Cisco Crosswork Workflow Manager ソリューション 2.0 フリートアップグレードのインストールガイド

最終更新：2026 年 3 月 31 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 1 章

フリートアップグレードのインストール 1

インストールの計画 1

インストール要件への適合 2

インストールパラメータ値の収集 13

vSphere を使用した VMware での Crosswork のインストール 20

Docker を使用した VMware での Crosswork のインストール 28

KVM 展開：ネットワークブリッジまたは SRIOV の構成 33

ネットワークブリッジの構成 33

SRIOV の構成 34

KVM への Crosswork のインストール 36

Crosswork サーバーのアクティベーションの監視 39

Crosswork Workflow Manager CAPP のインストール 42

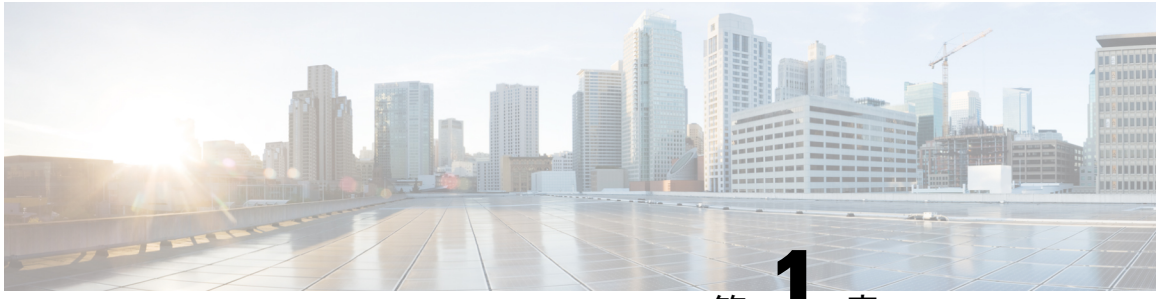
CWM ソリューション CAPP のインストール 44

ログイン情報プロファイルの作成 48

NSO パッケージのインストール前の作業 52

NSO プロバイダープロファイルの作成 54

NSO 機能パックの展開 58



第 1 章

フリートアップグレードのインストール

このドキュメントでは、以下のトピックについて説明します。

- インストールの計画 （1 ページ）
- インストール要件への適合 （2 ページ）
- インストールパラメータ値の収集 （13 ページ）
- vSphere を使用した VMware での Crosswork のインストール （20 ページ）
- Docker を使用した VMware での Crosswork のインストール （28 ページ）
- KVM 展開：ネットワークブリッジまたは SRIOV の構成 （33 ページ）
- KVM への Crosswork のインストール （36 ページ）
- Crosswork サーバーのアクティベーションの監視 （39 ページ）
- Crosswork Workflow Manager CAPP のインストール （42 ページ）
- CWM ソリューション CAPP のインストール （44 ページ）
- ログイン情報プロファイルの作成 （48 ページ）
- NSO パッケージのインストール前の作業 （52 ページ）
- NSO プロバイダープロファイルの作成 （54 ページ）
- NSO 機能パックの展開 （58 ページ）

インストールの計画

このトピックでは、Cisco Crosswork Workflow Manager ソリューションの SVM（単一仮想マシン）バージョンとそのサポートソフトウェアのインストールを計画する方法に関する導入情報を提供します。

インストール ワークフロー

Cisco Crosswork Workflow Manager ソリューションをインストールするには、次のコンポーネントをこの順序でインストールまたは構成する必要があります。

1. **Crosswork SVM サーバーのインストール**：Crosswork SVM サーバーをインストールして、プライマリ Cisco Crosswork プラットフォームインフラストラクチャをホストします。Crosswork SVM サーバーは、Crosswork Workflow Manager（CWM）および Crosswork Workflow Manager ソリューション（CWM-S）をホストします。

2. **NSO サーバーのインストール**：Cisco Network Services Orchestrator（NSO）をホストする 2 番目の**独立した**ネイティブLinux または Linux VM サーバーをインストールします。NSO は、ネットワークデバイスの直接操作を実行します。
3. **CWM および CWM-S CAPP のインストール**：プライマリ Crosswork SVM サーバーをインストールして構成したら、CWM および CWM-S CAPP をインストールできます。[1]。
4. **パッケージインストールのための NSO の準備**：NSO プロバイダーを作成し、Crosswork から NSO パッケージをインストールする前に、NSO サーバーが正しく構成されていることを確認します。
5. **Crosswork ログイン情報プロファイルと NSO プロバイダーの構成**：ログイン情報プロファイルのペアと、単一の NSO プロバイダープロファイルを構成します。これらのプロファイルによって、Crosswork、デバイス、および NSO サーバー間のセキュアな通信が可能になります。これらは、Crosswork サーバー上で Crosswork サーバーの管理ユーザーインターフェイスを使用して作成します。
6. **NSO パッケージのインストール**：NSO と Crosswork がデータを共有できるようにする一連の更新パッケージを NSO にインストールします。これらは、Crosswork サーバーの管理ユーザーインターフェイスを使用して、Crosswork サーバーから NSO サーバーにインストールします。

Crosswork SVM サーバーの展開方法の選択

Crosswork サーバーを SVM（単一仮想マシン）にインストールする必要があります。これを行うには、 VMwareまたは KVM の VM ハイパーバイザソフトウェアを使用します。VMware を選択した場合、Docker またはネイティブの VMware vCenter vSphere インストールツールを使用して VM を作成するオプションもあります。これにより、3 つの可能な展開方法から選択できます。

VM の展開を決定する前に、インストール要件への適合 （2 ページ）に記載されているハードウェア、ソフトウェア、ネットワーキング、ポート、およびその他の要件を確認することをお勧めします。また、インストールパラメータ値の収集 （13 ページ）に詳細が示されているように、各展開オプションに提供する必要がある情報を確認することもお勧めします。最後に、 VMware と KVM のどちらがニーズに最適であるかを検討してください。

インストール要件への適合

このドキュメントでは、Cisco Crosswork Workflow Manager ソリューションを正常にインストールするために満たす必要がある要件について説明します。

• ハードウェアの要件 （3 ページ）
• VMware のインストール要件 （4 ページ）

[1] CAPPとは、Cisco Crosswork プラットフォーム上で簡単にインストールできるように特別にパッケージ化された Crosswork **アプリケーション**です。

• KVM のインストール要件 （5 ページ）
• ネットワーク要件 （6 ページ）
• 管理ポートの要件 （9 ページ）
• デバイスのポート要件 （10 ページ）
• 追加の要件 （12 ページ）

ハードウェアの要件

仮想マシンのサーバーハードウェアリソースは次のとおりです。

1. **Crosswork サーバー要件**：VMwareと KVM 展開に必要な VM ハードウェア要件は似ています。
    1. **VMware**：NSO がインストールされているハードウェアサーバー以外のハードウェアサーバーに、vCenter vSphere または Docker ツールを使用して VMware ハイパーバイザをインストールできます。シスコでは、最低 24 個の仮想 CPU、128 GB のRAM、および 1 Tb のディスクストレージを備えたサーバーを推奨しています。その高いパフォーマンスのため、シスコでは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）を推奨しています。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。
    2. **KVM**：サーバーは 2.20 GHz 以上でインテル Xeon CPU E5-2699 v4 を実行し、最低 24 個の仮想 CPU、128 GB RAM、1 Tb ディスクストレージ、2 x 10 Gbps NIC を備えている必要があります。Red Hat Enterprise Linux（RHEL）9.4 以降をインストールします。スムーズなパフォーマンスを確保して問題を防ぐために、CPU とメモリに 20% のバッファ、ストレージに 30% のバッファを割り当てます。
2. **NSO サーバー要件**：ネイティブ Linux または任意のコンテナベースの実装を使用できます。Cisco NSO のインストールバージョンは 6.4.8.1 である必要があります。これは、**ローカル インストールではなく、システム インストールである必要があります**（リンクを参照して相違点を理解し、正しいインストール タイプを確認してください）。柔軟性の理由から、NSO サーバーは Crosswork プラットフォームサーバーから分離する必要があります。インストールされた NSO サーバーでは、Crosswork Workflow Manager 機能パックも実行されるため、シスコでは、少なくとも 16 個の仮想 CPU、256 GB の RAM、および 1Tb のディスクストレージ（基本的な NSO の実行に通常必要となるサイズよりも大きい値）を備えた NSO サーバーを推奨しています。これらの要件を満たす個別の NSO 展開をまだお持ちでないお客様は、VMware または KVM に Crosswork を展開した後に NSO をインストールすることができます。Crosswork プラットフォームインフラストラクチャが VM で起動するまでに約 1 時間かかり、この遅延により NSO のインストールに十分な時間が費やされます。さらに、CWM および CWM ソリューション CAPP をインストールする前に、前提条件の NSO パッケージをインストールし、NSO パッケージのインストール前の作業で詳しく説明している追加構成を実行する必要があります。

VMware のインストール要件

上記のハードウェア要件を満たすことに加えて、VMware を使用して実行される Crosswork サーバーのインストールは、次のインストール要件を満たしている必要があります（これには vSphere と Docker の両方が含まれます）。

- フリートアップグレードは、次の VMware ハイパーバイザおよび vCenter バージョンをサポートしています。
  - VMware vCenter Server 8.0（U2c 以降）および ESXi 8.0（U2b 以降）
  - VMware vCenter Server 7.0（U3p 以降）および ESXi 7.0（U3p 以降）
- Cisco Crosswork SVM 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。
- プロファイル駆動型ストレージが vCenter 管理者ユーザーによって有効になっていることを確認します。vCenter のルートレベル（すべてのリソースに対する）での vCenter ユーザーの権限をクエリします。
- シスコでは、vCenter ストレージ制御を有効にすることをお勧めします。
- 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（RTT が 10 ミリ秒以下の遅延）を許可する必要があります。
- 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：接続先ホストのリソースプール、またはリソースプールに 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。

KVM のインストール要件

上記のハードウェア要件を満たすことに加えて、次の手順を実行して、RHEL で KVM を使用して Crosswork サーバーの展開を設定する必要があります。

1. RHEL サーバーが仮想化をサポートしていることを確認します。これは通常、BIOS で有効になっています。次のコマンドを使用して確認します。
   - Intel CPU の場合：`grep -wo 'vmx' /proc/cpuinfo`
   - AMD CPU の場合：`grep -wo 'svm' /proc/cpuinfo`
2. `sudo dnf update -y` コマンドを使用して、システム上のすべてのパッケージを最新バージョンに更新します。
3. すべての更新が正常にインストールされたら、システムをリブートします（`sudo reboot`）。
4. 仮想化ツールをインストールします。
   1. 仮想マシンを作成し、操作するための virt-install および virt-viewer ツールをインストールします（`sudo dnf install virt-install virt-viewer -y`）。
   2. VM の管理に必要な libvirt 仮想化デーモンをインストールします（`sudo dnf install -y libvirt`）。
   3. VM を管理するためのグラフィカルインターフェイスである virt-manager をインストールします（`sudo dnf install virt-manager -y`）。
   4. VM を管理するための追加の仮想化ツールをインストールします（`sudo dnf install -y virt-top libguestfs-tools`）。
5. libvirtd 仮想化デーモンを実行します。
   1. libvirtd デーモンを起動します（`sudo systemctl start libvirtd`）
   2. libvertd デーモンを有効にします（`sudo systemctl enable libvirtd`）
   3. デーモンが実行されていることを確認します（`sudo systemctl status libvirtd`）
6. libvirt や qemu など、必要なグループにユーザーを追加します。次のコマンドでは、*your_username* を実際のユーザー名に置き換えます。

   ```
   sudo usermod --append --groups libvirt your_username
   sudo usermod --append --groups qemu your_username
   ```

7. [IOMMU] が有効になっていることを確認します。有効になっていない場合は、次のコマンドを実行して有効にします。

   ```
   grubby --update-kernel=ALL --args=intel_iommu=on
   dmesg | grep -I IOMMU
   ```

8. IOMMU を確認し、セットアップを検証します。すべてのチェックが [合格（PASS）] になっていることを確認します。

   ```
   virt-host-validate
   ```

IOMMUチェックが[合格（PASS）]でない場合は、次のコマンドを使用して有効にします。

```
 sudo grubby --update-kernel=ALL --args=intel_iommu=on
sudo reboot
```

9. `lsmod | grep kvm` コマンドを使用して、KVMモジュールがロードされていることを確認します

ネットワークブリッジまたはSRIOVの構成も参照してください。

ネットワーク要件

次の表は、すべてのVM展開のネットワーク要件の詳細を示しています。

表 *1:* ネットワークの要件

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（遅延は10ミリ秒未満）で設定されたリンクを使用する必要があります。 RHELでKVMを使用している場合：CrossworkVMをホストしているRHELベアメタルホストマシン上で、同じネットワーク名が使用され、構成されていることを確認してください。

要件	説明
IP アドレス	**IPv4 および/または IPv6 アドレス**：Crosswork SVM は、デュアルスタック（IPv4 および IPv6 プロトコルを使用した同時展開）をサポートしています。 Crosswork SVM 用に予約する IP アドレスの数とタイプは、次の要因によって異なります。 • シングルスタックまたはデュアルスタックのどちらを使用して展開しているか。 • 将来の成長、柔軟性、および地理的冗長性の実装に関する計画。この時点では、Crosswork 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。 Crosswork SVM 展開に必要な最低限の IP アドレス予約は次のとおりです。 • **シングル VM シングルスタック**：合計 4 個：管理用 2 個、データ用 2 個（4 個すべてが IPv4 または IPv6 のいずれか） • **シングル VM デュアルスタック**：合計 8 個：IPv4 管理用 2 個、IPv4 データ用 2 個、IPv6 管理用 2 個、IPv6 データ用 2 個 （注） • IP アドレスは、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。 • IPv6 またはデュアルスタックを使用して展開する場合、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。 • 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。

要件	説明
インターフェイス	Crosswork は **2 つのインターフェイス**を持つ単一の VM に展開されます。 • **NIC の数**：2 • **vNIC0**：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およびサーバー間で制御/データ情報を渡す場合）。 • **vNIC1**：デバイス アクセス トラフィック（デバイスアクセスおよびデータ収集の場合）。 （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2つの vNIC がある設定では、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 vNIC1 経由でルーティングされる必要があります。
NTP サーバー	使用する NTP サーバーの IPv4 および/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 および/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 25 GB のストレージが必要です。

要件	説明
FQDN（オプション）	インストールプロセスでは、VIP（仮想 IP アドレス）または FQDN（完全修飾ドメイン名）を使用して VM にアクセスできます。 FQDN を使用する場合は、管理用に 1 つ、データネットワーク用に 1 つ FQDN が必要です。 （注） 初期インストール時に FQDN を指定する場合は、VM の電源を投入する前に DNS サーバーに FQDN を入力する必要があります。入力しないと、インストールスクリプトで環境のセットアップを完了できません。

管理ポートの要件

次の表に、すべてのインストールの管理ネットワークポート要件の詳細を示します。

表 *2 :* 管理ネットワーク上の *Crosswork* 単一 *VM* 展開で使用されるポート

ポート	プロトコル	用途	方向
30602	TCP	インストールの監視（Crosswork Network Controller）	着信
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 でセキュアな接続をリッスンします）	着信
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）	着信
30653	TCP	RAF ピアクラスタ通信ポート	着信
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）	着信

ポート	プロトコル	用途	方向
30620	TCP	ZTP サーバーでのプラグアンドプレイ HTTP トラフィックの受信	着信
7	TCP/UDP	ICMP を使用したエンドポイントの検出	発信
22	TCP	管理対象デバイスとの SSH 接続の開始	発信
22	TCP	リモート SSH 接続	着信
53	TCP および UDP	DNS への接続	発信
123	UDP	ネットワーク タイム プロトコル（NTP）	発信
830	TCP	NETCONF の開始	発信

デバイスのポート要件

次の表に、両方のサーバーインストールのデバイスネットワークポートの要件の詳細を示します。

組み込みコレクタのポートを設定する場合は、次の表に記載されているポートがデバイスに設定されていることを確認します。たとえば、トラップの送信に使用されるポートがこれまで 1062 に設定されていた場合は、単一の仮想マシンを展開するための許容範囲内のポートに変更します。許容範囲は、次の表にポート番号とともに示されています。

表 *3:* デバイスネットワーク上の *Crosswork* 単一 *VM* 展開で使用されるポート

ポート	プロトコル	用途	方向
161	UDP	SNMP コレクタ	発信
31062 許容されるポートの範囲は 30160 ～ 31560 です。	UDP		着信
22	TCP	CLI コレクタ	発信

ポート	プロトコル	用途	方向
30614 許容されるポートの範囲は 30160 ～ 31560 です。	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。	着信
30898 許容されるポートの範囲は 30160 ～ 31560 です。	TCP		
30514 許容されるポートの範囲は 30160 ～ 31560 です。	UDP		
30621	TCP	アクティブな FTP サーバーが必要です。FTP（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。	着信

ポート	プロトコル	用途	方向
30622	TCP	アクティブな SFTP サーバーが必要です。SFTP（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。	着信
サイト固有[2]	TCP	gNMI コレクタ	発信
サイト固有[3]からポート番号を編集します。	サイト特定	Kafka と gRPC の接続先	発信

[2] デバイスのデフォルトポート情報については、プラットフォーム固有のマニュアルを参照してください。デバイスのポート番号が、**[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] > [デバイスの編集（Edit Device）]** で設定したものと同じであることを確認します。

[3] システムが作成した接続先のポート番号は、定義済みのポートを使用して作成されるため、変更できません。ユーザー定義の接続先ポートを変更するには、**[管理（Administration）] > [データコレクタのグローバル設定（Data Collector(s) Global Settings）] > [データの接続先（Data destinations）] > [接続先の編集（Edit destination）]**

追加の要件

サポートされているブラウザ：Google Chrome（バージョン 131.0.x）および Mozilla Firefox（134.0.1）。完全な機能を使用するために、ブラウザでは JavaScript と Cookie を有効にする必要があります。

サイトの準備：ユーザーのネットワーク環境に次のものが含まれている必要があります。

- すべてのネットワークデバイスがデータネットワークにアクセスできる必要があります。データネットワークは、IT 管理と制御トラフィックに最適化された管理ネットワークとは対照的に、ユーザーデータの伝送専用のネットワーク部分です。
- Cisco ソフトウェアダウンロード機能を利用するには、サーバーからインターネットへのアクセス、および software.cisco.com からイメージをダウンロードする承認を持つシスコのお客様のユーザー名とパスワードが必要です。

インストールパラメータ値の収集

以下の表では、 VMwareまたはKVM 展開に Crosswork をインストールする際に、 GUI またはインストールテンプレートで指定する必要がある重要なパラメータ値について説明しています。インストール前に、表に記載されている各パラメータに対して入力する関連する値を準備していることを確認してください。

一般パラメータ

これらのパラメータは、VMwareと KVM の両方のインストールで使用されます。

表 *4:*一般パラメータ

パラメータ名	説明
`ClusterIPStack`	IP スタックプロトコル：`IPv4`、`IPv6`、またはデュアルスタック。
`ManagementIPAddress`	VM の管理 IP アドレス（IPv4 や IPv6）。
`ManagementIPNetmask`	ドット付き 10 進法形式の管理 IP サブネット（IPv4 や IPv6）。
`ManagementIPGateway`	管理ネットワーク上のゲートウェイIP（IPv4 や 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`	Crosswork VM の管理仮想 IP。
`DataIPAddress`	VM のデータ IP アドレス（IPv4 や IPv6）。
`DataIPNetmask`	ドット付き 10 進法形式のデータ IP サブネット（IPv4 や IPv6）。
`DataIPGateway`	データネットワーク上のゲートウェイ IP（IPv4 や 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`	Crosswork VM のデータ仮想 IP。
`DNS`	DNS サーバーの IP アドレス（IPv4 や 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`	VM に使用されるドメイン名。

パラメータ名	説明
CWPassword	Cisco Crosswork にログインするためのパスワード。VM の設定時は、以下の条件を満たす強力なパスワードを設定します。 • パスワードは 8 文字以上とし、大文字、小文字、数字、および少なくとも 1 つの特殊文字を含める必要があります。 • バックスラッシュ（\）、引用符（'）二重引用符（"）は、特殊文字として使用できません。 • 辞書に載っている単語に似たパスワード（「Pa55w0rd!」など）の使用は避けてください。類似パスワードは基準を満たしていますが、脆弱であり、許可されないため、VM のセットアップに失敗します。
VMSize	VM のサイズ。Crosswork Workflow Manager ソリューションの展開の場合は、「超大規模」プロファイルを指定します。
VMName	VM の名前。
NodeType	VM のタイプを示します。**[ハイブリッド（Hybrid）]** を選択します。
IsSeed	[True] に設定します。
InitNodeCount	値を **1** に設定します。
InitMasterCount	値を **1** に設定します。
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35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。
ThinProvisioned	本番展開では、**[False]** を設定します。

パラメータ名	説明
SchemaVersion	構成マニフェストスキーマのバージョンこれは、このテンプレートで使用するインストーラのバージョンを示します。 スキーマのバージョンは、cisco.com のインストーラツールのサンプルテンプレートによってパッケージ化されるバージョンに対応している必要があります。テンプレートの要件はリリースごとに変更される可能性があるため、常に、展開するリリースで提供されるデフォルトのテンプレートから新しいテンプレートを作成する必要があります。
LogFsSize	ログパーティションサイズ（ギガバイト単位）。最小値は20GB、最大値は 1,000 GB です。 空白のままにすると、デフォルト値（20 GB）が選択されます。
EnableSkipAutoInstallFeature	[自動インストールをスキップ（skip auto install）] とマークされているポッドは、個別のアプリケーションまたはポッドが明示的に要求しない限り、起動されません。デフォルト値は、[False] です。 Crosswork Workflow Manager ソリューション展開の場合は、値を [True] に設定する必要があります。 （注） • 空白のままにすると、デフォルト値（[False]）が選択されます。 • このパラメータは、文字列値を許可するため、値をかならず二重引用符で囲います。
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。 このパラメータは、文字列値を許可するため、値をかならず二重引用符で囲います。
K8sServiceNetwork	kubernetes サービスネットワークのネットワークアドレス。デフォルトでは、CIDR 範囲は「/16」固定です。
K8sPodNetwork	kubernetes ポッドネットワークのネットワークアドレス。デフォルトでは、CIDR 範囲は「/16」固定です。

パラメータ名	説明
IgnoreDiagnosticsCheckFailure	診断チェックが失敗した場合のシステム応答を設定するために使用されます。[False] に設定すると、診断チェックがエラーを報告した場合、インストールは終了します。[True] に設定すると、診断チェックは無視され、インストールが続行します。 デフォルト値は [False] です。シスコでは、実稼働環境にインストールする場合、常に値を [False] のままにしておくことをお勧めします。この設定でインストールが失敗する場合は、シスコ カスタマー エクスペリエンスにお問い合わせください。 このパラメータは、文字列値を許可するため、値をかならず二重引用符で囲います。 （注） • ログファイル（diagnostic_stdout.log および diagnostic_stderr.log）は、**/var/log** にあります。各診断の実行結果は、**/home/cw-admin/diagnosis_report.txt** のファイルに保存されます。 • **diagnostic all** コマンドを使用して、N 日目に診断を手動で呼び出します。 • **diagnostic history** コマンドを使用して、以前のテストレポートを表示します。
ManagementVIPName	Crosswork VM の管理仮想 IP の名前。これは DNS 名を介して Crosswork の管理 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必要があります。
DataVIPName	Crosswork VM のデータ仮想 IP の名前。これは DNS 名を介して Crosswork のデータ 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必要があります。

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。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。このパラメータは、文字列値を許可するため、値をかならず二重引用符で囲います。 [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、不十分な CPU コアがパフォーマンスに影響を与えたり、インストールが失敗したりする可能性があります。
ManagerDataFsSize	このパラメータは、Dockerインストーラツールを使用してインストールする場合にのみ適用されます。 Crosswork ノードのデータディスクサイズを指します（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 485 です（有効な範囲は 485 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。
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。

パラメータ名	説明

Timezone	タイムゾーン名を入力します。名前は、標準 IANA「TZ」タイムゾーン名（英語）にする必要があります（「America/Chicago」など）。名前は文字列値であるため、値をかならず二重引用符で囲みます。
	
	IANA の TZ タイムゾーン名の公式リストは、https://data.iana.org/time-zones/tzdb-2021a/zone1970.tabで確認できます。また、任意の Ubuntu コマンドラインで次のように入力してリストを表示することもできます。
	
	`timedatectl list-timezones`
	
	この方法での TZ タイムゾーンの設定はオプションです。このフィールドを空白のままにすると、VM は、ローカル NTP サーバーの起動および接続時にシステムクロックを設定します。システムクロックは、NTP サーバーの UTC プロトコルを使用します。UTC を使用すると、ネットワーク全体で適切なサーバータイムの同期が確保されますが、ローカルタイムゾーンや DST の調整は行われないため、組織に NTP プロトコルの実装についてのポリシーが定義されていない限り、グローバルなネットワーク管理が複雑になる可能性があります。これに関するヘルプについては、『Use Best Practices for Network Time Protocol』を参照してください。
	
	後で、IANA の「TZ」タイムゾーン名を使用することにした場合は、CNC サーバー VM のコマンドラインを使用して、次のように設定できます。
	
	1. CNC サーバー VM のコマンドラインにアクセスします。
	`ssh cw-admin@VMIPaddress`
	2. 管理ユーザーに切り替えます（管理パスワードの入力を求められる場合があります）。
	`sudo su`
	3. 選択した IANA TZ 名を使用して、タイムゾーンを設定します。
	`timedatectl set-timezone TZName`
	4. 設定が受け入れられたことを確認します。
	`timedatectl status`

VMware パラメータ

VMware 展開を指定する場合は、VMware GUI オプションまたは VMware テンプレートで次のパラメータを構成する必要があります。

表 *5 : VMware GUI* またはテンプレートのパラメータ

パラメータ名	説明
VCenterAddress	vCenter IP またはホスト名。
VCenterUser	vCenter にログインするために必要なユーザー名。
VCenterPassword	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。 例：DCname = "WW-DCN-Solutions"
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。 このネットワークは VMware にすでに存在している必要があります。存在しない場合、インストールは失敗します。
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。 このネットワークは VMware にすでに存在している必要があります。存在しない場合、インストールは失敗します。
ホスト（Host）	VM が展開される ESXi ホストまたは vCenter VM/リソースグループの名前「のみ」。 第 1 のオプションは、ホストの IP または名前を使用することです（すべてのホストがデータセンターの下にある必要があります）。ホストがデータセンター内の VM の下にある場合は、VM 名のみを指定します（その VM 内のすべてのホストが選択されます）。 第 2 のオプションは、リソースグループを使用することです。この場合は、フルパスを指定する必要があります。 例：Host = "Main infrastructure/Resources/00_trial"
Datastore	このホストまたはリソースグループで使用可能なデータストア名。 第 1 のオプションは、ホストの IP または名前を使用することです。第2のオプションは、リソースグループを使用することです。 例：Datastore = "SDRS-DCNSOL-prodexsi/bru-netapp-01_FC_Prodesx_ds_15"
HSDatastore	このホストまたはリソースグループで使用可能な高速データストア。 高速データストアを使用しない場合は、データストアと同じ値に設定します。

パラメータ名	説明
Cw_VM_Image	vCenter の Crosswork VM イメージの名前。 この値は、インストーラツールの実行時にオプションとして設定されるため、テンプレートファイルで設定する必要はありません。
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。

デュアルスタックパラメータ

デュアルスタック展開を指定する場合は、管理、データ、および DNS パラメータの IPv4 と IPv6 の両方の値を設定する必要があります。

- ManagementIPv4Address、ManagementIPv6Address
- ManagementIPv4Netmask、ManagementIPv6Netmask
- ManagementIPv4Gateway、ManagementIPv6Gateway
- ManagementVIPv4、ManagementVIPv6
- DataIPv4Address、DataIPv6Address
- DataIPv4Netmask、DataIPv6Netmask
- DataIPv4Gateway、DataIPv6Gateway
- DataVIPv4、DataVIPv6
- DNSv4、DNSv6

vSphere を使用した VMware での Crosswork のインストール

VMware vSphere ユーザーインターフェイスを使用して単一の VM に Crosswork を展開するには、次の手順に従います。

始める前に

次の内容を確認してください。

- インストールの計画 （1 ページ）で説明されているワークフローと展開の決定事項に精通している。
- 選択した VMware ホストが、ハードウェアの要件 （3 ページ）および VMware のインストール要件 （4 ページ）で指定されている要件を満たしている。
- ネットワークが、ネットワーク要件 （6 ページ）で指定されているすべての要件を満たすように設定されている

- ホストおよびデバイスのポートが 管理ポートの要件 （9 ページ）および デバイスのポート要件 （10 ページ）で指定されている要件を満たすように設定されている。
- インストールパラメータ値の収集 （13 ページ）で指定されているように、必要なすべてのインストール値を準備している。

注目 このトピックで示しているダウンロードファイル名は、変更される可能性があります。最新バージョンは、ブラウザで https://software.cisco.com/download/home にアクセスし、**[Crosswork Network Controller]** > **[すべてのリリース（All Release）]** を検索することで常に確認できます。

手順

ステップ 1 Crosswork サーバーとして使用する予定のマシンに、VMware ESXi のサポートされているバージョンをインストールします。

ステップ 2 Cisco Software Central から、Cisco Crosswork プラットフォームの最新バージョンのイメージファイル `cnc-workflowmanager-single-node-deployment-7.2.0-45.ova` を、同じシステム上のストレージの場所にダウンロードします。

ステップ 3 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ウィンドウで、VM を展開する ESXi ホストを選択します。

ステップ 4 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、VM の UI にアクセスするために使用する管理ネットワークの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、データネットワークに使用される仮想スイッチに対してプロセスを繰り返します。

ステップ 5 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。

管理ネットワークとデータネットワークに使用するネットワークがホストに接続されていることを確認します。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 6 **[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。展開中に vCenter がタイムアウトすると、結果として VM はブート不可能になります。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 7 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 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、[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 7.2 Build 48 など）。

ステップ 9 [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 10 [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。

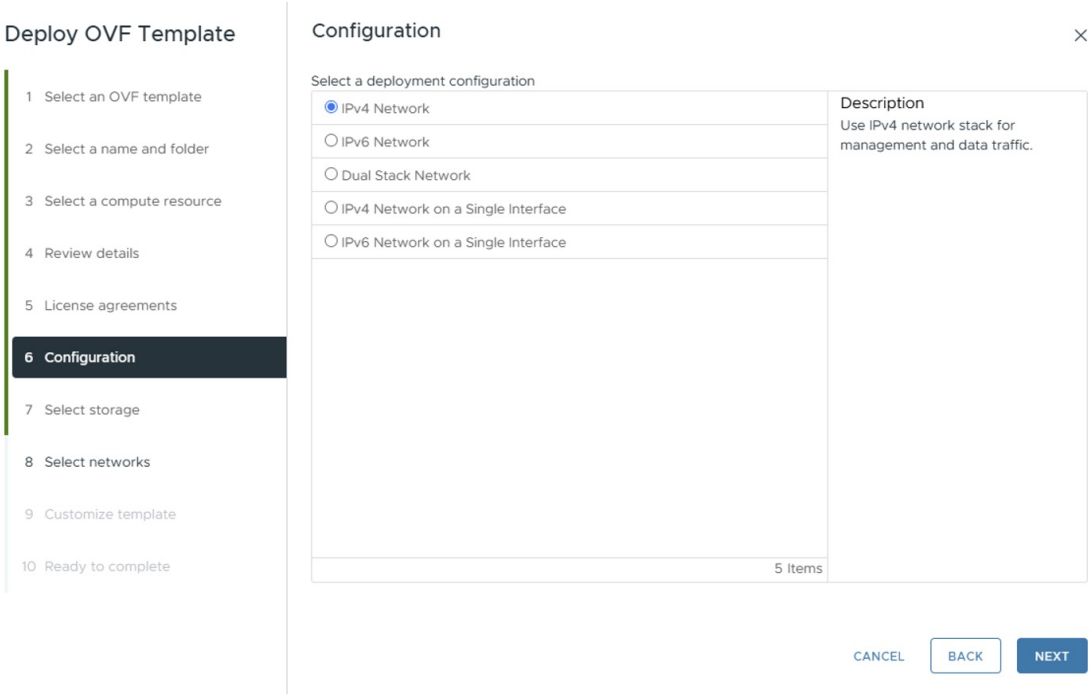
ステップ 11 展開する OVF テンプレートを確認します。この情報は OVF から収集され、変更はできません。

（注）
詳細な設定オプションを含むOVFパッケージや、信頼できる証明書に関するアラートが表示される場合があります。それらは一般的なアラートなので、[無視（Ignore）] オプションを選択しても問題ありません

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、[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。

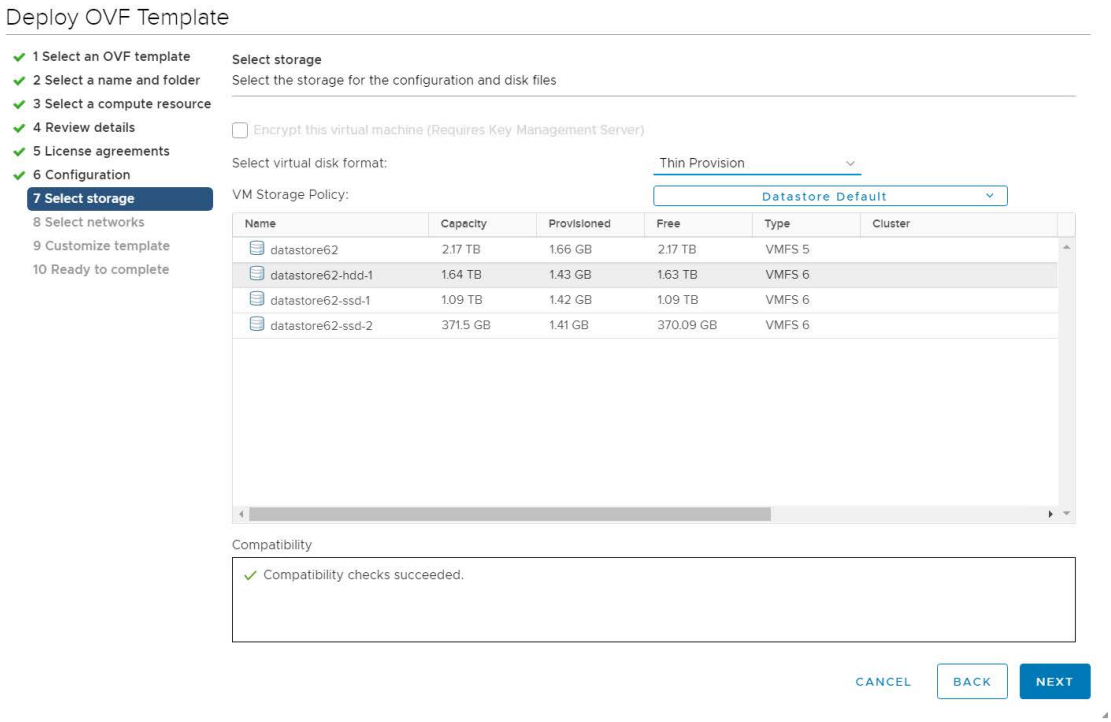
ステップ 13 [次へ（Next）] をクリックします。[OVFテンプレートの展開（Deploy OVF Template）] ウィンドウが更新され、[6 - 設定（6 - Configuration）] が強調表示されます。目的の展開設定を選択します。

図 *1* : 展開設定の選択



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、[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 *2:* ストレージの選択

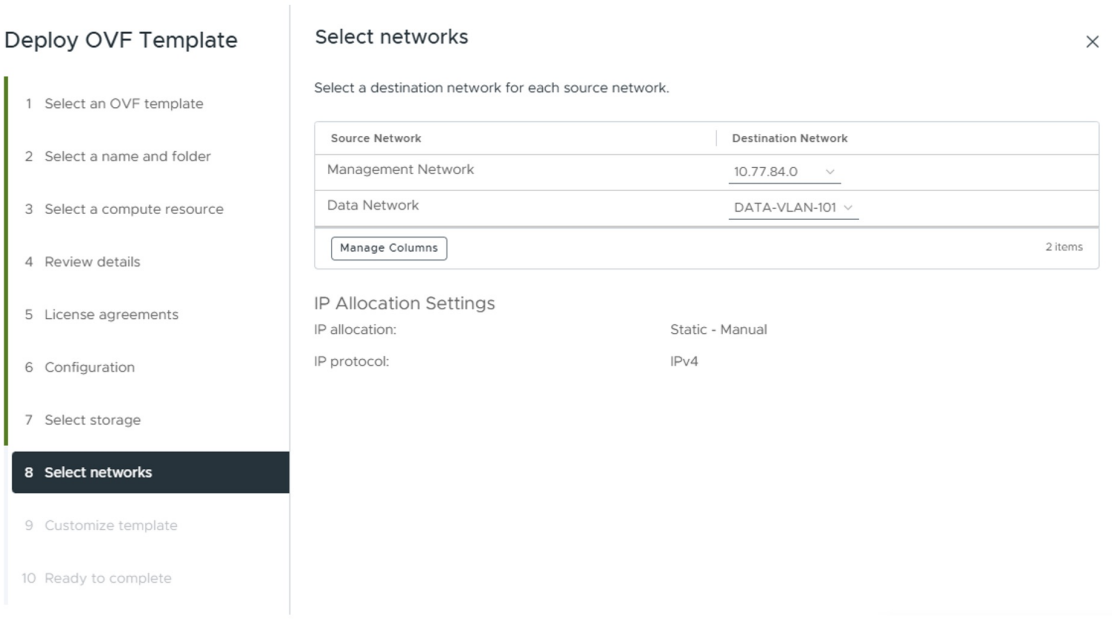


（注）
実稼働展開の場合は、[シックプロビジョニング（Eager Zeroed）（Thick Provision Eager Zeroed）] オプションを選択します。これにより、ディスク容量が事前に割り当てられ、最高のパフォーマンスが得られます。ラボで使用する場合は、ディスク容量を節約するため、[シンプロビジョニング（Thin Provision）] オプションを推奨します。

Crosswork は、単一 VM のインストールで 2TB のオプションをサポートしていません。

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、[8 - ネットワークの選択（8 - Select networks）] が強調表示されます。[接続先ネットワーク（Destination Network）] ドロップダウンリストから、管理ネットワークとデータネットワークに対する適切なネットワークを選択します。

図 *3* : ネットワークの選択（***Select networks***）



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、[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。IP アドレス、 IP ネットマスク、IP ゲートウェイ、仮想 IP アドレス、仮想 IP DNS 名など、IPv4 または IPv6 の展開に関する情報を（選択に従って）入力します。

b) [データネットワーク（Data Network）] 設定を展開します。IP アドレス、 IP ネットマスク、 IP ゲートウェイ、仮想 IP アドレス、仮想 IP DNS 名など、IPv4 または IPv6 の展開に関する情報を（選択に従って）入力します。

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）
辞書にある単語に似たパスワード（「Pa55w0rd!」など）や簡単に推測できるパターンは使用しないでください。このようなパスワードは、最初の基準を満たしている場合もありますが、脆弱であると見なされ、VM のセットアップが明確な説明なしに失敗する可能性があります。インストールを正常に完了させるために、大文字と小文字、数字、特殊文字を予測不可能な順序で組み合わせた 8 文字以上の複雑なパスワードを使用してください。

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。

- [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。
- [DNS 検索ドメイン（DNS Search Domain）]：DNS 検索ドメインの名前。
- **[タイムゾーン（Timezone）]**：タイムゾーンの詳細を入力します。デフォルト値は UTC です。

（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) **[ディスク構成（Disk Configuration）]** の設定を展開します。次のフィールドに該当する値を入力します。

- **Logfs ディスクサイズ**
- **Datafs ディスクサイズ**
- **Corefs パーティションサイズ**
- **高速ディスクサイズ**
- **バックアップパーティションの最小サイズ**

ディスク構成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）]： [ハイブリッド（Hybrid）] を選択します。
- [クラスタシードノード（Cluster Seed Node）]：[True] を選択します。
- **[Crosswork管理クラスタ仮想IP（Crosswork Management Cluster Virtual IP]）**：管理ネットワークの仮想 IP を入力します。
- **[Crosswork管理クラスタ仮想IP名（Crosswork Management Cluster Virtual IP Name）]**：管理ネットワークの仮想 IP インターフェイスの DNS ホスト名を入力します。
- **[Crosswork管理クラスタ仮想IP（Crosswork Data Cluster Virtual IP）]**：データネットワークの仮想 IP を入力します。
- **[Crossworkデータクラスタ仮想IP名（Crosswork Data Cluster Virtual IP Name）]**：データネットワークの仮想 IP インターフェイスの DNS ホスト名を入力します。
- **[ハイブリッドノードの初期数（Initial hybrid node count）]**： 1 に設定します。
- **[ノードの初期総数（Initial total node count）]**： 1 に設定します。
- **[VM の場所（Location of VM）]**：VM の地理的な場所を入力します。

- **[免責事項（Disclaimer）]**：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）。
- [インストールタイプ（Installation Type）]：単一の VM 展開には適用されません。いずれのチェックボックスもオンにしないでください。
- [自動インストールのスキップ機能の有効化（Enable Skip Auto Install Feature）]：[True] に設定します。
- [自動アクションマニフェスト定義（Auto Action Manifest Definition）]：デフォルト値（空）を使用します。
- **[製品固有の定義（Product specific definitio）]**: 製品固有の定義を入力します。
- **[失敗の診断を無視しますか?（Ignore Diagnose Failure?）]**：デフォルト値（**False**）を使用します。

ステップ 17 [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 18 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 19 展開が完了したら、VM を右クリックし、[設定の編集（Edit Settings）] を選択します。[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、次の属性を更新します。

- **VM プロファイル**：超大規模（XLarge）
- **CPU**：24
- **メモリ**：128 GB

[OK] をクリックして変更を保存します。

ステップ 20 Crosswork VM の電源を入れます。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。

VM 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ります。VM の作成とインストールの成功を追跡するには、Crosswork サーバーのアクティベーションの監視 （39 ページ）の手順に従います。

Docker を使用した VMware での Crosswork のインストール

Docker インストーラツールを使用して単一の VM に Crosswork を展開するには、次の手順に従います。

始める前に

次の内容を確認してください。

- ソフトウェアをダウンロードするマシンに Python がインストールされている。Python がインストールされていない場合は、インストールを開始する前に 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。
- インストールの計画 （1 ページ）で説明されているワークフローと展開の決定事項に精通している。
- 選択した VMware ホストが、ハードウェアの要件 （3 ページ）および VMware のインストール要件 （4 ページ）で指定されている要件を満たしている。
- ネットワークが、ネットワーク要件 （6 ページ）で指定されているすべての要件を満たすように設定されている
- ホストおよびデバイスのポートが 管理ポートの要件 （9 ページ）および デバイスのポート要件 （10 ページ）で指定されている要件を満たすように設定されている。
- インストールパラメータ値の収集 （13 ページ）で指定されているように、必要なすべてのインストール値を準備している。

取り付け中および取り付け後に、次の点に注意してください。

- `/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）が含まれています。このコンテンツへのアクセスを管理するのは、お客様の責任です。シスコでは、安全な環境でのインストールに使用されるテンプレートを保管するか、テンプレートを編集してパスワードを削除することをお勧めします。
- インストール時に、`install.log`、`install_tf.log`、および `.tfstate` ファイルが作成され、`/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、シスコのカスタマーエクスペリエンスチームにケースを開く必要がある場合は、必ずこれらのファイルを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。Docker インストーラ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ことがあります。
- インストールパラメータの変更や、インストールエラー後のパラメータの修正を行うには、インストールを管理して VM を正常に展開していたかどうかを区別することが重要で

す。インストーラが次のような出力を提供する場合、VM が正常に展開されたことを検出できます。

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

- 複数の Crosswork 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上に作成し、それぞれの新しいローカルディレクトリをコンテナに応じてマッピングすることです。

次の点に注意してください。

- インストーラツールを使用する場合は、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
- 単一 VM にインストールされた Crosswork は、現在、VMware vCenter のストレージフォルダや仮想フォルダ構造の下に整理されたデータストアをサポートしていません。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ます。

注目 このトピックで示しているダウンロードファイル名は、変更される可能性があります。最新バージョンは、ブラウザで https://software.cisco.com/download/home にアクセスし、**[Crosswork Network Controller]** > **[すべてのリリース（All Release）]** を検索することで常に確認できます。

手順

ステップ 1 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 2 https://software.cisco.com/download/home から、Crosswork プラットフォームインストーラバンドル（.tar.gz）および OVA イメージファイルを、以前に作成したディレクトリ（`CW-CWM-Solutions-Advantage-2.0.0-14-SVM-7.1.0-48-ova`）にダウンロードします。

ステップ 3 次のコマンドを使用して、インストーラバンドルを抽出します。

```
tar -xvf cnc-advantage-single-node-docker-deployment-7.1.0-48.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：`cnc-advantage-single-node-docker-deployment-7.1.0-48`）。抽出されるファイルには、インストーライメージ（`cw-na-cnc-advantage-svm-installer-7.1.0-48-releasecnc710-250606.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 4 README ファイルの内容を確認して、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 5 ワークステーションにインストールされている Python のバージョンが不明の場合は、`python --version` コマンドを使用して検出します。

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。

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 filename.cer -i filename.tar.gz -s Signaturefilename.tar.gz
-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。

```
python3 cisco_x509_verify_release.py3 -e filename.cer -i filename.tar.gz -s Signaturefilename.tar.gz
-v dgst -sha512
```

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 filename.tar.gz
```

次に例を示します。

```
docker load -i cw-na-cnc-advantage-svm-installer-7.1.0-48-releasecnc710-250606.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、必要な出力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-cnc-advantage-svm-7.1.0-48-releasecnc710-250606
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。これらを削除する場合は、`docker image rm {image id}` コマンドを使用します。

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、次のコマンドを使用します。

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

（注）
- 完全なイメージID値を入力する必要はありません。Dockerでは、インストールに使用するイメージを一意に識別できるだけのイメージ ID のみが必要です。この例では、 `docker run --rm -it -v `pwd`:/data a45` のようなコマンドも十分です。
- 上記のコマンドでは、バックティック（`）を使用しています。シェルでは全く異なる意味を持つため、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、テンプ

レートファイルと OVA ファイルは、コマンド実行時にコンテナ内ではなく、ローカルディスク上で現在いるディレクトリに保存されます。

- IPv6 セットアップを展開する場合、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
    ```

- **Centos/RHEL ホスト**：デフォルトでは、これらの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 run 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 2 つのエラーのいずれかが発生した場合は、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。次に、そのディレクトリに移動し、インストーラを再実行します。

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/7.1.0/vcentre
```

ステップ 11 `/opt/installer/deployments/7.1.0/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、すべての例でファイル名 `deployment.tfvars` を使用します。

ステップ 12 任意のテキストエディタを使用して、`/data` ディレクトリにコピーしたテンプレートファイルを開き、計画した展開のプロパティと一致するように編集します。

参考のために、サンプルパラメータ値を使用して編集された `deployment.tfvars` の例を次に示します。インストールパラメータ値の収集（13 ページ）で指定されているように、展開用に収集した値を使用する必要があります。

```
Cw_VM_Image = ""     # Line added automatically by installer.
ClusterIPStack         = "IPv4"
```

```
ManagementVIP         = "10.78.103.198"
ManagementIPNetmask   = "255.255.255.0"
ManagementIPGateway   = "10.78.103.1"
DataVIP               = "192.168.100.198"
DataIPNetmask         = "255.255.255.0"
DataIPGateway         = "0.0.0.0"
DNS                   = "72.163.128.140"
DomainName            = "cisco.com"
CWPassword            = "*****!"
VMSize                = "XLarge"
NTP                   = "ntp.esl.cisco.com"
Timezone              = "America/Los_Angeles"
EnableSkipAutoInstallFeature = "True"
CwVMs = {
    "0" = {
      VMName              = "SVM198",
      ManagementIPAddress = "10.78.103.197",
      DataIPAddress       = "192.168.100.197",
      NodeType            = "Hybrid"
    }
}
VCenterDC = {
  VCenterAddress = "10.64.80.220",
  VCenterUser = "vcenterUsername",
  VCenterPassword = "vCenterPassword",
  DCname = "Crosswork-Single-VM",
  MgmtNetworkName = "VM Network",
  DataNetworkName = "CW-7.1-VLAN21",
  VMs = [
      {
        HostedCwVMs = ["0"],
        Host = "10.78.103.62",
        Datastore = "5.2TB-SSD-62-2",
        HSDatastore="5.2TB-SSD-62-2"
      }
  ]
}
SchemaVersion = "7.1.0"
```

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 -m /data/template file name -o /data/filename.ova
```

次に例を示します。

```
./cw-installer.sh install -m /data/deployment.tfvars -o
/data/cnc-advantage-single-node-deployment-7.1.0-48.ova
```

ステップ 14 インストーラは、エンドユーザーライセンス契約（EULA）を表示します。内容を読み、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」と入力してインストール操作を開始します。

ステップ 16 VM の作成とインストールの成功を追跡するには、Crosswork サーバーのアクティベーションの監視 （39 ページ）の手順に従います。

ステップ 17 インストール操作が終了したら、次のように正常にインストールされたことを確認するか、失敗したインストールを再実行します。

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'.
```

以下のサンプル出力に示されているように、インストールプロセスが正常に完了した場合は、このような警告は無視できます。

正常なインストールのサンプル出力：

```
cw_vms = .......
INFO: Copying day 0 state inventory to CW
INFO: Waiting for deployment status server to startup on ip address. Elapsed time 0s, retrying in
 30s
Crosswork deployment status available at
http://ipaddress:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark

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

インストールが失敗した場合：

1. シスコのサポートケースを開きます。ケースには、インストール中に報告されたエラーメッセージのコピーを含めます。`/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）で作成した次のログファイルのコピーを必ず含めてください。`install.log`、`install_tf.log`、および `.tfstate`
2. インストールが失敗する最も一般的な 2 つの理由は、パスワードが十分に複雑でないこと、およびテンプレートファイル内のエラー（IP アドレスの入力ミスなど）です。このようなエラーが原因でインストーラが失敗する場合は、エラーを修正し、インストールスクリプトを再実行します。インストールを再実行する前に、必ずログファイルを削除してください。

KVM 展開：ネットワークブリッジまたは SRIOV の構成

次の手順は、KVM 展開を計画している場合にのみ関連します。VMware 展開を実行している場合は無視してください。

Crosswork は、大規模での機能をサポートするために、すべてのデータレイヤ通信に 10Gb インターフェイスが必要です。10G のスループットを提供できる任意のネットワーク構成を選択できます。

以下の 2 つのトピックでは、ネットワークブリッジおよび SRIOV ネットワーク構成を有効にする方法を説明しています。これにより、KVM 展開で 10Gb インターフェイスの要件を満たすことができます。KVM 展開では、ネットワークブリッジの構成（33 ページ） または SRIOV の構成（34 ページ） の**いずれか**が必要です。**ただし、両方は必須ではありません。**

ネットワークブリッジの構成

ネットワークブリッジは、仮想ネットワークスイッチのように動作し、複数のネットワークインターフェイスが同じネットワークにある場合、通信ができるように許可します。

次の手順を実行して、KVM 展開のネットワークブリッジを構成します。KVM 展開に SRIOV の構成 （34 ページ）を計画している場合、または VMware 展開を実行している場合は、この手順を無視してください。

手順

ステップ 1 インターフェイス名 `intMgmt` でタイプ「bridge」の新しいネットワーク接続を作成し、接続名 `intMgmt` を割り当てます。

```
nmcli connection add type bridge ifname intMgmt con-name intMgmt
```

ステップ 2 ブリッジとポート間に新しい接続を追加し、物理ネットワークインターフェイス `<interface1>` を以前作成したブリッジ `intMgmt` に関連付けます。

```
nmcli connection add type bridge-port ifname <interface1> controller intMgmt
```

ステップ 3 IP アドレスをブリッジに割り当てます。

```
nmcli connection modify intMgmt ipv4.addresses <IPv4-address>/<subnet-mask>
```

ステップ 4 `intMgmt` ネットワーク接続を確立します。

```
nmcli connection up intMgmt
```

ステップ 5 インターフェイス名が `intData` の別のネットワークブリッジ接続を作成し、それを接続名 `intData` に割り当てます。

```
nmcli connection add type bridge ifname intData con-name intData
```

ステップ 6 ブリッジとポート間に新しい接続を追加し、物理ネットワークインターフェイス `<interface2>` を以前作成したブリッジ `intData` に関連付けます。

```
nmcli connection add type bridge-port ifname <interface2> controller intData
```

ステップ 7 `intData` に IP アドレスを割り当てます。

```
nmcli connection modify intData ipv4.addresses <IPv4-address>/<subnet-mask>
```

ステップ 8 `intData` ネットワーク接続を起動します。

```
nmcli connection up intData
```

SRIOV の構成

SRIOV を使用すると、複数の仮想機能（VF）を作成することで、単一の物理ネットワーク インターフェイスを複数の VM 間で共有できます。

次の手順を実行して、KVM 展開の SRIOV を構成します。KVM 展開に ネットワークブリッジの構成 （33 ページ）を計画している場合、または VMware 展開を実行している場合は、この手順を無視してください。

手順

ステップ 1 vi エディタで `rc.local` ファイルを開きます。

```
vi /etc/rc.d/rc.local
```

ステップ 2 要件に基づいて、ネットワークインターフェイスの VF の数を設定します。たとえば、Cisco Crosswork Planning の単一の VM インストールでは、1 つは管理用で、もう 1 つはデータ用の少なくとも 2 つのネットワーク インターフェイスが必要です。デフォルトでは、各インターフェイスに 2 つの VF が構成されます。今後の拡張性のニーズに備えて追加の VF を構成することもできます。

たとえば、VF `<interface1>` と `<interface2>` の各数を 2 に設定するには、次のコマンドを使用します。この例では、`<interface1>` が管理インターフェイスを示し、`<interface2>` がデータインターフェイスを示します。

```
echo 2 > /sys/class/net/<interface1>/device/sriov_numvfs
echo 2 > /sys/class/net/<interface2>/device/sriov_numvfs
```

ステップ 3 `rc.local` ファイルの権限を変更し、実行可能にします。

```
chmod +x /etc/rc.d/rc.local
```

ステップ 4 いずれかのインターフェイスが VLAN 上に設定されている場合は、 VLAN ID をインターフェイスに構成します。

```
ip link set <interface1> vf 0 vlan <vlanid>
ip link set <interface2> vf 1 vlan <vlanid>
```

ステップ 5 変更を保存して、システムをリブートします。

ステップ 6 すべての仮想機能のすべての PCI デバイスをツリー形式で一覧します。これは、セットアップを確認し、KVM ハイパーバイザによって VF が正しく認識されることを確認するのに役立ちます。

```
virsh nodedev-list -\-tree
```

```
|+- pci_0000_17_00_0
|||
||+- net_ens1f0_40_a6_b7_ce_04_c8
||
|+- pci_0000_17_00_1
|||
||+- net_ens1f1_40_a6_b7_ce_04_c9
||
|+- pci_0000_17_00_2
|||
||+- net_ens1f2_40_a6_b7_ce_04_ca
||
|+- pci_0000_17_00_3
|||
||+- net_ens1f3_40_a6_b7_ce_04_cb
```

この手順では、ステップ 2 で VF の数を 2 に設定しているため、管理インターフェイスとデータインターフェイスごとに 2 つの VF が作成されます。その結果、2 つは管理用で、2 つはデータ用の合計 4 つの PCI デバイスが生成されます。

この PCI デバイス情報は、SRIOV のインストール プロセス中に使用されます（KVM への Crosswork のインストール （36 ページ） のステップ 4）。

KVM への Crosswork のインストール

KVM RHEL 上の単一の VM に Crosswork を展開するには、次の手順に従います。

（注） VM 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ります。

始める前に

次の内容を確認してください。

- インストールの計画 （1 ページ）で説明されているワークフローと展開の決定事項に精通している。
- KVM ホストが ハードウェアの要件 （3 ページ）で指定されている KVM ホストのすべての要件を満たしている。
- KVM のインストール要件 （5 ページ）で説明されているように、KVM RHEL 環境が設定および確認されている。
- ネットワークブリッジまたはSRIOVの構成で指定されているように、ネットワークブリッジまたは SRIOV が設定されている。
- ネットワークが、ネットワーク要件 （6 ページ）で指定されているすべての要件を満たすように設定されている。
- ホストおよびデバイスのポートが 管理ポートの要件 （9 ページ）および デバイスのポート要件 （10 ページ）で指定されている要件を満たすように設定されている。
- インストールパラメータ値の収集 （13 ページ）で指定されているように、必要なすべてのインストール値を準備している。

注目 このトピックで示しているダウンロードファイル名は、変更される可能性があります。最新バージョンは、ブラウザで https://software.cisco.com/download/home にアクセスし、**[Crosswork Network Controller] > [すべてのリリース（All Release）]** を検索することで常に確認できます。

手順

ステップ 1 Crosswork VM のインストール時に使用する構成 IOS ファイル（`ovf-env.xml`）を準備します。

次のサンプルテンプレートを使用して `ovf-env.xml` ファイルを準備します。

```
<Environment
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:ve="http://www.vmware.com/schema/ovfenv"
     oe:id=""
   <PlatformSection>
      <Kind>KVM</Kind>
      <Version>7.2.0</Version>
      <Vendor>KVM</Vendor>
      <Locale>en</Locale>
   </PlatformSection>
    <PropertySection>
         <Property oe:key="CWPassword" oe:value="**********"/>
         <Property oe:key="CWUsername" oe:value="cw-admin"/>
         <Property oe:key="ClusterCaKey" oe:value=""/>
         <Property oe:key="ClusterCaPubKey" oe:value=""/>
         <Property oe:key="CwInstaller" oe:value="False"/>
         <Property oe:key="DNSv4" oe:value="171.70.168.183"/>
         <Property oe:key="DNSv6" oe:value="::0"/>
         <Property oe:key="DataIPv4Address" oe:value="192.168.5.48"/>
         <Property oe:key="DataIPv4Gateway" oe:value="192.168.5.1"/>
         <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.0"/>
         <Property oe:key="DataIPv6Address" oe:value="::0"/>
         <Property oe:key="DataIPv6Gateway" oe:value="::1"/>
         <Property oe:key="DataIPv6Netmask" oe:value="64"/>
         <Property oe:key="DataPeerIPs" oe:value=""/>
         <Property oe:key="DataVIP" oe:value="192.168.5.51"/>
         <Property oe:key="DataVIPName" oe:value=""/>
         <Property oe:key="Deployment" oe:value="cw_ipv4"/>
         <Property oe:key="Disclaimer" oe:value="Cisco Crosswork"/>
         <Property oe:key="Domain" oe:value="cisco.com"/>
         <Property oe:key="EnableSkipAutoInstallFeature" oe:value="True"/>
         <Property oe:key="EnforcePodReservations" oe:value="True"/>
         <Property oe:key="IgnoreDiagnosticsCheckFailure" oe:value="True"/>
         <Property oe:key="InitMasterCount" oe:value="1"/>
         <Property oe:key="InitNodeCount" oe:value="1"/>
         <Property oe:key="IsSeed" oe:value="True"/>
         <Property oe:key="K8Orch" oe:value=""/>
         <Property oe:key="K8sPodNetworkV4" oe:value="10.244.0.0"/>
         <Property oe:key="K8sServiceNetworkV4" oe:value="10.96.0.0"/>
         <Property oe:key="ManagementIPv4Address" oe:value="10.19.70.148"/>
         <Property oe:key="ManagementIPv4Gateway" oe:value="10.19.70.1"/>
         <Property oe:key="ManagementIPv4Netmask" oe:value="255.255.255.0"/>
         <Property oe:key="ManagementIPv6Address" oe:value="::0"/>
         <Property oe:key="ManagementIPv6Gateway" oe:value="::1"/>
         <Property oe:key="ManagementIPv6Netmask" oe:value="112"/>
         <Property oe:key="ManagementVIP" oe:value="10.19.70.151"/>
         <Property oe:key="ManagementVIPName" oe:value=""/>
         <Property oe:key="ManagerPeerIPs" oe:value=""/>
         <Property oe:key="NTP" oe:value="ntp.esl.cisco.com"/>
         <Property oe:key="Timezone" oe:value="US/Pacific"/>
         <Property oe:key="VMLocation" oe:value="default"/>
         <Property oe:key="VMType" oe:value="Hybrid"/>
         <Property oe:key="bckup_min_percent" oe:value="35"/>
```

```
            <Property oe:key="corefs" oe:value="18"/>
            <Property oe:key="ddatafs" oe:value="485"/>
            <Property oe:key="logfs" oe:value="20"/>
            <Property oe:key="ramdisk" oe:value="0"/>
            <Property oe:key="ssd" oe:value="15"/>
            <Property oe:key="VMSize" oe:value="XLarge"/>
            <Property oe:key="ThinProvisioned" oe:value="False"/>
            <Property oe:key="UseNonDefaultCalicoBgpPort" oe:value="False"/>
            <Property oe:key="bootOptions.efiSecureBootEnabled" oe:value="True"/>
    </PropertySection>
</Environment>
```

ステップ 2 KVM 展開用に収集したパラメータ値を使用して、作成した `ovf-env.xml` ファイルを更新します（一般パラメータ （13 ページ）を参照）。

```
$ cat ovf-env.xml
```

ステップ 3 ISO ファイルを生成します。

```
$ mkisofs -R -relaxed-filenames -joliet-long -iso-level 3 -l -o cnc1.iso ovf-env.xml
```

（注）
上記のコマンドの `cnc1` は、Cisco Crosswork VM のホスト名です。

ステップ 4 https://software.cisco.com/download/home から、Cisco Crosswork プラットフォームの最新バージョンである `qcow2.tar.gz` ファイルを KVM ホスト上のストレージの場所にダウンロードします（`CW-CWM-Solutions-workflowmanager-2.1.0-14-SVM-7.2.0-45-qcow2.signed.bin`）。

ステップ 5 次のコマンドを使用して tar.gz ファイルを抽出します。

```
tar -xvf cnc-workflowmanager-single-node-deployment-7.2.0-45-qcow2.tar.gz
```

このコマンドは、次の 3 つの `qcow2` ファイルを作成します。

- `cnc-workflowmanager-single-node-deployment-7.2.0-45_dockerfs.qcow2`
- `cnc-workflowmanager-single-node-deployment-7.2.0-45_extrafs.qcow2`
- `cnc-workflowmanager-single-node-deployment-7.2.0-45_rootfs.qcow2`

ステップ 6 必要なインストールフォルダに移動し、3 つのディスクを作成します。

```
cd cnc1/
qemu-img create -f qcow2 disk3 20G
qemu-img create -f qcow2 disk4 485G
qemu-img create -f qcow2 disk6 15G

ls -1
cw_dockerfs.qcow2
cw_extrafs.qcow2
cw_rootfs.qcow2
disk3
disk4
disk6
```

ステップ 7 ネットワークブリッジまたは SRIOV を使用して Crosswork VM をインストールします。

この例では、`cnc1` は Crosswork VM のホスト名です。

- ネットワークブリッジの使用：

```
virt-install --boot uefi --boot hd,cdrom --connect qemu:///system --virt-type kvm --name cnc1
--ram 98304 --vcpus 12 --os-type linux --disk
path=cnc-workflowmanager-single-node-deployment-7.2.0-45_rootfs.qcow2,format=qcow2,bus=scsi
--disk
path=cnc-workflowmanager-single-node-deployment-7.2.0-45_dockerfs.qcow2,format=qcow2,bus=scsi
--disk path=disk3,format=qcow2,bus=scsi --disk path=disk4,format=qcow2,bus=scsi --disk
path=cnc-workflowmanager-single-node-deployment-7.2.0-45_extrafs.qcow2,format=qcow2,bus=scsi
--disk path=disk6,format=qcow2,bus=scsi --disk=cnckvm.iso,device=cdrom,bus=scsi --import --network
 bridge=intMgmt,model=virtio --network bridge=intData,model=virtio --noautoconsole --os-variant
 ubuntu22.04 --graphics vnc,listen=0.0.0.0
```

- SRIOV の使用：

```
virt-install --boot uefi --boot hd,cdrom --connect qemu:///system --virt-type kvm --name cnc1
--ram 98304 --vcpus 12 --cpu host-passthrough --disk path=cw_rootfs.qcow2,format=qcow2,bus=scsi
 --disk path=cw_dockerfs.qcow2,format=qcow2,bus=scsi --disk path=disk3,format=qcow2,bus=scsi
--disk path=disk4,format=qcow2,bus=scsi --disk path=cw_extrafs.qcow2,format=qcow2,bus=scsi --disk
 path=disk6,format=qcow2,bus=scsi --disk=cnc1.iso,device=cdrom,bus=scsi --import --network none
 --host-device=pci_0000_01_10_0 --host-device=pci_0000_01_10_0 --os-variant ubuntu-lts-latest
&
```

ステップ 8 VM の作成とインストールの成功を追跡するには、Crosswork サーバーのアクティベーションの監視 （39 ページ）の手順に従います。

Crosswork サーバーのアクティベーションの監視

このトピックでは、Crosswork サーバーのインストールが正常に完了したかどうかを監視し、確認する方法について説明します。

インストーラは、VM 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。続行することを確認したら、インストールが進行し、`installer.log` または `installer_tf.log` ファイルに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` ファイルに記録されます。

管理ユーザー ID について

インストール時に、Crosswork は特別な管理ユーザー ID を作成します（ユーザー名に *cw-admin*、説明に**仮想マシン（VM）管理者**を使用）。ユーザー名 *cw-admin* は、作成時に、インストールマニフェストテンプレートで指定したパスワードを使用します。インストーラがパスワード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* を使用して管理ユーザー ID を作成します。管理ユーザー名とデフォルトのパスワード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 ID ユーザー名 *cw-admin* 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。

展開の進行段階

Cisco Crosswork とその VM ホストの正常な展開は、通常、次の段階を経て進行します。

1. インストーラスクリプトは、Crosswork イメージファイルをサーバーにアップロードします。
2. インストーラは VM を作成し、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。
3. インストーラが VM の電源をオンにします。テンプレートで指定されたパラメータを VM に適用し、VM を再起動して、Kubernetes に登録します。
4. VM がアクセス可能になると、インストーラスクリプトは「Crosswork インストーラの操作が完了しました（Crosswork Installer operation complete）」などの成功メッセージを表示します。その後、インストーラスクリプトが終了し、CLI プロンプトに戻ります。

これらの展開段階のほとんどは、次のセクションインストール中の展開状況の監視 （40 ページ）に記載されている方法を使用して、進行中に監視することができます。

Crosswork インストーラの操作が正常に完了すると、Cisco Crosswork UI にアクセスできるようになり、『*Cisco Crosswork Network Controller Installation Guide*』の「Log into the Cisco Crosswork UI」の説明に従って、Cisco Crosswork UI に ログインして Crosswork のステータスを監視できます。ログインと正常性チェックのプロセスは、単一 VM インストールとクラスターインストールで同じです。

インストール中の展開状況の監視

次の方法を使用して、VMスタートアップと Crosswork インストールの進行状況を監視できます。

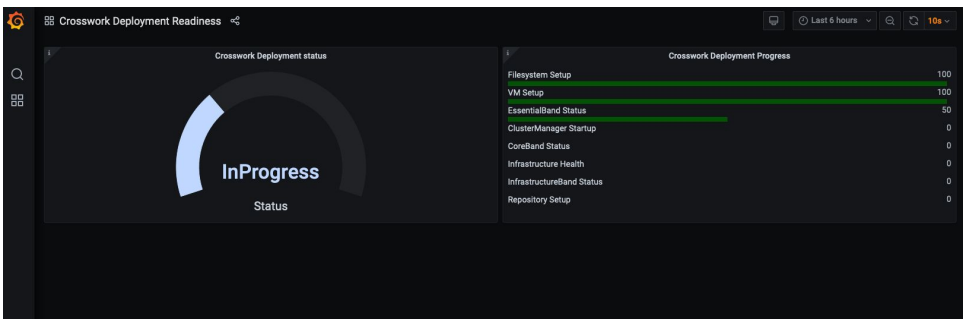
ブラウザでアクセス可能なダッシュボードの使用：

1. VM が作成されると（ステージ 2 の「作成完了」メッセージの後）、次のURL を使用して、ブラウザでアクセス可能な grafana ダッシュボードから Crosswork 展開の準備状況を監視できます。

   `http://{VIP}:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark`

   ここで、*{VIP}* は VM の仮想 IP アドレスです。

   図 *4 : Crosswork* 展開の準備状況



（注） ダッシュボードは次の場合のみ使用できます。

- インストーラが VM の作成を完了した後。
- 合計約 30 分。

2. 展開の最後に、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。

   ダッシュボード URL にアクセスできない場合は、以下で説明する SSH コンソールを使用してインストールプロセスを監視できます。

SSH コンソールの使用：

1. VM のコンソールから進行状況を確認するか、SSH を使用して VM の仮想 IP アドレスにアクセスします。
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モードに切り替えます。
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 Network Controller Installation Guide*』のトピックで説明されているように、Cisco Crosswork UI へのアクセスを試みることができます。

診断アセスメント

展開中に、システムはディスク遅延、IOPS、ネットワーク帯域幅などの VM データストアのリソース値を検証します。いずれかの値が推奨しきい値を下回った場合、診断アセスメントで障害が報告され、インストールを進めるにはユーザのアクションが必要です。『*Cisco Crosswork Network Controller Installation Guide*』の「Cisco Crosswork UI へのログイン（Log into the Cisco Crosswork UI）」のトピックを参照してください。

展開の障害

以下に示すいずれかの障害シナリオが発生した場合、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` ファイルを提供します。

- インストールが不完全である。
- 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。

Crosswork Workflow Manager CAPP のインストール

VMware または KVM 仮想マシンに Crosswork を展開したら、Crosswork CAPP として配布される Crosswork Workflow Manager（CWM）アプリケーションをインストールできます。

始める前に

VMware または KVM ホストに Crosswork を正常に展開していることを確認します。Crosswork がインストールされ、機能していることを確認するには、https://*CrossworkIP*:30603/ で管理 ID を使用して Crosswork にログインします。ここで、*CrossworkIP* は Crosswork がインストールされた仮想マシンの IP アドレスです。

注目 このトピックで示しているダウンロードファイル名は、変更される可能性があります。最新バージョンは、ブラウザで https://software.cisco.com/download/home にアクセスし、**[Crosswork Workflow Manager 2]** を検索することで常に確認できます。

手順

ステップ 1 Crosswork VM ホストから HTTP、HTTPS、または SCP によってアクセス可能なリモートホストで、この手順で使用するダウンロードを含むストレージディレクトリを作成します。

ステップ 2 https://software.cisco.com/download/home から、選択した VM 展開に適した Cisco Crosswork Workflow Manager Advantage Platform Deployment ファイルをリモートホストにダウンロードします。

- VMware 展開の場合：CW-CWM-Solutions-Advantage-2.0.0-14-SVM-7.1.0-48-ova.signed.bin
- KVM 展開の場合：CW-CWM-Solutions-Advantage-2.0.0-14-SVM-7.1.0-48-qcow2.signed.bin

ステップ 3 次のコマンドを使用して、適切な signed.bin ファイルから tar.gz インストーラバンドルを抽出します。

```
sh CW-CWM-Solutions-Advantage-2.0.0-14-SVM-7.1.0-48-ova.tar.gz
```

または

```
sh CW-CWM-Solutions-Advantage-2.0.0-14-SVM-7.1.0-48-qcow2.tar.gz
```

インストーラバンドルの内容と、イメージの検証に必要なファイルは、リモートホストの同じディレクトリに抽出されます。

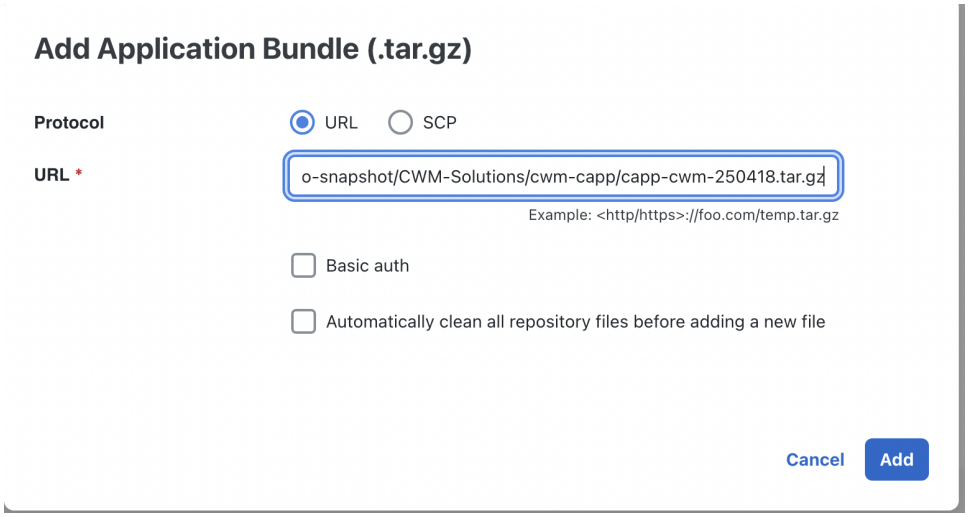
ステップ 4 管理者 ID を使用して Crosswork にログインし、**[管理（Administration）][> Crosswork Manager] > [アプリケーション管理（Application Management）]**を選択します。

ステップ 5 **[新しいファイルの追加（Add new file）]** をクリックし、**[CAPPファイルのアップロード(.tar.gz)（Upload CAPP file (.tar.gz)]** を選択します。

ステップ 6 **[ファイルの追加（.Tar.Gz）（Add File (.Tar.Gz)）]** ページを使用して、まず、CWM CAPP ファイルをシステムに追加するために使用する **[プロトコル（Protocol）]** を選択します。次のアクションを実行します。

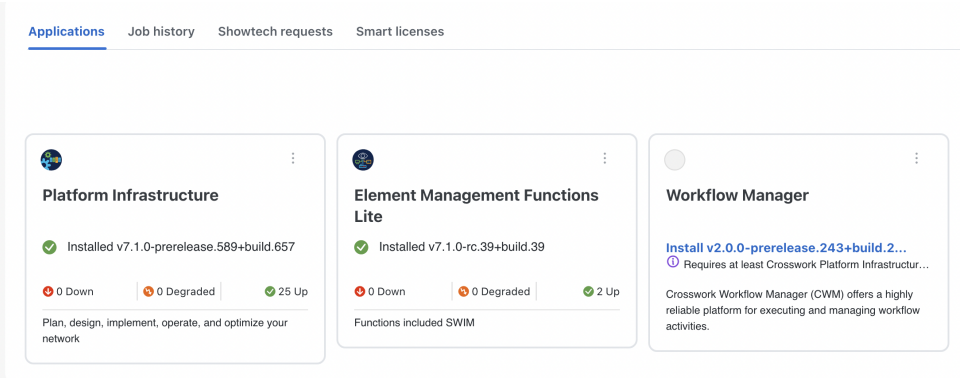
a) **[URL]** を選択した場合：次の図に示されているように、CAPP ファイルが保存されているリモートホストの **URL**（`tar.gz` ファイルへのパスを含む）を入力します。**[基本認証（Basic Auth）]** チェックボックスがオンになっている場合は、リモートホストにアクセスするために必要な **[ユーザー名（Username）]** と **[パスワード（Protocol）]** を入力します。

b) **[SCP]** を選択した場合：リモートホスト上のファイルの **[サーバーパス/場所（Server path/Location）]**、リモートホストサーバーの **[ホスト名/ IPアドレス（Host name/ IP address）]**、**[ポート（Port）]**、ログインの **[ユーザー名（Username）]** と **[パスワード（Password）]** を入力します。



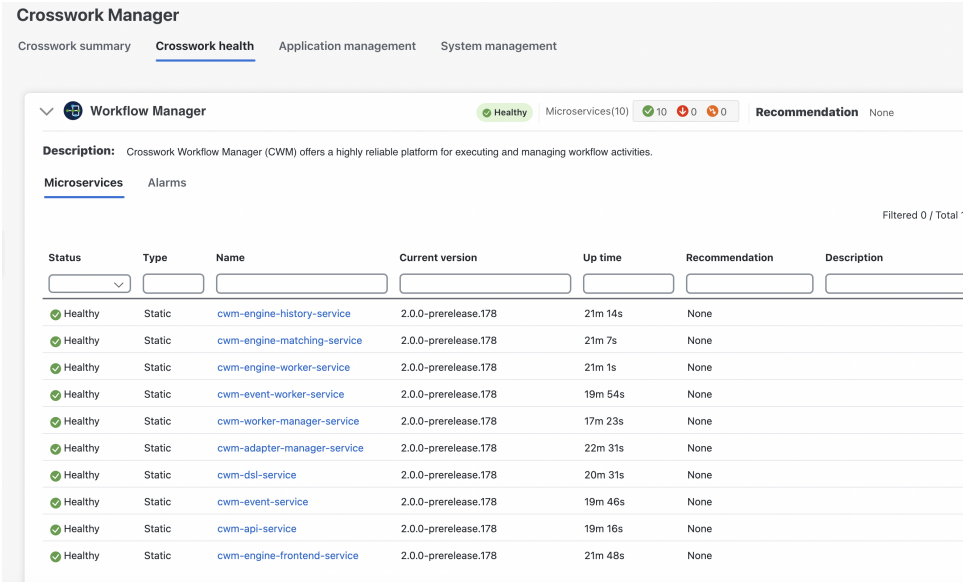
ステップ 7 [Add] をクリックします。**[ジョブ履歴（Job History）]** オプションを選択して、CAPP ファイルのアップロードの進行状況を監視できます。

ステップ 8 アップロードが完了すると、次の図に示すように、**[アプリケーション（Applications）]** ページに **[Workflow Manager]** タイルが表示され、アプリケーションをインストールする準備ができたことを示します。



ステップ 9 **[Workflow Manager]** タイルの **[詳細（More）]** アイコン（3 つのドット）をクリックして **[Workflow Manager]** インストール ポップアップを表示し、**[インストール（Install）]** をクリックします。インストールが完了すると、**[アプリケーション管理（Applications Management）]** > **[ジョブ履歴（Job History)]** タブに、「アクティベーションが成功しました（Activation Successful）」というメッセージが表示されます。

ステップ 10 **[管理（Administration）]** > **[Crosswork Manager]** > **[Crosswork の正常性（Crosswork Health）]** > **[Workflow Manager]**を選択して、インストールが正常に完了したことを確認します。**[マイクロサービス（Microservices）]** タブには、次の図に示されている 10 のマイクロサービスが表示され、すべてのマイクロサービスの **[ステータス（Status）]** 列に **[正常（Healthy）]** と表示されます。



CWM ソリューション CAPP のインストール

CWM をインストールしたら、CWM-S をインストールできます。

始める前に

Crosswork Workflow Manager CAPP のインストール （42 ページ）の説明に従って、Crosswork Workflow Manager（CWM）がインストール済みであることを確認します。これを行うと、Crosswork Workflow Manager ソリューション（CWM-S）インストーラバンドルは、Crosswork Workflow Manager（CWM）CAPPインストーラバンドルを抽出したリモートホスト上の同じディレクトリに抽出されます。

手順

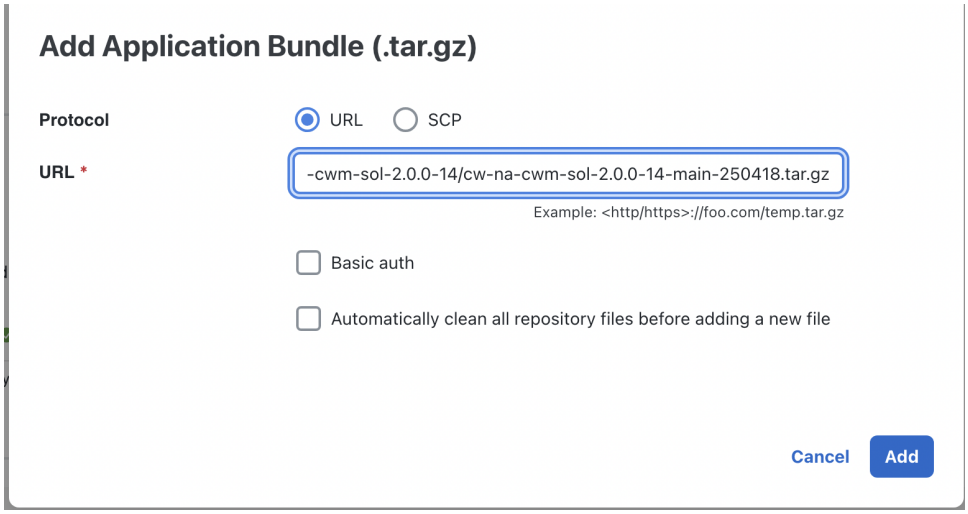
ステップ 1 まだ行っていない場合は、管理者 ID を使用して Crosswork にログインし、**[管理（Administration）][** > **[Crosswork Manager]** > **[アプリケーション管理（Application Management）]**を選択します。

ステップ 2 **[新しいファイルの追加（Add new file）]** をクリックし、**[CAPPファイルのアップロード(.tar.gz)（Upload CAPP file (.tar.gz)]** を選択します。

ステップ 3 **[ファイルの追加（.Tar.Gz）（Add File (.Tar.Gz)）]** ページを使用して、まず、CWM ソリューション CAPP ファイルをシステムに追加するために使用する **[プロトコル（Protocol）]** を選択します。次のアクションを実行します。

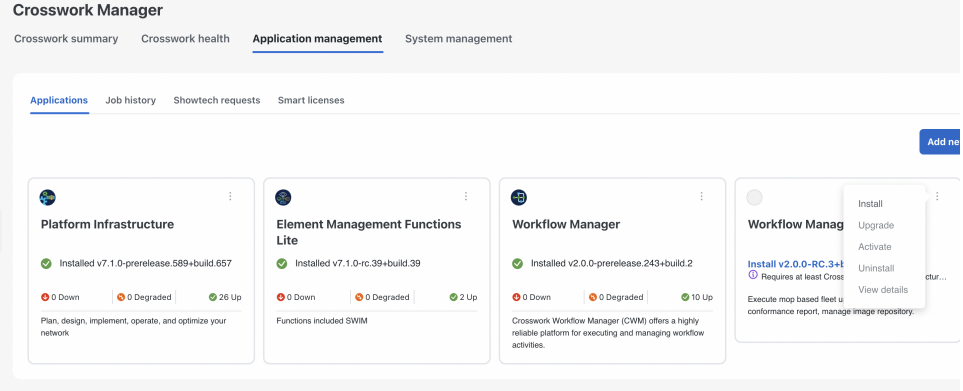
a) **[URL]** を選択した場合：次の図に示されているように、CAPP ファイルが保存されているリモートホストの **URL**（`tar.gz` ファイルへのパスを含む）を入力します。**[基本認証（Basic Auth）]** チェックボックスがオンになっている場合は、リモートホストにアクセスするために必要な **[ユーザー名（Username）]** と **[パスワード（Protocol）]** を入力します。

b) **[SCP]** を選択した場合：ファイルの **[サーバーパス/場所（Server path/Location）]**、サーバーの **[ホスト名/IPアドレス（Host name/ IP address）]**、**[ポート（Port）]**、ログインの **[ユーザー名（Username）]** と **[パスワード（Password）]** を入力します。

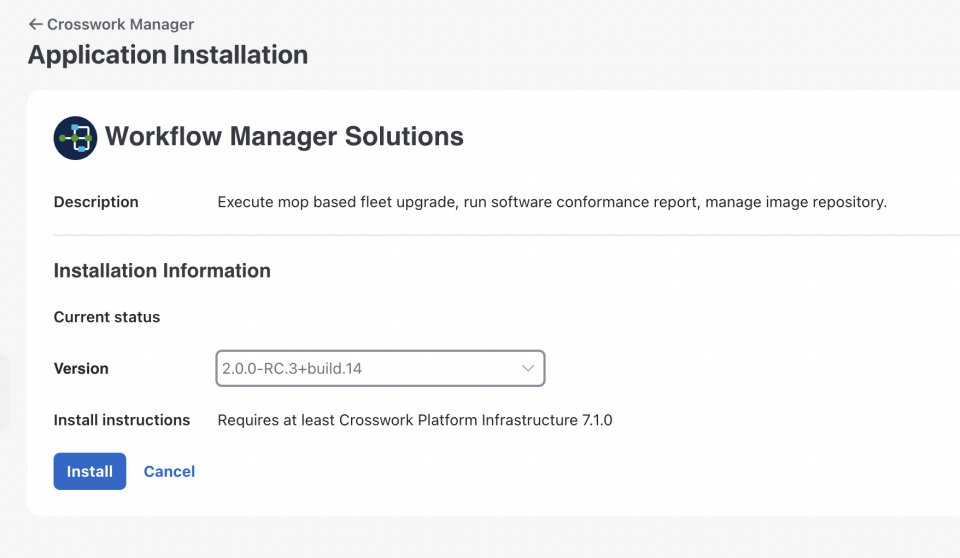


ステップ 4 [Add] をクリックします。アップロードの進行中は、**[ジョブ履歴（Job History）]** オプションを選択してアップロードを監視することができます。

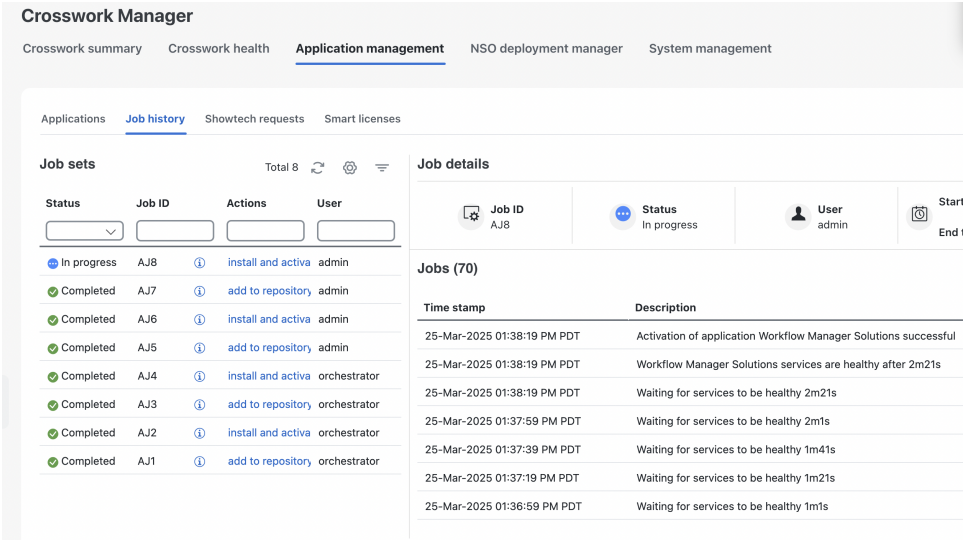
ステップ 5 追加が完了すると、**[アプリケーション（Applications）]** ページの右端にある **[Workflow Manager]** タイルの横に **[Workflow Manager Solutions]** タイルが表示され、**Workflow Manager Solutions** アプリケーションのインストール準備が整ったことが示されます。



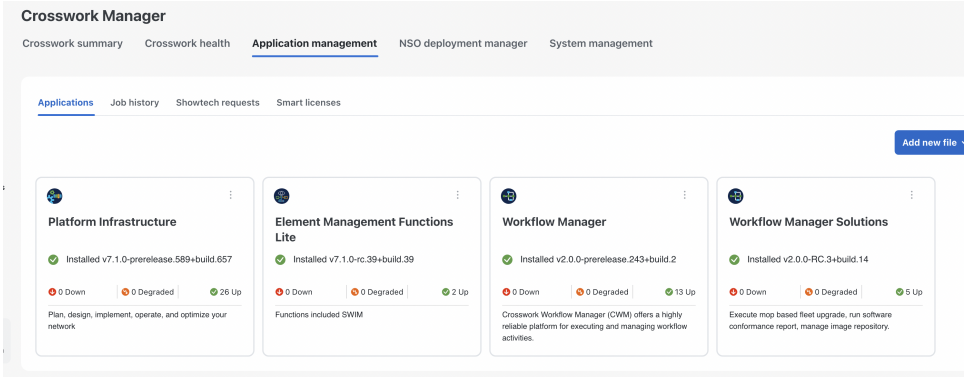
ステップ 6 **[Workflow Manager ソリューション（Workflow Manager Solutions）]** タイルの **[詳細（More）]** アイコン（3 つのドット）をクリックして、インストール ポップアップ メニューを表示し、**[インストール（Install）]** をクリックします。



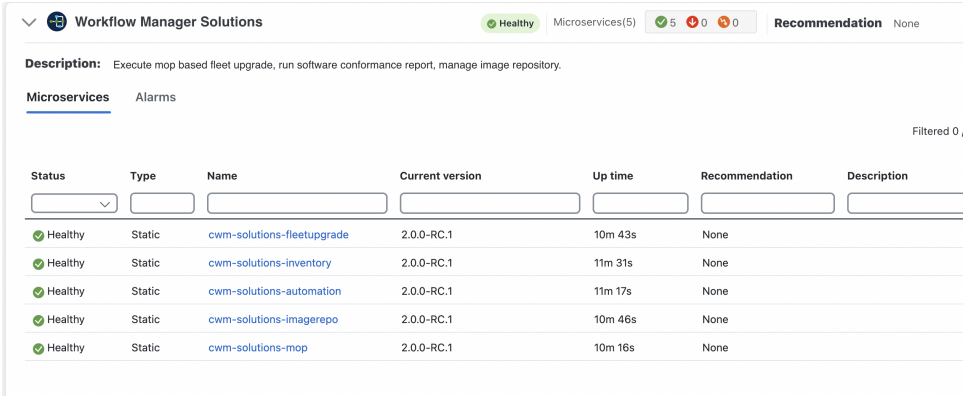
ステップ 7 インストールが完了すると、**[アプリケーション管理（Applications Management）]** > **[ジョブ履歴（Job History)]** タブに、「Workflow Manager ソリューションアプリケーションのアクティベーションが成功しました（Activation of application Workflow Manager Solutions Successful）」というメッセージが表示されます。



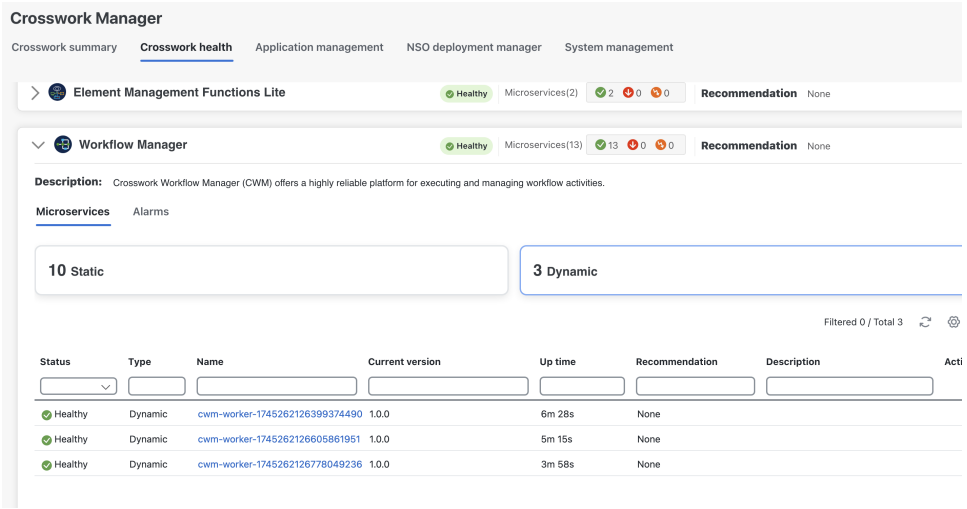
ステップ 8 **[アプリケーション管理（Application Management）] > [アプリケーション（Applications ）]** タブに、[Workflow Manager] と [Workflow Manager ソリューション（Workflow Manager Solutions）] の両方が稼働していることが表示されます。



ステップ 9 **[管理（Administration）] > [Crosswork Manager] > [Crosswork の正常性（Crosswork Health）] > [Workflow Manager ソリューション（Workflow Manager Solutions）]**を選択します。**[マイクロサービス（Microservices）]** タブに、5 つの CWM ソリューションのマイクロサービスがすべて **[正常（Healthy）]** 状態であると表示されている必要があります。



ステップ 10 最後に、CWM ソリューションは、3 つのダイナミックサービスポッドを CWM に追加します。これらは、CWM ソリューションによって自動的にインストールされた 3 つの CWM アダプタのワーカーポッドです。それらは、**[管理（Administration）] > [Crosswork Manager] > [Crosswork 正常性（Crosswork Health）] > [Workflow Manager]** の下にあります（[Workflow Manager ソリューション（Workflow Manager Solutions）] の下ではありません）。



ログイン情報プロファイルの作成

Crosswork ログイン情報プロファイルは、ログインユーザー名とパスワードを安全な方法で保存します。Crosswork はこれらのサービスを使用して、Crosswork 向けに特化したサービスを実行するヘルパーアプリケーションであるプロバイダー（Cisco NSO など）との認証を行います。また、Crosswork とそのプロバイダーは、ネットワークデバイスにアクセスする際にも、ログイン情報プロファイルを使用して認証を行います。

この手順では、2 つのログイン情報プロファイルを作成します。Crosswork Workflow Manager ソリューションは、最初のプロファイルを使用して NSO にログインし、NSO に対してネット

ワークデバイスへのアクセスや設定変更の実行を要求します。NSOは2番目のプロファイルを使用してネットワークデバイスにログインします。

ログイン情報プロファイルで提供するログイン情報はプロトコル固有です。つまり、各ログイン情報プロファイルで「通信タイプ」（プロトコルとも呼ばれる）を指定し、プロトコルごとに、デバイスまたはアプリケーションでそのプロトコルと連携するログイン情報のセット（通常は、ユーザー名とパスワード）を1セット指定します。次に、プロファイルに使用させるすべてのプロトコルとログイン情報がコレクションに追加されるまで、プロトコルを**さらに追加**し、対応するログイン情報のセットを追加します。

同じプロトコルに対して2つの異なるログイン情報セットを持つログイン情報プロファイルを設定することはできません。あるログイン情報プロファイルで指定済みのプロトコルの別のログイン情報セットを指定する場合は、別のログイン情報プロファイルを作成する必要があります。

ログイン情報プロファイルとプロバイダーの詳細については、『Cisco Crosswork Network Controller Administration Guide』の「Credential Profiles」を参照してください。

始める前に

CWM ソリューション CAPP のインストール （44 ページ）の手順に従ってCWM ソリューションがインストール済みであることを確認します。

手順

ステップ 1 Crossworkにログインし、**[デバイス管理（Device Management）]**>**[ログイン情報プロファイル（Credential Profiles）]**を選択します。Crossworkは、**[ログイン情報プロファイル（Credential Profiles）]**リストを表示します。

ステップ 2 **NSO プロバイダーのログイン情報プロファイルを次のように作成します。**

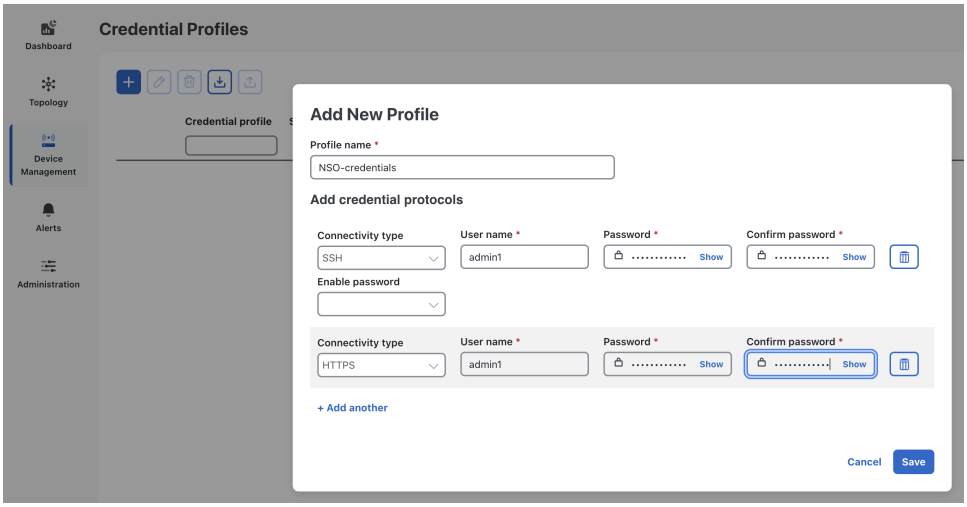
a) **+** をクリックして、NSO プロバイダーのログイン情報プロファイルを追加します。

b) **[新しいプロファイルの追加（Add New Profile）]** ウィンドウのフィールドに次のように入力します。

フィールドの内容	入力または選択する内容
プロファイル名（または意味のある任意の一意の名前）	**NSO ログイン情報**（または意味のある任意の一意の名前）
接続タイプ（Connectivity type）	**SSH**
ユーザー名（User name）	NSO サーバーの SSH 管理ユーザーのユーザー名。このユーザー名は、NSO サーバーで作成する管理者権限を持つ専用のCWMソリューション用ユーザー名にすることができます。いずれの場合も、この管理者ユーザー名は、NSO サーバーの `ncsadmin` グループに含まれているユーザー名である必要があります。

フィールドの内容	入力または選択する内容
パスワード（**Password**）	このユーザー名のパスワード。
パスワードの確認（**Confirm password**）	**[パスワード（Password）]** に入力したのと同じパスワード。
パスワードを有効にする（**Enable password**）	このフィールドは空欄のままにします。

c) **[さらに追加（+ Add another）]** をクリックして、同じ NSO ログイン情報プロファイルに追加する別の接続プロトコルのセットを表示します。今回は、**[接続タイプ（Connectivity type）]** として **[HTTPS]** を選択し、ステップ 2b と同じように、このプロトコルの NSO ユーザーとパスワードの情報を入力します。次に例を示します。



d) 作業が終了したら、**[保存（Save）]** をクリックして NSO ログイン情報プロファイルを保存します。指定した **[プロファイル名（Profile name）]** が **[ログイン情報プロファイル（Credential Profiles）]** リストに表示されます。

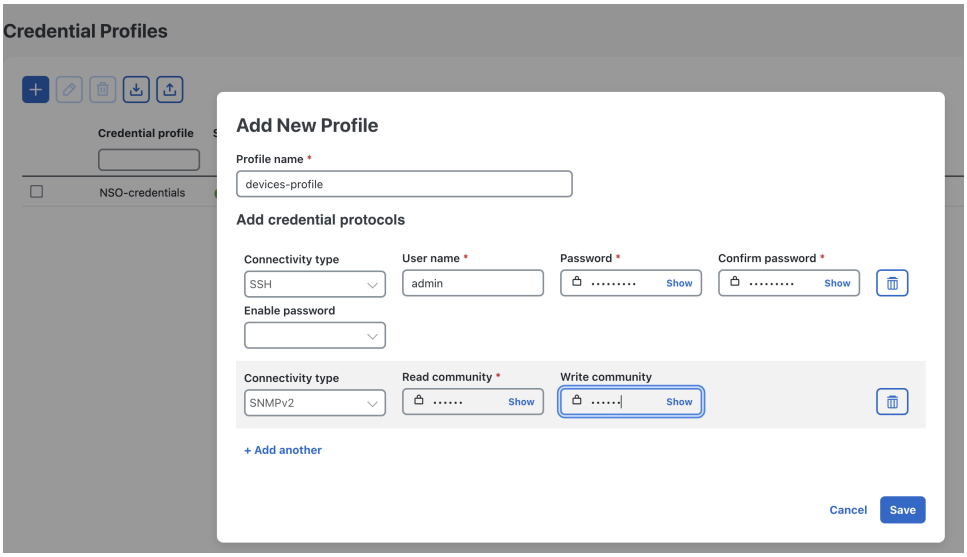
ステップ 3 （オプション）ステップ 2 を繰り返して、デバイスの別のログイン情報プロファイルを作成します。

Crosswork Workflow Manager ソリューションを使用して管理する予定のデバイスに適した数のデバイスログイン情報とプロトコルを追加することをお勧めします。管理対象のデバイスがそれらのプロトコルを使用していない場合は、ログイン情報プロファイルにプロトコルを追加しないでください。次の表は、Crosswork ログイン情報プロファイルに追加できるすべてのプロトコルと、それらがサポートするデバイス機能の種類をまとめたものです。

プロトコル	用途
SSH	IoT デバイス制御と安全なファイル転送を提供するデバイス。デバイス管理に一般的に使用されるプロトコル。

プロトコル	用途
NETCONF	リモート設定と RPC 交換。通常は SSH で使用されます。
HTTP	安全でない Web リソースへのアクセスを提供するホスト。
HTTPS	安全で暗号化された Web リソース交換を提供するホスト。
SCP	SSH を使用した安全な暗号化されたファイル交換を提供するデバイス。
TELNET	コンソールアクセス用の一般的なプロトコルであり、ほとんどの Cisco XR、Cisco XE、およびJuniper Junos デバイスに使用されます。
SNMPv2	多くのデバイスで使用される、デバイス管理の標準プロトコル。
gRPC	高パフォーマンス分散システムに参加するデバイス。これにより、クライアント アプリケーションは、ローカルであるかのように、サーバーアプリケーションでリモートプロシージャコールを直接呼び出すことができます。REST の代替手段。
SNMPv3	一部の新しいデバイスで使用される、デバイス管理用の標準プロトコルの最新バージョン。
gNMI	セキュアなストリーミング形式でリアルタイムのネットワーク監視、テレメトリ、およびデバイス管理を提供するデバイス。データセンターやサービスプロバイダーで SNMP の代わりによく使用されます。

次の図に、最も一般的に使用される 2 つのプロトコル用の単一のデバイスログイン情報プロファイルを作成する方法を示します。同じ 2 つのプロトコルを使用しているが、異なるログイン情報を持つデバイスのグループがある場合は、このように複数のログイン情報プロファイルを作成できます。



NSO パッケージのインストール前の作業

NSO の CWM ソリューションパッケージをインストールする前に、追加の Python パッケージが NSO にインストールされていること、および NSO が REST をサポートしていることを確認する必要があります。CWM ソリューションは SSL と HTTPS の両方を使用できるため、必要に応じて REST 設定で両方を有効にすることを選択できます。SSL を有効にする場合は、SSL 証明書ファイルをインストールし、RESTCONF 設定でその場所を指定する必要があります。

始める前に

インストール要件への適合 （2 ページ）で説明されているように、NSO インストールの基本要件を満たしていることを確認します。REST 設定の一部として HTTPS/ SSL を有効にする場合は、このタスクを完了する前に、NCS 構成ディレクトリに SSL 証明書とキーファイルを作成してインストールすることを推奨します。

手順

ステップ 1 NSO サーバーに次の Python パッケージをインストールします。

```
~$ sudo pip install textfsm
~$ sudo pip install jinja2
~$ sudo pip instapp pyyaml
~$ sudo pip install pycryptodome
```

ステップ 2 NSO `ncs.conf` ファイルを以下に示すように編集し、REST サポートを有効にします。*<ssl>* ブロックは任意であり、REST やその他のコマンドと区別するために、以下では*イタリック体*で示されています。次に例を示します。

```
sudo vi /etc/ncs/ncs.conf

 <webui>
    <enabled>true</enabled>
    <transport>

<ssl>
  <enabled>true</enabled>
  <ip>0.0.0.0</ip>
  <port>8888</port>
  <key-file>${NCS_CONFIG_DIR}/ssl/cert/host.key</key-file>
  <cert-file>${NCS_CONFIG_DIR}/ssl/cert/host.cert</cert-file>
  <extra-listen>
    <ip>::</ip>
    <port>8888</port>
  </extra-listen>
      </ssl>
    </transport>

    <cgi>
      <enabled>true</enabled>
      <php>
        <enabled>false</enabled>
      </php>
    </cgi>
```

```
  </webui>

  <restconf>
    <enabled>true</enabled>
  </restconf>
```

ステップ 3 編集が完了したら、ncs.conf ファイルを保存し、NSO を再起動します。次に例を示します。

```
sudo systemctl restart ncs
```

ステップ 4 管理者ユーザー ID を使用して、NSO インストールで REST が正しく機能していることを確認します。次に例を示します。

```
admin1@ncs% run show ncs-state rest
ncs-state rest listen ssl
 ip   ::
 port 8888
ncs-state rest listen ssl
 ip   0.0.0.0
 port 8888
```

ステップ 5 次の NSO グローバル構成設定を指定します。

```
admin1@ncs% show devices global-settings
connect-timeout 600;
read-timeout    600;
write-timeout   600;
ssh-algorithms {
    public-key [ ssh-rsa ];
}
trace           pretty;
}
```

ステップ 6 コメント付きの行 #End of file の前に Linux オペレーティングシステムの ulimit 値を追加します（まだない場合）。次に例を示します。

a) /etc/security/limits.conf ファイルを確認します。

```
$ grep hard /etc/security/limits.conf
$ grep soft /etc/security/limits.conf
```

b) 構成されていない場合は、/etc/security/limits.conf ファイルを編集し、次の行を追加します。

```
* soft nproc 65535
 * hard nproc 65535
 * soft nofile 65535
 * hard nofile 65535
 * soft memlock 65535
 * hard memlock 65535
```

c) sysctl -p スクリプトを実行してパラメータを設定します。

d) システムからログアウトし、再度ログインして新しい値を適用します。

e) Linux オペレーティングシステムの ulimit 値が適用されていることを確認します。

```
$ ulimit -a core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 95697
max locked memory       (kbytes, -l) 65536
max memory size         (kbytes, -m)
unlimited open files                         (-n) 65535
pipe size            (512 bytes, -p) 8
```

```
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t)
unlimited max user processes              (-u) 65535
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

ステップ 7 NETCONF Access Control Model（NACM）ルールリストが、ncsadmin および Linux ユーザーに NSO で機能を実行する権限を付与していることを確認します。次に例を示します。

```
admin1@ncs% show nacm
read-default     deny;
write-default    deny;
exec-default     deny;
groups {
    group ncsadmin {
        user-name [ admin1 private ];
    }
    group ncsoper {
        user-name [ public ];
    }
}
```

ユーザーを認証グループに追加するなど、ユーザーを追加する方法については、*NSO*アドミニストレーション ガイドのトピック「ユーザーの追加」を参照してください。

ステップ 8 フリートアップグレードを使用してサポートするデバイスを決定し、次のように、それらのデバイスに適した NSO Network Element Drivers （NED）をインストールします。

a) アカウントチームが提供した NED ライセンス証明書の URL を使用して、Cisco ソフトウェアダウンロードからデバイスの NED を NSO ホストのリソースにダウンロードします。NED は `signed.bin` ファイルで、これを実行して NED コードを検証および抽出する必要があります。

b) *NSO* アドミニストレーション ガイドののトピック「新しい NED のインストール」の説明に従って、ダウンロードした NED を確認、抽出、インストールします。

c) 新しい NED のインストールが完了したら、NSO を再起動します。例：

```
sudo systemctl restart ncs
```

NSO プロバイダープロファイルの作成

Crosswork プロバイダーは、Crosswork が特別な機能を実行できるようにするヘルパーアプリケーションです。このタスクでは、NSO ログイン情報プロファイルを使用して NSO プロバイダーを作成し、Crosswork での認証に必要な情報を提供します。これにより、NSO は、作成したデバイスログイン情報プロファイルに保存されているデバイス認証情報にアクセスできるようになります。

始める前に

ログイン情報プロファイルの作成 （48 ページ）で説明されているログイン情報プロファイルをすでに作成していることを確認します。次のタスクを完了するには、そのタスクで作成した NSO ログイン情報プロファイルの名前が必要です。

手順

ステップ 1 Crossworkにログインし、**[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 **[+]** をクリックして NSO プロバイダーを追加します。

ステップ 3 **[新しいプロファイルの追加（Add New Profile）]** ウィンドウの最初のフィールドセットに次のように入力します。

フィールドの内容	入力または選択する内容
プロバイダ名（Provider name）	プロバイダーの名前（**NSO**など）。
ログイン情報プロファイル（Credential Profile）	ログイン情報プロファイルの作成 （48 ページ）で作成した NSO ログイン情報プロファイルの名前。
ファミリ（Family）	**NSO**

ステップ 4 **[接続タイプ（Connection type(s)）]** セクションのフィールドに次のように入力します。

フィールドの内容	入力または選択する内容
プロトコル	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主要プロトコルを選択します。**[HTTPS]** を選択します。 このプロバイダの接続プロトコルをさらに追加するには、最初の行の最後にある ⊕ アイコンをクリックします。入力したプロトコルを削除するには、その行の横にある ⊗ アイコンをクリックします。 同じプロトコルを複数セットなど、必要な数の接続の詳細のセットを入力できます。
サーバーの詳細（Server details）	次のいずれかのオプションを選択します。 • **IPアドレス**、次にNSOホストの**IPアドレス**（IPv4またはIPv6、サブネットマスク）を入力します。 • **FQDN**、次にNSOホストの**[ドメイン名（Domain Name）]**と**[ホスト名（Host Name）]**を入力します。

フィールドの内容	入力または選択する内容
ポート	NSO ホストへの接続に使用するポート番号。これは、設定するプロトコルに対応するポートです。たとえば、NSO ホストとの通信に使用するプロトコルが SSH の場合、ポート番号は通常 22 です。
タイムアウト(秒)	接続がタイムアウトするまで待機する時間を入力します（秒単位）。デフォルトは 30 秒です。

ステップ 5 **[プロバイダプロパティ（Provider Properties）]** セクションのエントリはオプションです。必要に応じて、次のキー/値のペアのうち 1 つまたは複数を入力します。

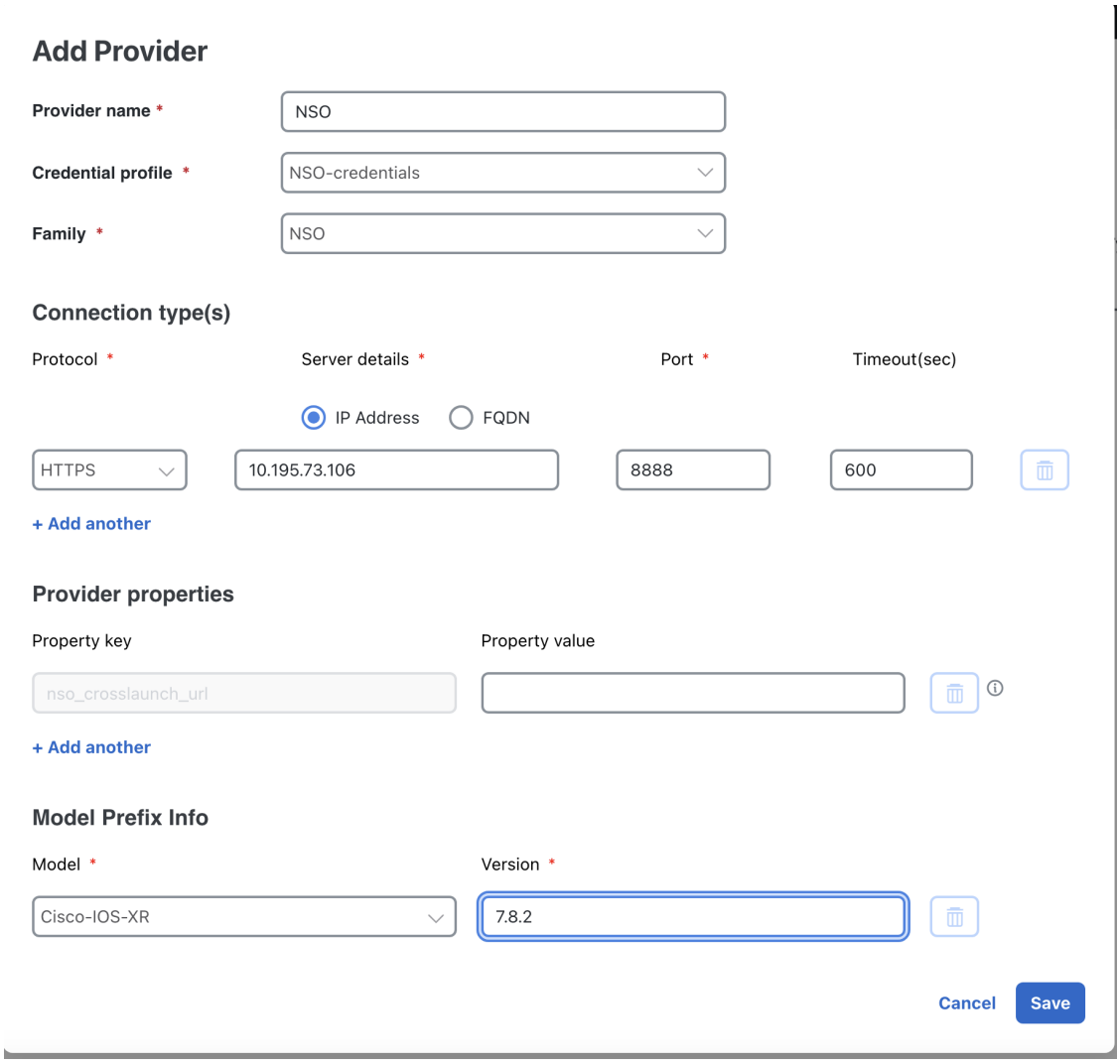
プロパティキー	値
forward	**true** このプロパティは、Crosswork を使用して UI 内でプロビジョニング操作をできるようにし、Crosswork API ゲートウェイを介して NSO へのノースバウンド インターフェイスを有効にする場合に必要です。 （注） **forward** のデフォルト値は「false」です。これが変更されていない場合、Crosswork に追加されたデバイスは NSO に追加されません。この設定は、**[ポリシーの編集（Edit Policy）]** オプションと組み合わせて使用されます。
nso_crosslaunch_url （注） このプロパティは、NSO プロバイダーにのみ使用されます。	クロス起動 NSO の URL を **https://<NSO IP address/FQDN>:port number** の形式で入力します。 Crosswork UI から NSO アプリケーションのクロス起動を有効にするには、有効なプロトコル（**HTTP** または **HTTPS**）が必要であり、プロバイダーに到達可能である必要があります。 クロス起動アイコンが **[プロバイダー名（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。

input_url_prefix
（注）
このプロパティは、NSO LSA プロバイダーにのみ使用されます。
	RFS ID を **/rfc-x** の形式で入力します。ここで、**x** は RFS ノードの番号を表します。
	`Example (for RFS node 1):`
	`input_url_prefix: /rfc-1`

ステップ 6 **[モデルプレフィックス情報（Model Prefix Info）]** セクションのフィールドに次のように入力します。

フィールドの内容	入力または選択する内容
モデル（**Model**）	Cisco NSO で使用される NED CLI に一致するモデルプレフィックスを選択します。有効な値は次のとおりです。 **`Cisco-IOS-XR`** **`Cisco-IOS-XE`** **`Cisco-NX-OS`** テレメトリでは、**`Cisco-IOS-XR`** のみがサポートされています。 この NSO プロバイダのモデルプレフィックス情報をさらに追加するには、**[モデルプレフィックス情報（Model Prefix Info）]** セクションの任意の行の末尾にある ⊕ アイコンをクリックします。入力したモデルプレフィックスを削除するには、その行の横にある ⊗ アイコンをクリックします。
バージョン（**Version**）	NSO サーバーで使用されている Cisco NSO NED ドライバのバージョンを入力します。

ステップ 7 作業が終了したら、**[保存（Save）]** をクリックして NSO プロバイダープロファイルを保存します。Crosswork が NSO に到達しようとしている間、遅延が発生すると、**[プロバイダーアクセスの管理（Manage Provider Access）]** リストにこのプロファイルが表示されます。



NSO 機能パックの展開

Crosswork の NSO 展開マネージャを使用して、NSO 機能パックを NSO に展開します。これらの機能パックは、基本的なインベントリ管理と、Crosswork Workflow Manager ソリューションを使用するために必要なその他の NSO 機能を提供します。また、NSO に直接ログインして、NACM が NSO で有効になっており、その他の NSO 設定が適切に設定されていることを確認する必要もあります。

始める前に

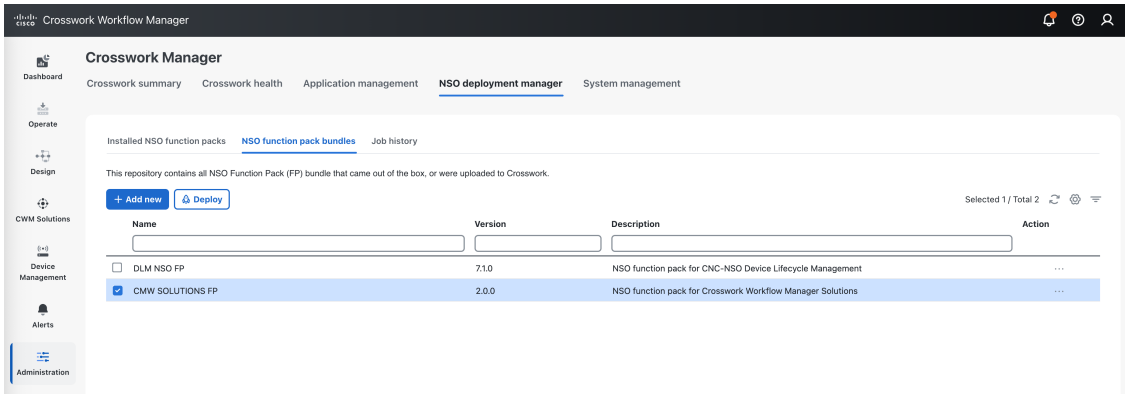
NSO プロバイダープロファイルの作成 （54 ページ）で説明されているように、プロバイダーとして NSO を追加したことを確認します。

手順

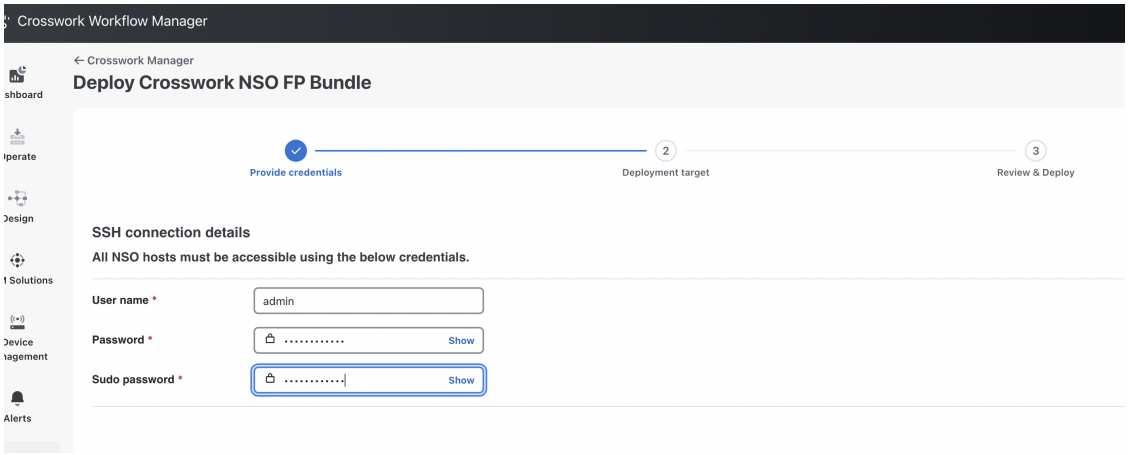
ステップ 1 シスコセールスチームに問い合わせて、ネットワーク環境に必要な Cisco NSO Network Element Drivers（NED）を特定してダウンロードしてください。先に進む前に、「新しいNEDのインストール」で説明されているように、これらの NED を NSO サーバーにインストールします。

ステップ 2 NED がインストールされたら、Crosswork Workflow Manager にログインし、**[管理（Administration）]** > **[Crosswork Manager]** > **[NSO展開マネージャ（NSO Deployment Manager）]**を選択します。

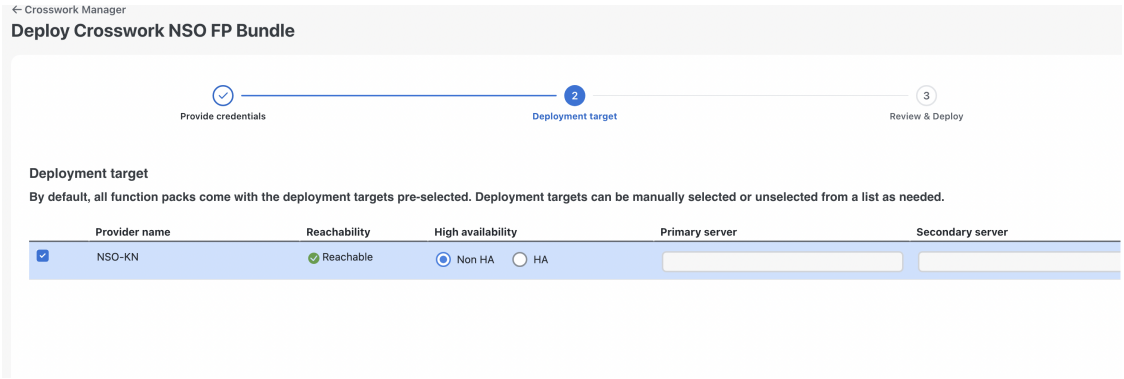
ステップ 3 **[NSO展開マネージャ（NSO Deployment Manager）]** で、**[NSO機能パックバンドル（NSO Function pack bundles）]** タブを選択し、**[CWMソリューションFPS（CWM SOLUTIONS FPS）]** の横にあるチェックボックスをオンにします。次に、**[展開（Deploy）]**ボタンをクリックして、展開プロセスを開始します。



ステップ 4 最初の **[ログイン情報の提供（Provide credentials）]** ページでプロンプトが表示されたら、SSH の**ユーザー名、パスワード**、および **Sudo パスワード**ログイン情報を入力します。

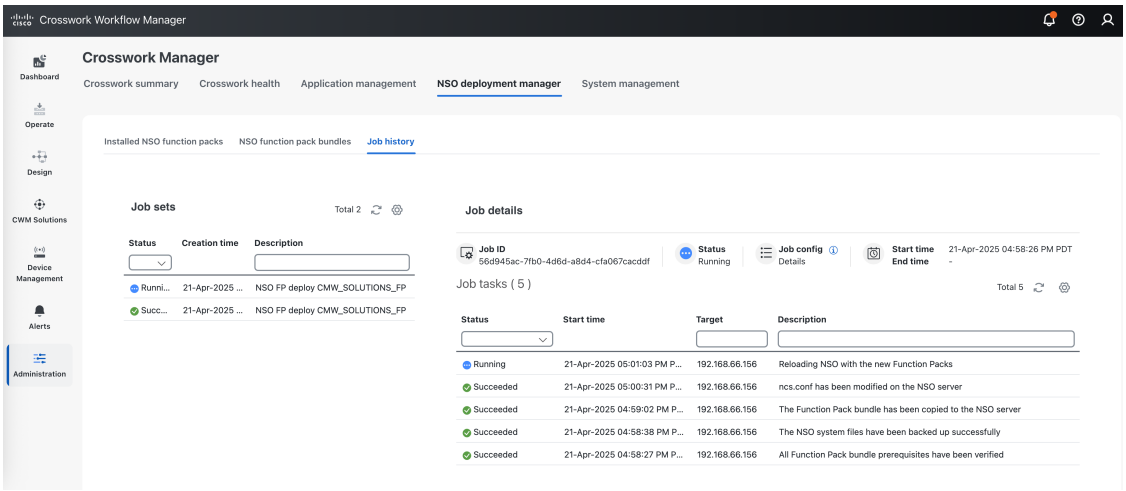


ステップ 5 **[展開ターゲット（Deployment target）]** ページで、以下に示すように、**[高可用性（High Availability）]** 列で **[非HA （Non-HA）]** を選択します。



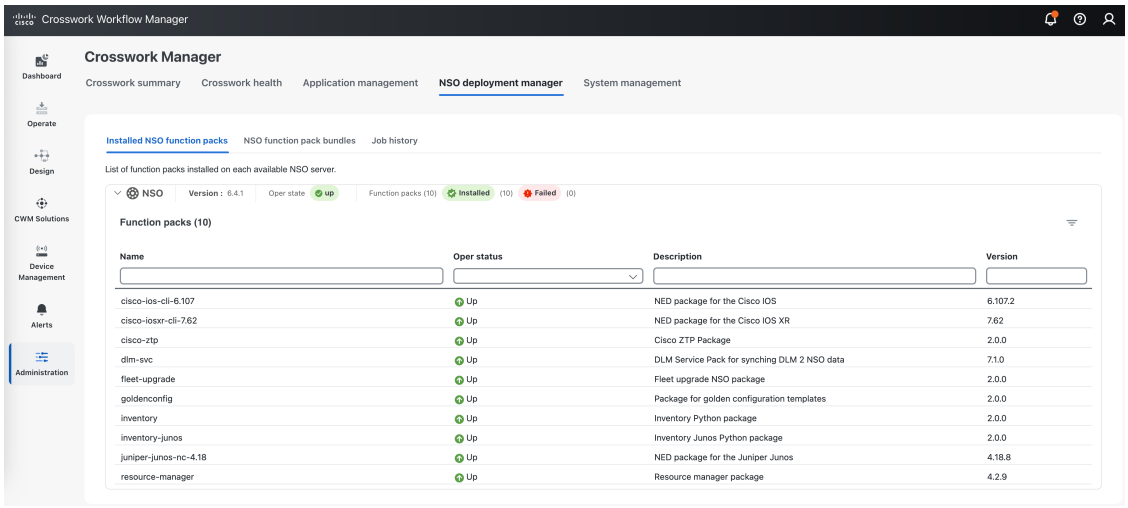
ステップ 6 **[確認と展開（Review & Deploy）]** ページでプロンプトが表示されたら、**[展開（Deploy）]**をクリックします。

ステップ 7 **[ジョブ履歴（Job History）]** タブをクリックして、NSO の展開を進行中に監視します。実行中のジョブの **[ジョブの詳細（Job Details）]** ウィンドウに一覧表示されるパッケージが表示されます。



ステップ 8 ジョブが **[成功（Succeeded）]** と表示されている場合は、**[インストールされているNSO機能パック（Installed NSO Function packs）]** タブをクリックし、NSO プロバイダーを展開して、パッケージがすべてインストールされていることを確認します。

パッケージリストは、以下の図のように表示されるはずです。



また、以下に示すオプションを指定して NSO で `show packages` コマンドを実行し、コマンド出力を次の図の結果と比較することで、すべてのパッケージが正しくインストールされていることを確認することもできます。この図は、パッケージの最小のリストを表しています。より多くのパッケージが含まれている場合や、一部のパッケージがより新しいバージョンになっている場合があります。

```
admin1@ncs% run show packages package oper-status | tab

                          PROGRAM
                          CODE      JAVA             PYTHON
NAME                      UP  ERROR     UNINITIALIZED  UNINITIALIZED
-------------------------------------------------------------------
cisco-ios-cli-6.107       X   -         -              -
cisco-iosxr-cli-7.62      X   -         -              -
cisco-ztp                 X   -         -              -
dlm-svc                   X   -         -              -
fleet-upgrade             X   -         -              -
goldenconfig              X   -         -              -
inventory                 X   -         -              -
inventory-junos           X   -         -              -
juniper-junos-nc-4.18     X   -         -              -
resource-manager          X   -         -              -

admin1@ncs% run show packages package package-version  | tab
                          PACKAGE
NAME                      VERSION
-------------------------------
cisco-ios-cli-6.107       6.107.2
cisco-iosxr-cli-7.62      7.62
cisco-ztp                 2.0.0
dlm-svc                   7.1.0
fleet-upgrade             2.0.0
goldenconfig              2.0.0
inventory                 2.0.0
inventory-junos           2.0.0
juniper-junos-nc-4.18     4.18.8
resource-manager          4.2.9
```

ステップ 9 まだ行っていない場合は、NSO にログインし、構成モードで次のデバイスグローバル設定を行います。これらの NSO 設定は、Crosswork Workflow Manager ソリューションに必要です。

```
admin@ncs% set devices global-settings connect-timeout 600
admin@ncs% set devices global-settings read-timeout 600
```

```
admin@ncs% set devices global-settings write-timeout 600
admin@ncs% set devices global-settings ssh-algorithms public-key ssh-rsa
admin@ncs% set devices global-settings trace pretty
admin@ncs% set devices global-settings ned-settings
                          cisco-iosxr read admin-show-running-config false
admin@ncs% commit

admin@ncs% show devices global-settings
connect-timeout 600;
read-timeout    600;
write-timeout   600;
ssh-algorithms {
    public-key [ ssh-rsa ];
}
trace           pretty;
ned-settings {
    cisco-iosxr {
        read {
            admin-show-running-config false;
        }
    }
}
```

ステップ 10 NSO にはNETCONFアクセス制御モデル（NACM）が必要です。NACMルールリストが、ncsadminおよびLinuxユーザーに対してNSO上で機能を実行する権限を付与していることを確認してください。次に例を示します。

```
admin@ncs% set nacm groups group ncsadmin user-name admin
admin@ncs% commit


admin@ncs% show nacm
read-default     deny;
write-default    deny;
exec-default     deny;
groups {
    group ncsadmin {
        user-name [ admin private ];
    }
    group ncsoper {
        user-name [ public ];
    }
}
```

ステップ 11 提供されたバンドルからncs_backup.sh、ncs_restore.sh、get_technical_support_data.shのスクリプトをNCS_RUN_DIRの下のscriptsディレクトリにコピーし、コピーしたスクリプトの権限を更新して実行可能にします。

```
# Locate the NCS_RUN_DIR using the following command
cat /etc/systemd/system/ncs.service | grep NCS_RUN_DIR=

# Update the permissions
chmod +x ncs_backup.sh ncs_restore.sh get_technical_support_data.sh
```

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。