Cisco Crosswork Network Controller 5.0 インストールガイド

初版：2023 年 5 月 8 日

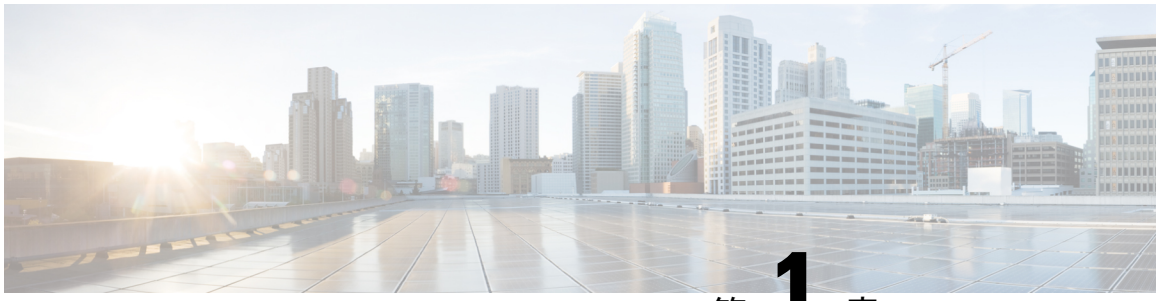
最終更新：2023 年 5 月 30 日

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
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

第 I 部

はじめに



第 1 章

概要

この章は次のトピックで構成されています。

このマニュアルについて

このガイドでは、Crosswork Network Controller solution ソリューションをインストールまたはアップグレードするための要件とプロセスについて説明します。

このドキュメントでは、すでにインストールされているか、独立して使用できる統合コンポーネント（Cisco NSO、Cisco SR-PCE、Cisco WAE など）のインストールについては説明していません。これらのコンポーネントの詳細については、それぞれのインストールマニュアルを参照してください。

（注） このガイドには、Amazon EC2 プラットフォームで Crosswork Network Controller をインストールまたはアップグレードする手順が含まれていますが、これは限定リリース機能としてのみ利用できます。サポートについては、シスコの営業担当者にご連絡ください。

対象読者

このガイドは、ネットワークに Crosswork Network Controller ソリューションをインストールしようとしている経験豊富なネットワークユーザーおよびオペレータを対象としています。このマニュアルは、次に関する知識があることを前提としています。

- Docker コンテナの使用

- Python でのスクリプトの実行
- VMware vCenter を使用した OVF テンプレートの展開
- OVF ツールを使用した展開
- アマゾンウェブサービス（AWS）、Amazon EC2 の概念、および CloudFormation テンプレートの作成

はじめに

Cisco Crosswork インフラストラクチャ、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）、および Crosswork アプリケーションで構成される統合ソリューションである **Cisco Crosswork Network Controller** は、エンドツーエンドのネットワークのプロアクティブな管理を可能にし、インテントベースのクローズドループ自動化ソリューションを提供することで、イノベーションの迅速化、最適なユーザーエクスペリエンス、優れた運用性を実現します。

Cisco Crosswork インフラストラクチャ

Cisco Crosswork インフラストラクチャ は、マイクロサービスベースのプラットフォームであり、Crosswork アプリケーションの実行に必要な基盤となります。拡張性、スケーラビリティ、高可用性を実現するクラスタアーキテクチャを採用しています。Crosswork クラスタは、ハイブリッド構成で動作する 3 つの VM またはノードで構成されます。必要な場合には、展開したアプリケーションの要件に合わせて VM やノードをワーカーの構成に追加できます（最大 2 つのノード）。ハイブリッドノードではインフラストラクチャポッドとアプリケーションポッドを実行できますが、ワーカーノードではアプリケーションポッドのみを実行できます。ハイブリッドノードとワーカーノードの合計数は、ネットワークのサイズと実行されているアプリケーションによって異なります。シスコ カスタマーエクスペリエンス チームと協力して、ネットワークに必要なノードの数を決定してください。

（注） 以降このガイドでは、Cisco Crosswork インフラストラクチャ を「Cisco Crosswork」と呼びます。

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）

Cisco Crosswork は 1 つ以上の Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）と統合し、管理対象デバイスから情報を収集して Cisco Crosswork や外部の宛先に転送します。その後、情報は Crosswork アプリケーションによって分析および処理され、ネットワークの管理やネットワークの変更への対応に使用されます。ネットワークに展開される Crosswork Data Gateway の数は、デバイスの数、収集されるデータの量、全体的なトポロジ、冗長性の要件によって異なります。Crosswork Data Gateway はそれぞれ個別の VM に展開されます。お客様のニーズに最適な展開に関するガイダンスについては、シスコのカスタマーエクスペリエンス チームにお問い合わせください。

Crosswork Data Gateway は、展開される Crosswork ソリューションの不可欠な部分です。このため、このドキュメントでは、Crosswork インフラストラクチャと並行してインストールする必要がある基本コンポーネントとして、Crosswork Data Gateway について説明します。

Crosswork アプリケーション

詳細については、「Cisco Crosswork Network Controller パッケージ （3 ページ）」を参照してください。

その他の統合コンポーネント

Cisco Network Services Orchestrator は、Cisco Crosswork のプロバイダーとして機能し、データ収集用の MDT センサーパスの構成（オプション）など、想定される機能に従ってデバイスを構成します。Cisco NSO はデバイスの管理、構成、およびメンテナンスサービスの重要な機能を提供します。

Cisco セグメントルーティングパス計算要素（SR-PCE）は、セグメント ルーティング トラフィック エンジニアリング（ST-TE）と Resource Reservation Protocol トラフィック エンジニアリング（RSVP-TE）の両方をサポートする IOS-XR マルチドメインステートフル PCE です。Cisco Crosswork は、テレメトリと Cisco SR-PCE から収集されたデータの組み合わせを使用して、最適な TE トンネルのパスを分析および計算したり、ネットワーク内のデバイスを検出したりします。

Cisco Crosswork は、他のプロバイダー（Cisco WAE、Syslog、Alert など）、外部サーバー（TACACS+、LDAP、RADIUS）、DHCP サーバー（Crosswork ZTP を使用する場合）、および外部 Kafka（外部のデータ収集の接続先用）と統合することもできます。これらの特定の統合に関する詳細は、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』またはアプリケーションガイドで説明されています。

Cisco Crosswork Network Controller パッケージ

次の表では、Crosswork Network Controller に展開できる Crosswork アプリケーションと、それらのパッケージ方法について説明します。

（注） Cisco Crosswork Optimization Engine は、他の Crosswork Network Controller アプリケーションなしで独立してインストールできます。詳細については、Crosswork アプリケーションのインストール （193 ページ）を参照してください。

表 *1 : Cisco Crosswork Network Controller* パッケージ

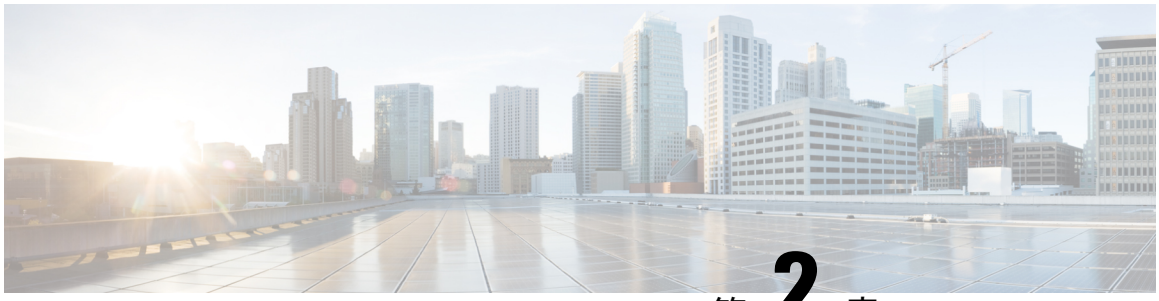
パッケージ	目次	説明
Essentials パッケージ	Cisco Crosswork Optimization Engine	ネットワーク状態のクローズドループ追跡を提供し、ネットワーク状態の変化に応じてネットワークをリアルタイムで最適化するアプリケーション。これにより、オペレータは、ネットワーク容量の使用率を適切に最大化し、サービス速度を向上させることができます。
	Cisco Crosswork アクティブトポロジ	論理マップと地理マップでトポロジとサービスの可視化を可能にする Crosswork Network Controller のコンポーネント。
	要素管理機能	インベントリ、障害、およびソフトウェアイメージ管理（SWIM）機能を使用して、詳細なインベントリ収集、アラーム管理、およびイメージ管理を提供する機能のライブラリ。
Advantage パッケージ	Cisco Crosswork Service Health	環境のサービスレベルビューをオーバーレイし、オペレータが、自分で確立したルールに基づいてサービス（たとえば、L2/L3 VPN）が正常かどうかを簡単にモニターできるようにするアプリケーション。
アドオンパッケージ	Cisco Crosswork Change Automation	ネットワークに変更を展開するプロセスを自動化するアプリケーション。組み込みの Ansible Playbook を使用してオーケストレーションを定義し、設定変更を Cisco Network Services Orchestrator（NSO）にプッシュしてネットワークに展開します。
	Cisco Crosswork Health Insights	リアルタイムで重要業績評価指標（KPI）のモニタリング、アラート、およびトラブルシューティングを実行するアプリケーション。Cisco Crosswork Health Insights は、プログラム可能なモニタリングと分析を実現にし、動的検出モジュールと分析モジュールを構築して、オペレータがユーザー定義のロジックに基づいてネットワークイベントを監視しアラートを生成することを可能にします。
	Cisco Crosswork ゼロタッチプロビジョニング	デイゼロ構成のオンボーディングとプロビジョニングを合理化し、より少ない運用コストで IOS-XR デバイスをより迅速に展開するアプリケーション。

セキュリティ

シスコは、すべての製品が業界の最新の推奨事項に準拠するように大きく進歩しています。セキュリティはエンドツーエンドのコミットメントであると固く信じており、環境全体を保護できるように支援を行っています。シスコのアカウントチームと協力して、ネットワークのセキュリティプロファイルを確認してください。

製品の検証方法について詳しくは、「Cisco Secure Products and Solutions」および「Cisco Security Advisories」を参照してください。

シスコ製品のセキュリティに関して質問や懸念がある場合は、シスコのカスタマーエクスペリエンスチームとのケースを開き、使用しているツールと、そのツールで報告された脆弱性についての詳細をお知らせください。



第 2 章

導入の計画

この章は次のトピックで構成されています。

はじめる前に

このセクションでは、Crosswork Network Controller ソリューションをお好みのプラットフォームにインストールする前に行う必要のあるセットアップオプションについて説明します。

1. 必要なアプリケーションの決定 （7 ページ）
2. リソースのフットプリントの特定 （9 ページ）
3. 特記事項 （12 ページ）

上記のステップで計画を完了したら、プラットフォームに関連するインストールワークフローの手順に従います。

- **VMware vCenter の場合**：VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）
- **AWS EC2 の場合**：AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

Crosswork Network Controller バージョン 4.1 以降、Crosswork 展開は Cisco CSP プラットフォームでサポートされなくなりました。詳細については、「End-of-Life Announcement for the Cisco Cloud Services Platform Operating System」を参照してください。

必要なアプリケーションの決定

まずは実稼働環境のニーズを満たす Crosswork アプリケーションを選択します。各 Crosswork アプリケーションが必要なリソース全体に影響を与える可能性があるため、これは重要なステップです。

（注） Crosswork Network Controller が顧客の展開用にサポートしているのは、「大規模な」展開プロファイルのみです。

Crosswork Network Controller は、次のパッケージで利用できます（詳細については「Cisco Crosswork Network Controller パッケージ （3 ページ）」を参照）。

表 *2 : Crosswork Network Controller* パッケージ

パッケージ [1]	目次	Crosswork Data Gateway の展開 [2]	クラスタ VM の推奨数 [3]
Cisco Crosswork Network Controller Essentials	Cisco Crosswork Optimization Engine	[オンプレミス標準（On-Premise Standard）]（デフォルト）：コレクタのみ。	Essentials パッケージが要素管理機能なしでインストールされている場合： • **3 つのハイブリッドノード** Essentials パッケージが要素管理機能付きでインストールされている場合： • **3 つのハイブリッドノード + 1 つのワーカーノード**
	Cisco Crosswork アクティブトポロジ	[オンプレミス標準（On-Premise Standard）]（デフォルト）：コレクタのみ。	
	要素管理機能	[オンプレミス標準（On-Premise Standard）]（デフォルト）：コレクタのみ。	
Cisco Crosswork Network Controller Advantage	Cisco Crosswork Service Health	[オンプレミス拡張（On-Premise Extended）]：コレクタとオフロードサービス。	**3 つのハイブリッドノード + 2 つのワーカーノード**
アドオンパッケージ [4]	Cisco Crosswork Change Automation	[オンプレミス拡張（On-Premise Extended）]：コレクタとオフロードサービス。	**3 つのハイブリッドノード + 2 つのワーカーノード**
	Cisco Crosswork Health Insights	[オンプレミス拡張（On-Premise Extended）]：コレクタとオフロードサービス。	
	Cisco Crosswork ゼロタッチプロビジョニング	[オンプレミス標準（On-Premise Standard）]（デフォルト）：コレクタのみ。	

[1] パッケージによってライセンスの内容が異なります。ご自身のユースケースに必要なパッケージとライセンスを確認するには、シスコアカウントチームにご相談ください。

[2] Crosswork Data Gateway の VM リソース要件はタイプごとに異なり、変更することはできません。したがって、要件が変わった場合は、Crosswork Data Gateway を再展開して、あるタイプから別のタイプに移動する必要があります。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Redeploy a Crosswork Data Gateway VM*」のトピックを参照してください。

[3] 記載されている VM の数は推奨数です。必要に応じて、さらにワーカーノード（最大 2 つのワーカーノード）を追加できます。要件が推奨数を超える場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

[4] クラスタリソースの見積もりは、Crosswork Network Controller パッケージでアドオンアプリケーションを使用することを前提とします。

クラスタに十分なワーカーノードがあることを確認します。いつでもクラスタの負荷を確認し、インストール後に新しいワーカーノードを追加することを選択できます。詳細については、『*Crosswork Network Controller 5.0 Administration Guide*』の「*Deploy New Cluster Nodes*」を参照してください。

リソースのフットプリントの特定

必要な Crosswork アプリケーションと、それらをホストするために展開する必要がある VM の数を決定したら、それらに必要なリソースがあることを確認します。CPU、メモリ、ストレージなど、VM ごとに必要なリソースは、VM がホストされるデータセンター（VMware または AWS）によって異なります。

このトピックの表では、Crosswork のハイブリッドノードまたはワーカーノード、Crosswork Data Gateway、NSO、および SR-PCE を展開するための VM ごとのリソース要件について説明しています（お使いのプラットフォームに関連する表を参照してください）。

（注）

- NSO にリストされているリソースは、Crosswork Network Controller が NSO に追加する要件があるため、他の NSO のユースケースよりも多くなっています。
- NSO フットプリントは、展開のタイプ（スタンドアロンまたは LSA）によって異なります。
- SR-PCE の数は、管理する必要があるヘッドエンドの数によって異なります。
- VM のタイプと各タイプの VM の数は、ユースケースとスケールに基づいて決定する必要があります。サポートが必要な場合は、シスコアカウントチームおよびシスコ カスタマー エクスペリエンス チームにご相談ください。
- [ストレージ（Storage）] 列の値は、Crosswork ファイルの保存に必要なスペースであり、必要になる可能性のある追加のオーバーヘッド（RAID 構成など）は考慮していません。
- 各バックアップに必要なストレージは、クラスタサイズ、クラスタ内のアプリケーション、およびスケールの要件によって異なります。
- クラスタのアップグレードには、クラスタによって使用される総ディスク容量の 2 倍の容量が一時的に必要になります。
- 必要なデータゲートウェイの数は、ネットワーク内にあるデバイスの数と、必要な冗長性のレベル（1：n から 1：1）によって異なります。必要な Crosswork Data Gateway の数を決定するには、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

VMware の Crosswork リソースフットプリント

（注）

- Crosswork インストーラツールをロードするための docker 対応ホストがあることを確認します。

表 *3 : VMware の Crosswork* リソースフットプリント

コンポーネント	vCPU	メモリ（RAM）	ネットワーク インターフェイスコントローラ（NIC）	ストレージ（ブートディスク + データディスク）
Crosswork のハイブリッドノードまたはワーカーノード	12 最小クロック予約：18 GHz	96 GB	10 Gbps	1 TB
CDG オンプレミス標準	12	48 GB	10 Gbps	70 GB（50 GB + 20 GB）

コンポーネント	vCPU	メモリ（RAM）	ネットワーク インターフェイスコントローラ（NIC）	ストレージ（ブートディスク + データディスク）
CDG オンプレミス拡張	20	112 GB	10 Gbps	570 GB（50 GB + 520 GB）
Cisco NSO	16	128 GB	10 Gbps	1 TB
Cisco SR-PCE	8	24 GB	10 Gbps	70 GB
基本 SCP サーバー（バックアップの保存用）	-	-	-	25 GB 以上（推奨）

AWS EC2 の Crosswork リソースフットプリント

（注） AWS EC2 の場合、追加のストレージサーバーは AWS クラウドまたはローカル環境にある可能性があります（AWS クラウドから到達可能である必要があります）。

表 *4 : AWS EC2* の *Crosswork* リソースフットプリント

コンポーネント	vCPU	メモリ（RAM）	ネットワーク インターフェイスコントローラ（NIC）	ストレージ（ブートディスク + データディスク）
Crosswork のハイブリッドノードまたはワーカーノード	12 最小クロック予約：18 GHz	96 GB	10 Gbps	1 TB
CDG オンプレミス標準	12	64 GB	10 Gbps	70 GB（50 GB + 20 GB）
CDG オンプレミス拡張	24	128 GB	10 Gbps	570 GB（50 GB + 520 GB）
Cisco NSO	16	128 GB	10 Gbps	1 TB
Cisco SR-PCE	8	24 GB	10 Gbps	70 GB
基本 SCP サーバー（バックアップの保存用）	-	-	-	25 GB 以上（推奨）

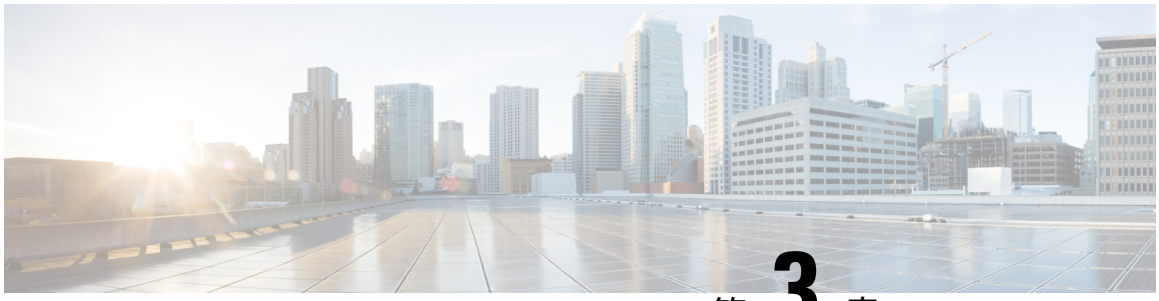
追加のリソース要件

- ストレージ要件は、サポートされているデバイスの数や選択した展開タイプなどの要因によって異なります。ただし、ほとんどの展開では 1 TB のディスク容量で十分です。
- パフォーマンスにより、従来のハードディスクドライブ（HDD）よりも、ソリッドステートドライブ（SSD）が優先されます。
- HDD を使用している場合、最低速度は 15,000 RPM 以上です。
- VM データストアのディスクアクセス遅延は 10 ミリ秒未満 または 5,000 IOPS より大きい必要があります。

特記事項

上記の手順に加えて、インストールを開始する前に考慮する必要のある特定のセットアップオプションがある場合があります。

- **自己署名証明書を使用しますか。**使用する場合、証明書を使用可能にする必要があります。サポートされている証明書のタイプとその管理方法の詳細については、『*Crosswork Network Controller 5.0 Administration Guide*』の「*Manage Certificates*」のセクションを参照してください。
- **Crosswork を外部認証サーバーと統合する予定はありますか。**TACACS+ または他の外部認証サーバーとの統合では、Crosswork ユーザーアカウントおよびロール用に作成された資格情報が必要になります。
- **オプションの管理ネットワーク プロキシ サーバーの URL を使用しますか。**パブリックインターネット上の URL にアクセスするために HTTP または HTTPS プロキシが必要な環境の場合は、Crosswork Data Gateway が Cisco Crosswork に接続できるようにプロキシサーバーを設定する必要があります。
- **Crosswork Data Gateway で、syslog サーバーを設定して syslog を収集しますか。**収集する場合は、外部 syslog サーバーのホスト名または IPv4 または IPv6 アドレスを提供します。
- **Crosswork Data Gateway で、Auditd Server を設定してイベントログを収集しますか。**収集する場合は、外部監査サーバーのホスト名または IPv4 または IPv6 アドレスを提供します。
- **リンクされたプレイブックの自動実行を有効にする予定はありますか。**予定している場合は、プレイブック ジョブ スケジュールを有効にし、[ネットワークの自動化（Network Automation）] 設定ウィンドウでプレイブックを実行するためのクレデンシャルプロンプトを無効にする必要があります。詳細については、『*Crosswork Change Automation and Health Insights 5.0 User Guide*』の「*Enable Automatic Playbook Execution*」のトピックを参照してください。



第 3 章

インストールワークフローの選択

この章は次のトピックで構成されています。

概要

この章では、サポートされている各環境（VMwareおよびAWS）のインストールワークフローについて説明します。

このワークフローでは、Crosswork Network Controller をインストールし、ソリューションの必要なコンポーネントと統合するために必要なタスクの概要が示されています。オプションのコンポーネントとの統合については、『*Crosswork Network Controller 5.0 Administration Guide*』を参照してください。

これらのワークフローのステップを、Crosswork Network Controller のエンドツーエンドのインストールのための、主要なインストールのガイドポストやロードマップとして使用する必要があります。それぞれの詳細なステップを完了したら、次のステップを実行するためにワークフローチャートを再度参照することをお勧めします。

（注） インストール全体の所要時間は、展開プロファイルのサイズとハードウェアのパフォーマンス特性によって異なることがあります。

VMware vCenter への Cisco Crosswork Network Controller のインストール

始める前に

- 必要な Crosswork のコンポーネントを特定し、インストールを完了するために必要なリソースを手配したことを確認してください。まだの場合は導入の計画 （7 ページ）のガイドラインを参照してください。
- Crosswork Network Controller と互換性のある NSO および SR-PCE のバージョンについては、『*Crosswork Network Controller 5.0 Release Notes*』を参照してください。

次の表では、Crosswork Network Controller を VMware vCenter にインストールするステージについて説明します。

表 *5 : Crosswork* のインストールワークフロー

手順	操作
インストールの準備	
1. ご使用の VMware 環境がすべての要件を満たしていることを確認します。	VMware vCenter のインストールの前提条件 （21 ページ）のガイドラインを参照してください。
Crosswork クラスタのインストール	
2. VMware vCenter へ Cisco Crosswork クラスタをインストールします。	以下の中からお好みの方法でインストールします。 • クラスタインストーラツールの使用： クラスタインストーラツールを使用した VMware vCenter への Cisco Crosswork のインストール （51 ページ） • 手動インストール：vCenter vSphere UI を使用した Cisco Crosswork の手動インストール （62 ページ）
3. インストールが成功したかどうかを確認し、Cisco Crosswork UI にログインします。	次のガイドラインを参照してください。 • インストールのモニター （73 ページ） • Cisco Crosswork UI へのログイン （76 ページ）
Crosswork Data Gateway のインストール	

手順	操作
4. VMware vCenter に 1 つ以上の Crosswork Data Gateway インスタンスをインストールします。	Cisco Crosswork Data Gateway VM（標準または拡張）のプロファイルを選択し、以下の中からお好みの方法でインストールします。 • *vSphere* の使用：vCenter vSphere クライアントを使用した Cisco Crosswork Data Gateway のインストール（100 ページ） • *OVF* ツールの使用：OVF ツールを使用した Cisco Crosswork Data Gateway のインストール（115 ページ） （注） 負荷や拡張の要件のために複数の Cisco Crosswork Data Gateway をインストールする場合や Cisco Data Gateway の高可用性を活用する場合は、すべての Cisco Crosswork Data Gateway VM をインストールしてから、それらを Data Gateway プールに追加することを推奨します。
5. Crosswork Data Gateway インストール後のタスクを実行します。	Crosswork Data Gateway インストール後のタスク（123 ページ） の手順を実行します。
6.Cisco Crosswork に Crosswork Data Gateway VM が正常に登録されたことを確認します。	Cisco Crosswork Data Gateway の認証と登録（122 ページ） の手順を実行します。 Crosswork Data Gateway VM が Cisco Crosswork に正常に登録されたことを確認したら、Cisco Crosswork Data Gateway プールを作成することで、Cisco Crosswork Data Gateway を収集用にセットアップします。『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Create a Crosswork Data Gateway Pool」のセクションを参照してください。
Cisco Crosswork アプリケーションのインストール	
7. Crosswork アプリケーションのインストール	その場合は、Crosswork アプリケーションのインストール（193 ページ）の手順に従ってください。
NSO と Crosswork の統合	
8. Cisco NSO をすでにインストールしましたか。	インストールしている場合は、ステップ 9 に進みます。 インストールしていない場合は、『NSO Installation Guide』のインストール手順に従ってください。

手順	操作
9. NSO 機能パックをインストールします。	その場合は、Ansible プレイブックを使用した Cisco NSO 機能パックのインストール（203 ページ）の手順に従ってください。
10. NSO プロバイダーを追加し、到達可能であることを確認します。	その場合は、Cisco NSO プロバイダの追加（211 ページ）の手順に従ってください。
SR-PCE と Crosswork の統合	
11. SR-PCE はインストールされていますか。	インストールされている場合は、ステップ 12 に進んでください。 インストールされていない場合は、使用する SR-PCE のタイプ（物理デバイスまたは仮想デバイス）を選択し、適切な指示に従ってデバイス（または仮想デバイス）を展開してください。詳細については、『Cisco IOS XRv 9000 Router Installation Guide』を参照してください。
12. SR-PCE の設定	その場合は、SR-PCE の設定（217 ページ）の手順に従ってください。
13. SR-PCE プロバイダーを追加し、到達可能であることを確認します。	その場合は、Cisco SR-PCE プロバイダの追加（220 ページ）の手順に従ってください。
14. （推奨）Crosswork Network Controller のバックアップを作成します。	『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Manage Backups*」の章の指示に従ってください。.

AWS EC2 への Cisco Crosswork Network Controller のインストール

始める前に

- 必要な Crosswork のコンポーネントを特定し、インストールを完了するために必要なリソースを手配したことを確認してください。まだの場合は導入の計画（7 ページ）のガイドラインを参照してください。
- Crosswork Network Controller と互換性のある NSO および SR-PCE のバージョンについては、『*Crosswork Network Controller 5.0 Release Notes*』を参照してください。

Crosswork Network Controller は**モジュールの展開**をサポートしており、展開したい Cisco Crosswork ソリューションのコンポーネント（Crosswork クラスタに必要なハイブリッドノードおよびワーカーノード、1 つ以上の Crosswork Data Gateway、および NSO）を選択してインストールできます。

次の表では、CloudFormation（CF）テンプレートを使用して AWS EC2 に Crosswork Network Controller をインストールするステージについて説明します。

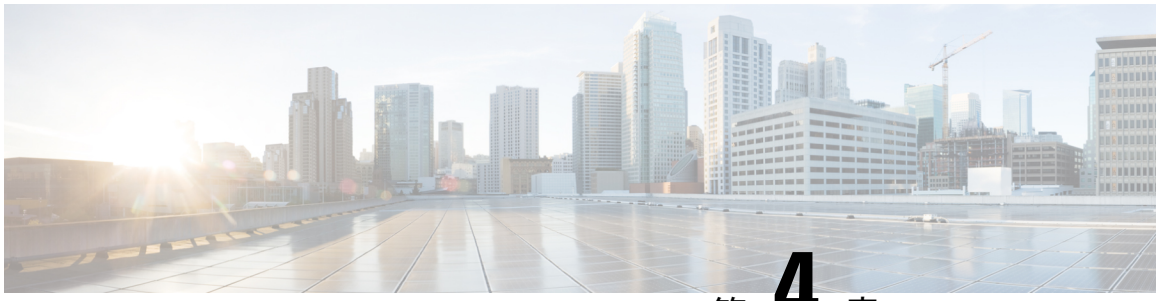
表 *6 : Crosswork* のインストールワークフロー

手順	操作
インストールの準備	
1. ご使用の AWS EC2 環境がすべての要件を満たしていることを確認します。	AWS EC2 のインストールの前提条件 （133 ページ）のガイドラインを参照してください。
2. CF テンプレートパッケージの抽出	その場合は、CF テンプレート画像の抽出 （152 ページ）の手順に従ってください。
Crosswork コンポーネントのインストール	
3.**モジュールの展開**：モジュールの展開を使用して Cisco Crosswork コンポーネントをインストールします。	以下の Crosswork コンポーネントを個別にインストールします。 • Crosswork クラスタのインストール：Amazon EC2 への Cisco Crosswork クラスタのインストール （169 ページ） • 1 つ以上の Crosswork Data Gateway のインストール：Amazon EC2 への Crosswork Data Gateway のインストール （171 ページ） Crosswork Data Gateway は、展開中に値を構成しなかった場合、デフォルトのパラメータ値で展開されます。詳細については、Crosswork Data Gateway を展開するための自動構成 （172 ページ）を参照してください。 • Cisco NSO のインストール：Amazon EC2 への Cisco NSO のインストール （176 ページ）
4. インストールの確認と Crosswork UI へのアクセス	Crosswork UI へのアクセス （180 ページ）のガイドラインを参照してください。
Crosswork アプリケーションのインストール	
5. Crosswork アプリケーションのインストール	その場合は、Crosswork アプリケーションのインストール （193 ページ）の手順に従ってください。
NSO と Crosswork の統合	

手順	操作
6. NSO 機能パックのインストール	その場合は、Ansible プレイブックを使用した Cisco NSO 機能パックのインストール（203 ページ）の手順に従ってください。
7. NSO プロバイダーを追加し、到達可能であることを確認します。	その場合は、Cisco NSO プロバイダの追加（211 ページ）の手順に従ってください。
SR-PCE と Crosswork の統合	
8. SR-PCE はインストールされていますか。	インストールされている場合は、ステップ 9 に進んでください。 インストールされていない場合は、SR-PCE タイプ（AWS の場合）を選択し、『Cisco IOS XRv 9000 Router Installation Guide』の関連するインストール手順に従ってください。
9. SR-PCE の設定	その場合は、SR-PCE の設定（217 ページ）の手順に従ってください。
10. SR-PCE プロバイダーを追加し、SR-PCE が到達可能であることを確認します。	その場合は、Cisco SR-PCE プロバイダの追加（220 ページ）の手順に従ってください。
11.（推奨）Crosswork Network Controller のバックアップを作成します。	『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Manage Backups*」の章の指示に従ってください。

第 II 部

VMware vCenter への Cisco Crosswork Network Controller のインストール



第 4 章

VMware vCenter のインストールの前提条件

この章は次のトピックで構成されています。

概要

この章では、各 Crosswork コンポーネントをインストールするための一般的な前提条件（VM 要件、ポート要件、アプリケーション要件など）およびプラットフォーム固有の前提条件について説明します。

他の統合コンポーネントまたはアプリケーション（WAE、DHCP、TFTP サーバーなど）の運用に必要なデータセンターリソースについては、このドキュメントでは取り上げていません。詳細については、各コンポーネントのインストールマニュアルを参照してください。

サポート対象のネットワークトポロジモデル

このセクションでは、VMware を使用してデータセンターに Cisco Crosswork およびその他のソリューションのコンポーネントを展開するときにサポートされるさまざまなトポロジモデルを紹介します。

ルーテッドネットワークとデバイスネットワーク

次の表では、Crosswork Network Controller から送信されるトラフィックのタイプについて説明します。このトラフィックは、単一の NIC（通常はラボでのインストール）またはデュアル NIC を使用できます。

表 *7: Crosswork* のネットワークトラフィックのタイプ

トラフィック	説明
管理	UI と Crosswork Network Controller のコマンドラインにアクセスし、サーバー間（Cisco Crosswork から Crosswork Data Gateway または NSO へなど）で情報を渡します。
データ	Cisco Crosswork と Crosswork Data Gateway、およびその他のデータの接続先（外部 Kafka/gRPC）間でのデータおよび構成の転送。
デバイスアクセス	サーバー（Crosswork、NSO、Crosswork Data Gateway など）がネットワーク内の管理対象デバイスと通信するために使用するデバイスアクセス。

さまざまなコンポーネント間の接続は、外部ルーティングエンティティを介して行う必要があります。このセクションにあるネットワークトポロジの図は、ルーテッドネットワーク内で可能なルーティングドメインを示すさまざまな線のスタイルを示しています。

- 実線：管理ルーティングドメイン。
- 点線：データ/制御ルーティングドメイン（Cisco Crosswork および Cisco Crosswork Data Gateway とその他のデータ接続先（外部の Kafka または gRPC）間での転送される情報）。
- 破線：デバイス アクセス ルーティング ドメイン（Cisco Crosswork Data Gateway と NSO から）。
- 青の破線：代替 SR-PCE 設定パス

これらの各ドメインの IP/サブネットアドレッシング方式は、展開のタイプによって異なります。

Crosswork と NSO がデバイスに到達するには、ドメイン間のルーティングが必要です。ただし、選択した送信元（Crosswork や NSO など）のみがデバイスに到達できるように適切なファイアウォールルールを設定する必要があります。

重要

- Crosswork Network Controller とネットワークデバイスの間に安全なファイアウォールを設置することが不可欠です。ただし、ファイアウォールは Crosswork Network Controller によって提供されないため、ユーザーが個別に設定する必要があります。このトピックでは、ユーザーが提供するファイアウォールシステムを通過することを許可する必要があるアプリケーションフローについて説明します。
- デバイスネットワークでは、各展開のローカル セキュリティ ポリシーに応じて、インバウンドで、またはアウトオブバンド管理インターフェイスを使用してデバイスに到達できます。

サポートされている 3 つの構成は次のとおりです。

- **1 NIC ネットワークトポロジ**Crosswork クラスタ、Crosswork Data Gateway、NSO、および SR-PCE は、1 つのネットワーク インターフェイスを使用して相互に通信し、ルーテッド インターフェイスを使用してネットワークデバイスと通信します。
- **2 NIC ネットワークトポロジ**：Crosswork クラスタ、Crosswork Data Gateway、NSO、および SR-PCE は、1 つのネットワーク インターフェイスを使用して管理インターフェイス間で通信し、2 番目のインターフェイスを使用して Crosswork Network Controller と Crosswork Data Gateway の間でデータを渡し、ルーテッドインターフェイスを使用してネットワークデバイスと通信します。
- **3 NIC ネットワークトポロジ**：Crosswork クラスタ、Crosswork Data Gateway、NSO、および SR-PCE は、1 つのネットワーク インターフェイスを使用して管理インターフェイス間で通信し、2 番目のインターフェイスを使用して Crosswork Network Controller と Crosswork Data Gateway の間でデータを渡し、Crosswork Data Gateway の 3 番目のインターフェイスを使用してネットワークデバイスと通信します。NSO は、ネットワークデバイスと通信するために、3 番目のインターフェイスまたはルーテッドインターフェイスのいずれかを使用できます。

図 *1 : Cisco Crosswork* : *1 NIC* ネットワークトポロジ

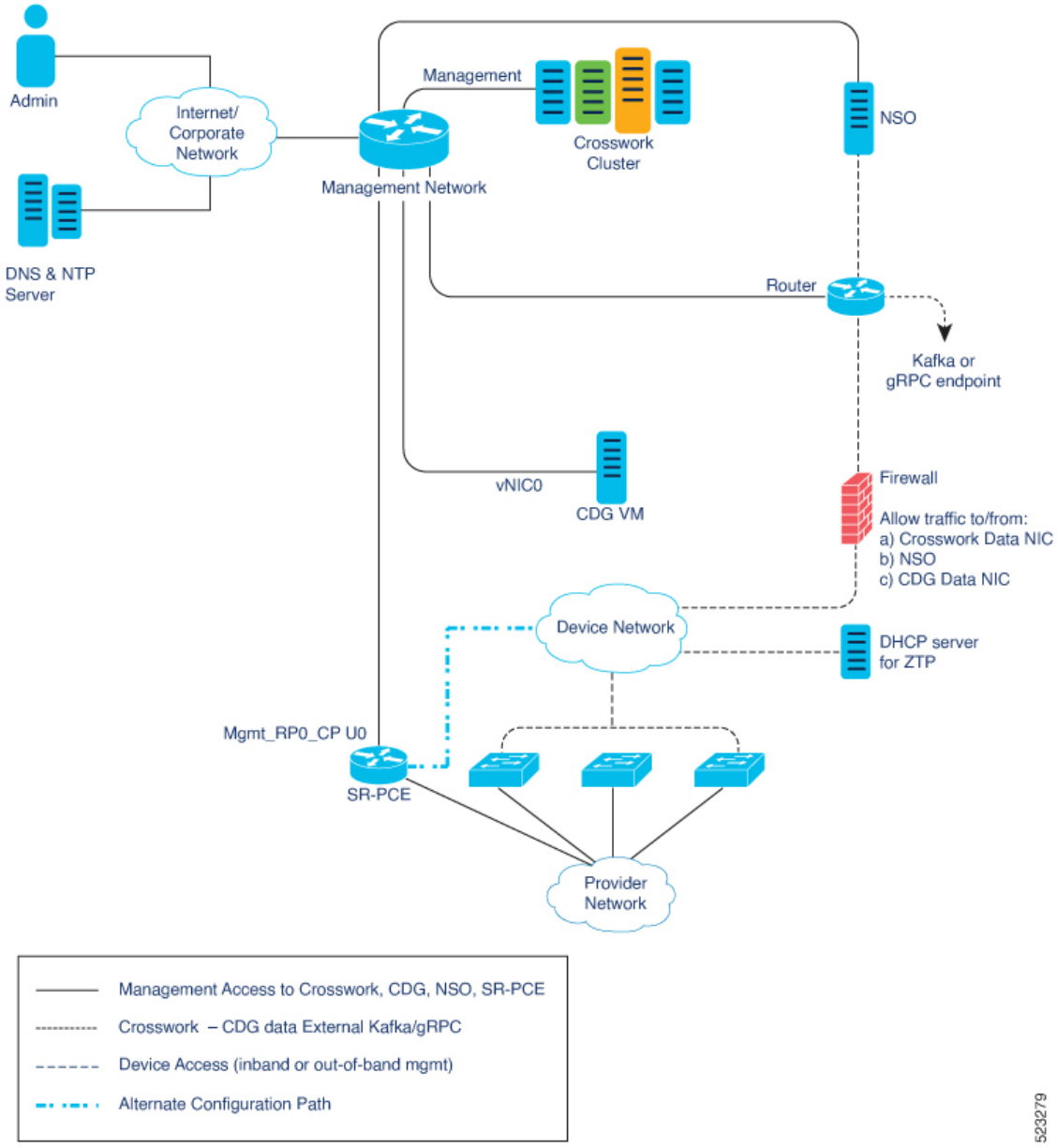


図 *2 : Cisco Crosswork* : *2 NIC* ネットワークトポロジ

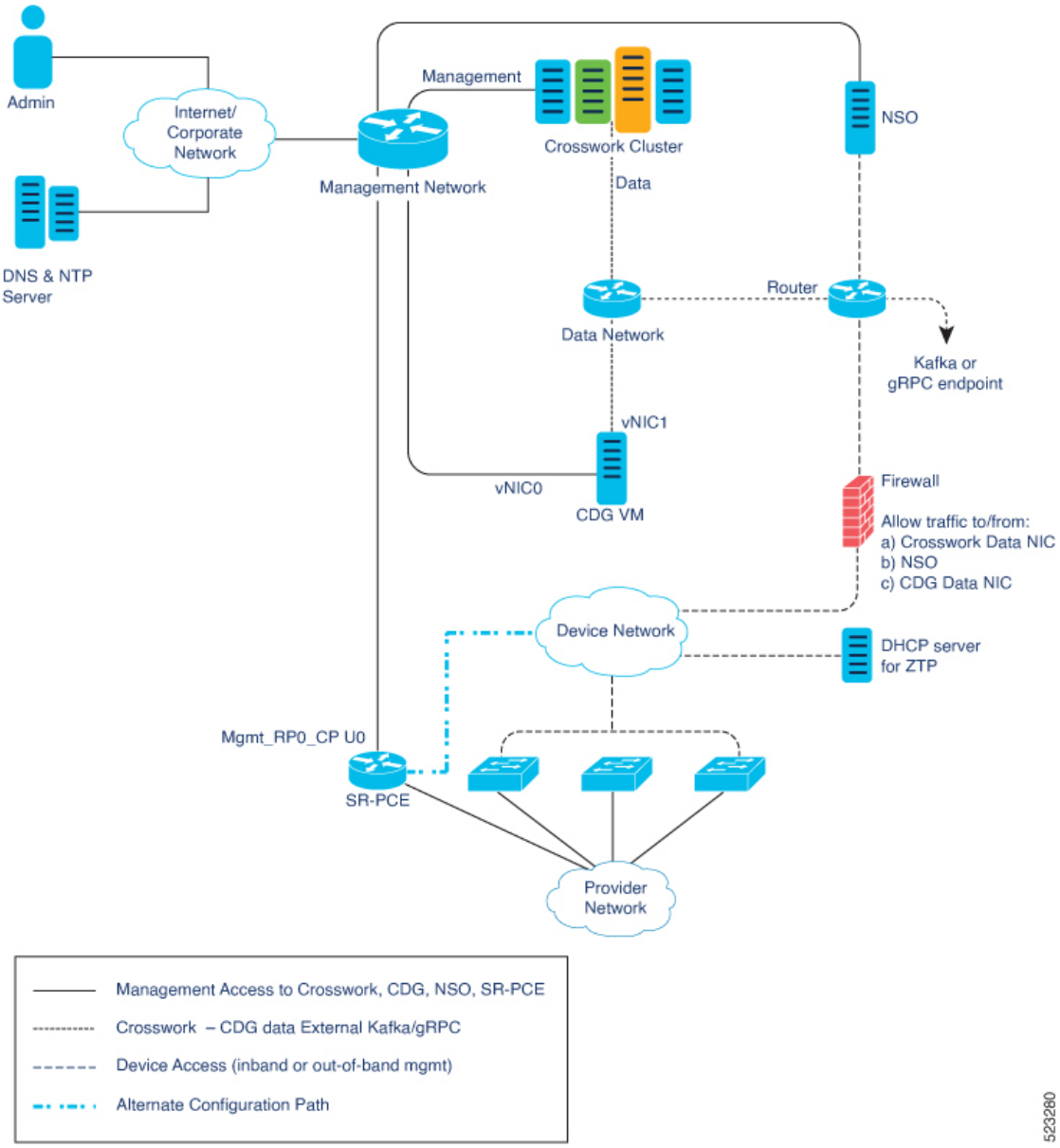
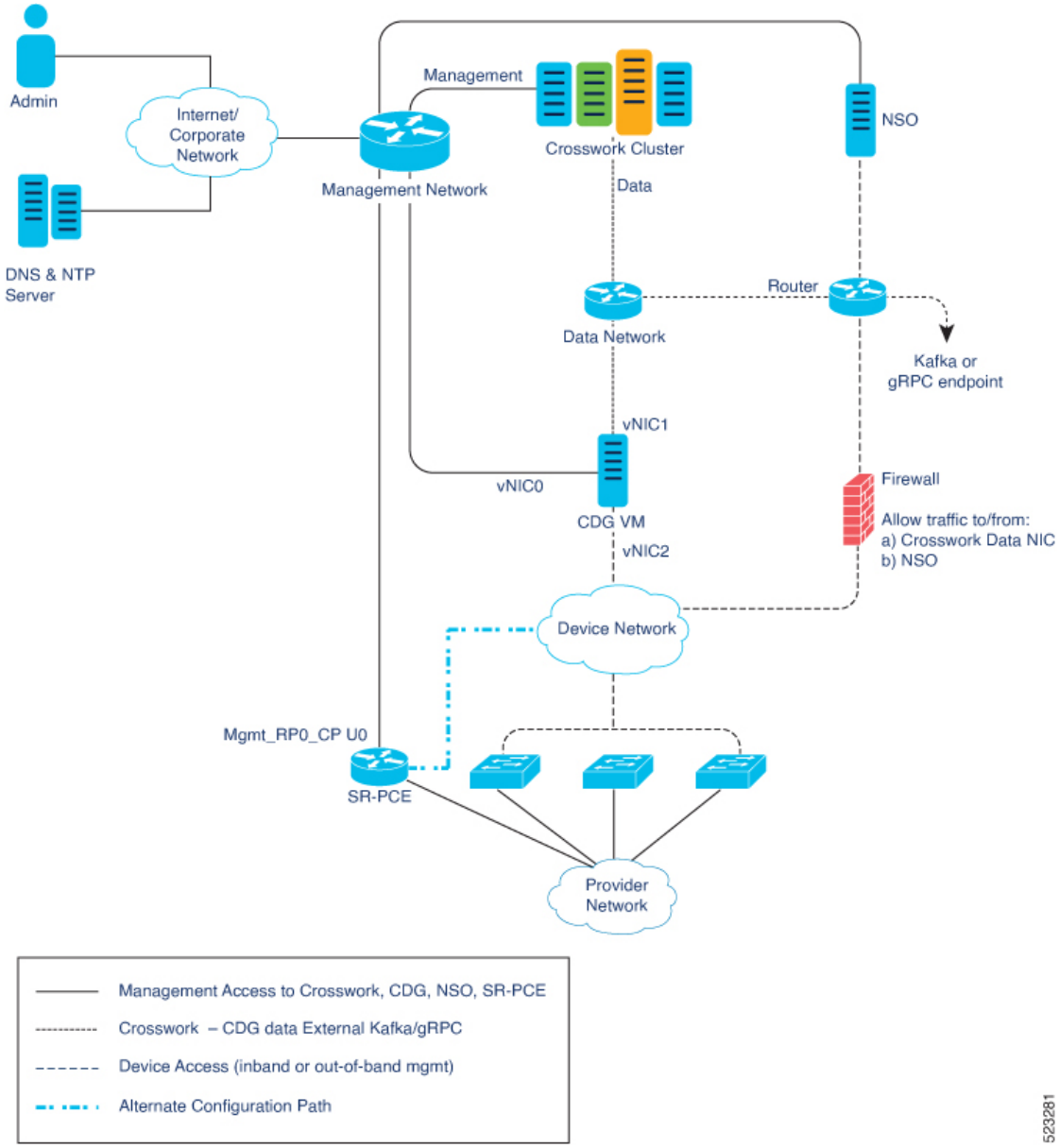


図 *3 : Cisco Crosswork* : *3 NIC* ネットワークトポロジ



Cisco Crosswork 仮想マシン（VM）

Cisco Crosswork VM には、次の vNIC 展開オプションがあります。

表 *8 : Cisco Crosswork vNIC* 展開モード

vNIC の数	vNIC	説明
1	管理	単一の NIC を通過する管理、データ、およびデバイスアクセス

vNIC の数	vNIC	説明
2	管理	管理
	データ	データおよびデバイスアクセス

Cisco Crosswork Data Gateway VM

Cisco Crosswork Data Gateway VM には、次の vNIC 展開オプションがあります。

（注） Crosswork クラスタで 1 つのインターフェイスを使用する場合は、Crosswork Data Gateway で 1 つのインターフェイスのみを使用する必要があります。Crosswork クラスタで 2 つのインターフェイスを使用する場合は、ネットワークの要件に応じて、Crosswork Data Gateway で 2 つまたは 3 つのインターフェイスを使用できます。

vNIC の数の設定は、展開環境によって異なることがあります。vNIC の数は、展開のセキュリティおよびトラフィック分離のニーズに応じて異なることがあります。Crosswork Data Gateway と Crosswork は、可変数の vNIC を導入することでこの変動に対応します。

表 *9 : Cisco Crosswork Data Gateway* のデフォルトの *vNIC* 展開モード

vNIC の数	vNIC	トラフィックのタイプ
1	vNIC0	単一の NIC を通過するデフォルトゲートウェイ、管理、外部ロギング、および管理トラフィック。
2	vNIC0	デフォルトゲートウェイ、管理、外部ロギング、および管理トラフィック。
	vNIC1	制御およびノースバウンド外部データトラフィック。
3	vNIC0	デフォルトゲートウェイ、管理、外部ロギング、および管理トラフィック。
	vNIC1	制御およびノースバウンド外部データトラフィック。
	vNIC2	サウスバウンド データトラフィック

SR-PCE の設定

セグメントルーティングパス計算要素（SR-PCE）は、デバイスと Software Defined Networking（SDN）コントローラの両方です。一部の展開では、SR-PCE インスタンスをデバイスとして扱う必要があります。その場合は、デバイスネットワーク経由でアクセスする必要があります。一部の展開では、SR-PCE インスタンスを SDN コントローラとして扱い、管理ルーティングドメインでアクセスする場合があります。Crosswork は両方のモデルをサポートしています。デフォルトでは、Crosswork は **eth0**（管理）を使用して、管理ドメイン上の SDN コントローラとして SR-PCE にアクセスします（図を参照）。デバイスネットワーク上のデバイスとして

SR-PCE インスタンスへの Crosswork アクセスを有効にする方法の詳細については、Cisco SR-PCE プロバイダの追加 （220 ページ）を参照してください。

ZTP の要件

ゼロタッチプロビジョニングを使用する場合は、デバイスネットワークに DHCP サーバーが装備されている必要があります（Cisco Crosswork の一部としては提供されません）。ZTP の一部の形式では、TFTP サーバーも必要です（Cisco Crosswork の一部としては提供されません）。さらに ZTP を使用するすべてのデバイスは、Crosswork クラスタからファイル（ソフトウェアや構成）を直接プルするため、Crosswork クラスタへのネットワーク接続も必要とします。ゼロタッチプロビジョニングの概念と機能の詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Zero Touch Provisioning*」の章を参照してください。

Cisco Network Services Orchestrator（NSO）VM

NSO VM には次の vNIC を備えています。

- 管理：NSO に到達するための Crosswork アプリケーションに使用します。
- デバイスアクセス：NSO がデバイスまたは NSO リソース側サービス（RFS）に到達するために使用します。

VMware 設定

クラスタインストーラを使用して Cisco Crosswork をインストールする場合は、次の要件が必須です。vCenter データセンターがこれらの要件を満たしていない場合は、VM を個別に展開する必要があり、VM 間で接続を手動で確立する必要があります。手動インストールの詳細については、vCenter vSphere UI を使用した Cisco Crosswork の手動インストール （62 ページ）を参照してください。

- ハイパーバイザと vCenter のサポート対象：
  - VMware vCenter Server 7.0 および ESXi 7.0
  - VMware vCenter Server 6.7（Update 3g 以降）および ESXi 6.7 (Update 1)
- クラスタインストーラツールを使用する場合、インストーラを実行するマシンは、クラスタをインストールする予定の vCenter データセンターにネットワーク接続できる必要があります。この必須要件を満たすことができない場合は、手動でクラスタをインストールする必要があります。手動インストールの詳細については、vCenter vSphere UI を使用した Cisco Crosswork の手動インストール （62 ページ）を参照してください。
- Cisco Crosswork クラスタ VM（ハイブリッドノードとワーカーノード）は、ハイパースレッディングが無効になっているハードウェアでホストする必要があります。
- Cisco Crosswork クラスタノードは VM に高い要求を課すため、ノードをホストするマシンの CPU またはメモリリソースがオーバーサブスクライブされていないことを確認してください。

- すべての物理ホストマシンは同じVMwareデータセンター内で編成する必要があります。また、すべてのクラスタノードを単一の物理ホストに展開することは可能ですが（要件を満たしている場合）、ノードは複数の物理ホストに分散することを推奨します。これにより、ホストがシングルポイント障害になることがなくなり、ソリューションの復元力が向上します。
- Crosswork の管理およびデータネットワークに必要なネットワークをデータセンターで構築および設定し、低遅延 L2 通信を許可する必要があります。

（注） Crosswork VM をホストしているすべての ESXi ホストマシンで同じネットワーク名を使用して構成する必要があります。

- VRRP の使用を許可するには、DVS ポートグループを次のように設定する必要があります。

プロパティ	値
無差別モード（Promiscuous mode）	拒否（Reject）
MAC アドレスの変更（MAC address changes）	拒否（Reject）

vCenter で設定を編集するには、**[Host]** > **[Configure]** > **[Networking]** > **[Virtual Switches]** に移動し、仮想スイッチを選択します。仮想スイッチで **[Edit]** > **[Security]** を選択し、提示された設定を確認します。クラスタで使用される仮想スイッチごとにこのプロセスを繰り返します。

- vCenterへのアクセスに使用するユーザーアカウントに次の権限があることを確認します。
  - VM（プロビジョニング）：複製する VM で VM を複製します。
  - VM（プロビジョニング）：ゲストオペレーティングシステムをカスタマイズする場合は、VM または VM フォルダをカスタマイズします。
  - VM（インベントリ）：データセンターまたは VM フォルダの既存の VM から作成します。
  - VM（設定）：データセンターまたは VM フォルダに新しいディスクを追加します。
  - リソース：接続先ホスト、クラスタ、またはリソースプールのリソースプールに VM を割り当てます。
  - データストア：接続先データストアまたはデータストアフォルダに領域を割り当てます。
  - ネットワーク：VM を割り当てるネットワークを割り当てます。
  - プロファイル駆動型ストレージ（クエリ）：この権限設定は、データセンターツリーレベルのルートで許可する必要があります。

- また、vCenter ストレージ制御を有効にすることを推奨します。

ホスト VM の要件

このセクションでは、Crosswork クラスタと Crosswork Data Gateway を展開するための VM ごとのリソース要件について説明します。

- Crosswork クラスタ VM の要件 （30 ページ）
- Crosswork Data Gateway VM の要件 （32 ページ）

Crosswork クラスタ VM の要件

Crosswork クラスタは、ハイブリッド構成で動作する 3 つの VM またはノードで構成されます。これは、標準的なネットワークでアプリケーションをサポートするために必要な最小限の設定です。必要に応じて、ネットワークの要件に合わせて、または他のアプリケーションの導入に合わせて、後でワーカー構成に VM やノード（最大 2 つのワーカーノード）を追加して展開を拡張できます（各 Crosswork Network Controller パッケージの VM 数についての詳細は 表 2 : Crosswork Network Controller パッケージ （8 ページ） を参照）。お客様のニーズに最適な展開に関するガイダンスについては、シスコのカスタマー エクスペリエンス チームにお問い合わせください。

次の表は、VM ホストごとのネットワーク要件を説明しています。

表 *10* : ネットワーク要件（*VM* ごと）

要件	説明
ネットワーク接続	実稼働環境への展開では、管理ネットワーク用とデータネットワーク用のデュアルインターフェイスを使用することを推奨します。 最適なパフォーマンスを得るには、管理ネットワークとデータネットワークでは 10 Gbps 以上で設定されたリンクを使用する必要があります。

要件	説明
IP アドレス	**デュアル NIC を使用する場合**（1 つは管理ネットワーク用、もう 1 つはデータネットワーク用）：展開される各ノード（ハイブリッドまたはワーカー）の管理およびデータ IP アドレス（IPv4 または IPv6）と、仮想 IP（VIP）アドレスとして使用される 2 つの追加 IP アドレス（1 つは管理ネットワーク用、もう 1 つはデータネットワーク用）。 **シングル NIC を使用する場合**：展開されるノード（ハイブリッドまたはワーカー）ごとに 1 つの IP アドレス（IPv4 または IPv6）と、仮想 IP（VIP）アドレスとして使用される 1 つの追加の IP アドレス。 たとえば、3 つのハイブリッド VM を備えたクラスタと単一の NIC を備えた 1 つのワーカー VM の場合は 5 つの IP アドレスが必要であり、同じ構成でデュアル NIC を備えている場合は 10 の IP アドレス（管理ネットワーク用に 5 つ、データネットワーク用に 5 つ）が必要です。 （注） • IP アドレスは、Cisco Crosswork Data Gateway がインストールされるネットワークのゲートウェイアドレスに到達できる必要があります。そうでない場合、インストールは失敗します。 • IPv6 クラスタを展開する場合、IPv6 対応のコンテナ/VM でインストーラを実行する必要があります。 • この時点では、IP の割り当ては永続的であり、再展開しない限り変更できません。詳細については、シスコ カスタマー エクスペリエンス チームにお問い合わせください。
NTP サーバー	使用する NTP サーバーの IPv4 または IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体で Crosswork アプリケーションの VM クロック、デバイス、クライアント、およびサーバーを同期するために使用するものと同じ NTP サーバーである必要があります。 インストールを試行する前に、NTP サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。
DNS サーバー	使用する DNS サーバーの IPv4 または IPv6 アドレス。これらは、ネットワーク全体でホスト名を解決するために使用する DNS サーバーと同じである必要があります。 インストールを試みる前に、DNS サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。

要件	説明
DNS 検索ドメイン	DNS サーバーで使用する検索ドメイン（cisco.com など）。検索ドメインは 1 つのみ設定できます。
バックアップ サーバ	Cisco Crosswork は、SCP を使用して、システムの設定を外部サーバーにバックアップします。SCP サーバーのストレージ要件は若干異なりますが、少なくとも 25 GB のストレージが必要です。

- Cisco Crosswork インフラストラクチャおよびアプリケーションは、Kubernetes によって管理されるコンテナの分散型集合体として動作するように構築されています。コンテナの数は、アプリケーションが追加または削除されると変わります。
- Crosswork プラットフォーム インフラストラクチャでは、デュアルスタック構成はサポートされていません。したがって、環境のアドレスは**すべて** IPv4 または IPv6 のいずれかである必要があります。

Crosswork Data Gateway VM の要件

ここでは、Crosswork Data Gateway をインストールするための一般的なガイドラインと最小要件について説明します。

- Crosswork Data Gateway の展開タイプの選択 （32 ページ）
- Crosswork Data Gateway VM の要件 （33 ページ）

Crosswork Data Gateway の展開タイプの選択

次の表に、各 Crosswork 製品に Crosswork Data Gateway をインストールするために使用する必要がある展開プロファイルのリストを示します。

（注） Crosswork Data Gateway の VM リソース要件はタイプごとに異なり、変更することはできません。したがって、要件が変わった場合は、Crosswork Data Gateway を再展開して、あるタイプから別のタイプに移動する必要があります。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Redeploy a Crosswork Data Gateway VM*」のトピックを参照してください。

表 *11 : Crosswork Data Gateway* の展開タイプ

Cisco Crosswork 製品	Crosswork Data Gateway の展開
Crosswork Network Controller（Crosswork Active Topology と Crosswork Optimization Engine の組み合わせ）	オンプレミス標準

Cisco Crosswork 製品	Crosswork Data Gateway の展開
Crosswork 最適化エンジン	オンプレミス標準
Crosswork ゼロタッチプロビジョニング	オンプレミス標準
Crosswork Change Automation	オンプレミス拡張
Crosswork Health Insights	オンプレミス拡張
Crosswork Service Health	オンプレミス拡張

Crosswork Data Gateway VM の要件

Crosswork Data Gateway の VM の要件を次の表に示します。

表 *12*：オンプレミス アプリケーションの *Crosswork Data Gateway* 要件

要件	説明
データセンター	VMware 「VMware vCenter のインストールの前提条件 （21 ページ）」を参照してください。

<table>
<tr><th>要件</th><th>説明</th></tr>
<tr><td>インターフェイス</td><td>最小値：1
最大値：3
Cisco Crosswork Data Gateway は、次の組み合わせに応じて、1 つ、2 つ、および 3 つのインターフェイスのいずれかで展開できます。
（注） Crosswork クラスタで 1 つのインターフェイスを使用する場合は、Crosswork Data Gateway で 1 つのインターフェイスのみを使用する必要があります。Crosswork クラスタで 2 つのインターフェイスを使用する場合は、ネットワークの要件に応じて、Crosswork Data Gateway で 2 つまたは 3 つのインターフェイスを使用できます。
<table>
<tr><th>NIC の数</th><th>vNIC0</th><th>vNIC1</th><th>vNIC2</th></tr>
<tr><td>1</td><td>• 管理トラフィック
• 制御/データトラフィック
• デバイス アクセス トラフィック</td><td>—</td><td>—</td></tr>
<tr><td>2</td><td>管理トラフィック</td><td>• 制御/データトラフィック
• デバイスアクセストラフィック</td><td>—</td></tr>
<tr><td>3</td><td>管理トラフィック</td><td>制御/データトラフィック</td><td>デバイス アクセス トラフィック</td></tr>
</table>
</td></tr>
</table>

要件	説明
	• 管理トラフィック：インタラクティブコンソールにアクセスする場合、およびサーバー間で制御/データ情報を渡す場合に使用されます（たとえば、Crosswork アプリケーションから Crosswork Data Gateway）。 • 制御/データトラフィック：Cisco Crosswork Data Gateway と Crosswork アプリケーション、および他の外部データ接続先間でデータと設定を転送します。 • デバイス アクセス トラフィック：デバイスにアクセスする場合、およびデータを収集する場合に使用されます。 （注） セキュリティポリシーにより、他の vNIC で受信された vNIC のサブネットからのトラフィックはドロップされます。たとえば、3 vNIC モデル設定では、すべてのデバイストラフィック（着信および発信）がデフォルトの vNIC2 経由でルーティングされる必要があります。Crosswork Data Gateway は、vNIC0 および vNIC1 経由で受信されたデバイストラフィックをドロップします。
IP アドレス	使用するインターフェイスの数に基づいて、1 つまたは 2 つの IPv4/IPv6 アドレス。 仮想 IP（VIP）アドレスとして使用する 1 つの追加 IP アドレス。アクティブなデータゲートウェイごとに、一意の VIP が必要です。 詳細については、表 24 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （81 ページ）の「Interfaces」のセクションを参照してください。 （注） Crosswork はデュアルスタック構成をサポートしていません。したがって、環境のすべてのアドレスは IPv4 または IPv6 である必要があります。 3-NIC 展開では、インストール時に管理インターフェイス（vNIC0）および制御/データインターフェイス（vNIC1）の IP アドレスを指定する必要があります。デバイス アクセス トラフィック（vNIC2）の仮想 IP アドレスは、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Create a Crosswork Data Gateway Pool」のセクションで説明されているように、Crosswork Data Gateway プールの作成時に割り当てられます。

要件	説明
NTP サーバー	使用する NTP サーバーの IPv4 または IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体でデバイス、クライアント、およびサーバを同期するために使用する NTP サーバと同じでなければなりません。NTP IP アドレスまたはホスト名がネットワーク上で到達可能であることを確認します。到達可能でない場合、インストールは失敗します。 また、Crosswork アプリケーションと Cisco Crosswork Data Gateway VM を実行する ESXi ホストには NTP が設定されている必要があります。そうでない場合、最初のハンドシェイクが「certificate not valid」エラーで失敗する可能性があります。
DNS サーバー	使用する DNS サーバーの IPv4 または IPv6 アドレス。これらは、ネットワーク全体でホスト名を解決するために使用する DNS サーバーと同じである必要があります。インストールを試みる前に、DNS サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。
DNS 検索ドメイン	DNS サーバーで使用する検索ドメイン（cisco.com など）。検索ドメインは 1 つのみ設定できます。

TCP および UDP ポートの要件

一般的なポリシーとして、不要なポートを無効にする必要があります。すべてのアプリケーションがインストールされアクティブになった後、開いているすべてのリスニングポートのリストを表示するには、任意の Crosswork クラスタ VM に Linux CLI の管理者ユーザーとしてログインし、**netstat -aln** コマンドを実行します。

（注） Crosswork クラスタ、Crosswork アプリケーション、および Crosswork Data Gateway 間のすべての IP アドレス（仮想 IP アドレスを含む）は、相互に到達可能（ping を実行可能）である必要があります。

Crosswork クラスタポートの要件

次の TCP および UDP のポート番号は、データセンター管理者が展開した外部ファイアウォールまたはアクセスリストのルールを通過できるようにする必要があります。NIC の展開によっては、これらのポートが一方のみの、または両方の NIC に適用される場合があります。

（注） Crosswork クラスタポートにより、双方向の情報フローが可能になります。

表 *13 : Crosswork* クラスタが使用する外部ポート

ポート	プロトコル	用途	場所（2 つの NIC 展開時）
22	TCP	リモート SSH トラフィック	管理ネットワーク / vNIC0
111	TCP/UDP	GlusterFS（ポートマッパー）	管理ネットワーク / vNIC0
179	TCP	Calico BGP（Kubernetes）	管理ネットワーク / vNIC0
80、443	TCP	EC2 API へのアクセス	管理ネットワーク / vNIC0
500	UDP	IPSec	管理ネットワーク / vNIC0
2379/2380	TCP	Kubernetes etcd	管理ネットワーク / vNIC0
4500	UDP	IPSec	管理ネットワーク / vNIC0
6443	TCP	kube-apiserver（Kubernetes）	管理ネットワーク / vNIC0
9100	TCP	Kubernetes メタモニターリング	管理ネットワーク / vNIC0
10250	TCP	kubelet（Kubernetes）	管理ネットワーク / vNIC0
24007	TCP	GlusterFS	管理ネットワーク / vNIC0
30603	TCP	ユーザーインターフェイス（NGINX サーバーはポート 443 でセキュア接続をリッスンします）	管理ネットワーク / vNIC0
30606	TCP	Docker レジストリ	管理ネットワーク / vNIC0
30621	TCP	FTP 用（データインターフェイスでのみ使用可能）。ファイル転送に使用される追加ポートは、31121（TCP）、31122（TCP）、および 31123（TCP）です。 このポートは、サポート対象アプリケーションが Cisco Crosswork にインストールされ、FTP 設定が有効になっている場合にのみ使用できます。	管理ネットワーク / vNIC0
30622	TCP	SFTP 用（データインターフェイスでのみ使用可能）。 このポートは、サポート対象アプリケーションが Cisco Crosswork にインストールされ、SFTP 設定が有効になっている場合にのみ使用できます。	管理ネットワーク / vNIC0

ポート	プロトコル	用途	場所（2 つの NIC 展開時）
49152-49370	TCP	GlusterFS	管理ネットワーク / vNIC0

表 *14* : 他の *Crosswork* コンポーネントが使用するポート

ポート	プロトコル	用途	場所（2 つの NIC 展開時）
30602	TCP	インストールのモニタリング用（Crosswork Network Controller）	管理ネットワーク / vNIC0
30603	TCP	Crosswork Network Controller Web ユーザーインターフェイス（NGINX サーバーはポート 443 でセキュア接続をリッスンします）	管理ネットワーク / vNIC0
30604	TCP	NGINX サーバーのクラシック ゼロ タッチ プロビジョニング（クラシック ZTP）に使用されます。	管理ネットワーク / vNIC0
30607	TCP	Crosswork Data Gateway のバイタルコレクション	データネットワーク / vNIC1
30608	TCP	Data Gateway VM を使用した Data Gateway gRPC チャネル	データネットワーク / vNIC1
30609	TCP	Expression Orchestrator（Crosswork Service Health）によって使用されます。	管理ネットワーク / vNIC0
30610	TCP	Metric Scheduler（Crosswork Service Health）によって使用されます。	管理ネットワーク / vNIC0
30611	TCP	Expression Tracker コンポーネント（Crosswork Service Health）によって使用されます。	管理ネットワーク / vNIC0
30617	TCP	ZTP サーバーのセキュア ゼロ タッチ プロビジョニング（セキュア ZTP）に使用されます。	管理ネットワーク / vNIC0
30620	TCP	ZTP サーバーでプラグアンドプレイ HTTP トラフィックを受信するために使用されます。	管理ネットワーク / vNIC0
30649	TCP	Crosswork Data Gateway の収集ステータスの設定および監視。	データネットワーク / vNIC1
30650	TCP	Data Gateway VM で実行されている astack-client を含む astack gRPC チャネル。	データネットワーク / vNIC1

ポート	プロトコル	用途	場所（2 つの NIC 展開時）
30993、30994、30995	TCP	収集されたデータを Crosswork Kafka の接続先に送信する Crosswork Data Gateway。	データネットワーク / vNIC1

表 *15 : Crosswork* クラスタが使用する宛先ポート

ポート	プロトコル	用途	場所（2 つの NIC 展開時）
7	TCP/UDP	ICMP を使用したエンドポイントの検出。	管理ネットワーク / vNIC0
22	TCP	管理対象デバイスとの SSH 接続の開始。	管理ネットワーク / vNIC0
53	TCP/UDP	DNS への接続	管理ネットワーク / vNIC0
123	UDP	ネットワーク タイム プロトコル（NTP）	管理ネットワーク / vNIC0
830	TCP	NETCONF の開始	管理ネットワーク / vNIC0
2022	TCP	Crosswork と Cisco NSO 間の通信に使用されます（NETCONF の場合）。	管理ネットワーク / vNIC0
8080	TCP	REST API から SR-PCE へ	管理ネットワーク / vNIC0
8888	TCP	Crosswork と Cisco NSO 間の通信に使用されます（HTTPS の場合）。	管理ネットワーク / vNIC0
20243	TCP	DLM と Cisco NSO 間の通信用に DLM 機能パックによって使用されます。	管理ネットワーク / vNIC0
20244	TCP	Cisco NSO でパッケージのリロードシナリオ中に DLM 機能パックリスナーを内部的に管理するために使用されます。	管理ネットワーク / vNIC0

Crosswork Data Gateway ポート要件

次の表に、Crosswork Data Gateway が正常に動作するために必要なポートの最小セットを示します。

インバウンド：Crosswork Data Gateway は指定されたポートでリッスンします。

アウトバウンド：Crosswork Data Gateway は、指定されたポートの外部宛先 IP に接続します。

表 *16 :* 管理トラフィック用に開くポート

ポート	プロトコル	用途	方向
22	TCP	SSH サーバ	着信

ポート	プロトコル	用途	方向
22	TCP	SCP クライアント	発信
123	UDP	NTP クライアント	発信
53	UDP	DNS Client	発信
30607	TCP	Crosswork コントローラ	発信

（注） SCP ポートは調整できます。

表 *17:* デバイス アクセス トラフィック用に開くポート

ポート	プロトコル	用途	方向
161	UDP	SNMP コレクタ	発信
1062	UDP	SNMP トラップコレクタ これはデフォルト値です。この値は、インストール後に Cisco Crosswork UI から変更できます。詳細については「Configure Crosswork Data Gateway Global Parameters」を参照してください。	着信
9010	TCP	MDT コレクタ	着信
22	TCP	CLI コレクタ	発信
6514	TLS	syslog コレクタ これはデフォルト値です。この値は、インストール後に Cisco Crosswork UI から変更できます。詳細については「Configure Crosswork Data Gateway Global Parameters」を参照してください。	着信
9898	TCP		
9514	UDP		

ポート	プロトコル	用途	方向
サイト特定 プラットフォーム固有のマニュアルを確認します。	TCP	gNMI コレクタ	発信

表 *18 :* 制御/データトラフィック用に開くポート

ポート	プロトコル	用途	方向
30649	TCP	Crosswork コントローラ	発信
30993 30994 30995	TCP	Crosswork Kafka	発信
サイト特定	サイト特定	Kafka と gRPC の接続先	発信

IP アドレスの制限

Crosswork クラスタでは、内部通信に次の IP 範囲が使用されます。これは変更できません。そのため、これらのサブネットは、ネットワーク内のデバイスやその他の目的のために使用できません。

Crosswork クラスタを分離して、すべての通信がクラスタ内にとどまるようにすることをお勧めします。また、アドレス空間が、外部統合ポイント（デバイスへの接続、Crosswork がデータを送信する先の外部サーバーへの接続、NSO サーバーへの接続など）と重複していないことも確認してください。

（注） これは、クラスタのインストールとスタティックルートの追加に適用されます。

表 *19 :* 保護された *IP* サブネット

IP タイプ	サブネット	備考
IPv4	172.17.0.0/16	Docker サブネット（インフラストラクチャ）
	169.254.0.0/16	リンク ローカル アドレス ブロック
	127.0.0.0/8	ループバックアドレス
	192.88.99.0/24	予約済み。以前はリレーサーバーが IPv6 over IPv4 を実行するために使用されました
	240.0.0.0/4	将来の使用のために予約済み（以前はクラス E ブロック）
	224.0.0.0/4	MCAST-TEST-NET
	0.0.0.0/8	現在のネットワーク、送信元アドレスとしてのみ有効
IPv6	2001:db8:1::/64	Docker サブネット（インフラストラクチャ）
	fdfb:85ef:26ff::/48	ポッドサブネット（インフラストラクチャ）
	fd08:2eef:c2ee::/110	サービスサブネット（インフラストラクチャ）
	::1/128	ループバックアドレス
	fe80::/10	リンク ローカル
	ff00::/8	IPv6 マルチキャスト
	2002::/16	予約済み。以前はリレーサーバーが IPv6 over IPv4 を実行するために使用されました
	2001:0000::/32	Terredo トンネルとリレー
	2001:20::/28	ORCHID で使用され、IPv6 ではルーティング不可です
	100::/64	破棄プレフィックス。Crosswork ゼロタッチプロビジョニングに適用されない特定のユースケースで使用されます
	::/128	未指定のアドレス。ホストに割り当てることはできません
	::ffff:0:0/96	IPv4 マッピングされたアドレス
	::ffff:0:0:0/96	IPv4 変換されたアドレス

サポートされる Web ブラウザ

インフラストラクチャのインストール後に Crosswork UI にアクセスするには、検証済みのブラウザのいずれかを使用することをお勧めします。

表 *20 :* サポートされる *Web* ブラウザ

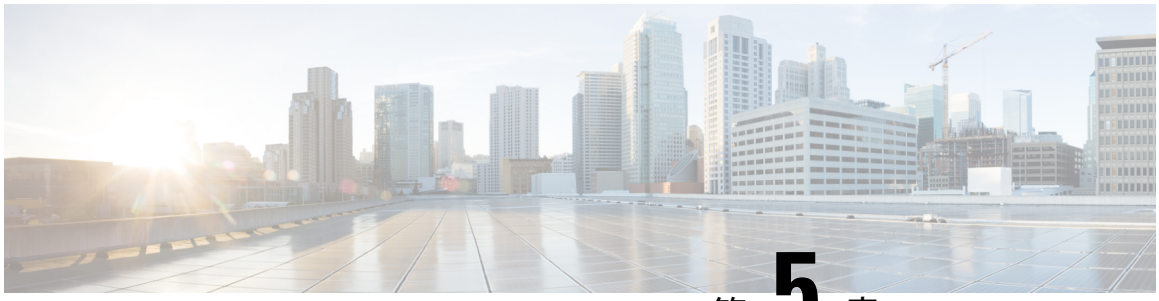
ブラウザ	バージョン
Google Chrome （推奨）	92 以降
Mozilla Firefox	70 以降

推奨される表示解像度は 1600 x 900 ピクセル以上（最小：1366 x 768）です。

サポートされているブラウザを使用することに加えて、Crosswork アプリケーション内の地理的マップにアクセスするすべてのクライアントデスクトップは、mapbox.com のサイトにアクセスできる必要があります。Cisco Crosswork が外部サイトにアクセスすることを望まないお客様は、マップファイルをローカルにインストールすることを選択できます。

次に行う作業：

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）



第 5 章

VMware vCenter への Crosswork クラスタのインストール

この章は次のトピックで構成されています。

インストールの概要

Crosswork Network Controller は、次の方法を使用してインストールできます。

- **インストーラを使用してインストール**：クラスタインストーラツールは、テンプレートファイルを介して提供されるユーザー指定のパラメータを使用して、Crosswork クラスタを展開するために使用されるデイゼロインストールツールです。このツールは、通常の PC/ラップトップを含む任意の Docker 対応プラットフォームでホストできる Docker コンテナから実行されます。Docker コンテナには、展開固有のデータを提供するために編集可能なテンプレートファイルのセットが含まれています。
- **手動インストール（VMware UI 経由）**：このオプションは、インストーラツールを使用できない展開で利用できます。

インストーラツールによる方法は、より高速で使いやすいため、推奨されるオプションです。

インストール パラメータ

このセクションでは、Crosswork クラスタのインストール時に指定する必要がある重要なパラメータについて説明します。表に記載されている各パラメータに入力する関連情報を把握していること、さらに使用中の環境が VMware vCenter のインストールの前提条件 （21 ページ） で指定されているすべての要件を満たしていることを確認してください。

（注） 以下のパラメータの一部には、インストール方法（自動または手動）および選択した IP スタック（IPv4 または IPv6）に応じて異なる名前が付けられる場合があります。

表 *21* : 一般パラメータ

パラメータ名	説明
ClusterName	クラスタファイルの名前。
ClusterIPStack	IP スタックプロトコル：IPv4 または IPv6
ManagementIPAddress	VM の管理 IP アドレス（IPv4 または IPv6）。
ManagementIPNetmask	ドット付き 10 進形式の管理 IP サブネット（IPv4 または IPv6）。
ManagementIPGateway	管理ネットワーク上のゲートウェイ IP（IPv4 または IPv6）。アドレスは到達可能である必要があります。そうでない場合、インストールは失敗します。
ManagementVIP	クラスタの管理仮想 IP。
ManagementVIPName	クラスタの管理仮想 IP の名前。これは DNS 名を介して Crosswork クラスタ管理 VIP に到達するために使用されるオプションのパラメータです。このパラメータを使用する場合、対応する DNS レコードが DNS サーバーに存在するとともに、それが ManagementVIP および ManagementVIPName と一致している必要があります。
DataIPAddress	VM のデータ IP アドレス（IPv4 または IPv6）。
DataIPNetmask	ドット付き 10 進形式のデータ IP サブネット（IPv4 または IPv6）。
DataIPGateway	データネットワーク上のゲートウェイ IP（IPv4 または IPv6）。アドレスは到達可能である必要があります。そうでない場合、インストールは失敗します。
DataVIP	クラスタのデータ仮想 IP。

パラメータ名	説明
DataVIPName	クラスタのデータ仮想 IP の名前。これは DNS 名を介して Crosswork クラスタデータ VIP に到達するために使用されるオプションのパラメータです。このパラメータを使用する場合、対応する DNS レコードが DNS サーバーに存在するとともに、それが DataVIP および DataVIPName と一致している必要があります。
DNS	DNS サーバーの IP アドレス（IPv4 または IPv6）。アドレスは到達可能である必要があります。そうでない場合、インストールは失敗します。
NTP	NTP サーバーのアドレスまたは名前。アドレスは到達可能である必要があります。そうでない場合、インストールは失敗します。
DomainName	クラスタに使用されるドメイン名。
CWusername	Cisco Crosswork にログインするためのユーザー名。 これは省略可能なパラメータです。
CWPassword	Cisco Crosswork にログインするためのパスワード。 強力な VM パスワード（大文字と小文字、数字、特殊文字を含む 8 文字の長さ）を使用します。ディクショナリの単語に類似したパスワード（「Pa55w0rd!」など）や関連する単語に類似したパスワード（C!sco123 や Cwork321! など）の使用は避けてください。そのようなパスワードは基準を満たしていますが、脆弱であり、VM のセットアップに失敗します。
VMSize	クラスタの VM サイズ。値は large です。
VMName	VM の名前 少なくとも 3 つの一意の名前（VM ごとに 1 つ）が必要です。参照先
NodeType	VM のタイプを示します。[ハイブリッド（Hybrid）] または [ワーカー（Worker）] を選択します。 （注） 5.0 リリースの Crosswork クラスタには、ハイブリッド構成で動作する 3 つ以上の VM が必要です。
IsSeed	新しいクラスタで最初に構築する VM の場合は、[True] を選択します。 他のすべての VM の場合、または障害が発生した VM を再構築する場合は、[False] を選択します。 このパラメータは、クラスタインストーラツールを使用してインストールする場合はオプションです。

パラメータ名	説明
InitNodeCount	ハイブリッドノードとワーカーノードを含むクラスタ内のノードの総数。デフォルト値は3です。これを、展開するVM（ノード）の数に一致するように設定します。VM数の詳細については、表2 : Crosswork Network Controller パッケージ （8 ページ）を参照してください。 このパラメータは、クラスタインストーラツールを使用してインストールする場合はオプションです。
InitMasterCount	クラスタ内のハイブリッドノードの総数。デフォルト値は3です。 このパラメータは、クラスタインストーラツールを使用してインストールする場合はオプションです。
BackupMinPercent	バックアップパーティションのサイズとして使用される、データディスク容量の最小パーセンテージ。デフォルト値は50です（有効な範囲は1 ー 80）。 別の値が推奨されない限り、デフォルト値を使用してください。 （注） 最終的なバックアップ パーティション サイズは動的に計算されます。このパラメータは最小値を定義します。
ManagerDataFsSize	ハイブリッドノードのデータディスクサイズを示します（ギガバイト単位）。これはオプションのパラメータであり、明示的に指定されない場合、デフォルト値は 450 です（有効な範囲は 450 ー 8000）。 別の値が推奨されない限り、デフォルト値を使用してください。
WorkerDataFsSize	ワーカーノードのデータディスクサイズを示します（ギガバイト単位）。これはオプションのパラメータであり、明示的に指定されない場合、デフォルト値は 450 です（有効な範囲は 450 ー 8000）。 別の値が推奨されない限り、デフォルト値を使用してください。
ThinProvisioned	実稼働の展開では「false」に設定します。

パラメータ名	説明
EnableHardReservations	VM CPUおよびメモリプロファイルの予約の適用を決定します（詳細については、VMware vCenter のインストールの前提条件 （21 ページ）を参照してください）。これはオプションのパラメータであり、明示的に指定されない場合、デフォルト値は true です。 true に設定すると、VM のリソースが独占的に提供されます。この状態では、CPU コア、メモリ、または CPU サイクルが不十分な場合、インストールに失敗します。 false に設定すると（ラボインストールの場合にのみ設定）、VM のリソースはベストエフォートで提供されます。この状態では、CPU コアが不十分な場合、インストールに失敗します。
RamDiskSize	RAM ディスクのサイズ。 このパラメータはラボインストールのみに使用されます（値は 2 以上にする必要があります）。RAMDiskSize にゼロ以外の値が指定されている場合、HSDatastore 値は使用されません。
OP_Status	このパラメータは、インストーラを使用せずにインベントリを手動でインポートする場合にのみ使用（コメント化を解除）します。 パラメータは、この VM の状態を参照します。実行中のステータスを示すには、値を 2（#OP_Status = 2）にする必要があります。 これは省略可能なパラメータです。
SchemaVersion	構成マニフェストスキーマのバージョン スキーマの値はインストーラツールに付属するテンプレートで提供されるため、このパラメータを設定する必要はありません。
LogFsSize	ログパーティションサイズ（ギガバイト単位）。最小値は 10 GB、最大値は 1000 GB です。デフォルト値の使用を推奨します。
Timezone	タイムゾーンを入力します。入力は、標準の IANA タイムゾーン（「America/Chicago」など）です。 空白のままにすると、デフォルト値（UTC）が選択されます。 これは省略可能なパラメータです。
EnableSkipAutoInstallFeature	自動インストールをスキップするようにマークされたポッドは、依存するアプリケーションやポッドが明示的に要求するまで起動されません。 空白のままにすると、デフォルト値（「False」）が選択されます。
EnforcePodReservations	ポッドの最小のリソース予約を強制します。 空白のままにすると、デフォルト値（「True」）が選択されます。

パラメータ名	説明
K8sServiceNetwork	kubernetes サービスネットワークのネットワークアドレス。CIDR 範囲は「/16」固定です。 これは省略可能なパラメータです。
K8sPodNetwork	kubernetes ポッドネットワークのネットワークアドレス。CIDR 範囲は「/16」固定です。 これは省略可能なパラメータです。

表 *22 : VMware* テンプレートのパラメータ

パラメータ名	説明
vCentreAddress	vCenter IP またはホスト名。
vCentreUser	vCenter にログインするために必要なユーザー名。
vCentrePassword	vCenter にログインするために必要なパスワード。
DCname	使用するデータセンターリソースの名前。
MgmtNetworkName	VM の管理インターフェイスに接続する vCenter ネットワークの名前。
DataNetworkName	VM のデータインターフェイスに接続する vCenter ネットワークの名前。
Host	VM が展開される ESXi ホストまたはリソースグループの名前。
Datastore	このホストまたはリソースグループで使用されるデータストア。
HSDatastore	このホストまたはリソースグループの高速データストア。
DCfolder	vCenter のリソースフォルダ名。 使用しない場合 は空のままにします。
Cw_VM_Image	vCenter の Crosswork クラスタ VM イメージの名前。
HostedCwVMs	ESXi ホストまたはリソースによってホストされる VM の ID。

Crosswork Network Controller のインストールパラメータの値を決定したら、好みの方法を選択して展開を開始します。

- クラスタインストーラツールを使用した VMware vCenter への Cisco Crosswork のインストール （51 ページ）
- vCenter vSphere UI を使用した Cisco Crosswork の手動インストール （62 ページ）

クラスタインストーラツールを使用した VMware vCenter への Cisco Crosswork のインストール

この項では、クラスタインストーラツールを使用して VMware vCenter に Cisco Crosswork をインストールする手順について説明します。

（注） クラスタの作成にかかる時間は、展開プロファイルのサイズとハードウェアのパフォーマンス特性によって異なることがあります。

始める前に

クラスタインストーラツールを使用する際に知っておくべきいくつかのポイントは以下のとおりです。

- 環境がVMware vCenter のインストールの前提条件 （21 ページ）で指定されている vCenter のすべての要件を満たしていることを確認します。
- `/data` ディレクトリ内の編集されたテンプレートには、機密情報（VM パスワードと vCenter パスワード）が含められます。オペレータは、このコンテンツへのアクセスを管理する必要があります。それらを安全な環境に保管するか、編集してパスワードを削除します。
- `install.log`、`install_tf.log`、および `crosswork-cluster.tfstate` ファイルがインストール時に作成され、`/data`ディレクトリに保存されます。インストールで問題が発生した場合は、ケースをオープンするときにこれらのファイルをシスコのカスタマーエクスペリエンス チームに提供してください。
- インストールスクリプトは複数回実行しても安全です。エラーが発生した場合は、入力パラメータを修正して再実行できます。再実行する前に、`install.log`、`install_tf.log`、および`tfstate` ファイルを削除する必要があります。ツールを複数回実行すると、VM が削除されて再作成される可能性があることに注意してください。
- 複数の Crosswork クラスタのインストールに同じインストーラツールを使用している場合は、異なるローカルディレクトリからツールを実行し、展開の状態ファイルを独立させることが重要です。これを行う最も簡単な方法は、各展開用のローカルディレクトリをホストマシン上に作成し、それぞれに応じてコンテナにマッピングすることです。
- クラスタ インストーラ オプションを使用する場合は、Docker バージョン 19 以降が必要です。Docker の詳細については、https://docs.docker.com/get-docker/を参照してください
- インストールパラメータを変更したり、インストールエラーに続いてパラメータを修正したりするには、インストールを管理して VM を展開していたかどうかを区別することが重要です。展開された VM は、次のようなインストーラの出力によってわかります。

```
vsphere_virtual_machine.crosswork-IPv4-vm["1"]: Creation complete after 2m50s
[id=4214a520-c53f-f29c-80b3-25916e6c297f]
```

- 展開済みの VM の場合、展開された VM の Crosswork VM 設定またはデータセンターホストへの変更はサポートされていません。展開済みの VM が存在するときにインストーラを使用して設定を変更するには、クリーン操作を実行し、クラスタを再展開する必要があります。詳細については、クラスタインストーラを使用した VM の削除 （259 ページ）を参照してください。

- VM を再展開すると、VM のデータが削除されるため、注意が必要です。VM パラメータの変更は、Crosswork UI から実行するか、または一度に 1 つの VM を実行することを推奨します。VM の展開前に発生したインストールパラメータの変更（誤った vCenter パラメータなど）は、変更を適用してインストール操作を再実行するだけで実行できます。

既知の制限事項：

次のシナリオは、クラスタインストーラツールを使用して Crosswork クラスタをインストールする場合の注意事項です。

- 定義された vCenter ホスト VM は、データセンター内のすべてのホストで同じネットワーク名（vSwitch）を使用する必要があります。

- vCenter ストレージフォルダや仮想フォルダ構造の下に編成されたデータストアは、現在サポートされていません。参照するデータストアがフォルダの下にグループ化されていないことを確認してください。

- デイゼロインストーラによって作成されていない VM（手動で起動された VM など）は、デイゼロインストーラによっても、後で Crosswork UI を使用しても変更できません。同様に、Crosswork UI で作成された VM は、デイゼロのインストーラを使用して変更することはできません。クラスタの最初の展開後に変更を行う場合は、インベントリ情報を確実に取得してください。詳細については、『*Crosswork Network Controller 5.0 Administration Guide*』の「*Manage Clusters*」の章を参照してください。

- Crosswork はデュアルスタック構成をサポートしていないため、環境のすべてのアドレスは IPv4 または IPv6 である必要があります。ただし、vCenter UI は、IPv4 経由でアクセスするユーザーが IPv6 ESXi ホストにイメージをアップロードできるサービスを提供します。クラスタインストーラはこのサービスを使用できません。IPv6 ESXi ホストの次のいずれかの回避策を実行します。

  1. GUI を使用して OVA テンプレートイメージを手動でアップロードし、それをテンプレートに変換します。

  2. IPv6 対応マシンからクラスタインストーラを実行します。これを行うには、ドッキングされたコンテナに IPv6 アドレスをマッピングするように Docker デーモンを設定します。

（注） インストーラツールがソフトウェアを展開し、仮想マシンの電源をオンにします。お客様ご自身で仮想マシンの電源をオンにする場合は、手動インストールを使用します。

ステップ 1 vCenter データセンターで、**[ホスト（Host）]**>**[設定（Configure）]**>**[ネットワーキング（Networking）]**>**[仮想スイッチ（Virtual Switches）]** に移動し、仮想スイッチを選択します。仮想スイッチで、**[編集（Edit）]**>**[セキュリティ（Security）]**を選択し、次の DVS ポートグループプロパティを構成します。

- [プロミスキャスモード（Promiscuous mode）] を [拒否（Reject）] に設定します
- [MACアドレスの変更（MAC address changes）] を [拒否（Reject）] に設定します

設定を確認し、クラスタで使用される仮想スイッチごとにこのプロセスを繰り返します。

ステップ 2 Docker 対応マシンで、このインストール時に使用するすべてのものを保存するディレクトリを作成します。

（注） Mac を使用している場合は、ディレクトリ名が小文字であることを確認してください。

ステップ 3 インストーラバンドル（.tar.gz ファイル）と OVA ファイルを cisco.com から以前に作成したディレクトリにダウンロードします。この手順では、ファイル名をそれぞれ「**cw-na-platform-5.0.0-signed-installer.tar.gz**」と「**cw-na-platform-5.0.0-81-release-230502.ova**」として使用します。

注目 このトピックで言及されているファイル名はサンプル名であり、cisco.com の実際のファイル名とは異なる場合があります。

ステップ 4 次のコマンドを使用して、インストーラバンドルを解凍します。

```
tar -xvf cw-na-platform-5.0.0-signed-installer.tar.gz
```

インストーラバンドルの内容が新しいディレクトリに解凍されます（例：`cw-na-platform-5.0.0-signed-installer`）。この新しいディレクトリには、インストーライメージ（**cw-na-platform-installer-4.0.0-37-release-210410.tar.gz**）とイメージの検証に必要なファイルが含まれます。

ステップ 5 ファイルを開いて作成したディレクトリにディレクトリを変更し、README ファイルに目を通して、パッケージの内容、および次の手順による検証方法を理解します。

ステップ 6 次のコマンドを使用して、インストーライメージの署名を確認します。

（注） `python --version` を使用して、マシンの Python バージョンを確認します。

Python 2.x を使用している場合は、次のコマンドを使用してファイルを検証します。

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Python 3.x を使用している場合は、次のコマンドを使用してファイルを検証します。

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

（注） python がインストールされていない場合は、python.org にアクセスして、ワークステーションに適したバージョンの python をダウンロードします。

ステップ 7 次のコマンドを使用して、インストーライメージファイルを Docker 環境にロードします。

```
docker load -i <.tar.gz file>
```

次に例を示します。

```
docker load -i cw-na-platform-installer-5.0.0-81-release-230502.tar.gz
```

ステップ 8 Docker image list コマンドまたは Docker images コマンドを実行して、「イメージ ID」を取得します（次の手順で必要になります）。

次に例を示します。

```
docker images
```

結果は、次のようになります（明確にするため、必要なセクションには下線が付いています）。

```
My Machine% docker images
REPOSITORY                          TAG                                                 IMAGE ID
           CREATED        SIZE
dockerhub.cisco.com/cw-installer  cw-na-platform-installer-5.0.0-81-release-230502   a4570324fad30
  7 days ago     276MB
```

（注） 以前のリリースのインストールからの他のイメージが存在する可能性があるため、`docker images` を実行するときに表示される表の「CREATED」タイムスタンプに注意してください。これらを削除したい場合は、`docker image rm {image id}` コマンドを使用できます。

ステップ 9 次のコマンドを使用して Docker コンテナを起動します。

```
docker run --rm -it -v `pwd`:/data {image id of the installer container}
```

この例でロードされたイメージを実行するには、コマンドは次のようになります。

```
docker run --rm -it -v `pwd`:/data a4570324fad30
```

（注）
- 完全な値を入力する必要はありません。この場合、「docker run --rm -it -v `pwd`:/data a45」で十分です。Docker では、インストールに使用するイメージを一意に識別するのに十分なイメージ ID が必要です。
- 上記のコマンドでは、バックティック（`）を使用しています。シェルの意味が大きく異なるため、引用符やアポストロフィ（'）は使用しないでください。バックティックを使用すると（推奨）、テンプレートファイルと OVA は、コンテナ内ではなく、コマンドを実行したローカルディスク上のディレクトリに保存されます。
- IPv6 クラスタを展開する場合、IPv6 対応のコンテナ/VM でインストーラを実行する必要があります。そのためには、インストーラを実行する前に、次のいずれかの方法で Docker デーモンを追加で設定する必要があります。
  - **Linux ホスト（のみ）**：Docker run コマンドラインに「–network host」フラグを追加し、ホスト ネットワーキング モードで Docker コンテナを実行します。

    ```
    docker run --network host <remainder of docker run options>
    ```

- デフォルトでは、Centos/RHEL ホストはインストーラコンテナによるマウントされたデータボリュームの読み取りまたは書き込みを許可しない厳密な SELinux ポリシーを適用します。このようなホストで、次のように Z オプションを指定して Docker volume コマンドを実行します。

  ```
  docker run --rm -it -v `pwd`:/data:Z <remainder of docker options>
  ```

（注） 提供される Docker コマンドは、現在のディレクトリを使用して、テンプレートと ova ファイルを読み取り、インストール中に使用されるログファイルを書き込みます。次のいずれかのエラーが発生した場合は、パスが小文字（すべて小文字、スペースまたはその他の特殊文字なし）のディレクトリにファイルを移動する必要があります。

エラー 1：

```
% docker run --rm -it -v `pwd`:/data a45
docker: invalid reference format: repository name must be lowercase.
See 'docker run --help'
```

エラー 2：

```
docker: Error response from daemon: Mounts denied: approving /Users/Desktop: file does
 not exist
ERRO[0000] error waiting for container: context canceled
```

ステップ 10 VMware テンプレートを含むディレクトリに移動します。

```
cd /opt/installer/deployments/5.0.0/vcentre
```

ステップ 11 `/opt/installer/deployments/5.0.0/vcentre/deployment_template_tfvars` にあるテンプレートファイルを、別の名前を使用して `/data` フォルダにコピーします。

例：`cp deployment_template_tfvars /data/deployment.tfvars`

この手順の残りの部分では、すべての例で `deployment.tfvars` を使用します。

ステップ 12 `/data` ディレクトリにあるテンプレートファイルをテキストエディタで編集して、計画した展開に合わせます。必須フィールドとオプションフィールド、およびそれらの適切な設定の詳細については、インストールパラメータ（46 ページ）の表を参照してください。VMware vCenter 用マニフェストテンプレートの例（56 ページ）には、適切な書式設定のために参照できる例が含まれています。説明のコメントが削除されたため、例はよりコンパクトになりました。

ステップ 13 `/opt/installer` ディレクトリから、インストーラを実行します。

```
./cw-installer.sh install -p -m /data/<template file name> -o /data/<.ova file>
```

次に例を示します。

```
./cw-installer.sh install -p -m /data/deployment.tfvars -o
/data/cw-na-platform-5.0.0-81-release-230502.ova
```

ステップ 14 内容を読み、エンドユーザーライセンス契約（EULA）に同意したら「yes」と入力します。同意しない場合は、インストーラを終了して、シスコの担当者にお問い合わせください。

ステップ 15 プロンプトが表示されたら「yes」と入力して操作を確認します。

（注） インストール中に次のような警告が表示されることは珍しくありません。

```
Warning: Line 119: No space left for device '8' on parent controller '3'.
Warning: Line 114: Unable to parse 'enableMPTSupport' for attribute 'key' on element 'Config'.
```

インストールプロセスの完了に成功した場合（以下の出力例を参照）、これらの警告は無視できます。

サンプル出力：

```
cw_cluster_vms = <sensitive>
INFO: Copying day 0 state inventory to CW
INFO: Waiting for deployment status server to startup on 10.90.147.66. Elapsed time 0s,
retrying in 30s
Crosswork deployment status available at
http://{VIP}:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark

Once deployment is complete login to Crosswork via: https://{VIP}:30603/#/logincontroller
INFO: Cw Installer operation complete.
```

（注） タイムアウトが原因でインストールが失敗した場合は、-pオプションを指定せずにインストール（手順 13）を再実行してください。これにより、VM は並行してでなく、順次展開されます。

他の理由（たとえば、IP アドレスの入力ミス）でインストーラが失敗した場合は、エラーを修正してインストールスクリプトを再実行します。

インストールが失敗した場合（-pの有無にかかわらず）、シスコでケースをオープンし、/data ディレクトリ（およびインストーラの Docker コンテナを起動したローカルディレクトリ）で作成された .log ファイルをシスコに提出して確認してもらいます。インストールが失敗する最も一般的な 2 つの理由は、（a）パスワードが十分に複雑でないこと、および（b）テンプレートファイル内のエラーです。

次のタスク

- インストールのステータスを確認する方法については、インストールのモニター（73 ページ）を参照してください。
- 一般的なトラブルシューティングのシナリオについてはクラスタのトラブルシューティング（59 ページ）を参照してください。

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール（13 ページ）

VMware vCenter 用マニフェストテンプレートの例

次の例では、3 つのハイブリッドノード（ID 0、1、2）と 2 つのワーカーノード（ID 3、4）を含む Crosswork クラスタを展開しています。

（注） リソースプールを使用している場合は、個々の ESXi ホストのターゲット設定は許可されず、vCenter がリソースプール内のホストに VM を割り当てることに注意してください。vCenter にリソースプールが設定されていない場合は、正確な ESXi ホストパスを渡す必要があります。

```
*******
vCenter Example
********

ClusterIPStack = "IPv4"
ManagementVIP = "172.25.87.94"
ManagementIPNetmask = "255.255.255.192"
ManagementIPGateway = "172.25.87.65"
DataVIP = "192.168.123.94"
DataIPNetmask = "255.255.255.0"
DataIPGateway = "0.0.0.0"
DNS = "171.70.168.183"
DomainName = "cisco.com"
CWPassword = "****"
VMSize = "Large"
NTP = "ntp.cisco.com"
CloneTimeOut = 90
ManagerDataFsSize = 450
ThinProvisioned = true
BackupMinPercent = 50
EnableHardReservations = false
ManagerDataFsSize     = 450
WorkerDataFsSize      = 450

CwVMs = {
  "0" = {
    VMName = "vm0",
    ManagementIPAddress = "172.25.87.82",
DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.82",
    NodeType = "Hybrid"
  },
  "1" = {
    VMName = "vm1",
    ManagementIPAddress = "172.25.87.83",
DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.83",
    NodeType = "Hybrid"
  },
  "2" = {
    VMName = "vm2",
    ManagementIPAddress = "172.25.87.84",
DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.84",
    NodeType = "Hybrid"
  },
  "3" = {

    VMName = "vmworker0",
    ManagementIPAddress = "172.25.87.85",
DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.84",
    NodeType = "Worker"
  },
  "4" = {
```

```
    VMName = "vmworker1",
    ManagementIPAddress = "172.25.87.86",
DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.86",
    NodeType = "Worker"
  },

}


/********* vCentre Resource Data with Cw VM assignment *********/

VCenterDC = {
  VCenterAddress = "172.25.87.90",
  VCenterUser = administrator@vsphere.local,
  VCenterPassword = "******",
  DCname = "dc-cr",
  MgmtNetworkName = "VM Network",
  DataNetworkName = "DPortGroup10",
  VMs = [
    {
      HostedCwVMs = [
        "0",
        "1",
        "2",
       "3", "4"
  ],
      Host = "172.25.87.93",
      Datastore = "datastore3"
     HSDatastore = "datastore3",
    },]
}
```

シードノードの明示的な設定

クラスタインストーラツールは、デフォルトでは最初のVM（VM0）をシードノードとして選択します。シードノードの固有のキーを示す次のセクションをマニフェストテンプレート（.tfvars ファイル）に追加することで、シードノードを明示的に設定できます。

（注） シスコ カスタマー エクスペリエンス チームからの指示がない限り、デフォルトのシードノード値を変更しないことを推奨します。

```
cluster_settings = {
#Default Minimum number of nodes in inventory
    min_inventory     = 3
#Default Max number of nodes in inventory
    max_inventory     = 9
#Default Min number of manager nodes
    min_mngr_nodes    = 2
#Default Max number of manager nodes
    max_mngr_nodes    = 3
#Default seed node key name
    default_seed_node = "0"
}
```

クラスタのトラブルシューティング

デフォルトでは、インストーラはコマンドラインに進行状況データを表示します。インストールログは問題を特定するための基礎であり、`/data` ディレクトリに書き込まれます。

シナリオ	可能な解決策
欠落しているか無効なパラメータ	インストーラは問題に関する手掛かりを提供しますが、マニフェストファイルの HCL シンタックスにエラーがある場合は、指示が適切でない可能性があります。「タイプエラー」が見つかった場合は、設定マニフェストの形式を確認してください。 マニフェストファイルは、単純な JSON ファイルとして渡すこともできます。https://www.hcl2json.com/ のコンバータを使用して検証または変換を実行します。
証明書エラー	Crosswork アプリケーションと Crosswork Data Gateway VM を実行する ESXi ホストには NTP が設定されている必要があります。そうでない場合、最初のハンドシェイクが「certificate not valid」エラーで失敗する可能性があります。
イメージのアップロードに時間がかかる、またはアップロードが中断される	イメージのアップロード時間は、リンクとデータストアのパフォーマンスによって異なり、約 10 分以上かかると予想されます。アップロードが中断された場合、ユーザーは vSphere UI を使用して vCenter から部分的にアップロードされたイメージファイルを手動で削除する必要があります。
vCenter 認証	vCenter ユーザーには、VMware vCenter のインストールの前提条件 （21 ページ） で説明されているアクションを実行するための権限が必要です。
フローティング VIP アドレスに到達できない	VRRP プロトコルでは、一意の router_id アドバタイズメントがネットワークセグメントに存在する必要があります。デフォルトでは、Crosswork は管理で ID 169、データ ネットワーク セグメントで ID 170 を使用します。競合が発生した場合は、VIP アドレスに到達できないという症状が表れます。競合する VRRP ルータマシンを削除するか、または別のネットワークを使用します。
Crosswork VM がログインを許可しない	指定したパスワードの強度が不十分です。設定マニフェストを変更し、もう一度展開します。

シナリオ	可能な解決策
次のようなエラーが発生する。 エラー：ロック状態のエラー：状態ロックを取得中のエラー：リソースが一時的に使用できません（Error: Error locking state: Error acquiring the state lock: resource temporarily unavailable） エラー：仮想マシンの取得エラー：VM が見つかりません（Error: error fetching virtual machine: vm not found） エラー：無効なインデックス（Error: Invalid index）	これらのエラーは、最初の実行が中断された後（Ctrl+C、TCP タイムアウトなど）にインストーラを再実行するときによく発生します。修復手順は次のとおりです。 1. クリーン操作を実行するか（`./cw-installer.sh clean -m <your manifest here>`）または vCenter から手動で VM ファイルを削除します。 2. 状態ファイル（`rm/data/crosswork-cluster.tfstate`）を削除し、再試行します。
展開が「Crosswork クラスタの初期化の検証に失敗しました（Failed to validate Crosswork cluster initialization）」というエラーで失敗する	クラスタのシード VM に到達できないか、または 1 つ以上のクラスタ VM が正しく設定されていません。 1. VM が到達可能かどうかを確認し、`/var/log/firstBoot.log` と `/var/log/vm_setup.log` からログを収集します。 2. 他のクラスタノードのステータスを確認します。

VM は展開されていますが、Crosswork クラスタは形成されていません。	展開が成功すると、オペレータは VIP または任意のクラスタ IP アドレスにログインし、次のコマンドを実行してクラスタのステータスを取得できます。
	`sudo kubectl get nodes`
	3 ノードクラスタの正常な出力は次のようになります。
	`NAME STATUS ROLES AGE VERSION`
	`172-25-87-2-hybrid.cisco.com Ready master 41d v1.16.4`
	`172-25-87-3-hybrid.cisco.com Ready master 41d v1.16.4`
	`172-25-87-4-hybrid.cisco.com Ready master 41d v1.16.4`
	異なる出力の場合は、`/var/log/firstBoot.log` と `/var/log/vm_setup.log` のログを収集します。
	さらに、Ready 状態を示していないクラスタノードについては、次の情報を収集します。
	`sudo kubectl describe node <name of node>`

シナリオ	可能な解決策
イメージのアップロード中に次のエラーが表示される govc：OVF ネットワークとシステムネットワーク間の指定されたネットワークマッピングがどのホストでもサポートされていません（govc: The provided network mapping between OVF networks and the system network is not supported by any host.）	vCenter の Dswitch の設定が誤っています。動作しており、ESXi ホストにマッピングされているかどうかを確認してください。
VM の展開に時間がかかる	vCenter へのディスク負荷は、VM の複製に大きな役割を果たします。システムの負荷を軽減するために、VM インストール操作を連続的な方法で実行できます。より性能が高いシステムでは、[-p] フラグを渡すことで展開を並行して実行します。
VM は展開されますが、「エラー：使用可能な IP アドレスを待機中にエラーが発生しました（Error: timeout waiting for an available IP address）」でインストールは失敗します。	最も可能性が高いと考えられる原因は、指定した VM パラメータまたはネットワーク到達可能性の問題です。vCenter コンソールから VM ホストに入り、`/var/log/firstBoot.log` と `/var/log/vm_setup.log` のログを確認および収集します。
クラスタノードで障害が発生すると、VIP は残りのノードに転送されません。	VM に接続されているスイッチまたは vCenter Dswitch が IP アドレスの移動を許可していることを（vCenter の [不正送信を許可する（Allow Forged Transmits）]）確認します。詳細については、VMware 設定 （28 ページ）を参照してください。
vCenter に展開すると、VM の起動の最後に次のエラーが表示されます。 Error processing disk changes post-clone: disk.0: ServerFaultCode: NoPermission: RESOURCE (vm-14501:2000), ACTION (queryAssociatedProfile): RESOURCE (vm-14501), ACTION (PolicyIDByVirtualDisk)	プロファイル駆動型ストレージを有効にします。vCenter のルートレベル（つまり、すべてのリソース）での vCenter ユーザーの権限を照会します。
インストーラレポートで現在の VM 数よりも多くのリソースを追加する予定がある	Crosswork クラスタの VM 以外に、インストーラは他のいくつかのメタリソースを追跡します。そのため、たとえば 3 VM クラスタのインストールを実行すると、インストーラは VM の数よりも多くのリソースを追加する「計画」を報告することがあります。

シナリオ	可能な解決策
実行中またはクリーニング中に、インストーラが「Error: cannot locate virtual machine with UUID "xxxxxxx": virtual machine with UUID "xxxxxxxx" not found」というエラーを報告します。	解決するには、`/data/crosswork-cluster.tfstate` ファイルを削除します。 インストーラは、`/data/crosswork-cluster.tfstate` として保存されている `tfstate` ファイルを使用して、操作対象の VM の状態を維持します。vCenter UI などを使用して VM がインストーラの外部で削除された場合、この状態は同期されません。

vCenter vSphere UI を使用した Cisco Crosswork の手動インストール

この項では、vCenter vSphere UI を使用して VMware に Cisco Crosswork を手動でインストールする手順について説明します。この手順は、クラスタ内のノードごとに繰り返す必要があります。

手動インストールワークフローは 2 つの部分に分けることができます。

1. OVF テンプレートの構築 （63 ページ）
2. テンプレートの展開 （69 ページ）

最初の部分では、テンプレートを作成します。2 番目の部分では、環境に必要なワーカーノードと（通常）3 つのハイブリッドノードで構成されるクラスタを構築するのに必要な回数、テンプレートを展開します。

（注） テンプレートがすでに存在し、ワーカーノードを再構築または展開する必要がある場合は、テンプレートの展開に直接進むことができます（この手順の 2 番目の部分）。

重要 Crosswork クラスタを手動でインストールする場合は、クラスタインベントリ ファイル（.tfvars ファイル）を Crosswork UI にインポートする必要があります。インベントリファイル（Crosswork UI からサンプルをダウンロードできます）には、クラスタ内の VM に関する情報と、データセンターのパラメータが含まれています。インベントリの手動インポートを有効にするには、パラメータ `OP_Status = 2` を設定する必要があります。

この操作が完了するまで、Cisco Crosswork はクラスタ内の VM ノードを展開または削除できません。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Import Cluster Inventory*」のトピックを参照してください。

始める前に

- 環境が Crosswork クラスタ VM の要件 （30 ページ）および VMware vCenter のインストールの前提条件 （21 ページ）で指定されている vCenter のすべての要件を満たしていることを確認します。

OVF テンプレートの構築

ステップ 1 使用可能な最新の Cisco Crosswork イメージファイル（*.ova）をシステムにダウンロードします。

ステップ 2 VMware ESXi を実行して VMware vSphere Web クライアントにログインします。左側のナビゲーションペインで、VM を展開する ESXi ホストを選択します。

ステップ 3 vSphere UI で、**[ホスト（Host）]** > **[設定（Configure）]** > **[ネットワーキング（Networking）]** > **[仮想スイッチ（Virtual Switches）]** に移動し、仮想スイッチを選択します。仮想スイッチで、**[編集（Edit）]** > **[セキュリティ（Security）]**を選択し、次の DVS ポートグループプロパティを構成します。

- [プロミスキャスモード（Promiscuous mode）] を [拒否（Reject）] に設定します
- [MACアドレスの変更（MAC address changes）] を [拒否（Reject）] に設定します

設定を確認し、クラスタで使用される仮想スイッチごとにこのプロセスを繰り返します。

ステップ 4 ネットワーク設定が要件を満たしていることを確認します。

ステップ 5 **[アクション（Actions）]** > **[OVFテンプレートの展開（Deploy OVF Template）]** を選択します。

注意 デフォルトの VMware vCenter の展開タイムアウトは 15 分です。OVA イメージファイルの展開に必要な合計時間は、ネットワークの速度やその他の要因によって 15 分よりもかなり長くかかる場合があります。展開中に vCenter がタイムアウトすると、生成される VM は起動できなくなります。これを防ぐには、選択内容（IP アドレス、ゲートウェイ、DNS サーバーなど）を文書化し、情報をすばやく入力して、VMware 構成の問題を回避できるようにすることをお勧めします。

ステップ 6 VMware の [OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが表示され、最初の手順の [1 - OVFテンプレートを選択（1 - Select an OVF template）] が強調表示されます。[ファイルの選択（Choose Files）] をクリックし、OVA イメージファイルをダウンロードした場所に移動してファイルを選択します。選択すると、ファイル名がウィンドウに表示されます。

ステップ 7 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[2 - 名前とフォルダの選択（2 - Select a name and folder）] が強調表示されます。名前を入力し、作成する Cisco Crosswork VM のそれぞれのデータセンターを選択します。

Cisco Crosswork のバージョンとビルド番号を名前に含めることを推奨します（Cisco Crosswork 5.0 Build 152 など）。

ステップ 8 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）]ウィンドウが更新され、[3-コンピューティングリソースの選択（3 - Select a compute resource）]が強調表示されます。Cisco Crosswork VM のホストを選択します。

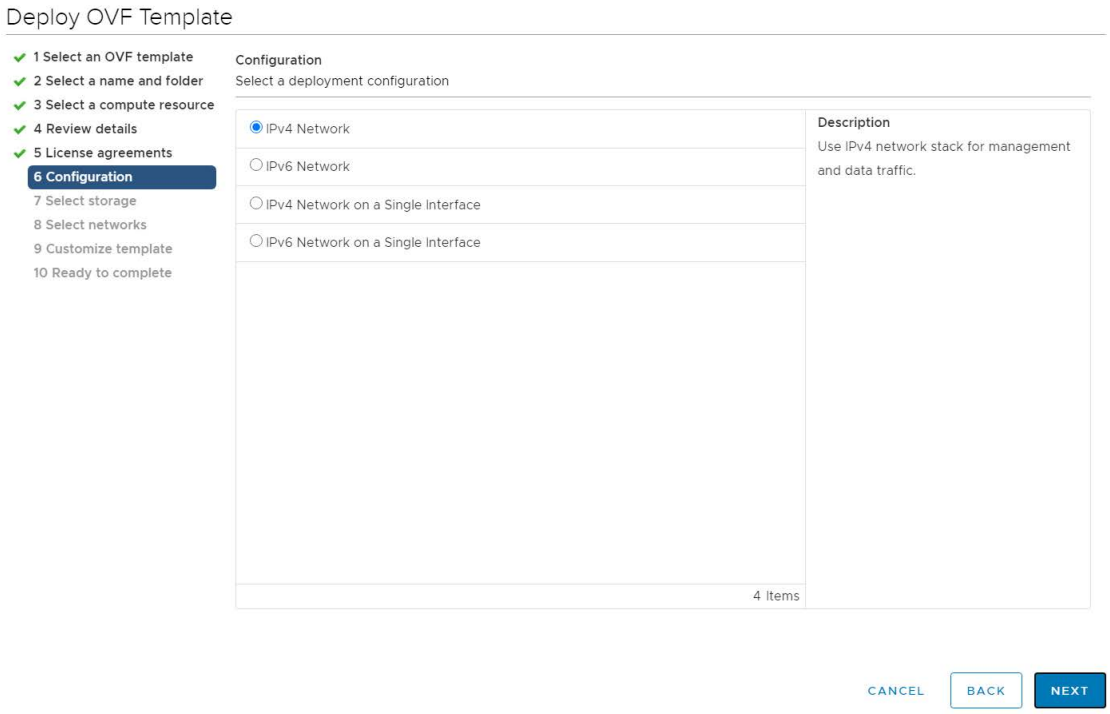
ステップ 9 [次へ（Next）] をクリックします。VMware vCenter Server が OVA を検証します。検証にかかる時間はネットワーク速度によって決まります。検証が完了すると、[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[4 - レビューの詳細（4 - Review details）] が強調表示されます。

ステップ 10 展開する OVF テンプレートを確認します。この情報は OVF から収集され、変更できないことに注意してください。

ステップ 11 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[5 - ライセンス契約（5 - License agreements）] が強調表示されます。エンドユーザーライセンス契約を確認し、同意する場合は [すべてのライセンス契約に同意する（I accept all license agreements）] チェックボックスをオンにします。同意しない場合は、シスコ エクスペリエンス チームに連絡してサポートを受けてください。

ステップ 12 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[6 - 設定（6 - Configuration）] が強調表示されます。目的の展開設定を選択します。

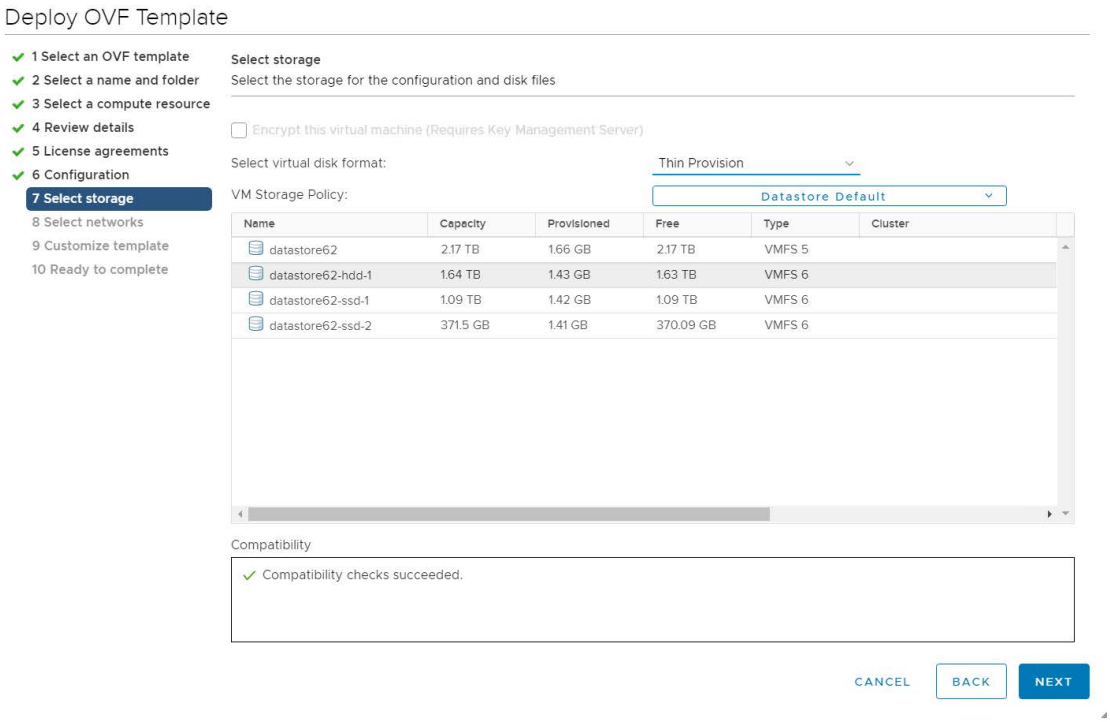
図 *4*：展開設定の選択



（注） Cisco Crosswork Data Gateway を単一のインターフェイスを使用して展開する場合は、Cisco Crosswork Data Gateway も単一のインターフェイスを使用して展開する必要があります（ラボ展開の場合にのみ推奨）。

ステップ 13 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[7 - ストレージの選択（7 - Select Storage）] が強調表示されます。[仮想ディスク形式の選択（Select virtual disk format）] ドロップダウン リストから、該当するオプションを選択します。テーブルから、使用するデータストアを選択し、そのプロパティを確認して、使用可能なストレージが十分にあることを確認します。

図 *5:* ストレージの選択



（注） 実稼働展開の場合は、[シックプロビジョニング（Eager Zeroed）（Thick Provision Eager Zeroed）] オプションを選択します。これにより、ディスク容量が事前に割り当てられ、最高のパフォーマンスが得られます。ラボで使用する場合は、ディスク容量を節約するため、[シンプロビジョニング（Thin Provision）] オプションを推奨します。

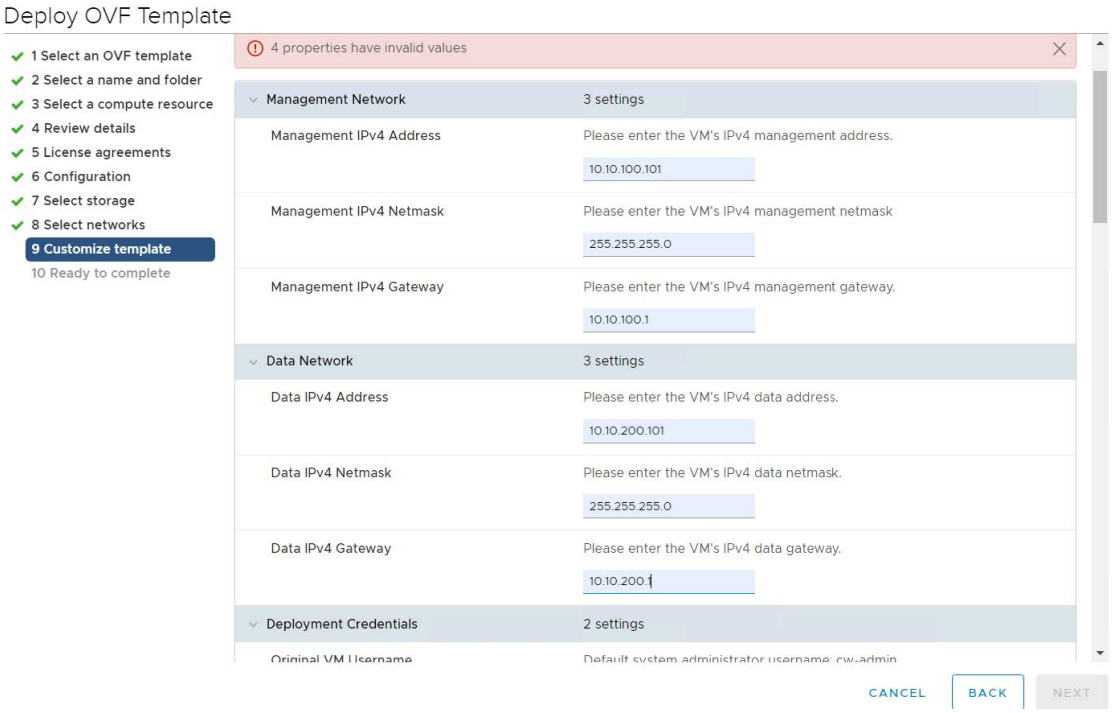
ステップ 14 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[8 - ネットワークの選択（8 - Select networks）] が強調表示されます。[データネットワーク（Data Network）] ドロップダウンリストと [ネットワーク管理（Management Network）] ドロップダウンリストから、適切な接続先ネットワークを選択します。

ステップ 15 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[9 - テンプレートのカスタマイズ（9 - Customize template）] が強調表示されます。

a) [管理ネットワーク（Management Network）] の設定を展開します。IPv4 または IPv6 の展開の情報を入力します（選択に応じて）。

b) [データネットワーク（Data Network）] 設定を展開します。IPv4 または IPv6 の展開の情報を入力します（選択に応じて）。

図 *6*: テンプレート設定のカスタマイズ



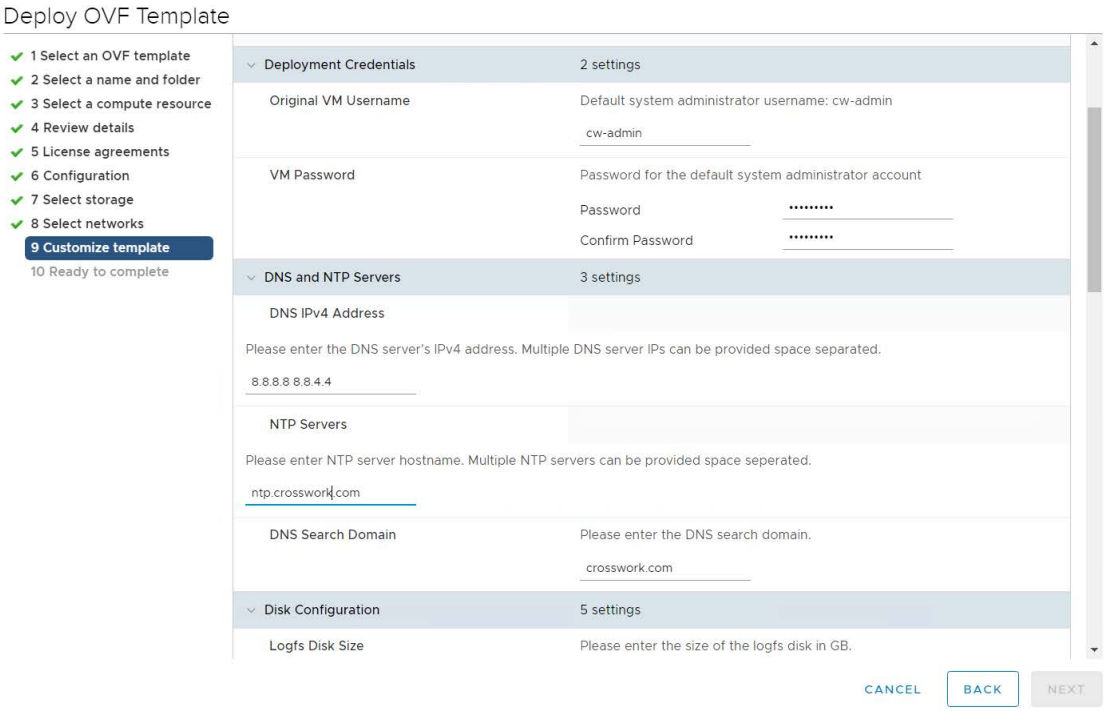
（注） [単一インターフェイス上のIPv4（IPv4 on a Single Interface）] または [単一インターフェイス上のIPv6（IPv6 on a Single Interface）] を選択した場合、[データネットワーク（Data Network）] の設定は表示されません。

c) [ログイン情報の展開（Deployment Credentials）] の設定を展開します。[VM ユーザー名（VM Username）] と [パスワード（Password）] に該当する値を入力します。

（注） 強力な VM パスワード（大文字と小文字、数字、特殊文字を含む 8 文字の長さ）を使用します。ディクショナリの単語に類似したパスワード（「Pa55w0rd!」など）や関連する単語に類似したパスワード（C!sco123 や Cwork321! など）の使用は避けてください。そのようなパスワードは基準を満たしていますが、脆弱であり、VM のセットアップに失敗します。

d) [DNS サーバーと NTP サーバー（DNS and NTP Servers）] の設定を展開します。展開の設定（IPv4 または IPv6）に応じて、表示されるフィールドは異なります。次の 3 つのフィールドに情報を入力します。

- [DNS IP アドレス（DNS IP Address）]：Cisco Crosswork サーバーで使用する DNS サーバーの IP アドレス。IP アドレスが複数ある場合はスペースで区切ります。
- [DNS 検索ドメイン（DNS Search Domain）]：DNS 検索ドメインの名前。
- [NTP サーバー（NTP Servers）]：使用する NTP サーバーの IP アドレスまたはホスト名。IP またはホスト名が複数ある場合はスペースで区切ります。



（注） DNS サーバーと NTP サーバーは、ホストにマッピングしたネットワーク インターフェイスを使用して到達可能である必要があります。そうしないと、VM の設定が失敗します。

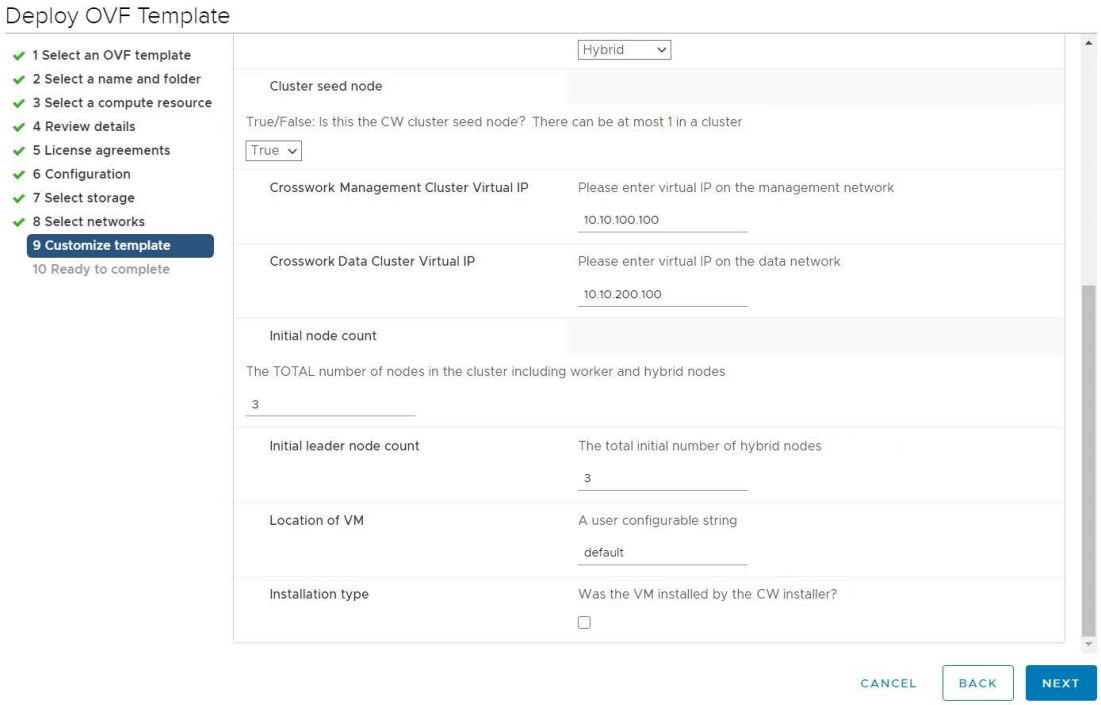
e) [Disk Configuration] のデフォルト設定は、ほとんどの環境で機能します。シスコ カスタマー エクスペリエンス チームから指示された場合にのみ、設定を変更してください。

f) [Crosswork の設定（Crosswork Configuration）] を展開し、免責事項のテキストを入力します（ユーザーが CLI にログインすると、このテキストが表示されます）。

g) [Crosswork クラスタの設定（Crosswork Cluster Configuration）] を展開します。次のフィールドに該当する値を入力します。

- [VM タイプ（VM Type）] :
  - 3 つのハイブリッドノードのいずれかである場合は、[ハイブリッド（Hybrid）] を選択します。
  - これがワーカーノードの場合は、[ワーカー（Worker）] を選択します。
- [クラスタシードノード（Cluster Seed node）] :
  - 新しいクラスタで最初に構築する VM の場合は、[True] を選択します。
  - 他のすべての VM の場合、または障害が発生した VM を再構築する場合は、[False] を選択します。
- [Crosswork Management Cluster Virtual IP]：管理仮想 IP アドレスと管理仮想 IP DNS 名を入力します。

- [Crosswork Data Cluster Virtual IP]：データ仮想 IP アドレスとデータ仮想 IP DNS 名を入力します。
- [初期ノード数（Initial node count）]：デフォルト値は 3 です。
- [初期リーダーノード数（Initial leader node count）]：デフォルト値は 3 です。
- [VM の場所（Location of VM）]：VM の場所を入力します。
- [インストール タイプ（Installation type）]：
  - 新しいクラスタのインストールの場合：チェックボックスを選択しないでください。
  - 障害が発生した VM を交換する場合：障害が発生した VM を交換するためにこの VM をインストールする場合は、このチェックボックスをオンにします。



ステップ 16 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[10 - 完了の準備（10 - Ready to Complete）] が強調表示されます。

ステップ 17 設定を確認し、展開を開始する準備ができたら [終了（Finish）] をクリックします。展開が完了するまで待ってから続行します。展開ステータスを確認するには、次の手順を実行します。

a) VMware vCenter クライアントを開きます。

b) ホスト VM の [最近のタスク（Recent Tasks）] タブに、[OVFテンプレートの展開（Deploy OVF template）] ジョブと [OVFパッケージのインポート（Import OVF package）] ジョブのステータスを表示します。

ステップ 18 テンプレートの作成を完了するには、ホストを選択し、新しくインストールしたVMを右クリックして、**[Template]** > **[Convert to Template]** を選択します。アクションを確認するプロンプトが表示されます。[はい（Yes）] をクリックして確定します。テンプレートは、vSphere Client UI の [VM とテンプレート（VMs and Templates）] タブに作成されます。

これで、手動インストールワークフローの最初の部分は終了しました。*2*番目の部分では、新しく作成したテンプレートを使用してクラスタ *VM* を構築します。

テンプレートの展開

ステップ 1 VM を構築するには、新しく作成したテンプレートを右クリックし、[New VM from This Template] を選択します。

ステップ 2 VMware の [テンプレートからの展開（Deploy From Template）] ウィンドウが開き、最初のステップの [1 - 名前とフォルダの選択（1 - Select a name and folder）] が強調表示されます。名前を入力し、VM それぞれのデータセンターを選択します。

ステップ 3 [次へ（Next）] をクリックします。[テンプレートからの展開（Deploy From Template）] ウィンドウが更新され、[2 - コンピューティングリソースの選択（2 - Select a compute resource）] が強調表示されます。Cisco Crosswork VM のホストを選択します。

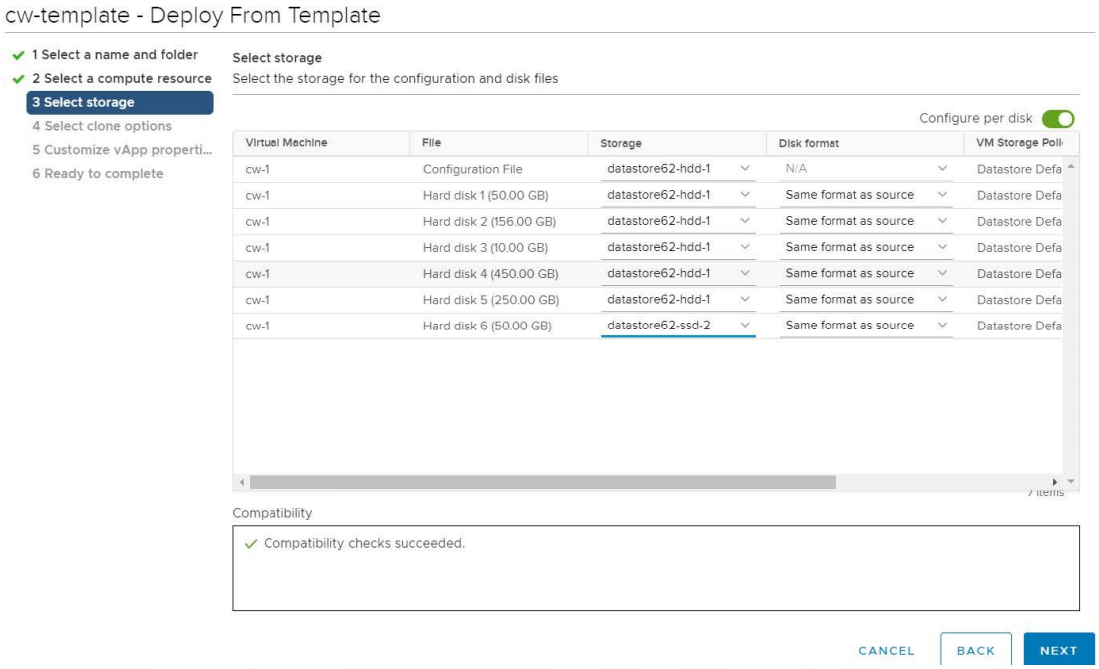
ステップ 4 [次へ（Next）] をクリックします。[テンプレートからの展開（Deploy From Template）] ウィンドウが更新され、[3 - ストレージの選択（3 - Select Storage）] が強調表示されます。仮想ディスク形式として [ソースと同じ形式（Same format as source）] オプションを選択します（推奨）。

ノードの推奨構成では、高速（通常は SSD ベース）ストレージとノーマル（通常はディスク）ストレージを組み合わせて使用します。推奨構成に従っている場合は、2 つのデータストアのステップに従います。それ以外の場合は、単一のデータストアを使用するステップに従います。

データストアを 2 つ（通常と高速）使用している場合：

- [ディスクごとの設定（Configure per disk）] オプションを有効にします。
- ディスク 1 ～ 5 の [ストレージ（Storage）] 設定と同じデータストア（通常）を選択します。このデータストアには 916 GB のスペースが必要です。
- ディスク 6 の [ストレージ（Storage）] の設定としてホストの高速（ssd）データストアを選択します。高速データストアには、少なくとも 50 GB のスペースが必要です。

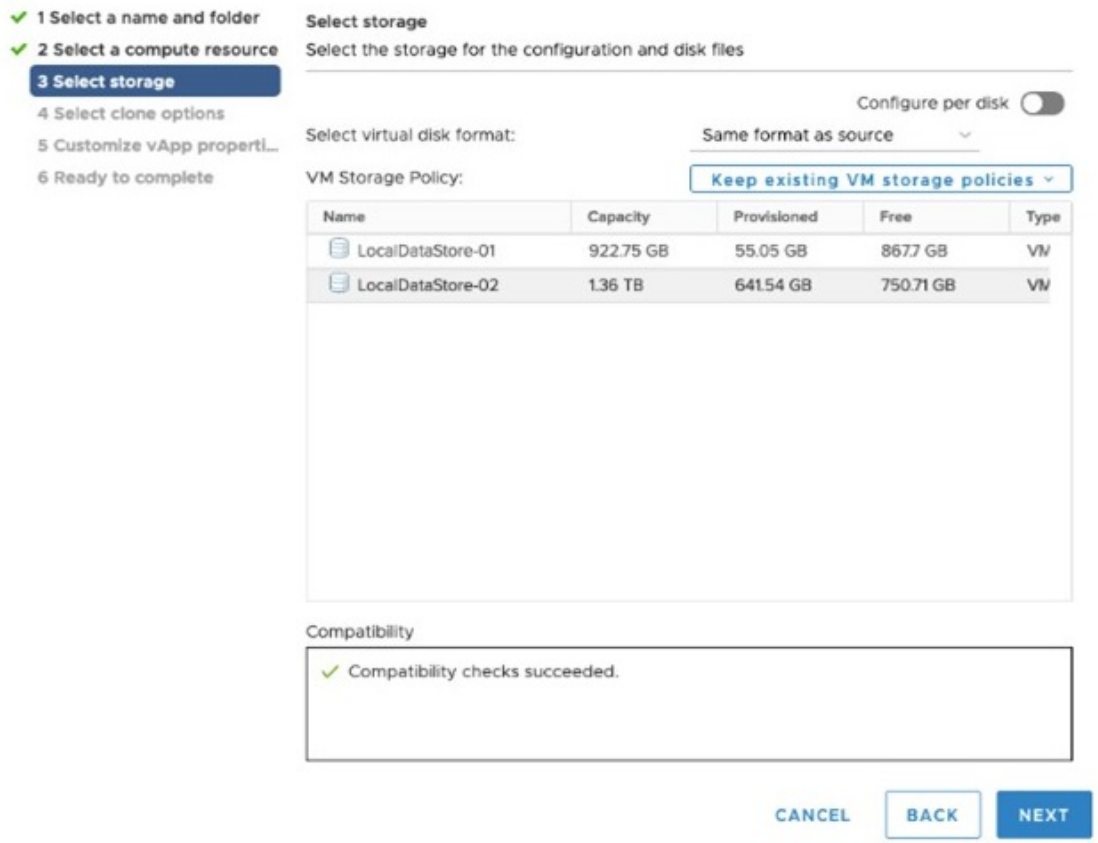
図 7:ストレージの選択：ディスクごとの設定



- [次へ（Next）] をクリックします。

単一のデータストアを使用している場合：使用するデータストアを選択し、[次へ（Next）] をクリックします。

図 *8*：ストレージの選択：単一のデータストア



ステップ 5 [テンプレートから展開（Deploy From Template）] ウィンドウが更新され、[4 - クローンオプションの選択（4 - Select clone options）] が強調表示されます。ここでクローンオプションをさらに選択できます。

（オプション）次の手順を実行して、ディスク、メモリ、および拡張ファームウェア インターフェイス（EFI）のブート設定を行います。

（注） ラボ以外の環境では、適切な量のメモリと CPU リソースを使用するようにハードウェアを再構成する必要があります。

- [この仮想マシンのハードウェアのカスタマイズ（Customize this virtual machine's hardware）] を選択し、[次へ（Next）] をクリックします。[設定の編集（Edit Settings）] ダイアログボックスが表示されます。
- [仮想ハードウェア（Virtual Hardware）] タブで、[CPU] と [メモリ（Memory）] に該当する値を入力します（Crosswork クラスタ VM の要件 （30 ページ）を参照）。
- [VM オプション（VM Options）] タブで、[ブートオプション（Boot Options）] を展開し、[ファームウェア（Firmware）] として [EFI] を選択し、[セキュアブート（Secure Boot）] チェックボックスをオンにします。

ステップ 6 [次へ（Next）] をクリックします。[テンプレートからの展開（Deploy From Template）] ウィンドウが更新され、[5 - vApp プロパティのカスタマイズ（5 - Customize vApp properties）] が強調表示されます。このウィンドウには、テンプレートの vApp プロパティがすでに入力されています。次のフィールドを確認する必要があります。

- [クラスタシードノード（Cluster Seed node）]：
  - 新しいクラスタで最初に構築する VM の場合は、[True] を選択します。
  - 他のすべての VM の場合、または障害が発生した VM を再構築する場合は、[False] を選択します。
- [管理ネットワーク設定（Management Network settings）]：クラスタ内の各 VM に正しい IP 値を入力します。
- [データネットワーク設定（Data Network settings）]：クラスタ内の各 VM に正しい IP 値を入力します。
- [Crosswork管理クラスタ仮想IP（Crosswork Management Cluster Virtual IP）]：仮想 IP は各クラスタノードで同じままになります。
- [Crosswork データクラスタ仮想 IP（Crosswork Data Cluster Virtual IP）]：仮想IPは各クラスタノードで同じままです。
- [展開ログイン情報（Deployment Credentials）]：クラスタ内の各 VM に同じ展開ログイン情報を入力します。

（注） （オプション）[仮想ハードウェア（Virtual Hardware）] タブの [予約（Reservation）] フィールドを使用して、VM の CPU 割り当て（MHz）とメモリプロファイル（MB）の予約を設定します。

（注） 障害が発生した VM を交換するためにこの VM を展開する場合は、IP とその他の設定を交換するマシンと一致させる必要があります。

ステップ 7 [次へ（Next）] をクリックします。[テンプレートからの展開（Deploy From Template）] ウィンドウが更新され、[6 - 完了の準備（6 - Ready to Complete）] が強調表示されます。設定を確認し、展開を開始する準備ができたら [終了（Finish）] をクリックします。

ステップ 8 **手順 1 ～ 7** を繰り返して、クラスタ内の残りの VM を展開します。

ステップ 9 これで、Cisco Crosswork VM の電源をオンにして、展開プロセスを完了することができます。クラスタシードノードとして選択された VM の電源を最初にオンにし、次に（数分後）残りの VM の電源を投入する必要があります。電源をオンにするには、ホストのエントリを展開し、[Cisco Crosswork VM] をクリックして、**[アクション（Actions）]** > **[電源（Power）]** > **[電源オン（Power On）]** を選択します。

ステップ 10 クラスタの作成にかかる時間は、展開プロファイルのサイズとハードウェアのパフォーマンス特性によって異なることがあります。インストールのステータスを確認する方法については、インストールのモニター （73 ページ）を参照してください。

（注） 障害が発生した VM を交換するためにこの手順を実行している場合は、Cisco Crosswork GUI からステータスを確認できます（**[管理（Administration ）] > [Crosswork マネージャ（Crosswork Manager）]** に移動し、クラスタタイルをクリックして [Crosswork クラスタ（Crosswork Cluster）] のステータスを確認します）。

（注） このプロセスを使用して新しいワーカーノードを構築する場合、ノードの電源を入れた後に追加の作業は必要ありません。ノードは既存の Kubernetes クラスタに登録されます。

リソースをワーカーノードに割り当てる方法の詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Rebalance Cluster Resources*」のトピックを参照してください。

次のタスク

Crosswork UI にログイン後、クラスタ インベントリ ファイル（.tfvars ファイル）を Crosswork UI にインポートします。インベントリファイル（Crosswork UI からサンプルをダウンロードできます）には、クラスタ内の VM に関する情報と、データセンターのパラメータが含まれています。インベントリの手動インポートを有効にするには、パラメータ `OP_Status = 2` を設定する必要があります。この操作が完了するまで、Cisco Crosswork はクラスタ内の VM ノードを展開または削除できません。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Import Cluster Inventory*」のトピックを参照してください。

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）

インストールのモニター

この項では、インストールが正常に完了したかどうかをモニターし、確認する方法について説明します。インストーラは、クラスタを構築および設定するときに、進捗状況を報告します。インストーラは、ライセンス契約に同意し、インストールを続行するかどうかを尋ねるプロンプトを表示します。確認後、インストールが進行し、`installer.log` または `installer_tf.log` のいずれかに発生する可能性のあるエラーが記録されます。VM が作成され、起動できる場合、オペレータが指定した構成を適用する際のエラーが VM の /var/log/firstboot.log に記録されます。

（注） インストール時に Cisco Crosswork は特別な管理 ID を作成します（マニフェストテンプレートで指定したパスワードの**仮想マシン（VM）管理者**、*cw-admin*。インストーラがログイン情報を適用できない場合、インストーラは、デフォルトのパスワード *cw-admin* で管理 ID を作成します）。管理 ID を使用して初めてログインした場合は、パスワードを変更するよう求められます。

管理ユーザー名は予約されており、変更できません。データセンター管理者はこの ID を使用して Crosswork アプリケーション VM にログインし、トラブルシューティングを行います。

次に、プロセスが予想どおりに進行していることを確認するために監視できるプロセス内の重要な手順のリストを示します。

1. インストーラは、Crosswork イメージファイル（.ova ファイル）を vCenter データセンターにアップロードします。

（注） 実行時に、インストーラは .ova ファイルがまだ存在しない場合は、そのファイルを vCenter にアップロードし、VM テンプレートに変換します。インストールが正常に完了した後、イメージが不要になった場合は、vCenter UIからテンプレートファイルを削除できます（VMおよびテンプレート）。

2. インストーラは VM を作成し、各 VM が作成された後に成功メッセージ（「作成が完了しました（Creation Complete）」など）を表示します。

（注） VMware 展開の場合、このアクティビティも vSphere UI からもモニターできます。

3. 各 VM が作成されると、（インストーラの完了時に自動的に、または手動インストール中に VM を電源オンした後に）電源オンされます。テンプレートで指定されたパラメータが VM に適用され、再起動されます。その後、VM は Kubernetes によって登録され、クラスタを形成します。

4. クラスタが作成され、アクセス可能になると、成功メッセージ（「Crosswork インストーラの操作が完了しました（Crosswork Installer operation complete）」など）が表示され、インストーラスクリプトが終了し、画面上のプロンプトに戻ります。

次の方法を使用して、スタートアップの進行状況をモニターできます。

- **ブラウザでアクセス可能なダッシュボードを使用**：

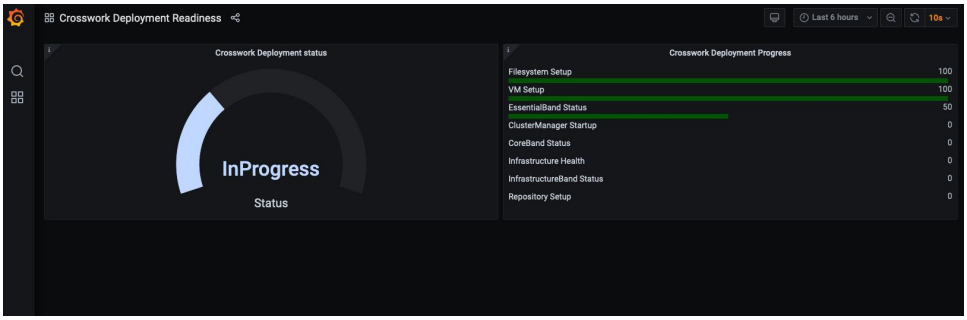
  1. クラスタの作成中に、ブラウザでアクセス可能なダッシュボードからセットアッププロセスをモニターできます。

  2. インストーラが完了すると、この grafana ダッシュボードの URL (`http://{VIP}:30602/d/NK1bwWxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark`

の形式）が表示されます。この URL は一時的なものであり、使用できるのは限られた時間（約 30 分）だけです。

3. 展開の最後に、grafana ダッシュボードに [準備完了（Ready）] ステータスが報告されます。URL にアクセスできない場合は、このセクションで説明する SSH コンソールを使用してインストールプロセスをモニターできます。

図 *9 : Crosswork* 展開の準備状況



- **コンソールを使用**：

1. いずれかのハイブリッド VM のコンソールから、または仮想 IP アドレスへの SSH を使用して、進行状況を確認できます。
2. 後者の場合、インストールテンプレートでそのアカウントに割り当てた *cw-admin* のユーザー名とパスワードを使用してログインします。
3. `sudo su -` コマンドを使用してスーパーユーザーに切り替えます。
4. `kubectl get nodes`（ノードの準備ができているかどうかを確認するため）および `kubectl get pods`（実行中のアクティブなポッドのリストを確認するため）コマンドを実行します。
5. アクティブなポッドのリストに `robot-ui` が表示されるまで、`kubectl get pods` コマンドを繰り返します。
6. この時点で、Cisco Crosswork UI へのアクセスを試すことができます。

Cisco Crosswork UI にアクセスできるようになったら、UI からステータスをモニターすることもできます。詳細については、Cisco Crosswork UI へのログイン （76 ページ）を参照してください。

障害シナリオ

障害が発生した場合（以下を参照）、シスコのカスタマーエクスペリエンスチームに連絡し、`installer.log` ファイル、`installer_tf.log` ファイル、および `firstBoot.log` ファイル（VM ごとに 1 つ）を提供します。

- インストールが不完全
- インストールは完了したが、VM が機能しない

- インストールは完了したが、/var/log/firstBoot.log または /opt/robot/bin/firstBoot.log ファイルを確認するように指示される。

次に行う作業：

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）

Cisco Crosswork UI へのログイン

クラスタのアクティブ化とスタートアップが完了した後、すべてのノードがクラスタ内で稼働しているかどうかを Cisco Crosswork UI から確認できます。Cisco Crosswork UI にログインし、クラスタの正常性を確認するには、次の手順を実行します。

（注） インストールの際、Cisco Crosswork UI にアクセスできない場合は、VMware または AWS UI からホストのコンソールにアクセスして、VM の設定に問題があったかどうかを確認してください。ログイン時に、firstboot.log ファイルを確認するように指示された場合は、ファイルを確認して問題を特定してください。エラーを特定できる場合は、エラーを修正し、インストーラを再実行します。サポートが必要な場合は、シスコのカスタマーエクスペリエンスチームにお問い合わせください。

ステップ 1 サポートされているブラウザのいずれかを起動します（サポートされる Web ブラウザ （43 ページ）を参照）。

ステップ 2 ブラウザのアドレスバーに次のように入力します。

`https://<Crosswork Management Network Virtual IP (IPv4)>:30603/`

または

`https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/`

（注） URL の IPv6 アドレスはブラケットで囲む必要があることに注意してください。

（注） Crosswork FQDN 名を使用して Crosswork UI にログインすることもできます。

[ログイン（Log In）] ウィンドウが開きます。

（注） 初めて Cisco Crosswork にアクセスすると、一部のブラウザでは、サイトが信頼できないという警告が表示されます。この場合は、指示に従ってセキュリティ例外を追加し、Cisco Crosswork サーバーから自己署名証明書をダウンロードします。セキュリティの例外を追加すると、ブラウザは今後のすべてのログイン試行で信頼できるサイトとしてサーバーを受け入れます。CA 署名付き証明書を使用する場合は、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Manage Certificates*」のトピックを参照してください。

ステップ 3 次のように Cisco Crosswork にログインします。

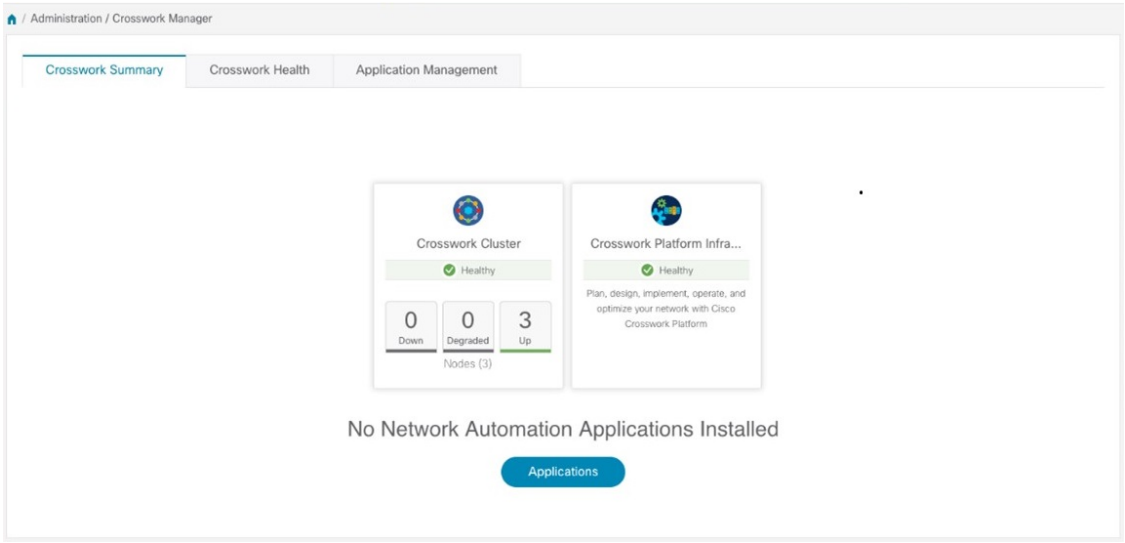
a) Cisco Crosswork 管理者のユーザー名の **admin** とデフォルトのパスワードの **admin** を入力します。

b) [ログイン（Log In）] をクリックします。

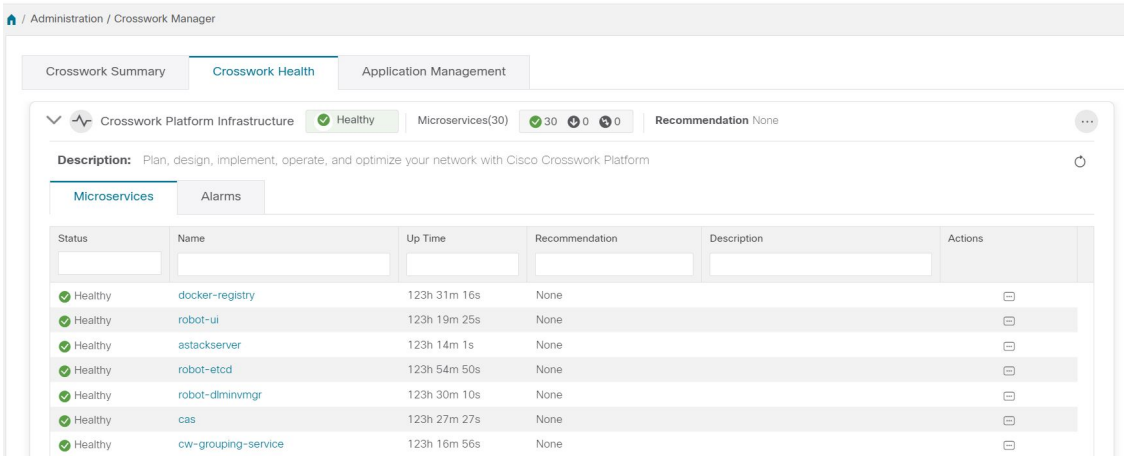
c) 管理者のデフォルトのパスワードを変更するように求められたら、表示されたフィールドに新しいパスワードを入力し、[OK] をクリックします。

（注） 強力な VM パスワード（大文字と小文字、数字、特殊文字を含む 8 文字以上の長さ）を使用します。ディクショナリの単語に類似したパスワード（「Pa55w0rd!」など）や関連する単語に類似したパスワード（C!sco123 や Cwork321! など）の使用は避けてください。

[Crosswork マネージャ（Crosswork Manager）] ウィンドウが表示されます。

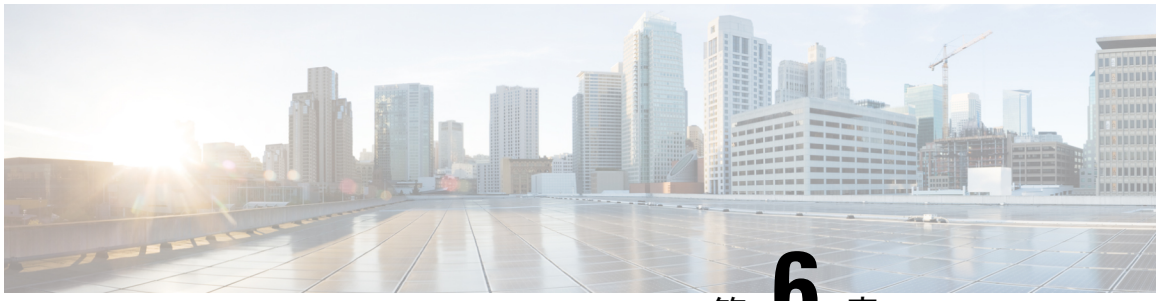


ステップ 4 （オプション）[Crossworkの正常性（Crosswork Health）] タブをクリックし、[Crossworkプラットフォームインフラストラクチャ（Crosswork Platform Infrastructure）] タブをクリックして Cisco Crosswork で実行されているマイクロサービスの正常性ステータスを表示します。



次のタスク

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）



第 6 章

VMware vCenter への Cisco Crosswork Data Gateway のインストール

この章は次のトピックで構成されています。

Cisco Crosswork Data Gateway のインストールワークフロー

Cisco Crosswork Data Gateway は、Cisco Crosswork に登録するのに十分なソフトウェアのみを含むベース VM としてインストールされます。

（注） 同じ Cisco Crosswork Data Gateway を Cisco Crosswork とともに再展開する場合は、Data Gateway Management の仮想マシンテーブルから以前の Crosswork Data Gateway エントリを削除します。Crosswork Data Gateway VM を削除する方法については、Cisco Crosswork から Crosswork Data Gateway VM を削除する （261 ページ）を参照してください。

Cisco Crosswork で使用する Crosswork Data Gateway VM をインストールするには、次の手順を実行します。

1. Crosswork Data Gateway VM の展開プロファイルを選択します。「Crosswork Data Gateway VM の要件 （32 ページ）」を参照してください。
2. 「Cisco Crosswork Data Gateway のパラメータと展開シナリオ」でインストールパラメータを確認し、希望する展開シナリオ（1、2、または 3 つの NIC）を使用して Crosswork Data

Gateway をインストールするために必要な情報がすべて揃っていることを確認してください。

3. 以下の中からお好みの方法で Cisco Crosswork Data Gateway をインストールします。

表 *23 : Crosswork Data Gateway* のインストールオプション

VMware	vCenter vSphere クライアントを使用した Cisco Crosswork Data Gateway のインストール （100 ページ）
	OVF ツールを使用した Cisco Crosswork Data Gateway のインストール （115 ページ）

4. 「Crosswork Data Gateway インストール後のタスク （123 ページ）」のセクションで説明されているインストール後のタスクを実行します。

（注） 負荷や拡張の要件のために複数の Cisco Crosswork Data Gateway をインストールする場合や Cisco Data Gateway の高可用性を活用する場合は、すべての Cisco Crosswork Data Gateway VM をインストールしてから、それらを Data Gateway プールに追加することを推奨します。

5. Cisco Crosswork に Crosswork Data Gateway VM が正常に登録されたことを確認します。登録プロセスを確認する方法については、Cisco Crosswork Data Gateway の認証と登録 （122 ページ）を参照してください。

Crosswork Data Gateway VM が Cisco Crosswork に正常に登録されたことを確認したら、Cisco Crosswork Data Gateway プールを作成することで、Cisco Crosswork Data Gateway を収集用にセットアップします。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Create a Crosswork Data Gateway Pool」のセクションを参照してください。

Cisco Crosswork Data Gateway のパラメータと展開シナリオ

Crosswork Data Gateway のインストールを開始する前に、このセクションに目を通し、展開パラメータと展開シナリオについてご確認ください。

Crosswork Data Gateway では、すべてのインターフェイスで IPv4 または IPv6 アドレスのいずれかがサポートされます。Cisco Crosswork はデュアルスタック構成をサポートしていません。そのため、環境のアドレスはすべて IPv4 または IPv6 のいずれかとしてプランニングしてください。

インストール時に、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） は 2 つのユーザーアカウントを作成します。

- インストール時にユーザー名 dg-admin とパスワードが設定された Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の管理者。管理者は Cisco Crosswork デー

タゲートウェイ（Cisco Crosswork Data Gateway） のログインやトラブルシューティングにこの ID を使用します。

- インストール時にユーザー名 dg-oper とパスワードが設定された Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のオペレータ。dg-oper ユーザーには、すべての「read」操作と限定された「action」コマンドを実行する権限があります。

  管理者およびオペレータが実行できる操作については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Supported User Roles」のトピックを参照してください。

dg-admin および **dg-oper** ユーザーアカウントは予約済みのユーザー名であり、変更できません。両方のアカウントに対して、コンソールでパスワードの変更を実行できます。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Change Passphrase」のセクションを参照してください。パスワードを紛失した場合や忘れた場合は必要に応じ、現在の VM を破棄し、新しい VM を作成して、新しい VM を Crosswork Cloud に再登録する必要があります。

次の表では、以下の点に注意してください。

* は必須パラメータであることを示します。このマークのないパラメータはオプションです。展開シナリオに基づいて選択できます。展開シナリオについては、（必要に応じて）[その他の情報（Additional Information）] 列で説明します。

** インストール中に入力できるパラメータ、または後で追加の手順を使用して入力できるアドレスを示します。

表 *24 : Cisco Crosswork* データゲートウェイ（*Cisco Crosswork Data Gateway*） 導入パラメータとシナリオ

ラベル	キー	説明	その他の情報
ホスト情報			
ホスト名（Hostname） *	`Hostname`	完全修飾ドメイン名（FQDN）として指定された Cisco Crosswork Data Gateway VM の名前。 大規模なシステムでは、複数の Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） VM が存在する可能性があります。したがって、ホスト名は一意であり、特定の VM を簡単に識別できるように作成する必要があります。	

ラベル	キー	説明	その他の情報
説明（Description）*	`Description`	Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の詳細です。	
ラベル	`Label`	複数の Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） VM を分類およびグループ化するために Cisco Crosswork で使用されるラベル。	
展開*	`Deployment`	Crosswork Data Gateway が展開されるコントローラアプリケーションのタイプを伝えるパラメータ。オンプレミスのインストールの場合は、Crosswork On-Premise です。 デフォルト値は `Crosswork On-Premise Standard` です。 プール内のすべてのデータゲートウェイは、展開タイプである必要があります。	
プロファイル*	`Profile`	パラメータは、VM リソースプロファイルを伝達します。オンプレミスインストールの場合は、次のいずれかを選択します。 • `Standard` • `Extended` デフォルトは `Standard` です。	VMware vCenter の場合、このパラメータを構成することはできません。OVF ツールは、このパラメータをデフォルト値で構成します。

ラベル	キー	説明	その他の情報
AllowRFC8190*	`AllowRFC8190`	使用可能な RFC 8190 の範囲内にあるインターフェイスアドレスを検証する方法を選択します。オプションは `Yes`、`No` または `Ask` です。初期構成スクリプトで確認が求められます。 デフォルト値は `Yes` で、RFC 8190 の範囲のインターフェイスアドレスを自動的に許可します。	

ラベル	キー	説明	その他の情報
秘密キー URI（Private Key URI）	DGCertKey	セッションキー署名用の秘密キーファイルへの SCP URI。これは SCP（user@host:path/to/file）を使用して取得できます。	Cisco Crosswork は、Cisco Crosswork Data Gateway とのハンドシェイクに自己署名証明書を使用します。これらの証明書はインストール時に生成されます。 ただし、サードパーティまたは独自の証明書ファイルを使用する場合は、これらのパラメータを入力します。 証明書チェーンは、Cisco Crosswork Data Gateway VM のプリセットまたは生成された証明書を上書きし、SCP URI（user:host:/path/to/file）として指定されます。 URI ファイルを持つホストは、ネットワーク上で（SCP を介して vNIC0 インターフェイスから）到達可能でなければならず、ファイルはインストール時に存在している必要があります。
証明書ファイルとキーパスフレーズ（Certificate File and Key Passphrase）	DGCertChainPwd	Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の PEM 形式の証明書ファイルと秘密キーを取得する SCP ユーザーのパスフレーズ。	
データディスクサイズ（Data Disk Size）	DGAppdataDisk	2 番目のデータディスクのサイズを示します（GB 単位）。各プロファイルのこのパラメータのデフォルト値は次のとおりです。 • Standard：20 GB。 • Extended：520 GB。	

ラベル	キー	説明	その他の情報
HA ネットワークモード*	HANetworkMode	HA ネットワークのモードを示します。 次のオプションがあります。 • L2 • L3 デフォルト値は L2 です。	
パスフレーズ			
dg-admin パスフレーズ（dg-admin Passphrase）*	dg-adminPassword	dg-admin ユーザ用に選択したパスワード。 パスワードは 8 ー 64 文字である必要があります。	
dg-oper パスフレーズ（dg-oper Passphrase）*	dg-operPassword	dg-oper ユーザ用に選択したパスワード。 パスワードは 8 ー 64 文字である必要があります。	
インターフェイス 3-NIC 展開では、管理トラフィック（vNIC0）および制御/データトラフィック（vNIC1）の IP アドレスのみを指定する必要があります。デバイスアクセストラフィック（vNIC2）の IP アドレスは、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Create a Crosswork Data Gateway Pool」のセクションで説明されているように、Crosswork Data Gateway プールの作成時に割り当てられます。 （注） vNIC の [IPv4メソッド（IPv4 Method）] フィールドと [IPv6メソッド（IPv6 Method）] フィールドの両方で [なし（None）] を選択すると、展開が機能しなくなります。			

ラベル	キー	説明	その他の情報
NicDefaultGateway*	NicDefaultGateway	DNS および NTP トラフィックを処理するためのデフォルトゲートウェイとして使用されるインターフェイス。 オプションは、eth0、eth1、または eth2 です。デフォルト値は eth0 です。	
NicAdministration*	NicAdministration	SSH アクセスを介して VM にアクセスするために使用されるインターフェイス。 オプションは、eth0、eth1、または eth2 です。デフォルト値は eth0 です。	
NicExternalLogging*	NicExternalLogging	ログを外部ロギングサーバーに送信するために使用されるインターフェイス。 オプションは、eth0、eth1、または eth2 です。デフォルト値は eth0 です。	
NicManagement*	NicManagement	登録およびその他の管理トラフィックを送信するために使用されるインターフェイス。 オプションは、eth0、eth1、または eth2 です。デフォルト値は eth0 です。	

ラベル	キー	説明	その他の情報
NicControl*	NicControl	宛先、デバイス、および収集設定の送信に使用されるインターフェイス。 オプションは、eth0、eth1、または eth2 です。デフォルト値は eth1 です。	
NicNBExternalData*	NicNBExternalData	収集データを外部の宛先に送信するために使用されるインターフェイス。 オプションは、eth0、eth1、または eth2 です。デフォルト値は eth1 です。	
NicSBData*	NicSBData	デバイスからデータを収集するために使用されるインターフェイス。 オプションは、eth0、eth1、または eth2 です。デフォルト値は eth2 です。	

vNIC IPv4 アドレス（使用するインターフェイスの数に応じて vNIC0、vNIC1、および vNIC2）

重要 1 つの NIC を使用する予定の場合は、vNIC0 に割り当てられた IPv4 または IPv6 アドレスを取得するように Crosswork Data Gateway を構成する必要があります。2 つの NIC を使用する場合は、vNIC0 と vNC1 のメソッド（[なし（None）] または [静的（Static）]）とタイプ（[Ipv4] または [IPv6]）の値を指定します。3 つの NIC の場合、vNIC0 と vNIC0 のメソッドとタイプを指定します。vNIC を使用していない場合は、メソッドの値として [なし（None）] を選択します。

ラベル	キー	説明	その他の情報

vNIC IPv4 メソッド（vNIC IPv4 Method）*
 	
たとえば、vNIC0 のパラメータ名は vNIC0 IPv4 方式（vNIC0 IPv4 Method）です。
	`Vnic0IPv4Method`
	`Vnic1IPv4Method`
	`Vnic2IPv4Method`
		インターフェイスに IPv4 アドレスを割り当てるメソッド（[なし（None）] または [静的（Static）]）。
		デフォルト値は `[なし（None）]` です。
			[メソッド（Method）] の選択に応じて、以下を実行します。
			• [なし（None）]：vNIC IPv4 パラメータの残りのフィールドをスキップします。vNIC IPv6 アドレスパラメータへの情報の入力に進みます。
			• [静的（Static）]：[アドレス（Address）]、[ネットマスク（Netmask）]、[スキップゲートウェイ（Skip Gateway）]、および [ゲートウェイ（Gateway）] フィールドに情報を入力します。

vNIC IPv4 アドレス（vNIC IPv4 Address）	`Vnic0IPv4Address`
	`Vnic1IPv4Address`
	`Vnic2IPv4Address`
		インターフェイスの IPv4 アドレス。	

vNIC IPv4 ネットマスク（vNIC IPv4 Netmask）	`Vnic0IPv4Netmask`
	`Vnic1IPv4Netmask`
	`Vnic2IPv4Netmask`
		ドット区切りの 4 つの数字列形式によるインターフェイスの IPv4 ネットマスク。	

vNIC IPv4 スキップゲートウェイ（vNIC IPv4 Skip Gateway）	`Vnic0IPv4SkipGateway`
	`Vnic1IPv4SkipGateway`
	`Vnic2IPv4SkipGateway`
		デフォルト値は `False` です。
		これを `True` に設定すると、ゲートウェイの設定がスキップされます。	

vNIC IPv4 ゲートウェイ（vNIC IPv4 Gateway）	`Vnic0IPv4Gateway`
	`Vnic1IPv4Gateway`
	`Vnic2IPv4Gateway`
		vNIC ゲートウェイの IPv4 アドレス。	

vNIC IPv6 アドレス（使用するインターフェイスの数に応じて vNIC0、vNIC1、および vNIC2）			

ラベル	キー	説明	その他の情報

vNIC IPv6 メソッド（vNIC IPv6 Method）*	`Vnic0IPv6Method`
	`Vnic1IPv6Method`
	`Vnic2IPv6Method`
		vNIC インターフェイスに IPv6 アドレスを割り当てるメソッド（[なし（None）]、[静的（Static）] または [SLAAC]）。
		デフォルト値は `[なし（None）]` です。
			[メソッド（Method）] の選択に応じて、以下を実行します。
			• [なし（None）]：vNIC IPv6 パラメータの残りのフィールドをスキップします。vNIC IPv4 アドレスパラメータに情報を入力します。
			• [静的（Static）]：[アドレス（Address）]、[ネットマスク（Netmask）]、[スキップゲートウェイ（Skip Gateway）]、および [ゲートウェイ（Gateway）] フィールドに情報を入力します。
			VnicxIPv6Address のデフォルト値は変更しないでください。

vNIC IPv6 アドレス（vNIC IPv6 Address）	`Vnic0IPv6Address`
	`Vnic1IPv6Address`
	`Vnic2IPv6Address`
		インターフェイスの IPv6 アドレス。	

vNIC IPv6 ネットマスク（vNIC IPv6 Netmask）	`Vnic0IPv6Netmask`
	`Vnic1IPv6Netmask`
	`Vnic2IPv6Netmask`
		インターフェイスの IPv6プレフィックス。	

vNIC IPv6 スキップゲートウェイ（vNIC IPv6 Skip Gateway）	`Vnic0IPv6SkipGateway`
	`Vnic1IPv6SkipGateway`
	`Vnic2IPv6SkipGateway`
		オプションは `True` または `False` です。
		`True` を選択すると、ゲートウェイの設定がスキップされます。	

vNIC IPv6 ゲートウェイ（vNIC IPv6 Gateway）	`Vnic0IPv6Gateway`
	`Vnic1IPv6Gateway`
	`Vnic2IPv6Gateway`
		vNIC ゲートウェイの IPv6 アドレス。	

vNIC ロール			

ラベル	キー	説明	その他の情報
デフォルトゲートウェイ	DEFAULT_GATEWAY	すべてのタイプのトラフィックのフローを許可するインターフェイス。このインターフェイスは、ルートメトリックを使用して構成されます。 DNS および NTP トラフィックは DEFAULT_GATEWAY ロールを使用します。 デフォルト値は eth0 です。	vNIC に割り当てる必要があるロールのタイプについては、表 9 : Cisco Crosswork Data Gateway のデフォルトの vNIC 展開モード（27 ページ） を参照してください。
管理	ADMINISTRATION	SSH トラフィックは、管理ロールを使用してコンソールメニューにアクセスします。 デフォルト値は eth0 です。	
外部ロギング	EXTERNAL_LOGGING	ログを送信するための外部 syslog および auditd サーバーへの接続を許可するインターフェイス。 デフォルト値は eth0 です。	
管理	MANAGEMENT	登録およびその他の管理トラフィックのための dg-manager への接続を許可するインターフェイス。 デフォルト値は eth0 です。	
Control	CONTROL		

ラベル	キー	説明	その他の情報
		宛先、デバイス、および収集の設定の収集サービスへの接続を許可するインターフェイス。 デフォルト値は eth1 です。	
NB システムデータ	NB_SYSTEM_DATA	システムの接続先は、収集サービスへの接続を許可するインターフェイスと同じ IP を共有するため、システムの接続先のノースバウンドデータは、制御ロールのインターフェイスを使用します。	
NB 外部データ	NB_EXTERNAL_DATA	ユーザーが指定した接続先への接続を許可するインターフェイス。 デフォルト値は eth1 です。	
SB データ	SB_DATA	デバイスデータを収集するための接続を許可するインターフェイス。 SB データロールのみを持つインターフェイスは、展開時に IP を必要としません。 デフォルト値は eth2 です。	
DNS サーバ			
DNS アドレス（DNS Address）*	DNS	管理インターフェイスからアクセス可能な DNS サーバーの IPv4 または IPv6 アドレスのスペース区切りリスト。	

ラベル	キー	説明	その他の情報
DNS 検索ドメイン（DNS Search Domain）*	Domain	DNSの検索ドメイン。デフォルト値は localdomain です。	
DNSセキュリティ拡張機能（DNS Security Extensions）*。	DNSSEC	オプションは、False、True、Allow-Downgrade です。 デフォルト値は False です DNSセキュリティ拡張機能を使用するには、True を選択します。	
DNS over TLS*	DNSTLS	オプションは、False、True、および Opportunistic です。 デフォルト値は False です。 DNS over TLS を使用するには、True を選択します。	
マルチキャスト DNS*	mDNS	オプションは、False、True、および Resolve です。マルチキャスト DNS を使用するには、True を選択します。 デフォルト値は False です。	Resolve を選択すると、解決サポートのみが有効になります。応答は無効になります。

ラベル	キー	説明	その他の情報
リンクローカルマルチキャスト名前解決*	LLMNR	オプションは、False、True、Opportunistic、または Resolve です。 デフォルト値は False です。 リンクローカルマルチキャスト名前解決を使用するには、True を選択します。	Resolve を選択すると、解決サポートのみが有効になります。応答は無効になります。
NTPv4サーバ			
NTPv4 サーバ（NTPv4 Servers）*	NTP	管理インターフェイスでアクセス可能な NTPv4 サーバーの IPv4、IPv6 アドレスまたはホスト名のスペース区切りリスト。	ここには、pool.ntp.org などの値を入力する必要があります。NTP サーバーは、Crosswork Data Gateway VM、Crosswork、およびデバイス間の時刻同期に不可欠です。機能しないアドレスまたはダミーアドレスを使用すると、Cisco Crosswork と Crosswork Data Gateway が相互に通信を試みる際に問題が発生する可能性があります。NTP サーバーを使用していない場合は、Crosswork Data Gateway と Crosswork 間のタイムギャップが 10 時間以下であることを確認します。そうでない場合、Crosswork Data Gateway は接続に失敗します。

ラベル	キー	説明	その他の情報
NTPv4 認証の使用（Use NTPv4 Authentication）	`NTPAuth`	NTPv4 認証を使用するには、`True` を選択します。 デフォルト値は `False` です。	
NTPv4 キー（NTPv4 Keys）	`NTPKey`	サーバーリストにマッピングするためのキー ID。キー ID のスペース区切りリストを入力します。	
NTPv4 キーファイル URI（NTPv4 Key File URI）	`NTPKeyFile`	chrony キーファイルへの SCP URI。	
NTPv4 キーファイルパスフレーズ（NTPv4 Key File Passphrase）	`NTPKeyFilePwd`	chrony キーファイルへの SCP URI のパスワード。	
リモート Syslog サーバー（Remote Syslog Server）			

ラベル	キー	説明	その他の情報
リモート Syslog サーバーの使用*	UseRemoteSyslog	オプションは True および False です。リモートホストに Syslog メッセージを送信するには、True を選択します。 デフォルト値は False です。	外部 Syslog サーバーを設定すると、サービスイベント（CLI/MDT/SNMP/gNMI）が外部 Syslog サーバーに送信されます。それ以外の場合は、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） VM にのみ記録されます。 外部 syslog サーバーを使用する場合は、次の設定を行います。 • Syslog リモートサーバーの使用（Use Remote Syslog Server） • Syslog サーバーのアドレス（Syslog Server Address） • Syslog サーバーポート（Syslog Server Port） • Syslog サーバープロトコル（Syslog Server Protocol）
Syslog サーバーのアドレス（Syslog Server Address）	SyslogAddress	管理インターフェイスでアクセス可能な Syslog サーバーのホスト名、IPv4 または IPv6 アドレス。 （注） IPv6 アドレスを使用している場合は、アドレスを角カッコ（[1::1]）で囲みます。	
Syslog サーバーポート（Syslog Server Port）	SyslogPort	Syslog サーバのポート番号。 デフォルトのポート番号は 514 です。	
Syslog サーバープロトコル（Syslog Server Protocol）	SyslogProtocol	オプションは、Syslog を送信する UDP、RELP、または TCP です。 デフォルト値は UDP です。	
Syslog マルチサーバーモード	SyslogMultiserverMode		

ラベル	キー	説明	その他の情報
		フェールオーバーまたは同時モードの複数のサーバー。このパラメータは、プロトコルが非 UDP 値に設定されている場合にのみ適用されます。UDP は同時モードを使用する必要があります。 オプションは、`Simultaneous` または `Failover` です。 デフォルト値は `Simultaneous` です。	
TLS 経由の Syslog を使用するかどうか（Use Syslog over TLS?）	`SyslogTLS`	TLS を使用して syslog のトラフィックを暗号化するには、`True` を選択します。 デフォルト値は `False` です。	
Syslog TLS ピア名（Syslog TLS Peer Name）	`SyslogPeerName`	サーバー証明書の SubjectAltName またはサブジェクト共通名に入力されたとおりの Syslog サーバーのホスト名。	
Syslog ルート証明書ファイル URI（Syslog Root Certificate File URI）	`SyslogCertChain`	SCP を使用して取得した syslog サーバの PEM形式のルート証明書。 URI ファイルを含むホストは、ネットワーク上で（SCP を介して vNIC0 インターフェイスから）到達可能でなければならず、ファイルはインストール時に存在している必要があります。	

ラベル	キー	説明	その他の情報
Syslog 証明書ファイルのパスフレーズ（Syslog Certificate File Passphrase）	SyslogCertChainPwd	Syslog 証明書チェーンを取得する SCP ユーザのパスワード。	
リモート監査サーバー			
リモート監査サーバーの使用*	UseRemoteAuditd	オプションは True および False です。デフォルト値は False です。リモートホストに auditd メッセージを送信するには、True を選択します。	必要に応じて、外部の Auditd サーバーを構成できます。Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） は、構成され、ネットワーク上に存在する場合、Auditd サーバーに監査通知を送信します。 外部の Auditd サーバを使用するには、これらの 3 つの設定を指定します。
Auditd サーバアドレス（Auditd Server Address）	AuditdAddress	オプションの Auditd サーバーのホスト名、IPv4、または IPv6 アドレス。	
監査サーバポート（Auditd Server Port）	AuditdPort	オプションの監査サーバのポート番号。 デフォルトポートは 60 です。	
コントローラとプロキシの設定			
Crosswork コントローラ IP（Crosswork Controller IP） *	ControllerIP	Cisco Crosswork クラスタの仮想 IP アドレスまたはホスト名。 （注） IPv6 アドレスを使用している場合は、角カッコ（[1 :: 1]）で囲む必要があります。	これは、Crosswork Data Gateway がインストールおよび最初の起動中に Crosswork サーバーに登録できるようにするために必要です。このステップを除外すると、証明書を手動で取り込む必要があります。詳細については、コントローラ署名証明書ファイルのインポート（129 ページ）を参照してください。

ラベル	キー	説明	その他の情報
Crosswork コントローラポート（Crosswork Controller Port）*	ControllerPort	Cisco Crosswork コントローラのポート。 デフォルトポートは 30607 です。	
コントローラ署名証明書ファイル URI*	ControllerSignCertChain	SCP を使用して取得した署名証明書を検証するための Cisco Crosswork の PEM 形式のルート証明書。Cisco Crosswork は PEM ファイルを生成し、次の場所から入手できます。 cw-admin@<Crosswork_VM_Management_VIP_Address>:/home/cw-admin/controller.pem	Crosswork Data Gateway では、コントローラ署名証明書ファイルを Cisco Crosswork に自動的に登録する必要があります。 インストール時にこれらのパラメータを指定すると、証明書ファイルは Crosswork Data Gateway の起動時に初めてインポートされます。 インストール時にこれらのパラメータを指定しない場合は、コントローラ署名証明書ファイルのインポート（129 ページ） の手順に従って証明書ファイルを手動でインポートします。
コントローラの SSL/TLS 証明書ファイル URI（Controller SSL/TLS Certificate File URI）	ControllerTlsCertChain	SCPを使用して取得した Cisco Crosswork コントローラの PEM 形式の SSL/TLS 証明書ファイル。	
コントローラ証明書ファイルのパスフレーズ*	ControllerCertChainPwd	Cisco Crosswork の証明書チェーンを取得する SCP ユーザー（cw-admin）のパスワード。	

ラベル	キー	説明	その他の情報
プロキシ サーバの URL（Proxy Server URL）	ProxyURL	HTTP プロキシサーバーの URL。	プロキシパラメータは、Crosswork Data Gateway のクラウドの導入に適用されます。 Cisco Crosswork Data Gateway は TLS 経由でインターネットに接続する必要があり、プロキシサーバーが環境に存在しない場合は、プロキシサーバーが必要になる場合があります。 プロキシサーバーを使用する場合は、これらのパラメータを指定します。
プロキシ サーバ バイパス リスト（Proxy Server Bypass List）	ProxyBypass	プロキシサーバーを使用しないアドレスとホスト名のコンマ区切りリスト。	
認証プロキシのユーザ名（Authenticated Proxy Username）	ProxyUsername	認証済みプロキシサーバのユーザ名。	
認証プロキシのパスフレーズ（Authenticated Proxy Passphrase）	ProxyPassphrase	認証済みプロキシサーバのパスフレーズ。	
HTTPS プロキシ SSL/TLS 証明書ファイル URI（HTTPS Proxy SSL/TLS Certificate File URI）	ProxyCertChain	SCP を使用して取得した HTTPS プロキシの PEM 形式の SSL/TLS 証明書ファイル。	
HTTPS プロキシ SSL/TLS 証明書ファイルのパスフレーズ（HTTPS Proxy SSL/TLS Certificate File Passphrase）	ProxyCertChainPwd	プロキシ証明書チェーンを取得する SCP ユーザのパスワード。	

vNIC ロールの割り当て

ロールを割り当てることで、インターフェイスが処理する必要のあるトラフィックを制御できます。事前に割り当てられたロールが組織の特定のニーズを満たさない場合は、ロールをインターフェイスに明示的に割り当てることができます。たとえば、インターフェイスにロール「ADMINISTRATION」を割り当てて、SSH トラフィックのみをルーティングできます。

各パラメータには、事前に定義されたロールがあります。このパラメータは、インターフェイス値を eth0、eth1、または eth2 として受け入れます。

vCenter vSphere クライアントを使用した Cisco Crosswork Data Gateway のインストール

vCenter vSphere Client を使用して Cisco Crosswork Data Gateway をインストールするには、次の手順を実行します。

（注） 手順には、Cisco Crosswork Data Gateway オンプレミスの標準展開のサンプルイメージが含まれています。

ステップ 1 Cisco Crosswork Data Gateway 5.0 イメージファイルを cisco.com（*.ova）からダウンロードします。

警告 デフォルトの VMware vCenter の展開タイムアウトは 15 分です。OVF テンプレートの入力にかかる時間が 15 分を超えると、vCenter がタイムアウトし、最初からやり直す必要があります。これを防ぐには、必要なパラメータと要件を準備しておきインストールを計画することをお勧めします。必須およびオプションのパラメータのリストについては、表 24 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ（81 ページ）を参照してください。

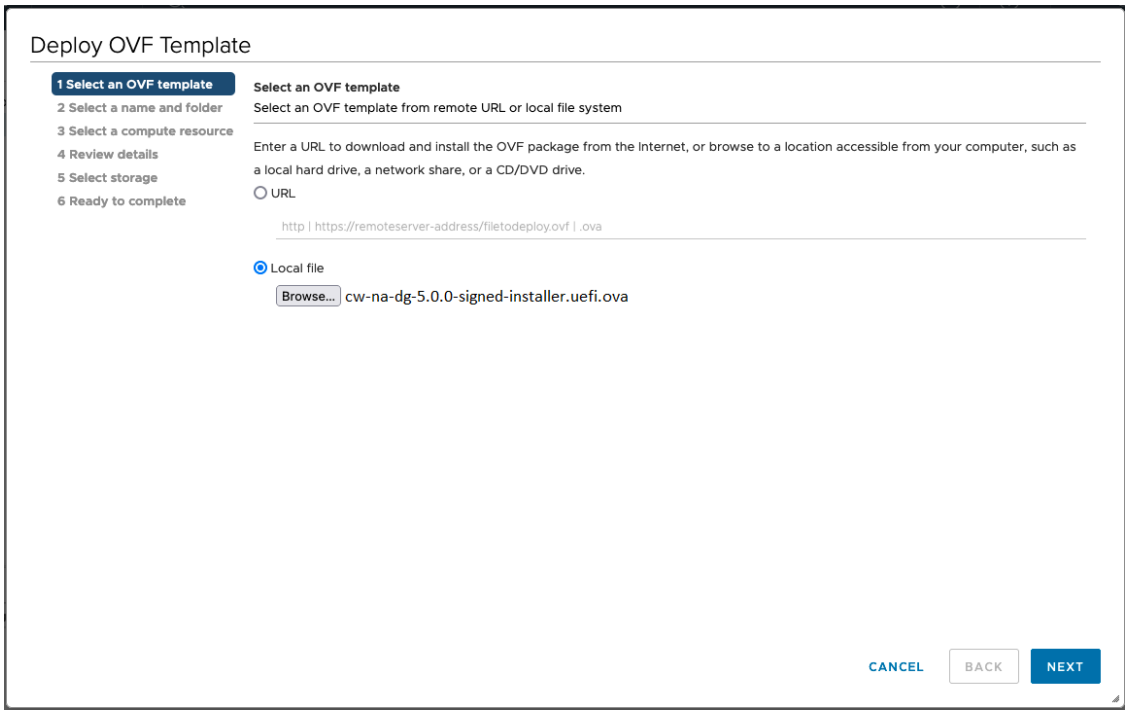
ステップ 2 vCenter vSphere Client に接続し、[アクション（Actions）] > [OVFテンプレートの展開（Deploy OVF Template）] を選択します。

ステップ 3 VMware の [OVFテンプレートの展開（Deploy OVF Template）] ウィザードが表示され、最初の手順 [1 テンプレートの選択（1 Select template）] が強調表示されます。

a) [参照（Browse）] をクリックし、OVA イメージファイルをダウンロードした場所に移動してファイルを選択します。

選択すると、ファイル名がウィンドウに表示されます。

図 *10 : [OVF*テンプレートの展開（*Deploy OVF Template*）*] - [OVF*テンプレートの選択（*Select an OVF Template*）*]* ウィンドウ

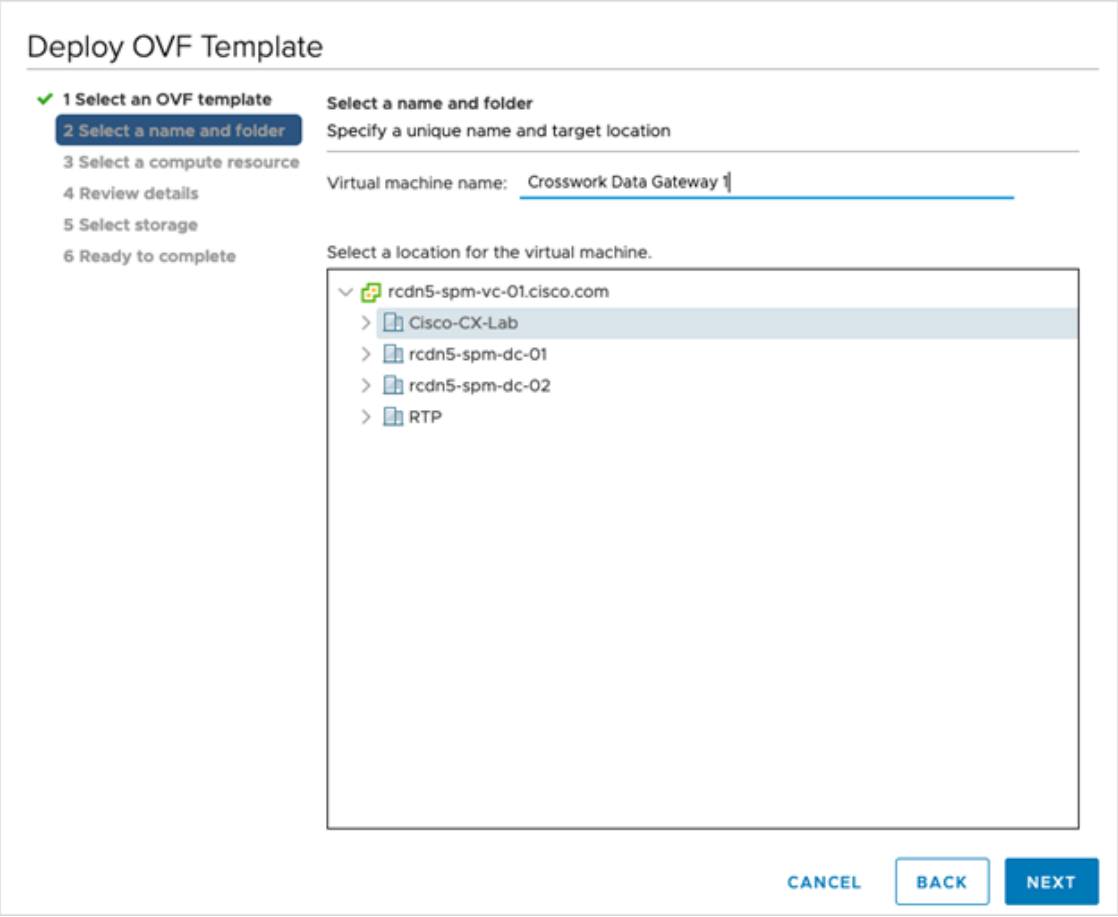


ステップ 4 次の図のように、[次へ（Next）] をクリックして、[2 名前とフォルダの選択（2 Select a name and folder）] に移動します。

a) 作成する VM の名前を入力します。

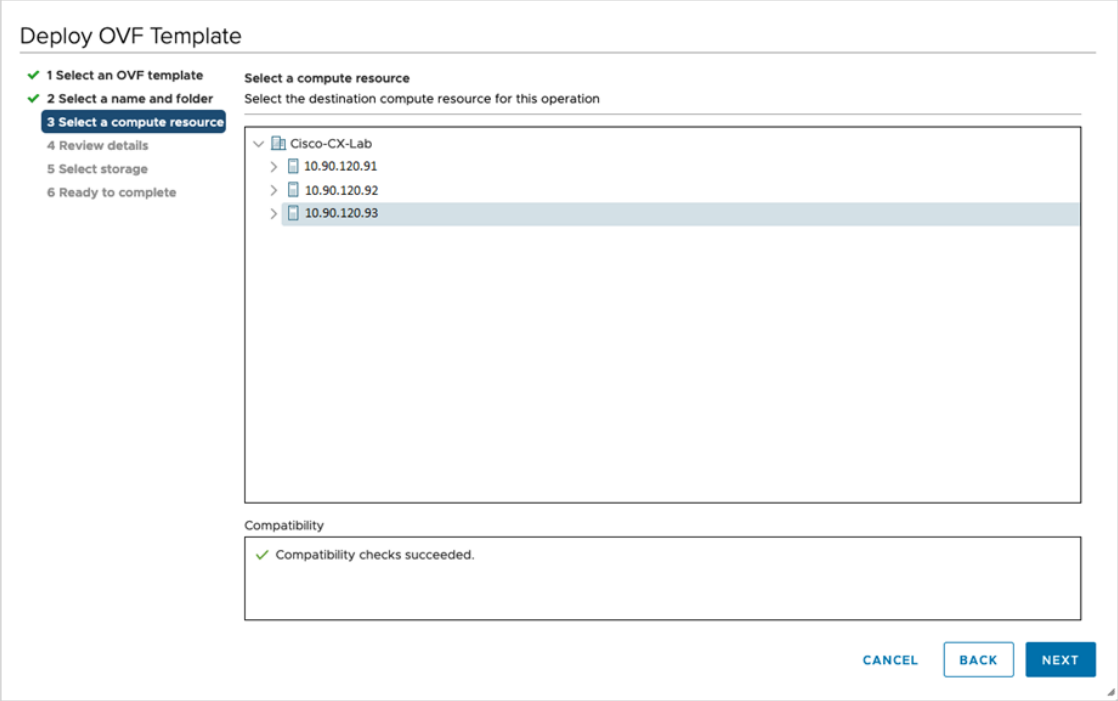
b) [仮想マシンの場所の選択（Select a location for the virtual machine）] リストで、VM を配置するデータセンターを選択します。

図 *11 : [OVF*テンプレートの展開（***Deploy OVF Template***）*] - [*名前とフォルダの選択（***Name and Folder Selection***）*]* ウィンドウ



ステップ 5 [次へ（Next）] をクリックして、[3 コンピュータリソースの選択（3 Select a computer resource）] に進みます。VM のホストを選択します。

図 *12 : [OVF*テンプレートの展開（*Deploy OVF Template*）*] - [*コンピュータリソースの選択（*Select a computer resource*）*]* ウィンドウ

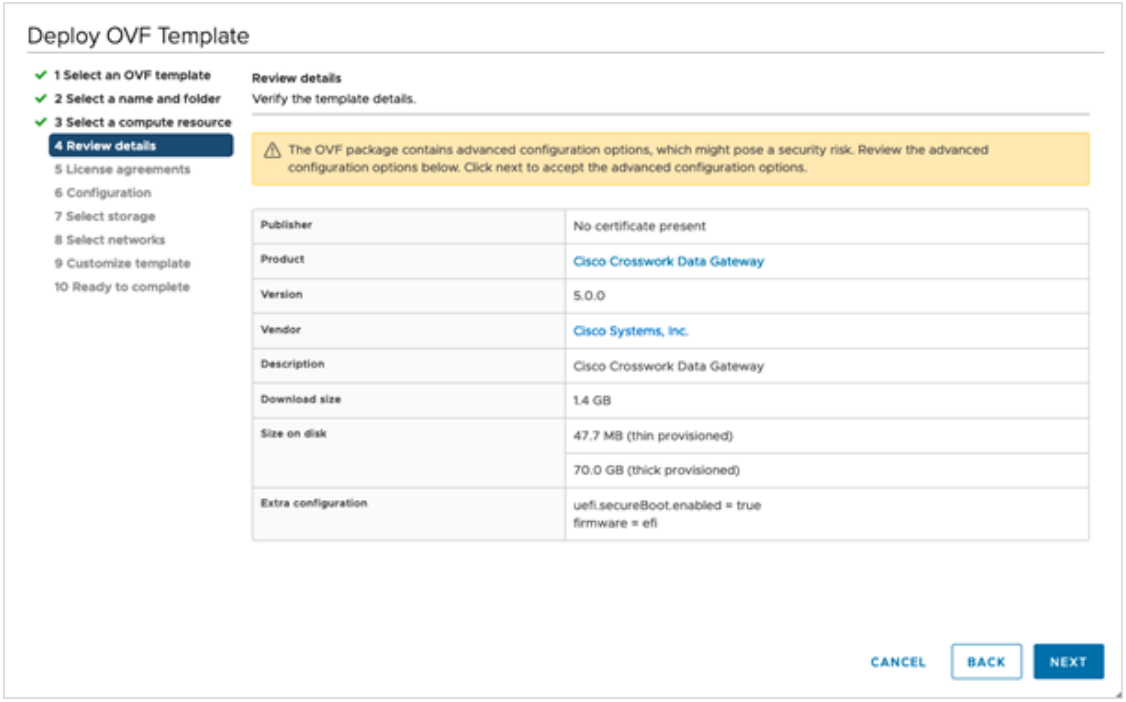


ステップ 6 [次へ（Next）] をクリックします。VMware vCenter Server が OVA を検証します。検証にかかる時間はネットワーク速度によって決まります。検証が完了すると、ウィザードは [4 詳細の確認（4 Review details）] に移動します。

展開する OVF テンプレートを確認し、[次へ（Next）] をクリックします。

（注） この情報は OVF から収集され、変更はできません。

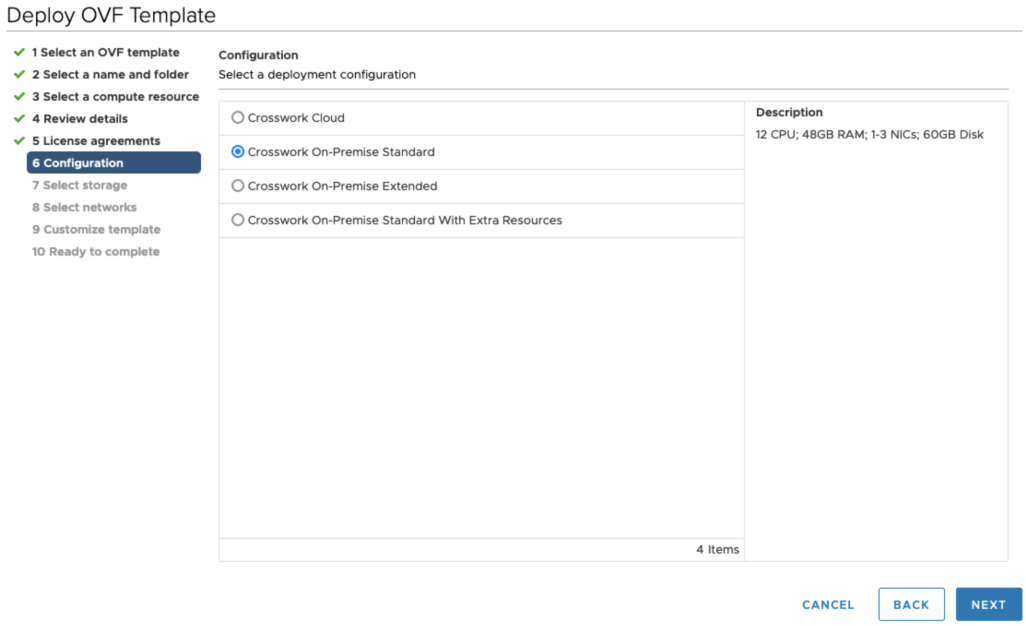
図 *13 : [OVF*テンプレートの展開（***Deploy OVF Template***）*] - [*詳細の確認（***Review details***）*]* ウィンドウ



ステップ 7 [次へ（Next）] をクリックして、[5 ライセンス契約書（5 License agreements）] に移動します。エンドユーザーライセンス契約を確認し、条件に同意する場合は [同意する（Accept）] をクリックします。条件に同意しない場合は、シスコの担当者にお問い合わせください。

ステップ 8 次の図のように、[次へ（Next）] をクリックして [6 設定（6 Configuration）] に移動します。[標準Crosswork On-Premise（Crosswork On-Premise Standard）] または [拡張Crosswork On-Premise（Crosswork On-Premise Extended）] を選択します。詳細については、Crosswork Data Gateway の展開タイプの選択 （32 ページ）を参照してください。

図 *14 : [OVF*テンプレートの展開（*Deploy OVF Template*）*] - [*設定（*Configuration*）*]* ウィンドウ



注目 Crosswork は、オンプレミス環境向けの [標準Crosswork On-Premise（Crosswork On-Premise Standard）] および [拡張Crosswork On-Premise（Crosswork On-Premise Extended）] の展開構成をサポートしています。

ステップ 9 次の図のように、[次へ（Next）] をクリックして [7 ストレージの選択（7 Select storage）] に移動します。

a) [仮想ディスク形式の選択（Select virtual disk format）] ドロップダウンリストから [シックプロビジョニング（Lazy Zeroed）（Thick provision lazy zeroed）] を選択することを推奨します。

b) [データストレージ（Datastores）] テーブルから、使用するデータストアを選択し、そのプロパティを確認して、使用可能なストレージが十分にあることを確認します。

図 *15 : [OVF*テンプレートの展開（***Deploy OVF Template***）*] - [*ストレージの選択（***Select storage***）*]* ウィンドウ

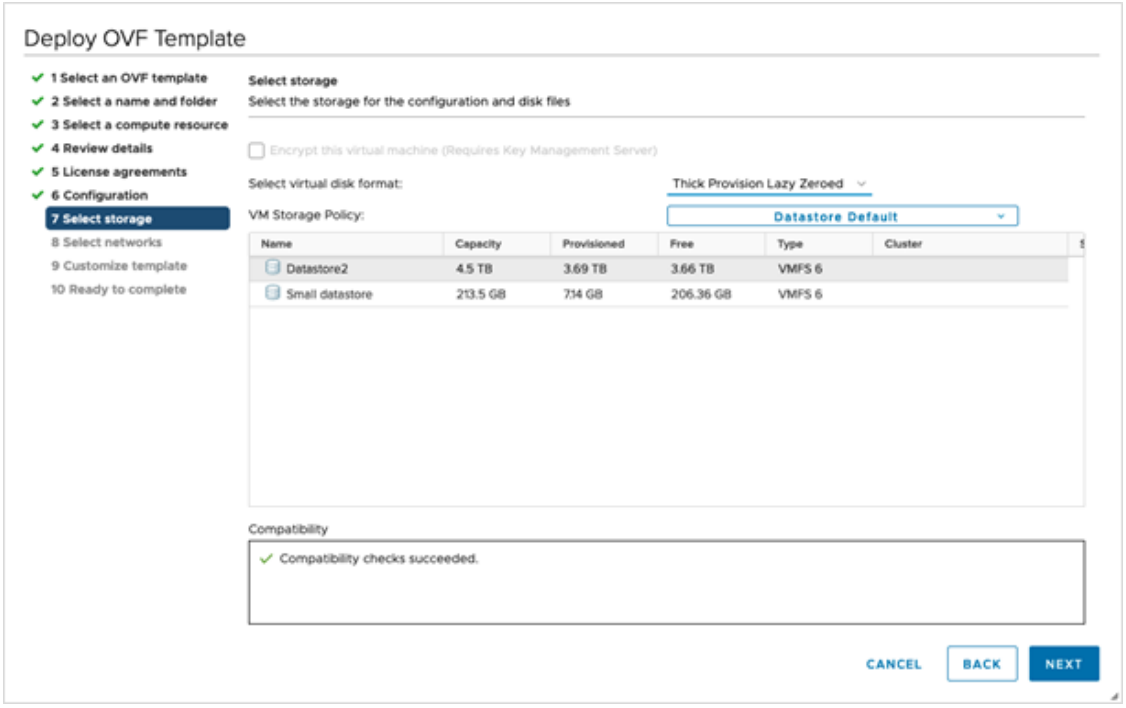
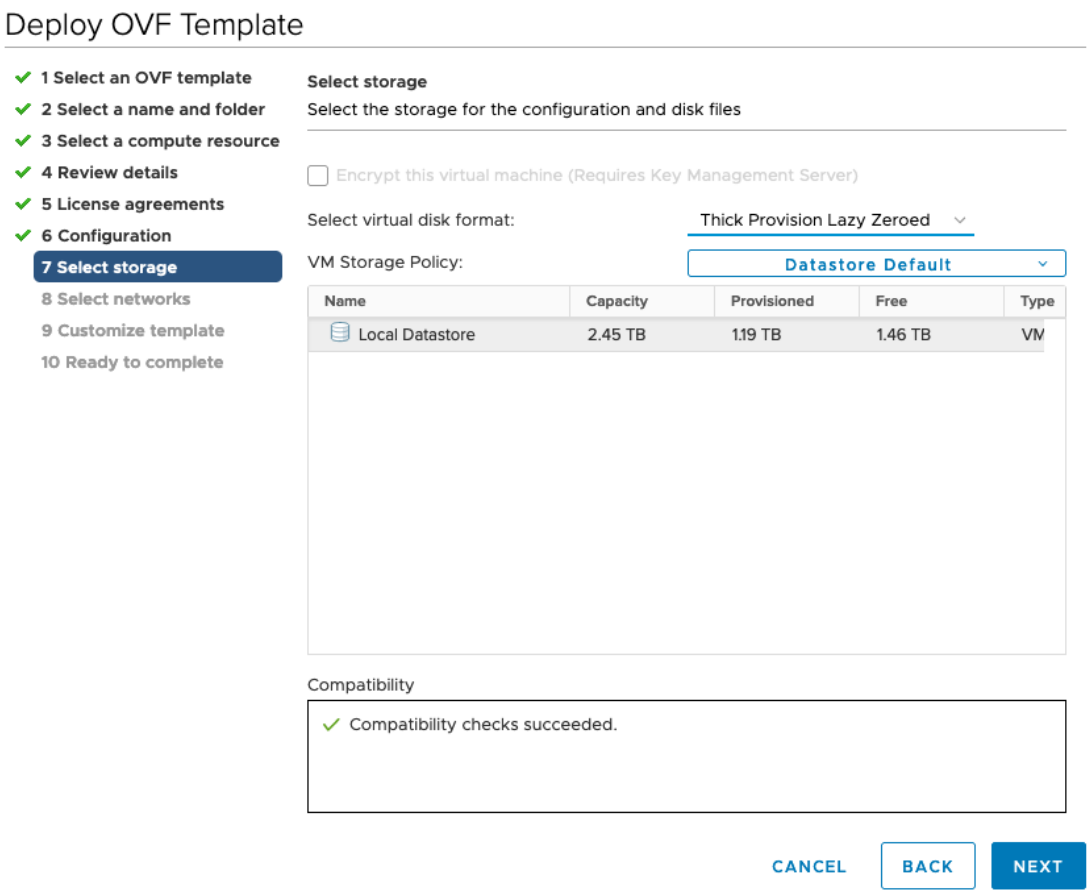
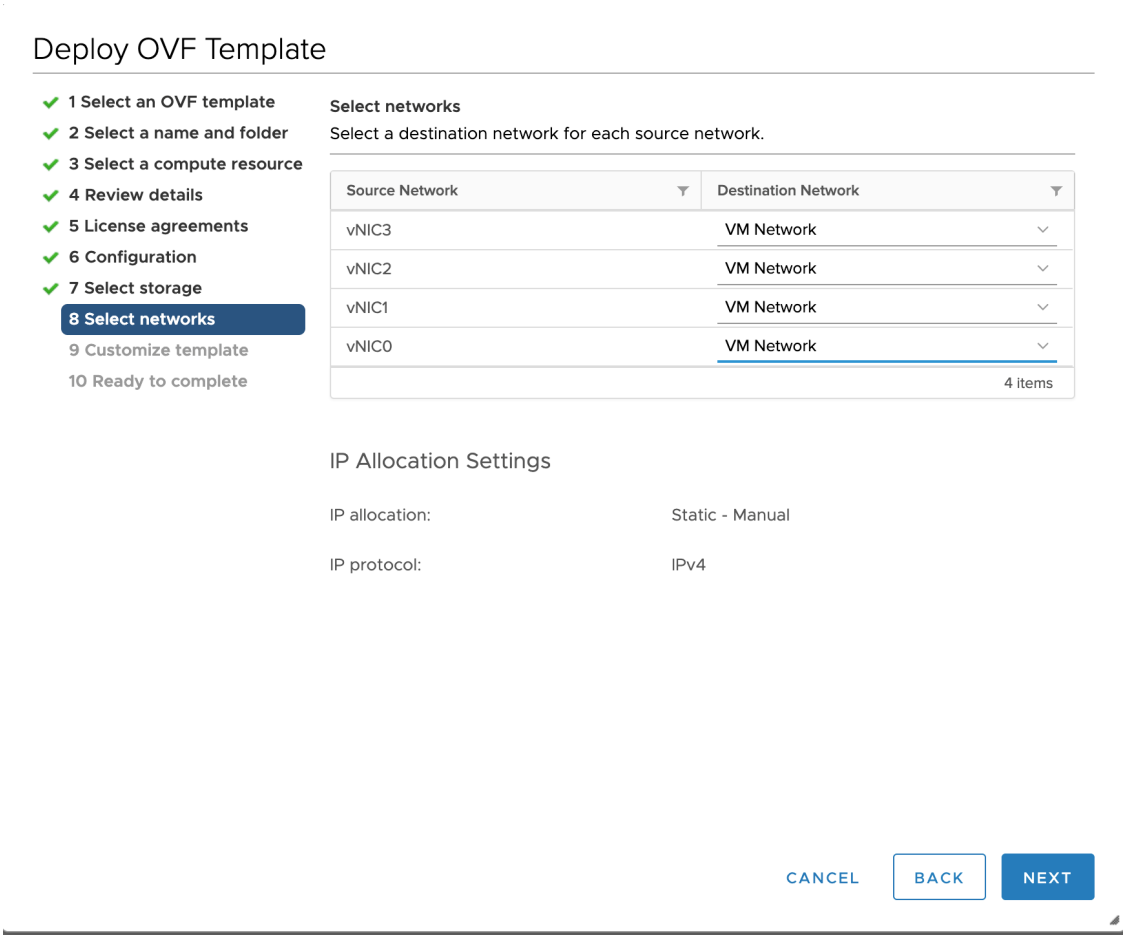


図 *16 : [OVF*テンプレートの展開（***Deploy OVF Template***）*] - [*ストレージの選択（***Select storage***）*]* ウィンドウ



ステップ 10 次の図のように、[次へ（Next）] をクリックして [8 ネットワークの選択（8 Select networks）] に移動します。ページの上部にあるドロップダウンから、各インターフェイスに適切な vNIC ロールを選択します。

図 *17 : [OVF*テンプレートの展開（*Deploy OVF Template*）*] - [*ネットワークの選択（*Select networks*）*]* ウィンドウ



注目 Crosswork は **vNIC3** ネットワークをサポートしていません。**vNIC3** の IPv4 および IPv6 アドレスを構成しないでください。

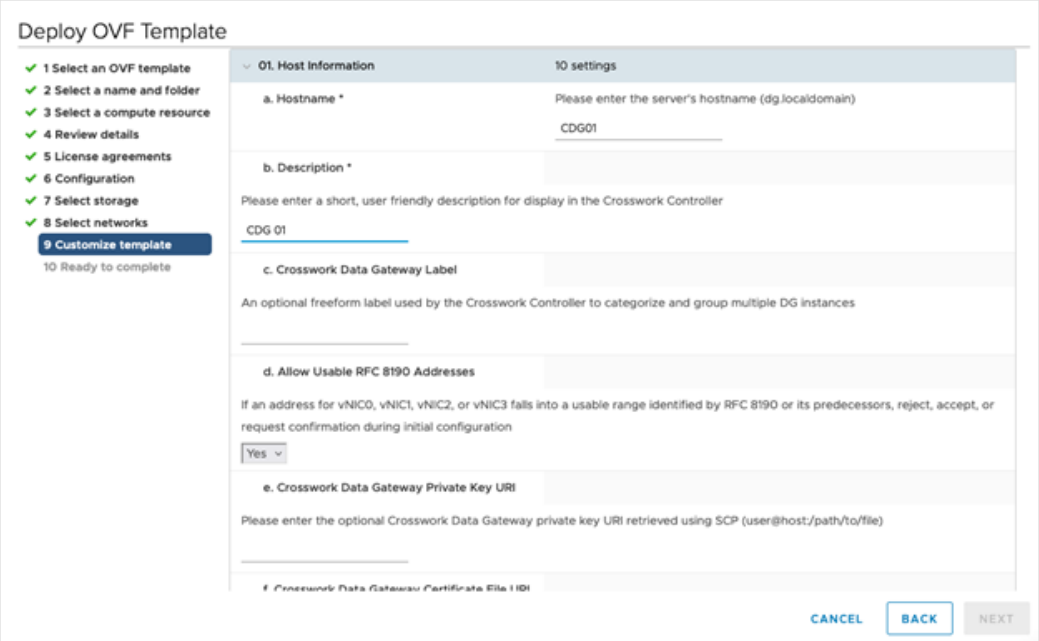
ステップ 11 [次へ（Next）] をクリックして、[ホスト情報（Host Information）] が展開された [9 テンプレートのカスタマイズ（9 Customize template）] に移動します。表 24 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （81 ページ） の説明に従って、パラメータの情報を入力します。

（注） 大規模なシステムでは、複数の Cisco Crosswork Data Gateway VM を使用する可能性があります。したがって、Cisco Crosswork Data Gateway のホスト名は一意であり、特定の VM を簡単に識別できるように作成する必要があります。

重要

- 1 つの NIC の展開では、vNIC0 のみの IP、サブネット、およびゲートウェイの値を構成します。Crosswork Data Gateway プールが作成されると、VIP アドレスが vNIC0 のセカンダリアドレスとして割り当てられます。
- 2 つおよび 3 つの NIC の展開では、vNIC0 および vNIC1 に IP、サブネット、およびゲートウェイの値が必要です。Crosswork Data Gateway プールが作成されると、VIP アドレスが vNIC1 のセカンダリアドレスとして割り当てられます。
- 3 つの NIC の展開では、Crosswork Data Gateway がプールに追加された後、VIP アドレスが vNIC2 に割り当てられます。
- プール内のスペア Crosswork Data Gateway には VIP アドレスがありません。

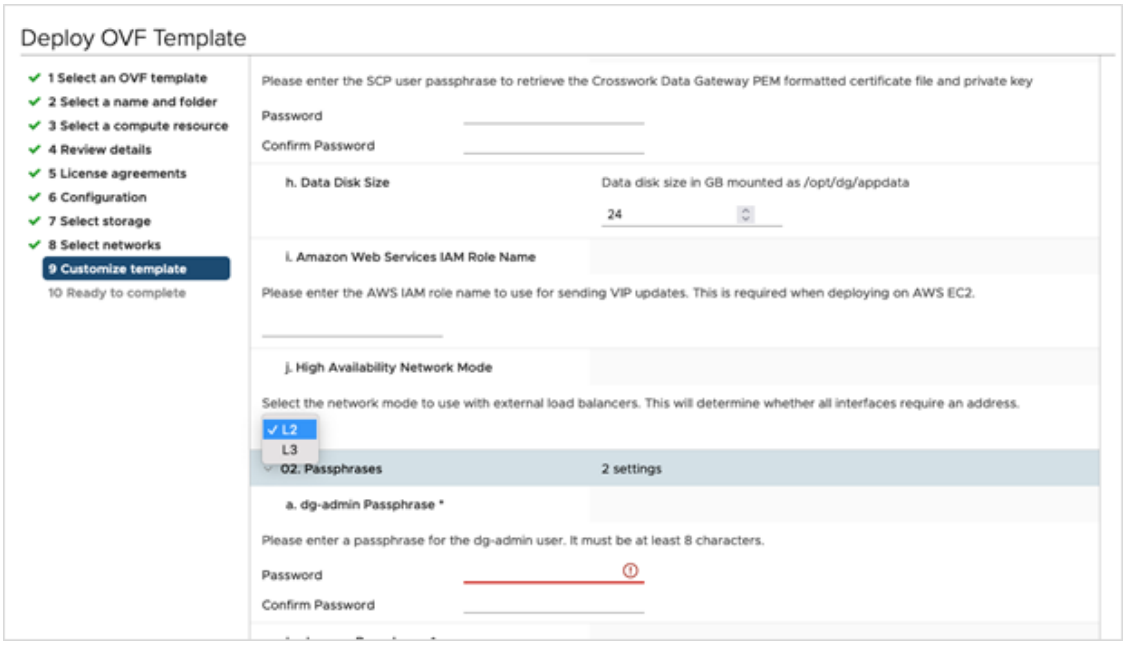
図 *18 : [OVF*テンプレートの展開（*Deploy OVF Template***）*] - [*テンプレートのカスタマイズ（***Customize template***）*] > [*ホスト情報（***Host information***）*] ウィンドウ**



Crosswork Data Gateway は、次のプールモードオプションをサポートしています。

- L2：HA プールを作成するために IP アドレスを指定することを選択した場合。
- L3：HA プールの作成とマルチサブネット展開のために FQDN を指定することを選択した場合。

図 *19 : [OVF*テンプレートの展開（***Deploy OVF Template***）*] - [*テンプレートのカスタマイズ（***Customize template***）*] > [*ホスト情報（***Host information***）*]* ウィンドウ *> [*高可用性ネットワークモード（***High Availability Network Mode***）*]*



1. 使用することを決定した NIC の数に基づいて、vNIC ロールの割り当てを構成します。

   NIC の数に基づいて、以下を参照してください。

   - [OVFテンプレートの展開（Deploy OVF Template）] - [1つのvNIC展開用のテンプレートのカスタマイズ（Customize Template for 1 vNIC deployment）] を参照してください。
   - [OVFテンプレートの展開（Deploy OVF Template）] - [2つのvNIC展開用のテンプレートのカスタマイズ（Customize Template for 2 vNICs deployment）] を参照してください。
   - [OVFテンプレートの展開（Deploy OVF Template）] - [3つのvNIC展開用のテンプレートのカスタマイズ（Customize Template for 3 vNICs deployment）] を参照してください。

図 *20 : [OVF*テンプレートの展開（*Deploy OVF Template*）*] - [1*つの*vNIC*展開用のテンプレートのカスタマイズ（*Customize Template for 1 vNIC deployment*）*]*

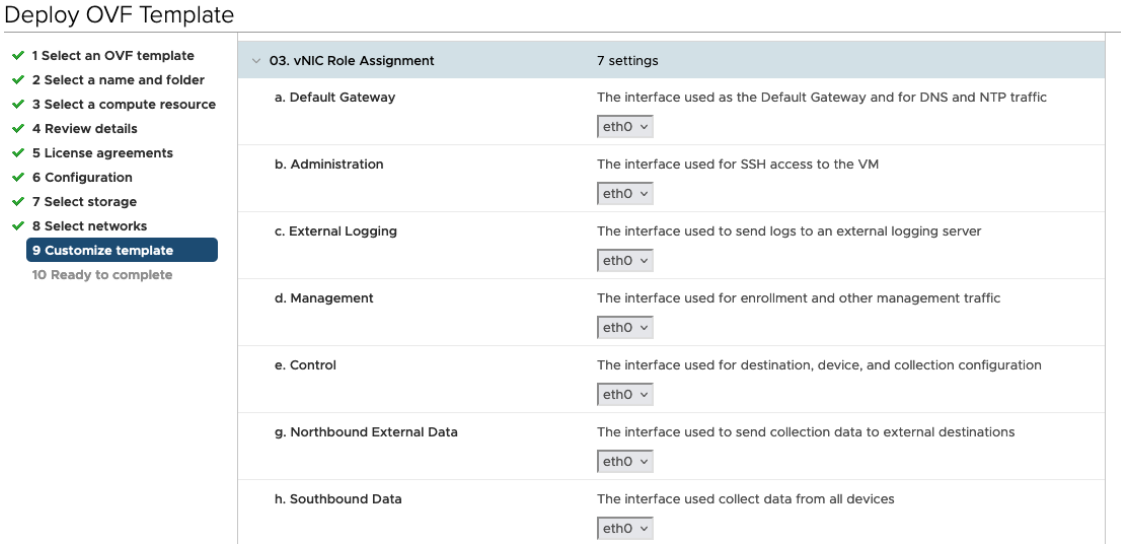
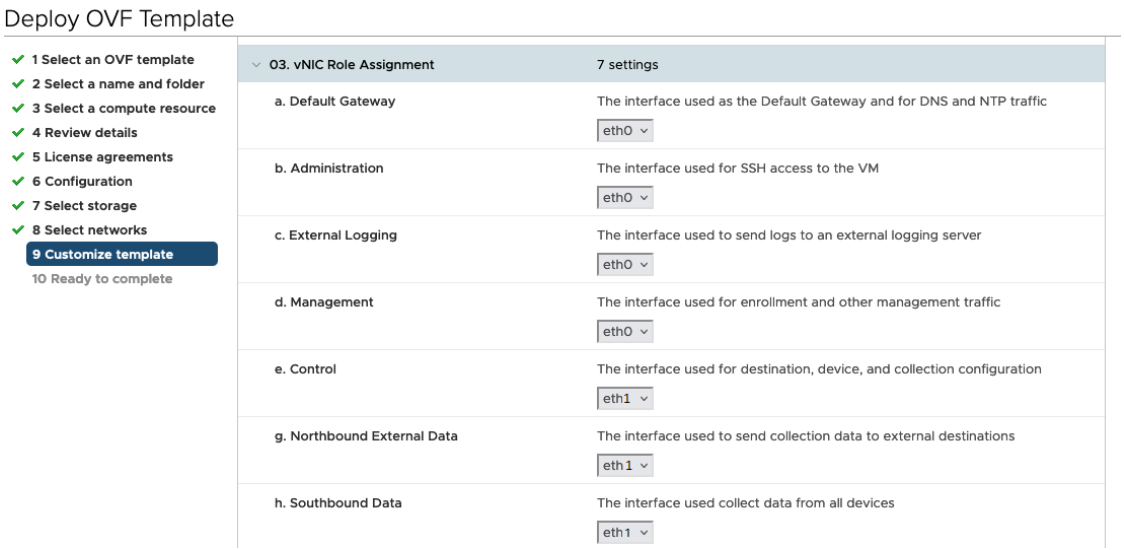
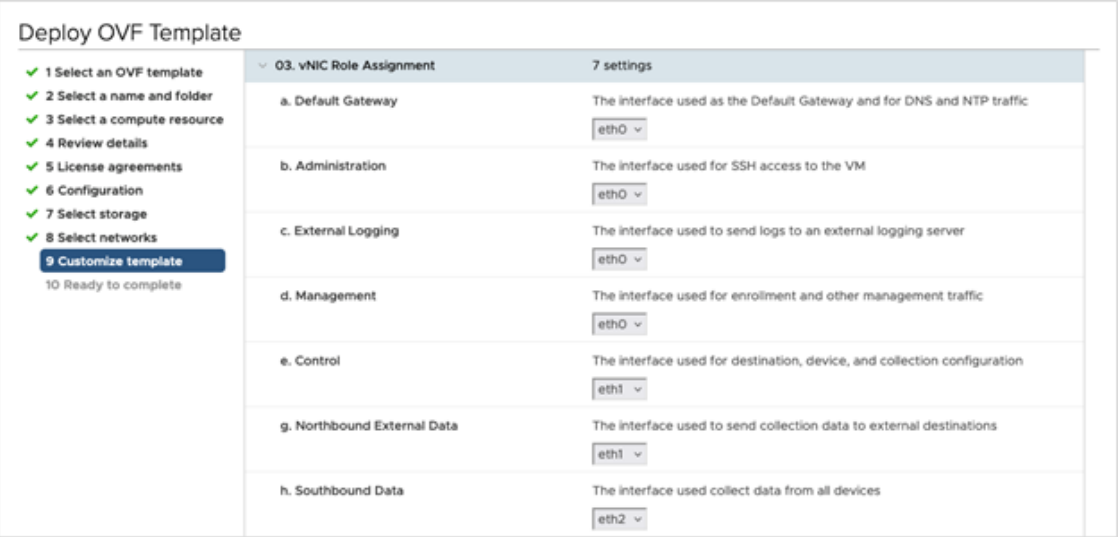


図 *21 : [OVF*テンプレートの展開（*Deploy OVF Template*）*] - [2*つの*vNIC*展開用のテンプレートのカスタマイズ（*Customize Template for 2 vNICs deployment*）*]*



3 つの vNIC の展開では、設定をデフォルト値のままにすることができます。

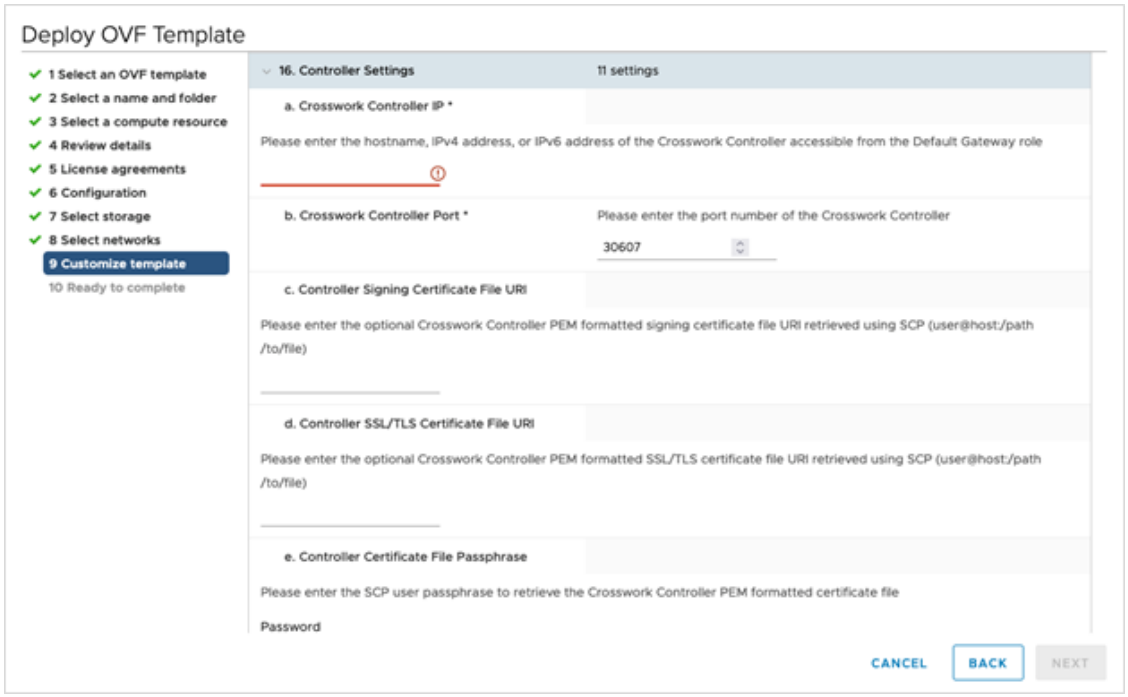
図 *22 : [OVF*テンプレートの展開（*Deploy OVF Template*）*] - [3*つの *vNIC*展開用のテンプレートのカスタマイズ（*Customize Template for 3 vNICs deployment*）*]*



注目 VMware vCenter Server 6.5、6.7 には、正しいパラメータの展開に関する問題があります。この問題を無効にするには、OVF テンプレートを展開するときに、[OVFテンプレートの展開（Deploy OVF Template）] ウィザード > [テンプレートのカスタマイズ（Customize template）] ページで、次のように構成します。

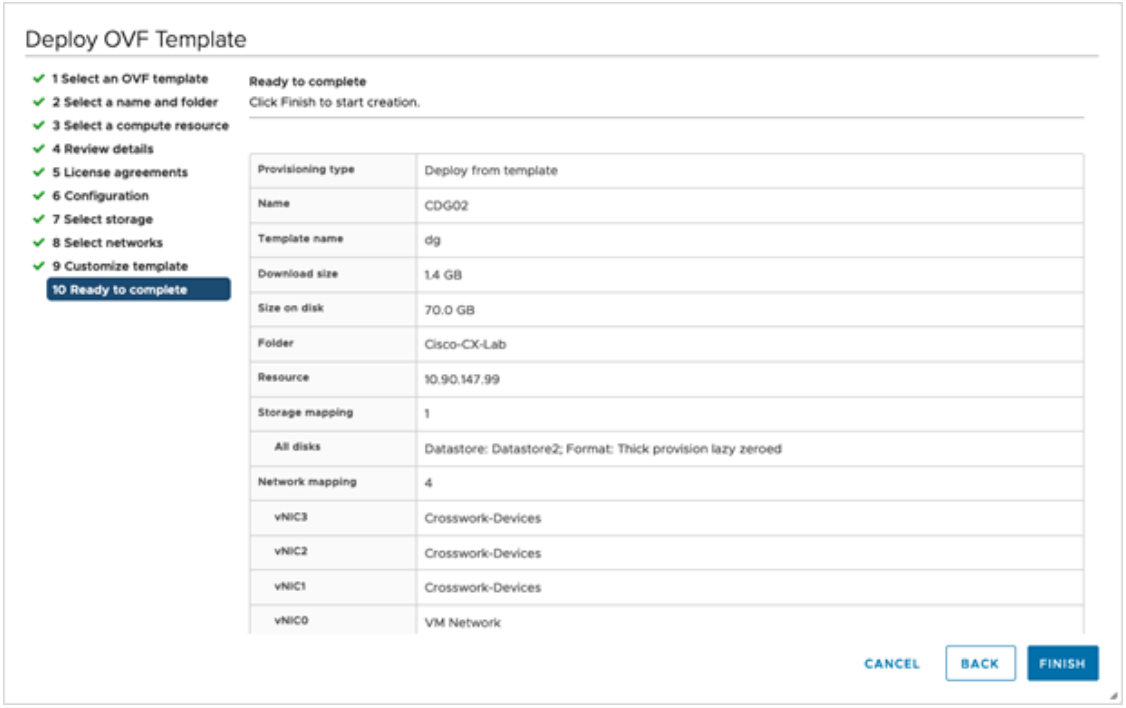
- [16. コントローラの設定（16. Controller Setting）] > [a. Crossworkコントローラ IP（a. Crosswork Controller IP）] のセクションで、DNS サーバー構成でクラスタに割り当てた DNS ホスト名のクラスタの IP アドレスを入力します。
- [16. コントローラの設定（16. Controller Setting）] > [b. Crossworkコントローラポート（b. Crosswork Controller Port）] のセクションで、ポート番号を `30607` に設定します。

図 *23 : [OVF*テンプレートの展開（***Deploy OVF Template***）*] - [*テンプレートのカスタマイズ（***Customize template***）*] > [*コントローラの設定（***Controller Settings***）*]*



ステップ 12 [次へ（Next）] をクリックして、[10 完了の準備（10 Ready to complete）] に移動します。設定を確認し、展開を開始する準備ができたら [終了（Finish）] をクリックします。

図 *24 : [OVF*テンプレートの展開（***Deploy OVF Template***）*] - [*準備完了（***Ready to Complete***）*]* ウィンドウ



ステップ 13 展開が完了するまで待ってから続行します。展開ステータスを確認するには、次の手順を実行します。

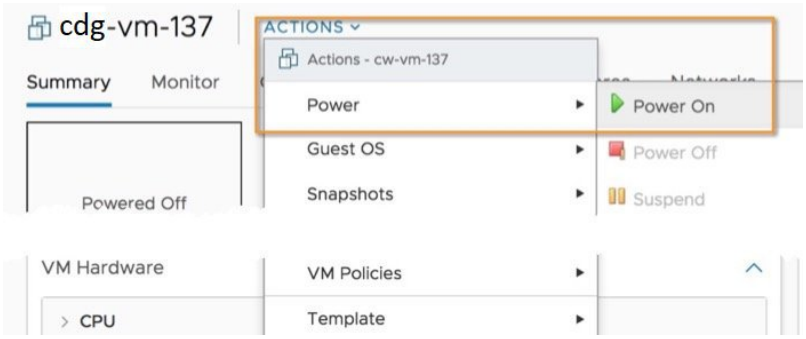
a) vCenter vSphere クライアントを開きます。

b) ホスト VM の [最近のタスク（Recent Tasks）] タブに、[OVFテンプレートの展開（Deploy OVF template）] ジョブと [OVFパッケージのインポート（Import OVF package）] ジョブのステータスを表示します。

展開ステータスが 100% になるまで待ちます。これで、VM の電源をオンにできます。

ステップ 14 展開ステータスが 100% になったら、VM の電源を入れて展開プロセスを完了します。次の図に示すように、ホストのエントリを展開して VM をクリックし、[アクション（Actions）] > [電源（Power）] > [電源オン（Power On）] の順に選択します。

図 *25 : [*電源オン（***Power On***）*]* アクション



VM が起動するまで少なくとも 5 分間待機し、次に説明するように vCenter または SSH 経由でログインします。

警告 vCenter で VM のネットワーク設定を変更すると、意図しない重大な結果になる可能性があります。これには、スタティックルートと接続の損失などが含まれます。設定は、最適なネットワークパフォーマンスを提供できるように検証されています。これらの設定を変更する場合は、自己責任で行ってください。

次のタスク

ログインすると、Crosswork Data Gateway にインストールが正常に完了したことを示すウェルカム画面とオプションメニューが表示されます。ログイン方法の詳細については、Crosswork Data Gateway VM へのログインとログアウト （120 ページ）を参照してください。

ログアウトし、次のセクションで説明するインストール後のタスクに進みます。

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）

OVF ツールを使用した Cisco Crosswork Data Gateway のインストール

要件に応じて、スクリプトの必須またはオプションのパラメータのリストを変更し、OVF ツールを実行する必要があります。インストールパラメータとそのデフォルト値のリストについては、表 24 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （81 ページ）を参照してください。

（注） このトピックで言及されているファイル名はサンプル名であり、cisco.com の実際のファイル名とは異なる場合があります。

SSH で Cisco Crosswork Data Gateway VM にログインするには、次のステップを実行します。

始める前に

- vCenter データセンターで、[ホスト（Host）] > [設定（Configure）] > [ネットワーキング（Networking）] > [仮想スイッチ（Virtual Switches）] に移動し、仮想スイッチを選択します。
- 仮想スイッチで、[編集（Edit）] > [セキュリティ（Security）] を選択し、次の DVS ポートグループプロパティを次のようにします。
  - [プロミスキャスモード（Promiscuous mode）] を [拒否（Reject）] に設定します
  - [MACアドレスの変更（MAC address changes）] を [拒否（Reject）] に設定します

設定を確認し、Crosswork Data Gateway により使用される仮想スイッチごとにこのプロセスを繰り返します。

ステップ 1 cisco.com から OVA およびサンプルスクリプトファイルをダウンロードします。これらの手順では、ファイル名 **cw-na-dg-5.0.0-45-release-20230418.uefi.ova** および **cw-na-dg-5.0.0-sample-install-scripts.tar.gz** を使用します。

ステップ 2 次のコマンドを使用して、OVA バンドルを解凍します。

```
tar -xvzf cw-na-dg-5.0.0-45-release-20230418.uefi.ova
```

ファイルバンドルの内容が新しいディレクトリに解凍されます。この新しいディレクトリには、イメージの検証に必要な OVA サンプルインストールのスクリプトとファイルが含まれています。

ステップ 3 README ファイルの内容を確認して、パッケージに含まれるコンポーネントとそれらがどのように検証されるかを理解してください。

ステップ 4 使用する展開に対応するサンプルスクリプトを選択します。シスコは、1 つ、2 つ、および 3 つの vNIC 展開用に 3 つの異なるサンプルスクリプトを提供しており、ニーズに合わせて最適化できます。

このドキュメントには、3 つの vNIC 展開用のサンプルスクリプトが含まれています。詳細については、Crosswork Data Gateway IPv4 展開のためのサンプルスクリプト （117 ページ）および Crosswork Data Gateway IPv6 展開のためのサンプルスクリプト （119 ページ）を参照してください。

ステップ 5 次のコマンドを使用して、スクリプトを実行可能にします。

```
chmod +x {filename}
```

ステップ 6 次のコマンドを使用して、OVA およびスクリプトファイルが保存されているディレクトリからスクリプトを実行します。

```
./{script name} {path and ova file name}
```

次に例を示します。

```
./three-nic /home/admin/CDG_Install/cw-na-dg-5.0.0-45-release-20230418.uefi.ova
```

ステップ 7 スクリプトで指定された値が有効な場合は、プロンプトが表示されたら、vCenter ユーザーのパスワードを入力します。

無効な値が原因でスクリプトが失敗した場合、次のようなメッセージが表示されます。

```
admin@nso-576-tsdn-410-aio:~/CDG_Install$ ./three-nic
/home/admin/CDG_Install/cw-na-dg-5.0.0-45-release-20230418.uefi.ova
Opening OVA source: /home/admin/CDG_Install/cw-na-dg-5.0.0-45-release-20230418.uefi.ova
The manifest does not validate
Warning:
- Line -1: Unsupported value 'firmware' for attribute 'key' on element 'ExtraConfig'.
- Line -1: Unsupported value 'uefi.secureBoot.enabled' for attribute 'key' on element 'ExtraConfig'.
Enter login information for target vi://rcdn5-spm-vc-01.cisco.com/
Username: johndoe
Password: ******
```

パスワードを入力したら、画面または vCenter コンソールを監視して、インストールの進行状況を確認します。たとえば、

```
Opening VI target: vi://johndoe@rcdn5-spm-vc-01.cisco.com:443/Cisco-sample-sample/host/10.10.100.10
Warning:
```

```
- Line 146: Unable to parse 'enableMPTSupport' for attribute 'key' on element 'Config'.
- Line 229: Unable to parse 'vmxnet3.noOprom' for attribute 'key' on element 'Config'.
Deploying to VI: vi://johndoe@rcdn5-spm-vc-01.cisco.com:443/Cisco-sample-sample/host/10.10.100.10
Disk progress: 65%
```

インストールが完了すると、Crosswork Data Gateway VM の電源がオンになり、スクリプトで指定した設定に基づいて自動的に構成され、Crosswork クラスタに登録されます。

次のタスク

VM にログインします。詳細については、Crosswork Data Gateway VM へのログインとログアウト（120 ページ）を参照してください。ログインすると、Crosswork Data Gateway にインストールが完了したことを示すウェルカム画面とオプションメニューが表示されます。ログアウトし、Crosswork Data Gateway インストール後のタスク（123 ページ）で説明するインストール後のタスクに進みます。

Crosswork Data Gateway IPv4 展開のためのサンプルスクリプト

次の例では、IPv4 アドレスを使用して Crosswork Data Gateway を展開します。

（注） スクリプトを実行する前に、OVFtool バージョンが 4.4.x であることを確認してください。

```
#!/usr/bin/env bash
DM="<thin/thick>"
Disclaimer="<Disclaimer>"
DNSv4="<DNS Server>"
NTP="<NTP Server>"
Domain="<Domain>"
Hostname="<CDG hostname>"

VM_NAME="<VM name on vcenter>"
DeploymentOption="<onpremise-standard/onpremise-extended>"
DS="<Datastore>"
Host="<ESXi host>"
ManagementNetwork="<vSwitch/dvSwitch>"
DataNetwork="<vSwitch/dvSwitch>"
DeviceNetwork="<vSwitch/dvSwitch>"
ManagementIPv4Address="<CDG managment IP>"
ManagementIPv4Netmask="<CDG managment mask>"
ManagementIPv4Gateway="<CDG managment gateway>"
DataIPv4Address="<CDG Data network IP>"
DataIPv4Netmask="<CDG Data network mask>"
DataIPv4Gateway="<CDG Data network gateway>"
dgadminpwd="<CDG password for dg-admin user>"
dgoperpwd="<CDG password for dg-admin user>"
ControllerIP="<CNC Managment VIP>"
ControllerPassword="<CNC Password>"
ControllerPort="30607"


ROBOT_OVA_PATH=$1

VCENTER_LOGIN="Administrator%40vsphere.local@<vCenter-IP>"
VCENTER_PATH="<vCenter-DC-NAME>/host"
```

```
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"ControllerIP=${ControllerIP}" \
--prop:"ControllerPort=${ControllerPort}" \
--prop:"ControllerSignCertChain=cw-admin@${ControllerIP}:/home/cw-admin/controller.pem"
 \
--prop:"ControllerCertChainPwd=${ControllerPassword}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"Vnic0IPv4Method=Static" \
--prop:"Vnic0IPv4Address=${ManagementIPv4Address}" \
--prop:"Vnic0IPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"Vnic0IPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$ROBOT_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

############################################################
Append section below for Two NIC deployment
############################################################
#--net:"vNIC1=${DataNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \
#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth1" \

############################################################
Append section below for three NIC deployment
############################################################
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic2IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \
#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
```

```
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \
```

Crosswork Data Gateway IPv6 展開のためのサンプルスクリプト

次の例では、IPv6 アドレスを使用して Crosswork Data Gateway を展開します。

（注） スクリプトを実行する前に、OVFtool バージョンが 4.4.x であることを確認してください。

```
#!/usr/bin/env bash
DM="<thin/thick>"
Disclaimer="<Disclaimer>"
DNSv4="<DNS Server>"
NTP="<NTP Server>"
Domain="<Domain>"
Hostname="<CDG hostname>"

VM_NAME="<VM name on vcenter>"
DeploymentOption="<onpremise-standard/onpremise-extended>"
DS="<Datastore>"
Host="<ESXi host>"
ManagementNetwork="<vSwitch/dvSwitch>"
DataNetwork="<vSwitch/dvSwitch>"
DeviceNetwork="<vSwitch/dvSwitch>"
ManagementIPv6Address="<CDG managment IP>"
ManagementIPv6Netmask="<CDG managment mask>"
ManagementIPv6Gateway="<CDG managment gateway>"
DataIPv6Address="<CDG Data network IP>"
DataIPv6Netmask="<CDG Data network mask>"
DataIPv6Gateway="<CDG Data network gateway>"
dgadminpwd="<CDG password for dg-admin user>"
dgoperpwd="<CDG password for dg-admin user>"
ControllerIP="<CNC Managment VIP>"
ControllerPassword="<CNC Password>"
ControllerPort="30607"

ROBOT_OVA_PATH=$1

VCENTER_LOGIN="Administrator%40vsphere.local@<vCenter-IP>"
VCENTER_PATH="<vCenter-DC-NAME>/host"

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"ControllerIP=${ControllerIP}" \
--prop:"ControllerPort=${ControllerPort}" \
--prop:"ControllerSignCertChain=cw-admin@${ControllerIP}:/home/cw-admin/controller.pem"
 \
--prop:"ControllerCertChainPwd=${ControllerPassword}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"Vnic0IPv6Method=Static" \
--prop:"Vnic0IPv6Address=${ManagementIPv6Address}" \
--prop:"Vnic0IPv6Gateway=${ManagementIPv6Gateway}" \
```

```
--prop:"Vnic0IPv6Netmask=${ManagementIPv6Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$ROBOT_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

############################################################
Append section below for Two NIC deployment
############################################################
#--net:"vNIC1=${DataNetwork}" \
#--prop:"Vnic1IPv6Method=Static" \
#--prop:"Vnic1IPv6Address=${DataIPv6Address}" \
#--prop:"Vnic1IPv6Gateway=${DataIPv6Gateway}" \
#--prop:"Vnic1IPv6Netmask=${DataIPv6Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth1" \

############################################################
Append section below for three NIC deployment
############################################################
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv6Method=Static" \
#--prop:"Vnic1IPv6Address=${DataIPv6Address}" \
#--prop:"Vnic1IPv6Gateway=${DataIPv6Gateway}" \
#--prop:"Vnic1IPv6Netmask=${DataIPv6Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \
```

Crosswork Data Gateway VM へのログインとログアウト

次のいずれかの方法で Crosswork Data Gateway VM にログインできます。

- SSH による Crosswork Data Gateway VM へのアクセス （121 ページ）
- vCenter を介した Crosswork Data Gateway へのアクセス （121 ページ）

Crosswork Data Gateway VM からログアウトするには、Crosswork Data Gateway VM からのログアウト （122 ページ）を参照してください。

SSH による Crosswork Data Gateway VM へのアクセス

SSH プロセスは、多数のログイン失敗後にクライアント IP をブロックすることにより、ブルートフォース攻撃から保護されます。不正なユーザ名またはパスワード、接続の切断、あるいはアルゴリズムの不一致などの失敗は、IP に対してカウントされます。20 分の時間枠内で最大 4 回失敗すると、クライアント IP は少なくとも 7 分間ブロックされます。失敗が累積し続けると、ブロックされる時間が長くなります。各クライアント IP は個別に追跡されます。

SSH で Cisco Crosswork Data Gateway VM にログインするには、次のステップを実行します。

ステップ 1 Cisco Crosswork Data Gateway の管理 IP にネットワークアクセスできるワークステーションから、次のコマンドを実行します。

ssh <username>@<ManagementNetworkIP>

ここで、**ManagementNetworkIP** は管理ネットワークの IP アドレスです。

次の例を参考にしてください。

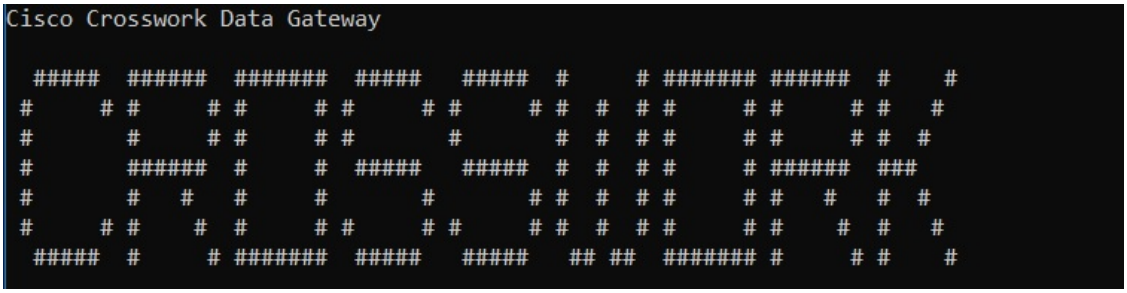
管理者ユーザーとしてログインする場合：**ssh dg-admin@<ManagementNetworkIP>**

オペレータユーザとしてログインする場合： **ssh dg-oper@<ManagementNetworkIP>**

ステップ 2 対応するパスワード（インストールプロセスで作成したパスワード）を入力し、**Enter** を押します。

Crosswork Data Gateway のフラッシュ画面が開き、パスワードの入力が求められます。

図 *26 : Crosswork* の画面



Cisco Crosswork Data Gateway VM にアクセスできない場合は、ネットワーク設定に問題があります。コンソールからネットワーク設定を確認します。正しくない場合は、Cisco Crosswork Data Gateway VM を削除し、正しいネットワーク設定で再インストールすることをお勧めします。

vCenter を介した Crosswork Data Gateway へのアクセス

vCenter 経由でログインするには、次の手順を実行します。

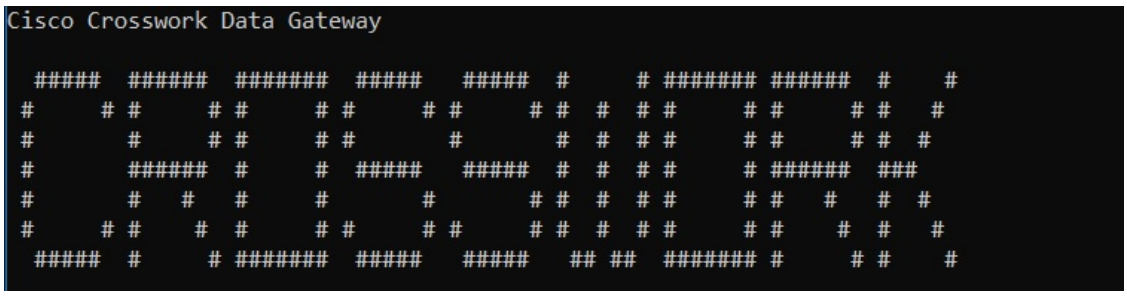
ステップ 1 vCenter で VM を右クリックし、[コンソールを開く（Open Console）] を選択します。

Crosswork Data Gateway コンソールが起動します。

ステップ 2 ユーザー名（割り当てられたロールに応じて `dg-admin` または `dg-oper`）と、対応するパスワード（インストールプロセスで作成したパスワード）を入力し、**Enter** を押します。

Crosswork Data Gateway のフラッシュ画面が開き、パスワードの入力が求められます。

図 *27 : Crosswork* の画面



Crosswork Data Gateway VM からのログアウト

ログアウトするには、メインメニューから [1 ログアウト（1 Logout）] を選択し、Enter を押すか、[OK] をクリックします。

Cisco Crosswork Data Gateway の認証と登録

Crosswork Data Gateway がインストールされると、Cisco Crosswork に対して自己識別し自動的に登録します。次に、Cisco Crosswork は新しい Crosswork Data Gateway インスタンスをデータベースでインスタンス化し、Crosswork Data Gateway VM からの「first-sign-of-life」を待機します。

接続が確立されると、Crosswork Data Gateway インスタンスはコントローラ アプリケーション（Cisco Crosswork）のアイデンティティを確認し、署名付き証明書を使用してそれ自体のアイデンティティ証明を提供します。その後、Cisco Crosswork Data Gateway は、Cisco Crosswork からコンフィギュレーション ファイルと機能イメージ（コレクションプロファイル）をダウンロードします。

Crosswork Data Gateway VM が Cisco Crosswork に正常に登録されているかどうかを確認するには、次の手順を実行します。

1. Cisco Crosswork UI にログインします。「Cisco Crosswork UI へのログイン （76 ページ）」を参照してください。
2. [Administration] > [Data Gateway Management] に移動します。

3. [Data Gatewayインスタンス（Data Gateway Instances）] タブをクリックします。

   Cisco Crosswork に正常に登録されているすべての Cisco Crosswork Data Gateway VM がここに表示されます。

Crosswork Data Gateway VM の [操作の状態（Operational State）] は [不明（Unknown）] になっています。ハンドシェイクおよびイメージのダウンロード中、ステータスは[低下（Degraded）] になっています。ハンドシェイクが完了すると、ステータスは [未準備（Not Ready）] になります。Crosswork Data Gateway VM と Cisco Crosswork の間の帯域幅によって異なりますが、通常、この操作には 5 分から 10 分程度かかります。規定の期間より長くかかる場合は、シスコ カスタマー エクスペリエンス チームに連絡してサポートを受けてください。

VM のさまざまな操作の状態に関する情報については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Overview of Cisco Crosswork Data Gateway*」のセクションを参照してください。

（注） 以前に導入準備された Cisco Crosswork Data Gateway VM の [Operational Status] が [Degraded] のままになっている場合は、調査する必要があります。シスコ カスタマーエクスペリエンス チームにお問い合わせください。

VM のさまざまな操作の状態に関する情報については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Overview of Cisco Crosswork Data Gateway*」のセクションを参照してください。

（注） [ロール（Role）] が [未割り当て（Unassigned）] の Crosswork Data Gateway VM は、使用する前にプールに割り当てる必要があります。Cisco Crosswork Data Gateway VM は、物理的な Crosswork Data Gateway です。デバイスを接続または切断することはできません。デバイスは、Cisco Crosswork Data Gateway プールにのみ接続できます。

次に行う作業：

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）

Crosswork Data Gateway インストール後のタスク

Cisco Crosswork Data Gateway をインストールしたら、Crosswork Data Gateway VM のタイムゾーンを設定します。

- Crosswork Data Gateway VM のタイムゾーンの設定 （124 ページ）

次に行う作業：

以下のインストールワークフローに戻ります。VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）

Crosswork Data Gateway VM のタイムゾーンの設定

Crosswork Data Gateway VM は、最初にデフォルトのタイムゾーン（UTC）で起動します。すべての Crosswork Data Gateway プロセス（showtech ログを含む）が、選択した場所に対応したタイムスタンプを反映するように、所在地に合わせてタイムゾーンを更新します。

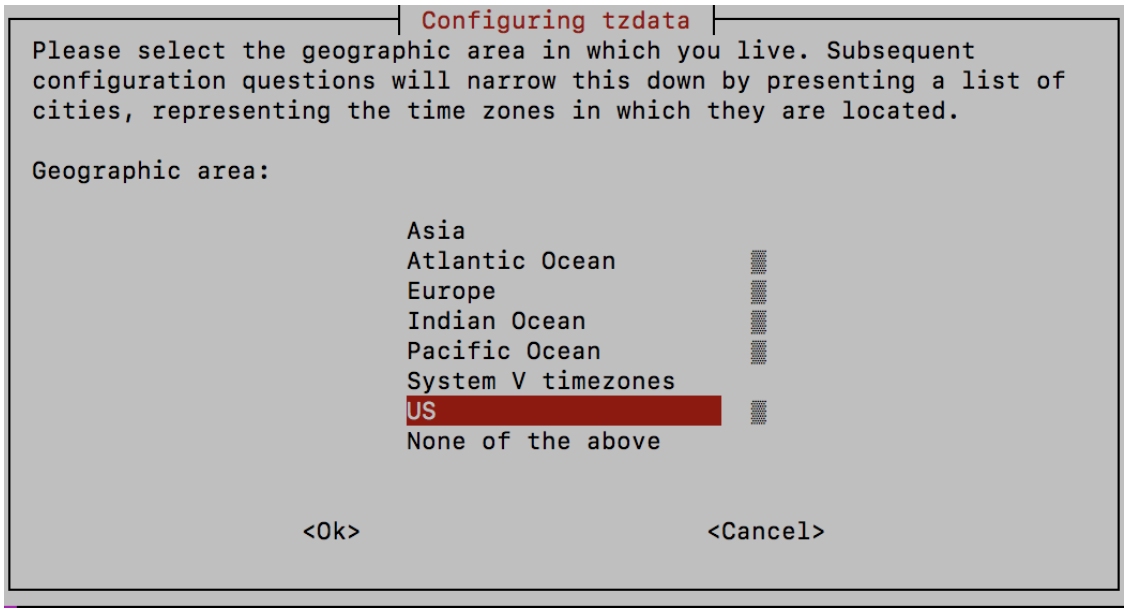
ステップ 1 Crosswork Data Gateway VM にログインします。

ステップ 2 Crosswork Data Gateway VM のインタラクティブメニューで、[3 現在のシステム設定の変更（3 Change Current System Settings）] を選択します。

ステップ 3 メニューから [9 タイムゾーン（9 Timezone）] を選択します。

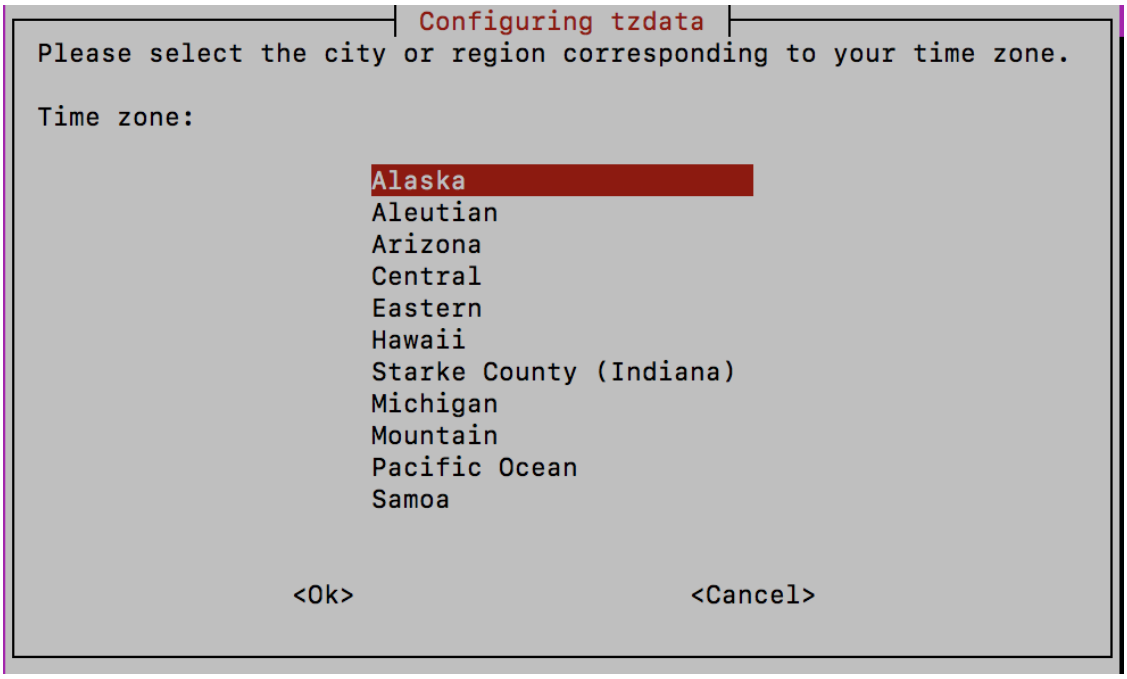
ステップ 4 居住地域を選択します。

図 28 : [タイムゾーン設定（Timezone Settings）] - [地理的エリアの選択（Geographic Area Selection）]



ステップ 5 タイムゾーンに対応する都市または地域を選択します。

図 *29* : *[*タイムゾーン設定（***Timezone Settings***）*] - [*地域の選択（***Region Selection***）*]*



ステップ 6 [OK] を選択して設定を保存します。

ステップ 7 Crosswork Data GatewayVM をリブートして、すべてのプロセスで新しいタイムゾーンが選択されるようにします。『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Reboot Crosswork Data Gateway VM*」セクションを参照してください。

ステップ 8 Crosswork Data Gateway VM からログアウトします。

Crosswork Data Gateway のインストールと登録のトラブルシューティング

Cisco Crosswork での Crosswork Data Gateway の自動登録に失敗した場合は、Crosswork Data Gateway show-tech を収集し（[メインメニュー（Main menu）] > [5トラブルシューティング（5 Troubleshooting）] > [2show-techの実行（2 Run show-tech）] を選択）、`controller-gateway` のログで理由を確認します。show-tech ログを収集する方法の詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Collect show-tech logs from the Interactive Console*」のセクションを参照してください。セッションの確立または証明書に関連する問題がある場合は、インタラクティブコンソールを使用して `controller.pem` 証明書がアップロードされていることを確認します。

重要 IPv6 アドレスを使用している場合は、角カッコ（[1 :: 1]）で囲む必要があります。

次の表に、Crosswork Data Gateway のインストール時または登録時に発生する可能性のある一般的な問題をリストし、問題の原因を特定して解決するためのアプローチを示します。

表 *25 :* インストール/登録のトラブルシューティング

問題	操作
NTP の問題により Crosswork Data Gateway を Cisco Crosswork に登録できません。つまり、2 つの間にクロックのずれがあります。 **クロックのずれは、Crosswork Data Gateway または Cisco Crosswork のいずれかで発生する可能性があります。** **また、Cisco Crosswork と Crosswork Data Gateway の NTP サーバーでは、初期時間は ESXi サーバーに設定されます。このため、ESXi サーバーにも NTP を設定する必要があります。** **ホストのクロックタイムを同期して、再試行します。**	1.Crosswork Data Gateway VM にログインします。 2. メインメニューから、[5 トラブルシューティング（5 Troubleshooting）] > [2show-techの実行（2 Run show-tech）] を選択します。 ログとバイタルを含む tarball を保存する接続先を入力し、[OK] をクリックします。 show-tech は、.tar.xz で終わるファイル拡張子で暗号化されるようになりました。 3. 次のコマンドを実行して、show-tech ファイルを復号化します。 `openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>` show-tech のログ（`/opt/dg/log/controller-gateway/session.log` にある `session.log` ファイル）に「`UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid`」というエラーが表示された場合は、Crosswork Data Gateway と Cisco Crosswork の間にクロックのずれがあります。 3. メインメニューから、[3 現在のシステム設定の変更（3 Change Current System Settings）] > [1 NTP設定（1 Configure NTP）] に移動します。 Cisco Crosswork サーバーのクロックタイムと同期するように NTP を設定し、Crosswork Data Gateway の再登録を試行します。

問題	操作
証明書エラーが原因の「バイタルを収集できませんでした（**Could not collect vitals**）」という理由で **Crosswork Data Gateway** が **10** 分以上にわたって劣化状態のままになる。	1.Crosswork Data Gateway VM にログインします。 2. メインメニューから、[5トラブルシューティング（5 Troubleshooting）] > [2show-techの実行（2 Run show-tech）] を選択します。 ログとバイタルを含む tarball を保存する接続先を入力し、[OK] をクリックします。 show-tech は、.tar.xz で終わるファイル拡張子で暗号化されるようになりました。 3. 次のコマンドを実行して、show-tech ファイルを復号化します。 `openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>` show-tech ログ（`/opt/dg/log/controller-gateway/gateway.log` にある `gateway.log` ファイル）に証明書エラーがある場合は、次の手順で説明するように、コントローラ署名証明書を再度アップロードします。 1. メインメニューから、[3現在のシステム設定の変更（3 Change Current System Settings）] > [7証明書のインポート（7 Import Certificate）] を選択します。 2. [証明書のインポート（Import Certificates）] メニューから、[1コントローラ署名証明書ファイル（1 Controller Signing Certificate File）] を選択し、[OK] をクリックします。 3. 証明書ファイルの SCP URI を入力し、[OK] をクリックします。

問題	操作
証明書エラーが原因で「gRPC接続を確立できません（gRPC connection cannot be established）」という理由で、Crosswork Data Gateway が 10 分以上にわたって劣化状態のままになる。	1. 次のステップを使用して、証明書ファイルを再アップロードします。 a. メインメニューから、[3 現在のシステム設定の変更（3 Change Current System Settings）] > [7証明書のインポート（7 Import Certificate）] を選択します。 b. [証明書のインポート（Import Certificates）] メニューから、[1 コントローラ署名証明書ファイル（1 Controller Signing Certificate File）] を選択し、[OK] をクリックします。 c. 証明書ファイルの SCP URI を入力し、[OK] をクリックします。 2. 次の手順に従って Crosswork Data Gateway VM をリブートします。 a. メインメニューから [5 トラブルシューティング（5 Troubleshooting）] を選択し、[OK] をクリックします。 b. [Troubleshooting] メニューから [4 Reboot VM] を選択し、[OK] をクリックします。 c. リブートが完了したら、Crosswork Data Gateway の動作ステータスが [稼働中（Up）] になっているかどうかを確認します。
Crosswork Data Gateway がエラー状態になる	vCenter の場合は OVF テンプレートの vNIC 値を確認します。
1 つの NIC Cisco Crosswork での Crosswork Data Gateway の登録が失敗する	vCenter の場合は OVF テンプレートの vNIC 値を確認します。1 つの NIC と 2 つの NIC の ActiveVnics プロパティが欠落している場合は、Crosswork Data Gateway はデフォルトで 3 つの NIC を展開しようとします。 このため、Crosswork Data Gateway が 1 つの NIC を予期しているが NIC が 1 つではない gateway.log 内のエラーで展開後に 1 つの NIC Cisco Crosswork での Crosswork Data Gateway の登録が失敗します。

問題	操作
Crosswork Data Gateway が拡張プロファイルの代わりに標準プロファイルを展開する	vCenter の場合は、OVF テンプレートの `Deployment` パラメータを確認します。`Deployment` パラメータが一致しないか、拡張プロファイルに存在しない場合、Crosswork Data Gateway はデフォルトで標準プロファイルを展開します。
Crosswork のアップグレード中に、一部の **Crosswork Data Gateway** がアップグレードまたは再登録されず、**dg-manager** ログに複数のエラーメッセージが記録されることがある。	Crosswork Data Gateway を再登録または再展開します。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Redeploy a Crosswork Data Gateway Instance*」のセクションと「*Reenroll Crosswork Data Gateway*」のセクションを参照してください。

以前 **Crosswork** にアタッチされていた **Crosswork Data Gateway** インスタンスが別の **Crosswork** バージョン **4.x** または **5.0** に再アタッチされた場合、インスタンスの動作状態は、**robot-astack-influxdb** エラーで **[**低下（**Degraded**）**]** になることがある。	1. SSH から Crosswork Data Gateway VM にログインします。
	2. Docker のエグゼクティブコマンドを実行して、**robot-astack-influxdb** ポッドにアクセスします。
	3. ポッドで、次のディレクトリに移動して削除します。
	`/mnt/datafs/influxdb`
	4. 次のコマンドを使用して、サービスを再起動します。
	`supervisorctl restart all`

ゲートウェイをメンテナンスモードに移行せずに **Data Gateway** を再展開すると、**Crosswork** の登録が失敗し、**dg-manager** および **controller-gateway** ログにエラーが記録される。	Data Gateway を**メンテナンス**モードに移行するか、ゲートウェイを手動で再登録します。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Reenroll Crosswork Data Gateway*」のセクションを参照してください。

コントローラ署名証明書ファイルのインポート

コントローラ証明書ファイルは、VM の起動後に自動的にインポートされます。次の理由により、この手順は手動で実行する必要があります。

- インストール時に [Controller Settings] で [Controller Signing Certificate File URI] が指定されませんでした。

- Cisco Crosswork がアップグレードまたは再インストールされたため、Cisco Crosswork で Crosswork Data Gateway を認証および登録する必要があります。

コントローラ署名証明書ファイルをインポートするには、次の手順を実行します。

ステップ 1 Cisco Crosswork Data Gateway VM のインタラクティブメニューから、[3 Change Current System Settings] を選択します。

[システム設定の変更（Change System Settings）] メニューが開きます。

ステップ 2 [7 証明書のインポート（7 Import Certificate）] を選択します。

ステップ 3 [証明書のインポート（Import Certificates）] メニューから、[1 コントローラ署名証明書ファイル（1 Controller Signing Certificate File）] を選択します。

ステップ 4 証明書ファイルの SCP URI を入力します。

URI の例を以下に示します。

```
cw-admin@{server ip}:/home/cw-admin/controller.pem
```

ステップ 5 SCP パスフレーズ（SCP ユーザーパスワード）を入力します。

証明書ファイルがインポートされます。

ステップ 6 証明書が正常にインストールされたことを確認します。コントローラ署名証明書ファイルの表示（130ページ）を参照してください。

コントローラ署名証明書ファイルの表示

次のステップを実行して署名証明書を表示します。

ステップ 1 Crosswork Data Gateway VM のインタラクティブメニューから、[2 システム設定の表示（2 Show System Settings）] を選択します。

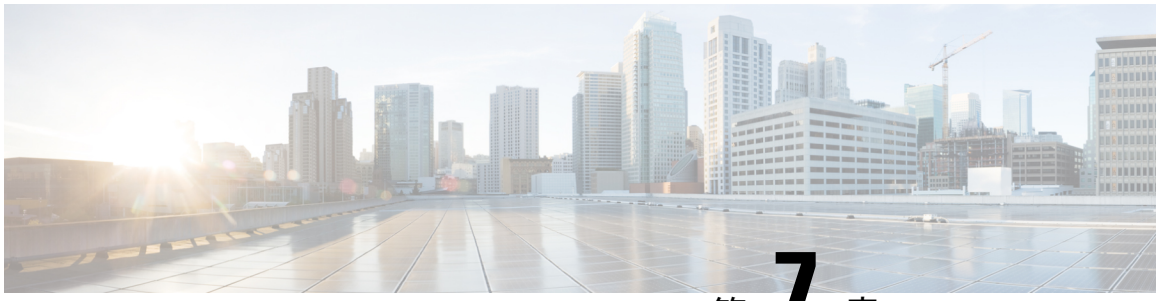
ステップ 2 [現在のシステム設定の表示（Show Current System Settings）] メニューから、[7 証明書（7 Certificates）] を選択します。

ステップ 3 [2 コントローラ署名証明書ファイル（2 Controller Signing Certificate File）] を選択します。

新しい証明書がインポートされていない場合は、Crosswork Data Gateway にデフォルトの証明書が表示されます。正常にインポートされている場合は、新しい証明書が表示されます。

第 III 部

AWS EC2 への Cisco Crosswork Network Controller のインストール



第 7 章

AWS EC2 のインストールの前提条件

この章は次のトピックで構成されています。

概要

この章では、各 Crosswork コンポーネントをインストールするための一般的な前提条件（VM 要件、ポート要件、アプリケーション要件など）およびプラットフォーム固有の前提条件について説明します。

他の統合コンポーネントまたはアプリケーション（WAE、DHCP、TFTP サーバーなど）の運用に必要なデータセンターリソースについては、このドキュメントでは取り上げていません。詳細については、各コンポーネントのインストールマニュアルを参照してください。

Amazon EC2 設定

このセクションでは、Amazon EC2 に Crosswork Network Controller をインストールする際に構成する必要がある設定について説明します。

Crosswork は、Amazon Elastic Compute Cloud（EC2）に展開できます。Amazon EC2 は、Crosswork アプリケーションをホストするためにクラウドでコンピューティングリソースを提供する Web サービスです。

Crosswork は、CloudFormation（CF）テンプレートを使用して Amazon EC2 に展開されます。CloudFormation プロセスは、クラスタを構築する手動の手順よりも高速でエラーが発生しにくいですが、クラスタの展開の詳細を含む CloudFormation テンプレートを準備するために必要なスキルを持っている必要があります。

Crosswork とそのコンポーネントを AWS 環境にインストールするには、次の前提条件を確認して満たす必要があります。

注目 このセクションで説明する要件のほとんどは AWS の概念であり、Crosswork だけが課すものではありません。

表 *26 : AWS* 前提条件と設定

要件	説明
VPC とサブネット	仮想プライベートクラウド（VPC）は、Crosswork インターフェイス（管理、データ）および Crosswork Data Gateway（管理、データ、デバイス）インターフェイスの専用サブネットで作成および構成されます。 すべてのサブネット間で直接 IP 接続が必要です。
エンドポイント	次のパラメータを使用して、VPC にエンドポイントが作成されます。 • **サービス名**：展開するリージョン（可用性ゾーン）の EC2 サービス。 • **プライベート DNS 名**：有効 • **エンドポイントタイプ**：インターフェイス • [サブネット（Subnets）] で、インストールに使用する予定の管理サブネットを指定します。Crosswork VM と Crosswork Data Gateway VM に異なる管理サブネットを使用している場合は、両方の管理サブネットを指定して、エンドポイントが両方のサブネットにアクセスできるようにしてください。 **重要** インターフェイスのサブネットは、ネットワークロードバランサ（NLB）と競合しないようにする必要があります。 エンドポイントの設定方法については、AWS のドキュメントを参照してください。
IAM ロール	Identity and Access Management（IAM）で、関連する権限ポリシーを使用してロールが作成されます。IAM ロールは、短期間有効なログイン情報を持つ、特定の権限を持つ ID です。信頼するエンティティがロールを引き受けることができます。 （注） • Crosswork ロールに必要な最小限の権限は、**ec2:DescribeNetworkInterfaces**、**ec2:AssignPrivateIpAddresses**、および **ec2:UnassignPrivateIpAddresses** です。 • ロールの信頼ポリシーには、**"Action": "sts:AssumeRole"** 条件が必要です。

要件	説明
キーペア	キーペア（VM へのログインに使用される秘密キー）が作成および構成されます。
配置グループ	クラスタ戦略の配置グループが作成されます。 クラスタ配置グループでは、インスタンスは単一の可用性ゾーンに論理的にグループ化され、ネットワーク遅延が短く、ネットワークのスループットが高いというメリットがあります。 この要件は、Crosswork クラスタインスタンスを起動する場合にのみ必要です。
IP アドレス	**Crosswork クラスタ**：単一の NIC を使用する場合、展開されるノード（ハイブリッドまたはワーカー）ごとに 1 つの IP アドレス（IPv4 または IPv6）と、仮想 IP（VIP）アドレスとして使用される 1 つの追加の IP アドレスが必要です。デュアル NIC を使用する場合（1 つは管理ネットワーク用、もう 1 つはデータネットワーク用）、展開される各ノード（ハイブリッドまたはワーカー）の管理およびデータ IP アドレス（IPv4 または IPv6）と、管理およびデータ仮想 IP（VIP）アドレスとして使用される 2 つの追加 IP アドレスが必要です。 たとえば、単一の NIC を備えた 3 つの VM クラスタの場合は 4 つの IP アドレスが必要であり、デュアル NIC を備えた 3 つの VM クラスタの場合は 8 つの IP アドレス（管理ネットワーク用に 4 つ、データネットワーク用に 4 つ）が必要です。 **Crosswork Data Gateway**：管理トラフィックとデータトラフィック専用の IP アドレス。デバイス アクセス トラフィックの IP アドレスは、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Create a Crosswork Data Gateway Pool」のセクションで説明されているように、Crosswork Data Gateway プールの作成時に割り当てられます。 • IP アドレスは、Cisco Crosswork Data Gateway がインストールされるネットワークのゲートウェイアドレスに到達できる必要があります。到達できない場合、インストールは失敗します。 • この時点では、IP の割り当ては永続的であり、再展開しない限り変更できません。詳細については、シスコ カスタマー エクスペリエンス チームにお問い合わせください。
セキュリティ グループ	許可するポートまたはトラフィックを指定するには、セキュリティグループを作成して構成する必要があります。

要件	説明
インスタンス タイプ	インスタンス展開のリソースプロファイル。AWSインスタンスタイプは、「導入の計画 （7 ページ）」に記載されている VM リソースとネットワーク要件に準拠するように選択する必要があります。 • **Crosswork クラスタ**： • デモまたはラボ用の展開には、**m5.4xlarge** を選択します。 • 実稼働の展開には **m5.8xlarge** を選択します。 • **Crosswork Data Gateway**（実稼働およびラボ用展開）： • **標準**：**m5.4xlarge** を選択 • **拡張**：**m5.8xlarge** を選択
CloudFormation（CF）テンプレート	インストール中にアップロードする必要がある Crosswork コンポーネントの CF テンプレート（.yaml）ファイル。詳細については、CF テンプレート画像の抽出 （152 ページ）を参照してください。
Route53DomainName	Route53 DNS ホストゾーン用に構成されたドメイン名。
ユーザーデータ	手動インストール手順中に指定する必要がある VM 固有のパラメータスクリプト。
ホストゾーン ID	ホストゾーン ID には、ドメイン名（Route53DomainName）を指定する必要があります。 ネットワークロードバランサ（NLB）の展開には、事前定義された Route53 ホストゾーンが必要です。

ホスト VM の要件

このセクションでは、Crosswork クラスタと Crosswork Data Gateway を展開するための VM ごとのリソース要件について説明します。

- Crosswork クラスタ VM の要件 （30 ページ）
- Crosswork Data Gateway VM の要件 （32 ページ）

Crosswork クラスタ VM の要件

Crosswork クラスタは、ハイブリッド構成で動作する 3 つの VM またはノードで構成されます。これは、標準的なネットワークでアプリケーションをサポートするために必要な最小限の設定です。必要に応じて、ネットワークの要件に合わせて、または他のアプリケーションの導入に

合わせて、後でワーカー構成に VM やノード（最大 2 つのワーカーノード）を追加して展開を拡張できます（各 Crosswork Network Controller パッケージの VM 数についての詳細は 表 2 : Crosswork Network Controller パッケージ （8 ページ） を参照）。お客様のニーズに最適な展開に関するガイダンスについては、シスコのカスタマー エクスペリエンス チームにお問い合わせください。

次の表は、VM ホストごとのネットワーク要件を説明しています。

表 *27* : ネットワーク要件（*VM* ごと）

要件	説明
ネットワーク接続	実稼働環境への展開では、管理ネットワーク用とデータネットワーク用のデュアルインターフェイスを使用することを推奨します。 最適なパフォーマンスを得るには、管理ネットワークとデータネットワークでは 10 Gbps 以上で設定されたリンクを使用する必要があります。
NTP サーバー	使用する NTP サーバーの IPv4 または IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体で Crosswork アプリケーションの VM クロック、デバイス、クライアント、およびサーバーを同期するために使用するものと同じ NTP サーバーである必要があります。 インストールを試行する前に、NTP サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。
DNS サーバー	使用する DNS サーバーの IPv4 または IPv6 アドレス。これらは、ネットワーク全体でホスト名を解決するために使用する DNS サーバーと同じである必要があります。 インストールを試みる前に、DNS サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。
DNS 検索ドメイン	DNS サーバーで使用する検索ドメイン（cisco.com など）。検索ドメインは 1 つのみ設定できます。
バックアップ サーバ	Cisco Crosswork は、SCP を使用して、システムの設定を外部サーバーにバックアップします。SCP サーバーのストレージ要件は若干異なりますが、少なくとも 50 GB のストレージが必要です。

- Cisco Crosswork インフラストラクチャおよびアプリケーションは、Kubernetes によって管理されるコンテナの分散型集合体として動作するように構築されています。コンテナの数は、アプリケーションが追加または削除されると変わります。

- Crosswork プラットフォーム インフラストラクチャでは、デュアルスタック構成はサポートされていません。したがって、環境のアドレスは**すべて** IPv4 または IPv6 のいずれかである必要があります。

Crosswork Data Gateway VM の要件

ここでは、Crosswork Data Gateway をインストールするための一般的なガイドラインと最小要件について説明します。

- Crosswork Data Gateway の展開タイプの選択 （138 ページ）
- Crosswork Data Gateway VM の要件 （138 ページ）

Crosswork Data Gateway の展開タイプの選択

次の表に、各 Crosswork 製品に Crosswork Data Gateway をインストールするために使用する必要がある展開プロファイルのリストを示します。

（注） Crosswork Data Gateway の VM リソース要件はタイプごとに異なり、変更することはできません。したがって、要件が変わった場合は、Crosswork Data Gateway を再展開して、あるタイプから別のタイプに移動する必要があります。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Redeploy a Crosswork Data Gateway VM*」のトピックを参照してください。

表 *28 : Crosswork Data Gateway* の展開タイプ

Cisco Crosswork 製品	Crosswork Data Gateway の展開
Crosswork Network Controller（Crosswork Active Topology と Crosswork Optimization Engine の組み合わせ）	オンプレミス標準
Crosswork 最適化エンジン	オンプレミス標準
Crosswork ゼロタッチプロビジョニング	オンプレミス標準
Crosswork Change Automation	オンプレミス拡張
Crosswork Health Insights	オンプレミス拡張
Crosswork Service Health	オンプレミス拡張

Crosswork Data Gateway VM の要件

Crosswork Data Gateway の VM の要件を次の表に示します。

表 *29* : オンプレミス アプリケーションの *Crosswork Data Gateway* 要件

要件	説明
データセンター	VMware 「VMware vCenter のインストールの前提条件 （21 ページ）」を参照してください。

<table>
<tr><th>要件</th><th>説明</th></tr>
<tr><td>インターフェイス</td><td>最小値：1
最大値：3
Cisco Crosswork Data Gateway は、次の組み合わせに応じて、1 つ、2 つ、および 3 つのインターフェイスのいずれかで展開できます。
（注） Crosswork クラスタで 1 つのインターフェイスを使用する場合は、Crosswork Data Gateway で 1 つのインターフェイスのみを使用する必要があります。Crosswork クラスタで 2 つのインターフェイスを使用する場合は、ネットワークの要件に応じて、Crosswork Data Gateway で 2 つまたは 3 つのインターフェイスを使用できます。
<table>
<tr><th>NIC の数</th><th>vNIC0</th><th>vNIC1</th><th>vNIC2</th></tr>
<tr><td>1</td><td>• 管理トラフィック
• 制御/データトラフィック
• デバイス アクセス トラフィック</td><td>—</td><td>—</td></tr>
<tr><td>2</td><td>管理トラフィック</td><td>• 制御/データトラフィック
• デバイスアクセストラフィック</td><td>—</td></tr>
<tr><td>3</td><td>管理トラフィック</td><td>制御/データトラフィック</td><td>デバイス アクセス トラフィック</td></tr>
</table>
</td></tr>
</table>

要件	説明
	• 管理トラフィック：インタラクティブコンソールにアクセスする場合、およびサーバー間で制御/データ情報を渡す場合に使用されます（たとえば、Crosswork アプリケーションから Crosswork Data Gateway）。 • 制御/データトラフィック：Cisco Crosswork Data Gateway と Crosswork アプリケーション、および他の外部データ接続先間でデータと設定を転送します。 • デバイス アクセス トラフィック：デバイスにアクセスする場合、およびデータを収集する場合に使用されます。 （注） セキュリティポリシーにより、他の vNIC で受信された vNIC のサブネットからのトラフィックはドロップされます。たとえば、3 vNIC モデル設定では、すべてのデバイストラフィック（着信および発信）がデフォルトの vNIC2 経由でルーティングされる必要があります。Crosswork Data Gateway は、vNIC0 および vNIC1 経由で受信されたデバイストラフィックをドロップします。
IP アドレス	使用するインターフェイスの数に基づいて、1 つまたは 2 つの IPv4/IPv6 アドレス。 仮想 IP（VIP）アドレスとして使用する 1 つの追加 IP アドレス。アクティブなデータゲートウェイごとに、一意の VIP が必要です。 詳細については、表 24 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （81 ページ）の「Interfaces」のセクションを参照してください。 （注） Crosswork はデュアルスタック構成をサポートしていません。したがって、環境のすべてのアドレスは IPv4 または IPv6 である必要があります。 3-NIC 展開では、インストール時に管理インターフェイス（vNIC0）および制御/データインターフェイス（vNIC1）の IP アドレスを指定する必要があります。デバイス アクセス トラフィック（vNIC2）の仮想 IP アドレスは、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Create a Crosswork Data Gateway Pool」のセクションで説明されているように、Crosswork Data Gateway プールの作成時に割り当てられます。

要件	説明
NTP サーバー	使用する NTP サーバーの IPv4 または IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体でデバイス、クライアント、およびサーバを同期するために使用する NTP サーバと同じでなければなりません。NTP IP アドレスまたはホスト名がネットワーク上で到達可能であることを確認します。到達可能でない場合、インストールは失敗します。 また、Crosswork アプリケーションと Cisco Crosswork Data Gateway VM を実行する ESXi ホストには NTP が設定されている必要があります。そうでない場合、最初のハンドシェイクが「certificate not valid」エラーで失敗する可能性があります。
DNS サーバー	使用する DNS サーバーの IPv4 または IPv6 アドレス。これらは、ネットワーク全体でホスト名を解決するために使用する DNS サーバーと同じである必要があります。インストールを試みる前に、DNS サーバーがネットワーク上で到達可能であることを確認します。サーバーに到達できない場合、インストールは失敗します。
DNS 検索ドメイン	DNS サーバーで使用する検索ドメイン（cisco.com など）。検索ドメインは 1 つのみ設定できます。

TCP および UDP ポートの要件

Crosswork クラスタポートの要件

次の TCP および UDP のポート番号は、データセンター管理者が展開した外部ファイアウォールまたはアクセスリストのルールを通過できるようにする必要があります。NIC の展開によっては、これらのポートが一方のみの、または両方の NIC に適用される場合があります。

（注） Crosswork クラスタポートにより、双方向の情報フローが可能になります。

表 *30 : Crosswork* クラスタが使用する外部ポート

ポート	プロトコル	用途
22	TCP	リモート SSH トラフィック
111	TCP/UDP	GlusterFS（ポートマッパー）
179	TCP	Calico BGP（Kubernetes）
80、443	TCP	EC2 API へのアクセス。

ポート	プロトコル	用途
500	UDP	IPSec
2379/2380	TCP	Kubernetes etcd
4500	UDP	IPSec
6443	TCP	kube-apiserver（Kubernetes）
9100	TCP	Kubernetes メタモニターリング
10250	TCP	kubelet（Kubernetes）
24007	TCP	GlusterFS
30603	TCP	ユーザーインターフェイス（NGINX サーバーはポート 443 でセキュア接続をリッスンします）
30606	TCP	Docker レジストリ
30621	TCP	FTP 用（データインターフェイスでのみ使用可能）。ファイル転送に使用される追加ポートは、31121（TCP）、31122（TCP）、および 31123（TCP）です。 このポートは、サポート対象アプリケーションが Cisco Crosswork にインストールされ、FTP 設定が有効になっている場合にのみ使用できます。
30622	TCP	SFTP 用（データインターフェイスでのみ使用可能）。 このポートは、サポート対象アプリケーションが Cisco Crosswork にインストールされ、SFTP 設定が有効になっている場合にのみ使用できます。
49152:49370	TCP	GlusterFS

表 *31* : 他の *Crosswork* コンポーネントが使用するポート

ポート	プロトコル	用途
30602	TCP	インストールのモニタリング用（Crosswork Network Controller）
30603	TCP	Crosswork Network Controller Web ユーザーインターフェイス（NGINX サーバーはポート 443 でセキュア接続をリッスンします）
30604	TCP	NGINX サーバーのクラシック ゼロ タッチ プロビジョニング（クラシック ZTP）に使用されます。

ポート	プロトコル	用途
30607	TCP	Crosswork Data Gateway のバイタルコレクション
30608	TCP	Data Gateway VM を使用した Data Gateway gRPC チャネル
30609	TCP	Expression Orchestrator（Crosswork Service Health）によって使用されます。
30610	TCP	Metric Scheduler（Crosswork Service Health）によって使用されます。
30611	TCP	Expression Tracker コンポーネント（Crosswork Service Health）によって使用されます。
30617	TCP	ZTP サーバーのセキュア ゼロ タッチ プロビジョニング（セキュア ZTP）に使用されます。
30620	TCP	ZTP サーバーでプラグアンドプレイ HTTP トラフィックを受信するために使用されます。
30649	TCP	Crosswork Data Gateway の収集ステータスを設定およびモニターします。
30650	TCP	Data Gateway VM で実行されている astack-client を含む astack gRPC チャネル
30993、30994、30995	TCP	収集されたデータを Crosswork Kafka の接続先に送信する Crosswork Data Gateway。

表 *32 : Crosswork* クラスタが使用する宛先ポート

ポート	プロトコル	用途
7	TCP/UDP	ICMP を使用したエンドポイントの検出。
22	TCP	管理対象デバイスとの SSH 接続の開始。
53	TCP/UDP	DNS への接続
123	UDP	ネットワーク タイム プロトコル（NTP）
830	TCP	NETCONF の開始
2022	TCP	Crosswork と Cisco NSO 間の通信に使用されます（NETCONF の場合）。
8080	TCP	REST API から SR-PCE へ

ポート	プロトコル	用途
8888	TCP	Crosswork と Cisco NSO 間の通信に使用されます（HTTPS の場合）。
20243	TCP	DLM と Cisco NSO 間の通信用に DLM 機能パックによって使用されます。
20244	TCP	Cisco NSO でパッケージのリロードシナリオ中に DLM 機能パックリスナーを内部的に管理するために使用されます。

Crosswork Data Gateway ポート要件

次の表に、Crosswork Data Gateway が正常に動作するために必要なポートの最小セットを示します。

インバウンド：Crosswork Data Gateway は指定されたポートでリッスンします。

アウトバウンド：Crosswork Data Gateway は、指定されたポートの外部宛先 IP に接続します。

表 *33* : 管理トラフィック用に開くポート

ポート	プロトコル	用途	方向
22	TCP	SSH サーバ	着信
22	TCP	SCP クライアント	発信
123	UDP	NTP クライアント	発信
53	UDP	DNS Client	発信
30607	TCP	Crosswork コントローラ	発信

（注） SCP ポートは調整できます。

表 *34* : デバイス アクセス トラフィック用に開くポート

ポート	プロトコル	用途	方向
161	UDP	SNMP コレクタ	発信

ポート	プロトコル	用途	方向
1062	UDP	SNMP トラップコレクタ （注） これはデフォルト値です。この値は、インストール後に Cisco Crosswork UI から変更できます。詳細については「Configure Crosswork Data Gateway Global Parameters」を参照してください。	着信
9010	TCP	MDT コレクタ	着信
22	TCP	CLI コレクタ	発信
6514	TLS	syslog コレクタ これはデフォルト値です。この値は、インストール後に Cisco Crosswork UI から変更できます。詳細については「Configure Crosswork Data Gateway Global Parameters」を参照してください。	着信
9898	TCP		
9514	UDP		

ポート	プロトコル	用途	方向
サイト特定 デフォルトポートは、ベンダーによって XR、XE とは異なります。プラットフォーム固有のマニュアルを確認します。	TCP	gNMI コレクタ	発信

表 *35 :* 制御/データトラフィック用に開くポート

ポート	プロトコル	用途	方向
30649	TCP	Crosswork コントローラ	発信
30993 30994 30995	TCP	Crosswork Kafka	発信
サイト特定	サイト特定	Kafka と gRPC の接続先	発信

IP アドレスの制限

Crosswork クラスタでは、内部通信に次の IP 範囲が使用されます。これは変更できません。そのため、これらのサブネットは、ネットワーク内のデバイスやその他の目的のために使用できません。

Crosswork クラスタを分離して、すべての通信がクラスタ内にとどまるようにすることをお勧めします。また、アドレス空間が、外部統合ポイント（デバイスへの接続、Crosswork がデータを送信する先の外部サーバーへの接続、NSO サーバーへの接続など）と重複していないことも確認してください。

（注） これは、クラスタのインストールとスタティックルートの追加に適用されます。

表 *36 :* 保護された *IP* サブネット

IP タイプ	サブネット	備考
IPv4	172.17.0.0/16	Docker サブネット（インフラストラクチャ）
	169.254.0.0/16	リンク ローカル アドレス ブロック
	127.0.0.0/8	ループバックアドレス
	192.88.99.0/24	予約済み。以前はリレーサーバーが IPv6 over IPv4 を実行するために使用されました
	240.0.0.0/4	将来の使用のために予約済み（以前はクラス E ブロック）
	224.0.0.0/4	MCAST-TEST-NET
	0.0.0.0/8	現在のネットワーク、送信元アドレスとしてのみ有効
IPv6	2001:db8:1::/64	Docker サブネット（インフラストラクチャ）
	fdfb:85ef:26ff::/48	ポッドサブネット（インフラストラクチャ）
	fd08:2eef:c2ee::/110	サービスサブネット（インフラストラクチャ）
	::1/128	ループバックアドレス
	fe80::/10	リンク ローカル
	ff00::/8	IPv6 マルチキャスト
	2002::/16	予約済み。以前はリレーサーバーが IPv6 over IPv4 を実行するために使用されました
	2001:0000::/32	Terredo トンネルとリレー
	2001:20::/28	ORCHID で使用され、IPv6 ではルーティング不可です
	100::/64	破棄プレフィックス。Crosswork ゼロタッチプロビジョニングに適用されない特定のユースケースで使用されます
	::/128	未指定のアドレス。ホストに割り当てることはできません
	::ffff:0:0/96	IPv4 マッピングされたアドレス
	::ffff:0:0:0/96	IPv4 変換されたアドレス

サポートされる Web ブラウザ

インフラストラクチャのインストール後に Crosswork UI にアクセスするには、検証済みのブラウザのいずれかを使用することをお勧めします。

表 *37* : サポートされる *Web* ブラウザ

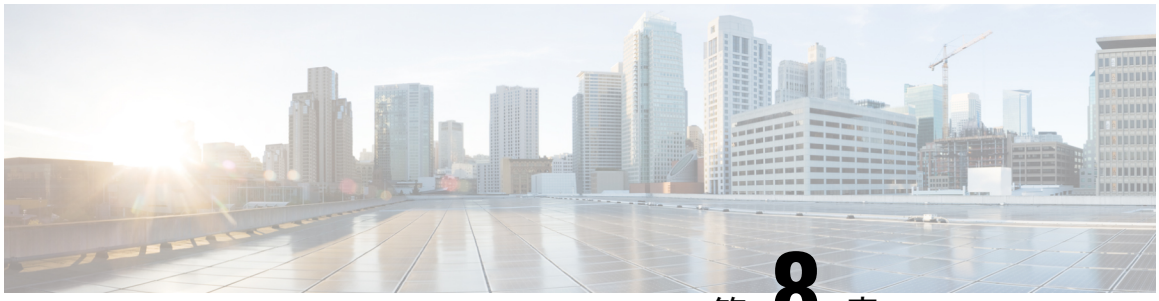
ブラウザ	バージョン
Google Chrome （推奨）	92 以降
Mozilla Firefox	70 以降

推奨される表示解像度は 1600 x 900 ピクセル以上（最小：1366 x 768）です。

サポートされているブラウザを使用することに加えて、Crosswork アプリケーション内の地理的マップにアクセスするすべてのクライアントデスクトップは、mapbox.com のサイトにアクセスできる必要があります。Cisco Crosswork が外部サイトにアクセスすることを望まないお客様は、マップファイルをローカルにインストールすることを選択できます。

次に行う作業：

以下のインストールワークフローに戻ります。AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）



第 8 章

AWS EC2 への Cisco Crosswork Network Controller のインストール

この章は次のトピックで構成されています。

インストールの概要

このセクションでは、Amazon EC2 に Cisco Crosswork をインストールする方法の概要を説明します。

Cisco Crosswork は、CloudFormation（CF）テンプレートを使用してクラスタスタックを展開します。CF プロセスは、クラスタを構築する手動の手順よりも高速でエラーが発生しにくいですが、クラスタの展開の詳細を含む CF テンプレートを準備するために必要なスキルを持っている必要があります。

（注） 「スタック」と「インスタンス」という用語は、それぞれクラスタと VM を指します。

重要 提供される CF テンプレート（.yaml ファイル）はサンプルであり、本番環境設定に従ってカスタマイズし、この章で説明するステップに従って実行する必要があります。

CF テンプレート画像の抽出

このセクションでは、Cisco Crosswork CF テンプレートイメージを抽出して検証する手順について説明します。

注目 このトピックで言及されているファイル名はサンプル名であり、リリースバージョンの実際のファイル名とは異なる場合があります。

ステップ 1 CF テンプレートパッケージ（**cw-na-platform-cft-5.0.0-signed.tar.gz**）をダウンロードします。

ステップ 2 次のコマンドを使用して、パッケージを解凍します。

```
tar -xzvf cw-na-platform-cft-5.0.0-signed.tar.gz
```

パッケージの内容が新しいディレクトリに解凍されます。この新しいディレクトリには、CFテンプレートイメージと、イメージの検証に必要なファイルが含まれています。

次に例を示します。

```
tar -xzvf cw-na-platform-cft-5.0.0-signed.tar.gz
x CFT-5.0.0_release500_2.tar.gz
x CFT-5.0.0_release500_2.tar.gz.signature
x README
x CW-CCO_RELEASE.cer
x cisco_x509_verify_release.py3
x cisco_x509_verify_release.py
```

ステップ 3 README ファイルに目を通して、パッケージの内容、および次の手順による検証方法を理解します。

ステップ 4 前の手順で作成したディレクトリに移動し、次のコマンドを使用してインストーライメージの署名を確認します。

（注） `python --version` を使用して、マシンの Python バージョンを確認します。

Python 2.x を使用している場合は、次のコマンドを使用してファイルを検証します。

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Python 3.x を使用している場合は、次のコマンドを使用してファイルを検証します。

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

次に例を示します。

```
python cisco_x509_verify_release.py3 -e CW-CCO_RELEASE.cer -i CFT-5.0.0_release450_2.tar.gz -s
CFT-5.0.0_release450_2.tar.gz.signature -v dgst -sha512
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of CFT-5.0.0_release450_2.tar.gz using CW-CCO_RELEASE.cer
```

パッケージの内容が抽出され、正常に検証されます。

ステップ 5 ディレクトリで install-cnc-templates ファイルを見つけ、その [説明（Description）] セクションに記載されている指示に従います。

ディレクトリ内の CF テンプレートをカスタマイズして、Amazon EC2 に Cisco Crosswork をインストールします。

次のタスク

以下のインストールワークフローに戻ります。AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

ロールとポリシーの権限

このセクションでは、Amazon に CF テンプレートを展開するときに必要なロールとポリシーの権限について説明します。ロールを作成および管理する方法については、Amazon のドキュメントを参照してください。

表 *38 : Amazon EC2* のロールと、ロールに割り当てられたアクション

役割	アクション（Actions）
EC2	DescribeInternetGateways、DescribeNetworkInterfaces、DescribeImages、DeleteLaunchTemplate、DescribeSubnets、DescribeAccountAttributes、DescribeSecurityGroups、RunInstances、DescribeVpcs、DescribeInstances、CreateNetworkInterface、CreateTags、DescribeKeyPairs、CreateLaunchTemplate、DeleteNetworkInterface、TerminateInstances
ELB	DescribeLoadBalancers、CreateLoadBalancer、ModifyLoadBalancerAttributes、AddTags、DeleteLoadBalancer
ELB v2	DescribeLoadBalancers、CreateLoadBalancer、AddTags、DeleteLoadBalancer、CreateTargetGroup、CreateListener、DeleteListener、DescribeTargetGroups、ModifyLoadBalancerAttributes、DescribeListeners、RegisterTargets、DeleteTargetGroup、ModifyTargetGroupAttributes、DescribeTargetHealth
IAM	CreateNodegroup、DescribeNodegroup、DeleteNodegroup

CloudFormation（CF）テンプレートパラメータの構成

このセクションでは、モジュールの展開に指定する必要がある重要なパラメータについて説明します。

- Cisco Crosswork クラスタ VM をインストールするための CF テンプレートパラメータ （154 ページ）
- Crosswork Data Gateway をインストールするための CF テンプレートパラメータ （161 ページ）
- NSO をインストールするための CF テンプレートパラメータ （165 ページ）
- 単一のハイブリッドクラスタまたはワーカーノードをインストールするための CF テンプレートパラメータ （166 ページ）

重要

- テンプレートの作成に必須のパラメータを、明示的に示しています。この表示のないパラメータはオプションであり、デフォルト値が設定されています。これは、展開要件に基づいて変更できます。
- パラメータとして入力するすべての IP アドレスが使用可能である必要があります。

Cisco Crosswork クラスタ VM をインストールするための CF テンプレートパラメータ

このセクションでは、Amazon EC2 に 3 つのハイブリッド VM を備えた Cisco Crosswork Cluster VM を展開するために必要なパラメータについて説明します。また、管理およびデータの NLB パラメータについても説明します。

クラスタノードおよび展開するその他の仮想マシンのサブネットを決定したら、必要な数の VM（および仮想 IP アドレス）をサポートするのに十分な IP アドレスがあることを確認します。

表 *39 : Cisco Crosswork* クラスタ *VM* 展開パラメータ

パラメータ	説明
`VpcId`	既存の仮想プライベートクラウド（VPC）の VPC ID。たとえば、vpc-0f83aac74690101a3 です。
`SecGroup`	スタックに適用する必要がある事前作成されたセキュリティグループ。たとえば、sg-096ff4bc355af16a0 です。グループは、ポート 22、30160:31560 への入力アクセスを許可する必要があります。

パラメータ	説明
CwSSHPassword	Crosswork Network Controller の SSH パスワード。 **重要** パスワードには外部のシークレットストアを使用することをお勧めします。
CwAmiId	Crosswork の AMI ID。 これは必須パラメータです。
CwMgmtSubnet1Id	Crosswork VM 1 の管理サブネット。 これは必須パラメータです。
CwMgmtSubnet2Id	Crosswork VM 2 の管理サブネット。 これは必須パラメータです。
CwMgmtSubnet3Id	Crosswork VM 3 の管理サブネット。 これは必須パラメータです。
CwMgmtSubnet1Netmask	ドット付き10進数形式の最初の管理サブネットネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、単一のインターフェイスに展開する場合は無視されます。 これは必須パラメータです。
CwMgmtSubnet2Netmask	ドット付き 10 進数形式の 2 番目の管理サブネットネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、単一のインターフェイスに展開する場合は無視されます。 これは必須パラメータです。
CwMgmtSubnet3Netmask	ドット付き 10 進数形式の 3 番目の管理サブネットネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、単一のインターフェイスに展開する場合は無視されます。 これは必須パラメータです。
CwMgmtSubnet1Gateway	選択したデータサブネット上の管理デフォルトゲートウェイ。通常、サブネットの最初のアドレスです。このパラメータは、シングル インターフェイス モードで展開されている場合は無視されます。 これは必須パラメータです。

パラメータ	説明
CwMgmtSubnet2Gateway	選択したデータサブネット上の管理デフォルトゲートウェイ。通常、サブネットの最初のアドレスです。このパラメータは、シングル インターフェイス モードで展開されている場合は無視されます。 これは必須パラメータです。
CwMgmtSubnet3Gateway	選択したデータサブネット上の管理デフォルトゲートウェイ。通常、サブネットの最初のアドレスです。このパラメータは、シングル インターフェイス モードで展開されている場合は無視されます。 これは必須パラメータです。
ManagementVIPName	Crosswork Management VIP 名。たとえば、dev1-cwmgnt です。 これは Crosswork クラスタにアクセスするためのホスト名になります。
DataVIPName	Crosswork Data VIP 名。たとえば、dev1-cwdata です。
Route53DomainName	すべての Route53 オブジェクトに使用されるドメイン名。 Crosswork クラスタの DNS ドメイン名です。 これは必須パラメータです。
HostedZoneId	ドメイン名（Route53DomainName）が指定されたホストゾーン ID。ネットワークロードバランサ（NLB）の展開には、事前定義された Route53 ホストゾーンが必要です。 これは必須パラメータです。
UseExternalNLB	Crosswork クラスタ（マルチ AZ またはサブネット）または Crosswork VIP（単一の AZ またはサブネットのみ）に外部 NLB を使用するかどうかを決定します。オプションは `True` または `False` です。 これは必須パラメータです。
CwClusterPlacementStrategy	単一の可用性ゾーンに有効な EC2 インスタンスの配置戦略。デフォルトの「クラスタ」では、最大スループットが保証されます。次のオプションがあります。 • `cluster` • `partition` • `spread`

パラメータ	説明
CwNodeType	展開用の Crosswork ノードタイプ。オプションは Hybrid または Worker です。 交換用のハイブリッドノードは、交換するハイブリッドノードと同じ IP アドレスを再利用する必要があります。 デフォルト値は Worker です。 これは必須パラメータです。
InterfaceDeploymentMode	導入モード。 オプションは、管理インターフェイスを展開する場合は 1、管理インターフェイスとデータインターフェイスを展開する場合は 2 です。
CwDataSubnet1Id	Crosswork VM 1 のデータサブネット。 単一のインターフェイスでは、管理インターフェイスが展開されているサブネットで展開が行われます。 これは必須パラメータです。
CwDataSubnet2Id	Crosswork VM 2 のデータサブネット。 単一のインターフェイスでは、管理インターフェイスが展開されているサブネットで展開が行われます。 これは必須パラメータです。
CwDataSubnet3Id	Crosswork VM 3 のデータサブネット。 単一のインターフェイスでは、管理インターフェイスが展開されているサブネットで展開が行われます。 これは必須パラメータです。
CwDataSubnet1Netmask	ドット付き 10 進数形式の最初のデータ サブネット ネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、シングル インターフェイス モードで展開する場合は無視されます。 これは必須パラメータです。
CwDataSubnet1Gateway	選択したデータサブネットの最初のデフォルト データ ゲートウェイ。通常、この値はサブネットの最初のアドレスです。このパラメータは、シングル インターフェイス モードで展開する場合は無視されます。 これは必須パラメータです。

パラメータ	説明
CwDataSubnet2Netmask	ドット付き 10 進数形式の 2 番目のデータ サブネット ネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、シングル インターフェイス モードで展開する場合は無視されます。 これは必須パラメータです。
CwDataSubnet2Gateway	ドット付き 10 進数形式の 2 番目のデータ サブネット ネットマスク。このパラメータは、シングル インターフェイス モードで展開する場合は無視されます。 これは必須パラメータです。
CwDataSubnet3Netmask	ドット付き 10 進数形式の 3 番目のデータ サブネット ネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、シングル インターフェイス モードで展開する場合は無視されます。 これは必須パラメータです。
CwDataSubnet3Gateway	ドット付き 10 進数形式の 3 番目のデータ サブネット ネットマスク。このパラメータは、シングル インターフェイス モードで展開する場合は無視されます。 これは必須パラメータです。
CwMgmtVIP	現在の Crosswork Management VIP アドレス。
CwDataVIP	現在の Crosswork Data VIP アドレス。外部 NLB を使用する場合は、このパラメータを空のままにすることができます。
Cw1MgmtIP	管理サブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
Cw1DataIP	データサブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
Cw2MgmtIP	管理サブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
Cw2DataIP	データサブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
Cw3MgmtIP	管理サブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
Cw3DataIP	データサブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。

パラメータ	説明
OtherCwMgmtIP1	既存の Crosswork ノードの管理 IP アドレス \#1。これは、展開が外部ロードバランサで行われる場合に使用されます。
OtherCwMgmtIP2	既存の Crosswork ノードの管理 IP アドレス \#2。このパラメータは、展開が外部ロードバランサで行われる場合に使用されます。
OtherCwDataIP1	既存の Crosswork ノードのデータ IP アドレス \#1。このパラメータは、展開が外部ロードバランサで行われる場合に使用されます。
OtherCwDataIP2	既存の Crosswork ノードのデータ IP アドレス \#2。このパラメータは、展開が外部ロードバランサで行われる場合に使用されます。

表 *40 : Crosswork VM* のカスタマイズ

パラメータ	説明
InstanceType	ノードインスタンスの EC2 インスタンスタイプ。 これは必須パラメータです。
RunAsSpotInstance	スポットインスタンス。 次のオプションがあります。 • True：機能を有効にします。 • False：機能を無効にします。 デフォルト値は False です。 これは必須パラメータです。
DataDiskSize	Crosswork のデータディスクサイズ。デフォルトは 450 GB で、ほとんどの展開で問題ないはずです。シスコ カスタマーエクスペリエンス チームから特に指示がない限り、デフォルトを入力します。 これは必須パラメータです。
K8sServiceNetwork	Kubernetes サービスネットワークのネットワークアドレス。CIDR 範囲は「/16」固定です。指定しない場合、デフォルト、つまり 10.96.0.0 が使用されます。 これは必須パラメータです。

パラメータ	説明
K8sPodNetwork	Kubernetes ポッドネットワークのネットワークアドレス。CIDR 範囲は「/16」固定です。 これは必須パラメータです。
SkipAutoInstall	自動インストールのスキップ機能を構成します。次のオプションがあります。 • True：機能を有効にします。 • False：機能を無効にします。 デフォルト値は False です。 これは必須パラメータです。

表 *41 : Cisco Crosswork* クラスタ管理 *NLB* 展開パラメータ

パラメータ	説明
VpcId	既存の仮想プライベートクラウド（VPC）の VPC ID。たとえば、vpc-0f83aac74690101a3 です。
CwTargetSubnetIdList	これは Crosswork 管理サブネットのリストです。 これは必須パラメータです。
CwTargetIP1	これは Crosswork VM 管理 IP です。このテンプレートでは、これは必須パラメータです。
CwTargetIP2	これは Crosswork VM 管理 IP です。このテンプレートでは、これは必須パラメータです。
CwTargetIP3	これは Crosswork VM 管理 IP です。このテンプレートでは、これは必須パラメータです。
Route53DomainName	すべての Route53 オブジェクトに使用されるドメイン名。 これは必須パラメータです。
HostName	すべての Route53 オブジェクトに使用されるドメイン名。 これは必須パラメータです。
HostedZoneId	ホストゾーン ID。 これは必須パラメータです。

表 *42 :* データ *NLB* 展開パラメータ

パラメータ	説明
VpcId	既存の仮想プライベートクラウド（VPC）の VPC ID。たとえば、vpc-0f83aac74690101a3 です。
CwTargetSubnetIdList	Crosswork VM の最初の管理サブネット。 これは必須パラメータです。
CwTargetIP1	管理サブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
CwTargetIP2	管理サブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
CwTargetIP3	管理サブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
Route53DomainName	すべての Route53 オブジェクトに使用されるドメイン名。 これは必須パラメータです。
HostName	すべての Route53 オブジェクトに使用されるドメイン名。 これは必須パラメータです。
HostedZoneId	ホストゾーン ID。 これは必須パラメータです。

Crosswork Data Gateway をインストールするための CF テンプレートパラメータ

このセクションでは、Crosswork Data Gateway コントロールプレーン、ノード、プール、およびその他の重要なコンテナを作成するときに必要なパラメータについて説明します。EC2 Crosswork Data Gateway NLB スタックの作成に必要なパラメータもあります。

表 *43 : Crosswork Data Gateway* 展開パラメータ

パラメータ	説明
VpcId	既存の仮想プライベートクラウド（VPC）の VPC ID。たとえば、vpc-0f83aac74690101a3 です。

パラメータ	説明
SecGroup	スタックに適用する必要がある事前作成されたセキュリティグループ。たとえば、sg-096ff4bc355af16a0 です。グループは、Crosswork、NSO、Crosswork Data Gateway、および IOS-XR が使用するすべてのポートへの入力アクセスを許可する必要があります。
CDGSSHPassword	Crosswork Data Gateway ノードで設定する SSH パスワード。
CDGOperPassword	Dg-Oper ユーザー用に Crosswork Data Gateway に設定するパスワード。
CDGAmiId	Crosswork Data Gateway の AMI ID。
InstanceType	ノードインスタンスの EC2 インスタンスタイプ。 これは必須パラメータです。
CNCControllerIP	Crosswork Data Gateway コントローラのホストアドレスまたはホスト名。マルチ AZ 展開では、この値は名前である必要があります。 これは必須パラメータです。
CNCControllerPassword	Crosswork または CNC コントローラにアクセスするために使用される cw-admin ユーザーのパスワード。
InterfaceDeploymentMode	Crosswork Data Gateway の展開モード。 次のオプションがあります。 • 1：すべてのインターフェイスを展開します。 • 2：管理およびデータインターフェイスを展開します。 • 3：管理、データ、および制御インターフェイスを展開します。
CDGInterface0IPAddress	サブネットのフリー IP アドレス。0.0.0.0 に設定すると、IP アドレスが自動的に割り当てられます。 これは必須パラメータです。
CDGInterface0SubnetId	Crosswork Data Gateway VM の最初のインターフェイスサブネット。
CDGInterface0Gateway	選択したサブネットのデフォルトゲートウェイ。通常、サブネットの最初のアドレスです。

パラメータ	説明
CDGInterface0SubnetNetmask	ドット付き 10 進数形式の最初のインターフェイス サブネット ネットマスク。たとえば、255.255.255.0 と指定します。 これは必須パラメータです。
CDGInterface1IPAddress	最初のサブネットのフリー IP アドレス。0.0.0.0 に設定すると、IP アドレスが自動的に割り当てられます。 これは必須パラメータです。
CDGInterface1SubnetId	Crosswork Data Gateway の 2 番目のインターフェイスサブネット。サブネットは、CDGInterface0SubnetId と同じ可用性ゾーンにある必要があります。
CDGInterface1Gateway	選択したサブネット上の 2 番目のインターフェイスのデフォルトゲートウェイ。通常、サブネットの最初のアドレスです。 これは必須パラメータです。
CDGInterface1SubnetNetmask	ドット付き 10 進数形式の 2 番目のインターフェイス サブネット ネットマスク。たとえば、255.255.255.0 と指定します。デュアル インターフェイス モードが使用されていない場合、このパラメータは無視されます。 これは必須パラメータです。
CDGInterface2IPAddress	2 番目のサブネット上のフリー IP アドレス。0.0.0.0 に設定すると、IP アドレスが自動的に割り当てられます。 これは必須パラメータです。
CDGInterface2SubnetId	Crosswork Data Gateway VM の 3 番目のインターフェイスサブネット。サブネットは、CDGInterface0SubnetId と同じ可用性ゾーンにある必要があります。
CDGInterface2Gateway	選択したサブネット上の 3 番目のインターフェイスのデフォルトゲートウェイ。通常、サブネットの最初のアドレスです。 これは必須パラメータです。
CDGInterface2SubnetNetmask	ドット付き 10 進数形式の 3 番目のインターフェイス サブネット ネットマスク。たとえば、255.255.255.0 と指定します。トリプル インターフェイス モードが使用されていない場合、このパラメータは無視されます。 これは必須パラメータです。
CNCControllerIP	Crosswork Data Gateway コントローラのホストアドレス。

パラメータ	説明
HANetworkMode	Crosswork Data Gateway の HA モード。 プールモードのオプションは次のとおりです。 • L2：このオプションは、HA プールを作成するための IP アドレスを指定するときに使用します。 • L3：このオプションは、HA プールの作成とマルチサブネット展開のための FQDN を指定するときに使用します。 プールタイプの詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Create a Cisco Crosswork Data Gateway Pool*」のセクションを参照してください。 これは必須パラメータです。
DataDiskSize	Crosswork データディスクのサイズ。最小サイズは 20 です。デフォルトサイズは 50 です。 これは必須パラメータです。
CDGProfile	Crosswork Data Gateway の展開プロファイル。 • Standard • Extended これは必須パラメータです。
CdgInstanceHostname	Crosswork Data Gateway インスタンス名（CDG-01 など）。

表 *44 : Crosswork Data Gateway* および *Network Load Balancer*（*NLB*）スタックパラメータ

パラメータ	説明
VpcId	ワーカーインスタンスの VPC ID。 これは必須パラメータです。
SubnetId1	サブネット 1 の管理 ID。 これは必須パラメータです。
SubnetId2	サブネット 2 の管理 ID。 これは必須パラメータです。
DomainName	ドメイン名。 これは必須パラメータです。

パラメータ	説明
HostedZoneId	ホストゾーン ID。 これは必須パラメータです。
CdgPoolHostname	Route53 レコードの名前。 これは必須パラメータです。
CdgTargetIP1	管理ノードの IP アドレス 1。 Crosswork Data Gateway が 1 つの場合は、1 つのターゲット IP を構成する必要があります。
CdgTargetIP2	管理ノードの IP アドレス 2。
LBIPaddress1	サブネット上の最初の LB IP アドレス。 これは必須パラメータです。
LBIPaddress2	サブネット上の 2 番目の LB IP アドレス。 これは必須パラメータです。

NSO をインストールするための CF テンプレートパラメータ

このセクションでは、Amazon EC2 に NSO を展開するために必要なパラメータについて説明します。

表 *45 : NSO* 展開パラメータ

パラメータ	説明
VpcId	既存の仮想プライベートクラウド（VPC）の VPC ID。たとえば、vpc-0f83aac74690101a3 です。
SecGroup	スタックに適用する必要がある事前作成されたセキュリティグループ。たとえば、sg-096ff4bc355af16a0 です。グループは、ポート 22、30160:31560 への入力アクセスを許可する必要があります。
NSOSubnetId	NSO VM のサブネット。
KeyName	インスタンスへの SSH アクセスを有効にする既存の EC2 KeyPair の名前。
NSOAmiId	NSO の AMI ID。 これは必須パラメータです。

パラメータ	説明
NSOInterface0IPAddress	2 番目のサブネット上のフリー IP アドレス。0.0.0.0 に設定すると、IP アドレスが自動的に割り当てられます。 これは必須パラメータです。
InstanceType	ノードインスタンスの EC2 インスタンスタイプ。 これは必須パラメータです。

単一のハイブリッドクラスタまたはワーカーノードをインストールするための CF テンプレートパラメータ

このセクションでは、単一のクラスタノード（ハイブリッドまたはワーカー）を展開するために必要なパラメータについて説明します。

注目

- 交換用のハイブリッドノードは、交換するハイブリッド VM と同じ IP アドレスを再利用する必要があります。
- 既存のクラスタに別のノード（ワーカーまたはハイブリッド）を追加することになるので、使用されているサブネットを特定し、そのサブネットで使用可能な追加の IP を見つけます。

表 *46* : 単一のハイブリッドクラスタまたはワーカー *Cisco Crosswork* ノードの展開パラメータ

パラメータ	説明
VpcId	既存の仮想プライベートクラウド（VPC）の VPC ID。たとえば、vpc-0f83aac74690101a3 です。
SecGroup	スタックに適用する必要がある事前作成されたセキュリティグループ。たとえば、sg-096ff4bc355af16a0 です。グループは、ポート 22、30160:31560 への入力アクセスを許可する必要があります。
EC2ENIRole	Crosswork クラスタの既存のロール名。ロールは EC2 アクセスを許可する必要があります。
CwAmiId	Crosswork の AMI ID。 これは必須パラメータです。

パラメータ	説明
CwSSHPassword	Crosswork Network Controller の SSH パスワード。 **重要** パスワードには外部のシークレットストアを使用することをお勧めします。
InstanceType	ノードインスタンスの EC2 インスタンスタイプ。 これは必須パラメータです。
ManagementVIPName	Crosswork Management VIP 名。たとえば、dev1-cwmgnt です。
DataVIPName	Crosswork Data VIP 名。たとえば、dev1-cwdata です。
Route53DomainName	すべての Route53 オブジェクトに使用されるドメイン名。 これは必須パラメータです。
UseExternalNLB	Crosswork クラスタ（マルチ AZ またはサブネット）または Crosswork VIP（単一の AZ またはサブネットのみ）に外部 NLB を使用するかどうかを決定します。オプションは True または False です。 これは必須パラメータです。
CwMgmtSubnetId	Crosswork VM の管理サブネット。
CwMgmtSubnetNetmask	ドット付き 10 進数形式の管理サブネットネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、シングル インターフェイス モードで展開する場合は無視されます。 これは必須パラメータです。
CwDataSubnetGateway	選択したデータサブネット上の管理デフォルトゲートウェイ。通常、サブネットの最初のアドレスです。このパラメータは、シングル インターフェイス モードで展開されている場合は無視されます。 これは必須パラメータです。
CwDataSubnetId	Crosswork VM のデータサブネット。
CwDataSubnetNetmask	ドット付き 10 進数形式のデータ サブネット ネットマスク。たとえば、255.255.255.0 と指定します。このパラメータは、シングルインターフェイスモードで展開する場合は無視されます。 これは必須パラメータです。

パラメータ	説明
CwDataSubnetGateway	選択したデータサブネット上のデータ デフォルト ゲートウェイ。通常、サブネットの最初のアドレスです。このパラメータは、シングル インターフェイス モードで展開されている場合は無視されます。 これは必須パラメータです。
CwNodeType	展開用の Crosswork ノードタイプ。オプションは Hybrid または Worker です。 交換用のハイブリッドノードは、交換するハイブリッドノードと同じ IP アドレスを再利用する必要があります。 これは必須パラメータです。
DataDiskSize	Crosswork のデータディスクサイズ。デフォルトは 450（GB 単位）で、ほとんどの展開で問題ないはずです。シスコ カスタマーエクスペリエンス チームから特に指示がない限り、デフォルトを入力します。 これは必須パラメータです。
K8sServiceNetwork	Kubernetes サービスネットワークのネットワークアドレス。CIDR 範囲は「/16」固定です。指定しない場合、デフォルト（10.96.0.0）が使用されます。
K8sPodNetwork	Kubernetes ポッドネットワークのネットワークアドレス。CIDR 範囲は「/16」固定です。指定しない場合、デフォルト（10.244.0.0）が使用されます。

表 *47*：オプションの *VM* パラメータ

パラメータ	説明
CwMgmtVIP	現在の Crosswork Management VIP アドレス。
CwDataVIP	現在の Crosswork Data VIP アドレス。外部 NLB を使用する場合は、このパラメータを空のままにすることができます。
Cw1MgmtIP	管理サブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
Cw1DataIP	データサブネット上のフリーアドレス。指定しない場合、アドレスは自動的に割り当てられます。
OtherCwMgmtIP1	既存の Crosswork ノードの最初の管理 IP アドレス。これは、展開が外部ロードバランサで行われる場合に使用されます。

パラメータ	説明
OtherCwMgmtIP2	既存の Crosswork ノードの 2 番目の管理 IP アドレス。このパラメータは、展開が外部ロードバランサで行われる場合に使用されます。
OtherCwDataIP1	既存の Crosswork ノードの最初のデータ IP アドレス。このパラメータは、展開が外部ロードバランサで行われる場合に使用されます。
OtherCwDataIP2	既存の Crosswork ノードの 2 番目のデータ IP アドレス。このパラメータは、展開が外部ロードバランサで行われる場合に使用されます。

モジュールの展開方法を使用したインストール

モジュールベースの展開手順では、各リソースを個別に展開します。各リソースには独自のテンプレートファイルがあり、個別に展開するために使用できます。詳細は、次のトピックを参照してください。

- Amazon EC2 への Cisco Crosswork クラスタのインストール （169 ページ）
- Amazon EC2 への Crosswork Data Gateway のインストール （171 ページ）
- Amazon EC2 への Cisco NSO のインストール （176 ページ）
- 追加の Crosswork クラスタノードの展開 （177 ページ）

Amazon EC2 への Cisco Crosswork クラスタのインストール

このセクションでは、Amazon EC2 に Cisco Crosswork クラスタをインストールする方法の概要を説明します。

Cisco Crosswork は、一連の CF テンプレートを使用して Crosswork クラスタを展開します。

Crosswork クラスタの展開ワークフロー

Crosswork クラスタの展開手順では、対応する YAML ファイルを使用してさまざまな Crosswork のリソースを展開します。

表 *48 : Crosswork* クラスタの展開中に展開されるリソース

リソース	説明
EC2 クラスタ	EC2 CW NLB を作成するために他のネストされたスタックを展開するメインスタック（**cw-cluster.yaml**）。

リソース	説明
管理 NLB	**cw-mgmt-nlb.yaml** ファイルは、EC2 CW 管理ノードのネットワークロードバランサ、ターゲットグループ、リスナー、および Route53 レコードを作成します。
データ NLB	**cw-data-nlb.yaml** ファイルは、EC2 CW データノードのネットワークロードバランサ、ターゲットグループ、リスナー、および Route53 レコードを作成します。

インストール パラメータ

Crosswork クラスタの展開に使用される CF テンプレートで指定する必要がある重要なパラメータのリストについては、Cisco Crosswork クラスタ VM をインストールするための CF テンプレートパラメータ （154 ページ）を参照してください。Crosswork クラスタは、テンプレートで指定されたパラメータに基づいて Amazon EC2 に展開されます。

（注） クラスタノードおよび展開するその他の仮想マシンのサブネットを決定したら、必要な数の VM（および仮想 IP アドレス）をサポートするのに十分な IP アドレスがあることを確認します。

CF テンプレートの展開

CF テンプレートをカスタマイズすることで、Amazon EC2 に Crosswork クラスタをインストールできます。Crosswork クラスタの展開に使用される CF テンプレートのリストについては、Crosswork クラスタの展開ワークフロー （169 ページ）を参照してください。

Amazon EC2 に CF テンプレートを展開する方法については、CF テンプレートの展開 （178 ページ）を参照してください。

インストールの確認

インストールのモニター （180 ページ）のステップに従って、Crosswork クラスタのインストールが成功したことを確認します。

追加の Crosswork クラスタノードの展開

Crosswork クラスタに追加のワーカーノードまたはハイブリッドノードを展開する方法については、追加の Crosswork クラスタノードの展開 （177 ページ）を参照してください。

次の作業

以下のインストールワークフローに戻ります。AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

Amazon EC2 への Crosswork Data Gateway のインストール

このセクションでは、Amazon EC2 に Crosswork Data Gateway をインストールする方法の概要を説明します。

Crosswork Data Gateway の展開ワークフロー

Crosswork Data Gateway の展開手順では、対応する YAML ファイルを使用してさまざまな Crosswork のリソースを展開します。

メインファイル **cdg-stack-ec2.yaml** は、1 つの CDG NLB（**cdg-nlb.yaml**）と 2 つの CDG（**cdg.yaml**）のスタックを展開します。

- Crosswork Data Gateway の高可用性プールに追加する Crosswork Data Gateway VM は、**cdg.yaml** ファイルを使用して展開されます。追加の VM の展開ごとに、展開の手順を繰り返す必要があります。
- 追加の NLB および Crosswork Data Gateway の高可用性プールは、**cdg-nlb.yaml** ファイルを使用して展開されます。

次の表に、インストールされているコンポーネントに関する情報を示します。

表 *49 : Crosswork Data Gateway* の展開中に展開されるリソース

リソース	説明
EC2 Crosswork Data Gateway	EC2 ノードに関連するリソースは、**cdg.yaml** ファイルを展開することで作成されます。
Crosswork Data Gateway ネットワークロードバランサ	EC2 NLB コンポーネント（ターゲットグループ、ネットワークロードバランサ、データリスナー、および NLB route 53 レコード）は、**cdg-nlb.yaml** ファイルを展開することによって作成されます。

インストール パラメータ

Crosswork Data Gateway CF テンプレートの重要なパラメータのリストについては、Crosswork Data Gateway をインストールするための CF テンプレートパラメータ （161 ページ）を参照してください。

Crosswork Data Gateway は、CF テンプレートで指定されたパラメータに基づいて Amazon EC2 に展開されます。Crosswork Data Gateway の展開に使用される CF テンプレートのリストについては、「Crosswork Data Gateway の展開ワークフロー （171 ページ）」を参照してください。

CF テンプレートの展開

Amazon EC2 に CF テンプレートを展開する方法については、CF テンプレートの展開 （178 ページ）を参照してください。

（注） Amazon EC2 では、Crosswork Data Gateway が 3 つの NIC を使用して展開されている場合、vNIC2 インターフェイスの IP アドレスを入力する必要があります。これは AWS EC2 の要件であり、Crosswork によって課されたものではありません。

インストールの確認

インストールのモニター（180 ページ）のステップに従って、Crosswork Data Gateway のインストールが成功したことを確認します。

次の作業

以下のインストールワークフローに戻ります。AWS EC2 への Cisco Crosswork Network Controller のインストール（16 ページ）

Crosswork Data Gateway を展開するための自動構成

自動構成手順は、欠落している構成パラメータを検出し、ベース VM をインストールするための必須パラメータを自動的に定義します。構成パラメータは、Dynamic Host Configuration Protocol（DHCP）フレームワークを使用して渡されます。デイゼロ構成では、自動構成メカニズムは必須パラメータのみをデフォルト値で定義します。

セキュリティポリシーに準拠するために、自動構成中にデフォルトのパスワードが提供されます。最初のログイン時に、dg-admin および dg-oper ユーザーはデフォルトのパスワードを変更する必要があります。Crosswork Data Gateway サービスは、デフォルトのパスワードが変更されるまで非アクティブです。

自動構成プロセスは、デフォルトの 3 NIC 展開をサポートします。特に、eth0 のみが管理ネットワーク用に構成されています。

DHCP の相互作用は、eth0 インターフェイスを介して行われます。自動構成手順では、DHCP サーバーに保存されているデフォルト値を使用します。ベース VM が展開されたら、インタラクティブコンソールを使用してデフォルト値を構成または変更できます。コンソールについての詳細は、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』を参照してください。

重要 Crosswork Data Gateway を VMware プラットフォームに展開する場合、自動構成メカニズムはサポートされていません。

自動構成時に使用されるパラメータ

自動構成ユーティリティは、次のパラメータをデフォルト値で構成します。これらのパラメータの詳細については、Cisco Crosswork Data Gateway のパラメータと展開シナリオ（80 ページ）を参照してください。

表 *50 : Cisco Crosswork Data Gateway* 必須展開パラメータ

名前	パラメータ	デフォルト値
AllowRFC8190	`AllowRFC8190`	デフォルト値は [Yes] です。
監査サーバポート（Auditd Server Port）	`AuditdPort`	デフォルトポートは `60` です。
Crosswork コントローラポート	`ControllerPort`	デフォルトポートは `30607` です。
説明	`Description`	デフォルト値は `CDG auto configure` です。
dg-admin パスフレーズ	`dg-adminPassword`	デフォルトのパスワードは `changeme` です。 デフォルト値を dg-admin ユーザー用に選択したパスワードでリセットします。 パスワードは 8 ー 64 文字である必要があります。
dg-oper パスフレーズ	`dg-operPassword`	デフォルトのパスワードは `changeme` です。 デフォルト値を dg-oper ユーザー用に選択したパスワードでリセットします。 パスワードは 8 ー 64 文字である必要があります。
データディスクサイズ（Data Disk Size）	`DGAppdataDisk`	このパラメータのデフォルト値は `5` です。

DNS アドレス（DNS Address）	`DNS`	このパラメータのデフォルト値は以下になります。
		`208.67.222.222`
		`208.67.220.220`

DNS セキュリティ拡張機能（DNS Security Extensions）	`DNSSEC`	このパラメータのデフォルト値は `False` です。
DNS over TLS	`DNSTLS`	このパラメータのデフォルト値は `False` です。
DNS 検索ドメイン（DNS Search Domain）	`Domain`	このパラメータのデフォルト値は `localdomain` です。
Crosswork Data Gateway の HA モード	`HANetworkMode`	このパラメータのデフォルト値は `L2` です。

名前	パラメータ	デフォルト値
ホストネーム	Hostname	このパラメータのデフォルト値は dg-<eth0 address> です。 この <eth0-address> は vNIC0 のアドレスです。
リンクローカル マルチキャスト名前解決（Link-Local Multicast Name Resolution）	LLMNR	このパラメータのデフォルト値は False です。
マルチキャスト DNS（Multicast DNS）	mDNS	このパラメータのデフォルト値は False です。
NicAdministration	NicAdministration	このパラメータのデフォルト値は eth0 です。
NicControl	NicControl	このパラメータのデフォルト値は eth1 です。
NicDefaultGateway	NicDefaultGateway	このパラメータのデフォルト値は eth0 です。
NicExternalLogging	NicExternalLogging	このパラメータのデフォルト値は eth0 です。
NicManagement	NicManagement	このパラメータのデフォルト値は eth0 です。
NicNBExternalData	NicNBExternalData	このパラメータのデフォルト値は eth1 です。
NicNBSystemData	NicNBSystemData	このパラメータのデフォルト値は eth1 です。
NicSBData	NicSBData	このパラメータのデフォルト値は、1 つの NIC 展開の場合は eth0、2 つの NIC の場合は eth1 など、最後にアクティブになったインターフェイスです。
NTPv4サーバ	NTP	このパラメータのデフォルト値は以下になります。 162.159.200.1 65.100.46.164 40.76.132.147 104.131.139.195
NTPv4 認証の使用（Use NTPv4 Authentication）	NTPAuth	このパラメータのデフォルト値は False です。
Profile	Profile	このパラメータのデフォルト値は Standard です。

名前	パラメータ	デフォルト値
Syslog マルチサーバーモード	SyslogMultiserverMode	このパラメータのデフォルト値は Simultaneous です。
Syslog サーバーポート（Syslog Server Port）	SyslogPort	このパラメータのデフォルト値は 514 です。
Syslog サーバープロトコル（Syslog Server Protocol）	SyslogProtocol	このパラメータのデフォルト値は UDP です。
TLS 経由の Syslog を使用する（Use Syslog over TLS）	SyslogTLS	このパラメータのデフォルト値は False です。
リモート監査サーバーの使用（Use Remote Auditd Server）	UseRemoteAuditd	このパラメータのデフォルト値は False です。
Syslog リモートサーバーの使用（Use Remote Syslog Server）	UseRemoteSyslog	このパラメータのデフォルト値は False です。
vNIC IPv4 方式	Vnic0IPv4Method	このパラメータのデフォルト値は DHCP です。
vNIC IPv4 スキップゲートウェイ（vNIC IPv4 Skip Gateway）	Vnic0IPv4SkipGateway	このパラメータのデフォルト値は False です。
vNIC IPv6 方式	Vnic0IPv6Method	デフォルト値は [なし（None）] です。
vNIC IPv6 スキップゲートウェイ（vNIC IPv6 Skip Gateway）	Vnic0IPv6SkipGateway	デフォルト値は False です。
vNIC IPv4 方式	Vnic1IPv4Method	デフォルト値は DHCP です。
vNIC IPv4 スキップゲートウェイ（vNIC IPv4 Skip Gateway）	Vnic1IPv4SkipGateway	デフォルト値は False です。
vNIC IPv6 方式	Vnic1IPv6Method	デフォルト値は [なし（None）] です。
vNIC IPv6 スキップゲートウェイ（vNIC IPv6 Skip Gateway）	Vnic1IPv6SkipGateway	デフォルト値は False です。
vNIC IPv4 方式	Vnic2IPv4Method	デフォルト値は DHCP です。

名前	パラメータ	デフォルト値
vNIC IPv4 スキップゲートウェイ（vNIC IPv4 Skip Gateway）	`Vnic2IPv4SkipGateway`	デフォルト値は `False` です。
vNIC IPv6 方式	`Vnic2IPv6Method`	デフォルト値は `[なし（None）]` です。
vNIC IPv6 スキップゲートウェイ（vNIC IPv6 Skip Gateway）	`Vnic2IPv6SkipGateway`	デフォルト値は `False` です。

Amazon EC2 への Cisco NSO のインストール

このセクションでは、Amazon EC2 に Cisco NSO をインストールする方法の概要を説明します。

Cisco Crosswork は、一連の CF テンプレートを使用して NSO を展開します。

NSO 展開ワークフロー

NSO の展開手順では、対応する YAML ファイルを使用してさまざまな Crosswork のリソースを展開します。

nso-stack-ec2.yaml ファイルは、1 つの NSO NLB（**nso-nlb-ec2.yaml**）と 2 つの NSO（**nso.yaml**）のスタックを展開します。詳細については、次の表を参照してください。

表 *51 : NSO* 展開中に展開されるリソース

リソース	説明
EC2 NSO	**nso.yaml** ファイルは、スタックに EC2 ノードリソース（ネットワーク インターフェイスとインスタンス）を作成するために展開されます。
NSO NLB	**nso-nlb-ec2.yaml** ファイルは、スタックに EC2 NLB リソース（ターゲットグループ、ネットワークロードバランサ、データリスナー、および NLB Route 53 レコード）を作成するために展開されます。

インストール パラメータ

NSO の展開に使用される CF テンプレートで指定する必要がある重要なパラメータのリストについては、NSO をインストールするための CF テンプレートパラメータ （165 ページ）を参照してください。NSO は、テンプレートで指定されたパラメータに基づいて Amazon EC2 に展開されます。

（注） NSO セットアップの削除中に、NSO Route53 レコード（NsoRoute53RecordName）を手動で削除します。

CF テンプレートの展開

CF テンプレートをカスタマイズすることで、Amazon EC2 に NSO をインストールできます。NSO の展開に使用される CF テンプレートのリストについては、NSO 展開ワークフロー （176 ページ）を参照してください。

Amazon EC2 に CF テンプレートを展開する方法については、CF テンプレートの展開 （178 ページ）を参照してください。

インストールの確認

インストールのモニター （180 ページ）のステップに従って、NSO のインストールが成功したことを確認します。

次の作業

以下のインストールワークフローに戻ります。AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

追加の Crosswork クラスタノードの展開

このセクションでは、Crosswork クラスタに追加のワーカーノードまたはハイブリッドノードを展開する方法について説明します。

Crosswork クラスタに追加のノードを展開するには、**cw-add-vm.yaml** ファイルを使用して Crosswork ネットワーク構成と VM のカスタマイズリソースを展開する必要があります。

重要 追加のワーカーノードを展開する前に、Crosswork クラスタと Crosswork アプリケーションが作成されていることを確認してください。

（注） 新しいハイブリッドノードは、置き換えるハイブリッド VM と同じ IP アドレスを再利用する必要があり、最大 3 つのハイブリッドノードが許可されます。

インストール パラメータ

Crosswork クラスタに追加のノードを展開するために使用される CF テンプレートで指定する必要がある重要なパラメータのリストについては、単一のハイブリッドクラスタまたはワーカーノードをインストールするための CF テンプレートパラメータ （166 ページ）を参照して

ください。テンプレートで指定されたパラメータに基づいて、追加のノードが Crosswork クラスタに展開されます。

CF テンプレートの展開

CF テンプレートをカスタマイズすることで、Crosswork クラスタに追加のワーカーノードまたはハイブリッドノードをインストールできます。

Amazon EC2 に CF テンプレートを展開する方法については、CF テンプレートの展開 （178 ページ）を参照してください。

インストールの確認

ノードが Crosswork クラスタに接続されていることを確認します。EC2 コンソールで、Crosswork クラスタを選択し、追加したノードが [コンピューティング（Compute）] セクションの下に表示されていることを確認します。詳細については、インストールのモニター （180 ページ）を参照してください。

次の作業

以下のインストールワークフローに戻ります。AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

CF テンプレートの展開の管理

以下のセクションでは、Amazon EC2 に CF テンプレートを展開し、そのインストールを確認する方法について説明します。

- CF テンプレートの展開 （178 ページ）
- インストールのモニター （180 ページ）

CF テンプレートの展開

カスタムリソースを使用して Amazon EC2 に Crosswork をインストールできます。構成したパラメータに応じて、機能を備えた必要なコンポーネントもインストールされます。

始める前に

- Amazon EC2 に Crosswork をインストールするために規定されている表 26 : AWS 前提条件と設定とAmazon EC2 設定を満たしていることを確認してください。
- S3 バケットまたはローカルマシンに保存されている CloudFormation テンプレートにアクセスできることを確認します。テンプレートが Amazon S3 にある場合は、テンプレートファイルの URL をコピーしたままにしておきます。

ステップ 1 AWS アカウントにログインし、S3 バケットに移動します。CF テンプレートがローカルコンピュータにある場合は、テンプレートをアップロードできます。

ステップ 2 AWS CloudFormation コンソールで、[スタック（Stacks）] ページに移動し、[スタックの作成（Create stack）] > [新しいリソースを使用（標準）（With new resources (standard)）] を選択します。[スタックの作成（Create stack）] ページが開きます。

ステップ 3 次の詳細を入力します。

1. [前提条件 - テンプレートの準備（Prerequisite - Prepare template）] で、[テンプレート準備完了（Template is ready）] を選択します。
2. [テンプレートの指定（Specify template）] > [テンプレートソース（Template source）] で、次のいずれかのオプションを選択します。
   - CF テンプレートが配置されている S3 バケットを指す YAML または JSON ファイルの URL がある場合は、[Amazon S3 URL] を選択します。[Amazon S3 URL] フィールドに URL を入力し、[次へ（Next）] をクリックします。
   - CF テンプレートがローカルコンピュータに保存されている場合は、[テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose File）] をクリックして、アップロードするファイルを選択します。テンプレートを選択すると、Amazon によってファイルがアップロードされ、S3 URL が表示されます。[Next] をクリックします。

（注） （オプション）[デザイナで表示（View in Designer）] をクリックして、CF テンプレートの実行フローを視覚的に表示します。

ステップ 4 [スタックの詳細を指定（Specify stack details）] ページで、スタック名とパラメータ値に関連する値を入力します。[Next] をクリックします。

（注） このウィンドウに表示されるパラメータフィールド名は、CF テンプレートのパラメータによって定義されます。

ステップ 5 構成したパラメータ値を確認します。

ステップ 6 [機能（Capabilities）] で、次の横にあるチェックボックスをオンにします。

- AWS CloudFormation がカスタムの名前を持つ IAM リソースを作成することを認める。（I acknowledge that AWS CloudFormation might create IAM resources with custom names.）
- AWS CloudFormation が次の機能を必要とする可能性があることを認める：CAPABILITY_AUTO_EXPAND。（I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND.）

ステップ 7 **[送信（Submit）]** をクリックします。

次のタスク

クラスタの作成にかかる時間は、展開プロファイルのサイズとハードウェアのパフォーマンス特性によって異なることがあります。インストールのステータスを確認する方法については、インストールのモニター （180 ページ）を参照してください。

インストールのモニター

このセクションでは、展開がエラーなしで完了したかどうかを確認する方法について説明します。

ステップ 1 CloudFormation コンソールの左側の [スタック（Stacks）] ペインから、展開したスタックを選択します。

ステップ 2 スタックの詳細が右側に表示されます。このウィンドウの各タブをクリックして、スタックの詳細を表示します。スタックの作成が進行中の場合、[イベント（Events）] タブのスタックのステータスは CREATE_IN_PROGRESS です。

ステップ 3 スタックが作成されたら、次の手順を実行します。

- スタックのステータスが CREATE_COMPLETE に変わり、[論理ID（Logical ID）] にスタック名が表示されます。
- [リソース（Resources）] タブには、物理 ID を含む、CF テンプレートが作成したすべてのリソースの詳細が表示されます。
- [出力（Outputs）] タブには、VM のインターフェイス IP アドレスの詳細が表示されます。

次のタスク

スタックの作成が完了したら、Crosswork UI にアクセスして、クラスタの正常性を監視できます。Crosswork UI にログインする方法の詳細については、Crosswork UI へのアクセス （180 ページ）を参照してください。

Crosswork UI へのアクセス

クラスタが作成されたら、すべてのノードがクラスタ内で稼働しているかどうかを Cisco Crosswork UI から確認できます。

始める前に

- スペアのネットワークロードバランサ（NLB）があることを確認します。Crosswork UI にアクセスするには、指定したプロトコルの DNS とポート番号を使用してリクエストをターゲットにルーティングする外部 NLB を使用します。
- Crosswork クラスタとポッドが実行状態であることを確認します。クラスタのステータスを表示する方法については、インストールのモニター （180 ページ）を参照してください。

- 管理ノードの IP アドレスは必ずコピーしておいてください。この IP アドレスは、Crosswork UI にアクセスするために使用されます。CloudFormation コンソールの [出力（Outputs）] タブから IP アドレスをコピーできます。[出力（Outputs）] タブへのアクセスについては、インストールのモニター （180 ページ）を参照してください。

ステップ 1 AWS コンソールにログインし、[ターゲットグループ（Target Groups）] に移動してターゲットを登録します。

ステップ 2 [ターゲット（Targets）] で、[ターゲットの登録（Register targets）] をクリックします。[ターゲットの登録（Register targets）] ページが開きます。

ステップ 3 [IPv4アドレス（IPv4 address）] で、CloudFormation コンソールからコピーした管理 IP アドレスを指定します。

ステップ 4 ポートを 30603 として指定します。[以下の保留中として含める（Include as pending below）] をクリックします。

ステップ 5 [保留中のターゲットの登録（Register pending targets）] をクリックします。

使用されなくなったターゲットを登録解除するには、ターゲットを選択して [Deregister（登録解除）] をクリックします。

ステップ 6 ターゲットが正常な状態になったら、[詳細（Details）] でロードバランサ名をクリックします。[ロードバランサ（Load balancer）] ページが開きます。

ステップ 7 [DNS名（DNS name）] 列から DNS 名をコピーします。

ステップ 8 サポートされているブラウザとして起動し、アドレスバーに次のように入力します。

```
https://<DNS_name>:30603/
```

（注） 初めて Cisco Crosswork にアクセスすると、一部のブラウザでは、サイトが信頼できないという警告が表示されます。この場合は、指示に従ってセキュリティ例外を追加し、Cisco Crosswork サーバーから自己署名証明書をダウンロードします。セキュリティの例外を追加すると、ブラウザは今後のすべてのログイン試行で信頼できるサイトとしてサーバーを受け入れます。CA 署名付き証明書を使用する場合は、『*Crosswork Network Controller 5.0 Administration Guide*』の「*Manage Certificates*」のセクションを参照してください。

ステップ 9 次のように Cisco Crosswork にログインします。

1. Cisco Crosswork 管理者のユーザー名の **admin** とデフォルトのパスワードの **admin** を入力します。
2. [ログイン（Log In）] をクリックします。
3. 管理者のデフォルトのパスワードを変更するように求められたら、表示されたフィールドに新しいパスワードを入力し、[OK] をクリックします。

（注） 強力な VM パスワード（大文字と小文字、数字、特殊文字を含む 8 文字以上の長さ）を使用します。ディクショナリの単語に類似したパスワード（「Pa55w0rd!」など）や関連する単語に類似したパスワード（C!sco123 や Cwork321! など）の使用は避けてください。

ステップ 10 （オプション）[Crossworkの正常性（Crosswork Health）] タブをクリックし、[Crossworkインフラストラクチャ（Crosswork Infrastructure）] タイルをクリックして Cisco Crosswork で実行されているマイクロサービスの正常性ステータスを表示します。

次のタスク

以下のインストールワークフローに戻ります。AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

Crosswork Data Gateway インストール後のタスク

このセクションでは、Crosswork Data Gateway を展開した後に実行できるステップを示します。

Crosswork Data Gateway VM のタイムゾーンの設定

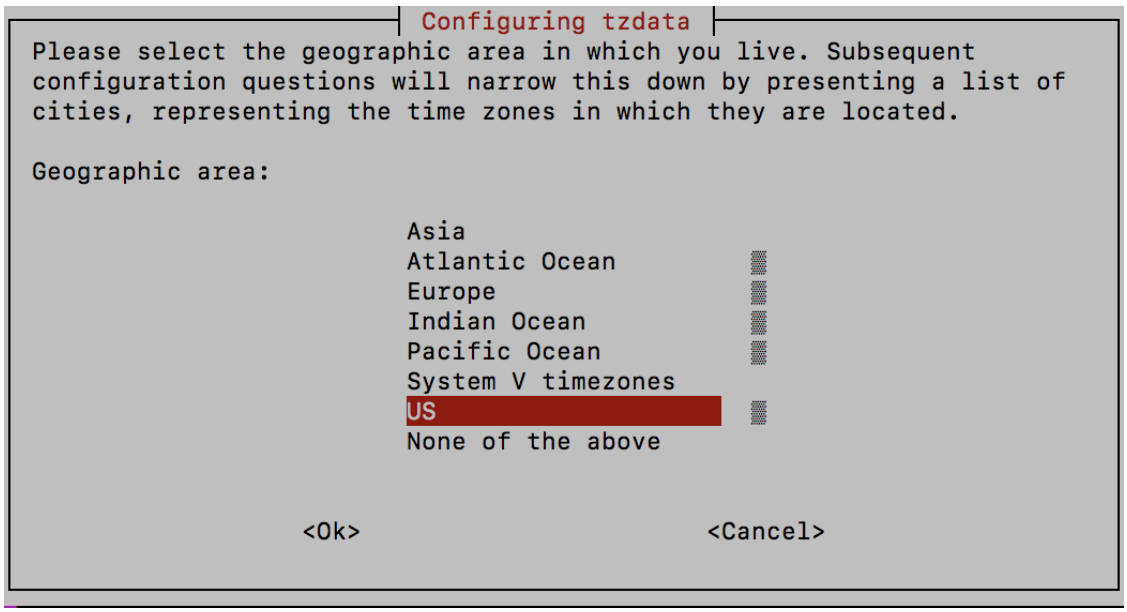
一般に、Crosswork Data Gateway VM はデフォルトのタイムゾーンを UTC として起動します。ご自身の地理的エリアに合わせてタイムゾーンを設定することをお勧めします。この構成では、Showtech ログを含むすべての Crosswork Data Gateway プロセスが、構成された同じタイムゾーンを使用します。

ステップ 1 Crosswork Data GatewayVM のインタラクティブメニューで、[Change Current System Settings] を選択します。

ステップ 2 [9 Timezone] を選択します。

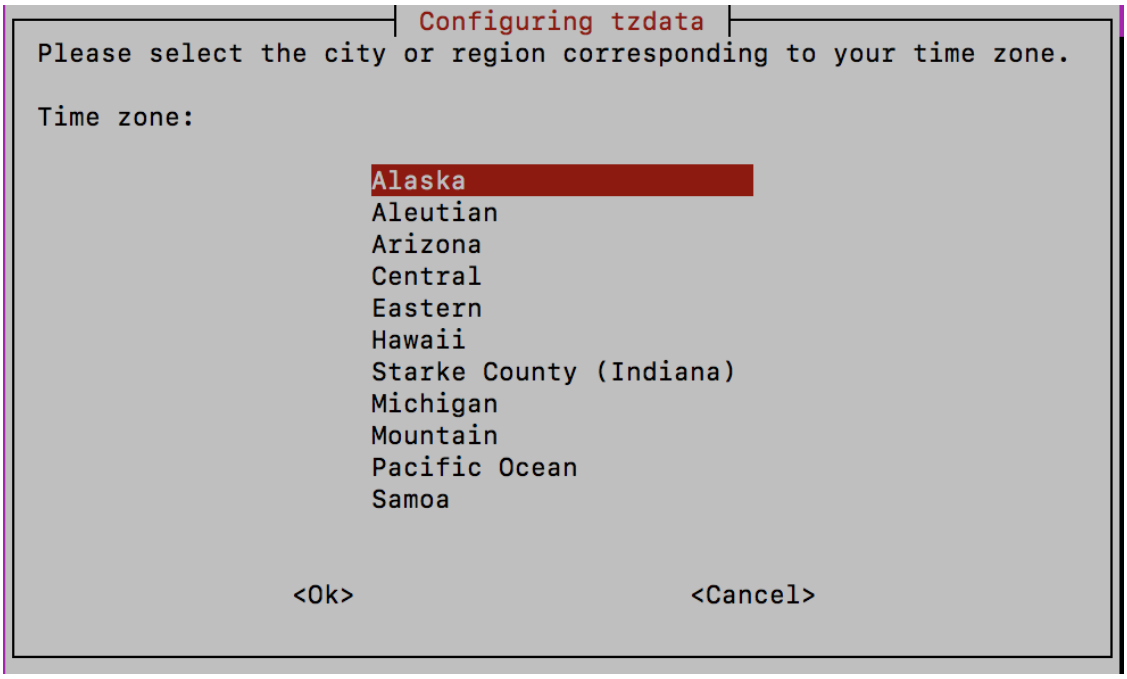
ステップ 3 居住地域を選択します。

図 *30 : [*タイムゾーン設定（*Timezone Settings***）*] - [*地理的エリアの選択（***Geographic Area Selection***）*]**



ステップ 4 タイムゾーンに対応する都市または地域を選択します。

図 *31 : [*タイムゾーン設定（*Timezone Settings***）*] - [*地域の選択（***Region Selection***）*]**



ステップ 5 [OK] を選択して設定を保存します。

ステップ 6 Crosswork Data GatewayVM をリブートして、すべてのプロセスで新しいタイムゾーンが選択されるようにします。

ステップ 7 Crosswork Data Gateway VM からログアウトします。

Crosswork Data Gateway VM へのログインとログアウト

このセクションでは、Crosswork Data Gateway VM にログインおよびログアウトする方法について説明します。

Crosswork Data Gateway VM にアクセスしてログアウトするには、次のステップに従います。

- SSH による Crosswork Data Gateway VM へのアクセス （183 ページ）
- Crosswork Data Gateway VM からのログアウト （184 ページ）

SSH による Crosswork Data Gateway VM へのアクセス

セキュアシェル（SSH）は、複数回ログインに失敗した後でクライアント IP をブロックすることにより、ブルートフォース攻撃から保護します。不正なユーザ名またはパスワード、接続の切断、あるいはアルゴリズムの不一致などの失敗は、IP に対してカウントされます。20 分の時間枠内で最大 4 回失敗すると、クライアント IP は少なくとも 7 分間ブロックされます。失

敗が累積し続けると、ブロックされる時間が長くなります。各クライアント IP は個別に追跡されます。

SSH で Cisco Crosswork Data Gateway VM にログインするには、次の手順を実行します。

ステップ 1 Cisco Crosswork Data Gateway の管理 IP にネットワークアクセスできるワークステーションから、次のコマンドを実行します。

ssh <username>@<ManagementNetworkIP>

ここで、**ManagementNetworkIP** は管理ネットワークの IP アドレスです。

次の例を参考にしてください。

管理者ユーザーとしてログインする場合：**ssh dg-admin@<ManagementNetworkIP>**

オペレータユーザーとしてログインする場合：**ssh dg-oper@<ManagementNetworkIP>**

Crosswork Data Gateway のフラッシュ画面が開き、パスワードの入力が求められます。

ステップ 2 対応するパスワード（インストールプロセスで作成したパスワード）を入力し、**Enter** を押します。

Cisco Crosswork Data Gateway VM にアクセスできない場合は、ネットワーク設定に問題があります。コンソールからネットワーク設定を確認します。正しくない場合は、Cisco Crosswork Data Gateway VM を削除し、正しいネットワーク設定で再インストールすることをお勧めします。

Crosswork Data Gateway VM からのログアウト

VM からログアウトするには、**メインメニュー**から [1 ログアウト（1 Logout）] を選択し、**Enter** を押すか、[OK] をクリックします。

Crosswork Data Gateway のインストールと登録のトラブルシューティング

Cisco Crosswork での Crosswork Data Gateway の自動登録に失敗した場合は、Crosswork Data Gateway show-tech を収集し（[メインメニュー（Main menu）] > [5 トラブルシューティング（5 Troubleshooting）] > [2show-techの実行（2 Run show-tech）] を選択）、`controller-gateway` のログで理由を確認します。show-tech ログを収集する方法の詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Collect show-tech logs from the Interactive Console*」のセクションを参照してください。セッションの確立または証明書に関連する問題がある場合は、インタラクティブコンソールを使用して `controller.pem` 証明書がアップロードされていることを確認します。

重要 IPv6 アドレスを使用している場合は、角カッコ（[1 :: 1]）で囲む必要があります。

次の表に、Crosswork Data Gateway のインストール時または登録時に発生する可能性のある一般的な問題をリストし、問題の原因を特定して解決するためのアプローチを示します。

表 *52 :* インストール/登録のトラブルシューティング

問題	操作
NTP の問題により Crosswork Data Gateway を Cisco Crosswork に登録できません。つまり、2 つの間にクロックのずれがあります。 **クロックのずれは、Crosswork Data Gateway または Cisco Crosswork のいずれかで発生する可能性があります。** **また、Cisco Crosswork と Crosswork Data Gateway の NTP サーバーでは、初期時間は ESXi サーバーに設定されます。このため、ESXi サーバーにも NTP を設定する必要があります。** **ホストのクロックタイムを同期して、再試行します。**	1.Crosswork Data Gateway VM にログインします。 2.メインメニューから、[5トラブルシューティング（5 Troubleshooting）] > [2show-techの実行（2 Run show-tech）] を選択します。 ログとバイタルを含む tarball を保存する接続先を入力し、[OK] をクリックします。 show-tech は、.tar.xz で終わるファイル拡張子で暗号化されるようになりました。 3. 次のコマンドを実行して、show-tech ファイルを復号化します。 `openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>` show-tech のログ（`/opt/dg/log/controller-gateway/session.log` にある `session.log` ファイル）に「`UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid`」というエラーが表示された場合は、Crosswork Data Gateway と Cisco Crosswork の間にクロックのずれがあります。 3. メインメニューから、[3 現在のシステム設定の変更（3 Change Current System Settings）] > [1 NTP設定（1 Configure NTP）] に移動します。 Cisco Crosswork サーバーのクロックタイムと同期するように NTP を設定し、Crosswork Data Gateway の再登録を試行します。

問題	操作
証明書エラーが原因の「バイタルを収集できませんでした（**Could not collect vitals**）」という理由で **Crosswork Data Gateway** が **10** 分以上にわたって劣化状態のままになる。	1.Crosswork Data Gateway VM にログインします。 2. メインメニューから、[5トラブルシューティング（5 Troubleshooting）] > [2show-techの実行（2 Run show-tech）] を選択します。 ログとバイタルを含む tarball を保存する接続先を入力し、[OK] をクリックします。 show-tech は、.tar.xz で終わるファイル拡張子で暗号化されるようになりました。 3. 次のコマンドを実行して、show-tech ファイルを復号化します。 `openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>` show-tech ログ（`/opt/dg/log/controller-gateway/gateway.log` にある `gateway.log` ファイル）に証明書エラーがある場合は、次の手順で説明するように、コントローラ署名証明書を再度アップロードします。 1. メインメニューから、[3現在のシステム設定の変更（3 Change Current System Settings）] > [7証明書のインポート（7 Import Certificate）] を選択します。 2. [証明書のインポート（Import Certificates）] メニューから、[1 コントローラ署名証明書ファイル（1 Controller Signing Certificate File）] を選択し、[OK] をクリックします。 3. 証明書ファイルの SCP URI を入力し、[OK] をクリックします。

問題	操作
証明書エラーが原因で「gRPC接続を確立できません（gRPC connection cannot be established）」という理由で、Crosswork Data Gateway が 10 分以上にわたって劣化状態のままになる。	1. 次のステップを使用して、証明書ファイルを再アップロードします。 a. メインメニューから、[3 現在のシステム設定の変更（3 Change Current System Settings）] > [7証明書のインポート（7 Import Certificate）] を選択します。 b. [証明書のインポート（Import Certificates）] メニューから、[1 コントローラ署名証明書ファイル（1 Controller Signing Certificate File）] を選択し、[OK] をクリックします。 c. 証明書ファイルの SCP URI を入力し、[OK] をクリックします。 2. 次の手順に従って Crosswork Data Gateway VM をリブートします。 a. メインメニューから [5 トラブルシューティング（5 Troubleshooting）] を選択し、[OK] をクリックします。 b. [Troubleshooting] メニューから [4 Reboot VM] を選択し、[OK] をクリックします。 c. リブートが完了したら、Crosswork Data Gateway の動作ステータスが [稼働中（Up）] になっているかどうかを確認します。
Crosswork Data Gateway がエラー状態になる	vCenter の場合は OVF テンプレートの vNIC 値を確認します。
1 つの NIC Cisco Crosswork での Crosswork Data Gateway の登録が失敗する	vCenter の場合は OVF テンプレートの vNIC 値を確認します。1 つの NIC と 2 つの NIC の ActiveVnics プロパティが欠落している場合は、Crosswork Data Gateway はデフォルトで 3 つの NIC を展開しようとします。 このため、Crosswork Data Gateway が 1 つの NIC を予期しているが NIC が 1 つではない gateway.log 内のエラーで展開後に 1 つの NIC Cisco Crosswork での Crosswork Data Gateway の登録が失敗します。

問題	操作
Crosswork Data Gateway が拡張プロファイルの代わりに標準プロファイルを展開する	vCenter の場合は、OVF テンプレートの `Deployment` パラメータを確認します。`Deployment` パラメータが一致しないか、拡張プロファイルに存在しない場合、Crosswork Data Gateway はデフォルトで標準プロファイルを展開します。
Crosswork のアップグレード中に、一部の Crosswork Data Gateway がアップグレードまたは再登録されず、dg-manager ログに複数のエラーメッセージが記録されることがある。	Crosswork Data Gateway を再登録または再展開します。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Redeploy a Crosswork Data Gateway Instance*」のセクションと「*Reenroll Crosswork Data Gateway*」のセクションを参照してください。

以前 Crosswork にアタッチされていた Crosswork Data Gateway インスタンスが別の Crosswork バージョン 4.x または 5.0 に再アタッチされた場合、インスタンスの動作状態は、robot-astack-influxdb エラーで [低下（Degraded）] になることがある。	1. SSH から Crosswork Data Gateway VM にログインします。
	2. Docker のエグゼクティブコマンドを実行して、**robot-astack-influxdb** ポッドにアクセスします。
	3. ポッドで、次のディレクトリに移動して削除します。
	`/mnt/datafs/influxdb`
	4. 次のコマンドを使用して、サービスを再起動します。
	`supervisorctl restart all`

ゲートウェイをメンテナンスモードに移行せずに Data Gateway を再展開すると、Crosswork の登録が失敗し、dg-manager および controller-gateway ログにエラーが記録される。	Data Gateway を**メンテナンス**モードに移行するか、ゲートウェイを手動で再登録します。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「*Reenroll Crosswork Data Gateway*」のセクションを参照してください。

コントローラ署名証明書ファイルのインポート

コントローラ証明書ファイルは、VM の起動後に自動的にインポートされます。次の理由により、この手順は手動で実行する必要があります。

- インストール時に [Controller Settings] で [Controller Signing Certificate File URI] が指定されませんでした。
- Cisco Crosswork がアップグレードまたは再インストールされたため、Cisco Crosswork で Crosswork Data Gateway を認証および登録する必要があります。

コントローラ署名証明書ファイルをインポートするには、次の手順を実行します。

ステップ 1 Cisco Crosswork Data Gateway VM のインタラクティブメニューから、[3 Change Current System Settings] を選択します。

[システム設定の変更（Change System Settings）] メニューが開きます。

ステップ 2 [7 証明書のインポート（7 Import Certificate）] を選択します。

ステップ 3 [証明書のインポート（Import Certificates）] メニューから、[1 コントローラ署名証明書ファイル（1 Controller Signing Certificate File）] を選択します。

ステップ 4 証明書ファイルの SCP URI を入力します。

URI の例を以下に示します。

```
cw-admin@{server ip}:/home/cw-admin/controller.pem
```

ステップ 5 SCP パスフレーズ（SCP ユーザーパスワード）を入力します。

証明書ファイルがインポートされます。

ステップ 6 証明書が正常にインストールされたことを確認します。コントローラ署名証明書ファイルの表示（130ページ）を参照してください。

コントローラ署名証明書ファイルの表示

次のステップを実行して署名証明書を表示します。

ステップ 1 Crosswork Data Gateway VM のインタラクティブメニューから、[2 システム設定の表示（2 Show System Settings）] を選択します。

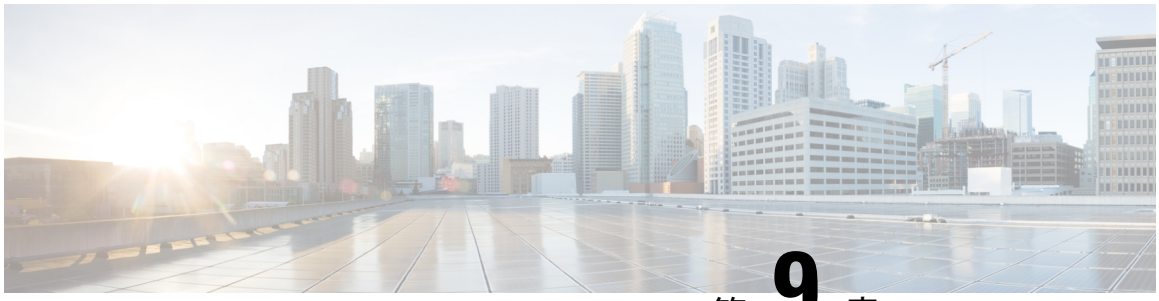
ステップ 2 [現在のシステム設定の表示（Show Current System Settings）] メニューから、[7 証明書（7 Certificates）] を選択します。

ステップ 3 [2 コントローラ署名証明書ファイル（2 Controller Signing Certificate File）] を選択します。

新しい証明書がインポートされていない場合は、Crosswork Data Gateway にデフォルトの証明書が表示されます。正常にインポートされている場合は、新しい証明書が表示されます。

第 IV 部

Crosswork アプリケーションのインストール



第 9 章

Crosswork アプリケーションのインストール

この章は次のトピックで構成されています。

Crosswork アプリケーションのインストール

このセクションでは、Cisco Crosswork UI に Crosswork アプリケーションをインストールする方法について説明します。

Crosswork Network Controller アプリケーションは、**Essentials**、**Advantage**、および **Add-on** パッケージとしてバンドルされています（詳細はCisco Crosswork Network Controller パッケージ （3 ページ）を参照）。すべてのパッケージには、CAPP（Crosswork APPlication）と呼ばれる Crosswork 固有の特定の形式で Crosswork アプリケーションが含まれています。最初のステップとして、アプリケーション CAPP ファイル（*.tar.gz）を含むパッケージを、cisco.com から Cisco Crosswork サーバーから到達可能なマシンにダウンロードする必要があります。その後パッケージが Crosswork UI に追加され、そこにアプリケーションをインストールできます。

まず関連する Crosswork Network Controller パッケージ（Essential または Advantage または Add-on）を cisco.com からダウンロードしてから、パッケージの一部であるアプリケーションのインストールに進む必要があります。

始める前に

アプリケーションのすべての要件が満たされていることを確認します。

ステップ 1　CAPP ファイルをダウンロードして検証します。

a) cisco.com に移動し、必要な Crosswork Network Controller パッケージと関連する署名ファイルをマシンのディレクトリにダウンロードします。これらの手順では、それぞれファイル名「**cw-na-cncessential-5.0.0-72-release-230502.tar.gz**」および「**cnc-5.0.0-capp-signatures.tar.gz**」を使用します。

b) 次の署名ファイルを解凍します。

Crosswork アプリケーションのインストール

```
tar -xvf <signature file>
```

例：

```
[test@cw-build sample]% tar -xvf cnc-5.0.0-capp-signatures.tar.gz
README
CW-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cisco_x509_verify_release.py
cw-na-cncessential-5.0.0-72-release-230502.tar.gz.signature
cw-na-cncadvantage-5.0.0-77-release-230425.tar.gz.signature
cw-na-cncaddon-5.0.0-68-release-230502.tar.gz.signature
```

c) Python スクリプトを使用して、使用する予定の各ファイルの署名を検証します。

（注） `python --version` を使用して、マシンの Python バージョンを確認します。

Python 2.x を使用している場合は、次のコマンドを使用してファイルを検証します。

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
 -v dgst -sha512
```

Python 3.x を使用している場合は、次のコマンドを使用してファイルを検証します。

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature
file> -v dgst -sha512
```

例：

```
[test@cw-build sample]% python cisco_x509_verify_release.py3 -s
cw-na-cncessential-5.0.0-72-release-230502.tar.gz.signature -i
cw-na-cncessential-5.0.0-72-release-230502.tar.gz -e CW-CCO_RELEASE.cer
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-cncessential-5.0.0-72-release-230502.tar.gz using
 CW-CCO_RELEASE.cer
```

（注） python がインストールされていない場合は、python.org にアクセスして、ワークステーションに適したバージョンの python をダウンロードします。

d) スタンドアロンの Crosswork アプリケーション（Crosswork Optimization Engine など）のダウンロードを予定している場合は、関連するファイルにカーソルを合わせ、MD5 または SHA512 チェックサムをクリップボードにコピーします。

Crosswork サーバーから到達可能なサーバーに CAPP ファイルをダウンロードします。選択したツールを実行してチェックサムを計算し、ダウンロードしたファイルのチェックサム値をクリップボードにコピーした値と比較します。

たとえば、MAC では、**md5** コマンドを使用してファイルの MD5 サムを計算できます。

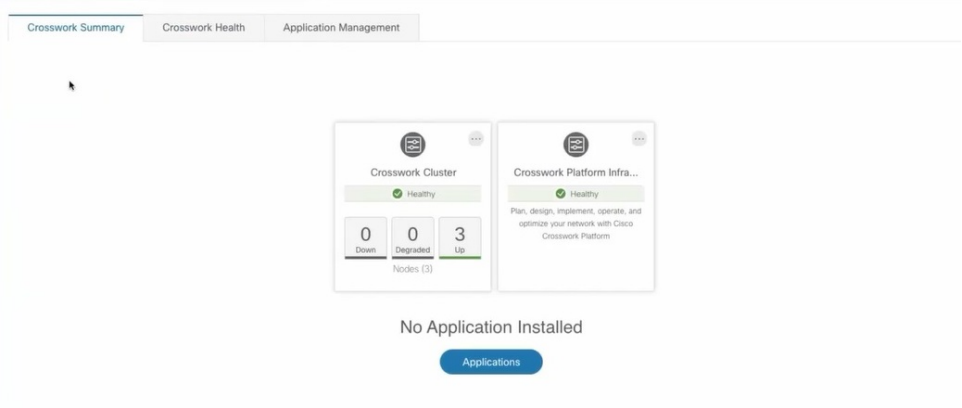
```
md5 <.tar.gz>
```

結果の値が cisco.com に投稿された値と一致することを確認します。

ステップ 2　ダウンロードした CAPP ファイルを Crosswork に追加します。

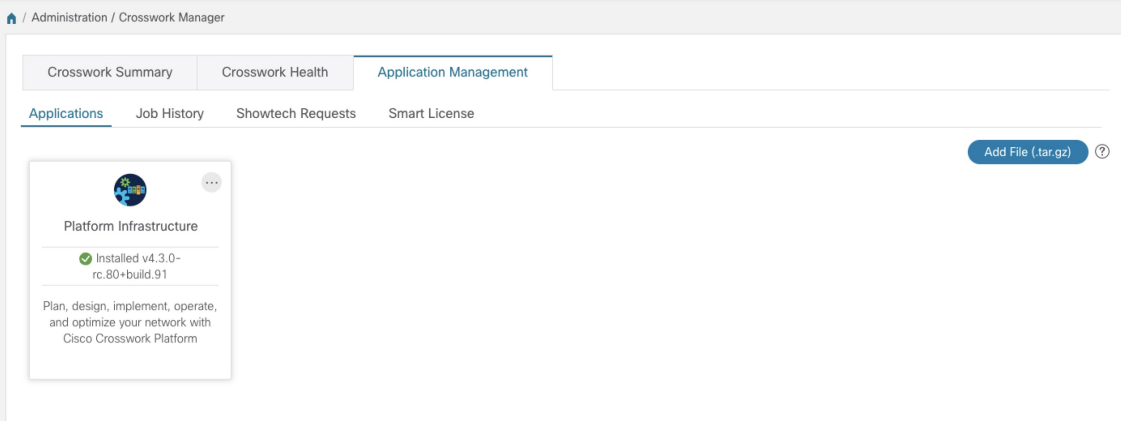
Crosswork アプリケーションのインストール

a) Cisco Crosswork にログインし、ホームページで **[管理（Administration）]** > **[Crossworkマネージャ（Crosswork Manager）]** をクリックします。[Crosswork の概要（Crosswork Summary）] ページが表示され、[Crosswork クラスタ（Crosswork Cluster）] タイルと [Crosswork プラットフォーム インフラストラクチャ（Crosswork Platform Infrastructure）] タイルが表示されます。



タイルをクリックすると、詳細情報が表示されます。

b) [アプリケーション管理（Application Management）] をクリックし、[アプリケーション（Applications）] タブを選択します。

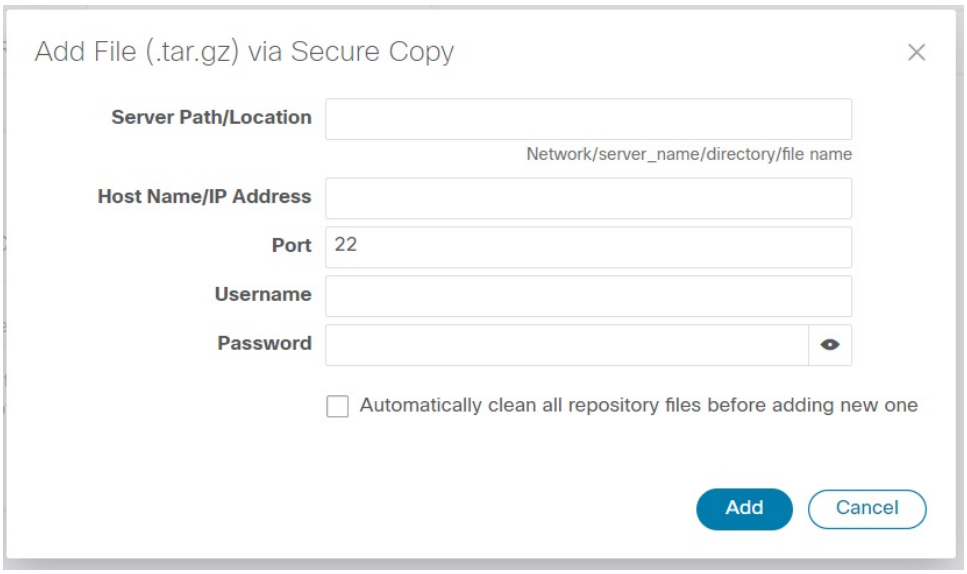


c) [ファイルの追加（.tar.gz）（Add File (.tar.gz)）] オプションをクリックして、CAPP ファイルを含むパッケージを追加します。

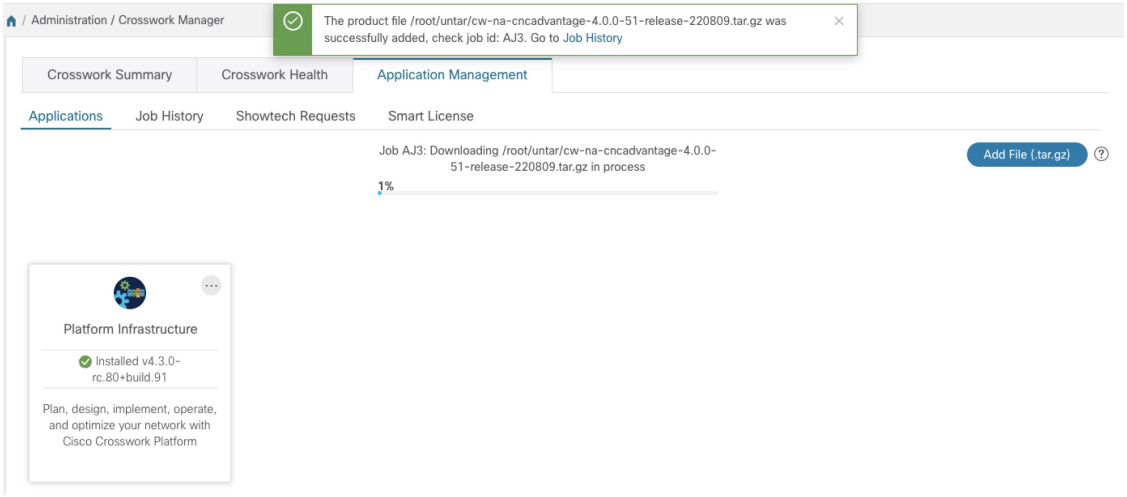
（注） Crosswork Network Controller パッケージをインストールする場合、パッケージを解凍する必要はありません。パッケージ tarball をそのまま Crosswork UI に追加でき、その中のアプリケーションが自動的に追加されます。その後、必要に応じて個々のアプリケーションをインストールできます。

d) [ファイルの追加（Add File）] ダイアログボックスで、該当する情報を入力し、[追加（Add）] をクリックします。

Crosswork アプリケーションのインストール



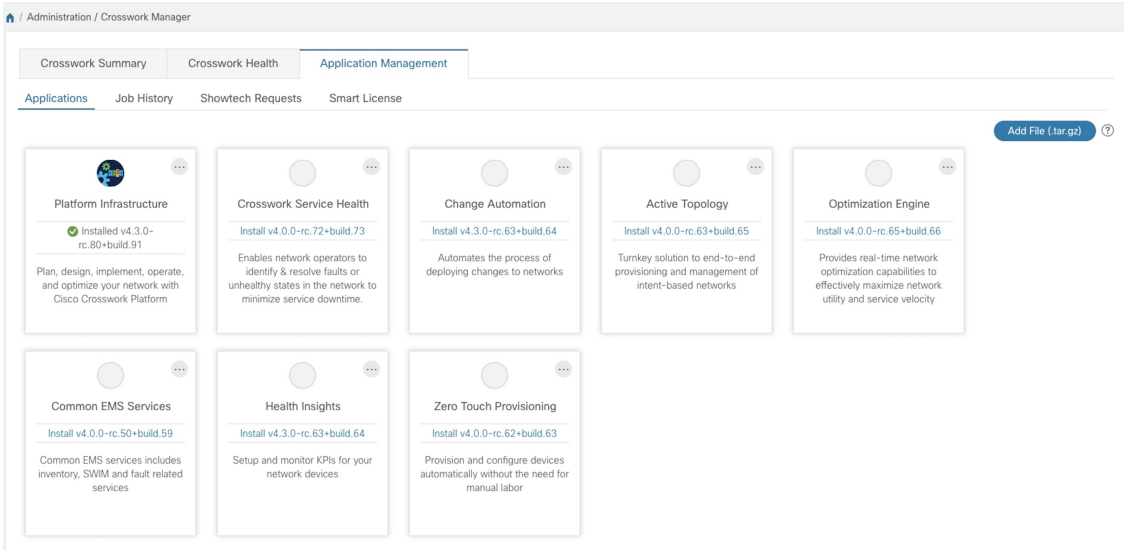
追加操作の進行状況が [アプリケーション（Applications）] 画面に表示されます。[ジョブ履歴（Job History）] タブにインストールの進行状況を表示することもできます。



（注） Crosswork Network Controller パッケージをロードするとき、ホストプラットフォームで使用できるリソースによっては、ロードプロセスがしばらく 50% で停止する場合があります。

新しく追加されたアプリケーションファイルは、[アプリケーション（Applications）] 画面にタイルとして表示されます。

Crosswork アプリケーションのインストール



ステップ 3　アプリケーション CAPP ファイルをインストールします。

a) アプリケーションタイルの [インストール（Install）] プロンプトをクリックします。タイルの ⋯ をクリックし、ドロップダウンリストから [インストール（Install）] オプションを選択することもできます。

重要　Crosswork クラスタおよび Crosswork Data Gateway をインストールしたら、次の順序で Crosswork Network Controller パッケージ（Essential または Advantage）のアプリケーションをインストールする必要があります。

1. Crosswork 最適化エンジン
2. Crosswork アクティブトポロジ
3. Crosswork Service Health（Advantage パッケージでのみ利用可能）
4. 要素管理機能（EMF）

Crosswork Change Automation、Crosswork Health Insights、および Crosswork Zero Touch Provisioning は、任意の順序で個別にインストールでき、他のアプリケーションを事前にインストールする必要はありません。

これで、アプリケーションがインストールされました。アプリケーション タイル アイコンの変化を確認できます。アプリケーションをインストールすると、すべての関連リソース、UI 画面、およびメニューオプションが Crosswork UI に動的にロードされます。

（注）　アプリケーションがインストールされると、90 日間の評価期間が自動的に開始されます。[スマートライセンス（Smart License）] タブで、Cisco スマートアカウントにアプリケーションを登録できます。

b) アプリケーションをインストールした後、そのアプリケーションを機能させるにはアクティブにする必要があります。初回インストールでは、CAPP ファイルもアクティブになります。ただし、インス

トールが成功した後にアクティブ化が失敗した場合は、手動でアプリケーションをアクティブにできます。アプリケーションを手動でアクティブにするには、アプリケーションタイルの をクリックし、[Activate] を選択します。

ステップ 4 残りのアプリケーションをインストールするには、手順 3 を繰り返します。

ステップ 5 （オプション）アプリケーションタイルの をクリックし、[詳細の表示（View Details）] オプションを選択して、インストールされているアプリケーションの詳細を表示します。

ステップ 6 アプリケーション（複数の場合はすべてのアプリケーション）をインストールしたら、環境の状態をチェックして、すべてのアプリケーションが正常であることを確認します。起動するすべてのプロセスと、アプリケーションが正常であると報告されるまでに、最大 1 時間かかることがあります。新しくインストールしたアプリケーションが 1 時間たっても正常に動作しない場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

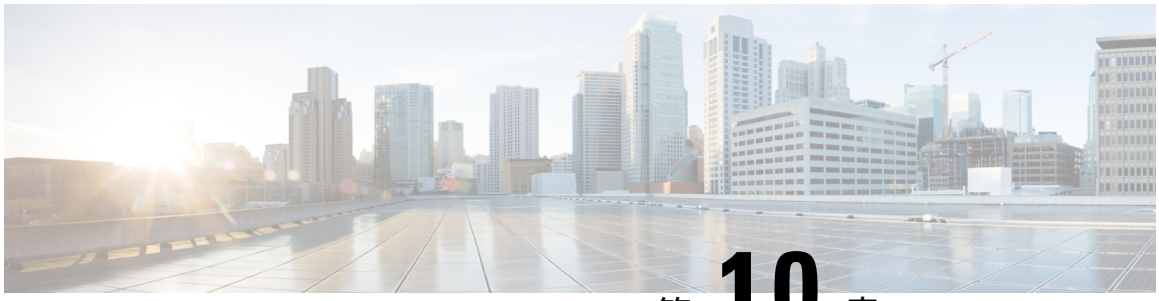
次のタスク

以下のインストールワークフローに戻ります。

- VMware：VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）
- AWS EC2：AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

第 V 部

Cisco NSO および SR-PCE の Cisco Crosswork Network Controller への統合



第 10 章

Cisco NSO の統合

この章は次のトピックで構成されています。

NSO の統合ワークフロー

このセクションでは、Cisco NSO を Crosswork Network Controller と統合するステップについて説明します。

1. 互換性のあるバージョンの Cisco NSO のインストール

互換性のあるバージョンの Cisco NSO がインストールされていることを確認します。

- VMware をお使いの場合は、NSO のドキュメント の指示に従ってください。
- AWS EC2 をお使いの場合は、Amazon EC2 への Cisco NSO のインストール （176 ページ）の手順に従ってください。

さらに、Cisco NSO LSA セットアップについては、（オプション）Cisco NSO Layered Service Architecture の設定 （214 ページ）を参照してください。

表 *53 : Cisco NSO* - 互換性のあるバージョン

ソフトウェア/ドライバ	バージョン
Cisco Network Services Orchestrator（Cisco NSO）	6.1

ソフトウェア/ドライバ	バージョン
Cisco Network Element Driver（NED） （注） Cisco NED は、管理しているデバイスタイプとバージョンに対してのみインストールする必要があります。たとえば、NETCONF を使用している場合は、IOS XR バージョンに対応する NED をインストールする必要があります。同様に、ネットワークに IOS デバイスがある場合は、Cisco IOS CLI NED をインストールする必要があります。	**Cisco IOS XR**： • CLI：7.46.3 • NETCONF：7.3.2、7.315、7.4.2、7.5.2、7.6.2、7.7.2、7.8、7.9 **Cisco IOS**： • CLI：6.86.6

2. 必須の NSO コア機能パックのインストール

使用中の Cisco Crosswork アプリケーションまたはソリューションに応じて、製品に互換性を持たせるために Cisco NSO にインストールする必要がある必須のコア機能パック（CFP）があります。

NSO コア機能パックは、次のように cisco.com にバンドルされています。

表 *54 : NSO* コア機能パック

パッケージ名	目次
Cisco Crosswork Network Controller Essential 機能パック **ファイル名**： cw-cnc-essential-fp-5.0.0-101-release-230503.tar.gz	• *Cisco NSO* トランスポート *SDN* 機能パックバンドル • *Cisco NSO DLM* サービスパック • *Cisco NSO Telemetry Traffic Collector* 機能パック
Cisco Crosswork Change Automation 機能パック **ファイル名**： *cw-ca-fp-5.0.0-5-release-230511.tar.gz*	• *Cisco Crosswork Change Automation NSO* 機能パック *4.4.0*

次のいずれかの方法を使用して、CFP をインストールできます。

- Ansible プレイブックを使用した Cisco NSO 機能パックのインストール （203 ページ）（推奨）
- 手動での Cisco NSO Function Pack のインストール （210 ページ）

（注） Cisco Crosswork Network Controller 機能パックの SDK アプリケーション（cw-na-platform-5.0.0-signed-tsdn-sdk.tar.gz）も cisco.com からダウンロードできます。SDK は、Crosswork Network Controller で TSDN 機能パックの開発、構築、パッケージ化、および展開に使用できるツールとソースコードの例を提供します。

3. NSO プロバイダーの追加と接続の確認

Cisco NSO プロバイダの追加 （211 ページ）の指示に従って操作します。

Ansible プレイブックを使用した Cisco NSO 機能パックのインストール

このセクションでは、Ansible プレイブックを使用して Cisco NSO コア機能パック（CFP）をインストールする方法について説明します。

Ansible プレイブックは、既存の NSO VM インスタンスに NSO CFP をインストールし、互換性のある NSO バージョンを実行します。プレイブックは、管理対象ノードとして NSO インスタンスを使用して Ansible コントローラから実行されます。この機能は、次の NSO 展開構成をサポートします。

- LSA （205 ページ）
- LSA HA（高可用性） （206 ページ）
- スタンドアロン （208 ページ）
- スタンドアロン HA（高可用性） （209 ページ）

インストールとアンインストールに必要なパラメータとスクリプトについては、それぞれの展開構成を参照してください。

CFP をインストールまたはアンインストールするには、次の手順を実行します。

始める前に

前提条件：

- CFP のクリーンインストールのみをサポートします。
- アップグレードはサポートされていません。
- NSO は、HA 構成とともに（展開要件に従って）すでにインストールされています。
- Ansible スクリプトは、すべての CFP パッケージ（トランスポート SDN（TSDN）、Change Automation（CA）、Device Lifecycle Management（DLM）、Telemetry Traffic Controller（TM-TC）とブートストラップ）をインストールします。

- LSA 構成には 3 つの VM（1 つの CFS ノードと 2 つの RFS ノード）が必要です。
- NSO は、システムインストールモード（ローカルインストールはサポートされていません）で、以下の標準の場所にインストールされます。
  - ncsdir：`/opt/ncs/current`
  - confdir：`/etc/ncs`
  - rundir：`/var/opt/ncs`
  - logdir：`/var/log/ncs`
- アップグレードがサポートされていないため、CFP がすでにインストールされていることを示す CFP パッケージ（`cisco-tsdn-core-fp-common` パッケージなど）が存在すると、インストールは失敗します。このメカニズムによって、機能している設定にパッケージを誤ってインストールすることを防ぐことができます。
- インストールに失敗した場合、または CFP を再インストールする場合は、最初にアンインストールスクリプトを実行して古いパッケージを削除（リンク解除）します。

前提条件：

- 最新の ansible および ansible プレイブックは、Ansible コントローラとして指定されたホストにインストールされます。
- CFP に必要な Java および Python バージョン（OpenJDK 11、python3）は、NSO VM にすでにインストールされています。
- HA 展開の場合、CFP インストールを実行する前に、Cisco Tail-f HCC（Tail-f High Availability Cluster Communications）パッケージがすでにインストールされ、構成され、動作している必要があります。

注意：

1. `ssh`、`netconf-north-bound`、または `webui transport` が以前に有効になっている場合、インストールを実行しても `dual-stack config` は追加されないため、手動で有効にする必要があります。次の構成を使用して、適切なポートで IPv6 リスナーを追加します。

```
<extra-listen>
      <ip>::</ip>
      <port>2024</port>
    </extra-listen>
```

2. アンインストールを開始する前に、CDB に追加されたすべてのサービスとデバイスを削除する必要があります。そうしないと、NSO はアップグレードプロセスを試行し、アンインストールが失敗します。
3. NSO インスタンスを Ansible コントローラとして使用して、それ自体に CFP をインストールしないでください。この展開構成はサポートされていません。

ステップ 1 NSO を構成するには、関連するパラメータを使用して `host` および `vars.yml` ファイルを編集します。

ステップ 2 CFP をインストールするには、インストールコマンドを実行します（詳細についてはそれぞれの展開構成を参照）。

例：

```
ansible-playbook -v -i hosts tsdn-lsa-ha-install.yml
```

CFP ファイルがインストールディレクトリ（`/opt/ncs/packages/`）にコピーされ、シンボリックリンクがランタイムディレクトリ（`/var/opt/ncs/packages/`）に作成されます。その後、パッケージを適用するために NSO が再起動されます。

ステップ 3 CFP をアンインストールするには、アンインストールコマンドを実行します（詳細についてはそれぞれの展開構成を参照）。

例：

```
ansible-playbook -v -i hosts tsdn-lsa-ha-uninstall.yml
```

シンボリックリンクはランタイムディレクトリで削除され、NSO は CFP パッケージなしで再起動されます。

次のタスク

以下のインストールワークフローに戻ります。

- VMware：VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）
- AWS EC2：AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

LSA

このプレイブックは、`vars.yml` ファイルに記述されているノードのロールに従って、CFP パッケージをインストールし、LSA クラスタを構成します。

Dir：lsa

インストール：`ansible-playbook -v -i hosts tsdn-lsa-install.yml`

アンインストール：`ansible-playbook -v -i hosts tsdn-lsa-uninstall.yml`

必須パラメータ：

ファイル：`lsa/vars.yml`

表 55 : LSA 展開構成に必要なパラメータ

パラメータ	説明
`ansible_user`	SSH ユーザ名

パラメータ	説明
ansible_ssh_pass	SSH パスワード
ansible_sudo_pass	sudo パスワード
nbi_port	NSO ノースバウンドインターフェイスの ポート（例：8888）
restconf_port	Restconf インターフェイスのポート（例：2022）
lsa_ned_id	NSO Netconf NED ID（例：cisco-nso-nc-6.1:cisco-nso-nc-6.1）
image_location	Ansible サーバー上の CFP パッケージの場所、Crosswork（例：/tmp/image）
tsdn_image	TSDN イメージ名（例：nso-6.1_230124-tsdn-5.0.0-M6）
ca_image	CA イメージ名（例：cw-na-fp-ca-5.0.0-nso-6.1）
dlm_image	DLM イメージ名（例：cw-na-dlm-fp-5.0.0-nso-6.1-eng）
tmtc_image	TM-TC イメージ名（例：cw-na-fp-tmtc-5.0.0-333-nso-6.1）
tmtc_internal	TM-TC の内部ディレクトリ名（例：TM-TC-5.0.0-333。これを取得するには、解凍する必要がある場合があります）
cli_ned_version	TM-TC に必要な IOS XR NED バージョン（例：7.45）
rfs_nodes	- name: rfs-1: ip: <RFS 1 IP address> - name: rfs-2: ip: <RFS 2 IP address> - name: rfs-x: ip: <RFS x IP address>

ファイル：lsa/hosts

```
[all]

[cfs_node]
10.0.0.2

[rfs_node]
10.0.0.3
10.0.0.4
10.0.0.x
```

host ファイルと vars.yml ファイルを準備したら、Ansible プレイブックを使用した Cisco NSO 機能パックのインストール（203ページ）の指示に従ってCFPのインストールを完了します。

LSA HA（高可用性）

このプレイブックは、vars.yml ファイルに記述されているノードのロールに従って、CFPパッケージをインストールし、LSA クラスタを構成します。

host ファイルと vars.yml ファイルを準備したら、Ansible プレイブックを使用した Cisco NSO 機能パックのインストール （203 ページ）の指示に従います。

Dir：lsa-ha

インストール：`ansible-playbook -v -i hosts lsa-ha-install.yml`

アンインストール：`ansible-playbook -v -i hosts lsa-ha-uninstall.yml`

必須パラメータ：

ファイル：`lsa-ha/vars.yml`

表 *56 : LSA HA* 展開の構成に必要なパラメータ

パラメータ	説明
ansible_user	SSH ユーザ名
ansible_ssh_pass	SSH パスワード
ansible_sudo_pass	sudo パスワード
nbi_port	NSO ノースバウンドインターフェイスのポート（例：8888）
restconf_port	Restconf インターフェイスのポート（例：2022）
lsa_ned_id	NSO Netconf NED ID（例：cisco-nso-nc-6.1:cisco-nso-nc-6.1）
image_location	Ansible サーバー上の CFP パッケージの場所、Crosswork（例：/tmp/image）
tsdn_image	TSDN イメージ名（例：nso-6.1_230124-tsdn-5.0.0-M6）
ca_image	CA イメージ名（例：cw-na-fp-ca-5.0.0-nso-6.1）
dlm_image	DLM イメージ名（例：cw-na-dlm-fp-5.0.0-nso-6.1-eng）
tmtc_image	TM-TC イメージ名（例：cw-na-fp-tmtc-5.0.0-333-nso-6.1）
tmtc_internal	TM-TC の内部ディレクトリ名（例：TM-TC-5.0.0-333。これを取得するには、解凍する必要がある場合があります）
cli_ned_version	TM-TC に必要な IOS XR NED バージョン（例：7.45）
rfs_nodes	- name: rfs-1: ip: <RFS 1 IP address> - name: rfs-2: ip: <RFS 2 IP address> - name: rfs-x: ip: <RFS x IP address>

ファイル：`lsa-ha/hosts`

```
[all]

[cfs_primary]
10.0.0.2

[cfs_secondary]
10.0.0.3

[rfs1_primary]
10.0.0.4

[rfs1_secondary]
10.0.0.5

[rfs2_primary]
10.0.0.7

[rfs2_secondary]
10.0.0.8

[rfsx_primary]
10.0.0.x1

[rfsx_secondary]
10.0.0.x2
```

`host` ファイルと `vars.yml` ファイルを準備したら、Ansible プレイブックを使用した Cisco NSO 機能パックのインストール（203ページ）の指示に従ってCFPのインストールを完了します。

スタンドアロン

このプレイブックは、CFP パッケージをスタンドアロン NSO ノードにインストールします。

Dir：standalone

インストール：`ansible-playbook -v -i hosts standalone-install.yml`

アンインストール：`ansible-playbook -v -i hosts standalone-uninstall.yml`

必須パラメータ：

ファイル：`standalone/vars.yml`

表 *57:* スタンドアロン展開の構成に必要なパラメータ

パラメータ	説明
`ansible_user`	SSH ユーザ名
`ansible_ssh_pass`	SSH パスワード
`ansible_sudo_pass`	sudo パスワード
`nbi_port`	NSO ノースバウンドインターフェイスのポート（例：8888）

パラメータ	説明
image_location	Ansible サーバー上の CFP パッケージの場所、Crosswork（例：/tmp/image）
tsdn_image	TSDN イメージ名（例：nso-6.1_230124-tsdn-5.0.0-M6）
ca_image	CA イメージ名（例：cw-na-fp-ca-5.0.0-nso-6.1）
dlm_image	DLM イメージ名（例：cw-na-dlm-fp-5.0.0-nso-6.1-eng）
tmtc_image	TM-TC イメージ名（例：cw-na-fp-tmtc-5.0.0-333-nso-6.1）
tmtc_internal	TM-TC の内部ディレクトリ名（例：TM-TC-5.0.0-333。これを取得するには、解凍する必要がある場合があります）
cli_ned_version	TM-TC に必要な IOS XR NED バージョン（例：7.45）

ファイル：standalone/hosts

```
[all]
10.0.0.2
```

hosts ファイルと vars.yml ファイルを準備したら、Ansible プレイブックを使用した Cisco NSO 機能パックのインストール（203 ページ）の指示に従って CFP のインストールを完了します。

スタンドアロン HA（高可用性）

このプレイブックは、vars.yml ファイルで説明されているように、HA 構成の NSO ノードに CFP パッケージをインストールします。

HA 展開の場合、CFP インストールを実行する前に、Cisco Tail-f HCC（Tail-f High Availability Cluster Communications）パッケージがすでにインストールされ、構成され、動作している必要があります。

Dir：ha

インストール：`ansible-playbook -v -i hosts ha-install.yml`

アンインストール：`ansible-playbook -v -i hosts ha-uninstall.yml`

必須パラメータ：

ファイル：ha/vars.yml

表 *58*：スタンドアロン *HA* 展開の構成に必要なパラメータ

パラメータ	説明
ansible_user	SSH ユーザ名
ansible_ssh_pass	SSH パスワード

パラメータ	説明
ansible_sudo_pass	sudo パスワード
nbi_port	NSO ノースバウンドインターフェイスのポート（例：8888）
image_location	Ansible サーバー上の CFP パッケージの場所、Crosswork（例：/tmp/image）
tsdn_image	TSDN イメージ名（例：nso-6.1_230124-tsdn-5.0.0-M6）
ca_image	CA イメージ名（例：cw-na-fp-ca-5.0.0-nso-6.1）
dlm_image	DLM イメージ名（例：cw-na-dlm-fp-5.0.0-nso-6.1-eng）
tmtc_image	TM-TC イメージ名（例：cw-na-fp-tmtc-5.0.0-333-nso-6.1）
tmtc_internal	TM-TC の内部ディレクトリ名（例：TM-TC-5.0.0-333。これを取得するには、解凍する必要がある場合があります）
cli_ned_version	TM-TC に必要な IOS XR NED バージョン（例：7.45）
vip_ip	仮想 IP アドレス
primary_node_ip	プライマリノードの IP アドレス
secondary_node_ip	セカンダリノードの IP アドレス

ファイル：ha/hosts

```
[all]

[primary_node]
  10.0.0.2

[secondary_node]
  10.0.0.3
```

hosts ファイルと vars.yml ファイルを準備したら、Ansible プレイブックを使用した Cisco NSO 機能パックのインストール（203 ページ）の指示に従ってCFPのインストールを完了します。

手動での Cisco NSO Function Pack のインストール

個々の機能パックを手動でインストールする必要がある場合は、以下の表の関連する手順に従ってください。

表 *59* : 必須の機能パックのリスト

Crosswork 製品	必要な機能パックのドキュメント
Crosswork Network Controller Essentials または Crosswork Network Controller Advantage	• *Cisco NSO Transport SDN Function Pack Bundle 5.0.0 User Guide* • *Cisco NSO Transport SDN Function Pack Bundle 5.0.0 Installation Guide* • *Cisco Network Services Orchestrator DLM Service Pack 5.0.0 Installation Guide* • *Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 5.0.0 Installation Guide* • *Cisco Crosswork Change Automation NSO Function Pack 5.0.0 Installation Guide*
Crosswork Optimization Engine（スタンドアロン）	• *Cisco Network Services Orchestrator DLM Service Pack 5.0.0 Installation Guide* • *Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 5.0.0 Installation Guide*

Cisco NSO プロバイダの追加

Cisco Network Services Orchestrator（Cisco NSO）プロバイダは次の機能を提供します。

- Cisco Crosswork アプリケーションへのネットワークサービスとデバイス設定サービス。
- デバイス管理サービスと設定メンテナンスサービス。

（注） Crosswork は、Cisco NSO Layered Service Architecture（LSA）展開をサポートしています。LSA 展開は、すべてのサービスを含む顧客向けサービス（CFS）NSO として機能する複数の NSO プロバイダーと、デバイスを含むリソース向けサービス（RFS）から構成されます。Crosswork は、NSO プロバイダーを CFS または RFS として自動的に識別します。許可される CFS は 1 つだけです。[マネージャ プロバイダー アクセス（Manager Provider Access）] ページの [タイプ（Type）] 列は、NSO プロバイダーを CFS として識別します。

（注） Cisco NSO 機能パックのサンプルは、Cisco Crosswork Network Controller の VPN サービスプロビジョニング機能の出発点として提供されます。これらのサンプルは、一部の限定されたネットワーク設定では「そのまま」使用できますが、Cisco Crosswork Network Controller の拡張可能な設計を示すことを意図としています。一般的な質問への回答は Cisco Devnet で確認できます。シスコ カスタマー エクスペリエンスの担当者は、サンプルに関する一般的な質問への回答を提供できます。特定のユースケースに合わせたサンプルのカスタマイズについては、シスコアカウントチームを通じてサポートを提供いたします。

始める前に

必要な作業は次のとおりです。

- Cisco NSO プロバイダーのクレデンシャルプロファイルを作成します。
- Cisco NSO プロバイダに割り当てる名前を確認します。
- トポロジで使用する Cisco NSO NED デバイスモデルとドライババージョンを確認します。

（注） `version` コマンドを使用して Cisco NSO のバージョンを検索できます。次に例を示します。

```
admin@ncs# show ncs-state version
ncs-state version 6.1
```

- Cisco NSO サーバーの IP アドレスとホスト名を確認します。NSO が HA で設定されている場合、IP アドレスは管理 VIP アドレスになります。
- Cisco NSO デバイスの設定を確認します。

UI から Cisco NSO プロバイダを追加するには、次の手順を実行します。すべてのプロバイダーの詳細を含む CSV ファイルを作成して Crosswork にインポートすることで、複数のプロバイダーを同時にインポートできることに注意してください。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋をクリックします。

ステップ 3 Cisco NSO プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：プロバイダの名前を入力します。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成した Cisco NSO のクレデンシャルプロファイルを選択します。

- [ファミリ（Family）]：[NSO] を選択します。
- [接続タイプ（Connection Type(s)）] の [プロトコル（Protocol）] で、Cisco Crosswork アプリケーションがプロバイダへの接続に使用するプロトコルを選択します。 通常は **HTTPS** が優先されます。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：Cisco NSO サーバーの IP アドレスサブネットマスクを入力します。

  重要 NSO プロバイダーの IP アドレスまたは FQDN を変更または更新する場合は、対応する仮想データゲートウェイからデバイスを切断し、再接続する必要があります。これを行わないと、プロバイダーの変更は MDT 収集ジョブに反映されません。

- [ポート（Port）]：HTTPS の場合、HTTPS を使用して NSO にアクセスするには、etc/ncs/ncs.conf で NSO VM の設定と一致するポートを入力します。NSO ではデフォルトポートとして 8888 を使用します。
- [モデル（Model）]：ドロップダウンリストからモデル（[Cisco-IOS-XR]、[Cisco-NX-OS]、または [Cisco-IOS-XE]）を選択し、関連付けられている NED ドライババージョンを入力します。トポロジで使用するデバイスのタイプごとにモデルを追加します。複数ある場合は、サポートされている別のモデルを追加します。
- [バージョン（Version）]：NSO のデバイスモデルにインストールされている NED ソフトウェアバージョンを入力します。

b) オプション値：

- [タイムアウト（Timeout）]：Cisco NSO サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 [プロバイダプロパティ（Provider Properties）] で、[プロパティキー（Property Key）] に **forward** 、[プロパティ値（Property Value）] に **true** と入力します。このプロパティは、Cisco Crosswork ネットワークコントローラ ソリューションを使用して UI 内でプロビジョニング操作をできるようにし、Crosswork API ゲートウェイを介して NSO へのノースバウンド インターフェイスを有効にする場合に必要です。

（注） Cisco Crosswork には、NSO アプリケーションを Crosswork UI から相互起動するオプションがあります（この機能は、読み取り専用権限を持つユーザーロールでは使用できません）。相互起動機能を有効にするには、次のいずれかの設定で Cisco NSO をプロバイダとして追加します。

- **Property Key nso_crosslaunch_url** では、[プロパティーキー（Property Key）] フィールドに有効な URL が入力されています。
- プロトコルは **HTTP** か **HTTPS** で、プロバイダは到達可能です。

上記の設定のいずれかが存在する場合、相互起動アイコン（ ）が [プロバイダ名（Provider Name）]列に表示されます。または、ウィンドウの右上隅にある起動アイコンを使用して、NSO アプリケーションを相互起動することができます。

ステップ 5 すべての必須フィールドに入力したら、[保存（Save）] をクリックしてプロバイダとして Cisco NSO を追加します。

ステップ 6 [プロバイダー（Providers）] ウィンドウで、作成した NSO プロバイダーを選択し、**[アクション（Actions）]** > **[ポリシーの詳細の編集（Edit Policy Details）]** をクリックします。

選択した NSO プロバイダーの [ポリシーの詳細の編集（Edit Policy Details）] ウィンドウが表示されます。

ステップ 7 環境の要件に合わせて構成フィールドを編集します。[保存（Save）] をクリックして変更を保存します。

次のタスク

以下のインストールワークフローに戻ります。

- VMware：VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）
- AWS EC2：AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

（オプション）Cisco NSO Layered Service Architecture の設定

このセクションは、Cisco NSO Layered Service Architecture（LSA）展開を選択した場合にのみ適用されます。

Cisco NSO LSA を使用すると、任意の数のデバイスノードを追加して、メモリとプロビジョニングのスループットを向上させることができます。大規模なサービスプロバイダーまたは企業は、Cisco NSO を使用して、数十万を超える管理対象デバイスに及ぶ、数百万の加入者またはユーザーのサービスを管理しています。これを実現するには、LSA と呼ばれる階層化された方法でサービスを設計できます。

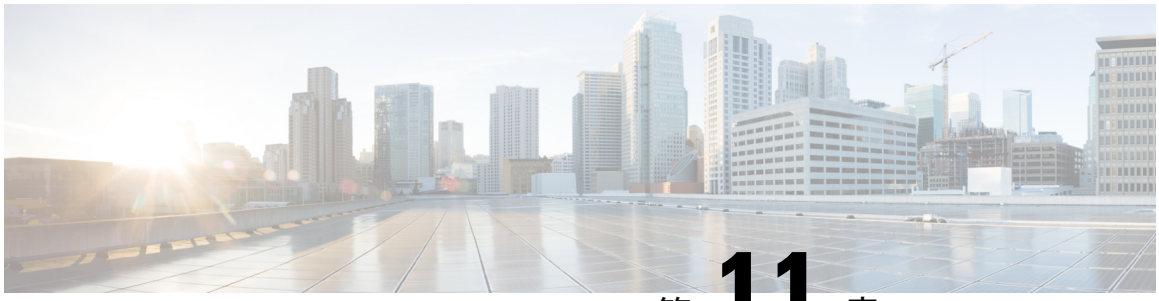
Cisco Crosswork Network Controller を大規模な顧客向けに位置付けるために、このソリューションは既存の Cisco NSO LSA アーキテクチャと互換性があります。

次の手順に従って、Cisco NSO LSA をいつ使用するかを決定します。

1. 展開がスタンドアロンか Cisco NSO LSA かを確認します。
2. 展開がスタンドアロンの場合は、使用可能な最大メモリを確認します。使用可能な最大メモリが現在のメモリ状態よりも多い場合は、Cisco NSO LSA を展開する必要があります。

（注） スタンドアロン展開から Cisco NSO LSA 展開への移行は、現在サポートされていません。

Cisco NSO LSA の詳細情報を取得し、Cisco NSO LSA を設定するには、「NSO Layered Service Architecture」を参照してください。



第 11 章

SR-PCE の統合

この章は次のトピックで構成されています。

SR-PCE 統合ワークフロー

このセクションでは、Cisco SR-PCE を Crosswork Network Controller と統合するステップについて説明します。

SR-PCE の互換バージョンは Cisco IOS XR 7.9.1 です。

1. 互換性のあるバージョンの Cisco SR-PCE のインストール

SR-PCE のタイプ（VMware ESXi または AWS の場合）を選択し、『Cisco IOS XRv 9000 Router Installation Guide』の関連するインストール手順に従います。 。

2. SR-PCE の設定

その場合は、SR-PCE の設定 （217 ページ）の手順に従ってください。

3. SR-PCE プロバイダーの追加と接続の確認

Cisco SR-PCE プロバイダの追加 （220 ページ）の指示に従って操作します。

SR-PCE の設定

このセクションでは、SR-PCE をインストールした後に構成する方法について説明します。

（注） Cisco IOS XRv 9000 は、SR-PCE として機能する推奨プラットフォームです。

表 *60 : SR-PCE* の設定

ステップ	コマンドまたはアクション	説明
1	**configure** 例： `RP/0/RP0/CPU0:router# configure`	モードを開始します。
2	**pce** 例： `RP/0/RP0/CPU0:router(config)# pce`	PCE を有効にし、PCE コンフィギュレーション モードを開始します。
3	**address ipv4** *address* 例： `RP/0/RP0/CPU0:router(config-pce)# address ipv4 192.168.0.1`	PCE IPv4 アドレスを設定します。
4	**state-sync ipv4** *address* 例： `RP/0/RP0/CPU0:router(config-pce)# state-sync ipv4 192.168.0.3`	リモート ピアに状態同期を設定します。
5	**tcp-buffer size** *size* 例： `RP/0/RP0/CPU0:router(config-pce)# tcp-buffer size 1024000`	各 PCEP セッションの送受信 TCP バッファ サイズをバイト単位で設定します。デフォルトのバッファ サイズは 256000 です。有効な範囲は 204800 ～ 1024000 です。
6	**password** {**clear** | **encrypted**} *password* 例： `RP/0/RP0/CPU0:router(config-pce)# password encrypted pwd1`	すべての PCEP ピアの TCP MD5 認証を有効にします。設定されたパスワードと一致する MAC を含まない PCC から来る TCP セグメントはすべて拒否されます。パスワードが暗号化されているか、またはクリア テキストであるかを指定します。 （注） TCP-AO と TCP MD5 を同時に使用することはできません。

ステップ	コマンドまたはアクション	説明
7	**tcp-ao** *key-chain* [**include-tcp-options**] [**accept-ao-mismatch-connection**] 例： `RP/0/RP0/CPU0:router(config-pce)# tcp-ao pce_tcp_ao include-tcp-options`	すべての PCEP ピアの TCP 認証オプション（TCP-AO）の認証を有効にします。設定されたキーチェーンと一致する MAC を含まない PCC から来る TCP セグメントはすべて拒否されます。 • **include-tcp-options**：MAC 計算用のヘッダーに他の TCP オプションを含めます。 • **accept-ao-mismatch-connection**：ピア間で AO オプションの不一致がある場合でも、接続を受け入れます。 （注） TCP-AO と TCP MD5 を同時に使用することはできません。
8	**segment-routing** {**strict-sid-only** | **te-latency**} 例： `RP/0/RP0/CPU0:router(config-pce)# segment-routing strict-sid-only`	厳格な SID または TE のレイテンシを使用するようにセグメント ルーティング アルゴリズムを設定します。 （注） この設定はグローバルで、このコントローラからパスを要求するすべての LSP に適用されます。
9	**timers** 例： `RP/0/RP0/CPU0:router(config-pce)# timers`	タイマー コンフィギュレーション モードを開始します。
10	**keepalive** *time* 例： `RP/0/RP0/CPU0:router(config-pce-timers)# keepalive 60`	ローカルで生成されたキープアライブ メッセージのタイマー値を設定します。デフォルトの時間は 30 秒です。
11	**minimum-peer-keepalive** *time* 例： `RP/0/RP0/CPU0:router(config-pce-timers)# minimum-peer-keepalive 30`	セッション確立中にリモート ピアが PCEP OPEN メッセージで提案できる最小の許容キープアライブ タイマーを設定します。デフォルトの時間は 20 秒です。

ステップ	コマンドまたはアクション	説明
12	**reoptimization** *time* 例： `RP/0/RP0/CPU0:router(config-pce-timers)# reoptimization 600`	再最適化タイマーを設定します。デフォルトのタイマーは 1,800 秒です。
13	**exit** 例： `RP/0/RP0/CPU0:router(config-pce-timers)# exit`	タイマー コンフィギュレーション モードを終了し、PCE コンフィギュレーション モードに戻ります。

次に行う作業：

以下のインストールワークフローに戻ります。

- VMware：VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）
- AWS EC2：AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

SR-PCE の設定例

これは SR-PCE の設定例です。

```
pce
address ipv4 1.1.1.98
api
  user cisco                                {This is the username and password that the
credential profile used for the PCE will need to have for HTTP}
   password encrypted 032752180500701E1D48
!
```

Cisco SR-PCE プロバイダの追加

Cisco セグメント ルーティング パス計算要素（Cisco SR-PCE）プロバイダは、デバイス検出、管理、設定メンテナンス、およびルート計算サービスを Cisco Crosswork アプリケーションに提供します。SR ポリシー、レイヤ 3 リンク、およびデバイスを学習および検出するには、少なくとも 1 つの SR-PCE プロバイダーが必要です。2 番目の SR-PCE をバックアップとして設定するオプションがあります。Crosswork ネットワークコントローラ が複数のドメインの管理をサポートしていないため、両方の SR-PCE デバイスを同じネットワークに接続する必要があります。

（注） 管理ドメインの SDN コントローラとして SR-PCE への Cisco Crosswork アプリケーションアクセスを有効にするには、SR-PCE をプロバイダとして追加する必要があります。

Cisco SR-PCE の 1 つ以上のインスタンスを（UI を介して）プロバイダとしての追加するには、次の手順を実行します。

始める前に

必要な作業は次のとおりです。

- SR-PCE として機能するようにデバイスを設定します。特定のデバイスプラットフォームの SR 設定ドキュメントを参照して、SR を有効にし（IS-IS または OSPF プロトコルの場合）、SR-PCE を設定します（例：Cisco NCS 540 シリーズ ルータのセグメントルーティング設定ガイド）。
- Cisco SR-PCE プロバイダーのクレデンシャルプロファイルを作成します。これは、基本的な HTTP テキスト認証クレデンシャルである必要があります（現在、MD5 認証はサポートされていません）。追加する Cisco SR-PCE サーバーが認証を必要としない場合でも、プロバイダのクレデンシャルプロファイルを指定する必要がありますが、HTTP プロトコルを使用しない任意のプロファイルを指定できます。
- Cisco SR-PCE プロバイダに割り当てる名前を確認します。通常、これは Cisco SR-PCE サーバーの DNS ホスト名です。
- Cisco SR-PCE サーバーの IP アドレスを確認します。
- Cisco SR-PCE と Cisco Crosswork アプリケーションサーバー間の通信に使用するインターフェイスを確認します。
- Cisco SR-PCE が検出するデバイスを自動でオンボーディングするかどうか、また、その場合は新しいデバイスの追加時にその管理ステータスを **off**、**managed**、または **unmanaged** にするかどうかを決定します。
- Cisco SR-PCE プロバイダが検出する自動オンボーディングデバイスを予定し、それらをデータベースに追加するときに管理対象の状態に設定する場合は、次の手順を実行します。
  - 新しい管理対象デバイスとの通信用に既存のクレデンシャルプロファイルを割り当てます。
  - クレデンシャルプロファイルは、SNMP プロトコルを使用して設定する必要があります。
- 高可用性を実現するには、一意の名前と IP アドレスを使用し、設定が一致する 2 つの個別の Cisco SR-PCE プロバイダーを設定します。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋をクリックします。

ステップ 3 SR-PCE プロバイダのフィールドに次の値を入力します。

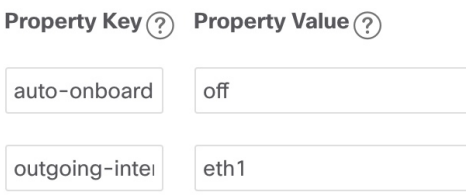
a) 必須フィールド：

- [プロバイダ名（Provider Name）]：SR-PCE プロバイダの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成した Cisco SR-PCE のクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[SR_PCE] を選択します。他のすべてのオプションは無視する必要があります。
- [プロトコル（Protocol）]：[HTTP] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号として **8080** を入力します。
- [プロバイダプロパティ（Provider Properties）]：最初のフィールドセットに、次のキー/値ペアのいずれかを入力します。

プロパティキー	値
auto-onboard	**off** （注） すべてのネットワークデバイスを手動で（UI または CSV インポート経由で）入力する場合は、このオプションを使用します。 デバイスが検出されると、デバイスデータは Cisco SR-PCE データベースに記録されますが、Cisco Crosswork インベントリ管理データベースには登録されません。
auto-onboard	**unmanaged** このオプションを有効にすると、Cisco Crosswork が検出するすべてのデバイスが Cisco Crosswork インベントリ管理データベースに登録され、設定済みの状態が **unmanaged** に設定されます。これらのデバイスの SNMP ポーリングが無効になり、管理 IP 情報は含められません。これらのデバイスを後で **managed** の状態にするには、UI を使用してデバイスを編集するか、CSV にエクスポートして変更を加え、更新した CSV をインポートする必要があります。インポート前にデバイス CSV ファイルに追加することによって、クレデンシャルプロファイルを割り当てることもできます（クレデンシャルプロファイルはすでに存在している必要があります）。

プロパティキー	値
auto-onboard	**managed** このオプションを有効にすると、Cisco SR-PCE が検出するすべてのデバイスが Cisco Crosswork インベントリ管理データベースに登録され、設定済みの状態が **managed** に設定されます。これらのデバイスに対して SNMP ポーリングが有効になり、Cisco SR-PCE は管理 IP アドレス（IPv4 の場合は TE ルータ ID、IPv6 展開の場合は IPv6 ルータ ID）も報告します。デバイスは、SR-PCE プロバイダ設定のデバイスプロファイルキーに関連付けられたクレデンシャルプロファイルを使用して追加されます。
device-profile	すべての新しいデバイスの SNMP クレデンシャルが含まれているクレデンシャルプロファイルの名前。 （注） このフィールドは、**auto-onboard** が **managed** または **unmanaged** に設定されている場合にのみ必要です。
outgoing-interface	**eth1** （注） 2 つの NIC 設定を使用する場合に、データ ネットワーク インターフェイスを介して Cisco Crosswork アプリケーションが SR-PCE にアクセスできるようにする場合にのみ、これを設定する必要があります。
topology	**off** または **on**。 これはオプションのプロパティです。指定しない場合、デフォルト値は **on** です。 値を **off** に指定している場合は、SR-PCE プロバイダが L3 トポロジにアクセスできないことを意味します。
pce	**off** または **on**。 これはオプションのプロパティです。指定しない場合、デフォルト値は **on** です。 値を **off** に指定している場合は、SR-PCE プロバイダが LSP とポリシーにアクセスできないことを意味します。

図 *32 :* プロバイダープロパティのキーと値の例



（注） [管理対象（managed）] または [管理対象外（unmanaged）] のオプションが設定されていて、後でデバイスを削除する場合は、次のいずれかを実行する必要があります。

- Cisco Crosswork からデバイスを削除する前に、ネットワークからデバイスを再設定して削除します。これにより、Cisco Crosswork がデバイスを再検出して追加しないようにします。
- auto-onboard を **off** に設定してから、デバイスを Cisco Crosswork から削除します。ただし、これを行うと、Cisco Crosswork はネットワーク内の新しいデバイスを検出または自動オンボーディングできなくなります。

b) オプション値：

- [タイムアウト（Timeout）]：SR-PCE サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックして SR-PCE プロバイダを追加します。

ステップ 5 SR-PCE プロバイダにエラーのない緑色の到達可能性ステータスが表示されていることを確認します。[イベント（Events）] ウィンドウ（**[管理（Administration）]** > **[イベント（Events）]**）を表示して、プロバイダが正しく設定されているかどうかを確認することもできます。

ステップ 6 SR-PCE プロバイダごとにこのプロセスを繰り返します。

（注） 一度設定した自動オンボーディングオプションを変更することは推奨されません。これらを変更する必要がある場合は、次の手順を実行します。

1. プロバイダを削除し、[イベント（Events）] ウィンドウに削除の確認が表示されるまで待ちます。
2. 更新した自動オンボーディングオプションでプロバイダを再追加します。
3. [イベント（Events）] ウィンドウで、正しい自動オンボーディングオプションを使用してプロバイダが追加されたことを確認します。

次のタスク

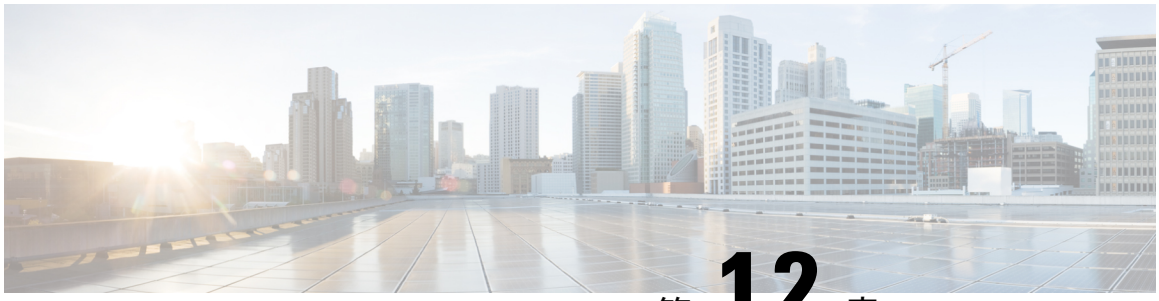
- **`auto-onboard`/`off`** ペアの場合は、**[デバイス管理（Device Management）]** > **[ネットワークデバイス（ Network Devices）]** に移動してデバイスを追加します。
- 自動的にデバイスをオンボーディングする選択をした場合は、**[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** に移動してデバイスリストを表示します。地理的な場所の詳細などのノード情報の詳細を追加するには、デバイスリスト（.csv）をエクスポートし、更新してからインポートします。地理的な場所データが欠落している場合は、論理マップを使用してのみデバイストポロジを表示できます。

以下のインストールワークフローに戻ります。

- VMware：VMware vCenter への Cisco Crosswork Network Controller のインストール （13 ページ）
- AWS EC2：AWS EC2 への Cisco Crosswork Network Controller のインストール （16 ページ）

第 VI 部

Cisco Crosswork Network Controller のアップグレード



第 12 章

Cisco Crosswork のアップグレード

この章は次のトピックで構成されています。

アップグレードの概要

このセクションでは、最新バージョンの Cisco Crosswork Network Controller にアップグレードするための概要を示します。このワークフローには、単一のメンテナンスウィンドウ内での Cisco Crosswork クラスタ、Cisco Crosswork Data Gateway、および Crosswork アプリケーションのアップグレード作業が含まれます。

次の方法で Cisco Crosswork をアップグレードできます。

1. 既存のハードウェアを使用したアップグレード （232 ページ）
2. 並列ハードウェアを使用したアップグレード （245 ページ）

アップグレードの最終的な所要時間は、展開プロファイルのサイズとハードウェアのパフォーマンス特性によって異なることがあります。

警告 Cisco Crosswork の以前のバージョンからの移行には、次の制限があります。

- ライセンスタグは、アップグレード操作の一部として自動登録されません。アップグレード後に手動で登録する必要があります。
- デバイスライフサイクル管理（DLM）およびCisco NSOに含まれるサードパーティ製デバイスの設定は移行されないため、移行後に新しい Cisco Crosswork バージョンでその設定を再適用する必要があります。
- Cisco Crosswork の以前のバージョンで作成されたカスタムユーザーロール（読み取り/書き込み、読み取り）は移行されないため、移行後に新しいバージョンで手動更新する必要があります。
- Cisco Crossworkの以前のバージョンで管理者権限を持つすべてのユーザーロールが、アップグレード後も引き続き管理者ユーザーとなるように、それらのユーザーロールに新しい権限を割り当てる必要があります。
- Crosswork Health Insights KPI アラート履歴が移行の一環として取得されることはありません。
- 移行が成功したら、システムの使用を続行する前に、ハードリフレッシュまたはブラウザキャッシュの削除を実行する必要があります。この手順を実行しないと、データの不一致が発生する可能性があります。

Crosswork アプリケーションは、マイナーアップデートまたはパッチリリースの場合、Cisco Crosswork UIから個別に更新できます。詳細については、Crosswork アプリケーションの更新（スタンドアロン アクティビティ） （254 ページ）を参照してください。

アップグレード要件

このセクションでは、Crosswork Optimization Engine を使用している場合に Cisco Crosswork をアップグレードするための要件について説明します。

Crosswork Optimization Engine の以前のバージョンで機能パック（LCM、帯域幅最適化、またはBWoD）を有効にしていて、最新バージョンにアップグレードする場合は、アップグレードする前に次のタスクを実行する必要があります。

LCM

- LCM の [構成（Configuration）] ページから、次の手順を実行します。

1. [無効化されたときに戦術的SRポリシーを削除（Delete Tactical SR Policies when Disabled）] オプションを [False] に設定します。このタスクは、LCM によって展開された戦術ポリシーがアップグレード後もネットワークに残るように、LCMを無効にする前に実行する必要があります。

2. [有効（Enable）] オプションを [False] に設定します。LCM が有効なままの場合、アップグレード後に戦術ポリシーが削除される可能性があります。
3. アップグレード後に同じ構成が移行されたことを確認できるように、LCM の [構成（Configuration）] ページのすべてのオプション（[基本（Basic）] および [詳細設定（Advanced）]）をメモしてください。

- LCMによって管理されているインターフェイスの現在のリストをエクスポートします（[トラフィックエンジニアリング（Traffic Engineering）]>[ローカル輻輳緩和（Local Congestion Mitigation）]>[エクスポート（Export）] アイコン）。CSV ファイルをエラーなしで再インポートして、インターフェイスが有効であることを確認します。詳細については、『Cisco Crosswork Optimization Engine 5.0 User Guide』の「Add Individual Interface Thresholds」を参照してください。
- アップグレード後、[トラフィックエンジニアリング（Traffic Engineering）] ページにすべてのノードとリンクが表示されるまで待ってから、LCM を有効にします。

（注）：

システムが安定した後、LCM に対してドメインを有効にする前に、以前にモニターしていたインターフェイスの移行が完了したこと、および各ドメインに必要な構成オプションがあることを確認します。

1. [管理（Administration）]>[アラーム（Alarms）]>[すべて（All）]>[イベント（Events）] に移動し、**LCM** と入力して [送信元（Source）] 列をフィルタリングします。
2. 次のイベントを探します：「移行が完了しました。移行されたすべてのLCMインターフェイスとポリシーは、IGPドメインにマップされます（Migration complete. All migrated LCM interfaces and policies are mapped to their IGP domains）」。このメッセージが表示されない場合、（LCM の [構成（Configuration）] ページで設定される）[輻輳確認間隔（Congestion Check Interval）] の期間待ってから、LCM を再起動します（**[管理（Administration）] > [Crossworkマネージャ（Crosswork Manager）] > [Optimization Engine] > [optima-lcm] > ... > [再起動（Restart）]**）
3. optima-lcm サービスが [低下（Degraded）] から [正常（Healthy）] 状態に変わるまで待ちます。
4. ドメインごとに [構成（Configuration）] ページに移動し、オプションが正常に移行されたことを確認します。ドメイン構成が正しくない場合、LCM を再起動します（[管理（Administration）]>[Crossworkマネージャ（Crosswork Manager）]>[Optimization Engine]>[optima-lcm]>...>[再起動（Restart）]）
5. 前述のイベントの [イベント（Events）] ページと [構成（Configuration）] ページを確認して、オプションを確認します。

（注）
- 確認メッセージが表示されない場合、またはドメイン構成オプションが正しくない場合は、シスコのテクニカルサポートに問い合わせて、showtech の情報とエクスポートされたリンク管理 CSV ファイルを提供してください。
- システムが安定した後に、以前にモニターされていた欠落しているインターフェイスを手動で追加することや、ドメイン構成オプションを更新することもできます。

BWoD

- [有効（Enable）] オプションを [False] に設定します。BWoD が有効なままの場合、アップグレード後に戦術ポリシーが削除される可能性があります。
- アップグレード後に同じ構成が移行されたことを確認できるように、BWoD の [構成（Configuration）] ページのすべてのオプション（[基本（Basic）] および [詳細設定（Advanced）]）をメモしてください。
- アップグレード後、[トラフィックエンジニアリング（Traffic Engineering）] ページにすべてのノードとリンクが表示されるまで待ってから、BWoD を有効にします。

既存のハードウェアを使用したアップグレード

このセクションでは、既存のクラスタを使用して Crosswork Network Controller の最新バージョンに移行する方法について説明します。

このアップグレードワークフローの各段階は、順番に実行する必要があります。詳細については、この章の後のセクションで説明します。ポリシーの段階は次のとおりです。

1. Cisco Crosswork Data Gateway VM のシャットダウン （233 ページ）
2. Cisco Crosswork のバックアップ作成とシャットダウン （234 ページ）
3. 最新バージョンの Cisco Crosswork クラスタのインストール （237 ページ）

（注） クラスタのインストール中に、NSO をバージョン 6.1 にアップグレードする必要があります。NSO をアップグレードするプロセスについては、このドキュメントでは扱われません。詳細については、関連する Cisco NSO のドキュメントを参照してください。また、SR-PCE をバージョン 7.7.1 にアップグレードする必要もあります。インストール手順については、『Cisco IOS XRv 9000 Router Installation Guide』を参照してください。。

4. Cisco Crosswork アプリケーションのインストール （238 ページ）

（注） 実際のアップグレードプロセスを開始する前に、アプリケーションのCAPPファイル（「Install Crosswork Applications」を参照）をダウンロードして検証することをお勧めします。これにより、アップグレードプロセスの途中でCAPPファイルをダウンロードするのとは対照的に、システムのダウンタイムが短縮されます。

5. Cisco Crosswork のバックアップの移行 （238 ページ）
6. Crosswork Data Gateway のアップグレード （240 ページ）
7. アップグレード後のチェックリスト （243 ページ）

Cisco Crosswork Data Gateway VM のシャットダウン

これはアップグレードワークフローの最初の段階です。

（注） Crosswork Data Gateway VM がシャットダウンされると、データがデータ送信先に転送されなくなります。アプリケーションプロバイダに問い合わせて、アラームやその他の問題を回避するための操作が必要かどうかを確認します。

始める前に

[Data Gateway管理（Data Gateway Management）] ページのすべてのタブのスクリーンショットを撮り、Crosswork Data Gateway のリストと、Cisco Crosswork UI の [接続デバイス数（Attached Device Count）] を記録します。[プール（Pools）] タブで、リストに表示されているプールごとに、プール内のアクティブ、スペア、および未割り当ての VM をメモします。この情報は Crosswork Data Gateway のアップグレード （240 ページ） の際に役立ちます。

ステップ 1 すべての VM が正常であり、クラスタ内で実行されていることを確認します。

ステップ 2 Crosswork Data Gateway VM をシャットダウンします。

a) Crosswork Data Gateway VM にログインします。「SSH による Crosswork Data Gateway VM へのアクセス （121 ページ）」を参照してください。

正常にログインすると、Crosswork Data Gateway がインタラクティブコンソールを起動します。

b) [5 Troubleshooting] を選択します。

c) [Troubleshooting] メニューから [5 Shutdown VM] を選択して、VM をシャットダウンします。

Cisco Crosswork のバックアップ作成とシャットダウン

これはアップグレードワークフローの第 2 段階です。現在のバージョンの Cisco Crosswork を新しいバージョンにアップグレードする場合は、バックアップの作成が前提条件となります。

（注） バックアップは、スケジュールされたアップグレード期間中にのみ作成することを推奨します。バックアップ操作の実行中は、Cisco Crosswork へのアクセスを試みないでください。

始める前に

バックアップを作成する場合は、次のガイドラインに従ってください。

- Cisco Crosswork は、SCP を使用して、システムの設定を外部サーバーにバックアップします。開始する前に、次の設定を行い、SCP サーバーに関する情報を用意しておく必要があります。
  - セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。
  - バックアップが保存される SCP サーバーの事前設定されたパス。
  - ディレクトリに対するファイルの読み取りおよび書き込み権限のあるユーザーのログイン情報。
  - SCP サーバーのストレージ要件は若干異なりますが、少なくとも 25 GB のストレージが必要です。
- バックアップファイルを保存する宛先 SCP サーバーが設定されていることを確認します。この設定は 1 回限りのアクティビティです。
- バックアップ操作が完了したら、宛先 SCP サーバーディレクトリに移動し、バックアップファイルが作成されていることを確認します。このバックアップファイルは、アップグレードプロセスの後の段階で必要になります。
- Cisco Crosswork クラスタと SCP サーバーの両方が同じ IP 環境内に存在する必要があります。たとえば、Cisco Crosswork が IPv6 で通信している場合は、バックアップサーバーも IPv6 で通信している必要があります。
- 現在のバージョンの Cisco Crosswork にインストールした Crosswork アプリケーションのリストを記録しておきます。これらのアプリケーションは、新しいバージョンの Cisco Crosswork に移行した後でなければインストールできません。
- 現在のバージョンの Cisco Crosswork でカスタム MIB パッケージを導入準備した場合は、パッケージのコピーをシステムにダウンロードします。新しいバージョンの Cisco Crosswork への移行が完了したら、パッケージをアップロードする必要があります。詳細については、アップグレード後のチェックリスト （243 ページ） を参照してください。
- サードパーティ製デバイスタイプを含めるように現在のバージョンの Cisco Crosswork を変更した場合は、サードパーティ製デバイスの構成ファイルをダウンロードし、新しい

バージョンの Cisco Crosswork に再適用する必要があります。デバイスのコンフィギュレーション ファイルは、クラスタノード（/mnt/cw_lusterfs/bricks/brick3/sys-oids.yaml）とポッド（/mnt/backup/sys-oids.yaml）にあります。

- Cisco Crosswork 最適化エンジン に有効にされた機能パック（Local Congestion Mitigation（LCM）、Bandwidth Optimization（BWOpt）、および Bandwidth on Demand（BWoD））がある場合は、先に進む前に無効にする必要があります。また、使用可能な場合は、LCM または BWOpt によって管理されているインターフェイスの現在のリストをエクスポートします（[トラフィックエンジニアリング（Traffic Engineering）]>[ローカル輻輳緩和（Local Congestion Mitigation）]>[ドメイン識別子<domain_id>（Domain Identifier <domain_id>）]>[インターフェイスのしきい値（Interface Thresholds）]>[エクスポート（Export）]、または、[トラフィックエンジニアリング（Traffic Engineering）]>[帯域幅最適化（Bandwidth Optimization）]>[インターフェイスのしきい値（Interface Thresholds）]>[エクスポート（Export）]アイコン）。アップグレード要件（230ページ）に記載されている手順に従います。

ステップ 1 すべての VM が正常であり、クラスタ内で実行されていることを確認します。

ステップ 2 **SCP バックアップサーバーを設定します。**

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Backup and Restore]** を選択します。

b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。表示されたフィールドに関連するエントリを入力します。

c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 3 **バックアップを作成します。**

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Backup and Restore]** を選択します。

b) **[Actions]** > **[Backup]** をクリックして、宛先サーバーの詳細が事前に入力された [Backup] ダイアログボックスを表示します。

c) [Job Name] フィールドに、バックアップに該当する名前を入力します。

d) いずれかの VM またはアプリケーションの状態が [Healthy] になっていないときに、あえてバックアップを作成する場合は、[Force] チェックボックスをオンにします。

（注） [Force] オプションは、シスコ カスタマーエクスペリエンス チームに相談した後にのみ使用する必要があります。

e) バックアップに Cisco NSO のデータを含めない場合は、[Backup NSO] チェックボックスをオフにします。

Cisco Crosswork バックアッププロセスに Cisco NSO のデータを含める場合は、ここで説明する手順ではなく、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「**Backup Cisco Crosswork with Cisco NSO**」のセクションに記載されている手順に従ってください。

f) 必要に応じて残りのフィールドにも入力します。

別のリモート サーバー アップロード先を指定する場合：事前に入力された [Host Name]、[Port]、[Username]、[Password]、および [Remote Path] フィールドを編集して、別の接続先を指定します。

g) （オプション）[バックアップ準備の確認（Verify Backup Readiness）] をクリックして、Cisco Crosswork にバックアップを完了するのに十分な空きリソースがあることを確認します。検証に成功すると、この操作には時間がかかることについての警告が Cisco Crosswork に表示されます。[OK] をクリックします。

検証に失敗した場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

h) [Start Backup] をクリックして、バックアップ操作を開始します。Cisco Crosswork は、対応するバックアップジョブセットを作成し、それをジョブリストに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

i) バックアップジョブの進行状況を表示するには、[Backup and Restore Job Sets] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

（注） バックアップ操作が完了したら、宛先 SCP サーバーディレクトリに移動し、バックアップファイルが作成されていることを確認します。このバックアップファイルは、アップグレードプロセスの後の段階で必要になります。

（注） リストにバックアップジョブが表示されない場合は、[Backup and Restore Job Sets] テーブルを更新します。

j) リモートサーバへのアップロード中にバックアップが失敗した場合：[Job Details] パネルの [Status] アイコンのすぐ下にある [Upload backup] ボタンをクリックして、アップロードを再試行します。

（注） SCP バックアップサーバーとの接続の問題（たとえば、ログイン情報の誤り、ディレクトリまたはディレクトリの権限の欠落、パスの欠落など）が原因でアップロードに失敗することがあります。こうした原因によることは、タスク **`uploadBackupToRemote`** の失敗によって示されます。このような状況が発生した場合は、SCP サーバーの詳細を確認し、誤りを修正してから再試行してください。または、[Upload backup] をクリックする前に、[Destination] ボタンを使用して、別の SCP サーバーとパスを指定できます。

ステップ 4 バックアップが正常に完了したら、各ノードをホストする VM の電源をオフにして（ハイブリッド VM から開始）、Cisco Crosswork クラスタをシャットダウンします。

a) VMware vSphere Web クライアントにログインします。
b) [ナビゲータ（Navigator）] ペインで、シャットダウンする VM を右クリックします。
c) **[電源（Power）] > [電源オフ（Power Off）]** を選択します。
d) VM のステータスが [オフ（Off）] に変わるまで待ちます。
e) 30 秒待ってから、残りの VM ごとにステップ 4a ー 4d を繰り返します。

ステップ 5 アップグレード中に Cisco NSO に対して意図しない更新が実行されないように、Cisco NSO を読み取り専用モードにします。

NSO を読み取り専用モードにするには、次のコマンドを使用します。

```
ncs_cmd -c maapi_read_only
```

最新バージョンの Cisco Crosswork クラスタのインストール

古いバージョンの Cisco Crosswork のバックアップが正常に完了した後、最新バージョンの Cisco Crosswork クラスタのインストールに進みます。

（注） 古いバージョンの Cisco Crosswork の VM ノード数以上の VM ノードが新しい Cisco Crosswork にインストールされる必要があります。

（注） クラスタのインストール中に、NSO をバージョン 5.7.6 にアップグレードする必要があります。NSO をアップグレードするプロセスについては、このドキュメントでは扱われません。詳細については、関連する Cisco NSO のドキュメントを参照してください。また、Cisco Optimization Engine を単独で使用したり、Cisco Network Controller ソリューションの一部として使用したりする場合は、SR-PCE をバージョン 7.7.1 にアップグレードしてください（詳細については『*Crosswork Network Controller 5.0 Release Notes*』を参照）。

始める前に

- ご使用の環境がすべてのインストールの前提条件を満たしていることを確認してください（VMware の場合はVMware vCenter のインストールの前提条件 （21 ページ）、AWS の場合はAWS EC2 のインストールの前提条件 （133 ページ）を参照）。

ステップ 1 使用するプラットフォームに Cisco Crosswork クラスタをインストールします（VMware の場合はVMware vCenter への Crosswork クラスタのインストール （45 ページ）、AWS の場合はAWS EC2 への Cisco Crosswork Network Controller のインストール （151 ページ）を参照）。

（注） インストール時に Cisco Crosswork は特別な管理 ID を作成します（ユーザー名に *cw-admin*、デフォルトパスワードに *cw-admin* を使用した**仮想マシン（VM）管理者**）。管理ユーザー名は予約されており、変更できません。管理 ID を使用して初めてログインした場合は、パスワードを変更するよう求められます。データセンター管理者はこの ID を使用して Crosswork アプリケーション VM にログインし、トラブルシューティングを行います。ユーザーはこれを使用して、VM が正しく設定されていることを確認します。

ステップ 2 インストールが完了したら、Cisco Crosswork UI にログインし、クラスタ内のすべてのノードが稼働しているかどうかを確認します。

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Crosswork Manager]** > **[Crosswork Summary]** の順に選択します。

b) [Crossworkクラスタ（Crosswork Cluster）] タイルをクリックして、ノード別のリソース使用率、使用中の IP アドレス、各ノードがハイブリッドとワーカーのどちらであるかなど、クラスタの詳細情報を表示します。

Cisco Crosswork アプリケーションのインストール

Cisco Crosswork クラスタの新しいバージョンを正常にインストールしたら、Cisco Crosswork アプリケーションの最新バージョンのインストールに進みます。

（注） インストールする Cisco Crosswork アプリケーションは、Cisco Crosswork のバックアップ作成とシャットダウン （234 ページ）でバックアップしたものと同じである必要があります。

ステップ 1 Crosswork アプリケーションのインストール （193 ページ）のステップに従って新しい Cisco Crosswork アプリケーションをインストールします。

ステップ 2 アプリケーションが正常にインストールされたら、新しい Cisco Crosswork クラスタの正常性を確認します。

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Crosswork Manager]** > **[Crosswork Summary]** の順に選択します。

b) [Crosswork Cluster] タイルをクリックして、クラスタの正常性に関する詳細情報を表示します。

Cisco Crosswork のバックアップの移行

Cisco Crosswork アプリケーションが正常にインストールされたら、以前に作成した Cisco Crosswork のバックアップを新しい Cisco Crosswork クラスタに移行します。

始める前に

作業を開始する前に、次を確認してください。

- Cisco Crosswork のバックアップ作成とシャットダウン （234 ページ） で使用されるセキュアな接続先 SCP サーバーのホスト名または IP アドレスおよびポート番号。
- Cisco Crosswork のバックアップ作成とシャットダウン （234 ページ） で作成したバックアップファイルの名前とパス。
- ディレクトリに対するファイルの読み取りおよび書き込み権限のあるユーザーのログイン情報。

ステップ 1 すべての VM が正常であり、クラスタ内で実行されていることを確認します。

ステップ 2 **SCP バックアップサーバーを設定します。**

a) メインメニューから、**[管理（Administration）] > [バックアップと復元（Backup and Restore）]** を選択します。

b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。

c) 表示されたフィールドに関連するエントリを入力します。

（注） [Remote Path] フィールドに、Cisco Crosswork のバックアップ作成とシャットダウン （234 ページ） で作成したバックアップの場所を入力してください。

d) [Save] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 3 **新しい Cisco Crosswork クラスタに以前の Cisco Crosswork のバックアップを移行します。**

a) Cisco Crosswork のメインメニューから、**[Administration] > [Backup and Restore]** を選択します。

b) **[Actions] > [Data Migration]** をクリックして、宛先サーバーの詳細が事前に入力された [Data Migration] ダイアログボックスを表示します。

c) [Backup File Name] フィールドに（Cisco Crosswork のバックアップ作成とシャットダウン （234 ページ） で作成した）データ移行バックアップの名前を入力します。

d) Cisco Crosswork アプリケーションまたはマイクロサービスの問題があるにもかかわらずデータ移行バックアップを実行する場合は、[Force] チェックボックスをオンにします。

e) [Start Migration] をクリックして、データ移行操作を開始します。Cisco Crosswork は、対応するデータ移行ジョブセットを作成し、[Backup and Restore Job Sets] テーブルに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

（注） リストにジョブが表示されない場合は、数分待ってから [Backup and Restore Job Sets] テーブルを更新してください。

f) データ移行ジョブの進捗を表示するには、[Backup and Restore Job Sets] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

（注） データ移行の操作中、Crosswork UI が一時的に使用できなくなることがあります。Crosswork UI がダウンしている場合、Grafana ダッシュボードでジョブのステータスを表示できます。Grafana リンクは、[ジョブの詳細（Job Details）] ウィンドウの右側にある [データ移行プロセスダッシュボードの表示（View Data Migration Process Dashboard）] オプションとして使用できます。

g) 途中でデータ移行が失敗した場合は、ステップ 1 に戻って手順を再開する必要があります。

ステップ 4 データの移行が正常に完了したら、新しい Cisco Crosswork クラスタの正常性を確認します。

a) Cisco Crosswork のメインメニューから、**[Administration] > [Crosswork Manager] > [Crosswork Summary]** の順に選択します。

b) [Crosswork Cluster] タイルをクリックして、クラスタの正常性に関する詳細情報を表示します。

Crosswork Data Gateway のアップグレード

これはアップグレードワークフローの最終段階です。最新バージョンの Crosswork Data Gateway のインストールに進む前に、移行が完了し、新しい Cisco Crosswork UI が使用可能であることを確認してください。

（注） これは Cisco Crosswork Data Gateway Base VM のアップグレードのみに必要な手順です。コレクタなど、他のコンポーネントのアップグレードは、Cisco Crosswork によって実行されます。

Crosswork Data Gateway は、ネットワーク内のパッシブデバイスとして機能します。Crosswork Data Gateway のアップグレードプロセスは、ネットワーク内のすべての古い Crosswork Data Gateway VM を Crosswork Data Gateway VM に置き換える次の手順で構成されます。

重要 この手順のステップ 8 では、Cisco Crosswork からログアウトし、最新の Crosswork Data Gateway VM の Cisco Crosswork への展開と登録を確認した後、再度ログインする必要があります。ログインすると、[実行するアクション（Action to be taken）] ウィンドウが表示され、アップグレードが完了したことを確認するように求められます。手順のステップ 3、ステップ 4、およびステップ 5 に記載されているすべての検証ステップを完了していない場合は、[確認（Acknowledge）] をクリックしないでください。

ステップ 1 Cisco Crosswork からログアウトし、再度ログインします。

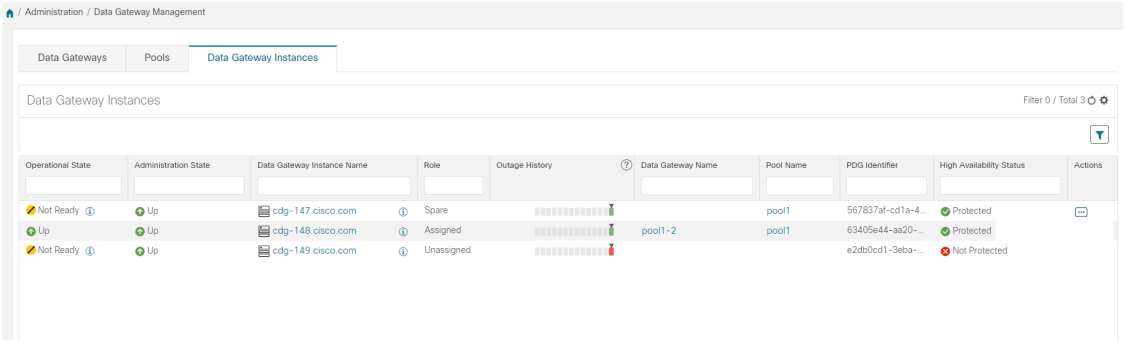
ステップ 2 ログインすると、[実行するアクション（Action to be taken）] ウィンドウが表示されます。このウィンドウを閉じて、[確認（Acknowledge）] をクリックしないでください。

ステップ 3 新しい Cisco Crosswork Data Gateway VM を、古い Crosswork Data Gateway VM と同じ数、同じ情報（管理インターフェイスが重要）を使用してインストールします。Cisco Crosswork Data Gateway のインストールワークフロー （79 ページ）の手順を実行します。

ステップ 4 約 5 分間待ってから、**[管理（Administration）]>[データゲートウェイ管理（Data Gateway Management）]** の順に移動します。

ステップ 5 [データゲートウェイインスタンス（Data Gateway Instances）] タブをチェックして、新しい Crosswork Data Gateway VM が Cisco Crosswork に登録され、[管理状態（Admin State）] が [アップ（Up）]、[操作の状態（Operational State）] が [未準備（Not Ready）] であることを確認します。

図 *33 : [データゲートウェイインスタンス（Data Gateway Instances）]ウィンドウ*



ステップ 6 VM の [操作の状態（Operational State）] が [準備完了（Ready）] に変わったら、[プール（Pools）] タブに移動し、以前のバージョンの Cisco Crosswork のすべての Crosswork Data Gateway プールがここにリストされていることを確認します。各 Crosswork Data Gateway プールを編集し、アクティブな Crosswork Data Gateway が以前のバージョンの Cisco Crosswork でメモしたものと同じであることを確認します。

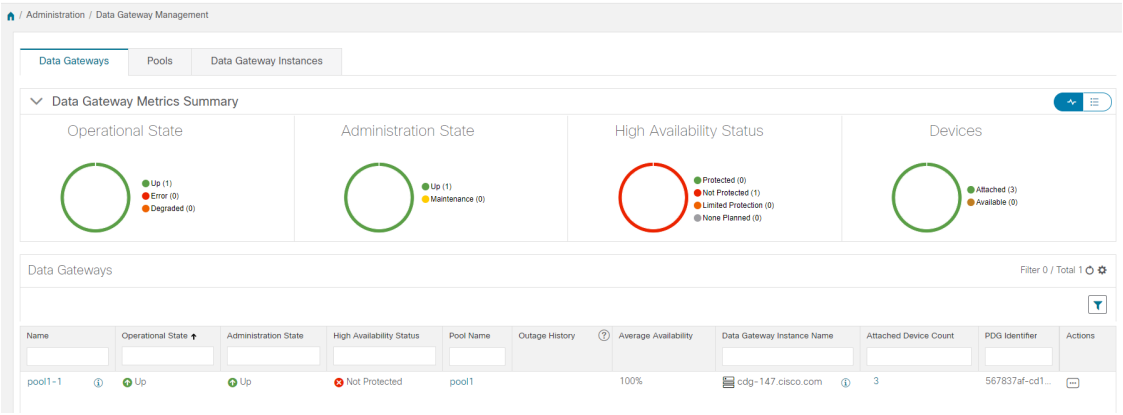
（注） プール名をクリックして、プールの詳細を確認することもできます。

ステップ 7 **Cisco Crosswork UI で、デバイスが Crosswork Data Gateways に接続されていることを確認します。**

a) [Administration] > [Data Gateway Management] ページに移動します。

b) Crosswork Data Gateway の [Attached Device Count] を確認します。

図 *34 : [データゲートウェイ（Data Gateway）]ウィンドウ*



ステップ 8 Cisco Crosswork からログアウトし、再度ログインします。

ステップ 9 ログインすると、Cisco Crosswork で、VM の確認を求める次のウィンドウが表示されます。表示されるポップアップで [確認（Acknowledge）] をクリックします。

図 *35 : [*確認応答（*Acknowledgment*）*]* ウィンドウ

重要 VM が [アップ（Up）] / [未準備（Not Ready）] 状態であることを確認していない場合は、[確認（Acknowledge）] をクリックしないでください。これを行うと、VM の状態が [エラー（Error）] になります。「Crosswork Data Gateway アップグレードに関連した問題のトラブルシューティング」を参照してください。

ステップ 10 （任意）Cisco NSO のメンテナンスモードまたは読み取り専用モードを終了します。

```
ncs_cmd -c maapi_read_write
```

アップグレード完了後は以下のようになります。

- Crosswork Data Gateway VM は Cisco Crosswork に登録されています。
- すべての宛先、Crosswork Data Gateway プール、デバイスマッピング情報は、アップグレードされた Crosswork Data Gateway VM を使用して Cisco Crosswork UI で表示できます。
- 収集ジョブは、新しい Cisco Crosswork Data Gateway VM で自動的に再開されます。
- Crosswork Data Gateway VM をアップグレードした後、収集リソースと無効化されたコンテナを再構成する必要があります。アップグレード前に構成されたグローバルパラメータのリソースは保持されません。リソースパラメータを構成するには、Crosswork UI で [管理（Administration）] > [データゲートウェイのグローバル設定（Data Gateway Global Settings）] > [データゲートウェイ（Data Gateway）] > [リソース（Resource）] に移動します。リソースについての詳細は、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』を参照してください。

Crosswork Data Gateway アップグレードに関連した問題のトラブルシューティング

次の表に、Crosswork Data Gateway のアップグレード時に発生する可能性のある一般的な問題を列挙し、問題の原因を特定して解決するためのアプローチを示します。

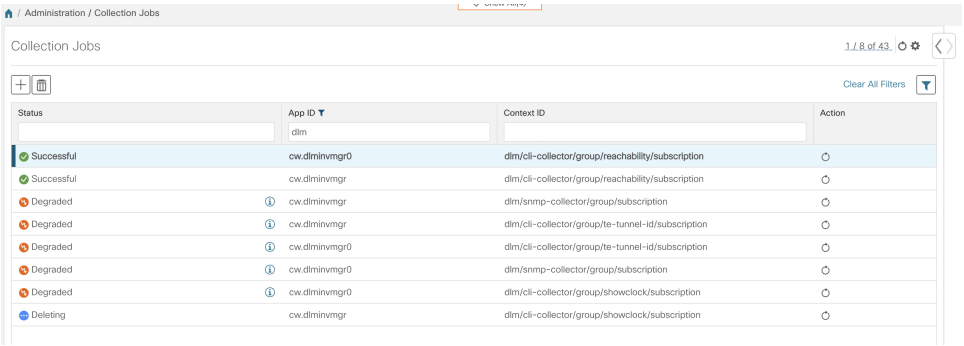
問題	推奨処置
一部の Crosswork Data Gateway VM は、VM が [アップ（Up）]/[未準備（Not Ready）] 状態になる前に [確認（Acknowledge）] をクリックしたため、[エラー（Error）] または [低下（Degraded）] 状態になっています	1. Crosswork Data Gateway VM の状態が [Up] または [Not Ready] になるまで待ちます。 2. VM の状態が [アップ（Up）] または [未準備（Not Ready）] になったら、Crosswork Data Gateway プールをすべて削除して、再度作成します。
一部の Crosswork Data Gateway VM は、VM が [アップ（Up）]/[未準備（Not Ready）] 状態になる前に [確認（Acknowledge）] をクリックしたため、[エラー（Error）] または [低下（Degraded）] 状態になっています。VM の状態は [アップ（Up）]/[準備完了（Ready）] に変化せず、まだ [エラー（Error）] のままです。	1. すべての Crosswork Data Gateway プールを削除します。 2. VM の状態が [アップ（Up）] または [未準備（Not Ready）] になっているかどうかを確認します。 3. VM がまだ [エラー（Error）] 状態の場合は、VM を新しいバージョンの Cisco Crosswork に手動で再登録します。詳細については、「Re-enroll Crosswork Data Gateway」を参照してください。
Crosswork Data Gateways VM が [低下（Degraded）] 状態のままスタックし、イメージマネージャが終了状態になります。Crosswork Data Gateway のコンポーネントのリストには、イメージマネージャが表示されないか、終了状態で表示されます。	1. Cisco Crosswork UI で、**[Data Gateway管理（Data Gateway Management）] > [仮想マシン（Virtual Machines）]** に移動します。 2. 低下した Crosswork Data Gateway をクリックします。 3. [アクション（Actions）] をクリックし、[再起動（Reboot）] をクリックします。

アップグレード後のチェックリスト

Cisco Crosswork を最新バージョンへアップグレードしたら、新しいクラスタの正常性を確認します。クラスタが正常であれば、次のアクティビティを実行します。

- システムの使用を続行する前に、ハードリフレッシュまたはブラウザキャッシュの削除を実行します。この手順を実行しないと、データの不一致が発生する可能性があります。
- Cisco Crosswork UI の [管理（Administration）] > [収集ジョブ（Collection Jobs）] に移動し、重複するシステムジョブを削除します。

図 *36 : [*収集ジョブ（*Collection Jobs*）*]* ウィンドウ



- [管理（Administration）]>[収集ジョブ（Collection Jobs）]ページで、Crosswork Data Gateway VM で収集ジョブが実行されていることを確認します。
- デフォルトのログイン情報を使用してログインして、復元したAAAデータを確認し、アップグレードした Cisco Crosswork でのカスタムユーザーロール（読み取り/書き込み、または読み取り）を設定します。
- （オプション）ネットワーク要件に基づいて、関連するマップファイルを cisco.com からダウンロードし、アップグレードした Cisco Crosswork に再アップロードします。
- （任意）Cisco Crosswork の以前のバージョンで NSO デバイス導入準備ポリシーが設定されている場合は、NSO で新しいネットワーク要素ドライバ（NED）を使用してポリシーを更新する必要があります。
- （オプション）（Cisco Crosswork の以前のバージョンで使用されていた）サードパーティ製デバイスの設定を新しいバージョンの Cisco Crosswork に再適用します。
- Crosswork Change Automation を使用している場合は、すべてのストックプレイブックとカスタムプレイブックが正常に移行されていることを確認します。
- Crosswork Health Insights を使用している場合は、外部宛先への収集が機能していることを確認します。また、アラートダッシュボードに正しいデータが表示されているかどうかも確認してください。
- Crosswork 最適化エンジン を使用している場合は、次のアクションを実行します。
  - 『Cisco Crosswork Optimization Engine Release Notes』に記載されているサポート対象 Cisco IOS XE/XR バージョンに従って、デバイスのソフトウェアバージョンをアップグレードします。
  - アップグレード要件 （230ページ）の手順を使用して、機能パック（ローカル輻輳緩和（LCM）、帯域幅最適化（BWOpt）、および帯域幅オンデマンド（BWoD））を確認します。

上記のアクティビティのいずれかでエラーが発生した場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

並列ハードウェアを使用したアップグレード

このセクションでは、新しいハードウェアを使用して Crosswork Network Controller の最新バージョンに移行する方法について説明します。この方法は、古い Cisco Crosswork クラスタのデータをバックアップしている間に、新しい Cisco Crosswork クラスタを新しいハードウェアに並行してインストールすることを前提とします。この方法は高速ですが、新しいクラスタを並行して作成するために 2 倍の量のリソースが必要です。

並行アップグレードワークフローの段階は次のとおりです。

1. 新しい Cisco Crosswork クラスタの展開 （245 ページ）

（注） クラスタのインストール中に、NSO をバージョン 6.1 にアップグレードする必要があります。NSO をアップグレードするプロセスについては、このドキュメントでは扱われません。詳細については、関連する Cisco NSO のドキュメントを参照してください。また、SR-PCE をバージョン 7.7.1 にアップグレードする必要もあります。インストール手順については、『Cisco IOS XRv 9000 Router Installation Guide』を参照してください。。

2. Cisco Crosswork クラスタをバックアップする （246 ページ）
3. DNS サーバーを更新して移行を実行する （249 ページ）
4. Crosswork Data Gateway を Cisco Crosswork に追加する （250 ページ）
5. 古い Cisco Crosswork クラスタのシャットダウン （253 ページ）

新しい Cisco Crosswork クラスタの展開

最新バージョンの Cisco Crosswork クラスタとアプリケーションを新しい VM セットに並行してインストールします。

（注） 新しい Cisco Crosswork クラスタは、古いバージョンの Cisco Crosswork と同じ FQDN および同じ数のノードでインストールする必要があります。

始める前に

- ご使用の環境がすべてのインストールの前提条件を満たしていることを確認してください（VMware の場合はVMware vCenter のインストールの前提条件 （21 ページ）、AWS の場合はAWS EC2 のインストールの前提条件 （133 ページ）を参照）。

ステップ 1 使用するプラットフォームに新しい Cisco Crosswork クラスタをインストールします（VMware の場合は VMware vCenter への Crosswork クラスタのインストール （45 ページ）、AWS の場合はAWS EC2 への Cisco Crosswork Network Controller のインストール （151 ページ）を参照）。

（注） インストール時に Cisco Crosswork は特別な管理 ID を作成します（ユーザー名に *cw-admin*、デフォルトパスワードに *cw-admin* を使用した**仮想マシン（VM）管理者**）。管理ユーザー名は予約されており、変更できません。管理 ID を使用して初めてログインした場合は、パスワードを変更するよう求められます。データセンター管理者はこの ID を使用して Crosswork アプリケーション VM にログインし、トラブルシューティングを行います。ユーザーはこれを使用して、VM が正しく設定されていることを確認します。

ステップ 2 インストールが完了したら、https://<NEW_VIP>:30603 に移動して Cisco Crosswork UI にログインします。

ステップ 3 すべてのノードがクラスタ内で稼働しているかどうかを確認します。

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Crosswork Manager]** > **[Crosswork Summary]** の順に選択します。

b) [Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、ノード別のリソース使用率、使用中の IP アドレス、各ノードがハイブリッドとワーカーのどちらであるかなど、クラスタの詳細情報を表示します。

ステップ 4 Cisco Crosswork の古いバージョンに含まれていたアプリケーションをインストールします。詳細については、Crosswork アプリケーションのインストール （193 ページ）を参照してください。

ステップ 5 アプリケーションが正常にインストールされたら、新しい Cisco Crosswork クラスタの正常性を確認します。

Cisco Crosswork クラスタをバックアップする

始める前に

バックアップを作成する場合は、次のガイドラインに従ってください。

- Cisco Crosswork は、SCP を使用して、システムの設定を外部サーバーにバックアップします。開始する前に、次の設定を行い、SCP サーバーに関する情報を用意しておく必要があります。
  - セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。
  - バックアップが保存される SCP サーバーの事前設定されたパス。
  - ディレクトリに対するファイルの読み取りおよび書き込み権限のあるユーザーのログイン情報。
  - SCP サーバーのストレージ要件は若干異なりますが、少なくとも 25 GB のストレージが必要です。

- バックアップファイルを保存する宛先SCPサーバーが設定されていることを確認します。この設定は 1 回限りのアクティビティです。
- Cisco Crosswork クラスタと SCP サーバーの両方が同じ IP 環境内に存在する必要があります。たとえば、Cisco Crosswork が IPv6 で通信している場合は、バックアップサーバーも IPv6 で通信している必要があります。
- 現在のバージョンの Cisco Crosswork にインストールした Crosswork アプリケーションのリストを記録しておきます。これらのアプリケーションは、新しいバージョンの Cisco Crosswork に移行した後でなければインストールできません。
- 以前のバージョンの Cisco Crosswork でカスタム MIB パッケージを導入準備した場合は、パッケージのコピーをシステムにダウンロードします。Cisco Crosswork のアップグレードが完了したら、パッケージをアップロードする必要があります。詳細については、アップグレード後のチェックリスト （243 ページ）を参照してください。
- サードパーティ製デバイスタイプを含めるように以前のバージョンの Cisco Crosswork を変更した場合は、サードパーティ製デバイスの構成ファイルをダウンロードし、アップグレードした Cisco Crosswork に再適用する必要があります。デバイスのコンフィギュレーション ファイルは、クラスタノード（`/mnt/cw_lusterfs/bricks/brick3/sys-oids.yaml`）とポッド（`/mnt/backup/sys-oids.yaml`）にあります。
- Cisco Crosswork 最適化エンジン に有効にされた機能パック（Local Congestion Mitigation（LCM）、Bandwidth Optimization（BWOpt）、および Bandwidth on Demand（BWoD））がある場合は、先に進む前に無効にする必要があります。また、使用可能な場合は、LCM または BWOpt によって管理されているインターフェイスの現在のリストをエクスポートします（[トラフィックエンジニアリング（Traffic Engineering）]>[ローカル輻輳緩和（Local Congestion Mitigation）]>[ドメイン識別子<domain_id>（Domain Identifier <domain_id>）]>[インターフェイスのしきい値（Interface Thresholds）]>[エクスポート（Export）]、または、[トラフィックエンジニアリング（Traffic Engineering）]>[帯域幅最適化（Bandwidth Optimization）]>[インターフェイスのしきい値（Interface Thresholds）]>[エクスポート（Export）]アイコン）。アップグレード要件 （230 ページ）に記載されている手順に従います。

（注） バックアップは、スケジュールされたアップグレード期間中にのみ作成することを推奨します。バックアップ操作の実行中は、Cisco Crosswork へのアクセスを試みないでください。

ステップ 1 ブラウザを使用して https://<FQDN>:30603 に移動して、Cisco Crosswork UI を起動します

ステップ 2 すべての VM が正常であり、クラスタ内で実行されていることを確認します。

ステップ 3 **SCP バックアップサーバーを設定します。**

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Backup and Restore]** を選択します。

b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。表示されたフィールドに関連するエントリを入力します。
c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 4 バックアップを作成します。

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Backup and Restore]** を選択します。
b) **[Actions]** > **[Backup]** をクリックして、宛先サーバーの詳細が事前に入力された [Backup] ダイアログボックスを表示します。
c) [Job Name] フィールドに、バックアップに該当する名前を入力します。
d) いずれかの VM またはアプリケーションの状態が [Healthy] になっていないときに、あえてバックアップを作成する場合は、[Force] チェックボックスをオンにします。

（注） [Force] オプションは、シスコ カスタマー エクスペリエンス チームに相談した後にのみ使用する必要があります。

e) バックアップに Cisco NSO のデータを含めない場合は、[NSOのバックアップ（Backup NSO）] チェックボックスをオフにします。

Cisco Crosswork バックアッププロセスに Cisco NSO のデータを含める場合は、ここで説明する手順ではなく、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「**Backup Cisco Crosswork with Cisco NSO**」のセクションに記載されている手順に従ってください。

f) 必要に応じて残りのフィールドにも入力します。

別のリモート サーバー アップロード先を指定する場合：事前に入力された [Host Name]、[Port]、[Username]、[Password]、および [Remote Path] フィールドを編集して、別の接続先を指定します。

g) （オプション）[バックアップ準備の確認（Verify Backup Readiness）] をクリックして、バックアップを完了するのに十分な空きリソースが Cisco Crosswork にあることを確認します。Cisco Crosswork は、リモートの接続先が正しく指定されていて、アプリケーションが正常である場合、どのアプリケーションも更新されていないことも確認します。検証に成功すると、この操作には時間がかかることについての警告が Cisco Crosswork に表示されます。[OK] をクリックします。

検証に失敗した場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

h) [Start Backup] をクリックして、バックアップ操作を開始します。Cisco Crosswork は、対応するバックアップジョブセットを作成し、それをジョブリストに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。
i) バックアップジョブの進行状況を表示するには、[Backup and Restore Job Sets] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

（注） リストにバックアップジョブが表示されない場合は、[Backup and Restore Job Sets] テーブルを更新します。

j) リモートサーバへのアップロード中にバックアップが失敗した場合：[Job Details] パネルの [Status] アイコンのすぐ下にある [Upload backup] ボタンをクリックして、アップロードを再試行します。

（注） SCP バックアップサーバーとの接続の問題（たとえば、ログイン情報の誤り、ディレクトリまたはディレクトリの権限の欠落、パスの欠落など）が原因でアップロードに失敗することがあります。こうした原因によることは、タスク **`uploadBackupToRemote`** の失敗によって示されます。このような状況が発生した場合は、SCP サーバーの詳細を確認し、誤りを修正してから再試行してください。または、[Upload backup] をクリックする前に、[Destination] ボタンを使用して、別の SCP サーバーとパスを指定できます。

DNS サーバーを更新して移行を実行する

始める前に

作業を開始する前に、次を確認してください。

- セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。
- 作成したバックアップファイルの名前とパス。
- ディレクトリに対するファイルの読み取りおよび書き込み権限のあるユーザーのログイン情報。

ステップ 1 DNS サーバーを更新して、以前のバージョンの Cisco Crosswork クラスタの FQDN が新しい Cisco Crosswork クラスタの <VIP> を指すようにします。

ステップ 2 https://<new_VIP>:30603 を使用して、アップグレードした Cisco Crosswork UI に移動します。

ステップ 3 **SCP バックアップサーバーを設定します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。

c) 表示されたフィールドに関連するエントリを入力します。

（注） [Remote Path] フィールドに、Cisco Crosswork クラスタをバックアップする （246 ページ）で作成したバックアップの場所を入力してください。

d) [Save] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 4 **古い Cisco Crosswork のバックアップを移行します。**

a) Cisco Crosswork のメインメニューから、**[Administration]** > **[Backup and Restore]** を選択します。

b) **[Actions]** > **[Data Migration]** をクリックして、宛先サーバーの詳細が事前に入力された [Data Migration] ダイアログボックスを表示します。

c) [Backup File Name] フィールドに（Cisco Crosswork クラスタをバックアップする （246 ページ） で作成した）データ移行バックアップの名前を入力します。

d) Cisco Crosswork アプリケーションまたはマイクロサービスの問題があるにもかかわらずデータ移行バックアップを実行する場合は、[Force] チェックボックスをオンにします。

e) [Start Migration] をクリックして、データ移行操作を開始します。Cisco Crosswork は、対応するデータ移行ジョブセットを作成し、[Backup and Restore Job Sets] テーブルに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

（注） リストにジョブが表示されない場合は、[Backup and Restore Job Sets] テーブルを更新します。

f) データ移行ジョブの進捗を表示するには、[Backup and Restore Job Sets] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

（注） データ移行の操作中、Crosswork UI と Grafana モニターリングが一時的に使用できなくなることがあります。

g) 途中でデータ移行が失敗した場合は、ステップ 1 に戻って手順を再開する必要があります。

ステップ 5 データの移行が正常に完了したら、新しい Cisco Crosswork クラスタの正常性を確認します。

a) Cisco Crosswork のメインメニューから、**[Administration] > [Crosswork Manager] > [Crosswork Summary]** の順に選択します。

b) [Crosswork Cluster] タイルをクリックして、クラスタの正常性に関する詳細情報を表示します。

（注） 移行が成功したら、システムの使用を続行する前に、ハードリフレッシュまたはブラウザキャッシュの削除を実行してください。この手順を実行しないと、データの不一致が発生する可能性があります。

Crosswork Data Gateway を Cisco Crosswork に追加する

新しいバージョンの Crosswork Data Gateway のインストールに進む前に、移行が完了し、新しい Cisco Crosswork UI が使用可能であることを確認してください。

（注） これは Cisco Crosswork Data Gateway Base VM のアップグレードのみに必要な手順です。コレクタなど、他のコンポーネントのアップグレードは、Cisco Crosswork によって実行されます。

Crosswork Data Gateway は、ネットワーク内のパッシブデバイスとして機能します。Crosswork Data Gateway のアップグレードプロセスは、ネットワーク内の古いすべての Crosswork Data

Gateway VM を Crosswork Data Gateway VM（最新のバージョン）に置き換える手順で構成されます。

重要 この手順のステップ 6 では、Cisco Crosswork からログアウトし、新しい CDG VM の Cisco Crosswork への展開と登録を確認した後、再度ログインする必要があります。ログインすると、[実行するアクション（Action to be taken）] ウィンドウが表示され、アップグレードが完了したことを確認するように求められます。手順のステップ 3、ステップ 4、およびステップ 5 に記載されているすべての検証ステップを完了していない場合は、[確認（Acknowledge）] をクリックしないでください。

ステップ 1 アップグレードした Cisco Crosswork からログアウトし、再度ログインします。

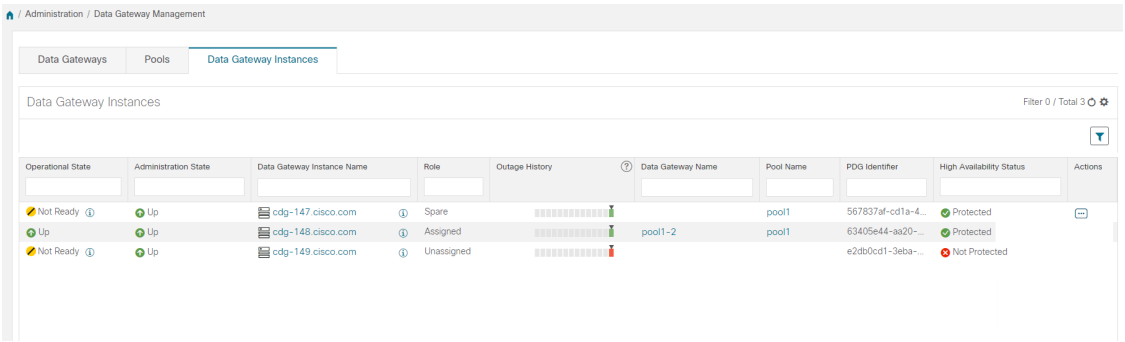
ステップ 2 ログインすると、[実行するアクション（Action to be taken）] ウィンドウが表示されます。このウィンドウを閉じて、[確認（Acknowledge）] をクリックしないでください。

ステップ 3 新しい Cisco Crosswork Data Gateway VM（最新のバージョン）を、古い Crosswork Data Gateway VM と同じ数、同じ情報（管理インターフェイスが重要）を使用してインストールします。Cisco Crosswork Data Gateway のインストールワークフロー （79 ページ）の手順を実行します。

ステップ 4 約 5 分間待ってから、**[管理（Administration）]>[データゲートウェイ管理（Data Gateway Management）]** の順に移動します。

ステップ 5 [データゲートウェイインスタンス（Data Gateway Instances）] タブをチェックして、新しい Crosswork Data Gateway VM が新しい Cisco Crosswork に登録され、[管理状態（Admin State）] が [アップ（Up）]、[操作の状態（Operational State）] が [未準備（Not Ready）] であることを確認します。

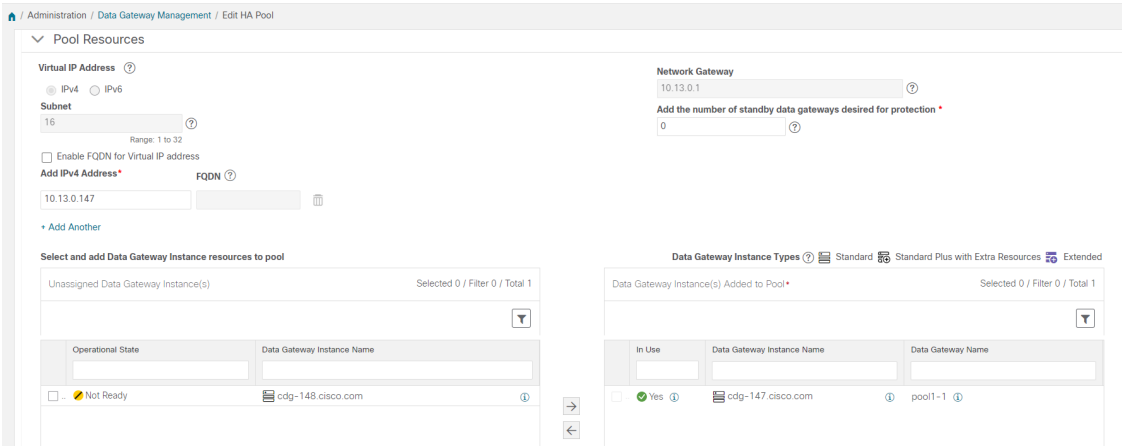
図 *37 : [データゲートウェイインスタンス（Data Gateway Instances）]* ウィンドウ



ステップ 6 VM の [操作の状態（Operational State）] が [準備完了（Ready）] に変わったら、[プール（Pools）] タブに移動し、古い Cisco Crosswork のすべての Crosswork Data Gateway プールがここにリストされていることを確認します。各 Crosswork Data Gateway プールを編集し、アクティブな Crosswork Data Gateway が古いバージョンの Cisco Crosswork でメモしたものと同じであることを確認します。

たとえば、次の図の Crosswork Data Gateway プールには 2 つの VM が含まれており、アクティブな VM は 172.23.247.78 です。

図 *38 : [HA*プールの編集（*Edit HA Pool*）*]* ウィンドウ



ステップ 7 アップグレードした **Cisco Crosswork UI** で、デバイスが新しい **Crosswork Data Gateway** に接続されていることを確認します。

a) [Administration] > [Data Gateway Management] ページに移動します。

b) Crosswork Data Gateway の [Attached Device Count] を確認します。

ステップ 8 Cisco Crosswork からログアウトし、再度ログインします。

ステップ 9 ログインすると、Cisco Crosswork で、VM の確認を求める次のウィンドウが表示されます。表示されるポップアップで [確認（Acknowledge）] をクリックします。

図 *39 : [*確認応答（*Acknowledgment*）*]* ウィンドウ

重要 VM が [アップ（Up）] / [未準備（Not Ready）] 状態であることを確認していない場合は、[確認（Acknowledge）] をクリックしないでください。これを行うと、VM の状態が [エラー（Error）] になります。「Crosswork Data Gateway アップグレードに関連した問題のトラブルシューティング」を参照してください。

ステップ 10 （任意）Cisco NSO のメンテナンスモードまたは読み取り専用モードを終了します。

```
ncs_cmd -c maapi_read_write
```

アップグレード完了後は以下のようになります。

- 新しい Crosswork Data Gateway VM はアップグレードした Cisco Crosswork に登録されています。
- すべての宛先、HA プール、デバイスマッピング情報は、アップグレードされた Crosswork Data Gateway VM を使用して Cisco Crosswork UI で表示できます。
- ジョブは、新しい Cisco Crosswork Data Gateway VM で自動的に再開されます。

古い Cisco Crosswork クラスタのシャットダウン

始める前に

Cisco Crosswork の古いバージョンをシャットダウンする前に、次の情報を収集してください。

- クラスタ内のすべての IP アドレス。
- CDG のすべての IP アドレス。

ステップ 1 バックアップが正常に完了したら、各ノードをホストする VM の電源をオフにして（ハイブリッド VM から開始）、Cisco Crosswork クラスタをシャットダウンします。

a) VMware vSphere Web クライアントにログインします。
b) [ナビゲータ（Navigator）] ペインで、シャットダウンする VM を右クリックします。
c) **[電源（Power）] > [電源オフ（Power Off）]** を選択します。
d) VM のステータスが [オフ（Off）] に変わるまで待ちます。
e) 30 秒待ってから、残りの VM ごとに手順 1a ー 1d を繰り返します。

ステップ 2 Crosswork Data Gateway VM をシャットダウンします。

a) 以前のバージョンの Crosswork Data Gateway VM にログインします。「SSH による Crosswork Data Gateway VM へのアクセス （121 ページ）」を参照してください。

正常にログインすると、Crosswork Data Gateway がインタラクティブコンソールを起動します。

b) [5 Troubleshooting] を選択します。
c) [Troubleshooting] メニューから [5 Shutdown VM] を選択して、VM をシャットダウンします。

ステップ 3 （任意）アップグレード中に Cisco NSO に対して意図しない更新が実行されないように、Cisco NSO を読み取り専用モードにします。

NSO を読み取り専用モードにするには、次のコマンドを使用します。

```
ncs_cmd -c maapi_read_only
```

詳細については、Cisco NSO 5.7.6 のマニュアルを参照してください。

Crosswork アプリケーションの更新（スタンドアロン アクティビティ）

このセクションでは、マイナーアップデートまたはパッチリリースの場合に、Cisco Crosswork UI から Crosswork アプリケーションを個別に更新する方法について説明します。この手順は、前のセクションで説明したアップグレードワークフローの一部ではありません。

作業を開始する前に、次を確認してください。

- 重要なアップグレードを行う前に、データのバックアップを作成します（バックアップ/復元機能を使用）。
- cisco.com からローカルマシンに Crosswork APPlication（CAPP）ファイルの最新バージョンをダウンロードします。

（注） Crosswork は、CAPP ファイルのダウングレード操作をサポートしていません。ただし、アプリケーションを古いバージョンに戻す場合は、アプリケーションをアンインストールして、古いバージョンのアプリケーションをインストールします。ダウングレードの場合は、操作の前にデータのバックアップを作成することを推奨します。

ステップ 1 **CAPP ファイルをダウンロードして検証します。**

a) cisco.com に移動し、必要な CAPP ファイル（.tar.gz）を見つけます。
b) ファイルにカーソルを合わせ、MD5 または SHA512 チェックサムをクリップボードにコピーします。
c) Crosswork サーバーから到達可能なサーバーに CAPP ファイルをダウンロードします。
d) 選択したツールを実行してチェックサムを計算し、ダウンロードしたファイルのチェックサム値をクリップボードにコピーした値と比較します。

たとえば、MAC では、**md5** コマンドを使用してファイルの MD5 サムを計算できます。

```
md5 cw-na-ztp-4.0.3-3-release-220614.tar.gz

ff47a72ed7dc4fc4be388db3a43fa13f
```

結果の値が cisco.com に投稿された値と一致することを確認します。

ステップ 2 **[管理（Administration）]>[Crossworkマネージャ（Crosswork Manager）]** をクリックし、[アプリケーション管理（Application Management）] タブを選択します。

Crosswork プラットフォーム インフラストラクチャと追加されたアプリケーションは、ここにタイルとして表示されます。

ステップ 3 [ファイルの追加（.tar.gz）（Add File (.tar.gz)）] オプションをクリックして、ダウンロードしたアプリケーション CAPP ファイルを追加します。

ステップ 4 [ファイルの追加（Add File）] ダイアログボックスで、該当する情報を入力し、[追加（Add）] をクリックします。

CAPP ファイルを追加すると、既存のアプリケーションタイル（この例では [Zero Touch Provisioning]）にアップグレードプロンプトが表示されます。

図 *40 : [アプリケーション（Applications）] ウィンドウ - アップグレードプロンプト*

ステップ 5 アップグレードする場合は、[アップグレード（Upgrade）] プロンプトをクリックすると、アプリケーションの新しいバージョンがインストールされます。

図 *41 : [アプリケーション（Applications）] ウィンドウ - 更新の進行状況*

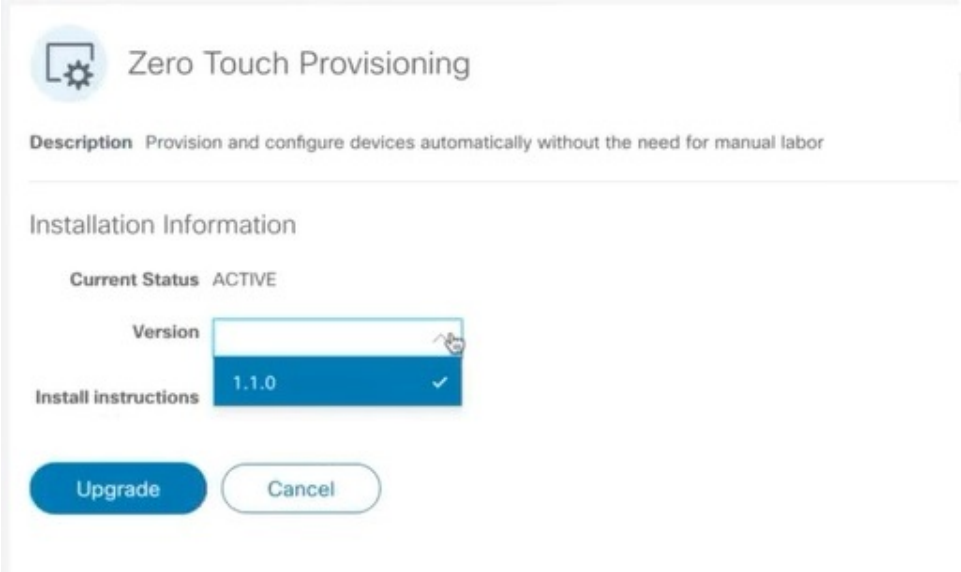
アップグレードの進行状況がアプリケーションタイルに表示されます。

ステップ 6 または、タイルの ··· をクリックし、ドロップダウンリストから [アップグレード（Upgrade）] オプションを選択します。

図 *42 : [アプリケーション（Applications）] ウィンドウ - アップグレードオプション*

[アップグレード（Upgrade）] 画面で、アップグレードする新しいバージョンを選択し、[アップグレード（Upgrade）] をクリックします。

図 *43 : [*アップグレードウィンドウ（***Upgrade Window***）*]*



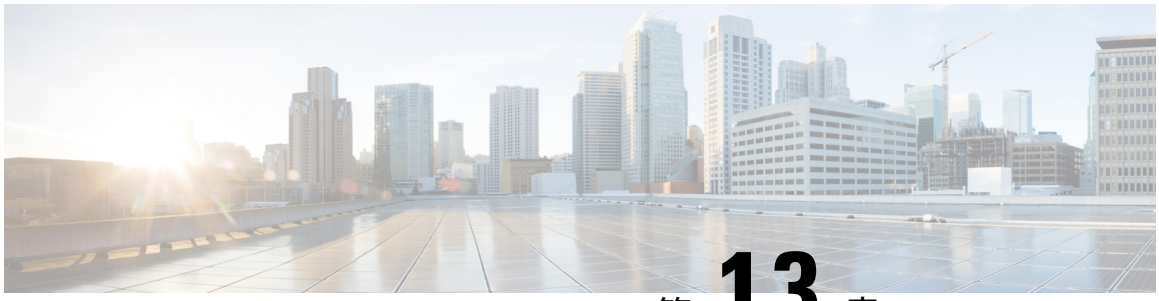
ステップ 7 （オプション）[ジョブ履歴（Job History）] をクリックして、アップグレード操作の進行状況を確認します。

（注） アップグレード操作では、通常、既存の CAPP ファイルと新しい CAPP ファイルの間で変更されたコンポーネントのみがインストールされます。これは、新しいバージョンが古いバージョンのリソースのほとんどを引き続き使用する可能性があるためです。これにより、現在のシステムとセッションを中断することなく迅速に操作を実行できます。

（注） アップグレード時は、更新が完了するまで更新中のアプリケーションは使用できません。この間、アプリケーションを使用している他のユーザーには、アップグレードに関するアラームが通知されます。

第 VII 部

Cisco Crosswork Network Controller のアンインストール



第 13 章

Cisco Crosswork のアンインストール

この章は次のトピックで構成されています。

Crosswork クラスタのアンインストール

このセクションでは、Cisco Crosswork クラスタをアンインストールするさまざまな方法について説明します。

クラスタインストーラを使用した VM の削除

インストールが失敗した場合は、クラスタインストーラツールを使用して、クラスタの状態に基づいて以前に作成した VM をクリーンアップするか、または削除します。これは、展開が失敗した場合の重要なアクティビティです。VM 設定またはデータセンターホストに変更を加えた場合は、再展開の前にクリーンアップ操作が必要です。

（注） インストーラ クリーンアップ オプションは、`/data` ディレクトリ内のインベントリに基づいてクラスタ展開を削除します。

ステップ 1 展開情報を保存するディレクトリを入力します。

たとえば、`_cd ~/cw-cluster` などです。

ステップ 2 ホストでコンテナを実行します。

```
docker run --rm -it -v `pwd`:/data <cw-installer docker container>
```

ステップ 3 テンプレートファイルのコピー（v4.tfvars など）をテキストエディタで編集し、データセンターのアクセスパラメータを追加します。残りのパラメータには、ダミー値を指定するか、または操作の実行時にコマンドラインで入力できます。

ステップ 4 -m フラグを使用して、_cw-installer.sh install_ スクリプトを clean ディレクティブとともに展開マニフェストで実行します。

-o オプションを追加して、データセンターから Cisco Crosswork イメージテンプレートを削除します。

次に例を示します。

```
./cw-installer.sh clean -m /data/deployment.tfvars -o
```

ステップ 5 プロンプトが表示されたら「yes」と入力して操作を確認します。

ステップ 6 （オプション）クラスタを迅速に（検証なしで）クリーンアップするには、次のコマンドを使用してインストーラを実行します。

```
docker run --rm -it -v `pwd`:/data <cw installer docker image> -exec './cw-installer.sh clean -m
/data/deployment.tfvars'
```

vSphere UI を使用した VM の削除

この項では、vCenter から VM を削除する手順について説明します。この手順は、アプリケーション Cisco Crosswork VM を削除するために使用されます。

（注）
- この手順では、すべてのアプリケーションデータが削除されることに注意してください。
- **Crosswork Data Gateway の削除のみを行う場合**は、次のことを実行しておく必要があります。
  - 削除する Crosswork Data Gateway VM からデバイスを切り離します。詳細については、『*Cisco Crosswork Network Controller 5.0 Administration Guide*』の「Delete Cisco Crosswork Data Gateway VM from Cisco Crosswork」のトピックを参照してください。
  - この章の説明に従って Cisco Crosswork から Crosswork Data Gateway VM を削除します。

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 [ナビゲータ（Navigator）] ペインで、削除するアプリケーション VM を右クリックし、[電源（Power）] > [電源オフ（Power Off）] を選択します。

ステップ 3 VM の電源がオフになったら、もう一度 VM を右クリックし、[ディスクから削除（Delete from Disk）] を選択します。

VM が削除されます。

Crosswork Data Gateway のアンインストール

このセクションでは、Cisco Crosswork Data Gateway を削除する方法について説明します。

• Cisco Crosswork から Crosswork Data Gateway VM を削除する （261 ページ）
• Crosswork クラスタからの Crosswork Data Gateway の削除 （262 ページ）

Cisco Crosswork から Crosswork Data Gateway VM を削除する

始める前に

削除する Crosswork Data Gateway VM は以下の状態にする必要があります。

- メンテナンスモードである必要があります。
- プールの一部であったり、デバイスに接続されたりしてはなりません。

ステップ 1 Cisco Crosswork UI にログインします。

ステップ 2 ナビゲーションパネルから、[管理（Administration）] > [Data Gatewayの管理（Data Gateway Management）] の順に選択します。

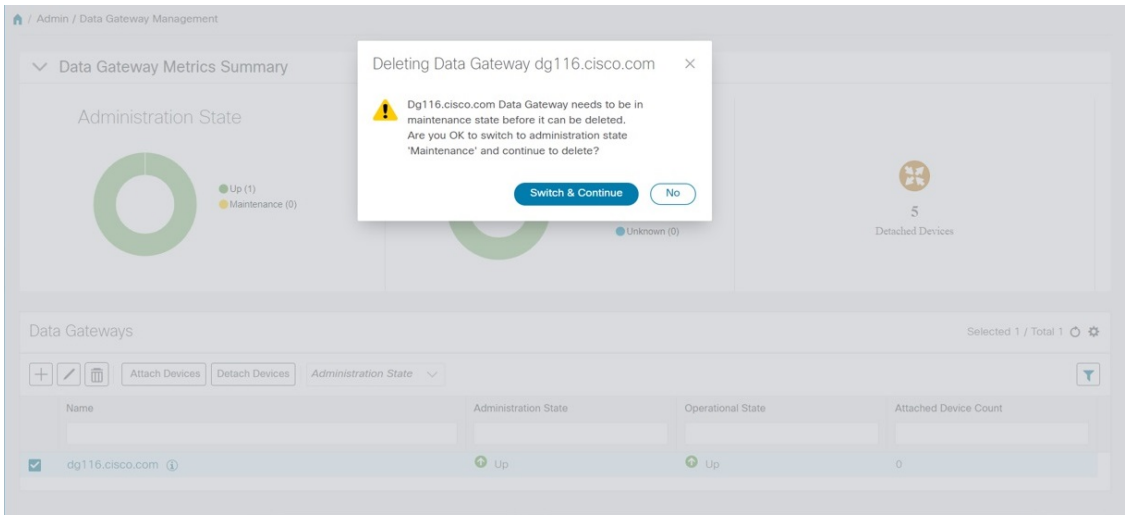
[Data Gatewayインスタンス（Data Gateway Instances）] タブをクリックします。

ステップ 3 [Data Gatewayインスタンス（Data Gateway Instances）] リストで、削除する Crosswork Data Gateway インスタンスを見つけ、[アクション（Actions）] 列の下にある … をクリックします。

[削除（Delete）] をクリックします。

ステップ 4 Crosswork Data Gateway インスタンスがメンテナンス状態でない場合は、Cisco Crosswork によってメンテナンス状態に切り替えるように求められます。[切り替えて続行（Switch & Continue）] をクリックします。

図 *44 : [*切り替えて続行（***Switch & Continue***）*]* ポップアップウィンドウ



Crosswork Data Gateway インスタンスが削除されます。

Crosswork クラスタからの Crosswork Data Gateway の削除

Crosswork クラスタから Crosswork Data Gateway を削除するには、次のステップに従います。

ステップ 1 Crosswork UI から Crosswork Data Gateway インスタンスを削除します。Crosswork UI から**データ ゲートウェイ インスタンス名**と **PDG 識別子**を書き留めます。

ステップ 2 次のコマンドを実行して、ポッドを Crosswork クラスタから削除します。

- `kubectl edit cdgoperator cdgoperator-cr -n cdg`
  - クラスタに Crosswork Data Gateway が 1 つしかない場合は、**spec** セクションの下にある **cdg_dep_plan** を含む CDG の配列を削除します。
  - クラスタに複数の Crosswork Data Gateway がある場合は、削除する必要がある cdg_dep_plan の**下の** CDG の配列エントリのみを削除して保存します。
- `kubectl delete infraservices <Data Gateway Instance Name> -n cdg`

  たとえば、`kubectl delete infraservices op-cdg -n cdg` です。
- `kubectl delete collectors collector-<PDG Identifier> -n cdg`

  たとえば、`kubectl delete collectors collector-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg` です。
- `kubectl delete icon icon-<PDG Identifier> -n cdg`

  たとえば、`kubectl delete icon icon-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg` です。
- オフロードポッドが存在する場合は、`kubectl delete offload offload-<PDG Identifier> -n cdg` です。

たとえば、`kubectl delete offload offload-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg` です。

Crosswork アプリケーションのアンインストール

このセクションでは、Crosswork UI でアプリケーションをアンインストールする方法について説明します。[Uninstall] オプションにより、アプリケーション、アプリケーション固有のメニュー、関連付けられたデータが削除されます。

注目 Crosswork アクティブトポロジ（インストールされている場合）は、Crosswork Optimization Engine をアンインストールする前にアンインストールする必要があります。

ステップ 1 **[管理（Admin）]** > **[Crossworkマネージャ（Crosswork Manager）]** をクリックし、[アプリケーション管理（Application Management）] タブを選択します。

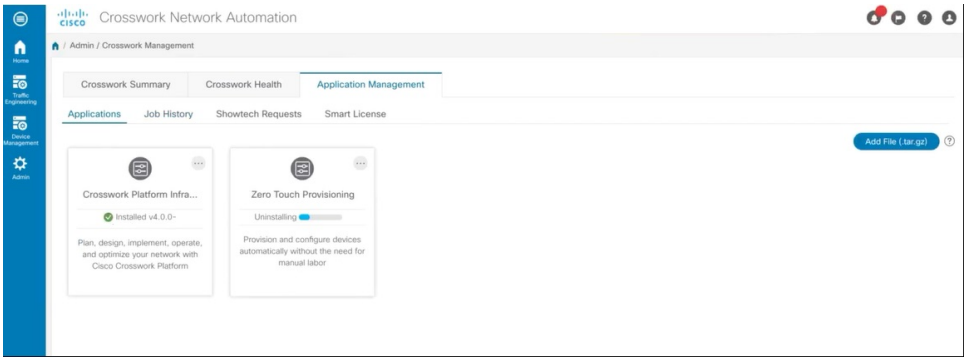
Crosswork プラットフォーム インフラストラクチャと追加されたアプリケーションは、ここにタイルとして表示されます。

ステップ 2 アンインストールするアプリケーションタイルで ··· をクリックし、ドロップダウンリストから [Uninstall] オプションを選択します。

ステップ 3 プロンプトが表示されたら、[アンインストール（Uninstall）] をクリックして確認します。

選択したアプリケーションがアンインストールされ、同じ内容を反映するようにアプリケーションタイルが変更されます。

図 *45 : [アプリケーション管理（Application Management）] ウィンドウ*



[Job History] ウィンドウ（**[Application Management]** > **[Job History]**）でアンインストールの進行状況を確認することもできます。アンインストールに失敗した場合は、[Job History] ウィンドウの関連オプションを使用して再試行できます。

（注） アンインストール操作で、リポジトリからCAPPファイルが削除されることはありません。ユーザーが将来インストールする場合に備えて、CAPP ファイルは Crosswork UI に表示されたままになります。

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。