



クラウド導入のための Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) 2.0.1 インストールおよび設 定ガイド

初版：2021年4月8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.

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)

© 2021 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 1

第 2 章	インストール要件 3
	VM 要件 3
	使用ポート 5

第 3 章	インストール タスク 7
	Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) のインストール 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 8
	vCenter vSphere Client を使用した Crosswork Data Gateway のインストール 22
	OVF ツールによる Crosswork Data Gateway のインストール 28
	Cisco CSP に Crosswork Data Gateway をインストールする 31
	登録パッケージの生成 39
	登録パッケージのエクスポート 40

第 4 章	Crosswork Data Gateway VM の設定 43
	インタラクティブなコンソールの使用 43
	Crosswork Data Gateway ユーザーの管理 44
	サポートされるユーザ ロール 45
	パスワードの変更 47
	現在のシステム設定の表示 47

現在のシステム設定の変更	49
NTP の設定	49
DNS の設定	50
制御プロキシの設定	50
スタティックルートの設定	51
スタティック ルートの追加	51
スタティック ルートの削除	52
Syslog の設定	52
新しい SSH キーの作成	53
証明書のインポート	53
vNIC2 MTU の設定	53
タイムゾーンの設定	54
パスワード要件の設定	55
Crosswork Data Gateway のバイタルの表示	56
Crosswork Data Gateway VM のトラブルシューティング	58
ホストへの Ping	59
ホストに対するトレースルート	59
NTP ステータスの確認	59
システム稼働時間の確認	60
show-tech の実行	60
SSH 接続のテスト	60
auditd ログのエクスポート	61
TAC シェルアクセスの有効化	61
TAC シェルイベントの監査	62

第 5 章	仮想マシンの削除	63
	vSphere UI を使用した VM の削除	63
	Cisco CSPからの Crosswork Data Gateway サービスの削除	64



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](#) (1 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。また、このガイドのユーザは、すでにシスコクラウド環境への有効なログインを行えるようになっている必要があります。このマニュアルは、次のトピックに関する知識があることを前提としています。

- ネットワーク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の十分な知識があること。
- VMware vCenter または OVF ツールを使用した OVF テンプレートの展開
- Cisco Cloud Services Platform (CSP) での QCOW2 イメージの展開

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

Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) は、監視対象デバイスからのデータ収集を有効にし、収集したデータを Cisco Crosswork Cloud アプリケーションに転送します。これらのアプリケーションは、さらに分析するためにデータを使用し、必要に応じて、管理者にさらなるアクションを促すことができます。



注目 このマニュアルでは、クラウド導入のための Cisco Crosswork Data Gateway のインストールおよび設定方法を説明します。

Crosswork On Premise 導入のための Crosswork Data Gateway のインストールについて詳しくは、『Cisco Crosswork インフラストラクチャ 4.0 およびアプリケーションインストールガイド』を参照してください。

Crosswork Data Gateway は、次の Crosswork Cloud アプリケーションと組み合わせて検証されています。

- Cisco Crosswork Trust Insights
- Cisco Crosswork Traffic Analysis



第 2 章

インストール要件

VMware または Cisco Cloud Services Platform (Cisco CSP) のいずれかに Crosswork Data Gateway を展開できます。ここでは、いずれか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。

ここでは、次の内容について説明します。

- [VM 要件 \(3 ページ\)](#)
- [使用ポート \(5 ページ\)](#)

VM 要件

特に明記されていない限り、要件は VMware と Cisco CSP の両方で同じです。

表 1: Cisco Crosswork Data Gateway VM の要件

要件	説明
データセンター	<p>VMware</p> <ul style="list-style-type: none">• VMware vCenter Server 6.7 Update 3g 以降 (ホストに ESXi 6.7 Update 1 がインストール済み)• VMware vCenter Server 6.5 Update 2d 以降 (ホストに ESXi 6.5 Update 2 インストール済み) <p>Cisco CSP</p> <ul style="list-style-type: none">• Cisco CSP 2.8.0.276 以降 <p>許可されたハードウェア: UCSC-C220-M4S、UCSC-C240-M4SX、N1K-1110-X、N1K-1110-S、CSP-2100、CSP-2100-UCSD、CSP-2100-X1、CSP-2100-X2、CSP-5200、CSP-5216、CSP-5228、CSP-5400、CSP-5436、CSP-5444、CSP-5456</p>
メモリ	32 GB

要件	説明			
ディスク容量	70 GB			
CPU	8			
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つ、2つ、または3つのインターフェイスのいずれかで展開できます。			
	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 デバイスアクセストラフィック 	—	—
	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 デバイスアクセストラフィック 	—
	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 	<ul style="list-style-type: none"> デバイスアクセストラフィック
<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、<code>dg-tac</code> ユーザとして 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 Data Gateway と Crosswork アプリケーションおよびその他の外部データ宛先間のデータと設定の転送の場合。 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。 				

要件	説明
IP アドレス	<p>使用するインターフェイスの数に基づいて、1つ、2つ、または3つのIPv4/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>
NTP サーバ	<p>使用する NTP サーバの IPv4/IPv6 アドレスまたはホスト名。複数の NTP サーバを入力する場合は、それぞれをスペースで区切ります。これらは、ネットワーク全体でデバイス、クライアント、およびサーバを同期するために使用する NTP サーバと同じでなければなりません。NTP IP アドレスまたはホスト名がネットワーク上で到達可能であることを確認します。到達可能でない場合、インストールは失敗します。</p> <p>Cisco Crosswork Data Gateway ホストと仮想マシンは NTP サーバに同期する必要があります。同期しないと、Crosswork Cloud への登録を完了できない場合があります。</p>
DNS サーバ	<p>使用する DNS サーバの IPv4/IPv6 アドレス。これらは、ネットワーク全体でホスト名を解決するために使用する DNS サーバ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、<code>cisco.com</code>）。検索ドメインは1つのみ設定できます。</p>



- (注) Cisco Crosswork Data Gateway アプリケーションは Ubuntu Server 20.04.2 にバンドルされています。シスコは、セキュリティやその他の修正に対処するため、必要に応じて更新プログラムを提供します。

使用ポート

次の表に、Cisco 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 Cisco Crosswork Data Gateway 機能のみを有効にするためのセットです。Cisco Crosswork Data Gateway で実行されているアプリケーションに応じて、追加のポートを使用することができます。



(注) SCP ポートを設定できます。

表 2: 管理トラフィック用に開くポート

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



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 \(7 ページ\)](#)
- [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 \(8 ページ\)](#)
- [vCenter vSphere Client を使用した Crosswork Data Gateway のインストール \(22 ページ\)](#)
- [OVF ツールによる Crosswork Data Gateway のインストール \(28 ページ\)](#)
- [Cisco CSP に Crosswork Data Gateway をインストールする \(31 ページ\)](#)
- [登録パッケージの生成 \(39 ページ\)](#)
- [登録パッケージのエクスポート \(40 ページ\)](#)

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 (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 Cloud は、分散 Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) VM からの収集をオーケストレーションします。

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

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

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

1. インストールの計画を立てます。展開パラメータと可能な展開シナリオについては、このトピックを参照してください。 [Cisco Crosswork データゲートウェイ \(Cisco Crosswork Data Gateway\) 導入パラメータとシナリオ \(8 ページ\)](#)

- 使用するプラットフォームに Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) をインストールします。

VMware	vCenter vSphere Client を使用した Crosswork Data Gateway のインストール (22 ページ)
	OVF ツールによる Crosswork Data Gateway のインストール (28 ページ)
Cisco CSP	Cisco CSP に Crosswork Data Gateway をインストールする (31 ページ)

- Crosswork Cloud に Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を登録します。



注 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、『Cisco Crosswork Cloud User Guide』の「Add Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) Information」の章を参照してください。

- [登録パッケージの生成 \(39 ページ\)](#)
- [登録パッケージのエクスポート \(40 ページ\)](#)

クラウド導入では、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、環境内に存在しているかどうかに応じてプロキシサーバが必要になる場合があります。ネットワークにプロキシサーバがある場合は、インストールプロセス中、またはインストール後に[インタラクティブ (Interactive)]メニューから設定する必要があります。参照先：

- [制御プロキシの設定 \(50 ページ\)](#)
- [Crosswork Data Gateway のバイタルの表示](#)

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

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

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

インストール時に、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) は2つのデフォルトユーザアカウントを作成します。

- ユーザ名が `dg-admin` で、インストール時に設定されたパスワードの 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。
- ユーザ名が `dg-oper` で、インストール時に設定されたパスワードの 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で、すべての「read」操作と一部の限定された「action」コマンドを実行する権限があります。
- これら2つの定義済みユーザ名は予約済みであり、変更できません。
- パスワードの変更は、両方のアカウントに対してコンソールから許可されます。[パスワードの変更 \(47 ページ\)](#) を参照してください。
- 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 \(45 ページ\)](#) 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、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。

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。その他はオプションです。必要な展開シナリオの種類に基づいて選択できます。展開シナリオについては、必要に応じて「その他の情報」列で説明します。

** インストール中に入力できるパラメータ、または追加の手順を使用して対処できるパラメータを示します。

表 3: 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

VMware パラメータ	CSP パラメータ	説明	その他の情報
ホスト情報			

VMware パラメータ	CSP パラメータ	説明	その他の情報
ホスト名 (Hostname) *	Hostname	<p>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。</p> <p>(注) 大規模なシステムでは、複数の Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) VM が存在する可能性があります。したがって、ホスト名は一意であり、特定の VM を簡単に識別できるように作成する必要があります。</p>	
説明 (Description) *	Description	Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) の詳細です。	

VMware パラメータ	CSP パラメータ	説明	その他の情報
ラベル (Label)	Label	複数の Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を分類およびグループ化するために Cisco Crosswork Cloud で使用されるラベル。	
アクティブな vNIC (Active vNICs)	ActiveVnics	トラフィックの送信に使用する vNIC の数。	ネットワーク要件に応じて、1つ、2つ、または3つのインターフェイスの使用を選択できます。 トラフィックのルーティング方法については、 VM 要件 (3 ページ) の表「インターフェイス」を参照してください。
AllowRFC8190	AllowRFC8190	使用可能な RFC 8190 の範囲内にあるインターフェイスアドレスを許可します。[はい (yes)]、[いいえ (no)]、または[問う (ask)]を選択します。デフォルト値は yes です。	

VMware パラメータ	CSP パラメータ	説明	その他の情報
秘密キー URI (Private Key URI)	DGCertKey	セッションキー署名用の秘密キーファイルへの SCP URI。これは SCP (user@host:path/to/file) を使用して取得できません。	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。
証明書ファイル URI (Certificate File URI)	DGCertChain	この VM の PEM 形式の署名証明書チェーンへの SCP 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、次の3つのパラメータを入力する必要があります。 (注) URI ファイルを持つホストは、ネットワーク上で (SCP を介して vNIC0 インターフェイスから) 到達可能でなければならず、ファイルはインストール時に存在する必要があります。

VMware パラメータ	CSP パラメータ	説明	その他の情報
データディスクサイズ (Data Disk Size)	DGAppdataDisk	独立したデータディスクのサイズ (GB 単位)。最小値は 20 GB で、これがデフォルト値です。最大 70 GB の値を入力してください。	
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 文字である必要があります。	
dg-oper パスフレーズ (dg-oper Passphrase) *	dg-operPassword	dg-oper ユーザ用に選択したパスワード。 パスワードは 8 - 64 文字である必要があります。	
インターフェイス			
(注) IPv4 アドレスまたは IPv6 アドレスのいずれかを選択する必要があります。[vNICx IPv4 メソッド (vNICx IPv4 Method)] フィールドと [vNICx IPv6 メソッド (vNICx IPv6 Method)] フィールドの両方で [なし (None)] を選択すると、展開が機能しなくなります。			
vNICx IPv4 アドレス (使用するインターフェイスの数に応じて VNIC0、VNIC1、および VNIC2)			

VMware パラメータ	CSP パラメータ	説明	その他の情報
vNICx IPv4 方式 (vNICx IPv4 Method) * たとえば、vNIC0 のパラメータ名は vNIC0 IPv4 方式 (vNIC0 IPv4 Method) です。	VnicxIPv4Method たとえば、vNIC0 のパラメータ名は Vnic0IPv4Method です。	vNICx インターフェイスがその IPv4 アドレスを取得する方法。	[方式 (Method)] のデフォルト値は [なし (None)] です。 IPv4 アドレスを使用する場合は、[方式 (Method)] を [スタティック (Static)] に指定し、[アドレス (Address)]、[ネットマスク (Netmask)]、[ゲートウェイをスキップ (Skip Gateway)]、および [ゲートウェイ (Gateway)] フィールドに情報を入力します。
vNICx IPv4 アドレス (vNICx IPv4 Address)	VnicxIPv4Address	vNICx インターフェイスの IPv4 アドレス。	
vNICx IPv4 ネットマスク (vNICx IPv4 Netmask)	VnicxIPv4Netmask	ドット区切りの4つの数字列形式による vNICx インターフェイスの IPv4 ネットマスク。	
vNICx IPv4 スキップゲートウェイ (vNICx IPv4 Skip Gateway)	VnicxIPv4SkipGateway	オプションは [はい (yes)] または [いいえ (no)] です。 [はい (yes)] を選択すると、ゲートウェイの設定がスキップされます。	
vNICx IPv4 ゲートウェイ (vNICx IPv4 Gateway)	VnicxIPv4Gateway	vNICx ゲートウェイの IPv4 アドレス。	
vNICx 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)			

VMware パラメータ	CSP パラメータ	説明	その他の情報
vNICx IPv6 方式 (vNICx IPv6 Method) * たとえば、vNIC0 のパラメータは vNIC0 IPv6 方式 (vNIC0 IPv6 Method) です。	VnicxIPv6Method たとえば、vNIC0 のパラメータは Vnic0IPv6Method です。	vNICx インターフェイスがその IPv6 アドレスを取得する方法。	[方式 (Method)] のデフォルト値は [なし (None)] です。 IPv6 アドレスを使用する場合は、[方式 (Method)] を [スタティック (Static)] に指定し、[アドレス (Address)]、[ネットマスク (Netmask)]、[ゲートウェイをスキップ (Skip Gateway)]、および [ゲートウェイ (Gateway)] フィールドに情報を入力します。
vNICx IPv6 アドレス (vNICx IPv6 Address)	VnicxIPv6Address	vNICx インターフェイスの IPv6 アドレス。	
vNICx IPv6 ネットマスク (vNICx IPv6 Netmask)	VnicxIPv6Netmask	vNICx インターフェイスの IPv6 プレフィックス。	
vNICx IPv6 スキップゲートウェイ (vNICx IPv6 Skip Gateway)	VnicxIPv6SkipGateway	オプションは [はい (yes)] または [いいえ (no)] です。 [はい (yes)] を選択すると、ゲートウェイの設定がスキップされません。	
vNICx IPv6 ゲートウェイ (vNICx IPv6 Gateway)	VnicxIPv6Gateway	vNICx ゲートウェイの IPv6 アドレス。	
DNS サーバ			
DNS アドレス (DNS Address) *	DNS	管理インターフェイスからアクセス可能な DNS サーバの IPv4/IPv6 アドレスのスペース区切りリスト。	
DNS 検索ドメイン (DNS Search Domain) *	ドメイン (Domain)	DNS 検索ドメイン	
DNS セキュリティ拡張機能 (DNS Security Extensions)	DNSSEC	DNS セキュリティ拡張機能を使用するかどうか。	

VMware パラメータ	CSP パラメータ	説明	その他の情報
DNS over TLS	DNSTLS	DNS over TLS を使用するかどうか。	
マルチキャスト DNS (Multicast DNS)	mDNS	マルチキャスト DNS を使用するかどうか。	
リンクローカルマルチ キャスト名前解決 (Link-Local Multicast Name Resolution)	LLMNR	Link-Local Multicast Name Resolution を使用 するかどうか。	
NTPv4サーバ			

VMware パラメータ	CSP パラメータ	説明	その他の情報
NTPv4 サーバ (NTPv4 Servers) *	NTP	管理インターフェイスからアクセス可能な NTPv4 サーバの IPv4/IPv6 アドレスまたはホスト名のスペース区切りリスト。	ここには、pool.ntp.org などの値を入力する必要があります。NTP サーバは、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。NTP サーバを使用していない場合は、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) と Crosswork Cloud 間のタイムギャップが 24 時間以下であることを確認します。そうでない場合、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) は接続に失敗します。
NTPv4 認証の使用 (Use NTPv4 Authentication)	NTPAuth	NTPv4 認証を使用するかどうか。	
NTPv4 キー (NTPv4 Keys)	NTPKey	サーバリストにマッピングするスペース区切りのキー ID。	

VMware パラメータ	CSP パラメータ	説明	その他の情報
NTPv4 キーファイル URI (NTPv4 Key File URI)	NTPKeyFile	chrony キーファイルへの SCP URI。	
NTPv4 キーファイルパスフレーズ (NTPv4 Key File Passphrase)	NTPKeyFilePwd	chrony キーファイルへの SCP URI のパスワード。	
リモート Syslog サーバ			

VMware パラメータ	CSP パラメータ	説明	その他の情報
リモート Syslog サーバを使用しますか? (Use Remote Syslog Server?)	UseRemoteSyslog	リモートホストに syslog メッセージを送信するか否か。	外部 syslog サーバを設定すると、サービスイベントが外部 syslog サーバに送信されます。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。
Syslog サーバのアドレス (Syslog Server Address)	SyslogAddress	管理インターフェイスからアクセス可能な syslog サーバの IPv4 または IPv6 アドレス。 (注) IPv6 アドレスを使用している場合は、角カッコ ([1::1]) で囲む必要があります。	外部 syslog サーバを使用する場合は、これらの 7 つの設定を行う必要があります。 (注) URI ファイルを含むホストは、ネットワーク上で (SCP を介して vNIC0 インターフェイスから) 到達可能でなければならず、ファイルはインストール時に存在する必要があります。
Syslog サーバポート (Syslog Server Port)	SyslogPort	Syslog サーバのポート番号。	
Syslog サーバプロトコル (Syslog Server Protocol)	SyslogProtocol	syslog の送信時に UDP、TCP、または RELP を使用します。	
TLS 経由の Syslog を使用するかどうか (Use Syslog over TLS?)	SyslogTLS	TLS を使用して syslog のトラフィックを暗号化します。	
Syslog TLS ピア名 (Syslog TLS Peer Name)	SyslogPeerName	サーバ証明書の SubjectAltName またはサブジェクトの共通名に入力されたとおりの syslog サーバのホスト名。	
Syslog ルート証明書ファイル URI (Syslog Root Certificate File URI)	SyslogCertChain	SCP を使用して取得した syslog サーバの PEM 形式のルート証明書。	
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。	

VMware パラメータ	CSP パラメータ	説明	その他の情報
リモート監査サーバ			
リモート監査サーバを使用しますか (Use Remote Auditd Server?)	UseRemoteAuditd	リモートホストに Auditd メッセージを送信するか。	必要に応じて、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) VM に変更が加えられると外部のリモート監査サーバが変更監査通知を送信するように設定できます。 外部の Auditd サーバを使用するには、これらの3つの設定を指定します。
Auditd サーバアドレス (Auditd Server Address)	AuditdAddress	オプションの監査サーバのホスト名、IPv4、または IPv6 アドレス。	
監査サーバポート (Auditd Server Port)	AuditdPort	オプションの監査サーバのポート番号。	
コントローラの設定			

VMware パラメータ	CSP パラメータ	説明	その他の情報
プロキシサーバの URL (Proxy Server URL)	ProxyURL	管理ネットワークプロキシサーバの URL。	クラウド導入では、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、プロキシサーバが環境に存在しない場合は、プロキシサーバが必要になる場合があります。 プロキシサーバを使用する場合は、これらのパラメータを指定する必要があります。
プロキシサーババイパスリスト (Proxy Server Bypass List)	ProxyBypass	プロキシサーバに送信されないサブネットとドメインのスペース区切りリスト。	
認証プロキシのユーザ名 (Authenticated Proxy Username)	ProxyUsername	認証済みプロキシサーバのユーザ名。	
認証プロキシのパスワード (Authenticated Proxy Passphrase)	ProxyPassphrase	認証済みプロキシサーバのパスワード。	
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)			

VMware パラメータ	CSP パラメータ	説明	その他の情報
登録の宛先ホストとパス (Enrollment Destination Host and Path) **	EnrollmentURI	SCP を使用して登録パッケージを転送する SCP ホストおよびパス (user@host:/path/to/file)。	Crosswork Cloud に Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を登録するには、登録パッケージが必要です。インストール中にこれらのパラメータを指定すると、登録パッケージは、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) の初回起動時にそのローカルホストに自動的に転送されます。 インストール時にこれらのパラメータを指定しない場合は、 登録パッケージのエクスポート (40 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する必要があります。
登録パスフレーズ (Enrollment Passphrase) **	EnrollmentPassphrase	登録パッケージを転送するための SCP ユーザパスフレーズ。	

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

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

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

- ステップ 1** Crosswork Data Gateway 2.0.x のリリースノートを参照し、CCO (*.ova) から推奨される Crosswork Data Gateway イメージファイルをダウンロードします。

警告 デフォルトの VMware vCenter の展開タイムアウトは 15 分です。OVF テンプレート展開の完了にかかる時間が 15 分を超えると、vCenter がタイムアウトし、最初からやり直す必要があります。これを防ぐために、展開を開始する前にテンプレートを確認し、入力する内容を決めておくことをお勧めします。

ステップ 2 vCenter Server クライアントに接続します。[アクション (Actions)] > [OVFテンプレートの展開 (Deploy OVF Template)] を選択します。

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

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

ファイル名がウィンドウに表示されます。

ステップ 4 次の図のように、[次へ (Next)] をクリックして [2 名前と場所の選択 (2 name and location)] に移動します。

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

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

Deploy OVF Template

✓ 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

- ✓ rcdn5-spm-vc-01.cisco.com
 - > Cisco-CX-Lab
 - > rcdn5-spm-dc-01
 - > rcdn5-spm-dc-02
 - > RTP

CANCEL

BACK

NEXT

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

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

展開する OVF テンプレートを確認します。

(注) この情報は OVF から収集され、変更はできません。

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

ステップ 8 次の図のように、[次へ (Next)] をクリックして [6 設定の選択 (6 Select configuration)] に移動します。[Crosswork Cloud] を選択します。

Deploy OVF Template

Configuration	Description
<input checked="" type="radio"/> Crosswork Cloud	8 CPU; 32GB RAM; 1-3 NICs; 70GB Disk
<input type="radio"/> Crosswork On-Premise Standard	
<input type="radio"/> Crosswork On-Premise Extended	

3 Items

CANCEL BACK NEXT

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

- a) [仮想ディスク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 provisioning)] を選択します。

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

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 10** 次の図のように、[次へ (Next)] をクリックして [8 ネットワークの選択 (8 Select networks)] に移動します。ページ上部のドロップダウンテーブルで、vNIC0、vNIC1、および vNIC2 に使用する vNIC の数に基づいて、各送信元ネットワークに適切な宛先ネットワークを選択します。

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

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
vNIC2	Crosswork-Devices
vNIC1	Crosswork-Internal
vNIC0	VM Network

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

ステップ 11 [次へ (Next)]をクリックして、[ホスト情報の設定 (Host Information Settings)]が展開された [9 テンプレートのカスタマイズ (Customize template)]に移動します。

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

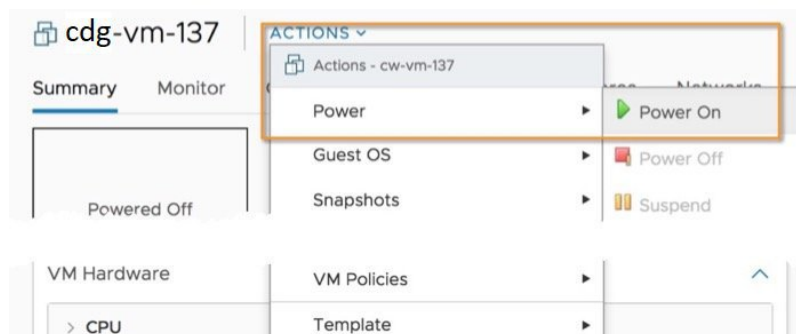
[Cisco Crosswork データゲートウェイ \(Cisco Crosswork Data Gateway\) 導入パラメータとシナリオ \(8 ページ\)](#) の説明に従って、パラメータの情報を入力します。

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

ステップ 13 展開ステータスを確認します。

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

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



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

警告 vCenter で VM のネットワーク設定を変更すると、意図しない重大な結果になる可能性があります。これには、スタティックルートと接続の損失などが含まれます。これらの設定を変更する場合は、自己責任で行ってください。IP アドレスを変更する場合は、現在の VM を破棄し、新しい VM を作成して、新しい VM を Crosswork Cloud に再登録します。

次のタスク

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

1. vCenter で VM を右クリックし、[コンソールを開く (Open Console)] を選択します。
2. ユーザ名（割り当てられたロールに応じて dg-admin または dg-oper）と、対応するパスワード（インストールプロセスで作成したパスワード）を入力し、Enter を押します。

SSH を介した Cisco Crosswork Data Gateway VM へのアクセス：

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

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

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

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

次の例を参考にしてください。

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

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

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

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。

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

要件に応じて、コマンドやスクリプトの必須またはオプションのパラメータを変更し、OVF ツールを実行できます。[Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）導入パラメータとシナリオ（8 ページ）](#)を参照してください。

スクリプトで OVF ツールを実行する場合のサンプルスクリプトを次に示します。

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

# robot.ova path

DG_OVA_PATH="<mention the orchestrator path>"

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

ActiveVnics="2"

Hostname="Hostname"
Vnic0IPv4Address="<Vnic0_ipv4_address>"
Vnic0IPv4Gateway="<Vnic0_ipv4_gateway>"
Vnic0IPv4Netmask="<Vnic0_ipv4_netmask>"
Vnic0IPv4Method="Static"
Vnic1IPv4Address="<Vnic1_ipv4_address>"
Vnic1IPv4Gateway="<Vnic1_ipv4_gateway>"
Vnic1IPv4Netmask="<Vnic1_ipv4_netmask>"
Vnic1IPv4Method="Static"

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

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

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

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

ProxyUsername="<username_for_proxy>"
```



```

ProxyPassphrase="<password_for_proxy>"

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

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

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
--powerOffTarget --powerOn \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"EnrollmentURI=$EnrollmentURI" \
--prop:"EnrollmentPassphrase=$EnrollmentPassphrase" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ActiveVnics=$ActiveVnics" \
--prop:"Vnic0IPv4Address=$Vnic0IPv4Address" \
--prop:"Vnic0IPv4Gateway=$Vnic0IPv4Gateway" \
--prop:"Vnic0IPv4Netmask=$Vnic0IPv4Netmask" \
--prop:"Vnic0IPv4Method=$Vnic0IPv4Method" \
--prop:"Vnic1IPv4Address=$Vnic1IPv4Address" \
--prop:"Vnic1IPv4Gateway=$Vnic1IPv4Gateway" \
--prop:"Vnic1IPv4Netmask=$Vnic1IPv4Netmask" \
--prop:"Vnic1IPv4Method=$Vnic1IPv4Method" \
--prop:"DNS=$DNS" \
--prop:"NTP=$NTP" \
--prop:"dg-adminPassword=$dg_adminPassword" \
--prop:"dg-operPassword=$dg_operPassword" \
--prop:"Domain=$Domain" $DG_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"

```

ステップ 1 コマンドプロンプトを開きます。

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

ステップ 3 OVF ツールをインストールした場所に移動します。

ステップ 4 次のいずれかの方法で OVF ツールを実行します。

a) コマンドの使用

次のコマンドを実行します。

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

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

次の例を参考にしてください。

```

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds="datastore130-2"
--deploymentOption="cloud" --diskMode="thin" --overwrite --powerOffTarget --powerOn
--noSSLVerify --allowExtraConfig --extraConfig:firmware=efi
--extraConfig:uefi.secureBoot.enabled=true --name="cdg147.cisco.com"
--prop:"Hostname=cdg147.cisco.com" --prop:"Description=CDG Base VM for Automation"
--net:"vNIC0=VM Network" --prop:"Vnic0IPv4Method=Static"
--prop:"Vnic0IPv4Address=<vNIC 0 IPv4 address>" --prop:"Vnic0IPv4Netmask=<vNIC0 IPv4 netmask>"

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

```

b) スクリプトの使用

コマンドと引数を含めて作成したスクリプトを実行するには、次の手順を実行します。

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

次のタスク

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

1. vCenter で VM を右クリックし、[コンソールを開く (Open Console)] を選択します。
2. ユーザ名 (割り当てられたロールに応じて dg-admin または dg-oper) と、対応するパスワード (インストールプロセスで作成したパスワード) を入力し、Enter を押します。

SSH を介した Cisco Crosswork Data Gateway VM へのアクセス :

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

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

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

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

次の例を参考にしてください。

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

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

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

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。

Cisco CSP に Crosswork Data Gateway をインストールする

Cisco CSP に 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 CSP にアップロードするための Crosswork Data Gateway のサービスイメージを準備します。

- a) Crosswork Data Gateway `qcow2` ビルドを CCO からローカルマシンまたは Cisco CSP が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て展開します。

ビルドは、`qcow2` および `config.txt` ファイルの `tarball` です。

- 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。[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 \(8 ページ\)](#) を参照してください。

(注) 複数の Data Gateway VM をインストールする予定の場合は、Data Gateway VM ごとに一意の `config.txt` ファイルを作成します。

次のパラメータには事前定義された値があります。

- 展開
 - 「クラウド」を使用します。

次に、`config.txt` ファイルの例を示します。

```
ActiveVnics=
AuditdAddress=
AuditdPort=
Deployment=cloud
Description=
DGAppdataDisk=
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=changeme
DNSSEC=False
DNSTLS=False
Domain=changeme
EnrollmentPassphrase=
EnrollmentURI=
Hostname=changeme
Label=
LLMNR=False
mDNS=False
NTP=changeme
NTPAuth=False
NTPKey=
NTPKeyFile=
```

Cisco CSP に Crosswork Data Gateway をインストールする

```

NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv6Address=:0
Vnic0IPv6Gateway=:1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic1IPv4Address=0.0.0.0
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=None
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv6Address=:0
Vnic1IPv6Gateway=:1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic2IPv4Address=0.0.0.0
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=None
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv6Address=:0
Vnic2IPv6Gateway=:1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
dg-adminPassword=changeme
dg-operPassword=changeme

```

ステップ 2 Cisco CSP に Crosswork Data Gateway のサービスイメージをアップロードする

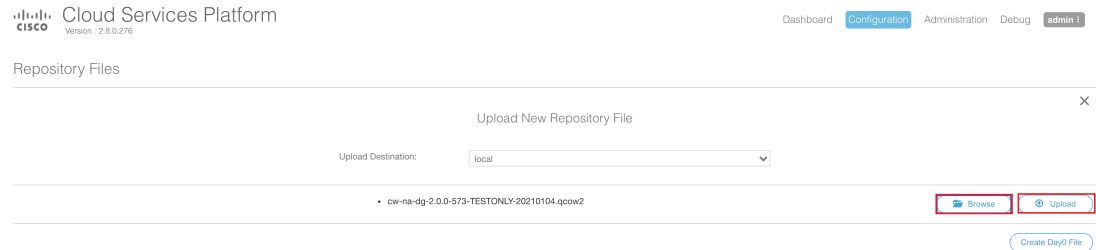
- Cisco CSP にログインします。
- [設定 (Configuration)] > [リポジトリ (Repository)] に移動します。
- [リポジトリファイル (Repository Files)] ページで、[Crosswork Data Gateway] ボタンをクリックします。



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

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

この手順を繰り返して、config.txt ファイルをアップロードします。

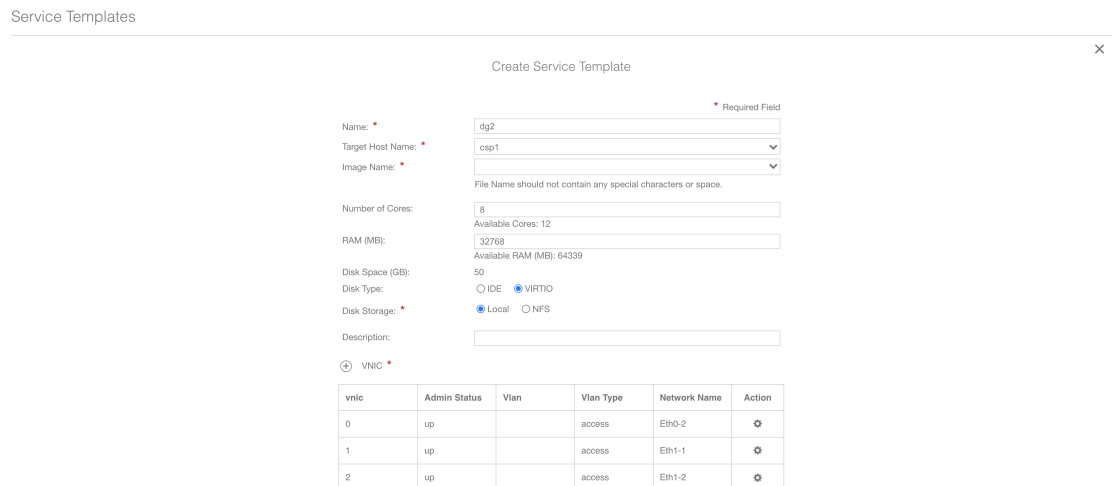


ファイルがアップロードされると、ファイル名とその他の関連情報が [リポジトリファイル (Repository Files)] テーブルに表示されます。

ステップ 3 Crosswork Data Gateway のサービスを作成する

- [設定 (Configuration)] > [サービス (Services)] に移動します。
- [サービス (Service)] ページで、[+] ボタンをクリックします。
- [サービスの作成 (Create Service)] オプションをオンにします。

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

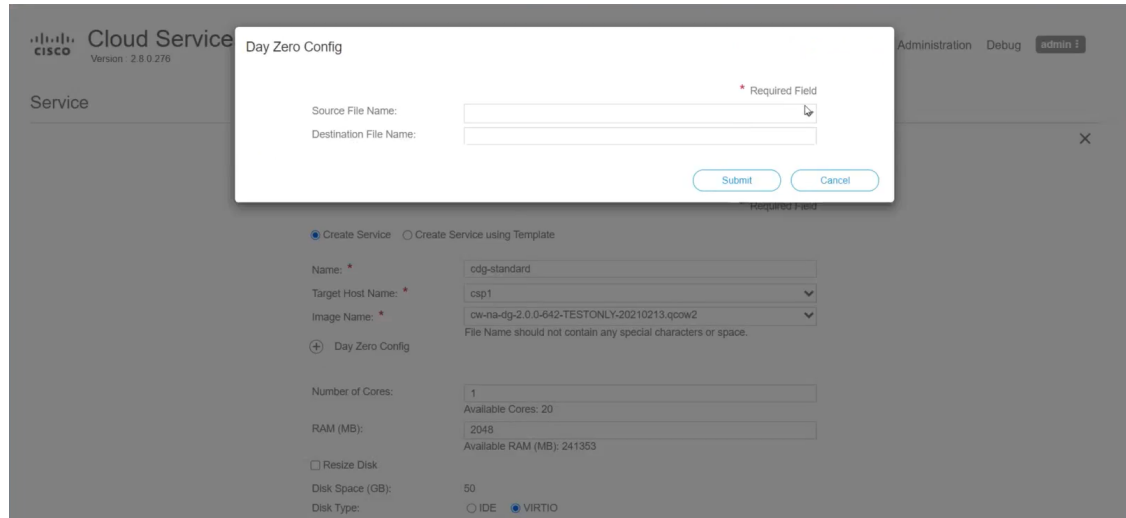


- d) 次のフィールドに値を入力します。

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

フィールド	説明
イメージ名 (Image Name)	qcow2 イメージを選択します。

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



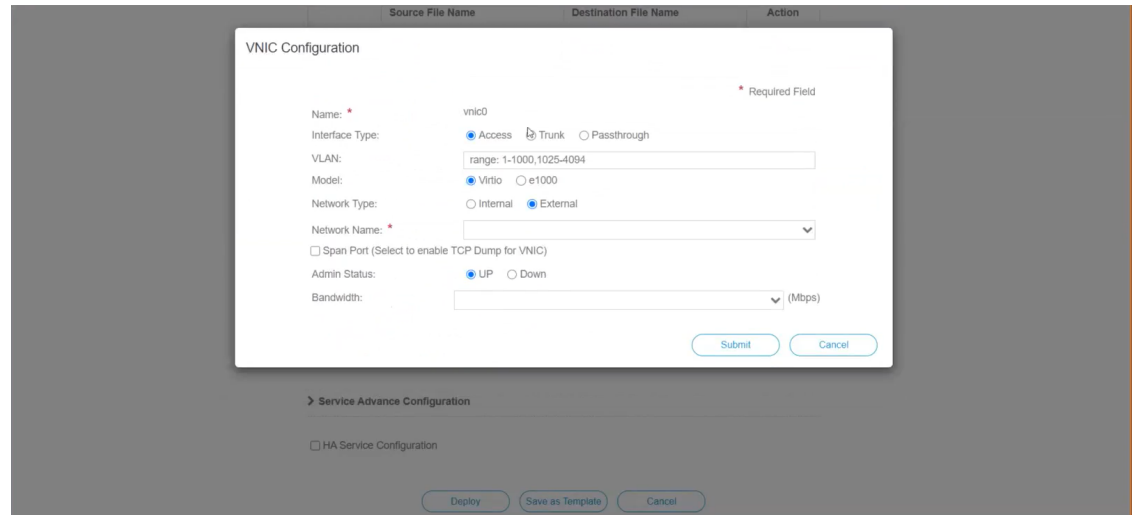
[デイゼロの設定 (Day Zero Config)] ダイアログボックスで、次の手順を実行します。

1. [ソースファイル名 (Source File Name)] ドロップダウンリストから、以前に変更してアップロードした config.txt ファイルを選択します。
2. [宛先ファイル名 (Destination File Name)] フィールドに「config.txt」と入力します。
3. [送信 (Submit)] をクリックします。

- f) 次のフィールドに値を入力します。

フィールド	説明
コア数 (Number of Cores)	8
RAM (MB)	32768

- g) [vNIC] をクリックします。



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

(注) VNIC 名はデフォルトで設定されます。

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

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

5. [管理ステータス (Admin Status)] として [稼働中 (UP)] を選択します。
6. [送信 (Submit)] をクリックします。
7. ネットワークで複数の VNIC を使用する予定の場合は、VNIC1 と VNIC2 に対して手順 g を繰り返します。

3つの VNIC をすべて追加すると、VNIC テーブルは次のようになります。

⊕ VNIC *

vnic	Admin Status	Vlan	Vlan Type	Network Name	Action
0	up		access	Eth0-1	⚙️
1	up		access	Eth1-1	⚙️
2	up		access	Eth1-2	⚙️

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

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

- i) [ストレージ (Storage)] をクリックします。

[ストレージの設定 (Storage Configuration)] ダイアログボックスで、次のように設定します。

フィールド	説明
名前	ストレージの名前。これはデフォルトで指定されます。
デバイスタイプ (Device Type)	[ディスク (Disk)] を選択します。
ロケーション (Location)	[ローカル (local)] を選択します。
ディスクの種類 (Disk Type)	[VIRTIO] を選択します。
フォーマット (Format)	[QCOW2] を選択します。
イメージファイルをディスクとしてマウントしますか。 (Mount image file as disk?)	このチェックボックスはオフのままにします。
サイズ (GB) (Size (GB))	ディスクサイズとして 70GB と入力します。

ストレージの設定が完了したら、[送信 (Submit)] をクリックします。

j) [展開 (Deploy)] をクリックします。

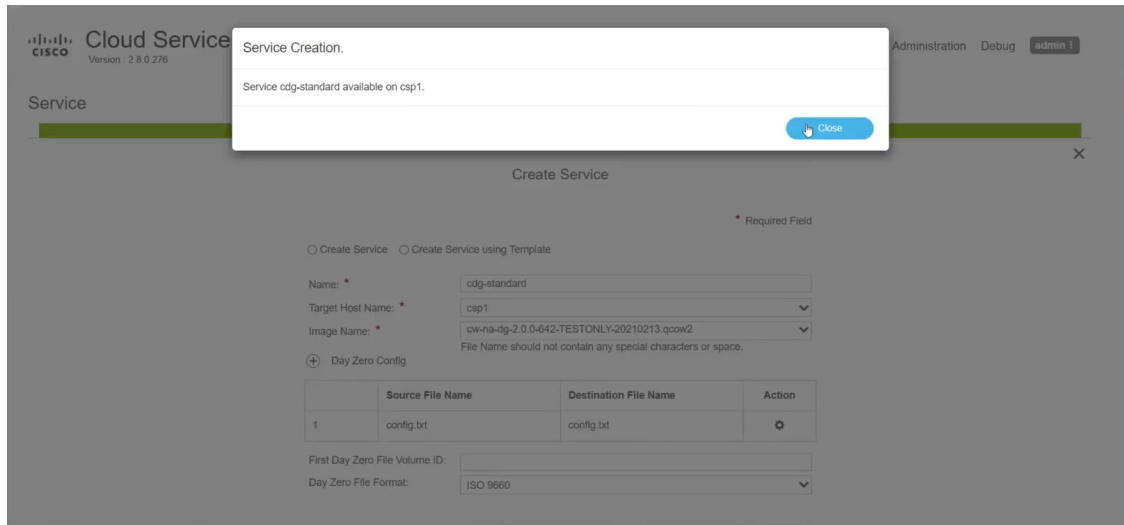
The screenshot shows a configuration form with the following fields and values:

- Cache Mode: none
- Emulator Range: [empty]
- Max Emulator Range: 0-7
- VM Health Monitoring Configuration:
 - Status: disabled
 - VNF Management IP: VNF Management IP x.x.x.x
 - VNF Group: default-vnf-group
 - VNC Port: VNC Port Range : 8721 - 8784
 - VNC Password: [empty]
 - Confirm VNC Password: [empty]
- Storage:

Storage	Storage Type	Size (GB) / Disk Image Name	Action
1	disk (virtio)	5	[gear icon]
- Serial Port: [empty]
- HA Service Configuration:

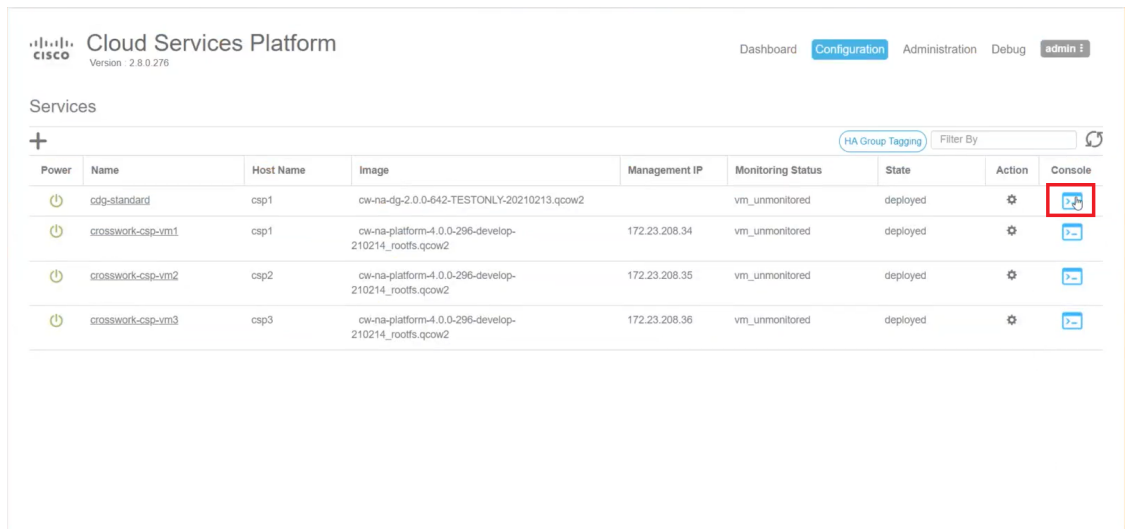
At the bottom, there are three buttons: **Deploy** (highlighted with a red box), **Save as Template**, and **Cancel**.

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



ステップ 4 Crosswork Data Gateway サービスの展開

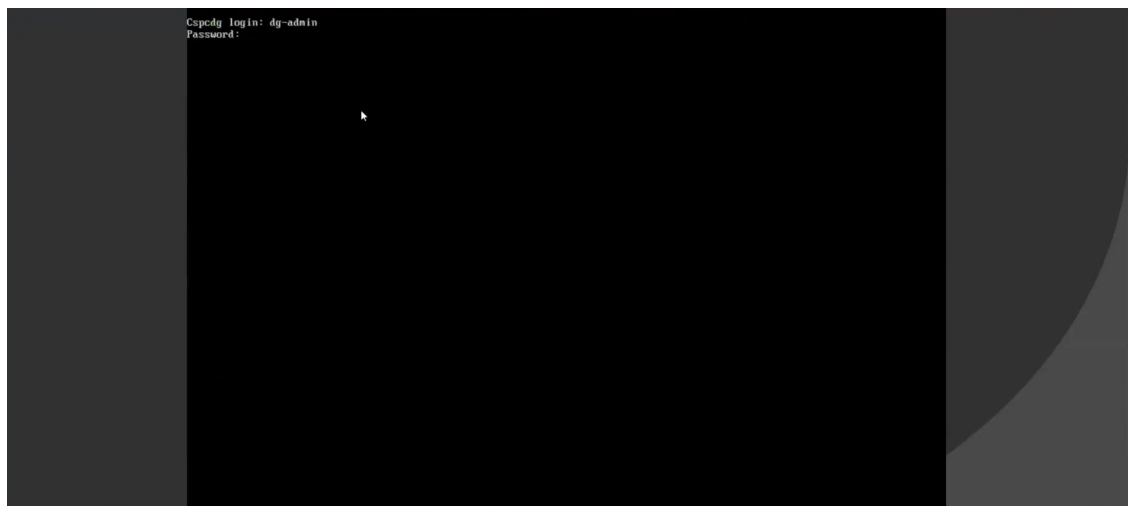
- [設定 (Configuration)] > [サービス (Services)] に移動します。
- [サービス (Services)] テーブルで、上記で作成した Crosswork Data Gateway サービスの [コンソール (Console)] 列の下にあるコンソールアイコンをクリックします。



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



- d) Crosswork Data Gateway サービスが接続されたら、`dg-admin` ユーザまたは `dg-oper` ユーザ（割り当てられたロールに応じて）と、`config.txt` ファイルに入力した対応するパスワードでログインします。



Crosswork Data Gateway コンソールを使用できます。

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（OVF 導入シナリオの「**自動登録パッケージ**」を参照）。

- インタラクティブメニューの[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 \(40 ページ\)](#) を参照)。

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

インストール時に登録パッケージをエクスポートしないことを選択した場合は、Crosswork Data Gateway を Crosswork Cloud に登録する前にエクスポートする必要があります。手順については、[登録パッケージのエクスポート \(40 ページ\)](#) を参照してください。



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

登録パッケージ JSON のサンプルを次に示します。

```
{
  "name": "dg116.cisco.com",
  "description": "CDG Base VM for Automation",
  "profile": {
    "cpu": 8,
    "memory": 31,
    "nics": 3
  },
  "interfaces": [
    {
      "name": "eth0",
      "mac": "00:50:56:9e:09:7a",
      "ipv4Address": "<ip_address>/24"
    },
    {
      "name": "eth1",
      "mac": "00:50:56:9e:67:c3",
      "ipv4Address": "<ip_address>/16"
    },
    {
      "name": "eth2",
      "mac": "00:50:56:9e:83:83",
      "ipv4Address": "<ip_address>/16"
    }
  ],
  "certChain": [
    "<cert_chain>"
  ],
  "version": "1.1.0 (branch dg110dev - build number 152)",
  "duuid": "d58fe482-fdca-468b-a7ad-dfbfa916e58b"
}
```

登録パッケージのエクスポート

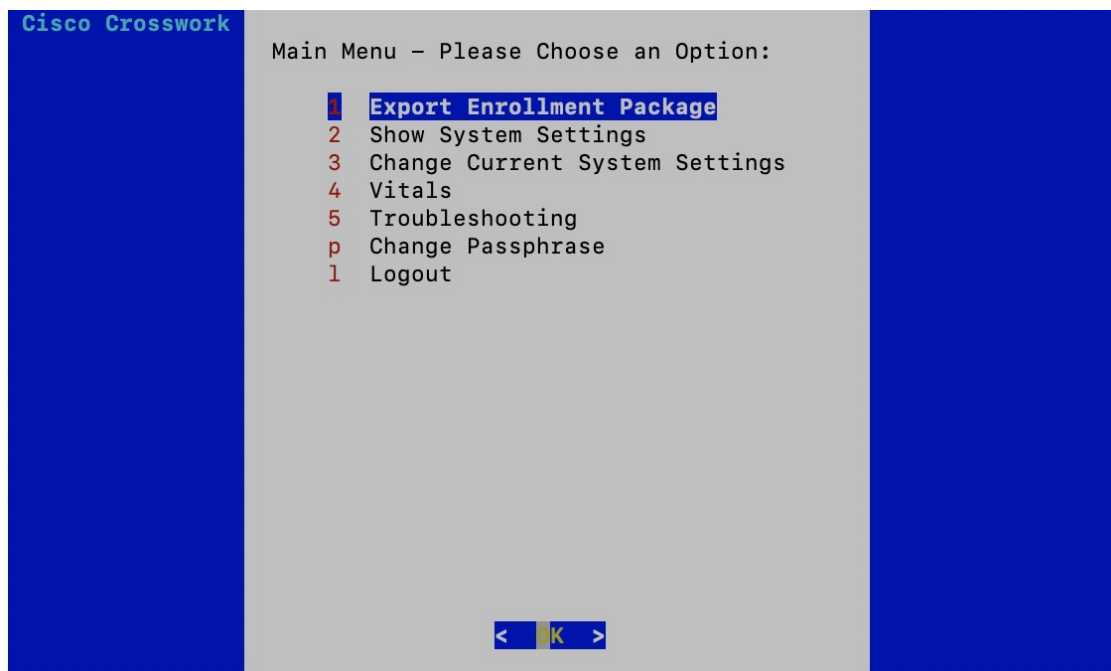
Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を Crosswork Cloud に登録するには、ローカルコンピュータに登録パッケージのコピーが必要です。



- (注) インストール時に**自動登録パッケージ転送設定**を指定していない場合のみ、コピーが必要になります。指定している場合、ファイルは VM の起動後に選択した SCP URI の宛先にコピーされます。

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

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



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

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

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

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

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

ステップ 6 Crosswork Cloud への Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) の登録を続行します。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、『Cisco Crosswork Cloud User Guide』の「Add Cisco Crosswork Data Gateway Information」の章を参照してください。

Cisco Crosswork Trust Insights または Cisco Crosswork Flow Insights に Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を登録する場合は、次の手順も実行します。これらの手順は任意であり、ネットワーク環境によって異なります。

- [制御プロキシの設定 \(50 ページ\)](#)
- [Crosswork Data Gateway のバイタルの表示](#)



第 4 章

Crosswork Data Gateway VM の設定

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

この章は次のトピックで構成されています。

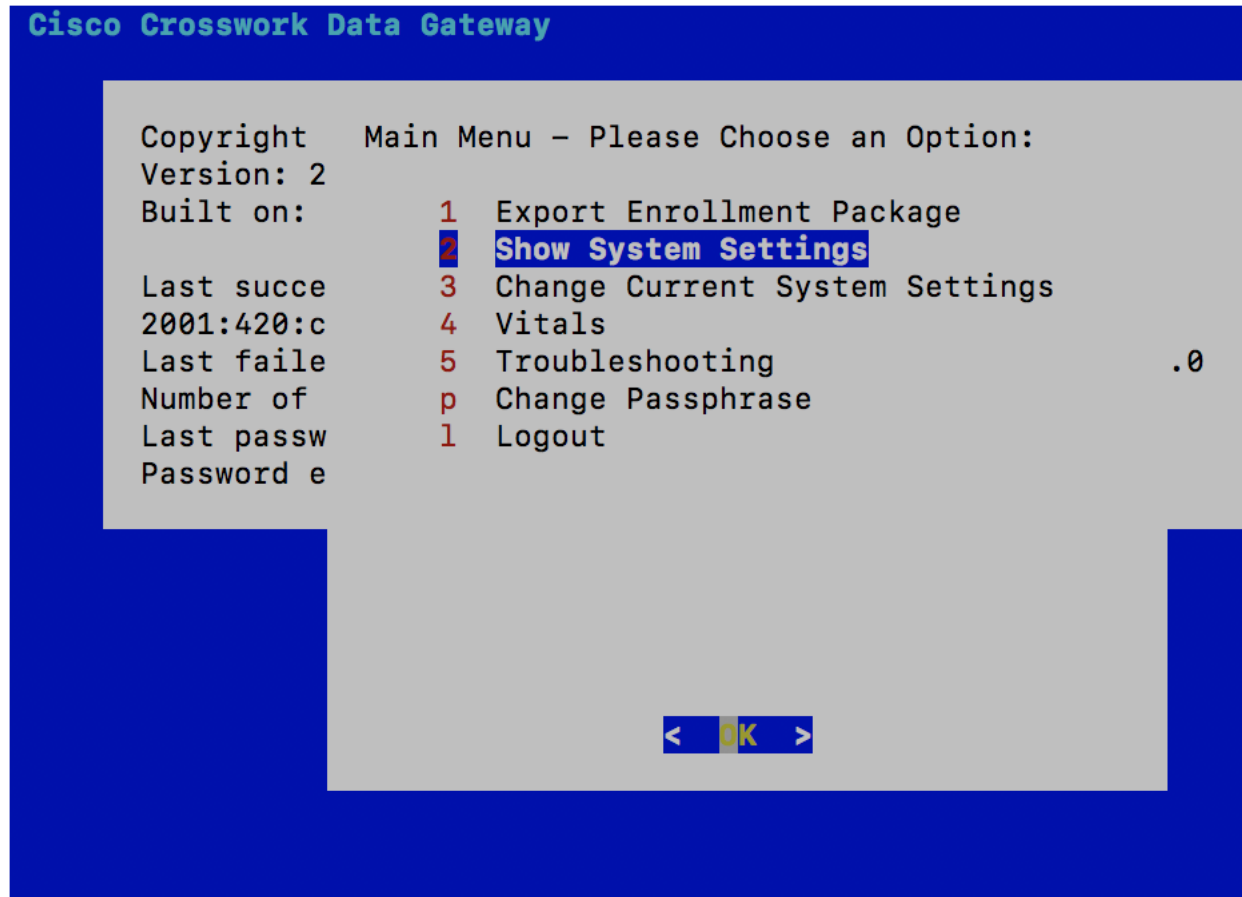
- [インタラクティブなコンソールの使用](#) (43 ページ)
- [Crosswork Data Gateway ユーザーの管理](#) (44 ページ)
- [現在のシステム設定の表示](#) (47 ページ)
- [現在のシステム設定の変更](#) (49 ページ)
- [Crosswork Data Gateway のバイタルの表示](#) (56 ページ)
- [Crosswork Data Gateway VM のトラブルシューティング](#) (58 ページ)

インタラクティブなコンソールの使用

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



(注) ここに示すメインメニューは、`dg-admin` ユーザに対応しています。オペレータには管理者と同じ権限はないため、`dg-oper` ユーザの場合とは異なります。[表 4: 各ロールの権限](#) (45 ページ) を参照してください。



メインメニューには、次のオプションが表示されます。

1. 登録パッケージのエクスポート
2. システム設定の表示
3. 現在のシステム設定の変更
4. バイタル
5. トラブルシューティング
 - p. パスフレーズの変更
 - l. ログアウト

Crosswork Data Gateway ユーザーの管理

ここでは、次の内容について説明します。

- [サポートされるユーザ ロール \(45 ページ\)](#)

- [パスワードの変更 \(47 ページ\)](#)

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。このユーザは削除できず、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) の起動/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、サーバの設定、カーネルのアップグレードなどの読み取りおよび書き込み権限があります。
- **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。オペレータは、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) の状態/正常性を確認し、正常性/エラーログを取得し、エラー通知を受け取り、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) インスタンスと出力先の間で接続テストを実行することができます。



(注)

- どちらのユーザのログイン情報も、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) のインストール時に設定されます。
- 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 4: 各ロールの権限

権限	管理者	オペレータ
登録パッケージのエクスポート	✓	✓
システム設定の表示		

権限	管理者	オペレータ
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		
NTP の設定 DNS の設定 制御プロキシの設定 スタティックルートの設定 Syslog の設定 新しい SSH キーの作成 証明書のインポート vNIC2 MTU の設定 タイムゾーンの設定 パスワード要件の設定	✓	×
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	✓	✓

権限	管理者	オペレータ
トラブルシューティング		
ホストへの Ping	✓	✓
ホストに対するトレースルート	✓	✓
NTP ステータス	✓	✓
システム稼働時間	✓	✓
show-tech の実行	✓	✓
すべてのコレクタの削除と VM の再起動	✓	×
SSH 接続のテスト	✓	✓
auditd ログのエクスポート	✓	×
TAC シェルアクセスの有効化		
パスフレーズの変更	✓	✓

パスワードの変更

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

自分のパスフレーズを変更するには、次の手順を実行します。

-
- ステップ 1** メインメニューから、[パスフレーズの変更 (Change Passphrase)] を選択し、[OK] をクリックします。
- ステップ 2** 現在のパスワードを入力し、[Enter] キーを押します。
- ステップ 3** 新しいパスワードを入力し、[Enter] キーを押します。パスワードをもう一度入力して、[Enter] キーを押します。
-

現在のシステム設定の表示

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

- 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を表示するには、次の手順を実行します。

- ステップ 1** 次の図に示すように、メインメニューから [2 システム設定の表示 (2 Show System Settings)] を選択します。
- ステップ 2** [OK] をクリックします。[現在のシステム設定の表示 (Show Current System Settings)] メニューが開きます。
- ステップ 3** 表示する設定を選択します。

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

設定オプション	説明
[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
- vNIC2 MTU
- タイムゾーン
- パスワード要件



- (注) • Crosswork Data Gateway システム設定は管理者のみが設定できます。

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 \(60 ページ\)](#) 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 \(56 ページ\)](#)」を参照してください。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 방법으로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

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。Crosswork クラウドへの接続に使用する場合、Data Gateway はパブリック HTTP サーバに接続する必要があります。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/HTTPS プロキシが必要な環境の場合は、Cisco Crosswork Data Gateway が Crosswork クラウドサービスに正常に接続できるようにプロキシサーバを設定する必要があります。

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

-
- ステップ 1** [現在のシステム設定の変更 (Change Current System Settings)] メニューから、[3 制御プロキシの設定 (3 Configure Control Proxy)] を選択し、[OK] をクリックします。
- ステップ 2** 続行する場合は、次のダイアログで [はい (Yes)] をクリックします。続行しない場合は、[キャンセル (Cancel)] をクリックします。
- ステップ 3** 次のように新しいプロキシサーバの詳細を入力します。
- サーバ URL
 - バイパスアドレス
 - プロキシユーザ名
 - プロキシパスフレーズ
- ステップ 4** 設定を保存するには [OK] をクリックします。
-

スタティックルートの設定

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



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

スタティックルートの追加

スタティックルートを追加するには、次の手順を実行します。

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

Syslog の設定



-
- (注) 異なる Linux ディストリビューションで IPv4/IPv6 をサポートする Syslog サーバ設定については、システム管理者および設定ガイドを参照してください。
-

次の手順に従い、Syslog を設定します。

- ステップ 1** [現在のシステム設定の変更 (Change Current System Settings)]メニューから、[5 Syslogの設定 (5 Configure Syslog)]を選択します。
- ステップ 2** 次の syslog 属性の新しい値を入力します。
- [サーバアドレス (Server address)] : 管理インターフェイスからアクセス可能な syslog サーバの IPv4 または IPv6 アドレス。IPv6 アドレスを使用している場合は、角カッコ ([1 :: 1]) で囲む必要があります。
 - [ポート (Port)] : syslog サーバのポート番号。
 - [プロトコル (Protocol)] : syslog の送信時に UDP、TCP、または RELP を使用します。
 - [TLS経由のSyslogを使用する? (Use Syslog over TLS?)] : TLS を使用して syslog トラフィックを暗号化します。
 - [TLSピア名 (TLS Peer Name)] : サーバ証明書の SubjectAltName またはサブジェクト共通名に入力されたとおりの Syslog サーバのホスト名。
 - [Syslogルート証明書ファイルURI (Syslog Root Certificate File URI)] : SCP を使用して取得した Syslog サーバの PEM 形式のルート証明書。
 - [Syslog証明書ファイルのパスフレーズ (Syslog Certificate File Passphrase)] : Syslog 証明書チェーンを取得する SCP ユーザのパスワード。

ステップ3 設定を保存するには [OK] をクリックします。

新しい SSH キーの作成

新しい SSH キーを作成すると、現在のキーが削除されます。

次の手順に従って、新しい SSH キーを作成します。

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

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

証明書のインポート

コントローラ署名証明書以外の証明書を更新すると、コレクタが再起動します。

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

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

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

ステップ2 インポートする証明書を選択します。

ステップ3 選択した証明書ファイルの SCP URI を入力します。

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

vNIC2 MTU の設定

3つのNICを使用している場合にのみ、vNIC2 MTU を変更できます。

インターフェイスがジャンボフレームをサポートしている場合、MTU 値の範囲は 60 ~ 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。

タイムゾーンの設定

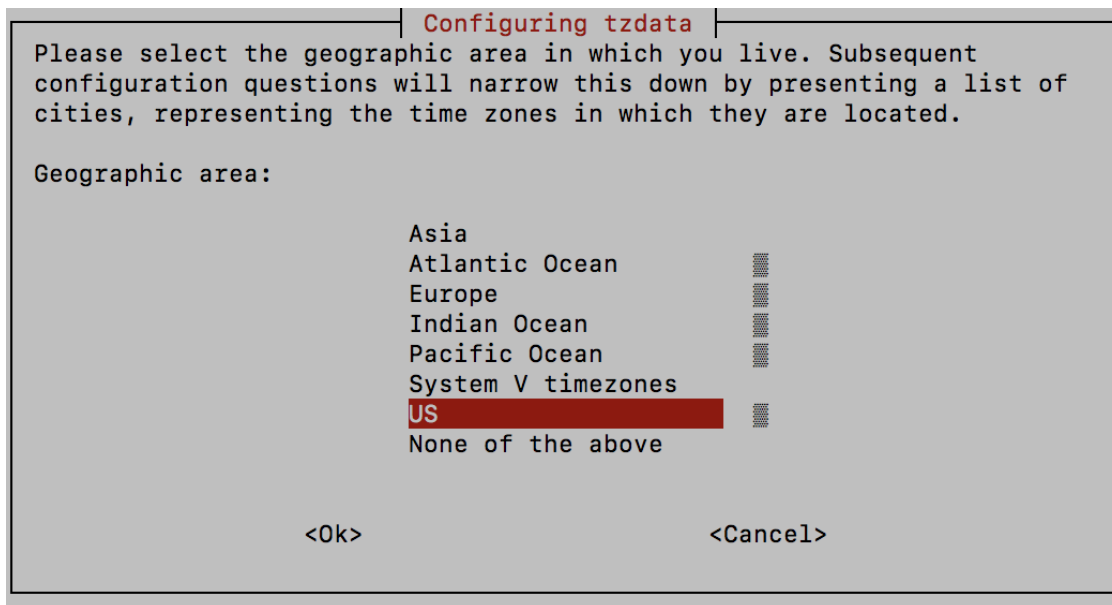
Crosswork Data Gateway は、最初にデフォルトのタイムゾーン (UTC) で起動します。

次の手順に従って、タイムゾーンを設定します。

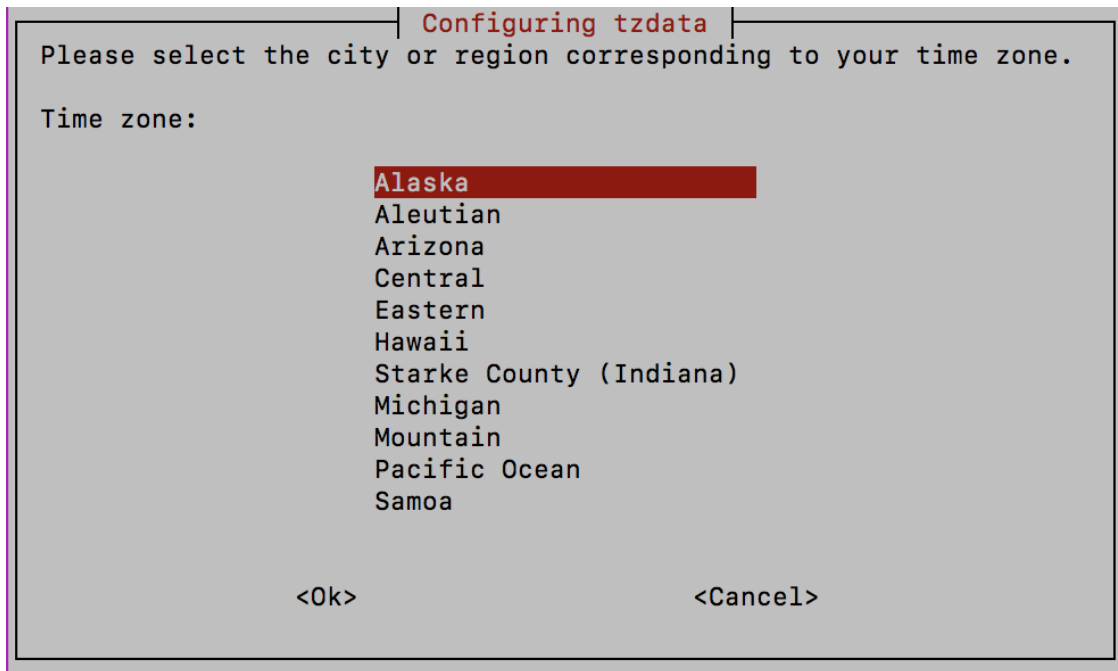
ステップ 1 Crosswork Data GatewayVM のインタラクティブメニューで、[現在のシステム設定の変更 (Change Current System Settings)] を選択します。

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

ステップ 3 居住地域を選択します。



ステップ 4 タイムゾーンに対応する都市または地域を選択します。



ステップ 5 [OK] を選択して設定を保存します。

ステップ 6 Crosswork Data GatewayVM をリブートして、すべてのプロセスで新しいタイムゾーンが選択されるようにします。

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。

Crosswork Data Gateway のバイタルの表示

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

ステップ 1 メインメニューで、**バイタル**を 4 つ選択します。

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

バイタル	説明
Docker コンテナ (Docker Containers)	<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>
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> <p>リポジトリ (Repository)</p> <p>イメージ ID (Image ID)</p> <p>作成時刻 (Created Time)</p> <p>サイズ (Size)</p> <p>タグ (Tag)</p>
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> <p>デフォルト IPv4 ゲートウェイ (Default IPv4 gateway)</p> <p>デフォルト IPv6 ゲートウェイ (Default IPv6 gateway)</p> <p>DNS サーバ (DNS server)</p> <p>コントローラ (Controller)</p> <p>コントローラセッションのステータス (Controller session status)</p>
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> <p>NTP サーバの解決 (NTP server resolution)</p> <p>Ping</p> <p>NTP ステータス (NTP Status)</p> <p>現在のシステム時間 (Current system time)</p>
ルートテーブル (Route Table)	<p>IPv4 および IPv6 ルーティングテーブルを表示します。</p>

バイタル	説明
ARP テーブル (ARP Table)	ARP テーブルを表示します。
ネットワーク接続 (Network Connections)	現在のネットワーク接続とリスニングポートを表示します。
ディスク領域使用率 (Disk Space Usage)	すべてのパーティションの現在のディスク容量の使用状況を表示します。
Linux サービス (Linux Services)	次の Linux サービスのステータスを表示します。 <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

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、次の図に示すように、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) 次の図に、dg-admin ユーザに対応する [トラブルシューティング (Troubleshooting)] メニューを示します。dg-oper ユーザはこれらのオプションの一部を使用できません。表 4: 各ロールの権限 (45 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。

- [ホストへの Ping \(59 ページ\)](#)
- [ホストに対するトレースルート \(59 ページ\)](#)
- [NTP ステータスの確認 \(59 ページ\)](#)
- [システム稼働時間の確認 \(60 ページ\)](#)
- [show-tech の実行 \(60 ページ\)](#)
- [SSH 接続のテスト \(60 ページ\)](#)

- [auditd ログのエクスポート \(61 ページ\)](#)

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 [トラブルシューティング (Troubleshooting)]メニューから [1 ホストへのPing (1 Ping a Host)]を選択します。

ステップ 2 次の情報を入力します。

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

ステップ 3 [OK] をクリックします。

ホストに対するトレースルート

Crosswork Data Gateway は、遅延の問題のトラブルシューティングに役立つ[ホストに対するトレースルート (Traceroute to a Host)] オプションを提供します。このオプションを使用すると、Crosswork Data Gateway がコントローラ アプリケーション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 [トラブルシューティング (Troubleshooting)]メニューから、[2 ホストに対するトレースルート (2 Traceroute to a Host)]を選択します。

ステップ 2 トレースルート先を入力します。

ステップ 3 [OK] をクリックします。

NTP ステータスの確認

NTP サーバのステータスを確認するには、このオプションを使用します。

ステップ 1 [トラブルシューティング (Troubleshooting)]メニューから、[3 NTPステータス (3 NTP Status)]を選択します。

ステップ2 [OK] をクリックします。cdg は NTP サーバのステータスを表示します。

システム稼働時間の確認

手順に従って、最後のリブート以降のシステム稼働時間を確認します。

ステップ1 [トラブルシューティング (Troubleshooting)]メニューから、[4 システム稼働時間 (4 System Uptime)]を選択します。

ステップ2 [OK] をクリックします。Crosswork Data Gateway にシステムの稼働時間が表示されます。

show-tech の実行

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

次のようなデータが収集されます。

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

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

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

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

ステップ2 ログとバイタルを含む tarball の保存先を入力します。

ステップ3 SCP パスフレーズを入力し、[OK] をクリックします。

SSH 接続のテスト

この操作は、クライアント側で完全なデバッグが有効な状態で SSH 接続を試行します。

1. [トラブルシューティング (Troubleshooting)]メニューから、[8 SSHのテスト (8 Test SSH)]を選択します。
2. 次の詳細を入力します。
 - ポート (Port)

- ホスト (Host)
- ユーザ名 (Username)
- パスフレーズ (Passphrase)

3. [OK] をクリックします。

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。

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。

TAC シェルイベントの監査

- 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** 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>`
- ステップ 8** `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。シスコのエンジニアは、SWIMS Aberto ツールを使用してこのトークンに署名する必要があります。
- ステップ 9** 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。トラブルシューティングについては、シスコのエンジニアの指示に従ってください。
`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。
- ステップ 10** 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 \(63 ページ\)](#)
- [Cisco CSPからの Crosswork Data Gateway サービスの削除 \(64 ページ\)](#)

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。

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

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

始める前に

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

ステップ 1 Cisco CSP にログインします。

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

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

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