



クラウドアプリケーション向け **Cisco Crosswork Data Gateway 5.0** インストールおよびコンフィギュレーションガイド

初版：2023年5月8日

最終更新：2023年5月12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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

概要 1

対象読者 1

Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) の概要 2

第 2 章

インストール要件 3

リソースと設定の要件 4

使用ポート 7

プロキシ サーバの要件 8

Amazon EC2 設定 9

第 3 章

インストール タスク 13

Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) のインストール 13

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 15

VMware への Crosswork Data Gateway のインストール 34

vCenter vSphere Client を使用した Crosswork Data Gateway のインストール 35

OVF ツールによる Crosswork Data Gateway のインストール 46

Crosswork Data Gateway IPv4 展開のためのサンプルスクリプト 48

Crosswork Data Gateway がインストールされていることを確認する 50

Crosswork Data Gateway VM へのログインとログアウト 50

vCenter を介した Crosswork Data Gateway へのアクセス 51

SSH による Crosswork Data Gateway VM へのアクセス 51

Crosswork Data Gateway VM からのログアウト 52

OpenStack プラットフォームへの Crosswork Data Gateway のインストール 52

OpenStack CLI を使用した OpenStack への Crosswork Data Gateway のインストール	52
OpenStack UI を使用した OpenStack への Crosswork Data Gateway のインストール	67
Amazon EC2 に Crosswork Data Gateway をインストールする	91
CloudFormation (CF) テンプレートを使用した Crosswork Data Gateway のインストール	92
CF テンプレート画像の抽出	92
ロールとポリシーの権限	93
Crosswork Data Gateway をインストールするための CF テンプレートのパラメータ	94
CF テンプレートの展開の管理	97
Amazon EC2 に Crosswork Data Gateway を手動でインストールする	99
Crosswork Data Gateway を展開するための自動構成	103
登録パッケージの生成	107
登録パッケージの入手	109
登録パッケージのエクスポート	109
エンコード済み登録パッケージの作成	111
Crosswork Cloud アプリケーションを使用した Crosswork Data Gateway の登録	112
Crosswork Data Gateway 接続のトラブルシューティング	113
<hr/>	
第 4 章	Crosswork Data Gateway インスタンスの設定
	115
	Crosswork Data Gateway ユーザーの管理
	115
	サポートされるユーザ ロール
	115
	パスフレーズの変更
	118
	現在のシステム設定の表示
	118
	現在のシステム設定の変更
	120
	NTP の設定
	121
	DNS の設定
	122
	制御プロキシの設定
	122
	スタティックルートの設定
	123
	スタティック ルートの追加
	123
	スタティック ルートの削除
	123
	Syslog の設定
	123
	新しい SSH キーの作成
	125

証明書のインポート	125
vNIC2 MTU の設定	125
Crosswork Data Gateway VM のタイムゾーンの設定	126
パスワード要件の設定	127
同時ログイン数の制限の設定	128
アイドルタイムアウトの設定	129
リモート監査サーバーの設定	129
インターフェイスアドレスの設定	129
Crosswork Data Gateway のバイタルの表示	132
Crosswork Data Gateway VM のトラブルシューティング	135
診断コマンドの実行	136
ホストへの Ping	136
ホストに対するトレースルート	137
トラブルシューティングのためのコマンドオプション	137
tcpdump のダウンロード	137
コントローラセッションテストの実行	138
show-tech の実行	140
Crosswork Data Gateway VM のシャットダウン	141
auditd ログのエクスポート	141
ローテーションされたログファイルの削除	141
TAC シェルアクセスの有効化	141
TAC シェルイベントの監査	143

第 5 章	仮想マシンの削除	145
	vSphere UI を使用した VM の削除	145
	OpenStack からの VM の削除	146



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 \(1 ページ\)](#)
- [Cisco Crosswork データゲートウェイ \(Cisco Crosswork Data Gateway\) の概要 \(2 ページ\)](#)

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 Crosswork Cloud 環境への有効なログインを行えるようになってい必要があります。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。

- Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) をインストールするデータセンターの理解。この知識を使用して、サポートされている仮想化プラットフォームのいずれかを使用してアプリケーションを展開できる必要があります。
 - VMware vCenter : VMware vCenter CLI または OVF ツールを使用した OVF テンプレートの展開。
 - OpenStack : CLI または UI を使用して OpenStack に Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を展開します。
 - Amazon EC2 : Amazon Elastic Compute Cloud (EC2) に CloudFormation テンプレートを展開します。
- ネットワークコンポーネントのモニタリングと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 Crosswork 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 このガイドでは、クラウドでホストされ、シスコが管理する Crosswork アプリケーションで使用するために、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。

データセンターまたは管理するクラウド環境に導入された Crosswork アプリケーションと共に Crosswork Data Gateway を導入する方法の詳細については、『Cisco Crosswork Network Controller 5.0 Installation Guide』を参照してください。

Crosswork Data Gateway が次の Crosswork Cloud SaaS 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 SaaS ソリューションです。
- Cisco Crosswork Cloud Traffic Analysis 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します。



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
- OpenStack プラットフォーム
- Amazon EC2

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。

- インストールを実行するために必要な情報を収集する。
- 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。

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（「[リソースと設定の要件 \(4 ページ\)](#)」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 \(7 ページ\)](#)」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 \(8 ページ\)](#) を参照してください。
4. Crosswork Data Gateway の展開を計画しているデータセンターを決定し、Crosswork Data Gateway の展開に使用する IP アドレスを収集します。必要な設定、および Crosswork Data Gateway のインストール中に提供する必要がある環境の詳細については、[リソースと設定の要件 \(4 ページ\)](#) を参照してください。
 - [リソースと設定の要件 \(4 ページ\)](#)
 - [使用ポート \(7 ページ\)](#)
 - [プロキシサーバの要件 \(8 ページ\)](#)

- [Amazon EC2 設定 \(9 ページ\)](#)

リソースと設定の要件

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。



(注) 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: クラウドアプリケーション用の VM 要件

要件	Description
データセンター	VMware <ul style="list-style-type: none"> • VMware vCenter Server 6.7、ESXi 6.5 • VMware vCenter Server 7.0、ESXi 6.5 および 6.7 Openstack <ul style="list-style-type: none"> • OpenStack OSP16 Amazon <ul style="list-style-type: none"> • Amazon Elastic Compute Cloud
メモリ	32 GB
合計ディスク領域 (ブートディスク + データディスク)	74 GB (50 GB + 24 GB) (注) データディスク領域はオプションの要件です。
vCPU	8

表 2: サポートされるインターフェイス

インターフェイス	Description			
インターフェイス	最小値 : 1 最大値 : 3 Crosswork Data Gateway は、次の組み合わせに従って、1、2、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。			
	NIC の数	vNIC0	vNIC1	vNIC2
	1	<ul style="list-style-type: none"> 管理トラフィック 制御/データトラフィック (ノースバウンドトラフィック) デバイスアクセストラフィック (サウスバウンドトラフィック) 	—	—
	2	<ul style="list-style-type: none"> 管理トラフィック 	<ul style="list-style-type: none"> 制御/データトラフィック (ノースバウンドトラフィック) デバイスアクセストラフィック (サウスバウンドトラフィック) 	—
	3	<ul style="list-style-type: none"> 管理トラフィック 	<ul style="list-style-type: none"> 制御/データトラフィック (ノースバウンドトラフィック) 	<ul style="list-style-type: none"> デバイスアクセストラフィック (サウスバウンドトラフィック)

インターフェイス	Description
	<ul style="list-style-type: none"> • 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。 <p>重要 Crosswork Data Gateway は、コントロールインターフェイスまたはデータインターフェイスがインターネットにアクセスできる場合にのみ、クラウドに接続できます。</p> <ul style="list-style-type: none"> • 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。 <p>複数の vNIC を使用した展開では、ネットワーク設計に基づいてさまざまな vNIC にトラフィックタイプを割り当てることができます。たとえば、2 vNIC 展開では、vNIC0 または vNIC1 のいずれかを選択して次のトラフィックを処理できます。</p> <ul style="list-style-type: none"> • 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

表 3: 設定オプション

インターフェイス	Description
IP アドレス	<p>使用するインターフェイスの数に基づいた、1～4 つの IPv4 または IPv6 アドレス。</p> <p>(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。</p>

インターフェイス	Description
NTP サーバー	<p>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。</p> <p>(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。到達可能でない場合、インストールは失敗します。</p> <p>Crosswork Data Gateway ホストと仮想マシンは NTP サーバー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。</p>
DNS サーバー	<p>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。</p>
DNS 検索ドメイン	<p>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。</p>
(オプション) プロキシサーバー	<p>オプションの管理ネットワーク プロキシサーバーの URL。</p> <p>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 に接続できるようにプロキシサーバーを設定する必要があります。</p>
(オプション) Syslog サーバー	<p>オプションの Syslog サーバーのホスト名、IPv4、または IPv6 アドレス。</p>
(オプション) Auditd サーバー	<p>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。</p>

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 4: 管理トラフィック用に開くポート

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

表 5: 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	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 が設定されたプロキシサーバーを使用できるようにします。Cisco Crosswork Data Gateway は、このプロキシサーバーを介して Crosswork Cloud サービスに接続します。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ログイン情報を入力する。「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 (15 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 \(122 ページ\)](#) を参照してください

Amazon EC2 設定

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



注目 このセクションで説明する要件のほとんどは Amazon EC2 の概念であり、Crosswork Cloud だけが課すものではありません。

表 6: Amazon EC2 の前提条件

要件	Description
VPC とサブネット	仮想プライベートクラウド (VPC) は、Crosswork インターフェイス (管理、データ) および Crosswork Data Gateway (管理、データ、デバイス) インターフェイスの専用サブネットで作成および構成されます。このセクションに記載されているアドレスは使用しないでください。
エンドポイント	次のパラメータを使用して、VPC にエンドポイントが作成されます。 <ul style="list-style-type: none"> • サービス名 : 展開するリージョン (可用性ゾーン) の EC2 サービス。 • プライベート DNS 名 : 有効 • エンドポイントタイプ : インターフェイス • [サブネット (Subnets)] で、インストールに使用する予定の管理サブネットを指定します。Crosswork VM と Crosswork Data Gateway VM に異なる管理サブネットを使用している場合は、両方の管理サブネットを指定して、エンドポイントがサブネットにアクセスできるようにしてください。

要件	Description
IAM ロール	<p>Identity and Access Management (IAM) で、関連する権限ポリシーを使用してロールが作成されます。IAM ロールは、短期間有効なログイン情報を持つ、特定の権限を持つ ID です。信頼するエンティティがロールを引き受けることができます。</p> <p>(注)</p> <ul style="list-style-type: none"> • Crosswork ロールに必要な最小限の権限は、ec2:AssignPrivateIpAddresses および ec2:UnassignPrivateIpAddresses です。 • ロールの信頼ポリシーには、"Action": "sts:AssumeRole" 条件が必要です。
キーペア	キーペア (VM へのログインに使用される秘密キー) が作成および構成されます。
IP アドレス	<p>Crosswork Data Gateway : 管理トラフィックとデータトラフィック専用の IP アドレス。</p> <ul style="list-style-type: none"> • IP アドレスは、Cisco Crosswork Data Gateway がインストールされるネットワークのゲートウェイアドレスに到達できる必要があります。到達できない場合、インストールは失敗します。 • 現在、IP の割り当ては永続的であり、再展開しない限り変更できません。詳細については、シスコカスタマーエクスペリエンス チームにお問い合わせください。
セキュリティ グループ	許可するポートまたはトラフィックを指定するには、セキュリティグループを作成して構成する必要があります。
インスタンス タイプ	m5.2xlarge インスタンスタイプは、Crosswork Data Gateway (実稼働およびラボ導入) での展開でサポートされています。
CloudFormation (CF) テンプレート	CloudFormation テンプレートの手順を使用してインストール中にアップロードする必要がある Crosswork Data Gateway VM の CF テンプレート (.yaml) ファイル。詳細については、 CloudFormation (CF) テンプレートを使用した Crosswork Data Gateway のインストール (92 ページ) を参照してください。

要件	Description
ユーザーデータ	<p>手動インストール手順中に指定する必要がある VM 固有のパラメータスクリプト。詳細については、以下を参照してください。</p> <ul style="list-style-type: none">• CloudFormation (CF) テンプレートを使用した Crosswork Data Gateway のインストール (92 ページ)• Amazon EC2 に Crosswork Data Gateway を手動でインストールする (99 ページ)



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 \(13 ページ\)](#)
- [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 \(15 ページ\)](#)
- [VMware への Crosswork Data Gateway のインストール \(34 ページ\)](#)
- [OpenStack プラットフォームへの Crosswork Data Gateway のインストール \(52 ページ\)](#)
- [Amazon EC2 に Crosswork Data Gateway をインストールする \(91 ページ\)](#)
- [Crosswork Data Gateway を展開するための自動構成 \(103 ページ\)](#)
- [登録パッケージの生成 \(107 ページ\)](#)
- [登録パッケージの入手 \(109 ページ\)](#)
- [Crosswork Cloud アプリケーションを使用した Crosswork Data Gateway の登録 \(112 ページ\)](#)
- [Crosswork Data Gateway 接続のトラブルシューティング \(113 ページ\)](#)

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。ここでは、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. Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を展開するプラットフォームを決定し、必要なソフトウェアイメージがあることを確認します。

VMware	<p>vCenter vSphere Client を使用した Crosswork Data Gateway のインストール (35 ページ)</p> <p>OVF ツールによる Crosswork Data Gateway のインストール (46 ページ)</p>
OpenStack	<p>OpenStack CLI を使用した OpenStack への Crosswork Data Gateway のインストール (52 ページ)</p> <p>OpenStack UI を使用した OpenStack への Crosswork Data Gateway のインストール (67 ページ)</p> <p>Crosswork Data Gateway を展開するための自動構成 (103 ページ)</p>
Amazon EC2	<p>CloudFormation (CF) テンプレートを使用した Crosswork Data Gateway のインストール (92 ページ)</p> <p>Amazon EC2 に Crosswork Data Gateway を手動でインストールする (99 ページ)</p> <p>Crosswork Data Gateway を展開するための自動構成 (103 ページ)</p>

2. 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 (15 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 (107 ページ)
 - 登録パッケージの入手 (109 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 (112 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、可能性のある導入シナリオと導入パラメータについて、このセクション全体をお読みください。

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 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 (141 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 \(115 ページ\)](#) 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、コンソールでパスワードの変更を実行できます。[パスワードの変更 \(118 ページ\)](#) を参照してください。パスワードを紛失したか忘れた場合は、必要に応じて、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。



注意 必須パラメータが設定されていない場合、Crosswork Data Gateway はデフォルト値を使用して展開されます。ただし、デフォルト値が環境要件と一致しない場合があります。

** 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。



(注) 展開時にパラメータを入力するときは、正しいパラメータを追加していることを確認してください。パラメータ値が正しくない場合は、現在の Crosswork Data Gateway VM を破棄し、新しい VM を作成してその新しい VM を Cisco Crosswork に再登録する必要があります。

表 7: 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	Description	その他の情報
ホスト情報			
ホスト名 (Hostname) *	Hostname	完全修飾ドメイン名 (FQDN) として指定された Cisco Crosswork Data Gateway VM の名前。 大規模なシステムでは、複数の Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) VM が存在する可能性があります。したがって、ホスト名は一意であり、特定の VM を簡単に識別できるように作成する必要があります。	
説明 (Description) *	Description	Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) の詳細です。	
ラベル (Label)	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。	

名前	パラメータ	Description	その他の情報
導入*	Deployment	コントローラタイプを伝えるパラメータ。クラウドの導入では、値に Crosswork Cloud を指定します。	VMware vCenter の場合、このパラメータを構成することはできません。OVFActive ツールは、このパラメータをデフォルト値で構成します。
プロファイル*	Profile	パラメータは、VM リソースプロファイルを伝達します。	VMware vCenter の場合、このパラメータを構成することはできません。OVF ツールは、このパラメータをデフォルト値で構成します。
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 No、Yes、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	Description	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せん。	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。
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。	ただし、サードパーティまたは独自の証明書ファイルを使用する場合は、これらのパラメータを入力します。 証明書チェーンは、Cisco Crosswork Data Gateway VM のプリセットまたは生成された証明書を上書きし、SCP URI (user:host/path/to/file) として指定されます。URI ファイルを持つホストは、ネットワーク上で (SCP を介して vNIC0 インターフェイスから) 到達可能でなければならず、ファイルはインストール時に存在している必要があります。
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)。デフォルトのサイズは 24GB です。シスコの担当者に相談せずにデフォルト値を変更しないでください。	

名前	パラメータ	Description	その他の情報
AwsIamRole	AwsIamRole	EC2のインストールに使用する AWS IAM のロール名。	AWS 環境の Identity and Access Management (IAM) で、関連する権限を使用してロールが作成されます。
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 - 64 文字で指定する必要があります。	
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 - 64 文字である必要があります。	
インターフェイス			
(注) Crosswork Data Gateway を正しくインストールするには、IPv4 または IPv6 アドレスを静的または DHCP に構成する必要があります。使用しないプロトコルは [なし (None)] に設定する必要があります。			
vNIC ロールの割り当て			

名前	パラメータ	Description	その他の情報
NicDefaultGateway*	NicDefaultGateway	<p>DNS および NTP トラフィックを処理するためのデフォルトゲートウェイとして使用されるインターフェイス。</p> <p>他のインターフェイスに割り当てられていないトラフィックは、デフォルトでこのインターフェイスに割り当てられます。</p> <p>オプションは、eth0、eth1、eth2、またはeth3です。デフォルト値はeth0です。</p>	<p>Crosswork Data Gateway を展開するために選択した vNIC モデルに基づいて、インターフェイスの数を設定できます。たとえば、2 つのアクティブな vNIC に Crosswork Data Gateway を展開した場合、eth0 および eth1 インターフェイスを使用するようにロールを構成する必要があります。</p>
NicAdministration*	NicAdministration	<p>Crosswork Data Gateway の管理に関連するトラフィックをルーティングするために使用されるインターフェイス。このインターフェイスでは、設定済みのポートを介して SSH プロトコルを使用します。</p> <p>オプションは、eth0、eth1、eth2、またはeth3です。デフォルト値はeth0です。</p>	<ul style="list-style-type: none"> • NicControl、NicNBExternalData、NicSBData ロールは、eth1 にマップされます。 • NicControl、NicNBExternalData、NicSBData ロールは、eth1 にマップされます。
NicExternalLogging*	NicExternalLogging	<p>Crosswork Cloud にログを送信するために使用されるインターフェイス。</p> <p>オプションは、eth0、eth1、eth2、またはeth3です。デフォルト値はeth0です。</p>	<ul style="list-style-type: none"> • NicSBData ロールは、eth2 にマップされます。 • NicControl および NicNBExternalData ロールは、eth1 にマップされます。
NicManagement*	NicManagement		

名前	パラメータ	Description	その他の情報
		登録およびその他の管理 トラフィックを送信する ために使用されるイン ターフェイス。 オプションは、eth0、 eth1、eth2、またはeth3 です。デフォルト値は eth0 です。	
NicControl*	NicControl	宛先、デバイス、および 収集設定の送信に使用さ れるインターフェイス。 オプションは、eth0、 eth1、eth2、またはeth3 です。デフォルト値は eth0 です。	
NicNBSystemData*	NicNBSystemData	収集されたデータをシス テムの宛先に送信するた めに使用されるインター フェイス。 オプションは、eth0、 eth1、eth2、またはeth3 です。デフォルト値は eth0 です。	
NicNBExternalData*	NicNBExternalData	Crosswork Cloud に収集 データを送信するために 使用されるインターフェ イス。 オプションは、eth0、 eth1、eth2、またはeth3 です。デフォルト値は eth0 です。	
NicSBData*	NicSBData		

名前	パラメータ	Description	その他の情報
		すべてのデバイスからデータを収集するために使用されるインターフェイス。 オプションは、eth0、eth1、eth2、またはeth3です。デフォルト値はeth0です。	
vNICIPv4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	Description	その他の情報
vNIC IPv4 メソッド (vNIC IPv4 Method) *	Vnic0IPv4Method Vnic1IPv4Method Vnic2IPv4Method	<p>オプションは、None、Static、または DHCP です。</p> <p>(注) DHCP サポートは、QCOW2 イメージを使用して実行される展開に対してのみ有効になります。</p> <p>IPv4 アドレスを使用するには、[方式 (Method)] を Static または DHCP と選択し、[vNICxIPv6方式 (vNICxIPv6 Method)] を None と選択します。[方式 (Method)] のデフォルト値は [なし (None)] です。</p>	<p>[メソッド (Method)] の選択に応じて、以下を実行します。</p> <ul style="list-style-type: none"> • [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] : vNIC IPv4 アドレスパラメータ値は自動的に割り当てられます。デフォルト値は変更しないでください。
vNIC IPv4 アドレス (vNIC IPv4 Address)	Vnic0IPv4Address Vnic1IPv4Address Vnic2IPv4Address	インターフェイスの IPv4 アドレス。	
vNIC IPv4 ネットマスク (vNIC IPv4 Netmask)	Vnic0IPv4Netmask Vnic1IPv4Netmask Vnic2IPv4Netmask	ドット区切りの4つの数字列形式によるインターフェイスの IPv4 ネットマスク。	
vNIC IPv4 スキップゲートウェイ (vNIC IPv4 Skip Gateway)	Vnic0IPv4SkipGateway Vnic1IPv4SkipGateway Vnic2IPv4SkipGateway	<p>オプションは True または False です。</p> <p>True を選択すると、ゲートウェイの設定がスキップされます。</p> <p>デフォルト値は False です。</p>	

名前	パラメータ	Description	その他の情報
vNIC IPv4 ゲートウェイ (vNIC IPv4 Gateway)	Vnic0IPv4Gateway Vnic1IPv4Gateway Vnic2IPv4Gateway	vNIC ゲートウェイの IPv4 アドレス。	
vNIC IPv6 アドレス (使用するインターフェイスの数に応じて vNIC0、vNIC1、および vNIC2)			

名前	パラメータ	Description	その他の情報
vNIC IPv6 メソッド (vNIC IPv6 Method) *	Vnic0IPv6Method Vnic1IPv6Method Vnic2IPv6Method	オプションは、None、Static、DHCP、または SLAAC (QCOW2 only) です。 [方式 (Method)]のデフォルト値は [なし (None)]です。 (注) DHCP サポートは、QCOW2 イメージを使用して実行される展開に対してのみ有効になります。	[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。 vNICx 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] : vNIC IPv6 アドレスパラメータ値は自動的に割り当てられます。 VnicxIPv6Address のデフォルト値は変更しないでください。
vNIC IPv6 アドレス (vNIC IPv6 Address)	Vnic0IPv6Address Vnic1IPv6Address Vnic2IPv6Address	インターフェイスの IPv6 アドレス。	
vNIC IPv6 ネットマスク (vNIC IPv6 Netmask)	Vnic0IPv6Netmask Vnic1IPv6Netmask Vnic2IPv6Netmask	インターフェイスの IPv6 プレフィックス。	
vNIC IPv6 スキップゲートウェイ (vNIC IPv6 Skip Gateway)	Vnic0IPv6SkipGateway Vnic1IPv6SkipGateway Vnic2IPv6SkipGateway	オプションは True または False です。 True を選択すると、ゲートウェイの設定がスキップされます。 デフォルト値は False です。	
vNIC IPv6 ゲートウェイ (vNIC IPv6 Gateway)	Vnic0IPv6Gateway Vnic1IPv6Gateway Vnic2IPv6Gateway	vNIC ゲートウェイの IPv6 アドレス。	
DNS サーバ			

名前	パラメータ	Description	その他の情報
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。	
DNS 検索ドメイン (DNS Search Domain)	Domain	DNS の検索ドメイン。 デフォルト値は localdomain です。	
DNS セキュリティ 拡張機能 (DNS Security Extensions)	DNSSEC	オプションは、False、True、Allow-Downgrade です。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。 デフォルト値は False です。	
DNS over TLS	DNSTLS	オプションは、False、True、または Opportunistic です。DNS over TLS を使用するには、True を選択します。 デフォルト値は False です。	
マルチキャスト DNS (Multicast DNS)	mDNS	オプションは、False、True、または Resolve です。マルチキャスト DNS を使用するには、True を選択します。 デフォルト値は False です。	

名前	パラメータ	Description	その他の情報
リンクローカルマルチキャスト名前解決 (Link-Local Multicast Name Resolution)	LLMNR	オプションは、False、True、Opportunistic、または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。 デフォルト値はFalseです。	
NTP Servers			
NTPv4 サーバ (NTPv4 Servers) *	NTP	NTPv4 サーバリスト。管理インターフェイスでアクセス可能な NTPv4 サーバの IPv4 アドレス、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、「<サンプル>.ntp.org」のような形式で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。

名前	パラメータ	Description	その他の情報
NTPv4 認証の使用 (Use NTPv4 Authentication)	NTPAuth	NTPv4 認証を使用するには、True を選択します。デフォルト値は False です。	NTPKey、NTPKeyFile、および NTPKeyFilePwd は、NTPAuth が True に設定されている場合にのみ構成できます。
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 キーファイルパスワード (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			

名前	パラメータ	Description	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、True を選択します。デフォルト値は False 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 サーバーの 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	オプションは、Syslog を送信する UDP、TCP、または RELP です。デフォルト値は UDP です。	
Syslog マルチサーバーモード	SyslogMultiserverMode		

名前	パラメータ	Description	その他の情報
		フェールオーバーまたは同時モードの複数のサーバー。このパラメータは、プロトコルが非UDP の場合に適用されます (UDP は、Simultaneous を使用する必要があります)。 オプションは、Simultaneous または Failover です。 デフォルト値は Simultaneous です。	
TLS 経由の Syslog を使用する (Use Syslog over TLS)	SyslogTLS	TLS を使用して syslog のトラフィックを暗号化するには、True を選択します。 デフォルト値は False です。	
Syslog TLS ピア名 (Syslog TLS Peer Name)	SyslogPeerName	サーバー証明書の SubjectAltName またはサブジェクト共通名に入力されたとおりの Syslog サーバーのホスト名。	
Syslog ルート証明書ファイル URI (Syslog Root Certificate File URI)	SyslogCertChain	SCP を使用して取得した syslog サーバーの 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	Description	その他の情報
			<p>外部 syslog サーバを設定すると、サーブスイベントが外部 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。</p> <p>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。</p> <p>(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</p>

名前	パラメータ	Description	その他の情報
			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 Auditd メッセージを送信するには、True を選択します。 デフォルト値は False です。	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。
Auditd サーバアドレス (Auditd Server Address)	AuditdAddress	オプションの Auditd サーバーのホスト名、IPv4、または IPv6 アドレス。	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。
監査サーバポート (Auditd Server Port)	AuditdPort	オプションの監査サーバのポート番号。 デフォルトのポート番号は 60 です。	
コントローラとプロキシの設定			

名前	パラメータ	Description	その他の情報
プロキシサーバの URL (Proxy Server URL)	ProxyURL	オプションとなる HTTP 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ーのユーザ名。	
認証プロキシのパスワード (Authenticated Proxy Passphrase)	ProxyPassphrase	認証済みプロキシサーバーのパスワード。	
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ワード (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	Description	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。
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。	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、 登録パッケージの入手 (109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。

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

VMware への Crosswork Data Gateway のインストール

次のいずれかの方法で VMware に Crosswork Data Gateway をインストールできます。

- [vCenter vSphere Client を使用した Crosswork Data Gateway のインストール \(35 ページ\)](#)
- [OVF ツールによる Crosswork Data Gateway のインストール \(46 ページ\)](#)

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 『Cisco Crosswork Data Gateway 5.0 Release Notes for Cloud Applications』を参照し、インストーラバンドル (.tar.gz ファイル) と OVA ファイルを [cisco.com](https://www.cisco.com) からディレクトリにダウンロードします。

これらの手順では、ファイル名 **cw-na-dg-5.0.0-45-release-20230418.uefi.ova** および **cw-na-dg-5.0.0-sample-install-scripts.tar.gz** を使用します。 **cw-na-dg-5.0.0-sample-install-scripts.tar.gz** には、1 つ、2 つ、および 3 つの vNIC 展開用のサンプルスクリプトが含まれており、ニーズに合わせて最適化できます。

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

(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、ログイン情報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 vSphere Client に接続し、[アクション (Actions)] > [OVFテンプレートの展開 (Deploy OVF Template)] を選択します。

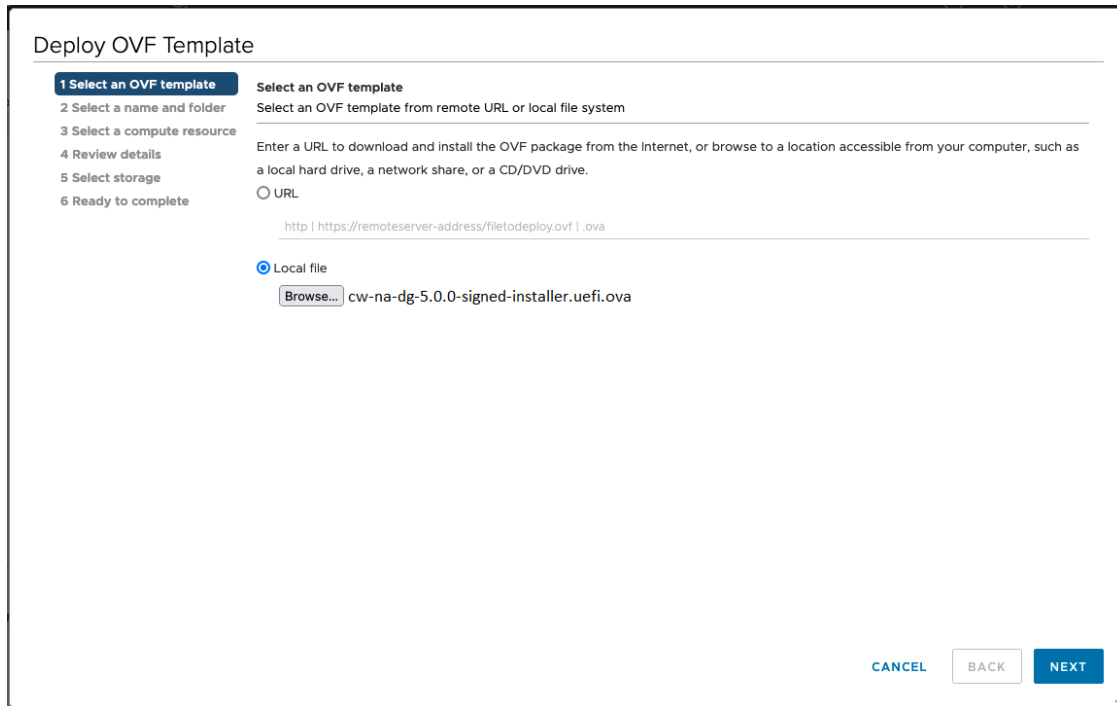
警告 デフォルトの VMware vCenter の展開タイムアウトは 15 分です。OVF テンプレートの入力にかかる時間が 15 分を超えると、vCenter がタイムアウトし、最初からやり直す必要があります。これを防ぐには、必要なパラメータと要件を準備しておきインストールを計画することをお勧めします。必須およびオプションのパラメータのリストについては、[Cisco Crosswork データゲートウェイ \(Cisco Crosswork Data Gateway\) 導入パラメータとシナリオ \(15 ページ\)](#) を参照してください。

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

選択すると、ファイル名がウィンドウに表示されます。

図 1: [OVFテンプレートの展開 (Deploy OVF Template)] - [OVFテンプレートの選択 (Select an OVF Template)] ウィンドウ



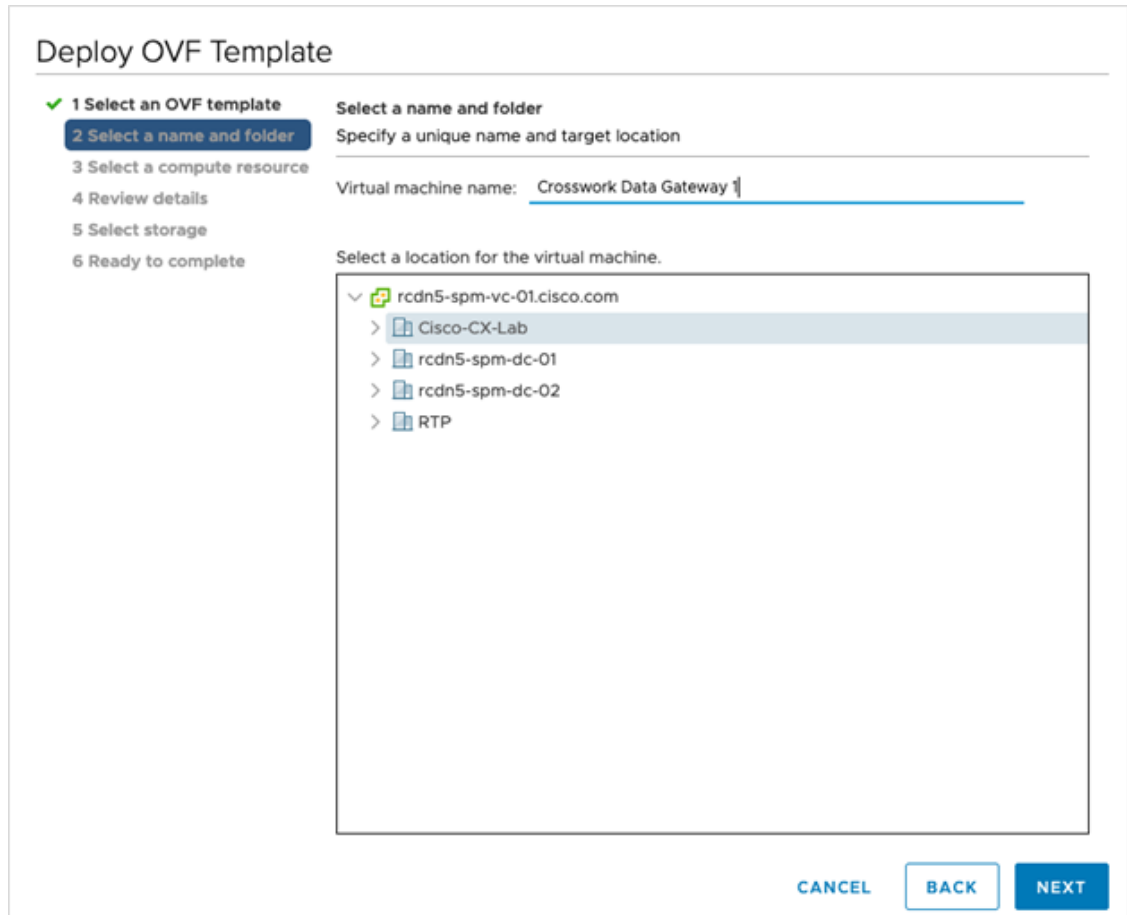
ステップ 6 次の図のように、[次へ (Next)] をクリックして、[名前とフォルダの選択 (2 Select name and folder)] に移動します。

a) 作成する 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。

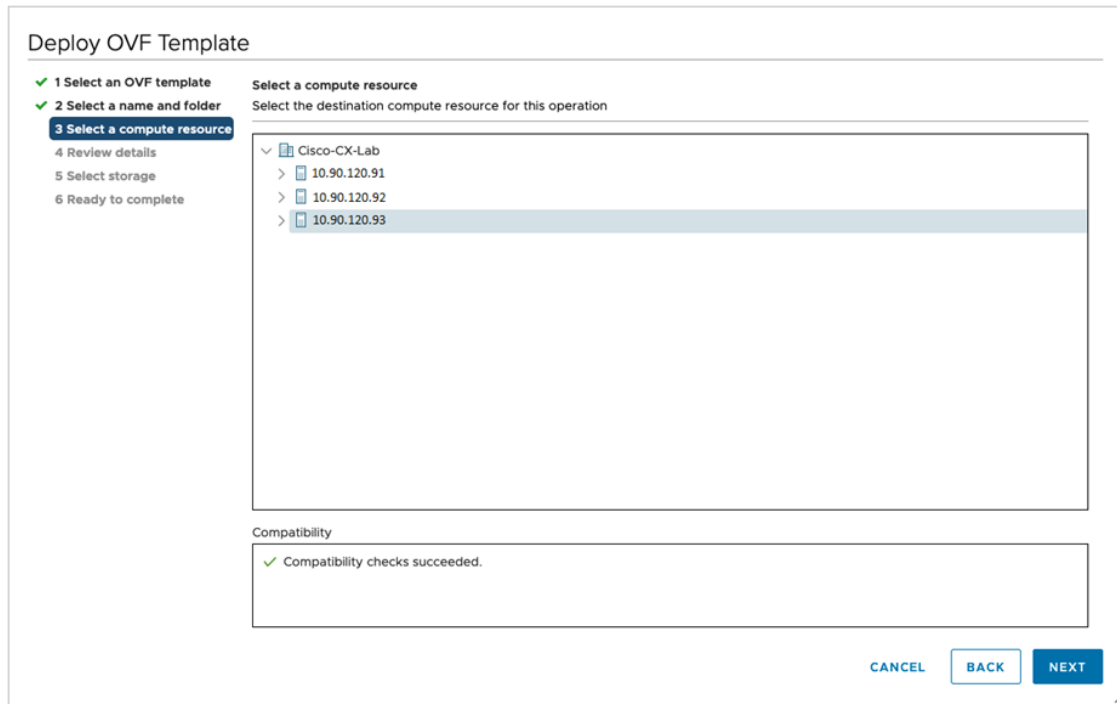
b) [仮想マシンの場所を選択 (Select a location for the virtual machine)] リストで、Crosswork Data Gateway を展開するデータセンターを選択します。

図 2: [OVFテンプレートの展開 (Deploy OVF Template)] - [名前とフォルダの選択 (Name and Folder Selection)] ウィンドウ



ステップ 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。

図 3: [OVFテンプレートの展開 (Deploy OVF Template)] - [コンピュータリソースの選択 (Select a computer resource)] ウィンドウ

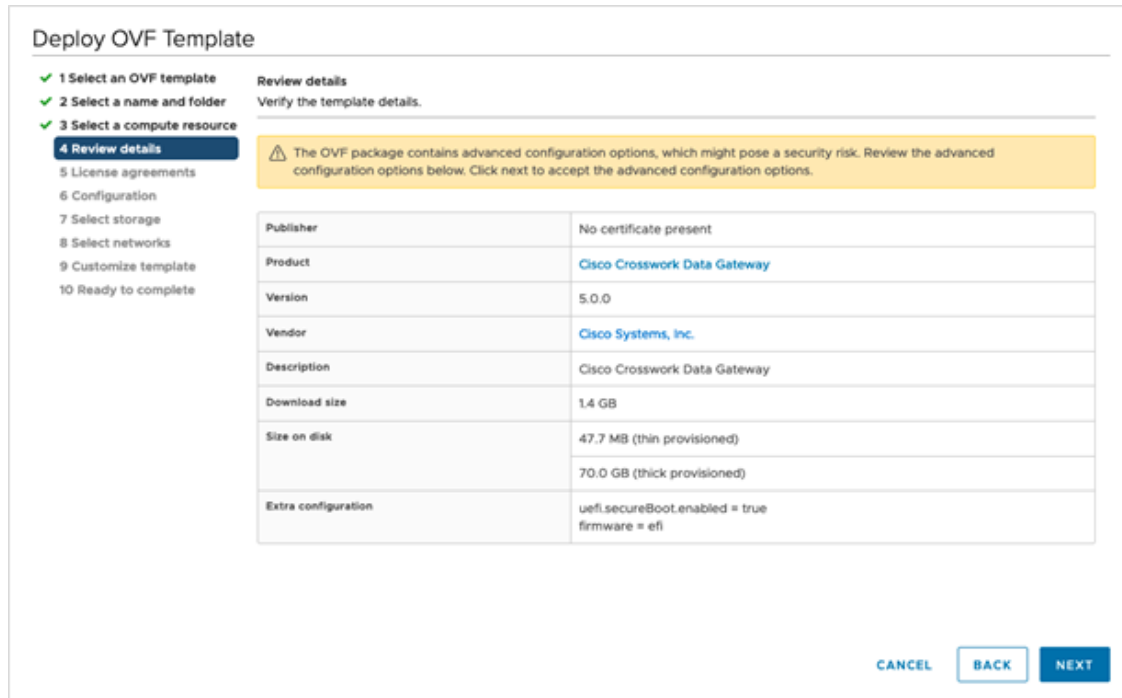


ステップ 8 [次へ (Next)] をクリックします。VMware vCenter Server が OVA を検証します。検証にかかる時間はネットワーク速度によって決まります。検証が完了すると、ウィザードは [4 詳細の確認 (4 Review details)] に移動します。OVA の情報を確認して [次へ (Next)] をクリックします。

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。ステップ 10 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。

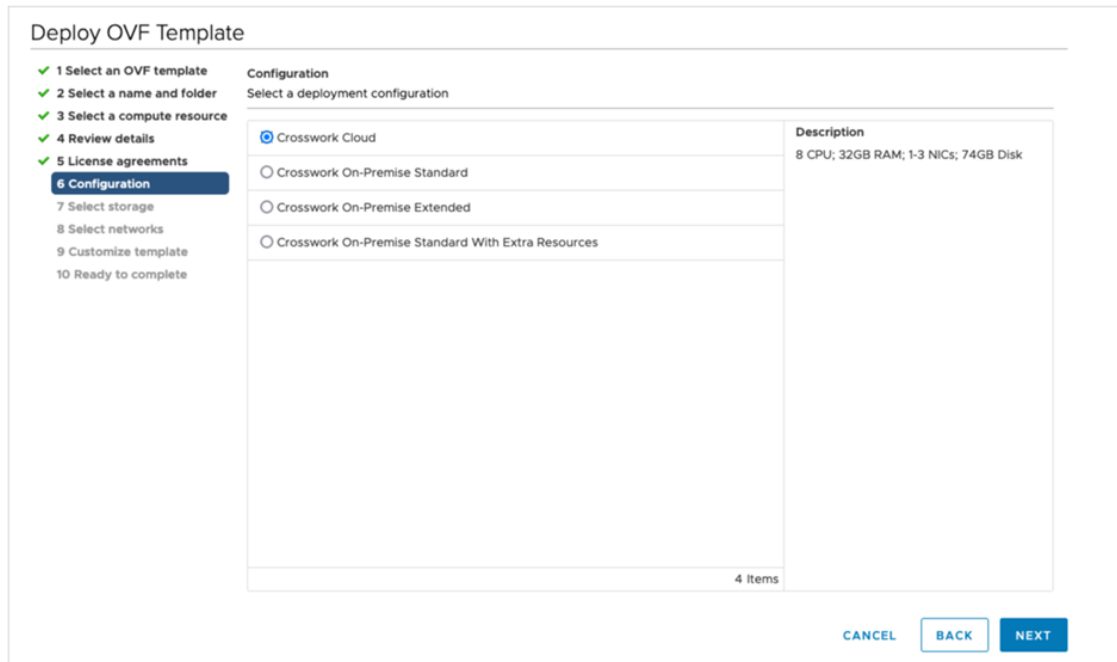
図 4: [OVFテンプレートの展開 (Deploy OVF Template)] - [詳細の確認 (Review details)] ウィンドウ



ステップ 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。

図 5: [OVFテンプレートの展開 (Deploy OVF Template)] - [設定 (Configuration)] ウィンドウ



- 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。

図 6: [OVFテンプレートの展開 (Deploy OVF Template)] - [ストレージの選択 (Select storage)] ウィンドウ

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed ▾

VM Storage Policy: Datastore Default ▾

Name	Capacity	Provisioned	Free	Type
Local Datastore	2.45 TB	1.19 TB	1.46 TB	VM

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

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。ページの上にあるドロップダウンから、各インターフェイスに適切な vNIC ロールを選択します。

ネットワークに使用される名前は、環境が最初にどのように構成されたかによって異なります。インストールパラメータを確認するときに構成した設定に基づいて、[ステップ 13](#) の名前を変更できます。

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してください。

(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。

図 7: [OVFテンプレートの展開 (Deploy OVF Template)] - [ネットワークの選択 (Select networks)] ウィンドウ

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
vNIC3	VM Network
vNIC2	VM Network
vNIC1	VM Network
vNIC0	VM Network

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL
BACK
NEXT

注目 Crosswork は vNIC3 ネットワークをサポートしていません。

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 (9 Customize template)] に移動します。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 (15 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時、「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。

(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。

図 8: [OVFテンプレートの展開 (Deploy OVF Template)] - [テンプレートのカスタマイズ (Customize template)] > [ホスト情報 (Host information)] ウィンドウ

The screenshot shows the 'Deploy OVF Template' wizard in the 'Customize template' step. The left sidebar lists steps 1 through 10, with '9 Customize template' selected. The main area is titled '01. Host Information' and contains the following fields:

- a. Hostname ***: A text input field containing 'CDG01'. The label indicates: 'Please enter the server's hostname (dg.localdomain)'. Below the field is the text 'CDG01'.
- b. Description ***: A text input field containing 'CDG 01'. The label indicates: 'Please enter a short, user friendly description for display in the Crosswork Controller'.
- c. Crosswork Data Gateway Label**: A text input field. The label indicates: 'An optional freeform label used by the Crosswork Controller to categorize and group multiple DG instances'.
- d. Allow Usable RFC 8190 Addresses**: A dropdown menu set to 'Yes'. The label indicates: 'If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC 8190 or its predecessors, reject, accept, or request confirmation during initial configuration'.
- e. Crosswork Data Gateway Private Key URI**: A text input field. The label indicates: 'Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP (user@host:/path/to/file)'.
- f. Crosswork Data Gateway Certificate File ID**: A text input field.

At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

図 9: [OVFテンプレートの展開 (Deploy OVF Template)] - [テンプレートのカスタマイズ (Customize template)] > [ホスト情報 (Host information)] ウィンドウ > [高可用性ネットワークモード (High Availability Network Mode)]

The screenshot shows the 'Deploy OVF Template' wizard in the 'Customize template' step, specifically the 'High Availability Network Mode' section. The left sidebar is the same as in Figure 8. The main area contains the following fields:

- h. Data Disk Size**: A dropdown menu set to '24'. The label indicates: 'Data disk size in GB mounted as /opt/dg/appdata'.
- i. Amazon Web Services IAM Role Name**: A text input field. The label indicates: 'Please enter the AWS IAM role name to use for sending VIP updates. This is required when deploying on AWS EC2'.
- j. High Availability Network Mode**: A dropdown menu with 'L2' selected. The label indicates: 'Select the network mode to use with external load balancers. This will determine whether all interfaces require an address.' Below the dropdown is a small warning icon.

Below this section, a new section '02. Passphrases' is visible, containing:

- a. dg-admin Passphrase ***: A password input field with a red error indicator. The label indicates: 'Please enter a passphrase for the dg-admin user. It must be at least 8 characters.' Below the field are 'Password' and 'Confirm Password' labels.

重要 1つまたは2つのNICを使用する場合は、vNIC0のみを構成する必要があります。3つのNICのセットアップの場合、vNIC0とvNIC1の両方を構成する必要があります。

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

- [03. vNICロールの割り当て (03. vNIC Role Assignment)] セクションで、すべてのロールを eth0 に設定します。

図 10 : [OVFテンプレートの展開 (Deploy OVF Template)] - [単一のvNIC展開用のテンプレートのカスタマイズ (Customize Template for Single vNIC deployment)]

Deploy OVF Template

<ul style="list-style-type: none"> ✓ 1 Select an OVF template ✓ 2 Select a name and folder ✓ 3 Select a compute resource ✓ 4 Review details ✓ 5 License agreements ✓ 6 Configuration ✓ 7 Select storage ✓ 8 Select networks <li style="background-color: #0070C0; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<table border="1"> <thead> <tr style="background-color: #D9E1F2;"> <th colspan="2">03. vNIC Role Assignment</th> <th>7 settings</th> </tr> </thead> <tbody> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic</td> <td>eth0 ▾</td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM</td> <td>eth0 ▾</td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server</td> <td>eth0 ▾</td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrollment and other management traffic</td> <td>eth0 ▾</td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration</td> <td>eth0 ▾</td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations</td> <td>eth0 ▾</td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices</td> <td>eth0 ▾</td> </tr> </tbody> </table>	03. vNIC Role Assignment		7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic	eth0 ▾	b. Administration	The interface used for SSH access to the VM	eth0 ▾	c. External Logging	The interface used to send logs to an external logging server	eth0 ▾	d. Management	The interface used for enrollment and other management traffic	eth0 ▾	e. Control	The interface used for destination, device, and collection configuration	eth0 ▾	g. Northbound External Data	The interface used to send collection data to external destinations	eth0 ▾	h. Southbound Data	The interface used collect data from all devices	eth0 ▾
03. vNIC Role Assignment		7 settings																							
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic	eth0 ▾																							
b. Administration	The interface used for SSH access to the VM	eth0 ▾																							
c. External Logging	The interface used to send logs to an external logging server	eth0 ▾																							
d. Management	The interface used for enrollment and other management traffic	eth0 ▾																							
e. Control	The interface used for destination, device, and collection configuration	eth0 ▾																							
g. Northbound External Data	The interface used to send collection data to external destinations	eth0 ▾																							
h. Southbound Data	The interface used collect data from all devices	eth0 ▾																							

図 11 : [OVFテンプレートの展開 (Deploy OVF Template)] - [2つのvNIC展開用のテンプレートのカスタマイズ (Customize Template for Two vNIC deployment)]

Deploy OVF Template

<ul style="list-style-type: none"> ✓ 1 Select an OVF template ✓ 2 Select a name and folder ✓ 3 Select a compute resource ✓ 4 Review details ✓ 5 License agreements ✓ 6 Configuration ✓ 7 Select storage ✓ 8 Select networks <li style="background-color: #0070C0; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<table border="1"> <thead> <tr style="background-color: #D9E1F2;"> <th colspan="2">03. vNIC Role Assignment</th> <th>7 settings</th> </tr> </thead> <tbody> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic</td> <td>eth0 ▾</td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM</td> <td>eth0 ▾</td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server</td> <td>eth0 ▾</td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrollment and other management traffic</td> <td>eth0 ▾</td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration</td> <td>eth1 ▾</td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations</td> <td>eth1 ▾</td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices</td> <td>eth1 ▾</td> </tr> </tbody> </table>	03. vNIC Role Assignment		7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic	eth0 ▾	b. Administration	The interface used for SSH access to the VM	eth0 ▾	c. External Logging	The interface used to send logs to an external logging server	eth0 ▾	d. Management	The interface used for enrollment and other management traffic	eth0 ▾	e. Control	The interface used for destination, device, and collection configuration	eth1 ▾	g. Northbound External Data	The interface used to send collection data to external destinations	eth1 ▾	h. Southbound Data	The interface used collect data from all devices	eth1 ▾
03. vNIC Role Assignment		7 settings																							
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic	eth0 ▾																							
b. Administration	The interface used for SSH access to the VM	eth0 ▾																							
c. External Logging	The interface used to send logs to an external logging server	eth0 ▾																							
d. Management	The interface used for enrollment and other management traffic	eth0 ▾																							
e. Control	The interface used for destination, device, and collection configuration	eth1 ▾																							
g. Northbound External Data	The interface used to send collection data to external destinations	eth1 ▾																							
h. Southbound Data	The interface used collect data from all devices	eth1 ▾																							

図 12: [OVFテンプレートの展開 (Deploy OVF Template)] - [3つのvNIC展開用のテンプレートのカスタマイズ (Customize Template for 3 vNICs deployment)]

03. vNIC Role Assignment		7 settings
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic	eth0
b. Administration	The interface used for SSH access to the VM	eth0
c. External Logging	The interface used to send logs to an external logging server	eth0
d. Management	The interface used for enrollment and other management traffic	eth0
e. Control	The interface used for destination, device, and collection configuration	eth1
g. Northbound External Data	The interface used to send collection data to external destinations	eth1
h. Southbound Data	The interface used collect data from all devices	eth2

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なら [終了 (Finish)] をクリックします。

図 13: [OVFテンプレートの展開 (Deploy OVF Template)] - [準備完了 (Ready to Complete)] ウィンドウ

Ready to complete	
Click Finish to start creation.	
Provisioning type	Deploy from template
Name	CDG02
Template name	d9g
Download size	1.4 GB
Size on disk	70.0 GB
Folder	Cisco-CX-Lab
Resource	10.90.147.99
Storage mapping	1
All disks	Datastore: Datastore2; Format: Thick provision lazy zeroed
Network mapping	4
vNIC3	Crosswork-Devices
vNIC2	Crosswork-Devices
vNIC1	Crosswork-Devices
vNIC0	VM Network

CANCEL BACK FINISH

ステップ 15 展開が完了するまで待つから続行します。展開ステータスを確認するには、次の手順を実行します。

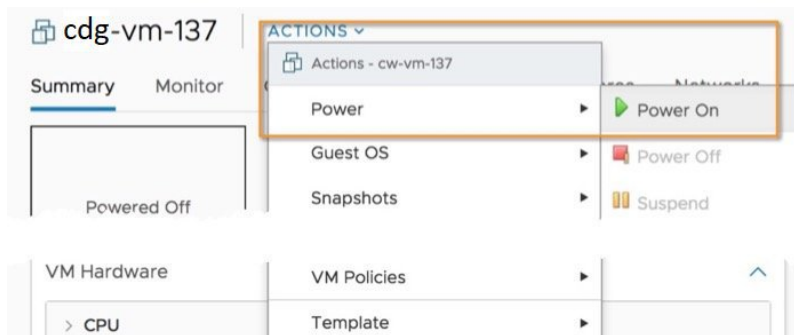
a) vCenter vSphere クライアントを開きます。

- 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 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 をクリックしてから右クリックし、[アクション (Actions)]>[電源 (Power)]>[電源オン (Power On)] の順に選択します。

図 14: 電源投入時の動作



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、その新しい VM を Crosswork Cloud に再登録します。

Crosswork Data Gateway がインストールされていることを確認します。検証を実行する方法の詳細については、[Crosswork Data Gateway がインストールされていることを確認する \(50 ページ\)](#) を参照してください。

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。[登録パッケージの入手 \(109 ページ\)](#) 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、スクリプトの必須またはオプションのパラメータのリストを変更し、OVF ツールを実行する必要があります。インストールパラメータとそのデフォルト値のリストについては、[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 \(15 ページ\)](#) を参照してください。



- (注) スクリプトを作成するときに、すべての必須パラメータおよびオプションのパラメータを目的の値で指定するようにしてください。スクリプトに含まれていないパラメータは、展開のデフォルト値と見なされます。

SSH で Cisco Crosswork Data Gateway VM にログインするには、次の手順を実行します。

始める前に

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

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

ステップ 1 cisco.com から OVA およびサンプルスクリプトファイルをダウンロードします。これらの手順では、ファイル名 `cw-na-dg-5.0.0-45-release-20230418.uefi.ova` および `cw-na-dg-5.0.0-sample-install-scripts.tar.gz` を使用します。`cw-na-dg-5.0.0-sample-install-scripts.tar.gz` には、1 つ、2 つ、および 3 つの vNIC 展開用のサンプルスクリプトが含まれており、ニーズに合わせて最適化できます。

ステップ 2 次のコマンドを使用して、OVA バンドルを解凍します。

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

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

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

ステップ 4 使用する展開に対応するサンプルスクリプトを選択します。シスコは、ニーズに合わせて最適化できる 3 つの vNIC 展開用のサンプルスクリプトを提供しています。「[Cisco Crosswork Data Gateway IPv4 展開のためのサンプルスクリプト \(48 ページ\)](#)」を参照してください。

- (注) サンプルのシェルスクリプトには、必須オプションのみが含まれています。OVF Tool コマンドのオプションパラメータをカスタマイズする場合は、[表 7: 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 \(16 ページ\)](#) でこれらのパラメータの詳細を確認してください。

ステップ 5 次のコマンドを使用して、スクリプトを実行可能にします。

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

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

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

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

次に例を示します。

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

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

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

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

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

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

インストールが完了すると、Crosswork Data Gateway VM の電源がオンになります。

次のタスク

VM にログインします。詳細については、[Crosswork Data Gateway VM へのログインとログアウト \(50 ページ\)](#) を参照してください。ログインすると、Crosswork Data Gateway にインストールが完了したことを示すウェルカム画面とオプションメニューが表示されます。ログアウトし、[Crosswork Data Gateway VM からのログアウト \(52 ページ\)](#) で説明するインストール後のタスクに進みます。

Crosswork Cloud での Crosswork Data Gateway の登録に進みます [登録パッケージの入手 \(109 ページ\)](#) を参照してください。

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

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



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

```

#!/usr/bin/env bash
DM=""
Disclaimer=""
DNSv4=""
NTP=""
Domain=""
Hostname=""

VM_NAME=""
DeploymentOption="cloud"
DS=""
Host=""
ManagementNetwork=""
DataNetwork=""
DeviceNetwork=""
ManagementIPv4Address=""
ManagementIPv4Netmask=""
ManagementIPv4Gateway=""
DataIPv4Address=""
DataIPv4Netmask=""
DataIPv4Gateway=""
DeviceIPv4Address=""
DeviceIPv4Netmask=""
DeviceIPv4Gateway=""
dgadminpwd=""
dgoperpwd=""
URI=""
Passphrase=""

ROBOT_OVA_PATH=$1

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

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"EnrollmentURI=${URI}" \
--prop:"EnrollmentPassphrase=${Passphrase}" \
--prop:"Vnic0IPv4Method=Static" \
--prop:"Vnic0IPv4Address=${ManagementIPv4Address}" \
--prop:"Vnic0IPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"Vnic0IPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$ROBOT_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

```

Crosswork Data Gateway がインストールされていることを確認する

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

#####
Append section below for three NIC deployment
#####
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic2IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \
#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \
#--prop:"Vnic2IPv4Address=${DeviceIPv4Address}" \
#--prop:"Vnic2IPv4Gateway=${DeviceIPv4Gateway}" \
#--prop:"Vnic2IPv4Netmask=${DeviceIPv4Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \
```

Crosswork Data Gateway がインストールされていることを確認する

Crosswork Data Gateway が vCenter を介して正常にインストールされていることを確認できます。

次の手順を実行して、Crosswork Data Gateway がインストールされていることを確認します。

-
- ステップ 1 vCenter 経由で Crosswork Data Gateway VM にログインします。
 - ステップ 2 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。
 - ステップ 3 ユーザー名 (割り当てられたロールに応じて dg-admin または dg-oper) と、対応するパスワード (インストールプロセスで作成したパスワード) を入力し、**Enter** を押します。
-

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

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

- [vCenter を介した Crosswork Data Gateway へのアクセス \(51 ページ\)](#)

- [SSH による Crosswork Data Gateway VM へのアクセス \(51 ページ\)](#)

Crosswork Data Gateway VM からログアウトするには、[Crosswork Data Gateway VM からのログアウト \(52 ページ\)](#) を参照してください。

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

vCenter 経由でログインするには、次の手順を実行します。

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

Crosswork Data Gateway コンソールが起動します。

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

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

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

SSH で Cisco Crosswork Data Gateway VM にログインするには、次の手順を実行します。

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

```
ssh <username>@<ManagementNetworkIP>
```

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

次の例を参考にしてください。

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

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

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

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

Crosswork Data Gateway VM からのログアウト

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。

OpenStack プラットフォームへの Crosswork Data Gateway のインストール

次のいずれかの方法で OpenStack プラットフォームに Crosswork Data Gateway をインストールできます。

- [OpenStack CLI を使用した OpenStack への Crosswork Data Gateway のインストール \(52 ページ\)](#)
- [OpenStack UI を使用した OpenStack への Crosswork Data Gateway のインストール \(67 ページ\)](#)

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 \(15 ページ\)](#) を参照してください。
- 1 つ以上の 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](https://www.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。これらの手順では、パッケージ名 **cw-na-dg-5.0.0-signed-qcow2.uefi.tar.gz** および **cw-na-dg-5.0.0-sample-install-scripts.tar.gz** を使用します。
- b) 次のコマンドを使用して、インストーラバンドルを解凍します。

```
tar -xvzf cw-na-dg-5.0.0-signed-qcow2.uefi.tar.gz
```

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。

```
README
cw-na-dg-5.0.0-45-release-20230418.uefi.tar.gz.signature
cw-na-dg-5.0.0-45-release-20230418.uefi.tar.gz
cisco_x509_verify_release.py3
cisco_x509_verify_release
CDG-CCO_RELEASE
```

- 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](https://www.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](https://www.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
```

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 \(15 ページ\)](#) 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 NIC を 1 つ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。

```
#### Required Parameters
### Deployment Settings
```

```
## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address:::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64
```

```
## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=: :1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
  role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
  DG instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC
8190 or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
  (user@host:/path/to/file)
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
  using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
  certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False
```

```
## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
# list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
# the Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
```

```
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File
URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
```

```
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

- 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 \(15 ページ\)](#) を参照してください。

DHCP を使用して、ホスト名 cdg1-nodhcp で NIC を 1 つ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。

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0
```

```
## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
  role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
  DG instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC
8190 or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
```

```
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
(user@host:/path/to/file)
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
```

```
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
the Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted certificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=
```

```
## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File
URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
```

```
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

- 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-5.0.0-65-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) 24 GB/秒のデータディスクを作成します。

```
openstack volume create --size
```

コマンド例 :

```
openstack volume create --size 24 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 1 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
```

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
```

- 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 1 つ以上の 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 NIC を 1 つ備えた 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>
--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
--config-drive True --user-data config-nodhcp-cdgl.txt --block-device-mapping
vdb=cdgl:::true cdgl-nodhcp
```

または

```
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 NIC を 1 つ備えた 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 <flavor_name> --image <image_name> --network <network1>
--config-drive True --user-data <config.txt> --host <boot_drive>
--block-device-mapping vdb=<volume_name>:::true <CDG_hostname>
```

または

```
openstack server create --config-drive true --flavor cdg --image --key-name default --network
--security-group --user-data
```

(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= ; network3-nodhcp=	cdg-cloud-bios-345	cdg-cloud
9c6d913f-c24b-43a3-9816-f865e58e7e95	cdg-bios-nodhcp	ACTIVE	network1-nodhcp= ; network2-nodhcp= ; network3-nodhcp=	cdg-cloud-bios-345	cdg-cloud

VM のステータスが [アクティブ (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 [登録パッケージの入手（109 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（15 ページ）](#) を参照してください。
- 1 つ以上の 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](https://www.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。これらの手順では、パッケージ名 **cw-na-dg-5.0.0-signed-qcow2.uefi.tar.gz** および **cw-na-dg-5.0.0-sample-install-scripts.tar.gz** を使用します。
- b) 次のコマンドを使用して、インストーラバンドルを解凍します。

```
tar -xvzf cw-na-dg-5.0.0-signed-qcow2.uefi.tar.gz
```

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。

```
README
cw-na-dg-5.0.0-45-release-20230418.uefi.tar.gz.signature
cw-na-dg-5.0.0-45-release-20230418.uefi.tar.gz
cisco_x509_verify_release.py3
cisco_x509_verify_release
CDG-CCO_RELEASE
```

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-5.0.0-65-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](https://www.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](https://www.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
```

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、[ステップ 3](#) または [ステップ 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 \(15 ページ\)](#) 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一 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 NIC を 1 つ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。

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
```

```
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or
services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=:0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or
```

```
services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=: :1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default
Gateway role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
DG instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC
8190 or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
(user@host:/path/to/file)
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
```

```
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
# list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
# the Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
# subjectAltName or subject common name
```

```
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted certificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent
to the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate
File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
EnrollmentURI=
```

```
## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

- 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、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 \(15 ページ\)](#) 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 NIC を 1 つ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。

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0
```



```
## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or
services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=:0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or
services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=:1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default
Gateway role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
DG instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC
```

```
8190 or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
(user@host:/path/to/file)
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
```

```
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
  the Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
  subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
  (user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
  the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent
  to the proxy server
```

```
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate
File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0
```

```
## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

- 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す保存します。
- 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 (VCPU)]、[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。

図 15: [フレーバー情報 (Flavor Information)] ウィンドウ

Flavor Information * Flavor Access

Name *
cdg-cloud-flavor

ID ⓘ
auto

VCPUs *
8

RAM (MB) *
32768

Root Disk (GB) *
50

Ephemeral Disk (GB)
24

Swap Disk (MB)
0

RX/TX Factor
1

Flavors define the sizes for RAM, disk, number of cores, and other resources and can be selected when users deploy instances.

Cancel Create Flavor

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。

図 16: [イメージの作成 (Create Image)] ウィンドウ

Create Image

Image Details

Specify an image to upload to the Image Service.

Image Name
cdg_bios_image

Image Description

Image Source

File*
Browse... cw-na-dg-4.0.0-6-TESTONLY-2022072

Format*
QCOW2 - QEMU Emulator

Image Requirements

Kernel
Choose an image

Ramdisk
Choose an image

Architecture

Minimum Disk (GB)
0

Minimum RAM (MB)
0

Image Sharing

Visibility
Private Shared **Public** Community

Protected
Yes **No**

Cancel < Back Next > Create Image

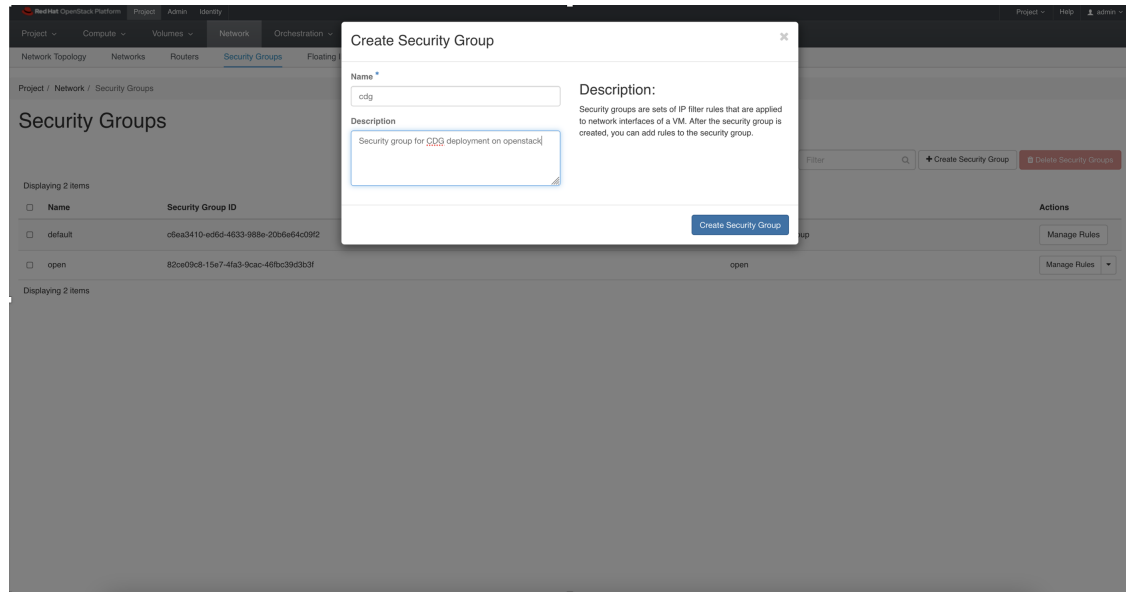
ステップ 8 着信 TCP/UDP/ICMP 接続を許可するセキュリティポリシーを作成します。

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。

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

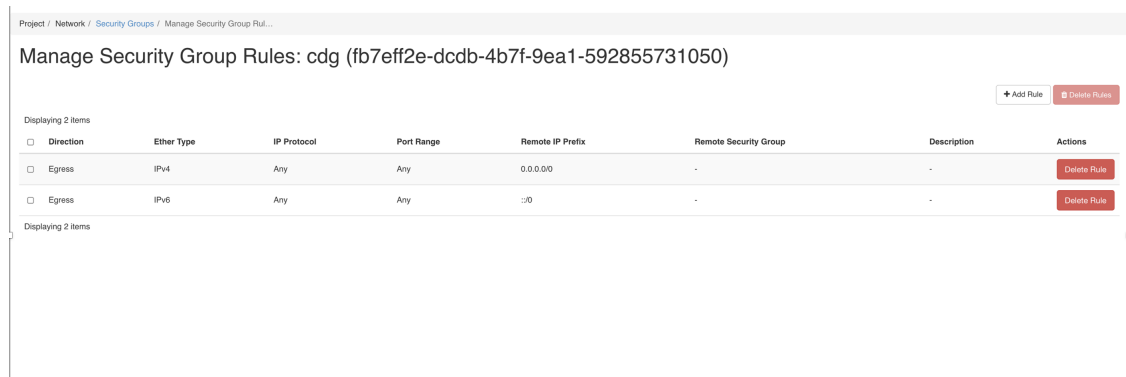
図 17: [セキュリティグループの作成 (Create Security Group)] ウィンドウ



- 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。

図 18: [セキュリティグループルールの管理 (Manage Security Group Rules)] ウィンドウ



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。

図 19: [ポートの作成 (Create Port)] ウィンドウ

Create Port

Info Security Groups

Name
mgmt-port1

Description:
You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.

Enable Admin State

Device ID

Device Owner

Specify IP address or subnet
Fixed IP Address

Fixed IP Address*
192.168.1.101

MAC Address

Port Security

VNIC Type
Normal

Binding: Host

Cancel Create

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一名前を入力することを推奨します。

図 20: [インスタンスの起動 (Launch Instance)] ウィンドウ

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。

図 21: [インスタンスの起動 (Launch Instance)] ウィンドウ - [ソース (Source)] タブ

Launch Instance

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source **Create New Volume**

Image

Allocated

Displaying 1 item

Name	Updated	Size	Format	Visibility
> cdg-cloud-bios-6	7/22/22 5:03 AM	1.41 GB	QCOW2	Public

Available Select one

Q Click here for filters or full text search.

Displaying 1 item

Name	Updated	Size	Format	Visibility
> cdg-cloud-uefi-6	7/22/22 5:14 AM	1.41 GB	QCOW2	Public

Displaying 1 item


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  をクリックし、[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。

図 22: [インスタンスの起動 (Launch Instance)]ウィンドウ -[フレーバー (Flavor)]タブ

Launch Instance

Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
cdg-cloud	8	32 GB	50 GB	50 GB	0 GB	Yes


Available 0

Select one

Q Click here for filters or full text search.

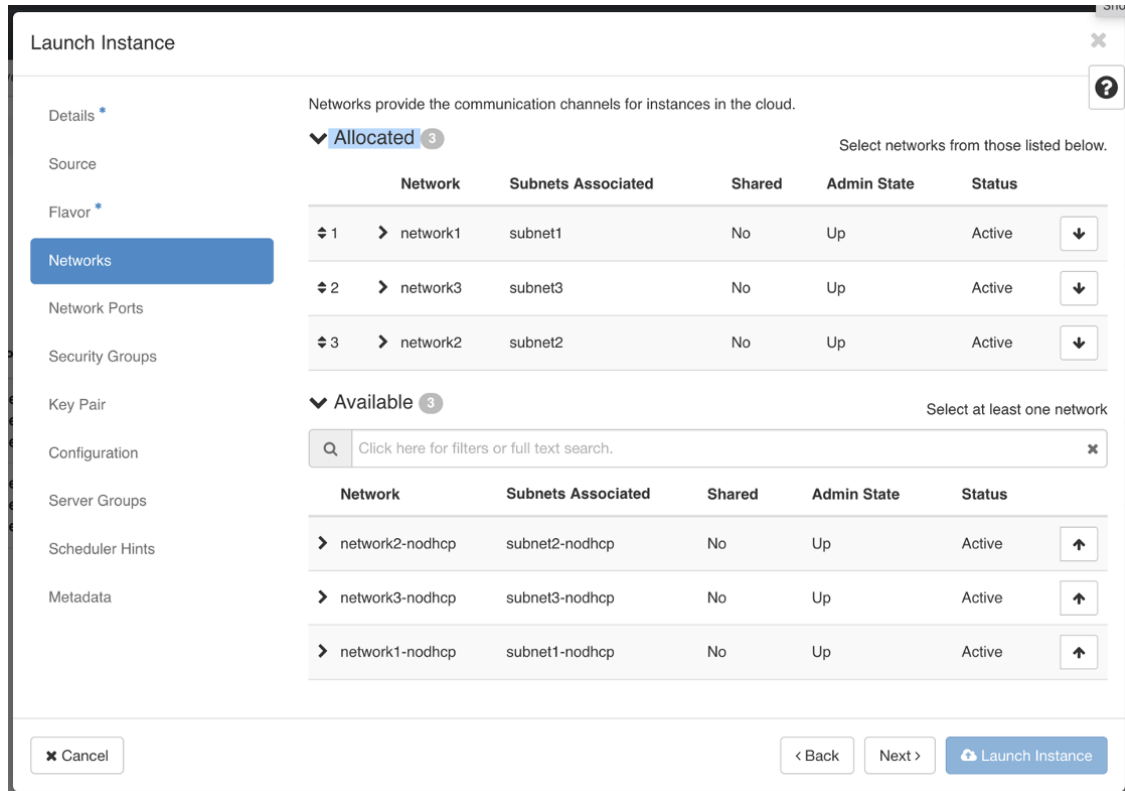
Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
------	-------	-----	------------	-----------	----------------	--------

Cancel < Back Next > Launch Instance

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。

図 23: [インスタンスの起動 (Launch Instance)]ウィンドウ - [ネットワーク (Networks)]タブ



ステップ 15 ポートを VM に割り当てます。


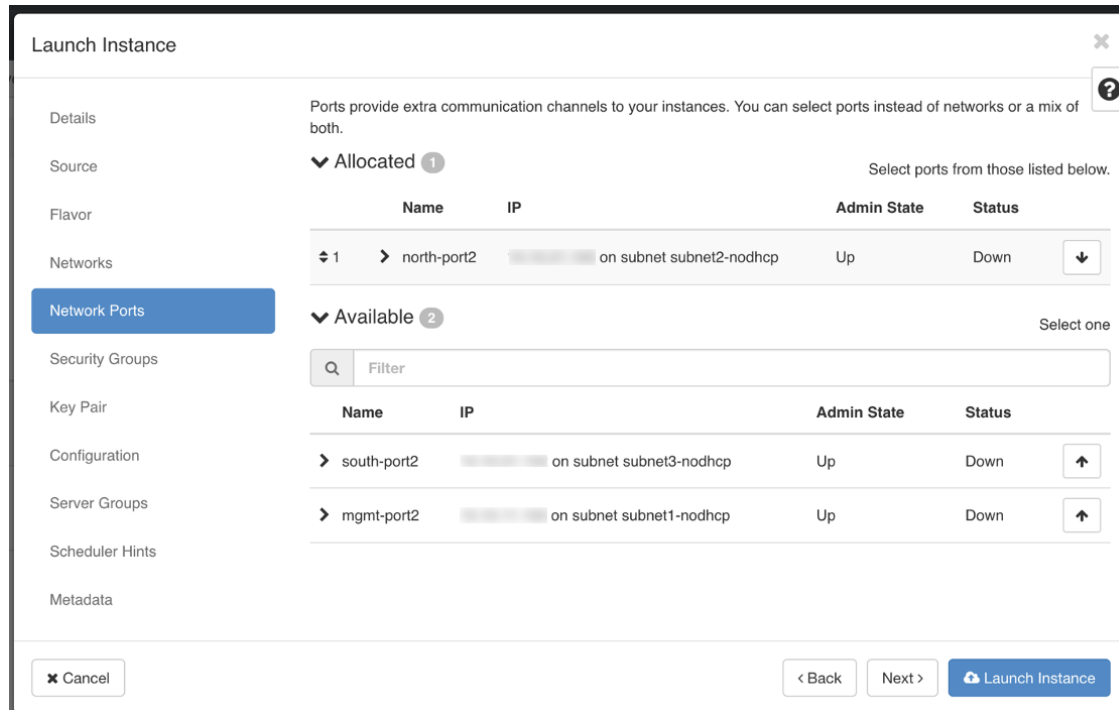
[使用可能 (Available)]ペインに表示されているポートのリストから、 をクリックしてポートを [割り当て済み (Allocated)]ペインに移動します。

図 24: [インスタンスの起動 (Launch Instance)] ウィンドウ - [ネットワークポート (Network Ports)] タブ



[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。

図 25: [インスタンスの起動 (Launch Instance)] ウィンドウ - [セキュリティグループ (Security Groups)] タブ

Launch Instance

Select the security groups to launch the instance in.

▼ Allocated 2

Name	Description
▼ default	Default security group

Direction	Ether Type	Protocol	Min Port	Max Port	Remote
egress	IPv4	-	-	-	0.0.0.0/0
ingress	IPv4	-	-	-	-
ingress	IPv6	-	-	-	-
egress	IPv6	-	-	-	::/0

Name	Description
▼ cdg	Security group for CDG deployment on openstack

Direction	Ether Type	Protocol	Min Port	Max Port	Remote
egress	IPv6	-	-	-	::/0
egress	IPv4	-	-	-	0.0.0.0/0

▼ Available 1 Select one or more

Q Click here for filters or full text search.

Name	Description
> open	open

✕ Cancel < Back Next > Launch Instance

[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。

図 26: [インスタンスの起動 (Launch Instance)] ウィンドウ - [構成 (Configuration)] タブ

Launch Instance

Details You can customize your instance after it has launched using the options available here. "Customization Script" is analogous to "User Data" in other systems.

Source Load Customization Script from a file
Choose File No file chosen

Flavor Customization Script (Modified) Content size: 1.48 KB of 16.00 KB

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

ActiveVnics=3
AllowRFC190=Yes
AuditAddress=
AuditPort=60
ControllerCertChainPwd=
ControllerIP=10.10.10.201
ControllerPort=30607
ControllerSignCertChain=
ControllerSignCertChain=

Disk Partition
Automatic

Configuration Drive

Cancel < Back Next > Launch Instance

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。

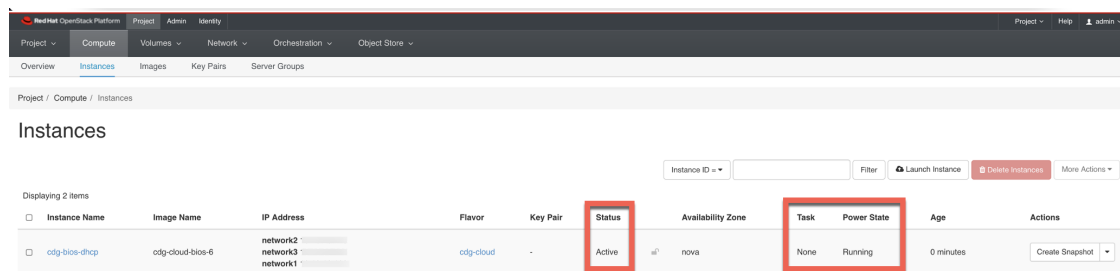
図 27: [インスタンス (Instances)] ウィンドウ - [CDG VMインストールのステータス (Status of CDG VM Installation)]

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
cdg-bios-dhcp	cdg-cloud-bios-6	network2 network3 network1	Not available	-	Build	nova	Spawning	No State	0 minutes	Associate Floating IP

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。

- 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。

図 28: [インスタンス (Instances)] ウィンドウ - [CDG VM インストールのステータス (Status of CDG VM Installation)]



- [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。
- 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 \(109 ページ\)](#) を参照してください。

Amazon EC2 に Crosswork Data Gateway をインストールする

次のいずれかの方法で Amazon EC2 に Crosswork Data Gateway をインストールできます。

- CloudFormation (CF) テンプレートを使用した Crosswork Data Gateway のインストール (92 ページ)
- Amazon EC2 に Crosswork Data Gateway を手動でインストールする (99 ページ)

CloudFormation (CF) テンプレートを使用した Crosswork Data Gateway のインストール

- [CF テンプレート画像の抽出 \(92 ページ\)](#)
- [ロールとポリシーの権限 \(93 ページ\)](#)
- [Crosswork Data Gateway をインストールするための CF テンプレートのパラメータ \(94 ページ\)](#)
- [CF テンプレートの展開の管理 \(97 ページ\)](#)

CF テンプレート画像の抽出

このセクションでは、Crosswork Data Gateway テンプレート画像を抽出して検証する手順について説明します。



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

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

ステップ 2 次のコマンドを使用して、パッケージを解凍します。

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

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

次に例を示します。

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

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

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

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

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

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

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

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

次に例を示します。

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

パッケージの内容が抽出され、正常に検証されます。

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

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

ロールとポリシーの権限

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

表 8: Amazon EC2 のロールと、ロールに割り当てられたアクション

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

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

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

表 9: Crosswork Data Gateway 展開パラメータ

パラメータ	Description
VpcId	既存の仮想プライベートクラウド (VPC) の VPC ID。たとえば、vpc-0f83aac74690101a3 です。
SecGroup	スタックに適用する必要がある事前に作成されたセキュリティグループ。たとえば、sg-096ff4bc355af16a0 です。グループは、Crosswork、NSO、Crosswork Data Gateway、および IOS-XR が使用するすべてのポートへの入力アクセスを許可する必要があります。
CDGSSHPassword	Crosswork Data Gateway ノードで設定する SSH パスワード。
CDGOperPassword	Dg-Oper ユーザー用に Crosswork Data Gateway に設定するパスワード。
CDGAmiId	Crosswork Data Gateway AMI ID。
InstanceType	ノードインスタンスの EC2 インスタンスタイプ。 デフォルト値は m5.2xlarge です。 これは必須パラメータです。
CNCControllerIP	Crosswork Data Gateway コントローラのホストアドレス。 これは必須パラメータです。
CNCControllerPassword	Crosswork または CNC コントローラにアクセスするために使用される cw-admin ユーザーのパスワード。
InterfaceDeploymentMode	Crosswork Data Gateway の展開モード。 次のオプションがあります。 <ul style="list-style-type: none"> • 1: すべてのインターフェイスを展開します。 • 2: 管理およびデータインターフェイスを展開します。 • 3: 管理、データ、および制御インターフェイスを展開します。

パラメータ	Description
CDGInterface0IPAddress	サブネットのフリー IP アドレス。0.0.0.0 に設定すると、IP アドレスが自動的に割り当てられます。 これは必須パラメータです。
CDGInterface0SubnetId	Crosswork Data Gateway VM の最初のインターフェイスサブネット。
CDGInterface0Gateway	選択したサブネットのデフォルトゲートウェイ。通常、サブネットの最初のアドレスです。
CDGInterface0SubnetNetmask	ドット付き 10 進数形式の最初のインターフェイス サブネット ネットマスク。たとえば、255.255.255.0 と指定します。 これは必須パラメータです。
CDGInterface1IPAddress	最初のサブネットのフリー IP アドレス。0.0.0.0 に設定すると、IP アドレスが自動的に割り当てられます。 これは必須パラメータです。
CDGInterface1SubnetId	Crosswork Data Gateway の 2 番目のインターフェイスサブネット。サブネットは、CDGInterface0SubnetId と同じ可用性ゾーンにある必要があります。
CDGInterface1Gateway	選択したサブネット上の 2 番目のインターフェイスのデフォルトゲートウェイ。通常、サブネットの最初のアドレスです。 これは必須パラメータです。
CDGInterface1SubnetNetmask	ドット付き 10 進数形式の 2 番目のインターフェイス サブネット ネットマスク。たとえば、255.255.255.0 と指定します。デュアルインターフェイス モードが使用されていない場合、このパラメータは無視されます。 これは必須パラメータです。
CDGInterface2IPAddress	2 番目のサブネット上のフリー IP アドレス。0.0.0.0 に設定すると、IP アドレスが自動的に割り当てられます。 これは必須パラメータです。
CDGInterface2SubnetId	Crosswork Data Gateway VM の 3 番目のインターフェイスサブネット。サブネットは、CDGInterface0SubnetId と同じ可用性ゾーンにある必要があります。
CDGInterface2Gateway	選択したサブネット上の 3 番目のインターフェイスのデフォルトゲートウェイ。通常、サブネットの最初のアドレスです。 これは必須パラメータです。

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

パラメータ	Description
CDGInterface2SubnetNetmask	ドット付き 10 進数形式の 3 番目のインターフェイス サブネット ネットマスク。たとえば、255.255.255.0 と指定します。トリプル インターフェイス モードが使用されていない場合、このパラメータは無視されます。 これは必須パラメータです。
CNCControllerIP	Crosswork Data Gateway コントローラのホストアドレス。
HANetworkMode	Crosswork Data Gateway の HA モード。 プールモードのオプションは次のとおりです。 <ul style="list-style-type: none"> • L2：このオプションは、HA プールを作成するための IP アドレスを指定するときに使用します。 • L3：このオプションは、HA プールの作成とマルチサブネット展開のための FQDN を指定するときに使用します。
DataDiskSize	Crosswork データディスクのサイズ。最小サイズは 20 です。デフォルトサイズは 50 です。 これは必須パラメータです。
CDGProfile	Crosswork Data Gateway の展開プロファイル。 <ul style="list-style-type: none"> • Standard • Extended これは必須パラメータです。
CdgInstanceHostname	Crosswork Data Gateway インスタンス名 (CDG-01 など)。

表 10: Crosswork Data Gateway および Network Load Balancer (NLB) スタックパラメータ

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

パラメータ	Description
DomainName	ドメイン名。 これは必須パラメータです。
HostedZoneId	ホステッドゾーン ID。 これは必須パラメータです。
CdgPoolHostname	Route53 レコードの名前。 これは必須パラメータです。
CdgTargetIP1	管理ノードの IP アドレス 1。
CdgTargetIP2	管理ノードの IP アドレス 2。
LBIPAddress1	サブネット上の最初の LB IP アドレス。 これは必須パラメータです。
LBIPAddress2	サブネット上の 2 番目の LB IP アドレス。 これは必須パラメータです。

CF テンプレートの展開の管理

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

- [CF テンプレートの展開 \(97 ページ\)](#)
- [インストールのモニター \(99 ページ\)](#)

CF テンプレートの展開

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

始める前に

- Amazon EC2 に Crosswork Data Gateway をインストールするために規定された [Amazon EC2 設定 \(9 ページ\)](#) を満たしていることを確認してください。
- S3 バケットまたはローカルマシンに保存されている CloudFormation テンプレートにアクセスできることを確認します。テンプレートが Amazon S3 にある場合は、テンプレートファイルの URL をコピーしたままにしておきます。

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

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

ステップ 3 次の詳細を入力します。

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

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

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

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

ステップ 5 構成したパラメータ値を確認します。

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

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

ステップ 7 [送信 (Submit)] をクリックします。

次のタスク

クラスタの作成にかかる時間は、展開プロファイルのサイズとハードウェアのパフォーマンス特性によって異なることがあります。インストールのステータスを確認する方法については、[インストールのモニター \(99 ページ\)](#) を参照してください。

インストールのモニター

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

-
- ステップ 1** CloudFormation コンソールの左側の [スタック (Stacks)] ペインから、展開したスタックを選択します。
- ステップ 2** スタックの詳細が右側に表示されます。このウィンドウの各タブをクリックして、スタックの詳細を表示します。スタックの作成が進行中の場合、[イベント (Events)] タブのスタックのステータスは `CREATE_IN_PROGRESS` です。
- ステップ 3** スタックが作成されたら、次の手順を実行します。
- スタックのステータスが `CREATE_COMPLETE` に変わり、[論理ID (Logical ID)] にスタック名が表示されます。
 - [リソース (Resources)] タブには、物理 ID を含む、CF テンプレートが作成したすべてのリソースの詳細が表示されます。
 - [出力 (Outputs)] タブには、VM のインターフェイス IP アドレスの詳細が表示されます。
-

Amazon EC2 に Crosswork Data Gateway を手動でインストールする

次の手順を実行して、EC2 に Crosswork Data Gateway をインストールします。



- (注)
- インスタンスの起動ワークフローには、要件に基づいて構成できる幅広い起動オプションが用意されています。次の手順は、Crosswork Data Gateway VM を正常にインストールするために構成する必要がある必須設定を示しています。
 - この手順のステップでは、3つのインターフェイスを備えた Extended Crosswork Data Gateway VM のインストールについて説明します。
-

始める前に

Crosswork Data Gateway VM を展開する前に、次の情報が用意されていることを確認してください。

- [Amazon EC2 設定 \(9 ページ\)](#) に指定されている要件を満たしていることを確認します。
- すべての Cisco Crosswork VM がインストールされています。
- インストールする Crosswork Data Gateway VM インスタンスの数を決定します。
- Crosswork Data Gateway AMI イメージを AWS にアクセス可能な場所に保存します。

ステップ1 Crosswork Data Gateway VM のユーザーデータを準備します。

- a) Crosswork Data Gateway VM のユーザーデータを準備します。パラメータの詳細については、[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（15 ページ）](#)を参照してください。参考のために、VM のユーザーデータの例をここに添付します。重要なパラメータが強調表示されています。

```

AwsIamRole=changeme
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=changeme
ControllerIP=
ControllerPort=30607
ControllerSignCertChain=cw-admin@<controller-IP>:/home/cw-admin/controller.pem
ControllerTlsCertChain=
Deployment=Crosswork On-Premise
Description=changeme
DGAppdataDisk=5
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=Extended
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 //IP address of management interface
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=:0
Vnic0IPv6Gateway=:1

```

```
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=0.0.0.0 //IP address of data interface
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=None
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address>:::0
Vnic1IPv6Gateway>:::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=0.0.0.0 //leave unchanged to default value.
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=None
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address>:::0
Vnic2IPv6Gateway>:::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=changeme
dg-operPassword=changeme
```

- b) 前の手順を繰り返して、インストールする予定の Crosswork Data VM ごとにユーザーデータを作成します。

ステップ 2 Crosswork Data Gateway VM をインストールします。

- a) AWS にログインし、EC2 サービスを検索します。EC2 ダッシュボードが開きます。
- b) ダッシュボードの [インスタンスの起動 (Launch Instance)] ペインに移動し、[インスタンスの起動 (Launch Instance)] > [インスタンスの起動 (Launch Instance)] の順にクリックします。
- [インスタンスの起動 (Launch an Instance)] ウィンドウが表示されます。
- c) [名前とタグ (Name and tags)] セクションで、Crosswork Data Gateway VM の名前を入力します。
- d) [アプリケーションおよびOSイメージ (Amazon マシンイメージ) (Application and OS Images (Amazon Machine Image))] セクションで、[マイAMI (My AMIs)] > [自分が所有 (Owned by me)] の順にクリックし、[Amazon マシンイメージ (AMI) (Amazon Machine Image (AMI))] フィールドで Crosswork Data Gateway AMI イメージを選択します。
- e) [インスタンスタイプ (Instance type)] セクションで、展開している Crosswork データ VM のプロフィールに基づいて、次のインスタンスタイプ (実稼働環境とラボ環境の両方) を選択します。
- **m5.4xlarge** : 標準 VM の場合。
 - **m5.8xlarge** : 拡張 VM の場合。
- f) [キーペア (ログイン) (Key pair(login))] セクションで、ドロップダウンリストから [キーペア名 (Key pair name)] を選択します。
- (注) Cisco Crosswork は、キーベースの認証をサポートしていません。これは AWS の要件であり、Cisco Crosswork では使用されません。
- g) [ネットワーク設定 (Network Settings)] セクションで、[編集 (Edit)] をクリックします。

1. 次のフィールドに値を入力します。

- [VPC] : 環境に適した VPC を選択します。
- [サブネット (Subnet)] : 管理インターフェイスに割り当てるサブネットを選択します。
- [パブリックIPの自動割り当て (Auto-assign public IP)] : [無効 (Disabled)] を選択します。
- [ファイアウォール (セキュリティグループ) (Firewall (security groups))] : VM のセキュリティグループを指定します。セキュリティグループを作成するか、すでに作成した既存のセキュリティグループを使用できます。

上記の詳細を入力すると、[高度なネットワーク設定 (Advanced network configuration)] の下に、[ネットワークインターフェイス1 (Network Interface1)] が自動的に作成されます。

2. [説明 (Description)]、[プライマリIP (Primary IP)] (ユーザーデータからの vNIC0 IP アドレス)、[サブネット (Subnet)]、[セキュリティグループ (Security groups)] を更新します。
3. [ネットワークインターフェイスの追加 (Add network interface)] をクリックし、VM の 2 番目のインターフェイス (vNIC1 に対応) と 3 番目のインターフェイス (vNIC2) の詳細を追加します。

重要 VM のユーザーデータには、プールの作成中に割り当てられる vNIC2 の IP アドレスがないことに注意してください。ネットワーク インターフェイスが作成されるたびに IP アドレスを割り当てることは AWS の要件です。3 番目のインターフェイスの [プライマリ IP (Primary IP)] フィールド (静的 IP) に IP アドレスを入力するか、空白のままにすることができます (AWS が IP を自動的に割り当てます)。

- h) [ストレージの構成 (Configure Storage)] セクションで、[詳細 (Advanced)] をクリックし、[新しいボリュームの追加 (Add new volume)] をクリックして、VM のパーティションを追加します。新しく作成されたボリュームの次のフィールドを更新します。

- [デバイス名 (Device name)] : /device/sdb
- [サイズ (GIB) (Size (GIB))] : 20 GB (標準 CDG) または 520 GB (拡張 CDG)
- [ボリュームタイプ (Volume type)] : gp2 または gp3 の使用をお勧めします。

- i) [詳細設定 (Advanced Settings)] セクションで、次のフィールドを更新します。

- [IAM インスタンスプロファイル (IAM instance profile)] : ユーザーデータで指定した AWS IAM ロールを選択するか、新しいロールを作成します。
- [メタデータにアクセス可能 (Metadata accessible)] : 有効。
- [メタデータのバージョン (Metadata version)] : V1 および V2 (トークンはオプション)
- [メタデータレスポンスのホップ制限 (Metadata response hop limit)] : 2
- [ユーザーデータ (User data)] : 手順 1 で準備したユーザーデータをコピーして、このウィンドウ内に貼り付けます。パラメータを base64 エンコード形式で指定する場合は、チェックボックスをオンにします。

- (注) ユーザーデータを貼り付けるときは、先頭に空白がないようにしてください。そうしないと、展開が失敗します。

ステップ 3 [インスタンスの起動 (Launch Instance)] をクリックします。Amazon EC2 が VM のインストールを開始します。

ステップ 4 手順 2 から 4 を繰り返して、残りの VM をインストールします。

VM が正常にインストールされたことを確認します

1. EC2 ダッシュボードで、左側のメニューから [インスタンス (Instances)] をクリックして、展開された VM を表示します。名前、属性、またはタグを使用して VM を検索できます。
VM が展開されるまで約 20 分間待ちます。
2. VM が正常に起動されると、[インスタンスの状態 (Instance State)] は [実行中 (Running)] になります。
3. VM が正常にインストールされたことを確認するには、VM を選択して [接続 (Connect)] (右上隅) をクリックします。
4. 表示される [インスタンスに接続 (Connect to instance)] ウィンドウで、[EC2 シリアルコントロール (EC2 Serial Control)] タブをクリックし、[接続 (Connect)] をクリックします。
5. ユーザーデータで構成したパスワードを使用して、`dg-admin` または `dg-oper` ユーザーとして VM にログインします。
ログインに成功すると、VM の対話型コンソールが表示されます。

Crosswork Data Gateway を展開するための自動構成

自動構成手順は、欠落している構成パラメータを検出し、ベース VM をインストールするための必須パラメータを自動的に定義します。構成パラメータは、Dynamic Host Configuration Protocol (DHCP) フレームワークを使用して渡されます。Day 0 構成では、自動構成メカニズムは必須パラメータのみをデフォルト値で定義します。

セキュリティポリシーに準拠するために、自動構成中にデフォルトのパスワードが提供されません。最初のログイン時に、`dg-admin` および `dg-oper` ユーザーはデフォルトのパスワードをリセットする必要があります。デフォルトのパスワードが変更されるまで、データゲートウェイインスタンスは収集サービスを開始しません。

自動構成プロセスは、単一の NIC 展開をサポートします。特に、`eth0` は管理ネットワーク用に構成されています。`eth0` インターフェイスは、DHCP インタラクションに使用されます。DHCP サーバーには、自動構成中にプロセスが使用するデフォルト値が含まれています。インタラクティブコンソールを使用して、デフォルト値を構成または変更できます。コンソールの使用方法については、[現在のシステム設定の変更 \(120 ページ\)](#) を参照してください。



重要 自動構成機能は、OpenStack および Amazon EC2 での Crosswork Data Gateway の展開をサポートします。

自動構成時に使用されるパラメータ

自動構成ユーティリティは、次のパラメータをデフォルト値で構成します。これらのパラメータの詳細については、[Cisco Crosswork 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 \(15 ページ\)](#) を参照してください。

表 11: Cisco Crosswork Data Gateway 必須展開パラメータ

名前	パラメータ	デフォルト値
AllowRFC8190	AllowRFC8190	デフォルト値は [Yes] です。
監査サーバポート (Auditd Server Port)	AuditdPort	デフォルトポートは 60 です。
展開	Deployment	デフォルト値は Crosswork Cloud です。
Crosswork コントローラポート	ControllerPort	デフォルトポートは 443 です。
説明	Description	デフォルト値は CDG auto configure です。
dg-admin パスフレーズ	dg-adminPassword	デフォルトのパスワードは changeme です。 デフォルト値を dg-admin ユーザー用に選択したパスワードでリセットします。 パスワードは 8 - 64 文字である必要があります。
dg-oper パスフレーズ	dg-operPassword	デフォルトのパスワードは changeme です。 デフォルト値を dg-oper ユーザー用に選択したパスワードでリセットします。 パスワードは 8 - 64 文字である必要があります。
データディスクサイズ (Data Disk Size)	DGAppdataDisk	このパラメータのデフォルト値は 5 です。
DNS アドレス (DNS Address)	DNS	このパラメータのデフォルト値は以下になります。 208.67.222.222 208.67.220.220

名前	パラメータ	デフォルト値
DNS セキュリティ拡張機能 (DNS Security Extensions)	DNSSEC	このパラメータのデフォルト値は False です。
DNS over TLS	DNSTLS	このパラメータのデフォルト値は False です。
DNS 検索ドメイン (DNS Search Domain)	Domain	このパラメータのデフォルト値は localdomain です。
Crosswork Data Gateway の HA モード	HANetworkMode	このパラメータのデフォルト値は L2 です。
ホストネーム	Hostname	このパラメータのデフォルト値は dg-<eth0 address> です。 この <eth0-address> は vNIC0 のアドレスです。
リンクローカルマルチキャスト名前解決 (Link-Local Multicast Name Resolution)	LLMNR	このパラメータのデフォルト値は False です。
マルチキャスト DNS (Multicast DNS)	mDNS	このパラメータのデフォルト値は False です。
NicAdministration	NicAdministration	このパラメータのデフォルト値は eth0 です。
NicControl	NicControl	このパラメータのデフォルト値は eth1 です。
NicDefaultGateway	NicDefaultGateway	このパラメータのデフォルト値は eth0 です。
NicExternalLogging	NicExternalLogging	このパラメータのデフォルト値は eth0 です。
NicManagement	NicManagement	このパラメータのデフォルト値は eth0 です。
NicNBExternalData	NicNBExternalData	このパラメータのデフォルト値は eth1 です。
NicNBSystemData	NicNBSystemData	このパラメータのデフォルト値は eth1 です。
NicSBData	NicSBData	このパラメータのデフォルト値は、1 つの NIC 展開の場合は eth0、2 つの NIC の場合は eth1 など、最後にアクティブになったインターフェイスです。

名前	パラメータ	デフォルト値
NTPv4サーバ	NTP	このパラメータのデフォルト値は以下になります。 162.159.200.1 65.100.46.164 40.76.132.147 104.131.139.195
NTPv4 認証の使用 (Use NTPv4 Authentication)	NTPAuth	このパラメータのデフォルト値は False です。
Profile	Profile	このパラメータのデフォルト値は Crosswork-Cloud です。
Syslog マルチサーバー モード	SyslogMultiserverMode	このパラメータのデフォルト値は Simultaneous です。
Syslog サーバーポート (Syslog Server Port)	SyslogPort	このパラメータのデフォルト値は 514 です。
Syslog サーバープロト コル (Syslog Server Protocol)	SyslogProtocol	このパラメータのデフォルト値は UDP です。
TLS 経由の Syslog を 使用する (Use Syslog over TLS)	SyslogTLS	このパラメータのデフォルト値は False です。
リモート監査サーバー の使用 (Use Remote Auditd Server)	UseRemoteAuditd	このパラメータのデフォルト値は False です。
Syslog リモートサー バーの使用 (Use Remote Syslog Server)	UseRemoteSyslog	このパラメータのデフォルト値は False です。
vNIC IPv4 方式	Vnic0IPv4Method	このパラメータのデフォルト値は DHCP です。
vNIC IPv4 スキップ ゲートウェイ (vNIC IPv4 Skip Gateway)	Vnic0IPv4SkipGateway	このパラメータのデフォルト値は False です。
vNIC IPv6 方式	Vnic0IPv6Method	デフォルト値は None です。

名前	パラメータ	デフォルト値
vNIC IPv6 スキップ ゲートウェイ (vNIC IPv6 Skip Gateway)	Vnic0IPv6SkipGateway	デフォルト値は False です。
vNIC IPv4 方式	Vnic1IPv4Method	デフォルト値は None です。
vNIC IPv4 スキップ ゲートウェイ (vNIC IPv4 Skip Gateway)	Vnic1IPv4SkipGateway	デフォルト値は False です。
vNIC IPv6 方式	Vnic1IPv6Method	デフォルト値は None です。
vNIC IPv6 スキップ ゲートウェイ (vNIC IPv6 Skip Gateway)	Vnic1IPv6SkipGateway	デフォルト値は False です。
vNIC IPv4 方式	Vnic2IPv4Method	デフォルト値は None です。
vNIC IPv4 スキップ ゲートウェイ (vNIC IPv4 Skip Gateway)	Vnic2IPv4SkipGateway	デフォルト値は False です。
vNIC IPv6 方式	Vnic2IPv6Method	デフォルト値は None です。
vNIC IPv6 スキップ ゲートウェイ (vNIC IPv6 Skip Gateway)	Vnic2IPv6SkipGateway	デフォルト値は False です。

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 7: 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 \(109 ページ\)](#) を参照）。
- インタラクティブコンソールの [base64でエンコードされた登録パッケージの表示 (Display base64 Encoded Enrollment Package)] オプションを使用する（[エンコード済み登録パッケージの作成 \(111 ページ\)](#) を参照）。


```
HpqNB3D+YDnFGdDCyM3E7gP4h4rDlwc0V6cSF75mMzGlasHbBiDrae1Q6y17LeWfA3eSZLXQ7yMhYa3WojwtAM17vI/9RnHZSSejyANBwUe="
],
"version": "5.0.0 (branch dg45x - build number 19)",
"duuid": "a3bf6411-1ad0-418c-9957-eb199e9395e0",
"profileType": "VM_PROFILE_STANDARD"
}
```

登録パッケージの入手

登録パッケージを入手するには、パッケージのエンコードされたコンテンツをエクスポートするか、コピーして貼り付けることで登録ファイルを作成します。

- 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 [登録パッケージの取得 (Get Enrollment Package)] を選択します。
- ステップ3 [登録パッケージのエクスポート (Export Enrollment Package)] または [base64でエンコードされた登録パッケージの表示 (Display base64 Encoded Enrollment Package)] を選択します。
- ステップ4 [OK] をクリックします。

次のタスク

選択したオプションに応じて[登録パッケージのエクスポート \(109ページ\)](#) または[エンコード済み登録パッケージの作成 \(111ページ\)](#) を参照し、登録パッケージを入手します。

登録パッケージのエクスポート

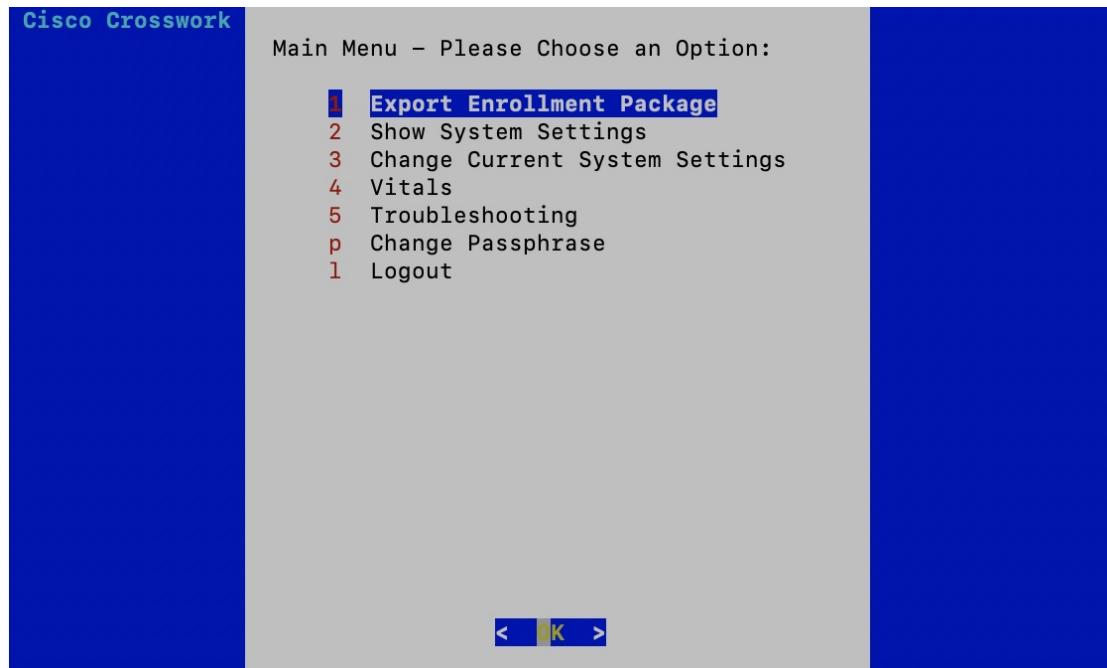
Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を Crosswork Cloud に登録するには、ローカルコンピュータに登録パッケージのコピーが必要です。



- (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 \(112ページ\)](#)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 登録パッケージの取得 (1 Get Enrollment Package)] を選択します。
- ステップ3 [登録パッケージのエクスポート (Export Enrollment Package)] を選択します。
- ステップ4 [OK] をクリックします。

図 29: メインメニュー



ステップ 5 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 サーバー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的な名前で作成されます。例：9208b9bc-b941-4ae9-b1a2-765429766f27.json

ステップ 6 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 7 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 \(112 ページ\)](#)」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。

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 \(112 ページ\)](#)」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 \(113 ページ\)](#)」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 12: Crosswork Data Gateway 接続のトラブルシューティング

問題	操作
<p>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。</p>	<p>1. Crosswork Data Gateway VM にログインします。</p> <p>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。</p> <p>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。</p> <p>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、</p> <pre>UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid</pre> <p>Crosswork Data Gateway と Cisco Crosswork Cloud の間にクロックのずれがあります。</p> <p>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。</p> <p>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。</p>
<p>Crosswork Data Gateway は、外部 Web サービスに直接接続されません。</p>	<p>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。</p> <p>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。</p> <p>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。</p> <p>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 (122 ページ)」を参照してください。</p>



第 4 章

Crosswork Data Gateway インスタンスの設定

Cisco Crosswork Data Gateway インスタンスはスタンドアロンインスタンス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（Crosswork Cloud です）。このインスタンスは、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。

- [Crosswork Data Gateway ユーザーの管理](#)（115 ページ）
- [現在のシステム設定の表示](#)（118 ページ）
- [現在のシステム設定の変更](#)（120 ページ）
- [Crosswork Data Gateway のバイタルの表示](#)（132 ページ）
- [Crosswork Data Gateway VM のトラブルシューティング](#)（135 ページ）

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](#)（115 ページ）
- [パスフレーズの変更](#)（118 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 13: 各ロールの権限

権限	管理者	オペレータ
登録パッケージの取得 (Get Enrollment Package)	✓	✓
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	✓	✓
現在のシステム設定の変更		

権限	管理者	オペレータ
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 vNIC 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 インターフェイスアドレスの設定	✓	×
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	✓	×
パスワードの変更	✓	✓

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ワードを変更できますが、相互に変更を行うことはできません。

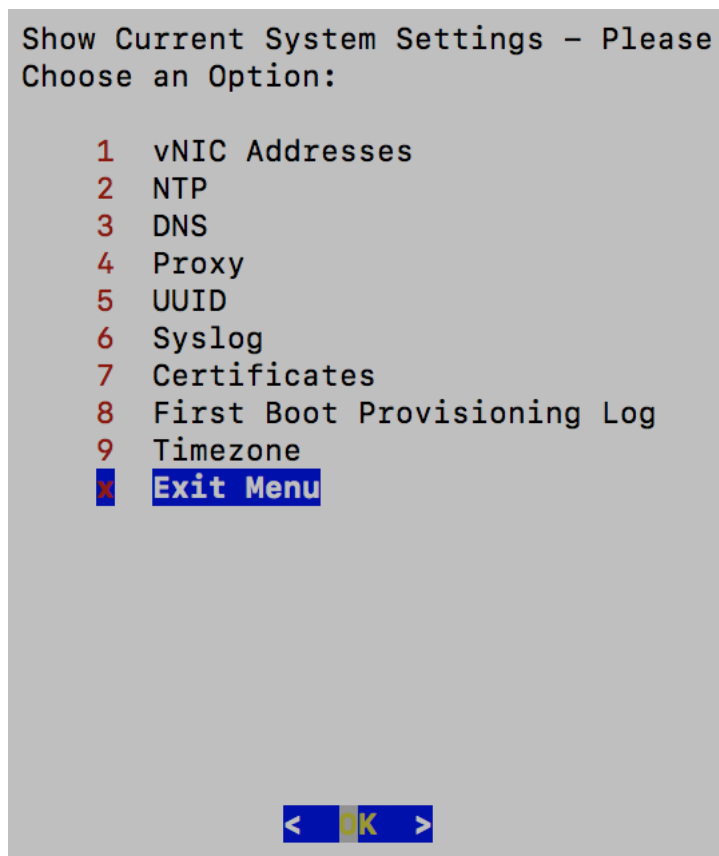
自分のパスワードを変更するには、次の手順を実行します。

-
- ステップ 1** メインメニューから、[パスワードの変更 (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。

図 31: [現在のシステム設定の表示 (Show Current System Settings)]メニュー



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	Description
[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)。

設定オプション	Description
[5 UUID]	システム UUID を表示します。
[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。 <ul style="list-style-type: none"> • 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
- 制御プロキシ
- スタティック ルート
- Syslog
- SSH キー
- 証明書
- vNIC MTU
- タイムゾーン
- パスワード要件

- 同時ログイン数の制限
- アイドル タイムアウト
- Auditd
- インターフェイス アドレス



- (注)
- Crosswork Data Gateway システム設定は管理者のみが設定できます。
 - 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。
 - SCP を使用する必要がある設定オプションで、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 \(140 ページ\)](#) 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 \(132 ページ\)](#)」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形式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。



注意 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

構成ファイルを使用して、Day0 のインストール中にリモートサーバーを構成できます。Day1 以降のインストールで Syslog サーバーリスト、ポート番号、プロトコル、および証明書ファイルを変更する場合は、インタラクティブコンソールを使用します。



- (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 サーバーを構成する場合は、システムの管理者ガイドと構成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。

始める前に

Crosswork Data Gateway では、次のモードで複数のサーバーを構成できます。

- [同時 (Simultaneous)] : Crosswork Data Gateway は、構成されたすべての Syslog サーバーアドレスにメッセージを送信します。いずれかのサーバーが応答しない場合、サーバーが応答するまで、メッセージはディスクのキューに入れられます。
- [フェールオーバー (Failover)] : Crosswork Data Gateway は、最初の Syslog サーバーアドレスにメッセージを送信します。サーバーが使用できない場合、メッセージはその次に構成されたアドレスに送信されます。リスト内のすべてのサーバーが応答しない場合、サーバーが応答するまで、メッセージはディスクのキューに入れられます。

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、[5 Syslog の設定 (5 Configure Syslog)] を選択します。

ステップ 2 [Syslog を使用する (Use Syslog)] ウィンドウで、[はい (True)] を選択して、Syslog サーバーの構成を続行します。

ステップ 3 [Syslog マルチサーバーモードの選択 (Select Syslog Multiserver Mode)] ウィンドウで、[同時 (Simultaneous)] または [フェールオーバー (Failover)] を選択します。

ステップ 4 次の Syslog 属性の値を入力します。

- [サーバーのアドレスまたはホスト名 (Server address or hostname)] : 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 アドレスのスペース区切りリスト。
- [ポート (Port)] : Syslog サーバーのポート番号。
- [プロトコル (Protocol)] : システムログの送信時に 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 サーバーの 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5 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60～9000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60～1500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。

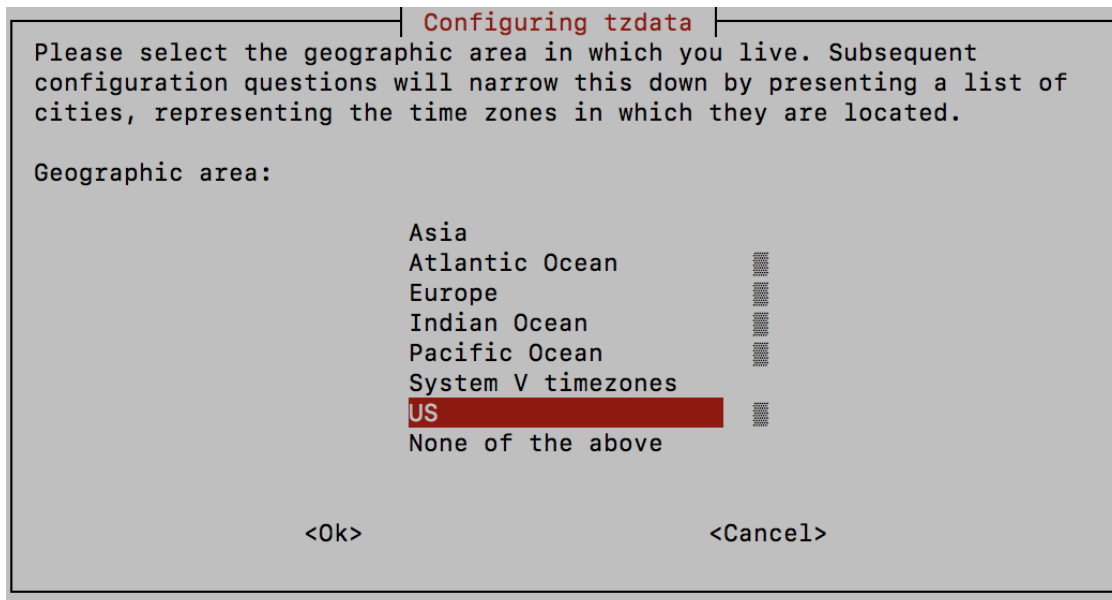
- ステップ 1 [現在のシステム設定の変更 (Change Current System Settings)] メニューから、[8 vNIC1 MTUの設定 (8 Configure vNIC1 MTU)] を選択します。
- ステップ 2 vNIC2 MTU 値を入力します。
- ステップ 3 設定を保存するには [OK] をクリックします。

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。

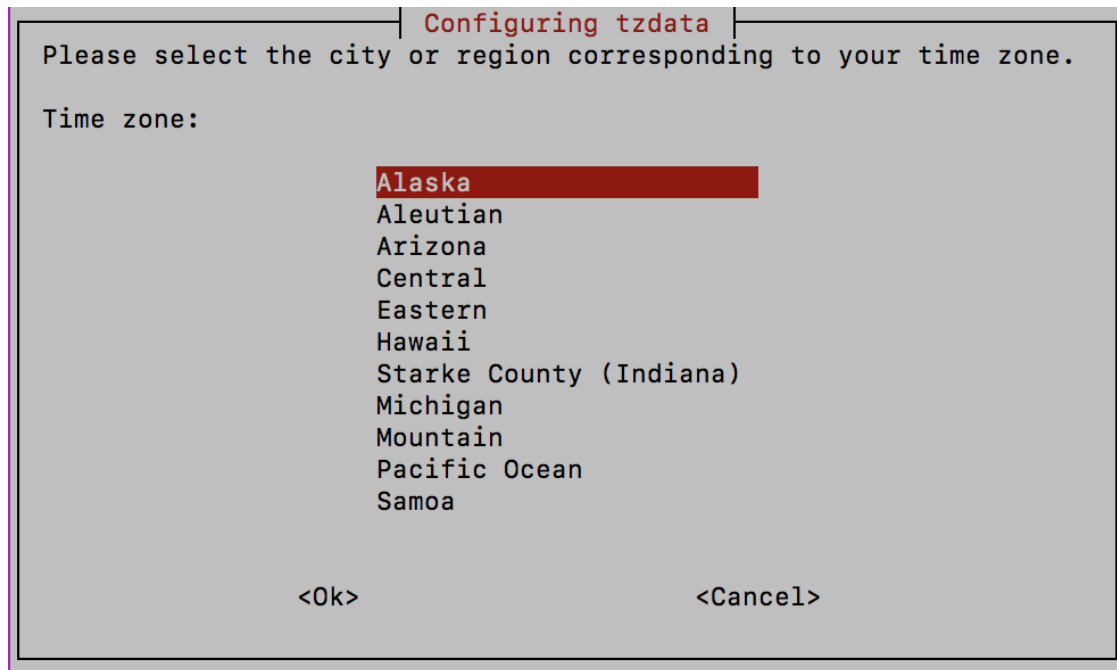
- ステップ 1 Crosswork Data Gateway VM にログインします。
- ステップ 2 Crosswork Data Gateway VM のインタラクティブメニューで、[3 現在のシステム設定の変更 (3 Change Current System Settings)] を選択します。
- ステップ 3 メニューから [9 タイムゾーン (9 Timezone)] を選択します。
- ステップ 4 居住地域を選択します。

図 32: [タイムゾーン設定 (Timezone Settings)] - [地理的エリアの選択 (Geographic Area Selection)]



- ステップ 5 タイムゾーンに対応する都市または地域を選択します。

図 33: [タイムゾーン設定 (Timezone Settings)] - [地域の選択 (Region Selection)]



ステップ 6 [OK] を選択して設定を保存します。

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

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

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。
-

インターフェイスアドレスの設定

Crosswork Data Gateway インスタンスを展開した後、インスタンスにすでに関連付けられているインターフェイスを再構成できます。インターフェイスを再構成すると、その名前を変更したり、IP アドレスを関連付けたり、インターフェイスに関連付けられているセキュリティグループにアクセスしたりできます。

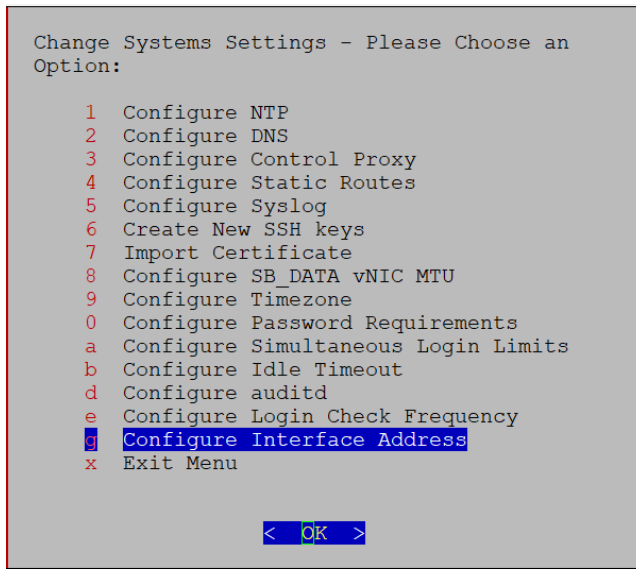
始める前に

- インターフェイスアドレスを再設定する Crosswork Data Gateway インスタンスからすべてのデバイスを切り離す必要があります。

- Crosswork Data Gateway インスタンスはメンテナンスモードにする必要があります。

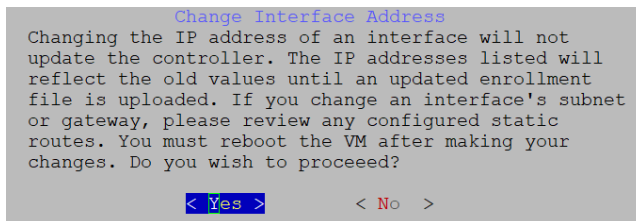
ステップ1 [システム設定の変更 (Change System Settings)] メニューから、[g インターフェイスアドレスの設定 (g Configure Interface Address)] を選択します。

図 34: [システム設定の変更 (Change System Settings)] メニュー



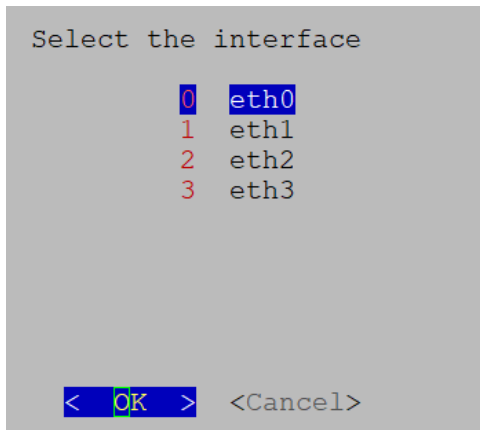
ステップ2 [インターフェイスアドレスの変更 (Change Interface Address)] 確認ボックスで、[はい (Yes)] をクリックします。

図 35: [インターフェイスアドレスの変更 (Change Interface Address)] 確認メッセージ



ステップ3 再構成するインターフェイスを選択し、[OK] をクリックします。オプションは、eth0、eth1、eth2、または eth3 です。

図 36: [インターフェイスの選択 (Interface Selection)]メニュー



ステップ 4 <interface>IPv4 アドレッシング方式を選択します。オプションは、DHCP、Static Address、または No address です。Day0 のインストール中に指定したオプションを選択することをお勧めします。

図 37: IPv6 アドレスの選択



ステップ 5 IPv4 アドレスを入力し、[OK] をクリックします。

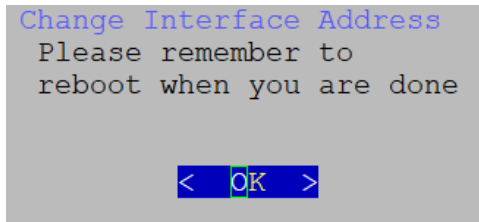
ステップ 6 IPv4 ネットマスクアドレスを入力し、[OK] をクリックします。

ステップ 7 [スキップ<interface> IPv4ゲートウェイの構成確認 (Skip <interface> IPv4 gateway configuration confirmation)] ボックスで、True または False を選択し、[OK] をクリックします。

ステップ 8 前の手順で True を選択した場合は、IPv4 ゲートウェイアドレスを指定します。

ステップ 9 [インターフェイスアドレスの変更 (Change Interface Address)] 確認ボックスで、[OK] をクリックします。

図 38: 確認メッセージ



インターフェイスを構成したら、必ず VM を再起動してください。

Crosswork Cloud に Crosswork Data Gateway を登録します。Crosswork Cloud アプリケーションに Cisco Crosswork Data Gateway を登録する手順については、[Crosswork Cloud アプリケーションを使用した Crosswork Data Gateway の登録 \(112 ページ\)](#) を参照してください。

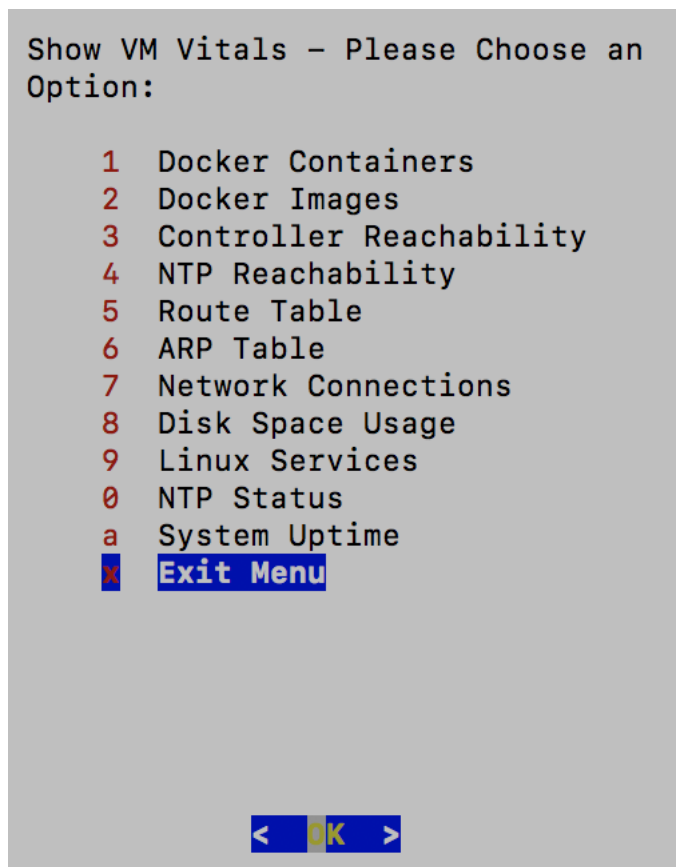
Crosswork Data Gateway のバイタルの表示

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。

図 39: [VMのバイタルの表示 (Show VM Vitals)]メニュー



バイタル	Description
Docker コンテナ (Docker Containers)	<p>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。</p> <p>コンテナ ID (Container ID)</p> <p>イメージ画像 (Image)</p> <p>名前 (Name)</p> <p>コマンド (Command)</p> <p>作成時刻 (Created Time)</p> <p>ステータス (Status)</p> <p>ポート (Port)</p>

バイタル	Description
Docker イメージ (Docker Images)	<p>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。</p> <ul style="list-style-type: none"> 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)	<p>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。</p> <ul style="list-style-type: none"> 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)	<p>NTP 到達可能性テストの結果を表示します。</p> <ul style="list-style-type: none"> 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。
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。

バイタル	Description
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。 <ul style="list-style-type: none"> • 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** ユーザーはこれらのオプションの一部を使用できません。[表 13:各ロールの権限 \(116 ページ\)](#) 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。



- (注) Crosswork Cloud では、[トラブルシューティング (Troubleshooting)] > [すべての非インフラストラクチャコンテナを削除して再起動 (Remove All Non-Infra Containers and Reboot)] オプションをサポートしていません。

- [診断コマンドの実行 \(136 ページ\)](#)
- [show-tech の実行 \(140 ページ\)](#)
- [Crosswork Data Gateway VM のシャットダウン \(141 ページ\)](#)
- [auditd ログのエクスポート \(141 ページ\)](#)
- [TAC シェルアクセスの有効化 \(141 ページ\)](#)

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 40: 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 メインメニューから、[トラブルシューティング (Troubleshooting)]>[診断の実行 (Run Diagnostics)]>[ping] に移動します。

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 メインメニューから、[トラブルシューティング (Troubleshooting)] > [診断の実行 (Run Diagnostics)] > [トレースルート (traceroute)] に移動します。

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 メインメニューから、[トラブルシューティング (Troubleshooting)] > [診断の実行 (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 nslookup

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** メインメニューから、[トラブルシューティング (Troubleshooting)] > [診断の実行 (Run Diagnostics)] > [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ユーティリティを実行するには、[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 ログイン情報を要求します。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。

コントローラセッションテストの実行

Crosswork Data Gateway をインストールすると、コントローラセッションテストオプションを使用して、インスタンスが Crosswork Cloud との接続を確立できるかどうかを検証できます。接続テストに加えて、ユーティリティは VM に割り当てられたリソース (CPU およびメモリ) と展開プロファイルで規定されたリソースとの間に不一致がないか検証および分析します。

メインメニューから、[トラブルシューティング (Troubleshooting)] > [診断の実行 (Run Diagnostics)] > [コントローラセッションテストの実行 (Run Controller Session Tests)] に移動します。接続が完了すると、インスタンスの接続が確立されたことを示すメッセージがコンソールに表示されます。接続に失敗すると、検証テストが追加で実施され、次の情報が表示されます。

- DNS サーバの IP アドレス
- DNS ドメイン
- NTP サーバのアドレス
- NTP ステータス (NTP status)
- プロキシ URL
- プロキシの到達可能性ステータス

- コントローラ URL
- コントローラの到達可能性ステータス
- テストが最後に実施された日付。

図 41: [コントローラセッションテストの実行 (*Run Controller Session Tests*)] メニュー

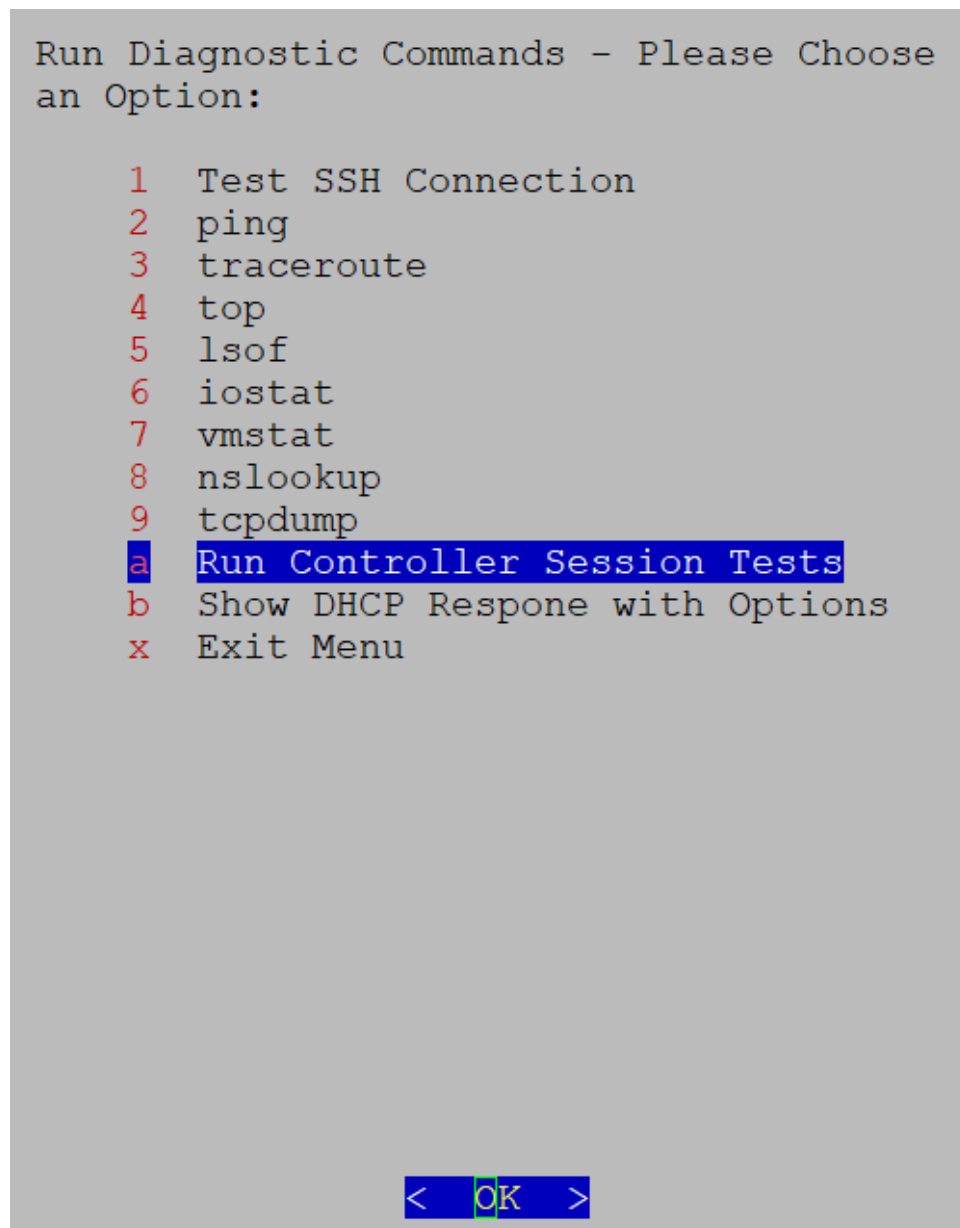


図 42: [コントローラセッションテストの実行 (Run Controller Session Tests)] メニューの結果

```
Controller Session: Established
Last Checked: Sun 23 Apr 2023 11:03:17 AM UTC
```

次のタスク

コントローラセッションが確立されなかった場合は、コンソールに表示された情報を確認して考えられる失敗の原因を特定し、コンソールで提案された修正アクションを実行します。

show-tech の実行

Crosswork Data Gateway は、ログファイルをユーザー定義の 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を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](#) (145 ページ)
- [OpenStack からの VM の削除](#) (146 ページ)

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。

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 User Guide』の「Delete Crosswork Data Gateways」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

- OpenStack の UI にログインします。
- [コンピューティング (Compute)] > [インスタンス (Instances)] に移動します。
- このページに表示される VM のリストから、削除する VM を選択します。
- [インスタンスの削除 (Delete Instances)] をクリックします。
- 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。

または

ステップ 2 OpenStack の CLI から実行する場合

- CLI から OpenStack VM にログインします。
- 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-ospdl
```
- (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。