Crosswork Data Gateway VM の設定

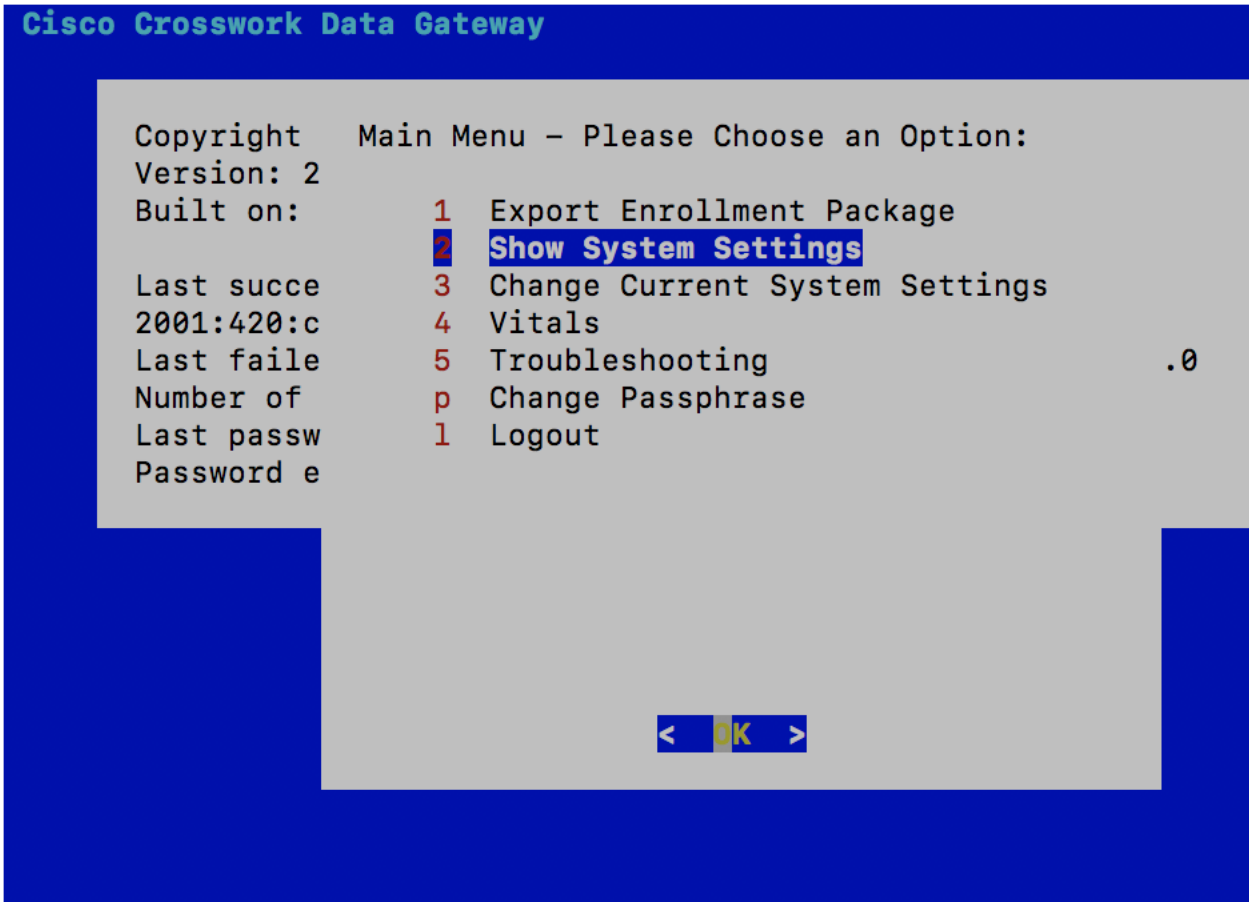
Cisco Crosswork Data Gateway インスタンスは、スタンドアロン VM として作成されており、コントローラ アプリケーションとは別の場所に配置することができます（コントローラ アプリケーションは、Crosswork Cloud です）。この VM は、ネットワークからのデータ収集を可能にするコントローラ アプリケーションに接続できます。

この章は次のトピックで構成されています。

インタラクティブなコンソールの使用

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

（注） ここに示すメインメニューは、**dg-admin** ユーザに対応しています。オペレータには管理者と同じ権限はないため、**dg-oper** ユーザーの場合とは異なります。表 1 : 各ロールの権限 （3 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

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 *1* : 各ロールの権限

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

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

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

パスワードの変更

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

自分のパスフレーズを変更するには、次の手順を実行します。

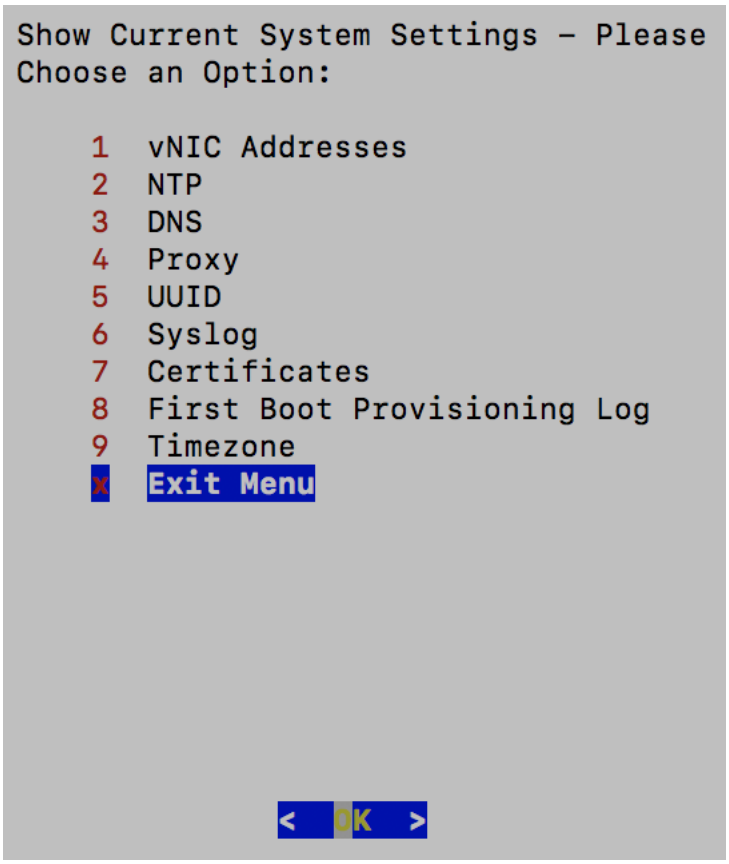
ステップ 1 メインメニューから、[パスフレーズの変更（Change Passphrase）] を選択し、[OK] をクリックします。

ステップ 2 現在のパスワードを入力し、[Enter] キーを押します。

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

現在のシステム設定の表示

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



現在のシステム設定を表示するには、次の手順を実行します。

ステップ 1 次の図に示すように、メインメニューから [2 システム設定の表示（2 Show System Settings）] を選択します。

ステップ 2 [OK] をクリックします。[現在のシステム設定の表示（Show Current System Settings）] メニューが開きます。

ステップ 3 表示する設定を選択します。

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

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

現在のシステム設定の変更

Crosswork Data Gateway では、次の設定を行います。

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

- Idle timeout.
- auditd を設定します。

（注）

- Crosswork Data Gateway システム設定は管理者のみが設定できます。
- SCP を使用する必要がある設定オプションで、SCP デフォルトの SCP ポート 22 を使用しない場合は、SCP コマンドの一部としてポートを指定できます。次の例を参考にしてください。

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

55 はカスタムポートです。

NTP の設定

NTP 時刻は、コントローラ アプリケーションおよびそのCrosswork Data Gatewayインスタンスと同期することが重要です。同期しないと、セッションハンドシェイクが行われず、機能イメージはダウンロードされません。その場合、「clock time not match and sync failed」というエラーメッセージが controller-gateway.log に記録されます。ログファイルにアクセスするには、show-tech の実行 （21 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 （16 ページ）」を参照）。NTP が正しく設定されていないと、「Session not established」というエラーが表示されます。

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

NTP 設定を構成するには、次の手順に従ってください。

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

ステップ 2 次のように新しい NTP サーバの詳細を入力します。

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

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

ステップ 3 設定を保存するには [**OK**] をクリックします。

DNS の設定

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

ステップ 2 新しい DNS サーバアドレスとドメインを入力します。

ステップ 3 設定を保存するには [**OK**] をクリックします。

制御プロキシの設定

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

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

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

ステップ 3 次のように新しいプロキシサーバの詳細を入力します。

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

ステップ 4 設定を保存するには [**OK**] をクリックします。

スタティックルートの設定

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

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

スタティック ルートの追加

スタティックルートを追加するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[4 スタティックルートの設定（4 Configure Static Routes）] を選択します。

ステップ 2 スタティックルートを追加するには、[追加（Add）] を選択します。

ステップ 3 スタティックルートを追加するインターフェイスを選択します。

ステップ 4 IP バージョンを選択します。

ステップ 5 プロンプトが表示されたら、CIDR 形式で IPv4 または IPv6 サブネットを入力します。

ステップ 6 設定を保存するには [**OK**] をクリックします。

スタティック ルートの削除

スタティックルートを削除するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[4 スタティックルートの設定（4 Configure Static Routes）] を選択します。

ステップ 2 スタティックルートを削除するには、[削除（Delete）] を選択します。

ステップ 3 スタティックルートを削除するインターフェイスを選択します。

ステップ 4 IP バージョンを選択します。

ステップ 5 CIDR 形式で IPv4 または IPv6 サブネットを入力します。

ステップ 6 設定を保存するには [**OK**] をクリックします。

Syslog の設定

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

次の手順に従い、Syslog を設定します。

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

ステップ 2 次の syslog 属性の新しい値を入力します。

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

ステップ 3 設定を保存するには [**OK**] をクリックします。

新しい SSH キーの作成

新しい SSH キーを作成すると、現在のキーが削除されます。

次の手順に従って、新しい SSH キーを作成します。

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

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

証明書のインポート

コントローラ署名証明書以外の証明書を更新すると、コレクタが再起動します。

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

- コントローラ署名証明書ファイル

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

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

ステップ 2 インポートする証明書を選択します。

ステップ 3 選択した証明書ファイルの SCP URI を入力します。

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

vNIC2 MTU の設定

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

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

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

ステップ 2 vNIC2 MTU 値を入力します。

ステップ 3 設定を保存するには [**OK**] をクリックします。

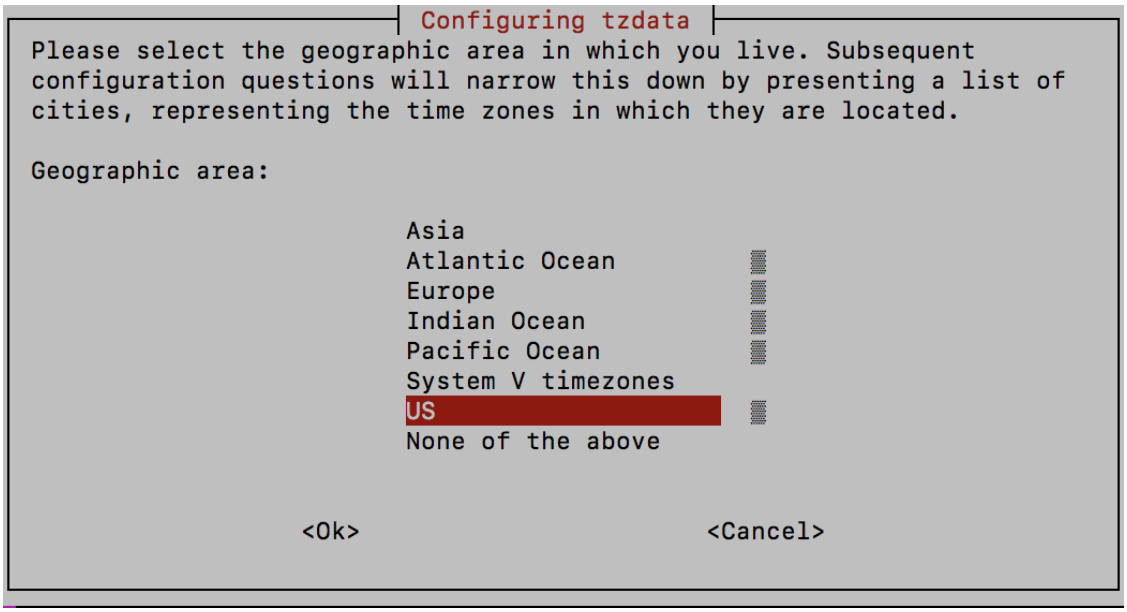
Crosswork Data Gateway VM のタイムゾーンの設定

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

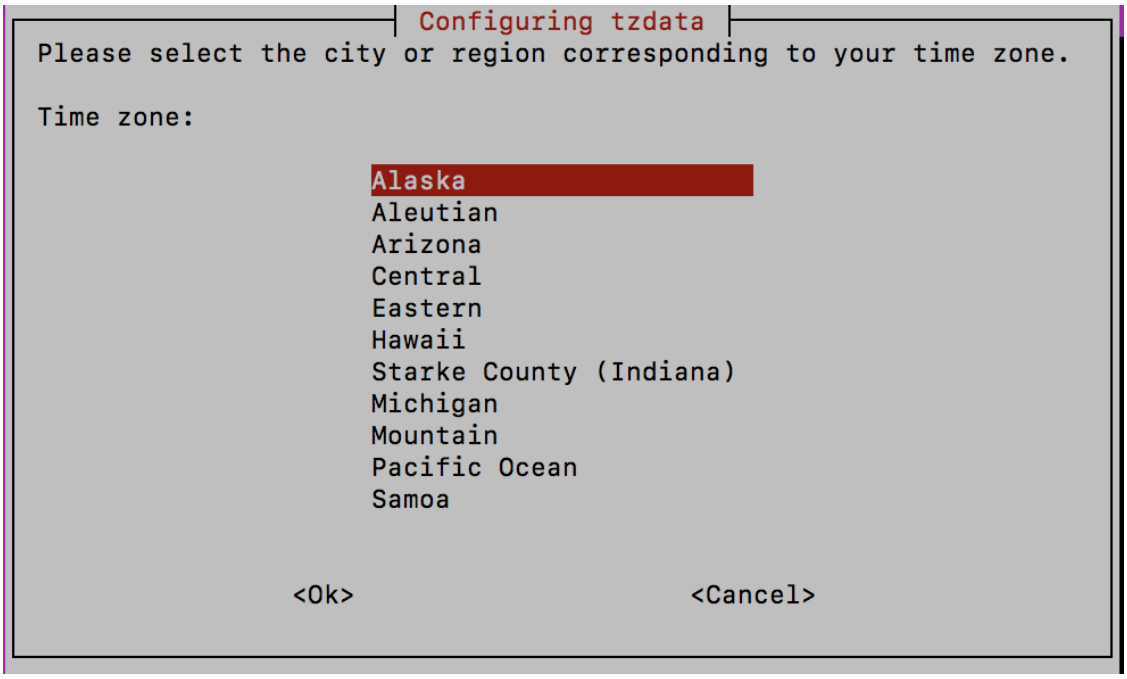
ステップ 1 Crosswork Data GatewayVM のインタラクティブメニューで、[Change Current System Settings] を選択します。

ステップ 2 [9 Timezone] を選択します。

ステップ 3 居住地域を選択します。



ステップ 4 タイムゾーンに対応する都市または地域を選択します。



ステップ 5 [OK] を選択して設定を保存します。

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

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

パスワード要件の設定

次のパスワード要件を設定できます。

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

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

ステップ 2 変更するパスワード要件を選択します。

変更するオプションを設定します。

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

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

ステップ 3 設定を保存するには [**OK**] をクリックします。

同時ログイン数の制限の設定

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

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

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

ステップ 3 [OK] を選択して変更内容を保存します。

アイドルタイムアウトの設定

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

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

ステップ 3 **Ok** と入力して、変更を保存します。

リモート監査サーバーの設定

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

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

ステップ 2 次の詳細を入力します。

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

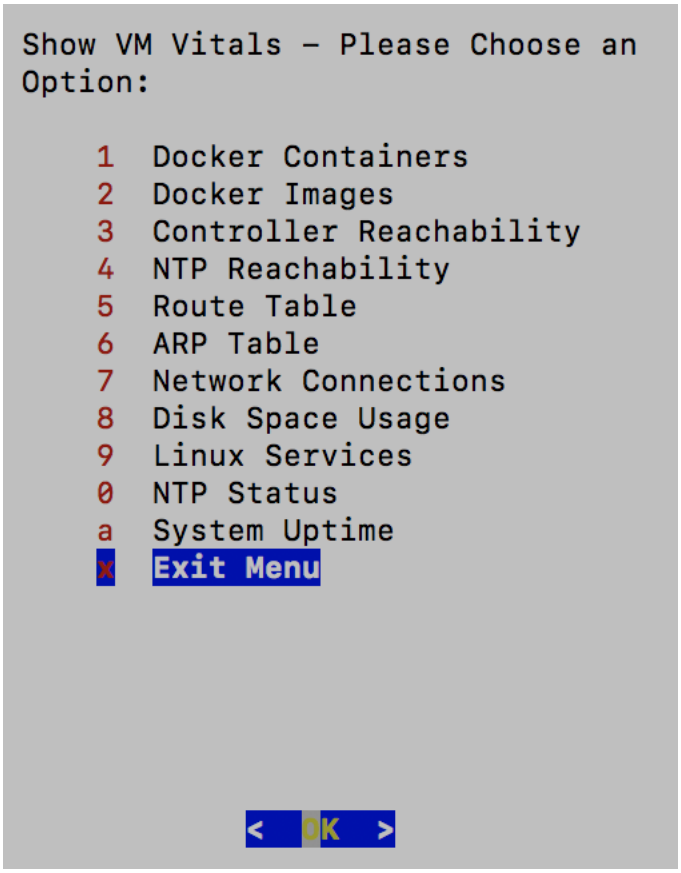
ステップ 3 [OK] を選択して変更内容を保存します。

Crosswork Data Gateway のバイタルの表示

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

ステップ 1 メインメニューで、**バイタルを 4 つ**選択します。

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



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

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

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

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

（注） 画像は、**dg-admin** ユーザーに対応する [トラブルシューティング（Troubleshooting）] メニューを示しています。**dg-oper** ユーザはこれらのオプションの一部を使用できません。表 1 : 各ロールの権限 （3 ページ） を参照してください。

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

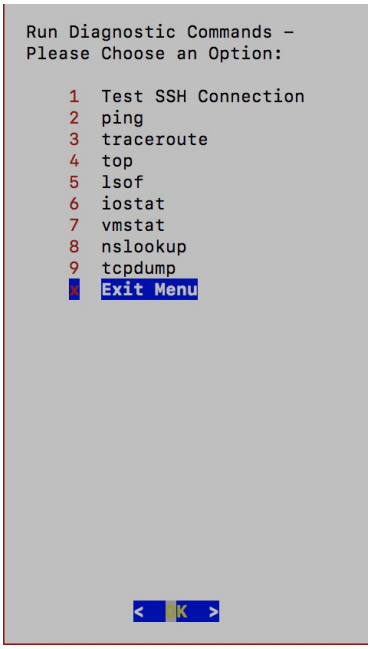
• 診断コマンドの実行 （19 ページ）
• show-tech の実行 （21 ページ）
• Crosswork Data Gateway VM のシャットダウン （22 ページ）
• auditd ログのエクスポート （22 ページ）

• TAC シェルアクセスの有効化 （22 ページ）

診断コマンドの実行

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

図 *1 : [診断の実行（Run Diagnostics）] メニュー*



ホストへの Ping

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

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

ステップ 2 次の情報を入力します。

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

ステップ 3 [OK] をクリックします。

ホストに対するトレースルート

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

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

ステップ 2 トレースルート先を入力します。

ステップ 3 [OK] をクリックします。

トラブルシューティングのためのコマンドオプション

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

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

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

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

ステップ 3 [OK] をクリックします。

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

tcpdump のダウンロード

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

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

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

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

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

ステップ 4 次の詳細を入力して、[OK] をクリックします。

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

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

show-tech の実行

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

次のようなデータが収集されます。

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

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

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

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

ステップ 2 ログとバイタルを含む tarball の保存先を入力します。

ステップ 3 SCP パスフレーズを入力し、[OK] をクリックします。

showtech ファイルは暗号化された形式でダウンロードされます。

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

ステップ 4 ダウンロードが完了したら、次のコマンドを実行して復号します。

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

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

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

Crosswork Data Gateway VM のシャットダウン

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

auditd ログのエクスポート

auditd ログをエクスポートするには、次の手順を実行します。

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

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

ステップ 3 [OK] をクリックします。

ローテーションされたログファイルの削除

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

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

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

TAC シェルアクセスの有効化

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

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

dg-tac ユーザを有効にする手順は、次のとおりです。

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

始める前に

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

b) **dg-tac** ユーザに設定したパスワードを入力します。

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

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

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

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

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

TAC シェルイベントの監査

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

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

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

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

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。