



ユーザーインターフェイスの設定

- [\(オプション\) デュアルスタックモード \(IPv6 サポート\) の要件と制限事項 \(1 ページ\)](#)
- [ユーザーインターフェイスの設定 \(3 ページ\)](#)

(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 も使用するよう設定できます。



- (注) リリース 3.6.1.5、3.7.1.5、および 3.8.1.1 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、この機能を有効にするオプションは使用できません。
-

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、物理ハードウェアまたは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 3.8.1.1、3.7.1.5、および 3.6.x に適用) AIX エージェントでの適用
 - (リリース 3.6.x のみに適用) 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 のみに適用) 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

- クラスタのデュアルスタックモードを有効にする前に、FQDN の A および AAAA DNS レコードの両方を設定します。
- 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、次の要件に従います。
 - 2つのクラスタリーフスイッチのそれぞれには、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 User Guide』を参照してください。

ユーザーインターフェイスの設定

始める前に

- この設定を完了するには、インターネットにアクセスするために、イーサネットポート付きのラップトップコンピューターなどのデバイスが必要です。
- Cisco Secure Workload クラスタの最上位のサーバーにデバイスを接続するには、イーサネットケーブルが必要です。
- Google Chrome は、この手順の一部で必要となるセットアップポータルでサポートされる唯一のブラウザです。
- (オプション) バージョン 3.6 以降では、デュアルスタックモードでクラスタを設定できるため、一部の Cisco Secure Workload コンポーネント間、および Cisco Secure Workload と NTP や DNS などのネットワークサービス間の通信に、IPv4 と IPv6 の両方を使用できます。(デュアルワークロードモードを有効化するかどうかにかかわらず、Cisco Secure Workload はすでに IPv6 トラフィックを処理しています。) このサポートは、展開時またはアップグレード時にのみ有効化できます。

IPv6 のサポート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。



重要 フィールド名に明示的に IPv6 と示されている場合を除き、次の手順のすべてのフィールドに IPv4 アドレスを入力します。

ステップ 1 インターネット デバイスに IP アドレス 2.2.2.1/30 (255.255.255.252) を設定します。

ステップ 2 Cisco Secure Workload クラスタの最上位のサーバーの LOM ポート 2 (LAN2) にインターネットデバイスのイーサネットポートを接続するには、イーサネットケーブルを使用します。

ステップ 3 インターネット デバイスで、Chrome ブラウザを開き <http://2.2.2.2:9000> に移動します。

(注) Chrome ブラウザは、このプロセスでテストした唯一のブラウザです。

セットアップ診断ページが開きます。

ステップ 4 診断ページにエラーがある場合は、この手順を継続する前に、クラスタ デバイスの間のケーブル接続に破損した接続がないかどうか、またはケーブルが間違っていて経路指定されていないかどうかをチェックします。完了したら、ステップ 2 に戻ります。

正しい配線については、[C1-Workload クラスタデバイスのケーブル配線](#)および[C1-Workload-M クラスタデバイスのケーブル配線](#)を参照してください。

ステップ 5 [継続 (Continue)] をクリックします。

RPM アップロード ページが開きます。

- (注) サイト設定ページが代わりに開いた場合、次の URL を入力して、RPM アップロード ページを開きます。

http://2.2.2.2:9000/upload

ステップ 6 Cisco Secure Workload クラウドに RPM ファイルをアップロードします。

次の順序でファイルをアップロードする必要があります。

- tetration_os_rpminstall_k9
 - tetration_os_UcsFirmware_k9
 - tetration_os_adhoc_k9
 - tetration_os_mother_rpm_k9
 - tetration_os_base_rpm_k9
- a) [ファイルの選択 (Choose File)] をクリックします。
 - b) RPM 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。

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。これは想定されている動作です。

tetration_os_mother_rpm_k9-2.1.1.31-1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、約 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が、エラーは Orchestrator の再起動によるものであり、問題ではありません。

- d) それぞれの RPM について a ~ c のステップを繰り返します。

RPM のアップロードが完了すると、[サイト設定 (Site Config)] ページが開きます。

ステップ 7 [サイト設定 (Site Config)] ページを使用して、次のように新しいサイトを設定します。

- [一般 (General)] をクリックします。
 1. [サイト名 (Site Name)] フィールドに、一意のクラスタ名を入力します。
 2. [SSH パブリックキー (SSH Public Key)] フィールドに、認証キーを貼り付けます。

(注) クラスタ SSH アクセスに使用できる独自の SSH キーペアを生成します。

ta_guest アクセスを使用してクラスタをトラブルシューティングまたは回復するために、SSH キーを安全で永続的な場所に保管しておくことを強く推奨します。
 3. [次へ (Next)] をクリックします。
- [電子メール (Email)] をクリックします。
 1. 必要な電子メールアドレスを入力します。

2. [次へ (Next)]をクリックします。
- [L3] をクリックします。

要求された各アドレスを入力します。* が付いたすべてのフィールドは必須フィールドです。

フィールド名に IPv6 が指定されていない場合は、すべてのアドレスを IPv4 として入力します。

(オプション) ソフトウェアバージョン 3.6 以降をインストールする場合：デュアルスタックモード (IPv4 と IPv6 の両方をサポート) を有効にします。

 1. [IPv6] チェックボックスを選択します。
 2. Leaf 1 と Leaf 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。
 3. Leaf 1 と Leaf 2 の IPv6 デフォルトゲートウェイを入力します。
 4. [次へ (Next)]をクリックします。
 - [ネットワーク (Network)] をクリックします。

フィールド名に IPv6 が指定されていない場合は、すべてのアドレスを IPv4 として入力します。

 1. [内部ネットワーク IP アドレス (Internal network IP address)] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
 2. [外部ネットワーク IP アドレス (External network IP address)] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
 3. [外部ゲートウェイ IP アドレス (External gateway IP address)] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
 4. [DNS リゾルバ IP アドレス (DNS resolver IP address)] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
 5. [DNS ドメイン (DNS Domain)] フィールドに、DNS ドメイン (たとえば「**cisco.com**」) を入力します。
 6. (ソフトウェアバージョン 3.6 以降) [L3] ページで IPv6 を有効化した場合は、[IPv6] が自動的に選択されます。

IPv6 が選択された場合は、Cisco Secure Workload 用に予約されている IPv6 アドレスを指定する必要があります。

 - [外部 IPv6 ネットワーク (External IPv6 Network)] を入力します。

[外部 IPv6 ネットワーク (External IPv6 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。
 - 特定のアドレスにのみ IPv6 を使用する場合は、[外部 IPv6 ネットワーク (External IPv6 Network)] フィールドにそれらのアドレスを入力します。

- (注)
- 39 RU クラスタの場合、[IPv6 外部 ネットワーク (IPv6 External Network)] または [外部 IPv6 IPs (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 外部 ネットワーク (IPv6 External Network)] または [外部 IPv6 IPs (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。

7. [次へ (Next)] をクリックします。

• [サービス (Service)] をクリックします。

1. [NTPサーバー (NTP Servers)] フィールドに、オーケストレータ展開出力から NTP サーバー名または IP アドレスのスペース区切りのリストを入力します。
2. [SMTPサーバー (SMTP Server)] フィールドに、Cisco Secure Workload が電子メールメッセージの送信に使用できる SMTP サーバーの名前または IP アドレスを入力します。このサーバーは Cisco Secure Workload からアクセス可能である必要があります。
3. [SMTPポート (SMTP Port)] フィールドに、SMTP サーバーのポート番号を入力します。AWS は、ポート 25 と 465 の使用を制限します。アカウントを正しく構成するか、またはポート 587 を使用する必要があります。
4. [SMTPユーザー名 (SMTP Username)] フィールドに、SMTP 認証用のユーザー名を入力します。
5. [SMTPパスワード (SMTP Password)] フィールドに、SMTP 認証用のパスワードを入力します。
6. (オプション) [HTTPプロキシサーバー (HTTP Proxy Server)] フィールドに、インターネットの外部サービスにアクセスするために Cisco Secure Workload で使用できる HTTP プロキシサーバーの名前または IP アドレスを入力します。
7. (オプション) [HTTPプロキシサーバー (HTTP Proxy Port)] フィールドに、HTTP プロキシサーバーのポート番号を入力します。
8. (オプション) [HTTPsプロキシサーバー (HTTPs Proxy Server)] フィールドに、インターネットの外部サービスにアクセスするために Cisco Secure Workload で使用できる HTTPs プロキシサーバーの名前または IP アドレスを入力します。
9. (オプション) [HTTPsプロキシサーバー (HTTPs Proxy Port)] フィールドに、HTTPs プロキシサーバーのポート番号を入力します。
10. (オプション) [Syslogサーバー (Syslog Server)] フィールドに、アラートを送信するために Cisco Secure Workload で使用できる syslog サーバーの名前または IP アドレスを入力します。
11. (オプション) [Syslogポート (Syslog Port)] フィールドに、syslog サーバーのポート番号を入力します。
12. (オプション) [Syslogのシビラティ (重大度) (Syslog Severity)] フィールドに、syslog メッセージのシビラティ (重大度) レベルを入力します。可能な値には、情報、警告、エラー、緊急、アラート、重要な注意が含まれます。

13. [次へ (Next)] をクリックします。

• [UI] をクリックします。

1. [UI VRRP VRID] フィールドに、一意の VRID が必要なければ [77] を入力します。
2. [UI FQDN] フィールドに、クラスタにアクセスする完全修飾ドメイン名を入力します。
3. [UI Airbrakeキー (UI Airbrake Key)] フィールドは空白のままにします。
4. [次へ (Next)] をクリックします。

Cisco Tetration (Cisco Secure Workload) は、構成時の設定を検証し、設定のステータスを表示します。

• [詳細設定 (Advanced)] をクリックします。

1. [外部IP (External IPs)] フィールドに、IPv4 アドレスを入力します。
2. [継続 (Continue)] をクリックします。

ステップ 8 障害がある場合は、[戻る (Back)] をクリックし、設定を編集してください (ステップ 7 を参照してください) 。

(注) このページを離れた後でこれらの設定をセットアップ GUI で変更することはできません。ただし、後で GUI の [会社 (company)] ページから設定を変更できます。

ステップ 9 設定に対して検出された障害がなく、変更を加える必要がない場合は、[続行 (Continue)] をクリックします。

Cisco Secure Workload は指定された設定に従って構成します。このプロセスは、ユーザー側の操作なしで 1 ~ 2 時間かかります。

次のタスク

ソフトウェアバージョン 3.6 以降を展開し、IPv6 接続を有効化した場合：

- IPv4 または IPv6 を使用して Cisco Secure Workload Web ポータルにアクセスできます。
- デフォルトでは、クラスタが IPv6 をサポートするために有効化されていても、ソフトウェアエージェントは IPv4 を使用して Cisco Secure Workload クラスタと通信します。この目的のためにサポートされているエージェントで IPv6 を使用する場合は、Cisco Secure Workload Web ポータルの [プラットフォーム (Platform)] > [クラスタ設定 (Cluster Configuration)] ページで、[センサーVIP FQDN (Sensor VIP FQDN)] フィールドを設定する必要があります。重要な指示については、Cisco Secure Workload Web ポータルまたは <https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html> から、オンラインヘルプとして入手可能なユーザーガイドを参照してください。

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。