様のネットワークの内部にあるスキャナーと外部にあるスキャナーの両方からスキャンして、その IP アドレスのデータを複数のリポジトリに格納する場合は、自動的なスキャン分散を無効にする。

エージェントスキャン

関連記事: *Tenable Nessus Agent デプロイメントとユーザーガイド* のエージェントの使用例 (高レイテンシネットワーク、モバイル / 分散型ワークフォース、堅牢化システム) と大規模デプロイメントの考慮点

Tenable Nessus Agents は、エージェントスキャナーがアクティブスキャナーと同じネットワークアーキテクチャの考慮事項によって制限されないため、Tenable Security Center デプロイメントの柔軟性を高めることができます。Tenable Nessus Agents はまた、高レイテンシネットワーク、到達できないネットワーク、および堅牢化システムに適したソリューションです。

Tenable Vulnerability Management (クラウドベース) または Tenable Nessus Manager (オンプレミス) といった中間マネージャーを介して通信するように、Tenable Nessus Agents を展開することができます。多数の Tenable Nessus Agents を展開する場合は、大規模デプロイメントにおける考慮事項を確認してください。

スキャン時間に影響を及ぼす変動要素

お客様の設定や環境には、スキャンのパフォーマンスに影響を及ぼす数多くの変動要素があります。デプロイメントを計画する際に考慮すべき、最も一般的な変動要素を下の表にまとめます。

ヒント: Tenable は、Professional Services に連絡して、Tenable Security Center の大規模デプロイメントを成功させるための共同設計を行うことを推奨します。

変数	影響
同時に行われる評価の割合	同時に評価できる IP アドレスの数は、2 つの要素に左右されます。 • 利用可能な Tenable Nessus スキャナーの数 • スキャンポリシーの**スキャンごとの同時ホストの最大数**の設定 これらの 1 つ、もしくは両方を増加させることが、同時に行われる評価の割合および全体のスキャン時間を改善するための一番の早道です。しかし、大規模エンタープライズネットワークには多くの場合、これらの値をある最大値以上に増やすことを妨げるインフラまたは技術上の制約があります。 Tenable Security Center は Tenable Nessus スキャナーにジョブをチャンクで送信し、8 個の IP スキャンセグメントがあるため、**スキャンごとの同時ホストの最大数**が 8 の倍数となる設定の検討をお勧めします。 **注意:** 実際のパフォーマンスは、ローカル環境に大きく依存します。
Tenable Nessus 環境の仕様	Tenable Nessus スキャナーは、可能な限りハードウェア要件を満たす必要があります。 まれに、性能を落とした環境に Tenable Nessus スキャナーをインストールする必要があるかもしれません。その場合は、性能を落とした Tenable Nessus スキャナーが担当するスキャン対象を限定してください。 同様に Tenable Nessus を仮想マシン上に導入する場合、20% のパフォーマンス低下を想定して仕様を調整してください。スキャンパフォーマンスが悪化してデータの破損が発生する可能性があるため、超過利用されている、またはオーバーサブスクライブされている仮想インフラには Tenable Nessus を展開しないでください。
Tenable	スキャンエンジンには、スキャンエンジンのランタイム動作を変更するために使用され

変数	影響
Nessus スキャンの設定	る、多くのパラメータがあります。これらのパラメータは、同時にスキャンできるホストの数から、並行して開くことのできる TCP セッションの数までに及びます。これらのパラメータは、お客様がエンジンのパラメータを個別に調整して、パフォーマンスを上下させることで、お使いのネットワークに適合させることができるように設計されています。
Tenable Security Center スキャンポリシーの設定	スキャンポリシーの設定では、スキャンの深度が規定されます。一般に、スキャンの深度を増加させると、スキャンの実行時間も増加します。スキャン深度を検討する際は、次のことを考慮してください。 • どんな種類のポートスキャンが実行されるか • どのポートがスキャンされるか • どんな脆弱性をスキャンするか • 認証スキャンを実行しているか • マルウェアチェック、ファイルシステムチェック、設定監査などを行うか Tenable が提供するテンプレートを使用して、対象とするチェックを行うことができます。可能なポリシー設定のすべてをカスタマイズする、カスタムポリシーを作成することもできます。
ターゲットとスキャナーの近接度	Tenable では、スキャナーをターゲットの近くに配置し、最小のレイテンシで接続することを推奨しています。レイテンシは、スキャナーとそのターゲットとの間で交換されるすべてのパケットに付加的に作用します。ネットワークレイテンシと同時実行のプラグインチェックが、最も大きな影響を与えることが多いです。 例 • ルーター、VPN、ロードバランサー、ファイヤーウォールを経由してスキャンを行うと、開いているはずのポートがブロックされたり、閉じたポートに自動応答したりして、スキャン結果の忠実度に影響を与えることがあります。 • 単一のネットワークインフラの背後にある多数のホストをスキャンすると、スキャナーとホストの間の大量のセッション交換により、装置の負荷が増大する可能性があります。
生きている	死んでいるホストのスキャンは、生きているホストのスキャンよりも時間が掛かりませ

変数	影響
ホストの数	ん。関連するホストの数が少ない IP アドレスの分布は、ホストの数が多い IP アドレスの分布よりもスキャンにかかる時間が短くなります。
ターゲットとなる設定	ネットワークサービスがほとんど公開されていないロックダウンされたシステムのスキャンは、複雑なターゲットの設定に比べて時間がかかりません。たとえば、ウェブサーバー、データベース、ホスト侵入防止ソフトを搭載した Windows サーバーは、スキャンに比較的時間がかかります。
ターゲットとなるリソース	スキャン対象で利用可能なリソースも、スキャン時間に影響を与える可能性があります。一般公開されているシステム(負荷のあるシステム)の方が、利用されていないバックアップシステムよりも、スキャンに必要な時間は長くなります。

データフロー

Tenable Security Center と Tenable Security Center Continuous View のデータフローについては、Tenable の継続的ネットワーク監視アーキテクチャの概要を参照してください。

構築済みのデプロイメントを運用可能にする

構築済みの Tenable Security Center デプロイメントを運用可能にする際は、次のことに留意してください。

- アップグレードおよび Tenable 製品のライフサイクル
- バックアップとフェールオーバー
- ログ
- セキュリティ
- パフォーマンス

アップグレードおよび Tenable 製品のライフサイクル

Tenable では、ほとんどの大規模環境に対して、Tenable 製品の最新バージョンによる機能とセキュリティのアップデートをご活用頂くために、Tenable 製品の四半期ごとの更新を推奨しています。

Tenable Security Center のアップグレードを計画し準備するには

- 新機能、バグ修正、対応するアップグレードパス、および統合製品のバージョン要件に関して、Tenable Security Center リリースノートを確認します。

  アップグレードにあたり Tenable Security Center のいくつかのバージョンをスキップする場合 (例: 5.6.2.1 から 5.12.0 へのアップグレード)、Tenable はスキップしたすべてのバージョンのリリースノートをお読みいただくことを推奨しています。スキップしたバージョンで追加された特徴や機能によっては、構成をアップグレードする必要がある場合があります。

  Tenable Security Center のバージョンによっては、以下が必要となる場合があります。

  - 完全な機能サポートのための、下流製品 (たとえば Tenable Nessus) に対する特定の最低限必要なバージョン
  - 更新されたハードウェア最小要件の一式
  - サードパーティ製品の統合のための個別のインストールまたは構成

- バックアップとフェールオーバー に記載の内容に従って、アップグレード開始前にバックアップおよびその検証を行ってください。
- アップグレードを実稼働環境に展開する前に、テスト環境で試してください。
- Tenable では、最も高い階層の Tenable Security Center インスタンスから最初にアップグレードを行うよう推奨しています。たとえば、レポート層の Tenable Security Center インスタンスをアップグレードし、次にスキャン層の Tenable Security Center インスタンスに対して行い、その後に個別のスキャナーに対して行います。

アーキテクチャの見直しとハードウェアの更新

Tenable では、3 年から 5 年ごとにアーキテクチャの見直しを行い、ハードウェアの更新を検討するよう推奨しています。基盤となる環境が変更された、あるいは規模が拡大された場合、または脆弱性のポリシーが変更された場合 (たとえば、データ保持期間を 180 日から 365 日に延長した場合) には、より頻繁に実施することをお勧めします。

Tenable 製品のライフサイクル

Tenable 製品のサポート終了 (EOS) および製品ライフ終了 (EOL) の期日に関する詳細は、Tenable ソフトウェアリリースライフサイクルマトリクスを参照してください。

バックアップとフェールオーバー

関連記事: *Tenable Security Center ユーザーガイド* の[バックアップと復元]

Tenable Security Center はすべての企業、特に大規模な企業に対して、障害復旧のために Tenable Security Center のバックアップを保持するようお勧めしています。

バックアップを計画および実行する際には、次について考慮してください。

- 一般に、リンクされたスキャナー(例: Tenable Nessus スキャナー)には脆弱性データが恒久的に保存されるわけではないため、バックアップは不要です。
- 一般に、脆弱性のトレンドのスナップショットが、Tenable Security Center デプロイメントのストレージの大部分を消費します。このデータに対して、バックアップポリシーを別途作成することを検討してください。一度 Tenable Security Center により毎夜の脆弱性の傾向スナップショットが作成されたら、そのデータは変更されません。
- Tenable では、揮発性のディレクトリ(たとえば `/opt/sc/admin/tmp` や `/opt/sc/data/scans`)のバックアップは推奨していません。
- Tenable Security Center ではディスク上のほとんどのデータを暗号化していないため、バックアップの暗号化を検討してください。

Tenable Security Center は、高可用性フェールオーバーのシナリオには対応していませんが、システムバックアップを利用したコールドスタンバイシステムを維持できます。

ログ

関連記事: *Tenable Security Center ユーザーガイド* のシステムログ

使用中の Tenable Security Center デプロイメントに関する、各種のログソースを監視する必要がある場合があります。

Tenable Security Center

ログの場所	説明
/opt/sc/admin/logs/<yyyymm>.log	通常とは異なるシステム、またはユーザーの挙動をトラブルシューティングする機能に関する詳細情報が含まれます。 同様のログアクティビティを、Tenable Security Center インターフェースでも表示できます。
/opt/sc/admin/logs/install.log	インストール時に記述されます。Tenable サポート の指示があった場合のみ、このログを確認してください。
/opt/sc/admin/logs/upgrade.log	アップグレード中に記述されます。Tenable サポート の指示があった場合のみ、このログを確認してください。

Tenable Nessus

注意: Tenable Nessus *data_directory* の場所は、*Tenable Nessus ユーザーガイド* のデータディレクトリで説明したように、オペレーティングシステムによって異なります。

ログの場所	説明
data_directory/logs/nessusd.messages	Tenable Nessus の起動とスキャンのパラメータ、および個別の IP アドレスの開始時間と終了時間が含まれます。タッチデバッグを使用することで、ログのトラブルシューティングが可能になりますが、Tenable では実稼働環境でタッチデバッグを有効にしたままにすることを推奨していません。
data_directory/logs/backend.log	バックエンドの Nessus アプリケーションプロセスが含まれます。Tenable サポート の指示があった場合のみ、このログを確認してください。

セキュリティ

関連記事: ユーザーアクセス (LDAP 認証、証明書認証、SAML 認証、WebSealを含む) と *Tenable Security Center ユーザーガイド* の暗号化強度

Tenable Security Center のセキュリティ機能と考慮事項に関して、以下の情報を確認してください。

Tenable Security Center

基本的に、Tenable Security Center は Apache により提供される、PHP で記述されたウェブアプリケーションです。ユーザーインターフェースを安全にする制御は導入されていますが、Tenable では Tenable Security Center を安全な内部ネットワーク上に展開することを推奨しています。高セキュリティ環境では、承認されたネットワークおよびシステムのみにインターフェースを制限することをお勧めします。詳細は、ポート要件を参照してください。

ユーザーの視点から見ると、Tenable Security Center はユーザーデータのやり取りおよび職務の分離に関して、ロールベースのアクセス制御モデルに対応しています。これにより、組織の脆弱性データを公表することなく、アプリケーションの管理者がタスク管理全体を制御することが可能になります。ユーザーは、ローカル認証、LDAP/AD 認証、証明書 / スマートカード認証、SAML 認証、および WebSeal 認証といったさまざまな方法で、Tenable Security Center のユーザー認証を行うことができます。ユーザー認証を含む、すべてのユーザーインターフェースによる対話は、HTTPS を介して行われます。

デフォルトの Tenable Security Center HTTPS 証明書をカスタマイズすることで、企業の要求に適合させることができます。

Tenable Nessus および Tenable Nessus Manager

ネットワークインターフェースの観点から見ると、Tenable Nessus は運用上、Tenable Security Center への接続のみを必要とします。従って、インターフェースのアクセスを、Tenable Security Center サーバーのみに制限することをお勧めします。アクセスを制限する前に、次について考慮してください。

- セットアップまたはトラブルシューティングのため、Tenable Nessus へのユーザーインターフェースによるアクセスが必要となる場合があります。
- Tenable Nessus Manager の運用には、ユーザーインターフェースのアクセスが必要です。

Tenable Security Center に接続すると、Tenable Nessus はいかなる脆弱性データや認証情報データも保存しません。Tenable Nessus はスキャンを実行し、HTTPS 接続を使用してスキャンデータを Tenable Security Center に送信します。その後、Tenable Nessus はスキャンデータを削除します。

Tenable Security Center とともに Tenable Nessus Agents を使用している場合、脆弱性データは Tenable Nessus Manager または Tenable Vulnerability Management に保存されます。

データストレージの暗号化

脆弱性データやアプリケーションデータは暗号化されませんが、認証情報は暗号化された状態で Tenable Security Center サーバーに保存されます。Tenable Security Center は PAM ソリューションとも統合しており、ネットワークスキャン中に Tenable Nessus が一元化されたパスワードストアにアクセスできるようになっています。

脆弱性データまたはバックアップデータに対する保存データの暗号化を企業で必要とする場合、Tenable ではハードウェアレベルのディスク暗号化を推奨しています。Tenable サポート では、ハードウェアレベルのディスク暗号化に対する支援は行っていません。

通信の暗号化

Tenable Security Center では、ネットワークを介する通信はすべて暗号化されます。これには、ユーザーインターフェースや API を使用したユーザーとの対話だけでなく、スキャナーの通信および Tenable との通信のすべてが含まれます。これらの暗号化をカスタマイズして、企業に特有のニーズに対応することができます。

デフォルトでは、Tenable Nessus はターゲットとの認証に暗号化されたプロトコルを使用しますが、このトラフィックの安全性は、ターゲットが認証用にサポートするプロトコルに基づきます。

製品のアップグレード

Tenable では、ほとんどの大規模環境に対して、Tenable 製品の最新バージョンによる機能とセキュリティのアップデートをご活用頂くために、Tenable 製品の四半期ごとの更新を推奨しています。

さらに、次のことが可能です。

- Tenable 製品セキュリティアドバイザリと RSS フィードで、セキュリティ関連の製品アップデートを表示。
- Tenable 製品の脆弱性の報告。Tenable では、未解決の問題への可視性を確保するために、当社のプラグインフィードで Tenable 製品の脆弱性検出を公開しています。

パフォーマンス

パフォーマンスの最適化を開始するには、次のセクションを使用してください。Tenable は、Professional Services のヘルスチェックを利用して、特定の環境や企業のプロセスに合わせて Tenable Security Center を最適化することを強く推奨します。

パフォーマンスの最適化を開始する前に、Tenable Security Center およびスキャナーのデプロイメントが一般要件ガイドに記載されている環境要件に適合することを確認してください。

Tenable Security Center

- 非常に大規模なデプロイメントでは、インスタンスをスキャン層、またはレポート層のインスタンスとして指定する必要があります。詳細は、階層化されたデプロイメントを参照してください。
- 複雑なレポート要件がある場合は、特定の機能を、頻繁なアクセス要求で非常に大量のデータを処理するように設計されたアプリケーション (たとえば SIEM) にオフロードすることを検討してください。
- スタンドアロンのインスタンスおよびレポート層のインスタンスに対しては、100,000 個のアクティブな IP アドレス毎に 128 GB の RAM (たとえば、150,000 個の IP アドレスの場合は 192 GB の RAM の割り当て) を割り当ててください。
- 特定の静的なディスク領域 (たとえばトレンドデータ) を使用しない場合は、マウントポイントを使用して、それらをより大容量で低速なストレージへとオフロードできます。
- Tenable サポート または Professional Services が特別に推奨または支援する場合を除き、すべての Tenable Security Center インスタンスについて、以下のリソース推奨事項を遵守してください。
    - 500 個以下の Tenable Security Center ユーザーアカウント
    - 50 以下の Tenable Security Center ユーザーアカウントの同時接続数
    - 50 以下の組織
    - 250 個以下の付属スキャナー
    - 200 以下のリポジトリ数

      注意: 一般に、複数の小さいリポジトリの方が、1 つの大きなリポジトリよりもパフォーマンスが高くなります (たとえば、それぞれ 5,000 個の IP アドレスを有する 5 つのリポジトリは、25,000 個の IP アドレスを有する単一のリポジトリよりも、一般的にパフォーマンスが高くなります)。

- Tenable Security Center 5.11 以降では、不要な場合にはサンプルコンテンツの作成を無効化してください(たとえば、サンプルのダッシュボードや資産)。

スキャナー

- アセスメントスキャンの方法の情報を考慮して、Tenable Nessus スキャナーネットワークが、スキャナーの環境に対して最適に配置されていることを確認してください。
- 過負荷となったスキャンに関連するパフォーマンスの問題の兆候を捉えるために、Tenable Nessus スキャナーのイベントログ記録を有効にして、ログを監視してください。
- 高パフォーマンス環境(たとえば、指定された期限までにスキャンが終了しなければならない環境)では、物理システムを通じて、または仮想環境の専用リソースプールを使用して、ハードウェアリソースを Tenable Nessus 専用に割り当ててください。
- スキャン時間に影響を及ぼす変動要素に記載されている影響を確認し、考慮してください。