Crosswork Data Gateway のインストール

ここでは、次の内容について説明します。

Cisco Crosswork Data Gateway のインストール

この手順は、Cisco Crosswork Data Gateway を初めてインストールする場合や、追加の Cisco Crosswork Data Gateway VM を追加する場合に使用できます。

（注） Cisco Crosswork で Cisco Crosswork Data Gateway を再展開する場合は、自動登録が機能するように以前の Cisco Crosswork エントリを削除します。

Cisco Crosswork Data Gateway の展開とセットアップのワークフロー

Cisco Crosswork で使用する Crosswork Data Gateway VM を展開して設定するには、次の手順を実行します。

1. Cisco Crosswork Data Gateway の展開タイプ（標準または拡張）を選択します。「Cisco Crosswork Data Gateway の要件」を参照してください。
2. 使用するプラットフォームに Cisco Crosswork Data Gateway をインストールします。

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 （13 ページ）
	OVF ツールを使用した Cisco Crosswork Data Gateway のインストール （19 ページ）

Cisco CSP	Cisco CSP への Cisco Crosswork Data Gateway のインストール （22 ページ）

3. Cisco Crosswork Data Gateway VM でタイムゾーンを設定します。「タイムゾーンの設定 （32 ページ）」を参照してください。
4. Cisco Crosswork への Cisco Crosswork Data Gateway の登録を確認します。「Cisco Crosswork Data Gateway の認証と登録 （34 ページ）」を参照してください。

Cisco Crosswork Data Gateway が Cisco Crosswork に正常に登録されたことを確認したら、Cisco Crosswork Data Gateway プールを作成し、Cisco Crosswork Data Gateway VM をプールに追加します。

（注） 負荷または拡張のために複数の Cisco Crosswork Data Gateway を使用する場合や 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、それらを Data Gateway のプールに追加することを推奨します。

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

Cisco Crosswork Data Gateway のインストールを開始する前に、次の項で説明するパラメータと可能な展開シナリオを確認してください。上記の方法を使用して Cisco Crosswork Data Gateway をインストールする場合は、この項を参照してパラメータ値を指定する必要があります。

（注） 証明書チェーンは、VM の事前設定された証明書または生成済みの証明書を上書きし、SCP URI（user:host:/path/to/file）として指定されます。

* は必須パラメータであることを示します。その他はオプションです。必要な展開シナリオの種類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、または追加の手順を使用して対処できるパラメータを示します。

表 *1 : Cisco Crosswork Data Gateway* の展開パラメータとシナリオ

パラメータ	説明	導入シナリオ
ホスト情報		

パラメータ	説明	導入シナリオ
ホスト名（Hostname）*	完全修飾ドメイン名（FQDN）として指定したサーバのホスト名。 （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、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。	
説明（Description）*	Cisco Crosswork Data Gateway インスタンスの詳細な説明。	
Crosswork Data Gateway ラベル（Crosswork Data Gateway Label）	複数の Cisco Crosswork Data Gateway インスタンス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。	

パラメータ	説明	導入シナリオ
アクティブな vNIC（Active vNICs）	トラフィックの送信に使用する vNIC の数。	次の組み合わせに従って、1 つ、2 つ、または 3 つの vNIC のいずれかを選択できます。 （注） Crosswork クラスタで 1 つの vNIC 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 vNIC を使用する場合は、Crosswork Data Gateway で 2 つまたは 3 つの vNIC を使用できます。 • **1**：すべてのトラフィックを vNIC0 経由で送信します。 • **2**：vNIC0 を介して管理トラフィックを送信し、vNIC1 を介してすべてのデータトラフィックを送信します。 • **3**：vNIC0 を介して管理トラフィックを、vNIC1 を介してノースバウンドデータを、vNIC2 を介してサウスバウンドトラフィックを送信します。
RFC8190 を許可（Allow RFC8190）	RFC 8190 範囲のアドレスを自動的に許可します。このボックスがオンになっていない場合、初期設定スクリプトによって確認が求められます。	

パラメータ	説明	導入シナリオ
秘密キー URI（Private Key URI）	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、次の 3 つのパラメータを入力する必要があります。 （注） 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 URI（Certificate File URI）	この VM の PEM 形式の署名証明書チェーンへの SCP URI。これは SCP（user@host:path/to/file）を使用して取得できます。	
証明書ファイルとキーパスフレーズ（Certificate File and Key Passphrase）	Cisco Crosswork Data Gateway PEM 形式の証明書ファイルと秘密キーを取得するための SCP ユーザのパスフレーズ。	
データディスクサイズ（Data Disk Size）	2 番目のデータディスクのサイズ（GB 単位）。デフォルトのサイズは、標準で 5 GB、拡張で 500 GB です。	

パスフレーズ

インストール時に、Crosswork Data Gateway は 2 つのデフォルトユーザアカウントを作成します。

1. インストール時にユーザ名に **dg-admin** とパスワードが設定された Cisco Crosswork Data Gateway の管理者。管理者は、この ID を使用してログインし、Crosswork Data Gateway のトラブルシューティングを行います。
2. インストール時にユーザ名に **dg-oper** とパスワードを設定した Cisco Crosswork Data Gateway のオペレータ。これは読み取り専用ユーザで、すべての「read」操作と一部の限定された「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 Infrastructure 4.0 and Applications Administration Guide*』の「*Supported User Roles*」の項を参照してください。

（注） これら 2 つの定義済みユーザ名は予約済みであり、変更できません。

パスワードの変更は、両方のアカウントのコンソールから許可されます。

パスワードを紛失したか、または忘れた場合、ユーザは新しい VM を作成し、現在の VM を破棄して、新しい VM を Cisco Crosswork で再登録する必要があります。

パラメータ	説明	導入シナリオ
dg-admin パスフレーズ（dg-admin Passphrase）*	dg-admin ユーザ用に選択したパスワード。	
dg-oper パスフレーズ（dg-oper Passphrase）*	dg-oper ユーザ用に選択したパスワード。	
（注） • Cisco Crosswork Data Gateway は、vNIC0 および vNIC1 インターフェイスに対して IPv4 または IPv6 をサポートしています。使用するように選択したインターフェイスとプロトコルについては、[方法（Method）] を [スタティック（Static）] に指定し、[アドレス（Address）]、[ネットマスク（Netmask）]、[ゲートウェイをスキップ（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。デフォルト値は **[なし（None）]** です。 • インストールプロセスは vNIC0 と vNIC1 IP のみを要求します。vNIC2 IP はCisco Crosswork Data Gateway プールを作成します。 （35 ページ）の項で説明したように、Cisco Crosswork Data Gateway プールの作成時に割り当てられます。 • Cisco Crosswork は、デュアルスタック構成をサポートしていません。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。		
[1]**vNIC0 IPv4 アドレス**		
vNIC0 IPv4 メソッド（vNIC0 IPv4 Method）*	vNIC0 インターフェイスが IPv4 アドレスを取得する方法。	
vNIC0 IPv4 アドレス（vNIC0 IPv4 Address）	vNIC0 インターフェイスの IPv4 アドレス。	
vNIC0 IPv4 ネットマスク（vNIC0 IPv4 Netmask）	ドット付きクワッド形式の vNIC0 インターフェイスの IPv4 ネットマスク。	
vNIC0 IPv4 スキップゲートウェイ（vNIC0 IPv4 Skip Gateway）	ゲートウェイの設定をスキップするかどうか。	
vNIC0 IPv4 ゲートウェイ（vNIC0 IPv4 Gateway）	vNIC0 ゲートウェイの IPv4 アドレス。	
[1]**vNIC0 IPv6 アドレス**		
vNIC0 IPv6 メソッド（vNIC0 IPv6 Method）*	vNIC0 インターフェイスが IPv6 アドレスを取得する方法。	

パラメータ	説明	導入シナリオ
vNIC0 IPv6 アドレス（vNIC0 IPv6 Address）	vNIC0 インターフェイスの IPv6 アドレス。	
vNIC0 IPv6 ネットマスク（vNIC0 IPv6 Netmask）	vNIC0 インターフェイスの IPv6 プレフィックス。	
vNIC0 IPv6 スキップゲートウェイ（vNIC0 IPv6 Skip Gateway）	ゲートウェイの設定をスキップするかどうか。	
vNIC0 IPv6 ゲートウェイ（vNIC0 IPv6 Gateway）	vNIC0 ゲートウェイの IPv6 アドレス。	
[1]**vNIC1 IPv4 アドレス**		
vNIC1 IPv4 メソッド（vNIC1 IPv4 Method）*	vNIC1 インターフェイスが IPv4 アドレスを取得する方法。	
vNIC1 IPv4 アドレス（vNIC1 IPv4 Address）	vNIC1 インターフェイスの IPv4 アドレス。	
vNIC1 IPv4 ネットマスク（vNIC1 IPv4 Netmask）	ドット区切りの 4 つの数字列形式による vNIC1 インターフェイスの IPv4 ネットマスク。	
vNIC1 IPv4 スキップゲートウェイ（vNIC1 IPv4 Skip Gateway）	ゲートウェイの設定をスキップするかどうか。	
vNIC1 IPv4 ゲートウェイ（vNIC1 IPv4 Gateway）	vNIC1 ゲートウェイの IPv4 アドレス。	
[1] **vNIC1 IPv6 アドレス**		
vNIC1 IPv6 メソッド（vNIC2 IPv4 Method）*	vNIC1 インターフェイスが IPv6 アドレスを取得する方法。	
vNIC1 IPv6 アドレス（vNIC1 IPv6 Address）	vNIC1 インターフェイスの IPv6 アドレス。	
vNIC1 IPv6 ネットマスク（vNIC1 IPv6 Netmask）	ドット区切りの 4 つの数字列形式による vNIC1 インターフェイスの IPv6 ネットマスク。	

パラメータ	説明	導入シナリオ
vNIC1 IPv6 スキップゲートウェイ（vNIC1 IPv6 Skip Gateway）	ゲートウェイの設定をスキップするかどうか。	
vNIC1 IPv6 ゲートウェイ（vNIC1 IPv6 Gateway）	vNIC1 ゲートウェイの IPv6 アドレス。	
DNS サーバ		
DNS アドレス（DNS Address）*	管理インターフェイスからアクセス可能な DNS サーバの IPv4/IPv6 アドレスのスペース区切りリスト。	
DNS 検索ドメイン（DNS Search Domain）*	DNS 検索ドメイン	
DNS セキュリティ拡張機能（DNS Security Extensions）	DNS セキュリティ拡張機能を使用するかどうか。	
DNS over TLS	DNS over TLS を使用するかどうか。	
マルチキャスト DNS（Multicast DNS）	マルチキャスト DNS を使用するかどうか。	
リンクローカル マルチキャスト名前解決（Link-Local Multicast Name Resolution）	Link-Local Multicast Name Resolution を使用するかどうか。	
NTPv4サーバ		

パラメータ	説明	導入シナリオ
NTPv4 サーバ（NTPv4 Servers）*	管理インターフェイスからアクセス可能な NTPv4 サーバの 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。
NTPv4 認証の使用（Use NTPv4 Authentication）	NTPv4 認証を使用するかどうか。	
NTPv4 キー（NTPv4 Keys）	サーバリストにマッピングするスペース区切りのキー ID。	
NTPv4 キーファイル URI（NTPv4 Key File URI）	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）	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		

パラメータ	説明	導入シナリオ
リモート Syslog サーバを使用しますか?（Use Remote Syslog Server?）	リモートホストに syslog メッセージを送信するかどうか。	外部 syslog サーバを使用する場合は、これらの 7 つの設定を行う必要があります。 （注） 外部 syslog サーバを設定している場合は、サービス（CLI/MDT/SNMP/gNMI）イベントがその外部 syslog サーバに送信されます。それ以外の場合は、Crosswork Data Gateway VM にのみ記録されます。ログを取得するには、メインメニューから [5 トラブルシューティング（5 Troubleshooting）] > [show-tech の実行（Run show-tech）] に移動します。 （注） 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。
Syslog サーバのアドレス（Syslog Server Address）	管理インターフェイスからアクセス可能なsyslogサーバの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、角カッコ（[1 :: 1]）で囲む必要があります。	
Syslog サーバポート（Syslog Server Port）	Syslog サーバのポート番号。	
Syslog サーバプロトコル（Syslog Server Protocol）	syslog の送信時に UDP、TCP、または RELP を使用します。	
TLS 経由の Syslog を使用するかどうか（Use Syslog over TLS?）	TLS を使用してsyslog のトラフィックを暗号化します。	
Syslog TLS ピア名（Syslog TLS Peer Name）	サーバ証明書の SubjectAltName またはサブジェクトの共通名に入力されたとおりの syslog サーバのホスト名。	
Syslog ルート証明書ファイル URI（Syslog Root Certificate File URI）	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。	
Syslog 証明書ファイルのパスフレーズ（Syslog Certificate File Passphrase）	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		

パラメータ	説明	導入シナリオ
リモート監査サーバを使用しますか（Use Remote Auditd Server?）	リモートホストに監査メッセージを送信するかどうか。	外部監査サーバを使用する場合は、これらの 3 つの設定を行う必要があります。
監査サーバアドレス（Auditd Server Address）	オプションの監査サーバのホスト名、IPv4、または IPv6 アドレス。	
監査サーバポート（Auditd Server Port）	オプションの監査サーバのポート番号。	
コントローラの設定		
Crosswork コントローラ IP（Crosswork Controller IP）*	Cisco Crosswork クラスタの仮想 IP アドレス。 （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。	
Crosswork コントローラポート（Crosswork Controller Port）*	Cisco Crosswork コントローラのポート。	
コントローラ署名証明書ファイル URI（Controller Signing Certificate File URI）**	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。PEM ファイルは Cisco Crosswork によって生成され、次の場所にあります。 `cw-admin@<Crosswork_VM_Management_IP_Address>:/home/cw-admin/controller.pem`	Crosswork Data Gateway を機能させるには、コントローラ署名証明書ファイルが必要です。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 のブート時に初めて自動的に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 （41 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する必要があります。

パラメータ	説明	導入シナリオ
コントローラの SSL/TLS 証明書ファイル URI（Controller SSL/TLS Certificate File URI）	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（Controller Certificate File Passphrase）**	Cisco Crosswork の証明書チェーンを取得する SCP ユーザ（cw-admin）のパスワード。	これは、コントローラ署名証明書ファイル URI を指定する場合に必要です。
プロキシサーバの URL（Proxy Server URL）	管理ネットワークプロキシサーバの URL。	プロキシサーバを使用する場合は、これらのパラメータを指定する必要があります。
プロキシサーババイパス リスト（Proxy Server Bypass List）	プロキシサーバに送信されないサブネットとドメインのスペース区切りリスト。	
認証プロキシのユーザ名（Authenticated Proxy Username）	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）	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）	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）	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。	

[1] 使用するインターフェイスに IPv4 または IPv6 アドレスを指定する必要があります。両方に [なし（None）] を選択すると、展開が機能しなくなります。

（注） デフォルトの SCP ポート 22 を使用しない場合は、SCP コマンドの一部としてポートを指定できます。次の例を参考にしてください。

```
-P55 user@host:path/to/file
```

55 はカスタムポートです。

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） ここに示すイメージは、Cisco Crosswork Data Gateway の標準的なオンプレミス展開の例にすぎません。

ステップ 1 Cisco Crosswork Data Gateway 2.0 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。表 1 : Cisco Crosswork Data Gateway の展開パラメータとシナリオ （2 ページ）を参照してください。

ステップ 2 vCenter vSphere クライアントに接続します。[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。

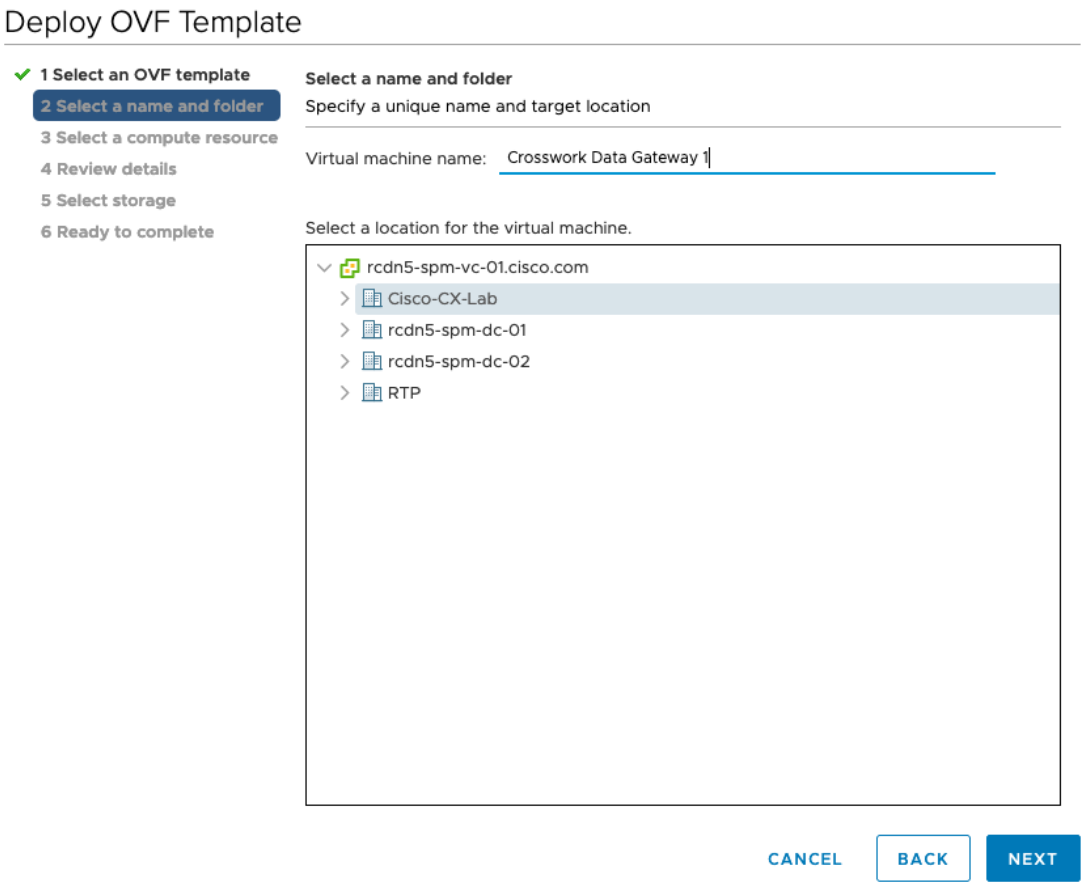
a) [参照（Browse）] をクリックし、OVA イメージファイルをダウンロードした場所に移動してファイルを選択します。

選択すると、ファイル名がウィンドウに表示されます。

ステップ 4 次の図に示すように、[次へ（Next）] をクリックして [2 名前と場所の選択（2 Select name and location）] 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。



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

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。OVA の情報を確認して [次へ（Next）] をクリックします。

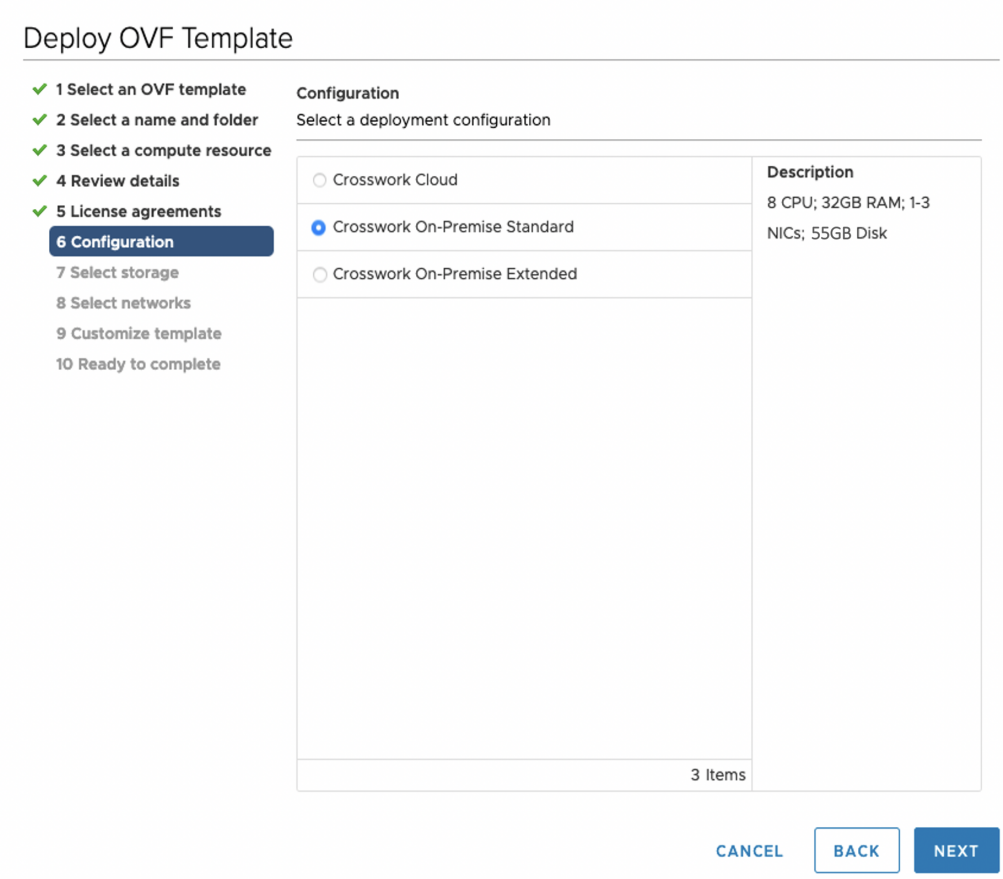
展開する OVF テンプレートを確認します。

（注） この情報は OVF から収集され、変更はできません。

ステップ 7 [次へ（Next）] をクリックして、[使用許諾契約に同意（Accept License Agreement）] に移動します。エンドユーザ ライセンス契約書を確認し、[承認（Accept）] をクリックします。

ステップ 8 次の図のように、[次へ（Next）] をクリックして [6 設定の選択（6 Select configuration）] に移動します。必要な設定のタイプ（[標準 Crosswork On-Premise（Crosswork On-Premise Standard）] または [拡張Crosswork On-Premise（Crosswork On-Premise Extended）] のいずれか）を選択します。

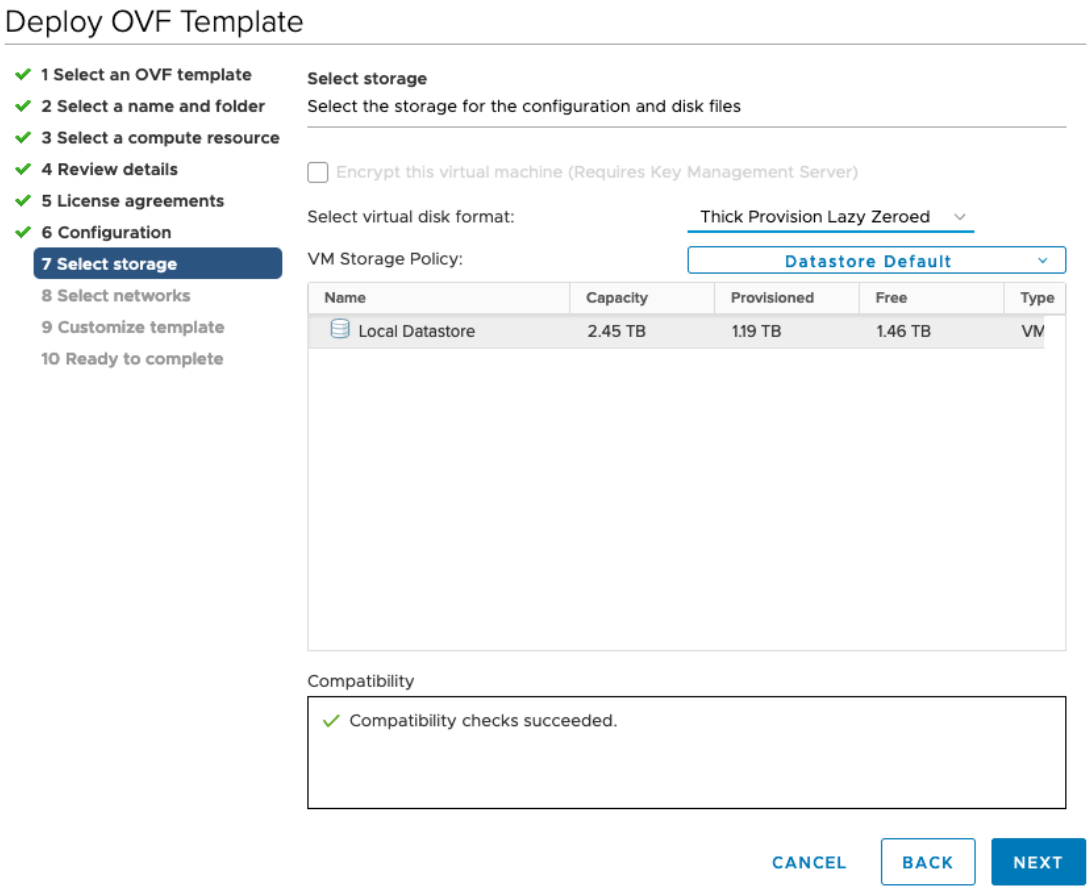
（注） Crosswork Change Automation and Health Insights を使用する場合は、[拡張Crosswork On-Premise（Crosswork On-Premise Extended）] を選択する必要があります。



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。

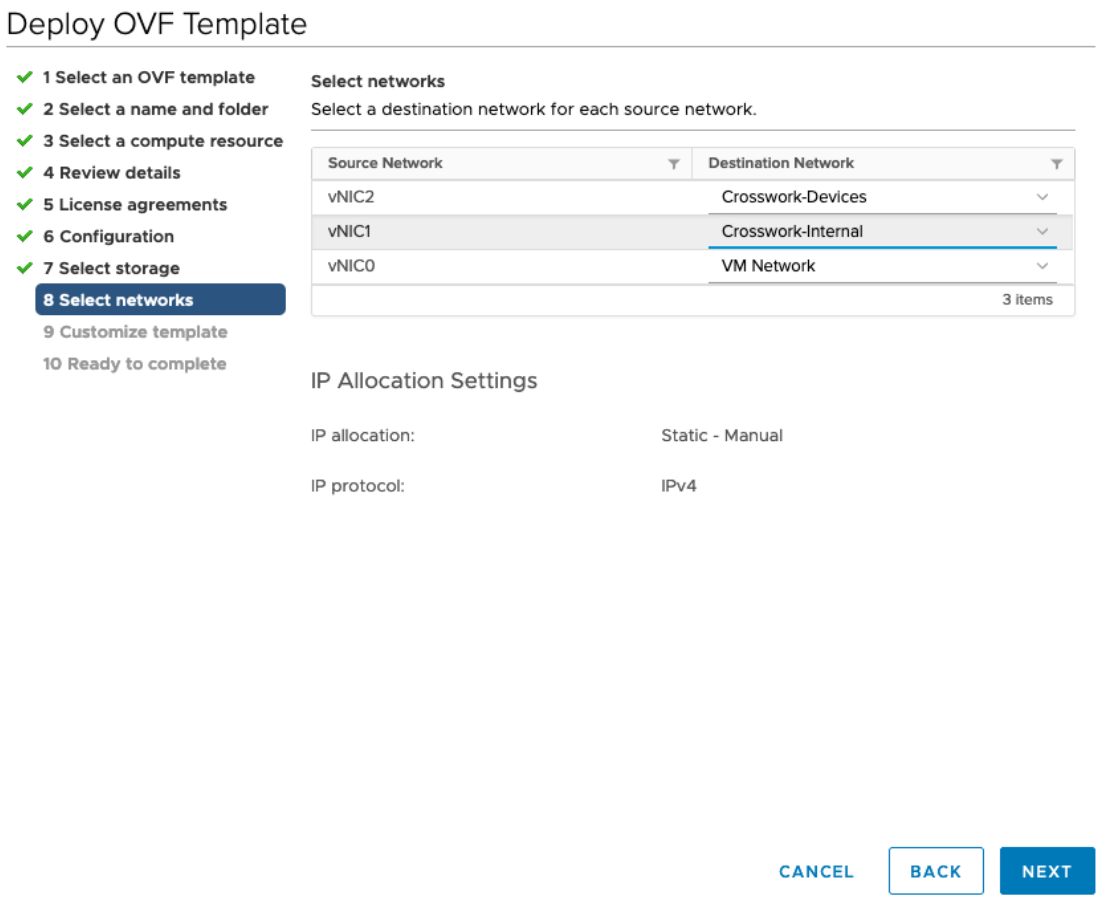
a) [仮想ディスク形式の選択（Select virtual disk format）] ドロップダウンリストから [シックプロビジョニング（Lazy Zeroed）（Thick provision lazy zeroed）] を選択することを推奨します。

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。

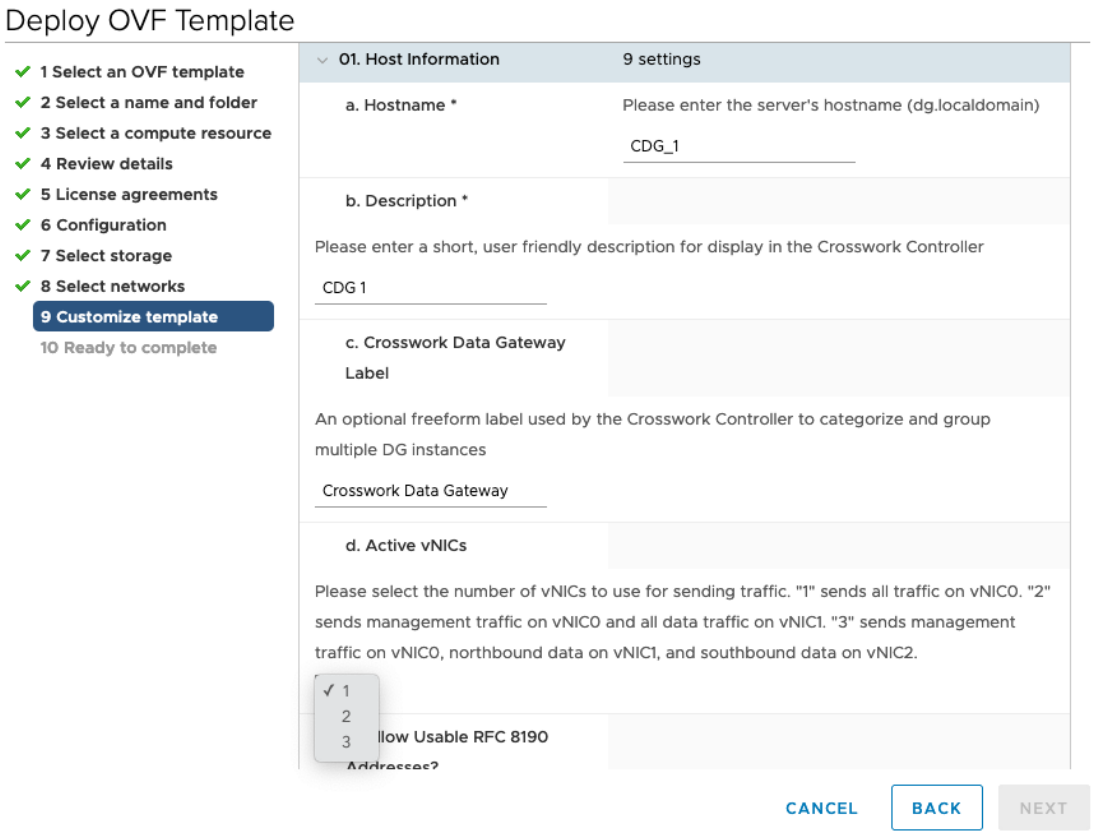


ステップ 10 次の図のように、[次へ（Next）] をクリックして [8 ネットワークの選択（8 Select networks）] に移動します。ページ上部にあるドロップダウンテーブルで、各送信元ネットワークに適切な接続先ネットワーク（[vNIC2]、[vNIC1]、および [vNIC0]）をそれぞれ選択します。

（注） 使用する vNIC の接続先ネットワークを [vNIC0] から選択し、未使用の vNIC をデフォルト値に設定します。



ステップ 11 [次へ（Next）] をクリックして、[ホスト情報の設定（Host Information Settings）] 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 1 : Cisco Crosswork Data Gateway の展開パラメータとシナリオ （2 ページ）の説明に従って、パラメータの情報を入力します。



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。

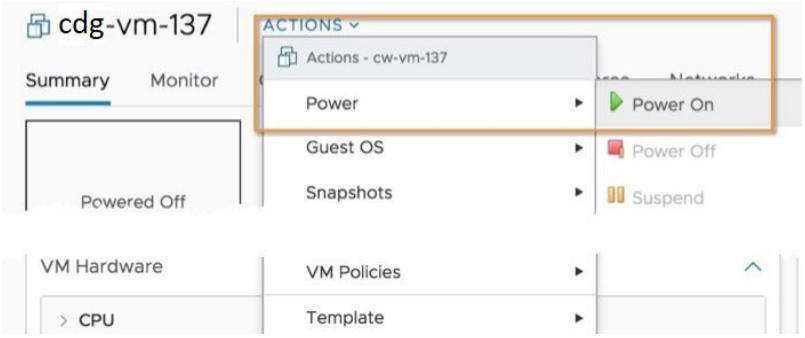
ステップ 13 展開が完了するまで待ってから続行します。展開ステータスを確認するには、次の手順を実行します。

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。



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おり、変更する場合はすべて自己責任で行ってください。

次のタスク

vCenter 経由でCisco Crosswork Data Gateway VM にログインします。

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。
2. ユーザ名（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。

ログインすると、Crossway 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。ログアウトし、次の項で説明するインストール後のタスクに進みます。

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

要件に応じてコマンド/スクリプトの必須/オプションのパラメータを変更し、OVF ツールを実行できます。表 表 1 : Cisco Crosswork Data Gateway の展開パラメータとシナリオ （2 ページ） を参照してください。

以下に、スクリプトで OVF ツールを実行する場合の例を示します。

```
#!/usr/bin/env bash

# robot.ova path
ROBOT_OVA_PATH="https://engci-maven.cisco.com/artifactory/cdg-group/build/2.0.0_dg200_7_2021-03-31_18-00-00/image/cw-na-dg-2.0.0-7-TESTONLY-20210331.ova"

VM_NAME="dg-32"
DM="thin"
Deployment="onpremise-standard"

ActiveVnics="3"
```

```
Hostname="dg-32.cisco.com"
Vnic0IPv4Address="172.23.213.32"
Vnic0IPv4Gateway="172.23.213.1"
Vnic0IPv4Netmask="255.255.255.0"
Vnic0IPv4Method="Static"
Vnic1IPv4Address="32.32.32.32"
Vnic1IPv4Gateway="32.32.32.1"
Vnic1IPv4Netmask="255.255.255.0"
Vnic1IPv4Method="Static"

DNS="171.70.168.183"
NTP="ntp.esl.cisco.com"
Domain="cisco.com"

ControllerIP="172.23.213.10"
ControllerPort="30607"
ControllerSignCertChain="cw-admin@172.23.213.10:/home/cw-admin/controller.pem"
ControllerCertChainPwd="Cwork123!"

Description="Description for Cisco Crosswork Data Gateway for 32"
Label="Label for Cisco Crosswork Data Gateway dg-32"

dg_adminPassword="cisco123"
dg_operPassword="cisco123"


ProxyUsername="cisco"
ProxyPassphrase="cisco123"


SyslogAddress="127.0.0.1"
SyslogPort=514
SyslogProtocol="UDP"
SyslogTLS=False
SyslogPeerName="combo-46.cisco.com"
SyslogCertChain="root@172.23.213.46:/root/stproxy/proxycert/CA.pem"
SyslogCertChainPwd="cisco123"

# Please replace this information according to your vcenter setup
VCENTER_LOGIN="administrator%40vsphere.local:Vtsisco%40123%21@172.23.213.21"
VCENTER_PATH="DC1/host/172.23.213.8"
DS="datastore1 (5)"

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
 --powerOffTarget --powerOn \
--allowExtraConfig --extraConfig:firmware=efi --extraConfig:uefi.secureBoot.enabled=true
 \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-2" \
--net:"vNIC2=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"ControllerIP=$ControllerIP" \
--prop:"ControllerPort=$ControllerPort" \
--prop:"ControllerSignCertChain=$ControllerSignCertChain" \
--prop:"ControllerCertChainPwd=$ControllerCertChainPwd" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ActiveVnics=$ActiveVnics" \
--prop:"Vnic0IPv4Address=$Vnic0IPv4Address" \
--prop:"Vnic0IPv4Gateway=$Vnic0IPv4Gateway" \
```

```
--prop:"Vnic0IPv4Netmask=$Vnic0IPv4Netmask" \
--prop:"Vnic0IPv4Method=$Vnic0IPv4Method" \
--prop:"Vnic1IPv4Address=$Vnic1IPv4Address" \
--prop:"Vnic1IPv4Gateway=$Vnic1IPv4Gateway" \
--prop:"Vnic1IPv4Netmask=$Vnic1IPv4Netmask" \
--prop:"Vnic1IPv4Method=$Vnic1IPv4Method" \
--prop:"DNS=$DNS" \
--prop:"NTP=$NTP" \
--prop:"dg-adminPassword=$dg_adminPassword" \
--prop:"dg-operPassword=$dg_operPassword" \
--prop:"Domain=$Domain" $ROBOT_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"
```

ステップ 1 コマンド プロンプトを開きます。

ステップ 2 OVF ツールをインストールした場所に移動します。

ステップ 3 次のいずれかの方法で OVF ツールを実行します。

a) **コマンドの使用**

このコマンドには、ソース OVF ファイルの場所と、コマンドの実行結果として作成される vmx ファイルの場所が含まれます。

```
ovftool <location_of_source_ovf_file> <location_of_vmx_file>
```

次の例を参考にしてください。

```
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds="datastore130-2"
 --deploymentOption="onpremise-standard" --diskMode="thin" --prop:"ControllerIP=<controller-ip>"

 --prop:"ControllerPort=30607" --prop:"ControllerSignCertChain=<location of controller.pem file>"

--prop:"ControllerCertChainPwd=<password>" --overwrite --powerOffTarget --powerOn
--noSSLVerify --allowExtraConfig --extraConfig:firmware=efi
--extraConfig:uefi.secureBoot.enabled=true --name="cdg147.cisco.com"
--prop:"Hostname=cdg147.cisco.com" --prop:"Description=CDG Base VM for Automation"
--net:"vNIC0=VM Network" --prop:"Vnic0IPv4Method=Static"
--prop:"Vnic0IPv4Address=<vNIC 0 IPv4 address>" --prop:"Vnic0IPv4Netmask=<vNIC0 IPv4 netmask>"

--prop:"Vnic0IPv4Gateway=<vNIC 0 IPv4 gateway>" --net:"vNIC1=DPG991"
--prop:"Vnic1IPv4Method=Static" --prop:"Vnic1IPv4Address=<vNIC1 IPv4 address>"
--prop:"Vnic1IPv4Netmask=<vNIC1 IPv4 netmask>" --prop:"Vnic1IPv4Gateway=<vNIC1 IPv4 gateway>"
--net:"vNIC2=DPG999" --prop:"dg-adminPassword=<password>"
--prop:"dg-operPassword=<password>" --prop:"DNS=<DNS address>"
--prop:"NTP=<NTP>"
--prop:"Domain=cisco.com" <image download url> vi://'Administrator@vsphere.local:<password>'@<IP
 address>/DC/host/<IP address>
```

b) **スクリプトの使用**

コマンドや引数を含めて作成したスクリプトを実行する場合は、次の手順を実行します。

```
root@cxcloudctrl:/opt# ./cdgovfdeployVM197
```

VM の電源がオンになったら、VM にログインします。「Crosswork Data Gateway VM へのログイン」を参照してください。ログインすると、Crossway 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。ログアウトし、次の項で説明するインストール後のタスクに進みます。

Cisco CSP への Cisco Crosswork Data Gateway のインストール

次を実行して、Cisco CSP に Cisco Crosswork Data Gateway をインストールします。

ステップ 1　Cisco Crosswork Data Gateway `qcow2` パッケージをダウンロードします。

a) cisco.com から Cisco Crosswork Data Gateway `qcow2` パッケージをローカルマシンまたは Cisco CSP にアクセス可能なローカルネットワーク上の場所にダウンロードします。この手順では、パッケージ名に「**cw-na-dg-2.0.0-18-release-qcow2-pkg.tar.gz**」を使用します。

b) 次のコマンドで `qcow2` パッケージを解凍します。

```
tar -xvf cw-na-dg-2.0.0-18-release-qcow2-pkg.tar.gz
```

`qcow2` パッケージの内容が新しいディレクトリ（`cw-na-dg-2.0.0-18-release-qcow2` など）に解凍されます。

この新しいディレクトリには、Cisco Crosswork Data Gateway `qcow2` ビルド（**cw-na-dg-2.0.0-18-release-20210409.tar.gz** など）と、ビルドの検証に必要なその他のファイルが含まれます。

ステップ 2　（オプション）Cisco Crosswork Data Gateway `qcow2` パッケージを確認します。

a) 前の手順で作成したディレクトリに移動します。

b) 次のコマンドを使用して、ビルドの署名を確認します。

（注）　スクリプトが実行されているマシンには、cisco.com への HTTP アクセスが必要です。セキュリティ制限のために cisco.com にアクセスできない場合か、またはスクリプトの実行後に確認メッセージが正常に受信されなかった場合は、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。

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

（注）　cisco_x509_verify_release.py スクリプトは、Python 2 とのみ互換性があります。提供されたスクリプトを使用する代わりに、cisco.com に掲載されているチェックサムに対して、シスコから最初にダウンロードしたファイルの md5 または SHA512 チェックサムを計算して確認することもできます。

ステップ 3　Cisco CSP へのアップロード用に Cisco Crosswork Data Gateway サービスイメージを準備します。

a) Cisco Crosswork Data Gateway `qcow2` ビルドは、`qcow2` ファイルと `config.txt` ファイルの tarball です。`.tar.gz`（**cw-na-dg-2.0.0-18-release-20210409.tar.gz** など）を次のコマンドで解凍します。

```
tar -xvf ccw-na-dg-2.0.0-18-release-20210409.tar.gz
```

b) `config.txt` ファイルを開き、インストールの要件に従ってパラメータを変更します。表 1 : Cisco Crosswork Data Gateway の展開パラメータとシナリオ （2 ページ）の項を参照してください。

次のパラメータには事前定義された値があります。

- 展開
  - Crosswork On-Premise には「Crosswork On-Premise」を使用します。

- Profile
  - 標準展開の場合は「Standard」を使用します。
  - 拡張展開の場合は「Extended」を使用します。

次に、config.txt ファイルの例を示します。

```
ActiveVnics=
AuditdAddress=
AuditdPort=
ControllerCertChainPwd=
ControllerIP=
ControllerPort=
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Crosswork On-Premise
Description=
DGAppdataDisk=
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=changeme
DNSSEC=False
DNSTLS=False
Domain=changeme
EnrollmentPassphrase=
EnrollmentURI=
Hostname=changeme
Label=
LLMNR=False
mDNS-False
NTP=changeme
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic1IPv4Address=0.0.0.0
Vnic1IPv4Gateway=0.0.0.1
```

```
Vnic1IPv4Method=None
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic2IPv4Address=0.0.0.0
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=None
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
dg-adminPassword=changeme
dg-operPassword=changeme
```

ステップ 4 **Cisco CSP に Cisco Crosswork Data Gateway サービスイメージをアップロードします。**

a) Cisco CSP にログインします。

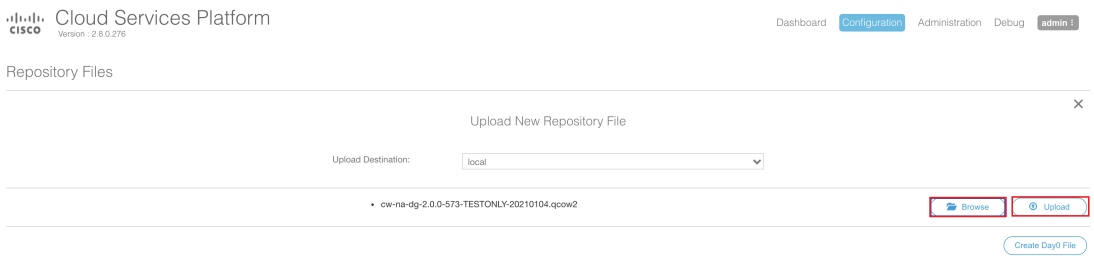
b) [設定（Configuration）] > [リポジトリ（Repository）] に移動します。

c) [リポジトリファイル（Repository Files）] ページで、[+] ボタンをクリックします。

d) [アップロード先（Upload Destination）] を選択します。

e) [参照（Browse）] をクリックして `qcow2` ファイルに移動して [開く（Open）] をクリックし、[アップロード（Upload）] をクリックします。

`config.txt` ファイルをアップロードするには、この手順を繰り返します。



ファイルがアップロードされると、ファイル名とその他の関連情報が [リポジトリファイル（Repository Files）] テーブルに表示されます。

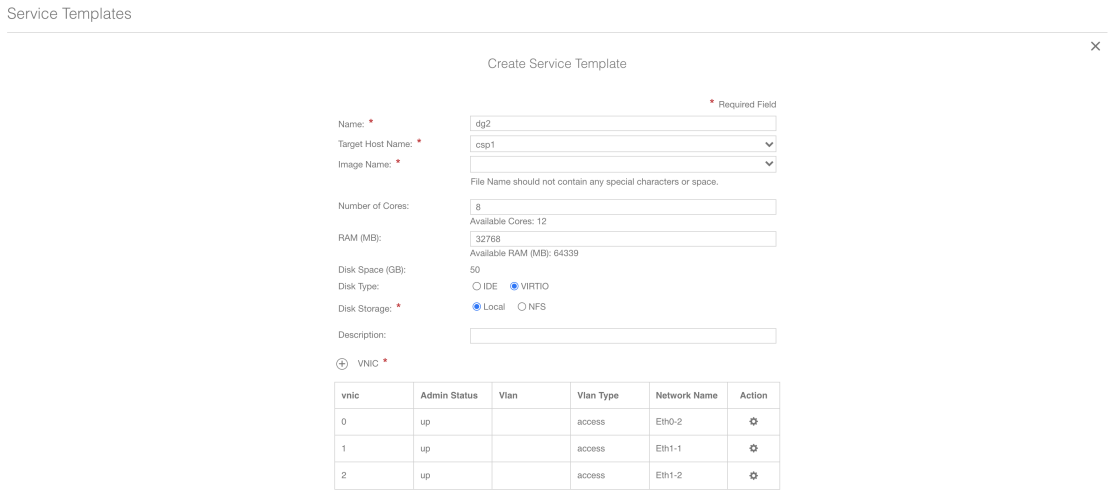
ステップ 5 **Crosswork Data Gateway VM の作成**：

a) [設定（Configuration）] > [サービス（Services）] に移動します。

b) [サービス（Service）] ページで、[+] ボタンをクリックします。

c) [サービスの作成（Create Service）] オプションをオンにします。

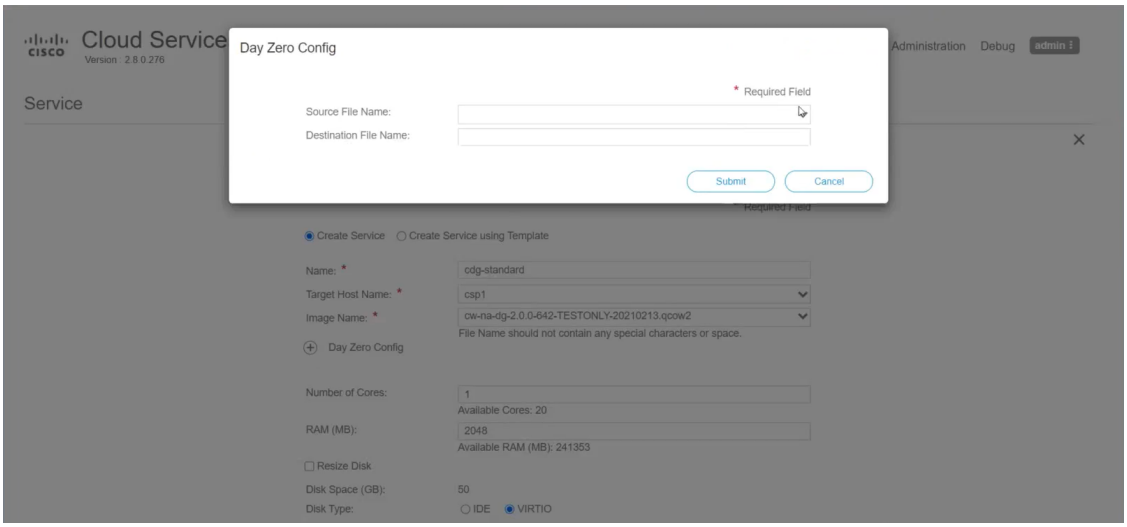
[サービス プロファイル テンプレートの作成（Create Service Profile Template）] ウィンドウが表示されます。



d) 次のフィールドに値を入力します。

フィールド	説明
名前（Name）	VM の名前。
ターゲット ホスト名（Target Host Name）	VM を展開するターゲットホストを選択します。
イメージ名（Image Name）	`qcow2` イメージを選択します。

e) [デイゼロの設定（Day Zero Config）] をクリックします。



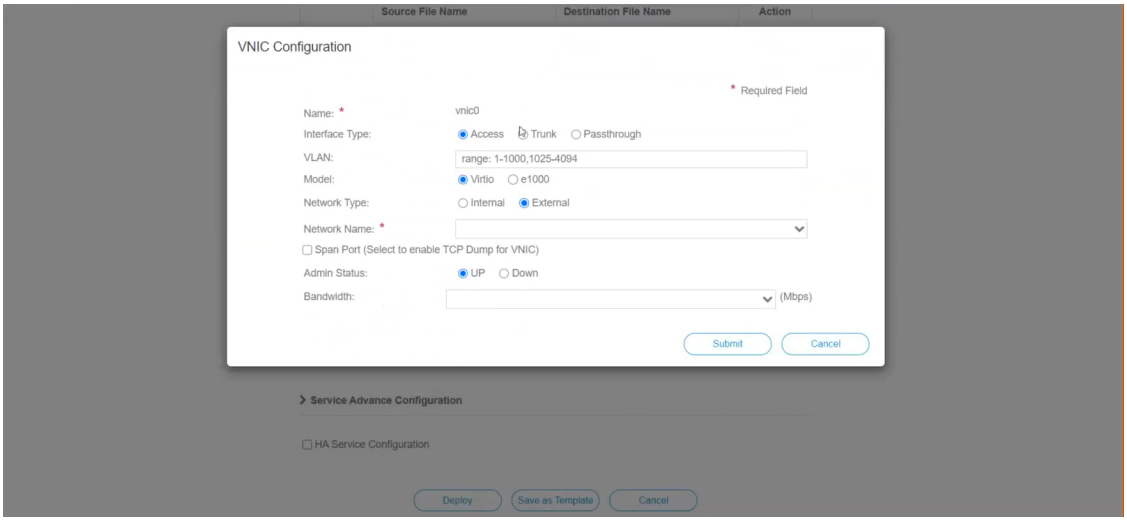
[デイゼロの設定（Day Zero Config）] ダイアログボックスで、次の手順を実行します。

1. [ソースファイル名（Source File Name）] ドロップダウンリストから、デイゼロ設定ファイル（つまり、以前に変更してアップロードした `config.txt` ファイル）を選択します。
2. [接続先ファイル名（Destination File Name）] フィールドで、デイゼロの接続先テキストファイルの名前を指定します。これは常に「config.txt」である必要があります。
3. [送信（Submit）] をクリックします。

f) 次のフィールドに値を入力します。

フィールド	説明
コア数（Number of Cores）	標準：8 拡張：16
RAM（MB）	標準：32768 拡張：98304

g) [vNIC] をクリックします。



[VNICの設定（VNIC Configuration）] ダイアログボックスで、次の手順を実行します。

（注） VNIC 名はデフォルトで設定されます。

1. [インターフェイスタイプ（Interface Type）] で [アクセス（Access）] を選択します。
2. [モデル（Model）] として [Virtio] を選択します。
3. [ネットワークタイプ（Network Type）] として [外部（External）] を選択します。
4. [ネットワーク名（Network Name）] は次のように選択します。

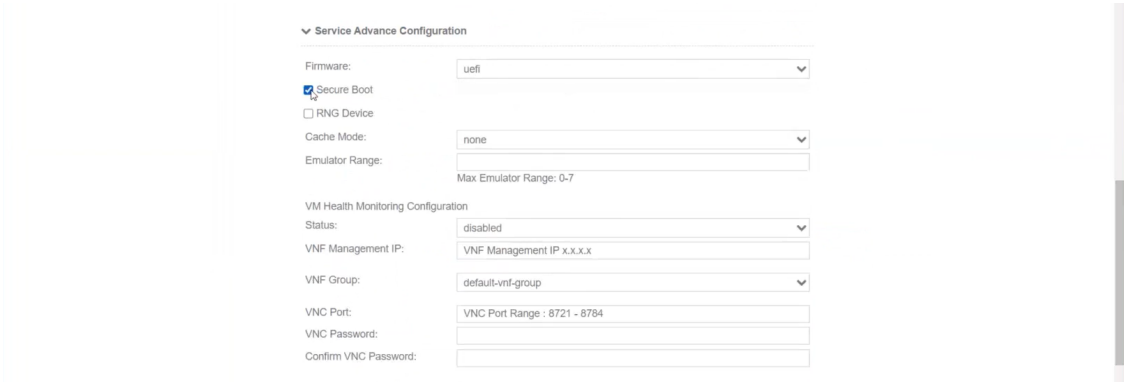
VNIC の場合	選択内容
vnic0	Eth0-1
vnic1	Eth1-1
vnic2	Eth1-2

5. [管理ステータス（Admin Status）] として [稼働中（UP）] を選択します。
6. [送信（Submit）] をクリックします。
7. vNIC1 と vNIC2 に対して手順 **i** ー **vi** を繰り返します。

3 つすべての vNIC を追加すると、VNIC テーブルは次のようになります。

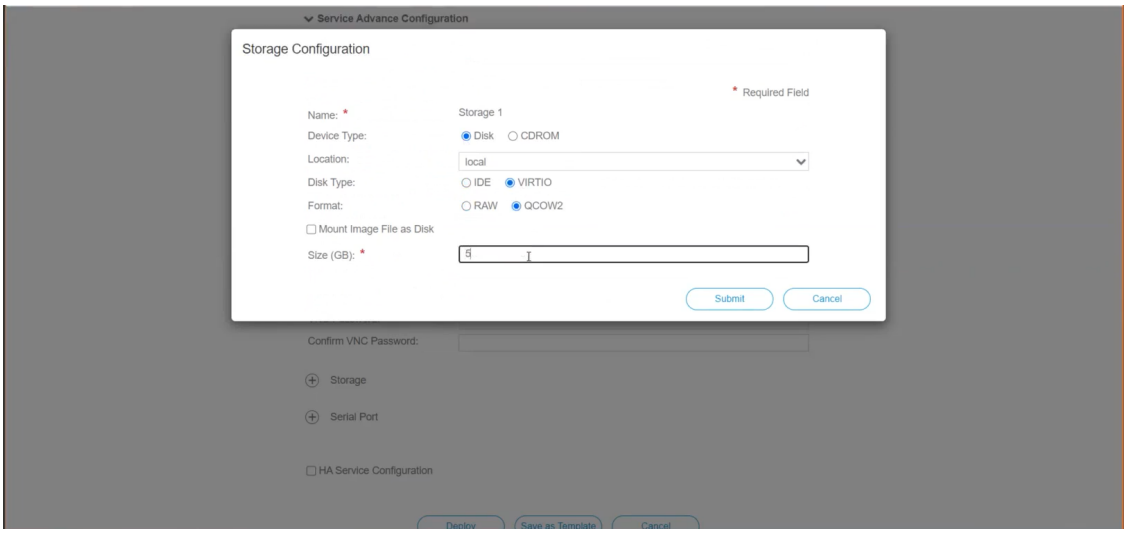
h) [サービスの詳細設定（Service Advanced Configuration）] を展開し、[ファームウェア（Firmware）] としてドロップダウンから [uefi] を選択します。

[セキュアブート（Secure Boot）] チェックボックスをオンにします。



i) [ストレージ（Storage）] をクリックします。

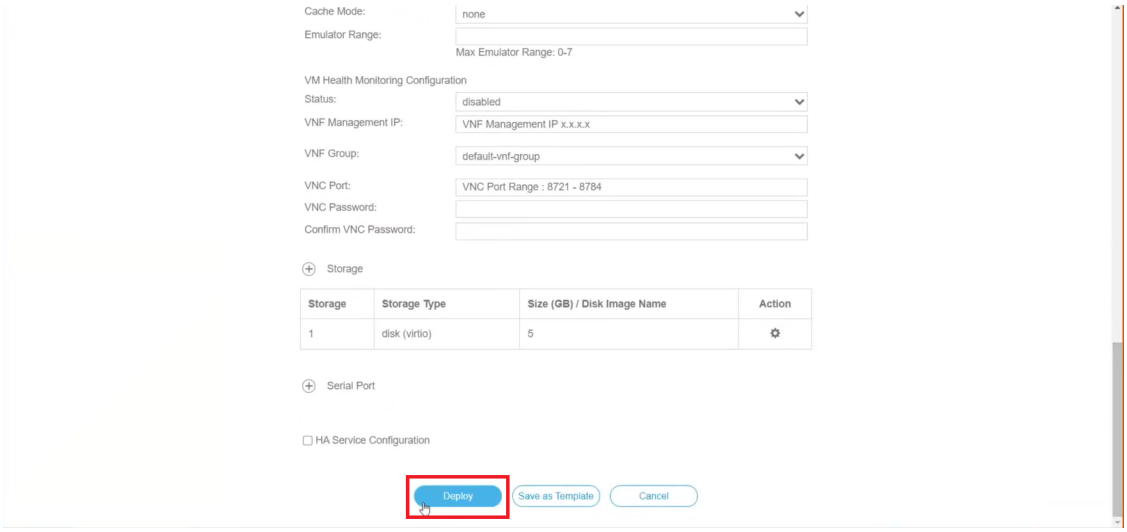
[ストレージの設定（Storage Configuration）] ダイアログボックスで、次の手順を実行します。



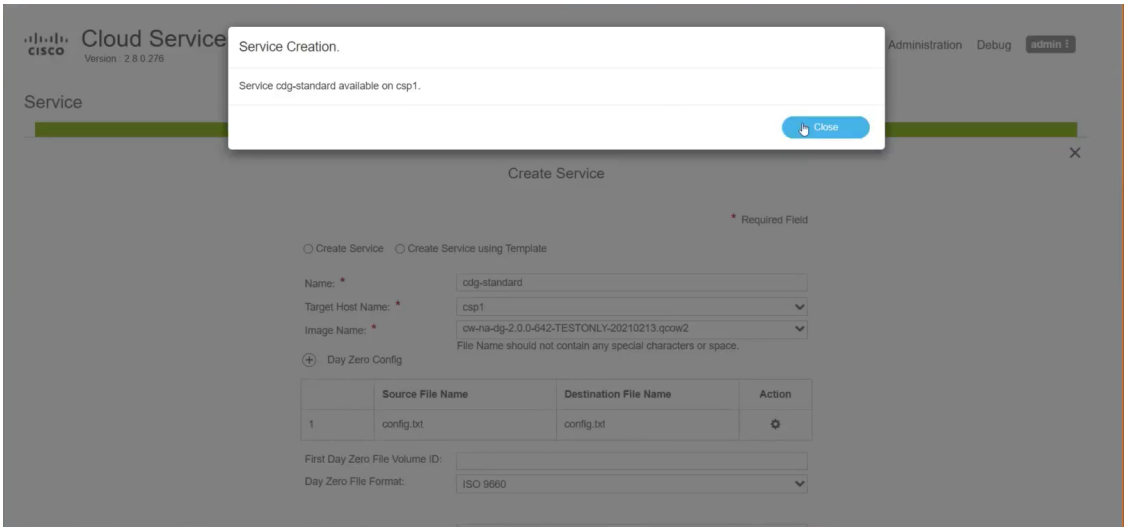
フィールド	説明
名前（Name）	ストレージの名前。これはデフォルトで指定されます。
デバイスタイプ（Device Type）	[ディスク（Disk）] を選択します。
ロケーション（Location）	[ローカル（local）] を選択します。
ディスクの種類（Disk Type）	[VIRTIO] を選択します。
フォーマット（Format）	[QCOW2] を選択します。
イメージファイルをディスクとしてマウントしますか（Mount image file as disk?）。	このチェックボックスはオフのままにします。
サイズ（GB）（Size (GB)）	ディスクサイズを入力します（標準の場合は**5**、拡張の場合は **500**）。

ストレージの設定が完了したら、[送信（Submit）] をクリックします。

j) [展開（Deploy）] をクリックします。



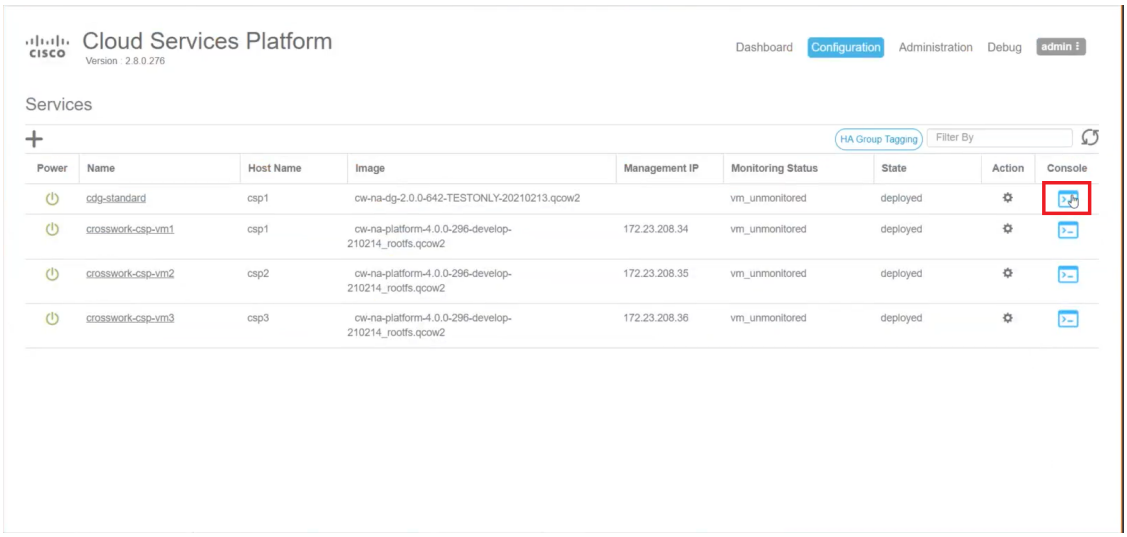
サービスが正常に展開されると、同様のメッセージが表示されます。[閉じる（Close）] をクリックします。



ステップ 6　Cisco Crosswork Data Gateway サービスを展開します。

a) [設定（Configuration）] > [サービス（Services）] に移動します。

b) [サービス（Services）] テーブルで、上記で作成した Cisco Crosswork Data Gateway サービスの [コンソール（Console）] 列の下にあるコンソールアイコンをクリックします。



c) [noVNC] ウィンドウが開きます。右上隅にある [接続（Connect）] オプションをクリックします。

d) Cisco Crosswork Data Gateway サービスに接続したら、ユーザ名とパスワードを入力します。

Cisco Crosswork Data Gateway コンソールを使用できます。

ログインすると、Crossway 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。ログアウトし、次の項で説明するインストール後のタスクに進みます。

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、次のタスクを実行します。

- SSH を使用した Crosswork Data Gateway へのアクセス （31 ページ）
- タイムゾーンの設定 （32 ページ）
- ログアウト （34 ページ）

SSH を使用した Crosswork Data Gateway へのアクセス

SSH から Cisco Crosswork Data Gateway VM にアクセスできることを確認します。

（注） 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 を使用してログインするには、次の手順を実行します。

ステップ 1 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>**

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。

（注） SSH を使用してログインできない場合は、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。

タイムゾーンの設定

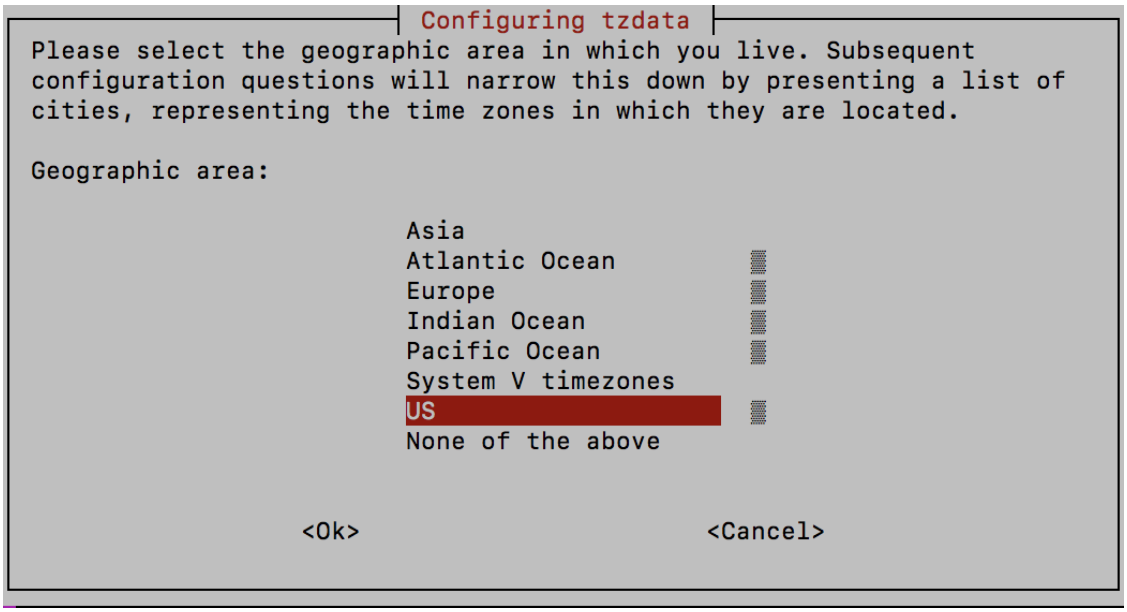
Crosswork Data Gateway は最初、デフォルトのタイムゾーン（UTC）で起動します。

次の手順に従い、タイムゾーンを設定します。

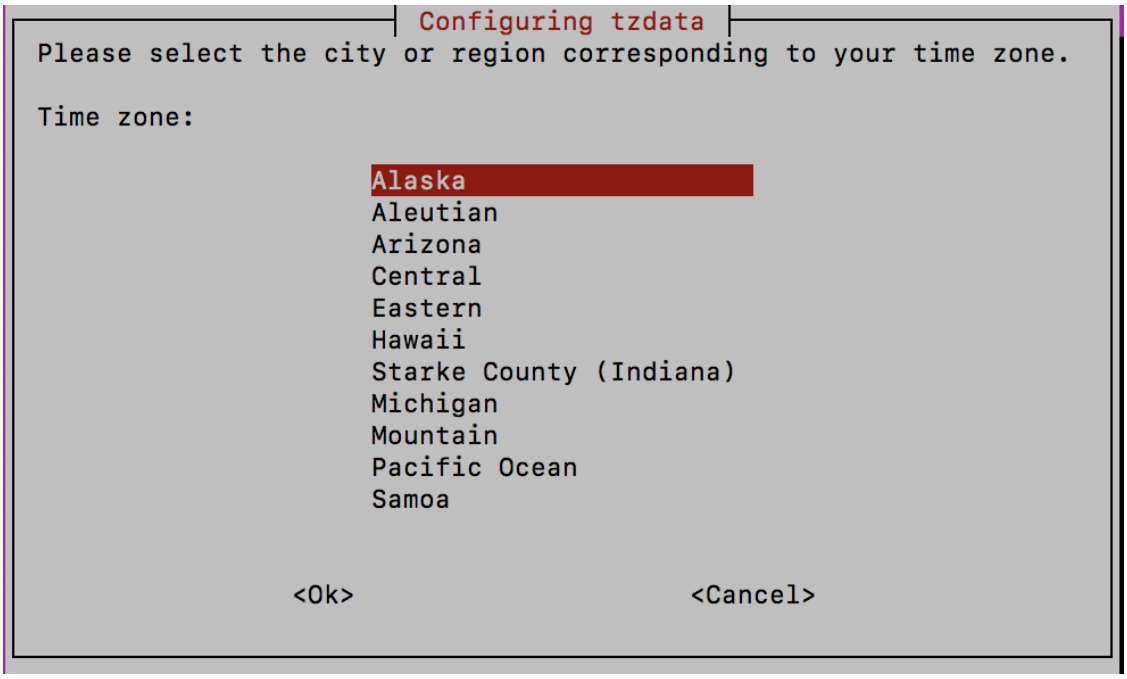
ステップ 1 Crosswork Data Gateway VM のインタラクティブメニューで、[現在のシステム設定の変更（Change Current System Settings）] を選択します。

ステップ 2 [9 タイムゾーンの設定（9 Configure Timezone）] を選択します。

ステップ 3 居住地域を選択します。



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。



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 Gateway VM をリブートして、すべてのプロセスが新しいタイムゾーンを取得するようにします。

ログアウト

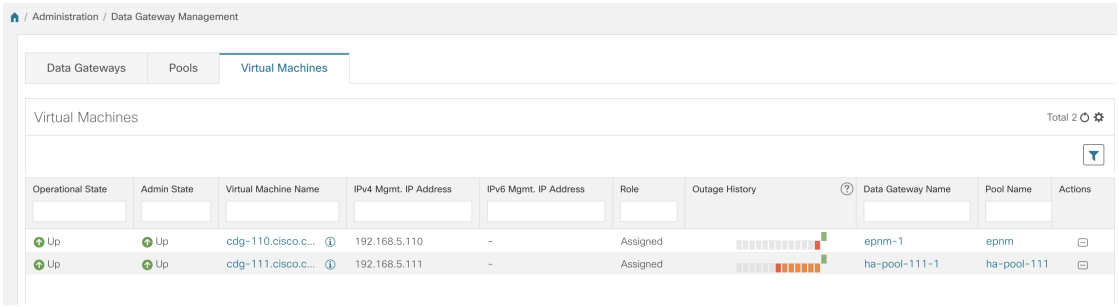
ログアウトするには、メインメニューから [1 ログアウト（1 Logout）] を選択し、Enter を押すか、[OK] をクリックします。

Cisco Crosswork Data Gateway の認証と登録

Cisco Crosswork Data Gateway が展開されると、Cisco Crosswork に対してそれ自体を識別し、登録します。次に、Cisco Crosswork は新しい Cisco Crosswork Data Gateway インスタンスをデータベースにインスタンス化し、Cisco Crosswork Data Gateway からの「first-sign-of-life」を待ちます。

接続が確立されると、Cisco Crosswork Data Gateway インスタンスはコントローラのアイデンティティを確認し、この最初の接続時に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。

Cisco Crosswork Data Gateway VM が Cisco Crosswork に登録されているかどうかを確認するには、Cisco Crosswork UI で [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] に移動します。[仮想マシン（Virtual Machines）] タブをクリックします。Cisco Crosswork 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。



新しくインストールされた Cisco Crosswork Data Gateway VM は、正常に Cisco Crosswork に登録されるまで、[動作ステータス（Operational Status）] が [低下（Degraded）] になります。

（注） 以前にオンボードされた Cisco Crosswork Data Gateway VM の [動作ステータス（Operational Status）] が [低下（Degraded）] である場合は、何が問題なのかを判断するた めに調査する必要があります。

Cisco Crosswork Data Gateway VM と Cisco Crosswork の間の帯域幅に依存しますが、通常、この操作にかかる時間は 5 分未満です。[仮想マシン（Virtual Machines）] ペインのアイコンをクリックしてペインを更新し、Cisco Crosswork Data Gateway VM の最新の動作ステータスを反映します。Cisco Crosswork Data Gateway VM の登録に失敗した場合は、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。

[ロール（Role）] が [未割り当て（Unassigned）] の Cisco 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。

（注） Cisco Crosswork Data Gateway VM は、物理的な Cisco 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。

Cisco Crosswork Data Gateway プールを作成します。

プールによってデバイスが管理され、最小限の中断または中断なく収集されます。プールは、高可用性を有効にするオプションを備えた 1 つ以上の Cisco Crosswork Data Gateway VM で構成できます。Crosswork Data Gateway VM がダウンすると、Cisco Crosswork は自動的にその VM をプール内のスペア VM に置き換えます。デバイスと既存の収集ジョブは、障害が発生した VM からスペアの Crosswork Data Gateway VM に自動的に移動されます。ダウンした VM が再びアクティブになると、プール内の新しいスペア VM になります。

複数のプールを作成できます。ただし、少なくとも 1 つのプールを作成し、Crosswork Data Gateway VM を割り当てる必要があります。

（注） 同様のプロファイルを持つ Cisco Crosswork Data Gateway でプールを作成することをお勧めします。つまり、プールをすべて標準的な Crosswork Data Gateway で作成するか、またはすべて拡張 Crosswork Data Gateway で作成するかのいずれかです。異種プール（つまり、異なるタイプの Crosswork Data Gateway を含むプール）は、デバイスまたはジョブの移行用としてのみ作成する必要があります。

次の手順を実行して、Cisco Crosswork Data Gateway プールを作成します。

始める前に

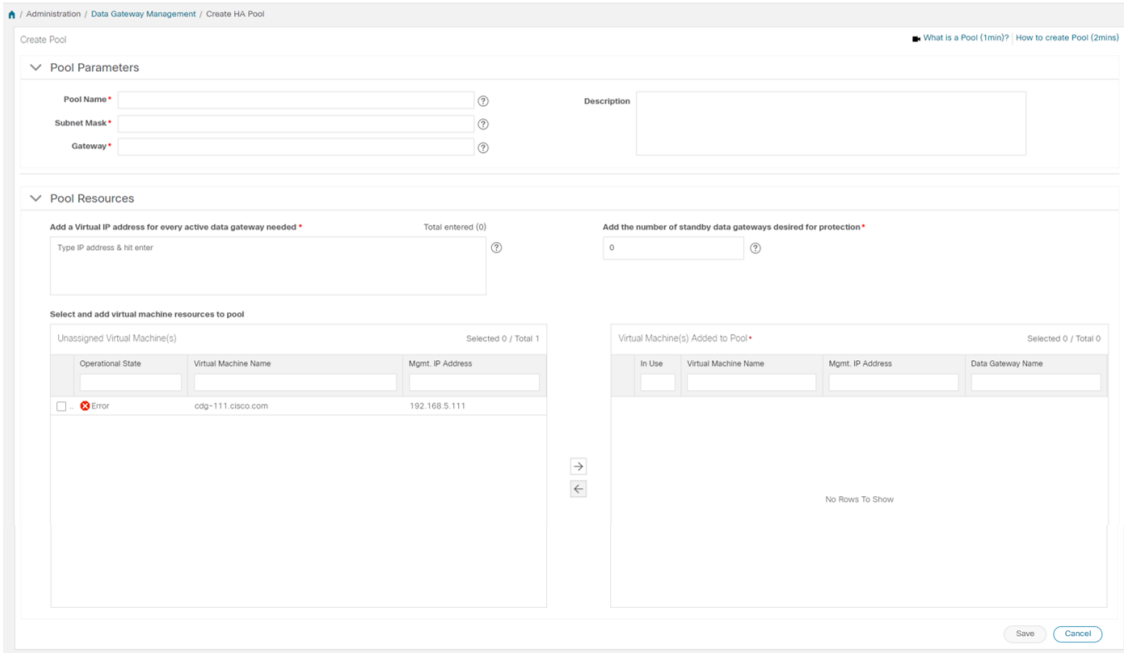
Cisco Crosswork Data Gateway プールを作成する前に、次のことを確認してください。

- プールに追加するすべての Cisco Crosswork Data Gateway VM がインストールされていること。
- サブネットマスクやゲートウェイ情報などのネットワーク情報が用意されていること。
- プールの高可用性を有効にするかどうかを決定すること。

ステップ 1 メインメニューから **[管理（Administration）] > [Data Gateway の管理（Data Gateway Management）]** を選択し、[プール（Pools）] タブをクリックします。

ステップ 2 [プール（Pools）] タブで、＋ボタンをクリックします。[プールの作成（Create Pool）] ページが開きます。

Cisco Crosswork Data Gateway プールを作成します。



ステップ 3 [プールのパラメータ（Pool Parameters）] ペインで、次のパラメータに値を入力します。

フィールド	説明
プール名（Pool Name）	ネットワークを適切に説明するプールの名前。
サブネット マスク（Subnet Mask）	デバイスと通信する Cisco Crosswork Data Gateway それぞれのサブネットマスク。
Gateway	デバイスと通信するための Cisco Crosswork Data Gateway それぞれのゲートウェイアドレス。 （注） Cisco Crosswork Data Gateway VM の vNIC が 3 つ未満の場合、このフィールドは適用されません。
説明（Description）	プールの説明。

ステップ 4 [プールリソース（Pool Resources）] ペインで、次の詳細を追加します。

- アクティブなすべての Crosswork Data Gateway VM の仮想IP アドレス。

  （注） ネットワークで使用されていない IPv4 または IPv6 アドレスを入力します。組み合わせることはできません。

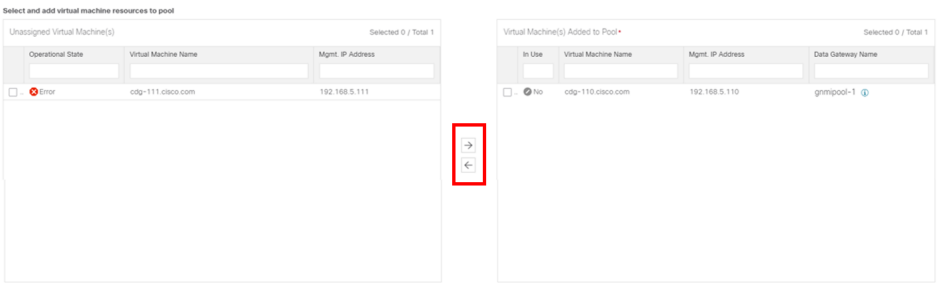
- 保護に必要なスタンバイ Cisco Crosswork Data Gateway の数。このフィールドに 0 より大きい値を入力すると、プールの高可用性が有効になります。

プールに追加する Cisco Crosswork Data Gateway VM の数は、仮想 IP とスタンバイ Cisco Crosswork Data Gateway VM の合計数と同じにする必要があります。たとえば、3 つの仮想 IP を入力し、2 つのスタンバイ VM が必要な場合は、5 つの Cisco Crosswork Data Gateway VM をプールに追加する必要があります。

ステップ 5 プールに Cisco Crosswork Data Gateway VM を追加します。

- Cisco Crosswork Data Gateway VM をプールに追加するには、左側の [未割り当ての仮想マシン（Unassigned Virtual Machine(s)）] から [VMs] を選択し、右矢印をクリックして VM を [プールに追加された仮想マシン（Virtual Machine(s) Added to Pool）] に移動します。
- プールから Cisco Crosswork Data Gateway VM を削除するには、右側の [プールに追加された仮想マシン（Virtual Machine(s) Added to Pool）] から VM を選択し、左矢印をクリックして [未割り当ての仮想マシン（Unassigned Virtual Machine(s)）] に移動します。

（注） Cisco Crosswork Data Gateway VM は、すべてのデバイスのマッピングが解除された場合にのみプールから削除できます。Cisco Crosswork Data Gateway VM がプールから削除されると、同じプール内にあるスタンバイ状態の Cisco Crosswork Data Gateway VM が自動的に置換されます。



ステップ 6 [保存（Save）] をクリックします。

Cisco Crosswork Data Gateway VM をプールに追加すると、仮想 Crosswork Data Gateway が自動的に作成され、[Data Gateways] タブに表示されます。その後、デバイスを仮想 Crosswork Data Gateway に対して接続するか切断して、収集ジョブを実行できます。

（注） デバイスは仮想 Crosswork Data Gateway に対してのみ接続または切断できます。

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 showtech 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）] > [show-tech の実行（Run show-tech）] を選択）、`controller-gateway` のログ

で理由を確認します。セッションの確立/証明書に関連する問題がある場合は、インタラクティブメニューを使用して `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。

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 *2:* インストール/登録のトラブルシューティング

問題	操作
1.Cisco Crosswork に Crosswork Data Gateway を登録できない	
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 サーバでは、初期時間は ESXi サーバに設定されます。このため、ESXi サーバにも 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）] > [show-tech の実行（Run show-tech）] に移動します。 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 のログ（`/cdg/logs/components/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。
2.「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	

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）] > [show-tech の実行（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 ログ（`/cdg/logs/components/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 Certification）] 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。
3.「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が続く	

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. 上記のトラブルシューティング シナリオ **2** の説明に従って、証明書ファイルを再度アップロードします。 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.[トラブルシューティング（Troubleshooting）] メニューから [7 VM のリブート（7 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、Cisco CSP の場合は config.txt 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、Cisco CSP の場合は config.txt 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。
Crosswork Data Gateway が拡張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、Cisco CSP の場合は config.txt の deploymentoption プロパティを確認します。「deploymentoption」プロパティが一致しないか、または拡張プロファイルテンプレートに存在しない場合は、Crosswork Data Gateway は標準プロファイルを展開します。

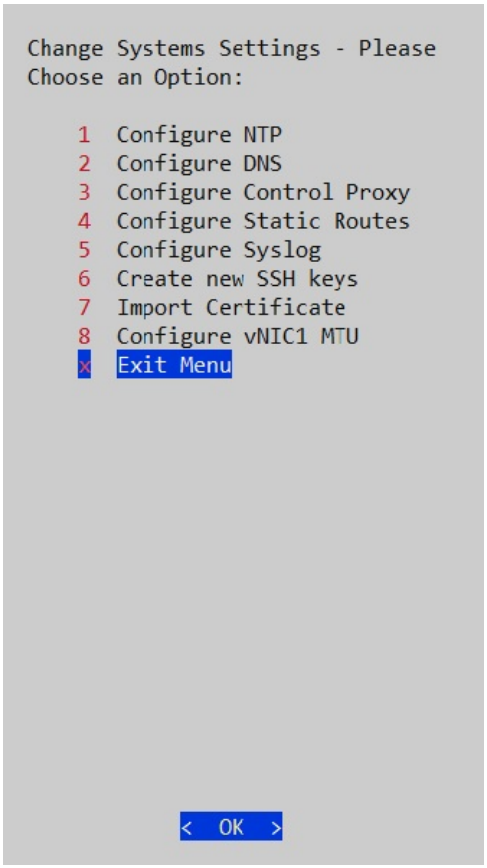
コントローラ署名証明書ファイルのインポート

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。

（注） これは、OVF テンプレートの [コントローラ設定（Controller Settings）] で [コントローラ設定証明書ファイルの URI（Controller Signing Certificate File URI）] を指定していない場合にのみ必要です。それ以外の場合は、VM の起動後にファイルは自動的にインポートされます。

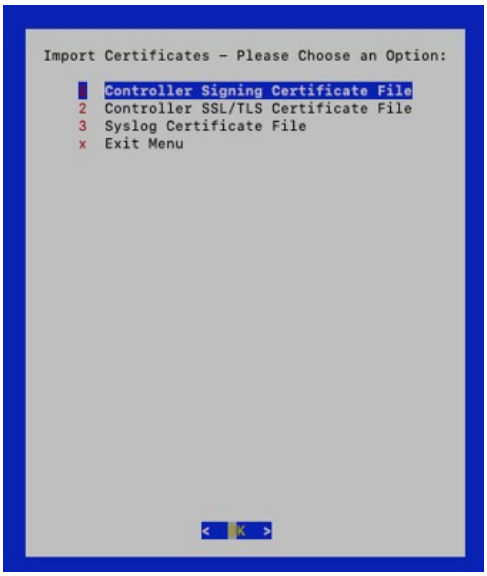
ステップ 1 Cisco Crosswork Data Gateway VM の対話型メニューから、[3 現在のシステム設定の変更（3 Change Current System Settings）] を選択します。

[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。

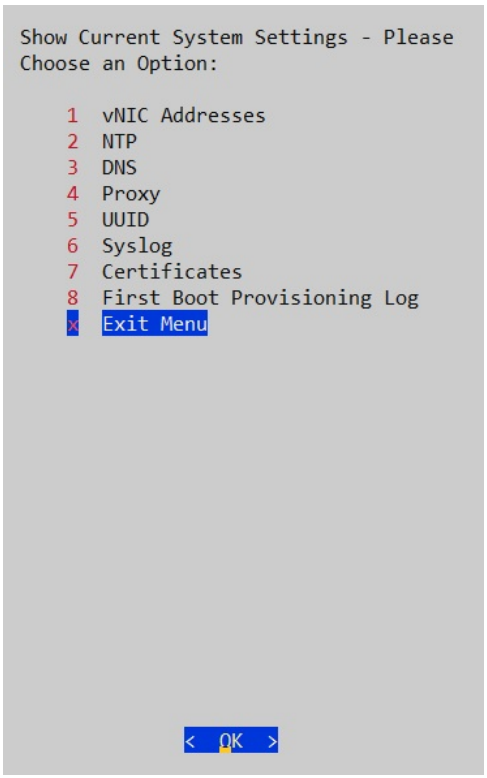
証明書ファイルがインポートされます。

ステップ 6 次の手順に従って、証明書がインストールされているかどうかを確認します。

コントローラ署名証明書ファイルの表示

次の手順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。