



Cisco Secure Workload の設定のモニタリング

この章では、モニタリングオプションにアクセスするために必要なロールについて概説し、サイト管理者とカスタマーサポートが詳細なエージェント情報を表示できること、および範囲所有者がインベントリとエージェントを表示できることを強調します。このドキュメントでは、エージェントモニタリングの概念を紹介し、使用可能なエージェントのタイプについて詳しく説明しています。これには、包括的なフローデータとプロセスの可視性を提供する詳細可視性エージェント、およびファイアウォールルールの適用機能を追加するポリシーエージェントが含まれています。さらに、AnyConnect および Identity Services Engine (ISE) エージェントについても説明します。ISE エージェントでは、メタデータの収集とエンドポイントの登録に Cisco ISE を利用します。エージェントのステータスと統計に移り、この章では、最適なパフォーマンスを確保するために、CPU や帯域幅のオーバーヘッドなどのさまざまなチャートでエージェントの状態を監視することの重要性について強調しています。また、CPU と帯域幅のオーバーヘッドチャートが、優れた可視性エージェントと適用エージェントのリソース使用率に関するインサイトを提供することを説明しています。さらに、[エージェント正常性 (Agent Health)] チャートは、構成サーバーとの定期的なチェックインに基づいて、アクティブなエージェントと非アクティブなエージェントを識別するために重要です。ソフトウェアの更新とパケット損失のモニタリングが重要になります。これは、これらのメトリックが、トラフィックを効率的にアップグレードおよび検査するエージェントの能力を示しているためです。

この章では、エージェント全体のソフトウェアバージョンとオペレーティングシステムの可視化についても説明し、展開の状況を理解するのに役立ちます。ユーザーは、AWS や Azure などのクラウドコネクタの適用ステータスを監視し、ポリシーの適用の問題に対処するための手順を提供する必要があるため、ネットワークリソース全体で堅牢なセキュリティとコンプライアンスが確保されます。

使用できる **モニタリング** オプションは、ユーザーロールによって異なります。



注目 最近の GUI の更新により、ユーザーガイドで使用されているイメージやスクリーンショットの一部に、製品の現在の設計が完全に反映されていない可能性があります。最も正確に視覚的に参照するには、このガイドを最新バージョンのソフトウェアと組み合わせて使用することを推奨します。

- [エージェントのモニタリング, on page 2](#)
- [エージェントのモニタリングタイプ, on page 2](#)
- [エージェントのステータスと統計, on page 4](#)
- [適用ステータス, on page 6](#)
- [クラウドコネクタの適用ステータス, on page 8](#)
- [ポリシー更新の一時停止, on page 8](#)

エージェントのモニタリング

このページには、現在選択されているルート範囲に基づいて、クラスタ内のすべての監視対象エージェントの数が表示されます。



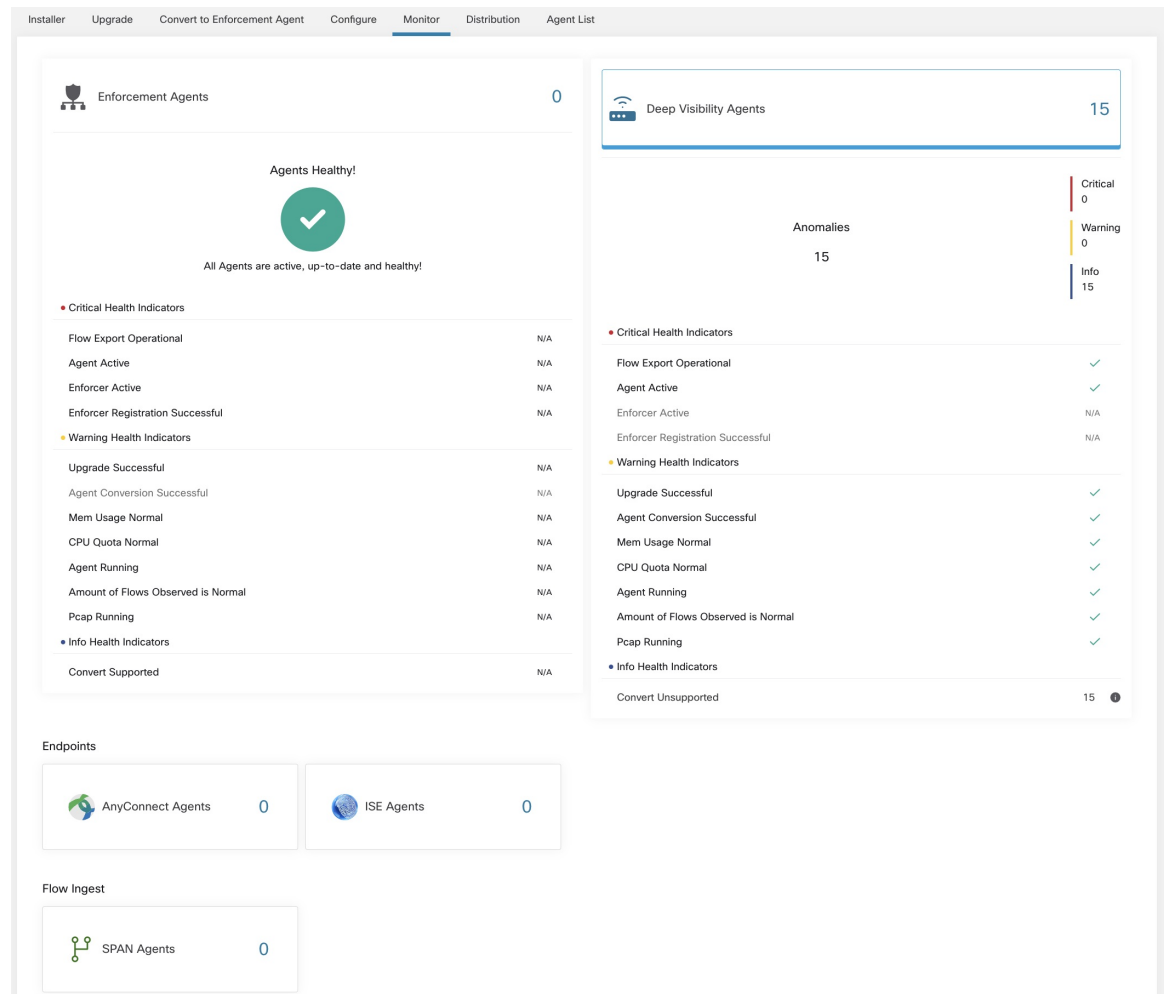
Note インベントリの総数は、収集ルールを適用した後にネットワーク上で観察されたすべてのインベントリの合計です。

エージェントのモニタリングタイプ

エージェントを監視するには、左側のナビゲーションバーで[管理 (Manage)] > [エージェント (Agents)] をクリックし、[監視 (Monitor)] タブをクリックします。

このページは、**サイト管理者**および**カスタマーサポート**の役割を持つユーザーのみが利用できます。**範囲所有者**は、インベントリ、優れた可視性エージェント、および適用エージェントを表示できます。

Figure 1: インストールされているエージェントの総数



次の表は、エージェントタイプごとの違いを示しています。

Agent Type	説明
優れた可視性	時系列フローデータ、ホストで実行されるプロセスに関して最高の忠実度を提供します。ほとんどの Linux および Windows プラットフォームがサポートされています。 <code>sw_agents_deployment-label</code> を参照してください。
施行	優れた可視性エージェントで使用可能なすべての機能を提供します。それに加えて、適用エージェントは、インストールされているホストに対してファイアウォールルールを設定することができます。

AnyConnect	Network Visibility Module (NVM) を備えた AnyConnect セキュア モビリティ エージェントを実行しているエンドポイントで時系列フローデータを提供します。Cisco Secure Workload エージェントのインストールは必要ありません。NVM によって生成された IPFIX レコードは、Secure Workload AnyConnect プロキシコネクタに送信されます。Windows、Mac、および特定のスマートフォンのプラットフォームがサポートされています。
ISE	Cisco ISE に登録されているエンドポイントに関するメタデータを提供します。ISE コネクタは、ISE pxGrid を介してメタデータを収集し、ISE エージェントが ISE アプライアンスから取得した属性とエンドポイントにログインしたユーザーの LDAP 属性に基づいてラベルをプッシュするときに ISE エンドポイントを Secure Workload に登録します。
次の表は、Cisco Secure Workload が提供するさまざまなアプライアンスエージェントの概要を示しています。	
アプライアンスエージェント	説明
SPAN	ホストごとのエージェントのインストールを必要とせずに、フロー分析を提供します。Secure Workload ERSPAN VM アプライアンスで実行されます。任意の Cisco スイッチから発信された ERSPAN パケットを消費します。



Note NetFlow、NetScaler、F5、AWS、AnyConnect Proxy などのアプライアンスエージェントが、コネクタとしてサポートされるようになりました。コネクタの詳細については、「[コネクタとは](#)」を参照してください。

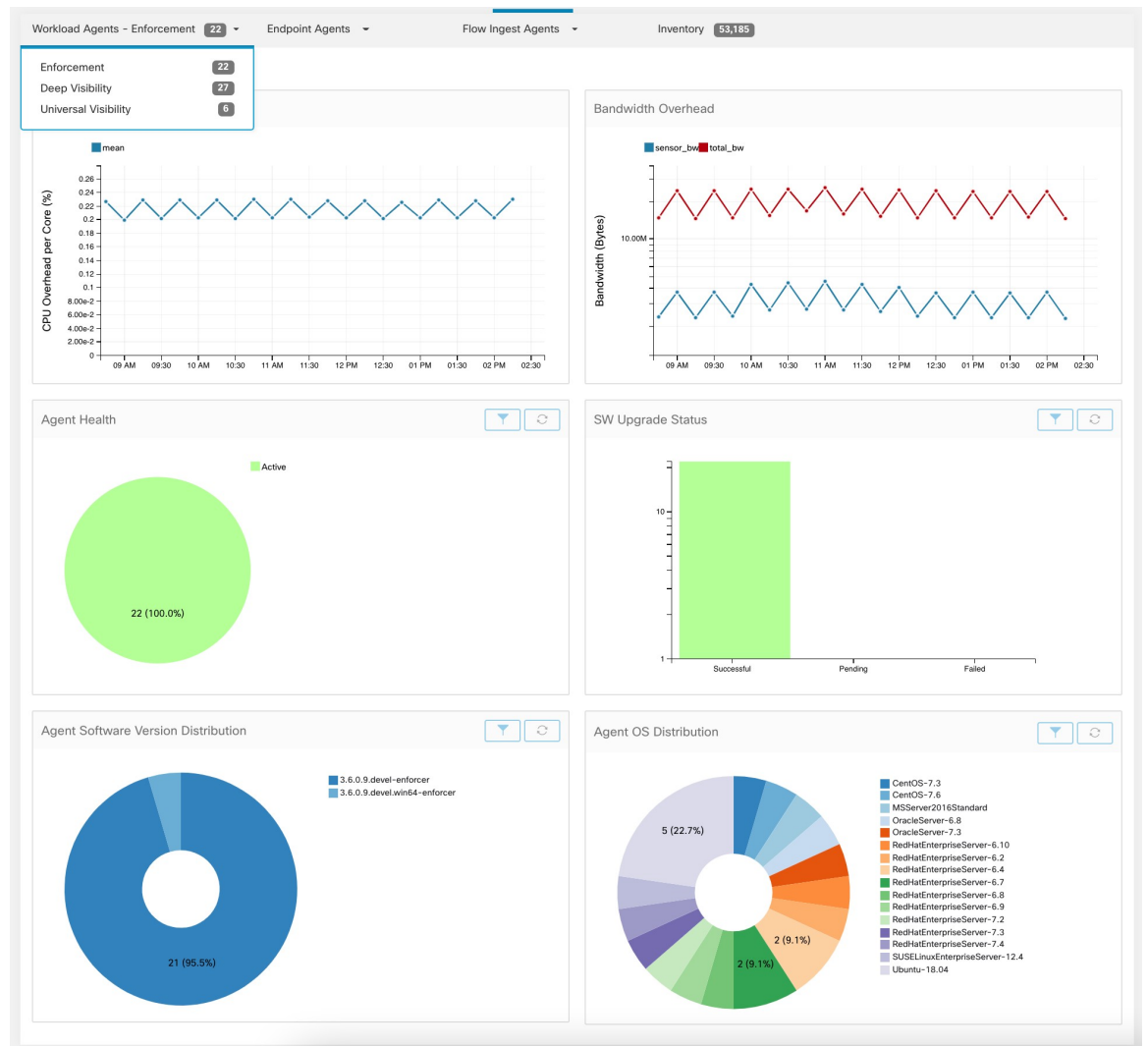
ゼロ以外のエージェントタイプのボタンを押すと、各エージェントタイプの分布にさらにドリルダウンできます。

エージェントのステータスと統計

このトピックで説明されているチャートを表示するには、[管理 (Manage)] > [エージェント (Agents)] を選択し、[分布 (Distribution)] タブをクリックします。

次のグラフは、詳細可視性タイプと適用エージェントタイプの両方で使用できます。

Figure 2: エージェントの分布



このページには、エージェントタイプごとに、全体的な CPU オーバーヘッド、帯域幅のオーバーヘッド、欠落したパケット、OS/バージョンの分布、エージェントのアップグレードステータスなど、登録されたエージェントの概要と正常性が表示されます。

[CPUオーバーヘッド (CPU Overhead)]チャート

[CPUオーバーヘッド (CPU Overhead)]チャートには、全エージェントからのコアごとのCPUオーバーヘッド集計ビューが表示されます。エージェントごとのCPUオーバーヘッドは、[ワークロードプロファイル](#)の一部として表示されます。このチャートは、詳細可視性タイプと適用エージェントタイプでのみ使用できます。

[帯域幅オーバーヘッド (Bandwidth Overhead)]チャート

[帯域幅オーバーヘッド (Bandwidth Overhead)]グラフには、総帯域幅とエージェントが使用する帯域幅の集約された統計が表示されます。エージェントごとの帯域幅オーバーヘッドは、

ワークロードプロファイルの一部として表示されます。このチャートは、詳細可視性タイプと適用エージェントタイプでのみ使用できます。

[エージェントの正常性 (Agent Health)] チャート

[エージェントの正常性 (Agent Health)] チャートには、アクティブなエージェントまたは非アクティブなエージェントの数が表示されます。アクティブなエージェントは、アップグレードのためにコンフィギュレーションサーバーに定期的にチェックインするエージェントです。チェックインの間隔は 30 分です。エージェントが 2 回を超えてチェックイン期間にチェックインしなかったことがわかった場合、そのエージェントは非アクティブなエージェントと宣言されます。

[最新のリリースへのソフトウェアエージェントの更新 (Software Agent Updates to Latest Revision)] チャート

エージェントがコンフィギュレーションサーバーにチェックインするたびに、エージェントは現在の RPM バージョンも提示します。エージェントが特定のバージョンに設定されていて、2 回のチェックイン期間後に更新できていなかった場合、そのエージェントは最新バージョンにアップグレードできないと宣言されます。

[欠落エージェントパケット (Agent Packet Missed)] チャート

まれに、ホストを通過するトラフィック量がエージェントの検査できるレートよりも多い場合、一部のパケットが分析からスキップされます。欠落パケット数と対応するエージェント名がこのチャートに表示されます。

エージェントソフトウェアバージョンおよび OS の分布のチャート

これらのグラフには、Secure Workload クラスターに登録されているすべてのエージェントのエージェントバージョン分布と親 OS プラットフォームが表示されます。

適用ステータス

適用ステータスを表示するには、ウィンドウの左側のナビゲーションバーの[保護 (Defend)]> [適用ステータス (Enforcement Status)] をクリックします。

このページは、サイト管理者/カスタマーサポートユーザーと範囲所有者が、全適用エージェントの現在のステータス概要 (ポリシーを適用しているクラウドコネクタを含む) を取得するために使用できます。

いずれかのチャートで赤またはオレンジが表示されている場合は、該当するトピックを参照してください。

Table 1: 適用ステータスチャート

チャート (Chart)	結果	アクションの実行
適用が有効なエージェント (Agent Enforcement Enabled)	有効化されていない (Not Enabled)	エージェント設定で適用が有効になっていることを確認します。 エージェント設定プロファイルの作成 を参照してください。

チャート (Chart)	結果	アクションの実行
エージェントポリシーの設定 (Agent Policy Config)	古いポリシー (Stale Policies)	一般的に、この状況は一時的なものであり、通常はアクションを必要としません。これは、ラベルに基づく Secure Workload 展開によってインベントリとポリシーが動的に更新されるために発生します。 ただし、個々のワークロードでこの状況が続く場合は、Cisco TAC にお問い合わせください。
エージェントの具体的なポリシー (Agent Concrete Policies)	スキップ (Skipped)	これは、ポリシーが一部のエージェントにプッシュされなかったことを示します。

**Tip**

- 個々の範囲またはテナント全体のステータスを表示するには、ページの左上にある [範囲でフィルタ (Filter by Scope)] オプションを使用します。
- チャートに問題が示されている場合は、チャートの関連部分をクリックして、問題のあるワークロードを特定します。

テーブルに、影響を受けるワークロードが表示されます。

または、フィルタリングオプションを表示するには、チャートの下にある [フィルタ (Filter)] ボックス内の [(i)] ボタンをクリックします。
- 豊富な追加の詳細を表示するには、フィルタされたワークロードのリスト内で IP アドレスリンクをクリックして、[ワークロードプロファイル (Workload Profile)] ページを表示します。

次の表で、適用ステータステーブルに表示されるフィールドについて説明します。

フィールド	説明
ホスト名 (Host Name)	ワークロードのホスト名。
アドレス (Address)	ワークロード上のすべてのインターフェイスの IP アドレス。
[有効化された適用 (Enforcement Enabled)]	エージェントで適用が有効になっているかどうかを示します。

[同期されている具体的なポリシー (Concrete Policies in Sync)]	必要なバージョンの具体的なポリシーが現在エージェントに適用されているかどうかを示します。
[具体的なポリシー (Concrete Polices)]	いずれかのホストでこの値が [スキップ (Skipped)] と表示されている場合は、そのホスト上のエージェントがポリシーの制限に達していることを意味します。(ポリシーに関連する制限 を参照。)
[ポリシー数 (Policy Count)]	エージェントの具体的なポリシーの数。
ステータス	最新のポリシー設定適用のステータス。ステータスが [CONFIG_SUCCESS] の場合、現在のバージョンが問題なく適用されていることを示します。

クラウドコネクタの適用ステータス

AWS または Azure クラウドコネクタを設定している場合：

すべてのインターフェイスの適用ステータスが、[適用ステータス (Enforcement Status)] ページに表示されます。ポリシーが正常に適用された場合、ポリシーは同期しています。同期していない場合は、対応するエラーメッセージが表示されます。

[適用ステータス (Enforcement Status)] ページのポリシー数は Secure Workload アカウンティングで、AWS または Azure ルールアカウンティングではありません。

(AWS のみ) このページのホスト名フィールドは、パブリック DNS から取得されます。指定された VPC でパブリック DNS が有効になっていない場合、ホスト名フィールドは空になります。

ポリシー更新の一時停止



Caution このオプションは、全範囲内のすべてのワークロードのポリシー更新を一時停止します。

この機能には、サイト管理者またはカスタマーサポートの権限が必要です。

全範囲内のすべての適用エンドポイントのルール更新を一時停止するには、次の手順を実行します。

1. ナビゲーションウィンドウで、[防御 (Defend)] > [適用 (Enforcement)] の順に選択します。
2. [ポリシー更新 (Policy Updates)] の横にあるステータスをクリックします。

3. 注意を読んで同意します。

Figure 3: ファイアウォールルールが継続的に更新されている場合

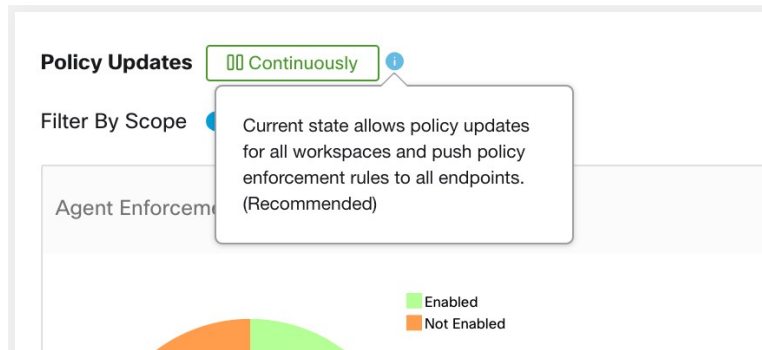
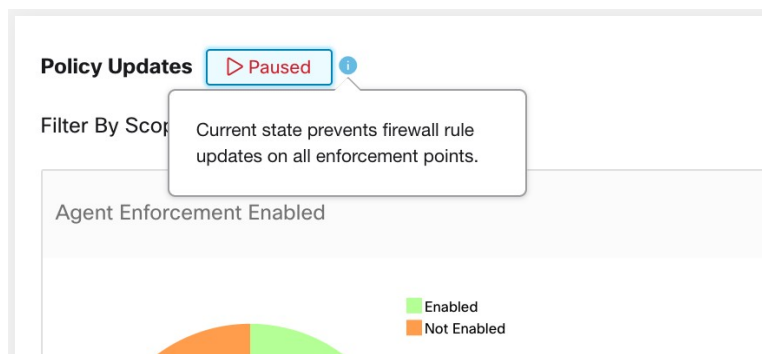


Figure 4: ファイアウォールルールの更新が一時停止されている場合



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。