Cisco Nexus Dashboard Insights リリース 6.5.1、スタートアップガイドガイド：Cisco ACI 向け

目次

初版：2024 年 6 月 28 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、本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。

Cisco Nexus Dashboard Insights の新機能と変更された動作

特長	説明	リリース	参照先
ポリシーベースのリダイレクト アシュアランスの異常	ポリシーベースのリダイレクト（PBR）アシュアランスのために、異常である [サービスチェーンリダイレクトポリシー違反（ Service Chain Redirect Policy Violation）] が追加されます。この異常は、コントラクトおよびサービス グラフ インスタンスの 1 つ以上のリダイレクト ゾーン分割分割ルールが欠落しているか、Cisco APIC 構成と一致しない場合に生成されます。その結果、トラフィックはコントラクトとサービス グラフ インスタンスに対して期待どおりにリダイレクトされません。	6.5.1	PBR の異常
Nexus Dashboard Insights のバックアップと復元	Nexus Dashboard Insights 6.5.1 リリースでは、 Cisco Nexus Dashboard レベルでの統合バックアップおよび復元機能が導入されています。これにより、Nexus Dashboard だけでなく、その Nexus Dashboard で実行されているサービス（Nexus Dashboard Insights など）の設定情報もバックアップされます。	6.5.1	Nexus Dashboard Insights のバックアップと 復元
技術変更	「サイト」という言葉は「ファブリック」に変更されました。	6.5.1	ドキュメント全体

このドキュメントは、Cisco Nexus Dashboard Insights の GUI およびオンラインで www.cisco.com で入手できます。本書の最新バージョンに関しては、「Cisco Nexus Dashboard Insights 」の「 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）]**：ファブリックと Nexus Dashboard Insights に関する基本情報を提供します。
  - **[グローバル ビュー（Global View）]**：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。
  - ジャーニー：スタートアップ ガイドに： Nexus Dashboard Insights でファブリックをセットアップするのに役立ち、いくつかの主要な機能の概要を示します。**[新機能（What's New）]** タブには、プラットフォームの更新と新機能に関する情報が表示されます。
  - 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。
  - カスタム ダッシュボード：頻繁に使用するページをピン留めできるダッシュボードを作成できます。これらのページはダッシュボードにウィジェットとして表示され、クリックして簡単にページに移動できます。
- 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。
  - ファブリック：ファブリックとは、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：ファブリック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：ファブリック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 つの時点でのファブリック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。ファブリックを追加した後、関連する機能を有効または構成できます。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。

- ファブリックを追加します。「ファブリックの追加」を参照します。
- ファブリック分析。「ファブリック分析」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。
- マイクロバーストを有効にします。「マイクロバースト」を参照にしてください。
- 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。

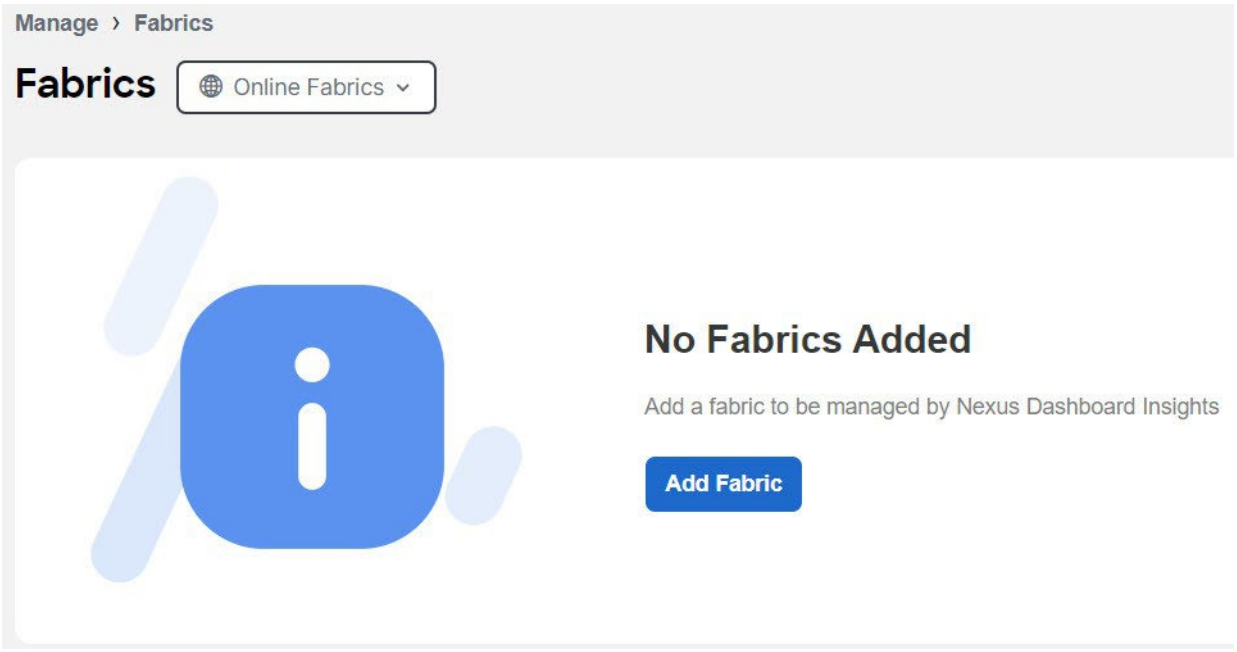
ファブリックの追加

次の方法を使用して、Nexus Dashboard Insights にファブリックを追加できます。

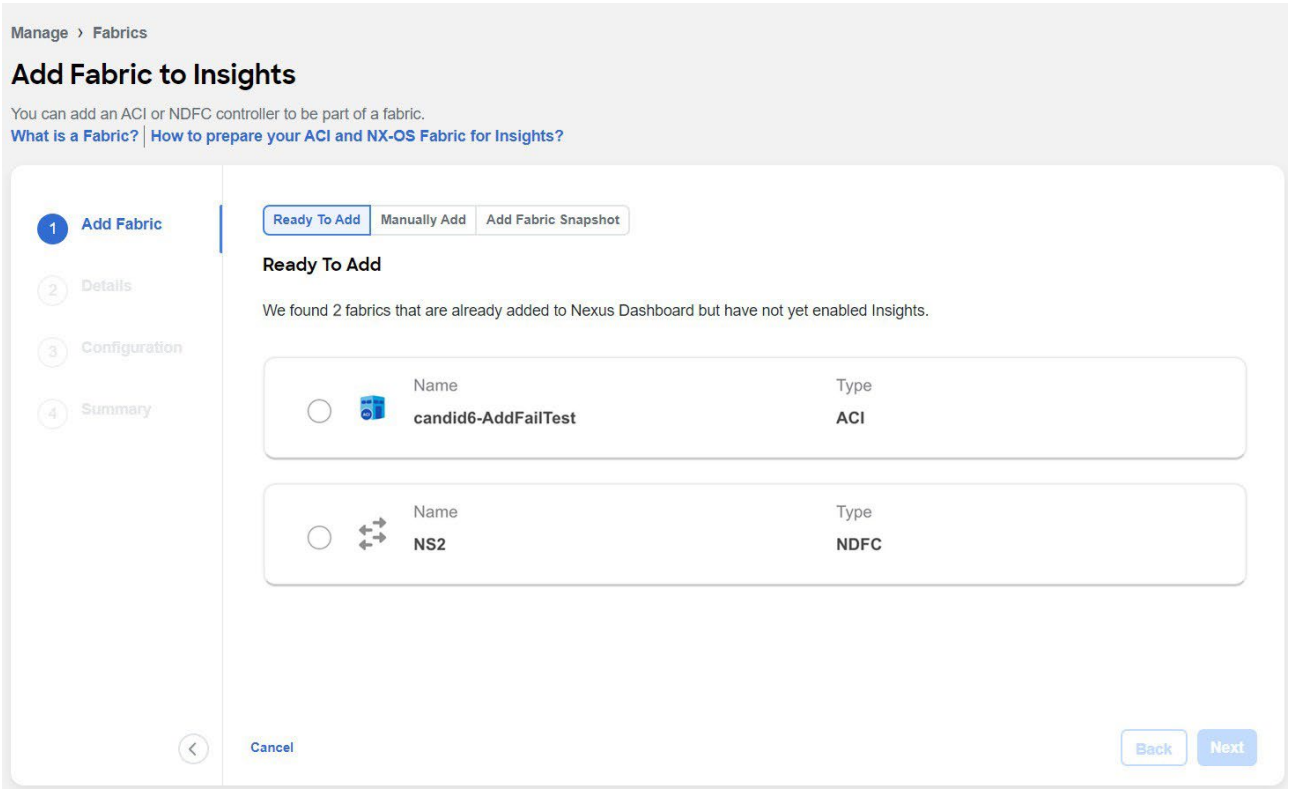
- オンラインファブリック
  - Nexus Dashboard にすでに追加されているファブリックを有効にします。Nexus Dashboard クラスタに追加されたファブリックは、デフォルトではサービスで有効になっていないため、Nexus Dashboard Insights から直接明示的に有効にする必要があります。
  - Nexus Dashboard にファブリックを追加し、Nexus Dashboard Insights の単一のワークフローでファブリックを有効にします。
- スナップショット ファブリック
  - ファブリック スナップショットを追加します。

オンライン ファブリックの追加

1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. **[ファブリック サイトの追加（Add fabric site）]** をクリックします。
   a. 初めて Nexus Dashboard Insights にファブリック 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。**[ファブリックの追加（Add Fabric）]** 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ファブリックを有効にするには、**[追加準備完了（Ready to Add）]** を選択します。Nexus Dashboard に追加されたファブリックが表示されます。Nexus Dashboard にファブリックを追加するには、『 Cisco Nexus Dashboard Fabrics 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. ファブリックを選択します。
   b. **[次へ（Next）]** をクリックします。
   c. マップからファブリックの場所を選択して、Nexus Dashboard でファブリックを識別します。
   d. **[次へ（Next）]** をクリックします。
   e. ドロップダウンリストからインバンド EPG を選択します。Nexus Dashboard Insights の場合、インバンド EPG は Nexus Dashboard とファブリック間の接続に使用されます。

f. トグルを使用して、IPv4 または IPv6 を選択してファブリックをオンボードします。Nexus Dashboard Insights は、この設定に基づいて、このファブリック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、ファブリックの IP アドレス構成と一致している必要があります。

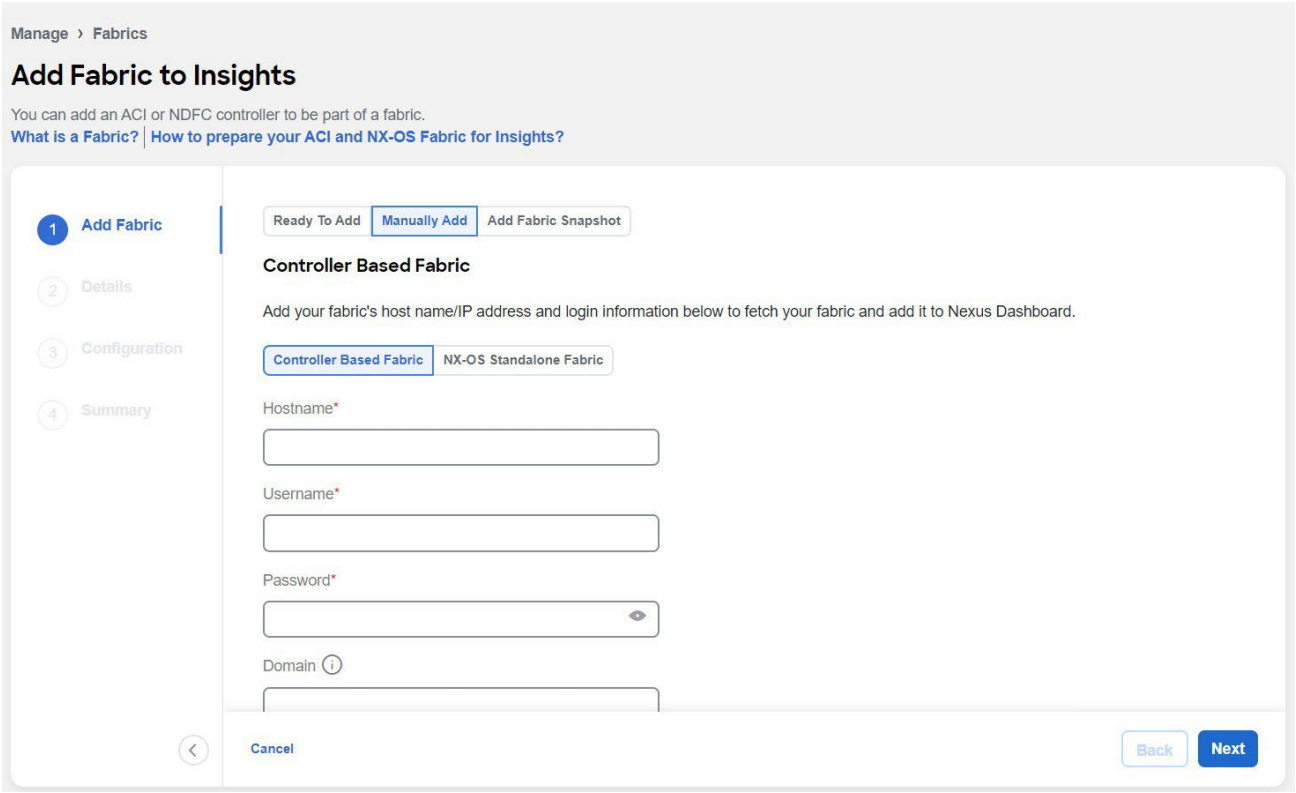
IPv6 は、Cisco APIC リリース 6.0(3) 以降でのみサポートされます。

g. **[次へ（Next）]** をクリックします。

h. 設定を確認します。

i. [送信（Submit）] をクリックします。

5. Nexus Dashboard にファブリックを追加し、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、ファブリック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 でファブリックを識別するためのサイト名を入力します。

f. マップからファブリックの場所を選択して、Nexus Dashboard でファブリックを識別します。

g. **[次へ（Next）]** をクリックします。

h. ドロップダウン リストからインバンド EPG を選択します。Nexus Dashboard Insights の場合、インバンド EPG は Nexus Dashboard とファブリック間の接続に使用されます。

i. トグルを使用して、IPv4 または IPv6 を選択してファブリックをオンボードします。Nexus Dashboard Insights は、この設定に基づいて、このファブリック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

j. は、ファブリックの IP アドレス構成と一致している必要があります。

IPv6 は、Cisco APIC リリース 6.0(3) 以降でのみサポートされます。

k. ユーザ名とパスワードを入力します。

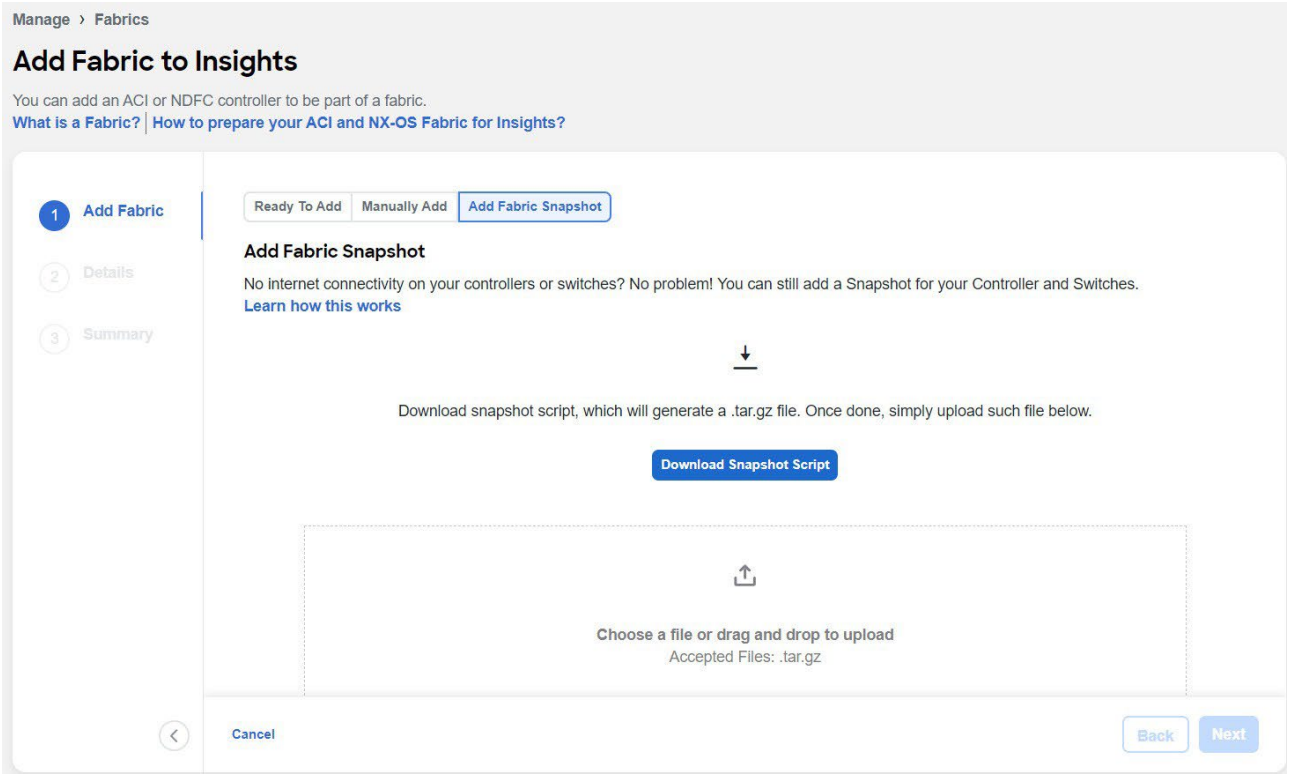
l. **[次へ（Next）]** をクリックします。

m. 設定を確認します。

n. [送信（Submit）] をクリックします。

ファブリック スナップショットを追加します。

1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. **[ファブリック ファブリックの追加（Add fabric site）]** をクリックします。
3. スナップショット ファブリックを追加するには、**[ファブリック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。

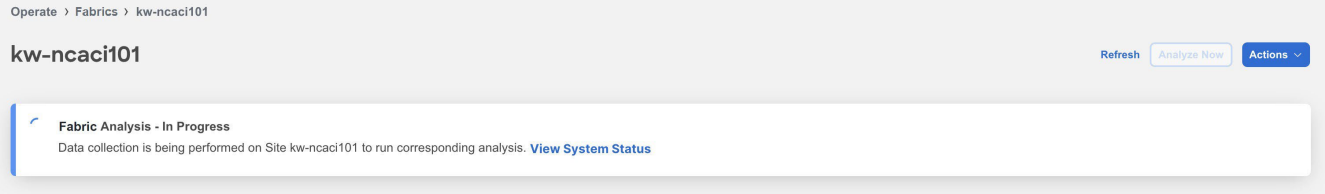
収集スクリプトを使用するには、システムに Python3 がインストールされている必要があります。

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 でファブリックを識別するためのファブリック名を入力します。

8. マップからファブリックの場所を選択して、Nexus Dashboard でファブリックを識別します。
9. **[次へ（Next）]** をクリックします。設定を確認します。
10. [送信（Submit）] をクリックします。

ファブリック分析

ファブリックがオンボーディングされ、完全に準備されると、{CiscoNIRShortName} はファブリック分析を開始してファブリックからデータを収集し、**[ファブリック（Fabrics）]** ページにファブリック情報を表示します。詳細については、「 ファブリック」を参照してください。[ファブリック分析（Fabric 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。

ファブリック分析中に、テレメトリ収集、アシュアランス分析、およびバグスキャン分析が自動的に実行されます。「分析ハブでの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、ファブリックからのデータ収集、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 ファブリック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 ファブリックの場合、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 ファブリックの場合、ワンタイム 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ガイドラインと制約事項

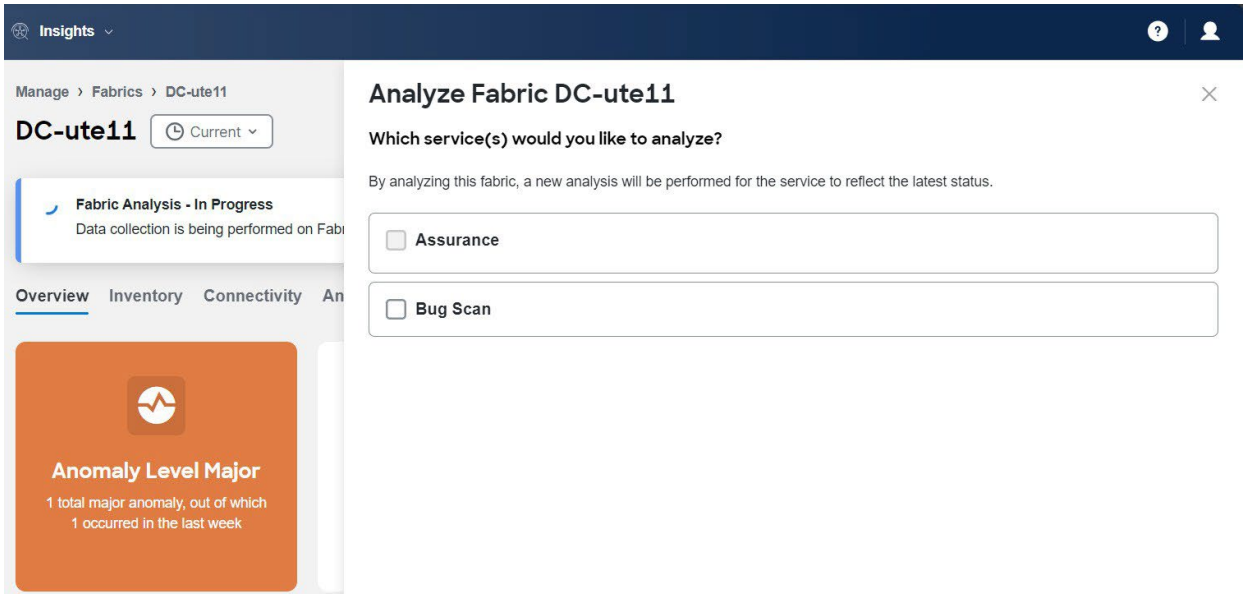
- ファブリックから保証分析を取得し、生データ セットをエクスポートしてファイルをスナップショット ファブリックにアップロードすると、スナップショット ファブリックの保証分析では保証関連の異常のみが生成されます。
- 現在、スナップショット ファブリックのアシュアランス分析を開始する場合、すでに進行中のファブリックのアシュアランス分析を同時に続行できます。アシュアランス分析はすべて、動作を中断することなく実行されます。
- アラート ルールとコンプライアンス ルールは、スナップショット ファブリックのアシュアランス分析で有効です。

オンデマンド分析

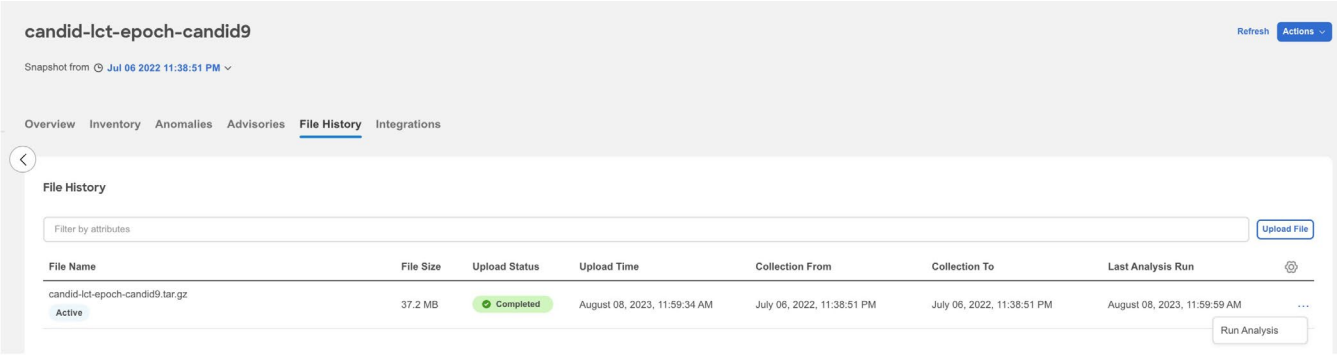
オンラインファブリックの場合、アシュアランス分析は自動的に実行されますが、いつでもリクエスト、要求など（文脈に応じて）することもできます。これは、ファブリック内の 1 つ以上の問題を解決し、次の自動実行を待たずに Nexus Dashboard Insights で最新の異常とアドバイザリ情報をポーリングする場合に役立ちます。

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）]** > **[ファブリック（Fabrics）]** に移動します。
2. ドロップダウンリストからオンライン ファブリックまたはスナップショット ファブリックを選択します。
3. オンライン ファブリックの場合は、ファブリック名をクリックして詳細を表示します。
   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。



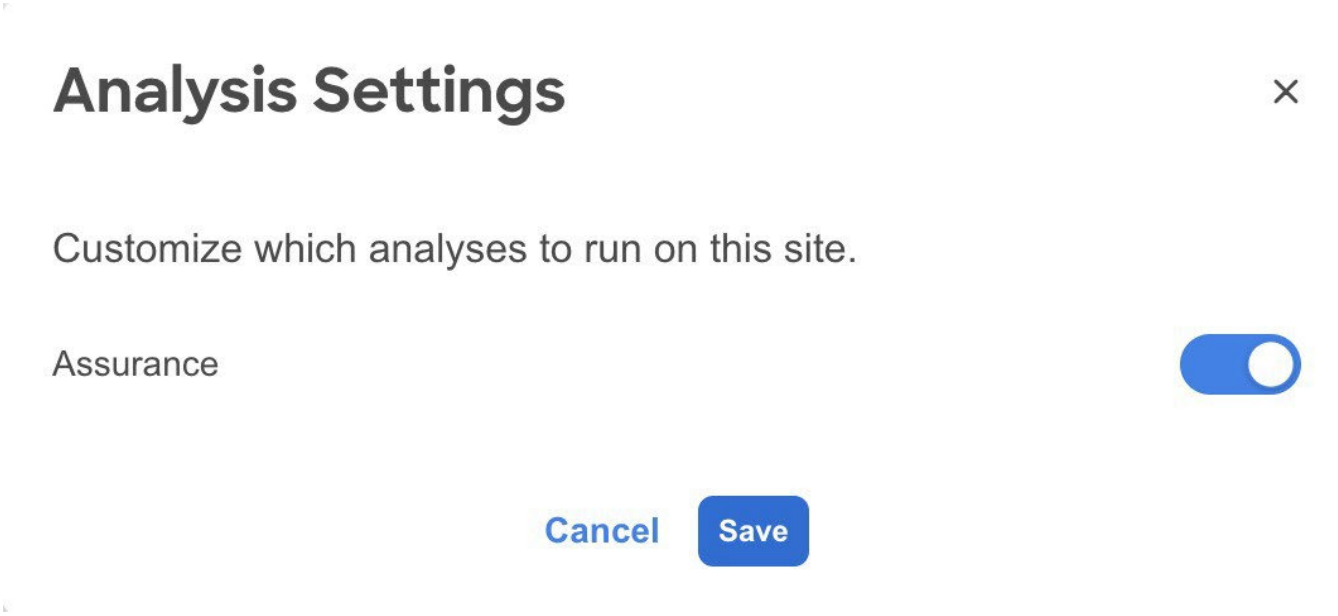
4. スナップショット ファブリックの場合は、ファブリック名をクリックして詳細を表示します。
5. **[ファイル履歴（File History）]** をクリックします。
6. **[ファイル履歴（File History）]** テーブルで、省略記号アイコンをクリックし、**[分析の実行（Run Analysis）]** を選択します。



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）]** > **[ファブリック（Fabrics）]** に移動します。
2. ドロップダウン リストからオンライン ファブリックを選択します。
3. ファブリック名をクリックして詳細を表示します。
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。



サービス チェーン アシュアランスのポリシーベースのリダイレクト

ポリシーベースのリダイレクト（PBR）のサポートにより、 Nexus Dashboard Insights アシュアランス エンジンは、デバイスクラスタ、デバイス選択ポリシー、vPC ノードの展開、および GoTo モードの管理されていない単一ノードのデバイスクラスタ展開との不整合をチェックします。

Nexus Dashboard Insights は、PBR サービス グラフを保証します。以下にリストされているすべての条件が満たされている場合、誤検出異常はありません。ただし、いずれかの条件が満たされていない場合、PBR サービスグラフは保証されず、誤検出が発生する可能性があります。

- サービス グラフ テンプレートは、ルート リダイレクトを有効にしておく必要があります。
- サポートされるサービス ノードは 1 つだけで、サービスノードは **[機能ノード（Function Node）]** プロパティで GoTo モードの機能タイプである必要があります。
- サービス グラフの直接接続オプションはサポートされていないため、値を **False** に設定する必要があります。
- プロバイダー/コンシューマ ブリッジ ドメインのセットは、シャドウ EPG ブリッジ ドメインのセットと重複してはなりません。さらに、すべてのシャドウ EPG に独自のブリッジ ドメインが必要です。
- プロバイダーEPG とコンシューマ EPG は、L3Out EPG、アプリケーション EPG、または vzAny EPG のいずれかのタイプである必要があります。
- PBR コントラクトを使用したトランジット回送の場合、プロバイダーL3Out とコンシューマ L3Out は異なる L3Out である必要があります。L3Out にある PBR 接続先はサポートされません。
- コントラクトごとに 1 つのサービスグラフが必要であり、サービスグラフは双方向である必要がありま

す。

- サービス グラフ テンプレートの下の関数ノード コネクタにフィルタが設定されていてはなりません。
- 契約ごとに 1 つのサービス グラフのみがサポートされます。
- 論理的なインターフェイス コンテキストのサブネットはサポートされていません。
- バックアップ PBR ポリシー機能（Cisco APIC リリース 4.2(1) で導入）はサポートされていません。
- threshold-redir コマンドを使用する場合は、しきい値の down アクションを permit に設定する必要があります。
- PBR サービス グラフ テンプレートのコントラクトからのフィルタはサポートされていません。

PBR の異常

Nexus Dashboard Insights リリース 6.5.1 では、異常であるサービスチェーンリダイレクトポリシー違反が PBR アシュアランスに追加されます。

サービス チェーン リダイレクト ポリシー違反 が生成される前に、次のチェックが実行されます。

- 1 つ以上のゾーン分割ルール コントラクトが欠落しているか、 APIC 構成と一致しない場合。
- 展開された PBR グラフによって使用されるリダイレクト接続先またはリダイレクト接続先グループが無効状態になっている場合。

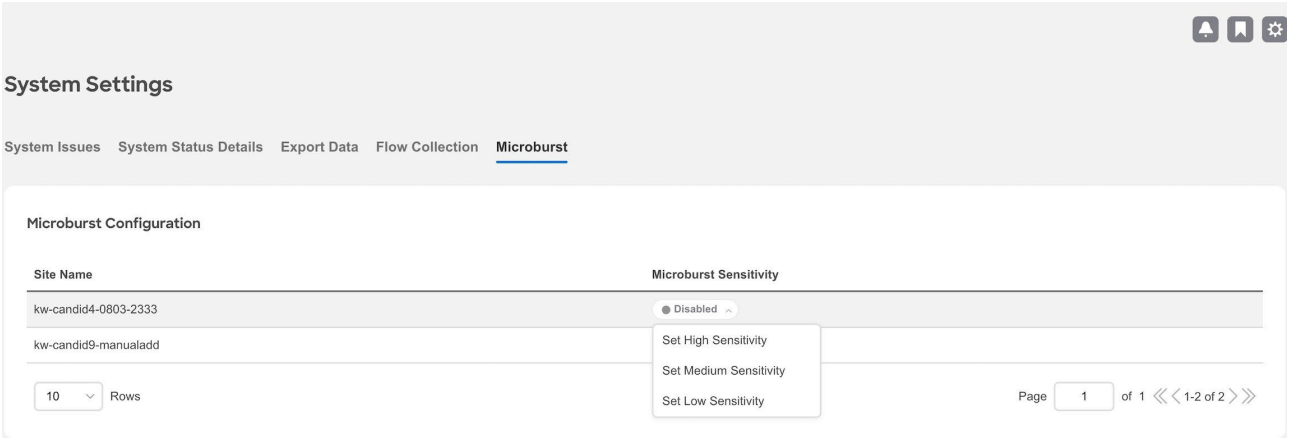
その結果、トラフィックはコントラクトとグラフ インスタンスで想定どおりにリダイレクトされません。

IP-SLA ポリシーまたは正常性グループが PBR リダイレクト ポリシーで有効になっていない場合、リダイレクト接続先に到達できない場合でも、異常 サービス チェーン リダイレクト ポリシー違反 は生成されません。この場合、異常 PBR リダイレクト接続先学習エラー が生成されます。

マイクロバースト

Nexus Dashboard Insights でマイクロバーストを設定するには、次の操作を実行します。

1. **[管理者（Admin）]** > **[システム設定（System Settings）]** > **[マイクロバースト（Microburst）]** に移動します。
2. **[マイクロバースト構成（Microburst Configuration）]** エリアで、ファブリックを選択し、**[マイクロバースト感度（Microburst Sensitivity）]** のドロップダウン メニューをクリックします。デフォルト値は **[無効（Disable）]** です。設定する適切な値を選択します。他の値には、**High Sensitivity** の設定、**Medium Sensitivity** の設定、**Low Sensitivity** の設定 があります。



しきい値の割合に基づいて、マイクロバーストは低、高、または中のいずれか分類されます。 次の

しきい値の割合は感度に反比例します。特定のインターフェイスでマイクロバーストの数が 100 を超える場合、異常が発生します。Nexus Dashboard Insights は、選択したファブリックのマイクロバース トデータを収集します。ノードのインターフェイスでマイクロバースト異常が発生します。

次の表に、マイクロバーストのしきい値を示します。

[機密性（Sensitivity）]	アップしきい値	ダウンしきい値
低	75%	50%
中	50%	25%
高	25%	5%

詳細はこちらをご覧ください。

- 詳細については、マイクロバーストの監視を参照してください。
- 詳細については、「サポート対象プラットフォーム」を参照してください。
- Nexus Dashboard Insights でマイクロバースト情報を表示するには、「インベントリ」を参照してください。

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。

使用上のガイドラインと制約事項

ここでは、Cisco Nexus Dashboard Insights の使用上のガイドラインと制限事項を示します。

- Nexus Dashboard Insights をダウングレードすることはできません。
- EPG のブリッジドメインまたは VRF インスタンスを変更した後、フロー分析が一時的に期待どおりに機能しません。
- マルチクラスタ設定では、リモート クラスタ システムの異常はローカル クラスタに表示されません。システム異常を表示するには、リモート クラスタにログインする必要があります。
- Nexus Dashboard Insights は、Cisco APIC に cisco_SN_NI というユーザーを作成します。このユーザーは、 Nexus Dashboard Insights が変更を加えたり、Cisco APIC から情報をクエリしたりする必要がある場合に使用されます。Cisco APIC GUI で、**[システム（System）] > [履歴（History）] > [監査ログ（Audit Logs）]**の順に選択します。 cisco_SN_NI ユーザーが **[ユーザー（User）]** 列に表示されます。

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、送信元と宛先の EPG と VRF 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
- 物理インターフェイス
- ポート チャネル インターフェイス
- Routed Sub-Interfaces
- SVI

UI からルーテッド サブインターフェイスを構成する場合は、[L3 Out] を選択します。

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

- Cisco APIC で NTP が設定され、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 Insights 展開ガイド』 および「Precision Time Protocol (PTP) for Cisco Nexus Dashboard Insights」を参照してください。
- すべてのフローは、ファブリック タイプ ACI および DCNM/NDFC の統合されたパイプラインの統合ビューとして監視され、フローは同じ Cisco Umbrella の下に集約されます。
- 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。
- ユーザーは、必要に応じて、フローテレメトリと NetFlow のトグルボタンを有効にできます。いずれかのオプションを有効にすることをお勧めします。
- 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 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)
- Nexus Dashboard クラスタが EPG 経由で ACI ファブリックに直接接続されている場合：

- mgmt:inb vrf にネイティブ ルートまたはリークされたデフォルト ルートがないことを確認します。
- Nexus Dashboard データ ネットワーク サブネットが ACI ファブリック インバンド サブネットと異なることを確認してください。

- 次の Cisco Nexus 9000 ACI モードスイッチバージョンは、Nexus Dashboard Insights フローテレメトリではサポートされていません。
  - 14.2(4i)
  - 14.2(4k)
  - 15.0(1k)

    1 つ以上のサポートされていないスイッチを含むファブリックのフロー収集を有効にすると、フローのステータスは **[**無効（**Disabled**）**]** と表示されます。スイッチをサポートされているバージョンにアップグレードすると、フローのステータスは [Enabled] と表示されます。

- インターフェイス ベースのフロー テレメトリは、リーフ スイッチでのみサポートされ、スパイン スイッチではサポートされません。
- 次の Cisco Nexus 9000 ACI モード スイッチ バージョンは、インターフェース ベースのフロー テレメトリ用の Nexus Dashboard Insights では、次のバージョンがサポートされています。
  - Cisco APIC リリース 6.0(3) 以降
  - Cisco NX-OS リリース 16.0(3) 以降

  インターフェイス ベースのフロー テレメトリは、 Cisco NX-OS リリース 16.0(2) のベータ機能です。

フロー テレメトリ ルールのガイドラインと制限事項：

- ノードは、VRF モードまたはインターフェイス モードのいずれかで動作できます。ルールが物理/ポートチャネル/L3out/ SVI で構成されている場合、ノードはインターフェイス モードで動作します。VRF ルールとインターフェイス ルールの両方が構成されている場合、インターフェイス ルールが優先されて有効になりますが、VRF ルールは有効になりません。ノードで複数の VRF ルールが構成され、インターフェイス ルールを構成するシナリオを考えてみましょう。その場合、ノード内のすべてのルールがインターフェイスルールに変換され、インターフェイス ルールのみがそのノードで現用系になります。そのノードからインターフェイス ルールを削除すると、ルールは VRF モードに変換されます。
- サブネットでインターフェイス ルール（physical/portchannel/L3out/SVI ）を構成すると、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。
- ノードで設定できる論理的なインターフェイスの最大数（物理インターフェイス、ポート チャネル、L3Out、および SVI の合計を含む）は 63 です。
- ノードには最大 500 のルールを構成できます。

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. **[ファブリックごとのフロー収集（Flow Collection per Fabric）]** テーブルで、ファブリックを選択し、省略記号アイコンをクリックします。
4. **[フロー収集モードの編集]** 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. **[ファブリックごとのフロー収集（Flow Collection per Fabric）]** テーブルで、ファブリックを選択し、省略記号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. **[テナントの選択（Choose a Tenant）]** ドロップダウンリストから、テナントを選択します。
      iii. **[VRF]** ドロップダウン リストから VRF を選択します。
      iv. **[サブネット（Subnets）]** エリアで、フロー トラフィックをモニターするサブネットを入力し

ます。同じエンドポイントグループにエンドポイントがある場合は、サブネットをモニターするルールを提供できます。

v. **[**サブネットの追加（**Add Subnet**）**]** 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. 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、構成は拒否されます。

iv. **[**サブネット（**Subnets**）**]** エリアで、フロー トラフィックをモニターするサブネットを入力します。

v. **[**サブネットの追加（**Add Subnet**）**]** をクリックします。

c. **[**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、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. 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。

iv. **[**サブネット（**Subnets**）**]** エリアで、フロー トラフィックをモニターするサブネットを入力します。

v. **[**サブネットの追加（**Add Subnet**）**]** をクリックします。

c. **[**保存（**Save**）**]** をクリックします。

8. L3Out ルールを追加するには、**[L3Out]** 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. それぞれのドロップダウン リストから、テナント、L3Out、カプセル化、およびインターフェイスを選択します。

ノードで L3Out が構成されていない場合は、ドロップダウン リストから項目を選択できず、フロー ルールを構成できません。

L3Out ベースのインターフェイス ルールの場合、サブインターフェイス タイプ L3Out を
L3Out ドロップダウン メニューから選択できます。
ポートチャネル、 SVI、物理インターフェイスなどの他の L3Out ルールを構成するには、それぞれのタブをクリックします。

iv. **[**サブネット（**Subnets**）**]** エリアで、フロー トラフィックをモニターするサブネットを入力します。

v. **[**サブネットの追加（**Add Subnet**）**]** をクリックします。

vi. **[**保存（**Save**）**]** をクリックします。

9. SVI ルールを追加するには、**[SVI]** 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. それぞれのドロップダウン リストから、テナント、L3Out、およびカプセル化を選択します。

iv. **[**サブネット（**Subnets**）**]** エリアで、フロートラフィックをモニターするサブネットを入力します。

v. **[**サブネットの追加（**Add Subnet**）**]** をクリックします。

c. **[**保存（**Save**）**]** をクリックします。

10. **[**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。ルールはファブリックにプッシュされ、ファブリック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. **[**操作（**Operate**）**]** > **[**ファブリック（**Fabrics**）**]** ページに移動します。
2. ファブリックを選択します。
3. **[**ファブリック（**Fabrics**）**]** と **[**スナップショット（**Snapshot**）**]** の値が適切であることを確認します。デフォルトのスナップショット値は 15 分です。選択すると、選択したファブリックまたはスナップショット ファブリック内のすべてのフローがモニターされます。
4. **[**接続（**Connectivity**）**]** > **[**フロー（**Flows**）**]** に移動し、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。

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	はい	はい	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	非対応	非対応	非対応

NetFlow タイプ

現在、Full NetFlow タイプは Cisco Nexus Dashboard Insights でサポートされています。

Full NetFlow では、設定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。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。

NetFlow のガイドラインと制約事項

- ACI タイプの Cisco Nexus Dashboard Insights では、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。ただし、ファブリック構成に基づいて、使用するフローのモードを決定できます。
- フロー テレメトリと Neflow の両方を有効にすることは、Cisco ACI ファブリックではサポートされていません。

- 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。
- NetFlow の場合、Cisco Nexus Dashboard では、クラスタ設定の下に永続的な IP アドレスを構成する必要があり、データ ネットワークと同じサブネットに 7 つの IP アドレスが必要です。
- Nexus Dashboard Insights で NetFlow を有効にしたら、NetFlow コレクタの IP アドレスを取得し、コレクタの IP アドレスを使用して Cisco APIC を設定する必要があります。「Cisco APIC と NetFlow」を参照してください。

  NetFlow コレクタの IP アドレスを取得するには、**[管理（Admin）]** > 、**[システム設定（System Setting）]** > **[フロー収集（Flow Collection）]** の順に選択します。**[ファブリックごとのフロー収集（Flow Collection per Fabric）]** テーブルで、**[コレクタ リスト（Collector List）]**列で **[表示（View）]** をクリックします。

- NetFlow および sFlow フロー収集モードは、異常をサポートしません。

NetFlow の設定

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. **[ファブリックごとのフロー収集（Flow Collection per Fabric）]** テーブルで、ファブリックを選択し、省略記号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。ACI タイプではサポートされていないため、[sFlow]ボタンはグレー表示のままになります。
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。デフォルトでは、エクスポートデータは 30 秒ごと、またはそれ以下の頻度で収集されます。

Nexus Dashboard Insights リリース 6.0.2 以降、個別のデータパイプラインを使用して、リーフスイッチとスパインスイッチから特定のリソース（CPU、メモリ、およびインターフェイス使用率）のデータを 10 秒ごとに*収集することもできます。*さらに、コントローラの CPU とメモリのデータが収集されます。収集されたデータは、Nexus Dashboard Insights によって Elasticsearch に保存されませんが、消費のために直接エクスポートされ、リポジトリにプッシュされます。その後、Kafka エクスポート機能を使用して、このデータを Kafka ブローカーにエクスポートし、データを消費してデータレイクにプッシュできます。

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約事項

- 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 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。
- 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。
- エクスポート データは、スナップショット ファブリックではサポートされていません。
- **[**アラートとイベント（**Alerts and Events**）**]** 用に現在サポートされている 5 つの Kafka Exporter に加えて、**[**使用状況（**Usage**）**]** 用の Kafka エクスポートのために最大 5 つのエクスポータがサポートされます。
- エクスポートごとに一意の名前を指定する必要があり、**[**アラートとイベント（**Alerts and Events**）**]** 用の Kafka エクスポートと **[**使用状況（**Usage**）**]** 用の Kafka エクスポートの間で名前を繰り返し使用することはできません。
- 次の各オプションに対して個別の Kafka エクスポートセッションを構成できます。**[**アラート（**Alerts**）**]** と **[**イベント（**Events**）**]** と **[**使用状況（**Usage**）**]**。
- 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。

アラートと収集タイプに対して Kafka エクスポータを p 構成します

アラートおよびイベント収集タイプの Kafka エクスポータを構成するには、次の手順を実行します。

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. **[新しいメッセージバス構成の追加（Add New Message Bus Configuration）]** ページの **[ログイン情報（Credentials）]** エリアにある **[ファブリック名（Fabric Name）]** フィールドで、適切なファブリックを選択します。
   b. **[IP アドレス（IP Address）]** および **[ポート（Port）]** フィールドに、適切な 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（Unsecured）]**、**[セキュア SSL（Secured SSL）]** および **[SASLPLAIN]** です。デフォルト値は **[非セキュア（Unsecured）]** です。

      [セキュア SSL（Secured SSL）] の場合は、次のフィールドに塗りつぶしします。

      - **[サーバー CA 証明書（Server CA Certificate）]**：コンシューマ証明書の署名に使用される CA 証明書 Nexus Dashboard Insights がコンシューマを信頼できるように、信頼ストアに保存されます。
      - クライアント証明書： Nexus Dashboard Insights の CA 署名付き証明書。通常、証明書は同じ CA によって署名され、同じ CA 証明書がコンシューマの信頼ストアに格納されます。これは、エクスポートに使用される Nexus Dashboard Insights の Kafka キーストアに保存されます。
      - クライアント キー（**Client Key**）： Kafka プロデューサの秘密キー（この場合は Nexus Dashboard Insights）。これは、エクスポートに使用される Nexus Dashboard Insights の Kafka キーストアに保存されます。

      SASLPLAIN の場合は、次のフィールドに入力します。

      - **[ユーザー名（Username）]**：SASL/PLAIN 認証のユーザー名。
      - **[パスワード（ パスワード）]**：SASL/PLAIN 認証のパスワード。

   d. **[収集タイプ（Collection Type）]** エリアで、**[アラートとイベント（Alerts and Events）]** を選択します。
   e. **[収集設定（Collection Settings）]** エリアで、[基本（Basic）] または [詳細（Advanced）] 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。電子メールスケジューラを設定する場合は、「電子メールの設定」の手順を参照してください。

収集タイプ（使用状況）用の Kafka Exporter の構成

使用状況収集タイプの Kafka エクスポータを構成するには、次の手順を実行します。

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. **[新しいメッセージバス構成の追加（Add New Message Bus Configuration）]** ページの **[ログイン情報（Credentials）]** エリアにある **[ファブリック名（Fabric Name）]** フィールドで、適切なファブリックを選択します。

   b. **[IP アドレス（IP Address）]** および **[ポート（Port）]** フィールドに、適切な 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（Unsecured）]**、**[セキュア SSL（Secured SSL）]** および **[SASLPLAIN]** です。デフォルト値は **[非セキュア（Unsecured）]** です。

      [セキュア SSL（Secured SSL）] の場合は、次のフィールドに塗りつぶしします。

      - **[サーバー CA 証明書（Server CA Certificate）]**：コンシューマ証明書の署名に使用される CA 証明書は Nexus Dashboard Insights がコンシューマを信頼できるように、信頼ストアに保存されます。
      - クライアント証明書： Nexus Dashboard Insights の CA 署名付き証明書。通常、証明書は同じ CA によって署名され、同じ CA 証明書がコンシューマの信頼ストアに格納されます。これは、エクスポートに使用される Nexus Dashboard Insights の Kafka キーストアに保存されます。
      - クライアントキー（**Client Key**）： Kafka プロデューサの秘密キー（この場合は Nexus Dashboard Insights）。これは、エクスポートに使用される Nexus Dashboard Insights の Kafka キーストアに保存されます。

      SASLPLAIN の場合は、次のフィールドに入力します。

      - **[ユーザー名（Username）]**：SASL/PLAIN 認証のユーザー名。
      - **[パスワード（ パスワード）]**：SASL/PLAIN 認証のパスワード。

   d. **[収集タイプ（Collection Type）]** エリアで、**[使用状況（Usage）]** を選択します。デフォルト値は **[アラートとイベント（Alerts and Events）]** です。選択した収集タイプに応じて、この領域に表示されるオプションが変わります。

3. **[収集設定（Collection Settings）]** エリアの **[データ（Data）]** の下に、収集設定の **[カテゴリ（Category）]** と **[技術情報（Resources）]** が表示されます。

   デフォルトでは、CPU、メモリ、およびインターフェイス使用率のデータが収集されて、エクスポートされます。これらのリソースのサブセットをエクスポートすることはできません。

4. [保存（Save）] をクリックします。

[使用状況]用の Kafka エクスポートが有効になっています。

電子メールの設定

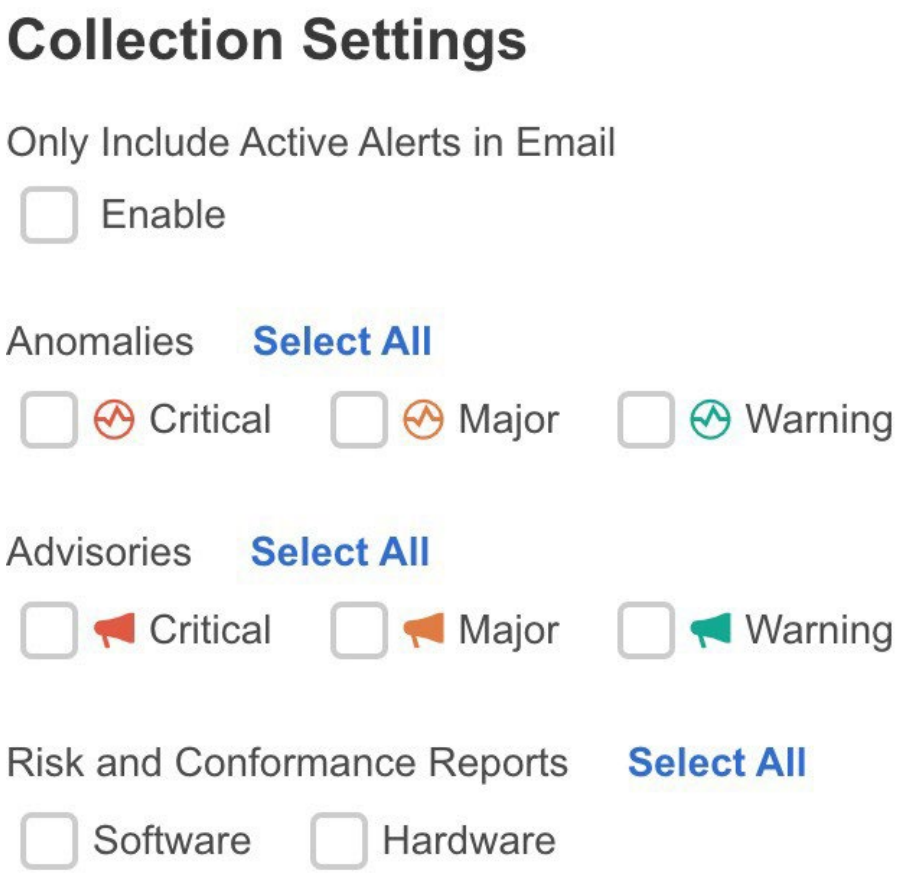
次の手順を使用して、Nexus Dashboard Insights から収集されたデータの概要を送信する電子メールスケジューラを設定します。

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 **[ファブリック名（Site Name）]** ィールドで、ファブリック名を選択します。
   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ファブリックを選択し、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。

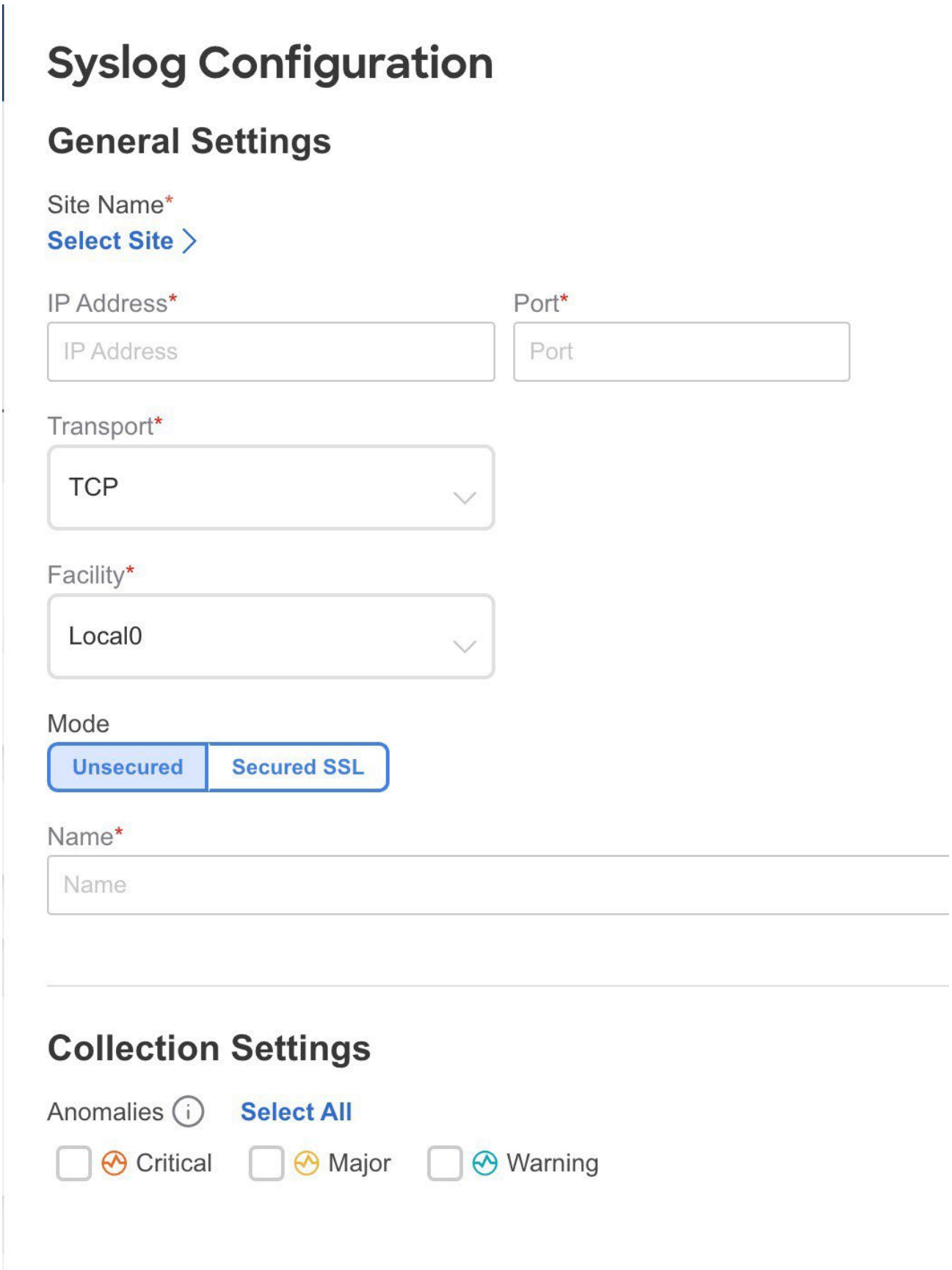
Syslog のガイドラインと制約事項

- 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。
- Nexus Dashboard Insights は、ファブリック全体で最大 5 つの syslog エクスポータ構成をサポートします。

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]** フィールドで、**[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. **[**ファブリック名（**Fabric Name**）**]**フィールドで、**[**ファブリックの選択（**Select Fabric**）**]** をクリックし、ファブリック名を選択します。

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（NDFC ファブリックのみ）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 の管理コンソールで、**[**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

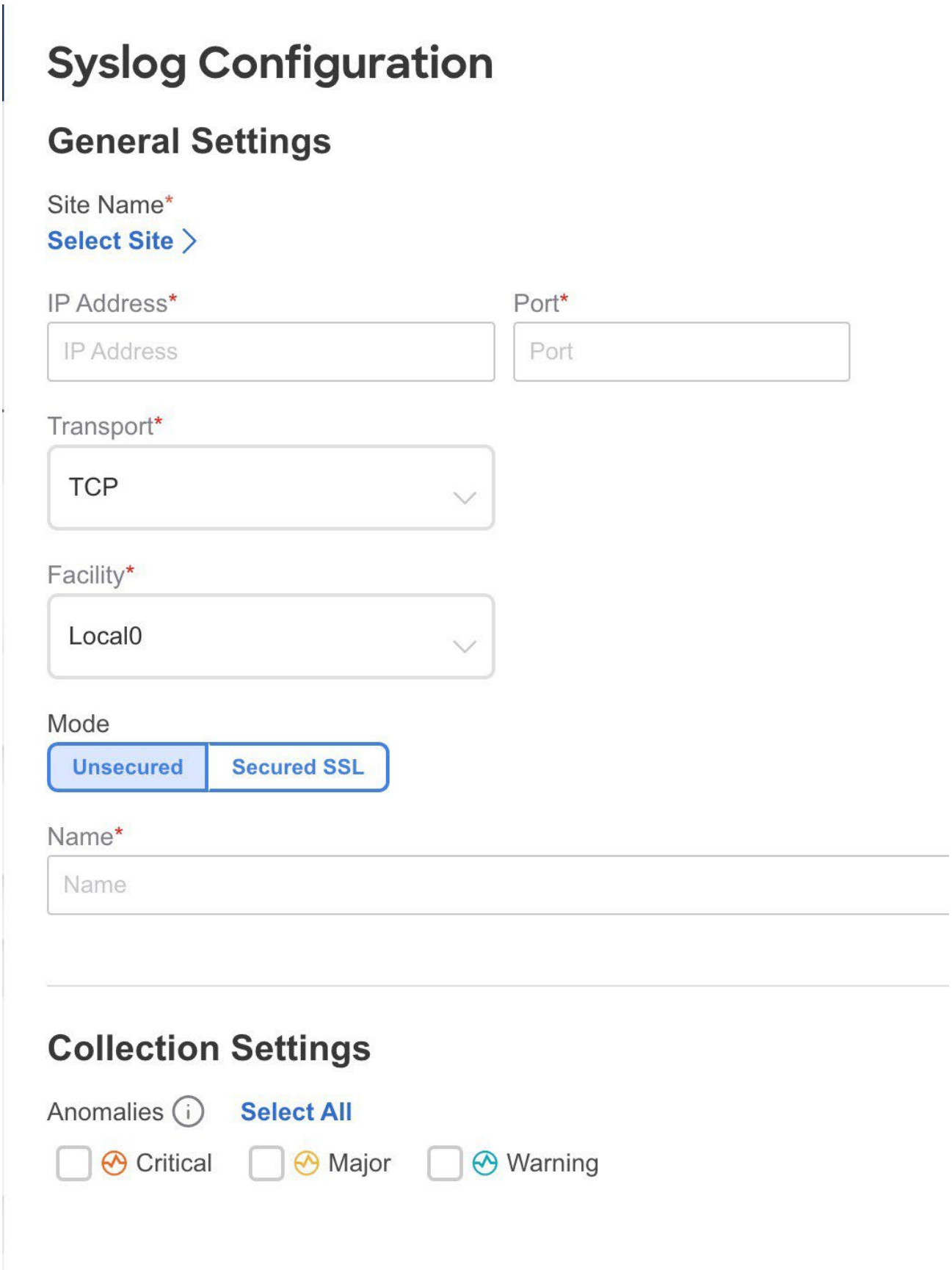
      NAS に書き込みます。

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. **[**ファブリックの選択（**Select Fabric**）**]** をクリックして、ファブリックを選択します。一度に選択できるファブリックは 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," ingressBur
st" :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,,,,,,,,\\\"]]" }

システム設定

システムの問題

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。

- ファブリック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。

システムの問題の表示

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。**[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。
3. 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、過去 1 時間のファブリックの収集ステータスが表示されます。

Nexus Dashboard Insights は、ファブリック 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。

- Fabric)
- ノード
- アシュアランス
- 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**）**]** > **[**ファブリック（**Fabrics**）**]** に移動します。
2. ファブリックを選択します。
3. [ファブリック（Fabrics）] 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
- 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。[ユーザー設定（User Preferences）] は、カスタム ダッシュボード と ブックマーク 情報 を指します。ユーザー設定は含まれません。

Nexus Dashboard Insights のバックアップと復元

Nexus Dashboard Insights 6.5.1 リリースでは、 Cisco Nexus Dashboard レベルでの統合バックアップおよび復元機能が導入されています。これにより、 Nexus Dashboard だけでなく、その Nexus Dashboard で実行されているサービス（Nexus Dashboard Insights など）の設定情報もバックアップされます。

統合バックアップと復元機能を使用して Nexus Dashboard レベルで構成をバックアップおよび復元する場合でも、 Nexus Dashboard Insights レベルでの設定の既存のインポートおよびエクスポート プロセスは、 Nexus Dashboard Insights 展開をバックアップおよび復元に引き続き使用できます。これは、Nexus Dashboard Insights 6.5.1 リリースより前のリリースから Nexus Dashboard Insights のバックアップを復元する場合に必要です。

例：

- Nexus Dashboard Insights リリース 6.5.1 以降から構成をバックアップし、そのバックアップから復元する場合は、「Nexus Dashboard およびサービスの統合バックアップおよび復元」で説明されているように、新しい統合バックアップおよび復元機能を使用します。
- Nexus Dashboard Insights の 6.5.1 以前を使用しており、そのバックアップを復元する場合は、そのバックアップを復元する Nexus Dashboard Insights での構成のインポートとエクスポートを使用します。

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 ファブリック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 ファブリックは、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設定の tar.gz ファイルと同じ名前で最初に Nexus Dashboard Insights でオンボード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。
- エクスポートされた APIC 構成を APIC にインポートすると、キーの不一致が原因で、 Nexus Dashboard Insights の一部の機能が期待どおりに動作しない場合があります。Nexus Dashboard の管理コンソールと Nexus Dashboard Insights からファブリックを削除してから、同じファブリック名を使用してファブリックを追加必要があります。

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。ファブリック、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。**[**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。
5. 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。
6. 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）。