# Cisco Nexus Dashboard Insights、リリース 6.4.1 スタートアップ ガイド：Cisco NDFC またはスタンドアロン NX-OS

Cisco Confidential

# 目次


新規情報および変更情報 ..... 2
Cisco Nexus ダッシュボード Insights セットアップ ..... 3
Nexus Dashboard Insightsの紹介 ..... 3
初期設定 ..... 4
サイトの追加 ..... 4
オンライン NDFC サイトの追加 ..... 4
コントローラなしでオンライン NX-OS サイトを追加する ..... 8
スナップショット サイトを追加します。 ..... 12
サイト分析 ..... 13
保証分析 ..... 15
アシュアランス分析の注意事項と制約事項 ..... 15
オンデマンド分析 ..... 15
アシュアランス分析を有効にする ..... 16
バグスキャン ..... 17
アクティブ バグと影響を受けやすいバグの表示 ..... 18
ベストプラクティス ..... 22
オンデマンドのベスト プラクティス ..... 22
デバイス コネクタについて ..... 22
Nexus Dashboard Insightsのスイッチ設定ステータス ..... 24
フローの設定 ..... 25
フローテレメトリ ..... 25
フローテレメトリのガイドラインと制約事項 ..... 25
フローの設定 ..... 26
フローテレメトリのサブネットの監視 ..... 29
Netflow ..... 30
NetFlowタイプ ..... 30
NetFlowのガイドラインと制約事項 ..... 31
NetFlowの設定 ..... 31
sFlow ..... 33
sFlowの注意事項および制約事項 ..... 33
sFlowの設定 ..... 34
エクスポートデータ ..... 35
エクスポートデータ ..... 35
Kafka Exporterの設定 ..... 35
電子メールの設定 ..... 36
Syslog ..... 37
Syslog の設定 ..... 37
ネットワーク接続ストレージへのフロー レコードのエクスポート ..... 39
注意事項と制約事項 ..... 39
ネットワーク接続ストレージをフロー レコードをエクスポートするために追加する ..... 39
システム設定 ..... 43

システムに関する問題 ..... 43
システムステータス ..... 43
設定のインポートとエクスポート ..... 45
注意事項と制約事項 ..... 45
設定のエクスポート ..... 46
設定のインポート ..... 46
著作権 ..... 47

初版：2024 年 3 月 6 日

最終更新日：2024 年 4 月 1 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883

# 新規情報および変更情報

次の表は、最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

*表 1. Cisco Nexus Dashboard Insightsの新機能と変更された動作*

| 機能 | 説明 | リリース | 参照先 |
|---|---|---|---|
| コントローラを使用しない NX-OS サイトのオンボーディング | スタンドアロン NX-OS ファブリックのサポート | 6.4.1 | コントローラなしでオンライン NX-OS サイトを追加する |
| 現用系バグと影響を受けやすいバグを表示する | バグ スキャンの完了後に、ネットワークに影響を与えるアクティブ バグと影響を受けやすいバグを表示できるようになりました。 | 6.4.1 | アクティブ バグと影響を受けやすいバグの表示 |

このドキュメントは、Nexus Insights の GUI とオンライン（www.cisco.com）から入手できます。このドキュメントの最新バージョンに関しては、「Cisco Nexus Dashboard Insights Documentation」を参照してください。

# Cisco Nexus ダッシュボード Insights セットアップ

## Nexus Dashboard Insightsの紹介

Cisco Nexus Dashboard Insights は、データ センター ネットワークの運用と管理を合理化する一括管理のコンソールです。

Nexus Dashboard Insightsは、次のコンポーネントで構成されています。

- [概要（Overview）]：グローバル ネットワーク インフラストラクチャの全体像を示します。Insightsを初めて使用する場合は、ジャーニーをすぐに開始できます。ここで、プラットフォームの更新と新機能も提供されます。
  - [トポロジ（Topology）]： Nexus Dashboard Insights のスイッチと、デバイスやエンドポイントなどの接続されたコンポーネントの相互接続性を可視化します。
- 管理：ネットワーク インフラストラクチャとその運用の詳細を確認します。
  - [サイト（Sites）]：サイトとは、アプリケーションやエンドポイントへの接続を提供する一連のスイッチやその他のネットワーク デバイスから構成されるオンプレミス ネットワーク リージョンです。
  - インベントリ（Inventory）：スイッチとコントローラに関する情報を表示します。
  - [ルール（Rules）]：サイトの異常とアドバイザリの構成を管理できるようにします。
  - ソフトウェア管理：すべてのデバイスで実行されているソフトウェアを 1 か所から簡単に管理し、更新をインストールし、更新前と更新後の分析を実行します。
- 分析：過去にさかのぼり、分析によって過去のネットワーク パターンを理解できるようになります。
  - 異常：ネットワーク全体でさまざまなタイプの異常をプロアクティブに検出し、異常の根本原因および修復方法を特定します。
  - アドバイザリ：ネットワークのサポートを維持し、最適な状態で稼働するための推奨事項を提供します。
- 分析ハブ：最適化された高度な分析ツールを使用してネットワークの分析およびトラブルシューティングを行い、ネットワークのパフォーマンスと正常性に関する貴重なインサイトを取得します。
  - 持続性：サイトのエネルギー使用量、コスト、排出量を調べます。
  - 適合性：ハードウェアとソフトウェアのライフサイクルを追跡します。
  - 順守性：ファブリックのカスタム異常ルールの遵守をモニターします。
  - 接続分析：あるエンドポイントから別のエンドポイントへのフローを分析します。
  - デルタ分析：2つの時点でのサイトの構成と違いを比較します。
  - 変更前分析：構成変更の潜在的な影響を表示します。
  - ログ収集：デバイスからのログを収集および分析します。
  - ポリシーCAM：ネットワークのポリシーをモニターします。
  - トラフィック分析：ネットワークの遅延、輻輳、ドロップをモニターできます。
  - バグスキャン：ネットワークに影響を与えるアクティブなバグと潜在的なバグについて学習します。
- 管理者：

- 統合： AppDynamics、 vCenter、 Domain Name System (DNS)、 Nexus Dashboard Orchestrator などの統合を追加できます。
- 設定のインポートとエクスポート機能を使用すると、Nexus Dashboard Insights で次の構成をインポートおよびエクスポートできます。

# 初期設定

次のワークフローでは、初期セットアップに必要な構成について説明します。サイトを追加した後、関連する機能を有効または設定できます。これらのタスクは順番に従って実行する必要はありません。タスクは任意の順序で実行または有効化できます。

- サイトを追加します。「サイトの追加」を参照してください。前提条件と注意事項については、「サイト」を参照してください。
- サイト分析「サイト分析」を参照してください。
- フローを構成します。「フローの構成」を参照してください。
- データをエクスポートします。「データのエクスポート」を参照してください。
- システム ステータス。「システム ステータス」を参照してください。

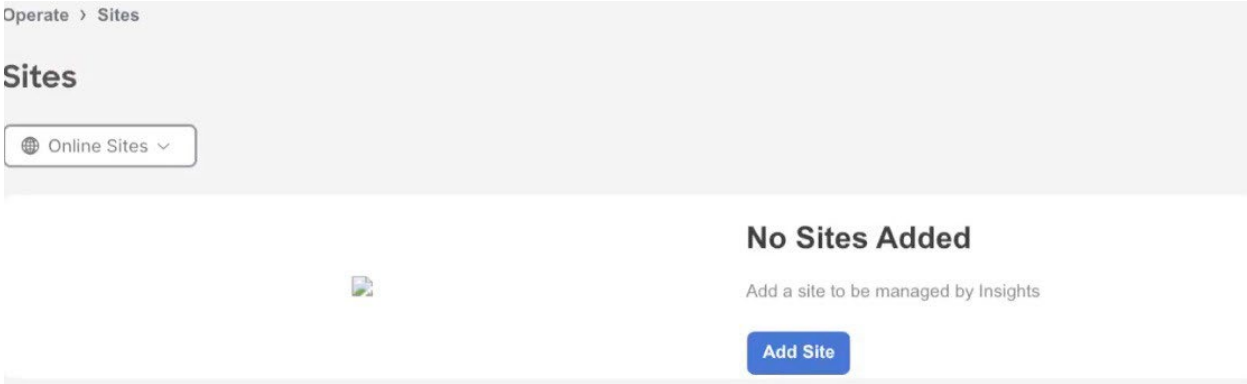
# サイトの追加

次の方法を使用して、Nexus Dashboard Insightsにサイトを追加できます。

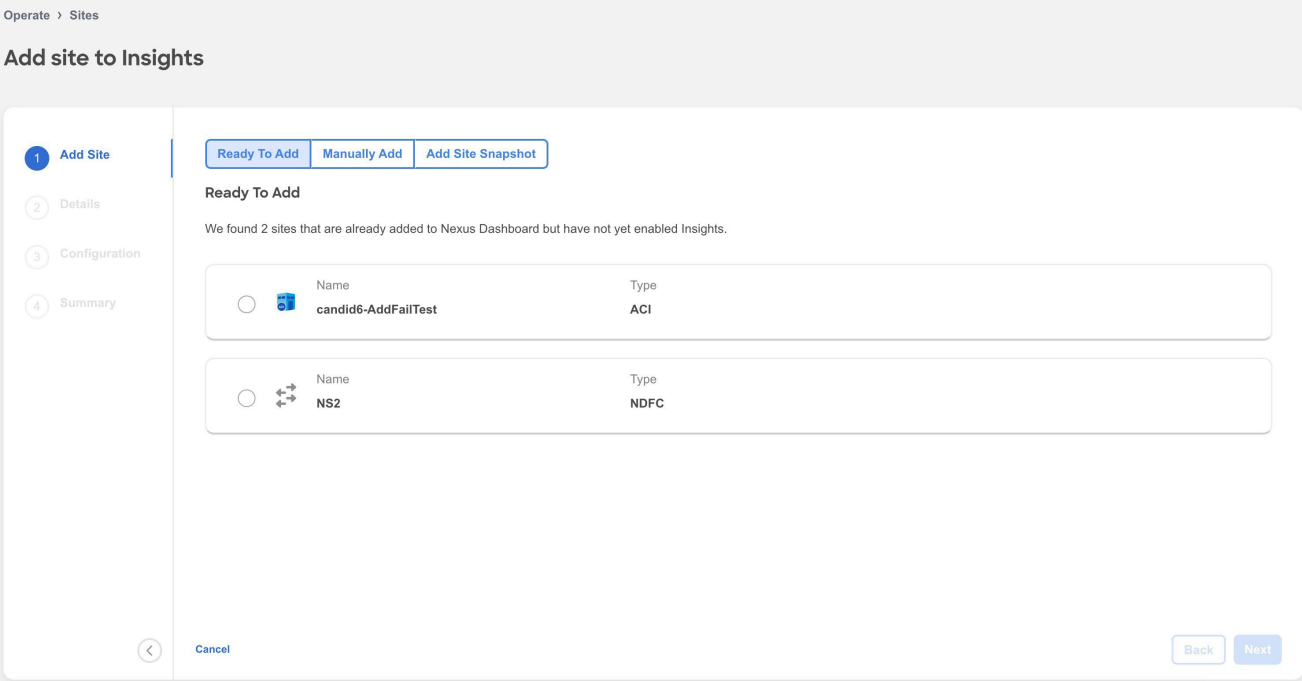
- オンラインサイト
  - Nexus Dashboard にすでに追加されているサイトを有効にします。Nexus Dashboard クラスタに追加されたサイトは、デフォルトではサービスで有効になっていないため、Nexus Dashboard Insights から直接明示的に有効にする必要があります。
  - Nexus Dashboard にサイトを追加し、Nexus Dashboard Insights の単一のワークフローでサイトを有効にします。
- サイトのスナップショット
  - スナップショット サイトを追加します。

# オンライン NDFC サイトの追加

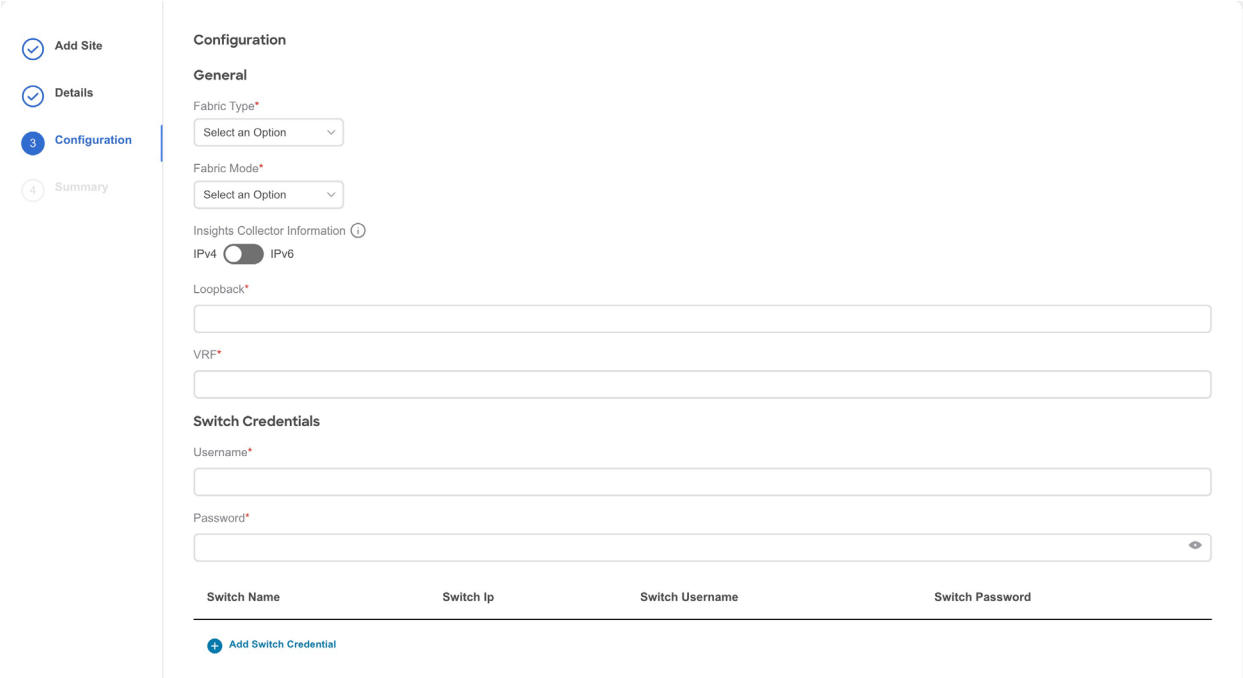
1. **[**管理（**Manage**）**]** > **[** サイト（**Sites**）**]** に移動します。
2. [サイトの追加（Add Site）] をクリックします。
   a. 初めて {CiscoNIRShortName} にサイトを追加する場合は、次のメッセージが表示されます。**[**サイトの追加（**Add Site**）**]** をクリックして続行します。




3. Nexus Dashboard にすでに追加されているサイトを有効にするには、[追加準備完了（**Ready to Add**）] を選択します。Nexus Dashboard に追加されたサイトが表示されます。Nexus Dashboard にサイトを追加するには、『Cisco Nexus Dashboard Sites Management』を参照してください。




4. [追加準備完了（**Read to Add**）] の次のフィールドを入力します。
   a. サイトを選択します。
   b. [次へ（**Next**）] をクリックします。
   c. マップからサイトの場所を選択して、Nexus Dashboard でサイトを識別します。
   d. [次へ（**Next**）] をクリックします。




e. **[ファブリック タイプ（Fabric Type）]** ドロップダウン メニューから、ファブリック タイプを選択します。**[Classic]**、**[VXLAN]**または**[SR-MPLS]**の選択肢があります。NX-OS ファブリックで SR-MPLS のフローを設定するには、SR-MPLS のオプションを選択します。Enhanced Classic LAN は NDFC サイトではサポートされていません。

f. **[ファブリック モード（Fabric Mode）]** ドロップダウン メニューから、ファブリック モードを選択します。オプションは、**[管理（Managed）]** または **[モニター（Monitored）]** です。管理対象モードでは、Nexus Dashboard Insights はファブリック内のすべてのスイッチにテレメトリ設定を展開します。モニター対象モードでは、Nexus Dashboard Insights はファブリック内のすべてのスイッチにテレメトリ設定を展開しません。

g. トグルを使用して、IPv4 または IPv6 を選択してサイトをオンボードします。Nexus Dashboard Insights は、この設定に基づいて、このサイトからテレメトリを受信するようにコレクタを構成します。この設定は、サイトのIPアドレス構成と一致している必要があります。

h. **[ループバック（Loopback）]** フィールドに、Cisco Nexus Dashboard のインバンド IP アドレスへの接続を提供するスイッチに設定されているループバックを入力します。

i. **[VRF]** フィールドに、ループバック インターフェイスに関連付けられた VRF 名を入力します。これは、Nexus ダッシュボードのインバンド IP アドレスへの接続を提供する VRF です。

> デフォルトおよびデフォルト以外のVRFがサポートされています。VXLAN/EVPNファブリックでは、これらはアンダーレイの一部である必要があります。

j. スイッチ ログイン情報の**[ユーザー名（User Name）]** と **[パスワード（Password）]** フィールドで、追加するサイトで管理者権限を持つ LAN ユーザーのログイン情報を示します。

k. リストにスイッチを追加し、スイッチのログイン情報が上記のデフォルトのログイン情報と一致しない場合にのみ、**[スイッチ ログイン情報の追加（Add Switch Creditials）]** をクリックします。

   i. **[スイッチ名（Switch Name）]** フィールドに、スイッチの名前を入力します。

   ii. **[スイッチIP（Switch IP）]** フィールドに、スイッチのIPアドレスを入力します。

   iii. **[スイッチ ユーザー名（Switch Username）]** フィールドに、スイッチのユーザー名を入力します。

   iv. **[スイッチ パスワード（Switch Password）]** フィールドに、パスワードを入力します。

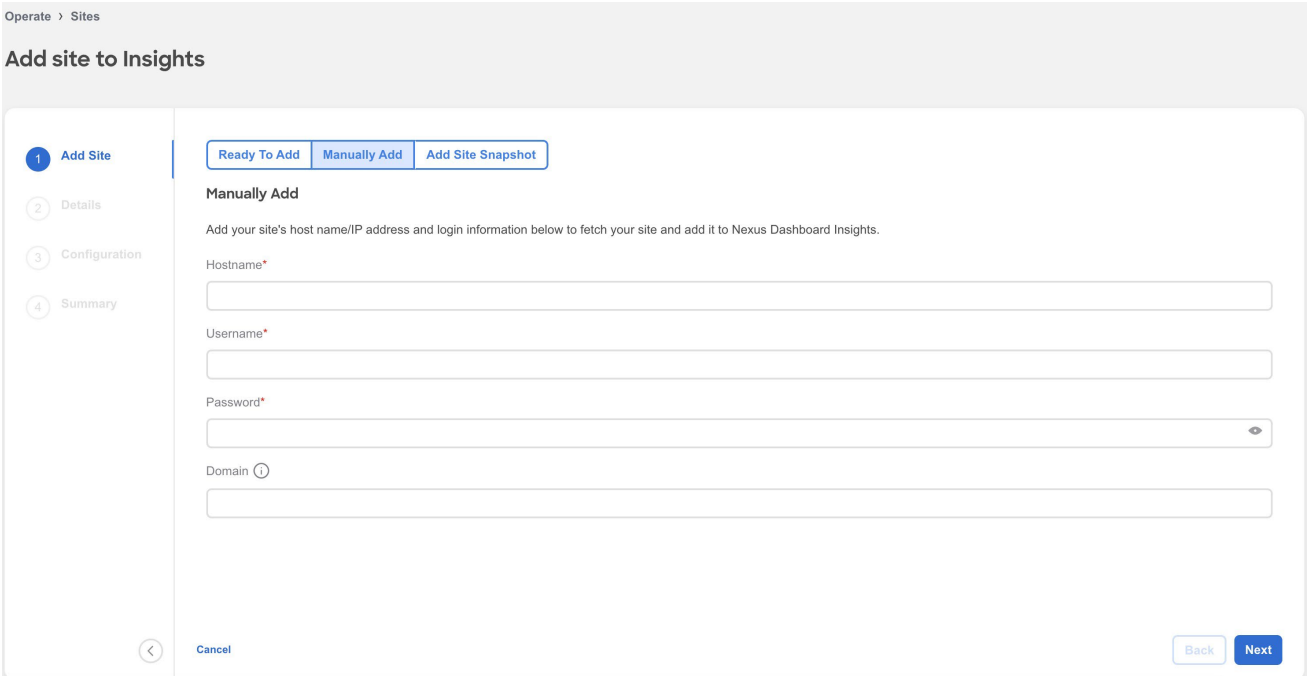
l. チェックマークをオンにしてエントリを追加し、必要に応じてスイッチを追加します。

m. **[次へ（Next）]** をクリックします。

n. 設定を確認します。

o. [送信（Submit）] をクリックします。

5. Nexus Dashboard にサイトを追加し、Nexus Dashboard Insights を使用してサイトを有効にするには、**[手動で追加（Manually Add）]** を選択します。




6. **[手動で追加（Manually Add）]** の次のフィールドを入力します。

   a. **[ホスト名（Hostname）]** フィールドに、サイトのコントローラとの通信に使用する IP アドレスを入力します。

   b. **[ユーザー 名（User Name）]** と **[パスワード（Password）]** フィールドに、追加する管理者権限を持つユーザーのログイン情報を指定します。

   c. **[ドメイン（Domain）]** フィールドで、コントローラのログイン ドメイン名を入力します。

   d. **[次へ（Next）]** をクリックします。

   e. Nexus Dashboard でサイトを識別するためのサイト名を入力します。

   f. マップからサイトの場所を選択して、Nexus Dashboard でサイトを識別します。

   g. **[次へ（Next）]** をクリックします。

   h. **[ファブリック タイプ（Fabric Type）]** ドロップダウン メニューから、ファブリック タイプを選択します。**[Classic]**、**[VXLAN]**または**[SR-MPLS]**の選択肢があります。NX-OS ファブリックで SR-MPLS のフローを設定するには、SR-MPLS のオプションを選択します。Enhanced Classic LAN は NDFC サイトではサポートされていません。

   i. **[ファブリック モード（Fabric Mode）]** ドロップダウン メニューから、ファブリック モードを選択します。オプションは、**[管理（Managed）]** または **[モニター（Monitored）]** です。管理対象モードでは、Nexus Dashboard Insights はファブリック内のすべてのスイッチにテレメトリ設定を展開します。モニター対象モードでは、Nexus Dashboard Insights はファブリック内のすべてのスイッチにテレメトリ設定を展開しません。

   j. トグルを使用して、IPv4 または IPv6 を選択してサイトをオンボードします。Nexus Dashboard Insights は、この設定に基づいて、このサイトからテレメトリを受信するようにコレクタを構成します。この設定は、サイトのIPアドレス構成と一致している必要があります。

   k. **[ループバック（Loopback）]** フィールドに、Cisco Nexus Dashboard のインバンド IP アドレス

への接続を提供するスイッチに設定されているループバックを入力します。

l. **[VRF]** フィールドに、ループバック インターフェイスに関連付けられた VRF 名を入力します。これは、Nexus ダッシュボードのインバンド IP アドレスへの接続を提供する VRF です。

> デフォルトおよびデフォルト以外のVRFがサポートされています。VXLAN/EVPNファブリックでは、これらはアンダーレイの一部である必要があります。

m. スイッチ ログイン情報の**[**ユーザー名（**User Name**）**]** と **[**パスワード（**Password**）**]** フィールドで、追加するサイトで管理者権限を持つ LAN ユーザーのログイン情報を示します。

n. リストにスイッチを追加し、スイッチのログイン情報が上記のデフォルトのログイン情報と一致しない場合にのみ、**[**スイッチ ログイン情報の追加（**Add Switch Creditials**）**]** をクリックします。

   i. **[**スイッチ名（**Switch Name**）**]** フィールドに、スイッチの名前を入力します。

   ii. **[**スイッチ**IP**（**Switch IP**）**]** フィールドに、スイッチのIPアドレスを入力します。

   iii. **[**スイッチ ユーザー名（**Switch Username**）**]** フィールドに、スイッチのユーザー名を入力します。

   iv. **[**スイッチ パスワード（**Switch Password**）**]** フィールドに、パスワードを入力します。

o. チェックマークをオンにしてエントリを追加し、必要に応じてスイッチを追加します。

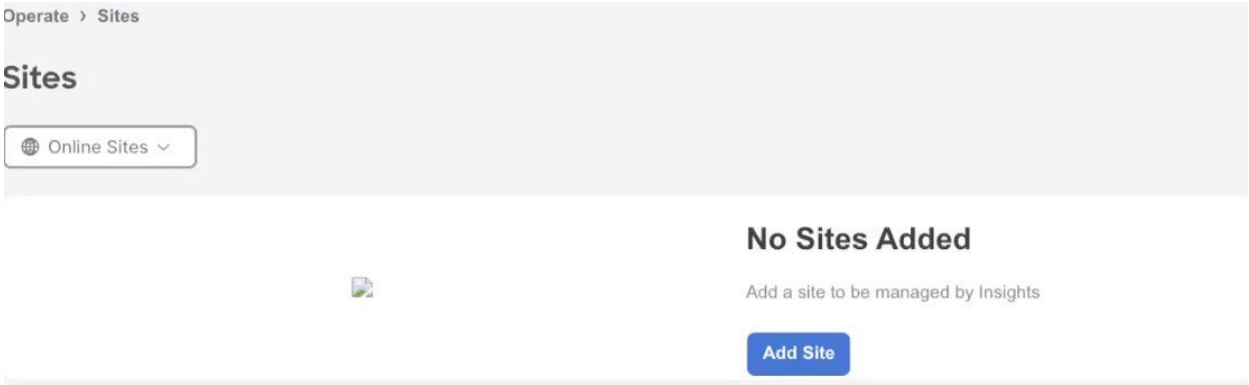
p. **[**次へ（**Next**）**]** をクリックします。

q. 設定を確認します。

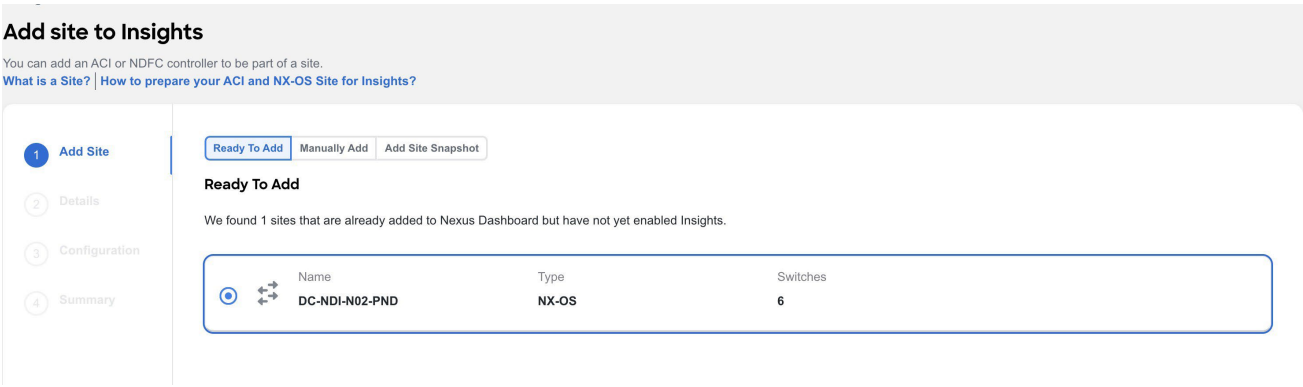
r. [送信（Submit）] をクリックします。

# コントローラなしでオンライン NX-OS サイトを追加する

1. **[**管理（**Manage**）**]** > **[** サイト（**Sites**）**]** に移動します。
2. [サイトの追加（Add Site）] をクリックします。
   a. 初めて {CiscoNIRShortName} にサイトを追加する場合は、次のメッセージが表示されます。**[**サイトの追加（**Add Site**）**]** をクリックして続行します。



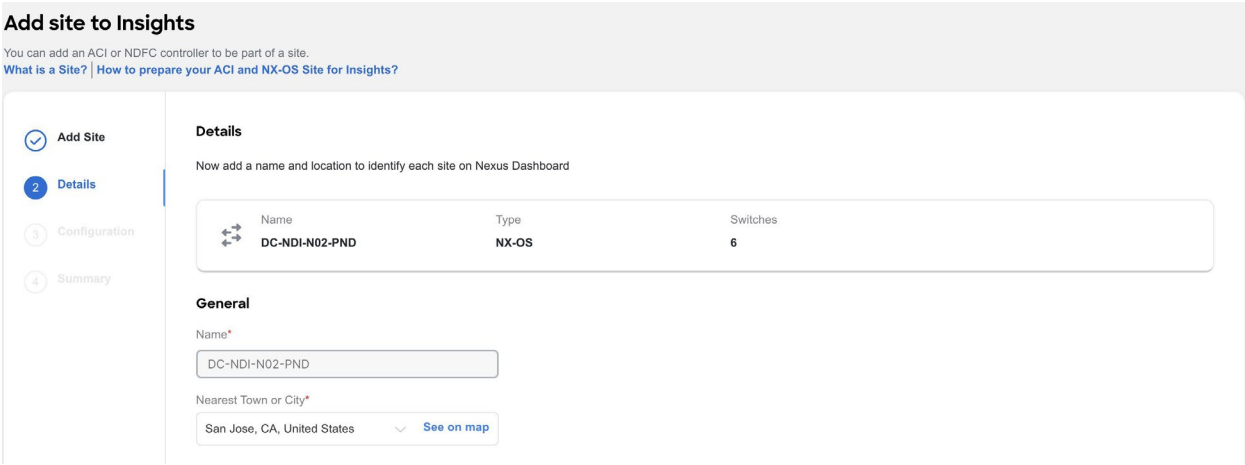

3. Nexus Dashboard にすでに追加されているサイトを有効にするには、**[**追加準備完了（**Ready to Add**）**]** を選択します。Nexus Dashboard に追加されたサイトが表示されます。Nexus Dashboard にサイトを追加するには、『Cisco Nexus Dashboard Sites Management』を参照してください。
4. **[**追加準備完了（**Read to Add**）**]** の次のフィールドを入力します。



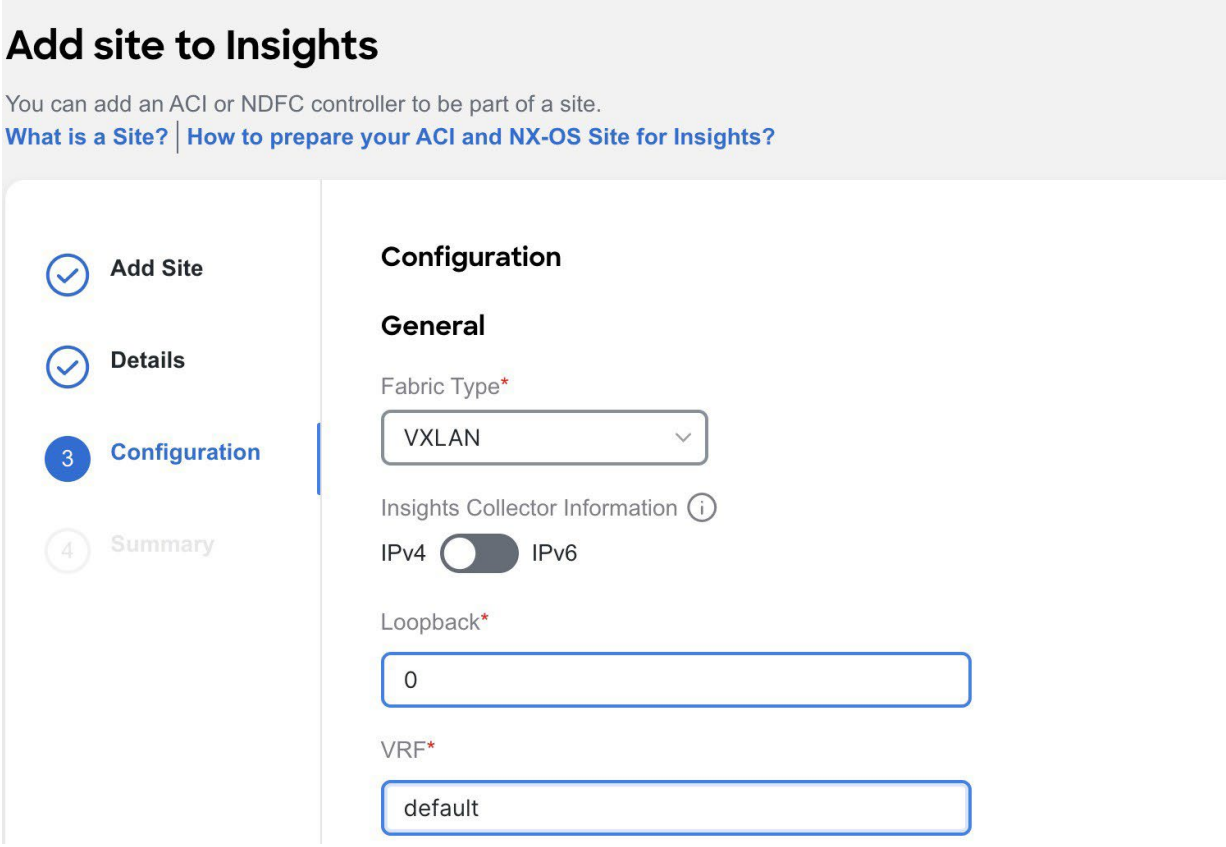

a. NX-OS サイトを選択します。

b. **[次へ（Next）]** をクリックします。

c. マップからサイトの場所を選択して、Nexus Dashboard でサイトを識別します。




d. **[次へ（Next）]** をクリックします。



e. **[ファブリック タイプ（Fabric Type）]** ドロップダウン メニューから、ファブリック タイプを選択します。**[Classic]**、**[VXLAN]**または**[SR-MPLS]**の選択肢があります。NX-OS ファブリックで SR-MPLS のフローを設定するには、SR-MPLS のオプションを選択します。

f. トグルを使用して、IPv4 または IPv6 を選択してサイトをオンボードします。Nexus Dashboard Insights は、この設定に基づいて、このサイトからテレメトリを受信するようにコレクタを構成します。この設定は、サイトのIPアドレス構成と一致している必要があります。

g. **[ループバック（Loopback）]** フィールドに、Cisco Nexus Dashboard のインバンド IP アドレスへの接続を提供するスイッチに設定されているループバックを入力します。

h. **[VRF]** フィールドに、ループバック インターフェイスに関連付けられた VRF 名を入力します。これは、Nexus ダッシュボードのインバンド IP アドレスへの接続を提供する VRF です。

> デフォルトおよびデフォルト以外のVRFがサポートされています。VXLAN/EVPNファブリックでは、これらはアンダーレイの一部である必要があります。

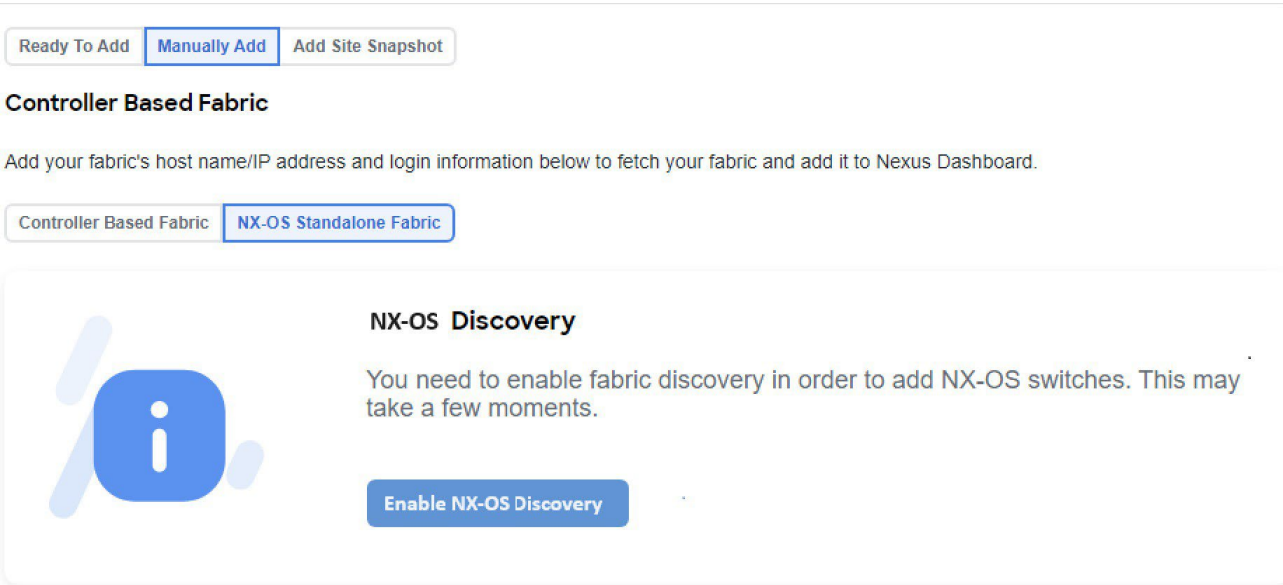
i. **[次へ（Next）]** をクリックします。

j. 設定を確認します。

k. [送信（Submit）] をクリックします。

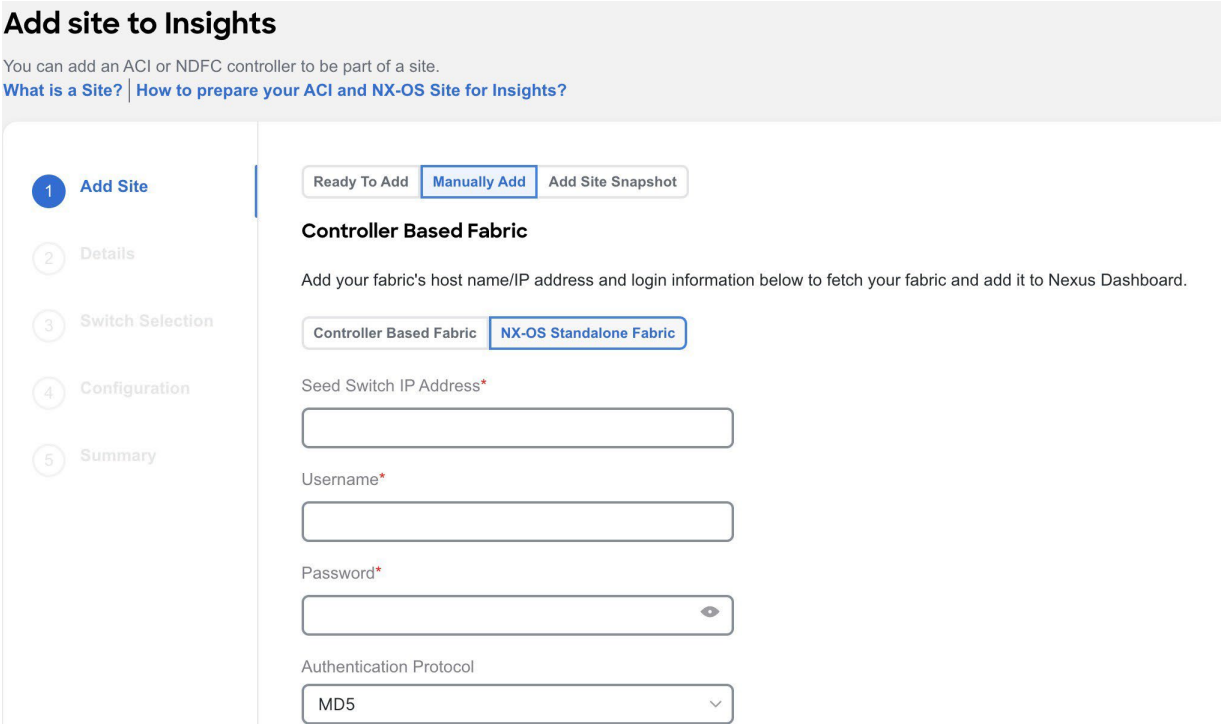
5. Nexus Dashboard にサイトを追加し、Nexus Dashboard Insights を使用してサイトを有効にするには、**[手動で追加（Manually Add）]** を選択します。

6. **[手動で追加（Manually Add）]** の次のフィールドを入力します。




a. **[NX-OS スタンドアロン ファブリック（NX-OS Standalone Fabric）]** を選択します。

b. **[NX-OS 検出の有効化（Enable NX-OS Discovery）]** をクリックして、Nexus Dashboard で NX-OS 検出を有効にします。

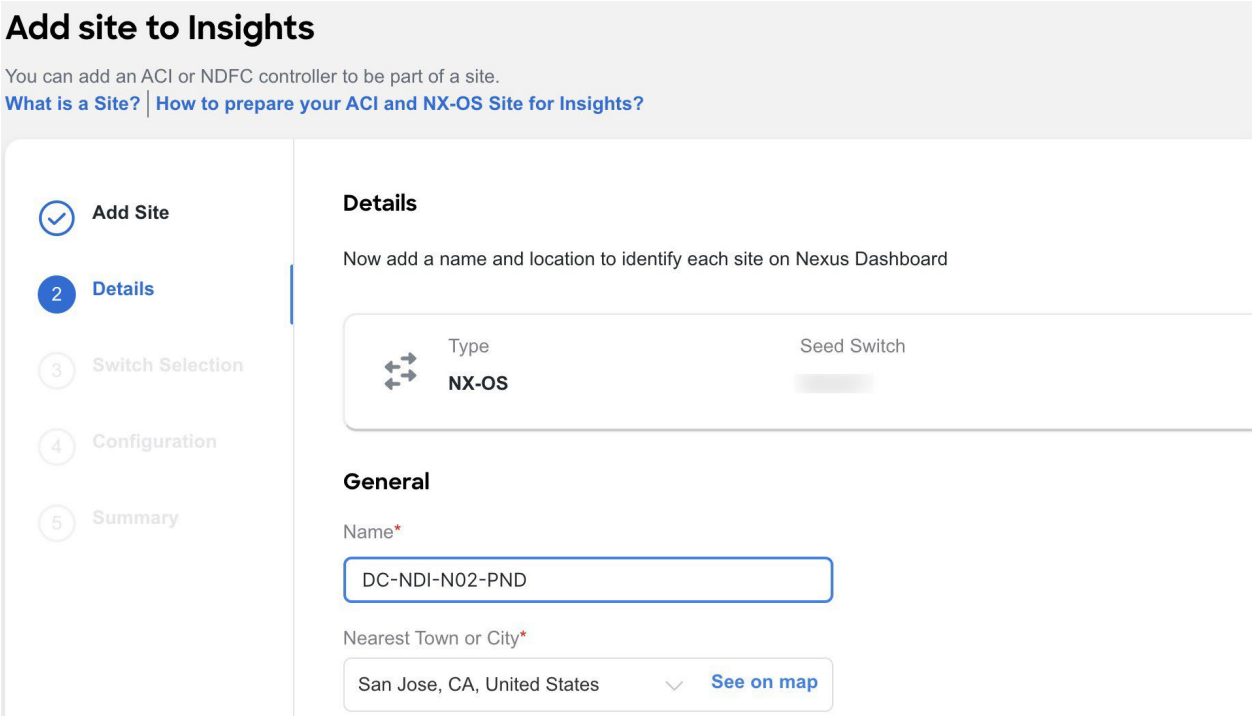



c. [シード スイッチ **IP** アドレス（**Seed Switch IP Address**）] フィールドにシード スイッチ管理 インターフェイスの IP アドレスを入力します。

d. [ユーザー名（**User Name**）]と [パスワード（**Password**）] フィールドに、追加するスイッチで管理者権限を持つユーザーのログイン情報を指定します。

e. [認証プロトコル（**Authentication Protocol**）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

f. [次へ（**Next**）] をクリックします。

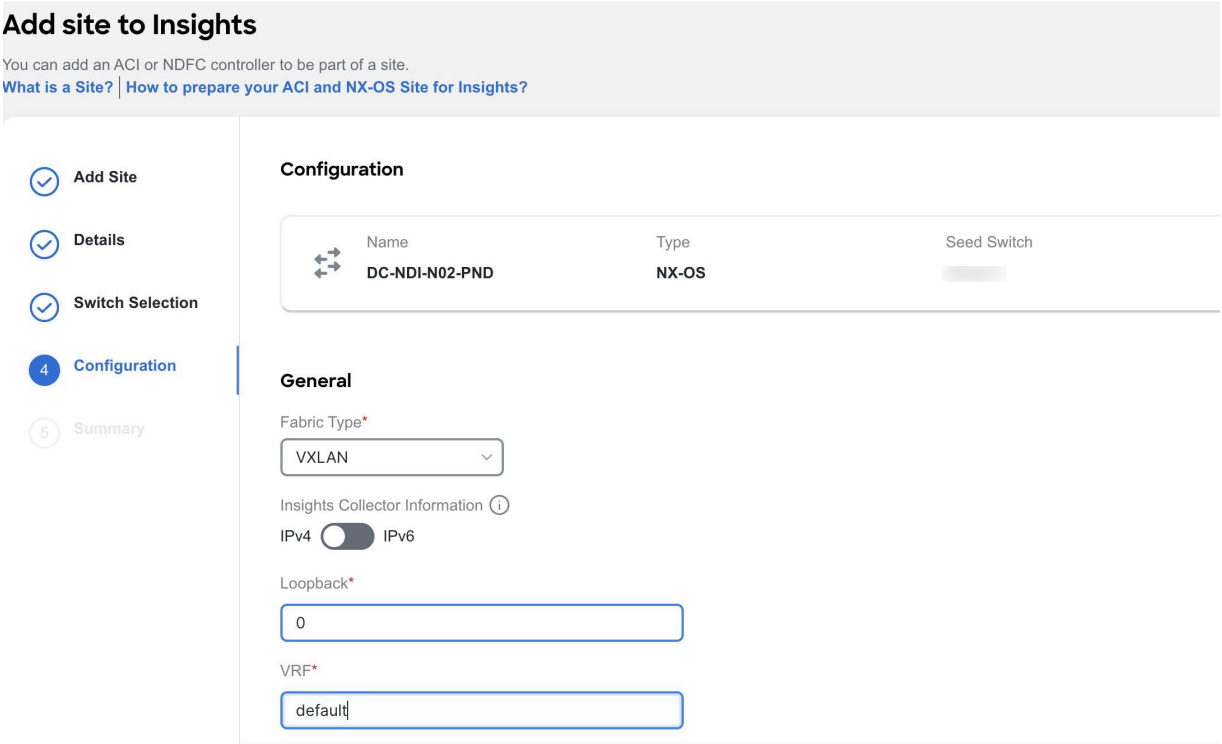



g. Nexus Dashboard でサイトを識別する NX-OS サイト名を入力します

h. マップから NX-OS サイトの場所を選択して、Nexus Dashboard でサイトを識別します。

i. サイトに追加するスイッチを選択します

j. **[次へ（Next）]** をクリックします。




k. **[ファブリック タイプ（Fabric Type）]** ドロップダウン メニューから、ファブリック タイプを選択します。**[Classic]**、**[VXLAN]**または**[SR-MPLS]**の選択肢があります。NX-OS ファブリックで SR-MPLS のフローを設定するには、SR-MPLS のオプションを選択します。

l. トグルを使用して、IPv4 または IPv6 を選択してサイトをオンボードします。Nexus Dashboard Insights は、この設定に基づいて、このサイトからテレメトリを受信するようにコレクタを構成します。この設定は、サイトのIPアドレス構成と一致している必要があります。

m. **[ループバック（Loopback）]** フィールドに、Cisco Nexus Dashboard のインバンド IP アドレスへの接続を提供するスイッチに設定されているループバックを入力します。

n. **[VRF]** フィールドに、ループバック インターフェイスに関連付けられた VRF 名を入力します。これは、Nexus ダッシュボードのインバンド IP アドレスへの接続を提供する VRF です。

> デフォルトおよびデフォルト以外のVRFがサポートされています。VXLAN/EVPNファブリックでは、これらはアンダーレイの一部である必要があります。

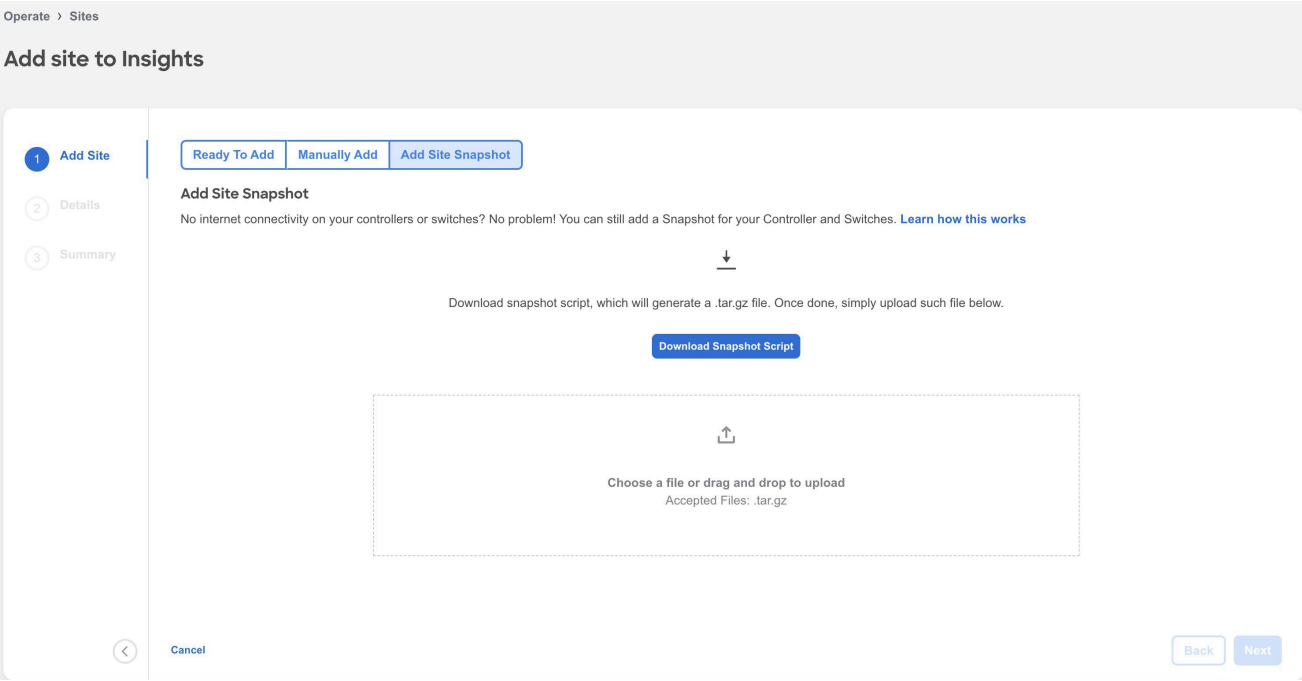
o. **[次へ（Next）]** をクリックします。

p. 設定を確認します。

q. [送信（Submit）] をクリックします。

# スナップショット サイトを追加します。

1. **[管理（Manage）]** > **[サイト（Sites）]** に移動します。
2. [サイトの追加（Add Site）] をクリックします。
3. スナップショット サイトを追加するには、**[サイトのスナップショットの追加（Add Site Snapshot）]** を選択します。



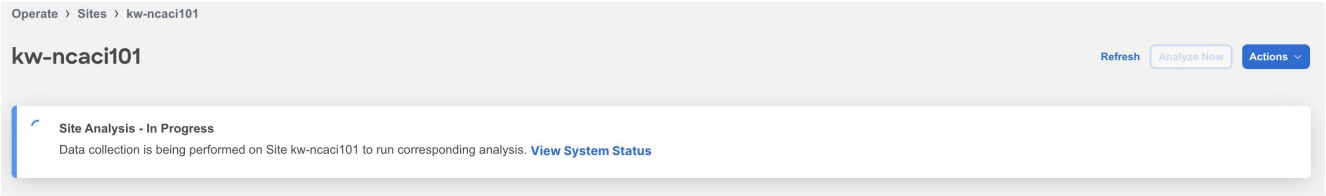

4. [スナップショット スクリプトのダウンロード（**Download Snapshot Script**）] をクリックして、data-collectors.tar.gz をマシンにダウンロードします。
5. ダウンロードしたファイルを抽出し、データ収集スクリプトを実行します。readme.md ファイルのセクションの指示に従ってください。スクリプトが正常に完了すると、データは <filename>.tar.gz ファイルに収集されます。

> 収集スクリプトを使用するには、システムに Python3 がインストールされている必要があります。

6. Nexus Dashboard Insightsにファイルをアップロードし、[次へ（**Next**）] をクリックします。
7. Nexus Dashboard でサイトを識別するためのサイト名を入力します。
8. マップからサイトの場所を選択して、Nexus Dashboard でサイトを識別します。
9. [次へ（**Next**）] をクリックします。
10. 設定を確認します。
11. [送信（Submit）] をクリックします。

# サイト分析

サイトがオンボーディングされ、完全に準備されると、Nexus Dashboard Insights はサイト分析を開始してサイトからデータを収集し、[サイト（**Sites**）] ページにサイト情報を表示します。詳細については、「サイト」を参照してください。[サイト分析（Site Analysis）] バナーに分析の進行状況が表示されます。分析の実行時間は、ファブリックのサイズによって異なります。




ステータスを表示するには、[システム ステータス（System Status）] をクリックします。「システム ステータス」を参照してください。

サイト分析中に、テレメトリ収集、アシュアランス分析、バグ スキャン、およびベスト プラクティス分析が自動的に実行されます。「アシュアランス分析 と バグスキャン」を参照してください。

# 保証分析

アシュアランス分析には、サイトからのデータ収集、モデルを作成するための収集データを使用した分析の実行、結果の生成が含まれています。

- アシュアランス分析は、リアルタイムでアシュアランスを提供します。オンライン サイトのアシュアランス分析では、データ収集、モデルの生成、および結果の生成は同時に実行されます。収集されたデータは収集後ただちに分析されて、結果が生成されます。これは、ユーザーが指定した一定の時間間隔後に繰り返されます。オンライン サイトの場合、アシュアランス分析は 2 時間ごとに自動的に実行されます。スケジュールは、ファブリックのサイズとスケールによって決まります。大規模なファブリックの場合、アシュアランス分析は 3 ～ 4 時間ごとに自動的に実行されます。
- スナップショット サイトの場合、1 回限りのアシュアランスが提供されます。このアシュアランス分析により、データ収集段階を分析段階から切り離すことができます。データは Python スクリプトを使用して収集され、収集されたデータは Nexus Dashboard Insights にアップロードされて、1 回限りのアシュアランスが提供されます。収集されたデータは、後で分析することもできるため、ユーザーは変更管理時間帯にデータを収集し、後で分析を実行できます。

# アシュアランス分析の注意事項と制約事項

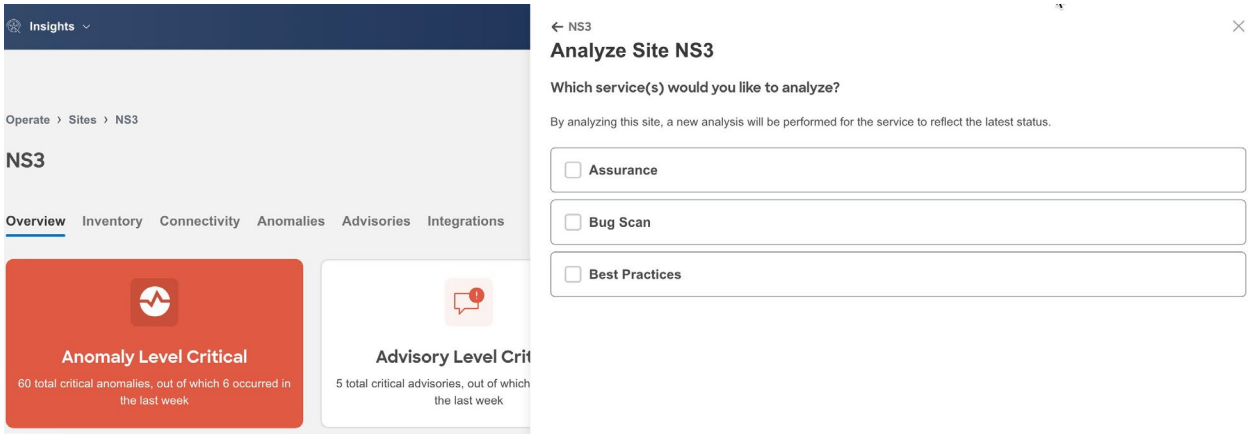
- サイト グループからアシュアランス分析を取得し、raw データセットをエクスポートしてファイルをサイト グループにアップロードする場合、アップロードされたファイルのアシュアランス分析ではアシュアランス関連の異常のみ生成されます。
- 現在、スナップショット サイトのアシュアランス分析を開始する場合、すでに進行中のサイトのアシュアランス分析を同時に続行できます。アシュアランス分析はすべて、動作を中断することなく実行されます。
- アラート ルールとコンプライアンス ルールは、スナップショット サイトのアシュアランス分析で有効です。

# オンデマンド分析

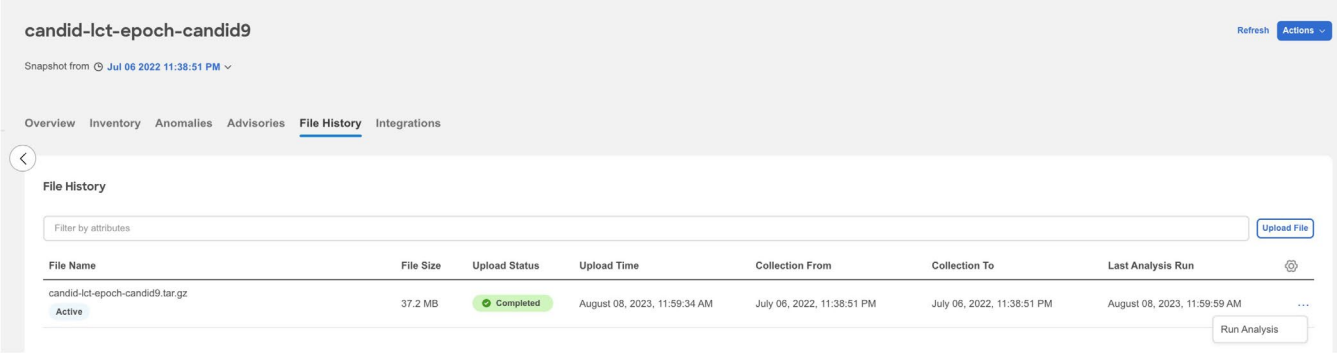
オンライン サイトの場合、アシュアランス分析は自動的に実行されますが、いつでもリクエストすることもできます。これは、サイト内の 1 つ以上の問題を解決し、次の自動実行を待たずに Nexus Dashboard Insights で最新の異常とアドバイザリ情報をポーリングする場合に役立ちます。

同様に、バグ スキャンまたはベスト プラクティスのオンデマンド分析を実行して、最新のステータスを反映することもできます。

1. **[**管理（**Manage**）**]** > **[** サイト（**Sites**）**]** に移動します。
2. ドロップダウン リストからオンラインまたはスナップショット サイトを選択します。
3. オンライン サイトの場合、サイト名をクリックすると、詳細が表示されます。
   a. **[**今すぐ分析（**Analyze Now**）**]** をクリックします。
   b. サービスを選択します。バグ スキャンとベスト プラクティスの場合は、スイッチを選択し、**[**今すぐ実行（**Run Now**）**]** をクリックします。



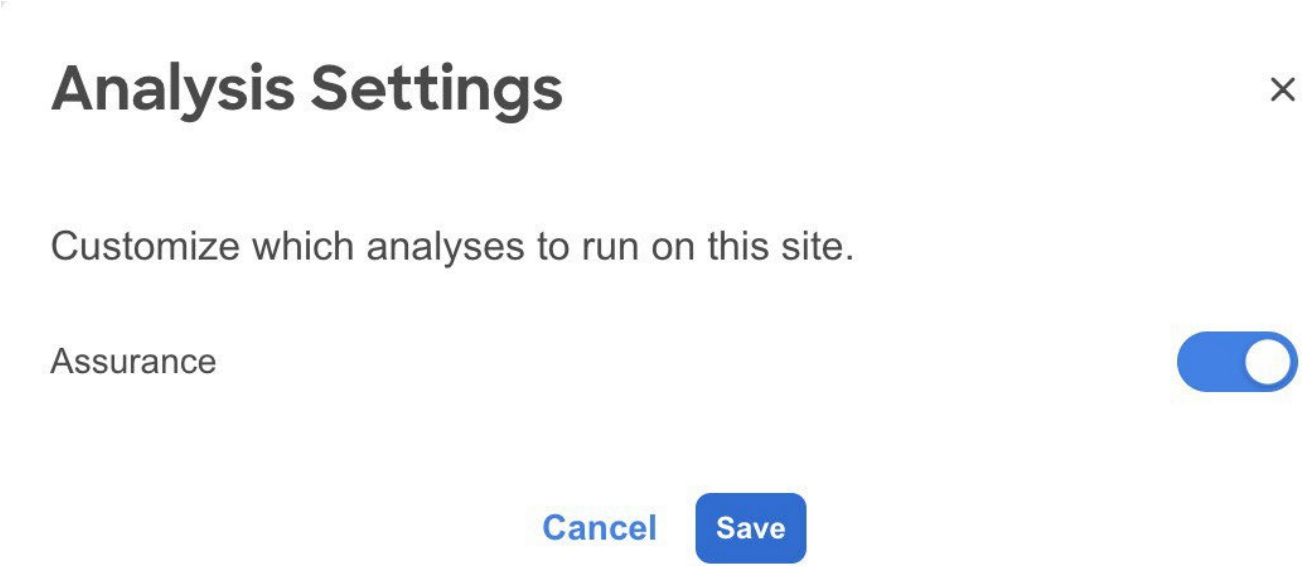

4. スナップショット サイトの場合、サイト名をクリックすると、詳細が表示されます。
5. **[**ファイル履歴（**File History**）**]** をクリックします。
6. **[**ファイル履歴（**File History**）**]** テーブルで、省略記号アイコンをクリックし、**[**分析の実行（**Run Analysis**）**]** を選択します。




# アシュアランス分析を有効にする

また、自動的にスケジュールされたアシュアランス分析ジョブを有効または無効化にすることもできます。

1. **[**管理（**Manage**）**]** > **[** サイト（**Sites**）**]** に移動します。
2. ドロップダウン リストからオンライン サイトを選択します。
3. サイト名をクリックすると、詳細が表示されます。
4. [アクション（Actions）] メニューから **[**システム ステータス（**System Status**）**]** を選択します。
5. [アクション（Actions）] メニューから **[**設定の分析（**Analyze Settings**）**]** を選択します。
6. トグルを活用して、スケジュールされたアシュアランス分析ジョブを有効または無効化にします。
7. **[**保存（**Save**）**]** をクリックします。




# バグスキャン

Nexus Dashboard Insightsは、すべてのデバイスからテクニカル サポート情報を収集し、既知の署名セットに対して実行し、対応する欠陥と PSIRT にフラグを立てます。Nexus Dashboard Insightsは、PSIRTのアドバイザリと欠陥の異常も生成します。メタデータのサポートの詳細については、「異常およびアドバイザリ」を参照してください。

バグ スキャン機能は、サイト内のデバイスからテクニカル サポート ログを収集し、ヒットした可能性のあるバグをスキャンします。CPU およびメモリの使用状況が設定されたしきい値 65% 以下であれば、テクニカル サポートのログが収集され、デバイスのバグ スキャンが実行されます。CPU およびメモリの使用状況が設定されたしきい値を超えている場合、そのデバイスはバグ スキャンから除外され、最終的に次のデフォルトのバグ スキャン、またはそのデバイスのオンデマンド バグ スキャンを実行する際に再検討されます。

デバイスのノードの相互作用が正常でない場合、ログ収集のためにバグスキャンを実行するデバイスを選択できません。ジョブを設定するデバイスを選択できません。

サイトのオンデマンドバグ スキャンを実行することもできます。「 オンデマンド分析」を参照してください。

## デフォルトのバグスキャン

バグ スキャンは、Nexus Dashboard Insights に導入準備されたすべてのサイトに対して実行され、各デバイスに対して 7 日ごとに自動スケジュールされます。このスケジュールは固定されており、カスタマイズできません。

バグ スキャンは、前回のバグ スキャン、またはバグ スキャンが以前に実行されていない場合はオンボーディング時間に基づいて、サイトに含まれるデバイスで実行されます。最後のバグ スキャンからの経過時間が長いデバイスが優先されます。デバイスでバグ スキャンが実行されると、成功したか失敗したかにかかわらず、次の 7 日間は同じデバイスに対して別のバグ スキャンが実行されません。

バグ スキャンは、デバイスの CPU とメモリのメトリックがストリーミングされ、使用率が 65% 未満の場合にのみ、デバイスで実行するように自動スケジュールされます。

ただし、オンデマンド バグ スキャンは例外であり、自動スケジュールされた実行よりも優先され、ユーザーが開始するため、CPU とメモリのメトリックは考慮されません。Nexus Dashboard ノードで使用可能なリソースに基づいて自動スケジュールされたバグ スキャンが進行中で、

オンデマンド バグ スキャンが開始されると、オンデマンド バグ スキャンは、現在のバグ スキャンの進行中または現在のバグ スキャンの完了後に開始されます。

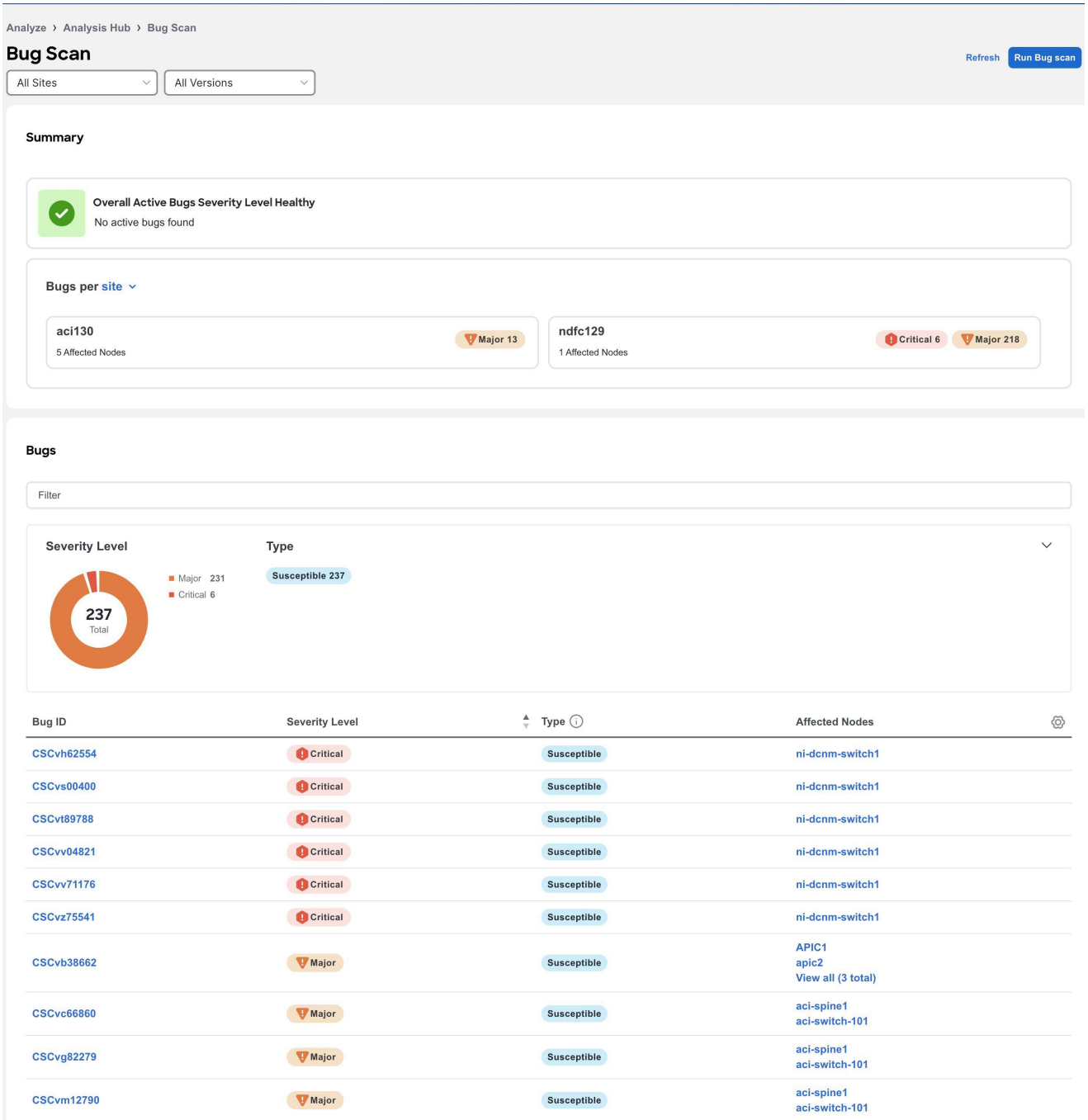
特定のデバイスで実行できるバグ スキャンは一度に 1 つだけです。ただし、バグ スキャンがすでに進行中の 1 つのデバイス セットがある場合、2 番目の（自動スケジュールまたはオンデマンドの）バグ スキャンは、Nexus Dashboard Insights に十分なリソースがある場合にのみ実行できます。それ以外の場合は、リソースが使用可能になるとすぐに保留され、開始されます。

# アクティブ バグと影響を受けやすいバグの表示

バグ スキャン機能は、サイト内のデバイスからテクニカル サポート ログを収集し、ヒットした可能性のあるバグをスキャンします。Nexus Dashboard Insights リリース6.4.1 以降では、バグスキャンの完了後に、ネットワークに影響を与える現用系バグと影響を受ける可能性のあるバグを表示できます。

- [アクティブ バグ（Active Bugs）] : 構成ファイルおよびテクニカル サポート ファイルに基づいてネットワークで検出された、バージョンに存在するバグ。
- [影響を受けやすいバグ（Susceptible Bugs）] : ネットワークに影響を与える可能性のある、バージョンに存在するバグ。

1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**バグ スキャン（**Bug Scan**）**]** の順に選択します。
2. ドロップダウン メニューから、1 つまたは複数のオンライン サイトを選択します。
3. ドロップダウン メニューからソフトウェア バージョンを選択します。選択したサイトとソフトウェア バージョンの現用系バグと影響を受けやすいバグが表示されます。

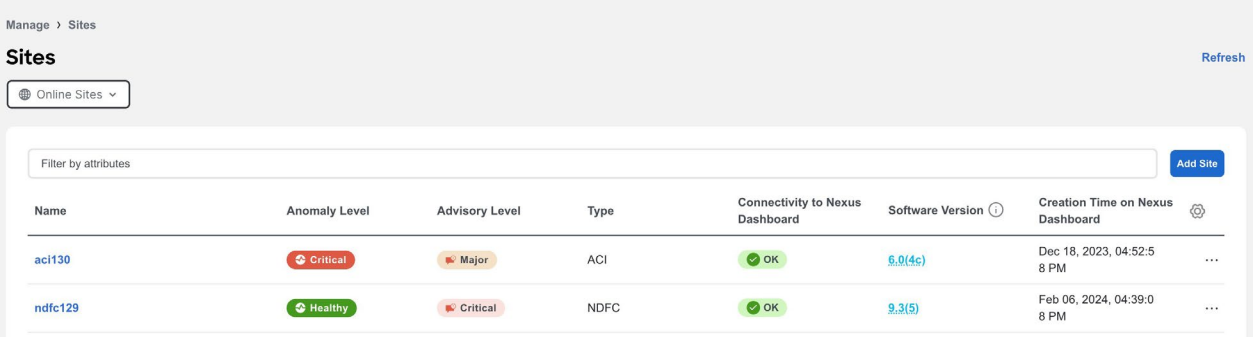



4. [概要（Summary）] エリアには、現用系バグ全体が重大度別に表示されます。ドロップダウン メニューを使用して、サイトまたはソフトウェア バージョンごとのバグを表示することもできます。
5. [バグ（Bugs）] エリアで、検索バーを使用して、バグ ID、重大度レベル、タイプ、および影響を受けるノードでバグをフィルタ処理します。
6. 重大度レベルのドーナツ チャートには、重大度がクリティカル、重大、および警告のバグの合計数が表示されます。、バグテーブルにフィルタ処理されたバグが表示されます。列の見出しをクリックして、テーブルのバグを並べ替えます。
7. 歯車アイコンをクリックして、テーブルの列を構成します。
8. [バグ識別子 （Bug ID）] をクリックしてバグの詳細を表示します。
9. **[**バグ スキャンの実行（**Run Bug Scan**）**]** をクリックして、オンデマンドバグ スキャンを実行します。サイトを選択し、**[**今すぐ実行（**Run Now**）**]**をクリックします。 「オン デマンド分析」を参照してください。

## 個々のサイトのアクティブなバグと影響を受けやすいバグの表示

Nexus Dashboard Insights では、次の方法で個々のサイトのバグを表示することもできます。

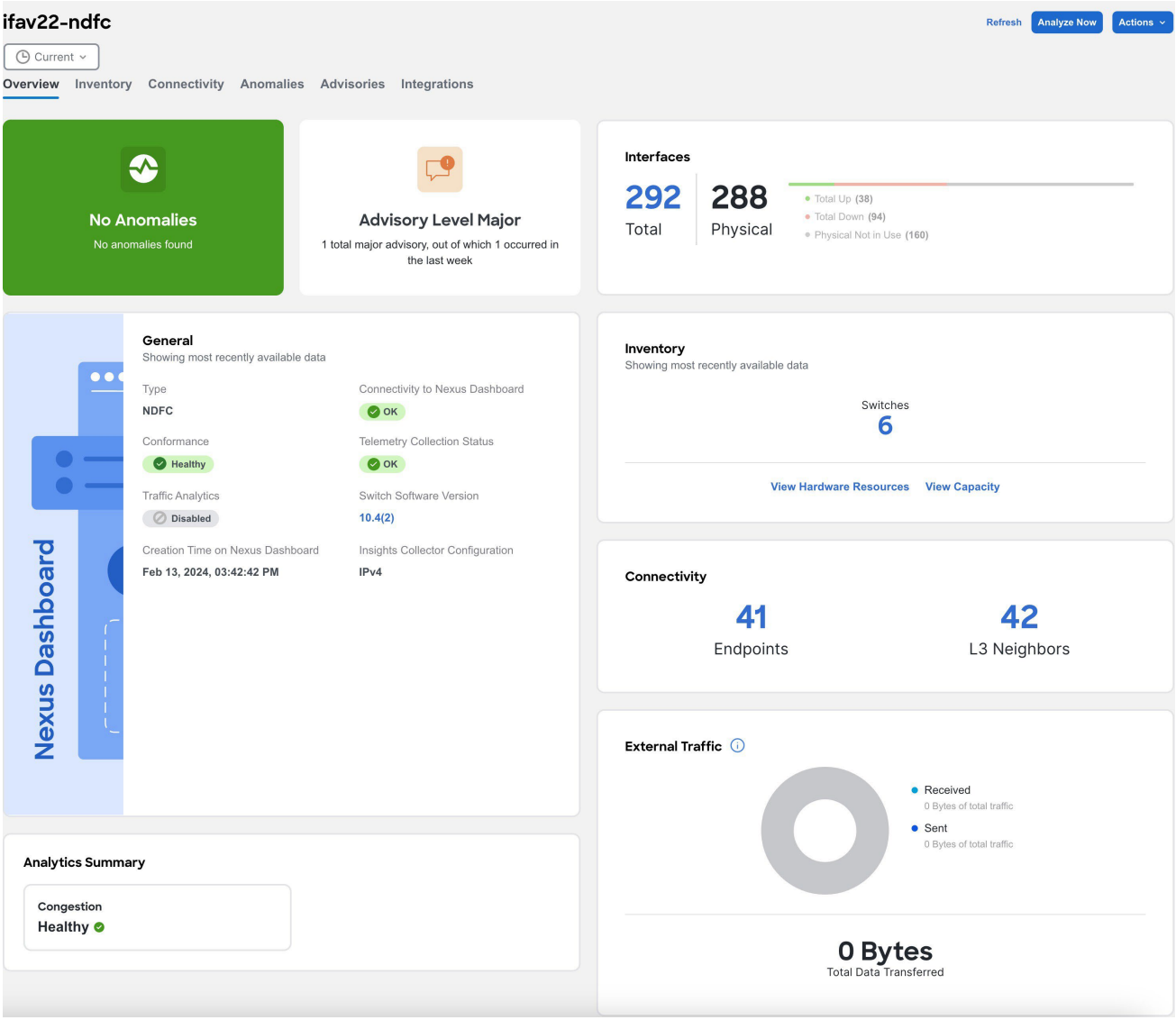
1. **[管理（Manage）] > [サイト（Sites）]** に移動します。
2. ドロップダウン リストから **[オンライン サイト（Online Sites）]** を選択します。




3. ソフトウェア バージョン列で、ソフトウェア バージョンにカーソルを合わせ、**[バグの表示（View Bugs）]** をクリックして、そのサイトの現用系のバグと影響を受けやすいバグを表示します。
4. [アクション（Actions）] ドロップダウンメニューから、**[バグ スキャンの実行（Run Bug Scan）]** をクリックして、オンデマンドのバグ スキャンを実行します。 「オン デマンド分析」を参照してください。

または

1. **[管理（Manage）] > [ サイト（Sites）]** に移動します。
2. ドロップダウン リストから **[オンライン サイト（Online Sites）]** を選択します。
3. サイトを選択します。




4. [全般（General）] 領域で、ソフトウェアバージョンにカーソルを合わせ、**[バグの表示（View Bugs）]** をクリックして、そのサイトのアクティブなバグと影響を受けやすいバグを表示します。
5. [アクション（Actions） ] ドロップダウンメニューから、**[バグ スキャンの実行（Run Bug Scan）]** をクリックして、オンデマンドのバグ スキャンを実行します。 「オン デマンド分析」を参照してください。

または

1. **[管理（Manage）]** > **[インベントリ（Inventory）]** の順に選択します。
2. ドロップダウン リストから **[オンライン サイト（Online Sites）]** を選択します。
3. [コントローラ（Controllers）] テーブルで、[ソフトウェア バージョン（Software Version）] 列のソフトウェア バージョンの上にマウスを合わせ、
   **[バグの表示（View Bugs）]** をクリックして、アクティブ バグと影響を受けやすいバグを表示します。
4. **[スイッチ（Switches）]** をクリックします。[スイッチ（Switches）] テーブルで、[ソフトウェア バージョン（Software Version）] 列のソフトウェア バージョンにカーソルを合わせ、**[バグの表示（ View Bugs）]** をクリックして、現用系バグと影響を受けやすいバグを表示します。
5. [アクション（Actions） ] ドロップダウンメニューから、**[バグ スキャンの実行（Run Bug Scan）]** をクリックして、オンデマンドのバグ スキャンを実行します。「オンデマンド 分析」を参照してください。

または

1. **[管理（Admin）] > [サイト ソフトウェア管理（Site Software Management）]** に移動します。
2. [ソフトウェア管理ジョブ（Software Management Jobs）] テーブルで、分析をクリックします。
3. [ファームウェアの概要（Firmware Summary）] エリアで、ノード ターゲット ファームウェアにカーソルを合わせ、**[バグの表示（View Bugs）]** をクリックして、そのサイトのアクティブなバグと影響を受けやすいバグを表示します。
4. [アクション（Actions） ] ドロップダウンメニューから、**[バグ スキャンの実行（Run Bug Scan）]** をクリックして、オンデマンドのバグ スキャンを実行します。 「オン デマンド分析」を参照してください。

# ベストプラクティス

Nexus Dashboard Insights は、サイトからテクニカル サポート情報を収集し、既知の署名セットに対してそれらを実行し、コンプライアンスに対応していない不具合にフラグを付けます。Nexus Dashboard Insights は、顧客の異常リストも生成します。メタデータのサポートの詳細については、「異常およびアドバイザリ」を参照してください。

ベスト プラクティスは、 Nexus Dashboard Insights に導入準備されたすべてのサイトに対して実行され、各デバイスに対して 7 日ごとに自動スケジュールされます。このスケジュールは固定されており、カスタマイズできません。

ベスト プラクティスは、最後のベスト プラクティスに基づいて、または以前にベスト プラクティスが実行されていない場合はオンボーディング時間に基づいて、サイトに含まれるデバイスで実行されます。最後のベスト プラクティスからの経過時間が長いデバイスが優先されます。デバイスでベスト プラクティスを実行すると、成功したか失敗したかにかかわらず、次の 7 日間は同じデバイスに対して別のベスト プラクティスが実行されることはありません。

ただし、オンデマンドのベスト プラクティスは例外であり、自動スケジュールされた実行よりも優先されます。自動スケジュールされたベスト プラクティスが進行中であり、オンデマンドのベスト プラクティスが開始された場合、 Nexus Dashboard ノードで使用可能なリソースに基づいて、現在のベスト プラクティスが進行中または現在のベスト プラクティスの完了の後にオンデマンドのベスト プラクティスが開始されます。

特定のデバイスで実行できるベスト プラクティスは一度に 1 つだけです。ただし、ベスト プラクティスがすでに進行中のデバイスのセットがある場合、 Nexus Dashboard Insightsに十分なリソースがある場合にのみ、2番目の（自動スケジュールまたはオンデマンド）ベスト プラクティスを実行できます。それ以外の場合は、リソースが使用可能になるとすぐに保留され、開始されます。

# オンデマンドのベスト プラクティス

サイトのベスト プラクティスをオンデマンドで実行することもできます。「 オンデマンド分析」を参照してください。

> Nexus Dashboard Insights では、特定のインスタンスで1つのオンデマンド バグ スキャンまたはベスト プラクティス ジョブのみを実行できます。オンデマンドジョブが開始されると、UI がグレー表示になるまで最大 1 分かかります。UI がグレー表示されていないときに別のオンデマンド ジョブをトリガーすると、ジョブは失敗します。

# デバイス コネクタについて

Cisco Nexus Dashboard Insights サービスなどのデータセンターアプリおよびサービスは、Cisco Nexus Dashboard プラットフォームの管理コントローラに組み込まれているデバイスコネクタを介して Cisco

Intersight Cloud ポータルに接続されます。

デバイス コネクタの設定とデバイスの要求については、Cisco Nexus Dashboard ユーザーガイドを参照してください。接続要件については、ネットワーク接続要件を参照してください。

# Nexus Dashboard Insightsのスイッチ設定ステータス

1. **[**管理者（**Admin**）**]** > **[**システム設定（**System Settings**）**]** > **[**システムステータスの詳細（**System Status Details**）**]** に移動します。
2. サイトを選択します。
3. 省略記号アイコンをクリックし、**[**予想される構成（**Expected Configuration**）**]** をクリックします。
4. ユーザーとして、推奨設定を使用して適切なスイッチを設定する必要があります。**[**予想される設定**]**領域から、**[**ソフトウェアテレメトリ**]**および**[**フローテレメトリ**]**の下にある設定を表示およびコピーできます。

## スイッチへのテレメトリ構成の適用

モニター対象モードの NDFC ファブリックの場合、Nexus Dashboard Insights は、次のシナリオでファブリック内のすべてのスイッチにテレメトリ構成を展開しません。

- Nexus Dashboard Insights をアップグレードする場合
- Nexus スイッチをアップグレードする場合

これらのシナリオでは、テレメトリ構成をすべてのスイッチに再適用する必要がありま

す。テレメトリ構成をスイッチに再適用するには、次の手順を活用します。

1. **[**管理者（**Admin**）**]** > **[**システム設定（**System Settings**）**]** > **[**システムステータスの詳細（**System Status Details**）**]** に移動します。
2. サイトを選択します。
3. 省略記号アイコンをクリックし、**[**予想される構成（**Expected Configuration**）**]** をクリックします。
4. **[**予想される構成（**Expected Configuration**）**]** 領域から **[**ソフトウェア テレメトリ（**Software Telemetry**）**]** および **[**フロー テレメトリ（**Flow Telemetry**）**]** の下にある設定を表示およびコピーできます。
5. コマンド ラインを使用して、スイッチにログインします。
6. 次のコマンドを入力します。

```
switch# configure terminal switch(config)#
no feature telemetry
switch(config)# copy running-config startup-config
```

# フローの設定

## フローテレメトリ

フローテレメトリを使用すると、ユーザーはさまざまなフローが通ったパスを詳細に確認できます。また、送信元とセッツ続先の VRF インスタンスも識別できます。ノードからフローテーブルをエクスポートして、フロー内のスイッチを確認できます。フローパスは、すべてのエクスポートをフローの順序で結合することで生成されます。

次のインターフェイス タイプのフロー テレメトリ ルールを設定できます。

- VRF インスタンス
- 物理インターフェイス
- ポート チャネルのインターフェイス

> 物理またはポート チャネル フロー ルールは、ルーテッドインターフェイスでのみサポートされます。

フロー テレメトリは、ファブリック グループ内のファブリック間が結合されていないため、各ファブリックのフローを個別に監視します。フローテレメトリは個々のフロー用です。たとえば、ファブリック グループ内に 2 つのファブリック（ファブリックA とファブリックB）があり、トラフィックが 2 つのファブリック間をフローしている場合、それらは 2 つの個別のフローとして表示されます。1 つのフローはファブリック A から始まり、フローの終了場所が表示されます。もう 1 つのフローはサイト B からで、開始場所と終了場所が表示されます。

## フローテレメトリのガイドラインと制約事項

- NDFC で NTP が構成され、PTP が有効になっていることを確認します。詳細については、『Cisco Nexus Dashboard Insights 展開ガイド』を参照してください。 Cisco NDFCファブリック用の外部NTPサーバーを使用してスイッチを設定する必要があります。
- Cisco Nexus Dashboard Insights リリース 6.0.1 以降、すべてのフローは、サイトタイプ ACI および NDFC の統合されたパイプラインの統合ビューとしてモニタされ、フローは同じ Cisco Umbrella の下に集約されます。
- **[**フローの編集（**Edit Flow**）**]** ページでは、3 つすべてを有効にすることも、製品に最適なモードを選択することもできます。 sFlow は最も制限が厳しく、Netflow では機能が増え、フロー テレメトリには最も多くの機能があります。そのため、お使いの設定で利用可能な場合は、フローテレメトリを有効にすることをお勧めします。フローテレメトリが利用できない場合は、Netflowを使用します。Netflowが使用できない場合は、sFlowを使用します。
- 特定のノード（サードパーティのスイッチなど）がフローテレメトリでサポートされていない場合でも、Cisco Nexus Dashboard Insights は、パス内の前後のノードからの LLDP 情報を使用して、スイッチ名と入力および出力インターフェイスを識別します。
- フロー テレメトリEventsを含むフロー テレメトリは、以下をサポートします。
  - 20,000ユニークフロー/秒(物理的基準)
  - 10,000ユニークフロー/秒(物理的に小規模)
  - 2,500ユニークフロー/秒(vND)
- Cisco Nexus Dashboard Insights にオンボードされた複数の NDFC クラスタがある場合、サイトごとに部分的なパスが生成されます。

- Cisco Nexus Dashboard Insights およびフロー テレメトリのサポートで使用するファブリックを手動で設定した場合、フロー エクスポータ ポートが 30000 から 5640 に変更されます。フローエクスポータの破損を防ぐには、オートメーションを調整します。
- Nexusダッシュボードは、フロー異常のKafkaエクスポートをサポートしています。ただし、フローイベントの異常では、Kafkaエクスポートは現在サポートされていません。
- フローテレメトリは、次のNX-OSバージョンの-FX3プラットフォームスイッチでサポートされています。
  - 9.3(7) 以降
  - 10.1(2) 以降
  - フローテレメトリは、NX-OS バージョン10.1(1) の -FX3 プラットフォームスイッチではサポートされていません。
- インターフェイス ベースのフロー テレメトリは、物理ポートおよびポート チャネル ルールに -FX ランド -GX 回線カードを備えたモジュラ シャーシでのみサポートされます。
- インターフェイス ベースのフロー テレメトリが Nexus Dashboard Insights for **Classic LAN** および
  外部接続ネットワーク ファブリックの場合は、NDFC で次の手順を実行します。
  - NDFC GUI で、ファブリックを選択します。
  - **[**ポリシー（**Policies**）**]**、**[**アクション（**Action**）**]**、**[**ポリシーの追加（**Add Policy**）**]**、**[**すべて選択（**Select all**）**]**、**[**テンプレートの選択（**Choose template**）**]**、[host_port_resync] の順に選択し、**[**保存（**Save**）**]** をクリックします。
  - [ファブリックの概要（Fabric Overview）] ページで、**[**アクション（**Actions**）**]** > **[**再計算と展開（**Recalculate and Deploy**）**]** をクリックします。
- VXLAN ファブリックの場合、インターフェイス ベースのフロー テレメトリは、スパイン スイッチとリーフ スイッチ間のスイッチリンクではサポートされません。

### フロー テレメトリ ルールのガイドラインと制限事項：

- サブネット上でインターフェイス ルール（物理/ポート チャネル）を設定すると、着信トラフィックのみをモニターできます。構成されたインターフェイス ルールで発信トラフィックをモニターすることはできません。
- 2 つの物理ポートを含む構成済みのポート チャネルの場合、ポート チャネル ルールのみが適用されます。ポートに物理インターフェイス ルールを設定した場合でも、ポート チャネル ルールのみが優先されます。
- ノードには最大 500 のルールを構成できます。
- NX-OS リリース 10.3(2) 以前では、フロー ルールがインターフェイスで設定されている場合、グローバル フロー ルールは一致しません。
- NX-OS リリース 10.3(3) 以降では、インターフェイスに設定されたフロー ルールが最初に照合され、次にグローバル フロー ルールが照合されます。

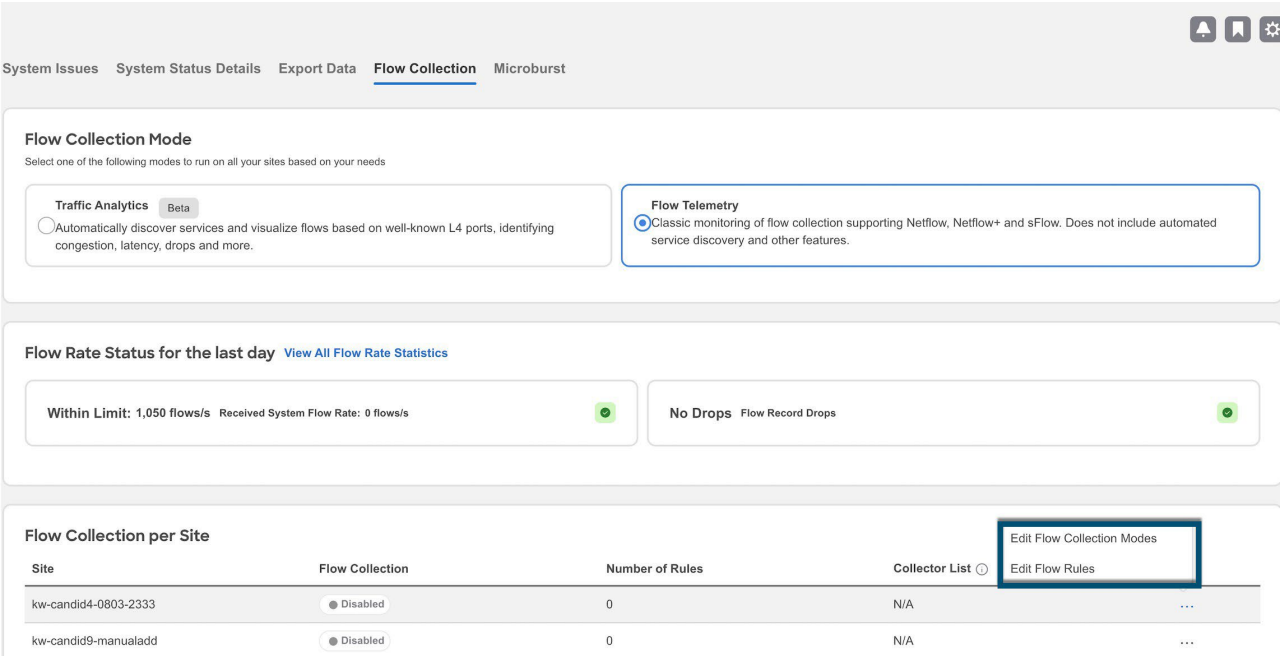
## フローの設定

### フロー収集モードの構成手順

1. **[**管理者（**Admin**）**]** > **[**システム設定（**System Settings**）**]** > **[**フロー収集（**Flow Collection**）**]** に移動します。
2. **[**フロー収集モード（**Flow Collection Mode**）**]**エリアで、**[**フロー テレメトリ（**Flow Telemetry**）**]** を

選択します。

3. **[サイトごとのフロー収集（Flow Collection per Site ）]** テーブルで、サイトを選択し、省略符アイコンをクリックします。
4. **[フロー収集モードの編集（Edit Flow Collection Modes）]** をクリックします。




5. **[フロー収集モードの編集（Edit Flow Collection Mode）]** ページで、**[フロー テレメトリ（Flow Telemetry）]** を選択してフロー テレメトリを有効にします。デフォルトでは、すべてのフローが無効になっています。
6. [保存（Save）] をクリックします。

> フロー テレメトリを有効にすると、フロー テレメトリ イベントが自動的にアクティブになります。互換性のあるイベントが発生するたびに、異常が生成され 、
> 影響とは？セクション に 関連 するフローが表示されます。フロー テレメトリ ルールを手動で構成して、問題のあるフローに関する包括的なエンドツーエンドの情報を取得できます。

## フロー収集ルールの構成手順

1. **[管理者（Admin）]** > **[システム設定（System Settings）]** > **[フロー収集（Flow Collection）]** に移動します。
2. **[フロー収集モード（Flow Collection Mode）]**エリアで、**[フロー テレメトリ（Flow Telemetry）]** を選択します。
3. **[サイトごとのフロー収集（Flow Collection per Site ）]** テーブルで、サイトを選択し、省略符アイコンをクリックします。
4. **[フロー ルールの編集（Edit Flow Rules）]** をクリックします。
5. VRF ルールを追加するには、[VRF] タブをクリックし、次の手順を実行します。
   a. **[アクション（Action）]** ドロップダウン メニューから、**[*新しいルールの作成 (Create New Rule）]** を選択します。
   b. **[全般（General）]** エリアで、次のフィールドに値を入力します。
      i. **[ルール名（Rule Name）]** フィールドにルールの名前を入力します。
      ii. VRF フィールドは無効になっています。フロー ルールはすべての VRF に適用されます。

iii. **[**フロー プロパティ（**Flow Properties**）**]** エリアで、フロー トラフィックをモニターするプロトコルを選択します。

iv. 送信元 IP アドレスおよび宛先 IP アドレスを入力します。送信元ポートと宛先ポートを入力します。

v. **[**保存（**Save**）**]** をクリックします。

6. 物理インターフェイスルールを追加するには、**[**物理インターフェイス（**Physical Interfaces**）**]** タブをクリックし、次の手順を実行します。

   a. **[**アクション（**Action**）**]** ドロップダウン メニューから、**[**新しいルールの作成 **(Create New Rule**）**]** を選択します。

   b. **[**全般（**General**）**]** エリアで、次のフィールドに値を入力します。

      i. **[**ルール名（**Rule Name**）**]** フィールドにルールの名前を入力します。

      ii. ステータスを有効にするには、**[**有効（**Enabled**）**]** チェック ボックスをオンにします。ステータスを有効にすると、ルールが有効になります。それ以外の場合、ルールはスイッチから削除されます。

      iii. **[**フロー プロパティ（**Flow Properties**）**]** エリアで、フロー トラフィックをモニターするプロトコルを選択します。

      iv. 送信元 IP アドレスおよび宛先 IP アドレスを入力します。送信元ポートと宛先ポートを入力します。

      v. **[**インターフェイス リスト（**Interface List**）**]** エリアで、**[**ノードの選択（**Select a Node**）**]** をクリックします。検索ボックスを活用してノードを選択します。

      vi. ドロップダウン リストから、[インターフェイス] を選択します。**[**インターフェイスの追加（**Add Interfaces**）**]** をクリックすると、複数の行（ノードとインターフェイスの組み合わせ）を追加できます。ただし、ルール内では、ノードは 1 回しか表示できません。複数のノードが追加されると、設定は拒否されます。

      vii. **[**保存（**Save**）**]** をクリックします。

7. ポート チャネル ルールを追加するには、**[**ポート チャネル（**Port Channel**）**]** タブをクリックし、次の手順を実行します。

   a. **[**アクション（**Action**）**]** ドロップダウン メニューから、**[***新しいルールの作成 **(Create New Rule**）**]** を選択します。

   b. **[**全般（**General**）**]** エリアで、**[**ルール名（**Rule Name**）**]** フィールドにルールの名前を入力します。

      i. ステータスを有効にするには、**[**有効（**Enabled**）**]** チェック ボックスをオンにします。ステータスを有効にすると、ルールが有効になります。それ以外の場合、ルールはスイッチから削除されます。

      ii. **[**フロー プロパティ（**Flow Properties**）**]** エリアで、フロー トラフィックをモニターするプロトコルを選択します。

      iii. 送信元 IP アドレスおよび宛先 IP アドレスを入力します。送信元ポートと宛先ポートを入力します。

      iv. ドロップダウン リストから、[インターフェイス] を選択します。**[**インターフェイスの追加（**Add Interfaces**）**]** をクリックすると、複数の行（ノードとインターフェイスの組み合わせ）を追加できます。ただし、ルール内では、ノードは 1 回しか表示できません。複数のノードが追加されると、設定は拒否されます。

      v. **[**保存（**Save**）**]** をクリックします。

8. **[**完了（**Done**）**]** をクリックします。

# フローテレメトリのサブネットの監視

フローテレメトリでは、次のようにサブネットを監視します。

次の例では、フロー用に設定されたルールが、提供された特定のサブネットを監視します。ルールはサイトにプッシュされ、サイトはスイッチにルールをプッシュします。したがって、スイッチが送信元 IP または接続先 IP からのトラフィックを検出し、そのトラフィックがサブネットと一致する場合、情報は TCAM にキャプチャされ、Cisco Nexus Dashboard Insights サービスにエクスポートされます。4 つのノード（A、B、C、D）があり、トラフィックが A > B > C > D と移動する場合、ルールは 4 つのノードすべてで有効になり、情報は 4 つのノードすべてでキャプチャされます。Cisco Nexus Dashboard Insights はフローを結合します。4つのノードについて、ドロップ数やパケット数、フローの異常、フローパスなどのデータが集約されます。

1. **[**管理（**Manage**）**]** > **[** サイト（**Sites**）**]** に移動します。
2. ドロップダウン リストから **[**オンライン サイト（**Online Sites**）**]** を選択します。
3. サイト名をクリックすると、そのサイトに関する詳細が表示されます。
4. **[**接続（**Connectivity**）**]** > **[**フロー（**Flows**）**]** に移動します。
5. 時間範囲を選択します。
6. フロー ページは、選択したスナップショットに基づいてキャプチャされているすべてのフローの概要を表示します。

関連する異常スコア、レコード時間、フローテレメトリを送信するノード、フロータイプ、入力ノードと出力ノード、および追加の詳細が表形式で表示されます。テーブル内の特定のフローをクリックすると、特定のフローテレメトリに関する特定の詳細がサイドバーに表示されます。サイドバーで[詳細]アイコンをクリックすると、より大きなページに詳細が表示されます。このページでは、他の詳細に加えて、送信元と接続先に関連する詳細とともに **[**パスの概要（**Path Summary**）**]** も表示されます。逆方向のフローがある場合もこの場所で確認できます。

双方向フローの場合、フローを逆にしてパスの概要を表示するオプションも選択できます。フローイベントを生成するパケットドロップがある場合は、異常ダッシュボードに表示できます。

# Netflow

NetFlowは業界標準となっており、インターフェイス上のネットワークトラフィックをCiscoルータが監視および収集します。Cisco Nexus Dashboard Insightsリリース6.0以降、NetFlowバージョン9がサポートされています。

NetFlowを使用すると、ネットワーク管理者は、送信元、宛先、サービスクラス、輻輳の原因などの情報を特定できます。NetFlowは、インターフェイス上のすべてのパケットを監視し、テレメトリデータを提供するために、インターフェイス上に設定されています。NetFlowではフィルタ処理はできません。

Nexusシリーズ スイッチのNetFlowは、ネットワークトラフィックの要約情報をキャプチャするための、パケット処理パイプラインの代行受信に基づいています。

フロー モニタリング セットアップのコンポーネントは次のとおりです。

- エクスポータ: パケットをフローに集約し、フローレコードを1つ以上のコレクタにエクスポートします。
- コレクタ: フロー エクスポータから受信したフローデータを受信、保存、および前処理します。
- 分析: トラフィック プロファイリングまたはネットワーク侵入に使用されます。
- NetFlowでは、次のインターフェイスがサポートされています。

*表 2. NetFlowでサポートされているインターフェイス*

| インターフェイス | 5タプル | ノード | 入力 | 出力 | パス | コメント |
|---|---|---|---|---|---|---|
| ルーテッドインターフェイス/ポートチャネル<br>注：ユーザーがホスト側のインターフェイスのみを監視している場合は、ポートチャネルのサポートを利用できます。 | はい | o | o | いいえ | はい | 入口ノードはパスに表示 |
| サブ インターフェイス/論理（スイッチ仮想インターフェイス） | はい | o | -いいえ | いいえ | いいえ | いいえ |

# NetFlowタイプ

NDFC タイプの Nexus 9000 シリーズ スイッチの場合、完全な Netflow がサポートされます。Nexus 7000 および Nexus 7700 シリーズ スイッチの場合、NDFC タイプの F/M ラインカードの場合、サンプリングされた Netflow がサポートされます。

## Full Netflow

Full NetFlow では、構成されたインターフェイス上のすべてのパケットがフロー テーブルのフロー レコードにキャプチャされます。
します。 フローはスーパーバイザモジュールに送信されます。レコードは、設定可能な間隔で集約され、コレクタにエクスポートされます。エイリアス（フローテーブル内の同じエントリにハッシュする複数のフロー）の場合を除いて、すべてのフローはそれぞれのパケットレートに関係なく監視できます。

### サンプル NetFlow

サンプリングされたNetflowでは、設定されたインターフェイスのパケットがタイムサンプリングされます。フローはスーパーバイザまたはネットワークプロセッサに送信されて集約されます。集約されたフローレコードは、設定された間隔でエクスポートされます。フローレコードがキャプチャされる確率は、同じインターフェイス上の他のフローと比較したフローのサンプリング頻度とパケットレートに依存します。

## NetFlowのガイドラインと制約事項

- **[**フローの編集（**Edit Flow**）**]** ページでは、3 つすべてを有効にすることも、製品に最適なモードを選択することもできます。 sFlow は最も制限が厳しく、Netflow では機能が増え、フロー テレメトリには最も多くの機能があります。そのため、お使いの設定で利用可能な場合は、フローテレメトリを有効にすることをお勧めします。フローテレメトリが利用できない場合は、Netflowを使用します。Netflowが使用できない場合は、sFlowを使用します。
- Cisco Nexus 9000 シリーズ スイッチのNetFlowは、RFCで公開されているエクスポートフィールドの小さなサブセットをサポートします。
- 入力スイッチのみがフローをエクスポートするため、NetFlowはフローの入力ポートでのみキャプチャされます。NetFlowはファブリックポートではキャプチャできません。
- Nexus 7000およびNexus 9000シリーズ スイッチでは、Netflow用に設定された入力ホスト側インターフェイスのみがサポートされます(VXLANまたは従来型LANのいずれか)。
- NetFlowの場合、Cisco Nexus Dashboardでは、クラスタ設定の下に永続的なIPを設定する必要があり、データネットワークと同じサブネットに7つのIPが必要です。
- NDFC タイプの場合、Netflow でサポートされるファブリックは従来型と VXLAN です。VXLANはファブリックポートではサポートされていません。
- Netflow設定はプッシュされません。ただし、サイトが管理されている場合は、ソフトウェアセンサーがプッシュされます。
- Cisco Nexus Dashboard Insightsおよび Netflowのサポートで使用するファブリックを手動で設定した場合、フローエクスポータポートが30000から5640に変更されます。フローエクスポータの破損を防ぐには、オートメーションを調整します。
- ファブリック スイッチで Netflow を設定するには、『Cisco Nexus 9000 シリーズ NX-OS システム管理コンフィギュレーション ガイド』の「**Netflow** の構成」のセクションを参照してください。

## NetFlowの設定

### はじめる前に

ユーザーは、推奨設定を使用して適切なスイッチを設定する必要があります。

### 手順

次の手順でNetFlowを設定します。

1. **[**管理者（**Admin**）**]** > **[**システム設定（**System Settings**）**]** > **[**フロー収集（**Flow Collection**）**]** に移動します。
2. **[**フロー収集モード（**Flow Collection Mode**）**]**エリアで、**[**フロー テレメトリ（**Flow Telemetry**）**]** を選択します。
3. **[**サイトごとのフロー収集（**Flow Collection per Site** ）**]** テーブルで、サイトを選択し、省略符アイコンをクリックします。
4. **[**フロー収集モードの編集（**Edit Flow Collection Modes**）**]** をクリックします。
5. **[**フロー収集モードの編集（**Edit Flow Collection Modes**）**]** ページで、**[Netflow]**を選択します。デフォルトでは、すべてのフローが無効になっています。
6. [保存（Save）] をクリックします。

# sFlow

sFlowは、スイッチとルーターを含むデータネットワークにおける業界標準のテクノロジトラフィックです。Cisco Nexus Dashboard Insightsは、Cisco Nexus 3000シリーズ スイッチでsFlowバージョン5をサポートしています。

sFlow は、パフォーマンスの最適化、アカウンティングと使用量に対する課金、およびセキュリティ上の脅威に対する防御を可能にする可視性を提供します。

sFlowでは、次のインターフェイスがサポートされています。

*表 3. sFlowでサポートされるインターフェイス*

| インターフェイス | **5**タプル | ノード | 入力 | 出力 | パス | コメント |
|---|---|---|---|---|---|---|
| ルーテッドインターフェイス | はい | ○ | ○ | ○ | ○ | 入口ノードはパスに表示 |

# sFlowの注意事項および制約事項

- Cisco Nexus Dashboard Insights は、NDFC を使用する Cisco Nexus 3000 シリーズ スイッチで sFlow をサポートしています。
- お使いの設定で利用可能な場合は、フローテレメトリを有効にすることをお勧めします。使用している構成で利用できない場合は、NetFlowを使用してください。Netflowがお使いの設定で利用できない場合は、sFlowを使用します。
- sFlowの場合、Cisco Nexus Dashboardでは、クラスタ設定の下に永続的なIPを設定する必要があり、データネットワークと同じサブネットに6つのIPが必要です。
- sFlow設定はプッシュされません。ただし、サイトが管理されている場合は、ソフトウェアセンサーがプッシュされます。
- Cisco Nexus Dashboard Insightsおよび sFlowのサポートで使用するファブリックを手動で設定した場合、フローエクスポータポートが30000から5640に変更されます。フローエクスポータの破損を防ぐには、オートメーションを調整します。
- Cisco Nexus Dashboard Insightsは、次の Cisco Nexus 3000シリーズ スイッチでsFlowをサポートしていません。
  - Cisco Nexus 3600-Rプラットフォームスイッチ(N3K-C3636C-R)
  - Cisco Nexus 3600-Rプラットフォームスイッチ(N3K-C36180YC-R)
  - Cisco Nexus 3100プラットフォームスイッチ(N3K-C3132C-Z)
- Cisco Nexus Dashboard Insightsは、次の Cisco Nexus 9000シリーズ ファブリック モジュールで sFlowをサポートしていません。
  - Cisco Nexus 9508-Rファブリックモジュール(N9K-C9508-FM-R)
  - Cisco Nexus 9504-Rファブリックモジュール(N9K-C9504-FM-R)
- ファブリックスイッチでsFlowを設定するには、 Cisco Nexus 9000シリーズNX-OSシステム管理コンフィギュレーション ガイドの**Configuring sFlow**セクションを参照してください。

# sFlowの設定

## はじめる前に

ユーザーは、推奨設定を使用して適切なスイッチを設定する必要があります。

## 手順

次の手順でsFlowテレメトリを設定します。

1. **[**管理者（**Admin**）**]** > **[**システム設定（**System Settings**）**]** > **[**フロー収集（**Flow Collection**）**]** に移動します。
2. **[**フロー収集モード（**Flow Collection Mode**）**]**エリアで、**[**フロー テレメトリ（**Flow Telemetry**）**]** を選択します。
3. **[**サイトごとのフロー収集（**Flow Collection per Site** ）**]** テーブルで、サイトを選択し、省略符アイコンをクリックします。
4. **[**フロー収集モードの編集（**Edit Flow Collection Modes**）**]** をクリックします。
5. **[**フロー収集モードの編集（**Edit Flow Collection Mode**）**]** ページで、**[sFlow]**を選択します。デフォルトでは、すべてのフローが無効になっています。
6. [保存（Save）] をクリックします。

# エクスポートデータ

## エクスポートデータ

データのエクスポート機能を使用すると、Kafka および電子メールを介して Nexus Dashboard Insights によって収集されたデータをエクスポートできます。Nexus Dashboard Insightsは、アドバイザリ、異常、監査ログ、障害、統計データ、リスクおよび適合性レポートなどのデータを生成します。Kafkaブローカーをインポートすると、すべてのデータがトピックとして書き込まれます。

さらに、電子メールスケジューラを設定して、電子メールで情報を受信するデータと頻度を指定できます。

Cisco Intersightは、電子メール通知に使用されます。詳細については、「デバイスコネクタについて」を参照してください。

### データのエクスポートに関するガイドラインと制限事項

- 定期的なジョブの構成では、1 日あたり最大 5 件の電子メールを構成できます。
- レポートを電子メールで受信するには、Intersight接続が必要です。
- Kafka Exportでは、最大5つのエクスポータがサポートされています。
- Kafkaエクスポートを設定する前に、Nexus Dashboardクラスタ設定の既知のルートとして外部Kafka IPアドレスを追加する必要があります。
- Nexusダッシュボードは、フロー異常のKafkaエクスポートをサポートしています。ただし、フローイベントの異常では、Kafkaエクスポートは現在サポートされていません。
- ファブリックでソフトウェア テレメトリを無効にし、NDFC からファブリックを削除する前に、*[メッセージバス設定（Message Bus Configuration）]* と *[電子メール（Email）]* ページのすべての設定が削除されていることを確認してください。
- Kafkaおよび電子メールメッセージの異常には、リソース、環境、統計情報、エンドポイント、フロー、バグのカテゴリが含まれます。
- カテゴリ(セキュリティ、転送、変更分析、コンプライアンス、システム)は、Kafkaおよび電子メールメッセージの異常には含まれません。
- データのエクスポートは、スナップショット サイトではサポートされていません。
- エクスポートごとに一意の名前を指定する必要があります。

## Kafka Exporterの設定

次の手順を使用して、Kafka Exporterを設定します。

1. **[管理者]** > **[システム設定]** > **[データのエクスポート]** に移動します。
2. **[メッセージバス構成（Message Bus Configuration）]** エリアで、**[新規追加（Add New）]** をクリックし、次のタスクを実行します。
   a. **[サイト名（Site Name）]** フィールドで、適切なサイトを選択します。
   b. [IPアドレス]フィールドと[ポート]フィールドに、KafkaブローカーのIPアドレスとポートを入力します。
   c. **[モード（Mode）]** フィールドで、セキュリティモードを選択します。サポートされているモードは、[非セキュア]、[セキュアSSL]、および[SASLPLAIN]モードです。
   d. **[一般設定]**領域で、データの送信先となる名前とトピック名を入力し、基本モードまたは詳細モー

ドを選択します。
異常とアドバイザリに関するKafkaエクスポートの詳細が表示されます。

3. 各カテゴリの **[**収集設定（**Collection Settings**）**]** エリアで、異常とアドバイザリの重大度を選択します。
4. [保存（Save）] をクリックします。

この設定により、選択した異常またはアドバイザリが発生すると、すぐに通知が送信されます。

# 電子メールの設定

次の手順を使用して、Nexus Dashboard Insightsから収集されたデータの概要を送信する電子メールスケジューラを設定します。

1. **[**管理者**]** > **[**システム設定**]** > **[**データのエクスポート**]** に移動します。
2. **[**電子メール（**Email**）**]** エリアで [新規追加（Add New）] をクリックし、次の操作を実行します。
   a. **[**全般設定（**General Settings**）**]** 領域の **[**サイト名（**Site Name**）**]** ィールドで、サイト名を選択します。
   b. In the **Name** field, enter the name.
   c. **[**電子メール（**Email**）**]** フィールドに、電子メールアドレスを入力します。複数の電子メール アドレスを入力する場合は、区切り文字としてコンマを使用します。
   d. **[**形式（**Format**）**]** フィールドで、電子メールの [テキスト] または [HTML] 形式を選択します。
   e. **[**開始日（**Start Date**）**]** フィールドに、開始日を入力します。
   f. **[**収集間隔（**Collect Every**）**]** フィールドで、頻度を日または週単位で指定します。
   g. **[**モード（**Mode**）**]**フィールドで、[基本（Basic）] または [詳細（Advanced）] を選択します。

      [基本（Basic）] モードでは、異常、アドバイザリ、および障害の重大度が **[**収集設定（**Collection Settings**）**]** エリアに表示されます。[詳細（Advanced）] モードでは、異常とアドバイザリのカテゴリと重大度が **[**収集設定（**Collection Settings**）**]** エリアに表示されます。
3. 各カテゴリの **[**収集設定（**Collection Settings**）**]** エリアで、異常およびアドバイザリの重大度を選択します。当てはまるものをすべて選択してください。**[**現用系アラート（**Active Alerts**）**]** の場合、有効または無効化のオプションを選択します。**[**適合性レポート（**Conformance Reports**）**]** については、ソフトウェア リリースの場合は **[**ソフトウェア（**Software**）**]**、ハードウェア プラットフォームの場合は **[**ハードウェア（**Hardware**）**]**、ソフトウェアとハードウェアの適合性の組み合わせの場合は両方を選択します。
4. [保存（Save）] をクリックします。設定された電子メールスケジューラが **[**電子メール（**Email**）**]** 領域に表示されます。

   指定した *[開始日（Start Date）]* の *[収集間隔（Collect Every）]* で指定した時刻に、スケジュールされたジョブに関する電子メールが届きます。後続の電子メールは、*[収集間隔（Collect Every）]* の頻度が終了した後で送信されます。指定した時刻が過去の場合は、すぐに電子メールが届き、指定した開始時刻からの期間が満了すると次の電子メールがトリガーされます。

5. (任意)編集領域で、次の手順を実行します。
   a. クリックして、電子メールスケジ

   ューラを編集します。b.
   クリックして、 電子メール スケジューラを削除します。

# Syslog

Nexus Dashboard Insights リリース6.1.1は、Syslog 形式での異常とアドバイザリのエクスポートをサポートしています。この機能を使用して、Nexus Dashboard Insights上でネットワーク監視および分析アプリケーションを開発し、Syslogサーバーと統合してアラートを取得し、カスタマイズされたダッシュボードと可視化を構築できます。

Syslogエクスポータを設定するサイトを選択し、Syslogエクスポートの設定をセットアップすると、Nexus Dashboard InsightsはSyslogサーバーとの接続を確立し、データをSyslogサーバーに送信します。

Nexus Dashboard Insightsは、Kafkaメッセージバスから異常とアドバイザリを読み取り、そのデータをSyslogサーバーにエクスポートします。Syslog のサポートにより、Kafka を使用していなくても、サードパーティのツールに異常をエクスポートできます。

### Syslogのガイドラインと制約事項

Syslogサーバーが特定の時間に動作していない場合、ダウンタイム中に生成されたメッセージは、サーバーが動作可能になった後もサーバーによって受信されません。

# Syslog の設定

次の手順を使用して、Syslogを設定して、異常およびアドバイザリデータをSyslogサーバーにエクスポートできるようにします。

1. **[管理者]** > **[システム設定]** > **[データのエクスポート]** に移動します。
2. **[Syslog]** エリアで、**[新規追加（Add New）]** をクリックします。
3. **[Syslog 構成（Syslog Configuration）]** ダイアログボックスの **[ログイン情報（Credentials）]**エリアで、次の操作を実行します。

   a. **[サイト名（Site Name）]**フィールドで、**[サイトの選択（Select Site）]**をクリックしてサイト名を選択します。

   b. **[IPアドレス（IP Address）]** および **[ポート（Port）]** フィールドに、IP アドレスとポートの詳細を入力します。

   c. **[トランスポート（Transport）]**フィールドで、ドロップダウン リストから適切なオプションを選択します。選択肢は、**[TCP]**、**[UDP]**、および**[SSL]**です。

   d. **[ファシリティ（Facility）]**フィールドで、ドロップダウンリストから適切なファシリティ文字列を選択します。

   ファシリティコードは、メッセージをロギングするシステムの種類を指定するために使用されます。この機能では、ローカルで使用されるファシリティの **local0-local7** キーワードがサポートされています。

4. **[モード（Mode）]** フィールドでトグルボタンをクリックして、**[非セキュア（Unsecured）]**

   か **[セキュアSSL（Secured SSL）]** を選択します。[セキュアSSL]を選択した場合は、サーバ

   ーCA証明書を提供する必要があります。

5. **[構成（Configuration）]** エリアに、エクスポートする Syslog 構成の一意の名前を入力します。
6. **[収集設定（Collection Settings）]** エリアで、必要な重大度オプションを選択します。

   選択可能なオプションは、**[クリティカル]**、**[エラー]**、**[警告]**、**[情報]** です。Nexus Dashboard Insights

の **[メジャー]** および **[マイナー]** の異常とアドバイザリは、**[エラー]** にマッピングされます。

7. [保存（Save）] をクリックします。

# ネットワーク接続ストレージへのフロー レコードのエクスポート

Nexus Dashboard Insights リリース 6.3.1 以降では、Nexus Dashboard Insights でキャプチャしたフローレコードを NFS 対応のリモート ネットワーク接続ストレージ (NAS) にエクスポートできます。

Nexus Dashboard Insights は、フローレコード がエクスポートされるNAS 上のディレクトリ構造を定義します。

フローレコードは、Base モードまたは Full モードでエクスポートできます。Base モードでは、フロー レコードの 5 タプルデータのみがエクスポートされます。Full モードでは、フロー レコードのデータ全体がエクスポートされます。

Nexus Dashboard Insights では、フロー レコードをエクスポートするために NAS への読み取りおよび書き込み権限が必要です。Nexus Dashboard Insights が NAS への書き込みに失敗すると、システムの問題が発生します。

# 注意事項と制約事項

- Nexus Dashboard Insights がフロー レコードを外部ストレージにエクスポートするには、 Nexus Dashboard に追加されたネットワーク接続ストレージが Nexus Dashboard Insights 専用である必要があります。
- Network File System（NFS）バージョン3 を使用したネットワーク Attached Storage を Nexus Dashboard に追加する必要があります。
- フローテレメトリ、NetFlow、および sflow レコードをエクスポートできます。
- FTE のエクスポートはサポートされていません。
- 1 秒あたり 20,000 フローで 2 年間のデータストレージの平均ネットワーク接続ストレージ要件：
  - 基本モード：500 TBデータ
  - フル モード：2.8 PBデータ
- 十分なディスク容量がない場合、新しいレコードはエクスポートされず、異常が生成されます。

# ネットワーク接続ストレージをフロー レコードをエクスポートするために追加する

フロー レコードをエクスポートするためにネットワーク接続ストレージ（NAS ）を追加するワークフローには、次の手順が含まれます。

1. Nexus Dashboard に NAS を追加します。
2. Nexus Dashboard のオンボード NAS を Nexus Dashboard Insights に追加して、フロー レコードのエクスポートを有効にします。

## Nexus Dashboard への NAS の追加

1. Nexus Dashboard で、**[**管理（**Admin**）**]** > **[**システム設定（**System Settings**））**]** > **[** ネットワーク **-** 接続ストレージ（**Network Attached Storage**）**]** に移動します。
2. **[**編集（**Edit**）**]** をクリックします。
3. **[**ネットワーク接続ストレージの追加**]** をクリックします。

4. **[**ネットワーク接続ストレージの追加（**Add Network-Attached Storage**）**]**の次のフィールドに値を入力します。
   a. **[**読み取り**/**書き込みタイプ（Read Write Type）] を選択します。Nexus Dashboard Insights には、フロー レコードを NAS にエクスポートするための読み取りおよび書き込み権限が必要です。Nexus Dashboard Insights が

> Nexus Dashboard Insights で、**[**管理（**Admin**）**]** > **[**システム設定（**System Settings**）**]** > **[**システムの問題（**System Issues**）**]** に移動して、システムの問題を表示します。

a. ネットワーク接続ストレージの名前を入力します。
b. ネットワーク接続ストレージの IP アドレスを入力します。
c. ネットワーク接続ストレージのポート番号を入力します。
d. NFS エクスポート パスを入力します。エクスポート パスを使用して、 Nexus Dashboard Insights は、フロー レコードをエクスポートするためのディレクトリ構造を NAS に作成します。
e. アラートしきい値時間を入力します。アラートしきい値は、 NASが特定の制限を超えて使用されたときにアラートを送信するために使用されます。
f. Mi/Gi で保存容量を入力します。
g. **[**保存（**Save**）**]** をクリックします。

## オンボードされた **NAS** を **Nexus Dashboard Insights** に追加する

1. Nexus Dashboard Insights で、**[**管理（**Admin**）**]**> **[**システム設定（**System Settings**）**]** > **[**データのエクスポート（**Export Data**）**]** に移動します。
2. [ネットワーク接続ストレージ（Network-Attached storage）] で、**[**新規追加（**Add New**）**]** をクリックします。
3. **[NAS** 構成（**NAS Configuration**）**]** の次のフィールドに値を入力します。
   a. 名前を入力します。
   b. ドロップダウンリストから、 Nexus Dashboard に追加された NAS サーバを選択します。
   c. **[**サイトの選択（**Select Site**）**]** をクリックしてサイトを選択します。一度に選択できるサイトは 1 つだけです。
   d. ドロップダウン リストからフローに対する収集設定を選択します。Base モードでは、フローレコードの 5 タプルデータのみがエクスポートされます。Full モードでは、フロー レコードのデータ全体がエクスポートされます。
   e. **[**保存（**Save**）**]** をクリックします。
4. **[**フロー（**Flows**）**]** ページに表示されるフローからのトラフィックは、次のディレクトリ階層の外部 NAS に JSON ファイルとしてエクスポートされます。

```
└── NDI-<VERSION>-FLOW-JSON/
    └── fabricName=<fabricName>/
        └── year=2022/
            ├── month=01/
            │   └── date=01/
            │       ├── hour=01/
            │       │   ├── 52170795-0b94-481c-800a-c47f0fa41fac.json
            │       │   └── fa92c70c-96fc-4e32-ac76-324bdd5139d4.json
            │       └── hour=23/
            │           ├── 737f4292-bf29-4630-bdd9-ccb80885ddc1.json
            │           └── 68b434d9-0957-4fe4-be01-e0688cb4336d.json
            └── month=02/
                └── date=20/
                    ├── hour=10/
                    │   ├── e05ce8fb-88af-45db-8c52-4b00e1841b16.json
                    │   └── 6fd2b652-dfe1-430e-905a-020abd399e3e.json
                    └── hour=23/
                        ├── eeb6784a-33a0-4ae3-b13e-db4db93fe48b.json
                        └── b289c75e-a709-4284-a018-b38ab101d90f.json
```

**[**分析（**Analyze**）**]> [**フロー（**Flows**）**]** に移動して、エクスポートされるフローを表示します。

5. 各フロー レコードは、行区切りの JSON として書き込まれます。

**Base** モードのフロー レコードの **JSON** 出力ファイル フォーマット


{" fabricName" :" myapic" ," terminalTs" :1688537547433," originTs" :1688537530376," srcIp" :" 2000:201:1:1::1" ," dstIp" :" 2000:201:1:1::3" ," srcPort" :1231," dstPort" :1232," ingressVrf" :" vrf1" ," egressVrf" :" vrf1" ," ingressTenant" :" FSV1" ," egressTenant" :" FSV1" ," protocol" :" UDP" }

{" fabricName" :" myapic" ," terminalTs" :1688537547378," originTs" :1688537530377," srcIp" :" 201.1.1.127" ," dstIp" :" 201.1.1.1" ," srcPort" :0," dstPort" :0," ingressVrf" :" vrf1" ," egressVrf" :" " ," ingressTenant" :" FSV2" ," egressTenant" :" " ," protocol" :" ANY-HOST" }


フル モードのフロー レコードの **JSON** 出力ファイル フォーマット


{" fabricName" :" myapic" ," terminalTs" :1688538023562," originTs" :1688538010527," srcIp" :" 201.1.1.121" ," dstIp" :" 201.1.1.127" ," srcPort" :0," dstPort" :0," ingressVrf" :" vrf1" ," egressVrf" :" vrf1" ," ingressTenant" :" FSV2" ," egressTenant" :" FSV2" ," protocol" :" ANY-HOST" ," srcEpg" :" ext-epg" ," dstEpg" :" ext-epg1" ," latencyMax" :0," ingressVif" :" eth1/15" ," ingressVni" :0," latency" :0," ingressNodes" :" Leaf1-2" ," ingressVlan" :0," ingressByteCount" :104681600," ingressPktCount" :817825," ingressBurst" :0," ingressBurstMax" :34768," egressNodes" :" Leaf1-2" ," egressVif" :" po4" ," egressVni" :0," egressVlan" :0," egressByteCount" :104681600," egressPktCount" :817825,"

egressBurst" :0," egressBurstMax" :34768," dropPktCount" :0," dropByteCount" :0," dropCode
" :" " ," dropScore" :0," moveScore" :0," latencyScore" :0," burstScore" :0," anomalyScore" :0,"
hashCollision" :false," dropNodes" :" []" ," nodeNames" :" [\" Leaf1-
2\" ]" ," nodeIngressVifs" :" [\" Leaf1-2,eth1/15\" ]" ," nodeEgressVifs" :" [\" Leaf1-2,po4\" ]“
," srcMoveCount" :0," dstMoveCount" :0," moveCount" :0," prexmit" :0," rtoOutside" :false," ev
ents" :" [[\\\" 1688538010527,Leaf1-2,0,3,1,no,no,eth1/15,,po4,po4,,,,,0,64,0,,,,,,,,,\\\" ]]" }

**base** モードのフロー レコードの **JSON** 出力ファイル フォーマット（**5** タプル）

{" fabricName" :" myapic" ," terminalTs" :1688537547433," originTs" :1688537530376," srcIp"
:" 2000:201:1:1::1" ," dstIp" :" 2000:201:1:1::3" ," srcPort" :1231," dstPort" :1232," ingressVrf"
:" vrf1" ," egressVrf" :" vrf1" ," ingressTenant" :" FSV1" ," egressTenant" :" FSV1" ," protocol" :" U
DP" }

# システム設定

## システムに関する問題

システムの問題は、 Nexus Dashboard Insights に直接影響する可能性のある問題であり、接続の問題、ステータスのアップグレード、オンボーディング構成などのシステム関連の問題で発生します。システムのカテゴリには、接続システムの問題と収集システムの問題が含まれます。

- サイト接続に障害がある場合、または Nexus Dashboard Insights に関連する接続の問題がある場合、接続システムの問題が発生します。
- テレメトリ 構成の有効化に失敗すると、収集システムの問題が発生します。

### システムの問題を表示

1. **[**管理者（**Admin**）**]** > **[**システム設定（**System Settings**）**]**> **[**システムの問題（**System Issues**）**]** に移動します。
2. 検索バーを使用してシステムの問題をフィルタリングします。
3. **[**システムの問題（**System Issues**）**]** テーブルには、フィルタ処理されたシステムの問題が表示されます。
4. 歯車アイコンをクリックして、[システムの問題（System Issues）] テーブルの列を構成します。
5. システムの問題をクリックすると、問題の原因などの追加の詳細が表示されます。追加の詳細を表示します。

## システムステータス

[システム ステータス（System Status）] ページには、サイトの過去 1 時間の収集ステータスが表示されます。

Nexus Dashboard Insights は、サイト テレメトリを処理し、次のジョブまたはサービスのステータスを表示します。

- サイト
- ノード
- 保証
- キャパシティ
- ハードウェアリソース
- 統計
- エンドポイント
- バグスキャン
- ベストプラクティス
- テレメトリ設定ステータス

## システム ステータスの表示

1. **[**管理者（**Admin**）**]** > **[**システム設定（**System Settings**）**]** > **[**システム ステータスの詳細（**System Status Details**）**]** に移動します。または

1. **[**管理（**Manage**）**]** > **[** サイト（**Sites**）**]** に移動します。
2. サイトを選択します。
3. [サイト（Sites）] ページで、[アクション（Actions）] ドロップダウンメニューから、**[**システム ステータス（**System Status**）**]** を選択します。

ステータス テーブルの **[**エンドポイント（**Endpoints**）**]** 列で、値が「データなし」の 場合、は、過去 1 時間のエンドポイント数に変化がありませんでした。この値 は必ずしも問題があることを示しているわけではありません。

# 設定のインポートとエクスポート

設定のインポートとエクスポート機能を使用すると、Nexus Dashboard Insightsで次の設定をインポートおよびエクスポートできます。

- フロー収集モード
- フローテレメトリ
- トラフィック分析
- マイクロバースト
- 異常ルール
- コンプライアンス
- エクスポート設定
- 電子メール
- メッセージ バス構成
- Syslog
- ネットワーク接続型ストレージ（NAS）
- フロールール
- ユーザー設定
- 統合

設定のインポートとエクスポートに関するすべての操作を管理できるのは管理者だけです。

# 注意事項と制約事項

- 設定をインポートまたはエクスポートするには、管理者ユーザーである必要があります。
- スナップショット サイトはサポートされていません。
- 複数のインポートジョブを同時に実行すると、予期しない結果が生じる可能性があるため、同時実行はサポートされていません。一度に1つのインポートジョブのみを実行します。
- 設定をインポートすると、Nexus Dashboard Insightsに既存の設定が追加されます。
- 設定をインポートしても、既存の異常および既存のアシュアランス分析には影響しません。設定をインポートした後も、既存の異常は存在し続けます。
- オンライン サイトは、すべての構成をインポートする前に、エクスポートされた構成の tar.gz ファイルと同じ名前で最初に Nexus Dashboard Insights で導入準備する必要があります。
- Nexus Dashboardクラスタにローカルな設定のみがエクスポートされ、リモートのNexus Dashboardクラスタの設定はエクスポートされません。
- Nexus Dashboard Insights が Cisco Intersight に接続されていない場合、エクスポート設定のインポートは失敗します。エクスポート設定をインポートする前に、Nexus Dashboard InsightsをCisco Intersight に接続する必要があります。
- 証明書またはパスワードを持つセキュアな構成のインポートはサポートされていません。
- Nexus Dashboard Insights リリース 6.3.1 より前のリリースから構成をエクスポートすると、次の動作が発生します。

- Nexus Dashboard Insights リリース6.3.1で廃止されたカテゴリと重大度を持つ異常ルールのインポートはサポートされていません。
- メッセージ バス設定での高速 Kafka のエクスポートはサポートされていません。

# 設定のエクスポート

1. **[管理（Admin）]> [構成のインポート/エクスポート]** に移動します。
2. **[構成のインポート/エクスポートの作成]** をクリックします。
3. **[構成のインポート/エクスポートの作成（Create Configuration Import/Export）]** ページで **[エクスポート（Export）]** をクリックします。
4. **[開始（Start）]** をクリックします。Nexus Dashboard Insightsで使用可能なすべての構成がエクスポートされます。サイト、アラートルール、コンプライアンス、エクスポート設定、フロールール、およびユーザー設定を含む、ホスト上の既存の構成がすべてエクスポートされます。
5. **[インポート/エクスポート（Import/Export）]** テーブルには、ステータス、タイプ、開始時間、最終更新日時、およびコンテンツの情報が表示されます。
6. エクスポートジョブのステータスが **[完了（Completed）]** に変わったら、省略符クリックして **[ダウンロード（Download）]** を選択します。エクスポートされた設定は、圧縮ファイルでダウンロードされます。
7. 省略記号アイコンをクリックし、**[削除（Delete）]** を選択して構成を削除します。

# 設定のインポート

1. **[管理（Admin）]> [構成のインポート/エクスポート]** に移動します。
2. **[構成のインポート/エクスポートの作成]** をクリックします。
3. **[構成のインポート/エクスポートの作成（Create Configuration Import/Export）]** ページで **[インポート（Import）]** をクリックします。
4. ダウンロードした圧縮 tar.gz 構成ファイルを選択し、**[開始（Start）]** をクリックします。インポートジョブの詳細が **[構成のインポート/エクスポート（Configuration Import/Export）]** テーブルに表示されます。
5. インポート ジョブのステータスが **[検証済み（Validated）]** に変わったら、省略符アイコンをクリックして **[適用（Apply）]** を選択します。
6. インポートする構成を選択し、**[適用（Apply）]** をクリックします。**[インポート/エクスポート（Import/Export）]** テーブルには、インポートされた構成の詳細が表示されます。

> インポート ジョブのステータスが [Partially Failed（部分的に失敗）]の場合 、 インポートジョブのステータスが の場合、一部の構成は追加され、一部は失敗によりスキップされます。失敗の理由を表示するには ステータス列の上にマウスを置きます。

# 著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。

© 2017-2024 Cisco Systems, Inc. All rights reserved.