Cisco Secure Workload アップグレードガイド

初版：2021 年 10 月 29 日

最終更新：2022 年 9 月 12 日

Cisco Secure Workload でサポートされているアップグレードパス

差出人	宛先
3.6.x	3.7.1.5
3.6.1.x	3.6 後期のパッチ。
3.5.1.x （Tetration のブランディング）	3.6.1.5
3.6 より前のバージョン。	3.6 より前のすべてのバージョン。 こちらで入手可能な『*Cisco Tetration Upgrade Guide*』の詳細を参照してください。

（オプション）デュアルスタックモード（IPv6 サポート）の要件と制限事項

物理ハードウェア上で実行される Cisco Secure Workload クラスタは、クラスタへの特定の通信とクラスタからの特定の通信に、IPv4 だけでなく IPv6 も使用するように設定できます。

（注） 3.6.1.5 リリースと 3.7.1.5 リリースをインストールまたはアップグレードする場合は、デュアルスタックモード（IPv6 サポート）機能を使用できますが、パッチリリースをインストールまたはアップグレードする場合は、この機能は使用できません。

制限事項

デュアルスタックモードの有効化を考慮している場合は、次の点に注意してください。

- IPv6 接続は、初期展開時またはメジャーリリースへのアップグレード時にのみ有効にできます（パッチアップグレード時にはこの機能は有効にできません）。

- デュアルスタックモードは、物理ハードウェア/ベアメタルクラスタでのみサポートされます。
- IPv6 専用モードはサポートされていません。
- クラスタでデュアルスタックモードを有効化した後は、IPv4 専用モードに戻すことはできません。
- デュアルスタック接続が有効な場合、データのバックアップと復元（DBR）はサポートされません。
- フェデレーションが設定されているクラスタでは、デュアルスタックモードを有効にしないでください。
- 次の機能では常に IPv4 のみを使用します（IPv6 が有効になっている場合も IPv4 は常に有効になっています）。
  - （リリース 3.7.1.5 と 3.6.x に適用）AIX エージェントでの適用
  - （リリース 3.6.x に適用）クラスタとのハードウェアエージェント通信
  - （リリース 3.6.x に適用）フローの取り込み、インベントリの強化、またはアラート通知用のコネクタ

要件

- FQDN の A および AAAA DNS レコードの両方を設定する必要があります。クラスタに対してデュアルスタックモードを有効にする前に、これを構成する必要があります。
- NTP、SMTP、DNS などの外部サービスは、冗長性のために IPv4 と IPv6 の両方で使用できる必要があります。
- クラスタにデュアルスタックモードを構成するには、次の手順を実行します。
  - 2 つのクラスタリーフスイッチには、冗長性を確保するため、異なる 2 つのネットワーク上のルーティング可能な IPv6 アドレスをそれぞれ割り当てる必要があります。また、各ネットワークにデフォルトゲートウェイを提供する必要があります。
  - 39RU クラスタの場合、少なくとも 29 個のホストアドレス用のスペースを持つ、サイトでルーティング可能な IPv6 ネットワークが必要です。
  - 8RU クラスタの場合、少なくとも 20 個 のホストアドレス用のスペースを持つ、サイトでルーティング可能な IPv6 ネットワークが必要です。
  - サイトでルーティング可能な IPv6 ネットワークの最初の 3 つのホストアドレスは、Cisco Secure Workload クラスタ HSRP 設定用に予約されています。他のデバイスでは使用しないでください。

その他の情報

エージェントは、IPv6 を使用するように設定しない限り、IPv4 を使用してクラスタと通信します。手順については、Cisco Secure Workload Web ポータルから入手可能なユーザーガイドを参照してください。

Cisco Secure Workload リリース 3.7.1.5 へのアップグレード

どの 3.6 リリースからもこのリリースにアップグレードできますが、このリリースにアップグレードする前に、最新の 3.6.1.x パッチリリースにアップグレードすることをお勧めします。

始める前に

⚠

注意 いずれかのノードが現在稼働停止状態にあるか、サービスが正常でない場合は、アップグレードしないでください。続行する前に、Cisco Technical Assistance Center に問い合わせて問題を修正してください。

次の点に注意してください。

- Kubernetes AKS 外部オーケストレータ：アップグレード後、AKS 外部オーケストレータは読み取り専用になります。アップグレード後に変更を加える場合は、新しい Azure コネクタを作成し、**Managed Kubernetes サービス**オプションを有効にします。
- 「カスタマーサポート」レベルのアカウントで、トラブルシューティングのために SSH キーがアップロードされていることを確認します。
- サイト管理者権限またはカスタマーサポート権限を持つユーザーとして次の手順を実行する必要があります。
- このアップグレードでサポートされるブラウザは Google Chrome のみです。
- ISE コネクタが構成されている場合は、それらの TLS 証明書にサブジェクト別名（SAN）セクションがあることを確認します。アップグレード後、ISE コネクタは、従来の CN 専用 TLS 証明書を提示する ISE エンドポイントに接続しません。ISE TLS 証明書が SAN 拡張で再生成されるまではアップグレードを続行しないでください。
- **ライセンシング**
  - Cisco Secure Workload 展開に現在有効なライセンスがない（または評価期間内でない）場合は、アップグレードする前に有効なライセンスを登録する必要があります。
  - ライセンスを管理するには、サイト管理権限が必要です。
  - ライセンスのステータスを表示するには、Cisco Secure Workload Web ポータルで **[モニタリング（Monitoring）]** > **[ライセンス（Licenses）]** を選択します。クラスタライセンスの登録がコンプライアンスに違反している場合は、[アクションの実行（Take action）] リンクを含むバナーが表示されます。ライセンスの取得と登録については、Cisco Secure Workload Web ポータルで、**[ヘルプ（Help）]** > **[ページレベルのヘルプ（Page-level Help）]** を選択し、ライセンスを探します。

手順

ステップ 1 Cisco.com からの展開に適用可能な RPM ファイルをダウンロードします。

a) https://software.cisco.com/download/home/286309796/type に移動します。

b) 必要に応じて次をダウンロードします。

- 8-RU または 39-RU システムの場合は、次の RPM をダウンロードします。
  - tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm
- 仮想システムの場合は、次の RPM をダウンロードします。
  - tetration_os_ova_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_enforcement_k9-3.7.1.5-5.el6.x86_64.rpm

c) ダウンロードした RPM の MD5 チェックサムが CCO の MD5 チェックサムと一致することを確認します。

ステップ 2 システムの正常性を確認します。正常でないサービスがある場合は、アップグレードを実行できません。

a) Secure Workload Web インターフェイスで、[設定（Settings）] をクリックし、[メンテナンス（Maintenance）] を選択します。

b) 左ペインで、[サービスステータス（Service Status）] を選択します。

c) グラフで、正常でないサービスを示す赤い円を探します。

または、グラフの上部にあるリストボタンをクリックしてサービス正常性のテーブルビューを表示し、[すべて展開（Expand All）] をクリックし、ページを下にスクロールしてすべてのサービスのステータスを表示します。

d) 正常でないサービスがある場合は、アップグレードを続行する前に、必要な修正を実行してサービスを正常な状態にします。

ステップ 3 左側のナビゲーションメニューで、**[メンテナンス（Maintenance）]** > **[アップグレード（Upgrade）]** を選択します。

ステップ 4 必要に応じて、[アップグレード（Upgrade）] タブをクリックします。

ステップ 5 画面に表示される手順を実行します。どの手順もスキップしないでください。

パッチ アップグレード オプションではなく、[アップグレード（Upgrade）] オプションを使用します。

ステップ 6 [Send Upgrade Link] をクリックします。

サイト管理者またはカスタマーサポートのロールでログインしたユーザーには、アップグレードの実行に使用する必要があるハイパーリンクが記載された電子メールが送信されます。電子メールの件名は次のようになります。

```
[Tetration Analytics] Upgrade Initiation Link
```

電子メールを開き、[クラスタのアップグレード（Upgrade Cluster）] の URL をコピーします。

または、**[メンテナンス（Maintenance）]** > **[Explore]** ページから、次の情報を入力するとアップグレード URL を取得できます。

- [Snapshot Action]：**POST**
- [Snapshot Host]：**orchestrator.service.consul**
- [Snapshot Path]：**upgrade_url**

ステップ 7 Google Chrome で、アップグレード URL をアドレスフィールドに貼り付け、**Enter** キーを押します。

Cisco Secure Workload Setup ポータルが表示されます。アップグレードでサポートされている Web ブラウザは Google Chrome のみであることに注意してください。

ステップ 8 Cisco Secure Workload Setup ポータルで、設定に応じて特定の順序で RPM をアップグレードする必要があります。RPM ファイルをアップロードするには、次のアクションを実行します。

a) [ファイルの選択（Choose File）] をクリックします。
b) RPM ファイルに移動して選択し、[開く（Open）] をクリックします。
c) [アップロード（Upload）] をクリックします。
d) RPM ファイルごとに **a** ～ **c** の手順を繰り返します。
各 RPM をアップロードしてもページの RPM のリストは更新されませんが、これは予期されたことです。*tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm* ファイルをアップロードした後にエラーが表示された場合は、5 ～ 10 分待ってからページをリロードします。これで、アップロードされた RPM のリストを表示できるはずです。

8-RU または 39-RU システムの場合は、次のファイルを指定された順序でアップロードします。

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm

- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm

仮想システムの場合は、次のファイルを指定された順序でアップロードします。

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_ova_k9-3.7.1.5-1.noarch.rpm

ステップ 9 [続行（Continue）] をクリックします。
[サイト構成（Site Config）] ポータルが表示されます。

ステップ 10 （オプション） [全般（General）] で、SSH 公開キーを変更し、[次へ（Next）] をクリックします。

ステップ 11 （オプション） [電子メール（Email）] で、UI 管理者または管理者の電子メールアドレスを変更し、[次へ（Next）] をクリックします。

ステップ 12 （オプション）[L3] で、アップグレード後に特定のクラスタ接続のためにクラスタが IPv4 に加えて IPv6 アドレスを使用できるようにします。IPv6 を有効にするには、次の手順を実行します。

a) [IPv6] チェックボックスをオンにします。
b) リーフ 1 とリーフ 2 の両方のスイッチの IPv6 アドレスを CIDR 表記で入力します。
c) リーフ 1 とリーフ 2 の IPv6 デフォルトゲートウェイを入力します。
d) [次へ（Next）] をクリックします。

このページで IPv6 を有効にする場合は、次の手順で説明するように [ネットワーク（Network）] ページで IPv6 フィールドも構成する必要があります。

重要 デュアルスタックモードの要件と制限については、（オプション）デュアルスタックモード（IPv6 サポート）の要件と制限事項 （1 ページ）を参照してください。

ステップ 13 [ネットワーク（Network）] で、次の手順を実行します。

a) 必要に応じて、[CIMC Internal Network]、[CIMC Internal Network Gateway]、[DNS Resolver]、および [DNS Domain] の値を変更します。
b) **重要**既存の [外部ネットワーク（External Network）] の値は変更したり、削除したりしないでください。ただし、別の IPv4 ネットワークを追加することはできます。
c) [L3] ページで IPv6 を有効にした場合は、[IPv6] チェックボックスが自動的に選択されます。次の手順で Cisco Secure Workload を使用するために予約されている IPv6 を指定します。

1. IPv6 外部ネットワークを CIDR 表記で入力します。
2. （オプション） 指定したアドレスにのみ IPv6 を使用するには、個別の外部 IPv6 IP を入力します。

次の点に注意してください。

- [IPv6 External Network] フィールドの最初の 3 つの IPv6 アドレスは、常に Cisco Secure Workload クラスタのスイッチ用に予約されており、他の目的には使用できません。
- 39 RU クラスタの場合、[IPv6 External Network] または [External IPv6 IPs] リストで、少なくとも 29 個の IPv6 アドレスが使用可能であることを確認します。
- 8 RU クラスタの場合、[IPv6 External Network] または [External IPv6 IPs] リストで、少なくとも 20 個の IPv6 アドレスが使用可能であることを確認します。

d) [Next] をクリックします。

ステップ 14 （オプション）[サービス（Service）] で、NTP と SMTP の値を変更し、[次へ（Next）] をクリックします。

syslog 値（ある場合）を変更する必要がある場合は、TAN アプライアンスを使用します。

ステップ 15 [セキュリティ（Security）] で、[エージェント接続用の強力な SSL 暗号（Strong SSL Ciphers for Agent Connections）] を有効または無効にして [次へ（Next）] をクリックします。

[UI] タブ、[詳細設定（Advanced）] タブ、および [復旧（Recovery）] タブの値は変更できません。

クラスタがスタンバイクラスタとして構成されている場合、[復旧（Recovery）] タブではクラスタはスタンバイモードで展開されますが、このモードに含まれている機能は制限されています（ウォームスタンバイモードのみをサポートする）。

ステップ 16 [続行（Continue）] をクリックします。
アップグレードプロセス中に次のチェックが確認のために実行されます。

- RPM のバージョンが正しいかどうか
- クラスタが正常かどうか
- 入力したサイト情報が有効かどうか
- スイッチは正しく構成されており、NX-OS ソフトウェアの新しいバージョンにアップグレードできる
- 情報フィールドが検証されているかどうか
- NTP は展開が開始される前に同期される
- 名前ノードとセカンダリ名前ノードはフェールオーバー状態でない

クラスタスイッチをアップグレードする必要がある場合、このチェックには数分から 1 時間かかることがあります。チェックが完了すると、`TETRATION CLUSTER MyCluster: Verify Token` という件名の電子メールが送信されます。メッセージには、アップグレードを続行するために必要なトークンが含まれています。この電子メールからトークンをコピーします。

ステップ 17 Cisco Secure Workload Setup ポータルで、トークンを [検証トークン（Validation Token）] フィールドに貼り付け、[続行（Continue）] をクリックします。

重要　シスコの従業員から特に指示されない限り、[障害時にインスタンス停止を無視する（Ignore instance stop failure）] チェックボックスをオンにしないでください。

アップグレード プロセスが開始される。3.7.1.5 リリースでは、オーケストレータ VM が残りのコンポーネントの前にアップグレードされます。これには、進行状況バーが 0% から 100% になるまでに 30 ～ 60 分かかることがあります。オーケストレータのアップグレードが完了すると、残りのコンポーネントがアップグレードされ、進行状況バーが 0% から開始されます。緑色の進行状況バーが 100％ に達すると、アップグレードが完了します。すべてのインスタンスのステータスが [展開済み（Deployed）] と表示されます。

ステップ 18　アップグレードを検証します。

a) ブラウザで Secure Workload Web インターフェイスを開きます。
b) 左側の黒いナビゲーションメニューから、[プラットフォーム（Platform）]>[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] を選択します。
c) [履歴（History）] をクリックします。
d) [ステータス（Status）] 列に [成功（Succeeded）] と表示されていることを確認します。

ステップ 19　アップグレードが成功した場合は、[パッチアップグレードリンクを無効にする（Disable Patch Upgrade Link）] をクリックします。

次のタスク

アップグレード後、このリリースの拡張機能を活用するために変更を加えます。

- IPv6 を有効にしている場合は、IPv4 アドレスまたは IPv6 アドレスを使用して Cisco Secure Workload Web インターフェイスにアクセスできます。デフォルトでは、エージェントは IPv4 を使用して引き続きクラスタに接続します。ソフトウェアエージェントが IPv6 を使用してクラスタと通信できるようにする場合は、次の手順を実行します。

  1. Cisco Secure Workload ポータルの左ペインで、**[プラットフォーム（Platform）] > [クラスタ構成（Cluster Configuration）]** を選択します。
  2. Cisco Secure Workload Web ポータルで入手できるユーザーガイドの説明に従って、[センサー VIP FQDN（Sensor VIP FQDN）] の設定を構成します。

- スコープ内で Kubernetes の通常のワークロードのクラスタリングを改善するには、リリース 3.7 へのアップグレード：ポリシー検出での Kubernetes ワークロードの改善されたクラスタリングの有効化 （8 ページ）を参照してください。

リリース 3.7 へのアップグレード：ポリシー検出での Kubernetes ワークロードの改善されたクラスタリングの有効化

この機能は、通常の Kubernetes にのみ適用されます（オーケストレータ構成では、「K8s マネージャータイプ」は「なし」です）。

Kubernetes 外部オーケストレータをすでに構成している場合は、クラスタリングに Kubernetes ラベルメタデータを使用することにより、Kubernetes ワークロードの ADM クラスタリングの結果の精度を向上させるリリース 3.7 の拡張機能を有効にできます。

この拡張機能を有効にするには、アップグレード後に通常の Kubernetes オーケストレータごとに次の手順の両方を実行します。

- 通常の Kubernetes 外部オーケストレータ構成（[管理（Manage）] > [外部オーケストレータ（External Orchestrators）] の下） で、[ポリシー検出クラスタリングに使用（Use for policy discovery clustering）] を有効にして、変更を保存します。
- サービスアカウントにバインドされた ClusterRole に次の権限を追加します。

リソース	Kubernetes の動詞
replicationcontrollers	[get list watch]
replicasets	[get list watch]
導入	[get list watch]
daemonsets	[get list watch]
statefulsets	[get list watch]
雇用	[get list watch]
cronjobs	[get list watch]

これらの権限を含むサンプル clusterrole.yaml（バージョンは若干異なる場合があります）：

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: tetration.read.only
rules:
  - apiGroups:
    - ""
      resources:
        - nodes
        - services
        - endpoints
        - namespaces
        - pods
        - replicationcontrollers
        - ingresses
      verbs:
        - get
        - list
        - watch
  - apiGroups:
    - extensions
    - networking.k8s.io
      resources:
        - ingresses
      verbs:
        - get
        - list
        - watch
```

```
- apiGroups:
  - apps
    resources:
      - replicasets
      - deployments
      - statefulsets
      - daemonsets
    verbs:
      - get
      - list
      - watch
- apiGroups:
  - batch
    resources:
      - jobs
      - cronjobs
    verbs:
      - get
      - list
      - watch
```

Cisco Secure Workload リリース 3.6.1.47 へのアップグレード

以前の 3.6 リリースからこのリリースにアップグレードできます。

始める前に

注意 いずれかのノードが現在稼働停止状態にあるか、サービスが正常でない場合は、アップグレードしないでください。続行する前に、Cisco Technical Assistance Center に問い合わせて問題を修正してください。

- インストーラパッケージをダウンロードします。

  ブラウザで、https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.47 に移動します。

  RPM（`tetration_os_patch_k9-3.6.1.47-1.noarch.rpm`）をダウンロードします。

- アップグレードを実行する前に、システムをバックアップする必要があります。詳細については、アップグレードに関するサブセクションを含む、ユーザーガイドのデータのバックアップと復元（DBR）に関する情報を参照してください。
- 「カスタマーサポート」レベルのアカウントで、トラブルシューティングのために SSH キーがアップロードされていることを確認します。
- サイト管理者権限またはカスタマーサポート権限を持つユーザーとして次の手順を実行する必要があります。
- このアップグレードの部分でサポートされるブラウザは Google Chrome のみです。

手順

ステップ 1 システムの正常性を確認します。正常でないサービスがある場合は、アップグレードを実行できません。

a) Secure Workload Web インターフェイスで、ウィンドウの左側にあるナビゲーションメニューから [トラブルシューティング（Troubleshoot）] > [サービスステータス（Service Status）] を選択します。

b) グラフで、正常でないサービスを示す赤い円を探します。

または、グラフの上部にあるリストボタンをクリックしてサービス正常性のテーブルビューを表示し、[すべて展開（Expand All）] をクリックし、ページを下にスクロールしてすべてのサービスのステータスを表示します。

c) 正常でないサービスがある場合は、アップグレードを続行する前に、必要な修正を実行してサービスを正常な状態にします。

ステップ 2 Secure Workload Web インターフェイスで、ウィンドウの左側にあるメニューから [プラットフォーム（Platform）] > [アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] をクリックします。

ステップ 3 表示される手順に従います。

続行する前に、事前チェックで見つかった問題に対処します。

[パッチアップグレード（Patch Upgrade）] が選択されていることを確認します。（これはパッチアップグレードです）。

[Send Upgrade Link] をクリックします。

ステップ 4 次の件名の電子メール メッセージを探します。

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

このメッセージには、アップグレードを実行するために使用する必要があるハイパーリンクが含まれています。

ステップ 5 電子メールのメッセージで、[パッチアップグレード <クラスタ>（Patch Upgrade <Cluster>）] リンクをクリックして Secure Workload セットアップ ユーザー インターフェイスを開きます。Google Chrome ブラウザを使用する必要があります。

ステップ 6 [ファイルの選択（Choose File）] をクリックします。

ステップ 7 上記でダウンロードしたパッチ RPM に移動して選択し、[開く（Open）] をクリックします。

ステップ 8 [アップロード（Upload）] をクリックします。

RPM をアップロードすると、アップグレードが開始されます。

このプロセスの間はセットアップユーザーインターフェイスへの接続が一時的に失われます。

ステップ 9 Web インターフェイスにアクセスしてアップグレード結果が表示できるようになるまで数分待ちます。

アップグレードに問題がある場合は、赤いバナーが表示されます。本の画像をクリックしてログを表示します。

ステップ 10 アップグレードを検証します。

a) ブラウザで Secure Workload Web インターフェイスを開きます。
b) 左側の黒いナビゲーションメニューから、[プラットフォーム（Platform）]>[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] を選択します。
c) [履歴（History）] をクリックします。
d) [ステータス（Status）] 列に [成功（Succeeded）] と表示されていることを確認します。

ステップ 11 アップグレードが成功した場合は、[パッチアップグレードリンクを無効にする（Disable Patch Upgrade Link）] をクリックします。

Cisco Secure Workload リリース 3.6.1.36 へのアップグレード

以前の 3.6 リリースからこのリリースにアップグレードできます。

始める前に

注意 いずれかのノードが現在稼働停止状態にあるか、サービスが正常でない場合は、アップグレードしないでください。続行する前に、Cisco Technical Assistance Center に問い合わせて問題を修正してください。

- インストーラパッケージをダウンロードします。

  ブラウザで、https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.36 に移動します。

  RPM（`tetration_os_patch_k9-3.6.1.36-1.noarch.rpm`）をダウンロードします。

- アップグレードを実行する前に、システムをバックアップする必要があります。詳細については、アップグレードに関するサブセクションを含む、ユーザーガイドのデータのバックアップと復元（DBR）に関する情報を参照してください。
- 「カスタマーサポート」レベルのアカウントで、トラブルシューティングのために SSH キーがアップロードされていることを確認します。
- サイト管理者権限またはカスタマーサポート権限を持つユーザーとして次の手順を実行する必要があります。
- このアップグレードの部分でサポートされるブラウザは Google Chrome のみです。

手順

ステップ 1 システムの正常性を確認します。正常でないサービスがある場合は、アップグレードを実行できません。

a) Secure Workload Web インターフェイスで、ウィンドウの左側にあるナビゲーションメニューから [トラブルシューティング（Troubleshoot）] > [サービスステータス（Service Status）] を選択します。

b) グラフで、正常でないサービスを示す赤い円を探します。

または、グラフの上部にあるリストボタンをクリックしてサービス正常性のテーブルビューを表示し、[すべて展開（Expand All）] をクリックし、ページを下にスクロールしてすべてのサービスのステータスを表示します。

c) 正常でないサービスがある場合は、アップグレードを続行する前に、必要な修正を実行してサービスを正常な状態にします。

ステップ 2 Secure Workload Web インターフェイスで、ウィンドウの左側にあるメニューから [プラットフォーム（Platform）] > [アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] をクリックします。

ステップ 3 表示される手順に従います。

続行する前に、事前チェックで見つかった問題に対処します。

[パッチアップグレード（Patch Upgrade）] が選択されていることを確認します。（これはパッチアップグレードです）。

[Send Upgrade Link] をクリックします。

ステップ 4 次の件名の電子メール メッセージを探します。

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

このメッセージには、アップグレードを実行するために使用する必要があるハイパーリンクが含まれています。

ステップ 5 電子メールのメッセージで、[パッチアップグレード <クラスタ>（Patch Upgrade <Cluster>）] リンクをクリックして Secure Workload セットアップ ユーザー インターフェイスを開きます。Google Chrome ブラウザを使用する必要があります。

ステップ 6 [ファイルの選択（Choose File）] をクリックします。

ステップ 7 上記でダウンロードしたパッチ RPM に移動して選択し、[開く（Open）] をクリックします。

ステップ 8 [アップロード（Upload）] をクリックします。

RPM をアップロードすると、アップグレードが開始されます。

このプロセスの間はセットアップユーザーインターフェイスへの接続が一時的に失われます。

ステップ 9 Web インターフェイスにアクセスしてアップグレード結果が表示できるようになるまで数分待ちます。

アップグレードに問題がある場合は、赤いバナーが表示されます。本の画像をクリックしてログを表示します。

ステップ 10 アップグレードを検証します。

a) ブラウザで Secure Workload Web インターフェイスを開きます。
b) 左側の黒いナビゲーションメニューから、[プラットフォーム（Platform）]>[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] を選択します。
c) [履歴（History）] をクリックします。
d) [ステータス（Status）] 列に [成功（Succeeded）] と表示されていることを確認します。

ステップ 11 アップグレードが成功した場合は、[パッチアップグレードリンクを無効にする（Disable Patch Upgrade Link）] をクリックします。

Cisco Secure Workload リリース 3.6.1.21 へのアップグレード

以前の 3.6 リリースからこのリリースにアップグレードできます。

始める前に

注意 いずれかのノードが現在稼働停止状態にあるか、サービスが正常でない場合は、アップグレードしないでください。続行する前に、Cisco Technical Assistance Center に問い合わせて問題を修正してください。

- インストーラパッケージをダウンロードします。

  ブラウザで、https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.21 に移動します。

  RPM（`tetration_os_patch_k9-3.6.1.21-1.noarch.rpm`）をダウンロードします。

- アップグレードを実行する前に、システムをバックアップする必要があります。詳細については、アップグレードに関するサブセクションを含む、ユーザーガイドのデータのバックアップと復元（DBR）に関する情報を参照してください。
- 「カスタマーサポート」レベルのアカウントで、トラブルシューティングのために SSH キーがアップロードされていることを確認します。
- サイト管理者権限またはカスタマーサポート権限を持つユーザーとして次の手順を実行する必要があります。
- このアップグレードの部分でサポートされるブラウザは Google Chrome のみです。

手順

ステップ 1 システムの正常性を確認します。正常でないサービスがある場合は、アップグレードを実行できません。

a) Secure Workload Web インターフェイスで、ウィンドウの左側にあるナビゲーションメニューから [トラブルシューティング（Troubleshoot）] > [サービスステータス（Service Status）] を選択します。

b) グラフで、正常でないサービスを示す赤い円を探します。

または、グラフの上部にあるリストボタンをクリックしてサービス正常性のテーブルビューを表示し、[すべて展開（Expand All）] をクリックし、ページを下にスクロールしてすべてのサービスのステータスを表示します。

c) 正常でないサービスがある場合は、アップグレードを続行する前に、必要な修正を実行してサービスを正常な状態にします。

ステップ 2 Secure Workload Web インターフェイスで、ウィンドウの左側にあるメニューから [プラットフォーム（Platform）] > [アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] をクリックします。

ステップ 3 表示される手順に従います。

続行する前に、事前チェックで見つかった問題に対処します。

[パッチアップグレード（Patch Upgrade）] が選択されていることを確認します。（これはパッチアップグレードです）。

[Send Upgrade Link] をクリックします。

ステップ 4 次の件名の電子メール メッセージを探します。

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

このメッセージには、アップグレードを実行するために使用する必要があるハイパーリンクが含まれています。

ステップ 5 電子メールのメッセージで、[パッチアップグレード <クラスタ>（Patch Upgrade <Cluster>）] リンクをクリックして Secure Workload セットアップ ユーザー インターフェイスを開きます。Google Chrome ブラウザを使用する必要があります。

ステップ 6 [ファイルの選択（Choose File）] をクリックします。

ステップ 7 上記でダウンロードしたパッチ RPM に移動して選択し、[開く（Open）] をクリックします。

ステップ 8 [アップロード（Upload）] をクリックします。

RPM をアップロードすると、アップグレードが開始されます。

このプロセスの間、セットアップユーザーインターフェイスへの接続が一時的に失われます。

ステップ 9 Web インターフェイスにアクセスしてアップグレード結果が表示できるようになるまで数分待ちます。

アップグレードに問題がある場合は、赤いバナーが表示されます。本の画像をクリックしてログを表示します。

ステップ 10 アップグレードを検証します。

a) ブラウザで Secure Workload Web インターフェイスを開きます。
b) 左側の黒いナビゲーションメニューから、[プラットフォーム（Platform）]>[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] を選択します。
c) [履歴（History）] をクリックします。
d) [ステータス（Status）] 列に [成功（Succeeded）] と表示されていることを確認します。

ステップ 11 アップグレードが成功した場合は、[パッチアップグレードリンクを無効にする（Disable Patch Upgrade Link）] をクリックします。

Cisco Secure Workload リリース 3.6.1.17 へのアップグレード

リリース 3.6.1.5 から 3.6.1.17 リリースにアップグレードできます。

始める前に

注意 いずれかのノードが現在稼働停止状態にあるか、サービスが正常でない場合は、アップグレードしないでください。続行する前に、Cisco Technical Assistance Center に問い合わせて問題を修正してください。

- インストーラパッケージをダウンロードします。

  ブラウザで、https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.17 に移動します。

  RPM（`tetration_os_patch_k9-3.6.1.17-1.noarch.rpm`）をダウンロードします。

- アップグレードを実行する前に、システムをバックアップする必要があります。詳細については、アップグレードに関するサブセクションを含む、ユーザーガイドのデータのバックアップと復元（DBR）に関する情報を参照してください。
- 「カスタマーサポート」レベルのアカウントで、トラブルシューティングのために SSH キーがアップロードされていることを確認します。
- サイト管理者権限またはカスタマーサポート権限を持つユーザーとして次の手順を実行する必要があります。
- このアップグレードの部分でサポートされるブラウザは Google Chrome のみです。

手順

ステップ 1 システムの正常性を確認します。正常でないサービスがある場合は、アップグレードを実行できません。

a) Secure Workload Web インターフェイスで、ウィンドウの左側にあるナビゲーションメニューから [トラブルシューティング（Troubleshoot）] > [サービスステータス（Service Status）] を選択します。

b) グラフで、正常でないサービスを示す赤い円を探します。

または、グラフの上部にあるリストボタンをクリックしてサービス正常性のテーブルビューを表示し、[すべて展開（Expand All）] をクリックし、ページを下にスクロールしてすべてのサービスのステータスを表示します。

c) 正常でないサービスがある場合は、アップグレードを続行する前に、必要な修正を実行してサービスを正常な状態にします。

ステップ 2 Secure Workload Web インターフェイスで、ウィンドウの左側にあるメニューから [プラットフォーム（Platform）] > [アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] をクリックします。

ステップ 3 表示される手順に従います。

続行する前に、事前チェックで見つかった問題に対処します。

[パッチアップグレード（Patch Upgrade）] が選択されていることを確認します。（これはパッチアップグレードです）。

[Send Upgrade Link] をクリックします。

ステップ 4 次の件名の電子メール メッセージを探します。

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

このメッセージには、アップグレードを実行するために使用する必要があるハイパーリンクが含まれています。

ステップ 5 電子メールのメッセージで、[パッチアップグレード <クラスタ>（Patch Upgrade <Cluster>）] リンクをクリックして Secure Workload セットアップ ユーザー インターフェイスを開きます。Google Chrome ブラウザを使用する必要があります。

ステップ 6 [ファイルの選択（Choose File）] をクリックします。

ステップ 7 上記でダウンロードしたパッチ RPM に移動して選択し、[開く（Open）] をクリックします。

ステップ 8 [アップロード（Upload）] をクリックします。

RPM をアップロードすると、アップグレードが開始されます。

このプロセスの間はセットアップユーザーインターフェイスへの接続が一時的に失われます。

ステップ 9 Web インターフェイスにアクセスしてアップグレード結果が表示できるようになるまで数分待ちます。

アップグレードに問題がある場合は、赤いバナーが表示されます。本の画像をクリックしてログを表示します。

ステップ 10 アップグレードを検証します。

a) ブラウザで Secure Workload Web インターフェイスを開きます。
b) 左側の黒いナビゲーションメニューから、[プラットフォーム（Platform）]>[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] を選択します。
c) [履歴（History）] をクリックします。
d) [ステータス（Status）] 列に [成功（Succeeded）] と表示されていることを確認します。

ステップ 11 アップグレードが成功した場合は、[パッチアップグレードリンクを無効にする（Disable Patch Upgrade Link）] をクリックします。

Cisco Secure Workload リリース 3.6.1.5 へのアップグレード

どの3.5.1.xリリースからもこのリリースにアップグレードできますが、このリリースにアップグレードする前に、最新の3.5.1.xパッチリリースにアップグレードすることをお勧めします。

これらの手順は、ハードウェア展開と仮想展開の両方に有効です。

始める前に

⚠

注意 いずれかのノードが現在稼働停止状態にあるか、サービスが正常でない場合は、アップグレードしないでください。続行する前に、Cisco Technical Assistance Center（TAC）に問い合わせて問題を修正してください。

追加の前提条件：

- **ライセンシング**

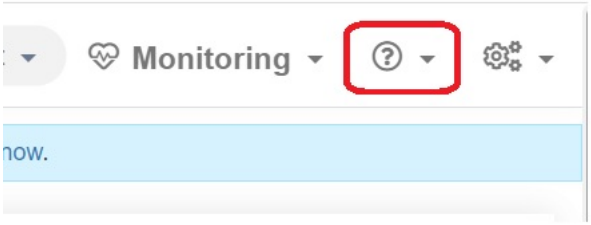
  Tetration展開に現在有効なライセンスがない（または評価期間内でない） 場合は、アップグレードする前に有効なライセンスを登録する必要があります。

  ライセンスを管理するには、サイト管理権限が必要です。

  ライセンスのステータスを表示するには、次の手順を実行します。

  Tetration Web ポータルで、[モニタリング（Monitoring）]>[ライセンス（Licenses）][管理（Manage）]>[ライセンス（Licenses）] を選択します。クラスタライセンスの登録がコンプライアンスに違反している場合は、[アクションの実行（Take action）] リンクを含むバナーが表示されます。

  ライセンスの取得と登録については、次をクリックして、Tetration Web ポータルのユーザー ガイドを参照してください。



ユーザーガイドで「ライセンス」を検索します。

- **IPv6 サポート（デュアルスタックモード）**

  （オプション）物理ハードウェア上で実行される Cisco Secure Workload クラスタは、クラスタおよびクラスタ内の特定の通信に、IPv4 だけでなく IPv6 も使用するように設定できます。（Cisco Secure Workload は、ポリシー目的にかかわらず、すでに IPv6 トラフィックを処理しています。）

  この機能は、初期展開時またはリリース 3.6.1.5 へのアップグレード時にのみ有効にできます。

  デュアルスタック（IPv6）接続の有効化を検討している場合は、（オプション）デュアルスタックモード（IPv6 サポート）の要件と制限事項 （1 ページ）を参照してください。

- **その他の機能**

  アップグレード前にアクションが必要なる可能性がある機能固有の影響：

  - **Firepower Management Center（FMC）の統合**：

    Cisco Secure Workload をアップグレードし、この統合を引き続き使用する場合は、最初に FMC を必要なバージョンにアップグレードする必要があります。

    3.6 でのこの統合は、3.5 の実装とは大きく異なります。https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html から入手可能な『*Cisco Secure Workload and Firepower Management Center Integration Guide*』のバージョン 3.6 の説明と要件をよく読んでください。

    Cisco Secure Workload のアップグレード後は、FMC のプレフィルタポリシーはアクセス コントロール ポリシーに変換され、インベントリフィルタは動的オブジェクトに変換されます。

  - **AWS コネクタ**：

    既存の AWS コネクタはアップグレード時に削除されます。アップグレード後、新しいAWSクラウドコネクタを再作成する必要があります。必要に応じて、アップグレード前に構成された情報をメモしておきます。

  - Kubernetes EKS 外部オーケストレータ

    アップグレード後、EKS外部オーケストレータは読み取り専用になります。アップグレード後に変更を加える場合は、新しい AWS コネクタを作成し、[マネージド Kubernetes サービス（Managed Kubernetes services）] オプションを有効にします。

- **データエクスポートコネクタ**：

  データエクスポートコネクタ（Alpha 機能）のサポートはこのリリース以降、除外されています。データエクスポートコネクタを構成していた場合は、このリリースにアップグレードする前に無効化するか、または削除することをお勧めします。

- **詳細の変更:**

  アップグレード前にアクションを必要としない追加の動作変更については、https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html から入手可能なバージョン 3.6.1.5 のリリースノートを参照してください。

- このアップグレードでは、新しいパブリックルーティング可能な IP アドレスは必要ありません。
- このアップグレードを実行するには、カスタマー サポートの権限が必要です。
- カスタマーサポート権限のあるユーザーアカウントにはトラブルシューティングのための SSH キーがアップロードされていることを確認します。詳細については、Tetration Web ポータルから入手可能なユーザーガイドの「SSH 公開キーのインポート」を参照してください。
- アップグレードを実行する前に、システムをバックアップする必要があります。詳細については、アップグレードに関するサブセクションを含む、ユーザーガイドのデータのバックアップと復元（DBR）に関する情報を参照してください。
- Google Chrome は、このアップグレードの一部で必要となる専用ポータルである Cisco Secure Workload Setup ポータルでサポートされる唯一のブラウザです。

手順

ステップ 1 Cisco.com からの展開に適用可能な RPM ファイルをダウンロードします。

a) https://software.cisco.com/download/home/286309796/type にアクセスします。

b) 必要に応じて次をダウンロードします。

- 8-RU または 39-RU システムの場合は、次の RPM をダウンロードします。
  - `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`
  - `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`
  - `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
  - `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
- 仮想システムの場合は、次の RPM をダウンロードします。
  - `tetration_os_ova_k9-3.6.1.5-1.el7.x86_64.rpm`

- `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
- `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
- `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
- `tetration_os_enforcement_k9-3.6.1.5-5.el6.x86_64.rpm`

c) ダウンロードした各 RPM の MD5 が CCO の MD5 と一致することを確認します。

ステップ 2 システムの正常性を確認します。正常でないサービスがある場合は、アップグレードを実行できません。

a) Cisco Tetration GUI で、[Settings] ボタンをクリックし、[Maintenance] を選択します。
b) 左ペインで、[Service Status] をクリックします。
c) グラフで、正常でないサービスを示す赤い円を探します。

または、グラフの上部にあるリストボタンをクリックしてサービス正常性のテーブルビューを表示し、[すべて展開（Expand All）] をクリックし、ページを下にスクロールしてすべてのサービスのステータスを表示します。

d) 正常でないサービスがある場合は、アップグレードを続行する前に、必要な修正を実行してサービスを正常な状態にします。

ステップ 3 左側のナビゲーションメニューで、[メンテナンス（Maintenance）] > [アップグレード（Upgrade）] をクリックします。

ステップ 4 必要に応じて、[アップグレード（Upgrade）] タブをクリックします。

ステップ 5 画面に表示される手順を実行します。どの手順もスキップしないでください。

パッチ アップグレード オプションではなく、[アップグレード（Upgrade）] オプションを使用します。

ステップ 6 [アップグレードリンクの送信（Send Upgrade Link）] をクリックした後、結果の電子メールメッセージを探します。

サイト管理者またはカスタマーサポートロールでログインしたユーザーには、アップグレードの実行に使用する必要があるハイパーリンクが記載された電子メールが送信されます。電子メールの件名は次のようになります。

```
[Tetration Analytics] Upgrade Initiation Link
```

電子メールメッセージを開き、[クラスタのアップグレード（Upgrade Cluster）] の URL をコピーします。

または、**[メンテナンス（Maintenance）] > [Explore]** ページから、次の情報を入力するとアップグレード URL を取得できます。

- [Snapshot Action]：**POST**
- [Snapshot Host]：**orchestrator.service.consul**
- [Snapshot Path]：**upgrade_url**

ステップ 7 新しい Google Chrome ブラウザタブを開き、アップグレード URL をアドレスフィールドに貼り付けて **Enter** を押します。

これにより Cisco Secure Workload Setup ポータルが開きます。このポータルは、Google Chrome ブラウザでのみサポートされます。

ステップ 8 Cisco Secure Workload Setup ポータルで、設定に応じて特定の順序で RPM をアップグレードする必要があります。

8-RU または 39-RU システムの場合は、次のファイルを指定された順序でアップロードします。

1. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
2. `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`
3. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
4. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
5. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
6. `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`

仮想システムの場合は、次のファイルを指定された順序でアップロードします。

1. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
2. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
3. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
4. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
5. `tetration_os_ova_k9-3.6.1.5-1.el7.x86_64.rpm`

各 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。

各 RPM をアップロードすると、ページの RPM のリストは更新されません。これは予想どおりの結果です。

`tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm` ファイルのアップロード後にエラーが表示された場合は、5 ～ 10 分待ってから、ページをリロードします。ページをリロードした後、アップロードされた RPM のリストが表示されるはずです。

d) 各 RPM の次のサブステップを繰り返します。

ステップ 9 [Continue] をクリックします。

[サイト構成（Site Config）] ポータルが開きます。

ステップ 10 [全般（General）] タブで次の手順を実行します。

（オプション）SSH 公開キーを変更します。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [電子メール（Email）] タブで次の手順を実行します。

（オプション）UI 管理者の電子メールアドレスまたはアドミラルアラート電子メールアドレスを変更します。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 [L3] タブで次の手順を実行します。

（オプション）アップグレード後の特定のクラスタ接続で、クラスタが IPv4 に加えて IPv6 を使用できるようにします。

重要：要件と制限については、この手順の前提条件にあるリンクを参照してください。

IPv6 を有効にするには、次の手順を実行します。

a) [IPv6] チェックボックスを選択します。
b) リーフ 1 と リーフ 2 の両方のスイッチの **IPv6 アドレスを CIDR 表記で**入力します。
c) リーフ 1 とリーフ 2 の **IPv6 デフォルトゲートウェイ**を入力します。

このページで IPv6 を有効にすると、次に示す [ネットワーク（Network）] ページで IPv6 フィールドも構成する必要があります。

ステップ 15 [次へ（Next）] をクリックします。

ステップ 16 [ネットワーク（Network）] タブで次の手順を実行します。

- 必要に応じて、[CIMC Internal Network]、[CIMC Internal Network Gateway]、[DNS Resolver]、および [DNS Domain] の値を変更します。
- **重要**既存の [外部ネットワーク（External Network）] の値は変更したり、削除したりしないでください。ただし、別の IPv4 ネットワークを追加することはできます。
- [L3] ページで IPv6 を有効にした場合は、次の手順を実行します。

  [IPv6] チェックボックスは自動的に選択されます。

  次の手順で Cisco Secure Workload を使用するために予約されている IPv6 を指定します。

  a. **IPv6 外部ネットワークを CIDR 表記で**入力します。

  b. （オプション） 指定したアドレスにのみ IPv6 を使用するには、個別の**外部 IPv6 IP** を入力します。

  次のことに注意してください。

  - [IPv6 External Network] フィールドの最初の 3 つの IPv6 アドレスは、常に Cisco Secure Workload クラスタのスイッチ用に予約されており、他の目的には使用できません。
  - 39 RU クラスタの場合、[IPv6 External Network] または [External IPv6 IPs] リストで、少なくとも 29 個の IPv6 アドレスが使用可能であることを確認します。
  - 8 RU クラスタの場合、[IPv6 External Network] または [External IPv6 IPs] リストで、少なくとも 20 個の IPv6 アドレスが使用可能であることを確認します。

ステップ 17 [Next] をクリックします。

ステップ 18 [サービス（Service）] タブで次の手順を実行します。

（オプション）NTP と SMTP の値を変更します。

syslog 値（ある場合）を変更する必要がある場合は、TAN アプライアンスを使用します。

ステップ 19 [次へ（Next）] をクリックします。

ステップ 20 [セキュリティ（Security）] タブで次の手順を実行します。

[エージェント接続用の強力な SSL 暗号（Strong SSL Ciphers for Agent Connections）] を有効または無効にます。

ステップ 21 [次へ（Next）] をクリックします。

[UI] タブのどの値も変更できません。

ステップ 22 [次へ（Next）] をクリックします。

[詳細設定（Advanced）] タブのどの値も変更できません。

ステップ 23 [次へ（Next）] をクリックします。

ステップ 24 [復旧（Recovery）] タブで次の手順を実行します。

クラスタがスタンバイクラスタとして構成されている場合、そのクラスタはスタンバイモードで展開されますが、このモードに含まれている機能は制限されています（ウォームスタンバイモードのみをサポート）。

このタブのどの値も変更できません。

ステップ 25 [Continue] をクリックします。

アップグレード プロセスが開始されます。

アップグレードプロセスでは、次を確認します。

- RPM のバージョンが正しいかどうか
- クラスタが正常かどうか
- 入力したサイト情報が有効かどうか
- スイッチが正しく設定されているかどうか
- 情報フィールドが検証されているかどうか
- NTP は展開が開始される前に同期される
- 名前ノードとセカンダリ名前ノードはフェールオーバー状態でない

チェックには数分かかります。チェックが完了すると、次のような件名の電子メールが届きます。

```
TETRATION CLUSTER MyCluster: Verify Token
```

メッセージには、アップグレードを続行するために必要なトークンが含まれています。

ステップ 26 電子メールメッセージの本文からトークンをコピーします。

ステップ 27 Cisco Secure Workload Setup ポータルで、トークンを [検証トークン（Validation Token）] フィールドに貼り付けます。

重要：シスコの従業員から特に指示されない限り、[Ignore instance stop failure] チェックボックスをオンにしないでください。

ステップ 28 [Continue] をクリックします。

アップグレードのインストールが開始されます。緑色の進行状況バーが 100% に達すると、アップグレードが完了します。すべてのインスタンスのステータスが「Deployed」になります。

ステップ 29 アップグレードを検証します。

a) ブラウザで Cisco Secure Workload Web ポータルを開きます。
b) 左側の黒いナビゲーションメニューから、[プラットフォーム（Platform）]>[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] を選択します。
c) [履歴（History）] をクリックします。
d) アップグレードステータスに [成功（Succeeded）] が表示されていることを確認します。

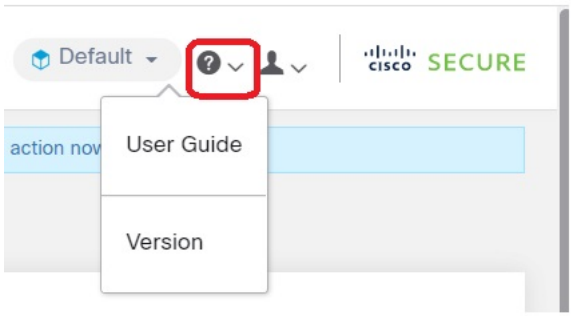
次のタスク

IPv6 を有効にした場合は、次の手順を実行します。

IPv6 または IPv4 を使用して、Cisco Secure Workload Web インターフェイスにアクセスできます。

デフォルトでは、エージェントはIPv4を使用して引き続きクラスタに接続します。ソフトウェアエージェントが IPv6 を使用してクラスタと通信できるようにもするには、次の手順を実行します。

1. Cisco Secure Workload ポータルで、ウィンドウの左側にあるナビゲーションメニューから [プラットフォーム（Platform）] > [クラスタ構成（Cluster Configuration）] を選択します。
2. Cisco Secure Workload Web ポータルのリンクから入手可能なユーザーガイドの説明に従って、[センサー VIP FQDN（Sensor VIP FQDN）] の設定を構成します。



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。