Tenable Agent 11.0.x ユーザーガイド

最終更新日: 11月 27, 2025

目次

Tenable Agent 11.0.x にようこそ

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

Tenable Agents について

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

Tenable Agents は、ネットワークベースのスキャンの課題に取り組むのに役立ちます。特に、組織のセキュリティ態勢に関する情報を一貫して収集するのが不可能またはほぼ不可能な資産がある場合に役立ちます。ネットワークスキャンは、通常は選択された間隔で、または指定された時間枠で行われ、スキャンの実行時にシステムにアクセス可能でなければなりません。スキャンの実行時にノートパソコンやその他の一時的デバイスにアクセスできないと、それらのデバイスはスキャンから除外されるため、そこにある脆弱性が見過ごされてしまいます。

今日の複雑な IT 環境にあるサーバー、ポータブルデバイス、またはその他の資産に Tenable Agents がインストールされると、インストール先のホストの脆弱性、ポリシー違反、設定ミス、マルウェアを特定し、結果を管理製品に報告します。Tenable Agents は Tenable Nessus Manager または Tenable Vulnerability Management で管理できます。

詳しくは、Tenable Agents 製品ページをご覧ください。

エージェントデプロイメントのワークフロー

以下のドキュメントは、Tenable Agents をデプロイする際に推奨されているワークフローについて概説しています。

始める前に

- Tenable Nessus Manager を使用して Tenable Agents を管理する場合、Tenable Agents をデプロイする前に Tenable Nessus Manager をデプロイして設定する必要があります。詳細について

は、*Tenable Nessus ユーザーガイド*の Tenable Nessus のインストール を参照してください。

- Tenable Vulnerability Management を使用して Tenable Agents を管理している場合、事前のデプロイは不要です。

Tenable Agents をデプロイするには、以下を実行します。

1. 各ホストに、Tenable Agents をインストールします。

   このステップの一部として、エージェントをマネージャーにリンクし、そのリンクを検証します。次のステップに進む前に、リンクが成功している必要があります。

2. (オプション) マネージャーで、エージェントグループを作成します。
3. (オプション) デフォルトのエージェント設定を変更します。
4. (オプション) フリーズ期間を設定します。
5. (オプション) エージェントプロファイルを作成します。詳細については、次を参照してください。

   - エージェントプロファイル (Tenable Nessus Manager)
   - エージェントプロファイル (Tenable Vulnerability Management)

6. エージェントグループをターゲットとするスキャンを作成します。詳細については、次を参照してください。

   - スキャンの作成 (Tenable Nessus Manager)
   - スキャンの作成 (Tenable Vulnerability Management)

   このステップの一部として、エージェントに実行させるスキャンのタイプと、エージェントがマネージャーと通信する期間のスキャンウィンドウを設定します。

   指定されたエージェントグループのエージェントがこのスキャンウィンドウ中に次回チェックインすると、Tenable Nessus Manager または Tenable Vulnerability Management からスキャンポリシーがダウンロードされ、スキャンが実行され、スキャン結果がマネージャーにアップロードされます。

利点と制限

エージェントスキャンとネットワークスキャンには、資産を検出し、ネットワーク上の脆弱性を分析する際に、それぞれ独自の利点と制限があります。

簡単に言えば、ネットワークスキャンは Tenable Nessus スキャナーから始まり、スキャン対象のホストに到達しますが、エージェントスキャンはネットワークの場所や接続性に関係なくホストで実行され、ネットワーク接続の再開時にその結果をマネージャー (例: Tenable Nessus Manager または Tenable Vulnerability Management) に報告します。

ネットワークスキャンが現在の環境と要件に十分である場合は、エージェントを使用する必要はないかもしれません。ただしほとんどの企業には、ネットワーク全体を完全に可視化できるように、エージェントとネットワークスキャンを組み合わせて使用することを Tenable は推奨しています。

自社のテクノロジーインフラに最適なスキャン戦略を設計する際は、利用可能なスキャンテクノロジーのそれぞれの違いを理解することが重要です。以降のセクションでは、各スキャン方式の利点と制限について説明します。

認証なしのネットワークスキャン

認証なしのネットワークスキャン (非認証スキャンとも呼ばれる) は、システム権限なしでシステムのセキュリティを評価するための一般的な方法です。非認証スキャンは、ホストの漏洩したポート、プロトコル、サービスを列挙し、攻撃者がネットワークを危険にさらす可能性のある脆弱性と設定ミスを特定します。

利点

- 従来のエンタープライズ環境での大規模な評価に最適です。
- 外部の攻撃者がネットワーク侵入に悪用する可能性のある脆弱性を発見します (悪意のある攻撃者目線で脆弱性を発見します)。

- 制限によりエージェントが実行できないネットワークベースのプラグインを実行します。
- 認証情報の総当たり攻撃などのターゲットを決めた操作を実行できます。

制限

- 他への影響があります。つまり、テストしているネットワーク、デバイス、またはアプリケーションに悪影響を与える場合があります。
- 詳細なパッチ情報などのクライアント側の脆弱性を検出しません。
- 常にネットワークには接続されていない一時的なデバイスは、スキャンの対象とならない場合があります。

認証されたネットワークスキャン

認証スキャンとも呼ばれる認証ネットワークスキャンでは、認証されていないスキャンよりも詳細な情報が得られます。このスキャンの場合、認証情報を使用してシステムおよびアプリケーションにログインし、必要なパッチや誤った設定の正確なリストを出力します。

認証スキャンは、バージョン番号を含め、インストールされているソフトウェアを直接検索するため、次のような項目を評価できます。

- ソフトウェアの脆弱性の特定
- パスワードポリシーの評価
- USB デバイスの列挙
- ウイルス対策ソフトウェア設定のチェック

デバイスへの影響を最小限に抑えて、これらのタスクをすべて実行します。

利点

- スキャンはネットワーク全体ではなくホスト自体で実行されるため、消費するリソースは非認証スキャンよりもはるかに少なくなります。
- 他への影響がありません。つまり、テストしているネットワーク、デバイス、アプリケーションに悪影響を与えません。
- より正確な結果 (ホストにインストールされているソフトウェアとパッチの完全な列挙) が出力されま

す。

- クライアント側のソフトウェアの脆弱性が明らかになります。

制限

- スキャンされる各ホストの認証情報を管理する必要があります。
    - 大規模な企業の場合、認証スキャンを安全に実行するために必要な適切な権限とアクセス権を持つサービスアカウントの作成が大変な場合があります。
    - パスワードローテーション要件により、管理がさらに複雑になる可能性があります。

    注意: は、Tenable 主要なパスワード保管場所やパスワードマネージャーと統合することにより、認証済みネットワークスキャンのこの制限を緩和します。

- 常にネットワークに接続されているとは限らない一時的なデバイスは、スキャンの対象となりません。

エージェントスキャン

Tenable Agent スキャンは、ホストにローカルでインストールされている、軽量で必要なスペースの少ないプログラムを使用します。Tenable Agents は脆弱性、コンプライアンス、システムデータを収集し、それらの情報を Tenable Nessus Manager または Tenable Vulnerability Management に分析のために報告します。Tenable Agents は、システムおよびネットワークへの影響を最小限に抑えるように設計されているため、エンドユーザーを混乱させることなく、すべてのホストに直接アクセスできるという利点があります。

利点

- 広いスキャン範囲と継続的なセキュリティを提供
    - ネットワークベースのスキャンを実行することが実用的ではないまたは可能でない場所にもデプロイできます。
    - インターネットに断続的に接続する、ネットワーク外の資産やエンドポイント (ノートパソコンなど) を評価できます。Tenable Agents は、ネットワークの場所に関係なくデバイスをスキャンし、結果をマネージャーに報告できます。
- 認証情報の管理が不要
    - 実行にホストの認証情報を必要としません。そのため、認証情報が変更されたときにスキャン設定の認証情報を手動で更新したり、管理者、スキャンチーム、企業内で認証情報を共

有したりする必要はありません。

- ドメインコントローラー、DMZ、認証局 (CA) ネットワークなど、リモートの認証アクセスが望ましくない場所にもデプロイできます。

- 効率的
  - ネットワークスキャンのオーバーヘッドを全体的に削減できます。
  - ローカルホストリソースに依存するので、パフォーマンスオーバーヘッドが最小ですみます。
  - ネットワーク帯域幅の必要量が減ります。これは、低速ネットワークで接続されているリモート設備にとって重要です。
  - セグメント化されたネットワークまたは複雑なネットワーク上にあるスキャンシステムの課題を排除します。
  - Tenable Agents は再起動やエンドユーザーの操作なしで自動的にアップデートできるため、メンテナンスが最小ですみます。
  - ネットワークにほとんど影響を与えずに大規模な同時並行エージェントスキャンを実行できます。
- デプロイメントとインストールが簡単
  - すべての主要なオペレーティングシステムに Tenable Agents をインストールして操作できます。
  - ノートパソコンなどの一時的なエンドポイントを含め、どこにでも Tenable Agents をインストールできます。
  - Microsoft の System Center Configuration Manager (SCCM) などのソフトウェア管理システムを使用して Tenable Agents をデプロイできます。

制限

エージェントはネットワークチェックを実行するように設計されていません。そのため、エージェントスキャンのみをデプロイする場合、特定のプラグイン項目はチェックまたは取得できません。ネットワークスキャンとエージェントベースのスキャンを組み合わせれば、このギャップを埋めることができます。

- エージェントは、DB サーバーへのログイン、デフォルトの認証情報 (総当たり) の試行、トラフィック関連の列挙など、リモート接続を通じてのみ実行できる操作を実行できません。

- エージェントがスキャン前にプラグインの更新を完了する十分な時間がない状況 (エージェントホストがオフになっている場合など) では、エージェントは古いプラグインセットを使用してスキャンを実行できます。これは、スケジュールされたスキャンがプラグイン更新の完了前に開始された場合、スケジュールされたスキャンがプラグインの更新よりも優先される可能性があるためです。

エージェントのユースケース

次のセクションでは、Tenable Agents のさまざまなユースケースについて説明します。

モバイルの分散型ワークフォース

Tenable では、モバイルワークフォース用にエージェントをデプロイすることを推奨しています。エージェントを使用すれば、デバイスをスキャンするために従業員が VPN を使って組織の本社ネットワークに接続する必要がなくなるためです。このシナリオで WAN または VPN 接続でアクティブスキャンを実行すると、リンク速度が遅くなったり、暗号化オーバーヘッドが高くなったり、リンクの安定性に問題が発生したりする可能性があります。しかし、エージェントを使用するとスキャン時間が数時間から数分に短縮されます。

モバイルワークフォースをサポートするために、Tenable では次のことを推奨しています。

- マネージャーを DMZ にデプロイし、エージェントが通信に使用できる公開 IP アドレスを割り当てます。エージェントとマネージャー間のすべての通信は、TLS 暗号化通信を介して行われます。
- エージェントスキャンに適切なスキャンウィンドウを設定します。スキャンウィンドウとは、エージェントがスキャンを実行し、その結果をマネージャーに報告する期間のことです。エージェントは、スキャンウィンドウが破棄された後に送信されたスキャンリクエストや結果を破棄し、システムを未スキャンとしてマークします。

  このアプローチにより、正確なセキュリティデータを確保すると同時に、重複する無関係なスキャンの必要性を減らすことができます。たとえば、従業員が 2 週間休暇を取った場合、休暇開けにキューで待機している 14 回分のスキャンを (その従業員のシステムがオフラインだった日につき 1 回) 行う必要はありません。

高遅延ネットワーク

Tenable Nessus ネットワークスキャンでは、スキャナーをスキャンターゲットの資産の近くに配置し、WAN 全体をスキャンしないようにするのがベストプラクティスでした。しかしこの戦略は、ターゲット資産にローカルの Tenable Nessus サーバーがないデプロイメントシナリオでは難しいことが判明しています。航行中の船、モバイルの軍事作戦、高遅延および低帯域幅のエリアなどがそうです。これらのネットワークは、通

常、衛星接続に依存しています。フルアクティブスキャンの実行時に、ポート、プロトコル、サービススキャンが生むネットワーク負荷により、サテライト接続が簡単にダウンしてしまう場合もあります。

Tenable Agents は、スキャンに関連するネットワークトラフィックを大幅に最小化することで、この問題を解決することができます。

Tenable Agents の使用時に送信されるデータには、3 つのタイプがあります。

- コマンドとコントロールのデータ – マネージャーから Tenable Agents に送信されるデータです。ローカルスキャンのタスクを実行するために必要な、誰が、何を、いつ、どこで、どのように関する情報を示します。このデータは、ネットワークを通過する最小のデータセットです。
- 結果データ – スキャン設定により、結果データのサイズは異なります。経験的に、コンプライアンススキャンは脆弱性スキャンよりも大きくなります。このデータは、マネージャーに送信され、集計されます。アップデートデータは、Tenable Agents を使用して送信される最大のデータタイプです。
- アップデート – Tenable Agent をインストールして Tenable Nessus Manager にリンクすると、エージェントはプラグインのフルセットをダウンロードします。初回のフルダウンロードが完了すると、エージェントは増分のプラグインアップデートのみをダウンロードします。ネットワークでコンテンツの差分のみを取得するこのアプローチは、進行中のネットワークトラフィックを大幅に削減します。また、System Center Configuration Manager (SCCM) や Yellowdog Updater Modified (YUM) などのパッチ管理システムによって、またはマネージャー自体を介して、コードのアップデートを処理することもできます。

要塞化されたシステム

エンタープライズ環境にあるシステムをスキャンする方法として、Tenable Nessus Professional などのスキャナーを使用したアクティブネットワークスキャンが長い間好まれてきました。アクティブスキャンはリモートで行われ、主要なサービスへのアクセスを必要とします (リモートレジストリへのアクセスなど)。しかしこれらは、システム要塞化の一環としてたいてい無効になっています。システムの要塞化により、アクティブスキャンによって収集されるデータが実際に制限される場合があるのです。この問題は、主要なサービスの列挙に認証情報スキャンが必要なことからさらに複雑になります。主要なデータセットにアクセスするには、昇格した権限 (root、ローカル管理者、またはドメイン管理者) が必要です。多くのセキュリティ専門家は、ネットワークでこれらの昇格された権限の使用を推奨していません。ドメインコントローラーなどさらに価値の高いターゲットでは、さらに注意する必要があります。

Tenable Agents は、システムレベルで動作するため、昇格した権限や追加のアカウントを必要としません。エージェントを使用すれば、セキュリティを低下させることなく要塞化されたシステムをスキャンできる低

リスクアプローチが可能になります。システムレベルでスキャンしながらも、認証情報の必要性は効果的に排除できます。

デプロイメントに関する考慮事項

すべての組織は、テクノロジーのデプロイメントに関してそれぞれ独自の課題に直面しています。したがって、以下に示すデプロイメントの考慮事項は、Tenable Agents をデプロイするための手順ガイドではありません。特定の製品問題に対処するには、Tenable テクニカルサポートチームに連絡してください。製品統合の要件、複雑なデプロイメントシナリオ、製品トレーニングについては、Tenable Professional Services チームに問い合わせることもできます。

以下のセクションには、デプロイメントガイダンスが含まれています。

- 一般的な考慮事項
- 大規模デプロイメントの考慮事項 (10,000 以上のホスト)

ファイルとプロセスの許可リスト

Tenable は、ファーストパーティ製およびサードパーティ製のエンドポイントセキュリティ製品 (ウイルス対策アプリケーションやホストベースの侵入防止システムなど) で、次の Tenable Agent フォルダーとプロセスを許可することを推奨しています。

Tenable Nessus プロセスの許可リスト登録の詳細については、*Tenable Nessus ユーザーガイド*のファイルとプロセスの許可リストを参照してください。

注意: Tenable では、以下にリストされているフォルダーとプロセスに加えて、ファイヤーウォールで特定の Tenable サイトを許可リストに入れることを推奨しています。詳細については、Which Tenable sites should I allow? (許可する必要がある Tenable のサイト)というKB の記事を参照してください。

Windows
フォルダー **ヒント:** Windows のインストール環境で標準以外のドライブやフォルダー構造を使用している場合は、%PROGRAMFILES% および %PROGRAMDATA% 環境変数を使用できます。
C:\Program Files\Tenable\Nessus Agent*
C:\Program Files (x86)\Tenable\Nessus Agent*

プロセス
C:\Program Files\Tenable\Nessus Agent\nasl.exe
C:\Program Files\Tenable\Nessus Agent\nessuscli.exe
C:\Program Files\Tenable\Nessus Agent\nessusd.exe
C:\Program Files\Tenable\Nessus Agent\nessus-service.exe
C:\Program Files\Tenable\Nessus Agent\nessus-agent-module.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nasl.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessuscli.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessusd.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessus-service.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessus-agent-module.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\libcrypto-3*.dll
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\libssl-3*.dll
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nasl.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nessuscli.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nessusd.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nessus-agent-module.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\agent.db
%SystemRoot%\tenable_ovaldi_2ef350e0435440418f7d33232f74f260.exe
%SystemRoot%\tenable_mw_scan_*.exe
%SystemRoot%\temp\nessus_*.bat
%SystemRoot%\tenable_ovaldi_2ef350e0435440418f7d33232f74f260.exe

%SystemRoot%\Tenable\Nessus Agent\tenable_mw_scan_*.exe
%SystemRoot%\Tenable\Nessus Agent\temp\nessus_*.bat
Linux
フォルダー
/opt/nessus_agent/sbin/*
/opt/nessus_agent/bin/*
/opt/nessus_agent/lib/nessus/*
ファイル
/opt/nessus_agent/bin/nasl
/opt/nessus_agent/sbin/nessusd
/opt/nessus_agent/sbin/nessuscli
/opt/nessus_agent/sbin/nessus-service
/opt/nessus_agent/sbin/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/libssl.so.3
/opt/nessus_agent/var/nessus/tmp/pre-install-check/libcrypto.so.3
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nasl
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessuscli
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessusd
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/openssl
/opt/nessus_agent/var/nessus/agent.db
プロセス
/opt/nessus_agent/bin/nasl

/opt/nessus_agent/bin/openssl
/opt/nessus_agent/sbin/nessusd
/opt/nessus_agent/sbin/nessuscli
/opt/nessus_agent/sbin/nessus-service
/opt/nessus_agent/sbin/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nasl
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessuscli
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessusd
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/openssl
macOS
フォルダー
/Library/NessusAgent/run/sbin/*
/Library/NessusAgent/run/bin/*
ファイル
/Library/NessusAgent/run/bin/nasl
/Library/NessusAgent/run/sbin/nessusd
/Library/NessusAgent/run/sbin/nessuscli
/Library/NessusAgent/run/sbin/nessus-service
/Library/NessusAgent/run/sbin/nessus-agent-module
/Library/NessusAgent/run/sbin/nessusmgt
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nasl
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessuscli

/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessusd
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessus-agent-module
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/openssl
/Library/NessusAgent/run/var/nessus/agent.db
プロセス
/Library/NessusAgent/run/bin/nasl
/Library/NessusAgent/run/bin/openssl
/Library/NessusAgent/run/sbin/nessusd
/Library/NessusAgent/run/sbin/nessuscli
/Library/NessusAgent/run/sbin/nessus-service
/Library/NessusAgent/run/sbin/nessus-agent-module
/Library/NessusAgent/run/sbin/nessusmgt
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nasl
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessuscli
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessusd
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessus-agent-module
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/openssl

一般的な考慮事項

Tenable Agents をデプロイする前に確認する必要がある、いくつかの一般的な質問を次に示します。

注意: これらのデプロイメントに関する考慮事項に加えて、Tenable は Tenable Agent のGeneral Best Practices.を確認することを推奨しています

- Tenable Agent をデプロイする予定のオペレーティングシステムは何ですか?
    - Linux (Debian/RHEL/Fedora/Ubuntu)
    - Windows (Win 10、Win Server 2012/2016 R2)
    - OS X (10.8+)
- Tenable Agents をいくつデプロイすることを計画していますか?
    - 1,000 未満
    - 1,000 以上 5,000 未満
    - 5,000 以上 10,000 未満
    - 10,000 以上

    注意: 10,000 を超えるエージェントのデプロイメントシナリオでは、大規模デプロイメントで説明されているように、エージェントグループのサイジングとスキャンスタガリングによるパフォーマンスの最適化を検討してください。
- Tenable Agents をインストールするホストの一般的なハードウェア仕様は何ですか?たとえば、ディスク容量、ディスクの種類と速度、CPU、コア、RAM を考慮します。
- Tenable Agent から Tenable Nessus Manager への出力通信を防ぐような対策がホストに存在しますか (DST: TCP/8834 [デフォルト、カスタマイズ可能])?
- エージェントプロセスの実行を防ぐような対策がホストに存在しますか?

    注意: オペレーティングシステムごとに許可するファイルとプロセスのリストについては、ファイルとプロセスの許可リストを参照してください。
- Tenable Agents をエンタープライズ全体にどのようにデプロイする予定ですか?たとえば、Active Directory、SMS、Microsoft SCCM、Red Hat Satellite などのエンタープライズデプロイメントテクノロジーを使用しますか?
- 仮想システムまたは非永続システムに Tenable Agents をデプロイしますか?その場合は、基となるデバイステンプレートにエージェントを追加することを検討してください。所属組織の仮想/非永続ホストのコミッションとデコミッションのプロセスを確認し、Tenable Agents のアクティブ化または非アクティブ化が正しく行われたことを見届けることを Tenable は推奨しています。

- 潜在的にデプロイメント可能なエージェント資産とデプロイされたエージェントの実際の資産の比率をどのように追跡する予定ですか?
- ホスト上のエージェントのヘルスとステータスをどのように追跡する予定ですか?たとえば、条件 *x* (*x* はサービスのステータスまたはエージェントの登録ステータス) を監視するとします。その状態が発生する場合は、アクションまたは通知がトリガーされます。
- デプロイされたエージェントが存在するインフラに最適な命名スキーマはどれですか?エージェントを実行しているホストの内訳を整理する方法を計画することが重要です。
- ネットワークスキャンでエージェントベースのスキャンを補完する予定ですか?エージェントスキャンとネットワークスキャンで脆弱性情報をどのように維持する予定ですか?複数のリポジトリをどのように管理する予定ですか?

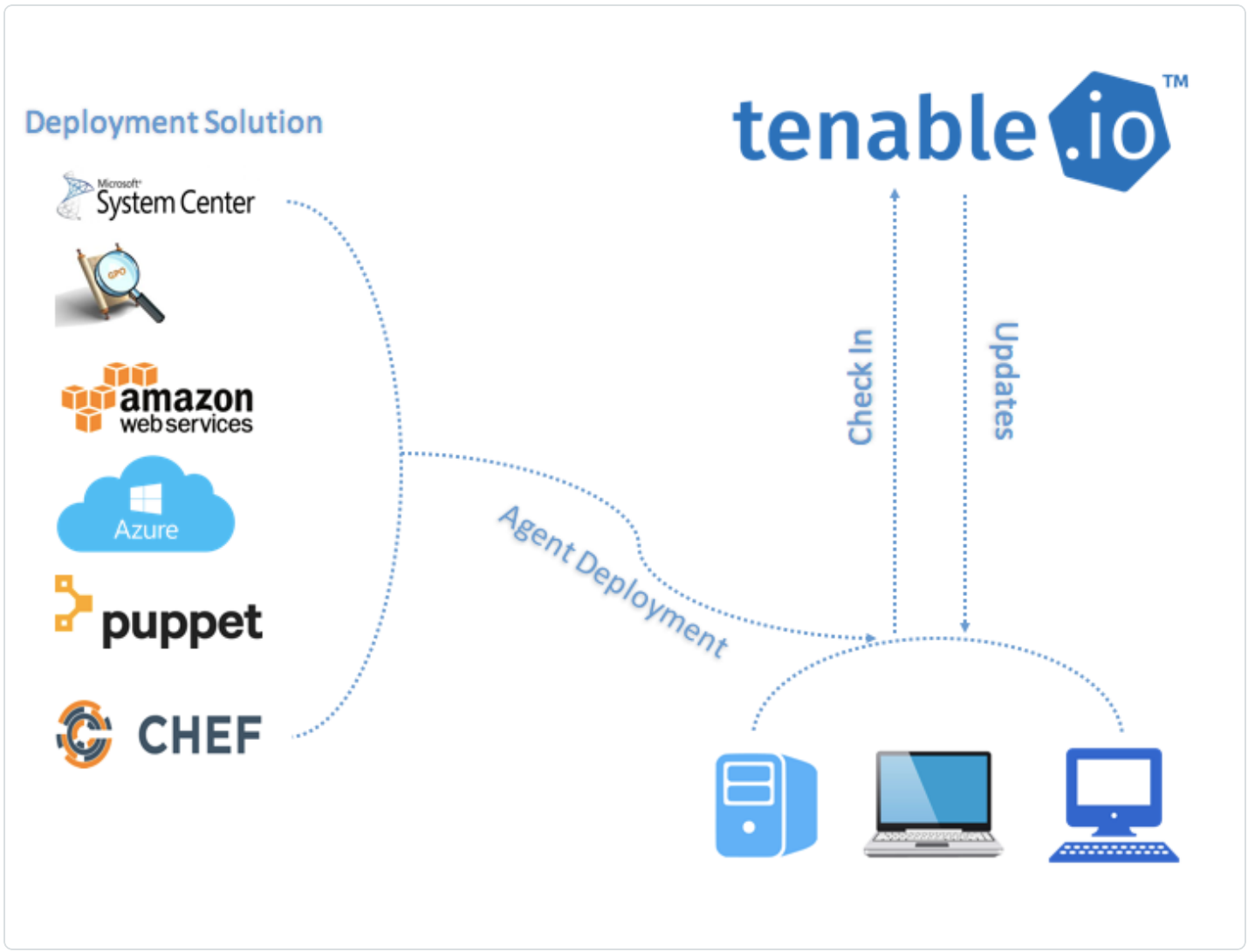
大規模デプロイメントに関する考慮事項

大規模な環境にエージェントをデプロイする場合、すべてのエージェントが継続的にアクティブであり、Tenable Vulnerability Management または Tenable Nessus Manager に接続された状態を保つようなデプロイメント戦略にする必要があります。

> **注意:** これらのデプロイメントに関する考慮事項に加えて、Tenable は Tenable Agent のGeneral Best Practices.を確認することを推奨しています

デプロイメント戦略

多数のエージェントをデプロイする場合は、ソフトウェアを使用してネットワーク経由でエージェントをプッシュすることを検討してください。例



Tenable は、多数のエージェントをデプロイするときは、24 時間かけてエージェントをバッチ処理でデプロイすることを推奨しています。この方法は、ネットワーク帯域幅が制限されており、ネットワークが一度にダウンロードするデータの量を制限する必要がある場合に特に役立ちます。

インストール後、エージェントが評価を実行する指示を受けると、最初のプラグインアップデートを受け取ります。エージェントは、最初のプラグインアップデート時刻から 24 時間後に次のアップデートを試行するようにタイマーを設定します (後続のプラグインダウンロードが成功すると、プラグインアップデート日が更新されます)。エージェントをバッチ処理でデプロイすると、過剰な数のエージェントが一度に製品のアップデートをチェックし、帯域幅が過剰に消費されることも回避できます。

エージェントは、0 ~ 5 分のランダムな遅延の後に Tenable Nessus Manager または Tenable Vulnerability Management にリンクします。この遅延は、エージェントが最初にリンクするとき、およびエージェントが手動またはシステムの再起動によって再起動するときにも発生します。遅延を強制すると、大

量のエージェントをデプロイまたは再起動する際のネットワークトラフィックを削減し、Tenable Nessus Manager または Tenable Vulnerability Management に対する負荷を軽減できます。

クラスタリング

Tenable Nessus Manager のクラスタリングを使用すると、単一の Tenable Nessus Manager インスタンスから多数のエージェントをデプロイおよび管理できます。10,000 ~ 200,000 のエージェントを持つ Tenable Security Center ユーザーの場合、Tenable Nessus Manager の複数のインスタンスを Tenable Security Center にリンクせずに、単一の Tenable Nessus Manager クラスタからエージェントスキャンを管理できます。

クラスタリングが有効になっている Tenable Nessus Manager インスタンスは*子ノードの親ノード*として機能し、それぞれが少数のエージェントを管理します。Tenable Nessus Manager インスタンスが親ノードになると、エージェントを直接管理しなくなります。代わりに、子ノード全体にわたるすべてのエージェントのスキャンポリシーとスケジュールを管理できる単一のアクセスポイントとして機能します。クラスタリングを使用すると、複数の異なる Tenable Nessus Manager インスタンスを個別に管理する場合よりも簡単にデプロイメントサイズを調整できます。

シナリオの例: 100,000 のエージェントをデプロイする

Tenable Security Center ユーザーの担当者が、Tenable Nessus Managerに管理されている 100,000 のエージェントをデプロイするとします。

*クラスタリングを使用しない*場合、それぞれが 10,000 のエージェントをサポートする、10 個の Tenable Nessus Manager インスタンスをデプロイします。エージェントスキャンポリシーとスケジュールの設定、ソフトウェアバージョンの更新など、各 Tenable Nessus Manager インスタンスを個別に手動で管理する必要があります。各 Tenable Nessus Manager インスタンスを、Tenable Security Center に個別にリンクする必要があります。

*クラスタリングを使用する*場合、1 つの Tenable Nessus Manager インスタンスを使用して 100,000 のエージェントを管理します。Tenable Nessus Manager でクラスタリングを有効にすると、それが親ノードとなり、子ノードの管理ポイントに変わります。10 個の子ノードをリンクし、それぞれが約 10,000 のエージェントを管理します。新しいエージェントをリンクするか、クラスタに既存のエージェントを移行できます。子ノードは、親ノードからエージェントスキャンポリシー、スケジュール、プラグイン、ソフトウェアの更新を受け取ります。Tenable Nessus Manager 親ノードのみを Tenable Security Center にリンクできます。

注意: クラスタ内のすべての Tenable Nessus ノードは、同じバージョンである必要があります (たとえば上記のクラスタの例を使用する場合、Tenable Nessus Manager 親ノードと 10 個の子ノードは同じ Tenable Nessus バージョンである必要があります)。バージョンが異なる場合、クラスタのデプロイメントはサポートされません。

詳細は *Tenable Nessus ユーザーガイド*のクラスタリングを参照してください。

エージェントグループ

Tenable Nessus Manager または Tenable Vulnerability Management でスキャンを管理し、スキャンデータを Tenable Security Center にインポートする場合は特に、エージェントグループのサイズを適切に設定することをお勧めします。Tenable Nessus Manager または Tenable Vulnerability Management でエージェントを管理すると、エージェントグループのサイズを設定できます。

スキャンして単一のエージェントグループに含めるエージェントが増えるほど、マネージャーが 1 つのバッチで処理するデータが増えます。エージェントグループのサイズに応じて、Tenable Security Center にインポートする必要がある .nessus ファイルのサイズが決まります。.nessus ファイルのサイズは、ハードドライブの容量と帯域幅に影響します。

グループのサイジング

製品	グループごとに割り当てられるエージェント
Tenable Vulnerability Management	Tenable Security Center に送信しない場合、グループあたりのエージェントは無制限 Tenable Security Center に送信する場合、グループあたり 20,000 エージェント
Tenable Nessus Manager	Tenable Security Center に送信しない場合、グループあたりのエージェントは無制限 Tenable Security Center に送信する場合、グループあたり 20,000 エージェント
Tenable Nessus Manager クラスタ	スキャンが個別の子ノードの数に応じて適切に自動的に分割されるため、無制限

注意: 1 回のスキャンで複数のエージェントグループをスキャンする場合、スキャンあたりのエージェントの合計数が、グループあたりのエージェントの合計数と一致しないことがあります。たとえば、Tenable Vulnerability Management に 7,500 のエージェントのグループが 3 つあり、すべてが 1 回のスキャンで行われる場合、22,500

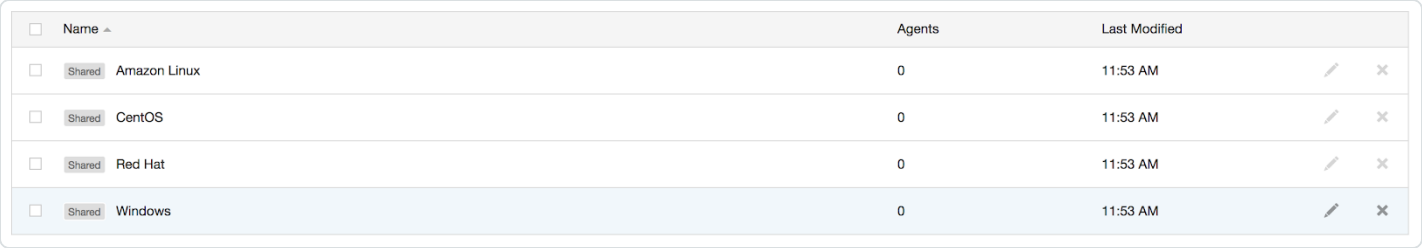
のエージェントのデータが一度に Tenable Security Center にインポートされるため、すべてを対処しきれない可能性があります。

グループタイプ

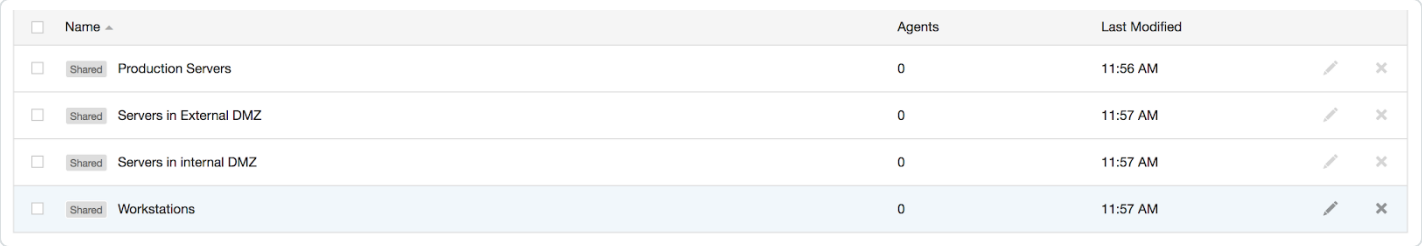
エージェントを環境にデプロイする前に、スキャン戦略に基づいてグループを作成します。

以下はグループタイプの例です。

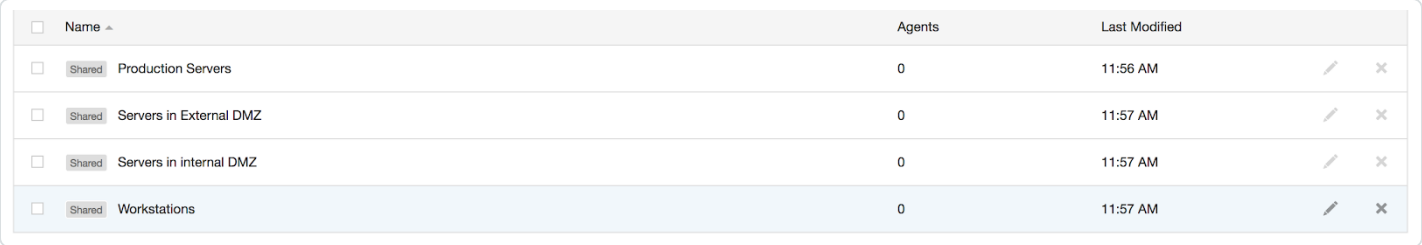
オペレーティングシステム



資産タイプまたは場所



複数のスキャン戦略がある場合は、複数のグループにエージェントを追加することもできます。



スキャンプロファイル戦略

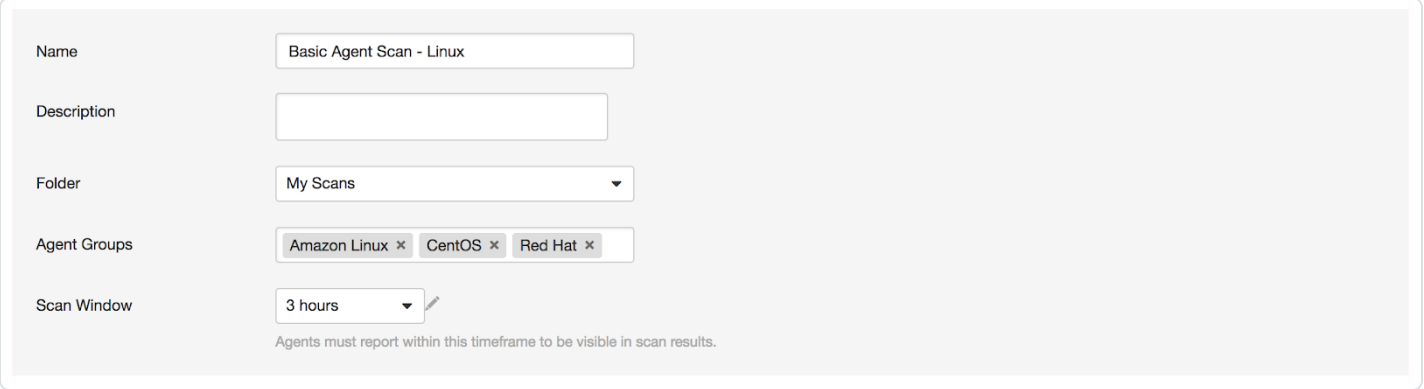
必要なすべての資産にエージェントをデプロイしたら、スキャンプロファイルを作成し、既存のエージェントグループにそれらを結び付けることができます。次のセクションでは、いくつかのスキャン戦略について説明します。

オペレーティングシステムのスキャン戦略

次の戦略は、スキャン戦略が資産のオペレーティングシステムに基づいている場合に有用です。

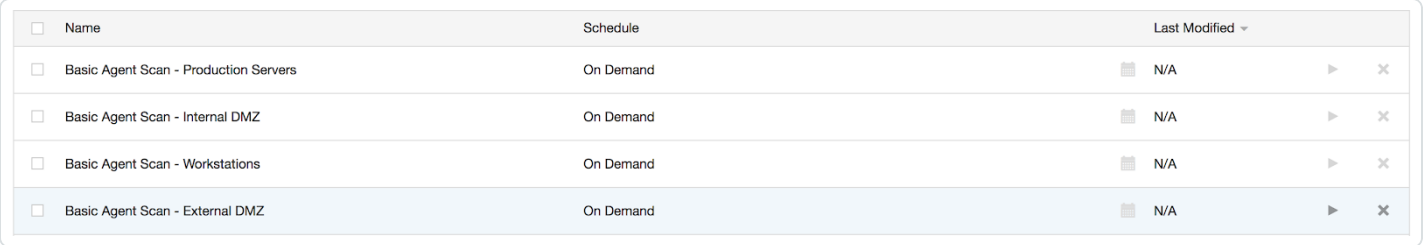
基本エージェントスキャン - Linux

この例では、スキャンは**基本エージェントスキャン**テンプレートに基づいて作成され、*Amazon Linux*、*CentOS*、*Red Hat* グループに割り当てられます。このスキャンは、これらの資産のみをスキャンします。



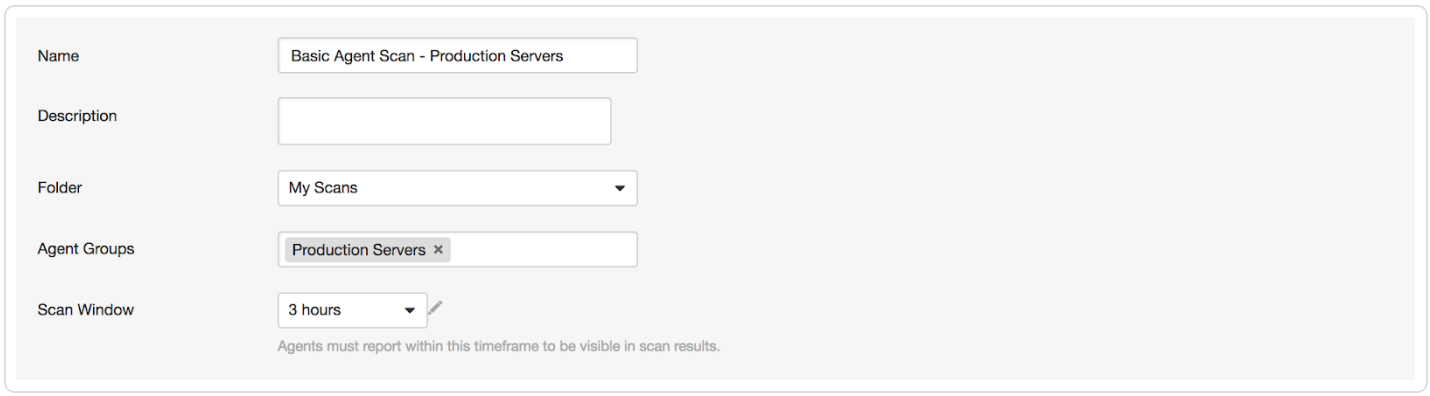
資産タイプまたは場所のスキャン戦略

次の戦略は、スキャン戦略が資産のタイプや場所に基づいている場合に役立ちます。



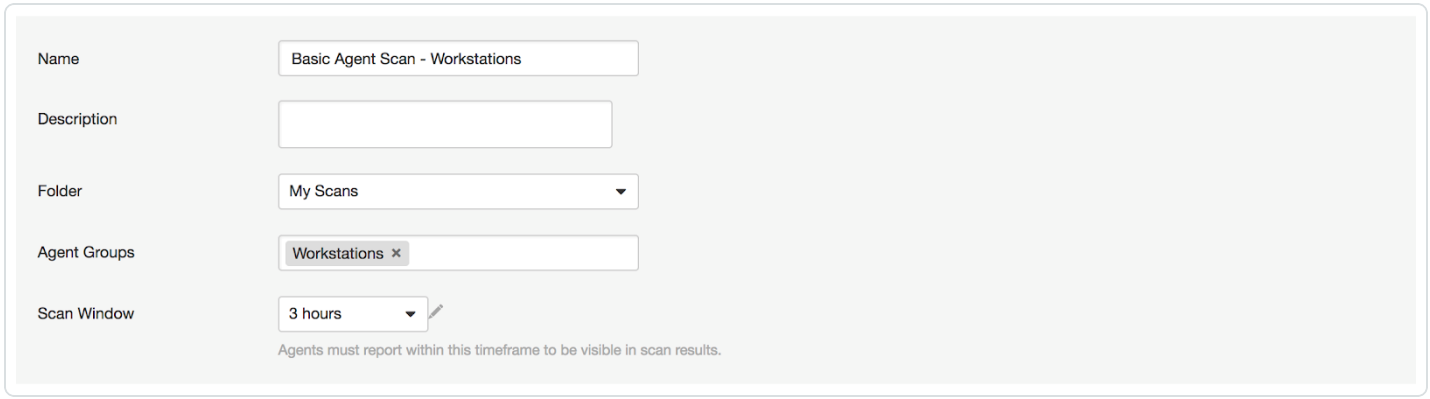
基本エージェントスキャン - 本番サーバー

この例では、スキャンは**基本エージェントスキャン**テンプレートに基づいて作成され、*本番サーバー*グループに割り当てられます。このスキャンは、本番サーバー資産のみをスキャンします。



基本エージェントスキャン - ワークステーション

この例では、スキャンは**基本エージェントスキャン**テンプレートに基づいて作成され、ワークステーショングループに割り当てられます。このスキャンは、ワークステーション資産のみをスキャンします。



注意: ほとんどの企業は、(通常 24 時間年中無休で稼働しているサーバーとは対照的に) これらのシステムがオンラインである時を保証できないため、ワークステーションスキャンではより長いスキャンウィンドウを設定することをお勧めします。

スキャンスタガリング

Tenable Agents を使用したスキャンは、多くの点でネットワークスキャンよりも効率的ですが、特定のタイプのシステムでは、スキャンスタガリングを検討することができます。

たとえば、仮想マシンに Tenable Agents をインストールする場合、複数のグループにエージェントを分散し、関連するスキャンウィンドウの開始時点を少しずらして起動させることができます。

スキャンをスタガリングすると、仮想ホストサーバーに対する 1 回の負荷が制限されます。これは、エージェントが、スキャンウィンドウの開始時に可能な限り早く評価を実行するためです。エージェントの評価がす

べてのシステムで同時に開始されると、オーバーサブスクライブの環境またはリソース制限のある仮想環境ではパフォーマンスの問題が発生する可能性があります。

Tenable Agents のベストプラクティス

以降のセクションで、ベストプラクティスのガイダンスを示します。

一般的なベストプラクティス

注意: エージェントデプロイメントのベストプラクティスと考慮事項については、デプロイメントに関する考慮事項を参照してください。

- ネットワークスキャンでは、ファイヤーウォールやスイッチなどのデバイスを通り越してスキャンしたり、バイパスしようとしたりしないでください。これらは、スキャンを複雑化したり妨げたりする造りになっているからです (ネットワークアドレス変換など)。
- すべてのセグメントでホストに最も近い場所に Tenable Nessus スキャナーを配置してください。*あるいは*システムのローカルでエージェントを実行してください。こうすれば、多くのファイヤーウォールルールを明示的に作成する必要はありません。どちらのソリューションも正しく実装されているなら、ファイヤーウォールルールが最小限でも接続可能です。
- Tenable では、ネットワークを完全に可視化するために、エージェントベースのスキャンとネットワークスキャンを組み合わせて、ネットワーク全体のリスクを特定することを推奨しています。このアプローチは米国連邦政府の組織にとって特に重要です。リスクの全範囲を評価することを要求する特有の法律や法令があるからです。
- VDI や ESXi のような共有リソース環境の場合、プラグインコンパイル中にエージェントが CPU 使用率に与える影響を最小限に抑えるため、Tenable はエージェントのプラグインコンパイルパフォーマンスを `medium` または `low` に設定することを推奨しています。

ハイブリッド環境のデータ集約

このセクションでは、Tenable Agent データを Tenable Nessus Manager から Tenable Security Center リポジトリに集約する際に考慮すべきことを簡潔に示します。Tenable Nessus Manager と通信してデータを取得する場合、その通信は Tenable Security Center から開始されることに注意してください。Tenable Agent データがインポートされると、脆弱性分析、コンプライアンス、ワークフロー自動化など、すべての通常の Tenable Security Center 操作が適用されます。

- 一度に Tenable Security Center にインポートされるデータの量を減らすには、エージェントグループのサイズを十分に検討してください。Tenable では、Tenable Nessus Manager または Tenable Vulnerability Management のスキャンあたりのエージェント数を 1,000 に制限することを推奨しています。並列操作をしながら大量のデータを Tenable Security Center にインポートすると、Tenable Security Center のパフォーマンスに悪影響を与えます。
- Tenable Nessus スキャナーと Tenable Security Center に接続されている Tenable Nessus Manager の数を適切に計画し、必要に応じて Tenable テクニカルサポートのスタッフにガイダンスを求めてください。
- エージェントスキャン (エージェントデータ取得プロセス) に含める同時並行スキャンの数、同時並行ユーザーの数、設定されているダッシュボードの数、Tenable Security Center で実行されるレポートの頻度やタイプを適切に計画し、必要に応じて Tenable テクニカルサポートのスタッフにガイダンスを求めてください。

システム要件

このセクションには、Tenable Agents のインストールに必要な要件に関連した情報が含まれます。

- ハードウェア
- ソフトウェア
- データフロー
- ライセンス
- エージェントの CPU リソースコントロール
- パフォーマンスメトリクス
  - Tenable Agent のパフォーマンス
    - ソフトウェアフットプリント
    - エージェントのライフサイクルと帯域幅
  - Tenable Nessus Manager のパフォーマンス

ハードウェア要件

Tenable Agents

Tenable Agents は、軽量のユーザースペースプログラムで、最小限のシステムリソースのみを使用します。

一般的には、エージェントが使用する RAM は 50 MB ~ 60 MB です (すべてページング可能)。ただしエージェントは、スキャン (すべてページング可能で、メモリの量はスキャン設定によって異なる) やプラグインの更新 (すべてページング可能) の際に、追加のメモリを使用します。エージェントはアイドル時には CPU をほとんど使用しませんが、ジョブの実行中には利用可能な CPU を最大 100% 使用するように設計されています。

Tenable Agent のリソース使用量の詳細については、Tenable Agent のパフォーマンスを参照してください。

次の表は、Tenable Agent の動作に推奨されるハードウェアの最小要件の概要です。Tenable Agents は、指定された同じ要件を満たす仮想マシンにインストールできます。

ハードウェア	最小要件
プロセッサー	デュアルコア CPU 1 個
プロセッサー速度	1 GHz 以上
RAM	1 GB 以上
ディスク容量	3 GB 以上 (ホストオペレーティングシステムで使用する容量は含まれていません) プラグインの更新の適用など、特定のプロセスの実行中は、エージェントにさらに多くの容量が必要になる場合があります。選択したスキャン頻度、検出結果の量、ログローテーションオプションは、エージェントのディスク使用率に影響を与えます。デプロイメントシナリオでディスク領域が主な懸念事項である場合は、最大 4 GB (ホストオペレーティングシステムによって使用される容量を除く) を割り当てることを Tenable では推奨しています。
ディスク速度	15 ~ 50 IOPS

注意: Tenable Agent のシステム上で実行されるその他のタスクに対する相対的な優先度を制御できます。詳細については、エージェントの CPU リソースコントロールを参照してください。

Tenable Nessus Manager

シナリオ	ハードウェアの最小要件
0 ~ 10,000 のエージェントがある Tenable Nessus Manager	**CPU** – 2 GHz コア x 4 **メモリ** – 16 GB RAM **ディスク容量** – 同時スキャン 5,000 エージェントあたり 5 GB **ディスク容量** – • トリガーされるエージェントスキャンのある環境の場合 – 5 MB ***x*** エージェント数 ***x*** (Tenable Nessus Manager 経由でスキャンを開始する場合は 7 日間でエージェントがトリガーされる回数 **または** Tenable Security Center 経由でスキャンを開始する場合は 2 日間でエージェントがトリガーされる回数) **+** 500 MB たとえば、次のようになります。 • スタンドアロンの Tenable Nessus Manager が 1,100 のエージェントで毎日スキャンする場合、必要なディスク容量は 5 MB x 1,100 x 7 + 500 MB = **39,000 MB** (**39 GB**) • Tenable Security Center が管理する Tenable Nessus Manager が 1,100 のエージェントで毎日スキャンする場合、必要なディスク容量は 5 MB x 1,100 x 2 + 500 MB = **11,500 MB** (**11.5 GB**) • トリガーされるエージェントスキャンのない環境の場合 – 同時スキャン 5,000 エージェントあたり 5 GB **注意:** 時の経過とともに、スキャン結果とプラグインアップデートに、より多くのディスク容量が必要になります。
10,001 ~ 20,000 のエージェントがある	**CPU** – 2 GHz コア x 8 **メモリ** – 32 GB RAM

シナリオ	ハードウェアの最小要件
Tenable Nessus Manager	**ディスク容量** – 同時スキャン 5,000 エージェントあたり 5 GB **ディスク容量** – • トリガーされるエージェントスキャンのある環境の場合 – 5 MB ***x*** エージェント数 ***x*** (Tenable Nessus Manager 経由でスキャンを開始する場合は 7 日間でエージェントがトリガーされる回数 **または** Tenable Security Center 経由でスキャンを開始する場合は 2 日間でエージェントがトリガーされる回数) **+** 500 MB たとえば、次のようになります。 • スタンドアロンの Tenable Nessus Manager が 15,000 のエージェントで毎日スキャンする場合、必要なディスク容量は 5 MB x 15,000 x 7 + 500 MB = **525,500 MB** (**525.5 GB**) • Tenable Security Center が管理する Tenable Nessus Manager が 15,000 のエージェントで毎日スキャンする場合、必要なディスク容量は 5 MB x 15,000 x 2 + 500 MB = **150,500 MB** (**150.5 GB**) • トリガーされるエージェントスキャンのない環境の場合 – 同時スキャン 5,000 エージェントあたり 5 GB **注意:** • 時の経過とともに、スキャン結果とプラグインアップデートに、より多くのディスク容量が必要になります。 • デプロイメントの規模が大きい場合は、Tenable の担当者にご連絡ください。

ソフトウェア要件

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

Tenable Agent 11.0

オペレーティン	対応バージョン	サポートされ

グシステム		るアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9 および 10	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2017、2018、2019、2020	x86_64
	Fedora 41、42	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降、10	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP3 以降	x86_64
	TencentOS	x86_64
	Ubuntu 16.04、18.04、20.04、22.04、24.04	x86_64
	Ubuntu 18.04、20.04、22.04、24.04	AArch64
macOS	macOS 13、14、15、26	x86_64 Apple Silicon

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

Tenable Agent 10.9

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2017、2018、2019、2020	x86_64
	Fedora 41、42	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP3 以降	x86_64

	TencentOS	x86_64
	Ubuntu 16.04、18.04、20.04、22.04、24.04	x86_64
	Ubuntu 18.04、20.04、22.04、24.04	AArch64
macOS	macOS 13、14、15	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022、2025	x86_64

Tenable Agent 10.8

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2017、2018、2019、2020	x86_64
	Fedora 40	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64

	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP2 以降	x86_64
	TencentOS	x86_64
	Ubuntu 16.04、18.04、20.04、22.04、24.04	x86_64
	Ubuntu 18.04、20.04、22.04、24.04	AArch64
macOS	macOS 13、14、15	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022、2025	x86_64

Tenable Agent 10.7

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

	Debian 11 および 12	x86_64
	Kali Linux 2017、2018、2019、2020	x86_64
	Fedora 38 および 39	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 7、8、および 9	x86_64 AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP2 以降	x86_64
	TencentOS	x86_64
	Ubuntu 16.04、18.04、20.04、22.04、24.04	x86_64
	Ubuntu 18.04、20.04、22.04、24.04	AArch64
macOS	macOS 12、13、14、15	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022	x86_64

Tenable Agent 10.6

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ

Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2017、2018、2019、2020	x86_64
	Fedora 38 および 39	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 6、7、8 および 9	x86_64 AArch64
	Red Hat EL 6.x および 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE 12 SP5、SUSE Enterprise 15 SP2 以降	x86_64
	TencentOS	x86_64
	Ubuntu 14.04、16.04、18.04、20.04、22.04	x86_64
	Ubuntu 18.04、20.04、22.04	AArch64
macOS	macOS 12、13、14	x86_64 Apple Silicon

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

Tenable Agent 10.5

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2023、Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 および 12	x86_64
	Kali Linux 2017、2018、2019、2020	x86_64
	Fedora 38 および 39	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 6、7、8 および 9	x86_64 AArch64
	Red Hat EL 6.x および 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64
	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE Enterprise 15 SP2 以降	x86_64

	Ubuntu 14.04、16.04、18.04、20.04、22.04	x86_64
	Ubuntu 18.04、20.04、22.04	AArch64
macOS	macOS 12、13、14	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022	x86_64

Tenable Agent 10.4

オペレーティングシステム	対応バージョン	サポートされるアーキテクチャ
Linux	AlmaLinux 8.10 および 9.5	x86_64 AArch64
	Amazon Linux 2	x86_64 AArch64
	Debian 11	x86_64
	Kali Linux 2017、2018、2019、2020	x86_64
	Fedora 34、35、36	x86_64
	Oracle Linux (Unbreakable Enterprise Kernel を含む) 6、7、8 および 9	x86_64 AArch64
	Red Hat EL 6.x および 7.9	x86_64
	Red Hat EL 8.4、8.6、8.8、8.10、9.0、9.2、9.4以降	x86_64 AArch64

	Rocky Linux 8.10 および 9.5	x86_64 AArch64
	SUSE Enterprise 15 SP2 以降	x86_64
	Ubuntu 14.04、16.04、18.04、20.04、22.04	x86_64
	Ubuntu 18.04、20.04、22.04	AArch64
macOS	macOS 11、12、13、14	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10、11	x86_64
	Windows Server 2012、2012 R2、2016、2019、2022	x86_64

注意:

- Tenable Agent は、Java などの外部ランタイム環境を必要としません。
- Microsoft Visual C++ 再頒布可能パッケージ 14.22 は、Tenable Agentと一緒にバンドルされているライセンスパッケージの一部として含まれています。
- Tenable Agent では、Windows ホストシステムで Universal Microsoft C Runtime Library (UCRT) の最新バージョンと PowerShell 5.0 以降が実行されている必要があります。Microsoft Windows の一部の古いバージョンでは、Tenable Agent が動作するための最低限の更新が必要です。
- Tenable Agent は、Linux AArch64 アーキテクチャの 4 KB ベースページサイズのみをサポートします。
- Tenable は現在、AWS Fargate 統合をサポートしていません。

SELinux の強制モードポリシーのカスタマイズ

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

Tenable サポート は SELinux ポリシーのカスタマイズのサポートはしませんが、SELinux のログを監視して、ポリシー設定のエラーとその解決策を特定することを Tenable は推奨しています。

始める前に

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

SELinux のログを監視して、エラーと解決策を特定する方法

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

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

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

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

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

ポート要件

Tenable Agent ポートの要件には、Tenable Agent 固有の要件とマネージャー固有の要件があります。デプロイメント設定に応じて、Tenable Nessus Manager と Tenable Nessus のクラスタノード および Tenable Security Center のポートの要件を参照してください。

Tenable Agent

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

送信トラフィック

次のポートへの送信トラフィックを許可する必要があります。

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

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

Tenable Nessus Manager と Tenable Nessus のクラスタノード

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

受信トラフィック

次のポートへの受信トラフィックを許可する必要があります。

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

送信トラフィック

次のポートへの送信トラフィックを許可する必要があります。

Port (ポート)	トラフィック
TCP 25	SMTP メール通知の送信
TCP 443	Tenable Vulnerability Management との通信 (sensor.cloud.tenable.com または sensor.cloud.tenablecloud.cn) プラグイン更新での `plugins.nessus.org` サーバーとの通信
UDP 53	DNS 解決の実行

Tenable Security Center

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

受信トラフィック

次のポートへの受信トラフィックを許可する必要があります。

Port (ポート)	トラフィック
TCP 22	別の Tenable Security Center とのリモートリポジトリ同期の実行
TCP 443	Tenable Security Center インターフェースへのアクセス。 Tenable Security Center Director インスタンスとの通信 OT Security インスタンスとの通信 別の Tenable Security Center とのリモートリポジトリ同期を行うための最初のキープッシュの実行 API とのインタラクション
TCP 8837	Sensor Proxy との通信。

送信トラフィック

次のポートへの送信トラフィックを許可する必要があります。

Port (ポート)	トラフィック
TCP 22	他の Tenable Security Center インスタンスからのリポジトリの同期。
TCP 25	SMTP メール通知の送信
TCP 389	顧客が管理する LDAP サーバーとの通信
TCP 443	同期のための Tenable One との通信 プラグイン更新での `plugins.nessus.org` サーバーとの通信
TCP 465	SMTP メール通知の送信
TCP 587	SMTP メール通知の送信
TCP 636	顧客が管理する LDAP サーバーとの通信
TCP 8834	Tenable Nessus との通信。
TCP 8835	Tenable Network Monitor との通信。
UDP 53	DNS 解決の実行

注意:Tenable Security Center インスタンスがオフラインインスタンスとして設定されていない場合は、Which Tenable sites should I allow? (許可する必要があるかもしれない [] のサイト)にリストされている Tenable ウェブサイトへの送信トラフィックも許可する必要があります。を参照してください。

Tenable 更新サイトとの間のトラフィックの SSL 検査はサポートされていません。更新サイトへのアクセスは確立できますが、トラフィックの SSL 検査が原因で更新を完了できない場合があります。

エージェントコンテンツ配信ネットワーク (CDN)

採用しているルールロジックによっては、エージェントコンテンツ配信ネットワーク (CDN) を利用するために、ファイヤーウォールまたはプロキシルールの調整が必要になる場合があります。

FQDN の更新

CDN は、`sensor.cloud.tenable.com` を使用してプラグインとバイナリアップデートをダウンロードし、スキャン結果をアップロードし、Tenable Vulnerability Management とのリンクおよび通信を行います。ファイヤーウォールまたはプロキシルールが `sensor.cloud.tenable.com` に対して設定されていれば、問題は発生しません。ただし、より厳格なルールがある場合は、ルールセットを更新する必要があります。

IP 許可リスト

sensor.cloud.tenable.com に関連付けられた IP アドレスは動的であり、エージェントのロケールとインターネット接続に依存しています。現在、プロキシおよびファイヤーウォールに IP ベースのルールを設定している場合、Amazon CloudFront が使用する IP 範囲に基づいてルールを更新する必要があります。Amazon のドキュメントの CloudFront エッジサーバーの場所と IP アドレス範囲には、ダウンロードできる IP 範囲のリストが掲載されています。

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

ライセンス要件

Tenable Agents は、それらを管理する製品 (Tenable Nessus Manager または Tenable Vulnerability Management) を通じてライセンス付与されます。

Tenable Nessus Manager

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

Tenable Nessus のインストールプロセスを開始してセットアップを行う前に、アクティベーションコードを取得する必要があります。

アクティベーションコード

- **ワンタイム**コードです。ただし、ライセンスまたはサブスクリプションが変更された場合は、Tenable が新しいアクティベーションコードを発行します。
- 発行後 24 時間以内に、Tenable Nessus のインストールで使用する必要があります。
- 複数のスキャナーで共有することはできません。
- 大文字と小文字が区別されません。

- Tenable Nessus のオフライン管理に必要です。

  注意: Tenable Nessus のオフラインでの管理については、*Tenable Nessus ユーザーガイド*を参照してください。

  注意: アクティベーションコードを取得するには、アクティベーションコードの取得のページを参照してください。

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

エージェントの CPU リソースコントロール

`process_priority` 設定を使用することで、システム上で実行中の他のタスクの優先度と比較して、Tenable Agent の相対的な優先度を制御できます。このように設定が相対的なことから、Tenable Agent が消費するシステムリソースの量は、`process_priority` 設定の値だけでなく、システムの全体的な負荷によっても異なります。このため、エージェントが優先度の高いプロセスよりもリソースを消費しているかのように、システムモニターに映る場合があります。リソースコントロールのコマンドについては、Tenable Agent CLI コマンド を参照してください。

注意: `process_priority` の値を設定してから、Linux の適切な値、macOS の適切な値、または Windows 優先度クラスに変更が反映されるまでに、少し時間がかかることがあります。

`process_priority` 設定の効果を確認するには、次の表を参照してください。

設定値	Windows の優先度クラス	macOS の適切な値	Linux の適切な値
normal	normal	0	0
low	low	10	10
high	high	-10	-5

注意: `process_priority` 設定値を「低」に設定すると、スキャンの実行が長くなる可能性があります。この値を考慮して、スキャンウィンドウの時間枠を増やす必要があるかもしれません。

エージェント CPU リソースコントロールの詳細設定

`nessuscli` ユーティリティを使用して、コマンドラインインターフェースで次のエージェント設定が可能です。

コマンド `# nessuscli fix --set setting=value` を使用します。詳細は、Tenable Agent CLI コマンドを参照してください。

詳細および CLI で変更可能な設定の全一覧については、詳細設定を参照してください。

ヒント: 多数のエージェント (10,000 以上) がある場合は、`agent_merge_audit_trail`、`agent_merge_kb`、`agent_merge_journal_mode`、`agent_merge_synchronous_setting` の設定を変更することもできます。これらの設定を変更すると、エージェントのスキャン結果のマージにかかる時間が大幅に短縮されます。推奨される設定については、次の表の説明を参照してください。

名前	[設定]	説明	デフォルト	有効な値
Plugin Compilation Performance (プラグインのコンパイルパフォーマンス)	plugin_load_performance_mode	プラグインのコンパイルパフォーマンスを設定します。この設定は CPU 使用率に影響を与えます。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。各設定値のターゲット	Tenable Agent 10.8.3 以降 - `medium` Tenable Agent 10.8.2 以前 - `high`	`low`、`medium`、または `high`

		範囲は次のとおりです。 • low – 1 つのスレッドを使用します。利用可能な時間よりも意図的に少ない時間を消費し、1 つのコアの使用率を約 50% にします。 • medium - 利用可能なコアの最大数のスレッドを使用し、8 コア以上のシステムで最大 4 コアまで使用します。常に 1 つ以上のスレッドを使用します。 • high - 使用可能なコアの数だけスレッドを使用し、最大 8 スレッドまで使用します。		

		注意: VDI や ESXi などの共有リソース環境の場合、Tenable は、プラグインコンパイルパフォーマンスを `medium` または `low` に設定することを推奨しています。		
Scan Performance (スキャンパフォーマンス)	scan_ performance_ mode	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。各設定値のターゲット範囲は次のとおりです。 • `low` - スキャン中に 1 つの CPU コアの約半分の	`high`	`low`、`medium`、または `high`

		使用率をターゲットにします。 • `medium` – スキャン中に利用可能な各コアの最大値 (最大 8 コア) を使用します。 • `high` – スキャン中に合計 8 個のコアを使用します。		

Tenable Agent のパフォーマンス

Tenable は、社内パフォーマンステストに基づくパフォーマンスメトリクスを開示しています。パフォーマンスは環境によって異なり、同様の結果が得られる場合とそうでない場合があります。

以降のセクションでは、Tenable Agents のさまざまなパフォーマンスメトリクスについて説明します。

ライフサイクルと帯域幅

注意: パフォーマンスは環境によって異なり、同様の結果が得られる場合とそうでない場合があります。

プロセスまたはファイル	Windows	mac0S	Linux
エージェントコアソフトウェアの初回インストール	~70 MB	~38 MB	~15 から 25 MB
エージェントコアソフトウェアのアップデート	~32 MB	~38 MB	~20 から 30 MB

プロセスまたはファイル	Windows	mac0S	Linux
プラグインの初回ダウンロード	301 MB	220 MB	242 MB
差分プラグインアップデート **注意:** プラグインのアップデートファイルのサイズは、提供されている新しいプラグインと、エージェントが最後に更新した日付のプラグインとの差分によって異なります。	0.1 ～ 301 MB	0.1 ～ 220 MB	0.1 ～ 242 MB
レポートサイズ **注意:** レポートのサイズは、スキャンによって大きく異なる場合があります。コンプライアンス監査スキャンは、特に大きくなる可能性があります。	1～100 MB 以上	1～100 MB 以上	1～100 MB 以上

ソフトウェアフットプリント

注意: パフォーマンスは環境によって異なり、同様の結果が得られる場合とそうでない場合があります。

標準エージェントスキャンを実行しているエージェント

ディスク上のエージェントのフットプリント	ディスク上のエージェントソフトウェアの合計フットプリント	非スキャン時の平均 RAM 使用量	スキャン時の平均 RAM 使用量	プラグインのコンパイル中の平均 RAM 使用量	ネットワーク帯域幅の平均使用量
~85 MB	プラグインアップデートを含めて ~875 MB **注意:** 特定の条	~50 MB RAM **注意:** Linux 環境では、`Hugepagesize` の値は、`systemctl status nessusagent` コマンドで表示される使用量に大きな影響を与えます。表示される使用量には、エージェントプロセスの RAM 消費量だけでなく、システ	~85 MB RAM	~150 MB RAM	~8 MB/日

ディスク上のエージェントのフットプリント	ディスク上のエージェントソフトウェアの合計フットプリント	非スキャン時の平均 RAM 使用量	スキャン時の平均 RAM 使用量	プラグインのコンパイル中の平均 RAM 使用量	ネットワーク帯域幅の平均使用量
	件下では、ディスクの使用量が 3 GB 以上まで増える可能性があります。	ムがメモリ不足に陥った場合にディスクに保存されるキャッシュデータも含まれます。 たとえば、x86-64 ベースの Linux システムでは通常、デフォルトの Hugepagesize 値が 2048 KB の場合、総使用量は 200 MB から 600 MB の範囲になります。Hugepagesize 値が大きい ARM64 ベースの Linux システムでは、それに応じてメモリ使用量も多くなります (たとえば、デフォルトの Hugepagesize が 512 M の場合、使用量は数ギガバイトとして表示されます)。			

インベントリスキャンを実行しているエージェント

ディスク上のエージェントのフットプリント	ディスク上のエージェントソフトウェアの合計フットプリント	非スキャン時の平均 RAM 使用量	スキャン時の平均 RAM 使用量	プラグインのコンパイル中の平均 RAM 使用量	ネットワーク帯域幅の平均使用量
~85 MB	~150 MB (プラグイン更新を含む)	~50 MB RAM **注意:** Linux 環境では、Hugepagesize の値は、	~80 MB RAM	~105 MB RAM	~8 MB/日

ディスク上のエージェントのフットプリント	ディスク上のエージェントソフトウェアの合計フットプリント	非スキャン時の平均 RAM 使用量	スキャン時の平均 RAM 使用量	プラグインのコンパイル中の平均 RAM 使用量	ネットワーク帯域幅の平均使用量
	注意: 特定の条件下では、ディスクの使用量は 200 MB まで増える可能性があります。	`systemctl status nessusagent` コマンドで表示される使用量に大きな影響を与えます。表示される使用量には、エージェントプロセスの RAM 消費量だけでなく、システムがメモリ不足に陥った場合にディスクに保存されるキャッシュデータも含まれます。 たとえば、x86-64 ベースの Linux システムでは通常、デフォルトの `Hugepagesize` 値が 2048 KB の場合、総使用量は 200 MB から 600 MB の範囲になります。`Hugepagesize` 値が大きい ARM64 ベースの Linux システムでは、それに応じてメモリ使用量も多くなります (たとえば、デフォルトの `Hugepagesize` が 512 M の場合、使用量は数ギガバイトとして表示されます)。			

インベントリスキャンについての詳細は、*Tenable Vulnerability Management ユーザーガイド*の Tenable が提供する Agent テンプレートを参照してください。

ホストシステムの利用

注意: パフォーマンスは環境によって異なり、同様の結果が得られる場合とそうでない場合があります。

一般的には、Tenable Agent が使用する RAM は 50 MB ~ 60 MB です (すべてページング可能)。Tenable Agent は、アイドル時には CPU をほとんど使用しませんが、ジョブ実行中に使用可能な場合は CPU を最大 100% まで使用するように設計されています。

結果をアップロードするときのネットワーク使用率を測定するため、Tenable は 7 日間にわたってエージェントから Tenable Vulnerability Management へのアップロードを36,000 件数監視しました。

- 平均サイズは 1.6 MB でした。
- 最大サイズは 37 MB でした。
- アップロード全体の 90% は 2.2 MB 以下でした。
- アップロード全体の 99% は 5 MB 以下でした。
- オペレーティングシステムによって異なりますが、Tenable Agent プロセスは休止状態で 45 MB から 60 MB の RAM を消費します。

  > **注意:** Linux 環境では、`Hugepagesize` の値は、`systemctl status nessusagent` コマンドで表示される使用量に大きな影響を与えます。表示される使用量には、エージェントプロセスの RAM 消費量だけでなく、システムがメモリ不足に陥った場合にディスクに保存されるキャッシュデータも含まれます。
  >
  > たとえば、x86-64 ベースの Linux システムでは通常、デフォルトの `Hugepagesize` 値が 2048 KB の場合、総使用量は 200 MB から 600 MB の範囲になります。`Hugepagesize` 値が大きい ARM64 ベースの Linux システムでは、それに応じてメモリ使用量も多くなります (たとえば、デフォルトの `Hugepagesize` が 512 M の場合、使用量は数ギガバイトとして表示されます)。

- Watchdog サービスは 3 MB を消費します。
- プラグインは、およそ 300 MB のディスク容量を消費します (オペレーティングシステムによって異なります)。ただし、特定の条件下では、ディスクまたはメモリの使用量は 1 GB 以上まで増える可能性があります。
- Tenable Agents から Tenable Nessus Manager と Tenable Vulnerability Management に送信するスキャン結果は、2 ~ 3 MB の範囲です。
- チェックイン頻度は少なくとも 30 秒で、管理システム負荷 (エージェントの数) に基づいて Tenable Nessus Manager または Tenable Vulnerability Management によって調整されます。

Tenable Nessus Manager のパフォーマンス

Tenable は、2 つのシナリオで Tenable Nessus Manager のパフォーマンスをテストしました。**シナリオ 1** は、Tenable Agents が Tenable Nessus Manager に接続され、ジョブをポーリングしている場合です。**シナリオ 2** は、Tenable Agents がアクティブにスキャンし、スキャン結果をアップロードしている場合です。

テスト環境

Tenable は、これら 2 つのシナリオに対して次のテスト環境を使用しました。

シナリオ 1

- OS: Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-75-generic x86_64)
- RAM: 16 GB
- CPU: Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz
- コア: 2

シナリオ 2

- OS: Windows 10 v. 1703 (OS ビルド: 15063.447)
- RAM: 16 GB
- CPU: Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.59GHz
- コア: 2

シナリオ 1: Tenable Agents が Tenable Nessus Manager に接続され、ジョブをポーリングしている場合

エージェントの数	1 回につきジョブリクエストを送信するエージェントの数 (2%)	最大 CPU 使用率	平均 CPU 使用率	エージェントの平均ページ読み込み時間
1,000	20	33%	5%	0.60 秒
2,000	40	34%	5%	1.05 秒
5,000	100	43%	6%	1.7 秒
7,500	150	92%	7%	3.22 秒

10,000	200	100%	7%	3.26 秒

エージェントの数	ジョブリクエストを一度に送信するエージェントの数 (5%)	最大 CPU 使用率	平均 CPU 使用率	エージェントの平均ページ読み込み時間
1,000	50	38%	7%	0.88 秒
2,000	100	39%	7%	1.14 秒
5,000	250	54%	6%	1.73 秒

シナリオ 2: Tenable Agents がアクティブにスキャンし、スキャン結果をアップロードしている場合

エージェントの数	最大 CPU 使用率	平均 CPU 使用率	エージェントの平均ページ読み込み時間	スキャンレポートのサイズ
1,000	65%	52%	1.16 秒	363 MB
2,000	82%	53%	1.45 秒	726 MB
3,000	82%	46%	1.67 秒	1079 MB
4,000	86%	40%	1.70 秒	1452 MB
5,000	99%	47%	1.73 秒	1780 MB

エージェントの管理

エージェントを管理するには、次のトピックを参照してください。

Tenable Agent のインストール

このセクションでは、次のオペレーティングシステムに Tenable Agent をインストールする方法について説明します。

- Windows
- macOS
- Linux

インストールされたエージェントは、0 ~ 5 分のランダムな遅延の後に Tenable Nessus Manager または Tenable Vulnerability Management にリンクします。遅延を強制すると、大量のエージェントをデプロイまたは再起動する際のネットワークトラフィックを削減し、Tenable Nessus Manager または Tenable Vulnerability Management に対する負荷を軽減できます。エージェントは、最初のスキャン開始時にマネージャーからプラグインをダウンロードします。このプロセスには数分かかる場合があります。これはエージェントがスキャン結果を返す前に実行する必要があります。

Linux での Tenable Agent のインストール

次の手順を使用して、Linux システムに Tenable Agent をインストールします。インストール後、エージェントをマネージャー (Tenable Vulnerability Management または Tenable Nessus Manager) にリンクします。これにより、インストールの完了後にエージェントがスキャンデータの送信を開始できるようになります。

始める前に

- Tenable Agent リンクキーを取得します。詳細については、使用しているマネージャーに応じて、*Tenable 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。
- Tenable Agent が事前にシステムにインストールされている場合、リンクエラーを回避する方法に関するナレッジベースの記事を参照してください。

警告: nessusd を実行している既存の Tenable Agent、Tenable Nessus Manager、Tenable Nessus スキャナーがすでに存在するシステムに Tenable Agent をインストールする場合、インストールプロセスにより他のすべての nessusd プロセスが強制終了されます。この結果スキャンデータが失われる場合があります。

Tenable Agent をダウンロードする

Tenable Agent のダウンロードページで、ご利用のオペレーティングシステムに固有のパッケージをダウンロードします。

エージェントパッケージをダウンロードしたら、エージェントをインストールします。

エージェントのインストール

注意: 次の手順は root 権限を必要とします。

コマンドラインインターフェースを使用して、Tenable Agent をインストールします。

Linux インストールコマンドの例

Debian / Ubuntu

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

Red Hat 8 以降、Oracle Linux 8 以降、Fedora 34 以降

```
# dnf install NessusAgent-<OS and version number> .rpm
```

Red Hat 7 以前 / Oracle Linux 7 以前

```
# rpm -ivh NessusAgent-<OS and version number> .rpm
```

SUSE

```
# sudo zypper install NessusAgent-<OS and version number> .rpm
```

ヒント: リンクする前にフルプラグインセットをインストールすると、一括インストール実行中に消費される帯域幅を減らすことができます。これは、プラグインセットの場所を指定する `--file` パラメーターを指定して `nessuscli agent update` コマンドを使用して行うことができます。この作業は Tenable Agent を開始する前に行う必要があります。例

```
/opt/nessus_agent/sbin/nessuscli agent update --file=./plugins_set.tgz
```

このプラグインセットは5日以内に入手したものである必要があります。入手後5日を超える古いプラグインセットでは、フルプラグインのダウンロードが強制的に開始されます。最新のプラグインセットは、Tenable Agent ダウンロードページからダウンロードできます。

注意: Tenable Agentをインストールした後に、**/sbin/service nessusagent start**コマンドを使用して手動でサービスを開始する必要があります。Tenableは、ホストが再起動するたびにTenable Agentサービスが開始されるよう、**systemctl enable nessusagent**を実行することも推奨しています。

コマンドラインを使用したエージェントのリンク付け

コマンドプロンプトで、`nessuscli agent link`コマンドを使用します。例

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

注意: リンクコマンド全体をコピーして、同じ行に貼り付ける必要があります。そうしないと、エラーが表示されます。

このコマンドがサポートする引数は次のとおりです。

引数	必須	値
--key	○	(必須) マネージャーから取得した値を使用してください。 マネージャーからリンクキーを取得するには、使用しているマネージャーに応じて、*Tenable 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。
--host	○	
--port	○	
--name	×	エージェントの名前を指定します。エージェントの名前を指定しない場合、エージェントをインストールしているコンピューターの名前にデフォルトで設定されます。
--groups	no	エージェントを追加する1つ以上のエージェントグループを指定します。インストールプロセス中にエージェントグループを指定しない場合、Tenable Nessus Manager または Tenable Vulnerability Management で、リンク

引数	必須	値
		されたエージェントをエージェントグループに後から追加できます。 **注意:** エージェントグループ名は、大文字と小文字を区別し、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"`)。
--offline-install	×	Tenable Agent は、オフラインでもシステムにインストールできます。コマンドラインオプション `offline-install="yes"` をコマンドライン入力に追加します。Tenable Agent は、定期的に Tenable Vulnerability Management または Tenable Nessus Manager へのリンクを試みます。 エージェントがコントローラーに接続できない場合、1 時間ごとに再試行します。また、コントローラーには接続できてもリンクに失敗する場合は、24 時間ごとに再試行します。
--cloud	×	`--cloud` の引数を指定し、Tenable Vulnerability Management にリンクします。 `--cloud` 引数は、`--host=sensor.cloud.tenable.com --port=443` を指定するためのショートカットです。 **警告:** `--cloud` 引数は、FedRAMP 環境ではサポートされていません。`--host=fedcloud.tenable.com --port=443` を指定する必要があります。 **注意:** 中国本土にある Tenable Nessus スキャナー、Tenable Agents、Tenable Web App Scanning スキャナー、または Tenable Network Monitor (NNM) を介して Tenable Vulnerability Management に接続している場合は、sensor.cloud.tenable.com ではなく sensor.cloud.tenablecloud.cn で接続する必要があります。 **注意:** エージェントの Tenable Vulnerability Management へのリンクについての詳細は、*Tenable Vulnerability Management ユーザーガイド*のセンサーのリンクを参照してください。
--network	×	Tenable Vulnerability Management にリンクされたエージェントの場合、エージェントをカスタムネットワークに追加します。ネットワークを指定しない場合、エージェントはデフォルトのネットワークに属することになります。

引数	必須	値
		注意: ネットワーク名は引用符で囲む必要があります (例: `--network="My Network"`)。
--profile-uuid	×	エージェントの割り当て先となるエージェントプロファイルの UUID (例: `12345678-9abc-4ef0-9234-56789abcdef0`)。詳細については、*Tenable Vulnerability Management ユーザーガイド*のエージェントプロファイルを参照してください。

エージェントをインストールしてリンクしたら、Tenable では、マネージャーのユーザーインターフェースでエージェントを表示して、エージェントがマネージャーに正常にリンクされていることを確認することを推奨しています。

ヒント: エージェントのクローンを作り、Tenable Nessus Manager または Tenable Vulnerability Management にリンクしようとすると 409 エラーが表示される場合があります。このエラーは、他のマシンが、**/etc/machine_id** または **/etc/tenable_tag** ファイル内の同じ UUID 値にリンクされたために表示されます。この問題を解決するには、**/etc/tenable_tag** ファイルの値を有効な UUIDv4 値に置き換えます。**/etc/machine_id** ファイルが存在しない場合、**/etc/tenable_tag** を削除して新しい値を生成できます。

リンクされたエージェントの検証

エージェントをインストールしてリンクしたら、次の手順に沿って、マネージャーのユーザーインターフェースで新しいエージェントを表示します。

- Tenable Vulnerability Management でリンクされたエージェントを検証する方法

  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。

     [Settings] (設定) ページが表示されます。

  3. **[Sensors]** (センサー) タイルをクリックします。

[Sensors] (センサー) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Nessus Scanners]** (Nessus スキャナー) が選択され、**[Cloud Scanners]** (クラウドスキャナー) タブがアクティブとなります。

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。

   [Nessus Agent] ページが表示され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブになります。

5. リンクされたエージェントの表で新しいエージェントを見つけます。

- Tenable Nessus Manager でリンクされたエージェントを検証する方法

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

     [Linked Agents] (リンクされたエージェント) ページが表示されます。

  2. リンクされたエージェントの表で新しいエージェントを見つけます。

Windows での Tenable Agent のインストール

次の手順を使用して、Windows システムに Tenable Agent をインストールします。インストールプロセス中に、エージェントをマネージャー (Tenable Vulnerability Management または Tenable Nessus Manager) にリンクします。これにより、インストールの完了後にエージェントがスキャンデータの送信を開始できるようになります。

始める前に

- Tenable Agent リンクキーを取得します。詳細については、使用しているマネージャーに応じて、*Tenable 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。
- Tenable Agent が事前にシステムにインストールされている場合、リンクエラーを回避する方法に関するナレッジベースの記事を参照してください。

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

警告: nessusd を実行している既存の Tenable Agent、Tenable Nessus Manager、Tenable Nessus スキャナーがすでに存在するシステムに Tenable Agent をインストールする場合、インストールプロセスにより他のすべての nessusd プロセスが強制終了されます。この結果スキャンデータが失われる場合があります。

Tenable Agent のダウンロード

Tenable Agent のダウンロードページで、ご利用のオペレーティングシステムに固有のパッケージをダウンロードします。

エージェントパッケージをダウンロードしたら、コマンドラインを使用してエージェントをインストールしてリンクできます。または、GUI インストールウィザードを使用してエージェントをインストールしてリンクすることもできます。

コマンドラインを使ったインストールとリンク付け

注意: コマンドラインからデプロイしてリンクするには、管理者レベルの権限が必要です。

注意: この手順ではコマンドラインを使った Tenable Agents のデプロイについて説明しています。アクティブディレクトリ(AD)、システム管理サーバー(SMS)やその他の MSI パッケージ向けソフトウェア配信システムなど、標準の Windows サービスで Tenable Agents をデプロイすることもできます。これらの方法によるデプロイについての詳細は、該当するベンダーのドキュメントを参照してください。

コマンドラインを使っていくつものリンク付けパラメーターを指定して、Tenable Agents をインストールしリンクすることができます。例:

```
msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS="Agent Group Name"
NESSUS_SERVER="192.168.0.1:8834" NESSUS_
KEY=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00 /qn
```

エージェントコマンドラインのリンク付けパラメーター

次のリンク付けパラメーターを使用できます。

パラメーター	説明
ADDLOCAL=ALL	*Tenable Agent ユーザーガイド*の Windows での Tenable Agent のインストールの手順 8 の説明に従って、Tenable Agent システムトレイアプリケーションをインストールします。
NESSUS_CA_PATH	マネージャーのサーバー証明書を検証するのに使用するカスタム CA 証明書を指定します。

NESSUS_GROUPS	エージェントを追加する 1 つ以上のエージェントグループを指定します。インストールプロセス中にエージェントグループを指定しない場合、Tenable Nessus Manager または Tenable Vulnerability Management で、リンクされたエージェントをエージェントグループに後から追加できます。 **注意:** エージェントグループ名は、大文字と小文字を区別し、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"`)。 **注意:** 複数のグループを列記する場合、あるいは 1 つのグループの名前にスペースが含まれている場合は、二重引用符 (") で囲む必要があります。例 • GroupName • "Group Name" • "Group, Another Group"
NESSUS_NAME	エージェントの名前を指定します。エージェントの名前を指定しない場合、エージェントをインストールしているコンピューターの名前にデフォルトで設定されます。
NESSUS_OFFLINE_INSTALL	Tenable Agent は、オフラインでもシステムにインストールできます。コマンドラインのオプション `NESSUS_OFFLINE_INSTALL="yes"` をコマンドライン入力に追加します。Tenable Agent は、定期的に Tenable Vulnerability Management または Tenable Nessus Manager へのリンクを試みます。エージェントがコントローラーに接続できない場合、1 時間ごとに再試行します。また、コントローラーには接続できてもリンクに失敗する場合は、24 時間ごとに再試行します。
NESSUS_PLUGINS_FILEPATH="C:\path\to\plugins_	一括インストールの実行中に消費される帯域幅を減らすために、リンクする前にフルプラグインセットをインス

set.tgz"	トールします。コマンドラインのオプション NESSUS_PLUGINS_FILEPATH="C:\path\to\plugins_set.tgz" を加えます。ここで *plugins_set.tgz* は、入手後 5 日以内の最新のプラグインセットの tarball です。入手後 5 日を超える古いプラグインセットでは、フルプラグインのダウンロードが強制的に開始されます。最新のプラグインセットは、Tenable ダウンロードページからダウンロードできます。
NESSUS_PROCESS_PRIORITY	システム上で実行されるその他のタスクと比較して、エージェントの相対的な優先度を決定します。有効な値、およびこの設定の動作方法に関する詳細は、*Tenable Agent デプロイメントとユーザーガイド* のエージェントの CPU リソースコントロールを参照してください。
NESSUS_PROXY_AGENT	プロキシが事前定義されているユーザーエージェントを要求する場合は、ユーザーエージェント名を指定します。
NESSUS_PROXY_PASSWORD	ユーザー名として指定したユーザーアカウントのパスワードを指定します。
NESSUS_PROXY_SERVER	プロキシサーバーのホスト名または IP アドレスを指定します。
NESSUS_PROXY_USERNAME	プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名を指定します。
NESSUS_SERVER	サーバーのホスト名または IP アドレスを指定します。 • Tenable Vulnerability Management にリンクする場合は、**sensor.cloud.tenable.com:443** と入力します。 • Tenable Nessus Manager にリンクする場合は、ポート **8834** を付けて、マネージャーの IP またはホスト名を入力します (例:

	192.168.2.1:8834)。
`NESSUS_SERVICE_AUTOSTART=false`	インストール後に Tenable Agent が起動しないようにします。 このパラメーターは、合理化されたデプロイメントオプション (JSON ファイルを使用したデプロイメントなど) で役立つ可能性があります。 **注意:** Windows では、エージェントサービスの `StartType` は **[Automatic]** (自動) に設定されます。そのため、Windows システムを再起動すると、エージェントサービスが常に開始されます。

エージェントをインストールしてリンクしたら、Tenable では、マネージャーのユーザーインターフェースでエージェントを表示して、エージェントがマネージャーに正常にリンクされていることを確認することを推奨しています。

インストールウィザードを使ったインストールとリンク付け

注意: Windows でインストールを完了するために、コンピューターの再起動が必要な場合があります。

1. Tenable Agent のインストーラをダウンロードしたフォルダーに移動します。
2. 次に、ファイル名をダブルクリックし、インストールのプロセスを開始します。**[Welcome to the InstallShield Wizard for Nessus Agent]** (Nessus Agent の InstallShield ウィザードへようこそ) ウィンドウが表示されます。
3. **[Welcome to the InstallShield Wizard for Nessus Agent]** (Nessus Agent の InstallShield ウィザードへようこそ) ウィンドウで、**[Next]** (次へ) をクリックして続行します。
4. **[License Agreement]** (ライセンス契約) ウィンドウで、Tenable, Inc. Nessus ソフトウェアライセンスとサブスクリプション契約の条項に目を通します。
5. **[I accept the terms of the license agreement]** (ライセンス契約の条項に同意します) をクリックします。
6. **[Next]** (次へ) をクリックします。

7. **[Destination Folder]** (保存先フォルダー) ウィンドウで、**[Next]** (次へ) をクリックし、デフォルトのインストールフォルダーを使用します。

   -または-

   [Change] (変更) をクリックし、Tenable Agents をインストールする別のフォルダーを参照して選択し、**[Next]** (次へ) をクリックします。

8. **[Setup Type]** (設定タイプ) ウィンドウで、次のいずれかを実行します。

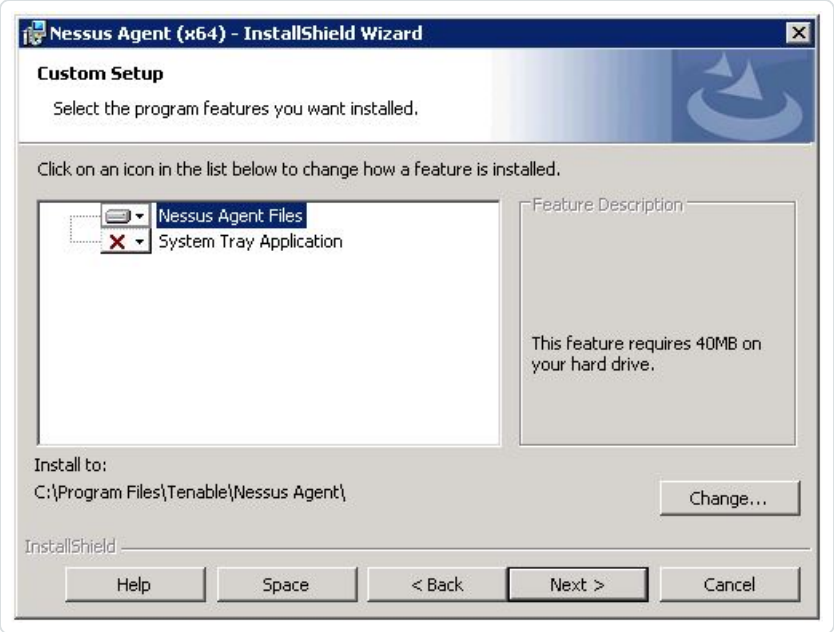
   - エージェントをシステムトレイアプリケーションを使用してインストールするは、**[Custom]** (カスタム) を選択し、**[Next]** (次へ) をクリックして、ドロップダウンメニューで次の手順を完了します。これにより、マシンでエージェントステータスを表示できます。

     システムトレイアプリケーションの設定

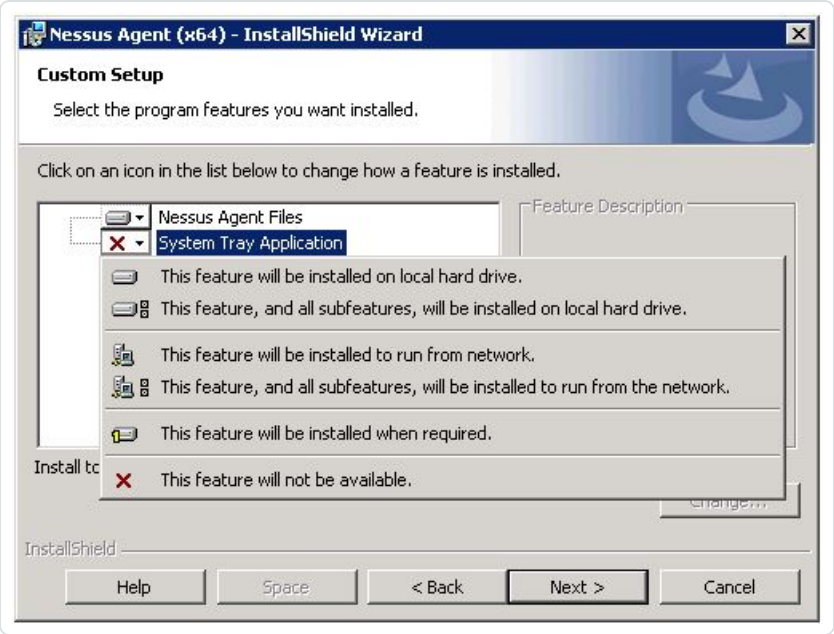
フィールド	値
キー	(必須) マネージャーから取得したリンクキーを使用します。 マネージャーからリンクキーを取得するには、使用しているマネージャーに応じて、*Tenable Nessus ユーザーガイド* または *Tenable Vulnerability Management ユーザーガイド*を参照してください。
サーバー	(必須) マネージャーのホストサーバーを入力します。 • Tenable Vulnerability Management にリンクする場合は、**sensor.cloud.tenable.com:443** と入力します。 **注意:** 中国本土にある Tenable Nessus スキャナー、Tenable Agents、Tenable Web App Scanning スキャナー、または Tenable Network Monitor (NNM) を介して Tenable Vulnerability Management に接続している場合は、sensor.cloud.tenable.com ではなく sensor.cloud.tenablecloud.cn で接続する必要があります。 **注意:** エージェントの Tenable Vulnerability Management へのリンクについての詳細は、*Tenable Vulnerability Management ユーザーガイド*のセンサーのリンクを参照してください。

	• Tenable Nessus Manager にリンクする場合は、ポート **8834** を付けて、マネージャーの IP またはホスト名を入力します (例: **192.168.2.1:8834**)。
グループ	エージェントを追加したい既存のエージェントグループを指定します。 インストールプロセス中にエージェントグループを指定しない場合、リンクされたエージェントを後からエージェントグループに追加できます。

a. **[Custom Setup]** (カスタムセットアップ) ページが表示されます。デフォルトでは、システムトレイアプリケーションはインストールパッケージに含まれていません。



b. **[SystemTray Application]** (SystemTray アプリケーション) ドロップダウンボックスをクリックします。



c. **[This feature will be installed on local hard drive]** (この機能をローカルハードドライブにインストールする) をクリックします。

d. **[Next]** (次へ) をクリックします。

- システムトレイアプリケーションを使用せずにエージェントをインストールするには、**[Typical]** (標準) を選択し、**[Next]** (次へ) をクリックします。

9. **[Configuration Options]** (設定オプション) ウィンドウで、次のように**エージェントキー**の値を入力します。

フィールド	値
キー	(必須) マネージャーから取得したリンクキーを使用します。 マネージャーからリンクキーを取得するには、使用しているマネージャーに応じて、*Tenable 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。
サーバー	(必須) マネージャーのホストサーバーを入力します。 • Tenable Vulnerability Management にリンクする場合は、**sensor.cloud.tenable.com:443** と入力します。

	注意: 中国本土にある Tenable Nessus スキャナー、Tenable Agents、Tenable Web App Scanning スキャナー、または Tenable Network Monitor (NNM) を介して Tenable Vulnerability Management に接続している場合は、sensor.cloud.tenable.com ではなく sensor.cloud.tenablecloud.cn で接続する必要があります。 **注意:** エージェントの Tenable Vulnerability Management へのリンクについての詳細は、*Tenable Vulnerability Management* ユーザーガイドのセンサーのリンクを参照してください。 • Tenable Nessus Manager にリンクする場合は、ポート **8834** を付けて、マネージャーの IP またはホスト名を入力します (例: **192.168.2.1:8834**)。
グループ	エージェントを追加したい既存のエージェントグループを指定します。 インストールプロセス中にエージェントグループを指定しない場合、リンクされたエージェントを後からエージェントグループに追加できます。

10. **[Next]** (次へ) をクリックします。
11. **[Ready to Install the Program]** (プログラムのインストールの準備完了) ウィンドウで **[Install]** (インストール) をクリックします。
12. **[User Account Control]** (ユーザーアカウント制御) メッセージが表示されたら、**[Yes]** (はい) をクリックし、Tenable Agent のインストールを許可します。
13. **[InstallShield Wizard Complete]** (InstallShield ウィザードが完了しました) ウィンドウで、**[Finish]** (終了) をクリックします。

エージェントをインストールしてリンクしたら、Tenable では、マネージャーのユーザーインターフェースでエージェントを表示して、エージェントがマネージャーに正常にリンクされていることを確認することを推奨しています。

注意: エージェント名は、エージェントをインストールしているコンピューターの名前にデフォルトで設定されます。

ヒント: エージェントのクローンを作り、Tenable Nessus Manager または Tenable Vulnerability Management にリンクしようとすると 409 エラーが表示される場合があります。このエラーは、`HKLM/Software/Tenable/TAG` ファイルで、別のマシンが同じ UUID 値でリンクされたために表示されます。この問題を解決するには、`HKLM/Software/Tenable/TAG` ファイルのこの値を有効な UUIDv4 値に置き換えます。

リンクされたエージェントの検証

エージェントをインストールしてリンクしたら、次の手順に沿って、マネージャーのユーザーインターフェースで新しいエージェントを表示します。

- Tenable Vulnerability Management でリンクされたエージェントを検証する方法

  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。

     [Settings] (設定) ページが表示されます。

  3. **[Sensors]** (センサー) タイルをクリックします。

     [Sensors] (センサー) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Nessus Scanners]** (Nessus スキャナー) が選択され、**[Cloud Scanners]** (クラウドスキャナー) タブがアクティブとなります。

  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。

     [Nessus Agent] ページが表示され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブになります。

  5. リンクされたエージェントの表で新しいエージェントを見つけます。

- Tenable Nessus Manager でリンクされたエージェントを検証する方法

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

     [Linked Agents] (リンクされたエージェント) ページが表示されます。

  2. リンクされたエージェントの表で新しいエージェントを見つけます。

macOS での Tenable Agent のインストール

次の手順を使用して、macOS システムに Tenable Agent をインストールします。インストール後、エージェントをマネージャー (Tenable Vulnerability Management または Tenable Nessus Manager) にリンクします。これにより、インストールの完了後にエージェントがスキャンデータの送信を開始できるようになります。

始める前に

- Tenable Agent リンクキーを取得します。詳細については、使用しているマネージャーに応じて、*Tenable 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。
- Tenable Agent が事前にシステムにインストールされている場合、リンクエラーを回避する方法に関するナレッジベースの記事を参照してください。

注意: フルディレクトリアクセス権の一部の監査では、エージェントがフルディスクアクセス権を必要とする場合があります。したがって、Tenable では、macOS にインストールされているエージェントにフルディスクアクセス権を許可することを推奨しています。

警告: `nessusd` を実行している既存の Tenable Agent、Tenable Nessus Manager、Tenable Nessus スキャナーがすでに存在するシステムに Tenable Agent をインストールする場合、インストールプロセスにより他のすべての `nessusd` プロセスが強制終了されます。この結果スキャンデータが失われる場合があります。

Tenable Agent のダウンロード

Tenable Agent のダウンロードページで、ご利用のオペレーティングシステムに固有のパッケージをダウンロードします。

エージェントパッケージをダウンロードしたら、エージェントをインストールします。

エージェントのインストール

注意: 次の手順を実行するには、root 権限が必要です。

GUI インストールウィザードまたはコマンドラインを使用して、Tenable Agent をインストールできます。

GUI インストール

1. Tenable Agent `.dmg` (macOS ディスクイメージ) ファイルをダブルクリックします。
2. `Install Nessus Agent.pkg` をダブルクリックします。
3. **Nessus Agent インストールウィザード**を終了します。

コマンドラインインストール

1. `Install Nessus Agent.pkg` と `.NessusAgent.pkg` を `NessusAgent-<version number>.dmg` から展開します。

注意: .NessusAgent.pkg ファイルは通常 macOS Finder では表示されません。

2. ターミナルを開きます。
3. コマンドラインから、次のコマンドを入力します。

```
# sudo installer -pkg /<path-to>/Install Nessus Agent.pkg -target /
```

エージェントのインストールが完了したら、エージェントをマネージャーにリンクします。

ヒント: リンクする前にフルプラグインセットをインストールすると、一括インストール実行中に消費される帯域幅を減らすことができます。これは、プラグインセットの場所を指定する --file パラメーターを指定して nessuscli agent update コマンドを使用して行うことができます。この作業は Tenable Agent を開始する前に行う必要があります。例

```
/opt/nessus_agent/sbin/nessuscli agent update --file=./plugins_set.tgz
```

このプラグインセットは 5 日以内に入手したものである必要があります。入手後 5 日を超える古いプラグインセットでは、フルプラグインのダウンロードが強制的に開始されます。最新のプラグインセットは、Tenable Agent ダウンロードページからダウンロードできます。

コマンドラインを使用したエージェントのリンク付け

macOS でエージェントをリンクするには、次のようにします。

1. ターミナルを開きます。
2. コマンドラインから、nessuscli agent link コマンドを使用します。

   例

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

注意: リンクコマンド全体をコピーして、同じ行に貼り付ける必要があります。そうしないと、エラーが表示されます。

エージェントコマンドラインのリンク付けパラメーター

このコマンドがサポートする引数は次のとおりです。

引数	必須	値
--key	○	(必須) マネージャーから取得した値を使用してください。 マネージャーからリンクキーを取得するには、使用しているマネージャーに応じて、*Tenable 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。
--host	○	
--port	○	
--name	×	エージェントの名前を指定します。エージェントの名前を指定しない場合、エージェントをインストールしているコンピューターの名前にデフォルトで設定されます。
--groups	×	エージェントを追加したい既存のエージェントグループを指定します。インストールプロセス中にエージェントグループを指定しない場合、Tenable Nessus Manager または Tenable Vulnerability Management で、リンクされたエージェントをエージェントグループに後から追加できます。 **注意:** エージェントグループ名は、大文字と小文字を区別し、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"`)。
--offline-install	×	Tenable Agent は、オフラインでもシステムにインストールできます。コマンドラインのオプション `NESSUS_OFFLINE_INSTALL="yes"` をコマンドライン入力に追加します。Tenable Agent は、定期的に Tenable Vulnerability Management または Tenable Nessus Manager へのリンクを試みます。 エージェントがコントローラーに接続できない場合、1 時間ごとに再試行します。また、コントローラーには接続できてもリンクに失敗する場合は、24 時間ごとに再試行します。
--cloud	×	`--cloud` の引数を指定し、Tenable Vulnerability Management にリンクします。 `--cloud` 引数は、`--host=cloud.tenable.com --port=443` を

		指定するためのショートカットです。 **警告:** `--cloud` 引数は、FedRAMP 環境ではサポートされていません。`--host=fedcloud.tenable.com --port=443` を指定する必要があります。 **注意:** 中国本土にある Tenable Nessus スキャナー、Tenable Agents、Tenable Web App Scanning スキャナー、または Tenable Network Monitor (NNM) を介して Tenable Vulnerability Management に接続している場合は、sensor.cloud.tenable.com ではなく sensor.cloud.tenablecloud.cn で接続する必要があります。 **注意:** エージェントの Tenable Vulnerability Management へのリンクについての詳細は、*Tenable Vulnerability Management ユーザーガイド* のセンサーのリンクを参照してください。
--network	×	Tenable Vulnerability Management にリンクされたエージェントの場合、エージェントをカスタムネットワークに追加します。ネットワークを指定しない場合、エージェントはデフォルトのネットワークに属することになります。
--profile-uuid	×	エージェントの割り当て先となるエージェントプロファイルの UUID (例: `12345678-9abc-4ef0-9234-56789abcdef0`)。詳細については、*Tenable Vulnerability Management ユーザーガイド* のエージェントプロファイルを参照してください。

エージェントをインストールしてリンクしたら、Tenable では、マネージャーのユーザーインターフェースでエージェントを表示して、エージェントがマネージャーに正常にリンクされていることを確認することを推奨しています。

ヒント: エージェントのクローンを作り、Tenable Nessus Manager または Tenable Vulnerability Management にリンクしようとすると 409 エラーが表示される場合があります。このエラーは、**`/private/etc/tenable_tag`** ファイルで、別のマシンが同じ UUID 値でリンクされたために表示されます。この問題を解決するには、**`/private/etc/tenable_tag`** ファイルのこの値を有効な UUIDv4 値に置き換えます。

リンクされたエージェントの検証

エージェントをインストールしてリンクしたら、次の手順に沿って、マネージャーのユーザーインターフェースで新しいエージェントを表示します。

- Tenable Vulnerability Management でリンクされたエージェントを検証する方法

  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。

     [Settings] (設定) ページが表示されます。

  3. **[Sensors]** (センサー) タイルをクリックします。

     [Sensors] (センサー) ページが表示されます。デフォルトでは、左側のナビゲーションメニューで **[Nessus Scanners]** (Nessus スキャナー) が選択され、**[Cloud Scanners]** (クラウド スキャナー) タブがアクティブとなります。

  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。

     [Nessus Agent] ページが表示され、**[Linked Agents]** (リンクされたエージェント) タブがアクティブになります。

  5. リンクされたエージェントの表で新しいエージェントを見つけます。

- Tenable Nessus Manager でリンクされたエージェントを検証する方法

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

     [Linked Agents] (リンクされたエージェント) ページが表示されます。

  2. リンクされたエージェントの表で新しいエージェントを見つけます。

Tenable Agent の開始または停止

エージェントによるデータ収集を一時的に停止し、エージェントを再起動してデータ収集を再開できます。エージェントの停止と開始は、トラブルシューティングに役立つことがあります。また、Tenable では、手動アップデートを実行するときは必ずエージェントを停止することを推奨しています。

以下のセクションで、ホストで Tenable Agent を開始および停止する際のベストプラクティスを説明します。

Windows

1. **[Services]** (サービス) に移動します。
2. **[Name]** (名前) 列で **[Tenable Nessus Agent]** をクリックします。
3. 次のいずれかを実行します。

    - エージェントのサービスを停止するには、**[Tenable Nessus Agent]** を右クリックしてから **[Stop]** (停止) をクリックします。

    - エージェントのサービスを再起動するには、**[Tenable Nessus Agent]** を右クリックしてから **[Start]** (開始) をクリックします。

または、次のコマンドを使用して、コマンドラインからエージェントを開始したり停止したりすることもできます。

開始または停止	Windows コマンドライン操作
開始	`C:\Windows\system32>net start "Tenable Nessus Agent"`
停止	`C:\Windows\system32>net stop "Tenable Nessus Agent"`

Linux

Linux システムでエージェントを開始または停止するには、次のコマンドを使用します。

開始または停止	Linux コマンドライン操作
開始	`# systemctl start nessusagent`
終了	`# systemctl stop nessusagent`

macOS

1. **[System Settings]** (システム設定) に移動します。
2. 🔄 ボタンをクリックします。
3. 🔒 ボタンをクリックします。
4. ユーザー名とパスワードを入力します。

5. 次のいずれかを実行します。

   - エージェントのサービスを停止するには、**[Stop Nessus Agent]** (Nessus Agent の停止) ボタンをクリックします。

   - エージェントのサービスを開始するには、**[Start Nessus Agent]** (Nessus Agent の開始) ボタンをクリックします。

または、次のコマンドを使用して、コマンドラインからエージェントを開始したり停止したりすることもできます。

開始または停止	macOS コマンドライン操作
開始	`# sudo launchctl start com.tenablesecurity.nessusagent`
停止	`# sudo launchctl stop com.tenablesecurity.nessusagent`

Tenable Agent のアップデート

インストールされたエージェントは、そのマネージャー (Tenable Vulnerability Management または Tenable Nessus Manager のいずれか) から自動的にアップデートを取得します。

どちらのマネージャーのユーザーインターフェースでも、エージェント更新プランを設定して、エージェントの自動更新後のバージョンを指定できます。詳細については、Tenable Vulnerability Management ユーザーガイドおよび Tenable Nessus Manager ユーザーガイドで説明されている手順に従ってください。

手動アップデート

エアギャップのネットワークやインターネットが制限されているネットワークなどの特定のケースでは、エージェントアップデートを手動でダウンロードする必要がある場合があります。また、アップデートを個別のエージェントに直接インストールすることも、一括アップデートファイル `tar.gz` を Tenable Nessus Manager ディレクトリにインストールすることもできます。後者の場合、Tenable Nessus Manager は `tar.gz` アップデートファイルを使用して、リンクされた各エージェントにアップデートを配布します。

> **注意:** 初期設定では、Tenable Vulnerability Management にリンクされたエージェントは、バージョンが一般公開 (GA) された一週間後に GA にアップデートされます。従って、その日以前に Tenable Vulnerability Management にリンクされたエージェントを手動で最新バージョンにアップデートする場合は、自動アップデートを

無効にするか、更新プランで早期アクセス版リリースを選択してください。これを行うことで、エージェントが前のバージョン (GA) に自動的にダウングレードされないようになります。

Tenable Agent にアップデートを手動でインストールするには

注意: 以下の手順をオフラインのマシンで実行する必要がある場合は、インターネットにアクセスできるマシンで手順 1 から 3 を実行してください。手順 3 の後に、ダウンロードしたファイルをオフラインのマシンにコピーし、オフラインのマシンで手順 4 を実行します。

1. Tenable Agent Downloads (Tenable Nessus Agent ダウンロード) ページに移動します。
2. ご使用のオペレーティングシステムに応じて、ダウンロードするエージェントアップデートファイルをクリックします。

   [License Agreement] (ライセンス契約) ウィンドウが表示されます。
3. **[I Agree]** (同意する) をクリックします。

   アップデートファイルがマシンにダウンロードされます。
4. ご使用のオペレーティングシステムに応じて、次のいずれかを実行します。

   注意: 以下の手順を完了するには、管理者レベルの権限が必要です。

   #### Windows

   次のいずれかを行います。

   - ダウンロードした `.msi` ファイルをダブルクリックして、画面上の指示に従います。
   - ダウンロードしたパッケージの場所とファイル名を使用して、次のコマンドをコマンドラインインターフェースで入力します。

     ```
     > msiexec /i <path-to>\NessusAgent-<version>.msi /qn
     ```

   #### Linux

   - コマンドラインインターフェースで、お使いの Linux 環境固有の install または upgrade コマンドを使用して、ダウンロードしたファイルをインストールします。

macOS

a. ダウンロードした `.dmg` ファイルをマウントします。

```
# sudo hdiutil attach <path-to>/NessusAgent-<version>.dmg
```

b. パッケージをインストールします。

```
# sudo installer -package /Volumes/Nessus\ Install/Install\ <path-
to>/NessusAgent-<version>.dmg -target /
```

オペレーティングシステムにより Tenable Agent アップデートがインストールされます。

場合によっては、アップデートをエージェントに直接インストールする代わりに、Tenable Nessus Manager にエージェントアップデートプログラムをインストールすることもできます。こうすると、リンクされたエージェントにアップデートが配布されます。

Tenable Agent の新しいバージョンがリリースされると、Tenable Nessus Manager はフィードアップデートを通じてそれらの新しいバージョンを認識し、リンクされたエージェントにそれらのアップデートを渡します。オフラインまたはエアギャップモードで登録された Tenable Nessus Manager は、新しいエージェントのバージョンを自動的には認識しません。次の手順に従って、最新の Tenable Agent アップデートファイルを手動でインストールし、エージェントのバージョンを更新する必要があります。

Tenable Nessus Manager にエージェントアップデートを手動でインストールするには

注意: 以下の手順をオフラインのマシンで実行する必要がある場合は、インターネットにアクセスできるマシンで手順 1 と 2 を実行してください。それから、手順 3 でダウンロードしたファイルをオフラインのマシンにコピーします。

1. Tenable Agent Downloads (Tenable Nessus Agent ダウンロード) ページに移動します。
2. `nessus-agent-updates-<version>.tar.gz` ファイルをダウンロードします。このファイルには、Tenable Agent をインストールできるすべてのオペレーティングシステムとプラットフォームのアップデートファイルが含まれています。

   パッケージはシステム間で転送されるため、転送後は必ず MD5 チェックサムをプルしてファイルの整合性を検証してください。

3. tar.gz ファイルを Tenable Nessus Manager ディレクトリにコピーします。ファイルは、Tenable Nessus Manager ディレクトリ内のアクセス可能な任意の子フォルダーに貼り付けることができます。

4. お使いのオペレーティングシステムに応じて、次のいずれかのコマンドを実行してエージェントのアップデートファイルを準備します。

   注意: 以下のコマンドを実行するには、管理者レベルの権限が必要です。

   Windows

   ```
   > C:\Program Files\Tenable\Nessus\nessuscli.exe update <\path\to\nessus-agents-update-<version>.tar.gz>
   ```

   Linux

   ```
   # /opt/nessus/sbin/nessuscli update </path/to/nessus-agent-updates-<version>.tar.gz>
   ```

   macOS

   ```
   # /Library/Nessus/run/sbin/nessuscli update </path/to/nessus-agent-updates-<version>.tar.gz>
   ```

   アップデートパッケージは /remote ディレクトリにプッシュされます。このディレクトリがローカルエージェントストアとして機能します。

5. Tenable Nessus Manager ユーザーインターフェースの **[Sensors]** (センサー) > **[Agent Updates]** (エージェントの更新) をクリックして、リンク済みエージェントを自動的に更新するように Tenable Nessus Manager が設定されていることを確認します。.**[Enable Agent Updates]** (エージェント更新を有効にする) オプションが有効になっている場合はオフにします。

   リンクされたエージェントは Tenable Nessus Manager に定期的にチェックインします。次回エージェントがマネージャーにチェックインしたときに、そのオペレーティングシステムに適用可能な新しいバージョンが自動的に提供されます。

Tenable Agent のダウングレード

Tenable Agents では、Tenable Nessus を以前のバージョンの Tenable Nessus にダウングレードできます。

以降の例では 2 つのシナリオを説明します。1 つはエージェントソフトウェアを手動でダウングレードするシナリオ、もう 1 つはエージェント更新プランの設定に従いエージェントが自動的にダウングレードするシナリオです。

例 1: エージェントを手動でダウングレード

シナリオ

早期アクセス用リリース 10.0.0 を現在実行していて、前のバージョン 8.3.0 にダウングレードしたいと考えています。

解決策

1. 次のいずれかを実行して、ソフトウェアの自動アップデートをオフにします。

    - Tenable Nessus Manager で、詳細設定の **[Automatically Download Agent Updates]** (エージェントの更新プログラムを自動ダウンロードする) または `agent_updates_from_feed` を無効にします。
    - Tenable Vulnerability Management で、エージェント設定の **[Exclude all agents from software updates]** (ソフトウェアの更新からすべてのエージェントを除外) を有効にします。
    - エージェントで、詳細設定の `disable_core_updates` を有効にします。

2. エージェントをアンインストールします。
3. 古いバージョンのパッケージを手動でダウンロードしてインストールします。この例では、Tenable Agent 8.3.0 です。

例 2: 自分の更新プランに合わせてエージェントを自動的にダウングレード

シナリオ

自動アップデートを有効にしている場合、Tenable Agent をどのバージョンにアップデートするかは Agent Update Plan (エージェント更新プラン) によって決定されます。このシナリオでは、更新プランが ga に設定されています。これは、エージェントが最新の一般提供 (GA) リリースに自動的に更新されることを意味します。現在 Tenable Agent の GA バージョン (10.0.0 など) を使用しています。

しかし、更新プランの設定を stable に変更しました。これにより、エージェントは更新を遅らせ、古いリリースを維持します。

結果

新しいエージェント更新プランの設定に従い、エージェントのバージョンは (現行の) 最新 GA バージョンより古いリリースになります。したがって、エージェントのバージョンをこの設定に合わせるために、次回エージェントがアップデートをチェックすると、エージェントは自動的に古いバージョンになります。Tenable Agent は、最新の GA バージョンの 1 つ前のリリースである 8.3.0 に自動的にダウングレードします。

Tenable Agent のバックアップ

Tenable Agent CLI コマンド を使用して Tenable Agent をバックアップし、後から任意のシステムで復元できます (異なるオペレーティングシステムでも復元可能です)。Tenable Agent をバックアップすると、個人設定は保存されます。Tenable Agent はスキャン結果はバックアップしません。

> **注意:** Linux システムと Windows システムとの間でプラットフォームをまたぐバックアップと復元を行った場合、Tenable Agent を復元した後に、スケジュールを使用する Tenable Agent の設定 (スキャンのスケジュールなど) は再度行う必要があります。これは、双方のオペレーティングシステムで異なるタイムゾーン名が使用されているため、これらのプラットフォームの間でスケジュールが正しく転送されないためです。

Tenable Agent をバックアップするには

1. コマンドターミナルから Tenable Agent にアクセスします。
2. Tenable Agent バックアップファイルを作成します。

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

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

   - Linux : `/opt/nessus_agent/var/nessus`
   - Windows: `C:\ProgramData\Tenable\Nessus Agent\nessus\`
   - Mac: `/Library/NessusAgent/run/var/nessus/`

次の手順

- Tenable Agent の復元

Tenable Agent の復元

Tenable Agent CLI コマンド を使用して、Tenable Agent の以前のバックアップを使用して後から任意のシステムで復元できます (異なるオペレーティングシステムでも復元可能)。Tenable Agent をバックアップすると、個人設定も保存されます。Tenable Agent はスキャン結果は復元しません。

注意: Linux システムと Windows システムとの間でプラットフォームをまたぐバックアップと復元を行った場合、Tenable Agent を復元した後に、スケジュールを使用する Tenable Agent の設定 (スキャンのスケジュールなど) は再度行う必要があります。これは、双方のオペレーティングシステムで異なるタイムゾーン名が使用されているため、これらのプラットフォームの間でスケジュールが正しく転送されないためです。

始める前に

- Tenable Agent のバックアップ

Tenable Agent を復元するには、以下を行います。

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

   例

   ```
   # systemctl stop nessusagent
   ```

   Tenable Agent によってすべてのプロセスが終了します。
3. 以前に保存したバックアップファイルから Tenable Agent を復元します。

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

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

   例

   ```
   # systemctl stop nessusagent
   # systemctl start nessusagent
   ```

   Tenable Agent が初期化を開始し、バックアップからの設定を使用します。

Tenable Agent のリンク解除

エージェントを手動でリンク解除すると、エージェントはマネージャーのリンク済みエージェントリストからは消えますが、関連データはエージェント設定で指定された期間保持されます。エージェントを手動でリンク解除すると、そのエージェントが Tenable Nessus Manager または Tenable Vulnerability Management に自動的に再リンクすることは*ありません*。エージェントのリンクを解除しても、エージェントサービス自体は停止しません。エージェントはホスト上で実行を続けます。

`# nessuscli agent unlink` コマンドを実行して、`nessuscli` ツールからエージェントのリンクを解除できます。

マネージャーからエージェントのリンクを解除することもできます。詳細は、次のドキュメントを参照してください。

- Tenable Nessus Manager でエージェントのリンクを解除するには、*Tenable Nessus ユーザーガイド*のエージェントのリンク解除を参照してください。
- Tenable Vulnerability Management でエージェントのリンクを解除するには、*Tenable Vulnerability Management ユーザーガイド*のエージェントのリンク解除を参照してください。

ヒント: エージェントの*リンク解除とは*、Tenable Nessus Manager または Tenable Vulnerability Management であれ、エージェントとマネージャーの間の接続を解除する行為を指します。マシンからエージェントを削除またはアンインストールする場合は、Tenable Agent の削除 を参照してください。

Tenable Agent の削除

このセクションでは、Tenable Agent をホストからアンインストールする方法について説明します。

注意: ホストにエージェントをインストールしたまま、マネージャーからエージェントを削除する方法については、Tenable Agent のリンク解除 を参照してください。

Windows での Tenable Agent のアンインストール

Windows ユーザーインターフェースまたは Windows CLI を使用して、Windows からエージェントをアンインストールできます。

始める前に

- 管理ツールからエージェントへのリンクを解除します。

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

1. Windows で、**[Add or Remove Programs]** (プログラムの追加または削除) または**[Uninstall or change a program]** (プログラムのアンインストールまたは変更) ができる場所に移動します。
2. インストール済みプログラムのリストで、**Tenable Agent** 製品を選択します。
3. **[Uninstall]** (アンインストール) をクリックします。

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

   Windows で Nessus 関連のファイルとフォルダーがすべて削除されます。

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

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

   ```
   msiexec.exe /x <path to Tenable Agent package>
   ```

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

次の手順

- Tenable Agent をシステムに再インストールする予定の場合、リンクエラーを回避する方法に関するナレッジベースの記事を参照してください。

Linux での Tenable Agent のアンインストール

コマンドラインから Linux 上のエージェントをアンインストールできます。

始める前に

- 管理ツールからエージェントへのリンクを解除します。

Tenable Agent を Linux からアンインストールする方法

1. ご使用の Linux 系オペレーティングシステム固有の削除コマンドを入力します。

   Tenable Agent 削除コマンドの例

Debian/Kali と Ubuntu

```
# dpkg -r NessusAgent
```

Red Hat 6 および 7、Oracle Linux 6 および 7

```
# yum remove NessusAgent
```

Red Hat 8 以降、Oracle Linux 8 以降、Fedora

```
# dnf remove NessusAgent
```

SUSE

```
# sudo zypper remove NessusAgent
```

注意: システムから Tenable Agent を完全に削除するには、削除コマンドの実行後にエージェントファイルシステムを手動で削除する必要があります。

次の手順

- Tenable Agent をシステムに再インストールする予定の場合、リンクエラーを回避する方法に関するナレッジベースの記事を参照してください。

macOS での Tenable Agent のアンインストール

macOS からエージェントをアンインストールするには、関連するエージェントディレクトリを削除し、エージェントサービスを無効にします。

始める前に

- 管理ツールからエージェントへのリンクを解除します。

Tenable Agent を macOS からアンインストールする方法

1. Tenable Agent ディレクトリを削除します。コマンドプロンプトから、次のコマンドを入力します。

   - `$ sudo rm -rf /Library/NessusAgent`
   - `$ sudo rm /Library/LaunchDaemons/com.tenablesecurity.nessusagent.plist`
   - `$ sudo rm -r "/Library/PreferencePanes/Nessus Agent Preferences.prefPane"`

   注意: システムから Tenable Agent を完全に削除するには、削除コマンドの実行後にエージェントファイルシステムを手動で削除する必要があります。

2. Tenable Agent のサービスを無効にします。

   a. コマンドプロンプトから、次のコマンドを入力します。

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

   b. 指示されたら、管理者パスワードを入力します。

次の手順

- Tenable Agent をシステムに再インストールする予定の場合、リンクエラーを回避する方法に関するナレッジベースの記事を参照してください。

エージェントのステータス

Tenable 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 (オンライン)	Tenable Agent を含むホストは、現在接続済みで、Tenable Nessus Manager または Tenable Vulnerability Management と通信しています。
Offline (オフライン)	Tenable 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 (初期化)	Tenable Agent は、Tenable Nessus Manager または Tenable Vulnerability Management でのチェックインが進行中です。
Unlinked (リンクなし)	(Tenable Nessus Manager のみ) エージェントはリンクされていない状態です。

ステータス	説明
	このステータスのエージェントは、**[Track unlinked agents]** (リンク解除されたエージェントの追跡) が有効になっている場合にのみ存在します。 **注意: [Unlink inactive agents after X days]** (X 日後非アクティブなエージェントをリンク解除する) の設定により自動的にリンク解除されたエージェントがオンラインに戻ると、Tenable Nessus Manager に自動的に再リンクされます。手動でリンクを解除したエージェントは、手動で再リンクする必要があります。

スキャン

Tenable Nessus ManagerとTenable Vulnerability Managementでは、Tenable Agentsスキャンの作成と設定ができます。

エージェントスキャン、エージェントグループ、エージェントテンプレート、エージェント設定の詳細については、組織で使用しているマネージャーに応じて、*Tenable 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。

設定

Tenable Agent 設定は、エージェントマネージャーからリモートで (Tenable Vulnerability Management または Tenable Nessus Manager)、またはエージェントのコマンドラインインターフェースでローカルでの 2 通りの方法で設定できます。

Manager で構成される設定

フリーズ期間、ログ記録、プロキシ設定など、ほとんどのエージェント設定は、マネージャーインターフェースから設定できます。

- リンクされたの全般設定を構成します Tenable Agents。
    - Tenable Vulnerability Management – エージェント設定
    - Tenable Nessus Manager – エージェント設定の変更
- 用のフリーズウィンドウを作成、変更、削除します Tenable Agents
    - Tenable Vulnerability Management - フリーズウィンドウ
    - Tenable Nessus Manager - フリーズウィンドウ
- (Tenable Nessus Managerのみ) エージェントログ設定を変更します。
    - Tenable Nessus Manager – ログを管理する

エージェントで設定された設定

コマンドラインインターフェースを使用して、エージェントで 詳細設定 や プロキシ設定を直接設定できます。

詳細設定

エージェントのコマンドラインインターフェースから詳細設定を行うことで、エージェントを手動で設定できます。システム全体のエージェント設定の中には、Tenable Nessus Manager の詳細設定 または Tenable Vulnerability Management の **[Linked Agents]** (リンクされたエージェント) タブから変更できるものもあります (詳細は、*Tenable Vulnerability Management ユーザーガイド*のエージェントの設定を参照してください)。Tenable Agent は、入力された値を検証して、有効な設定のみを許可します。

Tenable Agent の詳細設定

nessuscli ユーティリティを使用して、コマンドラインインターフェースで次のエージェント設定が可能です。

コマンド # nessuscli fix --set *setting=value* を使用します。詳細は、Tenable Agent CLI コマンドを参照してください。

ヒント: 多数のエージェント (10,000 以上) を抱えるお客様の場合、agent_merge_audit_trail、agent_merge_kb、agent_merge_journal_mode、および agent_merge_synchronous_setting の設定を変更することができます。これらの設定を変更すると、エージェントのスキャン結果のマージにかかる時間が大幅に短縮されます。推奨される設定については、次の表の説明を参照してください。

設定	説明	デフォルト	有効な値
agent_update_channel	(Tenable Vulnerability Management にリンクされたエージェントのみ) エージェント更新プランを設定して、エージェントが自動的に更新するバージョンを指定します。 **注意:** Tenable Vulnerability Management にリンクされているエージェントの場合は、エージェントの nessuscli ユーティリティから agent_update_channel コマンドを実行する必要があります。Tenable Nessus Manager にリンクされているエージェントの場合は、Tenable Nessus Manager の nessuscli ユーティリティから agent_	ga	• ga - 一般公開 (GA) され次第、自動的に最新の Agent バージョンへと更新されます。**注意:** この日付は通常、バージョンが一般公開された日から *1 週間後* です。重大なセキュリティ問題に対処するためのバージョンの場合は、Tenable から直ちに公開される場合があります。 • ea - 早期アクセス (EA) 用にリリースされ次第、自動的に最新

設定	説明	デフォルト	有効な値
	`update_channel` コマンドを実行する必要があります。		の Agent バージョンへとアップデートします。通常、一般公開よりも数週間早いタイミングです。 • `stable` - 自動的に最新の Tenable Agent バージョンに更新しません。Tenable が設定した、Tenable Agent の古いバージョンを維持します。これは通常、最新の一般公開バージョンよりも 1 リリース前のものとなりますが、7.7.0 よりも前のバージョンにはなりません。Tenable Agent が新しいバージョンがリリースすると、エージェントはソフトウェアバージョンをアップデートしますが、最新のリリースよりも前のバージョンに留まりま

設定	説明	デフォルト	有効な値
			す。
strict_certificate_validation	この機能を有効にすると、初期リモートリンク中であっても、SSL サーバー証明書を常に検証します (マネージャーが信頼できるルート CA を使用する必要があります)。	no	yes または no
update_hostname	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、新しいホスト名がエージェントのマネージャーで更新されます。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
connection_status_check_time	(Tenable Vulnerability Management にリンクされたエージェントのみ) オフライン時にエージェントが接続ステータスをチェックする頻度を秒単位で設定します。	900	299 より大きい整数
day_to_keep_unused_plugins	(Tenable Vulnerability Management にリンクされたエージェントのみ) エージェントが未使用の	14	7 よりも大きい整数

設定	説明	デフォルト	有効な値
	プラグインセットを削除するまでの期間 (日数) を決定します。 たとえば、この設定を **14** に設定し、エージェントが 14 日以上スキャンにプラグインセットのいずれかを使用しなかった場合、エージェントはそのプラグインセットを削除します。		
detect_duplicates	この設定に関係なく、エージェントは、MAC アドレスの現在のリストをエージェントがリンク時に保持していた MAC アドレスと比較することで、重複しているエージェントかどうかを自動的にチェックします。Tenable Vulnerability Management または Tenable Nessus Manager 8.11.1 以降にリンクされているエージェントの場合、マネージャーは同じチェックを実行して重複するエージェントを特定します。 無効にすると、エージェントは自動的に重複を `backend.log` に記録しますが、アクションは実行	no	yes または no

設定	説明	デフォルト	有効な値
	されません。 有効にした場合、エージェントまたはマネージャーのいずれかが重複するエージェントを検出すると、エージェントは自動的にそのリンクを解除し、識別情報 (例: UUID) を再生成して、再度リンクできるようにします。このイベントは、`backend.log` に記録されます。エージェントを手動で再リンクする必要があります。		
disable_core_updates	`yes` に設定すると、エージェントは自動コアアップデートをリクエストしません。ただし、ソフトウェアのバージョンは手動でアップグレードできます。エージェントは引き続きプラグインアップデートを受信できます。	no	`yes` または `no`
logfile_max_files	Tenable Agent がディスク上に保持する `nessusd.messages` ファイルの最大数を決定します。`nessusd.messages` ログファイル数が指定された値を超えると、	Tenable Nessus – 100 Tenable Agent – 2	1 から 1000 までの整数

設定	説明	デフォルト	有効な値
	Tenable Agent は最も古いログファイルを削除します。		
logfile_max_size	`nessusd.messages` ファイルの最大サイズ (MB) を決定します。ファイルサイズが最大サイズを超えると、Tenable Agent は新しいメッセージログファイルを作成します。	Tenable Nessus –512 Tenable Agent – 10	1 から 2048 までの整数
logfile_rotation_time	Tenable Agent メッセージログファイルのローテーションの頻度を日数で指定します。	1	1 から 365 までの整数
logfile_rot	Tenable Agent がメッセージログファイルをローテーションする基準が、ローテーションの最大サイズと時間のどちらであるかを決定します。	サイズ	• `size` – Tenable Agent は、`logfile_max_size` で指定されたサイズに基づいてログファイルをローテーションします。 • `time` – Tenable Agent は、`logfile_rotation_time` で指定された時間に基づいてログファイルをローテーションします。

設定	説明	デフォルト	有効な値
long_term_upload_interval_seconds	(Tenable Vulnerability Management にリンクされたエージェントのみ) スマートスキャン結果のアップロードを次回試行するまでエージェントが待機する秒数を設定します。	180	59 よりも大きい整数
report.max_ports	ポートの最大数です。スキャン結果にこの値より多くのポートが報告された場合、Tenable Nessus はポートのスキャン結果を破棄します。この制限は偽のターゲットのポートが大量に報告されるのを回避するためのものですが、スキャン結果データベースから有効な結果が削除されてしまう可能性もあります。このような問題が発生する場合は、デフォルト値を上げることをお勧めします。	1024	整数
portscanner.max_ports	Tenable Nessus ポートスキャンプラグインがオープンとしてマークできるポートの最大数。これには、適切なポートスキャナーと、NASL 関数 `scanner_add_port()`	1024	0 から 65535 までの整数

設定	説明	デフォルト	有効な値
	を呼び出すプラグインが含まれます。		
Maximum_scans_per_day	エージェントが 1 日につき実行できる最大スキャン数を設定します。	10	整数の 1 ～ 48
min_metadata_update_interval	(Tenable Vulnerability Management にリンクされたエージェントのみ) エージェントがメタデータの Tenable Vulnerability Management へのプッシュを次回試行するまでの最小分数を決定します。 **注意:** エージェントは、メタデータが変更された場合にのみ、メタデータを Tenable Vulnerability Management にプッシュしようとします。	10	4 よりも大きい整数
dumpfile_max_files	ディスク上に保存される `nessusd.dump` ファイルの最大数を設定します。この設定では、ファイル数が指定された値を超えると、最も古いダンプファイルが削除されます。	100	1 から 1000 までの整数
dumpfile_max_size	`nessusd.dump` ファイルの最大サイズ (MB) を設定します。ファイルサイズ	512	1 から 2048 までの整数

設定	説明	デフォルト	有効な値
	が最大サイズを超えると、新しいダンプファイルが作成されます。		
offline_agent_scan_trigger_ Execution_threshold_days	(Tenable Vulnerability Management にリンクされたエージェントのみ) ルールベースのスキャンが起動されなくなるまでのオフラインの日数を決定します。	14	ゼロより大きい整数
plugin_load_performance_mode	プラグインのコンパイルパフォーマンスを設定します。この設定は CPU 使用率に影響を与えます。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。 • `low`: 1 つのスレッドだけを使用します。利用可能な時間よりも意図的に少ない時間を消	Tenable Agent 10.8.3 以降 - `medium` Tenable Agent 10.8.2 以前 - `high`	`low`、`medium`、または `high`

設定	説明	デフォルト	有効な値
	費し、1 つのコアの使用率を約 50% にします。 • medium: 利用可能なコア数の最大半分のスレッドを使用します。8 コア以上のシステムでは最大 4 コアを使用します。常に 1 つ以上のスレッドを使用します。 • high: 利用可能なコアと同じ数のスレッドを使用します (最大 8 個のスレッド)。 詳細については、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。 **注意:** VDI や ESXi などの共有リソース環境の場合、Tenable は、プラグインコンパイルパフォーマンスを medium または low に設定することを推奨しています。		
scan_performance_mode	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	high	low、medium、または high

設定	説明	デフォルト	有効な値
	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、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。		
skip_asset_observation_on_update	Tenable Vulnerability Management にリンクするときに、エージェントが資産メタデータのみを更新するかどうかを決定します。この設定を no に設定すると、エージェントは詳細設定に基づいて新しい資産メタデータで Tenable Vulnerability Management を更新します。	no	yes または no
ssl_cipher_list	エージェントアウトバウンド接続に使用する暗号リストを設定します。	compatible	• legacy - 旧式の API と統合できる暗号のリスト。 • compatible - 安全な暗号のリスト。最新のす

設定	説明	デフォルト	有効な値
			べての暗号が含まれていない場合があります。 • modern - 最新の最も安全な暗号のリスト。 • custom - カスタム OpenSSL 暗号リスト。有効な暗号リストの形式については、OpenSSL のドキュメントを参照してください。 **ヒント**: Tenable でサポートされている暗号のリストについては、*Tenable Vulnerability Management ユーザーガイド*のシステム要件を参照してください。
ssl_mode	サポートされる TLS の最小バージョンです。	tls_1_2	• ssl_3_0 – SSL v3 以上 • tls_1_2 – TLS v1.2 以上

Tenable Agent の安全な設定

nessuscli ユーティリティを使用して、コマンドラインインターフェースで次の安全な設定が可能です。

コマンド `# nessuscli fix --secure --set setting=value` を使用します。詳細は、Tenable Agent CLI コマンドを参照してください。

警告: ドキュメントにない `--secure` 設定の変更は Tenable でサポートされない設定となるため推奨していません。

[設定]	説明	有効な値
`auto_proxy`	(Windows のみ) 有効な場合、エージェントは Web Proxy Auto Discovery (WPAD) を使用して Proxy Auto Config (PAC) ファイルを取得し、プロキシを設定します。この設定は、他のすべてのプロキシ設定に優先します。 無効な場合、エージェントは残りのプロキシ設定をデフォルトにします。	`true` または `false`
`ignore_proxy`	有効にした場合、エージェントは、設定されたプロキシを使用する代わりに、10 回失敗するまでマネージャーへの直接接続を試行します。 無効にした場合、エージェントは、設定されたプロキシを使用して、3 回失敗するまで接続を試行します。 プロキシ接続のフォールバックで説明されているように、この設定は自動的に変更されます。この設定を手動で設定することもできます。ただし、いずれかの時点で、エージェントがプロキシ接続のフォールバックで説明されている条件の 1 つを満たした場合、エージェントは自動的に設定を変更します。	`yes` または `no`
`ms_proxy`	有効にすると、エージェントはプロキシを使用してマネージャーに接続します。	`true` または `false`
`[proxy](プロキシ)`	プロキシサーバーのホスト名または IP アドレス。	文字列
`proxy_port`	プロキシサーバーのポート番号。	文字列
`proxy_auth`	(オプション) 認証を使用してプロキシに接続する場合は、認証スキームを指定します。	`basic`、`digest`、`ntlm`、また

[設定]	説明	有効な値
		は auto
proxy_username	認証を使用してプロキシに接続する場合、プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。	文字列(スペースがある場合は、引用符 (") を使用します)
proxy_password	プロキシで認証する場合、ユーザー名に関連付けられたパスワード。	文字列

Tenable Nessus Manager の詳細設定

Tenable Nessus Managerの **[設定]** > **[詳細設定]** > **[エージェントとスキャナー]** セクションで、次のシステム全体のエージェント設定が可能です。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。

設定	説明	デフォルト	有効な値	再起動が必要
agent_auto_delete	エージェントが非アクティブになってから agent_auto_delete_threshold で設定されている期間が経過した後、エージェントが自動的に削除されるかどうかを制御します。	×	yes または no	×
agent_auto_delete_threshold	agent_auto_delete が yes に設	60	1 から 365 までの整数	×

設定	説明	デフォルト	有効な値	再起動が必要
	定されている場合に、非アクティブなエージェントが自動的に削除されるまでの日数です。			
agent_auto_unlink	エージェントが非アクティブになってから agent_auto_unlink_threshold で設定されている期間が経過した後、エージェントが自動的にリンク解除されるかどうかを制御します。	×	yes または no	×
agent_auto_unlink_threshold	agent_auto_unlink が yes に設定されている場合に、非アクティブなエージェントが自動的にリンク解除されるまでの日数です。 **注意:** この値は、agent_auto_delete_threshold の値より少なくする必要があります。	30	30 から 90 までの整数	×
agents_progress_viewable	エージェント数がこの	100	これは整数で表示されま	×

設定	説明	デフォルト	有効な値	再起動が必要
	設定値を超えると、スキャンでエージェントから情報が収集されても、Tenable Nessus Manager はエージェントの詳細情報を表示しません。その代わりに、スキャンが完了したときに、スキャン結果が収集されて閲覧できることを示すメッセージが表示されます。		す。 ゼロに設定された場合、デフォルト値の 100 に戻ります。	
agent_updates_from_feed	この機能を有効にすると、Tenable Agent ソフトウェアの新しい更新プログラムが自動でダウンロードされます。	○	yes または no	○
cloud.manage.download_max	エージェントの更新プログラムを同時にダウンロードできる最大数です。	10	整数	×
agent_merge_audit_trail	エージェントスキャン結果の監査証跡データをメインのエージェントデータベースに含めるかどうかを	false	true または false	×

設定	説明	デフォルト	有効な値	再起動が必要
	決めます。監査証跡データを除外すると、エージェントスキャン結果の処理パフォーマンスが大幅に向上します。 この設定が [false] に設定されていると、個別のスキャンやポリシーの **[Audit Trail Verbosity]** (監査証跡の詳細) 設定がデフォルトで `[No audit trail]` (監査証跡なし) に設定されます。 Nessus 8.3 以降で利用できます。			
agent_merge_kb	メインのエージェントデータベースにエージェントのスキャン結果の KB データを含めます。KB データを除外すると、エージェントスキャン結果の処理パフォーマンスが大幅に向上します。	`false`	`true` または `false`	×

設定	説明	デフォルト	有効な値	再起動が必要
	この設定が [false] に設定されていると、個別のスキャンやポリシーの **[Include the KB]** (KB を含む) 設定がデフォルトで `[Exclude KB]` (KB を含まない) に設定されます。 Nessus 8.3 以降で利用できます。			

agent_merge_journal_mode	エージェントの結果を処理するときに使用するジャーナルモードを設定します。環境によっては、これによって処理パフォーマンスが向上する場合がありますが、クラッシュが発生した場合にスキャン結果が破損するリスクもあります。詳細は、sqlite3 のドキュメントを参照してください。
	
	Nessus 8.3 以降で利用できます。
		`DELETE`	`MEMORY`
			
			`TRUNCATE`
			
			`DELETE`
				×

設定	説明	デフォルト	有効な値	再起動が必要
agent_merge_synchronous_setting	エージェントの結果を処理するときに使用するファイルシステムの同期モードを設定します。この設定をオフにすると処理パフォーマンスは大きく向上しますが、クラッシュが発生した場合にスキャン結果が破損するリスクもあります。詳細は、sqlite3 のドキュメントを参照してください。 Nessus 8.3 以降で利用できます。	FULL	OFF NORMAL FULL	×
track_unique_agents	この機能を有効にすると、Tenable Nessus Manager はリンクしようとしているエージェントの MAC アドレスが、同じホスト名、プラットフォーム、ディストリビューションを持つ、リンク済みエージェントの MAC アドレスと一致するかどうかをチェックします。	×	yes または no	×

設定	説明	デフォルト	有効な値	再起動が必要
	Tenable Nessus Manager はエージェントの重複があればそれを削除します。			

プロキシ設定

プロキシ設定を行う

次のいずれかの方法で、プロキシを介してマネージャー (Tenable Nessus Manager または Tenable Vulnerability Management) に接続するように Tenable Agent を設定できます。

- 初期インストールおよびリンク中

  詳細については、Tenable Agent CLI コマンド のリンクコマンドのプロキシ設定を参照してください。

- インストールしてリンクした後

  初期リンク後、コマンドラインでプロキシを設定したり、既存のプロキシ設定を変更したりできます。詳細は、Tenable Agent の安全な設定を参照してください。

プロキシ接続のフォールバック

エージェントがマネージャーに接続するためにプロキシを使用している場合、接続に失敗した場合に備えてプロキシフォールバックが組み込まれています。

自動フォールバックプロセスは次のように行われます。

1. エージェントがプロキシ経由でマネージャーにアクセスできず、3 回続けて失敗する場合、エージェントはマネージャーへの直接接続を試みます。
2. エージェントがマネージャーに直接接続されると、エージェントは 安全な設定 である `ignore_proxy` を自動的に `yes` に設定します。ユーザーがこの設定を有効にすると、エージェントは、以降の試行でプロキシを使用せずに、マネージャーに直接接続します。

3. ただし、エージェントがマネージャーに直接 10 回続けて接続できない場合、エージェントはプロキシ経由の接続を再試行します。エージェントがプロキシ経由の接続に成功すると、エージェントは自動的に ignore_proxy を no に設定します。これは、エージェントが以降の試行でプロキシを使用して接続することを意味します。

4. このプロセスは、エージェントがプロキシへの接続に失敗するか、マネージャーへの直接接続に失敗するかによって、必要に応じて繰り返されます。

安全な設定である ignore_proxy を yes または no に変更して、自動フォールバックプロセスをいつでも中断できます。これにより、エージェントは、ユーザーの設定内容に応じて、直接接続かプロキシ経由の接続を試行します。ただし、いずれかの時点で、エージェントが上記のいずれかの条件を満たした場合(プロキシ経由で 3 回続けて接続できないなど)、自動フォールバックプロセスが再開します。

追加のリソース

このセクションには、次のリソースが含まれています。

- 大規模デプロイメントのサポート
- Tenable Agent をインストールした Windows または Linux のゴールデンイメージの作成
- ログを管理する
- Tenable Nessus サービス
- Tenable Agent CLI コマンド
- プラグインのアップデート
- Rule-based Trigger File Location

Tenable Vulnerability Management での資産重複を回避するためのエージェントプロファイルの設定

Tenable Nessus スキャナーと Tenable Agents の両方でホストをスキャンする Tenable Vulnerability Management 設定では、すでにエージェントがインストールされている資産を、スキャナーがスキャンして記録する場合があります。その場合、資産が Tenable Vulnerability Management の 2 つ (場合によってはそれ以上) の個別の資産として識別されます。

Tenable Agents バージョン 10.6.0 以降では、Tenable Vulnerability Management エージェントプロファイルで [**Open Agent Port**] (**高度な資産識別** 設定とも呼ばれます) を設定することで、このような資産の重複を回避できます。

エージェントプロファイルの **[Open Agent Port]** (エージェントポートを開く) を有効にして設定すると、そのプロファイルのエージェントは、インストールされているホストでエージェント識別サービスを実行できるようになります。このサービスは、ホスト上で設定可能なポートを開き、インストール済みのエージェントがすでにホストを資産としてインベントリに入れたことを、Tenable スキャナーが識別できるようにします。認証されていないリモートネットワークスキャンは、開いているエージェントポートを介してエージェントの Tenable UUID を識別します。

これにより、ホストがスキャナーのネットワークスキャンの対象であるか、エージェントスキャンを生成しているかに関わらず、ホストが Tenable Vulnerability Management に確実に単一の資産として記録されます。

エージェントプロファイルの **[Open Agent Port]** (エージェントポートのオープン) を設定する方法については、*Tenable Vulnerability Management ユーザーガイド*のエージェントプロファイルを参照してください。

考慮事項

[Open Agent Port] (エージェントポートのオープン) を設定する際は、次のことを考慮してください。

- **[Open Agent Port]** (エージェントポートのオープン) 設定を使用できるのは、エージェントのバージョン 10.6.0 以降のみです。この設定は、以前のバージョンのエージェントには適用されません。
- **[Open Agent Port]** (エージェントポートのオープン) を設定すると、ネットワークスキャナーは、選択されたポートで各ターゲットシステムをプローブできるようになります。
- エージェント識別サービスは、エージェントプロファイルで有効な **[Open Agent Port]** (エージェントポートのオープン) が指定されている場合にのみ開始されます。
- エージェント識別サービスは、エージェントプロファイルの **[Open Agent Port]** (エージェントポートのオープン) で指定された TCP ポートを開いてリッスンしようとします。ホストにローカルのファイヤーウォールまたはホスト保護製品がインストールされている場合は、エージェント識別サービスが着信接続に対してこのポートを開けるように設定する必要があります。Tenable では、**[Open Agent Port]** (エージェントポートのオープン) 機能が中断することなく動作するように、Tenable Agent ファイルとプロセスを許可リストに登録することを推奨しています。
- macOS および Linux では、エージェント識別サービスは実行のために使用する低い権限のサービスアカウントを作成します。Windows では、エージェント識別サービスは整合性の低いプロセスとして実行されます。
- エージェントに割り当てられた **[Open Agent Port]** (エージェントポートのオープン) は、エージェントがアップグレードまたは再起動したり、ホストが再起動したりするたびにポートを再び開きます。
- エージェント識別サービスが 2 つの Tenable ネットワークに属するレコードを検出した場合、資産を最後に検出したスキャナーのネットワークにマージされた資産が追加されます。
- macOS および Linux ホストで、エージェント識別サービスには実行するためのシステムユーザーが必要です。**[Open Agent Port]** (エージェントポートのオープン) を最初に構成するとき、エージェントは自動的に、macOS ホストの場合は **_tenabletag**、Linux ホストの場合は **tenabletag** というシステムユーザーを作成します。tenabletag ユーザーはロックされたシステムユーザーであるため、ログインには使用できません。

macOS または Linux ホストから Tenable Agent をアンインストールする際、UID マッピングを保持するために Tenabletag ユーザーは削除されません。このユーザーを削除するには、オペレーティングシステムのユーザー削除のドキュメントを参照してください。

- すべてのオペレーティングシステムで、資産 UUID サービスはオペレーティングシステムに基本レベルの IPv6 サポートがあることを必要としますが、どのネットワークインターフェースでも IPv6 自体を有効にする必要があるわけではありません。Linux では、カーネル起動パラメーターを介して Linux IPv6 ドライバを無効にすることを推奨する設定ガイドに従っている古い Linux ディストリビューションで、これが問題を引き起こす可能性があります。このようなシステムでは、カーネル起動コマンドラインで IPv6 を無効にする代わりに、/etc/sysctl.conf の `sysctl` パラメーターを通して IPv6 を無効にできます。これにより、システムで IPv6 を有効にすることなく、資産 UUID サービスが機能するようになります。

  ```
  net.ipv6.conf.all.disable_ipv6 = 1
  net.ipv6.conf.default.disable_ipv6 = 1
  ```

  これは、資産 UUID サービスを使用しながらホストで IPv6 を明示的に無効にしようとする場合にのみ必須になります。さまざまな Linux ディストリビューション用の最新の CIS ベンチマークでは、IPv6 を無効化することは推奨されなくなりました。ただし、CIS ベンチマークの古いエディションでは、IPv6 を無効化するためのより邪魔にならない方法として上記の設定が提供されています。

ログとトラブルシューティング

[Open Agent Port] (エージェントポートのオープン) に関するログ情報は、エージェントバグレポートのバンドルと、次のディレクトリで確認できます。

オペレーティングシステム	ログの場所
Windows	C:\ProgramData\Tenable\NessusAgent\nessus\mod\com.tenable.agent_identifier_service\data\com.tenable.agent_identifier_service.log
macOS	/Library/NessusAgent/run/var/nessus/mod/com.tenable.agent_identifier_service/data/com.tenable.agent_identifier_service.log
Linux	/opt/nessus_agent/var/nessus/mod/com.tenable.agent_identifier_service/data/com.tenable.agent_identifier_service.log

エージェント識別サービスが動作していることを確認するには、プラグイン 191492 - Tenable エージェント識別を表示します。エージェント識別サービスがトリガーされ、検出されたエージェントの Tenable UUID を提供すると、プラグインは情報レベルの検出結果を生成します。

NIAP に準拠する Tenable Agent の設定

Tenable Agent を National Information Assurance Partnership (NIAP) 標準に適合させる必要がある場合、関連する設定が NIAP 標準に準拠するように Tenable Agent を設定できます。

始める前に

- Tenable Agent が Tenable Nessus Manager にリンクされている場合は、Tenable Nessus Manager の CA 証明書が custom_CA.inc または known_CA.inc にあることを確認してください。
- Tenable Agent がインストールされているホストのオペレーティングシステムが提供するフルディスク暗号化機能が有効になっていることを確認します。

NIAP に準拠するよう Tenable Agent を設定するには、次の手順に従います。

1. コマンドラインインターフェースからエージェントにアクセスします。
2. コマンドラインインターフェースを使用して NIAP モードを有効にします。
    - コマンドラインで、次のコマンドを入力します。

      ```
      nessuscli fix --set niap_mode=enforcing
      ```

      Linux の例

      ```
      /opt/nessus_agent/sbin/nessuscli fix --set niap_mode=enforcing
      ```

    Tenable Agent は以下を実行します。

    注意: Tenable Agent が NIAP モードの場合、Tenable Agent が NIAP モードのままである限り、Tenable Agent は以下の設定をオーバーライドします。NIAP モードを無効にすると、Tenable Agent は以前の設定に戻ります。

- SSL モード (`ssl_mode`) を TLS 1.2 (`niap`) でオーバーライドします。
- SSL 暗号リスト (`ssl_cipher_list`) の設定を、NIAP 準拠の暗号 (`niap`) でオーバーライドします。そうすると、次の暗号が設定されます。
    - ECDHE-RSA-AES128-SHA256
    - ECDHE-RSA-AES128-GCM-SHA256
    - ECDHE-RSA-AES256-SHA384
    - ECDHE-RSA-AES256-GCM-SHA384
- 厳格な証明書検証を使用します。
    - 中間証明書に CA 拡張がない場合、証明書チェーンを許可しません。
    - 署名 CA 証明書を使用して、サーバー証明書を認証します。
    - ログインにクライアント証明書認証を使用する際に、クライアント証明書を認証します。
    - Online Certificate Status Protocol (OCSP) を使用して、CA 証明書の失効ステータスをチェックします。証明書が取り消されると、証明書は無効としてマークされます。応答がない場合、証明書は無効としてマークされず、他の方法で有効な場合はその使用が許可されます。
    - 証明書に、known_CA.inc にある有効で信頼できる CA があることを確認します。Tenable Vulnerability Management および plugins.nessus.org の CA 証明書は、プラグインディレクトリの known_CA.inc にすでにあります。
    - Tenable Nessus Manager にリンクされている場合は、Tenable Nessus Manager の CA 証明書が custom_CA.inc または known_CA.inc にあることを確認してください。
- エージェント通信およびデータベース暗号化で最新の検証済み FIPS モジュールを強制実行します。FIPS モジュールはスキャン暗号化に影響しません。

    注意: NIAP モードを強制実行せずに、エージェント nessuscli ユーティリティから FIPS モジュールを強制実行することができます。詳細は、Tenable Agent CLI コマンドを参照してください。

Tenable Agent をインストールした Windows または Linux のゴールデンイメージの作成

Windows または Linux のゴールデンイメージに Tenable Agent をインストールすることができます。ただし、ホストごとに設定する必要があるファイルおよびレジストリ設定があります。

注意: ファイルを削除および変更することで、エージェントは再起動後に新しいファイルを生成します。ホストがこれらのファイルを含めてイメージ化され、いくつかのイメージ化されたエージェントをリンクしようとすると、409 UUID エラーを受け取ります。

以降のステップは管理者権限または root 権限を必要とします。次の手順を実行する必要があるのは、イメージで使用するエージェントがすでに Tenable Vulnerability Management または Tenable Nessus Manager にリンクされている場合のみです。

Tenable Agent がインストールされたゴールデンイメージを作成する方法

1. エージェント サービスを停止します。
2. 次のように、`prepare-image` コマンドを実行します (例として Linux 構文を使用)。

   ```
   ./nessuscli prepare-image
   ```

   このコマンドを実行すると、以下のイメージ作成前のクリーンアップタスクが実行されます。

   - エージェントがリンクされている場合、解除します。
   - エージェント上のすべてのホストタグを削除します。たとえば、Windows ではレジストリキー、Unix では `tenable_tag` などです。
   - エージェントの UUID ファイル (例: `/opt/nessus/var/nessus/uuid` または macOS や Windows の同等ファイル) を削除します。
   - プラグイン dbs を削除します。
   - グローバル db を削除します。
   - `master.key` を削除します。
   - backups ディレクトリを削除します。

   注意: イメージを作成するまで、ホストでエージェント サービスを再起動しないでください。エージェント サービスを再起動すると、`prepare-image` コマンドがパージした UUID、タグ、ファイルが再生成されます。
3. コマンドの実行が完了したら、所属組織の標準に基づいてゴールデンイメージを作成します。

警告: ゴールデンイメージのインスタンスにエージェントをリンクする前に、ゴールデンイメージが適切に設定されていることを確認してください。不適切に設定されたゴールデンイメージを使用すると、複数のエージェントが同じ UUID を共有し、これにより重複資産の問題が発生する可能性があります。

4. config.json メソッドを使用するか、`nessuscli agent link` コマンドを実行することで、ゴールデンイメージの個々のインスタンスでエージェントを Tenable Vulnerability Management または Tenable Nessus Manager にリンクします。

その他のリソース

- 大規模デプロイメントのサポート

お客様のケーススタディ

このお客様のケーススタディでは、実際のお客様の環境における Tenable Agent デプロイメントを紹介します。これらのケーススタディでは、主要な設定とデプロイメントの考慮事項に焦点を当てて説明しています。

- ACME 社の環境には 70,000 個の資産があります。ACME 社は Tenable Vulnerability Management プラットフォームを利用してエージェントスキャン操作を管理し、単一の Tenable Security Center インスタンスを使用して 40 個のスキャナーを管理し、ネットワークと Tenable Agent の両方の評価結果を統合して分析しています。

  詳細については、ACME 社を参照してください。

- Initech 社は、30 以上の子会社、40,000 人のユーザー、60,000 個のデバイス、および 15 万以上のアクティブ IP アドレスを擁するグローバル企業です。Initech は、Tenable Agents を管理するために Tenable Vulnerability Management と Tenable Nessus Manager のハイブリッドソリューションを使用しました。Tenable Vulnerability Management はユーザーワークステーションの Tenable Agent スキャン操作に、Tenable Nessus Manager はサーバーおよびその他の恒久的なオンプレミスインフラに使用されました。その後、Initech 社は、すべての Tenable Agent スキャンデータを Tenable Security Center にインポートし、統合されたレポート作成と分析を実行しています。

  詳細は、Initechを参照してください。

- Sprocket 社は、Tenable Agent の管理とローカルのスキャンおよび監査情報、リモートネットワークスキャン機能、および Tenable Vulnerability Management API を介したサードパーティアプリケーションとの統合に Tenable Vulnerability Management を利用しました。

  詳細については、Sprocket を参照してください。

ACME 社のケーススタディ

ACME 社は、単一の Tenable Security Center インスタンスを使用して 40 個のスキャナーを管理し、約 1,200 店舗のネットワーク脆弱性評価を毎月実行していました。

ACME 社は、既存の運用モデルをアップデートして、Tenable Agents を利用して約 70,000 個の資産の評価結果を収集したいと考えていました。ACME 社は、Tenable Vulnerability Management プラットフォームを使用するハイブリッドアプローチを実装し、エージェントスキャン操作を管理し、エージェントスキャン結果を Tenable Security Center にインポートして、ネットワークとエージェントの両方の評価結果を統合して分析とレポート作成を行いました。

このケーススタディは、ACME 社が Tenable Agents のデプロイを進める際に実装された、設定に関する主な考慮事項をハイライトしています。

目的

Tenable Agent プロジェクトの成功を測定するために ACME 社が定めた主な目標は、ストアインフラ全体でエージェントを利用して詳細な資産データを収集するのと同時に、リモートネットワークスキャンで経験していた現在のネットワーク遅延を軽減することでした。

スキャン範囲

- 全店舗の資産に対するローカルホストスキャンを、エージェントを使用して実装し、現在の非認証ネットワークアクティブスキャンよりも詳細な脆弱性評価結果を、本部のデータセンターから店舗に提供する。
- エージェントスキャンを使用して ACME 社のネットワークへの影響を軽減し、より頻繁にスキャンを実行できるようにする。

ソリューション

このエンタープライズ環境には、Tenable Vulnerability Management と Tenable Security Center のハイブリッドデプロイメントが使用されました。エージェントのスキャン操作には Tenable Vulnerability Management が必要でした。高度な分析とレポートには既存の Tenable Security Center インフラが使用されました。Tenable Vulnerability Management をエージェントスキャン操作に利用することで、ACME 社はオンプレミスのソフトウェアやハードウェアを必要とせずに、多数のエージェントと資産に合わせて自動的にスケールできます。

ACME 社は、既存の Tenable Security Center インフラを利用して、エージェントスキャンデータを Tenable Vulnerability Management から Tenable Security Center にインポートし、統合されたレポート作成と分析を行うことで、脆弱性管理プログラムの目標を達成しました。環境をレポート (Tenable Security Center) と運用 (Tenable Vulnerability Management) の 2 つの層に分割するこのソリューションにより、ACME 社はプラットフォームのデータ取得機能に影響を与えずに、エンドユーザーのレポートエクスペリエンスを最適化することができました。

Tenable Agent 運用層 (Tenable Vulnerability Management)

運用層 (Tenable Vulnerability Management) の主な目的は、エージェント管理とエージェントスキャンの操作を実行することでした。

実行される機能

次のプロセスと使用が運用層 (Tenable Vulnerability Management) で行われます。

- デプロイされたエージェントは Tenable Vulnerability Management にリンクしています。
- エージェントは、エージェントグループに編成されています。インストールプロセス中に、エージェントをエージェントグループに割り当てることができます。
- エージェントスキャンは、エージェントグループを介してエージェントから評価結果を取得するために確立されます。
- Tenable Vulnerability Management によって、エージェントのプラグインとバージョンのアップデートが自動的に適用されます。
- お客様は、エージェントのバージョンアップデートの自動適用をオプトアウトできます。

考慮事項

- エージェントは、ACME 社の社内ソフトウェア配布プロセス (この場合は SCCM) を使用してデプロイされました。
- エージェントグループに含まれるエージェントは、グループあたり 20,000 以下です (推奨は 10,000)。各エージェントグループのエージェント数を制限することで、Tenable Security Center がスキャン結果を正常にインポートできるようになります。この制限は、Tenable Security Center がデプロイメントの一部である場合にのみ適用されます。
- エージェントスキャンは、1 回につき 1 つのエージェントグループに制限されていました。

- エージェントグループのメンバーシップは、企業の目的に応じて、機能的なゾーン (場所、ロールなど) 別に確立されました。
- ACME 社は、エージェントデプロイメントの問題 (インストールの失敗、リンクの失敗など) を帯域外 (ログクライアント、スクリプトなど) で監視しました。
- エージェントはローカルの脆弱性評価のみを実行し、ネットワークベースの評価 (SSL または CGI ネットワークベースの評価など) は行っていません。
- エージェントが https://cloud.tenable.com と通信できるように、ネットワークとファイヤーウォールが設定されました。

層の設計

設計の前提条件は、以下の通りです。

- ACME 社は、社内プロセスとツールを利用して、Tenable Agent ソフトウェアをデプロイします。
- ACME 社は 50～70 のエージェントグループを確立します。
- ACME 社は 50 ~ 70 のエージェントスキャンを設定します。

レポート層 (Tenable Security Center)

レポート層の主な目的は、Tenable Agent の運用層 (Tenable Vulnerability Management) から収集されたデータの一元的な分析とレポート作成を可能にすることでした。ダッシュボード、分析、レポート、および Assurance Report Card がこの層で利用されます。

実行される機能

次のプロセスと使用がレポート層で行われます (Tenable Security Center)。

- Tenable Vulnerability Management が「エージェント対応」スキャナーとして Tenable Security Center に追加されました。
- Tenable Security Center のエージェントスキャンは、Tenable Vulnerability Management からエージェントスキャン結果を取得するように設定されました。
- Tenable Security Center の分析、ダッシュボード、レポート、および Assurance Report Card が、すべての評価タイプ (エージェントおよびネットワークスキャン) で利用されました。

考慮事項

- Tenable は、Tenable Vulnerability Management がエージェントから評価結果を収集する同じ日に、Tenable Vulnerability Management からエージェントのスキャン結果を取得するように Tenable Security Center を設定することを ACME 社に推奨しました。このように設定すると、Tenable Security Center が確実に適切な検出日をキャプチャできるようになります。
- Tenable Security Center はエージェントの結果をサポートするために追加のデータリポジトリを必要としました。リポジトリはそれぞれ 50,000 個程度の資産しか処理できないため、Tenable は ACME 社がエージェントの結果用に Tenable Security Center で 2 つの新しいリポジトリを確立することを推奨しました。
- Tenable Security Center 5.7 で導入されたエージェント固有のリポジトリは、エージェント UUID を利用して、結果を Tenable Security Center にインポートする際の一意性をより適切に追跡できるようになっています。
- ACME 社は、エージェントスキャン結果のインポートから生じた追加データのために CPU/RAM/HDD がさらに必要かどうかを判断するため、現在の Tenable Security Center ハードウェア設定でフル分析を実行する必要がありました。

層の設計

設計の前提条件は、以下の通りです。

- ACME 社は、エージェントのスキャン結果を保存する 2 つのリポジトリを確立します。
- ACME 社は、50 ～ 70 のエージェントスキャンを確立して、Tenable Vulnerability Management からエージェントスキャン結果を取得します。
- ACME 社は、2 つの新しいリポジトリ間で各エージェントスキャンの取得を均等に分散します。
- ACME 社は現在のインフラを評価し、CPU/RAM/HDD がさらに必要かどうかを判断します。

Initech 社のケーススタディ

Initech 社は、30 以上の子会社、40,000 人のユーザー、60,000 個のデバイス、および 15 万以上のアクティブな IP を擁する大規模なフェデレーション環境全体に Tenable Security Center を複層式でデプロイメントしていました。Initech 社は、米国各地にある拠点に 75 個を超えるスキャナーを配置し、毎週ネットワーク脆弱性評価を行っていました。

Initech 社のレポート要件には、システムの評価をより頻繁に行うこと、およびユーザーのノートパソコンが持ち出されている間もリモートでデータを収集できるようにすることが含まれていました。Initech 社はこのタ

スクを完遂するために50,000を超えるTenable Agentsをデプロイしました。そして、Tenable Nessus ManagerとTenable Vulnerability Managementの両方でハイブリッドモデルを使用し、分析とレポートのためにデータをTenable Security Centerにフィードしました。

このケーススタディは、Initech社がTenable Agentsのデプロイを進める際に実装された、設定に関する主な考慮事項をハイライトしています。

目的

Tenable Agentプロジェクトの成功を測定するためにInitech社が定めた主な目標は、データをより頻繁に収集し、リモートシステムを評価し、分散している大規模なエンタープライズ全体の認証情報管理の負荷を軽減することでした。

ソリューション

このエンタープライズ環境のエージェントには、Tenable Nessus ManagerとTenable Vulnerability Managementのハイブリッドデプロイメントが使用されました。Tenable Vulnerability Managementはユーザーワークステーションの Tenable Agent スキャン操作に必須で、Tenable Nessus Managerはサーバーおよびその他の恒久的なオンプレミスインフラに使用しました。

- Tenable Vulnerability Managementのスケーリング機能、アップタイム保証、クラウドの柔軟性を利用して、絶えず変化するワークステーション環境の動的要件に対応しました。
- オンプレミスソリューションにTenable Nessus Managerを使用して、サーバーインフラなどのより機密性の高いシステムのスキャンデータをより詳細に制御できるようにしました。

Initech社は、既存のTenable Security Centerインフラを利用して、エージェントスキャンデータをTenable Nessus ManagerおよびTenable Vulnerability ManagementからTenable Security Centerにインポートして統合されたレポート作成と分析を行うことで、脆弱性管理プログラムの目標を達成しました。

エージェントのデプロイメント (Tenable Nessus ManagerとTenable Vulnerability Management)

Tenable Nessus Managerの主な目的は、オンプレミスインフラ(10,000システム)のエージェント管理とエージェントスキャン操作を実行することでした。一方、Tenable Vulnerability Managementはユーザーワークステーション(40,000システム)のエージェント管理とスキャン操作に使用されていました。

実行される機能

- デプロイされたエージェントは、システムタイプに応じて Tenable Nessus Manager または Tenable Vulnerability Management にリンクされます。
- エージェントは、エージェントグループに編成されています。インストールプロセス中に、エージェントをエージェントグループに割り当てることができます。
- エージェントスキャンは、エージェントグループを介してエージェントから評価結果を取得するために確立されます。
- Tenable Nessus Manager または Tenable Vulnerability Management によって、エージェントのプラグインとバージョンのアップデートが自動的に適用されます。

考慮事項

- Initech の社内ソフトウェア配布プロセス (このケースでは、Altiris、SCCM、Tivoli、Casper などを含む多様なプラットフォーム) を使用して、エージェントがデプロイされました。
- エージェントグループに含まれるエージェントは、グループあたり 2,000 以下です (推奨は 1,000)。各エージェントグループのエージェント数を制限することで、Tenable Security Center がスキャン結果を正常にインポートできるようになります。この制限は、Tenable Security Center がデプロイメントの一部である場合にのみ適用されます。
- エージェントスキャンは、1 回につき 1 つのエージェントグループに制限されていました。
- エージェントスキャン配布の効率が向上したため、エージェントスキャンポリシーは、ネットワークスキャンよりも詳細で冗長でした。
- オンプレミス/サーバーエージェントのスキャンウィンドウは、個々の組織の要件を満たすために、各サブ組織によって選択されたカスタムタイムフレームに制限されていました。
- ユーザーワークステーションのスキャンウィンドウは最大 24 時間に設定され、システムがいつオンになったかにかかわらず完全にカバーされるように、毎日繰り返されました。
- エージェントグループメンバーシップは、企業別に確立され、場合によっては運用層または他の部署の要件に合わせて確立されました。
- Initech 社は、エージェントのデプロイメントの問題 (インストールの失敗、リンクの失敗など) を帯域外 (ログクライアント、スクリプトなど) で監視しました。
- エージェントはローカルの脆弱性評価のみを実行し、ネットワークベースの評価 (SSL または CGI ネットワークベースの評価など) は行っていません。

- ネットワークとファイヤーウォールは、インフラのエージェントがオンプレミスの Tenable Nessus Manager とカスタムポート経由で通信し、ユーザーのワークステーションが https://cloud.tenable.com と通信できるように設定されていました。

層の設計

設計の前提条件は、以下の通りです。

- Initech 社は、社内プロセスとツールを利用して、エージェントソフトウェアをデプロイします。
- Initech 社は、Tenable Nessus Manager と Tenable Vulnerability Management の両方に 30 ～ 50 のエージェントグループを確立します。
- Initech 社は、Tenable Nessus Manager と Tenable Vulnerability Management の両方に 30 ～ 50 のエージェントスキャンを設定します。
- Initech 社は、接続している 10,000 エージェントを処理できるように Tenable Nessus Manager を設定しプロビジョニングします。

レポートおよびネットワークスキャン (Tenable Security Center)

レポート層の主な目的は、Tenable Agents と既存のネットワークスキャンから収集されたデータの一元的な分析とレポート作成を可能にすることでした。ダッシュボード、分析、レポート、および Assurance Report Card がこの層で利用されます。

実行される機能

次のプロセスと使用が Tenable Security Center で行われます。

- Tenable Nessus Manager および Tenable Vulnerability Management が「エージェント対応」スキャナーとして Tenable Security Center に追加されました。
- Tenable Security Center のエージェントスキャンは、Tenable Nessus Manager および Tenable Vulnerability Management からエージェントスキャン結果を取得するように設定されました。
- 既存のデータモデルに従って、エージェントデータが新しいリポジトリに配置されました。
- Tenable Security Center の分析、ダッシュボード、レポート、および Assurance Report Card が、すべての評価タイプ (エージェントおよびネットワークスキャン) で利用されました。

考慮事項

- Tenable Security Center はエージェントの結果をサポートするために追加のデータリポジトリを必要としました。Tenable は、Initech 社がエージェント結果用の複数の新しいリポジトリを Tenable Security Center で確立することを推奨しました。これは、同じリポジトリでエージェントとネットワークの評価結果を組み合わせると、レポート作成で問題が発生する可能性があるためです。
- Initech 社は、エージェントスキャン結果のインポートから生じた追加データのために CPU/RAM/HD がさらに必要かどうかを判断するため、現在の Tenable Security Center ハードウェア設定でフル分析を実行する必要がありました。
- エージェント評価が実行され、データが Tenable Security Center にインポートされた後、既存のネットワークスキャン構造/ポリシーを評価して、データの重複を確実に抑える必要がありました。

層の設計

設計の前提条件は、以下の通りです。

- Initech 社は、エージェントのスキャン結果を保存する複数のリポジトリを確立します。
- Initech 社は、60 ～ 100 のエージェントジョブを確立して、Tenable Vulnerability Management および Tenable Nessus Manager からエージェントスキャン結果を取得します。
- Initech 社は、現在のインフラを評価し、CPU/RAM/HDD がさらに必要かどうかを判断します。
- Initech 社は、既存のスキャン構造/ポリシーを評価して、データの重複を抑えます。

Sprocket 社のケーススタディ

Sprocket 社は、ほぼすべての国にオフィスと従業員を持つグローバル企業です。同社は規模が大きく分散した業務環境のため、セキュリティソリューションを選択および設計する際にいくつかの問題を抱えていました。そのため、以下を実現するソリューションが必要でした。

- 企業のデータセンターのサーバー、クラウドサーバー (Azure と AWS)、および従業員のノートパソコンなどの一時的なデバイスを含む、330,000 個のすべての資産でローカルスキャンを素早く一貫して即座に実行
- データセンターの能力が限界に達していたため、ネットワーク負荷を最低限に抑える
- グローバルに分散した業務環境と、企業のサイロ化に対応するための、認証情報管理の改善
- IT ランドスケープ全体で情報を管理および監視するために使用されるサードパーティアプリケーションと統合する機能

- OT Security、Tenable Web App Scanning、コンテナ環境の増加に合わせてスケールできるソリューション

ソリューション

Sprocket 社は、環境のすべての面を管理するために Tenable Vulnerability Management を利用しました。このソリューションでは、ローカルのスキャンおよび監査情報にはすべての Windows、Linux、macOS デバイスに Tenable Agents を使用し、リモートのネットワークスキャンには組織の各担当地域にあるプライベートクラウドインスタンスに配置された Tenable Nessus スキャナーを使用しました。Tenable Vulnerability Management は、サードパーティおよびカスタマイズされたアプリケーションを利用するために必要な API も提供しました。

Sprocket 社は、資産機能に基づいて、各オペレーティングシステム用にカスタマイズされたスクリプトを使用して Tenable Agents をデプロイしました。Tenable Agents は、オペレーティングシステムと資産所有者に基づいて、130 グループの 1 つに割り当てられました。

よくある質問

エージェントスキャンまたはネットワークベースのスキャンは比較的容易に実行できますか?

各スキャン方法の難易度は、環境や企業のニーズによって異なります。

次の質問事項を考慮してください。

- Tenable Nessus スキャナーおよび Tenable Network Monitor をすべてのネットワークセグメントにインストールすることは可能ですか?
- より少ない数の Tenable Nessus Manager (たとえば、1 ~ 3 つ) をインストールし、エージェントがホップやファイヤーウォールを越えて報告できるようにする方が簡単ですか?
- スキャンウィンドウ中、すべてのシステムがオンラインで接続されており、すべての結果を報告していますか?
- すべてのシステムがスリープ時に正しく設定され、wake-on-lan に適切に応答していますか?
- 多くのシステムの現在の認証情報を追跡または取得するのに時間を費やしていますか?
- ネットワークに、VPN 経由で認証情報をスキャンできない、または企業のネットワークに直接接続されていないときにリモートで動作するノートパソコンが含まれていますか?

エージェントや認証スキャンで連動するプラグインは何ですか?

注意: Tenable Research チームは、プラグインを常に追加したりアップデートしたりしています。プラグインの包括的なリストについては、https://jp.tenable.com/plugins を参照してください。

ほとんどのプラグインは Tenable Agents と連動します。例外は次のとおりです。

- リモートで公開される情報に基づいて動作したり、リモート接続により実行されるアクティビティ (DB サーバーへのログイン、デフォルトの認証情報 (総当たり) の試行、トラフィック関連の列挙など) を検出したりするプラグイン。
- ネットワークチェックに関連するプラグイン。

また、チェックの意図が重複している場合もあります。たとえば、ネットワークベーススキャンで認証なしの OS フィンガープリンティングを使用し、システムにクエリをかけて認証スキャンの OS の正確なバージョンを取得すると、この重複によりネットワーク上の認証検出結果が増えます。これは、ネットワークバージョンの推測の精度が上がるためです。

エージェントは Tenable Vulnerability Management / Tenable Nessus Managerにどのようなデータを送信しますか?

エージェントは次のデータを Tenable Vulnerability Management または Tenable Nessus Manager に送信します。

- 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 2019 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 (詳細は 詳細設定 を参照)
- AWS EC2 インスタンスメタデータ (ある場合)

- 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

ログを管理する

以下のトピックでは Tenable Agent ログファイルについて説明します。エージェントログファイルは次のディレクトリにあります。

オペレーティングシステム	ログの場所
Windows	C:\ProgramData\Tenable\Nessus Agent\nessus\logs
Linux	/opt/nessus_agent/var/nessus/logs
macOS	/Library/NessusAgent/run/var/nessus/logs

nessusd.dump

nessusd.dump は、デバッグ出力に使用されるエージェントのダンプログファイルです。

nessusd.dumpを設定するには

1. エージェントコマンドラインインターフェースを開きます。
2. コマンド `# nessuscli fix --set setting=value` を使用して、次の設定を行います。

名前	[設定]	説明	デフォルト	有効な値
Nessus Dump File Max Files (Nessus ダンプファイルの最大ファイル数)	dumpfile_max_files	ディスク上に保存される nessusd.dump ファイルの最大数を設定します。この設定では、ファイル数が指定された値を超えると、最も古いダンプファイルが削除されます。	100	1 から 1000 までの整数
Nessus Dump File Max Size (Nessus Dump ファイルの最大サイズ)	dumpfile_max_size	nessusd.dump ファイルの最大サイズ (MB) を設定します。ファイルサイズが最大サイズを超えると、新しいダンプファイルが作成されます。	512	1 から 2048 までの整数

詳細は、詳細設定を参照してください。

nessusd.messages

nessusd.messages はエージェントメッセージのログです。

nessusd.messagesを設定するには:

1. エージェントコマンドラインインターフェースを開きます。
2. コマンド `# nessuscli fix --set setting=value` を使用して、次の設定を行います。

名前	[設定]	説明	デフォルト	有効な値
Log File Maximum Files (ログファイルの最大ファイル数)	logfile_max_files	Tenable Agent がディスク上に保持する `nessusd.messages` ファイルの最大数を決定します。`nessusd.messages` のログファイル数が指定された値を超えると、Tenable Agent は最も古いログファイルを削除します。	2	1 から 1000 までの整数
Log File Maximum Size (ログファイルの最大サイズ)	logfile_max_size	`nessusd.messages` ファイルの最大サイズ (MB) を決定します。ファイルサイズが最大サイズを超えると、Tenable Agent は新しいメッセージログファイルを作成します。	10	1 から 2048 までの整数

詳細は、詳細設定を参照してください。

backend.log

`backend.log` はエージェントバックエンドのログです。

`log.json` ファイルを編集して、`backend.log` のログの場所とローテーション戦略を設定できます。また、新しい `reporters[x].reporter` セクションを作成してカスタムファイル名を作成することにより、カスタムログを設定することもできます。

`backend.log`を設定するには:

1. テキストエディターを使用して、対応するディレクトリにある log.json ファイルを開きます。
    - **Windows** – C:\ProgramData\Tenable\Nessus Agent\nessus\log.json
    - **Linux** – /opt/nessus_agent/var/nessus/log.json
    - **macOS** – /Library/NessusAgent/run/var/nessus/log.json
2. backend.log の reporters[x].reporter セクションを編集または作成し、次のパラメーターを追加または変更します。

パラメーター	デフォルト値	変更可能か?	説明
tags	log、info、warn、error、trace	○	ログに含めるログ情報を決定します。 • response – ウェブサーバーのアクティビティログ • info – 特定のタスクの情報ログ • warn – 特定のタスクの警告ログ • error – 特定のタスクのエラーログ • debug – デバッグ出力 • verbose – debug よりも情報の多いデバッグ出力

			• `trace` – 出力の追跡に使用するログ
`type`	`file`	非推奨	ログファイルの種類を決定します。
`rotation_strategy`	サイズ	○	ログがファイルをアーカイブする基準が最大循環サイズ、または循環時間のどちらであるかを指定します。 有効な値: • `size` – `max_size` の規定に従い、サイズを基準としてローテーションします • `daily` – `rotation_time` の規定に従い、時間を基準としてローテーションします
`rotation_time`	86400 (1 日)	○	循環時間 (秒単位)。 `rotation_strategy` が `daily` に設定されている場合にのみ使用します。

max_size	10485760 (10 MB)	○	循環サイズ (バイト単位)。 rotation_strategy が size に設定されている場合にのみ使用します。
max_files	2	○	ファイル循環で許容される最大ファイル数。 最大数には、メインファイルが含まれるため、10 の max_files はメインファイル 1 つとバックアップ 9 つで設定されます。この数を減らすと、古いログは Tenable Nessus によって削除されます。
file	オペレーティングシステムとログファイルに応じて異なる	yes	ログファイルの場所と名前。 デフォルトの Tenable Agent ログファイルの名前を変更した場合、一部の詳細設定でログ設定を変更できなくなる可能性があります。
context	true	非推奨	ログのより多くの文脈情報を有効にします。

format	system	非推奨	出力の形式を決定します。 • combined – ウェブサーバーのログに使用される形式で出力を行います • system – デフォルトのオペレーティングシステムのログ形式で出力を行います

3. log.json ファイルを保存します。
4. エージェントサービスを再起動します。

   エージェントにより、ログ設定が更新されます。

nessuscli.log

nessuscli.log には CLI イベントのレコードが含まれます。

大規模デプロイメントのサポート

環境変数または JSON 設定ファイルを使用して、エージェントを自動的に設定してデプロイできます。これにより、大規模なデプロイメントを効率化できます。

インストール後に初めてエージェントを起動すると、エージェントは最初に環境変数が存在するかどうかをチェックし、次に config.json ファイルがあるかチェックします。エージェントの初回起動時に、エージェントはその情報を使用してマネージャーにリンクし、環境設定を行います。

> **注意:** 情報が環境変数と config.json の両方にある場合、エージェントは両方の情報を使用します。競合する情報がある (たとえば、環境変数と config.json で異なるリンクキーを持つ) 場合、エージェントは環境変数の情報を使用します。

詳細については、次を参照してください。

- 環境変数
- JSON を使用した Tenable Agent のデプロイ

環境変数

環境変数に基づいてを設定する場合、が動作しているシェル環境に次の環境変数をセットすることができます。

インストール後に初めてを起動すると、は最初に環境変数が存在するかどうかをチェックし、次に `config.json` ファイルがあるかチェックします。

リンクの設定

リンクの設定には、次の環境変数を使用します。

- `NCONF_LINK_HOST`: リンク先となるマネージャーのホスト名または IP アドレスです。Tenable Vulnerability Management にリンクするには、cloud.tenable.com を使用します。
- `NCONF_LINK_PORT`: リンクするマネージャーのポート。
- `NCONF_LINK_NAME` - リンク時に使用するの名前。
- `NCONF_LINK_KEY`: リンクするマネージャーのリンクキー。
- `NCONF_LINK_CERT`: (オプション) マネージャーへの接続の検証に使用する CA 証明書。
- `NCONF_LINK_RETRY` - (オプション) がリンク付けを再試行する回数。
- `NCONF_LINK_GROUPS`: (オプション) エージェントを追加する 1 つ以上の既存のエージェントグループ。インストールプロセス中にエージェントグループを指定しない場合、Tenable Nessus Manager または Tenable Vulnerability Management で、リンクされたエージェントを後からエージェントグループに追加できます。コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。例: `"Atlanta,Global Headquarters"`

JSON を使用した Tenable Agent のデプロイ

インストール後に初めてエージェントを起動すると、エージェントは最初に環境変数が存在するかどうかをチェックし、次に `config.json` ファイルがあるかチェックします。エージェントの初回起動時に、エージェントはその情報を使用してマネージャーにリンクし、環境設定を行います。

config.json ファイルで Tenable Agent をデプロイするには

1. config.json ファイルを設定します。

   注意: config.json は ASCII 形式である必要があります。PowerShell などの一部のツールは、デフォルトで他の形式のテストファイルを作成します。

   注意: すべてのセクションは省略可能です。セクションを含めない場合、そのセクションは Tenable Agent を初めて起動したときには設定されません。その設定は、後で手動で設定できます。

   link セクションでは、エージェントをマネージャーにリンクする際の環境設定を設定します。

   ヒント: config.json でリンク設定を指定し、再試行設定を空白のままにすると、nessuscli で --install-offline リンク引数を使用した場合と同じ結果になります。これにより、オフラインであっても、指定されたホストに Tenable Agent がインストールされます。再試行回数が指定されていない場合、エージェントは無期限にホストへのリンクを試行します。

[設定]	説明
名前	(オプション) スキャナーの名前。 エージェントの名前。エージェントの名前を指定しない場合、名前はエージェントをインストールしているコンピューターの名前にデフォルトで設定されます。
[host](ホスト)	リンク先となるマネージャーのホスト名または IP アドレスです。 Tenable Vulnerability Management にリンクするには、cloud.tenable.com を使用します。
[port](ポート)	リンク先のマネージャーのポート。 Tenable Nessus Managerの場合: 8834 またはカスタムポート。 Tenable Vulnerability Managementの場合: 443
[key](キー)	Manager から取得したリンクキー。
[network](ネットワーク)	(オプション、Tenable Vulnerability Management にリンクされたエージェントのみ)

[設定]	説明
	リンク先にするカスタムネットワーク。ネットワークを指定しない場合、エージェントはデフォルトのネットワークに属すことになります。
ms_cert	(オプション) マネージャーのサーバー証明書の検証に使用するカスタム CA 証明書。
[groups](グループ)	(オプション) スキャナーを追加する、1 つ以上の既存のスキャナーグループ。コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。 例: "Atlanta,Global Headquarters" エージェントを追加する 1 つ以上の既存のエージェントグループ。インストールプロセス中にエージェントグループを指定しない場合、Tenable Nessus Manager または Tenable Vulnerability Management で、リンクされたエージェントを後からエージェントグループに追加できます。 コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。 例: "Atlanta,Global Headquarters" **注意:** エージェントグループ名は、大文字と小文字を区別し、正確に一致する必要があります。エージェントグループ名は引用符で囲む必要があります (例: --groups="My Group")。
[retry](リトライ)	(オプション) 最初の試行が失敗した場合に、エージェントがマネージャーへのリンクを試行する回数。 再試行の設定を含めない場合、エージェントはリンクを無期限に

[設定]	説明
	試行します。 **注意:** 再試行を 1 に設定すると、エージェントは最初の失敗から 30 秒後にマネージャーへのリンクを試みます。次の再試行は、前回の再試行の待機の 2 倍の時間になります。たとえば、再試行を 5 に設定した場合、エージェントは、最初の失敗から 30 秒後、2 番目の失敗から 60 秒後、3 番目の失敗から 120 秒後、4 番目の失敗から 240 秒後、5 番目の失敗から 480 秒後にリンクを試行します。
[proxy](プロキシ)	(オプション) プロキシサーバーを使用している場合は、次のように記載します。 • proxy : プロキシサーバーのホスト名または IP アドレス。 • proxy_port: プロキシサーバーのポート番号。 • auto-proxy (Windows のみ): 有効な場合、エージェントは WPAD (Web Proxy Auto Discovery) を使用してプロキシ自動設定 (PAC) ファイルを取得し、プロキシを設定します。この設定は、他のすべてのプロキシ設定に優先します。無効な場合、エージェントは残りのプロキシ設定をデフォルトにします。 **注意:** 設定ファイルに auto_proxy を含める場合は、proxy および proxy_port パラメーターも指定する必要があります。 • proxy_username: プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。 • proxy_password: ユーザー名として指定したユーザーアカウントのパスワード。 • user_agent: ユーザーエージェント名 (プロキシで事前定義されているユーザーエージェントが必要な場合)。 • proxy_auth: プロキシで使用する認証方法。

[設定]	説明
profile_uuid	(オプション) エージェントの割り当て先となるエージェントプロファイルのUUID (例: 12345678-9abc-4ef0-9234-56789abcdef0)。詳細については、「*Tenable Vulnerability Management ユーザーガイド*」のエージェントプロファイルを参照してください。

環境設定セクションでは、詳細な設定を行います。詳しくは、詳細設定を参照してください。

以下はconfig.jsonファイル形式の例です。

```
{ "link": { "name": "sensor name", "host": "hostname or IP address", "port": 443,
"key": "abcdefghijklmnopqrstuvwxyz", "ms_cert": "CA certificate for linking",
"retry": 1, "proxy": { "proxy": "proxyhostname", "proxy_port": 443, "proxy_
username": "proxyusername", "proxy_password": "proxypassword", "user_agent":
"proxyagent", "proxy_auth": "NONE" } }, "preferences": { "global.max_hosts": "500"
} }
```

auto_proxyを使用する場合のconfig.jsonの例を以下に示します。

```
{ "link": { "name": "sensor name", "host": "hostname or IP address", "port": 443,
"key": "abcdefghijklmnopqrstuvwxyz", "ms_cert": "CA certificate for linking",
"retry": 1, "proxy": { "proxy": "proxyhostname", "proxy_port": 443, "auto_proxy":
"true" } } }
```

2. ご使用のオペレーティングシステム用のTenable Agentインストールパッケージをダウンロードしてください。

3. (Windowsのみ) パッケージをインストールする前に、パッケージを変更して、インストール後にエージェントが自動的に起動しないようにする必要があります。これは、エージェントサービスを初めて起動するときに、エージェントがconfig.jsonファイルを読み取る必要があるためです。

   パッケージを変更するには、次のコマンドを実行します。

   ```
   msiexec /i <agent package>.msi NESSUS_SERVICE_AUTOSTART=false /qn
   ```

4. Tenable Agent をインストールします。詳細は、Windows での Tenable Agent のインストール、macOS での Tenable Agent のインストール、またはLinux での Tenable Agent のインストールを参照してください。

5. (macOS のみ) Windows とは異なり、Tenable Agent をインストールする前に自動起動をオフにする方法はありません。したがって、config.json を追加してエージェント サービスを開始する前に、Tenable Agent を新しい状態にリセットする必要があります。

   macOS で Tenable Agent を新しい状態に戻し、config.json を検証し、config.json を適切なディレクトリに配置するには、次のコマンドを実行します。

   ```
   /Library/NessusAgent/run/sbin/nessuscli prepare-image --json=<path to json file>
   ```

   注意: Tenable Agent の自動起動は、Linux パッケージではデフォルトで無効になっています。したがって、Linux を使用している場合は、手順 3 と 5 を無視できます。

6. config.json がまだない場合は、Tenable Agent ディレクトリに配置します。

オペレーティングシステム	config.json ディレクトリ
Windows	C:\ProgramData\Tenable\Nessus Agent\nessus\config.json
Linux	/opt/nessus_agent/var/nessus/config.json
macOS	/Library/NessusAgent/run/var/nessus/config.json

7. エージェント サービスを開始します。

8. オペレーティングシステムに応じて、次のコマンドを実行して config.json 環境設定を検証します。

オペレーティング システム	コマンド
Windows	"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" fix --secure --list

Linux	`/opt/nessus_agent/sbin/nessuscli fix --secure --list`
macOS	`/Library/NessusAgent/run/sbin/nessuscli fix --secure --list`

設定が正常に適用されたことを確認したら、リンク処理は完了です。

Tenable Agent チートシート

利点

- 広いスキャン範囲と継続的なセキュリティを提供
  - ネットワークベースのスキャンを実行することが実用的ではないまたは可能でない場所にもデプロイできます。
  - インターネットに断続的に接続する、ネットワーク外の資産やエンドポイント (ノートパソコンなど) を評価できます。Tenable Agents は、ネットワークの場所に関係なくデバイスをスキャンし、結果をマネージャーに報告できます。
- 認証情報の管理が不要
  - 実行するのにホストの認証情報を必要としません。そのため、認証情報が変更されたときにスキャン設定の認証情報を手動でアップデートしたり、管理者、スキャンチーム、企業内で認証情報を共有したりする必要はありません。
  - ドメインコントローラー、DMZ、認証局 (CA) ネットワークなど、リモートの認証アクセスが望ましくない場所にもデプロイできます。
- 効率的
  - ネットワークスキャンのオーバーヘッドを全体的に削減できます。
  - ローカルホストリソースに依存するので、パフォーマンスオーバーヘッドが最小ですみます。
  - ネットワーク帯域幅の必要量が減ります。これは、低速ネットワークで接続されているリモート設備にとって重要です。
  - セグメント化されたネットワークまたは複雑なネットワーク上にあるスキャンシステムの課題を排除します。

- Tenable Agents は再起動やエンドユーザーの操作なしで自動的にアップデートできるため、メンテナンスが最小ですみます。
- ネットワークにほとんど影響を与えずに大規模な同時並行エージェントスキャンを実行できます。

- デプロイメントとインストールが簡単
  - すべての主要なオペレーティングシステムに Tenable Agents をインストールして操作できます。
  - ノートパソコンなどの一時的なエンドポイントを含め、どこにでも Tenable Agents をインストールできます。
  - Microsoft の System Center Configuration Manager (SCCM) などのソフトウェア管理システムを使用して Tenable Agents をデプロイできます。

制限

- ネットワークチェック – エージェントはネットワークチェックを実行するように設計されていません。そのため、エージェントスキャンのみがデプロイされている場合、特定のプラグイン項目はチェックされず、取得もされません。ネットワークスキャンとエージェントベースのスキャンを組み合わせれば、このギャップを埋めることができます。
- リモート接続 – 特にリモート接続でのみ実行できることをエージェントは感知しません。たとえば、DB サーバーへのログイン、デフォルト認証情報の試行 (総当たり)、トラフィック関連の列挙などです。

Tenable Agents のシステム要件

データフローおよびライセンス要件については、ポート要件とライセンス要件を参照してください。

ハードウェア

Tenable Agents は、軽量で、最小限のシステムリソースのみを使用します。一般的には、Tenable Agent が使用する RAM は 50 ~ 60 MB です (すべてページング可能)。Tenable Agent は、アイドル時にはCPU をほとんど使用しませんが、ジョブ実行中に使用可能な場合は CPU を最大 100% まで使用するように設計されています。

Tenable Agent のリソース使用量の詳細については、ソフトウェアフットプリントを参照してください。

次の表は、Tenable Agent の動作に推奨されるハードウェアの最小要件の概要です。Tenable Agents は、指定と同じ要件を満たす仮想マシンにインストールできます。

ハードウェア	最小要件
プロセッサー	デュアルコア CPU 1 個
プロセッサー速度	1 GHz 以上
RAM	1 GB 以上
ディスク容量	• Agents 8.0 以降: 3 GB 超 (ホストオペレーティングシステムで使用される容量は含まれていません) • Agents 10.0.x 以降: 2 GB 超 (ホストオペレーティングシステムで使用される容量は含まれていません) エージェントは、特定のプロセス (`plugins-code.db` デフラグ処理など) の実行中に、さらに多くの容量を必要とする可能性があります。
ディスク速度	15 ~ 50 IOPS

ソフトウェア

Tenable Agent のソフトウェア要件を確認するには、Tenable Agent のソフトウェア要件を参照してください。

Tenable Agents のインストールとリンク

以下は、コマンドラインを使ったインストール手順です。ユーザーインターフェースを使用してインストールする方法については、Windows での Tenable Agent のインストールまたはmacOS での Tenable Agent のインストールを参照してください。

Linux

パッケージをインストールします。

Red Hat/CentOS/Oracle Linux

```
# dnf install NessusAgent-<version number>-es8.x86_64.rpm
```

Fedora

```
# dnf install NessusAgent-<version number>-fc34.x86_64.rpm
```

Ubuntu

```
# dpkg -i NessusAgent-<version number>-ubuntu1110_i386.deb
```

Debian

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

注意: エージェントをインストールした後に、**/sbin/service nessusagent start** コマンドを実行して手動でサービスを開始する必要があります。

エージェントを Tenable Nessus Manager または Tenable Vulnerability Management にリンクします。

コマンドプロンプトで、`nessuscli agent link` コマンドを使用します。例

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

注意: リンクコマンド全体をコピーして、同じ行に貼り付ける必要があります。そうしないと、エラーが表示されます。

Windows

コマンドラインから Tenable Agents をデプロイしてリンクできます。例

```
msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS="Agent Group Name"
NESSUS_SERVER="192.168.0.1:8834" NESSUS_
KEY=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00 /qn
```

macOS

パッケージをインストールします。

1. Install Nessus Agent.pkg と .NessusAgent.pkg を NessusAgent-<version number>.dmg から展開します。

   注意: .NessusAgent.pkg ファイルは通常 macOS Finder では表示されません。

2. ターミナルを開きます。
3. コマンドプロンプトで、次のコマンドを入力します。

```
# sudo installer -pkg /<path-to>/Install Nessus Agent.pkg -target /
```

エージェントを Tenable Nessus Manager または Tenable Vulnerability Management にリンクします。

1. ターミナルを開きます。
2. コマンドプロンプトで、nessuscli agent link コマンドを使用します。

   例

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

Tenable Agent CLI コマンド

Tenable Agent の一部の機能をコマンドラインインターフェースから実行するには、Agent nessuscli ユーティリティを使用します。

注意: どの Agent nessuscli コマンドも、管理者権限を持つユーザーとして実行する必要があります。

Nessuscli の構文

オペレーティングシステム	コマンド
Windows	`C:\Program Files\Tenable\Nessus Agent\nessuscli.exe <cmd> <arg1> <arg2>`
macOS	`# sudo /Library/NessusAgent/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Linux	`# /opt/nessus_agent/sbin/nessuscli <cmd> <arg1> <arg2>`

Nessuscli のコマンド

コマンド	説明
情報のコマンド	
`# nessuscli help`	`nessuscli` コマンドのリストを表示します。
`# nessuscli -v`	Tenable Agent の現在のバージョンを表示します。
`# nessuscli fix --get <agent setting>`	エージェント設定の現在の値を表示します。
バグレポートコマンド	
`# nessuscli bug-report-generator`	システム診断のアーカイブを作成します。 引数を付けずにこのコマンドを使用すると、ユーティリティによって値を入力するよう促されます。 **オプションの引数** • `--quiet` - ユーザーにフィードバックを求めることなく、バグレポートジェネレーターが実行されます。 • `--scrub` - バグレポートジェネレーターによって IPv4 アドレスの最後の 2 つの 8 ビットがサニタイズされます。

コマンド	説明
	• `--full` - バグレポートジェネレーターによって追加データが収集されます。
画像作成コマンド	
`# nessuscli prepare-image`	以下のように画像処理前のクリーンアップを行います。 • エージェントがリンクされている場合、解除します。 • エージェント上のすべてのホストタグを削除します。たとえば、Windows ではレジストリキー、Unix では `tenable_tag` などです。 • エージェント上のすべての UUID ファイルを削除します。例: `/opt/nessus/var/nessus/uuid` (MacOS/Windows ではこれと同等のもの)。 • プラグイン `dbs` を削除します。 • `global db` を削除します。 • `master.key` を削除します。 • backups ディレクトリを削除します。 **オプションの引数** • `--json=<file>` - 自動設定用の `.json` ファイルを検証し、適切なディレクトリに配置します。
ローカルエージェントのコマンド エージェントステータスのリンク、リンク解除、表示を行うために使用します。	
`# nessuscli agent link -`	Tenable Agent リンクキーを使用して、エージェ

コマンド	説明
`-key=<key> --host=<host> --port=<port>`	ントを Tenable Nessus Manager または Tenable Vulnerability Management にリンクします。 **必須の引数** • `--key` - マネージャーから取得したリンクキー。 • `--host` - Tenable Nessus Manager にリンクする場合: Tenable Nessus Manager のインストール中に設定した静的 IP アドレスまたはホスト名。 Tenable Vulnerability Management にリンクする場合: `sensor.cloud.tenable.com` (Tenable Agents 8.0.x 以前、`cloud.tenable.com` の場合) **注意:** Tenable Agent 8.1.0 以降では、Tenable Vulnerability Management にリンクされたエージェントは `sensor.cloud.tenable.com` を使用して Tenable Vulnerability Management と通信します。エージェントが `sensor.cloud.tenable.com` に接続できない場合は、代わりに `cloud.tenable.com` を使用します。それより前のバージョンのエージェントは、`cloud.tenable.com` ドメインを使用し続けます。 • `--port` - Tenable Nessus Managerにリンクするには、8834 またはカスタムポートを使用します。 Tenable Vulnerability Management にリンクするには、443 を使用します。

コマンド	説明
	Tenable Vulnerability Management の引数 • `--cloud` - Tenable Vulnerability Management にリンクするには、引数 `--cloud` を渡します。 `--cloud` 引数は、`--host=sensor.cloud.tenable.com --port=443` を指定するためのショートカットです。`--cloud` を使用する場合は、`--host` および `--port` を設定する必要はありません。 **警告:** `--cloud` 引数は、FedRAMP 環境ではサポートされていません。`--host=fedcloud.tenable.com --port=443` を指定する必要があります。 **注意:** 中国本土にある Tenable Nessus スキャナー、Tenable Agents、Tenable Web App Scanning スキャナー、または Tenable Network Monitor (NNM) を介して Tenable Vulnerability Management に接続している場合は、sensor.cloud.tenable.com ではなく sensor.cloud.tenablecloud.cn で接続する必要があります。 **オプションの引数** • `--auto-proxy` – (Windows のみ) 設定した場合、エージェントはプロキシを設定するために、Web Proxy Auto Discovery (WPAD) を使用して Proxy Auto Config (PAC) ファイルを取得します。この設定は、他のすべてのプロキシ設定に優先します。

コマンド	説明
	• `--name` - エージェントの名前。エージェントの名前を指定しない場合、名前はエージェントをインストールしているコンピューターの名前にデフォルトで設定されます。 • `--groups` - エージェントを追加する 1 つ以上の既存のエージェントグループ。インストールプロセス中にエージェントグループを指定しない場合、Tenable Nessus Manager または Tenable Vulnerability Management で、リンクされたエージェントを後からエージェントグループに追加できます。コンマ区切りリストで複数のグループをリストにします。グループ名にスペースが含まれる場合は、リスト全体を引用符で囲みます。例: `"Atlanta,Global Headquarters"` **注意:** エージェントグループ名は、大文字と小文字を区別し、正確に一致する必要があります。エージェントグループ名は引用符で囲む必要があります (例: `--groups="My Group"`)。 • `--ca-path` - マネージャーのサーバー証明書の検証に使用するカスタム CA 証明書。 • `--offline-install` – 有効にすると、オフラインの状態でも Tenable Agent がシステムにインストールされます。Tenable Agent は定期的にマネージャーへのリンクを試みます。 エージェントがコントローラーに接続できない場合、1 時間ごとに再試行します。コン

コマンド	説明
	トローラーには接続できるがリンクに失敗する場合は、24 時間ごとに再試行します。 **ヒント:** `config.json` でリンク設定を指定し、再試行設定を空白のままにすると、`--install-offline` リンク引数を使用した場合と同じ結果になります。 • `--network` - Tenable Vulnerability Management にリンクされたエージェントの場合、エージェントをカスタムネットワークに追加します。ネットワークを指定しない場合、エージェントはデフォルトのネットワークに属することになります。 • `--profile-uuid` - エージェントを割り当てるエージェントプロファイルの UUID (例: `12345678-9abc-4ef0-9234-56789abcdef0`)。詳細については、「*Tenable Vulnerability Management ユーザーガイド*」のエージェントプロファイルを参照してください。 • `--proxy-host` - プロキシサーバーのホスト名または IP アドレス。 • `--proxy-port` - プロキシサーバーのポート番号。 • `--proxy-password` - ユーザー名として指定したユーザーアカウントのパスワード。 • `--proxy-username` - プロキシサーバーへのアクセスと使用が許可されているユーザーアカウント名。 • `--proxy-agent` - プロキシに事前定義さ

コマンド	説明
	れたユーザーエージェントが必要とされる場合のユーザーエージェント名。
`# nessuscli agent relink --host=<new_host> --port=<new_port>`	リンクされたエージェントを Tenable Vulnerability Management から Tenable Sensor Proxy に、またはその逆に再リンクします。 **注意:** このコマンドは、Tenable Nessus Manager に接続されたエージェントには対応していません。
`# nessuscli agent unlink`	エージェントを Tenable Nessus Manager または Tenable Vulnerability Management からリンク解除します。 **オプションの引数** • `--force` – エージェントがマネージャーと通信できない場合でも、エージェントを Tenable Nessus Manager または Tenable Vulnerability Managementから強制的にリンク解除します。Tenable では、Tenable Nessus Manager または Tenable Vulnerability Management と通信できないエージェントのリンクを解除するため、このフラグを使用することを推奨しています。 `--force` フラグを使用する場合は、Tenable Nessus Manager または Tenable Vulnerability Management でエージェントのリンクを解除する必要が生じる場合もあります。
`# nessuscli scan-triggers --list`	エージェントのルールベーススキャンについての詳細をリストします。

コマンド	説明
	• スキャン名 • ステータス (**uploaded** (アップロード済み) など) • 最後にアクティビティがあった時間 (ステータスの隣に表示されます) • スキャンの説明 • 最新のポリシー変更の時間 • 最終実行時間 • スキャントリガー • スキャン設定テンプレート • スキャンを開始するためのコマンド (`nessuscli scan-triggers --start --UUID=<scan-uuid>`)
`# nessuscli scan-triggers --start --UUID=<scan-uuid>`	(Tenable Vulnerability Management にリンクされたエージェントのみ) UUID に基づくルールベーススキャンを手動で実行します。
`# nessuscli agent status`	エージェントのステータス、ルールベーススキャンの情報、保留中のジョブ、およびエージェントがサーバーにリンクしているかどうかを表示します。 コマンド出力には、次の情報の一部が表示されます。 • Running (実行中) – エージェントが現在ホスト上でアクティブであるかどうかを示します。 • Linked to (リンク先) – エージェントがリンクされているマネージャーを示します。

コマンド	説明
	• Link status (リンクステータス) – エージェントのマネージャーとの現在のリンクステータスを示します。 • Proxy (プロキシ) – エージェントが接続しているプロキシを示します (該当する場合)。 • Plugin set (プラグインセット) – エージェントの現在のプラグインセットを示します。 • Scanning (スキャン中) – エージェントが現在ホストをスキャンしているかどうかを示します。この値は、保留中のスキャンジョブの数と、エージェントに対して設定されたスキャントリガーの数も示します (この値は、出力では **smart scan configs** (スマートスキャン設定) とラベル付けされます)。 • Scans run today (今日実行されたスキャン) – エージェントが今日実行したスキャンの数を示します。 • Last scanned (最終スキャン日) – エージェントが最後にスキャンを実行した日時を示します。 • Last connect (最終接続日) – エージェントがマネージャーに最後に接続した日時を示します。 • Last connection attempt (最終接続試行日) – エージェントがマネージャーに最後に接続を試行した日時を示します。 **オプションの引数** • `--local` – (デフォルトの動作) ステータス、現在のジョブ数、保留中のジョブを示

コマンド	説明
	します。このオプションは、エージェントがステータスを取得するためにその管理ソフトウェアに接続しないようにします。代わりに、最後の同期時に取得した最新情報が表示されます。 • `--remote` – マネージャーからジョブ数が取得され、ステータスが表示されます。 **注意:** Tenable では、`--remote` オプションによる頻繁なステータスチェックの実行を推奨していません (自動化の利用時など)。 • `--offline` – Tenable Nessus Manager または Tenable Vulnerability Management に接続できない場合、最後にキャッシュされたエージェントステータスを表示します。 • `--show-token` – 管理ツールにより特定および認証に利用された、エージェントのトークンを表示します。 • `--show-uuid` – エージェントの Tenable UUID を表示します。
`# nessuscli plugins --info`	エージェントのフルおよびインベントリプラグインセットの詳細をリストします。 • インストールされているバージョン • 最後にダウンロードされた日時 • 最後に必要とされた日時 • 有効期限 – プラグインセットが期限切れとなる日時 (つまり、プラグインセットが不要になるタイミング)。

コマンド	説明
	• プラグイン – プラグインセット内のプラグインの総数。 • 非圧縮時のソースサイズ エージェントのプラグインに関する、以下の詳細および統計情報を一覧表示します。 • 最後にプラグインが更新された日時 • 最後にプラグインの更新を確認した日時 • 圧縮後のプラグインソースの合計サイズ • コンパイル後のプラグインの合計サイズ • プラグイン属性データの合計 • ディスク上のプラグインの合計サイズ
`# nessuscli plugins --reset`	すべてのプラグインとプラグインに関連するデータをディスクから削除します。エージェントは、削除が完了した直後にプラグインをダウンロードできます。 **注意:** このコマンドは、エージェントのディスクにプラグインデータがある場合にのみトリガーされます。
`# nessuscli profile --show`	該当する場合、エージェントに割り当てられている Tenable Vulnerability Management エージェントプロファイルに関する情報を取得します。
`# nessuscli install-relay --linking-key=<Tenable Identity Exposure relay linking key>`	エージェントに Tenable Identity Exposure セキュアリレーをインストールします。 Tenable Identity Exposure リレーリンクキーを取得するには、*Tenable Identity Exposure 管理者ガイド*のセキュアリレーを参照してください。

コマンド	説明
	install-relay は、以下の任意のパラメーターをサポートしています。 • proxy_address – プロキシが Tenable ドメインに到達する必要がある場合に使用するプロキシ IP または DNS。proxy_address を入力すると、proxy_port も入力する必要があります。 • proxy_address – プロキシが Tenable ドメインに到達する必要がある場合に使用するプロキシポート。proxy_port を入力すると、proxy_address も入力する必要があります。 • proxy_basic_login – プロキシログインのユーザー名。proxy_basic_login を入力すると、proxy-basic-password も入力する必要があります。 • proxy-basic-password – プロキシのログインパスワード。proxy_basic_login を入力すると、proxy_basic_login も入力する必要があります。 プロキシを指定しない場合は、プロキシパラメーターを一切入力しないでください。認証されていないプロキシを指定するには、proxy_address と proxy_port を入力します。認証されているプロキシを指定するには、proxy_address、proxy_port、proxy_basic_login、および proxy-basic-password を入力します。
アップデートコマンド	
# nessuscli agent update --file=<plugins_set.tgz>	プラグインセットを手動でインストールします。

コマンド	説明
修正コマンド	
`# nessuscli fix --list`	エージェントの設定とその値のリストを表示します。
`nessuscli fix --set <setting>=<value>`	エージェント設定を特定の値にセットします。 エージェント設定の一覧は、詳細設定を参照してください。
`# nessuscli fix --set update_ hostname="<value>"`	Tenable Vulnerability Management または Tenable Nessus Manager のエージェントホスト名を自動的に更新します。 update_hostname パラメーターは、yes または no に設定できます。デフォルトでは、この環境設定は無効になっています。 **注意:** 変更を Tenable Nessus Manager で有効にするためにエージェントサービスを再起動します。
`# nessuscli fix --set agent_update_ channel=<value>`	(Tenable Vulnerability Management にリンクされたエージェントのみ) エージェント更新プランを設定して、エージェントが自動的に更新するバージョンを指定します。 値: • **ga** - 一般公開 (GA) され次第、自動的に最新の Agent バージョンへと更新されます。**注意:** この日付は通常、バージョンが一般公開された日から *1 週間後* です。重大なセキュリティ問題に対処するためのバージョンの場合は、Tenable から直ちに公開される場合があります。 • **ea** - 早期アクセス (EA) 用にリリースされ

コマンド	説明
	次第、自動的に最新の Agent バージョンへとアップデートします。通常、一般公開よりも数週間早いタイミングです。 • **stable** - 自動的に最新の Tenable Agent バージョンに更新しません。Tenable が設定した、Tenable Agent の古いバージョンを維持します。これは通常、最新の一般公開バージョンよりも 1 リリース前のものとなりますが、7.7.0 よりも前のバージョンにはなりません。Tenable Agent が新しいバージョンがリリースすると、エージェントはソフトウェアバージョンをアップデートしますが、最新のリリースよりも前のバージョンに留まります。 **注意:** Tenable Vulnerability Management にリンクされているエージェントの場合は、エージェントの `nessuscli` ユーティリティから `agent_update_channel` コマンドを実行する必要があります。Tenable Nessus Manager にリンクされているエージェントの場合は、Tenable Nessus Manager の `nessuscli` ユーティリティから `agent_update_channel` コマンドを実行する必要があります。
`# nessuscli fix --set maximum_scans_per_day=<value>`	(Tenable Vulnerability Management にリンクされたエージェントのみ) エージェントが 1 日につき実行できる最大スキャン数を設定します。最小数量は **1**、最大数量は **48** で、デフォルト数量は **10** となります。
`# nessuscli fix --set max_retries="<value>"`	`agent link`、`agent status`、または `agent unlink` コマンドの実行中に不具合が生じた場合、エージェントが再試行する最大回数が設定されます。コマンドは、試行間隔を `retry_`

コマンド	説明
	sleep_milliseconds に設定することで休止時間を徐々に増やしながら、指定回数にわたり、連続して再試行されます。max_retries のデフォルト値は 0 です。最小値は 0 で、最大値は 10 です。 たとえば、max_retries を 4 に、retry_sleep_milliseconds を 1500 (デフォルト) に設定した場合は、エージェントが 1 回目の試行後に 1.5 秒間、2 回目の試行後に 3 秒間、3 回目の試行後に 4.5 秒間休止します。 **注意:** この設定はオフラインの更新やリンク後 24 時間経過してから通常実行されるエージェントのチェックインには影響しません。
`# nessuscli fix --set retry_sleep_milliseconds="<value>"`	agent link、agent status、または agent unlink コマンドの実行中に不具合が生じた場合、エージェントの再試行間隔がミリ秒単位で設定されます。デフォルトは 1500 ミリ秒 (1.5 秒) です。
`# nessuscli fix --set niap_mode=enforcing`	Tenable Agent に NIAP モードを適用します。NIAP モードの詳細については、NIAP に準拠する Tenable Agent の設定を参照してください。
`# nessuscli fix --set niap_mode=non-enforcing`	Tenable Agent の NIAP モードを無効にします。NIAP モードの詳細については、NIAP に準拠する Tenable Agent の設定を参照してください。
`# nessuscli fix --set fips_mode=enforcing`	Tenable Agent 通信およびデータベース暗号化に対して最新の検証済み FIPS モジュールを適用します。FIPS モジュールはスキャン暗号化に影響しません。 **注意:** NIAP モードを適用すると、Tenable Agent

コマンド	説明
	はFIPSモジュールも適用します。詳細については、NIAPに準拠するTenable Agentの設定を参照してください。
`# nessuscli fix --set fips_mode=non-enforcing`	Tenable Agent通信およびデータベース暗号化に対してFIPSモジュールを無効にします。 **注意:** NIAPモードを無効にすると、Tenable AgentはFIPSモジュールも無効にします。詳細については、NIAPに準拠するTenable Agentの設定を参照してください。
セキュア設定の修正	
`nessuscli fix`	`--list`、`--set`、 `--get`、`--delete`コマンドを使用して、詳細なエージェント設定を変更したり表示したりすることができます。 `--secure`オプションを選択すると、登録関連情報が含まれる暗号化の環境設定に影響が及びます。 **警告:** ドキュメントにない`--secure`設定の変更はTenableでサポートされない設定となるため推奨していません。 エージェント設定の一覧は、詳細設定を参照してください。
`nessuscli fix [--secure] --list`	
`nessuscli fix [--secure] --set <setting=value>`	
`nessuscli fix [--secure] --get <setting>`	
`nessuscli fix [--secure] --delete <setting>`	
`# nessuscli fix --secure --get agent_linking_key`	(Tenable Nessus Managerバージョン10.4.0以降のみ) 一意のエージェントリンクキーを取得します。 **注意:** このリンクキーは、エージェントをリンクする目的でのみ使用できます。スキャナーまたは子ノードとのリンクには使用できません。

コマンド	説明
リソース管理コマンド	

`# nessuscli fix --set process_priority="<value>"`
 	
`# nessuscli fix --get process_priority`
 	
`# nessuscli fix --delete process_priority`
	コマンド
	
	process_priority 設定をセット、取得、または削除します。
	
	process_priority 設定を使用することで、システム上で実行中の他のタスクの優先度に対する Tenable Agent の相対的な優先度を制御できます。
	
	有効な値、および本設定の動作方法に関する詳細については、エージェント CPU リソースコントロールを参照してください。

Tenable Nessus サービス

Nessus サービスを起動または停止する必要がある場合は、できるだけオペレーティングシステムのインターフェースから Nessus サービスコントロールを使用してください。

ただし、コマンドラインインターフェースを通じて実行可能な **nessus-service** 機能も多数あります。

nessusd コマンドは **nessus-service** サーバーコマンドと互換的に使用できます (特記される場合を除きます)。

 # killall nessusd コマンドは、Nessus のすべてのサービスと実行中のスキャンを停止するために使用されます。

注意: どのコマンドも管理者権限を持つユーザーが実行する必要があります。

Nessus のサービス構文

オペレーティングシステム	コマンド
Linux	# /opt/nessus_agent/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-

オペレーティングシステム	コマンド
	number>] [-a <address>] [-S <ip[,ip,...]>]
macOS	# /Library/NessusAgent/run/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]

コマンド出力データを抑制する例

コマンド出力は **-q** オプションを使用して抑制できます。

Linux

```
# /opt/nessus_agent/sbin/nessus-service -q -D
```

Nessusd のコマンド

オプション	説明
-c <config-file>	このコマンドは、nessusd サーバーを起動するとき、サーバー側で使用される nessusd 設定ファイルを指定するために使用されます。標準 db の代わりに代替設定ファイルの使用が可能です。
-S <ip [,ip2,...]>	nessusd サーバーを開始するとき、スキャン中に Nessus が確立する <ip> 接続のソース IP を強制します。このオプションは、デフォルトの IP アドレスの代わりに複数のパブリック IP アドレスを使用するマルチホーム型マシンを所有する場合にのみ有用です。この設定が機能するには、nessusd を実行するホストにこれらの IP アドレスセットを備える複数の NIC が必要です。
-D	このオプションでは、開始時に nessusd サーバーが強制的にバックグラウンドで実行されます (daemon モード)。
-v	バージョン番号を表示して終了します。
-l	サードパーティ製ソフトウェアのライセンスリストが表示されます。
-h	コマンドの要約を表示し、終了します。
--ipv4-only	IPv4 ソケットでのみリッスンします。

オプション	説明
--ipv6-only	IPv6 ソケットでのみリッスンします。
-q	「quiet」モードで作動し、すべてのメッセージを stdout に抑制します。
-R	プラグインの再処理を強制します。
-t	開始時に各プラグインのタイムスタンプをチェックして、新たに更新されるプラグインのみをコンパイルします。
-K	スキャナー用のマスターパスワードを設定します。 マスターパスワードが設定されている場合、Nessus ではポリシーに含まれるすべてのポリシーと認証情報が暗号化されます。パスワードが設定されている場合、Nessus UI からパスワードの入力を促されます。 マスターパスワードを設定後に紛失した場合、管理者も Tenable サポートも復元できません。

注意事項

nessusd をゲートウェイで実行していて、nessusd に外部者が接続しないようにする場合は、`listen_address` 詳細設定を行います。

この設定を行うには、次を実行します。

```
nessuscli fix --set listen_address=<IP address>
```

この設定により、アドレス *<address>* (マシン名でなく IP アドレス) での接続のみをリッスンするようにサーバーに指示します。

プラグインのアップデート

次の表は、Tenable Vulnerability Management または Tenable Nessus Manager にリンクされているエージェントの差分プラグインアップデートの動作を示しています。

注意: Tenable Agent は、リンクされたマネージャーのプラグイン更新を 24 時間ごとにチェックします。

リンクされたマネー	差分更新	フルアップデート

ジャー		
Tenable Vulnerability Management	エージェントプラグインセットのいずれかとTenable Vulnerability Managementプラグインセットの差が15日以内である場合、エージェントは差分アップデートを実行します。	エージェントにそのプラグインセットのプラグインがない場合、エージェントはスキャン時に必要なプラグインセットのプラグインのフルアップデートを実行します。このため、エージェント脆弱性スキャンまたはインベントリコレクションスキャンを初めて実行する場合、スキャンがその後の脆弱性スキャンやインベントリスキャンよりも多くの帯域幅を使用することを予期してください。 また、エージェントプラグインセットのいずれかとTenable Vulnerability Managementプラグインセットの差が15日より長い場合、エージェントはフルプラグインアップデートを実行します。 エージェントは、設定可能な時間が経過すると、未使用のプラグインセットを削除します(詳細については、days_to_keep_unused_pluginsの詳細設定を参照してください)。時間の経過後、エージェントは未使用のプラグインセットを削除します。
Tenable Nessus Manager	エージェントプラグインセットとTenable Nessus Managerプラグインセットの差が5日以内である場合、エージェントは差分プラグインアップデートを実行します。	エージェントプラグインセットとTenable Nessus Managerプラグインセットの差が5日より長い場合、エージェントはフルプラグインアップデートを実行します。

セーフモード

注意: Tenable Vulnerability ManagementおよびTenable Nessus Managerでセーフモードをサポートするユーザーインターフェースがリリースされ次第、エージェントのセーフモードに関する詳細なドキュメントが公開される予定です。

セーフモードは、エージェントにプラグインコンパイル、スキャン、ホストメモリ、環境の問題が発生したとき、モニタリングと修正ができるようにTenable AgentがTenable Vulnerability ManagementやTenable Nessus Managerとの接続状態を維持できる機能です。

エージェントがセーフモードに入ると、Tenable Vulnerability ManagementまたはTenable Nessus Managerとの通信を維持しますが、プラグインコンパイルやスキャンはブロックされます。これにより、お客様の組織はエージェントを安全にリモートでモニタリング、トラブルシューティング、復元することができます。セーフモードにより、問題発生時に個々のエージェントを手動で管理する必要がなくなるため、大規模なエージェントデプロイメントでは特に役立ちます。

セーフモードのアクティベーション

エージェントは次のいずれかのエラーを検出すると、自動的にセーフモードに入ります。

- スキャン中にエージェントがクラッシュする
- プラグインコンパイル中またはプラグインセットの変更に反応して、エージェントがクラッシュまたはハングする
- プラグインアップデートの失敗により、エージェントが使用できなくなる
- バグにより、エージェントが使用できなくなる
- ホストメモリの問題により、エージェントが繰り返し終了する
- ウイルス対策またはエンドポイントセキュリティソフトウェアにより、エージェントが繰り返し終了する

エージェントはセーフモードをアクティブ化したことをマネージャーに通知し、Tenable Vulnerability ManagementまたはTenable Nessus Managerのエージェントユーザーインターフェースを通してユーザーに通知します。エージェントはマネージャーとの接続を維持するので、モニタリングされ、ユーザーからのプラグインコマンドを受け入れますが、スケジュールされたプラグインタスクやスキャンはブロックされます。

セーフモードでエージェントを修正および復元する

セーフモードのエージェントを修正および復元するには、connect.tenable.comでセーフモードに入ったエージェントを報告してTenableサポートのサポートを受けるか、**[Linked Agents]**(リンクされたエージェント)メニューを使用して自己修正できます。

> **注意:** Tenableでは、1つまたは複数のエージェントがセーフモードに移行した場合、サポートチケットを送信することを強く推奨します。以下の修正アクションのいずれかを試行する前にサポートチケットを送信し、セーフモードに入ったいずれかのエージェントのデバッグファイルを必ず含めてください。そうすることで、Tenableサポートは問題

の根本原因を特定し、修正を計画することができます。デバッグファイルがないと、問題の根本原因は不明なままとなり、対処できません。

警告: Tenable のサポートを受けずに自己修正を行う場合、Tenable は、大規模なグループまたはすべてのエージェントで自己修正を試す前に、エージェントのごく一部だけで試すことを強く推奨します。

セーフモードのエージェントへの対応については、*Tenable Vulnerability Management* および *Tenable Nessus* ユーザーガイドの**エージェント セーフモード**のトピックを参照してください。