Cisco Nexus Dashboard Insights Analysis Hub、リリース 6.5.1 - Cisco NDFC またはスタンドアロン NX-OS

Cisco Confidential

目次

Cisco Confidential

初版：2024 年 7 月 23 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。

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
バグ スキャンに含まれるバグ説明	バグ スキャンの [バグ（Bugs）] エリアのバグのテーブルに、各バグの説明が含まれるようになりました。	6.5.1	
サステナビリティ レポートの上位 5 デバイス	サステナビリティ レポートでは、推定コスト、消費エネルギー、温室効果ガス（GHG）排出量の上位 5 デバイスが表示されます。	6.5.1	スイッチのサステナビリティ レポートの表示
Cisco エネルギーの活用マネージャの代わりに電力マップ	Nexus Dashboard Insights は、エネルギーコストと温室効果ガス（GHG）の排出量データを Cisco Energy Manager [電気マップ（Electricity Maps）] の代わりに取得します。オプション 2 は、Cisco Energy Manager は、より堅牢なメソッドをデータの収集に提供し、シングルポイント障害の可能性や、あるリージョンのデータがないことを避けることができます。	6.5.1	持続可能性レポート
オペレーション、 [メンテナンス（OAM）（Maintenance (OAM)）] の [OAM] オプションでは、トラフィックを必要とせずに、接続の分析	[管理（Administration）] および接続の分析 ホスト間のアクティブなアクティブなホストの潜在的なドロップで NDFC のサポ	6.5.1	接続の分析

	ートを見つけたり、VXLAN EVPN ベースのファブリック トポロジでフローの到達可能性や実際のルートなどの詳細を追跡したりすることを可能にします。		
特長	説明	リリース	参照先
用語の	「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、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。

適合性レポート

適合性レポート

適合性レポートでは、ネットワークのハードウェアおよびソフトウェアのライフサイクルを可視化し、理解できます。これは、アップグレードとハードウェアの更新を計画するのに役立ちます。適合性レポートは、ハードウェアおよびソフトウェアの適合性についてはファブリックごとに毎日、スケールの適合性についてはファブリックごとに毎週作成されます。レポートでは、ソフトウェア、ハードウェア、ソフトウェアとハードウェアの組み合わせ、ファブリックのスケールの適合性ステータスを確認することができます。

適合性レポートを活用し、既知の EoS および EoL 通知に対してネットワークでソフトウェアおよびハードウェア インベントリの現在のステータスを確認し今後の見通しを予測して、適合性を確認します。オンボード ファブリックのスケール適合性ステータスもモニタできます。

適合性レポートを使用すると、次のことができます。

- 販売終了（EoS）またはサポート終了（EoL）スイッチを実行するリスクを最小限に抑えます。
- 既知の EoS および EoL 通知に対してネットワークでソフトウェアおよびハードウェア インベントリの現在のステータスを表示して、適合性を確認します。
- ネットワーク内のソフトウェアおよびハードウェアのインベントリの将来的な見通しを予測します。
- オンボード ファブリックのスケール適合性ステータスをモニタします

適合性レポートは、選択されたファブリックのソフトウェア、ハードウェア、およびスケールの適合性ステータスの概要を表示します。

適合性レポートでは、ハードウェアおよびソフトウェアの場合、適合スイッチはソフトウェアのリリースまたはハードウェアのプラットフォーム EoL の日付および PSIRT の終了日に基づき、3 つの重大度に分類されます。重大度には次のものがあります。

- [重大（Critical）] : PSIRT 終了日または最終サポート日が過去に発生しました。
- [注意（Warning）] : ソフトウェア リリースの EoL 日付またはハードウェア リリースの EoS が過去に発生しました。
- [正常性（Healthy）] : PSIRT 終了日、または サポート終了日、および EoL 日、またはソフトウェア リリースあるいはハードウェア リリースの EoS が将来発生する、またはソフトウェア リリースの EoL、ハードウェア リリースの EoS が発表されません

販売終了およびライフサイクル終了のお知らせにあるソフトウェアメンテナンスリリースの終了日、およびPSIRTの終了日は、インベントリをクリティカル、警告、または正常のカテゴリに分類するための参照マイルストーンとして使用されます。

適合性レポートでは、ファブリックのスケール適合性ステータスは、該当する場合、スイッチおよびコントローラで実行しているソフトウェア バージョンの Cisco の検証済みスケーラビリティ ガイドラインに基づいています。重大度には次のものがあります。

- 適合：すべてのメトリック値が90%未満です。
- 到達制限：1つ以上のメトリック値が90% ~ 100%です。

- 違反制限：1つ以上のメトリック値が100%を超えています。

適合性レポートへのアクセス

[分析（Analyze）] > [分析ハブ（Analysis Hub）] > [適合性

（Conformance）] に移動します。ドロップダウン メニュー

からファブリックを選択します。

または

[操作（Operate）] > [ファブリック

（Fabrics）] ページに移動します。フ

ァブリックを選択します。

[全般（General）] セクションで、[適合性

（Conformance）] をクリックします。**[**レポー

トの表示（**View Report**）**]** をクリックします。

適合性レポートの表示

ブラウザ印刷オプションがある PDF として適合性レポートを保存できます（Chrome および Firefox でのみサポート）。

1. [適合レポート（Conformance Report）] に移動します。「適合性レポートへのアクセス」を参照してください。
2. ドロップダウン メニューからファブリックまたはすべてのファブリックを選択します。
3. ドロップダウン メニューから現在の月または前の月を選択します。前の月のレポートが使用可能な場合にのみ、前の月を選択できます。

   適合性レポートには、適合性の概要、ハードウェアとソフトウェアの適合性、およびスケール適合性が表示されます。

4. [概要（Summary）] ページには、ハードウェアの適合性ステータス別のデバイス、ソフトウェアの適合性ステータス別のデバイス、ファブリックまたはスイッチのスケールの適合性ステータスが表示されます。詳細については、[適合基準の表示（View Conformance Criteria）] をクリックしてください。
5. [ハードウェア（Hardware）] または [ソフトウェア（Software）] ページには、適合性ステータス、適合性の見通し、デバイスの詳細が表示されます。
   a. [適合性見通し（Conformance Outlook）]セクションで、[全体（ **Overall**）]、[ソフトウェア（ **Software**）]、または [ハードウェア（ **Hardware** ）] をクリックして、ソフトウェアとハードウェア、ソフトウェアのみ、またはハードウェアのみの適合性を表示します。
   b. [デバイスの詳細（Device Details）] リストで、ハードウェアおよびソフトウェアの詳細を説明します。
   c. ハードウェアの詳細には、デバイス名、ファブリック名、ハードウェア適合性ステータス、モデル、ロール、特定のデバイスの脆弱性サポート終了ハードウェアが含まれます。デバイス名をクリック

して、追加の詳細を表示します。

d. ソフトウェアの詳細には、デバイス名、ファブリック名、ソフトウェア適合性ステータス、モデル、ソフトウェア バージョン、ロール、特定のデバイスの脆弱性サポート終了ソフトウェアが含まれます。デバイス名をクリックして、追加の詳細を表示します。

e. 検索を使用して、デバイス、ファブリック、ハードウェア適合性ステータス、ソフトウェア適合性ステータス、モデル、ソフトウェア バージョン、およびロールなど属性別にフィルタします。

f. 歯車アイコンを使用して、テーブルの列をカスタマイズします。

6. [スケール（Scale）] ページには、すべてのファブリックの概要、スケール適合性、およびスケール メトリックが表示されます。

a. [すべてのファブリックの概要（All Fabrics Summary）] セクションには、全体的なスケール適合レベル、拡張性メトリック違反による上位 5 つのスイッチ、コントローラとスイッチの拡張性メトリック、および拡張性メトリック違反の合計が表示されます。

b. 詳細については、[適合基準の表示（View Conformance Criteria）] をクリックしてください。

c. [スケール適合性（Scale Conformance）]セクションには、過去 6 ヵ月間のコントローラとスイッチのスケール適合性が表示されます（前の月のスケール レポートが使用可能な場合）。

d. [すべてのスケール メトリック（All Scale Metrics）] セクションには、ファブリックとスイッチのスケール メトリックの詳細が表示されます。ドロップダウン メニューから [すべてのファブリック（All fabrics）] を選択すると、[すべてのスケール メトリック（All Scale Metrics）] セクションが表示されます。

i. ファブリックの詳細には、ファブリック名、タイプ、ソフトウェア バージョン、コントローラ メトリクス適合性、スイッチ メトリクス適合性を含みます。ファブリック名をクリックして、追加の詳細を表示します。

ii. スイッチの詳細には、スイッチ名、ファブリック名、ソフトウェア バージョン、モデル、転送スケール プロファイル、メトリクス適合性などが含まれます。スイッチ名をクリックすると、追加の詳細が表示されます。

iii. 検索を使用して、ファブリック、タイプ、ソフトウェア バージョンなどの属性でフィルタします。

iv. 歯車アイコンを使用して、テーブルの列をカスタマイズします。

e. [ファブリック レベル スケール メトリック（Fabric Level Scale Metrics）] および [スイッチ レベル スケール メトリック（Switch Level Scale Metrics）] では、ファブリックおよびファブリックに関連付けられているスイッチのスケール メトリックを表示します。ドロップダウン メニューからファブリックを 1 つ選択すると、これらのセクションが表示されます。

i. ファブリックの詳細には、メトリック、適合性ステータス、およびリソースの使用状況が含まれます。

ii. スイッチの詳細には、スイッチ名、ファブリック名、ソフトウェア バージョン、モデル、転送スケール プロファイル、メトリクス適合性などが含まれます。スイッチ名をクリックすると、追加の詳細が表示されます。

7. [アクション（Actions）] メニューから、**[**レポートの実行（**Run Report**）**]** をクリックして、オンデマンド レポートを実行します。

接続の分析

接続の分析

接続分析を使用すると、2つの異なるエンドポイント間のフローを分析して、エンドポイントがどのように接続されているかを把握し、問題が発生している可能性のある場所を特定できます。

接続性分析は、特定のフローについてネットワーク内の問題のあるノードを検出して分離するものであり、次の機能を備えています。

- 送信元から宛先エンドポイントまでの特定のフローについて、考えられるすべての転送パスをトレースします。
- 問題のあるデバイスを特定し、フローをドロップさせます。
- 転送パス チェックの実行、整合性チェッカーによるソフトウェアおよびハードウェア状態のプログラミングの不整合、パケット ウォークスルーに関する詳細など、問題の根本原因を絞り込むのに役立ちます。

接続分析オプション

- Embedded Logic Analyzer Module (ELAM) : ELAM は、イーサネット トラフィック フローのトラブルシューティングに役立つ診断ツールです。アクティブフローからパケットをキャプチャし、イーサネットフレームのパケットドロップを分析します。ELAMでは、送信元ホストと宛先ホスト間のアクティブフローが必要です。このオプションを有効にして、利用可能なアクティブ フローを分析できます。
- Operations, Administration, and Maintenance (OAM) : OAM は、イーサネットネット ワークをモニタリングおよびトラブルシューティングするためのプロトコルです。このオプションを有効にすると、ホスト間にアクティブトラフィックがない状態でも、アクティブホストの潜在的なドロップを特定したり、VXLAN EVPN ベースのファブリックトポロジ内にあるフローの到達可能性や想定ルートなどの詳細を追跡したりできます。OAMは、VXLAN ファブリックでのみサポートされます。
- [整合性チェッカー（Consistency Checker）] : 整合性チェッカーは、ソフトウェアとハードウェアのテーブル間の配置性を検証することで、システムの一貫性を確保し、根本原因の分析と障害の切り分けを支援します。これらのチェックは、選択されたエンドポイント カンバセーションに関連するすべてのネットワーキング エンティティのデータ プレーンとコントロール プレーン間の各スイッチ内で実行されます。このオプションを有効にすると、指定されたエンドポイントまたはルート間のフローに沿って、コントロール プレーン'およびデータプレーンの構成と動作の不整合が検出されます。

レイヤ **2 ToR** サポート

レイヤ 2 ToR のサポートにより、接続分析は次の機能を提供します。

- 接続分析ジョブのトポロジにデバイスを組み込みます。
- 入力インターフェイスや出力パスなど、ノードレベルの詳細なフロー情報を提供します。
- ELAM（Embedded Logic Analyzer Module）を開始し、ToR スイッチでパケットの詳細をキャプチャします。
- ToR スイッチで整合性チェック検証を実行します。サポー

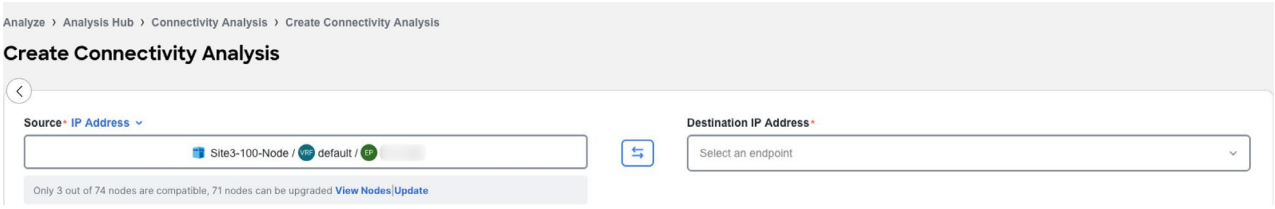
トされるトポロジ

- ポート チャネルがリーフ スイッチに直接接続されている ToR スイッチ。
- vPC ペアのリーフ スイッチに接続されている ToR スイッチ。

- ポート チャネルがリーフ スイッチに個別に接続されている ToR スイッチ。リーフ スイッチは vPC ペアにあります。
- vPC ペアのホストに接続された ToR スイッチとリーフ スイッチを使用した vPC の ToR スイッチ。

注意事項と制約事項

- ファブリックごとに最大 10 個のジョブを送信できます。
- どの時点でも、ファブリックごとに 1 つの接続分析ジョブのみを実行できます。キューのジョブを停止し、別のジョブを実行できます。
- 接続分析は、 Cisco NX-OSリリース9.3(7a) 以降でサポートされています。
- 搭載されているすべてのデバイスが互換性がないと表示されている場合、接続分析ジョブはトリガされません。
- 使用可能な最新の RPM にアップグレードする必要があります。RPM をアップグレードしても、トラフィック転送やスイッチには影響がなく、スイッチのリロードは必要ありません。[ノードの表示（View Nodes）] バナーには、互換性があり最新のノードの数が表示されます。**[更新（Update）]** をクリックしてアップグレードします。アップグレードが完了したら、[ノード（Node）] ページで **[更新（Refresh）]** をクリックしてステータスを表示します。



- 接続分析は、モニタ対象モードの NDFC ファブリックではサポートされていません。
- OAMは、VXLAN ファブリックでのみサポートされます。
- OAM は VTEPS 間でのみサポートされるため、OAM経路はレイヤ 3 ネットワーク間で表示されます。
- オンライン ファブリックでのみ [接続性分析（Connectivity Analysis）] を実行できます。

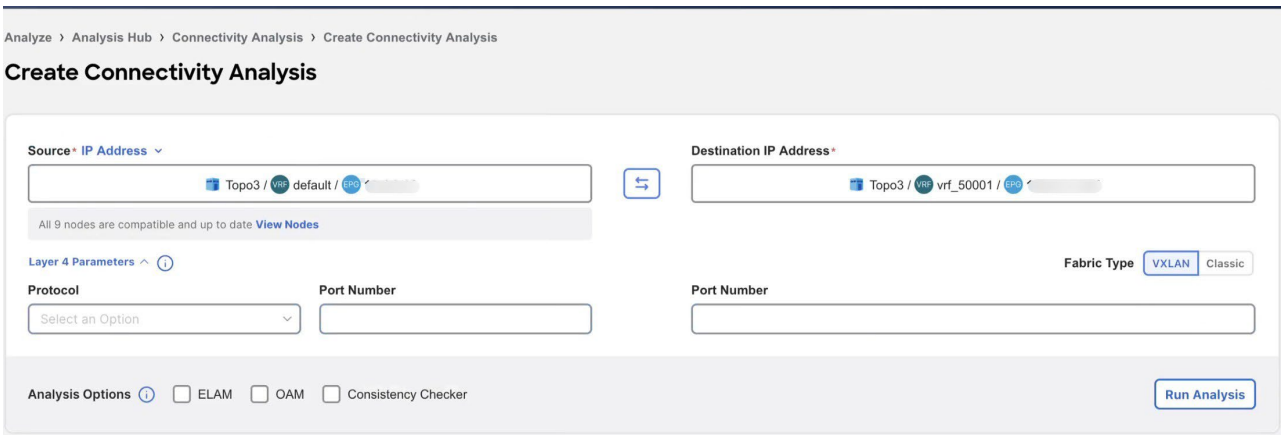
サポートされるトポロジ

- エンドポイントの組み合わせ：
  - EP-EP
  - EP - L3OUT
  - L3Out - EP
  - L3Out - L3Out
- 変換タイプ：
  - L2、L3、L4（TCP/UDP）
  - V4 および V6 のサポート
  - 移動およびプロキシ フロー
  - 共有サービス
- トポロジ：
  - VXLAN

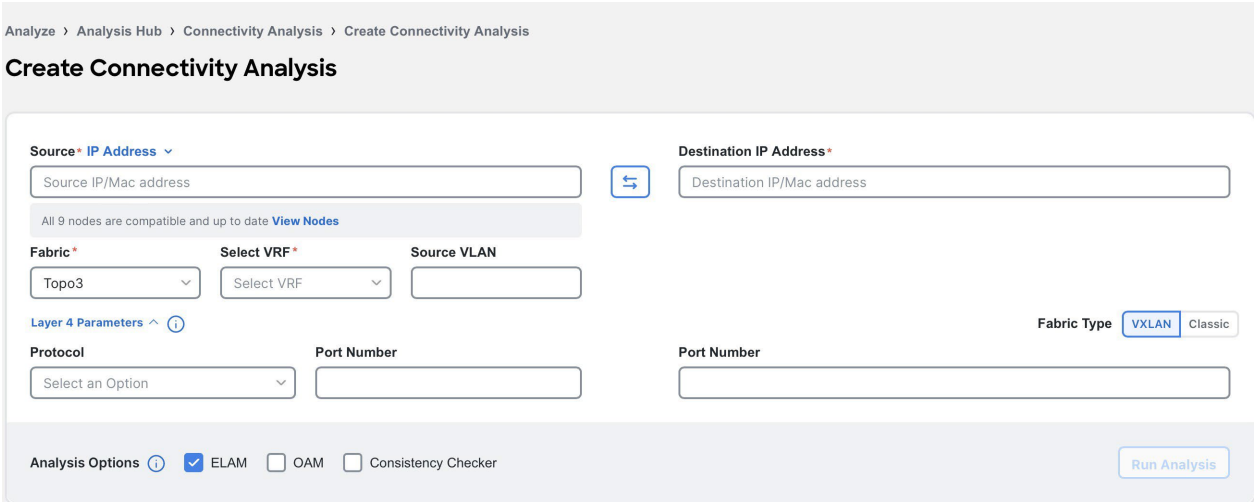
- vPC
- 従来の LAN

接続性分析の作成

1. **[分析（Analyze）]** > **[分析ハブ（Analysis Hub）]** > **[接続性分析（Connectivity Analysis）]** に移動します。
2. **[接続性分析の作成（Create Connectivity Analysis）]** をクリックします。



3. レイヤ 2 およびレイヤ 3 パラメータについては、次のように入力します。
   a. [送信元（Source）]ドロップダウン リストから、2 つのエンドポイント間のフローを分析する **IP** アドレスまたは **MAC** アドレスを選択します。
   b. ドロップダウン リストから送信元 IP または MAC アドレスを選択するか、送信元 IP または MAC アドレスを入力します。一度に最大 20 個の IP アドレスまたは MAC アドレスを表示します。
   c. レイヤ 2 およびレイヤ 3 パラメータを手動で入力することもできます。**[詳細を手動で編集（Edit Details Manually）]** をクリックして、送信元IP または MAC アドレス、接続先 IP または MAC アドレス、ファブリック タイプ、VRF、および送信元 VLAN を入力します。



   d. [ノードの表示（View Nodes）] バナーには、互換性があり最新のノードの数が表示されます。**[ノードの表示（View Nodes）]** をクリックして、ノードのリストと、名前、シリアル番号、デバイス バージョン、現在および最新の CA バージョン、プラットフォーム、ファブリック、互換性、ステータスなどの詳細を表示します。**[更新（Update）]** をクリックして、スイッチの Cisco Nexus Insights Cloud Connector （NICC）RPM をアップグレードします。アップグレードが完了したら、[ノード（Node）] ページで **[更新（Refresh）]** をクリックしてステータスを表示します。

e. [接続先（Destination）] ドロップダウン リストから、2 つのエンドポイント間のフローを分析するIPアドレスまたはMAC アドレスを

選択します。

f. ドロップダウン リストから接続先 IP または MAC アドレスを選択するか、接続先 IP または MAC アドレスを入力します。

4. VXLAN またはクラシック ファブリック タイプを選択します。
5. レイヤ 4 パラメータに対して、以下を入力します。
   a. [プロトコル（Protocol）] ドロップダウン メニューから、[TCP] または [UDP] を選択します。
   b. 送信元ポートと接続先ポート番号を入力します。
6. [分析オプション（Analysis Option）] を選択します。
   a. [ELAM] オプションを有効にして、利用可能なアクティブ フローを分析できます。
   b. このオプションを有効にすると、ホスト間にアクティブトラフィックがない状態でも、アクティブホストの潜在的なドロップを特定したり、VXLAN EVPN ベースのファブリックトポロジ内にあるフローの到達可能性や実際のルートなどの詳細を追跡したりできます。OAMは、VXLAN ファブリックでのみサポートされます。
   c. [整合性チェッカー（Check Consistency Checker）] オプションを有効にすると、指定されたエンドポイントまたはルート間のフローに沿って、コントロール プレーン'およびデータ プレーンの構成と動作の不整合が検出されます。

[接続分析（Connectivity Analysis）] に ELAM オプションと OAM オプションの両方を選択することはできません。

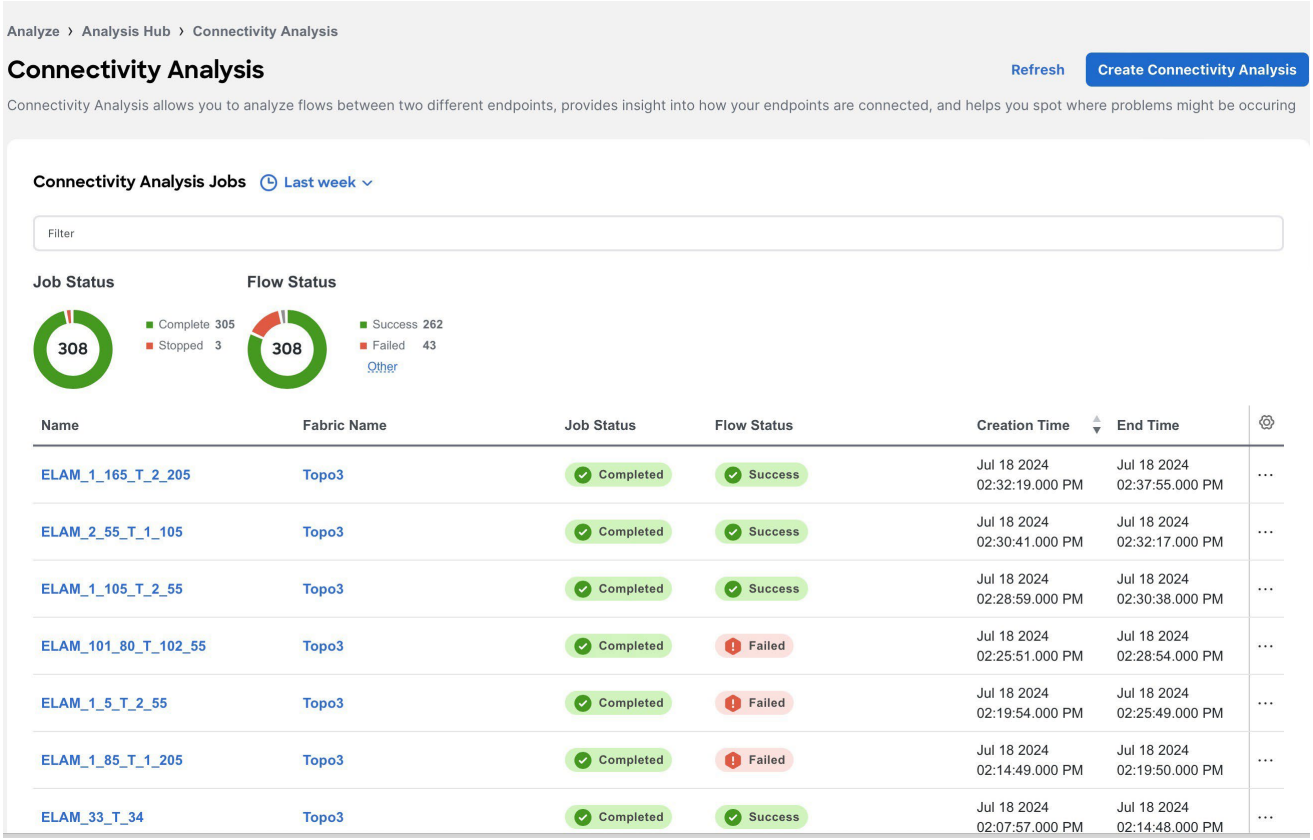
7. [分析の実行（Run Analysis）] をクリックします。
8. [接続分析（Connectivity Analysis）] が完了すると、分析が **[Connectivity Analysis Jobs**（接続分析ジョブ）**]** テーブルに表示されます。**[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**接続性分析（**Connectivity Analysis**）**]** に移動して、[接続分析ジョブ（Connectivity Analysis Jobs）] ジョブを表示します。[分析（Analysis）] は、デフォルト名が割り当てられ、分析の名前を変更できます。
   a. 分析を選択し、[アクション（Actions）] ドロップダウン メニューから **[**分析の名前変更（**Rename Analysis**）**]** をクリックして名前を変更します。

または

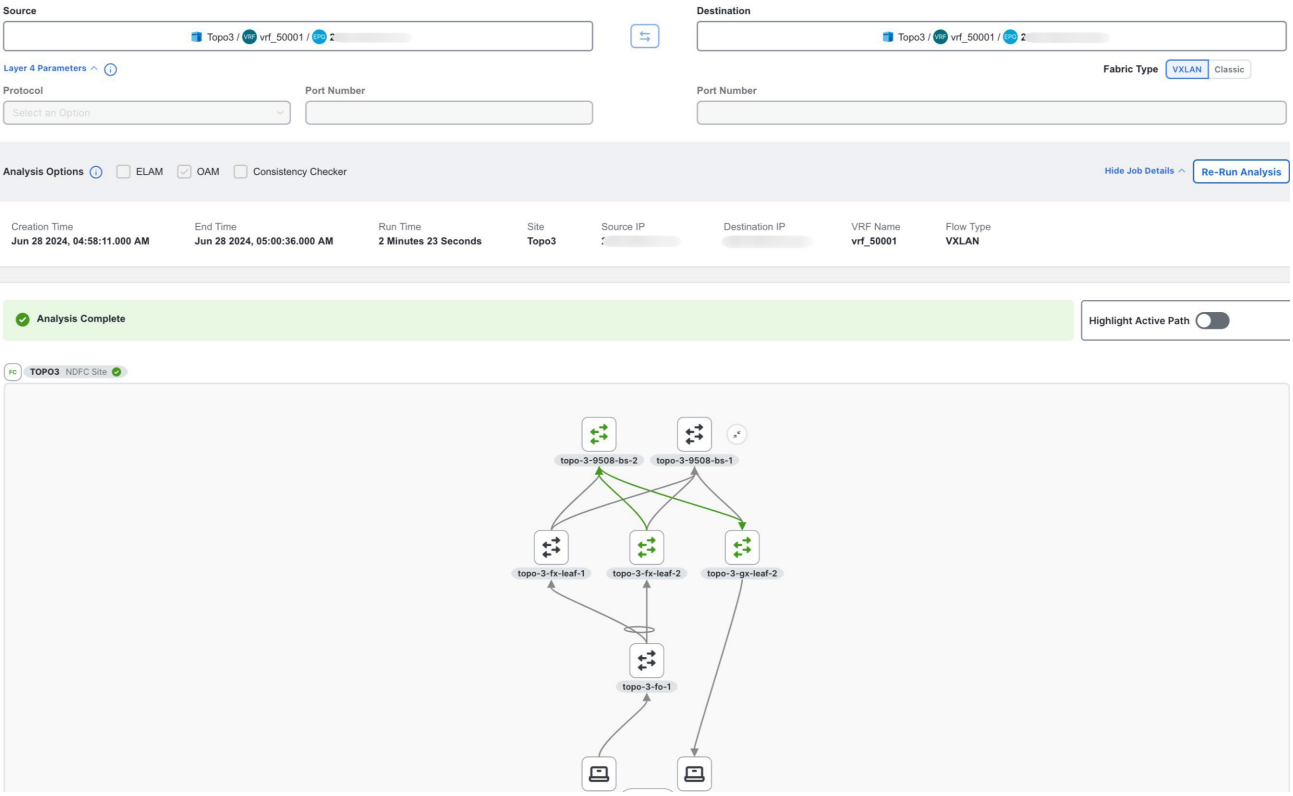
a. 分析名をクリックします。[接続分析の表示（View Connectivity Analysis）] ページで、[アクション（Actions）] ドロップダウン メニューから **[**分析の名前変更（**Rename Analysis**）**]** をクリックして名前を変更します。

接続性分析の表示

1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**接続分析（**Connectivity Analysis**）**]** に移動します。[接続分析（Connectivity Analysis）] ジョブが表示されます。



2. ドロップダウン メニューから時間範囲を選択します。
3. [概要（Summary）] エリアには、[接続分析（Connectivity Analysis）] ジョブの全体的なステータスとフロー ステータスが表示されます。
4. フィルタバーを使用して、分析をフィルタします。[接続分析（Connectivity Analysis）] テーブルには、フィルタされたジョブが表示されます。
   a. 列の見出しをクリックして、テーブルのジョブを並べ替えます。
   b. 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。
   c. 失敗した [フロー ステータス（Flow Status）] の上にカーソルを合わせると、詳細が表示されます。
5. **[名前（Name）]** をクリックして、接続分析の詳細を表示します。[接続分析の表示（View Connectivity Analysis）] ページでは、ジョブに入力した入力パラメータ、ジョブの詳細、トポロジを表示します。

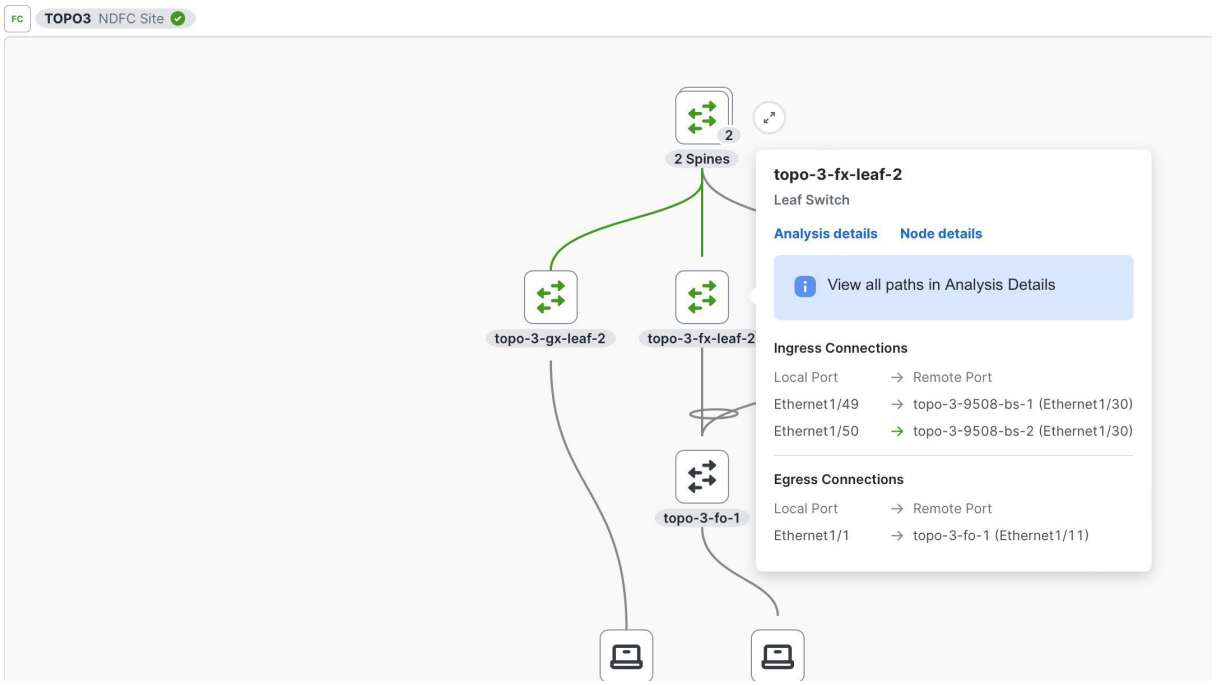


a. [ジョブの詳細の表示（**Show Job Details**）] をクリックして、作成時間、終了時間、実行時間、ファブリック、送信元 IP、接続先 IP、VRF 名、送信元ポート、宛て先ポート、プロトコル、フロー タイプなどのジョブの詳細を表示します。バナーにはジョブのステータスが表示されます。緑色のバナーは分析が成功したことを表し、赤色のバナーは分析に機能不全たことを表します。

b. トグルを活用して、[アクティブ パスの強調表示（**Highlight Active Path**）] を有効または無効化にします。[アクティブ パスの強調表示（**Highlight Active Path**）] を有効にすると、トポロジ内のすべての OAM パスが強調表示されます。

c. [分析の再実行（**Re-run Analysis**）] をクリックして、分析を再度実行します。

d. [トポロジ（topology）] エリアで、ファブリックの階層ビューを視覚化できます。ノードをダブルクリックして、ファブリック内のノードの相互接続を表示できます。ノード間のアクティブ パスは、緑色で強調表示されています。「トポロジ」を参照してください。



e. ノードをクリックしてツールチップを表示します。ツールチップには、ノード名、ノード タイプ、そのノードの入力接続と出力接続、および OAM 情報（該当する場合）が表示されます。入力接続と出力接続では、物理インターフェイスのみが表示され、出力情報は最初の VTEPノードに表示されません。

f. **[**分析の詳細（**Analysis Details**）**]** をクリックして、パスおよびデータ プレーン情報を表示します。

   i. **[**パス（**Paths**）**]** をクリックして、入力と出力の情報、OAM 情報（該当する場合）などのパスの詳細を表示します。入力および出力接続エリアには、論理的なインターフェイスが表示されます。

   ii. **[**データ プレーン（**Data Plane**）**]** をクリックして、分析オプションの結果を表示します。

   iii. **[ELAM]** をクリックし、ELAM レポートを表示します。**[**フル レポートの表示（**View Full Report**）**]** をクリックして、レポートをダウンロードします。

topo-3-fx-leaf-1 の分析結果

パス　データ プレーン

データ プレーンの詳細

ELAM

基本情報

受信インターフェイス	**Ethernet1/1**

外部L2ヘッダー

802.1Q タグは有効な	**yes(0x1)**
Access Encap VLAN	**2301(0x8FD)**
CoS です	**0(0x0)**
接続先 MAC 送信	**0017.0100.0001**
元 MAC	**0011.0100.0001**

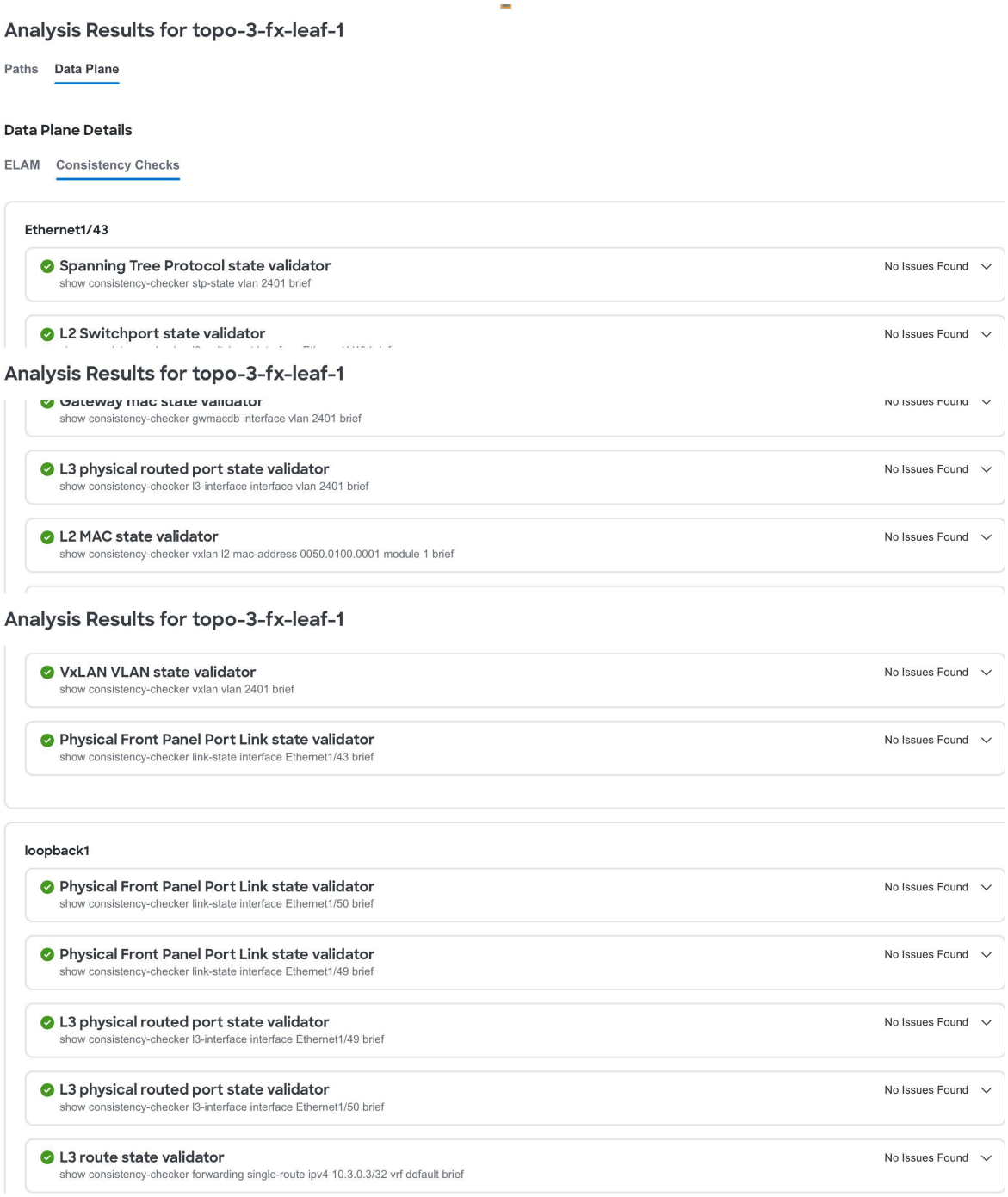
外部L3ヘッダー

DSCP	**0**
接続先 IP をフラグ	**182.31.1.165**
メント化しないビ	**not set**
ット IP チェックサ	**2927(0xB6F)**
ム	**106(= IP ヘッダー + IP ペイロー**
IP パケット長 IP プ	**ド) 未定義**
ロトコル番号 IP バ	**4**
ージョン	**IPv4**
L3 タイプ送	**182.31.1.5**
信元 IP TTL	**64**

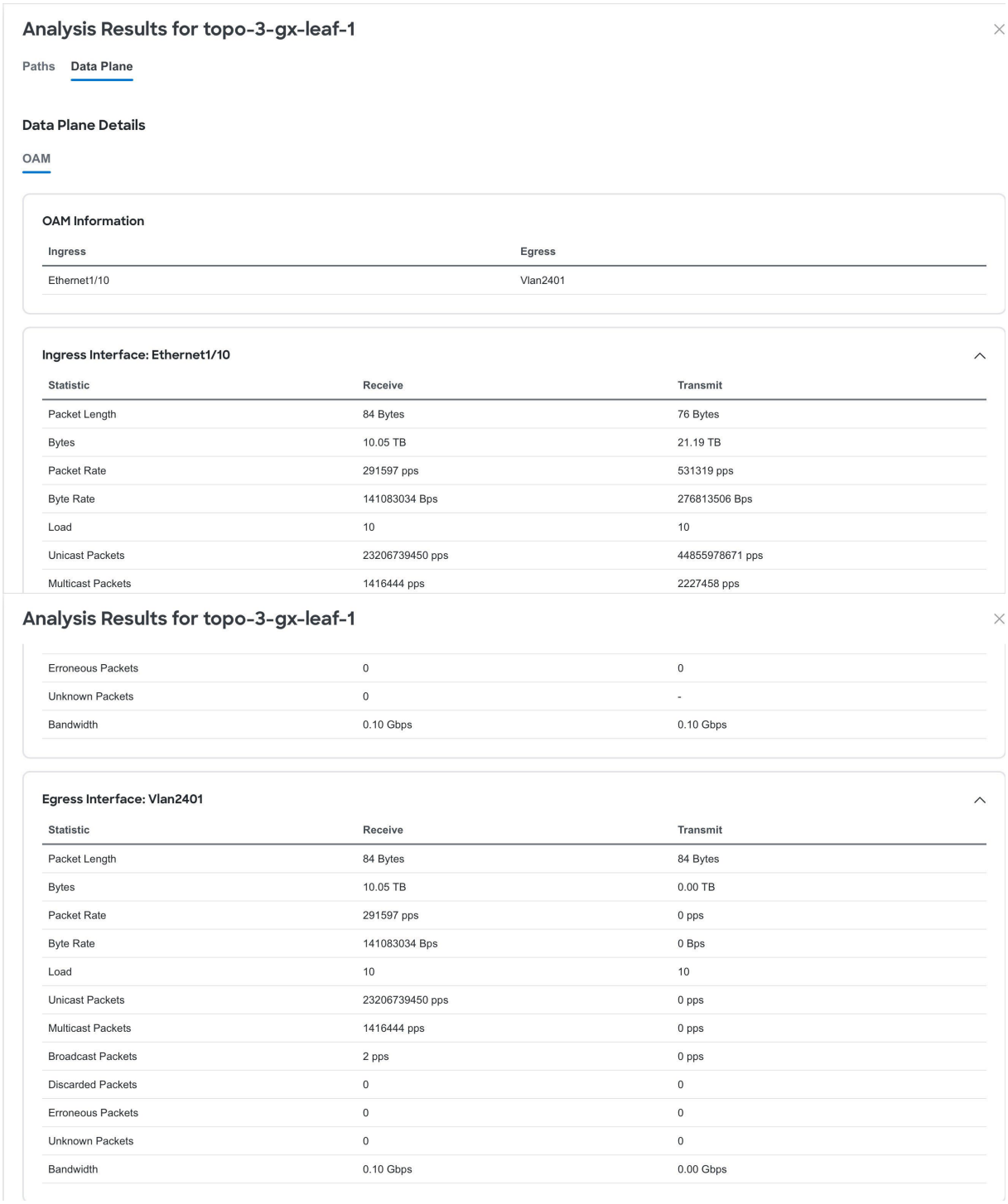
レポート全体の表示

Cisco Confidential

iv. **[整合性チェック（Consistency Checks）]** をクリックして、整合性チェックの結果を表示します。



v. **[OAM]** をクリックして、OAM レポートを表示します。



Analysis Results for topo-3-gx-leaf-1

Paths | Data Plane

Data Plane Details

OAM

OAM Information

Ingress	Egress
Ethernet1/10	Vlan2401

Ingress Interface: Ethernet1/10

Statistic	Receive	Transmit
Packet Length	84 Bytes	76 Bytes
Bytes	10.05 TB	21.19 TB
Packet Rate	291597 pps	531319 pps
Byte Rate	141083034 Bps	276813506 Bps
Load	10	10
Unicast Packets	23206739450 pps	44855978671 pps
Multicast Packets	1416444 pps	2227458 pps

Analysis Results for topo-3-gx-leaf-1

Erroneous Packets	0	0
Unknown Packets	0	-
Bandwidth	0.10 Gbps	0.10 Gbps

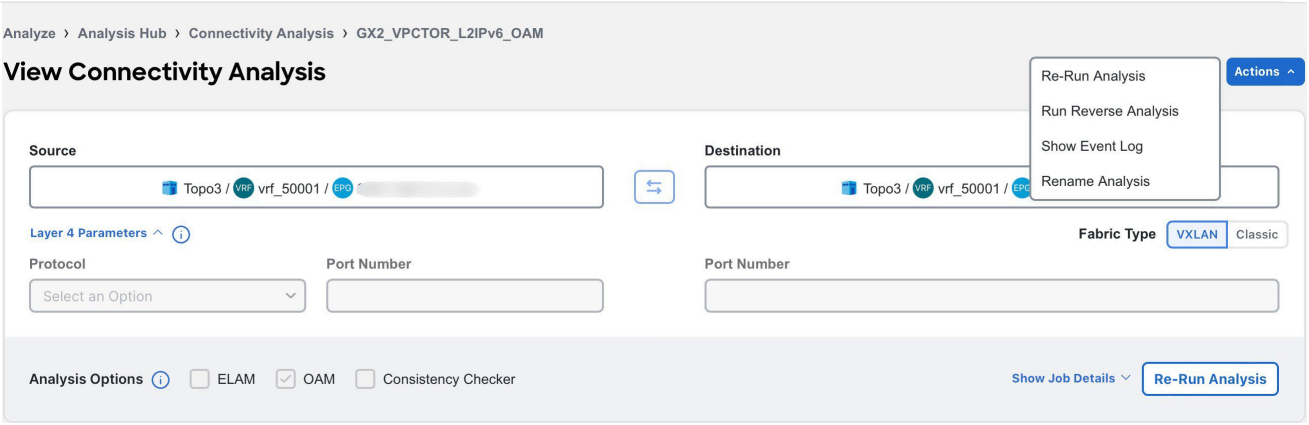
Egress Interface: Vlan2401

Statistic	Receive	Transmit
Packet Length	84 Bytes	84 Bytes
Bytes	10.05 TB	0.00 TB
Packet Rate	291597 pps	0 pps
Byte Rate	141083034 Bps	0 Bps
Load	10	10
Unicast Packets	23206739450 pps	0 pps
Multicast Packets	1416444 pps	0 pps
Broadcast Packets	2 pps	0 pps
Discarded Packets	0	0
Erroneous Packets	0	0
Unknown Packets	0	0
Bandwidth	0.10 Gbps	0.00 Gbps

g. **[**ノードの詳細（**Node Details**）**]** をクリックして、インベントリのノードの詳細を表示します。「インベントリ（Inventory）」を参照してください。

接続分析の管理

1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**接続性分析（**Connectivity Analysis**）**]** に移動します。
2. **[**名前（**Name**）**]** をクリックして、接続分析の詳細を表示します。



3. [アクション（Actions）] ドロップダウン メニューから、[分析の再実行（**Re-Run Analysis**）] を選択し、分析を再度実行します。
4. [アクション（Actions）] ドロップダウン メニューから、[反対分析の実行（**Run Reverse Analysis**）] を選択し、反対方向に分析を実行します。
5. [アクション（Actions）] ドロップダウン メニューから、[イベント ログの表示（**Show Event Log**）] を選択し、分析のログを表示します。イベント ログでは、失敗した分析のエラー メッセージを確認できます。
6. [アクション（Actions）] ドロップダウン メニューから、[分析の名前の変更（**Rename Analysis**）] を選択し、分析の名前を変更します。

フィルタリング情報

一部のケースで、結果をフィルタして、より簡単に情報を見つけることができる可能性があります。

たとえば、単一のリーフスイッチの下に多数のエンドポイントがあるが、特定の VLAN 値を持つエンドポイントにのみ関心がある場合があります。

このような場合、情報をフィルタして特定のエンドポイントのみを表示することもできます。

フィルタの絞り込みには次の演算子を使用します。

演算子	説明
==	最初のフィルタ タイプでこの演算子および後続の値を使用すると、完全一致のデータが返されます。
!=	最初のフィルタ タイプ。この演算子および後続の値を使用すると、同じ値を含まないすべてのデータが返されます。
~ を含む	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含むすべてのデータが返されます。
!contains	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含まないすべてのデータが返されます。
<	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値より小さい一致データが返されます。

演算子	説明
< =	最初のフィルタ タイプ。この演算子および後続の値を使用すると、その値以下の一致データが返されます。
>	最初のフィルタ タイプ。この演算子および後続の値を使用すると、その値より大きい一致データが返されます。
> =	最初のフィルタ タイプ。この演算子および後続の値を使用すると、その値以上の一致データが返されます。

ログ コレクタ

ログ コレクタ

ログコレクタ機能を使用すると、ネットワーク内のデバイスのログを収集してCisco Intersight Cloudにアップロードできます。また、Cisco TAC はファブリック上のデバイスに関するログのオンデマンド収集をトリガし、Cisco Intersight Cloud からログを取得できるようになります。

ログコレクタには次の2つのモードがあります。

- [ユーザー開始（User initiated）]：ユーザーはファブリック上のデバイスのログを収集し、ログ収集ジョブの完了後に収集したログを Cisco Intersight Cloud にアップロードします。ログ収集ジョブの完了後、ログファイルを Cisco Intersight Cloud に自動的にアップロードできます。
- TAC開始 – Cisco TACは、指定されたデバイスのログのオンデマンド収集をトリガーし、Cisco Intersight Cloudからログをプルします。

TAC開始コレクタのデバイス接続通知機能

Nexus Dashboard Insightsは、Cisco Nexus Dashboardのデバイス接続問題通知機能を使用してデバイスと通信します。通知機能は、TACによってトリガーされたオンデマンドのログ収集をチェックします。デバイスと通信するようにファブリックが適切に構成されていない場合、Nexus Dashboard Insights から次の通知が表示されます。

- デバイスはノードの相互作用向けに設定されていません。
- デバイスでログコレクタジョブは実行できません。
- Nexus Dashboard Insightsがデバイスに接続できません。

デバイスのノードの相互作用が正常でない場合、ログ コレクタがログを収集するデバイスを選択できません。GUIでは、デバイスはグレー表示されています。

Cisco Intersight Cloudへのログのアップロード

- Nexus Dashboard Insights が Cisco Intersight Cloud に接続されていることを確認します。
- Nexus Dashboard InsightsがCisco Intersightデバイスコネクタに接続されていることを確認

します。**[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**ログ コレクタ（**Log**

Collector）**]** > **[**ログ コレクタ ジョブの作成（**Create Log Collector Job**）**]** を選択します。

1. 名前を入力します。
2. **[**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。
3. （オプション）ログ収集ジョブの完了後にログ ファイルを Cisco Intersight Cloud に自動的にアップロードするには、[ログファイルの自動アップロード（Auto Upload Log Files）] をオンにします。
4. **[**次へ（**Next**）**]** をクリックします。
5. **[**ノードの追加（**Add Nodes**）**]** をクリックし、**[**ノードの選択（**Select Nodes**）**]** メニューからノードを選択します。
6. [追加（Add）] をクリックします。ノードが **[**ノードの選択（**Select Nodes**）**]** テーブルに表示されます。

7. **[収集の開始（Start Collection）]** をクリックして、ログ収集プロセスを開始します。

   ジョブが完了すると、新しいジョブが**[ログコレクタ]**テーブルに表示されます。

8. テーブルでジョブをクリックして、追加のジョブの詳細を表示します。
9. アイコンをクリックして、**[ログ収集（Log Collection）]** ステータス ページを表示します。10.
   ノードを選択し、 アイコンをクリックします。
11. **[TAC アシストにファイルをアップロード（Upload File to TAC Assist）]** をクリックして、選択したノードの単一のファイルを手動でアップロードします。
12. **[アップロード（Upload）]** をクリックして、選択したノードに対して生成された

    すべてのログ ファイルを手動でアップロードします。アップロードのステータスは、

    [選択されたノード]テーブルに表示されます。

注意事項と制約事項

- ログのアップロードが一部のノードで失敗し、残りのノードで成功した場合、**[選択されたノード]** テーブルのステータスには[完了]と表示されます。
- 一部のノードの収集が失敗しても、他のノードの収集は続行されます。収集が完了すると、アップロードが開始されます。**[選択されたノード（Selected Nodes）]** テーブルでは、統合されたステータスが [ステータス（Status）] 列に表示されます。
- 一部のノードで収集が成功したが、アップロードが失敗した場合、**[選択されたノード]** テーブルのステータスには[失敗]と表示されます。
- **[ログファイルの自動アップロード]**は、一度に1つのノードでのみ実行できます。

ログコレクタダッシュボード

[分析（Analyze）] > **[分析ハブ（Analysis Hub）]** > **[ログ コレクタ（Log Collector）]** に移動します。

[ログ コレクタ（Log Collector）] ダッシュボードには、特定のファブリックのジョブ ステータス別のログのグラフが表示され、最新のログ収集が表示されます。

フィルタ バーを使用すると、ステータス、名前、タイプ、ノード、開始時刻、および終了時刻でログ

をフィルタ処理できます。フィルタの絞り込みには次の演算子を使用します。

演算子	説明
==	最初のフィルタ タイプでこの演算子および後続の値を使用すると、完全一致のデータが返されます。
!=	最初のフィルタ タイプ。この演算子および後続の値を使用すると、同じ値を含まないすべてのデータが返されます。
~ を含む	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含むすべてのデータが返されます。

!contains	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含まないすべてのデータが返されます。

このページには、ログ収集ジョブも表形式で表示されます。ジョブはステータスでソートされています。テーブルのログ収集ジョブを選択し、追加の詳細を表示します。

全般

これは、ジョブのステータスと、ステータス別のデバイス数を示すグラフを表示します。

詳細

次の情報が一覧表示されます。

- 作成時刻
- 終了時間（End Time）
- ノード
- Job ID

選択したノード

これにより、各ジョブのステータスおよびアップロードされたファイルのアップロードステータスとともに、ノードのリストがタブ形式で表示されます。

[すべてのファイルのアップロード（**Upload All Files**）] では、すべてのファイルをアップロードできます。

... 各ファイルを個別にダウンロードすることもできます。

TAC開始のログコレクタ

TAC 開始のログコレクタにより、Cisco TAC は、Cisco Intersight Cloud 内の指定されたユーザーデバイスのログのオンデマンド収集をデバイスコネクタにトリガーできます。

TAC アシスト ジョブが完了すると、新しいジョブが [ログ コレクタ（**Log Collector**）] テーブルに表示されます。テーブルのログ収集ジョブを選択し、追加の詳細を表示します。[ログ収集ステータス（**Log Collection**）] には、ステータス、一般的な情報、ノードの詳細などの情報が表示されます。

ブラウザ印刷オプションがある PDF として TAC アシスト ジョブの詳細を保存できます（Chrome および Firefox でのみサポート）。

トラフィック分析

トラフィック分析

トラフィック分析では、ネットワークの遅延、輻輳、ドロップをモニタできます。

トラフィック分析は、既知のレイヤ 4 ポートを対応するサービス エンドポイント カテゴリと照合することで、ファブリック ネットワークで実行されているサービスを自動的に検出します。Nexus Dashboard Insights は、次のメトリックに対してしきい値に基づいてサービス パフォーマンスを評価できます。

- [遅延（Latency）]：パケットがある場所から別の場所に移動するのにかかる全体の時間（ミリ秒）を測定します。
- 輻輳：ネットワーク帯域幅の使用率とQuality of Service (QoS)のアクティブ化メカニズムを測定して、サービスでネットワークの輻輳が発生しているかどうかを判断します。
- [ドロップ（Drops）]：CRC エラー、ケーブルの障害、その他のデバイスなどの要因を考慮して、ドロップされたパケットと送信されたパケットのスコアまたは数を測定します。

遅延、輻輳、ドロップなどのパフォーマンスメトリックに偏差がある場合、異常が発生します。パフォーマンス スコアは、各カンバセーションごとに計算され、サービス エンドポイントまたはエンドポイントレベルに集計され、異常を提起します。

パフォーマンス スコアは、以下に基づいて計算されます。

- 輻輳：エンドポイント間でアクティブな一貫した輻輳回避が計算されます。
- [レイテンシ（Latency）]：前のカンバセーションの平均遅延からの偏差が計算されます。
- ドロップ：カンバセーションまたはサービスの問題に直接対応します。[ト

ラフィック分析（Traffic Analytics）] を使用すると、以下のことが可能になり

ます。

- トラフィックを広範囲にモニターできます。
- パフォーマンス メトリックに発生した異常を使用してパフォーマンスの問題を報告します。
- 上位通話サービスとクライアントをソートし、システム内の上位トーカーを特定します。
- サービスごとの SYN または RST カウントを決定します。
- オンデマンドでカンバセーションまたはフローをトラブルシューティングします。

トラフィック分析カンバセーション

TCP カンバセーションは、送信元 IP アドレス、接続先 IP アドレス、接続先ポート、およびプロトコルを含む 4 タプルです。非 TCP カンバセーションは、送信元 IP アドレス、接続先 IP アドレス、およびプロトコルを含む 3 タプルです。単一のクライアントが、サービス エンドポイントに向けて複数の送信元ポートによって開始された複数の通信フローを確立する場合、関連するすべての統計情報がトラフィック分析テーブルの単一のエントリとして集約されます。サービスエンド ポイントは、IP アドレス、ポート、およびプロトコルによって定義されます。

カンバセーションのレート制限を超えると、異常が発生します。**[**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。[過去 1 時間のトラフィック分析ステータス（Traffic Analytics status）] 領域で、カンバセーション レートが制限に近づいているか、または超過しているかを確認できます。また、トラフィック分析レコードのドロップがあるかどうかを確

認することもできます。

Cisco Confidential

トラフィック分析のスケール制限

表には、トラフィック分析スケール制限を示します。

トラフィック分析のスケール制限

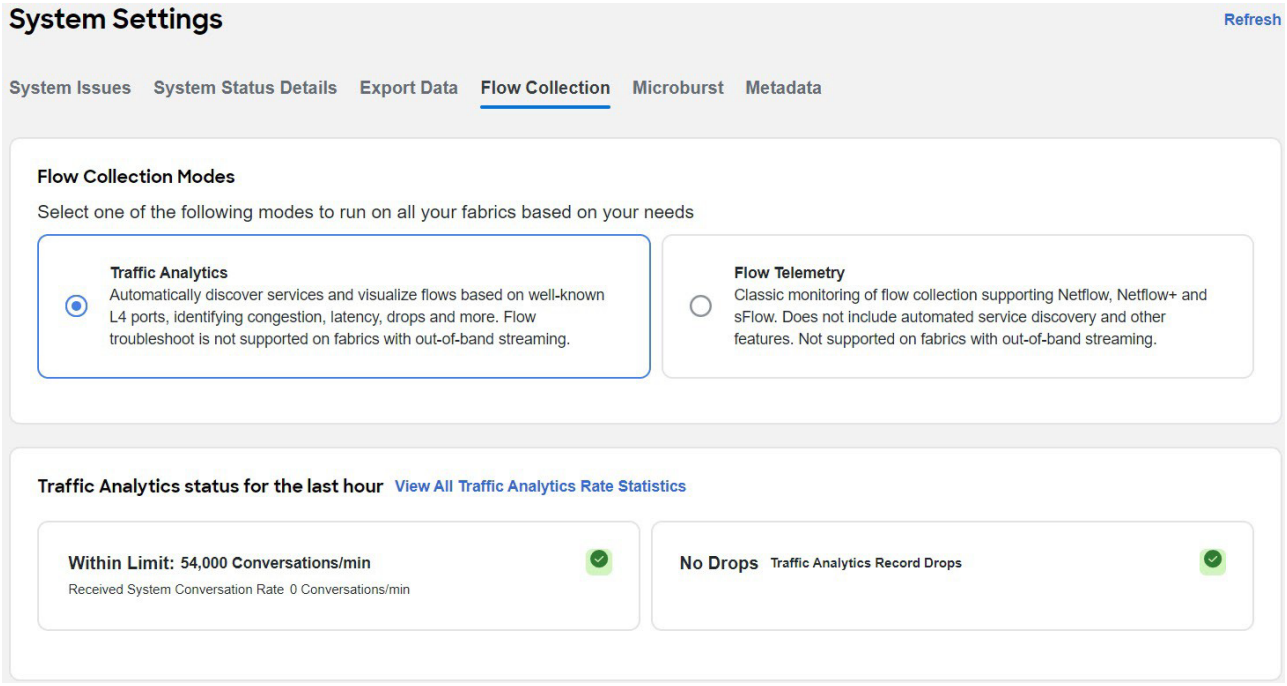
Nexus Dashboardクラスタ	**1** 分あたり固有のカンバセーション	同時進行のトラブルシューティング ジョブ
6 物理	100,000	8
3 物理	50,000	5
1 物理	5,000	1
6 仮想	10,000	5
3 仮想	5,000	1

トラフィック分析の注意事項および制限事項

- トラフィック分析は、Cisco NX-OS リリース 10.4(2)F 以降でサポートされています。
- トラフィック分析は、レイヤ 4 ~ レイヤ 7 サービスではサポートされていません。
- トラフィック分析はマルチサイトではサポートされていません。
- NetFlow 構成の Cisco NDFC ファブリックでトラフィック分析を有効にする前に、リーフ スイッチにフリーフォーム ポリシーを追加する必要があります。これにより、トラフィック分析が Nexus Dashboard Insights から無効になっている場合、Netflow 構成は削除されません。
- トラフィック分析ではマルチキャストはサポートされていません。
- トラフィック分析は、ファブリック内に含まれる IPv4 または IPv6 エンドポイント間のトラフィック フローでのみ使用できます。これらのエンドポイントは、**[**管理（**Manage**）**]** > **[**ファブリック（**Fabrics**）**]** > **[**接続（**Connectivity**）**]** > **[**エンドポイント（**Endpoints**）**]** ページに表示されます。送信元または接続先エンドポイントがファブリックの外部に存在する場合、トラフィック分析移行はトラフィック分析テーブルに表示されません。
- トラフィック分析の設定またはエクスポートは、Cisco Nexus 9500 モジュラ型シャーシではサポートされていませんが、フローのトラブルシューティング ジョブは、FX プラットフォーム スイッチおよび Cisco Nexus 9500 モジュラ型シャーシでサポートされています。
- **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**トラフィック分析（**Traffic Analytics**）**]** に移動して、TCP サービスおよびクライアント/カンバセーションに関する情報を表示します。**[**エンドポイント トラフィック分析（**Endpoint Traffic Analytics**）**]** タブに移動して、非 TCP サービスおよびクライアント/カンバセーションに関する情報を表示します。
- VRF インスタンスが新しい L3VNI モードで設定されている場合、トラフィック分析に部分的なデータが表示されることがあります。新しい L3VNI モードの詳細については、『Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド』 を参照してください。
- 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』および「Precision Time Protocol (PTP) for Cisco Nexus Dashboard Insights」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。
- トラフィック分析は、スタンドアロン NX-OS および NDFC ファブリックの VxLAN ファブリックでのみサポートされます。クラシック LAN ファブリックはサポートされていません。

トラフィック分析の構成

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、**[トラフィック分析（Traffic Analytics）]** 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ます。
4. 省略記号アイコンをクリックし、**[有効化（Enable）]** をクリックしてトラフィック分析を有効にします。

> フロー テレメトリがファブリック上ですでに有効な場合、
> すべてのファブリックのフロー テレメトリを最初に無効にして、[トラフィック分析 (Traffic Analytics)]を有効にする前にすべてのフロー ルールを削除する必要があります。

5. **[スイッチ構成ステータス（Switch Configuration Status）]** 列で、各ノードのフロー収集ステータスを表示
確認します。
   - グリーン：フロー収集が正常に有効になっています。
   - レッド：フロー収集が有効になっていません。
   - オレンジ：フロー収集が部分的に有効です。
   - グレー：フロー収集がサポートされていないか、データが見つかりません。スイッチが無効状態の場合、[グレー（Gray）] カテゴリに含まれます。
6. [過去 1 時間のトラフィック分析ステータス（Traffic Analytics Status For The Last Hour）] 領域で、制限を超えたカンバセーションの数とトラフィック分析ドロップの数を確認できます。最大カンバセーション レート制限を超えないようにする必要があります。最大カンバセーション レート制限を超えると、フロー レコードでドロップが表示され、可視性に影響します。
7. ファブリック内の各スイッチの統計を表示するには、**[すべてのトラフィック分析レート統計の表示（View All Traffic Analytics Rate Statistics）]** をクリックします。

トラフィック分析構成の適用

モニタ対象モードの NDFC ファブリックの場合、Nexus Dashboard Insights はファブリック内のすべてのスイッチにトラフィック分析構成を展開しません。すべてのスイッチにトラフィック分析構成を適用する

必要があります。

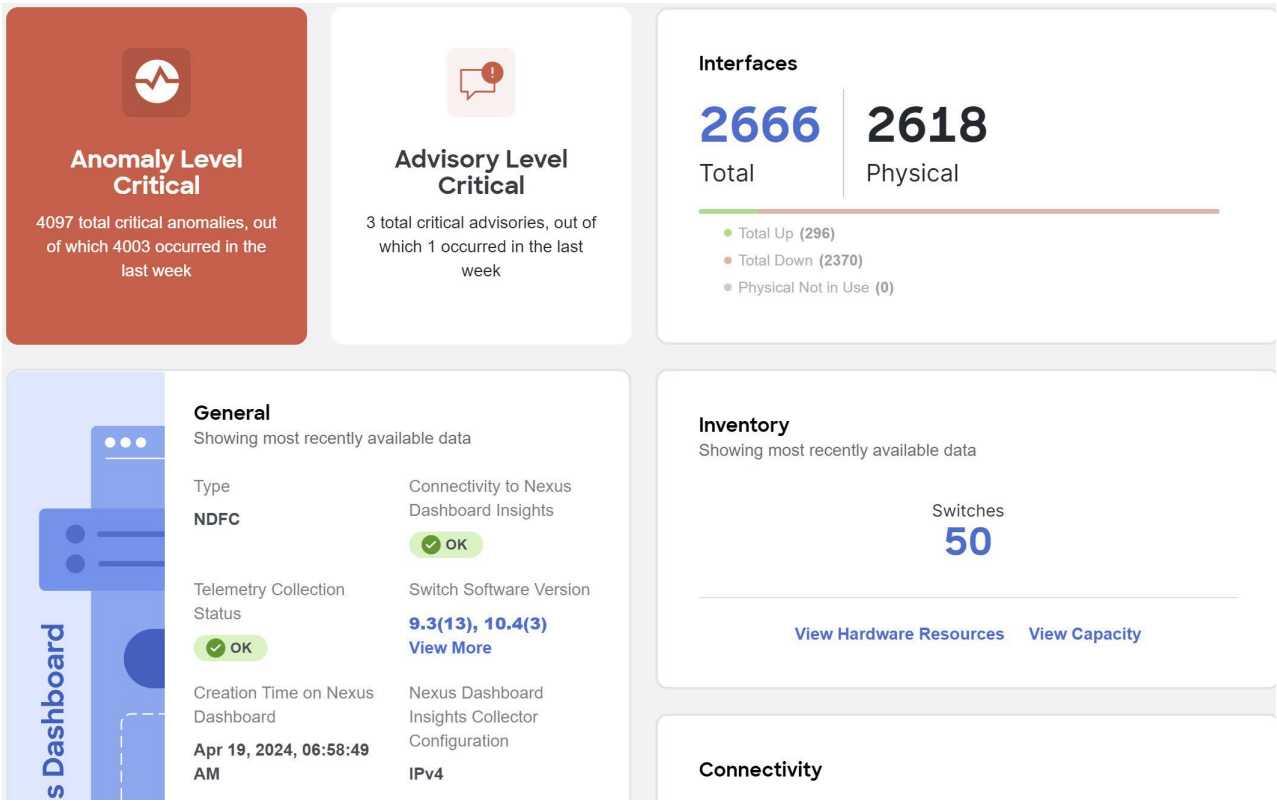
1. **[管理者（Admin）] > [システム設定（System Settings）] > [システムステータスの詳細（System Status Details）]** に移動します。
2. ファブリックを選択します。
3. 省略記号アイコンをクリックし、**[予想される構成（Expected Configuration）]** をクリックします。
4. **[予想される構成（Expected Configuration）]** 領域から **[ソフトウェア テレメトリ（Software Telemetry）]** および **[フロー テレメトリ（Flow Telemetry）]** 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)# copy running-config startup-config
```

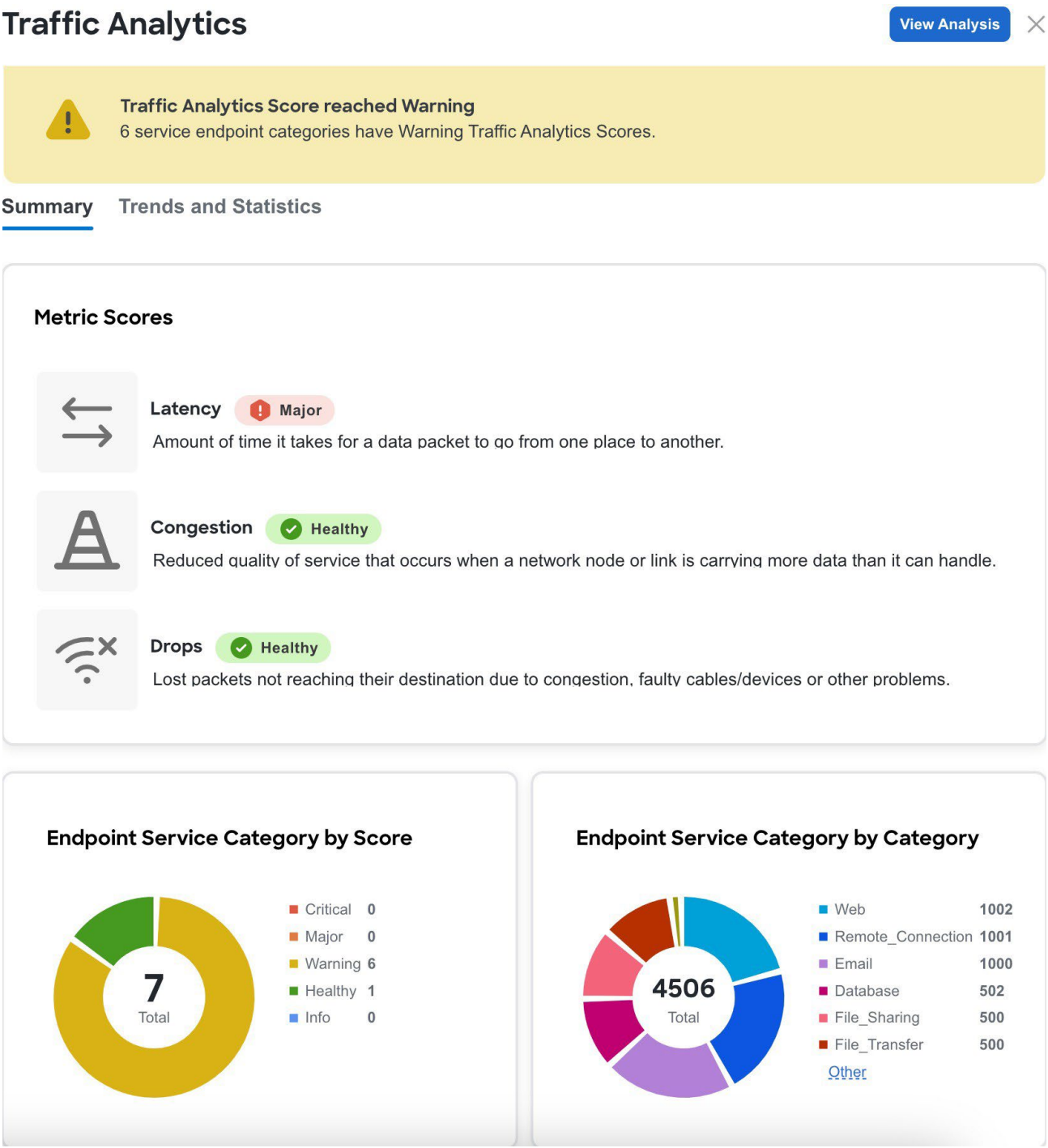
トラフィック分析の表示

個々のファブリックのトラフィック分析の表示

1. **[管理（Manage）] > [ファブリック（Fabrics）]** に移動します。
2. ファブリック名をクリックします。



3. ドロップダウン メニューから時間範囲を選択します。デフォルトでは、[現在の時刻（過去 2 時間）（Current time (last 2 hours)）] が選択されています。
4. [全般（General）] 領域で、**[トラフィック分析（Traffic Analytics）]** をクリックして、そのファブリックのトラフィック分析の詳細を表示します。[トラフィック分析（Traffic Analytics）] ページでは、すべての情報がそのファブリックのサービス カテゴリとしてグループ化されます。



5. [概要（Summary）] 領域には、トラフィック分析スコアと、メトリックの決定方法が表示されます。エンドポイント サービス カテゴリのトラフィック プロファイルをスコアおよびカテゴリ別に表示できます。
6. **[傾向と統計（Trends and Statistics）]** をクリックして、トラフィック プロファイル、上位エンドポイント サービス スコアの変更、および上位エンドポイント カテゴリを表示します。

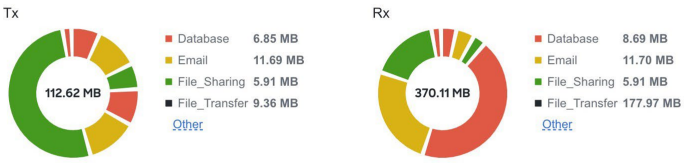
Traffic Analytics

View Analysis

Traffic Analytics Score reached Warning
6 service endpoint categories have Warning Traffic Analytics Scores.

Summary | Trends and Statistics

Traffic Profile



Top Endpoint Service Score Changes

Categories	Score Change	Affecting Metric
Database	Warning → Healthy	Latency ↘
File_Transfer	Warning → Healthy	Latency ↘
Remote_Connection	Warning → Healthy	Latency ↘
Email	Warning → Warning	Latency →
File_Sharing	Warning → Warning	Latency →
RoCE	Unknown → Healthy	-
Web	Warning → Warning	Latency →

7 items found Rows per page 10 1

Top Endpoint Categories by Rx Latency

Categories	Average	Trend
File_Transfer	2.01 us	↗ 3%
Remote_Connection	2 us	↗ 1%
Database	2 us	↘ 0%
Email	2 us	↘ 0%
File_Sharing	2 us	→
RoCE	0 us	→
Web	2 us	↘ 0%

Cisco Confidential

a. [トラフィック プロファイル（Traffic Profile）] 領域で、エンドポイント サービス カテゴリのトラフィック量を表示できます。

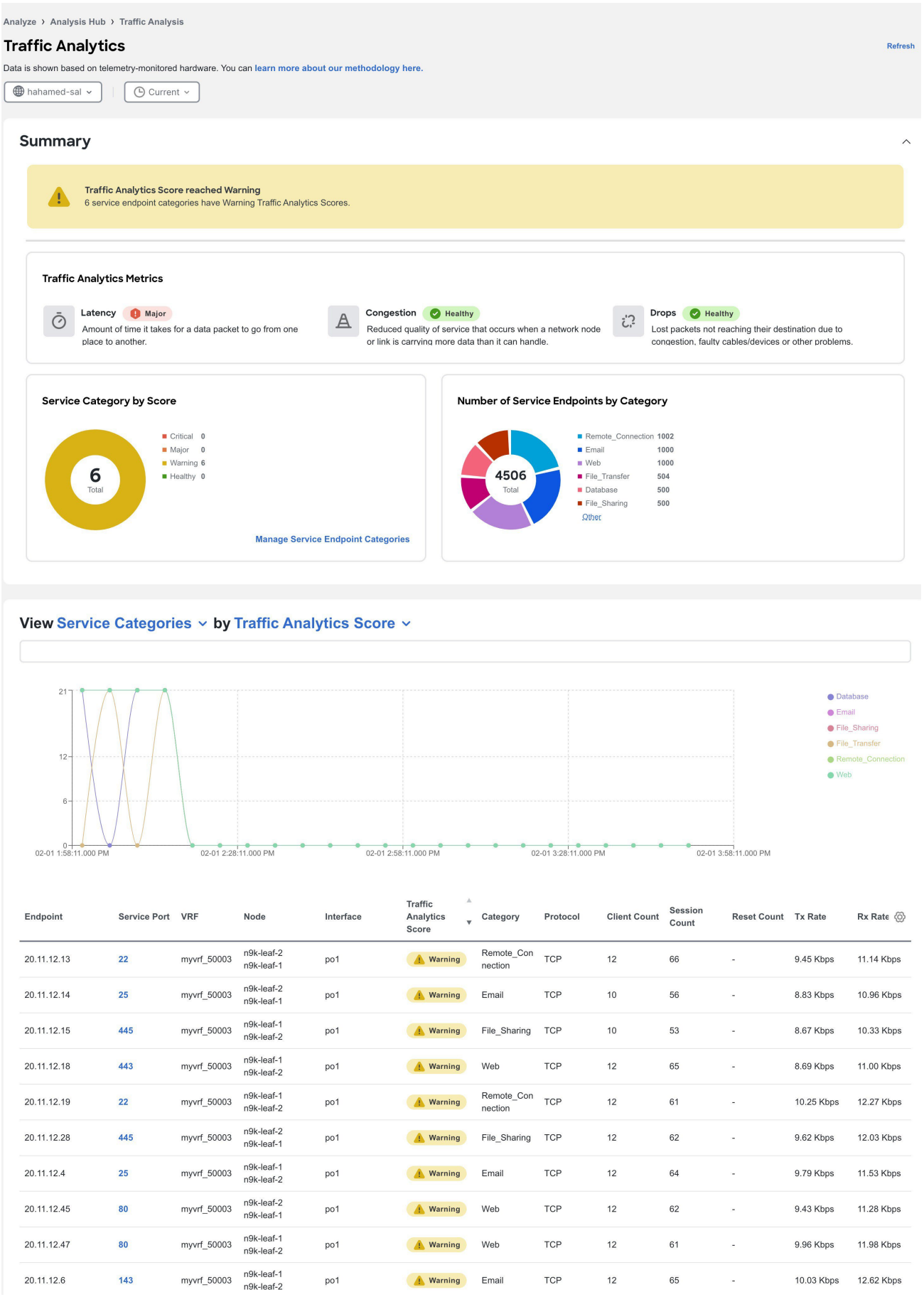
b. [上位エンドポイント サービス スコアの変化（Top Endpoint Service Score Changes）] 領域では、2 時間にわたる異常スコアの変化と、スコアの変化に影響するメトリック（遅延、輻輳、ドロップなど）を表示できます。

c. [上位エンドポイント カテゴリ（Top Endpoint Categories by）] 領域では、Rx および Tx 遅延、輻輳スコア、およびドロップ スコア別に上位カテゴリを確認できます。

7. **[**分析の表示（**View Analysis**）**]** をクリックして、すべてのファブリックのトラフィック分析を表示します。

すべてのファブリックのトラフィック分析の表示

1. **[**分析（**Analyze**）**]** > **[**ハブの 分析（**Analyze Hub** ）**]** > **[**トラフィック分析（**Traffic Analytics**）**]** の順に選択します。
2. ドロップダウン メニューからファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。デフォルトでは、[現在の時刻（過去 2 時間）（Current time (last 2 hours)）] が選択されています。[現在の時刻（Current time）] を選択すると、過去 2 時間にトラフィック分析スコアで確認された問題が表示されます。

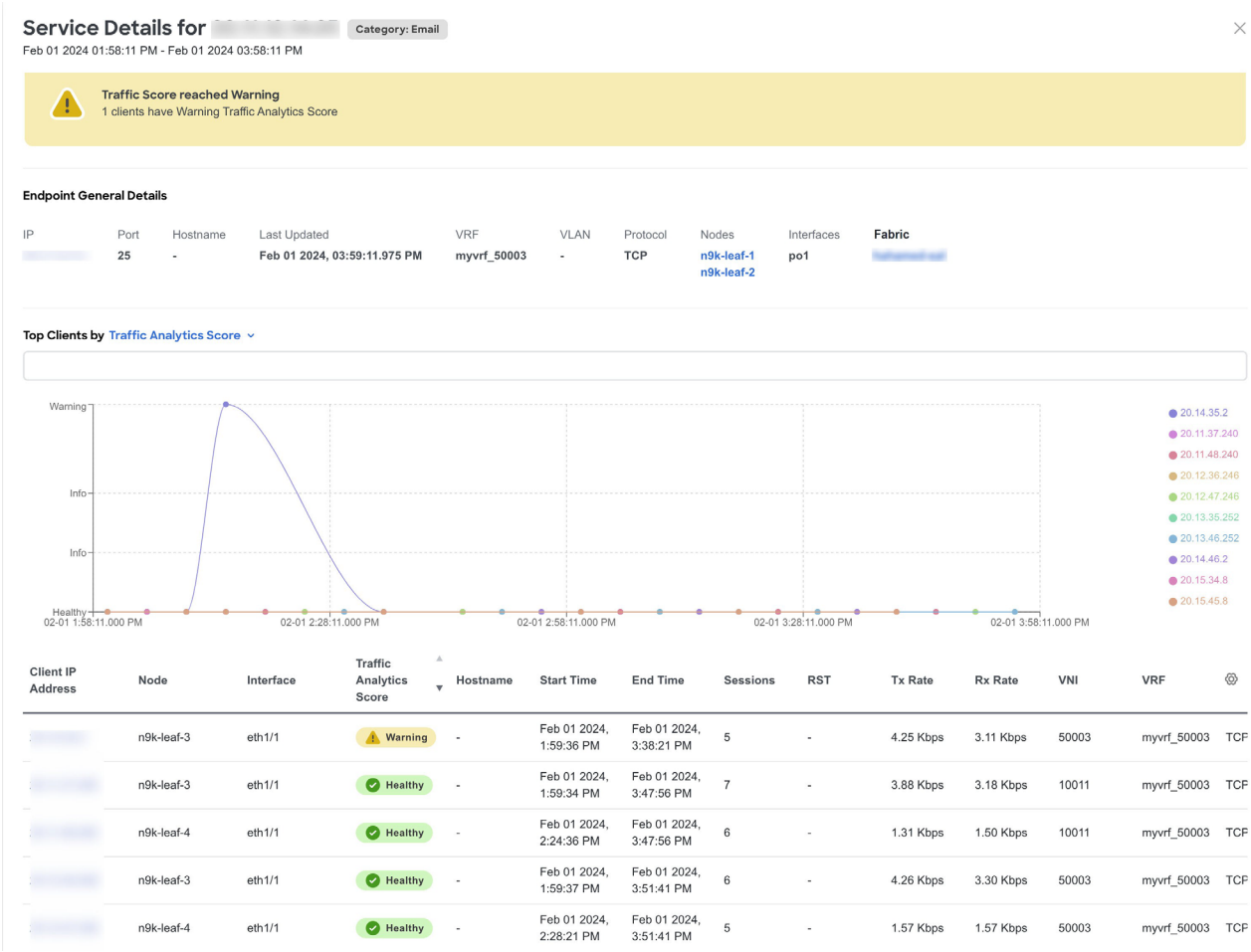


Endpoint	Service Port	VRF	Node	Interface	Traffic Analytics Score	Category	Protocol	Client Count	Session Count	Reset Count	Tx Rate	Rx Rate
20.11.12.13	22	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Remote_Connection	TCP	12	66	-	9.45 Kbps	11.14 Kbps
20.11.12.14	25	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Email	TCP	10	56	-	8.83 Kbps	10.96 Kbps
20.11.12.15	445	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	File_Sharing	TCP	10	53	-	8.67 Kbps	10.33 Kbps
20.11.12.18	443	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	65	-	8.69 Kbps	11.00 Kbps
20.11.12.19	22	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Remote_Connection	TCP	12	61	-	10.25 Kbps	12.27 Kbps
20.11.12.28	445	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	File_Sharing	TCP	12	62	-	9.62 Kbps	12.03 Kbps
20.11.12.4	25	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	64	-	9.79 Kbps	11.53 Kbps
20.11.12.45	80	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Web	TCP	12	62	-	9.43 Kbps	11.28 Kbps
20.11.12.47	80	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	61	-	9.96 Kbps	11.98 Kbps
20.11.12.6	143	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	65	-	10.03 Kbps	12.62 Kbps

4. [概要（Summary）] 領域には、トラフィック分析スコアとメトリックの決定方法が表示されます。次に、スコアとカテゴリ別にサービス エンドポイント カテゴリの情報を表示できます。[サービス エンドポイント カテゴリの管理] 領域では、標準のネットワークのデフォルトと作成したカテゴリに基づいてカテゴリに割り当てられたポートから構成されます。これらのカテゴリは動的であり、

いつでも更新できます。「サービス エンドポイント カテゴリの管理」を参照してください。

5. 次に、ドロップダウンリストを使用して、トラフィックスコア、輻輳スコア、遅延スコア、ドロップスコアなどの属性のサービス カテゴリまたはサービス エンドポイント情報をグラフ形式で表示します。[サービス エンドポイント（Service Endpoints）] を選択すると、トラフィック分析スコア、遅延スコア、輻輳スコア、ドロップ スコア、セッション数、リセット数、TX レート、Rx レートなどのさまざまな属性の上位 10 のエンドポイントも表示できます。[現在の時刻（Current Time）] で、**[トラフィック分析スコア（Traffic Analytics Score）]** の **[サービス カテゴリの表示（view Service Categories）]** を選択すると、グラフを使用して正常なスコアと異常なスコアの間の遷移を表示できます。
6. [トラフィック分析（Traffic Analytics）] テーブルでは、サービス カテゴリまたはサービス エンドポイントの情報を表示できます。サービス カテゴリまたはエンドポイントのトラフィックスコア情報は、輻輳スコア、遅延スコア、およびドロップスコアの組み合わせです。スコアが計算されると、輻輳スコアの重みが最小になり、ドロップスコアの重みが最大になります。
   a. [トラフィック分析スコア（Traffic Analytics Score）] 列にカーソルを合わせると、サービスのトラフィック分析スコアの内訳を表示できます。
   b. 検索バーを使用して、サービスカテゴリまたはサービスエンドポイントの値でフィルタリングします。
   c. 歯車アイコンをクリックして、[トラフィック分析（Traffic Analytics）] テーブルの列を設定します。
7. **[サービス ポート（Service Port）]** をクリックして、特定のサービスの詳細を表示します。



   a. [概要（Overview）] 領域では、エンドポイントの詳細と、上位クライアントやクライアントとサービス間の会話などのクライアントの詳細を表示できます。
      i. [エンドポイントの一般的な詳細（Endpoint General Details）] で、[クライアント IP アドレス（Client IP Address）] をクリックしてエンドポイントの詳細を表示します。そのエンドポイ

ントでホストされているすべてのサービスと、このエンドポイントから他のサービスへの接続と IP アドレスを表示できます。

ii. ドロップダウン リストを使用して、トラフィック分析スコア別の上位クライアント、遅延スコア、ドロップ スコアなどの情報を表示します。

iii. [クライアント（Clients）] テーブルで、[トラフィック分析スコア（Traffic Analytics Score）] にカーソルを合わせると、そのサービスのトラフィック分析スコアの内訳が表示されます。

b. [トレンドと統計（Trends and Statistics）]領域には、そのサービスのクライアント、サービス、遅延などの値のトレンドが表示されます。

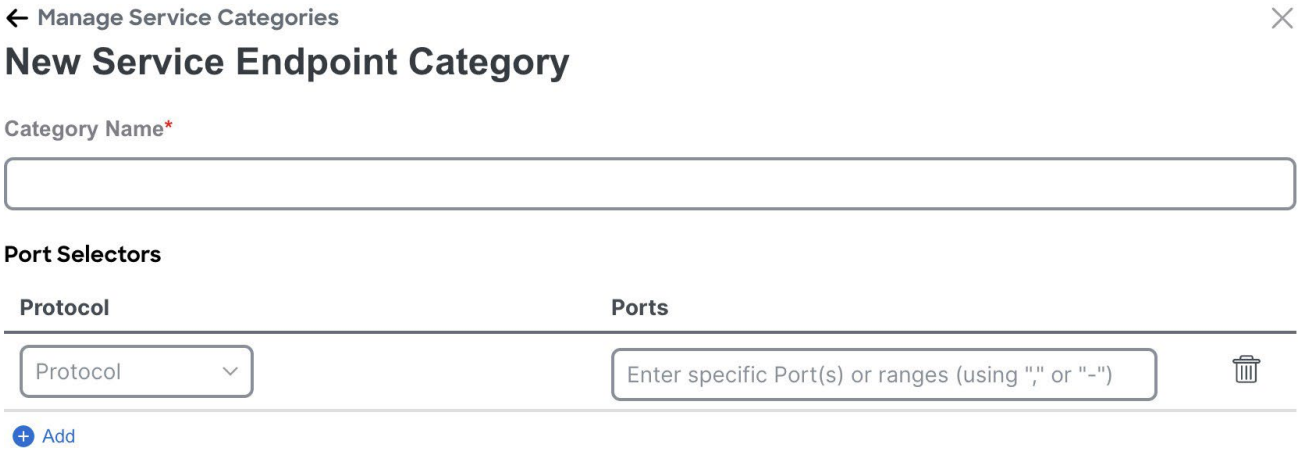
c. [異常（Anomalies）] 領域では、トラフィック スコアに基づいて特定のサービス エンドポイントの異常を表示できます。

d. [フロー収集（Flow Collections）] 領域で、そのサービスのフロー収集を表示できます。

サービス エンドポイント カテゴリの管理

[サービス エンドポイント カテゴリの管理] 領域では、標準のネットワークのデフォルトと作成したカテゴリに基づいてカテゴリに割り当てられたポートを表示できます。ポートがカテゴリに割り当てられていない場合は、既存のカテゴリのいずれかに割り当てるか、新しいカテゴリを作成できます。これにより、ネットワークポートをより効率的に整理および管理できます。

1. **[分析（Analyze）]** > **[ハブの 分析（Analyze Hub ）]** > **[トラフィック分析（Traffic Analytics）]** の順に選択します。
2. ドロップダウン メニューからファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。デフォルトでは、[現在の時刻（過去 2 時間）（Current time (past 2 hours)）] が選択されています。
4. [スコア別サービス カテゴリ（Service Category by Score）] 領域で、**[サービス エンドポイント カテゴリの管理（Manage Service Endpoint Categories）]** をクリックします。
5. 新しいカテゴリを作成するには、**[新しいカテゴリ（New Categories）]** をクリックします。

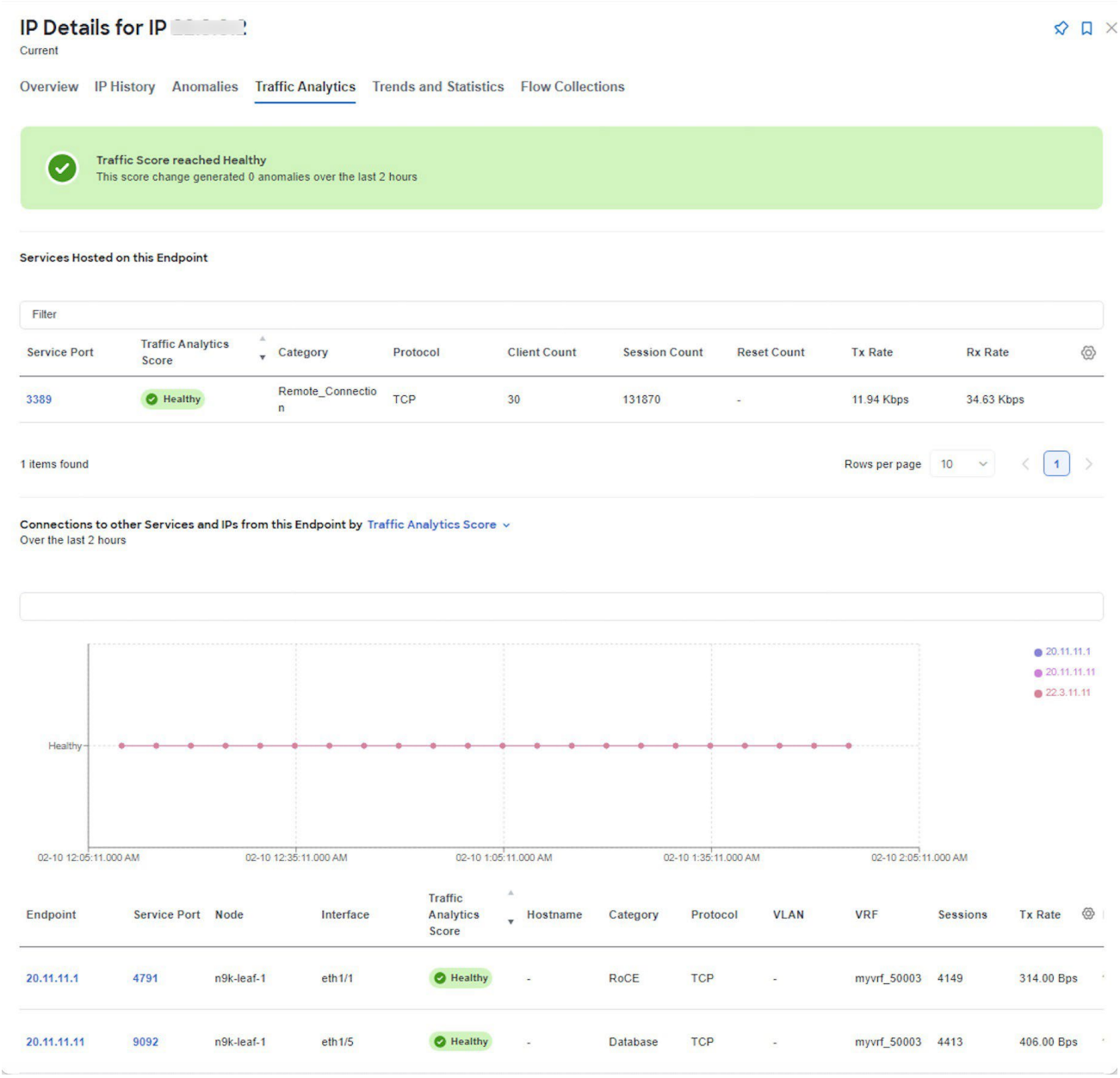


6. カテゴリの名前を入力します。
7. [プロトコル（Protocol）] ドロップダウン リストから、プロトコルを選択します。
8. [ポート（Ports）] フィールドで、ポートまたはポート範囲を入力します。
9. **[追加（Add）]** をクリックして、プロトコルを追加します。
10. **[保存（Save）]** をクリックします。

11. カテゴリを編集するには、省略記号アイコンをクリックし、[編集（edit）] を選択します。
    a. 値を編集し、**[保存（Save）]** をクリックします。
12. カテゴリを削除するには、省略記号アイコンをクリックし、[削除（delete）] を選択します。
    a. **[確認（Confirm）]** をクリックします。

エンドポイントのトラフィック分析の表示

1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. ファブリック名をクリックします。
3. **[接続（Connectivity）]** > **[エンドポイント（Endpoints）]** に移動します。
4. エンドポイント テーブルで、IP アドレスをクリックします。
5. [IP の詳細（IP Details）] ページで、**[トラフィック分析（Traffic Analytics ）]** をクリックして、エンドポイントのトラフィック分析ビューを表示します。



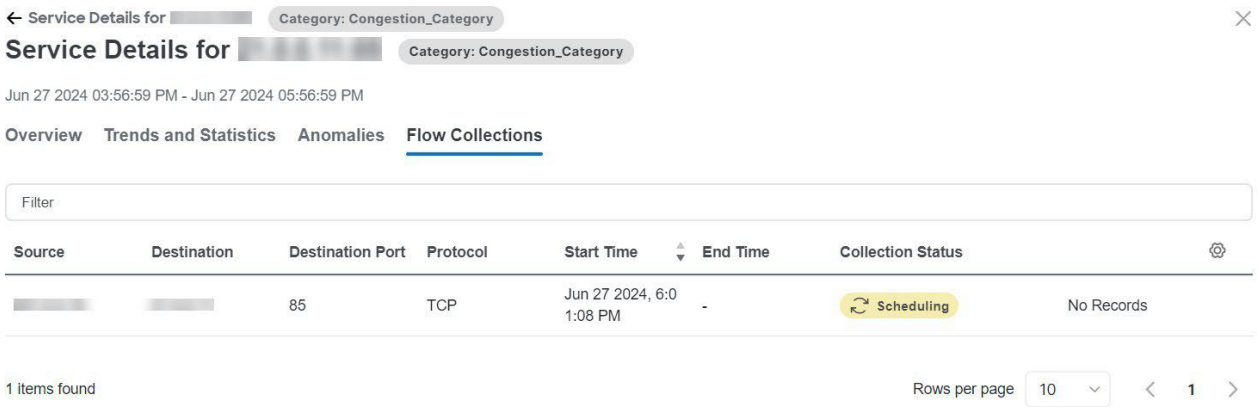
フローのトラブルシューティング ワークフロー

フロー トラブルシューティング ワークフローでは、2 つのエンドポイント間のすべてのフロー レコード

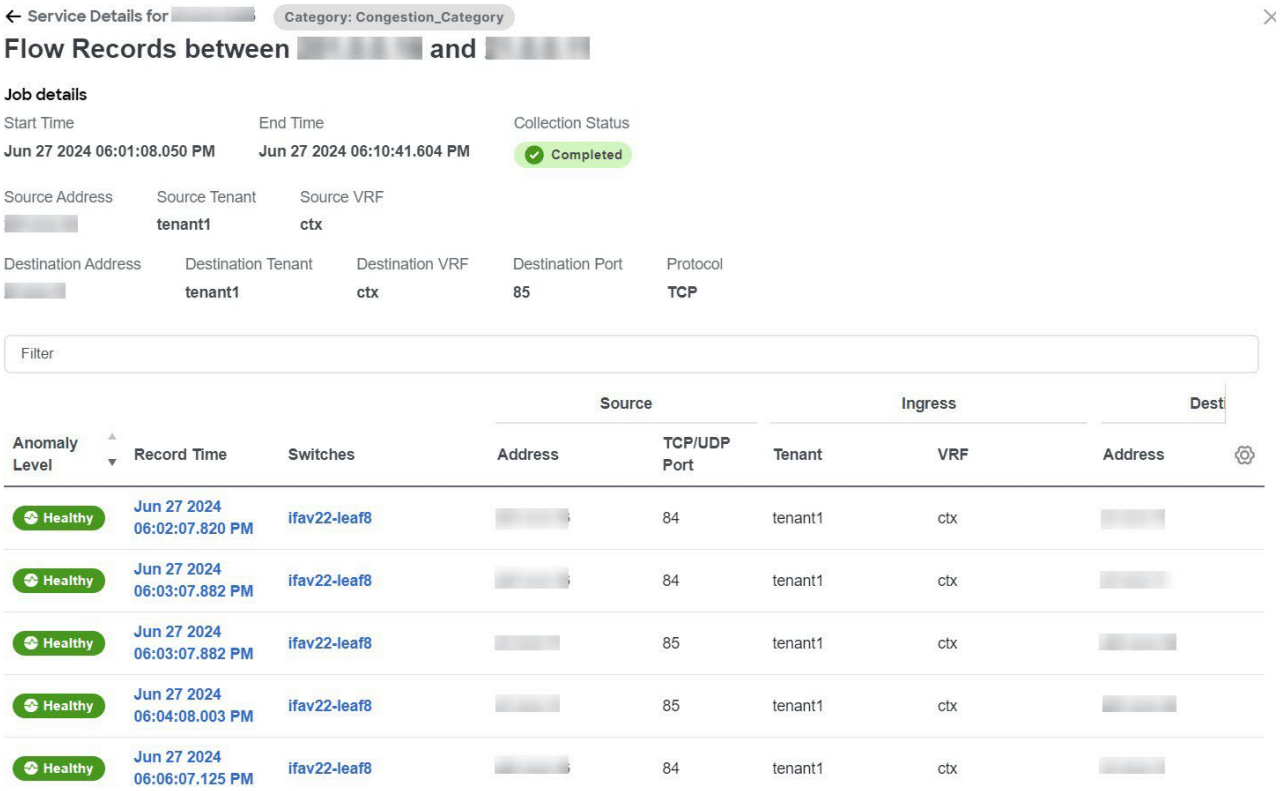
を収集できます。{CiscoNIRShortName} を使用すると、フロー収集の期間を指定し、指定した期間の特定のエンドポイント間のレコードを収集できます。結果として、パスの可視化、

5 タプルのフロー情報、および個々のフローで発生した問題を表示できます。

1. **[**分析（**Analyze**）**]** > **[**ハブの 分析（**Analyze Hub** ）**]** > **[**トラフィック分析（**Traffic Analytics**）**]** の順に選択します。
2. ドロップダウン メニューからファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。デフォルトでは、[現在の時刻（過去 2 時間）（Current time (last 2 hours)）] が選択されています。
4. **[**表示方法（**View by** ）**]** エリアで、最初のドロップダウン メニューから **[**サービス エンドポイント（**Service Endpoints** ）**]** を選択します。デフォルトでは、**[**サービス カテゴリ（**Service Categories**）**]** が選択されます。
5. **[**ビュー別（**View by**）**]** エリアのテーブルで、エンドポイントを選択し、[サービス ポート（Service Port）] にあるエンドポイントのポート番号をクリックします。
6. [サービスの詳細（Service Details）] ページで、クライアント IP アドレスの省略記号アイコンをクリックし、**[**フロー収集の開始（**Start Flow Collection**）**]** を選択します。省略記号アイコンを確認するには、クライアント IP アドレスのテーブルを右までスクロールする必要がある可能性があります。
7. 特定の期間のフロー レコードのサンプルを収集する期間を選択します。**[**開始してフロー収集タブに移動する（**Start and go to Flow Collections Tab**）**]** をクリックします。



8. [収集ステータス（Collection Status）] に [完了（Completed）] と表示されたら、**[**レコードの表示（**View Records**）**]** をクリックして、その特定のサービス エンドポイントのフロー レコードの詳細を表示します。



ファブリックのフロー収集を表示するには、**[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。ファブリックを選択します。**[接続（Connectivity）]** > **[フロー収集（Flow Collections）]** をクリックします。

フローのトラブルシューティングでは、次のシナリオでは、各レコード のパケットが通過するすべてのスイッチが表示されない場合があります。

- Nexus Dashboard Insights にフロードロップがある場合
- ハードウェアでテーブルの衝突が発生した場合

持続可能性レポート

持続可能性レポート

Nexus Dashboard Insights サステナビリティ レポートは、ネットワークのエネルギー使用量、関連する炭素排出量、総エネルギー コストをモニタリング、予測、改善するために役立ちます。サステナビリティ レポートでは、すべてのファブリックのエネルギー使用量、CO2 排出量、エネルギー コストに関するインサイトを月単位で取得できます。

レポートは、消費電力の月次値を計算し、選択した月の 1 日ごとに、各ファブリックのすべてのデバイスの使用量データを合計することで作成されます。このデータを Cisco Energy Manager と組み合わせることで、エネルギー コスト、推定排出量、推定スイッチ消費電力の観点で、その使用状況が何を意味するのかをより深く理解することができます。Cisco Energy Manager に関する詳細は、「Cisco Energy Manager」を参照してください。

レポートの概要エリアには、総低コスト、想定スイッチ電力消費、排出源、推定排出量などの情報を含んでいます。

- 推定コストでは、毎月のエネルギー使用量に基づいて、ファブリックの電気料金の予想される増減を把握できます。
- 予想されるスイッチ消費電力を使用すると、スイッチが電力をどの程度効率的に使用しているかを把握できます。[予想される PDU 電力消費量（Estimated PDU Power Consumption）] により、デバイスまたは Panduit 配電ユニット（PDU）が使用している電力量の詳細を示します。
- 推定CO2排出量では、使用する電力源と量に基づいて、ファブリックによる持続可能性への取り組みが総CO2排出量に及ぼす影響を把握できます。

Nexus Dashboard に Panduit PDU をオンボードしている場合、you can use the **[データ ソース（Data Source）]** トグルを使用して、サステナビリティ レポートで 2 つの異なる電気数値を確認できます。1 つはスイッチのみ、1 つは PDU です。

- [スイッチ データ（Switch Data）]：ファブリックに追加された個々のスイッチによって報告された電力データのみを使用
- [PDU データ（PDU Data）]：サポートされているPDUによって報告された電力データを使用します。このデータには、スイッチ、ファン、および PDU に物理的に接続されているその他のデバイスが含まれます。

[データソース（Data Source）] トグルで選択した値に応じて、推定コストや CO2 排出量など、他のメトリックに対して計算される値が変わります。

サステナビリティを活用して、以下のことが可能です。

- ファブリックのエネルギー料金の上昇をさらに予測し、予算が実際の使用量をより正確に反映するようにします。
- 個々のファブリックの 1 時間ごとのエネルギー使用量をより追跡します。使用料を分散させてピーク時間帯の割増料金を避けることで、長期的に電気代を下げることができる可能性があります。
- ファブリックを実行している際に気候変動に与える直接的なサステナビリティへの影響を確認します。経時的に CO2 排出量を追跡することで、低炭素排出源を選択し、ESG 目標の達成に向けた進捗状況を追跡することも促進されます。

Nexus Dashboard Insights のサステナビリティ レポートの保持時間は 12 か月間です。

Cisco Energy Manager

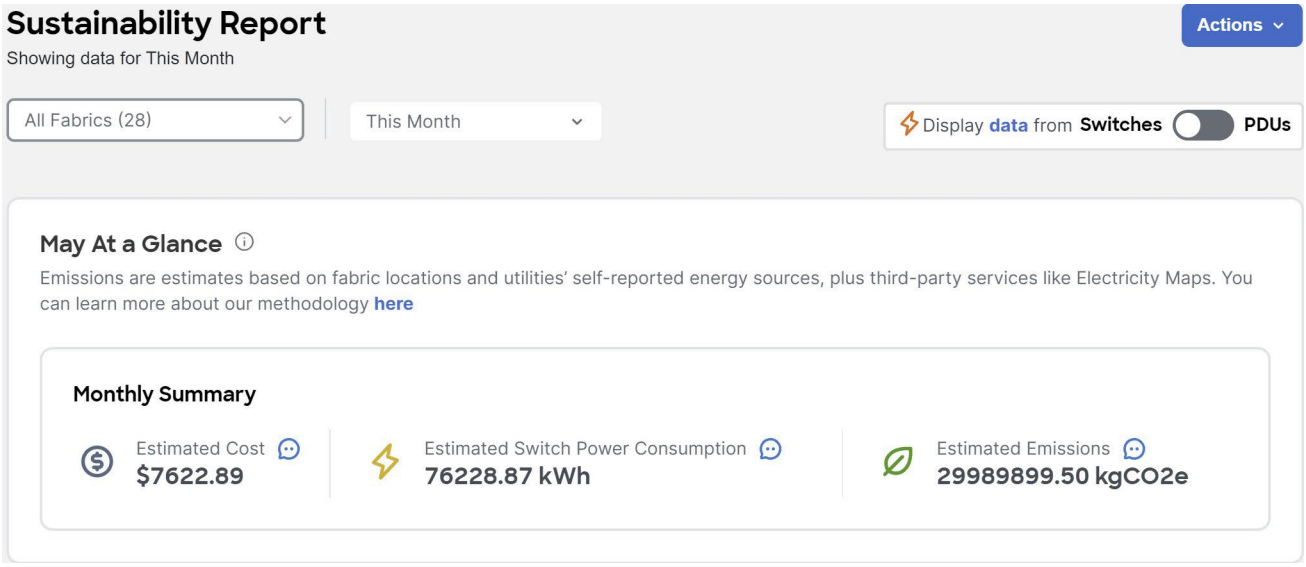
Cisco Energy Manager は Cisco により開発されたサービスであり、さまざまなデータ プロバイダからデータを収集し、データから GHG 排出量とエネルギー源を統合します。Cisco Energy Manager は、Cisco Intersight クラウドでホストされます。

スイッチのサステナビリティ レポートの表示

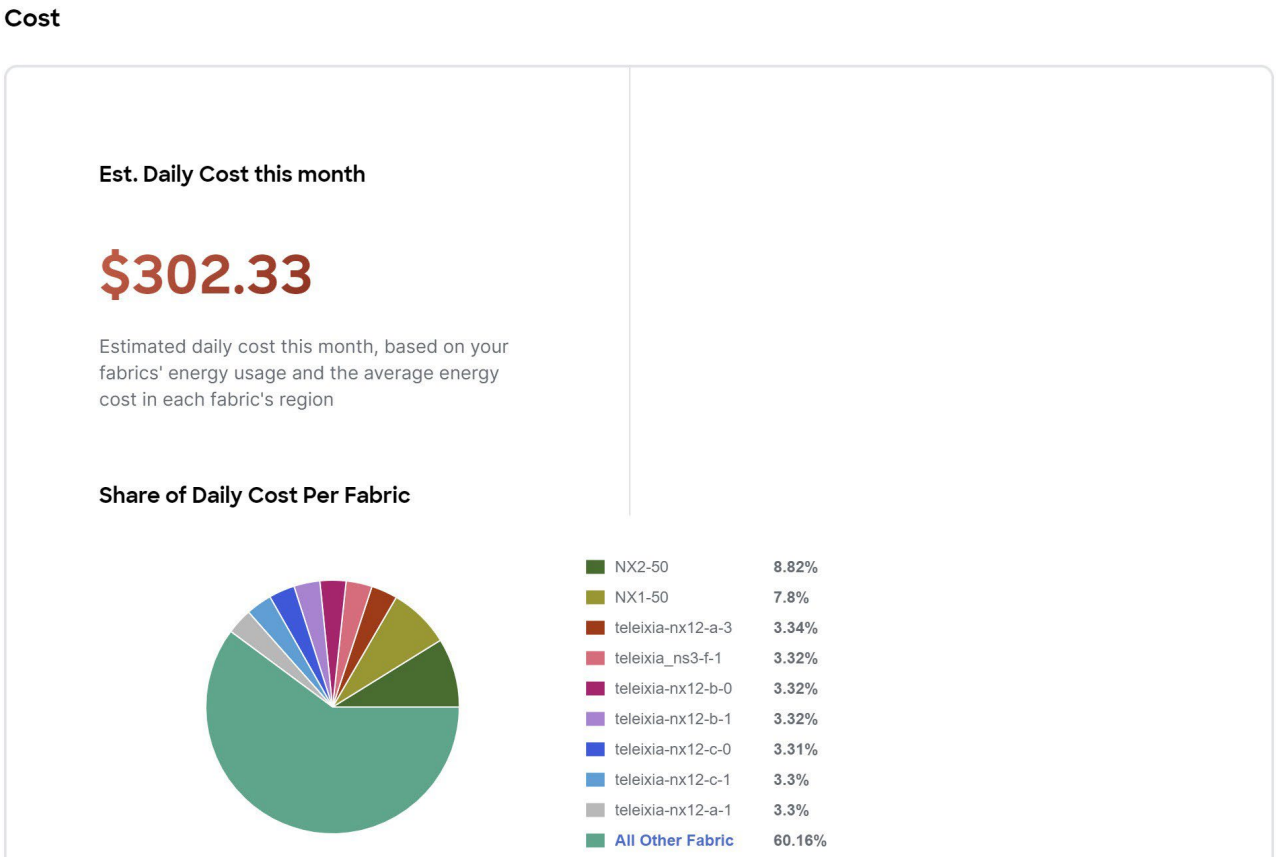
1. **[分析（Analyze）] > [分析ハブ（Analysis Hub）] > [サステナビリティ レポート（Sustainability Report）]** に移動します。
2. ドロップダウン メニューから、オンライン ファブリックまたは複数のオンライン ファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。
4. [データ ソース（Data Source）] トグルを活用して、スイッチからのデータを表示 します。
5. **[レポートの準備（Prepare Report）]** をクリックします。

   サステナビリティレポートには、選択した月の特定のファブリックの概要、コスト、エネルギー、および排出量の情報が表示されます。

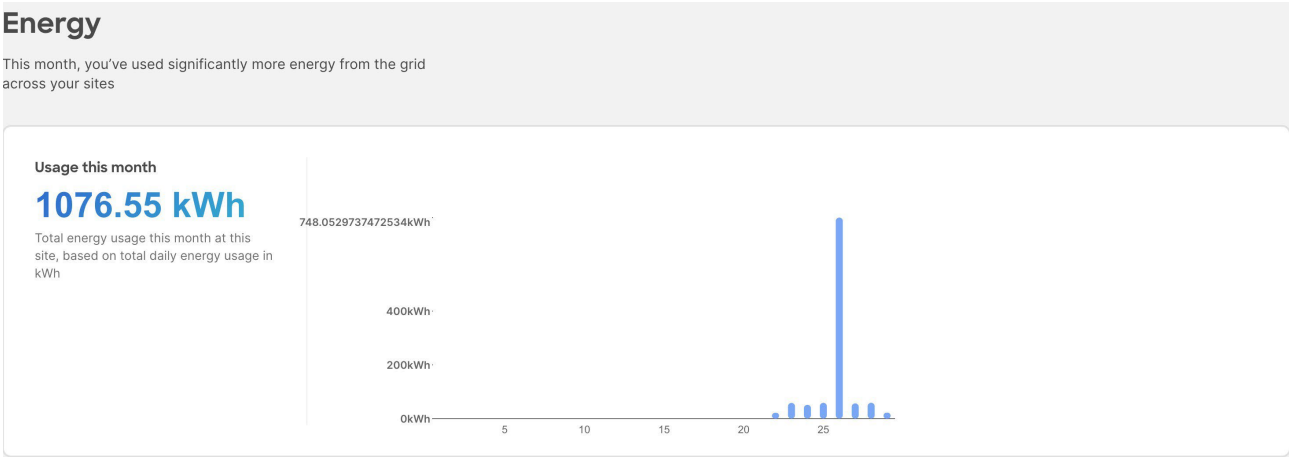
6. **[At A Glance]** エリアを調べて、選択した月の推定コスト、推定スイッチ電力消費量、および推定排出量の概要を確認します。詳細については、**[詳細（Learn More）]** アイコンをクリックします。



7. **[コスト（Cost）]** エリアを確認し、選択した月の 1 日あたりの推定コストと、ファブリックごとの 1 日あたりのコスト共有を確認します。

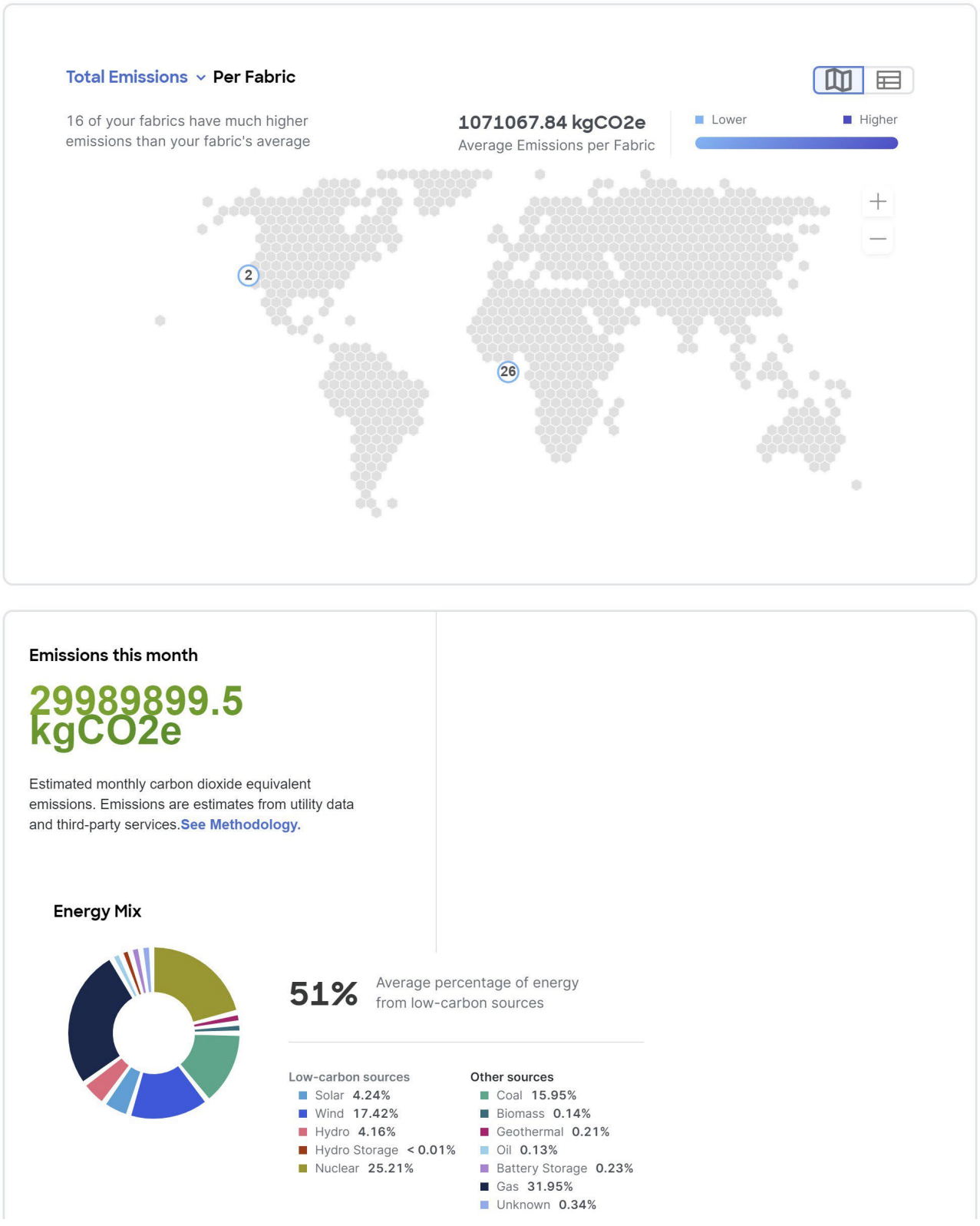


8. （オプション）[アクション（ **Actions** ）] メニューから [ファブリックエネルギー設定（ **Fabric Energy** 設定 ）] を選択し、より正確な見積書を得るために当月の平均コストをカスタマイズします。推定コストを算出するには、Nexus Dashboard Insights は、各リージョンのグリッド エネルギーの平均コストに基づく値を使用しています。
9. **[**エネルギー（ **Energy**） **]** エリアを調べて、選択した月のエネルギー使用量を kWh 単位で確認します。

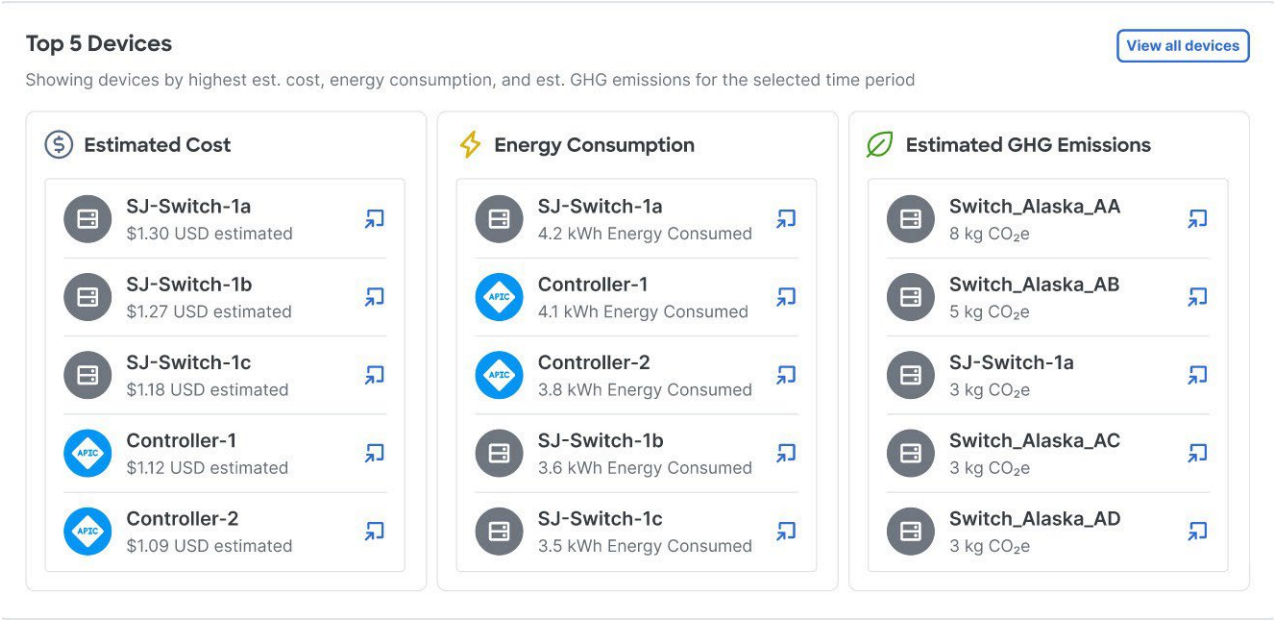


10. **[**排出量（**Emissions**）**]** エリアでは、ファブリックごとの総排出量または効率指標、月ごとの推定される二酸化炭素換算排出量、低炭素エネルギー源およびその他のエネルギー源からのエネルギーの平均割合、選択した月のすべての日で各 3 時間のレポート期間中に使用されたエネルギー源の総排出量の割合を確認することができます。

    ファブリックごとの総排出量または効率指標については、トグルを使用してグラフ形式または表形式で情報を表示します。



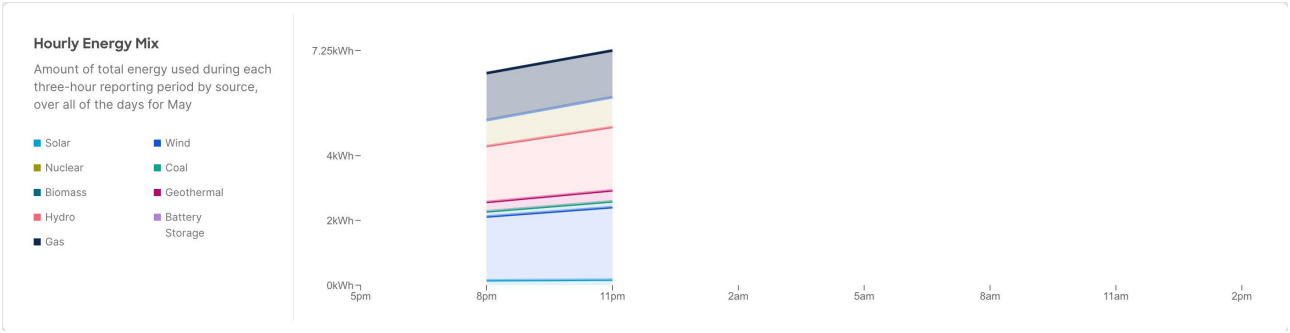
11. [上位5つのデバイス（**Top 5 Devices**）]エリアを調べて、推定コスト、消費電力量、および推定温室効果ガス（GHG）排出量が最も高い上位 5 つのデバイスを確認します。



[すべてのデバイスの表示（**View all devices**）**]** をクリックし、上位 5 デバイスだけではなく、すべてのデバイスのデータを確認します。

12. [ファブリック（fabric）] ドロップダウン メ ニューからファブリックを選択して、1 時間あたりのエネルギー混合を表示します。

    時間ごとのエネルギー効率は、選択した月のすべての日で各 3 時間のレポート期間中に使用された総エネルギー量をソース別に表示します。次のレポートを生成できるようになるまでの最小期間は 3 時間です。



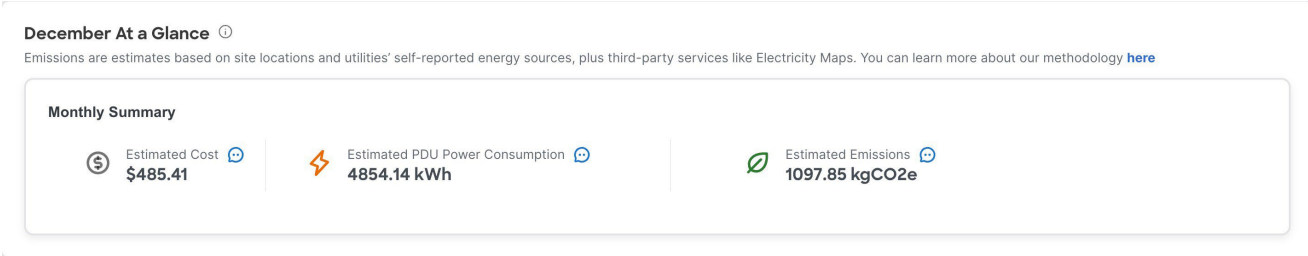
次のレポートを生成できるようになるまでの最小期間は 3 時間です。

PDU のサステナビリティ レポートの表示

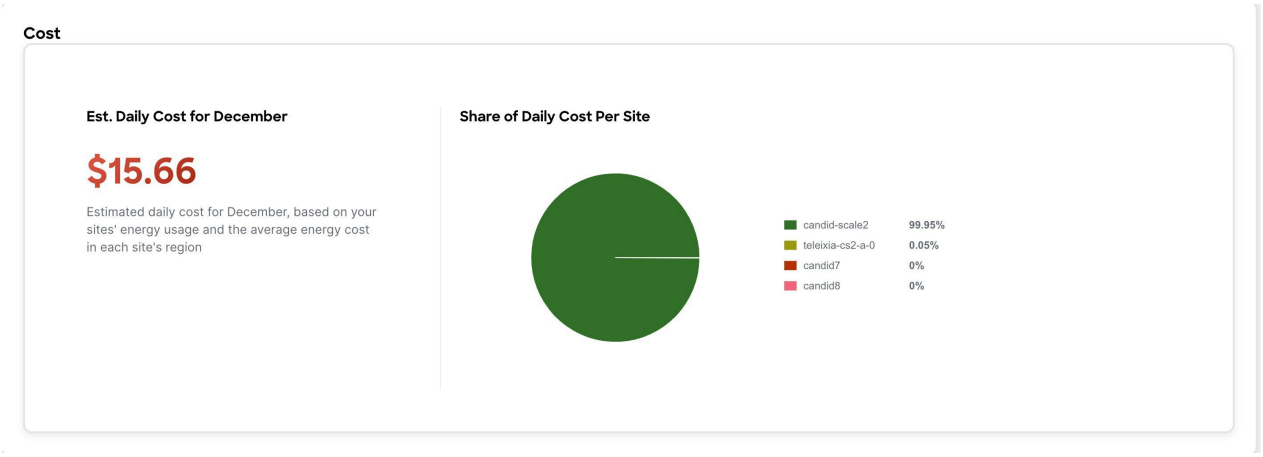
1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**サステナビリティ レポート（**Sustainability Report**）**]** に移動します。
2. ドロップダウン メニューから、オンライン ファブリックまたは複数のオンライン ファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。
4. [データ ソース（Data Source）] トグルを活用して、PDU からのデータを表示します。
5. **[**レポートの準備（**Prepare Report**）**]** をクリックします。

   サステナビリティレポートには、選択した月の特定のファブリックの概要、コスト、エネルギー、および排出量の情報が表示されます。

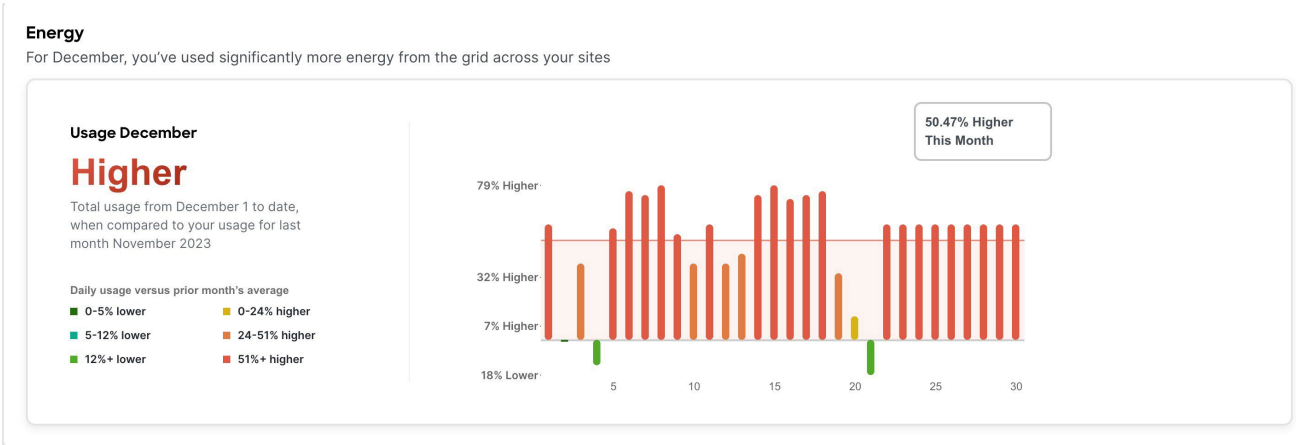
6. [**At A Glance**] エリアを調べて、選択した月の推定コスト、推定スイッチ電力消費量、および推定排出量の概要を確認します。[詳細（**Learn More**）] アイコンをクリックします。



7. [コスト（**Cost**）] エリアを確認し、選択した月の 1 日あたりの推定コストと、ファブリックごとの 1 日あたりのコスト共有を確認します。

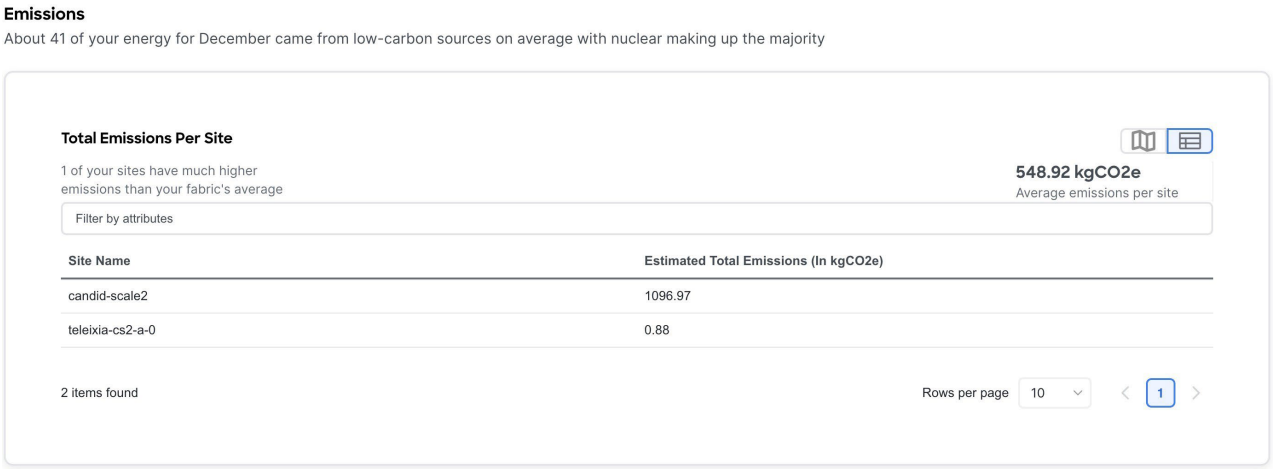


8. （オプション）[アクション（ **Actions** ）] メニューから [ファブリックエネルギー設定（ **Fabric Energy** 設定 ）] を選択し、より正確な見積書を得るために当月の平均コストをカスタマイズします。推定コストを算出するには、Nexus Dashboard Insights は、各リージョンのグリッド エネルギーの平均コストに基づく値を使用しています。
9. [エネルギー（ **Energy**）] エリアを調べて、選択した月のエネルギー使用量を kWh 単位で確認します。



10. [排出量（**Emissions**）] エリアでは、ファブリックごとの総排出量、月ごとの推定される二酸化炭素換算排出量、低炭素エネルギー源およびその他のエネルギー源からのエネルギーの平均割合、選択した月のすべての日で各 3 時間のレポート期間中に使用されたエネルギー源の総排出量の割合を確認することができます。

    ファブリックごとの総排出量については、トグルを使用して、グラフ形式または表形式で情報を表示します。

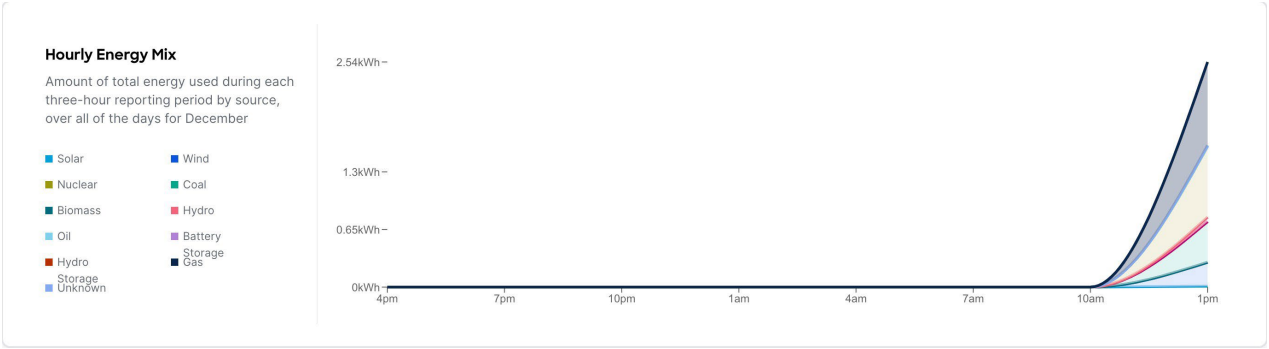


11. [上位5つのデバイス（**Top 5 Devices**）]エリアを調べて、推定コスト、消費電力量、および推定温室効果ガス（GHG）排出量が最も高い上位 5 つのデバイスを確認します。

    [すべてのデバイスの表示（**View all devices**）**]** をクリックし、上位 5 デバイスだけではなく、すべてのデバイスのデータを確認します。

12. [ファブリック（fabric）] ドロップダウンメ ニューからファブリックを選択して、1 時間あたりのエネルギー混合を表示します。

    時間ごとのエネルギー効率は、選択した月のすべての日で各 3 時間のレポート期間中に使用された総エネルギー量をソース別に表示します。次のレポートを生成できるようになるまでの最小期間は 3 時間です。



デルタ分析

デルタ分析

Nexus Dashboard Insights は定期的にサイトの分析を実行し、データはノード数に応じた間隔で収集されます。

ノード数	**Interval**
100 人未満	2 時間
100 ~ 400	3時間
400 以上	12時間

Nexus Dashboard Insightsは、各間隔でコントローラポリシーとファブリックに関する実行時の状態のスナップショットをキャプチャし、分析を実行して、異常を生成します。生成された異常は、スナップショット時点でのネットワークの状態を表します。

差分分析を使用すると、2つのスナップショット間のポリシー、実行時の状態、およびネットワークの状態の違いを分析できます。

[差分分析の作成（Create Delta Analysis）]：新しい差分分析を作成し、既存の分析を管理できます。「差分分析の作成」を参照してください。

正常性の差分

正常性の差分では、2つのスナップショット間におけるファブリックの正常性の違いを分析しま

す。詳細については、 「正常性デルタ分析の表示」 を参照してください。

NDFC のポリシーの差分

NDFC ファブリックのポリシー差分では、2つのスナップショット間で変更されたノードまたはスイッチを分析し、NX-OS スイッチで変更された内容の相互に関連するビューを取得します。

詳細については、 「ポリシー差分分析のビュー」 を参照してください。

デルタ分析の注意事項と制約事項

- 差分分析機能は現在、ローカル認証ドメインのみをサポートしています。
- 現在、一度に複数の差分分析を作成できますが、一度に複数の差分分析をキューに入れないことをお勧めします。さらに、オンライン ファブリックの同時分析の実行時間に悪影響を与えるリスクを回避するために、新しい分析を作成する前に少し（約 10 分）待つことをお勧めします。

  差分分析によってデータベースの負荷が増加するため、相互依存が発生します。複数の連続した差分分析によりデータベースの負荷が高い状態が維持されると、オンライン分析の実行時間に影響を与える可能性があります。

- **[変更されたノード（Changed Nodes）]** エリアの **[ポリシー差分（Policy Delta）]** ページでスイッチを選択すると、2つのスナップショット間の構成の違いが表示されます。
- [ポリシー デルタ（Policy Delta）] では、**[監査ログ（Policy Delta）]** は現在サポートされていません。

デルタ分析を作成

[分析（Analyze）] > **[分析ハブ（Analysis Hub）]** > **[差分分析（Delta Analysis）]** > **[差分分析の作成（Create Delta Analysis）]** を選択します。

1. **[差分分析の 名前（Delta Analysis Name）]** フィールドに、名前を入力します。名前は、すべての分析で一意である必要があります。
2. **[ファブリック（Fabric）]** をクリックして、ファブリックを選択します。
3. **[前のスナップショットの選択（Choose Earlier Snapshot）]** をクリックし、差分分析の最初のスナップショットを選択します。[適用（Apply）] をクリックします。
4. **[後のスナップショットの選択（Choose Later Snapshot）]** をクリックし、差分分析の 2 番目のスナップショットを選択します。クリックします。
   [適用]をクリックします：

   デルタ分析用に選択した 2 つのスナップショットは、同じファブリックに属している必要があります。

5. **[概要（Summary）]** で作成された差分分析の概要をビューします。
6. [保存（Save）] をクリックします。デルタ分析のステータスは、**[デルタ分析（Delta Analysis）]** テーブルに表示されます。完了後、**[差分分析の表示（View Delta Analysis）]** または **[別の差分分析の作成（Create another Delta Analysis）]** を実行できます。

一度に1つの差分分析を実行できます。別の差分分析を実行するには、現在の差分分析を停止してから、別の差分分析を開始する必要があります。

1. (任意) [ステータス（Status）] 列から、進行中またはスケジュールされた分析を選択し、**[...]** オプションの
   [停止（STOP）] をクリックして差分分析を停止します。
2. **[...**] をクリックすると、作成した分析を 削除できます。

差分ルールの作成中にエラーが発生した場合は、ルール作成の概要ページにバナーとして表示されます。

デルタ分析の表示

差分分析ページには、分析が表形式で表示されます。分析はステータスでソートされています。**[差分分析の作成（Create Delta Analysis）**] ボタンを使用すると、新しい差分分析を作成できます。差分分析をクリックすると、詳細が表示されます。

分析のステータスは、**[中断（Aborted）]**、**[保留中（Pending）]**、**[停止済み（Stopped）]**、**[停止中（Stopping）]**、**[成功（Success）]**、**[失敗（Failed）]**、**[一部失敗（Partially Failed）]**、**[キュー済み（Queued）]**、**[完了（Completed）]**、**[進行中（In progress）]** のいずれかになります。

フィルタ バーを使用すると、次の要因で分析をフィルタ処理できます。

- status

- name
- 送信者 ID
- fabric

差分分析ダッシュボードには、正常性性とポリシーの差分とともに一般情報が表示されます。

- 正常性の差分分析の結果を表示するには、「正常性の差分分析の表示」を参照してください。
- ポリシーの差分分析の結果を表示するには、「ポリシーの差分分析の表示」を参照してください。

正常性の差分分析の表示

正常性の差分では、2つのスナップショット間におけるファブリックの正常性の違いを分析します。結果は次のエリアに表示されます。

[承認済みの異常を含める（Include Acknowledged Anomalies）] のトグルをオンにすると、承認済みの異常を表示結果から除外することができます。無効な場合、手動で承認された異常は [異常カウント（Anomaly Count）] に含まれます。

- **[異常数]**：スナップショット全体の重大度ごとに異常数の差が表示されます。

最初の数は、以前のスナップショットでのみ見つかった異常数を表します。2 番目の数は、後のスナップショットでのみ見つかった異常数を表します。

デルタ分析は、カウント デルタではなくオブジェクト デルタを実行するようになりました。そのため、カウントとともにクリアされた異常の数、変更されていない異常の数、および新しい異常の数を表示できるようになりました。

異常カウントには、さまざまなタイプの異常の差も表示されます。[クリティカル（Critical）]、**[主要（Major）]** および **[注意（Warning）]** に表示されます。

- **[リソース別デルタ（Delta by Resources）]**：新規、失われた、または変更されていないリソースの数をタイプ別に表示します。**[変更のみ表示（View Changed Only）]** トグルをクリックして、カウントが変更されたリソースを具体的に表示することもできます。フィルタ バーを使用すると、リソースでデータをフィルタ処理できます。歯車アイコンにより、ビューに従って列をカスタマイズすることができます。この表には、カウント差分と正常性差分も表示されます。カウント差分には、正常なリソースと異常なリソースの両方が含まれます。フィルタされた場合、正常なリソースには異常が関連付けられません。正常性の差分には、異常なリソースのみが表示され、異常でフィルタされた場合は異常が返されます。

この分析は、次のリソースで使用できます。

- インターフェイス
- エンドポイント
- スパイン
- ボーダーゲートウェイ
- リーフ
- ボーダーリーフ
- VLAN
- VRF

- SVI
- L2VNI
- L3VNI
- VNI
- VPC

[カウント（Count）] および [正常性デルタ（Health Delta）] リソースのいずれかのカウントをクリックすると、ノード情報とともにリソースのリストを表示できます。SVI の場合、ノード列に VNI の関連付けが表示されます。

- **[**すべての異常（**All Anomalies**）**]** : **[**タイトル別にグループ化（**Grouped by title**）**]** ビューには、2 つのスナップショット間で集約された異常の差分ステータスが表示されます。**[**タイトル別にグループ化（**Grouped by title**）**]** ビューには、2 つのスナップショット間における異常ごとの差分ステータスが表示されます。

異常は、次のタイプについてリストできます。

- 新規
- [変更なし（Unchanged）]
- クリア済み
- 以前のスナップショットから
- 後のスナップショットから

異常が以下のフィールドで表形式で表示されます。

- タイトル
- レベル
- Category
- 数

> 歯車アイコンにより、ビューに従って列をカスタマイズできます。

次の属性に基づいて結果をフィルタできます。

- ボーダー ゲートウェイ（リーフ）
- ボーダーリーフ（リーフ）
- インターフェイス
- L2VNI
- L3VNI
- リーフ
- スパイン
- SVI
- VLAN
- VNI

- VPC
- VRF

異常を選択し、異常の詳細を表示します。

Cisco Confidential

ポリシー差分分析の表示

[ポリシーの差分（**Policy Delta**）**]** をクリックして、2 つのスナップショット

間におけるポリシーの変更を表示します。ポリシー差分には以下の 2 つのセク

ションが含まれます。変更されたオブジェクトとポリシー ビューア

- **[**変更されたポリシー オブジェクト（**Changed Policy Object**）**]** には、2 つのスナップショット間で変更されたオブジェクトが表示されます。
- **[**ポリシービューア（**Policy Viewer**）**]** には、以前のスナップショットと後のスナップショットにわたる構成が表示されます。以前のスナップショットのスイッチ設定は、以前のスナップショットポリシーと呼ばれます。後のスナップショットのスイッチ設定は、後のスナップショットポリシーと呼ばれます。
  - より多くのコンテンツを表示するには、**[**上に追加のコードを表示**]**または**[**下に追加のコードを表示**]** をクリックします。
  - [ダウンロード]アイコンをクリックして、スナップショットポリシーをエクスポートします。
  - また、**[**変更された設定のみ表示（ **View Changed Only**）**]** トグル を切り替えます。

バグスキャン

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、ファブリック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。

ファブリック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。詳細については『スタートアップガイド』の「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 にオンボーディングされたすべてのファブリックに対して実行され、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、ファブリック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。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。

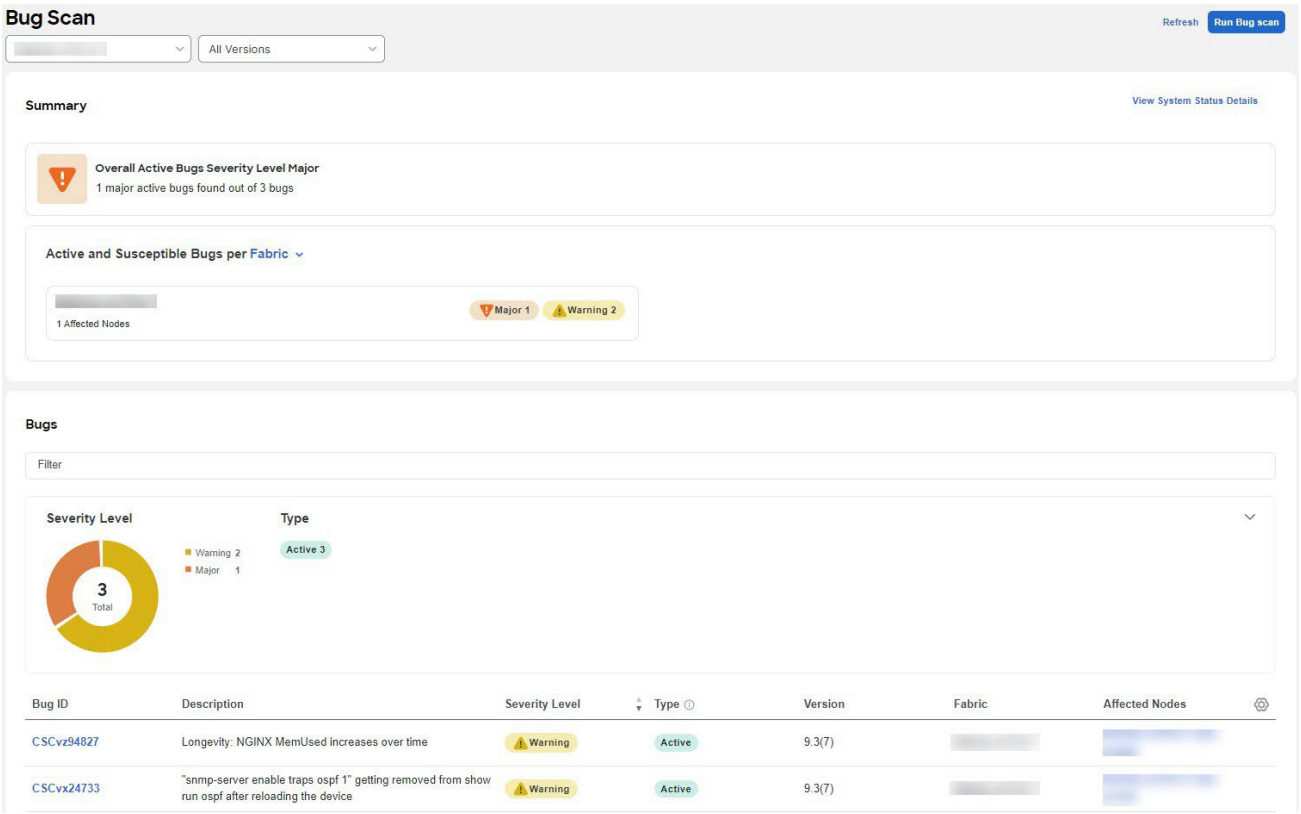
特定のデバイスで実行できるバグ スキャンは一度に 1 つだけです。ただし、バグ スキャンがすでに進行中の 1 つのデバイス セットがある場合、2 番目の（自動スケジュールまたはオンデマンドの）バグ スキャンは、Nexus Dashboard Insights に十分なリソースがある場合にのみ実行できます。それ以外の場合は、リソースが使用可能になるとすぐに保留され、開始されます。

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、ファブリック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。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。

- [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、オンライン ファブリックまたは複数のオンライン ファブリックを選択します。
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。選択したファブリックとソフトウェア バージョンのアクティブ バグと影響を受けやすいバグが表示されます。

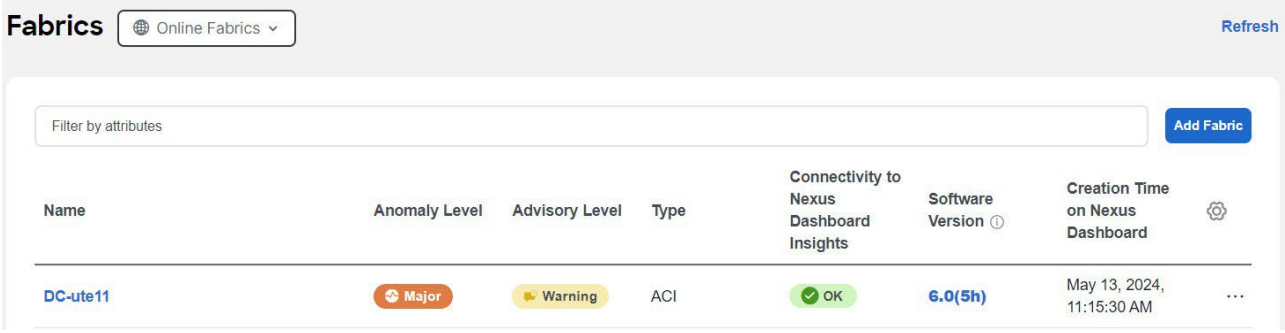


4. [概要（Summary）] エリアには、現用系バグ全体が重大度別に表示されます。ドロップダウン メニューを使用して、ファブリックまたはソフトウェア バージョンごとのバグを表示することもできます。
5. [バグ（Bugs）] エリアで、フィルタ バーを使用して、バグ ID、説明、重大度レベル、タイプ、および影響を受けるノードでバグをフィルタ処理します。
6. **[重大度レベル（Severity Level）]** の円グラフには、重大、主要、注意の重大度のバグの合計数が表示されます。
7. バグ テーブルを表示して、フィルタされたバグを確認します。
   a. 列の見出しをクリックして、テーブルのバグを並べ替えます。
   b. 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。
   c. **[バグ ID （Bug ID）]** をクリックしてバグの詳細を表示します。
8. **[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。ファブリックを選択し、**[今すぐ実行（Run Now）]** をクリックします。詳細については『スタートアップ ガイド』の「オンデマンド分析」を参照してください。

個々のファブリックのアクティブなバグと潜在的なバグのビュー

Nexus Dashboard Insights では、次の方法で個々のファブリックのバグを表示することもできます。

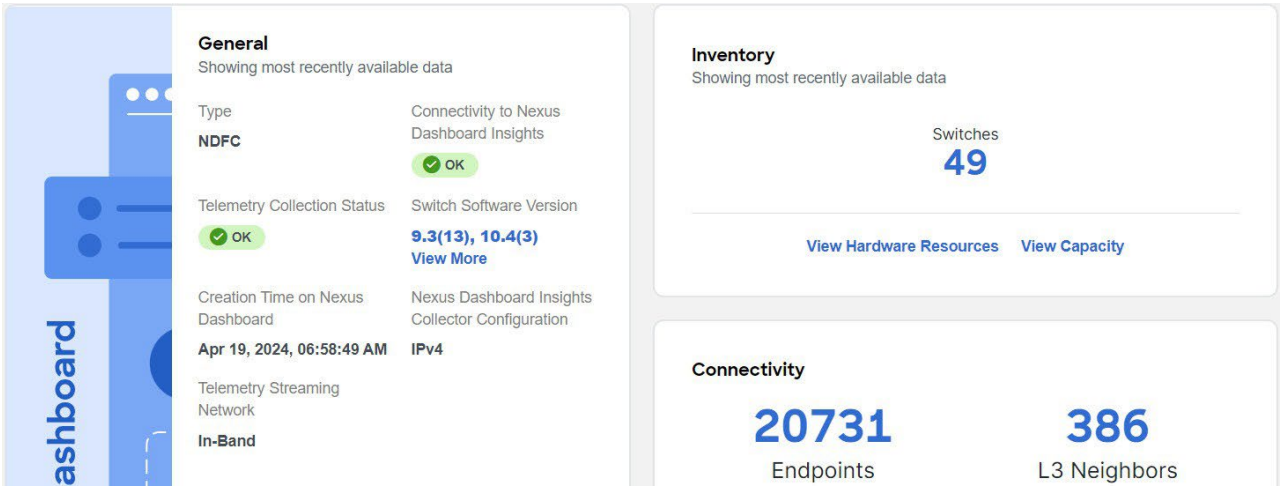
1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. ドロップダウン メニューから **[オンライン ファブリック（Online Fabrics）]** を選択します。



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、そのファブリック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。詳細については『スタートアップ ガイド』の「オンデマンド分析」を参照してください。

または

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 メニューから **[オンライン ファブリック（Online Fabrics）]** を選択します。
3. ファブリックを選択します。



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、そのファブリック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。詳細については『スタートアップ ガイド』の「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 メニューから **[オンライン ファブリック（Online Fabrics）]** 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. オンデマンドバグ スキャンを実行するには、[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** ）] をクリックします。詳細については、『 スタートアップ ガイドに』の「オンデマンド分析」セクションを参照してください。

または

1. **[管理（Admin）] > [ファブリック ソフトウェア管理（Fabric 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、そのファブリックのアクティブ バグと影響を受けやすいバグを表示します。
4. [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。詳細については『スタートアップ ガイド』の「オンデマンド分析」を参照してください。

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.