クラウドアプリケーション向け Cisco Crosswork Data Gateway 4.0.1 インストールおよび設定ガイド

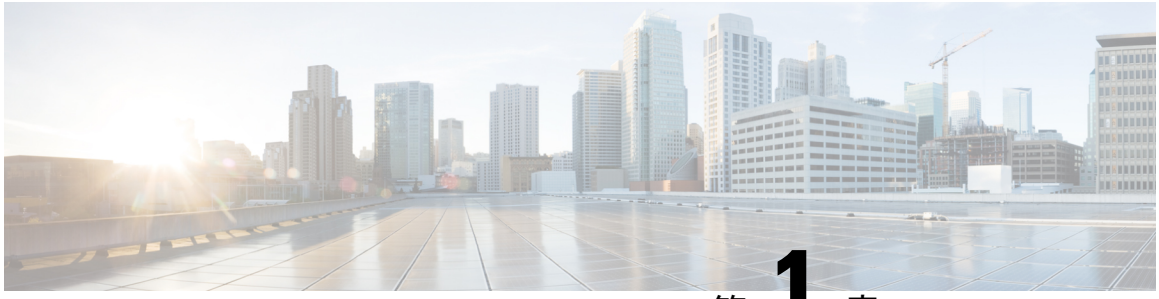
初版：2022 年 12 月 16 日

最終更新：2023 年 3 月 16 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

概要

ここでは、次の内容について説明します。

対象読者

このガイドは、ネットワークに Crosswork Cloud 用の Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） を導入する経験豊富なネットワーク管理者を対象としています。このガイドのユーザーは、Cisco Cloud 環境への有効なログインを行えるようになっている必要があります。このマニュアルは、次のトピックに関する知識があることを前提としています。

- VMware vCenter または OVF ツールを使用した OVF テンプレートの展開。
- Cisco Cloud Services Platform（CSP）での QCOW2 イメージの展開。
- OpenStack プラットフォーム。
- ネットワークのモニタリングおよびトラブルシューティング。
- Cisco IOS-XR、IOS-XE、NX-OS など、ネットワークを形成するデバイスで使用されるさまざまなオペレーティングシステム。
- 会社の内部ネットワークから Cisco Cloud に接続するために必要なプロキシ設定。

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

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） は、監視対象デバイスからのデータ収集を有効にし、収集したデータを Cisco Crosswork Cloud アプリケーションに転送

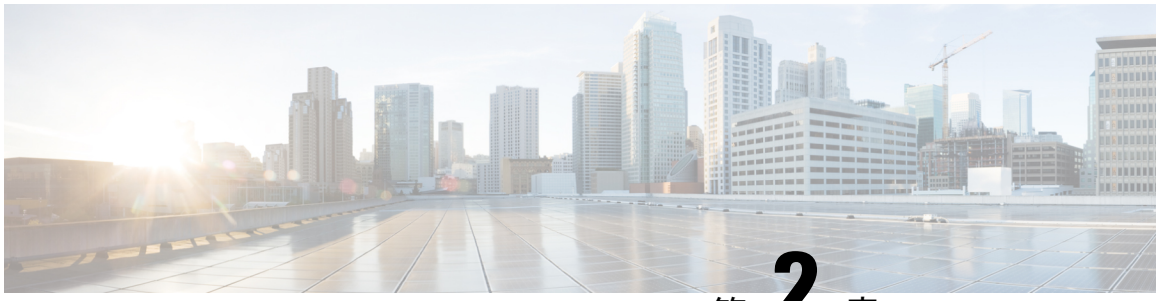
します。これらのアプリケーションは、さらに分析するためにデータを使用し、必要に応じて、管理者にさらなるアクションを促すことができます。

注目 このマニュアルでは、クラウドアプリケーション向けに Cisco Crosswork Data Gateway をインストールおよび設定する方法について説明します。

オンプレミスのアプリケーションを使用した Crosswork Data Gateway の導入について詳しくは、『*Cisco Crosswork Infrastructure 4.3 and Applications Installation Guide*』[英語] を参照してください。

Crosswork Data Gateway が次の Crosswork Cloud アプリケーションで使用できることが検証済みです。

- Cisco Crosswork Trust Insights は、デバイスの完全性についてレポートし、インベントリ確保のためのフォレンジックを提供するクラウドベースの SaaS ソリューションです。
- Cisco Crosswork Cloud Traffic Analysis サービスは、ネットワーク トラフィック フローに関する豊富な分析、可視化、および最適化の推奨事項を提供するホステッドアプリケーションです。



第 2 章

インストール要件

この章では、次のプラットフォームに Crosswork Data Gateway をインストールするための一般的なガイドラインと最小要件について説明します。

- VMware
- Cisco Cloud Services Platform（Cisco CSP）
- OpenStack プラットフォーム。

Crosswork Data Gateway インストール前のチェックリスト

インストール前のチェックリストは、次の場合に役立ちます。

- すべてのシステム要件が満たされており、必要なすべてのポートが有効になっていることを確認する。
- インストールを実行するために必要な情報を収集する。

Crosswork Data Gateway のインストールを開始する前に、インストール前のチェックリストを完成させてください。

1. ホストサーバーがリソース要件を満たしていることを確認します（「VM 要件 （4 ページ）」を参照）。
2. Crosswork Data Gateway の動作に必要なポートを有効にします（「使用ポート （6 ページ）」を参照）。
3. ご使用の環境でプロキシサーバーが必要かどうかを把握しますプロキシ サーバの要件 （7 ページ） を参照してください。

VM 要件

次の表は、サポートされている仮想プラットフォームのソフトウェア要件と、Crosswork Data Gateway をサポートするために必要な物理要件およびネットワークリソースの要件を示しています。

特に明記されていない限り、Crosswork Data Gateway をインストールするためのリソース要件は、すべてのデータセンターで同じです。

表 *1 : Cisco Crosswork Data Gateway VM* の要件

要件	説明
データセンター	VMware • VMware vCenter 7.0、ESXi 7.0 をホストにインストール済みであること • VMware vCenter Server 6.7（Update 3g 以降）、ESXi 6.7 Update 1 をホストにインストール済みであること Cisco CSP • Cisco CSP 2.8.0.276 以降 許可されたハードウェア：CSP-2100、CSP-2100-UCSD、CSP-2100-X1、CSP-2100-X2、CSP-5200、CSP-5216、CSP-5228、CSP-5400、CSP-5436、CSP-5444、CSP-5456 OpenStack • OpenStack OSP16
メモリ	32 GB
ディスク容量	74 GB
vCPU	8

<table>
<tr><th>要件</th><th>説明</th></tr>
<tr><td>インターフェイス</td><td>最小値：1
最大値：3
Crosswork Data Gateway は、次の組み合わせに従って、1 つ、2 つ、または 3 つのインターフェイスのいずれかで展開できます。
<table>
<tr><th>NIC の数</th><th>vNIC0</th><th>vNIC1</th><th>vNIC2</th></tr>
<tr><td>1</td><td>• 管理トラフィック
• 制御/データトラフィック
• デバイス アクセス トラフィック</td><td>—</td><td>—</td></tr>
<tr><td>2</td><td>• 管理トラフィック</td><td>• 制御/データトラフィック
• デバイス アクセス トラフィック</td><td>—</td></tr>
<tr><td>3</td><td>• 管理トラフィック</td><td>• 制御/データトラフィック</td><td>• デバイス アクセス トラフィック</td></tr>
</table>
• 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し、Crosswork Data Gateway VM をトラブルシューティングする場合。
• 制御/データトラフィック：Crosswork Cloud から収集ジョブの設定を受信し、収集したデータを Crosswork Cloud に転送します。
• デバイスアクセストラフィック：デバイス管理およびテレメトリデータの場合。</td></tr>
<tr><td>IP アドレス</td><td>使用するインターフェイスの数に基づいて、1 つ、2 つ、3 つの IPv4 または IPv6 アドレス。
（注） Crosswork はデュアルスタック構成をサポートしていません。したがって、環境のアドレスはすべて IPv4 または IPv6 のいずれかである必要があります。</td></tr>
</table>

要件	説明
NTP サーバ	使用する NTP サーバーの IPv4 または IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体でデバイス、クライアント、およびサーバを同期するために使用する NTP サーバと同じでなければなりません。 （注） NTP IP アドレスまたはホスト名がネットワーク上で到達可能であることを確認します。到達可能出ない場合、インストールは失敗します。 Cisco Crosswork Data Gateway ホストと仮想マシンは NTP サーバに同期する必要があります。同期しないと、Crosswork Cloud への登録を完了できない場合があります。
NTPv4 認証	強力な暗号認証に使用する NTPv4 認証プロセス。
DNS サーバー	使用する DNS サーバーの IPv4 または IPv6 アドレス。複数の DNS サーバーを入力する場合は、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ホスト名を解決するために使用する DNS サーバと同じである必要があります。
DNS 検索ドメイン	DNS サーバで使用する検索ドメイン（たとえば、cisco.com）。検索ドメインは 1 つのみ設定できます。
Syslog サーバーのアドレス（Syslog Server Address）	管理インターフェイスからアクセス可能な Syslog サーバーの IPv4 または IPv6 アドレス。 Syslog サーバーの設定方法の詳細については、「表 4 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （11 ページ）」を参照してください。
Auditd サーバアドレス（Auditd Server Address）	オプションの Auditd サーバーのホスト名、IPv4、または IPv6 アドレス。 Auditd サーバーアドレスの設定方法の詳細については、「表 4 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （11 ページ）」を参照してください。

使用ポート

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

（注） これは、基本的な Crosswork Data Gateway 機能のみを有効にするためのセットです。Crosswork Data Gateway で実行されているアプリケーションに応じて、追加のポートを有効にできます。

表 *2:* 管理トラフィック用に開くポート

ポート	プロトコル（Protocol）	使用対象	方向
22	TCP	SSH サーバ	着信
22	TCP	SCP クライアント （注） SCP ポートを設定できます。	発信
123	UDP	NTP クライアント	発信
53	UDP	DNS Client	発信
443	TCP	Crosswork コントローラ	発信

表 *3:* 制御/データ トラフィック用に開くポート

ポート	プロトコル（Protocol）	使用対象	方向
179	TCP	BGP	発信
179	TCP	BGP	着信
161	UDP	SNMP	発信
2055	UDP	NetFlow	着信

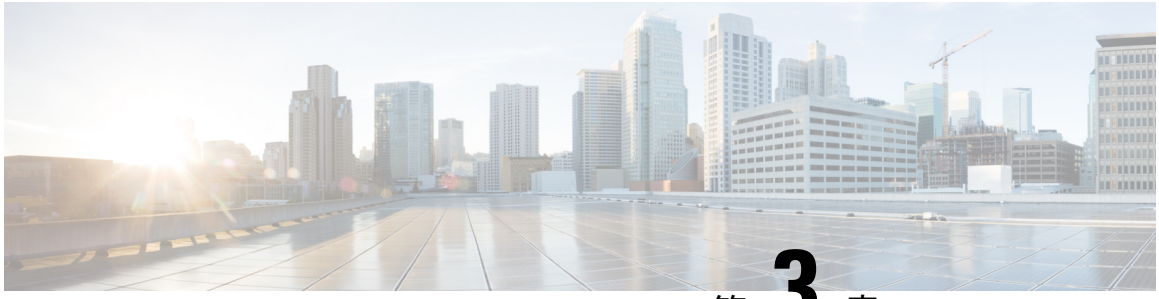
プロキシ サーバの要件

多くの実稼働環境では、パブリック インターネット サイトへの直接接続を許可しません。パブリックインターネット上の URL にアクセスするために HTTP または HTTPS プロキシが必要な環境の場合は、Cisco Crosswork Data Gateway が Crosswork Cloud サービスに正しく接続できるようにプロキシサーバーを設定する必要があります。プロキシサーバーが必要かどうかについては、ネットワーク管理者に問い合わせてください。

プロキシサーバーが必要な場合、Crosswork Data Gateway のプロキシサーバーの詳細は、次のいずれかの方法で設定します。

- （推奨）インストール時にプロキシサーバーのクレデンシャルを入力する。「Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）」の「**コントローラとプロキシの設定**」を参照してください。

- インストール後、Crosswork Data Gateway のインタラクティブコンソールから設定する。制御プロキシの設定 （75 ページ）を参照してください



第 3 章

インストール タスク

ここでは、次の内容について説明します。

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のインストール

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） は、最初に Base VM と呼ばれる VM として展開されます（Crosswork Cloud に登録するのに必要なソフトウェアしか含まれていません）。Crosswork Data Gateway が Crosswork Cloud に登録されると、Crosswork Cloud は収集ジョブの設定を Crosswork Data Gateway にプッシュし、ネットワーク デバイスから必要なデータを収集できるようにします。

ネットワークのサイズと地域に基づいて、複数の Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） を展開できます。

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）展開および設定ワークフロー

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） を展開および設定して Crosswork Cloud で使用するには、次の手順を実行します。

1. インストールの計画を立てます。展開パラメータと可能な展開シナリオについては、このトピックを参照してください。Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）
2. 使用するプラットフォームに Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） をインストールします。

VMware	vCenter vSphere Client を使用した Crosswork Data Gateway のインストール （26 ページ）
	OVF ツールによる Crosswork Data Gateway のインストール （33 ページ）
OpenStack	OpenStack CLI を使用した OpenStack への Crosswork Data Gateway のインストール （36 ページ） OpenStack UI を使用した OpenStack への Crosswork Data Gateway のインストール （43 ページ）

3. 登録パッケージの生成とエクスポート
   - 登録パッケージの生成 （61 ページ）
   - 登録パッケージのエクスポート （62 ページ）
4. Crosswork Cloud アプリケーションに Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） を登録します Crosswork Cloud アプリケーションを使用した Crosswork Data Gateway の登録 （64 ページ） を参照してください。

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

Crosswork Data Gateway のインストールを開始する前に、導入パラメータと導入シナリオについて、この項全体をお読みください。

インターフェイス アドレス

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

ユーザ アカウント

インストール時に、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） は 3 つのデフォルト ユーザー アカウントを作成します。

- インストール時に、ユーザー名 **dg-admin** とパスワードが設定された Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の管理者。管理者は、この ID を使用してログインし、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のトラブルシューティングを行います。
- インストール時に、ユーザー名 **dg-oper** とパスワードが設定された Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のオペレータ。これは読み取り専用ユーザーで、すべての「read」操作と限定された「action」コマンドを実行する権限があります。
- Crosswork Data Gateway の問題のトラブルシューティングをシスコが支援できるようにするために使用される **dg-tac** ユーザーアカウント。（TAC シェルアクセスの有効化 （88 ページ））。このアカウントの一時パスワードは、トラブルシューティング アクセスを有効にすると作成されます。

管理者とオペレータが実行できる操作については、サポートされるユーザ ロール （69 ページ） を参照してください。

dg-admin および **dg-oper** ユーザーアカウントは予約済みのユーザー名であり、変更できません。両方のアカウントに対して、コンソールからパスワードの変更を実行できます。（「パスワードの変更 （71 ページ）」を参照）。パスワードを紛失したか忘れた場合は、新しい VM を作成し、現在の VM を破棄して、新しい VM を Crosswork Cloud に再登録する必要があります。

インストールのパラメータとシナリオ

次の表では、以下の点に注意してください。

* は必須パラメータであることを示します。その他のパラメータはオプションです。必要な展開シナリオに基づいて選択できます。展開シナリオについては、必要に応じて「**その他の情報**」列で説明します。

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

表 *4 : Cisco Crosswork* データゲートウェイ（*Cisco Crosswork Data Gateway*） 導入パラメータとシナリオ

名前	パラメータ	説明	その他の情報
ホスト情報			

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

名前	パラメータ	説明	その他の情報
ラベル（Label）	`Label`	複数の Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） を分類およびグループ化するために Cisco Crosswork Cloud で使用されるラベル。	
展開	導入	コントローラタイプを伝えるパラメータ。値には `Crosswork Cloud` を指定します。	
アクティブな vNIC*	`ActiveVnics`	トラフィックの送信に使用する vNIC の数。	ネットワーク要件に応じて、1 つ、2 つ、または 3 つのインターフェイスの使用を選択できます。 トラフィックのルーティング方法については、VM 要件 （4 ページ） の表「インターフェイス」を参照してください。
AllowRFC8190 *。	`AllowRFC8190`	RFC 8190 範囲のアドレスを自動的に許可します。オプションは `yes`、`no` または `ask` です。初期構成スクリプトで確認が求められます。デフォルト値は `yes` です。	

名前	パラメータ	説明	その他の情報
秘密キー URI（Private Key URI）	DGCertKey	セッションキー署名用の秘密キーファイルへの 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 URI（Certificate File URI）	DGCertChain	この VM の PEM 形式の署名証明書チェーンへの 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）	DGCertChainPwd	Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の PEM 形式の証明書ファイルと秘密キーを取得する SCP ユーザパスフレーズ。	

名前	パラメータ	説明	その他の情報
			Crosswork Cloud は、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） とのハンドシェイクに自己署名証明書を使用します。これらの証明書はインストール時に生成されます。 ただし、サードパーティまたは独自の証明書ファイルを使用する場合は、これら 3 つのパラメータを入力します。 証明書チェーンは、Cisco Crosswork Data Gateway VM のプリセットまたは生成された証明書を上書きし、SCP URI（user:host:/path/to/file）として指定されます。 （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

名前	パラメータ	説明	その他の情報
			に存在している必要があります。
データディスクサイズ（Data Disk Size）	`DGAppdataDisk`	2 番目のデータディスクのサイズ（GB 単位）。最小サイズは24 GB です。	
パスフレーズ			
dg-admin パスフレーズ（dg-admin Passphrase）*	`dg-adminPassword`	dg-admin ユーザ用に選択したパスワード。 パスワードは 8 ー 64 文字である必要があります。	
dg-oper パスフレーズ（dg-oper Passphrase）*	`dg-operPassword`	dg-oper ユーザ用に選択したパスワード。 パスワードは 8 ー 64 文字である必要があります。	
インターフェイス （注） IPv4 アドレスまたは IPv6 アドレスのいずれかを選択する必要があります。[vNIC IPv4メソッド（vNIC IPv4 Method）] フィールドと [vNICx IPv6メソッド（vNICx IPv6 Method）] フィールドの両方で [なし（None）] を選択すると、展開が機能しなくなります。			
vNIC IPv4 アドレス（使用するインターフェイスの数に応じて vNIC0、vNIC1、および vNIC2）			

名前	パラメータ	説明	その他の情報

vNIC IPv4 メソッド（vNIC IPv4 Method）*	`Vnic0IPv4Method`
	`Vnic1IPv4Method`
	`Vnic2IPv4Method`
		[なし（None）]、[静的（Static）]、または [DHCP]。
		[メソッド（Method）] のデフォルト値は [なし（None）] です。
			[メソッド（Method）] の選択に応じて、以下を実行します。
			• [なし（None）]：IPv4アドレスの残りのフィールドをスキップします。vNIC IPv6 アドレスパラメータに情報を入力します。
			• [静的（Static）]：[アドレス（Address）]、[ネットマスク（Netmask）]、[スキップゲートウェイ（Skip Gateway）]、および [ゲートウェイ（Gateway）] フィールドに情報を入力します。
			• [DHCP]：すべての Vnic IPv4 アドレスパラメータをデフォルト値のままにします。これらの値は自動的に割り当てられます。

vNIC IPv4 アドレス（vNIC IPv4 Address）	`Vnic0IPv4Address` `Vnic0IPv4Address` `Vnic0IPv4Address`	インターフェイスの IPv4 アドレス。	
vNIC IPv4 ネットマスク（vNIC IPv4 Netmask）	`Vnic0IPv4Netmask` `Vnic0IPv4Netmask` `Vnic0IPv4Netmask`	ドット区切りの4つの数字列形式によるインターフェイスの IPv4 ネットマスク。	

vNIC IPv4 スキップゲートウェイ（vNIC IPv4 Skip Gateway）	`Vnic0IPv4SkipGateway`
	`Vnic1IPv4SkipGateway`
	`Vnic2IPv4SkipGateway`
		オプションは `True` または `False` です。
		デフォルト値は `False` です。
		`True` を選択すると、インターフェースのゲートウェイ設定がスキップされます。	

vNIC IPv4 ゲートウェイ（vNIC IPv4 Gateway）	`Vnic0IPv4Gateway`
	`Vnic1IPv4Gateway`
	`Vnic2IPv4Gateway`
		インターフェイスゲートウェイの IPv4 アドレス。	

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

名前	パラメータ	説明	その他の情報

vNIC IPv6 メソッド（vNIC IPv6 Method）*	`Vnic0IPv6Method`
	`Vnic1IPv6Method`
	`Vnic2IPv6Method`
		[なし（None）]、[静的（Static）]、または [DHCP]。
		[メソッド（Method）] のデフォルト値は [なし（None）] です。
			[メソッド（Method）] の選択に応じて、以下を実行します。
			• [なし（None）]：IPv6アドレスの残りのフィールドをスキップします。vNIC IPv4 アドレスパラメータに情報を入力します。
			• [静的（Static）]：[アドレス（Address）]、[ネットマスク（Netmask）]、[スキップゲートウェイ（Skip Gateway）]、および [ゲートウェイ（Gateway）] フィールドに情報を入力します。
			• [DHCP]：すべての Vnicx IPv6 アドレスパラメータをデフォルト値のままにします。これらの値は自動的に割り当てられます。

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

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

vNIC IPv6 スキップゲートウェイ（vNIC IPv6 Skip Gateway）	`Vnic0IPv6SkipGateway`
	`Vnic1IPv6SkipGateway`
	`Vnic2IPv6SkipGateway`
		オプションは `True` または `False` です。
		デフォルト値は `False` です。
		`True` を選択すると、インターフェースのゲートウェイ設定がスキップされます。	

vNIC IPv6 ゲートウェイ（vNIC IPv6 Gateway）	`Vnic0IPv6Gateway`
	`Vnic1IPv6Gateway`
	`Vnic2IPv6Gateway`
		インターフェイス ゲートウェイの IPv6 アドレス。	

DNS サーバ			
DNS アドレス（DNS Address）*	`DNS`	管理インターフェイスからアクセス可能な DNS サーバーの IPv4 または IPv6 アドレスのスペース区切りリスト。	

名前	パラメータ	説明	その他の情報
DNS 検索ドメイン（DNS Search Domain）*	ドメイン（Domain）	DNS 検索ドメイン	
DNSセキュリティ拡張機能（DNS Security Extensions）*。	DNSSEC	オプションは、False、True、Allow-Downgrade です。DNSセキュリティ拡張機能を使用するには、True を選択します。このパラメータは、デフォルトで False に設定されます。	
DNS over TLS*	DNSTLS	オプションは、False、True、および Opportunistic です。DNS over TLS を使用するには、True を選択します。このパラメータは、デフォルトで False に設定されます。	
マルチキャスト DNS*	mDNS	オプションは、False、True、および Resolve です。マルチキャスト DNS を使用するには、True を選択します。このパラメータは、デフォルトで False に設定されます。	
リンクローカルマルチキャスト名前解決*	LLMNR	オプションは、False、True、Opportunistic、および Resolve です。リンクローカルマルチキャスト名前解決を使用するには、True を選択します。このパラメータは、デフォルトで False に設定されます。	

名前	パラメータ	説明	その他の情報
NTPv4サーバ			
NTPv4 サーバ（NTPv4 Servers）*	NTP	NTPv4 サーバーリスト。管理インターフェイスからアクセス可能な NTPv4 サーバーの IPv4/IPv6 アドレスまたはホスト名のスペース区切りリストを入力します。	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、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）、Crosswork Cloud 、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、Crosswork Cloud と Cisco Crosswork データゲートウェイ（Cisco 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。
NTPv4 認証の使用（Use NTPv4 Authentication）	NTPAuth	NTPv4 認証を使用するには、Yes を選択します。デフォルト値は [いいえ（No）] です。	
NTPv4 キー（NTPv4 Keys）	NTPKey	サーバーリストにマッピングするためのキー ID。キー ID のスペース区切りリストを入力します。	
NTPv4 キーファイル URI（NTPv4 Key File URI）	NTPKeyFile	chrony キーファイルへの SCP URI。	
NTPv4 キーファイルパスフレーズ（NTPv4 Key File Passphrase）	NTPKeyFilePwd	chrony キーファイルへの SCP URI のパスワード。	
リモート Syslog サーバー（Remote Syslog Server）			

名前	パラメータ	説明	その他の情報
リモート Syslog サーバーの使用*	UseRemoteSyslog	リモートホストに Syslog メッセージを送信するには、Yes を選択します。デフォルト値は [いいえ（No）] です。	
Syslog サーバーのアドレス（Syslog Server Address）	SyslogAddress	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、アドレスを角カッコ（[1::1]）で囲みます。	
Syslog サーバーポート（Syslog Server Port）	SyslogPort	オプションの syslog サーバーのポート番号。ポート値の範囲は 1 ～ 65535 です。デフォルトでは、この値は 514 に設定されます。	
Syslog サーバープロトコル（Syslog Server Protocol）	SyslogProtocol	Syslog の送信時に UDP または TCP を使用します。デフォルト値は UDP です。	
TLS 経由の Syslog を使用するかどうか（Use Syslog over TLS?）	SyslogTLS	TLS を使用して Syslog のトラフィックを暗号化するには、Yes を選択します。デフォルトでは、このパラメータは [いいえ（No）] に設定されています。	
	SyslogPeerName		

名前	パラメータ	説明	その他の情報
Syslog TLS ピア名（Syslog TLS Peer Name）		サーバー証明書の SubjectAltName またはサブジェクト共通名に入力されたとおりの Syslog サーバーのホスト名。	
Syslog ルート証明書ファイル URI（Syslog Root Certificate File URI）	`SyslogCertChain`	SCP を使用して取得した syslog サーバーの PEM形式のルート証明書への URI。	
Syslog 証明書ファイルのパスフレーズ（Syslog Certificate File Passphrase）	`SyslogCertChainPwd`	Syslog 証明書チェーンを取得する SCP ユーザのパスワード。	

名前	パラメータ	説明	その他の情報
			外部 syslog サーバを設定すると、サービスイベントが外部 syslog サーバーに送信されます。それ以外の場合は、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） VM にのみ記録されます。 外部 syslog サーバーを使用する場合は、次の設定を行う必要があります。 • Syslog リモートサーバーの使用（Use Remote Syslog Server） • Syslog サーバーのアドレス（Syslog Server Address） • Syslog サーバーポート（Syslog Server Port） • Syslog サーバープロトコル（Syslog Server Protocol） （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

名前	パラメータ	説明	その他の情報
			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。
リモート監査サーバー			
リモート監査サーバーの使用*	`UseRemoteAuditd`	リモートホストに監査メッセージを送信するには、Yes を選択します。	監査メッセージをリモートサーバーに送信するように Crosswork Data Gateway を設定します。 外部の Auditd サーバーに監査メッセージを転送するには、これらの 3 つのパラメータを指定します。
Auditd サーバアドレス（Auditd Server Address）	`AuditdAddress`	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）	`AuditdPort`	オプションの監査サーバのポート番号。	
コントローラとプロキシの設定			

名前	パラメータ	説明	その他の情報
プロキシ サーバの URL（Proxy Server URL）	ProxyURL	オプションの管理ネットワーク プロキシ サーバーの URL。	クラウドの導入では、Cisco Crosswork Data Gateway は TLS 経由でインターネットに接続する必要があります。 プロキシサーバーを使用する場合は、これらのパラメータを指定します。
プロキシ サーバ バイパス リスト（Proxy Server Bypass List）	ProxyBypass	プロキシを使用しないアドレスとホスト名のカンマ区切りリスト	
認証プロキシのユーザ名（Authenticated Proxy Username）	ProxyUsername	認証済みプロキシサーバのユーザ名。	
認証プロキシのパスフレーズ（Authenticated Proxy Passphrase）	ProxyPassphrase	認証済みプロキシサーバのパスフレーズ。	
HTTPS プロキシ SSL/TLS 証明書ファイル URI（HTTPS Proxy SSL/TLS Certificate File URI）	ProxyCertChain	SCP を使用して取得した HTTPS プロキシの PEM 形式の SSL/TLS 証明書ファイル。	
HTTPS プロキシ SSL/TLS 証明書ファイルのパスフレーズ（HTTPS Proxy SSL/TLS Certificate File Passphrase）	ProxyCertChainPwd	プロキシ証明書チェーンを取得する SCP ユーザのパスワード。	
自動登録パッケージの転送（Auto Enrollment Package Transfer）			

名前	パラメータ	説明	その他の情報
登録の宛先ホストとパス（Enrollment Destination Host and Path）**	`EnrollmentURI`	SCP を使用して登録パッケージを転送する SCP ホストおよびパス（`user@host:/path/to/file`）。	Crosswork Cloud に Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） を登録するには、登録パッケージが必要です。インストール中にこれらのパラメータを指定すると、登録パッケージは、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の初回起動時にそのローカルホストに自動的に転送されます。 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、登録パッケージのエクスポート （62 ページ）の手順に従って登録パッケージを手動でエクスポートします。
登録パスフレーズ（Enrollment Passphrase）**	`EnrollmentPassphrase`	登録パッケージを転送するための SCP ユーザパスフレーズ。	

次の作業：Cisco Crosswork Data Gateway VM のインストールに進みます。

vCenter vSphere Client を使用した Crosswork Data Gateway のインストール

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

ステップ 1 *Crosswork Data Gateway 4.0.1* のリリースノートを参照し、Crosswork Data Gateway のイメージ（*.ova）ファイルをダウンロードします。

（注） 最新の Mozilla Firefox バージョンを使用して .ova イメージをダウンロードする場合、ダウンロードしたファイルの拡張子が .dms である場合は、インストール前に拡張子を .ova に戻します。

ステップ 2 vCenter に接続し、クレデンシャルを使用してログインします。

ステップ 3 Crosswork Data Gateway VM を展開するデータセンターを選択します。

ステップ 4 vCenter Server 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。

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 テンプレート展開の完了にかかる時間が 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。これを防ぐために、展開を開始する前にテンプレートを確認し、入力する内容を決めておくことをお勧めします。

vCenter に接続し、クレデンシャルを使用してログインします。

ステップ 5 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) [ローカルファイル（Local File）] を選択し、[参照（Browse）] をクリックして、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。

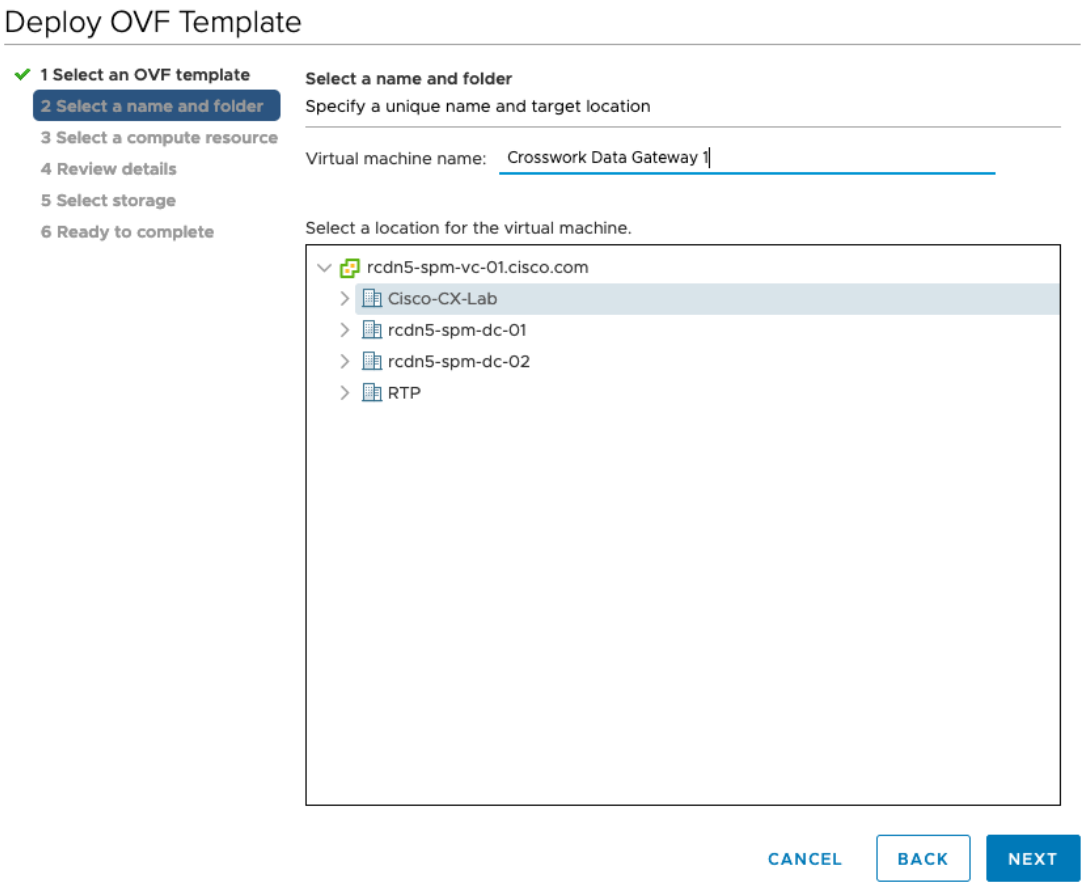
ファイル名がウィンドウに表示されます。

ステップ 6 次の図のように、[次へ（Next）] をクリックして、 [2 名前とフォルダの選択（2 Select name and folder）] に移動します。

a) 作成する Cisco Crosswork Data Gateway VM の名前を入力します。

大規模なシステムでは、複数の Cisco Crosswork Data Gateway VM を使用する可能性があります。したがって、Cisco Crosswork Data Gateway の名前は一意であり、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。

b) [仮想マシンの場所を選択（Select a location for the virtual machine）] リストで、Cisco Crosswork Data Gateway VM が存在するデータセンターを選択します。



ステップ 7 [次へ（Next）] をクリックして、[3 コンピューティングリソースの選択（3 Select a compute resource）] に進みます。VM のホストを選択します。

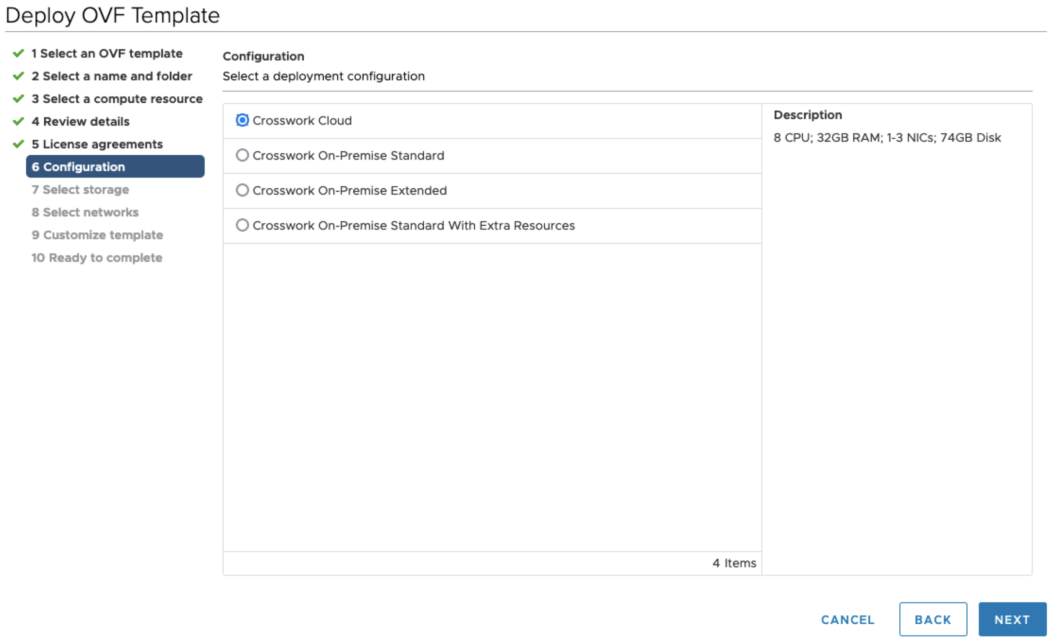
ステップ 8 [次へ（Next）] をクリックします。VMware vCenter Server が OVA を検証します。検証にかかる時間はネットワーク速度によって決まります。検証が完了すると、ウィザードは [4 詳細の確認（4 Review details）] に移動します。OVA の情報を確認して [次へ（Next）] をクリックします。

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。テンプレートは、オンプレミス展開のディスク要件を報告します。次の手順で正しいディスク構成を選択するため、これは無視してかまいません。

ステップ 9 [次へ（Next）] をクリックして、[5 ライセンス契約書（5 License agreements）] に移動します。エンドユーザ 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 10 次の図のように、[次へ（Next）] をクリックして [6 設定（6 Configuration）] に移動します。[Crosswork Cloud] を選択します。

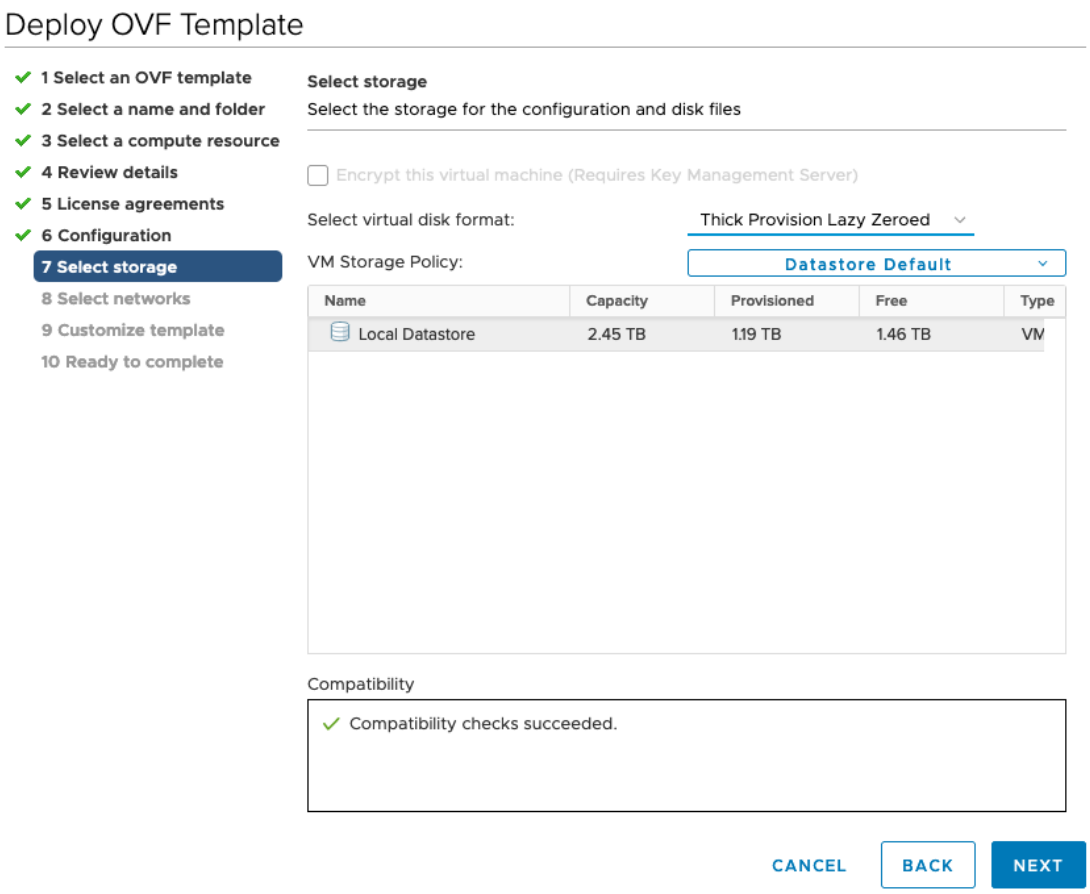


ステップ 11 次の図のように、[次へ（Next）] をクリックして [7 ストレージの選択（7 Select storage）] に移動します。

a) [仮想ディスクフォーマットの選択（Select virtual disk format）] フィールドで次のように選択します。

- 実稼働環境の場合、[シックプロビジョニングLazy Zeroed（Thick Provision Lazy Zeroed）] を選択します。
- 開発環境の場合、[シンプロビジョニング（Thin Provision）] を選択します。

b) [データストア（Datastores）] テーブルから、使用するデータストアを選択します。

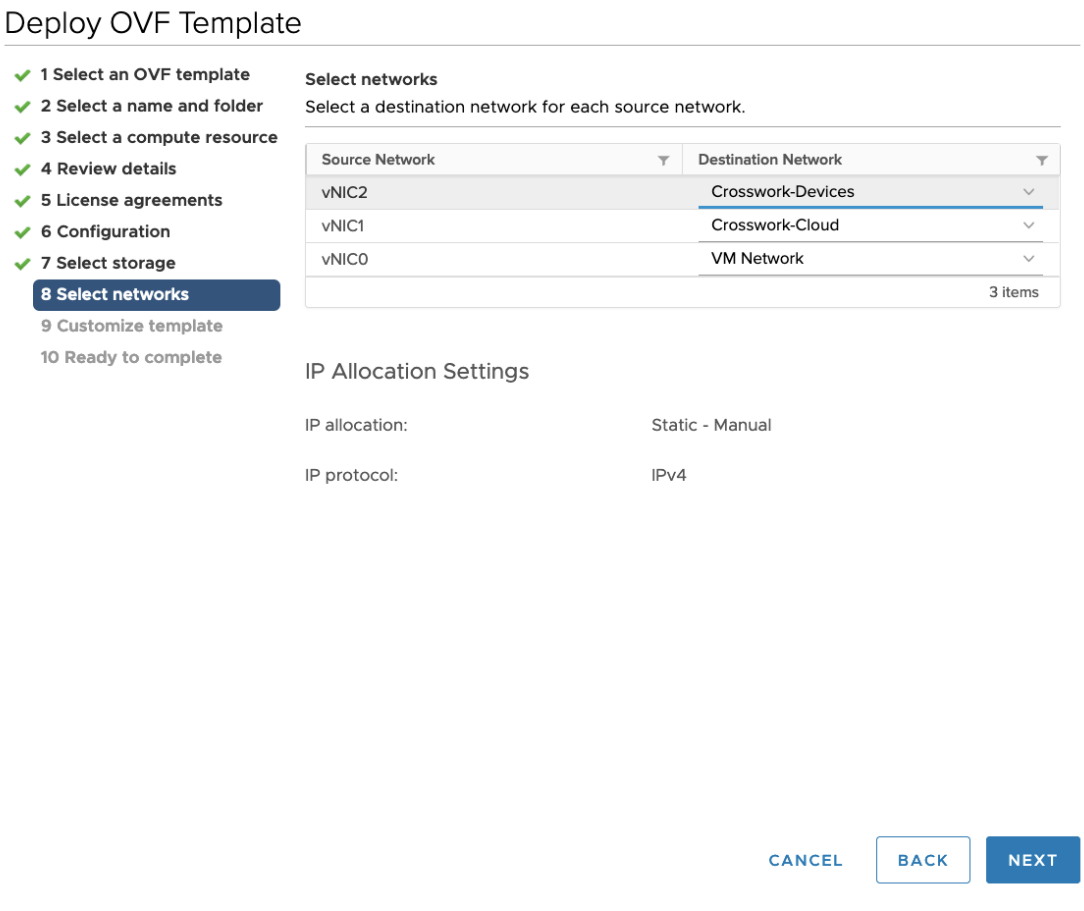


ステップ 12 次の図のように、[次へ（Next）] をクリックして [8 ネットワークの選択（8 Select networks）] に移動します。ページ上部のドロップダウンテーブルで、使用予定の vNIC の数に基づいて、各送信元ネットワークに適切な宛先ネットワークを選択します。

vNIC0 から順に、使用する宛先ネットワークを選択してください。未使用の **vNIC** は、デフォルト値のままにてください。

（注） 次のイメージ画像では、以下のネットワークが選択されています。

- **VM Network** は、インタラクティブコンソールにアクセスして、Crosswork Data Gateway VM のトラブルシューティングを行うための管理ネットワークです。
- **Crosswork-Cloud** は、Crosswork Data Gateway が Crosswork Cloud に接続するコントローラネットワークです。
- **Crosswork-Devices** は、デバイス アクセス トラフィック用のネットワークです。



ステップ 13 [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（Customize template）] に移動します。

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

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ） の説明に従って、パラメータの情報を入力します。

（注） このメニューが最初に表示されるとき、「7つのプロパティに無効な値があります（7 properties have invalid values）」というエラーが発生します。これは正常な動作であり、適切な値を入力するとクリアされます。

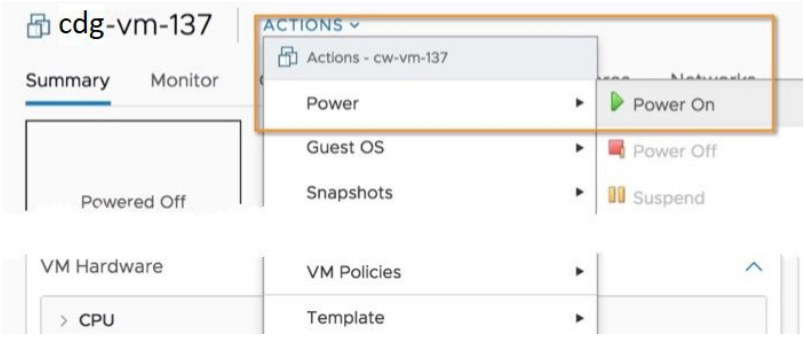
ステップ 14 [次へ（Next）] をクリックして、[10 完了の準備（10 Ready to complete）] に移動します。設定を確認し、展開を開始する準備ができたら [終了（Finish）] をクリックします。

ステップ 15 展開ステータスを確認します。

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。

ステップ 16 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、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。これらの設定を変更する場合は、自己責任で行ってください。IP アドレスを変更する場合は、現在の VM を破棄し、新しい VM を作成して、新しい VM を Crosswork Cloud に再登録します。

インストールが成功したことを確認します。

1. vCenter 経由で 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。

2. SSH 経由で Crosswork Data Gateway VM にアクセスします。

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

   ssh <username>@<ManagementNetworkIP>

   ここで、**ManagementNetworkIP** は、IPv4 または IPv6 アドレス形式の管理ネットワーク IP アドレスです。

   次の例を参考にしてください。

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

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

（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。

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**] キーを押します。

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

次のタスク

登録パッケージを生成およびエクスポートして、Crosswork Cloud に Crosswork Data Gateway を登録します。登録パッケージのエクスポート （62 ページ） を参照してください。

OVF ツールによる Crosswork Data Gateway のインストール

要件に応じて、コマンドやスクリプトの必須または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。Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）導入パラメータとシナリオ （10 ページ）を参照してください。

スクリプトで OVF ツールを実行する場合のサンプルスクリプトを次に示します。次のサンプルでは、2 つのネットワーク インターフェイスを使用して、ホスト名が「dg-141」の Crosswork Data Gateway VM を作成します。

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

# robot.ova path

DG_OVA_PATH="<mention the orchestrator path>"

VM_NAME="dg-141"
DM="thin"
Deployment="cloud"

ActiveVnics="2"

Hostname="Hostname"
Vnic0IPv4Address="<Vnic0_ipv4_address>"
Vnic0IPv4Gateway="<Vnic0_ipv4_gateway>"
Vnic0IPv4Netmask="<Vnic0_ipv4_netmask>"
Vnic0IPv4Method="Static"
Vnic1IPv4Address="<Vnic1_ipv4_address>"
```

```
Vnic1IPv4Gateway="<Vnic1_ipv4_gateway>"
Vnic1IPv4Netmask="<Vnic1_ipv4_netmask>"
Vnic1IPv4Method="Static"

DNS="<DNS_ip_address>"
NTP="<NTP Server>"
Domain="cisco.com"


Description="Description for Cisco Crosswork Data Gatewayi : "dg-141""
Label="Label for Cisco Crosswork Data Gateway dg-141"

dg_adminPassword="<dg-admin_password>"
dg_operPassword="<dg-oper_password>"

EnrollmentURI="<enrollment_package_URI>"
EnrollmentPassphrase="<password>"

ProxyUsername="<username_for_proxy>"
ProxyPassphrase="<password_for_proxy>"

SyslogAddress="<syslog_server_address>"
SyslogPort=<syslog_server_port>
SyslogProtocol="<syslog_server_protocol>"
SyslogTLS=False
SyslogPeerName="<syslog_server_peer_name>"
SyslogCertChain="<syslog_server_root_certificate>"
SyslogCertChainPwd="<password>"

# Please replace this information according to your vcenter setup
VCENTER_LOGIN="<vCenter login details>"
VCENTER_PATH="<vCenter path>"
DS="<DS details>"

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
 --powerOffTarget --powerOn \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"EnrollmentURI=$EnrollmentURI" \
--prop:"EnrollmentPassphrase=$EnrollmentPassphrase" \
--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" $DG_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"
```

ステップ 1 インストールを実行するマシンでコマンドプロンプトを開きます。

ステップ 2 テンプレートファイルを開き、Cisco Crosswork Data Gateway 用に選択した設定と一致するように編集します。

ステップ 3 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 4 スクリプトを使用して OVF ツールを実行します。

```
root@cxcloudctrl:/opt# ./<script_file>
```

次に例を示します。

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

インストールが成功したことを確認します。

1. vCenter 経由で 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. ユーザー名（`dg-admin`）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。

2. SSH 経由で Crosswork Data Gateway VM にアクセスします。

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

   ssh <username>@<ManagementNetworkIP>

   ここで、**ManagementNetworkIP** は、IPv4 または IPv6 アドレス形式の管理ネットワーク IP アドレスです。

   次の例を参考にしてください。

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

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

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**] キーを押します。

（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。

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

次のタスク

Crosswork Cloud での Crosswork Data Gateway の登録に進みます 登録パッケージのエクスポート （62 ページ） を参照してください。

OpenStack CLI を使用した OpenStack への Crosswork Data Gateway のインストール

この項では、OpenStack プラットフォームに Crosswork Data Gateway をインストールする際の手順について詳しく説明します。

（注）
1. この手順では、OpenStack 環境でネットワーク、ポート、およびボリュームを作成するためのコマンド一覧を記載します。これにはいくつかの方法があることをご留意ください。
2. ここに記載されているすべての IP アドレスは、マニュアルで参照することを目的としたサンプルの IP アドレスです。

始める前に

次の情報を用意しておきます。

- インストールする Crosswork Data Gateway VM インスタンスの数。
- インストールの計画を立てます。Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）を参照してください。
- VM に使用するアドレス指定方法（DHCP または静的）を決定します。
- 静的アドレス指定を使用する場合は、各 VM の IP アドレス、サブネット、ポートなどのネットワーク情報を用意します。
- セキュリティグループのルールとポリシーを作成して使用する前に理解します。

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

a) 入手可能な最新の Cisco Crosswork Data Gateway イメージ（*.bios.signed.bin）を cisco.com からローカルマシン、または OpenStack にアクセスできる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-4.0.1-65-release-20221130.bios.signed.bin**」を使用します。

b) 次のコマンドを実行して bin ファイルの内容を現在のディレクトリに抽出します。

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
```

このコマンドにより、製品の真正性が確認されます。ディレクトリには、以下のファイルが格納されています。

```
CDG-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
README
cisco_x509_verify_release.py
cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz.signature
```

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

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

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

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

d) 次のコマンドを使用して、QCOW2 ファイル（**cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz**）を解凍します。

```
tar -xvf cw-na-dg-4.0.1-65-release-20221130.uefi.tar.gz
```

これにより、config.txt ファイルを含む新しいディレクトリが作成されます。

ステップ 2 Crosswork Data Gateway VM に使用するアドレス指定のタイプに基づいて、手順 3 **または**手順 4 を実行します。

ステップ 3 **Crosswork Data Gateway VM の `config.txt` を静的アドレス指定で更新します。**

a) Crosswork Data Gateway リリースイメージをダウンロードしたディレクトリに移動します。

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。詳細については、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）を参照してください。

静的アドレス指定を使用して、ホスト名 `cdg1-nodhcp` で 3 つの NIC を展開する場合のサンプル `config.txt` ファイルを以下に示します。このリスト内の必須パラメータは強調表示されています。

（注） 展開する NIC が 1 つまたは 2 つの場合は、`config.txt` の `ActiveVnics` パラメータはそれぞれ 1 または 2 になります。

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
```

```
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=<Hostname of VM>
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
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=10.10.11.101 //Same IP address needs to be entered when creating ports of the
 VM.
Vnic0IPv4Gateway=10.10.11.1
Vnic0IPv4Method=Static
Vnic0IPv4Netmask=255.255.255.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=10.10.21.101 // Same IP address needs to be entered when creating ports of the
 VM.
Vnic1IPv4Gateway=10.10.21.1
Vnic1IPv4Method=Static
Vnic1IPv4Netmask=255.255.255.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=10.10.31.101 //Same IP address needs to be entered when creating ports of the
 VM.
Vnic2IPv4Gateway=10.10.31.1
Vnic2IPv4Method=Static
```

```
Vnic2IPv4Netmask=255.255.255.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Admin user password>
dg-operPassword=<Operator user password>
```

c) config.txt ファイルを VM のホスト名や更新した VM を識別しやすい名前で保存します。

d) （重要）config.txt で vNIC IP アドレスとして入力した IP アドレスを書き留めておいてください。手順 9 で VM のポートを作成するときに、同じ IP アドレスを指定する必要があります。

e) **手順 3（b）と手順 3（d）**を繰り返して、各 VM の一意の config.txt ファイルを静的アドレス指定を使用してを更新および保存します。

f) **手順 5** に進みます。

ステップ 4　Crosswork Data Gateway VM の `config.txt` を DHCP を使用して更新します。

a) Crosswork Data Gateway リリースイメージをダウンロードしたディレクトリに移動します。

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。詳細については、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）を参照してください。

DHCP を使用して、ホスト名 cdg1-nodhcp で 3 つの NIC を展開する場合のサンプル config.txt ファイルを以下に示します。このリスト内の必須パラメータは強調表示されています。

（注）　展開する NIC が 1 つまたは 2 つの場合は、config.txt の ActiveVnics パラメータはそれぞれ 1 または 2 になります。

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=cdg1-nodhcp
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
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 //Leave the default value unchanged
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=DHCP
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=DHCP
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=DHCP
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Administrator user password>
dg-operPassword=<Operator user password>
```

c) `config.txt` ファイルを VM のホスト名や更新した VM を識別しやすい名前で保存します。

d) **手順 4**（**b**）と**手順 4**（**c**）を繰り返して、各 VM の一意の config.txt ファイルを DHCP アドレス指定を使用してを更新および保存します。

e) **手順 5** に進みます。

ステップ 5 CLI から OpenStack VM にログインします。

ステップ 6 **VM のリソースプロファイルまたはフレーバーを作成します。**

```
openstack flavor create --public --id auto --vcpus 8 --ram 32768 --disk 74 cdg-cloud
```

ステップ 7 **OpenStack インストール用のイメージを作成します。**

```
openstack image create --public --disk-format qcow2 --container-format bare --file
<bios_release_image_file> <image_name>
```

次に例を示します。

```
openstack image create --public --disk-format qcow2 --container-format bare --file
cw-na-dg-4.0.1-65-release-20221130.bios.qcow2 cdg-cloud-bios
```

ステップ 8 各 **Crosswork Data Gateway VM** に対して、**VM** 固有のパラメータを作成します。

インストールする Crosswork Data Gateway VM インスタンスごとに、次のパラメータを作成します。

a) （オプション）**10 GB/秒のデータディスクを作成します。**

```
openstack  volume create --size <volume_size> <volume_name>
```

コマンド例：

```
openstack volume create --size 10 cdg-vol1
```

b) **着信 TCP/UDP/ICMP 接続を許可するセキュリティポリシーを作成します。**

OpenStack は、デフォルトで着信 TCP/UDP/ICMP 接続を許可しません。TCP/UDP/ICMP プロトコルからの着信接続を許可するセキュリティポリシーを作成します。

```
openstack security group create open
openstack security group rule create open --protocol tcp --dst-port <port_number> --remote-ip
<IP_address>
openstack security group rule create open --protocol udp --dst-port <port_number> --remote-ip
<IP_address>
openstack security group rule create --protocol icmp open
```

c) **静的アドレス指定を使用した Crosswork Data VM に対してのみ、IP アドレスを指定してポートを作成します。**

重要 この手順は、静的アドレス指定を使用する場合にのみ必要です。DHCP アドレス指定を使用する場合、ポートの IP アドレスは、サブネットの IP アドレス割り当てプールから自動的に割り当てられます。

```
openstack port create --network network_name --fixed-ip
subnet=subnet_name,ip-address=port_ip_address port_name
```

静的アドレス指定を使用する 3 つの NIC を備えた CDG VM のポートを作成する場合のコマンド例：

```
openstack port create --network network1 --fixed-ip subnet=subnet1,ip-address=10.10.11.101
mgmt-port1
openstack port create --network network2 --fixed-ip subnet=subnet2,ip-address=10.10.21.101
north-port1
openstack port create --network network3 --fixed-ip subnet=subnet3,ip-address=10.10.31.101
south-port1
```

上記のコマンドで、`network1` は環境内の管理ネットワーク、`subnet1` は管理ネットワーク上のサブネット、`mgmt-port1` は、VM の `config.txt` ファイルで指定した vNIC0 の IP アドレス（`10.10.11.101`）で作成するポートです。

d) **ポートにセキュリティポリシーを適用します。**

```
openstack port set <port_name> --security-group open
```

次に例を示します。

```
openstack port set mgmt-port1 --security-group open
openstack port set north-port1 --security-group open
openstack port set south-port1 --security-group open
```

e) インストールするすべての VM について、手順 **9** を繰り返します。

ステップ 9 Crosswork Data Gateway VMをインストールします。

静的アドレス指定を使用する 3 つの NIC を備えた Crosswork Data Gateway VM をインストールするためのコマンド

```
openstack server create --flavor <flavor_name> --image <image_name> --port <mgmt-port> --port
<north-port> --port <south-port> --config-drive True --user-data <config.txt> --block-device-mapping
 vdb=<volume_name>:::true <CDG_hostname>
```

次に例を示します。

```
openstack server create --flavor  cdg-cloud --image cdg-cloud-bios --port mgmt-port1 --port north-port1
 --port south-port1 --config-drive True --user-data config-nodhcp-cdg1.txt --block-device-mapping
vdb=cdg1:::true cdg1-nodhcp
```

OR

```
openstack server create --config-drive true --flavor cdg --image <image_name> --key-name default
--nic net-id=<network id>,v4-fixed-ip=<CDG static IP> --security-group <security group name>
--user-data <config.txt> <CDG_hostname>
```

DHCP を使用する 3 つの NIC を備えた Crosswork Data Gateway VM をインストールするためのコマンド

```
openstack server create --flavor <flavor_name> --image <image_name> --network <network1> --network
 <network2> --network <network3> --config-drive True --user-data <config.txt> --host <boot_drive>
--block-device-mapping vdb=<volume_name>:::true <CDG_hostname>
```

次に例を示します。

```
openstack server create --flavor cdg-cloud --image cdg-cloud-bios --network network1 --network
network2 --network network3 --config-drive True --user-data config-dhcp-cdg1.txt --block-device-mapping
 vdb=cdg1:::true cdg1-dhcp
```

OR

```
openstack server create --config-drive true --flavor cdg --image <image_name> --key-name default
--network <network with dhcp> --security-group <security group name> --user-data <config.txt>
<CDG_name>
```

（注） VM をインストールするためのコマンドで指定するネットワークの数は、展開する NIC の数によって異なります。

たとえば、2 つの NIC を備えた VM をインストールする場合のコマンドは次のとおりです。

```
openstack server create --flavor cdg-cloud --image cdg-cloud-bios --port mgmt-port2 --port
south-port2 --config-drive True --user-data config-nodhcp_2nic.txt --block-device-mapping
vdb=cdg-vol:::true cdg-bios-nodhcp_2NIC
```

Crosswork Data Gateway VM が正常にインストールされたことを確認します。

次のコマンドを実行して、VM のインストールのステータスを表示します。

```
openstack server list
```

```
(osp16VTS) [stack@ospd16-director cdg-image]$ openstack server list
+--------------------------------------+---------------------+--------+----------------------------------------------------------------------------------------------+-------------------+-----------+
| ID                                   | Name                | Status | Networks                                                                                     | Image             | Flavor    |
+--------------------------------------+---------------------+--------+----------------------------------------------------------------------------------------------+-------------------+-----------+
| 8b039d3c-1bb9-4ce2-9b24-1654216c4dd6 | cdg-bios-nodhcp_2NIC | ACTIVE | network1-nodhcp=[illegible]; network3-nodhcp=[illegible]                                   | cdg-cloud-bios-345 | cdg-cloud |
| 9c6d913f-c24b-43a3-9816-f865e58e7e95 | cdg-bios-nodhcp     | ACTIVE | network1-nodhcp=[illegible]; network2-nodhcp=[illegible]; network3-nodhcp=[illegible]      | cdg-cloud-bios-345 | cdg-cloud |
+--------------------------------------+---------------------+--------+----------------------------------------------------------------------------------------------+-------------------+-----------+
```

VM のステータスが **Active** と表示されたら、約 10 分間待って、CLI または OpenStack UI から VM が適切に展開され、想定通りに稼働していることを 確認します。

OpenStack の CLI から実行する場合

1. OpenStack の CLI で次のコマンドを実行して、VM インスタンスの URL を取得します。

   ```
   openstack console url show <CDG hostname>
   ```

   次に例を示します。

   ```
   openstack console url show cdg-dhcp
   ```

2. dg-admin ユーザーまたは dg-oper ユーザー（割り当てられたロールに応じて）のアカウントと、VM の `config.txt` ファイルに入力した対応するパスワードを使用してログインします。正常にログインすると、Crosswork Data Gateway のインタラクティブコンソールが表示されます。

OpenStack の UI から実行する場合

1. OpenStack の UI にログインします。
2. [コンピューティング（Compute）] > [インスタンス（Instances）] に移動します。
3. Crosswork Data Gateway の VM 名をクリックします。VM コンソールへのリンクが新しいタブで開きます。
4. dg-admin ユーザーまたは dg-oper ユーザー（割り当てられたロールに応じて）のアカウントと、VM の `config.txt` ファイルに入力した対応するパスワードを使用してログインします。正常にログインすると、Crosswork Data Gateway のインタラクティブコンソールが表示されます。

次のタスク

Crosswork Cloud での Crosswork Data Gateway の追加に進みます 登録パッケージのエクスポート（62 ページ） を参照してください。

OpenStack UI を使用した OpenStack への Crosswork Data Gateway のインストール

この項では、OpenStack プラットフォームに Crosswork Data Gateway をインストールする際の手順について詳しく説明します。

（注） ここに記載されているすべての IP アドレスは、マニュアルで参照することを目的としたサンプルの IP アドレスです。

始める前に

次の情報を用意しておきます。

- インストールする Crosswork Data Gateway VM インスタンスの数。
- インストールの計画を立てます。Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）を参照してください。
- VM に使用するアドレス指定方法（DHCP または静的）を決定します。
- 静的アドレス指定を使用する場合は、各 VM の IP アドレス、サブネット、ポートなどのネットワーク情報を用意します。
- VM に適用するセキュリティグループを作成する前に、セキュリティグループのルールとセキュリティ ポリシーを理解します。

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

a) 入手可能な最新の Cisco Crosswork Data Gateway イメージ（*.bios.signed.bin）を cisco.com からローカルマシン、または OpenStack にアクセスできる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-4.0.1-65-release-20221130.bios.signed.bin**」を使用します。

b) bin ファイルの内容を現在のディレクトリに抽出します。

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
```

このコマンドにより、製品の真正性が確認されます。ディレクトリには、以下のファイルが格納されています。

```
CDG-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
README
cisco_x509_verify_release.py
cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz.signature
```

ネットワーク接続の問題が発生した場合は、この検証をスキップして、次の手順の説明に従って手動検証を実行します。

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin --skip-verification
```

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

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

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

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

d) 次のコマンドを使用して、QCOW2 ファイル（**cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz**）を解凍します。

```
tar -xvf cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
```

これにより、config.txt ファイルを含む新しいディレクトリが作成されます。

ステップ 2 Crosswork Data Gateway VM に使用するアドレス指定のタイプに基づいて、手順 3 **または**手順 4 を実行します。

ステップ 3 **Crosswork Data Gateway VM の `config.txt` を静的アドレス指定で更新します。**

a) Crosswork Data Gateway リリースイメージをダウンロードしたディレクトリに移動します。

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。詳細については、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）を参照してください。

重要 VM のポートを作成するために使用している IP アドレスを書き留めます。各 VM の `config.txt` ファイルの vNIC IP アドレスには、ここで入力したものと同じ IP アドレスを指定する必要があります。

静的アドレス指定を使用して、ホスト名 `cdg1-nodhcp` で 3 つの NIC を展開する場合のサンプル `config.txt` ファイルを以下に示します。このリスト内の必須パラメータは強調表示されています。

（注） 展開する NIC が 1 つまたは 2 つの場合は、`config.txt` の `ActiveVnics` パラメータはそれぞれ 1 または 2 になります。

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
```

```
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=<Hostname of VM>
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
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=10.10.11.101 //Same IP address needs to be entered when creating ports of the
 VM.
Vnic0IPv4Gateway=10.10.11.1
Vnic0IPv4Method=Static
Vnic0IPv4Netmask=255.255.255.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=10.10.21.101 // Same IP address needs to be entered when creating ports of
the VM.
Vnic1IPv4Gateway=10.10.21.1
Vnic1IPv4Method=Static
Vnic1IPv4Netmask=255.255.255.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=10.10.31.101 //Same IP address needs to be entered when creating ports of the
 VM.
Vnic2IPv4Gateway=10.10.31.1
Vnic2IPv4Method=Static
Vnic2IPv4Netmask=255.255.255.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
```

```
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Admin user password>
dg-operPassword=<Operator user password>
```

c) config.txt ファイルを VM のホスト名や更新した VM を識別しやすい名前で保存します。

d) （**重要**） config.txt の vNIC IP アドレスとしてここで入力した IP アドレスを書き留めておいてください。手順 9 で VM のポートを作成するときに、同じ IP アドレスを指定する必要があります。

e) **手順 3**（**b**）と**手順 3**（**d**）を繰り返して、各 VM の一意の config.txt ファイルを静的アドレス指定を使用してを更新および保存します。

f) **手順 5** に進みます。

ステップ 4 **Crosswork Data Gateway VM の config.txt を DHCP を使用して更新します。**

a) Crosswork Data Gateway リリースイメージをダウンロードしたディレクトリに移動します。

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。詳細については、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ （10 ページ）を参照してください。

静的アドレス指定を使用して、ホスト名 cdg1-nodhcp で 3 つの NIC を展開する場合のサンプル config.txt ファイルを以下に示します。このリスト内の必須パラメータは強調表示されています。

（注） 展開する NIC が 1 つまたは 2 つの場合は、config.txt の ActiveVnics パラメータはそれぞれ 1 または 2 になります。

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=cdg1-nodhcp
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
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 //Leave the default value unchanged
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=DHCP
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=DHCP
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=DHCP
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Administrator user password>
dg-operPassword=<Operator user password>
```

c) `config.txt` ファイルを VM のホスト名や更新した VM を識別しやすい名前で保存します。

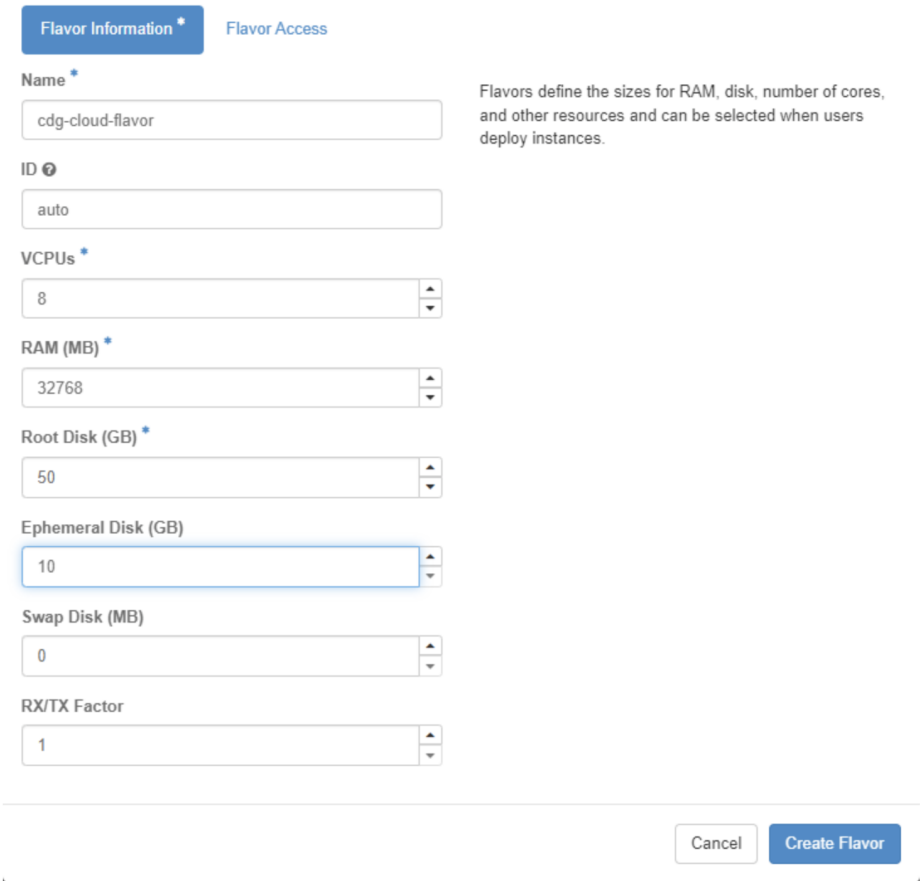
d) **手順 4（b）**と**手順 4（c）**を繰り返して、各 VM の一意の `config.txt` ファイルを静的アドレス指定を使用してを更新および保存します。

e) **手順 5** に進みます。

ステップ 5 OpenStack の UI から OpenStack VM にログインします。

ステップ 6 [コンピューティング（Compute）] > [フレーバー（Flavors）] に移動して、リソースプロファイルまたはフレーバーを作成します。

次の図に示すように、[名前（Name）]、[VCPU（VCPUs）]、[RAM]、[ルートディスク（Root Disk）]、および[エフェメラルディスク（Ephemeral Disk）] フィールドに詳細を入力し、[フレーバーの作成（Create Flavor）] をクリックします。

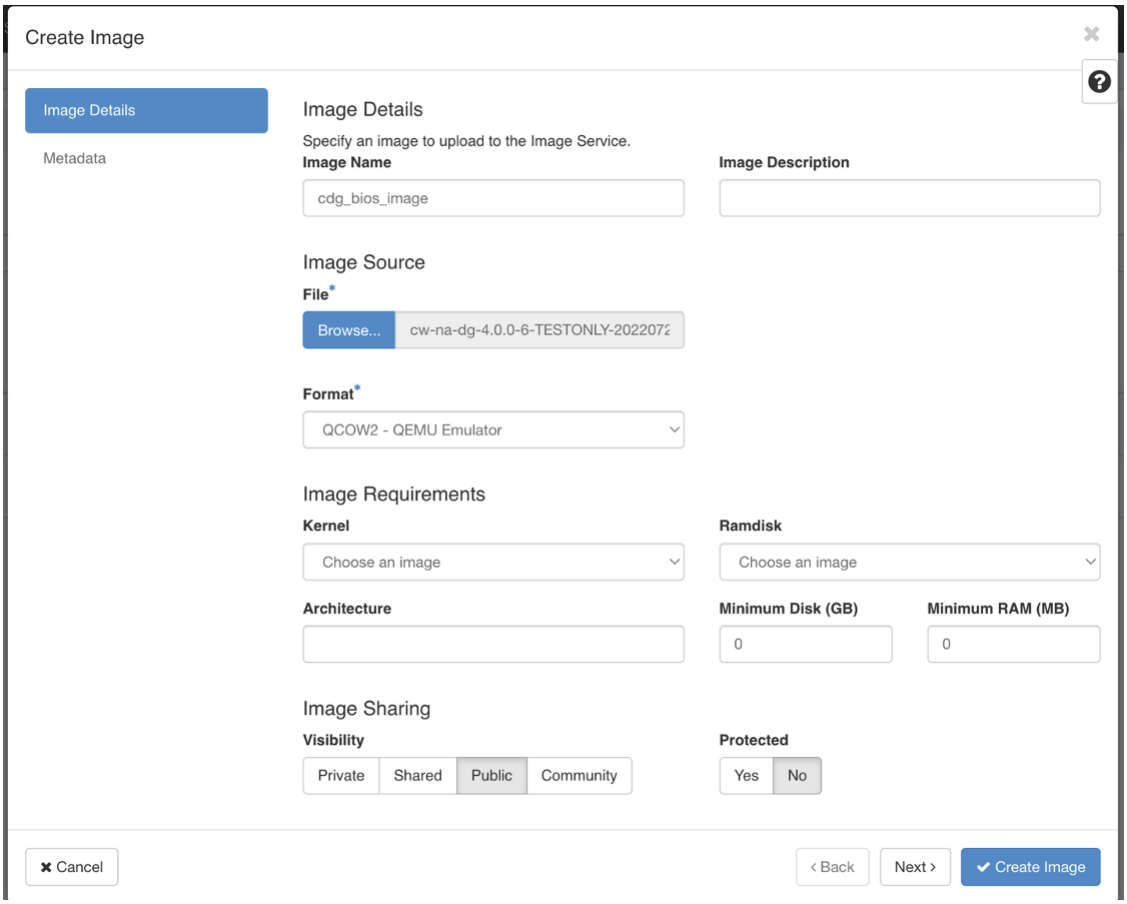


ステップ 7 **OpenStack インストール用のイメージを作成します。**

a) 次のフィールドに詳細情報を入力します。

1. [イメージ名（Image Name）]：作成するイメージの名前を指定します。
2. [ファイル（File）]：Crosswork Data Gateway リリースイメージをダウンロードしたディレクトリに移動して、イメージを選択します。
3. [フォーマット（Format）]：ドロップダウンリストから [QCOW2 - QEMUエミュレータ（QCOW2 - QEMU Emulator）] を選択します。
4. 他の設定は、図に示されている値のままにします。

b) [イメージの作成（Create Image）] をクリックします。



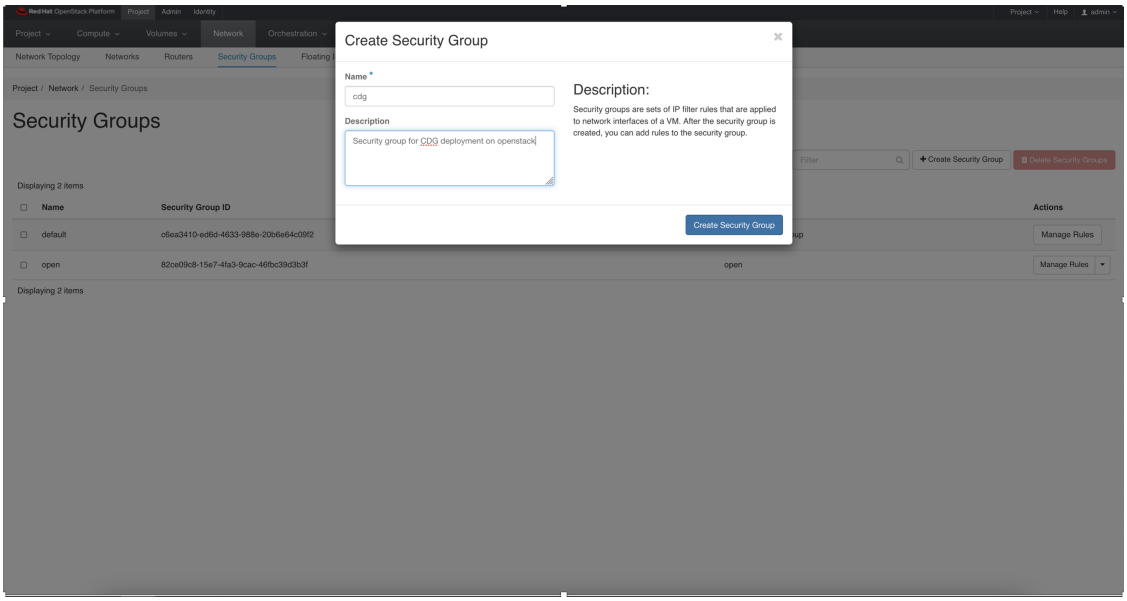
ステップ 8 **着信 TCP/UDP/ICMP 接続を許可するセキュリティポリシーを作成します。**

OpenStack は、デフォルトで着信 TCP/UDP/ICMP 接続を許可しません。TCP/UDP/ICMP プロトコルからの着信接続を許可するセキュリティポリシーを作成します。

（注） Crosswork Data Gateway を展開した後でも、セキュリティグループを作成して VM に適用できます。

a) OpenStack の UI で、[ネットワーク（Networks）] > [セキュリティグループ（Security Groups）] に移動します。。

b) [+セキュリティグループの作成（+ Create Security Group）] をクリックします。



c) セキュリティグループの名前と説明を [名前（Name）] と[説明（Description）] にそれぞれ指定します。[セキュリティグループの作成（Create Security Group）] をクリックします。

d) セキュリティルールの作成用に表示される新しいウィンドウで[ルールの追加（Add Rule）] をクリックし、方向、ポート範囲、およびIPアドレス範囲を指定して、各プロトコルのセキュリティポリシーを作成します。

セキュリティグループには、デフォルトで 2 つのルールが割り当てられています。これらのルールを削除するには、[ルールの削除（Delete Rule）] オプションを使用します。

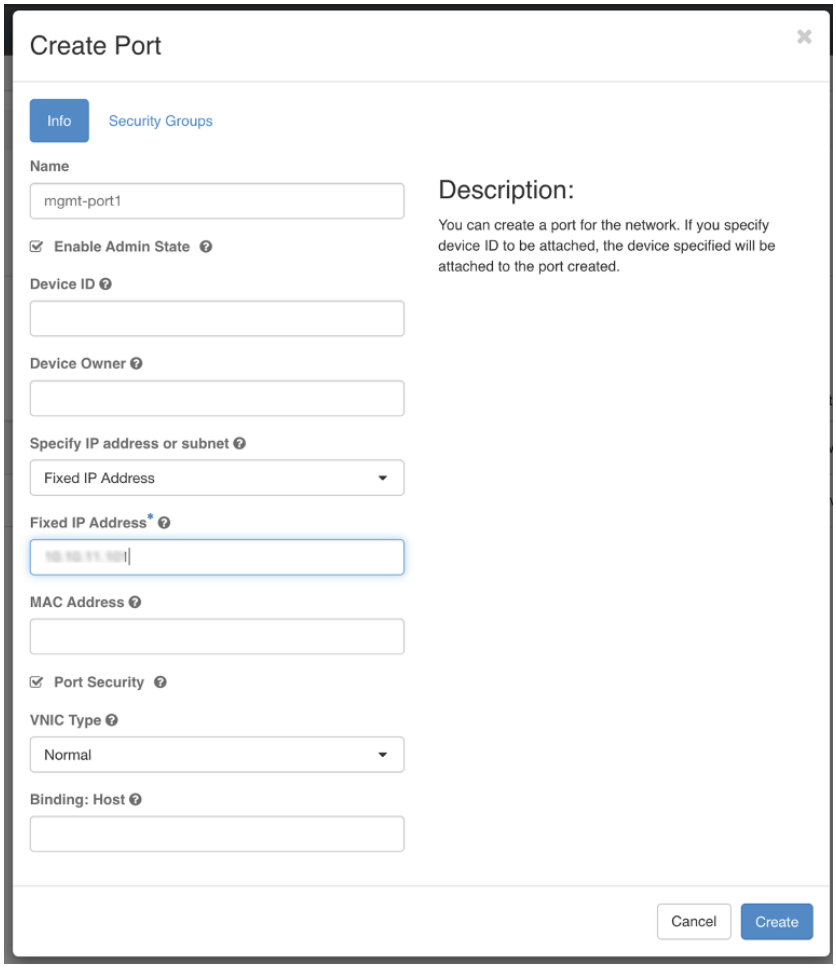
ステップ 9　静的アドレス指定を使用する場合にのみ、IP アドレスを指定してポートを作成します。

重要　この手順は、静的アドレス指定を使用する場合にのみ必要です。DHCP アドレス指定を使用する場合、ポートの IP アドレスは、サブネットの IP アドレス割り当てプールから自動的に割り当てられます。

a) OpenStack の UI で、[ネットワーク（Network）] > [ネットワーク（Networks）] に移動します。

b) 展開する NIC の数に応じて 、（管理ネットワークから順に）ネットワークを選択し、[+ポートの作成（+ Create Ports）] をクリックします。

c) [名前（Name）] および [固定IPアドレス（Fixed IP Address）] フィールドに詳細を入力します。[管理状態を有効にする（Enable Admin State）] と [ポートセキュリティ（Port Security）] チェックボックスをオンにします。

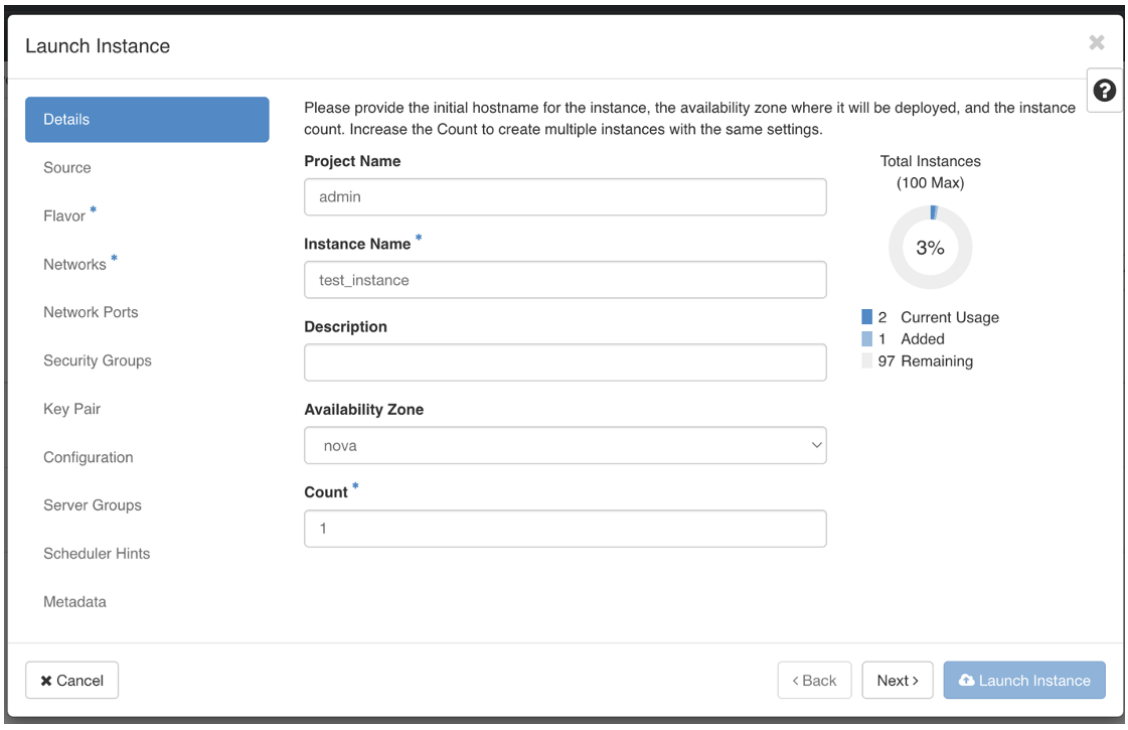


ステップ 10 [コンピューティング（Compute）]>[インスタンス（Instances）] に移動します。このページで [インスタンスの起動（Launch Instance）] をクリックします。

[インスタンスの起動（Launch Instance）] ウィンドウが表示され、VM のインストールが開始されます。

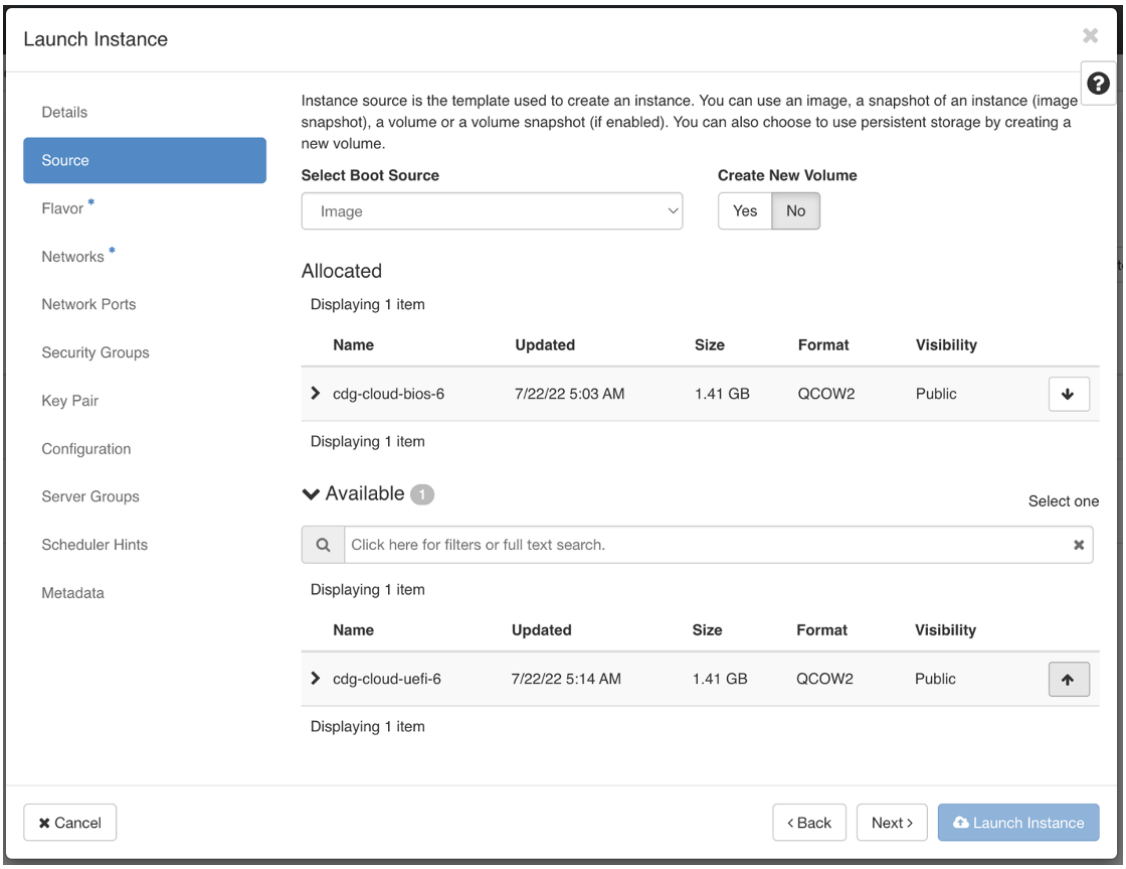
ステップ 11 [詳細（Details）] タブの [インスタンス名（Instance Name）] フィールドに VM 名を指定し、[カウント（Count）] を 1 にします。[次へ（Next）] をクリックします。

（注） 大規模なシステムでは、複数の Cisco Crosswork Data Gateway VM を使用する可能性があります。したがって、Cisco Crosswork Data Gateway の名前は一意であり、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。VM の `config.txt` ファイルの `Hostname` パラメータで指定したものと同じ名前を入力することを推奨します。

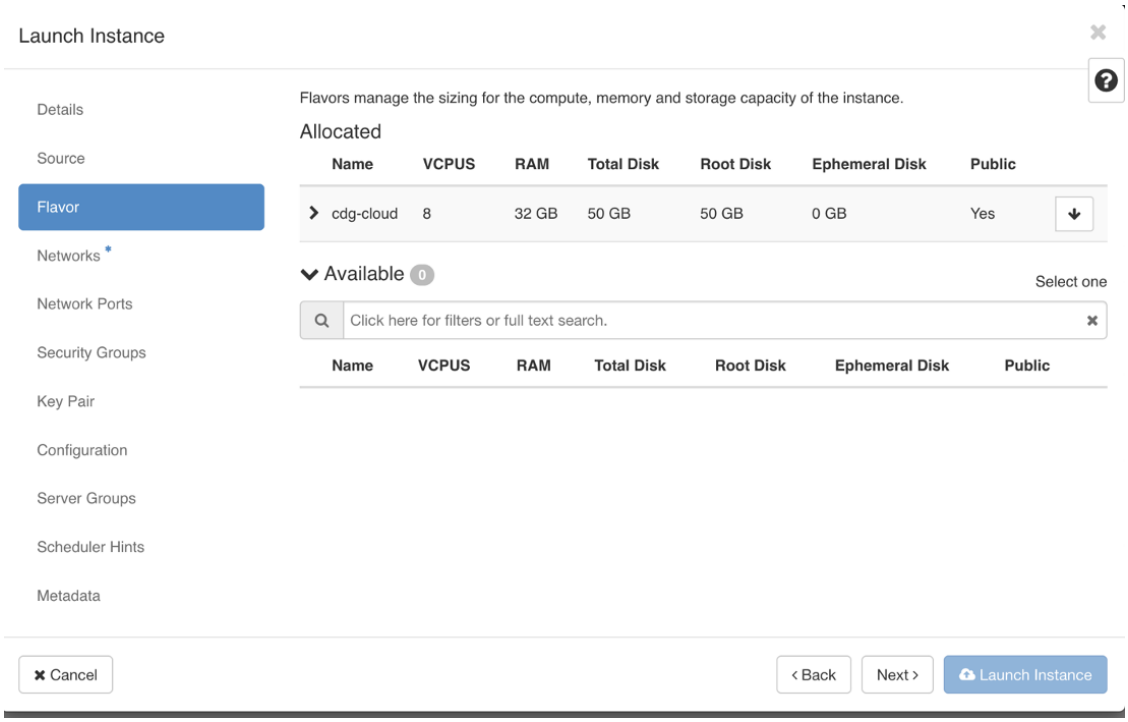


ステップ 12 [ソース（Source）] タブでは次の操作を行います。

1. [ブートソースの選択（Select Boot Source）]：ドロップダウンリストから [イメージ（Image）] を選択します。
2. 新しいボリュームの作成（Create New Volume）]：[いいえ（No）] を選択します。
3. OpenStack 環境で使用可能なすべてのイメージは、[使用可能（Available）] ペインの下に一覧表示されます。 をクリックして、イメージを選択します。これによりイメージが [割り当て済み（Allocated）] ペインに移動し、イメージを選択したことが示されます。
4. [次へ（Next）] をクリックします。

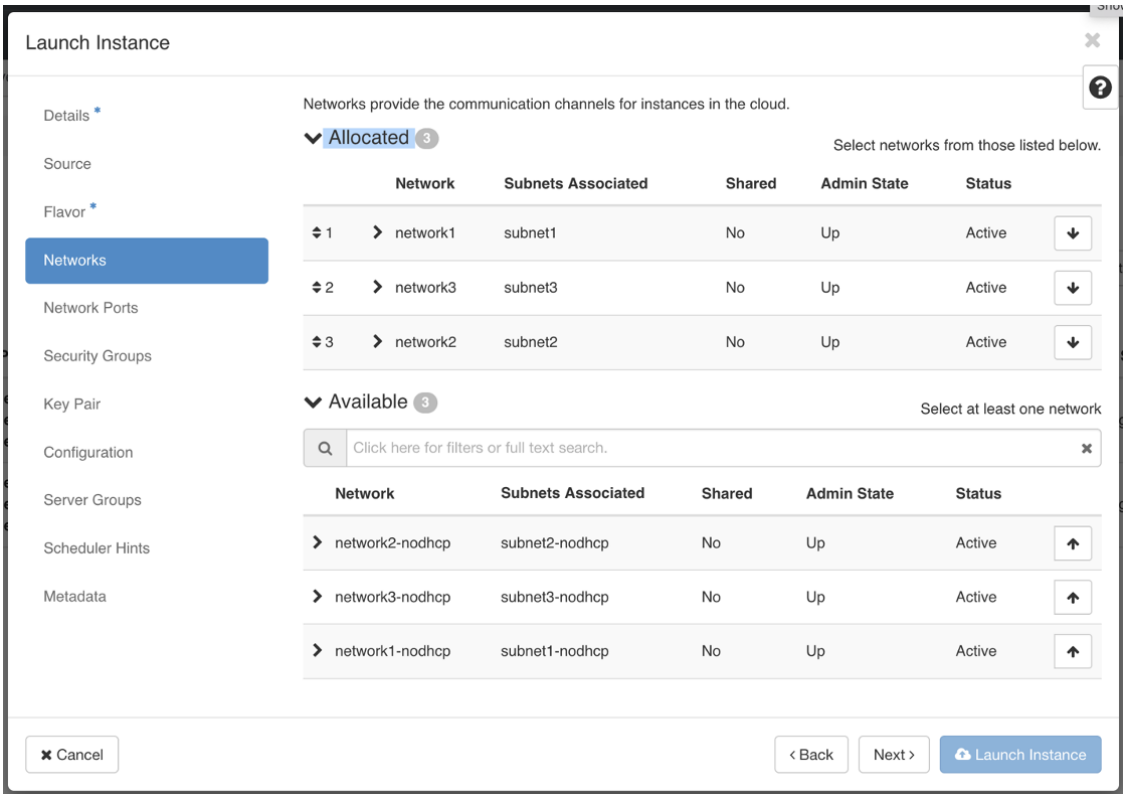


ステップ 13 [使用可能（Available）] ペインの [フレーバー（Flavor）] タブで 、VM に選択するフレーバーについて  クリックし、[使用可能（Available）] ペインから [割り当て済み（Allocated）] ペインに移動します。[次へ（Next）] をクリックします。



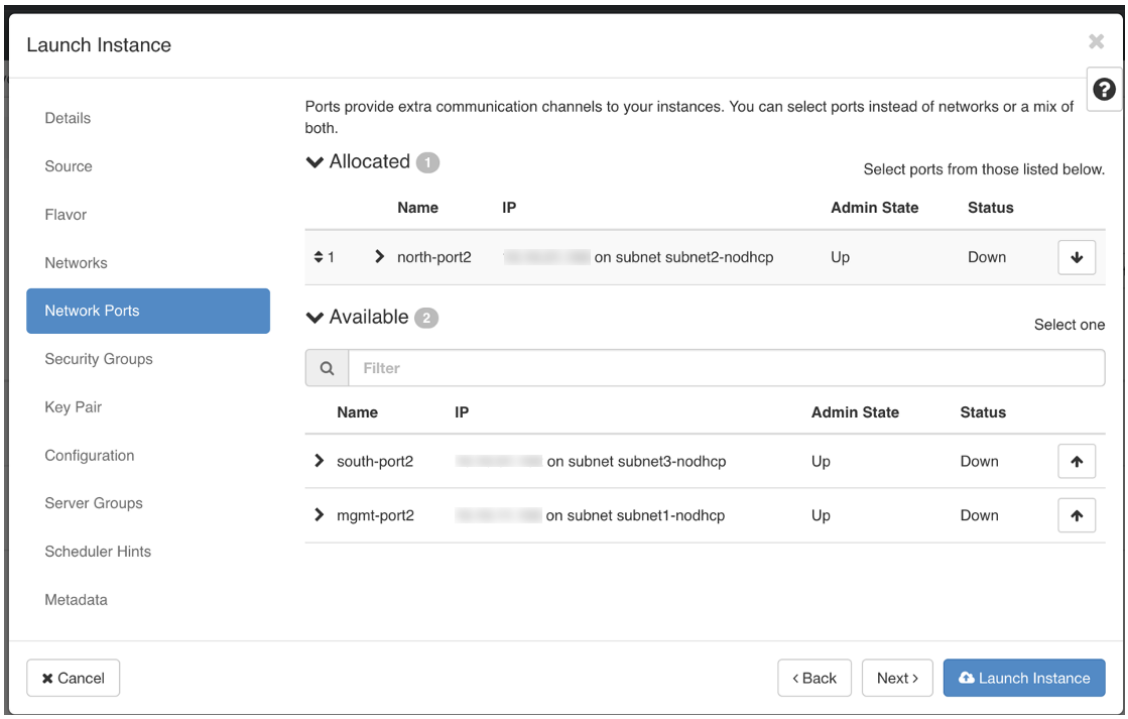
ステップ 14 VM にネットワークを割り当てます。展開する vNIC の数に応じて、[使用可能（Available）] ペインのネットワークのリストから各ネットワークで をクリックして、VM に最大 3 つのネットワークを選択します。これにより、選択したネットワークが [割り当て済み（Allocated）] ペインに移動します。[次へ（Next）] をクリックします。

重要 ネットワークを選択する順序は重要です。NIC を 3 つ展開する場合、最初に選択したネットワークが vNIC0 インターフェイスに、2 番目が vNIC1 インターフェイスに、3 番目が vNIC2 インターフェイスに割り当てられます。



ステップ 15 ポートを VM に割り当てます。

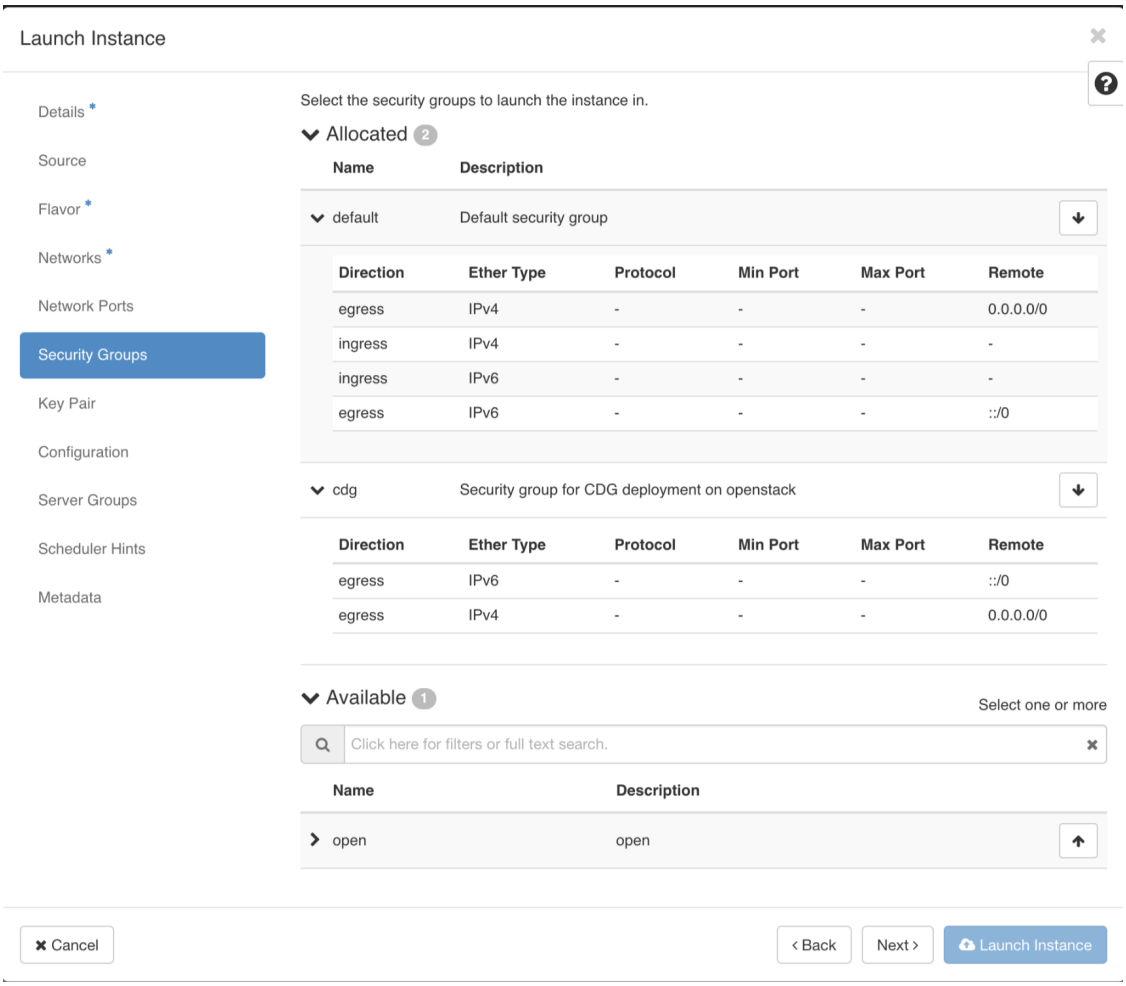
[使用可能（Available）]ペインに表示されているポートのリストから、 をクリックしてポートを[割り当て済み（Allocated）]ペインに移動します。.



[Next] をクリックします。

ステップ 16 VM に適用するセキュリティグループを [使用可能（Available）] ペインから [割り当て済み（Allocated）] ペインに移動して、**セキュリティグループ**を VM に割り当てます。。

次の図では、2 つのセキュリティグループ（default と cdg）が VM に適用されています。

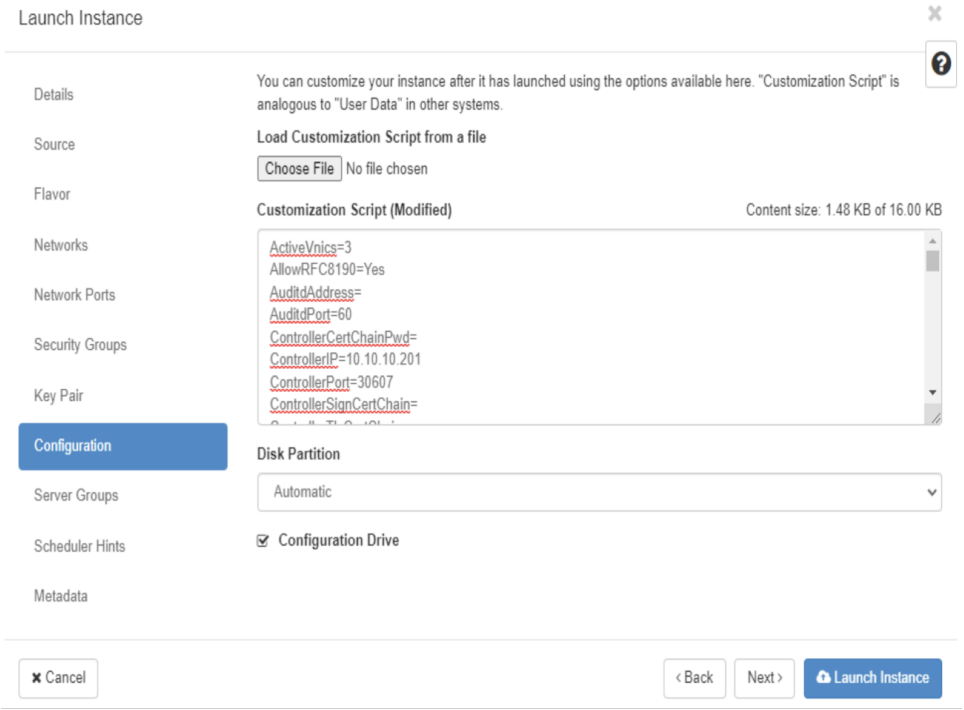


[次へ（Next）] をクリックします。

ステップ 17 [キーペア（Key Pair）] タブで、[次へ（Next）] をクリックします。

ステップ 18 [設定（Configuration）] タブでは次の操作を行います。

- [ファイルの選択（Choose File）] をクリックして、VM 用に変更して保存した `config.txt` ファイルを選択してアップロードします。
- [設定ドライブ（Configuration Drive）] チェックボックスをオンにします。



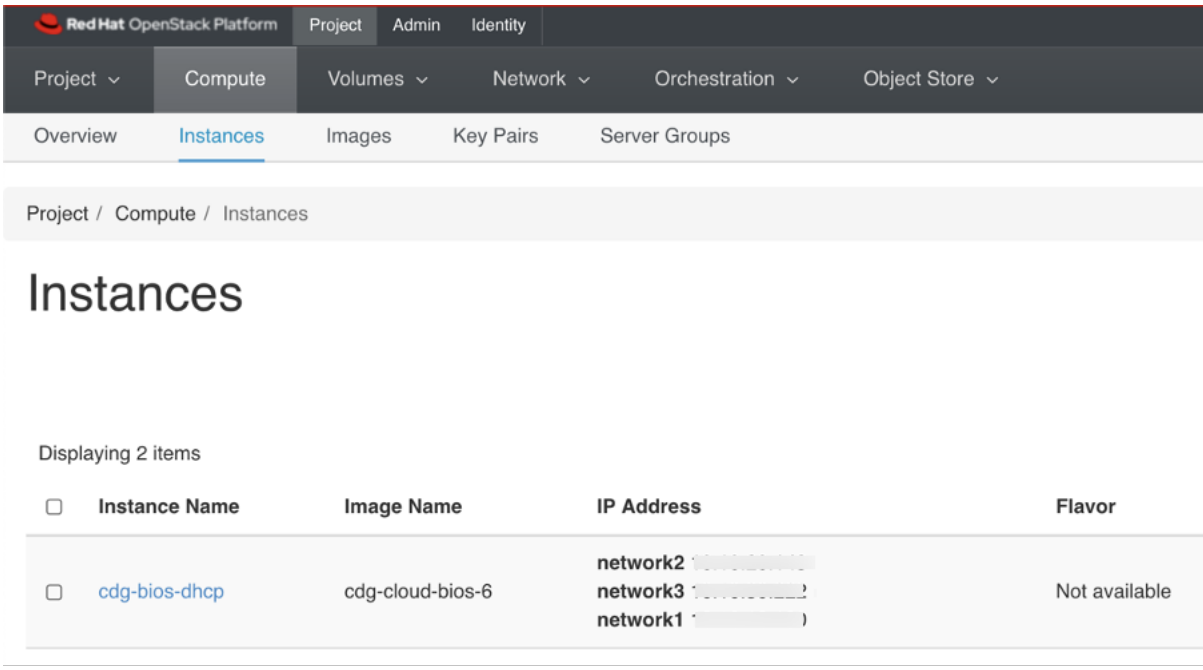
ステップ 19 [インスタンスの起動（Launch Instance）] をクリックします。

OpenStack で VM のインストールが開始されます。

ステップ 20 **手順 9** から**手順 20** を繰り返して、すべての Crosswork Data Gateway VM をインストールします。

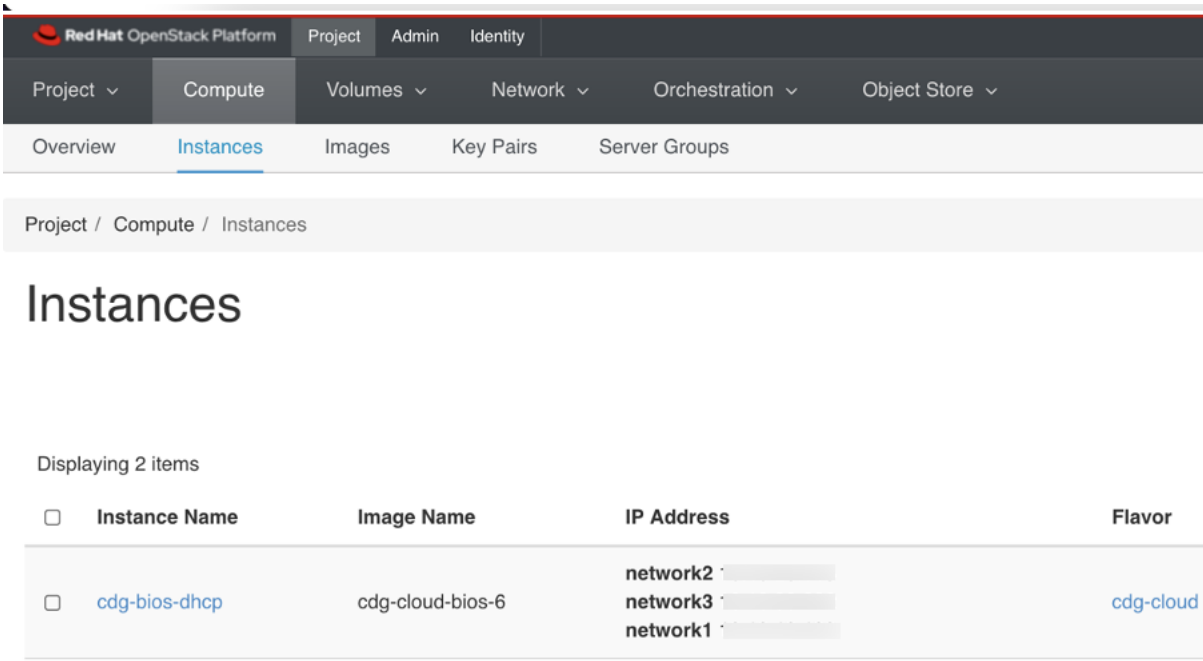
Crosswork Data Gateway VM が正常にインストールされたことを確認します。

1. OpenStack の UI で [コンピューティング（Compute）] > [インスタンス（Instances）] に移動します。
2. インストール済みおよびインストール中の Crosswork Data Gateway VM のリストがここに表示されます。



インストール中の Crosswork Data Gateway VM の [ステータス（Status）] は [ビルド（Build）]、[タスク（Task）] は [生成（Spawning）]、[電源の状態（Power State）] は [状態なし（No State）] になります。

3. VM が正常にインストールされると、[ステータス（Status）] は [アクティブ（Active）] に変わります。また、[タスク（Task）] は [なし（None）]、[電源状態（Power State）] は [稼働中（Running）] になります。



4. [ステータス（Status）] が [アクティブ（Active）] に変わったら、約 10 分間待ちます。

Crosswork Data Gateway の VM 名をクリックします。VM コンソールへのリンクが開きます。

5. dg-admin ユーザーまたは dg-oper ユーザー（割り当てられたロールに応じて）のアカウントと、VM の `config.txt` ファイルに入力した対応するパスワードを使用してログインします。正常にログインすると、Crosswork Data Gateway のインタラクティブコンソールが表示されます。

次のタスク

登録パッケージを生成およびエクスポートして、Crosswork Cloud に Crosswork Data Gateway を登録します。登録パッケージのエクスポート （62 ページ） を参照してください。

登録パッケージの生成

それぞれの Crosswork Data Gateway は、不変の識別子によって識別する必要があります。そのためには、登録パッケージの生成が必要です。登録パッケージは、次のいずれかの方法で生成できます。

- インストールプロセス中に**自動登録パッケージ**パラメータを指定する（「表 4 : Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） 導入パラメータとシナリオ」の「自動登録パッケージ」を参照）。
- インタラクティブコンソールの [登録パッケージのエクスポート（Export Enrollment Package）] オプションを使用する（登録パッケージのエクスポート （62 ページ）を参照）。

登録パッケージは、インストール時にユーザが入力した OVF テンプレートから取得した情報で作成された JSON ドキュメントです。証明書、Crosswork Data Gateway の UUID、メタデータ（Crosswork Data Gateway の名前、作成時間、バージョン情報など）など、登録に必要な Crosswork Data Gateway に関するすべての情報が含まれます。

インストール時に登録パッケージをエクスポートしないことを選択した場合は、Crosswork Data Gateway を Crosswork Cloud に登録する前にエクスポートする必要があります。手順については、登録パッケージのエクスポート （62 ページ） を参照してください。

（注） 登録パッケージは、各 Crosswork Data Gateway で固有です。

登録パッケージ JSON のサンプルを次に示します。

```
{
  "name": "dg116.cisco.com",
  "description": "CDG Base VM for Automation",
  "profile": {
    "cpu": 8,
    "memory": 31,
    "nics": 3
  },
```

```
  "interfaces": [
    {
      "name": "eth0",
      "mac": "00:50:56:9e:09:7a",
      "ipv4Address": "<ip_address>/24"
    },
    {
      "name": "eth1",
      "mac": "00:50:56:9e:67:c3",
      "ipv4Address": "<ip_address>/16"
    },
    {
      "name": "eth2",
      "mac": "00:50:56:9e:83:83",
      "ipv4Address": "<ip_address>/16"
    }
  ],
  "certChain": [
    "<cert_chain>"
  ],
  "version": "1.1.0 (branch dg110dev - build number 152)",
  "duuid": "d58fe482-fdca-468b-a7ad-dfbfa916e58b"
}
```

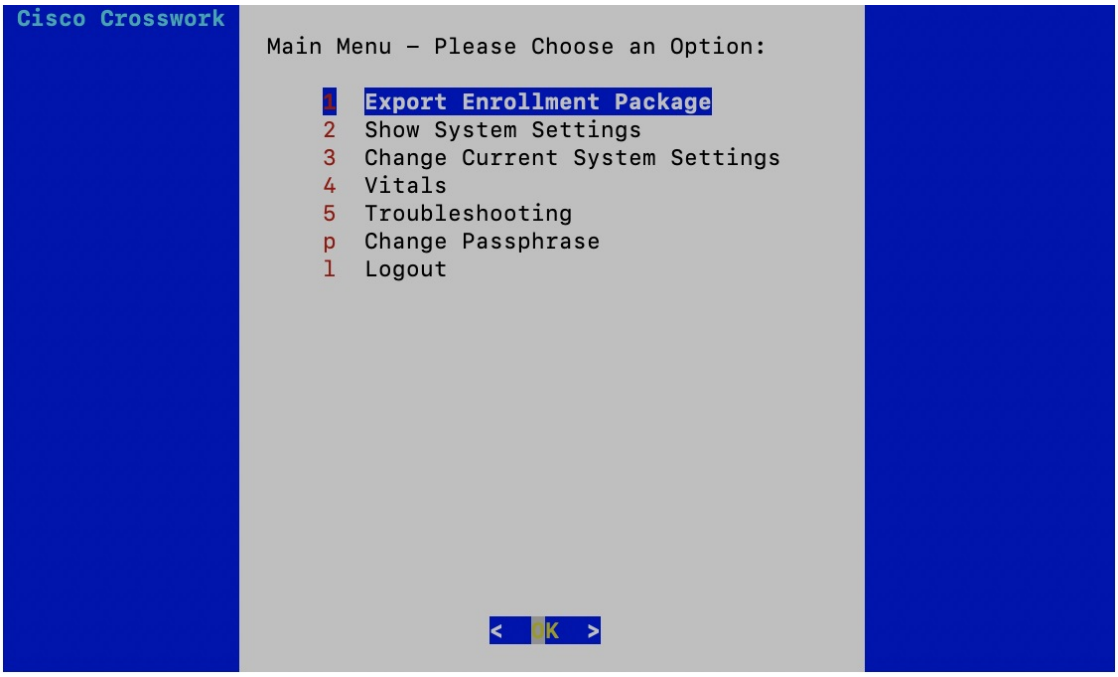
登録パッケージのエクスポート

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）を Crosswork Cloud に登録するには、ローカルコンピュータに登録パッケージのコピーが必要です。

（注） インストール時に**自動登録パッケージ転送**設定を指定していない場合のみ、コピーが必要になります。指定している場合、ファイルは VM の起動後に選択した SCP URI の宛先にコピーされます。インストール時に**自動登録パッケージ転送**を設定した場合のみ、Crosswork Cloud アプリケーションを使用した Crosswork Data Gateway の登録 （64 ページ） に進みます。

ステップ 1 Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） にログインします。

ステップ 2 メインメニューから [1 登録パッケージのエクスポート（1 Export Enrollment Package）] を選択し、[OK] をクリックします。



ステップ 3 登録パッケージをエクスポートするための SCP URI を入力し、[OK] をクリックします。

（注）
- ホストは SCP サーバを実行する必要があります。理想的には、Crosswork サーバへのアクセスに使用するローカルコンピュータに登録パッケージをエクスポートする必要があります。
- デフォルトのポート 22 を使用していない場合は、SCP コマンドの一部としてポートを指定できます。たとえば、登録パッケージを管理者ユーザとしてエクスポートし、そのユーザのホームディレクトリにポート 4000 でファイルを配置するには、次のコマンドを実行します。

  ```
  scp -P4000 admin@<ip_address>:/home/admin
  ```

- 登録ファイルは一意の名前で作成されます。例：9208b9bc-b941-4ae9-b1a2-765429766f27.json

ステップ 4 SCP パスフレーズ（SCP ユーザパスワード）を入力し、[OK] をクリックします。

ステップ 5 登録パッケージをローカルコンピュータに直接コピーできなかった場合は、SCP サーバからローカルコンピュータに登録パッケージを手動でコピーします。

次のタスク

「Crosswork Cloud アプリケーションを使用した Crosswork Data Gateway の登録（64 ページ）」の説明に従い、Crosswork Cloud への Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の登録に進みます。

Crosswork Cloud アプリケーションを使用した Crosswork Data Gateway の登録

Crosswork Data Gateway の .json 登録ファイルには、 Crosswork Cloud に Crosswork Data Gateway を登録する際に使用される一意のデジタル証明書が含まれています。以下の説明に従い、Crosswork Cloud にその情報を追加します。

（注） Crosswork Data Gateway の出力トラフィックでファイアウォールを使用する場合は、ファイアウォールの設定で cdg.crosswork.cisco.com および crosswork.cisco.com が許可されていることを確認します。

ステップ 1 Crosswork Cloud にログインします。

ステップ 2 メインウィンドウで、[設定（Configure）] > [データゲートウェイ（Data Gateways）] の順にクリックしてから、[追加（Add）] をクリックします。

ステップ 3 [登録（Registration File）] をクリックして、Crosswork Data Gateway からダウンロードした登録データファイルをアップロードし、.json ファイルの場所に移動してから、[次へ（Next）] をクリックします。

ステップ 4 Cisco Crosswork Data Gateway の名前を入力します。

ステップ 5 [アプリケーション（Application）] フィールドで、この Crosswork Data Gateway インスタンスを使用している Crosswork Cloud アプリケーションを選択します。各 Crosswork Data Gateway は、1 つの Crosswork Cloud アプリケーションにのみ適用できます。

ステップ 6 残りの必須フィールドに入力してから、[次へ（Next）] をクリックします。

ステップ 7 （オプション）タグ名を入力します。これにより、同じタグを持つ Crosswork Data Gateway をグループ化できます。その後、[次へ（Next）] をクリックします。

ステップ 8 入力した Crosswork Data Gateway の情報を確認してから、[次へ（Next）] をクリックします。

ステップ 9 [承認（Accept）] をクリックして、セキュリティ証明書を受け入れます。

Crosswork Data Gateway の追加に成功したことを示すメッセージが表示されます。

次のタスク

この手順を繰り返して、ネットワーク内のすべての Crosswork Data Gateway を Crosswork Cloud に登録します。

Crosswork Data Gateway が正常に接続されたことを確認するには、[データゲートウェイ（Data Gateways）] をクリックしてから、Crosswork Data Gateway の名前をクリックし、追加した Crosswork Data Gateway に関する次の値を確認します。

- [セッションアップ（Session Up）] : [アクティブ（Active）]

• [接続（Connectivity）]：[セッションアップ（Session Up）]

Crosswork Data Gateway が Crosswork Cloud サービスに正常に接続されていない場合は、「Crosswork Data Gateway 接続のトラブルシュート （65 ページ）」の項を参照してください。

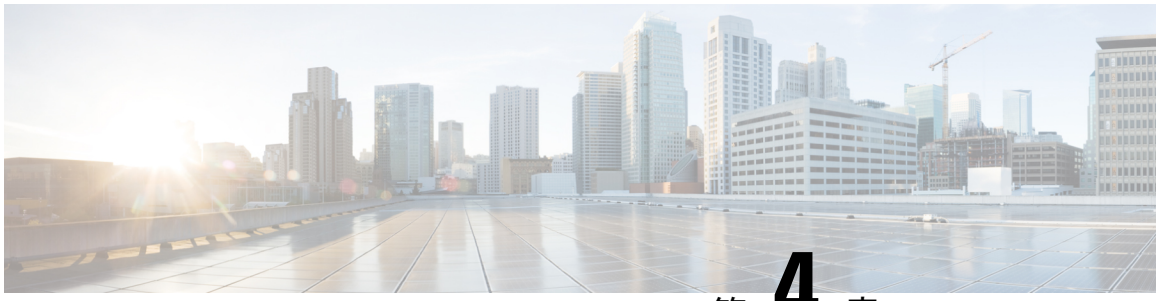
Crosswork Data Gateway 接続のトラブルシュート

次の表では、Crosswork Data Gateway を Crosswork Cloud アプリケーションに接続する際に発生する可能性のある一般的な問題を列挙し、問題の原因を特定して解決するためのアプローチを示します。

表 *5 : Crosswork Data Gateway* 接続のトラブルシューティング

問題	操作
NTP の問題により Crosswork Data Gateway を Cisco Crosswork Cloud 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。	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 ログ（`/cdg/logs/components/controller-gateway/session.log` にある `session.log` ファイル）でエラーが表示された場合、 `UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid` Crosswork Data Gateway と Cisco Crosswork Cloud 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 Cloud サーバーのクロック時刻と同期するように NTP を設定し、Crosswork Cloud に対して Crosswork Data Gateway の登録を再度試みます。

問題	操作
Crosswork Data Gateway は、外部 Web サービスに直接接続されません。	1. お使いの環境にプロキシサーバーがない場合は、プロキシサーバーを設定します。 2. プロキシサーバーが環境内に既に存在する場合は、プロキシの URL が正しいかどうかを確認します。 3. プロキシのクレデンシャル（証明書、プロキシ名など）が正しいかどうかを確認します。 Crosswork Data Gateway のプロキシサーバーの詳細を更新するには、「制御プロキシの設定（75 ページ）」を参照してください。



第 4 章

Crosswork Data Gateway VM の設定

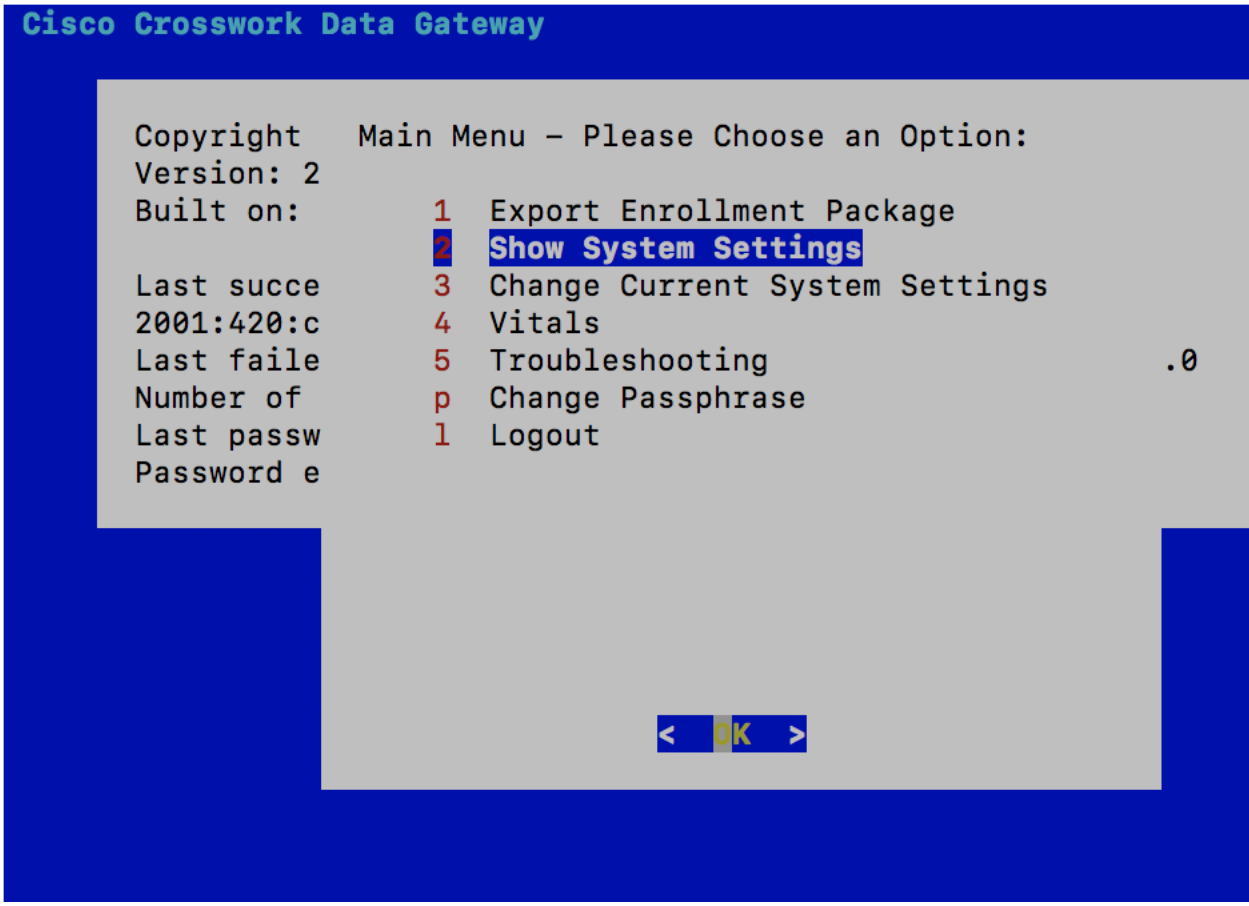
Cisco Crosswork Data Gateway インスタンスは、スタンドアロン VM として作成されており、コントローラ アプリケーションとは別の場所に配置することができます（コントローラ アプリケーションは、Crosswork Cloud です）。この VM は、ネットワークからのデータ収集を可能にするコントローラ アプリケーションに接続できます。

この章は次のトピックで構成されています。

インタラクティブなコンソールの使用

Cisco Crosswork Data Gateway は、ログインに成功するとインタラクティブコンソールを起動します。次の図に示すように、インタラクティブコンソールにメインメニューが表示されます。

（注） ここに示すメインメニューは、**dg-admin** ユーザに対応しています。オペレータには管理者と同じ権限はないため、**dg-oper** ユーザーの場合とは異なります。表 6 : 各ロールの権限 （69 ページ） を参照してください。



メインメニューには、次のオプションが表示されます。

1. 登録パッケージのエクスポート

2. システム設定の表示

3. 現在のシステム設定の変更

4. バイタル

5. トラブルシューティング

p. パスフレーズの変更

l. ログアウト

Crosswork Data Gateway ユーザーの管理

ここでは、次の内容について説明します。

- サポートされるユーザ ロール （69 ページ）
- パスワードの変更 （71 ページ）

サポートされるユーザ ロール

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） は次のユーザロールを持つ 2 ユーザのみをサポートしています。

- **管理者**：Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） が初めて起動されたときに、管理者ロールを持つ 1 人のデフォルトの **dg-admin** ユーザが作成されます。このユーザーは削除できず、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の VM の起動やシャットダウン、アプリケーションの登録、認証証明書の適用、サーバー設定の構成、カーネルアップグレードの実行などの読み取りと書き込みの両方の権限が設定されています。
- **オペレータ**：VM の最初の起動時に、デフォルトで **dg-oper** ユーザも作成されます。このユーザーは、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の正常性を確認し、エラーログを取得し、エラー通知を受信し、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） インスタンスと出力の接続先間との接続テストを実行できます。

（注）
- ユーザーク レデンシャルは、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のインストール時に両方のユーザーアカウントに設定されます。
- ユーザはローカル認証されています。

次の表に、各ロールで使用できる権限を示します。

表 *6 :* 各ロールの権限

権限	管理者	オペレータ
登録パッケージのエクスポート	✓	✓
システム設定の表示		
vNIC アドレス NTP DNS プロキシ UUID Syslog 証明書 ファースト ブート プロビジョニング ログ タイムゾーン	✓	✓

権限	管理者	オペレータ
現在のシステム設定の変更		
NTP の設定 DNS の設定 制御プロキシの設定 スタティックルートの設定 Syslog の設定 新しい SSH キーの作成 証明書のインポート vNIC2 MTU の設定 タイムゾーンの設定 パスワード要件の設定 同時ログイン数の制限の設定 アイドルタイムアウトの設定	✓	×
バイタル		
Docker コンテナ Docker イメージ コントローラの到達可能性 NTP の到達可能性 ルート テーブル ARP テーブル ネットワーク接続 ディスク領域使用率 Linux サービス NTP ステータス システム稼動時間	✓	✓
トラブルシューティング		

権限	管理者	オペレータ
診断コマンドの実行	✓	✓
show-tech の実行	✓	✓
auditd ログのエクスポート	✓	✓
TAC シェルアクセスの有効化	✓	×
パスフレーズの変更	✓	✓

パスワードの変更

管理者ユーザとオペレータユーザの両方が自分のパスフレーズを変更できますが、相互に変更を行うことはできません。

自分のパスフレーズを変更するには、次の手順を実行します。

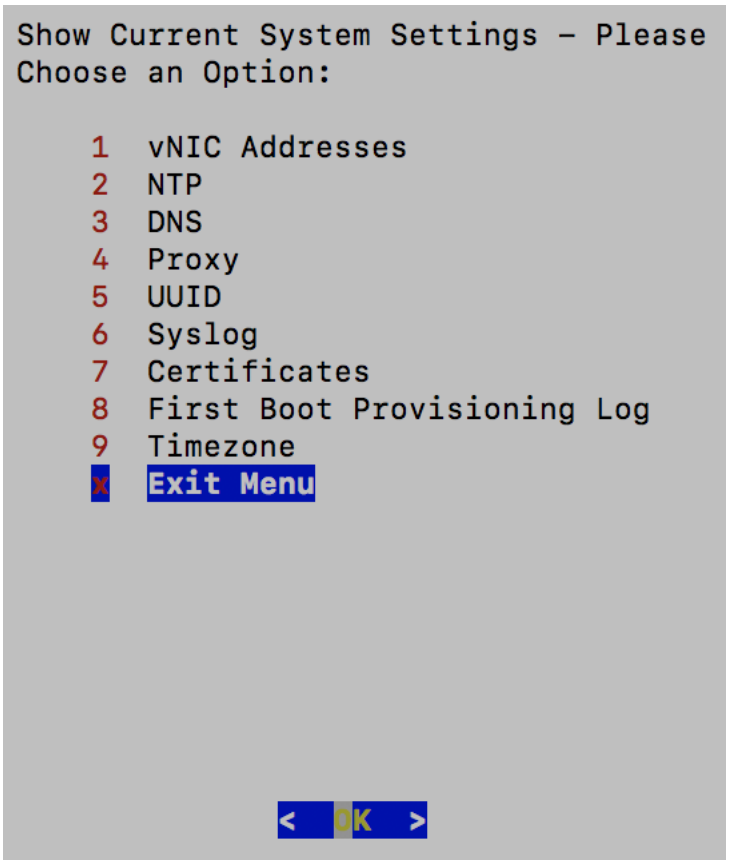
ステップ 1 メインメニューから、[パスフレーズの変更（Change Passphrase）] を選択し、[OK] をクリックします。

ステップ 2 現在のパスワードを入力し、[Enter] キーを押します。

ステップ 3 新しいパスワードを入力し、[Enter] キーを押します。パスワードをもう一度入力して、[Enter] キーを押します。

現在のシステム設定の表示

Crosswork Data Gateway では、次の設定を表示できます。



現在のシステム設定を表示するには、次の手順を実行します。

ステップ 1 次の図に示すように、メインメニューから [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 [OK] をクリックします。[現在のシステム設定の表示（Show Current System Settings）] メニューが開きます。

ステップ 3 表示する設定を選択します。

設定オプション	説明
[1 vNICアドレス（1 vNIC Addresses）]	アドレス情報を含む、vNIC 設定を表示します。
[2 NTP]	現在設定されている NTP サーバの詳細を表示します。
[3 DNS]	DNS サーバの詳細を表示します。
[4 プロキシ（4 Proxy）]	プロキシサーバの詳細を表示します（設定されている場合）。
[5 UUID]	システム UUID を表示します。

設定オプション	説明
[6 Syslog]	Syslog の転送設定を表示します。Syslog の転送が設定されていない場合は、画面に「# Forwarding configuration follows」と表示されます。
[7 証明書（7 Certificates）]	次の証明書ファイルを表示するオプションがあります。 • Crosswork Data Gateway 署名証明書ファイル • コントローラ署名証明書ファイル • コントローラの SSL/TLS 証明書ファイル • Syslog 証明書ファイル • コレクタ証明書ファイル
[8 ファーストブートプロビジョニングログ（8 First Boot Provisioning Log）]	最初のブートログファイルの内容を表示します。
[9 タイムゾーン（9 Timezone）]	現在の時間帯設定を表示します。

現在のシステム設定の変更

Crosswork Data Gateway では、次の設定を行います。

- NTP。
- DNS 用です。
- 制御プロキシ。
- スタティック ルート
- Syslog。
- SSH キー。
- 証明書。
- vNIC2 MTU。
- タイムゾーン。
- パスワード要件。
- 同時ログイン制限。

- Idle timeout.
- auditd を設定します。

（注）

- Crosswork Data Gateway システム設定は管理者のみが設定できます。
- SCP を使用する必要がある設定オプションで、SCP 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。

NTP の設定

NTP 時刻は、コントローラ アプリケーションおよびそのCrosswork Data Gatewayインスタンスと同期することが重要です。同期しないと、セッションハンドシェイクが行われず、機能イメージはダウンロードされません。その場合、「clock time not match and sync failed」というエラーメッセージが controller-gateway.log に記録されます。ログファイルにアクセスするには、show-tech の実行 （87 ページ） を参照してください。メインメニューの [バイタル（Vitals）] から [コントローラの到達可能性（Controller Reachability）] および [NTP到達可能性（NTP Reachability）] オプションを使用して、Crosswork Data Gateway と同様にコントローラ アプリケーションの NTP の到達可能性を確認できます。（「Crosswork Data Gateway のバイタルの表示 （82 ページ）」を参照）。NTP が正しく設定されていないと、「Session not established」というエラーが表示されます。

キーファイルによる認証を使用するように Crosswork Data Gateway を設定する場合、chrony.keys ファイルはhttps://chrony.tuxfamily.org/doc/3.5/chrony.conf.html#keyfile に記載されている特定の方法でフォーマットする必要があります。ntpd を使用しており、ntp.keys ファイルを使用するように設定されているサイトでは、ツール https://github.com/mlichvar/ntp2chrony/blob/master/ntp2chrony/ntp2chrony.py を使用して、ntp.keys から chrony.keys に変換できます。ツールは ntpd 設定を chrony 互換形式に変換しますが、キーファイルのみをCrosswork Data Gatewayにインポートする必要があります。

NTP 設定を構成するには、次の手順に従ってください。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[1 NTPの設定（1 Configure NTP）] を選択します。

ステップ 2 次のように新しい NTP サーバの詳細を入力します。

- サーバリスト、スペース区切り
- NTP 認証を使用するかどうか
- キーリスト、スペース区切り。サーバリストと数が一致する必要がある

- VM への SCP へのキーファイル URI
- VM への SCP へのキーファイルパスフレーズ

ステップ 3 設定を保存するには [**OK**] をクリックします。

DNS の設定

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[2 DNSの設定（2 Configure DNS）] を選択し、[OK] をクリックします。

ステップ 2 新しい DNS サーバアドレスとドメインを入力します。

ステップ 3 設定を保存するには [**OK**] をクリックします。

制御プロキシの設定

インストール時にプロキシサーバを設定していない場合は、このオプションを使用してプロキシサーバを設定します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[3 制御プロキシの設定（3 Configure Control Proxy）] を選択し、[OK] をクリックします。

ステップ 2 続行する場合は、次のダイアログで [はい（Yes）] をクリックします。続行しない場合は、[キャンセル（Cancel）] をクリックします。

ステップ 3 次のように新しいプロキシサーバの詳細を入力します。

- サーバ URL
- バイパスアドレス
- プロキシ ユーザ名
- プロキシパスフレーズ

ステップ 4 設定を保存するには [**OK**] をクリックします。

スタティックルートの設定

スタティックルートは、Crosswork Data Gateway がコレクタから追加/削除要求を受信したときに設定されます。メインメニューの [スタティックルートの設定（Configure Static Routes）] オプションは、トラブルシューティングに使用できます。

（注） このオプションを使用して設定されたスタティックルートは、Crosswork Data Gateway のリブート時に失われます。

スタティック ルートの追加

スタティックルートを追加するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[4 スタティックルートの設定（4 Configure Static Routes）] を選択します。
ステップ 2 スタティックルートを追加するには、[追加（Add）] を選択します。
ステップ 3 スタティックルートを追加するインターフェイスを選択します。
ステップ 4 IP バージョンを選択します。
ステップ 5 プロンプトが表示されたら、CIDR 形式で IPv4 または IPv6 サブネットを入力します。
ステップ 6 設定を保存するには [**OK**] をクリックします。

スタティック ルートの削除

スタティックルートを削除するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[4 スタティックルートの設定（4 Configure Static Routes）] を選択します。
ステップ 2 スタティックルートを削除するには、[削除（Delete）] を選択します。
ステップ 3 スタティックルートを削除するインターフェイスを選択します。
ステップ 4 IP バージョンを選択します。
ステップ 5 CIDR 形式で IPv4 または IPv6 サブネットを入力します。
ステップ 6 設定を保存するには [**OK**] をクリックします。

Syslog の設定

（注） 複数の Linux ディストリビューションで IPv4 または IPv6 をサポートするように Syslog サーバーを設定する場合は、システム管理者ガイドおよび設定ガイドを参照してください。

次の手順に従い、Syslog を設定します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[5 Syslogの設定（5 Configure Syslog）] を選択します。

ステップ 2 次の syslog 属性の新しい値を入力します。

- [サーバアドレス（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。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。
- [ポート（Port）]：syslog サーバのポート番号。
- [プロトコル（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?（Use Syslog over TLS?）]：TLS を使用して syslog トラフィックを暗号化します。
- [TLSピア名（TLS Peer Name）]：サーバ証明書の SubjectAltName またはサブジェクト共通名に入力されたとおりの Syslog サーバのホスト名。
- [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。

ステップ 3 設定を保存するには [**OK**] をクリックします。

新しい SSH キーの作成

新しい SSH キーを作成すると、現在のキーが削除されます。

次の手順に従って、新しい SSH キーを作成します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[6 新しいSSHキーの作成（6 Create new SSH keys）] を選択します。

ステップ 2 [OK] をクリックします。Crosswork Data Gateway は、新しい SSH キーを生成する自動設定プロセスを開始します。

証明書のインポート

コントローラ署名証明書以外の証明書を更新すると、コレクタが再起動します。

Crosswork Data Gateway では、次の証明書をインポートすることができます。

- コントローラ署名証明書ファイル

- コントローラの SSL/TLS 証明書ファイル
- Syslog 証明書ファイル
- プロキシ証明書ファイル

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[7 証明書のインポート（7 Import Certificate）] を選択します。

ステップ 2 インポートする証明書を選択します。

ステップ 3 選択した証明書ファイルの SCP URI を入力します。

ステップ 4 SCP URI のパスフレーズを入力し、[OK] をクリックします。

vNIC2 MTU の設定

3 つの NIC を使用している場合にのみ、vNIC2 MTU を変更できます。

インターフェイスがジャンボフレームをサポートしている場合、MTU 値の範囲は 60 ー 9000 です。ジャンボフレームをサポートしないインターフェイスの場合、有効な範囲は 60 ー 1500 です。無効な MTU を設定すると、Crosswork Data Gateway は変更を現在設定されている値に戻します。有効な範囲を確認するには、ハードウェアのマニュアルを参照してください。エラーは、showtech の実行後に表示される MTU 変更エラーの kern.log に記録されます。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[8 vNIC1 MTUの設定（8 Configure vNIC1 MTU）] を選択します。

ステップ 2 vNIC2 MTU 値を入力します。

ステップ 3 設定を保存するには [**OK**] をクリックします。

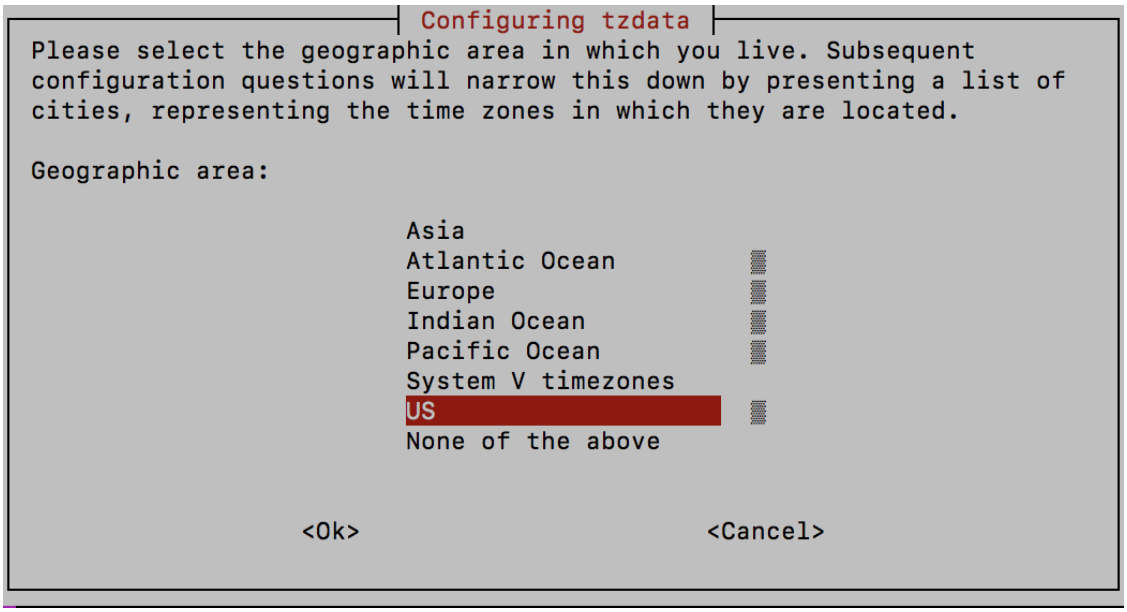
Crosswork Data Gateway VM のタイムゾーンの設定

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

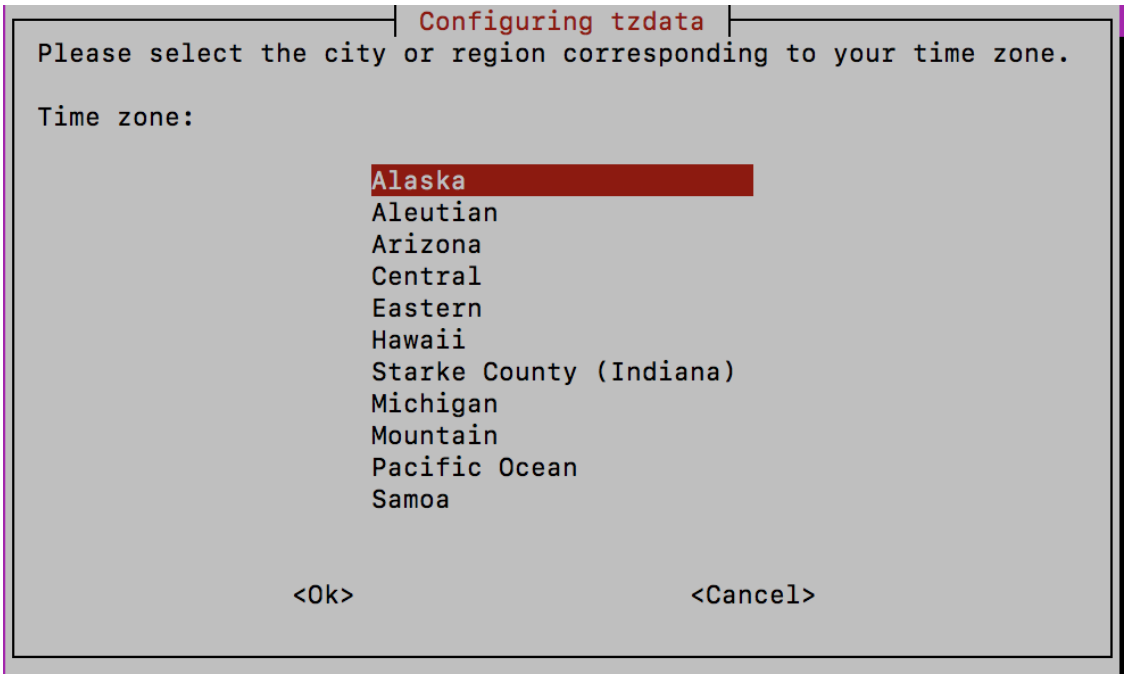
ステップ 1 Crosswork Data GatewayVM のインタラクティブメニューで、[Change Current System Settings] を選択します。

ステップ 2 [9 Timezone] を選択します。

ステップ 3 居住地域を選択します。



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 GatewayVM をリブートして、すべてのプロセスで新しいタイムゾーンが選択されるようにします。

ステップ 7 Crosswork Data Gateway VM からログアウトします。

パスワード要件の設定

次のパスワード要件を設定できます。

- パスワードの強度
- パスワード履歴
- パスワードの有効期限
- ログインエラー

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[0 パスワード要件の設定（0 Configure Password Requirements）] を選択します。

ステップ 2 変更するパスワード要件を選択します。

変更するオプションを設定します。

- **[パスワードの強度（Password Strength）]**
  - [クラスの最小数（Min Number of Classes）]
  - [最小長（Min Length）]
  - [最小変更文字数（Min Changed Characters）]
  - [クレジットの最大桁数（Max Digit Credit）]
  - [クレジットの最大大文字数（Max Upper Case Letter Credit）]
  - [クレジットの最大小文字数（Max Lower Case Letter Credit）]
  - [クレジットのその他の文字の最大文字数（Max Other Character Credit）]
  - [最大単調シーケンス（Max Monotonic Sequence）]
  - [連続する最大文字数（Max Same Consecutive Characters）]
  - [同じクラスの最大連続文字数（Max Same Class Consecutive Characters）]
- **[パスワード履歴（Password History）]**
  - [変更の再試行（Change Retries）]
  - [履歴数（History Depth）]
- [パスワードの有効期限（Password expiration）]
  - [最小日数（Min Days）]
  - [最大日数（Min Days）]
  - [警告日（Warn Days）]

- **[ログインエラー（Login Failures）]**
  - [ログインエラー（Login Failures）]
  - [初期ブロック時間（秒）（Initial Block Time (sec)）]
  - [アドレスキャッシュタイム（秒）（Address Cache Time (sec)）]

ステップ 3 設定を保存するには [**OK**] をクリックします。

同時ログイン数の制限の設定

デフォルトでは、Crosswork Data Gateway は、各 VM の **dg-admin** および **dg-oper** ユーザーに対して 10 の同時セッションをサポートします。これを変更するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[同時ログイン数の制限の設定（Configure Simultaneous Login Limits）] を選択します。

ステップ 2 表示されるウィンドウで、**dg-admin** および **dg-oper** ユーザーの同時セッション数を入力します。

ステップ 3 [OK] を選択して変更内容を保存します。

アイドルタイムアウトの設定

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[b アイドルタイムアウトの設定（b Configure Idle Timeout）] を選択します。

ステップ 2 表示されるウィンドウに、アイドルタイムアウトの新しい値を入力します。

ステップ 3 **Ok** と入力して、変更を保存します。

リモート監査サーバーの設定

この手順を使用して、リモートサーバーへの auditd daemon のエクスポートを設定します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[c auditdを設定（c Configure auditd）] を選択します。

ステップ 2 次の詳細を入力します。

- リモート Auditd サーバーアドレス。
- リモート auditd サーバーポート。

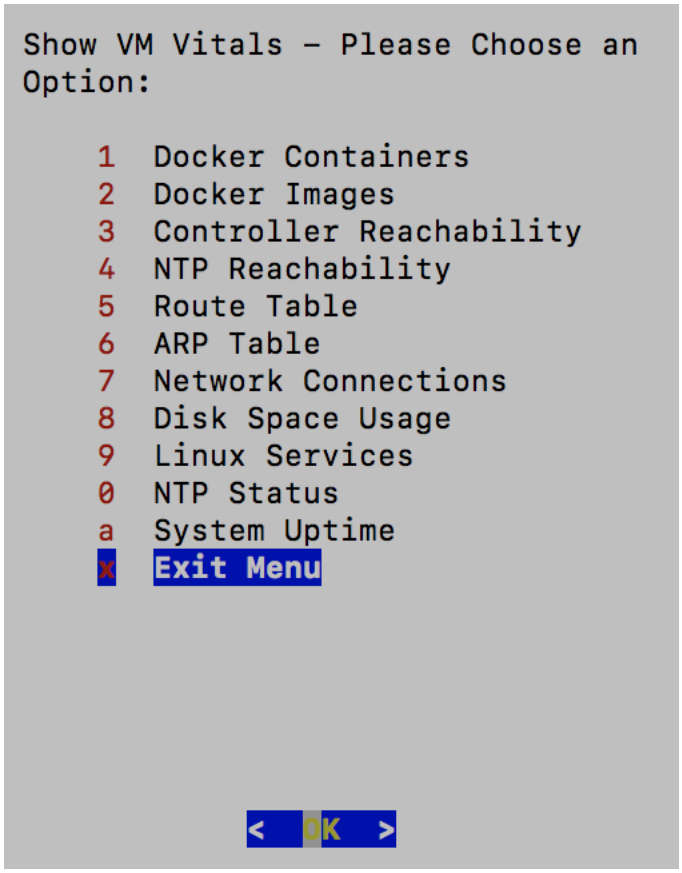
ステップ 3 [OK] を選択して変更内容を保存します。

Crosswork Data Gateway のバイタルの表示

以下の手順に従って、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のバイタルを表示します。

ステップ 1 メインメニューで、**バイタルを 4 つ**選択します。

ステップ 2 [VMのバイタルの表示（Show VM Vitals）] メニューから、表示するバイタルを選択します。



バイタル	説明
Docker コンテナ（Docker Containers）	システムで現在インスタンス化されている Docker コンテナの次のバイタルを表示します。 コンテナ ID（Container ID） イメージ画像（Image） 名前（Name） コマンド（Command） 作成時刻（Created Time） ステータス（Status） ポート（Port）
Docker イメージ（Docker Images）	システムで現在保存されている Docker イメージの次の詳細を表示します。 リポジトリ（Repository） イメージ ID（Image ID） 作成時刻（Created Time） サイズ（Size） タグ（Tag）
コントローラの到達可能性（Controller Reachability）	コントローラの到達可能性テストの実行結果を表示します。 デフォルト IPv4 ゲートウェイ（Default IPv4 gateway） デフォルト IPv6 ゲートウェイ（Default IPv6 gateway） DNS サーバ（DNS server） コントローラ（Controller） コントローラセッションのステータス（Controller session status）
NTP の到達可能性（NTP Reachability）	NTP 到達可能性テストの結果を表示します。 NTP サーバの解決（NTP server resolution） Ping NTP ステータス（NTP Status） 現在のシステム時間（Current system time）
ルート テーブル（Route Table）	IPv4 および IPv6 ルーティングテーブルを表示します。

バイタル	説明
ARP テーブル（ARP Table）	ARP テーブルを表示します。
ネットワーク接続（Network Connections）	現在のネットワーク接続とリスニングポートを表示します。
ディスク領域使用率（Disk Space Usage）	すべてのパーティションの現在のディスク容量の使用状況を表示します。
Linux サービス（Linux Services）	次の Linux サービスのステータスを表示します。 • NTP • SSH • Syslog • Docker • Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） インフラストラクチャコンテナ
NTP ステータスの確認	NTP サーバーのステータスを表示します。
システム稼働時間の確認	システム稼働時間を表示します。

Crosswork Data Gateway VM のトラブルシューティング

[トラブルシューティング（Troubleshooting）] メニューにアクセスするには、メインメニューから [5 トラブルシューティング（5 Troubleshooting）] を選択します。

（注） 画像は、**dg-admin** ユーザーに対応する [トラブルシューティング（Troubleshooting）] メニューを示しています。**dg-oper** ユーザはこれらのオプションの一部を使用できません。表 6：各ロールの権限 （69 ページ） を参照してください。

[トラブルシューティング（Troubleshooting）] メニューには、次のオプションがあります。

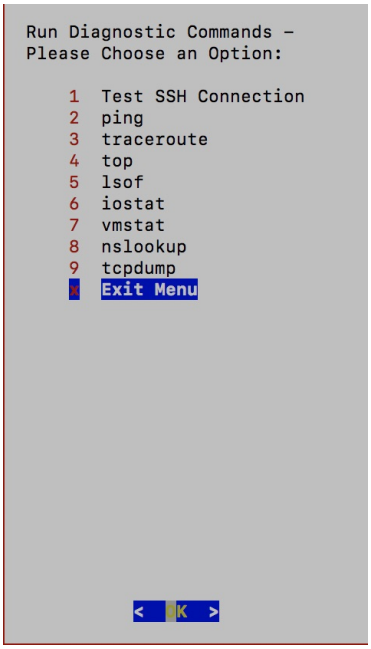
• 診断コマンドの実行 （85 ページ）
• show-tech の実行 （87 ページ）
• Crosswork Data Gateway VM のシャットダウン （88 ページ）
• auditd ログのエクスポート （88 ページ）

• TAC シェルアクセスの有効化 （88 ページ）

診断コマンドの実行

[診断の実行（Run Diagnostics）] メニューでは、コンソールに次のオプションが表示されます。

図 *1 : [*診断の実行（***Run Diagnostics***）*]* メニュー



ホストへの Ping

Crosswork Data Gateway は、任意の IP アドレスへの到達可能性を確認するために使用できる ping ユーティリティを提供します。

ステップ 1 [診断の実行（Run Diagnostics）] メニューから [2 ping] を選択します。

ステップ 2 次の情報を入力します。

- Ping 回数
- 宛て先ホスト名または IP
- 送信元ポート（UDP、TCP、TCP 接続）
- 宛て先ポート（UDP、TCP、TCP 接続）

ステップ 3 [OK] をクリックします。

ホストに対するトレースルート

Crosswork Data Gateway には遅延の問題のトラブルシューティングに役立つ [トレースルート（traceroute）] オプションが用意されています。このオプションを使用すると、Crosswork Data Gateway が接続先に到達するまでの大まかな時間を予測できます。

ステップ 1 [診断の実行（Run Diagnostics）] メニューから、[3 トレースルート（3 traceroute）] を選択します。

ステップ 2 トレースルート先を入力します。

ステップ 3 [OK] をクリックします。

トラブルシューティングのためのコマンドオプション

Crosswork Data Gateway には、トラブルシューティング用のコマンドがいくつか用意されています。

ステップ 1 [5 トラブルシューティング（5 Troubleshooting）] > [1 診断の実行（1 Run Diagnostics）] に移動します。

ステップ 2 コマンドと各コマンドの他のオプションまたはフィルタを選択します。

- **4 top**
- **5 lsof**
- **6 iostat**
- **7 vmstat**
- **8 nsolookup**

ステップ 3 [OK] をクリックします。

すべてのオプションを選択すると、Crosswork Data Gateway は画面をクリアし、指定したオプションを使用してコマンドを実行します。

tcpdump のダウンロード

Crosswork Data Gateway には、ネットワークトラフィックのキャプチャと分析を可能にする tcpdump オプションがあります。

（注） このタスクは、**dg-admin** ユーザーのみが実行できます。

ステップ 1 [5 トラブルシューティング（5 Troubleshooting）] > [診断の実行（Run Diagnostics）] > [9 tcpdump] に移動します。

ステップ 2 tcpdump ユーティリティを実行するインターフェイスを選択します。すべてのインターフェイスに対して実行するには、[すべて（All）] オプションを選択します。

ステップ 3 適切なチェックボックスをオンにして、画面にパケット情報を表示するか、またはキャプチャしたパケットをファイルに保存します。

ステップ 4 次の詳細を入力して、[OK] をクリックします。

- パケット数の制限（Packet count limit）
- 収集時間の制限（Collection time limit）
- フルサイズの制限（File size limit）
- フィルタ式

選択したオプションに応じて、Crosswork Data Gateway はパケットキャプチャ情報を画面に表示するか、またはファイルに保存します。tcpdumpユーティリティが指定した制限に達すると、Crosswork Data Gatewayはファイルを圧縮し、ファイルをリモートホストに転送するためのSCPクレデンシャルを要求します。転送が完了するか、または完了前にファイル転送をキャンセルする場合、圧縮したファイルは削除されます。

show-tech の実行

Crosswork Data Gateway は、ログファイルをユーザ定義の SCP の宛先にエクスポートするオプション **show_tech** を提供します。

次のようなデータが収集されます。

- Docker コンテナで実行されているすべての Data Gateway コンポーネントのログ
- VM バイタル

実行場所のディレクトリに tarball を作成します。出力は `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc` という名前の tarball です。

Crosswork Data Gateway の状態によって、このコマンドの実行に数分かかる場合があります。

ステップ 1 [トラブルシューティング（Troubleshooting）] メニューから [5 Show-tech] を選択し、[OK] をクリックします。

ステップ 2 ログとバイタルを含む tarball の保存先を入力します。

ステップ 3 SCP パスフレーズを入力し、[OK] をクリックします。

showtech ファイルは暗号化された形式でダウンロードされます。

（注） システムの使用時間によっては、showtech ファイルのダウンロードに数分かかる場合があります。

ステップ 4 ダウンロードが完了したら、次のコマンドを実行して復号します。

（注） ファイルを復号するには、OpenSSL バージョン 1.1.1i を使用する必要があります。システムの openssl バージョンを確認するには、`openssl version` コマンドを使用します。

MAC でファイルを復号するには、OpenSSL 1.1.1+ をインストールする必要があります。これは、LibreSSL の `openssl` コマンドが OpenSSL の `openssl` コマンドでサポートされているすべてのスイッチはサポートしていないためです。

```
openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Crosswork Data Gateway VM のシャットダウン

[トラブルシューティング（Troubleshooting）] メニューから [5 VM のシャットダウン（5 Shutdown VM）] を選択して、Crosswork Data Gateway VM の電源をオフにします。

auditd ログのエクスポート

auditd ログをエクスポートするには、次の手順を実行します。

ステップ 1 [トラブルシューティング（Troubleshooting）] で、[9 監査ログのエクスポート（9 Export audit Logs）] を選択します。

ステップ 2 auditd ログの tarball 暗号化用のパスフレーズを入力します。

ステップ 3 [OK] をクリックします。

ローテーションされたログファイルの削除

この手順を使用して、`/var/log` および `/opt/dg/log` フォルダ内のローテーションされたすべてのログファイル（*.gz または *.xz）を削除します。

ステップ 1 [トラブルシューティング（Troubleshooting）] メニューから、[8ローテーションログファイルの削除（8 Remove Rotated Log files）] を選択します。

ステップ 2 表示されるダイアログで [はい（Yes）] を選択して、変更を保存します。

TAC シェルアクセスの有効化

TAC シェルアクセス機能を使用すると、シスコのエンジニアは、**dg-tac** という名前の予約済みのユーザを使用して、多要素認証によって Ubuntu シェルに直接ログインできます。

最初は、ユーザがシェルプロンプトを取得しないように**dg-tac**ユーザアカウントがロックされていて、パスワードが期限切れになっています。有効にすると、dg-tac ユーザは次の暦日の 12:00 a.m UTC（午前 0 時 UTC）までアクティブになります。これは 24 時間未満です。

dg-tac ユーザを有効にする手順は、次のとおりです。

（注） このアクセスを有効にするには、シスコのエンジニアに連絡する必要があります。

始める前に

シスコの担当エンジニアが SWIMS Aberto ツールにアクセスできることを確認してください。

ステップ 1 **dg-admin** ユーザとして Data Gateway VM にログインします。

ステップ 2 メインメニューから、[5 トラブルシューティング（5 Troubleshooting）] を選択します。

ステップ 3 [トラブルシューティング（Troubleshooting）] メニューから、[TACシェルアクセスの有効化（Enable TAC Shell Access）] を選択します。

dg-tac ユーザのログインには設定済みのパスワードと TAC からチャレンジトークンへの応答が必要であることを警告するダイアログが表示されます。この時点で有効化プロセスを停止するには [いいえ（No）] を、続行するには [はい（Yes）] を選択します。

ステップ 4 続行すると、使用する新しいパスワードの入力が求められ、アカウントが無効になる日が表示されます。

ステップ 5 コンソールメニューでアカウントのロックを解除するためのパスワードを入力します。

ステップ 6 Crosswork Data Gateway からログアウトします。

ステップ 7 シスコのエンジニアが Crosswork Data Gateway の VM に直接アクセスできる場合は、次の手順を実行します。それ以外の場合は、**手順 8** に進みます。

a) **dg-tac** ユーザーの手順 5 で設定したパスワードを、担当のシスコエンジニアと共有します。

b) 設定したパスワードを使用してシスコのエンジニアが **dg-tac** ユーザーとして SSH 経由でログインします。

パスワードを入力すると、チャレンジトークンが表示されます。シスコのエンジニアは、SWIMS Aberto ツールを使用してチャレンジトークンに署名し、署名済みの応答を Crosswork Data Gateway の VM でチャレンジトークンに貼り付けます。

c) シスコのエンジニアは **dg-tac** ユーザーとして正常にログインし、トラブルシューティングを実行します。

dg-tac ユーザのアイドルタイムアウト時間は 15 分間です。ログアウトした場合、シスコのエンジニアは、再度ログインするために新しいチャレンジに署名する必要があります。

d) トラブルシューティングが完了したら、シスコのエンジニアは TAC シェルからログアウトします。

ステップ 8 シスコのエンジニアが Crosswork Data Gateway の VM に直接アクセスできない場合は、デスクトップ共有を有効にしてシスコのエンジニアとのミーティングを開始します。

a) 次のコマンドを使用して、**dg-tac** ユーザとして SSH 経由でログインします。

```
ssh dg-tac @<DG hostname or IP>
```

b) **dg-tac** ユーザに設定したパスワードを入力します。

パスワードを入力すると、チャレンジトークンが表示されます。このトークンをシスコのエンジニアと共有します。そのシスコのエンジニアはSWIMS Abertoツールを使用してトークンに署名し、応答を共有します。

c) チャレンジトークンに対する署名付き応答を Crosswork Data Gateway VM に貼り付けます。Enter キーを押すとシェルプロンプトが表示されます。

d) トラブルシューティングを行うには、デスクトップを共有するか、またはシスコのエンジニアの指示に従います。

dg-tac ユーザのアイドルタイムアウト時間は 15 分間です。ログアウトした場合、シスコのエンジニアは、再度ログインするために新しいチャレンジに署名する必要があります。

e) トラブルシューティングが完了したら、TAC シェルからログアウトします。

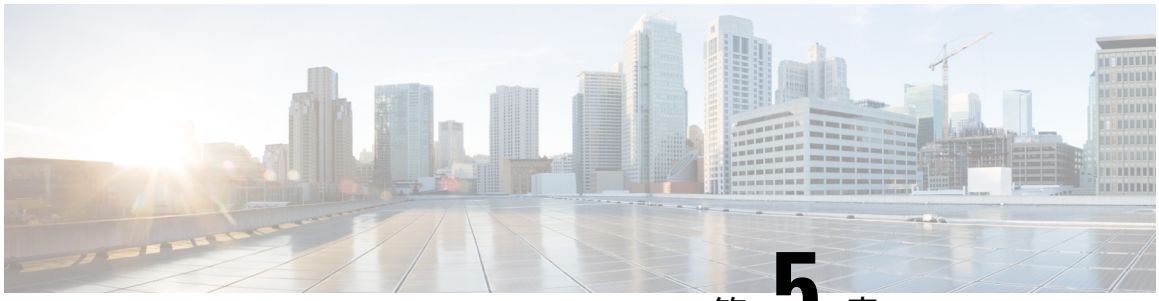
TAC シェルイベントの監査

次のリストにある TAC シェルイベントのタイムスタンプ情報は、**tac_shell.log** ファイルに記録されます。TAC シェルイベントは Crosswork Cloud コントローラにも送信されます。

- TAC シェルの有効化
- TAC シェルの無効化
- dg-tac のログイン
- dg-tac のログアウト

Data Gateway が Crosswork Cloud コントローラに接続できない場合、TAC シェルイベントは `/opt/dg/data/controller-gateway/audit/pending` フォルダに記録されます。Crosswork Cloud コントローラが到達可能になると、これらのイベントは 5 分以内に送信されます。

tac_shell.log ファイルは、Crosswork Data Gateway VM の showtech バンドルで使用できます。



第 5 章

仮想マシンの削除

ここでは、次の内容について説明します。

vSphere UI を使用した VM の削除

このセクションでは、vCenter から Crosswork Data Gateway VM を削除する手順について説明します。

（注） この手順によって、すべての Crosswork Data Gateway データが削除されることに注意してください。

始める前に

各 Crosswork Cloud アプリケーションのユーザガイドの「*Delete Crosswork Data Gateways* の削除」の項の説明に従って、Crosswork Cloud から Crosswork Data Gateway を削除したことを確認します。

ステップ 1 VMware vSphere Web クライアントにログインします。

ステップ 2 [ナビゲータ（Navigator）] ペインで、削除するアプリケーション VM を右クリックし、[電源（Power）] > [電源オフ（Power Off）] を選択します。

ステップ 3 VM の電源がオフになったら、もう一度 VM を右クリックし、[ディスクから削除（Delete from Disk）] を選択します。

VM が削除されます。

Cisco CSPからの Crosswork Data Gateway サービスの削除

Cisco CSPから Crosswork Data Gateway サービスを削除するには、次の手順を実行します。

始める前に

Crosswork Cloud アプリケーションそれぞれのユーザガイドの「*Crosswork Data Gateway* の削除」の項の説明に従って Crosswork Cloud から Crosswork Data Gateway を削除したことを確認します。

ステップ 1 Cisco CSP にログインします。

ステップ 2 [設定（Configuration）] > [サービス（Services）] に移動します。

[サービス（Service）] テーブルにサービスの現在のステータスが表示されます。

ステップ 3 [サービス名（Service Name）] 列でサービスインスタンスを見つけ、[アクション（Action）] 列の下にある [削除（Delete）] をクリックします。

OpenStack からの VM の削除

OpenStack UI を使用して、OpenStack から Crosswork Data Gateway サービスを削除する手順に従います。

（注） この手順により、Crosswork Data Gateway VM データが削除されます。Crosswork Data Gateway VM は、削除すると復元できません。

始める前に

『*Cisco Crosswork Cloud* ユーザーガイド』の「*Crosswork Data Gateways* の削除」の項の説明に従って、Crosswork Cloud から Crosswork Data Gateway を削除したことを確認します。

ステップ 1 **OpenStack の UI から実行する場合**

a) OpenStack の UI にログインします。
b) [コンピューティング（Compute）] > [インスタンス（Instances）] に移動します。
c) このページに表示される VM のリストから、削除する VM を選択します。
d) [インスタンスの削除（Delete Instances）] をクリックします。
e) VM を削除する際に表示される確認ウィンドウで [インスタンスの削除（Delete Instances）] をクリックします。

OR

ステップ 2 OpenStack の CLI から実行する場合

a) CLI から OpenStack VM にログインします。

b) 次のコマンドを実行します。

```
openstack server delete CDG_VM_name
```

次に例を示します。

```
openstack server delete cdg-ospd1
```

c) （オプション）すべての VM のリストを表示して、VM が削除されたことを確認します。

```
openstack server list
```

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。