Cisco Tetration 3.3 ラボ v1.0

最終更新日：2019 年 11 月 29 日

日本語版：2019 年 12 月 8 日（英語版には含まれない内容が一部あります）

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

要件

次の表に、このデモンストレーションの要件の概要を示します。

表 1. 要件

必須	オプション
ラップトップ	Cisco AnyConnect®

このソリューションについて

Cisco Tetration プラットフォームは、マルチクラウド インフラストラクチャ全体にわたり、包括的なワークロード保護機能および類を見ない情報を提供することで、データセンターおよびクラウドのセキュリティの課題に対応します。

さまざまなアプリケーションによって、データセンター インフラストラクチャの設計が推進されています。現在のアプリケーションは非常に動的で、仮想化、コンテナ化、マイクロサービス、ワークロードモビリティ技術が使用されています。しかも、アプリケーション コンポーネント間の通信パターンは常に変化を続けています。現在のアプリケーションの導入には、過去のトラフィックパターンからの根本的な変化を表す、かなりの割合の East-West トラフィック（75% 以上）が必要です。このパターンの変化により、攻撃対象領域が拡大し、これらのアプリケーション インフラストラクチャ内で自由なラテラルムーブメントが行われる可能性が高まりました。このようなダイナミズムによって、組織が取り組むべき次のような重要な課題が生じています。

- アプリケーションフローと依存関係の理解の欠如
- 現在のニーズに対応できず、将来のニーズにはさらに対応できなくなる静的な境界ベースのセキュリティモデル
- アプリケーションの動作に基づくセグメンテーションのためのホワイトリストポリシーの生成と管理の難しさ
- マルチクラウド インフラストラクチャ全体にセグメンテーションポリシーを適用するための一貫性のないアプローチ
- 攻撃対象領域を体系的に縮小する包括的な方法がない
- 感染拡大を最小化したり、異常な動作を検出する機能がほとんどない

Cisco Tetration™ プラットフォームは、オンプレミスおよび複数のクラウドプロバティ内のアプリケーション ワークロード（サーバ、VM、コンテナ）から収集された包括的なフローテレメトリデータを使用して、これらの課題に対応するために構築されました。Tetration は、教師なしの機械学習と高度な分析アルゴリズムを使用して、さまざまな導入環境でアプリケーション環境の包括的なワークロード保護を行います。

Tetration には、次のような目的のためにすぐに使用可能なソリューションがあります。

- アプリケーション コンポーネント、通信、および依存関係の優れた可視性

- アプリケーションの動作に基づくゼロトラストポリシーの自動生成
- ビジネスおよび規制要件によって義務付けられている階層型のセキュリティポリシー管理
- ラテラルムーブメントを最小化するための、インフラストラクチャ全体におけるセグメンテーションポリシーの一貫性のある適用
- 攻撃対象領域を縮小するための、ソフトウェアの脆弱性の露出の特定
- フォレンジック検出と侵害の兆候（IOC）動作の記録のためのプロセス動作のベースラインと異常の特定

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザとコンポーネントが含まれています。コンポーネントのほとんどは、あらかじめ定義された管理ユーザアカウントを使用してすべて設定できます。コンポーネントへのアクセスに使用する IP アドレスとユーザアカウント資格情報は、アクティブセッションの [トポロジ（Topology）] メニューのコンポーネントアイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[**手順を見る**]

注：セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 最適なパフォーマンスを得るには、Cisco AnyConnect VPN [**手順を見る**] およびラップトップのローカル RDP クライアント [**手順を見る**] を使用してワークステーションに接続します。

- ワークステーション 1：198.18.133.36、ユーザ名：dCloud\demouser、パスワード：C1sco12345

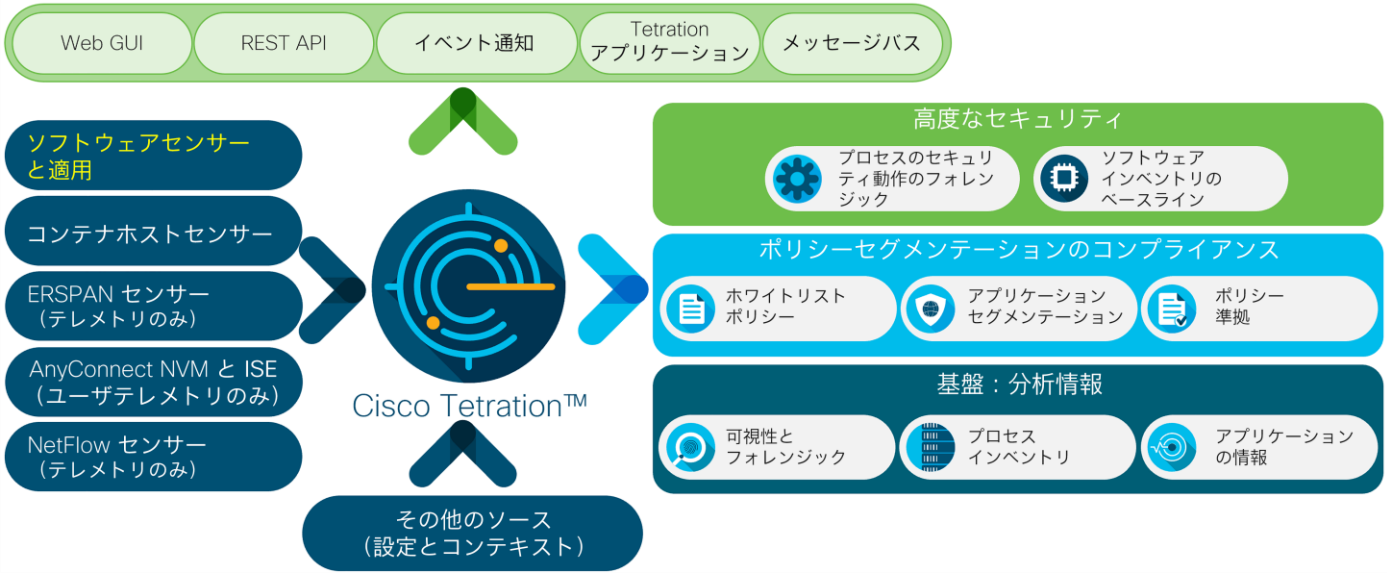
Cisco Tetration の概要

このラボシナリオの目的は、以下の内容を含む **Cisco Tetration** の概要を説明することです。

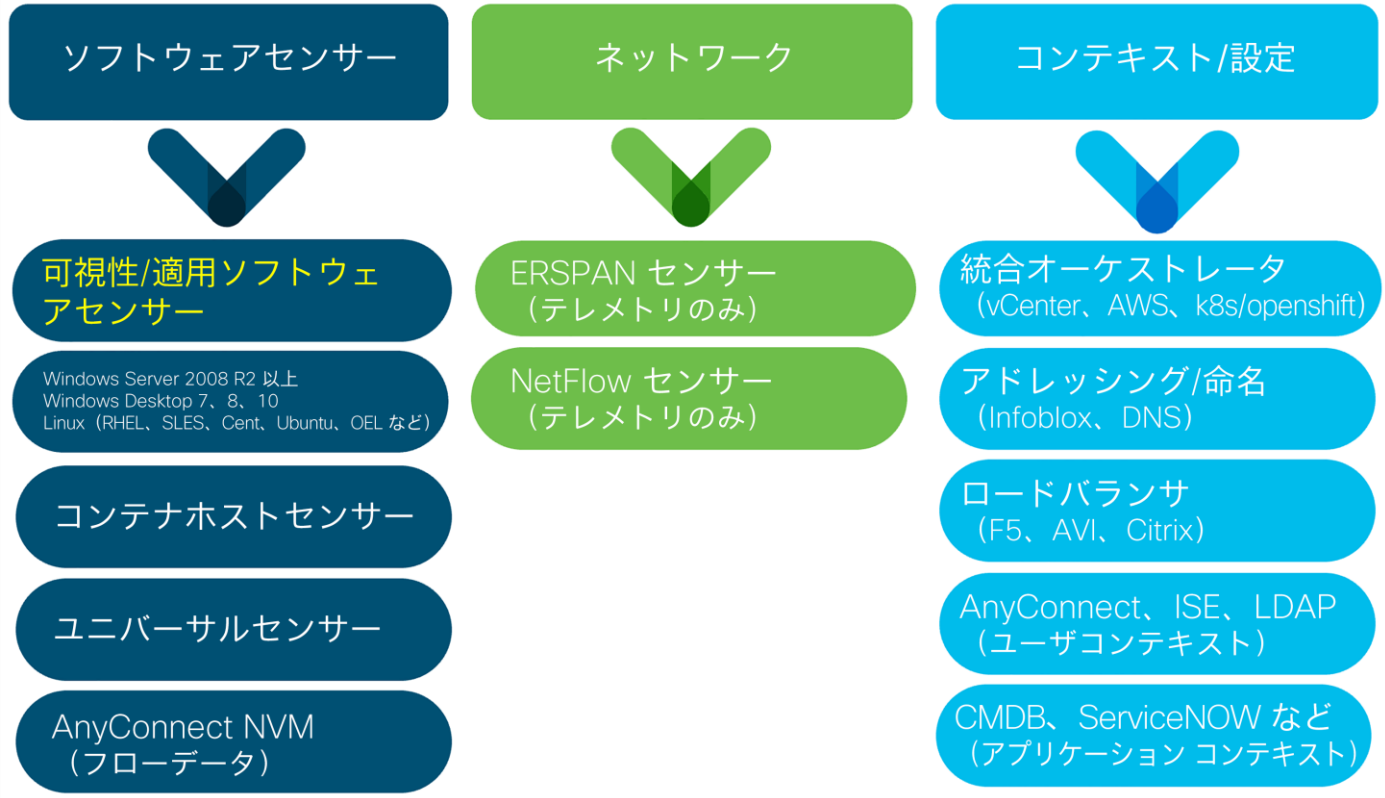
- 仕組み
- 解決するビジネス上の問題
- Tetration データを使用して問題を解決し、優れたビジネス上の判断を下す方法
    - アプリケーションの情報
    - ポリシーの検出
    - セキュリティとポリシーの適用
    - コンプライアンス

仕組み

Cisco Tetration の中核となるのは、ビッグ データ プラットフォームです。これは、リッチなテレメトリの大容量ストリーミングの処理、膨大なワークロードにわたる数千種類のアプリケーションのマッピング、アプリケーションに関する数百万種類のポリシールールの適用に対応するよう設計されています。お客様は、教師なしの機械学習、アルゴリズム的アプローチ、自動適用により、このプラットフォームを活用したターンキーソリューションを手に入れることができます。さらに、このプラットフォームは、履歴フローとイベントデータに加え、詳細なフォレンジックを可能にする長期のデータ保持（数ヵ月）向けに設計されています。



データの収集および Tetration への入力の方法は数通りあります。



データ収集の詳細

3. Tetration がテレメトリを収集する場合は主にソフトウェアセンサーを使用します。これはターゲットワークロードのオペレーティングシステムで動作する軽量のバイナリで、そのワークロードの動作に関する情報およびプロセスとデータを含むアクティブな会話を収集します。このデータがクラスタに報告されると、Tetration は、サーバが SQL プロセスを使用して Web サーバと通信したり、DNS ルックアップを実行したり、DBA がそのサーバで管理またはメンテナンス作業を行ったりするときなどに、関連する会話を関連付けることができます。

4. ソフトウェアセンサーでは、単一バイナリで完全な機能を提供できます。これには、テレメトリの収集とレポート、ホワイトリストのセグメンテーションルールの適用に加え、システムの動作や異常の監視およびこれらの異常な動作に関連するフォレンジックデータの記録が含まれます。

注：現行リリースでは、Linux および Windows サーバベースのワークロードをサポートしています。ベアメタルサーバまたは VM のいずれも使用できます。ソフトウェアセンサーは、ホストのネットワークスタックから送受信されるパケットヘッダーからメタデータ情報を収集します。パケットのメタデータに加えて、プロセス情報とその他の OS 特性も収集します。センサーはペイロードからは情報を収集しません。これは、PII やその他の規制、法律、データの整合性またはセキュリティ上の関心事項を考慮する際に重要な点です。

ソフトウェアセンサーは、設定可能な SLA に対してパフォーマンスを自己調整して、センサーがプライマリ アプリケーション サービスのパフォーマンスの問題を引き起こすのを防ぎます。Tetration クラスタは、CPU 使用率を管理するためのメカニズムを提供します。デフォルトでは、CPU 全体の約 3% が平均で使用されています。

ソフトウェアセンサーは、アプリケーション セグメンテーションのエンフォースメントポイントとしても機能します。Tetration プラットフォームがセグメンテーションのポリシーを提供し、ソフトウェアセンサーが Linux IPTables/IPSets や Windows Advanced Firewall などの OS 機能を使用してポリシーを調整します。

セキュリティの目的で、センサーは、それらを管理するクラスタに対して認証およびコード署名されます。センサーからクラスタへの通信は認証および保護されるため、クラスタによって生成されたセンサーだけがクラスタと通信できるようになります。また、センサーは、その作成元のクラスタとのみ通信できます。すべてのセンサー管理は、Tetration クラスタのユーザインターフェイスを通じて実行されます。

5. ネットワーク専用のテレメトリソースがいくつかあります。その 1 つが Tetration ERSPAN センサーです。この収集の使用例では、ネットワークトラフィックのコピーが ERSPAN を介してアプライアンス VM に送信され、VM で関連するデータがキャプチャされて、関連メタデータがクラスタにストリーミングされます。NetFlow や Nexus 9000 スイッチのハードウェアセンサーなど、ネットワークデータの他のソースを使用することは可能ですが、サンプリングレートの性質やデータ取得の不完全な性質により、これらは Tetration が提供しようとしている結果よりも劣るデータソースと見なされます。

6. Tetration が収集するアクティブなフローおよびプロセスデータを向上させる最良の方法の 1 つは、取り込み時にコンテキストデータを収集して付加することです。このタイプのデータを追加するにはさまざまな方法があります。製品に完全に統合されていたり、外部に統合されていたり、手動で、または API を使用してロードできる単なる情報ソースの場合もあります。以下に、適切なコンテキストソースをいくつか示します。

   - VMware vCenter*
   - AWS*
   - Kubernetes*
   - ロードバランサ（F5、Citrix、AVI）*
   - Infoblox*
   - DNS*
   - ISE*
   - LDAP（ネイティブまたは ISE/AnyConnect 経由で直接）
   - CMDB（ServiceNow など）

注：Tetration では、F5、IP アドレス管理データベース、DNS 設定など、サードパーティのデータソースからコンテキストを追加することができ、アプリケーション環境の理解を深めることができます。さらに、アセットタギングや注釈を使用して、ワークロードやトラフィックタイプに関する情報をインポートすることもできます。これらのコンテキスト情報の追加ソースは、Tetration を通じて自動的に統合するか、Tetration API を使用してスクリプトで外部か

ら追加するか、Tetration UI を使用して手動で追加することができます。上記の（*）は、Tetration プラットフォームに組み込まれている統合を示しています。

これにより、Tetration は、利用可能なほぼすべての導入環境で機能することができます。Tetration は、シスコおよびシスコ以外の環境、オンプレミスのデータセンターに加え、パブリッククラウドとプライベートクラウドの環境からデータを収集して分析できます。

テレメトリ収集の一環として、Tetration は、ネットワークフローの詳細、プロセスデータ、ソフトウェアインベントリ、環境コンテキストの詳細など、さまざまな種類のデータをキャプチャして保存します。たとえば、Tetration は、システムユーザ、プロセス、データフロー、仮想ホストとインフラストラクチャ、および IP アドレス以外の内容も含む送信元と宛先の情報をキャプチャし、すべてのフローそれぞれにその情報を結び付けます。これにより、システムとすべてのユーザがフローデータを確認し、その会話が実際に何をしているかを完全に把握できます。

個々のセンサーは、パケットヘッダーからメタデータのみをキャプチャします。センサーは、ペイロードから情報を収集することはありません。ペイロードは機密性が高い可能性があり、暗号化されることがよくあり、Tetration プラットフォームで実行される分析には影響しません。

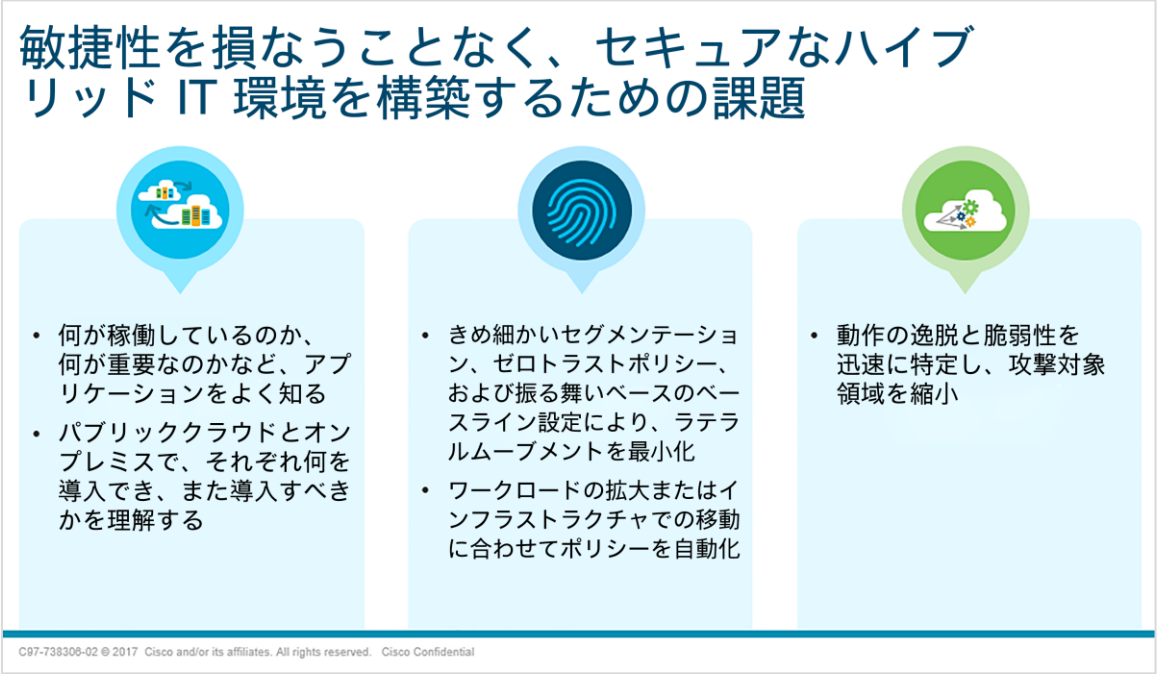
Tetration では、データおよび情報に対するさまざまなアクセス メカニズムを利用可能です。堅牢な Web ベースのユーザインターフェイスを使用して情報を可視化できるだけでなく、高度なインデックスアルゴリズムにアクセスして非常に短時間（通常は数秒）で数十億のフローのデータレイクから特定の情報を検索して検査することができます。Tetration プラットフォームはオープンな設計になっているため、ユーザは REST API アクセスを利用して生成されたデータの多くをクエリできます。発信メッセージの場合、Tetration は多数の一般的なメッセージングシステムを通じて通知をプッシュできます。発信通知は、フローが受け入れ可能ポリシーに準拠していない場合や、システムの動作の異常が発生した場合など、さまざまな条件でトリガーされます。

ビジネス上の問題の解決

Cisco Tetration で解決されるビジネス上の主な問題は、アプリケーションクリープ、データセンターセキュリティ、および攻撃対象領域の脆弱性の 3 つです。Cisco Tetration では次のことが可能です。

- アプリケーションの理解：実行内容、通信相手、共通の通信パターンは、アプリケーション機能にとって重要なものを判断するのに役立ちます。
- ラテラルムーブメントを最小化：アプリケーションの理解に基づいたポリシーの検出により、ゼロトラストポリシーを作成し、それらのポリシーのセグメンテーションを適用するために必要な作業が容易になります。
- 脆弱なソフトウェアの特定：脆弱性のあるコンポーネントの影響を受けるアプリケーションを識別し、脆弱性に関連するセキュリティポリシーを拡張することでリスクの影響を管理するメカニズムを提供します。

- 攻撃対象領域の縮小：ゼロトラストポリシーを作成し、脆弱なソフトウェアを特定することによって、攻撃対象となる可能性のある領域を縮小し、リスクをできる限り効果的に管理できます。
- 動作の逸脱の特定：異常な動作のイベントを監視して、アラートを生成し、重要なアプリケーションのワークロードにおける予期しないアクティビティで検出された異常なイベントを記録します。



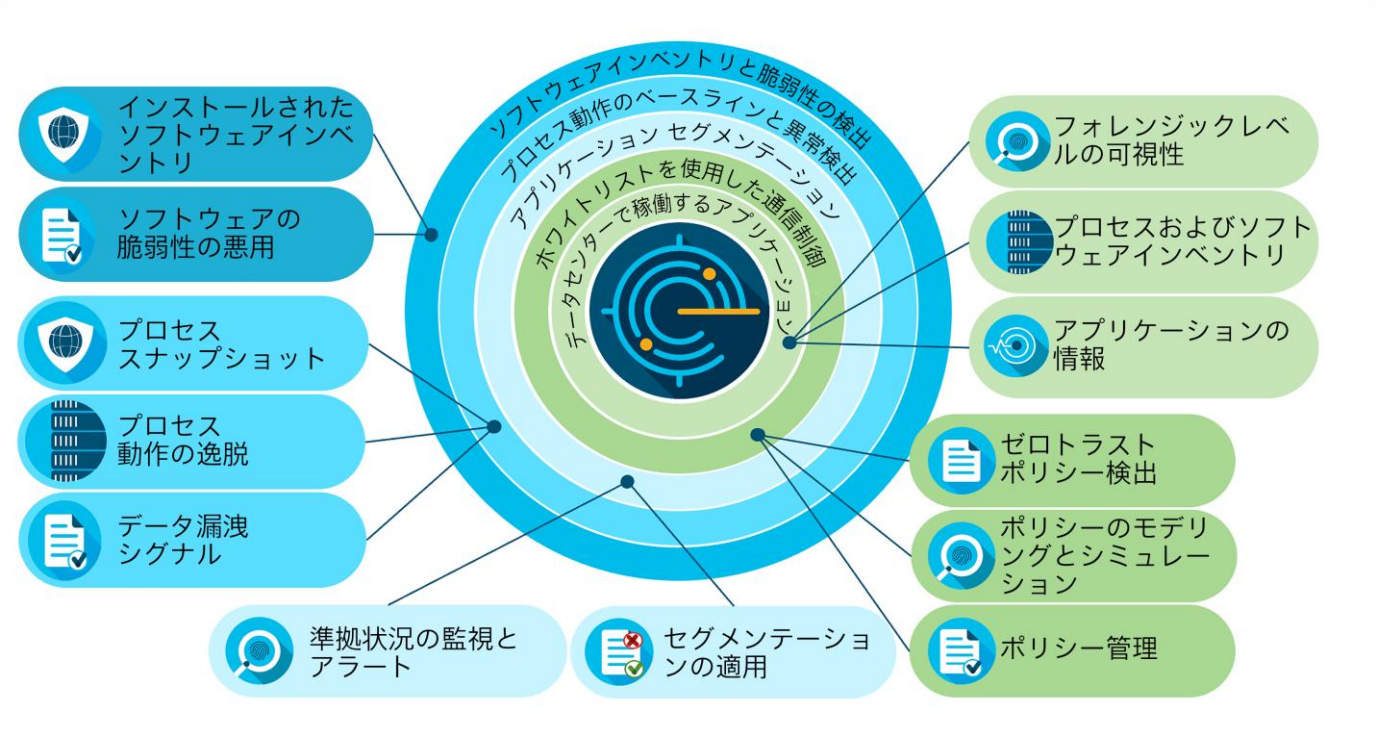
注：今日では、アプリケーションが現代のデータセンターとクラウド インフラストラクチャを促進しています。動的な最新のアプリケーションにより、お客様は俊敏性を損なうことなくアプリケーションのセキュアなインフラストラクチャを構築することに苦労しています。この課題の誘因となっている理由は主に 3 つあります。

1. データセンターまたはクラウド導入環境内には、数百、場合によっては数千のアプリケーションがあり、それぞれが共有サービスやその他のアプリケーションまたはアプリケーションのワークロードに大きく依存しています。実行内容、存在する相互依存関係、およびアプリケーション通信の詳細な計画を理解することが重要です。
2. データセンター内の攻撃対象領域を最小化することが重要です。現在、ほとんどのデータセンター セキュリティ モデルは境界ベースですが、攻撃者はそれらの境界内で自由なラテラルムーブメントが可能です。このような動的なアプリケーションの性質により、ネットワークの境界に実装される現在の静的なセキュリティポリシーでは不十分であり、現代のアプリケーション環境のセキュリティ要件を満たすことができません。ホワイトリストポリシーを使用して、ゼロトラストモデルでセグメント化する必要があります。これは、アプリケーションの動作に基づいて自動化されたホワイトリストポリシーを生成する能力が不足していることが原因です。手動によるポリシー生成アプローチは拡張されず、ポリシーレコードを最新の状態に維持するのはほぼ不可能です。

3. 脆弱性を最小限に抑えたり、攻撃対象領域を縮小するためのタイムリーな対策を実施するために、ワークロードの動作をベースライン化し、疑わしいアクティビティを迅速に特定して、確実に脆弱性を判断する能力が広範囲に展開されていません。

使用例

Cisco Tetration には、重要なセキュリティ使用例のためのターンキーソリューションが用意されています。Tetration の性質により、社内のデータサイエンティストやその他のプログラミング専門家が関連データの実用的な出力を認識するという要件が取り除かれます。これらの機能はインフラストラクチャや場所にとらわれず、主要な運用の使用例とともにセキュリティ使用例の基盤を形成します。



使用例

- **フローの可視性とフォレンジック**：Tetration では、フローを検索し、関心のある内容について確認して、監視されているトラフィックについて、次のような関心のある観測結果を明確に示すことができます。
    - 先月 1 台のマシンからどのようなフローが発生したか。
    - 企業の DNS サーバには送信されなかった、どのような DNS 要求が生成されたか。
    - データの伝送に長時間を要した（漏洩の可能性がある）DNS 要求はどれか。

- 1 時間以上続く HTTP または HTTPS 要求があったかどうか。
- 非 HR ユーザのいずれかが HR データベースにアクセスしているかどうか。
- 管理者が、特権のないネットワークまたはデバイスを使用して重要なサーバにアクセスしているかどうか。

- **アプリケーション情報**：Tetration プラットフォームは豊富なテレメトリを取得し、それを教師なし機械学習と組み合わせてアプリケーション動作の理解を提供します。Tetration は、アプリケーション通信とその依存関係を自動的に検出し、明確に表示できるように設計されています。
- **ポリシー検出**：アプリケーション情報の基盤の上に構築されている Cisco Tetration では、セグメンテーションに必要なゼロトラスト/ホワイトリストポリシーを自動的に生成できます。ポリシーの自動作成は、解決すべき困難で固有の問題ですが、それと同様の課題として、ポリシーまたはそのポリシーに関連する動作の変更を継続的に行う必要もあります。
- **ポリシーのモデリングとシミュレーション**：Tetration にはネイティブのポリシーシミュレーションと影響分析またはモデリングも含まれています。これは、履歴データを使用してモデル化し、検出されたポリシーの適用による影響の種類を示すことができます。同じ分析ツールはリアルタイムデータに対するポリシー分析にも対応し、アクティブなフローが現在のポリシーセットに準拠しているかどうかを示します。このアクティブフローのポリシー分析を設定して、現在のポリシーに準拠していないフローが確認されたときに発信アラートを送信することもできます。
- **アプリケーション セグメンテーションの適用**：Tetration プラットフォームでは、ポリシーの検出によって生成されたポリシーに基づいてアクションを実行できます。このポリシーは、Tetration によって適用することができ、どのような導入においても（オンプレミスまたはクラウドプロパティ）一貫したセグメンテーション方式が使用されます。そのメリットは、セグメンテーションポリシーの適用を各サーバの個々のポリシーセットに分割することができるため、仮想化、ベアメタル、またはコンテナいずれのワークロードであっても大規模で一貫した実装を提供できる点です。このモデルでは、ワークロードが拡大、縮小、または移動してもポリシーをそのまま使用できます。
- **コンプライアンス**：ポリシーが適用されると、プラットフォームはコンプライアンスを継続的に監視します。ポリシーに準拠していないフローが観察された場合は、通知が送信され、プロアクティブなセキュリティ運用が可能になります。
- **フォレンジック**：Tetration はソフトウェアセンサーをワークロードに対して実行し、実行イベントのカーネルイベントモニタを継続的に監視します。プラットフォームは、正常な動作と一致しないイベントを監視します。たとえば、Web サーバで Apache を実行している場合、Apache プロセスでシェルセッションが生成され、ソフトウェアがインストールされてネットワークのスキャンが開始されますが、それは本来通常の動作ではありません。Tetration

では、このタイプのイベントに関するアラートを送信するだけでなく、イベントの前、途中、後に観察された動作も記録できます。

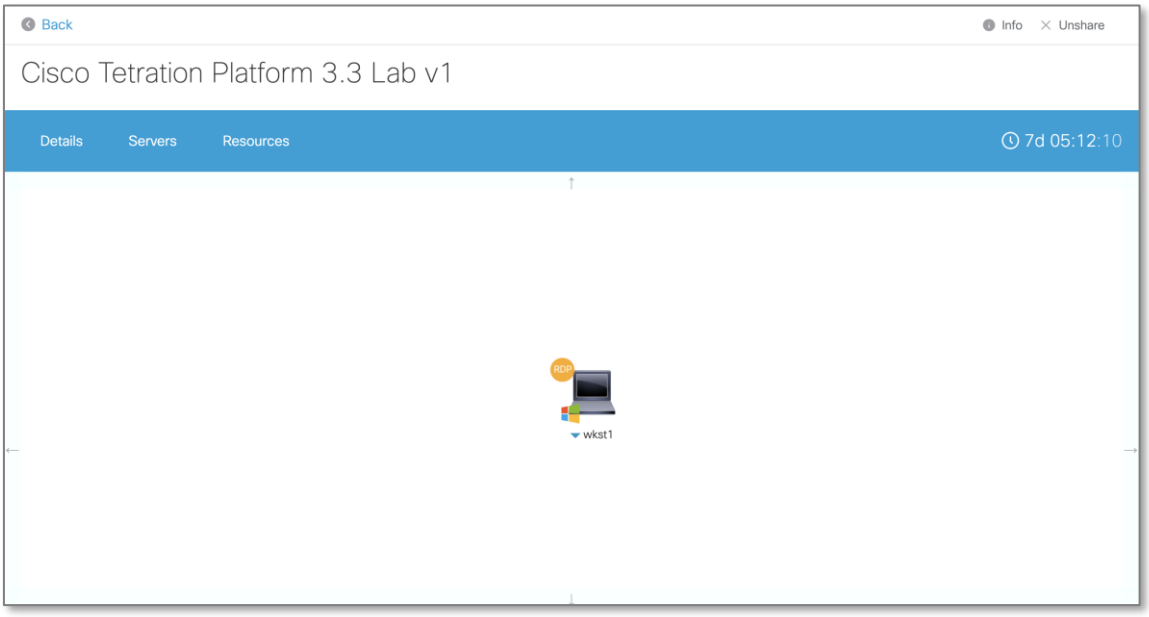
シナリオ 1.　すべての仮想マシンが正しく動作していることの確認

このシナリオでは、次の方法を学習します。

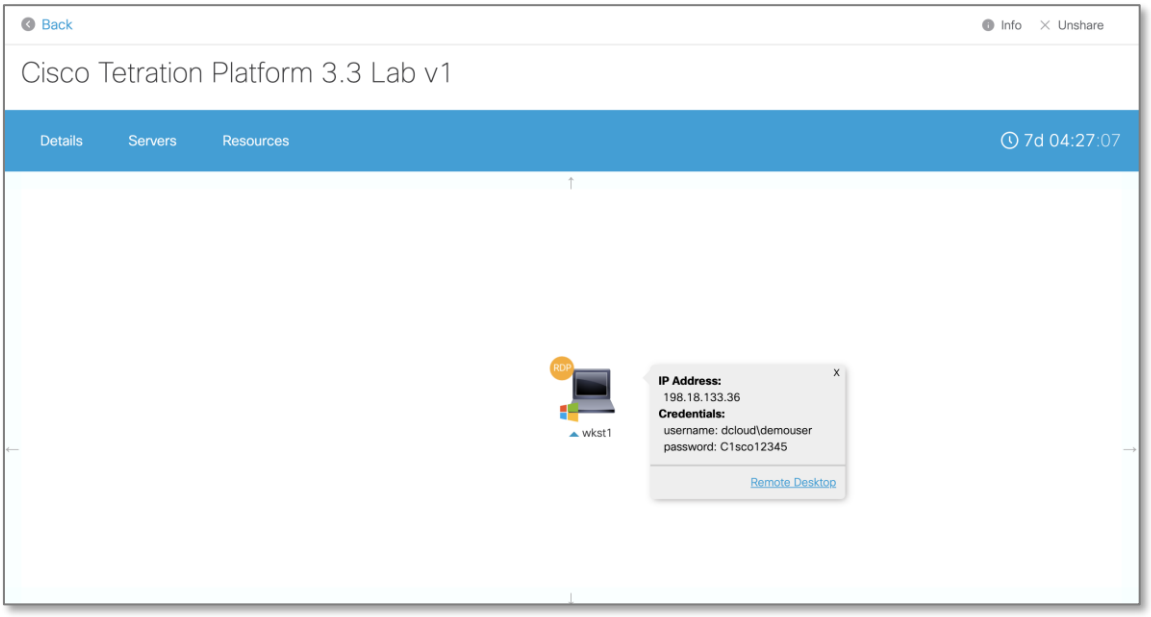
- Tetration の展開にサインインします。
- 各仮想マシンの [State（状態）] が [Powered On（電源オン）] になっていることを確認します。
- 各仮想マシンの [Status（ステータス）] が [Normal（正常）] になっていることを確認します。
- 各仮想マシンが [Running（実行中）] であることを確認します。
- 各仮想マシンに IP **アドレス**が割り当てられていることを確認します。

手順

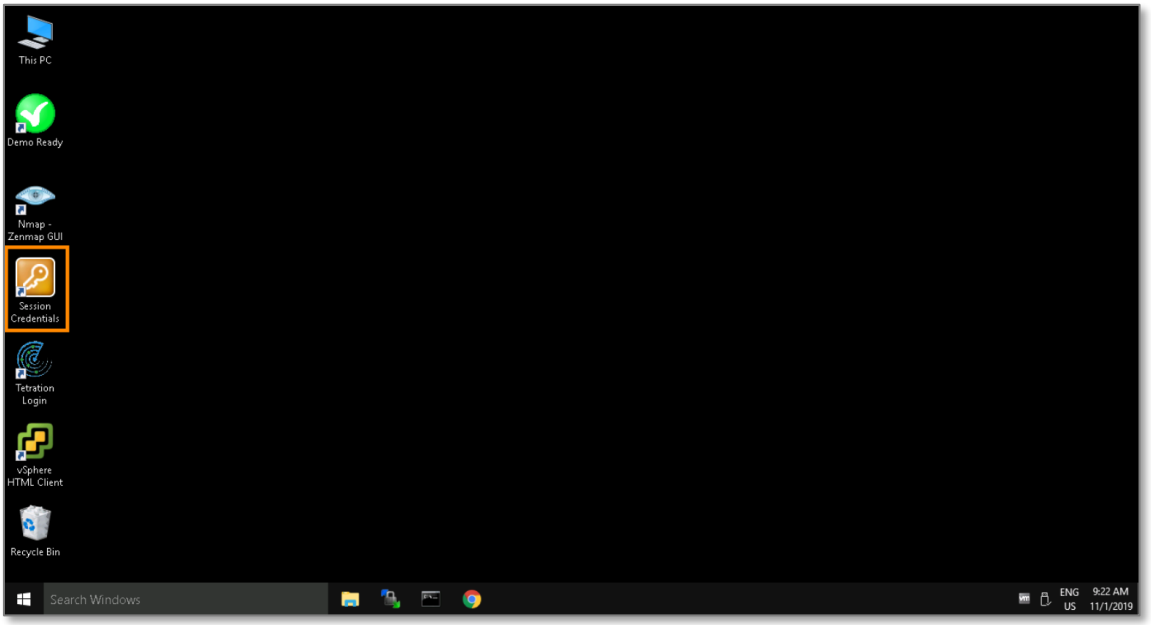
Cisco Tetration Platform 3.3 **ラボ** v1 セッションが実行されている場合は、次の画面が表示されます。



1. ワークステーションアイコンをクリックします。コンテキストに応じたダイアログが開きます。

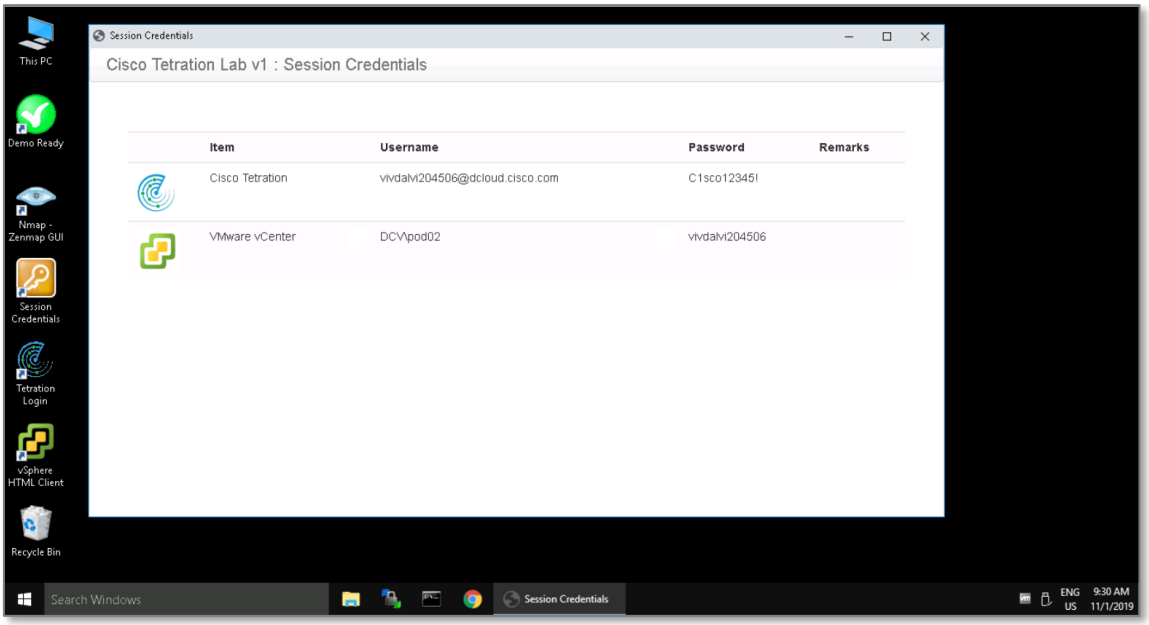


2. [Remote Desktop（リモートデスクトップ）] リンクをクリックすると、新しいブラウザタブが開き、リモートデスクトップ セッション（下）が表示されます。



[セッションクレデンシャル（Session Credentials）] ウィンドウ

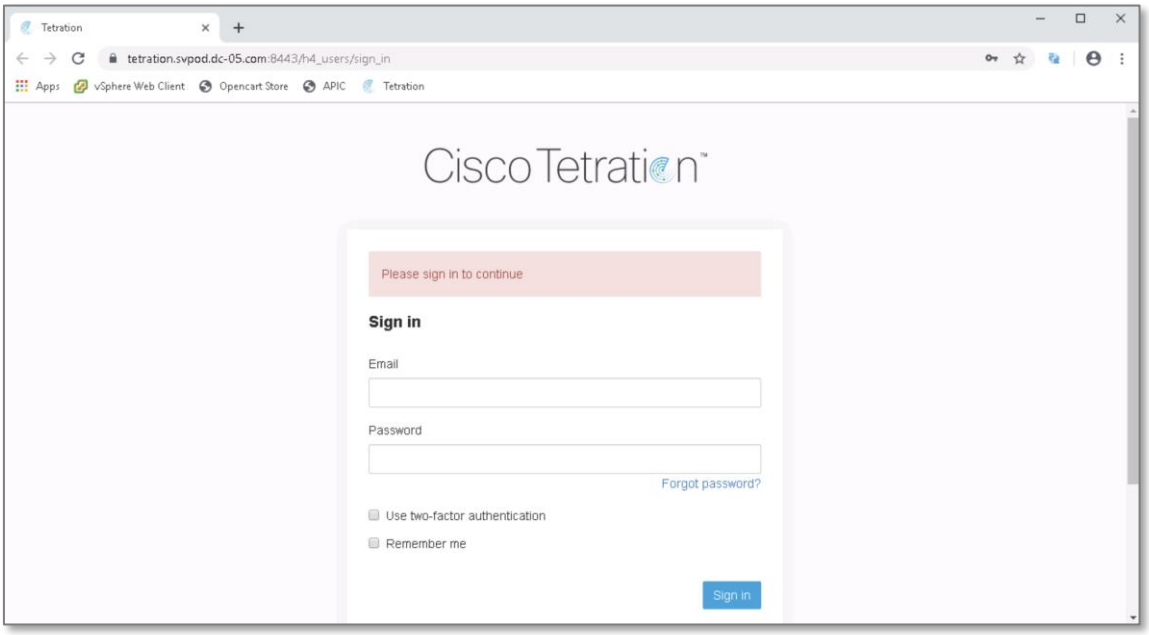
3. （上図で強調表示されている）[Session Credentials（セッションクレデンシャル）] ショートカットをダブルクリックすると、ウィンドウが開きます。



注：[Session Credentials（セッションクレデンシャル）] ウィンドウを開いたままにしておくと、後の手順で必要なユーザクレデンシャルが表示されます。

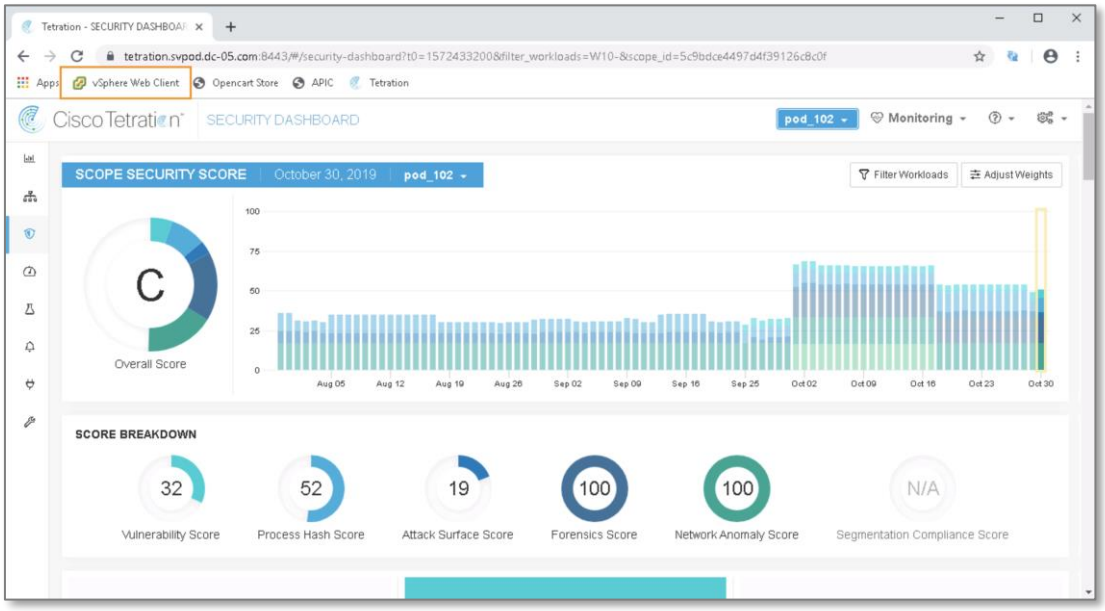
リモート デスクトップ セッションの**タスクバー**で、以下を実行します。

4. Google Chrome アイコンをクリックします。Google Chrome が起動し、Cisco Tetration のサインインダイアログが表示されます。



[Session Credentials（セッションクレデンシャル）] ウィンドウに表示される Cisco Tetration ログイン情報を使用して、以下を実行します。

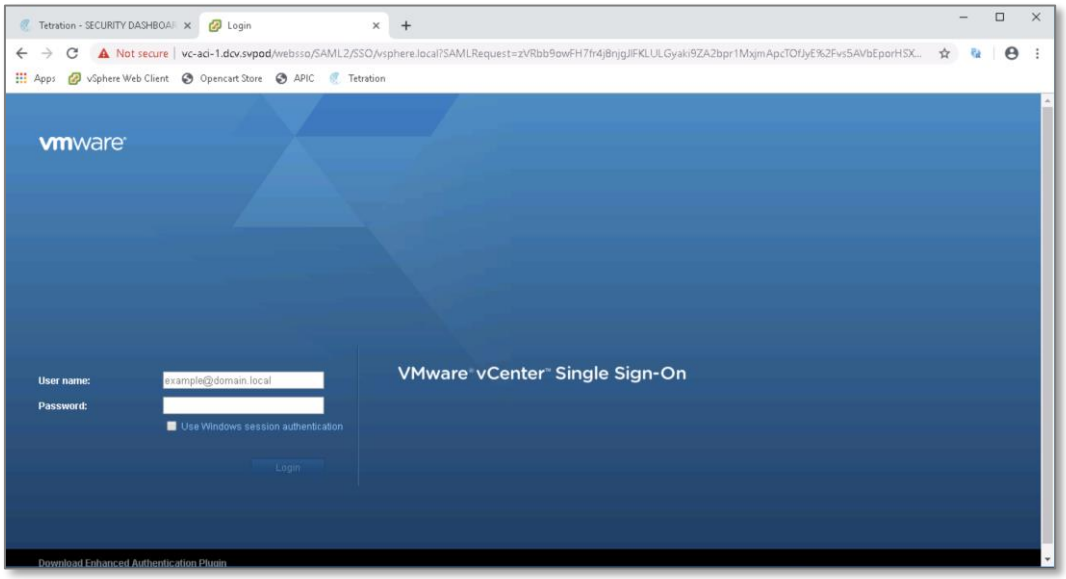
5. Cisco Tetration にサインインします。Cisco Tetration が開き、[SECURITY DASHBOARD（セキュリティダッシュボード）] タブが表示されます。



Google Chrome で以下を実行します。

6. 新しいタブを開きます。

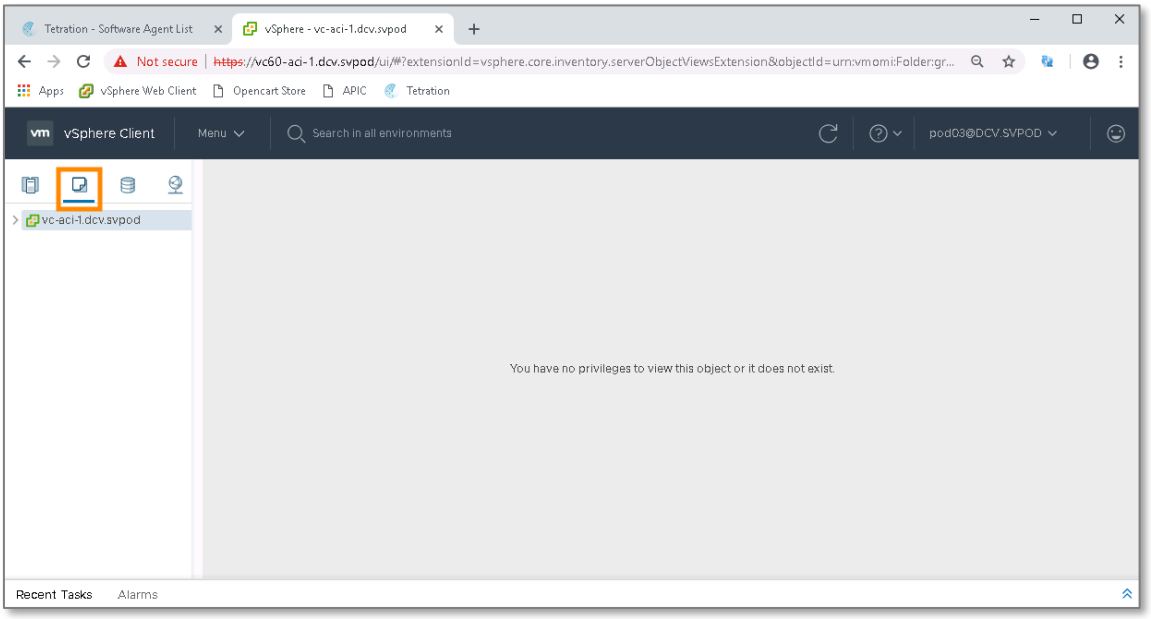
7. （上図で強調表示されている）vSphere Web **クライアント**のブックマークをクリックすると、[vSphere Web Client（vSphere Webクライアント）] ページがロードされます。



[Session Credentials（セッションクレデンシャル）] ウィンドウに表示される VMware vCenter クレデンシャルを使用して、以下を実行します。

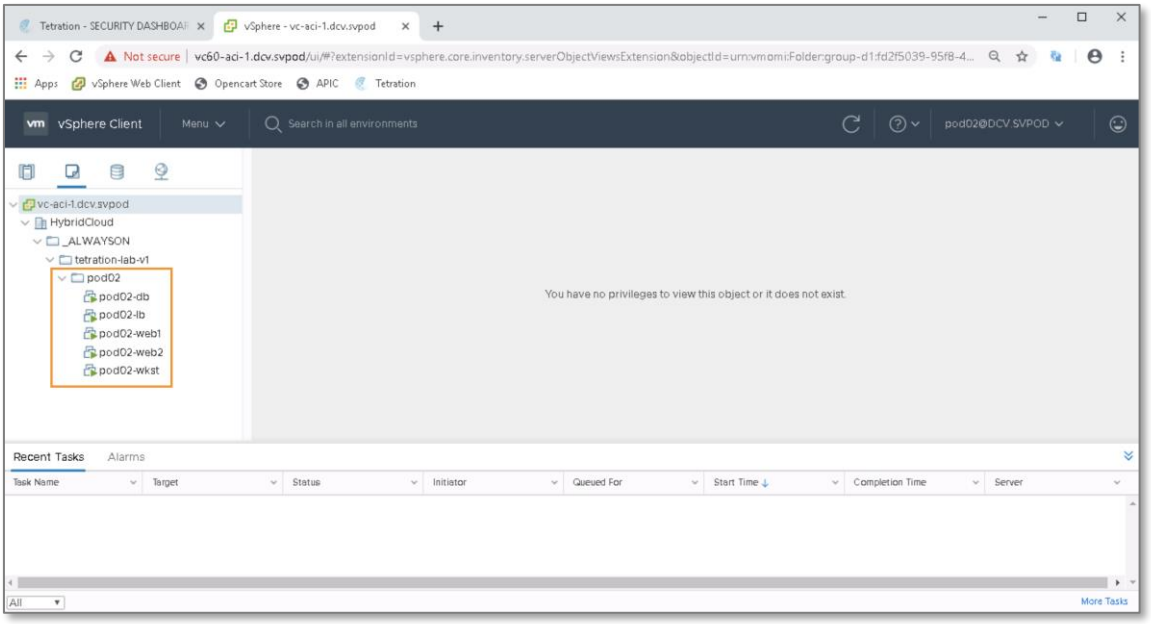
8. vSphere Web **クライアント**にサインインします。vSphere Web **クライアント**が開きます。

9. （下図で強調表示されている）VM とテンプレートがアクティブなタブであることを確認します。



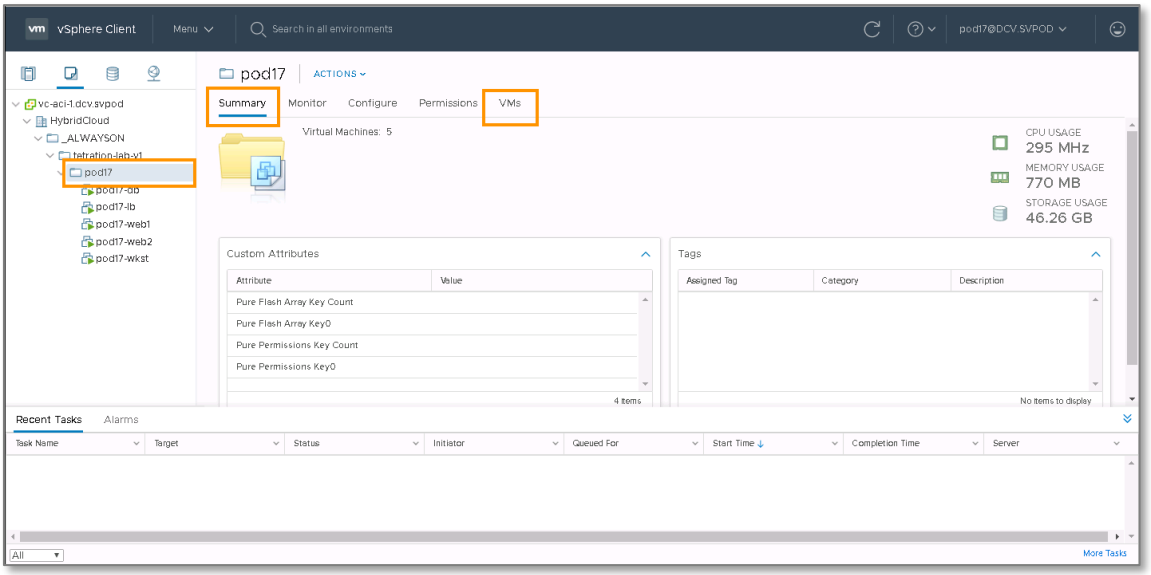
vSphere Web **クライアント**で、以下を実行します。

10. （下図で強調表示されているように）ルートフォルダの下にあるサブ構造を完全に展開します。

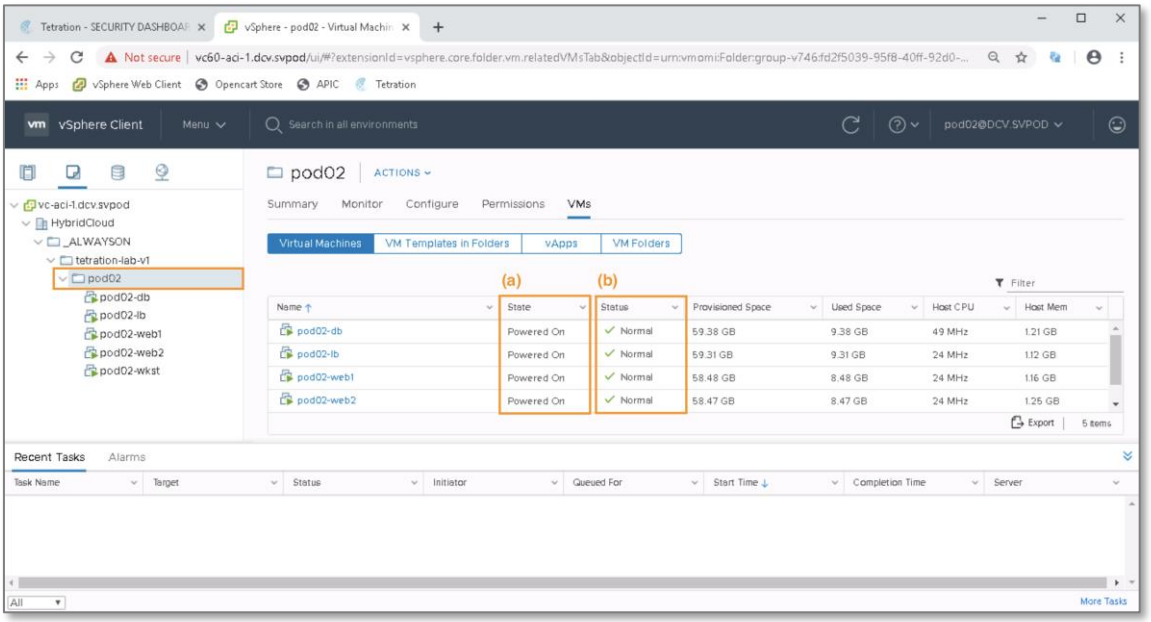


ルートフォルダの下のサブ構造で、以下を実行します。

11. （下図で強調表示されている）*podxx* フォルダをクリックします。[Summary（サマリー）] タブに [podxx] ページが表示されます。



12. （上図で強調表示されている）[VM] タブをクリックすると、[VM] タブが開き、各仮想マシンの動作の詳細が表示されます。

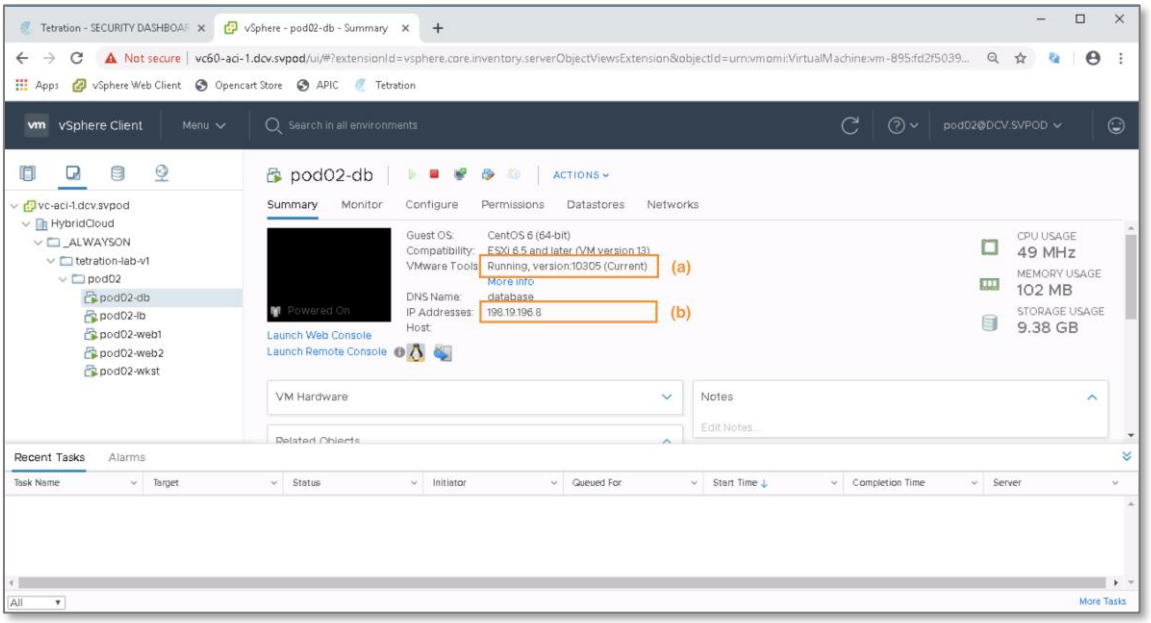


注：（a）各仮想マシンの [状態（State）] は [電源オン（Powered On）] で、（b）各仮想マシンの [ステータス（Status）] は [正常（Normal）] です。

13. [Summary（サマリー）] タブをクリックしタブを開き、「pod」フォルダのサマリーの詳細が表示されます。

「pod」フォルダ内の各仮想マシンで、以下を実行します。

14. (a)それぞれ 1 つずつクリックして、[VMware Tools] が [Running] であること、および(b)[IP アドレス(IP Address)] が割り当てられていることを確認します。



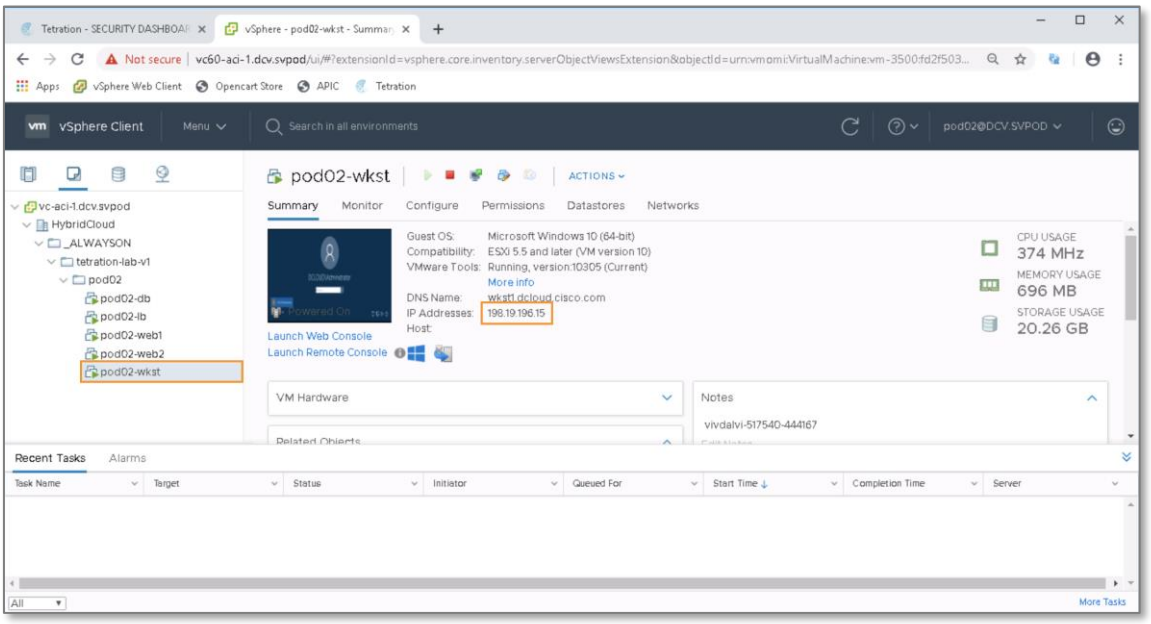
シナリオ 2.　Tetration エージェントのインストール

このシナリオでは、Tetration **エージェント**を**ワークステーション**にインストールする方法を学習します。

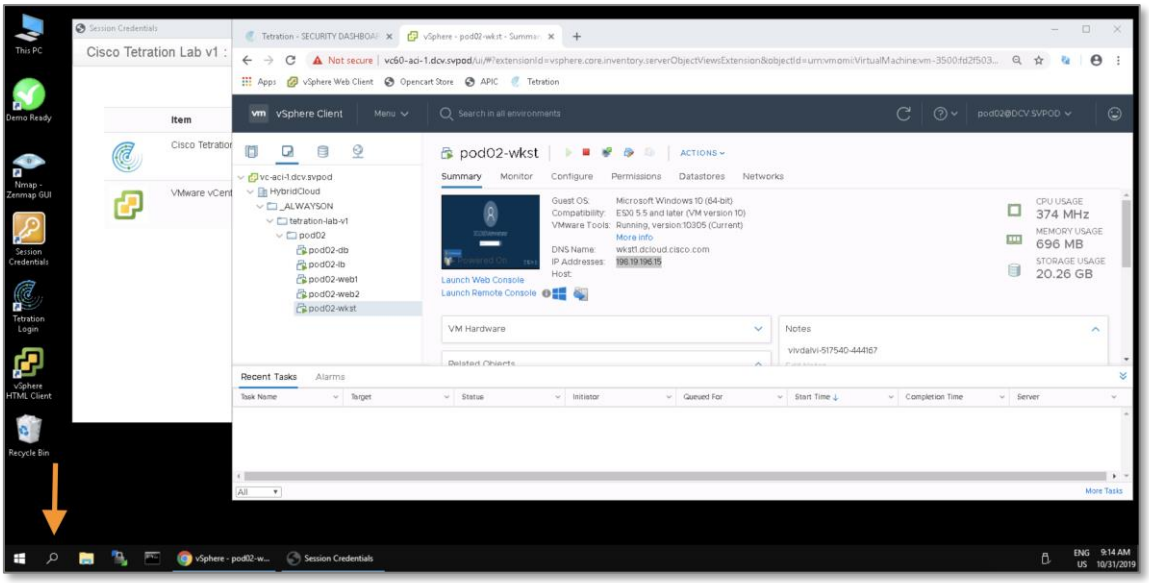
手順

シナリオ 1 すべての仮想マシンが正しく動作の最後の手順からの続きです。

1. （下図で強調表示されている）仮想マシン *podXX-wkst* の IP **アドレス**をコピーします。

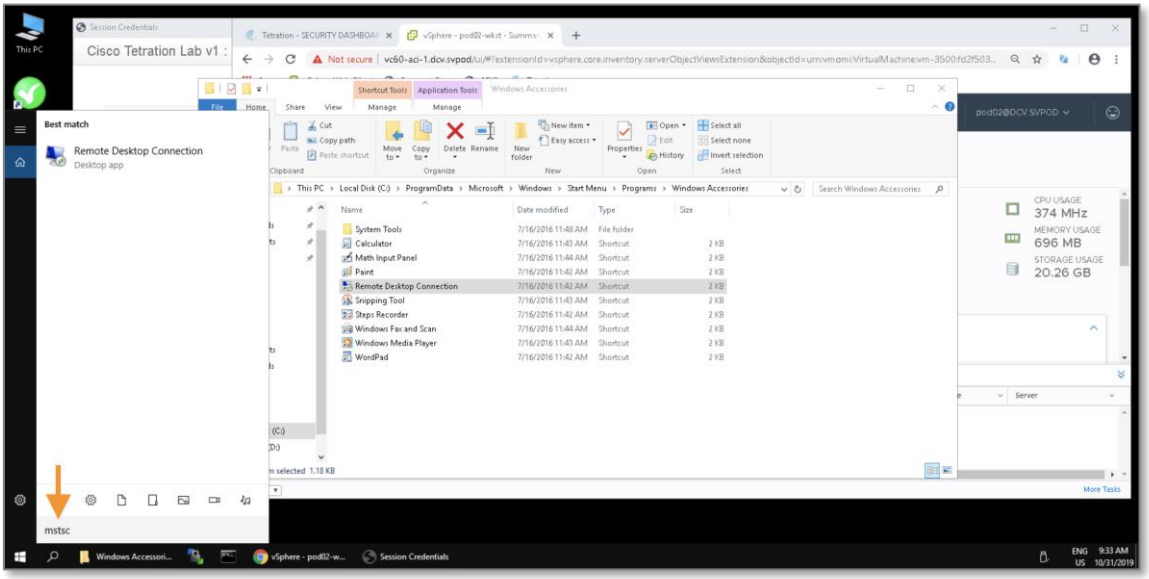


別のリモートデスクトップ接続の開始

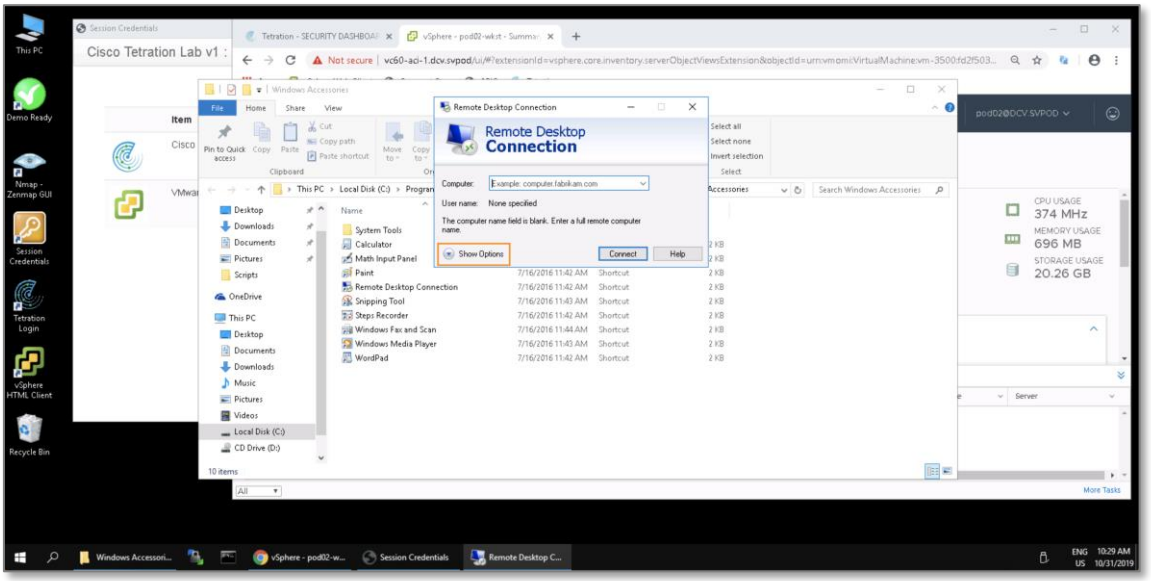


タスクバーで、以下を実行します。

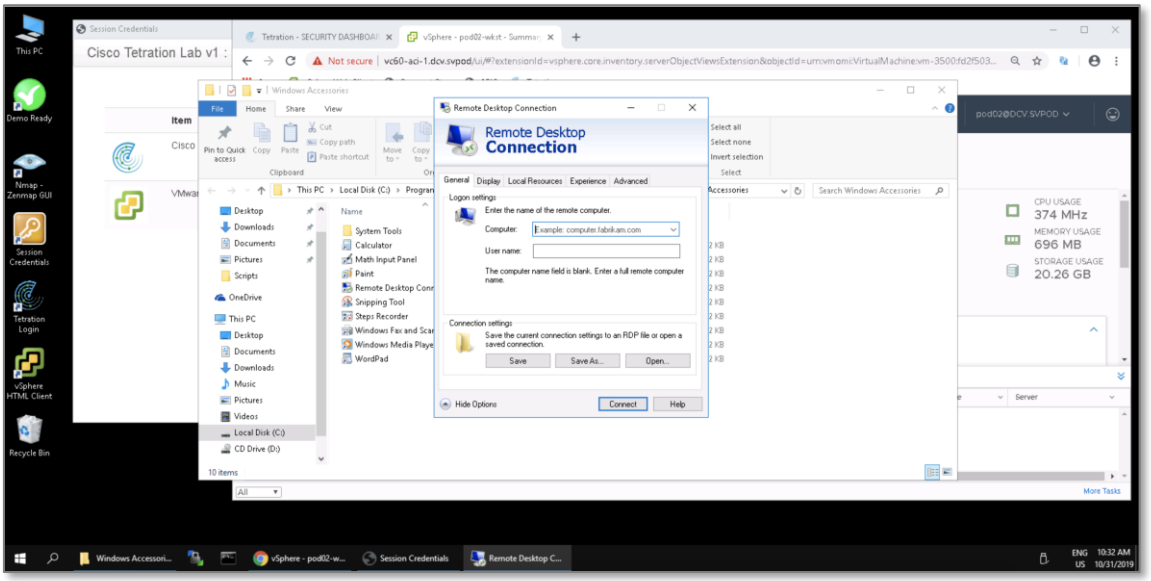
1. （上図で強調表示されている）虫眼鏡アイコンをクリックすると、Windows **検索**ダイアログが開きます。



2. （上図で強調表示されているように）mstsc と入力し、Enter キーを押すと、[Remote Desktop Connection（リモートデスクトップ接続）] ダイアログが開きます。



3. （上図で強調表示されている）[Show Options] ボタンをクリックすると、オプションが表示されます。



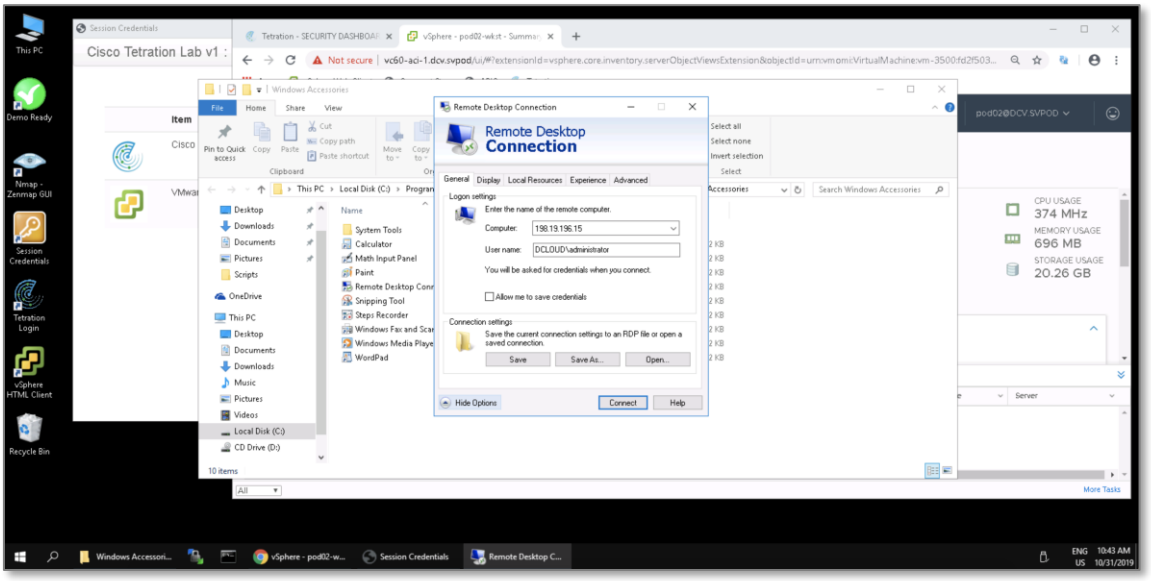
[Computer] フィールドで、以下を実行します。

4. 仮想マシン *podXX-wkst* の IP **アドレス**を貼り付けます。

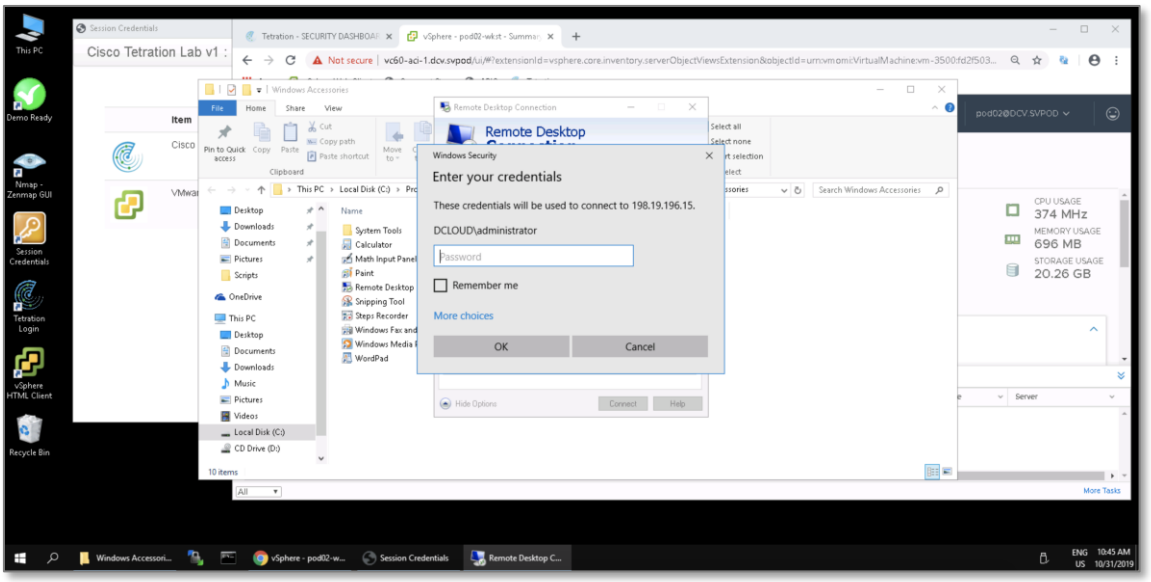
[User name] フィールドで、以下を実行します。

5. DCLOUD\administrator と入力します。

※注意：ユーザ名は demouser ではありません。ここで正しく DCLOUD\administrator として接続しなければ、この後の作業ができませんので注意してください。



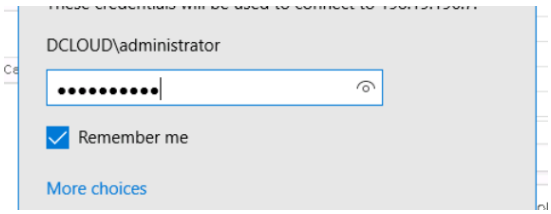
6. [Connect] ボタンをクリックします。



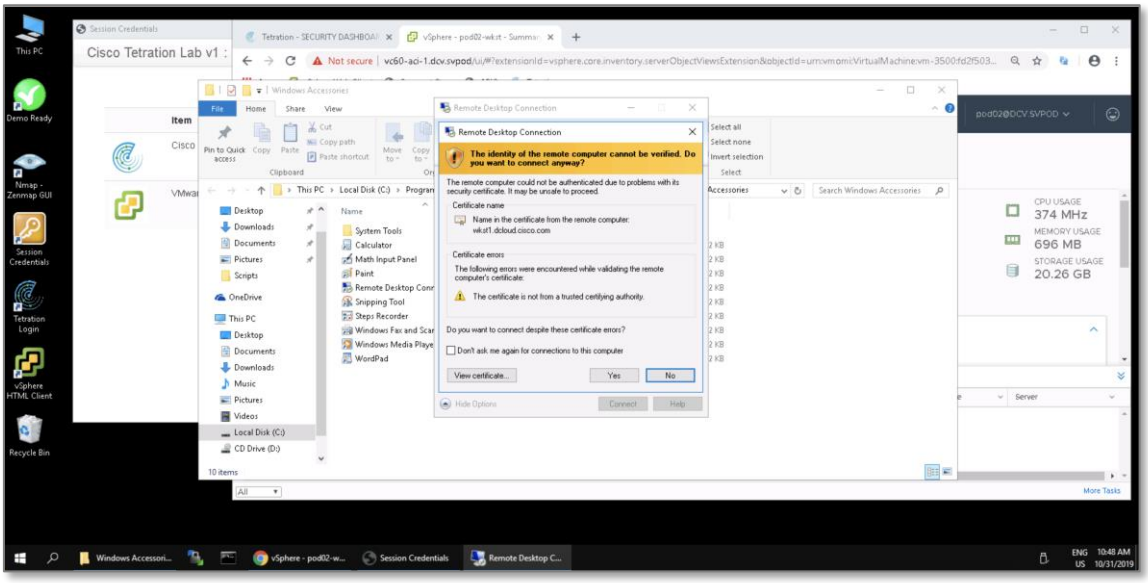
[Password] フィールドで以下を実行します。

7. C1sco12345 とパスワードを入力します。

8. [Remember me] チェックボックスをオンにします。



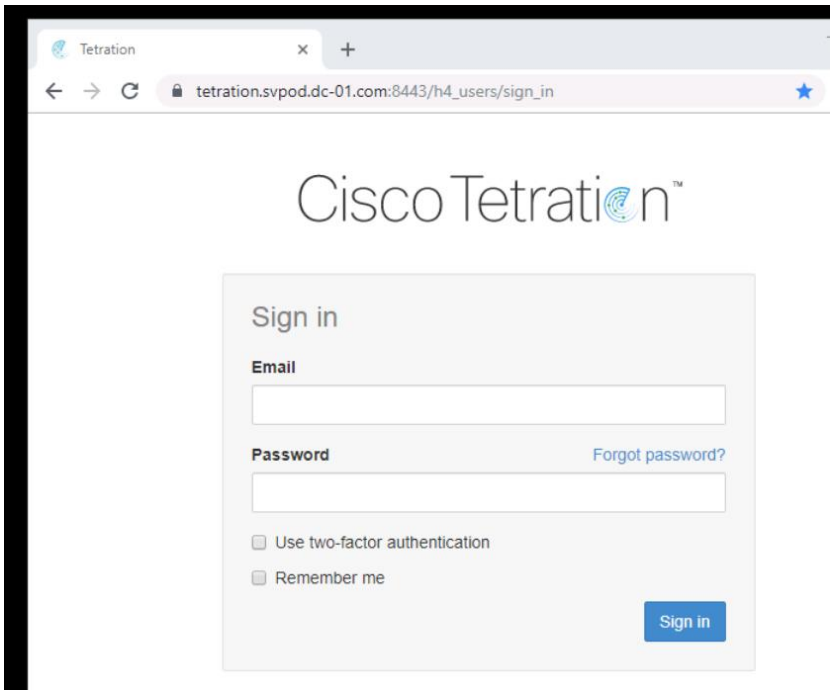
9. [OK] ボタンをクリックすると、「The identity of the remote computer cannot be verified」という通知が表示されます。



10. [Yes] ボタンをクリックします。[Remote Desktop Connection] ウィンドウが開きます。

[Remote Desktop Connection] の**タスクバー**で、以下を実行します。

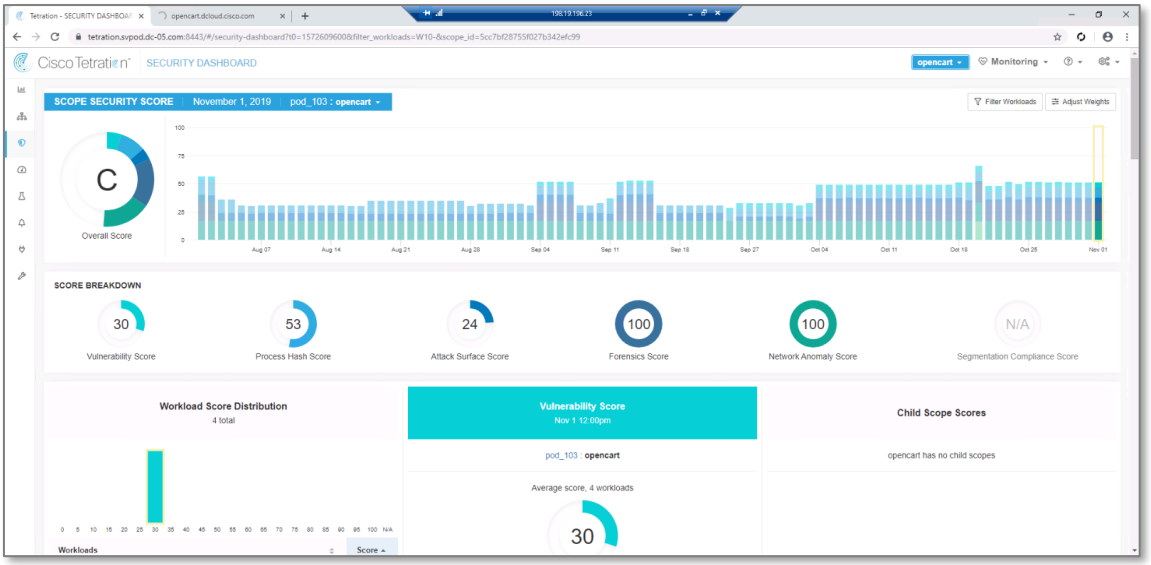
1. Google Chrome アイコンをクリックします。Google Chrome が開き二つのタブ（[Tetration]と[Your Store]）が開きます。※ポッドによってはタブが開かずブックマークに [Tetration] と [Opencart]が表示される環境となっている場合があります。
2. [Tetration]のブックマークボタンをクリックし Tetration のログイン画面を表示します。



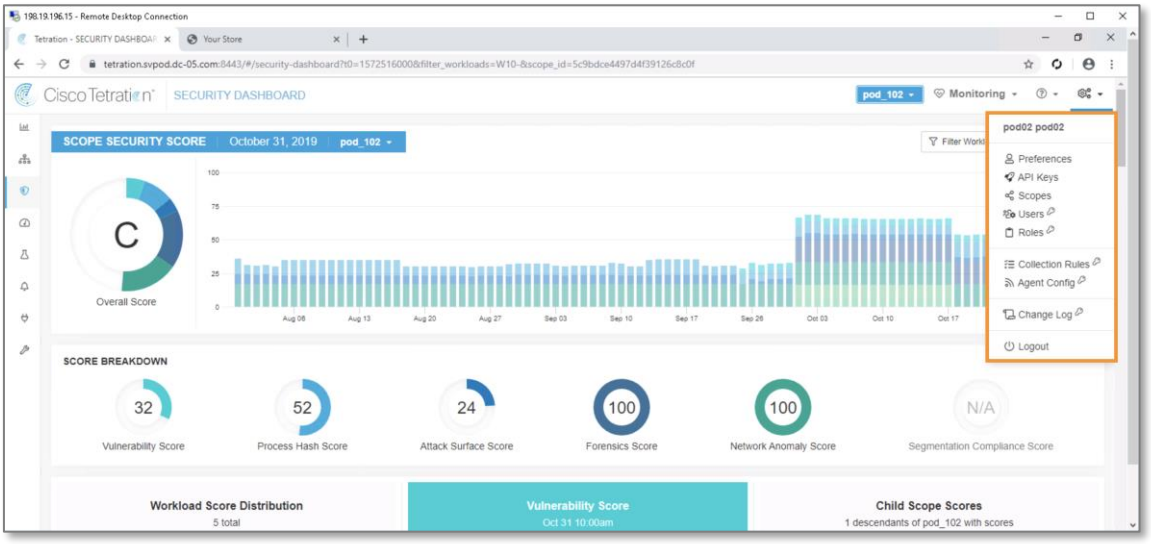
3. リモートデスクトップ接続元である方の wkst1 のデスクトップにある 

[Session Credentials（セッションクレデンシャル）] ウィンドウを開きます。

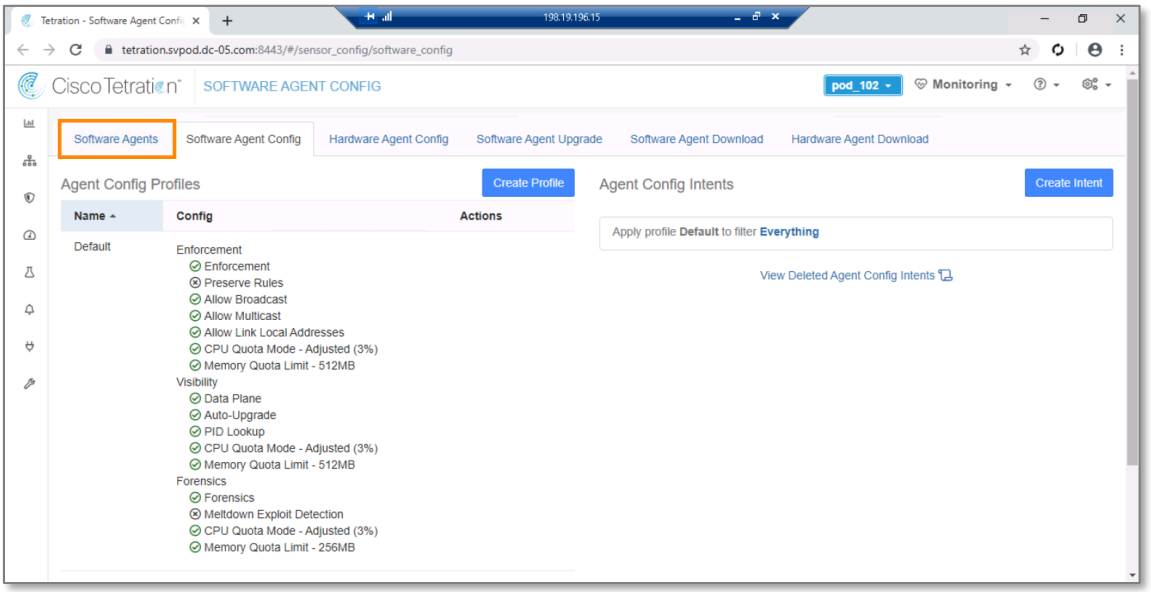
4. 表示される Tetration クレデンシャルを使用して、Tetration にサインインします。— Tetration が開き、[SECURITY DASHBOARD] タブが表示されます。



5. 画面右上の  歯車 マークをクリックして下さい。(下図で強調表示されているように)[Settings] メニューが開きます。

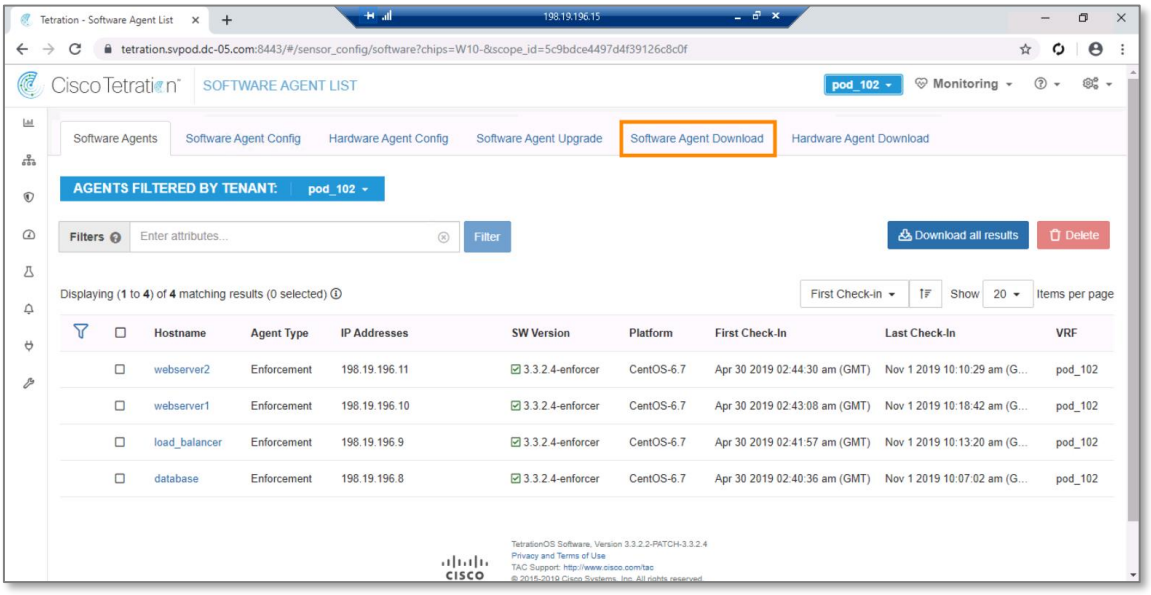


6. [Agent Config（エージェント設定）] オプションをクリックします。[Software Agent Config（ソフトウェアエージェント設定）] タブが開きます。

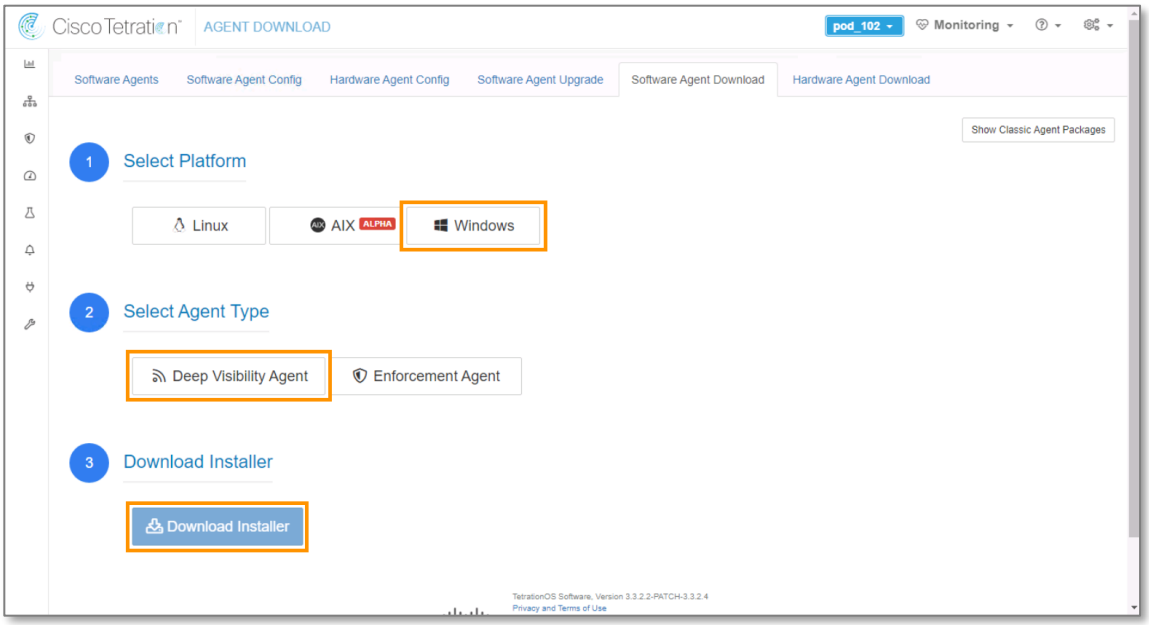


7. （上図で強調表示されているように）[Software Agent] タブをクリックします。

注：ここで表示されるエージェントのリストに、Hostname が wkst1 である仮想マシンがリストされていないことを確認してください。wkst1(今操作しているこのマシン)にこの時点ではソフトウェアエージェントがインストールされていないためです。



8. （上図で強調表示されている）[Software Agent Download] タブをクリックします.。

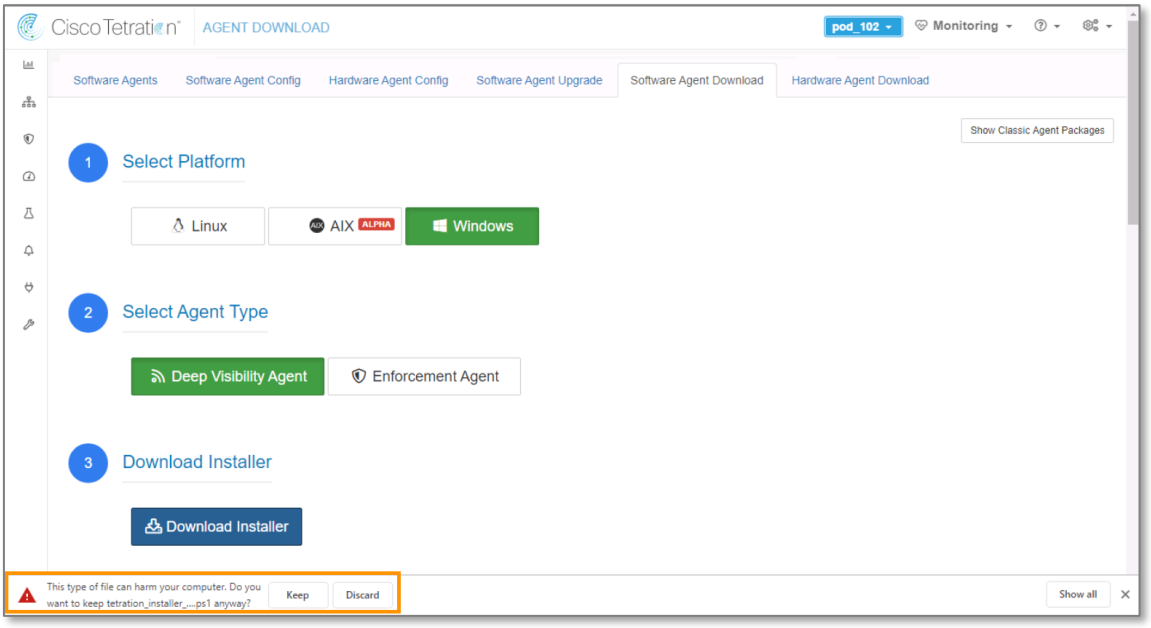


9. [Software Agent Download] タブで、以下を実行します。

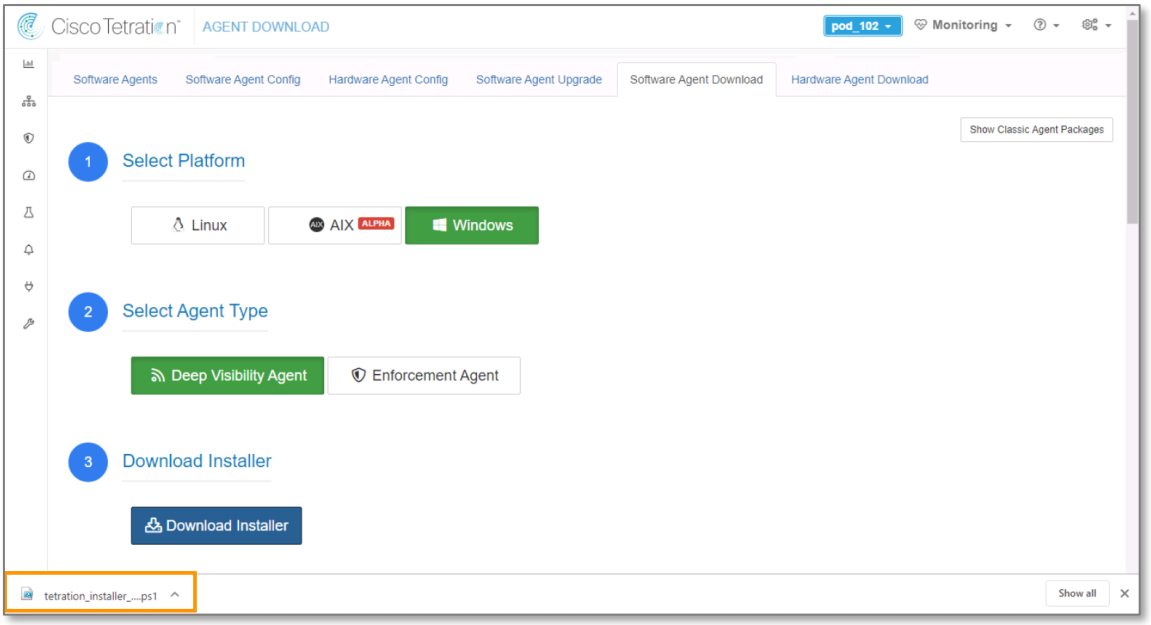
10. （上図で強調表示されている）[Windows] ボタンをクリックします。

11. （上図で強調表示されている）[Deep Visibility Agent] ボタンをクリックします。

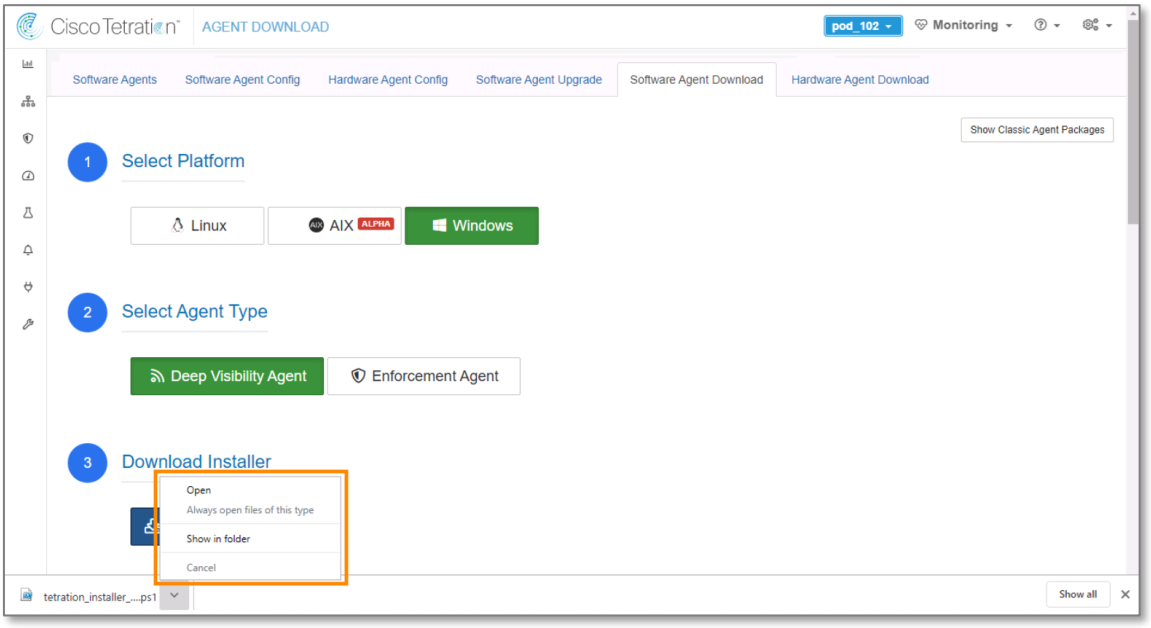
12. （上図で強調表示されている）[Download Installer] ボタンをクリックすると、Google Chrome にインストーラがダウンロードされ、（下図で強調表示されているように）このタイプのファイルの潜在的な危険性について警告が表示されます。



13. [Keep] ボタンをクリックすると、ファイルがダウンロード保存されます。

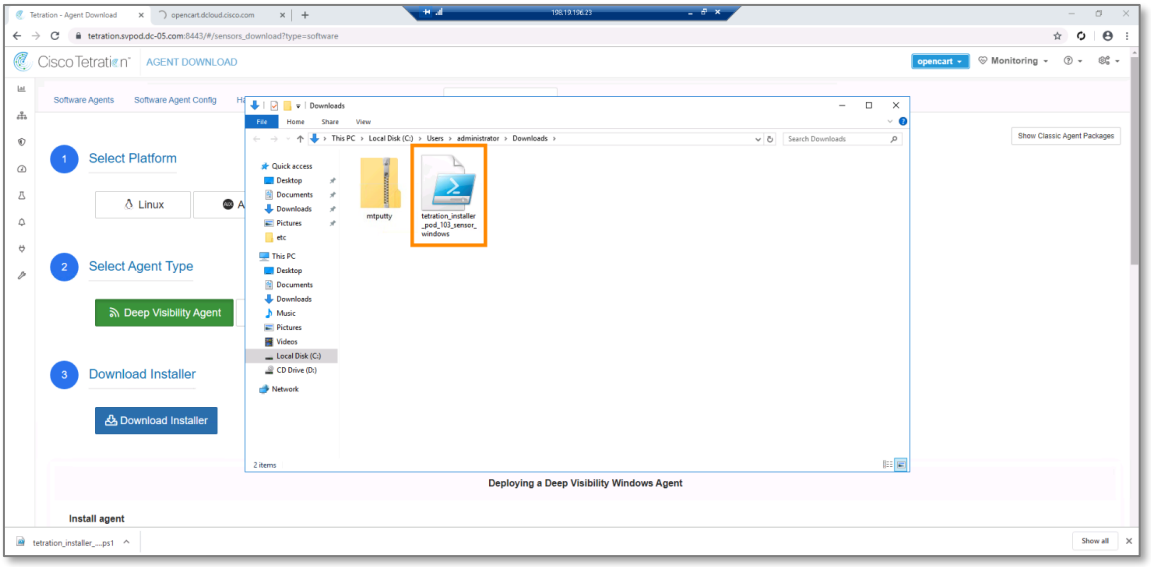


14. （上図で強調表示されている）ダウンロード通知 の上矢印をクリックすると、（下図で強調表示されている）コンテキストメニューが開きます。

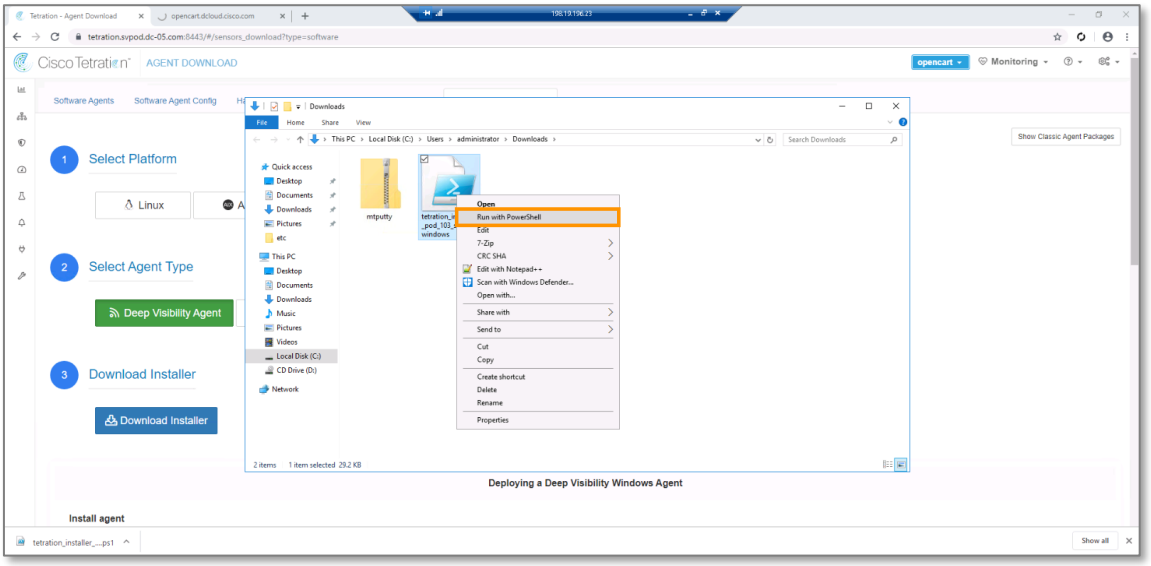


コンテキストメニューで、以下を実行します。

15. [Show in folder] オプションをクリックすると、Administrator > Downloads フォルダが開き、保存した（下図で強調表示されている）インストーラスクリプトが表示されます。

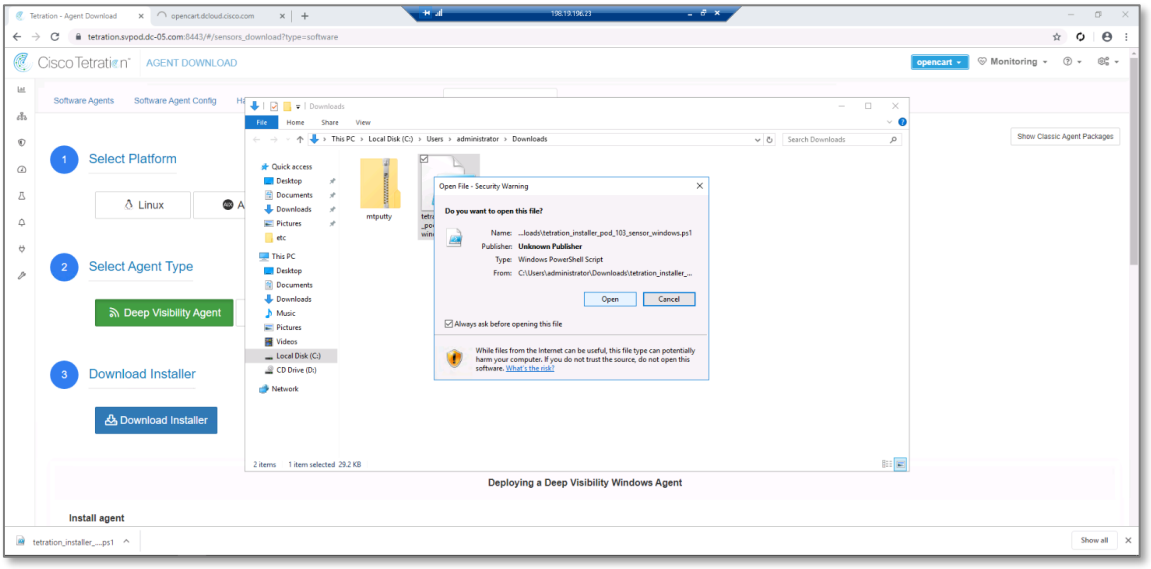


16. インストーラスクリプトを右クリックすると、コンテキストメニューが開きます。



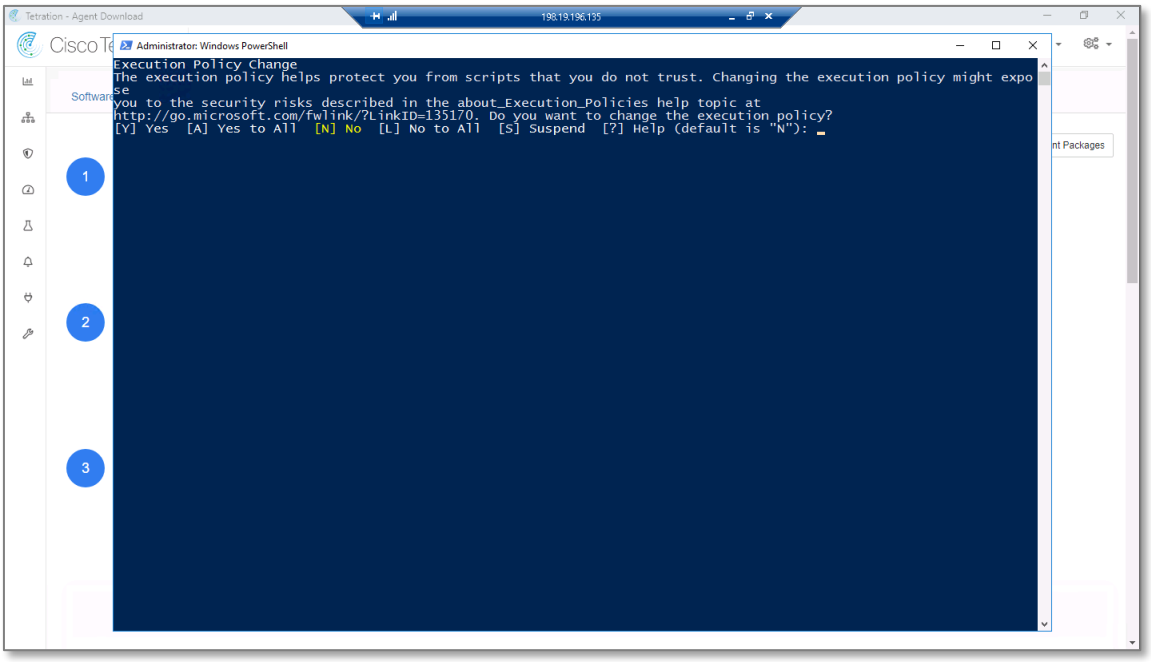
コンテキストメニューで、以下を実行します。

17. （上図で強調表示されているように）[Run with PowerShell] オプションをクリックし PowerShell で実行します。[ファイルを開く - セキュリティ警告（Open File – Security Warning）] ダイアログが開きます。



18. [Open] ボタンをクリックします。[Windows PowerShell] ウィンドウが開き、インストーラスクリプトが実行されます。

インストーラスクリプトで、**実行ポリシー**を変更するかどうかの確認が行われます。



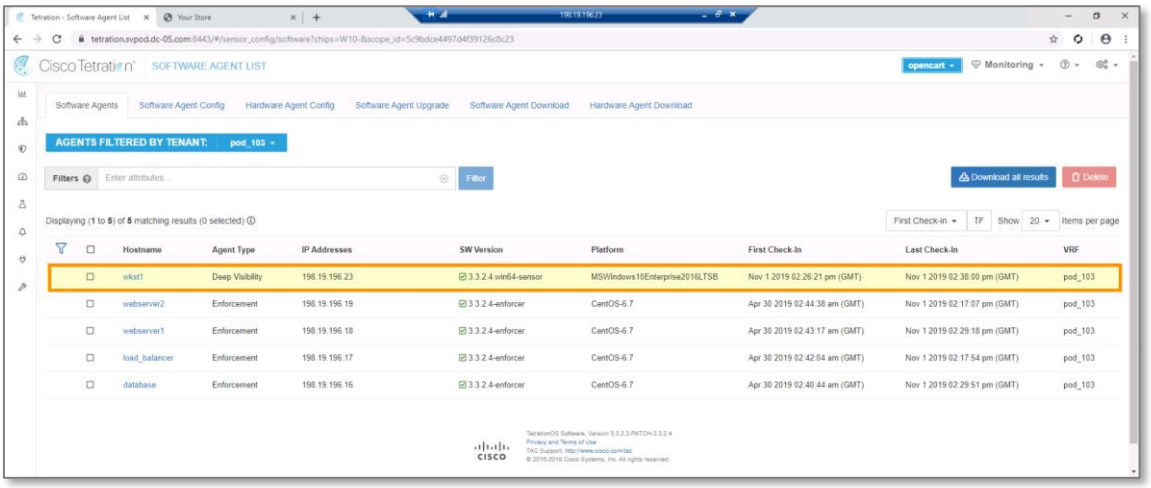
19. 「y」または「Y」を押します。

20. Enter キーを押します。インストーラスクリプトが続行されます。

インストーラスクリプトが完了すると、[Windows PowerShell] ウィンドウが閉じます。

21. [Software Agent] タブをクリックします。次の内容が表示されます。

- wkst1 がエージェントとともに仮想マシンのリストに追加された。
- wkst1 には、[Deep Visibility] の [Agent Type（エージェントタイプ）] を持つエージェントがインストールされています。



シナリオ 3.　インベントリ、フィルタ、およびアプリケーションの依存関係マップの設定

このセクションの目的は、インベントリファイルを Tetration クラスタにインポートして注釈を設定する方法を説明することです。

インベントリのアップロード

ユーザアノテーション(ユーザ注釈)は、Tetration がプラットフォームの内外でさらに多くの情報を取得するために最も有用なマークアップツールです。アノテーション(注釈)を使って、観察および報告されるフローデータに重要なコンテキストを追加できます。環境に関する追加情報を提供できるほぼすべてのものがアノテーション(注釈)のソースになります。ユーザアノテーションの基本の方法は、IP アドレスのテーブルとそれらのアドレスに関するコンテキスト情報を組み合わせた CSV ファイルをアップロードすることです。有用なアノテーション（注釈）の一例として、アプリケーションのオーナーがあります。フローのフォレンジックを確認したユーザが質問をする必要がある場合に、フローの観測結果に直接埋め込まれたアプリケーションのオーナーのレコードを利用できます。

次に、ユーザアノテーションファイルの例を示します。

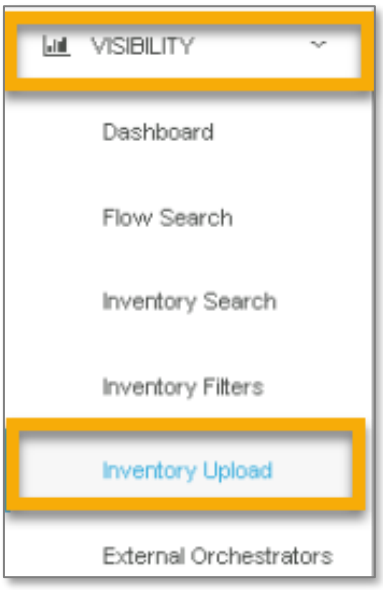
IP アドレス	場所	FQDN	ネットワーク	ゾーン	オーナー	ネットワーク接続	脅威	アプリケーション	機能
172.16.1.90	オースティン	dns.crisco.com	オースティン インフラストラクチャ	共有サービス	Brandon（内線 1234）	aus1-leaf1 | aus1-leaf2	False	DNS LDAP NTP ActDir	共有インフラ
168.92.33.222		z.tac.com	TAC 外部	パートナー イントラネット	TAC, Inc.（800-553-2447）	vpn1	True	サポートのスタッフ配置	
10.101.10.0/24	デンバー		デンバー アクセス	デンバー キャンパス	Sally（内線 4321）		False		ユーザアクセス
192.168.99.12	デンバー	a.crisco.com	デンバー PCI Prod	PCI	James（内線 9876）	den2-leaf7 | den2-leaf8	False	B2B – Visa	クレジット カード トランザクション

その他の例として、持続的標的型攻撃のソースのリストや、デバイスが接続されている機器のタイプ、または物理的な場所などがあります。

上記は、静的なアノテーション（注釈）のユーザアップロードの例です Tetration の新しいバージョンでは、他にもコンテキスト情報を動的に Tetration クラスタにプッシュする方法があります。Tetration プラットフォームに動的に組み込まれた統合により、AWS、VMW vCenter、Kubernetes、Infoblox、DNS、ロードバランサー（F5、Citrix、AVI）などの外部システムから注釈が自動的にプルされます。また、シスコの Identity Services Engine、Cisco AnyConnect、ASA、Cisco Meraki との統合など、コンテキストを収集する他の方法もあります。

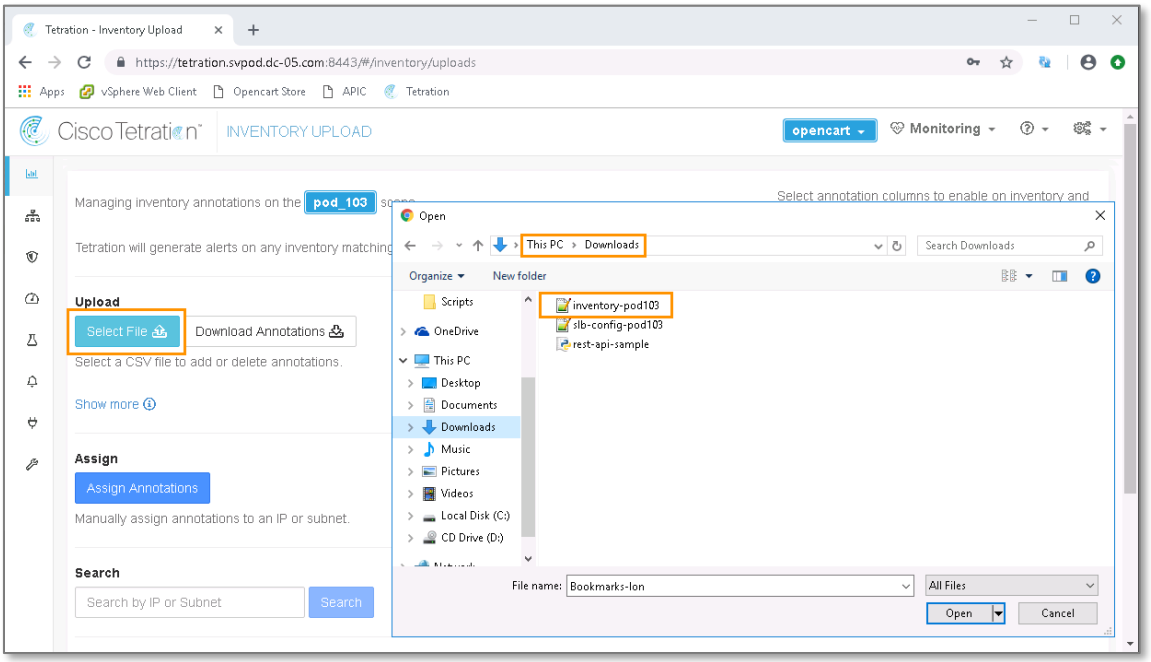
手順

1. プライマリデスクトップ(前のシナリオでエージェントをインストールしたwkst1 ではない)に戻ります。[Tetration] タブのメニューで、[VISIBILITY（可視性）] > [Inventory Upload] を選択します。



2. [Select File] をクリックしてインベントリファイルをアップロードします。

3. Downloads フォルダを参照します。



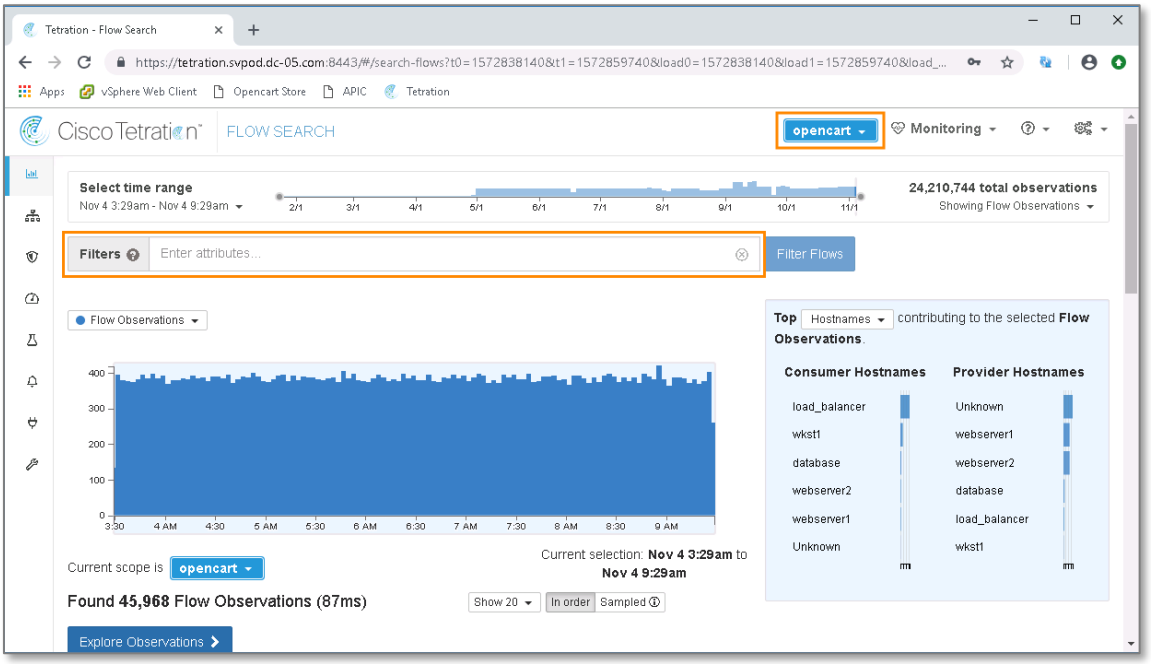
4. inventory-podxxx.csv ファイルをダブルクリックすると、[Upload] ダイアログが開きます。

5. [Add（追加）] が選択されていることを確認します。

6. [Upload] をクリックすると、アップロードが完了したことがポップアップで確認されます。

サイドメニューで、以下を実行します。

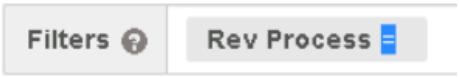
7. [VISIBILITY] > [Flow Search] を選択すると、フロー検索のタブが開きます。



（上図で強調表示されている）[Scope Selector] で、以下を実行します。

8. pod_xxx が選択されていることを確認します。

（上図で強調表示されている）[Filters] フィールドで、以下を実行します。

9. 「Rev Process」と入力し 

“=”記号が自動補完されたらバックスペースでこれを削除し、そのまま続けて「*contains* http」と入力します。 

”http”が含まれるプロセス名の受信プロセスを持つフローが表示されます。

10. [フローのフィルタ（Filter Flow）] ボタンをクリックします。

注：”Filters”の横の?マークで表示されるフィルタ可能なプロパティのリストの中で* 付きで示されているフィールドは、インベントリファイルとしてアップロードされるユーザアノテーションです。これらのフィルタを使って、アプリケーション名、ステージ（「プロダクション環境」や「開発環境」等）、またはユーザがインベントリファイルに含めたその他のパラメータでフローを絞り込むことができます。

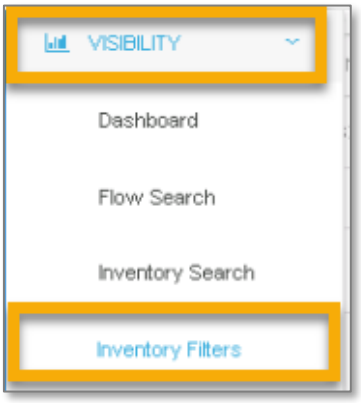
* Provider Application-Name
* Provider Application-Stage
* Provider Application-Type
* Provider Datacenter
* Provider Department
* Provider OS-Type
* Provider OS-Version
* Provider Owner
* Provider Role
* Provider Sensor-Type
* Provider TA bogon ipv4
* Provider TA zeus
* Provider VRF
* Consumer Application-Name
* Consumer Application-Stage
* Consumer Application-Type
* Consumer Datacenter
* Consumer Department
* Consumer OS-Type
* Consumer OS-Version
* Consumer Owner
* Consumer Role
* Consumer Sensor-Type
* Consumer TA bogon ipv4
* Consumer TA zeus
* Consumer VRF

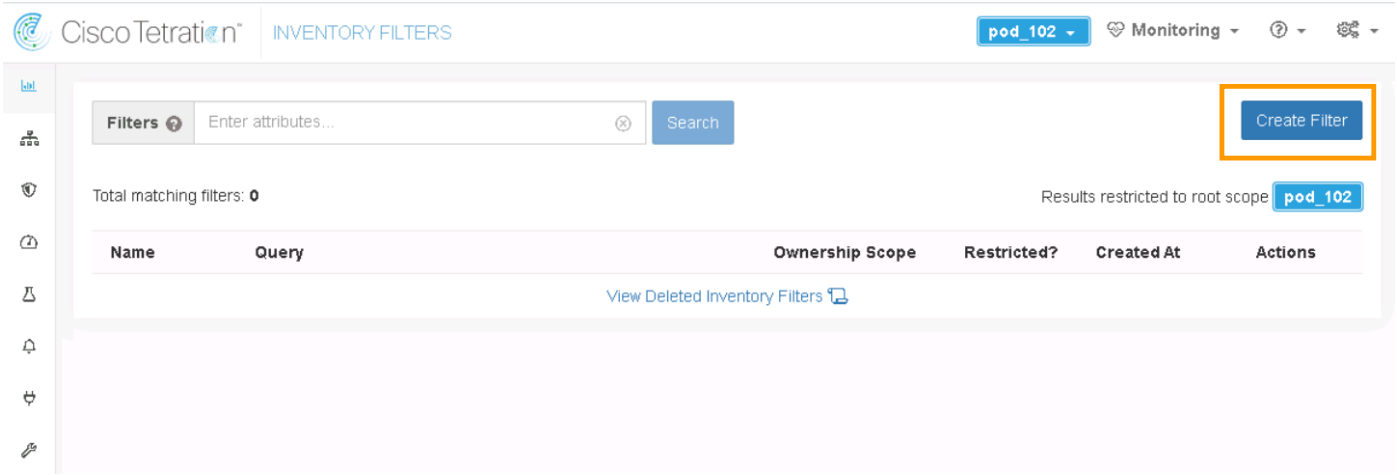
インベントリフィルタの作成

このセクションの目的は、ラボ環境で事前設定されている OpenCart アプリケーションからフローを分離するフィルタを作成することです。

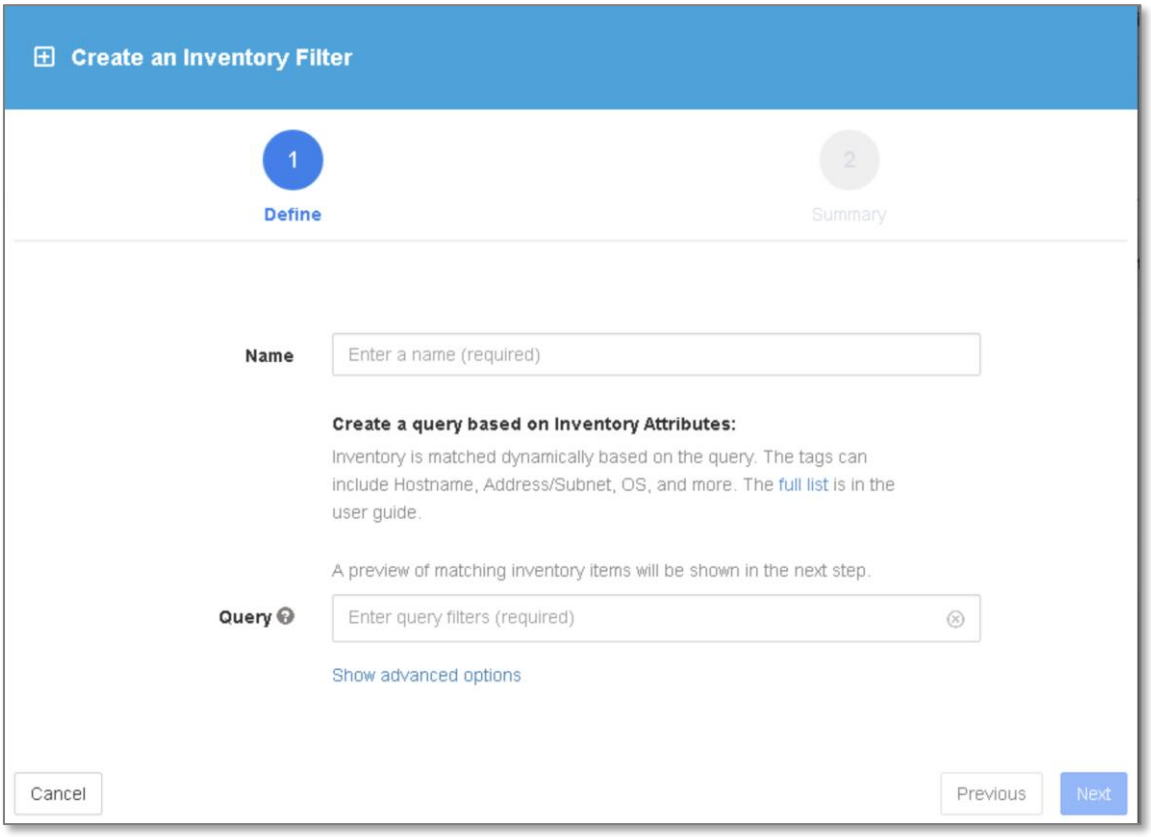
新しいフィルタを作成するには、サイドメニューで、以下を実行します。

1. [VISIBILITY] > [Inventory Filters] を選択します。





2. （上図で強調表示されている）[Create Filter] ボタンをクリックします。[Create an Inventory Filter] ダイアログが開きます。



[Name] フィールドで以下を実行します。

3. *Pod_XXX_servers* を入力します（XXX はポッド番号に一致します）。

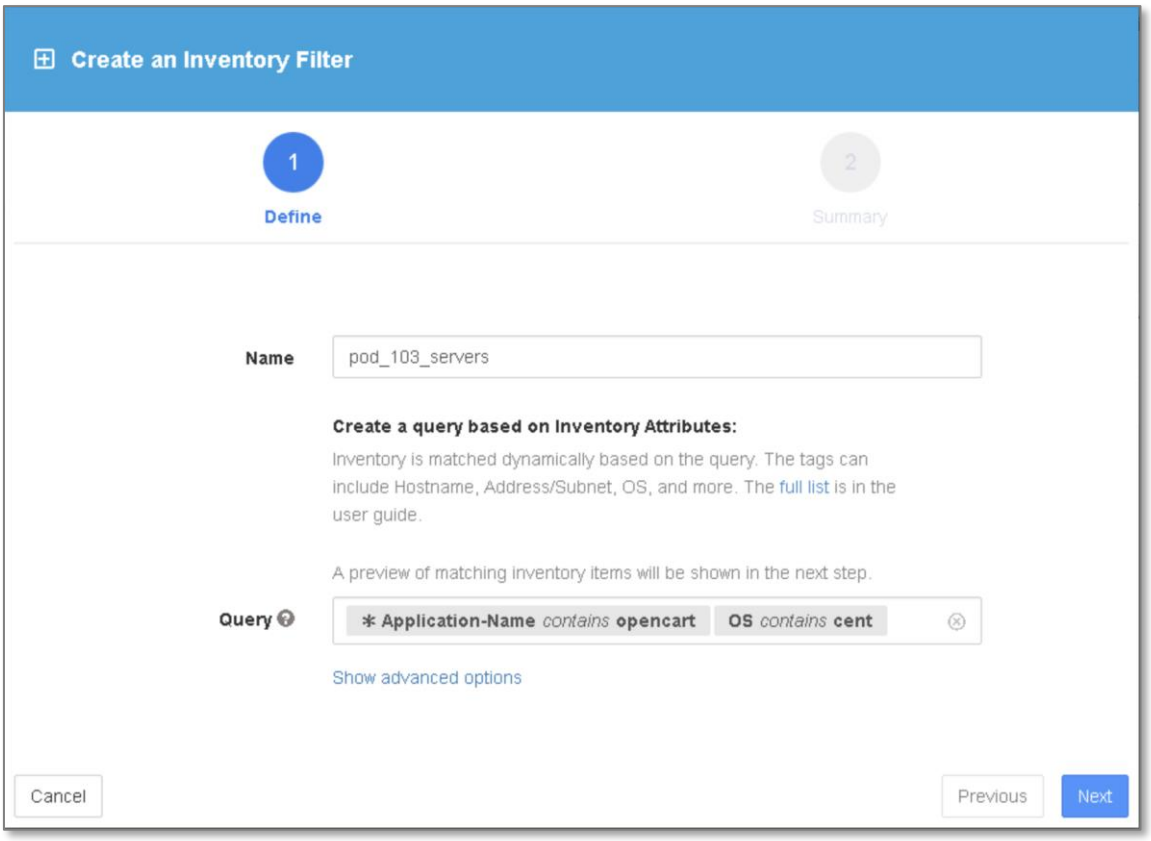
[Query] フィールドで、以下を実行します。

4. 「Application-Name *contains* opencart」と入力します。（*が自動補完されます）

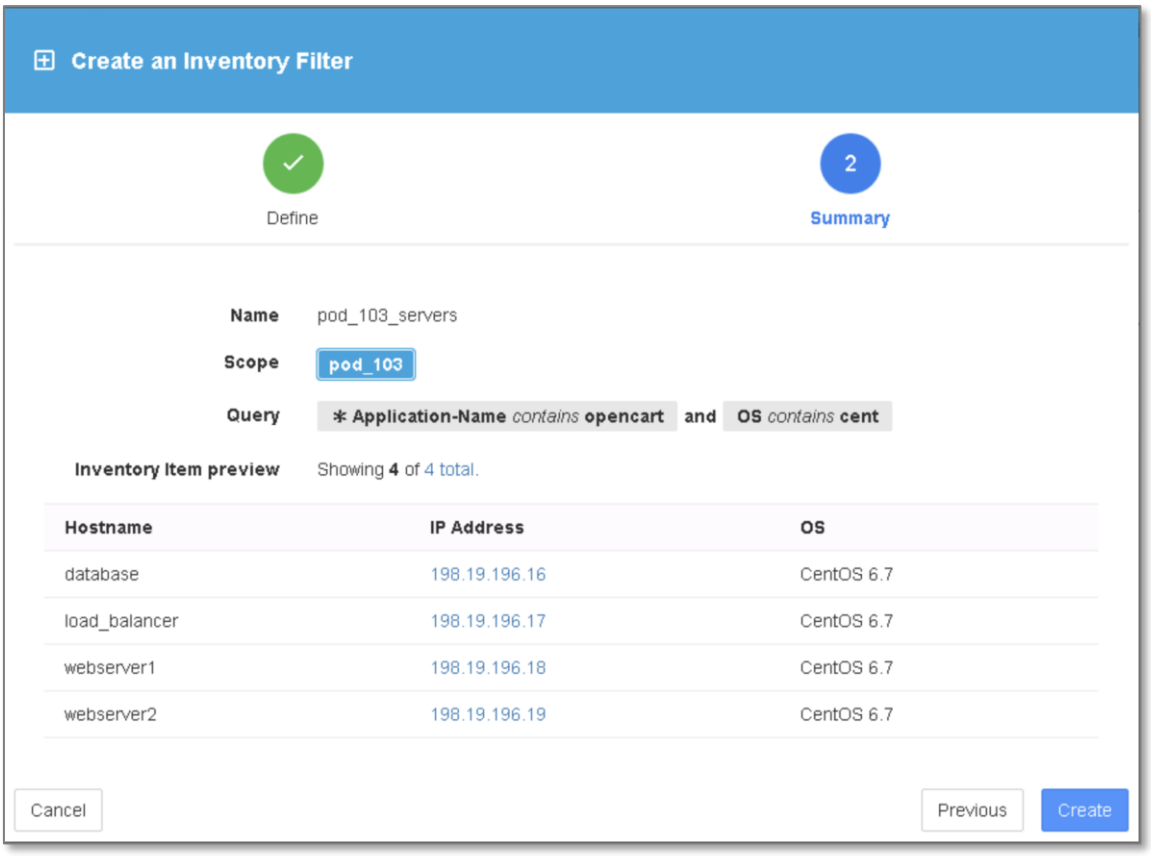
5. キーボードの Enter キーを押します。

6. そのまま続けて「OS *contains* cent」と入力します。

7. キーボードの Enter キーを押すと、次のように表示されます。



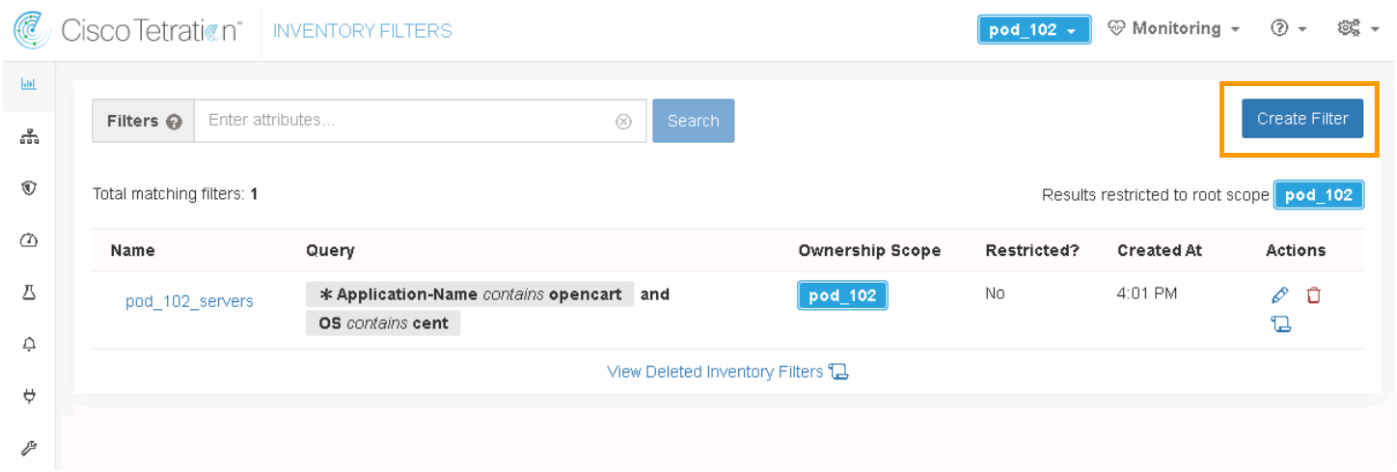
8. [Next] ボタンをクリックすると、次のように表示されます。



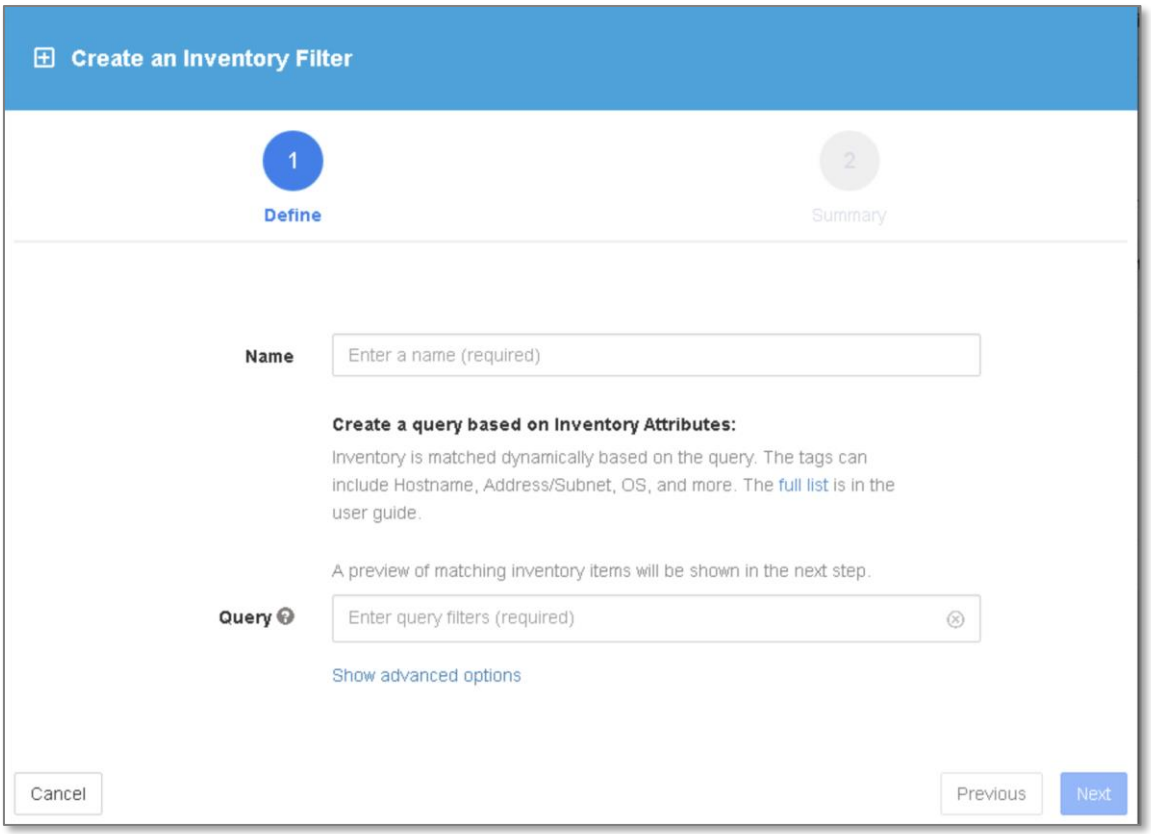
9. [Create] ボタンをクリックします。

フィルタのもう 1 つの使用例として、ポッド内のワークステーションマシンだけを表示するフィルタを作成します。

手順



10. （上図で強調表示されている）[Create Filter] ボタンをクリックします。[Create an Inventory Filter（インベントリフィルタの作成）] ダイアログが開きます。



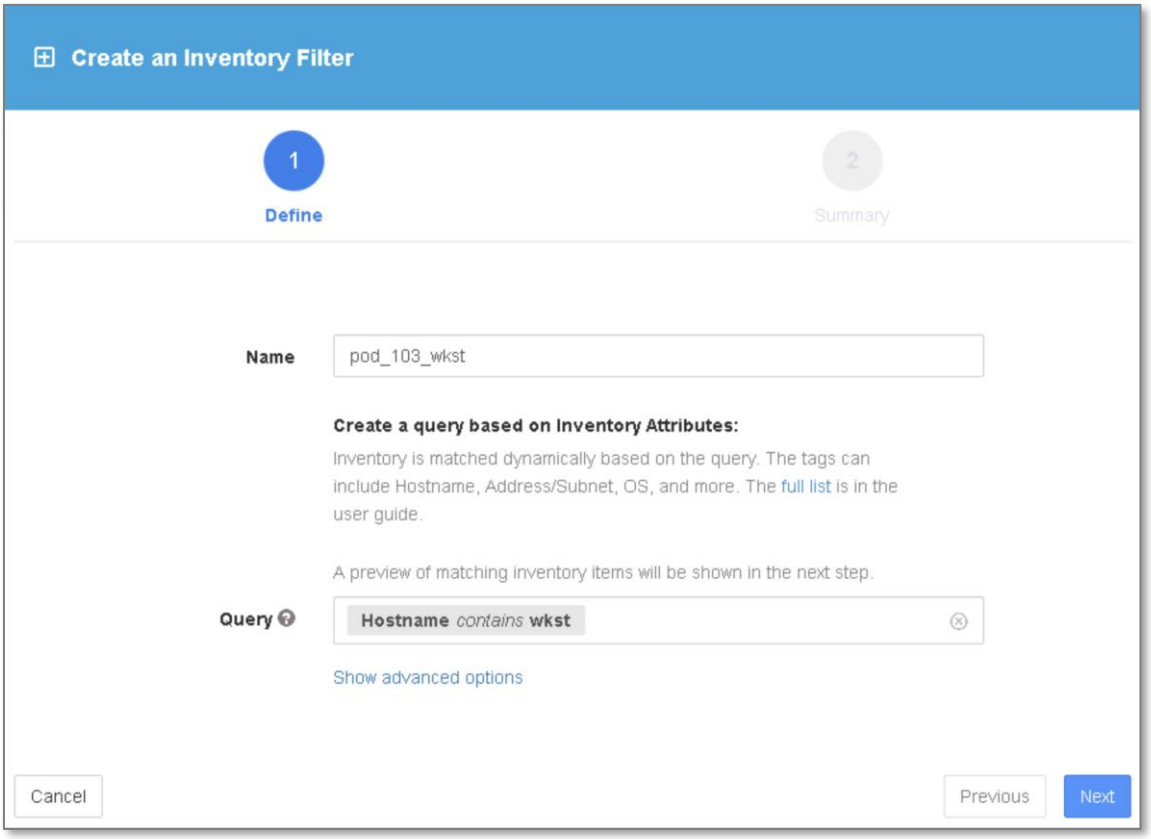
[Name] フィールドで以下を実行します。

1. 「pod_XXX_wkst」と入力します（XXX はポッド番号に一致します）。

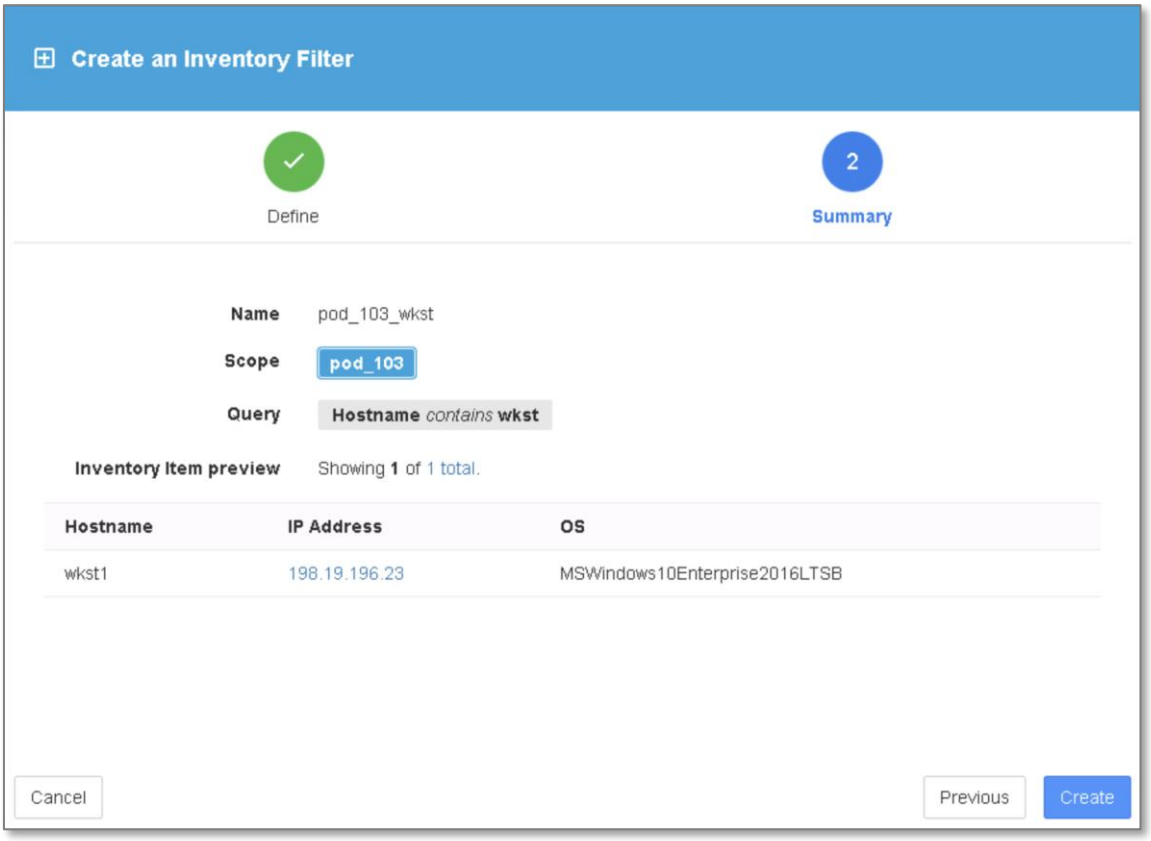
[Query] フィールドで、以下を実行します。

2. 「Hostname *contains* wkst」と入力します。

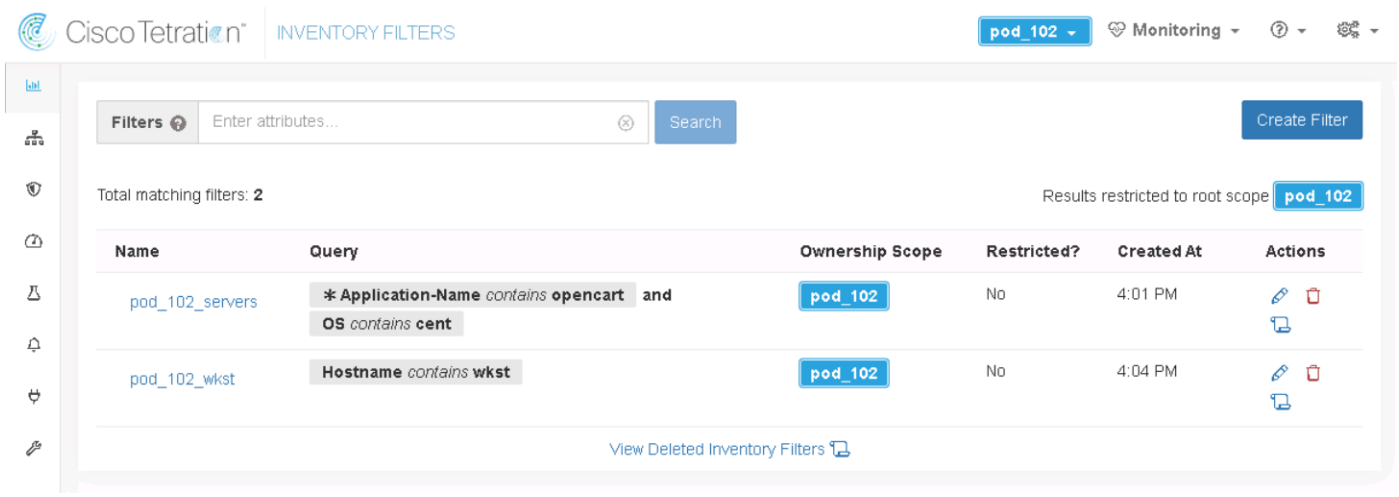
3. キーボードの Enter キーを押すと、次のように表示されます。



4. [Next] ボタンをクリックします。



5. [Create] ボタンをクリックすると、フィルタがフィルタのリストに追加されます。



注：フィルタはさまざまな方法で柔軟に使用できます。たとえば、Windows 2008 を実行するすべての項目をすばやく表示したり、CVE スコアが 9 以上（クリティカルなソフトウェアの脆弱性）のすべてのマシン、または AWS East 1 で実行されているすべての実稼働ワークロードを表示することができます。フィルタを使用して、適用する柔軟なポリシーを作成することもできます。たとえば、インターネットと WannaCry に対して脆弱な PCI ゾーン内の任意

の Windows サーバとのすべての通信をブロックするルールを簡単に作成できます。他にも多くの用途があり、これはほんの一例です。

シナリオ 4.　アプリケーションの依存関係のマッピングを使用するポリシー検出

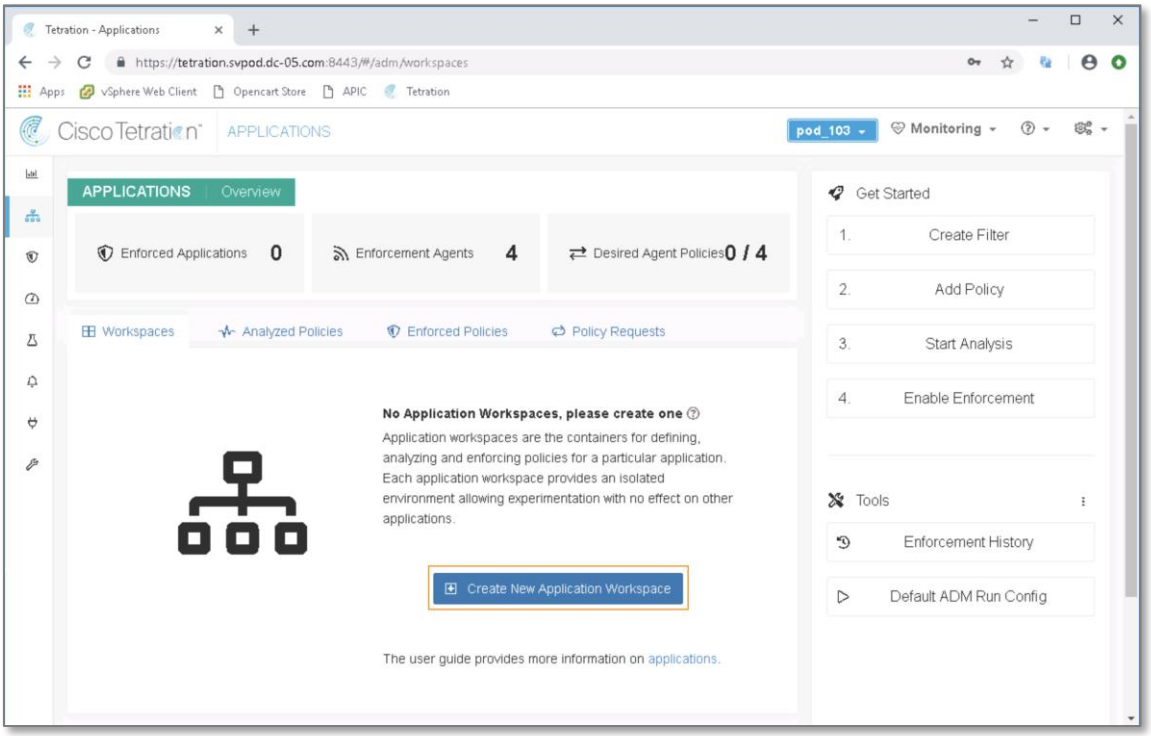
Tetration は、アプリケーションに関連するポリシーを自動的に検出できます。Tetration では、このプロセスをアプリケーションの依存関係マッピング（別名 ADM）と呼びます。このセクションの目的は、事前設定された OpenCart アプリケーションで ADM を実行するプロセスを説明することです。

Tetration はあらゆるワークロードに対して機械学習アルゴリズムを実行できますが、処理を制限したり、処理に重点を置くメカニズムを利用できれば便利です。その点をサポートするために、Tetration には「範囲指定」と呼ばれる概念があります。範囲指定では、フォーカスの範囲の作成を行います。これは、Tetration で分析する特定の項目についてフェンスを設定することに例えられます。このラボでは、すべての範囲と関連する設定がすでに作成されています。

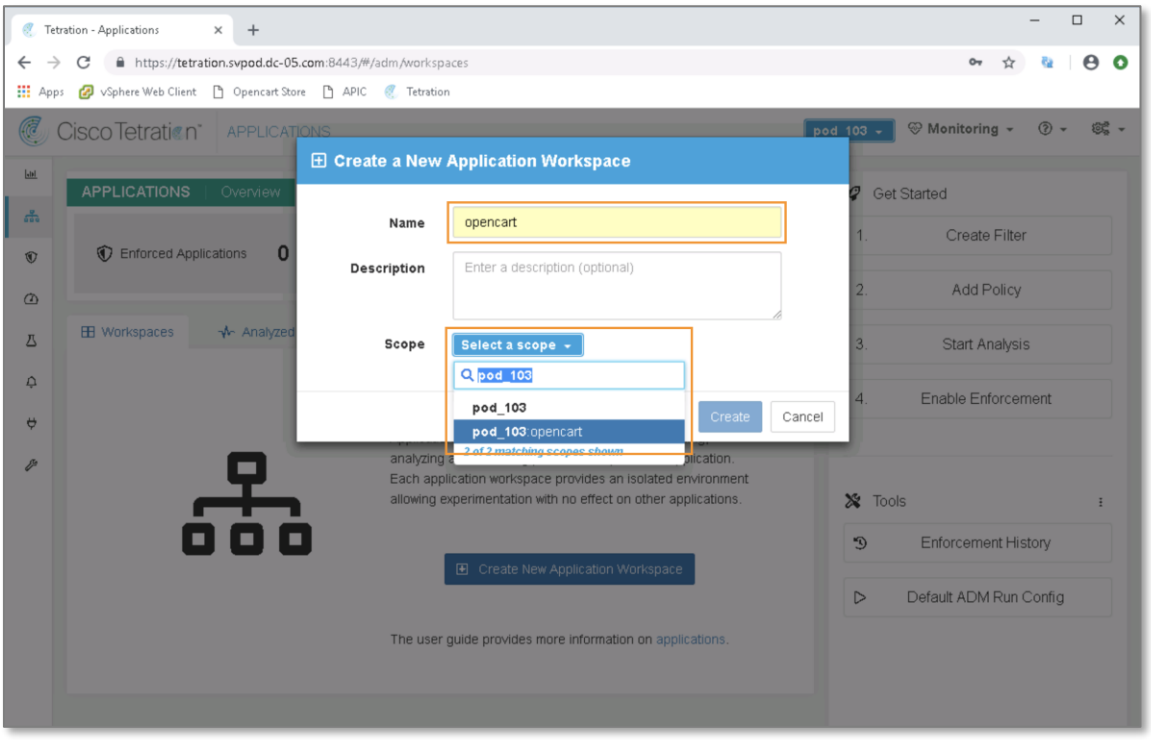
手順

サイドメニューで、以下を実行します。

1. [APPLICATIONS] をクリックして、タブを開きます。



2. （上図で強調表示されている）[Create New Application Workspace] ボタンをクリックすると、ダイアログが開きます。新しいアプリケーションワークスペースの作成を始めます。



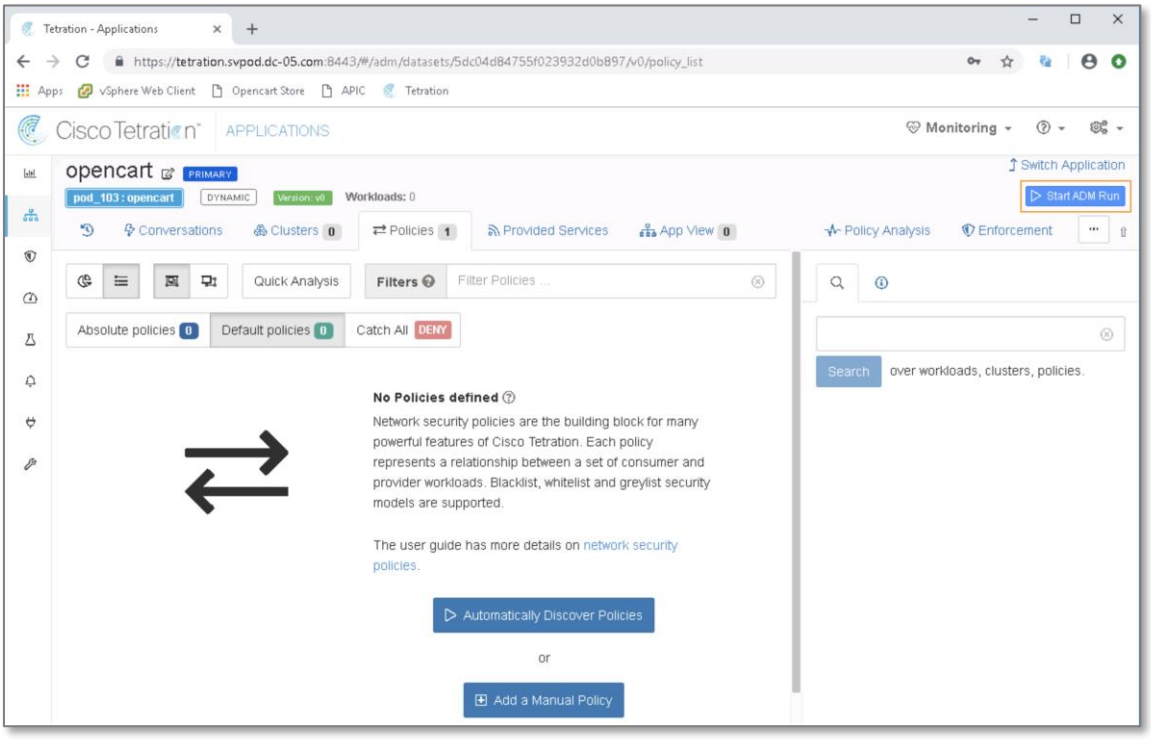
[Name] フィールドで以下を実行します。

3. 「opencart」と入力します。

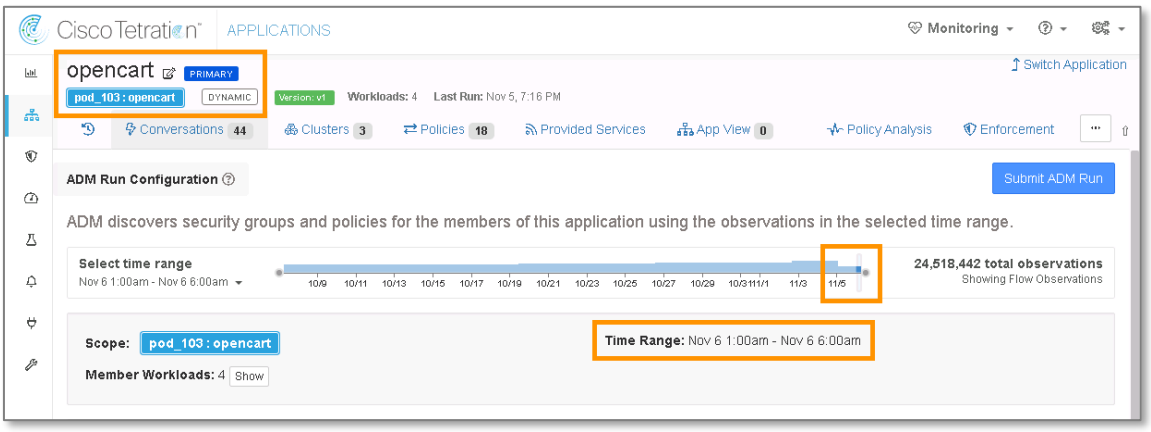
[Scope] ドロップダウンで、以下を実行します。

4. [pod_xxx:opencart] を選択します。

5. [Create] ボタンをクリックすると、新しいアプリケーション ワークスペースが作成されます。（チュートリアルが表示された場合は閉じてください）



6. （上図で強調表示されている）[Start ADM Run] ボタンをクリックすると、[ADM Run Configuration] ページが開き、（下図で強調表示されているように）選択した過去の時間範囲が表示されます。

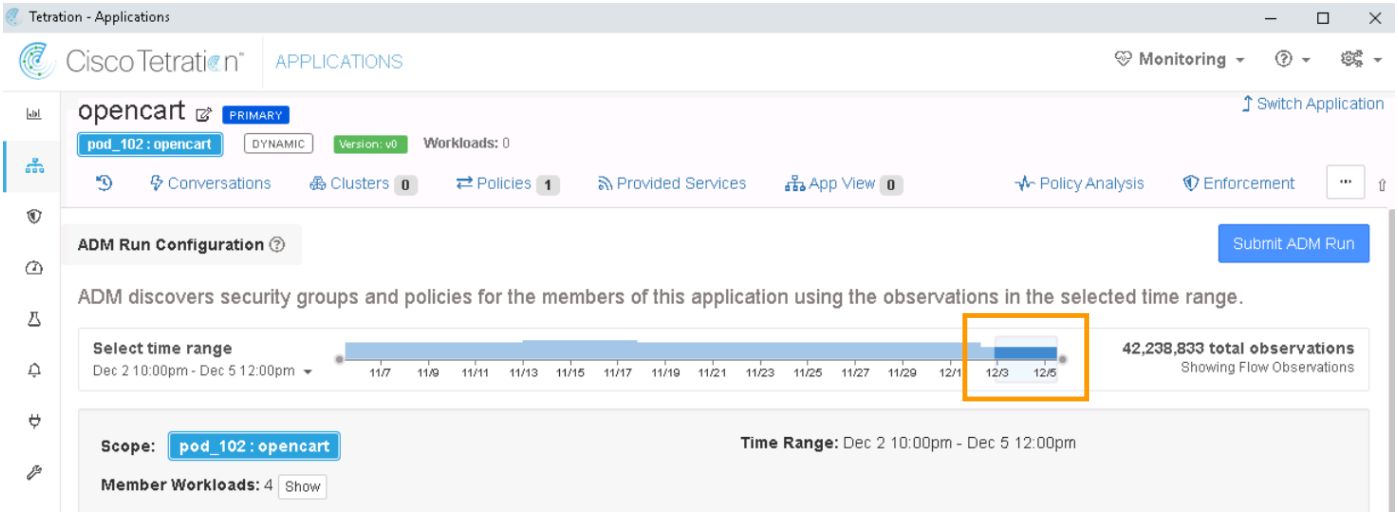


注：ラボ環境では *pod_xxx* の範囲が事前に作成されているため、一部のトラフィックは範囲内に存在し、ADM の実行をただちに要求できます。実稼働環境では、範囲が作成された後にトラフィックが生成されるまで待機してから ADM の実行を要求する必要があります。

ADM 実行の時間範囲の選択

この ADM を実行するために、今日から約 2 日前にさかのぼって時間範囲を選択してみましょう。

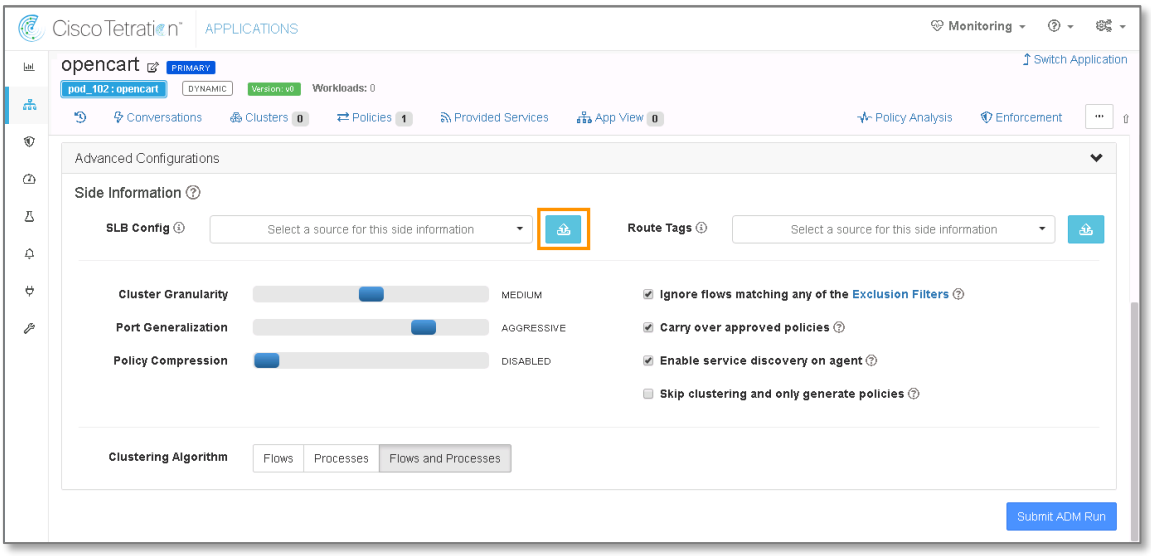
7. 水色の時間範囲セレクタの左側をポイントします。
8. 左マウスボタンを押したままにします。
9. 時間範囲セレクタの左側を約 2 日分左にドラッグします。
10. 左マウスボタンを離すと、（下図で強調表示されているように）時間範囲が選択されます。



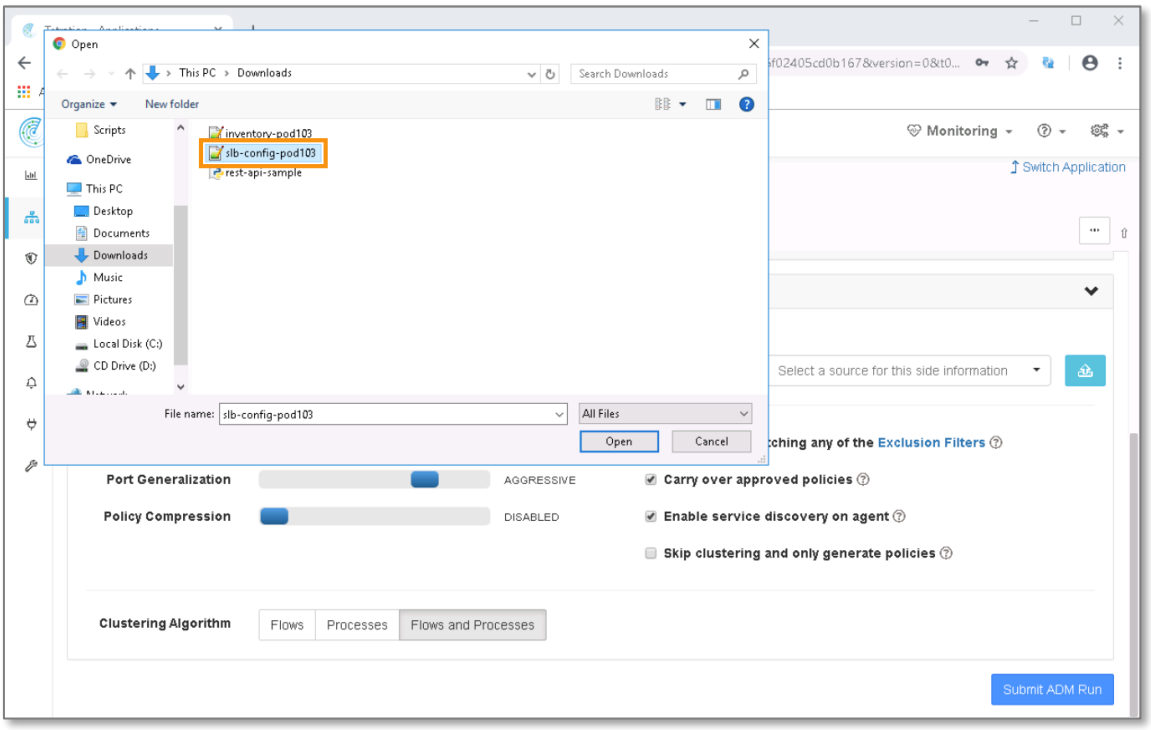
注：時間範囲にはセレクタ機能があり、ADM の実行に使用するフローデータの日付/時間の範囲を選択できます。選択したフローデータの量が多いほど、ADM の実行にかかる時間が長くなります。

フローデータの量が少ないと、ADM の結果が完全に正確ではない可能性が高くなります。時間範囲セレクタで、数日分のデータを選択します。

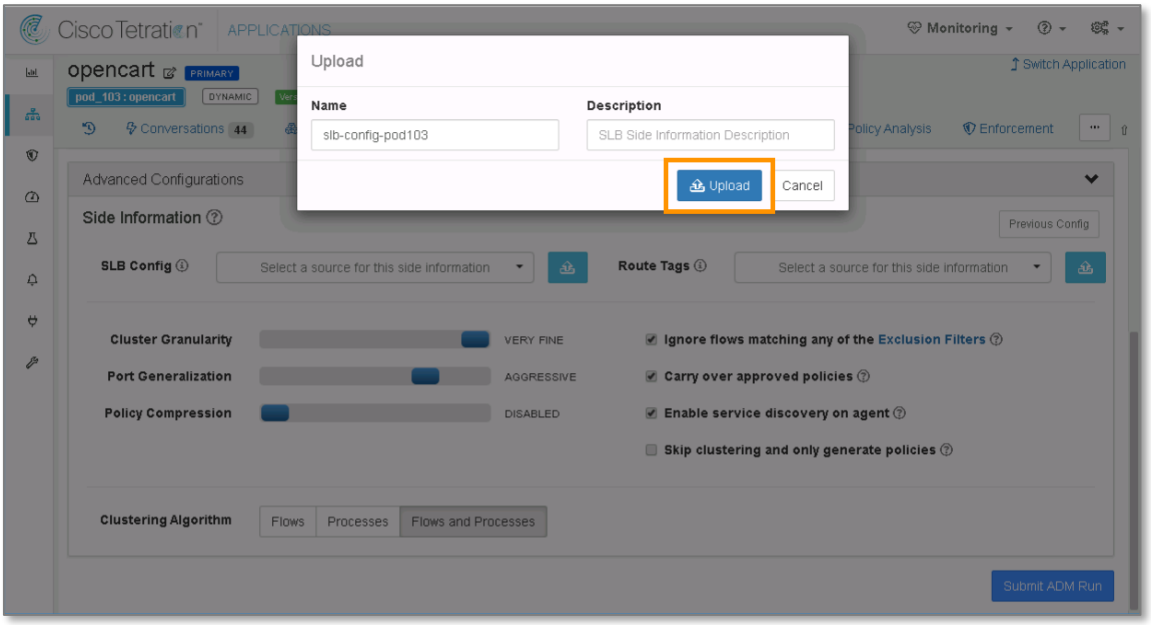
11. 下にスクロールして、[Advanced Configurations] パネル全体を表示します。



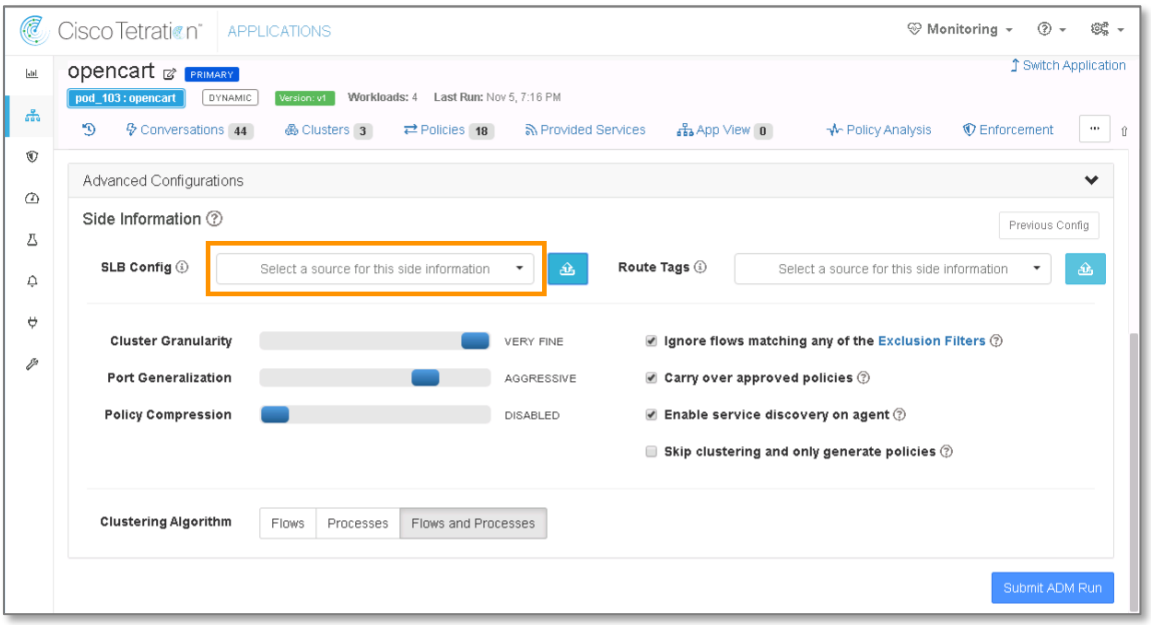
12. （上図で強調表示されている） [Upload]  ボタンをクリックすると、ファイルを開くダイアログが開きます。



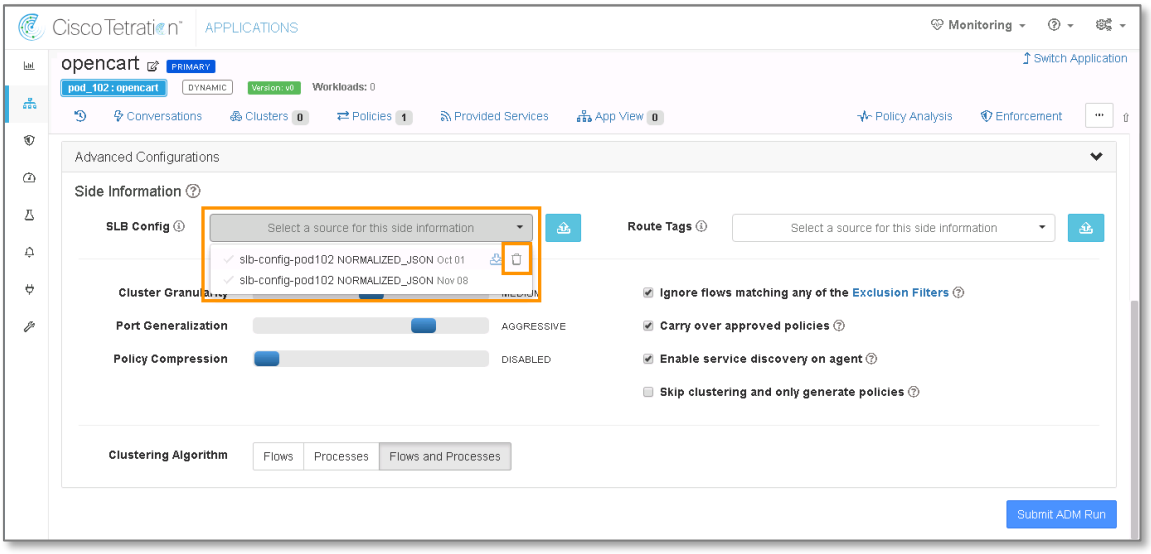
（上図で強調表示されている）*slb-config-podxxx* ファイルをダブルクリックすると、[Upload] ダイアログが開きます。



13. [Upload] ボタンをクリックすると、*slb-config-podxxx* ファイルがアップロードされます。



14. （上図で強調表示されている）[SLB Config] ドロップダウンをクリックするとドロップダウンが開きます。

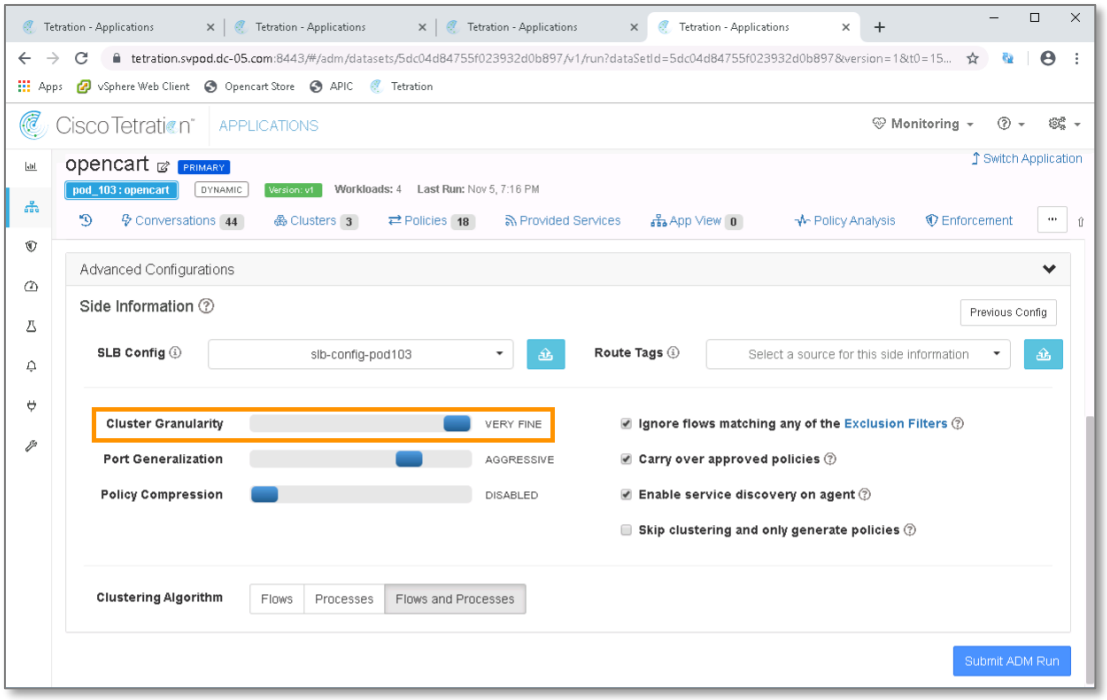


[SLB Config] ドロップダウンで、以下を実行します。

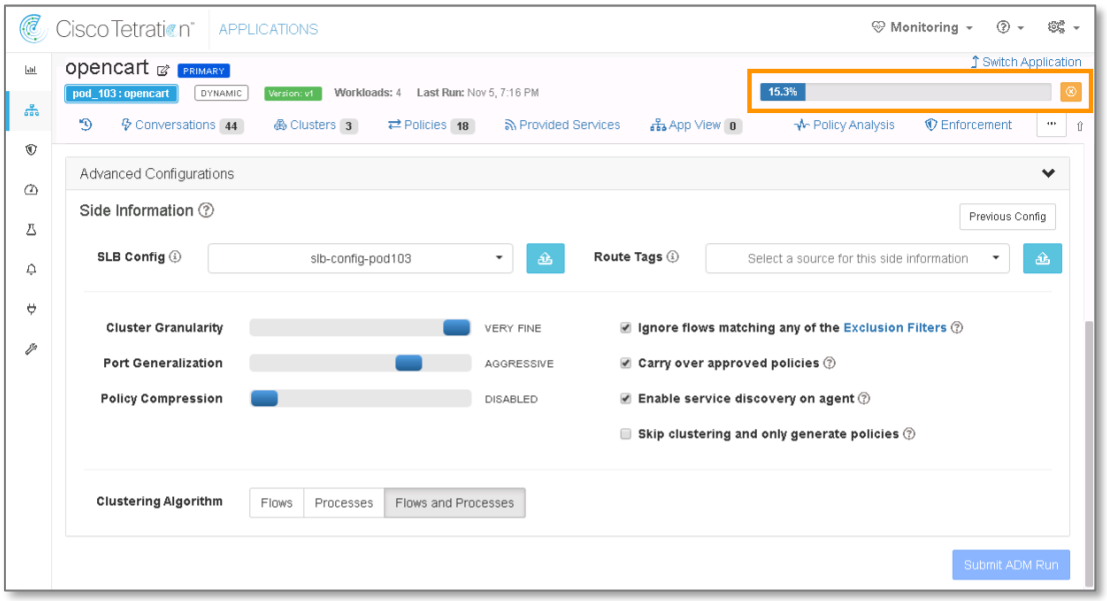
15. 直近の日付のファイルを選択します。

注：（ブラウザウィンドウが十分に広い場合）ドロップダウンの行の上にマウスポインタを置くと、削除アイコン（ごみ箱）が表示されます。このごみ箱をクリックすると（「確認」のダイアログが表示された後）ドロップダウンから行が削除されます。

16. [Cluster Granularity（クラスタ粒度）] スライダが（下図で強調表示されているように）[Very Fine（非常に細かい）] 値に設定されていることを確認します。



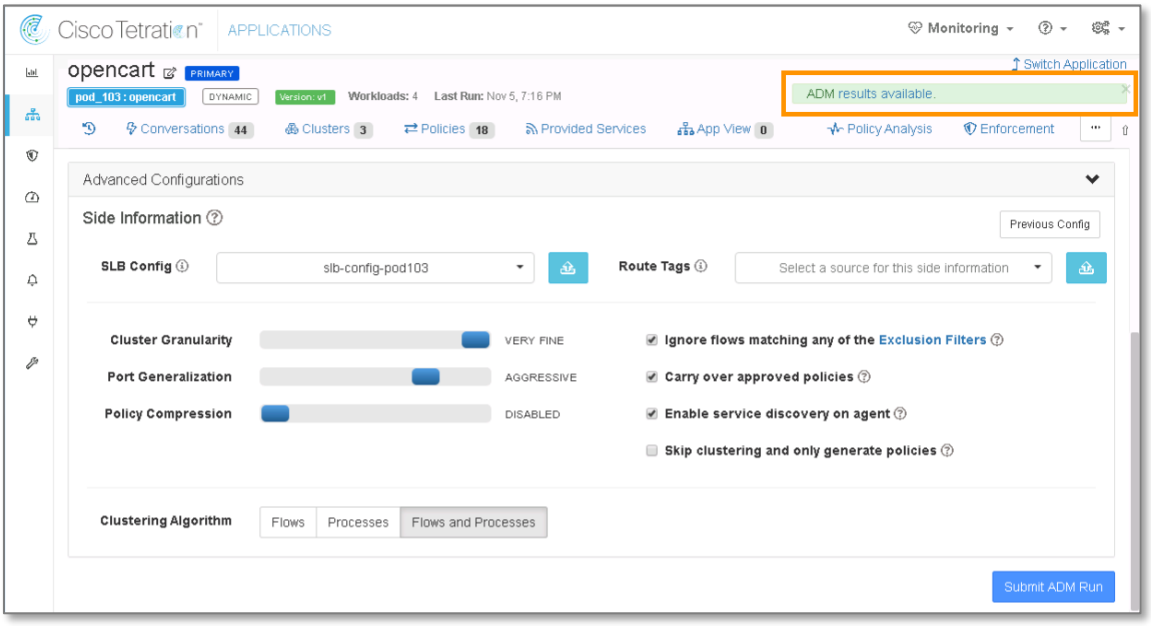
17. [Submit ADM Run] ボタンをクリックすると、ADM **の実行**が開始され、（下図で強調表示されているように）進行状況の情報が返されます。



注：選択した日付範囲に応じて、ADM の実行に 2 ～ 5 分かかる場合があります。

ADM の実行中に、Tetration は教師なしの機械学習を使用して、対象範囲のデータのすべてのメタデータを分析し、エンドポイントをクラスタにグループ化します。作成されたクラスタを確認し、必要に応じて、4 つのクラスタ（1 つ

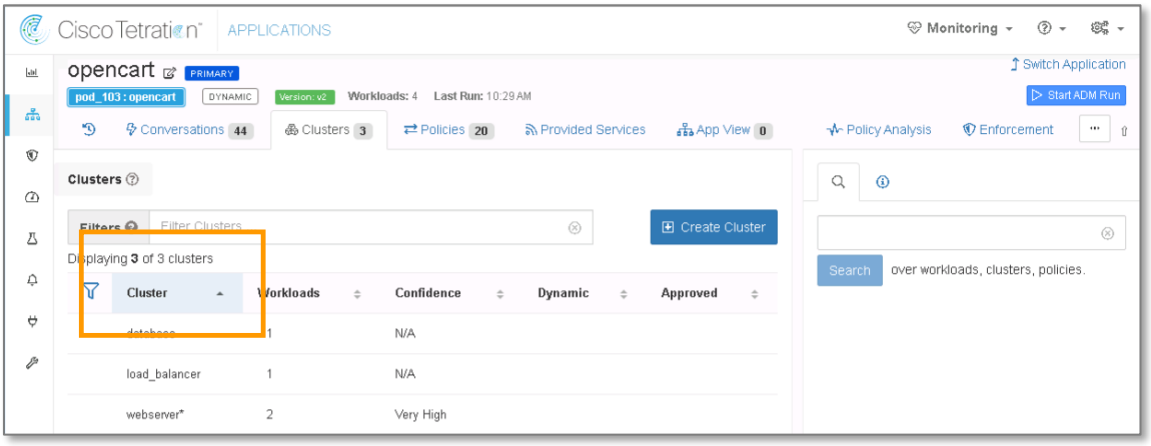
目のクラスタに webserver、load-balancer はそれ自体のクラスタ、3 つ目のクラスタに database、4 つ目のクラスタに wkst）が存在するよう編集します。実稼働環境では、ADM 実行用に 4 ～ 6 週間のデータを選択します。それらのデータが得られない場合は、大規模なデータセットを選択し、ADM を再実行します。



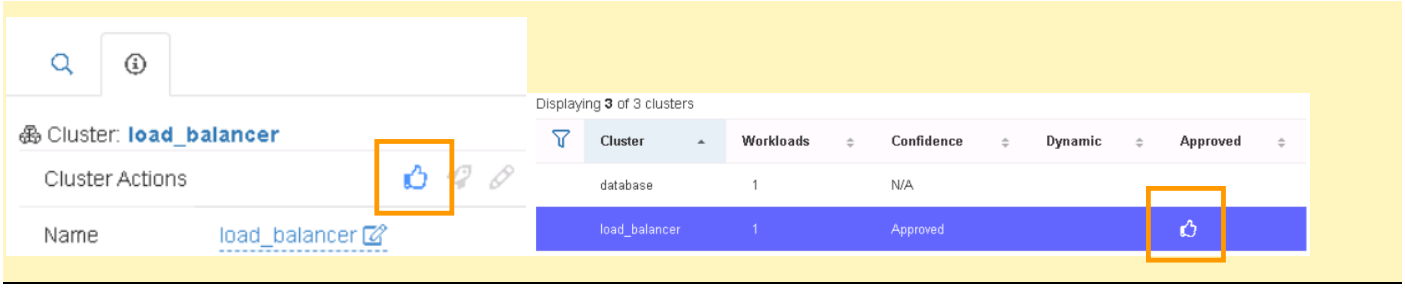
ADM **の実行**が完了したら、以下を実行します。

18. （上図で強調表示されている）[ADM results available] リンクをクリックし ADM 結果の表示に移ります。

19. （下図で強調表示されている）[Clusters] タブをクリックします。Clusters タブが開き、ホストをグループ化する方法の「最適な推測」が表示されます。



注：クラスタごとに [クラスタの承認（Approve Cluster）] をクリックすると、次の ADM 実行中、ADM でクラスタは再作成されません。

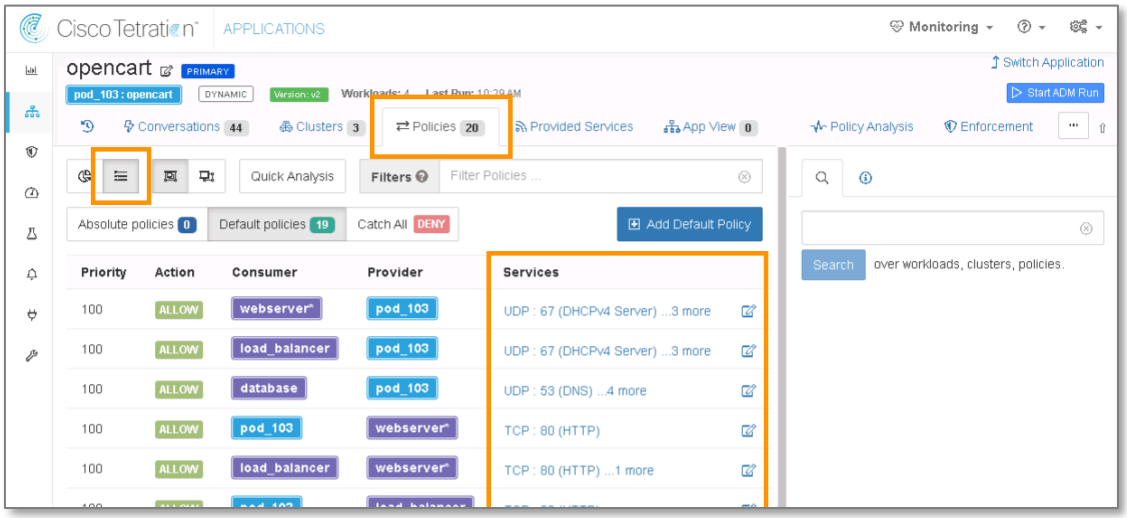


アプリケーションの依存関係マップについて

このセクションの目的は、**アプリケーションの依存関係マップ**の機能を説明することです。

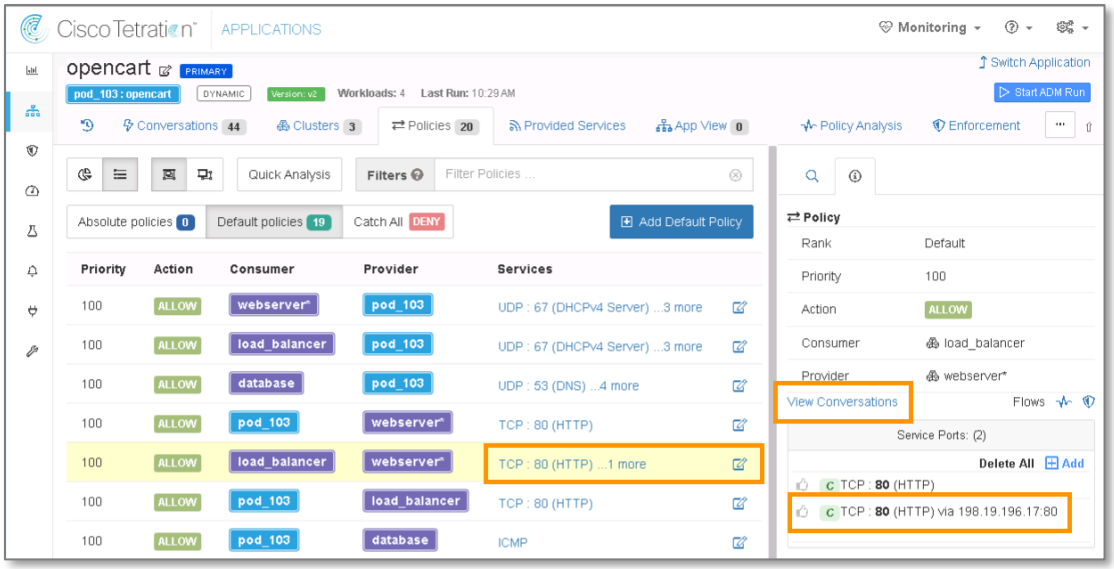
リストビュー

1. [Policies] タブをクリックすると、[Policies] タブが開きます。
2. [List View] がアクティブで、（下図で強調表示されているように）ポリシーがリストとして表示されていることを確認します。

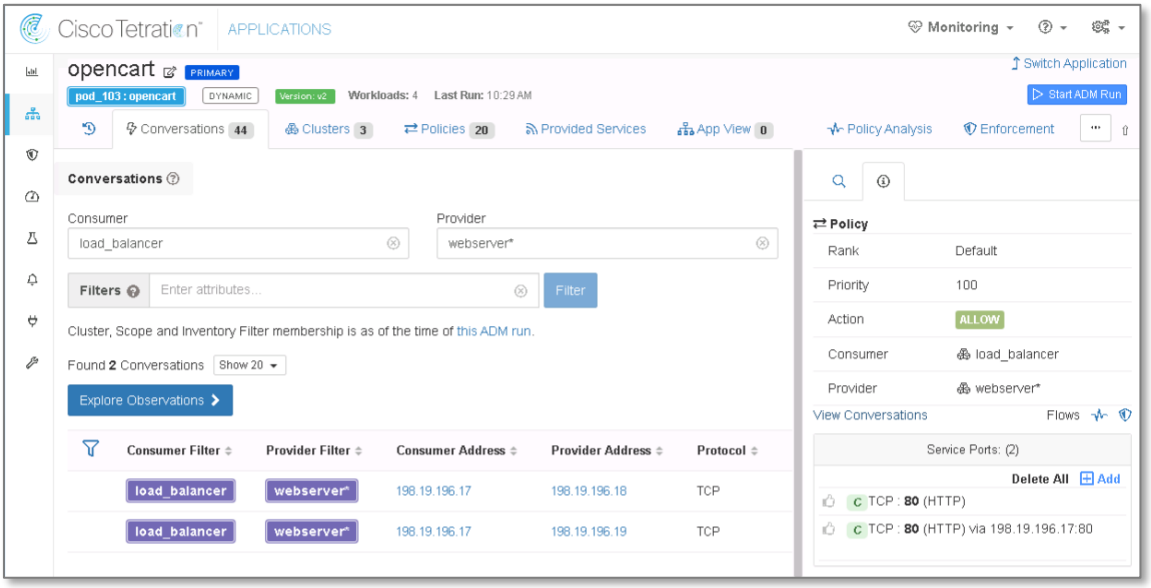


（上図で強調表示されているように）[Services] 列で、以下を実行します。

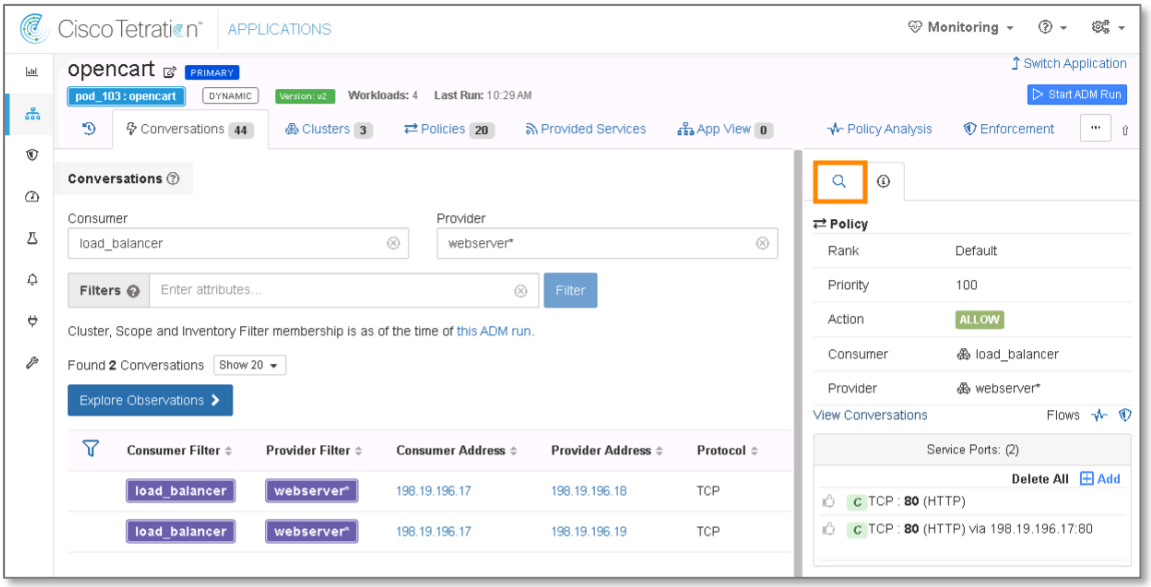
3. いずれかのリンクをクリックすると、（下図で強調表示されているように）**サービスポート**の詳細が表示されます。



4. （上図で強調表示されている）[View Conversations] リンクをクリックします。タブが開き、そのポート経由でサービスを提供および使用しているクラスタのリストが、プロバイダーとコンシューマの IP アドレスとともに表示されます。

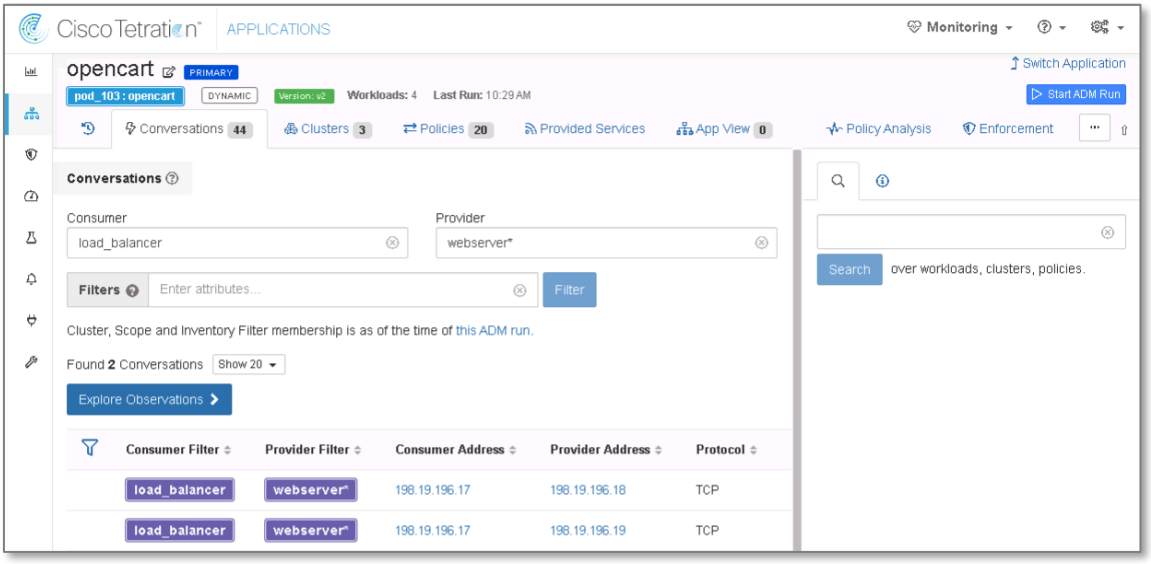


検索



検索するには、以下を実行します。

1. （上図に表示されている）[Search] タブをクリックしタブを開きます。

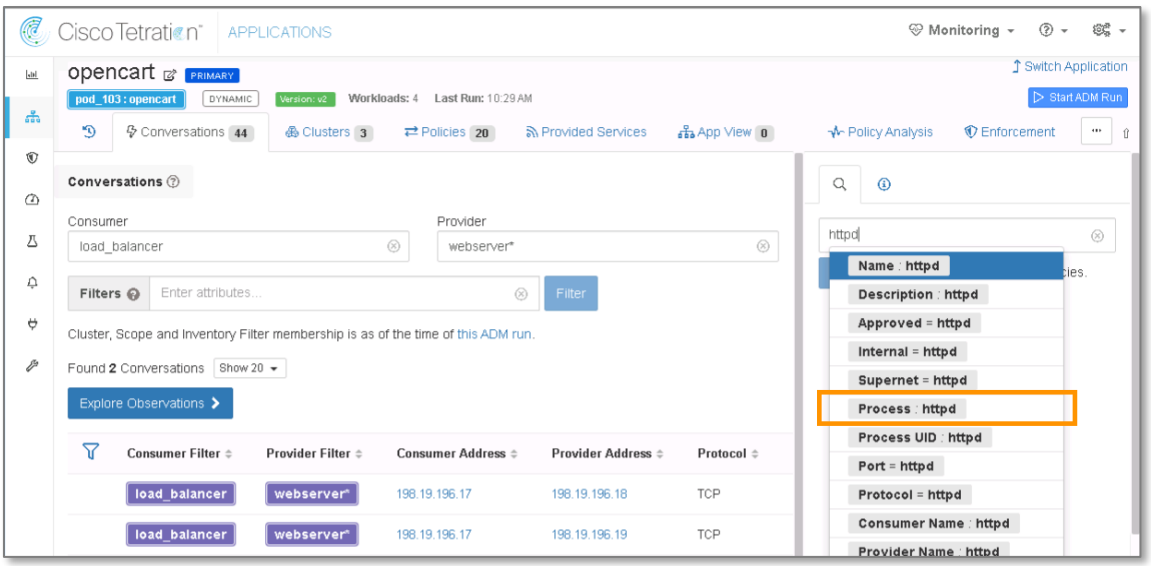


[Search] フィールドで、以下を実行します。

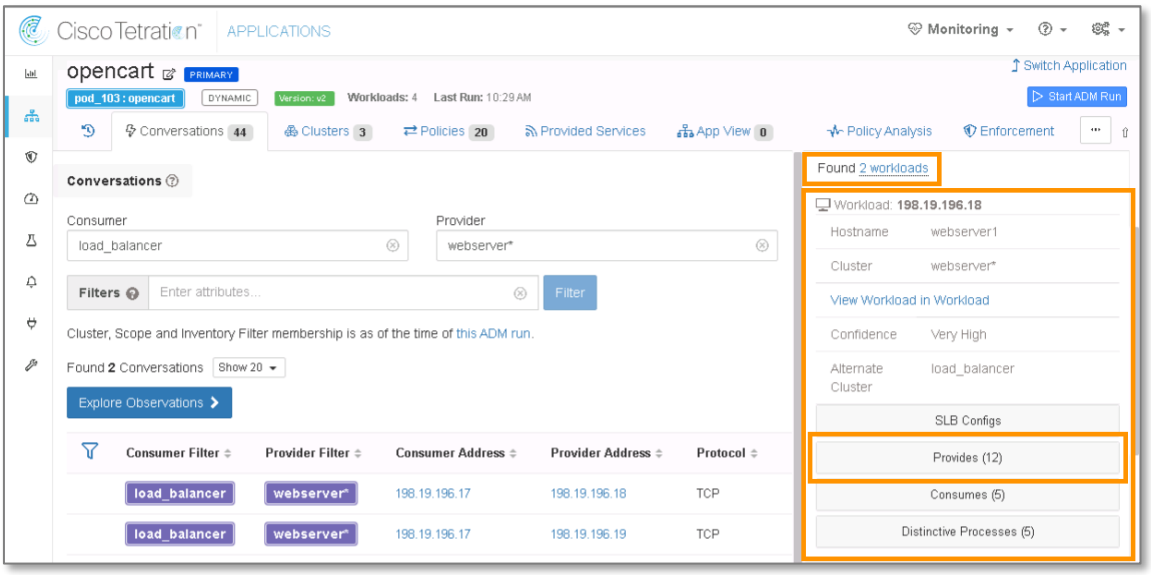
2. *httpd* と入力します。

生成されたオプションから、以下を実行します。

3. [Process: httpd] オプションを選択します（下図を参照）。

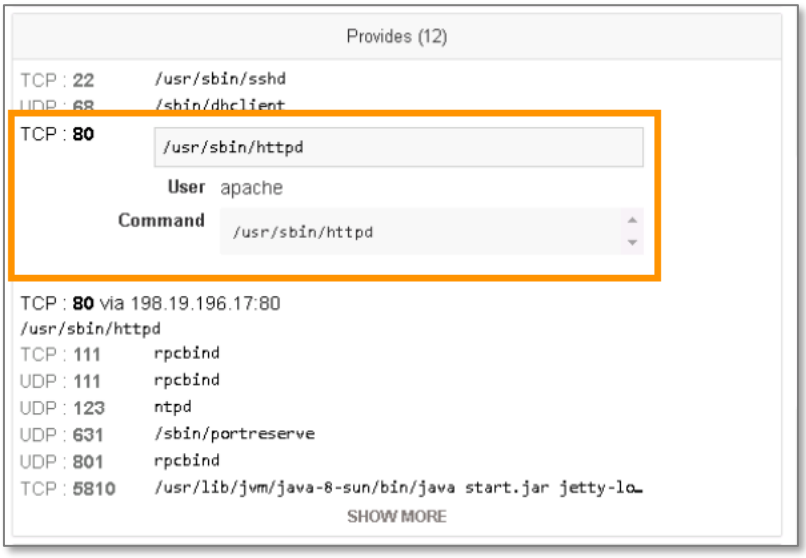


4. [Search] ボタンをクリックすると、httpd プロセスを実行している、このワークステーション内のサーバのリストが返されます（下図では 2 つのうち最初の方が強調表示されています）。



5. （たとえば）[Provides] ボタンをクリックすると、以下の パネルが開きます。

6. プロセス（上図のように httpd など）をクリックすると、詳細が表示されます。



※表示は異なることがあります

注: このセクションに含まれる情報にネットワークオペレータがアクセスするのは、今までは非常に困難でした。Tetration はそれをリアルタイムで提供し、数秒でアクセスできます。

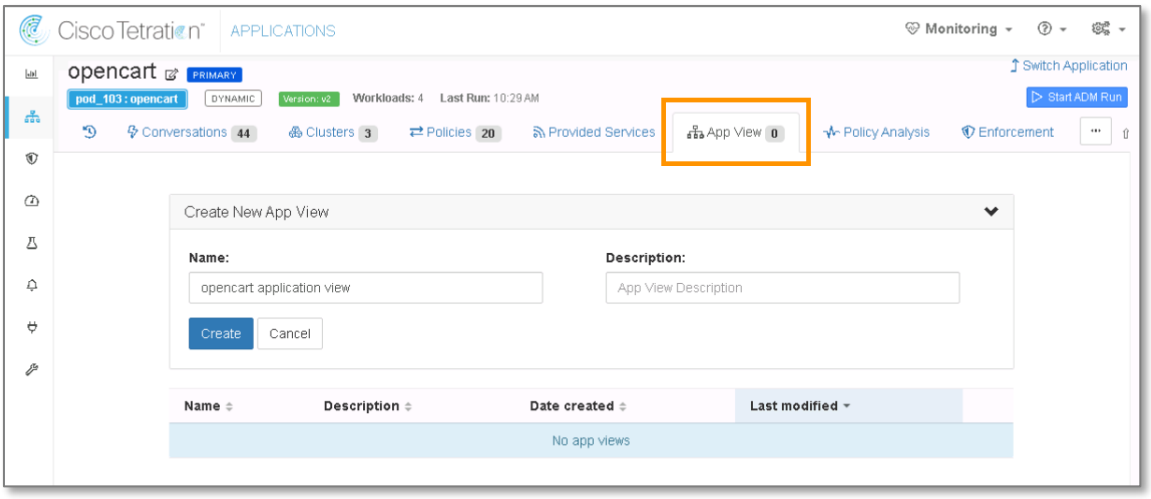
[提供（Provides）]：ホストがトラフィックを提供しているオープンポートのリストと、オープンポートを扱うローカルプロセスが表示されます。太字で示されているポートは、Tetration がアクティブフローを確認したオープンポートを表しますが、明るいグレーポートはネットワークトラフィックを認識していないオープンポートです（これはセキュリティの脆弱性のポイントで、解決すると攻撃対象領域を縮小できる可能性があります）。

[消費（Consumes）]：ホストがトラフィックを消費しているポートのリストが表示されます。

[特殊なプロセス（Distinctive Processes）]：トラフィックフローの特定のしきい値に達しているプロセスが表示されます。この値は Tetration アルゴリズムおよびプロセスの起点に基づいて決定されます。

アプリケーションビューの作成

1. [App View] タブをクリックします。

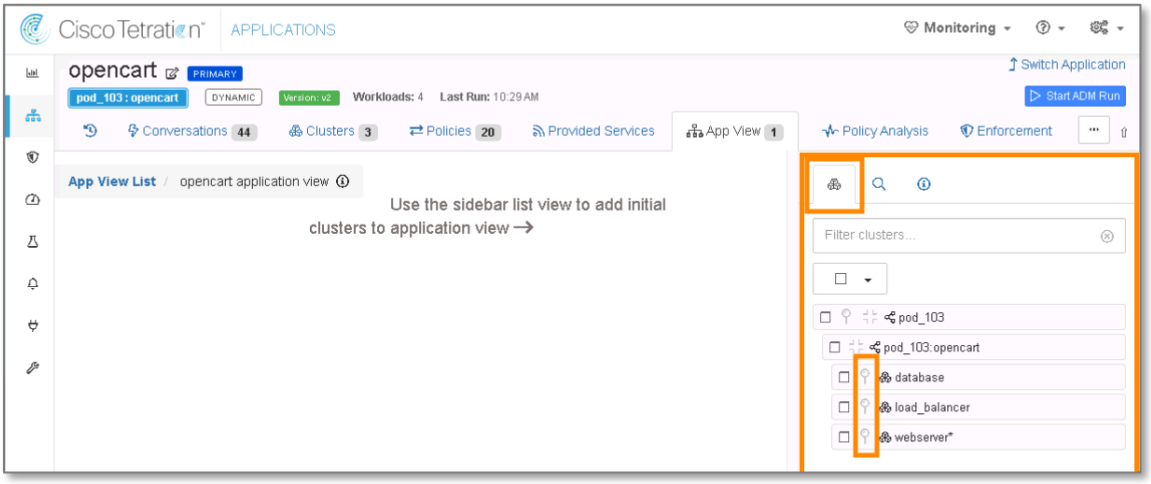


2. [Create New App View]で パネルが開くことを（クリックして）確認します。

[Name] フィールドで以下を実行します。

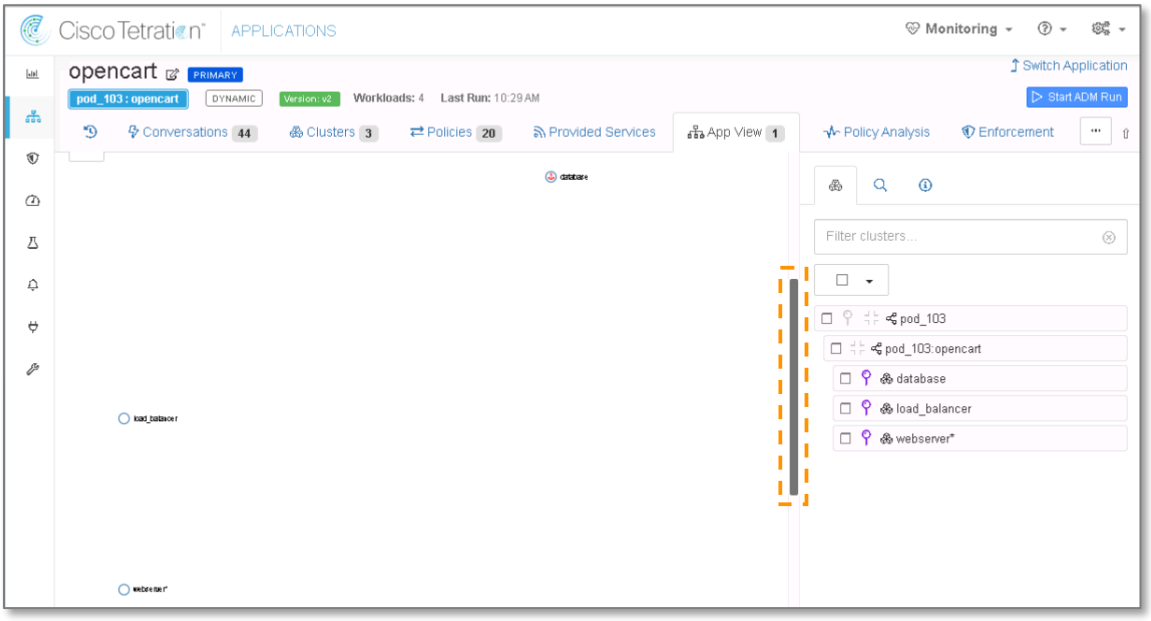
3. *opencart application view* と入力します。

4. [Create] ボタンをクリックすると、表示が変わり、右側にタブ付きのパネルが表示されます。



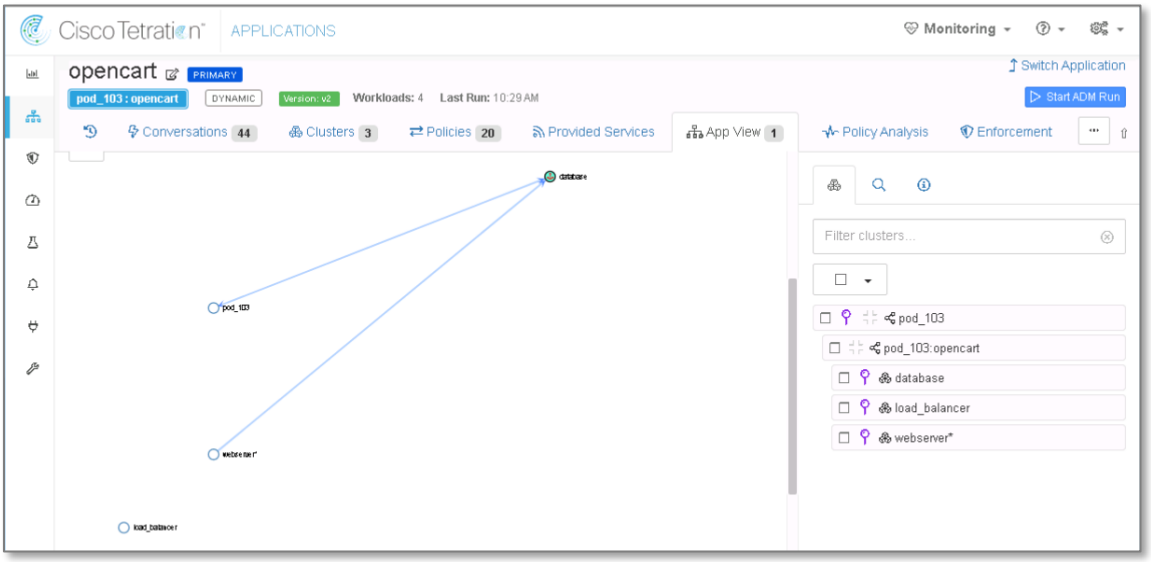
5. （上図で強調表示されている）[Cluster] タブがアクティブなタブであることを（クリックして）確認します。

6. （上図で強調表示されている）[database]、[load_balancer]、および [webserver*] のピン  をクリックします。これらはそれぞれマップに追加されますが、これらを表示するには（下図で強調表示されているように）マップを上方向にスクロールしなければならない場合があります。

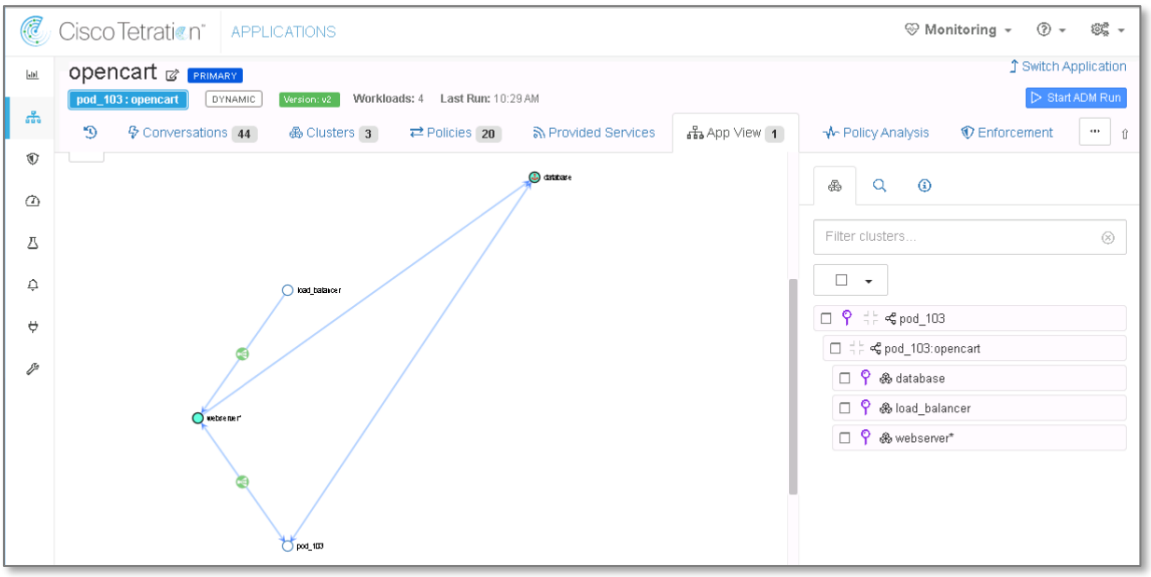


7. [database] をダブルクリックすると、マップが再描画されて以下が表示されます。

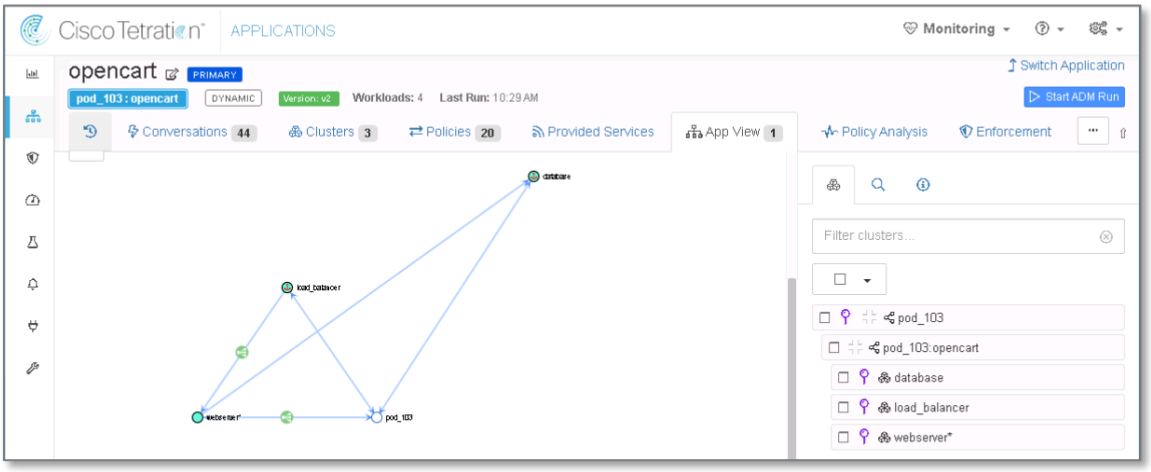
- pod_XXX
- database と pod_XXX 間の接続
- database と webserver* 間の接続



8. [webserver*] をダブルクリックすると、マップが再描画されて、load_balancer と pod_XXX への接続が示されます。



9. [load_balancer] をダブルクリックすると、マップが再描画されて、pod_XXX への接続が示されます。



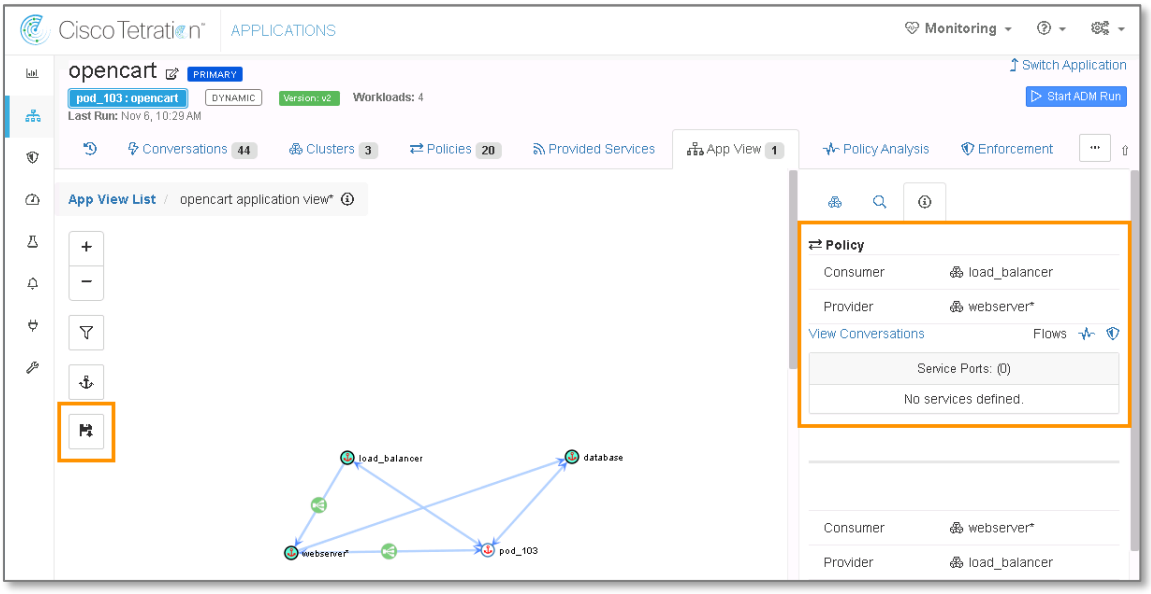
以下の操作を実行できます。

クラスタを（ドラッグして）並べ替え、マップの外観を好きなように変えることができます。

マップから任意のクラスタを削除（ピン解除）できます。

クラスタをクリックすると、そのクラスタが「提供および消費」するときのポートが示されます。

ポリシーコネクタをクリックすると、（下図で強調表示されているように）適用されたポリシーの詳細が表示されます。



10. （上図左側に強調表示されている）[Save（保存）] ボタンをクリックすると、コンテキストメニューが開きます。

11. [Save（保存）] オプションをクリックすると、**アプリケーションビュー**が保存されます。

シナリオ 5.　ポリシーの分析と適用

Cisco Tetration プラットフォームでは、包括的なポリシー分析と適用を実行できます。

ポリシー分析

注：ポリシー分析により、ユーザは、ポリシーがエンドポイントに導入される前に、ポリシーが環境内でどのような影響を与えるかを把握できます。また、ポリシーが現在の日付より前に導入されていた場合の影響を把握するために使用することもできます。

Tetration のポリシー分析では、フローの発信元 IP アドレスとポートまでの間に許可、誤廃棄、エスケープ、および拒否されたフローに関する情報が提供されます。Tetration は、ポリシーに準拠していないことを示すアラートを送信することもできます。

[許可（Permitted）] はポリシーによって許可されることになっていて、実際に許可されたフローです。これは、このポリシーが適切に機能していることを示しています。

[誤廃棄（Misdropped）] には、ネットワークによってドロップされたが、ポリシーでは許可されているはずのフローが表示されます。通常は、一方の側または他方の側が応答できなかったか、ネットワークによって何らかの中断が生じていることを示します。

[エスケープ（Escaped）] には、ネットワークによって許可されたが、本来はポリシーに従ってネットワークでドロップされるはずだったフローが表示されます。ネットワークオペレータは、このフローにドリルダウンして、ホワイトリスト化する必要があるかどうかを判断するための十分な情報を取得できます。ホワイトリスト化すべきでない場合は、IOC であるか、アプリケーションの動作や設定が変更されている可能性があります。

[拒否（Rejected）] には、ネットワークによって拒否されているフローおよび拒否されたはずのフローが表示され、ポリシーが適切に機能していることを意味します。この分類を見て興味深い点は、ポリシーに拒否されるものが示されている場合でも、それが試行されるのはなぜかということです。これは IOC である可能性があります。

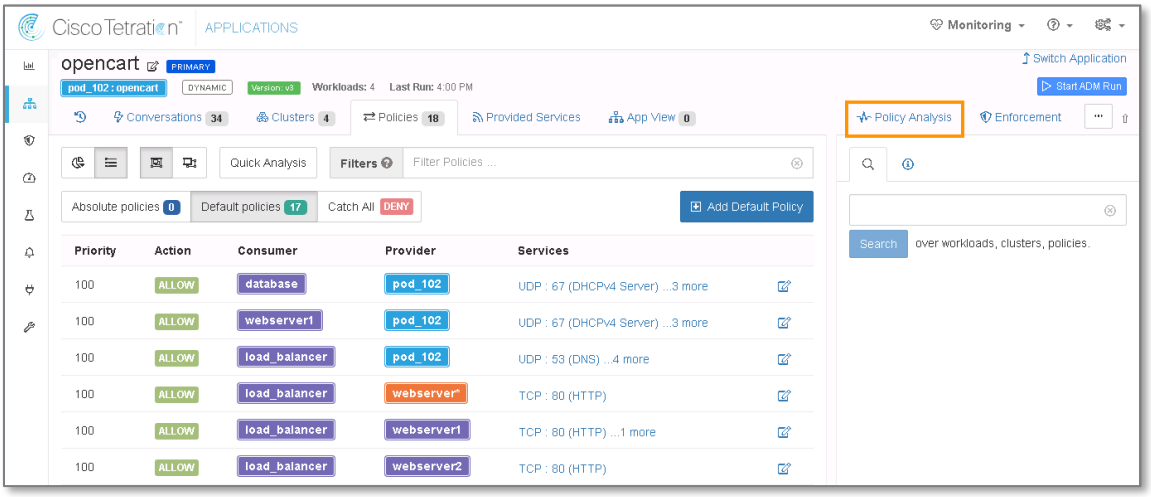
手順

12. [ポリシーの分析（Policy Analysis）] をクリックして、フローの次の 4 つの分類を示す UI のツールを確認します。

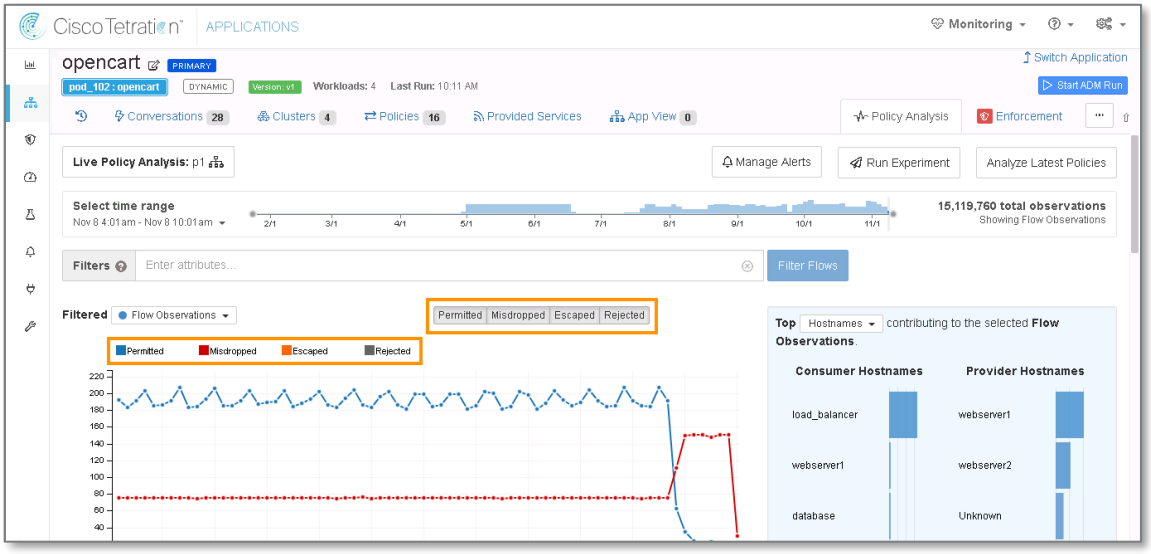
- Permitted （許可）
- Misdropped （誤破棄）
- Escaped（エスケープ）
- Rejected（拒否）

注：前のシナリオで、アプリケーションビューを保存しなかった場合、[Save] または [Don't Save] のどちらを選択するか確認するメッセージが表示されます。[Don't Save] ボタンをクリックし保存せずに進みます。

13. まだアクティブになっていない場合は、[Start Live Policy Analysis] をクリックしライブポリシー分析に移り、ポップアップで [Analyze] をクリックします。

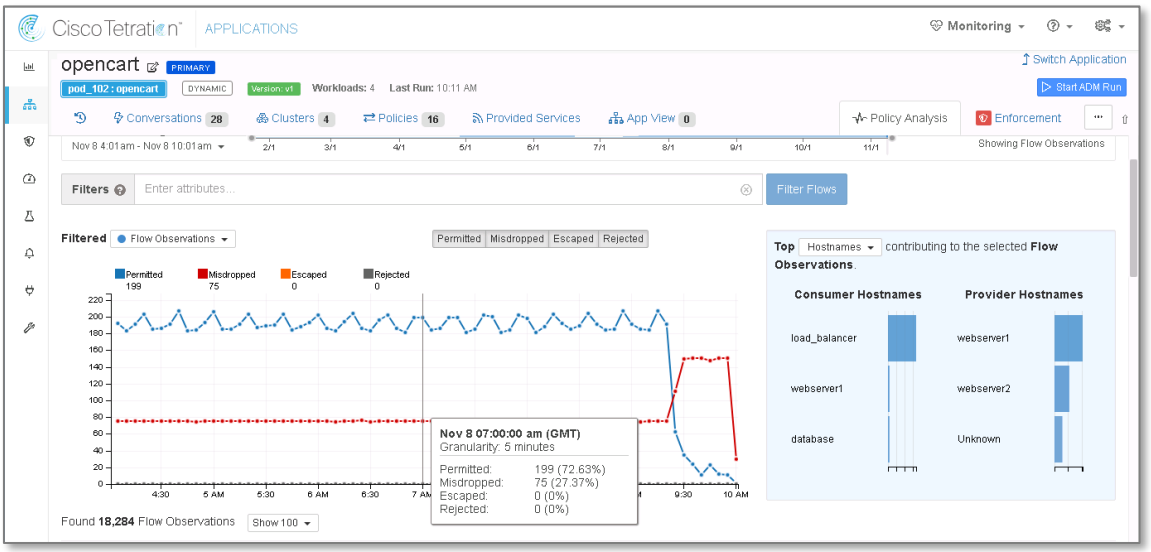


14. （上図で強調表示されている）[Policy Analysis] タブをクリックします。



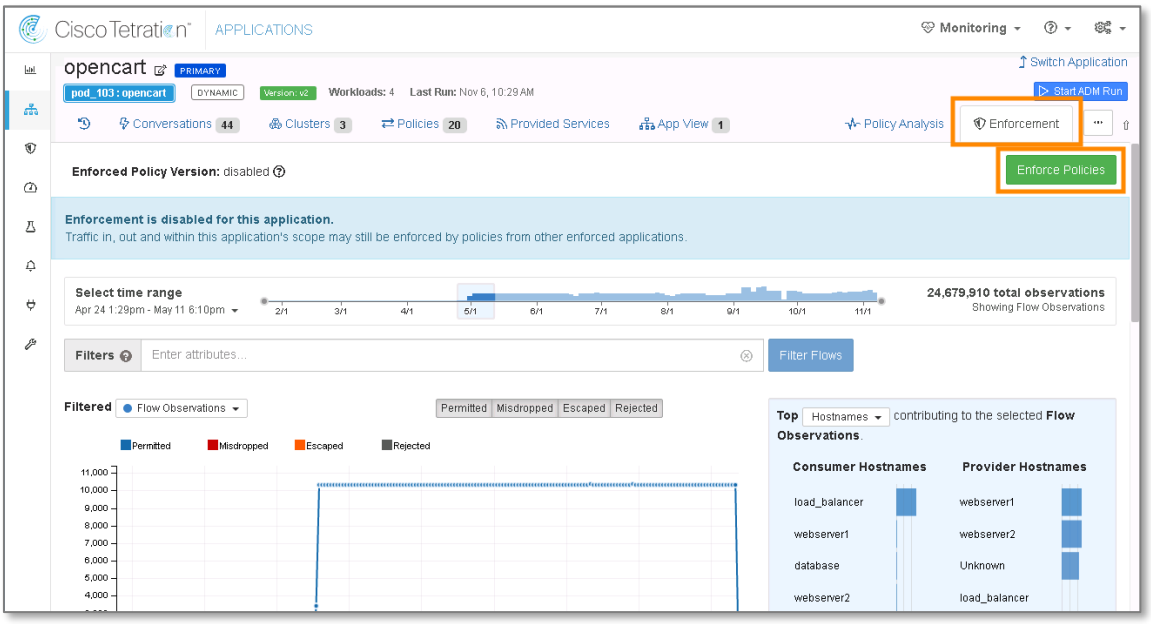
注：（上図で強調表示されている）一連のボタンでグラフの各フロータイプのオンとオフを切り替えます。たとえば、**エスケープされた**フローを表示する場合は、[Permitted（許可）]、[Misdropped（誤破棄）]、[Rejected（拒否）] ボタンをクリックします。色付きの四角形の行は、グラフ内の色付きの線のキーになります。

グラフのタイムスライスをクリックすると、そのタイムスライスで観測されたフローが表示されます。

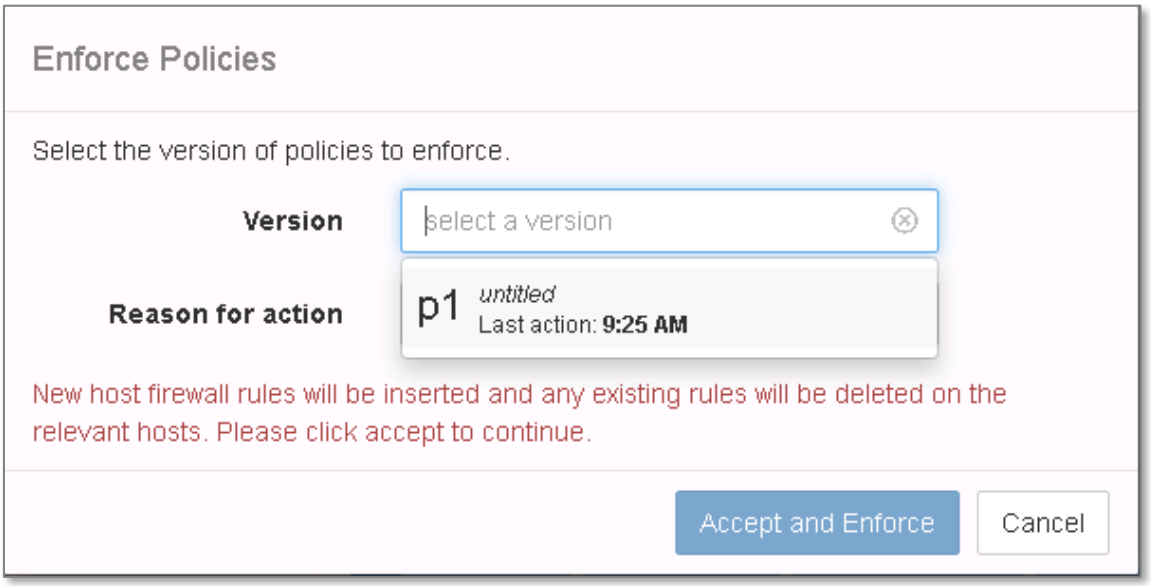


ポリシーの適用

1. [Enforcement] タブをクリックするとタブが開きます。



2. [Enforce Policies] ボタンをクリックすると、ポリシーの適用に関する[Enforce Policies] ダイアログが開きます。



[Version] ドロップダウンで、以下を実行します。

3. 最新のポリシーを選択します。

4. [Accept and Enforce] ボタンをクリックすると、[Enforce Policies（ポリシーの適用）] ダイアログが閉じます。

注：適用することで、Windows VM への特定のトラフィックのみを許可するファイアウォールポリシーと、Linux VM に対するファイアウォールルールをプッシュします。

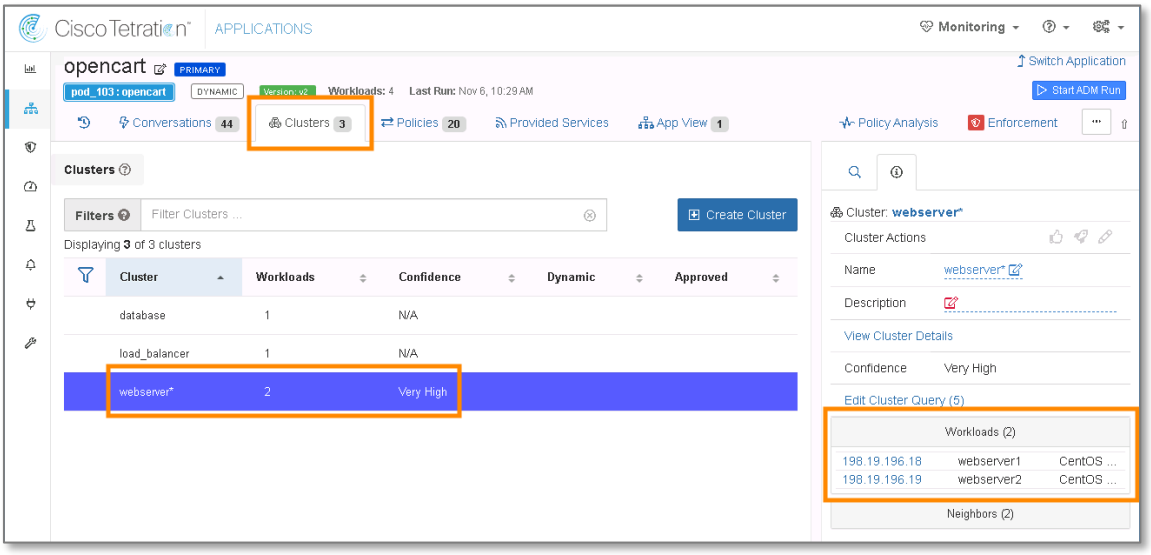
適用が完全に有効になる前に、ルールがワークロードにプッシュダウンされるまで、最大 60 秒ほど待たなければならない場合があります。

次に、ワークロードの 1 つにプッシュされたルールを見てみましょう。

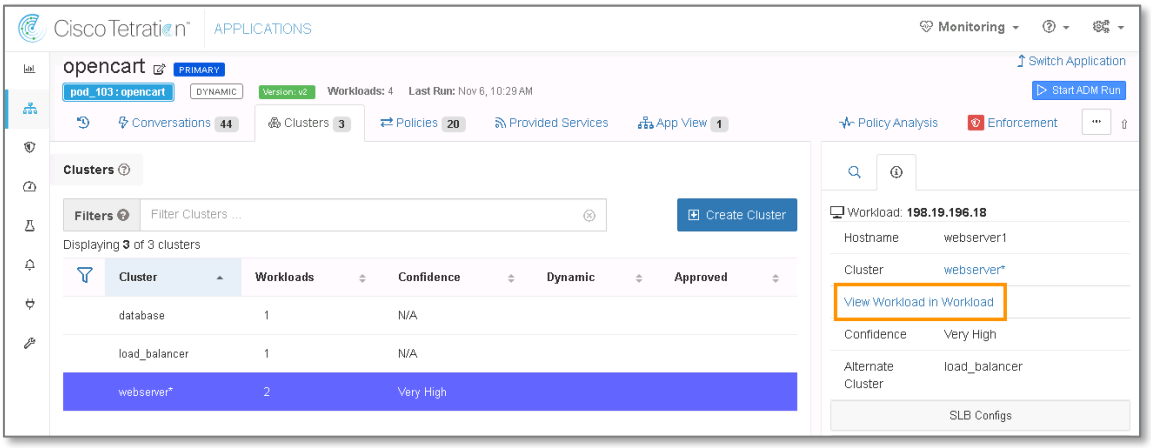
5. [Clusters] タブをクリックして タブを開きます。

6. （下図で強調表示されている）[webserver*] をクリックします。

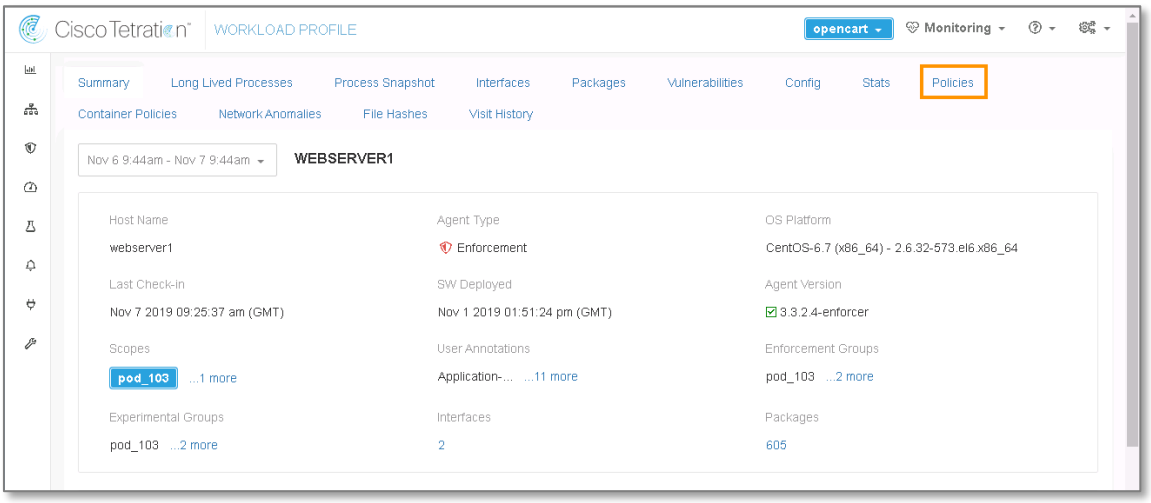
7. （下図で強調表示されている）[Workloads] パネルが開いていることを（クリックして）確認します。



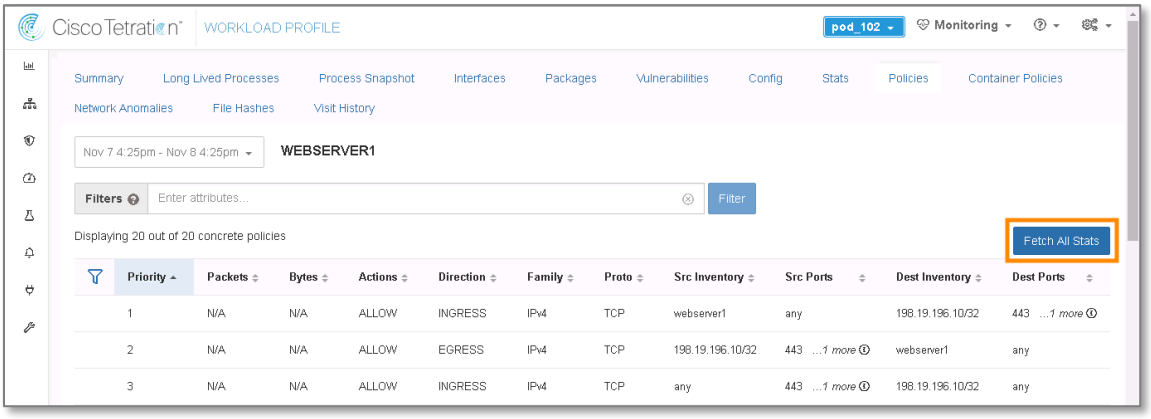
8. リストの一つ目のワークロードをクリックすると、ワークロードが展開されて詳細が表示されます。



9. （上図で強調表示されている）[View Workload in Workload] リンクをクリックすると、完全なワークロードプロファイルが開きます。



10. （上図で強調表示されている）[Policies] をクリックするとタブが開き、エンドポイントにプッシュされたポリシールールが表示されます。

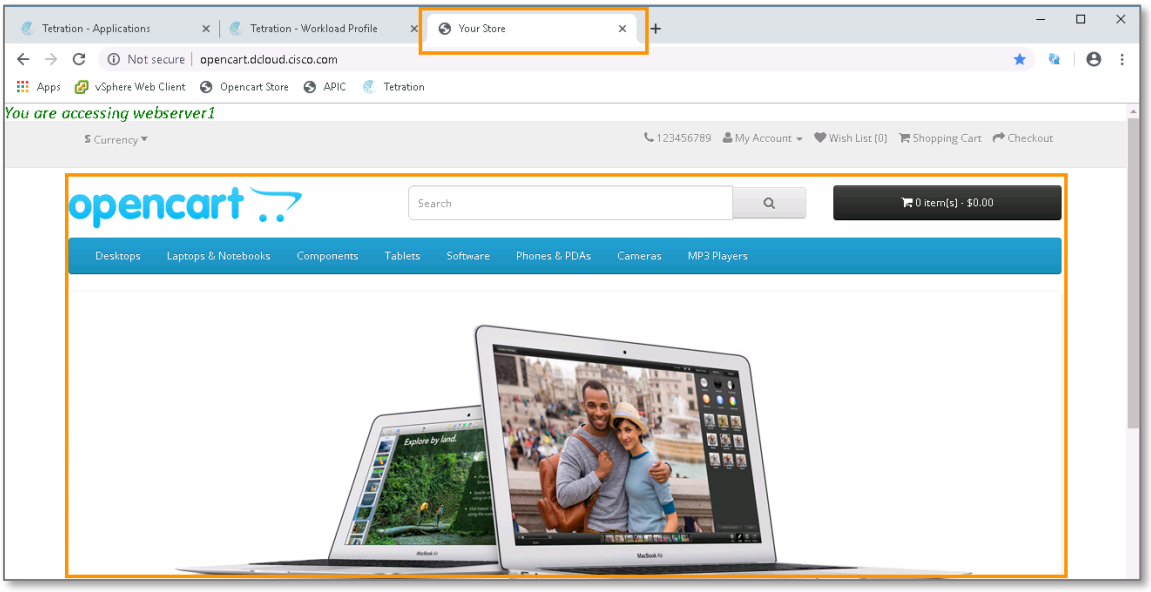


より多くの統計情報を取得するには、以下を実行します。

11. [Fetch All Stats] ボタンをクリックします。

適用後のアプリケーションの可用性テスト

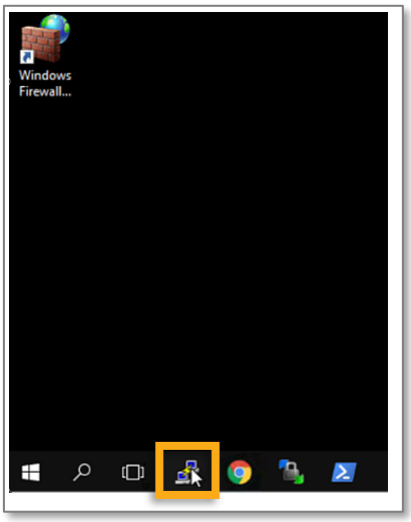
1. wkst1 リモートデスクトップ接続に戻ります。
2. Google Chrome を開き、OpenCart 稼働していること、アプリケーションに影響がないことを確認します。
3. ホワイトリストポリシーによって許可されているフロータイプのみが許可され、それ以外はすべてブロックされます。



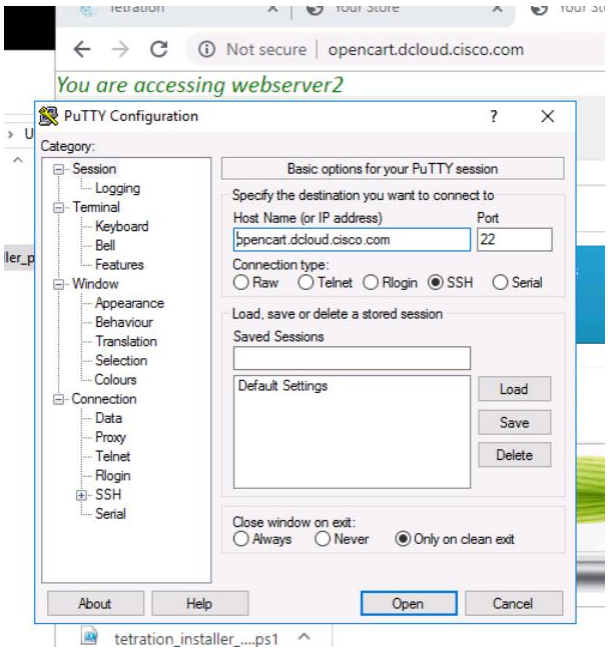
注：いずれかのアプリケーションサーバではなく、デモンストレーション ワークステーションの Google Chrome から OpenCart（opencart.dcloud.cisco.com）にアクセスします。

4. これをテストするには、wkst1 リモートデスクトップ接続から opencart.dcloud.cisco.com に SSH 接続でアクセスします。

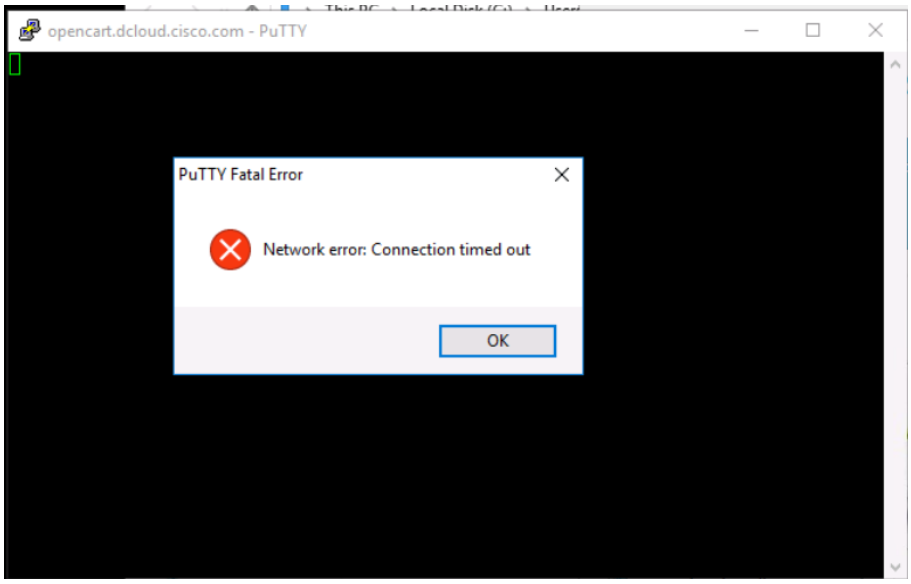
5. wkst1 リモートデスクトップで、タスクバーから「Putty」というアプリケーションを開きます。



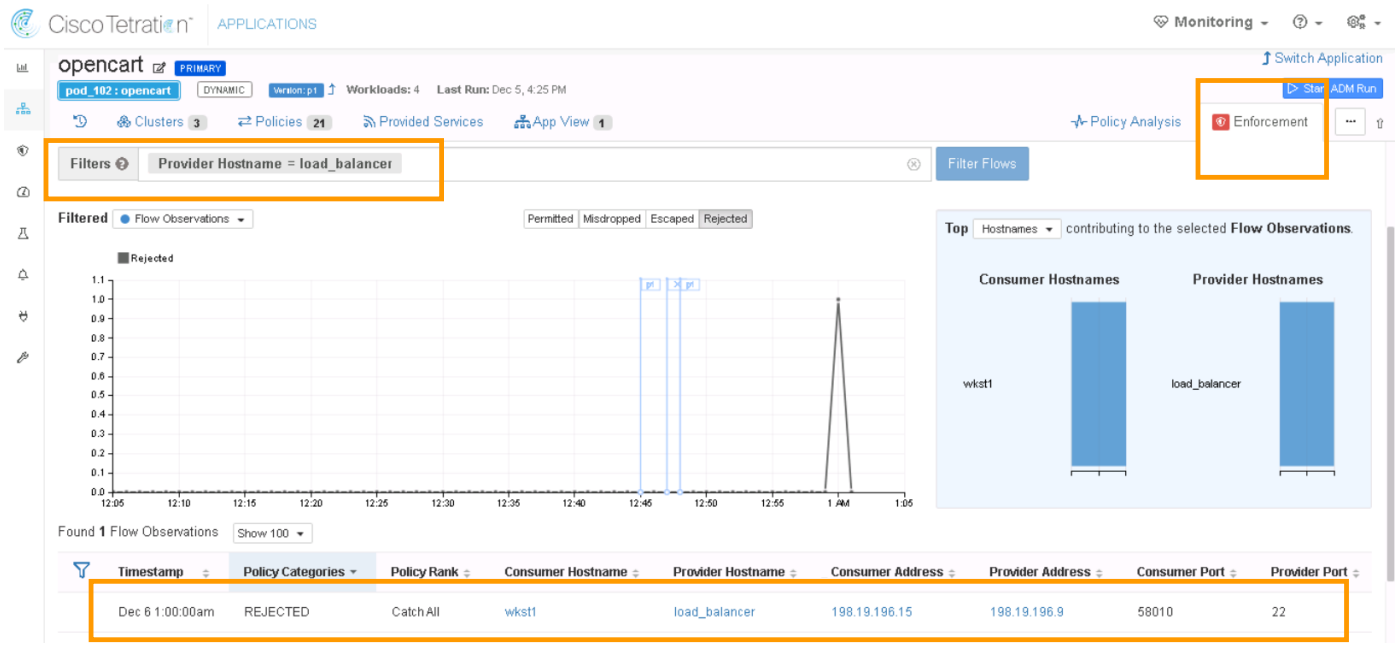
6. [Putty Configuration] ページが表示されたら、SSH 接続するホストとして opencart.dcloud.cisco.com 、Port に 22（SSH）を入力します。



7. [Open] をクリックします。wkst1 はこのエンドポイントに SSH 接続できず、接続がタイムアウトします。



8. この時の通信は、5 分程すると Enforcement の画面にも表れますので確認してください。
   opencart.dcloud.cisco.com のワークロードは Hostname が load_balancer のものです。以下の図のように「Provider Hostname = load_balancer」として表示を絞り込むこともできます。



9. そのほかにも[Select time range]から[Range: 1 hr] 等を選んで調査対象の時間を絞り込んだり、フローの昇順降順の切り替え等お試しください。

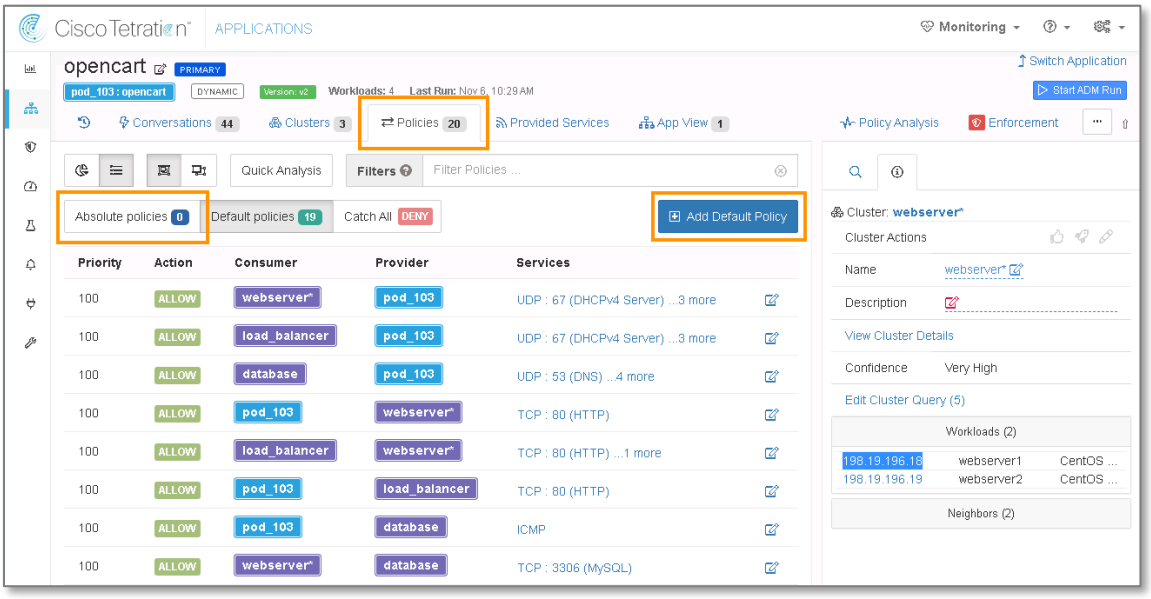
シナリオ 6.　ポリシーのシミュレーションとコンプライアンスのデモンストレーション

このセクションの目的は、Tetration に絶対ポリシーを追加して、データベースサーバと通信するための OpenCart アプリケーション権限で Web サーバを拒否することです。これにより、OpenCart アプリケーションがダウンします。

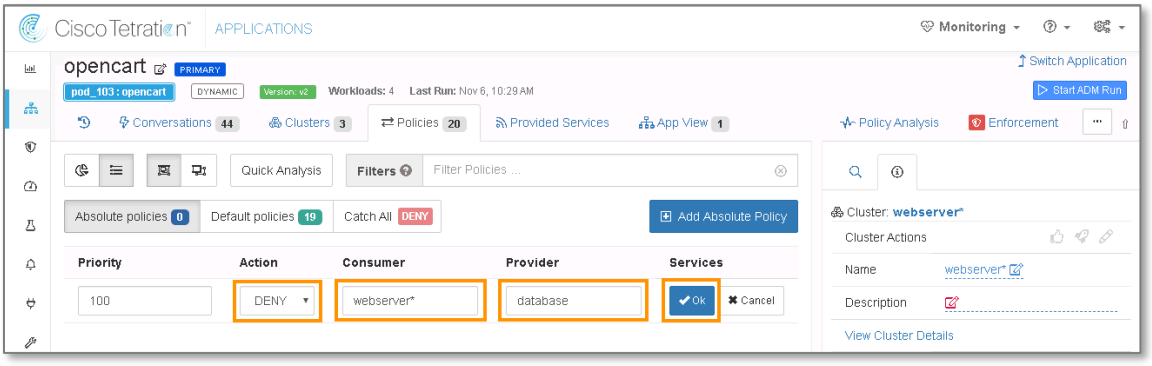
注：絶対ポリシーは、デフォルトまたは catch-all ポリシーの前に適用されます。

手順

1. Tetration の [APPLICATIONS] ページで、[Policies] タブをクリックし、[Absolute Policies（絶対ポリシー）] を選択します。
2. [Absolute Policy] をクリックし絶対ポリシーの追加に進みます。

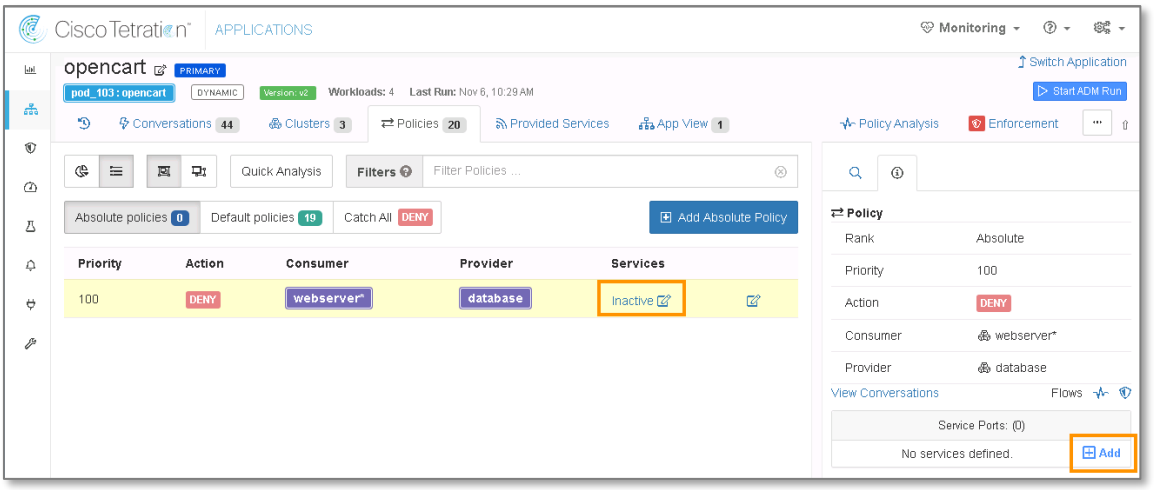


3. [Action] ドロップダウンリストの [DENY（拒否）] をクリックし、[Consumer（コンシューマ）]に[webservers *Cluster] そして[Provider（プロバイダ）] ドロップダウンから[database Cluster]をそれぞれ選択します。[OK] をクリックします。

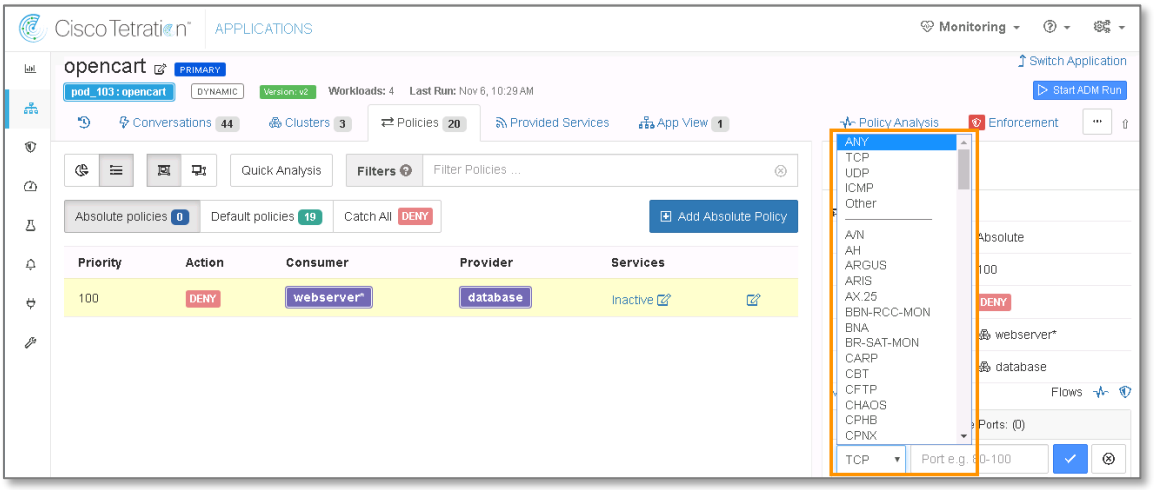


4. Services の下の[Inactive]と表示されているリンクをクリックし、サービス設定を開始します。

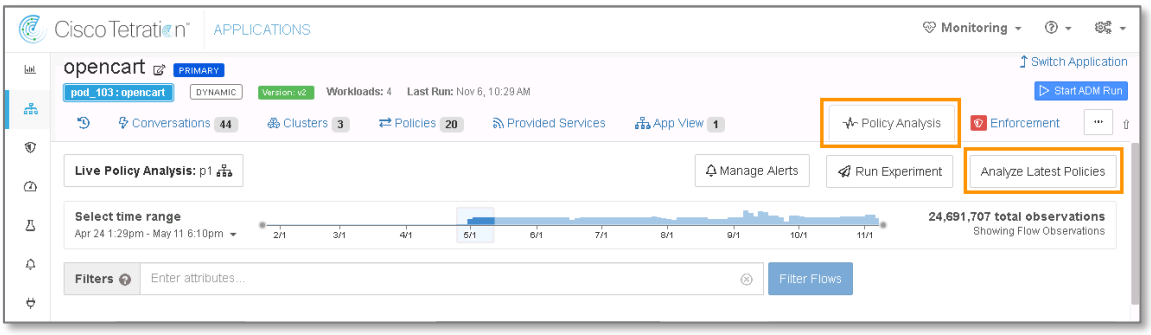
5. UI の右側にあるサービス記述子のブロックで、[Add] をクリックしサービスを追加していきます。



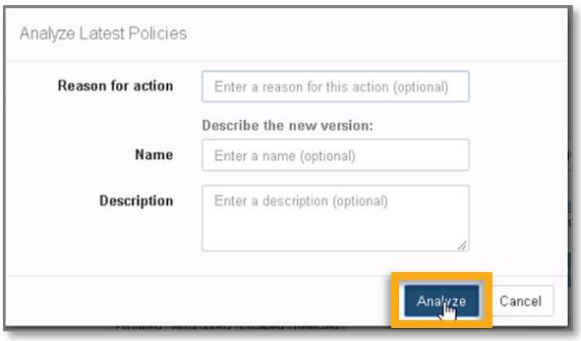
6. Services Ports メニューから [ANY] を選択して、webserver クラスタと database クラスタ間のすべてのトラフィックを拒否します。[OK] アイコン をクリックします。



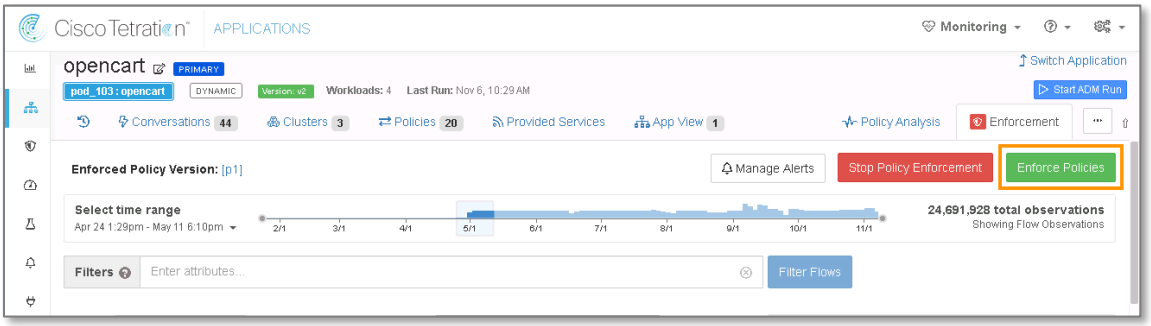
7. [Policy Analysis] タブをクリックし、[Analyze Latest Policies（最新のポリシーの分析）] をクリックして新しいポリシーの影響を判断します。



8. プロンプトが表示されたら、[Analyze] をクリックします。

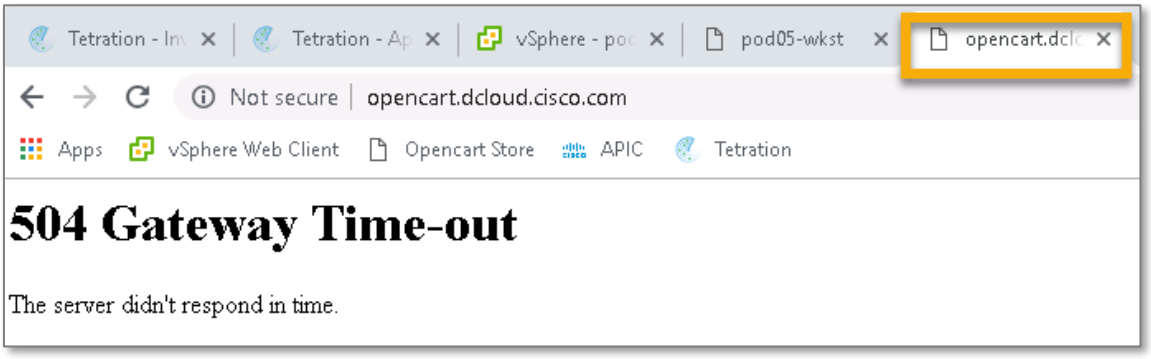


[適用（Enforcement）] タブをクリックし、[ポリシーの適用（Enforce Policies）] をクリックします。



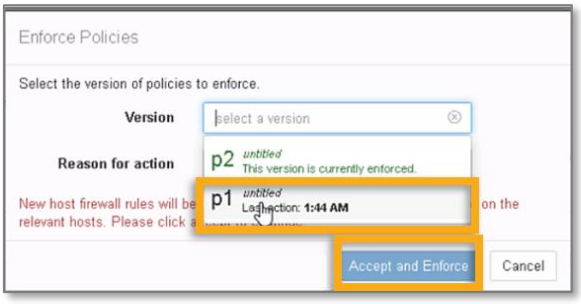
9. [バージョンの適用(Enforce a version)] ポップアップで、ポリシーの最新バージョンをクリックし、[適用(Enforce)] をクリックします。

10. 適用が開始されるまで待機が必要になる場合があります。適用にかかる時間は、ポリシーのチェックインサイクル内におけるワークロードの場所によって異なり、完全なポリシーがプッシュされるまで最大 60 秒かかる場合があります。**pod_xxx workstation** または **wkst1** で、OpenCart アプリケーションの更新を試みます。504 エラーが発生するか、長時間不完全な接続になります。

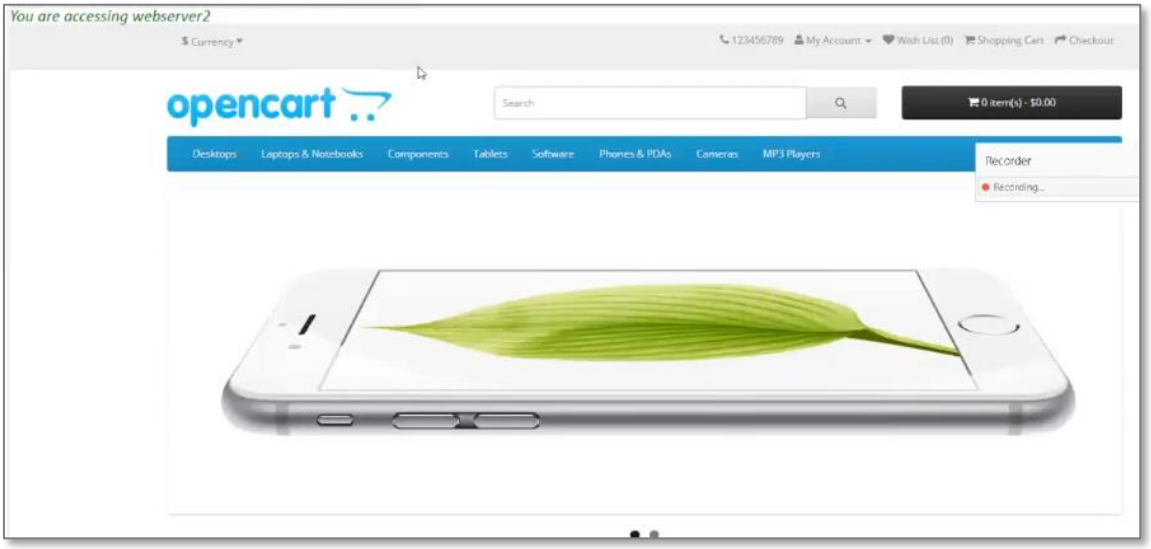


11. 直前に設定したルールのセットを元に戻すために、前のバージョンのポリシーにロールバックしてみましょう。[Enforcement] タブをクリックし、[Enforce Policies] をクリックしポリシーの適用します。

12. バージョンの選択を求められたら、最後のポリシーバージョンを選択して、直前の設定手順で追加した変更をロールバックしてみましょう。次の例では、ポリシーバージョン P1 にロールバックしています。[Accept and Enforce] をクリックして適用します。



13. リモートデスクトップ wkst1 に戻り、サイトが再度機能するかテストします。ポリシーを再度プッシュするには、最大 60 秒待機する必要がある場合があります。



シナリオ 7.　高度なセキュリティ

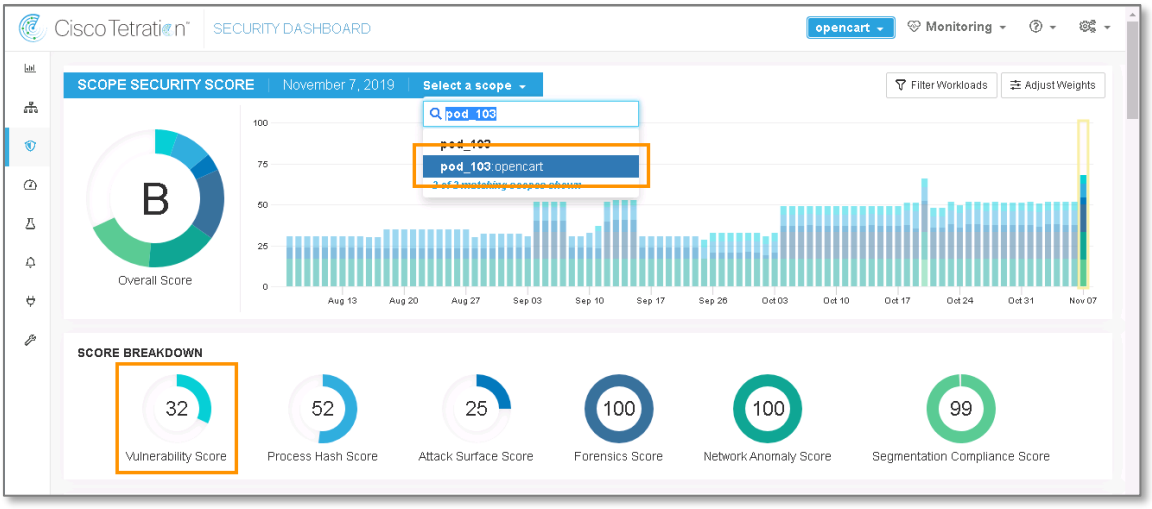
手順

セキュリティダッシュボード

1. UI の左側で、[SECURITY] をクリックし、[Dashboard] をクリックします。

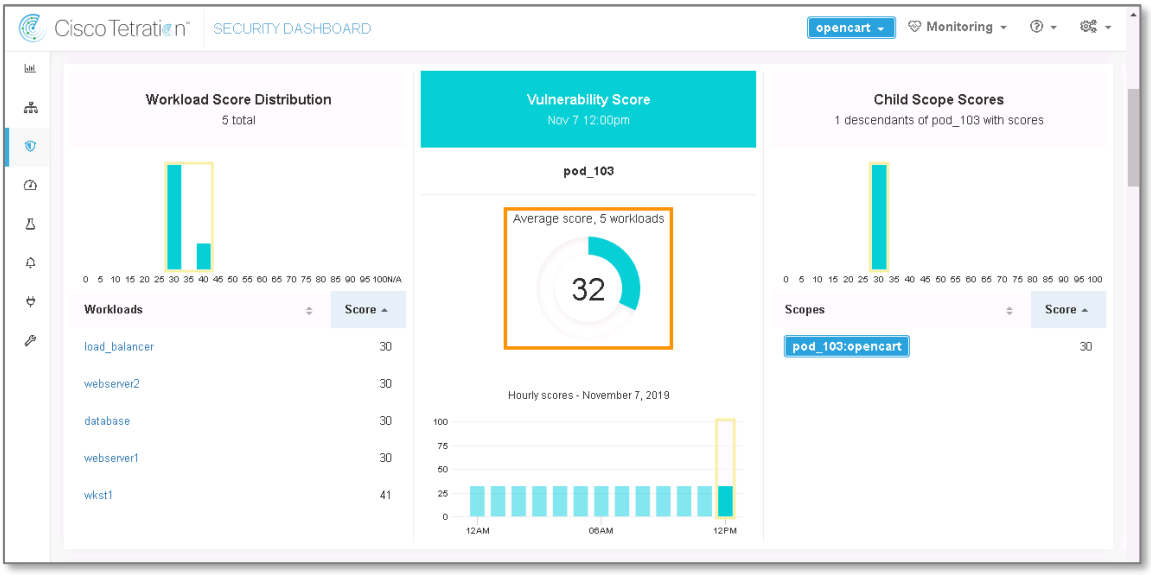
2. ダッシュボードを参照します。

3. opencart の範囲を選択します。このセレクタを使って、ダッシュボードを企業レベル、場所/DC/クラウドレベル、または個々のアプリケーションレベルで表示できます。

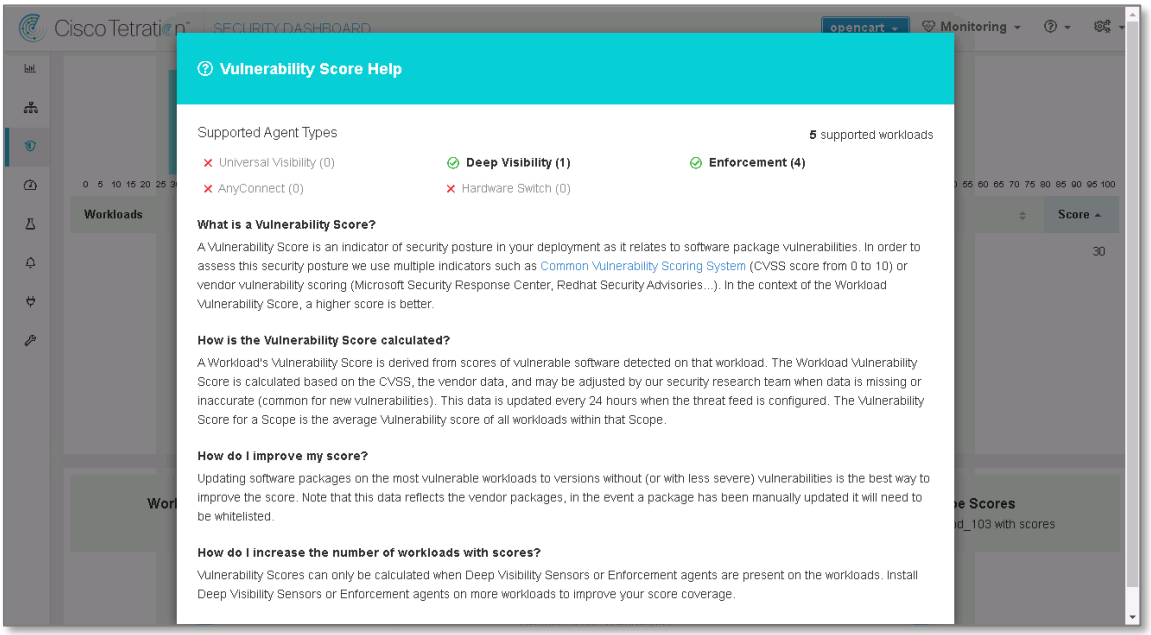


4. [スコアの内訳（Score Breakdown）] セクションまで下にスクロールして、スコア対象の各項目を確認します。

5. スコアの内訳の数字のいずれかをクリックすると、UI がその内訳項目に関する詳細情報に移動します。ここでは、脆弱性スコアの内訳の詳細を示しています。



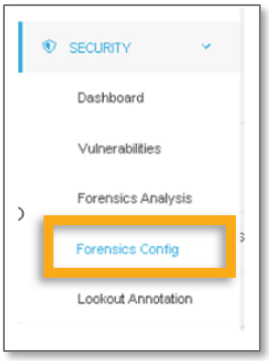
6. スコアの数値にマウスポインタを合わせると、疑問符のカーソルが表示されます。これは、この数値に関する詳細な説明があることを示しています。この数値をクリックすると、プラットフォーム アルゴリズムにおけるこのスコアの計算方法の詳細が示されます。



7. 他のスコアの内訳セクションで各項目をクリックして自由に確認してください。

フォレンジック

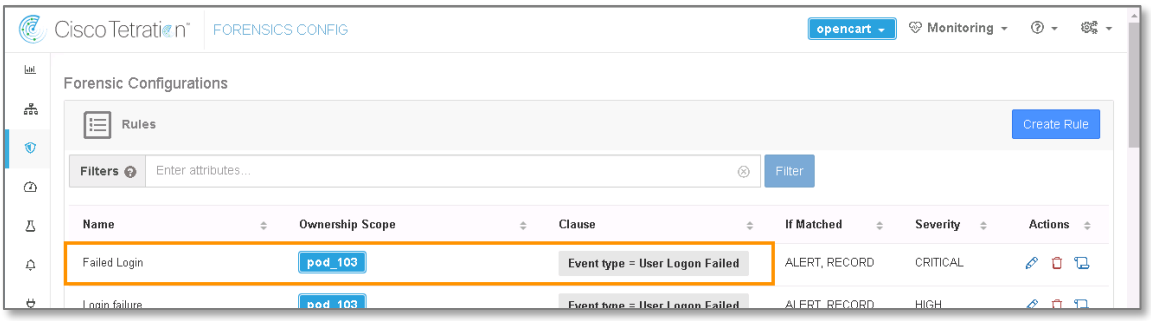
1. UI の左側で、[SECURITY] をクリックし、[Forensics Config（フォレンジック設定）] をクリックします。



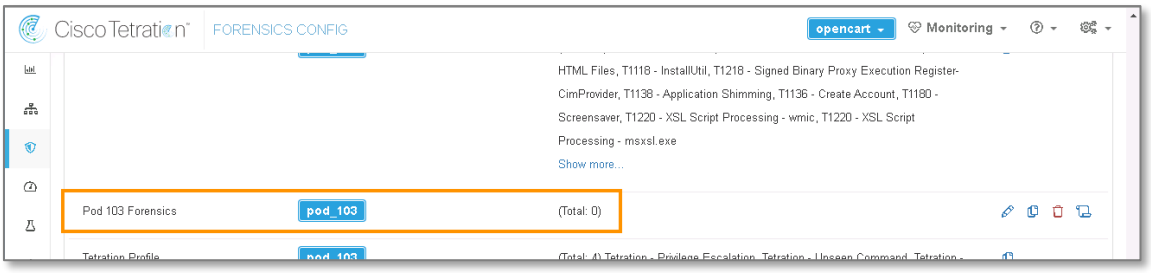
2. フォレンジックの設定ページは 3 つの部分に分かれています。[フォレンジックルール（Forensics Rules）]、[フォレンジックプロファイル(Forensics Profiles)](ルールのグループ)、[フォレンジックインテント(Forensics Intents)]（プロファイル/ルールが範囲/アプリケーションに適用される）です。

3. ユーザログインの失敗に関するルールが作成されています。ルール、プロファイル、およびインテントが作成されると、次のように表示されます。これらを表示するには、下にスクロールする必要がある場合があります。[ルール（Rules）] ページでは、結果の「ページ 2」をクリックして表示することもできます。

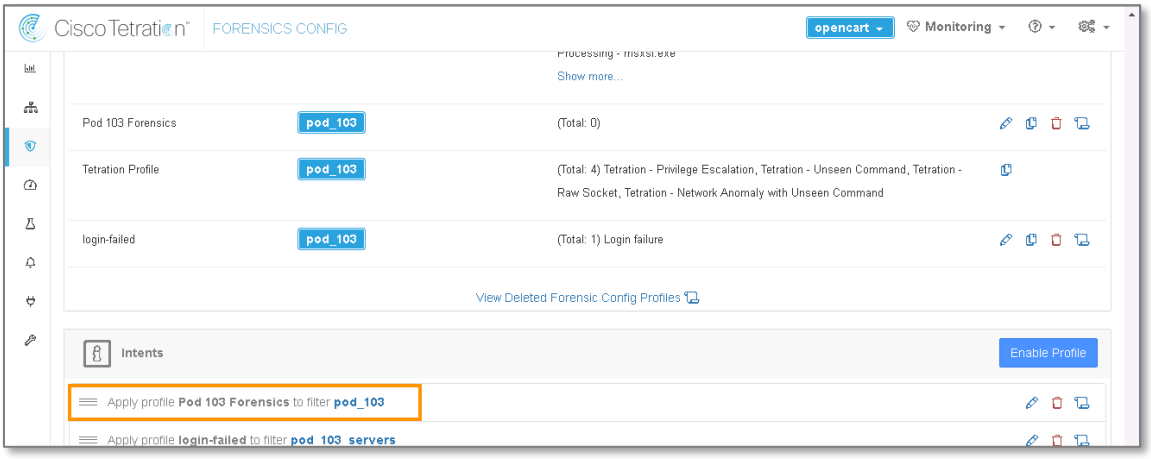
   ルールの設定は次のとおりです。



   プロファイル設定は次のとおりです。



   フォレンジックインテントは次のとおりです。



4. この設定例は非常にシンプルですが、ラボユーザがトリガーされたイベントに直接関係するものを表しています。

5. ルール、プロファイル、およびインテントを作成する方法を説明します。上部にある [Create Rule] をクリックします。

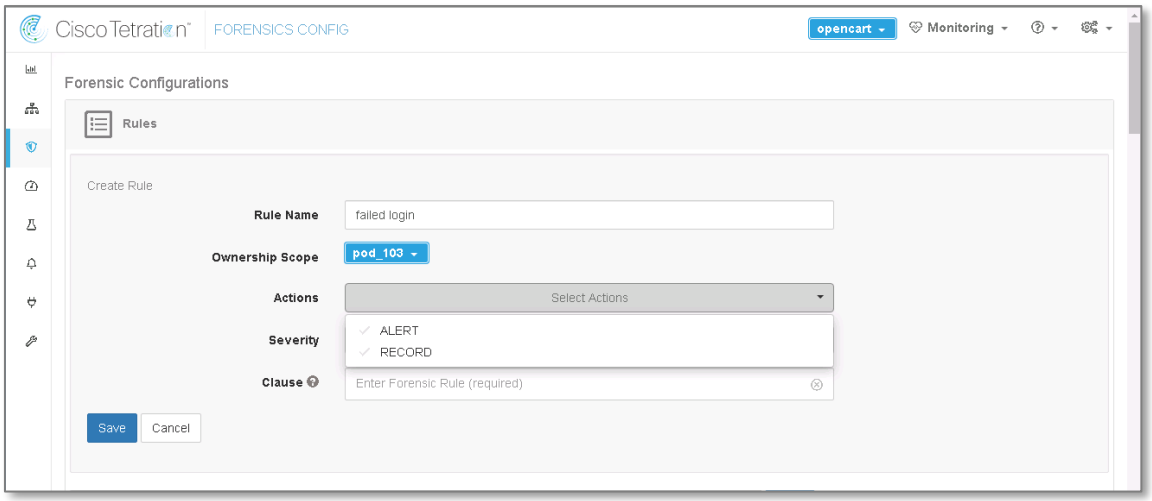
6. ルールに「Failed Login」という名前を付け、次のようにルールを設定します。

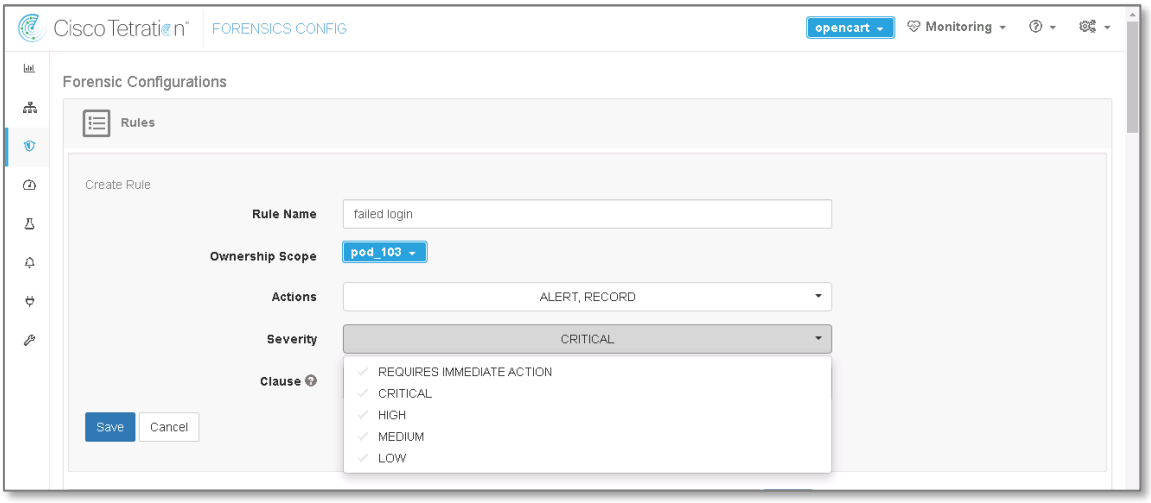
   a. 範囲：pod_XXX。特定のポッドを選択します。お使いのポッドですでに作成済みのものが表示されている場合は pod_*XXX_MMDD(日付)*のように別のものを作成してください。

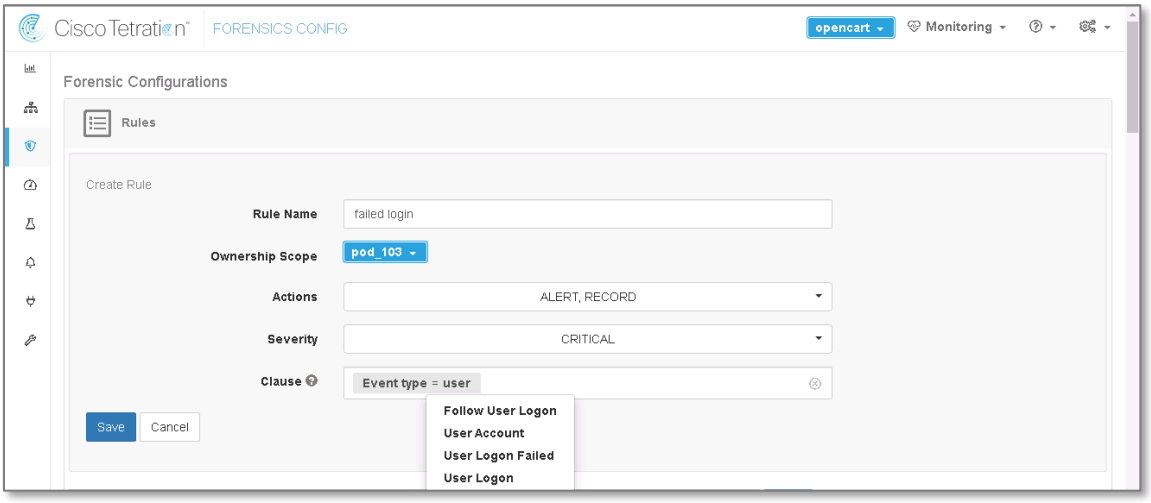
   b. アクション：[ALERT（アラートを発報）]、[RECORD（記録する）]。

   c. 重大度：[CRITICAL（重要）]（または任意の重大度）。

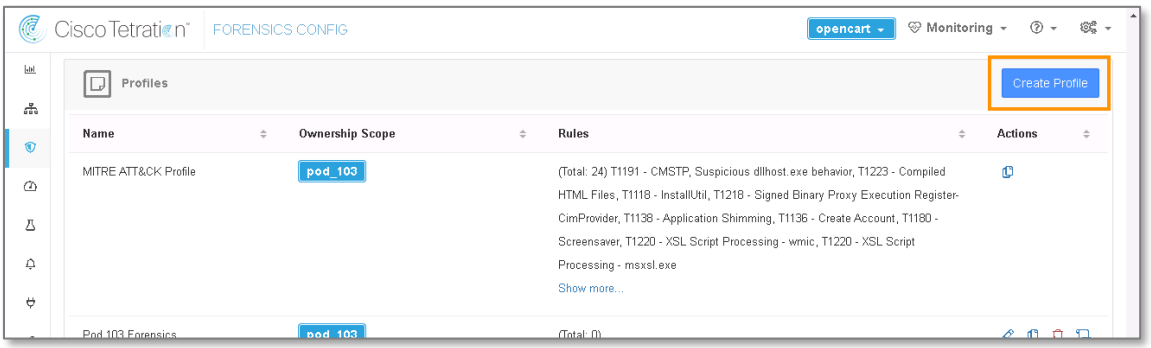
   d. 条件：[Event type]=[User Logon Failed（ユーザログインの失敗）]。



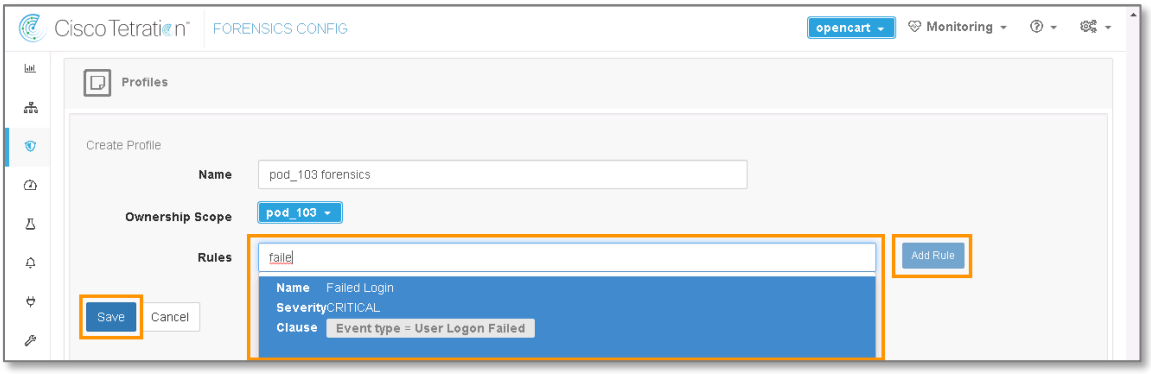




7. この設定はプロファイルで参照できます。[Create Profile] をクリックしプロファイルの作成に移ります。

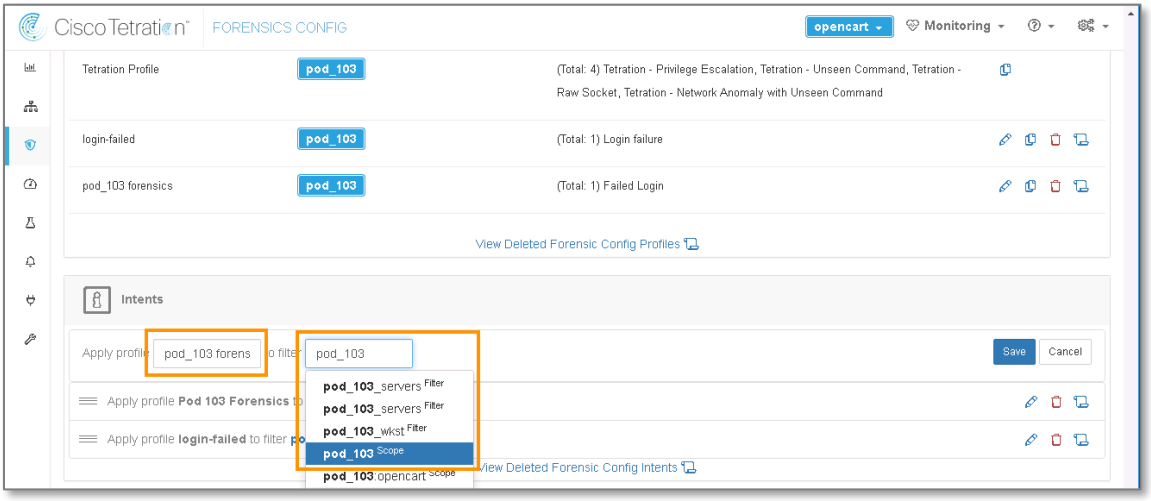


8. ここで、作成したルールをプロファイルに追加します。プロファイルに名前を付け、[Rules] ボックスをクリックして、入力を開始します。先ほど作成したルールの名前を使用します。これにより、リストがドロップダウンされます。ルールを選択し、[Add Rule] をクリックします。そのルールが追加されたら、[Save] をクリックし保存します。

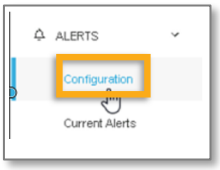


9. 次に、プロファイルやルールを範囲またはアプリケーションに適用するインテントを作成する必要があります。[Enable Profile] をクリックします。

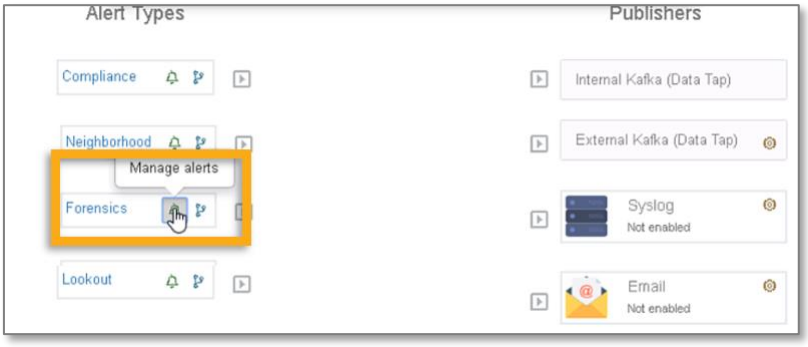
10. 次に示される入力で、適用するプロファイルとそのプロファイルを適用する範囲/アプリケーションを選択します。



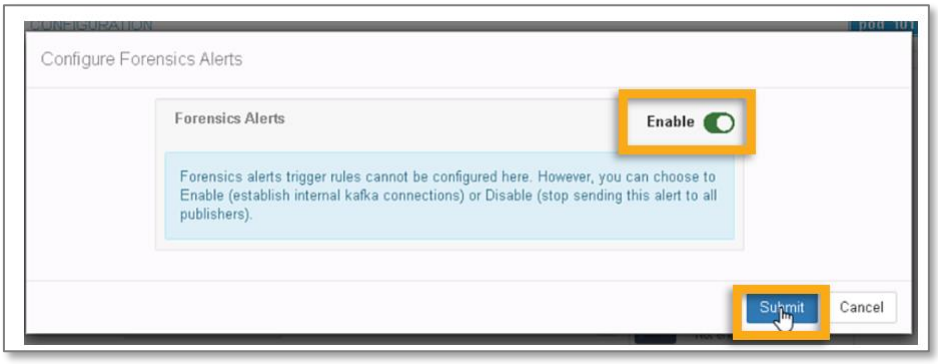
11. また、アラートがまだ有効になっていない場合は、オンにしてみましょう。UI の左側にある [ALERTS] -> [Configuration] をクリックし設定を確認します。



12. アラートの設定ページが表示されます。フォレンジックの基本アラートを有効にしてみましょう。[Forensics] の [Manage alerts（アラートの管理）] をクリックします。



13. スライダをクリックしてアラートを有効にし、[Submit] をクリックします。



14. 次に、設定したスコープにあるワークロードに対して意図的にログインの失敗をし、イベントをトリガーしましょう。

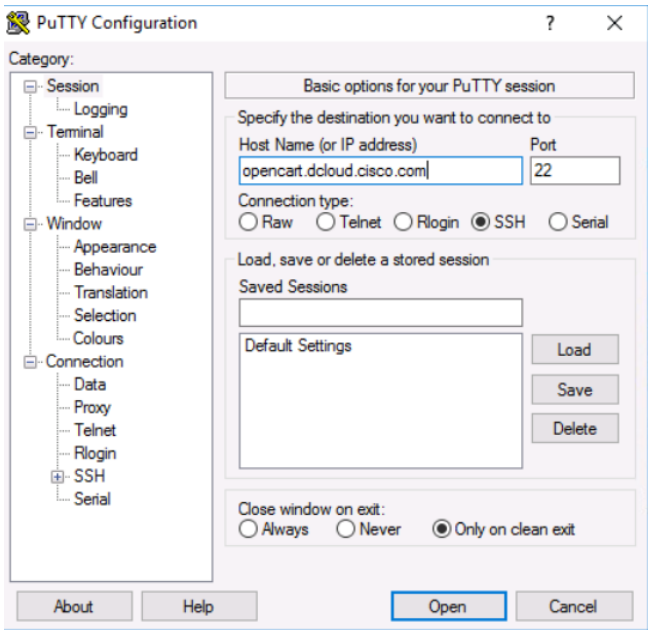
    ※この時点でポリシーが Enforce(適用)されている場合はここでは一旦それを止めます。そのためには UI の左から  [APPLICATIONS]をクリックし[Enforcement]タブから[Stop Policy Enforcement] 

    を押します。次に出てくる画面で[Accept]を押してポリシーの適用を止めます。（ポリシーの反映に 1 分ほどかかることがあります）

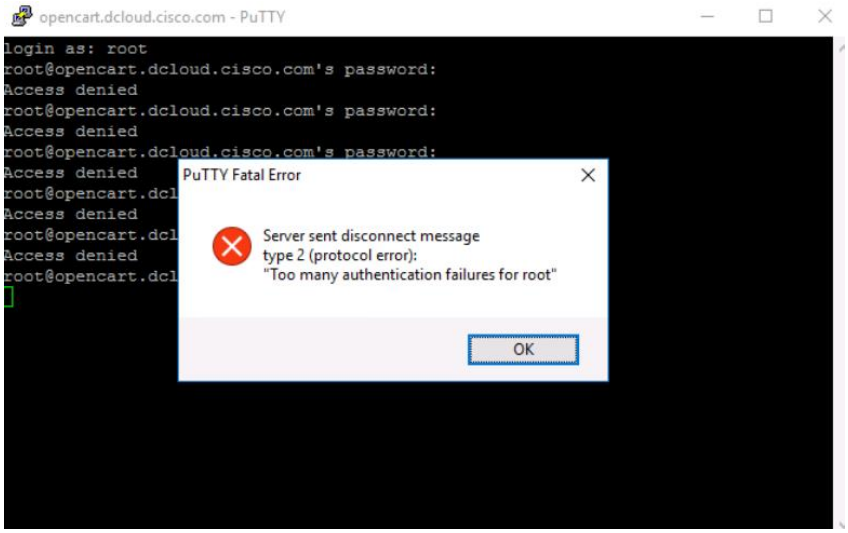
15. リモートデスクトップ先の wkst1 で、PuTTY を起動します。

16. Host Name に opencart.dcloud.cisco.com と入力し Port は 22(Connection type: SSH)を入力します。

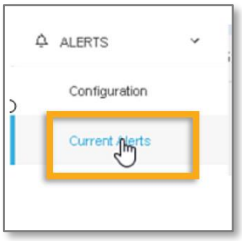
    (load_balancer への SSH アクセス)



17. [Open] をクリックします。ログインするウィンドウが開いたら、ユーザ名「root」を入力し、ランダムなテキストを入力して意図的にログインを失敗します。

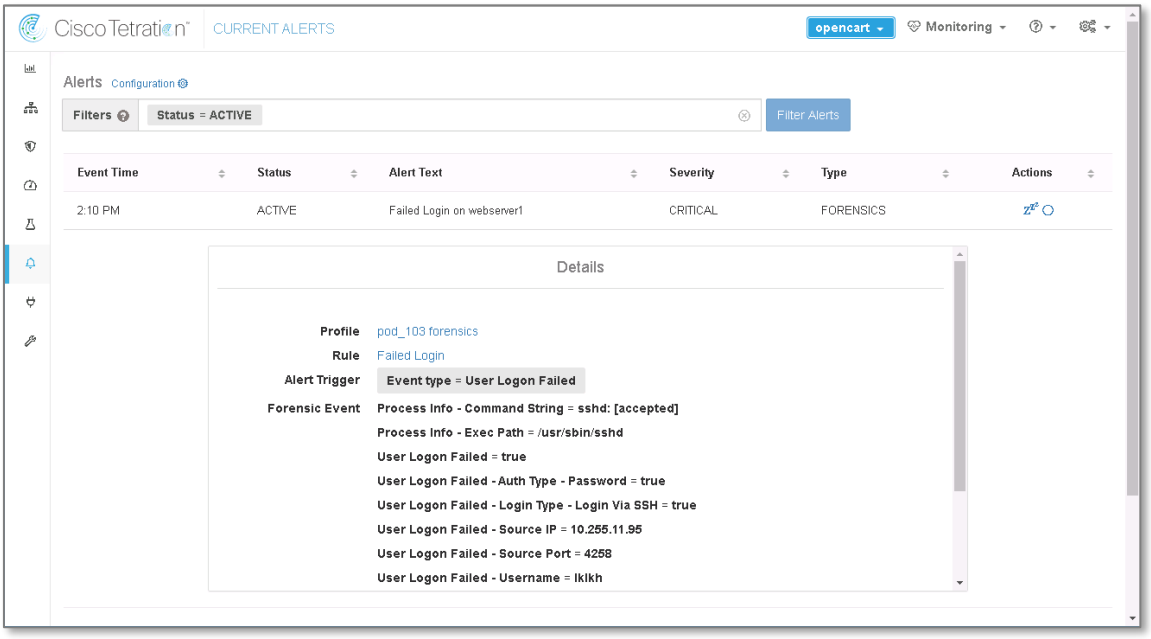


18. 次に、プライマリーのワークステーションに戻ります。Tetration の UI で[ALERTS]の[Current Alerts]からアクティブなアラートを確認します。

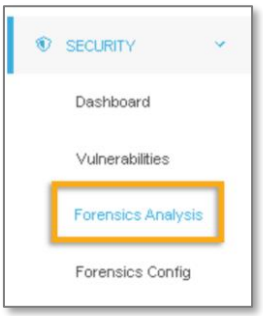


19. アラートとフォレンジックのアラートはほぼリアルタイムで行われますが、UI の表示はバックエンドの処理より数分遅れます。アラートとフォレンジックイベントが UI に表示されるまでに、1 ～ 2 分かかる場合があります。先ほど作成したトリガーイベントに関連するアラートをクリックします。

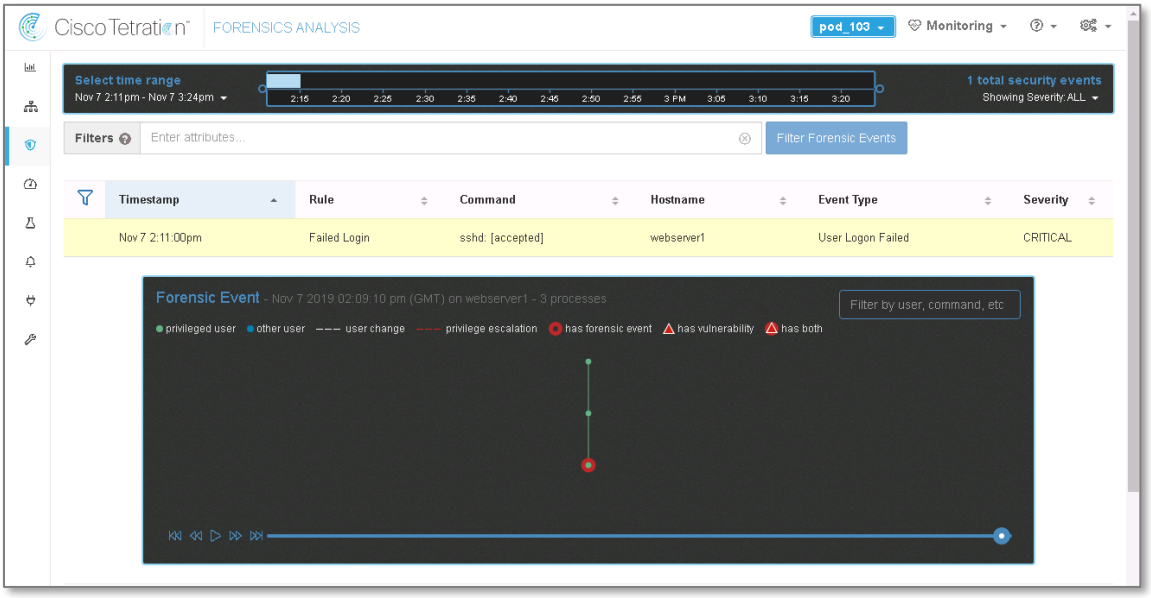
20. これにより、アラートで報告されたイベントの詳細情報が公開されます。この詳細情報は、設定されているどのアラートでも示されます（電子メール、Slack、syslog など）。



21. 次に、イベントのフォレンジックの詳細を見ていきましょう。UI の左側にある [SECURITY] -> [Forensics Analysis] をクリックします。



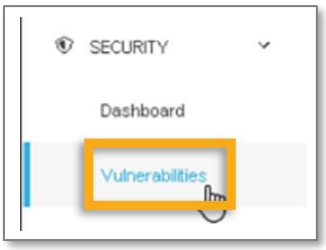
22. フォレンジックイベントのリストが表示されます。イベントをクリックすると、イベントに関するフォレンジック情報と、イベントの前後に何があったかを把握できます。現在表示されているのは非常にシンプルでユーザ対話型のイベントであるため、このイベントの詳細情報は非常に少量です。



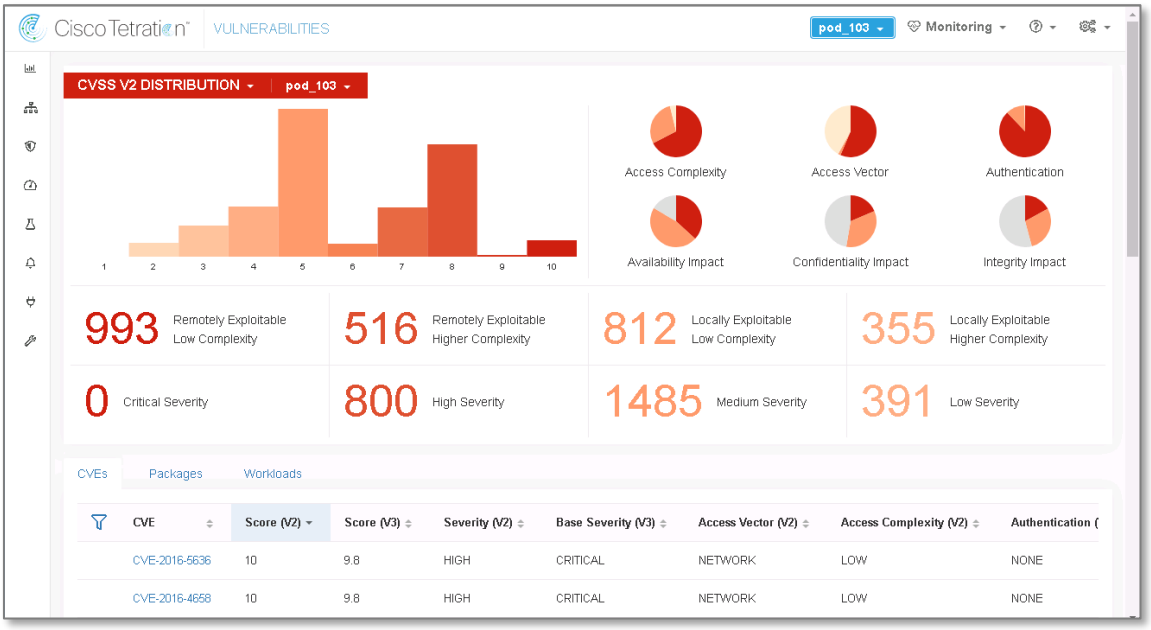
23. このフォレンジックの詳細レコードはインタラクティブです。マウスを動かして結果を操作します。強調表示されたイベントをクリックし、イベントから取得できる詳細レベルを確認します。

脆弱性の特定とアクション

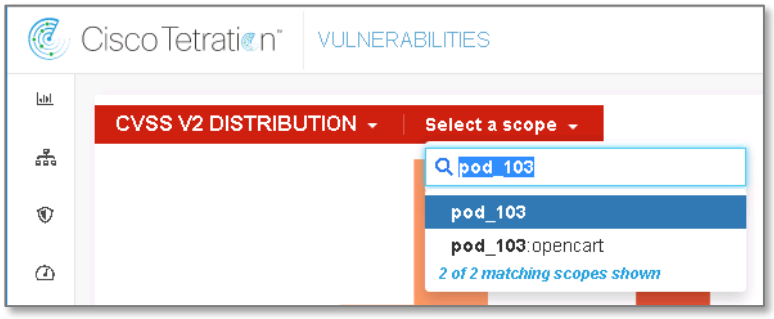
1. UI の左側で、[SECURITY] をクリックし、[Vulnerabilities（脆弱性）] をクリックします。



2. [Vulnerabilities（脆弱性）] ダッシュボードを参照します。このダッシュボードで範囲を変更して、組織、場所、運用会社、クラウド/データセンターから個々のアプリケーションまで、さまざまなディメンションで脆弱性の悪用を表示できます。

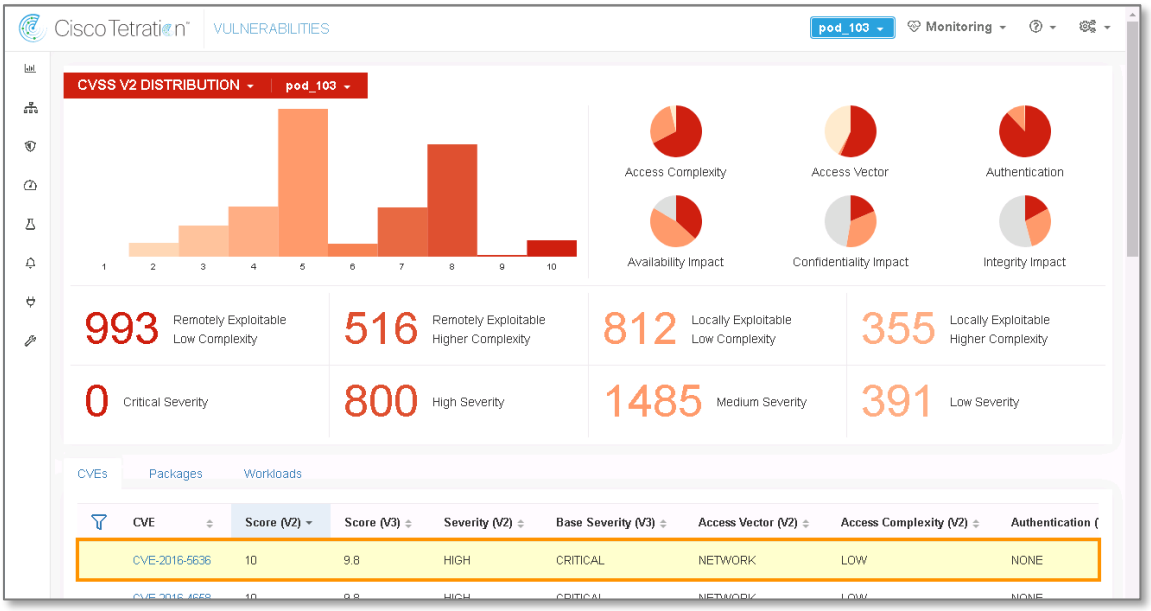


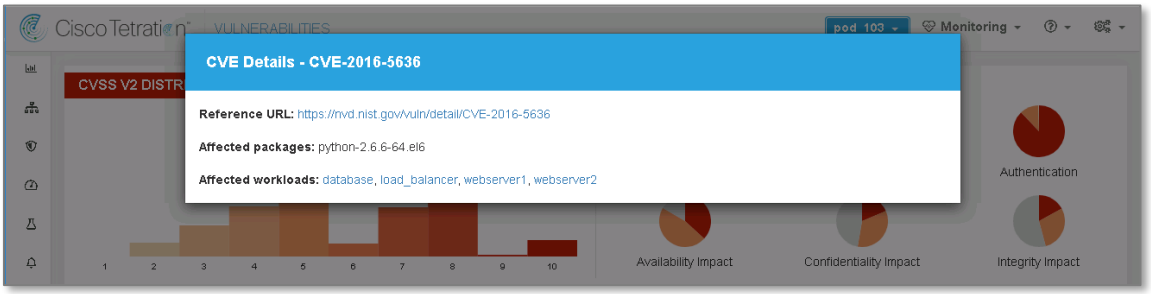
3. さまざまな範囲と各種スコア分布を確認します。



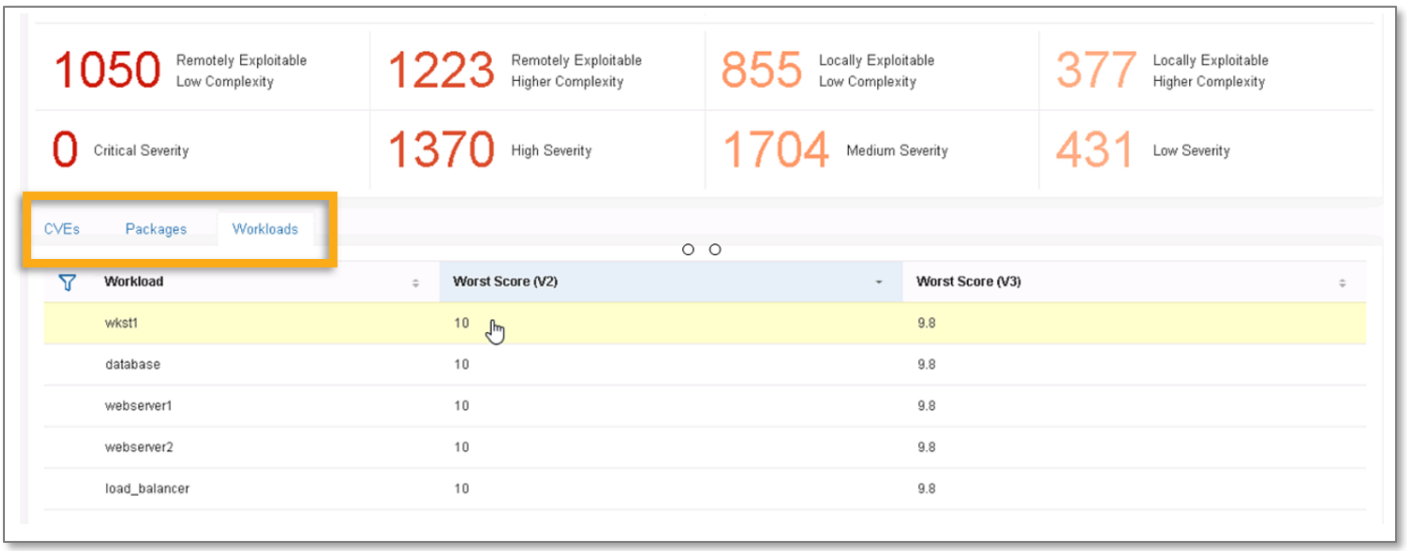
4. いくつかのカテゴリをクリックして、表示がどのように変更されるかを確認します。UI のほぼすべてのカテゴリはクリック可能で、データを別の方法で視覚化できます。

5. 下部のいずれかの行をクリックすると、詳細が表示されます。



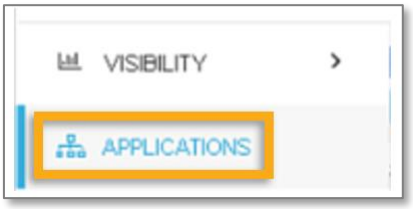


6. 次に、[Packages] と [Workloads] をクリックして、データを可視化するさまざまな方法を確認します。

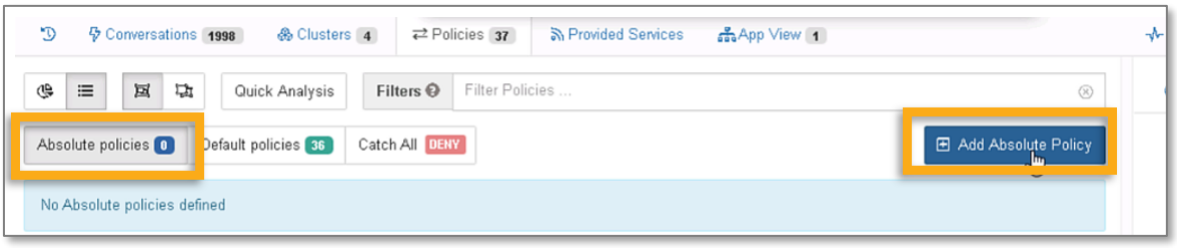


7. 次に、そのデータを使用して何かアクションを実行してみましょう。

8. 左側のツールバーの [APPLICATIONS] をクリックします。

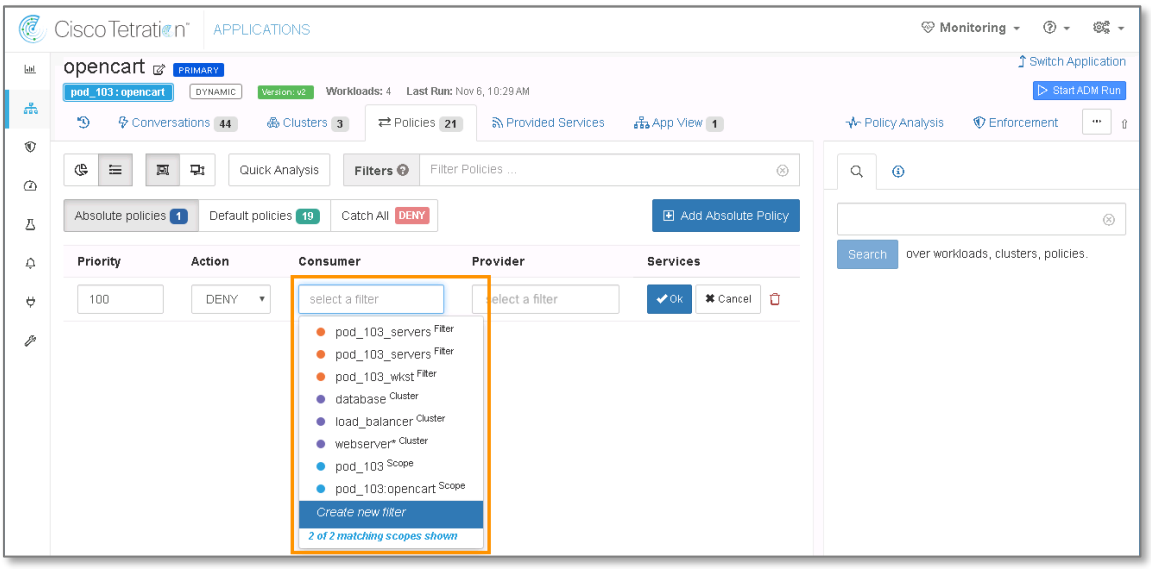


9. [Policies] をクリックし、[Absolute Policies] をクリックします。

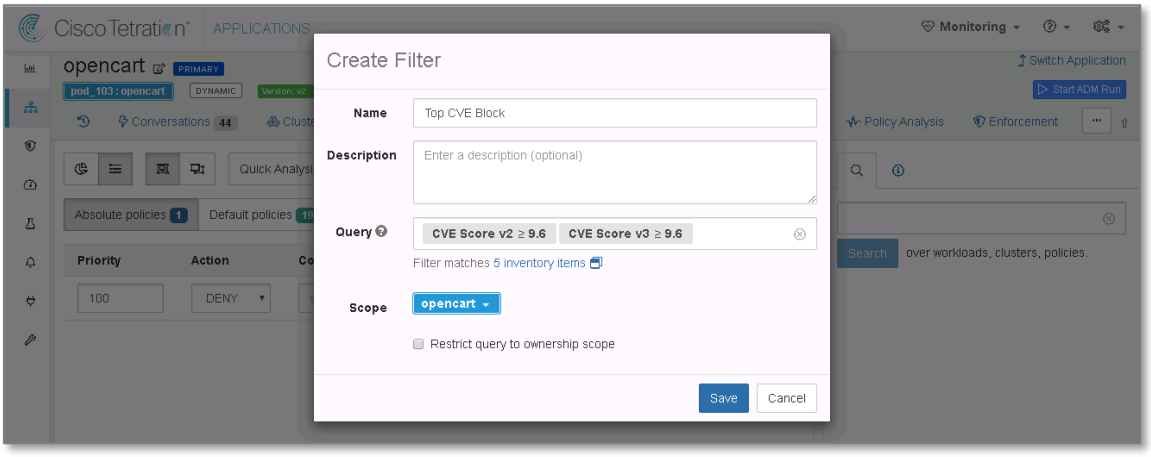


10. 新しい Absolute Policy を作成してみましょう。

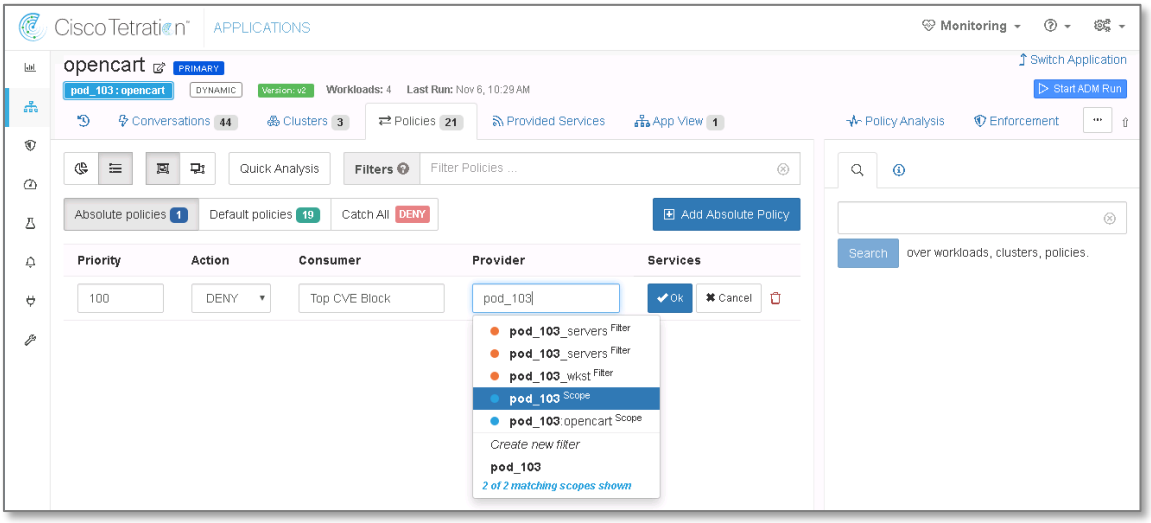
11. このフィルタはまだ作成されていないため、このポリシーのコンシューマのドロップダウンボックスにある [Create new filter] をクリックします。



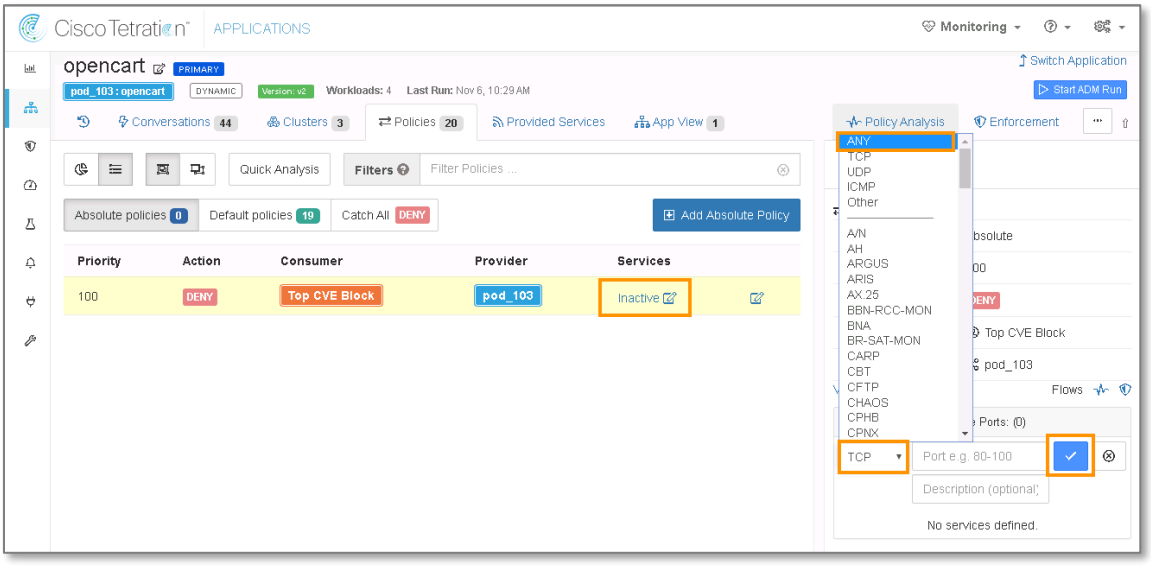
12. 次に示す設定を使用して、Top CVE Block などの名前でフィルタを作成します。これにより、CVE v2 および v3 スコアが 9.6 以上の、opencart アプリケーションのすべてのワークロードに一致する柔軟なフィルタが作成されます。これらのワークロードのいずれかが修復されて、スコアが高いパッケージにパッチが適用されるか、パッチが削除された場合、これらのワークロードは、このフィルタリストの結果から完全に削除されます。



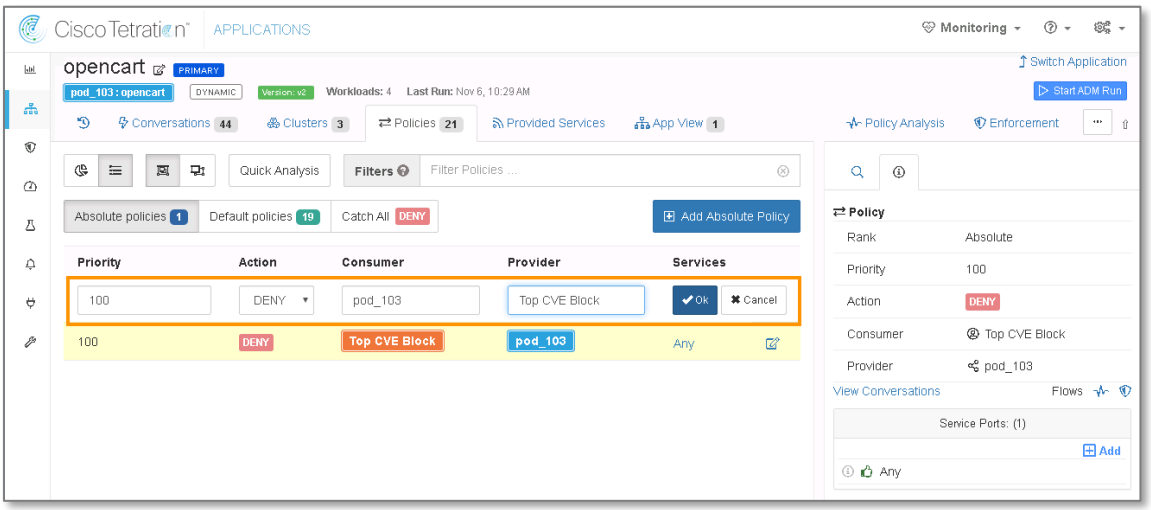
13. このフィルタは、ポリシーを作成する際に活用できます。このような高い CVE スコアを持つワークロードが、アプリケーションの外部に接続することを拒否するポリシーを作成しましょう。この例では、「pod_xxx」という範囲を選択します。これは、未知のネットワーク（インターネットなど）を含むその上位レイヤにある他のノードを意味します。



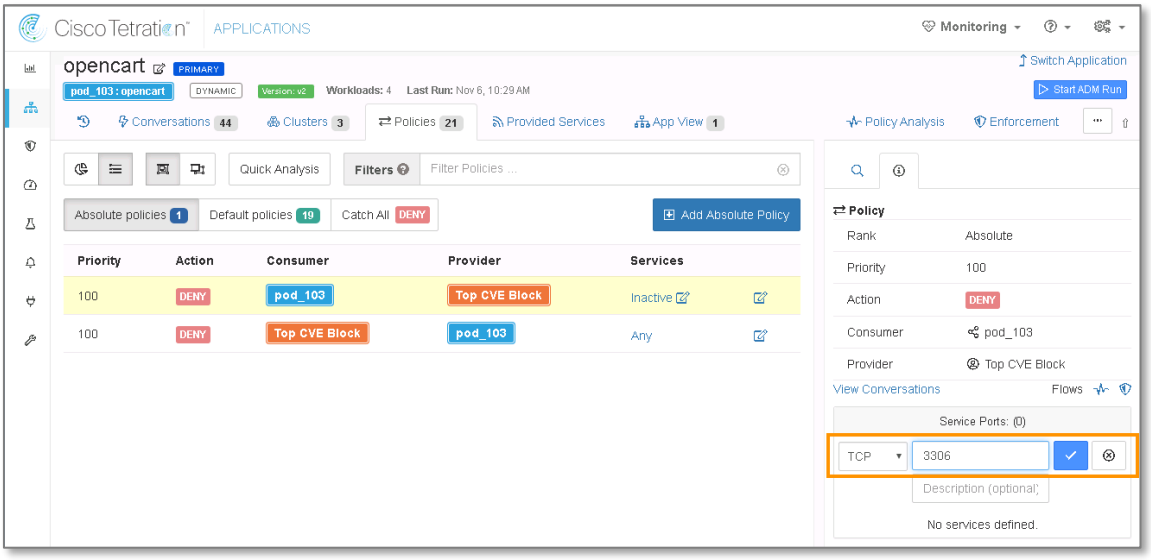
14. 次に、このタイプの通信フローでブロックするサービスを定義します。すべてをブロックするか、特定のトラフィックのみをブロックする制限を設定できます。たとえば、MS ファイル共有サービスに対する脆弱性を持つ Windows サーバの TCP 445 をブロックすることができます。この例では、すべてのタイプの接続をブロックしてみましょう。[非アクティブ（Inactive）] サービス定義を選択し、[任意（Any）] を選択して、チェックマークをクリックします。



15. 次に、反対方向の（着信）トラフィックに固有なサービスを定義してみましょう。別の絶対ポリシーを作成してみます。[絶対ポリシーの追加（Add Absolute Policy）] をクリックし、先ほど作成したものと同じフィルタを使用してポリシーを作成します。これは、（直前の手順で作成した Top CVE Block フィルタを使用して）pod_xxx（デフォルト）から上位 CVE 攻撃者へのトラフィックを拒否します（最後の手順で作成した Top CVE Block フィルタを使用します）。



16. TCP 3306 のサービスを定義して、着信 SQL トラフィックをブロックしてみましょう。



これをテストする場合は、[適用（enforcement）] に移動して [最新のポリシーを適用（Enforce latest policies）] をクリックします。Tetration は、ここで作成したポリシーを取得し、以前検出したデフォルトポリシーよりも前にそれらのポリシーを適用します。これにより、アプリケーション規制ルールに到達する前に、このリスクの高いトラフィックをブロックすることができます。

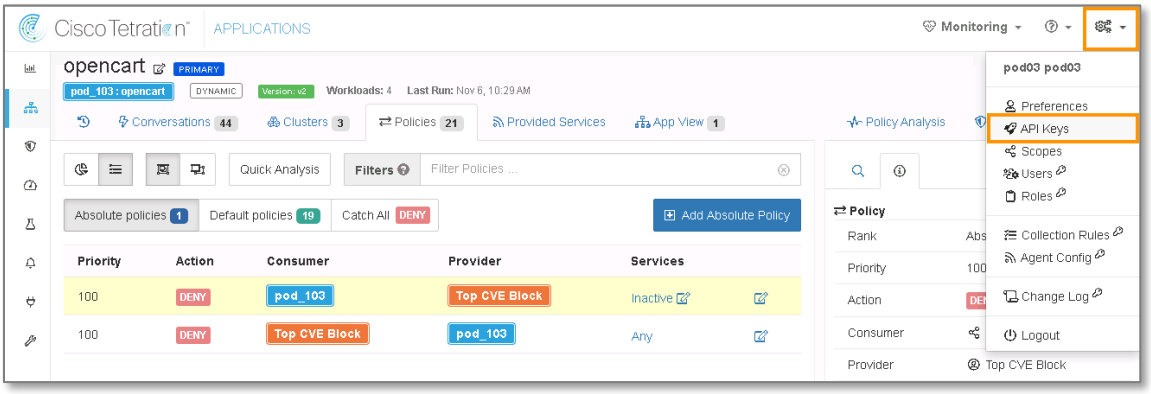
付録 A.　（付録 1）REST API のデモンストレーション

このセクションの目的は、RestClient をインストールした後に、Tetration で API キーを作成し、API の統合を示すことです。

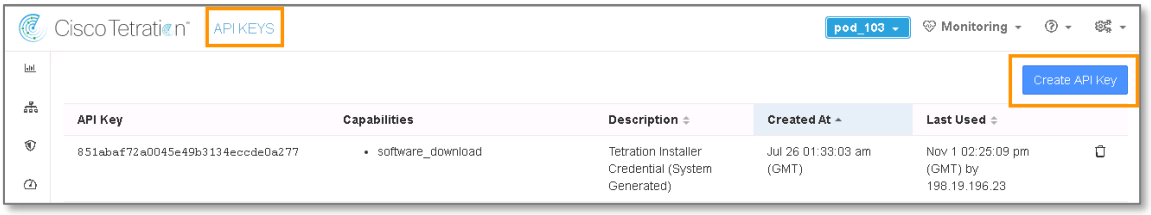
手順

API キーの作成

1. [Tetration] タブで、サイドメニューの [設定（Settings）] > [API キー（API Keys）] をクリックします。



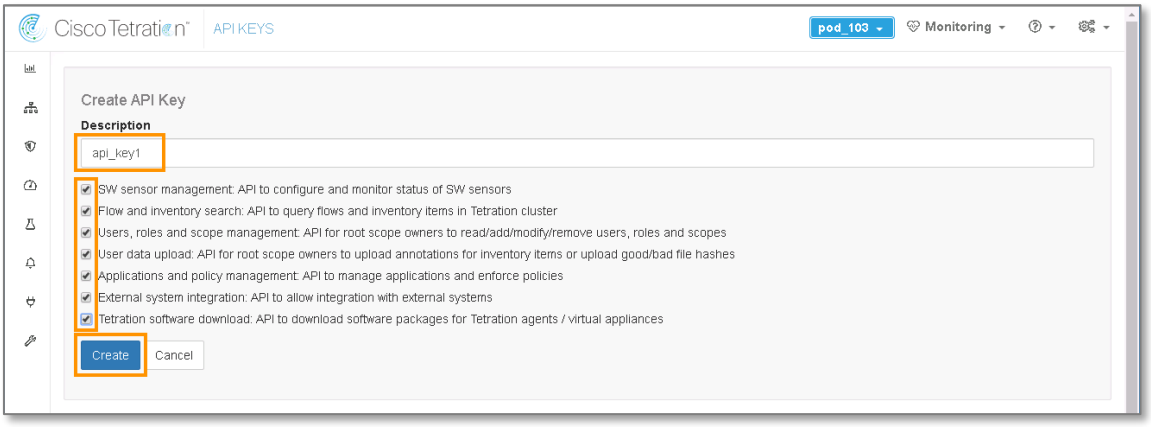
2. [API キーの作成（Create API Key）] をクリックします。



3. [API キーの作成（Create API Key）] ウィンドウで、API キーに名前 api_key1 を付けます。

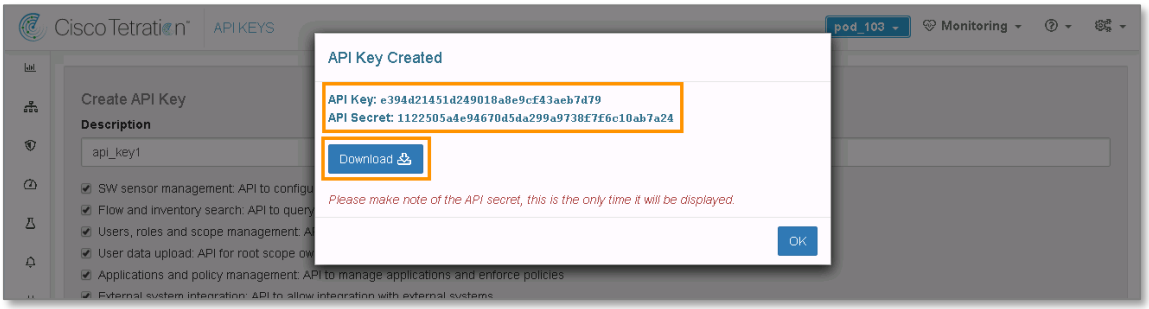
4. API **を使用する対象の操作**を選択します。[作成（Create）] をクリックします。

注：ユーザは、リスト内の 1 つの機能、複数の機能、またはすべての機能を選択できます。

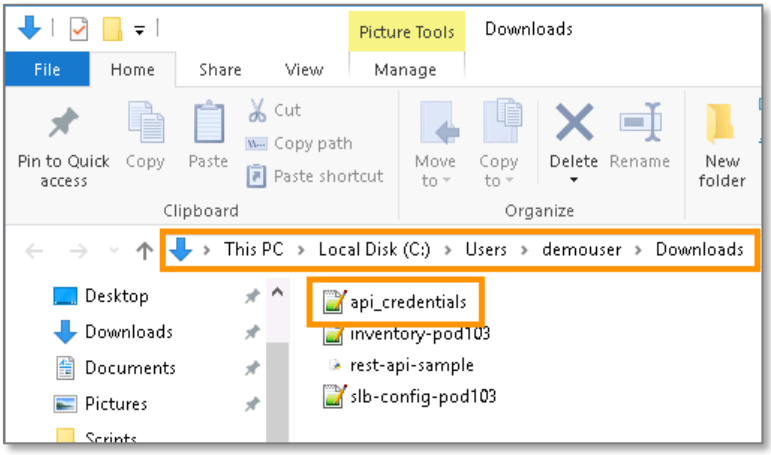


5. API シークレットをメモして、[ダウンロード（Download）] をクリックします。API シークレットは再度表示されません。

注：API シークレットを忘れたり紛失した場合、新しい API シークレットを生成できます。

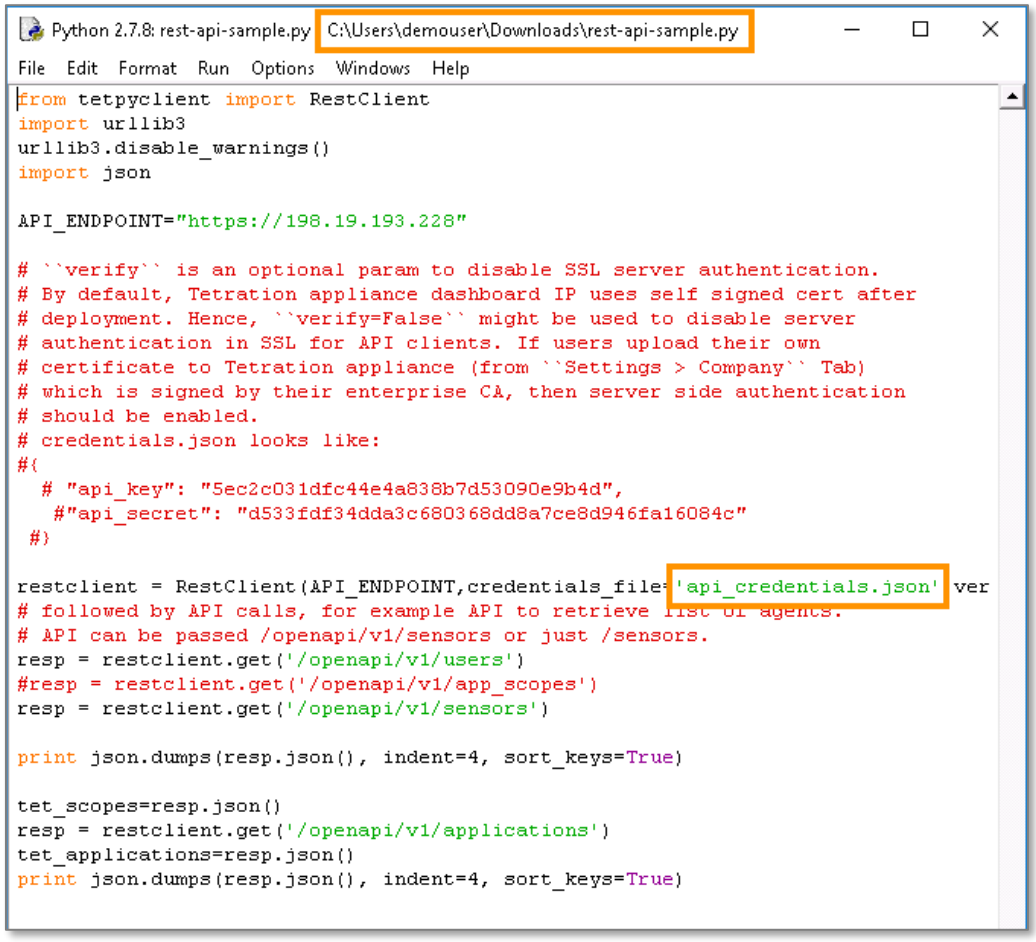


6. Downloads フォルダに api_credentials.json ファイルがあるかどうかを確認します。



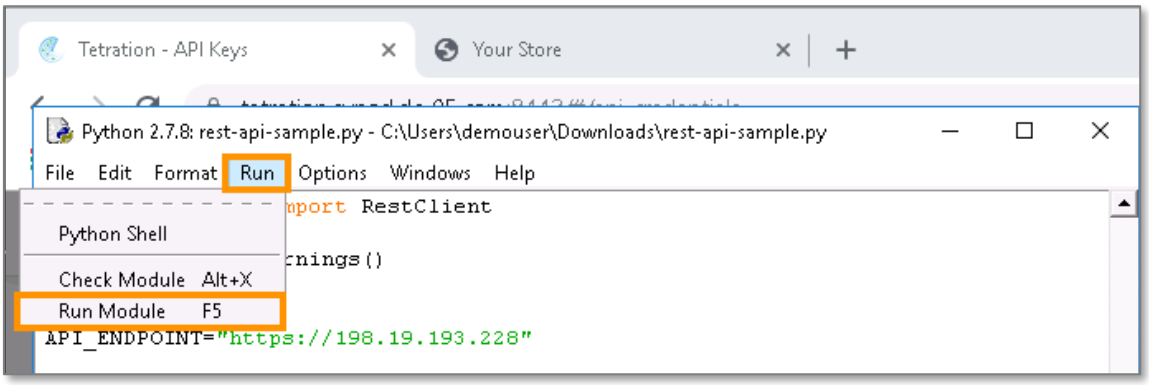
7. rest-api-sample.py ファイルを右クリックし、[IDLE で編集（Edit in IDLE）] を選択します。

注：このファイルのコマンドでは、すべてのセンサーが収集されて出力されます。



注：python スクリプトは、先ほど作成してダウンロードした API クレデンシャルを指しています。

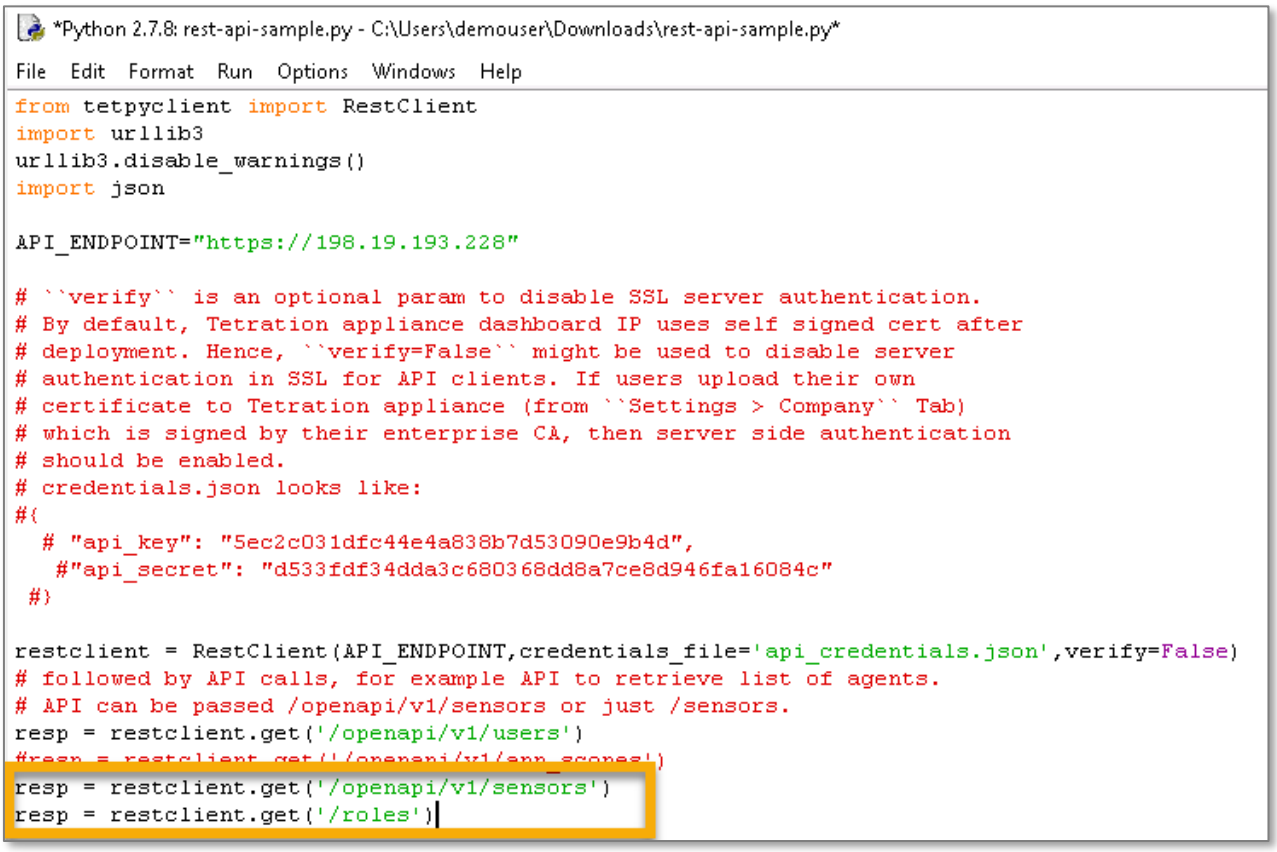
8. IDLE ウィンドウで、[実行（Run）] > [モジュールの実行（Run Module）] をクリックしてスクリプトを実行します。



9. スクリプトで、すべての Tetration センサーが出力されます。

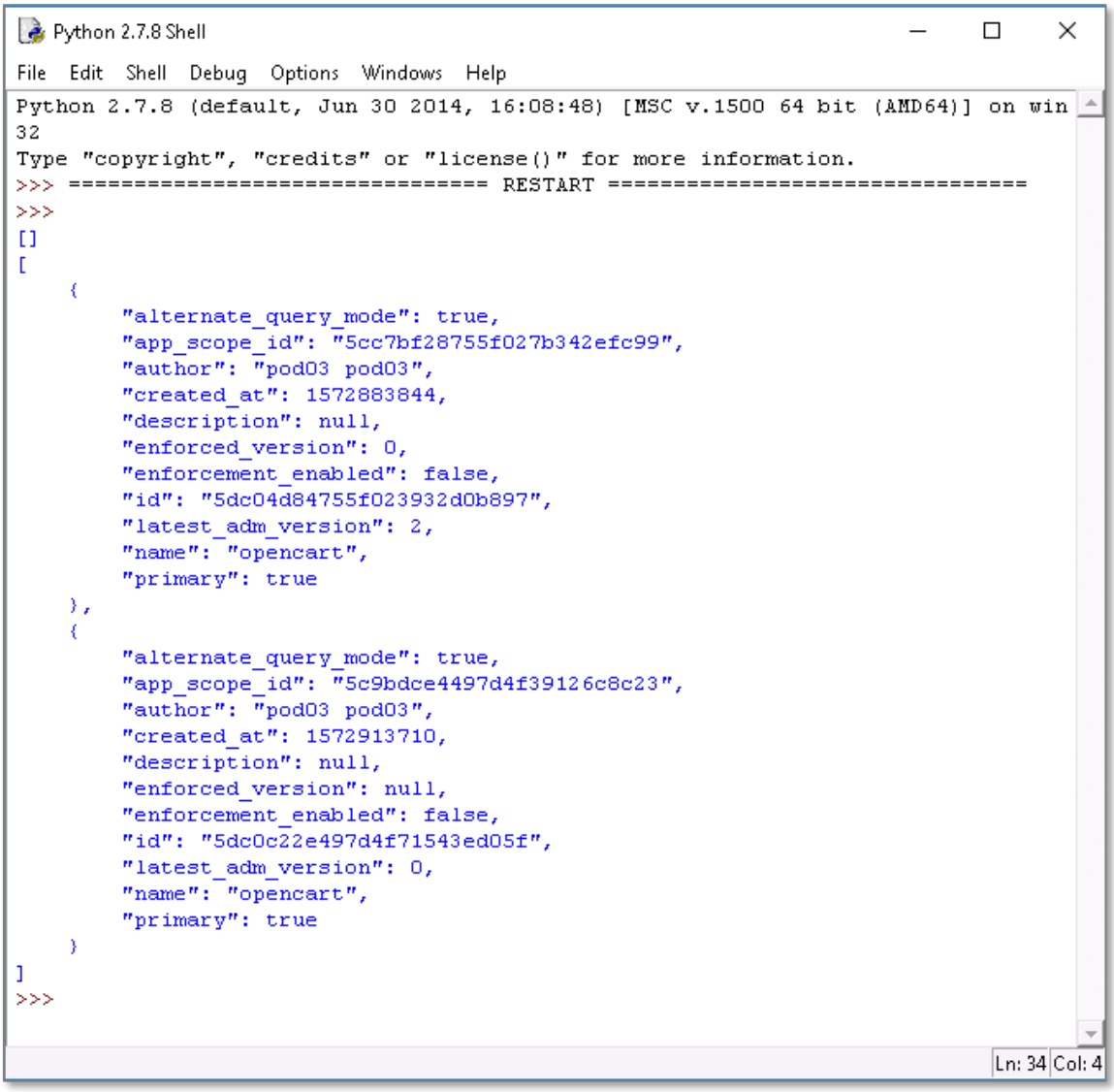
注：ロールベース アクセス コントロール（RBAC）により、スクリプトで、表示が許可されていない情報が収集されるのを防ぎます。返されるすべてのセンサーは、ユーザ自身のポッドから取得されます。

10. IDLE ウィンドウで、既存の resp 行の下に resp = restclient.get(`roles`) という行を追加します。ソースを**保存**します。



11. [実行（Run）] > [モジュールの実行（Run Module）] をもう一度クリックします。

12. スクリプトで、ユーザのロールが返されます。



次に必要な作業

Tetration の詳細については、関連するデモンストレーションと提案を参照してください。

Cisco Tetration Platform 3.3 v1 [英語]

Cisco Tetration Analytics - Proposal Template for Cisco Sales [英語]

Cisco Tetration - Proposal Template for Partner Sales [英語]

Tetration Advise and Implement Service - Proposal Template [英語]

Tetration Analytics Services - Proposal Template [英語]

Cisco Tetration Analytics: **マルチクラウド環境の可視化とセキュリティ**[日本語]

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp