Cisco Secure Workload Virtual（Tetration-V）導入ガイド

初版：2021 年 8 月 17 日

最終更新：2023 年 1 月 5 日

Secure Workload Virtual の展開

Secure Workload Virtual の展開について

Secure Workload Virtual （別名 Tetration-V）は、VMware ESXi 環境に Cisco Secure Workload（旧称 Cisco Tetration）を展開するためのソフトウェアソリューションです。

Cisco Secure Workload の詳細については、https://www.cisco.com/c/en/us/products/security/tetration/index.html を参照してください。

制限事項

- 2021 年 9 月 1 日以降：

  Cisco Secure Workload Virtual（Tetration-V）は、非実稼働環境でのコンセプト実証（POC）または価値の実証（POV）にのみ使用できます。

  2021 年 9 月 1 日より前に購入した場合：

  Tetration-V は、仮想化が使用可能な唯一のコンピューティング オプションである小規模な展開または環境を対象としていました。

- VM のスナップショットはサポートされません。
- ハードウェアセンサーは、Secure Workload Virtual ではサポートされません。

前提条件

VMware ESXi 環境で Secure Workload Virtual アプライアンスを展開するためには、セットアップは次の要件を満たす必要があります。

ソフトウェア前提条件

- ハイパーバイザ

- サポートされる VMware vSphere バージョンを実行している VMware 高可用性クラスタ：
  - Cisco Secure Workload バージョン 3.6.x の場合：VMware vSphere 6.5、6.7、または 7.0.3
  - Tetration バージョン 3.5.x までの場合：VMware vSphere バージョン 6.5 または 6.7
- 展開には HTML5 クライアントを備えた vSphere 6.7U3 以降をお勧めします。
- バージョン要件は、ハイパーバイザ、コア管理、認証とサービス、アップグレードとパッチ管理などのすべてのコンポーネントに適用されます。
- 展開は、VMware でサポートされる構成で実行する必要があります。
- すべてのホストは、分散リソース スケジューラ (DRS) が有効になっている 1 つの HA クラスタの一部である必要があります。

- [VMware ESXi環境用Tetration仮想アプライアンスインストールOVA（Tetration virtual appliance install OVA for VMware ESXi environment）] OVA ファイル。Cisco.com の [ソフトウェアダウンロード（Software Downloads）] ページから入手できます。
- 必要な Secure Workload（Tetration）RPM。Cisco.com の [ソフトウェアダウンロード（Software Downloads）] ページから入手できます。
  - OS Adhoc
  - OS Enforcement

    （3.5.1.x より前のリリースには適用されません）
  - OS Mother
  - OS OVA
  - OS RPMInstall

ハードウェアの前提条件

- 最高のパフォーマンスを確保するには、クラスタ専用のハードウェアを使用することをお勧めします。
- インフラストラクチャのホスティングの対応:
  - 最小 2 GHz クロック速度の 128 個の物理的な CPU コア
  - 2 TB RAM
    - 仮想マシンは最大 128 GB です。
    - メモリをオーバーコミットすることはできません。
  - 18.1 TB ストレージ

- ストレージは、1 秒あたり最小 5,000 回の I/O 操作（IOPS）が可能なフラッシュメモリまたは SSD など、高性能でなければなりません。
- ストレージはクラスタのすべてのノードからアクセスできる必要があります。
- ストレージは、1 つの共有 VMware vSphere データストアとしてプロビジョニングする必要があります。Hyperflex、vSAN、FC/FCoESAN、NFS、および iSCSI がサポートされます。
- ストレージは、永続的な必要があります。

- リソースチェックは展開時に実行されますが、インフラストラクチャが要件内に収まるように管理する必要があります。

- ネットワーク インフラストラクチャ
  - クラスタ内のすべてのホストは、少なくとも 10 ギガビット イーサネット (GbE) インターフェイスに接続する必要があります。
  - すべてのホストで Secure Workload 目的のために使用可能な 3 つの仮想ネットワークが必要です。
    - **パブリックネットワーク**：センサーおよびクライアントから到達可能でなければならない外部クラスタトラフィックのための専用または共有のパブリックネットワークで、vCenter へのアクセス権を持ちます。このネットワークは、Secure Workload アプリケーションアクセスに使用されます。/28 の最小のサブネットを指定する必要があります。外部ネットワークが専用で、IP アドレスの全範囲が使用可能な場合、8 個の IP アドレスは次の表に示すように自動的に消費されます。

表 *1*：範囲内の *IP* アドレス

IP アドレス	説明文
1 番目	ゲートウェイ IP アドレス（予約済み）。
2 番目と 3 番目	予約済み
4 番目	Web UI の仮想 IP アドレス。
5 番目	センサー管理仮想 IP アドレス。
6 番目	コレクタ。
7 番目	コレクタ。
8 番目	アプリケーション インターフェイス。
9 番目	アプリケーション インターフェイス。
10 番目	アドホック Kafka。

IP アドレス	説明文
11 番目。	オーケストレータ。必要に応じてを使用します。

パブリック ネットワークの共有されている場合は、特定の使用可能なアドレスを定義する必要があります。

- **プライベートネットワーク**：ルーティング可能であってはならず、共有されてもならない内部クラスタ通信に対する専用プライベートネットワーク。/26 の最小のサブネットを指定する必要があります。/24 のサブネットをお勧めします。
- **設定のネットワーク**：導入を実行しているユーザーが到達可能でなければならないブートストラップクラスタの一時ネットワークで、VMware vCenter へのアクセス権も持たなければなりません。これは、パブリック サブネットとは別のサブネットでなければならず、導入が完了した後でシャットダウンする必要があります。このネットワークは、Secure Workload セットアップ インターフェイス アクセスに使用されます。

- VMware vSphere 分散スイッチ（vDS）
  - VDS にはネイティブまたは Cisco ACI 制御があります。
  - すべてのホストには、共通の VDS と一貫性のあるネットワーク構成が必要です。
- VDS を使用する場合は、クラスタ内のすべてのホストを含める必要があります。

（注） ハードウェアの推奨事項が満たされている場合でも、他の要因が Cisco Secure Workload ソフトウェアの全体的なパフォーマンスに影響を与える可能性があるため、パフォーマンスの保証や SLA を実装することはできません。

展開時のネットワーク接続/ファイアウォールの要件

展開時、ブートストラップ オーケストレータには、次の 2 つのパブリック IP アドレスが割り当てられます。

- 設定のネットワーク
- パブリック ネットワーク

オーケストレータは、パブリックネットワークの最後のアドレスを自動的に割り当て、そのアドレスを使用してサイトチェッカーの検証を実行します。この検証には、SMTP、DNS、NTP、Ping、vCenter 接続テストが含まれます（ただし、これらに限定されません）。サイトチェッカーの検証が完了すると、オーケストレータは IP アドレスを削除し、設定のネットワークを使用して残りの展開を続行します。次の接続が確立されます。

ネットワーク	接続先	プロトコル	ポート
設定およびパブリック	DNS サーバー	UDP	53
設定およびパブリック	NTP サーバー	UDP	123
パブリック	SMTP サーバ	TCP	SMTP ポート（SMTP Port）
設定およびパブリック	vCenter ホスト	TCP	443
設定	ESXi ホスト*（表の下の注を参照）	TCP	443

* OVF ツールが vCenter との接続を確立し、ESX にリダイレクトされて大規模なファイル転送を行います。

展開が完了すると、設定のネットワークは IP アドレスを削除し、インターフェイスをシャットダウンします。アップグレードはすべてパブリックネットワークを使用して行われます。

SSH 公開キー

GUI が仕様できない場合は、Secure Workloadプラットフォームへのリモート サポート アクセスに SSH 公開キーが必要です。Secure Workload仮想アプライアンスのインストールを開始する前に、RSA 4096 ビットのキーペアを生成します。インストール時にこのキーを指定します。秘密キーを将来使用するために安全に保管します。

電子メール アドレス

初期システムアクセスとアウトバウンドアラートに使用される 3 つの一意の電子メールアドレスを指定する必要があります。

表 *2:* 電子メール アドレス

電子メール アドレス	説明文
サイト管理	このアドレスは、デフォルトの管理者アカウントを作成するために使用されます。
カスタマーサポート	このアドレスは、デフォルトのカスタマー サポート アカウントを作成するために使用されます。
アラート	このアドレスは、アウトバウンドアラートに使用されます。

推奨される VMware 設定

各 VMware vSphere の導入には、管理者が実施したさまざまな要件、制約、およびベスト プラクティスを入れることができます。Secure Workload インストーラが VMware vSphere 導入に設定変更を加えることはできません。このセクションの推奨事項は、VMware エキスパートのアドバイスと入念に計画を置き換えてはなりません。これらの推奨事項に従わない場合、データの可用性が低下する可能性があり、Secure Workloadは完全に、または期待通りに機能しない可能性があります。

次のリストには、推奨される VMware 構成時の設定が含まれています。

- VMware vSphere 分散リソース スケジューラ (DRS)、ホストの障害に対して VMware vSphere 高可用性（HA）、Secure Workloadが導入されるクラスタの VMware vMotion を有効にします。これは、Secure Workloadクラスタのインスタンスに対して可用性とパフォーマンスを提供する上で役立ちます。
- データストアは、可用性と、永続的なデータが重複しては保存され、ハードウェア障害には抵抗ことを意味をする必要があります。
- ハイパーバイザ ホストと VMware vCenter サーバーは正しくクロックを設定し、Network Time Protocol（NTP） を使用してクロックを同期します。

導入後、以下の導入手順の説明に従って、アンチアフィニティルールを設定します。

VMware の権限

Secure Workload のインストーラには、データストアで仮想マシン、フォルダ、ファイルを作成するために VMware vSphere にアクセスし、仮想スイッチとデータストアに接続するための資格情報が必要です。

Secure Workload インストーラには、インストールを実行するのに最低限必要な権限を持つ別のユーザーアカウントを使用することを強く推奨します。

次の権限は、VMware ユーザ アカウントのロールを作成するための開始点として使用できます。

- コンテンツ ライブラリ
- Datastore
- フォルダ\フォルダの作成
- ネットワーク\ネットワークの割り当て
- Resource
- タスク
- 仮想マシン
- dvPort グループ

- vApp
- vSphere タグ指定（ラベル付け）

オープンソース ユーティリティ Terraform は、vSphere の一部のリソースを管理するために使用されます。Terraform に必要な権限の詳細については、https://www.terraform.io/docs/providers/vsphere/index.html#notes-on-required-privileges を参照してください。

サイト情報

設定は、次のサイト情報要件を満たす必要があります。

[Network] タブ

- **外部ネットワーク**: 少なくとも 8 個の空き IP アドレスをもつ外部ネットワークのサブネット。
  - [Advanced] タブで外部の IP アドレスを設定する場合を除き、自動割り当ては、次のルールで使用されます。
    - 自動割り当ては、IP アドレスを自動的に割り当てようとします。
    - 自動割り当ては、最初の 3 個と最後の 3 個の IP アドレスをスキップして、4 番目の IP アドレスから最後の IP アドレスまでを割り当てます。
    - サブネットの最初の使用可能な IP アドレスは、ゲートウェイとして使用されます。

    たとえば、サブネットに`192.168.0/28`を指定すると、`192.168.1.1`はゲートウェイであり、`192.168.1.4`から`192.168.1.11`までの IP アドレスが使用されます。

ESX タブ

- [vSphereホスト（vSphere Host）]：VMware vCenter サーバーの IP アドレスまたはホスト名。
- **vSphere ユーザ名**: ファイルのアップロードおよび仮想マシンの作成のために必要な権限を持つ VMware vSphere アカウントのユーザ名。
- **vSphere パスワード**: VMware vSphere アカウントのパスワード。
- **vSphere データセンター**: ターゲットのVMware vSphere データセンターの名前。
- **クラスタ**: 仮想マシンが配置されるクラスタ。
- [VMのフォルダ名（VM Folder Name）]：Secure Workload 仮想マシンを配置するフォルダの名前。ネストされたフォルダはサポートされていません。
- [データストア（Datastore）]：仮想マシンがストレージ用に割り当てるデータストア。

- **プライベート ネットワーク ポート グループ**: プライベート ネットワークに使用する仮想スイッチ ポート グループの名前。
- **パブリック ネットワーク**:パブリック ネットワークで使用する仮想スイッチ ポート グループの名前。
- [クラウドInitフォルダ（Cloud Init Folder）] : 導入構成ファイルを保存するのに使用されるデータストアのフォルダの名前。

[Advanced] タブ（オプション）

- **外部 IP アドレス**: パブリック ネットワークの共有サブネットを使用する場合は、導入で使用する IP アドレスのリストを指定します。IP アドレスは、次の要件を満たす必要があります。
  - 8 個の IP アドレスが必要です。
  - サブネット内の最初の 3 個の IP アドレスを指定することはできません。
  - サブネットの最初の使用可能な IP アドレスは、ゲートウェイとして使用されます。

  たとえば、**192.168.1.0/24**サブネットでは、8 個の IP アドレスを指定することができますが、**192.168.1.3** から **192.168.1.3** までの IP アドレスは使用することはできません。192.168.1.1 は、ゲートウェイです。

外部サービス パラメータ

次の表は、外部サービス パラメータについての情報を提供します。

表 *3:* 外部サービス パラメータ

サービス	パラメータ	必須/オプション
vCenter	vCenter ホスト User Credentials VM のフォルダ クラスタとデータセンター名 ポート グループ—Orchestrator、パブリック、およびプライベート Datastore Name	必須
DNS	1 つまたは複数の DNS サーバー	必須
NTP	1 つ以上の NTP サーバー	必須

サービス	パラメータ	必須/オプション
SMTP	SMTP Host SMTP Port 認証の資格情報 (オプション)	必須
Proxy	HTTP プロキシサーバーとポート HTTPS プロキシサーバーとポート	オプション
Syslog	Syslog サーバとポート	オプション

Cluster Parameters

次の表は、クラスタ パラメータについての情報を示しています。

表 *4 : Cluster Parameters*

パラメータ	必須/オプション	注
サイト名	必須	導入後に名前を変更することはできません。名前は、UI FQDN のホスト部と一致する必要があります。
UI FQDN	必須	FQDN は、DNS で解決できる必要があります。

VMware ESXi 環境での Secure Workload Virtual アプライアンスの展開

次の手順では、VMware ESXi 環境で Secure Workload Virtual アプライアンスを展開します。最初に、オーケストレータ OVA を導入し、次に Secure Workload を設定します。

手順

ステップ 1 VMware vSphere Web インターフェイスにログインします。
ステップ 2 クラスタの目的のサイト名で新しいフォルダを作成します。
ステップ 3 ターゲット クラスタを右クリックし、**OVF テンプレートの導入** を選択します。
ステップ 4 OVF テンプレートの場所を入力します。

ESX クラスタに近いところの Web サーバでオーケストラ OVA をホストすることをお勧めします。オーケストレータ OVA は 5 GB 以上であるため、ファイルは低速リンクでの転送に時間がかかる場合があります。

ステップ 5 [Next] をクリックします。

ステップ 6 仮想マシン名に **`orchestrator-1`** と入力します。目的のデータセンターと、クラスタサイト名で名前を指定した Cisco Secure Workload 展開フォルダに仮想マシンが展開されていることを確認します。

ステップ 7 [Next] をクリックします。

ステップ 8 選択したクラスタが目的のターゲットであることを確認します。

ステップ 9 [Next] をクリックします。

ステップ 10 ライセンス契約を確認し、利用規約に同意する場合は **[Accept]**] をクリックします。

ステップ 11 [Next] をクリックします。

ステップ 12 デフォルト構成プロファイル (**2CPU-8 GB**) を使用し、**[Next]**] をクリックします。

ステップ 13 導入に使用するデータストアを選択します。環境にその他の設定が必要な場合を除き、デフォルト設定ではその他のすべてのオプションをそのままにすることができます。

ステップ 14 [Next] をクリックします。

ステップ 15 適切なネットワーク マッピングを選択します。

- **構成**: クラスタの導入段階が呼び出されている間にオーケストレータが到達できるルーティング可能なネットワークを入力します。パブリック ネットワークとは異なるネットワークを使用します。導入が完了した後、**orchestrator-1** からネットワークを切断します。
- **プライベート**: Secure Workloadが内部の通信に使用する非ルーティング内部ネットワークを入力します。
- **パブリック**: GUI、コレクタは、および仮想 IP アドレスが到達できるルーティング可能なネットワークを入力します。

ステップ 16 [Next] をクリックします。

ステップ 17 構成のネットワークに対して、オーケストレータの到達可能性の詳細を入力します。

- **IP アドレス**: オーケストレータの IP アドレスのドット区切りの 4 つの数字列表記を入力します。
- **ネットマスク**: ネットワークのネットマスクのドット区切りの 4 つの数字列表記を入力します。
- **ゲートウェイ**—オーケストレータの構成ネットワークのドット区切りの4つの数字列表記ゲートウェイの IP を入力します。

ステップ 18 構成パラメータのすべてを確認します。

ステップ 19 [Finish] をクリックします。

数分後、OVF が導入されます。OVA アップロードが完了したら、電源をオンにし、オーケストレータ仮想マシンにアクセスするために、VMware vSphere GUI セッションを更新する必要があります。

ステップ 20 必要に応じて、VMware vSphere コンソールの右上にあるログインユーザ名の横にある [**Refresh**] ボタンをクリックします。

ステップ 21 **orchestrator-1** 仮想マシンの電源をオンにします。

数分以内に、ステップ 17 に入力した IP アドレスは、ping 要求に応答を始めます。

ステップ 22 オーケストレータが起動した後は、新しいブラウザ タブを開き、次の URL をブラウザをポイントします。

```
http://orchestrator-ip:9000/
```

ブラウザで [セットアップ（Setup）] ウィンドウが開きます。

（注） Cisco Secure Workload リリース 3.8 以降では、Cisco Secure Workload セットアップ ユーザーインターフェイスを使用してサイト構成のテキストフィールドに非 ASCII 文字を入力することはできません。

ステップ 23 [セットアップ（Setup）] ウィンドウでは、次の順序で RPM をアップロードします。

1. `rpminstall`
2. `adhoc`
3. `mother`
4. `enforcement`（3.5.1.x より前のリリースには適用されません）
5. `os_ova`

RPM をアップロードするためには、以下のサブステップを実行します。

a) [Choose File] をクリックします。
b) RPM に移動して選択し、**[Open]** をクリックします。
c) [Upload] をクリックします。
d) 各 RPM の次のステップを繰り返します。

ステップ 24 標準のインストール手順に従ってサイト情報を入力し、ハーパーバイザー固有のガイドラインについては サイト情報 （7 ページ） を参照してください

ステップ 25 **[Continue]** をクリックし、標準的なサイトのインストール手順に従います。

導入が開始された後で、**オーケストレータ-2**および**オーケストレータ-3**、残りの Secure Workload スタックの順序で、VMware vSphere で作成された仮想マシンが表示され始めます。15 分後に作成された仮想マシンがまったく表示されない場合は、[詳細（Details）] ボタンをクリックして [セットアップ（Setup）] ウィンドウで使用可能な導入ログを確認します。

ステップ 26 ハードウェアが推奨する仕様を満たすハードウェアの Secure Workload セットアップ プロセスをモニタリングします。完了には約 1.5 時間かかります。

導入が100%に達すると、ステータス行で示されている仮想IPアドレスを書き留めます。偶発的に、インストーラを閉じてしまった場合は、仮想 IP アドレスの IP アドレスを書き留めます。仮想 IP アドレスは、最初に示されたものが最初に使用できる IP アドレスです。

ステップ 27 ブラウザでタブ ページを開き、サイト情報セクションで入力した GUI 完全修飾ドメイン名 (FQDN) をブラウザにポイントさせます。

ステップ 28 [パスワードを忘れた場合（Forgot Password?）] をクリックします。

ステップ 29 サイト管理者に入力した電子メールアドレスを入力し、[パスワードのリセットリンクの送信（Send password reset link）] をクリックします。

ステップ 30 電子メールの受信トレイを確認し、含まれている指示に従います。

必要に応じて、**Spam** フォルダを確認します。

ステップ 31 Secure Workload インフラストラクチャの中に冗長性を与える特定の VM ロールに対して、アンチアフィニティルールを設定します。アンチ アフィニティ ルールは、次の基本タイプのインスタンスに配置しなければなりません。

- orchestrator
- adhoc
- appServer
- collectorDatamover
- datanode
- druidCoordinator
- druidHistoricalBroker
- Elasticsearch
- enforcementCoordinator
- enforcementPolicyStore
- happobat
- hbaseMaster
- hbaseRegionServer
- launcherHost
- mongodb
- namenode と secondaryNamenode
- redis
- tsdbBosunGrafana
- zookeeper

ステップ 32 **VMware VM** 構成画面で [orchestrator-1] を右クリックし、[設定の編集（Edit Settings）] を選択します。

ステップ 33 [Virtual Hardware] タブをクリックします。

ステップ 34 [ネットワークアダプタ3（Network Adapter 3）] で、[接続中（Connected）] ボックスの選択を解除します。

ステップ 35 **[OK]**をクリックして変更を適用します。

[接続中（Connected）]ボックスのチェックマークを外さないと、インストールプロセスが完了した後、その他の構成にクラスタが公開されたままになる場合があります。

ライセンシング

このプラットフォームのクラスタは、展開時に 30 日間のトライアルライセンスに制限されます。30日後、クラスタは新しいデータの処理を停止しますが、クラスタがアクティブであったときに収集および処理されたデータとユーザーインターフェイスには引き続きアクセスできます。サービスの中断を避けるためには、評価期間が終了する前に有効なライセンスを適用する必要があります。詳細については、Cisco Secure Workload Web ポータルのオンラインヘルプまたはユーザーガイドを参照してください。

コミッション/デコミッションの管理ガイドライン

Secure Workload Virtual 環境でコミッション/デコミッション機能を使用する場合は、次の重要なガイドラインに従ってください。

- この機能は Cisco TAC の支援を受けている場合に限って使用することを意図しており、誤って使用すると回復不能な障害を引き起こす可能性があります。TACからの明示的な承認がない限り、2つの VM を同時にデコミッションしないでください。次の VM の組み合わせは、同時にデコミッションしないでください。
  - 複数のオーケストレータ
  - 複数のデータノード
  - 複数の namenode（namenode または secondaryNamenode）
  - 複数の resourceManager
  - 複数の happobat
  - 複数の mongodb（mongodb または mongoArbiter）
- 一度に実行できるデコミッション/コミッションプロセスは 1 つだけです。異なる VM のデコミッション/コミッションプロセスを同時にオーバーラップしないでください。

- esx_commission スナップショット エンドポイントを使用する前に、必ず Cisco TAC にお問い合わせください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。