



Cisco Crosswork Data Gateway

ここでは、次の内容について説明します。

- [Cisco Crosswork Data Gateway の概要](#) (1 ページ)
- [データを収集するための Crosswork Data Gateway の設定](#) (7 ページ)
- [Crosswork Data Gateway の設定後の管理](#) (16 ページ)
- [Crosswork Data Gateway のグローバル設定の設定](#) (28 ページ)
- [Crosswork Data Gateway の収集ジョブの管理](#) (45 ページ)
- [Crosswork Data Gateway のトラブルシューティング](#) (95 ページ)

Cisco Crosswork Data Gateway の概要

Cisco Crosswork Data Gateway は、マルチベンダーデバイスからネットワークデータを収集するためのセキュアな共通の収集プラットフォームです。これは、MDT、SNMP、CLI、gNMI、Syslog、および NETCONF を含む複数のデータ収集プロトコルをサポートする、ネットワークデバイスの近くに展開される、オンプレミスのアプリケーションです。必要な Crosswork Data Gateway の数は、サポートされるデバイスの数、処理するデータの量、収集する頻度、およびネットワークアーキテクチャによって異なります。

Crosswork Data Gateway が Cisco Crosswork インフラストラクチャ（このガイドでは Cisco Crosswork と呼ばれます）とともに展開されている場合、Cisco Crosswork はコントローラアプリケーションとして機能します。

Crosswork Data Gateway では次の概念を使用します。

- **Crosswork Data Gateway インスタンス** : インストールする Crosswork Data Gateway インスタンス。
- **Crosswork Data Gateway プロファイル** : Crosswork Data Gateway は、次の展開プロファイルをサポートしています。
 - [標準 (Standard)] : Crosswork Health Insights と Crosswork Service Health (Automated Assurance) を除くすべての Crosswork アプリケーションで使用します。
 - [拡張 (Extended)] : Crosswork Health Insights と Crosswork Service Health (Automated Assurance) で使用します。



注目 [追加のリソースを備えた標準 (Standard with Extra Resources)]プロファイルは、利用制限付きの機能として使用できますが、データセンターに Crosswork Data Gateway を展開している間は使用しないでください。支援が必要な場合は、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。

- **Crosswork Data Gateway プール** : 高可用性を有効にするオプションを備えた 1 つ以上の Crosswork Data Gateway インスタンスで構成される論理ユニット。Crosswork Data Gateway インスタンスがダウンすると、Cisco Crosswork は自動的にインスタンスをプールのスペアで置き換えてデバイスを管理し、データ収集の中断を最小限に抑えます。
- **Crosswork Data Gateway** : 仮想 IP アドレスが Crosswork Data Gateway プールに追加されたときに割り当てられる Crosswork Data Gateway インスタンス。
デバイスの接続または切断、収集ジョブの作成などの操作は、Crosswork Data Gateway で行われます。
- **データ送信先** : Crosswork Data Gateway によって収集されたデータの内部または外部の受信者。デフォルトでは、Cisco Crosswork はデータの接続先として定義されます。その他の接続先 (外部ユーザー) は、Cisco Crosswork の UI または API を使用して定義できます。
- **収集ジョブ** : Crosswork Data Gateway がデータを収集するために実行する必要があるタスク。Crosswork アプリケーションは、デバイスの到達可能性を確認し、ネットワークとサービスの正常性を判断するために必要なテレメトリデータを収集する収集ジョブを作成します。Cisco Crosswork の UI と API を使用すると、Crosswork 以外のアプリケーションの収集ジョブを設定できます。
- **カスタム ソフトウェア パッケージ** : デバイスカバレッジを拡張し、現在サポートされていないデバイスからのデータ収集をサポートするためのファイルとデバイスモデルの定義。



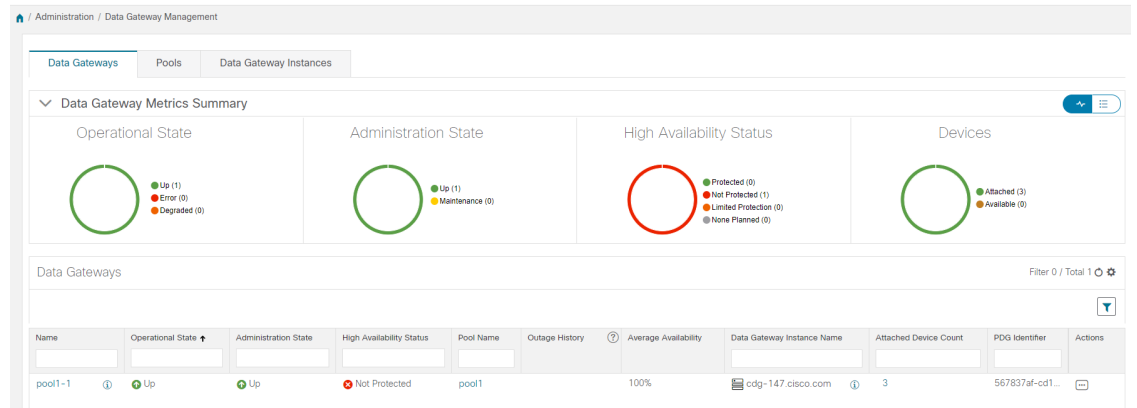
(注) この章では、Cisco Crosswork の UI を介してアクセスできる Cisco Crosswork Data Gateway の機能についてのみ説明します。

Cisco Crosswork Data Gateway インスタンスのインタラクティブコンソールとその管理方法の詳細については、「付録 A : [Crosswork Data Gateway インスタンスの設定](#)」を参照してください。

Crosswork Data Gateway の UI の概要

Cisco Crosswork Data Gateway の管理ビューを開くには、Cisco Crosswork にログインし、左側のナビゲーションバーから [管理 (Administration)] > [Data Gateway の管理 (Data Gateway Management)] を選択します。

図 1:[データゲートウェイの管理 (Data Gateway Management)]ウィンドウ



[Data Gateway の管理 (Data Gateway Management)] ページには、次の 3 つのタブがあります。

- **Data Gateways** : ネットワーク内の仮想 Cisco Crosswork Data Gateway の詳細を表示します。このタブから Data Gateway にデバイスを接続または切断できます。
- [プール (Pools)] : Cisco Crosswork Data Gateway プールを管理します。
- [データゲートウェイインスタンス (Data Gateways Instances)] : 物理的な Cisco Crosswork Data Gateway インスタンスを管理します。

ドーナツグラフの可視化の横にある凡例をクリックして、テーブルをフィルタリングできます。たとえば、管理状態が [アップ (Up)] になっているプールを表示するには、[管理状態 (Administration State)] チャートの横にある [アップ (Up)] アイコンをクリックします。テーブルは、[アップ (Up)] 状態のプールをフィルタリングします。

テーブルに表示する必要がある列を選択するには、テーブルの右上隅にある [設定 (Settings)] アイコンをクリックし、関連するチェックボックスをオンにします。列を非表示にするには、チェックボックスをオフにします。


Crosswork Data Gateway UI のすべてのテーブルでは、空のフィールドをクリックし、メニューから [すべて選択 (Select all)] を選択することで、項目を複数選択できます。選択したすべての項目がテーブルに表示されます。選択を解除するには、選択した項目の横にある [X] アイコンをクリックします。


次の表では、[データゲートウェイの管理 (Data Gateway Management)] ページのさまざまな列について説明します。

表 1 : Cisco Crosswork Data Gateway の UI

カラム	説明
動作状態 (Operational State)	<p>Cisco Crosswork Data Gateway インスタンスの動作状態。</p> <p>Crosswork Data Gateway インスタンスの動作状態は次のとおりです。</p> <ul style="list-style-type: none">  [低下 (Degraded)] : Cisco Crosswork Data Gateway インスタンスは到達可能ですが、1 つ以上のコンポーネントが [OK] 以外の状態です。  [アップ (Up)] : Cisco Crosswork Data Gateway インスタンスが動作しており、個々のすべてのコンポーネントは「OK」です。  [エラー (Error)] : Cisco Crosswork Data Gateway インスタンスが到達不能であるか、またはその一部のコンポーネントがエラー状態になっています。
管理状態 (Administration State)	<p>Cisco Crosswork Data Gateway インスタンスの管理状態。</p> <ul style="list-style-type: none">  [アップ (Up)] : インスタンスは管理上のアップ状態です。  [メンテナンス (Maintenance)] : アップグレードやその他のメンテナンスアクティビティ (証明書のアップロードなど) を実行するために、Cisco Crosswork と Cisco Crosswork Data Gateway 間の操作が中断されます。
高可用性のステータス (High Availability Status)	<p>Crosswork Data Gateway の高可用性のステータスは次のいずれかです。</p> <ul style="list-style-type: none"> [保護されている (Protected)] : すべてのインスタンスが稼働しており、プール内に 1 つ以上のスタンバイがあります。 [保護されていない (Not Protected)] : すべてのスタンバイインスタンスがダウンしています。 [限定的な保護 (Limited Protection)] : 一部のスタンバイインスタンスがダウンしていますが、1 つ以上のスタンバイインスタンスが稼働しています。 [計画なし (None Planned)] : プールの作成時にスタンバイインスタンスがプールに追加されませんでした。

カラム	説明
デバイス (Devices)	Cisco Crosswork Data Gateway のプールに接続されているデバイスの数。
Name	<p>Cisco Crosswork Data Gateway インスタンスの名前。</p> <p>名前の横にある ⓘ アイコンをクリックすると、各インスタンスの登録の詳細が表示されます。これには、次が含まれます。</p> <ul style="list-style-type: none"> • 仮想 IP アドレス • データ ゲートウェイ インスタンス名 • 説明 • Crosswork Data Gateway のプロファイルを示すデータゲートウェイのインスタンスタイプ。 • データ ゲートウェイ インスタンスの UUID <p>インスタンス名をクリックして、Crosswork Data Gateway のバイタルページを開きます。このページには、Crosswork Data Gateway の動作と正常性の概要が表示されます。</p>
プール名 (Pool Name)	Crosswork Data Gateway プールの名前。プール名をクリックすると、Crosswork Data Gateway のバイタルページが開きます。
停止履歴 (Outage History)	<p>Cisco Crosswork Data Gateway インスタンスの 14 日間の停止履歴。</p> <p>1 日の状態集約は、[エラー (Error)]、[低下 (Degraded)]、[アップ (Up)]、[不明 (Unknown)]、[準備中 (Not Ready)] の優先順位で実行されます。</p> <p>たとえば、Crosswork Data Gateway インスタンスが [不明 (Unknown)] から [低下 (Degraded)] の後、[アップ (Up)] になった場合、当日は [低下 (Degraded)] の色 (オレンジ) で表示されます。これは、[アップ (Up)] や [不明 (Unknown)] よりも [低下 (Degraded)] のほうが優先されるためです。</p> <p>Crosswork Data Gateway がその日の任意の時点で [エラー (Error)] 状態になった場合、タイルは赤になります。Data Gateway が [エラー (Error)] ではなく、[低下 (Degraded)] 状態の場合、そのタイルはオレンジ色になります。DG が [エラー (Error)] または [低下 (Degraded)] 状態ではなく、[アップ (Up)] のみであった場合、タイルは緑色です。</p>

カラム	説明
平均可用性 (Average Availability)	<p>Cisco Crosswork Data Gateway インスタンスの正常性を示す値。このパーセンテージは、最初のイベントの開始時刻と最後のイベントの終了時刻の間に、Crosswork Data Gateway が稼働状態であった合計時間 (ミリ秒単位) として計算されます。</p> <p>(注) 最後のイベントの終了時刻は現在のタイムスタンプであるため、最後のイベントの期間は開始時刻と現在のタイムスタンプの間になります。</p>
データゲートウェイインスタンス名 (Data Gateway Instance Name)	<p>Crosswork Data Gateway インスタンスをプールに追加するときに自動的に作成される Cisco Crosswork Data Gateway の名前。</p> <p>インスタンス名の横にある  アイコンをクリックすると、各インスタンスの登録の詳細が表示されます。これには、次が含まれます。</p> <ul style="list-style-type: none"> • データゲートウェイインスタンス名 • 説明 • データゲートウェイインスタンスのタイプ • データゲートウェイインスタンスのロール • CPU • メモリ • NIC の数 • データゲートウェイインスタンスの UUID • バージョン • データゲートウェイインスタンスの OS • インターフェイス名 (Interface Name) • インターフェイスロール • インターフェイス Mac • インターフェイス名 (Interface Name) <p>[追加のインターフェイスロール情報 (Additional Interface Role Information)] では、Crosswork Data Gateway で使用できるインターフェイスロールについて説明します。</p>
接続デバイス数 (Attached Device Count)	Cisco Crosswork Data Gateway のプールに接続されているデバイスの数を示します。

カラム	説明
PDG識別子 (PDG Identifier)	Cisco Crosswork Data Gateway インスタンスの一意の識別子。
アクション (Actions)	<p> をクリックして、プールで実行できるアクションを表示します。</p> <ul style="list-style-type: none"> • デバイスを接続します。詳細については、Crosswork Data Gateway へのデバイスの接続 (15 ページ) を参照してください。 • デバイスを切り離します。詳細については、Cisco Crosswork Data Gateway デバイス割り当ての管理 (22 ページ) を参照してください。 • デバイスを移動します。詳細については、Cisco Crosswork Data Gateway デバイス割り当ての管理 (22 ページ) を参照してください。 • フェールオーバーを開始します。詳細については、手動フェールオーバーの実行 (14 ページ) を参照してください。

[Crossworkホーム (Crosswork Home)] ページ > [ダッシュボード (Dashboard)] で Crosswork Data Gateway ダッシュレットを設定できます。ダッシュボードでは、ダッシュレットをカスタマイズして、Crosswork Data Gateway インスタンスとプールの概要を表示できます。ダッシュボードの使用の詳細については、[ダッシュボードでのクイックビューの取得](#) を参照してください。

データを収集するための Crosswork Data Gateway の設定

Crosswork Data Gateway では、収集ジョブを実行する前に、まず次の設定タスクを実行する必要があります。



- (注) このワークフローでは、『[Cisco Crosswork Network Controller 5.0 Installation Guide](#)』で説明されているように、Cisco Crosswork Data Gateway がすでにインストールされていることを前提としています。

次の表の手順 1 から手順 3 までを実行して、Crosswork Data Gateway を設定し、Cisco Crosswork とその他の Crosswork アプリケーションで実行します。手順 4 – 手順 6 はオプションであり、外部のデータ送信先とカスタム収集ジョブを作成してデータを収集および転送する Crosswork Data Gateway の機能を拡張する場合にのみ必要です。

表 2: データの収集を目的とした **Cisco Crosswork Data Gateway** の設定を実行するためのタスク

タスク	次の手順を実行します。
1. Crosswork Data Gateway プールを作成します。	Cisco Crosswork Data Gateway プールの作成 (10 ページ)
2. デバイスを Crosswork Data Gateway に接続します。	Crosswork Data Gateway へのデバイスの接続 (15 ページ)
3. デフォルトの収集ジョブが作成され、正常に実行されていることを確認します。	収集ジョブのモニター (89 ページ)
4. (オプション) デバイスカバレッジを拡張して、現在サポートされていないデバイスまたはサードパーティ製デバイスからデータを収集します。	デバイスパッケージの管理 (37 ページ)
5. (オプション) データを外部のデータ送信先に転送します。	外部データ送信先の作成と管理 (29 ページ)
6. (オプション) カスタム収集ジョブ (Cisco Crosswork によって作成されたもの以外) を作成します。	Crosswork Data Gateway の収集ジョブの管理 (45 ページ)

プールによる Crosswork Data Gateway の高可用性

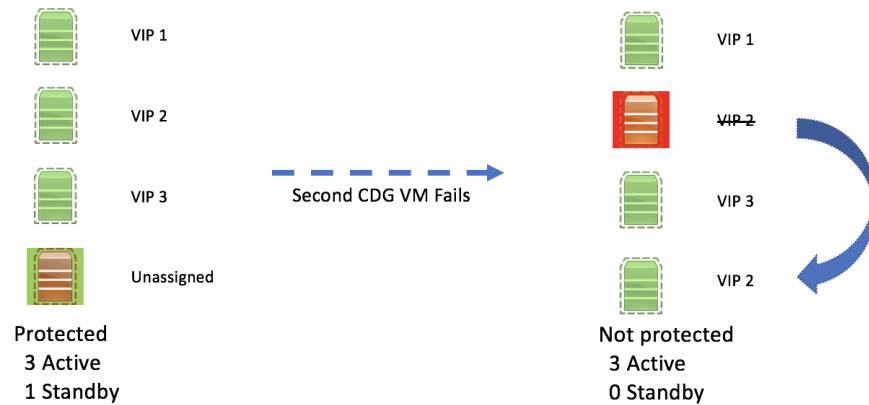
Cisco Crosswork Data Gateway プールによって、デバイスが管理され、最小限の中断で収集が行われます。

プールは、高可用性を有効にするオプションを備えた 1 つ以上の Cisco Crosswork Data Gateway インスタンスで構成できます。

プール内の Crosswork Data Gateway インスタンスがダウンした場合、Cisco Crosswork はそのインスタンスをプールのスタンバイインスタンスに自動的に置き換える (フェールオーバー) か、手動でフェールオーバーを開始できます。フェールオーバーを開始する方法については、[手動フェールオーバーの実行 \(14 ページ\)](#) を参照してください。

[動作状態 (Operational state)] が [エラー (Error)] で、[保護されている (Protected)] プールの一部である Crosswork Data Gateway インスタンスは、フェールオーバーに適格です。障害が発生したインスタンスからスタンバイインスタンスへ、デバイスと既存の収集ジョブが自動的に割り当てられます。ダウンしたインスタンスが動作可能になると、プール内のスタンバイインスタンスになります。

図 2: Crosswork Data Gateway の高可用性



(注) プール内の Crosswork Data Gateway の複数のインスタンスに同じサウスバウンド IP アドレスがある場合にスタンバイ Crosswork Data Gateway を再起動すると、そのスタンバイ Crosswork Data Gateway インスタンスの起動後にそのサウスバウンド IP アドレスが失われます。

たとえば、サウスバウンド IP アドレスが IP1 の CDG1 (アクティブ) はダウンします。Cisco Crosswork は、CDG1 を新しいアクティブな VM として CDG2 (スタンバイ) に置き換え、CDG2 のサウスバウンド IP と同じ IP1 をプログラムします。後で CDG1 が起動し、プール内の新しいスタンバイになります。サウスバウンド IP アドレスと同じ IP1 を保持します。これにより、CDG1 と CDG2 の両方がサウスバウンド IP と同じ IP1 になります。

Crosswork Data Gateway のプールには次の状態があります。

- [保護されている (Protected)] : すべてのインスタンスが稼働しており、プール内に 1 つ以上のスタンバイインスタンスがあります。
- [保護されていない (Not Protected)] : すべてのスタンバイインスタンスがダウンしており、使用中のインスタンスを置き換えることができません。
- [限定的な保護 (Limited Protection)] : 一部のスタンバイインスタンスがダウンしていますが、1 つ以上のスタンバイが稼働しています。
- [計画なし (None Planned)] : プールの作成時にスタンバイインスタンスがプールに追加されませんでした。

データゲートウェイが 3 回連続のバイタルサイクル (30 秒) の間にそのヘルスの報告に失敗した場合、データゲートウェイの [動作状態 (Operational state)] は [エラー (Error)] であると見なされます。ヘルスレポートの失敗は、次のことが原因である可能性があります。

- データゲートウェイインスタンスの問題。たとえば、データゲートウェイで正常性を報告するためのリソースが不足しています。

- Cisco Crosswork と Crosswork Data Gateway 間のネットワークの問題。

Crosswork Data Gateway の [動作状態 (Operational state)] は 20 秒ごとにチェックされます。アクティブなインスタンスが [エラー (Error)] 状態の場合、フェールオーバーがトリガーされ、プール内のスペアインスタンスがプール内のアクティブなインスタンスになります。

セキュアな Syslog 通信の FQDN を有効にする

Crosswork Data Gateway は、syslog 証明書に Crosswork Data Gateway の仮想 IP アドレスの代わりにホスト名または完全修飾ドメイン名 (FQDN) が含まれている必要があるデバイスへの安全な syslog 通信をサポートします。これは、syslog 証明書にホスト名または FQDN を持つことを義務付けるデバイスで有効にできるオプション機能です。有効にすると、Cisco Crosswork は、DNS サーバーから Crosswork Data Gateway の各仮想 IP アドレスのホスト名または FQDN をフェッチします。新しく追加された仮想 IP の FQDN は、プールを保存した後に取得されます。その後、syslog 証明書には、Crosswork Data Gateway の仮想 IP アドレスの代わりに、CN および SAN の FQDN が含まれます。デバイスでセキュア Syslog を設定する方法の詳細については、「[デバイスでのセキュア Syslog の設定 \(65 ページ\)](#)」を参照してください。



- (注) Crosswork Data Gateway プールは、FQDN を有効にせずに作成できます。この場合、syslog 証明書には Crosswork Data Gateway の仮想 IP アドレスが含まれます。後でいつでもプールを編集して、FQDN を有効または無効にして、syslog 証明書に FQDN と仮想 IP アドレスを切り替えることができます。

DNS サーバーで FQDN 値が更新されたら、プール内の仮想 IP の FQDN 値を更新する必要があります。

FQDN を更新するには、[プール (Pools)] タブで、FQDN を更新するプールに移動します。[アクション (Actions)] 列で (...) アイコンをクリックし、[FQDN を更新 (Refresh FQDN)] を選択します。

Cisco Crosswork Data Gateway プールの作成

Cisco Crosswork Data Gateway プールを作成する場合は、次のガイドラインに従います。

- 少なくとも 1 つのプールを作成し、Crosswork Data Gateway インスタンスをそのプールに割り当てる必要があります。収集用の Crosswork Data Gateway を設定するには、この手順が必須です。
- プール内のすべての Crosswork Data Gateway インスタンスは、同じ構成 (Standard、または Extended) である必要があります。
- VM を Amazon EC2 に展開した場合、プール内のすべての Crosswork Data Gateway インスタンスは、同じ可用性ゾーンからのものである必要があります。

Crosswork Data Gateway プールを作成するには、次の手順を実行します。

始める前に

Cisco Crosswork Data Gateway のプールを作成する前に、次を確認してください。

- プールの高可用性を有効にするかどうかを決定すること。
- プールに追加する Crosswork Data Gateway のすべてのインスタンスをインストールしたことを確認すること。
- プールの種類について十分に理解していることを確認すること。
 - [L2ストレッチ (L2 Stretch)] : 単一の IP サブネットに存在する HA プールの一部である Crosswork Data Gateway インスタンスに、ネットワークデバイスが接続するプール。サブネットは、DC (データセンター) 内または拡張された DC 間の場合があります。
 - [ロードバランサを使用したL3 (L3 with Load Balancer)] : 同じ HA プールの一部である複数の異なるサブネットに存在する Crosswork Data Gateway インスタンスに、ネットワークデバイスが接続するプール。この構成では、Crosswork Data Gateway HA プールの内部サブネットアドレスを保護しながら、外部ネットワークロードバランサ (NLB) がネットワークデバイスに対して VIP をホストする必要があります。



(注) [ロードバランサを使用したL3 (L3 with Load Balancer)] プールタイプは、Amazon EC2 環境でプールを作成する場合にのみサポートされます。

- Crosswork Data Gateway インスタンスの動作状態が [準備中 (Not Ready)] であることを確認します。
- 仮想 IP アドレス (アクティブなデータゲートウェイごとに1つの仮想 IP)、サブネットマスク、ゲートウェイ情報などのネットワーク情報を用意します。



(注) ゲートウェイは、3つのNICを使用する場合にのみ必要です。

展開内の vNIC の数に応じて、仮想 IP アドレスは次のようになります。

- 単一の NIC 展開での管理ネットワーク上の追加の IP アドレス。
- 2 NIC 展開用のデータネットワーク上の追加 IP アドレス。
- 3 NIC 展開用のサウスバウンドネットワーク上の IP アドレス。

これらの仮想 IP アドレスは、ネットワーク設計段階で計画する必要があります。

- プール内の仮想 IP アドレスに対して完全修飾ドメイン名 (FQDN) を有効にするかどうかを決定します。はいの場合、プールを正常に作成するために、DNS サーバーで仮想 IP の FQDN が設定されていることを確認してください。

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


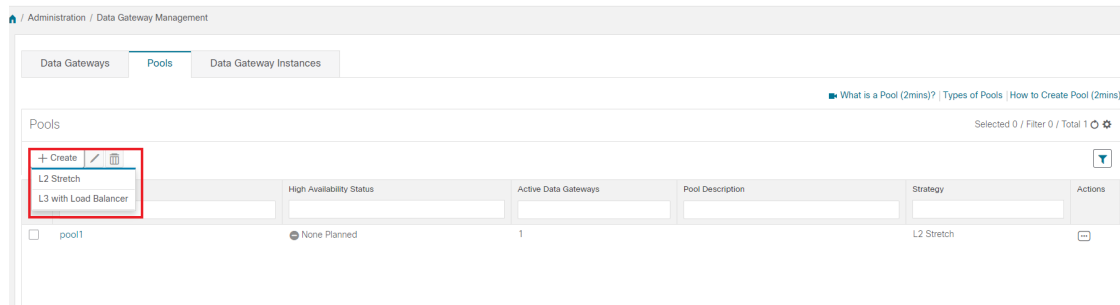
ステップ 2 [プール (Pools)] タブで  ボタンをクリックし、[L2ストレッチ (L2 Stretch)] または [ロードバランサを使用したL3 (L3 with Load Balancer)] を選択します。プールの種類については、右上の [プールの種類 (Types of Pools)] をクリックしてください。

図 3: [プール (Pools)] ウィンドウ



[プールの作成 (Create Pool)] ページが開きます。

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

- [プール名 (Pool Name)] : ネットワークを適切に説明するプールの名前。
- [説明 (Description)] : プールの説明。

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

プールの種類に応じて、プールリソースのパラメータが変わります。たとえば、[L2ストレッチ (L2 Stretch)] の場合、プールリソースは IPv4 アドレスを考慮します。

- [IPv4] または [IPv6] : 仮想 IP の IPv4 または IPv6 アドレスファミリーを選択します。IP アドレスには、次のパラメータが必要です。
 - [サブネット (Subnet)] : 各 Cisco Crosswork Data Gateway のサブネットマスク。IPv4 サブネットマスクの範囲は 1 ~ 32、ポートの範囲は 1024 ~ 65535 です。
 - [ネットワークゲートウェイ (Network Gateway)] : デバイスと通信するための Cisco Crosswork Data Gateway それぞれのゲートウェイアドレス。
 - (オプション) [仮想IPアドレスのFQDNを有効にする] : このオプションを選択して、syslog 証明書の Crosswork Data Gateway の各仮想 IP アドレスにホスト名または完全修飾ドメイン名 (FQDN) を使用します。
- [FQDN] : syslog 証明書の Crosswork Data Gateway の各仮想 IP アドレスに対する完全修飾ドメイン名 (FQDN)。

- [もう1つ追加する (Add Another)] : 前に選択したアドレスファミリー (IPv4またはIPv6、FQDN) に基づいて、すべてのアクティブな Cisco Crosswork Data Gateway インスタンスの仮想 IP アドレスまたは FQDN を入力します。
- [保護に必要なスタンバイ データ ゲートウェイの数を追加する (Add the number of standby data gateways desired for protection)] : このフィールドに 0 より大きい値を入力すると、プールの高可用性が有効になります。アクティブなデータゲートウェイがダウンした場合、保護を確保するためにプール内の「スタンバイ」が置き換わります。

プールに追加する Cisco Crosswork Data Gateway インスタンスの数は、仮想 IP とスタンバイ Cisco Crosswork Data Gateway インスタンスの合計数と同じにする必要があります。たとえば、仮想 IP を 3 つ入力し、2 つのスタンバイインスタンスが必要な場合は、5 つの Cisco Crosswork Data Gateway インスタンスをプールに追加します。
- [プールするデータゲートウェイインスタンスのリソースを選択して追加する (Select and add Data Gateway Instance resources to pool)] : 左側の [未割り当てのデータゲートウェイインスタンス (Unassigned Data Gateway Instance(s))] からデータゲートウェイインスタンスを選択し、右矢印をクリックしてインスタンスを [プールに追加されたデータゲートウェイインスタンス (Data Gateway Instance(s) Added to Pool)] に移動します。

図 4:[プールの作成 (Create Pool)] ウィンドウ

ステップ 5 [保存 (Save)] をクリックします。

Amazon EC2 で、プールが作成されたら、アクティブな Crosswork Data Gateway の NLB が正常な状態であることを確認します。

[保存 (Save)] をクリックし、仮想 Crosswork Data Gateway が自動的に作成され、[データゲートウェイインスタンス (Data Gateway Instances)] タブに表示されます。デバイスをこの仮想 Crosswork Data Gateway に接続して収集ジョブを実行します。



(注) DNS サーバーの仮想 IP の FQDN 構成が欠落している場合、プールの作成は失敗します。DNS サーバーの FQDN 構成を確認するか、FQDN オプションを無効にして再試行してください。

手動フェールオーバーの実行

計画されたメンテナンススケジュールがある場合、インスタンスから同じプール内にあるスタンバイインスタンスへのフェールオーバーを強制できます。

始める前に

Crosswork Data Gateway プールでフェールオーバーを開始する前に、次の点に注意してください。

- 自動フェールオーバーが進行中のデータゲートウェイでは、手動フェールオーバーを試行できません。
- Crosswork は、一度に1つのフェールオーバー要求のみを考慮します。同時に複数のフェールオーバー要求をサポートしていません。
- 少なくとも1つのインスタンスの動作状態が **UP** または **NOT_READY** であることを確認します。Crosswork は、このインスタンスをフェールオーバーが発生するスタンバイと見なします。
- 少なくとも1つのスタンバイデータゲートウェイインスタンスが **NOT_READY** 状態である必要があります。
- メンテナンスモードのデータゲートウェイは、稼働状態が **UP** になるまで、将来のフェールオーバー手順のスペアとして使用できません。
- フェールオーバーに使用する予定の予備のデータゲートウェイインスタンスは、**NOT_READY** 状態である必要があります。

以下の手順に従って、Crosswork Data Gateway インスタンスの手動フェールオーバーを開始します。

-
- ステップ 1** メインメニューから、[管理 (Administration)] > [データゲートウェイの管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] タブの順に選択します。
 - ステップ 2** フェールオーバーを開始する Crosswork Data Gateway の [アクション (Actions)] 列で、[フェールオーバーの開始 (Initiate Failover)] をクリックして選択します。
 - ステップ 3** [警告 (Warning)] ウィンドウで、フェールオーバーの完了後に、選択したデータゲートウェイをメンテナンスモードに移行する場合は、チェックボックスをオンにします。
 - ステップ 4** [続行 (Continue)] をクリックします。
-

次のタスク

データベース接続または OAM チャネルの問題が原因でフェールオーバーが完了しない場合は、少なくともスタンバイインスタンスが **NOT_READY** 状態であることを確認してから、フェールオーバーを再試行します。

後続のフェールオーバーを開始する前に、スタンバイデータゲートウェイが **NOT_READY** 状態に移行するまで 10 ~ 30 秒待ちます。スタンバイインスタンスが 30 秒後に **UP** 状態のままである場合は、データゲートウェイの `oam-manager` を再起動して、動作状態を **NOT_READY** として復元します。

Crosswork Data Gateway へのデバイスの接続

Crosswork Data Gateway にデバイスを接続する場合は、次のガイドラインに従います。

- デバイスは 1 つの Crosswork Data Gateway のみに接続できます。
- 最適なパフォーマンスを得るには、300 台以下のデバイスで数回に分けて Crosswork Data Gateway に接続することをお勧めします。



(注) Crosswork Data Gateway では、SSH 接続が失敗する可能性があるため、古い安全でない鍵交換アルゴリズム (KEX) の使用をサポートしていません。

始める前に

デバイスを接続する Crosswork Data Gateway の [管理状態 (Admin state)] と [動作状態 (Operational state)] が [アップ (Up)] であることを確認します。


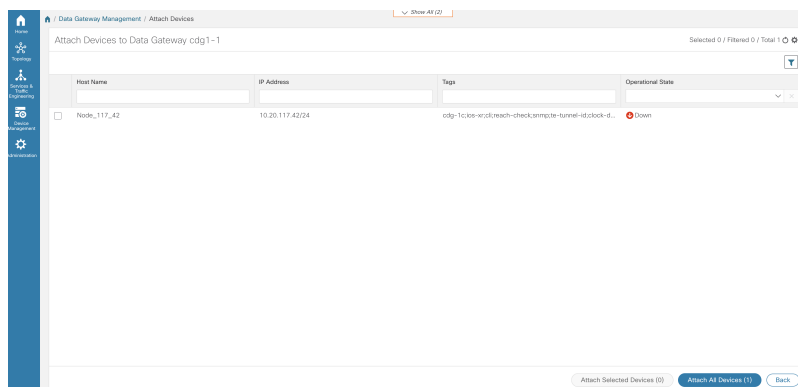
- ステップ 1** (オプション) 既存の Crosswork Data Gateway にデバイスを接続する前に、Crosswork Data Gateway の正常性を確認することをお勧めします。詳細については、「[Crosswork Data Gateway 正常性のモニタリング \(16 ページ\)](#)」を参照してください。
- ステップ 2** メインメニューから、[管理 (Administration)] > [Data Gateway の管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] に移動します。
- ステップ 3** デバイスを接続する Crosswork Data Gateway の [アクション (Actions)] 列で、 をクリックして [デバイスの接続 (Attach Devices)] を選択します。[デバイスの接続 (Attach Devices)] ウィンドウが開き、接続可能なすべてのデバイスが表示されます。

図 5: [デバイスの接続 (Attach Devices)] ウィンドウ



ステップ 4 すべてのデバイスを接続するには、[すべてのデバイスの接続 (Attach All Devices)] をクリックします。それ以外の場合は、接続するデバイスを選択し、[選択したデバイスの接続 (Attach Selected Devices)] をクリックします。

ステップ 5 [確認：デバイスの接続 (Confirm-Attach Devices)] ダイアログで、[接続 (Attach)] をクリックします。

[データゲートウェイ (Data Gateways)] ペインの [接続デバイス数 (Attached Device Count)] 列を確認して、変更が成功したことを確認します。

Crosswork Data Gateway の正常性をモニターし、Crosswork Data Gateway が新しく接続されたデバイスで正常に機能していることを確認します。正常性をモニターする方法については、[Crosswork Data Gateway 正常性のモニタリング \(16 ページ\)](#) を参照してください。

Crosswork Data Gateway の設定後の管理

この項では、Crosswork Data Gateway 内のさまざまなメンテナンスタスクについて説明します。

- [Crosswork Data Gateway 正常性のモニタリング \(16 ページ\)](#)
- [プールによる Crosswork Data Gateway の高可用性 \(8 ページ\)](#)
- [Cisco Crosswork Data Gateway デバイス割り当ての管理 \(22 ページ\)](#)
- [Crosswork Data Gateway インスタンスの維持 \(25 ページ\)](#)

Crosswork Data Gateway 正常性のモニタリング

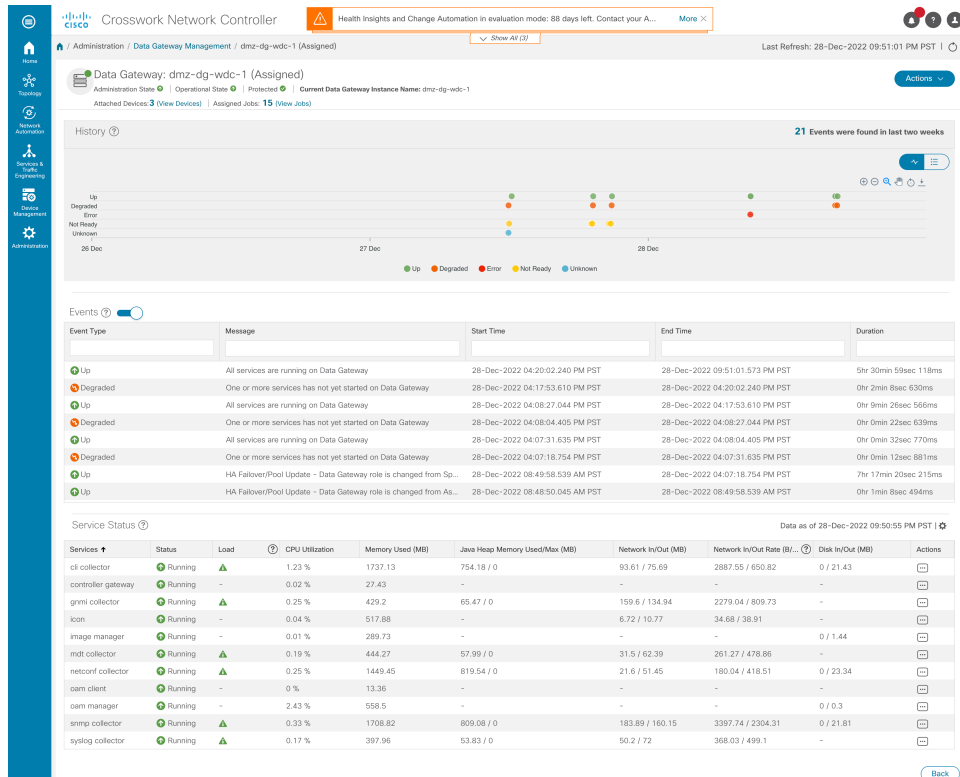
Crosswork Data Gateway の動作と正常性の概要は、[管理 (Administration)] > [データゲートウェイの管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] > (クリック) {Crosswork Data Gateway} の順にアクセスし、Crosswork Data Gateway のバイタルページから表示できます。このページには、Crosswork Data Gateway で実行されているさまざまなコンテナ化されたサービスの状態の詳細も含まれています。Crosswork Data Gateway の全体的な正常性は、コンテナ化された各サービスの正常性にも依存します。

[アクション (Actions)] ボタンをクリックし、適切なメニューを選択することで、トラブルシューティング アクティビティを実行できます。

- [Ping] : 任意の IP アドレスへの到達可能性をチェックします。
- [トレースルート (Trace Route)] : 遅延の問題のトラブルシューティングに役立ちます。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。
- [サービスマトリックのダウンロード (Download Service Metrics)] : Cisco Crosswork の UI から Crosswork Data Gateway のすべての収集ジョブのメトリックをダウンロードします。
- [Showtechのダウンロード (Download Showtech)] : Cisco Crosswork の UI から showtech ログをダウンロードします。

- [ログレベルの変更 (Change Log Level)] : Crosswork Data Gateway のコンポーネント (コレクタ (cli-collector) やインフラサービス (oam-manager) など) のログレベルを変更できます。ログレベルの変更は、変更を加える Crosswork Data Gateway にのみ適用されます。

図 6: [データゲートウェイ (Data Gateway)] ウィンドウ



次のパラメータがこのページに表示されます。

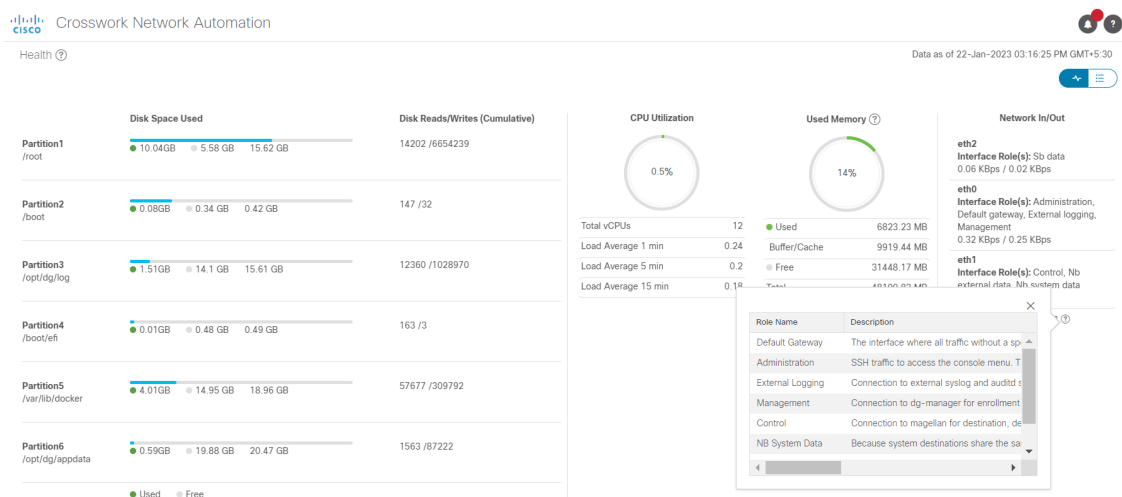
- [一般的なCisco Crosswork Data Gatewayの詳細 (General Cisco Crosswork Data Gateway)] : 動作状態、高可用性の状態、接続されているデバイスの数、割り当てられたジョブなど、Crosswork Data Gateway の一般的な詳細を表示します。[アクション (Actions)] オプション UI から使用できるさまざまなトラブルシューティングのオプションについて説明します。
- [履歴 (History)] : タイムスタンプ、停止時間、クリア時間を含む、14 日間の Cisco Crosswork Data Gateway の停止履歴チャートを表示します。ページの右上隅のオプションを使用して、グラフ内の特定の期間の履歴チャートの拡大、縮小、パンを実行したり、SVG と PNG をダウンロードします。
- [イベント (Events)] : 過去 14 日間のすべての Cisco Crosswork Data Gateway の遷移状態の変更のリストを表示します。これには、動作状態の変更、ルールの変更、ステータス変更の理由を示すメッセージ、タイムスタンプ、期間を含むイベントの詳細などの情報が含まれます。

- [正常性 (Health)] : Cisco Crosswork Data Gateway の正常性情報を表示します。右上隅のタイムスタンプは、最後の正常性データが収集されたときのタイムスタンプです。Crosswork Data Gateway が [エラー (Error)] 状態の場合、または何らかの理由でデータが古い場合、タイムスタンプラベルはデータが古いことを示します。Crosswork Data Gateway の [CPU 使用率 (CPU Utilization)] が 80% を超える場合は、[CPU 使用率 (CPU Utilization)] がさらに増加して Crosswork Data Gateway の障害につながる前に、是正措置を講じることをお勧めします。

[ネットワーク入出力率 (Network In/Out)] セクションには、vNIC がネットワークデータを送受信する速度が表示されます。

[追加のロール情報 (Additional Role Information)] の横にある [?] アイコンをクリックすると、vNIC に割り当てられたインターフェイスロールを表示できます。ポップアップには、使用可能なロールに関する情報が表示されます。

図 7: [Crosswork Data Gateway の正常性 (Crosswork Data Gateway Health)] ウィンドウ



- [サービスステータス (Service Status)] : Crosswork Data Gateway で実行されている個々のコンテナサービスの正常性情報と、個々のサービスを再起動するオプション ([アクション (Actions)] > [再起動 (Restart)]) を使用したリソース消費が表示されます。[負荷 (Load)] 列は、その特定のコレクタ/サービスの処理負荷を示します。コレクタの負荷スコアは、いくつかのメトリックを使用して計算されます。負荷スコアは、低、中、または高の重大度ゾーンにマップされます。コレクタが常に高ゾーンで動作している場合、そのコレクタが特定の CPU/メモリリソースプロファイルのピーク容量に達したことを意味します。負荷スコアの計算方法の詳細については、「[Load Score Calculation](#)」を参照してください。



(注) コンテナサービスのリストは、標準の Crosswork Data Gateway と拡張 Crosswork Data Gateway で異なります。拡張 Crosswork Data Gateway には、より多くのコンテナがインストールされています。

表示されるリソース消費データは、docker 統計からのものです。これらの値は、コンテナ化されたサービスによって消費される実際のリソースよりも高くなります。

図 8: [サービスステータス (Service Status)] ウィンドウ

Services	Status	Load	CPU Utilization	Memory Used (MB)	Java Heap Memory Used/Max (MB)	Network In/Out (MB)	Network In/Out Rate (B/Sec)	Disk In/Out (MB)	Actions
cli collector	Running	▲	0.22 %	857.74	325.36 / 460	202 / 50.5	136 / 236	0 / 514	
controller gateway	Running	-	0.02 %	13.47	-	482 / 526	1658 / 1305	0 / 191	
gmni collector	Running	▲	0.12 %	289.41	51.81 / 76	19.6 / 14.7	114 / 169	0 / 205	
icon	Running	-	0.13 %	393.43	-	15.1 / 12.3	27 / 41	0 / 172	
image manager	Running	-	0.12 %	348.86	99.24 / 147	103 / 125	6 / 13	0.25 / 249	
mlt collector	Running	▲	0.12 %	299.37	48.17 / 80	19.6 / 14.7	129 / 184	0 / 206	
netconf collector	Running	▲	0.15 %	636.8	267.08 / 330	19.6 / 14.7	110 / 158	0 / 242	
oam manager	Running	-	0.14 %	445.54	95.56 / 138	391 / 160	1099 / 2167	55.6 / 905	
snmp collector	Running	▲	0.28 %	1215.48	401.32 / 840	56.2 / 29.3	155 / 234	0.02 / 441	
syslog collector	Running	▲	0.11 %	403.6	62.29 / 94	23.2 / 24	144 / 157	0 / 229	

ネットワーク内の Crosswork Data Gateway の正常性を定期的に監視して、過負荷を防止し、追加のリソースを追加したり、Crosswork Data Gateway の負荷を適切なタイミングで削減するなどの是正措置を積極的に講じることをお勧めします。

1. Crosswork Data Gateway に障害が発生した場合、またはリソース容量の制限に近づいている場合、DG-Manager はアラームを生成します。[Crosswork UI] > [Showtech要求 (Showtech Requests)] から、またはアラームポッドにログインして、アラームの詳細を確認できます。

アラームには、イベントのタイトル、重大度、構成ステージ (Day 0、1、または 2)、説明、および修復アクションが含まれます。[Showtech要求 (Showtech Requests)] ウィンドウに移動する方法については、[Crosswork Data Gateway アラームの表示 \(20 ページ\)](#) を参照してください。

2. Crosswork Data Gateway の [CPU使用率 (CPU Utilization)] が 80% を超える場合は、デバイスを別の CDG に移動する、他の VM をプールに追加する、または既存の収集ジョブの頻度を増やすことによって、[CPU使用率 (CPU Utilization)] を下げるまで、収集ジョブを作成しないことをお勧めします。
3. Crosswork Data Gateway の [CPU使用率 (CPU Utilization)] が 90% を超える場合は、[CPU使用率 (CPU Utilization)] の低い別の Crosswork Data Gateway にデバイスを移動することをお勧めします。
4. システムアラームを毎週確認することをお勧めします。リソースの問題ではなく、データのドロップが頻繁に発生していないことを確認してください。次に、データの宛先の問題を修正するか、収集ジョブの頻度を増やします。

Crosswork Data Gateway アラームの表示

Crosswork Data Gateway は、データ収集を妨げる異常を検出すると、アラームを生成します。アラームを確認して、データ収集に影響を与える問題を理解し、必要に応じて修復アクションを実行できます。

アラームを表示するには、Crosswork UI に移動します。



(注) または、アラームポッドにログインして、DgManager.yaml ファイルでアラームを表示することもできます。


- ステップ 1** メインメニューから、[管理 (Administration)] > [Crosswork Manager] > [アプリケーション管理 (Application Management)] タブを選択し、[アプリケーション (Applications)] をクリックします。
- ステップ 2** [プラットフォームインフラストラクチャ (Platform Infrastructure)] タイルで、[詳細の表示 (View Details)] をクリックします。[アプリケーション詳細 (Application Details)] ウィンドウが開きます。
- ステップ 3** [マイクロサービス (Microservices)] タブで、[名前 (Name)] フィールドにアラームを入力して、アラームポッドを見つけます。アラームポッドのステータスは、正常である必要があります。
- ステップ 4** [アクション (Actions)] の下の  アイコンをクリックし、[Showtechリクエスト (Showtech Requests)] を選択します。[Showtech 要求 (Showtech Requests)] ウィンドウに、showtech ジョブの詳細が表示されます。
- ステップ 5** (オプション) アラームポッドにログインしてアラームを表示するか、[公開 (Publish)] をクリックしてアラームをダウンロードして showtech ログを公開します。[宛先サーバーの入力 (Enter Destination Server)] ダイアログボックスが表示されます。関連する詳細を入力し、[公開 (Publish)] をクリックします。

図 9: [Showtechリクエスト (Showtech Requests)] ウィンドウ

アラームは、指定した接続先で公開されます。

Crosswork Data Gateway プールの管理

次の手順を実行して Cisco Crosswork Data Gateway プールを編集または削除します。プールを作成するには、「[Cisco Crosswork Data Gateway プールの作成 \(10 ページ\)](#)」を参照してください。

始める前に

プールを編集または削除する前に考慮すべき重要なポイント：

- デバイスが接続されている仮想データゲートウェイまたはプールは削除できません。
- データゲートウェイインスタンスは、すべてのデバイスのマッピングが Crosswork Data Gateway から削除された場合にのみ、プールから削除できます。Crosswork Data Gateway インスタンスがプールから削除されると、フェールオーバー手順の実行後に、同じプールのスタンバイインスタンスがその代わりになります。手動フェールオーバーの詳細については、[手動フェールオーバーの実行 \(14 ページ\)](#)を参照してください。
- Crosswork Data Gateway プールを削除する前に、最初に Crosswork Data Gateway からデバイスを切り離すか、デバイスを別の Crosswork Data Gateway に移動します。

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

ステップ 2 Cisco Crosswork Data Gateway プールの編集：

- a) このページに表示されるプールの一覧から編集するプールを選択します。
- b) [高可用性 (HA) プールの編集 (Edit High Availability (HA) Pool)] ページを開くには、 ボタンをクリックします。

リソースプールを編集する場合、[プールリソース (Pool Resources)] ペインのパラメータのみを変更できます。[プールパラメータ (Pool Parameters)] ペインでパラメータを編集することはできません。[プールパラメータ (Pool Parameters)] ペインでパラメータを変更するには、必要な値で新しいプールを作成し、Cisco Crosswork Data Gateway インスタンスをそのプールに移動します。


図 10: [データゲートウェイの管理 (Data Gateway Management)] - [HAプールの編集 (Edit HA Pool)] ウィンドウ

The screenshot shows the 'Edit HA Pool' configuration page. At the top, there's a breadcrumb: Administration / Data Gateway Management / Edit HA Pool. The main form has several sections:

- Pool Name:** A text input field containing 'dev-test-pool' with a note: 'Alphabets, numbers, underscore, hyphen and dot are allowed.'
- Description:** A large empty text area.
- Pool Resources:** A section with a sub-section for 'FQDN' containing 'kantdev2test.cwisco.com' and a trash icon. Below it is an 'Add Another' link.
- Standby Gateways:** A field to 'Add the number of standby data gateways desired for protection' with a value of '0' and a help icon.
- Data Gateway Instance Types:** Radio buttons for 'Standard', 'Standard Plus with Extra Resources', and 'Extended'.
- Unassigned Data Gateway Instance(s):** A table with columns 'Operational State' and 'Data Gateway Instance Name'. It shows 'Selected 0 / Filter 0 / Total 0'.
- Data Gateway Instance(s) Added to Pool:** A table with columns 'In Use', 'Data Gateway Instance Name', and 'Data Gateway Name'. It shows 'Selected 0 / Filter 0 / Total 1' and one instance: 'kant-dev2test' with name 'dev-test-pool-1'.

- c) [プールリソース (Pool Resources)] ペインでは、プールタイプに応じて変化するリソースパラメータを変更できます。
- 必要なアクティブ データ ゲートウェイごとに仮想 IP アドレスまたは FQDN を追加および削除します。
 - スタンバイ Crosswork Data Gateway インスタンスの数を変更します。
 - Crosswork Data Gateway インスタンスをプールから追加および削除します。
 - プールの FQDN を有効または無効にします。
- d) 変更が完了したら、[保存 (Save)] をクリックします。

ステップ 3 Crosswork Data Gateway プールの削除 :

- 削除するプールを選択し、 をクリックします。
- [高可用性 (HA) プールの削除 (Delete High Availability (HA) Pool)] ウィンドウで [削除 (Delete)] をクリックして、プールを削除します。

Cisco Crosswork Data Gateway デバイス割り当ての管理

Crosswork Data Gateway からデバイスを移動または切り離す場合は、次のガイドラインに従います。

- デバイスは 1 つの Crosswork Data Gateway のみに接続できます。
- デバイスを異なるプールの Crosswork Data Gateway に移動する場合は、プールのゲートウェイが現在のプールのゲートウェイと同じであることを確認してください。ゲートウェイが一致しない Crosswork Data Gateway にデバイスを移動すると、収集が失敗します。

- Cisco Crosswork Data Gateway からデバイスを切り離すと、そのデバイスに対応するすべての収集ジョブが削除されます。切り離すデバイスに送信された収集ジョブを失いたくない場合は、代わりに別の Cisco Data Gateway にデバイスを移動します。

Crosswork Data Gateway プールからデバイスを移動または切り離すには、次の手順に従います。プールにデバイスを追加するには、「[Crosswork Data Gateway へのデバイスの接続 \(15 ページ\)](#)」を参照してください。

ステップ 1 Cisco Crosswork メインメニューから、[管理 (Administration)] > [Data Gateway の管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] に移動します。

図 11: [データゲートウェイ (Data Gateways)] ウィンドウ

The screenshot shows the 'Data Gateway Management' interface. At the top, there are tabs for 'Data Gateways', 'Pools', and 'Data Gateway Instances'. Below this is a 'Data Gateway Metrics Summary' section with four circular gauges: 'Operational State' (Up: 1, Error: 0, Degraded: 0), 'Administration State' (Up: 1, Maintenance: 0), 'High Availability Status' (Protected: 1, Not Protected: 0, Limited Protection: 0, None Planned: 0), and 'Devices' (Attached: 3, Available: 0). Below the metrics is a table of Data Gateways. The table has columns: Name, Operational State, Administration State, High Availability Status, Pool Name, Outage History, Average Availability, Data Gateway Instance Name, Attached Device Count, PDG Identifier, and Actions. The first row shows 'pool1-1' with 'Up' operational state, 'Up' administration state, 'Protected' high availability status, 'pool1' pool name, '100%' average availability, 'cdg-147.cisco.com' instance name, '3' attached device count, and '567837af-cd1...' PDG identifier. The 'Actions' column for 'pool1-1' is highlighted with a red box, showing a dropdown menu with options: 'Attach Devices', 'Detach Devices', 'Move Devices', and 'Initiate Failover'.

ステップ 2 デバイスを移動するには、次の手順を実行します。


- デバイスを移動する Crosswork Data Gateway の [アクション (Actions)] 列で、 をクリックして [デバイスの移動 (Move Devices)] を選択します。[接続されているデバイスの移動 (Move Attached Devices)] ウィンドウが開き、移動可能なすべてのデバイスが表示されます。
- [このデータゲートウェイに移動 (To this Data Gateway)] ドロップダウンから、デバイスの移動先のデータゲートウェイを選択します。

図 12: [接続デバイスの移動 (Move Attached Devices)] ウィンドウ

Move Attached Devices

From this Data Gateway: cdg1-1

To this Data Gateway: **Select Data Gateway** (dropdown menu showing cdg2-1 and cdg5-coe4-1)

Attached Devices: Selected 0 / Filtered 0 / Total 5113

	Host Name	IP Address	Tags	Operational State
<input type="checkbox"/>	Node_117_20	10.20.117.20/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_22	10.20.117.22/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_18	10.20.117.18/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_21	10.20.117.21/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_28	10.20.117.28/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_29	10.20.117.29/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_46	10.20.117.46/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_48	10.20.117.48/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_100	10.20.117.100/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_16	10.20.117.16/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_19	10.20.117.19/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_25	10.20.117.25/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_30	10.20.117.30/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok

Buttons: Move Selected Devices (0) | Move All Devices (5113) | Back

- c) すべてのデバイスを移動するには、[すべてのデバイスの移動 (Move All Devices)] をクリックします。それ以外の場合は、移動するデバイスを選択し、[選択したデバイスの移動 (Move Selected Devices)] をクリックします。
- d) [確認: デバイスの移動 (Confirm-Move Devices)] ウィンドウで、[移動 (Move)] をクリックします。

ステップ 3 デバイスを切り離すには、次の手順を実行します。

- a) デバイスを切り離す Crosswork Data Gateway の [アクション (Actions)] 列で、 をクリックして [デバイスの切断 (Detach Devices)] を選択します。[デバイスの切断 (Detach Devices)] ウィンドウが開き、接続されているすべてのデバイスが表示されます。

図 13: [デバイスの切断 (Detach Devices)] ウィンドウ

Detach Devices from Data Gateway cdg1-1

Selected 0 / Filtered 0 / Total 5114

	Host Name	IP Address	Tags	Operational State
<input type="checkbox"/>	Node_117_42	10.20.117.42/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_20	10.20.117.20/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_22	10.20.117.22/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_18	10.20.117.18/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_21	10.20.117.21/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_28	10.20.117.28/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_29	10.20.117.29/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_46	10.20.117.46/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_48	10.20.117.48/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_100	10.20.117.100/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_16	10.20.117.16/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_19	10.20.117.19/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_25	10.20.117.25/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_30	10.20.117.30/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_31	10.20.117.31/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_32	10.20.117.32/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_35	10.20.117.35/24	cdg-1;cjos-xr;cli;reach-check;snmp;te-tunnel-id;clock-d...	Ok
<input type="checkbox"/>	Node_117_19	10.20.117.19/24	cdg-1;cjos-xr;cli;snmp;reach-check;te-tunnel-id;clock-d...	Ok

Buttons: Detach Selected Devices (0) | Detach All Devices (5114) | Back

- b) すべてのデバイスを切り離すには、[すべてのデバイスの切断 (Detach All Devices)] をクリックします。それ以外の場合は、切り離すデバイスを選択し、[切断 (Detach)] をクリックします。
- c) [確認：デバイスの切断 (Confirm - Detach Devices)] ウィンドウで、[切断 (Detach)] をクリックします。

[データゲートウェイ (Data Gateways)] ペインの [接続デバイス数 (Attached Device Count)] を確認して、変更が成功したことを確認します。接続デバイス数の横にある ⓘ アイコンをクリックすると、選択した Crosswork Data Gateway に接続されているデバイスのリストが表示されます。

フェールオーバーを開始する方法については、[手動フェールオーバーの実行 \(14 ページ\)](#) を参照してください。

Crosswork Data Gateway インスタンスの維持

この項では、Crosswork Data Gateway インスタンスのメンテナンスタスクについて説明します。

- [Cisco Crosswork Data Gateway インスタンスの管理状態の変更 \(25 ページ\)](#)
- [Crosswork Data Gateway インスタンスを Cisco Crosswork から削除 \(27 ページ\)](#)
- [Crosswork Data Gateway インスタンスの再展開 \(28 ページ\)](#)

Cisco Crosswork Data Gateway インスタンスの管理状態の変更

Cisco Crosswork プラットフォームと Cisco Crosswork Data Gateway 間での動作を一時停止するために、データセンター内でアップグレードまたはその他のメンテナンスを実行することが必要になる場合があります。これは、Cisco Crosswork Data Gateway を [メンテナンス (Maintenance)] モードにすることで実現できます。ダウンタイム時に、管理者は証明書の更新などの変更を、Cisco Crosswork Data Gateway に加えることができます。



- (注) メンテナンスアクティビティが Crosswork と Crosswork Data Gateway の間の通信に影響を与えている場合は収集は中断され、通信が復元されると再開されます。同様に、メンテナンスアクティビティが Crosswork Data Gateway と外部接続先 (Kafka/gRPC) 間の通信に影響している場合は収集が相互に中断され、通信が復元されると再開されます。

変更が完了すると、管理者は管理状態を [アップ (Up)] に変更できます。Crosswork Data Gateway インスタンスが起動すると、Cisco Crosswork がジョブの送信を再開します。



- (注) [割り当て済み (Assigned)] 状態では、データゲートウェイをメンテナンスモードに直接切り替えることはできません。メンテナンスモードにするには、スタンバイが使用可能なときに手動フェールオーバーを実行するか、プールからデータゲートウェイを削除する必要があります。手動フェールオーバーの詳細については、[手動フェールオーバーの実行 \(14 ページ\)](#) を参照してください。

Crosswork Data Gateway インスタンスの管理状態を変更するには、次の手順を実行します。

始める前に

ロールが割り当てられている場合は、データゲートウェイを [メンテナンス (Maintenance)] モードに移行できません。これは、データゲートウェイがプールでアクティブであることを示しています。ただし、ゲートウェイには次のロールを割り当てることができます。

- 手動または自動フェールオーバーが発生した場合のスペアのロール。
- プール内の唯一のゲートウェイである場合に割り当てられるロール。

ステップ 1 メインメニューから、[管理 (Administration)] > [データゲートウェイの管理 (Data Gateway Management)] > [データゲートウェイインスタンス (Data Gateway Instances)] の順に選択します。

テーブル内のデータゲートウェイインスタンスまたはプール名をクリックして、インスタンスの動作と正常性の概要を表示する **Crosswork Data Gateway** の詳細ページに移動することもできます。データゲートウェイインスタンス名の横にある ⓘ をクリックすると、インターフェイスロールの詳細を含む登録の詳細が表示されます。

ステップ 2 Cisco Crosswork Data Gateway の場合に管理ステータスを変更するには、[アクション (Actions)] 列で ⋮ をクリックします。

図 14: [データゲートウェイインスタンス (Data Gateway Instances)] ウィンドウ

Operational State	Administration State	Data Gateway Instance Name	Role	Outage History	Data Gateway Name	Pool Name	PDG Identifier	High Availability Status	Actions
Not Ready ⓘ	Up	cdg-147.cisco.com ⓘ	Spare			pool1	567837af-cd1a-4...	Protected	⋮
Up	Up	cdg-148.cisco.com ⓘ	Assigned		pool1-2	pool1	63405e44-a220-...	Protected	⋮
Not Ready ⓘ	Up	cdg-149.cisco.com ⓘ	Unassigned				e2db0cd1-3eba-...	Not Protect	⋮

ステップ 3 切り替える管理状態を選択します。

Crosswork Data Gateway インスタンスを Cisco Crosswork から削除

Cisco Crosswork Data Gateway インスタンスを Cisco Crosswork から削除するには、次の手順を実行します。

始める前に

これらのデバイスに対応するジョブが失われないように、接続されているデバイスを別のデータゲートウェイに移動することをお勧めします。Cisco Crosswork Data Gateway インスタンスからデバイスを切り離すと、対応するジョブが削除されます。

ステップ 1 メインメニューから、[管理 (Administration)] > [データゲートウェイの管理 (Data Gateway Management)] > [データゲートウェイインスタンス (Data Gateway Instances)] の順に選択します。


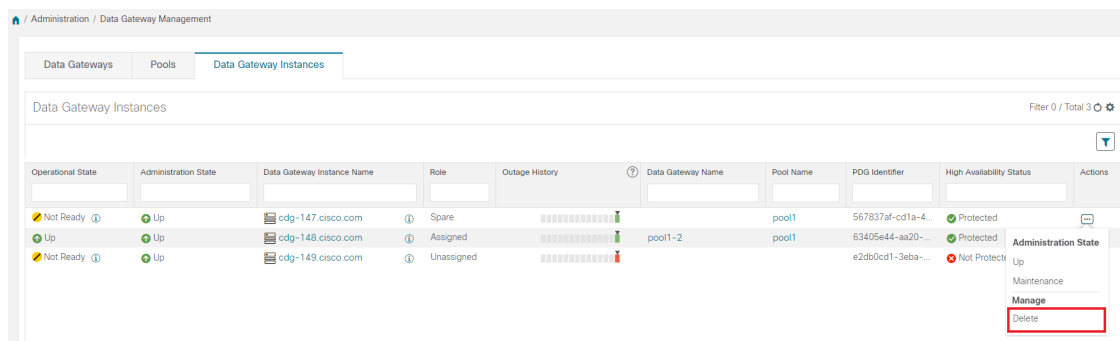
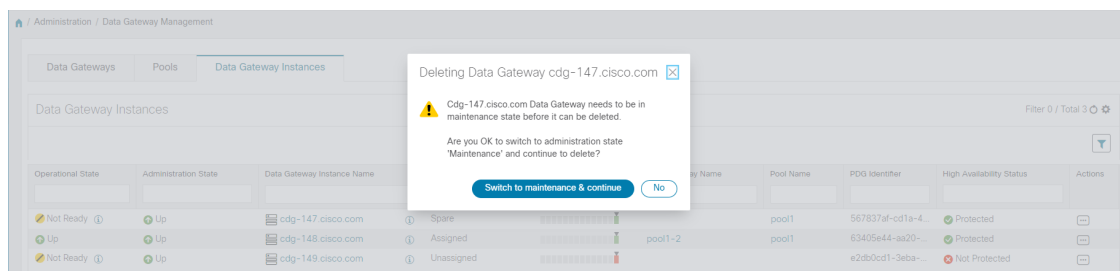
ステップ 2 Crosswork Data Gateway を削除する場合は、[アクション (Actions)] 列の下にある  をクリックし、[削除 (Delete)] をクリックします。

図 15: [データゲートウェイインスタンス (Data Gateway Instances)] ウィンドウ



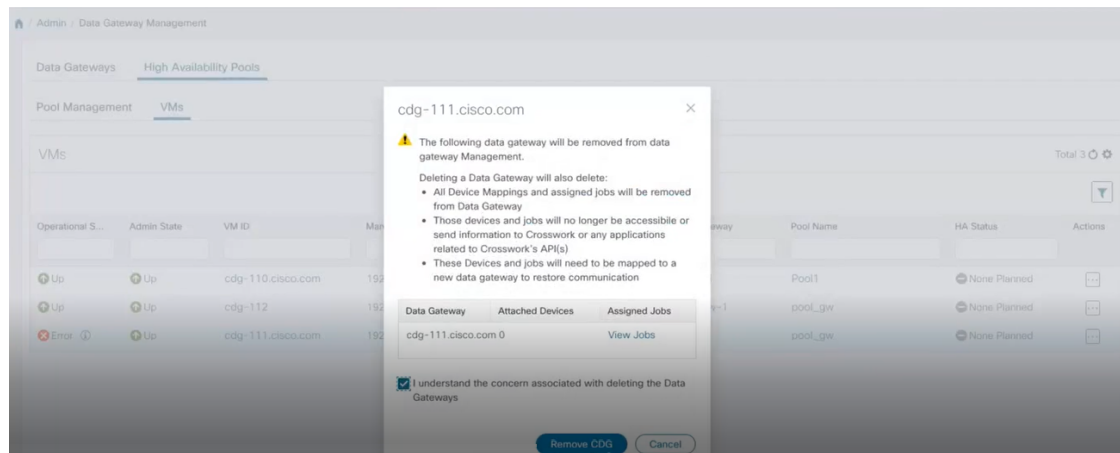
ステップ 3 削除する Cisco Crosswork Data Gateway インスタンスは、メンテナンスモードになっている必要があります。[メンテナンス (Maintenance)] モードに切り替えるように求められたら、[メンテナンスに切り替えて続行 (Switch to maintenance & continue)] をクリックします。

図 16: [メンテナンスに切り替えて続行 (Switch to maintenance & continue)] ポップアップウィンドウ



ステップ 4 [データゲートウェイの削除に関連する事項を理解しました (I understand the concern associated with deleting the Data Gateways)] のチェックボックスをオンにします。[CDGの削除 (Remove CDG)] をクリックします。

図 17: [データゲートウェイの削除確認 (Delete Data Gateway Confirmation)]ダイアログボックス



Crosswork Data Gateway インスタンスの再展開

Crosswork Data Gateway インスタンスを再展開するには、古いインスタンスを削除して新しいインスタンスをインストールします。新しい Crosswork Data Gateway インスタンスをインストール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。』

インスタンスの展開プロファイルを変更するために Crosswork Data Gateway インスタンスを再展開する場合（たとえば、プロファイルを Standard から Extended に変更する場合）、Crosswork Data Gateway インスタンスの再展開を試みる前に、Data Gateway グローバルパラメータの変更を手動でロールバックしてください。

考慮すべき重要な点

1. Crosswork Data Gateway インスタンスがすでに Cisco Crosswork に登録されており、同じ名前でインスタンスを再度インストールした場合は、Crosswork Data Gateway インスタンスの [管理状態 (Administration State)] を [メンテナンス (Maintenance)] に変更して自動登録を実行します。
2. Crosswork Data Gateway インスタンスがすでに Cisco Crosswork に登録されており、Cisco Crosswork を再度インストールした場合は、既存の Crosswork Data Gateway インスタンスを Cisco Crosswork に再登録します。

[Crosswork Data Gateway の再登録](#) を参照してください。

Crosswork Data Gateway のグローバル設定の設定

このセクションでは、Cisco Crosswork Data Gateway のグローバル設定を設定する方法について説明します。これらの設定は次のとおりです。

- [外部データ送信先の作成と管理 \(29 ページ\)](#)
- [デバイスパッケージの管理 \(37 ページ\)](#)
- [Crosswork Data Gateway のグローバルパラメータの設定 \(40 ページ\)](#)
- [Crosswork Data Gateway リソースの割り当て \(43 ページ\)](#)

外部データ送信先の作成と管理

Cisco Crosswork では、収集ジョブでデータをデポジットするために使用できる外部データ送信先 (Kafka または外部 gRPC) を作成できます。

これには、[管理 (Administration)] > [データゲートウェイのグローバル設定 (Data Gateway Global Settings)] > [データ送信先 (Data Destinations)] に移動してアクセスできます。新しいデータ送信先の追加、既存のデータ送信先の設定の更新、データ送信先の削除を行うことができます。

[データ送信先 (Data Destinations)] ページのテーブルには、データをデポジットするために収集ジョブで使用できる承認済みのデータ送信先のリストが表示されます。



(注) **Crosswork_Kafka** と **cd-astack-pipeline** は内部データ送信先であり、更新または削除はできません。

図 18: [データ送信先 (Data Destinations)] ウィンドウ

Destination Name	Server Type	Compression Type	Encoding	UUID
<input type="checkbox"/> Crosswork_Kafka	① Kafka	snappy	gbkv	c2a8fba8-8363-3d22-b0c2-a9e449693fae
<input type="checkbox"/> D1	① Kafka	snappy	gbkv	7e635a06-b203-4b07-a137-80f99a4b00f3
<input type="checkbox"/> External-non-ssl-kafka	① Kafka	snappy	gbkv	c4a0b41d-bf7d-4242-a8d0-9c19fc3d0d33
<input type="checkbox"/> External-non-ssl-kafka-json	① Kafka	none	json	3925e312-3039-4fde-9e57-4b234442c6a4
<input type="checkbox"/> cdg-astack-pipeline	① gRPC	gzip	gbkv	e9b4c2ec-b2e6-4db0-a942-0402dd347a1d
<input type="checkbox"/> external-grpc-destination	① gRPC	gzip	gbkv	e6cd875f-c2c3-4116-9210-d9ca37ff4114
<input type="checkbox"/> grpc-external-destination	① gRPC	gzip	gbkv	ccd82ff2-03e9-4325-a943-67d575738605

UUID は、データ送信先の一意的識別子です。Cisco Crosswork は、外部データ送信先が作成されると、この ID を自動的に生成します。Cisco Crosswork UI を使用して収集ジョブを作成する場合、設定済みの送信先のドロップダウンリストを使用してデータの送信先を選択します。API を介して収集ジョブを作成する場合、収集したデータをコレクタが送信する宛先の UUID を知る必要があります。

データ送信先の詳細を表示するには、[データ送信先 (Data Destinations)] ペインで、詳細を表示するデータ送信先名の横にある ⓘ アイコンをクリックします。

外部収集ジョブのライセンス要件

データを外部のデータ送信先に転送できる収集ジョブを作成できるようにするには、次のライセンス要件を満たしていることを確認します。

1. メインメニューから、[管理 (Administration)] > [アプリケーション管理 (Application Management)] > [スマートライセンス (Smart License)] に移動します。
2. アプリケーションフィールドで [Crossworkプラットフォームサービス (Crosswork Platform Services)] を選択します。
3. ステータスが次のようになっていることを確認します。
 - [登録ステータス (Registration Status)] : [登録済み (Registered)]
Cisco Smart Software Manager (CSSM) に登録済みであり、予約済みライセンス機能の使用が許可されていることを示します。
 - [ライセンス認証ステータス (License Authorization Status)] : [認証済み (Authorized)] ([準拠 (In Compliance)])
外部収集ジョブのデバイス数を超えていないことを示します。
 - [スマートライセンスの使用状況 (Smart Licensing Usage)] で、**CW_EXTERNAL_COLLECT** のステータスが [準拠 (In Compliance)] になっています。

評価期間が終了した後、または外部収集ジョブのデバイス数を超えた場合 ([ライセンス認証ステータス (License Authorization Status)] が [コンプライアンス違反 (Out of Compliance)])、Cisco Smart Software Manager (CSSM) に登録しないと、外部収集ジョブを作成できません。ただし、この場合も既存の収集ジョブは表示および削除できます。

データ宛先の追加または編集

新しいデータ送信先を追加するには、次の手順を実行します。その後、このデータ宛先を使用してデータを転送できます。複数のデータ送信先を追加することができます。

外部データの宛先を追加する際の注意点は次のとおりです。

- 既存の外部 Kafka データの送信先を同じ IP アドレスで再インストールする場合は、コレクタを再起動して変更を有効にする必要があります。
- Cisco Crosswork および指定したデータ送信先、つまり Crosswork Kafka または外部 Kafka のいずれかの間通信チャンネルをセキュリティで保護できます。(この手順の **ステップ 6** に進みます)。ただし、セキュリティを有効にすると、パフォーマンスに影響する可能性があります。
- 外部データ送信先で TLS 接続が必要な場合は、公開証明書を準備するか、クライアント認証が必要な場合は、クライアント証明書とキーファイルを準備します。クライアントキーはパスワードで暗号化されている可能性があり、データ送信先のプロビジョニングの

一部として設定する必要があります。現在、Crosswork Data Gateway は IP ベースの証明書のみをサポートしています。

- 認証局で証明書を生成する場合は、証明書が PEM でエンコードされ、キーファイルが PKCS # 8 形式であることを確認します。
- Cisco Crosswork にジョブを送信する前に、Kafka トピックを作成してください。外部 Kafka とその外部 Kafka でのトピックの管理方法によっては、収集されたデータをその特定の外部 Kafka/トピックにディスパッチするときにトピックが存在しない場合、Cisco Crosswork ログに次の例外が表示されます。これは、トピックがまだ作成されていないか、収集ジョブが完了する前にトピックが削除されたことが原因である可能性があります。

```
destinationContext: topicmdt4
org.apache.kafka.common.errors.UnknownTopicOrPartitionException: This server does not host this topic-partition.
```

- データ宛先のポート接続を確認して検証します。宛先でポートに到達できない場合、収集が失敗します。
- Crosswork Data Gateway では、Kafka 宛先の宛先プロパティでカスタム値を設定できます（この手順のステップ 4 を参照）。



(注) この機能は、gRPC 宛先ではサポートされていません。

- [宛先の詳細 (Destination Details)] ペインに入力されたグローバルプロパティは必須であり、個々のコレクタレベルでカスタム値が指定されていない限り、デフォルトで Kafka 宛先に適用されます。コレクタに指定するカスタム値は、そのコレクタにのみ適用されます。
- Crosswork Data Gateway の展開時に指定されたプロトコルに応じて、外部宛先は IPv4 または IPv6 である必要があります。たとえば、展開中に IPv4 が選択された場合、外部宛先も IPv4 である必要があります。
- ホスト名と IP アドレスマッピングの変更は、DNS サーバーの [存続可能時間 (TTL) (Time to Live (TTL))] フィールドで構成された期間が完了した後のみ、Crosswork Data Gateway に反映されます。変更をすぐに反映させたい場合は、VM を再起動することをお勧めします。

始める前に

データ収集に外部 Kafka サーバーを使用している場合は、次のことを確認します。

- 外部 Kafka サーバーで次のプロパティを設定した。



(注) この説明はこのドキュメントの対象範囲外であるため、これらのプロパティの説明と使用方法については、Kafka のドキュメントを参照してください。

- num.io.threads = 8
- num.network.threads = 3
- message.max.bytes= 30000000

- データ収集に使用する Kafka トピックを作成している。
- 新規の収集ジョブを開始する前に、「reachability-topic」がこの Kafka 接続先に設定されていることを確認します。この構成は、Kafka 接続先の正常性を監視するために必要です。

ステップ 1 メインメニューから、[管理 (Administration)] > [Data Gateway のグローバル設定 (Data Gateway Global Settings)] > [データ宛先 (Data Destinations)] を選択します。

ステップ 2 [データ送信先 (Data Destinations)] ページで、 ボタンをクリックします。[接続先の追加 (Add Destination)] ページが開きます。

既存の接続先を編集する場合は、 ボタンをクリックして [接続先の編集 (Edit Destination)] ページを開き、パラメータを編集します。

(注) データ送信先を更新すると、更新内容に従って Cisco Crosswork Data Gateway がそのデータ送信先とのセッションを再確立するようになります。データ収集は一時停止され、セッションが再確立されると再開されます。

ステップ 3 次のパラメータの値を入力するか、または変更します。

フィールド	値	利用可能 gRPC	利用可能 Kafka
接続先名 (Destination Name)	わかりやすいデータ送信先名を入力します。名前には、最大 128 文字の英数字と、アンダースコア (「_」)、またはハイフン (「-」) を含めることができます。その他の特殊文字は使用できません。 多数のデータ送信先がある場合は、後で識別できるように、できるだけわかりやすい名前にします。	対応	対応
サーバタイプ (Server Type)	ドロップダウンから、データ送信先のサーバタイプを選択します。	対応	対応
エンコーディング (Encoding)	ドロップダウンから、エンコーディング (json または gpbkv) を選択します。	対応	対応

フィールド	値	利用可能 gRPC	利用可能 Kafka
圧縮タイプ (Compression Type)	ドロップダウンから、圧縮タイプを選択します。	対応 サポートされている圧縮タイプは、snappy、gzip、lz4、zstd、および none です。 (注) zstd 圧縮タイプは、Kafka 2.0 以降でのみサポートされています。	対応 サポートされている圧縮タイプは、snappy、gzip、および deflate です。
ディスパッチの種類 (Dispatch Type)	このフィールドは、[サーバータイプ (Server Type)] フィールドが gRPC に設定されている場合に使用できます。 ドロップダウンから、ディスパッチ方法としてストリームまたは単項を選択します。 Crosswork Data Gateway は、収集したデータをデータストリームまたは単項として宛先に送信します。デフォルト値は、単項です。	対応	非対応
最大メッセージサイズ (バイト単位) (Maximum Message Size (bytes))	最大メッセージサイズを入力します (バイト単位)。 <ul style="list-style-type: none"> • デフォルト値 : 100000000 バイト/30 MB • 最小 : 1000000 バイト/1 MB • 最大 : 100000000 バイト/30 MB 	非対応	対応

フィールド	値	利用可能 gRPC	利用可能 Kafka
バッファメモリ (Buffer Memory)	必要なバッファメモリをバイト単位で入力します。 <ul style="list-style-type: none"> デフォルト値：52428800 バイト 最小：52428800 バイト 最大：314572800 バイト 	非対応	対応
バッチサイズ (バイト単位) (Batch Size (bytes))	必要なバッチサイズを入力します (バイト単位)。 <ul style="list-style-type: none"> デフォルト値：6400000 バイト/6.4 MB 最小：16384 バイト/16.38 KB 最大：6400000 バイト/6.4 MB 	非対応	対応
リンガー (ミリ秒) (Linger (milliseconds))	必要なリンガー時間を入力します (ミリ秒単位)。 <ul style="list-style-type: none"> デフォルト値：5,000 ms 最小：0 ms 最大：5000 ms 	非対応	対応
要求のタイムアウト (Request Timeout)	要求が応答を待機する時間を入力します。構成された時間が経過すると、要求は期限切れになります。 <ul style="list-style-type: none"> デフォルト値：30 ミリ秒 最小：30 ミリ秒 最大：60 ミリ秒 	対応	対応

テレメトリベースの収集の場合は、最適な結果を得るために、[バッチサイズ (Batch size)] を 16,384 バイト、[リンガー (Linger)] を 500 ミリ秒に設定することをお勧めします。

ステップ 4 (オプション) Kafka 接続先のグローバルプロパティとは異なるカスタム値を設定するには、[コレクタ設定のカスタマイズ (Customize Collector Settings)] ペインで、

- a) [コレクタ (Collector)] を選択します。
- b) 以下のフィールドに値を入力します。
 - カスタムバッファメモリ
 - カスタムバッチサイズ

(注) [カスタムバッチサイズ (Custom Batch Size)] は [カスタムバッファメモリ (Custom Buffer Memory)] の実行時の値を超えることはできません。 [カスタムバッファメモリ (Custom Buffer Memory)] フィールドに値を指定しない場合、 [カスタムバッチサイズ (Custom Batch Size)] は [バッファメモリ (Buffer Memory)] フィールドの値に対して検証されます。

- [カスタムリンガー (Custom Linger)]
- [カスタム要求タイムアウト (Custom Request Timeout)]

図 19: [接続先の追加 (Add Destination)] ウィンドウ

c) [+別を追加 (+ Add Another)] をクリックしてこの手順を繰り返し、別のコレクタのカスタム設定を追加します。

(注) ここで入力した個々のコレクタのプロパティは、ステップ 3 で入力したグローバル設定よりも優先されます。ここでフィールドに値を入力しない場合、同じ値はステップ 3 で入力したグローバルプロパティから取得されます。

ステップ 5 [接続の詳細 (Connection Details)] オプションから TCP/IP スタックを選択します。サポートされているプロトコルは、IPv4、IPv6、および FQDN です。

(注) FQDN アドレスは、Kafka 接続先に対してのみサポートされます。

ステップ 6 次の表に従って [接続の詳細 (Connection Details)] フィールドに入力します。表示されるフィールドは、選択した接続タイプによって異なります。入力する値は、外部 Kafka または gRPC サーバーで設定されている値と一致する必要があります。

接続タイプ (Connectivity Type)	フィールド	gRPC で利用可能	Kafka で利用可能
IPv4	必要な [IPv4 アドレス/サブネットマスク (IPv4 Address/Subnet Mask)] と [ポート (Port)] に入力します。[+ もう 1 つ追加する (+ Add Another)] をクリックして、複数の IPv4 アドレスを追加できます。 IPv4 サブネットマスクの範囲は 1 ～ 32、ポートの範囲は 1024 ～ 65535 です。	対応	対応
IPv6	必要な [IPv6 アドレス/サブネットマスク (IPv6 Address/Subnet Mask)] と [ポート (Port)] に入力します。[+ もう 1 つ追加する (+ Add Another)] をクリックして、複数の IPv6 アドレスを追加できます。 IPv6 サブネットマスクの範囲は 1 ～ 128、ポートの範囲は 1024 ～ 65535 です。	対応	対応
FQDN	必要な [ホスト名 (Host Name)]、[ドメイン名 (Domain Name)]、および[ポート (Port)] に入力します。サポートされるポートの範囲は 1024 ～ 65535 です。 [+ もう 1 つ追加する (+ Add Another)] をクリックして、複数の FQDN アドレスを追加できます。	対応	対応

ステップ 7 (オプション) Kafka または gRPC ベースのデータ送信先に安全に接続するには、[セキュリティの詳細 (Security Details)] スライダを移動して [セキュア通信の有効化 (Enable Secure Communication)] オプションを有効にします。

ステップ 8 Kafka または gRPC ベースのデータ送信先の場合、次のいずれかを選択して、認証プロセスのタイプを選択します。

- 相互認証 (Mutual-Auth) : CA 証明書の後に外部サーバーと Crosswork Data Gateway コレクタを認証し、中間証明書またはキーが Crosswork UI にアップロードされます。
- サーバー認証 (Server-Auth) : CA 証明書を Crosswork UI にアップロードしてから、外部サーバーと Crosswork Data Gateway コレクタを認証します。[サーバー認証 (Server-Auth)] がデフォルトの認証プロセスです。

(注) 認証オプションは、[セキュア通信の有効化 (Enable Secure Communication)] が有効になっている場合にのみ使用できます。

ステップ9 [保存 (Save)] をクリックします。

次のタスク

[セキュア通信の有効化 (Enable Secure Communication)] オプションを有効にした場合は、Cisco Crosswork UI ([管理 (Administration)] > [証明書の管理 (Certificate Management)]) に移動し、新たに追加したデータ送信先に関連する証明書を追加します。この手順は、デバイスとのセキュアな通信を確立するには必須です。詳細については、[証明書の管理](#)を参照してください。



(注) [セキュア通信の有効化 (Enable Secure Communication)] オプションを有効にした後、データ送信先の証明書を追加しなかった場合、Cisco Crosswork はすべての収集ジョブに対して非セキュアモードで接続先に接続します。


データ送信先の削除

データ送信先を削除するには、次の手順を実行します。

始める前に

データ送信先は、どの収集ジョブにも関連付けられていない場合にのみ削除できます。[収集ジョブ (Collection Jobs)] ビューで、データ送信先を使用している収集ジョブがあるかどうかを確認することをお勧めします。

ステップ1 メインメニューから、[管理 (Administration)] > [データゲートウェイのグローバル設定 (Data Gateway Global Settings)] > [データ宛先 (Data Destinations)] を選択します。

ステップ2 表示された宛先一覧から削除したいデータ宛先を選択し、 ボタンをクリックします。

ステップ3 [データ送信先の削除 (Delete Data Destination(s))] ポップアップで、[削除 (Delete)] をクリックして確認します。

デバイスパッケージの管理

デバイス管理により、Crosswork Data Gateway は、デバイスパッケージを介してデータ収集機能をシスコのアプリケーションとサードパーティデバイスに拡張できます。Crosswork Data Gateway は、システムおよびカスタムデバイスパッケージをサポートします。

システムデバイスと MIB パッケージは、Crosswork ソフトウェアにバンドルされており、システムインスタンスに自動的にダウンロードされます。システムデバイスと MIB パッケージは変更できません。

カスタムデバイスパッケージは、デバイスの対象範囲と収集機能をサードパーティデバイスに拡張します。

[パッケージ (Packages)]ペインには、[管理 (Administration)]>[データゲートウェイのグローバル設定 (Data Gateway Global Settings)]>[パッケージ (Packages)]からアクセスできます。

カスタムパッケージ

次の3つのタイプのカスタムパッケージを Cisco Crosswork にアップロードできます。

1. **CLI デバイスパッケージ** : CLI ベースの KPI を使用して、サードパーティ製デバイスのデバイス正常性をモニターします。すべてのカスタム CLI デバイスパッケージは、対応する YANG モデルとともにファイル `custom-cli-device-packages.tar.xz` に含まれている必要があります。複数のファイルをサポートできます。
2. **カスタム MIB パッケージ** : カスタム MIB およびデバイスパッケージは、サードパーティ製デバイスに固有であるか、または収集されたデータをフィルタ処理したり、シスコデバイス用に異なる形式にしたりするために使用できます。これらのパッケージは編集できます。すべてのカスタム SNMP MIB パッケージは、YANG モデルとともにファイル `custom-mib-packages.tar.xz` に含める必要があります。複数のファイルをサポートできます。



(注) Cisco Crosswork Data Gateway は、システムにすでに含まれている標準的な MIB のサードパーティ製デバイスで SNMP ポーリングを有効にします。独自の MIB は、収集要求が独自の MIB から MIB テーブル名またはスカラー名を参照する場合にのみ必要です。ただし、要求が OID ベースの場合、MIB は必要ありません。

3. **SNMP デバイスパッケージ** : Cisco Crosswork Data Gateway では、必要な MIB と YANG の説明を追加したカスタム SNMP デバイスパッケージをアップロードすることで、SNMP カバレッジを拡張できます。

カスタムパッケージの追加

これは、Cisco Crosswork へのパッケージのアップロードに関するガイドラインのリストです。

1. 1つのパッケージ tar.gz ファイルに1つ以上の xar ファイルをアップロードできます。
2. Cisco Crosswork では、カスタム MIB パッケージファイルでシステム MIB パッケージファイルを上書きすることはできません。その結果、アップロード試行が失敗します。
3. カスタムパッケージの TAR ファイルに含まれているのはパッケージフォルダのみであり、TAR ファイルの一部として親フォルダまたはフォルダの階層が含まれていないことを確認します。正しくインポートされなかった場合、Cisco Crosswork はカスタムパッケージでジョブを実行すると例外をスローします。



(注) Cisco Crosswork は、ファイル拡張子をチェックする以外に、アップロードされるファイルを検証しません。

次の手順を実行してカスタム ソフトウェア パッケージをアップロードします。


始める前に

カスタム MIB パッケージの一部として新しい MIB をアップロードする場合は、それらの新しい MIB ファイルを既存のシステム MIB ファイルとともにコレクタ内にアップロードできることを確認します。つまり、ファイル内のすべての依存関係が適切に解決されます。



- (注) カスタムパッケージを実行する収集ジョブのパフォーマンスは、カスタムパッケージがどの程度最適化されているかによって異なります。Cisco Crosswork にアップロードする前に、パッケージが展開したい規模に最適化されていることを確認してください。

カスタム MIB と YANG を検証する方法、つまり、それらが Cisco Crosswork にアップロードできるかどうかを確認する方法については、『[Use Custom MIBs and Yangs on Cisco DevNet](#)』を参照してください。

-
- ステップ 1** メインメニューから、[管理 (Administration)] > [データゲートウェイのグローバル設定 (Data Gateway Global Settings)] を選択します。
- ステップ 2** [カスタムパッケージ (Custom Packages)] ペインで、 をクリックします。
- 既存のカスタム CLI デバイスパッケージを更新するには、テーブルのファイル名の横にあるアップロードアイコンをクリックします。
- ステップ 3** 表示される [カスタムパッケージの追加 (Add Custom Package)] ウィンドウで、インポートするパッケージのタイプを [タイプ (Type)] ドロップダウンから選択します。
- ステップ 4** [ファイル名 (FileName)] の空白フィールドをクリックしてファイルブラウザウィンドウを開き、インポートするパッケージを選択して [開く (Open)] をクリックします。
- ステップ 5** [メモ (Notes)] フィールドにパッケージの説明を追加します。多数のパッケージがある場合は、それらを区別できるようにこの手順で説明を加えることをお勧めします。
- ステップ 6** [アップロード (Upload)] をクリックします。
-


次のタスク

影響を受けたすべてのサービスを再起動して、最新のカスタム MIB パッケージの更新を取得します。

カスタムパッケージの削除

カスタムパッケージを削除すると、すべての YANG ファイルと XAR ファイルが Cisco Crosswork から削除されます。これは、カスタムパッケージを使用するすべての収集ジョブに影響します。

カスタムパッケージを削除するには、次の手順に従います。

- ステップ 1** メインメニューから、[管理 (Administration)] > [データゲートウェイのグローバル設定 (Data Gateway Global Settings)] > [パッケージ (Packages)] > [カスタム (Custom)] を選択します。
- ステップ 2** [カスタムパッケージ (Custom Packages)] ペインに表示されているリストから、削除するパッケージを選択して  をクリックします。
- ステップ 3** 表示された [カスタムパッケージの削除 (Delete Custom Package)] ウィンドウで、[削除 (Delete)] をクリックして確認します。

システムデバイスパッケージ

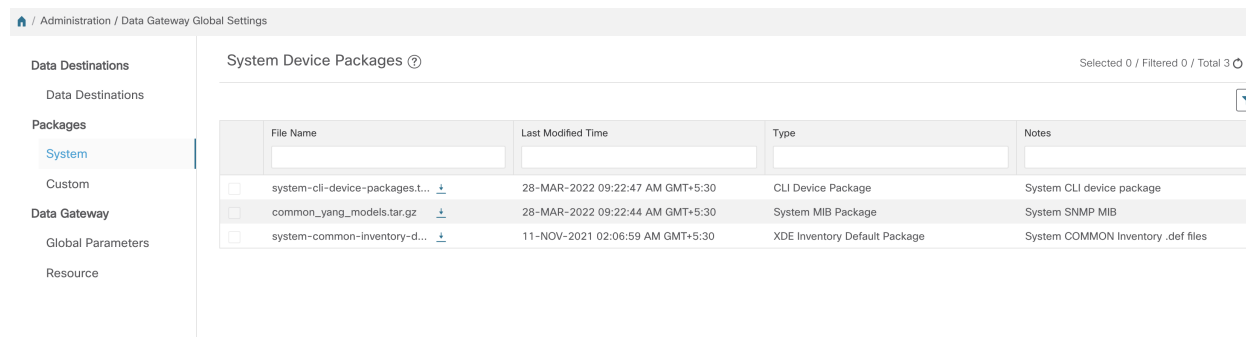
システムデバイスパッケージには、1 つ以上の個別のインストール可能ファイルが含まれています。パッケージ内の各ファイルセットは、同じアプリケーションに属します。

システムデバイスパッケージは、アプリケーション固有のマニフェストファイルを通じて単純な JSON ファイルとして提供されます。アプリケーションがインストールまたは更新されるたびに、システムデバイスパッケージが追加または更新されます。アプリケーションは、複数のデバイスパッケージをインストールできます。




重要 管理者は、システムデバイスパッケージを変更できません。これらのファイルを変更できるのは、アプリケーションのみです。システムデバイスパッケージを変更するには、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。

図 20: システムデバイスパッケージ (System Device Packages) ウィンドウ



File Name	Last Modified Time	Type	Notes
system-cli-device-packages.t...	28-MAR-2022 09:22:47 AM GMT+5:30	CLI Device Package	System CLI device package
common_yang_models.tar.gz	28-MAR-2022 09:22:44 AM GMT+5:30	System MIB Package	System SNMP MIB
system-common-inventory-d...	11-NOV-2021 02:06:59 AM GMT+5:30	XDE Inventory Default Package	System COMMON Inventory .def files

デバイスパッケージをダウンロードするには、[ファイル名 (File Name)] 列の名前の横にある  ボタンをクリックします。

Crosswork Data Gateway のグローバルパラメータの設定

Crosswork Data Gateway を使用すると、ネットワーク内のすべての Crosswork Data Gateway で次のパラメータを更新できます。



(注) これらの設定には、管理者ユーザーのみがアクセスできます。

ステップ 1 [管理 (Administration)] > [データゲートウェイのグローバル設定 (Data Gateway Global Settings)] > [データゲートウェイ (Data Gateway)] > [グローバルパラメータ (Global Parameters)] に移動します。

図 21: [グローバルパラメータ (Global Parameters)] ウィンドウ

ステップ 2 次のパラメータの 1 つ以上を変更します。

(注) 更新するポート値が有効なポートであり、既存のポート値と競合しないことを確認してください。デバイス上で同じポート値を設定する必要があります。

パラメータ名	説明
CLI セッションの数	Crosswork Data Gateway とデバイス間の CLI セッションの最大数。デフォルト値は 3 です。 (注) この値は、同じパラメータに設定されている内部構成をオーバーライドします。
SNMP Trap Port	デフォルト値は 1062 です。
Syslog UDP ポート	デフォルト値は 9514 です。
Syslog TCP ポート	デフォルト値は 9898 です。
Syslog TLS ポート	デフォルト値は 6514 です。

パラメータ名	説明
NMPV3 の USM エンジンの詳細を強制的に再同期する	<p>USMの詳細は、デバイスが再起動または再イメージ化されるたびに変更されます。SNMPV3 コレクションは、USMの詳細のいずれかが変更されるたびに機能を停止します。</p> <p>このオプションを有効にすると、最初の収集が失敗した後、変更があるたびに USM の詳細が自動的に同期されます。</p> <p>デフォルト値は [False] です。</p>

ステップ 3 ポートを更新する場合は、表示される [グローバルパラメータ (Global Parameters)] ウィンドウで [はい (Yes)] を選択して、コレクタを再起動できることを確認します。ポートを更新すると、コレクタは再起動し、実行中の収集ジョブを一時停止します。再起動が完了すると、ジョブは自動的に再開されます。

ステップ 4 [保存 (save)] をクリックして変更を適用します。

ネットワーク内の Crosswork Data Gateway でのパラメータの更新が成功したかどうかを示すウィンドウが表示されます。

1. すべての Crosswork Data Gateway が正常に更新された場合、更新が成功したことを示す成功メッセージが UI に表示されます。
2. ネットワーク内の Crosswork Data Gateways のいずれかを更新できなかった場合、UI にエラーウィンドウが表示されます。Crosswork Data Gateway は、復旧中に障害が発生した Crosswork Data Gateway のパラメータを自動的に更新しようとします。一部のコレクタは、リカバリの一環として再始動される場合があります。



(注) Crosswork Data Gateway でグローバルパラメータの更新に失敗する理由の 1 つは、OAM チャンネルがダウンしている可能性があります。OAM チャンネルが再確立された後、Crosswork Data Gateway はこれらのパラメータを Crosswork Data Gateway に再度送信しようとし (同期していません) 、既存の値と比較した後に値を更新します。

次のタスク

いずれかのポートを更新した場合は、[管理 (Administration)] > [データゲートウェイの管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] タブに移動し、すべての Crosswork Data Gateways の [動作状態 (Operational State)] が [アップ (Up)] になっていることを確認します。

Crosswork Data Gateway リソースの割り当て

Crosswork Data Gateway を使用すると、コレクタサービスの実行時にメモリを動的に設定して割り当てることができます。使用頻度の高いコレクタにさらに多くのメモリを割り当てたり、UI からリソースのバランスを調整したりできます。



(注) これらの設定には、管理者ユーザーのみがアクセスできます。

このページには、コレクタサービス用に現在設定されているメモリと CPU のセットが表示されます。このページでメモリ値に加えた変更は、現在登録済み、および将来の Crosswork Data Gateway に適用されます。



(注) このページに表示されるコレクタのリストは動的です。つまり、展開に固有です。

コレクタのリソース割り当てを更新するには、次の手順を実行します：



(注) Cisco Customer Experience (CX) チームと協力していない限り、これらの設定を変更しないことをお勧めします。

ステップ 1 コレクタのリストと、コレクタごとに消費されたリソースがここに表示されます。

図 22: [リソース (Resource)] ウィンドウ

Collector	Memory (MB)	CPU Set	Enable Collector
*CLI	8192 <small>0 or Range 500 - 153600 mb</small>	2-11	<input checked="" type="checkbox"/>
GNMI	9216 <small>0 or Range 500 - 153600 mb</small>	2-11	<input checked="" type="checkbox"/>
MDT	5120 <small>0 or Range 500 - 153600 mb</small>	2-11	<input type="checkbox"/>
*NETCONF	3072 <small>0 or Range 500 - 153600 mb</small>	2-11	<input checked="" type="checkbox"/>
*SNMP	9216 <small>0 or Range 500 - 153600 mb</small>	2-11	<input checked="" type="checkbox"/>
SYSLOG	5120 <small>0 or Range 500 - 153600 mb</small>	2-11	<input checked="" type="checkbox"/>

ステップ 2 メモリ割り当てを変更するコレクタの [メモリ (Memory)] フィールドに、更新された値を入力します。

注目 CLI および SNMP コレクタには 2000 MB、NETCONF コレクタには 1000 MB の最小メモリサイズをお勧めします。

ステップ 3 [コレクタの有効化 (Enable Collector)] スライダをオンの位置にドラッグして、データ収集を有効にします。

ステップ 4 変更が完了したら、[保存 (Save)] をクリックします。

コレクタの値を更新すると、コレクタが再起動し、実行中の収集ジョブが一時停止します。再起動が完了すると、ジョブは自動的に再開されます。

コレクタの有効化または無効化

Crosswork Data Gateway は、データ収集を有効にすると、構成されたコレクタを介してデータの収集を開始し、無効にするまで継続します。リソースを最適化するために、またはデータ収集に影響を与えるコレクタに問題がある場合は、コレクタサービスを無効にすることができます。

コレクタを有効または無効にするには：

始める前に

コレクタを有効または無効にする前に、次の情報を確認してください。

- SNMP および CLI コレクタ (コンテナ) のデータ収集を無効にすることはできません。これらのコレクタは、デバイスの到達可能性を確認するために必要です。
- デフォルトでは、コレクタは有効な状態になっています。

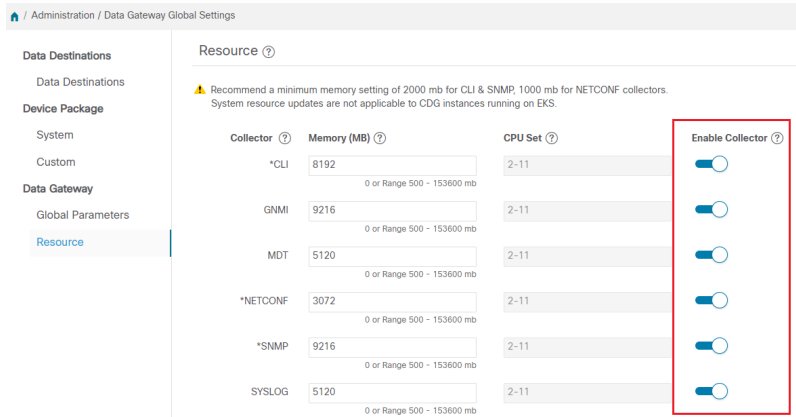


注目 コレクタは、Day 0 または Day 1 の構成中にのみ無効にする必要があります。Day 1 の後にコレクタを無効にする予定の場合、管理者は関連する収集ジョブを手動でクリアする必要があります。

ステップ 1 [管理 (Administration)] > [データゲートウェイのグローバル設定 (Data Gateway Global Settings)] > [データゲートウェイ (Data Gateway)] > [リソース (Resource)] に移動します。

コレクタのリストとリソース制限が表示されます。

図 23: コレクタの有効化または無効化



ステップ 2 [コレクタの有効化/無効化 (Enable/Disable Collectors)] スライダをオンの位置にドラッグして、コレクタを有効にします。有効化または無効化によってコレクタが再起動することを示す確認ダイアログボックスが表示されます。

ステップ 3 [Yes] をクリックします。

ステップ 4 [保存 (save)] をクリックして変更を適用します。

データ収集を有効にしたら、コレクタサービスのメモリ使用率を設定できます。リソース割り当ての詳細については、「[Crosswork Data Gateway リソースの割り当て](#)」を参照してください。

Crosswork Data Gateway の収集ジョブの管理

収集ジョブは、Cisco Crosswork Data Gateway が実行する予定のタスクです。アプリケーションは、収集ジョブを介してデータ収集を要求します。次に、Cisco Crosswork はこれらの収集ジョブを Cisco Crosswork Data Gateway に割り当てて、要求に対応できるようにします。

Crosswork Data Gateway は、CLI、MDT、SNMP、gNMI (ダイヤルイン)、syslog、NETCONF などの複数のデータ収集プロトコルをサポートしています。サポートされているプロトコルのいずれかを介して転送可能である限り、Crosswork Data Gateway ではどのようなタイプのデータでも収集できます。

Cisco Crosswork には、次の 2 種類のデータ収集要求があります。

1. Cisco Crosswork 内の内部プロセスのデータを転送するためのデータ収集要求。Cisco Crosswork は、この目的のためにシステムジョブを作成します。システムジョブを作成または編集することはできません。
2. 外部データの送信先にデータを転送するためのデータ収集要求。外部データの送信先 (Kafka または gRPC) の構成の詳細については、[外部データ送信先の作成と管理 \(29 ページ\)](#) を参照してください。

KPI プロファイルの作成時に外部データ送信先を追加することにより、単一の収集要求で、収集されたデータを外部データ送信先と Cisco Crosswork Health Insights に転送できます。詳細については、『*Cisco Crosswork Change Automation and Health Insights 4.3 User Guide*』の「*Create a New KPI Profile*」の項を参照してください。



- (注)
1. Cisco Crosswork Data Gateway は、対応する（リスニング）収集ジョブの要求がない場合は着信トラフィックをドロップします。また、未承認デバイス（つまり、Cisco Crosswork Data Gateway に接続されていないデバイス）から受信したデータ、syslog イベント、および SNMP トラップもドロップします。
 2. ポーリングされたデータは、Cisco Crosswork Data Gateway がデータを処理して送信する準備ができるまでデバイスから要求できません。

[収集ジョブ (Collection Jobs)] ページから、Cisco Crosswork に登録されているすべての Crosswork Data Gateway インスタンスで現在アクティブな収集ジョブを表示できます。

Cisco Crosswork の UI の左側のナビゲーションバーで、[管理 (Administration)] > [収集ジョブ (Collection Jobs)] を選択します。

[収集ジョブ (Collection Jobs)] ページの左側のペインには、[一括ジョブ (Bulk Jobs)] と [パラメータ化されたジョブ (Parametrized Jobs)] の 2 つのタブがあります。[一括ジョブ (Bulk Jobs)] には、システムによって、またはこの UI および API から作成されたすべての収集ジョブが一覧表示されます。[パラメータ化されたジョブ (Parametrized Jobs)] ペインには、Cisco Crosswork Service Health アプリケーションによって作成されたすべてのアクティブなジョブが一覧表示されます。



- (注) [パラメータ化されたジョブ (Parametrized Jobs)] ペインにはデータがなく、Cisco Crosswork Service Health が展開されていない場合は空のままです。

詳細については、[収集ジョブのモニター \(89 ページ\)](#) を参照してください。

収集ジョブのタイプ

Cisco Crosswork の UI (CLI) から、または API を使用してデータを要求する収集ジョブの次のリストを作成できます。



- (注) SNMP OID ベースの収集ジョブは、Cisco Crosswork UI から、または API を使用して作成でき、SNMP トラップは API を使用して作成できます。

- [CLI 収集ジョブ \(47 ページ\)](#)
- [SNMP 収集ジョブ \(48 ページ\)](#)

- [MDT 収集ジョブ \(58 ページ\)](#)
- [Syslog 収集ジョブ \(59 ページ\)](#)
- [gNMI 収集ジョブ \(69 ページ\)](#)
- [NETCONF 収集ジョブ \(81 ページ\)](#)

作成した収集ジョブごとに、Cisco Crosswork Data Gateway は収集要求を実行し、収集したデータを優先データ送信先に転送します。

この章では、Cisco Crosswork の UI から収集ジョブを作成する方法について説明します。API を使用して収集ジョブを作成するには、『[Crosswork Data Gateway APIs on Cisco Devnet](#)』を参照してください。

Cisco Crosswork の UI のすべての収集ジョブの初期ステータスは [不明 (Unknown)] です。収集ジョブを受信すると、Cisco Crosswork Data Gateway は基本的な検証を実行します。収集ジョブが有効な場合、そのステータスは [成功 (Successful)] に変わります。それ以外の場合は [失敗 (Failed)] に変わります。

[パターン (Cadence)] の値は秒単位です。この値は、設定されたセンサーデータの収集頻度に応じて、10 - 2764800 秒 (最大 32 日間) の範囲で設定できます。



(注) パターンは 60 秒にすることをお勧めします。

前の実行がまだ進行中であるためにデバイスからの収集がスキップされると、Cisco Crosswork Data Gateway は警告ログを生成します。このシナリオではアラートは生成されません。

CLI 収集ジョブ

Cisco Crosswork Data Gateway は、ネットワークデバイスからの CLI ベースのデータ収集をサポートしています。このタイプの収集ジョブでは、次のコマンドがサポートされています。

- show と、短縮バージョンの sh
- traceroute
- dir

CLI 収集を適切に動作させるためには、デバイスにバナー設定を含めないでください。これをオフにする方法については、デバイスのマニュアルを参照してください。

CLI 収集ジョブは、Cisco Crosswork の UI からか、または API を使用して作成できます。詳細については、[Cisco DevNet](#) を参照してください。

次に、Kafka 外部接続先の CLI 収集ジョブのペイロードの例を示します。この例では、特に 2 つの値に注意してください。

1. デバイスは、IP アドレスではなく UUID で識別されます。

- 宛先も UUID によって参照されます。UI を使用して作成された収集ジョブの場合、Cisco Crosswork は UUID を検索します。独自の収集ジョブを作成するときは、これらの値を調べる必要があります。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APPL1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "CLI_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "658adb03-cc61-448d-972f-4fcec32cbfe8"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "cadence_in_millisec": "tel:60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "destination": {
          "destination_id": "1e71f2fb-ea65-4242-8efa-e33cec71b369",
          "context_id": "topic1"
        }
      }
    ]
  }
}
```

SNMP 収集ジョブ

Cisco Crosswork Data Gateway では、デバイスでサポートされている OID に基づく SNMP ベースのデータ収集をサポートしています。

SNMP コレクタは、設定プロファイル（収集する MIB オブジェクトのリストと取得先のデバイスのリスト）を取得するためのポーリング要求を Cisco Crosswork に行います。事前にパッケージ化された MIB モジュールのリストまたは MIB モジュールのカスタムリストを検索して、対応する OID を決定します。



- (注) Cisco Crosswork Data Gateway は、システムにすでに含まれている標準的な MIB のサードパーティ製デバイスで SNMP ポーリングを有効にします。独自の MIB は、収集要求が独自の MIB から MIB テーブル名またはスカラー名を参照する場合にのみ必要です。ただし、要求が OID ベースの場合、MIB は必要ありません。

OID が解決されると、SNMP コレクタへの入力として提供されます。

セクション [カスタムパッケージの追加 \(38 ページ\)](#) の説明に従って、Crosswork Data Gateway インスタンスにデバイスパッケージをインポートできます。

データポーリングとトラップでサポートされている SNMP バージョンは次のとおりです。

- ポーリングデータ
 - SNMP V2
 - SNMP V3 (no auth nopriv、auth no priv、authpriv)
 - サポートされている認証プロトコル : SHA-1、MD5
 - サポートされている priv プロトコル : AES-128、AES-192、AES-256、CiscoAES192、CiscoAES256、DES、および 3-DES。
- トラップ
 - SNMP V2
 - SNMP V3 (no auth nopriv、auth no priv、authpriv)

デバイスでの設定例 :

次の表に、さまざまな SNMP 機能を有効にするサンプルコマンドを示します。詳細については、プラットフォーム固有のドキュメントを参照してください。

表 3: デバイスで **SNMP** を有効にする設定例

バージョン	コマンド	目的
V2c	<pre>snmp-server group <group_name> v2c snmp-server user <user_name> <group_name> v2c</pre>	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。
	<pre>snmp-server host <host_ip> traps SNMP version <community_string> udp-port 1062 snmp-server host a.b.c.d traps version 2c v2test udp-port 1062</pre>	トラップデータの転送先を定義します。 (注) ここに記載されている IP アドレスは、Crosswork Data Gateway の仮想 IP アドレスである必要があります。
	<pre>snmp-server traps snmp linkup snmp-server traps snmp linkdown</pre>	リンクステータスを通知するトラップを有効にします。

バージョン	コマンド	目的
V3 (注) SNMPv3 ユーザーのパスワードは、8バイト以上にする必要があります。	<pre>snmp-server host <host_IP> traps version 3 priv <user_name> udp-port 1062</pre>	トラップデータの転送先を定義します。 (注) ここに記載されている IP アドレスは、Crosswork Data Gateway の仮想 IP アドレスである必要があります。
	<pre>snmp-server user <user_name> <group_name> v3 auth md5 <password> priv aes 128 <password></pre>	指定した名前付きアクセスリストのメンバに対して認証をイネーブルにするように SNMP サーバグループを設定します。
	<pre>snmp-server view <user_name> < MIB > included</pre>	何を報告する必要があるかを定義します。
	<pre>snmp-server group <group_name> v3 auth notify <user_name> read <user_name> write <user_name></pre>	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。
	<pre>snmp-server enable trap snmp [authentication] [linkup] [linkdown] [warmstart] [coldstart]</pre>	

バージョン	コマンド	目的
		<ul style="list-style-type: none"> オプションのキーワードを一切指定せずに使用した場合、authenticationFailure、linkUp、linkDown、warmStart、および coldStart の各トラップをイネーブルにします。 キーワード指定で使用した場合は、指定したタイプのトラップのみがイネーブルになります。たとえば、すべてのインターフェイスに対して linkUp と linkDown の SNMP トラップだけをグローバルにイネーブルにするには、このコマンドの snmpserver enable snmp linkup linkdown という形式を使用します。

SNMP コレクタは、次の操作をサポートしています。

- スカラー



(注) 1つの収集で複数のスカラー OID を要求する場合は、デバイスへの1つの `getbulkrequestquery` で複数の SNMP GET 要求をパックできます。

- TABLE
- WALK
- COLUMN

これらの操作は、センサー設定で定義されます（以下のペイロード例を参照）。



- (注) デバイスの応答時間が 1,500 ミリ秒を超える場合は、オプションの **deviceParams** 属性 **snmpRequestTimeoutMillis** (ペイロード例には表示されていない) を使用する必要があります。デバイスの応答時間が長いことが確実にない限り、**snmpRequestTimeoutMillis** を使用することは推奨されません。

snmpRequestTimeoutMillis の値はミリ秒単位で指定する必要があります。

デフォルトの最小値は 1,500 ミリ秒です。ただし、この属性の最大値に制限はありません。

次に、SNMP 収集ジョブの例を示します。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SNMP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c70fc034-0cbd-443f-ad3d-a30d4319f937",
            "8627c130-9127-4ed7-ace5-93d3b4321d5e",
            "c0067069-c8f6-4183-9e67-1f2e9bf56f58"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.1.3.0",
              "snmp_operation": "SCALAR"
            }
          }
        }
      },
      {
        "cadence_in_millisec": "60000"
      }
    ],
    {
      "sensor_data": {
        "snmp_sensor": {
          "snmp_mib": {
            "oid": "1.3.6.1.2.1.31.1.1",
            "snmp_operation": "TABLE"
          }
        }
      }
    },
    {
      "cadence_in_millisec": "60000"
    }
  ],
  "sensor_output_configs": [
    {
      "sensor_data": {
```

```

        "snmp_sensor": {
          "snmp_mib": {
            "oid": "1.3.6.1.2.1.1.3.0",
            "snmp_operation": "SCALAR"
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic1_461cb8aa-a16a-44b8-b79f-c3daf3ea925f"
        }
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.31.1.1",
              "snmp_operation": "TABLE"
            }
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic2_e7ed6300-fc8c-47ee-8445-70e543057f8a"
        }
      }
    ]
  }
}

```

SNMP トラップ収集ジョブ

SNMP トラップ収集ジョブは、API を介してのみ作成できます。トラップリスナーはポートでリスンし、（関心のあるトピックに基づいて）受信者にデータをディスパッチします。



重要 SNMP トラップ収集を開始する前に、Common EMS Services アプリケーションをインストールし、SNMP のホスト情報を構成します。

Crosswork Data Gateway は、UDP ポート 1062 でトラップをリスンします。



(注) SNMP トラップ収集ジョブを送信する前に、SNMP トラップをデバイス上で正しく設定して、Crosswork Data Gateway の仮想 IP アドレスに送信する必要があります。

SNMP トラップ収集ジョブのワークフロー

SNMP トラップを受信すると、Cisco Crosswork Data Gateway は以下を実行します。

1. デバイスに対して収集ジョブが作成されているかどうかを確認します。
2. トラップバージョンとコミュニティ文字列を確認します。



- (注) Crosswork Data Gateway が SNMP トラップのコミュニティ文字列をチェックしないようにするには、Crosswork UI を介してデバイスを追加するときに、[SNMP トラップ無効化チェック (SNMP Disable Trap Check)] チェックボックスをオンにします。このオプションの詳細については、[UI を使用したデバイスの追加](#)を参照してください。

3. SNMP v3 の場合は、ユーザー認証と priv プロトコルとクレデンシャルも検証します。



- (注) SNMPV3 auth-priv トラップは、デバイスまたはルータの engineId に依存して、ローカル USM ユーザーテーブルを維持します。したがって、デバイスまたはルータの engineId が変更されるたびに、トラップの受信が中断されます。トラップの受信を再開するには、それぞれのデバイスを取り外して取り付けてください。

Crosswork Data Gateway は、センサーパスに示されたトラップ OID に基づいてトラップをフィルタ処理し、要求されたトラップのみを送信します。

収集ジョブが無効か、デバイスに設定がないか、またはトラップが受信されない場合、ジョブのステータスは [不明 (Unknown)] のままです。サポートされているトラップと MIB のリストについては、「[SNMP での収集用に事前にロードしたトラップと MIB のリスト](#)」を参照してください。

Crosswork Data Gateway は、次の 3 つのタイプの非 YANG/OID ベースのトラップをサポートします。

表 4: サポートされている非 YANG/OID ベースのトラップのリスト

センサーパス	目的
*	フィルタなしでデバイスからプッシュされたすべてのトラップを取得します。
MIB レベルトラップ	1 つの MIB 通知の OID (例: すべての isis-mib レベルトラップを取得する場合は 1.3.6.1.2.1.138.0)
特定のトラップ	特定のトラップの OID (例: linkUp トラップを取得する場合は 1.3.6.1.6.3.1.1.5.4)

次に、SNMP トラップ収集ジョブの例を示します。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
```

```

    "lifetime_type": "APPLICATION_MANAGED",
    "collector_type": "TRAP_COLLECTOR"
  },
  "job_device_set": {
    "device_set": {
      "devices": {
        "device_ids": [
          "a9b8f43d-130b-4866-a26a-4d0f9e07562a",
          "8c4431a0-f21d-452d-95a8-84323a19e0d6",
          "eaab2647-2351-40ae-bf94-6e4a3d79af3a"
        ]
      }
    }
  },
  "sensor_input_configs": [
    {
      "sensor_data": {
        "trap_sensor": {
          "path": "1.3.6.1.6.3.1.1.4"
        }
      },
      "cadence_in_millisecc": "60000"
    }
  ],
  "sensor_output_configs": [
    {
      "sensor_data": {
        "trap_sensor": {
          "path": "1.3.6.1.6.3.1.1.4"
        }
      },
      "destination": {
        "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
        "context_id": "topic1_696600ae-80ee-4a02-96cb-3a01a2415324"
      }
    }
  ]
}

```

外部アプリケーションへのトラップ転送の有効化

デバイス上の Crosswork に必要なトラップのみを選択して有効にすることをお勧めします。

接続先で受信したデータのトラップタイプを識別するには、*oid* (OBJECT_IDENTIFIER。1.3.6.1.6.3.1.1.4.1.0 など) と *OidRecords* の *oid* に関連付けられている *strValue* を検索します (アプリケーションは対象の OID を照合してトラップの種類を特定できます)。

次に、トラップを外部アプリケーションに転送するための値とペイロードの例を示します。

- リンク アップ

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4

- Link Down

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3

- Syslog

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1

- Cold Start

```

1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1

{
  "nodeIdStr": "BF5-XRV9K1.tr3.es",
  "nodeIdUuid": "C9tZ5lJoSJKf5OZ67+U5JQ==",
  "collectionId": "133",
  "collectionStartTime": "1580931985267",
  "msgTimestamp": "1580931985267",
  "dataGpbkv": [
    {
      "timestamp": "1580931985267",
      "name": "trapsensor.path",
      "snmpTrap": {
        "version": "V2c",
        "pduType": "TRAP",
        "v2v3Data": {
          "agentAddress": "172.70.39.227",
          "oidRecords": [
            {
              "oid": "1.3.6.1.2.1.1.3.0",
              "strValue": "7 days, 2:15:17.02"
            },
            {
              "oid": "1.3.6.1.6.3.1.1.4.1.0", // This oid is the Object Identifier.
              "strValue": "1.3.6.1.6.3.1.1.5.3" // This is the value that determines the
kind of trap.
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.1.8",
              "strValue": "8"
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.2.8",
              "strValue": "GigabitEthernet0/0/0/2"
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.3.8",
              "strValue": "6"
            },
            {
              "oid": "1.3.6.1.4.1.9.9.276.1.1.2.1.3.8",
              "strValue": "down"
            }
          ]
        }
      }
    }
  ],
  "collectionEndTime": "1580931985267",
  "collectorUuid": "YmNjZjEzMTktZjFLOS00NTE5LWI4OTgtY2YlZmQxZDFjNWExO1RSQVBfQ09MTEVDVE9S",
  "status": {
    "status": "SUCCESS"
  },
  "modelData": {},
  "sensorData": {
    "trapSensor": {
      "path": "1.3.6.1.6.3.1.1.5.4"
    }
  },
  "applicationContexts": [
    {
      "applicationId": "APP1",
      "contextId": "collection-job-snmp-traps"
    }
  ]
}

```

```

    }
  ]
}

```

MDT 収集ジョブ

Crosswork Data Gateway は、モデル駆動型テレメトリ (MDT) を使用してネットワークデバイスからのデータ収集をサポートし、デバイスからのテレメトリストリームを直接消費します (IOS-XR ベースのプラットフォームのみ)。

Crosswork Data Gateway は、次のトランスポートモードのデータ収集をサポートしています。

- MDT TCP ダイアルアウトモード

Cisco Crosswork は NSO を利用して必要な MDT 設定をデバイスにプッシュし、対応する収集ジョブの設定を Crosswork Data Gateway に送信します。



- (注)
- バックアップ操作と復元操作の間に既存の MDT ジョブに何らかの変更 (更新) がある場合、Cisco Crosswork はデバイス上で設定更新のジョブを再生しません。これには NSO が関係するためです。NSO/デバイスの設定を復元する必要があります。Cisco Crosswork はデータベース内のジョブのみを復元します。
 - YANG モジュールを使用する前に、サポートされているかどうかを確認します。「[MDT での収集用に事前にロードした YANG モジュールのリスト](#)」の項を参照してください。

次に、MDT 収集のペイロードの例を示します。

```

{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "device_group": "mdt"
      }
    },
    "sensor_output_configs": [{
      "sensor_data": {
        "mdt_sensor": {
          "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"
        }
      },
      "destination": {
        "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
        "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
      }
    },
    {
      "sensor_data": {
        "mdt_sensor": {
          "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"
        }
      },
      "destination": {

```

```

    "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
    "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
  }
},
"sensor_input_configs": [{
  "sensor_data": {
    "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"
    }
  },
  "cadence_in_millise": "70000"
}, {
  "sensor_data": {
    "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"
    }
  },
  "cadence_in_millise": "70000"
}
],
"application_context": {
  "context_id": "c4",
  "application_id": "a4-mdt"
},
"collection_mode": {
  "lifetime_type": "APPLICATION_MANAGED",
  "collector_type": "MDT_COLLECTOR"
}
}
}

```

MDT 収集ジョブのワークフロー

MDT ベースの KPI がデバイスでアクティブ化されると、Cisco Crosswork

1. 構成要求を NSO に送信して、ターゲットデバイスでのデータ収集を有効にします。
2. Crosswork Data Gateway に収集ジョブ作成リクエストを送信します。
3. Crosswork Data Gateway は、収集したデータを指定した宛先に送信するためのディストリビューションを作成します。

Syslog 収集ジョブ

Crosswork Data Gateway は、デバイスからの Syslog ベースのイベント収集をサポートしています。



重要 Syslog トラップ収集を開始する前に、Common EMS Services アプリケーションをインストールし、Syslog のホスト情報を構成します。

サポートされている Syslog 形式は、次のとおりです。

- RFC5424 syslog 形式

- RFC3164 syslog 形式



(注) ネットワーク内の Crosswork Data Gateway から Syslog データを収集するには、デバイスを追加するときに YANG_CLI 機能を選択し、Crosswork Data Gateway から Syslog データを受信するように他のパラメータを設定します。プラットフォーム固有のマニュアルを参照してください。

構成手順の順序は重要ではありませんが、両方の手順を完了する必要があります。そうしないと、データが送信または収集されません。デバイスの設定例については、「[デバイスでの Syslog \(非セキュア\) の設定 \(64 ページ\)](#)」を参照してください。Cisco Crosswork では、デバイスへのセキュアな Syslog 通信を設定することもできます。詳細については、[デバイスでのセキュア Syslog の設定 \(65 ページ\)](#) を参照してください。

以下は、Syslog 収集ペイロードの例です。

```
{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c6f25a33-92e6-468a-ba0d-15490f1ce787"
          ]
        }
      }
    },
    "sensor_output_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
              "facilities": [0, 1, 3, 23,4],
              "severities": [0, 4, 5, 6, 7]
            }
          }
        },
        "destination": {
          "context_id": "syslogtopic",
          "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
        }
      }
    ],
    "sensor_input_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
              "facilities": [0,1, 3, 23,4],
              "severities": [0,4, 5, 6, 7]
            }
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "application_context": {
      "context_id": "demomilesstone2syslog",
      "application_id": "SyslogDemo2"
    }
  }
}
```



```

    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SYSLOG_COLLECTOR"
    }
  }
}
}

```

- Syslog データ収集の出力は、PRI ベースの SyslogSensor またはフィルタベースの SyslogSensor を指定することでフィルタ処理することができます。ペイロードに記載されている機能と重大度に一致する Syslog イベントが、指定された宛先に送信されます。一致しない他のすべての Syslog イベントはドロップされます。正規表現、重大度、または機能に基づいてフィルタを指定できます。
- 重大度と機能の値を指定した場合、両方の条件は、フィルタレベルで指定された論理演算子に基づいて結合されます。
- 論理演算子 AND または OR を使用して、最大 3 つのフィルタの組み合わせを指定できます。デフォルトでは、演算子を指定しない場合、AND 演算子が適用されます。

Syslog 収集ジョブの出力

Cisco Crosswork の UI からデバイスをオンボーディングする場合 ([デバイス管理 (Device Management)] > [ネットワークデバイス (Network Devices)] > [デバイスの詳細 (Device Details)])、[Syslog 形式 (Syslog Format)] フィールドで選択した値によって、デバイスから受信した syslog イベントを Syslog コレクタで解析する形式が設定されます。[不明 (UNKNOWN)]、[RFC5424]、または [RFC3164] のいずれかを選択できます。

次に、各オプションの出力例を示します。

1. [不明 (UNKNOWN)] : Syslog 収集ジョブの出力に、デバイスから受信した syslog イベントが含まれています。



- (注) デバイスは RFC5424/RFC3164 形式で syslog イベントを生成するように設定されていても [Syslog 形式 (Syslog Format)] フィールドに形式が指定されていない場合、デフォルトでは [不明 (UNKNOWN)] と見なされます。

サンプル出力 :

```

node_id_str: "xrv9k-VM8"
node_id_uuid: ":i\300\216>\366BM\262\270@\337\225\2723&"
collection_id: 1056
collection_start_time: 1616711596200
msg_timestamp: 1616711596201
data_gpbkv {
  timestamp: 1616711596201
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<6>1 Mar 25 15:34:41.321 PDT - SSHD_ 69570 - - 98949:
RP/0/RP0/CPU0:SSHD_[69570]: %SECURITY-SSHD-6-INFO SUCCESS : Successfully authenticated
user \'admin\' from \'40.40.40.116\' on \'vty0\'(cipher \'aes128-ctr\', mac
\'hmac-sha1\') \n"
  }
}

```

```

    fields {
      name: "DEVICE_IP"
      string_value: "40.40.40.30"
    }
  }
  collection_end_time: 1616711596200
  collector_uuid: "17328736-b726-4fe3-b922-231a4a30a54f:SYSLOG_COLLECTOR"
  status {
    status: SUCCESS
  }
  model_data {
  }
  sensor_data {
    syslog_sensor {
      pris {
        facilities: 0
        facilities: 3
        facilities: 4
        facilities: 23
        severities: 0
        severities: 5
        severities: 6
        severities: 7
      }
    }
  }
  application_contexts {
    application_id: "SyslogApp-xr-8-job1"
    context_id: "xr-8-job1"
  }
  version: "1"

```

2. [RFC5424] : デバイスが syslog イベントを RFC5424 形式で生成するように設定され、[Syslog 形式 (Syslog Format)] フィールドで [RFC5424] 形式が選択されている場合、Syslog 収集ジョブ収集の出力には、デバイスから受信した syslog イベント (RAW) とデバイスからの RFC5424 のベストエフォート解析済みの syslog イベントが含まれます。



- (注) Syslog コレクタは、次の Java RegEx パターンに従ってベストエフォートで syslog イベントを解析します。

RFC5424

```

"^(?<pri>\d+)>(?!<version>\d{1,3})\s*(?!<date>([0-9]{4})\s+)?[a-zA-Z]{3}\s+\d+\s+\d+:\d+:\d+\.\d{3}\s+[a-zA-Z]{3}
9T:Z-+))\s*(?!<host>\S+)\s*(?!<processname>\S+)\s*(?!<procid>\S+)\s*(?!<msgid>\S+)\s*(?!<structureddata>(-|\.|+|\\
<message>.+)$";

```

サンプル出力 :

```

.....
.....

```

```

collection_start_time: 1596307542398
msg_timestamp: 1596307542405
data_gpbkv {
  timestamp: 1596307542405
  name: "syslogsensor.path"
}

```

```

fields {
  name: "RAW"
  string_value: "<13>1 2020 Aug 1 12:03:32.461 UTC: iosxr254node config 65910 -
- 2782: RP/0/RSP0/CPU0:2020 Aug 1 12:03:32.461 UTC: config[65910]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin on vty0 (10.24.88.215) \n"
}
fields {
  name: "RFC5424"
  string_value: "pri=13, severity=5, facility=1, version=1,
date=2020-08-01T12:03:32.461, remoteAddress=/172.28.122.254, host='iosxr254node',
message='2782: RP/0/RSP0/CPU0:2020 Aug 1 12:03:32.461 UTC: config[65910]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin on vty0 (10.24.88.215) \',
messageId=null, processName=config, structuredDataList=null"
}
fields {
  name: "DEVICE_IP"
  string_value: "172.28.122.254"
}
}
collection_end_time: 1596307542404
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
...
...

```

3. [RFC3164] : デバイスが syslog イベントを RFC3164 形式で生成するように設定され、[Syslog 形式 (Syslog Format)] フィールドで [RFC3164] 形式が選択されている場合、Syslog ジョブ収集の出力には、RAW (デバイスから受信したもの) syslog イベントとデバイスかの RFC3164 のベストエフォート解析済みの syslog イベントの両方が含まれます。



- (注) Syslog コレクタは、次の Java RegEx パターンに従ってベストエフォートで syslog イベントを解析します。

RFC3164

```

"^(?<pri>\d+>[:]?\s*)?(?<date>\[a-zA-Z]{3}\s+\d+\s+[0-9]{4}\s+\d+:\d+:\d+\.\d{3}\s+)+[[a-zA-Z]{3}:]??\s
[a-zA-Z]{3}\s+\d+\s+\d+:\d+:\d+.\d{3}\s+)+[[a-zA-Z]{3}:]??)([0-9T.:Z-])\s+(?<host>\S+)\s+(?<tag>[^\s\
<procid>\d+\])?)"*\s*(?<message>.+)$";

```

サンプル出力 :

```

....
....
collection_id: 20
collection_start_time: 1596306752737
msg_timestamp: 1596306752743
data_gpbkv {
  timestamp: 1596306752743
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<14>2020 Aug 1 11:50:22.799 UTC: iosxr254node 2756:
RP/0/RSP0/CPU0:2020 Aug 1 11:50:22.799 UTC: config[65910]: %MGBL-CONFIG-6-DB_COMMIT
: Configuration committed by user 'admin'. Use 'show configuration commit changes
1000000580\' to view the changes. \n"

```

```

}
fields {
  name: "RFC3164"
  string_value: "pri=14, severity=6, facility=1, version=null,
date=2020-08-01T11:50:22.799, remoteAddress=/172.28.122.254, host='\iosxr254node\',
message='\RP/0/RSP0/CPU0:2020 Aug 1 11:50:22.799 UTC: config[65910]:
%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user \'admin\'. Use \'show
configuration commit changes 1000000580\' to view the changes. \', tag=2756"
}
fields {
  name: "DEVICE_IP"
  string_value: "172.28.122.254"
}
}
collection_end_time: 1596306752742
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
....
....

```

Syslog コレクタが [Syslog 形式 (Syslog Format)] フィールドで指定された形式に従って syslog イベントを解析できない場合、Syslog 収集ジョブの出力には、デバイスから受信した syslog イベント (RAW) が含まれます。

デバイスでの Syslog (非セキュア) の設定

この項では、デバイスで RFC3164 形式または RFC5424 形式の syslog を設定するための設定例を示します。

RFC3164 Syslog 形式の設定



(注) 次のコードで強調表示されている設定は、解析された出力でのフォーマットの問題を回避するために必要です。

Cisco IOS XR デバイスの場合 :

```

logging <CDG IP> port 9514 OR logging <CDG IP> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>

```

Cisco IOS XE デバイスの場合 :

```

no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host <CDG IP> transport tcp port 9898 session-id string <sessionidstring> -->
To use TCP channel
OR
logging host <CDG IP> transport udp port 9514 session-id string <sessionidstring> ---->
To use UDP channel
OR
logging host <CDG IP> vrf Mgmt-intf transport udp port 9514 session-id string

```

```
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
```

RFC5424 Syslog 形式の設定

Cisco IOS XR デバイスの場合：

```
logging <CDG IP> port 9514 OR logging <server 1> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>
logging format rfc5424
```

Cisco IOS XE デバイスの場合：

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host <CDG IP> transport tcp port 9898 session-id string <sessionidstring> -->
To use TCP channel
OR
logging host <CDG IP> transport udp port 9514 session-id string <sessionidstring> --->
To use UDP channel
OR
logging host <CDG IP> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
logging trap syslog-format 5424 --> if applicable
```




デバイスでのセキュア Syslog の設定

デバイスへのセキュアな syslog 通信を確立するには、次の手順を実行します。

1. Cisco Crosswork の [証明書管理 UI (Certificate Management)] ページから Cisco Crosswork 信頼チェーンをダウンロードします。
2. Cisco Crosswork 信頼チェーンを使用してデバイスを設定します。

Syslog 証明書のダウンロード

1. Cisco Crosswork の UI で、[管理 (Administration)] > [証明書管理 (Certificate Management)] に移動します。
2. 「**crosswork-device-syslog**」行で [i] をクリックします。
3. [すべてエクスポート (Export All)] をクリックして、証明書をダウンロードします。
次のファイルがシステムにダウンロードされます。

Name
 intermediate.key
 intermediate.crt
 ca.crt

デバイスでの Cisco Crosswork トラストポイントの設定

TLS を有効にする XR デバイスの設定例

```
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-root
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k(config-trustp)#end
RP/0/RSP0/CPU0:ASR9k#
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-root
Fri Jan 22 11:07:41.880 GMT
```

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIGKzCCBB0gAwIBAgIRAKfyU89yjmrXVDRKBWuSGPgWdQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.....
jPQ/Uro8N3sC1gGJX7CIh5cE+KIJ51ep8i1eKSJ5WHWRTmv342MnG2StgOTtaFF
vrkWHd02o6jRuYXDWEUptDog8oEritZb+SNPXWUc/2mbYog6ks6EeMC69VjkzP0=
-----END CERTIFICATE-----
```

```
Read 1583 bytes as CA certificate
Serial Number : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
Subject:
          CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Issued By :
          CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:09 UTC Sat Jan 16 2021
Validity End   : 02:37:09 UTC Thu Jan 15 2026
SHA1 Fingerprint:
          209B3815271C22ADF78CB906F6A32DD9D97BBDBA
```

Fingerprint: 2FF85849EBAAB9B059ACB9F5363D5C9CDo you accept this certificate? [yes/no]:
yes

```
RP/0/RSP0/CPU0:ASR9k#config
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-inter
Fri Jan 22 11:10:30.090 GMT
```

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIGFDCCA/ygAwIBAgIRAKhqHQXcJzQzeQK6U2wn8PIwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.....
5lBk617z6cxFER5c+/PmJFhcreisTxXg1aJbFdnB5C8f+0uUIIdLghykQ/zaZGuBn
AAB70c9r9OeKJWzvv1e2U8HH1pdQ/nd
-----END CERTIFICATE-----
```

```
Read 1560 bytes as CA certificate
Serial Number : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
Subject:
          CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
```

```

Issued By      :
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:11 UTC Sat Jan 16 2021
Validity End   : 02:37:11 UTC Mon Jan 16 2023
SHA1 Fingerprint:
                B06F2BFDE95413A8D08A01EE3511BC3D42F01E59

```

```

CA Certificate validated using issuer certificate.
RP/0/RSP0/CPU0:ASR9k#show crypto ca certificates
Fri Jan 22 15:45:17.196 GMT

```

```

Trustpoint     : syslog-root
=====
CA certificate
Serial Number  : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
Subject:
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Issued By      :
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:09 UTC Sat Jan 16 2021
Validity End   : 02:37:09 UTC Thu Jan 15 2026
SHA1 Fingerprint:
                209B3815271C22ADF78CB906F6A32DD9D97BBDBA

```

```

Trustpoint     : syslog-inter
=====
CA certificate
Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
Subject:
                CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Issued By      :
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:11 UTC Sat Jan 16 2021
Validity End   : 02:37:11 UTC Mon Jan 16 2023
SHA1 Fingerprint:
                B06F2BFDE95413A8D08A01EE3511BC3D42F01E59
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname 10.13.0.159
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#severity debugging
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#vrf default
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#commit
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#exit
RP/0/RSP0/CPU0:ASR9k(config)#exit
RP/0/RSP0/CPU0:ASR9k#exit
RP/0/RSP0/CPU0:ASR9k#show running-config logging
Fri Jan 22 11:17:19.385 GMT
logging tls-server syslog-tb131
vrf default
severity debugging
trustpoint syslog-inter
tls-hostname <CDG Southbound IP>
!
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

RP/0/RSP0/CPU0:ASR9k#

```

TLS を有効にする XE デバイスの設定例

```

csr8kv(config)#crypto pki trustpoint syslog-root
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation stop
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-root

```

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```

-----BEGIN CERTIFICATE-----
MIIFPjCCAyYCCQC06pK5AOGYdjANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExETAPBgNVBACMCe1pbHBpdGFzMQ4wDAYDVQQKDAVDaXNj
.....
JbimOpXAncoBLol14DXOJLvMVRjn1EULE9AXXCnfnrnBx7jL4CV+qHgEtF6oqclFW
JEA=
-----END CERTIFICATE-----

```

Certificate has the following attributes:

```

    Fingerprint MD5: D88D6D8F E53750D4 B36EB498 0A435DA1
    Fingerprint SHA1: 649DE822 1C222C1F 5101BEB8 B29CDF12 5CEE463B

```

```

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

```

```

csr8kv(config)#crypto pki trustpoint syslog-intermediate
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation continue syslog-root
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-intermediate

```

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```

-----BEGIN CERTIFICATE-----
MIIFfTCCA2WgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMakGA1UEBhMCVVMx
EzARBgNVBAGMCkNhG1mb3JuaWEwDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQQLDAVt
.....
Nmz6NQynD7bxqQa9Xq9kyPuY3ZVKXkf3l2IRH0MEy2yFX/tAen9JqOeZlg8canmw
TxSWA5TLzylRmxqQh88f0CM=
-----END CERTIFICATE-----

```

Trustpoint 'syslog-intermediate' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required

Certificate has the following attributes:

```

    Fingerprint MD5: FE27BDBE 9265208A 681670AC F59A2BF1
    Fingerprint SHA1: 03F513BD 4BEB689F A4F4E001 57EC210E 88C7BD19

```

```

csr8kv(config)#logging host <CDG Southbound IP> transport tls port 6514
csr8kv(config)#logging trap informational syslog-format rfc5424
csr8kv(config)#logging facility user
csr8kv(config)#service timestamps log datetime msec year show-timezone

```

```

csr8kv(config)#logging tls-profile tlsv12

```

FQDN をサポートするための Syslog 構成

サンプルのデバイス構成に加えて次のコマンドを実行して、TLSがFQDNをサポートできるようになります。

1. ドメイン名を設定し、DNS IP をデバイスで設定する必要があります。

```
RP/0/RSP0/CPU0:ASR9k#config
RP/0/RSP0/CPU0:ASR9k(config)#domain name <DNS domain name>
RP/0/RSP0/CPU0:ASR9k(config)#domain name-server <DNS server IP>
```

2. tls-hostname の CDG VIP FQDN を構成する

```
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname <CDG VIP FQDN>
```

gNMI 収集ジョブ

Cisco Crosswork は、Cisco Crosswork Data Gateway を介した gRPC ネットワーク管理インターフェイス (gNMI) ベースのテレメトリデータの収集をサポートしています。サブスクリプションに基づく gNMI ダイアルイン (gRPC ダイアルイン) ストリーミングのテレメトリデータと、要求した接続先への後続のサブスクリプション応答 (通知) のリレーのみをサポートします。



- (注) モデルがターゲットのデバイスプラットフォームでサポートされている限り、gNMI 収集はサポートされます。gNMI 収集ジョブを送信するには、デバイスで gNMI を設定しておく必要があります。プラットフォーム固有のマニュアルを確認します。

デバイスで gNMI を設定するには、「[デバイスの設定例：gNMI \(76 ページ\)](#)」を参照してください。

gNMI では、セキュアモードと非セキュアモードの両方をデバイスで共存させることができます。Cisco Crosswork は、インベントリで渡された情報に基づいて、非セキュアモードよりもセキュアモードを優先します。

デバイスがリロードされると、gNMI コレクタは既存のサブスクリプションがデバイスに再サブスクライブされるようにします。

gNMI 仕様には、メッセージの終わりをマークする方法がありません。したがって、接続先とディスパッチのパターンは gNMI コレクタではサポートされません。

Cisco Crosswork Data Gateway は、gNMI の次のタイプのサブスクライブオプションをサポートしています。

表 5: gNMI のサブスクリプションオプション

タイプ	サブタイプ	説明
[1 回 (Once)]		指定したすべてのパスについて、システム設定の現在のスナップショットを 1 回だけ収集して送信します。

タイプ	サブタイプ	説明
Stream	SAMPLE	パターンベースの収集。
	ON_CHANGE	最初の応答には、サブスクライブしているパスのすべての要素の状態が含まれ、その後、変更リーフ値に対する後続の更新が含まれています。
	TARGET_DEFINED	ルータ/デバイスは、サブスクライブしているパス（つまり、SAMPLE または ON_CHANGE のいずれか）に基づいてリーフ単位でサブスクリプションのモードを選択します。

Crosswork Data Gateway は、デバイスへの単一のサブスクリプションリストで複数のサブスクリプションパスをサブスクライブする機能をサポートしています。たとえば、ON_CHANGE とサブスクリプションモードの ONCE 収集ジョブの組み合わせを指定できます。ON_CHANGE モードは、指定したパスの特定の要素の変更時にのみデータを収集します。一方、サブスクリプションモードの ONCE は、指定したパスの現在のシステムデータを 1 回だけ収集して送信します。



- (注)
- Crosswork Data Gateway は、1 つ以上のモードのサポートの宣言をデバイスに依存します。
 - デフォルト値の gNMI センサーパスはペイロードに表示されません。これは既知の protobuf の動作です。

boolean の場合、デフォルト値は false です。enum の場合は、gnmi.proto が指定されます。

例 1 :

```
message GNMIDeviceSetting {
  bool suppress_redundant = 1;
  bool allow_aggregation = 4;
  bool updates_only = 6;
}
```

例 2 :

```
enum SubscriptionMode {
  TARGET_DEFINED = 0; //default value will not be printed
  ON_CHANGE = 1;
  SAMPLE = 2;
}
```

次に、gNMI 収集ペイロードのサンプルを示します。このサンプルでは、デバイスグループ「milpitas」の 2 つの集まりが表示されます。最初は、60 秒ごとに「mode」=「SAMPLE」を使

用してインターフェイス統計情報を収集します。2番目のジョブは、インターフェイスの状態（アップ/ダウン）の変更をキャプチャします。これが検出されると、単に「mode="STREAM"」がコレクタに送信されます。

```
{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "device_group": "milpitas"
      }
    },
    "sensor_output_configs": [{
      "sensor_data": {
        "gnmi_standard_sensor": {
          "Subscribe_request": {
            "subscribe": {
              "subscription": [{
                "path": {
                  "origin": "openconfig-interfaces",
                  "elem": [{
                    "name": "interfaces/interface/state/ifindex"
                  }]
                },
                "mode": "SAMPLE",
                "sample_interval": 1000000000
              }, {
                "path": {
                  "origin": "openconfig-interfaces",
                  "elem": [{
                    "name":
"interfaces/interfaces/state/counters/out-octets"
                  }]
                },
                "mode": "ON_CHANGE",
                "sample_interval": 1000000000
              }
            ],
            "mode": "STREAM",
            "encoding": "JSON"
          }
        }
      }
    },
    "destination": {
      "context_id": "hukarz",
      "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
    }
  }],
  "sensor_input_configs": [{
    "sensor_data": {
      "gnmi_standard_sensor": {
        "Subscribe_request": {
          "subscribe": {
            "subscription": [{
              "path": {
                "origin": "openconfig-interfaces",
                "elem": [{
                  "name": "interfaces/interface/state/ifindex"
                }]
              },
              "mode": "SAMPLE",
              "sample_interval": 1000000000
            }, {
              "path": {
```


デバイス証明書の生成

この項では、OpenSSL を使用して証明書を作成する方法について説明します。

証明書を生成する手順は、Open SSL と Microsoft で検証済みです。この手順では、Open SSL を使用してデバイス証明書を生成する手順について説明しました。



- (注) Open SSL または Microsoft 以外のユーティリティを使用してデバイス証明書を生成するには、シスコサポートチームにお問い合わせください。

1. rootCA の作成

```
# openssl genrsa -out rootCA.key
# openssl req -subj /C=/ST=/L=/O=/CN=CrossworkCA -x509 -new -nodes -key rootCA.key
-sha256 -out rootCA.pem -days 1024
```

上記のコマンドでは、days 属性によって証明書の有効期間が決まります。最小値は 30 日です。つまり、30 日ごとに証明書を更新する必要があります。値を 365 日に設定することをお勧めします。

2. デバイスキーと証明書の作成

```
# openssl genrsa -out device.key
# openssl req -subj /C=/ST=/L=/O=/CN=Crosswork -new -key device.key -out device.csr
# openssl x509 -req -extfile <(printf "subjectAltName=IP.0: 10.58.56.18") -in
device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -sha256 -out device3.crt
-days 1024
```

複数のデバイスがある場合、複数のデバイス証明書を作成する代わりに、subjectAltName に複数のデバイス IP アドレスをカンマで区切って指定できます。

```
# openssl x509 -req -extfile <(printf "subjectAltName=IP.0: 10.58.56.18, IP.1:
10.58.56.19, IP.2: 10.58.56.20 ..... ") -in device.csr -CA rootCA.pem -CAkey rootCA.key
-CAcreateserial -sha256 -out device.crt -days 1024
```

gNMI 証明書の設定

Crosswork Data Gateway は gNMI クライアントとして機能し、デバイスは gNMI サーバーとして機能します。Crosswork Data Gateway は、信頼チェーンを使用してデバイスを検証します。すべてのデバイスにグローバルな信頼チェーンがあることが期待されます。信頼チェーンが複数ある場合は、すべてのデバイス信頼チェーン（単一または複数のベンダー）を 1 つの .pem ファイルに追加し、この .pem ファイルを Crosswork 証明書管理の UI にアップロードします。



- (注) Crosswork にアップロードできる gNMI 証明書は 1 つのみです。

gNMI 証明書を設定するには、次の手順を実行します。

ステップ 1 Cisco Crosswork の UI から、[管理 (Administration)] > [証明書管理 (Certificate Management)] に移動します。

ステップ2 [+] アイコンをクリックして証明書を追加します。

ステップ3 [証明書の追加 (Add Certificate)] ウィンドウで、次の詳細情報を入力します。

- [デバイス証明書名 (Device Certificate Name)] : 証明書の名前を入力します。
- [証明書のロール (Certificate Role)] : ドロップダウンリストから [デバイス gNMI 通信 (Device gNMI Communication)] を選択します。
- [デバイス信頼チェーン (Device Trust Chain)] : rootCA ファイルの場所までローカルファイルシステムを参照し、そのファイルをアップロードします。

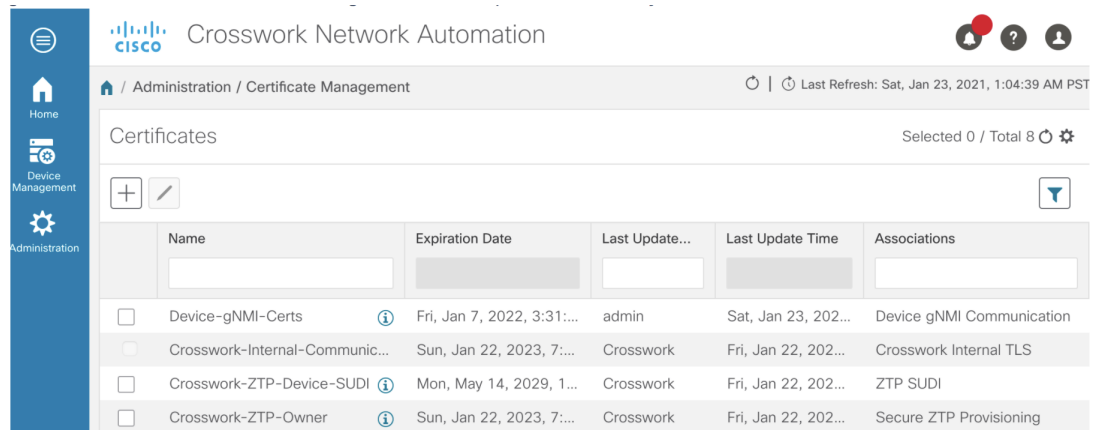
図 24: 証明書の追加 (Add Certificate) ウィンドウ

(注) gNMI 証明書がすでに設定されている場合で、別の信頼チェーンを使用してデバイスをオンボーディングするときは、既存の .pem ファイルを更新して新しい CA の詳細を含めます。リストから既存の gNMI 証明書を選択し、[編集 (Edit)] アイコンをクリックして、新しい .pem ファイルをアップロードします。

ステップ4 [保存 (Save)] をクリックします。

gNMI 証明書が正常に追加されると、設定済みの証明書のリストに表示されます。

図 25: [証明書 (Certificate)] ウィンドウ



Cisco Crosswork からのデバイスのプロトコルの更新

Cisco Crosswork で gNMI 証明書を設定したら、Cisco Crosswork の UI ([デバイス管理 (Device Management)] > [ネットワークデバイス (Network Devices)]) から、または .csv ファイルでプロトコルの詳細を **GNMI_SECURE** ポートとして指定して、デバイスをセキュアなプロトコルの詳細を使用して更新します。

次の図に、デバイスの更新されたセキュアプロトコルの詳細を示します。

図 26: [デバイスの詳細の編集 (Edit Device Details)] ウィンドウ

Edit Device Details

General

Configured State* DOWN

Reachability Check* ENABLE

Credential Profile* xrvr

Host Name xrvr2

Inventory ID

Data Gateway None

Software Type IOS XR

Software Version 6.6.2

UUID 3166bf90-bbbd-4d19-933e-817caacfa1

Serial Number

Mac Address

Capability* SNMP, YANG_CLI

Tags

Product Type CISCO-XRv9000

Syslog Format UNKNOWN

Connectivity Details

Protocol *	IP Address / Subnet Mask *	Port *	Timeout	Encoding Type *
SSH	10.11.0.11 / 16	22	30	
SNMP	10.11.0.11 / 16	161	30	
GNMI_SECURE	10.11.0.11 / 16	57400	1500	PROTO

+ Add Another

Routing Info

Save Cancel

デバイスの設定例：gNMI

Cisco IOS XR デバイス

1. HTTP/2 接続で gRPC を有効にします。

```
Router#configure
Router(config)#grpc
Router(config-grpc)#port <port-number>
```

ポート番号の範囲は 57344 ~ 57999 です。ポート番号が使用できない場合は、エラーが表示されます。

2. セッションパラメータを設定します。

```
Router(config)#grpc{ address-family | dscp | max-request-per-user | max-request-total
| max-streams |
max-streams-per-user | no-tls | service-layer | tls-cipher | tls-mutual |
tls-trustpoint | vrf }
```

値は次のとおりです。

- address-family: アドレスファミリ識別子タイプを設定します
 - dscp: 送信された gRPC で QoS マーキング DSCP を設定します
 - max-request-per-user: ユーザーあたりの同時要求の最大数を設定します
 - max-request-total: 合計同時要求の最大数を設定します
 - max-streams: 同時 gRPC 要求の最大数を設定します。サブスクリプションの上限は 128 要求です。デフォルトは 32 要求です
 - max-streams-per-user: ユーザーあたりの同時 gRPC 要求の最大数を設定します。サブスクリプションの上限は 128 要求です。デフォルトは 32 要求です
 - no-tls: トランスポートレイヤセキュリティ (TLS) を無効化します。TLS はデフォルトで有効になっています。
 - service-layer: gRPC サービスレイヤの設定を有効にします
 - tls-cipher: gRPC TLS 暗号スイートを有効にします
 - tls-mutual: 相互認証を設定します
 - tls-trustpoint: トラストポイントを設定します
 - vrf: サーバー VRF を有効にします
3. TPA (サードパーティ製アプリケーションのトラフィック保護) を有効にします。

```
tpa
vrf default
address-family ipv4
default-route mgmt
update-source dataports MgmtEth0/RP0/CPU0/0
```

Cisco IOS XE デバイス

次に、gNMI サーバを非セキュア モードで有効にする例を示します。

```
Device# configure terminal
Device(config)# gnmi-yang
Device(config)# gnmi-yang server
Device(config)# gnmi-yang port 50000 <The default port is 50052.>
Device(config)# end
Device
```

次に、gNMI サーバをセキュア モードで有効にする例を示します。

証明書とトラストポイントは、セキュア gNMI サーバにのみ必要です。

```
Device# configure terminal
Device(config)# gnmi-yang server
Device(config)# gnmi-yang secure-server
Device(config)# gnmi-yang secure-trustpoint trustpoint1
Device(config)# gnmi-yang secure-client-auth
Device(config)# gnmi-yang secure-port 50001 <The default port is 50051.>
Device(config)# end
Device
```

デバイスの証明書

証明書とトラストポイントは、セキュア gNMI サーバにのみ必要です。

Linux での OpenSSL を使用した証明書の作成

次に、Linux マシン上で OpenSSL を使用して証明書を作成する例を示します。

```
# Setting up a CA
openssl genrsa -out rootCA.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=rootCA -x509 -new -nodes -key rootCA.key -sha256 -out
rootCA.pem

# Setting up device cert and key
openssl genrsa -out device.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=<hostnameFQDN> -new -key device.key -out device.csr
openssl x509 -req -in device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
device.crt -sha256
# Encrypt device key - needed for input to IOS
openssl rsa -des3 -in device.key -out device.des3.key -passout pass:<password - remember
this for later>

# Setting up client cert and key
openssl genrsa -out client.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=gnmi_client -new -key client.key -out client.csr
openssl x509 -req -in client.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
client.crt -sha256
```

Cisco IOS XR デバイスへの証明書のインストール

Cisco IOS XR に証明書をインストールするには、次のパスのファイルを置き換えます。

1. XR マシンにログインします。
2. 端末プロンプトで run コマンドを入力します。

```
RP/0/RP0/CPU0:xrvr-7.2.1#run
```
3. 次のディレクトリに移動します。

```
cd /misc/config/grpc
```
4. 次のファイルの内容を置き換えます。

- `ems.pem` の内容を `device.crt` に置き換えます。
- `ems.key` の内容を `device.key` に置き換えます。
- `ca.cert` の内容を `rootCA.pem` に置き換えます。

Cisco IOS XE デバイスへの証明書のインストール

次に、Cisco IOS XE デバイスに証明書をインストールする例を示します。

```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

# Receive:
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of rootCA.pem, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.

# Send:
# Contents of device.des3.key, followed by newline + 'quit' + newline:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20
<snip>
-----END RSA PRIVATE KEY-----
quit

# Receive:
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of device.crt, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% PEM files import succeeded.
Device(config)#

# Send:
Device(config)# crypto pki trustpoint trustpoint1
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device#
```

gNMI バンドルの構成

IOS XR では、SubscribeResponse メッセージの通知メッセージに含まれるいくつかの更新メッセージを結合するために、gNMI バンドルが実装されています。これらのメッセージは、IOS XR デバイスに送信されます。更新メッセージをバンドルするには、IOS XR デバイスでバンドルを有効にし、メッセージのサイズを指定する必要があります。

始める前に

次の点に注意してください。

- IOS XR リリースバージョン 7.8.1 以降では、gNMI バンドル機能がサポートされています。バンドル機能の動作の詳細については、『[Programmability Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.8.x](#)』を参照してください。
- gNMI バンドル機能は、デバイスからのみ構成できます。このオプションは、Crosswork インターフェイスでは使用できません。

ステップ 1 次のコマンドを使用して、バンドル機能を有効にします。

```
telemetry model-driven
  gnmi
  bundling
```

gNMI バンドル機能は、デフォルトで無効になっています。

ステップ 2 次のコマンドを使用して、gNMI バンドルサイズを指定します。

```
telemetry model-driven
  gnmi
  bundling
    size <1024-65536>
```

デフォルトのバンドルサイズは、32768 バイトです。

重要 (N-1) インスタンスを処理した後で、メッセージサイズがバンドルサイズよりも小さい場合、もう 1 つのインスタンスが許可される可能性があり、結果としてバンドルサイズを超えます。

次のタスク

次を使用して、バンドル機能が構成されていることを確認します。

```
RP/0/RP0/CPU0:R0(config)#telemetry model-driven
RP/0/RP0/CPU0:R0(config-model-driven)#gnmi ?
  bundling  gNMI bundling of telemetry updates
  heartbeat gNMI heartbeat
  <cr>
RP/0/RP0/CPU0:R0(config-model-driven)#gnmi bundling ?
  size  gNMI bundling size (default: 32768)
  <cr>
RP/0/RP0/CPU0:R0(config-model-driven)#gnmi bundling
RP/0/RP0/CPU0:R0(config-gnmi-bdl)#size ?
  <1024-65536>  gNMI bundling size (bytes)
```

デバイスへの証明書のインポート

Cisco IOS XR デバイスへの証明書のインストール

Cisco IOS XR デバイスに証明書をインストールするには、次の手順を実行します。

1. rootCA.pem、device.key、および device.crt を /tmp フォルダの下のデバイスにコピーします。
2. IOS XR デバイスにログインします。
3. run コマンドを使用して VM シェルを開始します。

```
RP/0/RP0/CPU0:xrvr-7.2.1#run
```

4. 次のディレクトリに移動します。

```
cd /misc/config/grpc
```

5. 次のファイルの内容を作成または置換します。



(注) デバイスで TLS が以前に有効になっていた場合は、次のファイルがすでに存在します。その場合、以下で説明するようにこれらのファイルの内容を置き換えます。初めて行う場合は、デバイスで TLS を有効にし、/tmp フォルダからこのフォルダにファイルをコピーします。

- ems.pem with device.crt
- ems.key with device.key
- ca.cert with rootCA.pem

6. 変更を有効にするには、デバイスで TLS を再起動します。これを行うには、「no-tls」コマンドを使用して TLS を無効にし、デバイスで「no no-tls」設定コマンドを使用して再度有効にします。

Cisco IOS XE デバイスへの証明書のインストール

次に、Cisco IOS XE デバイスに証明書をインストールする例を示します。

```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

# Receive:
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of rootCA.pem, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
```

```

# Send:
# Contents of device.des3.key, followed by newline + 'quit' + newline:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20
<snip>
-----END RSA PRIVATE KEY-----
quit

# Receive:
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of device.crt, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% PEM files import succeeded.
Device(config)#

# Send:
Device(config)# crypto pki trustpoint trustpoint1
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device#

```

NETCONF 収集ジョブ

Crosswork Data Gateway は、ネットワークデバイスからのネットワーク設定プロトコル (NETCONF) ベースのデータ収集をサポートしています。

NETCONF 収集の場合、Crosswork Data Gateway は、CLI 収集ジョブ用にロードされる次のデバイスパッケージを利用します。

- システムデバイスパッケージ : Crosswork Data Gateway の起動後にダウンロードされるシステムデバイスパッケージ。
- カスタムデバイスパッケージ : UI または API からアップロードされたカスタムデバイスパッケージ。

NETCONF コレクタは、次の 2 つのタイプのデータ収集をサポートしています。

- プルベースの収集
パターンベースの収集とオンデマンド収集をサポートします。



(注) NETCONF コマンドベースの収集はサポートされていません。

- イベントベースの収集

<https://tools.ietf.org/html/rfc5277> のドキュメントに記載されている NETCONF イベント通知をサポートしています。オンデマンド収集はこのタイプの収集ではサポートされておらず、これらの収集ジョブに指定されたパターンは無視されます。

NETCONF 収集ジョブのワークフロー

1. NETCONF 収集ジョブが収集サービス (Helios/Magellan) に送信され要求された収集のパターンまたは数、あるいはイベント通知 RPC を指定します。
2. 収集サービス (Helios / Magellan) は、収集ジョブを Crosswork Data Gateway の NETCONF コレクタに送信します。
3. 収集のタイプ (イベントベースの収集かプルベースの収集か) に応じて、NETCONF コレクタはデバイスから収集を開始します。
4. 収集されたデータは、指定されたデータ送信先 (gRPC/Kafka) に転送されます。

サンプル ペイロード :

```
{
  "createUpdateJob": {
    "jobId": {
      "deviceId": "6fa90381-95f3-4a95-ac32-37754e002225",
      "sensorPath": {
        "netconfSensor": {
          "devicePackage": {
            "devicePackageName": "optical_inventory_svo_mne",
            "functionName": "getRawNodeInfo"
          }
        }
      }
    },
    "collectionType": "PERSISTENT_COLLECTION_TYPE"
  },
  "collectionType": "PERSISTENT_COLLECTION_TYPE",
  "deviceId": "6fa90381-95f3-4a95-ac32-37754e002225",
  "sensorConfig": {
    "sensorPath": {
      "netconfSensor": {
        "devicePackage": {
          "devicePackageName": "optical_inventory_svo_mne",
          "functionName": "getRawNodeInfo"
        }
      }
    }
  },
  "cadenceInMillisec": "60000"
},
"destinationSensorConfigs": [
  {
    "jobDestinationId": {
      "destinationId": "6dbc2a4c-e827-438f-9bab-bbeb508c06e2",
      "destinationContextId": "NativeNetconfTopic"
    },
    "destinationId": "6dbc2a4c-e827-438f-9bab-bbeb508c06e2",
    "destinationContextId": "NativeNetconfTopic",
    "sensorConfigHandler": {
      "action": "NORMAL"
    }
  },
  "applicationContext": [
    {
      "applicationId": "EPNM-APP",
```

```

        "contextId": "Native-Netconf"
      }
    ]
  }
}

```

NETCONF コレクタの問題のトラブルシューティング

NETCONF コレクタが継続的に再起動する

次のコマンドを実行して、NETCONF コレクタの docker ログを確認します。

```
docker logs netconf-collector
```

[jarが無効または破損している (invalid or corrupt jar)]というメッセージが表示された場合は、コンテナ用にダウンロードされた Docker イメージが破損していることを意味します。

問題を軽減するための回避策として、次の手順に従います。

1. Crosswork Data Gateway VM にログインします。
2. インタラクティブコンソールから [5 トラブルシューティング (5 Troubleshooting)] を選択します。
3. [3 すべての非インフラコンテナを削除してVMを再起動する (3 Remove all Non-Infra Containers and Reboot VM)] を選択します。

この手順により、インストール後にダウンロードされたコンテナ (コレクタとオフロード) が削除され (Crosswork インフラストラクチャ コンテナを除く)、Docker からイメージが削除され、コレクタデータと構成が削除され、VM が再起動され、VM は、インフラストラクチャ コンテナのみが実行されている初期構成が完了した後の状態に戻ります。

Crosswork Data Gateway の再起動後、コンテナは Cisco Infrastructure から再度ダウンロードされます。

Cisco Crosswork UI からの収集ジョブの作成

収集ジョブを作成するには、次の手順を実行します。



- (注) Cisco Crosswork の UI ページを使用して作成した収集ジョブは、1 回のみパブリッシュできます。

始める前に

収集したデータを保存するためのデータ送信先が作成されている (アクティブになっている) ことを確認します。また、データを収集する予定のセンサーパスと MIB の詳細を確認します。

ステップ 1 メインメニューから、[管理 (Administration)]>[収集ジョブ (Collection Jobs)]>[一括ジョブ (Bulk Jobs)] に移動します。

ステップ 2 左側のペインで **+** ボタンをクリックします。

ステップ 3 [ジョブの詳細 (Job details)] ページで、次のフィールドに値を入力します。

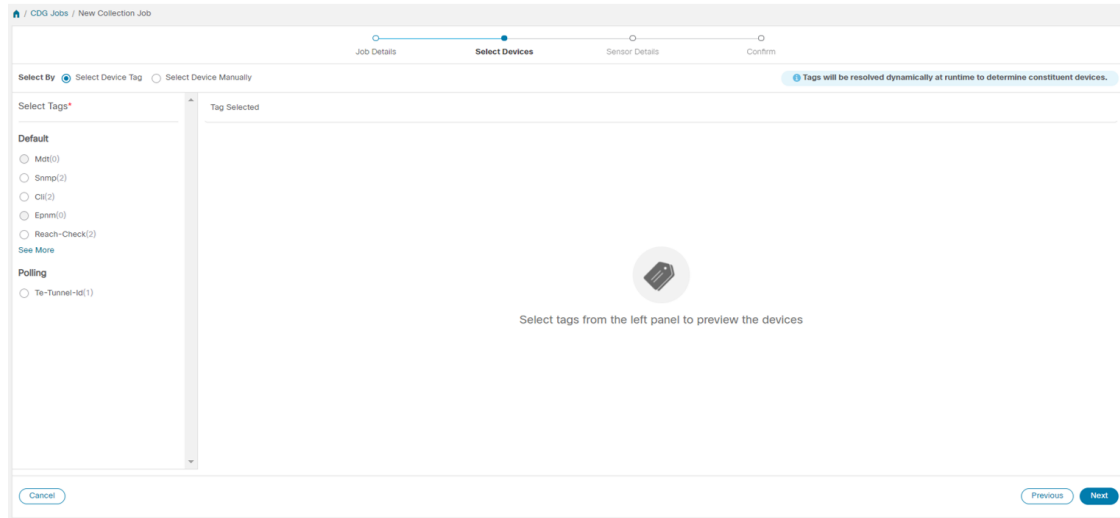
図 27:[ジョブの詳細 (Job Details)] ウィンドウ

- [アプリケーション ID (Application ID)] : アプリケーションの一意的識別子。
- [コンテキスト (Context)] : すべての収集ジョブでアプリケーションのサブスクリプションを識別するための一意的識別子。
- [コレクタタイプ (Collector Type)] : 収集のタイプ (CLI または SNMP) を選択します。

[次へ (Next)] をクリックします。

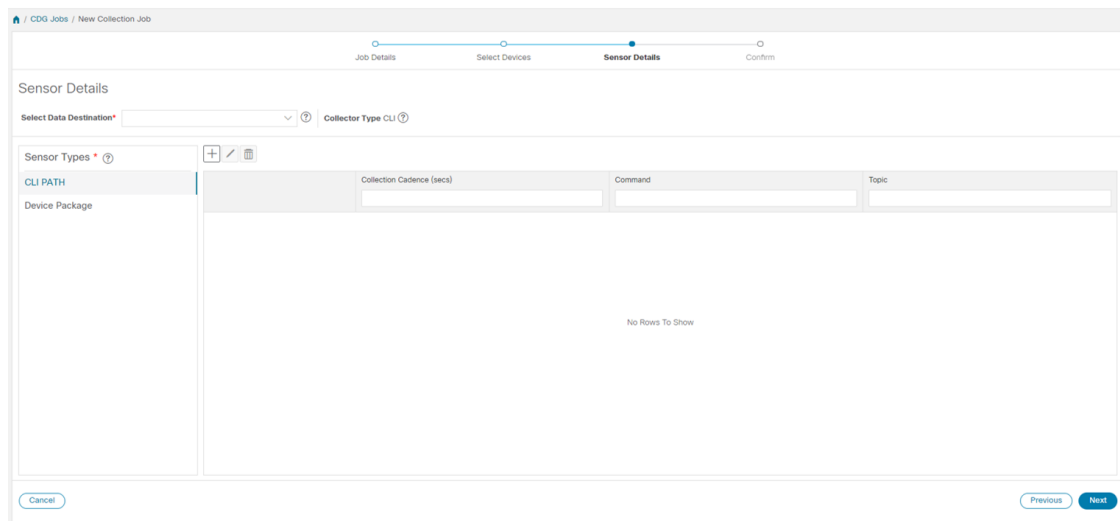
ステップ 4 データを収集するデバイスを選択します。デバイスタグに基づいて選択することも、手動で選択することもできます。[次へ (Next)] をクリックします。

図 28: [デバイスの選択 (Select Devices)] ウィンドウ



ステップ 5 (CLI での収集の場合にのみ適用) 次のセンサーの詳細を入力します。

図 29: [センサーの詳細 (Sensor Details)] ウィンドウ



- [データ送信先の選択 (Select Data Destination)] ドロップダウンからデータ送信先を選択します。
- 左側の [センサータイプ (Sensor Types)] ペインからセンサータイプを選択します。


[CLI パス (CLI PATH)] を選択した場合は、 ボタンをクリックして、[CLI パスの追加 (Add CLI Path)] ダイアログボックスに次のパラメータを入力します。

図 30: [CLI]パスの追加 (Add CLI Path) ダイアログボックス

- [収集パターン (Collection Cadence)]: プッシュまたはポーリングパターンを秒単位で指定します。
- [コマンド (Command)]: CLI コマンド
- [トピック (Topic)]: 出力先に関連付けられているトピック。

(注) 外部 gRPC サーバーを使用する場合、トピックは任意の文字列にできます。

[デバイスパッケージ (Device Package)]を選択した場合は、**+** ボタンをクリックし、[デバイスパッケージセンサーの追加 (Add Device Package Sensor)]ダイアログボックスに次のパラメータの値を入力します。

図 31: [デバイスパッケージセンサーの追加 (Add Device Package Sensor)]ダイアログボックス

- [収集パターン (Collection Cadence)]: プッシュまたはポーリングパターンを秒単位で指定します。

- [デバイスパッケージ名 (Device Package Name)] : デバイスパッケージの作成時に使用するカスタム XDE デバイスパッケージの ID。
- [関数名 (Function Name)] : カスタム XDE デバイスパッケージ内の関数名。
- [トピック (Topic)] : 出力先に関連付けられているトピック。

パラメータのキーと文字列の値を入力します。

[保存 (Save)] をクリックします。

ステップ 6 (SNMP での収集の場合にのみ適用) 次のセンサーの詳細を入力します。

図 32: [センサーの詳細 (Sensor Details)] ウィンドウ

OID	Collection Cadence (secs)	Operation Type	Topic
No Rows To Show			

- [データ送信先の選択 (Select Data Destination)] ドロップダウンからデータ送信先を選択します。
- 左側の [センサータイプ (Sensor Types)] ペインからセンサータイプを選択します。

[SNMP MIB] を選択した場合は、**+** ボタンをクリックして、[SNMP MIB の追加 (Add SNMP MIB)] ダイアログボックスに次のパラメータを入力します。

図 33: [SNMP MIBの追加 (Add SNMP MIB)] ダイアログボックス

- [収集パターン (Collection Cadence)] : プッシュまたはポーリングパターンを秒単位で指定します。
- OID
- [操作 (Operation)] : リストから操作を選択します。
- [トピック (Topic)] : 出力先に関連付けられているトピック。

[デバイスパッケージ (Device Package)] を選択した場合は、**+** ボタンをクリックし、[デバイスパッケージセンサーの追加 (Add Device Package Sensor)] ダイアログボックスに次のパラメータの値を入力します。

図 34: [デバイスパッケージセンサーの追加 (Add Device Package Sensor)] ダイアログボックス

- [収集パターン (Collection Cadence)] : プッシュまたはポーリングパターンを秒単位で指定します。

- [デバイスパッケージ名 (Device Package Name)]: デバイスパッケージの作成時に使用するカスタムデバイスパッケージの ID。
- [関数名 (Function Name)]: カスタムデバイスパッケージ内の関数名。
- [トピック (Topic)]: 出力先に関連付けられているトピック。

パラメータのキーと文字列の値を入力します。

[保存 (Save)] をクリックします。

ステップ 7 [収集ジョブの作成 (Create Collection Job)] をクリックします。

(注) 外部の Kafka 接続先 (つまり安全でない Kafka) に対して収集ジョブが送信されると、Kafka へのディスパッチジョブは接続に失敗します。コレクタのログに

```
「org.apache.kafka.common.errors.TimeoutException: Topic cli-job-kafka-unsecure not present
in metadata after 60000 ms」というエラーが表示されます。Kafka のログには「SSL
authentication error "[2021-01-08 22:17:03,049] INFO [SocketServer brokerId=0] Failed
authentication with /80.80.80.108 (SSL handshake failed)
(org.apache.kafka.common.network.Selector)」というエラーが表示されます。
```

これは、外部の Kafka VM でポートがブロックされているために発生します。次のコマンドを使用して、ポートが Kafka Docker/サーバーポートでリッスンしているかどうかを確認できます。

```
netstat -tulpn
```

Kafka サーバーの問題を修正し、Kafka サーバープロセスを再起動します。

収集ジョブのモニター

[収集ジョブ (Collection Jobs)] ページから、Cisco Crosswork に登録されているすべての Crosswork Data Gateway インスタンスで現在アクティブな収集ジョブのステータスをモニターできます。

Cisco Crosswork の UI の左側のナビゲーションバーで、[管理 (Administration)] > [収集ジョブ (Collection Jobs)] を選択します。

この左側のペインには、すべてのアクティブな収集ジョブが、ステータス、アプリ ID、およびコンテキスト ID とともに一覧表示されます。[ジョブの詳細 (Job Details)] ペインには、左側ペインの特定のジョブに関連付けられているすべての収集タスクの詳細が表示されます。[収集ジョブ (Collection Jobs)] ペインの収集ジョブの全体的なステータスは、[ジョブの詳細 (Jobs Details)] ペインのすべての収集タスクの集約ステータスです。

[収集ジョブ (Collection Jobs)] ペインでジョブを選択すると、[ジョブの詳細 (Job Details)] ペインに次の詳細が表示されます。

- 収集ジョブに関連付けられたアプリケーション名とコンテキスト。
- 収集ジョブのステータス。



(注)



- デバイスが Crosswork Data Gateway に接続された後にそのデバイスに関連付けられている収集タスクのステータスは、[不明 (Unknown)] になります。
- 次のいずれかの理由で、ジョブのステータスが [不明 (Unknown)] になる可能性があります。
 - Crosswork Data Gateway がまだそのステータスを報告していない。
 - Crosswork Data Gateway と Cisco Crosswork 間の接続が失われた。
 - Crosswork Data Gateway は収集ジョブを受信したが、実際の収集はまだ保留中になっている。たとえば、トラップが Crosswork Data Gateway のサウスバウンドインターフェイスに送信されていない場合や、デバイスがテレメトリ更新を送信していない場合などです。
 - 監視している SNMP トラップ収集ジョブのトラップ状態が発生していません。たとえば、リンクアップまたはリンクダウンの遷移を探していて、コレクタが確立されてからリンク状態が変更されていない場合、状態は [不明 (Unknown)] として報告されます。したがって、トラップベースのコレクションが機能していることを検証するには、実際にトラップをトリガーする必要があります。
- 収集ジョブが処理された後、処理が成功した場合はステータスが [成功 (Successful)] に変わり、それ以外の場合は [失敗 (Failed)] に変わります。
- 収集ジョブが低下状態の場合、その原因の 1 つとして、デバイスへの静的ルートが Crosswork Data Gateway から消去されていることが考えられます。
- エラー状態にある宛先へのコレクションは停止しません。宛先状態はバックグラウンドで識別されます。宛先がエラー状態の場合、エラーカウントがインクリメントされます。[ディストリビューション (Distribution)] ステータスに表示されるエラーメッセージをドリルダウンし、それぞれのコレクタログを調べて問題を特定して解決します。
- Cisco Crosswork Health Insights : KPI ジョブは、拡張 Crosswork Data Gateway インスタンスにマッピングされたデバイスでのみ有効にする必要があります。標準の Crosswork Data Gateway インスタンスにマッピングされているデバイスで KPI ジョブを有効にすると、[ジョブの詳細 (Jobs Details)] ペインで収集ジョブのステータスが [低下 (Degraded)]、収集タスクの

ステータスが [失敗 (Failed)] として報告されます。

- REST API 要求で渡す収集ジョブのジョブ設定。ジョブの設定を表示するには、[設定の詳細 (Config Details)]の横にある ⓘ アイコンをクリックします。Cisco Crosswork では、次の2つのモードで設定を表示できます。
 - ビュー モード
 - テキストモード
- 収集タイプ
- 収集ジョブの最終変更日時。
- [収集 (x) (Collections (x))] : x は、センサーパスによってデバイスにまたがる要求された収集の入力を指します。対応する [(y) 問題 ((y) Issues)] は [不明 (UNKNOWN)] 状態または [失敗 (FAILED)] 状態の入力収集の数です。
- [配布 (x) (Distributions (x))] : x は、センサーパスによってデバイスにまたがる要求された出力収集を指します。対応する [(y) 問題 ((y) Issues)] は [不明 (UNKNOWN)] 状態または [失敗 (FAILED)] 状態の出力収集の数です。

Cisco Crosswork は、収集と配布に関する次の詳細も表示します。

フィールド	説明
収集/配布ステータス (Collection/Distribution Status)	収集/配布のステータス。Crosswork Data Gateway から変更ベースで報告されます。詳細については、[収集/配信ステータス (Collection/Distribution Status)]の横にある ⓘ をクリックします。
ホスト名 (Hostname)	収集ジョブが関連付けられているデバイスのホスト名。
デバイス ID (Device Id)	データの収集元のデバイスの一意の識別子。

フィールド	説明
センサーデータ (Sensor Data)	<p>センサーパス</p> <p>収集/配布の概要を表示するには、 をクリックします。センサーデータの概要ポップアップから [クリップボードにコピー (Copy to Clipboard)] をクリックしてセンサーデータをコピーできます。</p> <p>収集/配布メトリックの概要を表示するには、 をクリックします。メトリックはパターンベース、つまりデフォルトでは10分ごとに1回報告されます。収集に関する次のメトリックが表示されます。</p> <ul style="list-style-type: none"> • last_collection_time_msec • total_collection_message_count • last_device_latency_msec • last_collection_cadence_msec <p>収集に関する次のメトリックが表示されます。</p> <ul style="list-style-type: none"> • total_output_message_count • last_destination_latency_msec • last_output_cadence_msec • last_output_time_msec • total_output_bytes_count
接続先 (Destination)	ジョブのデータ接続先。
最後のステータス変更の報告時刻 (Last Status Change Reported Time)	デバイスセンサーペアの最後のステータス変更が Crosswork Data Gateway から報告された日時。



- (注)
- Create Failed エラーは、N 台のデバイスのうちの一部のデバイスの設定に失敗したことを示します。ただし、収集は正常に設定されたデバイスで行われます。Control Status API を使用して、このエラーの原因となっているデバイスを特定できます。
 - NSO エラーが原因で特定のデバイスでジョブの作成が失敗した場合は、NSO エラーを修正した後、デバイスの管理状態を手動で最初に [ダウン (Down)] にしてから [アップ (Up)] に変更する必要があります。ただし、これを行うと、デバイス上の収集がリセットされます。



- (注) [作成/削除失敗 (Create/Delete failed)] エラーが別の画面ポップアップに表示されます。エラーの詳細を表示するには、ジョブステータスの横にある ⓘ をクリックします。
- 同じペイロードで PUT 収集ジョブ API を使用してジョブを再作成することもできます。


イベントベースの収集ジョブの収集ステータス

1. データの収集が成功すると、[収集ジョブ (Collection Jobs)] ペインで収集ジョブのステータスが [不明 (Unknown)] から [成功 (Success)] に変わります。
2. デバイスが Crosswork Data Gateway から切断されると、対応するすべての収集ジョブが削除され、[収集ジョブ (Collection Jobs)] ペインに収集ジョブのステータスが [成功 (Success)] と表示されます。[ジョブの詳細 (Job Details)] ペインに表示されるデバイスまたは収集タスクはありません。
3. デバイスが Crosswork Data Gateway に接続されると、Crosswork Data Gateway は、ステータスが [不明 (Unknown)] に設定されている新しい収集ジョブを受信します。このステータスは、デバイスからイベントを受信した後に [成功 (Success)] に変わります。
4. すでに Crosswork Data Gateway に接続されているデバイスでデバイス設定が誤って更新された場合、Crosswork Data Gateway がジョブとイベントを受信しても、[ジョブの詳細 (Jobs Details)] ペインの収集タスクのステータスは変わりません。
5. デバイスインベントリが誤ったデバイス IP で更新された場合、[ジョブの詳細 (Jobs Details)] ペインの収集タスクのステータスは [不明 (Unknown)] になります。

収集ジョブの削除

システムジョブ (さまざまな Crosswork アプリケーションによって作成されたデフォルトのジョブ) は、問題が発生する可能性があるため、削除しないでください。Health Insights によって作成されたジョブは、展開された収集ジョブを削除する KPI プロファイルを無効にすることによってのみ削除する必要があります。[収集ジョブ (Collection Jobs)] ページからは、外部収集ジョブを削除するには、次の手順を使用します。

収集ジョブを削除するには、次の手順を実行します。

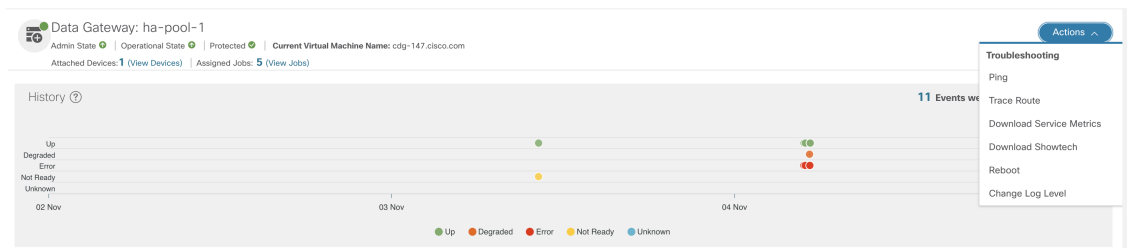
- ステップ 1 [管理 (Administration)] > [収集ジョブ (Collection Jobs)] に移動します。
- ステップ 2 [一括ジョブ (Bulk Jobs)] タブまたは [パラメータ化されたジョブ (Parameterized Jobs)] タブのいずれかを選択します。
- ステップ 3 左側の [収集ジョブ (Collection Jobs)] ペインで、削除する収集ジョブを選択します。
- ステップ 4  をクリックします。
- ステップ 5 確認を求められたら、[削除 (Delete)] をクリックします。

Crosswork Data Gateway のトラブルシューティング

Crosswork Data Gateway は、UI または Crosswork Data Gateway VM のインタラクティブコンソールからトラブルシューティングできます。

この項では、Cisco Crosswork UI から使用できるさまざまなトラブルシューティングのオプションについて説明します。

図 35: データゲートウェイ - トラブルシューティング



Crosswork Data Gateway VM のインタラクティブコンソールから使用できるトラブルシューティングオプションの詳細については、「[Crosswork Data Gateway VM のトラブルシューティング](#)」を参照してください。

接続先への接続の確認

Cisco Data Gateway から接続先への接続を確認するには、[トラブルシューティング (Troubleshooting)] メニューの [Ping] オプションと [トレースルート (Traceroute)] オプションを使用します。



- (注) 接続先を正常に ping するには、ネットワークで ping トラフィックを有効にする必要があります。

1. [管理 (Administration)]>[Data Gateway の管理 (Data Gateway Management)]>[データゲートウェイ (Data Gateways)]に移動します。
2. 接続を確認する Cisco Crosswork Data Gateway の名前をクリックします。
3. [Crosswork Data Gateway の詳細 (Crosswork Data Gateway details)] ページの右上隅で、[アクション (Actions)] をクリックし、[Ping] または [トレースルート (Traceroute)] を選択します。
 - [Ping] : [パケット数 (Number of Packets)] フィールドと [接続先アドレス (Destination Address)] フィールドに詳細を入力し、[Ping] をクリックします。
 - [トレースルート (Traceroute)] : [接続先アドレス (Destination Address)] に入力し、[トレースルート (Traceroute)] をクリックします。
4. 接続先が到達可能な場合、Cisco Crosswork は同じウィンドウに [Ping] または [トレースルート (Traceroute)] のテストの詳細を表示します。

サービスメトリックのダウンロード

Cisco Crosswork の UI から Crosswork Data Gateway のすべての収集ジョブのメトリックをダウンロードするには、次の手順を実行します。

ステップ 1 [管理 (Administration)]>[Data Gateway の管理 (Data Gateway Management)]>[データゲートウェイ (Data Gateways)]に移動します。

ステップ 2 サービスメトリックをダウンロードする Crosswork Data Gateway の名前をクリックします。

ステップ 3 [Crosswork Data Gateway の詳細 (Crosswork Data Gateway details)] ページの右上隅で、[アクション (Actions)] > [サービスメトリックのダウンロード (Download Service Metrics)] をクリックします。

ステップ 4 パスフレーズを入力します。

(注) このパスフレーズを必ずメモしておいてください。このパスフレーズは、後でファイルを復号するために使用します。

ステップ 5 [サービスメトリックのダウンロード (Download Service Metrics)] をクリックします。ファイルは、システムのデフォルトのダウンロードフォルダに暗号化された形式でダウンロードされます。

ステップ 6 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。openssl version コマンドを使用して、システムの openssl バージョンを確認します。

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <service metrics file> -out
<decrypted filename> -pass pass:<encrypt string>
```

Showtech ログのダウンロード

Cisco Crosswork の UI から showtech ログをダウンロードする手順を実行します。



- (注) Crosstech Data Gateway が [エラー (ERROR)] 状態の場合、Showtech ログは UI から収集できません。Cisco Crosswork Data Gateway が [低下 (DEGRADED)] 状態の場合、OAM-Manager サービスが実行されており、低下していなければ、ログを収集できます。

ステップ 1 [管理 (Administration)] > [Data Gateway の管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] に移動します。

ステップ 2 showtech をダウンロードする Crosswork Data Gateway の名前をクリックします。

ステップ 3 Crosswork Data Gateway の詳細ページの右上隅にある [アクション (Actions)] をクリックし、[Showtech のダウンロード (Download Showtech)] をクリックします。

図 36: データゲートウェイ - Showtech のダウンロード

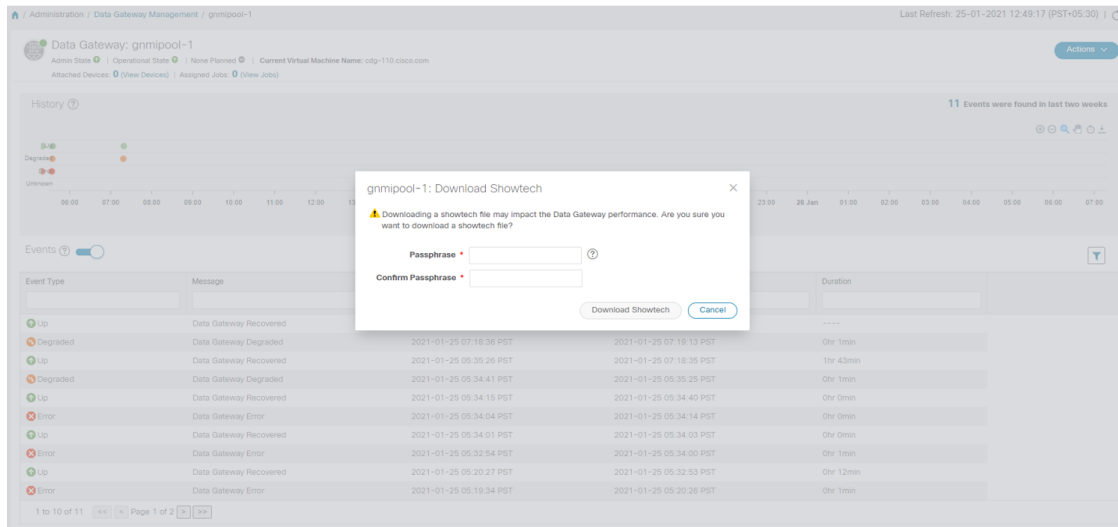
The screenshot displays the management interface for a Data Gateway named 'gnmipool-1'. At the top, there are status indicators for Admin State (Operational), None Planned, and Current Virtual Machine Name (csp-110.cisco.com). Below this is a 'History' section with a chart showing the gateway's status over time, with markers for Up, Degraded, Error, and Unknown. The 'Events' section is expanded, showing a table of recent events. The 'Actions' menu is open, and the 'Download Showtech' option is highlighted with a red box.

Event Type	Message	Start Time	End Time	Duration
Up	Data Gateway Recovered	2021-01-25 07:19:14 PST	----	----
Degraded	Data Gateway Degraded	2021-01-25 07:18:36 PST	2021-01-25 07:19:13 PST	0hr 1min
Up	Data Gateway Recovered	2021-01-25 05:35:26 PST	2021-01-25 07:18:35 PST	1hr 43min
Degraded	Data Gateway Degraded	2021-01-25 05:34:41 PST	2021-01-25 05:35:25 PST	0hr 1min
Up	Data Gateway Recovered	2021-01-25 05:34:15 PST	2021-01-25 05:34:40 PST	0hr 0min
Error	Data Gateway Error	2021-01-25 05:34:04 PST	2021-01-25 05:34:14 PST	0hr 0min
Up	Data Gateway Recovered	2021-01-25 05:34:01 PST	2021-01-25 05:34:03 PST	0hr 0min
Error	Data Gateway Error	2021-01-25 05:32:54 PST	2021-01-25 05:34:00 PST	0hr 1min
Up	Data Gateway Recovered	2021-01-25 05:20:27 PST	2021-01-25 05:32:53 PST	0hr 12min
Error	Data Gateway Error	2021-01-25 05:19:34 PST	2021-01-25 05:20:26 PST	0hr 1min

ステップ 4 パスフレーズを入力します。

- (注) このパスフレーズを必ずメモしておいてください。showtech ファイルを復号するには、このパスフレーズを後で入力する必要があります。

図 37: [Showtechのダウンロード (Download Showtech)] ポップアップウィンドウ



ステップ 5 [Showtech のダウンロード (Download Showtech)] 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 6 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-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>
```

Cisco Crosswork Data Gateway VM の再起動

次の手順を実行して、Cisco Crosswork UI から Crosswork Data Gateway を再起動します。



(注) Crosswork Data Gateway を再起動すると、機能が再びアップするまで一時停止します。

ステップ1 [管理 (Administration)] > [Data Gateway の管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] に移動します。

ステップ2 再起動する Cisco Crosswork Data Gateway の名前をクリックします。

ステップ3 Crosswork Data Gateway の詳細ページの右上隅にある [アクション (Actions)] をクリックし、[再起動 (Reboot)] をクリックします。

図 38: [データゲートウェイ (Data Gateway)] - [再起動 (Reboot)]

The screenshot shows the 'Data Gateway: gnmipool-1' management page. The 'Actions' menu is open, and the 'Reboot' option is highlighted with a red box. The page includes a status bar, a history chart, and an events table.

Event Type	Message	Start Time	End Time	Duration
Up	Data Gateway Recovered	2021-01-25 07:19:14 PST	----	----
Degraded	Data Gateway Degraded	2021-01-25 07:18:36 PST	2021-01-25 07:19:13 PST	0hr 1min
Up	Data Gateway Recovered	2021-01-25 05:35:26 PST	2021-01-25 07:18:35 PST	1hr 43min
Degraded	Data Gateway Degraded	2021-01-25 05:34:41 PST	2021-01-25 05:35:25 PST	0hr 1min
Up	Data Gateway Recovered	2021-01-25 05:34:15 PST	2021-01-25 05:34:40 PST	0hr 0min
Error	Data Gateway Error	2021-01-25 05:34:04 PST	2021-01-25 05:34:14 PST	0hr 0min
Up	Data Gateway Recovered	2021-01-25 05:34:01 PST	2021-01-25 05:34:03 PST	0hr 0min
Error	Data Gateway Error	2021-01-25 05:32:54 PST	2021-01-25 05:34:00 PST	0hr 1min
Up	Data Gateway Recovered	2021-01-25 05:20:27 PST	2021-01-25 05:32:53 PST	0hr 12min
Error	Data Gateway Error	2021-01-25 05:19:34 PST	2021-01-25 05:20:26 PST	0hr 1min

ステップ4 [ゲートウェイの再起動 (Reboot Gateway)] をクリックします。

図 39: [ゲートウェイの再起動 (Reboot Gateway)] ポップアップウィンドウ

The screenshot shows the same management page as Figure 38, but with a confirmation dialog box open. The dialog box is titled 'gnmipool-1: Reboot Gateway' and contains the following text:

Rebooting the Data Gateway will pause its functionality until it is up again.
Are you sure you want to reboot the Data Gateway?

The dialog box has two buttons: 'Reboot Gateway' and 'Cancel'.

再起動が完了したら、[管理 (Administration)] > [データゲートウェイの管理 (Data Gateway Management)] > [データゲートウェイインスタンス (Data Gateway Instances)] ウィンドウで Cisco Crosswork Data Gateway の動作ステータスを確認します。

Crosswork Data Gateway コンポーネントのログレベルの変更

Cisco Crosswork の UI には、Crosswork Data Gateway のコンポーネント (コレクタ (cli-collector) やインフラサービス (oam-manager) など) のログレベルを変更するオプションがあります。ログレベルの変更は、変更を加える Crosswork Data Gateway にのみ適用されます。



(注) オフロードサービスのログレベルの変更はサポートされていません。

ステップ 1 [管理 (Administration)] > [Data Gateway の管理 (Data Gateway Management)] > [データゲートウェイ (Data Gateways)] に移動します。

ステップ 2 Crosswork インフラストラクチャサービスのコレクタのログレベルを変更する Crosswork Data Gateway 名をクリックします。

ステップ 3 [Crosswork Data Gateway の詳細 (Crosswork Data Gateway details)] ページの右上隅で、[アクション (Actions)] > [ログレベルの変更 (Change Log Level)] をクリックします。

[ログレベルの変更 (Change Log Level)] ウィンドウが表示され、各コンテナサービスの現在のログレベルが表示されます。

図 40: [ログレベルの変更 (Change Log Level)] ウィンドウ

Change Log Level: ha-pool-1 ×

Selected 0 / Filtered 0 / Total 66

Change Log Level ▼ Reset to Default ▼

	Container Service Name ↑	Component	Log Level
<input type="checkbox"/>	cli collector	grpc	Info
<input type="checkbox"/>	cli collector	xde runtime	Error
<input type="checkbox"/>	cli collector	xde cli_transport	Error
<input type="checkbox"/>	cli collector	dispatcher	Info
<input type="checkbox"/>	cli collector	kafka	Info
<input type="checkbox"/>	cli collector	xde function	Error
<input type="checkbox"/>	cli collector	all	Info
<input type="checkbox"/>	cli collector	xde session	Error
<input type="checkbox"/>	cli collector	xde snmp	Error
<input type="checkbox"/>	cli collector	spring web	Info
<input type="checkbox"/>	cli collector	netty	Info
<input type="checkbox"/>	cli collector	coordinator	Info
<input type="checkbox"/>	controller gateway	all	Info
<input type="checkbox"/>	gnmi collector	spring web	Info

Save
Discard Changes
Cancel

ステップ 4 ログレベルを変更するコンテナサービスのチェックボックスをオンにします。

ステップ 5 テーブルの上部にある [ログレベルの変更 (Change Log Level)] ドロップダウンリストから、[デバッグ (Debug)]、[トレース (Trace)]、[警告 (Warning)]、[情報 (Info)]、および [エラー (Error)] からログレベルを選択します。

(注) すべてのログのログレベルをデフォルトのログレベル ([情報 (Info)]) にリセットするには、[デフォルトにリセット (Reset to Default)] をクリックします。

ステップ6 [保存 (Save)]をクリックして変更したログレベルを保存します。

[保存 (Save)]をクリックして、コンポーネントのログレベルが正常に変更されたことを示す UI メッセージを表示します。

ネットワークロードバランサがアクティブな Crosswork Data Gateway の誤ったヘルステータスを表示

プールの作成中に、Crosswork Data Gateway はネットワークロードバランサ (NLB) のヘルスポートを開き、Crosswork Data Gateway のヘルステータスを示します。ただし、NLB FQDN が eth2 の異なるサブネット上にある IP アドレスに解決される場合、Crosswork Data Gateway は VM に静的ルートを追加します。ネットワーク構成の問題が原因で、静的ルートの組み込みがエラーで失敗する場合があります。Crosswork Data Gateway は失敗を無視し、HA プールを作成します。その結果、Crosswork Data Gateway はデバイスからデータを収集しません。

この問題を解決するには、次の手順を実行します。

ステップ1 NLB として識別されたシステムにログインし、Crosswork Data Gateway のヘルステータスを表示します。

ステップ2 ステータスが異常な場合は、NLB サブネットアドレスが eth1 や eth0 などのインターフェイスと競合しているかどうかを確認します。競合を解決するには、次のいずれかを実行します。

- NLB IP アドレスを変更し、インフラサービス (oam-manager) を再起動します。
- 新しいサブネット構成を使用して Crosswork Data Gateway VM を再展開します。

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。