Cisco Secure Workload リリース 3.7 クイックスタートガイド

初版：2022 年 8 月 17 日

最終更新：2023 年 2 月 2 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。セグメンテーション（この場合はマイクロセグメンテーションとも呼ばれる）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、ネットワーク上のワークロードを保護するために役立ちます。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、セグメンテーション 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、データセンターの極秘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（多くの場合、コンプライアンスが低く、保護が不十分である）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、組織の実際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するセグメンテーションポリシーを提案します。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

このガイドは、Cisco Secure Workload リリース 3.7 で使用できます。

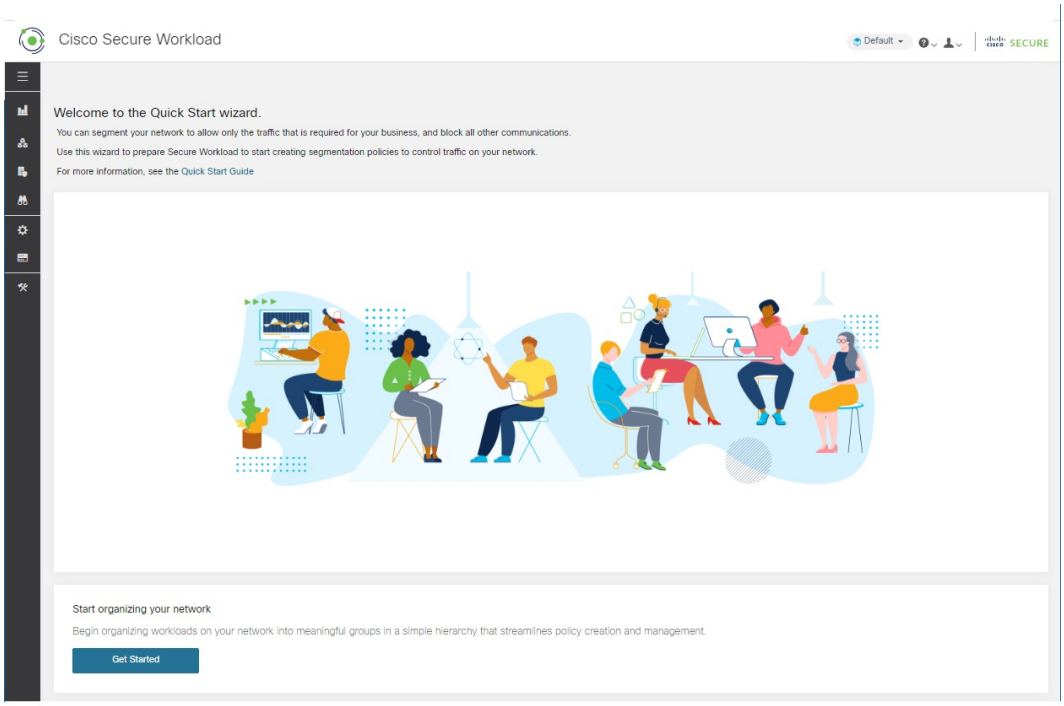
このドキュメント：

- 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。
- 単一のアプリケーションの範囲ツリーの最初のブランチを作成するプロセスを順を追って説明します（Cisco Secure Workload の初回ユーザーエクスペリエンス ウィザードを使用）。そして、
- 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自動的に生成する方法を示します。

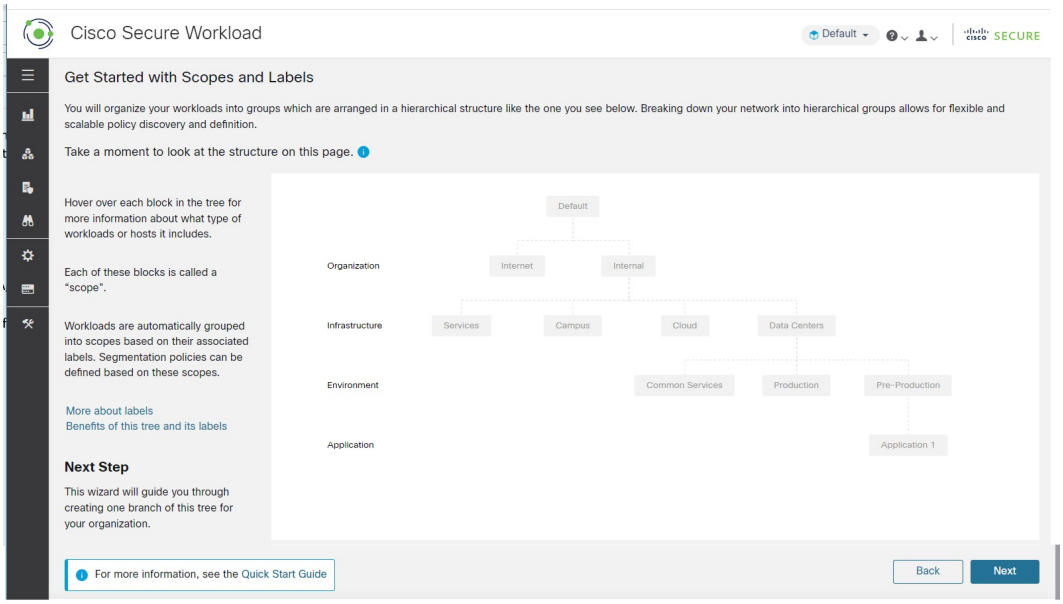
Cisco Secure Workload クイックスタートウィザードには外部ドキュメントは必要ありませんが、新しい製品で作業する前に先読みしたい方々にとって、このオンボーディングガイドはオプションの手引書であり、補足的な情報源です。

ウィザードのツアー

開始ページ



範囲とラベルの利用開始



このページは、構築する必要があるものについて説明しています。ラベルと範囲とは何か、それらがどのように連携するかを示します。

ラベルについて

Cisco Secure Workload のパワーは、ワークロードに割り当てられたラベルに基づきます。

ラベルは、各ワークロードを説明するキーと値のペアです。

上のツリーを見てください。ツリーの左側にラベルキーが表示されます。ラベル値は、各キーに沿ったグレーのボックス内のテキストです。ウィザードは、これらのラベルをワークロードに適用するために役立ちます。

ワークロードにラベルを割り当てると、ワークロードを範囲と呼ばれるグループにグループ化できます。上のツリーの各グレーのボックスが範囲です。

上のツリーでわかるように、アプリケーション1範囲（このツリーの右下）に属するすべてのワークロードは、次の一連のラベル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。

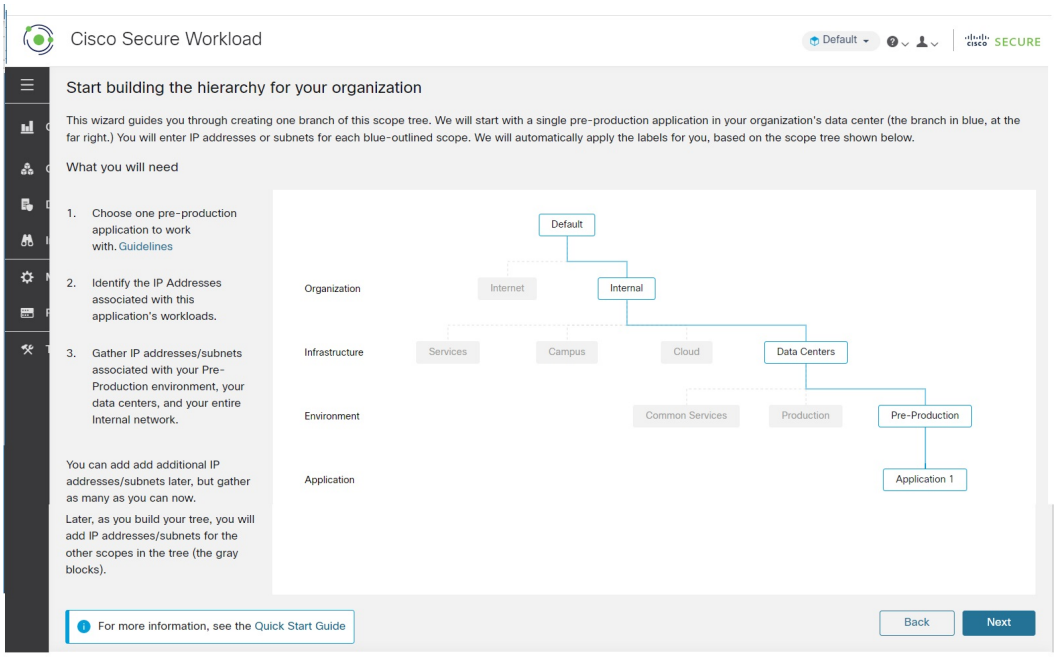
- 単一の範囲で一度作成されたポリシーは、ツリー内の子孫範囲のすべてのワークロードに自動的に適用できるため、管理する必要のあるポリシーの数を最小限に抑えることができます。

  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。

組織階層の構築の開始

これで、何をなぜ構築しているのかを理解したので、独自の範囲ツリーの構築を開始できます。

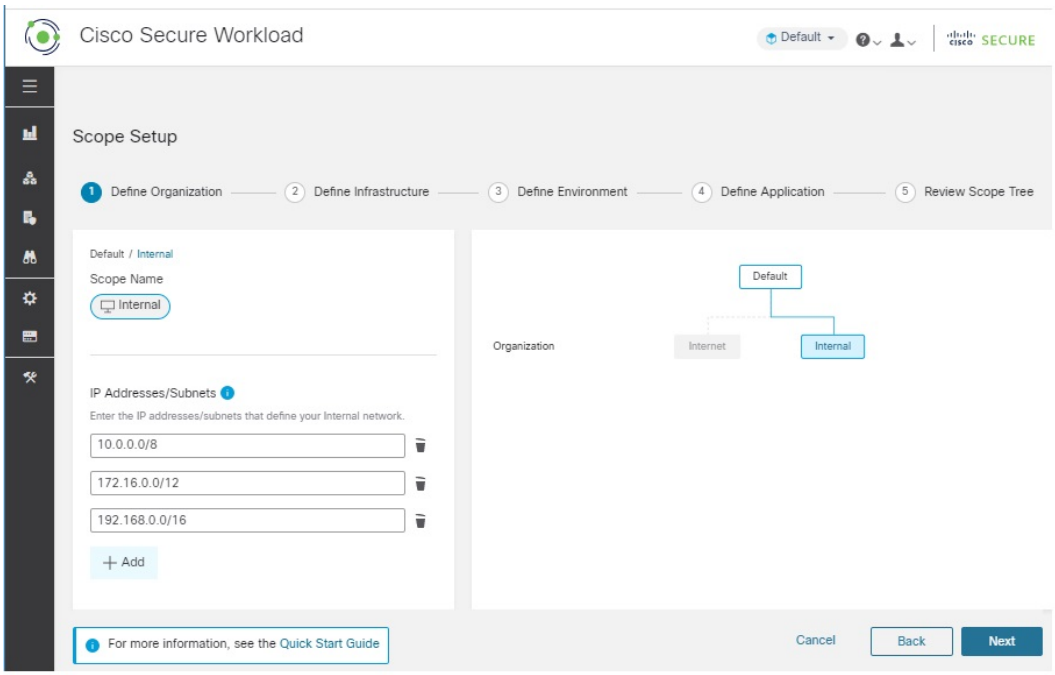


続行する前に、作業するアプリケーションを選択する必要があります。このウィザードのアプリケーションを選択する （12 ページ） のガイドラインを参照してください。

ウィザードを実行すると、ウィザードを再起動しない限り、これらの情報ページに戻ることができない点に注意してください。

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。

したがって、このページで、ウィザードはラベル

```
Organization = Internal
```

を入力した各 IP アドレスに割り当てます。

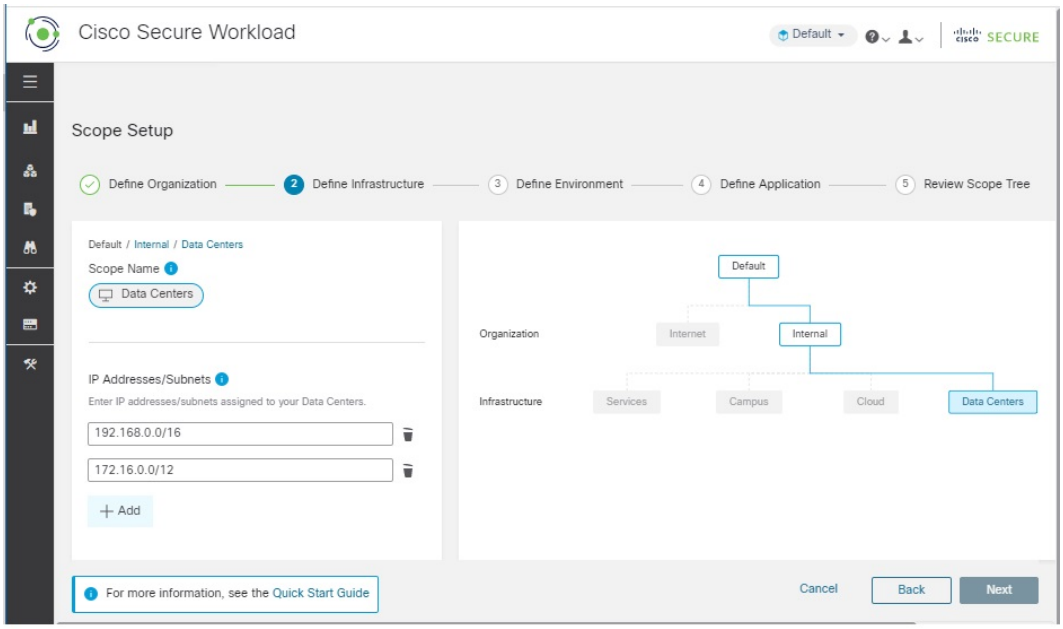
デフォルトでは、ウィザードは、RFC 1918 で定義されているように、プライベート インターネット アドレス空間の IP アドレスを追加します。

ここで、内部ネットワークのすべての IP アドレスを追加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た IP アドレスを含める必要があります。さらに、容易に含めることができるな他 IP アドレスを可能な限り含める必要があります。残り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。

範囲名は変更できますが、意味は同じまま保持されます。範囲名は短く、意味のあるものにする必要があります。



このページで入力する IP アドレスは、前のページで入力した内部ネットワークのアドレスのサブセットである必要があります。選択したアプリケーションに関連付けられた IP アドレスも含める必要があります。理想的には、データセンターのワークロードを表す他のアドレスを含める必要があります。ただし、それらが利用できない場合は、それらを使用せずに続行しても問題ありません（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）。後からいつでもアドレスを追加できます。

ウィザードはラベル

```
Organization = Internal
```

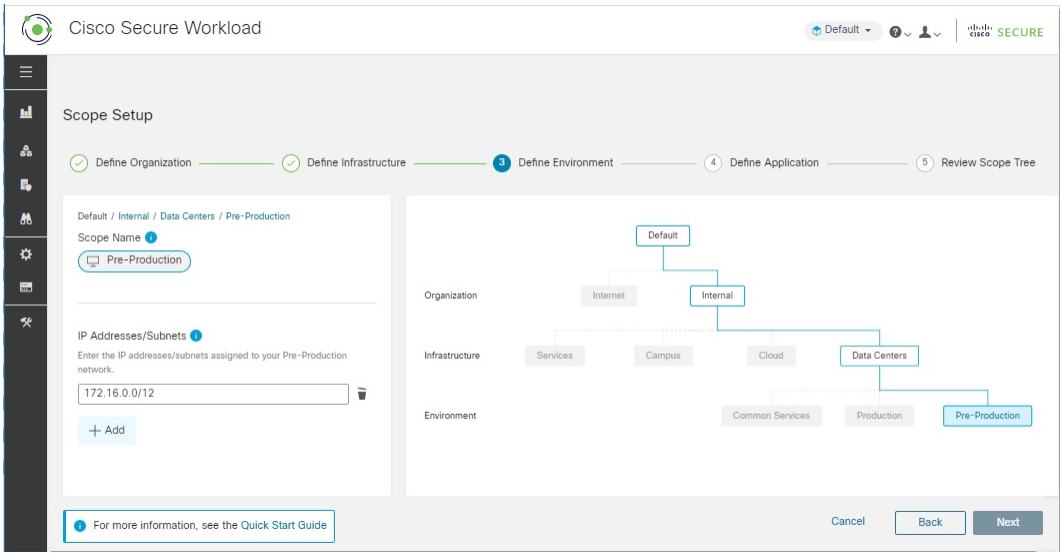
および

```
Infrastructure = Data Centers
```

を入力した各 IP アドレスに割り当てます。

生産前範囲の定義

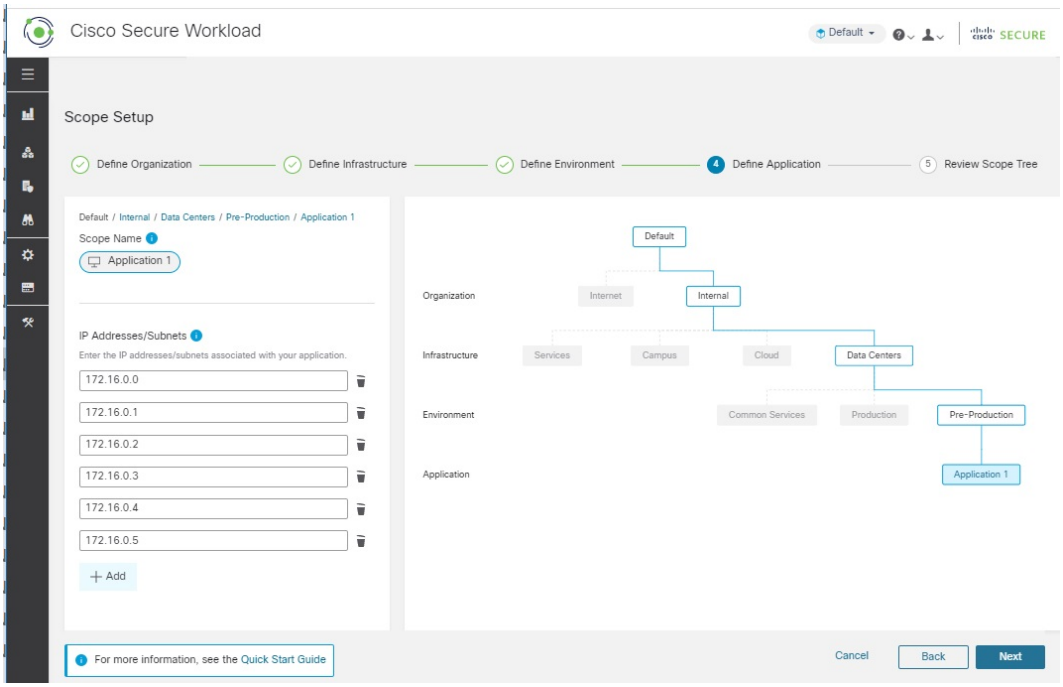
この範囲には、開発、ラボ、テスト、またはステージングシステムなどの非生産アプリケーションおよびホストの IP アドレスが含まれます。実際のビジネスを遂行するために使用しているアプリケーションのアドレスは含めないでください。これは、後で定義する生産範囲の一部になります。



このページで入力する 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である必要があり、ここで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。繰り返しますが、後でさらにアドレスを追加できます。

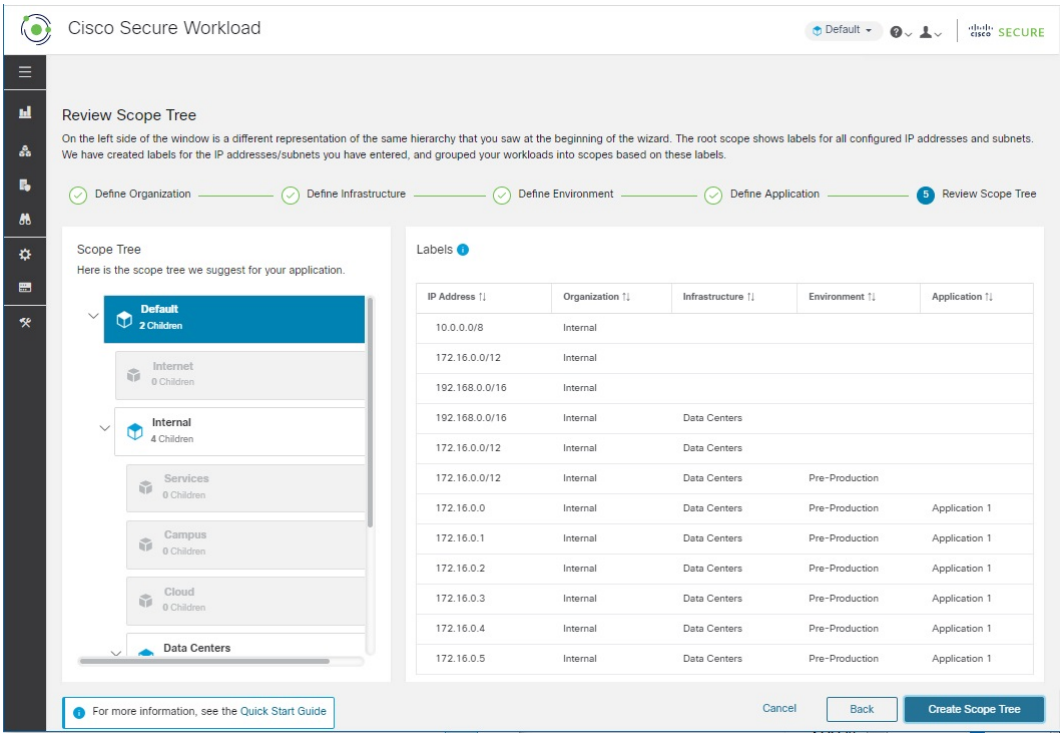
アプリケーション 1 の範囲の定義

「アプリケーション 1」は、あなたが選択したアプリケーションです。このウィザードのアプリケーションを選択する （12 ページ） のガイドラインを参照してください。アプリケーションは複数のワークロードで構成されています。



アプリケーションを構成するワークロードのIPアドレスを追加します。たとえば、データベース、Webサービス、バックアップボリューム、スタンバイインスタンスなどを高可用性展開に含めます。後でさらにアドレスを追加できますが、ここでそれらのほとんどを含めるように試みてください。

範囲ツリー、範囲、およびラベルの確認



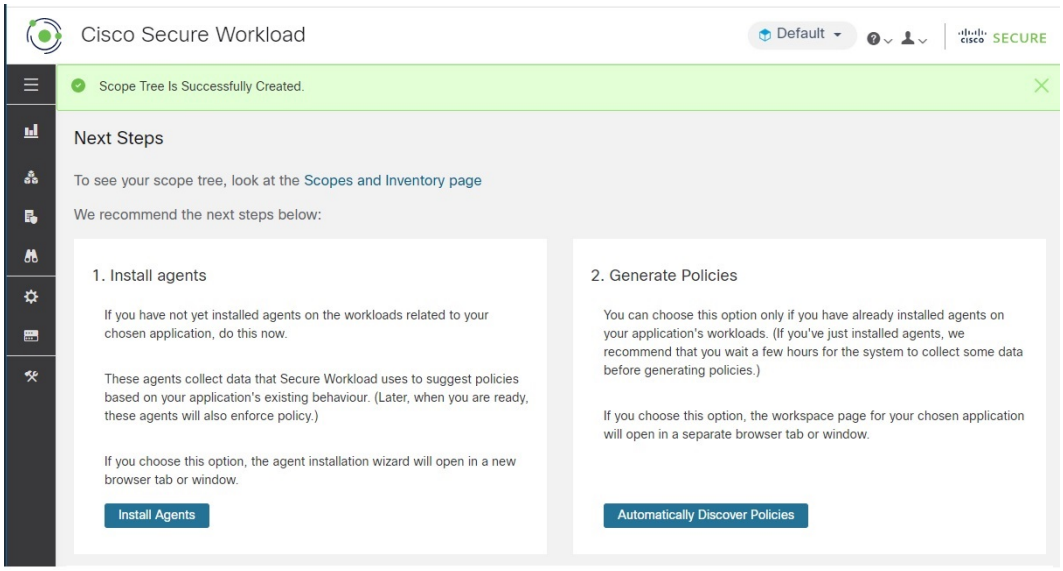
左側には、他のページに表示されている同じ範囲ツリーの別の表現が示されます。ブランチを展開したり折りたたんだり、下にスクロールして特定の範囲をクリックしたりすることができます。

右側には、左側でクリックした範囲内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。列見出しはラベルキーであり、テーブルセルはラベル値を示します。

上の画像では、最上位の範囲が選択されているため、ウィザードで指定したすべてのIPアドレスのデータが表示されます。テーブルの空のセルは、将来のラベル付けを待機しています。たとえば、データセンターにないワークロードや、選択したアプリケーション以外の非生産アプリケーションの一部であるワークロードなどです。

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

次の手順ページ



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、できるだけ早く Cisco Secure Workload エージェントをインストールする必要があります。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、ワークロードへのエージェントのインストール （13 ページ） を参照してください。

ポリシーの生成

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、そのトラフィックに基づいてポリシーを生成（「検出」）するように Cisco Secure Workload に指示できます。詳細については、ポリシーの自動生成 （15 ページ） を参照してください。

その他

ウィンドウの左側にあるナビゲーションバーを使用する場合は、新しいページを個別のウィンドウまたはタブで開きます。そうしないと、このページに戻ることができません。

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 （2 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 （12 ページ） のガイドラインに従ってください。

手順	操作手順	詳細
3	IPアドレスを収集する	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 （12 ページ） を参照してください。
5	アプリケーションのワークロードに Cisco Secure Workload エージェントをインストールする	ワークロードへのエージェントのインストール （13 ページ）を参照してください。
6	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。
7	実際のフローデータに基づいてポリシーを生成（「検出」）する	ポリシーの自動生成 （15 ページ）を参照してください。
8	生成されたポリシーを確認する	生成されたポリシーの確認 （16 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、作業する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、わかりやすくするために、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する必要があります。

- データセンターで実行中
- ベアメタルおよび/または仮想マシンで実行中
- Cisco Secure Workload エージェントがサポートする Windows、Linux、または AIX プラットフォームで実行中：

  https://www.cisco.com/go/secure-workload/requirements/agents [英語] を参照してください。

  （今後の手順で、この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必要があります）
- 生産前環境に展開済み

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）最初からやり直すために、範囲ツリーをリセットする （17 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。

次のステップ

ヒント ウィザードを完了したら、[整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）] に移動して、ウィザードを使用して作成した範囲ツリーを表示して作業きます。

アプリケーションの範囲ツリーのブランチを作成したら、次の手順を実行します。

ワークロードへのエージェントのインストール

ポリシー提案を自動的に生成するために使用されるフローデータを収集するには、ワークロードにエージェントをインストールします。後で、これらのエージェントはポリシーを適用できますが、**エージェントは、指示するまでポリシーを適用しません。**

データの収集を開始するには、エージェントをできるだけ早くインストールする必要があります。データが多いほど、より正確なポリシー提案が生成されます。

選択したアプリケーションに関連する各ワークロードにエージェントをインストールします。

正当な理由がない限り、デフォルト設定を使用してください。

エージェントのインストールに関する追加情報が必要な場合は、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「Deploying Software Agents」の章を参照してください。

始める前に

- エージェントをインストールするすべてのワークロードが、サポートされているプラットフォームで実行されていることを確認します。https://www.cisco.com/go/secure-workload/requirements/agents [英語] を参照してください。
- 各ワークロードにエージェントをインストールする権限があることを確認します。必要に応じて、必要な権限を持つ人に依頼します。

手順

ステップ 1 ウィザードの [エージェントのインストール（Install Agents）] ボタンをクリックします。

または、次の方法でエージェントインストーラーにアクセスできます。

a) Cisco Secure Workload Web ポータルにサインインします。
b) 左側のナビゲーションバーで、[管理（Manage）] > [エージェント（Agents）] を選択します。
c) [インストーラ（Installer）] タブをクリックします。

ステップ 2 [インストーラーを使用してエージェントを自動インストール（Auto-Install Agent using an Installer）] をクリックし、[次へ（Next）] をクリックします。

ステップ 3 オンプレミスの Cisco Secure Workload を使用している場合：

オプション[エージェントをどのテナントにインストールしますか？（Which tenant is your agent going to be installed under?）] が表示された場合：他のものを選択する理由がない限り、デフォルトを選択します

（このオプションは、オンプレミスの Cisco Secure Workload を使用している場合にのみ表示されます）。

ステップ 4 次のオプションはスキップします：[このワークロードにどのラベルを適用しますか？（オプション）（Which tenant is your agent going to be installed under? (Optional)）]

ステップ 5 アプリケーションが実行されているプラットフォームを選択します。

ステップ 6 環境に必要な場合は、HTTP プロキシを入力します。

ステップ 7 必要に応じて、インストーラーの有効期限オプションを選択します。

ステップ 8 [インストーラのダウンロード（Download Installer）] をクリックします。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 インストールの事前チェックの指示に従い、[次へ（Next）] をクリックします。

ステップ 11 インストールの指示に従います。

変更する正当な理由がない限り、デフォルト設定を使用してください。

インストーラースクリプトにリストされているフラグを変更する必要はありません。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 画面の指示に従って、エージェントが正常にインストールされたことを確認します。

ステップ 14 アプリケーションに関連付けられた各ワークロードにエージェントをインストールします。

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 （16 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 （16ページ）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。

ポリシーの表示

ポリシー検出を開始した後に（またはそれ以外のときでも）ポリシーページから移動した場合は、範囲に関連付けられたアプリケーション ワークスペースに移動することで、生成された（「検出された」）ポリシーを表示できます。

始める前に

ポリシーを検出します。ポリシーの自動生成 （15 ページ） 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バーで、[防御（Defend）]>[セグメンテーション（Segmentation）] を選択します。

ステップ 2 ウィンドウの左側にある範囲のリストで、ポリシーを表示する範囲までスクロールしてクリックします。

ステップ 3 ポリシーを表示するワークスペースをクリックします。

これは、ポリシー検出を開始したときにどのワークスペースにいたかに応じて、プライマリワークスペースまたはセカンダリワークスペースになります。

ステップ 4 [ポリシーの管理（Manage Policy）] をクリックします。

ステップ 5 ポリシー提案のリストが表示されない場合は、[絶対ポリシーとデフォルトポリシー（Absolute and Default Policies）] をクリックします。

ステップ 6 （オプション）別のワークスペースバージョン（プライマリまたはセカンダリ）のポリシーを表示するには、ページの上部にあるドロップダウンリストを使用します。

ステップ 7 （オプション）別の範囲のポリシーを表示するには、ページの上部にある [ワークスペース（Workspace）] をクリックし、左側のリストで別の範囲をクリックします。

次のタスク

検索対象については、生成されたポリシーの確認 （16 ページ） を参照してください。

（オプション）最初からやり直すために、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 の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、次を参照してください。

- Cisco Secure Workload のオンラインヘルプ
- ご使用のリリースの *Cisco Secure Workload* ユーザーガイド PDF、https://www.cisco.com/c/en/us/support/security/tetration-analytics-g1/model.html [英語] から入手可能

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。