ソフトウェアエージェントのアップグレード

ソフトウェアエージェントのアップグレードプロセス中は、次のようになります。

- すべてのプロセスが終了し、新しいバージョンに置き換えられます。
- アップグレード中は、フローはキャプチャされません。
- エージェントがポリシーを適用していた場合、そのポリシーはワークロードに適用されたままになります。

新しいバージョンのエージェントが起動すると、次のようになります。

- 許可/拒否されたフローのキャプチャが再開されます。
- エージェントがコレクタ（CLC）に接続されるまで、フローはディスクに保存されます。これは、[フローのディスククォータ（Flow Disk Quota）] 設定がオフになっていない限り適用されます。

適用プロセスがエンドポイントファイアウォール適用（EFE）に再接続される前に、最後に受信され、適用されたポリシーが Cisco Secure Workload のファイアウォールにそのまま保持されることが確認されます。

- UI からのエージェントのアップグレード （2 ページ）
- Kubernetes/Openshift エージェントの動作のアップグレード （6 ページ）
- Deep Visibility または Enforcement Linux Agent のアンインストール （6 ページ）
- Deep Visibility または Enforcement Windows Agent のアンインストール （8 ページ）
- Deep Visibility エージェントまたは Enforcement AIX エージェントのアンインストール （9 ページ）
- Universal Linux Agent のアンインストール （10 ページ）
- Universal Windows Agent のアンインストール （10 ページ）
- 適用 Kubernetes または OpenShift エージェントのアンインストール （11 ページ）
- Deep Visibility Solaris Agent のアンインストール （11 ページ）
- リホームの有効化 （12 ページ）
- リホームするエージェントの選択 （14 ページ）

• リホームの無効化 （14 ページ）

UI からのエージェントのアップグレード

エージェントは、「ソフトウェアエージェントの設定」で説明されているエージェント設定インテントワークフローを使用してアップグレードできます。エージェント設定プロファイルの設定時に、有効または無効にできる [自動アップグレード（Auto Upgrade）] オプションがあります。オプションが有効になっている場合、インベントリフィルタ条件に一致するエージェントは、利用可能な最新バージョンに自動的にアップグレードされます。

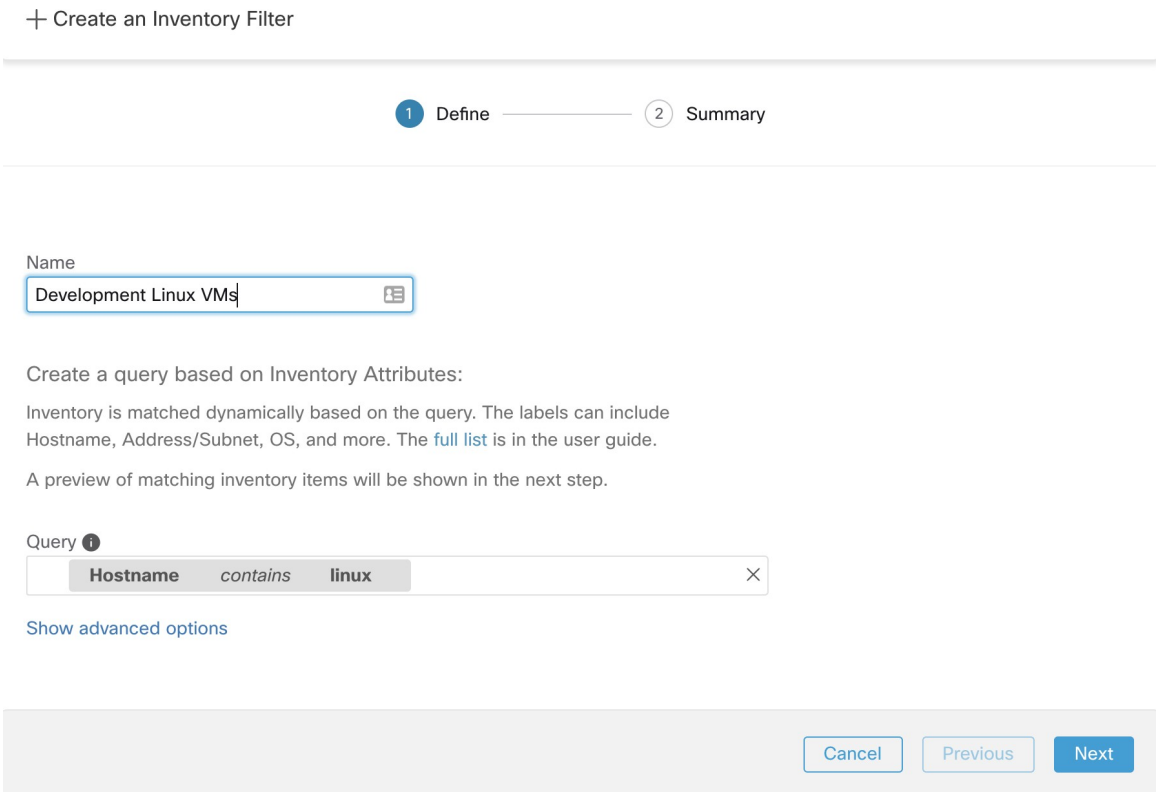
[ソフトウェアエージェント（Software Agents）] > [エージェントリスト（Agent List）]ページで、古いバージョンのソフトウェアエージェントが強調表示され、[SWバージョン（SW Version）] 列の下に警告記号が表示されます。これらのエージェントをクラスタで利用可能な最新バージョンにアップグレードすることが重要です。

ソフトウェアエージェント設定インテントワークフローを使用してソフトウェアエージェントのアップグレードを設定するには、次の手順を実行します。

手順

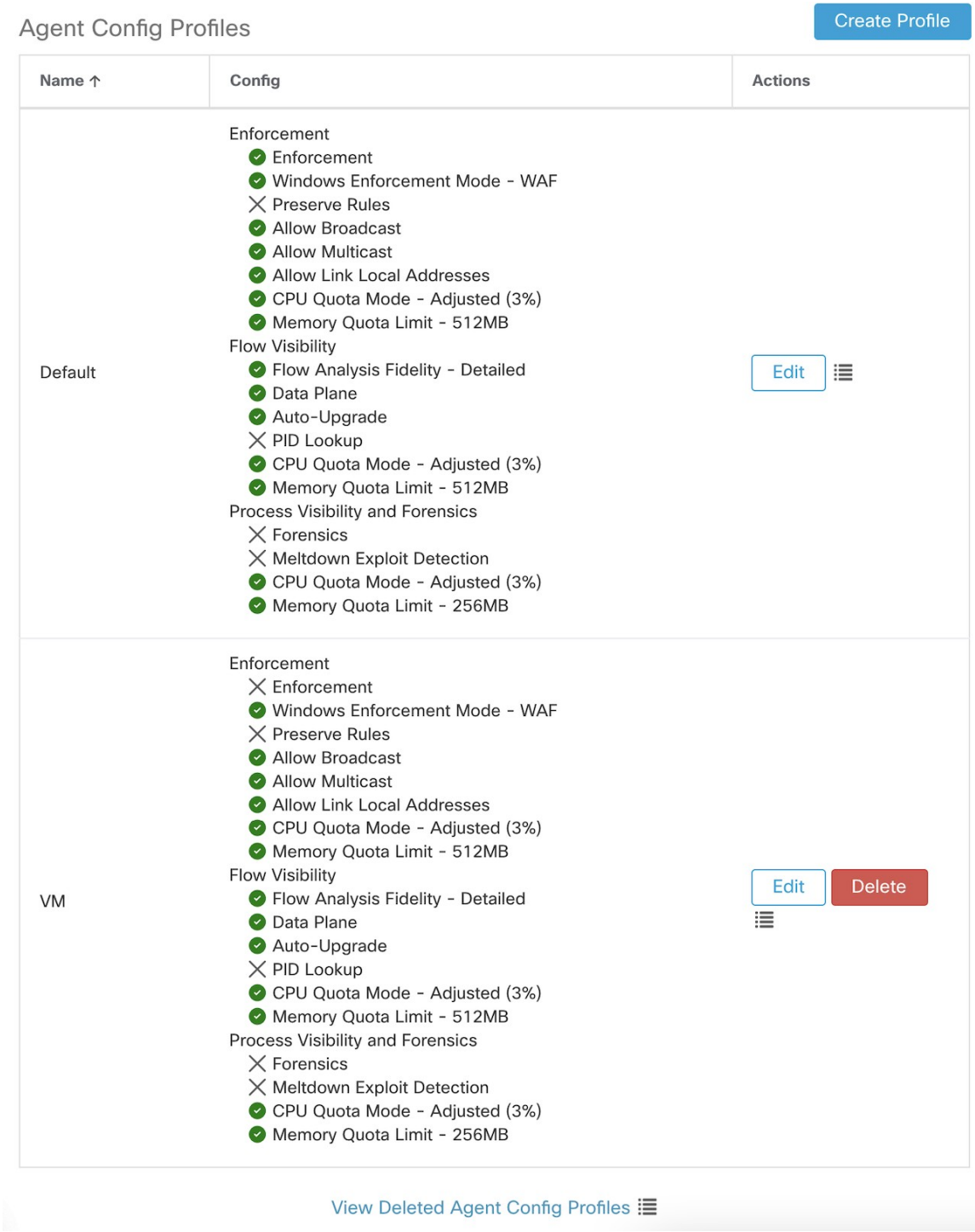
ステップ 1 [インベントリフィルタ（Inventory Filters）] ページでインベントリフィルタを作成します。詳細については、「フィルタ」を参照してください。

図 *1*:インベントリフィルタ



ステップ 2 インベントリフィルタによって選択されたエージェント用のエージェント設定プロファイルを作成します。必要に応じて、[自動アップグレード（Auto Upgrade）]オプションを有効にして、選択したエージェントを自動的にアップグレードできます。

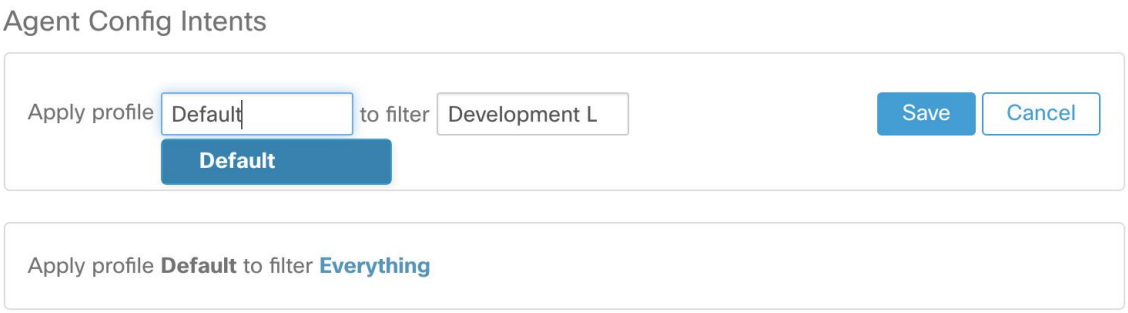
図 *2:* エージェント設定



ステップ 3 インベントリフィルタを使用して選択されたエージェントに設定プロファイルを適用するためのエージェント設定インテントを作成します。自動アップグレードオプションが有効になっている場合、選択したエージェントは自動的にアップグレードされます。

通常、エージェントプロファイルがエージェントに適用された後、エージェントがアップグレードされるまでに最大 30 分かかります。

図 *3:* エージェント設定インテント



（注）
デフォルトのエージェントプロファイルの自動アップグレード設定は、ERSPANに適用されます。他のすべてのコネクタエージェントは、パッチリリースを含むクラスタのアップグレードがあるたびに自動にアップグレードされます。

エージェントの手動アップグレード

次のセクションでは、センサー設定インテントワークフローを使用せずに、エージェントを手動でアップグレードする方法について説明します。

手順

ステップ 1 左側のナビゲーションウィンドウで、**[管理（Manage）] > [ワークロード（Workloads）] > [エージェント（Agents）]** の順にクリックします。

ステップ 2 [アップグレード（Upgrade）] タブをクリックします。
詳細可視性エージェントと適用エージェントが表示され、エージェントごとに、アップグレード可能な新しいバージョンのみが一覧表示されます。デフォルトでは、最新バージョンが選択されています。

ステップ 3 特定のエージェントをフィルタ処理するには、フィルタボックスに検索クエリを入力します。たとえば、「Platform = CentOS-7.6」と入力します。

ステップ 4 選択したバージョンにアップグレードするエージェントを選択し、[アップグレード（Upgrade）] をクリックします。

（注）
通常の状況では、エージェントに自動的にアップグレードさせることが強く推奨されます。これがサポートされている唯一のアップグレード方法です。最新バージョンを手動でダウンロー

ドし、ワークロードで実行されているエージェントに直接展開することによってアップグレードを制御する場合は、必ず、安全上の注意事項に従ってください。

Kubernetes/Openshift エージェントの動作のアップグレード

daemonset インストーラスクリプトを使用して Kubernetes/Openshift ノードにインストールされたエージェントは、セルフアップグレードが可能です。アップグレードプロセスは、自動アップグレードオプションによって、または Kubernetes/Openshift クラスタ内の任意のノードに対してアップグレードを手動でトリガーすることによって制御されます。この環境でのアップグレードのメカニズムでは、daemonset 仕様で Docker イメージをアップグレードします。つまり、次の段落で説明するように、1 つのエージェントのアップグレードが、daemonset によってカバーされるすべてのエージェントに影響します。

Daemonset Pod 仕様が変更されると、Kubernetes/Openshift はグレースフルシャットダウンをトリガーし、新しい Docker イメージを取得して、Kubernetes/Openshift クラスタ内のすべてのノードで Secure Workload エージェントポッドを開始します。これにより、アップグレードを許可するポリシーがクラスタ内のノードのサブセットにのみ適用される場合でも、エージェントは他のノードでアップグレードされます。

すべてのノードで自動アップグレードが無効になっている場合は、新しいインストーラスクリプトをダウンロードしてインストールを再実行することにより、手動アップグレードが可能です。インストールスクリプトは、新しいインストールと既存のインストールのアップグレードの場合を自動検出し、インストール済みであることを検出すると、daemonset ポッドを手動でアップグレードするように機能します。

Deep Visibility または Enforcement Linux Agent のアンインストール

RPM ベースのインストール：

1. **rpm -e tet-sensor** コマンドを実行します。

エージェントのアンインストールイベントがクラスタに通知され、[ソフトウェアエージェント（Software Agent）] ページでエージェントがアンインストール済みとしてマークされます。

[ソフトウェアエージェント（Software Agent）] ページの UI からエージェントを手動で削除します。また、ユーザーは、エージェント設定プロファイルから [クリーンアップ期間（cleanup period）] をオンにして、エージェントの自動クリーンアップまたは削除を有効にすることもできます。

（注） デフォルトでは、[クリーンアップ期間（cleanup period）] はオフになっています。

Ubuntu.deb ベースのインストール：

Ubuntu エージェントの新規インストールでは、ネイティブの .deb 形式が使用されるようになりました。

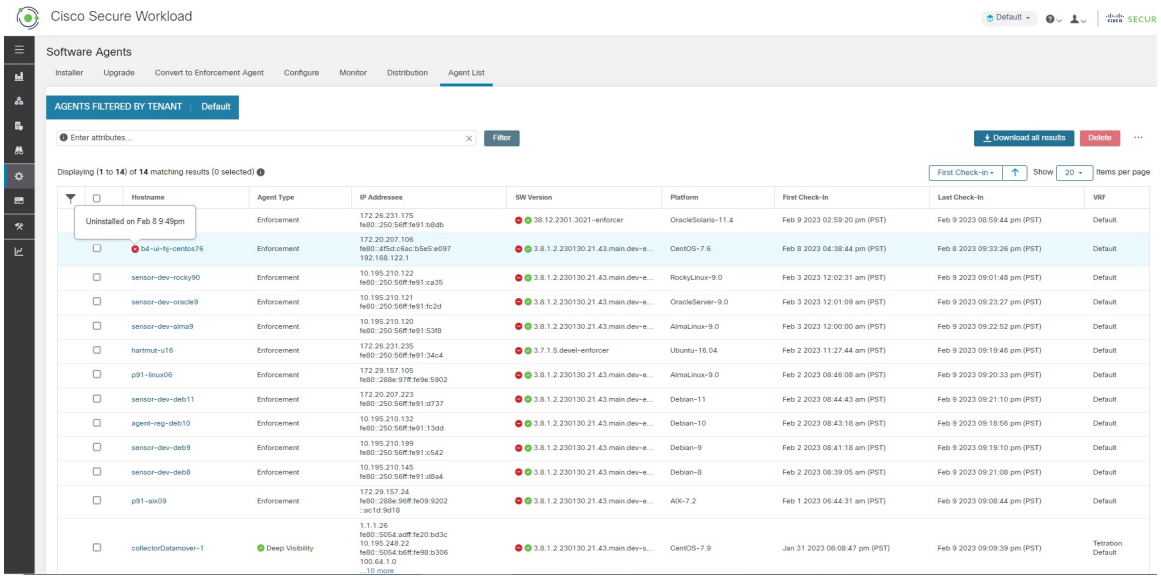
1. **dpkg –purge tet-sensor** コマンドを実行します。

エージェントのアンインストールイベントがクラスタに通知され、[ソフトウェアエージェント（Software Agent）] ページでエージェントがアンインストール済みとしてマークされます。

[ソフトウェアエージェント（Software Agent）] ページからエージェントを手動で削除します。また、ユーザーは、エージェント設定プロファイルから [クリーンアップ期間（cleanup period）] をオンにして、エージェントの自動クリーンアップまたは削除を有効にすることもできます。

（注）
- デフォルトでは、[クリーンアップ期間（cleanup period）] はオフになっています。
- エージェントの操作中に、一部のカーネルモジュールがカーネルによって自動的にロードされる可能性があります。たとえば、Linux で適用が有効になっている場合、Netfilter モジュールがロードされる可能性があります。エージェントには、カーネルによってロードされたモジュールのリストがありません。したがって、エージェントのアンインストール中に、カーネルモジュールをアンロードできない可能性があります。
- 適用エージェントがシステムファイアウォールにポリシーを適用した場合、エージェントをアンインストールすると、適用されたポリシーがクリアされ、システムファイアウォールが開きます。

図 *4:* エージェントのアンインストールアラート



Deep Visibility または Enforcement Windows Agent のアンインストール

Secure Workload エージェントをアンインストールするには、次の 2 つのオプションがあります。

手順

ステップ 1 **[コントロールパネル（Control Panel）] > [プログラム（Programs）] > [プログラムと機能（Programs and Features）]**に移動し、**Cisco Secure Workload Agent** をアンインストールします。

ステップ 2 または、ショートカット **Uninstall.lnk** を実行します。

```
C:\Program Files\Cisco Tetration
```

ステップ 3 適用エージェントがシステムファイアウォールにポリシーを適用する場合、エージェントをアンインストールすると、適用されたポリシーがクリアされ、システムファイアウォールが開きます。

エージェントをアンインストールすると、クラスタ情報が更新されます。エージェントのステータスが [ソフトウェアエージェント（Software Agent）] ページで更新され、エージェントがアンインストール済みとしてマークされます。

[ソフトウェアエージェント（Software Agent）]ページからエージェントを手動で削除します。また、ユーザーはエージェント設定プロファイルで[クリーンアップ期間（cleanup period）]をオンにして、エージェントの自動クリーンアップまたは削除を有効にすることもできます。

（注）
デフォルトでは、[クリーンアップ期間（cleanup period）] はオフのままになります。

（注）
- エージェントのインストール中にNpcapをインストールした場合、エージェントのアンインストール中に Npcap もアンインストールされます。
- デフォルトでは、ログファイル、設定ファイル、および証明書はアンインストール中に削除されません。それらを削除したい場合は、同じフォルダでショートカット**UninstallAll.lnk**を実行します。

Deep Visibility エージェントまたは Enforcement AIX エージェントのアンインストール

手順

ソフトウェアエージェントをアンインストールするには、次のコマンドを実行します。

```
installp -u tet-sensor
```

ソフトウェアエージェントがアンインストールされて UI で使用できなくなると、この情報がクラスタに送信され、エージェントは [ソフトウェアエージェント（Software Agent）] ページで [アンインストール済み（Uninstalled）] とマークされます。

UI からエージェントを削除するには、次の 2 つの方法があります。

- [ソフトウェアエージェント（Software Agent）]ページから不要になったエージェントを直接削除します。さらに、次のコマンドを実行して、Tetrationエージェントのインストールディレクトリ `/opt/cisco/tetration` を削除できます。

  ```
  rm -rf /opt/cisco/tetration
  ```

- [エージェント構成プロファイル（Agent Configuration Profiles）] ページで**クリーンアップ期間**を構成して、自動クリーンアップを有効にします。

（注）
- デフォルトで、[クリーンアップ期間（cleanup period）] はオフに設定されています。

- System Resource Controller は、優れた可視性エージェントを tet-sensor として制御します。起動、停止、再起動、削除が可能です。このサービスは、inittab を tet-sen-engine として使用して永続化されます。
- System Resource Controller は、適用エージェントを tet-enforcer として制御します。起動、停止、再起動、削除が可能です。このサービスは、inittab を tet-enf-engine として使用して永続化されます。
- エージェント運用中、カーネルはいくつかのカーネルモジュールを自動的にロードする場合があります。たとえば、AIX で適用が有効になっている場合、ipfilter モジュールがロードされます。エージェントには、カーネルによってロードされるモジュールのリストはありません。エージェントのアンインストール中に、カーネルモジュールをアンロードできません。
- 適用エージェントがシステムファイアウォールにポリシーを適用した場合、エージェントをアンインストールすると、適用されたポリシーがクリアされ、システムファイアウォールが開きます。

Universal Linux Agent のアンインストール

手順

ステップ 1 アンインストールスクリプト **‘/usr/local/tet-light/uninstall.sh‘** を実行します。
ステップ 2 [ソフトウェアエージェント（Software Agent）] ページからエージェントを削除します。

Universal Windows Agent のアンインストール

手順

ステップ 1 アンインストールスクリプト **‘C:\Program Files\Cisco Tetration\Lightweight Sensor\uninstall.cmd‘** を実行します。
ステップ 2 [ソフトウェアエージェント（Software Agent）] ページからエージェントを削除します。

適用 Kubernetes または OpenShift エージェントのアンインストール

手順

ステップ 1 元のインストーラスクリプトを見つけるか、Secure Workload UI から新しいスクリプトをダウンロードします。

ステップ 2 アンインストールオプション **install.sh –uninstall** を実行します。インストール時と同じ考慮事項が適用されます。

- Linux x86_64 アーキテクチャでのみサポートされます。
- ~/.kube/config に含まれている管理者ユーザーログイン情報を使用するか、または–kubeconfig オプションを使用して kubectl 管理者ログイン情報ファイルを指定します。

ステップ 3 [ソフトウェアエージェント（Software Agent）] ページからすべての Kubernetes ノードのエージェントを削除します。

Deep Visibility Solaris Agent のアンインストール

手順

ステップ 1 ソフトウェアエージェントをアンインストールするには、次のコマンドを実行します。

- Solaris 11.4 の場合：`pkg uninstall tet-sensor`
- Solaris 10 の場合：`pkgrm -a /opt/cisco/secure-workload/noask.admin -n tet-sensor`

ステップ 2 [ソフトウェアエージェント（Software Agent）] ページからエージェントを削除します。

リホームの有効化

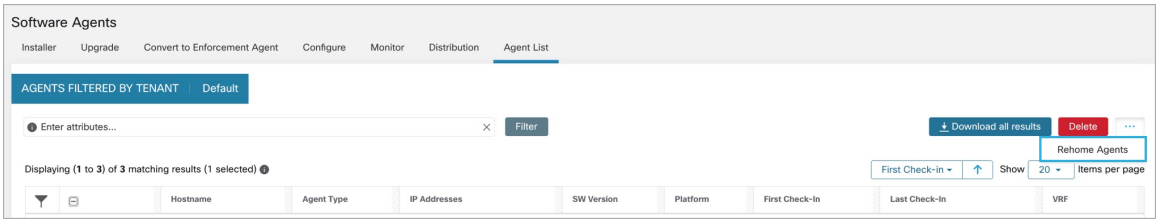
手順

ステップ 1 左側のナビゲーションメニューで、[管理（Manage）] > [ワークロード（Workloads）] > [エージェント（Agents）] をクリックします。

ステップ 2 [エージェントリスト（Agent List）] タブをクリックします。

ステップ 3 メニューアイコンをクリックし、[エージェントのリホーム（Rehome Agents）] を選択します。

図 *5*: エージェントのリホーム（*Rehome Agents*）

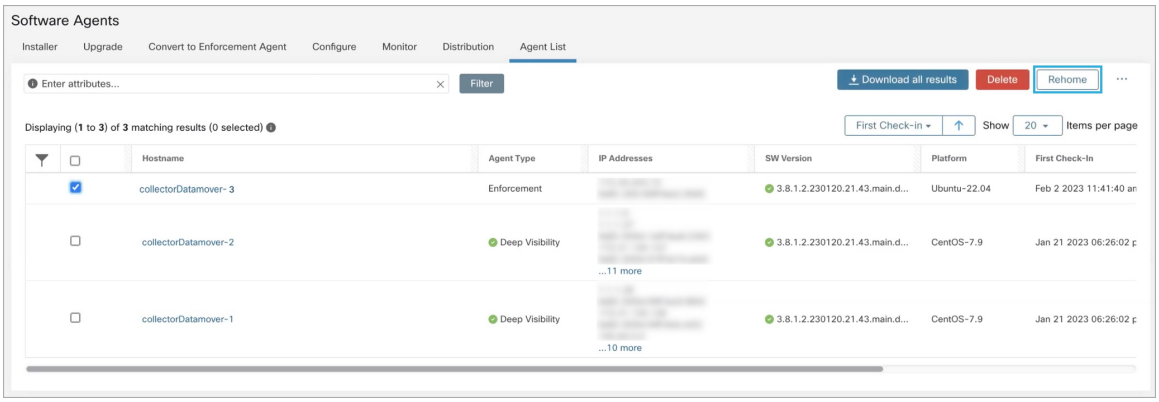


ステップ 4 [エージェントのリホーム（Agent Rehoming）] ウィンドウで、次の詳細を入力します。

フィールド	説明
宛先範囲のアクティベーションキー（Destination Scope Activation Key）	1. [管理（Manage）] > [ワークロード（Workloads）] > [エージェント（Agents）] に移動します。 2. [インストーラ（Installer）] タブをクリックします。 3. [従来のパッケージインストーラを使用した手動インストール（Manual install using classic packaged installers）] を選択します。 4. [次へ（Next）] をクリックします。 5. [エージェントのアクティベーションキー（Agent Activation Key）] をクリックします。 6. [キー（Key）] の値をコピーし、[宛先範囲のアクティベーションキー（Destination Scope Activation Key）] フィールドに貼り付けます。

フィールド	説明
宛先センサーVIP（Destination Sensor VIP）	1. [プラットフォーム（Platforms）]>[クラスタ設定（Cluster Configuration）] に移動します。 2. [センサーVIP（Sensor VIP）] をコピーし、[宛先センサーVIP（Destination Sensor VIP）] フィールドに貼り付けます。
HTTPS プロキシ	アウトバウンド通信にプロキシを使用するためにエージェントで必要となる場合は、 プロキシドメインまたはアドレスを入力します。
宛先センサーCA証明書（Destination Sensor CA Cert）	1. [プラットフォーム（Platforms）]>[クラスタ設定（Cluster Configuration）] に移動します。 2. [センサーCA証明書のダウンロード（Download Sensor CA Cert）] をクリックします。

図 *6 :* エージェントのリホームの有効化



ステップ 5 [エージェントのリホームの有効化（Enable Agent Rehomeing）] をクリックします。

設定が保存されます。[リホーム（Rehome）] ボタンが右上に表示されます。

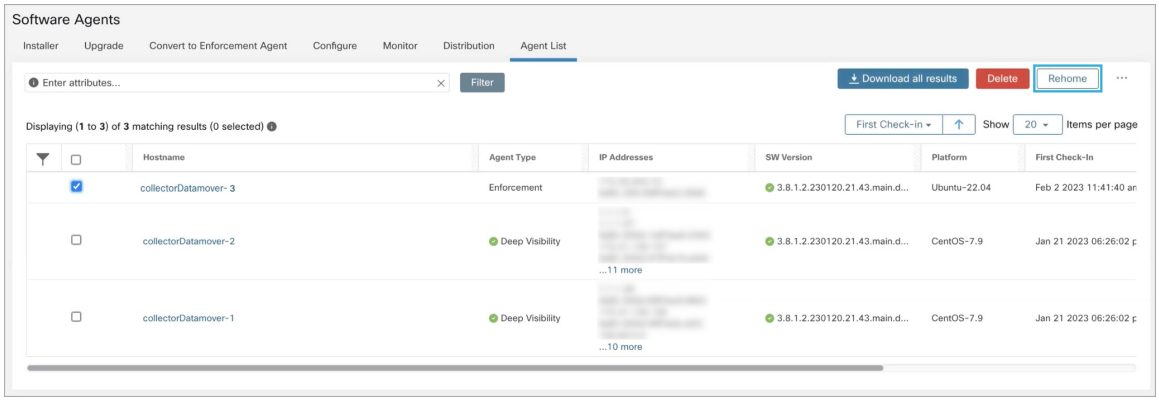
リホームするエージェントの選択

手順

ステップ 1 エージェントを選択します。

ステップ 2 [リホーム（Rehome）] をクリックします。

図 7: リホームするエージェントの選択



ステップ 3 確認のために [はい（Yes）] をクリックします。

リホームの無効化

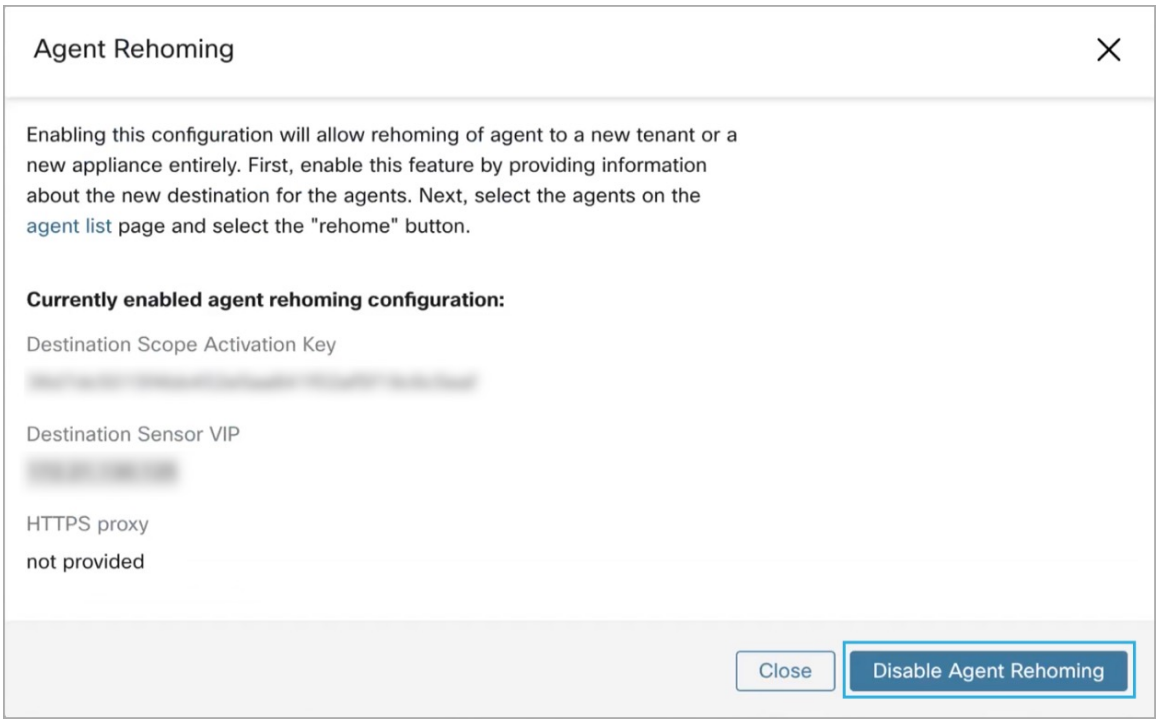
（注） 複数のユーザーが SaaS との間でリホームする場合、サイト管理者は各テナントやアプライアンスを個別に移動する必要があります。移動するには、リホームを無効化して設定をクリアし、新しいユーザーのリホームを有効にします。

手順

ステップ 1 メニューアイコンをクリックし、[エージェントのリホーム（Rehome Agents）] を選択します。

ステップ 2 [エージェントのリホーム（Agent Rehomeing）] ウィンドウで、[エージェントのリホームの無効化（Disable Agent Rehomeing）] をクリックします。

図 *8 :* エージェントのリホームの無効化（***Disable Agent Rehoming***）



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。