

DCNM NX-OS v2 向け Cisco Network Insights



最終更新日：11-May-2020

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

このデモンストレーションについて	1
このソリューションについて	2
はじめに	3
シナリオ 1. Network Insights Advisor	4
シナリオ 2. Network Insights Resources	16
次に必要な作業	28

このソリューションについて

Cisco Network Insights for Resources (NIR) アプリケーションは、ハードウェアとソフトウェアのテレメトリデータを継続的にモニタして記録し、ファブリック内の異常を特定します。また、トラブルシューティング、根本原因の分析、キャパシティプランニング、修復作業を自動化します。NIR により、インフラストラクチャの所有者は、顧客が求めている SLA を遵守することができます。NIR アプリケーションは、ACI/APIC および NXOS/DCNM プラットフォームのいずれでも機能します。

Cisco® Network Insights Advisor (NIA) アプリケーションを利用すれば、さまざまな情報が事前に通知されるため、データセンターネットワークの計画外停止を回避し、ダウンタイムを短縮できます。通知内容には、セキュリティアドバイザリ、重要なバグ、ライフサイクル終了のお知らせ、サポート終了のお知らせ、および、プラットフォーム、導入済みソフトウェア、機能に応じて推奨されるソフトウェア/ハードウェアのアップグレードなどがあります。また、問題発生時に Cisco Technical Assistance Center (TAC) にサービスを依頼するために必要なデータを収集できるため、迅速なトラブルシューティングが可能になります。これらの機能により、運用コストを削減し、トラブルシューティング時間を短縮しながら円滑に運用することができます。NIA アプリケーションは、Cisco ACI™ /APIC および Cisco NX-OS/Data Center Network Manager (DCNM) プラットフォームの両方で機能します。

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

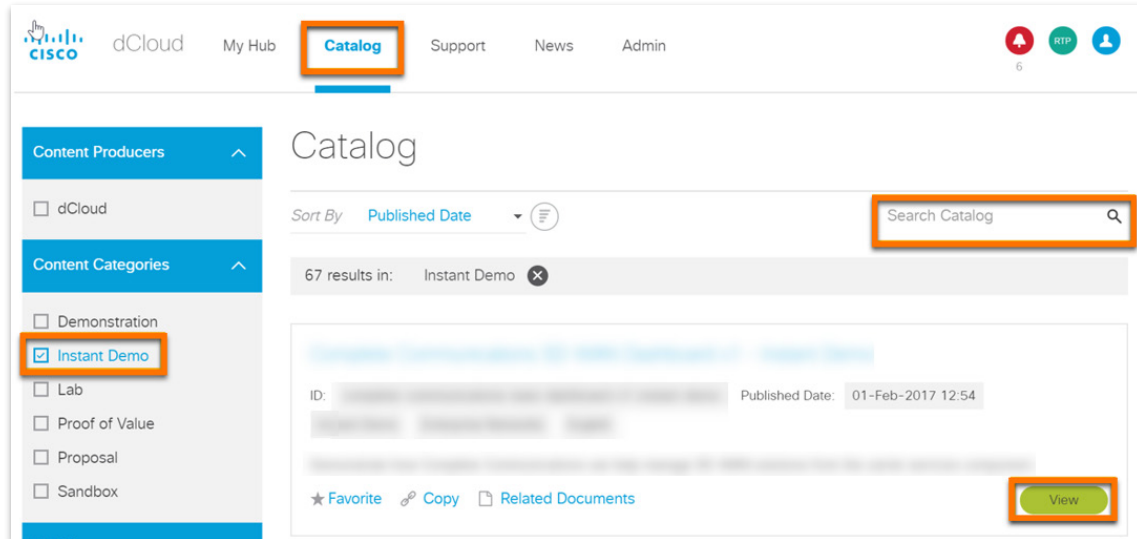
場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. [カタログ (Catalog)] をクリックして、サイドバーから [インスタントデモ (Instant Demo)] を選択します。これで、すべての dCloud インスタントデモが一覧表示されます。
2. 該当する [表示 (View)] ボタンをクリックします。

注：あるいは、[カタログ検索 (Search Catalog)] ボックスを使用してインスタントデモの名前を検索することもできます。



注： 2 時間有効な一意のログイン情報を使用して DCNM に自動的にログインされます。セッションを延長して新しくログインするには、dCloud UI のインスタントデモエントリに戻ります。

シナリオ 1. Network Insights Advisor

注：「LAN スイッチのログイン情報を今すぐ設定しますか？ (Do you want to set the LAN switch credentials now?) 」という確認メッセージが表示されたら、[いいえ (No)]をクリックします。

左側のメニューで次の手順を実行します。

1. [アプリケーション (Application)]をクリックします。
2. [Network Insights Advisor] をクリックします。

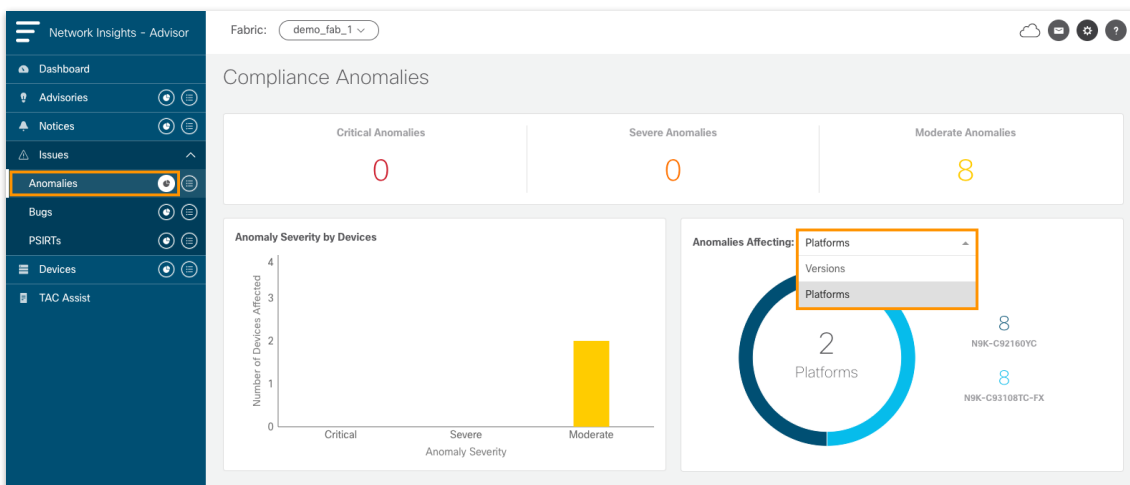


問題

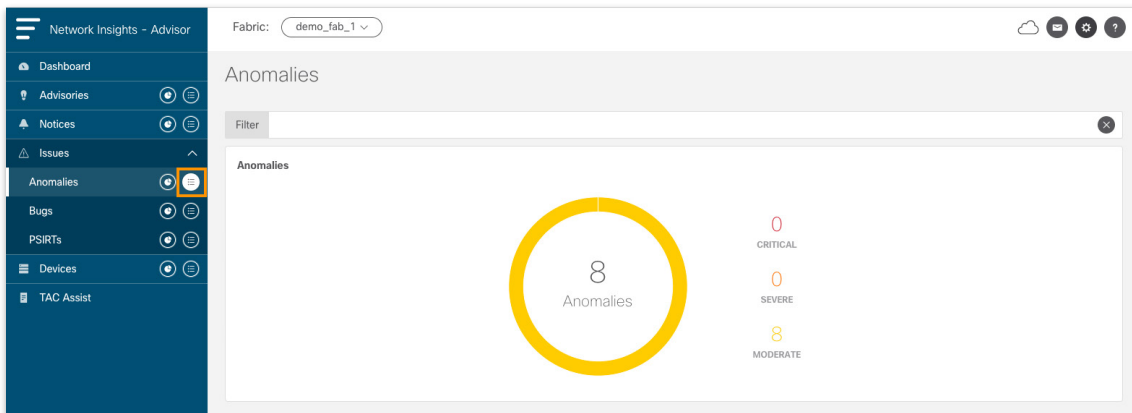
異常

左側のメニューで次の手順を実行します。

1. [異常 (Anomalies)]をクリックします。
2. [異常の影響 (Anomalies Affecting)]ドロップダウンから [プラットフォーム (Platform)]を選択します。



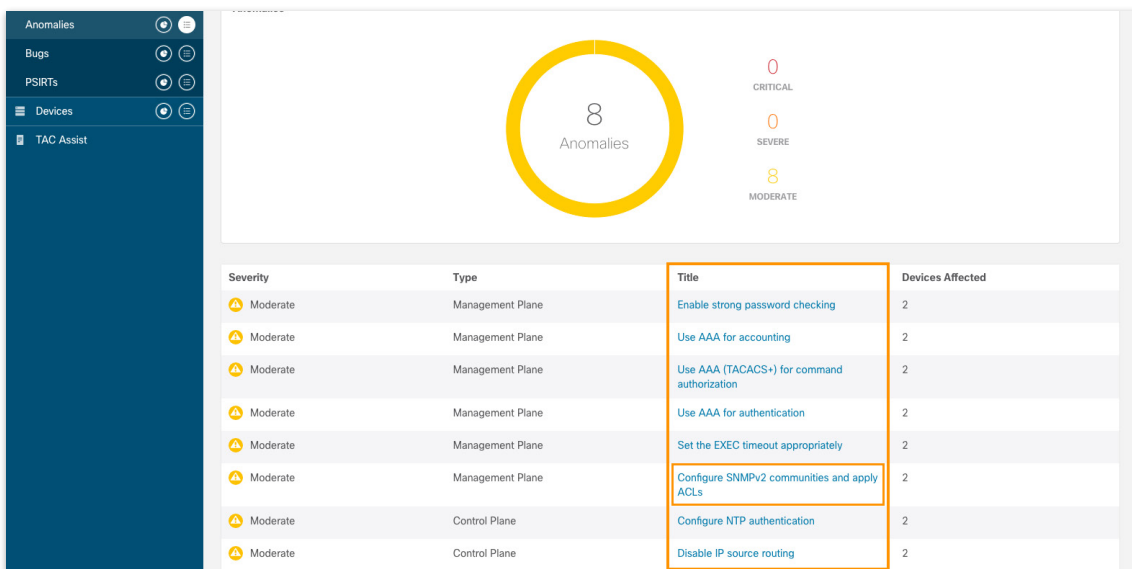
3. [異常 (Anomalies)] > [参照 (Browse)] をクリックします。



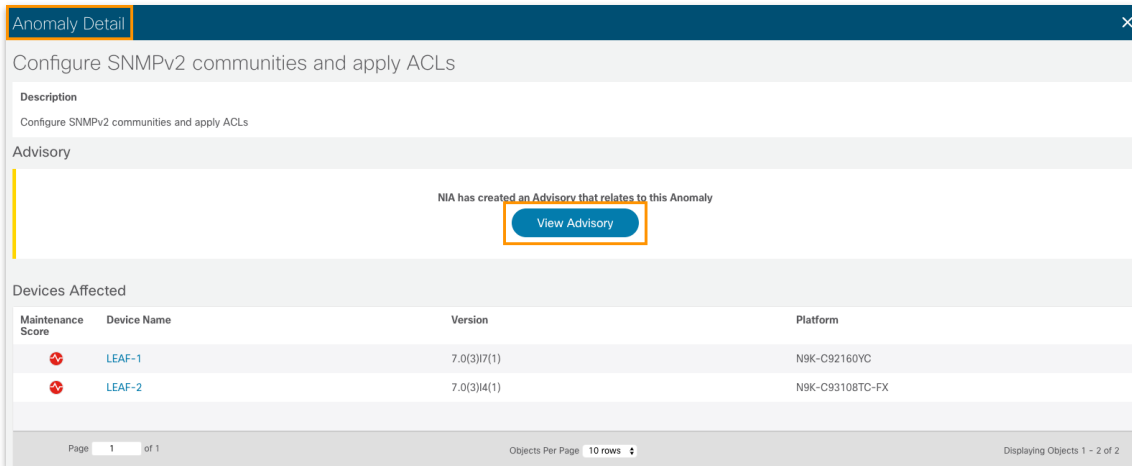
4. ページを上スクロールしてテーブルを表示します。

[タイトル (Title)] 列で次の手順を実行します。

5. [SNMPv2 コミュニティの設定と ACL の適用 (Configure SNMPv2 communities and apply ACLs)] リンクをクリックします。

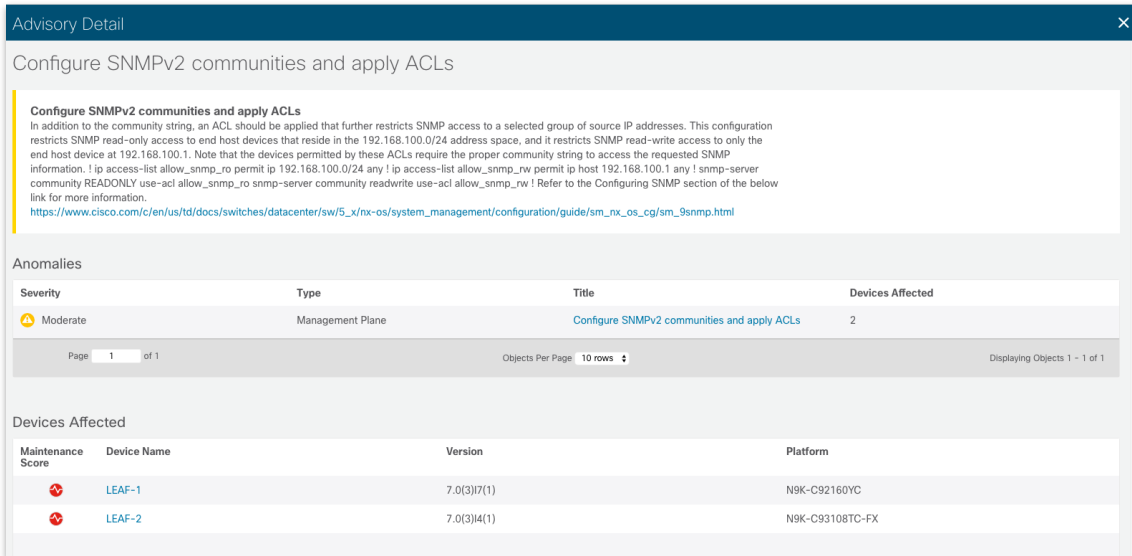


6. [アドバイザリの表示 (View Advisory)]をクリックします。



The screenshot shows the 'Anomaly Detail' window for the configuration 'Configure SNMPv2 communities and apply ACLs'. The 'Advisory' section contains a message: 'NIA has created an Advisory that relates to this Anomaly' with a 'View Advisory' button highlighted by a red box. Below this is a table of affected devices.

Maintenance Score	Device Name	Version	Platform
⚠	LEAF-1	7.0(3)17(1)	N9K-C92160YC
⚠	LEAF-2	7.0(3)14(1)	N9K-C93108TC-FX



The screenshot shows the 'Advisory Detail' window for the configuration 'Configure SNMPv2 communities and apply ACLs'. It provides detailed information about the advisory, including a link to the Cisco documentation. Below the advisory text is a table of anomalies and a table of affected devices.

Severity	Type	Title	Devices Affected
Moderate	Management Plane	Configure SNMPv2 communities and apply ACLs	2

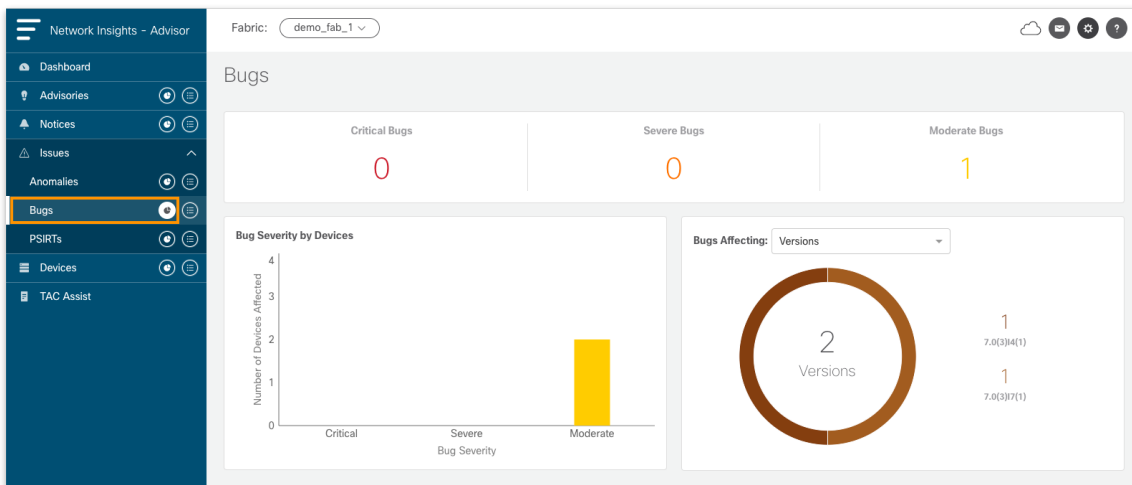
Maintenance Score	Device Name	Version	Platform
⚠	LEAF-1	7.0(3)17(1)	N9K-C92160YC
⚠	LEAF-2	7.0(3)14(1)	N9K-C93108TC-FX

7. [アドバイザリの詳細 (Advisory Detail)]ページを閉じます。

バグ

左側のメニューで次の手順を実行します。

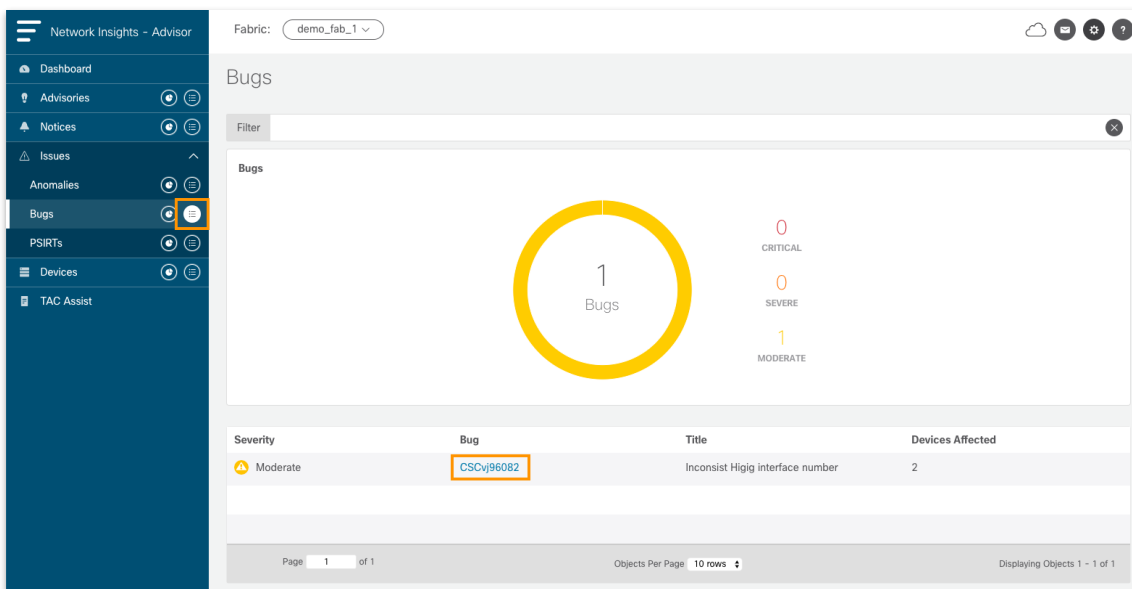
1. [バグ (Bug)] をクリックします。
2. 表示された情報を確認します。



3. [バグ (Bug)] > [参照 (Browse)] をクリックします。

[バグ (Bug)] 列で次の手順を実行します。

4. [CSCvj96082] リンクをクリックします。



5. ページを上スクロールして [アドバイザリ (Advisory)] パネルを表示します。
6. [アドバイザリの表示 (View Advisory)] をクリックします。

7. 表示された情報を確認します。
 8. [アップグレードの影響 (Upgrade Impact)] をクリックします。
 9. [アップグレードの影響を実行 (Run Upgrade Impact)] をクリックします。
- [結果 (Result)] 列で次の手順を実行します。
10. [中断 (DISRUPTIVE)] リンクをクリックします。
 11. [LEAF-1 - 中断 (LEAF-1 - DISRUPTIVE)] ダイアログを閉じます。
 12. [アドバイザリの詳細 (Advisory Detail)] ページを閉じます。

Advisory Detail

Recommended version is 7.0(3)I7(6)

Recommended version is 7.0(3)I7(6)
 We recommend upgrading to version 7.0(3)I7(6). Please find the release notes for this version in the following link(s).
<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html>

Release Notes: [7.0\(3\)I7\(5a\)](#) [7.0\(3\)I7\(6\)](#) [7.0\(3\)I4\(9\)](#)

Upgrade Paths

Recommended Upgrade Paths	Devices Affected	Non Disruptive	Disruptive
7.0(3)I7(1) → 7.0(3)I7(5a) → 7.0(3)I7(6)	1	0	1
7.0(3)I4(1) → 7.0(3)I4(9) → 7.0(3)I7(6)	1	1	-

Page: 1 of 1 Objects Per Page: 10 rows Displaying Objects 1 - 2 of 2

Upgrade Impact Result

Device Name	Version	Version To	Result	Upgrade Impact Status	Last Run Time
LEAF-1	7.0(3)I7(1)		DISRUPTIVE		Feb 25, 2020 09:14 am
LEAF-2	7.0(3)I4(1)		NONDISRUPTIVE		Feb 25, 2020 09:14 am

Page: 1 of 1 Objects Per Page: 10 rows Displaying Objects 1 - 2 of 2

PSIRT

左側のメニューで次の手順を実行します。

1. [PSIRT (PSIRTs)] をクリックします。
2. 表示された情報を確認します。

Network Insights - Advisor Fabric: demo_fab_1

PSIRTs

Critical PSIRTs: 0 Severe PSIRTs: 42 Moderate PSIRTs: 11

PSIRT Severity by Devices

PSIRT Severity	Number of Devices Affected
Critical	0
Severe	2
Moderate	2

PSIRTs Affecting: Versions

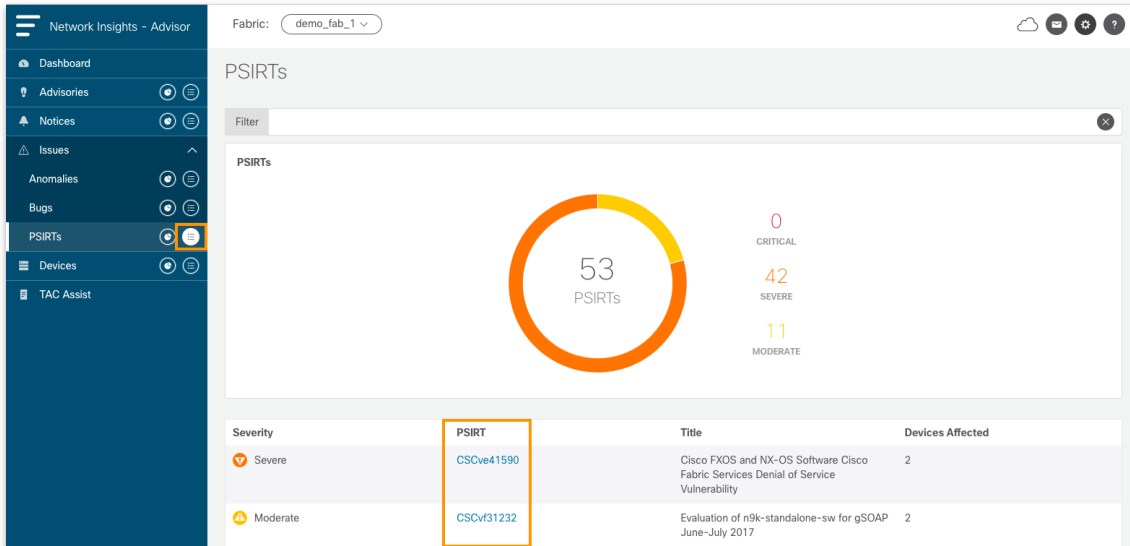
2 Versions

53	7.0(3)I4(1)
53	7.0(3)I7(1)

3. [PSIRT (PSIRTs)] > [参照 (Browse)] をクリックします。

[PSIRT (PSIRTs)] 列で次の手順を実行します。

4. [CSCvh75886] リンクをクリックします。



5. ページを上スクロールして [アドバイザリ (Advisory)] パネルを表示します。

6. [アドバイザリの表示 (View Advisory)] をクリックします。

7. 表示された情報を確認します。

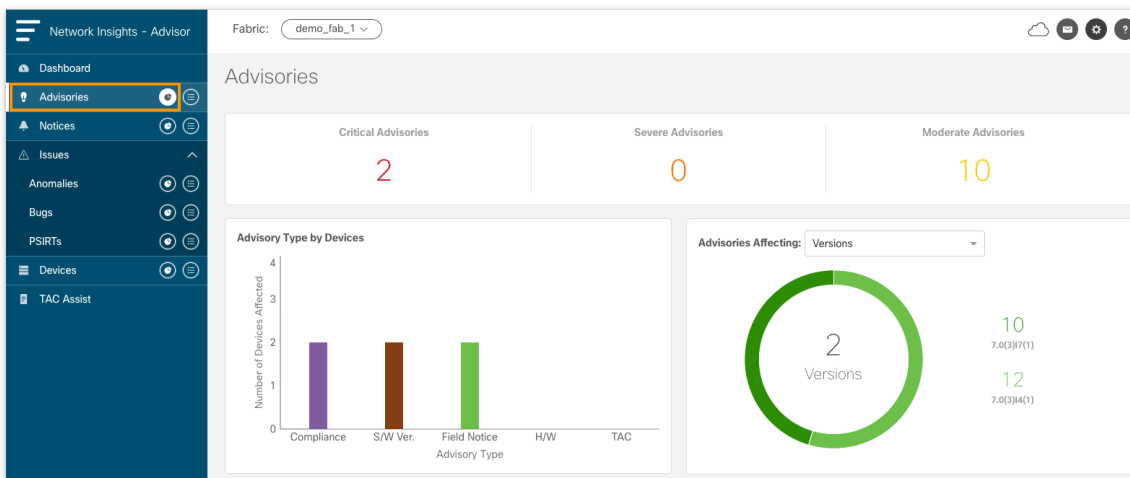
8. ページを閉じます。

アドバイザリ

左側のメニューで次の手順を実行します。

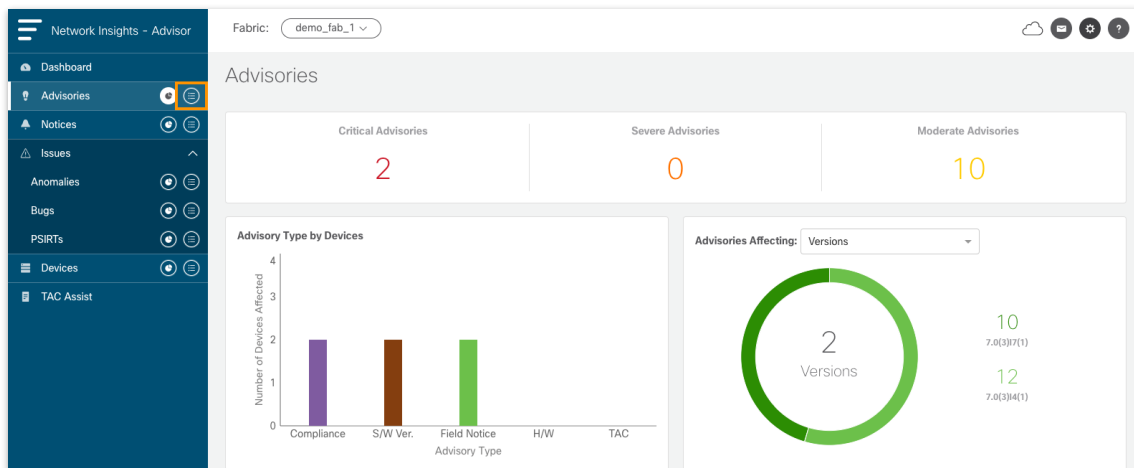
1. [アドバイザリ (Advisories)] をクリックします。

2. 表示された情報を確認します。



3. [アドバイザリ (Advisories)] > [参照 (Browse)] をクリックします。

4. 表示された情報を確認します。



5. ページを上スクロールして [アドバイザリ (Advisories)] テーブルを表示します。

6. 右矢印をクリックして、[アドバイザリ (Advisories)] テーブルの 2 ページ目を表示します。

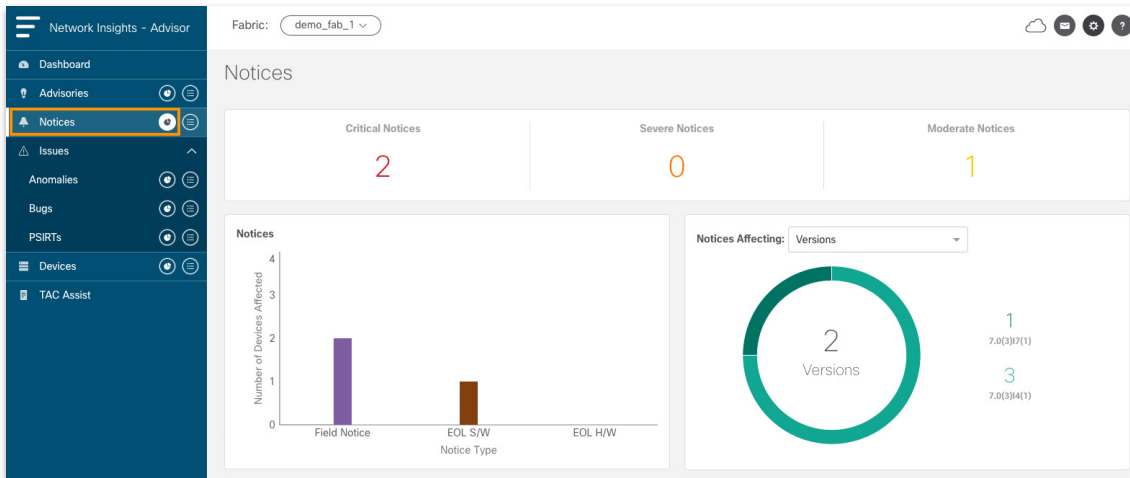
Severity	Last Updated Time	Type	Title	Devices Affected
Moderate	Feb 24, 2020 04:16 pm	Compliance	Use AAA for authentication	2
Moderate	Feb 24, 2020 04:16 pm	Compliance	Set the EXEC timeout appropriately	2
Moderate	Feb 24, 2020 04:16 pm	Compliance	Use AAA (TACACS+) for command authorization	2
Moderate	Feb 24, 2020 04:16 pm	Compliance	Configure SNMPv2 communities and apply ACLs	2
Moderate	Feb 24, 2020 04:16 pm	Compliance	Use AAA for accounting	2
Moderate	Feb 24, 2020 04:16 pm	Compliance	Enable strong password checking	2
Moderate	Feb 24, 2020 04:16 pm	Compliance	Configure NTP authentication	2
Moderate	Feb 24, 2020 04:16 pm	Compliance	Disable IP source routing	2
Moderate	Feb 24, 2020 04:14 pm	S/W Ver.	Recommended version is 7.0(3)7(6)	2
Critical	Feb 19, 2020 07:42 pm	Field Notice	Field Notice : FN70320	2

Page 1 of 2 Objects Per Page 10 rows Displaying Objects 1 - 10 of 12

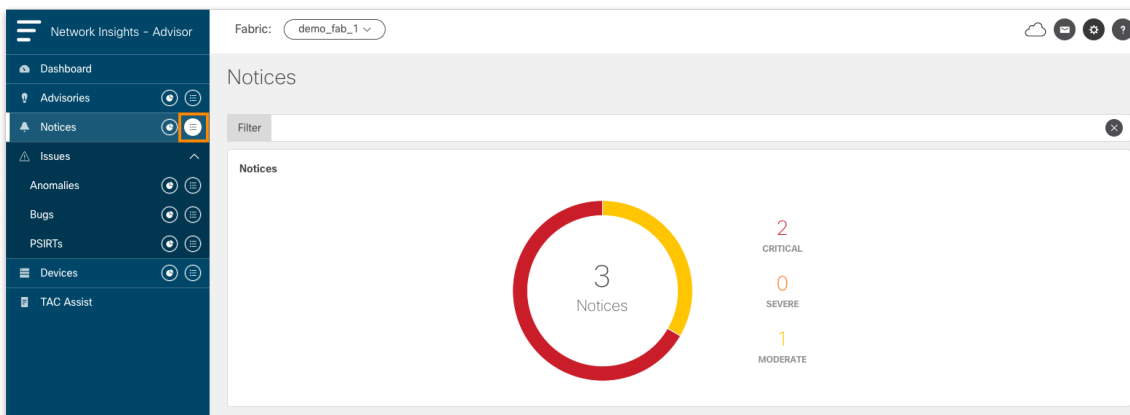
通知

左側のメニューで次の手順を実行します。

1. [通知 (Notify)]をクリックします。
2. 表示された情報を確認します。



3. [通知 (Notify)] > [参照 (Browse)]をクリックします。
4. 表示された情報を確認します。

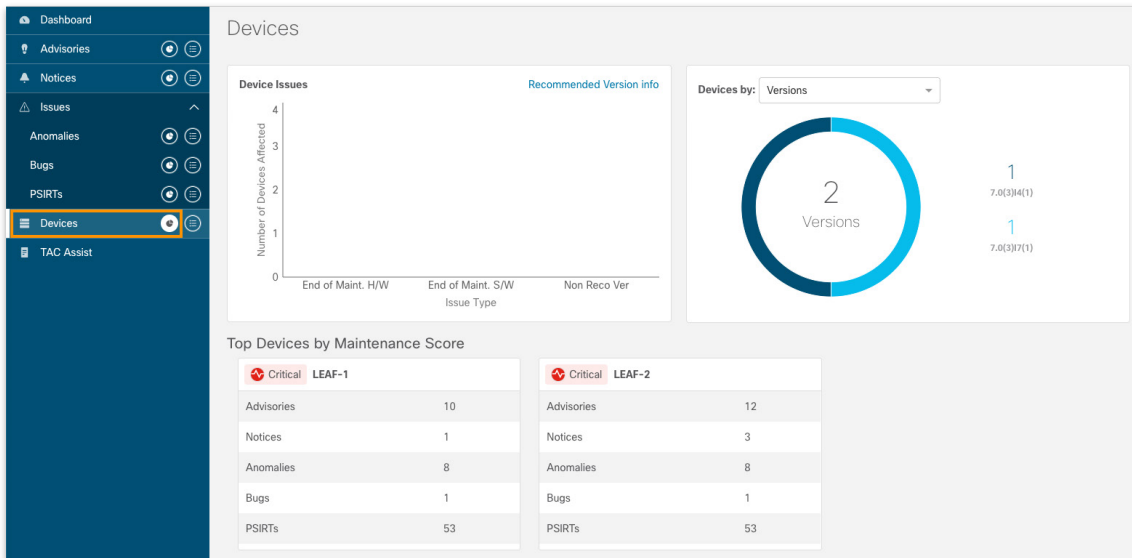


5. ページを上スクロールしてテーブルを表示します。
[タイトル (Title)]列で次の手順を実行します。
6. [フィールド通知 : FN - 70016... (Field Notice: FN - 70016 ...)]で始まるリンクをクリックします。
7. [アドバイザリの表示 (View Advisory)]をクリックします。
8. 表示された情報を確認します。
9. ページを閉じます。

デバイス

左側のメニューで次の手順を実行します。

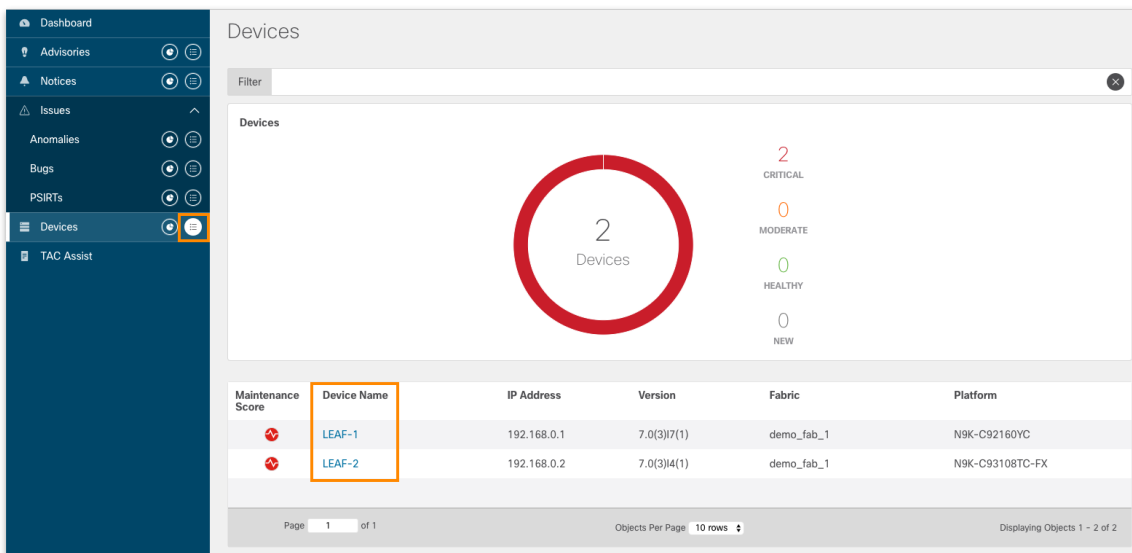
1. [デバイス (Devices)]をクリックします。
2. 表示された情報を確認します。



3. [デバイス (Devices)] > [参照 (Browse)]をクリックします。

[デバイス名 (Devices Name)]列で次の手順を実行します。

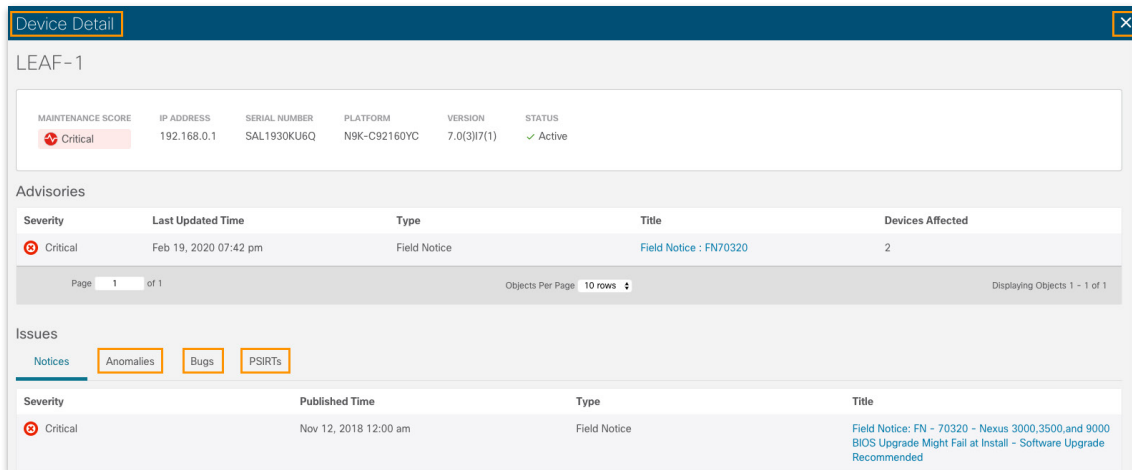
4. [LEAF-1]リンクをクリックします。



5. ページを上スクロールしてタブ付きのパネルを表示します ([通知 (Notices)]が選択されている状態)。

6. [異常 (Anomalies)]をクリックします。

7. 表示された情報を確認します。
8. [バグ (Bug)]をクリックします。
9. 表示された情報を確認します。
10. [PSIRT (PSIRTs)]をクリックします。

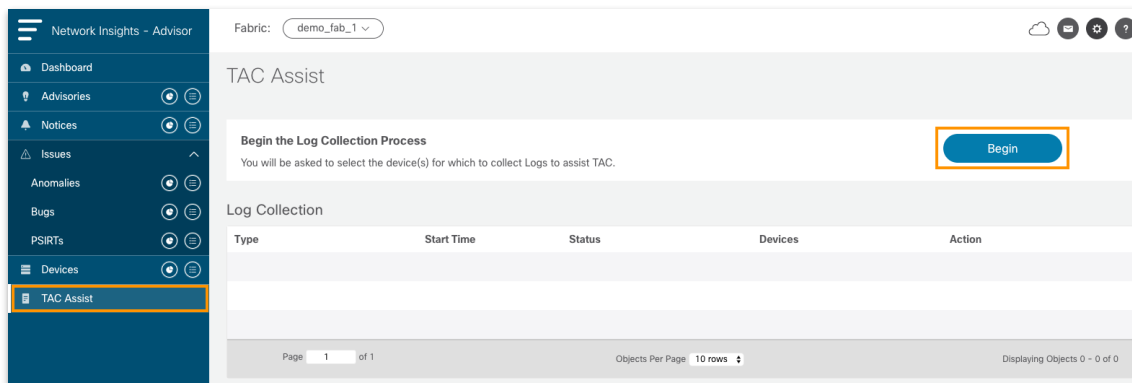


11. ページを閉じます。

TAC アシスト

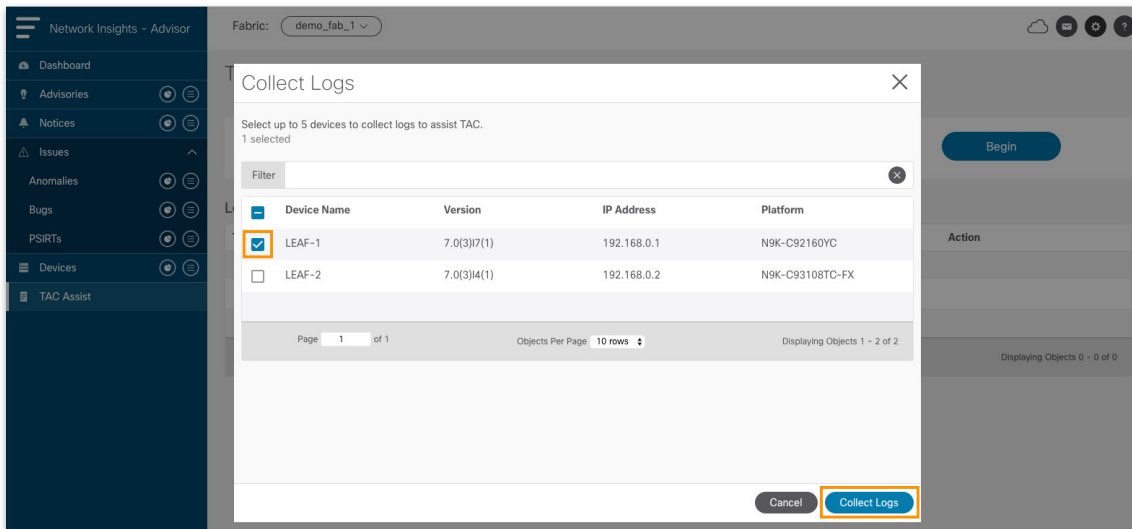
左側のメニューで次の手順を実行します。

1. [TAC アシスト (TAC Assist)]をクリックします。
2. [開始 (Begin)]をクリックします。



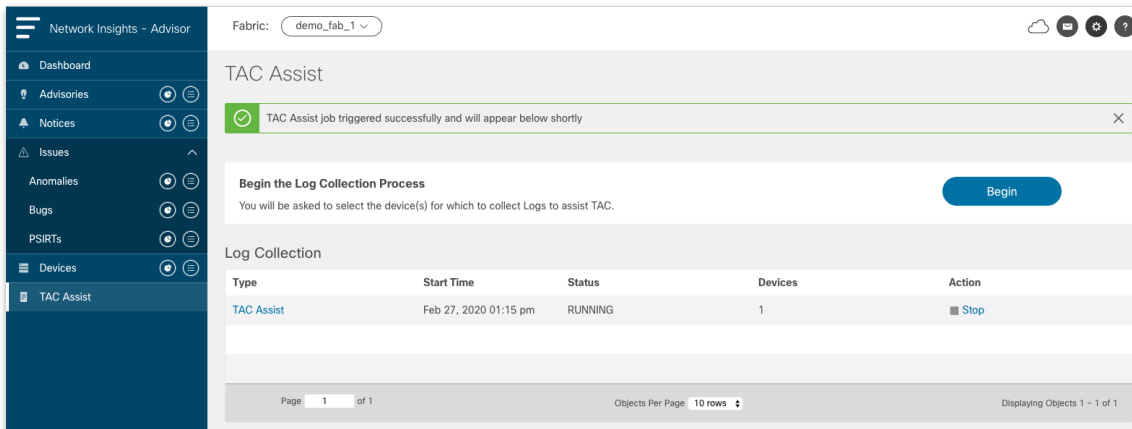
3. [LEAF-1] チェックボックスをオンにします。

4. [ログの収集 (Collect Logs)] をクリックします。



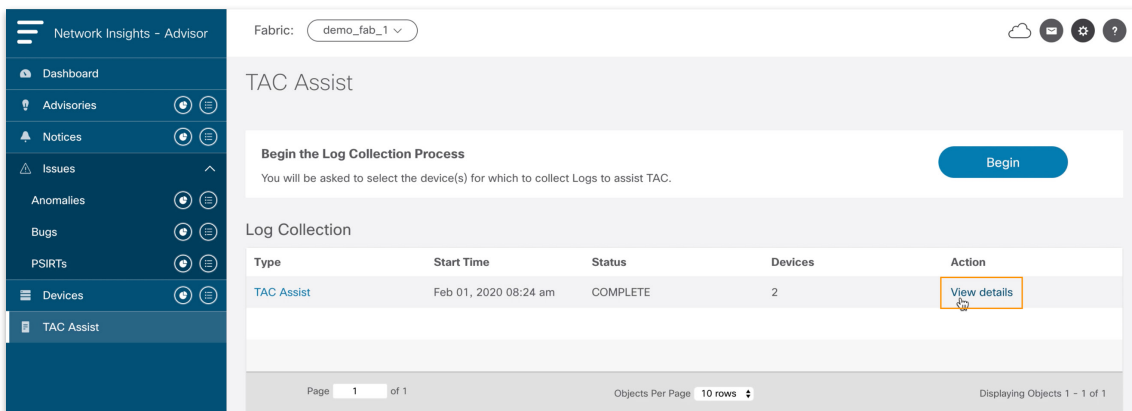
ログ収集プロセスが実行されます。

注 : DCNM が共有されているため、このプロセスにはしばらく時間がかかることがあります。

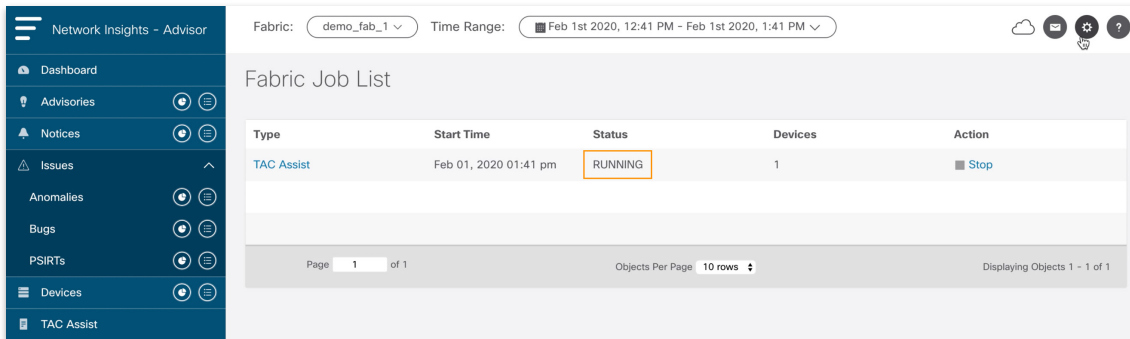


ログ収集プロセスが完了します。

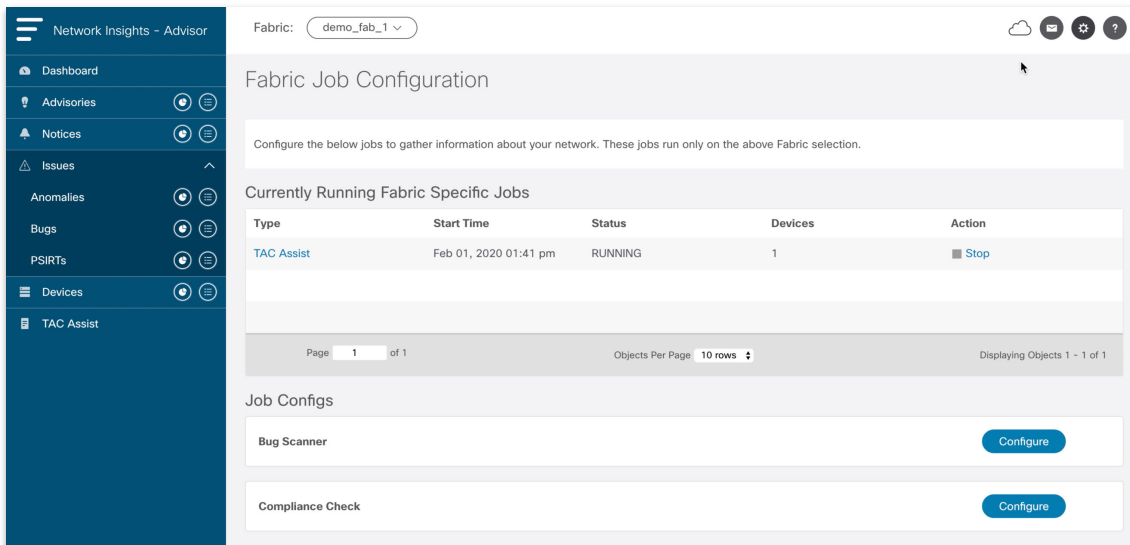
5. [詳細を表示 (View details)] リンクをクリックします。



6. 表示された情報を確認します。
7. ページを閉じます。
8. [設定 (Configuration)] をクリックします。
9. [設定 (Configuration)] ドロップダウンから、[ファブリックジョブリスト (Fabric Job List)] を選択します。



10. [設定 (Configuration)] をクリックします。
11. [設定 (Configuration)] ドロップダウンから、[ファブリックジョブ設定 (Fabric Job Configuration)] を選択します。



シナリオ 2. Network Insights Resources

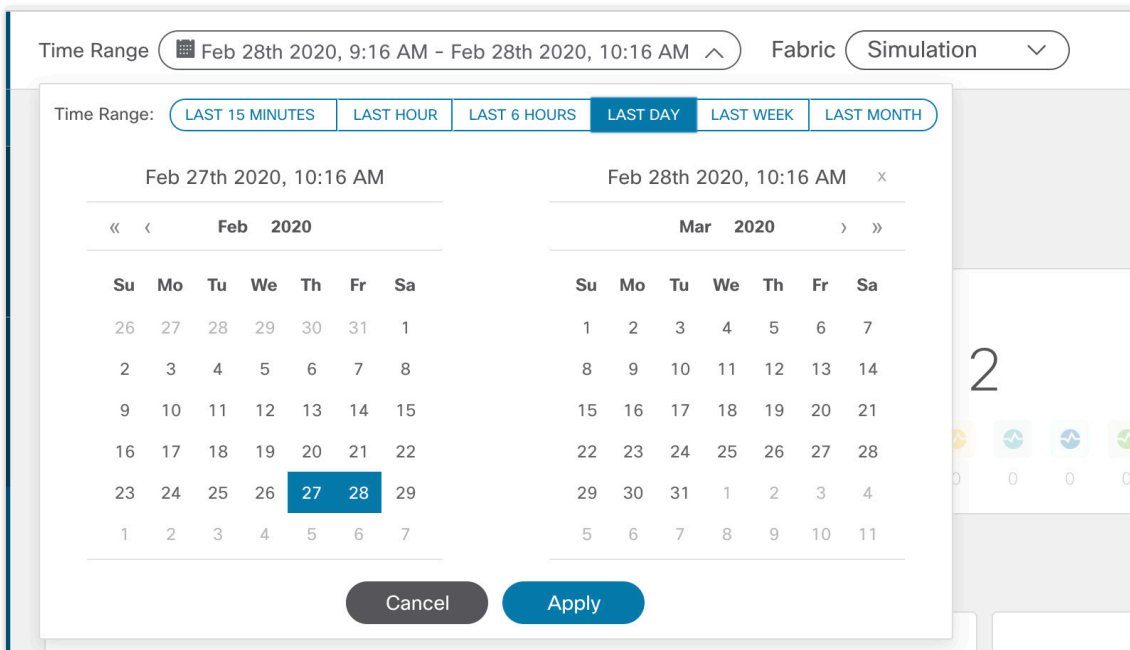
左側のメニューで次の手順を実行します。

1. [アプリケーション (Application)] をクリックします。
2. [Network Insights Resources] をクリックします。



[ダッシュボード (Dashboard)] で次の手順を実行します。

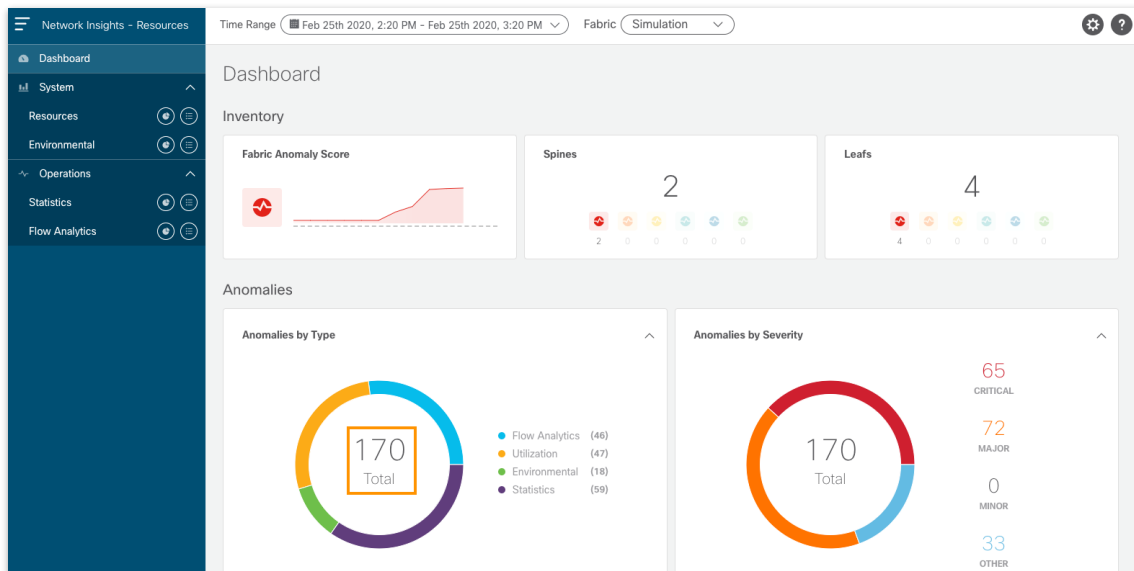
3. [時間範囲 (Time Range)] ドロップダウンから、[過去 1 日間 (Last Day)] を選択します。
4. [適用 (Apply)] をクリックします。



異常

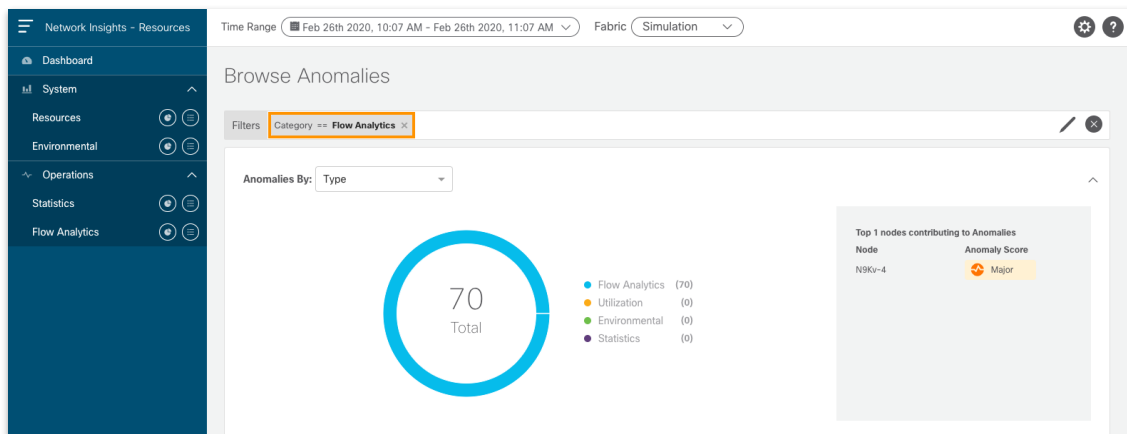
[タイプ別の異常 (Anomalies by Type)] タイルで次の手順を実行します。

1. 円の中の [合計 (Total)] をクリックします。



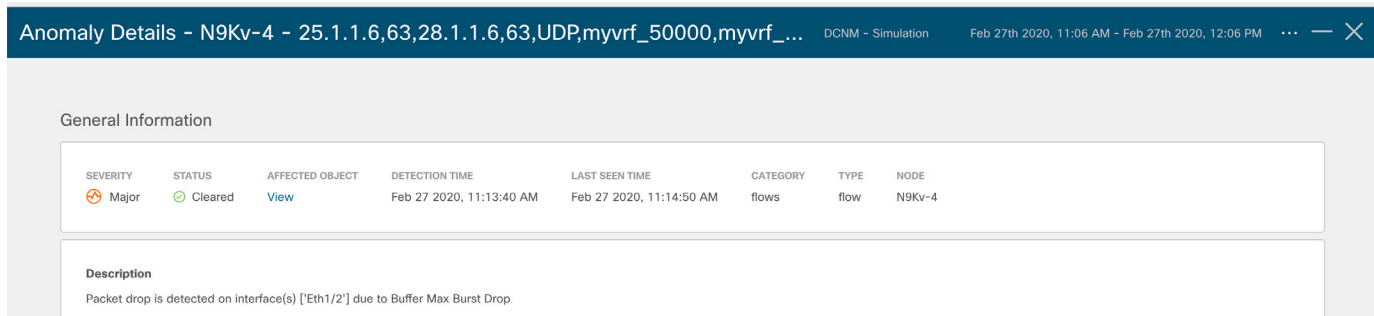
フロー分析

1. [フロー分析 (Flow Analytics)] をクリックします。



2. ページを上スクロールして [異常の合計 (Total Anomalies)] テーブルを表示します。
3. 異常の 1 つをダブルクリックします。

4. [表示 (View)] をクリックします。



5. ページを上スクロールして、表示された情報を確認します。

6. [完了 (Done)] をクリックします。

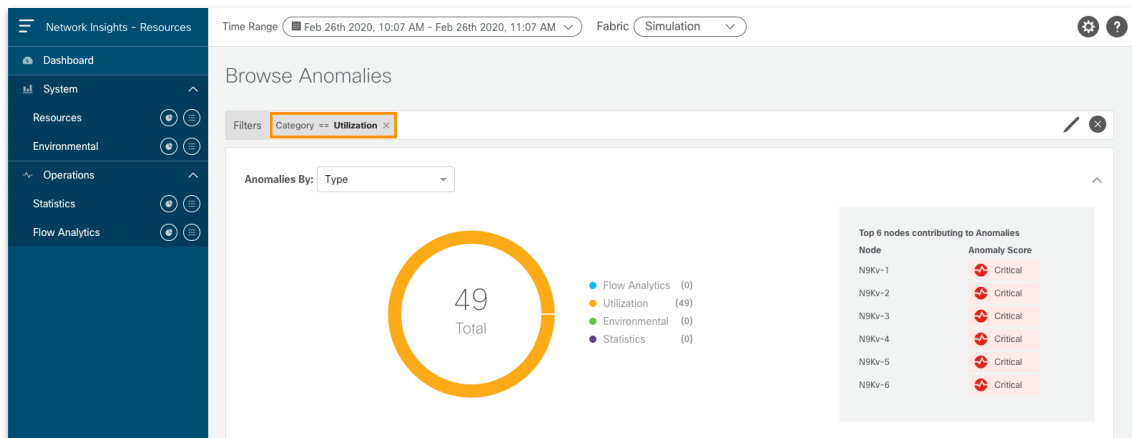
7. [完了 (Done)] をクリックします。

8. ページを下スクロールして [フィルタ (Filters)] を表示します。

9. [フロー分析 (Flow Analytics)] フィルタを削除します。

使用率

10. [使用率 (Utilization)] をクリックします。



11. ページを上スクロールして [異常の合計 (Total Anomalies)] テーブルを表示します。

12. 異常の 1 つをダブルクリックします。

13. [表示 (View)] をクリックします。

14. ページを上スクロールして、表示された情報を確認します。

15. [完了 (Done)] をクリックします。

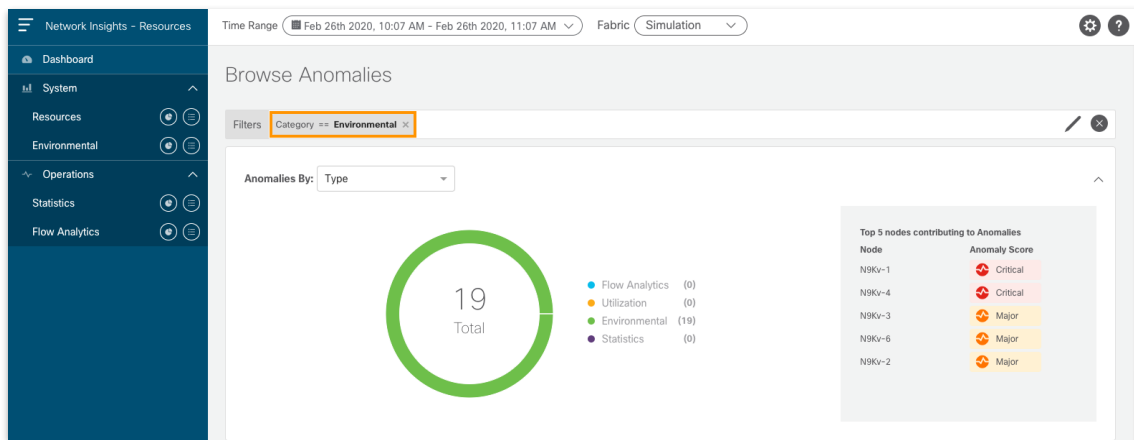
16. [完了 (Done)] をクリックします。

17. ページを下スクロールして [フィルタ (Filters)] を表示します。

18. [使用率 (Utilization)] フィルタを削除します。

環境

1. [環境 (Environmental)] をクリックします。



2. ページを上スクロールして [異常の合計 (Total Anomalies)] テーブルを表示します。

3. 異常の 1 つをダブルクリックします。

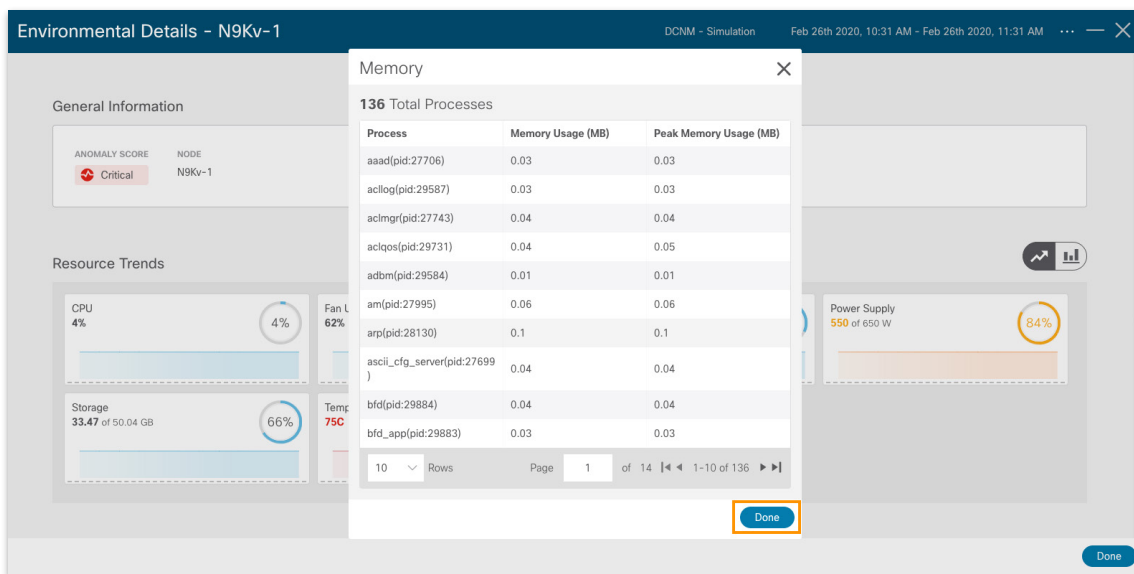
4. [表示 (View)] をクリックします。

メモリ

5. [メモリ (Memory)] をクリックします。

6. プロセスを確認します。

7. [完了 (Done)] をクリックします。



8. [CPU] をクリックします。

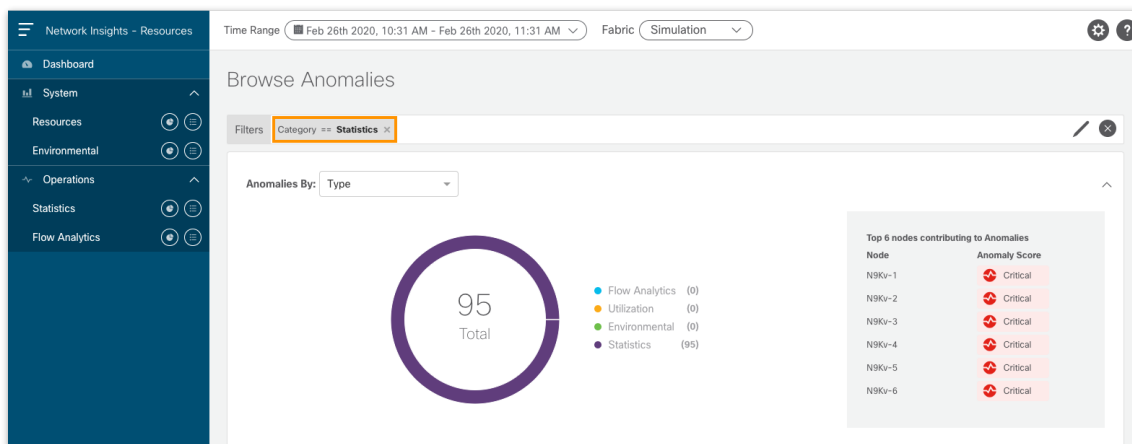
9. プロセスを確認します。

10. [完了 (Done)] をクリックします。

11. [完了 (Done)]をクリックします。
12. [完了 (Done)]をクリックします。
13. ページを下にスクロールして [フィルタ (Filters)]を表示します。
14. [環境 (Environmental)] フィルタを削除します。

統計情報

1. [統計情報 (Statistics)]をクリックします。

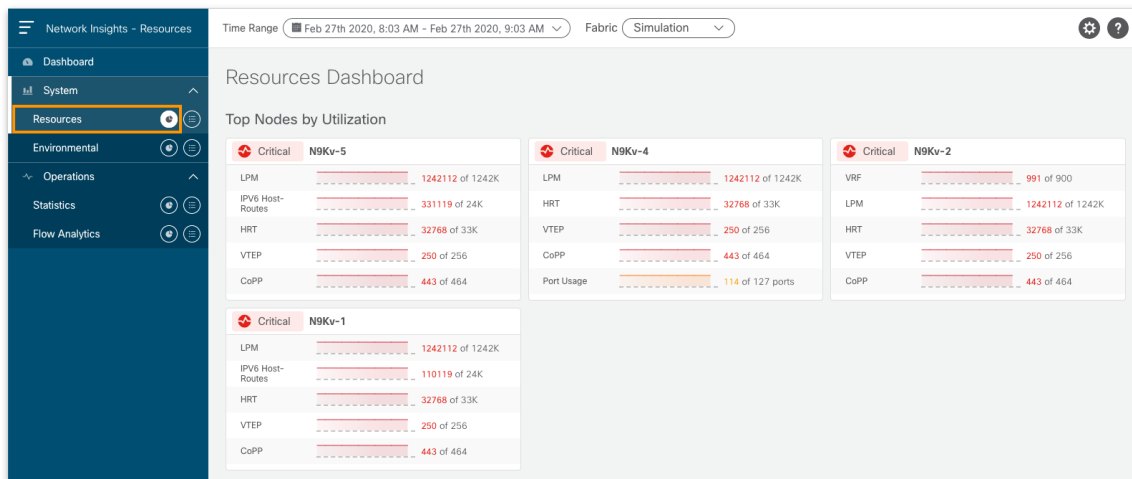


2. 異常の 1 つをダブルクリックします。
3. [表示 (View)]をクリックします。
4. ページを上スクロールして、表示された情報を確認します。
5. [完了 (Done)]をクリックします。
6. [完了 (Done)]をクリックします。
7. [統計情報 (Statistics)] フィルタを削除します。

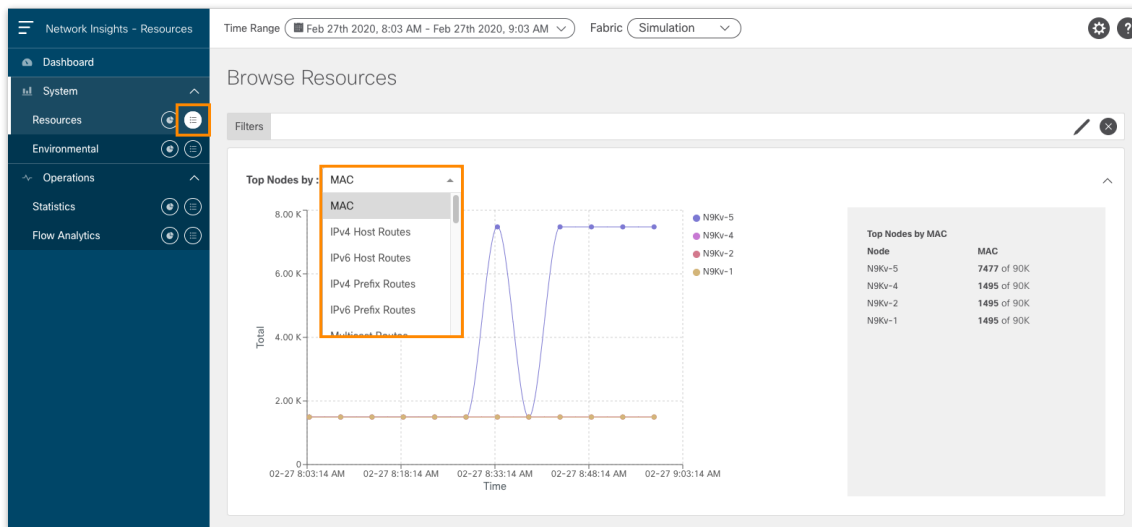
リソース

左側のメニューで次の手順を実行します。

1. [リソース (Resources)]をクリックします。
2. このページの情報を確認します。



3. [リソースの参照 (Resources Browse)]をクリックします。
4. [上位ノード (Top Node by)]ドロップダウンをクリックし、オプションを確認します。



5. ページを上スクロールしてタブ付きのパネルを表示します ([運用リソース (Operational Resources)]が選択されている状態)。
6. 表示された情報を確認します。
7. [設定リソース (Configuration Resources)]をクリックします。
8. 表示された情報を確認します。

9. [ハードウェアリソース (Hardware Resources)] をクリックします。

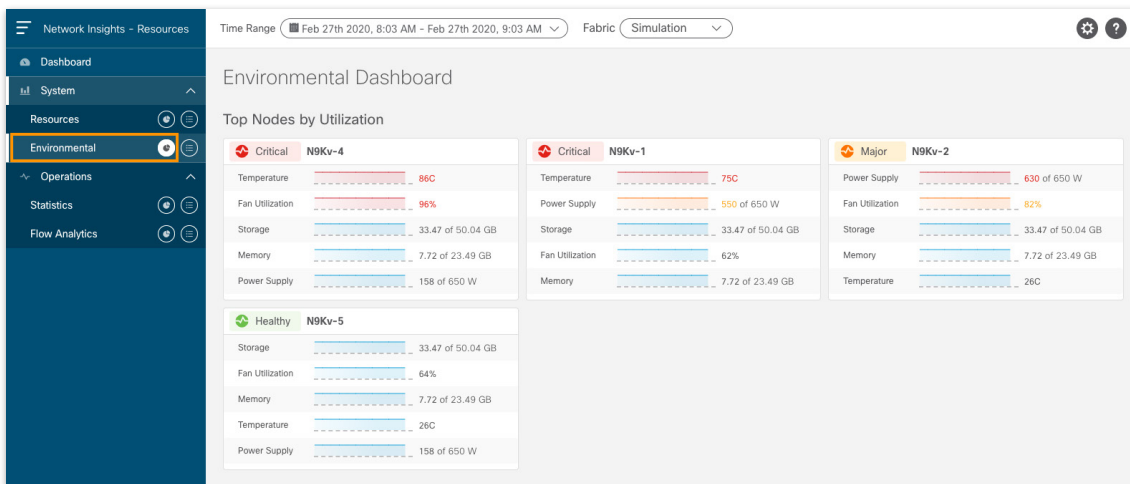
10. 表示された情報を確認します。

環境

左側のメニューで次の手順を実行します。

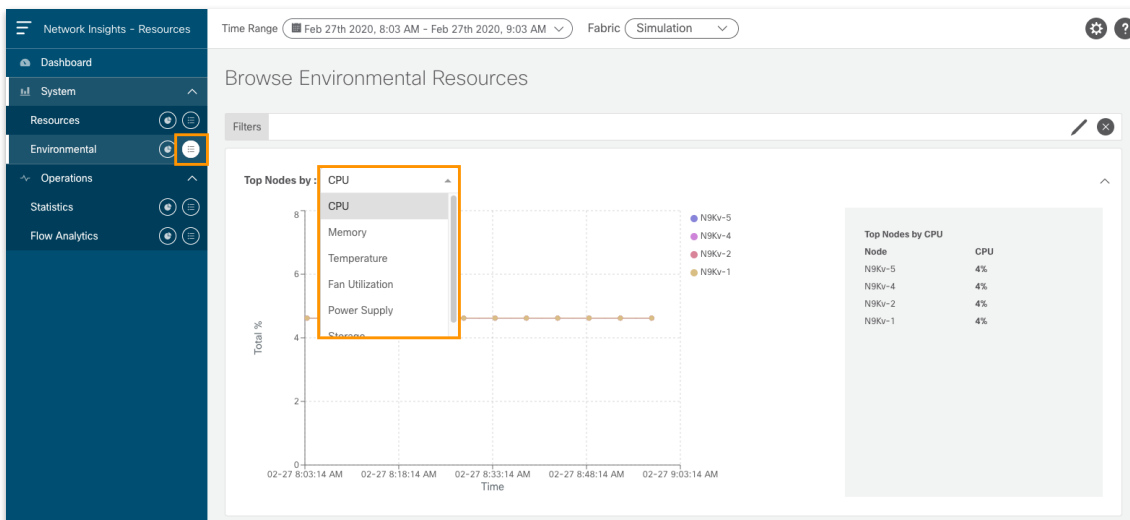
1. [環境 (Environmental)] をクリックします。

2. 表示された情報を確認します。



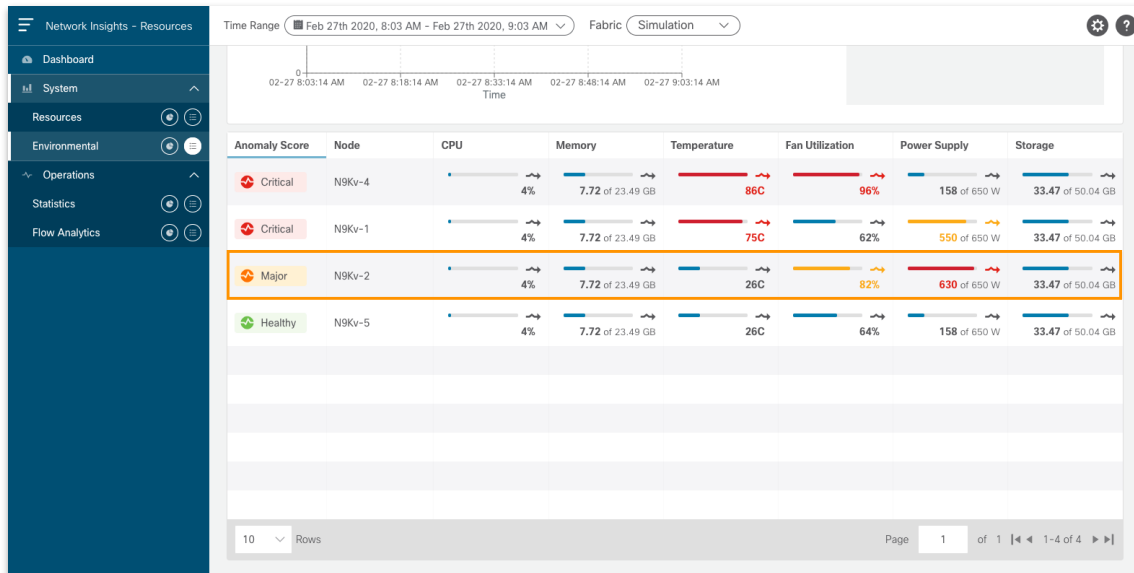
3. [環境の参照 (Environmental Browse)] をクリックします。

4. [上位ノード (Top Node by)] ドロップダウンをクリックし、オプションを確認します。



5. ページを上スクロールしてタブ付きのパネルを表示します ([異常スコア (Anomaly Score)] が選択されている状態)。

6. 任意の行をダブルクリックします。



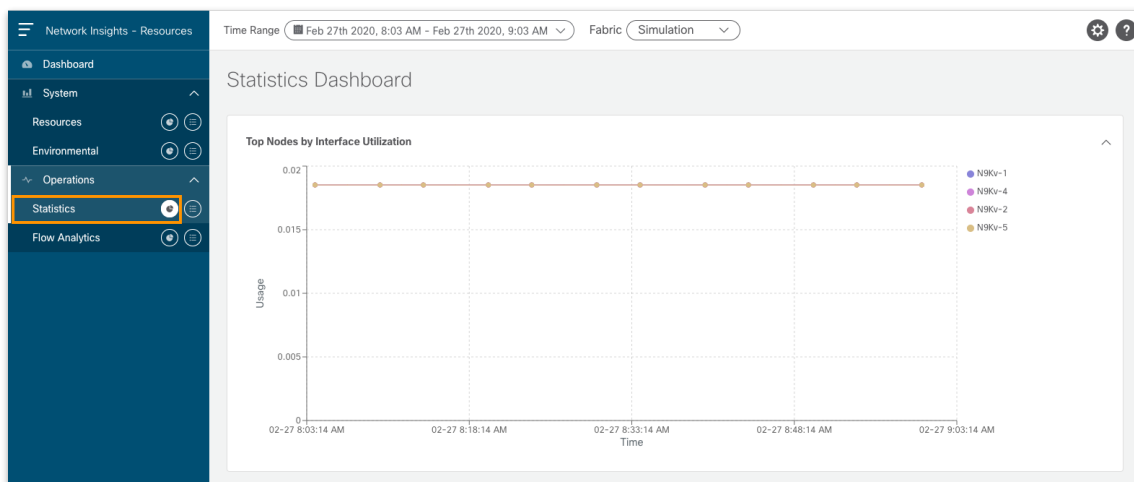
7. ページを上スクロールして、表示された情報を確認します。

8. [完了 (Done)] をクリックします。

統計情報

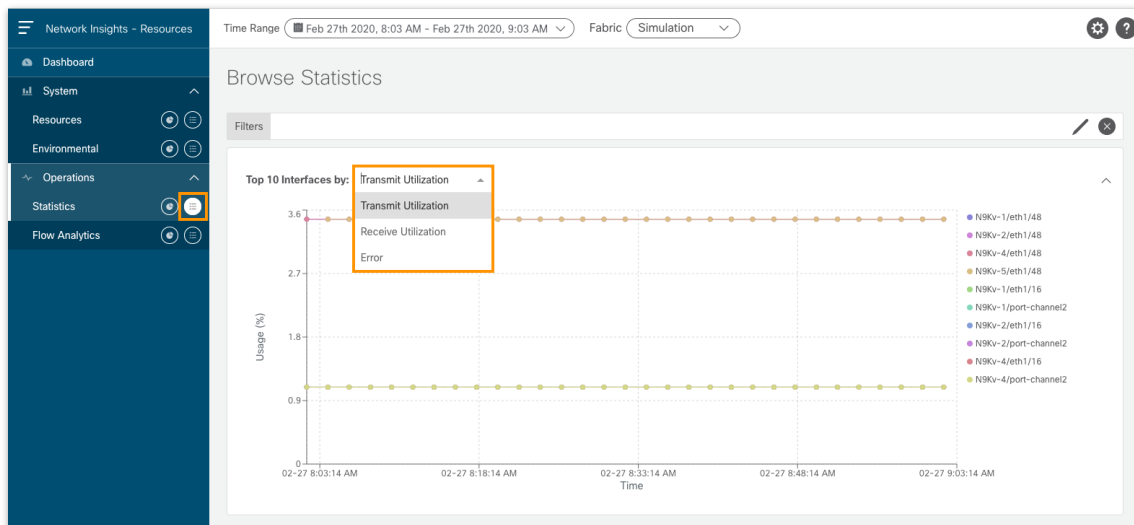
左側のメニューで次の手順を実行します。

1. [統計情報 (Statistics)] をクリックします。
2. 表示された情報を確認します。



3. [統計情報の参照 (Statistics Browse)] をクリックします。

- [上位 10 インターフェイス (Top 10 Interfaces by)] ドロップダウンをクリックし、[送信使用率 (Transmit Utilization)] を選択します。



- ページを上スクロールしてタブ付きのパネルを表示します ([インターフェイス統計情報 (Interface Statistics)] が選択されている状態)。

タブ付きサブパネルで次の手順を実行します ([異常スコア (Anomaly Score)] が選択されている状態)。

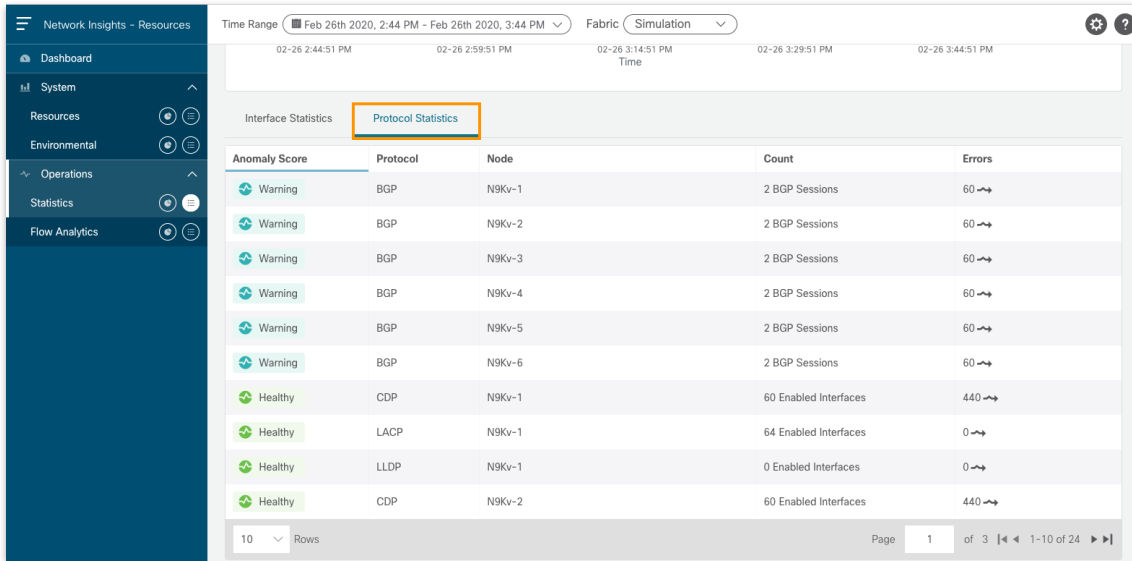
- [インターフェイス (Interface)] をクリックします。

- 表示された情報を確認します。

Anomaly Score	Interface	Interface Type	Node	Receive Utilization	Transmit Utilization	Errors
Healthy	eth1/1	physical	N9Kv-1	0.1%	0%	130
Healthy	eth1/1	physical	N9Kv-2	0.1%	0%	130
Healthy	eth1/1	physical	N9Kv-3	0.1%	0%	130
Healthy	eth1/1	physical	N9Kv-4	0.1%	0%	130
Healthy	eth1/1	physical	N9Kv-5	0.1%	0%	130
Healthy	eth1/1	physical	N9Kv-6	0.1%	0%	130
Healthy	eth1/2	physical	N9Kv-1	0%	0%	0
Healthy	eth1/2	physical	N9Kv-2	0%	0%	0
Healthy	eth1/2	physical	N9Kv-3	0%	0%	0
Healthy	eth1/2	physical	N9Kv-4	0%	0%	0

- [プロトコル統計情報 (Protocol Statistics)] をクリックします。

9. 表示された情報を確認します。



Anomaly Score	Protocol	Node	Count	Errors
Warning	BGP	N9Kv-1	2 BGP Sessions	60 →
Warning	BGP	N9Kv-2	2 BGP Sessions	60 →
Warning	BGP	N9Kv-3	2 BGP Sessions	60 →
Warning	BGP	N9Kv-4	2 BGP Sessions	60 →
Warning	BGP	N9Kv-5	2 BGP Sessions	60 →
Warning	BGP	N9Kv-6	2 BGP Sessions	60 →
Healthy	CDP	N9Kv-1	60 Enabled Interfaces	440 →
Healthy	LACP	N9Kv-1	64 Enabled Interfaces	0 →
Healthy	LLDP	N9Kv-1	0 Enabled Interfaces	0 →
Healthy	CDP	N9Kv-2	60 Enabled Interfaces	440 →

10. 任意の行をダブルクリックします。

11. 表示された情報を確認します。

12. [完了 (Done)]をクリックします。

13. [インターフェイス統計情報 (Interface Statistics)]をクリックします。

14. 任意の行をダブルクリックします。

15. ページを上スクロールして、表示された情報を確認します。

16. [完了 (Done)]をクリックします。

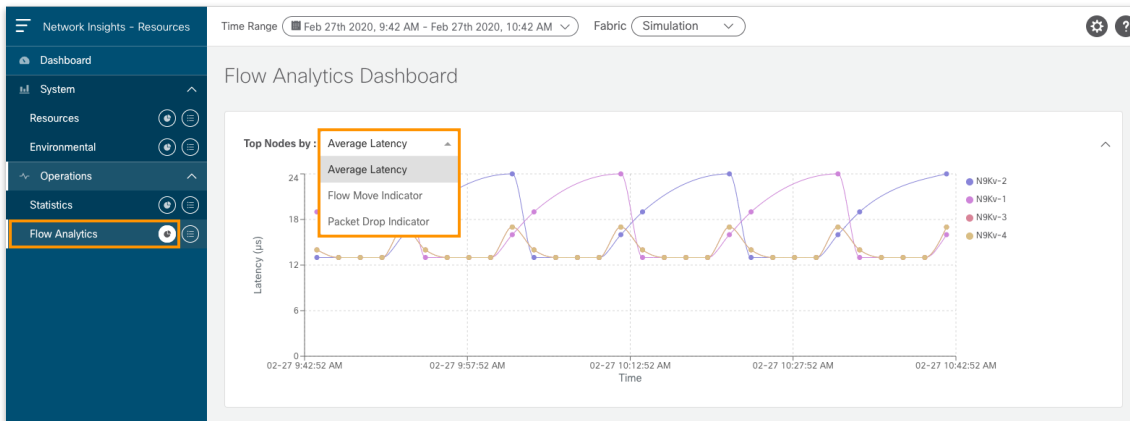
フロー分析

左側のメニューで次の手順を実行します。

1. [フロー分析 (Flow Analytics)]をクリックします。

2. 表示された情報を確認します。

3. [上位ノード (Top Node by)]ドロップダウンをクリックし、オプションを確認します。



4. [フロー分析の参照 (Flow Analytics Browse)]をクリックします。

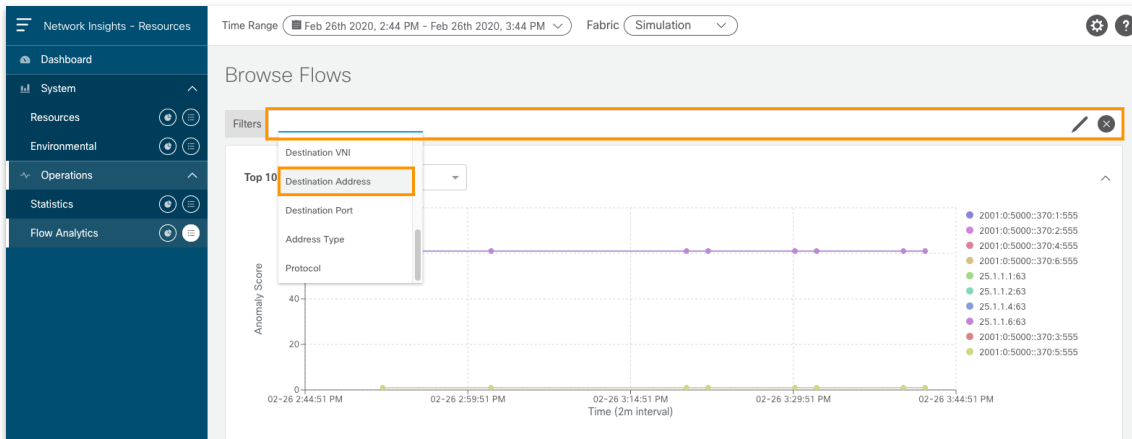
5. [上位 10 フロー (Top 10 flows by)]ドロップダウンをクリックし、オプションを確認します。



6. ページを上スクロールして、表示された情報を確認します。

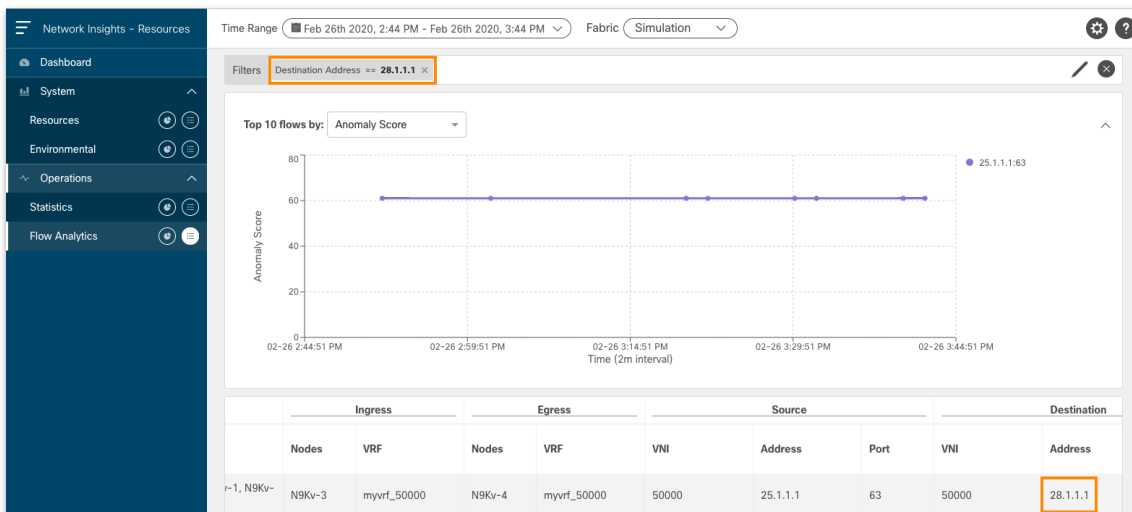
フィルタ

1. [フィルタ (Filters)]ドロップダウンをクリックし、[宛先アドレス (Destination Address)]を選択します。
2. [=]をクリックします。
3. 「28.1.1.1」を入力します。



4. ページを左にスクロールして、[宛先 (Destination)] 列を表示します。

5. (テーブル内の) [アドレス (Address)] の値が (フィルタ内の) [アドレス (Address)] の値に対応していることを確認します。



6. 行をダブルクリックします。

7. ページを上スクロールして、表示された情報を確認します。

8. [完了 (Done)] をクリックします。



次に必要な作業

詳細については、関連するデモンストレーションを参照してください。

- [Cisco ACI with AppDynamics v1](#) [英語]
- [Getting Started with Cisco ACI v1](#) [英語]
- [Cisco Network Assurance Engine 4.1 v1](#) [英語]

© 2020 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2020 年 5 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



お問い合わせ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>