Cisco Secure Workload リリース 3.8 クイックスタートガイド

初版：2023 年 4 月 12 日

セグメンテーションの概要

従来、ネットワークセキュリティは、ネットワークのエッジにファイアウォールを配置することで、悪意のあるアクティビティをネットワークに侵入させないようにすることを目的としていました。ただし、ネットワークを侵害した脅威、またはネットワーク内部で発生した脅威から組織を保護する必要もあります。ネットワークのセグメンテーション（またはマイクロセグメンテーション）は、ネットワーク上のワークロードと他のホストとの間のトラフィックを制御できるようにすることでワークロードを保護できます。これにより、組織がビジネス目的で必要とするトラフィックのみを許可し、他のすべてのトラフィックを拒否できます。

たとえば、ポリシーを使用して、一般向けの Web アプリケーションをホストするワークロード間のすべての通信がデータセンターの研究開発データベースと通信するのを防止したり、非生産ワークロードが生産ワークロードに接続するのを防止したりできます。

Cisco Secure Workload は、組織のフローデータを使用して、適用する前に評価および承認できるポリシーを提案します。または、ネットワークをセグメント化するためにこれらのポリシーを手動で作成することもできます。

このマニュアルについて

このドキュメントは、Cisco Secure Workload リリース 3.8 に適用されます。

- セグメンテーション、ワークロードラベル、範囲、階層型範囲ツリー、ポリシー検出など、Cisco Secure Workload の主要な概念を紹介します。
- 初回ユーザー エクスペリエンス ウィザードを使用して、範囲ツリーの最初のブランチを作成するプロセスを説明します。
- 実際のトラフィックフローに基づいて、選択したアプリケーションのポリシーを生成する自動プロセスについて説明します。

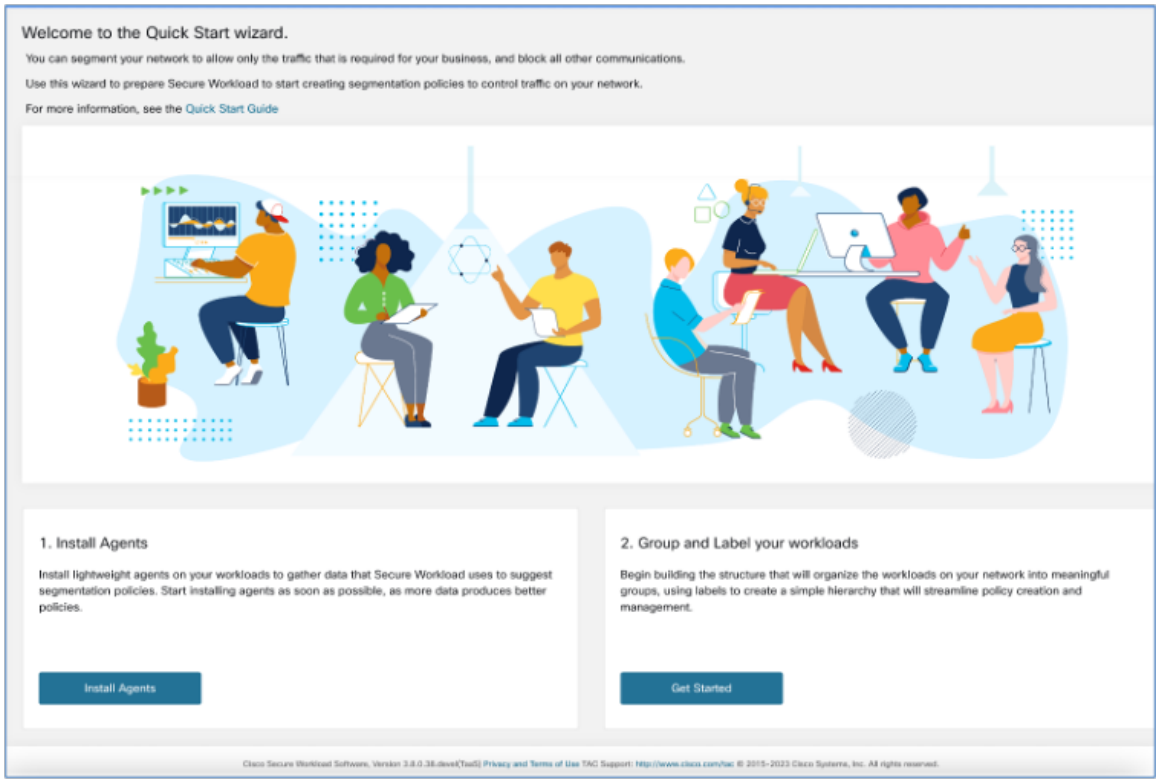
ウィザードのツアー

はじめる前に

次のユーザーロールがこのウィザードにアクセスできます。

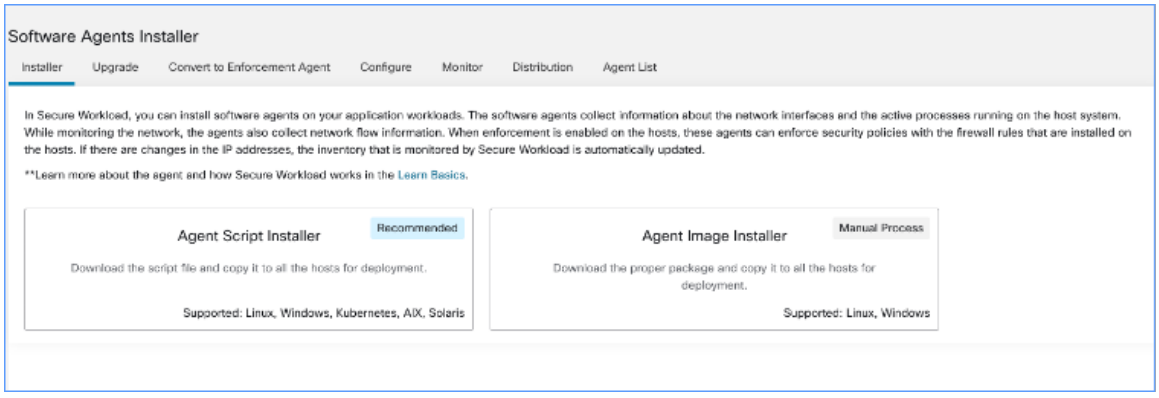
- サイト管理者
- カスタマーサポート
- 範囲所有者

図 *1 : [*ようこそ（*Welcome***）*]* ウィンドウ**



エージェントのインストール

Cisco Secure Workload では、アプリケーションのワークロードにソフトウェアエージェントをインストールできます。ソフトウェアエージェントによって、ネットワークインターフェイスや、ホストシステムで実行されているアクティブなプロセスに関する情報を収集します。



ソフトウェアエージェントをインストールするには、次の 2 つの方法があります。

- エージェント スクリプト インストーラ：ソフトウェアエージェントをインストールしながら、インストール、追跡、および問題のトラブルシューティングを行います。サポートされているプラットフォームは、Linux、Windows、Kubernetes、AIX、および Solaris です。
- エージェントイメージインストーラ：ソフトウェアエージェントのイメージをダウンロードして、プラットフォームに対応する特定のバージョンとタイプのソフトウェアエージェントをインストールします。Linux および Windows プラットフォームがサポートされています。

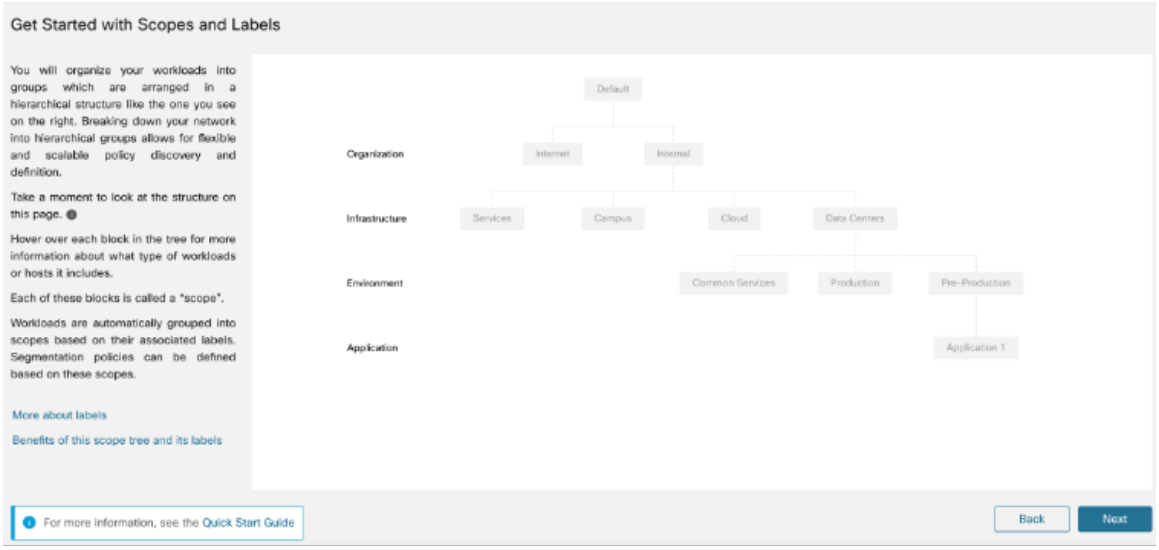
オンボーディングウィザードでは、選択したインストーラ方式に基づいてエージェントをインストールするプロセスを、順を追って説明します。ソフトウェアエージェントのインストールに関する詳細については、UI のインストール手順とユーザーガイドを参照してください。

ワークロードのグループとラベル

ワークロードのグループにラベルを割り当てて、範囲を作成します。

階層型範囲ツリーによって、ワークロードを小さなグループに分割できます。範囲ツリーの最も下にあるブランチは、個々のアプリケーション用に予約されています。

範囲ツリーから親範囲を選択して、新しい範囲を作成します。新しい範囲には、親範囲のメンバーのサブセットが含まれます。



このウィンドウでは、ワークロードを整理してグループに分割し、階層構造で配置します。ネットワークを階層グループに分割すると、柔軟でスケーラブルなポリシーの検出と定義が可能になります。

ラベルは、ワークロードまたはエンドポイントを説明する主要なパラメータであり、キーと値のペアとして表されます。ウィザードは、ワークロードにラベルを適用し、これらのラベルを範囲と呼ばれるグループごとにまとめるのに役立ちます。ワークロードは、関連付けられたラ

ベルに基づいて各範囲に自動的にグループ化されます。この範囲に基づいて、セグメンテーションポリシーを定義できます。

ツリーの各ブロックまたは範囲にカーソルを合わせると、含まれるワークロードまたはホストのタイプに関する詳細情報が表示されます。

（注） [範囲とラベルの利用開始（Get Started with Scopes and Labels）] ウィンドウでは、[組織（Organization）]、[インフラストラクチャ（Infrastructure）]、[環境（Environment）]、[アプリケーション（Application）] がキーであり、各キーの横にある灰色のボックスに表示されたテキストが値です。

たとえば、[アプリケーション1（Application 1）] に属するすべてのワークロードは、次のラベルのセットによって定義されます。

- 組織 = 内部
- インフラストラクチャ = データセンター
- 環境 = 生産前
- アプリケーション = アプリケーション 1

ラベルと範囲ツリーのパワー

ラベルは Cisco Secure Workload のパワーを促進し、ラベルから作成された範囲ツリーは、ネットワークの単なるサマリーではありません。

- ラベルによってポリシーを瞬時に理解できます。

  ```
  "Deny all traffic from Pre-Production to Production"
  ```

  これを、ラベルのない同じポリシーと比較します。

  ```
  "Deny all traffic from 172.16.0.0/12 to 192.168.0.0/16"
  ```

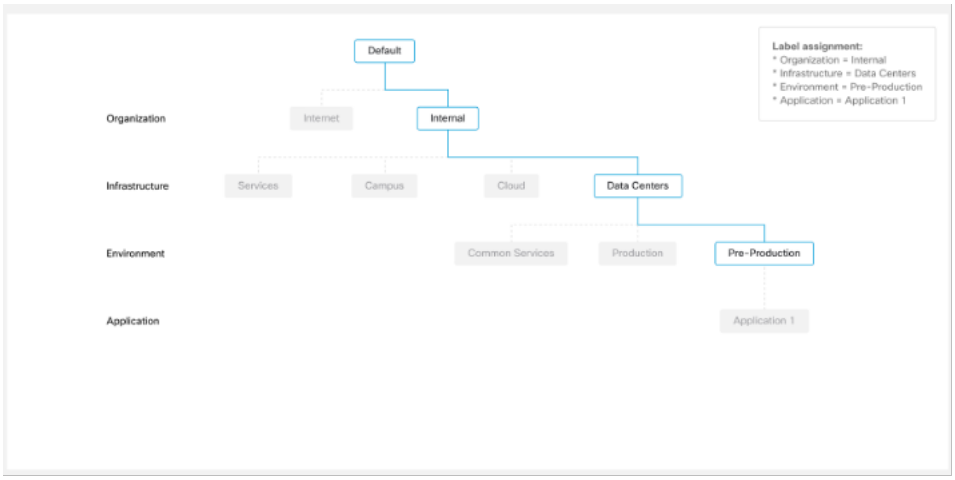
- ラベルに基づくポリシーは、ラベル付きのワークロードがインベントリに追加（または削除）されると、自動的に適用（または適用を停止）します。時間の経過とともに、ラベルに基づいたこれらの動的グループ化により、展開を維持するために必要な労力が大幅に削減されます。
- ワークロードは、ラベルに基づいて範囲にグループ化されます。これらのグループ化により、関連するワークロードにポリシーを容易に適用できます。たとえば、生産前範囲内のすべてのアプリケーションにポリシーを容易に適用できます。
- 単一の範囲で一度作成されたポリシーは、ツリー内の子孫範囲のすべてのワークロードに自動的に適用できるため、管理する必要のあるポリシーの数を最小限に抑えることができます。

  ポリシーを広く（たとえば、組織内のすべてのワークロードに）または狭く（特定のアプリケーションの一部であるワークロードにのみ）、またはその中間の任意のレベル（たとえば、データセンター内のすべてのワークロード）に容易に定義して適用できます。

- 各範囲の責任をさまざまな管理者に割り当て、ネットワークの各部分に最も精通している人々にポリシー管理を委任できます。

組織階層の構築

階層または範囲ツリーの構築を開始します。これには、アセットの特定と分類、範囲の決定、ロールと責任の定義、範囲ツリーのブランチを作成するためのポリシーと手順の作成が含まれます。



ウィザードの指示に従って、範囲ツリーのブランチを作成します。青色で囲まれた各範囲のIPアドレスまたはサブネットを入力すると、範囲ツリーに基づいてラベルが自動的に適用されます。

前提条件：

- 実稼働前環境、データセンター、および内部ネットワークに関連付けられている IP アドレス/サブネットを収集します。
- できるだけ多くのIPアドレス/サブネットを収集してください。IPアドレス/サブネットは後で追加できます。
- 後でツリーを構築するときに、ツリー内の他の範囲（灰色のブロック）に IP アドレス/サブネットを追加できます。

範囲ツリーを作成するには、次の手順を実行します。

内部範囲の定義

内部範囲には、パブリックおよびプライベート IP アドレスを含む、組織の内部ネットワークを定義するすべての IP アドレスが含まれます。

ウィザードは、ツリーブランチの各範囲に IP アドレスを追加する手順を案内します。アドレスを追加すると、ウィザードは各アドレスにその範囲を定義するラベルを割り当てます。

たとえば、この [範囲の設定（Scope Setup）] ウィンドウでは、ウィザードによって

```
Organization=Internal
```

ラベルが各 IP アドレスに割り当てられます。

デフォルトでは、ウィザードは、RFC 1918 で定義されているように、プライベート インターネット アドレス空間の IP アドレスを追加します。

（注） すべての IP アドレスを一度に入力する必要はありませんが、選択したアプリケーションに関連付けられている IP アドレスを含める必要があります。残りの IP アドレスは後で追加できます。

データセンターの範囲の定義

この範囲には、オンプレミスデータセンターを定義する IP アドレスが含まれます。内部ネットワークを定義する IP アドレス/サブネットを入力します。

（注） 範囲名は短く、意味のあるものにする必要があります。

このウィンドウで、組織用として指定した IP アドレスを入力します。これらのアドレスは、内部ネットワークのアドレスのサブセットにする必要があります。複数のデータセンターがある場合は、それらすべてをこの範囲に含めて、単一のポリシーセットを定義できるようにします。

（注） アドレスは、後の段階でいつでも追加できます。たとえば、ウィザードは各 IP アドレスに次のラベルを割り当てます。

```
Organization=Internal
Infrastructure=Data Centers
```

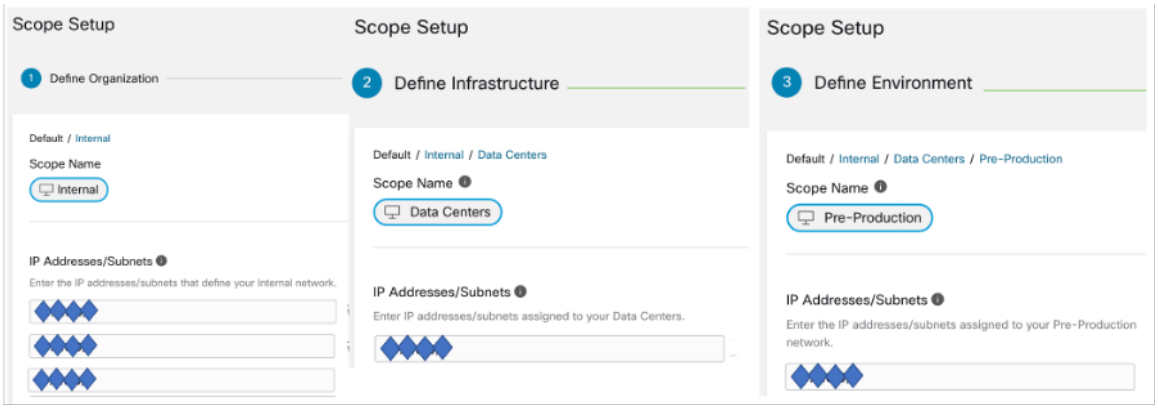
生産前範囲の定義

この範囲には、開発、ラボ、テスト、またはステージングシステムなどの非生産アプリケーションおよびホストの IP アドレスが含まれます。

（注） 実際のビジネスを遂行するために使用するアプリケーションのアドレスは含めないでください。これは、後で定義する生産範囲の一部になります。

このウィンドウで入力する IP アドレスはデータセンター用に入力したアドレスのサブセットとし、これにも選択したアプリケーションのアドレスが含まれている必要があります。理想としては、選択したアプリケーションの一部ではない生産前アドレスも含める必要があります。

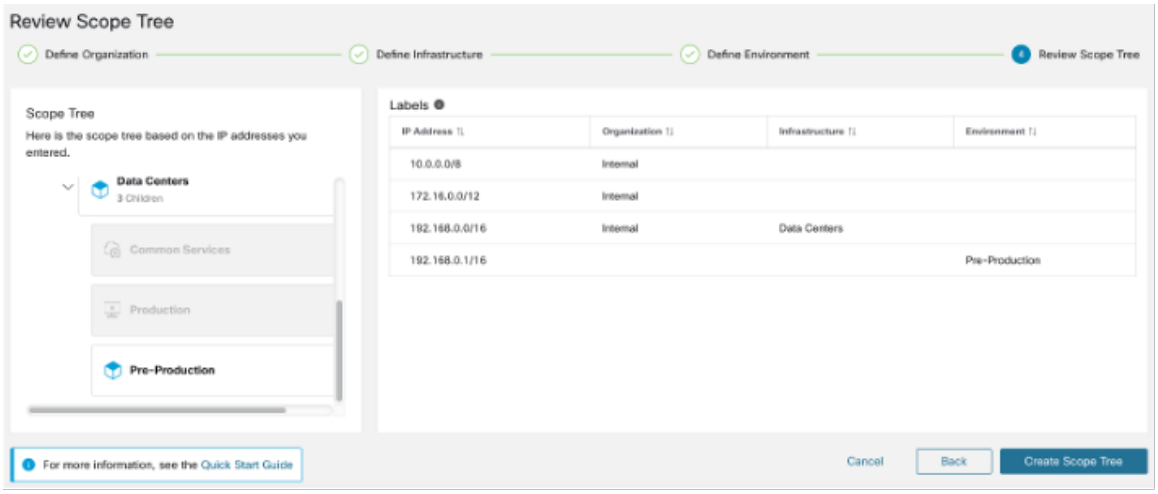
（注） アドレスは、後の段階でいつでも追加できます。



範囲ツリー、範囲、およびラベルの確認

範囲ツリーの作成を開始する前に、左側のウィンドウに表示される階層を確認します。ルート範囲には、設定済みのすべての IP アドレスとサブネットに対して自動的に作成されたラベルが表示されます。プロセスの後の段階で、アプリケーションがこの範囲ツリーに追加されます。

図 *2:*

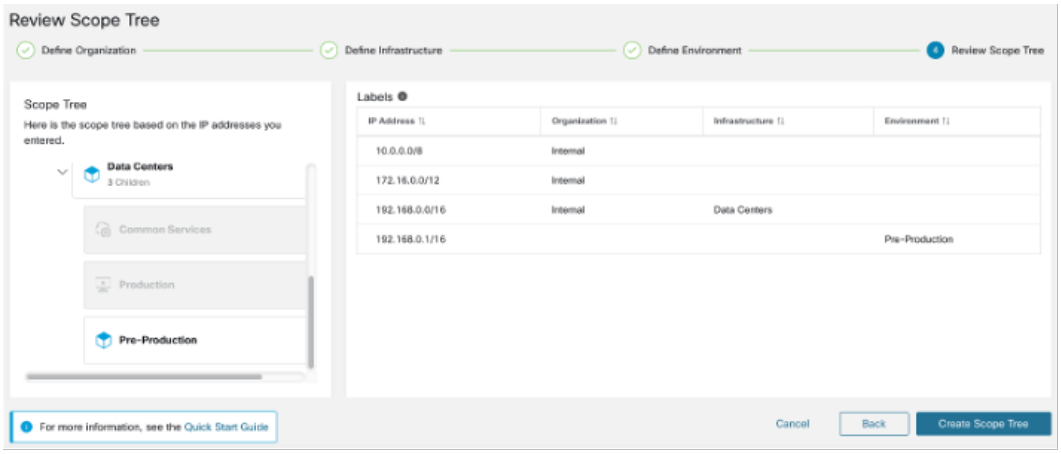


ブランチを展開したり折りたたんだりできるほか、下にスクロールして特定の範囲を選択することもできます。右側のペインには、特定の範囲のワークロードに割り当てられた IP アドレスとラベルが表示されます。このウィンドウでは、この範囲にアプリケーションを追加する前に、範囲ツリーを確認および変更できます。

（注） ウィザードを終了した後にこの情報を表示するには、メインメニューから [整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）] を選択します。

範囲ツリーの確認

範囲ツリーの作成を開始する前に、左側のウィンドウに表示される階層を確認します。ルート範囲には、設定済みのすべての IP アドレスとサブネットに対して自動的に作成されたラベルが表示されます。プロセスの後の段階で、アプリケーションがこの範囲ツリーに追加されます。

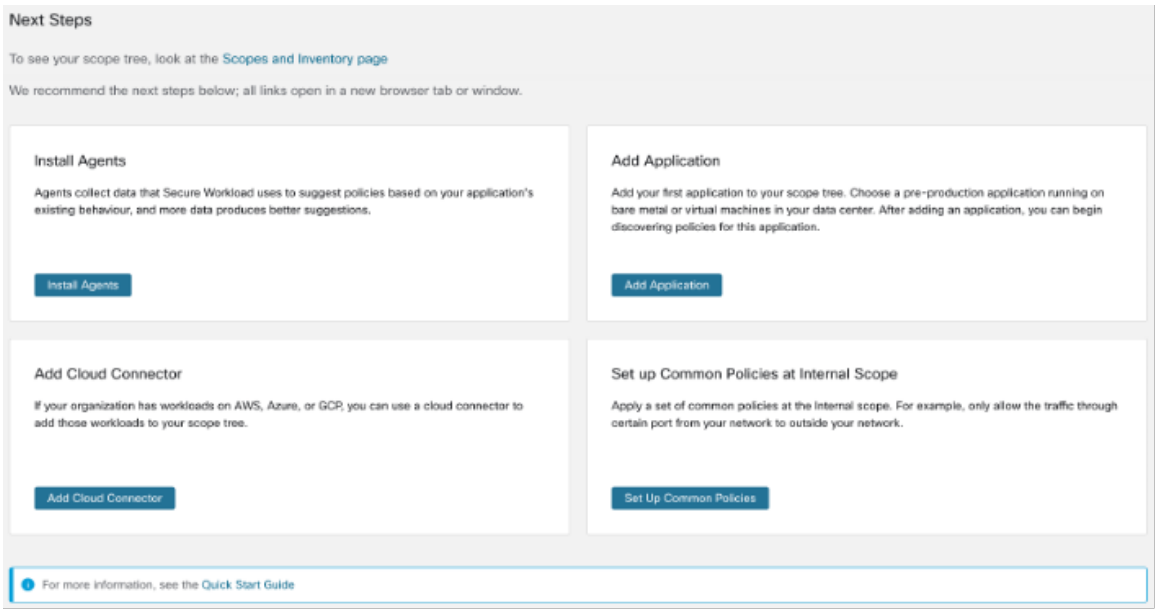


ブランチを展開したり折りたたんだりできるほか、下にスクロールして特定の範囲を選択することもできます。右側のペインには、特定の範囲のワークロードに割り当てられた IP アドレスとラベルが表示されます。このウィンドウでは、この範囲にアプリケーションを追加する前に、範囲ツリーを確認および変更できます。

（注） ウィザードを終了した後にこの情報を表示するには、メインメニューから [整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）] を選択します。

範囲ツリーの作成

範囲ツリーを確認したら、範囲ツリーの作成に進みます。



範囲ツリーの詳細については、ユーザーガイドの「Scopes and Inventory」セクションを参照してください。

次のステップ

エージェントのインストール

選択したアプリケーションに関連付けられたワークロードに、Cisco Secure Workload エージェントをインストールします。エージェントが収集したデータは、ネットワーク上の既存のトラフィックに基づいて推奨されるポリシーを生成するために使用されます。データが多いほど、より正確なポリシーが生成されます。詳細については、『Cisco Secure Workload ユーザーガイド』の「ソフトウェアエージェント」セクションを参照してください。

アプリケーションの追加

最初のアプリケーションを範囲ツリーに追加します。データセンターのベアメタルまたは仮想マシンで実行されている、実稼働前のアプリケーションを選択します。アプリケーションを追加したら、このアプリケーションに対応するポリシーの作成を開始できます。詳細については、『Cisco Secure Workload ユーザーガイド』の「範囲とインベントリ」セクションを参照してください。

内部範囲での共通ポリシーの設定

内部範囲で一連の共通ポリシーを適用します。たとえば、ネットワークからネットワーク外部への特定のポートを通過するトラフィックのみを許可します。

ユーザーは、クラスタ、インベントリフィルタ、および範囲を使用してポリシーを手動で定義することも、自動ポリシー検出を使用してフローデータから検出し、生成することもできます。

エージェントをインストールし、トラフィックフローデータが蓄積されるまで少なくとも数時間待った後、Cisco Secure Workload を有効にしてそのトラフィックに基づいたポリシーを生成（「検出」）できます。詳細については、『Cisco Secure Workload ユーザーガイド』の「ポリシーの自動検出」セクションを参照してください。

これらのポリシーを内部（または内部またはルート）範囲で適用すると、ポリシーを効果的に確認できます。

クラウドコネクタの追加

組織に AWS、Azure、または GCP のワークロードがある場合は、クラウドコネクタを使用してそれらのワークロードを範囲ツリーに追加します。詳細については、『Cisco Secure Workload ユーザーガイド』の「Cloud Connectors」セクションを参照してください。

クイック スタート ワークフロー

手順	操作手順	詳細
1	（オプション）ウィザードの注釈付きツアーに参加する	ウィザードのツアー （1 ページ）
2	セグメンテーションの工程を開始するためのアプリケーションを選択します。	最良の結果を得るには、このウィザードのアプリケーションを選択する （11 ページ） のガイドラインに従ってください。
3	IP アドレスを収集します。	ウィザードは、 4 つのグループの IP アドレスを要求します。 詳細については、IPアドレスの収集 （11 ページ） を参照してください。
4	ウィザードを実行する	要件を表示してウィザードにアクセスするには、ウィザードの実行 （13 ページ）を参照してください。
5	エージェントがフローデータを収集する時間を確保します。	データが多いほど、より正確なポリシーが生成されます。 必要最小限の時間は、アプリケーションがどの程度アクティブに使用されているかによって異なります。
6	実際のフローデータに基づいてポリシーを生成（「検出」）します。	ポリシーの自動生成 （14 ページ）を参照してください。
7	生成されたポリシーを確認します。	生成されたポリシーの確認 （15 ページ） を参照してください。

IPアドレスの収集

以下の各箇条書きの IP アドレスの少なくとも一部が必要です。

- 内部ネットワークを定義するアドレス

  デフォルトでは、ウィザードはプライベートインターネット用に予約されている標準アドレスを使用します。

- データセンター用に予約されているアドレス。

  これには、従業員のコンピューター、クラウドまたはパートナーサービス、集中型IT サービスなどで使用されるアドレスは含まれません。

- 非生産ネットワークを定義するアドレス
- 選択した非生産アプリケーションを構成するワークロードのアドレス

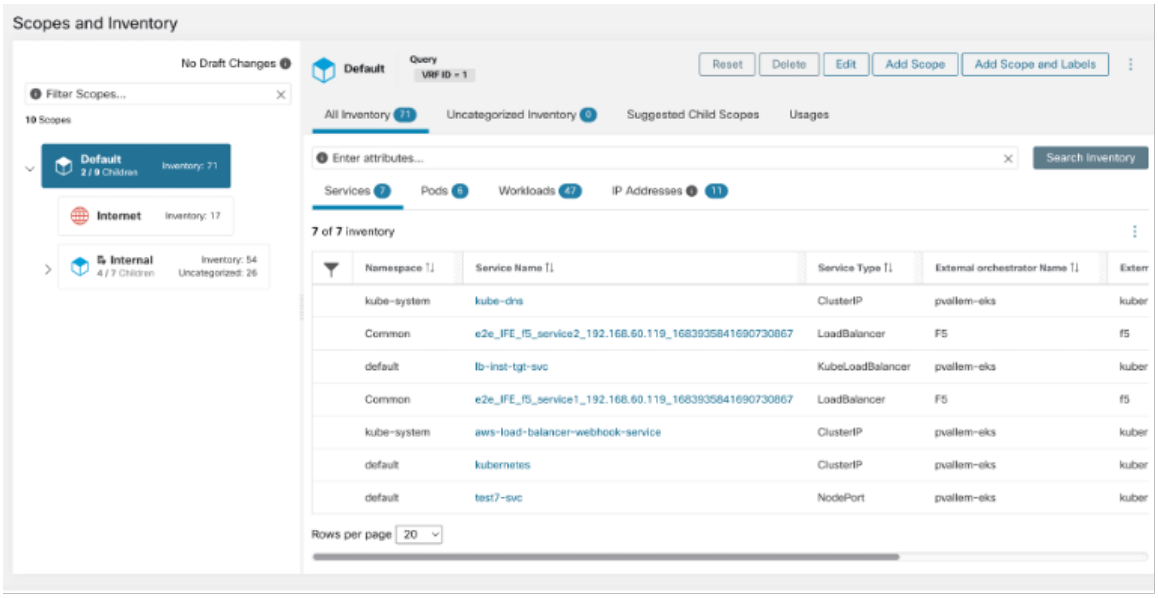
現時点では、上記の各箇条書きのすべてのアドレスを用意する必要はありません。後からいつでもアドレスを追加できます。

重要 4つの箇条書きはそれぞれ、その上の箇条書きのIPアドレスのサブセットを表すため、各箇条書きの各 IP アドレスは、リストの上の箇条書きの IP アドレスにも含まれている必要があります。

このウィザードのアプリケーションを選択する

このウィザードでは、単一のアプリケーションを選択します。

通常、アプリケーションは、Webサービスやデータベース、プライマリサーバーとバックアップサーバーなど、さまざまなサービスを提供する複数のワークロードで構成されます。これらのワークロードが一緒になって、アプリケーションの機能をユーザーに提供します。



アプリケーションを選択するためのガイドライン

Cisco Secure Workload は、クラウドベースのワークロードやコンテナ化されたワークロードなど、広範なプラットフォームとオペレーティングシステムで実行されるワークロードをサポートします。ただし、このウィザードでは、次のようなワークロードを持つアプリケーションを選択してください。

- データセンターで実行中。
- ベアメタルや仮想マシンで実行中。
- Cisco Secure Workload の各エージェントでサポートされている Windows、Linux、または AIX プラットフォーム上で実行中。
  https://www.cisco.com/go/secure-workload/requirements/agents を参照してください。
- 生産前環境に展開済み。

（注） アプリケーションを選択せずにIPアドレスを収集した場合でもウィザードを実行できますが、これらの操作を行わずにウィザードを完了することはできません。

（注） Cisco Secure Workloadアプリケーションからサインアウト（またはタイムアウト）する前にウィザードを完了しなかった場合、または左側のナビゲーションバーを使用してアプリケーションの別の部分に移動した場合、ウィザードの構成は保存されません。

任意の範囲を追加する方法や[範囲とラベル（Scope and Labels）]を追加する方法の詳細については、『Cisco Secure Workload ユーザーガイド』の「範囲とインベントリ」セクションを参照してください。

ウィザードの実行

アプリケーションを選択して IP アドレスを収集したかどうかにかかわらず、ウィザードを実行できますが、これらの操作を行わずにウィザードを完了することはできません。

重要 Cisco Secure Workload からサインアウト（またはタイムアウト）する前にウィザードを完了しなかった場合、または左側のナビゲーションバーを使用してアプリケーションの別の部分に移動した場合、ウィザードの構成は保存されません。

始める前に

次のユーザーロールがこのウィザードにアクセスできます。

- サイト管理者
- カスタマーサポート
- 範囲所有者

手順

ステップ 1 Cisco Secure Workload にサインインします。

ステップ 2 ウィザードを起動します。

現在、範囲が定義されていない場合、Cisco Secure Workload にサインインすると、ウィザードが自動的に表示されます。

または、下記の手順も実行できます。

- 任意のページの上部にある青いバナーにある[今すぐウィザードを実行する（Run the wizard now）]リンクをクリックします。
- ウィンドウの左側にあるメインメニューから[概要（Overview）]を選択します。

範囲を既に作成している場合は、既存の範囲をすべて削除しない限り、ウィザードに再度アクセスすることはできません。これを行うには、（オプション）範囲ツリーをリセットする（15 ページ）を参照してください。

ステップ 3 ウィザードが、知るべき情報を説明します。

次の役立つ要素を見逃さないでください。

- ウィザードのグラフィック要素にカーソルを合わせると、その説明が表示されます。

- リンクと情報ボタン（）をクリックすると、重要な情報が表示されます。

ポリシーの自動生成

Cisco Secure Workload は、ワークロードと他のホスト間の既存のトラフィックに基づいて、ポリシーを生成（「検出」）します（ポリシー検出機能は、以前は「ADM」と呼ばれていたため、その名前を見聞きする場合があります）。準備ができたら、これらのポリシーを変更、補足、分析し、最終的に承認して適用することができます。

（注） ポリシーは、指示があるまで適用されません。

始める前に

- アプリケーションのワークロードにエージェントをインストールする
- エージェントのインストール後、フローデータが蓄積されるまでしばらく待機します。

手順

ステップ 1 クイックスタートウィザードの [次の手順（Next Steps）] ページで、[ポリシーの自動生成（Automatically Generate Policies）] をクリックします。

または、いつでも次の操作を実行できます。

a) Cisco Secure Workload ウィンドウの左側から [防御（Defend）] > [セグメンテーション（Segmentation）] を選択します。
b) 左側のペインの範囲ツリーまたは範囲のリストで、アプリケーションの範囲まで下にスクロールします。
c) その範囲で [プライマリ（Primary）] をクリックします

（ウィザードによって、アプリケーションのプライマリワークスペースが作成されます）。

ステップ 2 [ポリシーの管理（Manage Policy）] をクリックします。

ステップ 3 [ポリシーを自動的に検出（Automatically Discover Policies）] をクリックします。

ステップ 4 含めるフローデータの時間範囲を選択します。

一般に、データが多いほど、より正確なポリシーが生成されます。

ステップ 5 [ポリシーの検出（Discover Policies）] をクリックします。

生成されたポリシーは、このページに表示されます。

次のタスク

生成されたポリシーの確認 （15 ページ）。

生成されたポリシーの確認

検出されたポリシーを調べます（ページから移動した場合は、「ポリシーの表示」セクションの手順に従ってそのページに戻ることができます）。

ポリシーは理にかなっていますか？ラベルは、各ワークロードが通信しているホストのタイプを理解するために役立ちます。

何か不審な点がありますか？不審なワークロードまたは通信の詳細を判断できるかどうかを確認してください。

このアプリケーションに精通している同僚に、提案されたポリシーの評価を依頼できます。

フローデータが蓄積されるにつれ、トラフィックに対処するポリシーを生成する必要が生じるたびに、構成された時間範囲を拡張し、ポリシーを再検出する必要があります。

（オプション）範囲ツリーをリセットする

ウィザードを使用して作成した範囲、ラベル、および範囲ツリーを削除し、必要に応じてウィザードを再度実行することができます。

ヒント 作成した範囲の一部のみを削除し、ウィザードを再度実行したくない場合は、ツリー全体をリセットする代わりに、個々の範囲を削除できます。削除する範囲をクリックしてから、[削除（Delete）] をクリックします。

始める前に

ルート範囲の範囲所有者権限が必要です。

追加のワークスペース、ポリシー、またはその他の依存関係を作成した場合は、範囲ツリーのリセットに関する詳細な情報について、『Cisco Secure Workload ユーザーガイド』を参照してください。

手順

ステップ 1 左側のナビゲーションメニューから、[整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）] を選択します。

ステップ 2 ツリーの上部にある範囲をクリックします。

ステップ 3 [リセット（Reset）] をクリックします。

ステップ 4 選択を確認します。

ステップ 5 [リセット（Reset）] ボタンが [破棄の保留中（Destroy Pending）] に変わった場合は、ブラウザページを更新する必要がある場合があります。

詳細情報

ウィザードの概念の詳細については、『Cisco Secure Workload ユーザーガイド』を参照してください。

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。