Cisco Nexus Dashboard Insights ユーザーガイド、リリース 6.1.x - Cisco DCNM 向け

目次

初版: 2022-05-03

最終更新日: 2022-05-27

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
電話: 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 UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

このマニュアルで使用している Internet Protocol（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。このドキュメント一式における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ーインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。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。Third-party trademarks mentioned are the property of their respective owners. 「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。（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、今リリースまでの変更点や新機能の一部は表に記載されていません。

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

機能	説明	リリース	参照先
Cisco Nexus Dashboard Fabric Controller (NDFC) のサポート	Cisco Nexus Dashboard プラットフォームを Nexus Dashboard Fabric Controller ファブリックと一緒に使用する Cisco Nexus Dashboard Insights サービスの機能と使用例。Nexus Dashboard Fabric Controller は以前は Data Center Network Manager と呼ばれていました。	6.1.1	--
syslog サポート	異常とアドバイザリの Syslog 形式でのエクスポートをサポートしています。	6.1.1	*Syslog*
VMware vCenter の統合	VMware vCenter の統合を追加して、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ます。	6.1.1	*VMware vCenter Server の統合について*
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。	6.1.1	*エアギャップ環境のメタデータサポート*

機能	説明	リリース	参照先
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	ソフトウェアとハードウェアの適合性ダッシュボードでは、サイトの全体的なソフトウェアとハードウェアの適合性インベントリのステータスを確認できます。	6.1.1	*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*
異常のチェックコード	異常をチェックコードでフィルタ処理すると、結果が[異常]テーブルに表示されます。	6.1.1	*異常の分析*
L4-L7 トラフィックパスの可視性	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しました。	6.1.1	*L4-L7 トラフィックパスの可視性*
列のカスタマイズ	テーブルの**[列のカスタマイズ]**機能を使用して、テーブルの列をカスタマイズし、ログインインスタンスとその後のログイン中に設定が維持されるようにできます。	6.1.1	*Nexus Dashboard Insights の[概要]ページのナビゲーション*
マルチサイト トラフィック パス	ベータ機能: 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。	6.1.1	*マルチサイト トラフィック パス - ベータ機能*
SR-MPLS フロー	ベータ機能: NX-OS ファブリックでの SR-MPLS フロー分析とフローラベルがサポートされます。	6.1.1	*SR-MPLS フロー - ベータ機能*

このドキュメントは、www.cisco.com のオンラインだけでなく、Nexus Insights GUI からも入手できます。このドキュメントの最新バージョンについては、Cisco Nexus Insights のドキュメントにアクセスしてください。

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。

このユーザーコンテンツでは、Cisco Nexus Dashboard プラットフォームを Nexus Dashboard Fabric Controller ファブリックと一緒に使用する Cisco Nexus Dashboard Insights サービスの機能と使用例について説明します。Nexus Dashboard Fabric Controller は、以前は Data Center Network Manager と呼ばれていました。

Cisco Data Center Network Manager（DCNM）は、リリース 12.0.1a 以降、 Cisco Nexus Dashboard Fabric Controller（NDFC）に名前が変更されました。

Cisco Nexus Dashboard Insights のコンポーネント

Cisco Nexus Dashboard Insights (Nexus Dashboard Insights)は、データセンター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 と連携するとき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。

DCNM サイトは、NX-OS を実行しているファブリックで構成されています。このファブリックは、DCNM によって完全に管理されるか、または監視だけされています。ファブリック内のすべてのスイッチをサイトの一部として分析できます。NX-OS ベースのファブリックでは、ファブリックは DCNM 管理対象ファブリックである場合もあれば、CLI、Ansible、またはその他の設定自動化メカニズムなど、他の手段を使用して設定されている場合もあります。設定管理に DCNM を使用していないファブリックの場合、DCNM をインストールし、ファブリックを読み取り専用モードまたはモニターモードで検出する必要があります。Nexus Dashboard Insights は、DCNM を使用してトポロジディスカバリを行い、ファブリック内のスイッチの役割を識別します。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。

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。
- [サイトグループの設定] - フローを設定し、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をスケジュールします。
    - [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。

- [ベストプラクティス] - 選択したサイトに対して実行されるオンデマンドのコンプライアンスジョブを設定、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。コンプライアンスジョブは、テクニカルサポート情報を収集し、既知の署名セットに対してそれらを実行し、コンプライアンスに対応していない不具合にフラグを付けます。
- [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。
- [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。
- [コンプライアンス要件] - この機能は現在サポートされていません。
- [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 Nexus 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。
- トラブルシューティング
  - [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。
  - [接続性分析] - 接続性分析ジョブは、特定のフローについて考えられるすべての転送パスを追跡し、特定のフローに対してネットワーク内の違反しているノードを分離し、トラブルシューティングを支援して、問題の根本原因を絞り込みます。

- 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。

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。

詳細については、Cisco 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ておきます。
- 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]**をクリックします。
3. **[サイト]**ページで、**[サイトの追加]**をクリックします。
4. **[サイトの追加]**ページの**[サイトタイプ]**フィールドで、**[DCNM]**を選択し、次のアクションを実行します。
5. **[ホスト名/IP アドレス]**フィールドに、サイトコントローラとの通信に使用する帯域内 IP アドレスを追加します。
6. **[ユーザー名]**および**[パスワード]**フィールドに、サイトの管理に使用する値を追加します。読み取り/書き込み権限を持つ管理者として、DCNM のユーザー名とパスワードの値を入力します。
7. (任意) **[ログインドメイン]**フィールドを空のままにすると、サイトのローカルログインが使用されます。
8. **[DCNM 上のサイト]**領域で、**[サイトの選択]**をクリックして、指定したコントローラによって管理される DCNM ファブリックを選択します。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。
9. サイトを選択し、**[選択]**をクリックします。複数のサイトを選択できます。
10. **[サイトタイプ]**フィールドで、**[追加]**をクリックします。**[サイト]**ページで新しいサイトを確認できます。
11. (オプション)**[サイト]**テーブルで、必要に応じて編集アイコンをクリックしてサイト名を変更できます。サイト名は一意である必要があります。別の Cisco DCNM から複数のサイトを追加するには、上記の手順を繰り返します。
12. (任意)サイトの場所を指定するには、[地理的な位置]マップをクリックします。
13. 続けて、GUI を使用して Cisco Nexus Dashboard に Cisco Nexus Dashboard Insights をインストールします。

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。

はじめる前に

- Cisco Nexus Dashboard Insights サービスをインストールしていること。
- 適切なサイトが Cisco Nexus Dashboard に追加されていること。

Nexus Dashboard Fabric Controller (NDFC)サイトのオンボーディングについて:

- テレメトリ用のスイッチのデータポートとスイッチの管理ポートは、Cisco Nexus Dashboard Insights クラスタのデータネットワークを使用して到達可能である必要があります。
- NDFC のデータネットワークは、Cisco Nexus Dashboard Insights クラスタのデータネットワークを使用して到達可能である必要があります。

Nexus Dashboard Fabric Discovery (NDFD)サイトのオンボーディングについて:

- テレメトリ用のスイッチのデータポートとスイッチの管理ポートは、Cisco Nexus Dashboard Insights クラスタのデータネットワークを使用して到達可能である必要があります。

> Cisco Nexus Dashboard Insights クラスタでは常に NDFD をオンボードする必要があります。

手順

1. [Cisco Nexus Dashboard Insights サービス]ページの**[基本設定]**ページにある**[サイトグループのセットアップ]**領域で、**[設定]**をクリックします。
2. **[サイトグループのセットアップ]**ページで、**[新しいサイトグループの追加]**をクリックします。
3. **[新しいサイトグループの追加]**ダイアログボックスで、**[全般]**領域の**[名前]**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]**領域で**[サイトの追加]**をクリックし、**[エンティティ]**領域で**[メンバーの追加]**をクリックします。
5. **[メンバーの選択]**をクリックします。
6. **[サイトの選択]**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]**ダイアログボックスの**[設定]**領域で、**[サイトの追加]**を選択します。
8. 適切なサイトを選択し、**[選択]**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]**ダイアログボックスの**[ステータス]**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**[設定]**リンクをクリックします。
11. **[設定]**ダイアログボックスの**[全般設定]**領域で、**[ユーザー名]**および**[パスワード]**フィールドに値を入力します。

> これらのアクションを実行するには、管理者の読み取り/書き込み権限が必要です。DCNM 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]**ページで、**[完了]**をクリックします。

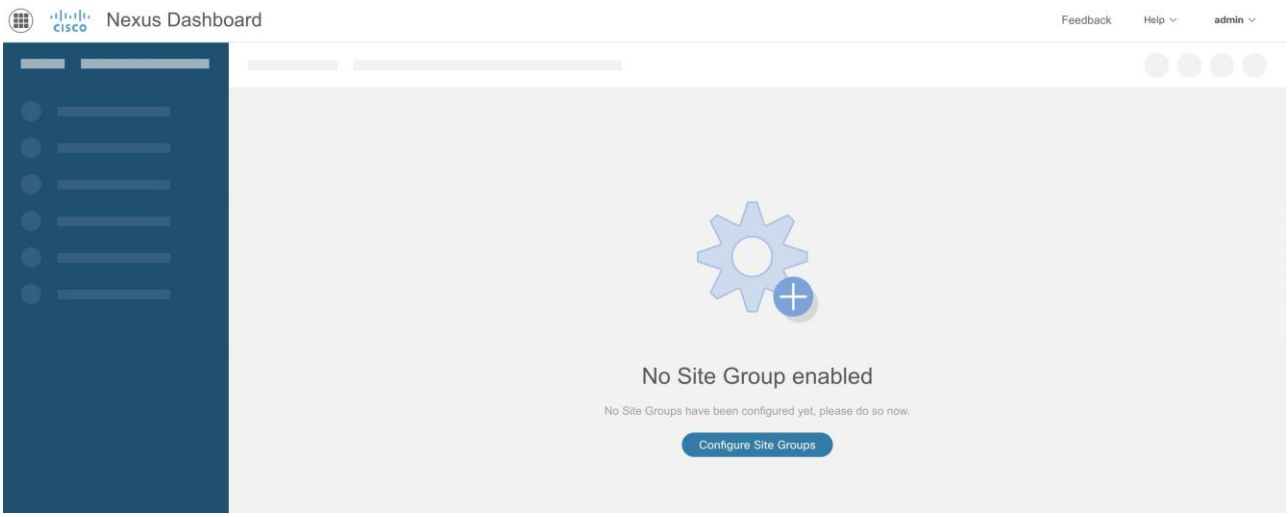
サイトは、**[サイトグループの設定]** > **[全般]**タブで有効になっています。これで初期セットアップは完了です。

> 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有効にする場合は、サイトを有効にする必要があります。

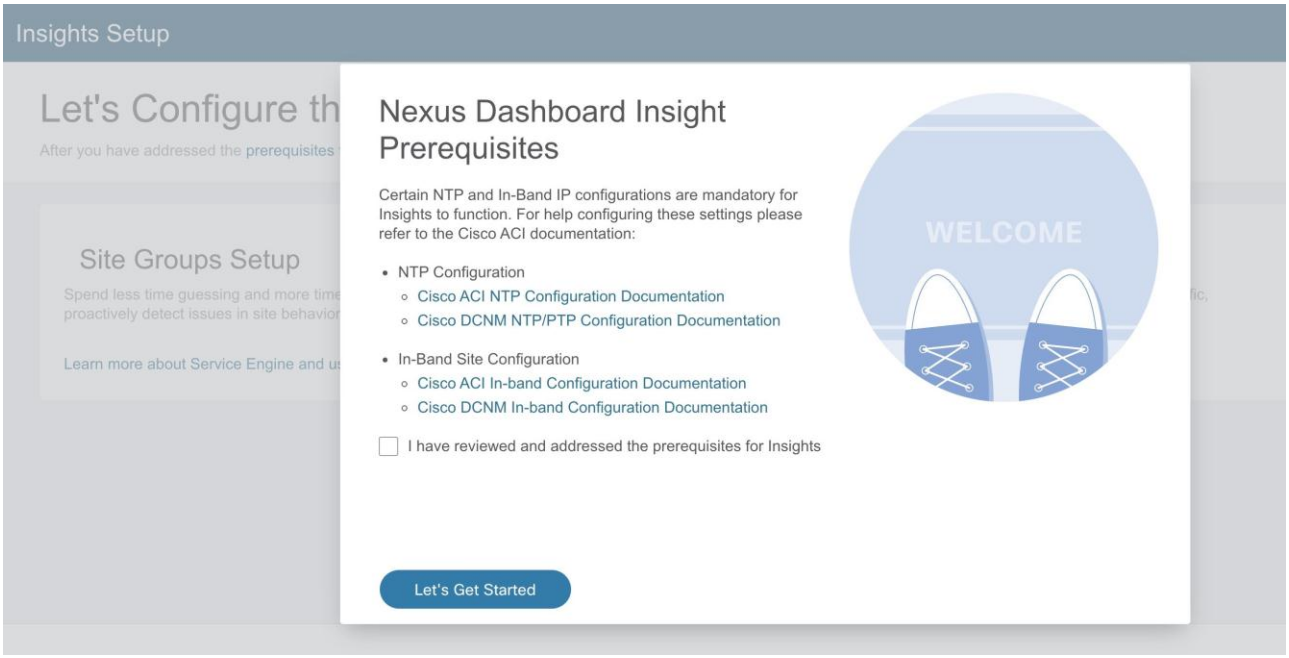
Cisco Nexus Dashboard Insights 0 日目のセットアップの基本設定

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]**領域で、**[サイトグループの設定]**をクリックします。



2. **[Nexus Dashboard Insights の前提条件]**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。



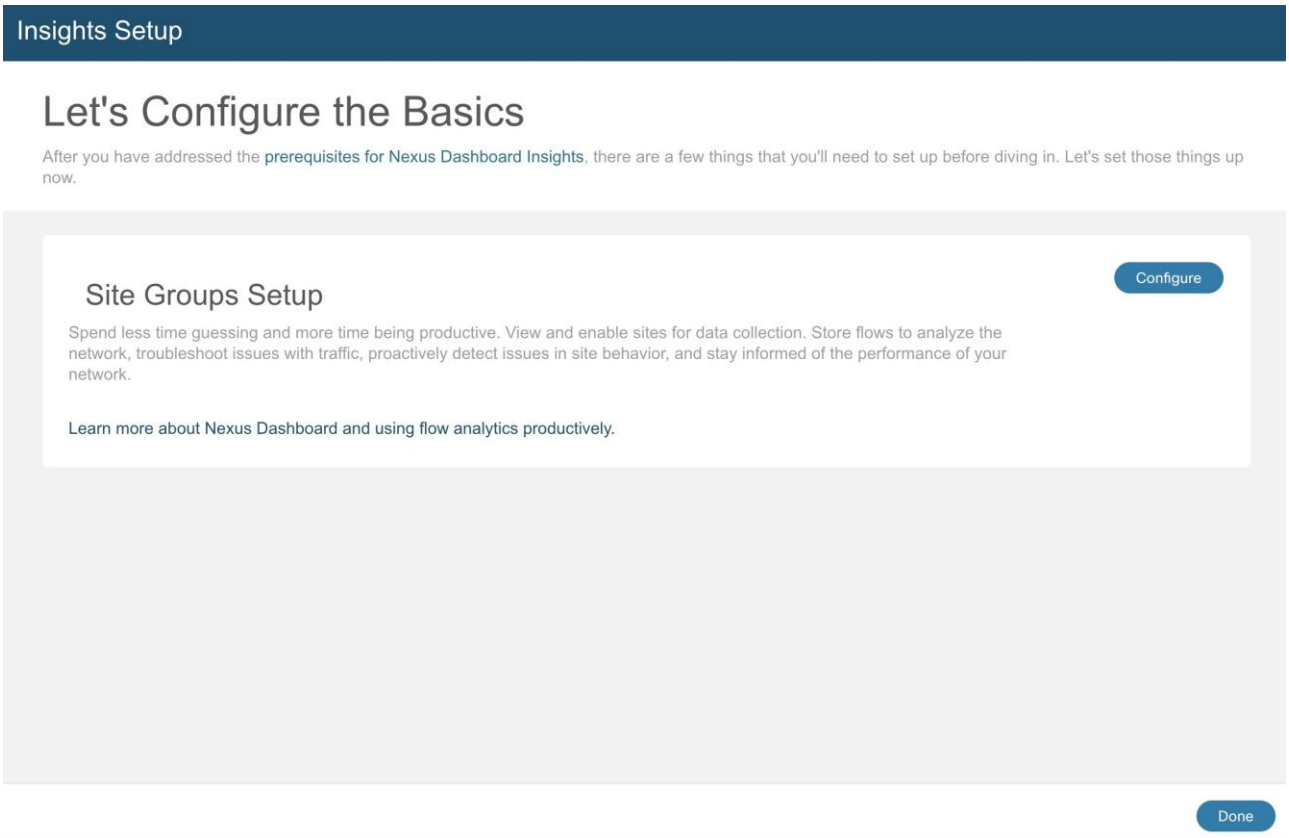
必須設定の設定に関するサポートが必要な場合は、ドキュメントリンクを参照してください。

a. NTP Configuration for Cisco DCNM Cisco DCNM NTP/PTP Configuration Documentation

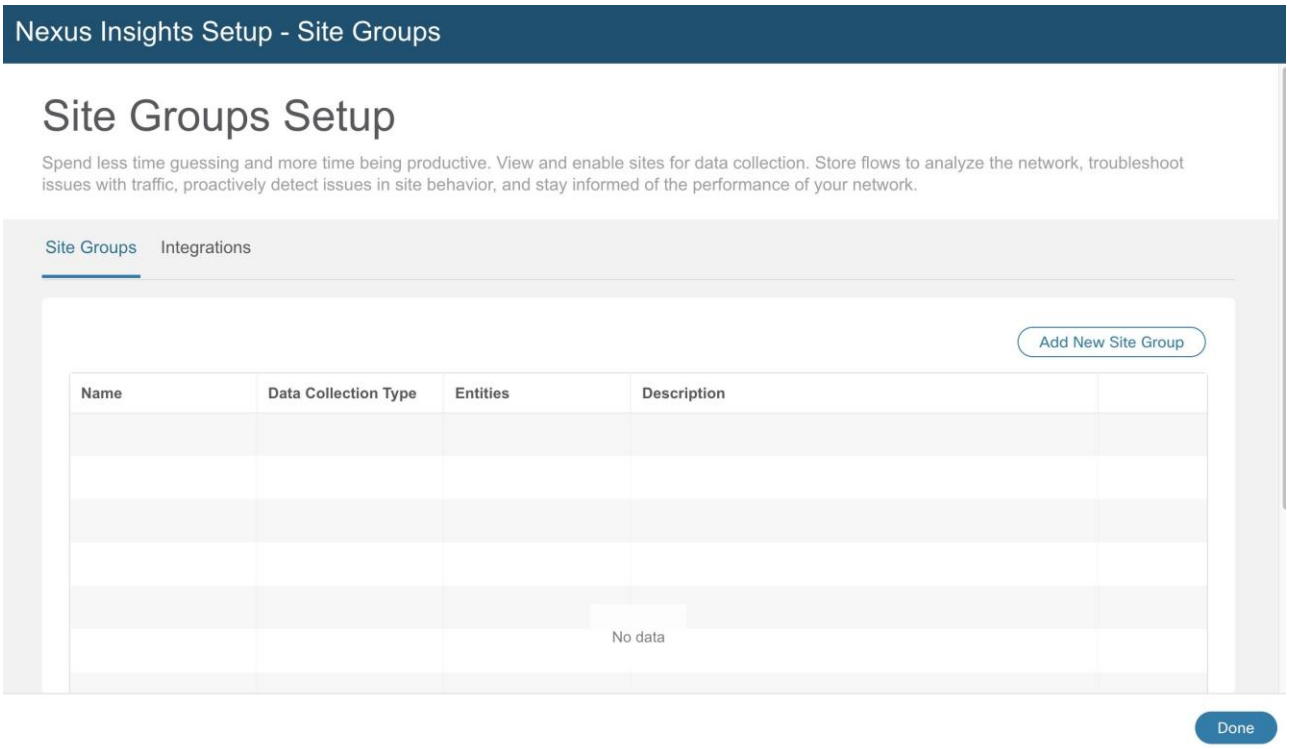
b. Cisco DCNM のインバンドサイト設定 Cisco DCNM インバンド設定に関するマニュアル

c. **[Cisco Nexus Dashboard Insights の前提条件を確認して対処しました]**チェックボックスをオンにして、**[開始]**をクリックします。

3. **[基本設定]**ページの**[サイトグループのセットアップ]**領域で、**[設定]**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。



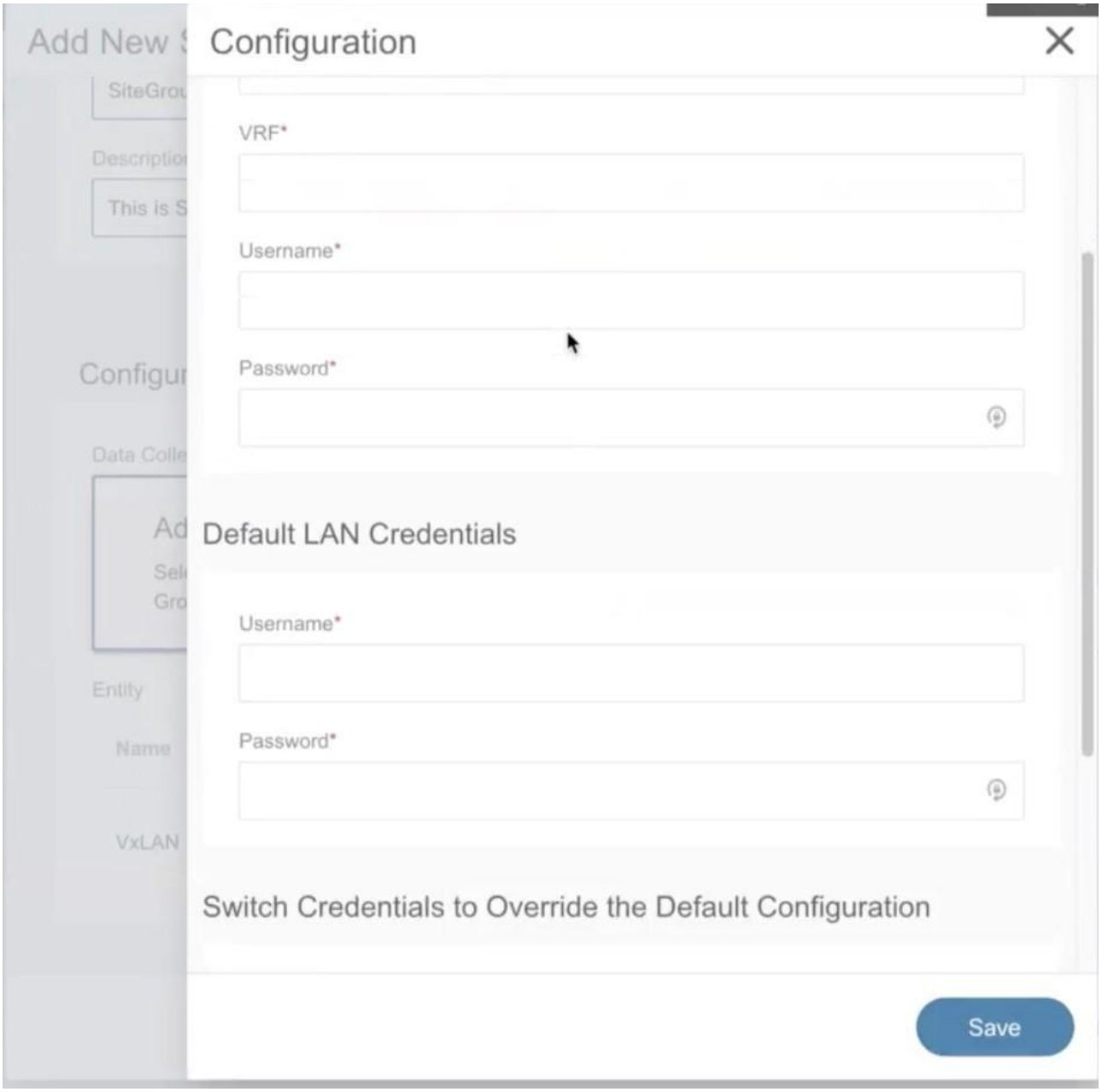
4. **[サイトグループのセットアップ]**領域で、**[新しいサイトグループの追加]**をクリックします。



5. **[新しいサイトグループの追加]**ダイアログボックスの**[全般]**領域で、サイトグループの名前と説明を追加します。
6. **[設定]**領域の**[データ収集タイプ]**領域で、**[サイトの追加]**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]**領域で、**[メンバーの追加]**をクリックし、**[メンバーの選択]**をクリックします。
8. **[サイトの選択]**ダイアログボックスから適切なサイトを選択し、**[選択]**をクリックします。

   [新しいサイトグループの追加]ダイアログボックスで、追加したサイトが**[エンティティ]**領域テーブルに表示されます。

9. **[設定]**列で**[設定]**をクリックします。
10. **[設定]**ダイアログボックスの**[一般設定]**領域で、次の操作を実行します。



a. **[ファブリックタイプ]**フィールドで、適切なオプションを選択します。**[Classic]**、**[VXLAN]**または**[SR-MPLS]**の選択肢があります。

これは、Nexus Dashboard Insights リリース 6.1.1 の**ベータ**機能です。**[ファブリックタイプ]**フィールドでは、**[SR-MPLS]**オプションも使用できます。NX-OS ファブリックで SR-MPLS のフローを設定するには、このオプションを選択します。詳細については、「SR-MPLS フロー - ベータ機能」を参照してください。

a. **[ループバック]**フィールドに、インターフェイス ID を入力します。Cisco Nexus Dashboard インバンド IP アドレスを入力します。これは、ノードが Cisco Nexus Dashboard に接続するための論理インターフェイスです。

b. **[VRF]**フィールドに、適切な VRF 名を入力します。

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

d. **[ユーザー名]**フィールドと**[パスワード]**フィールドに、読み取り/書き込み権限を持つ管理者として、DCNM のユーザー名とパスワードを入力します。

11. **[デフォルト LAN クレデンシャル]**領域の**[ユーザー名]**および**[パスワード]**フィールドに、スイッチの管理者として、LAN ユーザー名と LAN パスワードを入力します。

> リストにスイッチを追加し、スイッチのクレデンシャルが上記のデフォルトのクレデンシャルと一致しない場合にのみ、それらのスイッチのクレデンシャルをその下で指定します。

12. **[デフォルト設定を上書きするスイッチクレデンシャル]**領域で、**[スイッチクレデンシャルの追加]**をクリックし、**[スイッチクレデンシャル]**領域で、適切なスイッチに関する次の情報を追加します。
    a. **[スイッチ名]**フィールドに、スイッチの名前を入力します。
    b. **[スイッチ IP]**フィールドに、スイッチの IP アドレスを入力します。
    c. **[スイッチユーザー名]**フィールドに、スイッチのユーザー名を入力します。
    d. **[スイッチパスワード]**フィールドに、パスワードを入力します。
    e. チェックマークをオンにしてエントリを追加し、必要に応じてスイッチを追加します。
13. **[保存（Save）]** をクリックします。
14. **[新しいサイトグループの追加]**ダイアログボックスで、サイトの**[ステータス]**列の**[有効にする]**を選択します。
15. サイトのチェックマークをオンにして、設定を完了します。

    サイトグループにサイトを追加するには、**[エンティティ]**領域の**[メンバーの追加]**をクリックして、前の一連の手順を繰り返します。

16. **[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。

17. **[サイトグループのセットアップ]**領域で、**[完了]**をクリックします。
18. **[基本設定]**ページで、**[完了]**をクリックします。

サイトグループのタブを有効にして設定するには、次のタスクに進みます。

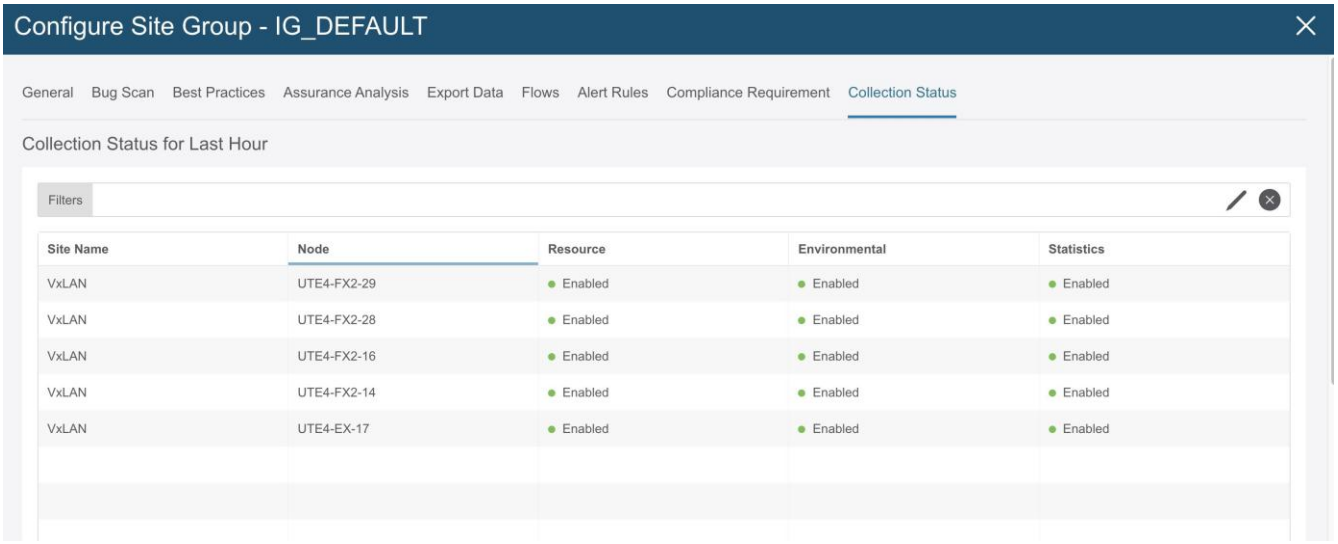
[サイトグループ]タブの有効化または設定

[概要]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]メニューをクリックし、**[サイトグループの設定]**を選択します。**[サイトグループの設定]**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]**タブ: 詳細については、「バグスキャン」を参照してください。
- **[ベストプラクティス]**タブ: 詳細については、「ベストプラクティス」を参照してください。
- **[アシュアランス分析]**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」、および「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。

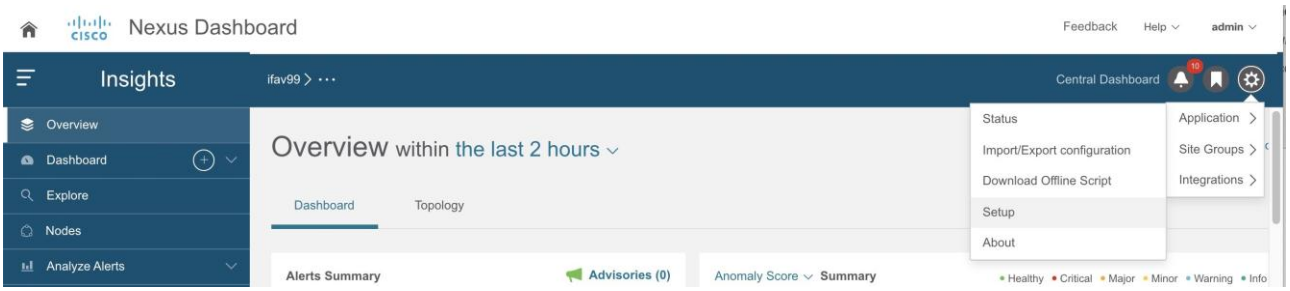
- **[データのエクスポート]**タブ: 詳細については、「データのエクスポート」を参照してください。
- **[フロー]**タブ: 詳細については、「フロー」を参照してください。
- **[アラートルール]**タブ: 詳細については、「アラートルール」を参照してください。
- **[収集ステータス]**タブ: サイト名、ノード、リソース、環境、統計情報、フロー、エンドポイント、イベントなどのステータスチェックを表示するテレメトリデータが表示されます。次の例のページを参照してください。



Cisco Nexus Dashboard Insights N 日目のセットアップの基本設定

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]** > **[セットアップ]**をクリックします。



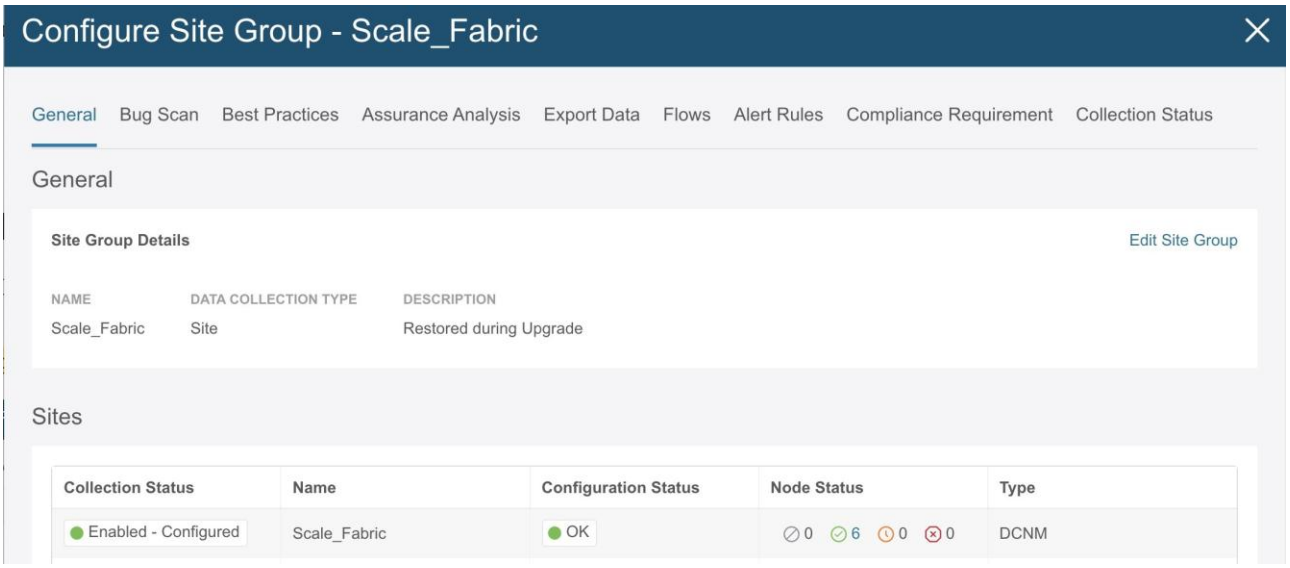
3. **[基本設定]**ページで、**[Cisco Nexus Dashboard Insights の前提条件をクリック]**リンクをクリックし、必須設定が設定されていることを確認します。
4. 確認後、必要に応じて、**[Cisco Nexus Dashboard Insights の前提条件を確認して対処しました]**チェックボックスをオンにして、**[開始]**をクリックします。
5. **[サイトグループのセットアップ]**領域で、**[設定の編集]**をクリックし、**[サイトグループのセットアップ]**領域で、サイトグループが期待どおりに表示されていることを確認します。

サイトグループを編集する場合は、[アクション]メニュー > **[サイトグループの編集]**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] をクリックします。

Nexus Dashboard Insights のスイッチ設定ステータス

1. **[概要]**ページの上部で、選択したサイトグループの横にある[アクション]メニューをクリックし、**[サイトグループの設定]**をクリックします。
2. **[サイトグループの設定]**ページの**[サイト]**領域テーブルに、オンボーディングされたサイトが表示されます。

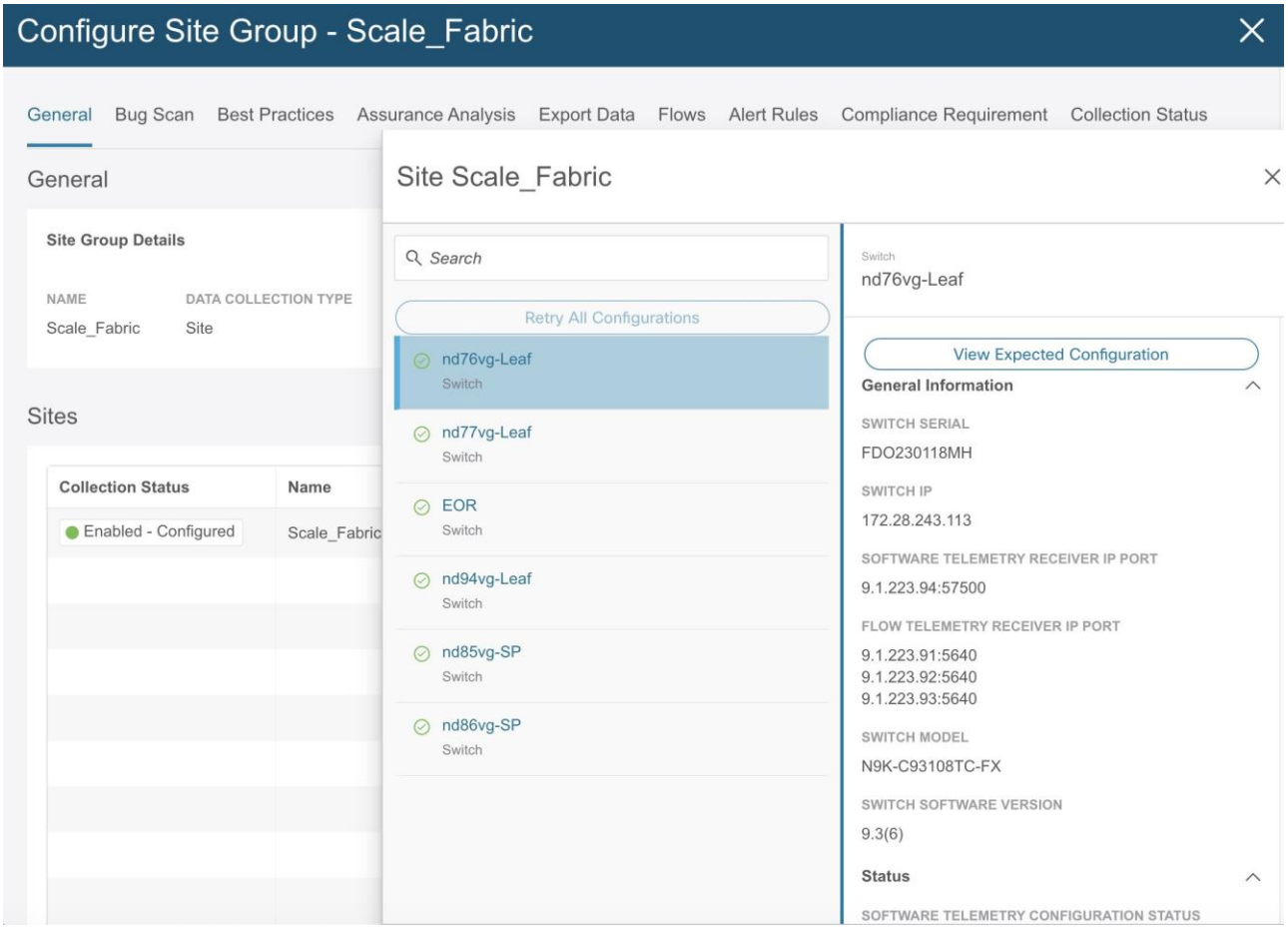


3. **[ノードステータス]**列に表示されている値をダブルクリックして、オンボーディングされたスイッチの設定、ステータス、および追加の詳細を表示します。

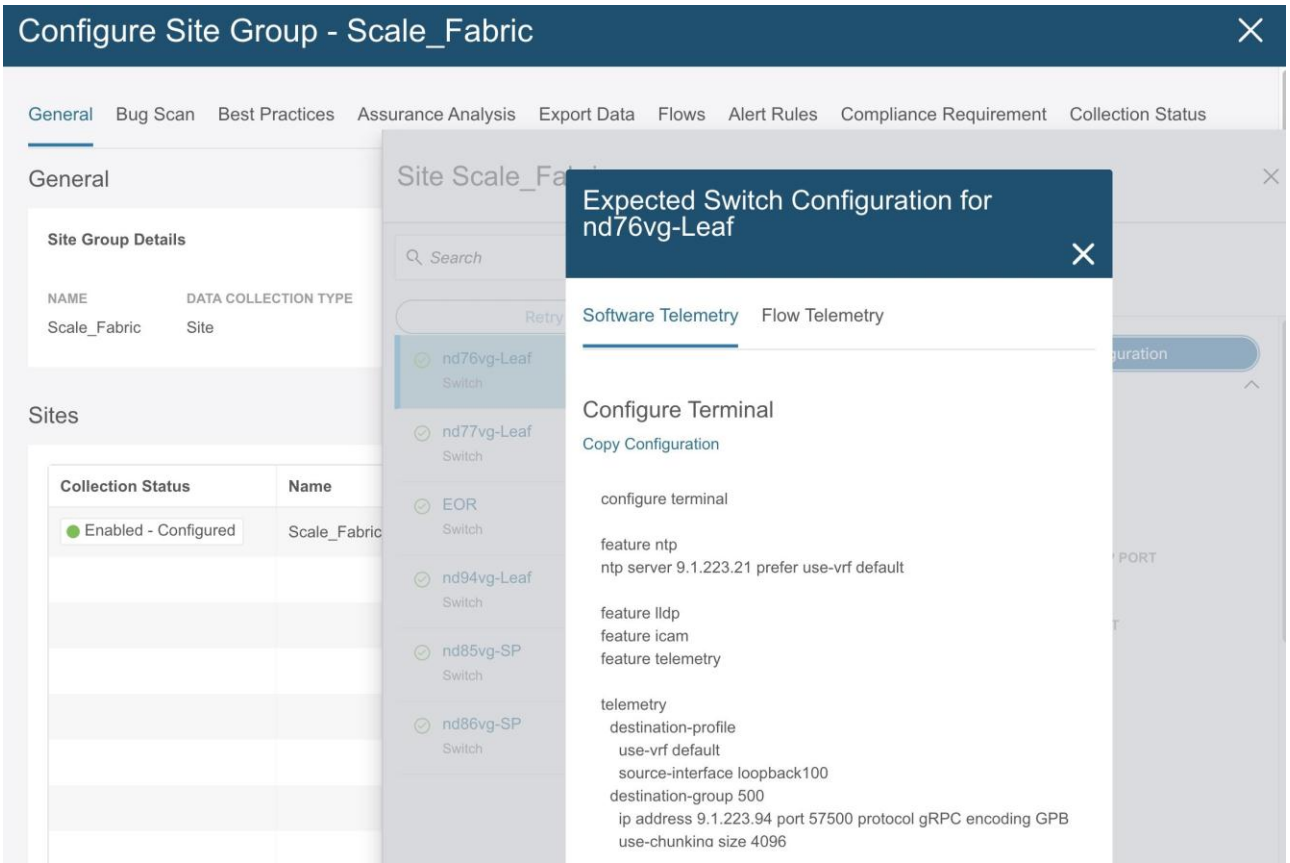
スイッチのステータスには次のものが含まれます。

- **グレー** - ノードは初期状態で未設定です。
- **緑** - ノードは正常に設定されています。
- **オレンジ** - ノードは現在設定中です。
- **赤** - ノードの設定に失敗しました。

注: サイトのテレメトリ構成を有効にしたときに、レッド カウントが 0 より大きい場合、これは、サイトを有効または無効にするために開始された操作が成功しなかったことを意味します。
[カウント]をクリックし、[再試行]をクリックして構成をノードに再度プッシュします。
[Any Counts]をクリックして、予想される構成を表示します。
{CiscoNIRFullName} セットアップページを終了して、ページをすぐに更新するために戻ることができます。



4. スイッチを選択し、**[予想される設定の表示]**をクリックすると、**[予想される設定]**領域に予想されるスイッチ設定の詳細が表示されます。



ユーザーは、推奨設定を使用して適切なスイッチを設定する必要があります。**[予想される設定]**領域から、**[ソフトウェアテレメトリ]**および**[フローテレメトリ]**の下にある設定を表示およびコピーできます。詳細については、「フローの設定」を参照してください。

注意事項と制約事項

Cisco Nexus Dashboard Insights サービスのリリース 6.0.1 では、ACI サイトと DCNM サイトの両方を検出できます。

デバイス コネクタについて

Cisco Nexus Dashboard Insights 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。

概説

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]：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]：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]：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]：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]：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。

[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]：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]：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]：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]：分析 - 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]：分析 - 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。

[変更管理]：この領域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。

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]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]メニューをクリックし、**[サイトグループの設定]**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]メニュー > **[追加]** > **[コンプライアンス要件]**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]メニュー > **[追加]** > **[アラートルール]**をクリックします。

[ヘルプセンター]：**[集中ダッシュボード]**、**[通知]**、**[ブックマーク]**、および**[設定]**アイコンの上に、**[ヘルプ]**ドロップダウンメニューがあります。**[ヘルプ]** > **[ヘルプセンター]**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]**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]ページに移動します。

[通知]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て保存して、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。

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]、[環境の参照]、[統計情報の参照]、[ダッシュボード]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]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]**、**[サイトグループ]**、**[統合]**が表示されます。

[アプリケーション]アイコンをクリックすると、**[ステータス]**、**[設定のインポート/エクスポート]**、**[オフラインスクリプトのダウンロード]**、**[セットアップ]**、**[バージョン情報]**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]：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]アイコンをクリックすると、**[サイトグループの管理]**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]アイコンをクリックすると、**[統合の管理]**または**[統合の追加]**を選択できます。詳細については、「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]**ページを表示すると、**[ダッシュボード]**タブと**[トポロジ]**タブがあります。

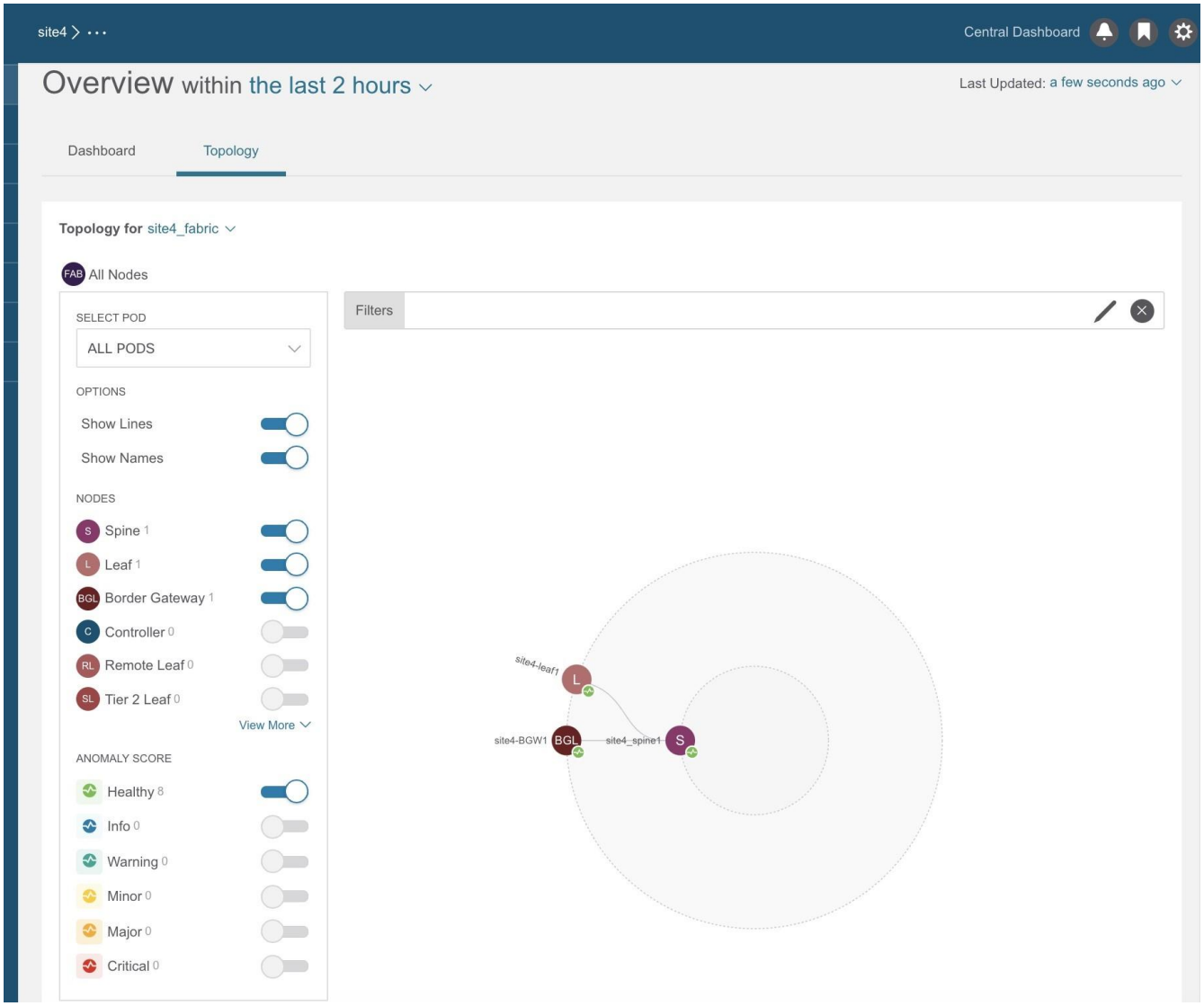
[ダッシュボード] タブ

Nexus Dashboard Insights ダッシュボードビューには、[アラートの概要]、[異常スコア]、[アラート検出タイムライン]、[異常の内訳]、[アドバイザリの内訳]、[異常スコア別の上位ノード]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 のトポロジビューでは、選択したサイトグループについて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]**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。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]**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]** > **[ユーザー設定]**を選択します。
3. **[ユーザー設定]**ページの**[タイムゾーン]**領域では、デフォルトのタイムゾーン値として**[自動]** 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]**フィールドで、**[手動]**を選択します。
5. **[最寄りの都市]**フィールドに、希望する都市を入力して、**[タイムゾーン]**フィールドに適切なタイムゾーンを入力します。

   または、地図内の選択した都市にピンをドラッグすると、**[最寄りの都市]**と**[タイムゾーン]**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

作業ウィンドウの**[概要]**ページには、**[ダッシュボード]**タブと**[トポロジ]**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]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。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。

サイト内の各ノードは、テレメトリデータとイベントを Nexus Dashboard Insights のサービスにストリーミングし、データを分析して異常を検出します。ダッシュボードには関連情報が表示されます。

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
- ソフトウェアのアップグレードパスとアップグレードの影響

メインダッシュボードからは、ネットワークで発生している異常にすぐにアクセスできます。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逸脱であり、タイプと重大度別に表示されます。リソース使用率、環境、およびインターフェイスレベルのエラーなどが異常の対象となり、重大度に基づいて色分けされます。

- 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

[異常スコア]の[概要]領域にはノードの総数が表示されます。設定によって表示が異なる場合があります。DCNM VXLAN サイトの場合、内訳には**リーフノード**と**スパインノード**が表示されます。DCNM クラシックサイトの場合、内訳には**ノード**のみが表示されます。

このページでは、**[重大度別の異常の内訳]**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]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 • アプリケーション • 環境 • 統計 • エンドポイント • 接続の分析 • バグ
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。領域をクリックすると、**[ノード]**や**[異常スコア]**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
コントローラ合計数	ネットワーク内のコントローラの総数を表示します。
スイッチ総数	ネットワーク内のスイッチの総数を表示します。
[重要 | 中程度 | 正常]デバイス	次のいずれかのカテゴリにあると判断されたデバイスの総数を表示します。 • 重要なデバイス • 中程度のデバイス • 正常なデバイス数 上位カテゴリ([重要]が最も高い)のデバイス数が、表示された数に表示されます。現時点で[重要]カテゴリにあるデバイスがない場合は、[中程度]カテゴリのデバイス数が表示されます。どのデバイスでも問題が検出されない場合は、[正常]カテゴリのデバイス数が表示されます。
アドバイザリ	ネットワーク内のソフトウェアとハードウェアに対して配信されたアドバイザリの総数を表示します。

プロパティ	説明
重大度別の問題	ネットワーク内のソフトウェアとハードウェアに配信された問題(異常、バグ、PSIRT 通知)の総数を表示します。

[カテゴリ別異常]および**[カテゴリ別アドバイザリ]**から任意のプロパティをクリックして、*[アラートの分析]*作業ウィンドウにアクセスします。

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。
ノード	異常のあるサイトのノードの総数を表示します。 注: DCNM 設定によっては、単一の**ノード**数、または**リーフノード**と**スパインノード**の内訳が表示される場合があります。

- 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。
- ノード番号をクリックすると、個々のノードの詳細が表示されます。

[トポロジ]タブ

Cisco Nexus Dashboard Insights ダッシュボードでは、サイト内の異常があるすべてのノードのトポロジビューにアクセスできます。

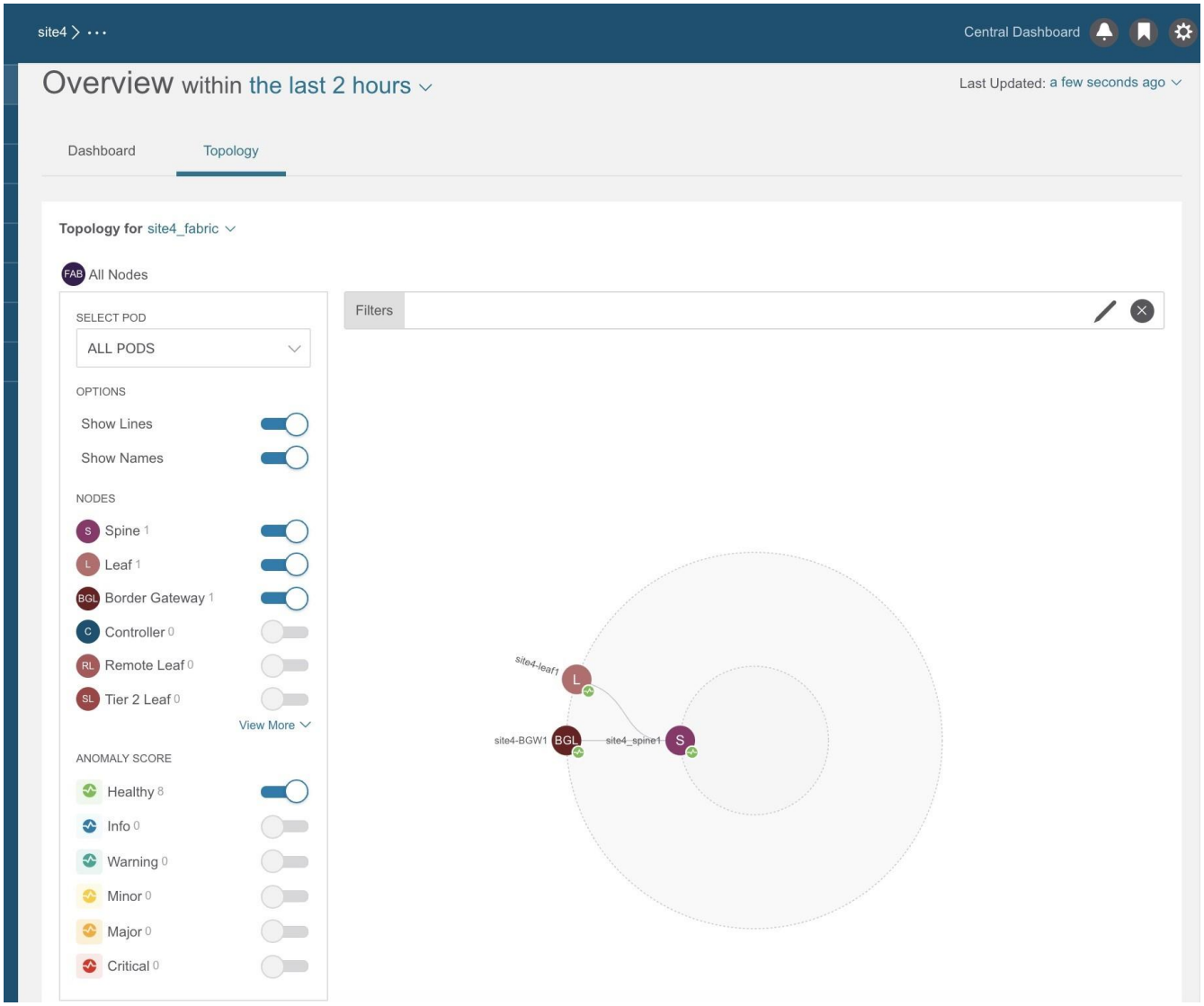
右側のダッシュボードペインで、**[サイトダッシュボード]** > **[トポロジ]**タブをクリックします。

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ビューについては、**[概要]**ページで、作業ウィンドウの**[概要]**領域を表示します。**[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異常を表示、並べ替え、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。
- [VRF] - 特定の VRF から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。サイドパネルには、ノードの一般的な追加の異常の詳細が表示されます。

[トポロジ]タブの制限事項

LLDP 情報がないノードは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]**ページの作業ウィンドウ、**[ダッシュボード]**タブ、**[アラート検出タイムライン]**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

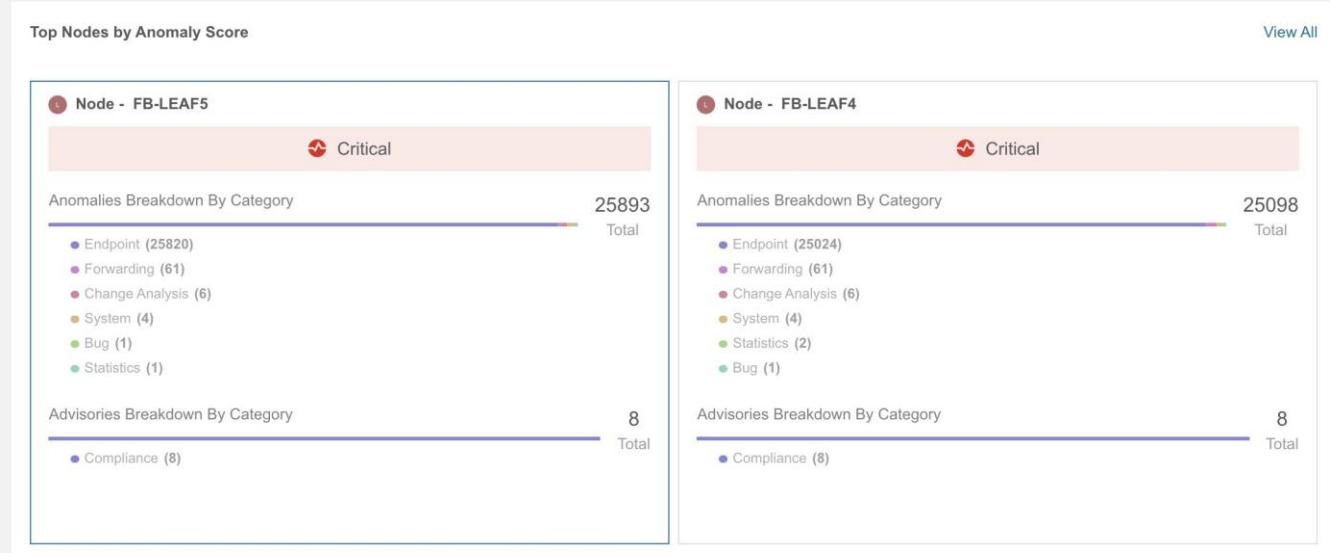
- 色付きの丸いドットは、ノードのイベント、障害、および監査ログに対応しています。
- タイムラインの周りにある複数のリングは、オブジェクトのグループを表します。タイムライン内の単独のリングは、単一のオブジェクトを表します。
- ハートのアイコンは、異常のみを表します。青い円は、現在選択されている異常を示します。

異常スコア別上位ノード

[概要]ページの作業ウィンドウの**[ダッシュボード]**タブに、**[異常スコア別上位ノード]**領域が表示されます。

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]*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]*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]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最悪のケースです。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。

注意事項と制約事項

- デバイスコネクタがオンプレミスの GUI Nexus Dashboard Insights から要求されていない場合、ログコレクタの接続された TAC 機能が機能するには、デバイスコネクタが Intersight から要求されていない必要があります。
- Cisco DCNM では、network-admin および network-operator ロールが特定のファブリックに読み取りまたは書き込みアクセスを割り当てることができます。Cisco Nexus Dashboard Insights は、アクセス権が付与されているファブリックのみを表示します。
- Nexus Dashboard Insights では、Cisco DCNM での RBAC ロールは許可されません。
- Telemetry Manager/Policy Gateway では、Cisco DCNM のサイトモードの変更(管理対象モードからモニターモードへの変更、またはその逆)を検出するのに約 10 分かかります。
- Nexus Dashboard Insights を介して監視対象サイトでテレメトリを有効にするには、まず監視対象サイトのすべてのノードで既存のテレメトリ設定をすべて削除し、その後 Nexus Dashboard Insights からこのサイトを有効にする必要があります。次に、テレメトリによって受信側の IP アドレスがこれらのノードに割り当てられ、[データ収集のセットアップ]ページに表示されます。ノードは監視対象であるため、テレメトリ設定がノードにテレメトリ設定をプッシュすることはありません。したがって、[データ収集のセットアップ]ページから受信者の IP アドレスを確認し、ノードを手動で設定する必要があります。
- 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。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。
- 1 つ以上のサイトが無効状態から回復しない場合は、Cisco Nexus Dashboard で Nexus Dashboard Insights を停止して再起動する必要があります。これにより、失敗した無効状態が回復します。

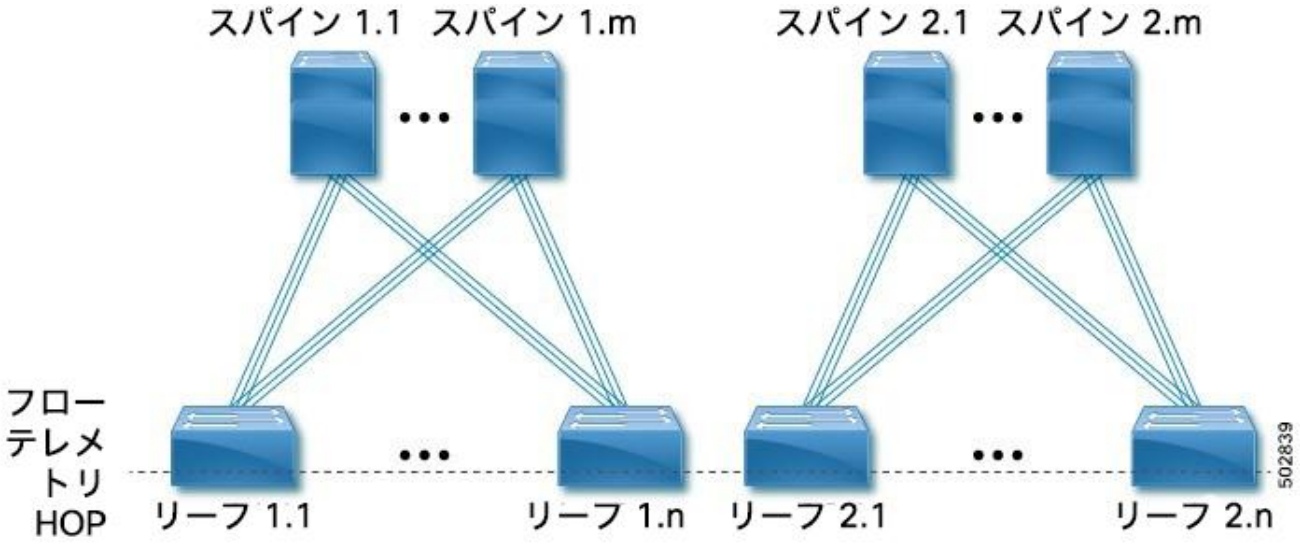
- Nexus Dashboard Insights が Cisco Nexus Dashboard で管理モードまたはモニターモードになっている場合、異なる vPC ペアの vPC ドメイン ID をファブリック全体で同じにすることはできません。
- Cisco Nexus 7000 スイッチは、デフォルト VDC のソフトウェアテレメトリのみをサポートします。デフォルト VDC にモジュールとインターフェイスがない場合、ソフトウェアテレメトリを有効にできません。
- Nexus Dashboard Insights フローパススティッチングが機能し、正しい VNI 情報を表示するには、すべてのリーフスイッチ、ボーダーリーフ、およびボーダーゲートウェイでレイヤー2 VNI スイッチ仮想インターフェイスを作成する必要があります。この対称設定は、転送時には必要ないかもしれませんが、Nexus Dashboard Insights がファブリック情報を取得するために必要になります。
- すべてのホスト側 VLAN に対してスイッチ仮想インターフェイスを設定する必要があります。これにより、Nexus Dashboard Insights は、ルーティングされたフローまたはブリッジされたフローを問わず、対応する VNI を見つけることができます。
- 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。
- 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。

Cisco Nexus Dashboard Insights のトポロジ

Cisco DCNM の Nexus Dashboard Insights は、次のトポロジをサポートします。

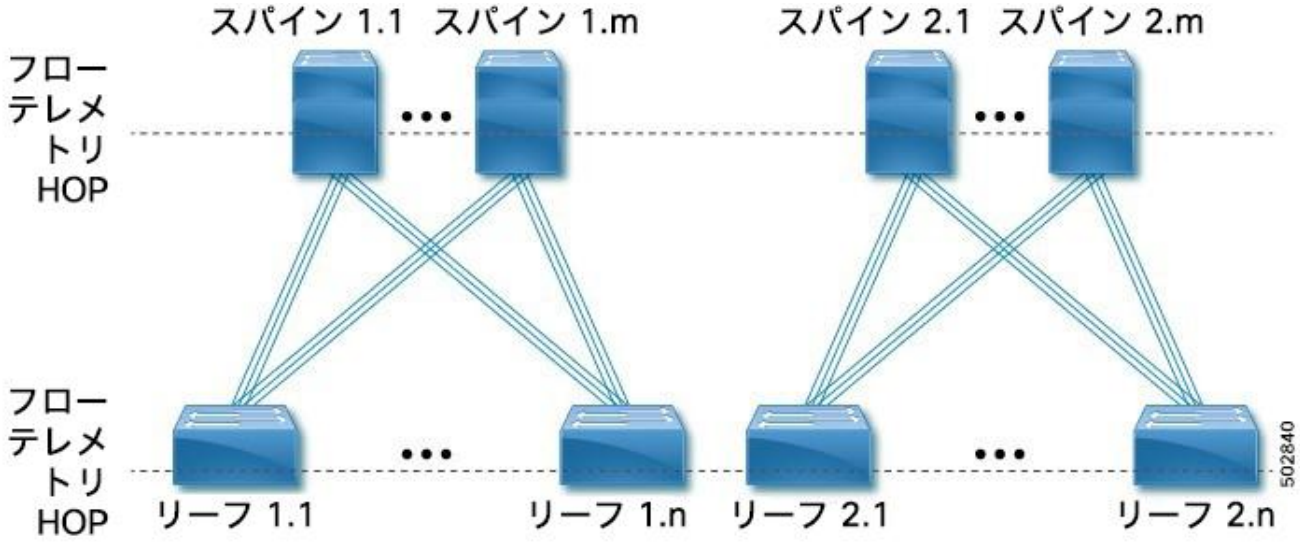
- 2-HOP および 3-HOP フローテレメトリ相関用のリーフスイッチ - スパインスイッチ。
- 3-HOP および 4-HOP フローテレメトリ相関用のリーフスイッチ - スパインスイッチ - スーパースパインスイッチ。

次の図は、2-HOP フローテレメトリ相関用のリーフスイッチ - スパインスイッチのトポロジを示しています。



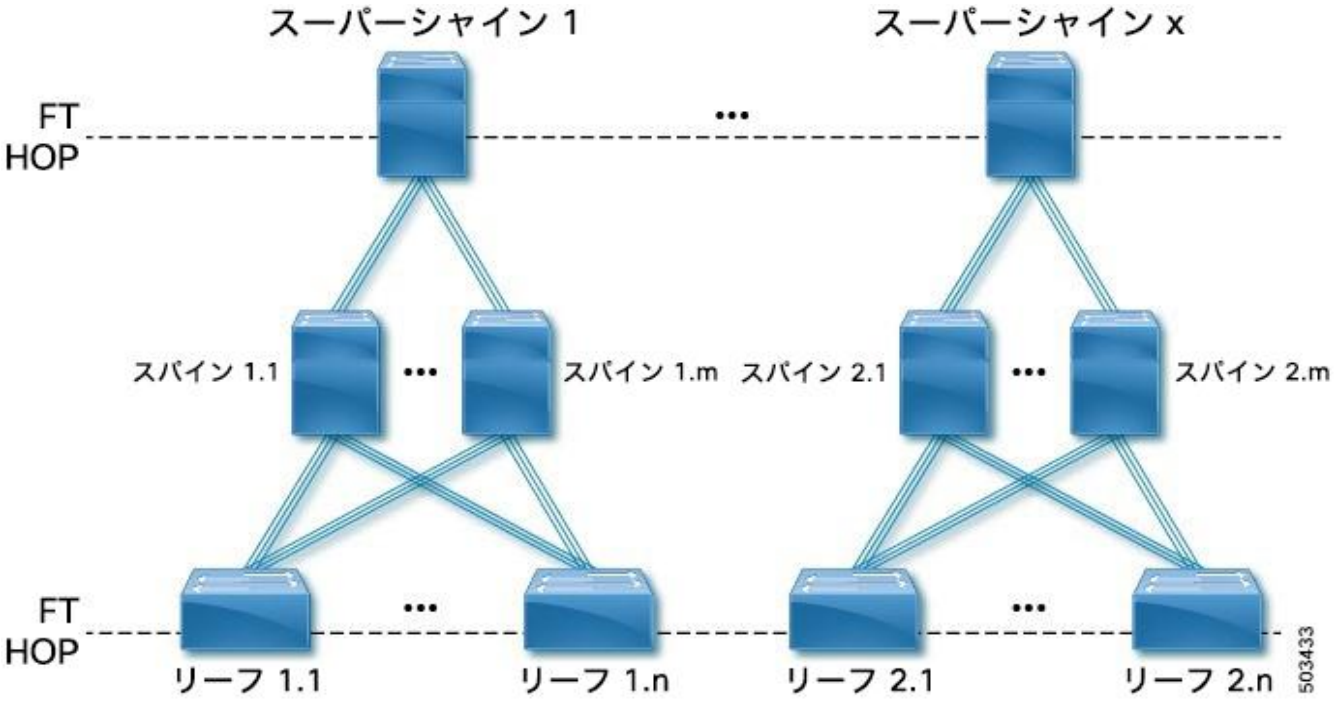
図のすべてのスイッチと交差するフローテレメトリ HOP ラインは、フローテレメトリデータをエクスポートできるスイッチを表します。例: フローテレメトリ HOP ラインでは、リーフ 1.1 からリーフ 1.n へのパケットフローは 2 つのフローテレメトリホップと見なされます。

次の図は、3-HOP フローテレメトリ相関用のリーフスイッチ - スパインスイッチのトポロジを示しています。



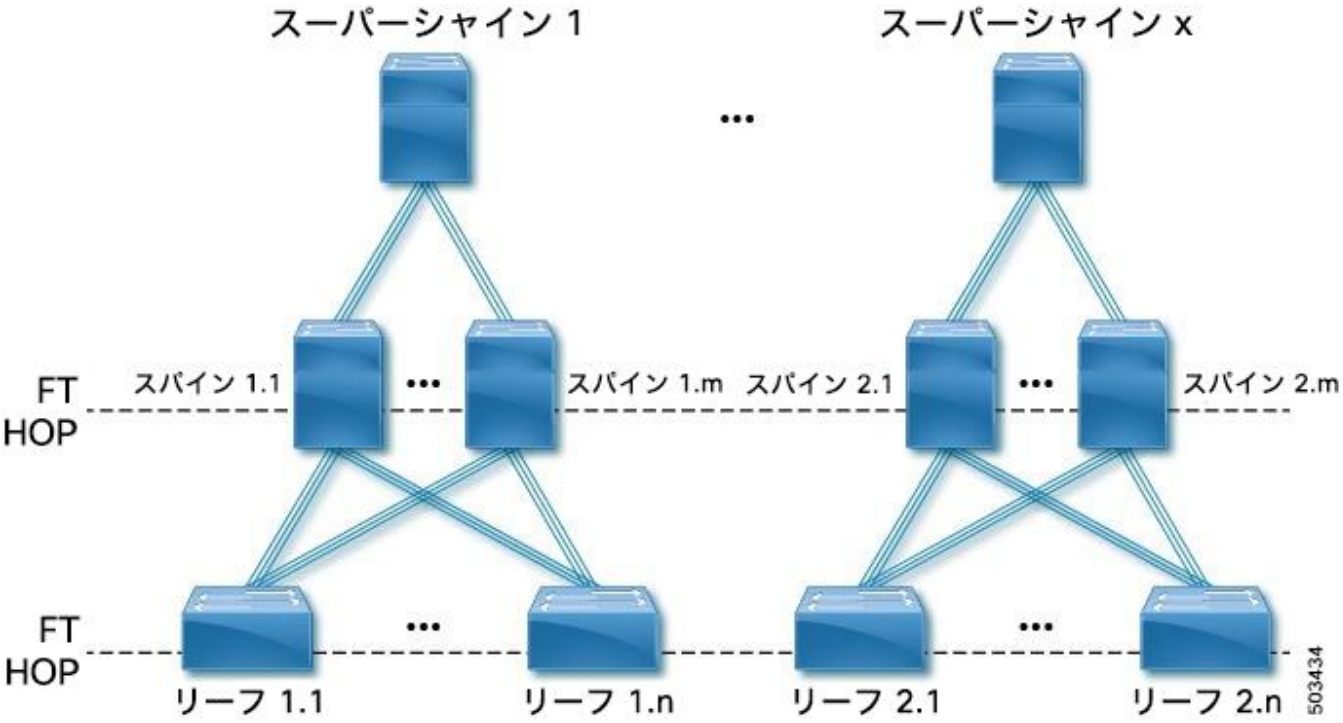
図のすべてのスイッチと交差するフローテレメトリ HOP ラインは、フローテレメトリデータをエクスポートできるスイッチを表します。例: 2 つのフローテレメトリ HOP ラインがある場合、リーフ 1.1 からスパイン 1.1 へ移動し、次にリーフ 1.n に移動するパケットフローは、3 つのフローテレメトリホップと見なされます。

次の図は、3-HOP フローテレメトリ相関用のリーフスイッチ - スパインスイッチ - スーパースパインスイッチを示しています。



図のすべてのスイッチと交差するフローテレメトリ HOP ラインは、フローテレメトリデータをエクスポートできるスイッチを表します。例: リーフ 1.1 からスーパースパイン-1 へ移動し、次にリーフ 1.n に移動するパケットフローは、3 つのフローテレメトリホップと見なされます。

次の図は、4-HOP フローテレメトリ相関用のリーフスイッチ - スパインスイッチ - スーパースパインスイッチを示しています。



図のすべてのスイッチと交差するフローテレメトリ HOP ラインは、フローテレメトリデータをエクスポートできるスイッチを表します。例: 2 つのフローテレメトリ HOP ラインがある場合、リーフ 1.1 からスパイン 1.1 へ移動し、次にスパイン 1.m からリーフ 1.n へと移動するパケットフローは、4 つのフローテレメトリホップと見なされます。

サポートされているシナリオ

Nexus Dashboard Insights トポロジは、次のシナリオをサポートします。

VXLAN

- リーフスイッチの vPC
- ボーダースパインスイッチ
- ボーダーリーフスイッチ
- IR またはマルチキャストアンダーレイ
- EBGP または IBGP
- IPv4 アンダーレイ
- IPv4 または IPv6 オーバーレイ

レガシー/クラシック LAN

- リーフスイッチの vPC
- IPv4 または IPv6

サポートされるロール

Nexus Dashboard Insights トポロジは、次のロールをサポートします。

VXLAN とクラシック LAN

- リーフスイッチ
- ボーダースイッチ
- アクセス
- スパインスイッチ
- ボーダースパインスイッチ
- 集約
- スパインスイッチのボーダーゲートウェイ
- スーパースパインスイッチ
- ボーダー スーパースパイン スイッチ
- コア ルータ
- エッジ ルータ
- ボーダー ゲートウェイ スーパースパイン スイッチ

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、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する方法、サイトグループの一部であるファイルをアップロードして分析する方法のいずれかです。

- 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する

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ファイルをアップロードし、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

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、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 で利用可能な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]**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]**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。

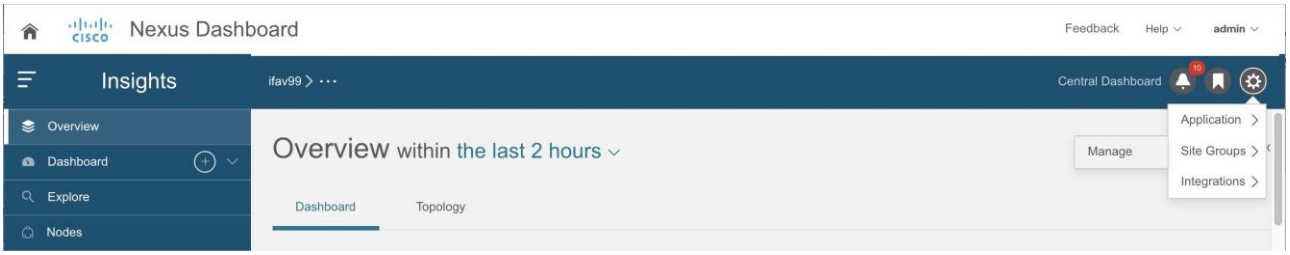
Cisco Nexus Dashboard Insights にサイトグループがまだ作成されていない場合、サービスを開始すると**[有効なサイトグループがありません]**ページが表示されます。**[サイトグループの設定]**タブをクリックし、以下の手順に従います。Cisco Nexus Dashboard Insights を開始したときにサイトグループがすでに設定されている場合は、**[概要]**ページが表示されます。

> SR-MPLS フロー(ベータ機能)を使用するようにサイトグループを設定している場合、以下の手順で**[ファブリックタイプ]**フィールドを設定するときに、**[SR-MPLS]**を選択する必要があります。詳細については、Cisco Nexus Dashboard Insights の「Cisco Nexus Dashboard Insights 0 日目のセットアップの基本設定」および「SR-MPLS フロー - ベータ機能」を参照してください。

手順

次の手順に従って、サイトグループにサイトを追加します。

1. **[概要]**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]アイコン > **[サイトグループ]** > **[管理]**をクリックします。



3. **[サイトグループの管理]**ページで、**[新しいサイトグループの追加]**をクリックします。
4. **[新しいサイトグループの追加]**ダイアログボックスの**[全般]**領域で、サイトグループの名前と説明を追加します。
5. **[設定]**領域の**[データ収集タイプ]**領域で、**[サイトの追加]**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]**領域で、**[メンバーの選択]**をクリックします。
7. **[サイトの選択]**ダイアログボックスから適切なサイトを選択し、**[選択]**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]**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]**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

サイトがサイトグループに追加されます。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]**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]メニューをクリックし、**[サイトグループの設定]**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]**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]**ダイアログボックスで、**[状態]**フィールドを**[有効]**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. **[サイトグループの設定]**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]**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]**タブの**[今すぐ実行]**ボタンをクリックして、そのサイトの 1 回限りのインスタント分析を実行できます。

オフラインスクリプト

Cisco Nexus Dashboard Insights の**[概要]**ページで、[設定]アイコン > **[オフライン収集スクリプトのダウンロード]**をクリックして、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。

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

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。DCNM 用の Nexus Dashboard Insights データ収集スクリプトは、アウトオブバンド管理接続のみをサポートします。REST API 呼び出しと CLI 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 DCNM、スパインスイッチ、リーフスイッチか

ら収集されたオブジェクトと show コマンドの完全なリストがあります。readme.md ファイルは、スクリプトファイルと同じ zip ファイル内にあります。スクリプトは、Nexus Dashboard Insights の設定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 ACI 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 DCNM 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 と 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。設定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 6.0.1 の特定のサイトグループ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、Cisco NAE 5.1 セットアップからエクスポートされた設定ファイルが必要です。

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]領域の**[概要]**ページに表示されます。

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]**ページに移動します。**[ノード]**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)

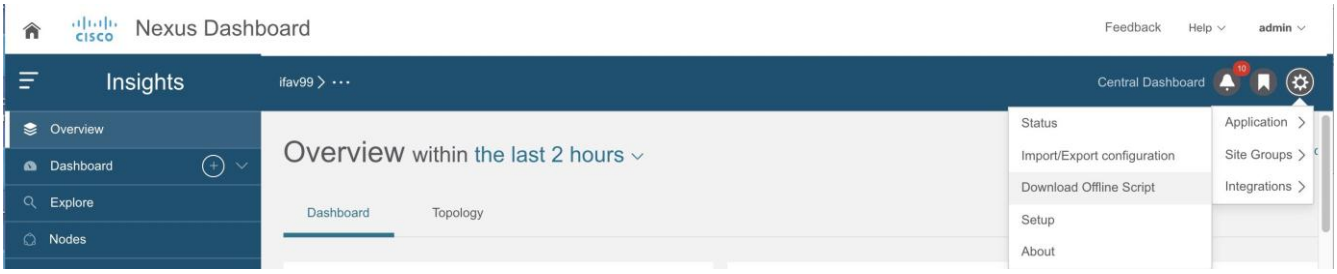
サイトグループへのファイルのアップロードとアシュアランス分析の実行

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**ファイルのアップロード**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]**ページで、[設定]アイコン > **[オフライン収集スクリプトのダウンロード]**をクリックして、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。

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。

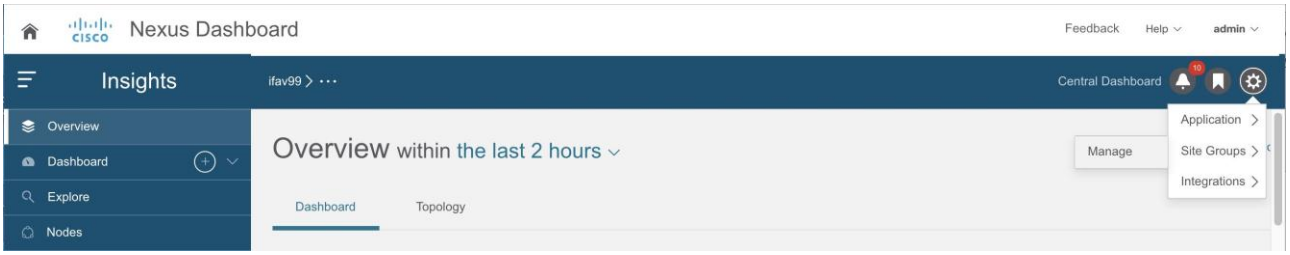
Cisco Nexus Dashboard Insights にファイルをアップロードしても、Cisco Nexus Dashboard サイトマネージャはこうしたファイルを認識しません。

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]**ページが表示されます。**[サイトグループの設定]**タブをクリックし、以下の手順に従います。Cisco Nexus Dashboard Insights サービス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]**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]アイコン > **[サイトグループ]** > **[管理]**をクリックします。



2. **[サイトグループの管理]**ページで、**[新しいサイトグループの追加]**をクリックします。
3. **[新しいサイトグループの追加]**ダイアログボックスの**[全般]**領域で、サイトグループの名前と説明を追加します。
4. **[設定]**領域の**[データ収集タイプ]**領域で、**[ファイルのアップロード]**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]**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]**領域で、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]**ページの上部で、サイトグループを選択します。
2. 選択したサイトグループの横にある[アクション]メニューをクリックし、**[サイトグループの設定]**をクリックします。
3. **[サイトグループの設定]**ページの**[全般]**タブの**[サイト]**で、ファイルの**[収集ステータス]**が有効になっていることを確認します。
4. **[アシュアランス分析]**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]**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]**ページの**[アラート検出タイムライン]**領域で、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]**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。
- **[サイトグループの設定]** > **[アシュアランス分析]**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]**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]アイコン > **[サイトグループ]** > **[管理]**をクリックします。
3. **[サイトグループの管理]**ページの**[サイトグループ]**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]メニューをクリックし、**[編集]**を選択します。
4. **[サイトグループの編集]**ページでサイトを変更し、**[保存]**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]**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]アイコン > **[サイトグループ]** > **[管理]**をクリックします。
3. **[サイトグループの管理]**ページの**[サイトグループ]**タブで、編集するサイトの右側にある[アクション]メニューをクリックし、**[編集]**を選択します。
4. **[サイトグループの編集]**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]**をクリック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]**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]メニューをクリックし、**[サイトグループの設定]**を選択します。
2. **[全般]**タブで、**[サイトグループの編集]**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]**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]**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]アイコン > **[サイトグループ]** > **[管理]**をクリックします。
3. **[サイトグループの管理]**ページの**[サイトグループ]**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]メニューをクリックし、**[削除]**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]**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]メニューをクリックし、**[サイトグループの設定]**をクリックします。
3. **[サイトグループの設定]**ページで、**[ファイル管理]**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。

- 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。スケジュールされたバグスキャンは、テクニカルサポートログの収集をトリガーします。テクニカルサポートログの収集は CPU とメモリを集中的に使用するため、スケジュールされたバグスキャンの一部としてテクニカルサポートログの収集をトリガーする前に、ノードにおける CPU とメモリの使用量のしきい値を設定できます。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とベストプラクティスは、次のスケジュールに従って実行されます。

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。既定のベストプラクティスは、月曜日の午前 5 時(バグスキャンジョブの 5 時間後)から 1 日 1 回スケジュールされています。
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。既定のベストプラクティスは、毎日バグスキャン時間の 5 時間後にスケジュールされています。このスケジュールは、5 つのサイトすべてで毎日午前 5 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	ベストプラクティスのスケジュール
サイト 1	週に 1 回、月曜日の午前 12 時に開始	1 日 1 回午前 5 時から(12+5)
サイト 2	週に 1 回、最も近い月曜日の午前 6 時に開始	1 日 1 回午前 11 時から(6+5)
サイト 3	週に 1 回、月曜日の午後 12 時に開始	1 日 1 回午後 5 時から(12+5)
サイト 4	週に 1 回、月曜日の午後 6 時に開始	1 日 1 回午後 11 時から(6+5)
サイト 5	週に 1 回、火曜日の午前 12 時に開始	1 日 1 回午前 5 時から(12+5)

注意事項と制約事項

- 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]メニューから、**[サイトグループの設定]** > **[バグスキャン]**を選択して、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]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。**[全般]**テーブルには、すべてのサイトが表示されます。

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]**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]**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]**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、**[バグスキャンステータス]**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]**をクリックしてジョブを停止します。

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]メニューから、**[サイトグループの設定]** > **[バグスキャン]**を選択して、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]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]**をクリックします。

   [履歴]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、**[バグスキャンステータス]**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]**をクリックしてジョブを停止します。

ベストプラクティス

ネットワーク上でベストプラクティスジョブをスケジュールまたは実行できます。Nexus Dashboard Insights は、サイトからテクニカルサポート情報を収集し、既知の署名セットに対してそれらを実行し、コンプライアンスに対応していない不具合にフラグを付けます。Nexus Dashboard Insights は、顧客の異常リストも生成します。詳細については、「アラートの分析」を参照してください。

Nexus Dashboard Insights がインストールされると、サービスはサイトごとにデフォルトのベストプラクティスを実行します。Nexus Dashboard Insights でサイトを有効にすると、ベストプラクティスのデフォルトのスケジュールと頻度が有効になります。ベストプラクティスジョブのデフォルトのスケジュールは編集できます。

スケジュールについては、「デフォルトのバグスキャン」を参照してください。

ベストプラクティスのスケジュール設定

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]メニューから、**[サイトグループの設定]** > **[ベストプラクティス]**を選択します。

   [ベストプラクティス]ページが表示されます。デフォルトでは、サイトのベストプラクティスが有効になっています。**[全般]**テーブルには、すべてのサイトが表示されます。
3. をクリックして、選択したサイトのベストプラクティスジョブをスケジュールします。
4. [開始時刻]、[繰り返し間隔]、[期日]、[終了日]を選択します。
5. [保存（Save）] をクリックします。
6. **[今すぐスキャン]**をクリックします 。
7. **[履歴]**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ベストプラクティスジョブ情報が表示されます。
8. 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。
9. アイコンをクリックすると、**[ベストプラクティス]**のステータスページが表示されます。
10. (任意)進行中のジョブを選択し、**[停止]**をクリックしてジョブを停止します。

オンデマンドのベストプラクティス

次の手順を使用して、オンデマンドのベストプラクティスを実行します。

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]メニューから、**[サイトグループの設定]** > **[ベストプラクティス]**を選択して、選択したサイトでオンデマンドのベストプラクティスを実行します。

   [ベストプラクティス]ページが表示されます。デフォルトでは、サイトのベストプラクティスが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]**をクリックします。

   [履歴]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ベストプラクティス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、**[ベストプラクティス]**の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]**をクリックしてジョブを停止します。

収集ステータス

[概要]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]メニューをクリックし、**[サイトグループの設定]**を選択して、**[収集ステータス]**タブをクリックします。

[収集ステータス]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]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。

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

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

データのエクスポートに関するガイドラインと制限事項

- 定期的なジョブの設定では、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 Export では、最大 5 つのエクスポータがサポートされています。
- Kafka エクスポートを設定する前に、Nexus Dashboard クラスタ設定の既知のルートとして外部 Kafka IP アドレスを追加する必要があります。
- Nexus ダッシュボードは、フロー異常の Kafka エクスポートをサポートしています。ただし、フローイベントの異常では、Kafka エクスポートは現在サポートされていません。
- ファブリックでソフトウェアテレメトリを無効にし、Cisco DCNM からファブリックを削除する前に、[メッセージバス設定]と[電子メール]ページのすべての設定が削除されていることを確認してください。
- Kafka および電子メールメッセージの異常には、リソース、環境、統計情報、エンドポイント、フロー、バグのカテゴリが含まれます。
- カテゴリ(セキュリティ、転送、変更分析、コンプライアンス、システム)は、Kafka および電子メールメッセージの異常には含まれません。
- データ収集タイプ**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。

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]**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]メニューをクリックし、**[サイトグループの設定]**を選択して、**[データのエクスポート]**タブをクリックします。
3. *[メッセージバス設定]*領域で、**[新規追加]**をクリックし、次のタスクを実行します。
   a. **[サイト名]**フィールドで、適切なサイトを選択します。

b. [IP アドレス]フィールドと[ポート]フィールドに、Kafka ブローカーの IP アドレスとポートを入力します。

c. **[モード]**フィールドで、セキュリティモードを選択します。サポートされているモードは、[非セキュア]、[セキュア SSL]、および[SASLPLAIN]モードです。

d. **[一般設定]**領域で、データの送信先となる名前とトピック名を入力し、基本モードまたは詳細モードを選択します。

異常とアドバイザリに関する Kafka エクスポートの詳細が表示されます。

4. 各カテゴリの**[収集設定]**領域で、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。

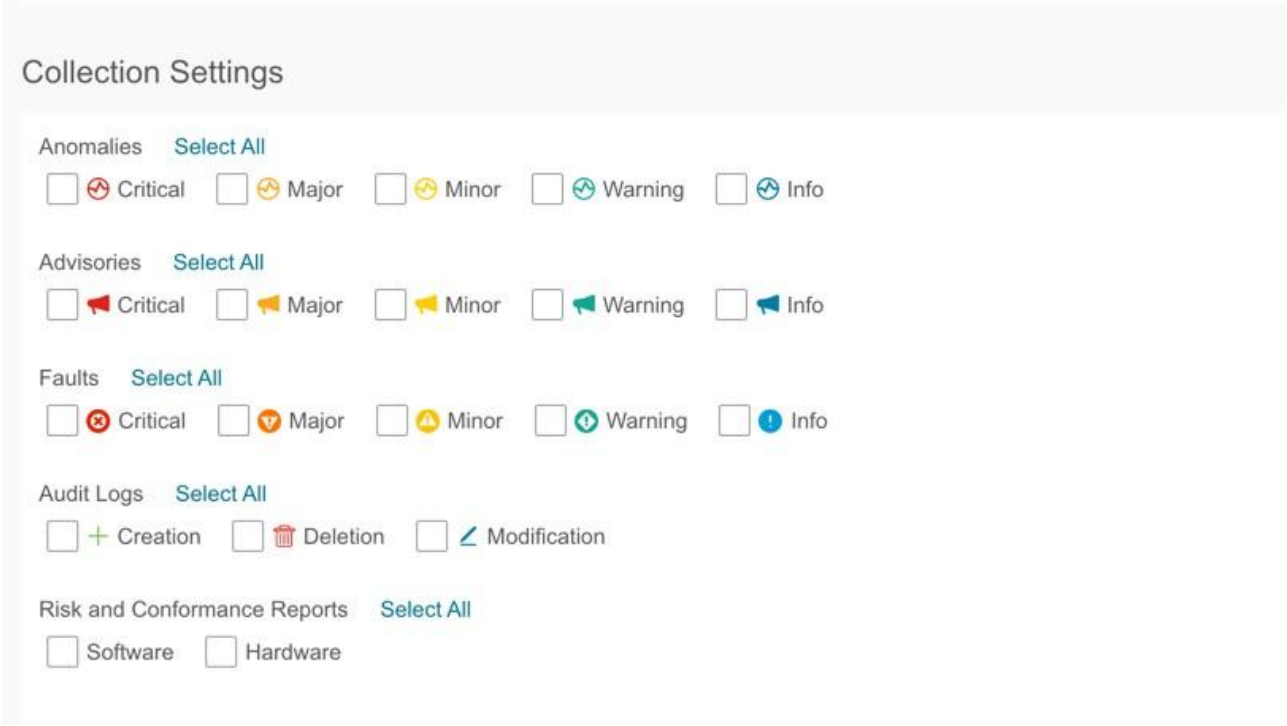
電子メールの設定

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]**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]メニューをクリックし、**[サイトグループの設定]**を選択して、**[データのエクスポート]**タブをクリックします。
3. **[電子メール]**領域で**[新規追加]**をクリックし、次の操作を実行します。
   a. **[全般設定]**領域の**[サイト名]**フィールドで、サイト名を選択します。
   b. **[名前]**フィールドに、名前を入力します。
   c. **[電子メール]**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]**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]**フィールドに、開始日を入力します。
   f. **[収集間隔]**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]**フィールドで、[基本]または[詳細]を選択します。

   [基本]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]**領域に表示されます。[詳細]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]**領域に表示されます。

4. 各カテゴリの**[収集設定]**領域で、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**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**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]**、ハードウェア プラットフォームの場合は**[ハードウェア]**、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。



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]**領域に表示されます。

   指定した*[開始日]*の*[収集間隔]*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]*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. をクリックして電子メールスケジューラを編集します。
   b. をクリックして、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するための参照マイルストーンとして使用されます。

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]** > **[ソフトウェア/ハードウェア適合性]**を選択して、適合性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]、[警告]、[クリティカル]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]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]**をクリックします。**[適合性レポート]**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]**メニューの**[印刷/ダウンロード]**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]**メニューの**[電子メールのスケジュール]**をクリックして、電子メールスケジューラを設定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、異常をサードパーティのツールにエクスポートできます。

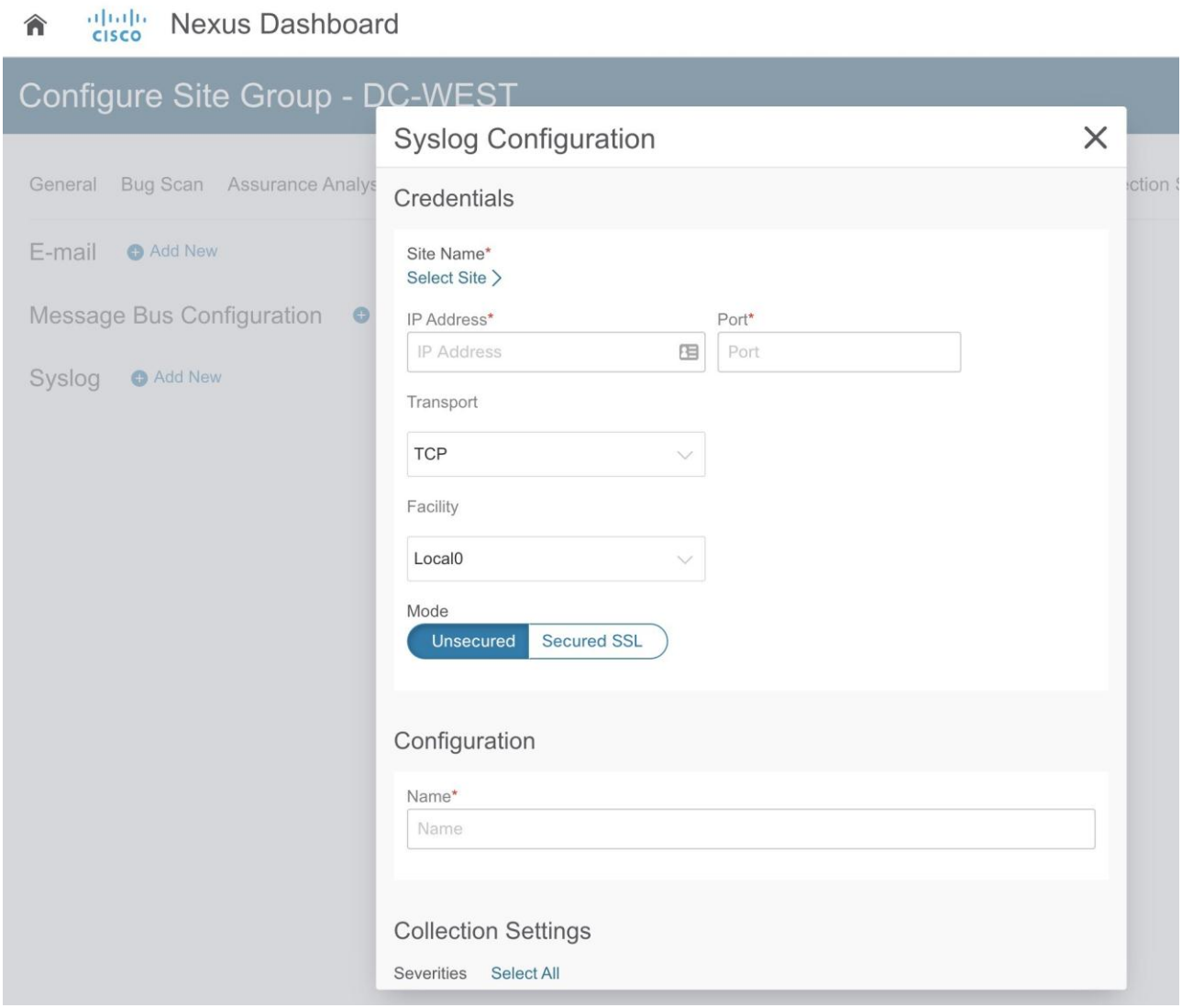
Syslog のガイドラインと制約事項

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]**ページの上部で、適切なサイトグループを選択し、**[サイトグループの設定]**をクリックします。
2. サイトグループの**[サイトグループの設定]**ページで、**[データのエクスポート]**タブをクリックします。
3. **[Syslog]**フィールドで、**[新規追加]**をクリックします。
4. **[Syslog 設定]**ダイアログボックスの**[ログイン情報]**領域で、次の操作を実行します。



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

b. **[IP アドレス]**および**[ポート]**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]**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]**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]**フィールドでトグルボタンをクリックして、**[非セキュア]**か**[セキュア 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. **[設定]**領域に、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]**領域で、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。

設定が完了すると、**[サイトグループの設定]**ページの**[データのエクスポート]**タブにある**[Syslog]**領域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

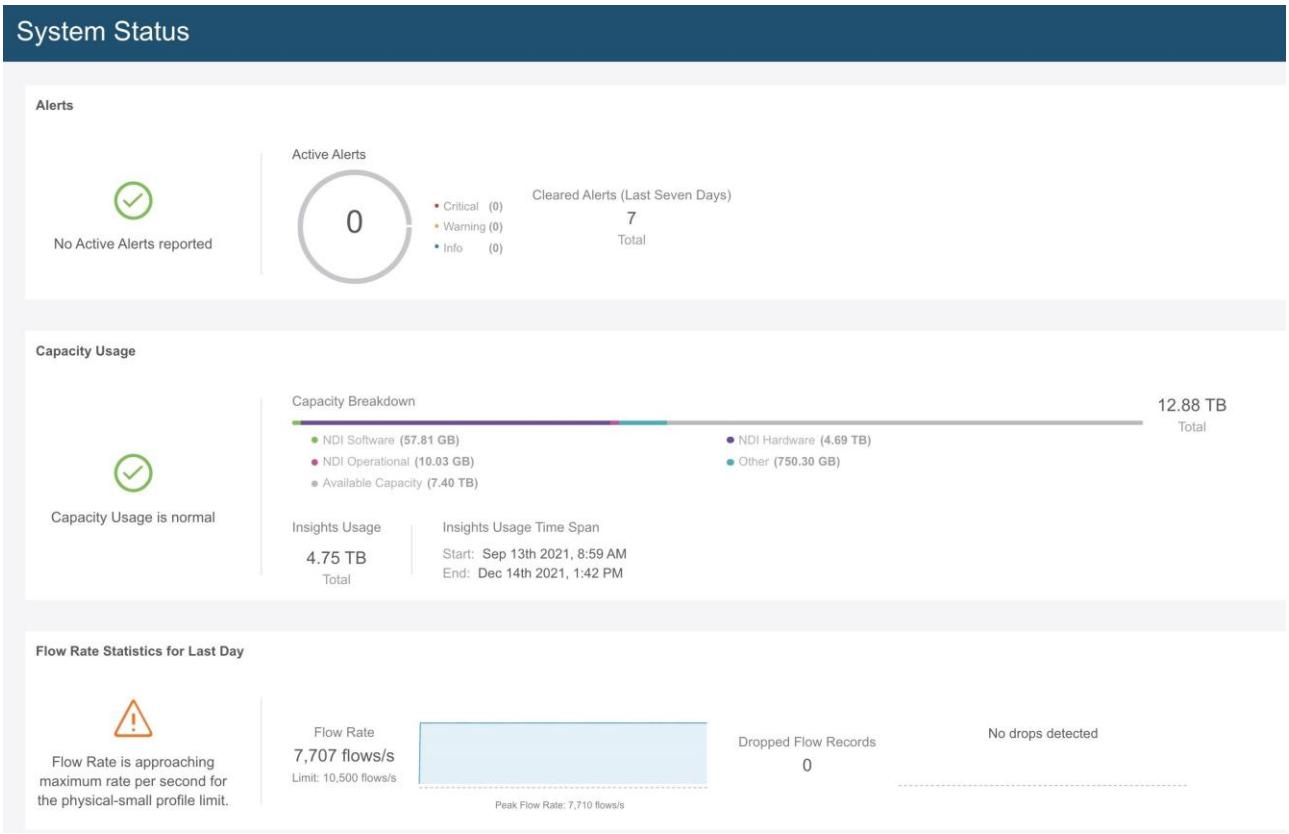
システムステータス

[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]アイコンで、**[アプリケーション]** > **[ステータス]**をクリックします。

   [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]**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]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]領域には、**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]領域で**[さらに表示]**をクリックして、**[ノードのフローレート]**と**[フロー]**の詳細を展開して表示します。**[ノードのフローレート]**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]**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。フローの設定の詳細については、「フローの設定」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、既存のサイトとして" 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" の設定は更新されません。

- 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]**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。
- 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]** > **[アプリケーション]** > **[設定のインポート/エクスポート]**を選択します。
2. **[新規インポート/エクスポート]**をクリックします。
3. **[新規インポート/エクスポート]**ページで、**[エクスポート]**をクリックします。
4. **[開始]**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]**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]**に変わったら、 ··· をクリックして**[ダウンロード]**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. ··· をクリックして**[削除]**を選択し、設定を削除します。

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]** > **[アプリケーション]** > **[設定のインポート/エクスポート]**を選択します。
2. **[新規インポート/エクスポート]**をクリックします。
3. **[新規インポート/エクスポート]**ページで、**[インポート]**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]**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]**に変わったら、··· をクリックして**[適用]**を選択します。

6. インポートする設定を選択し、**[適用]**をクリックします。**[インポート/エクスポート]**テーブルには、インポートされた設定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]の場合、一部の設定は追加され、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]**タブでは、複数のクラスタを一緒に接続して、Single Pane of Glass (SPoG)ビューを作成し、クラスタとそのサイト、サービス、および設定を管理できます。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。

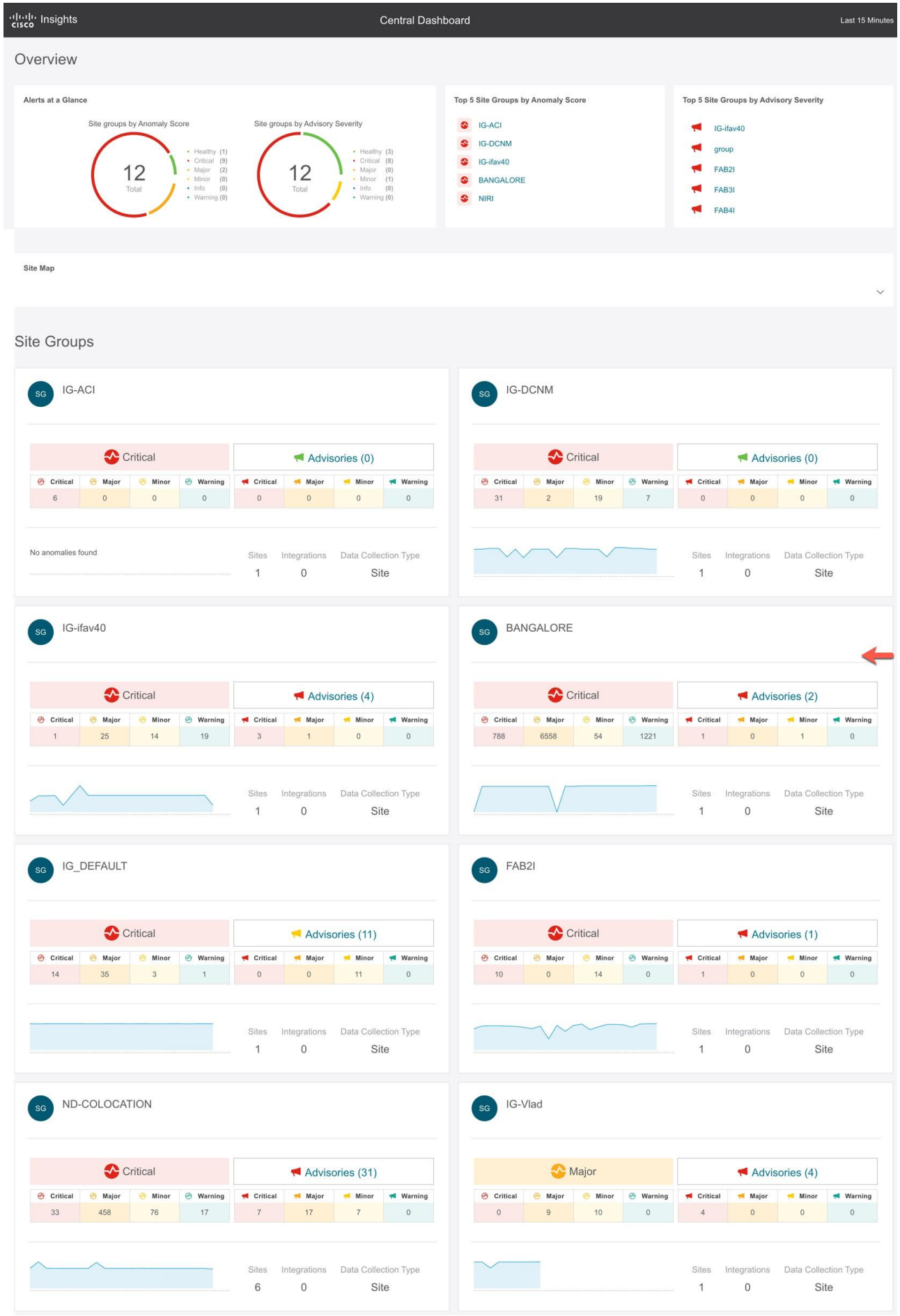
Cisco Nexus Dashboard では、作成したクラスタグループ全体にわたるすべてのクラスタ、サイト、およびサービスを含むシステム全体の概要とステータスが**[集中ダッシュボード]**に表示されるため、1 つのクラスタへの接続の損失など、明らかな問題を迅速に特定できます。

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。

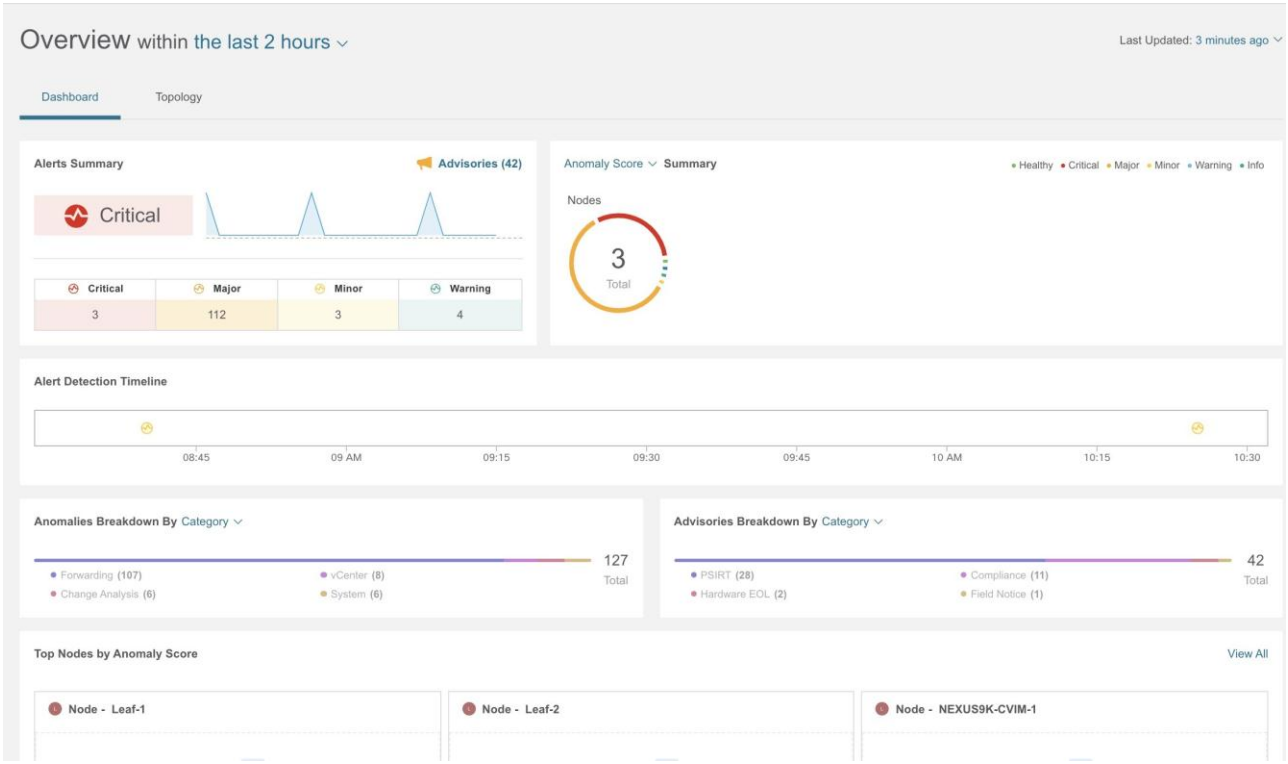
1. [Nexus Dashboard Insights]ページの右上にある**[集中ダッシュボード]**をクリックします。



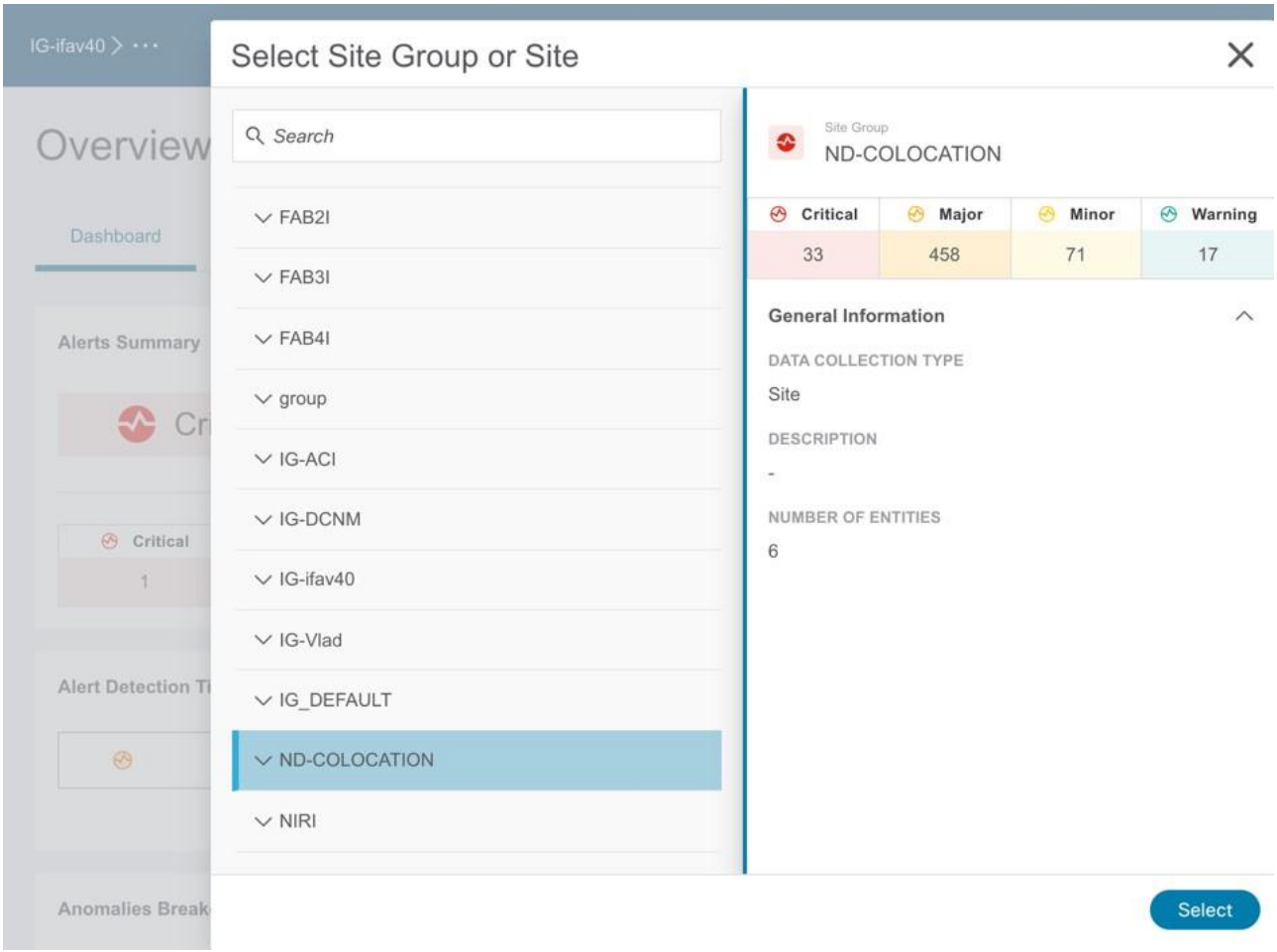
[集中ダッシュボード]の[概要]領域には、異常スコアとアドバイザリの重大度別にサイトグループが表示され、サイトマップにはサイトの場所が示されます。

[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]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]**ページに表示します。



3. [サイトグループ]領域で[サイトグループ]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]**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。**[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で、サイトグループまたはサイトを選択し、**[選択]**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ウィンドウには、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

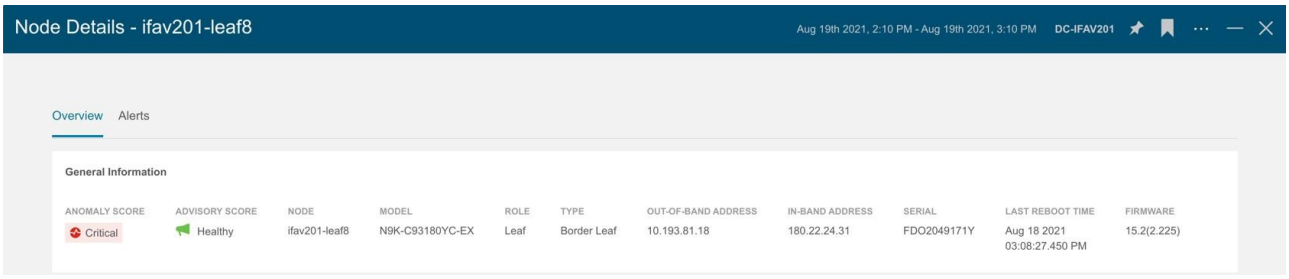
1. [+]アイコンをクリックしてカスタムダッシュボードを作成します。

2. 一意の名前を入力します。 ✓ を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、 ⧉ を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]**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]**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]** > **[カスタムダッシュボード]**を選択します。
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]** > **[カスタムダッシュボード]**を選択します。
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

NX-OS を使用した DCNM の探索について

Explore 機能により、Cisco NX-OS からの構成スナップショットが分析され、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実行可能になります。

- NX-OS ネットワーキングアセットを調べる
- 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 Cisco NX-OS 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。

現在、DCNM サイトグループを介して利用可能な NX-OS ネットワーキングアセットを調べるため、**What クエリ**がサポートされています。**Can クエリ**と **How クエリ**はサポートされていません。

- **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。

NX-OS の例:

1. What VLANs are associated with VRF: secure
2. What EPs are associated with INF: eth1/3 | leaf-1 or VRF: vrf_1 | leaf-1
3. What VLANs are associated with EP:100.x.x.x | vrf_secure

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。

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。
- **[Explore]**ページで、分析が失敗すると、エラーメッセージ*[分析に失敗しました]*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]** > **[テクニカルサポート]**を選択し、**[アクション]** > **[テクニカルサポートの収集]**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
```

- NX-OS ファブリックの場合、**Explore** 機能は、ファブリック内の VRF、VLAN、インターフェイス、エンドポイント、およびリーフスイッチのリソースのスイッチ全体のビューを提供します。また、レイヤ 2 VNI およびレイヤ 3 VNI をリソースとして提供します。
- リソース集約は、VLAN および VRF リソースでサポートされています。リソース集約では、VRF や VLAN などのリソースがファブリック全体で検出され、すべてのリーフスイッチがこれらのリソースによって集約されます。**[クエリ結果]**領域で、**What VLANs are associated with any?**のクエリを実行すると、ファブリック全体で使用可能なすべての VLAN のリストが表示されます。EP と LEAF の数は VLAN ごとに集約され、集約されたリソースカウントをクリックすると、単一の VLAN に関連付けられているすべての EP と LEAF を見つけることができます。また、VLAN および VRF クエリはファブリック全体が対象となるため、特定のリーフスイッチ上の VLAN リソースを調べる場合は、クエリで **AND** 演算子を使用する必要があります。たとえば、**What EPs are associated with VRF:vrf-vrf_51020 and LEAF:CANDID-SYS-S1-L1** などです。
- リーフスイッチのインターフェイスなどのネットワークアセットは、**Explore** で調べることができるように、リーフスイッチのエンドポイントに関連付ける必要があります。
- VRF が動作していない場合、**Explore** はエンドポイントをレイヤ 2 エンドポイントとして検出します。
- エンドポイントは、レイヤー3 またはレイヤー2 エンドポイントとして検出されます。VLAN に存在するすべてのエンドポイントが検出され、他のエンドポイントは無視されます。
- **Explore** でエンドポイントまたはその他のネットワークアセットが表示されない場合は、関連するスナップショットでシステムの異常を探します。すべてのリーフスイッチで収集が成功したことを確認します。収集が失敗した場合、結果的にエンドポイントが検出されないことがあります。
- DCNM サイトグループを備えた NX-OS の場合、**Explore** では IPv4 エンドポイントのサポートのみを利用できます。**Explore** での IPv6 エンドポイントのサポートは現在利用できません。

- **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。
- Explore 機能は VNI および/または VRF で学習されたエンドポイントに基づいているため、DCNM ベースのファブリックの Explore 機能で特定の WHAT クエリが機能するには、VNI または VRF でエンドポイントを使用できる必要があります。エンドポイントが利用できない場合、VRF または L3 VNI の What クエリは正確な結果を表示しません。

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]**ページで、適切な[サイトグループ] > [サイト]を選択します。
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]**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。
5. [クエリセレクタ]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。送信元および宛先リストに追加できます。例えば、**送信元は宛先と通信できますか?**などです。

[どのエンティティが通信できますか]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]**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]**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、NX-OS ネットワーキングアセット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。

サポートされているクエリ

次の表は、NX-OS 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 EP	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
関連付けられている INF	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
関連付けられている LEAF	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI

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 VLAN	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
関連付けられている VRF	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
関連付けられている L2VNI	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI

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 L3VNI	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI

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。テスト環境では**ベータ**とマークされた機能を使用し、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]**ページで、左側のナビゲーションウィンドウで**[参照]** > **[フロー]**をクリックします。
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]アイコンをクリックして表示し、**[フローの詳細]**ページを表示します。
3. **[フローの詳細]**ページに、**[フローレコード情報]**と**[集約されたフロー情報]**が表示されます。
4. **[フローパスの概要]**領域のフローパスで、**[マルチサイトフロー - フローExplore で表示]**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、送信元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として**[Explore]**ページに表示されます。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。

送信元サイトと宛先サイトの特定の詳細は、各**[集約されたフローレコード]**テーブルに表示されます。**[異常]**テーブルで、**[集約]**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]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]*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]、[環境]、[統計情報]、[エンドポイント]、および[フロー]に基づいた上位ノードのグラフが表示されます。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]*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]*セクションには、Nexus Dashboard Insights の上位 5 つのリソース([リソース使用率]、[環境]、[統計情報]、および[フロー])が、障害とイベントの内訳とともに表示されます。*[異常]*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。

- [サマリー]ペインで*[ノード]*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。
- 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] 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、[一般的な情報]、[ノードの概要]、および[異常]が表示されます。*[ノードの概要]*セクションには、Nexus Dashboard Insights の上位 5 つのリソース([リソース使用率]、[環境]、[統計情報]、および[フロー])が、障害とイベントの内訳とともに表示されます。*[異常]*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]、[統計情報]、[リソース]、[異常]、[環境リソース]など、ノードの追加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、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]**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、異常の根本原因を特定できます。

- 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、および静的分析のために発生した異常で構成されます。
- 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々の異常が、重大度、ステータス、カテゴリ、影響を受けるノード、検出時間、タイトル、説明、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。

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。[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。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]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」を参照してください。
- 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。
- [コメント] - 指定したコメント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。
- [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。

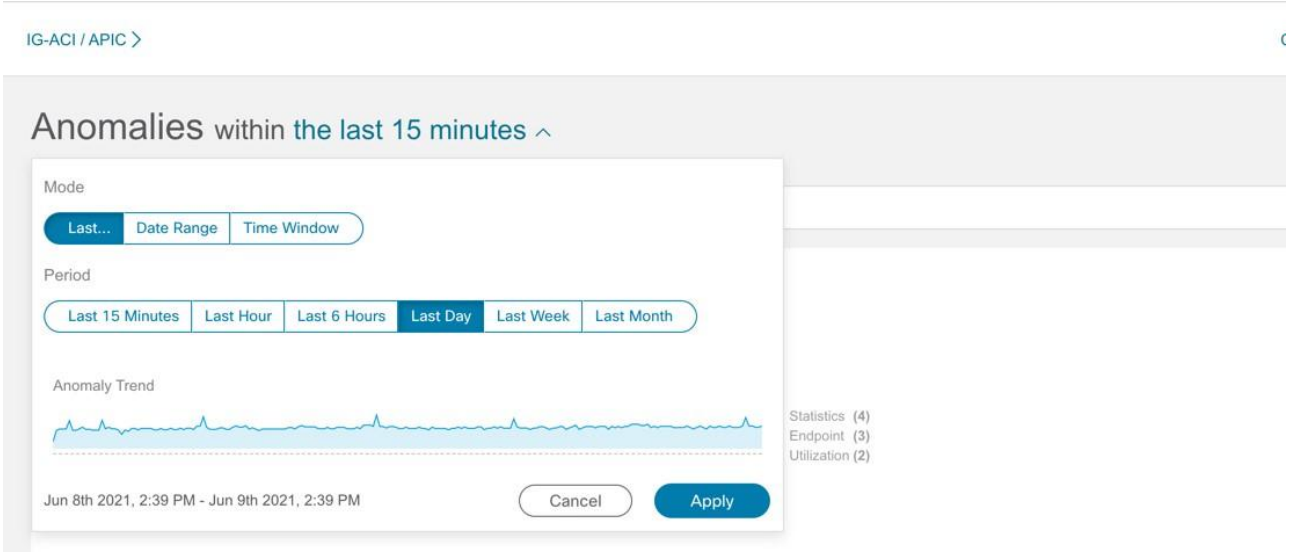
> - 最初のフィルタタイプ。この演算子および後続の値を使用すると、その値より大きい一致データが返されます。

>= - 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

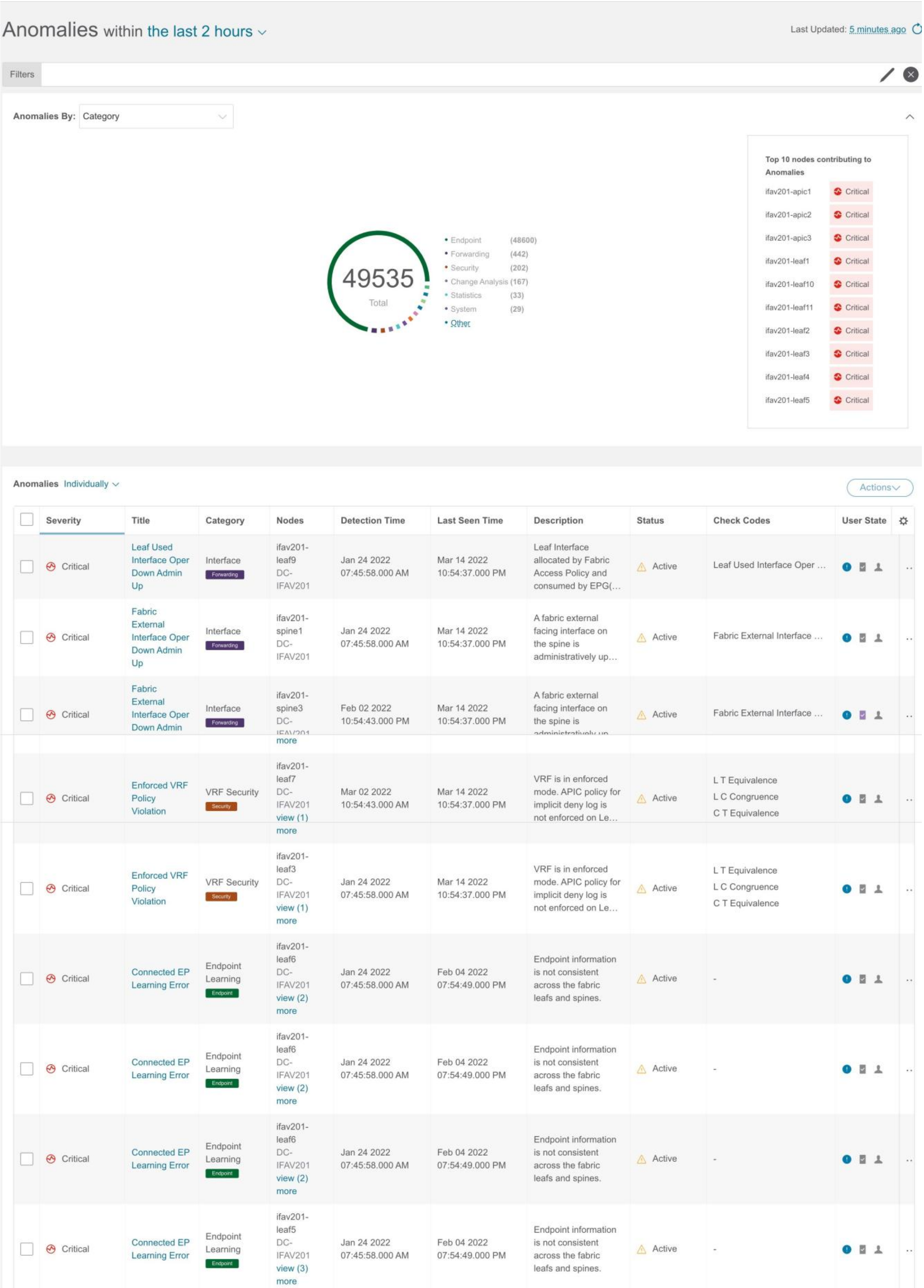
次の手順を使用して、異常を分析します。

1. **[アラートの分析]** > **[異常]**を選択します。
2. **異常**ダッシュボードで、[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. 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]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。



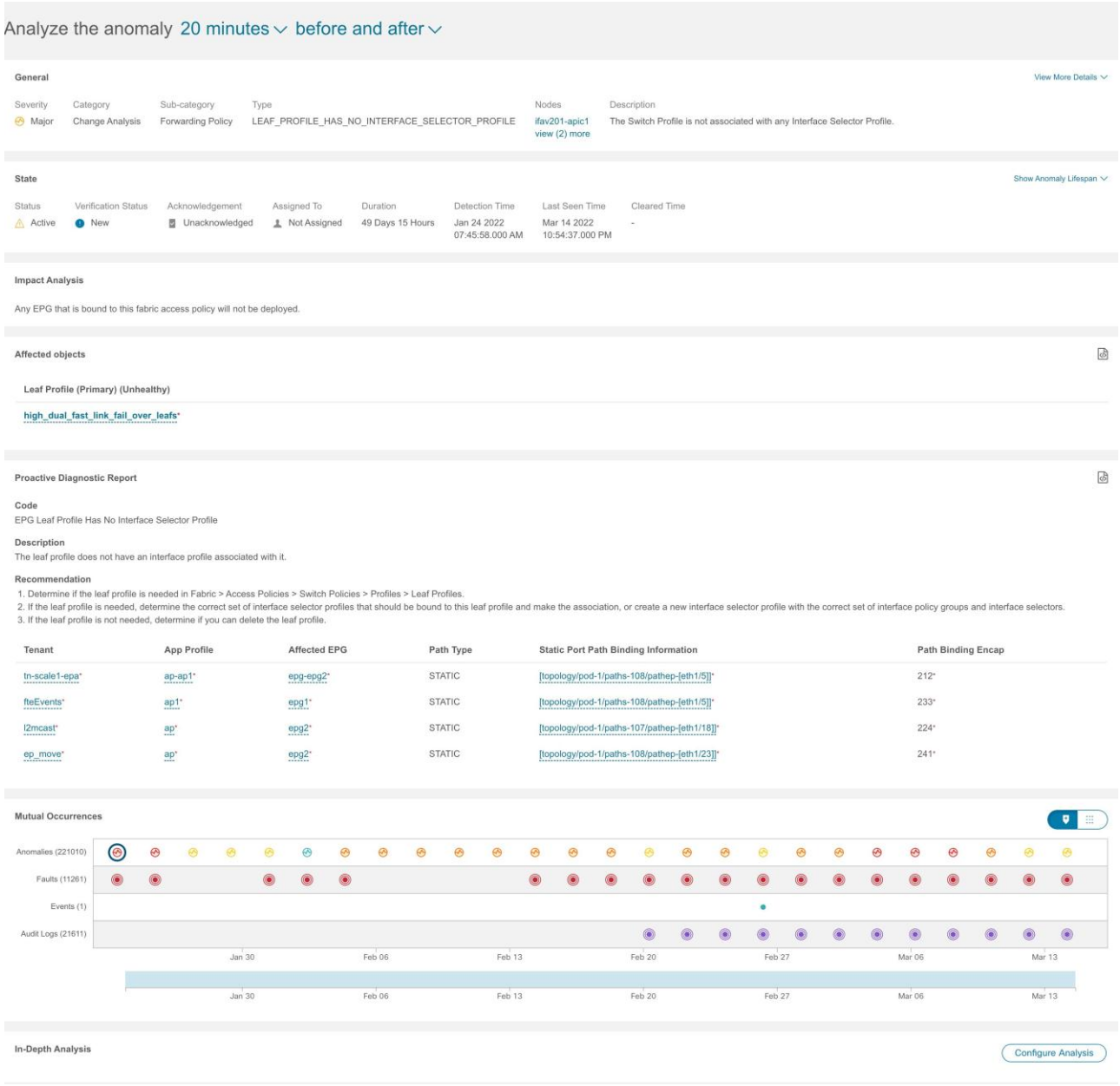
4. 次のいずれかを実行します。

   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]ドロップダウンリストから**[集約]**を選択して、タイトルに基づいて集約された異常を表示します。

c. [異常]ドロップダウンリストから**[サイト間]**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、異常をソートます。**[ノード]**列のフィルタリング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]**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]**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. **[分析]**をクリックします。**[異常の分析]**ページには、異常の一般的な情報、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]**ページの**[プロアクティブな診断レポート]**領域にチェックコードが表示されます。



a. **[全般]**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]**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]**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]**領域で**[レポートの表示]**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]**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]**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]**を選択し、ドロップダウンリストから**[チャート名]**を選択します。

iii. [保存（Save）] をクリックします。

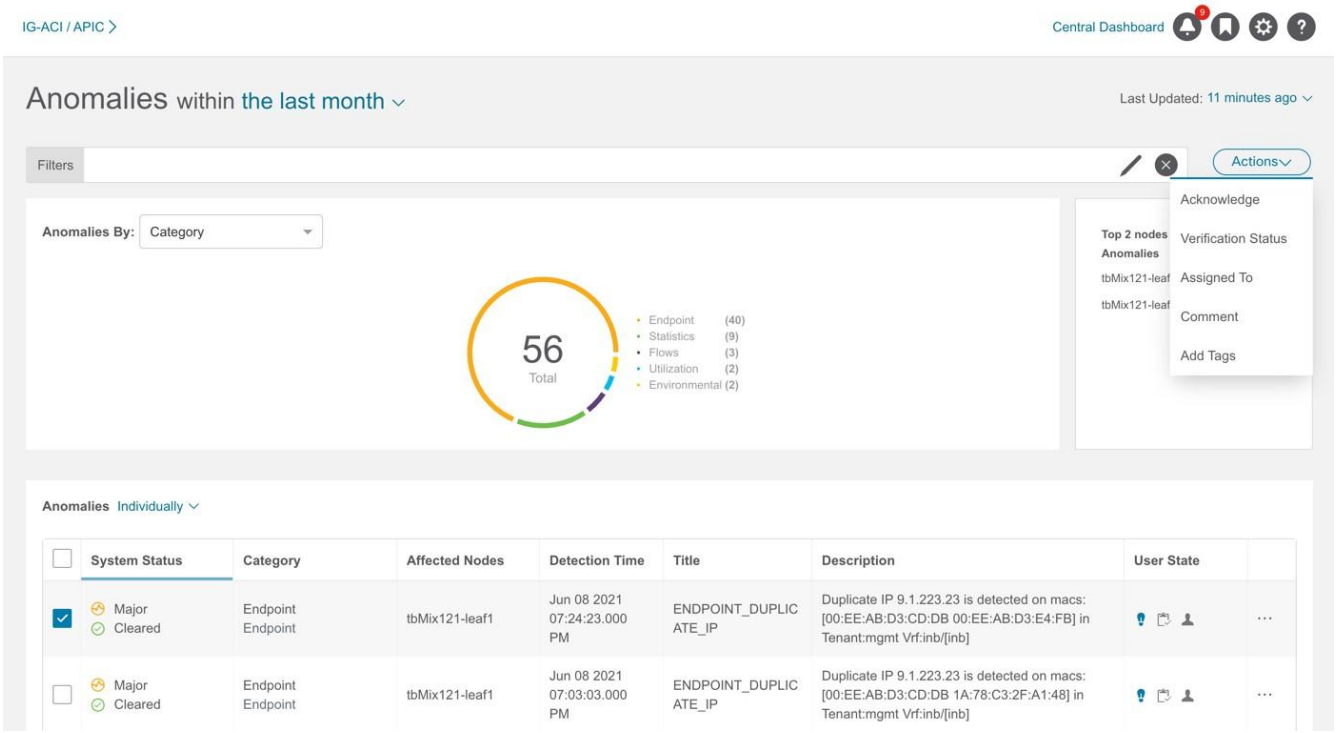
比較チャートが自動的に更新され、選択した異常があるノードのリソース使用率が表示されます。選択した異常があるノードのリソースを比較して分析できます。

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]** > **[異常]**を選択します。
2. **異常**ダッシュボードで、[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. 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]ドロップダウンリストから**[個別]**を選択します。
5. テーブルから異常を選択し、**[アクション]**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]**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]**テーブルに異常を表示するには、Acknowledge=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]ドロップダウンリストから**[集約]**を選択した場合、Acknowledgement=false フィルタは適用されません。[異常]ドロップダウンリストから**[個別]**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]**を選択します。[保存（Save）] をクリックします。

c. **[割り当て先]**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]**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]**をクリックします。

e. **[タグの追加]**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]**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]列に表示されます。

注:

- **[アクション]**メニューを使用して異常のプロパティを設定すると、**[異常]**テーブルの `···` アイコンを使用して、個別の異常で設定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。

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]** > **[異常]**を選択します。
2. **異常**ダッシュボードで、[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. 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]テーブルには、承認された異常が表示されます。
   b. **[異常]**ドロップダウンリストから[個別]を選択します。
   c. 承認された異常を選択し、**[アクション]**メニューから**[未承認]**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]**を選択します。

アドバイザリ

アドバイザリ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]ドロップダウンリストから、**[重大度]**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]ドロップダウンリストから**[カテゴリ]**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、メタデータにバンドルされた署名を使用して、新しいバグ、PSIRT、Field Notice、およびサポート終了通知を検出します。

メタデータには、バグシグネチャ、PSIRT、アップグレードイメージ、リリースノート、Field Notice、EOL 通知などの情報が含まれています。この情報は、Nexus Dashboard Insights によって定期的に取得され、バージョン管理されたパッケージイメージを生成するために検証されます。このパッケージは、検証後に Intersight クラウドにプッシュされ、Cisco Secure クラウドに接続されているすべてのサービスですぐに利用できるようになります。Nexus Dashboard Insights などのサービスは、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 ポータルに接続されます。

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。「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] > **[アプリケーション]** > **[バージョン情報]**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]**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、Field Notice、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

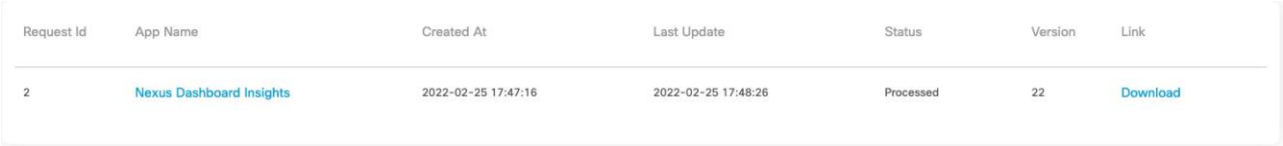
次の手順を使用して、エアギャップまたはオフライン環境で最新のメタデータバージョンを更新します。

1. Cisco DC App Center にログインします。
2. [ユーザー]ドロップダウンメニューから **[マイアカウント]**を選択します。
3. **[設定ファイルのリクエスト]**タブをクリックします。
4. **[設定ファイルをリクエスト]**をクリックします。
5. **[アプリ ID の選択]**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]**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]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]**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。



Request Id	App Name	Created At	Last Update	Status	Version	Link
2	Nexus Dashboard Insights	2022-02-25 17:47:16	2022-02-25 17:48:26	Processed	22	Download

8. Cisco Nexus Dashboard Insights にログインします。
9. **[設定]** > **[アプリケーション]** > **[バージョン情報]**を選択します。
10. **[更新]** をクリックします。
11. [メタデータバージョンの更新]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]**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。

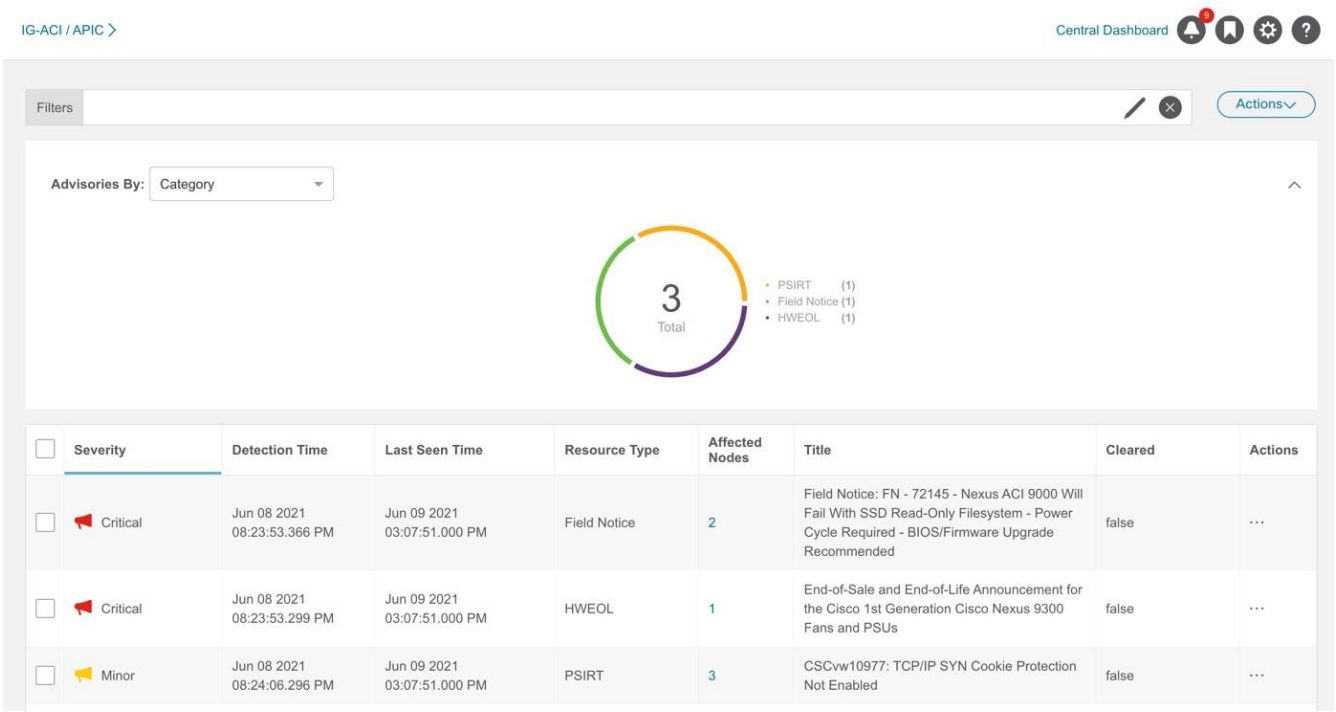
2 次フィルタの絞り込みとして、次の演算子を使用します。

- == - 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。

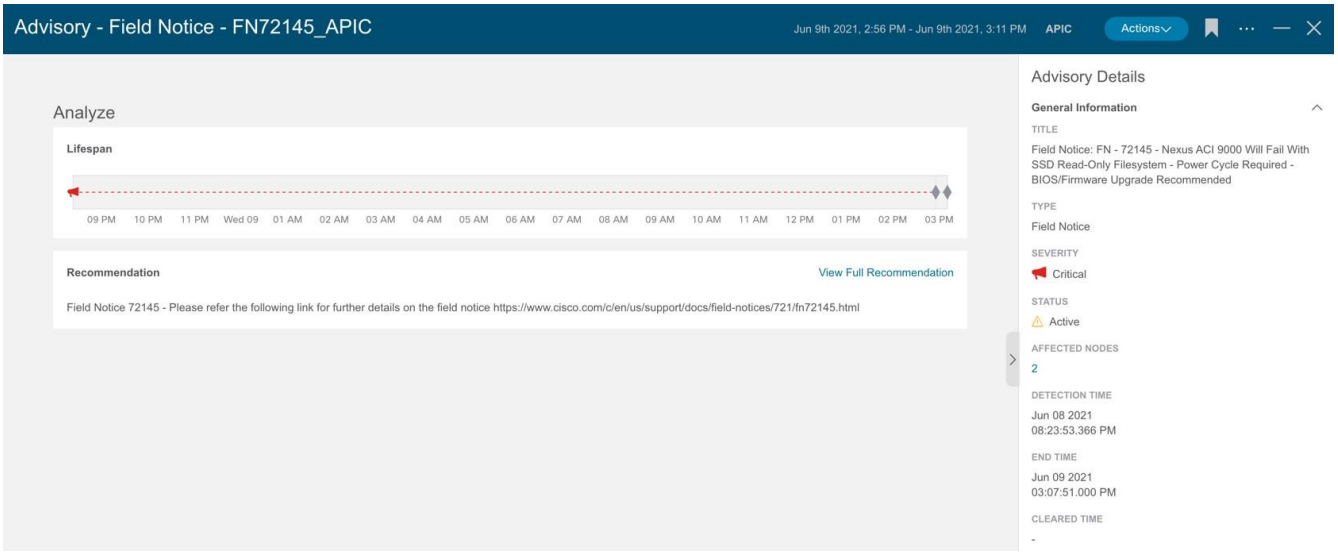
アドバイザリの分析

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]** > **[アドバイザリ]**を選択します。
2. **[アドバイザリダッシュボード]**ページで、[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. 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]**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、アドバイザリは重大度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. **[分析]**をクリックします。**[アドバイザリの分析]**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. **[一般的な情報]**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]**領域で、**[完全な推奨事項を表示]**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]**テーブルからアドバイザリを選択し、**[アクション]**メニューから[承認]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]**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]**を含む**[一致基準]**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]**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]と[異常のカスタマイズ]アクションの両方が含まれていて、[承認]と[異常のカスタマイズ]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]**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]**セクションの[プロアクティブな診断レポート]領域には推奨事項が引き続き表示されます。

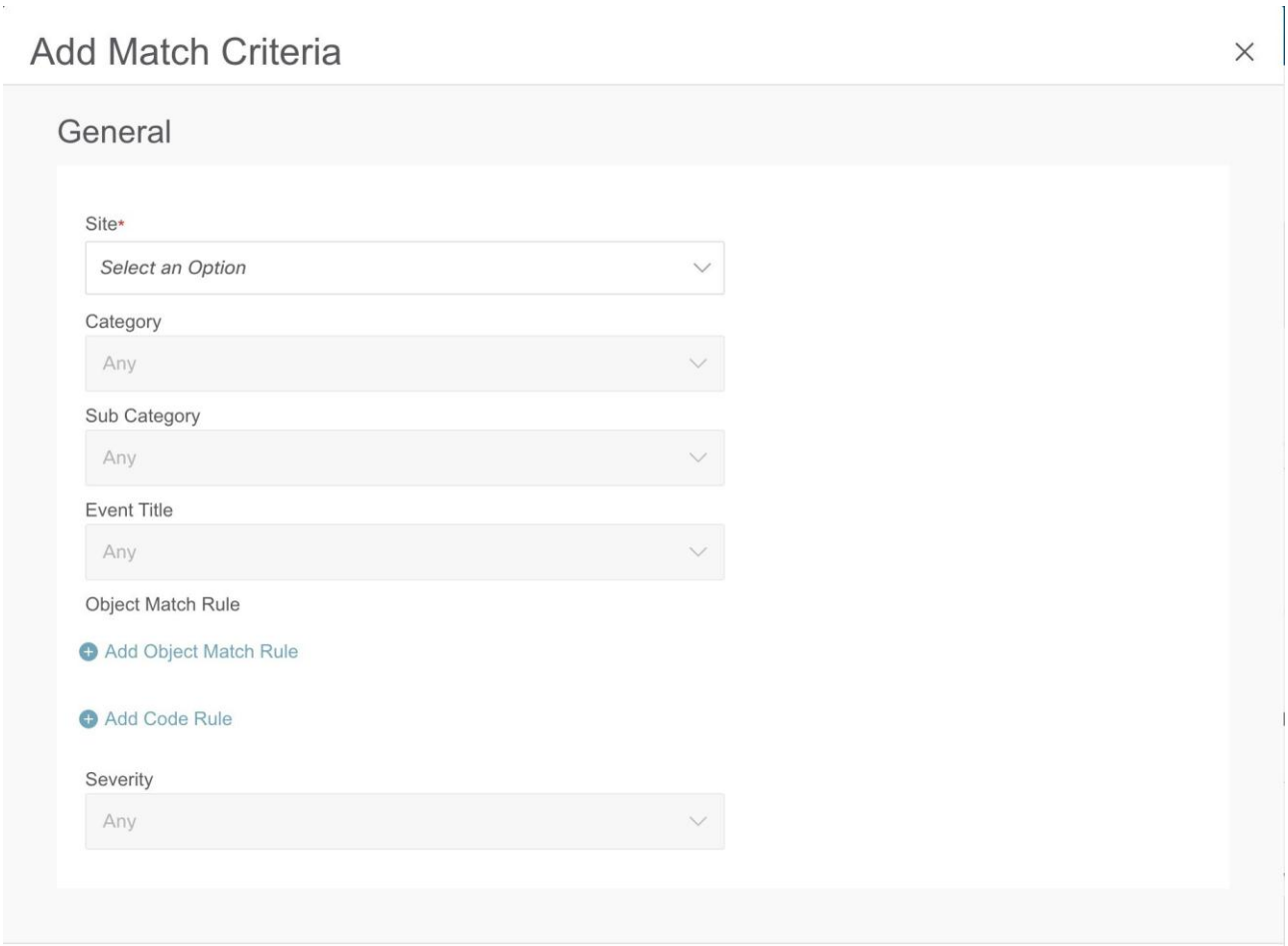
- アラートルールによって自動的に承認されたものを含め、異常は手動でのみ未承認にできます。アラートルールを無効化または削除することで、異常を自動的に未承認にすることはできません。「異常の管理」を参照してください。

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]メニューから、**[サイトグループの設定]** > **[アラートルール]**を選択します。
3. **[アラートルールの作成]**をクリックします。
4. **[アラートルールの作成]**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。
   b. [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]**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]**の次のフィールドに入力します。



a. **[サイト]**ドロップダウンリストから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]**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]**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]タイルから、 **[承認]**または**[異常のカスタマイズ]**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]**バーで、**[Acknowledged == True]**を選択します。結果が**[異常]**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]**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]**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]ページでは、**[ルールベースの推奨事項]**セクションの**[プロアクティブな診断レポート]**領域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]**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]**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]メニューから、**[サイトグループの設定]** > **[アラートルール]**を選択します。アラートルールが**[アラートルール]**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]**を選択して、アラートルールを編集します。
   b. **[有効化]**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]**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]**を選択して、アラートルールを削除します。

      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。

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。結果は次の領域に表示されます。

- **[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。

- 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を表示する。
- 2 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。
- 2 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。

- **[変更されたノード]**領域の**[ポリシーデルタ]**ページでスイッチを選択すると、2 つのスナップショット間の設定の違いが表示されます。
- [ポリシーデルタ]では、**[監査ログ]**は現在サポートされていません。

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。

手順

1. **[トラブルシュート]** > **[差分分析]**を選択します。
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]**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。

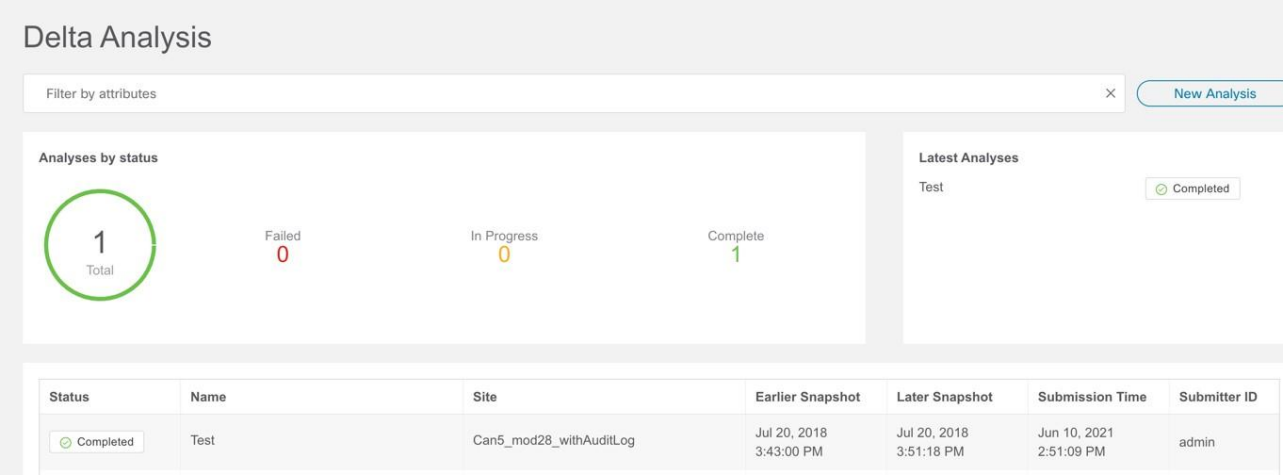
   b. **[サイト]**をクリックしてサイトを選択します。

   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。**[適用(Apply)]** をクリックします。

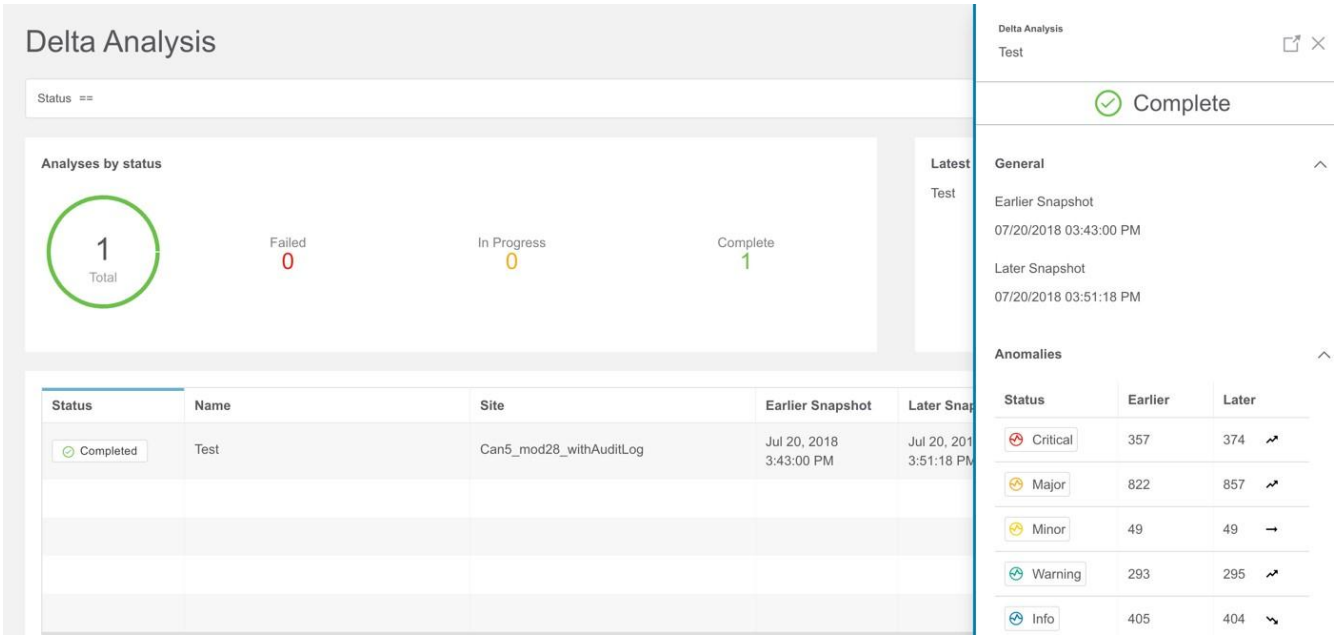
   差分分析用に選択した 2 つのスナップショットは、同じサイトグループに属している必要があります。

5. [作成（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。



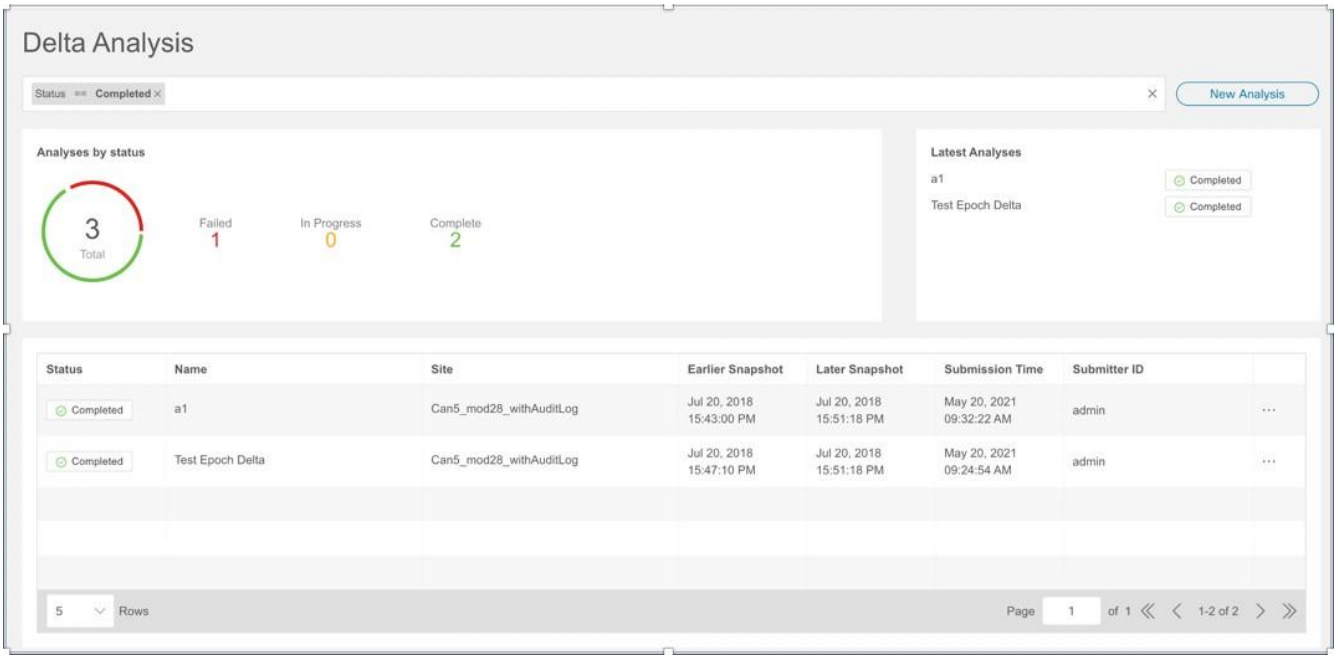
一度に 1 つの差分分析を実行できます。別の差分分析を実行するには、現在の差分分析を停止してから、別の差分分析を開始する必要があります。

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。
8. 差分分析の結果を表示するには、**[差分分析]**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]** > **[差分分析]**を選択します。
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]**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]**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]**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]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]**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。

DCNM のポリシーデルタ分析の表示

次の手順を使用して、DCNM サイトグループのポリシーデルタ分析の結果を表示します。

手順

1. **[トラブルシュート]** > **[差分分析]**を選択します。
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]**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。[ポリシーデルタ]には、[変更されたノード]、および[*<スイッチ名>*ポリシービューア]の 2 つのパネルが含まれます。
5. **[変更されたノード]**パネルには、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が表示されます。

6. **[変更の表示]**をクリックすると、[***<スイッチ名>*ポリシービューア**]パネルの変更内容が表示されます。
7. [***<スイッチ名>*ポリシービューア**]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設定が表示されます。以前のスナップショットのスイッチ設定は、以前のスナップショットポリシーと呼ばれます。後のスナップショットのスイッチ設定は、後のスナップショットポリシーと呼ばれます。
   a. 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。
   b. [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。

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]** > **[差分分析]**を選択します。
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]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。
7. 差分分析の結果を表示するには、**[差分分析]**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

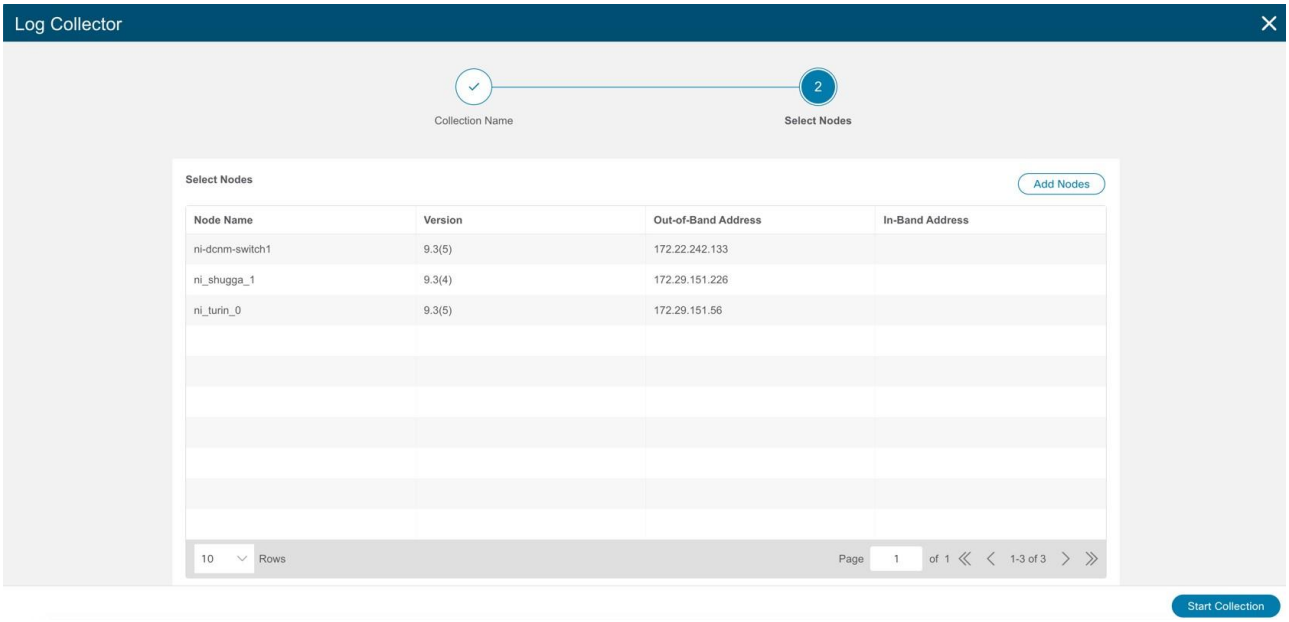
次の手順を使用して、ログを Cisco Intersight Cloud にアップロードします。

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]** > **[ログコレクタ]** > **[新しいログ収集]**を選択します。
2. 名前を入力します。
3. **[サイトの選択]**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]**をクリックし、**[ノードの選択]**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。

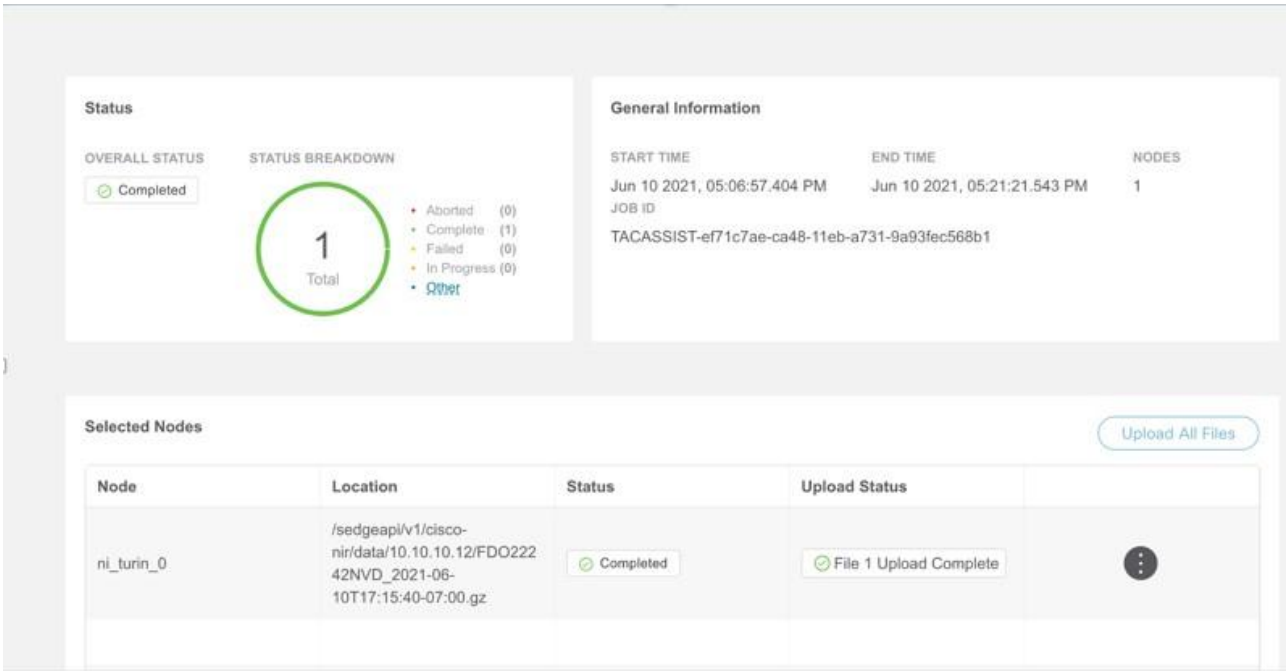


8. **[収集の開始]**をクリックして、ログ収集プロセスを開始します。

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

接続の分析

接続性分析機能を使用すると、ファブリック内または複数のファブリックにまたがるフローに対して、クイック分析または完全な分析を実行できます。これは、Nexus Dashboard Insights を通じて起動されるマイクロサービスであり、特定のフローのエンドツーエンドの転送パスを追跡し、そのパス上の問題のあるデバイスを絞り込むために使用されます。

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

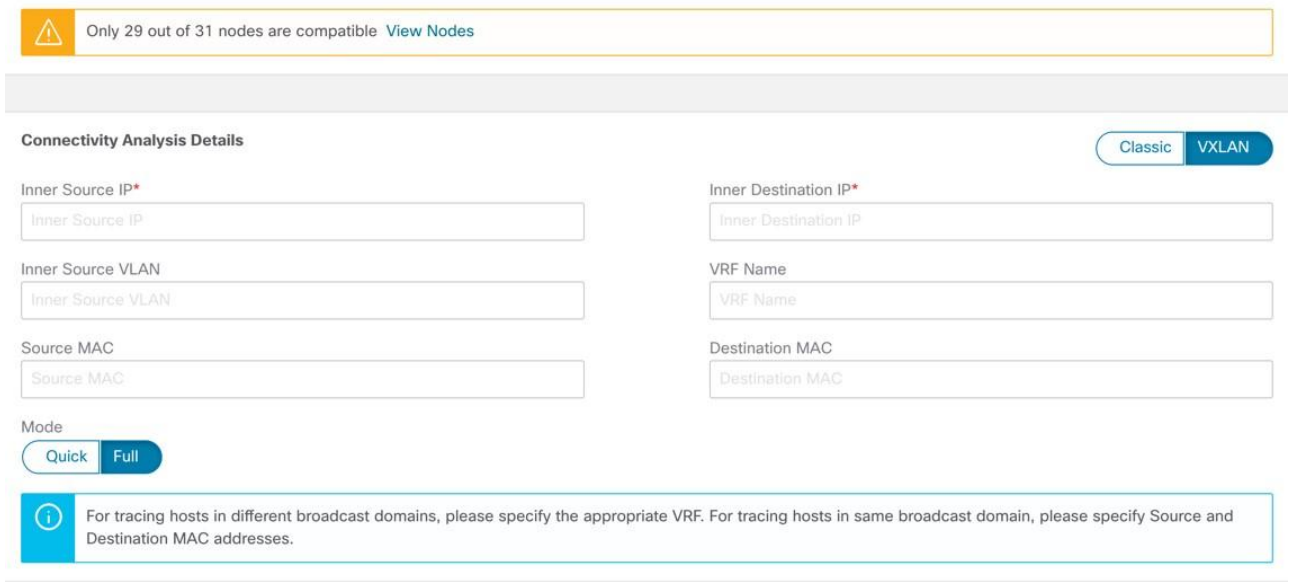
- 送信元から宛先エンドポイントまでの特定のフローについて、考えられるすべての転送パスをトレースします。
- 問題のあるデバイスを特定し、フローをドロップさせます。
- フォワード転送パスチェックの実行、整合性チェッカーによるソフトウェアおよびハードウェア状態のプログラミングの一貫性、パケットウォークスルーに関する詳細など、問題の根本原因を絞り込むのに役立ちます。

Nexus Dashboard Insights エージェントは、RPM ベースのアプリケーションサービスであり、Cisco NX-OS に事前にインストールされています。Nexus Dashboard Insights エージェントは、特定のフローのパスを取得します。このジョブは、エージェントから返されたパスを使用して、接続性分析ジョブを実行している次のホップに移動します。

接続性分析のスケジュール

この手順を使用して、ジョブと互換性のあるすべてのデバイスの新しい接続性分析ジョブをスケジュールします。

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. **[トラブルシュート] > [接続性分析]**を選択します。
3. **[新しい接続性分析]**をクリックします。**[接続性の分析]**ページが表示されます。
4. **[VXLAN]**または**[クラシック LAN]**インストールモードを選択します。
5. 必須フィールドとオプションフィールドに入力して、ジョブを設定します。

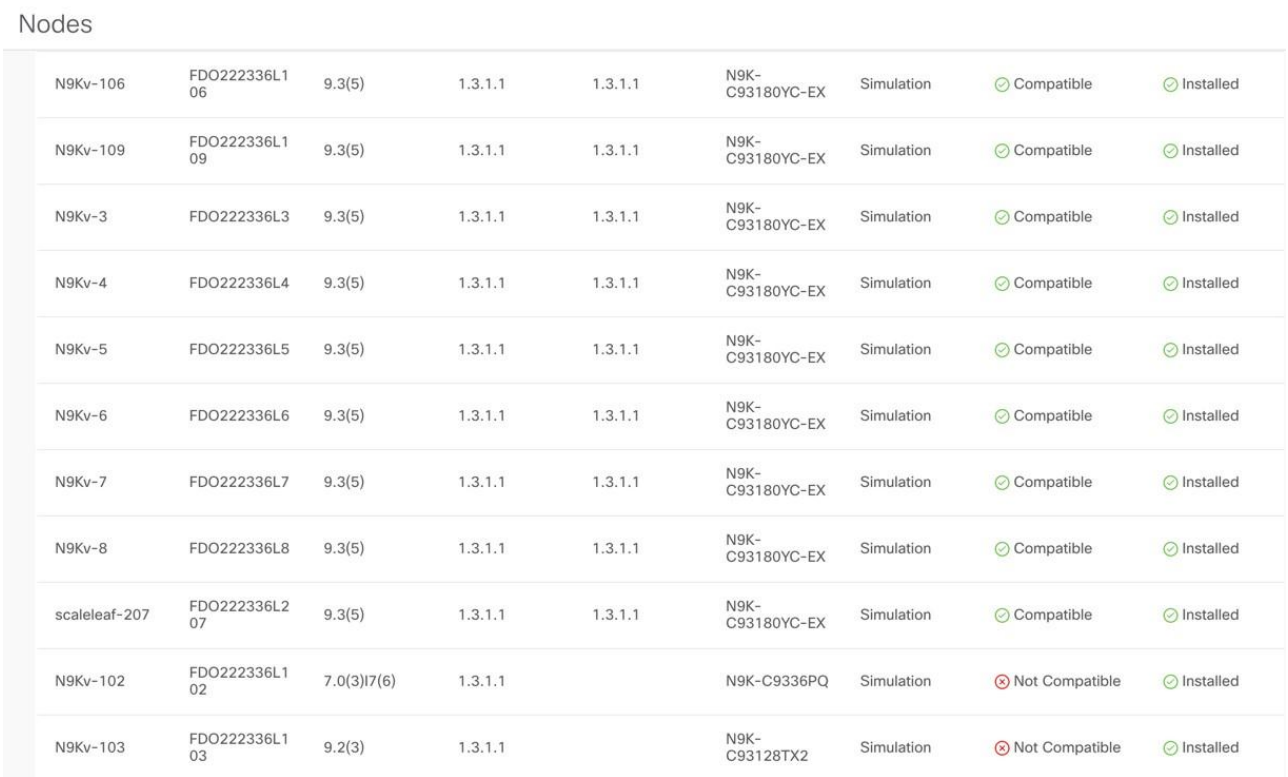


接続性分析ジョブ	入力フィールド
クラシック LAN - L3 ルーテッドフロー	必須: 送信元 IP アドレス、宛先 IP アドレス、および VRF 名(デフォルト以外の場合)。 オプション: 送信元 MAC アドレス、宛先 MAC アドレス、送信元 VLAN など、他のすべてのフィールド。
VXLAN - L2 VNI スイッチドフロー	必須: 送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、および宛先 MAC アドレス。 オプション: UI の他のすべてのフィールド。
VXLAN - L3 VNI ルーテッドフロー	必須: 送信元 IP アドレス、宛先 IP アドレス、および VRF 名。 オプション: 送信元 MAC アドレス、宛先 MAC アドレス、送信元 VLAN など、他のすべてのフィールド。

6. **[モード]**を**[クイック]**または**[完全]**に切り替えます。**[クイック]**検証は、特定のフローについて、L2、L3、および VXLAN CLI を使用してネットワーク パスを追跡し、フロードロップの原因となっている問題のあるノードを検出して分離します。

   [完全]検証は、プログラミングの一貫性を確認するためにソフトウェアとハードウェア間で一貫性チェッカーを実行します。また、特定のフローについて、L2、L3、および VXLAN CLI を使用してネットワークパスを追跡します。

7. **[ノードの表示]**をクリックすると、そのジョブおよび RPM バージョンと互換性のあるデバイスが表示されます。



8. **[アップグレード]**をクリックすると、最新バージョンと互換性のあるすべてのデバイスに対して、最新の Nexus Dashboard Insights エージェントの RPM のインストールが開始されます。

9. **[分析の実行]**をクリックします。接続性分析ジョブは、**接続性分析**ダッシュボードに表示されます。

接続性分析ダッシュボード

接続性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、最新の接続性分析が表示されます。

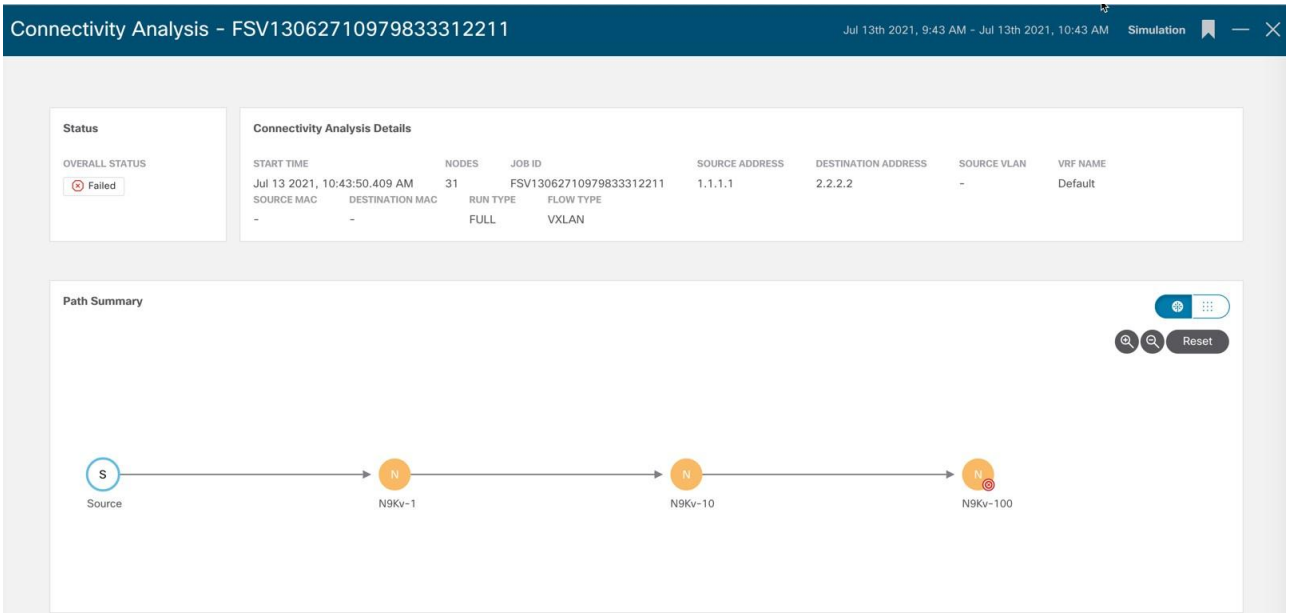
フィルタバーを使用すると、ステータス、ジョブ ID、ノード、送信元、宛先ごとに分析をフィルタリングできます。

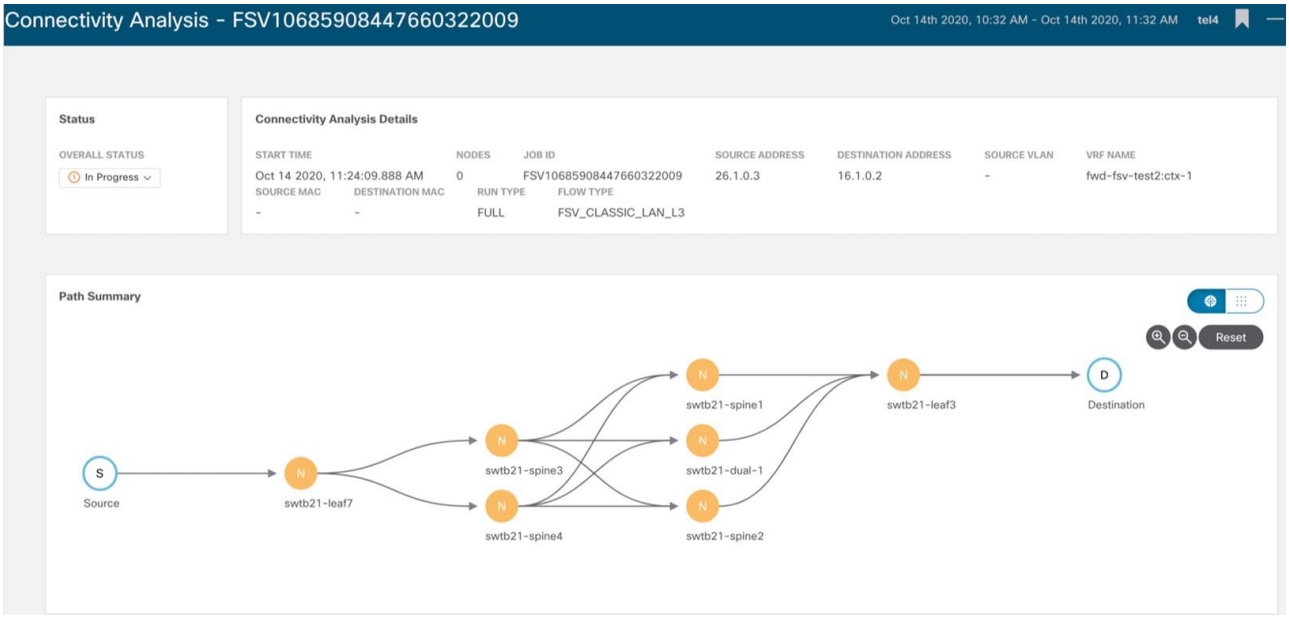
フィルタバーの有効な演算子は次のとおりです。

- == - 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、接続性分析ジョブが表形式でも表示されます。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接続性分析ジョブを選択して、追加の詳細を表示します。
2. アイコンをクリックして、**[接続性分析ステータス]**ページを表示します。**[接続性分析ステータス]**ページには、ステータス、ノードの詳細、パスの概要などの情報が表示されます。




Connectivity Analysis - FSV10685908447660322009
Oct 14th 2020, 10:32 AM - Oct 14th 2020, 11:32 AM
tel4
Status
OVERALL STATUS
In Progress
Connectivity Analysis Details
START TIME
Oct 14 2020, 11:24:09.888 AM
NODES
0
JOB ID
FSV10685908447660322009
SOURCE ADDRESS
26.1.0.3
DESTINATION ADDRESS
16.1.0.2
SOURCE VLAN
-
VRF NAME
fwd-fsv-test2:ctx-1
SOURCE MAC
-
DESTINATION MAC
-
RUN TYPE
FULL
FLOW TYPE
FSV_CLASSIC_LAN_L3
Path Summary
Reset
S
Source
N
swtb21-leaf7
N
swtb21-spine3
N
swtb21-spine4
N
swtb21-spine1
N
swtb21-dual-1
N
swtb21-spine2
N
swtb21-leaf3
D
Destination

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]** - サイト全体で収集されたノードのエンドポイントの異常が表示されます。
- **[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。

関連資料

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	リーフノードの観察結果の検索は、上位リーフノードで情報をフィルタリングすることにより、さらに絞り込むことができます。
使用率別の上位ノード	リソースタイプごとにノードの傾向の観察結果を表示します。 • 運用リソース • 設定のリソース • ハードウェアリソース

注意事項と制約事項

リソース使用率ダッシュボードの[ハードウェアリソース]タブは、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。ハードウェアリソースには、Nexus Dashboard Insights に表示されるオブジェクトへの直接マッピングはありません。ハードウェアの詳細を表示するコマンドでは、使用中のエントリの割合と、特定の機能に割り当てられたエントリの最大数は提供されません。Nexus Dashboard Insights は、Cisco Nexus 7000 シリーズ スイッチの[ハードウェアリソース]タブのリソースの異常と詳細ページを表示します。

[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。

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。

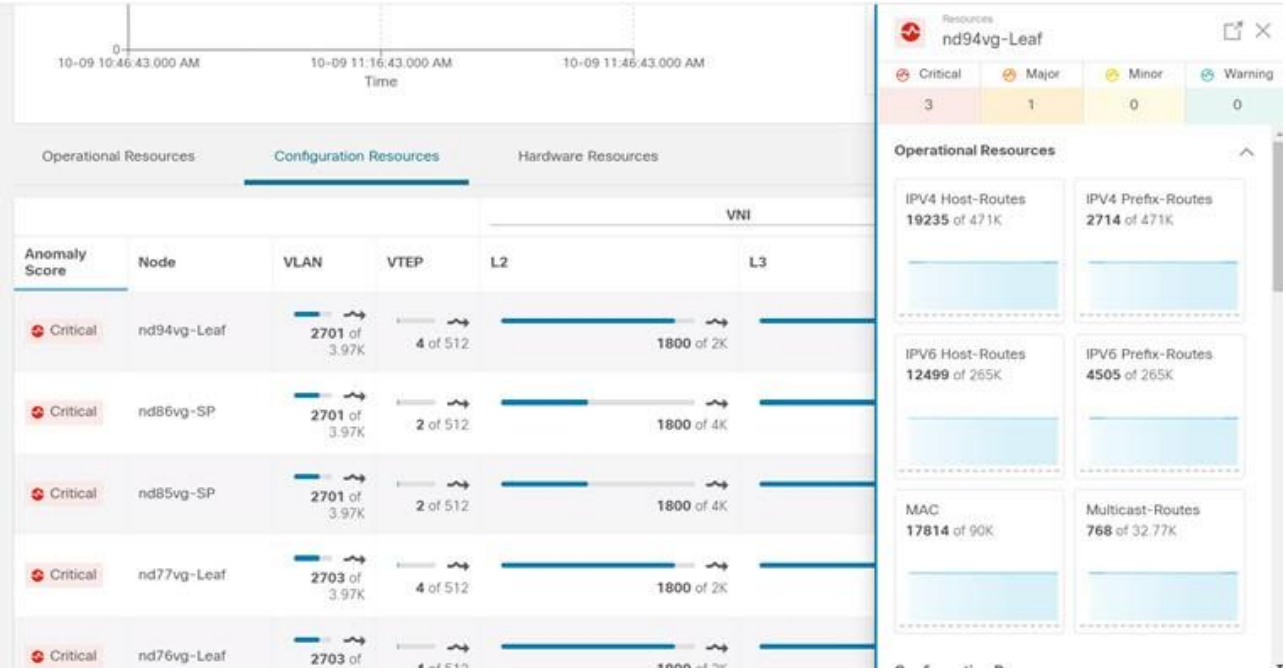
- == - 最初のフィルタタイプ。この演算子および後続の値を使用すると、完全一致のデータが返されます。
- != - 最初のフィルタタイプ。この演算子および後続の値を使用すると、同じ値を含まないすべてのデータが返されます。
- contains - 最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含むすべてのデータが返されます。
- !contains - 最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含まないすべてのデータが返されます。

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 • IPv4 ホストルート • IPv6 ホストルート • IPv4 プレフィックスルート • IPv6 プレフィックスルート • マルチキャスト ルート • VLAN • VRF • ポートの使用 • 入力ポートの帯域幅 • 出力ポート帯域幅 • CoPP • LPM • HRT • L2 QoS TCAM • L3 QoS TCAM • VTEP • VNI L2 • VNI L3 • VLAN • 入力 VLAN ACL • 出力 VLAN ACL • 入力ポート ACL • 入力ルーテッド ACL • 出力ルーテッド ACL

プロパティ	説明
運用リソース	異常スコア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 • IPv4 ホストルート • IPv6 ホストルート • IPv4 プレフィックスルート • IPv6 プレフィックスルート • マルチキャスト ルート
設定のリソース	異常スコアに基づいて設定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 • VLAN • VTEP • VNI ◦ L2 ◦ L3 • VRF

プロパティ	説明
ハードウェアリソース	異常スコアに基づいて設定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 • CoPP • LPM • HRT • QoS TCAM ◦ L2 ◦ L3 • VLAN ACL ◦ 入力 ◦ 出力 • ポート ACL ◦ 入力 • ルーテッド ACL ◦ 入力 ◦ 出力

- 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。
- [概要] 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。

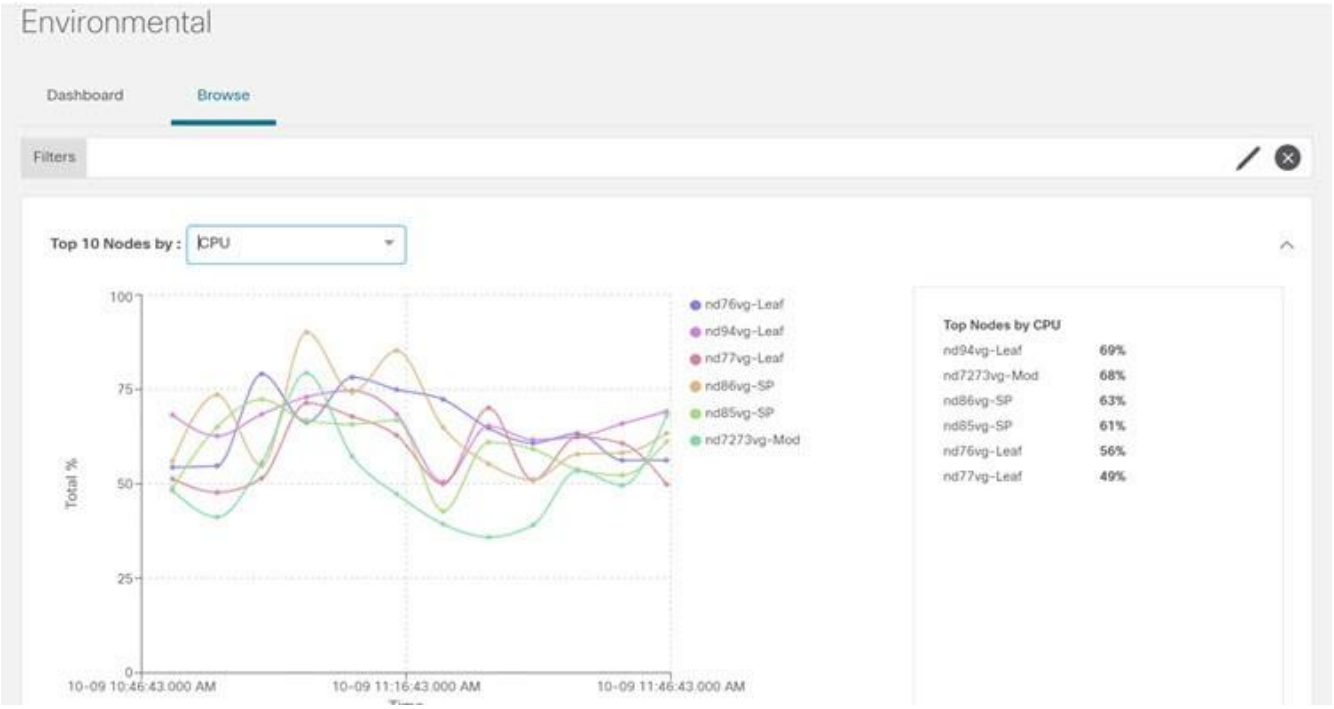
- [ノードの詳細]ページの**[アラート]**タブには、ノードで発生した異常が表示されます。

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
ノードの詳細	環境リソースタイプごとにノードの傾向の観察結果を表示します。

[使用率別の上位ノード]のノードカードをクリックして、*[環境の詳細]*ページを表示します。詳細には、一般的な情報、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。

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。

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。 • CPU (使用率) • メモリ(使用率) • 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] 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]、[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。

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。
- [インターフェイスタイプ] - 特定のインターフェイスタイプのみ表示されます。
- [プロトコル] - プロトコルのみ表示されます。
- [運用状態] - 特定の運用状態のノードを表示します。
- [管理状態] - 特定の管理状態のノードを表示します。

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。

プロパティ	説明
上位 10 のインターフェイスの表示基準	上位インターフェイスを次の基準で表示します。 • 送信側使用率 • 受信側使用率 • エラー
インターフェイス統計情報	異常スコアに基づいてインターフェイス統計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 • インターフェイス • インターフェイスタイプ • ノード • 受信側使用率 • 送信側使用率 • エラー
プロトコル統計	異常スコアに基づいてプロトコル統計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 • プロトコル • ノード • 応答数 • エラー

Nexus Dashboard Insights がノードからデータを受信するには、サイト内のすべてのノードが、ハードウェアテレメトリの PTP グランドマスターおよびソフトウェアテレメトリの NTP クロックと同期していることを確認します。Cisco NDFC ファブリック用の外部 NTP サーバーを使用してスイッチを設定する必要があります。

[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。

オプション(**[エラー]**、**[送信使用率]**、または**[受信使用率]**)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]**タブの**[上位インターフェイス]**領域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**[ネイバー]**タブの下に表示されます。L4-L7 カテゴリがサポートされています。

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。

DCNM で Nexus Dashboard Insights を使用する場合、ファブリックごとに 1000 の SVI がサポートされるため、ホスト側の SVI のみが表示されます。SVI の数がファブリックあたり 1000 を超えると、異常が発生します。このしきい値を超えると、動作は未定義になります。

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。

既存のファブリックで初めて Nexus Dashboard Insights サービスを開始するときは、NX-OS exec プロンプトで clear queuing burst-detect コマンドを実行して、マイクロバーストの履歴をクリアする必要があります。これは clear コマンドなので、プロンプト以外の応答はありません。これにより、新しいマイクロバーストを検出して適切な異常を生成する、クリーンなマイクロバースト状態が確保されます。

マイクロバーストの設定と監視

詳細については、「マイクロバーストの監視」を参照してください。

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。

[インターフェイス統計の概要]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. **[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が表示されます。
   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]*サイドビューペインで、フローを選択し、をクリックして[フローの詳細]ページを表示します。

マイクロバースト診断の影響と推奨事項

ノードのマイクロバースト出力インターフェイスおよびノードのその他の詳細は、フローデータベース内のフローレコードに関連付けられます。

1. **[アラートの分析]** > **[異常]**をクリックして、異常を参照します。
2. ResourceType == Interface; Description == Microburst でフィルタします。

3. 概要ペインに、異常のリストがマイクロバーストの重大度(マイナーまたはメジャー)とともに表示されます。
4. サイドペインで異常とマイクロバーストの重大度をクリックすると、影響を受けるオブジェクトが表示されます。
    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すると、影響を受けるエンティティと、影響を受けるオブジェクトに関連付けられている異常が表示されます。
5. サマリーペインで異常をクリックすると、詳細を示すサイドペインが開きます。
    a. サイドペインで**[分析]**をクリックすると、フローレコードの詳細が表示されます。
    b. サイドペインの右隅にあるをクリックします。

        フローレコードの詳細ページには、**[概要]**、**[アラート]**、および**[傾向]**タブが表示されます。

    c. **[概要]**タブをクリックします。[パスサマリー]セクションには、マイクロバースト異常が発生したノードが表示されます。
    d. **[アラート]**タブをクリックすると、マイクロバーストに関連する異常が表示されます。
    e. *[相互発生]*セクションで円をクリックすると、特定の時間に発生した異常が表示されます。

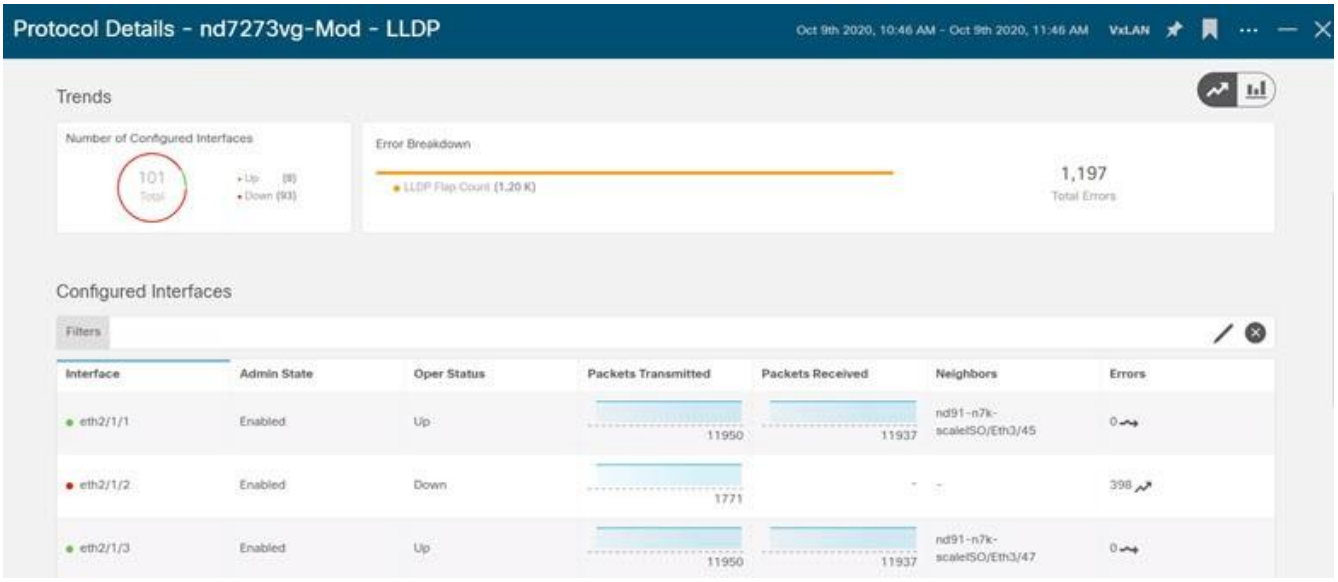
        相互発生は、マイクロバーストの影響を受ける集約されたフローを示します。影響を受ける個々のフローではありません。

プロトコル

Nexus Dashboard Insights の[参照]セクションには、タイプが CDP、LLDP、LACP、BGP 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[プロトコルサマリー]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、エラーなどのノードのプロトコルの詳細およびインターフェイス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]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。

[一般的な情報]セクションには、異常スコア、ノード名、プロトコル、ドメインの数、インターフェイスの数、およびプロトコルのグループの数が表示されます。

[異常]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]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、VRF が有効または無効な場合の管理状態、ランデブーポイントアドレスなどの基本情報を表示します。

- 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。
- ランデブーポイントアドレス(たとえば *1*)をクリックすると、IP アドレスの詳細を含むサイドペインが表示されます。これには、ランデブーポイントアドレスが参照するグループ範囲が含まれ、特定のランデブーアドレスのグループ範囲がリストされます。

[マルチキャスト PIM インターフェイス]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を示すサマリーテーブルが表示されます。特定の PIM インターフェイスの VRF、IP アドレス、指定ルータアドレス、ネイバーアドレス、および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。これには、ネイバーの統計情報、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]セクションでは、RPF 送信元、RPF ネイバー、VRF、グループアドレス、着信インターフェイス、および PIM グループに対して有効になっているフラグなど、PIM グループに関連する詳細が要約されています。

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 インターフェイスに関する特定のノードの概要を表示します。**[一般的な情報]**セクションには、異常スコア、ノード名、プロトコル、特定のノードで有効になっているインターフェイスの数、インターフェイスで有効になっているグループの数が表示されます。Cisco DCNM では、IGMP グループを VLAN で有効にすることも、インターフェイスで有効にすることもできます。

[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。

[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。インターフェイス名、VRF、IP アドレス、IGMP クエリア、メンバーシップ数、バージョン、およびエラーが表示されます。

IGMP インターフェイスは、特定のノードで 3 つの方法で設定できます。Nexus Dashboard Insights から設定することはできません。

- インターフェイスで PIM を有効にします。
- インターフェイスをプロトコルに統計的にバインドします。
- リンクレポートを有効にします。
- サイド ペインの行をダブルクリックして、追加のインターフェイスの詳細を表示します。詳細には、グループの有効化ステータス、エラーカウンター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その他のプロパティが含まれます。

[マルチキャストグループ]セクションには、送信元、マルチキャストグループ、VRF、バージョン、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。複数の発信インターフェイスがある場合があります。

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。VLAN では、IGMP はデフォルトで有効になっており、IGMP は情報を得るために VLAN でスヌープします。**[一般的な情報]**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 VLAN ごとに表示されます。

[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。

- **[アップ]**は、IGMP スヌープが有効になっているインスタンス数を表します。
- **[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]セクションには、VLAN ごとの情報が表示されます。これには、VLAN、管理状態、クエリアアドレス、クエリアバージョン、マルチキャストルーティング状態(有効または無効)、ノードクエリア状態(有効または無効)、およびエラーの概要が含まれます。

- 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。これには、VLAN 名、VLAN ID、有効または無効になっているプロパティ、統計の詳細、および 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]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、VLAN、バージョン、最後のレポータ、発信インターフェイスなどの詳細が表示されます。

マルチキャストプロトコル統計の制限事項

- PIM、IGMP、および IGMP スヌープのマルチキャスト統計プロトコルは、Cisco Nexus 9000 シリーズスイッチでのみサポートされています。
- PIM、IGMP、および IGMP スヌープのマルチキャスト統計プロトコルは、以下ではサポートされていません。
  - Cisco Nexus 7000 および 3000 シリーズ スイッチ。
  - Cisco N9K-X9636C-R、N9K-X9636Q-R、N9K-X96136YC-R、および N3K-C3636C-R ラインカード。
- Nexus Dashboard Insights がこれらのデバイスを管理モードでプログラムする場合、サポートされていないデバイスでは NXAPI エクスポートが有効にされないようにします。ファブリックが監視モードの場合、生成された設定では、サポートされていないデバイスに対する NXAPI コマンドが回避されます。直接スイッチ設定を使用してこれらのエクスポートを手動で設定し、これらの機能のデータがサポートされていないデバイスから取得される場合、Nexus Dashboard Insights GUI にマルチキャスト統計データが表示されることがあります。
- デバイスごとにサポートされるマルチキャストルートの合計(S、G、および*G を合わせて)は 8000 で、ファブリックあたり 64000 です。

プロトコル統計の制限事項

- CDP プロトコル統計は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。
- Nexus Dashboard Insights は、次の BGP PrefixSaved 統計をサポートしていません。
  - Cisco Nexus 3000、7000、および 9000 シリーズ スイッチ。
  - Cisco N9K-X9636C-R、N9K-X9636Q-R、N9K-X96136YC-R、および N3K-C3636C-R ラインカード。

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: 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**サービスによって監視されます。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、**警告**付きの異常が発生します。異常が 30 期間続く場合は、メジャー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 4. 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。	変化のペース > 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。	error-increase > 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 interfaceStomped カウンタが増加していないことを監視します。	error-increase > 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

Nexus Dashboard Insights の[フロー]セクションには、サイト内のさまざまなノードから収集された平均遅延、パケットドロップ表示、フロー移動表示など、フローで検出された異常が表示されます。

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]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。

フローのハードウェア要件

Cisco Nexus プラットフォームスイッチ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「Compatibility Information」セクションを参照してください。

フローのガイドラインと制約事項

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 Dashboard Insights リリースノートの「Compatibility Information」セクションを参照してください。

- N9K-C93180YC-EX、N9K-C93108TC-EX、および N9K-C93180LC-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。
- フローはマルチキャストトラフィックをサポートしていません。アクセスリストは、マルチキャストトラフィック フローを除外するようにプロビジョニングする必要があります。
- 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。
- **サイト概要**ダッシュボードの異常の数は、フロー参照ページの異常の数と一致しません。サイトダッシュボードには、選択した時間範囲の異常カウントの合計が含まれています。複数のフローレコードが同じ異常エントリを指す場合があるフローブラウズビューでは、フローレコードは集約されません。
- VXLAN フローが入力ノードでドロップされた場合、L3-VNI フローは L2-VNI フローとして表示されます。VXLAN パケットが最初のホップでドロップされると、エクスポートされた VXLAN フローテレメトリレコードにドロップが示されます。ただし、それらには VNI 情報が含まれていません。フロー テレメトリ エクスポートからの入力インターフェイスとインターフェイスに関連付けられた VRF は、フローが L2-VNI または L3-VNI のどちらであるかを推測しません。この場合、Nexus Dashboard Insights ではフローに L2-VNI を関連付けます。
- VXLAN カプセル化パケットが Cisco Nexus 9500-EX スイッチに入り、機能オーバーレイ(EVPN)が設定されている場合、パケットは VXLAN トランジットノードパケットのように扱われます。また、フロー テレメトリ エクスポートでは、入力インターフェイスと出力インターフェイスがゼロに設定されます。フローのこのレコードを考慮するには、入力および出力インターフェイスが必要です。こうしたスイッチの制限事項が原因で、スイッチが入力、トランジット、または出力方向にある場合、Cisco Nexus 9500-EX スイッチはパススティッチングおよび相関で考慮されません。Cisco Nexus 9500-EX スイッチは、オーバーレイパケットのトランジットノードのように扱われます。

- Nexus Dashboard Insights が VXLAN 展開で機能するには、オーバーレイに含まれるスイッチで対称設定が必要です。これにより、Nexus Dashboard Insights がオーバーレイフローを関連付けてつなぎ合わせることができます。このような対称設定が存在しない場合、VXLAN の機能と転送は機能しますが、Nexus Dashboard Insights はフローを正しくつなぎ合わせません。スイッチの対称設定の意味を理解するには、次の例を参照してください。
  - レイヤー2 VXLAN VNI の場合: vlan-x が PE1 の VNI-A にマッピングされている場合、同じ vlan-x を PE2 の VNI-A にマッピングする必要があります。ここで、PE1 と PE2 はレイヤー2 オーバーレイの VTEP エンドポイントです。
  - レイヤ 3 VXLAN VNI の場合: SVI-x が PE1 の VRF-A でマッピングされた VNI-P にマッピングされている場合、同じ SVI-x を PE2 の VRF-A でマッピングされた VNI-P にマッピングする必要があります。ここで、PE1 と PE2 は VTEP であり、レイヤ 3 オーバーレイのエンドポイントです。
- この ID は 'overlay-id' に使用されるため、論理インターフェイス ID のエンコードのためにフローテレメトリ 'tenant-id' を使用するすべてのインターフェイスで、入力および VRF 情報は表示されません。論理インターフェイス(トランクポートを持つ SVI、サブインターフェイス、トランクとポートチャネルを持つ SVI)を導出し、それに関連付けられた VRF を取得することはできません。これを行うと、フローの参照ページと詳細ページに入力および出力 VRF が表示されなくなります。
- 現在の設計では、VPC ペアに接続された Cisco Nexus 9500-EX スイッチの VPC ペア間の入力リーフノードの識別が制限されており、その結果 Nexus Dashboard Insights でフローが失われます。
- インデックスに 2900 万の異常がある場合、フローデータベースの書き込みが遅すぎるため、ソフトウェアテレメトリとフローテレメトリでサポートされている 350 のノードで、KAFKA のラグが発生します。KAFKA のラグの結果、Nexus Dashboard Insights のユーザーインターフェイスにデータが部分的に表示されるようになります。
- フロー情報は 7 日間、またはフローデータベースが 80%に達するまで(どちらか早い方)保持され、その後、古いフロー情報はデータベースから削除されます。
- Cisco Nexus FX スイッチで出力 ACL の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。
- Nexus Dashboard Insights がフローテレメトリデータを受信するには、ing-netflow の TCAM リージョンを 512 に設定する必要があります。Nexus 9000 TCAM Carving を参照してください。

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 DCNM 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。フローエンジンは、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]ページには、アクティブノード、入力ノード、出力ノード、およびサイトノードの異常を表示するフローコレクションフィルタが表示されます。

[フローレコードの参照]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。

プロパティ	説明
ノード	フローが報告されるすべてのノードを表示します。

プロパティ	説明
フィルタ	次のフィルタでソートされた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 VRF • 送信元 VNI • 出力ノード • 出力 VRF • 宛先 VNI
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。

プロパティ	説明
トップ フロー	次の項目で最高のスコアを獲得した、サイト全体の上位フローを一覧表示します。 • **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。 • **記録時間** - ノードフローは、選択した開始時間と終了時間の間の個々の記録時間にキャプチャされます。フローは、個々のレコード時間にキャプチャされるフローについて複数のエントリを記録します。 • **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

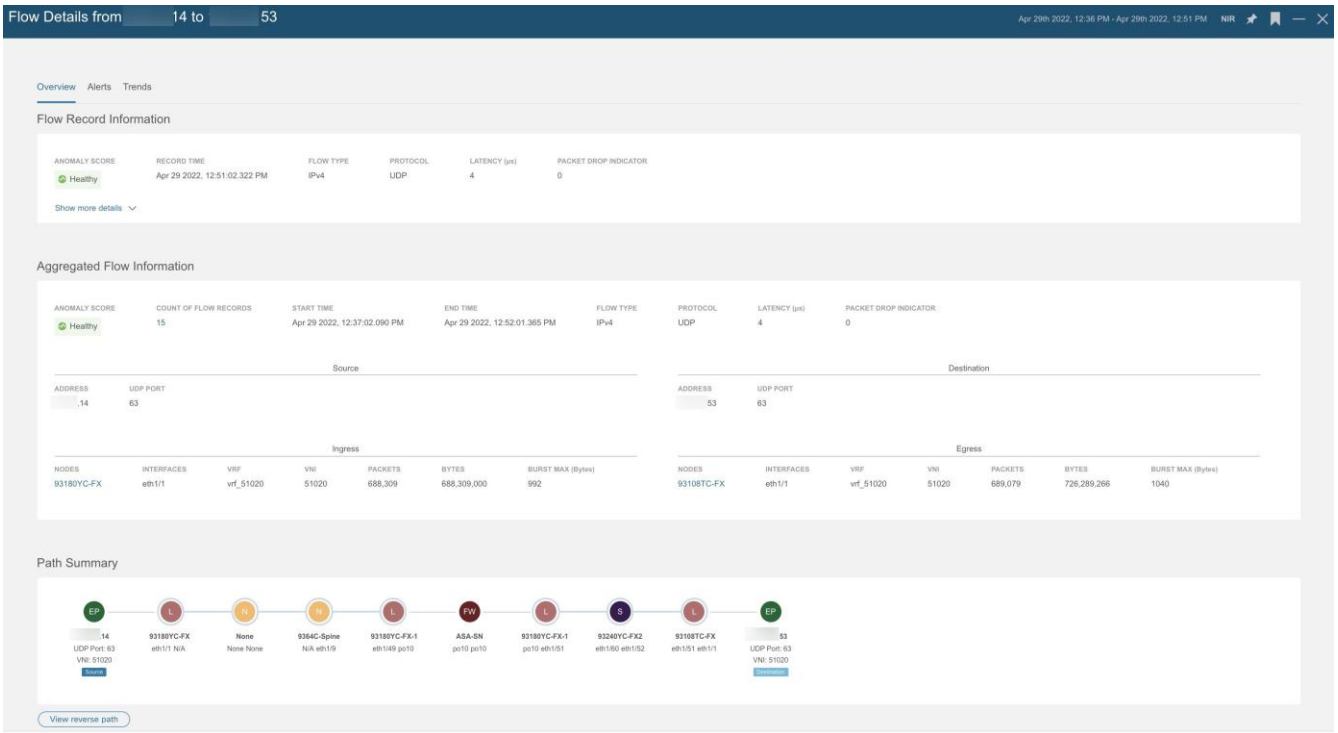
Nexus Dashboard Insights リリース 6.1.1 以降、フローパスの可視性をファイアウォールなどの L4-L7 外部デバイスに拡張できるようになりました。Nexus Dashboard Insights は、サービスチェーン全体のエンドツーエンドフローをリアルタイムで追跡し、デバイスサイロ全体のデータプレーンの問題を特定するのに役立ちます。現在のリリースでは、すべてのサードパーティベンダーの非 NAT 環境がサポートされています。

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。

[パスの概要]領域では、送信元から宛先までのエンドツーエンドの情報がグラフィカルなフローパスで表示され、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]**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]**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ガイドラインと制約事項

- この機能は現在、NDFC の L4-L7 サービス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。
- サービスノードが直接接続されている場合は、サービスノードのタイプが検出されます。ただし、複数のサービスノードが同じ物理ポートに接続されている場合、Nexus Dashboard Insights は正確なサービスノードのタイプ情報を識別しません。その結果、不明なサービスノードとして識別されます。
- 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。
- 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契約がないため、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て、フロールールが設定されている場合、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。

Nexus Dashboard 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 DCNM 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]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。

- **Cisco ACL ドロップ** - パケットが sup-tcam ルールに抵触していて、そのルールがパケットをドロップするルールである場合、ドロップされたパケットは ACL_Drop としてカウントされ、転送ドロップカウンタでカウントされます。これが発生した場合、通常は、パケットが基本的な Cisco ACI の転送の原則に反する転送をされようとしていることを意味します。sup-tcam ルールは主に一部の例外やコントロールプレーンのトラフィックを処理するためのものであり、ユーザーがチェックしたりモニタしたりするようには意図されていません。
- **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宛先 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。ポリシードロップは、通信を許可する契約がないために発生します。

- **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。

TCP パケット RTO の異常は、Cisco DCNM ではサポートされていません。

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の異常が集約されます。たとえば、T0 から T1 の間にパケットドロップの異常が発生したとします。時刻 T1 から T2 まではパケットドロップの異常は発生していません。時刻 T2 から T3 にかけて、別のパケットドロップの異常が発生しました。T1 から T2 まで異常がないにもかかわらず、集約されたパケットドロップの異常のタイムスタンプは T0 から T3 となります。
- 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 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]** > **[異常]**をクリックして、異常を参照します。
2. カテゴリ別フィルタ==フロー
3. リソースタイプが **flowEvent** の異常をクリックします。
4. サイドペインで**[分析]**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、推定される影響、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]**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、およびバッファドロップの異常を表示します。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。

ホスト オーバーレイ フロー モニタリング

Cisco DCNM でのホスト オーバーレイ フロー モニタリングおよびフロートラフィック分析により、サイトで次のことが可能になります。

- サーバーVTEP からのオーバーレイでの IPv4 および IPv6 ホストフローの監視。
- ホストオーバレイフローの VNI、ファブリック入力、ファブリック出力インターフェイスに関する情報を提供します。
- ファブリック内のホストオーバーレイフローのネットワークパス、ファブリック内のホストオーバーレイフローで発生したドロップ、パケットカウント、バイトカウント、およびトラフィックのバースト情報に関する情報を提供します。

トランクおよびサブインターフェイスの入力インターフェイスには、サイト VRF が表示されません。

従来のファブリックタイプは、ホスト オーバーレイ フロー モニタリングでサポートされています。VXLAN ファブリックタイプは、ホスト オーバーレイ フロー モニタリングではサポートされていません。Cisco DCNM サイトが従来のサイトタイプとして設定されている場合、次のフローテレメトリが収集されます。

- ホスト アンダーレイ フロー トラフィックは、従来のフローとして関連付けられます。
- オーバーレイフローは、ホスト オーバーレイ フロー トラフィックとして関連付けられます。
- インターフェイスから VLAN へのマッピングを収集するためのノード設定は、テレメトリマネージャによって行われます。

ホスト オーバーレイ フロー モニタリングの設定

1.  > **[NI セットアップ] > [データ収集のセットアップ] > [設定の編集]**をクリックします。
2. *[データ収集のセットアップ]*ページで、サイトを選択します。
   a. *[モード]*列でモードを選択します。
   b. 選択したサイトの*[フローテレメトリ ACL 設定ステータス]*を有効にします。
   c. 選択したサイトの*[ソフトウェアテレメトリ設定ステータス]*を有効にします。
   d. *[VXLAN/クラシック]*列で**[従来型]**を選択します。
3. [保存（Save）] をクリックします。

ホスト オーバーレイ フロー モニタリングのガイドラインと制限事項

- 従来のファブリックタイプはサポートされています。
- VXLAN ファブリックタイプはサポートされていません。
- Cisco Nexus 9000 -FX、-FX2、および-GX プラットフォームスイッチはサポートされています。

ホスト オーバーレイ フロー モニタリングの参照

1. **[参照] > [フロー]**をクリックします。
2. ノードでフィルタリングします。
3. 概要ペインで異常をダブルクリックします。
4. *フローレコードの詳細*ページが開き、**[概要]**、**[アラート]**、および**[傾向]**タブが表示されます。

   *[フローレコード情報]*セクションには、フロータイプ、プロトコル、および異常スコアが表示されます。*[集約フロー]*セクションには、送信元と宛先の IP アドレス、VLAN 情報が記載されています。*[パスサマリー]*セクションには、送信元、宛先、ノード/インターフェイスの詳細、パケット例外(サイトの外部データパケットの転送ドロップ、バッファドロップなど)が表示されます。

5. 概要ペインで異常をクリックすると、一般情報、送信元、入力、およびフロータイプを含むサイドペインが表示されます。

   ホストオーバーレイフローの場合、参照テーブルの*[論理カプセル化]*列には、フローの VNI 情報が表示されます。

エンドポイント

Nexus Dashboard Insights の[エンドポイント]セクションには、Cisco DCNM 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 - エンドポイントの検出設定および運用情報を表示します。

エンドポイントでは次の異常が検出されます。

- 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
- IP アドレスが重複しているエンドポイント
- 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
- 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]**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]** > **[エンドポイント]**をクリックします。
4. **[エンドポイント]**ページの**[参照]**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。

- テーブル内のエンドポイント異常をダブルクリックして、*[エンドポイントの詳細]*ページを表示します。
- または、サイドバーのサマリーテーブルでエンドポイントをクリックして、設定、動作、エンドポイントのステータス、および異常に関する追加の詳細を表示します。
- サイドペインの右上隅にあるアイコンをクリックして、*[エンドポイントの詳細]*ページを表示します。

エンドポイント分析の一部として次の異常が検出されます。

- 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
- 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

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。

エンドポイントの表示、並べ替え、およびフィルタ処理は作業ウィンドウで行えます。**[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。

- [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。
- [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。テスト環境ではベータとマークされた機能を使用し、実稼働環境では使用しないことをお勧めします。

- [カプセル化] - 特定のカプセル化を行ったノードを表示します。
- [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

*[概要]*タブには、エンドポイントに関する一般情報が表示されます。*[エンドポイントの詳細]*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的な情報が表示されます。[設定]セクションには、選択したエンドポイントの MAC アドレス、BD、VRF、およびカプセル化の詳細が表示されます。[操作]セクションには、ノード名、インターフェイス、VM ID、ハイパーバイザーID、およびその他の詳細が表示されます。

このページには、*[エンドポイント履歴]*、*[IP 履歴]*、および*[重複]*も一覧表示されます。

*[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。インターフェイス間およびノード間を一定期間の間に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。

L2 エンドポイントには VLAN 情報があり、L3 エンドポイントには VRF 情報があります。

*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。

*[重複]*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。重複する IP アドレスは、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に発生します。

*[アラート]*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]**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。

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ガイドラインと制約事項

- Cisco DCNM 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 NDFC ファブリック用の外部 NTP サーバーを使用してスイッチを設定する必要があります。
- Cisco Nexus Dashboard Insights リリース 6.0.1 以降、すべてのフローは、サイトタイプ ACI および 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。
- **[フローの編集]**ページでは、3 つすべてを有効にすることも、製品に最適なモードを選択することもできます。 sFlow は最も制限が厳しく、Netflow では機能が増え、フローテレメトリには最も多くの機能があります。そのため、お使いの設定で利用可能な場合は、フローテレメトリを有効にすることをお勧めします。フローテレメトリが利用できない場合は、Netflow を使用します。Netflow が使用できない場合は、sFlow を使用します。
- 特定のノード(サードパーティのスイッチなど)がフローテレメトリでサポートされていない場合でも、Cisco Nexus Dashboard Insights は、パス内の前後のノードからの LLDP 情報を使用して、スイッチ名と入力および出力インターフェイスを識別します。
- 設定で必要な場合は、ユーザーがフローテレメトリ、Netflow、および sFlow のトグルボタンを有効にすることができます。
- フローテレメトリは、以下をサポートします。
  - 20,000 ユニークフロー/秒(物理的基準)
  - 10,000 ユニークフロー/秒(物理的に小規模)
  - 2,500 ユニークフロー/秒(vND)
- Cisco Nexus Dashboard Insights にオンボードされた複数の DCNM クラスタがある場合、サイトごとに部分的なパスが生成されます。
- Cisco Nexus Dashboard Insights およびフローテレメトリのサポートで使用するファブリックを手動で設定した場合、フローエクスポータポートが 30000 から 5640 に変更されます。フローエクスポータの破損を防ぐには、オートメーションを調整します。

- Nexus ダッシュボードは、フロー異常の Kafka エクスポートをサポートしています。ただし、フローイベントの異常では、Kafka エクスポートは現在サポートされていません。
- フローテレメトリは、次の NX-OS バージョンの-FX3 プラットフォームスイッチでサポートされています。
  - 9.3(7)以降
  - 10.1(2)以降
  - フローテレメトリは、NX-OS バージョン 10.1(1)の-FX3 プラットフォームスイッチではサポートされていません。

フローテレメトリの設定

はじめる前に

ユーザーは、推奨設定を使用して適切なスイッチを設定する必要があります。詳細については、「Nexus Dashboard Insights のスイッチ設定ステータス」を参照してください。

手順

次の手順でフローテレメトリを設定します。

1. **[概要]**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]メニューをクリックし、**[サイトグループの設定]**を選択します。
3. **[サイトグループの設定]**ページで、**[フロー]**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]**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]**ページの**[フロー収集モード]**領域で、**[フローテレメトリ]**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。
6. [保存（Save）] をクリックします。
7. **[フローテレメトリルール]**領域に、フィルタが表示されます。
8. ルールを追加するには、**[追加]**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]**領域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 または宛先 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]** > **[フロー]**をクリックし、**[ダッシュボード]**タブをクリックします。
2. **[サイトグループ]**と**[スナップショット]**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]**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すべてのフローの概要を表示します。

関連する異常スコア、レコード時間、フローテレメトリを送信するノード、フロータイプ、入力ノードと出力ノード、および追加の詳細が表形式で表示されます。テーブル内の特定のフローをクリックすると、特定のフローテレメトリに関する特定の詳細がサイドバーに表示されます。サイドバーで[詳細]アイコンをクリックすると、より大きなページに詳細が表示されます。このページでは、他の詳細に加えて、送信元と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 5. 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 注: ユーザーがホスト側のインターフェイスのみを監視している場合は、ポートチャネルのサポートを利用できます。	はい	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

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

Full Netflow

Full NetFlow では、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。エイリアシング(フローテーブル内の同じエントリにハッシュする複数のフロー)の場合を除いて、すべてのフローはそれぞれのパケットレートに関係なく監視できます。

サンプル NetFlow

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

NetFlow のガイドラインと制約事項

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

NetFlow の設定

はじめる前に

ユーザーは、推奨設定を使用して適切なスイッチを設定する必要があります。

詳細については、「Nexus Dashboard Insights のスイッチ設定ステータス」を参照してください。

手順

次の手順で NetFlow を設定します。

1. **[概要]**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]メニューをクリックし、**[サイトグループの設定]**を選択します。
3. **[サイトグループの設定]**ページで、**[フロー]**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]**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]**ページの**[フロー収集モード]**領域で、**[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。
6. [保存（Save）] をクリックします。

NetFlow プロセスが開始されます。

sFlow

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

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

sFlow では、次のインターフェイスがサポートされています。

表 6. sFlow でサポートされるインターフェイス

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

sFlow の注意事項および制約事項

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

sFlow の設定

はじめる前に

ユーザーは、推奨設定を使用して適切なスイッチを設定する必要があります。詳細については、「Nexus Dashboard Insights のスイッチ設定ステータス」を参照してください。

手順

次の手順で sFlow テレメトリを設定します。

1. **[概要]**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]メニューをクリックし、**[サイトグループの設定]**を選択します。
3. **[サイトグループの設定]**ページで、**[フロー]**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]**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]**ページの**[フロー収集モード]**領域で、**[sFlow]**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。
6. [保存（Save）] をクリックします。

sFlow プロセスが開始されます。

SR-MPLS フロー - ベータ機能

NX-OS ファブリックの SR-MPLS フロー

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

リリース 6.1.1 以降、Nexus Dashboard Insights では次の領域の SR-MPLS フローをサポートします。

- NX-OS ファブリックでの SR-MPLS フローのフロー分析
- 関連する**[トランスポート]**および**[VPN]**ラベルを持つフロー情報
- **[VPN]**ラベルでフローを検索する機能

SR-MPLS は、Nexus Dashboard Insights の次の領域をサポートします。

- SR-MPLS ラベルでカプセル化されたフローのフロー分析
- フローに関連付けられたラベルを使用して、内部フローのフローパスを提供する
- SR-MPLS フローパスの変更内容を、変更されたパスに関連付けられたラベルとともに提供する
- ホップごとのトランスポートラベルを提供し、ラベル操作がフローで実行される
- フローで使用されるエンドツーエンドの VPN ラベルを提供する
- SR-MPLS フローで発生するエンドツーエンドの遅延を提供する
- SR-MPLS フローの最大バースト、パケット、およびバイトカウンタを提供する
- SR-MPLS フローの転送、バッファ、ACL、および QoS ドロップなどのドロップ表示を提供する
- 特定のトランスポートまたは VPN ラベルに一致するフローの検索機能を提供する(フローがフローテレメトリ分析を使用して追跡されている場合)

サポートされているプラットフォームは次のとおりです。

- SR-MPLS フロー分析は、NX-OS ファブリックでのみサポートされます。
- NX-OS でサポートされるプラットフォームは ToR と EoR です。
  - Nexus 9300-GX プラットフォームスイッチ
  - Nexus 9300-FX プラットフォームスイッチ
  - Nexus 9300-FX2 プラットフォームスイッチ
- NX-OS のサポートされるリリース 10.2.3F
- Nexus Dashboard リリース 2.2
- DCNM リリース 11.5.3 および NDFC リリース 12.0.2

サポートされるトポロジ

以下のトポロジがサポートされます。

- リーフ/スパイン/リーフ
- リーフ/スパイン/スーパースパイン/スパイン/リーフ
- ボーダースパイン(ボーダースーパースパインのケースはサポートされていません)

エンドツーエンドの遅延のみがサポートされます。

NX-OS 向けの SR-MPLS フローのワークフロー

NX-OS ファブリックで SR-MPLS フローのフローをセットアップして監視するには、次のワークフローシーケンスに従います。

1. **SR-MPLS ファブリックタイプを使用してサイトグループを設定します。**新しいサイトグループを追加する場合、いずれかの手順で、**[設定]**ダイアログボックスの**[一般設定]**領域で**ファブリックタイプ**を選択する必要があります。**[ファブリックタイプ]**フィールドのドロップダウンリストから**[SR-MPLS]**を選択し、残りの手順を完了する必要があります。サイトグループの追加方法の詳細については、「Cisco Nexus Dashboard Insights 0 日目のセットアップの基本設定」または「サイトグループの追加」(お使いのセットアップに該当するもの)を参照してください。
2. **フローの設定**: SR-MPLS ファブリックタイプのサイトグループに必要なフローを設定します。詳細については、「フローの設定」を参照してください。
3. **SR-MPLS フローの表示**: GUI の[ナビゲーション]ペインで、**[参照]** > **[フロー]**をクリックして、目的のフローを表示します。詳細については、「SR-MPLS フローの表示」を参照してください。

SR-MPLS フローの表示

GUI のナビゲーションペインで、お使いのサイトグループの**[参照]** > **[フロー]**をクリックします。**[フロー]**ページで、**[参照]**タブをクリックします。**[フローの個別レコード]**テーブルでは、他の列に加えて、**[VPN]**列と**[トランスポート]**列、およびそれらのラベル値がテーブルの**[入力]**と**[出力]**領域に表示されます。**[VPN]**と**[トランスポート]**のラベル値は数値です。VPN は単一の値であり、トランスポートは値のリストである場合があります。

[参照]タブの**[フィルタ]**フィールドで特定のラベルを検索すると、関連するフローが[異常]テーブルに表示されます。[異常]テーブルの適切な行をクリックして、概要ペインを開きます。概要ペインの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。

[フローの詳細]ページには、**[フローレコード情報]**、**[集約されたフロー情報]**、および**[フローパスの概要]**領域が表示されます。**[フローの詳細]**ページの**[集約されたフロー情報]**領域では、[入力]および[出力]領域で**[VPN ラベル値]**を表示できます。

[フローパスの概要]領域で、パスの各セグメントにカーソルを合わせると、**[VPN]**ラベルとその値を表示できます。**[トランスポート]**ラベルはすべてのホップに存在します。ノード上のすべてのインターフェイスに、**[表示]**リンクがあります。ホップの下の**[表示]**リンクにカーソルを合わせると、トランスポートの詳細が表示されます。

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。

ファームウェアアップデート分析機能は、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]** > **[ファームウェアアップデート分析]**を選択します。
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]**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]** > **[アドバイザリ]**を選択します。PSIRT アドバイザリを選択し、**[分析]**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。

b. [Next] をクリックします。

7. **[ノードの選択]**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ノードは 10 個だけです。

   b. [追加（Add）] をクリックします。

8. [保存（Save）] をクリックします。

9. ファームウェアアップデート分析ジョブは、**[ファームウェアアップデート分析]**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]**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]**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]**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適用され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]**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 DCNM 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]**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、**[分析を再実行]**をクリックして検証します。

13. **[更新後の分析]**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]**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]**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]**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]**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]**をクリックします。

Cisco DCNM の事前検証基準

事前検証基準	説明	リリース
デバイスに接続できませんでした	この検証では、すべてのデバイスが接続されているかどうかを確認します。	6.0.1

事前検証基準	説明	リリース
モジュールが ok/アクティブ/スタンバイ状態かどうかを確認してください	この検証では、すべてのモジュールがオンラインかどうかを確認します。	6.0.1
モジュールで例外ログメッセージが見つかりました	この検証では、ユーザーが開始していないリセットを確認します。	6.0.1
デバイスでコアファイルが見つかりました	この検証では、コアファイルを確認します。	6.0.1
HA スタンバイのないアクティブなスーパーバイザが見つかりました	この検証では、デュアル スーパーバイザ システムの冗長ステータスを確認します。	6.0.1
1 つ以上のポートチャネルメンバーが稼働していません	この検証では、すべてのポートチャネルメンバーが稼働状態であるかどうかを確認します。	6.0.1
ユーザーが開始していないシステムリセットが見つかりました	この検証では、システムリセットがユーザーが開始した以外の理由によるものであるかどうかを確認します。	6.0.1
ユーザーが開始していないモジュールリセットが見つかりました	この検証では、モジュールリセットがユーザーが開始した以外の理由によるものかどうかを確認します。	6.0.1
正常な状態ではなく、バックアップ電源のないモジュールが見つかりました	この検証では、すべてのモジュールが正常な状態であり、バックアップ電源が存在するかどうかを確認します。	6.0.1
モジュールで FAILURE/ABORT/INCOMPLETE/ ErrorDisabled が見つかりました	この検証では、すべてのモジュールで FAILURE/ABORT/INCOMPLETE/ ErrorDisabled の結果を確認します。	6.0.1
検出された vPC ステータスが稼働状態ではありません	この検証では、vPC ステータスが稼働状態であるかどうかを確認します。	6.0.1
検出された vPC スティッキビットが false です	この検証では、vPC スティッキビットが false であるかどうかを確認します。	6.0.1
検出された vPC ロールがセカンダリではありません	この検証では、vPC ロールがセカンダリであるかどうかを確認します。	6.0.1
検出された OSP が FULL FULL/DR 状態です	この検証では、OSPF インターフェイスとプロセスの稼働時間の安定性を確認します(12 時間) 。	6.0.1
検出された BGP セッションが稼働状態ではありません	この検証では、BGP ネイバーの稼働時間の安定性を確認します(12 時間)。	6.0.1
検出された HSRP MGO の状態がアクティブ/スタンバイではありません	この検証では、HSRP MGO の状態がアクティブ/スタンバイであるかどうかを確認します。	6.0.1

事前検証基準	説明	リリース
検出された ARP が不完全な状態です	この検証では、ARP が不完全な状態にあるかどうかを確認します。	6.0.1
続行するのに十分な空き容量がありません	この検証では、ブートフラッシュの空き領域がしきい値の 5GB を超えているかどうかを確認します。	6.0.1
使用率が 85%を超えるファイルシステムが見つかりました	この検証では、すべてのファイルシステムの使用率が 85%以下であるかどうかを確認します。	6.0.1
検出されたコンソールレジスタビットが RTS、DTR、または DSR ではありません	この検証では、コンソールレジスタビットが RTS、DTR、または DSR であるかどうかを確認します。	6.0.1
重大度 1、2、または 3 のメッセージが見つかりました	この検証では、重大度 1、2、または 3 のメッセージを確認します。	6.0.1
ISSU の影響チェックが破壊的でした	この検証では、ISSU が破壊的か非破壊的かを確認します。	6.0.1
すべてのスパインが同じアップグレードグループで選択されているか、一部のノードで使用可能な冗長スパインがありません	この検証では、トラフィックの損失を避けるために、スパインノードが少なくとも 2 つの個別のグループでアップグレードされているかどうかを確認します。	6.0.2
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回避するために、ノードに非冗長接続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。

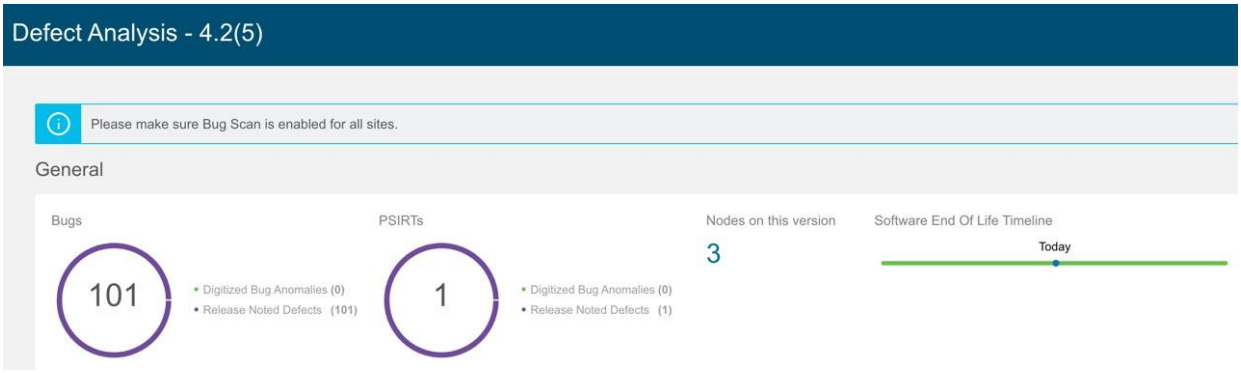
はじめる前に

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]** > **[アプリケーション]** > **[バージョン情報]**を選択します。
    a. **[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。

2. **[概要]**ページで、**[ダッシュボード]**を選択します。
   a. [異常の概要]ドロップダウンリストから、**[ファームウェア]**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]**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]**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]**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 はまだ確認できませんが、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]**または**[リリースノートの不具合]**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]**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]**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]**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]** > **[ファームウェアアップデート分析]**を選択します。
   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]**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]**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]**をクリックします。

DNS の統合

DNS の統合について

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。Nexus Dashboard Insights はファイルの整合性を検証します。必要に応じて、GUI からファイルをダウンロードまたは削除することもできます。

VRF またはサイト名が指定されていない場合、DNS は、**[統合の追加]**ページの**[関連付け]**セクションでの選択に基づいて、DNS サーバーが設定されているサイトに適用されます。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。

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。

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。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、Nexus Dashboard Insights では、トランザクションを開始するゾーンの TSIG キーを設定できます。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。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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

2. **[統合の管理]**ページで、**[統合の追加]**をクリックします。

3. **[統合の追加]**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. **[設定]**領域で、次の操作を実行します。

    a. **[DNS タイプ]**フィールドで、タイプとして**[マッピングファイル]**を選択します。

    b. **[名前]**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]**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]**領域で、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]**領域で、**[関連付けの追加]**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]**をクリックして設定を完了します。

[統合の管理]ページの**[統合]**領域には、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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

   [統合の管理]ページの**[統合]**領域には、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 設定を編集するには、**[統合]**テーブルで[アクション]アイコンをクリックし、**[編集]**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]**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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

   [統合の管理]ページの**[統合]**領域には、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 設定を削除するには、**[統合]**テーブルで[アクション]アイコンをクリックし、**[削除]**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 またはサイト名情報を含めることができます。サイト名を含むファイルがある場合、VRF の指定はオプションです。

json 形式

```
[
  {
          "recordType": "dnsEntry",
          "fqdn": "host1.cisco.com",
          "ips": ["1.1.0.0"],
          "vrf": "vrf-1",
          "siteName": "swmp3",
   },
  {
          "recordType": "dnsEntry",
          "fqdn": "host2.cisco.com",
          "ips": ["1.1.0.1"],
          "vrf": "vrf-1",
          "siteName": "swmp3",
   }
 {
           "recordType": "dnsEntry",
           "fqdn": "host3.cisco.com",
           "ips": ["1.1.0.2"],
 },
]です
```

.csv 形式

```
recordType,fqdn,ips,siteName,vrf
dnsEntry,swmp3-leaf1.cisco.com," 101.22.33.44" ,swmp3,vrf-1
dnsEntry,swmp5-leaf1.cisco.com," 10.2.3.4,10.4.5.6,1.2.3.4" ,fabric2,vrf-
2 dnsEntry,swmp4-leaf1.cisco.com, " 1.1.1.1" ,,,
```

クエリ用の DNS サーバーオンボーディングの設定

クエリサーバー方式を使用して DNS サーバーオンボーディングを設定するには、次の手順に従います。

手順

1. Cisco Nexus Dashboard Insights の**[概要]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。
2. **[統合の管理]**ページで、**[統合の追加]**をクリックします。
3. **[統合の追加]**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. **[設定]**領域の**[DNS タイプ]**フィールドで、タイプとして**[クエリサーバー]**を選択します。
5. **[名前]**フィールドに、統合の名前を入力します。
6. **[DNS サーバー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]**領域で、**[関連付けの追加]**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]**をクリックしてタスクを完了します。

[統合の管理]ページの**[統合]**領域には、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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

[統合の管理]ページの**[統合]**領域には、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 設定を編集するには、**[統合]**テーブルで[アクション]アイコンをクリックし、**[編集]**をクリックします。
3. **[セカンダリコントローラ]**領域で、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]**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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

[統合の管理]ページの**[統合]**領域には、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 設定を削除するには、**[統合]**テーブルで[アクション]アイコンをクリックし、**[削除]**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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

2. **[統合の管理]**ページで、**[統合の追加]**をクリックします。
3. **[統合の追加]**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. **[設定]**領域の**[DNS タイプ]**フィールドで、タイプとして**[ゾーン転送]**を選択します。
5. **[名前]**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]**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]**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]**領域で、[ゾーン名]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]**領域で、**[関連付けの追加]**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]**をクリックしてタスクを完了します。

[統合の管理]ページの**[統合]**領域には、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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

   [統合の管理]ページの**[統合]**領域には、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 設定を編集するには、**[統合]**テーブルで[アクション]アイコンをクリックし、**[編集]**をクリックします。
3. **[統合の編集]**ダイアログボックスの**[ゾーン]**領域で、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]**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]**ページで、[設定]アイコン > **[統合]** > **[管理]**をクリックします。

[統合の管理]ページの**[統合]**領域には、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 設定を削除するには、**[統合]**テーブルで[アクション]アイコンをクリックし、**[削除]**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]**ページで、[設定]アイコン > **[アプリケーション]** > **[セットアップ]**をクリックします。**[基本設定]**ページの**[サイトグループのセットアップ]**領域で、**[設定の編集]**をクリックします。**[サイトグループのセットアップ]**ページで、**[統合]**タブをクリックして**[統合]**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も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]**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 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ためのインサイトを提供します。

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、収集した情報をサイトノードから収集され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。アプリケーション固有の情報が豊富な AppDynamics コントローラからのこのデータは、Nexus Dashboard Insights に送信されるため、サイトノードを通過するトラフィックが Cisco Nexus Dashboard Insights に提供されます。

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 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。

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]**ページで、**[設定]**アイコン > **[統合]** > **[管理]**をクリックします。
2. **[統合の追加]**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。

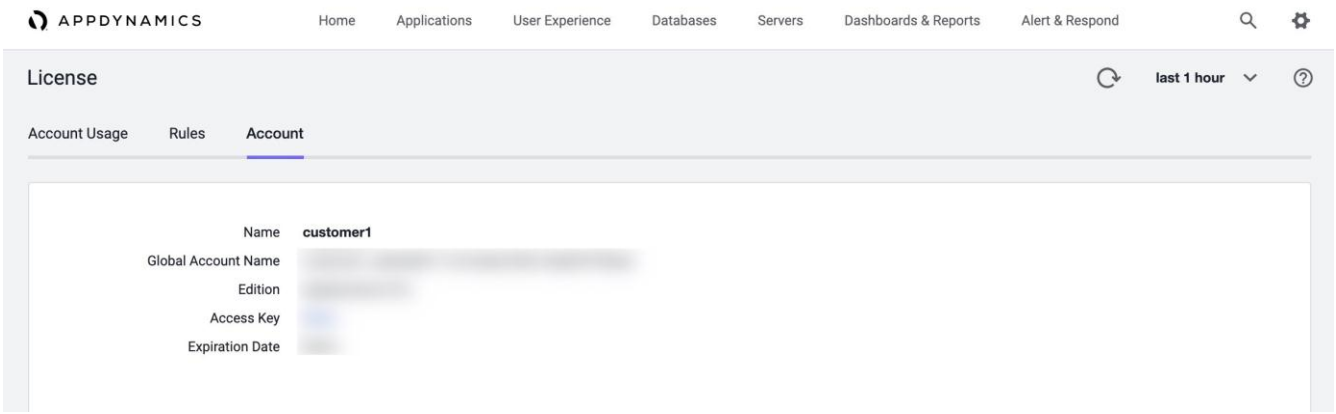
    > AppDynamics コントローラ名を Nexus Dashboard サイト名と同じにすることはできません。

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]** > **[インフラストラクチャ]** > **[クラスタ設定]** > **[プロキシ設定]**を選択して、プロキシを設定します。

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] (歯車アイコン) > [ライセンス] > [アカウント]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]**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]**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]**ページに表示されます。**[ステータス]**が[アクティブ]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]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]**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。

Cisco 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]**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。

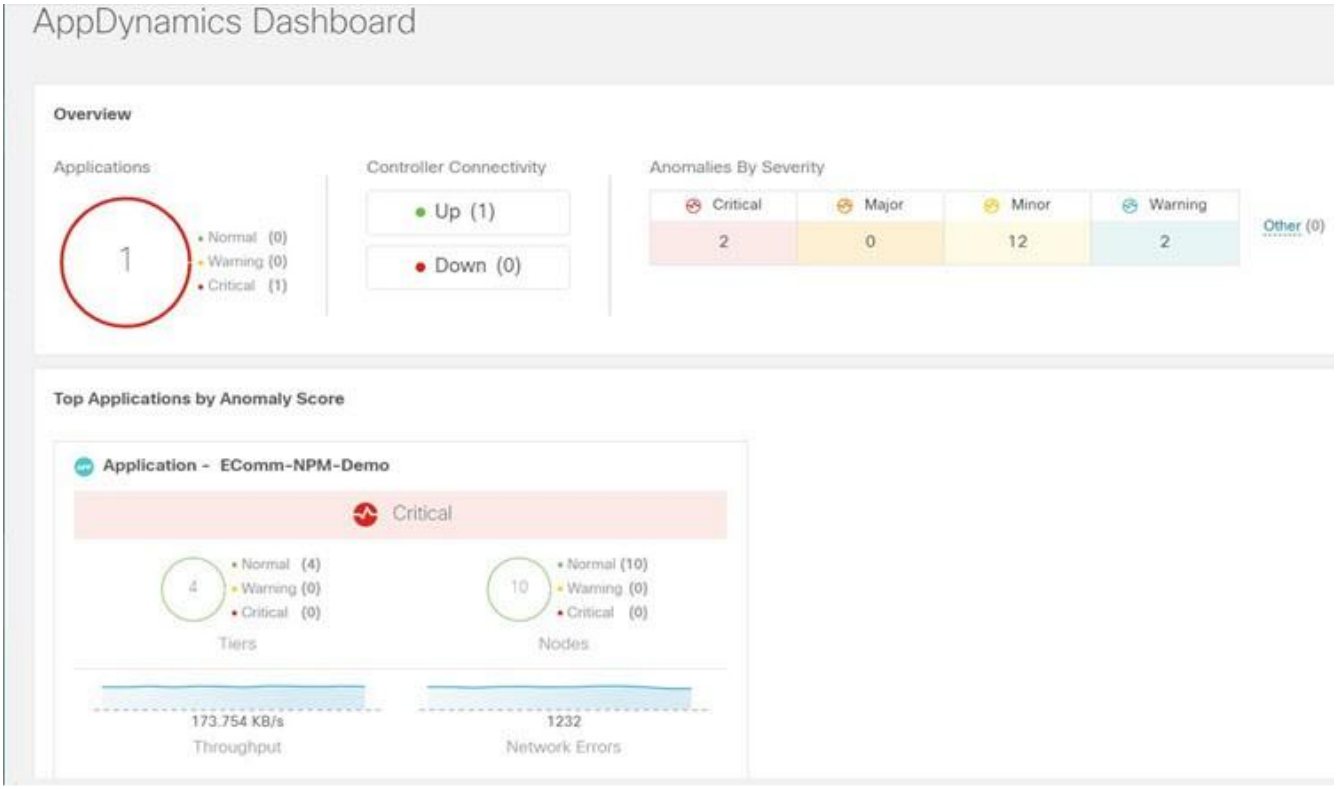
[コントローラの接続性] - **[アップ]**または**[ダウン]**状態の統合の数を表します。

[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]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]**の番号をクリックして、[異常]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. **[分析]**をクリックします。

      *[異常の分析の詳細]*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]**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]**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]**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]**をクリックして、アプリケーションの一般的な情報、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]**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]**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]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]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]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]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]**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]**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]に移動します。

   [異常]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]**セクションの各行をクリックすると、異常の詳細がポップアップ表示されます。
4. **[分析]**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。

注意事項と制約事項

- Nexus Dashboard Insights 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 にエクスポートされないため、Nexus Dashboard Insights 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 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。

トポロジ ビュー

トポロジビューは、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。

トポロジビューには、**[アプリケーション] > [ノード] > [リーフ]**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。

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。リーフノード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 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、5 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。

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]**ページで、**[設定]** > **[統合]** > **[管理]**をクリックします。
2. **[統合の追加]**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]**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]**をクリックします。
5. [追加（Add）] をクリックします。
6. vCenter Server が**[統合の管理]**ページに表示されます。**[ステータス]**が[アクティブ]になったら、統合の追加は完了です。
7. (任意) **[統合の管理]**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]**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]**または**[異常スコア別のホスト]**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]** > **[vCenters]**を選択して、vCenter ダッシュボードにアクセスします。
- ドロップダウンリストから、**[仮想マシン]**または**[ホスト]**を選択します。

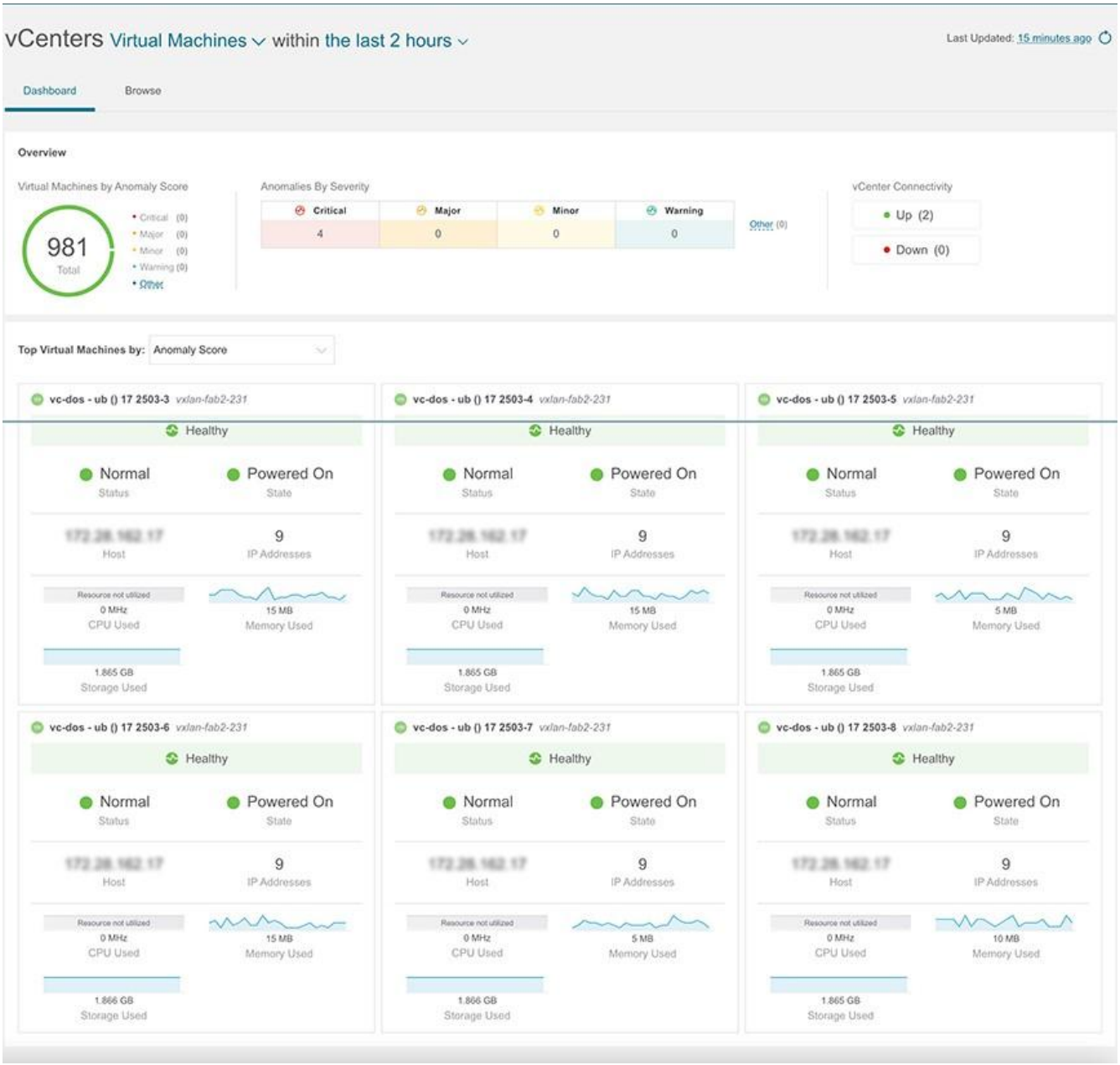
vCenter 仮想マシンダッシュボード

ダッシュボードの**[概要]**領域には、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] - **[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]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**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。

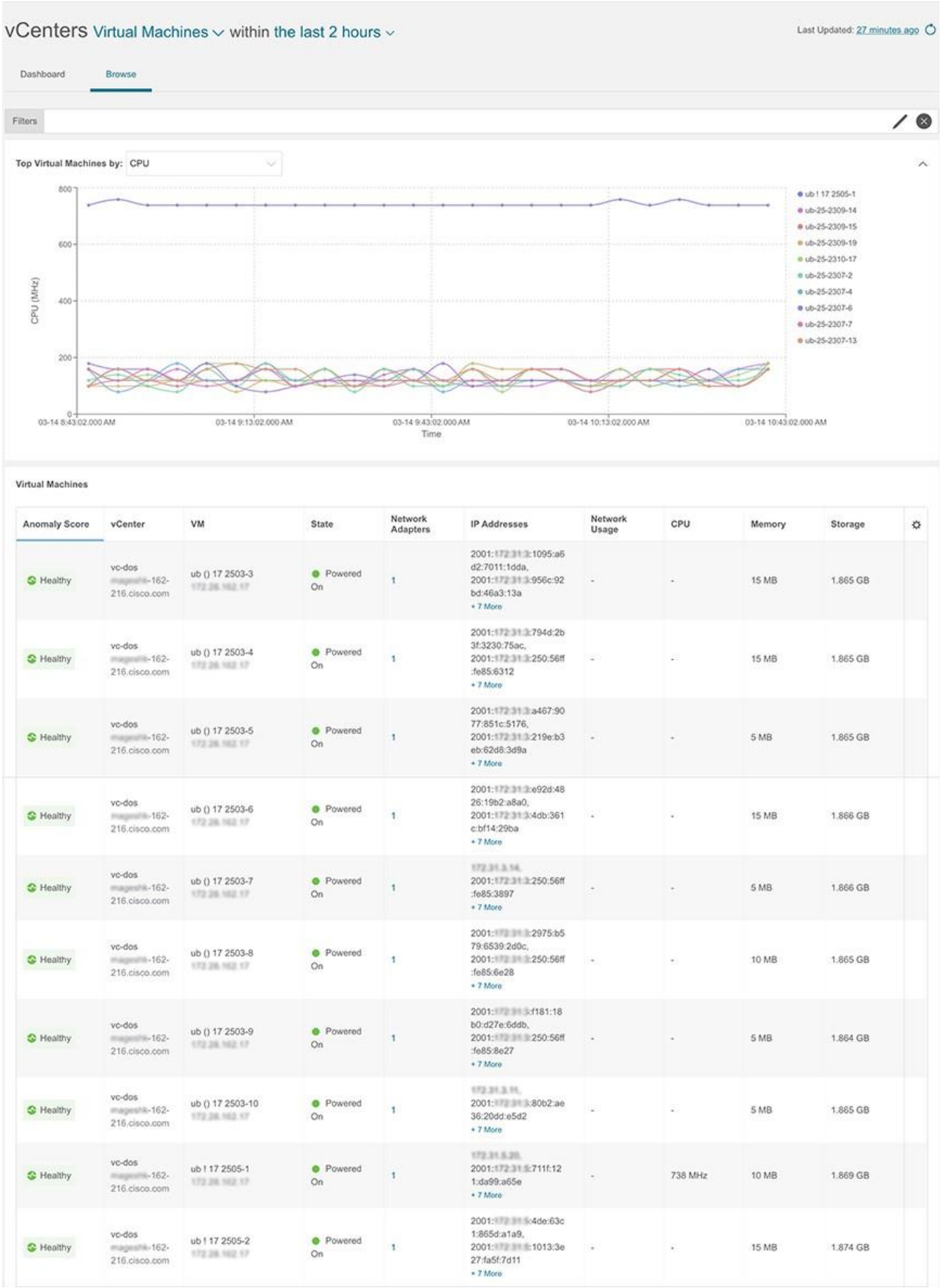
- == - 完全に一致するログを表示します。この演算子の後には、テキストや記号を続ける必要があります。
- contains - 入力されたテキストまたは記号を含むログを表示します。この演算子の後には、テキストや記号を続ける必要があります。

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]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]**メニューをクリックして、**[仮想マシン]**または**[ホスト]**テーブルに表示される列をカスタマイズします。
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。


vCenters Virtual Machines within the last 2 hours
Last Updated: 27 minutes ago
Dashboard
Browse
Filters
Top Virtual Machines by: CPU
CPU (MHz)
800
600
400
200
0
03-14 8:43:02.000 AM
03-14 9:13:02.000 AM
03-14 9:43:02.000 AM
03-14 10:13:02.000 AM
03-14 10:43:02.000 AM
Time
ub ! 17 2505-1
ub-25-2309-14
ub-25-2309-15
ub-25-2309-19
ub-25-2310-17
ub-25-2307-2
ub-25-2307-4
ub-25-2307-6
ub-25-2307-7
ub-25-2307-13
Virtual Machines
Anomaly Score
vCenter
VM
State
Network Adapters
IP Addresses
Network Usage
CPU
Memory
Storage
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-3
Powered On
1
2001:172:31:3:1095:a6d2:7011:1dda, 2001:172:31:3:956c:92bd:46a3:13a
+ 7 More
15 MB
1.865 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-4
Powered On
1
2001:172:31:3:794d:2b3f:3230:75ac, 2001:172:31:3:250:56ff:fe85:6312
+ 7 More
15 MB
1.865 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-5
Powered On
1
2001:172:31:3:a467:9077:851c:5176, 2001:172:31:3:219e:b3eb:62d8:3d9a
+ 7 More
5 MB
1.865 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-6
Powered On
1
2001:172:31:3:e92d:4826:19b2:a8a0, 2001:172:31:3:4db:361c:bf14:29ba
+ 7 More
15 MB
1.866 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-7
Powered On
1
2001:172:31:3:250:56ff:fe85:3897
+ 7 More
5 MB
1.866 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-8
Powered On
1
2001:172:31:3:2975:b579:6539:2d0c, 2001:172:31:3:250:56ff:fe85:6e28
+ 7 More
10 MB
1.865 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-9
Powered On
1
2001:172:31:3:f181:18b0:d27e:6ddb, 2001:172:31:3:250:56ff:fe85:8e27
+ 7 More
5 MB
1.864 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub () 17 2503-10
Powered On
1
2001:172:31:3:80b2:ae36:20dd:e5d2
+ 7 More
5 MB
1.865 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub ! 17 2505-1
Powered On
1
2001:172:31:5:711f:121:da99:a65e
+ 7 More
738 MHz
10 MB
1.869 GB
Healthy
vc-dos magenta-162-216.cisco.com
ub ! 17 2505-2
Powered On
1
2001:172:31:5:4de:63c1:865d:a1a9, 2001:172:31:5:1013:3e27:fa5f:7d11
+ 7 More
15 MB
1.874 GB

[仮想マシンの詳細]ページ

- [仮想マシン]ページの**[概要]**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]**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]**タブには、ファブリック内の**[仮想マシン]** > **[ホスト]** > **[リーフスイッチ]**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。

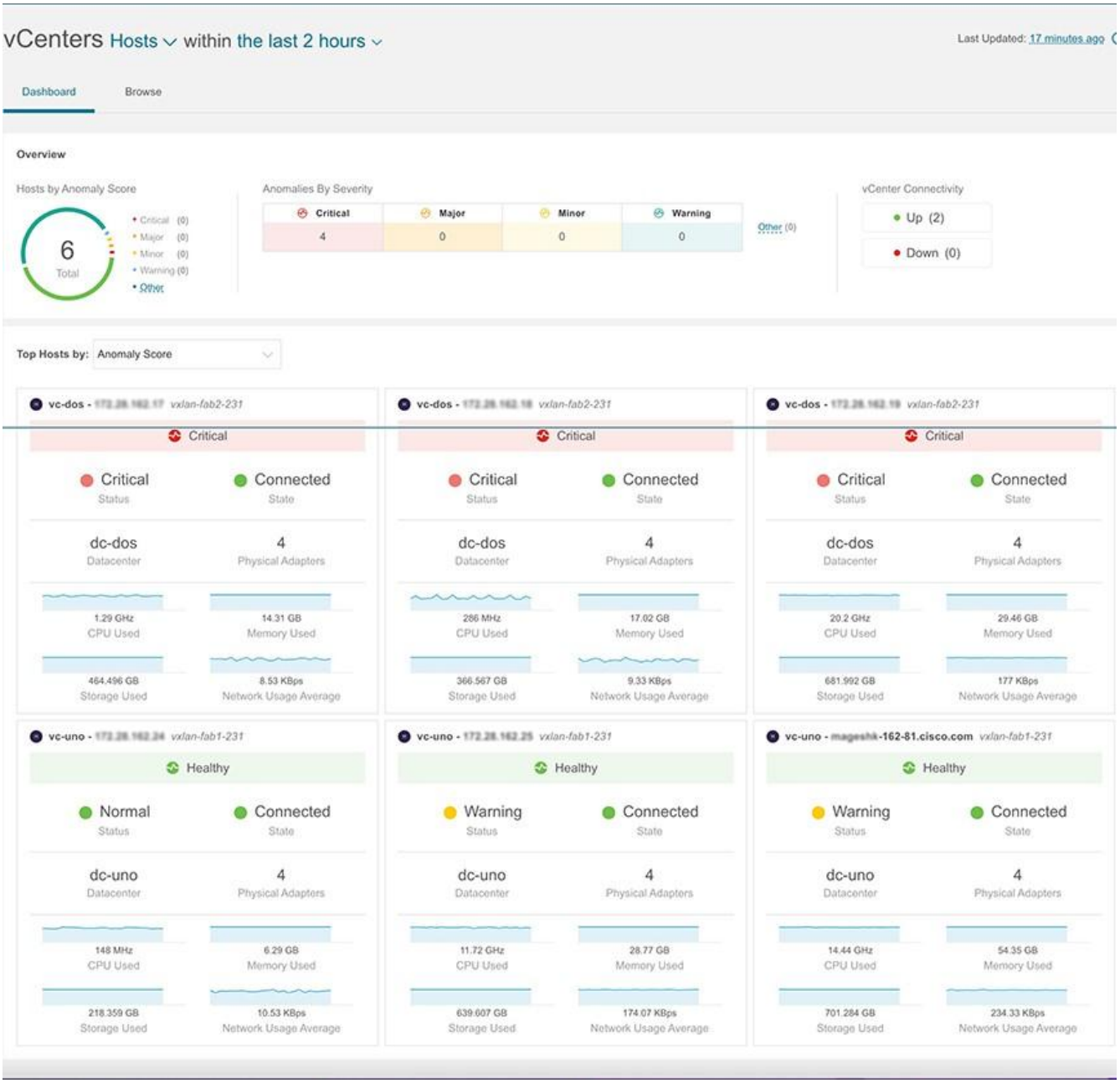
vCenter ホストダッシュボード

ダッシュボードの**[概要]**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] - **[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

[参照]ページには、CPU ごとの**上位ホスト**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。

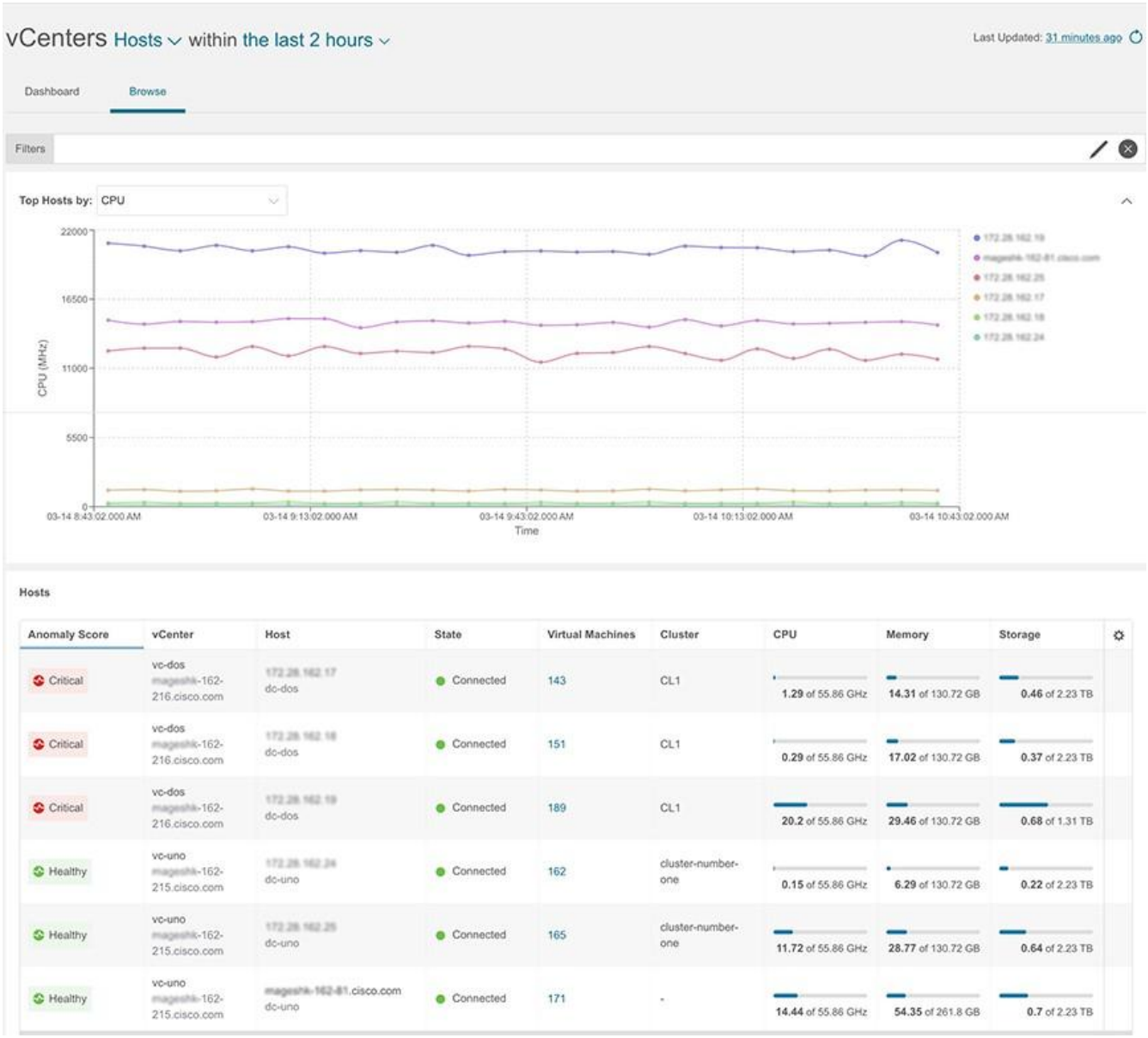
[ホスト]テーブルには、異常スコア、vCenter IP アドレス、ホスト IP アドレス、状態、仮想マシン、クラスタ、CPU、メモリ、ストレージなどの情報が表示されます。

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]**メニューをクリックして、**[仮想マシン]**または**[ホスト]**テーブルに表示される列をカスタマイズします。

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]**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]**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]**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。

Cisco Nexus Dashboard Insights のサードパーティノードのサポート

Nexus Dashboard Insights のサードパーティノードのサポートについて

Cisco Nexus Dashboard Insights は、サードパーティノードからデータを収集する方法を提供します。

データは、コレクタサービスによって提供される REST ベースの EAPI メソッドの呼び出しを使用して、サードパーティのコレクタサービスを通じて取得されます。

次のテレメトリ情報がサイト内のサードパーティノードから収集されます。

- [環境統計] : サイトノードの CPU、メモリ、ファン、温度、電力使用量、およびストレージの詳細などの環境統計の監視が含まれます。
- [インターフェイス統計] : LLDP および LACP を使用した Cisco DCNM およびサイトノードのノード、インターフェイス、およびプロトコル統計の監視が含まれます。
- [リソース統計] : IPv4 ユニキャスト、IPv4 マルチキャスト、および MAC を使用した Cisco DCNM 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。

Cisco DCNM のサードパーティハードウェアのサポート

Nexus Dashboard Insights は、Arista 7050SX および 7280SR プラットフォームスイッチをサポートします。

Nexus Dashboard Insights のサードパーティノードの制限事項

- LLDP および LACP のインターフェイス統計は、*[フラップ数]*、*[エントリの期限切れ回数]*、および *[PDU タイムアウト数]*をサポートしていません。
- MAC のインターフェイス統計は、ローカルエンドポイントおよび静的エンドポイントをサポートしていません。
- サードパーティノードは別のファブリックで検出されます。
- サードパーティノードは、監視モードでのみサポートされます。
- サードパーティノードは、データをストリーミングするために非特権モードでアクセスできます。

データ収集のためのサードパーティノードの有効化

サードパーティノードをサイトに追加または削除すると、コントロールメッセージが生成され、UTR パイプラインに存在するサードパーティ コレクタ サービスがトリガーされて、特定のノードからのデータの収集が開始または停止されます。

サードパーティノードを検出して Cisco DCNM サイトに対して有効にするには、次の手順を実行します。

- サードパーティノードを検出するための外部サイトを作成します。詳細については、外部ファブリックの作成を参照してください。
- サードパーティノードを検出する方法の詳細については、新しいスイッチの検出を参照してください。
- サードパーティノードを外部サイトに追加します。詳細については、非 Nexus デバイスを外部ファブリックに追加するを参照してください。

Cisco DCNM でのサードパーティノードの設定

Cisco DCNM のサイトにサードパーティノードを追加する前に、次の要件を満たしていることを確認してください。

- サードパーティノードの検出を行うには、管理者の資格情報が必要です。

インターフェイス統計データのほとんどがサードパーティノードの特定の設定なしで取得されます。ポートチャネルとストレージの統計情報を収集するには、次の設定が必要です。

1. LACP のポートチャネルを設定します。詳細については、ポートチャネルの設定手順を参照してください。
2. aaa authorization exec default local CLI コマンドを実行して、ストレージの統計情報を収集します。