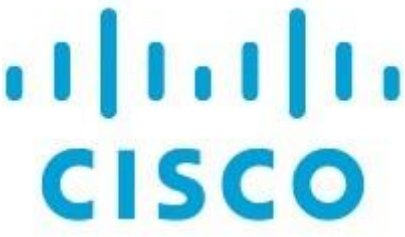


Cisco Nexus Dashboard Insights ユーザーガイド、リリース 6.1.3 - Cisco Application Centric Infrastructure 向け

目次

初版: 2022-08-15

最終更新日：2023-01-26

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

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』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco 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カリフォルニア大学バークレイ校（UCB）によるパブリック ドメインバージョンの一部として、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。

シスコおよびシスコのロゴは、シスコ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については、http://www.cisco.com/go/trademarks を参照してください。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シップ関係が存在することを意味するものではありません。(1110R)

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。

表 1. 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
このマニュアルの初版。	これはこのマニュアルの初版です。	6.1.3	該当なし

このドキュメントは、Cisco Nexus Dashboard Insights のGUI およびインターネット上の www.cisco.com から入手できます。本書の最新バージョンに関しては、「文書」の「Cisco Nexus Dashboard Insights」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

Cisco Nexus Dashboard Insights について

Cisco Nexus Dashboard Insights (Nexus Dashboard Insights)は、リアルタイムの監視および分析サービスです。

Cisco Nexus Dashboard Insights のコンポーネント

Cisco Nexus Dashboard Insights（Nexus Dashboard）は、データセンターのネットワークを監視し、対処可能な問題を特定して、可用性を維持し、突発的な停止回数を削減します。Nexus Dashboard Insights はお客様のネットワークの状況を把握することで、可用性を維持し、アップタイムに影響を与える可能性がある潜在的な問題についてアラートを出すことに重点を置いた、プロアクティブなアドバイスを提供できます。

Nexus Dashboard Insights は、Cisco TAC と連携する際に役立つログ収集機能を提供します。また、シスコのお客様が複数のデバイスのテクニカルサポートを収集し、テクニカルサポートをCisco Intersight Cloudにアップロードする方法を提供します。さらに、Cisco TACチームが特定のデバイスのテクニカルサポートをオンデマンドで収集できるようにします。

ACIサイトは、ACIファブリック全体で構成されます。ACI ファブリックは、APIC ホストと、APIC コントローラによって制御されるすべてのリーフ スイッチとスパイン スイッチで構成されます。すべてのネットワークノード(APICコントローラ、リーフスイッチとスパインスイッチ(ボーダーリーフスイッチとボーダースパインスイッチを含む))は、サイトの一部として一緒に分析されます。サイトグループは、単一のサイトまたは複数のサイトを含むことができる論理エンティティです。

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

- [Explore] -
  使いやすい自然言語クエリ形式でアセットとそのオブジェクトの関連付けを検出できます。
- [変更前分析] -
  意図した変更をモデル化し、その変更で目的の結果が生成されるかどうかを確認できます。
- [サイトグループ構成] - フローの構成と、ソフトウェア テレメトリおよびフロー テレメトリ データを収集するジョブのスケジュールを設定します。
  - [バグスキャン] -
    選択したサイトに対して実行されるオンデマンドのバグスキャンを設定、スケジュー

ル、および実行するためのアクセスを提供します。バグスキャンでは、サイトの特定のノードにとってクリティカルなシステム異常とアラートが生成されます。

- [アシュアランス分析] - リアルタイムでアシュアランスを提供します。サイトグループ内のサイトのアシュアランス分析では、データ収集、モデルの生成、および結果の生成は同時に実行されます。
- [データのエクスポート] - 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。
- [フロー] - Nexus Dashboard Insightsで有効になっているサイトのフロー設定ルールを管理します。
- [マイクロバースト] - Nexus Dashboard Insights はインターフェイスレベルでのマイクロバーストの数に基づいて異常を報告します。
- [アラートルール] - 基準に一致する新たに検出された異常をすべて承認し、異常の内容に応じて異常スコアを調整できます。
- [コンプライアンス] - セキュリティ ポリシーとコンプライアンス チェックへの継続的なコンプライアンスを実現できます。
- [収集ステータス] - サポートされている機能とサポートされていない機能について、ノードの機能とノードの収集ステータスを表示します。

- [サードパーティの統合] - AppDynamics コントローラを NexusNexus Dashboard Insights にオンボードするためのアクセスを提供します。
- [データのエクスポート] - Nexus Dashboard Insights から収集したデータを Kafka Exporter 経由でストリーミングし、データの概要を電子メールで送信します。
- [ノード] - リソース使用率、環境、統計情報、エンドポイント、およびフローに基づいてノードの動作を表示するさまざまな方法を提供します。
- [アラートの分析] - ネットワークに適用可能なアドバイザリ、通知、PSIRT、ハードウェア、ソフトウェア、およびハードニング チェック アドバイザリの合計にアクセスします。
  - [異常] - 異常は、リソース使用率、環境の問題、インターフェイスおよびルーティングプロトコルの問題、フロー、エンドポイント、イベント、およびアシュアランス分析、コンプライアンス、変更分析、静的分析のためのサイトの追加とファイルのアップロードに対して発生した異常で構成されます。
  - [アドバイザリ] - アドバイザリは、Field Notice、ソフトウェアとハードウェアのEOL/EOS、ノードレベルでのPSIRT、およびコンプライアンスが原因の関連する影響で構成されます。
    - [Field Notice] - スイッチのハードウェアおよびソフトウェアのライフサイクル終了通知などを通知します。

        - [PSIRT] - Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）の通知には、ネットワーク内のスイッチハードウェアおよびソフトウェアに関する 3 つのレベルのアドバイザリ重大度が表示されます。

- トラブルシュート
    - [差分分析] - 差分分析を使用すると、ポリシー、実行時の状態、および 2 つのスナップショット間のネットワークの正常性の違いを分析できます。
    - [ログコレクタ] - ネットワーク内のデバイスのログを収集して、Cisco Intersight Cloud にアップロードします。Cisco TAC がサイト上にあるユーザー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 からログをプルできるようにします。
- 変更管理
    - [ファームウェア アップデート分析] - この機能は、推奨されるソフトウェアバージョンへのアップグレード パスを提案し、アップグレードの潜在的な影響を判断します。また、アップグレード前後の検証チェックにも役立ちます。
    - [変更前分析] - この機能を使用すると、意図した変更をモデル化し、サイト内の既存の基本スナップショットに対して変更前の分析を実行し、その変更で目的の結果が生成されるかどうかを確認できます。

Cisco Nexus Dashboard へのサイトの追加

次の手順を使用し、GUIを使用してCisco Nexus Dashboardにサイトを追加します。Cisco Nexus Dashboard にインストールされているサービスはすべて、追加されたサイトにアクセスできます。

Cisco Nexus Dashboard ユーザーガイドを参照してください。

はじめる前に

- Cisco Nexus Dashboardをインストールして設定します。
- Cisco Nexus Dashboardにサイトを追加するには、管理者のログイン情報が必要です。
- ファブリック接続を設定します。詳細については、『Cisco Nexus Dashboard User Guide』を参照してください。

手順

1. 管理者権限でCisco Nexus DashboardのGUIにログインします。
2. 左側のナビゲーションウィンドウで、**[サイト（Sites）]** をクリックします。
3. **[サイト（Sites）]** ページで、**[サイトの追加（Add Site）]** をクリックします。
4. **[サイトの追加（Add Site）]** ページで、次の操作を実行します。

a. **[サイトタイプ（Site Type）]** フィールドで、**[ACI]** を選択します。

b. [サイト名]と[ホスト名/IPアドレス]に適切な値を入力します。

c. [ユーザー名]と[パスワード]に値を入力します。

> 管理者権限を使用して、APICのユーザー名とパスワードの値を入力します。サイト名は、Cisco Nexus Dashboard Insights サービスで一意である必要があります。

d. （任意）**[ログイン ドメイン（Login Domain）]** フィールドを空欄のままにすると、サイトのローカル ログインが使用されます。

e. **[インバンド EPG（In-band EPG）]** フィールドに、コントローラからのインバンド EPG 名を入力します。

5. **[追加（Add）]** をクリックして、ノードにサイトを追加します。Cisco Nexus Dashboard にインストールされているサービスはすべて、追加されたサイトにアクセスできます。**[サイト]** ページで新しいサイトを確認できます。
6. **[サイトタイプ（Site Type）]** エリアで、**[追加（Add）]** をクリックします。
7. GUI を使用して Cisco Nexus Dashboard への Cisco Nexus Dashboard Insights のインストールを続行します。

Cisco Nexus Dashboard Insights の設定

次のタスクを使用して、Cisco Nexus Dashboard Insightsの初期セットアップを完了します。

> サイトグループは、単一のサイトまたは複数のサイトを含むことができる論理エンティティです。サイトグループ内のサイトはすべて同じタイプである必要があります。

前提条件

Cisco Nexus Dashboard Insights サービスをインストールしていること。

手順

1. [Cisco Nexus Dashboard Insights サービス（Cisco Nexus Dashboard Insights service）] ページの **[基本構成（Let's Configure the Basics）]** ページにある **[サイトグループのセットアップ（Site Groups Setup）]** エリアで、**[構成（Configure）]** をクリックします。
2. **[サイトグループのセットアップ（Site Groups Setup）]** ページで、**[新しいサイトグループの追加（Add New Site Group）]** をクリックします。
3. **[新しいサイトグループの追加（Add New Site Group）]** ダイアログボックスの **[全般（General）]** エリアにある **[名前（Name）]** フィールドに、サイトグループの名前を入力します。

> サイトグループ名は、Cisco Nexus Dashboard Insightsサービスで一意である必要があります。

4. **[設定（Configuration）]** エリアで **[サイトの追加（Add Site(s)）]** をクリックし、**[エンティティ（Entity）]** エリアで **[メンバーの追加（Add Member）]** をクリックします。
5. **[メンバーの選択（Select Member）]** をクリックします。
6. **[サイトの選択（Select a Site）]**
   ダイアログボックスをクリックして、リストされている検出済みのサイトを表示します。
7. **[新しいサイトグループの追加（Add New Site Group）]** ダイアログボックスの **[構成（Configuration）]** エリアで、**[サイトの追加（Add Site）]** を選択します。
8. 適切なサイトを選択し、**[選択（Select）]** をクリックしてサイトを追加します。
9. **[新しいサイトグループの追加（Add New Site Group）]** ダイアログボックスの **[状態（Status）]**
   フィールドで、適切なステータスを選択してサイトを有効または無効にします。
10. サイトの **[構成（Configure）]** リンクをクリックします。
11. **[構成（Configuration）]** ダイアログボックスの **[全般構成（General Configuration）]** エリアで、
    [ユーザー名（Username）] フィールドと **[パスワード（Password）]**
    フィールドに入力します。

    各操作を実行するには、管理者アカウントを使用する必要があります。APIC のユーザー名とパスワードの値を入力します。

12. 完了したら、サイトのチェックマークをオンにします。**[保存（Save）]** をクリックします。
13. **[サイトグループのセットアップ（Site Groups Setup）]** ページで、**[完了（Done）]**
    をクリックします。

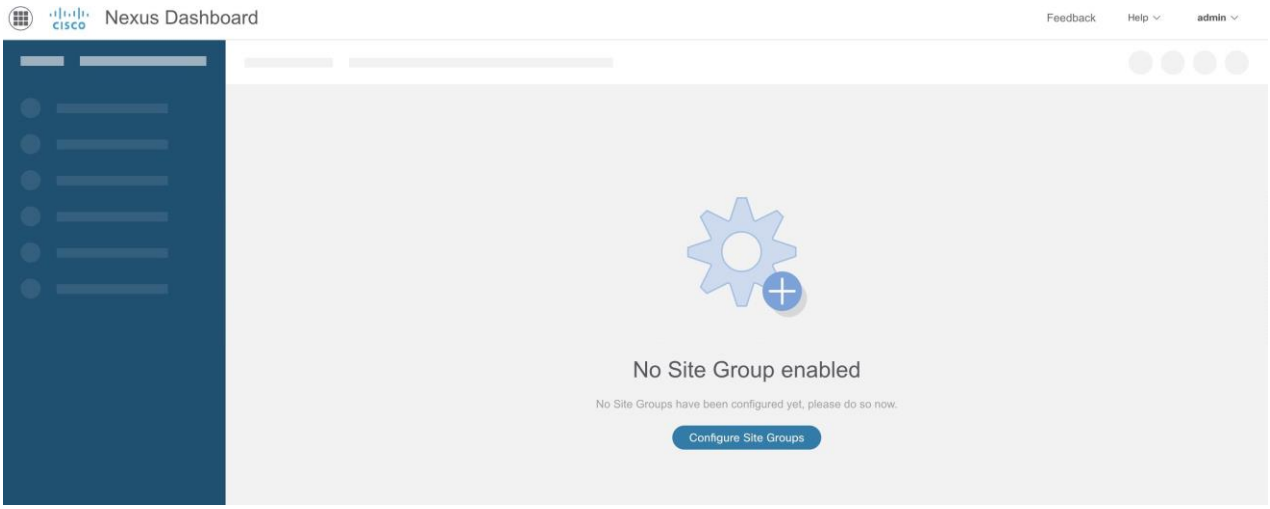
このサイトは、**[サイトグループの構成（Configure Site Group）]** の **[全般（General）]** タブで有効化されています。これで初期セットアップは完了です。

追加の設定を実行する、またはサービス内の他のタスクを

Cisco Nexus Dashboard Insights Day 0 セットアップの基本構成

Cisco Nexus Dashboard Insightsで初めてセットアップを実行する場合は、Cisco Nexus Dashboard Insights の初期セットアップが完了した後に、このセクションの手順を実行してください。

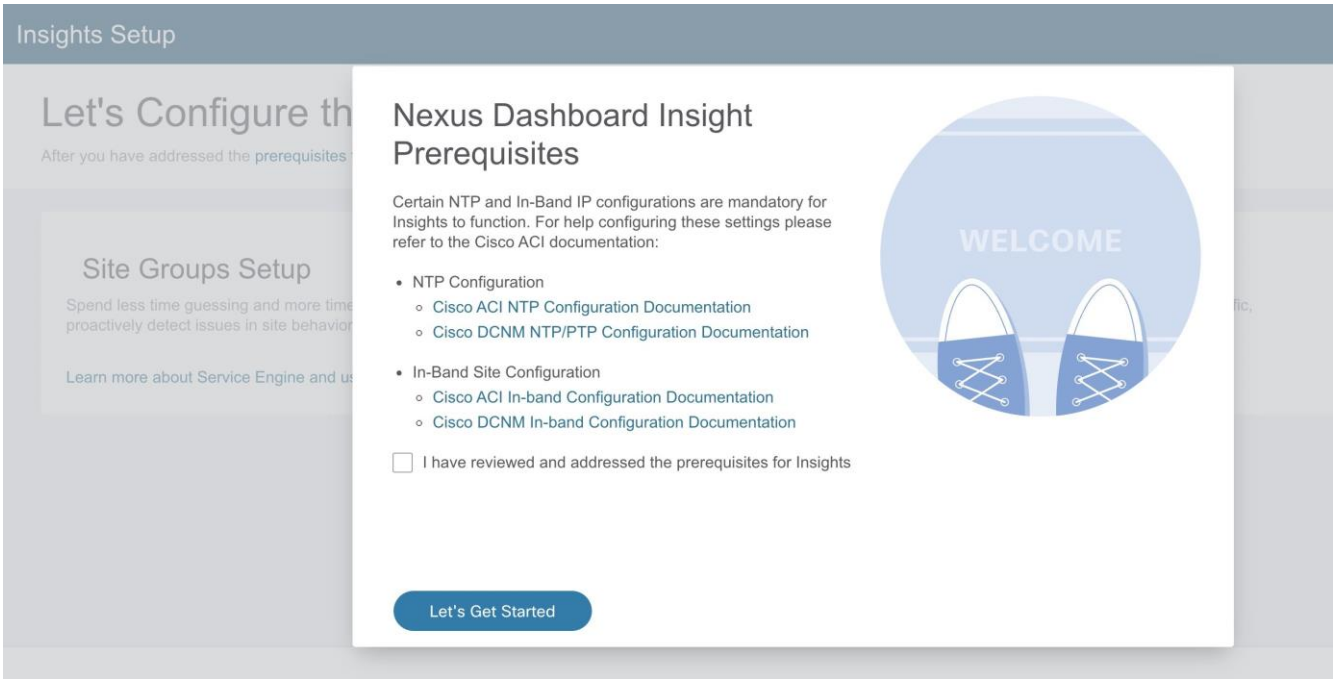
1. Nexus Dashboard Insights を起動したら、**[有効なサイトグループがありません（No Site Groups enabled ）]** 領域で、
   [サイトグループの設定（Configure Site Groups）] をクリックします。



2. **[Nexus Dashboard Insights の前提条件（Nexus Dashboard Insights Prerequisites）]** ダイアログボックスで、必須設定が設定されていることを確認します。必須設定の設定に関するサポートが必要な場合は、ドキュメントリンクを参照してください。

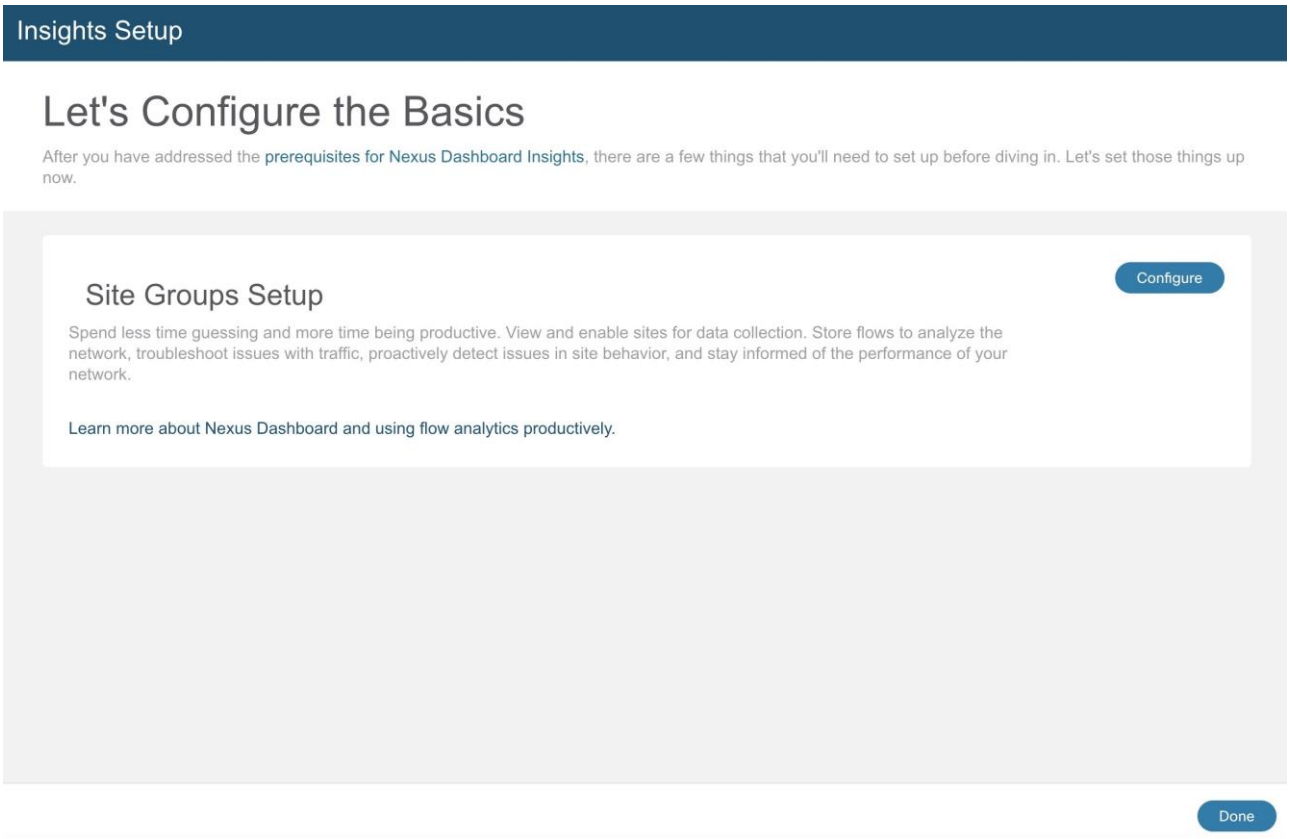
   a. Cisco ACI の NTP 構成 Cisco ACI NTP 構成マニュアル

   b. Cisco ACI インバンドサイト構成 Cisco ACI インバンド構成に関するマニュアル

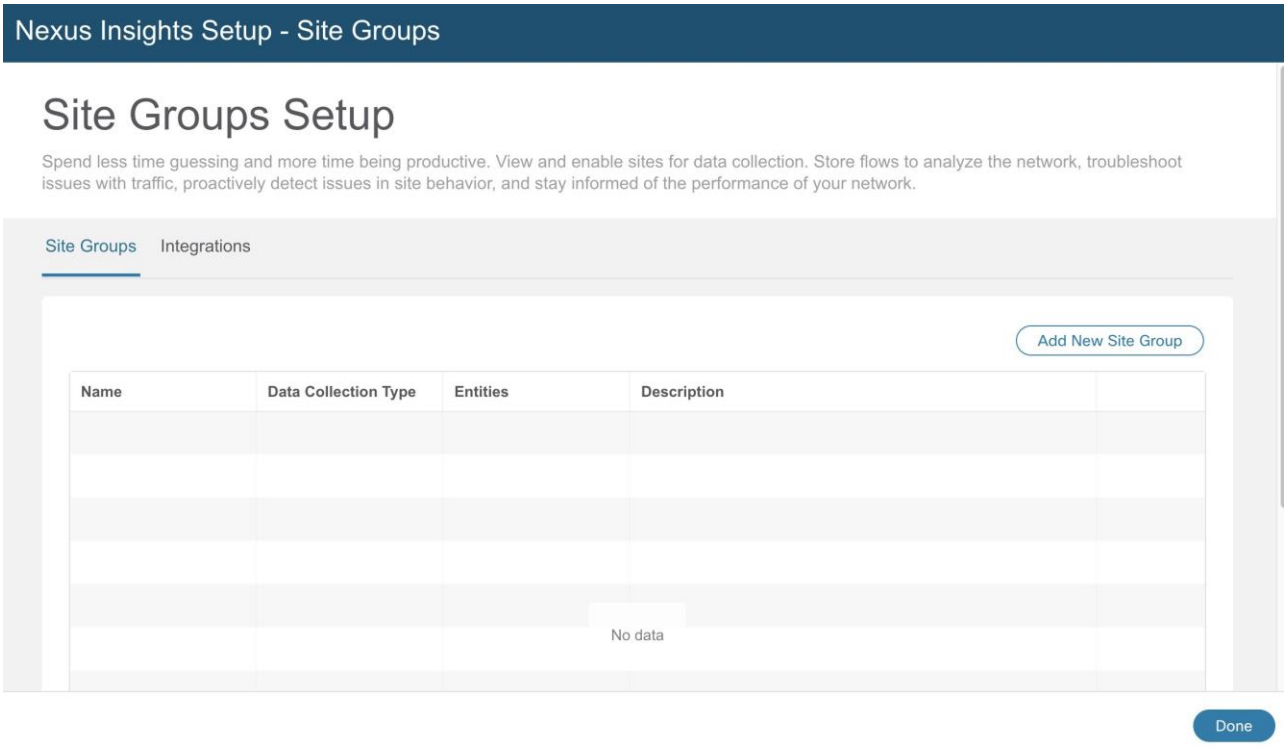


   c. **[Cisco Nexus Dashboard Insights の前提条件を確認して対処しました（I have reviewed and addressed the prerequisites for Cisco Nexus Dashboard Insights ）]** チェックボックスをオンにして、**[開始（Let's Get Started）]** をクリックします。

3. **[基本構成（Let's Configure the Basics）]** ページの **[サイトグループのセットアップ（ Site Groups Setup ）]** エリアで、**[構 成 （ Configure ）]** をクリックし、サイトグループが期待どおりに表示されることを確認します。



4. **[サイトグループのセットアップ（Site Groups Setup）]** エリアで、**[新しいサイトグループの追加（Add New Site Group）]** をクリックします。



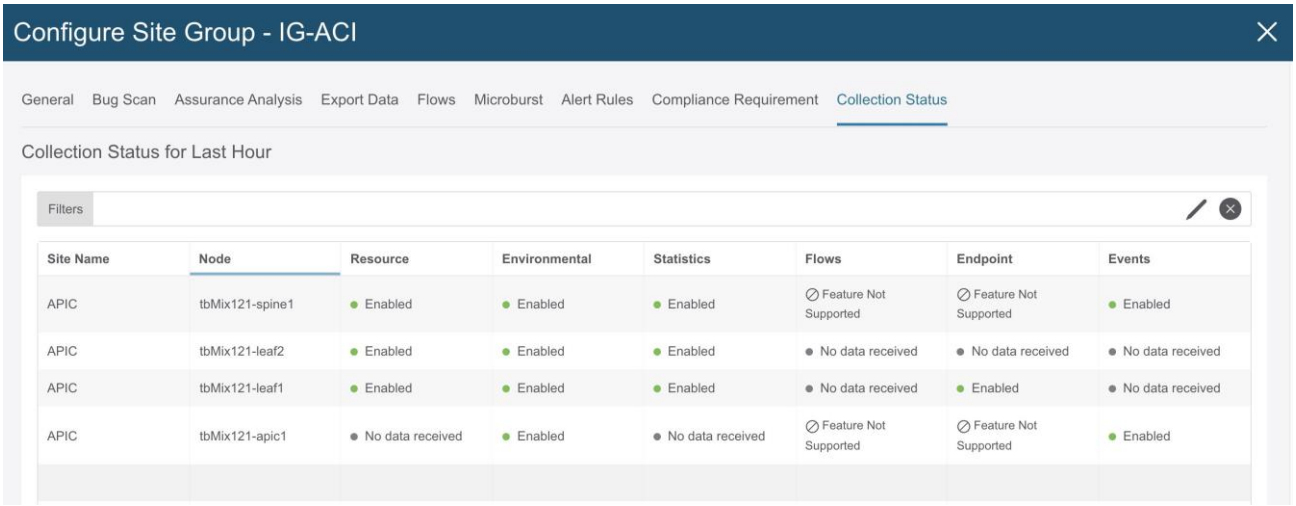
5. **[新しいサイト グループの追加（Add New Site Group）]** ダイアログボックスの **[全般（General）]** エリアで、サイト グループの名前と説明を追加します。
6. **[構成**（Configuration）] エリアの **[データ収集タイプ**（Data Collection Type）] エリアで、**[サイトの追加**（Add Site(s)）] を選択します。これで、このサイト グループに追加するサイトを選択できます。
7. **[エンティティ**（Entity）] エリアで、**[メンバーの選択**（Select Member）] をクリックします。

8. **[サイトの選択（Select a Site）]** ダイアログボックスから適切なサイトを選択し、**[選択（Select）]** をクリックします。サイトグループにサイトを追加するには、この手順を繰り返します。
9. **[新しいサイト グループの追加（Add New Site Group）]** ダイアログボックスで、チェックマークをクリックしてタスクを完了し、**[保存（Save）]** をクリックします。サイトがサイトグループに追加されます。
10. **[サイトグループのセットアップ（Site Groups Setup）]** エリアで、**[完了（Done）]** をクリックします。
11. **[基本構成（Let's Configure the Basics）]** ページで、**[完了（Done）]** をクリックします。

サイトグループタブの有効化または設定

Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページの上部で、サイトグループを選択します。サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。**[サイトグループの設定（Configure Site Group）]** ページで、タブ別に一覧表示された関連機能を有効化または設定します。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および有効化できます。

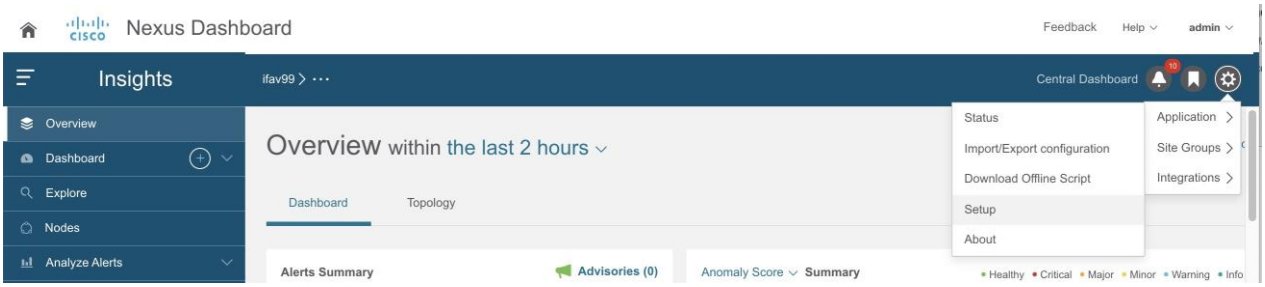
- **[全般]** タブ：サイトグループ名、データ収集タイプなどを含む、サイトグループの詳細が表示されます。サイトグループに含まれるサイトに関連するサイトの詳細も、収集ステータス、設定ステータス、ノードステータス、およびタイプに関連する詳細とともに一覧表示されます。
- **[バグスキャン（Bug Scan）]** タブ: 詳細については、バグスキャンを参照してください。
- **[アシュアランス分析（Assurance Analysis）]** タブ: サイトまたはアップロードされたファイルを含むサイトグループでのアシュアランス分析の実行の詳細については、サイトグループの追加とサイトのアシュアランス分析の実行を参照してください。また、サイトグループへのファイルのアップロードとアシュアランス分析の実行も参照してください。
- データのエクスポート（Export Data） **タブ：詳細については、**データのエクスポートを参照してください。
- [フロー（Flows）] **タブ: 詳細については、**フローの構成を参照してください。
- [マイクロバースト（Microburst）] **タブ: 詳細については、**インターフェイス統計のマイクロバーストサポート**を参照してください。**
- [アラートルール（Alert Rules）] **タブ: 詳細については、**アラートルールを参照してください。
- **[コンプライアンス要件**（Compliance Requirement）タブ: 詳細については、コンプライアンスを参照してください。
- **[収集ステータス（Collection Status）]** タブ: サイト名、ノード、リソース、環境、統計情報、フロー、エンドポイント、イベントなどのステータスチェックを表示するテレメトリデータが表示されます。次の例のページを参照してください。


Configure Site Group - IG-ACI
General
Bug Scan
Assurance Analysis
Export Data
Flows
Microburst
Alert Rules
Compliance Requirement
Collection Status
Collection Status for Last Hour
Filters
Site Name
Node
Resource
Environmental
Statistics
Flows
Endpoint
Events
APIC
tbMix121-spine1
Enabled
Enabled
Enabled
Feature Not Supported
Feature Not Supported
Enabled
APIC
tbMix121-leaf2
Enabled
Enabled
Enabled
No data received
No data received
No data received
APIC
tbMix121-leaf1
Enabled
Enabled
Enabled
No data received
Enabled
No data received
APIC
tbMix121-apic1
No data received
Enabled
No data received
Feature Not Supported
Feature Not Supported
Enabled

Cisco Nexus Dashboard Insights Day N セットアップの基本構成

0日目のセットアップが完了し、Cisco Nexus Dashboard Insightsサービスを再度起動する場合は、次の操作を実行します。

1. Nexus Dashboard Insightsサービスを起動すると、**概要**ページが表示されます。
2. ページの右上で、[設定]アイコン > **[アプリケーション（Application）]** > **[セットアップ（Setup）]**をクリックします。



3. **[基本設定（Let's Configure the Basics）]** ページで、**[Cisco Nexus Dashboard Insightsの前提条件をクリック（ Click the Prerequisites for Cisco Nexus Dashboard Insights）]**リンクをクリックし、必須設定が設定されていることを確認します。
4. 確認後、必要な場合には、**[Cisco Nexus Dashboard Insights の前提条件を確認して対処しました**（I have reviewed and addressed the prerequisites for Cisco Nexus Dashboard Insights）] チェックボックスをオンにして、**[開始（Let's Get Started）]** をクリックします。
5. **[サイトグループのセットアップ（Site Groups Setup）]** 領域で、**[設定の編集（Edit configuration）]** をクリックし、**[サイトグループのセットアップ（Site Groups Setup）]** 領域で、サイトグループが期待どおりに表示されていることを確認します。

> サイトグループを編集する場合は、[アクション（Actions）] メニュー > [サイトグループの編集（Edit for your Site Group）] をクリックし、編集を実行します。サイトグループのサイトを編集するには、「サイトグループの管理」を参照してください。

6. **[完了（Done）]** をクリックします。

注意事項と制約事項

- Cisco Nexus Dashboard の再起動後、Cisco Nexus Dashboard の機能復元のために、次の処理が完了するまで待つことをお勧めします。
  - Cisco Nexus Dashboardクラスタは緑色で表示されます。または
  - acs health CLIコマンドで正常と表示されます。
- ファブリックポリシーをアップグレードするか、ノードをアップグレードするときに、ファブリックと Cisco Nexus Dashboard クラスタ間の接続が失われると、Nexus Dashboard Insights が誤った欠落エンドポイント異常を発生させることがあります。
- インターフェイスおよびポートチャネルの 動 作 状 態 がNexus Dashboard

Insightsのインストール前にダウンしている場合、インターフェイスおよびポートチャネルのダウン異常は発生しません。Nexus Dashboard Insightsのインストール後、動作状態がアップまたはダウンの場合にのみ異常がキャプチャされます。

- Nexus Dashboard Insights は、ファブリックとのすべての通信をインバンドネットワークのみに依存しているため、Cisco Nexus Dashboard には Nexus Dashboard Insights の到達可能性ステータスが正確に反映されていない場合があります。
- フローテレメトリの場合、Nexus Dashboard Insights は、ユーザーが指定した時間範囲のサイクル全体に対して特定のフローの最大異常スコアをキャプチャします。この異常スコアの計算は、他のリソースの異常計算と一致しません。

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。

概要

Nexus Dashboard Insights の[概要]ページのナビゲーション

Nexus Dashboard
InsightsのGUIは、ナビゲーションウィンドウと作業ウィンドウで構成されています。

ナビゲーション ウィンドウ

Nexus Dashboard Insightsのナビゲーションウィンドウには、次のカテゴリが含まれています。

[概要（Overview）]：Nexus Dashboard Insightsのメインページで、アドバイザリ、異常、アラート、タイムライン、異常スコア別上位ノード、トポロジビューがあるサイト グループにすぐにアクセスできます。

[ダッシュボード（Dashboard）]：カスタムダッシュボードを使用すると、独自のダッシュボードを作成し、ダッシュボードにビューを追加できます。

[Explore]：Explore機能を使用すると、使いやすい自然言語クエリ形式でアセットとそのオブジェクトの関連付けを検出できます。

[ノード]: 上位ノードと上位リソースのグラフ表示を含むノードの詳細ビュー。

[アラートの分析（Analyze Alerts）]：アドバイザリの総数、Field Notice、PSIRT、および異常スコア、重大度、その他の詳細別の上位ノードを含む異常にアクセスできます。この領域のサブタブは次のとおりです。

- [異常（Anomalies）]：異常ダッシュボードは、リソース使用率、環境の問題、インターフェイスとルーティングプロトコルの問題、フロー、エンドポイント、イベント、サイトとアップロードされたファイルのアシュアランス分析、コンプライアンス、変更分析、および静的分析に対して発生した異常で構成されます。
- [アドバイザリ（Advisories）]：アドバイザリダッシュボードは、Field Notice、ソフトウェアとハードウェアのEOL/EOS、ノードレベルでのPSIRT、およびコンプライアンスが原因の関連する影響で構成されます。

[コンプライアンス（Compliance）]：コンプライアンスを使用すると、セキュリティポリシーとコンプライアンス
チェックへの継続的なコンプライアンスを実現できます。

[トラブルシュート]: この領域のサブタブは次のとおりです。

- [差分分析（Delta Analysis）] - 差分分析を使用すると、ポリシー、実行時の状態、および2つのスナップショット間のネットワークの正常性の違いを分析できます。

- [ログコレクタ] - ネットワーク内のデバイスのログを収集して、Cisco Intersight Cloudにアップロードします。Cisco
  TACがサイト上にあるユーザー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 からログをプルできるようにします。

[参照] : この領域のサブタブは次のとおりです。

- [リソース] : Cisco
  APIC上のサイトノードのソフトウェアおよびハードウェアリソースの監視が含まれます。
- [環境] :
  サイトノードのファン、CPU、メモリ、電力などのハードウェアリソースの環境統計情報の監視が含まれます。
- [フロー（Flows）] :
  この機能は、フローレベルでの深い洞察を提供し、平均遅延、パケット ドロップ インジケータ、フロー移動インジケータなどの詳細を提供します。
- [エンドポイント（Endpoint）] :
  シスコサイトノードのエンドポイントの迅速な移動に関するエンドポイントと、Cisco ACI全体での再起動後に学習されないエンドポイントの監視が含まれます。
- [インターフェイス] : Cisco
  APICおよびサイトノードのインターフェイスの監視が含まれます。
- [プロトコル] : Cisco APICおよびサイトノードの監視プロトコルが含まれます。
- [イベント] : イベント、障害、および設定変更の監視が含まれます。

[変更管理] : このエリアのサブタブは次のとおりです。

- [ファームウェアアップデート分析] -
  この機能は、推奨されるソフトウェアバージョンへのアップグレードパスを提案し、アップグレードの潜在的な影響を判断します。また、アップグレード前後の検証チェックにも役立ちます。
- [変更前の分析] :
  この機能を使用すると、意図した変更をモデル化し、その変更で目的の結果が生成されるかどうかを確認できます。

トップ メニュー

[Nexus Dashboard Insights]ページの上部と作業ウィンドウの上に、次のような追加のリンクとアイコンがあります。

[サイトグループまたはサイト] :
リンクにはサイトグループまたはサイトの名前が表示されます。選択を別のサイトグループまたはサイトに変更するには、[サイトグループまたはサイト（Site Group or Site）] リンクをクリックして **[サイトグループまたはサイトの選択]** ダイアログボックスを表示し、選択内容を変更します。

選択したサイトグループまたはサイトを設定するには、サイトグループの横にある

[アクション（Actions）] メニューをクリックし、
[サイトグループの設定（Configure Site Group）] **をクリックします。**

選択したサイトグループにコンプライアンス要件を追加するには、[アクション（Actions）] メニュー > **[追加（Add）]** > **[コンプライアンス要件（Compliance Requirement）]** をクリックします選択したサイトグループにアラートルールを追加するには、[アクション（Actions）] メニュー > **[追加（Add）]** > **[アラートルール（Alert Rules）]** をクリックします。

[ヘルプセンター（Help Center）]：**[集中ダッシュボード（Central Dashboard）]**、**[通知（Notifications）]**、**[ブックマーク（Bookmark）]**、および **[設定（Settings）]** アイコンの上に、**[ヘルプ（Help）]** ドロップダウンメニューがあります。**[ヘルプ（Help）]** > **[ヘルプセンター（Help Center）]** をクリックして、ドキュメントリソースへのリンクを含む **[ヘルプセンター（Help Center）]** ページにアクセスします。[Nexus Dashboard Insights]タイルをクリックして、適切なリソースを見つけます。

[集中ダッシュボード]：このリンクをクリックすると、アラートの概要、異常またはアドバイザリ別の上位サイトグループ、およびその他のサイトグループ関連の詳細が表示される
[集中ダッシュボード（Central Dashboard）] ページに移動します。

[通知（Notifications）] アイコン: このアイコンをクリックして、シスコからの通知を表示します。

- 選択した時間範囲に基づいて発生した異常
- 進行中の異常
- 新しいプロセス、新しいアドバイザリ、新しい異常通知

ブックマーク アイコン：詳細ビューまたはページをブックマークし、保存すると、後で使用できます。ブックマークは、ビュー全体、時間範囲、選択したノードを保存し、ビューのスナップショットを作成します。リストに追加できるブックマークの数に制限はありません。

ブックマークの追加:

1. 左側のナビゲーションウィンドウから、[リソースの参照（Browse Resources）]、[環境の参照（Browse Environmental）]、[統計情報の参照（Browse Statistics）]、[ダッシュボード]（Dashboard）
   ビュー、または特定のビューなどの詳細ビューをクリックします。
2. 上部のナビゲーションウィンドウで[ブックマーク]アイコンをクリックします。
3. オレンジ色の[ブックマーク]アイコンは、選択した詳細ビューが保存され、ブックマークのリストに追加されていることを示します。ブックマークには、詳細ビューが作成され、ビューまたはページがリストに保存された時の元の時間範囲、開始日時、終了日時が記録されます。

ブックマークの表示:

1. 上部のナビゲーションウィンドウで[ブックマーク]アイコンをクリックします。
2. リストからブックマークをクリックして、ノードビューと選択した時間範囲を含むブックマークされたページを開きます。これは、後で使用するために[詳細ビュー]ページのスナップショットを作成するのに役立ちます。

ブックマークの削除:

1. 上部のナビゲーションウィンドウで[ブックマーク]アイコンをクリックします。
2. リストからブックマークされたページをクリックすると、ブックマークされたページが開きます。
3. [ブックマーク]アイコンの選択を解除します。

[設定（Settings）] アイコン:

このアイコンのドロップダウンメニューには、**[アプリケーション（Application）]**、**[サイトグループ（Site Groups）]**、**[統合（Integrations）]** が表示されます。

[アプリケーション（Application）] アイコンをクリックすると、**[ステータス（Status）]**、**[設定のインポート/エクスポート（Import/Export Configuration）]**、**[オフラインスクリプトのダウンロード（Download Offline Script）]**、**[セットアップ（Setup）]**、**[バージョン情報（About）]** から選択できます。

- [ステータス]:
  クリックして、アラートやキャパシティ使用率などのアプリケーションステータスを表示します。
- [設定のインポート/エクスポート]:
  この機能を使用すると、サイトグループ、アラートルール、エクスポート設定などの設定をインポートおよびエクスポートできます。
- [オフラインスクリプトのダウンロード（Download Offline Script）]:
  クリックして、ファイルをアップロードしてアシュアランス分析を実行するために必要なオフラインスクリプトをダウンロードします。
- [セットアップ]: クリックして、[Nexus Dashboard Insightsセットアップ]ページへのリンクを表示します。
- [バージョン情報]: クリックして、Nexus Dashboard Insightsのバージョン番号に関する詳細を取得します。

[サイトグループ（Site Groups）] アイコンをクリックすると、**[サイトグループの管理（Manage Site Groups）]** を選択できます。詳細については、「サイトグループの管理」を参照してください。

[統合（Integrations）] アイコンをクリックすると、**[統合の管理（Manage Integrations）]** または **[統合の追加（Add Integrations）]** を選択できます。詳しくは 統合を参照してください。

作業ペイン

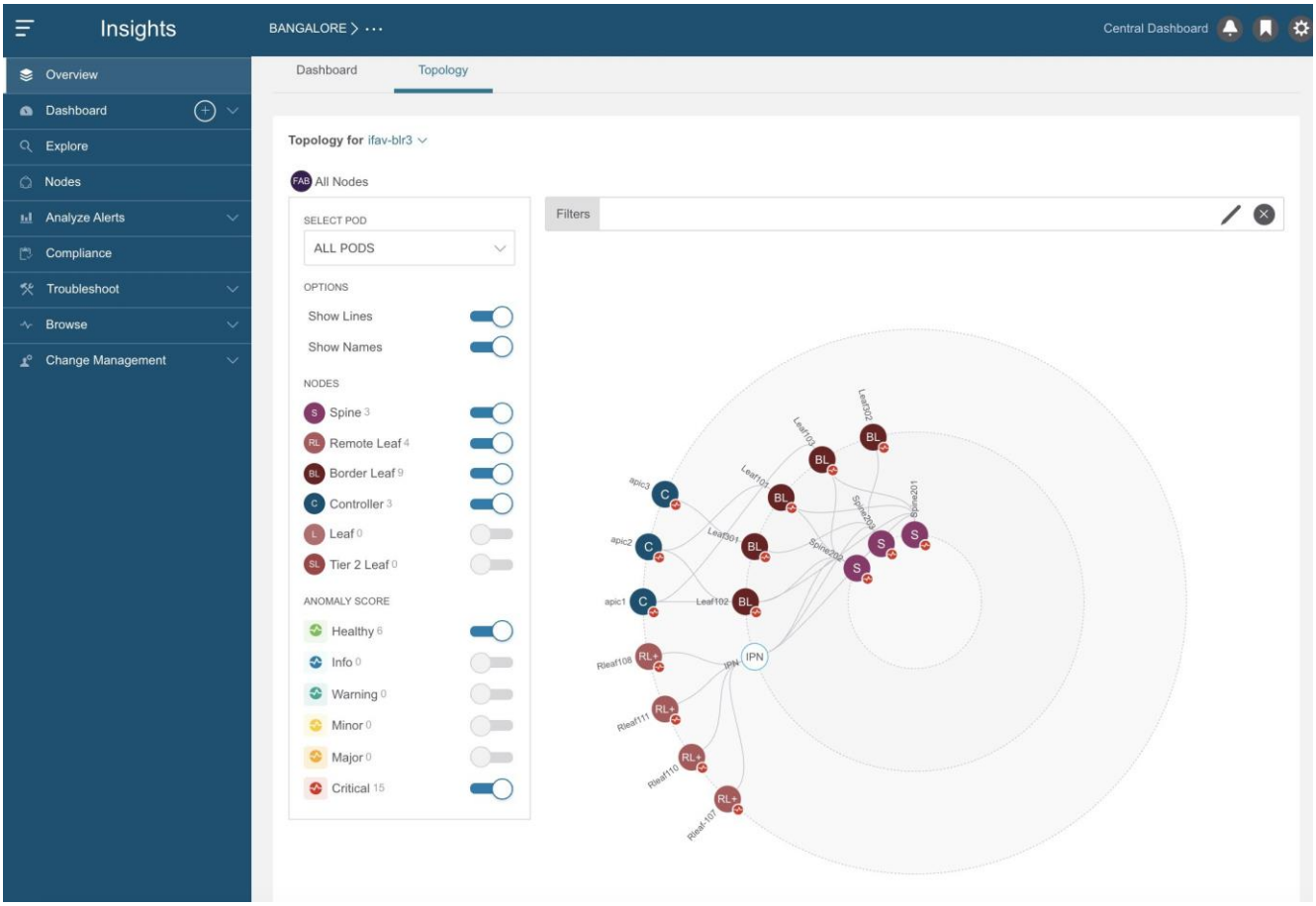
作業ペインは、Nexus Dashboard Insightsの主な表示場所です。すべての情報タイル、グラフ、チャート、テーブル、およびリストが作業ウィンドウに表示されます。**[概要（Overview）]** ページを表示すると、**[ダッシュボード（Dashboard）]** タブと **[トポロジ（Topology）]** タブがあります。

[ダッシュボード] タブ

[ダッシュボード（Dashboard）] タブには、[アラートの概要（Alerts Summary）]、[異常スコア（Anomaly Score）]、[アラート検出タイムライン（Alert Detection Timeline）]、[異常の内訳（Anomalies Breakdown）]、[アドバイザリの内訳（Advisories Breakdown）]、[異常スコア別上位ノード（Top Nodes by Anomaly Score）] など、さまざまなタイルが表示されます。情報タイルでは、数値をクリックして切り替えて、クリックした特定の項目に関する詳細を表示できます。

トポロジタブ

Nexus Dashboard Insights のトポロジ表示では、選択したサイトグループに関する放射状グラフで情報が表示されます。ノードや異常スコアなど、表示対象を選択するためのフィルタオプションがあります。



テーブル

GUIのテーブルに列の1つとして[設定]アイコン がある場合は、列のカスタマイズに使用できます。アイコンをクリックすると、項目のリストを含む **[列のカスタマイズ（Customize Columns）]**

ダイアログボックスが表示されます。一部の設定は必須であるため、それらを設定するオプションはグレー表示されています。パラメータのユーザーが選択可能な項目については、テーブルの各列を表示または削除できます。列のタイトルをクリックアンドドラッグして、テーブル内の位置を再配置することもできます。**[保存（Save）]**をクリックしてテーブルを更新します。カスタマイズした列設定は、このログインインスタンスとその後のログインで保持されます。

Nexus Dashboard Insights のタイムゾーンの設定

デフォルトでは、Nexus Dashboard InsightsのGUIには、ユーザーのローカルタイムゾーンの日付と時刻が表示されます。このリリース以降、Nexus Dashboardでタイムゾーン設定を別のタイムゾーンに設定できます。タイムゾーン機能はユーザーごとに利用でき、ユーザー設定に保存されます。

選択したタイムゾーンは、GUIに表示される時間値に反映されます。GUIに表示されるすべての検出タイムラインとタイムスタンプには、選択したタイムゾーンの時間値が反映されます。

手順

1. Nexus Dashboardにログインします。
2. [管理（admin）] > [ユーザー設定（User Preferences）] **の順に選択します**。
3. **[ユーザー設定（User Preferences）]** ページの **[タイムゾーン（Time Zone）]** エリアでは、デフォルトのタイムゾーン値として **[自動（Automatic）]** が選択されています。

   これは、ユーザーのローカルタイムゾーンです。
4. **[タイムゾーン設定（Time Zone Preference）]** フィールドで、**[手動（Manual）]** を選択します。
5. **[最寄りの都市（Nearest City）]** フィールドに、希望する都市を入力して、**[タイムゾーン（Time Zone）]** フィールドに適切な値を設定します。

   または、地図内で選択した都市にピンをドラッグすると、**[最寄りの都市（Nearest City）]** と **[タイムゾーン（Time Zone）]** のフィールドに入力されます。
6. **[保存（Save）]** をクリックします。

選択したタイムゾーンは、Nexus Dashboard InsightsのGUIに表示される時間値に反映されます。Nexus Dashboard InsightsのGUIに表示されるすべての検出タイムラインとタイムスタンプには、選択したタイムゾーンの時間値が反映されます。

[概要] ページ

作業ペインの **[概要（Overview）]** ページには、**[ダッシュボード（Dashboard）]** タブと **[トポロジ（Topology）]**

タブがあります。このセクションでは、これらのタブについて説明します。

[ダッシュボード] タブ

[ダッシュボード（Dashboard）]
タブには、サイトノードで検出されたアラートと異常が表示されます。さらに、また、選択したサイトのノードに推奨されるアドバイザリも表示されます。

各 Cisco ACI ノードは、サイトからのテレメトリイベントを Nexus Dashboard Insights にストリーミングします。Nexus Dashboard Insights はイベントを分析して、サイトの問題をプロアクティブに検出します。Nexus Dashboard Insightsでは、関連情報を表示し、特定の項目を選択して詳細を表示できます。Cisco Nexus Dashboard Insights ダッシュボードからは、ネットワークで発生したアドバイザリと異常にすぐにアクセスできます。

ダッシュボードのアドバイザリには、ネットワーク内のスイッチハードウェアおよびソフトウェアに関する3つのレベルのアドバイザリ重大度が表示されます。重大度によって分類され、アドバイザリが適用されるソフトウェアバージョンとハードウェアプラットフォームが特定されます。アドバイザリは、関連するField Notice、PSIRT、バグ、ソフトウェア、ハードウェア、およびハードニング違反の検出に基づいて配信されます。Cisco Nexus Dashboard Insights はこの情報を考慮し、次のことを推奨します。

- バグ、PSIRT、およびField Noticeに対処するためにソフトウェアまたはハードウェアをアップグレードする
- TACに連絡する
- シスコの推奨事項
- ソフトウェア アップグレード パス

異常は、スイッチの最後に認識された「良好な」状態から学習された成果であり、タイプと重大度別に表示されます。異常には、リソース使用率、環境、フローの異常、インターフェイスおよびプロトコルレベルのエラーが含まれます。異常スコアは、重大度に基づいて色分けされています。

- クリティカル: 赤色
- メジャー: オレンジ色
- マイナー: 黄色
- 警告: ターコイズ色
- 情報: 青色
- 正常: 緑色

ダッシュボードの
[リーフ（Leafs）]、[スパイン（Spines）]、[コントローラ（Controllers）]
ブロックでは、中央の大きな数字が各デバイスの総数を示しています。

このページでは、**[重大度別の異常の内訳（Anomalies Breakdown by Severity）]**を選択すると、重大度別の異常の内訳も表示できます。色付きの重大度ドットの横にある数字は、その異常レベルにあるデバイスの数です。異常カウンタの合計は、異常の大きな総数と同じになります。

異常の一因となる要因には、しきい値の超過や過剰な変化のペースなどがあります。

[ダッシュボード（Dashboard）]タブのタイルには、次の詳細が表示されます。

プロパティ	説明
カテゴリ別異常	異常の数がカテゴリ別に表示されます。異常カテゴリには次のものがあります。 • フロー • リソース • 環境 • 統計 • エンドポイント • バグ • Orchestratorアシュアランス
カテゴリ別アドバイザリ	異常（内部サイト障害）の数とその重大度が表示されます。エリアをクリックすると、**[ノード（Node）]**や**[異常スコア（Anomaly Score）]などの詳細な障害情報が表示されます。** • PSIRT • フィールド通知 • HW EOL • SW EOL • コンプライアンス
異常スコア別上位ノード	上位ノードとその異常ステータスの概要が表示されます。異常ステータスは、異常の一因となる機能に基づいて表示されます。各機能をクリックして、選択したノードの特定の情報を表示します。 • PSIRT • Field Notice • HW EOL • SW EOL

[カテゴリ別異常（Anomalies by Category）] および **[カテゴリ別アドバイザリ（Advisories by Category）]** から任意のプロパティをクリックして、*[アラートの分析（Analyze Alerts）]* 作業ペインにアクセスします。

ノードインベントリ

このダッシュボードには、サイトにあるノードの次の情報が表示されます。

プロパティ	説明
異常スコア	上位ノードとその異常スコアの概要が表示されます。異常スコアは、異常の一因となる機能に基づいて表示されます。
リーフノード	異常があるサイトのリーフノードの総数が表示されます。
スパインノード	異常があるサイトのスパインノードの総数が表示されます。
コントローラ	サイト内の Cisco APIC の総数が表示されます。

- 異常スコアとファームウェアを切り替えます。各ノードタイプには、異常スコアによる内訳ではなく、検出されたファームウェアバージョンに基づいた異常の内訳が表示されます。
- **[リーフノード（Leaf Nodes）]**、**[スパインノード（Spine Nodes）]**、および **[コントローラ（Controllers）]** をクリックして、*[ノードの参照（Browse Nodes）]* 作業ペインからサイト内の個々のノードに関する詳細を表示します。

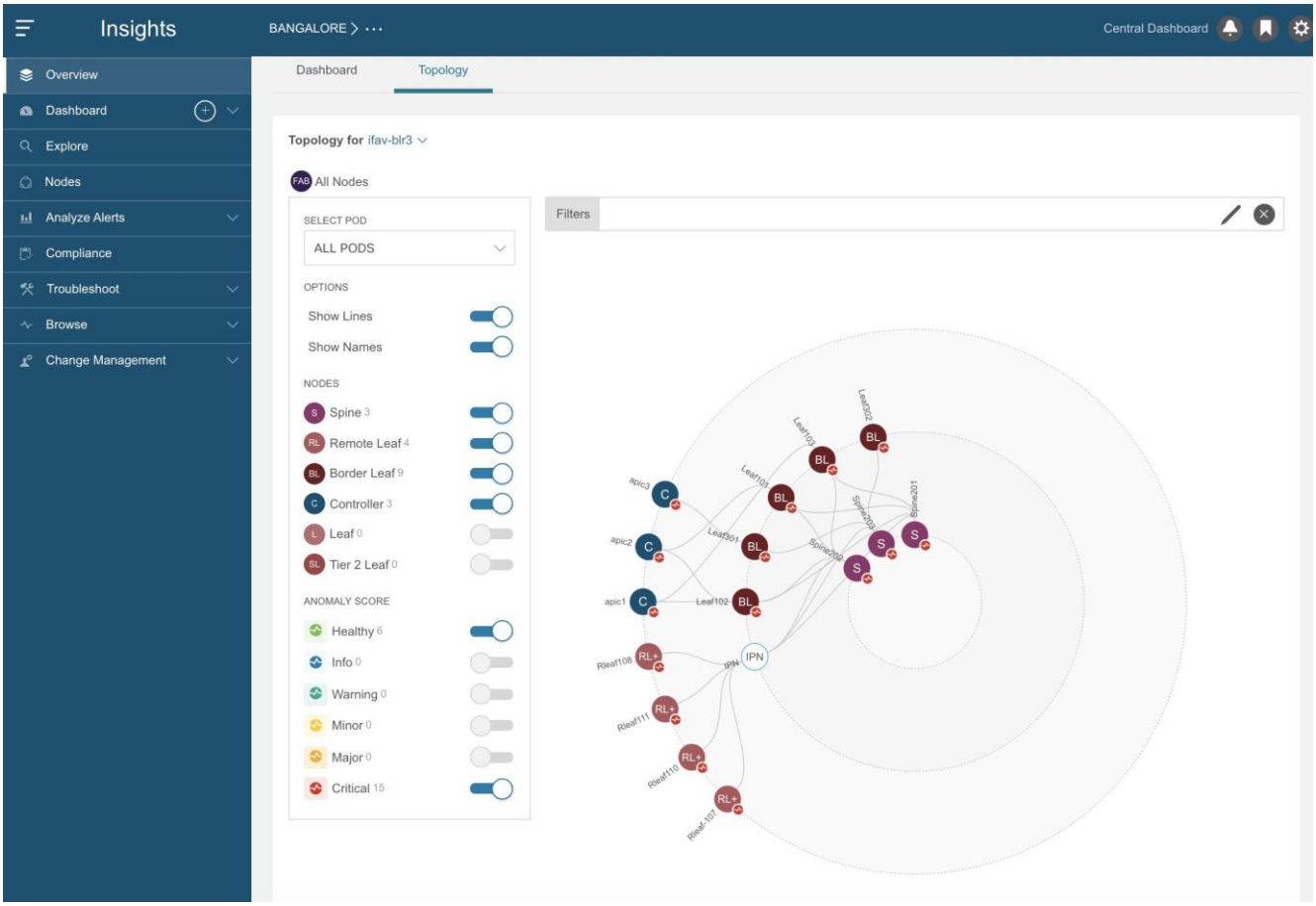
トポロジタブ

サイトグループ内の異常があるすべてのノードのトポロジ表示については、**[概要（Overview）]** ページで、作業ペインの **[概要（Overview）]** エリアを表示します。**[トロポジ]** タブをクリックします。

トポロジには、LLDPプロトコル情報を使用した、ファブリック内のノードの相互接続が表示されます。このページには、ノード、ノードタイプ、インターフェイス名、リーフノード間の LLDP 情報、IPN、およびリンク上の異常スコアのリストが表示されます。このビューでは、スパインノード、リーフノード、およびボーダーリーフノードを、異なる色とインターフェイス名で区別できます。

IPNリンクは、IPNに接続されたスパインノードリンクであり、内部リーフノードに接続されたリンクとは区別されます。IPNは、トポロジ内の物理エンティティとして表示されます。

スパインノード、リーフノード、およびコントローラを切り替えて、トポロジビューのノードを追加または削除します。各異常スコアを切り替えて、トポロジビューに追加したり、ビューから削除したりします。



ズームイン機能を使用して、EPG、VRF、テナントなどの論理構造に基づいてインフラストラクチャの一部に範囲を限定します。

トポロジ作業ウィンドウでノードを表示、ソート、およびフィルタ処理します。次のフィルタを使用して、表示されるノードを絞り込むことができます。

- [名前] - 特定の名前を持つノードのみ表示されます。
- [テナント] - 特定のテナントを持つノードのみ表示されます。
- [アプリケーション プロファイル] -
  指定されたプロファイルを持つノードのみ表示されます。
- [EPG] - 特定のEPGに対するノードのみ表示されます。
- [VRF] - 特定のVRFからのノードのみ表示されます。
- [BD] - 特定のブリッジドメインのノードのみ表示されます。
- [契約] - 特定の契約のノードのみ表示されます。
- [エンドポイント] - 特定のエンドポイントのノードのみ表示されます。
- [IP] - 特定のIPアドレスのノードのみ表示されます。

フィルタの絞り込みには演算子を使用します。

異常スコアは、トポロジ内のドットで表されます。トポロジビューは、異常の影響を受けるノードを見つけるのに役立ちます。

トポロジ上のノードをクリックして、ノードの追加の詳細を表示します。サイドペイン

には、ノードの一般的な追加の異常詳細が表示されます。

注意事項と制約事項

- LLDP情報がないノードはトポロジに表示されません。
- Cisco Nexus 9200、9300-EX、9300-FX、および 9300-GX プラットフォームスイッチ、N9K-C9316D-GX および N9K-C9364C-GX スイッチは検出されず、トポロジに表示されません。

アラート検出タイムライン

タイムラインには、ユーザーが選択した時間範囲のサイクル全体で発生したさまざまなアラートが表示されます。**[概要（Overview）]** ページの作業ペイン、**[ダッシュボード（Dashboard）]** タブ、**[アラート検出タイムライン（Alert Detection Timeline）]** のグラフには、アラートが発生したときのタイムゾーンが表示されます。タイムラインに異常とアドバイザリが表示されます。異常またはアドバイザリの色は、その重大度に基づいています。

詳細については、アラートの分析を参照してください。

[アラート検出タイムライン]アイコン

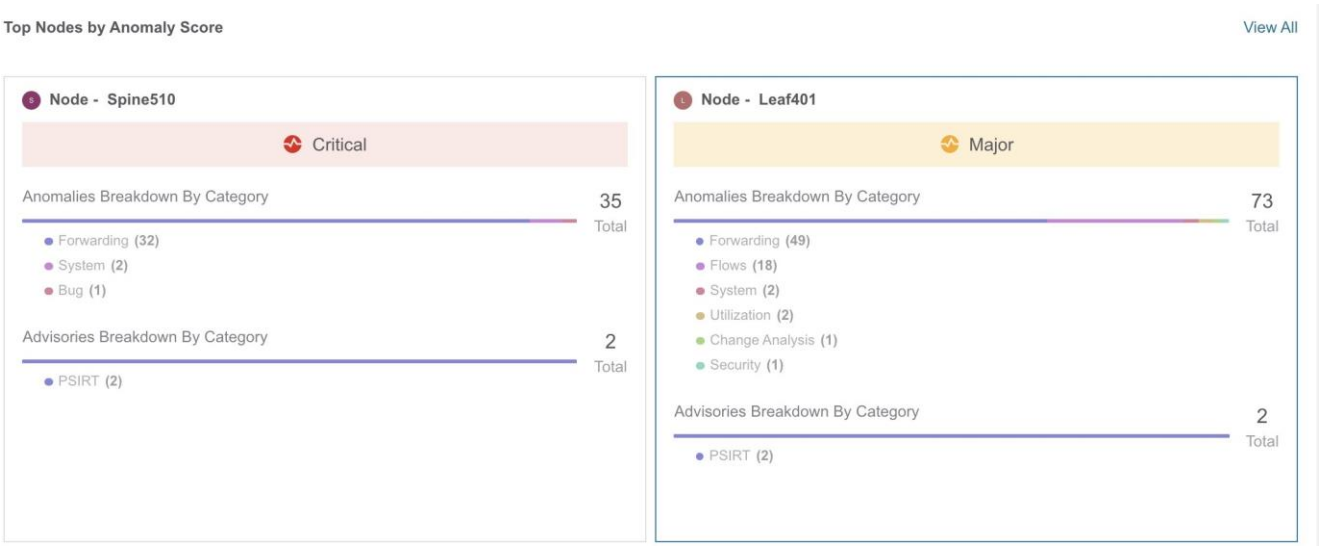
- 色付きの丸いドットは、ノードのイベント、障害、および監査ログに対応しています。
- タイムラインの周りにある複数のリングは、オブジェクトのグループを表します。タイムライン内の単独のリングは、単一のオブジェクトを表します。
- ハートのアイコンは、異常のみを表します。青い円は、現在選択されている異常を示します。

異常スコア別上位ノード

[概要（Overview）] ページの作業ウィンドウの **[ダッシュボード（Dashboard）]** タブに、**[異常スコア別上位ノード（Top Node by Anomaly Score）]** エリアが表示されます。

このセクションには、上位ノードとその異常スコアの概要が表示されます。各ノードカードには、さらにカテゴリ別に分類された異常とアドバイザリが表示されます。

[ノードの詳細（Node Details）] ページのノードカードの見出しをクリックして、一般的な情報、ノードの概要、およびノードに適用される異常のテーブルを表示します。*[ノードの概要（Node Overview）]* セクションには、リソース使用率、環境、統計情報、フロー、イベントなどのノードのカテゴリが表示されます。各機能をクリックして、選択したノードの特定の情報を表示します。



異常スコアと異常の優先順位

[異常別上位ノード（Top Nodes by Anomalies）]
ページには、異常の重大度に基づいて異常が要約されています。

以下は、異常の重大度に基づいた一群の異常または個別の異常に関する異常の優先順位の例です。

- リーフノードにはクリティカルな異常が1つあり、別のリーフノードにはメジャーな異常が9つあります。この場合、メジャーな異常が 9 つあるリーフノードは、クリティカルな異常が 1 つあるリーフノードよりも優先されます。
- あるノードには 2 つのクリティカルな異常と 4 つのメジャーな異常があり、別のノードには 2 つのクリティカルな異常と 3 つのメジャーな異常があるとします。ほとんどの場合、異常スコアが高く、異常の数が少ないノードが、異常スコアが低く、異常の数が多いノードよりも優先されます。
- あるノードにはスコア91の異常が1つあり、別のノードにはそれぞれスコア89の異常が9つあるとします。89% を消費した 9 つの異常があるノードは、91% を消費した 1 つの異常があるノードよりも悪いケースです。この場合、9つの異常があるノードが優先されます。
- リーフノード1とリーフノード2の異常スコアがリーフノード4よりも高い場合。リーフノード 1 とリーフノード 2 の異常に関する異常スコアは 88 で、リーフノード 4 の両方の異常に関する異常スコアが 81 の場合、異常スコアが 88 のリーフノードが優先されます。
  - リーフノード1 およびリーフノード2の異常に関する異常スコアは、4^8.8 = 198668です。
  - リーフノード4の両方の異常に関する異常スコアは、4^8.1 + 4^8.1 = 150562です。

サイトグループでのサイトの追加と管理およびアシュアランス分析の実行

保証分析

Nexus Dashboard Insightsでは、次の2つの方法を使用してアシュアランス分析を実行できます。

- サイトグループの一部であるサイトを選択して分析できます。
- サイトグループの一部としてファイルをアップロードし、アップロードしたファイルに対してアシュアランス分析を実行できます。

サイトグループの一部であるサイトを選択して分析： アシュアランス分析には、サイトからのデータ収集、モデルを作成するための収集データを使用した分析の実行、結果の生成が含まれています。

アシュアランス分析は、リアルタイムでアシュアランスを提供します。サイトグループ内のサイトのアシュアランス分析では、データ収集、モデルの生成、および結果の生成は同時に実行されます。収集されたデータは収集後ただちに分析されて、結果が生成されます。これは、ユーザーが指定した一定の時間間隔後に繰り返されます。詳細については、サイトグループの追加とサイトのアシュアランス分析の実行を参照してください。

サイトグループの一部としてアップロードしたファイルおよびアップロードしたファイルでアシュアランス分析を実行 アップロードしたファイルのアシュアランス分析については、1回限りのアシュアランスが提供されます。このアシュアランス分析により、データ収集段階を分析段階から切り離すことができます。データは Python スクリプトを使用して収集され、収集されたデータは Nexus Dashboard Insights にアップロードされて、1回限りのアシュアランスが提供されます。収集されたデータは、後で分析することもできるため、ユーザーは変更管理時間帯にデータを収集し、後で分析を実行できます。詳細については、オフラインスクリプトとサイトグループへのファイルのアップロードとアシュアランス分析の実行を参照してください。

サイトグループの追加

この手順では、Cisco Nexus Dashboard Insights でサイトグループを追加し、Cisco Nexus Dashboard Insights に表示されるサイトを選択します。サイトグループのサイトを選択するには、まず Cisco Nexus Dashboard にサイトを追加する必要があります。

前提条件

この手順を開始する前に、Cisco Nexus Dashboardの管理者は、適切なサイトを **[サイト（Sites）]** 領域に追加しておく必要があります。詳細については、*Cisco Nexus Dashboard ユーザーガイド* を参照してください。Cisco Nexus Dashboard

でこのタスクを完了したら、Cisco Nexus Dashboard のナビゲーションウィンドウの **[サービス（Service）]** 領域で、[Cisco Nexus Dashboard Insights サービス] をクリックし、サービスがロードされるのを待ちます。

Cisco Nexus Dashboard Insights にサイトグループがまだ作成されていない場合、サービスを開始すると **[有効なサイトグループがありません（No Site Group enabled）]** ページが表示されます。**[サイトグループの構成（Configure Site Group）]** タブをクリックし、以下の手順に従います。Cisco Nexus Dashboard Insights を開始したときにサイトグループがすでに設定されている場合は、**[概要（Overview）]** ページが表示されます。

手順

次の手順に従って、サイトグループにサイトを追加します。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. 右上の [設定（Settings）] アイコン > **[サイトグループ（Site Groups）]** > **[管理（Manage）]** の順に選択します。

3. **[サイトグループの管理（Manage Site Groups）]** ページで、**[新しいサイトグループの追加（Add New Site Group）]** をクリックします。
4. **[新しいサイト グループの追加（Add New Site Group）]** ダイアログボックスの **[全般（General）]** エリアで、サイト グループの名前と説明を追加します。
5. [**構成**（Configuration）] エリアの [**データ収集タイプ**（Data Collection Type）] エリアで、[**サイトの追加**（Add Site(s)）] を選択します。これで、このサイト グループに追加するサイトを選択できます。
6. [**エンティティ**（Entity）] エリアで、[**メンバーの選択**（Select Member）] をクリックします。
7. [**サイトの選択**（Select a Site）] ダイアログボックスから適切なサイトを選択し、[**選択**（Select）] をクリックします。サイトグループにサイトを追加するには、この手順を繰り返します。
8. [**新しいサイト グループの追加**（Add New Site Group）] ダイアログボックスで、チェックマークをクリックしてタスクを完了し、[**保存**（Save）] をクリックします。サイトがサイトグループに追加されます。

サイトグループのアシュアランス分析を実行するには、サイトをサイトグループに追加後、サイトのアシュアランス分析の実行を参照してください。

サイトのアシュアランス分析の実行

前提条件

必要なサイトがサイトグループに追加されていること。詳細については、サイトグループの追加を参照してください。

手順

次の手順に従って、サイトグループのアシュアランス分析を実行します。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。

3. **[サイトグループの設定]** ページで、次の操作を実行します。
   a. **[アシュアランス分析（Assurance Analysis）]** タブをクリックし、鉛筆/編集アイコンをクリックします。
   b. **[設定（Configuration）]** ダイアログボックスで、**[状態（State）]** フィールドを **[有効（Enabled）]** に設定して、アシュアランス分析を有効にします。
   c. 適切な分析開始時刻、分析サイクルの繰り返し頻度、および分析終了時刻を指定します。**[保存（Save）]** をクリックします。
4. **[サイトグループの構成**（Configure Site Group）**]** ページにサイトが表示され、アシュアランス分析が有効になっていることが **[状態（State）]** に示されます。

> サイトに対して現在実行中の分析がない場合は、**[アシュアランス分析（Assurance Analysis）]** タブの **[今すぐ実行（Run Now）]** ボタンをクリックすると、そのサイトの 1 回限りのタイムインスタント分析。

オフラインスクリプト

Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、**[設定（Settings）]** > **[アプリケーション（Application）]** > **[オフラインスクリプトのダウンロード（Download Offline Script）]** を選択して、Python スクリプトをダウンロードします。ダウンロードしたスクリプトを実行して、アシュアランスのためのデータを収集します。

> Pythonオフラインデータ収集スクリプトは、Mac OSまたはCentosOSでのみサポートされています。Windows サーバーからこのスクリプトを実行するとエラーが発生し、APICバージ

ョンはサポートされていないことが Cisco Nexus Dashboard Insightsに示されます。

オフラインスクリプトには以下のスクリプトがあります。

- アシュアランス分析のためのデータ収集スクリプト
- アラートルール移行スクリプト
- コンプライアンス要件移行スクリプト
- オフラインサイトのPSIRT、Field Notice、EOLアドバイザリを表示するスクリプト
- オフラインサイトのファームウェアアップデート分析用スクリプト

アシュアランス分析のためのデータ収集スクリプト

Nexus Dashboard Insights データ収集スクリプトは、一連の REST API および CLI 呼び出しのために Cisco APIC および Cisco DCNM クラスタをポーリングする Python スクリプトです。REST API 呼び出しと CL I呼び出しについては、スクリプトに含まれている readme.md ファイルを参照してください。

Pythonの依存関係と、仮想環境に依存関係をインストールするプロセスについては、readme.mdファイルを参照してください。readme.md ファイルには、Cisco APIC、スパインスイッチ、リーフ スイッチから収集されるオブジェクトと **show** コマンドの完全なリストがあります。readme.md ファイルは、オフライン分析スクリプトファイルと同じ zip ファイル内にあります。オフライン分析スクリプトは、Nexus Dashboard Insights アプライアンスの [設定（Settings）] アイコンから直接ダウンロードできます。

スクリプトが起動されるワークステーションには、Cisco APIC および Cisco DCNM クラスタへのアウトオブバンド管理接続が必要です。Cisco ACI ファブリック内のすべてのノードにアウトオブバンド管理 IP アドレスが設定されていることを確認してください。ファイアウォールが（REST API を使用するための）HTTPS および（リーフスイッチおよびスパインスイッチに接続するための）SSH をブロックしていないことを確認してください。プロキシ設定がHTTPS接続を許可するように正しく設定されていることを確認してください。

readme.mdファイルには、スクリプトを使用するためのシンタックスがあります。デフォルトでは、スクリプトはデータ収集を 3 分間隔で 3 回反復して実行しますが、**-iterations** オプションを使用して反復回数を指定できます。予想される合計収集時間の範囲は、約 20 のリーフスイッチを備えたファブリックの場合、3 つのスナップショットの開始から終了まで 18～20 分です。構成の複雑さとファブリックのスケールによっては、大きなファブリックほど時間がかかります。

アラートルール移行スクリプト

これは、Cisco Network Assurance Engine (Cisco NAE)リリース5.1のイベントルールをCisco

Nexus Dashboard Insightsリリース6.0.1のアラートルールに移行するスクリプトです。このスクリプトを実行するには、エクスポートされた構成ファイルとCisco NAEセットアップのアシュアランスグループ名が必要です。

コンプライアンス要件移行スクリプト

これは、コンプライアンス要件を Cisco Network Assurance Engine（Cisco NAE）リリース 5.1 から Cisco Nexus Dashboard Insights リリース 6.0.x の特定のサイトグループに移行するスクリプトです。

オフライン サイトの PSIRT、Field Notice、EOL アドバイザリを表示するスクリプト

これは、オフラインサイトのPSIRT、Field Notice、EOLアドバイザリを表示するスクリプトです。また、オフラインサイトに対するシスコ推奨バージョンも表示されます。

ファイルをサイトグループにアップロードしたら、サイトグループまたはサイトを選択します。サイト グループへのファイルのアップロードとアシュアランス分析の実行を参照してください。PSIRT、Field Notice、EOL アドバイザリは、[アドバイザリの内訳（Advisories Breakdown）] 領域の **[概要ページ（Overview Page）]** に表示されます。

オフラインサイトに対するシスコ推奨バージョンを表示するには、**[ノード（Nodes）]** ページに移動します。ノードで テーブルで、オレンジ色の三角形のアイコンにカーソルを合わせると、ノードに対するシスコ推奨バージョンが表示されます。

Anomaly Score	Node	Model	Role	Type	Serial	Last Reboot Time	Firmware
Critical	ifav201-spine4 DC-IFAV201	N9K-C9336PQ	Spine	Spine	SAL18474VGN	Apr 10 2021 05:10:12.311 PM	14.2(4n)
Critical	ifav201-spine3 DC-IFAV201	N9K-C9316D-GX	Spine	Spine	FDO23300GUG	Oct 18 2021 03:36:38.957 PM	15.2(3e)
Critical	ifav201-spine1 DC-IFAV201	N9K-C9364C	Spine	Spine	FDO21520XZJ	Oct 18 2021 03:36:28.086 PM	15.2(3e)
Critical	ifav201-leaf9 DC-IFAV201	N9K-C93180YC-FX	Leaf	Remote Leaf	FDO22152M56	Oct 18 2021 03:36:40.975 PM	15.2(3e)
Critical	ifav201-leaf8 DC-IFAV201	N9K-C93180YC-EX	Leaf	Border Leaf	FDO2049171Y	Oct 18 2021 03:26:50.508 PM	15.2(3e)

オフラインサイトのファームウェアアップデート分析用スクリプト

このスクリプトは、必要な引数が指定されている場合に、オフライン サイトのファームウェア アップデート分析に必要な追加情報を Cisco APIC から収集します。

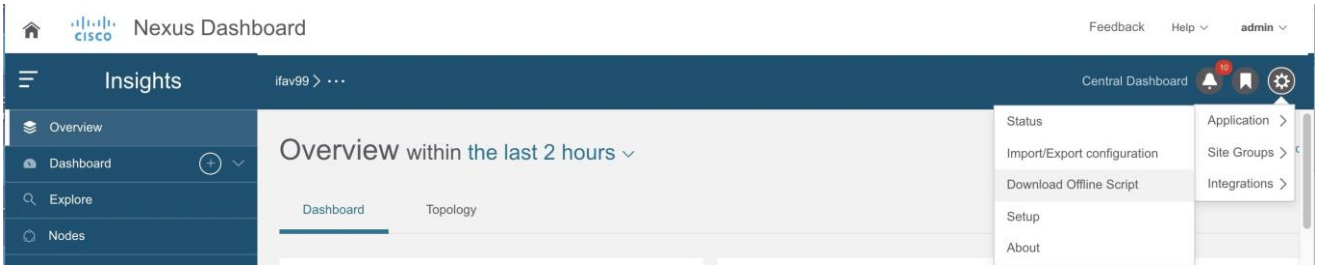
サイト グループへのファイルのアップロードとアシュアランス分析の実行

この手順では、Cisco Nexus Dashboard Insights でサイト グループを追加し、データ収集タイプが**アップロード ファイル**であるファイルをサイト グループにアップロードします。次に、サイトグループのアシュアランス分析を実行します。

前提条件

必要に応じて、Pythonスクリプトをダウンロードして、アシュアランスのためのデータを収集します。

Cisco Nexus Dashboard Insights の **[概 要 （ Overview ）]** ページで、[設定（Settings）] アイコンをクリックし、[**オフライン収集スクリプトのダウンロード**（Download Offline Collection Script）] を選択して、Python スクリプトをダウンロードします。ダウンロードしたスクリプトを実行して、アシュアランスのためのデータを収集します。



Pythonオフラインデータ収集スクリプトは、Mac OSまたはCentosOSでのみサポートされています。Windows サーバからスクリプトを実行すると、エラーが発生し、Cisco Nexus Dashboard Insights は、APIC バージョンがサポートされていないことを示します。

次の手順を使用して、ファイルをサイトグループにアップロードし、アシュアランス分析を実行します。このアシュアランス分析は、ポイントインタイムのスナップショットベースの分析です。アップロードされたファイルに対してアシュアランス分析を実行するには、最初にサイトグループを作成します。次に、データを含むファイルをアップロードして、サイトグループに関連付けます。

Cisco Nexus Dashboard Insights にファイルをアップロードしても、Cisco Nexus Dashboard Site Manager はアップロードされたファイルを認識しません。

収集したデータを含むファイルをアップロードし、サイトグループに関連付けます。

作成済みのCisco Nexus Dashboard Insightsサービスにサイトグループがない場合、サービスを開始すると **[有効なサイトグループがありません（No Site Group enabled）]** ページが表示されます。**[サイト グループの構成**（Configure Site Group）] タブをクリックし、以下の手順に従います。Cisco Nexus Dashboard Insights を開始したときにサイトグループがすでに設定されている場合は、**[概 要（Overview）]** ページが表示されます。

次の手順に従って、サイトグループにファイルを追加します。

1. 右上の [設定（Settings）] アイコン > **[サイトグループ（Site Groups）]** > **[管理（Manage）]** の順に選択します。
2. **[サイトグループの管理（Manage Site Groups）]** ページで、**[新しいサイトグループの追加（Add New Site Group）]** をクリックします。

3. **[新しいサイト グループの追加（Add New Site Group）]** ダイアログボックスの **[全般（General）]** エリアで、サイト グループの名前と説明を追加します。
4. **[構成（Configuration）]** エリアの **[データ収集タイプ**（Data Collection Type）] エリアで、**[ファイルのアップロード**（Upload File）] を選択します。これで、このサイトグループに追加するファイルをアップロードできます。
5. **[サイト（Site）]** フィールドに名前を追加します。
6. **[ファイルを選択するか、ここでドラッグアンドドロップする（Select a file or drag and drop it in here）]**
エリアで、ファイルを選択するか、ドラッグアンドドロップします。許可されるファイルは .gz です。
7. [保存（Save）] をクリックします。ファイルがサイトグループに追加されます。

次の手順に従って、サイトグループのアシュアランス分析を実行します。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。
3. [サイトグループの構成（Configure Site Group）] **ページにある** [全般（General）] **タブの** [サイト（Sites）] **で、ファイルの** [収集ステータス（Collection Status）] **が** あなたのファイルが有効になっています。
4. **[アシュアランス分析（Assurance Analysis）]**
タブをクリックし、アップロードしたファイルを見つけて、**[オフライン分析の実行（Run Offline Analysis）]**
タブをクリックして、1 回限りのインスタント分析を実行します。
5. 分析が完了したら、**[概要（Overview）]** ページの **[アラート検出タイムライン（Alert Detection Timeline）]**
エリアで、アップロードされたファイルのデータが収集されたときのスナップショット時刻を選択します。

スナップショットは、アップロードされたファイルで分析が実行されたときではなく、アップロードされたファイルのデータが収集されたときに追加す

る必要があります。

6. **[適用（Apply）]** をクリックしてアラートを表示します。

サイトグループのアシュアランス分析の設定に関するガイドラインと制約事項

- Cisco Nexus Dashboard Insightsでは、ACIファブリックとDCNMファブリックが同時にサポートされますが、サイトグループへの追加については、同種のファブリックタイプのみサポートされています。1つのサイトグループでは、1つのサイトタイプのみサポートされます。サイトグループ内でACIサイトとDCNMサイトを組み合わせることはできません。
- サイトグループにサイトを追加するには、最初に Cisco Nexus Dashboard **サイトマネージャでサイトを追加する必要があります**。その後、サイトグループでサイトを有効にできます。
- サイト
  グループからアシュアランス分析を取得し、rawデータセットをエクスポートしてファイルをサイト
  グループにアップロードする場合、アップロードされたファイルのアシュアランス分析ではアシュアランス関連の異常のみ生成されます。
- 現在、Cisco Nexus Dashboard Insightsでアップロードされたファイルサイトのアシュアランス分析を開始する場合、すでに進行中のサイトのアシュアランス分析を同時に続行できます。アシュアランス分析はすべて、動作を中断することなく実行されます。
- サイトグループに複数のファイルがある場合は、特定のサイトを選択し、そのサイトでアシュアランス分析を実行します。アップロードされたファイルについては、オンデマンドでアシュアランス分析を実行する必要があります。アシュアランス分析は、同じデータに対して複数回実行できます。
- アップロードされたファイルのアシュアランス分析では、特定のサイトグループにファイルをアップロードすると、そのファイルを別のサイトグループに関連付けることはできません。
- アラートルールとコンプライアンスルールは、アップロードされたファイルのアシュアランス分析で有効です。
- **[サイトグループの構成（Configure Site Group）]** > **[アシュアランス分析（Assurance Analysis）]** ページでは、15分ごとに実行するようにデフォルトの頻度率が設定されています。スケジュールしたジョブがキューに入っていることがわかった場合、または頻度がジョブの完了にかかる時間よりも短い時間に設定されている場合は、ジョブを調整します。つまり、ジョブが重複せず、次のジョブがスケジューラ キューに追加される前にスケジューラが 1つのジョブを完了できるように、頻度の時間間隔を増やします。頻度率は30分に設定することをお勧めします。

サイトグループの管理

このセクションでは、サイトグループと統合からサイトを編集または削除する方法について説明します。

サイトグループ内のサイトの編集

サイトグループ内のサイトを編集するには、次の操作を実行します。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. 右上の [設定（Settings）] アイコン > **[サイトグループ（Site Groups）]** > **[管理（Manage）]** の順に選択します。
3. **[サイトグループの管理（Manage Site Groups）]** ページの **[サイトグループ（Site Groups）]** タブで、編集するサイトに関連付けられている [アクション（Actions）] メニューをクリックし、**[編集（Edit）]** を選択します。
4. **[サイトグループの編集（Edit Site Group）]** ページでサイトを変更し、**[保存（Save）]** をクリックして編集内容を保存します。

サイトグループのサイトの削除

サイトグループからサイトを削除するには、次の操作を実行します。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. 右上の [設定（Settings）] アイコン > **[サイトグループ（Site Groups）]** > **[管理（Manage）]** の順に選択します。
3. **[サイトグループの管理（Manage Site Groups）]** ページの **[サイトグループ（Site Groups）]** タブで、編集するサイトの右側にある [アクション（Actions）] メニューをクリックし、**[編集（Edit）]** を選択します。
4. **[サイトグループの編集（Edit Site Group）]** ダイアログボックスで、編集するサイトの右側にある **[x]** をクリックし、**保存してサイトを削除します。**

または、次の手順でサイトグループからサイトを削除できます。

1. **[概要（Overview）]** ページで、選択したサイトグループ名の横にある [アクション（Actions）] メニューをクリックし、[サイトグループの構成（Configure Site Group）] **を選択します。**
2. **[全般（General）]** タブで、**[サイトグループの編集（Edit Site Group）]** をクリックします。
3. 編集するサイトの右側にある **[x]** をクリックし**[保存（Save）]** をクリックしてサイトを削除します。

削除するサイトがサイトグループにある最後のサイトの場合、すべてのサイトグループに少なくとも 1 つのサイトを含める必要があるため、サイトグループ全体を削除する必要があります。

サイトグループにある最後のサイトの削除

サイトグループとその最後のサイトを削除するには、次の操作を実行します。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. 右上の [設定（Settings）] アイコン > **[サイトグループ（Site Groups）]** > **[管理（Manage）]** の順に選択します。
3. **[サイトグループの管理（Manage Site Groups）]** ページの **[サイトグループ（Site Groups）]** タブで、削除するサイトに関連付けられている [アクション（Actions）] メニューをクリックし、**[削除（Delete）]** を選択します。

サイトグループと最後に残っていたサイトが削除されます。

サイトの削除後に修正措置を実行し、そのサイトを再び追加する場合は、Nexus Dashboard Insights のサイト追加手順に従ってください。

サイトグループからのアップロードされたファイルの削除

アップロードされたファイルと関連サイトをサイトグループから削除するには、次の操作を実行します。

1. **[概要（Overview）]** ページで、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。
3. **[サイトグループの構成（Configure Site Group）]** 画面で、**[ファイル管理（File Management）]** タブをクリックします。
4. 削除するサイトの右側にある削除アイコンをクリックします。

サイトグループからアップロードされたファイルを削除すると、関連付けられているサイトも削除されます。

統合

統合の詳細については、次のセクションを参照してください。

- Nexus Dashboard Orchestratorの統合
- DNSの統合
- AppDynamicsの統合について
- vCenter の統合

サイトグループの設定

バグスキャン

バグスキャン機能を使用すると、バグスキャンをスケジュールしたり、ネットワーク上でオンデマンドバグスキャンを実行したりできます。Nexus Dashboard Insightsは、すべてのノード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。詳細については、アラート の分析を参照してください。

この機能により、テレメトリデータを収集するノードを含むサイトを選択できます。CPUとメモリの使用量が設定されたしきい値を下回っている場合、テクニカルサポートログが収集され、ノードに対してスケジュールされたバグスキャンが実行されます。CPUとメモリの使用量が設定されたしきい値を超えている場合、ノードはスケジュールされたバグスキャンから除外されます。

デバイスと通信するようにサイトが適切に設定されていない場合、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。
- デバイスでオンデマンドのバグスキャン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。

デフォルトのバグスキャン

Nexus Dashboard Insightsがインストールされている場合、サービスはサイトごとにデフォルトのバグスキャンを実行します。Nexus Dashboard Insightsでサイトを有効にすると、バグスキャンのデフォルトのスケジュールと頻度が有効になります。バグスキャンのデフォルトのスケジュールは編集できます。

デフォルトのバグスキャンのスケジュールは、次のとおりです。

1. 最初のサイトがNexus Dashboard Insightsに追加されると、デフォルトのバグスキャンは、最も近い月曜日の午前12時(GMT)から週に1回スケジュールされます。
2. 新しいサイトがNexus Dashboard Insightsに追加されると、デフォルトのバグスキャンは、以前のデフォルト時刻の6時間後から週に1回スケジュールされます。スケジュールは、28のサイトで月曜日の午前12時にループバックします。

表 2. 例

サイト番号	バグスキャンスケジュール
サイト 1	週に1回、月曜日の午前12時に開始
サイト 2	週に1回、最も近い月曜日の午前6時に開始
サイト 3	週に1回、月曜日の午後12時に開始
サイト 4	週に1回、月曜日の午後6時に開始
サイト 5	週に1回、火曜日の午前12時に開始

バグスキャンのガイドラインと制約事項

- バグスキャンのスケジュール設定に推奨される時間間隔は、Cisco Nexus Dashboardの負荷、サイト内のノード数、およびテクニカルサポートファイルのサイズによって異なります。24時間にわたって100ノードでバグスキャンを実行することをお勧めします。

  たとえば、複数のサイト（サイト 1 に 100 ノード、サイト 2、サイト 3、サイト 4、サイト 5 にそれぞれ 25 ノード）がある場合、サイト 1 のバグスキャンを隔日の午前 12 時にスケジュールできます。残りのサイトを合計すると 100 ノードになるため、サイト 1 とは異なる別の日に一緒にスケジュールすることもできます。サイト2、サイト3、サイト4、およびサイト5にはそれぞれ25ノードあり、合計すると100になるため、バグスキャンは時間をずらして、午前12時から6時間ごとにスケジュールできます。前述の内容に基づいたスケジュールは次のようになります。

  1 日目

  - サイト

    1、午前12時2

    日目

  - サイト2、午前12時
  - サイト3、午前6時
  - サイト4、午後12時
  - サイト5、午後6時

    各サイトの所要時間を測定し、各サイトのバッファ時間を使用し、所要時間に応じてバグスキャンをスケジュールできます。

- スケジュールの頻度を更新後、バグスキャンのステータスが**使用不可**と表示されます。
- バグスキャンジョブが実行中で、別のバグスキャンジョブがスケジュールされている場合、2 番目のバグスキャンジョブは失敗します。

バグスキャンのスケジュール

次の手順を使用して、バグスキャンをスケジュールします。

手順

1. [サイトグループ]メニューから、サイトグループまたはサイトを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューから、**[サイトグループの構成（Configure Site Group）]** > **[バグスキャン（Bug Scan）]** の順に選択し、選択したサイトでバグスキャンをスケジュールします。

   [バグスキャン（Bug Scan）] ページが表示されます。デフォルトでは、サイトのバグスキャンは有効になっています。一般表すべてのサイトを表示します。

3. をクリックして、選択したサイトのバグスキャンジョブをスケジュールします。
4. 次のフィールドに入力します。
   a. **[有効（Enabled）]**を選択して、バグスキャンを有効にします。
   b. [開始時刻]、[頻度]、および[終了時刻]を選択します。
   c. [保存]をクリックします。
   d. [今すぐスキャン（Scan Now）] をクリックします。

   > CPU とメモリの使用率が 65% を超えている場合、ノードはバグスキャンから除外されます。

5. **[履歴（History）]**
   テーブルには、サイト名、ステータス、タイプ、ノード、開始時刻と終了時刻などのバグスキャンジョブ情報が表示されます。
6. サイドペインの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。
7. アイコンをクリックすると、**[バグスキャン（Bug Scan）]** ステータスページが表示されます。
8. （任意）進行中のジョブを選択し、**[停止（Stop）]** をクリックするとジョブを停止できます。

オンデマンドバグスキャン

次の手順を使用して、オンデマンドバグスキャンを実行します。

手順

1. [サイトグループ]メニューから、サイトグループまたはサイトを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューから、**[サイトグループの構成（Configure Site Group）]** > **[バグスキャン（Bug Scan）]** の順に選択し、選択したサイトでオンデマンドバグスキャンを実行します。

[バグスキャン（Bug Scan）]
ページが表示されます。デフォルトでは、サイトのバグスキャンは有効になっています。

3. **[全般]**テーブルには、すべてのサイトが表示されます。サイトを選択し、**[今すぐスキャン（Scan Now）]**をクリックします。

   [履歴（History）]
   テーブルには、サイト名、ステータス、タイプ、ノード、開始時刻と終了時刻などのバグスキャンジョブ情報が表示されます。

4. サイドペインの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。
5. アイコンをクリックすると、**[バグスキャン（Bug Scan）]**
   ステータスページが表示されます。
6. （任意）進行中のジョブを選択し、**[停止（Stop）]**
   をクリックするとジョブを停止できます。

収集ステータス

[概要（Overview）]
画面の上部で、サイトグループを選択します。サイトグループの横にある
[アクション（Actions）] メニューをクリックし、**[サイトグループの設定（Configure Site Group）]** を選択して、**[データのエクスポート（Export Data）]** タブをクリックします。

[収集ステータス（Collection Status）]
ページには、ノードの収集ステータスと、各ノードでサポートされている機能とサポートされていない機能が表示されます。ノードごとに、リソース、環境、統計情報、フロー、エンドポイント、イベントなどのカテゴリの収集ステータスが表示されます。

設定の異常

[設定の異常（Configuration Anomalies）]ページには、サイトグループの設定に関連するシステムの異常が表示されます。

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

- 定期的なジョブの設定では、1日あたり最大10件の電子メールを設定できます。
- 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。
- データ収集タイプ**ファイルのアップロード**では、データのエクスポートはサポートされていません。サイトグループへのファイルのアップロードとアシュアランス分析の実行を参照してください。
- **[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。
- **[アラートとイベント（Alerts and Events）]** と および使用法。
- 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。

収集タイプごとの Kafka Exporter の構成：アラートとイベント

次の手順を使用して、Kafka Exporterを設定します。

1. **[概要（Overview）]** 画面の上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの設定（Configure Site Group）]** を選択して、**[データのエクスポート（Export Data）]** タブを選択します。
3. **[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 **[サイト名（Site Name）]** フィールドで、適切なサイトを選択します。
   b. **[IP アドレス（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。
   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。
4. 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。
5. **[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 の設定

次の手順を使用して、Kafka Exporterを設定します。

1. **[概要（Overview）]** 画面の上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの設定（Configure Site Group）]** を選択して、**[データのエクスポート（Export Data）]** タブを選択します。
3. **[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 **[サイト名（Site Name）]** フィールドで、適切なサイトを選択します。

b. **[IP アドレス（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。

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。

4. [**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 **[リソース（Resources）]** 設定が表示されます。

   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。

5. **[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。

[サイトグループの設定（Configure Site Group）] ページの **[データのエクスポート（Export Data）]** タブにある **[メッセージバス構成（Message Bus Configuration）]** エリアに、エクスポートジョブの詳細が表示されます。このエリアには、サイト名、IP アドレス/ポート、トピック名、収集タイプ、カテゴリなどの詳細が表示されます。Kafka エクスポートのステータスは、**[有効（Enabled）]** または **[失敗（Failed）]** としてここに表示されます。

電子メールの設定

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

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの設定（Configure Site Group）]** を選択して、**[データのエクスポート（Export Data）]** タブをクリックします。
3. **[電子メール（Email）]** エリアで **[新規追加（Add New）]** をクリックし、次の操作を実行します。

   a. **[全般設定（General Settings）]** 領域の **[サイト名（Site Name）]** フィールドで、サイト名を選択します。

   b. **[名前（Name）]** フィールドに、名前を入力します。

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。

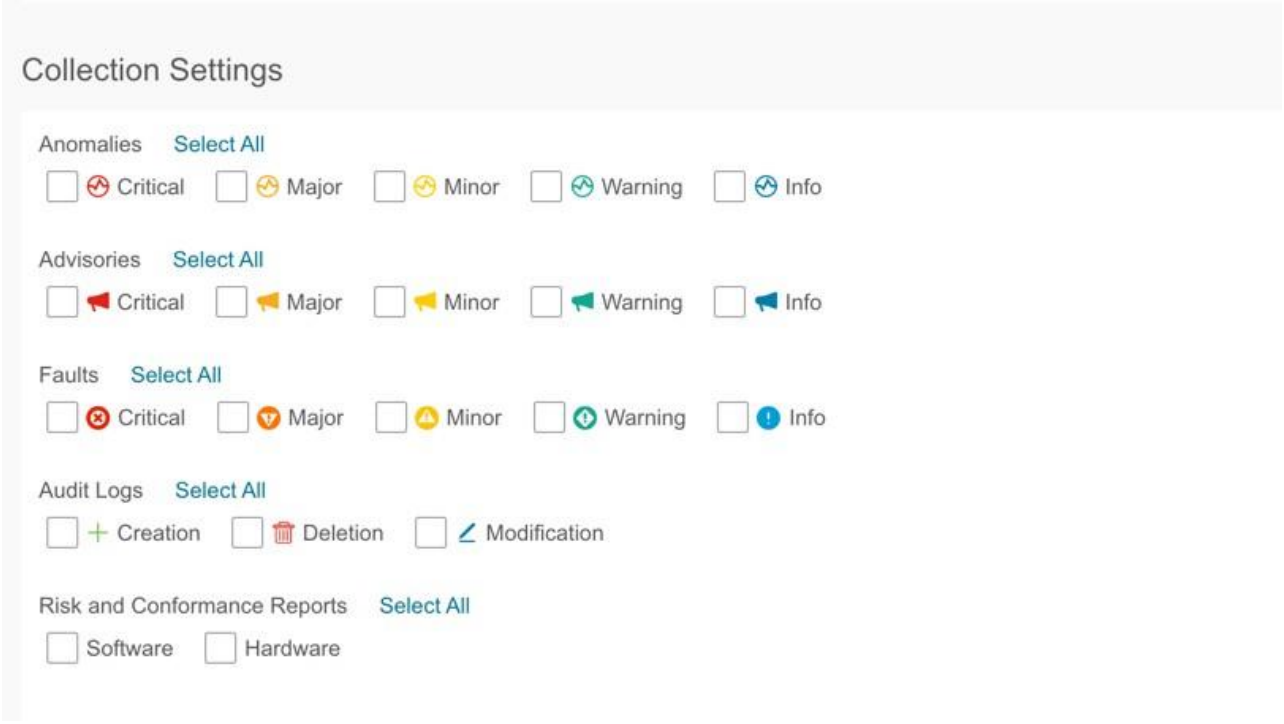
e. **[開始日（Start Date）]** フィールドに、開始日を入力します。

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。

4. 各カテゴリの **[収集設定（Collection Settings）]** エリアで、異常、アドバイザリ、および障害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。**[監査ログ（Audit Logs）]** については、作成、削除、および変更のオプションを選択します。**[リスクおよび適合性レポート（Risk and 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。「リスクおよび適合性レポート」を参照してください。



5. [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。

6. (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。

リスクおよび適合性レポート

リリース 6.0.2 以降、リスクおよび適合性レポートはサイトごとに毎日生成されるようにスケジュールされており、電子メールスケジューラを設定することで最新のレポートを登録できます。「電子メールの設定」を参照してください。

Nexus Dashboard Insightsリリース6.1.1以降、適合性ダッシュボードでも最新のレポートを確認できます。ソフトウェアおよびハードウェアの適合性ダッシュボードを参照してください。

リスクおよび適合性レポートには、ソフトウェアリリース、ハードウェアプラットフォーム、およびソフトウェアとハードウェアの適合性の組み合わせを含む、サイトの全体的なインベントリのステータスが表示されます。

リスクおよび適合性レポートには、次の情報が含まれています。

- 電子メールスケジューラで指定されたタイムスタンプ
- 対象サイト
- 電子メールスケジューラで指定された頻度
- デバイスの重大度の分類
- ノード名
- ソフトウェアおよびハードウェアの適合性ステータス
- シリアル番号
- IP アドレス
- ソフトウェアバージョン
- ハードウェアモデル
- ソフトウェアおよびハードウェアのEOL日

リスクおよび適合性レポートには、ソフトウェアおよびハードウェアコンポーネントの詳細なリストも含まれています。ハードウェアコンポーネントについては、スイッチ、ラインカード、ファン、電源装置などのモジュールもリストされています。

リスクおよび適合性レポートでは、デバイスは、ソフトウェアリリースまたはハードウェア

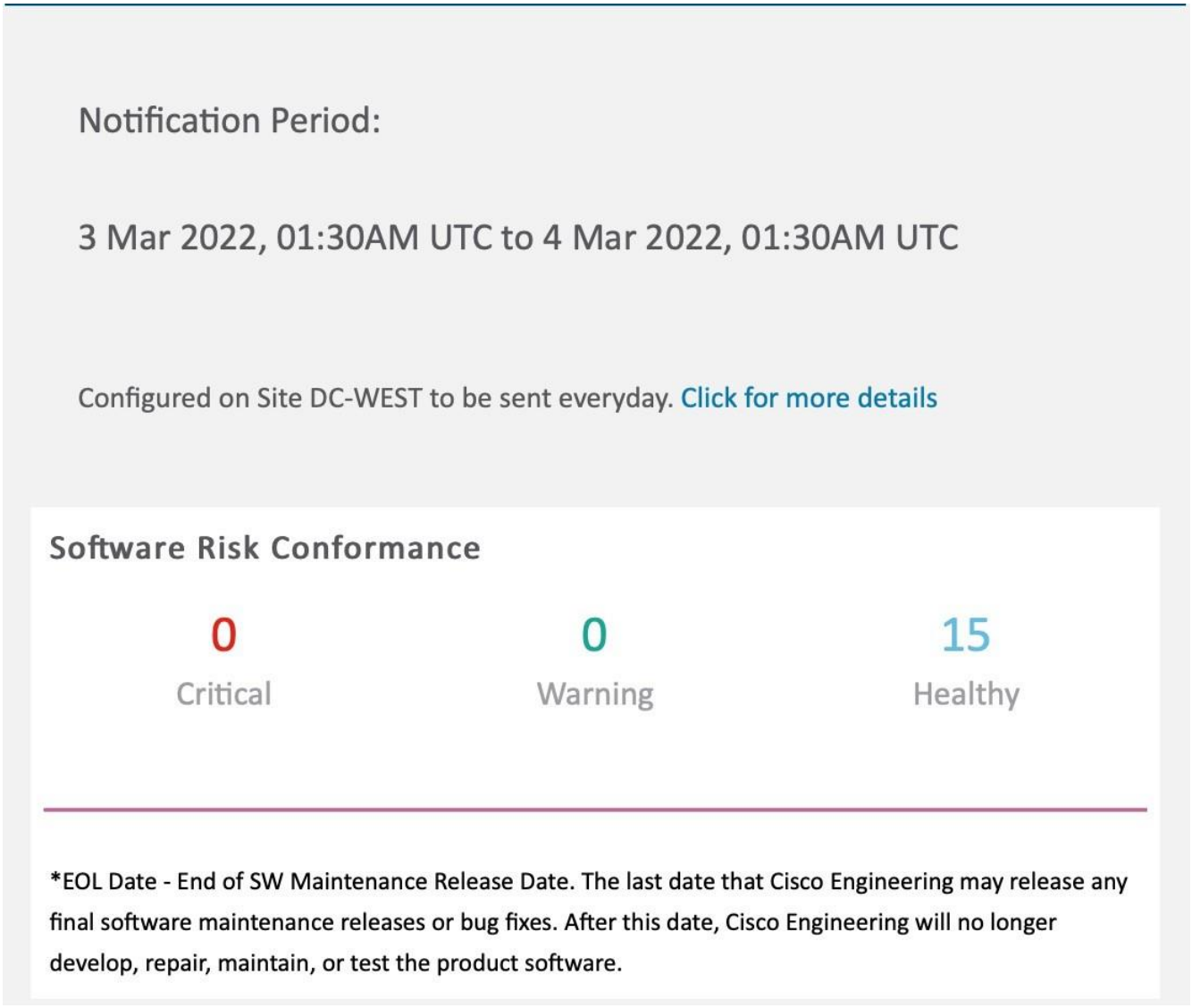
プラットフォームのEOL日とPSIRTの終了日に基づいて、次の3つの重大度に分類されます。重大度には次のものがあります。

- クリティカル: EOL日は本日から3ヵ月未満です。
- 警告: EOL日は本日から3～9ヵ月です。
- 正常: EOL日は本日から9ヵ月以上先か、EOLがアナウンスされていません。

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します。

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。

ソフトウェアのリスクおよび適合性レポートの例



ハードウェアのリスクおよび適合性レポートの例

Notification Period:

3 Mar 2022, 01:31AM UTC to 4 Mar 2022, 01:31AM UTC

Configured on Site DC-WEST to be sent everyday. Click for more details

Hardware Risk Conformance

8	0	7
Critical	Warning	Healthy

Critical (EOL less than 3 months from now)

Node Name	Serial	IP	Hardware Model	EOL Date
ifc-1	FCH2210V0HQ	192.168.0.1	APIC-SERVER-M2	2020-06-19
ifc-2	FCH2220V0HQ	192.168.0.2	APIC-SERVER-M2	2020-06-19
ifc-3	FCH2230V0HQ	192.168.0.3	APIC-SERVER-M2	2020-06-19
scaleleaf-207	FDO220720HC	192.168.0.207	N9K-C93128TX2	2018-10-30
scaleleaf-208	FDO220820HC	192.168.0.208	N9K-C93128TX2	2018-10-30
scaleleaf-209	FDO220920HC	192.168.0.209	N9K-C9372PX	2019-02-03
scaleleaf-210	FDO221021HC	192.168.0.210	N9K-C9372PX	2019-02-03
scalespine-602	SAL60260MHM	192.168.2.94	N9K-C9336PQ	2020-03-04

*EOL Date - End of SW Maintenance Release Date. The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.

ソフトウェアとハードウェアのリスクおよび適合性レポートの例

Notification Period:

3 Mar 2022, 01:32AM UTC to 4 Mar 2022, 01:32AM UTC

Configured on Site DC-WEST to be sent everyday. Click for more details

Software-Hardware Risk Conformance

8	0	7
Critical	Warning	Healthy

Critical(EOL less than 3 months from now)

Node Name	SW Conformance	HW Conformance	Serial	IP	SW Version	HW Model	SW EOL Date	HW EOL Date
ifc-1	healthy	critical	FCH2210V0HQ	192.168.0.1	4.2(5)	APIC-SERVER-M2		2020-06-19
ifc-2	healthy	critical	FCH2220V0HQ	192.168.0.2	4.2(5)	APIC-SERVER-M2		2020-06-19
ifc-3	healthy	critical	FCH2230V0HQ	192.168.0.3	4.2(5)	APIC-SERVER-M2		2020-06-19
scaleleaf-207	healthy	critical	FDO220720HC	192.168.0.207	14.2(4p)	N9K-C93128TX2		2018-10-30
scaleleaf-208	healthy	critical	FDO220820HC	192.168.0.208	14.2(4p)	N9K-C93128TX2		2018-10-30
scaleleaf-209	healthy	critical	FDO220920HC	192.168.0.209	14.2(4p)	N9K-C9372PX		2019-02-03
scaleleaf-210	healthy	critical	FDO221021HC	192.168.0.210	14.2(4p)	N9K-C9372PX		2019-02-03
scalespine-602	healthy	critical	SAL60260MHM	192.168.2.94	14.2(4p)	N9K-C9336PQ		2020-03-04

*EOL Date - End of SW Maintenance Release Date. The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.

ソフトウェアおよびハードウェアの適合性ダッシュボード

ナビゲーションウィンドウから、**[コンプライアンス（Compliance）]** > **[ソフトウェア/ハードウェア適合性（Software/Hardware Conformance）]**を選択して、[適合性（Conformance）] ダッシュボードにアクセスします。

- ソフトウェアおよびハードウェアの適合性ダッシュボードには、サイトの適合性インベントリ全体のステータスのグラフィカルビューが表示されます。ソフトウェアリリース、ハードウェア
  プラットフォーム、およびソフトウェアとハードウェアの適合性の組み合わせについ

て、18ヵ月間の適合性を確認できます。

適合性ダッシュボードでは、ノードは、ソフトウェア リリースまたはハードウェア プラットフォームの EOL 日と PSIRT の終了日に基づいて、[正常（Healthy）]、[警告（Warning）]、[クリティカル（Critical）] の重大度に分類されます。

- このページには、ノードの適合性も表形式で表示されます。

  [ノード（Nodes）]テーブルには、ノードの名前、全体的な適合性、ソフトウェア適合性、ハードウェア適合性、IPアドレス、シリアル番号、モデル番号、ソフトウェアバージョンなどの情報が表示されます。[ノード]テーブルは、ノードの全体的な適合性によってソートされています。ノードをクリックして、追加の詳細を表示します。

- フィルタバーを使用して、名前、全体的な適合性、ソフトウェア適合性、ハードウェア適合性、IPアドレス、シリアル番号、モデル番号、およびソフトウェアバージョンでノードをフィルタ処理します。

  フィルタバーの有効な演算子は次のとおりです。

  - == - 完全に一致するログを表示します。この演算子の後には、テキストや記号を続ける必要があります。
  - contains - 入力されたテキストまたは記号を含むログを表示します。この演算子の後には、テキストや記号を続ける必要があります。

- 詳細レポートを表示するには、**[詳細レポートを表示（View Detailed Report）]** をクリックします。**[適合性レポート（Conformance Report）]**ページには、一般的な情報、適合性インベントリ、ソフトウェア適合性、ハードウェア適合性、全体的な適合性、ノードの詳細、モジュールの詳細などの情報が表示されます。
  - **[アクション（Actions）]** メニューの **[印刷/ダウンロード（Print/Download）]** をクリックして、レポートを PDF としてダウンロードします。
  - **[アクション（Actions）]** メニューの **[電子メールのスケジュール（Schedule Email）]** をクリックして、電子メールスケジューラを構成して最新のレポートを登録します。「電子メールの設定」を参照してください。

Syslog

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

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

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

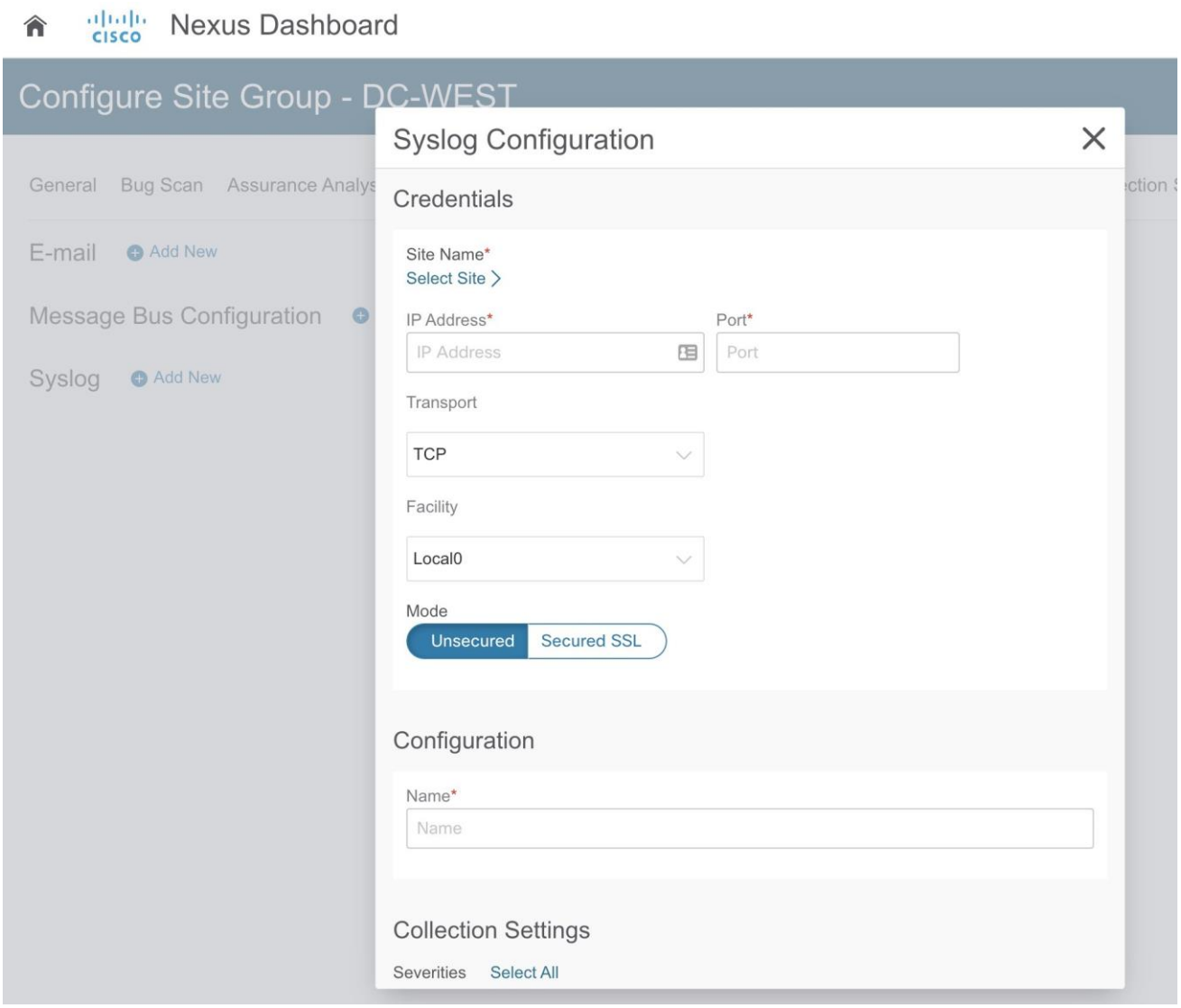
Syslog のガイドラインと制約事項

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

Syslog の設定

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

1. **[概要（Overview）]** ページの上部で、適切なサイトグループを選択し、**[サイトグループの構成**（Configure Site Group）] をクリックします。
2. サイトグループの **[サイトグループの構成（Configure Site Group）]** ページで、**[データのエクスポート（Export Data）]** タブをクリックします。
3. **[Syslog]** フィールドで、**[新規追加（Add New）]** をクリックします。
4. **[Syslog 構成（Syslog Configuration）]** ダイアログボックスの **[ログイン情報（Credentials）]** エリアで、次の操作を実行します。



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

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

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

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

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

5. **[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。
6. **[構成（Configuration）]** エリアに、エクスポートするSyslog設定の一意の名前を入力します。
7. **[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。
8. **[保存（Save）]** をクリックします。

構成が完了すると、**[サイトグループの設定（Configure Site Group）]** ページの **[データのエクスポート（Export Data）]** タブにある **[Syslog]** エリアに設定の詳細が表示されます。

アプリケーションメニュー

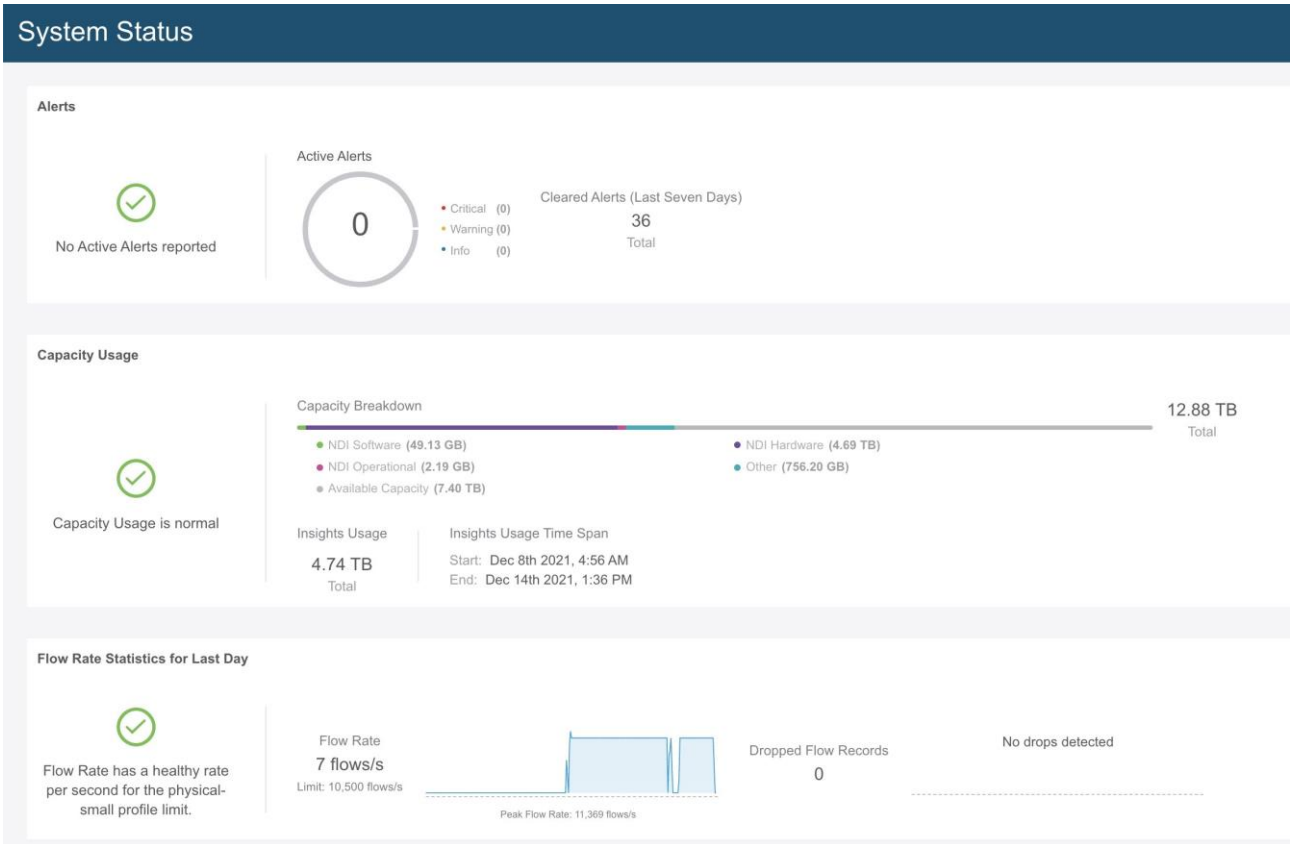
システムステータス

[システムステータス]ページには、Nexus Dashboard Insightsの[アラート]、[キャパシティ使用率]、および[フローレート統計情報]が表示されます。

Nexus Dashboard Insightsは、リソース使用率を収集し、しきい値を超えたとき、または通常動作からの急激な変化が観察されたときに、使用率、トレンド、およびアラートを表示します。

1. [設定（Settings）] アイコンで、**[アプリケーション（Application）]** > **[ステータス（Status）]** の順に選択します。

   [システムステータス]ページには、[アラート]、[キャパシティ使用率]、および[フローレート統計情報]が表示されます。



   [アラート]領域には、過去7日間にアクティブであり、クリアされたアラートが表示されます。[キャパシティ使用率]領域には、キャパシティ使用率ステータス、キャパシティの内訳、および期間が表示されます。[フローレート統計情報]領域には、フローレートが表示され、ドロップされたフローの数が追跡されます。

2. **[すべてのアラートを表示（Show All Alerts）]** をクリックして、すべてのアラートを表示します。
3. フィルタバーを使用して、アラートをフィルタ処理します。

アラート

[アラート（Alert）] テーブルには、Nexus Dashboard Insights で発生したアラートと、警告またはクリティカルに設定された重大度、ステータス、開始時刻と終了時刻、説明、推奨事項などの詳細が一覧表示されます。統計情報は、フローコレクタおよびフロー相関器から収集されます。正常性コンテナは定期的に統計情報を監視し、異常を検出するとアラートを生成します。以下のアラートは要約されています。

- **フローコレクタレベル** - フローコレクタは、30秒間の平均フローイベントと呼ばれるフローテレメトリレコードの数を報告し、2つのしきい値（一定期間の侵害に関するローカルしきい値の下限と上限）を指定します。コレクタコンテナは、ローカルのしきい値よりも多くのフローテレメトリレコードを処理しているため、負荷がかかっています。
- **フロー相関器レベル** - フロー相関器は、結合された30秒間の平均フローを報告し、2つのしきい値（一定期間の侵害に関するローカルグローバルしきい値の下限と上限）を指定します。しきい値は、固有のフローの数が増加し、システムに負荷がかかると発生します。

  ローカルの下限しきい値を超えると警告アラートが発生し、上限しきい値を超えるとクリティカルアラートが発生します。

  サービスレベルしきい値

システム異常	説明
フローコレクタレベル	フローのしきい値は次のとおりです。 • 下限しきい値 - 18000 • グローバル下限しきい値 - 54000 • 上限しきい値 - 20000 • グローバル上限しきい値 - 60000
フロー相関器レベル	フローのしきい値は次のとおりです。 • 下限しきい値 - 54000 • 上限しきい値 - 60000

キャパシティ使用率

[キャパシティ使用率]領域には、キャパシティ使用率ステータス、キャパシティの内訳、および期間が表示されます。

フローレート統計情報

Nexus Dashboard Insightsは、ファブリック内のスイッチごとのフローレートおよびドロップされたフローの数を追跡し、システムダッシュボードにフローレート統計情報を表示します。フローレー

ト、ドロップされたフローレコード、ノードフローレートなどの詳細が表示され、フローテレメトリと NetFlow に適用されます。ユーザーは、ファブリックの着信パイプラインレートをスイッチレベルごとに表示することで、特定のセットアップの着信フローレートを把握できます。

[フロー レート統計情報（Flow Rate Statistics）] エリアには、**フローレートとドロップされたフローレコード** が集約されたフローレコードとして視覚的に表示されます。フローレートは、プラットフォームに応じて変化する、パイプラインに取り込まれたフローの総数です。フローレート制限に基づいて、しきい値があります。このページのビジュアルキューは、システムが最大レートに達していることを示しています。ドロップされたフローレコードは追跡され、ドロップ数とパイプラインでの予測不可能な動作が視覚的に表示されます。この情報に基づいて、システムの異常を確認後、フィルタを調整してフローのドロップを防ぐことができます。異常の詳細については、異常の分析を参照してください。

[フローレート統計情報（Flow Rate Statistics）] 領域で **[さらに表示（Show More）]**をクリックして、**[ノードのフローレート（Node Flow Rate）]** と **[フロー（Flows）]** の詳細を展開して表示します。**[ノードのフローレート（Node Flow Rate）]**領域では、個々のノードによる1秒あたりのフローレコードのスケールを確認できます。**[フロー（Flows）]** 領域には、個々のサイトによるフロー収集の詳細が表示されます。フローの構成の詳細については、「フローの構成（Configure Flows）」を参照してください。

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。

- サイトグループ
  - サイト
  - フロー設定
  - マイクロバースト
  - 分析、バグスキャン、ベストプラクティスなどのジョブ
- 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
- ユーザー設定

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

注意事項と制約事項

- 設定をインポートまたはエクスポートするには、管理者ユーザーである必要があります。
- **ファイルのアップロード**
  データ収集タイプのサイトグループおよびサイトはサポートされていません。
- 複数のインポートジョブを同時に実行すると、予期しない結果が生じる可能性があるため、同時実行はサポートされていません。一度に1つのインポートジョブのみを実行します。
- 設定をインポートすると、Nexus Dashboard Insightsに既存の設定が追加されます。
- サイトグループ名が送信元と宛先で同じ場合、サイトグループのインポートプロセスは無視されます。
- 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。
- インポートされた設定からのホストパスワードは有効ではありません。インポートされたサイトグループの設定を正しく機能させるには、パスワードを再入力する必要があります。設定をインポートする前に、既存の設定をエクスポートして設定のバックアップを作成することをお勧めします。NAT設定は無視され、サイトグループ設定とともにエクスポートされません。
- サイトを含むサイトグループをインポートする前に、そのサイトをCisco Nexus Dashboardインスタンスにオンボードする必要があります。
  - サイトが存在しない場合、サイト設定のインポートは失敗します。

- サイトグループのサイト名が Cisco Nexus Dashboard のサイト名と異なる場合、サイト設定のインポートは失敗します。

- いずれかのサイトが別のサイトグループにある場合、サイトグループのインポートは失敗します。たとえば、既存のサイト「Site1」を持つサイトグループ「IG1」がある場合に、「Site1」を持つ「IG2」をインポートすると、IG2 のインポートは失敗し、「Site1」の構成は更新されません。
- このリリースでは、サイトグループのインポートとエクスポートは、GUI の **[メッセージバス設定（Message Bus Configuration）]** ダイアログボックスを使用した Kafka データのエクスポート機能に対して無効になっています。
- Nexus Dashboardのマルチクラスタ接続機能では、設定のインポートとエクスポートはサポートされていません。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。
- 統合では、設定のインポートとエクスポートはサポートされていません。
- 次の項目に関しては、構成のインポートおよびエクスポートはサポートされていません。
  - テンプレートベースのコンプライアンス
  - JSON/XML コンプライアンスのインポート
- 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。
- このリリースでは、構成のインポートとエクスポートは、サイトグループのsyslog構成に対してサポートされていません。

設定のエクスポート

次の手順を使用して、設定をエクスポートします。

手順

1. **[設定（Settings）]** > **[アプリケーション（Application）]** > **[構成のインポート/エクスポート（Import Export Configuration）]** の順に選択します。
2. **[新規インポート/エクスポート（New Export Configuration）]** をクリックします。
3. **[新規インポート/エクスポート（New 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設定がエクスポートされます。サイトグループ、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、ホスト上の既存の設定がすべてエクスポートされます。
5. **[インポート/エクスポート（Import/Export）]** テーブルには、エクスポートされたファイルのステータス、タイプ、コンテンツなど

の情報が表示されます。

6. エクスポートジョブのステータスが **[完了（Completed）]** に変わったら、クリック ⋯ して **[ダウンロード（Download）]** を選択します。エクスポートされた設定は、圧縮ファイルでダウンロードされます。
7. ⋯ クリックして **[削除（Delete）]** を選択し、構成を削除します。

設定のインポート

次の手順を使用して、設定をインポートします。

手順

1. **[設定（Settings）]** > **[アプリケーション（Application）]** > **[構成のインポート/エクスポート（Import Export Configuration）]** の順に選択します。
2. **[新規インポート/エクスポート（New Export Configuration）]** をクリックします。
3. **[新規インポート/エクスポート（New 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**[インポート/エクスポート]**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、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 [部分的に失敗（Partially Failed）] 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。

集中ダッシュボード

集中ダッシュボード

Cisco Nexus Dashboard の **[マルチクラスタ接続（Multi-cluster Connectivity）]** タブでは、複数のクラスタをまとめて接続し、単一のペインでクラスタとそのサイト、サービス、設定を表示、管理できます。2番目のクラスタを追加すると、クラスタのグループが形成されます。グループの作成元のクラスタは"プライマリ"クラスタとなり、グループ内の他のクラスタには適用されない多くの固有の特性を持ちます。

マルチクラスタ接続の詳細については、Cisco Nexus Dashboard ユーザーガイドを参照してください。

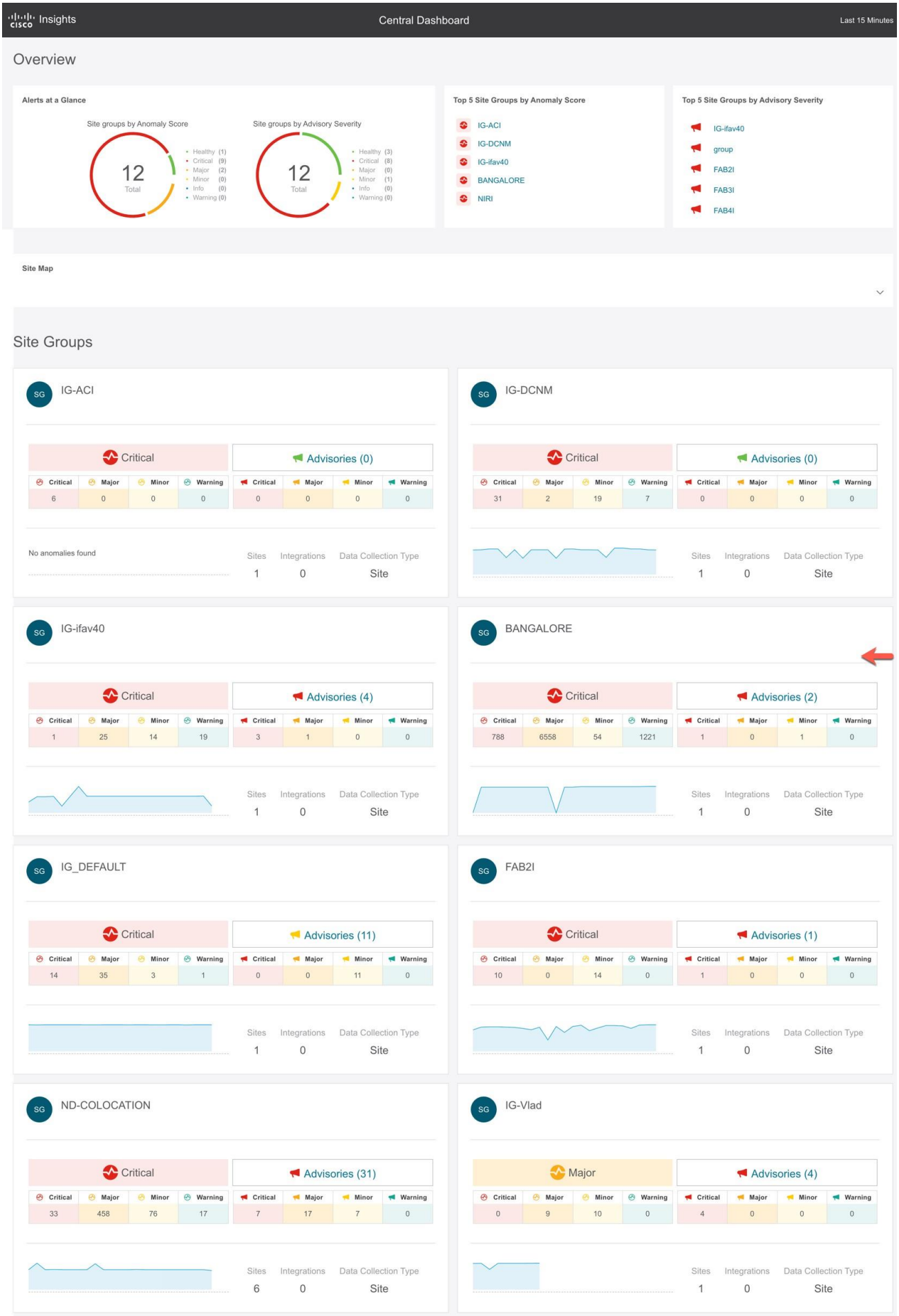
Cisco Nexus Dashboardでは、作成したクラスタグループ全体にわたるすべてのクラスタ、サイト、およびサービスを含むシステム全体の概要とステータスが **集中ダッシュボード** に表示されるため、1
つのクラスタへの接続の損失など、明らかな問題を迅速に特定できます。

Cisco Nexus Dashboardでクラスタを設定すると、Cisco Nexus Dashboard Insightsのサイトグループまたはサイトにアクセスしてすべての操作を実行できます。新しいサイトグループを追加する場合は、サイト グループの追加を参照してください。

Cisco Nexus Dashboard Insightsでは、マルチクラスタ設定で使用可能なサイトグループの概要と、そのサイトグループに関連付けられたアラート(異常とアドバイザリ)が**[集中ダッシュボード]**に表示されます。

サイト名とサイトグループ名は、マルチクラスタ設定で一意である必要があります。

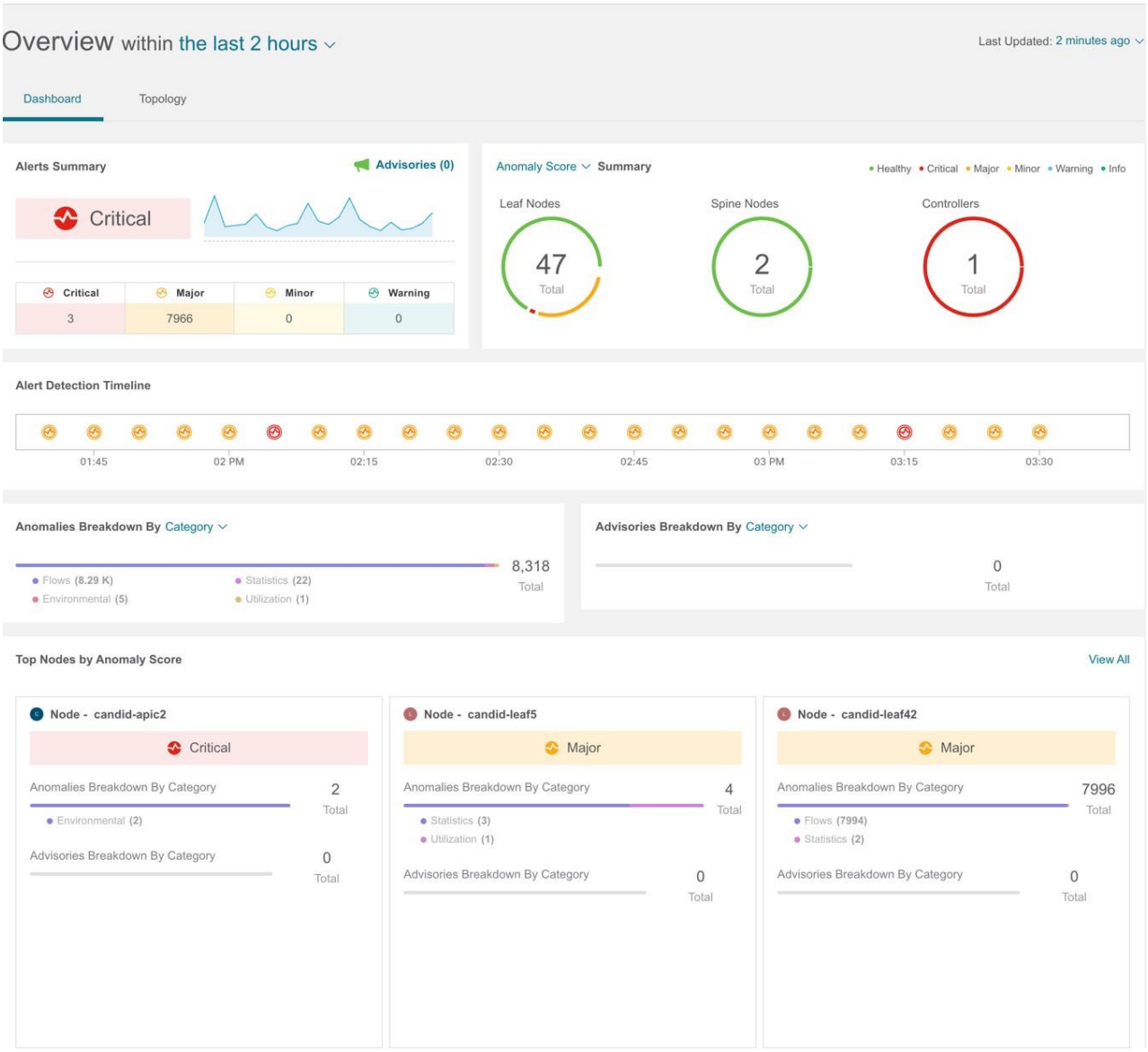
1. [Nexus Dashboard Insights] ページの右上にある **[集中ダッシュボード（Central Dashboard）]** をクリックします。



[集中ダッシュボード]の[概要]領域には、異常スコアとアドバイザリの重大度別にサイトグループが表示され、サイトマップにはサイトの場所が示されます。

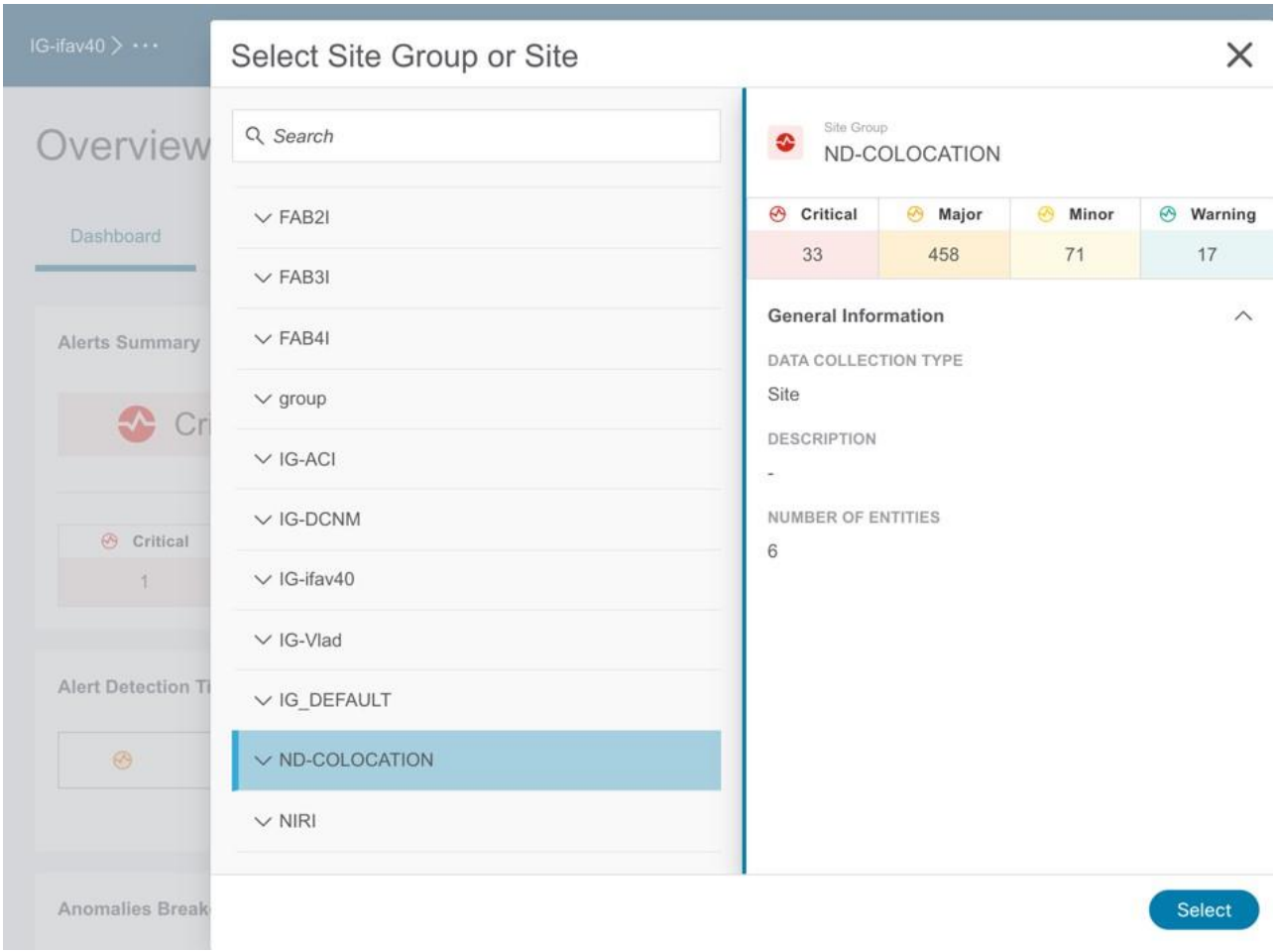
[サイトグループ]領域には、サイトグループに関連付けられた異常やアドバイザリ、サイトの数、統合、データ収集タイプなど、個々のサイトグループに関する情報が表示されます。

2. [概要]領域で [サイトグループ（Site Group）] をクリックして、そのサイトグループに関する特定の情報を [概要（Overview）] ページに表示します。
   概要（Overview）ページ



3. [サイト グループ（Site Group）] 領域で [サイト グループ（Site Group）] をクリックして、そのサイトグループに関する特定の情報を**[概要（Overview）]**ページに表示します。

4. サイトグループまたはサイトグループ内のサイト間を移動するには、上部の[サイトグループ]をクリックします。次に
   [サイトグループまたはサイトの選択（Select Site Group or Site）]**ダイアログボックスで、サイトグループまたはサイトを選択し、[選択（Select）]**をクリックします。


IG-ifav40
Overview
Dashboard
Alerts Summary
Critical
1
Alert Detection Ti
Anomalies Break
Select Site Group or Site
Search
FAB2I
FAB3I
FAB4I
group
IG-ACI
IG-DCNM
IG-ifav40
IG-Vlad
IG_DEFAULT
ND-COLOCATION
NIRI
Site Group
ND-COLOCATION
Critical
Major
Minor
Warning
33
458
71
17
General Information
DATA COLLECTION TYPE
Site
DESCRIPTION
-
NUMBER OF ENTITIES
6
Select

ダッシュボード

カスタムダッシュボード

カスタムダッシュボードを使用すると、独自のダッシュボードを作成し、ダッシュボードにビューを追加できます。カスタムダッシュボードの作業ペインには、ダッシュボードにピン留めされた各ビューに関するトップレベルの情報が表示されます。カスタムダッシュボードの数に制限はありません。

カスタム ダッシュボードの作成

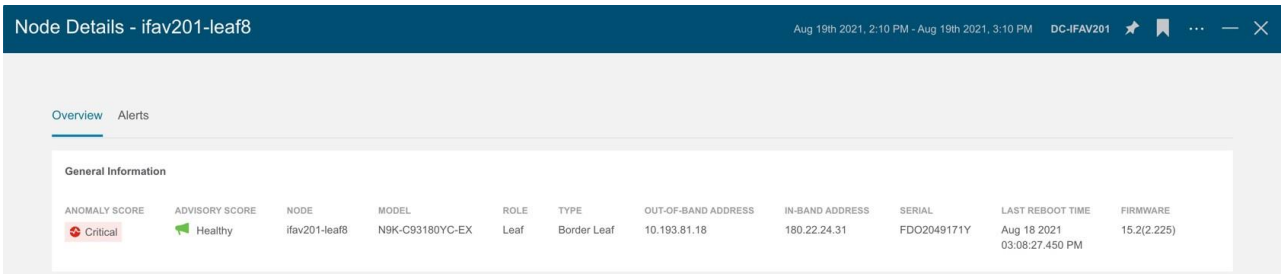
1. [+]アイコンをクリックしてカスタムダッシュボードを作成します。

2. 一意の名前を入力します。クリックして ✓ 保存します。
3. 時間範囲を選択します。**[適用（Apply）]** をクリックします。
4. (任意)名前の横にある編集アイコンをクリックして、カスタムダッシュボードの名前を編集します。
5. (任意)右側にある削除アイコンをクリックして、カスタムダッシュボードを削除します。

カスタムダッシュボードへのビューの追加

1.左側のナビゲーションウィンドウで任意のカテゴリ(ノード、リソース、フロー、エンドポイントなど)をクリックします。2.
特定のオブジェクトを選択し、 クリックして詳細ページを表示します。

3. ピンアイコンをクリックします。



4. **[ダッシュボードにピン留め（Pin to Dashboards）]**
ダイアログボックスで、次の手順を実行します。
   a. カスタムダッシュボードを選択して、既存のカスタムダッシュボードにピン留めします。
   b. **[ダッシュボードの追加**（Add

Dashboard）]をクリックして、新しいカスタムダッシュボードにピン留めします。カスタムダッシュボードの一意の名前を入力します。

5. **[保存（Save）]** をクリックします。

カスタムダッシュボードの表示

1. **[ダッシュボード（Dashboard）]** > **[カスタムダッシュボード（Custom Dashboard）]** の順に選択します。
2. 作業ウィンドウからピン留めされたビューをクリックします。

カスタムダッシュボードの各ビューには、特定のノードについてユーザーが選択した時間範囲を含む、ページのスナップショット全体が保存されます。

カスタムダッシュボードのビューの削除

1. **[ダッシュボード（Dashboard）]** > **[カスタムダッシュボード（Custom Dashboard）]** の順に選択します。
2. 作業ウィンドウでピン留めされたビューを選択します。ピンアイコンをクリックして、カスタムダッシュボードからビューを削除またはピン留め解除します。

詳細

Explore for ACI について

Explore 機能により、Cisco APIC からのポリシースナップショットが分析されます。これにより、データセンターのオペレータやアーキテクトは以下のことができます。

- ACIオブジェクトモデルと関連付けの調査
- ネットワーク資産間の接続とセグメンテーションの検証

Explore機能を使用すると、ネットワークオペレータは、使いやすい自然言語クエリ形式でアセットとそのオブジェクトの関連付けを検出できます。オペレータは、インフラストラクチャと、アセット間の接続またはセグメンテーションをすばやく可視化できます。**Explore** 機能を使用すると、オペレータは、VRF、EP、VLAN などの従来のネットワーク構造と ACI オブジェクトモデルとの関連付けを簡単に検出できます。

Explore機能は、自然言語のクエリインターフェイスをベースとしています。この機能でサポートされるクエリのタイプには次のものがあります。

- **What クエリ** :
  さまざまなネットワークエンティティの相互関連に関する情報を得られます。

ACIの例:

1. What EPGS は、VRF : */uni/tn-secure/ctx-secure* に関連付けられています。
2. What EP は、 INF: *topology/pod-1/paths-101/pathep-[eth1/3]* または *VRF:uni/tn-secure/ctx-ctx1 に関連付けられています。*
3. What EPG は BD: *uni/tn-secure/BD-BD1* および *LEAF: :topology/pod-1/node-103* に関連付けられています。

- **Can クエリ** : ACI ポリシー内のエンティティの相互通信に関する情報を得られます。Can クエリは、TCP、UDP、ICMP などのプロトコル、および通信に使用される送信元と宛て先ポートを使用して、ACI ポリシー内のエンティティが通信可能かどうかを判断するためにも使用されます。

例：

1. エンティティ *A* はエンティティ *B* と通信できます。
2. Can EPG: *uni/tn-secure/ap-AP0/epg-B*は、tcp dport: *80*、sport:10 で、*EPG: uni/tn-secure/ap-AP0/epg-A* と通信できます。
   スポーツ: 10

- **How クエリ**: ACI ポリシー内のエンティティ間の通信に関する詳細を提供します。

例: EPG *X* と EPG *Y* の通信方法。

- **View クエリ:** サイトグループの任意のリーフスイッチに関するインターフェイスステータスを視覚的に示します。

例: リーフ *X* のインターフェイスの表示。

使用例

- **設計検証:** アドホッククエリモデルを使用すると、オペレータはインフラストラクチャを迅速に理解して推論できます。自然言語クエリモデルは、検索結果と関連付けを理解しやすい表形式で返します。オペレータは、単一の簡潔なビューで、設計検証の質問に答えたり、組織のベストプラクティスからの逸脱を発見したりできます。
- **軽量な簿記:** 管理および保守チームは、ポリシーとネットワークインフラストラクチャの現在の状態をオンデマンドで可視化できるため、インベントリ、簿記、およびアセットトラッキングの手順を軽量化できます。
- **接続性とセグメンテーション:** アセットのペアまたはアセットのコンテナ間の接続性に関する質問に簡単に答えます。たとえば、EPG のグループを隔離する必要がある場合、ポリシーが正しく設定されていれば、**Can** クエリはすぐに応答できます。

ワークフロー

[Explore]
ページには、クエリに基づいたすべてのセキュリティ、転送、およびエンドポイントの問題の統合ビューが表示されます。

クエリを作成することで、エンティティ間の接続を調査できます。Canクエリでは、エンティティが相互に通信できるかどうか、および接続の正常性が判断されます。**[How クエリ（How do they talk?）]**エリアでは、エンティティ間の通信に使用される設定と接続の正常性が表示されます。

[Explore]
ページでは、ヘッダーで見つかった、選択したサイトグループ内の最初のサイトにデフォルトで設定されます。サイトの最新のスナップショットを選択し、モデルを生成します。モデルに十分なデータがあれば、入力ボックスに入力してクエリを開始できます。

Can クエリの結果

Can クエリの結果は、**放射状ビュー**に表示されます。**放射状ビュー**には、Canクエリの関連付けビューと接続ビューが表示されます。関連付けビューでは、内側と外側の放射状バンドを使用して、さまざまなオブジェクト間の関連付けを調査できます。接続ビューでは、単一の放射状バンドを使用して、プレフィックスまたはEPGをエンティティ

として表示できます。

[ビューコントロール（View Controls）] を使用すると、放射状ビューに表示される情報をフィルタ処理できます。EPGビューには、APICポリシーで設定されているさまざまなEPG間の接続情報が表示されます。プレフィックスビューには、APICポリシーで設定されているプレフィックスまたは学習したプレフィックス間の接続情報が表示されます。オブジェクトビューには、テナントやVRFなどのさまざまなオブジェクト間の関連付けが表示されます。正常性ビューには、接続の正常性が表示されます。接続は正常な場合と異常な場合があります。

デフォルトの放射状ビューには、EPGの接続と正常性が表示されます。

放射状ビューのさまざまなコンポーネントは、さまざまなタイプの情報を表します。

- **[ビューコントロール（View Controls）]** で、EPG、テナント、および両方を選択した場合、外側のリングはテナントを表し、内側のリングはアプリケーション プロファイルを表し、中央の弧線は契約の健全性。
- **[ビューコントロール（View Controls）]** で、EPG、VRF、および両方を選択した場合、外側のリングはVRFを表し、内側のリングはブリッジドメインを表し、中央の弧線は契約の状態を示します。
- **[ビューコントロール（View Controls）]** で、プレフィックス、VRF、および両方を選択した場合、外側のリングはVRFを表し、内側のリングはブリッジドメインまたはL3Outを表し、中央の弧線は契約の状態を示します。

弧線の色は、異常の重大度に対応しています。赤色の線はクリティカルな異常、オレンジ色はメジャーな異常、黄色はマイナー異常、緑色は警告と情報の異常を示します。

GUI の **[How クエリ（How do the talk）]** エリアには、結果が **[接続（Connectivity）]** テーブル、**[プレフィックス（Prefix）]** テーブル、および **[異常（Anomalies）]** テーブルに表示されます。

接続は正常な場合と異常な場合があります。接続が正常な場合は、**[接続（Connectivity）]** テーブルを使用して接続の正常性を判断できます。接続が異常な場合は、**[ポリシー（Policy）]**、**[転送（Forwarding）]**、および **[エンドポイント（Endpoint）]** タブを使用すると、考えられる原因を特定できます。接続異常の考えられる原因には、セキュリティ違反、転送違反、エンドポイント違反などがあります。

EPG ペア間のフローの色は、
[ポリシー]、[転送]、および [エンドポイント] タブ。

- 赤色はクリティカルな異常を示します。
- オレンジ色はメジャーな異常を示します。
- 黄色はマイナーな異常を示します。
- 緑色は警告と情報の異常を示します。

たとえば、問題がセキュリティ違反に関連している場合、**[接続（Connectivity）]** テーブル、**[プレフィックス（Prefix）]** テーブル、および **[異常（Anomalies）]** テーブルを使用して、セキュリティの問題に関連する異常を特定できます。**[プレフィックス（Prefix）]** テーブルで、**[サブネット/ルート（Subnet/Route）]** をクリックすると、プレフィックスに関する情報を確認できます。**[異常（Anomalies）]** テーブルで異常をクリックして、問題の影響を受けるファブリック内のオブジェクト、異常に対して実行された合格または不合格のチェック、および問題を解決するための推奨手順を特定できます。

詳細については、「Can クエリの作成」と「How Do They Talk?」の表示を参照してください。エリアの表示」を参照してください。

注意事項と制約事項

- **[Explore]** ページでは、すべてのサイトを調査するための 4 つのアクティブなスナップショットがサポートされています。スナップショットは、同じユーザーまたは複数のユーザーが調査に使用できます。追加のスナップショットを調査するには、調査の前に既存のスナップショットをオフロードする必要があります。**[Explore からのスナップショットのオフロード]** ページで、オフロードするスナップショットを選択できます。このダイアログボックスは、4つのスナップショットをメモリにロードすると自動的に表示されます。
- Explore機能は、IPv4プレフィックスに対してのみサポートされています。
- Explore機能を使用して作成されたクエリはすべて一方向です。
- 分析が失敗すると、**[Explore]** ページに、エラーメッセージ *[分析が失敗しました（Analysis has failed）]* が表示されます。**Explore** のテクニカル サポート ログをダウンロードし、Cisco TAC に連絡して問題を解決してください。
  a. Cisco Nexus Dashboardで、**[運用（Operations）]** > **[テクニカルサポート（Tech Support）]** を選択し、**[アクション（Actions）]** > **[テクニカルサポートの収集（Collect Tech Support）]** を選択し、Cisco Nexus Dashboard Insights の適切なサービスを選択して、テクニカル サポート ログをダウンロードします。
  b. */data/services/app_logs/cisco-nir-logger/nae/nae/explorerService/* ディレクトリに移動して、Explore 機能のログを見つけます複数の Explore インスタンスが実行されている場合、各インスタンスのログは個別のディレクトリにあります。

```
nae-policyexplorer-0/explorer.log
nae-policyexplorer-1/explorer.lo
nae-policyexplorer-2/explorer.log
nae-policyexplorer-3/explorer.log
```

- 学習されたルートがない状態で L3extSubnet に設定されたプレフィックスは、検索バーにクエリを入力する際に、自動提案の一部として表示されません。
- Explore 機能を使用して APIC リソースを正常に調査するには、APIC ポリシーに fv:CEp などの有効なエンドポイント、または有効な EPG が含まれている必要があります。

- **[コンプライアンス（Compliance）]**
  ページでは、コントラクトに基づいたポリシーインテントを使用してコンプライアンスを判断します。
- **Explore** には次のスケール制限があります。
  - 仮想Nexus Dashboardでは、100,000の論理ルールと350,000(頂点+エッジ)のスナップショットをサポートしています。
  - 物理Nexus Dashboardでは、300,000の論理ルールと1000,000(頂点+エッジ)のスナップショットをサポートしています。

Whatクエリの作成

次の手順を使用し、Explore機能を使用してWhatクエリを作成します。このクエリは、"どのエンティティが相互に関連付けられていますか" という質問に答えるのに役立ちます。

手順

1. **[概要（Overview）]** ページで、適切な [サイトグループ（Site Group）] > [サイト（Site）] の順に選択します。
2. 左側のナビゲーションで、**[Explore]** タブをクリックします。
3. **[タイムライン（Timeline）]** で、分析用のスナップショットを選択します。スナップショットを選択すると、調査するデータがオンデマンドで読み込まれます。
4. モデルを生成し、十分なデータがあれば、入力フィールドにクエリを入力できます。

   a.[クエリセレクタ（Query Selector）] フィールドに、**What** クエリを入力します。クエリには、**検索** バーで使用できる1つ以上のエンティティがある2つのグループを含める必要があります。「サポートされているクエリ」を参照してください。デフォルトでは、**What** エンドポイントが Any クエリビューに関連付けられています。

クエリの結果がページに表示されます。ドリルダウンして関連するエンティティを表示することもできます。送信元および接続先リストに追加できます。(送信元は宛先と通信できますか)

[どのエンティティが通信できますか（In the What entities can talk?）] 領域には、追加のフィルタリングのために **[ビューコントロール（View Controls）]** とともに放射状の構造が表示されます。必要に応じて、放射状の構造の内側をクリックして詳細情報を取得します。詳細を表示するには、**[クエリ結果（Query Results）]** テーブルのエンティティをクリックします。結果テーブルの数字をクリックして、ACIポリシーのエンティティに関する詳細を表示します。

異常とアラートの詳細については、アラートの分析を参照してください。

クエリを作成し、どのように話すかを表示します。エリア

次の手順を使用し、Explore機能を使用してクエリを作成します。Canクエリでは、「2つ

のエンティティは相互通信できますか」の質問に対する回答が得られます。

手順

1. **[概要（Overview）]** ページで、適切な [サイトグループ（Site Group）] > [サイト（Site）] の順に選択します。
2. 左側のナビゲーションで、**[Explore]** タブをクリックします。
3. **[タイムライン（Timeline）]** で、分析用のスナップショットを選択します。スナップショットを選択すると、調査するデータがオンデマンドで読み込まれます。
4. モデルを生成し、十分なデータがある場合は、次の操作を実行します。
   a. [クエリセレクタ（Query Selector）] フィールドに、**Can** クエリを入力します。クエリには、ACIポリシーからの 1 つ以上のエンティティがある 2 つのグループを含める必要があります。詳細については、「サポートされているクエリ」を参照してください。

   > 送信元エンティティが宛先エンティティと通信できるか確認するために、自動チェックが実行されます。**[リバース クエリ（Reverse Query）]** をクリックすると、クエリの送信元エンティティと接続先エンティティを逆にできます。

   b. 詳細については、**[ビューコントロール（View Controls）]** を使用してさまざまなエンティティを選択してください。

放射状の構造がレンダリングされます。必要に応じて、放射状の構造にドリルダウンして、より詳細な情報を取得できます。放射状の構造の下にある **[通信方法（How do they talk?）]** エリアには、2 つのエンティティの相互通信方法が表示されます。関連ポリシー、転送、およびエンドポイント情報が、関連する異常とともにテーブルに表示されます

フローの色は、**[ポリシー（Policy）]**、**[転送（Forwarding）]**、および **[エンドポイント（Endpoints）]** タブでの異常の最大重大度を示します。各タブのアイコンの色は、対応するタブに含まれる個別の異常の重大度を示します。

- 赤色はクリティカルな異常を示します。
- オレンジ色はメジャーな異常を示します。
- 黄色はマイナーな異常を示します。
- 緑色は警告および情報イベントを示します。
- **[ポリシー（Policy）]** タブでは、クエリに基づいてセキュリティポリシーの問題を調査できます。
- **[転送（Forwarding）]** タブでは、クエリに基づいてプレフィックスまたはプレフィックスのペアを調査できます。
- **[エンドポイント（Endpoints）]**

タブでは、クエリに基づいてエンドポイントの問題を調査できます。

クエリの結果が大きい場合は、"クエリから返されたデータが多すぎて表示できません"というメッセージが表示されます。**[ビューコントロール（View Controls）] > [詳細（Advanced）] > [EPG から（From EPG）]** および **[EPG へ（To EPG）]** 検索バーを使用して、より具体的なクエリを作成して、結果を表示します。

vzAnyなどの大きな関連付けを含むCanクエリはタイムアウトする可能性があります。ビューコントロールを使用する > **[詳細（Advanced）] > [EPG から（From EPG）]** および **[EPG へ（To EPG）]** 検索バーを使用して、より具体的なクエリを作成します。

プレフィックス間のクエリの場合、プレフィックスで共有されているEPG数が 25 を超える場合、[エンドポイント（Endpoint）] テーブルへのデータのロードに失敗し、エラーメッセージが表示されます。EPG to EPG クエリを作成して、[エンドポイント（Endpoint）] テーブルに結果を表示します。

Can クエリと How do they talk? の詳細については、ワークフローを参照してください。エリア。クエリ結果については、View クエリ結果の を参照してください。異常とアラートの詳細については、アラートの分析を参照してください。

View クエリの結果の表示

View クエリには、ACI ポリシーからの 1 つ以上のエンティティがある 2 つのグループを含める必要があります。サポートされている クエリを参照してください。

これは、リーフスイッチの特定のインターフェイスを表示できるインターフェイスクエリを実行する方法の例です。**[インターフェイス（Interface）]** ページには、物理インターフェイスの状態が表示され、クエリに基づいてサイト内のリーフスイッチのインターフェイスステータスが視覚的に示されます。**[インターフェイス（Interface）]** エリアには、一度に 1 つのリーフスイッチに関する情報が表示されます。

手順

1. **[概要（Overview）]** ページで、適切な [サイトグループ（Site Group）] > [サイト（Site）] の順に選択します。
2. 左側のナビゲーションで、**[Explore]** タブをクリックします。
3. **[タイムライン（Timeline）]** で、分析用のスナップショットを選択します。スナップショットを選択すると、ポリシー インスペクションのモデルが生成されます。
4. [クエリセレクタ（Query Selector）] フィールドに **View** と入力し、表示するインターフェイスを選択します。
5. **[ビュー コントロール（View Control）]** の適切なオプションを切り替えて必要な情報をフィルタ処理すると、**[異常（Anomalies）]** テーブルのオプションが更新されます。

リーフの物理的な表現により、さまざまなビューを切り替えて設定を表示し、以下の関連する異常を確認できます。異常をドリルダウンして、詳細を確認できます。必要に応じて、異常を個別または集約データ別に表示できます。エンドポイントが特定のインターフェイスに接続されている場合、リーフスイッチのイメージが2次元イメージとして表示されます。スイッチポートは、各ポートのステータスを表示するために色分けされています。各ポートの色は、その色による異常の重大度と一致しています。スイッチイメージにあるスイッチポートの 1 つをクリックして、そのポートに関連付けられた異常の詳細を **[異常（Anomalies）]** テーブルに表示します。

[ビューコントロール（View Controls）] エリアで切り替え可能ないくつかのオプション:

[インターフェイスの使用状況（Interface Usage）] エリアでは、インターフェイスは usage status:name: value によって分類されます。

- [設定されたインターフェイス] :
  このインターフェイスはサイトグループポリシーによって使用可能になり、EPGで使用できるようになっています。
- [部分的に設定されたインターフェイス] :
  このインターフェイスは、EPGによる消費のために割り当てることができ、未設定または部分的に設定された状態のいずれかになります。
- [使用されるインターフェイス] :
  このインターフェイスはサイトグループポリシーによって割り当てられ、EPGによって消費されます。

  デフォルトでは、**[使用されるインターフェイス（Used Interfaces）]** タブが選択されています。

[インターフェイス動作ステータス（Interface Operational Status）] では、インターフェイスは以下の動作ステータスによって分類されます。

- [動作停止] : インターフェイスは、リンク障害、エラーディセーブル、中断状態などの問題により動作が停止しています。
- [稼働中] : インターフェイスは、既知の問題がない状態で稼働しています。
- [管理上ダウン]: オペレータが管理上、インターフェイスをシャットダウンしました。

[インターフェイス動作ステータス（Interface Operational Status）] では、**[動作停止（Oper Down）]**、**[稼働中（Oper Up）]**、**[管理上ダウン（Admin Down）]** のタブがデフォルトで選択されています。

異常とアラートの詳細については、アラートの分析を参照してください。

サポートされているクエリ

次の表は、ACI の **Explore** 機能でサポートされているクエリの一覧です。

サポートされている What クエリ

表 3. サポートされている What クエリ

クエリ	エンティティ	演算子	エンティティ
関連付けられているBD	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
関連付けられている ENCAP	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
関連付けられている EPG	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF

クエリ	エンティティ	演算子	エンティティ
関連付けられているEP	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
関連付けられているINF	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
関連付けられているインベントリ	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF

クエリ	エンティティ	演算子	エンティティ
関連付けられている LEAF	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
関連付けられている VRF	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF

サポートされている Can クエリ

表 4. サポートされている Can クエリ

クエリ	エンティティ	演算子	プロトコル	接続先ポート	送信元ポート
bd_name を BD できますかと話す	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート

クエリ	エンティティ	演算子	プロトコル	接続先ポート	送信元ポート
ENCAPができる encap_name は次と通信可能か：	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート
EP ep_name はできますか と話す	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート
EPGできます epg_name は次と通信可能か：	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート

クエリ	エンティティ	演算子	プロトコル	接続先ポート	送信元ポート
INFできます inf_name は次と通信可能か：	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート
葉ができます leaf_name は次と通信可能か：	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート
VRFできます vrf_name は次と通信可能か：	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート

クエリ	エンティティ	演算子	プロトコル	接続先ポート	送信元ポート
Can Subnet subnet_name talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• [TCP] • [UDP] • ICMP	• ポート番号 • ポート範囲 • ウェルノウンポート	• ポート番号 • ポート範囲 • ウェルノウンポート
Can ANY talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • ANY	—	—	—	—

Can クエリでは、ANY のエンティティ（**[演算子（Operator）]**、**[プロトコル（Protocol）]**、**[宛て先ポート（Destination Port）]**、**[送信元ポート（Source Port）]**）はサポートされていません。

表 5. サポートされている View クエリ

クエリ	エンティティ
インターフェイスの表示	Leaf leaf_name

Nexus Dashboard Orchestrator アシュアランスを調査

このセクションを読む前に、Nexus Dashboard Orchestrator 統合についてを確認してください。

Nexus Dashboard Insights の **Explore** 機能を使用すると、ネットワークオペレータは、使いやすい自然言語クエリ形式でアセットとそのオブジェクトの関連付けを検出できます。Explore ワークフローの Nexus Dashboard Orchestrator アシュアランスは、現在、**Can EPG talk to EPG** クエリをサポートしています。このクエリには、接続を表示するために 2 つの異なる Nexus Dashboard Orchestrator ポリシーエンティティを含める必要があります。

Nexus Dashboard Orchestrator 展開よサイトグループのサイトに対してアシュアランス分析を実行後、EPG 間の関連性をナビゲートし、EPG to EPG 通信を調査し、サイト間の可視性とトラブルシューティングを有効にできます。

Exploreビューには、プログラムされたNexus Dashboard Orchestratorテンプレートまたはスキーマからの EPGの詳細が表示されます。通信可能なEPGエンティティを表示できます。エンティティは、サイト グループ内のサイト全体に広がっています。それらの接続で異常が発生した場合、それらの異常もここに表示されます。

Nexus Dashboard Orchestratorは、

1つまたは複数サイトへの設定のプッシュをサポートしています。例：

- Can EPG_1_ talk to EPG_2_.
- Can any talk to any

現在、Nexus Dashboard Orchestrator アシュアランスでは、**Can** EPG to EPG クエリのみサポートされています。**What** および **View** クエリはサポートされていません。**Can** EPG to EPG クエリの場合、プロトコルとポートに基づく追加のフィルタリングはサポートされていません。

例：

- 次はサポートされているクエリの例です。Can EPG: uni/tn-secure/ap-AP0/epg-B talk to EPG: uni/tn-secure/ap-AP0/epg-A
- 次はサポートされて**いない**クエリの例です。Can EPG: uni/tn-secure/ap-AP0/epg-B talk to EPG: uni/tn-secure/ap-AP0/epg-A on tcp dport: 80

ユーザーは、Nexus Dashboard Orchestratorアシュアランス サイトグループ内のすべてのEPGの自動提案されたクエリリストから選択できます。**Can** クエリの結果は、ACI サイトごとではなく、Nexus Dashboard Orchestrator アシュアランス サイト グループ内のすべてのサイトに関する集約ビューとして利用できます。クエリはすべてサイト全体のクエリであり、すべてのサイトにおけるアセットと関連付けの最大重大度

が結果に表示されます。

Nexus Dashboard Orchestrator の Explore に関連する注意事項

- クエリを実行後、**[接続（Connectivity）]** テーブルと **[ポリシー（Policy）]** テーブルを表示すると、EPG が対応するサイトのシャドウである場合、**[送信元 EPG（Source EPG）]** 列と **[接続先 EPG（Destination EPG）]** 列に、EPG へのシャドウタグが表示されます。例:
<epgname>(shadow)。EPGがシャドウでない場合、EPG名の後にシャドウタグは表示されません。ただし、ただし、シャドウ注釈のないバージョンの APIC/Nexus Dashboard Orchestrator を使用している場合、シャドウタグはシャドウ EPG に対しても表示されません。
- **[エンドポイント（Endpoints）]**、**[転送（Forwarding）]**、および **[ポリシー（Policy）]** テーブルで、サイトをクリックすると特定の異常の詳細を表示できます。
- **[異常（Anomalies）]** テーブルには、選択したクエリに基づいて、個別の異常、集約された異常、またはサイト間の異常が表示されます。Nexus Dashboard Orchestrator 固有の異常の詳細については、「異常」を参照してください。

Explore ワークフローの Nexus Dashboard Orchestrator アシュアランスのユースケース

- **設計検証:** 即時クエリモデルを使用すると、オペレータはインフラストラクチャを迅速に理解して推論できます。自然言語クエリモデルは、検索結果と関連付けを理解しやすい表形式で返します。オペレータは、単一の簡潔なビューで、設計検証の質問に答えたり、組織のベストプラクティスからの逸脱を発見したりできます。
- **軽量な簿記:** 管理および保守チームは、ポリシーとネットワークインフラストラクチャの現在の状態をオンデマンドで可視化できるため、インベントリ、簿記、およびアセットトラッキングの手順を軽量化できます。
- **接続性とセグメンテーション:** アセットのペアまたはアセットのコンテナ間の接続性に関する質問に簡単に答えます。たとえば、EPG
のグループを隔離する必要がある場合、ポリシーが正しく設定されていれば、**Can** クエリはすぐに明らかにできます。

Nexus Dashboard Orchestrator サイト間での Can クエリの作成

次の手順を使用し、Nexus Dashboard OrchestratorのExplore機能を使用してクエリを作成します。

はじめる前に

これで、Nexus Dashboard Orchestrator デプロイメントおよびサイトグループ内のサイトに対するアシュアランス分析の実行が完了しました。詳細については、「Nexus Dashboard Orchestrator

統合」でアシュアランス分析を有効にする方法を参照してください。

手順

1. **[概要（Overview）]** ページの左側のナビゲーションで、**[Explore]** を選択します。
2. 作業ウィンドウの上部で、適切なサイトグループを選択します。

   デフォルトでは、**[Explore]** フィールドのドロップダウンメニューには、**サイト間アシュアランスのポリシー接続**が表示されます。

3. **[スナップショット（Snapshot）]** フィールドで、分析に適したスナップショットを選択します。調査するデータはオンデマンドで読み込まれます。これで、選択した特定のスナップショットをクエリできます。

   > Explore ワークフローの Nexus Dashboard Orchestrator アシュアランスは、現在、**Can EPG talk to EPG** クエリをサポートしています。このクエリには、この接続性をチェックするために Nexus Dashboard Orchestrator ポリシーの 1 つ以上のエンティティがある 2 つのグループを含める必要があります。

4. **[検索（Search）]** バーに、Can クエリを入力します。クエリには、サポートされている1つ以上のエンティティがある2つのグループを含める必要があります。デフォルトでは、Any to Anyクエリビューが表示されます。

   > Can クエリの場合、結果は **[どのエンティティが通信できますか（Which Entities Can Talk）]** エリアに放射状に表示されます。クエリされたEPGが相互に通信できる場合、結果が表示されます。矢印の色は、接続の最大重大度を表します。クエリの結果が大きい場合は、"クエリから返されたデータが多すぎて表示できません" というメッセージが表示されます。**[単一リソースの接続を確認しますか（Would you like to check connectivity of a single resource）]** ドロップダウンリストから単一のリソースを選択して、具体的なクエリを作成します。

6. **[送信元は接続先と通信できますか（Can Source Talk to Destination）]** エリアでは、送信元が接続先と通信できるかどうかを確認できます。
7. （任意）**[リバースクエリ（Reverse Query）]** をクリックすると、クエリの送信元エンティティと接続先エンティティを逆にできます。
8. **[どのエンティティが通信できますか（Which entities Can Talk?）]** エリアの **[ビューコントロール（View Control）]** で、**[EPG]** タブをクリックして、EPG間の通信を表示します。EPGビューには、異なるEPG間の接続情報が表示されます。

   放射状ビューでは、弧線の色が異常の重大度に対応しています。

9. 放射状の構造の内側にある適切な矢印をクリックして、ページの詳細を表示します。

[通信方法（How do they talk?）] エリアで、エンティティの相互通信方法を確認します。

放射状ビューで特定の接続をクリックすると、次の表に接続の詳細が表示されます。EPGの一部としてプログラムされているポリシーを確認できます。接続の一部であるプレフィックスを確認できます。この通信によって影響を受けるエンドポイントも確認できます。

Nexus Dashboard Orchestrator サイト間アシュアランスExploreの場合、[ポリシー（Policy）] 、[転送（Forwarding）] 、および[エンドポイント（Endpoints）] テーブルに、追加の **[サイト（Sites）]** 列が表示されます。クエリの一部である各サイトの接続情報がここに表示されます。各サイトについて、生成された異常がある場合は、ここで確認できます。

たとえば、エンドポイントの一部として、 **メジャーな** 異常がある場合、クリックしてその異常を選択し、**[分析（Analyze）]** をクリックすると異常の詳細を表示できます。詳細は、Nexus Dashboard Orchestrator コンテキストで提供されます。複数のサイトでNexus Dashboard Orchestratorによってプログラムされている内容を学習し、クエリを確認して、使用されているさまざまなEPG間の通信を確認できます。

サイト間ビューには、Nexus Dashboard Orchestrator に関連付けられたサイトグループの異常が表示されます。異常の詳細については、異常の分析を参照してください。

Nexus Dashboard Orchestrator のサポートされているクエリ

次の表は、Nexus Dashboard Orchestrator アシュアランスで **Explore** 機能に対してサポートされているクエリの一覧です。

サポートされている Can クエリ

表 6. サポートされている Can クエリ

クエリ	エンティティ	演算子	プロトコル	接続先ポート	送信元ポート
EPGできます `epg_name` は次と通信可能か：	EPG	—	—	—	—
Can ANY talk to	• EPG • ANY	—	—	—	—

[演算子プロトコル（Operator Protocol）]、**[宛て先ポート（Destination Port）]**、**[送信元ポート（Source Port）]** はサポートされていません。

マルチサイト トラフィック パス - ベータ機能

マルチサイト トラフィック パス トレースと障害相関

これはベータ機能です。ベータ
とマークされた機能はテスト環境で使用し、実稼働環境では使用しないことをお勧めします。

フローを監視するために、サイトグループ内の2つの異なるサイトからのフローを1つのビューに結合できます。結合することで、パスのエンドツーエンドビュー、特定のフローのエンドツーエンドの詳細、およびそのフローの遅延情報を表示できます。

マルチサイト トラフィック パス トレースと障害相関のユースケース:

- サイト間でフローを関連付け、フローの詳細を結合されたパスで表示できます。
- サイト全体のフローを監視し、トリガーベースのサイト間の異常を生成できます。
- サイト間のフローを監視し、エンドツーエンドの遅延を提供できます。

マルチサイト トラフィック パス トレースと障害相関の設定

サイトグループ内の**[Explore]**領域で、2つのポート間のフローパス、各ポートのIPアドレスとVRFを表示できます。

1. Cisco Nexus Dashboard Insights の GUI の **[概要（Overview）]** ページにある左側のナビゲーションウィンドウで **[参照（Browse）] > [フロー（Flows）] の順に選択します。**
2. 目的のノードをクリックし、サイドバーの右上隅にある [詳細（Details）] アイコンをクリックして表示し、**[フローの詳細（Flow Details）]** ページを表示します。
3. **[フローの詳細（Flow Details）]** ページに、**[フローレコード情報（Flow Record Information）]** と **[集約されたフロー情報（Aggregated Flow Information）]** が表示されます。
4. **[フローパスの概要（Flow Path Summary）]** エリアのフローパスで、**[マルチサイトフロー - フローExplore で表示（Multi-Site Flow - View in Flow Explore）]** タブをクリックして、**[Explore]** ページに移動します。

[Explore フロー]ページの[検索]フィールドにフロー情報のフィルタが自動入力され、フローが存在するサイトを確認できます。**[View クエリ]**領域には、送信元IPアドレス、送信元ポート情報、および宛先IPアドレス、宛先ポート情報を含む情報が表示されます。**Explore**は、指定されたVRFでこのフローが検出されたすべてのサイトを検索して返します。

次に、適切な送信元サイトと宛先サイトを選択して、集約された情報、パスの概要、お

よび異常を表示します。送信元として使用するサイトと宛先として使用するサイトを指定する必要があります。Cisco Nexus Dashboard Insightsは、入力に基づいて情報を結合します。この情報を結合するために、一度に1つの送信元と1つの宛先のみ選択できます。選択した送信元サイトと宛先サイトに基づいて、Cisco Nexus Dashboard Insightsは見つかったサイトの名前を返します。

[フロー パスの概要] 領域では、2 つのサイトの詳細が [探索] ページに表示されます。ソースから宛先までのエンドツーエンドの情報を表示するグラフィカルなフローパス。エンドポイントと一連のノードがある最初のサイトが表示され、2番目のノードのセットの後にエンドポイントが続く2番目のサイトに接続されていることがわかります。ファイアウォールが存在する場合は、パス内のファイアウォールも特定されます。このグラフでは、エンドツーエンドのフローパスネットワークの遅延もキャプチャされます。

送信元サイトと接続先サイトの特定の詳細は、各 **[集約されたフローレコード（Aggregated Flow Records from）]** テーブルに表示されます。**[異常（Anomalies）]** テーブルで、**[集約（Aggregated）]** を選択して、選択したフローの集約された異常を表示します。

[Explore]ページの[検索]フィールドに別のフローの詳細を入力すると、入力したフローが存在するサイトを表示できます。または、**[Explore]**ページの[検索（Search）]フィールドに詳細を入力して、サイトグループ内の複数のサイトにわたるフローおよびフローパスに関する詳細の検索を直接開始できます。

ノード

ノード

[ノード（Nodes）] ペインには、ノードの動作を表示するさまざまな方法である[リソース使用率（Resource Utilization）]、[環境（Environmental）]、[統計情報（Statistics）]、[エンドポイント（Endpoints）]、および [フロー（Flows）] に基づいた上位ノードの比較チャートが表示されます。カテゴリごとに選択された上位ノードに基づいて、概要ペインにノードとその異常スコア、ファームウェア、シリアル、モデル、およびタイプが表示されます。

- 概要ペインで *[ノード（Node）]* をクリックして、選択したノードについて収集されたすべての情報を表示します。

  [ノードの概要（Node Overview）] セクションには、各 Nexus Dashboard Insights の上位 5 つのリソース（[リソース使用率（Resource Utilization）]、[環境（Environmental）]、[統計情報（Statistics）]、[フロー（Flows）]、[イベント（Events）]、および [エンドポイント（Endpoints）]）が、障害とイベントの内訳とともに表示されます。*[異常（Anomalies）]*セクションには、システムが検出した異常が表示されます。

- 概要ペインの右上隅にあるをクリックして、[ノードの詳細]ページを表示します。
- **[概要（Overview）]** タブをクリックします。

[概要（Overview）] タブの [ノードの詳細（Node Details）] ページには、[一般的な情報（General Information）]、[ノードの概要（Node Overview）]、および [異常（Anomalies）] が表示されます。*[ノードの概要（Node Overview）]* セクションには、Cisco Nexus Dashboard Insights の上位 5 つのリソース（[リソース使用率（Resource Utilization）]、[環境（Environmental）]、[統計情報（Statistics）]、および [フロー（Flows）]）が、障害とイベントの内訳とともに表示されます。*[異常（Anomalies）]*セクションには、システムが検出した異常が表示されます。

- 選択したノードの詳細ページで、右上のナビゲーションウィンドウにある省略記号（ ）アイコンをクリックして、ノードの [フロー（Flows）]、[統計情報（Statistics）]、[リソース（Resources）]、[異常（Anomalies）]、[エンドポイント（Endpoints）]、[イベント（Events）]、[環境リソース（Environmental Resources）] など、ノードの追加の関連情報を表示します。
- リストのカテゴリをクリックして、その特定のノードの参照作業ウィンドウを開きます。

[ノードの詳細（Node Details）] ページの *[アラート（Alerts）]* タブには、選択した上位ノードのノードで発生した異常がカテゴリ別に表示されます。

- [ノードの詳細]ページで異常をクリックして、その異常の一般的な詳細を示すサイド

ペインを開きます。

- 異常の詳細ページで **[分析（Analyze）]** をクリックして、異常の存続期間、推定される影響、推奨事項、相互発生、および詳細な分析を表示します。
- 相互発生グラフの異常、障害、イベントにカーソルを合わせます。クリックすると、異常の相互発生に関する詳細な分析が表示されます。

アラート分析

アラート分析

[アラートの分析]には、Nexus Dashboard Insightsによって生成された異常とアドバイザリが表示されます。Nexus Dashboard Insightsは、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。

異常ダッシュボード

異常ダッシュボードは、リソース使用率、環境の問題、インターフェイスとルーティングプロトコルの問題、フロー、エンドポイント、イベント、アシュアランス分析、コンプライアンス、変更分析、静的分析、および Orchestrator アシュアランスのために発生した異常で構成されます。

サイト間異常には2つのタイプがあります。1 つは、集約された Nexus Dashboard Orchestrator **[Orchestrator アシュアランス（Orchestrator Assurance）]** カテゴリの異常です。これらの異常は、存在するデータセットで生成され、Nexus Dashboard Orchestratorから取得した詳細によって提供されます。2番目のタイプは、サイトグループ内の複数のサイトで見つかった一連の集約された異常です。**[異常（Anomalies）]** テーブルの [サイト（Sites）] 列には、そのような異常の影響を受けるサイトが一覧表示されます。

アドバイザリダッシュボード

アドバイザリダッシュボードは、Field Notice、ソフトウェアとハードウェアのEOL/EOS、ノードレベルでのPSIRT、およびコンプライアンスが原因の関連する影響で構成されます。

PSIRT(プロダクト セキュリティ インシデント レスポンス チーム)の通知には、ネットワーク内のノードのハードウェアおよびソフトウェアに関する3つのレベルのアドバイザリ重大度が表示されます。重大度によって分類され、アドバイザリが適用されるソフトウェアバージョンとハードウェア プラットフォームが特定されます。

異常

異常ダッシュボードには、特定のサイトグループまたはサイトのタイプと重大度、およびユーザーが選択した時間範囲に基づいた異常スコア別の上位ノードのグラフが表示されます。

フィルタバーを使用すると、異常をフィルタ処理できます。詳細については、異常

フィルタを参照してください。このページには、異常の個別ビューまたは集約ビュ

ーも表形式で表示されます。

- 個別ビューには、サイトで発生した個別の異常が、重大度、タイトル、カテゴリ、ノード、検出時間、最終確認時刻、ステータス、説明、チェックコード、ユーザー状態などの詳細とともに表示されます。
- 集約ビューには、異常のタイトルに基づいて異常の集約ビューが表示され、各タイトルの異常の数が表示されます。
- サイト間ビューには、Nexus Dashboard Orchestratorに関連付けられたサイトグループの異常が表示されます。

Nexus Dashboard Insightsは、Cisco APICおよびCisco DCNMで強化されたフレームワークとワークフローマッピングを使用して、強化された異常診断と影響の推奨事項を示します。インパクト分析とプロアクティブな診断レポート]領域には、異常診断の影響と推奨事項が記述されています。個別の異常の詳細を表示する場合は、異常の分析を参照してください。

異常には次のプロパティを設定できます。

- ユーザーの割り当て
- タグの追加
- コメントの追加
- 検証ステータスの設定
- 異常を承認して、承認された異常が [異常（Anomalies）] テーブルに表示されないようにします。異常のプロパティを設定するには、異常のプロパティの設定を参照してください。

次の方法で異常を承認できます。

- 異常を手動で承認します。異常のプロパティの設定を参照してください。
- 複数の異常を手動で承認します。 異常のプロパティの設定。
- アラートルールを使用して、アラートルールに一致する異常を自動的に承認します。アラートルールの作成を参照してください。

異常フィルタ

異常ダッシュボード
では、次のフィルタを使用して、表示される異常を絞り込むことができます。

- [承認] - ステータスが[承認済み]の異常のみ表示されます。
- [アクティブ] - ステータスが[アクティブ]な異常のみ表示されます。
- [異常ID] - 指定した異常IDの異常のみ表示されます。
- [担当者] - 指定したユーザーに割り当てられた異常のみ表示されます。
- [カテゴリ] - 特定のカテゴリの異常のみ表示されます。

- [チェックコード] - 指定したチェックコードの異常のみ表示されます。
- [コメント] - 指定したコメントの異常のみ表示されます。
- [説明] - 指定した説明の異常のみ表示されます。
- [検出時間] - 特定の検出時間の異常のみ表示されます。
- [エンティティ名] - 指定した名前の異常のみ表示されます。
- [最終確認時刻] - 特定の時刻の異常のみ表示されます。
- [ノード] - ノードの異常のみ表示されます。
- [重大度] - 特定の重大度の異常のみ表示されます。
- [サブカテゴリ] - 特定のサブカテゴリの異常のみ表示されます。
- [タグ] - 指定したタグの異常のみ表示されます。
- [タイトル] - 指定したタイトルの異常のみ表示されます。
- [検証ステータス] - 特定の検証ステータスの異常のみ表示されます。

フィルタの絞り込みには、次の演算子を使用します。

== -
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、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。

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。

⇐ -
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。

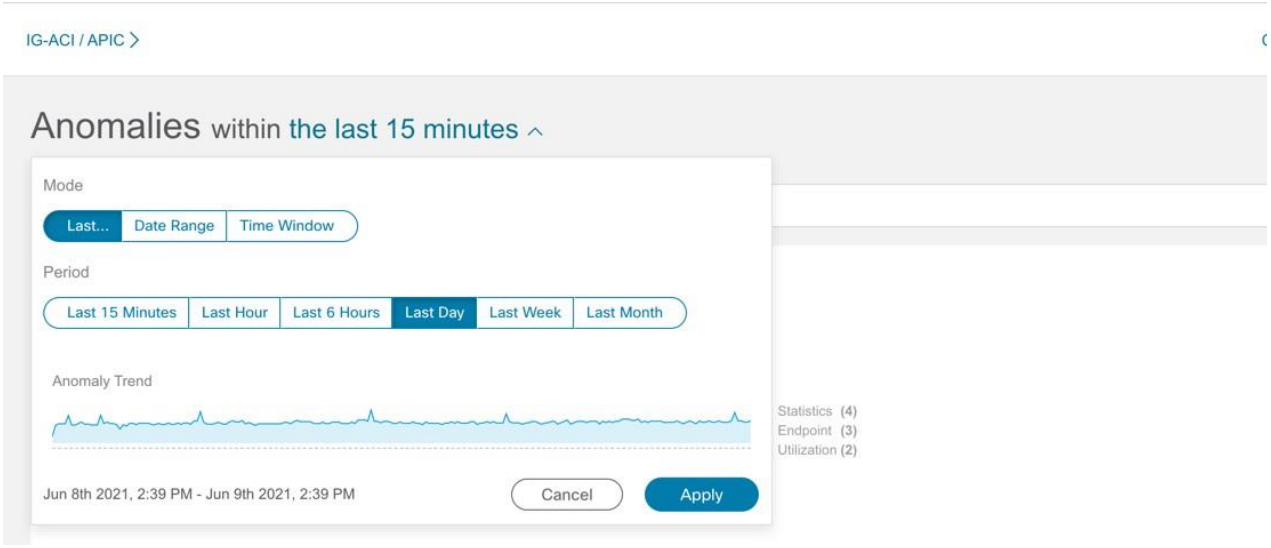
> -
最初のフィルタタイプ。この演算子および後続の値を使用すると、その値より大きい一致データが返されます。

>= -
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。

異常の分析

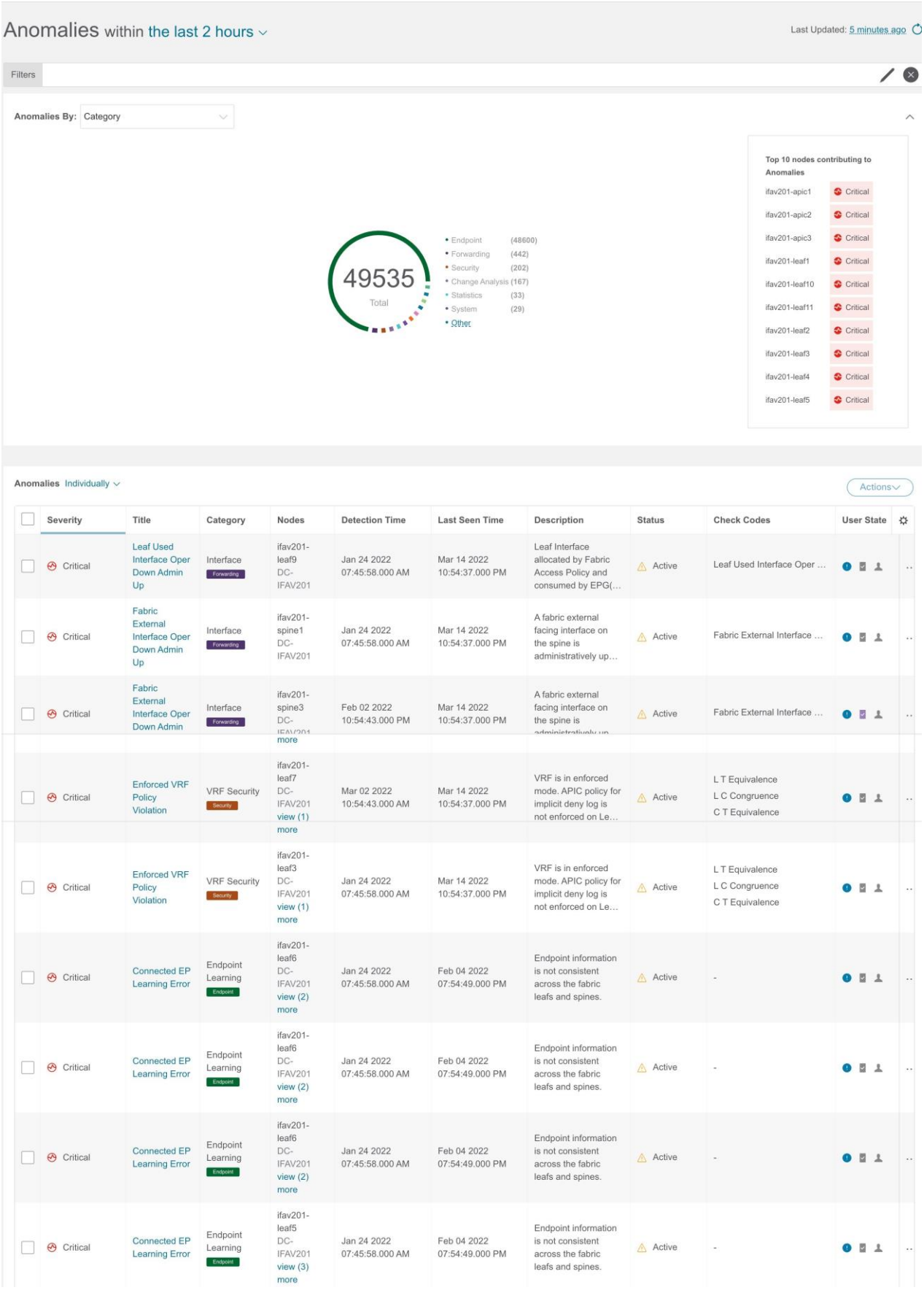
次の手順を使用して、異常を分析します。

1. **[アラートの分析（Analyze Alerts）] > [異常（Anomalies）]** の順に選択します。
2. **異常**ダッシュボードで、[サイトグループ（Site Group）] メニューからサイトグループまたはサイトを選択します。
3. ドロップダウンメニューから時間範囲を選択します。



時間範囲で、少なくとも**過去 2 時間**を選択して、選択したサイトのすべての異常を表示します。

[異常（Anomalies）]テーブルには、選択したサイトと時間範囲に基づいて、個別の異常、集約された異常、またはサイト間の異常が表示されます。デフォルトでは、異常はシステムステータスでソートされています。異常ステータスには、[アクティブ]と[クリア]があります。[アクティブ]は、ネットワークに異常な状態が存在することを示しています。[クリア]は、異常な状態がネットワークに存在しないことを示しているため、異常はクリアとマークされています。



4. 次のいずれかを実行します。

   a. 個別の異常を表示するには、[異常]ドロップダウンリストから **[個別]** を選択します。

   b. [異常（Anomalies）] ドロップダウンリストで **[集約（Aggregated）]** を選択して、タイトルに。

   c. [異常（Anomalies）] ドロップダウンリストで **[サイト間（Inter-Site）]**

を選択して、Nexus Dashboard Orchestratorに関連付けられたサイトグループの異常を表示します。

5.  アイコンをクリックして、テーブルの列をカスタマイズします。

6. 各列の[フィルタ]アイコンを使用して、異常をソートします。**[ノード（Nodes）]** 列のフィルタ処理はサポートされていません。

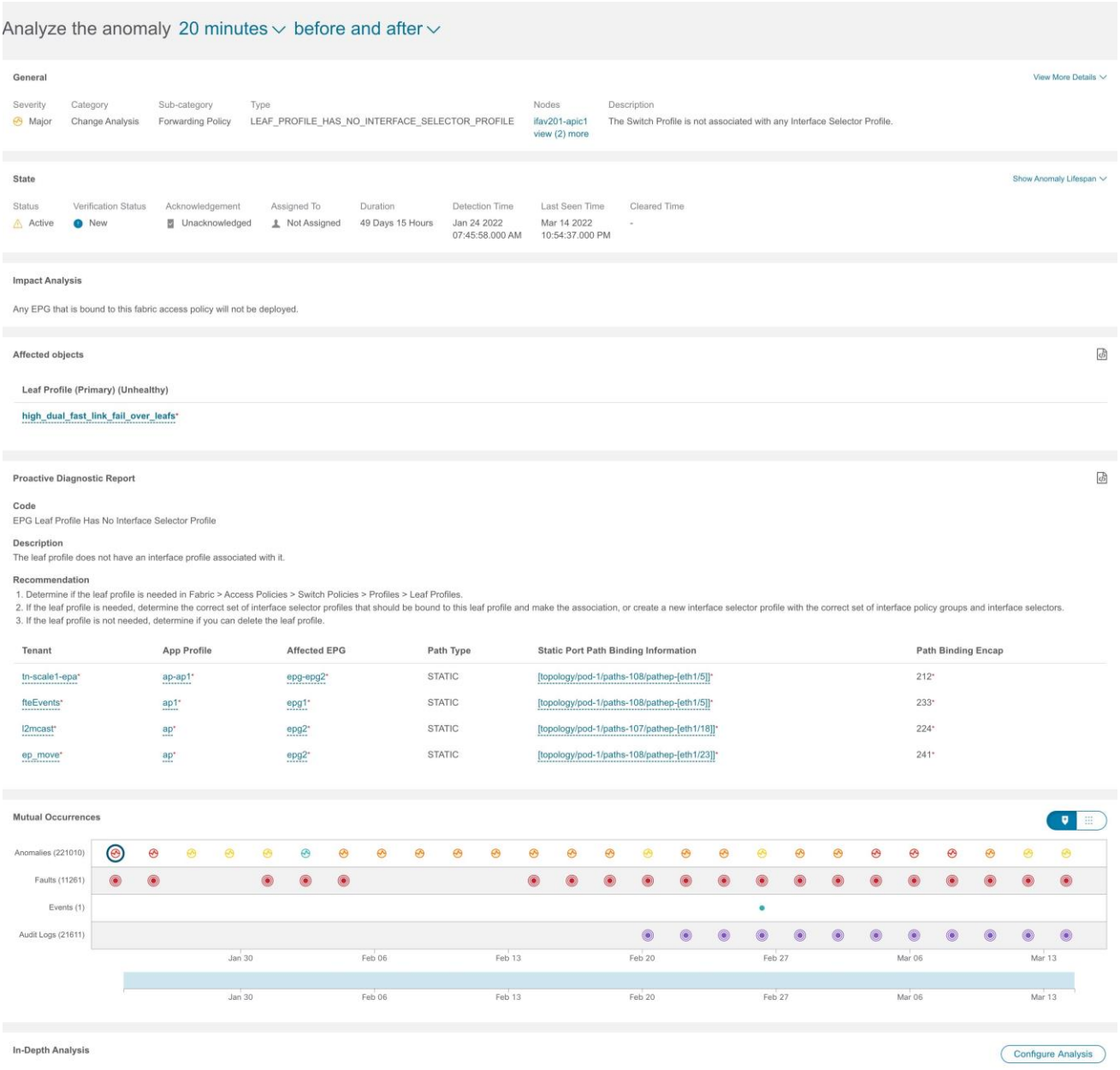
   a. リリース6.1.1以降、チェックコードで異常をフィルタ処理でき、結果が[異常]テーブルに表示されます。異常には複数のチェックコードが含まれる場合があります。

   b. **[詳細を表示（View More）]**をクリックして、特定の異常のチェックコードをすべて表示します。

   c. 検索バーに検索条件を入力して、特定のチェックコードを検索します。

7. サイドペインの **[異常（Anomalies）]** テーブルで異常をクリックして、その異常に関する追加の詳細を表示します。集約ビューでは、サイドペインに個別の異常のリストが表示されます。異常をクリックすると、個別の異常に関する追加の詳細が表示されます。サイト間ビューでは、追加の**[サイト]** 列が表示され、異常の影響を受けるサイトグループ内のNexus Dashboard Orchestratorに関連付けられたサイトが一覧表示されます。

8. [Analyze（分析）] をクリックします。**[異常の分析（Analyze Anomaly）]** ページには、異常の一般情報、状態、影響分析、影響を受けるオブジェクト、プロアクティブな診断レポート、相互発生、および詳細な分析が表示されます。**[異常の分析（Analyze Anomaly）]** ページの **[プロアクティブな診断レポート（Proactive Diagnostic Report）]** 領域にチェックコードが表示されます。



a. **[全般（General）]** 領域で、ノードをクリックして追加の詳細を表示します。

b. **[状態（State）]**領域には、検出時間とクリア時間が表示されます。

c. **[影響を受けるオブジェクト（Affected Object）]**
領域で、影響を受けるオブジェクトをクリックして追加の詳細を表示します。

d. **[影響分析（Impact Analysis）]** 領域で **[レポートの表示（View Report）]**
をクリックして、影響を受けたエンティティの詳細を表示します。

e. [**プロアクティブな 診断 レポート（Proactive Diagnostic Report）]**
には、 チェックコード 、 説明
、および推奨事項が表示されます。

f. [**相互発生**（Mutual Occurrences）]
領域で、異常、障害、およびイベントにカーソルを合わせます。クリックすると
、異常の相互発生に関する詳細な分析が表示されます。

g. **[分析の設定]**をクリックして、カスタマイズ可能なグラフでノードの異常を分析します。

i. [オブジェクト選択]テーブルで、**[オブジェクトの追加]**をクリックします。

ii. [チャート選択]テーブルで、**[チャートタイプ**（Chart
Type）]を選択し、ドロップダウンリストから**[チャート名**（Chart

Name）]を選択します。

iii. **[保存（Save）]** をクリックします。

比較チャートが自動的に更新され、選択した異常があるノードのリソース使用率が表示されます。選択した異常があるノードのリソースを比較して分析できます。

8. ページの右上にある楕円の

アイコンをクリックします。リストからノードを選択して、その特定のノードの参照作業ウィンドウを開きます。

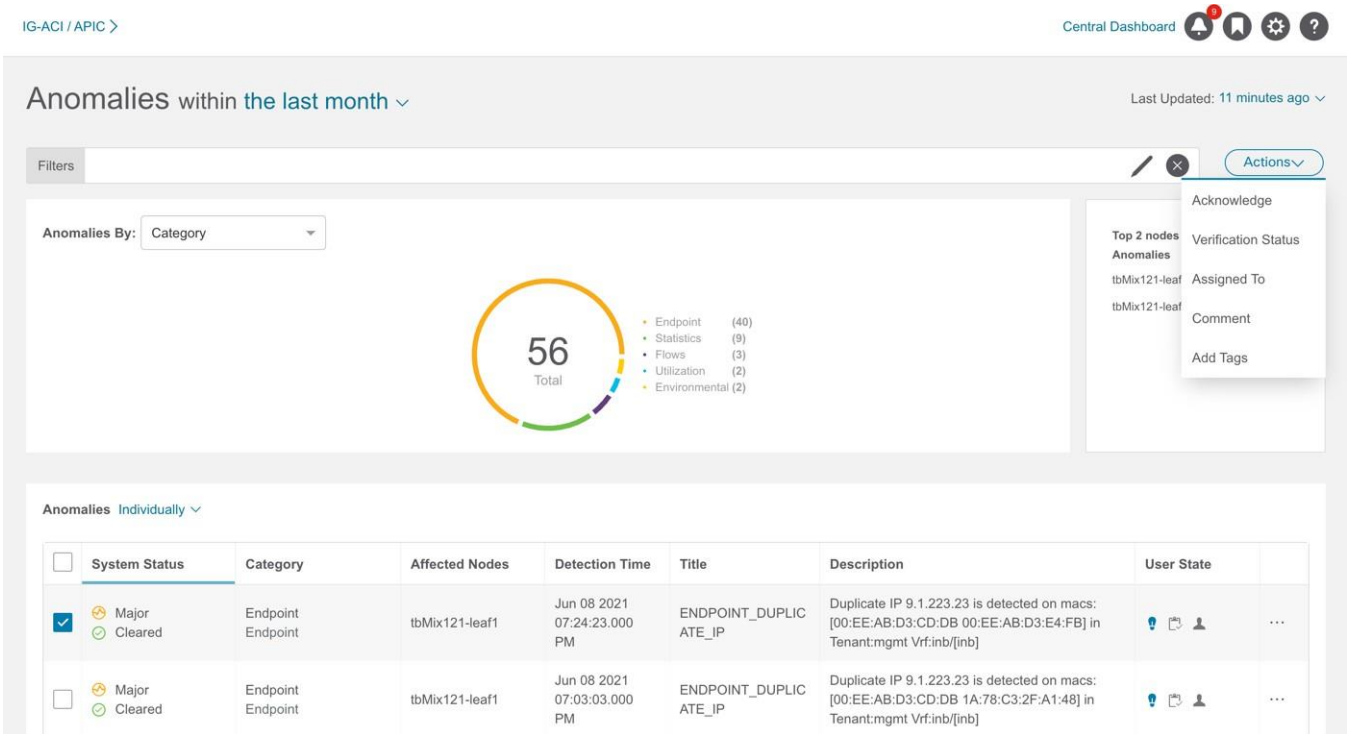
9. 
アイコンをクリックして、ページをブックマークします。

10. **[完了（Done）]** をクリックします。

異常のプロパティの設定

次の手順を使用して、異常のプロパティを設定します。

1. **[アラートの分析（Analyze Alerts）]** > **[異常（Anomalies）]** の順に選択します。
2. **異常**ダッシュボードで、[サイトグループ（Site Group）]
メニューからサイトグループまたはサイトを選択します。
3. ドロップダウンメニューから時間範囲を選択します。[異常]テーブルには、選択したサイトと時間範囲に基づいて、個別の異常または集約された異常が表示されます。
4. [異常（Anomalies）]ドロップダウンリストから**[個別（individual）]**を選択します。
5. テーブルから異常を選択し、**[アクション（Actions）]**
メニューからプロパティを選択します。



a. 異常を手動で承認するには、**[承認（Acknowledge）]**を選択します。異常を承認しても、その異常は[異常]テーブルには表示されません。**[異常（Anomalies）]**

テーブルに異常を表示するには、Acknowledgement=true フィルタを使用します。

デフォルトのフィルタはAcknowledgement=falseです。[異常（Anomalies）] ドロップダウンリストから **[集約（Aggregated）]** を選択した場合、Acknowledgement=false フィルタは適用されません。[異常（Anomalies）]ドロップダウンリストから**[個別（individual）]**を選択した場合に適用されます。

b. [新規]、[進行中]、[クローズ]などのユーザー定義ステータスを異常に設定するには、**[検証ステータス（Verification Status）]** を選択します。**[保存（Save）]** をクリックします。

c. [割り当て先（Assigned To）] を選択して、異常をユーザーに割り当てます。ユーザー名を入力し、**[保存]** をクリックします。

d. [コメント（Comment）] を選択して、異常にコメントを割り当てます。コメントを入力して、**[保存（Save）]** をクリックします。

e. **[タグの追加（Add Tags）]**を選択して、ユーザー定義のタグを異常に追加します。タグ名を入力して、**[保存]**をクリックします。複数のタグを入力できます。タグ名を入力したら、Enterを押します。

6. 個別の異常のプロパティを設定するには、異常を選択します。 ･･･ アイコンをクリックし、ドロップダウンリストからプロパティを選択します。

7. **[異常（Anomalies）]**テーブルでは、異常に割り当てられたプロパティは[ユーザー状態（User State）] 列に表示されます。

注:

- **[アクション（Actions）]** メニューを使用して異常のプロパティを構成する際、**[異常（Anomalies）]** テーブルの ･･･ アイコンを使用して、個別の異常で構成したすべてのプロパティがオーバーライドされます。
- 異常に設定されたプロパティを表示するには、タイムライン範囲を更新する必要があります。
- 異常に設定されたすべてのプロパティは、将来の分析にのみ適用されます。
- ファイルのアップロード データ収集タイプ分析のアクティブな異常を表示するには、分析が作成されたときの時間範囲を選択する必要があります。

ワンクリック修復

ワンクリック修復機能は、推奨事項に基づいて異常を修復可能にすることで、MTTRを短縮します。

Nexus Dashboard Insights は、Cisco APIC の強化されたフレームワークとワークフローマッピングを使用して、異常診断と影響の推奨事項を示します。[異常の分析]ページの[推定される影響と推奨事項]領域には、異常診断の影響と推奨事項が記載されています。ワンクリック修復機能を使用すると、提案された

推奨事項をファブリックで実行できます。

このリリースでは、次の異常に対する修復がサポートされています。

- ACCESS_ENTITY_PROFILE_NOT_ASSOCIATED_WITH_ANY_DOMAINS
- CONNECTED_EP_LEARNING_ERROR

注意事項と制約事項

CONNECTED_EP_LEARNING_ERRORR異常の場合、次のユースケースの修復はサポートされていません。

- ローカルに接続されていないエンドポイントの IP アドレスまたは MAC が、リーフスイッチのグローバルエンドポイント転送テーブルに存在し、ファブリック内にある他のどのリーフスイッチにもローカルに接続されたホストとして存在していない場合。
- グローバル エンドポイント テーブルのエンドポイントの詳細に、誤ったネクスト ホップ トンネル エンドポイント(TEP) IP アドレス。
- ス
パインスイッチで見つかったエンドポイントが、どのリーフスイッチでもローカルとしてマークされていない場合。
- 静的エンドポイントの修復はサポートされていません。

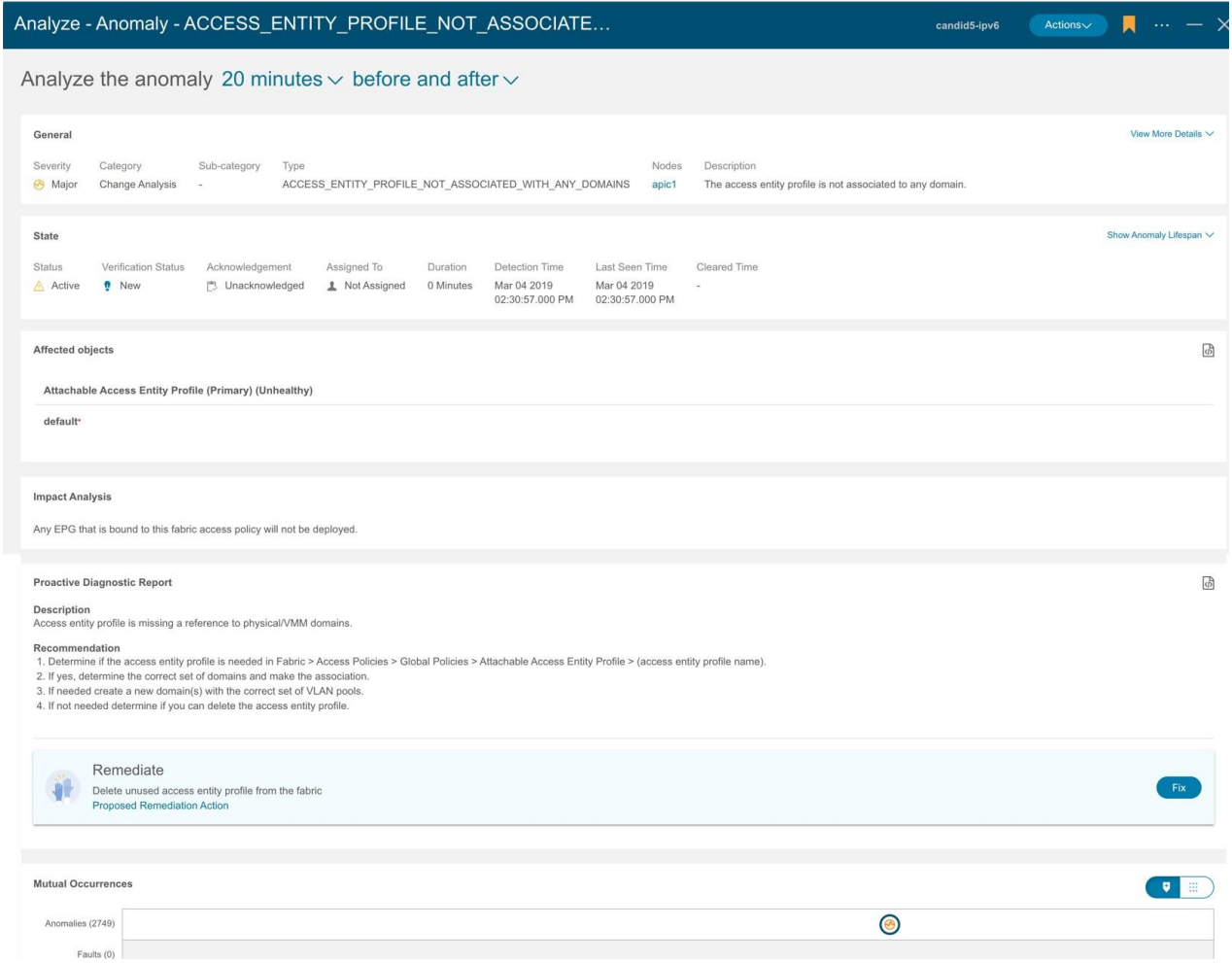
異常の修復

次の手順を使用して、異常を修復します。

1. **[アラートの分析（Analyze Alerts）]** > **[異常（Anomalies）]** の順に選択します。
2. **[異常（Anomalies）]** ダッシュボードの [サイトグループ（Site Group）] メニューでサイトグループまたはサイトを選択します。
3. ドロップダウンメニューから時間範囲を選択します。

   [異常（Anomalies）]
   テーブルには、選択したサイトと時間範囲に基づいて、個別の異常または集約された異常が表示されます。

4. 個別の異常を表示するには、[異常（Anomalies）] ドロップダウンリストで **[個別（Individual）]** を選択します。
5. サイドペインの **[異常（Anomalies）]** テーブルで異常をクリックして、追加の詳細を表示します。
6. [Analyze（分析）] をクリックします。**[異常の分析（Analyze Anomaly）]** ページには、異常の一般情報、状態、影響を受けるオブジェクト、推定される影響、予防的な診断レポート、相互発生、および詳細な分析が表示されます。



7. **[プロアクティブな診断レポート（Proactive Diagnostic Report）]** エリアには、異常の修復に必要な推奨事項が表示されます。
8. [修復（Remediate）] タイルで、**[提案された修復アクション（Proposed Remediation Action）]** をクリックして、異常を修復するために必要なアクションを表示します。
9. **[修正（Fix）]** をクリックして、修復アクションを実行します。修復アクションのステータスは **[進行中（In Progress）]** と表示されます。修復アクションが完了すると、ステータスは **[完了（Completed）]** と表示され、異常の **[修復（Remediate）]** タイルは表示されなくなります。

[プロアクティブな診断レポート（Proactive Diagnostic Report）] エリアでは、推奨事項に複数の手順を含めることができますが、**[提案された修復アクション（Proposed Remediation Action）]** は、 ステップのひとつ。

異常の管理

次の手順を使用して、異常を管理します。

手順

1. **[アラートの分析（Analyze Alerts）]** > **[異常（Anomalies）]** の順に選択します。
2. **異常**ダッシュボードで、[サイトグループ（Site Group）] メニューからサイトグループまたはサイトを選択します。
3. 異常を未承認にするには、次の手順を実行します。
   a. フィルタバーで、フィルタ Acknowledgement == True を適用します。[異常（Anomaly）] テーブルには、承認された異常が表示されます。

b. [異常（Anomalies）]ドロップダウンリストから**[個別（individual）]**を選択します。

c. 承認された異常を選択し、**[アクション（Action）]**メニューから**[未承認（Unacknoledge）]**を選択します。

d. 個別の異常を未承認にするには、異常を選択します。 ••• アイコンをクリックし、ドロップダウンリストから**[未承認（Unacknoledge）]**を選択します。

アドバイザリ

[アドバイザリ（Advisories）]
ダッシュボードには、ユーザーが選択した時間範囲に基づいて、特定のサイトグループまたはサイトのタイプと重大度別にアドバイザリが表示されます。

- [アドバイザリ別（Advisories By）]ドロップダウンリストから、**[シビラティ（重大度）（Severity）]**を選択して、メジャー、マイナー、およびクリティカルのアドバイザリの総数を表示します。このページには、重大度、検出時間、リソースタイプ、影響を受けるノード、およびタイトルを含むアドバイザリが要約されています。
- [アドバイザリ別（Advisories By）]ドロップダウンリストから**[カテゴリ（Category）]**を選択して、PSIRT、Field Notice、HW EOL、SW EOL、コンプライアンスなどのカテゴリ別のアドバイザリの総数を表示します。このページには、重大度、検出時間、リソースタイプ、影響を受けるノード、およびタイトルを含むアドバイザリが要約されています。

Nexus Dashboard Insightsは、メタデータバンドルを使用して、新しいバグ、PSIRT、フィールド通知、およびサポート終了通知を検出します。メタデータパッケージは常に更新され、検証後にCisco Intersight Cloudに投稿されます。Nexus Dashboard Insightsは、Nexus Dashboardプラットフォームに組み込まれているデバイスコネクタを介してCisco Intersightポータルに接続し、定期的に更新されるメタデータパッケージ。Nexus DashboardがCisco Intersight Cloudに接続されていない場合、エアギャップ環境のメタデータサポートを使用し、ユーザーは手動で、安全で信頼できる方法により最新のメタデータをNexus Dashboard Insightsにアップロードできます。バンドルの更新は、Cisco DC App Centerからダウンロードできます。エアギャップ環境のメタデータサポートを参照してください。

[設定（Settings）] > **[アプリケーション（Application）]** > **[バージョン情報（About）]**を選択して、メタデータのバージョンを表示します。

- [メタデータバージョン]にカーソルを合わせると、現在のリリースのメタデータバージョンのデジタル化された欠陥が表示されます。ファームウェアバージョンに関連付けられたデジタル化された欠陥を表示するには、欠陥分析の表示を参照してください。
- **[更新（Update）]**をクリックして、エアギャップ環境のメタデータをアップロードします。エアギャップ環境のメタデータサポートを参照してください。

エアギャップ環境のメタデータサポート

エアギャップ環境のメタデータサポートにより、Nexus DashboardがCisco Secure Cloudに接続されていない場合、安全で信頼できる方法で最新のメタデータをNexus Dashboard Insightsに定期的にアップロードできます。

暗号化されたメタデータファイルを Cisco DC App Center からダウンロードし、Nexus Dashboard Insights にアップロードして、バグ、PSIRT、欠陥、フィールド通知、およびサポート終了通知が発生したときに復号化された更新を取得できます。

メタデータバージョンの更新

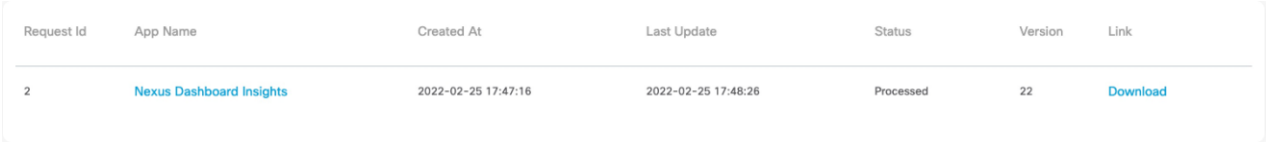
次の手順を使用して、エアギャップまたはオフライン環境で最新のメタデータバージョンを更新します。

1. Cisco DC App Center にログインします。
2. [ユーザー（User）] ドロップダウンメニューから **[マイアカウント（My Account）]** を選択します。
3. **[構成ファイルのリクエスト（Config Files Requests）]** タブをクリックします。
4. **[構成ファイルをリクエスト（Request Config File）]** をクリックします。
5. **[アプリ ID の選択（Choose App ID）]** ドロップダウンリストから、[Nexus Dashboard] を選択します。

6. サポートされているアプリの最小バージョンを確認し、**[リクエスト（Request）]** をクリックします。

   リクエストの完了まで約15分かかります。[設定ファイルのリクエスト（Config Files Request）] ページの下の表に、生成されたファイルが表示されます。

7. ファイルを選択し、**[ダウンロード（Download）]** をクリックしてファイルをローカルにダウンロードします。



8. Cisco Nexus Dashboard Insightsにログインします。

9. **[設定（Settings）] > [アプリケーション（Application）] > [バージョン情報（About）]** の順に選択します。
10. **[更新（Update）]** をクリックします。
11. [メタデータ バージョンの更新（Metadata Version Update）] ページで、Cisco DC App Center からダウンロードしたファイルをアップロードします。
12. **[完了（Done）]** をクリックして、最新のメタデータを Nexus Dashboard Insights にアップロードします。

アドバイザリフィルタ

フィルタバーを使用すると、アドバイザリをフィルタ処理できます。

アドバイザリダッシュボード
では、次のフィルタを使用して、表示される異常を絞り込むことができます。

- [検出時間] - 特定の検出時間のアドバイザリのみ表示されます。
- [最終確認時刻] - 特定の時刻のアドバイザリのみ表示されます。
- [クリア] - クリアまたは未クリアのステータスのアドバイザリのみ表示されます。
- [タイトル] - クリアまたは未クリアのステータスのアドバイザリのみ表示されます。
- [影響を受けるノード] - 特定のノードのアドバイザリのみ表示されます。
- [カテゴリ] - 特定のカテゴリのアドバイザリのみ表示されます。
- [リソースタイプ] - 特定のリソースタイプのアドバイザリのみ表示されます。
- [重大度] - 特定の重大度のアドバイザリのみ表示されます。
- [承認済み] - ステータスが[承認済み]の異常のみ表示されます。

2次フィルタの絞り込みとして、次の演算子を使用します。

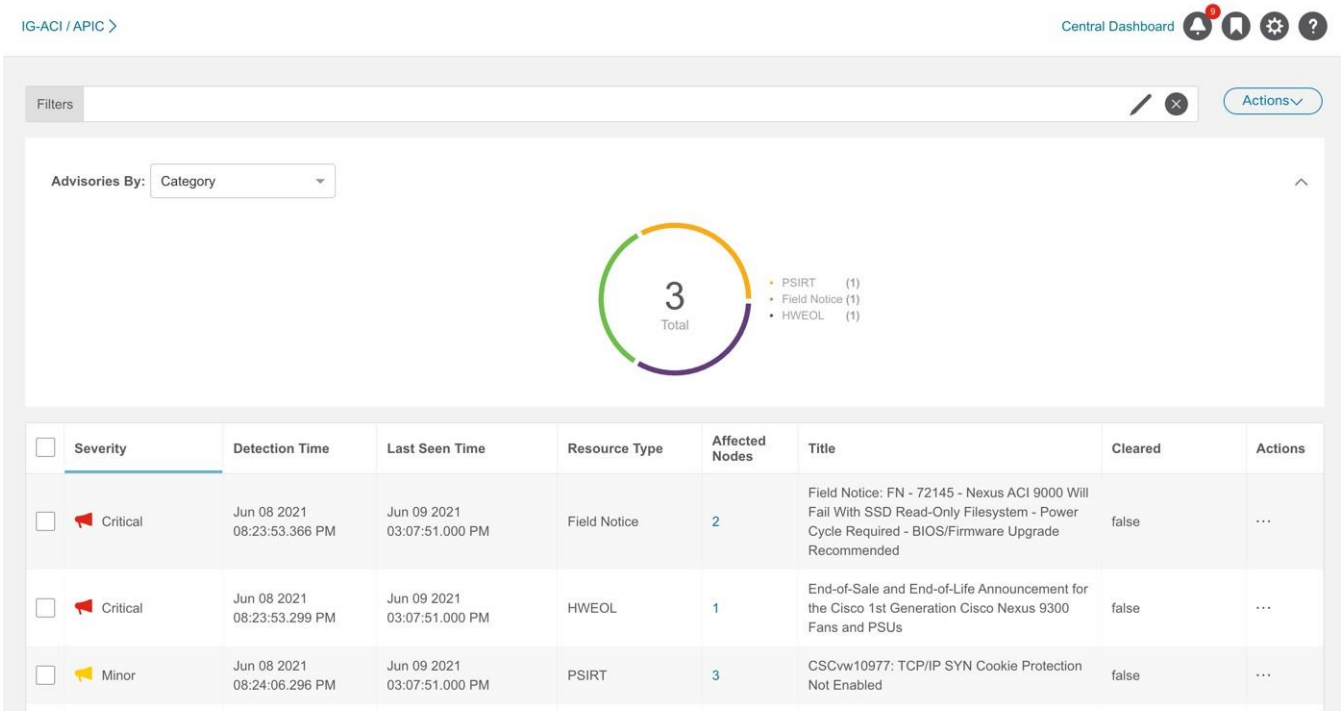
- == -
  最初のフィルタタイプ。この演算子および後続の値を使用すると、完全一致のデータが返されます。
- != -
  最初のフィルタタイプ。この演算子および後続の値を使用すると、同じ値を含まないすべてのデータが返されます。
- contains -
  最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含むすべてのデータが返されます。
- !contains -
  最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含まないすべてのデータが返されます。

アドバイザリの分析

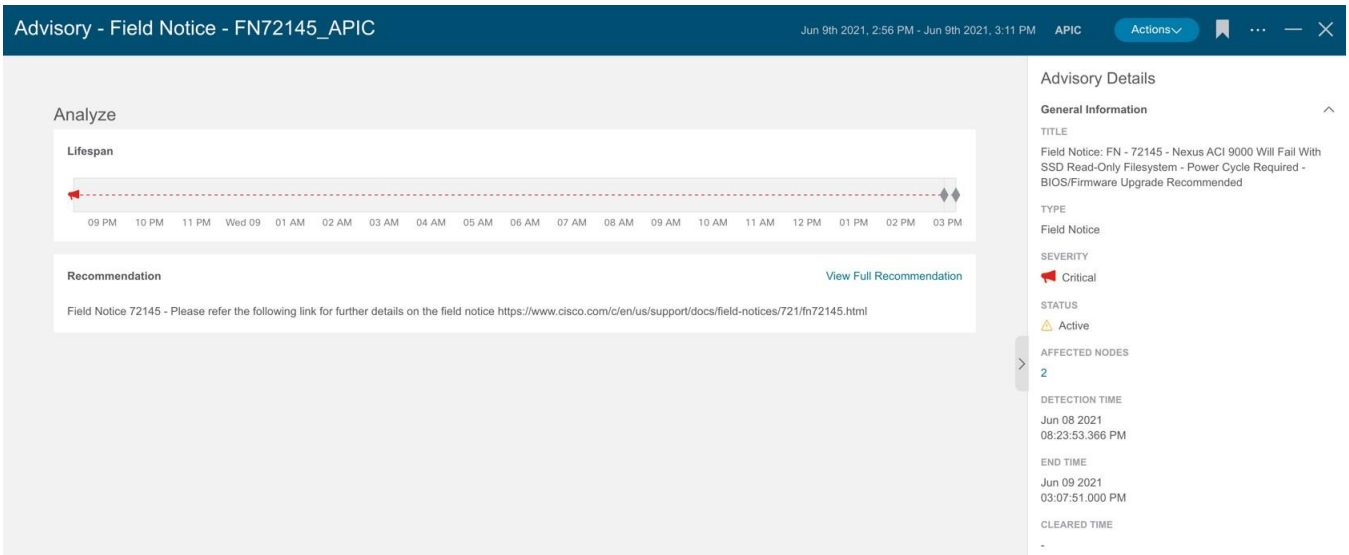
次の手順を使用して、アドバイザリを分析します。

1. **[アラートの分析（Analyze Alerts）] > [アドバイザリ（Advisories）]** の順に選択します。

2. **[アドバイザリ（Advisories）]** ダッシュボードページの [サイトグループ（Site Group）] メニューからサイトグループまたはサイトを選択します。
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. **[アドバイザリ（Advisories）]** テーブルには、選択したサイトと時間範囲に基づいた個別のアドバイザリが表示されます。デフォルトでは、アドバイザリは [シビラティ（重大度）（Severity）]でソートされています。



5. アドバイザリをクリックすると、サイドペインに詳細情報が表示されます。
6. **[Analyze（分析）]** をクリックします。**[アドバイザリの分析**（Analyze Advisory）]ページには、一般的な情報、存続期間、および推奨事項が表示されます。



a. **[一般情報（General Information）]** 領域で、影響を受けるノードをクリックして追加の詳細を表示します。
b. **[推奨事項（Recommendation）]**領域で、**[完全な推奨事項を表示（View Full Recommendation）]**をクリックして追加の詳細を表示します。

c. ページの右上にある楕円の 
アイコンをクリックします。リストからノードを選択して、その特定のノードの参照作業ウィンドウを開きます。

d.  アイコンをクリックしてページをブックマークします。

e. [完了（Done）] をクリックします。

7. **[アドバイザリ（Advisory）]** テーブルからアドバイザリを選択し、**[アクション（Actions）]** メニューから [承認（Acknowledge）] を選択して、アドバイザリを手動で承認します。

8. 承認ステータスでアドバイザリをフィルタ処理するには、**[フィルタ（Filters）]** バーで [**Acknowledged == True**] を選択します。

アラートルール

アラートルール

アラートルール機能を使用すると、基準に一致する新たに検出された異常をすべて承認し、異常の内容に応じて異常スコアを調整できます。一致基準を使用して、アラートをアラートルールと一致させることもできます。

また、アラートルールに基づいて異常が発生した場合に表示されるカスタムメッセージを追加することで、異常をカスタマイズできます。

- アラートルールには、アラートとルールの照合に必要な一致基準と、一致したアラートに適用する必要があるアクションが含まれています。
- アラートルールには、複数の一致基準を含めることができます。
- 重大度、カテゴリ、サブカテゴリ、イベント名、オブジェクト一致ルールなどの属性を使用して、アラートルールの一致基準を定義できます。
- 一致基準には、 1つまたは複数の属性を含めることができます。
  - 一致基準に複数の属性が含まれている場合、すべての属性を含むアラートが一致します。**AND** 演算子は属性に適用されます。
  - 一致基準に影響を受ける複数のオブジェクトの一致ルールが含まれている場合、影響を受けるすべてのオブジェクトの一致ルールを含むアラートが一致します。
- アラートルールに複数の一致基準が含まれている場合、一致基準の結合を含むアラートが一致します。いずれかの基準に一致するアラートはすべてルールに適用されます。**OR**演算子は基準に適用されます。
- **[オブジェクト一致ルール（Object Match Rule）]** を含む **[一致基準（Match Criteria ）]** を使用するアラートルールは、**[Equals to]**正規表現基準のみをサポートします。
- アラートルールは、少なくとも1つの一致基準が含まれている場合にのみ有効にできます。

注意事項と制約事項

- **[承認（Acknowledge）]** または **[異常のカスタマイズ（Customize Anomaly）]** アクションを含むアラートルールを削除または無効化しても、そのアラートルールはアクティブな異常からは削除も無効化もされません。アラートルールは、異常の新しいインスタンスにのみ適用されます。
- [承認]または[異常のカスタマイズ]アクションを含むアラートルールを編集する場合、更新はアクティブな異常には適用されません。アラートルールの更新は、異常の新しいインスタンスにのみ適用されます。
- アラートルールに [承認（Acknowledge）] と [異常のカスタマイズ（Customize Anomaly）] アクションの両方が含まれていて、[承認（Acknowledge）] と [異常のカスタマイズ（Customize Anomaly）]

アクションのいずれかを削除してアラートルールを編集した場合、更新はアクティブな異常には適用されません。

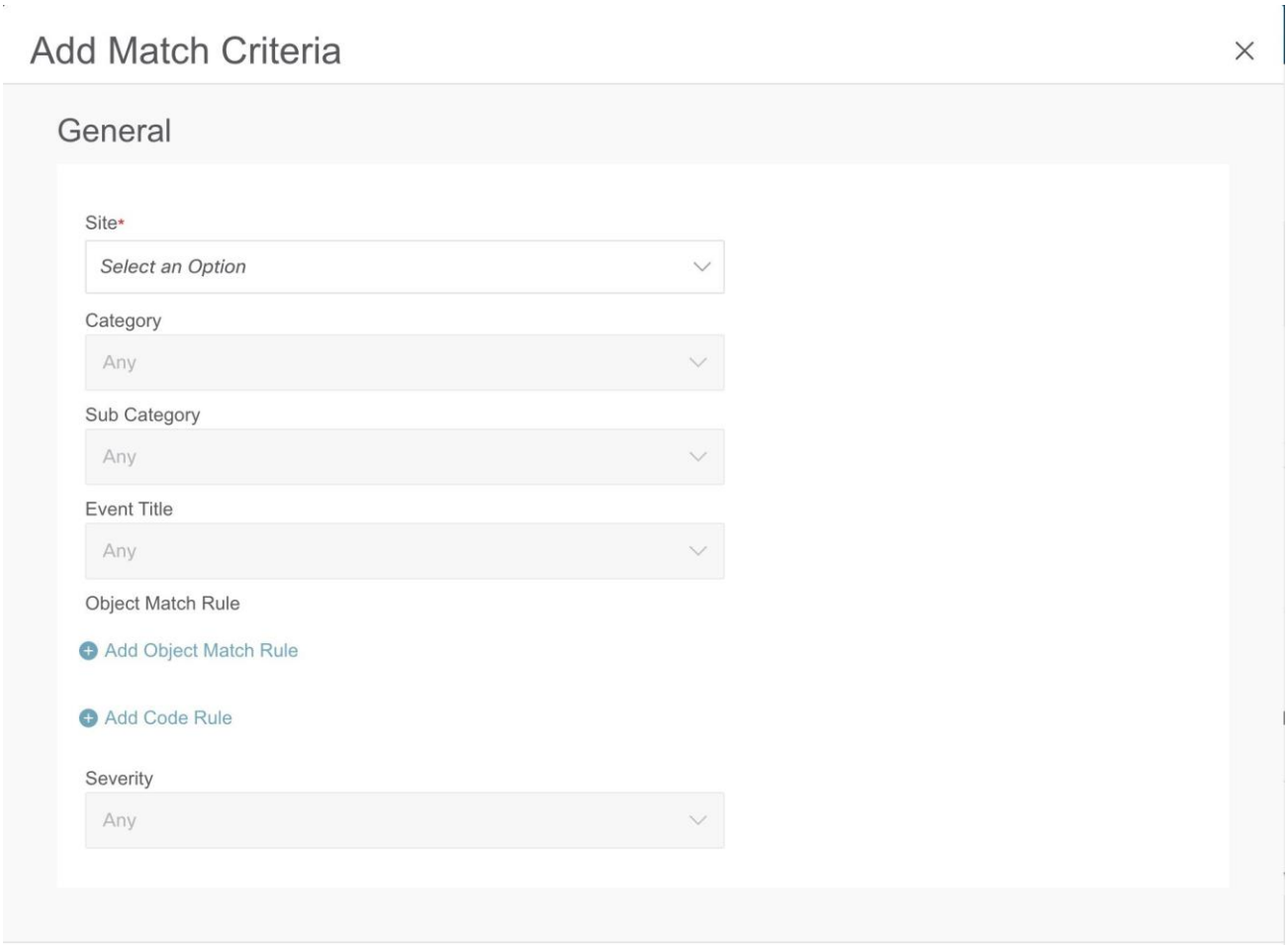
- **[異常のカスタマイズ（Customize Anomaly）]** アクションを含むアラートルールを削除または無効にしても、**[ルール ベースの推奨事項（Rule Based Recommendation）]** セクションの [プロアクティブな診断レポート（Proactive Diagnostic Report）] 領域には推奨事項が引き続き表示されます。
- アラートルールによって自動的に承認されたものを含め、異常は手動でのみ未承認にできます。アラートルールを無効化または削除することで、異常を自動的に未承認にすることはできません。異常の管理を参照してください。
- すべてのサイトでサポートされるアラート ルールの最大数は 500 です。

アラートルールの作成

次の手順を使用して、アラートルールを作成します。

手順

1. [サイトグループ]メニューから、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューで、**[サイトグループの設定（Configure Site Group）] > [アラートルール（Alert Rules）]** の順に選択します。
3. **[アラートルールの作成（Create Alert Rule）]** をクリックします。
4. **[アラートルールの作成（Create Alert Rule）]** の次のフィールドを入力します。
   a. **[名前]**フィールドに、名前を入力します。
   b. **[説明（Description）]** フィールドに、説明を入力します。
   c. 状態を選択して、ルールをアクティブにします。状態が有効な場合、ルールは次の分析に適用されます。状態が無効の場合、ルールは次の分析中に適用されません。
   d. **[一致基準の追加（Add Match Criteria）]** をクリックして、アラートルールの一致基準を定義します。
5. **[一致基準の追加（Add Match Criteria）]** の次のフィールドを入力します。



a. **[サイト（Site）]**
ドロップダウンリストでサイトを選択します。サイトグループには複数のサイトを含めることができます。ステップ 1 で選択したサイトグループに属するサイトを選択していることを確認してください。分析を実行しているサイトの一致基準のみが選択され、アラートと照合されてアクションが実行されます。

b. 一致基準の属性を選択します。カテゴリ、サブカテゴリ、イベントタイトル、オブジェクト一致ルール、コードルール、および重大度を使用して、一致基準の属性を定義できます。

c. **[オブジェクト一致ルールの追加（Add Object Match Rule）]** をクリックして、一致基準の主な影響を受けるオブジェクトを定義します。

> 複数の影響を受けるオブジェクトが一致基準に含まれている場合、影響を受けるすべてのオブジェクトを含むアラートが一致します。アラートルールに複数の一致基準が含まれている場合、一致基準の結合を含むアラートが一致します。

f.**[コードルールの追加（Add Code Rule）]**
をクリックして、一致基準のチェックコードを定義します。

g. **[保存（Save）]** をクリックします。

6. [アクション（Actions）] タイルから、**[承認（Acknowledge）]** または **[異常のカスタマイズ（Customize Anomaly）]** を選択します。[承認] を選択すると、基準に一致する新たに検出された異常をすべて承認し、異常の内容に

応じて異常スコアを調整できます。[異常のカスタマイズ]
を選択すると、アラートルールに基づいて異常が発生した場合に表示されるカスタムメッセージを追加することで、異常をカスタマイズできます。

a. **[承認]**
チェックボックスをオンにします。このオプションを選択すると、アラートルールに基づいてアラートが抑制されますが、アラートはデータベースに保存されます。Acknowledge=trueフィルタを使用して、**[異常]**テーブルにアラートを表示できます。

i. 承認ステータスで異常をフィルタ処理するには、**[アラートの分析]** > **[異常]**を選択します。**[フィルタ（Filters）]** バーで、**[Acknowledged == True]**を選択します。結果が **[異常（Anomalies）]** テーブルに表示されます。

ii. **[既存のアクティブな異常に適用（Apply to existing active anomalies）]**
チェックボックスをオンにして、アラートルールに一致する異常の既存のインスタンスにアラートルールを適用します。異常の新しいインスタンスに一致するアラートルールを適用するには、チェックボックスをオフにします。

b. **[カスタマイズ（Customize）]**
チェックボックスをオンにします。アラートに表示する推奨事項を入力します。さまざまな一致基準に基づいて複数のルールを作成し、アラートに複数のカスタマイズされた推奨事項を表示できます。[異常の分析（Analyze Anomaly）]
ページでは、**[ルールベースの推奨事項（Rule Based Recommendation）]**
セクションの **[プロアクティブな診断レポート（Proactive Diagnostic Report）]**
エリアに推奨事項が表示されます。

i. **[既存のアクティブな異常に適用（Apply to existing active anomalies）]**
チェックボックスをオンにして、アラートルールに一致する異常の既存のインスタンスにアラートルールを適用します。異常の新しいインスタンスに一致するアラートルールを適用するには、チェックボックスをオフにします。

c. [Add] をクリックします。

新しいアラートルールが**[アラートルール（Alert Rule）]** テーブルに表示されます。

アラートルールの管理

次の手順を使用して、アラートルールを編集、有効化、無効化、および削除します。

手順

1. [サイトグループ]メニューから、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューで、**[サイトグループの設定（Configure Site Group）]** > **[アラートルール（Alert Rules）]**
の順に選択します。アラートルールが **[アラートルール（Alert Rule）]**
テーブルに表示されます。
3. アラートルールを選択し、 ⋯ * アイコンをクリックします。
   a. **[編集（Edit）]** を選択して、アラートルールを編集します。
   b. **[有効化（Enable）]**
   を選択して、アラートルールを有効にします。アラートルールを有効にする前に、アラートルールに少なくとも1つの一致基準が存在することを確認してください。

c. **[無効化（Disable）]** を選択して、アラート ルールを無効にします。

サイトがサイトグループから関連付け解除されると、サイトのすべての一致基準がアラートルールから削除されます。一致条件が見つからない場合、アラート ルールは無効になります。

d. **[削除（Delete）]** を選択して、アラート ルールを削除します。

保持され

サイト グループが削除されると、そのサイト グループに関連付けられているすべてのアラート ルールが削除されます。

コンプライアンス

コンプライアンス

コンプライアンス機能を使用すると、ユーザーはコンプライアンスの結果を達成できます。コンプライアンスには、**通信コンプライアンス**と**構成**コンプライアンスの**2**種類があります。

- **通信コンプライアンスは、**次のコンプライアンス要件タイプで構成されます。
  - サービスレベル契約（SLA）コンプライアンス：他のエンティティと通信する必要があるエンティティのルールを設定できます。コンプライアンス機能を使用して、規制コンプライアンスルールを設定できます。
  - トラフィック制限コンプライアンス:
    オブジェクト間の通信のプロトコルとポートに関する制限を指定できます。
  - セグメンテーション
    コンプライアンス：他のエンティティと通信してはいけない一連のエンティティの周囲にファイアウォールで囲まれたエリアを確立できます。
- **構成コンプライアンス**を使用すると、指定した設定に対して構成コンプライアンスチェックを実行できます。

UI でコンプライアンス要件を指定すると、Cisco Nexus Dashboard Insights は後続のスナップショットで、コンプライアンス要件が Cisco APIC で構成されたポリシーによって満たされているかどうかをを確認します。満たされている場合、コンプライアンス要件が満たされていることを示す異常が発生します。各スナップショットの要件ごとに1つの異常が発生します。たとえば、アシュアランスグループが 15 分ごとにスナップショットでコンプライアンス分析を実行し、スナップショットに 2 つの要件が関連付けられている場合、2 つの異常が発生します。

次の例では、コンプライアンスの**包含**ルールと**除外**ルールに関する情報を説明します。

- 名前が "a" で始まり、"z" で終わるテナントのEPGが含まれます。両方の基準を満たす "abz" などのテナント内のEPGは、1回だけ含まれます。
- 名前が "a" で始まり、テナントが "xyz" でVRF名に "c" が含まれるVRFにもあるテナントのEPGが含まれます。例: DN uni/tn-xyz/ctx-abcde のVRFにあるテナント「abc」の下の EPG が選択されている場合、テナントと VRF の両方の基準が一致することを確認します。VRFテナントが一致しないため、DNがuni/tn-xyz1/ctx-abcdeのVRFにあるテナント "abc" の下のEPGは選択されません。
- "d" を含むものを除く、"a" で始まるテナントの下にあるすべてのEPGが含まれます。例: テナント「abc」 の下の EPG が選択されています。テナント "abcd" の下のEPGは選択されていません。
- DNがuni/tn-rrr/ctx-sssのVRFにもあるEPGを除く、"a" で始まるテナントの下にあるすべてのEPGが含まれます。

コンプライアンス要件のガイドラインと制約事項

- 1 つのコンプライアンス要件を複数のサイトに関連付けることができます。ただし、あるコンプライアンス要件に対して作成されたトラフィックセレクタとオブジェクトセレクタは、別のコンプライアンス要件によって再利用されます。セレクタを新しいコンプライアンス要件に追加するたびに、新しいセレクタを作成する必要があります。
- **[コンプライアンス要件タイプ（Compliance Requirement Type）]** フィールドの **[構成（Configuration）]** および **[通信（Communication）]** タブを選択すると、変更をコントローラに適用する前に、Cisco Nexus Dashboard Insights を介して変更を実行することを選択した場合にのみ満たされるベストプラクティスとビジネス要件を満たすように設定を有効にして適用できます。それ以外の場合、Cisco Nexus Dashboard Insights はコンプライアンスを適用せず、違反として報告します。**[構成（Communication）]** タブを選択すると、ベストプラクティスとビジネス要件を満たす構成を有効にして適用できます。**[通信（Communication）]** タブを選択すると、ビジネスおよび規制目的を満たすネットワークオブジェクト間の通信または分離が可能になります。
- コンプライアンス要件はサイトグループレベルで作成されるため、選択するサイトはそのサイトグループの一部である必要があります。
- コンプライアンス要件のアクションルールは、コンプライアンスルールとアクションを定義するサイトグループ内で使用できます。
- サイトごとに、最大30のアクティブな通信コンプライアンス要件を設定できます。この制限を超えると、**[コンプライアンスの管理（Manage Compliance）]** エリアに要件を追加できません。
- 1つ以上のサイトでコンプライアンスジョブが進行中の場合は、それらのサイトのバグスキャンを開始しないでください。

コンプライアンス要件の作成

次の手順を使用して、コンプライアンスの要件を作成します。

はじめる前に

サイトグループ内に少なくとも1つのサイトを作成する必要があります。

手順

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[追加（Add）]** > **[コンプライアンス要件（Compliance Requirement）]** の順に選択します。
3. **[コンプライアンス要件の作成（Create Compliance Requirement）]**

ダイアログボックスで、次の操作を実行します。

4. **[名前（Name）]** フィールドに、**要件**名を入力します。

   コンプライアンス要件名は、グローバルに一意である必要があります。2
   つの異なるサイトグループに同じコンプライアンス要件名を付けることはできません。

5. **[コンプライアンス要件タイプ（Compliance Requirement Type）]** フィールドで、**[通信（Communication）]** タブを選択します。
6. **[サイト（Sites）]** エリアで、**[サイトの追加（Add Site）]** をクリックします。
7. **[サイトの選択（Select Site）]** ダイアログボックスで、適切な **[サイト名（Site Name）]** を選択します。

   コンプライアンス要件を作成する場合、複数のサイトを選択できますが、同じタイプのサイトを選択する必要があります。

8. **[選択（Select）]** をクリックします。
9. **[基準（Criteria）]** エリアの **[通信タイプ（Communication Type）]** フィールドで、適切な通信タイプを選択します。たとえば、**[要通信（Must Talk To）]**、**[通信不可（Must Not Talk To）]**、**[通信可（May Talk To）]** などのオプションがあります。選択に基づいて設定されているコンプライアンス要件タイプの詳細については、この手順の後にある表を参照してください。
10. **[オブジェクトタイプ（Object Type）]** フィールドと **[トラフィックセレクタ（Traffic Selector）]** エリアで、必要に応じて、適切なオブジェクトとトラフィックセレクタを選択します。

    通信タイプは、2つの異なるオブジェクトグループ間に適用されます。両方のグループに適切な基準を選択します。**[基準の追加（Add Criteria）]** エリアで基準を定義したら、**[選択したオブジェクトの表示（View Selected Objects）]** リンクをクリックして、選択したオブジェクトが適切であることを確認します。選択した通信タイプとトラフィックセレクタルールに基づいて、定義したコンプライアンス要件タイプが表示されます。

11. 必要に応じて、サイトのオブジェクト、基準、トラフィック制限の定義を完了したら、**[保存（Save）]** をクリックして設定を完了します。

次の表は、選択した通信タイプとトラフィックセレクタルールに基づいて構成されているコンプライアンス要件タイプを示しています。

表の後に、通信タイプに関する追加の説明があります。

表7. 通信タイプとトラフィックセレクタルールの選択と結果のコンプライアンス要件タイプ

通信タイプ	トラフィックセレクタルールの選択	選択できるオブジェクト	コンプライアンス要件タイプ
通話先	必須の選択肢	EPG	サービスレベル契約（SLA）　レベル
通話不可	必須でない選択肢	• EPG • テナント	• トラフィックセレクターを選択した場合ルール、コンプライアンスルールはトラフィックの制限 • トラフィックセレクタルールを選択しない場合、遵守ルールはセグメンテーションです。
通話先	必須の選択肢	EPG	トラフィック制限

[要通信（Must Talk To）]：定義されたトラフィック制限ルールの下で、**セレクタ B によって選択された**オブジェクトとセレクタ A が通信する必要があるオブジェクトを設定できます。

[通信不可（Must Not Talk To）]：オブジェクトセレクタ A によって選択されたオブジェクトが、定義されたタイプのトラフィックを使用して、オブジェクトセレクタ B によって選択されたオブジェクトと通信しないようにする場合は、この構成を選択します。この設定では、トラフィック制限ルールはオプションです。これは異なる 2 のタイプのコミュニケーションです。遵守は、次のオプションを使用して構成できます：

- トラフィック制限コンプライアンス：セレクタ A によって選択されたオブジェクトが、トラフィック制限ルールを使用する選択されたタイプのトラフィックを使用して、セレクタ B によって選択されたオブジェクトと通信しないようにするトラフィックセレクタルールを指定できます。この通信は制限されています。
- セグメンテーションコンプライアンス: トラフィックセレクタルールを定義しないことで、セレクタAのオブジェクトがどのタイプのトラフィックを使用してもセレクタBのオブジェクトと通信できないセグメンテーション
  コンプライアンスを設定できます。この場合、ユーザーが定義するトラフィック制限ルールはありません。

[通信可]：トラフィック制限コンプライアンスを作成できます。セレクタ A によって選択されたオブジェクトは、トラフィック制限ルールを使用し特定のタイプのトラフィックのみを使用して、セレクタ B によって選択されたオブジェクトと通信できます。たとえば、EPG A と EPG B

は接続されていますが、フィルタを使用して Cisco APIC 契約で定義されている特定のトラフィックタイプのみを使用して互いに通信できます。Nexus Dashboard Insights ユーザーとして、EPG A がトラフィックタイプ TCP IP を使用して EPG B と通信できることを確認するには、EPG A が TCP IP を使用して EPG B と**通信可能**なトラフィック制限ルールを設定します。

コンプライアンス要件の表示、編集、削除

既存のコンプライアンス要件を表示、編集、または削除するには、次の操作を実行します。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** をクリックします。
3. **[サイトグループの構成（Configure Site Group）]** ページで、**[コンプライアンス要件（Compliance Requirement）]** タブをクリックします。
4. リストされている適切なコンプライアンス要件について、**[アクション（Actions）]** をクリックし、適切なアクションを選択して、適切な手順を完了します。

設定コンプライアンスチェック

次の手順を使用して、設定コンプライアンスチェックを実行します。

指定した設定に対して設定コンプライアンスチェックを実行できます。構成ファイルまたはスナップショットを指定すると、Cisco Nexus Dashboard Insights が継続的にチェックするため、Cisco APIC で定義されたオブジェクトと構成可能な属性の変更を識別できます。構成が指定した設定と異なる場合、違反が発生します。違反ごとに、個別の違反の異常が表示されます。さらに、違反ではないテナントのすべてのオブジェクトに対するすべての変数を含む単一の異常が発生します。

設定コンプライアンスチェックの新しい要件を作成する場合は、次の手順を参照してください。

手順

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[追加（Add）]** > **[コンプライアンス要件（Compliance Requirement）]** の順に選択します。
3. **[新しい要件の作成（Create New Requirement）]** ページの **[名前（Name）]** フィールドに、構成遵守要件の名前を入力します。
4. （任意）**[説明（Description）]** フィールドに説明を入力します。
5. **[状態（State）]** フィールドで、必要に応じて **[有効（Enabled）]** または **[無効（Disabled）]** を選択します。
6. **[コンプライアンス要件タイプ（Compliance Requirement Type）]** で、**[構成（Configuration）]** を選択します。
7. **[サイト（Sites）]** エリアで、サイトグループから適切なサイトを追加します。

8. **[設定（Settings）]** エリアの **[基本構成の設定**（Base Configuration Settings）] フィールドで、**[構成のインポート**（Import Configuration）] を選択します。
アップロードするには、提供されたフィールドにファイルをドラッグ アンド ドロップします。

ファイルをインポートする代わりに選択できる代替オプションがあります。このフィールドの選択内容に応じて、**[設 定 （ Settings ）]** エリアで入力できるさまざまなフィールドが使用可能になります。

9. [保存（Save）] をクリックします。**[管理コンプライアンス（Management Compliance）]** ページに、新しいコンプライアンス要件が表示されます。

JSON/XMLファイルをアップロードする場合、設定要件は編集できません。そのような場合、ファイルをアップロード後、**[アクション（Actions）]** タブから移動して、ファイルを表示またはダウンロードできます。

命名コンプライアンス要件

次の手順を使用して、命名コンプライアンス要件を設定します。

BD、VRF、EPG、契約、サブジェクト、フィルタなどの特定のオブジェクトに命名コンプライアンス要件を設定できます。すべてのオブジェクトタイプがサポートされているわけではありません。

手順

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[追加（Add）]** > **[コンプライアンス要件（Compliance Requirement）]** の順に選択します。
3. **[新しい要件の作成（Create New Requirement）]** ページの **[名前（Name）]** フィールドに、要件の名前を入力します。
4. （任意）**[説明（Description）]** フィールドに説明を入力します。
5. **[状態（State）]** フィールドで、必要に応じて **[有効（Enabled）]** または **[無効（Disabled）]** を選択します。
6. **[コンプライアンス要件タイプ（Compliance Requirement Type）]** で、**[構成（Configuration）]** を選択します。
7. **[サイト（Sites）]** エリアで、サイトグループから適切なサイトを追加します。
8. **[設定（Settings）]** エリアの **[基本構成の設定（Base Configuration Settings）]** フィールドで、**[手動構成（Manual Configuration）]** を選択します。
9. 選択内容に基づいて表示されるフィールドで、オブジェクトタイプを選択し、必要に応じて基準を追加します。
10. **[ルールの追加（Add Rule）]** をクリックし、**[ルールの追加（Add Rule）]** ダイアログボックスで、**[属性（Attribute）]** フィールドのドロップダウンリストから **[名前（Name）]** または **[名前のエイリアス（Name Alias）]** オプションを選択します。
11. [保存（Save）] をクリックします。Cisco Nexus Dashboard Insights は、指定した命名コンプライアンス要件に基づいてチェックの実行を開始します。

[コンプライアンスの管理（Manage Compliance）] ページで、**[アクション（Actions）]** タブで **[要件の表示（View Requirement）]** を選択して、新しい要件を表示します。スナップショットをダウンロードするには、**[設定（Settings）]** タブの **[ダウンロード（Download）]** リンクをクリックします。

BD と EPG 間の関係の設定

この機能を使用すると、固定数のEPGを持つBDセレクタを指定できます。BD コンプライアンスルールを設定することで、BD を関連付けられる EPG の最大数を設定できます。

このコンプライアンスルールの結果として、要件セットが満たされていない場合、違反の異常が発生します。要件が満たされている場合、適用異常が発生します。BDセレクタが解決されていない場合のみ、警告異常が発生します。

ユーザーは、指定された数のEPGがBDに関連付けられていることを確認するための要件を設定できます。この要件でサポートされている演算子は、**At least /At most /Equal to** です。たとえば、BD に少なくとも 5 つの EPG が関連付けられている必要がある要件が設定されており、BD に関連付けられている EPG が 5 未満（0 ～ 4）の場合、違反の異常が発生します。ただし、BD に 5 以上の異常がある場合は、強制異常が発生します。

はじめる前に

この手順を開始する前に、BDを作成しておく必要があります。

BDとEPG間の関係を設定するには、次の手順を実行します。

手順

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[追加（Add）]** > **[コンプライアンス要件（Compliance Requirement）]** の順に選択します。
3. **[新しい要件の作成**（Create New Requirement）] ページの **[名前（Name）]** フィールドに、BD と EPG 間の関係の構成の名前を入力します。
4. （任意）**[説明（Description）]** フィールドに説明を入力します。
5. **[状態（State）]** フィールドで、必要に応じて **[有効（Enabled）]** または **[無効（Disabled）]** を選択します。
6. **[コンプライアンス要件タイプ（Compliance Requirement Type）]** で、**[構成（Configuration）]** を選択します。
7. **[サイト（Sites）]** エリアで、サイトグループから適切なサイトを追加します。
8. **[設定（Settings）]** エリアの **[基本構成の設定（Base Configuration Settings）]** フィールドで、**[手動構成（Manual Configuration）]** を選択します。結果として、追加のフィールドが表示されます。
9. 追加のフィールドで、次の操作を実行します。

a. **[オブジェクトタイプ（Object Type）]** フィールドで、[BD] を選択します。

b. **[一致基準（Matching Criteria）]** フィールドで **[基準の追加（Add Criteria）]** をクリックし、名前または DN 別に適切な選択肢を選択します。

c. **[構成コンプライアンスルール（Configuration Compliance Rules）]** エリアで、**[ルールの追加（Add Rule）]** をクリックして、**[ルールの追加（Add Rule）]** ダイアログボックスを開きます。

d. **[属性（Attribute）]** フィールドで、**[EPG 関連付けカウント（EPG Association Count）]** を選択します。

e. **[演算子（Operator）]** フィールドで、目的の演算子を選択します。

10. **[保存（Save）]** をクリックします。

スナップショット選択のコンプライアンス要件

次の手順を使用して、スナップショット選択の設定コンプライアンスを実行します。

これは、設定コンプライアンスチェックの方法に似ていますが、スナップショットも選択します。この方法を使用すると、スナップショット間を移動するときに、オブジェクトの特定の属性が変更されないようにできます。

手順

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[追加（Add）]** > **[コンプライアンス要件（Compliance Requirement）]** の順に選択します。
3. **[新しい要件の作成（Create New Requirement）]** ページの **[名前（Name）]** フィールドに、要件の名前を入力します。
4. （任意）**[説明（Description）]** フィールドに説明を入力します。
5. **[状態（State）]** フィールドで、必要に応じて **[有効（Enabled）]** または **[無効（Disabled）]** を選択します。
6. **[コンプライアンス要件タイプ（Compliance Requirement Type）]** で、**[構成（Configuration）]** を選択します。
7. **[サイト（Sites）]** エリアで、サイトグループから適切なサイトを追加します。
8. **[設定（Settings）]** エリアの **[基本構成の設定（Base Configuration Settings）]** フィールドで、**[スナップショットの設定（Snapshot Settings）]** を選択します。
9. **[スナップショットの時間（Time of Snapshot）]** フィールドで、目的のスナップショット時間を選択し、**[適用（Apply）]** をクリックします。
10. **[新しい要件（New Requirement）]** ページで、**[保存（Save）]** をクリックします。Cisco Nexus Dashboard Insights がチェックの実行を開始します。

[コンプライアンスの管理（Manage Compliance）] ページで、**[アクション（Actions）]** タブで **[要件の表示（View Requirement）]** を選択して、新しい要件を表示します。スナップショットをダウンロードするには、**[設定**

（Settings）] タブの **[ダウンロード（Download）]** リンクをクリックします。

テンプレートベースのコンプライアンス

テンプレートベースのコンプライアンスを使用すると、任意の属性に基づいてオブジェクトを柔軟に選択し、他のコンプライアンスタスクの設定時にサポートされないさまざまなタイプの一致基準を提供できます。

テンプレートベースのコンプライアンスにより、テンプレートを設定し、クエリのタイプを指定して、有効になっているときに特定の条件を適用するオブジェクトと属性を選択できます。テンプレートクエリ言語を使用すると、構成定可能なオブジェクトを選択し、コンプライアンスに適用する属性を定義できます。**SELECT** では、指定するオブジェクトの特定のサブセットを選択でき、**MATCH** では、コンプライアンスルールを定義できます。

他のタイプのコンプライアンス構成のリリースでは、JSON/XML ファイルをアップロードできます。ファイル内の属性はすべてそのまま一致します。または、名前の一致に基づいて特定のオブジェクトをいくつか選択し、それらのオブジェクトでサポートされる選択属性も設定できます。これにより、指定されたパラメータへのコンプライアンスをチェックする名前に一致する既存または将来のオブジェクトを検索できます。

テンプレートベースのコンプライアンスに関する検証済みの拡張性の制限

- テンプレート要件の数は、設定可能なオブジェクトの総数が150,000のAPICの場合は5です。
- テンプレートごとに、平均して15,000個のオブジェクトを選択します。
- テンプレートあたりのテナント数は 30 テナントで、テナントごとに平均 500 個のオブジェクトを選択します。
- すべてのテンプレートで選択されたオブジェクトの総数が 5*15,000 未満であり、APIC 内の設定の総数が 150,000 オブジェクト未満の場合、5 つ以上のテンプレートを作成できます（要件の上限は合計 30 です）。

テンプレートのガイドライン

テンプレートを定義するときは、次のガイドラインに従ってください。

- テンプレートクエリではJSONファイル形式がサポートされています。XML フォーマットはサポート*されていません*。
- テンプレートには、APICファイルで使用される構造と同じ構造が使用され、オブジェクト、属性、および子があります。
- アップロードできるテンプレートファイルのサイズは、空白を含めて最大15 MBです。Pretty JSON ファイルには、インデントをサポートするための空白があります。ファイルサイズを小さくする場合、空白を削除してからファイルをアップロードしてください。

テンプレートの構文ガイドライン

次のシンタックス例とガイドラインに従ってください。

SELECT のテンプレートシンタックス

SELECT を使用すると、ユーザーは KEYWORDS を使用して定義した基準に基づいてオブジェクトのサブセットを選択できます。次の例では、**SELECT** の後にオブジェクトの属性である属性名が続いています。次のいずれかのキーワードを使用する必要があります。

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

構文：

SELECT(<attribute_name>):

KEY_WORD(<value>)attribute_name（オブジェクトの任意の属性）KEY_WORDS→>

"STARTS_WITH(abc)" "ENDS_WITH(xzy)" "EXACT(abc)" "OR(abc, xyz)"

REGEX(<value>) - 値は標準の正規表現シンタックス "SELECT(name)": "REGEX(Ctrct_[1-3])" に従う必要があります。

キーワードの正規表現の詳細については、正規表現構造の概要を参照してください。

以下はシンタックス例です。

```
{
"fvAEPg":
{
"attributes":
{
"dn": "EXACT(uni/tn-aepg_vzanycons_imd_ctx_pass_7/ap-CTX1_AP1/epg- CTX1_BD1_AP1_EPG7)",
"MATCH(isAttrBasedEPg)": "EXACT(no)"
}
}
}
```

属性に **SELECT** が指定されていない場合、**rn** と **dn** はデフォルトで **SELECT** と見なされます。

MATCH のテンプレートシンタックス

MATCH 基準は、コンプライアンスルールを定義するために使用されます。コンプライアンスルールは、**SELECT**

基準を使用して選択されたオブジェクトに適用されます。属性に一致するキーワードはMATCHであり、一致は指定されたタイプのすべてのオブジェクトに適用されます。一致させる属性と値を指定します。属性は、指定されたタイプのすべてのオブジェクトに一致します。

値は完全に一致する必要はありません。属性と値は次のとおりです。

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

MATCH(<attribute_name>): KEY_WORD(<value>)

以下は、すべての **vzBrCP** コントラクト
オブジェクトを選択した場合の構文例です。コントラクト オブジェクトの名前は
Ctrct_1 または Ctrct_2 または Ctrct_3。次に、スコープがコンテキストであることを定義します。

```
"vzBrCP": {
  "attributes": {
    "SELECT(name)": "REGEX(Ctrct_[1-3])",
    "MATCH(scope)": "EXACT(context)"
  }
}
```

以下は、KEY_WORD が定義されていない場合の、デフォルトの動作が
EXACT.であるシンタックス例です。MATCH(dn)およびMATCH(rn)を使用すると、これらは一致基準として定義されます。

属性（**dn** および **rn** 以外）に **MATCH** または **SELECT**
が指定されていない場合、デフォルトで **MATCH**と見なされます。

```
{
  "fvAEPg": {
    "attributes": {
      "SELECT(dn)": "uni/tn-aepg_vzanycons_imd_ctx_pass_7/ap-CTX1_AP1/epg-
CTX1_BD1_AP1_EPG7",
      "MATCH(isAttrBasedEPg)": "EXACT(no)",
      "prio": "OR(unspecified, prio1)"
    }
  }
}
```

前述の例では、デフォルトで「prio」が **MATCH** になります。

以下は、**KEY_WORD** が **{}**
である汎用テンプレートのシンタックス例です。このテンプレートを使用して、要件のカスタマイズ、属性の選択、正規表現を行うことができます。

KEY_WORD の値は次のようになります。

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

```
{
  "<MO type>": {
    "attributes": {
      "SELECT(<attribute>)": "KEY_WORD(<expression>)",
      "MATCH(<attribute>)": " KEY_WORD (<value>)"
    },
    "children": [
      {
        "<MO type>": {
          "attributes": {
            "SELECT(<attribute>)": " KEY_WORD (<value>)",
            "MATCH(<attribute>)": " KEY_WORD (<value>)"

          },
          "children": [
            {
              "<MO type>": {
                "attributes": {
                  "SELECT((<attribute>)": " KEY_WORD (<value>)",
                  "MATCH(<attribute>)": " KEY_WORD (<value>,<value>)"

                }
              }
            }
          ]
        }
      }
    ]
  }
}
```

以下は、テンプレートベースの設定コンプライアンスの例です。この例では、 **名前が** Ctrct_(1-3) **で始まる**すべてのコントラクトを選択します。それから、**scope をマッチさせます。** これは **context** である必要があります。それらのコントラクトのサブジェクトの **children** については、**name を** any（ワイルドカード）として選択し、**nameAlias は** ABC にする必要があります。

```
{
  "vzBrCP": {
    "attributes": {
      "SELECT(name)": "REGEX(Ctrct_[1-3])",
      "MATCH(scope)": "EXACT(context)"
    },
    "children": [
      {
        "vzSubj": {
          "attributes": {
            "SELECT(name)": "REGEX(.*)",
            "nameAlias": "ABC"
          },
          "children": [
            {
              "vzRsSubjFiltAtt": {
                "attributes": {
                  "SELECT(tnVzFilterName)": "ENDS_WITH(3_1_1)",
                  "MATCH(action)": "deny"
                }
              }
            }
          ]
        }
      }
```

以下は、属性値がnullまたは空のテンプレートの例です。

```
"REGEX(^.{0}$)"
"EXACT()"
"OR(test, )" <- use space
```

```
{
  "fvTenant": {
    "attributes": {
      "MATCH(annotation)": "OR(orchestrator:msc, )",
      "SELECT(name)": "REGEX(aepg_aepg_imd_tnt_pass_[0-9]+)",
    }
  }
}
```

- テンプレートでは、遵守が属性に適用されるため、**属性** の定義は必須です。
- テンプレートでは、**children** の定義は任意です。クエリに children が定義されている場合、選択内容は選択したオブジェクトの実際の children に適用されます。
- テンプレートでは、子配列ごとに1回だけ同じオブジェクトタイプを含めることができます。そうすることで、違反の異常を引き起こすコンプライアンスルールの競合に

つながる要件が作成される可能性を回避できます。

次の *無効な* 例では、**ABCXYZ** という名前の BD がある場合、**fvBD** の両方の子オブジェクト テンプレート スニペットによって選択されますが、**type** は **regular** or **fc** のいずれかであるため、いずれか 1 つが違反になります。

```
{
  "fvTenant": {
    "attributes": {
      "SELECT(name)": "EXACT(tenantABC)"
    },
    "children": [
      {
        "fvBD": {
          "attributes": {
            "MATCH(type)": "EXACT(regular)",
            "SELECT(name)": "REGEX(.*ABC.*)"
          }
        }
      },
            {
        "fvBD": {
          "attributes": {
            "MATCH(type)": "EXACT(fc)",
            "SELECT(name)": "REGEX(.*XYZ.*)"
          }
        }
      }
    ]
```

テンプレートベースのコンプライアンスの設定

次の手順を使用し、テンプレートベースのコンプライアンスを使用して命名コンプライアンスのオブジェクトセレクタを設定します。

手順

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[追加（Add）]** > **[コンプライアンス要件（Compliance Requirement）]** の順に選択します。
3. **[新しい要件の作成（Create New Requirement）]** ページの **[名前（Name）]** フィールドに、要件の名前を入力します。
4. （任意）**[説明（Description）]** フィールドに説明を入力します。
5. **[状態（State）]** フィールドで、必要に応じて **[有効（Enabled）]** または **[無効（Disabled）]** を選択します。
6. **[コンプライアンス要件タイプ（Compliance Requirement Type）]** で、**[構成（Configuration）]** を選択します。
7. [設定（Settings）] エリアで、**[構成の種類（Configuration Type）] をクリックします。**
8. **[基本構成の設定（Base Configuration Settings）]** フィールドで、**[テンプレートベースのコン**

プライアンス（Template Based Compliance）] を選択します。

9. **[サイト（Sites）]** エリアで、サイトグループから適切なサイトを追加します。
10. **[アップロードするファイルを選択またはドラッグアンドドロップ（Choose a file or drag and drop to upload ）]** エリアで、テンプレートベースのファイルをアップロードします。ファイルのアップロードが完了したら、[表示]アイコンをクリックして、アップロードしたファイルの内容を確認できます。

現在、JSONファイルがサポートされています。XMLファイルはサポートされていません。アップロードできるテンプレートファイルのサイズは最大15 MBです。ファイルサイズが 5 MBを超える場合、表示機能は使用できません。ファイルサイズが5 MBを超える場合、ファイルをダウンロードして内容を表示できます。

11. **[保存（Save）]** をクリックします。
12. **[サイトグループの構成**（Configure Site Group）] ページの **[コンプライアンス要件**（Compliance Requirements）] タブに、新しいコンプライアンス要件が表示されます。

ステータスが **[有効（Enabled）]** の場合、コンプライアンス要件は次のスナップショットで使用する準備ができています。ステータスが **[無効（Disabled）]** の場合は、行の [アクション（Actions）] メニューをクリックし、**[編集（Edit）]** をクリックして **[コンプライアンス要件の編集（Edit Compliance Requirement ）]** ページを開くことができます。**[状態（State ）]** フィールドで、状態を **[有効（Enabled）]** に変更し、**[保存（Save）]** をクリックします。

これで、設定は完了です。

テンプレートを使用した命名コンプライアンスのためのオブジェクトセレクタの設定

命名コンプライアンス要件タスクを使用してコンプライアンスを構成する場合、少数の特定のオブジェクトセレクタのみサポートされます（BD、EPG、VRF など）。テンプレートを使用すると、命名コンプライアンス要件の *任意* のオブジェクトを設定できます。

オブジェクトは、APICの任意の管理対象オブジェクトにすることができ、その選択はオブジェクトの識別名に基づきます。選択基準として別の属性を使用する場合は、そのオブジェクトの有効な属性を使用できます。**SELECT** 基準は、次のいずれかのキーワードを使用して定義できます。

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

以下はシンタックス例です。

```
{
   "<object>":{
      "attributes":{
         "SELECT(dn)":"<KEY_WORD>(<value>)",
         "MATCH(nameAlias/name)":"<KEY_WORD>(<value>)"
      }
   }
}
```

命名コンプライアンスの場合、コンプライアンスルールは、**MATCH** によって示される [name] および [nameAlias] フィールドにあります。**MATCH** 基準は、このセクションの前述したキーワードを使用して再度定義できます。

次のサンプルテンプレートを使用して命名コンプライアンスを構成し、選択したオブジェクトが
name または **nameAlias** にマッチするようにします。

```
{
   "vzSubj":{
      "attributes":{
         "SELECT(dn)":"EXACT(subj1)",
         "MATCH(nameAlias)":"STARTS_WITH(ABC)"
      }
   }
}
```

前述のテンプレートでは、"vzSubj"
の代わりに任意のオブジェクトを使用でき、"dn"
の代わりに任意の属性を使用できます。

属性 **dn** はデフォルトで常に **SELECT** と見なされ、他の属性は常に **MATCH** と見なされるため、前述のテンプレートは次の例のように簡略化できます。さらに、キーワードが定義されていない場合、デフォルトの動作は **EXACT** です。

```
{
   "vzSubj":{
      "attributes":{
         "dn":"subj1""nameAlias":"STARTS_WITH(ABC)"
      }
   }
}
```

前述のテンプレートでは、"vzSubj"
の代わりに任意のオブジェクトを使用でき、"dn"
の代わりに任意の属性を使用できます。

前述のテンプレートを使用して命名コンプライアンスのオブジェクトセレクタを設定する手順については、テンプレートベースのコンプライアンスの構成を参照してください。

テンプレートを使用したタグと注釈に基づいたオブジェクトセレクタの設定

APIC ユーザーとして、管理対象オブジェクト（MO）にタグを作成し、使用している APIC バージョンに基づいて、tagInst **または** tagAnnotation **タイプの子オブジェクトを作成できます。**

したがって、APIC
で作成されたタグに基づいてオブジェクトを選択する場合は、このセクションで提供されるテンプレートに従い、タグと注釈に基づいてオブジェクトセレクタを設定できます。

以下は、子オブジェクトを **tagInst** タイプとして表示する例です。

```
{
   "<object>":{
      "attributes":{
         "MATCH(<attribute_name>)":"<KEY_WORD(<value>)"
      },
      "children":[
         {
            "<tagInst>":{
               "attributes":{
                  "SELECT(<attribute_name>)":"<KEY_WORD(<value>)"
               }
            }
         }
      ]
   }
}
```

以下は、子オブジェクトを **tagAnnotation** タイプとして表示する例です。

```
{
   "<object>":{
      "attributes":{
         "MATCH(<attribute_name>)":"<KEY_WORD(<value>)"
      },
      "children":[
         {
            "<tagAnnotation>":{
               "attributes":{
                  "SELECT(<key or value>)":"<KEY_WORD(<value>)"
               }
            }
         }
      ]
   }
}
```

オブジェクトは、**tagAnnotation** または **tagInst** を子として持つ有効な APIC オブジェクトです。オブジェクトの選択は、**tagInst** の場合は名前、**tagAnnotation** の場合は**[キーまたは値（key or value）]**に **SELECT** を使用して、**tagInst** または **tagAnnotation** オブジェクトで定義されます。選択基準は、次のいずれかのキーワードです。

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

遵守ルールは **MATCH** を使用して親オブジェクトレベルで定義され、基準は任意の **KEY_WORD** を使用して定義できます。 **tagInst** または **tagAnnotation** は、次のように遵守ルールには関係しません。それらは選択基準のみを提供します。

次に、タグが「BDs_in_cisco」であるすべての fVBD を **SELECT** するテンプレートの例を示します。BD の名前は **BD** または **app1BD** である必要があります。

```
{
   "fvBD":{
      "attributes":{
         "MATCH(name)":"OR(BD, app1BD)"
      },
      "children":[
         {
            "tagInst":{
               "attributes":{
                  "SELECT(name)":"EXACT(BDs_in_cisco)"
               }
            }
         }
      ]
   }
}
```

テンプレートを使用してタグと注釈に基づいてオブジェクトセレクタを設定する手順については、テンプレートベースのコンプライアンスの構成を参照してください。

「テンプレートベースのコンプライアンスの構成」の手順を使用してタグと注釈のオブジェクトセレクタを設定する場合は、追加の手順を実行する必要があります。**[保存（Save）]** をクリックする前に、**[新しい要件の作成（Create New Requirement）]** ページで、**[tagAnnotation/tagInst に基づいたオブジェクト選択を有効にする（Enable Object Selection Based on tagAnnotation/tagInst）]** フィールドのチェックボックスをオンにする必要があります。したがって、いずれかのオブジェクトにtagAnnotationまたはtagInstがある場合、2つのオブジェクトの選択基準に基づいて親が選択されます。

コンプライアンス分析のスケジュール

次の手順を使用して、コンプライアンス分析をスケジュールします。

はじめる前に

サイトグループ内に少なくとも1つのサイトを作成する必要があります。

手順

1. **[概要（Overview）]** ページの上部で、コンプライアンス分析を実行するサイトグループを選択します。必要に応じて、リストされているサイトグループを展開し、表示されているサイトを確認してサイトを選択します。
2. サイトの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** をクリックします。
3. **[サイトグループの構成（Configure Site Group）]** ページで、**[アシュアランス分析（Assurance Analysis）]** タブをクリックします。**[全般（General）]** エリアの下に、選択したサイトで実行される分析の詳細が、デフォルト値に基づいて一覧表示されます。スケジュールされた分析を実行するためのデフォルト値はすでに入力されています。
4. 分析を開始するには、サイトの編集アイコンをクリックします。
5. **[構成（Configuration）]** ダイアログボックスで、**[状態（State）]** を **[無効（Disabled）]** から **[有効（Enabled）]** に変更します。
6. 必要に応じて、**[開始時刻（Start Time）]**、**[繰り返し間隔（Repeat Every）]**、および **[終了日（End On）]** フィールドの値を変更します。**[保存（Save）]** をクリックします。

分析は、スケジュールされた選択内容に基づいて実行されます。

同じページの **[履歴（History）]** テーブルに分析ジョブが表示され、**[開始時刻（Start Time）]** の下にステータスが表示されます。たとえば、**[スケジュール済み（Scheduled）]** または **[進行中（In-Progress）]** と表示されます。分析が完了すると、ステータスに **[完了（Completed）]** と表示されます。分析に使用できるようになると、**[終了時刻（End Time）]** と **[実行時間（Run Time）]** も表示されます。

インスタント コンプライアンス分析の実行

次の手順を使用して、インスタント コンプライアンス分析を実行します。

はじめる前に

サイトグループ内に少なくとも1つのサイトを作成する必要があります。

手順

1. **[概要（Overview）]**

ページで、コンプライアンス分析を実行するサイトグループを選択します。必要に応じて、リストされているサイトグループを展開し、表示されているサイトを確認してサイトを選択します。

2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。
3. **[サイトグループの構成（Configure Site Group）]** ページで、**[アシュアランス分析（Assurance Analysis）]** タブをクリックします。**[全般（General）]** エリアの下に、選択したサイトで実行される分析の詳細が、デフォルト値に基づいて一覧表示されます。
4. インスタント分析を実行するには、サイトの **[今すぐ実行（Run Now）]** ボタンをクリックします。というメッセージが表示されます。メッセージが表示されます。

同じページの **[履歴（History）]** テーブルに分析ジョブが表示され、**[開始時刻（Start Time）]** の下にステータスが表示されます。たとえば、**[スケジュール済み（Scheduled）]** または **[進行中（In-Progress）]** と表示されます。分析が完了すると、[完了（Completed）] と表示されます。分析に使用できるようになると、**[終了時刻（End Time）]** と **[実行時間（Run Time）]** も表示されます。

コンプライアンス分析の表示

次の手順を使用して、コンプライアンス分析の詳細を表示します。

はじめる前に

サイトのコンプライアンス分析を少なくとも1回完了する必要があります。

手順

1. **[概要（Overview）]** ページの左側のナビゲーションで、**[コンプライアンス（Compliance）]** をクリックします。
2. **[コンプライアンス分析**（Compliance Analysis）] ページで異常を表示するには、適切なサイトとスナップショットを選択します。
3. ページの上部で、適切なサイトを選択します。
4. ドロップダウンリンクをクリックして時間を表示し、分析を確認する適切なモードを表示します。選択したモードに基づいて、追加のフィールドを選択できる場合があります。
5. 選択が完了したら、**[適用（Apply）]** をクリックします。

分析が生成された任意の期間およびスナップショットの選択に対して、使用可能なモードから分析を表示できます。また、設定されたコンプライアンス要件の結果としてサイトに生成された異常も表示できます。**[コンプライアンスの概要（Compliance summary）]** エリアには、生成された異常の総数が重大度別に表示されます。**[非準拠リソース（Non-compliant resources）]** エリアには、定義された要件の影響を受けたオブジェクトが表示されます。**[要件違反（Requirement Violations）]**

エリアには、完全に満たされているコンプライアンス要件の割合が表示されます。**[要件タイプ（Requirement Type）]** エリアには、このサイトに関連付けられている各要件タイプの数が表示されます。このフィールドのドロップダウン矢印をクリックしてビューを展開すると、関連付けられている要件タイプと一緒に、違反、適用済み、または検証済みの詳細が表示されます。

異常とアラートの詳細については、アラートの分析を参照してください。

コンプライアンス要件の表示

Nexus Dashboard Insightsリリース6.1.1以降では、ページから移動しなくても、コンプライアンス異常に関連付けられたコンプライアンス要件を確認できます。

はじめる前に

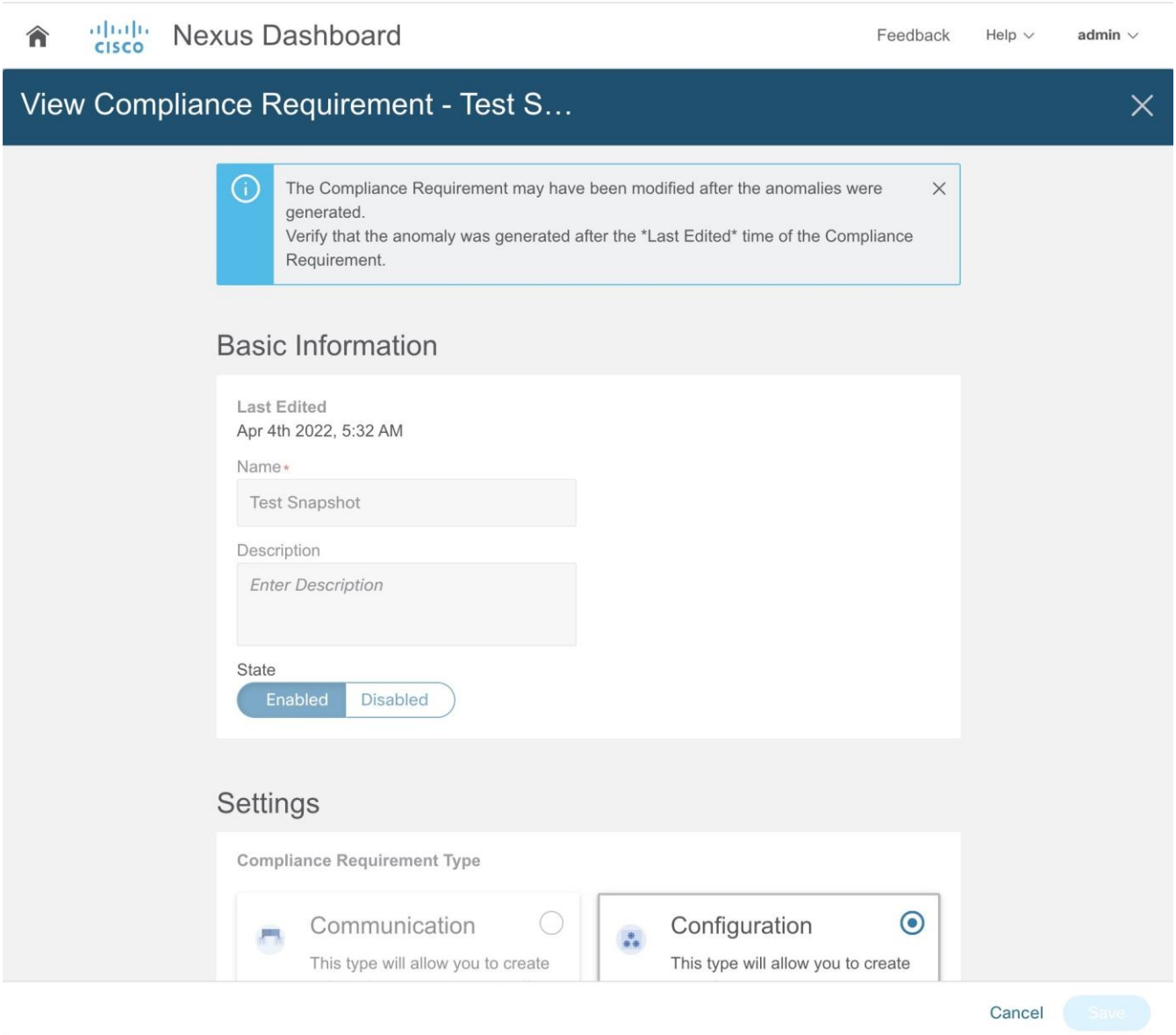
コンプライアンス要件のアシュアランス分析を実行する必要があります。

手順

1. **[概要（Overview）]** ページの左側のナビゲーションで、**[コンプライアンス（Compliance）]** > **[コンプライアンス（Compliance）]** の順に選択します。
2. **[コンプライアンス分析（Compliance Analysis）]** ページで、**[異常（Anomalies）]** セクションまで下にスクロールし、ドロップダウンメニューから **[集約（Aggregated）]** を選択します。

   選択内容に基づいて、異常がテーブルに表示されます。*集約された異常* についてのみ、コンプライアンス要件の詳細を表示できます。
3. **[異常（Anomalies）]** テーブルで、目的の異常の適切な行をクリックします。
4. 開いた異常のタイトルページの **[影響を受けるオブジェクト（Affected Object）]** エリアで、適切な行をクリックして概要ペインを開きます。
5. 概要ペインの右上隅にある [詳細（Details）] アイコンをクリックして、**[コンプライアンス要件の表示**（View Compliance Requirement）] ページを開きます。

[コンプライアンス要件の表示（View Compliance Requirement）] ページでは、基本情報や設定情報など、コンプライアンス要件の詳細を確認できます。



ページの上部にあるバナーは次のとおりです。*コンプライアンス要件は、異常が生成された後に異常が発生した後。コンプライアンス要件の最終編集時刻の後に異常が生成されたことを確認します。*

ページの上部には、このコンプライアンス要件の最終編集日時（異常に関連付けられた日時）を表示する **[最終編集日（Last Edited）]** フィールドがあります。

[コンプライアンス要件の表示（View Compliance Requirement）] ページの **[最終編集日（Last Edited）]** フィールドにスナップショットのタイムスタンプより後の日時が表示されている場合、**[コンプライアンス要件の表示（View Compliance Requirement）]** ページのコンテンツに基づいた異常は生成されません。**[コンプライアンス要件の表示（View Compliance Requirement）]** ページに更新された正確な詳細を表示するには、異常を再生成する必要があります。

[サイトグループの構成（Configure Site Group）] エリアでコンプライアンス要件を編集すると、このエリアで日時が更新されます。コンプライアンス要件の編集の詳細については、「コンプライアンス要件の編集、削除」を

参照してください。

異常とアラートの詳細については、アラートの分析を参照してください。

コンプライアンス要件のガイドラインと制約事項の表示

異常を生成した後の任意の時点で、次のいずれかの変更が行われます。

- 既存のコンプライアンス要件の名前が編集および変更されます。
- 既存のコンプライアンス要件が削除され、同じ名前の新しいコンプライアンス要件が作成されます。
- 既存のコンプライアンス要件の名前が変更され(ABCがXYZに変更)、以前のコンプライアンス要件名を持つ新しいコンプライアンス要件が作成されます(たとえば、ABC)。

[コンプライアンス要件の表示（View Compliance Requirement）] ページに更新された正確な詳細を表示するには、異常を再生成する必要があります。**[コンプライアンス要件の表示（View Compliance Requirement）]** ページの **[最終編集日（Last Edited）]** フィールドにスナップショットのタイムスタンプより後の日時が表示されている場合、**[コンプライアンス要件の表示（View Compliance Requirement）]** ページのコンテンツに基づいた異常は生成されません。

ポリシー CAM

ポリシー CAM

ポリシーCAM機能は、ファブリック内のリソースの使用方法と使用場所を決定します。ポリシー CAM は、ネットワーク内のリソース使用率と、ポリシー連想メモリ（ポリシー CAM）使用率の量に関する情報を提供します。

Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページの左側のナビゲーションで、**[参照（Browse）]**> **[リソース使用率（Resource Utilization）]** の順に選択します。**[リソース使用率（Resource Utilization）]** 作業ペインで、**[参照（Browse）]** タブをクリックして [ポリシーCAM（Policy CAM）] タブを見つけます。

サイトグループ内のすべてのノードに関するポリシー CAM アナライザの詳細の表示

サイトグループ内のノードのポリシーCAMの詳細を表示するには、次の手順に従います。

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページの上部で、適切なサイトグループを選択します。
2. 左側のナビゲーションで、**[参照（Browse）]**>**[リソース使用率（Resource Utilization）]** の順に選択します。
3. 作業ペインの [時間セレクタ（Time Selector）] フィールドで、リソース使用率を表示する時間内の適切なスナップショットを選択し、**[適用（Apply）]** をクリックします。

   選択した時間範囲内で、サイトグループに含まれる各サイトの最後のスナップショットが考慮されます。したがって、選択した時間範囲内のアプリケーションの最新の状態を取得できます。

4. **[参照（Browse）]** をクリックし、**[上位ノード（Top Nodes by）]** フィールドで、ドロップダウンリストから **[ポリシー TCAM（Policy TCAM）]** を選択します。リソース使用率に基づいて、サイトグループ内の各ノードのリストとともに棒グラフが表示されます。使用率が最大のノードから始まり、次に TCAM 使用率が低いノードが続きます。グラフの特定のバーにカーソルを合わせると、最大容量、ハードウェア数、使用率など、そのノードの詳細が表示されます。
5. 次の表で、ページの **[ポリシー CAM（Policy CAM）]** タブをクリックして、各ノードの異常スコアの詳細を表示します。異常スコアには、そのノードに関連付けられた異常の最高カテゴリが表示されます。たとえば、ノードに 1 つの警告異常と 1 つのクリティカルな異常が関連付けられている場合、そのノードの異常スコアには [クリティカル（Critical）] と表示されます。
6. **[ポリシーCAM アナライザの起動（Launch Policy CAM Analyzer）]** ボタンをクリックします。

7. **[ポリシーCAM アナライザ（Policy CAM Analyzer）]** ページの **[サイトの分析（Analyze Site）]** エリアで、適切なサイトとスナップショットを選択し、**[適用（Apply）]** をクリックします。サイトグループ内のすべてのノードの詳細が表示されます。
8. ページ内の情報の表示を変更するには、ページの右上にあるアイコンを切り替えます。アイコンを左側に切り替えると、サイト内の選択したスナップショットに対して生成されたポリシー CAM の異常概要が表示されます。重大度に基づいて異常数が表示されます。アイコンを右側に切り替えると、情報が表形式で表示されます。

各ノードで生成されたルールの使用率と異常を表示できます。また、各ノードに関連する異常スコアも表示されます。**[関連するポリシー（Associated Policies）]** エリアで、特定のノードの契約フィルタとして **[フィルタ（Filter）]** 列を使用できます。各列の各項目を選択して、テナント、契約、EPG間の関連付けと関係を表示できます。**[ポリシー CAM 統計情報（Policy CAM Statistics）]** テーブルには、すべてのノードと関連するルールが表示され、特定のノードの詳細にドリルダウンできます。**[ポリシー CAM ルール（Policy CAM Rules）]** テーブルでは、選択したスナップショットに基づいてすべてのノードのリストを表示できます。**[異常（Anomalies）]** テーブルでは、選択した時間のスナップショットで生成された異常を、ノードごとに個別に、または集約して表示できます。

異常とアラートの詳細については、アラートの分析を参照してください。

サイトグループ内の特定のノードに関するポリシーCAM アナライザの詳細の表示

サイトグループ内の特定のノードに関するポリシーCAMの詳細を表示するには、次の手順に従います。

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページの上部で、適切なサイトグループを選択します。
2. 左側のナビゲーションで、**[参照（Browse）]** > **[リソース使用率（Resource Utilization）]** の順に選択します。
3. 作業ペインの [時間セレクタ（Time Selector）] フィールドで、リソース使用率を表示する時間内の適切なスナップショットを選択し、**[適用（Apply）]** をクリックします。

> 選択した時間範囲内で、サイトグループに含まれるすべてのサイトの最後のスナップショットが考慮されます。

4. 次の表で、ページの **[ポリシー CAM（Policy CAM）]** タブをクリックして、各ノードの異常スコアの詳細を表示します。異常スコアには、そのノードに関連付けられた最高カテゴリが表示されます。
5. **[ノード（Node）]** 列で特定のノードをクリックすると、サイドバーにそのノードのリソース数の詳細が

表示されます。特定のノードのリソース使用率に対して生成された異常も、クリティカル、メジャー、マイナー、警告などのタグ付きで表示されます。

6. サイドバーで、右上の [詳細（Detail）] アイコンをクリックして、そのノードの **[リソースの詳細（Resource Details）]** ページを表示します。**[リソースの詳細（Resource Details）]** ページの **[ポリシーCAM（Policy CAM）]** セクションには、特定のノードのリソース使用率の詳細が表示されます。

ページ内の情報の表示を変更するには、ページの右上にあるアイコンを切り替えます。アイコンを左側に切り替えると、特定のノードの選択したスナップショットに対して生成されたポリシーCAM異常の概要が表示されます。重大度に基づいて異常数が表示されます。アイコンを右側に切り替えると、情報が表形式で表示されます。

1.**[完了]**をクリックして、**[リソースの詳細]**ページを閉じます。

[ポリシーCAM（Policy CAM）] タブを表示しているときに **[ポリシーCAM アナライザの起動（Launch Policy CAMM Analyzer）]** ボタンをクリックすると、選択したノードに基づいてポリシー CAM アナライザのフィルタリングが起動します。

異常とアラートの詳細については、アラートの分析を参照してください。

トラブルシューティング

デルタ分析

Nexus Dashboard Insightsでは、サイトグループの分析が定期的に実行され、データは15分間隔で収集されます。

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。差分分析は、次のワークフローで構成されています。

- **[新規分析の作成]**: 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。
- **[差分分析の表示]**: 正常性の差分やポリシーの差分など、成功した差分分析の結果を表示できます。差分分析結果の表示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。結果は次のエリアに表示されます。

- **[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。
- **[リソース別の正常性の差分]**: 正常性に変化が見られたリソースの数がタイプ別に表示されます。変化は、解決された問題または新たに検出された問題のいずれかです。
- **[異常]**: **集約**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。**個別**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。

ポリシーの差分

ACI のポリシーの差分

ポリシーの差分では、2つのスナップショット間のポリシーの違いを分析し、ACIファブリックの変更点の

相互に関連するビューを提供します。

ポリシーの差分ビューでは、次のことができます。

- つのスナップショット間で変更されたポリシーオブジェクトを表示する。
- つのスナップショット間で追加、変更、および削除されたポリシー設定を表示する。
- 以前のスナップショットポリシーと後のスナップショットポリシーのポリシー設定をエクスポートする。
- ポリシーの差分の追加、変更、削除された領域、および変更されていない領域のテキストを検索する。
- ポリシーの差分で変更された領域のコンテキストを表示する。
- つのスナップショット間のAPIC監査ログの違いを表示する。

DCNM のポリシーの差分

DCNM サイトグループのポリシーの差分では、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。

ポリシーの差分ビューでは、次のことができます。

- 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表示する。
- ポリシーの差分で変更された領域のコンテキストを表示する。

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、オンラインサイトグループ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。

- **APIC 設定エクスポートポリシー**は、両方のスナップショットで同じフォーマット（XML/JSON）である必要があります。
- APIC設定エクスポートポリシーの収集エラーがある場合、ポリシーの差分は実行されません。

差分分析の作成

次の手順を使用して、差分分析を作成します。

はじめる前に

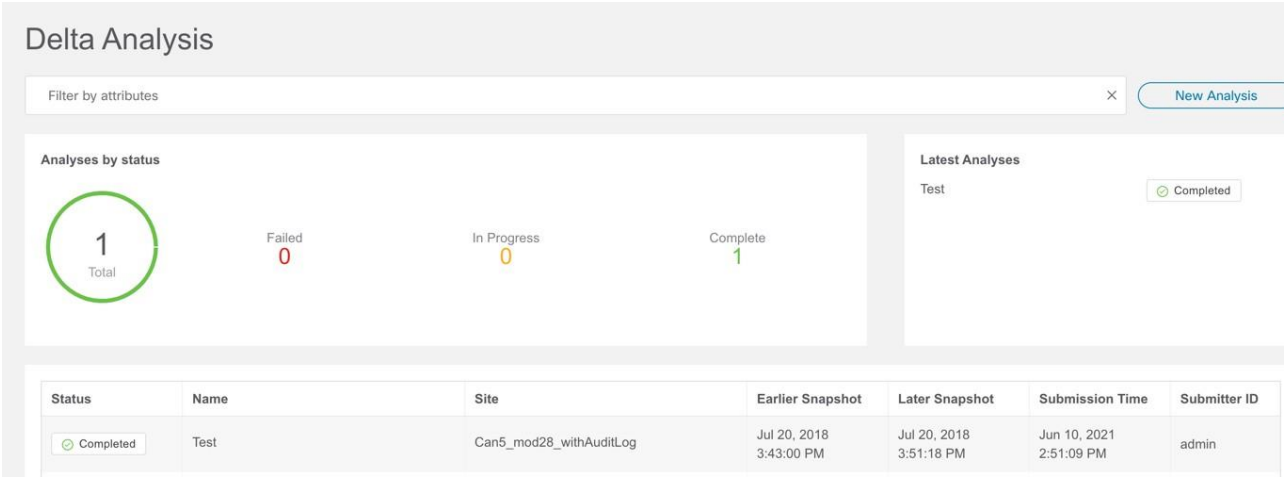
ACIアシュアランス　　グループ
ユーザーの場合、APIC管理者のwritePriv権限により、APICホストとリーフスイッチで情報を収集できます。**APIC 設定エクスポートポリシー**を構成するには、APIC 管理者の writePriv 権限が必要です。

手順

1. **[トラブルシュート（Troubleshoot）]** > **[差分分析（Delta Analysis）]** の順に選択します。
2. [サイトグループ]メニューから、サイトグループを選択します。
3. **[新規差分分析（New Delta Analysis）]** をクリックします。
4. **[差分分析の作成]**の次のフィールドに入力します。
   a. **[名前]**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。
   b. **[サイト]**をクリックしてサイトを選択します。
   c. **[日付と時刻の選択]**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。
   d. **[日付と時刻の選択]**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。[保存（Save）] を **[適用]**をクリックします：

> 差分分析用に選択した2つのスナップショットは、同じサイトグループに属している必要があります。

5. [Create] をクリックします。
6. 差分分析のステータスは、**[差分分析]**テーブルに表示されます。



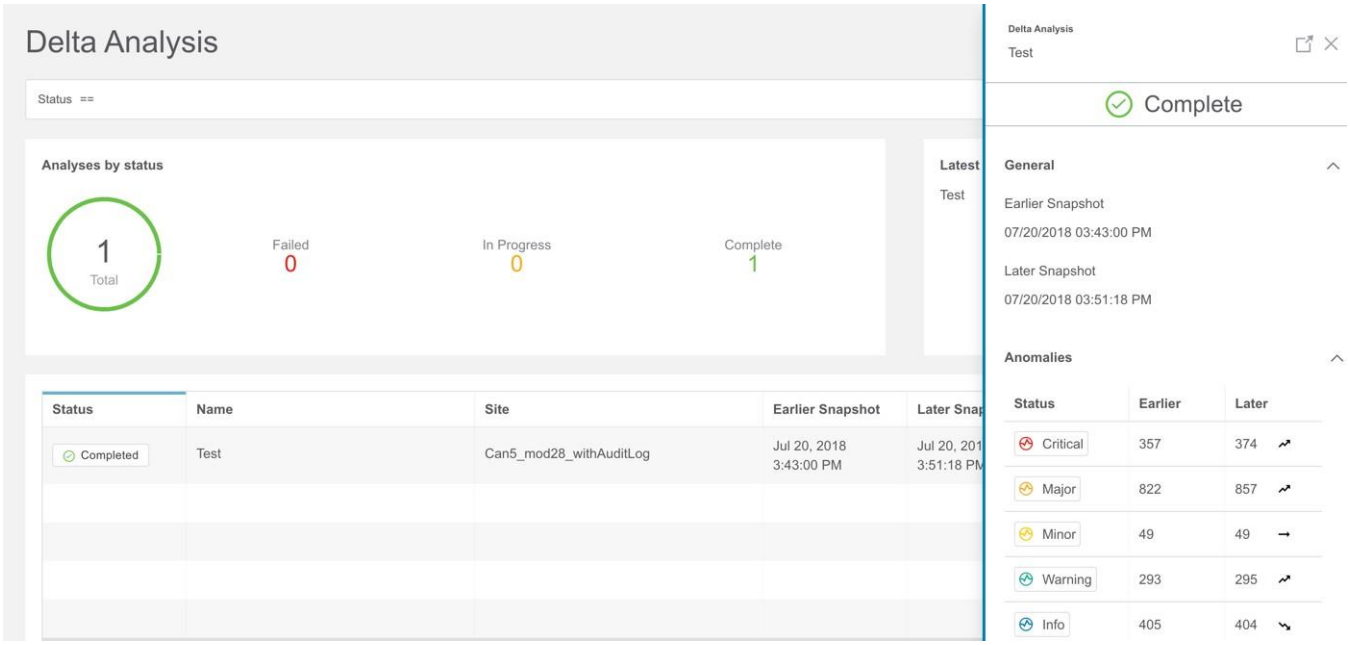
一度に1つの差分分析を実行できます。別の差分分析を実行するには、現在の差分分析を停止してから、別の差分分析を開始する必要があります。

7. (任意) [ステータス]列から、進行中またはスケジュールされた分析を選択し、**[停**

止]をクリックして差分分析を停止します。
デルタ分析を停止します。

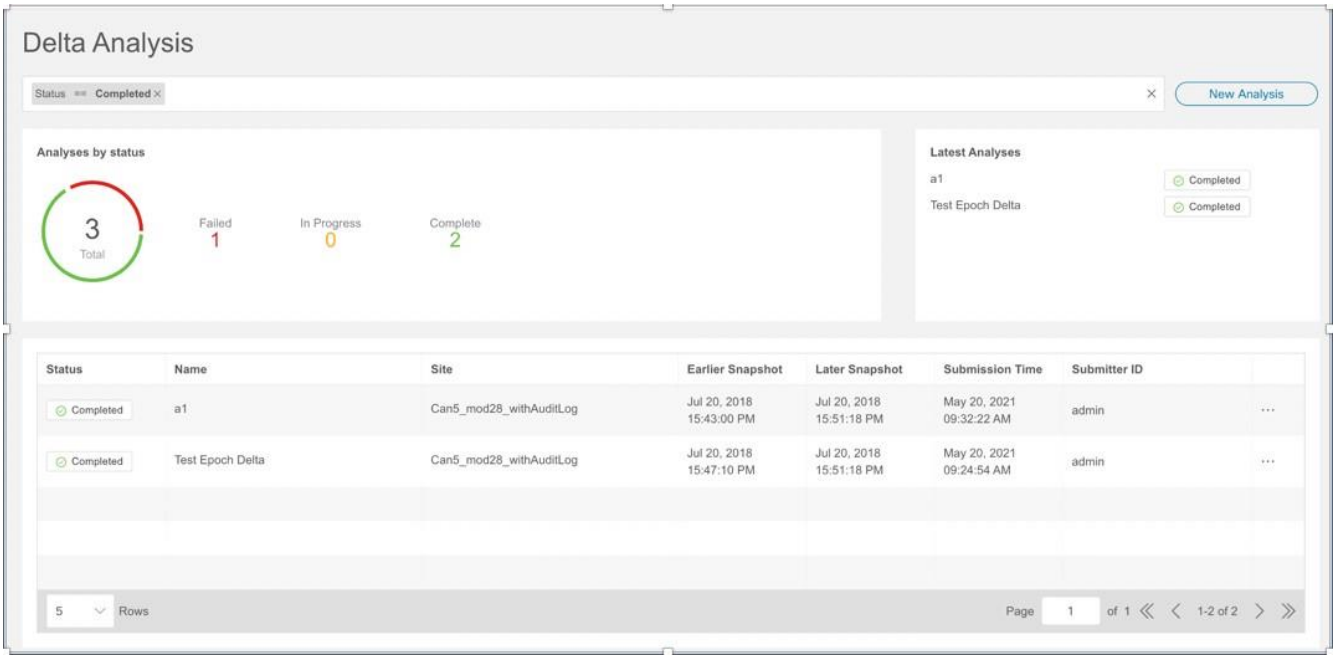
8. 差分分析の結果を表示するには、**[差分分析（Delta Analysis）]**
テーブルから差分分析を選択します。概要ペインには、一般的な情報や異常情報などの詳細が表示されます。

9. [詳細]アイコンをクリックして、正常性の差分とポリシーの差分の詳細を表示します。



差分分析の表示

差分分析ダッシュボードには、特定のサイトグループまたはサイトのステータスごとの分析グラフが表示され、最新の分析が表示されます。



フィルタバーを使用すると、ステータス、名前、および送信者別に分析をフィルタ処理できます。

このページには、分析が表形式でも表示されます。分析はステータスでソートされています。

- 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。
- 差分分析を編集または削除するには、差分分析の管理を参照してください。

正常性の差分分析の表示

次の手順を使用して、正常性の差分分析の結果を表示します。

手順

1. **[トラブルシュート（Troubleshoot）]** > **[差分分析（Delta Analysis）]** の順に選択します。
2. [サイトグループ]メニューから、サイトグループを選択します。
3. [差分分析]テーブルから完了した分析を選択します。概要ペインで、[詳細]アイコンをクリックして、正常性とポリシーの差分の詳細を表示します。
4. **[正常性の差分（Health Delta）]** をクリックして、ファブリックの正常性の結果を表示します。

General

07/20/2018 03:43:00 PM	07/20/2018 03:51:18 PM	8mins 18secs
Earlier	Later	Time Range

Health Delta | Policy Delta

Anomaly Count

Health Delta by Resources

Only Show Mismatch

Resources	Total Earlier	Total Later	Unhealthy Earlier	Unhealthy Later	Total Unhealthy in Earlier Only	Total Unhealthy in Later Only	Total Unhealthy in Both	No issues Earlier	No issues Later
App Profiles	127	127	90	90	0	0	90	37	37
BDs	179	180	105	108	0	3	105	74	72
Contracts	122	122	48	48	0	0	48	74	74
Endpoints	1435	1435	185	202	0	17	185	1250	1233
EPGs	460	461	307	306	2	1	305	153	155
External Routes	226	226	18	20	0	2	18	208	206
Interfaces	590	593	81	81	0	0	81	509	512
Internal Subnets	1527	1529	113	135	0	22	113	1414	1394
L3Outs	86	85	83	82	1	0	82	3	3
Leafs	4	4	4	4	0	0	4	0	0
Tenants	54	55	50	51	0	1	50	4	4
VRFs	86	86	78	78	0	0	78	8	8

Anomalies Individually

Filter by attributes

System Status	Category	Affected Nodes	Detection Time	Title	Description
Critical Active	vrfSecurity Security	candid5-leaf1	Jul 20 2018 03:43:00.000 PM	ENFORCED_VRF_POLICY_VIOLATION	VRF is in enforced mode. APIC policy for implicit deny log is not enforced on Leaf hardware.
Critical Active	vrfSecurity Security	candid5-leaf1	Jul 20 2018 03:43:00.000 PM	ENFORCED_VRF_POLICY_VIOLATION	VRF is in enforced mode. APIC policy for implicit deny log is not enforced on Leaf hardware.
Critical Active	Subnet Route Forwarding	candid5-leaf1, candid5-leaf3	Jul 20 2018 03:43:00.000 PM	BD_SUBNET_DEPLOYMENT_ERROR	A bridge domain (BD) subnet that should be deployed by APIC onto a leaf switch is not present.
Critical Active	Subnet Route Forwarding	candid5-leaf3	Jul 20 2018 03:43:00.000 PM	EXTERNAL_ROUTED_NETWORK_INTERFACE_SUBNET_DEPLOYMENT_ERROR	An interface belonging to an L3Out is not deployed on the leaf switch(es) where it is expected to be deployed.
Critical Active	Subnet Route Forwarding	candid5-leaf3	Jul 20 2018 03:43:00.000 PM	EXTERNAL_ROUTED_NETWORK_INTERFACE_SUBNET_DEPLOYMENT_ERROR	An interface belonging to an L3Out is not deployed on the leaf switch(es) where it is expected to be deployed.
Critical Active	Subnet Route Forwarding	candid5-leaf1	Jul 20 2018 03:43:00.000 PM	EXTERNAL_ROUTED_NETWORK_INTERFACE_SUBNET_DEPLOYMENT_ERROR	An interface belonging to an L3Out is not deployed on the leaf switch(es) where it is expected to be deployed.
Critical Active	Interface Forwarding	candid5-spine2	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.
Critical Active	Interface Forwarding	candid5-spine1	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.
Critical Active	Interface Forwarding	candid5-spine1	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.
Critical Active	Interface Forwarding	candid5-spine2	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.

10 Rows | Page 1 of 192 | 1-10 of 1915

5. **[異常数]**には、2つのスナップショット間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、両方のスナップショットに共通する異常数を表します。3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。
6. 異常数をクリックして異常の詳細を表示します。
7. **[リソース別の正常性の差分]**には、さまざまなリソースタイプの正常性の差分が表示されます。また、問題のあるリソースの数、異常なリソース、およびリソースの総数も表示されます。
   a. リソース数をクリックして、そのリソース数に関連付けられたリソースを表示します。
   b. リソース名をクリックして、そのリソースの異常の詳細を表示します。
   c. 2つのスナップショット間の変更を表示するには、**[不一致のみを表示]**チェックボックスをオンにします。
8. **[異常（Anomalies）]** テーブルには、異常の集約ビューと個別ビューが表示されます。
   a. ドロップダウンメニューから **[集約（Aggregated）]** を選択して、2つのスナップショット間で集約された異常を表示します。
   b. ドロップダウンメニューから**[個別]**を選択して、2つのスナップショット間における個別の異常を表示します。
   c. 異常を選択してその異常の詳細を表示します。詳細については、異常の分析を参照してください。
9. **[フィルタ（Filter）]** バーで、複数のフィルタを使用して異常を検索します。
   a. [スナップショット（Snapshot）]アイコンをクリックして、前のスナップショット、後のスナップショット、前のスナップショットのみ、後のスナップショットのみ、両方のスナップショット、および差分分析に使用される統合スナップショットなどのスナップショットでフィルタ処理します。
   b. フィルタバーを使用して、リソースでフィルタ処理し、次にリソース名またはDNでフィルタ処理します。
   c. 結果が**[異常（Anomalies）]**テーブルに表示されます。異常を選択してその異常の詳細を表示します。

ACI に関するポリシーの差分分析の表示

次の手順を使用して、ACIサイトグループに関するポリシーの差分分析の結果を表示します。

手順

1. **[トラブルシュート（Troubleshoot）]** > **[差分分析（Delta Analysis）]** の順に選択します。
2. [サイトグループ]メニューから、サイトグループを選択します。
3. [差分分析]テーブルから完了した分析を選択します。概要ペインで、[詳細]アイコンをクリックして、正常性とポリシーの差分の詳細を表示します。

4. **[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。ポリシーの差分には、[変更されたポリシーオブジェクト]、[ポリシービューア]、および[監査ログ]の3つのパネルが含まれています。
5. **[変更されたポリシーオブジェクト**（Changed Policy Object）] パネルには、2つのスナップショット間で変更されたポリシーオブジェクトツリーが表示されます。
   a. 特定のオブジェクトをドリルダウンして、変更されたオブジェクトタイプを表示します。数字は、オブジェクトに対する変更の数を示します。
   b. 変更されたオブジェクトタイプを選択して、変更された異常を表示します。
   c. [DN]リンクをクリックして、APICで影響を受けるオブジェクトタイプにアクセスします。
   d. **[変更の表示（Show Changes）]** をクリックして、[ポリシービューア（Policy Viewer）] および [監査ログ（Audit Log）] パネルに変更を表示します。[ポリシービューア]および[監査ログ]パネルでは、対応する変更が強調表示されます。
   e. **[検索]** バーを使用して、DN 検索を実行します。
6. **[ポリシービューア（Policy Viewer）]** パネルには、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ポリシー構成が表示されます。以前のスナップショットのポリシー設定は、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ポリシー設定は、後のスナップショットポリシーと呼ばれます。
   a. カラーコードを使用して、2つのポリシー間で追加、削除、変更されたコンテンツ、および変更されていないコンテンツを可視化します。
   b. 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。
   c. [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。
   d. **[検索]** バーに値を入力して、テキスト検索を実行します。
7. Cisco Nexus Insightsは、APICから監査ログを収集し、2つのスナップショット間の監査ログの違いを計算します。**[監査ログ（Audit Log）]** パネルには、2つのスナップショット間で作成されたすべての監査ログが表示されます。データセンターで変更された内容の相関ビューが **[監査ログ（Audit Log）]** パネルに表示されます。**[変更されたポリシーオブジェクト（Changed Policy Objects）] パネルで特定のオブジェクトを選択すると、関連する相違点が [ポリシービューア（Policy Viewer）]** パネルで強調表示され、関連する監査ログが **[監査ログ（Audit Log）]** パネルで強調表示されます。APIC監査ログは、監査可能である必要があるログインとログアウトや構成の変更など、ユーザーが開始したイベントのレコードです。すべてのスナップショットについて、監査ログの履歴は過去24時間までに制限されています。
   a. **[検索]** バーを使用して、DN、ユーザー ID、またはテキスト検索を実行します。
   b. 監査ログエントリで **[詳細を表示（View More）]**

をクリックして、変更時刻と変更者を表示します。監査ログエントリのタイムスタンプは、APIC監査ログのタイムスタンプに対応します。

c. [監査ログ]エントリをクリックして、APICで影響を受けるオブジェクトタイプにアクセスします。

差分分析の管理

次の手順を使用して、差分分析を編集および削除します。

手順

1. **[トラブルシュート（Troubleshoot）]** > **[差分分析（Delta Analysis）]** の順に選択します。
2. [サイトグループ]メニューから、サイトグループを選択します。
3. **[差分分析（Delta Analysis）]** テーブルから差分分析を選択します。
4. その他アイコンをクリックし、[編集]を選択して分析を編集します。
5. その他アイコンをクリックし、[削除]を選択して分析を削除します。進行中の差分分析を削除するには、削除する前に差分分析を停止する必要があります。
6. [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、**[停止（STOP）]** をクリックして差分分析を停止します。
7. 差分分析の結果を表示するには、**[差分分析（Delta Analysis）]** テーブルから差分分析を選択します。概要ペインには、一般的な情報や異常情報などの詳細が表示されます。
8. [詳細]アイコンをクリックして、正常性の差分とポリシーの差分の詳細を表示します。

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はサイト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ーし、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 - ユーザーはサイト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。このリリース以降、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。

ログコレクタダッシュボード

ログコレクタ
ダッシュボードには、特定のサイトグループまたはサイトの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、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。フィルタバーの有効な演算子は次のとおりです。

- == - 完全に一致するログを表示します。この演算子の後には、テキストや記号を続ける必要があります。

- contains -
  入力されたテキストまたは記号を含むログを表示します。この演算子の後には、テキストや記号を続ける必要があります。

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。

1. サイドペインのテーブルでログ収集ジョブを選択して、追加の詳細を表示します。
2. アイコンをクリックして 、**[ログ収集ステータス]**ページを表示します。**[ログ収集ステータス]**ページには、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。

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。

1. **[トラブルシュート]** > **[ログコレクタ]**をクリックします。

   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]**テーブルに表示されます。

2. サイドペインのテーブルでジョブを選択して、追加のジョブの詳細を表示します。
3. アイコンをクリックして　　、**[ログ収集ステータス]**ページを表示します。**[ログ収集ステータス　]**ページには、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。

Cisco Intersight Cloud へのログのアップロード

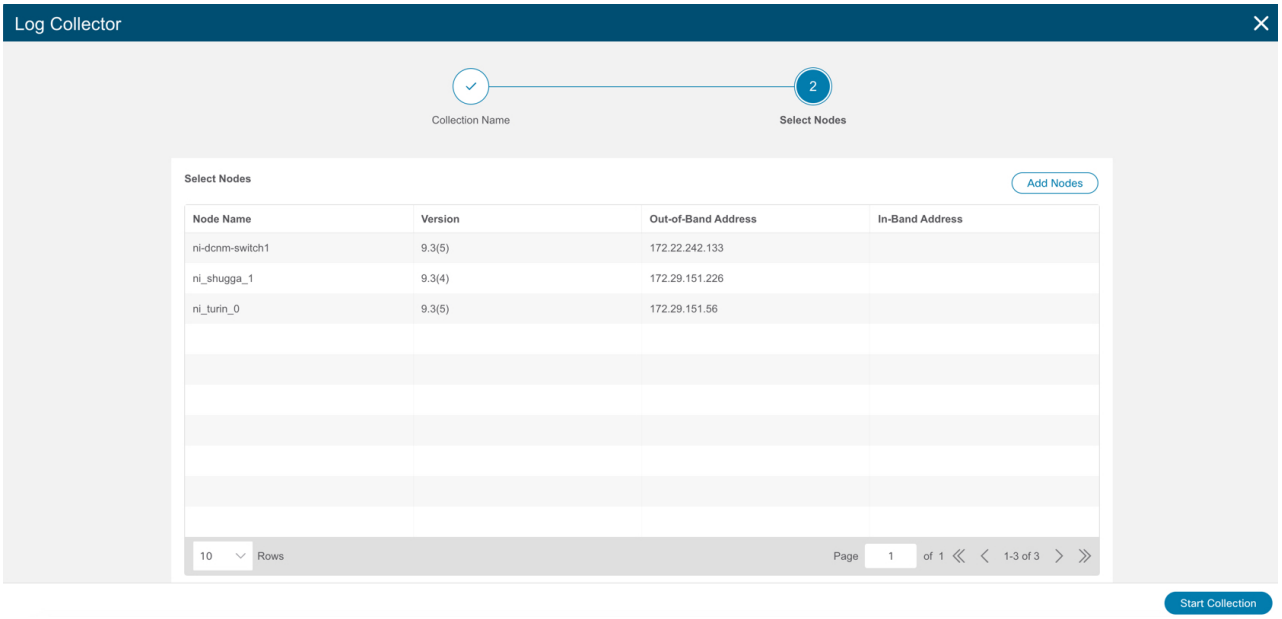
次の手順を使用して、ログをCisco Intersight Cloudにアップロードします。

はじめる前に

- 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。デバイスコネクタについてを参照してください。

手順

1. **[トラブルシュート（Troubleshoot）]** > **[ログコレクタ（Log Collector）]** > **[新しいログ収集（New Log Collection）]** の順に選択します。
2. 名前を入力します。
3. **[サイトの選択（Select Site）]** をクリックしてサイトを選択します。
4. (任意)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]**をオンにします。
5. [次へ（Next）] をクリックします。
6. **[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。
7. [追加（Add）] をクリックします。ノードが**[ノードの選択]**テーブルに表示されます。

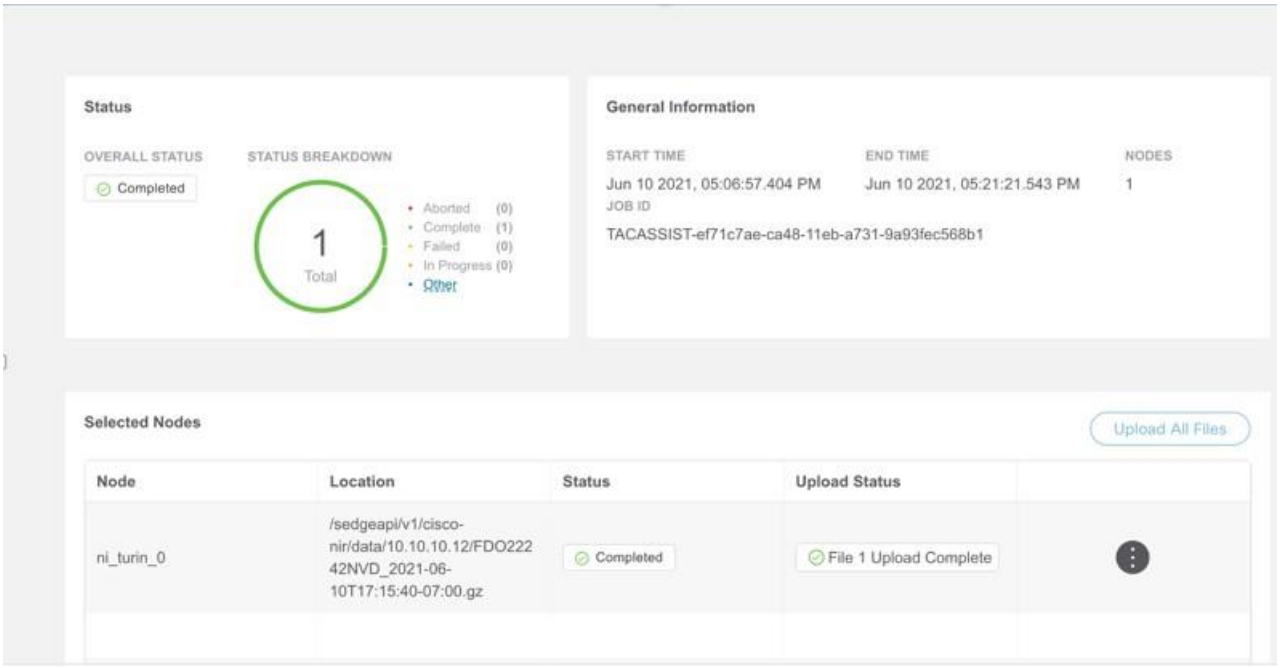


8. **[収集の開始（Start Collection）]** をクリックして、ログ収集プロセスを開始します。

   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。

9. サイドペインの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。
10. アイコンをクリックして、**[ログ収集ステータス]**ページを表示します。
11. ノードを選択し、 アイコンをクリックします。
12. **[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。
13. **[アップロード]**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

- ログ収集は一度に5ノードでのみ実行できます。
- 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] テーブルでは、ステータスは [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]** 表では、ステータスは失敗として表示されます。
- **[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。

参照

Nexus Dashboard Insightsの[参照]セクションには、統計および分析情報の次の領域が含まれています。

- **[リソース]** - 運用、設定、およびハードウェアリソースの使用率、変化のペース、トレンド、およびリソースの異常が経時的に表示されます。
- **[環境]** - ファン、電源、CPU、メモリなど、スイッチの環境リソースが表示されます。
- **[フロー]** - サイト内のさまざまなデバイスから収集されたテレメトリ情報が表示されます。
- **[エンドポイント（Endpoints）]** - サイト全体で収集されたノードのエンドポイントが表示されます。
- **[インターフェイス]** - スイッチノードのインターフェイスの使用状況が表示されます。
- **[プロトコル]** - プロトコル統計情報が表示されます。
- **[イベント]** - 経時的なイベント発生のグラフが表示されます。

リソース

Nexus Dashboard Insightsの[リソース]には、**[ダッシュボード]**タブと**[参照]**タブの作業ウィンドウで使用できるデータ収集の領域が含まれています。

[ダッシュボード] タブ

リソースダッシュボードには、運用、設定、およびハードウェアリソースの使用率、変化のペース、トレンド、およびリソースの異常が経時的に表示されます。上位のリーフノードとスパインノードは、高い使用率を生み出した要因に基づいて表示されます。

プロパティ	説明
使用率別のサイトキャパシティ	サイト内の Cisco APIC オブジェクトの運用キャパシティが表示されます。
使用率別の上位ノード	リソース使用率の異常スコアに基づいて上位ノードが表示されます。

[使用率別の上位ノード（Top Nodes by Utilization）] のノードカードをクリックして、*[リソースの詳細（Resource Details）]* ページを表示します。詳細には、一般情報、リソース使用率プロパティに関するリソースの傾向、およびリソースの異常が含まれます。

[参照]タブ

[参照]タブの**[フィルタ]**フィールドを使用して、統計情報を表示、ソート、およびフィルタ処理します。次のフィルタを使用して、表示された統計情報を絞り込むことができます。

- [ノード] - ノードのみ表示されます。

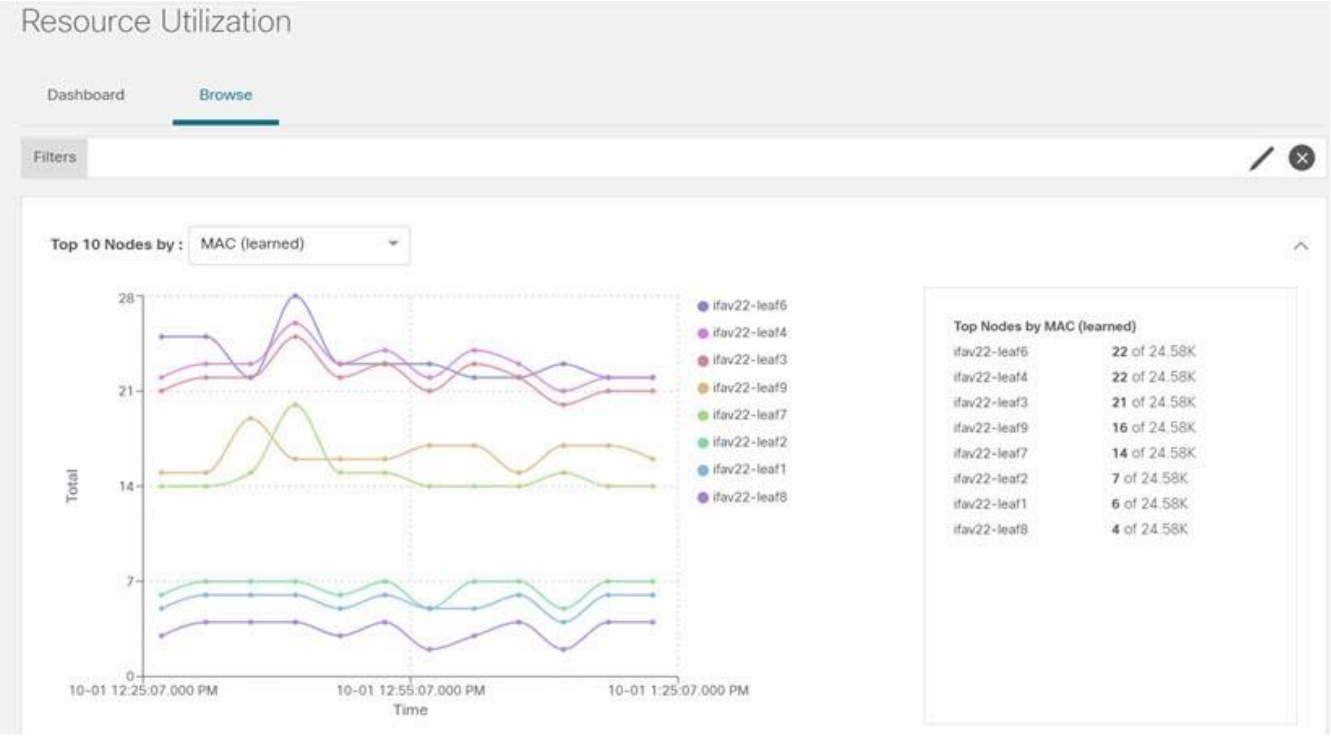
フィルタの絞り込みでは、フィルタ、演算子、および値を選択できます。次の演算子を使用できます。

- == -
  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、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。
- 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。

[フィルタ（Filters）] フィールドに続いて、次の項目が表示されます。

プロパティ	説明
上位ノード	上位ノードを次の基準で表示します。 • MAC(学習済み) • IPv4(学習済み) • IPv6(学習済み) • IPv4 ホストルート • IPv6ホストルート • マルチキャスト ルート • エンドポイント グループ • ブリッジドメイン • VRF • ポートの使用 • 入力ポートの帯域幅 • 出力ポート帯域幅 • LPM • ポリシーTCAM • VLAN

プロパティ	説明
運用リソース	リソース使用率に基づいて運用リソースのリストを表示します。リスト情報には次のものが含まれます。 • 異常スコア • ノード • MAC(学習済み) • IPv4(学習済み) • IPv6(学習済み) • IPv4 ホストルート • IPv6ホストルート • マルチキャスト ルート
設定のリソース	リソース使用率に基づいて構成リソースのリストを表示します。リスト情報には次のものが含まれます。 • 異常スコア • ノード • VRF • BD • EPG • VLAN
ハードウェアリソース	リソース使用率に基づいて構成リソースのリストを表示します。リスト情報には次のものが含まれます。 • 異常スコア • ノード • ポートの使用 • ポート帯域幅 • LPM • ポリシーTCAM



- ノードの追加の詳細を表示するには、サイドペインの概要ペインでノードをクリックします。
- サイドの概要ペインで、右上隅にある　アイコンをクリックして*[リソースの詳細]*ページを開きます。
  ページで設定しなければならない場合があります。
- **[概要（Overview）]** タブをクリックします。

  [概要]タブの[ノードの詳細]ページには、リソース使用率のプロパティに関する一般的な情報、異常スコア、ノードの概要、およびリソースのトレンドが表示されます。
- 選択したノードの詳細ページで、右上のナビゲーションウィンドウにある省略記号（ ）アイコンをクリックして、ノードの[フロー]、[統計情報]、[リソース]、[異常]、[エンドポイント]、[イベント]、[環境リソース]、[ノードの詳細]など、ノードの追加の関連情報を表示します。

  リストのカテゴリをクリックして、その特定のノードの参照作業ウィンドウを開きます。
- [ノードの詳細]ページの**[アラート]**タブには、ノードで発生した異常が表示されます。

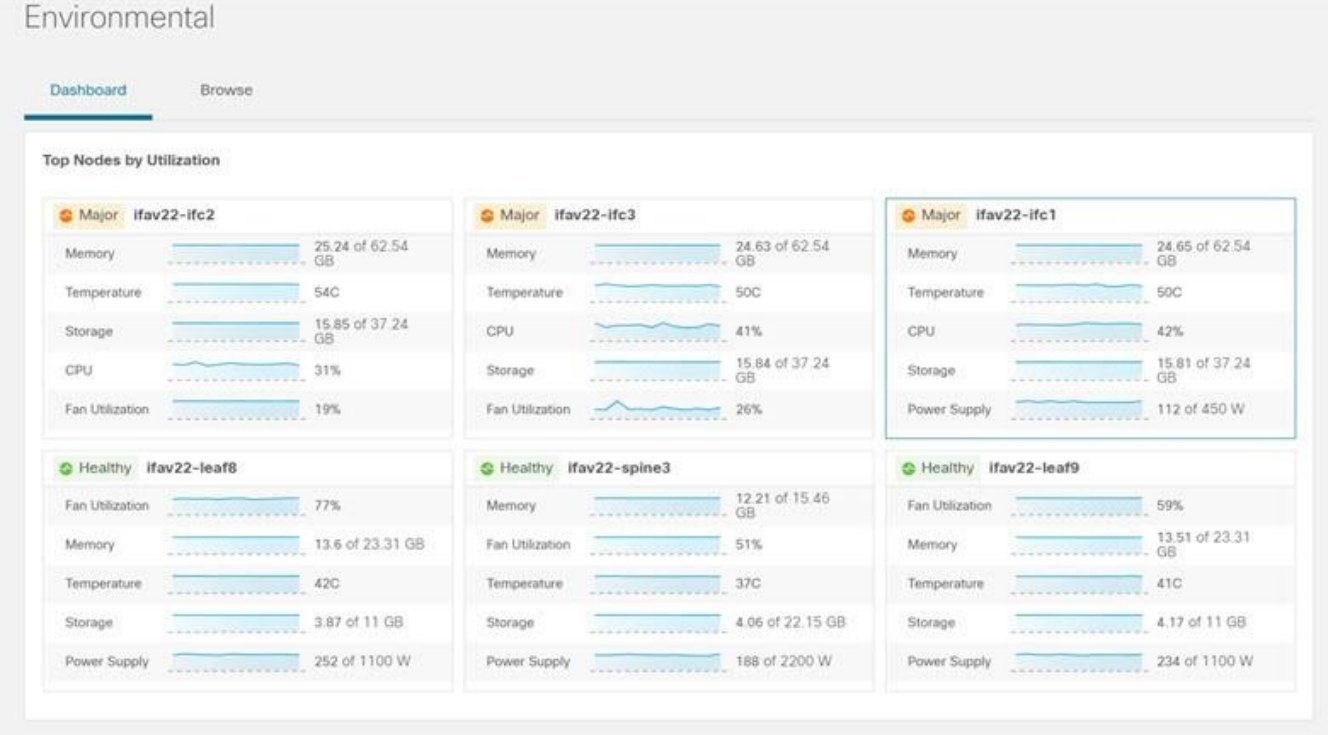
環境

Nexus Dashboard Insightsの**[環境]**には、**[ダッシュボード]**タブと**[参照]**タブの作業ウィンドウで使用できる2つのデータ収集領域が含まれています。

[ダッシュボード] タブ

環境ダッシュボードには、ファン、電源、CPU、メモリなど、スイッチの環境リソースの使用率、変化のペース、トレンド、および異常が経時的に表示されます。

プロパティ	説明
使用率別の上位ノード	コンポーネントごとの使用率が表示されます。 • CPU • メモリー • 温度 • ファン使用率 • 電源 • ストレージ



[使用率別の上位ノード（Top Nodes by Utilization）] のノードカードをクリックして、*[環境の詳細（Environmental Details）]* ページを表示します。詳細には、一般情報、環境プロパティのリソースのトレンド、環境リソースの異常が含まれます。

[参照]タブ

[参照]タブの**[フィルタ]**フィールドを使用して、統計情報を表示、ソート、およびフィルタ処理します。次のフィルタを使用して、表示された統計情報を絞り込むことができます。

- [ノード] - ノードのみ表示されます。

フィルタの絞り込みでは、フィルタ、演算子、および値を選択できます。次の演算子を使用できます。

- == -
  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、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。
- 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。

プロパティ	説明
上位ノード	上位ノードのグラフを次の基準で表示します。 • CPU • メモリー • 温度 • ファン使用率 • 電源 • ストレージ
環境リソースのサマリー	異常スコア別の上位ノードのリストが表示されます。表の列には次のものが含まれます。 • 異常スコア • ノード • CPU • メモリー • 温度 • ファン使用率 • 電源 • ストレージ

- ノードの追加の詳細を表示するには、サイドペインの概要ペインでノードをクリックします。
- サイドの概要ペインで、右上隅にあるアイコンをクリックして、[*環境の詳細*]ページを開きます。
- **[概要（Overview）]** タブをクリックします。

  [概要]タブの[ノードの詳細]ページには、環境リソースプロパティに関する一般的な情報、異常スコア、ノードの概要、およびリソースのトレンドが表示されます。

- 選択したノードの詳細ページで、右上のナビゲーションウィンドウにある省略記号  アイコンをクリックして、ノードの [フロー（Flows）]、[統計情報（Statistics）]、[リソース（Resources）]、[異常（Anomalies）]、[エンドポイント（Endpoints）]、[イベント（Events）]、[環境リソース（Environmental Resources）]、[ノードの詳細（Node Details ）] など、ノードの追加の関連情報を表示します。

  リストのカテゴリをクリックして、その特定のノードの参照作業ウィンドウを開きます。

- [ノードの詳細]ページの**[アラート]**タブには、ノードで発生した異常が表示されます。

インターフェイス

左側のナビゲーションウィンドウで、**[参照]** > **[インターフェイス]**をクリックして、作業ウィンドウに**[インターフェイス]**ページを表示します。

作業ウィンドウの上部には、選択されているサイトグループがあり、2つのタブを表示できます。

- **[ダッシュボード]** タブ
- **[参照]**タブ

[ダッシュボード] タブ

[ダッシュボード]タブには、ノードのインターフェイス使用率に基づいてグラフが表示される**[インターフェイス使用率別の上位ノード]**が表示されます。

このタブには、**[インターフェイス別の上位ノード]**も表示され、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、仮想ポートチャネル(PCおよびvPC)インターフェイス、およびスイッチ仮想インターフェイス（SVI）のノードに関する異常別に上位インターフェイスの詳細が表示されます。

インターフェイス名の横にある緑色のドットは、動作ステータスを表し、インターフェイスがアクティブであることを示しています。インターフェイス名の横にある赤いドットは、インターフェイスが非アクティブであることを示しています。

[参照]タブ

[参照]タブの**[フィルタ]**フィールドを使用して、統計情報を表示、ソート、およびフィルタ処理します。次のフィルタを使用して、表示された統計情報を絞り込むことができます。

- [ノード] - ノードのみ表示されます。
- [インターフェイス] - インターフェイスのみ表示されます。
- [プロトコル] - プロトコルのみ表示されます。
- [インターフェイスタイプ] - プロトコルに基づいてインターフェイスタイプが表示されます。
- [動作状態] - インターフェイスのアクティブ状態が表示されます。
- [管理状態] - インターフェイスの有効化状態が表示されます。

フィルタの絞り込みでは、フィルタ、演算子、および値を選択できます。次の演算子を使用できます。

== -
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、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。

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。

表 8. 監査ログ、イベント、および障害の合計

プロパティ	説明
作成時刻	監査ログ、イベント、または障害インスタンスが発生した日時です。
重大度	イベントの現在の重大度レベル。 レベルは次のとおりです。 • **[クリティカル]** - サービスに影響する状態であり、すぐに修正措置を実行する必要があります。 たとえばこの重大度は、管理対象オブジェクトがアウト オブ サービスであり、機能を回復させる必要があることを示している場合があります。 • **[メジャー]** - 1 つ以上のコンポーネントに重大な問題があります。 これらの問題を調査し、すぐに修正する必要があります。 • **[マイナー]** - システムパフォーマンスに悪影響を及ぼす可能性のある問題が 1 つ以上のコンポーネントにあります。 それらの問題を調査し、クリティカルな問題に発展する前にできるだけ早く修正する必要があります。 • **[警告]** - 解消されなければシステムパフォーマンスに悪影響を及ぼす可能性のある潜在的な問題が 1 つ以上のコンポーネントにあります。 それらの問題を調査し、クリティカルな問題に発展する前にできるだけ早く修正する必要があります。 • **[情報（Info）]**：基本的な通知または情報メッセージで、おそらく 単独では重要ではありません。 • **[クリア]** - 障害の原因となった状態が解決され、障害が解消されたという通知です。
コード	さまざまなタイプの障害インスタンスオブジェクトを分類および識別するのに役立つコードです。
最終移行	重大度が最後に変更された日時。 重大度が変更されたことがない場合、このフィールドには元の作成日が表示されます。
説明	監査ログ、イベント、または障害に関する追加の説明情報。

[参照]タブの作業ウィンドウに、[エラー]、[送信使用率]、[受信使用率]など、さまざまなオプション別の上位インターフェイスが表示されます。

次の項目からオプションを選択した場合：**エラー**、**送信使用率**、**[受信使用率（Transmit Utilization）]**を選択し、３日以上前のスナップショットを選択し、時間範囲が１時間以下の場合、**[参照（Browse）]**タブの**[上位インターフェイス（Top Interfaces）]**エリアにデータは入力されません。

[インターフェイス]テーブルには、[異常スコア]、[インターフェイス]、[インターフェイスタイプ]、[ノード]、[L2ネイバー]、[論理ネイバー]、[受信使用率]、[送信使用率]などの情報が表示されます。

サイドバーの**[インターフェイス]**ページの行をシングルクリックすると、特定のインターフェイスに関する詳細が右側に表示されます。

[インターフェイス]ページの各行をダブルクリックして、インターフェイスに関する詳細情報がある**[インターフェイスの詳細]**ページを表示します。このページには、次のタブがあります。

- **概要**:
- **アラート**:
- **プロトコル**:
- **ネイバー**:

[概要]タブの**[一般的な情報]**領域に、インターフェイスに関する一般的な情報が表示されます。**[トレンド]**領域には、インターフェイスを流れるトラフィックと使用状況に関する情報が表示されます。**[統計情報]**領域では、QoS、DOM、およびマイクロバーストのさまざまな統計情報を確認できます。

このページの**[アラート]**タブに、異常が表示されます。

インターフェイスでプロトコルが有効になっている場合、**[プロトコル]**タブに詳細が表示されます。**[ネイバー]**タブには、2種類のネイバーがあります。

- [L2ネイバー]：
  この領域には、[名前]、[ピアインターフェイス名]、[ピアデバイスタイプ]、[プラットフォーム情報]、[ピア管理IP]、[ピアノードID]などの詳細が表示されます。
- [論理ネイバー]：
  この領域には、[ピアIP]、[動作状態]、[プロトコル名]、[VRF名]、[ネイバータイプ]などの詳細が表示されます。

ネイバーの詳細を表示するには、インターフェイスがアクティブになっている必要があります。

サポートされるインターフェイス タイプ

[物理インターフェイス]：**[物理]**タイプをダブルクリックして、ノード名、物理インターフェイス名、動作ステータス、

管理状態など、ノードのインターフェイスの詳細を表示します。このページには、物理インターフェイスのプロトコル、QoS、およびDOMプロパティも表示されます。

[ポートチャネルインターフェイス]：ポートチャネルは物理インターフェイスの集合体であり、統計的にチャネル化したり、LACPプロトコルを使用して動的にしたりできます。パケット、バイト、およびさまざまなエラーのカウンタを収集する統計データは、物理インターフェイスの統計データと同様です。*送信元名*で、物理インターフェイスをポートチャネル(集約インターフェイス)と区別します。運用データは、管理ステータス、運用ステータス、およびPCとvPCの両方のメンバーインターフェイスのリストを提供する追加のオブジェクトセットを調べることによって取得されます。

[vPCインターフェイス]：vPCは、耐障害性のために2つの物理スイッチにまたがる論理インターフェイスです。**[インターフェイス]**ページの各行をダブルクリックして、ノード名、仮想ポートチャネル名、ドメインID、動作ステータス、および管理状態が要約されている**[インターフェイスの詳細]**ページを表示します。このページには、仮想ポートチャネル内のノードに関連付けられている異常、トラフィック、およびメンバーインターフェイスも表示されます。vPCインターフェイスタイプの場合、**論理ネイバー**情報も表示されます。サポートされているカテゴリは、L3Out、IPN、ISN、L4-L7 です。

SVIインターフェイス：SVIは、仮想ルーテッドインターフェイスであり、デバイスのVLANを同じデバイスのレイヤ3ルータエンジンに接続します。SVIが展開されているメンバーインターフェイス、VLAN ID、VLANタイプ、カプセル化VLANなど、SVIインターフェイスの特定の情報が表示されます。

インターフェイスの制約事項

- インターフェイス統計は、eqptIngrCrcErrPkts5min カウンタをサポートしていません。
- ポートチャネル インターフェイスのインターフェイス統計の異常は生成されません。

インターフェイス統計のマイクロバーストサポート

チャネルがすでにラインレートフローで登録されている場合、トラフィックのバーストは物理インターフェイスポートの出力バッファに影響します。

バッファ使用量のバリアンスが大きいため、トラフィックのバーストは、使用されているバッファセルや未使用のバッファセルなど、指定されたキューイングパラメータだけでは検出が難しいことがよくあります。

Cisco Nexus 9000 シリーズスイッチは、キューの占有率が*x*バイト上回った場合、および*y*バイトを下回った場合にトリガーされる割り込みを発行することによって、バーストを検出する機能を提供します。この*x_&_y*バイトは、インターフェイスごとにキュー単位で設定できます。物理インターフェイスポートごとに最大8つの出力キューを設定できます。

UTRソフトウェアコレクタがパスshow queuing burst-detect detailのGRPCテレメトリストリームを受信すると、エンコードパスのパーサーに従って、データがフォーマットされ、Kafkaのテレメトリ出力トピックに書き込まれます。

マイクロバーストの設定と監視

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. **[概要（Overview）]**
   ページで適切なサイトグループを選択し、[アクション（Actions）] メニュー > **[サイトグループの構成（Configure Site Group）]** の順に選択します。
2. **[サイトグループの構成（Configure Site Group）]** ページの **[マイクロバースト構成（Microburst Configuration）]** エリアで、適切なサイト名に対して、**[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。他の値は、**[高感度設定（Set High Sensitivity）]** と **[低感度設定（Set Low Sensitivity）]** です。

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。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を超えると、異常が発生します。Nexus Dashboard Insightsは、選択したサイト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。

詳細については、マイクロバーストの監視も参照してください。

サポートされるプラットフォーム

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。

マイクロバースト異常

インターフェイスレベルでのマイクロバーストの数に基づいて、Nexus Dashboard Insightsで異常が発生します。マイクロバースト異常ジョブは、コンテナ環境で5分ごとに実行され、マイクロバースト
データベース内のマイクロバーストレコードがチェックされます。インターフェイスごとのマイクロバーストの数が任意の時点でマイクロバースト数のしきい値よりも大きい場合、ノードのインターフェイスごとにマイナーな異常が発生します。その時点で、異常レコードがElasticsearchに書き込まれます。

Nexus Dashboard Insightsは、それらの異常を**[参照]** > **[インターフェイス]**ページに表示します。

1. 概要テーブルに表示されるフローは、対応する出力インターフェイスのフローテレメトリデータから収集されます。Nexus Dashboard Insightsは、出力インターフェイスと出力キューを照合して、対応するマイクロバーストを収集します。
2. 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に分類されます。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を超えると、異常が発生します。

3. フローテレメトリが有効になっていて、マイクロバーストも有効になっている場合、Nexus Dashboard Insights は、特定のマイクロバースト異常に対するフローの推定される影響を表示します。
4. フローテレメトリが無効になっていて、マイクロバースト異常が有効になっている場合、Nexus Dashboard Insights は、その異常に対する**推定される影響**は表示しません。
5. マイクロバーストに寄与しているフローまたは影響を受けるフロー。

「マイクロバースト異常」を参照

マイクロバースト異常を参照するには、フローテレメトリが有効になっていて、フロールールがサイトで設定されていることを確認してください。フロールールが設定されている場合、フローは概要テーブルで使用できます。

[インターフェイスの概要]ペインで、次の手順を実行します。

1. 異常をクリックして、追加の詳細を含むサイドペインを表示します。
2. **[Analyze（分析）]** をクリックします。
3. [詳細ビュー]ページには、影響を受けるフロー、相互発生、存続期間、および推奨事項の要約されています。

> Nexus Dashboard Insightsリリース6.0以降、「*識別されたX フローは、大きな最大バースト値を持つ上位 X であり、それらのフローによるバッファ使用率*が高いことを示している可能性があります」という内容は[推奨事項]領域には表示されません。

   a. サイドペインで**[影響を受けるオブジェクト]**をクリックして、ノードの*[インターフェイスの詳細]*を表示します。このページには、インターフェイスの詳細、バースト数、タイムスタンプ、集約されたフローの詳細、およびピーク値による上位 25 のマイクロバースト。

   b. **[レポートの表示]**をクリックして、マイクロバーストに寄与している、またはマイクロバースの影響を受けた上位100のフローを表示します。

   c. *[影響を受けるエンティティ（Affected Entities）]*サイド表示ペインで、フローを選択し、クリックして[フローの詳細]ページを表示します。

プロトコル

Nexus Dashboard Insights の [参照（Browse）] セクションには、タイプが CDP、LLDP、LACP、BGP、PIM、IGMP、および IGMP スヌーププロトコルであるノードの異常ごとに上位インターフェイスのプロトコル情報が表示されます。このページには、ノード名と、プロトコルが使用しているインターフェイスの数、またはプロトコルがノードに使用しているセッションの数である*[カウント]*も表示されます。

BGPプロトコルデータは、運用データと統計データに大別できます。運用データは、管理ステータス、*運用ステータス*、VRFのリスト、*vrfName*、*vrfOperState*、*vrfRouteId*などのVRFレベル情報、各VRFに関連付けられたアドレスファミリのリスト、ピアおよび各VRFに関連付けられたピアエントリ情報のリストを提供する追加のオブジェクトセットで構成されます。統計データは、オープン数、更新数、キープアライブ数、ルートリフレッシュ、機能、メッセージ、通知、送受信バイト数などのピアエントリカウンタで構成されます。また、ピアエントリアドレス ファミリ レベルのルートカウントも含まれます。

- サイドバーの **[プロトコル（Protocols）]** ページの行をクリックして、特定のノードに関する追加の詳細を表示します。
- ノード名、プロトコル名、管理状態、動作状態、および追加の詳細など、ノードのプロトコルの詳細については、プロトコル**BGP**の行をダブルクリックします。このページには、異常、アクティブなネイバーノード、ノードのエラー、ネイバーIPアドレス、ノードファミリからBGPプロトコルを使用している確立されたネイバーおよび接続されていないネイバーに関する詳細も表示されます。
- インターフェイス、管理状態、動作状態、送信済みパケット、受信済みパケット、ネイバー、エラーなど、ノードのプロトコルの詳細を表示する場合は、プロトコル**[CDP]**、**[LLDP]**、または **[LACP]** の行をダブルクリックします。

マルチキャストプロトコル

[統計の参照（Browse Statistics）] ダッシュボードには、PIM、IGMP、および IGMP スヌーププロトコルタイプのノードの異常別に上位インターフェイスのプロトコルが表示されます。

プロトコル独立マルチキャスト

プロトコルタイプ**[PIM]**をダブルクリックして、PIMに関する特定のノードの概要を表示します。

[一般情報（General Information）] セクションには、異常スコア、プロトコル、ドメインの数、インターフェイス、およびプロトコルのノード名が表示されます。

[異常（Anomalies）]

セクションには、PIMに固有のノードで生成された異常が表示されます。**[トレンド（Trends）]**

セクションには、特定のノードのPIMに関連するエラーとエラーの内訳が表示されます。

[マルチキャストPIMドメイン]セクションには、ノードに固有のPIMに関するドメインの詳細が表示されます。テナント、VRF、管理状態、ランデブーポイントアドレスなどの基本情報が表示されます。

- サイドペインの行をダブルクリックして、特定のマルチキャストPIMドメインに関する追加の詳細を表示します。詳細には、VNI ID、有効になっているフラグ、さまざまなエラー、および統計情報が含まれます。

[マルチキャストPIMインターフェイス（Multicast PIM Interfaces）]セクションには、PIMで有効になっているインターフェイスが表示されます。また、インターフェイス名、テナント名、IPアドレス、指定ルータアドレス、ネイバーアドレス、エラーが表示されます。

- サイドペインの行をダブルクリックして、ネイバー固有の詳細を表示します。詳細には、統計情報、ネイバーで有効になっているフラグ、およびノードに固有のエラーが含まれます。

[マルチキャストPIMグループ（Multicast PIM Groups）]セクションには、送信元、グループアドレス、テナント、VRF、着信インターフェイス、RPF ネイバー、発信インターフェイス、フラグ、および PIM グループのステータスなど、PIMグループに関連する詳細が表示されます。PIMグループにデータが流れていない場合、ステータスは非アクティブです。

インターネットグループ管理プロトコル

[統計の参照]ページでフィルタを使用して、IGMPに関する特定のノードの概要を表示します。**[一般情報（General Information）]**セクションには、異常スコア、プロトコル、インターフェイスの数、ノードの数、およびプロトコルが属するノード名が表示されます。

[異常]セクションには、IGMPに固有のノードで生成された異常が表示されます。固有のノードについては、IGMPに関連するエラーは表示されません。

[設定済みIGMPインターフェイス]セクションには、IGMPが有効になっているインターフェイスが表示されます。また、インターフェイス名、テナント名、VRF、メンバーシップ数、バージョン、エラーが表示されます。

- サイドペインの行をダブルクリックして、追加の詳細を表示します。詳細には、VRF ID、エラーカウンタに関する統計データ、IGMPで有効になっているフラグ、およびノードに固有の受信パケットが含まれます。

[マルチキャストグループ（Multicast Groups）]セクションには、送信元、マルチキャストグループ、テナント、VRF名、最後のレポータ、IGMP グループに固有の発信インターフェイスなど、IGMPグループに関連する詳細が表示されます。

Internet Group Management Protocol スヌープ

[統計の参照]ページでフィルタを使用して、IGMPスヌープに関する特定のノードの概要を表示します。**[一 般 情 報 （ General Information ）]** セクションには、異常スコア、プロトコル、ノード名、グループの数、およびインスタンスで IGMP スヌープが有効になっているインスタンスの数が表示されます。

[異常]セクションには、IGMPスヌープインスタンスに固有のノードに存在する異常が表示されます。

[トレンド]セクションには、特定のノードのIGMPスヌープに関連するインスタンス数とエラーの内訳が表示されます。インスタンス数は任意のブリッジドメイン数であり、一部は IGMP スヌープが有効になっており、一部は IGMP スヌープが無効になっています。**Up** はインスタンス数を表します IGMP スヌープが有効になっています。**[ダウン]**は、IGMPスヌープが無効になっているインスタンスの数を表します。

[IGMP スヌープインスタンス（ IGMP Snoop Instances ）] セクションには、テナント、VRF、BD、管理状態、クエリアアドレス、クエリアバージョン、ルーティング状態（有効または無効）、サイトクエリア状態（有効または無効）、エラーの概要など、ブリッジドメインに関する情報が表示されます。

- サイドペインの行をダブルクリックして、IGMPスヌープインスタンスに固有のその他の設定済みの詳細を表示します。詳細には、統計の詳細と、IGMP スヌープインスタンスに固有のさまざまなエラーカウンタが含まれます。

[マルチキャストグループ（ Multicast Group ）] セクションには、各 IGMP スヌープグループの送信元、マルチキャストグループ、テナント、VRF 名、BD、EPG、バージョン、最後のレポータ、および発信インターフェイスなどの詳細が表示されます。

プロトコル統計の異常検出

プロトコル統計カウンタは、異常検出のために監視されます。各異常の発生方法については、以下に説明するスキームに基づいています。異常は、ノード内の送信元(インターフェイスなど)に固有のカウンタで発生します。異常検出アルゴリズムは、監視されているカウンタのすべてのインスタンスについて指数加重移動平均(EWMA)を計算することによって機能します。EWMA は定期的に更新され、更新は既存の EWMA に対する 90% の重み + カウンタの新しい着信値に対する 10% の重みに基づいて実行されます。更新の周期は1分です。最初の30期間では、データが収集され、EWMAが安定するようになります。この間、異常は発生しません。安定期間はサービスの開始時点であり、その時点ですべてのカウンタのEWMA計算が開始されます。さらに、ファブリックの動作中に新しいノードがアクティブになった場合、そのノードのカウンタはEWMAを構築するために安定期間を経ます。その新しいノードのカウンタのEWMA計算も30期間で行われます。EWMAは、異常を検出するために着信値と比較されます。

プロトコル統計カウンタでは、2種類の異常が処理されます。

しきい値ベースの異常。InterfaceUtilizationIngressやInterfaceUtilizationEgress などの使用率カウンタは、インターフェイスの使用率について監視されます。最大使用率しきい値が定義されています。使用率がクリティカルしきい値を超えると、しきい値異常が発生します。使用率がしきい値を下回ると、異常は解消されます。変更された検出の異常は、EWMA に基づいています。すべてのカウンタの EWMA は、statsdbに新しい値をクエリすることにより、予測サービスによって毎分継続的に更新されます。変更検出の異常は、次のカウンタに適用されます。

[変化率異常（Rate-of-Change Anomaly）]：連続した 3 回の検出期間（データは 1 分ごとに更新されるため、3 分）で帯域幅の使用量に10%を超える増減がある場合、使用率の変化率異常が発生します。変化率が10%を下回ると、異常は解消されます。エラーカウンタの異常検出は、プロトコルカウンタのエラー検出にフラグを立てるために使用されます。監視されるエラーカウンタのリストを次の表に示します。エラー カウンタは、予測サービスによってモニタされます。エラーカウンタが連続した 3 回の検出期間で 1 以上増加すると、対応するエラー異常が発生します。エラーが 5 期間存在する場合、Warning（警告） の異常が発生します。異常が 30 期間続く場合は、major（重大）な異常に変わります。1 期間は、実時間の 1 分を指します。

表 9. 監視されるエラーカウンタ

プロトコルカウンタ	異常検出方法	しきい値	重大度	異常の種類
InterfaceUtilizationIngress InterfaceUtilizationEgress	使用率が指定されたしきい値を超えているかどうかを監視します。	> 90%	クリティカル（Critical）	high_threshold
InterfaceUtilizationIngress InterfaceUtilizationEgress	新しい値が EWMA より 10% 以上大きいか小さいかを監視します。	の率 変化 > 10%	警告	high_rate_of_change

プロトコルカウンタ	異常検出方法	しきい値	重大度	異常の種類
プロトコルエラー。エラーを監視する具体的なプロトコルカウンタは次のとおりです。 -interfaceForwardingDropIngress -interfaceAfdDropEgress -interfaceBufferDropIngress -interfaceBufferDropEgress -interfaceErrorDropIngress -interfaceErrorDropEgress -interfaceCrc -interfaceIngressError -interfaceEgressError -interfaceIngressDiscard -interfaceEgressDiscard -lldpFlaps -lacpFlaps	過去5分間にカウンタ値が増加したかどうかを監視します。	エラー増加 > 0	メジャー	エラー
interfaceStomped	カウンタ値が増加しているかどうか、およびこのポートのネイバーノードで interfaceSto カウンタが増加していないか監視します。	エラー増加 > 0	メジャー	エラー

ルーティングプロトコルの受信パスの異常検出

Nexus Dashboard Insightsは、受信したBGPピアプレフィックス数の変化を監視し、過去5分間のバリアンスの割合を計算します。バリアンスの割合が10%を超える場合、Nexus Dashboard Insightsは異常を生成し、異常の種類は**hige_rate_of_change**です。

フロー

フローは、フローレベルでの深い洞察を提供し、平均遅延、パケットドロップインジケータ、フロー移動インジケータなどの詳細を提供します。また、フローの遅延が増加した場合、あるいは輻輳や転送エラーのためにパケットがドロップされた場合に異常が発生します。

各フローには、一定期間にそのフローのASICに入るパケット数を表すパケットカウンタがあります。この期間は、集約間隔と呼ばれます。特定のフローのフロー統計を集約できるポイントがいくつかあります。集約は、ASIC、スイッチソフトウェア、およびサーバーソフトウェアで発生する可能性があります。

Nexus Dashboard Insightsの[フロー（Flows）]セクションには、サイトに追加されたサイト内のさまざまなデバイスから収集されたテレメトリ情報が表示されます。

Cisco Nexusシリーズスイッチおよびラインカードのフローテレメトリサポートの詳細については、「Nexus Dashboard Insights リリースノート」の**互換性に関する情報**セクションを参照してください。

Nexus Dashboard Insightsの[フロー]には、**[ダッシュボード]**タブと**[参照]**タブの作業ウィンドウで使用できる2つのデータ収集領域が含まれています。

フローのガイドラインと制約事項

- Nexus Dashboard Insightsは、ユーザーが指定した時間範囲のサイクル全体について、特定のフローの最大異常スコアをキャプチャします。
- 不明な IPアドレスの場合、スパインノードからのトラフィックはドロップされ、フローレコードはフローテレメトリで生成されません。
- パケット数は、送信元および接続先 IPアドレスと一致しない特定のフローのサイトに入るパケットの数を表します。
- フローテレメトリノードでは、最大63のVRFがサポートされます。
- フローは、エンドポイント セキュリティ グループではサポートされていません。
- ブリッジ フローがスパイン スイッチからレポートされるように、ブリッジ ドメイン サブネットをプログラムする必要があります。

- フローの場合、選択した時間範囲が 6
  時間を超える場合、データが表示されないことがあります。6
  時間以下の時間範囲を選択します。

Cisco Nexus EX スイッチのフローの制限。

フローテレメトリのハードウェアサポートの詳細については、 Nexus ダッシュボードインサイト リリース ノートを産所湯してください互換性情報セクション。

- N9K-C93180YC-EX、N9K-C93108TC-EX、N9K-C93180LC-EX、およびN9K-X9732C-EXラインカードからの発信トラフィックの出力ポート情報は表示されません。
- N9K-C93180YC-EX、N9K-C93108TC-EX、N9K-C93180LC-EX、N9K-X9732C-EX ラインカードのバースト情報は、表示されません。
- EPG名は、フローキャプチャの数分後、かつフローを有効にした後に反映されます。この情報は、EX ASICからではなく、ソフトウェアから取得されます。
- L3Out外部EPGの場合、EPG名、バッファドロップ異常、転送ドロップ異常、およびQoSポリシングドロップ異常はサポートされていません。
- Cisco Nexus 9300-EXプラットフォームスイッチは、VRFベースのフィルタリングをサポートしていません。フローテレメトリルールのブリッジドメインまたはサブネットフィルタリングのみをサポートしています。サブネットが複数のVRFにまたがっている場合、Nexus Dashboard Insightsはサブネットからフローを取得します。
- Tier-1リーフスイッチは、リモートリーフスイッチからサブリーフスイッチにフローテレメトリデータをエクスポートしません。

Cisco Nexus FX スイッチのフローの制限。

- スパインスイッチは、共有サービスフローレコードをエクスポートしません(VRFAからVRFB、およびその逆)。この制限により、Nexus Dashboard Insightsのフローパスのサマリーは不完全になります。
- Nexus Dashboard Insightsはすべてのipサイズをサポートしていますが、実際のipサイズとは異なります。たとえば、1000バイトのipパケットサイズの場合:
  - IPv4 インターリーフ ノード トラフィック（スパインノードあり）の場合、Nexus Dashboard Insights には、1050 バイトの入力 IP サイズと 1108 バイトの出力 IP サイズが表示されます。IPv4イントラリーフトラフィックの場合、Nexus Dashboard Insightsには、入力と出力の両方のipサイズが1050バイトと表示されます。
  - IPv6 インターリーフ ノード トラフィック(スパインノードあり)の場合、Nexus Dashboard Insights には、1070 バイトの入力 IP サイズと 1128 バイトの出力 IP サイズが表示されます。IPv4イントラリーフトラフィックの場合、Nexus Dashboard Insightsには、入力と出力の両方のipサイズが1070バイトと表示されます。
- スイッチに出力 ACL ドロップがある場合、フローテレメトリおよびフローテレメトリイベントはドロップビット

をエクスポートしません。

- 共有サービスを使用する同じノード内のローカルでスイッチングされたトラフィックには、宛先VRFまたはテナントとEPGに関する情報はありません。
  - これは、EPGとExtEPGの両方に有効です。
  - 共有サービスには、VRFが同じでテナントが異なるEPGの場合も含まれます。

Nexus ダッシュボード インサイトでの Cisco ACI Tier-3 トポロジへのフローの拡張

フローは、リーフノードの2番目の階層がリーフノードの最初の階層に接続される3層トポロジを実装します。3 層トポロジでは、フローパケットが複数の階層を使用して 1 つのホストから別のホストにトラバースする場合、接続先ホストに到達する前に Tier-1 リーフノードをトラバースしたパケットは iVXLAN パケットになります。

注意事項と制約事項

- Cisco APIC リリース4.2(4o)は、iVXLAN パケットの場合にフローテレメトリをエクスポートするリーフノードをサポートしていないため、フローパスが不完全になり、すべてのフローを結合するための情報が不足します。

フローダッシュボード

フローダッシュボードには、サイト内のさまざまなデバイスから収集されたテレメトリ情報が表示されます。フローレコードを使用することで、ユーザーはサイト内のフローと、Cisco ACI サイト全体におけるフローの特性を可視化できます。

プロパティ	説明
上位ノード	フローエンジンは、フローの動作に対して機械学習アルゴリズムも実行し、平均遅延、パケット ドロップ インジケータ、フロー移動インジケータなどにおける動作の異常を発生させます。グラフは一定期間における動作の異常数を表します。
フロー異常別の上位ノード	フローテレメトリと分析により、データプレーンの詳細な可視性が得られます。フローは、ノードからストリーミングされたフローレコードを収集し、理解可能な EPG ベースのフローレコードに変換します。[フロー異常別の上位ノード]には、ネットワーク内で異常が最も多いノードが表示されます。

[フ ロ ー 異 常 別 の 上 位 ノ ー

ド]のノードカードをクリックして、[フローレコード]ページを表示します。

フローレコードの詳細

[フロー異常別の上位ノード]のノードカードをクリックして、フローレコードの詳細を表示します。詳細には、異常スコア、レコード時間、フロータイプ、集約されたフロー情報、異常の概要、パスの概要、およびフロープロパティのチャートが含まれます。

[概要]タブの*[集約されたフロー]*セクションには、送信元、宛先、入力、および出力の詳細を含むフロー異常の詳細な分析が表示されます。

*[パスの概要]*セクションには、異常があるノードの送信元IPアドレスと宛先IPアドレスが表示されます。

[アラート]タブの*[異常]*セクションには、異常検出の詳細が要約されています。

[トレンド]タブの*[関連の詳細]*セクションには、時間に対する各フロープロパティの比較チャートを含む異常分析が表示されます。

フローレコードの参照

[フローレコードの参照（Browse Flows Records）] ページには、異常スコア、パケットドロップ
インジケータ、平均遅延、およびフロー移動インジケータごとにサイトフローが表示されます。グラフには、サイト全体で記録されたフロープロパティの時系列プロットが表示されます。上位の送信元と上位の宛先について記録されたノードフローも表示されます。

プロパティ	説明
フィルタ	次のフィルタを使用して、ノードフローの観察結果を表示します。 • レコード時間 • ノード • フロー タイプ • プロトコル • 送信元アドレス • 送信元ポート • 宛先アドレス • 宛先ポート • 入力ノード • 入力テナント • 入力EPG • 出力ノード • 出力テナント • 出力EPG

プロパティ	説明
次の基準別サイトフロー	選択した時間間隔にサイト全体で記録された、異常スコア、平均遅延、パケットドロップ インジケータ、フロー移動インジケータなどのフロープロパティの時系列プロット。**上位の送信元**と**上位の宛先**について記録されたノードフローも表示されます。 • **異常スコア** - スコアは、データベースに記録された検出済みの異常の数に基づいています。 • **パケットドロップインジケータ** - フローレコードのドロップが分析されます。ドロップを検出する主な方法は、スイッチから受信したドロップビット(フローレコード)に基づいています。 • **遅延** - パケットがサイト内の送信元から宛先までトラバースするのにかかる時間。サイト遅延測定の前提条件は、すべてのノードが一定の時間で同期されることです。 • **フロー移動インジケータ** - フローがリーフノード間を移動する回数。エンドポイントによって送信される最初のARP/RARPまたは通常のパケットは、新しいリーフノードを介してサイトに入るフローとして表示されます。

詳細については、フローをダブルクリックしてください。**[フローの詳細]**ページには、フローの一般的な情報、異常、パスの概要、チャート、および関連する詳細が表示されます。

L4-L7 トラフィックパスの可視性

Nexus Dashboard Insightsリリース6.1.1以降、フローパスの可視性をファイアウォールなどのL4-L7外部デバイスに拡張できるようになりました。Nexus Dashboard Insightsは、サービスチェーン全体のエンドツーエンドフローをリアルタイムで追跡し、デバイスサイロ全体のデータプレーンの問題を特定するのに役立ちます。現在のリリースでは、すべてのサードパーティベンダーの非NAT環境がサポートされています。

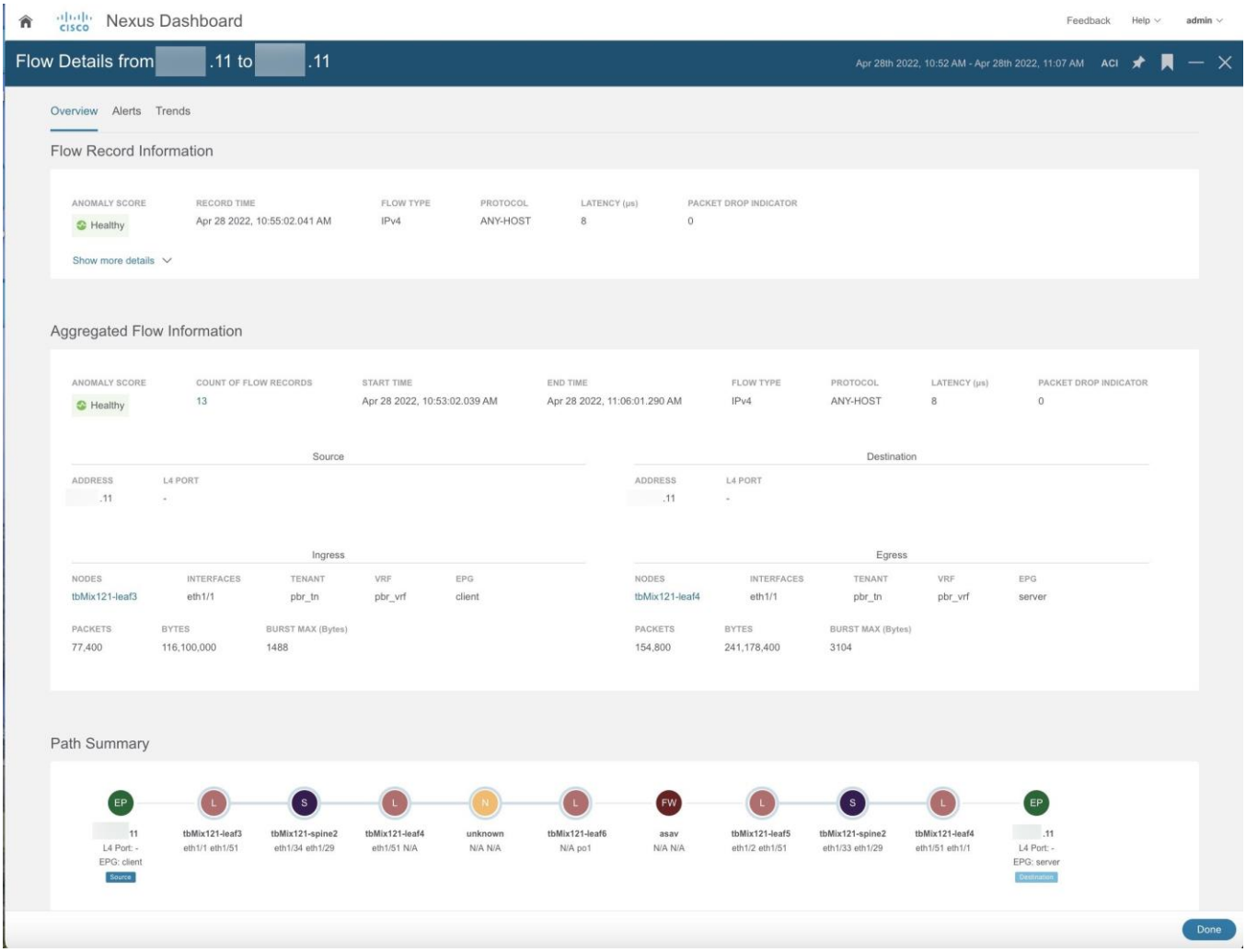
L4-L7トラフィックパスを可視化するには、フローテレメトリを有効にし、適切なルールを

設定する必要があります。設定の詳細については、フローテレメトリを参照してください。ルールに基づいて、フローがポリシーベースのリダイレクト(ファイアウォールなど)を通過している場合、フローパスにその情報が表示されます。

GUIでトラフィックパスの可視性を表示するには、**[フロー]**ページに移動し、**[参照]**タブの下にあるグラフに続くテーブルの**[ノード]**列で、適切なノードをクリックします。概要ペインが表示されます。概要ペインの右上隅にある[詳細]アイコンをクリックして、**[フローの詳細]**ページを開きます。このページを下にスクロールして、**[パスの概要]**グラフを表示します。

送信もとから接続先から**[パスサマリ（Path Summary）]**エリアでグラフィカルなフロー パスにエンドツーエンドの情報が表示され、。

ファイアウォールが存在する場合は、パス内のファイアウォールも特定されます。このグラフでは、発生しているエンドツーエンドのフローパスネットワークの遅延もキャプチャされます。**[フローの詳細（Flow Details）]**ページの次の例を参照してください。ファイアウォールであるポリシーベースのリダイレクトを通過する **[パスの概要（Path Summary）]** が表示されています。



グラフでは、異常がある場合、リーフスイッチまたはスパインスイッチの記号の横に赤いドットが表示されます。**[フローの詳細]**ページの**[アラート]**タブをクリックして、異常に関連する詳細を表示します。

現在のリリースでは、ファイアウォールは異常に対してサポートされていません。

L4〜L7 トラフィックパスの可視性に関する注意事項と制限事項

- この機能は現在、ACI のサービスグラフを使用してポリシーベースのリダイレクトを設定できる場合にのみ推奨されています。
- 現在のリリースでは、ファイアウォールは異常に対してサポートされていません。
- 現在のリリースでは、表示されている遅延情報はネットワーク遅延であり、ファイアウォールで発生している遅延はキャプチャされません。
- 現在のリリースでは、NATはサポートされていません。
- この機能は現在、次のスイッチを使用する場合にサポートされています。
  - Cisco Nexus 9300-FXプラットフォームスイッチ
  - Cisco Nexus 9300-FX2プラットフォームスイッチ
  - Cisco Nexus 9300-GXプラットフォームスイッチ
- L3Outでのポリシーベースのリダイレクトの宛先はサポートされていません。そのような設定では内部VRFが使用されるため、部分的なフローパスのみ使用できるためです。
- ACI ファブリックでは、L4-L7 トラフィックがレイヤー2（ブリッジモード）で転送されている場合、フロー分析のサポートは制限されます。イングレスノードとエグレスノードの検出は正確ではなく、パスサマリーは利用できません。
- L4-L7のサービスグラフがない場合、クライアント > サービスノードがVRF_Aであり、サービスノード > サーバーがVRF_Bである場合、フローをステッチする共通または単一のコントラクトがないため、パスは個別のフローとして記録されます。
- ロードバランサはサポートされていません。

フローテレメトリイベント

フローテレメトリが有効になっている場合、フローテレメトリイベントは暗黙的に有効になります。フローテレメトリにより、設定されたルールが満たされたときにイベントをトリガーでき、パケットが分析のためにコレクタにエクスポートされます。

フローテレメトリイベントは、Nexus Dashboard Insightsの現在のフローを強化および補完します。また、フローテレメトリおよびフローテレメトリイベントの異常生成を強化します。

セキュリティ、パフォーマンス、トラブルシューティングを監視します。これは、毎秒エクスポートされる定期的なフロー テーブル イベント レコードを使用して実現されます。

Insightsへのデータのエクスポートは、データを処理するために必要なコントロールプレーンなしでハードウェアから直接実行されます。統計は、設定可能なMTUサイズと定義されたヘッダーを持つパケットとして集められます。それらのパケットは、Cisco ACIファブリックからインバンドトラフィックとして送信されます。ヘッダーはソフトウェアによって設定され、ストリーミングされるパケットはUDPパケットです。

トリガーされたフローテレメトリイベントでフローテレメトリを使用できる場合は、[フローの詳細（Flow Details）]
ページに移動して集約された情報を確認できます。それらのイベントは、次のドロップイベントに基づいています。

- **バッファドロップ** - スイッチがフレームを受信し、入力または出力インターフェイスで使用できるバッファクレジットがない場合、フレームはバッファでドロップされます。これは通常、ネットワークで輻輳が発生していることを示唆しています。障害を示すリンクがいっぱいか、宛先を含むリンクが輻輳している可能性があります。この場合、フローテレメトリイベントでバッファドロップが報告されます。
- **転送ドロップ** - Cisco ASICのLookUp (LU)ブロックでドロップされるパケットです。LUブロックでは、パケット転送の判断はパケットヘッダー情報に基づいて行われます。パケットがドロップされた場合、転送ドロップがカウントされます。転送ドロップがカウントされる理由はさまざまです。
- **ポリシードロップ** — パケットがファブリックに入ると、スイッチは送信元と接続先 EPG を参照して、この通信を可能にする契約をチェックします。送信元と宛先が異なる EPG にあり、EPG 間でこのパケットタイプを許可する契約がない場合、スイッチはパケットをドロップし、SECURITY_GROUP_DENY であると分類するため、転送ドロップカウンタが増えます。この場合、フローテレメトリイベントでポリシードロップが報告されます。ポリシー ドロップが発生する理由は、通信を許可する契約の欠如です。
- **ポリシングドロップ** - EPGレベルまたは入力インターフェイスで設定されたポリサーが原因でパケットがドロップされると、フローテレメトリイベントでポリシングドロップ異常が報告されます。
- **IDSドロップ** - IDSのパーサーで検出されたヘッダーエラー。該当する場合、内部ヘッダーと外部ヘッダーの両方に関するヘッダーcksumエラー、IP長の不一致、CFG_ft_ids_drop_mask、ゼロDMACなどが表示されます。IDSエラーコードが検出および変換され、フローテレメトリイベントでIDSドロップ異常として報告されます。
- **RTO内部** - ファブリック内のドロップが原因でフローに対してTCP再送信が発生すると、RTO
内部の異常が発生します。この異常は、宛先IPおよび出力VRFに基づいてフロー全体で集約されます。
- **RTO外部** - フローでTCP再送信が発生したが、そのフローのファブリック内でドロップが発生していない場合、RTO
外部異常が発生します。この異常は、宛先IPおよび出力VRFに基づいてフロー全体で集約されます。

フローテレメトリイベントとフローテレメトリ

- フローテレメトリイベントのパケットは、設定されたイベントが発生した場合にのみエクスポートされ、フローテレメトリのパケットは継続的にストリーミングされます。
- フローテレメトリイベントはすべてのトラフィックに対してキャプチャされますが、フローテレメトリはフィルタ処理されたトラフィックに対してキャプチャされます。
- フローテレメトリとフローテレメトリイベント間のコレクタの総数は256です。

フローテレメトリイベントのガイドラインと制約事項

- フローテレメトリイベントは、出力データプレーンポリサーがフロントパネルポートに設定されていて、トラフィックドロップがある場合、Nexus Dashboard Insightsアプリでポリシングドロップ異常を報告しません。
- FXプラットフォームスイッチでフローテレメトリイベントをエクスポートするには、フローテレメトリフィルタを設定する必要があります。

フローテレメトリイベントの参照

1. **[アラートの分析（Analyze Alerts）]** > **[異常（Anomalies）]** の順に選択し、異常を参照します。
2. カテゴリ別フィルタ==フロー
3. リソースの種類が **flowEvent** の異常をクリックします。
4. サイドペインで **[分析（Analyze）]** をクリックして、異常の詳細を表示します。
5. パケットドロップ、TCPパケット再送信、ポリシードロップ、転送ドロップ、および累積ドロップカウントについては、異常の説明を参照してください。

   異常の分析
   ページには、見積もられる影響、推奨事項、および相互発生が表示されます。推定される影響には、影響を受けるフローが表示されます。

   a. サイドペインの **[レポートの表示（View Report）]** をクリックして、フローのリスト、時間の経過とともにドロップされたか影響を受けたパケットの数、影響を受けるインターフェイス、インターフェイスごとのドロップ フローイベントの詳細な分析、そしてバッファ ドロップ異常を表示します。すべてのフロー テレメトリ ドロップ イベントは、影響を受けるインターフェイスを示しています。

   b. *[推奨事項]*セクションには、ノードレベルでのバッファドロップの原因となったフロー、フローの詳細、およびフローテレメトリイベントが表示されます。

エンドポイント

Nexus Dashboard Insights の [エンドポイント（Endpoints）] セクションには、Cisco ACI

サイト全体で収集されたエンドポイント異常のあるノードのエンドポイント情報、チャート、および履歴が含まれています。

エンドポイントは、サイトで学習したエンドポイントの詳細な分析と、次の情報を提供します。

- リーフスイッチに存在するエンドポイント -
  IPアドレス、MACアドレス、ノード、エンティティ名などのフィルタオプションを使用してエンドポイントを参照します。
- 特定の時点におけるサイト内のエンドポイント - エンドポイントの履歴を表示します。
- コンピューティング管理者のエンドポイント情報 -
  エンドポイントの配置情報と、仮想マシンとハイパーバイザとの相関関係を表示します。
- エンドポイントに適用されるポリシー -
  エンドポイントの構成情報および運用情報を表示および検出します。

次の異常は、エンドポイントの一部として検出されます。

- ノード、インターフェイス、およびエンドポイントグループ間のエンドポイントの迅速な移動
- ノードの再起動後に学習に失敗したエンドポイントの欠落
- IPアドレスが重複しているエンドポイント
- スプリアスエンドポイント

Nexus Dashboard Insightsの**[エンドポイント]**には、**[ダッシュボード]**タブと**[参照]**タブの作業ウィンドウで使用できる2つのデータ収集領域が含まれています。

エンドポイント ダッシュボード

エンドポイント
ダッシュボードには、エンドポイントの数が変化する上位ノードの時系列情報が表示されます。エンドポイントは、サイトで学習したエンドポイントの詳細な分析を提供します。

プロパティ	説明
エンドポイント数別の上位ノード	アクティブなエンドポイントの数に基づいて上位ノードが表示されます。
エンドポイント異常別の上位ノード	エンドポイントの異常が最も多いネットワーク内のノードが表示されます。

[エンドポイント異常別の上位ノード]で、ノードカードをクリックして*[エンドポイントの詳細]*ページを表示します。

エンドポイントの[参照]タブ

次の手順で**[参照]**ページに移動します。

1. **[概要（Overview）]** ページで適切なサイトグループを選択します。
2. タイムラインで適切なスナップショットを選択します。
3. 左側のナビゲーションで、**[参照（Browse）]** > **[エンドポイント（Endpoints）]**をクリックします。
4. 作業ペインで表示される **[エンドポイント（Endpoints）]** ページの **[参照（Browse）]** タブをクリックします。

[エンドポイントの参照]ページには、異常スコアでソートされたエンドポイントが要約されています。

- 概要テーブルでエンドポイントをダブルクリックして、*[エンドポイントの詳細（Endpoint Details）]* ページを表示します。*[エンドポイントの詳細（Endpoint Details）]* ページには、エンドポイントの設定と操作に基づいたエンドポイントに関する一般情報が表示されます。
- または、概要テーブルでエンドポイントをクリックして、エンドポイントの一般情報、構成、および操作の詳細を含むサイドバーを表示します。
- サイドバーの右上隅にある [詳細（Details）] アイコン をクリックして、[*エンドポイントの詳細*（Endpoint Details）] ページを表示します。
  ページで設定しなければならない場合があります。

エンドポイントフィルタ

[エンドポイントの参照]には、一定期間における異常スコア別の上位5つのエンドポイントのグラフが表示されます。

[参照]タブの**[フィルタ]**フィールドを使用して、統計情報を表示、ソート、およびフィルタ処理します。表示された統計情報をフィルタで絞り込むことができます。

[フィルタ]フィールドを使用して、次のフィルタから選択してエンドポイントを絞り込みます。

- [テナント] - テナント名を持つノードが表示されます。
- [VRF] - IPアドレスを持つノードが表示されます。
- [BD] - ドメインIDを持つノードが表示されます。
- [EPG/L3out] - エンティティタイプ(L3outまたはEPG)を持つノードが表示されます・
- [MACアドレス] - MACアドレスを持つノードが表示されます。
- [ノード] - ノードのみ表示されます。
- [削除されたIPを検索] - 削除されたIPアドレスが表示されます。

- [インターフェイス] - インターフェイスのみ表示されます。
- [IPアドレス/ホスト名] - IPアドレスとホスト名を持つノードが表示されます。

ホスト名のサポートはベータ機能です。ベータとマークされた機能はテスト環境で使用し、実稼働環境では使用しないことをお勧めします。

- [ステータス] - ノードとステータスが表示されます。
- [時間] - この時点で最後に更新が行われたエンドポイントが表示されます。

フィルタの絞り込みでは、フィルタ、演算子、および値を選択できます。次の演算子を使用できます。

== -
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、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。

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。

[上位5]ドロップダウンフィールドでは、選択に基づいてグラフをモデル化するオプションを選択でき、グラフにはエンドポイントの数がタイムラインとともに表示されます。また、ページの**[フィルタ]**フィールドを使用して、検索する特定の項目を指定できます。

[エンドポイント]ページのテーブルでは、フィルタリングに基づいてコンテンツがフィルタ処理されます。項目をクリックして詳細を表示できます。たとえば、エンドポイントのMACアドレスをクリックして、特定のエンドポイントに関する詳細が記述されているサイドバーを開きます。サイドバーの[詳細]アイコンをクリックして**[エンドポイントの詳細]**ページを開くと、**[一般的な情報]**および**[IP 履歴]**領域の下に詳細が表示されます。

エンドポイントの詳細

このページには、[エンドポイント履歴（Endpoint History）]、[IP 履歴（IP History）]、および [重複エンドポイント（Duplicate Endpoints）] も表示されます。

*[エンドポイント履歴]*には、エンドポイントが更新日の降順で一覧表示されます。一定期間にインターフェイス間およびノード間で移動するエンドポイントが一覧表示されます。強調表示された値

にカーソルを合わせると、その値の変更が表示されます。[変更]列にカーソルを合わせると、すべての変更が表示されます。

IP 履歴 には、特定のIPアドレスに基づいた履歴が一覧表示されます。**[ルーティング（Routing）]** テーブルには、ファブリック内の BD の展開場所が表示されます。

> ACI サイトの場合、IP アドレスをクリックし、サイドバーの [詳細（Details）] アイコンをクリックして [IPの詳細（IP Details）] ページに移動すると、サイト内の特定のノードに展開されたサブネットの場所を表示する **[ルーティング（Routing）]** テーブルが利用可能になります。

[重複（Duplicates）] セクションには、エンドポイントに接続されている重複する IP アドレスが一覧表示されます。同じ IP アドレスを持つ 2 つの異なるノードが一定期間内にエンドポイントに接続された場合。

[アラート（Alerts）] タブには、選択したエンドポイントのノードで発生した異常の概要が表示されます。概要テーブルで異常をクリックして、異常の詳細を含むサイドバーを表示します。

- 異常の詳細ページで **[分析（Analyze）]** をクリックして、異常の存続期間、推定される影響、推奨事項、相互発生、および詳細な分析を表示します。
- 相互発生グラフの異常、障害、イベント、および監査ログにカーソルを合わせます。クリックすると、異常の相互発生に関する詳細な分析が表示されます。
- *[詳細分析]*セクションで、**[分析の設定]をクリックします。** 詳細については、異常の分析を参照してください。

エンドポイントのガイドラインと制約事項

- allow-micro-seg および useg epgs が有効になっている場合、エンドポイントは、エンドポイントグループに対してサポートされません。
- エンドポイント履歴では、エンドポイントの移動ステータスが「タイムアウト」の異常レコードは、異常がアクティブな間は正常、つまり緑色で表示されます。
- エンドポイントは、ネットワークに展開されたポリシーベースのリダイレクトグラフではサポートされていません。
- エンドポイントは、dot1Qトンネルではサポートされていません。
- エンドポイントは、エンドポイント セキュリティ グループではサポートされていません。
- Cisco Nexus Dashboard Insightsを強制的に無効にしても、エンドポイントストリーミングMO (管理対象オブジェクト)は削除されません。新しいMOを投稿するには、回避策として、Cisco Nexus Dashboard Insightsからサイトを無効にしてから有効にします。

イベント

Nexus Dashboard Insights の [イベント（Events）]
セクションには、上位のスイッチノードのイベント発生情報のチャートが表示されます。

ダッシュボードタブ

[イベント（Events）]
ダッシュボードには、時間の経過に伴うイベントの発生、アクション別の監査ログ、重大度別のイベント、重大度別の障害のチャートが表示されます。

プロパティ	説明
時間別のイベント	すべての監査ログ、イベント、および障害がタイムラインチャートで表示されます。タイムラインを変更するには、作業ペインの上部にある [時間範囲（Time Range）] に移動します。
アクション別監査ログ	実行されたアクションに基づいて、すべての監査ログが表示されます。 監査ログには、直接的および間接的なアクションを含む、ユーザーが実行したアクションが記録されます。監査ログの各エントリは、単一の非永続的なアクションを表します。たとえば、ユーザーがログイン、ログアウト、またはサービスプロファイルなどのオブジェクトを作成、変更、削除すると、スイッチマネージャはそのアクションの監査ログにエントリを追加します。

プロパティ	説明
重大度別のイベント	すべてのイベントが重大度別に表示されます。 イベントは、スイッチマネージャによって管理される不変オブジェクトです。各イベントは、インスタンスの非永続的な状態を表します。イベントは、作成されてログに記録された後は変更されません。たとえば、サーバーの電源を入れると、スイッチマネージャはそのリクエストの開始と終了のイベントを作成してログに記録します。
重大度別の障害	すべての障害が重大度別に表示されます。 障害は、可変かつステートフル、永続的な管理対象オブジェクト（MO）として表されます。障害が発生するか、アラームが発生すると、主に障害に関連する MO の子オブジェクトとして障害 MO が作成されます。フォールトオブジェクトクラスでは、親オブジェクトクラスのフォールトルールによりフォールト状態が定義されます。各障害には、障害の発生時に影響を受けたオブジェクトの動作状態に関する情報が含まれます。障害の状態が移行して解決すると、そのオブジェクトは機能状態に移行します。

参照タブ

次のフィルタを使用して、表示された統計情報を絞り込むことができます。

- [作成時間] - 特定の日付のログ、イベント、および障害のみ表示されます。
- [タイプ] - 指定されたタイプのログ、イベント、および障害のみ表示されます。
- [重大度] - 指定された重大度のログ、イベント、および障害のみ表示されます。
- [アクション（Actions）] -
  指定されたアクションタイプのログ、イベント、および障害のみ表示されます。このフィルタは監査ログに適用されます。
- [ノード] - 指定されたノード名のログ、イベント、および障害のみ表示されます。
- [影響を受けるオブジェクト] -
  指定された管理対象オブジェクトのログ、イベント、および障害のみ表示されます。
- [説明] - 指定された説明のログ、イベント、および障害のみ表示されます。

フィルタの絞り込みとして、次の演算子を使用します。

- == -
  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、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。

- < -
  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。
- ⇐ -
  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。
- 監査ログ(タイプ) - 監査ログのみ表示されます。
- イベント(タイプ) - イベントのみ表示されます。
- 障害(タイプ) - 障害のみ表示されます。
- [クリア] (重大度) - クリアされたイベントと障害のみ表示されます。
- 情報(重大度) - 情報イベントと障害のみ表示されます。
- 警告(重大度) - 警告イベントと障害のみ表示されます。
- マイナー(重大度) - マイナーなイベントと障害のみ表示されます。
- メジャー(重大度) - メジャーなイベントと障害のみ表示されます。
- クリティカル(重大度) - クリティカルなイベントと障害のみ表示されます。
- 作成(アクション) - 作成された監査ログのみ表示されます。
- 削除(アクション) - 削除された監査ログのみ表示されます。
- 変更(アクション) - 変更された監査ログのみ表示されます。

プロパティ	説明
アクション別監査ログ	次の基準別の監査ログが表示されます。 • 削除 • 作成 • 変更内容
重大度別のイベント	重大度に基づいてすべてのイベントが表示されます。 • 重大 • やや重大 • 比較的重大でない • その他

プロパティ	説明
重大度別の障害	重大度に基づいてすべての障害が表示されます。 • 重大 • やや重大 • 比較的重大でない • その他

監査ログ、イベント、および障害の参照

[監査ログ、イベント、および障害の参照]
作業ペインを使用して、監査ログ、イベント、障害を表示、ソート、およびフィルタ処理します。

- サイドペインの概要ペインでイベントをクリックして、イベントの詳細を表示します。
- 概要ペインの右上隅にある　をクリックします。
- *[全般（General）]*
  タブの詳細ページには、一般情報、診断、および変更セットが表示されます。
- *[タイムライン（Timeline）]*
  タブには、選択した時間間隔で発生した障害、イベント、および監査ログのグラフが表示されます。ドットにカーソルを合わせると、詳細情報が表示されます。概要テーブルには、選択した時間間隔の障害、イベント、および監査ログが表示されます。

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。

フローテレメトリは、サイトグループ内のサイト間が結合されていないため、各サイトのフローを個別に監視するため、フローテレメトリは個々のフロー用です。たとえば、サイトグループ内に2つのサイト(サイトAとサイトB)があり、トラフィックが2つのサイト間を流れている場合、それらは2つの異なるフローとして表示されます。1つのフローはサイト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注意事項と制限事項

- 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 Dashboard Insights導入ガイドを参照してください。
- Cisco Nexus Dashboard Insights リリース 6.0.1 以降、すべてのフローは、サイトタイプ ACI および DCNM 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)
- mgmt:inb vrf 管理対象オブジェクト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てください。これにより、フローがスパインスイッチから転送されなくなる可能性があります。

- 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サイトグループ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 **有効** と表示されます。

フローテレメトリの設定

次の手順でフローテレメトリを設定します。

1. **[概要（Overview）]** 画面の上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。
3. **[サイトグループの構成（Configure Site Group）]** ページで、**[フロー（Flows）]** をクリックします。
4. **[全般]**タブで適切なサイトを見つけて、[編集]アイコンをクリックします。 **（[全般（General）]**タブのテーブルには、サイト名と、フロー収集が有効か無効かが表示されます）。
5. **[フローの編集（Edit Flow）]** ページの **[フロー収集モード（Flow Collection Modes）]** エリアで、**[フローテレメトリ（Flow Telemetry）]** ボタンを有効にします。すべてのフローはデフォルトで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。
7. **[フローテレメトリルール（Flow Telemetry Rules）]** エリアに、フィルタが表示されます。
8. ルールを追加するには、**[追加（Add）]**
   リンクをクリックし、必要に応じてルール名、テナント、VRF
   の詳細を選択し、チェックマークをクリックします。
9. 次に、**[ルールサブネット（Rule Subnets）]** エリアでサブネットを追加します。
10. **[ルールサブネット]**フィールドに、送信元と宛先のIPアドレスを入力します。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、サブネットを監視するルールを提供できます。
11. **[保存（Save）]** をクリックします。

これで、フローテレメトリプロセスのルールを開始できます。

フローテレメトリのサブネットの監視

フローテレメトリでは、次のようにサブネットを監視します。

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

1. 左側のナビゲーションで、**[参照（Browse）]** > **[フロー分析（Flow Analytics）]** をクリックし、**[ダッシュボード（Dashboard）]** タブをクリックします。
2. **[サイトグループ（Sites Group）]** 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、選択したサイトグループ内のすべてのフローが監視されます。
3. ページの **[参照（Browse）]** タブをクリックして、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選択したスナップショットに基づいています。

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、送信元と宛先に関連する詳細とともに**[パスの概要]**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。

異常とアラートの詳細については、アラートの分析を参照してください。

Netflow

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

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

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

フロー モニタリング セットアップのコンポーネントは次のとおりです。

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

表10. 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	はい	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/ロジカル(スイッチ仮想インターフェイス)	はい	はい	いいえ	いいえ	いいえ	いいえ

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。
- 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を設定する必要があり、データネットワークと同じサブネットに7つのIPが必要です。
- 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、**[概 要 （ Overview ）]** ページのサイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。**[サイトグループの構成（Configure Site Group）]** ページで、**[フロー（Flows）]** をクリックします。**[フロー（Flows）]** ページで、**[コレクタリスト（Collector List）]** 列の **[表示（View）]** をクリックします。

NetFlow の設定

次の手順でNetFlowを設定します。

1. **[概要（Overview）]** 画面の上部で、サイトグループを選択します。
2. サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。
3. **[サイトグループの構成（Configure Site Group）]** ページで、**[フロー（Flows）]** をクリックします。
4. **[全 般]**タブで適切なサイトを見つけて、[編集]アイコンをクリックします。 **（ [全 般 （ General ）]**タブのテーブルには、サイト名と、フロー収集が有効か無効かが表示されます）。

5. **[フローの編集（Edit Flow）]** ページの **[フロー収集モード（Flow Collection Modes）]** エリアで、**[NetFlow]**
   ボタンを有効にします。デフォルトでは、すべてのフローが無効になっています。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。

NetFlowプロセスが開始されます。

ファームウェアアップデート分析

ファームウェアアップデート分析

アップグレードを実行する前に、複数の検証を実行する必要があります。同様に、アップグレードプロセス後、複数のチェックを実行すると、アップグレード手順の変更と成功を判断するのに役立ちます。

ファームウェアの更新分析機能は、推奨されるソフトウェアバージョンへのアップグレードパスを提案し、アップグレードの潜在的な影響を判断します。また、アップグレード前後の検証チェックにも役立ちます。

ファームウェアアップデート分析機能には、次の利点があります。

- ネットワークの正常なアップグレードの準備と検証を支援します。
- アップグレード前のチェックに関する可視性を提供します。
- アップグレード後のチェックとアップグレード後のステータスに関する可視性を提供します。
- 実稼働環境への影響を最小限に抑えます。
- アップグレードプロセスが単一のステップであるか複数のステップであるかを可視化します。
- 特定のファームウェアバージョンに該当するバグを表示します。

注意事項と制約事項

アップグレード後の分析を実行する前に、すべてのノードがアップグレード済みであることを確認してください。

ファームウェアアップデート分析の作成

次の手順を使用して、新しいファームウェアアップデート分析を作成します。

手順

1. **[変更管理（Change Management）] > [ファームウェアの更新分析（Firmware Update Analysis）]** の順に選択します。
2. [サイトグループ]メニューから、サイトグループまたはサイトを選択します。
3. **[新規分析（New Analysis）]** をクリックします。

PSIRTアドバイザリの[アラートの分析]ページからも分析を作成できます。**[アラートの分析（Analyze Alerts）] > [アドバイザリ（Advisories）]** の順に選択します。PSIRTアドバイザリを選択し、**[分析（Analyze）]**をクリックします。[推奨事項]領域で、**[ファームウェアアップデート分析]**をクリックします。

4. 分析名を入力します。
5. サイトを選択します。**[次へ（Next）]** をクリックします。
6. ファームウェアを選択します。シスコ推奨リリースと最新のファームウェアリリースが表示されます。
   a. **[リリースノート]**をクリックして、ファームウェアリリースのリリースノートを表示します。
7. **[ノードの選択 (Select Nodes)]** をクリックします。
   a. ノードを選択します。更新が必要なノードのみ表示されます。分析ごとに一度に選択できるのは10 ノードだけです。
   b. **[追加（Add）]** をクリックします。
8. [保存]をクリックします。
9. ファームウェアの更新分析ジョブは、**[ファームウェアの更新分析（Firmware Update Analysis）]** ダッシュボードに表示されます。
10. 完了した分析をクリックして、詳細を表示します。**[分析の詳細（Analysis Detail）]** ページには、分析の概要、サイトの概要、ノードの概要、ファームウェアとノードのアップグレードパスなどの情報が表示されます。ステップ6でファームウェアを選択した場合、ファームウェアとノードのアップグレードパスは個別に表示されます。
11. **[分析の詳細を表示（View Analysis Detail）]** をクリックして、ファームウェアまたはノードの更新前の分析と更新後の分析を表示します。
12. **[更新前の分析（Pre-Update Analysis）]** タブをクリックして、ノードステータス、検証結果、影響を受ける可能性のあるオブジェクト、アップグレード後に予測されるクリアアラート、アップグレード後に当てはまる潜在的なリリース障害などの詳細を表示します。
    a. **[すべての検証を表示（Show All Validations）]** をクリックして、更新前の検証基準と、各基準で検出された問題を表示します。「Cisco APIC の事前検証基準」を参照してください。
    b. テーブルの任意のオブジェクトをクリックして、追加の詳細を表示します。
    c. [分析を再実行（Rerun Analysis）] **をクリックします。[検証結果]領域で強調表示されている問題を修正したら、**
    領域で、[Rerun Analysis] をクリックして確認します。
13. **[更新後の分析（Post-Update Analysis）]** タブをクリックして、更新後の分析の詳細を表示します。
    a. 推奨されるファームウェアまたはノードのアップグレードを実行します。更新後の概要には、アップグレードのステータスが表示されます。
    b. **[分析を実行（Run Analysis）]** をクリックして、更新後の分析の詳細を表示します。
    c. [**正常性の差分**（Health Delta）]
    タブをクリックして、アップグレード前とアップグレード後の分析間の異常の違いを表示します。
    d. **[運用の差分（Operational Delta）]**
    タブをクリックして、アップグレード前とアップグレード後の分析間の運用リソー

スの違いを表示します。

e. **[ポリシーの差分（Policy Delta）]**
タブをクリックして、アップグレード前とアップグレード後の分析が実行されたときのポリシーの違いを表示します。これは、ACIサイトにのみ適用されます。

f. **[分析を再実行（Rerun Analysis）]** をクリックします。

データ収集タイプがアップロードファイルに対するファームウェアの更新分析の作成

次の手順を使用して、データ収集タイプが**ファイルのアップロード**の新しいファームウェアの更新分析を作成します。

手順

1. **[設定（Settings）]** > **[アプリケーション（Application）]** > **[オフラインスクリプトのダウンロード**（Download Offline Script）] の順に選択して、オフラインデータ収集スクリプト。
2. readmeで指定されている引数を使用してダウンロードしたスクリプトを実行し、ファームウェアアップデート分析のためのデータ収集を有効にします。データ収集が完了すると、tar.gzファイルが作成されます。
3. ファイルをアップロードし、アシュアランス分析を実行します。サイトグループへのファイルのアップロードとアシュアランス分析の実行を参照してください。
4. [サイトグループ（Site Group）] メニューから、データ収集タイプが**アップロードファイル**のサイトグループまたはサイトを選択します。
5. **[変更管理（Change Management）]** > **[ファームウェアの更新分析（Firmware Update Analysis）]** の順に選択します。
6. **[新規分析（New Analysis）]** をクリックします。
7. 分析名を入力します。
8. サイトを選択します。**[次へ（Next）]** をクリックします。
9. ファームウェアを選択します。データを収集するためにスクリプトで使用されたファームウェアバージョンが表示されます。
   a. **[リリースノート]**をクリックして、ファームウェアリリースのリリースノートを表示します。
10. **[ノードの選択 (Select Nodes)]** をクリックします。
    a. ノードを選択します。

    更新が必要なノードのみ表示されます。分析ごとに一度に選択できるのは10 ノードだけです。

    b. **[追加（Add）]** をクリックします。
11. [保存]をクリックします。
12. ファームウェアの更新分析ジョブは、**[ファームウェアの更新分析（Firmware Update Analysis）]** ダッシュボードに表示されます。

13. 完了した分析をクリックして、詳細を表示します。**[分析の詳細（Analysis Detail）]** ページには、ファームウェアとノードの分析ステータス、ファームウェアの概要、アップグレードパスなどの情報が表示されます。

14. **[分析の詳細を表示（View Analysis Detail）]** をクリックして、ファームウェアまたはノードの更新前の分析を表示します。

15. **[概要（Overview）]** タブをクリックして、更新の概要、アップグレードパス、ノードの詳細などの詳細を表示します。

16. **[更新前の分析（Pre-Update Analysis）]** タブをクリックして、ノードステータス、検証結果、影響を受ける可能性のあるオブジェクト、アップグレード後に予測されるクリアアラート、アップグレード後に当てはまる潜在的なリリース障害などの詳細を表示します。

    a. **[すべての検証を表示（Show All Validations）]** をクリックして、更新前の検証基準と、各基準で検出された問題を表示します。「Cisco APIC の事前検証基準」を参照してください。

    b. テーブルの任意のオブジェクトをクリックして、追加の詳細を表示します。

    Python
    スクリプトを再度実行し、ファイルをアップロードしてから、アシュアランス分析を再度実行して、変更がアップグレード前の検証に影響したかどうかを確認することをお勧めします。

    c. [分析を再実行（Rerun Analysis）] **をクリックします。[検証結果]領域で強調表示されている問題を修正したら、**
    領域で、[Rerun Analysis] をクリックして確認します。

Cisco APIC の事前検証基準

事前検証基準	説明	リリース
非アクティブなデバイスが見つかりました	この検証では、すべてのデバイスがアクティブかどうかを確認します。	6.0.1
互換性のあるターゲットバージョンを選択してください	この検証では、ターゲットのファームウェアバージョンが現在実行中のバージョンと互換性があるかどうかを確認します。	6.0.1
リモートリーフの互換性	この検証では、ターゲットのファームウェアバージョンでリモートリーフ機能がサポートされているか、ファブリックがリモートリーフ機能を使用しているかどうかを確認します。	6.0.1
多層互換性	この検証は、ターゲットのファームウェアバージョンで多層トポロジがサポートされているか、ファブリックにTier-2リーフノードがあるかどうかを確認します。	6.0.1
ファブリックにアクティブなクリティカルな設定障害が4つあります	この検証では、ファームウェアの更新に影響を与える可能性があるクリティカルな設定障害または特定の障害の存在を確認します。	6.0.1
ポッドにあるインフラ MP-BGP用のルートリフレクタが 2 つ未満	この検証では、各ポッドに、インフラMP-BGPのルートリフレクタとして設定されたスパインノードが少なくとも2つあるかどうかを確認します。	6.0.1
ノードがvPCにありません	この検証では、ファームウェアの更新中に冗長性/高可用性を確保するために、リーフノードがvPCで設定されているかどうかを確認します。	6.0.1

ノードにアウトオブバンド管理IPがありません	この検証では、OOB (アウトオブバンド) 管理IP設定のないノードの存在を確認して、常にすべてのノードにアクセスできるようにします。	6.0.1
NTPが設定されていません	この検証では、Network Time Protocol (NTP)がCisco APICに設定されているかどうかを確認します。	6.0.1
スイッチ アップグレード メンテナンス グループ チェック	この検証では、APICにメンテナンスグループとファームウェアグループがあるかどうかを確認します。	6.0.1
ルールを検証できませんでした	この検証では、ターゲットのファームウェアバージョンが現在実行中のCIMCバージョンと互換性があるかどうかを確認します。	6.0.1
クラスタ内のCisco APICに異なるインフラVLAN IDが設定されています	この検証では、クラスタ内のAPICに同じインフラVLAN IDが設定されているかどうかを確認します	6.0.1
Cisco APICクラスタのステータスが、すべてのAPICノードに完全には適合していません	この検証では、APICクラスタのステータスがすべてのAPICノードに完全に適合しているかどうかを確認します。	6.0.1
ファブリックリカバリが進行中です	この検証では、進行中のファブリックリカバリがあるかどうかを確認します。	6.0.1
設定されたSNMPv3ユーザー認証やプライバシータイプは、ターゲットのCisco APICファームウェアバージョンでサポートされていません	この検証は、設定されたSNMPv3ユーザー認証やプライバシータイプがターゲットのAPICファームウェアバージョンでサポートされているかどうかを確認します。	6.0.1
エンドポイントネットワークの冗長性	この検証では、ノードの再起動中のトラフィック損失を避けるために、ノードに非冗長エンドポイントがあるかどうかを確認します。	6.0.2

欠陥分析の表示

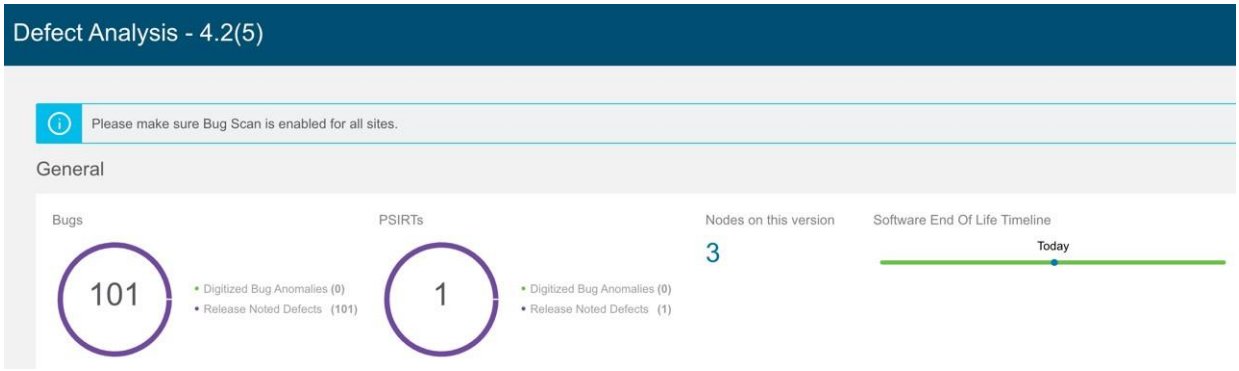
次の手順を使用して、ファームウェアバージョンに関連するデジタル化された欠陥を表示します。

はじめる前に

すべてのサイトでバグスキャンが有効になっていることを確認してください。バグスキャンを参照してください。

手順

1. **[設定（Settings）]** > **[アプリケーション（Application）]** > **[バージョン情報（About）]** の順に選択します。
   a. **[メタデータバージョン（Metadata Version）]** にカーソルを合わせると、現在のリリースのメタデータバージョンのデジタル化された欠陥が表示されます。
2. **[概要（Overview）]** ページで、**[ダッシュボード（Dashboard）]** を選択します。
   a. [異常の概要（Anomaly Summary）] ドロップダウンリストから、**[ファームウェア（Firmware）]** を選択します。
   b. コントローラのファームウェアバージョンにカーソルを合わせ、[リリースノート（Release Notes）] をクリックして、ファームウェアバージョンのリリースノートを表示します。
   c. ノードまたはコントローラのファームウェアバージョンにカーソルを合わせ、**[欠陥分析（Defect Analysis）]** をクリックして、ファームウェアバージョンに関連する欠陥を表示します。
   d. **[欠陥分析（Defect Analysis）]** ページでは、バグ、PSIRT、ノード、およびソフトウェアの EOL タイムラインを確認できます。



デジタル化されたバグの異常は、バグスキャン機能でシステム異常としても検出されるデジタル化されたバグです。リリースノートの不具合は、特定のファームウェアバージョンのリリースノートで既知の問題として言及されているバグです。ソフトウェアのEOLタイムラインには、ファームウェアバージョンのEOLタイムラインが表示され、重大度に基づいて色分けされています。

- クリティカル: 赤色 - EOLは本日から90日未満です。
- 警告: 黄色 - EOLは本日から90日から249日の間です。
- 正常: 緑色 - EOLは本日から250日以上後であるか、EOLはまだ確認できないものの、製品サポートがアクティブになっています。

e. **[デジタル化されたバグの異常（Digitized Bug Anomalies）]** または **[リリースノートの不具合（Release Noted Defects）]**
をクリックして、タイプ、カテゴリ、タイトル、説明などの詳細を下の表に表示します。

f. **[このバージョンのノード（Nodes in this version）]**
をクリックして、ファームウェアバージョンに関連付けられているノードの詳細を表示します。

[欠陥分析]ページには、GUIの次の領域からもアクセスできます。

3. **[ノード（Nodes）]** を選択します。

a. ノードのファームウェアバージョンにカーソルを合わせ、**[欠陥分析（Defect Analysis）]**
をクリックして、ファームウェアバージョンに関連する欠陥を表示します。

4. **[変更管理（Change Management）] > [ファームウェアの更新分析（Firmware Update Analysis）]** の順に選択します。

a. [サイトグループ]メニューから、サイトグループまたはサイトを選択します。

b. **[ノードターゲットファームウェア（Node Target Firmware）]**
列からファームウェアバージョンを選択します。

c. [分析の詳細（Analysis Details）] ページで、ノードターゲット
ファームウェアにカーソルを合わせ、**[欠陥分析（Defect Analysis）]** をクリックします。

変更前の分析

変更前の分析

Cisco Nexus Dashboard InsightsのGUIで、左側のナビゲーション列から[変更前の分析]ページにアクセスできます。**[変更管理（Change Management）]** > **[変更前の分析（Pre-Change Analysis）]** の順に選択します。サイトの設定を変更する場合、Cisco Nexus Dashboard Insightsのこの機能を使用すると、意図した変更をモデル化し、サイト内の既存の基本スナップショットに対して変更前の分析を実行し、その変更で目的の結果が生成されるかどうかを確認できます。

変更前の分析ジョブに対する変更をモデル化したら、**[保存（Save）]** または **[保存して分析（Save And Analyze）]** を選択できます。**[保存（Save）]** を選択すると、すぐに分析を開始しなくても、変更前の分析ジョブを保存できます。後でジョブに戻り、必要に応じて変更を編集し、分析を実行できます。**[保存（Save）]** オプションは、手動で変更した変更前の分析ジョブでのみサポートされています。**[保存して分析（Save And Analyze）]** を選択すると、ジョブがスケジュールされ、分析が提供されます。

ジョブに対して **[保存して分析（Save And Analyze）]** を選択すると、選択した基本スナップショットに変更が適用されて分析が実行され、結果が生成されます。表にリストされているすべての変更前の分析ジョブについて、基本スナップショットと新たに生成されたスナップショットの間で差分分析が実行されます。

> [変更前の分析（Pre-Change Analysis）] ページで、完了した変更前の分析ジョブの詳細を表示するには、テーブル内のそのジョブをクリックします。右側に新しいページが開き、そのジョブの一般的な情報が表示されます。情報には、サイト名、スナップショットの詳細、タイプなどに加え、そのジョブのためにモデル化された変更のリストも含まれます。ジョブが完了すると、[重大度]領域に、それらの変更に対して生成された異常が表示されます。

分析で異常が発生した場合は、結果に基づいて必要な修正を加え、満足のいく結果が得られるまで分析を再実行します。変更前の分析ジョブのダウンロードオプションを使用すると、Cisco APIC にアップロードできる JSON ファイルをダウンロードできます。ただし、ファイル アップロードアプローチを選択した場合は、JSON または XML Cisco APIC 構成ファイルをアップロードして、変更前の分析ジョブを実行できます。

分析が開始されると、ジョブのステータスは[実行中]と表示されます。この間、指定された変更は基本スナップショットの上にモデル化され、ポリシー分析とコンプライアンスを含む完全な論理チェックが実行されます。スイッチソフトウェアまたはTCAMのチェックは実行されません。差分分析を含む分析全体が完了すると、変更前の分析ジョブのステータスが **[完了（Completed）]**

とマークされます。差分分析が自動的にトリガーされ、関連する変更前の分析ジョブがその間 [実行中（Running）] として表示されます。差分分析は、変更前の分析ジョブでサポートされているチェックに対してのみ実行されます。

[変更前の分析]テーブルで変更前の分析ジョブをクリックすると、特定の変更前の分析ジョブにユーザーが適用した変更を表示できます。完了した変更前の分析をクリックすると、変更をサイドバーに表示できます。または、サイドバーの [分析の表示（View Analysis）] をクリックして、表示されているページの [ダッシュボード（Dashboard）] タブに変更を表示できます。変更前の分析ジョブの変更を手動で適用すると、ユーザーが選択したさまざまな変更を表示できます。プレ分析ジョブが JSON ファイルを使用して作成されている場合、[変更定義（Change Definition）] フィールドに、変更のインポート元の JSON ファイルの名前が表示されます。

変更前の分析オプション

次のリストは、変更前の分析ジョブに追加するために選択できるオプションを示しています。リストされているオブジェクトのみサポートされています。

1. テナントを追加、変更、または削除します。
2. アプリ EPG を追加、変更、または削除します（サポートされている属性: 優先グループメンバー、EPG 内分離、アプリ EPG の関係: BD、提供、消費、タブーコントラクト。コントラクトのエクスポート/インポートはサポートされていません）。
3. VRF を追加、変更、または削除します（サポートされている属性: ポリシーコントロールの適用設定、ポリシーコントロールの適用方向、BD 適用ステータス、優先グループメンバー、説明）。
4. BD を追加、変更、または削除します（サポートされている属性: 説明、WAN 帯域幅の最適化、タイプ、ARP フラッディング、IP ラーニング、IP ラーニングをサブネットに制限、L2 不明ユニキャスト、ユニキャストルーティング、マルチデスティネーション フラッディング、マルチキャスト許可、L3 不明マルチキャスト フラッディング）。
5. 契約を追加、変更、または削除します(サポートされている属性: スコープ、説明)。
6. 契約サブジェクトを追加、変更、または削除します（サポートされている属性: リバースフィルタポート、説明、優先順位、ターゲット DSCP、フィルタ名、転送フィルタ名、リバースフィルタ名）。
7. サブネットを追加、変更、または削除します（サポートされている属性: スコープ、優先、説明、プライマリ IP アドレス、仮想 IP アドレス、サブネットコントロール）。
8. アプリプロファイルを追加、変更、または削除します(優先順位、説明)。
9. L3Out を追加、変更、または削除します（サポートされている属性: 説明、VRF 名、ターゲット DSCP、ルート制御適用）。

10. L2Out を追加、変更、または削除します（サポートされている属性: 説明、BD 名、カプセル化タイプ、カプセル化 ID）。
11. L3 Ext EPG を追加、変更、または削除します（サポートされている属性: 優先グループメンバー、説明、優先順位、サポートされている関係: VRF、提供された契約、消費された契約、タブー、ターゲット DSCP）。
12. L2 Ext EPG を追加、変更、または削除します（サポートされている属性: 優先グループメンバー、説明、優先順位、ターゲット DSCP および提供された契約、サポートされている契約、タブー契約）。
13. L3 Ext EPGサブネットを追加、変更、または削除します(サポートされている属性: 説明、スコープ)。
14. タブー契約を追加、変更、または削除します(サポートされている属性: 説明)。
15. タブーサブジェクトを追加、変更、または削除します（サポートされている属性: 名前、説明、サポートされている関係: vzRsDenyRule）。
16. フィルタ、フィルタエントリを追加、変更、または削除します。

ファブリック アクセス ポリシーの場合、変更前の分析ジョブに以下の内容を追加できます。

1. EPGと物理ドメイン間の関係を追加、変更、または削除します。
2. 物理ドメインと対応するVLANプール間の関係を追加、変更、または削除します。
3. 物理ドメインと接続可能なエンティティプロファイル間の関係を追加、変更、または削除します。
4. リーフ インターフェイス プロファイルを追加、変更、または削除します。
5. ポートセレクタを追加、変更、または削除します。
6. スイッチプロファイルを追加、変更、または削除します。
7. スイッチセレクタを追加、変更、または削除します。
8. インターフェイス ポリシー グループを追加、変更、または削除します。
9. CDPおよびLLDPのインターフェイスポリシーを追加、変更、または削除します。

変更前の分析のガイドラインと制約事項

変更前の分析を使用する場合は、次のガイドラインと制約事項に従ってください。

- サイトおよびアップロードされたファイルに対して変更前の分析を実行できます。
- 同じ基本スナップショットで複数の変更前の分析を実行できます。
- 変更前の分析は、基本スナップショットとして使用されている変更前のスナップショットに対しては実行できません。
- 論理構成の異常のみがモデル化され、変更前の分析で実行されます。スイッチソフトウェアと TCAM の変更はモデル化されていません。分析が完了すると、差分分析が自動的に開始され、変更前の分析によって生成されたスナップショットと基本スナップショットが比較されます。差分分析は、変更前の分析ジョブでサポートされているチェックに対してのみ実

行されます。

- 変更前の分析中、基本スナップショットに存在する特定の異常は、変更前の分析では分析されません。その結果、違反が引き続き存在する場合でも、それらの異常は変更前の分析スナップショットには表示されません。そのようなイベントが変更前の分析で分析されない理由は、それらの異常の分析には論理データだけでなく、スイッチソフトウェアと TCAM データも必要だからです。
- コンプライアンス分析には、変更前の分析スナップショットのコンプライアンスチェックの結果が表示されます。
- 変更前の分析スナップショットから異常のローカル検索を実行し、**[ダッシュボード（Dashboard）]**、**[差分分析（Delta Analysis）]**、**[コンプライアンス分析（Compliance Analysis）]**、および **[Explore]** の特定のタブに移動して、結果セクションに表示します。
- 変更前の分析では、サービスチェーンに関連する変更やオブジェクトはサポートも分析もされません。
- [差分分析]タブでは、変更前の分析スナップショットを選択できません。
- 構成スナップショットの設定データが存在しない場合に、このスナップショットを使用して変更前の分析ジョブを実行すると、新しい論理構成ファイルは生成されません。このような変更前の分析ジョブの場合、[ダウンロード（Download）] アイコンはサイドパネルでグレー表示または無効になります。新しい論理構成をダウンロードすることはできません。
- インポートされた構成にサポートされていないオブジェクトが含まれている場合、変更前の分析は [失敗（Failed）] 状態になる可能性があります。変更前の分析オプションセクションを参照してサポートされていない Cisco ACI オブジェクトを特定し、サポートされていないオブジェクトを削除して、別の変更前分析ジョブを開始する前に、構成を再設定してください。失敗した変更前の分析がある場合、失敗のエラーメッセージが **[分析ステータス（Analysis Status）]** の [変更前の分析（Pre-Change Analysis）] テーブルに表示されます。
- 変更前の分析機能は、Cisco APICリリース3.2以降でサポートされています。リリース 3.2 より前の Cisco APIC リリースで変更前の分析を実行しようとすると、変更前の検証は APIC 3.2 以降でサポートされていることを示すエラーメッセージが表示され、分析を実行できません。
- 変更前の分析の開始時に現在実行中の分析がある場合、実行中のジョブが最初に完了します。新しいジョブはスケジュールされた順序で処理されます。Cisco Nexus Dashboard Insights は、スケジュールと使用可能なリソースに最適な順序でジョブを実行します。変更前の分析ジョブを含むすべてのジョブには、同じ優先順位が与えられます。
- 変更前の分析の実行に優先順位を付けるか、強制的に分析を実行するには、スケジューラを開始してジョブに優先順位を割り当てます。そのためには、**[概要（Overview）]** ページの上部で、サイトグループを選択します。サイトグループの横にある [アクション（Actions）] メニューをクリックし、**[サイトグループの構成（Configure Site Group）]** を選択します。**[サイトグループの構成（Configure Site Group）]** ページで、**[アシュアランス分析（Assurance Analysis）]**

タブを選択すると、スケジュールされた分析を停止できます。このページで、すべてのサイトのアシュアランス分析ジョブをすべて無効化できます。

- 現在のところ、JSONまたはXML Cisco APIC構成ファイルをアップロードして、変更前の分析ジョブを実行できます。サポートされる**変更ファイルの最大サイズ**は、vND の場合は 10 MB、pND の場合は 50 MB です。アップロードされたファイルは、ファイルサイズを削減するために空白とエンドポイントオブジェクト（FvCEP）を削除することによってプルーニングされます。
- 変更前分析ジョブは、必要な数だけ保存できます。ただし、サイトの場合、変更前分析ジョブは一度に 1 つしか実行できません。

変更前の分析における複数オブジェクトのサポート

複数のテナントに加えて、変更前の分析のJSONまたはXMLジョブの一部として複数のインフラストラクチャ
オブジェクトを追加することもできます。変更前の分析のアップロードパスを使用すると、ポリシーユニバース全体で複数のオブジェクトを追加、変更、および削除できます。この機能を使用するために必要な追加の設定はありません。アップロードしたファイルに基づいて、複数オブジェクトの変更前の分析ジョブが実行されます。

次のファイルアップロード形式を使用できます。

- サイズが1のIMDATAを含むJSONまたはXMLファイル。
- 意図した変更の単一のサブツリーを含むIMDATA。サブツリーのルートは、変更が単一のサブツリーとして表される限り、UNI
  または他の管理対象オブジェクトにすることができます。
- JSONまたはXMLパスからアップロードしたファイルを使用して、変更前の分析を実行します。変更前の分析が完了したら、同じファイルをACIにアップロードして、変更に使用できます。

変更前の分析に関する既知の問題

- 変更前の分析のスケール制限を超えると、エラーメッセージが表示されずに分析が失敗する可能性があります。
- 変更前の分析ジョブでは、EPG、BD、VRF の総数が 16,000 を超える設定を変更しないでください。
- 新しい変更前の分析を作成するときは、次の点に注意してください。
  - アップロードされる JSON/XML ファイルのサイズが 100 MB未満で 15 MB を超える場合、API がファイルを検証し、*「アップロードファイルのサイズが 15MB(pND)/8MB(vND) の上限を超えています（Uploaded file size exceeds the 15MB(pND)/8MB(vND) maximum limit. ）」*
    のような検証エラーがスローされます。ユーザーがCisco Nexus Dashboard Insights にアクセスし、15MB(pND)/8MB(vND)
    を超えるファイルサイズで変更前の分析ジョブを作成しようとすると、*「ファイルサ*

イズは15MB(pND)/8MB(vND)を超えることはできません（File size cannot be larger than 15MB(pND)/8MB(vND).）」というエラーが UI からスローされます。
したがって、15MB(pND)/8MB(vND)を超えるファイルは変更前の分析ではサポートされていません。

- サポートされていないオブジェクトを含むファイルをアップロードすると、Cisco Nexus Dashboard Insights はサポートされていないオブジェクトを削除し、ジョブを実行します。

- Cisco ACI 構成に Cisco Nexus Dashboard Insights でサポートされていない機能が含まれている場合、変更前の分析ジョブは失敗するか、誤った結果を返すことがあります。
- サービスチェーンを含むCisco ACI設定では、変更前の分析はサポートされていません。
- Cisco Nexus Dashboard Insightsは、変更前の分析のためにアップロードされたJSONファイルに対して限定された一連のチェックを実行します。Cisco ACIは、このファイルを拒否する場合があります。
- 変更前の分析では、外部ルーテッドネットワークのサブネットの属性に関するエラーが誤って報告される場合があります。
- 変更前の分析は、次のCisco APICリリースでサポートされています。
  - 3.2(x)リリースでは、3.2(9h)以前がサポートされています。
  - 4.0(x)リリースでは、4.0(1h)以前がサポートされています。
  - 4.1(x)リリースでは、4.1(2x)以前がサポートされています。
  - 4.2(x) リリースでは、4.2(7s) 以前がサポートされています。
  - 5.0(x)リリースでは、5.0(2e)以前がサポートされています。
  - 5.1(x)リリースでは、5.1(4c)以前がサポートされています。
  - 5.2(x) リリースでは、5.2(4d) 以前がサポートされています。

変更前の分析ジョブの作成

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. 左側のナビゲーションで、**[変更管理（Change Management）]** > **[変更前の分析（Pre-Change Analysis）]** をクリックします。
3. [変更前の分析（Pre-Change Analysis）] ページで、**[アクション（Actions）]** > **[変更前の分析の作成（Create Pre-Change Analysis）]** の順に選択します。**[変更前の分析の作成**（Create Pre-Change Analysis）] ページで、次の操作を実行します。
   a. **[変更前の分析名（Pre-Change Analysis Name）]** フィールドに、名前を入力します。
   b. **[サイト（Site）]** フィールドで、適切なサイトを選択します。
   c. **[スナップショット（Snapshot）]** フィールドで、適切なスナップショットを指定します。
   d. **[変更定義（Change Definition）]** フィールドで、適切なオプションを選択します（**JSON/XML ファイルのインポート**または手動変更)。

選択内容に応じて、入力する関連フィールドが表示されます。JSON または XML ファイルをアップロードするファイル インポート オプションを選択した場合は、**[保存して実行（Save & Run）]** をクリックして、変更前の分析操作を開始する必要があります。手動変更オプションを選択した場合は、ジョブを保存して実行するか、ジョブを保存して後で開始できます（**[アクション（Actions）] > [変更前の分析の編集（Edit Pre-Change Analysis）]** をクリックし、**[保存して実行（Save & Run）]** をクリック）。**[編集（Edit）]** ページでは、必要に応じて一部のフィールドを変更することもできます。

e. 必要に応じて選択を完了し、**[保存（Save）]** または **[保存して実行（Save & Run）]** をクリックします。

変更前の分析ジョブが完了すると、**[変更前の分析（Pre-Change Analysis）]** テーブルにジョブのステータスが [完了（Completed）] として表示されます。詳細を表示する変更前の分析名をクリックします。右側のサイドバーでは、ジョブの名前、スナップショット、変更定義タイプなどの一般情報を含む列に詳細が表示されます。ジョブ用にモデル化された変更のリストも使用できます。完了したジョブを表示している場合は、変更の結果として生成された異常がこのページの上部に表示されます。

完了したジョブの場合は、サイドバーの右上にあるアイコンをクリックして、結果ページに移動します。ジョブの詳細は、**[ダッシュボード（Dashboard）]**、**[差分分析（Delta Analysis）]**、**[コンプライアンス分析（Compliance Analysis）]**、および **[Explore]** に関する特定のタブの下に表示されます。

異常とアラートの詳細については、アラートの分析を参照してください。

変更前の分析ジョブの複製

手動変更の場合のみ、変更前の分析ジョブのクローンを作成できます。

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. 左側のナビゲーションで、**[変更管理（Change Management）] > [変更前の分析（Pre-Change Analysis）]** をクリックします。
3. **[変更前の分析（Pre-Change Analysis）]** ページで、複製する適切な変更前の分析名を選択します。
4. **[アクション（Actions）] > [変更前の分析の複製（Clone Pre-Change Analysis）]** の順に選択します。
5. 新しいページで、次の操作を実行します。
   a. **[変更前の分析名（Pre-Change Analysis Name）]** フィールドに、複製したジョブの名前を入力します。
   b. **[保存（Save）]** をクリックして、変更前の分析ジョブを複製します。

変更前の分析ジョブのダウンロード

次の手順で、既存の変更前の分析をダウンロードできます。

- **[変更前の分析（Pre-Change Analysis）]** テーブルで、完了した変更前の分析ジョブの適切な変更前の分析名をクリックします。変更前の分析のサイドバーで、[ダウンロード]アイコンをクリックしてファイルをダウンロードします。
- 変更前の分析は、JSON 形式で表示される変更前の分析コンテンツを含むオフライン tar ファイルとしてダウンロードされます。

ダウンロードしたファイルでは、変更された属性と変更されていない属性を含むすべての属性を表示できます。必要に応じて、ダウンロードしたファイルCisco APIC にアップロードできます。

変更前の分析ジョブの削除

1. **[概要（Overview）]** ページの上部で、サイトグループを選択します。
2. 左側のナビゲーションで、**[変更管理（Change Management）]** > **[変更前の分析（Pre-Change Analysis）]** をクリックします。
3. **[変更前の分析（Pre-Change Analysis）]** ページで、削除するジョブのチェックボックスをオンにします。
4. **[アクション（Actions）]**> **[変更前の分析の削除（Delete Pre-Change Analysis）]** をクリックします。
5. **[変更前の分析の削除（Delete Pre-Change Analysis）]** ダイアログボックスで、**[削除（Delete）]** をクリックして確定します。

選択したジョブが削除されて、[変更前の分析]ページが更新され、更新されたページが表示されます。

一度に最大10個の変更前の分析ジョブを削除できます。**[実行（Running）]** 状態のジョブは削除できません。削除しようとすると、適切な通知が表示されます。

Nexus Dashboard Orchestrator の統合

Nexus Dashboard Orchestrator の統合

Nexus Dashboard Orchestratorアシュアランスでは、次の機能を利用できます。

- サイト間接続を調査する
- Nexus Dashboard Orchestratorに固有の異常を確認する
- サイト間の不整合に関する異常を発生させる
- 単一サイトグループの集約された異常を確認する
- 個々のサイトの異常を確認する

調査ワークフローの Nexus Dashboard Orchestrator アシュアランスに関する詳細は、Nexus Dashboard Orchestrator アシュアランスの調査を参照してください。

Nexus Dashboard Orchestrator ライブセットアップの追加

次の手順に従って、Nexus Dashboard Orchestratorライブセットアップを追加します。

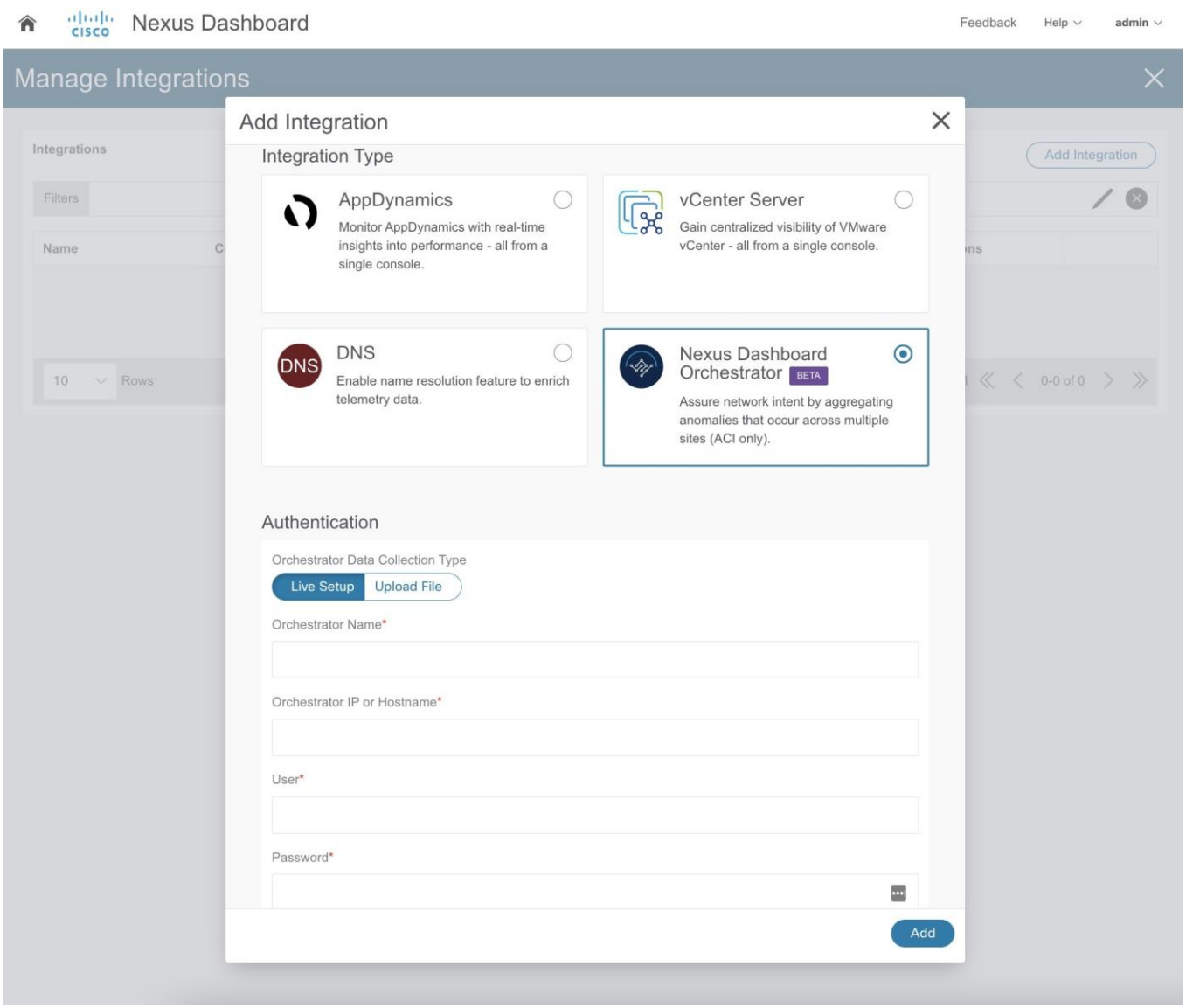
はじめる前に

Nexus Dashboard Orchestrator を Nexus Dashboard Insights と統合する前に、Nexus Dashboard Insights に少なくとも 1 つのサイトグループを追加する必要があります。サイトグループは、Nexus Dashboard Orchestrator の統合時にサイトグループを関連付ける必要があるために追加します。

詳細については、Cisco Nexus Dashboard Insights Day 0 セットアップの基本構成およびCisco Nexus Dashboard Insights Day N セットアップの基本構成を参照してください。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **[管理（Manage）]** の順に選択します。
2. [統合の管理（Manage Integrations）] **ページで、**[統合の追加（Add Integration）] をクリックします。
3. **[統合の追加（Add Integration）]** ダイアログボックスで、**[Nexus Dashboard Orchestrator]** を選択します。
4. **[認証（Authentication）]** エリアで、次の操作を実行します。
   a. **[Orchestrator データ収集タイプ（Orchestrator Data Collection Type）]** フィールドで、**[ライブセットアップ（Live Setup）]** を選択します。



b. **[Orchestrator 名前（Orchestrator Name）]** フィールドに、名前を入力します。

c. **[Orchestrator IP またはホスト名（Orchestrator IP or Hostname）]** フィールドに Orchestrator IP アドレスまたはホスト名を入力します。

d. **[ユーザー（User）]** および **[パスワード（Password）]** フィールドに、Orchestrator ユーザー名とパスワードのログイン情報を入力します。

各操作を実行するには、管理者アカウントを使用する必要があります。Nexus Dashboard Orchestratorのユーザー名とパスワードの値を入力します。

5. **[関連付け（Associations）]** エリアで、**[関連付けの追加（Add Associations）]** をクリックして、適切なサイトグループを関連付けます。

サイトグループに追加されたサイトはすべて、そのサイトグループの一部です。追加されたサイトは、Nexus Dashboard Orchestratorによって管理されるすべてのサイトのサブセットである場合があります。サイトグループに属するすべてのサイトがNexus Dashboard Orchestratorによって管理されている必要はありません。

6. **[管理対象サイト（Managed Sites）]** エリアで、**[管理対象サイトの検出（Detect Managed Sites）]** をクリックします。Nexus Dashboard Orchestrator が管理するすべてのサイトが一覧表示されます。サイトをクリックすると、そのサイト自

体に移動します。

このリストには、サイトグループの一部であるが、Nexus Dashboard Orchestrator が管理しないサイトが含まれている場合があります。

7. **[追加（Add）]** をクリックして、オンボーディングを完了します。

アシュアランス分析を構成するには、Nexus Dashboard Orchestrator ライブセットアップのアシュアランス分析の設定を参照してください。

Nexus Dashboard Orchestrator ライブセットアップのアシュアランス分析の設定

次の手順に従って、Nexus Dashboard Orchestratorライブセットアップのアシュアランス分析を設定します。

はじめる前に

Nexus Dashboard Orchestratorライブセットアップを追加します。

次の手順に従って、Nexus Dashboard Orchestratorライブセットアップのアシュアランス分析を有効にします。

手順

1. アシュアランス分析を有効にするには、**[概要（Overview）]** ページでサイトグループの **[サイトグループの構成**（Configure Site Group）] をクリックします。

   [サイトグループの構成（Configure Site Group）] ページの **[全般（General）]** タブの **[全般（General）]** エリアにある **[Orchestrator]** 列に、Nexus Dashboard Orchestrator の名前が表示されます。**[サイト（Sites）]** エリアには、Nexus Dashboard Insights によってアシュアランスされる Nexus Dashboard Orchestrator の管理対象サイトが一覧表示されます。

2. [**サイトグループの構成**（Configure Site Group）] ページの [**アシュアランス分析**（Assurance Analysis）] タブにある [**サイト間の詳細**（Inter-Site Details）] エリアの [**サイト間アシュアランス**（Inter-Site Assurance）] で、Nexus Dashboard Orchestrator 名を見つけます。
3. **[サイト間の詳細（Inter-Site Details）]** エリアで **[編集（Edit）]** をクリックし、**[サイト間アシュアランスの編集（Edit Inter-Site Assurance）]** ダイアログボックスで状態を **[有効（Enabled）]** に切り替えて、**[保存（Save）]** をクリックします。

このアクションは、サイトグループ内のすべてのサイトに対して、Nexus Dashboard Orchestratorアシュアランス プロセスを暗黙的に有効にします。

アシュアランスプロセスが完了すると、**[サイト間アシュアランスの詳細（Inter-Site Assurance Details）]** エリアで、サイト間アシュアランス名の状態が [有効（Enabled）] になります。アシュアランス分析が完了すると、最後の実行時間と、有効になっているサ

イトの数を確認できます。

サイト間アシュアランスが有効になっているサイトグループ内の各サイトは、サイト間アシュアランスとして表示されます。

Nexus Dashboard Orchestrator 固有の異常の詳細については、 異常を参照してください。

アップロードファイル方式を使用した Nexus Dashboard Orchestrator の設定

次の手順に従って、アップロードされたファイルオプションを使用してNexus Dashboard Orchestratorを追加します。**[新しいサイトグループの追加（Add New Site Group）]** ページでファイルをアップロードします。適切なサイト グループが作成された後、Nexus Dashboard
Orchestratorをサイトグループに関連付けるために、統合を完了する必要があります。

はじめる前に

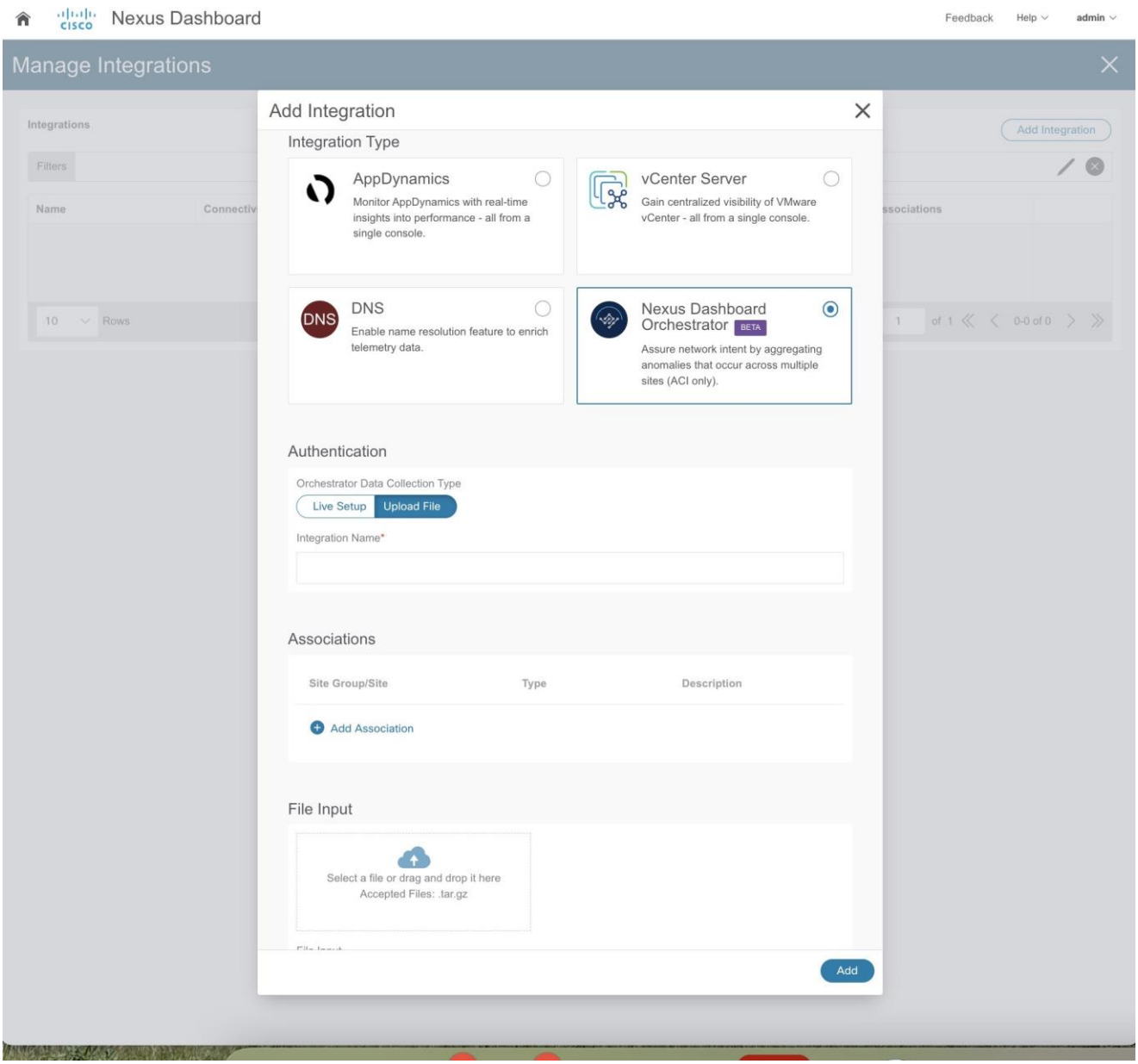
Orchestrator データ収集タイプ の場合、Nexus Dashboard Orchestrator と Nexus Dashboard Insights を統合する前に Nexus Dashboard Insight に追加されたアップロード済みファイルがあるサイトグループを少なくとも 1 つ保持する必要があります。サイトグループは、Nexus Dashboard Orchestrator の統合時にサイトグループを関連付ける必要があるために追加します。

詳細については、Cisco Nexus Dashboard Insights Day 0 セットアップの基本構成およびCisco Nexus Dashboard Insights Day N セットアップの基本構成を参照してください。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **[管理（Manage）]** の順に選択します。
2. [統合の管理（Manage Integrations）] **ページで、**[統合の追加（Add Integration）] をクリックします。
3. **[統合の追加（Add Integration）]** ダイアログボックスで、**[Nexus Dashboard Orchestrator]** を選択します。
4. **[認証（Authentication）]** エリアで、次の操作を実行します。

   a.**[Orchestrator データ収集タイプ（Orchestrator Data Collection Type）]** フィールドで、**[ファイルのアップロード（Upload File）]** を選択します。



サイトグループの一部であり、Nexus Dashboard Orchestrator が管理するファイルのみをアップロードしてください。

a. **[統合名（Integration Name）]** フィールドに、Orchestrator の名前を入力します。

b. **[関連付け（Associations）]** エリアで、**[関連付けの追加（Add Associations）]** をクリックして、適切なサイトグループを関連付けます。

5. **[ファイル入力（File Input）]** エリアで、ファイルを選択するか、ファイルをボックスにドラッグアンドドロップします。許可されるファイルは.gzファイルです。

6. **[追加（Add）]** をクリックして、オンボーディングプロセスを完了します。**[統合の管理（Manage Integrations）]** ページでは、統合名、接続ステータス、タイプなどの詳細に統合タイプが表示され、**[関連付け（Association）]** 列には関連付けられたサイトグループが表示されます。

7.

このサイトグループに追加のファイルをアップロードするには、**[概要（Overview）]** を選択し、**[サイトグループの構成（Configure Site Group）]** ページで、**[ファイル管理（File Management）]** タブをクリックします。**[新しいファイルのアップロード（Upload New File）]** ボタンを使用して、サイトグループの追加ファイルをアップロードします。

アップロードファイル方式を使用した Nexus Dashboard Orchestrator のアシュアランス分析の設定

次の手順に従って、アップロードされたファイルオプションを使用してNexus Dashboard Orchestratorのアシュアランス分析を有効にします。

はじめる前に

アップロードされたファイルオプションを使用して、Nexus Dashboard Orchestratorを追加している必要があります。

手順

1. アシュアランス分析を有効にするには、**[概要（Overview）]** ページに移動し、サイトグループの **[サイトグループの構成（Configure Site Group）]** をクリックします。

   [サイトグループの構成（Configure Site Group）] ページの **[全般（General）]** タブの **[全般（General）]** エリアにある **[Orchestrator]** 列に、Nexus Dashboard Orchestrator の名前が表示されます。**[サイト（Sites）]** エリアには、Nexus Dashboard Insights によってアシュアランスされる Nexus Dashboard Orchestrator の管理対象サイトが一覧表示されます。

2. [**サイトグループの構成**（Configure Site Group）] ページの [**アシュアランス分析**（Assurance Analysis）] タブにある [**サイト間の詳細**（Inter-Site Details）] エリアの [**サイト間アシュアランス**（Inter-Site Assurance）] で、Nexus Dashboard Orchestrator 名を見つけます。
3. **[サイト（Site）]** エリアで適切なサイトの **[オフライン分析の実行（Run Offline Analysis）]** をクリックし、ステータスが [完了（Complete）] になるまで待ちます。
4. [**オフライン分析の実行**（Run Offline Analysis）] をクリックして、**[サイト間の詳細（Inter-Site Details）]** エリアで適切なサイト間アシュアランスを開始します。

[**サイト間アシュアランスの詳細**（Inter-Site Assurance Details）] エリアには、サイト間アシュアランスの名前、状態が有効か無効か、最後の実行時間、アシュアランスされているサイトの数が表示されます。

Nexus Dashboard Orchestrator 固有の異常の詳細については、 異常を参照してください。

Nexus Dashboard Orchestrator のガイドラインと制約事項

- Nexus Dashboard Orchestrator を Nexus Dashboard Insights と統合する前に、Nexus Dashboard Insights に少なくとも 1 つのサイトグループを追加する必要があります。サイトグループは、Nexus Dashboard Orchestrator の統合時にサイトグループを関連付ける必要があるために追加します。
- 後で、Nexus Dashboard Orchestrator

が管理するサイトグループにサイトを追加すると、Nexus Dashboard Insightsは、追加されたサイトをアシュアランスするために自動的に組み込みます。

- サイトグループがNexus Dashboard Orchestratorでアシュアランスされている場合は、サイトグループごとに一意のNexus Dashboard Orchestratorインスタンスを関連付ける必要があります。1つのサイトグループに複数のNexus Dashboard Orchestratorを追加することはできません。1つのNexus Dashboard Orchestratorに複数のサイトグループを追加することもできません。
- サイトグループには、Nexus Dashboard Orchestrator を関連付ける前に、Nexus Dashboard Orchestrator によってアシュアランスされるサイトが少なくとも 1 つ含まれている必要があります。したがって、必要に応じて特定のサイトを Nexus Dashboard Orchestrator によってアシュアランスする場合、それらのサイトは Nexus Dashboard Orchestrator と関連付けられているサイトグループに属している必要があります。
- 設定のインポートとエクスポートは、Nexus Dashboard Orchestratorの統合ではサポートされていません。
- ライブセットアップを使用してNexus Dashboard Orchestratorの統合を作成した後は、統合を編集できません。
- Nexus Dashboard Orchestratorの統合を使用してファイルをアップロードしてアシュアランスを実行した後、必要に応じて、アップロード済みのファイルを新しいファイルに交換できます。ただし、アップロードされたファイルに対してNexus Dashboard Orchestratorアシュアランス分析を実行すると、サイトグループ内のアップロードされたファイルの最新のスナップショットが検索されます。
- アップロードされたファイルの場合、分析を 1 回実行した後でサイト間アシュアランスのオフライン分析を実行するには、最初に個々のサイトで **[オフライン分析の実行（Run Offline Analysis）]** を実行する必要があります。その後、サイト間アシュアランスの **[オフライン分析の実行（Run Offline Analysis）]** をクリックできます。

DNS の統合

DNS の統合について

Cisco Nexus Dashboard Insightsのドメインネームシステム(DNS)統合機能により、名前解決機能でデータをテレメトリできます。DNSの統合は、サイトグループレベルまたはサイトレベルで関連付けることができます。

DNSの統合では、次の3つのデータソースメソッドのいずれかを使用できます。

DNS ファイルのアップロード

マッピングは頻繁に変更されないため、この方法は簡単です。GUIでは、マッピングを含むファイルをアップロードできます。サポートされている形式(.csvおよび.json)のいずれかを使用します。Cisco Nexus Dashboard Insightsはファイルの整合性を検証します。

VRF、サイト名、またはテナント情報が指定されていない場合、**[統合の追加（Add Integrations）]** ページの **[関連付け（Associations）]** セクションの選択に基づいて、DNSサーバーが構成されているサイトに DNS が適用されます。DNSサーバーがサイトグループ用に設定されている場合、DNSはそのサイトグループ内のすべてのサイトに適用されます。

DNSファイルのアップロードサイズは1.8 MBに制限されています。

DNS クエリ

一度に1つのクエリを使用し、逆引きルックアップを使用してDNSサーバーからデータを取得します。DNSサーバーで逆引きルックアップゾーンを設定する必要があります。

Cisco Nexus Dashboard Insights は、定期的に DNS サーバーにクエリを実行し、**エンドポイント**を使用して学習した IP アドレスを解決します。

DNSサーバーで情報が変更された場合、Cisco Nexus Dashboard Insightsで対応する名前マッピングを更新するのに最大3時間かかる場合があります。その間、同期が完了するまで、エンドポイントには古い名前が表示されます。

Cisco Nexus Dashboard Insights では、 1 つのプライマリ DNS サーバーと複数のセカンダリ DNS サーバーが許可されており、プライマリ DNS サーバーが最初にポーリングされます。解決に失敗すると、その後、セカンダリサーバーがポーリングされます。

DNS ゾーン転送

DNSゾーン転送は、AXFRダウンロードとも呼ばれます。Nexus Dashboard Insightsは、AXFRダウンロードを使用して、DNSサーバーからゾーンデータを一括で取得できます。この方法は、一度に1つのクエリを処理する必要がないため、大量データの処理

に便利です。

DNSサーバーで情報が変更された場合、Cisco Nexus Dashboard Insightsで対応する名前マッピングを更新するのに最大3時間かかる場合があります。その間、同期が完了するまで、エンドポイントには古い名前が表示されます。

ゾーン転送には、少なくとも1つのDNSゾーンが必要です。フォワードマッピングゾーンを設定すると、すべてのAおよびAAAAレコードがDNSサーバーから取得され、リバースマッピングゾーンを設定すると、PTRレコードが取得されます。DNSサーバーをオンボーディングするときは、データを取得するゾーンのリストを提供する必要があります。Cisco Nexus Dashboard Insightsは、設定された各ゾーンのデータをDNSサーバーから取得します。

TSIG (トランザクション署名)は、RFC 2845で定義されているコンピュータネットワーキング プロトコルです。主に、DNSがDNSデータベースへの更新を認証できるようにします。安全な転送のために、Cisco Nexus Dashboard Insights では、トランザクションを開始するゾーンの TSIG キーを構成できます。TSIGキーと関連するアルゴリズムを使用してゾーンを設定します。Cisco Nexus Dashboard InsightsのGUIでは、サポートされているアルゴリズムがドロップダウンリストに表示されます。

オンボードDNSサーバーを削除すると、すべてのゾーンが自動的に設定解除されます。ゾーンは、フォワードマッピングまたはリバースマッピングゾーンにすることができます。

DNS ファイルアップロードの設定

次の手順に従って、ファイルアップロード方法を使用してDNSを設定します。

> このタスクで使用される.jsonまたは.csvファイルは、特定のスキーマでアップロードする必要があります。使用するフォーマットについては、次のセクションを参照してください。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **[管理（Manage）]** の順に選択します。
2. [統合の管理（Manage Integrations）] **ページで、**[統合の追加（Add Integration）] をクリックします。
3. **[統合の追加（Add Integration）]** ダイアログボックスで、**DNS** のオプションボタンを選択します。
4. **[構成（Configuration）]** エリアで、次の操作を実行します。
   a. **[DNS タイプ（DNS Type）]** フィールドで、**[マッピングファイル（Mapping File）]** のタイプを選択します。
   b. **[名前（Name）]**

フィールドに、オンボーディングを識別するためにファイルに関連付けられた名前を入力します。

c. [説明（Description）] フィールドに、説明を入力します。

d. **[ファイルを選択するか、ここにドラッグアンドドロップします（Select a file or drag and drop it here area）] エリア**
で、ファイルを追加します。許可されるファイルは.csvまたは.jsonです。

e. **[関連付け（Associations）]** エリアで、**[関連付けの追加（Add Associations）]**
をクリックして、サイトグループまたはサイトを関連付けます。

f. **[追加（Add）]** をクリックして構成を完了します。

[統合の管理（Manage Integrations）] ページの**[統合（Integrations）]**
エリアには、名前、接続ステータス、タイプ、IP
アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

DNS ファイルのアップロード設定の編集

次の手順に従って、DNS設定を編集します。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）]
アイコン > **[統合（Integrations）]** >
管理

[統合の管理（Manage Integrations）] **ページの**[統合（Integrations）]
エリアには、名前、接続ステータス、タイプ、IP
アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

2. DNS 構成を編集するには、**[統合（Integrations）]** テーブルで [アクション（Actions）]
アイコンをクリックし、**[編集（Edit）]** をクリックします。

3. 必要に応じて、ここでファイルを再アップロードできます。

4. アップロードが完了したら、**[追加（Add）]**
をクリックします。これで編集手順は完了です。

DNS ファイルアップロード設定の削除

次の手順に従って、DNS設定を削除します。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）]
アイコン > **[統合（Integrations）]** >
管理

[統合の管理（Manage Integrations）] **ページの**[統合（Integrations）]
エリアには、名前、接続ステータス、タイプ、IP
アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

2. DNS 構成を削除するには、**[統合（Integrations）]** テーブルで [アクション（Actions）] アイコンをクリックし、[削除（Delete）]を**クリックします**。この操作により、DNS設定が削除されます。

DNS ファイルのアップロードで使用されるファイルの形式

DNSファイルのアップロードを設定する場合、.jsonおよび.csv形式がサポートされます。アップロードするファイルには、以下の形式を使用してください。

DNSファイルアップロードのフィールドには、オプションのVRF、サイト名、またはテナント情報を含めることができます。いずれかのオプションの詳細を指定する場合は、すべてのオプションを指定する必要があります。サイト名を含むファイルがある場合は、VRFとテナントも指定する必要があります。

.json 形式

```
[
  {
        "recordType": "dnsEntry",
        "fqdn": "host1.cisco.com",
        "ips": ["1.1.0.0"],
        "vrf": "vrf-1",
        "siteName": "swmp3",
        "tenant": "tenant-1"
  },
  {
        "recordType": "dnsEntry",
        "fqdn": "host2.cisco.com",
        "ips": ["1.1.0.1"],
        "vrf": "vrf-1",
        "siteName": "swmp3",
        "tenant": "tenant-1"
 }
 {
         "recordType": "dnsEntry",
         "fqdn": "host3.cisco.com",
         "ips": ["1.1.0.2"],
 },
]
```

.csv 形式

```
recordType,fqdn,ips,siteName,tenant,vrf
dnsEntry,swmp3-leaf1.cisco.com,"101.22.33.44",swmp3,tenant-1,vrf-1
dnsEntry,swmp5-leaf1.cisco.com,"10.2.3.4,10.4.5.6,1.2.3.4",fabric2,tenant-2,vrf-2
dnsEntry,swmp4-leaf1.cisco.com, "1.1.1.1",,,
```

DNS クエリサーバーの設定

次の手順に従って、DNSクエリサーバー方式を設定します。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **[管理（Manage）]** の順に選択します。
2. [統合の管理（Manage Integrations）] **ページで、**[統合の追加（Add Integration）] をクリックします。
3. **[統合の追加（Add Integration）]** ダイアログボックスで、**DNS** のオプションボタンを選択します。
4. **[構成（Configuration）]** エリアの **[DNS タイプ（DNS Type）]** フィールドで、タイプとして **[クエリサーバー（Query Server）]** を選択します。
5. **[名前（Name）]** フィールドに、統合の名前を入力します。
6. **[DNS サーバーIP（DNS Server IP）]** フィールドに、IP アドレスを入力します。
7. **[DNS サーバーポート]**フィールドに、ポート番号を入力します。デフォルトポートの値は53です。
8. **[セカンダリコントローラ]**領域で、セカンダリコントローラのIPアドレスとポート番号を追加します。必要に応じて、追加のセカンダリコントローラを追加します。
9. 完了したら、選択項目の横にあるチェックマークをクリックします。
10. **[関連付け（Associations）]** エリアで、**[関連付けの追加（Add Associations）]** をクリックして、サイトグループまたはサイトを関連付けます。
11. **[追加（Add）]** をクリックしてタスクを完了します。

[**統合の管理**（Manage Integrations）] ページの**[統合（Integrations）]** エリアには、名前、接続ステータス、タイプ、IP アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

DNS クエリサーバーの設定の編集

次の手順に従って、DNS設定を編集します。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **管理**

   [統合の管理（Manage Integrations）] **ページの**[統合（Integrations）] エリアには、名前、接続ステータス、タイプ、IP アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

2. DNS 構成を編集するには、**[統合（Integrations）]** テーブルで [アクション（Actions）] アイコンをクリックし、**[編集（Edit）]** をクリックします。
3. **[セカンダリコントローラ（Secondary Controllers）]** エリアで、IP アドレスの詳細を追加できます。
4. 編集が完了したら、**[保存（Save）]** をクリックします。これで編集手順は完了です。

クエリサーバー設定の削除

次の手順に従って、DNS設定を削除します。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **管理**

   [統合の管理（Manage Integrations）] **ページの**[統合（Integrations）] エリアには、名前、接続ステータス、タイプ、IP アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

2. DNS 構成を削除するには、**[統合（Integrations）]** テーブルで [アクション（Actions）] アイコンをクリックし、[削除（Delete）]を **クリックします**。この操作により、DNS設定が削除されます。

DNS ゾーン転送の設定

次の手順に従って、ゾーン転送方式を使用してDNSを設定します。

手順

次の手順に従って、DNSゾーン転送方法を設定します。

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **[管理（Manage）]** の順に選択し

ます。

2. [統合の管理（Manage Integrations）] **ページで、**[統合の追加（Add Integration）] をクリックします。
3. **[統合の追加（Add Integration）]** ダイアログボックスで、**DNS** のオプションボタンを選択します。
4. **[構成（Configuration）]** エリアの **[DNS タイプ（DNS Type）]** フィールドで、タイプとして **[ゾーン転送（Zone Transfer）]** を選択します。
5. **[名前（Name）]** フィールドに、Cisco Nexus Dashboard Insights でコントローラを一意に識別する統合の名前を入力します。
6. **[DNS サーバーIP（DNS Server IP）]** フィールドに、DNS サーバーの IP アドレスを入力します。
7. **[DNS サーバーポート（DNS Server Port）]** フィールドに、ポート番号を入力します。デフォルトのポート(53)と異なる場合は、ポートを指定します。
8. **[ゾーン（Zones）]** エリアで、[ゾーン名（Zone Name）] の値を入力します。入力できるオプションの値は、TSIGキー名、TSIGキー値、TSIGアルゴリズムです。

   [TSIG アルゴリズム]ドロップダウンメニューの選択肢は、hmac-sha1、hmac-sha256、hmac-sha512、hmac-md5です。

9. 完了したら、選択項目の横にあるチェックマークをクリックします。
10. **[関連付け（Associations）]** エリアで、**[関連付けの追加（Add Associations）]** をクリックして、サイトグループまたはサイトを関連付けます。
11. **[追加（Add）]** をクリックしてタスクを完了します。

[統合の管理（Manage Integrations）] ページの**[統合（Integrations）]** エリアには、名前、接続ステータス、タイプ、IP アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

DNS ゾーン転送設定の編集

次の手順に従って、DNS設定を編集します。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **管理**

   [統合の管理（Manage Integrations）] **ページの**[統合（Integrations）] エリアには、名前、接続ステータス、タイプ、IP アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

2. DNS 構成を編集するには、**[統合（Integrations）]** テーブルで [アクション（Actions）] アイコンをクリックし、**[編集（Edit）]** をクリックします。
3. **[統合の編集（Edit Integration）]** ダイアログボックスの **[ゾーン（Zones）]**

エリアで、ゾーン名、TSIG キー名、TSIG キー値、TSIG アルゴリズムの値を編集できます。必要に応じて、ゾーンを追加することもできます。

4. 編集が完了したら、**[保存（Save）]** をクリックします。これで編集手順は完了です。

DNS ゾーン転送設定の削除

次の手順に従って、DNS設定を削除します。

手順

1. Cisco Nexus Dashboard Insights の **[概要（Overview）]** ページで、[設定（Settings）] アイコン > **[統合（Integrations）]** > **管理**

   [統合の管理（Manage Integrations）] ページの[統合（Integrations）] エリアには、名前、接続ステータス、タイプ、IP アドレス、最終アクティブ、関連付けごとに各統合の詳細が一覧表示されます。

2. DNS 構成を削除するには、**[統合（Integrations）]** テーブルで [アクション（Actions）] アイコンをクリックし、[削除（Delete）]を**クリックします**。この操作により、DNS設定が削除されます。

[統合]ページにアクセスする別の方法

既存の統合の詳細を表示し、統合を追加する別の方法は次のとおりです。

DNS設定を表示するには、Cisco Nexus Dashboard Insightsの**[概要（Overview）]**ページで、[設定（Settings）]アイコン > **[アプリケーション（Application）]** > **[セットアップ（Setup）]**をクリックします。 **[基本構成（Let's Configure the Basics）]** ページの **[サイトグループのセットアップ（Site Groups Setup）]** エリアで、**[構成の編集（Edit configure）]** をクリックします。**[サイトグループのセットアップ（Site Groups Setup ）]**ページで、**[統 合 （ Integrations ）]**タブをクリックして**[統 合（Integrations ）]**ページを表示します。

DNS の統合のガイドラインと制約事項

- DNSオンボーディングは、サイトグループレベルまたはサイトレベルで実行できます。
- 1つのサイトグループまたは1つのサイトでは、DNSの統合方式は1種類のみサポートされます。たとえば、
  1つのサイトグループまたはサイトで、DNSファイルアップロード方式およびDNSゾーン転送方式を使用して設定することはできません。
- 同じタイプの複数のDNSの統合オンボーディングは、サイトグループまたはサイトで許可されます。たとえば、DNSファイルアップロード方式を使用して、複数のファイルをサイトグループまたはサイトにオンボーディングできます。
- サイトグループレベルでDNSの統合オンボーディングを実行する場合、同じサイトグループ内のサイトをオンボーディングすることはできません。
- 破損しているか、不正な.CSV形式の.JSONファイルがDNSサーバーにアップロードされると、Cisco Nexus Dashboard Insightsはシステム異常を発生させます。ただし、サードパーティのオンボーディングサーバーの**[接 続 ス テ ー タ ス （ Connectivity Status ）]**は、初期化状態のままであり、変更されて失敗状態が表示されることはありません。サードパーティのオンボーディングサーバーが[初期化]状態のままの場合は、特定の統合に関連する異常がないか、システムの異常を確認します。
- DNSの統合でサポートされるスケールは40,000 DNSエントリです。vNDアプリケーションプロファイルの場合、DNSの統合でサポートされるスケールは10,000 DNSエントリです。
- DNSサーバーからのデータは、3時間ごとにポーリングまたは更新されます。したがって、DNSサーバーでのマッピングの変更は、次のポーリングサイクル後に反映されます。
- 設定のインポートとエクスポートは、DNSの統合ではサポートされていません。

AppDynamics との統合

AppDynamics の統合について

Cisco Nexus Dashboard Insights には、ネットワークの問題の監視、トラブルシューティング、識別、および解決を含む、インフラストラクチャ運用のメンテナンスにおける最も一般的で複雑な課題を監視する機能があります。

AppDynamics は、データセンター内のアプリケーションのパフォーマンスと可用性の管理に役立つアプリケーション パフォーマンス管理（APM）と IT 運用分析を提供します。AppDynamicsは、AppDynamicsエージェントで計測されたアプリケーションを監視、識別、および分析するために必要なメトリクスを提供します。

AppDynamicsはサイトレベルでのみ関連付けられます。AppDynamicsコントローラのオンボーディングはサイトレベルでのみ行われ、サイトグループレベルではサポートされていません。

AppDynamics階層は、次のコンポーネントで構成されています。

- ネットワークリンク -
  ネットワークエンティティ間でデータを転送する機能的な手段を提供します。
- ノード -
  アプリケーションの作業エンティティであり、仮想マシン上で実行されるプロセスです。
- 階層 -
  ノードを論理エンティティにグループ化します。各階層には1つ以上のノードを含めることができます。
- アプリケーション - 一連の階層でアプリケーションが構成されます。
- コントローラ -
  コントローラは、アプリケーションのリストを構成する各アカウントを持つ一連のアカウントで構成されます。コントローラの各アカウントはインスタンスです。

AppDynamics を統合すると、Nexus Dashboard Insightsは、AppDynamics によって監視されるアプリケーションの運用データとメトリクスを収集し、収集した情報をCisco ACI サイトから収集したデータと関連付けることができます。

アプリケーションが Cisco ACI サイトを介して通信するシナリオでは、AppDynamics は、異常の原因を特定するために使用できる、アプリケーションとネットワークに関するさまざまなメトリクスを提供します。異常は、アプリケーションまたは基礎となるネットワークにある可能性があります。その結果、ネットワークオペレータはネットワークアクティビティを監視し、異常を検出できます。

AppDynamicsエージェントは、アプリケーションでホストされるプラグインまたは拡張機能です。エージェントは、ネットワークノードと階層の正常性とパフォーマンスを最小限

のオーバーヘッドで監視し、AppDynamics
コントローラに報告します。コントローラは、何千ものエージェントからリアルタイムのメトリクスを受け取り、フローのトラブルシューティングと分析を支援します。

Nexus Dashboard InsightsはAppDynamicsコントローラに接続し、定期的にデータをプルします。AppDynamics コントローラからのこのデータは、アプリケーション固有の情報が豊富な状態で Nexus Dashboard Insights に送信されるため、Cisco ACI サイトを通過するトラフィックに Cisco Nexus Dashboard Insights が提供されます。

AppDynamicsから、エンティティの全体的な異常スコアに寄与する利用可能なメトリクスに関する独自の正常性ルールを作成できます。

Nexus Dashboard InsightsとAppDynamicsの統合により、次のことが可能になります。

- Nexus Dashboard InsightsでのAppDynamics階層の監視と表示。
- ネットワーク関連のメトリクスを収集し、Nexus Dashboard Insightsにインポートします。
- AppDynamicsコントローラから収集されたデータに関する統計分析、フロー分析、およびトポロジビューを表示します。
- AppDynamicsコントローラから収集されたメトリクスの異常トレンドを検出し、当該イベントの検出時に異常を発生させます。
- AppDynamicsの統合では、APIサーバーとTelegraphデータ収集コンテナの複数のインスタンスを使用して、オンボードコントローラのロードバランシングをサポートします。
- AppDynamicsの異常に対するファブリックフローの影響の計算。

SaaS またはクラウドの導入のオンボーディング

Nexus Dashboard Insightsリリースリリースリリースリリースリリースリリースリリースリリースリリース6.0.2以降、SaaSまたはクラウドの導入のプロキシを使用してAppDynamicsコントローラに接続できます。クラウドで実行されているAppDynamicsコントローラをオンボードするために、Nexus Dashboard Insightsは、Cisco Nexus Dashboardで設定されたプロキシを使用してAppDynamicsコントローラに接続します。

注意事項と制約事項

- Nexus Dashboard Insightsリリースリリースリリースリリースリリースリリースリリースリリースリリースのアップグレード後、AppDynamicsがAppDynamics GUIに情報を報告するのに約5分かかります。
- アプリケーションの詳細ページに表示されるAppDynamicsビジネストランザクションの正常性とカウントは、Nexus Dashboard Insightsのフローカウントと一致しません。
- トランジットリーフにはVRFが展開されておらず、トランジットリーフのフローテーブルではフローレコードがNexus Dashboard Insightsリリースリリースリリースリリースリリースリリースリリースリリースリリースにエクスポートされないため、Nexus Dashboard Insightsリリースリリースリリースリリースリリースリリースリリースリリースリリースはファブリックトポロジをサポートしません。したがって、Nexus Dashboard Insightsリリースリリースリリースリリースリリースリリースリリースリリースリリースはパスを完全に結合せず、すべての情報を含む完全なパスの概要を表示しませ

ん。

- HTTPプロキシを使用してHTTPS AppDynamicsコントローラに接続するには、Nexus DashboardでHTTPプロキシサーバーのURLアドレスを使用してHTTPS プロキシを設定する必要があります。
- HTTPプロキシを使用してHTTP AppDynamicsコントローラに接続するには、Nexus DashboardでHTTPプロキシサーバーのURLアドレスを使用してHTTPプロキシを設定する必要があります。
- AppDynamicsの統合では、設定のインポートとエクスポートはサポートされていません。
- AppDynamics 統合のスケール制限:
  - アプリケーションの数：5
  - 階層数：50
  - ノード数: 250
  - ネットリンク数：300
  - フローグループの数: 1000

AppDynamics のインストール

Nexus Dashboard Insightsの **統合** の使用を開始する前に、AppDynamics Application Performance Managementおよびコントローラをインストールする必要があります。詳細については、スタートアップガイドを参照してください。

AppDynamics コントローラのオンボード

次の手順を使用し、GUIを使用してAppDynamicsコントローラをNexus Dashboard Insightsにオンボードします。Cisco Nexus Dashboard InsightsとAppDynamicsの統合の場合、Cisco Nexus Dashboardのデータネットワークは、AppDynamicsコントローラへのIP到達可能性を提供する必要があります。Cisco Nexus Dashboard 導入ガイドを参照してください。

はじめる前に

- AppDynamicsアプリケーションとコントローラをインストールしておく必要があります。
- Nexus Dashboard Insightsの管理者ログイン情報が必要です。
- AppDynamicsコントローラのユーザーログイン情報が必要です。
- プロキシを使用してAppDynamicsコントローラに接続するには、Nexus Dashboardでプロキシを設定しておく必要があります。Cisco Nexus DashboardユーザーガイドのCluster Configurationを参照してください。

手順

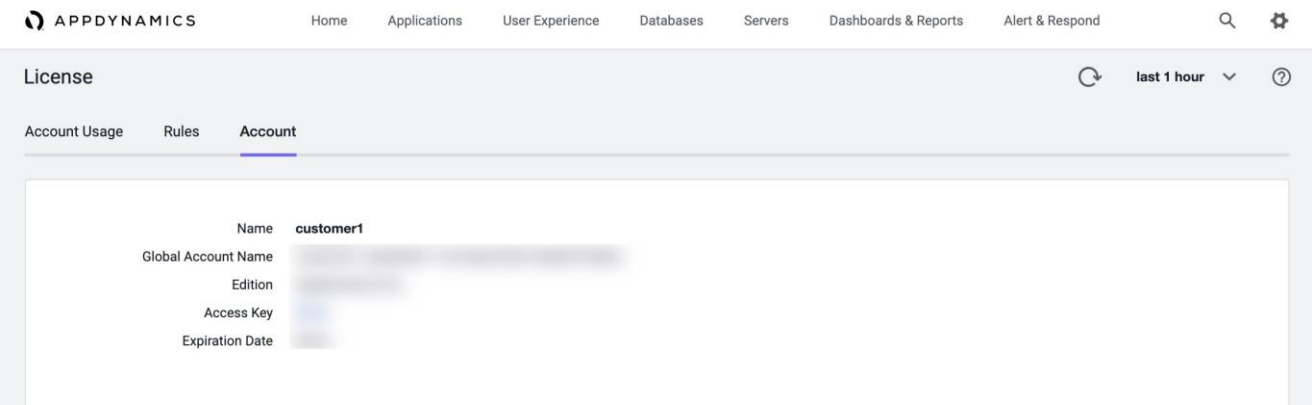
1. **[概要（Overview）]** ページで、**[設定（Settings）]** アイコン > **[統合（Integrations）]** > **[管理（Manage）]** の順に選択します。
2. **[統合の追加（Add Integration）]**をクリックします。
3. **[AppDynamics]** を選択します。
   a. コントローラ名、コントローラIPまたはホスト名、コントローラポートを入力します。コントローラ名には英数字を使用でき、スペースは使用できません。

   > AppDynamicsコントローラ名をNexus Dashboardサイト名と同じにすることはできません。

   a. コントローラプロトコルを選択します。
   b. **[有効化]**チェックボックスをオンにし、プロキシを使用してAppDynamicsコントローラに接続します。プロキシはNexus Dashboardで設定する必要があります。Nexus Dashboardで、**[管理コンソール（Admin Console）]** > **[インフラストラクチャ（Infrastructure）]** > **[クラスタ構成（Cluster Configuration）]** > **[プロキシ構成（Proxy Configuration）]** を選択して、プロキシを構成します。
   c. AppDynamicsアカウント名、ユーザー名、およびパスワードを入力します。Nexus

Dashboard Insightsは、コントローラのオンボーディング中にパスワードベースの認証のみをサポートします。

[設定（Settings）] (歯車アイコン) > [ライセンス（License）] > [アカウント（Account）]に移動して、AppDynamicsセットアップからこの情報を取得できます。



4. **[関連付けの追加（Add Association）]** をクリックして、サイトグループまたはサイトを関連付けます。
   a. サイトグループまたはサイトを選択します。
   b. **[選択（Select）]** をクリックします。
5. **[追加（Add）]** をクリックします。

AppDynamics コントローラが、**[統合の管理（Manage Integration）]** ページに表示されます。**[ステータス（Status）]**が[アクティブ（Active）]の場合、コントローラのオンボーディングは完了です。

Nexus Dashboard Insights の AppDynamics コントローラ

[統合の管理（Manage Integration）]ページのアクティブステータスは、コントローラがデータを取得するためにアクティブになっていることを示します。ダウンステータスは、Nexus Dashboard InsightsがAppDynamicsコントローラからデータを取得しないことを示します。赤いドットにカーソルを合わせると、[ダウン]ステータスの理由を確認できます。

フィルタバーを使用して、特定の統合を検索します。 ... をクリックして **[削除（Delete）]** を選択し、統合を削除します。 ... をクリックして**[編集]**を選択し、統合を編集します。

各コントローラは、同じホスト名に対して複数のアカウント名をサポートします。各アカウント名は、コントローラによって監視される複数のアプリケーションをサポートします。したがって、コントローラは、AppDynamicsによって監視される複数のアプリケーションをサポートできます。

Nexus Dashboard Insights と AppDynamics の統合ダッシュボード

AppDynamicsダッシュボードを使用すると、コントローラをオンボードして、さまざまなメトリクスとともに**[異常スコア別の上位アプリケーション（Top Applications by Anomaly Score）]**のビューを表示できます。コントローラがオンボードされると、そのコントローラによって監視されるアプリケーションに関連するデータがNexus Dashboard Insightsによってプルされます。最初のデータセットがGUIに表示されるまでに最大5分かかることがあります。各エンティティに提供されるAppDynamicsの正常性状態の情報は、ダッシュボード上のNexus Dashboard Insightsによって集計され、報告されます。

AppDynamicsダッシュボードには、AppDynamicsコントローラによって監視されるアプリケーションの概要が表示されます。

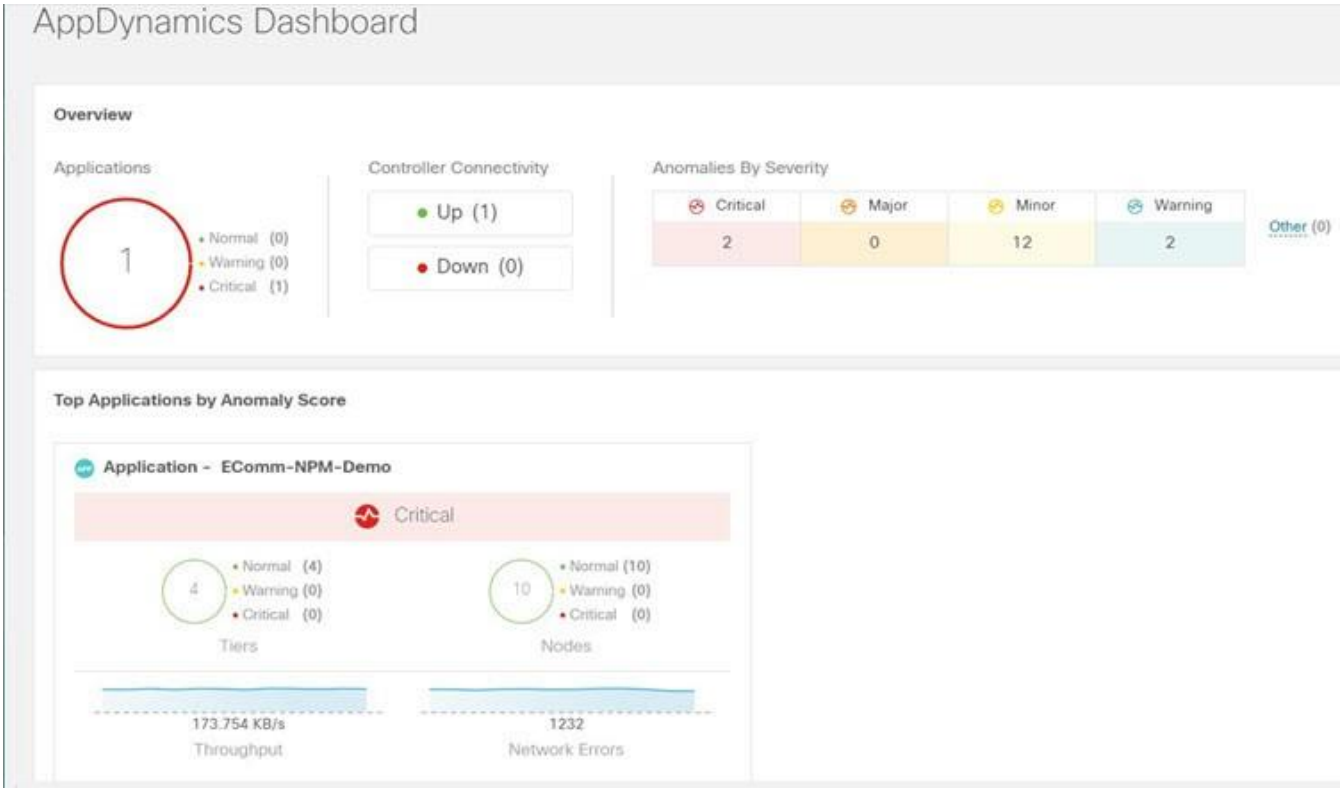
[コントローラの接続性（Controller Connectivity）] - **[アップ（Up）]**または**[ダウン（Down）]**状態の統合の数を表します。

[重大度別の異常] - Nexus Dashboard Insights は、AppDynamics コントローラから受信したメトリクスに対して統計分析を実行します。

[異常スコア別の上位アプリケーション（Top Applications by Anomaly Score）]には、異常スコアに基づいて、すべてのアプリケーションのうち上位6つが表示されます。

- **•[重大度別の異常（Anomalies by Severity）]** の番号をクリックして、[異常（Anomalies）] ページを表示します。

アプリケーション
ウィジェットには、異常スコア別の上位アプリケーションが表示されます。Nexus Dashboard
Insightsで計算されたアプリケーションの異常スコア、AppDynamicsによって報告された階層とノードの正常性の状態も含まれます。



ウィジェットをクリックすると、監視対象アプリケーションの詳細が表示されます。

AppDynamics の統合アプリケーションを参照

[参照]ページには、タイムライン上にプロットされた異常スコアのアプリケーションと履歴が表示されます。各階層またはアプリケーションの運用、統計情報、およびメトリクスを含む詳細情報も表示されます。

異常を一覧表示するには、概要ペインにCategory == Applicationフィルタを使用します。概要ペインには、異常スコア、コントローラ名、アカウント、アプリケーション名、階層数、ノード数、スループット、TCP損失、およびエラーが一覧表示されます。

1. サイドペインの概要ペインで異常をクリックして、追加の詳細を表示します。
   a. **[Analyze（分析）]** をクリックします。

      *[異常の分析の詳細（Analyze Anomaly）]*ページには、アプリケーションの推定される影響、推奨事項、相互発生、および異常の影響を受けるその他の詳細が表示されます。

   b. **[レポートの表示（View Report）]** をクリックします。

      サイドペインには、影響を受けるフローグループが表示されます。各フローグループは、複数のファブリックフローに対応できます。[レポートの表示]には、プロキシ/エンティティのIPアドレス、ノードの送信元、ノードの宛先IPアドレスも表示されます。

2. サイドペインの概要ペインで **[階層数（Number of Tiers）]** をクリックして、使用可能な階層を一覧表示します。リストから各階層をクリックし

て、正常性スコア、ノード数、および使用状況の統計を表示します。

3. サイドペインの概要ペインで **[ノード数（Number of Nodes）]** をクリックして、使用可能なノードを一覧表示します。リストから各ノードをクリックして、ノードに関する統計情報を表示します。
4. サイドペインの概要ペインで **[アプリケーション名（Application Name）]** をクリックして、アプリケーションの一般情報、コントローラ名、コントローラIP、アカウント名、階層の正常性、ノードの正常性、ビジネストランザクションの正常性、使用状況分析などの追加の詳細を表示します。
5. サイドの概要ペインで、右上隅にある アイコンをクリックして、**[AppDynamics アプリケーションの詳細（AppDynamics Application）]** ページを開きます。このページには、異常スコア、アプリケーション階層の概要、アプリケーションノードの概要、ノード通信のネットワークチャート、異常の概要テーブルなどのアプリケーション統計の詳細が表示されます。

   [アプリケーション ネットワーク リンク（Application Network Links）]の表は、AppDynamicsアプリケーション ネットワーク フローマップのさまざまなコンポーネントが相互に通信する方法を示しています。フローカウントや異常など、ネットワークリンクに関する詳細情報は、詳細な分析に使用されます。

6. 特定の AppDynamics 監視対象アプリケーションの概要ペインで各行をダブルクリックして、**[AppDynamics アプリケーションビュー（AppDynamics Application View）]** ページを表示します。

AppDynamics アプリケーションビュー

[AppDynamicsアプリケーションビュー]ページには、階層の正常性、ノードの正常性、ビジネストランザクションの正常性など、アプリケーションの正常性状態の概要が表示されます。

[アプリケーション統計（Application Statistics）]
セクションには、フロープロパティのグラフ表示と、プロパティを表すタイムライングラフが表示されます。

[階層（Tiers）]セクションには、アプリケーションの階層に関する正常性の状態が表示されます。サイドパネルの階層セクションの各行をクリックして、追加の階層の使用状況に関する詳細を表示します。

[ノード（Nodes）]セクションには、アプリケーションのノードに関する正常性の状態が表示されます。サイドパネルの[ノード]セクションの各行をクリックして、追加のノードの使用状況に関する詳細を表示します。

[アプリケーションネットワークリンク（Application Network Links）]セクションには、ノードのリンクの概要が表示されます。

1. サイドパネルの **[ネットワーク接続（Network Connection）]**

をクリックして、追加のフロー接続の詳細を表示します。

2. サイドペインで **[ネットワークフローの参照（Browse Network Flows）]** をクリックして、フィルタに設定されたフロープロパティがある [フローレコードの参照（Browse Flows Records）] に移動します。

   [異常（Anomalies）]セクションには、異常の重大度やその他の重要な詳細とともに異常が要約されています。

3. サイドペインの **[異常（Anomalies）]** セクションの各行をクリックすると、異常の詳細が異常。

4. **[分析（Analyze）]** をクリックして、異常に関する詳細な分析、相互発生、推定される影響、存続期間、および推奨事項を表示します。

5. **[完了（Done）]** をクリックします。

トポロジビュー

トポロジ表示は、Cisco ACI サイトに接続されているノード間のステッチングを表します。

トポロジビューには、アプリケーションノードとリーフノードが含まれます。異常スコアのあるノードを表示するかどうかを切り替えます。異常スコアは、トポロジ内のドットで表されます。

トポロジ表示には、**[アプリケーション（Application）] > [ノード（Node）] > [Cisco ACI リーフ（Cisco ACI Leaf）]** の階層型ビューと、さまざまなオブジェクト間の関連を示す論理ビューまたはネットワークビューとともにオブジェクト間のリンクが表示されます。

AppDynamics の異常

AppDynamicsアプリケーションから、エンティティの全体的な異常スコアに寄与する利用可能なメトリクスに独自の正常性ルールを作成できます。正常性ルールに違反し、AppDynamicsコントローラによって違反が生成された場合、Nexus Dashboard Insightsはそれらの正常性違反をプルし、違反に関する異常を生成します。

概要テーブルに含まれる異常には、次のものがあります。

- AppDynamicsコントローラからのメトリクスで発生した異常。
- AppDynamicsコントローラが発生させたネットワークメトリクスの正常性違反。
- アプリケーションレベルおよびノードレベルでの異常。

インターフェイスの影響を受けるアプリケーションのインターフェイスに異常がある場合、異常が特定されて表示されます。

異常スコアと異常が発生したレベルに応じて、影響を受ける対応するフローが特定されます。Cisco ACI

リーフ情報を含むフローメトリクスに関連する情報により、統計分析が可能になり、アプリケーションかネットワークかを問わず、異常の原因を特定し、影響を受けるエンティティを特定できます。

AppDynamicsの異常に対するファブリックフローの影響計算では、フローAPIを呼び出して、異常の影響を受けたAppDynamicsフローグループに対応するファブリックフローが取得されます。Nexus Dashboard Insights アプリは、AppDynamicsの異常に関する異常スコア順に上位 100 のファブリックフローを表示します。

vCenter の統合

VMware vCenter Server の統合について

VMware vCenter Serverを統合すると、Nexus Dashboard Insightsは、VMware vCenterによって監視される仮想マシンとホストのデータとメトリクスを収集し、収集した情報をCisco ACIまたはCisco DCNMファブリックから収集されたデータと関連付けることができます。

vCenterから収集されるデータには、次のものが含まれます。

- 仮想マシンデータ
- ネットワークデータ
- 仮想マシンNICデータ
- ホストデータ
- データストアデータ
- 標準スイッチ情報
- DVS情報
- vCenterアラーム

Nexus Dashboard Insightsは、15分ごとにvCenterからデータを収集します。Nexus Dashboard InsightsがvCenterに到達できない場合、システム異常が発生します。

vCenter の異常

Nexus Dashboard Insightsでは、vCenterからのアラームが異常として表示されます。次のタイプの異常は、vCenterカテゴリの**vCenter**の統合に対して生成されます。

- vCenterからのホスト、VM、およびデータストアのアラーム
- CPU、メモリ、ストレージなど、チェックの基準の異常
- しきい値の異常

異常の分析を参照して

ください。

前提条件

VMware vCenter 6.5以降がインストールされている。

注意事項と制約事項

- VMware
  vCenterの統合では、設定のインポートとエクスポートはサポートされていません。
- VMware vCenter 統合でサポートされる VM の数は 1000 です。
- VMware vCenter 統合でサポートされる vNIC ホストの数は 10,000 です。

vCenter Server の統合の追加

次の手順を使用して、VMware vCenter ServerをNexus Dashboard Insightsに追加します。

手順

1. **[概要（Overview）]** ページで、**[設定（Settings）]** > **[統合（Integrations）]** > **[管理（Manage）]** の順に選択します。
2. **[統合の追加（Add Integration）]**をクリックします。
3. **[vCenter Server]**を選択します。
   a. コントローラ名、コントローラIPまたはホスト名、コントローラポートを入力します。コントローラ名には英数字を使用でき、スペースは使用できません。
   b. vCenterのユーザー名とパスワードを入力します。
4. **[関連付けの追加（Add Association）]** をクリックして、サイトグループまたはサイトを関連付けます。
   a. サイトグループまたはサイトを選択します。
   b. **[選択（Select）]** をクリックします。
5. **[追加（Add）]** をクリックします。
6. vCenter サーバーが、**[統合の管理（Manage Integration）]** ページに表示されます。**[ステータス（Status）]**が[アクティブ（Active）]になったら、統合の追加は完了です。
7. （任意）**[統合の管理（Manage Integration）]** ページで、フィルタバーを使用して特定の統合を検索します。
   a. `...` をクリックして **[削除（Delete）]** を選択し、統合を削除します。

vCenter Server ダッシュボード

vCenterダッシュボードには、**[異常スコア別の上位仮想マシン（Top Virtual Machines by Anomaly Score）]**または**[異常スコア別のホスト（Hosts by Anomaly Score）]**のビューが、さまざまなメトリクスとともに表示されます。vCenterが追加されると、そのvCenterによって監視される仮想マシンに関連するデータがNexus Dashboard Insightsによってプルされます。最初のデータセットがGUIに表示されるまでに最大5分かかることがあります。

- ナビゲーションウィンドウから**[参照（Browse）]** > **[vCenters]**を選択して、vCenterダッシュボードにアクセスします。
- ドロップダウンから、**[仮想マシン（Virtual Machine）]** または **[ホスト（Hosts）]** を選択します。

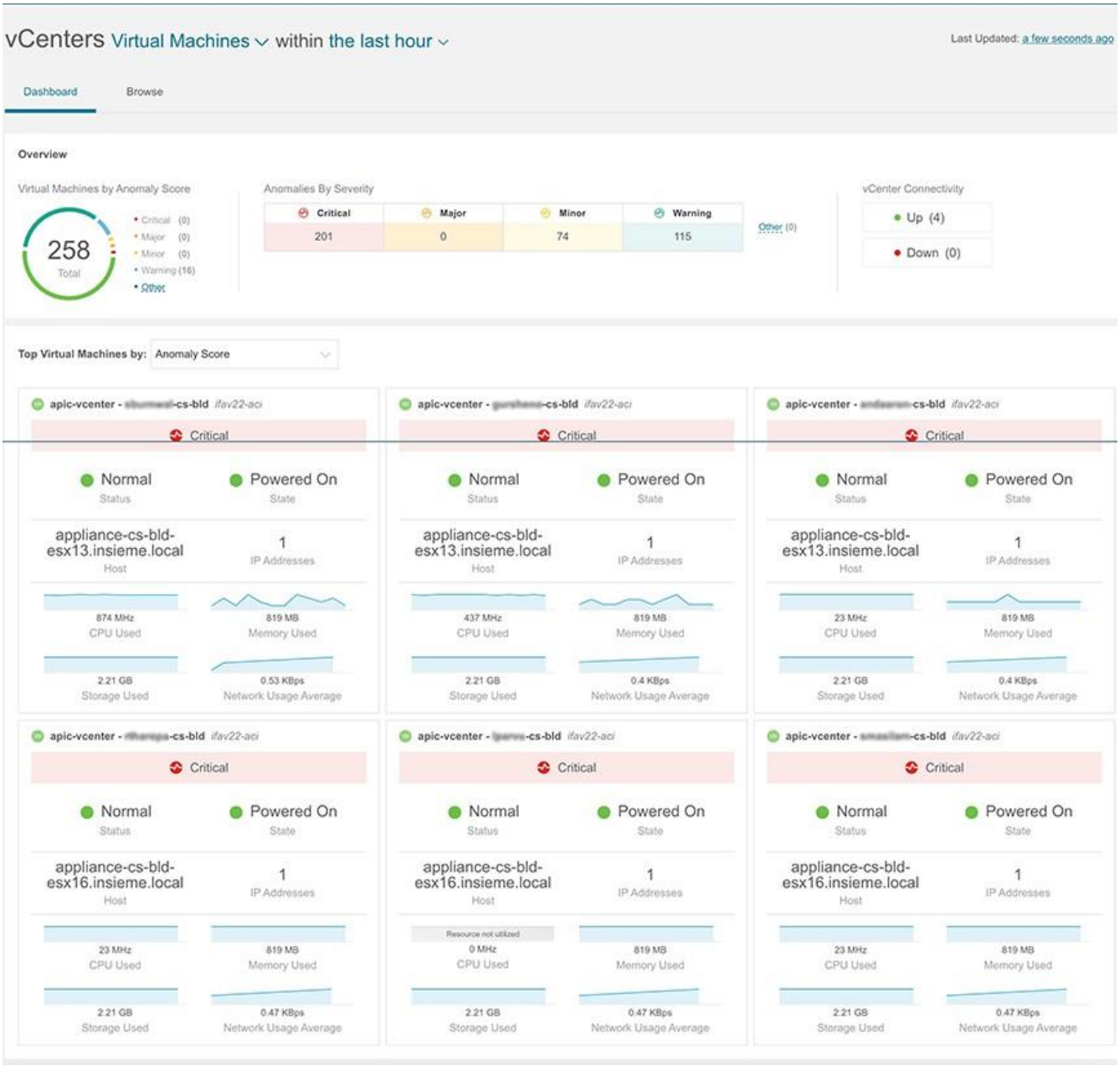
vCenter 仮想マシンダッシュボード

ダッシュボードの **[概要（Overview）]** エリアには、異常スコア別の仮想マシン、重大度別の異常、および vCenter 接続ステータスが表示されます。

- [異常スコア別の仮想マシン] - 仮想マシンの集約された正常性の状態を表します。
- [重大度別の異常] - vCenter Serverからのアラームを表します。[重大度別の異常]の番号をクリックして[異常]ページを表示します。
- [vCenter 接続（vCenter Connectivity）] -**[アップ]**または**[ダウン]**状態になっているvCenterの統合の数を表します。

[異常スコア別の上位仮想マシン（Top Virtual Machines by Anomaly Score）]には、異常スコアに基づいて、すべての仮想マシンのうち上位6つが表示されます。

ドロップダウンリストから、CPU、メモリ、ストレージ、またはネットワークの使用状況を選択すると、ドロップダウンリストの選択に基づいてすべての仮想マシンのうち6つが表示されます。



参照

[参照]ページには、CPUごとの**[上 位 仮 想 マ シ ン （ Top Virtual Machines ）]**がタイムラインにプロットされて表示されます。ドロップダウンリストから、CPU、メモリ、ストレージ、またはネットワークの使用状況を選択すると、ドロップダウンリストの選択に基づいて上位仮想マシンのグラフ表示が表示されます。

1. フィルタバーを使用して、vCenter IP、vCenterコントローラ、VM、ホスト、状態、ステータス、ゲストOS、DNS名、データセンター、ネットワークアダプタ、ネットワークの使用状況、CPU、メモリ、およびストレージでフィルタ処理します。

   フィルタバーの有効な演算子は次のとおりです。

   - == -
     完全に一致するログを表示します。この演算子の後には、テキストや記号を続ける必要があります。
   - contains -
     入力されたテキストまたは記号を含むログを表示します。この演算子の後には、テキストや記号を続ける必要があります。

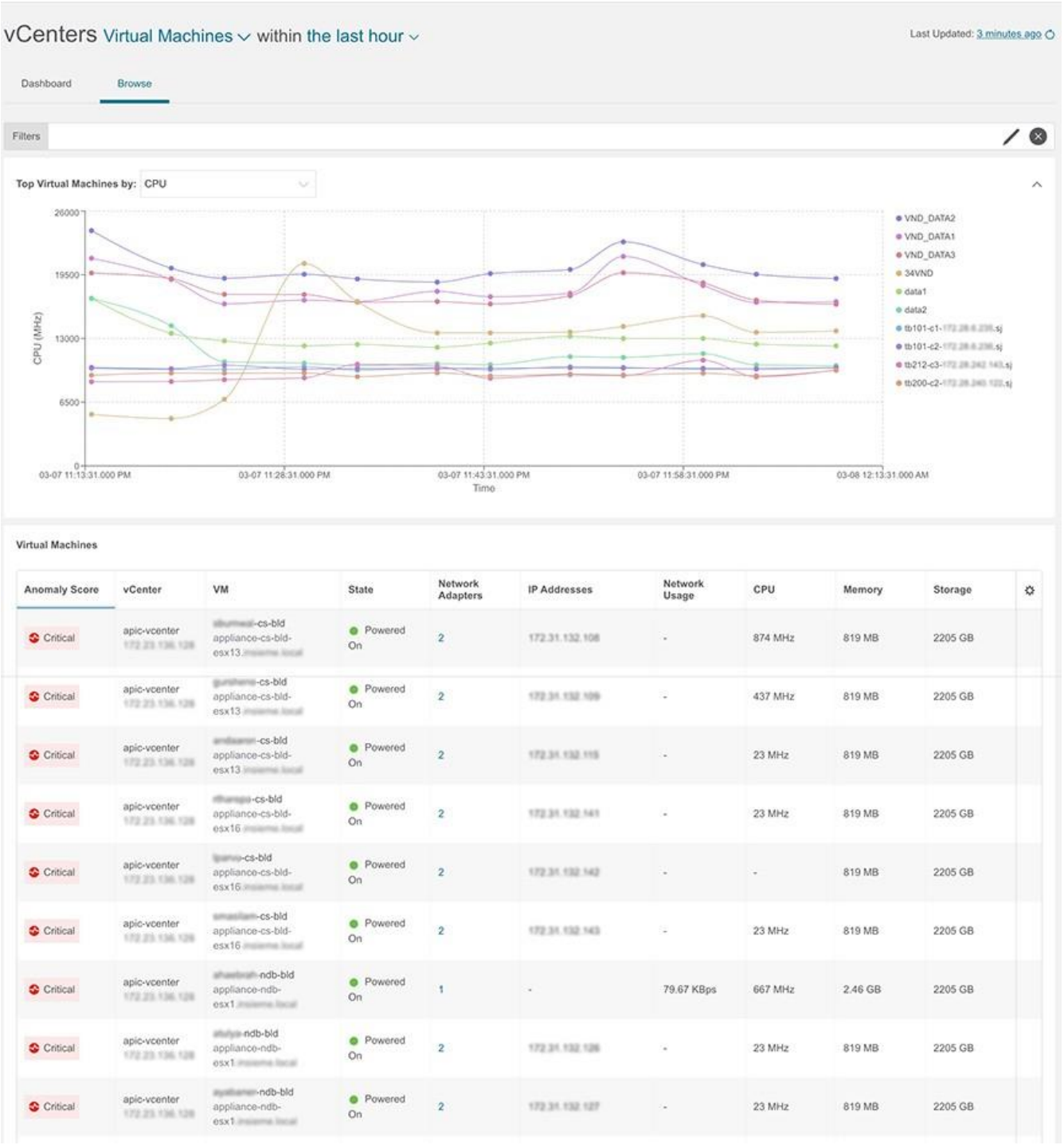
2. このページには、仮想マシンも表形式で表示されます。

   [仮 想 マ シ ン （ Virtual Machines ）]テーブルには、異常スコア、vCenter IPアドレス、仮想マシンのIPアドレス、状態、ネットワークアダプタの数、IPアドレス、ネットワークの使用状況、CPU、メモリ、ストレージなどの情報が表示されます。

   CPU、メモリ、およびストレージについて表示される情報は、VMware vCenter VM の [概要] ページに表示される情報と一致します。

   a. **[設定（Settings）]** メニューをクリックして、**[仮想マシン（Virtual Machines）]** または Hosts テーブル。
   b. 追加の詳細を表示するには、サイドペインのテーブル内の項目を選択します。
   c. アイコンをクリックすると、選択した項目の詳細ページが表示されます。



[仮想マシンの詳細]ページ

- [仮想マシン]ページの**[概要（Overview）]**タブには、異常スコア、使用状況、ホスト、データストア、ネットワークアダプタなどの情報が表示されます。
- [仮想マシン]ページの**[アラート（Alerts）]**タブには、vCenterからのアラームが表示されます。Nexus Dashboard Insightsでは、vCenterからのアラームが異常として表示されます。**[アクション]**ドロップダウンメニューから、異常のプロパティを設定するアクションを選択します。異常のプロパティの設定 を参照してください。
- 仮想マシンの**[トポロジ（Topology）]**タブには、ファブリック内の**[仮想マシン（virtual machine）] > [ホスト（host）] > [リーフスイッチ（leaf switch）]**の階層ビューと、さまざまなオブジェクト間の関連を示す論理ビューまたは

ネットワークビューとともにオブジェクト間のリンクが表示されます。

ホストとリーフスイッチの間に中間スイッチがある場合、ホストトポロジビューのリーフスイッチは切り離された状態で表示されます。Nexus Dashboard Insightsは、このようなトポロジで接続されているリーフスイッチポートを判別できません。これは、ホストブレードとリーフスイッチの間にファブリックスイッチがあるCisco UCS B シリーズブレードサーバーに影響し、中間スイッチを持つ他のトポロジにも影響します。

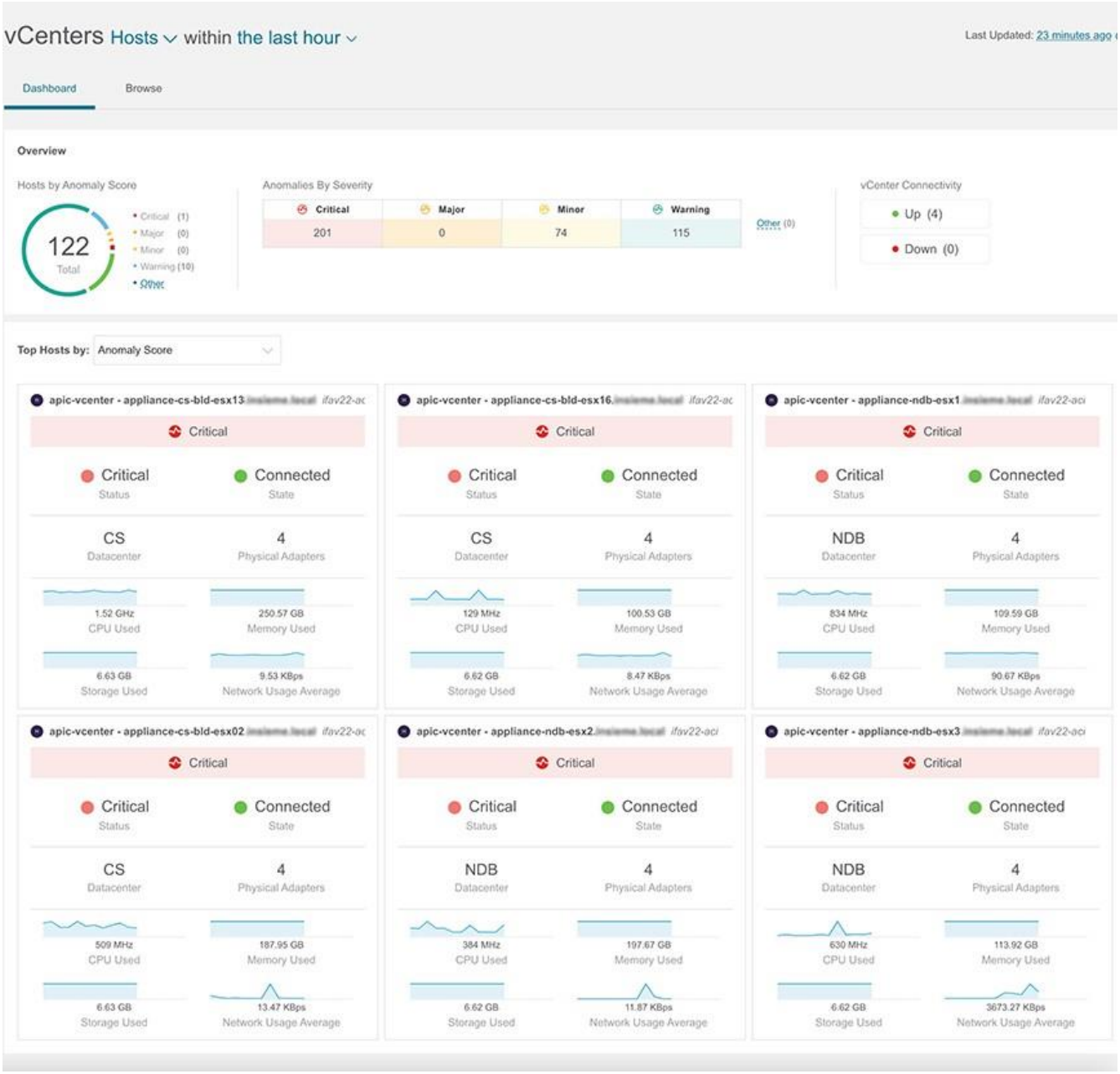
vCenter ホストダッシュボード

ダッシュボードの**[概要（Overview）]**領域には、異常スコア別のホスト、重大度別の異常、およびvCenter接続ステータスが表示されます。

- [異常スコア別の仮想マシン] - 仮想マシンの集約された正常性の状態を表します。
- [重大度別の異常] - vCenter Serverからのアラームを表します。[重大度別の異常]の番号をクリックして[異常]ページを表示します。
- [vCenter 接続（vCenter Connectivity）] -**[アップ]**または**[ダウン]**状態になっているvCenterの統合の数を表します。

[異常スコア別の上位ホスト]には、異常スコアに基づいて、すべての仮想マシンのうち上位6つが表示されます。

ドロップダウンリストから、CPU、メモリ、ストレージ、またはネットワークの使用状況を選択すると、ドロップダウンリストの選択に基づいてすべてのホストのうち6つが表示されます。



参照（Browse）

[参照]ページには、CPUごとの**[上位ホスト（Top Hosts）]**がタイムラインにプロットされて表示されます。ドロップダウンリストから、CPU、メモリ、ストレージ、またはネットワークの使用状況を選択すると、ドロップダウンリストの選択に基づいて上位ホストのグラフ表示が表示されます。

1. フィルタバーを使用して、vCenter IP、vCenterコントローラ、VM、ホスト、データセンター、状態、ステータス、稼働時間、仮想マシン、クラスタ、ハイパーバイザ、モデル、プロセッサタイプ、論理プロセッサ、CPU、メモリ、およびストレージでフィルタ処理します。

   フィルタバーの有効な演算子は次のとおりです。

   - == -
     完全に一致するログを表示します。この演算子の後には、テキストや記号を続ける必要があります。
   - contains -

入力されたテキストまたは記号を含むログを表示します。この演算子の後には、テキストや記号を続ける必要があります。

2. このページには、ホストも表形式で表示されます。

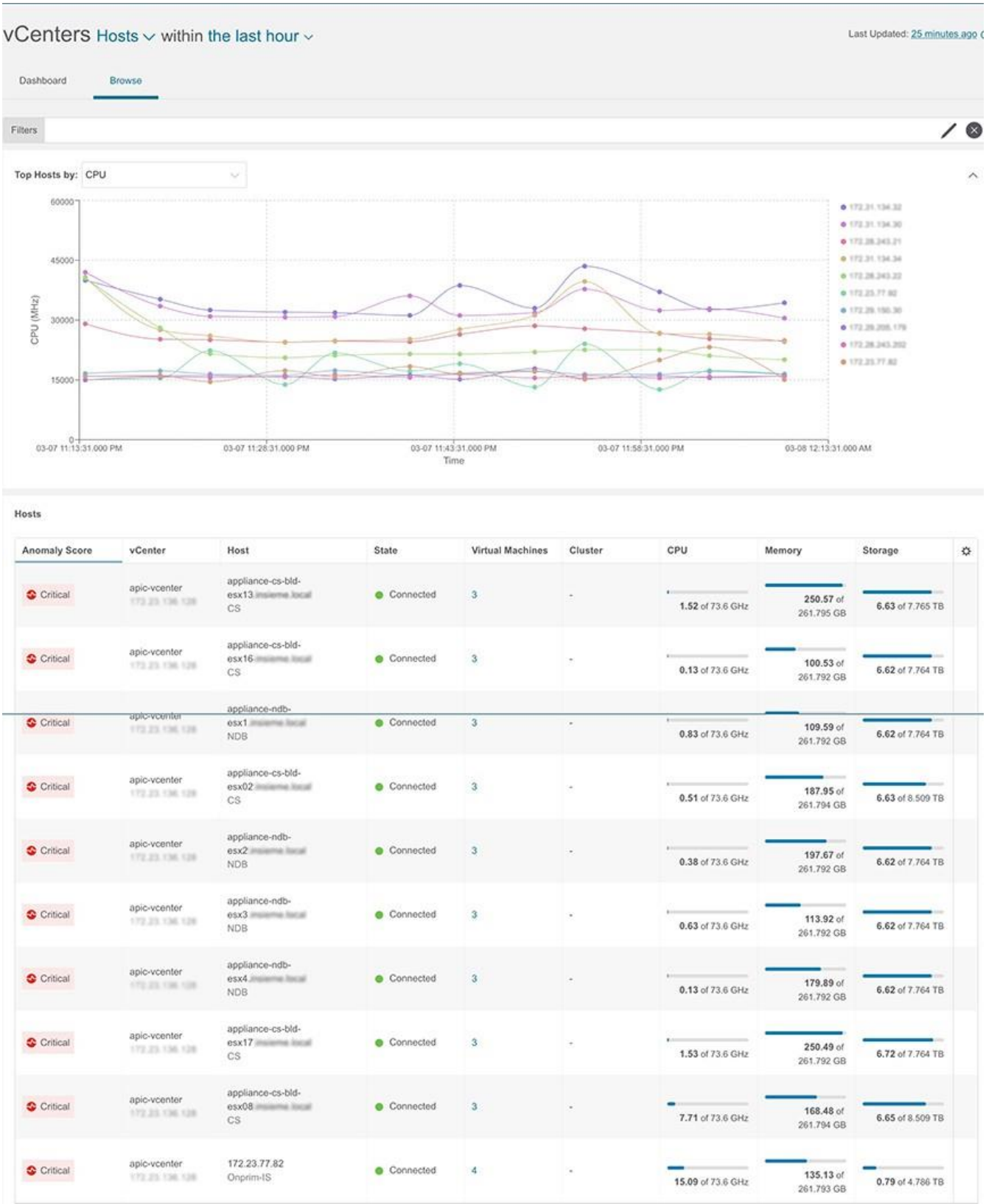
[ホスト（Hosts）]テーブルには、異常スコア、vCenter IPアドレス、ホストIPアドレス、状態、仮想マシン、クラスタ、CPU、メモリ、ストレージなどの情報が表示されます。

CPU、メモリ、およびストレージについて表示される情報は、VMware vCenterホストの[概要]ページに表示される情報と一致します。

a. **[設定（Settings）]** メニューをクリックして、**[仮想マシン（Virtual Machines）]** または Hosts テーブル。

b. 追加の詳細を表示するには、サイドペインのテーブル内の項目を選択します。

c. アイコンをクリックすると、選択した項目の詳細ページが表示されます。



[ホストの詳細]ページ

- [ホスト]ページの**[概要（Overview）]**タブには、異常スコア、使用状況、仮想マシン、データストア、分散スイッチ、標準スイッチなどの情報が表示されます。
- [仮想マシン]ページの**[アラート（Alerts）]**タブには、ホストのvCenterからのアラームが表示されます。
- 仮想マシンの**[トポロジ（Topology）]**タブには、ファブリック内の**[ホスト]**>**[仮想マシン]**>**[DVS]または仮想スイッチの階層ビューと**、さまざまなオブジェクト間の関連を

示す論理ビューまたはさまざまなオブジェクトがどのように関連しているかを示すネットワーク ビュー。