テレメトリの設定

アプリケーションテレメトリの概要

アプリケーションテレメトリを使用すると、デバイスの正常性をモニターおよび評価するためのグローバルネットワーク設定を構成できます。

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定

Catalyst Center では、デバイスを特定のサイトに割り当てる際のグローバルネットワーク設定を構成できます。テレメトリを使用すると、ネットワークデバイスがポーリングされ、SNMP サーバー、syslog サーバー、NetFlow コレクタ、または有線クライアントの設定に従ってテレメトリデータが収集されます。

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『サイトの作成、編集、削除』を参照してください。

ステップ 1 [Design] > [Network Settings] > [Telemetry] の順に選択します。左上隅にあるメニューアイコンをクリックして次を選択します：

ステップ 2 [SNMP Traps] エリアで、次のいずれかを実行します。

- [Use Cisco DNA Center as SNMP trap server] チェックボックスをオンにします。
- [Add an external SNMP trap server] チェックボックスをオンにし、外部 SNMP トラップサーバーの IP アドレスを入力します。選択したサーバーによってネットワークデバイスから SNMP トラップとメッセージが収集されます。

ステップ 3 [Syslogs] エリアで、次のいずれかを実行します。

- [Use Cisco DNA Center as syslog server] チェックボックスをオンにします。
- [Add an external syslog server] チェックボックスをオンにし、外部 syslog サーバーの IP アドレスを入力します。

ステップ 4 [Application Visibility] 領域で、[Enable by default on wireless access devices] チェックボックスをオンにして、ネットワークデバイスサイトの割り当て時にアプリケーションテレメトリおよびコントローラベースのアプリケーション認識（CBAR）をデフォルトで有効にします。

次のいずれかを実行します。

- [Use Cisco DNA Center as NetFlow collector] オプションボタンをクリックします。デバイスインターフェイスの NetFlow の構成は、デバイスでアプリケーションテレメトリを有効にした場合にのみ完了します。NetFlow の宛先サーバーをデバイスに設定するには、サイトレベルで NetFlow コレクタを選択します。
- [Add Cisco Telemetry Broker (CTB)] オプションボタンをクリックし、Cisco Telemetry Broker の IP アドレスとポート番号を追加します。Cisco Telemetry Broker はデバイスから NetFlow レコードを収集し、その情報を宛先に送信します。

（注） NetFlow レコードを受信するには、Cisco Telemetry Broker で Catalyst Center が宛先として設定されている必要があります。Catalyst Center が宛先として設定されていない場合、アプリケーション エクスペリエンスは機能しません。

ステップ 5 [Wired Endpoint Data Collection] エリアで、[Enable Cisco DNA Center Wired Endpoint Data Collection At This Site] オプションボタンをクリックして、サイトのアクセスデバイスで IP デバイストラッキング（IPDT）をオンにします。

サイトの IPDT を有効にしない場合は、[Disable] オプションボタン（デフォルト）をクリックします。

（注） CLI 構成をプレビューするには、IPDT を有効にする必要があります。デバイスをプロビジョニングする場合、デバイスに展開する前に CLI 構成をプレビューできます。

ステップ 6 [Wireless Controller, Access Point and Wireless Clients Health] エリアで、[Enable Wireless Telemetry] チェックボックスをオンにして、ネットワーク内のワイヤレスコントローラ、AP、およびワイヤレスクライアントの状態をモニターします。

ステップ 7 [Save] をクリックします。

デバイスでのアプリケーションテレメトリ有効化の基準

Catalyst Center では、新しい自動選択アルゴリズムに基づいてインターフェイスと WLAN を選択し、該当するすべてのインターフェイスと WLAN でアプリケーションテレメトリを自動的に有効にします。

（注）
- 従来のタギングベースのアルゴリズムがサポートされ、インターフェイスまたは WLAN の新しい自動選択アルゴリズムよりも優先されます。
- 自動選択アルゴリズムからタギングベースのアルゴリズムに切り替える場合は、タグ付き SSID をデバイスに対してプロビジョニングする前にテレメトリを無効にする必要があります。

次の表に、サポートされているすべてのプラットフォームについて、従来のタギングベースのアルゴリズム（キーワード **lan** を使用）と新しい自動選択アルゴリズムに基づくインターフェイスと WLAN の選択基準を示します。

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Router	• インターフェイスの説明に **lan** キーワードが含まれている。[12] • インターフェイスに管理 IP アドレス以外の IP アドレスがある。	• インターフェイスに管理 IP アドレス以外の IP アドレスがある。 • インターフェイスが次のいずれでもない。 • WAN （注） インターフェイスにパブリック IP アドレスがあり、パブリック IP アドレスがインターフェイスを経由するルートルールがある場合、そのインターフェイスは WAN 側インターフェイスとして扱われます。 このコンテキストでは、パブリック IP アドレスはプライベート範囲にない（たとえば、192.168.x.x、172.16.y.y、10.z.z.z にない）か、システムの IP プールにない IP アドレスです。 ルートルールは動的に学習できます。このコンテキストでは、**show ip route** コマンドでこのインターフェイスを通過するパブリック IP アドレスへのルートは表示されません。 • ループバック • 管理インターフェイス：GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、FASTETHERNET1

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム

スイッチ	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2]
	• スイッチポートがアクセスポートとして設定されている。
	• スイッチポートに **switch-mode access** コマンドが設定されている。
		• インターフェイスが物理インターフェイスである。
		• アクセスポートにネイバーがない。
		• インターフェイスが次のいずれでもない。
		  • 管理インターフェイス：FASTETHERNET0、FASTETHERNET1、GIGABITETHERNET0/0、MGMT0
		  • LOOPBACK0、Bluetooth、App Gigabit、WPAN、Cellular、Async
		  • VSL インターフェイス

Cisco AireOS コントローラ	WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合、Wireless Service Assurance（WSA）の処理が有効になります。すべての SSID がローカルモードの場合、NetFlow が有効になります。
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと最適化アプリケーション パフォーマンス モニタリング（APM）プロファイルおよび IOS 16.12.1 以降	WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSID が混在している場合、つまり中央スイッチング、フレックスモード、およびファブリックモードの場合は、Cisco Application Visibility and Control（AVC）の基本レコードが設定されます。すべての SSID で中央スイッチングを使用している場合、最適化 APM レコードが設定されます。 IOS 17.10 以降を備える Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、Catalyst Center は、フレックスおよびファブリック SSID に対して、AVC 基本プロファイルではなく、APM プロファイルをプッシュします。
	（注） テレメトリ設定を更新する場合は、テレメトリを無効にしてから、設定の変更後にテレメトリを有効にする必要があります。	

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Catalyst Center トラフィックテレメトリアプライアンスと最適化 APM プロファイルおよび IOS 17.3 以降	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2] • インターフェイスが物理インターフェイスである。	• インターフェイスが物理インターフェイスである。 • インターフェイスが管理インターフェイス（GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、および FASTETHERNET1）ではない。

[1] **lan** キーワードは、大文字と小文字の区別はなく、スペース、ハイフン、または下線で区切ることができます。
[2] ネットワークデバイスを再同期して、**lan** インターフェイスの説明を読み取ります。

アプリケーションテレメトリ設定のプロビジョニング

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （1 ページ） の説明に従って、グローバルテレメトリ設定を構成します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、ビルディング、またはフロアを選択します。

ステップ 2 プロビジョニングするデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、[Telemetry] を選択し、次のいずれかを実行します。

（注） [Enable Application Telemetry] および [Disable Application Telemetry] オプションは、デバイスで Catalyst Center からのアプリケーションテレメトリがサポートされている場合のみ有効です。

a) [Enable Application Telemetry]：選択したデバイスでアプリケーションテレメトリを設定します。
b) [Disable Application Telemetry]：選択したデバイスからアプリケーションテレメトリ設定を削除します。

ステップ 4 [Apply] をクリックします。

[Application Telemetry] 列には、テレメトリの設定ステータスが表示されます。デフォルトの列設定で

[Application Telemetry] 列が表示されない場合は、列見出しの右端にある省略記号アイコン（⋮）をクリックし、[Application Telemetry] チェックボックスをオンにします。

ワイヤレスコントローラのアプリケーションテレメトリを有効化する

新規および既存のデバイスのアプリケーションテレメトリを有効にすることができます。

（注） [Application Visibility Setup] ウィンドウからアプリケーションテレメトリを有効にすることもできます。詳細については、アプリケーションテレメトリの有効化/無効化を参照してください。

始める前に

アプリケーションテレメトリを有効にするには、デバイスにCatalyst CenterAdvantageライセンスが必要です。

（注） Catalyst Center でアプリケーションテレメトリを有効にする前に、必ず、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI を使用して **[Configuration]** > **[Services]** > **[Application Visibility]** > **[Flow Monitors]**から手動で設定された既存のフローモニターを削除してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、建物、またはフロアを選択します。

ステップ 3 [Inventory] ウィンドウで、デバイスを選択します。複数のデバイスを同時に選択できます。

ステップ 4 [Actions] ドロップダウンリストから、[Telemetry] > [Enable Application Telemetry] の順に選択します。

ステップ 5 [Enable Telemetry] slide-in paneで、次の設定を完了します。

a) [AP mode]：[Flex/Fabric] または [Local] チェックボックスをオンにします。両方のオプションを選択することもできます。

b) [Include Guest SSID] チェックボックスをオンにして、ゲスト SSID のテレメトリを有効にします。

c) [Telemetry Source]：

- 組み込みワイヤレスコントローラ - NetFlow
- AireOSワイヤレスコントローラ（ローカルモード）- NetFlow
- AireOSワイヤレスコントローラ（Flex/Fabricモード）- ワイヤレス サービス アシュアランス（WSA）

d) すべてのワイヤレスコントローラに同じ設定を適用するには、[Apply this selection to all wireless controllers] をオンにします。

ステップ 6 [Enable] をクリックします。

ステップ 7 [Application Telemetry] ウィンドウで、[OK] をクリックします。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

テレメトリステータスは、[Inventory] ウィンドウの [Application Telemetry] 列に表示されます。

新しいクラスタ仮想IPアドレスを使用するためのテレメトリ設定の更新

Catalyst Center アプリケーションテレメトリを使用してデバイスデータをモニターし、Catalyst Center クラスタ仮想 IP アドレス（VIP）を変更する必要がある場合は、次の手順を実行して VIP を変更し、ノードテレメトリデータが新しい VIP に送信されることを確認します。

始める前に

- 使用している Catalyst Center のバージョンを確認します。それには、Catalyst Center GUI にログインし、[About] オプションを選択して Catalyst Center のバージョン番号を表示します。
- SSH クライアントソフトウェアを入手します。
- Catalyst Center プライマリノード上のエンタープライズ ネットワーク側の 10 GB インターフェイスに設定された VIP アドレスを特定します。ポート 2222 上のこのアドレスを使用してアプライアンスにログインします。このポートを特定するには、『*Cisco Catalyst Center Installation Guide*』の「Front and Rear Panels」セクションにある背面パネルの図を参照してください。
- プライマリノードに設定されている Linux ユーザー名（**maglev**）とパスワードを取得します。
- 割り当てるクラスタ VIP を特定します。クラスタ VIP は、『*Cisco Catalyst Center Installation Guide*』の「Required IP Addresses and Subnets」セクションで説明されている要件に準拠している必要があります。

ステップ 1 Catalyst Center GUI にアクセスし、次の手順に従ってすべてのサイトでアプリケーションテレメトリを無効にします。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、建物、またはフロアを選択します。

b) 現在モニターしているすべてのサイトとデバイスを選択します。

c) [Actions] ドロップダウンリストから、[Telemetry] > [Disable Application Telemetry] の順に選択します。
d) サイトとデバイスでテレメトリが無効になったことが示されるまで待ちます。

ステップ 2 アプライアンス構成ウィザードを使用して、次のようにクラスタ VIP を変更します。

a) SSH クライアントを使用して、Catalyst Center プライマリノード上のエンタープライズネットワーク側の 10 GB インターフェイスに設定された VIP アドレスにログインします。ポート 2222 にログインしていることを確認します。
b) プロンプトが表示されたら、Linux のユーザー名とパスワードを入力します。
c) 次のコマンドを入力すると、プライマリノード上で構成ウィザードにアクセスできます。

```
$ sudo maglev-config update
```

Linux パスワードを入力するようプロンプトが表示されたら、再度入力します。

d) クラスタ仮想 IP の入力を求める画面が表示されるまで [Next] を繰り返しクリックします。新しいクラスタ VIP を入力し、以降のすべての画面で [Next] をクリックしてウィザードを終了します。

設定したインターフェイスごとに 1 つの仮想 IP を設定する必要があります。**sudo maglev-config update** コマンドを入力して、設定したインターフェイスごとに 1 つの VIP を入力するよう指示されるようにウィザードを設定することを推奨します。

最後の画面に到達すると、変更を適用する準備ができたことを示すメッセージが表示されます。

e) [proceed] をクリックして、クラスタ VIP の変更を適用します。

設定プロセスの最後に成功メッセージが表示され、SSH プロンプトに復帰します。

ステップ 3 SSH プロンプトで次の一連のコマンドを入力して、必要な Catalyst Center サービスを再起動します。

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```

ステップ 4 すべてのサービスが再起動するまで待ちます。次のコマンドを入力して、再起動の進行状況をモニターリングできます。必要に応じて、使用している Catalyst Center のバージョンが属するリリーストレインに適したサービス名に置き換えてください。

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap -e
wirelesscollector
```

必要なすべてのサービスが実行されている場合は、次のようなコマンド出力が表示され、正常に再起動した各サービスの実行ステータスが表示されます。

```
assurance-backend  wirelesscollector-123-bc99s  1/1   Running   0   25d   <IP>   <IP>
ndp   collector-netflow-456-lxvlx   1/1   Running   0   1d   <IP>   <IP>
ndp   collector-syslog-789-r0rr1    1/1   Running   0   25d   <IP>   <IP>
ndp   collector-trap-101112-3ppllm  1/1   Running   0   25d   <IP>   <IP>
```

ステップ 5 Catalyst Center GUI にアクセスし、次の手順に従ってすべてのノードでアプリケーションテレメトリを有効にします。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
b) モニターするすべてのサイトとデバイスを選択します。

c) [Actions] ドロップダウンリストから、[Telemetry] > [Enable Application Telemetry] の順に選択します。
d) サイトとデバイスでテレメトリが有効になったことが示されるまで待ちます。

テレメトリを使用したデバイス設定の更新

デバイスの可制御性が有効か無効かに関係なく、デバイスに設定の変更をプッシュできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、ビルディング、またはフロアを選択します。

ステップ 2 設定の変更を反映するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、**[Telemetry]** > **[Update Telemetry Settings]** の順に選択します。

[Update Telemetry Settings] slide-in paneが開きます。

ステップ 4 （オプション）構成の変更をデバイスにプッシュするには、[Force Configuration Push] チェックボックスをオンにします。

構成に変更がない場合は、既存の構成がデバイスに再度プッシュされます。

ステップ 5 [Next] をクリックします。

ステップ 6 [Update Telemetry Settings] slide-in paneで、[Visibility and Control of Configurations] の設定に応じて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ワイヤレスデバイス構成の可視性と制御を参照してください。

ステップ 7 [Task Name] フィールドにタスク名を入力します。

ステップ 8 [Apply] をクリックします。

ステップ 9 [Update Telemetry Settings] slide-in paneで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、[Preview Configuration] ウィンドウで、次の手順を実行します。

1. デバイス構成を確認します。

詳細については、ワイヤレスデバイス構成の可視性と制御を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

（注） 設定のプレビュー中、PKCS12 証明書は、15 分以内に使用する必要があるため生成されません。[Preview Configuration] ウィンドウには、関連する設定コマンドのみが表示されます。設定をプレビューした後に展開すると、PKCS12 証明書が生成され、デバイスにプッシュされます。

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。