

セキュアなワークロード(Tetration)でのスナップショットファイルの生成

内容

[概要](#)

[前提条件](#)

[使用するコンポーネント](#)

[背景説明](#)

[スナップショットバンドルの収集](#)

[クラシックスナップショットバンドルの生成](#)

[CIMCバンドルの生成](#)

[Tetration Agentログバンドルの生成](#)

[仮想アプライアンスコネクタスナップショットバンドルの生成](#)

[シスコサービスリクエスト\(SR\)へのバンドルのアップロード](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Secure Workload(Tetration)で各種のログ収集に関するスナップショットバンドルファイルを生成する方法について説明します。

前提条件

使用するコンポーネント

次の製品に関する知識があることが推奨されます。

- Cisco Secure Workload(Tetration)
- Cisco インテグレートド マネージメント コントローラ (CIMC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

注： スナップショットツールにアクセスするには、カスタマーサポートの役割が必要です。

警告： このドキュメントの手順は、ソフトウェアバージョン3.4.1.x以降が稼働するCisco Secure Workload(Tetration)に適用されます。

Tetration Clusterのハードウェア、ソフトウェア、および統合のステータスを判別するために使用されるスナップショットバンドルは次のとおりです。

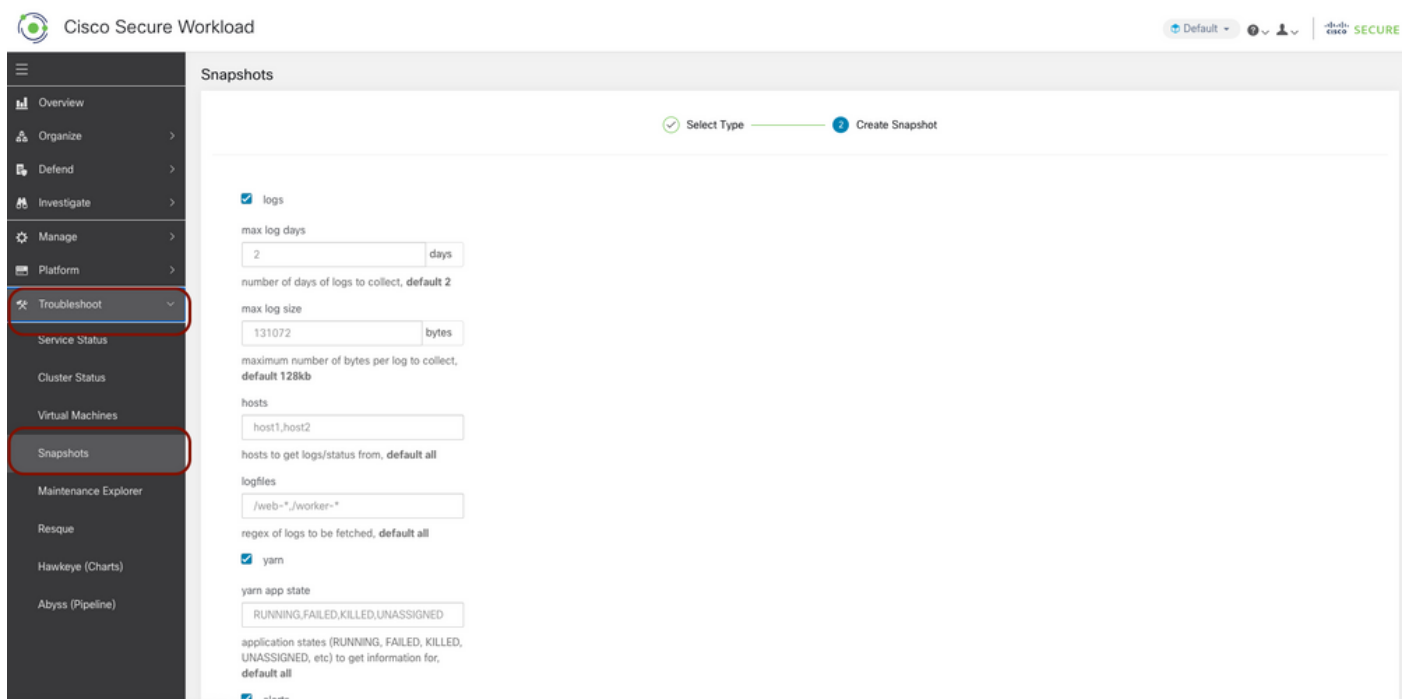
- Classical Snapshotバンドル：Cisco Unity Expressの クラスタ関連データのログメッセージ、設定データ、コマンド出力、アラート、時系列データベース(tsd)などのコレクション。
- CIMCスナップショットバンドル：Unified Computing System(UCS)からテクニカルサポート ファイルを収集し、ハードウェアアプライアンス(8RU、39RU)クラスタに適用できます。
- ソフトウェアエージェントバンドル：テレメトリデータ収集のためにエンドシステムにインストールされるTetrationエージェントのログが含まれます。
- 仮想アプライアンスコネクタバンドル：フローの取り込み、インベントリの強化、アラート通知をサポートするTetration Virtualアプライアンスからのログが含まれます。

シスコのエンジニアからSecure Workloadクラスタからのスナップショットバンドルの送信を要求された場合は、このドキュメントに記載されている手順を使用できます。

スナップショットバンドルの収集

クラシックスナップショットバンドルの生成

Secure Workload User Interface(UI)にログインし、左側のナビゲーション・パネルに移動して、**Troubleshoot > Snapshot [Maintenance > Snapshot (3.4.xまたは3.5.x)]**オプションを選択します。「スナップショットの作成」をクリックし、「クラシック・スナップショット」を選択します。スナップショットページが表示され、デフォルトオプションが表示されます。Cisco TACエンジニアから特別に要求された場合は、デフォルトオプションを上書きできます。



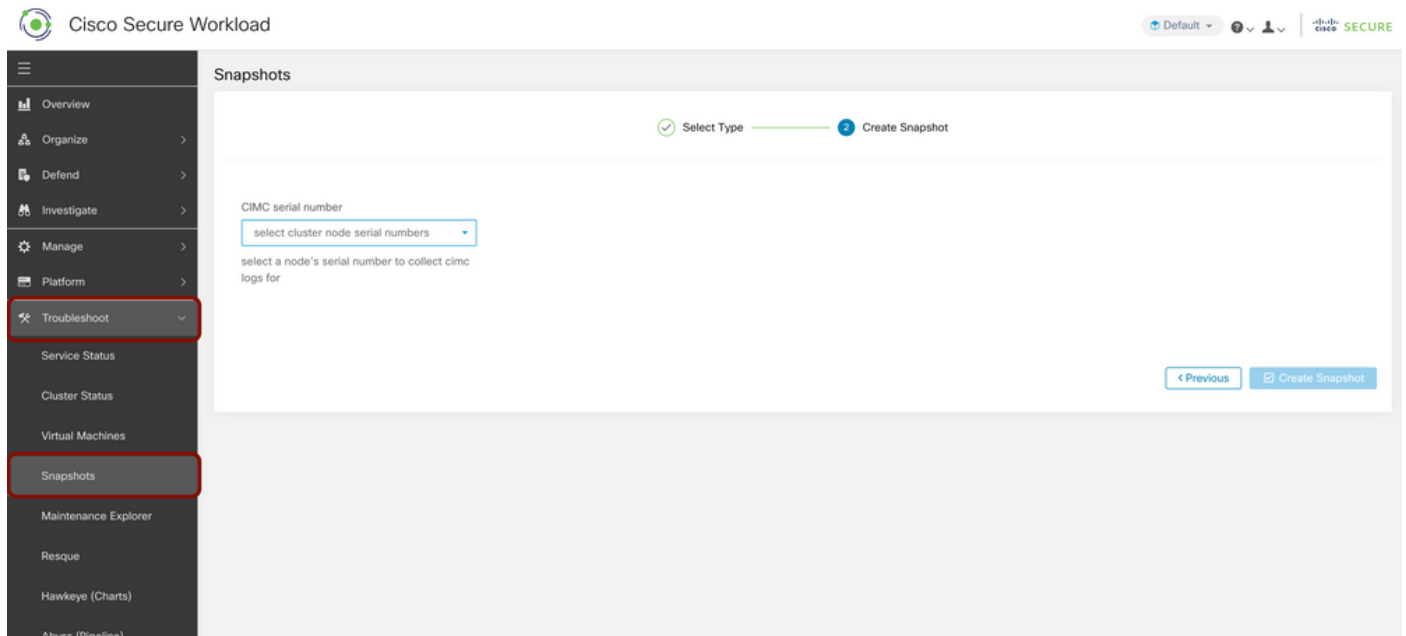
The screenshot displays the 'Snapshots' configuration page in the Cisco Secure Workload UI. The left-hand navigation pane is visible, with 'Troubleshoot' and 'Snapshots' highlighted. The main area shows a 'Create Snapshot' wizard with the following settings:

- logs
- max log days: 2 days
- number of days of logs to collect, default 2
- max log size: 131072 bytes
- maximum number of bytes per log to collect, default 128kb
- hosts: host1,host2
- hosts to get logs/status from, default all
- logfiles: /web-*/worker-*
- regex of logs to be fetched, default all
- yarn
- yarn app state: RUNNING,FAILED,KILLED,UNASSIGNED
- application states (RUNNING, FAILED, KILLED, UNASSIGNED, etc) to get information for, default all
- alerts

ページの下部までスクロールし、コメント・セクションを使用してケース番号または問題の説明を指定し、「スナップショットの作成」をクリックしてクラシック・スナップショット・バンドルの生成手順を開始します。スナップショットの生成が完了するまでに時間がかかることがあります。スナップショットの生成が100%に達したら、[ダウンロード]をクリックしてクラシックスナップショットバンドルをダウンロードします。下にスクロールして、ファイルをケース番号にアップロードするオプションを表示します。

CIMCバンドルの生成

Secure Workload UIにログインし、左側のナビゲーション・パネルに移動し、[Troubleshoot] > [Snapshot Maintenance] > [Snapshot (3.4.xまたは3.5.x)]を選択します。[Create Snapshot]をクリックし、[CIMC Snapshot]を選択します。CIMCスナップショットページが表示され、ドロップダウンオプションを使用してノードのシリアル番号を選択します。ノードを検索または選択し、[スナップショットの作成]をクリックして、CIMCスナップショットバンドルの生成手順を開始します。



スナップショットの生成が完了するまでに時間がかかることがあります。スナップショットの生成が100%に達したら、[ダウンロード]をクリックしてCIMC Snapshotバンドルをダウンロードします。下にスクロールして、ファイルをケース番号にアップロードするオプションを表示します。

Tetration Agentログバンドルの生成

ログバンドルを収集するには、Tetrationエージェントがアクティブである必要があります。

- 3.6.xバージョンの場合は、左側のナビゲーションパネルに移動し、[Manage] > [Agent]の順に選択し、[Agent List]をクリックします。
- 3.4.xおよび3.5.xバージョンの場合は、右上のドロップダウン・メニューから[Monitoring]に移動し、[Agent List]を選択します。

フィルタオプションを使用してエージェントを検索し、エージェントをクリックします。エージェントのワークロードプロファイルが表示されます。ここでは、エージェントの設定、ステータスなどの詳細を確認できます。

ワークロードプロファイルページ(3.6.x)の左側のナビゲーションパネルで、[ログのダウンロード (Download Logs)]を選択します(3.4.xおよび3.5.xで、[サマリー(summary)]タブに従います)。「ログ収集の開始」をクリックし、Tetration Agentからログ収集を開始します。ログ収集の完了に時間がかかる場合があります。ログ収集が完了したら、[Download here]オプションをクリックしてログをダウンロードします。下にスクロールして、ファイルをケース番号にアップロードするオプションを表示します。

Cisco Tetration WORKLOAD PROFILE

Monitoring

Summary Long Lived Processes Process Snapshot Interfaces Packages Vulnerabilities Config Stats Network Anomalies File Hashes Visit History

Apr 13 6:03am - Apr 14 6:03am JBLOMART-WIN-1 **3.4.x and 3.5.x Version**

Host Name: jblomart-win-1
 Agent Type: Deep Visibility
 OS Platform: MSServer2012R2Standard - Version 6.3 (OS Build 9600 20144) (x86_64)
 Last Check-in: Apr 14 2022 05:56:19 am (CEST)
 Agent Version: 3.4.1.20.win64-sensor
 Scopes: Default
 User Annotations: None
 Enforcement Groups: jbl_tenant
 Experimental Groups: jbl_tenant
 Interfaces: 20
 Packages: 159

Traffic Volume

Download Logs

Status: ● Log collection is complete and they can be downloaded here

Requested at: Apr 13 2022 06:11:35 pm (CEST)

[+ Initiate Log Collection](#)

3.4.xおよび3.5.xバージョン

Cisco Secure Workload

Default

Agent List / Workload Profile / Log Download **3.6.x Version**

Log Download

worker1

Enforcement: CentDS 7.9

Agent Health

- Agent Active
- Flow Export Operational
- Upgrade Success
- Cpu Usage Normal
- Mem Usage Normal
- Agent Version Not Current

Enforcement Health: Good

Download Logs

Status: ● Log collection is complete and they can be downloaded here

Requested at: Apr 13 2022 09:30:27 pm (IST)

Available for download at: Apr 13 2022 09:30:59 pm (IST)

Size: 33.86 MB

[+ Initiate Log Collection](#)

3.6.xバージョン

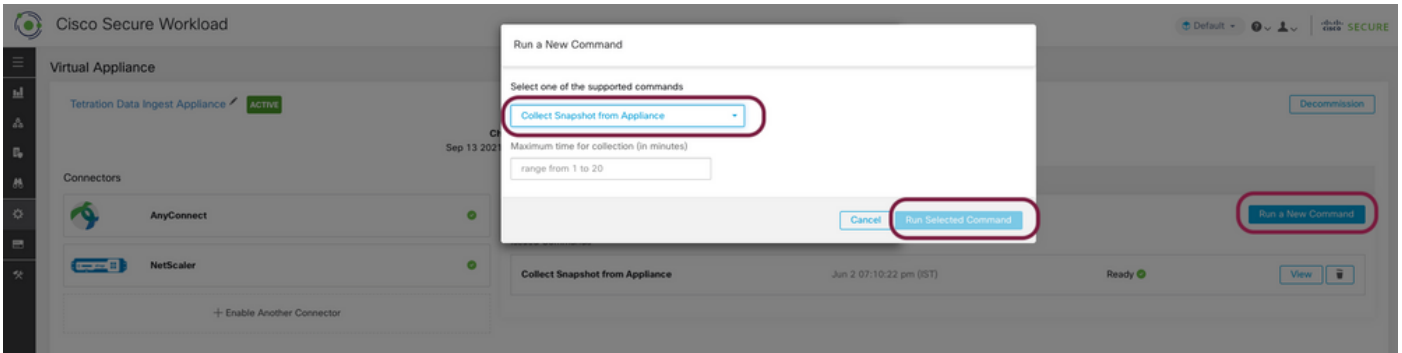
仮想アプライアンスコネクタスナップショットバンドルの生成

仮想アプライアンスのスナップショットバンドルを取得するには、仮想アプライアンスがアクティブ状態であることを確認する必要があります。

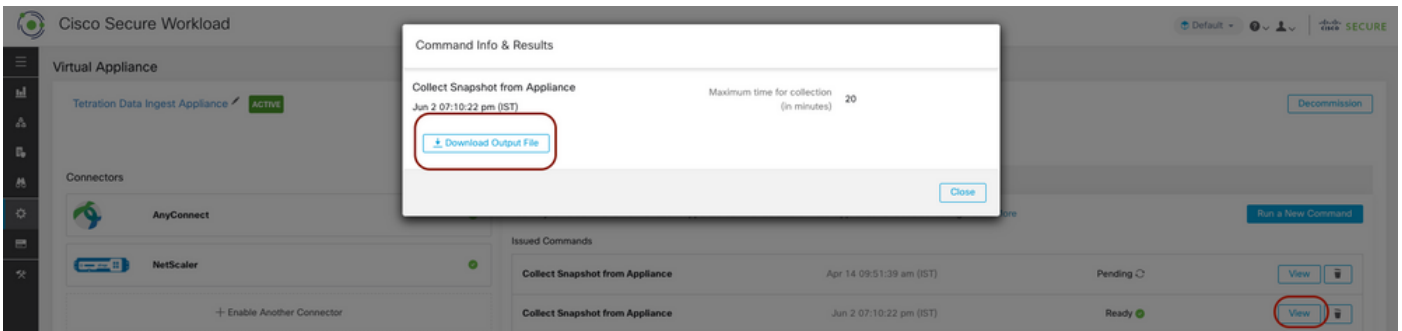
- 3.6.xバージョンの場合は、左側のナビゲーションパネルに移動し、[Manage] > [Virtual Appliance]を選択します。
- バージョン3.4.xおよび3.5.xの場合は、左側のナビゲーションパネルに移動し、[Connectors]

> [Virtual Appliance]を選択します。

スナップショットバンドルを生成する仮想アプライアンスを選択します。[トラブルシュート]をクリックし、もう一度[トラブルシュートオプション]をクリックします。[新しいコマンドを実行]をクリックすると、ダイアログボックスが開きます。このダイアログボックスには、コマンドを選択するためのドロップダウンメニューがあります。ドロップダウンメニューから、アプライアンスからスナップショットの収集を選択し、時間の範囲（たとえば、20分）を分単位で指定し、[Run Selected Command]をクリックします。仮想アプライアンスからスナップショットバンドルを収集する手順を開始します。仮想アプライアンスからログバンドルを収集するのに時間がかかることがあります。



スナップショットバンドルの収集が完了したら、[表示]をクリックしてスナップショットバンドルをダウンロードします。下にスクロールして、ファイルをケース番号にアップロードするオプションを表示します。



シスコサービスリクエスト(SR)へのバンドルのアップロード

ケース(SR)にスナップショットバンドルをアップロードする方法は複数あります。詳細については、「[Customer File Uploads to the Cisco Technical Assistance Center](#)」ページを参照してください。

- [Cisco Secure Workload\(Tetration\)](#)
- [Cisco Secure Workload\(Tetration\)製品の概要](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)