

Cisco Nexus Dashboard Insights  
異常とアドバイザリ、リリース  
6.5.1 - Cisco ACI 向け

# 目次

新機能および変更情報 .....	2
異常 .....	3
異常 .....	3
異常の表示 .....	5
異常の分析 .....	5
異常の注意事項と制約事項 .....	7
異常のプロパティの構成 .....	8
異常フィルタ .....	10
グローバル ルール .....	14
グローバル ルール .....	14
異常レベルしきい値のカスタマイズ .....	14
異常ルール .....	15
異常ルール .....	15
注意事項と制約事項 .....	15
異常ルールの作成 .....	16
異常ルールの管理 .....	17
アドバイザリ .....	19
アドバイザリ .....	19
アドバイザリの表示 .....	20
アドバイザリの分析 .....	20
アドバイザリフィルタ .....	22
メタデータのサポート .....	22
著作権 .....	25

初版：2024 年 6 月 28 日

米国本社

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax : 408 527-0883

# 新機能および変更情報

次の表は、最新リリースまでの主な変更点の概要を示したものです。ただし、本リリースまでの変更点や新機能の一部は表に記載されていません。

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

特長	説明	リリース	参照先
異常の相関	異常の機能は、他の異常を引き起こす、または他の異常によって引き起こされた異常を相関させるようになりました。他の異常を引き起こす異常は、根本原因異常と呼ばれ、根本原因の異常によって引き起こされる異常は相関異常と呼ばれます。根本原因または相関異常のどちらでもない異常は、非相関異常と呼ばれます。根本原因異常、相関異常、根本原因異常のみ、非相関異常のみ、またはすべての異常をフィルタできるドロップダウンメニューがあります。	6.5.1	<a href="#">根本原因異常、相関異常、非相関異常、異常の分析</a>
キャパシティおよびハードウェアの異常に関するカスタムしきい値	異常に注意、重大、または主要のレベルが割り当てられているかどうかを決定するしきい値をカスタマイズできます。	6.5.1	<a href="#">グローバルルール、カスタマイズ、異常レベルのしきい値</a>
Field Notice のアドバイザリ結果の誤検出を減らすためのデバイスのシリアル番号の検証。	Cisco Nexus Dashboard Insights のアドバイザリ機能が、モニタリングしているネットワークファブリックに影響を与える可能性のある Field Notice を特定すると、Nexus Dashboard Insights は、各 Field Notice の影響を受けるデバイスのシリアル番号のリストに対して、ファブリック内のデバイスのシリアル番号を検証するようになりました。シリアル番号が field notice に含まれない場合、Nexus Dashboard Insights はその field notice を除外します。	6.5.1	<a href="#">Advisories</a>
技術変更	「サイト」という言葉は「ファブリック」に変更されました。	6.5.1	ドキュメント全体

このドキュメントは、Cisco Nexus Dashboard Insights のGUI およびオンラインで [www.cisco.com](http://www.cisco.com) で入手できます。本書の最新バージョンに関しては、「[Cisco Nexus Dashboard Insights](#)」の「[Documentation](#)」を参照してください。

# 異常

## 異常

Nexus Dashboard Insights は、ネットワーク全体でさまざまなタイプの異常をプロアクティブに検出し、異常の根本原因および修復方法を特定します。

Nexus Dashboard Insights は、ファブリック内のすべてのノードからのさまざまなデータ セットをモニタリ、データを基準にして「正常な」動作を識別します。偏差は異常と示されます。問題を追跡するのではなく、問題を解決することをお勧めします。さらに、以上の影響を想定し、異常の性質に応じて推奨を生成することで、トラブルシューティングと解決までの平均時間 (MTTR) が短縮できます。

[異常 (Anomalies) ] ページでは、

- ・ トラブルシューティングの平均解決時間を短縮し、
- ・ プロアクティブなモニタリングによって運用効率とネットワークの可用性を高め、
- ・ 修復します。

異常ページには、選択した時間範囲で、特定のファブリックのレベル別そしてカテゴリ別の異常を表示します。

異常レベルには、重大、主要、注意が含まれます。いくつかの

カテゴリには次が含まれます。

- ・ ハードウェア
- ・ 容量
- ・ 提供されず
- ・ 接続
- ・ configuration
- ・ 統合、および
- ・ アクティブ バグ。

## 根本原因異常

根本原因異常は、他の異常を引き起こす異常であり、相関異常と呼ばれます。根本原因異常を解決することで、相関異常も解決します。

## 相関異常

相関異常は、他の異常が原因で発生した異常のことで、根本原因異常と呼ばれます。根本原因異常を解決することで、相関異常に対してさらなる対応を行うことなく、相関異常が解決されます。

## 非相関異常

非相関異常は、相関異常を引き起こさず、そして根本原因異常によって引き起こされていない

異常です。したがって、そのような異常は他の異常に影響を与えることはありません。これらの異常は個別に解決する必要があります。

非相関異常は、Nexus Dashboard Insights が相関異常をまだ評価していない異常である可能性もあります。Nexus Dashboard Insights は、今後のリリースで相関異常に関してこれらの異常を評価できます。

## 異常機能が異常を相関させる方法

異常機能、特定の時間範囲内のさまざまな異常の関係の原因と影響を分析します。機能により、デバイス、インターフェイス、プロトコルなどさまざまな属性に基づいて異常を相関させ、第 2 の異常（相関異常）を発生させる可能性がある根本原因異常を見つけます。

## 異常レベル

異常は次のレベルに分類されます。

- ・ **クリティカル**：ネットワークがダウンする場合は、異常は重大と表示されます。いくつかの例には次のものが含まれます。
  - 特定のプレフィックスまたはエンドポイントへの接続が失われた場合。
  - ファブリックまたはスイッチが動作していない場合。
- ・ **メジャー**：特定のプレフィックスまたはエンドポイントへの接続が侵害される可能性がある場合、異常は主要と表示されます。例には次のものが含まれます。
  - IP アドレスまたはサブネットの重複
- ・ **注意**：ネットワークに影響がある場合は、異常は注意として表示されます。次に例を示します。
  - 特定のプレフィックスまたはエンドポイントへの接続が劣化した場合。

## 異常のプロパティ

異常には次のプロパティを構成できます。

- ・ ユーザーの割り当て
- ・ タグの追加
- ・ コメントの追加
- ・ 検証ステータスの設定
- ・ 異常を承認して、承認された異常が [異常 (Anomalies) ] テーブルに表示されないようにします。

異常のプロパティを構成するには、「[異常のプロパティの構成](#)」を参照してください。

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構成](#)」を参照してください。
- ・ 複数の異常を手動で承認します。「[異常の分析](#)」を参照してください。
- ・ 異常ルールを使用して、異常ルールに一致する異常を自動的に承認します。「[異常ルールの作成](#)」を参照してください。

# 異常の表示

Nexus Dashboard Insights では、以下の方法で異常を表示できます。

1. [分析 (Analyze) ] > [異常

(Anomalies) ] に移動します。または

1. [概要 (Overview) ] > [グローバル ビュー (Global View) ] に移動します。
2. ドロップダウン メニューからオンライン ファブリックまたはスナップショット ファブリックを選択します。
3. [異常レベル (Anomalies Level) ] カードをクリックします。
4. 異常ページで、[すべての異常の表示 (View all

anomalies) ] をクリックします。または

1. [管理 (Manage) ] > [ファブリック (Fabrics) ] に移動します。
2. ファブリックを選択します。
3. [異常

(Anomalies) ] をク

リックします。また

は

1. [管理 (Manage) ] > [インベントリ (Inventory) ] に移動します。
2. [コントローラ (Controllers) ] または [スイッチ (Switches) ] をクリックします。
3. コントローラまたはスイッチを選択します。
4. [異常 (Anomalies) ] をクリックします。

# 異常の分析

1. [分析 (Analyze) ] > [異常 (Anomalies) ] に移動します。
2. ドロップダウン メニューから [オンライン ファブリック (Online fabrics) ] または [スナップショット ファブリック (Snapshot fabrics) ] を選択します。
3. [すべての異常 (All Anomalies) ] ドロップダウン メニューから、[グループ化 (Grouped) ] または [グループ解除 (Ungrouped) ] を選択します。
  - [グループ解除 (Ungrouped) ] ビューでは、ファブリックに関して発生した個別の異常を表示します。
  - [グループ化 (Grouped) ] ビューでは、異常タイプに基づき異常の集約ビューを表示します。
4. [日時 (Date and Time) ] セレクタから、時間範囲を選択します。デフォルトでは、[今すぐアクティブ (Active Now) ] が選択されています。

異常ページには、選択した時間範囲で、ファブリックのレベル別そしてカテゴリ別の異常を表示します。

- 円グラフでは、異常の重大、主要、注意の深刻度の合計数を表示します。
- カテゴリの円グラフには、ハードウェア、キャパシティ、コンプライアンス、接続性、構成、統合、アクティブなバグなど、さまざまなカテゴリ別に異常の合計数が表示されます。

- スナップショット ファブリックに表示されている異常については、異常レベルが最新のスナップショットだけでなく、すべてのスナップショットにわたっています。

5. 異常をフィルタ処理するには、フィルタ フィールドを活用します。インターフェイス、VRF インスタンス、EPG、または BD などの影響を受けるオブジェクトをフィルタし、関連する異常を表示できます。

- a. グループ解除異常を表示する場合は、フィルタ フィールドの横にあるドロップダウンメニューを使用して、未承認または承認済みの異常をフィルタできます。デフォルトは【未承認 (Unacknowledged)】です。
- b. 未承認および承認済みの異常のドロップダウン メニューの隣にあるドロップダウン メニューを使用して、根本原因および非相関異常、根本原因異常のみ、非相関異常のみ、またはすべての異常でフィルタできます。デフォルトは、根本原因と非相関異常です。

フィルタに関する詳細は、「[フィルタの異常](#)」を参照してください。

6. [異常タイプ (Anomaly Type)] テーブルには、フィルタされた異常が表示されます。デフォルトでは、異常はレベルでソートされます。列の見出しをクリックして、テーブルの異常をソートします。

グループ解除異常を表示し、[ステータス (Status)] 列をディスプレイするようにテーブルを構成した場合、ステータスは【アクティブ (Active)】または【クリア (Cleared)】になります。【アクティブ (Active)】ステータスは、ネットワークに異常が存在しないことを示します。【クリア (Cleared)】ステータスは、ネットワークに異常が存在しないことを示します。

7. 歯車アイコンをクリックして、[異常 (Anomalies)] テーブルに表示する列を構成します。

デフォルトでは、[異常タイプ (Anomaly Type)]、[レベル (Level)]、[カテゴリ (Category)]、[根本原因 (Root-Cause)]、および [非相関異常 (Uncorrelated Anomalies)] 列がグループ化された異常に表示されます。[根本原因 (Root-Cause)] 列には、そのグループ内の異常のうち根本原因異常の数が表示されます。

デフォルトでは、[問題点 (What's wrong)]、[レベル (Level)]、[カテゴリ (Category)]、[ファブリック (Fabric)]、[検出時間 (Detection Time)]、および [相関異常 (Correlated Anomalies)] 列がグループ化された異常に表示されます。

8. 異常をクリックすると、詳細情報が表示されます。

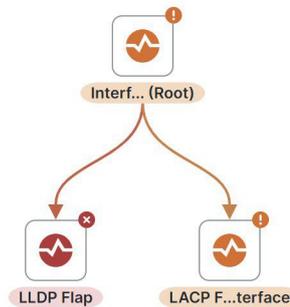
- 問題点：特定の影響を受けるオブジェクトの問題を説明します。
- 異常のトリガ：異常の根本原因が表示されます。リンクをクリックすると、根本原因異常に関する情報を表示できます。このエリアには、根本原因の異常と関連するすべての異常を示すグラフが含まれます。グラフ内の異常をクリックすると、その異常に関する詳細情報を取得できます。エリアの右下にあるコントロールを使用すると、グラフを拡大または縮小したり、トポロジの凡例を表示したりできます。このエリアは、相関異常の場合にのみ表示されます。
- どのような影響があるか？では、問題が修正されなかった場合の動作について説明します。異常が根本原因である場合、このエリアには相関する異常の数が表示されます。クリックすると、異常のテーブルが表示されます。

根本原因の異常の場合、このエリアには、根本原因の異常と関連するすべての異常を示すグラフが含まれます。グラフ内の異常をクリックすると、その異常に関する詳細情報を取得できます。エリアの右下にあるコントロールを使用すると、グラフを拡大または縮小したり、トポロジの凡例を表示したりできます。

## What's the impact?

- 3 IP(s) will be affected.  
[View Report](#)

**2 additional correlated anomalies** may have been caused by this root anomaly. View all associated anomalies in the graph below, including root-cause and correlated anomalies.



相関異常ページを表示し、[ステータス (**Status**)] 列を表示するようにテーブルを構成した場合、ステータスは [アクティブ (Active)]、[クリア (Cleared)]、または [削除 (Deleted)] になります。[アクティブ (Active)] ステータスは、ネットワークに異常が存在しないことを示します。[クリア (Cleared)] ステータスは、ネットワークに異常が存在しないことを示します。[削除 (Deleted)] ステータスは、期限切れのためシステムによって異常データベースから異常を削除したが、相関異常の一部がまだ存在しているため異常がこのページからまだ削除されていないことを示します。

- 修正方法：規範的な推奨事項を示します。

9. [異常 (Anomalies)] ドロップダウンメニューから、[グループ化解除 (**Ungrouped**)] を選択します。
  - a. [異常 (Anomalies)] テーブルから異常をセレクトし、[異常の承認 (**Acknowledge Anomalies**)] をクリックして異常を確認します。
  - b. 異常をクリックし、[異常 (Anomalies)] ページで [アクション (**Actions**)] メニューから、[異常の承認 (**Acknowledge Anomaly**)] を選択することもできます。
  - c. デフォルトでは、すべての未承認の異常が異常テーブルに表示されます。異常を確認した後、ドロップダウンメニューから [承認済み (**Acknowledged**)] を選択して、承認済みのすべての異常を表示します。
10. 異常をブックマークするには、異常をクリックして [異常 (Anomaly)] ページを表示し、ブックマークアイコンをクリックします。
11. 異常のウィジェットをカスタム ダッシュボードに追加するには、異常をクリックして、[異常 (Anomaly)] ページを表示し、[アクション (**Actions**)] > [カスタム ダッシュボードにページをピン留めする (**Pin page to custom dashboards**)] をクリックします。

## 異常の注意事項と制約事項

- 次のシナリオでは、異常は [異常 (Anomalies)] ページに表示されません。
  - カテゴリ「システム」に属する異常は、デフォルトでは [異常 (Anomalies)] ページに表示されません。
  - 収集またはログインの不具合が発生する場合、[管理 (**Admin**)] > [システム設定

[**SystemSettings**] > [システム ステータスの詳細 (**System Status Details**)] ページで、[アシュアランス (Assurance)] ステータスが [正常 (Healthy)] と表示されます。同時に、[管理 (**Admin**)] > [システム設定 (**System Settings**)] > [システム問題 (**System Issues**)] ページで、収集またはログインの不具合に関連する異常

は表示されません。

異常を表示するには、次の手順を実行します。

1. これらの異常を表示するには、[分析 (**Analyze**)] > [異常 (**Anomalies**)] の順に選択します。
  2. ドロップダウン リストから [オンライン ファブリック (**Online Fabrics**)] を選択します。
  3. [異常 (Anomalies)] ドロップダウン リストから [グループ解除 (**Ungrouped**)] を選択します。
  4. 検索バーを活用して、カテゴリ== システムでフィルタ処理します。すべてのシステム異常が異常テーブルに表示されます。
- ・ ファブリックの場合、データは次のいずれかのシナリオで消去されます。
    - 30 日間の保持期間の後
    - ストレージのしきい値に達した場合

その結果、そのファブリックの異常とアドバイザリは表示されません。異常とアドバイザリを表示するには、分析を再実行する必要があります。

## 異常のプロパティの構成

次の手順を使用して、異常のプロパティを設定します。

1. [分析 (**Analyze**)] > [異常 (**Anomalies**)] に移動します。
2. ドロップダウン メニューから [オンライン ファブリック (Online fabrics)] または [スナップショット ファブリック (Snapshot fabrics)] を選択します。
3. [異常 (Anomalies)] ドロップダウンメニューから、[グループ化解除 (**Ungrouped**)] を選択します。  
[グループ解除 (Ungrouped)] ビューでは、ファブリックに関して発生した個別の異常を表示します。
4. [時間選択 (**Time Selection**)] ダイアログから、希望のモードを選択し、[適用 (**Apply**)] をクリックします。デフォルトでは、[今すぐアクティブ (**Active Now**)] です。
  - [最終... (**Last...**)] では、期間も選択する必要があります。
  - [日付と時刻の範囲 (**Date and Time Range**)] では、範囲も選択する必要があります。
5. テーブルから異常をクリックして、[アクション (**Actions**)] メニューからプロパティを選択します。
  - a. 異常を確認するには、[異常の承認 (**Acknowledge Anomaly**)] を選択します。デフォルトでは、すべての未確認の異常が異常テーブルに表示されます。異常を確認した後、ドロップダウンリストから [承認済み (Acknowledged)] を選択して、承認済みのすべての異常を表示します。
  - b. [新規 (New)]、[進行中 (In Progress)]、[クローズ (Closed)] などのユーザー定義ステータスを異常に設定するには、[検証ステータス (**Verification Status**)] を選択します。ドロップダウンリストからステータスを選択し、[保存 (**Save**)] をクリックします。
  - c. [割り当て先 (**Assigned To**)] を選択して、異常をユーザーに割り当てます。ユーザー名を入力し、[保存] をクリックします。
  - d. [コメント (**Comment**)] を選択して、異常にコメントを割り当てます。コメントを入力して、[保

存]をクリックします。

- e. [タグの管理 (**Manage Tags**) ]を選択して、ユーザー定義のタグを異常に追加します。タグ名を入力して、  
[保存 (Save) ] 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. 複数の異常を承認するには、異常を選択します。[異常の承認 (**Acknowledge anomalies**) ] をクリックします。
7. 異常に割り当てられたプロパティを表示するには、異常をクリックして [異常 (Anomaly) ] ページを表示します。[異常 (Anomaly) ] ページで、[検証ステータス (**Verification Status**) ]、[承認 (**Acknowledge**) ]、および[割当先 (**Assigned To**) ] などのプロパティが

表示されます。異常に割り当てられたコメントとタグを表示するには、[アクション (Actions)] メニューから、  
[コメント (Comment)] または [タグの管理 (Manage Tags)] を選択します。

Analyze > Anomalies > Physical Device Cluster Has No Physical Domain

### Physical Device Cluster Has No Physical Domain

Refresh Actions

**What's wrong?**

The device cluster of device type 'PHYSICAL' has no physical domain association.

**Anomaly Level Major**

**Status Active**  
Last Seen: Jun 26, 2024, 03:21:39 PM

Category: Configuration      Fabric: DC-ute11

Nodes: ute11-apic1      Initial Detection Time: Jun 26 2024 11:21:41.000 AM  
Recent

- ・ [アクション (Actions)] メニューを使用して異常を承認際、[異常 (Anomalies)] テーブルの省略アイコンを使用して、個別の異常で構成したすべてのプロパティがオーバーライドされません。
- ・ 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。
- ・ スナップショット ファブリック分析のアクティブな異常を表示するには、分析が作成された時間範囲を選択する必要があります。

## 異常フィルタ

フィルタ フィールドにより、グループ解除された異常を表示するときの異常のテーブルをフィルタするか、グループ化された異常を表示するときの異常のテーブルをフィルタ出来るようになります。

[異常 (Anomalies)] ページでは、次のフィルタを使用して、テーブルのエントリを絞り込むことができます。

- ・ [異常タイプ (Anomaly Type)] : 特定のタイプの異常を表示します。
- ・ [割当先 (Assigned To)] : (グループ解除のみ) 特定のユーザーに割り当てられている異常を表示します。
- ・ [BD] : 特定のブリッジ ドメインの異常を表示します。
- ・ [カテゴリ (Category)] : 特定のカテゴリの異常が表示されます。
- ・ [チェック コード (Check code)] : (グループ解除のみ) 特定のチェック コードの異常を表示します。
- ・ [クリア時刻 (Cleared Time)] : (グループ解除のみ) 特定の時刻がクリアされた異常を表示します。
- ・ [コメント (Comment)] : (グループ解除のみ) 特定のコメントの異常を表示します。
- ・ [検出時間 (Detection Time)] : (グループ解除のみ) 特定の検出時間の異常を表示します。
- ・ [EPG] : 特定の EPG の異常を表示します。
- ・ [ファブリック (Fabric)] : (グループ解除のみ) 特定のファブリックのアドバイザリを表示します。
- ・ [インターフェイス (Interface)] : 特定のインターフェイスの異常を表示します。
- ・ [IP アドレス (IP address)] : (グループ解除のみ) 特定の IP アドレスを持つ異常を表示します。

- ・ [最終確認時刻 (Last Seen Time) ] : (グループ解除のみ) 特定の最終確認時刻の異常を表示します。前回の検出

時間は、アクティブ ステータス中に異常が更新された時間を示します。異常のステータスがクリアになっていない場合、異常はアクティブです。

- ・ [レベル (Level) ] : 特定のレベルの異常を表示します。
- ・ [MAC アドレス (MAC address) ] - MAC アドレスを持つ異常が表示されます。
- ・ [ノード (Nodes) ] : 特定のノードの異常表示します。
- ・ [ステータス (Status) ] : 指定されたステータスの異常を表示します。
- ・ [タグ (Tags) ] : (グループ解除のみ) 特定のタグの異常を表示します。
- ・ [VPC] : 特定のリモート対応ポート チャンネル (vPC) の異常を表示します。
- ・ [VRF] : (グループ解除のみ) 特定の仮想ルーティングおよび転送 (VRF) インスタンスの異常を表示します。
- ・ [検証ステータス (Verification Status) ] : (グループ解除のみ) 特定の検証ステータスの異常を表示します。
- ・ [問題点 (What's Wrong) ] : (グループ解除のみ) 特定の影響を受けるオブジェクトの

異常を表示します。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 タイプでこの演算子および後続の値を使用すると、完全一致のデータが返されます。この演算子は、すべてのフィルタで使用できます。
- ・ != : 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、同じ値を含まないすべてのデータが返されます。この演算子は、ほとんどのフィルタで使用できます。
- ・ 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。この演算子は、一部のフィルタで使用できます。
- ・ !contains : 最初のフィルタ タイプ。この演算子および後続の値を使用すると、その値を含まないすべてのデータが返されます。この演算子は、一部のフィルタで使用できます。

## 承認済みまたは未承認の異常のフィルタリング

フィルタ フィールドの横にあるこのドロップダウン メニューを使用すると、異常を未承認または承認済みのステータスでフィルタできます。未承認の異常をフィルタするには、[承認済み (Acknowledged) ] を選択しフィルタします。承認済みの異常を除外するには、[未承認 (Unacknowledged) ] を選択しフィルタします。

## 根本原因と非相関異常のフィルタリング

フィルタ処理フィールドの近くにあるこのドロップダウン メニューを使用すると、根本原因と無相関異常をフィルタできます。これにより、異常のテーブルがフィルタリングされます。

次のフィルタを選択できます。

- ・ 根本原因と非相関異常 : テーブルには、根本原因の異常と相関のない異常が表示されますが、相関の異常は表示されません。手動で解決する必要がある異常のみが表示されるため、これはデフォルト値です。根本原因の異常を解決すると、関連する異常も解決されます。このため、相関する異常を確認することはそれほど重要ではありません。
- ・ [根本原因異常のみ (Root Cause Anomalies Only) ] : テーブルには、根本原因異常のみが表示されま

す。

- ・ [無相関異常 (Uncorrelated Anomalies) ] : テーブルには無相関異常のみが表示されます。
- ・ [すべての異常タイプ (All Anomaly Types) ] : テーブルにはすべての異常が表示されます。

## 異常の主な影響を受けるオブジェクトを特定する

IP アドレス、MAC アドレス、インターフェイス、VPC、EPG、および VRF など影響を受けるオブジェクト フィルタの組み合わせを使用して異常をフィルタするには、すべての提供されるフィルタ オブジェクトを特定の異常に対して主に影響を受けるオブジェクトにする必要があります。クエリにプライマリ以外の影響を受けるオブジェクトが含まれている場合、フィルタによる結果を返しません。

特定の異常の主な影響を受けるオブジェクトを特定するには、次の手順を実行します。

1. 特定の異常の主に影響を受けるオブジェクトを決定するには、[分析 (Analyze) ] > [異常 (Anomalies) ] に移動します。
2. グループ化されていない異常からオブジェクトを特定する場合は、ドロップダウン メニューから [グループ解除 (Ungrouped) ] を選択します。
3. グループ化された異常からオブジェクトを特定する場合は、ドロップダウン メニューから [グループ化 (Grouped) ] を選択し、テーブルで目的の異常タイプをクリックします。
4. [異常 (Anomalies) ] テーブルから異常を選択します。
5. [影響 (What's the impact?) ] エリアでは、影響を受ける主要なオブジェクトが太字で強調表示されています。

# グローバル ルール

## グローバル ルール

グローバル ルール ページにより、異なる異常カテゴリのどの異常レベルが有効になっているか確認できます。異常に注意、重大、または主要のレベルが割り当てられているかどうかを決定するしきい値をカスタマイズできます。

## 異常レベルしきい値のカスタマイズ

これらの手順に従い、異常レベルしきい値をカスタマイズします。

1. [管理 (Manage) ] > [ルール (Rules) ] > [グローバルルール (Global Rules) ] に移動します。
2. 目的の異常カテゴリの [ステータス (Status) ] 列で、[カスタマイズ (Customize) ] をクリックします。
3. [キャパシティ異常のしきい値のカスタマイズ (Customize thresholds for capacity anomalies) ] テーブルで、しきい値をカスタマイズする異常を見つけて、編集 (鉛筆) アイコンをクリックします。

[キャパシティ異常のしきい値のカスタマイズ (Customize thresholds for capacity anomalies) ] テーブルには、複数のページが存在可能です。必要な場合、テーブルの下にあるページ コントロールを使用して、求める異常を見つけます。

4. 各異常レベルに必要なパーセンテージを入力し、緑色のチェックマークをクリックします。

しきい値をカスタマイズしたら、Nexus Dashboard Insights は既存の異常の異常レベルを再計算します。これには 30 分程度かかります。

[リセット (Reset) ] をクリックして値をデフォルトにリセットするか、[X] をクリックして編集をキャンセルできます。

- 値は 0 から 100 の間です。値 0 は、Nexus Dashboard Insights がその重大性の異常を発生させないことを示します。すべての重大度に 0 を入力すると、Nexus Dashboard Insights は異常を完全に抑制します。
- 注意の値は、[メジャー (Major) ] の値より小さく、[メジャー (major) ] の値は [クリティカル (Critical) ] の値より小さい必要があります。
- [メジャー (Major) ] に定義されている値は、[注意 (Warning) ] に定義された範囲の上限を設定し、[クリティカル (Critical) ] に定義された値は [メジャー (Major) ] に定義された範囲の上限を設定します。

# 異常ルール

## 異常ルール

異常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、アラートを異常ルールと一致させることもできます。

また、異常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。

- ・ 異常ルールには、異常をルールと照合するために必要な一致基準と、一致した異常に適用するアクションが含まれています。
- ・ 異常ルールには、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、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、異常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異常が一致します。**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異常が一致します。
- ・ 異常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異常が一致します。いずれかの基準に一致する異常はすべてルールに適用されます。**OR** 演算子は基準に適用されます。
- ・ [オブジェクト一致ルール (Object Match Rule)] を含む [一致基準 (Match Criteria)] を使用する異常ルールは、[Equals to]正規表現基準のみをサポートします。
- ・ 異常ルールは、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。
- ・ 異常ルールはアドバイザーではサポートされていません。
- ・ 複数の異常ルールが作成された場合、一致するすべてのルールが適用されます。
- ・ 異常ルールで複数の属性が指定された場合、各属性の条件は、適用するルールを満たしている必要があります。
- ・ 属性に複数の条件を指定した場合、条件のいずれかは属性を満たしていて、true として評価する必要があります。
- ・ 影響を受けるオブジェクト内で複数の一致条件を指定した場合、各条件を満たしている必要があります。

## 注意事項と制約事項

- ・ [承認 (Acknowledge)] または [異常のカスタマイズ (Customize Anomaly)] アクションのどちらかを含む異常ルールを削除または無効にすると、アクティブな異常から異常ルールを削除または無効にしません。異常のルールは、異常の新しいインスタンスにのみ適用されません。
- ・ [承認 (Acknowledge)] または [異常のカスタマイズ (Customize Anomaly)] アクションを含む異常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。異常ルールの更新は、異常の新しいインスタンスにのみ適用されます。

- ・ 異常ルールに [承認 (Acknowledge) ] と [異常のカスタマイズ (Customize Anomaly) ] アクションの両方が含まれていて、[承認 (Acknowledge) ] と [異常のカスタマイズ (Customize Anomaly) ] アクションのいずれかを削除して異常ルールを編集した場合、更新はアクティブな異常には適用されません。
- ・ [異常のカスタマイズ (Customize Anomaly) ] アクションを含む異常ルールを削除または無効化しても、推奨は [修正方法 (How do I fix it) ] に表示されたままになります。
- ・ 異常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。異常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。
- ・ すべてのファブリックでサポートされる異常ルールの最大数は 500 です。
- ・ 以下のシナリオでは、[異常ルールの作成 (Create Anomaly Rule) ] ページで [既存のアクティブな異常に適用する (Apply to existing active anomalies) ] チェック ボックスを選択すると、一致する条件に一致する既存のアクティブな異常を自動的に承認するアラート ルールを使用することはできません。
  - 異常はアラート ルールが作成される前に発生したため、アラート ルールが作成された後異常へのさらなる更新はありません。

このシナリオでは、手動で異常を承認できます。「 [異常 プロパティの構成](#) 」を参照してください。

- ・ このリリースにアップグレードすると、一部の異常ルールが更新または削除される場合があります。新しいカテゴリと重大度に基づいて、アップグレード後にこれらのルールを手動で追加できます。
- ・ オブジェクト一致ルールまたはコード ルールと一致基準を使用する異常ルールは、アクティブなバグ、キャパシティ、ハードウェア、統合、または接続のカテゴリのいずれかを持つ異常には適用されません。

## 異常ルールの作成

1. [管理 (Manage) ] > [ルール (Rules) ] > [異常ルール (Anomaly Rules) ] に移動します。
2. [異常ルールの作成 (Create Anomaly Rule) ] をクリックします。
3. [全般 (General) ] タブの次のフィールドに入力します。
  - a. In the **Name** field, enter the name.
  - b. [説明 (Description) ] フィールドに、説明を入力します。
  - c. 状態を選択して、ルールをアクティブにします。

状態が有効な場合、ルールは次の分析に適用されます。状態が無効の場合、ルールは次の分析中に適用されません。

- d. [次へ (Next) ] をクリックします。
4. [設定 (Settings) ] タブの次のフィールドに入力します。
    - a. [基準の追加 (Add Criteria) ] をクリックして、異常ルールの一致基準を定義します。
    - b. [ファブリック (Fabric) ] ドロップダウン メニューから、ファブリックを選択します。分析を実行しているファブリック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。
    - c. 一致基準の属性を選択します。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。ドロップダウン リストからカテゴリとイベント タイトルを選択します。

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

主要な影響を受けるオブジェクトを特定するには、「[異常の主要な影響を受けるオブジェクトを特定する](#)」を参照してください。

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異常が一致します。異常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異常が一致します。

- e. [コードルールの追加 (Add Code Rule)] をクリックして、一致基準のチェックコードを定義します。
- f. ドロップダウン リストから重大度を選択します。
- g. [保存 (Save)] をクリックします。

5. [アクション (Actions)] の次のフィールドに値を入力します。

- a. トグルを活用して、[承認 (Acknowledge)] 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。

- i. [既存のアクティブな異常に適用 (Apply to existing active anomalies)] チェックボックスをオンにして、異常アラートに一致する異常の既存のインスタンスに異常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異常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. トグルを活用して、[異常のカスタマイズ (Customize Anomaly)] を選択します。

[異常のカスタマイズ (Customize Anomaly)] を選択すると、異常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。

- i. 異常ルール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、異常ルール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 (Anomaly)] ページの [修正方法 (How do I fix it?)] エリアを選択します。
- ii. [既存のアクティブな異常に適用 (Apply to existing active anomalies)] チェックボックスをオンにして、異常ルールに一致する異常の既存のインスタンスに異常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異常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。
6. [概要 (Summary)] で選択内容を確認し、[異常ルールの追加 (Add Anomaly Rule)] をクリックします。新しい異常ルールは、[異常ルール (Anomaly Rule)] テーブルに表示されます。

## 異常ルールの管理

1. [管理 (Manage)] > [ルール (Rules)] > [異常ルール (Anomaly Rules)] に移動します。異常ルールは、[異常ルール (Anomaly Rule)] テーブルに表示されます。
2. 検索バーを使用して、名前、アクション、状態に基づきルールをフィルタします。

3. 異常ルールを選択し、編集する [ルール編集 (Edit Rule) ] をクリックします。
4. システムからルールを削除するには、異常ルールを選択し、[ルール削除 (Delete Rule) ] をクリックします。
5. 異常のルールを選択し、省略記号アイコンをクリックします。[有効 (Enable) ] をクリックしてルールを有効にします。状態が有効な場合、ルールは次の分析に適用されます。異常ルールを有効にする前に、異常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。
6. 異常のルールを選択し、省略記号アイコンをクリックします。[無効 (Disable) ] をクリックして、ルールを無効にします。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。

# アドバイザー

## アドバイザー

Nexus Dashboard Insights は、モニタリングしているネットワーク ファブリックに影響を与える可能性のある field notices、ソフトウェア、およびハードウェアの使用終了や販売終了のアナウンス、PSIRT を特定し、アドバイザーを生成します。アドバイザーでは、ネットワークのサポートを維持し、最適な状態で稼働するための推奨事項を提供します。

Nexus Dashboard Insights のアドバイザーでは、ハードウェアおよびソフトウェアの field notices、PSIRT、EoL/EoS からの関連する影響と、ベスト プラクティスの詳細を提供します。選択された時間範囲に基づき、特定のファブリックのレベルとカテゴリ別にアドバイザーを表示できます。

アドバイザーが、モニタリングしているネットワーク ファブリックに影響を与える可能性のある Field Notice を特定すると、Nexus Dashboard Insights は、各 Field Notice の影響を受けるデバイスのシリアル番号のリストに対して、ファブリック内のデバイスのシリアル番号を検証するようになりました。シリアル番号が field notice に含まれない場合、Nexus Dashboard Insights はその field notice を除外します。アドバイザーでデバイスのシリアル番号を検証には、Cisco Nexus Dashboard がインターネットに接続され、Cisco Intersight に接続され、登録されている必要があります。このような接続がないと、アドバイザーはシリアル番号を検証できません。そのため、アドバイザーには適用されない Field Notice が誤って含まれる可能性があります。すべての Field Notice にシリアル番号の検証が含まれているわけではありません。

特定のアドバイザーをクリックすると、問題点、影響、修正方法などの情報が表示されます。

- ・ 問題点：特定の影響を受けるオブジェクトの問題を説明します。
- ・ 影響：問題が修正されなかった場合に何が起るかを説明し、主要な販売終了日を含めます。
- ・ 修正方法：規範的な推奨事項を示します。

アドバイザーにより、最新の状態を維持できます。

- ・ 可用性を常に把握することができます。
- ・ ハードウェアやソフトウェアの EoS や EoL のアナウンス、PSIRT や field notices アップグレードの
- ・ リード タイムにより、安全性とコンプライアンスを維持し、適用可能なバグを即座に
- ・ 把握することができます。

アドバイザーは次の 3 レベルに分類されます。重大、主要、注意。

- ・ [クリティカル (**Critical**) ]: サポートされていないインフラストラクチャがあり、通知に関連付けられているバグの重大度が Severity1 である場合、アドバイザーは重大として表示されます。いくつかの例には次のものが含まれます。
  - ファブリック内のスイッチがサポート終了状態で実行されている場合。現在ネットワークで動作しているスイッチまたはソフトウェアのバージョンに対して、重大 (Severity1) field notice または PSIRT が発行されている場合。
- ・ [メジャー (**Major**) ]: アドバイザーは、通知に関連するバグの重大度が Severity2 の場合に、主要と表示されます。いくつかの例には次のものが含まれます。

- 現在ネットワークで動作しているスイッチまたはソフトウェアのバージョンに対して、重大 (Severity2) field notice または PSIRT が発行されている場合。
- ・ **[注意 (Warning)]** : アドバイザリは、潜在的にリスクがあるインフラストラクチャをサポートしている場合に注意として表示され、通知に関連するバグの深刻度は Severity3 です。いくつかの例には次のものが含まれます。
  - ファブリック内のスイッチがサポート終了状態に近づいている場合。現在ネットワークで動作しているスイッチまたはソフトウェアのバージョンに対して、Severity3 field notice または PSIRT が発行されている場合。

## アドバイザリの表示

Nexus Dashboard Insights では、以下の方法でアドバイザリを表示できます。

1. **[分析 (Analyze)]** > **[アドバイザリ**

**(Advisories)]** に移動します。または

1. **[概要 (Overview)]** > **[グローバル ビュー (Global View)]** に移動します。
2. ドロップダウンメニューからオンライン ファブリックまたはスナップショット ファブリックを選択します。
3. **[アドバイザリ レベル (Advisories Level)]** カードをクリックします。
4. **[アドバイザリ (Advisories)]** ページで、**[すべて**

のアドバイザリの表示 (**View all advisories**) ] をクリ

ックします。または

1. **[管理 (Manage)]** > **[ファブリック (Fabrics)]** に移動します。
2. ファブリックを選択します。
3. **[アドバイザリ**

**(Advisories)]** をク

リックします。また

は

1. **[管理 (Manage)]** > **[インベントリ (Inventory)]** に移動します。
2. **[コントローラ (Controllers)]** または **[スイッチ (Switches)]** をクリックします。
3. コントローラまたはスイッチを選択します。
4. **[アドバイザリ (Advisories)]** をクリックします。

## アドバイザリの分析

1. **[分析 (Analyze)]** > **[アドバイザリ (Advisories)]** に移動します。
2. ドロップダウンメニューからオンライン ファブリックまたはスナップショット ファブリックを選択します。
3. **[日付と時刻 (Date and Time)]** セレクタをクリックして、時間範囲を選択します。

[アドバイザリ (Advisories) ] ページには、選択した時間範囲に基づいて、アカウントのレベルとカテゴリ別にアドバイザリが表示されます。

- レベルの円グラフでは、アドバイザリのクリティカル、メジャー、注意の深刻度の合計数を表示します。

- カテゴリ円グラフは、PSIRT、Field Notice、HW EoL、SW EoL、およびベスト プラクティスなどカテゴリ別にアドバイザリの合計数を表示します。

- スナップショット ファブリックに表示されているアドバイザリについては、アドバイザリレベルが最新のスナップショットだけでなく、すべてのスナップショットにわたっています。

4. 検索バーを使用してアドバイザリをフィルタリングします。

5. [アドバイザリ (Advisories) ] テーブルにはフィルタされたアドバイザリが表示されます。アドバイザリはデフォルトでレベル別にソートされます。テーブル内のアドバイザリをソートするには、列見出しをクリックします。

アドバイザリ ステータスには、[アクティブ (Active) ] と [クリア (Cleared) ] が含まれます。[アクティブ (Active) ] 状態は、ネットワークにアドバイザリが存在することを示しています。[クリア (Cleared) ] 状態は、アドバイザリ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。

6. 歯車アイコンをクリックして、[アドバイザリ (Advisories) ] テーブルの列を構成します。デフォルトでは、タイトル、レベル、カテゴリ、ファブリック、および影響を受ける項目が表示されます。

7. アドバイザリをクリックして、問題点、影響、修正方法など追加の詳細を表示します。

- 問題点：特定の影響を受けるオブジェクトの問題を説明します。

- 影響：問題が修正されなかった場合に何が起こるかを説明し、主要な販売終了日を含めません。

- 修正方法：規範的な推奨事項を示します。

8. [アドバイザリ (Advisory) ] テーブルからアドバイザリを選択し、[アドバイザリの承認 (Acknowledge Advisories) ] をクリックして、アドバイザリを承認します。

a. アドバイザリをクリックして、[アドバイザリ (Advisory) ] ページで [アクション (Actions) ] メニューから [アドバイザリの承認 (Acknowledge Advisory) ] を選択できます。

デフォルトでは、すべての未承認アドバイザリがアドバイザリ テーブルに表示されます。アドバイザリを承認したら、ドロップダウン リストから [承認済み (Acknowledged) ] を選択し、承認されたすべてのアドバイザリを表示します。

9. アドバイザリをクリックして、[アドバイザリ (Advisory) ] ページを表示します。ブックマーク アイコンをクリックして、アドバイザリをブックマークします。

10. アドバイザリをクリックして、[アドバイザリ (Advisory) ] ページを表示します。ピン アイコンをクリックして、アドバイザリをピン接続します。

# アドバイザリフィルタ

検索バーを使用すると、アドバイザリをフィルタ処理できます。[アドバイザリ (Advisories) ] ページでは、次のフィルタを使用して、表示されるアドバイザリを絞り込むことができます。

- ・ [タイトル (Title) ] : 指定したタイトルのアドバイザリを表示します。
- ・ [アドバイザリ レベル (Advisory Level) ] : 特定のレベルのアドバイザリを表示します。
- ・ [検出時間 (Detection Time) ] : 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 (Last Seen time) ] - 特定の時刻のアドバイザリのみ表示されます。[最終確認時刻 (Last Seen Time) ] は、アクティブ ステータス中にアドバイザリが更新された時間を示します。アドバイザリのステータスがクリアになっていない場合、アドバイザリがアクティブになります。
- ・ [カテゴリ (Category) ] : 特定のカテゴリのアドバイザリを表示します。
- ・ [ファブリック (Fabric) ] : 特定のファブリックのアドバイザリを表示します。
- ・ [ノード (Nodes) ] : 特定のノードのアドバイザリを表示します。
- ・ 問題点 : 特定の影響を受けるオブジェクトのアドバイザリを表示し

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

## メタデータのサポート

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 パッケージは常に更新され、検証後に Cisco Intersight Cloud にポストされます。Nexus Dashboard Insights は、Nexus Dashboard プラットフォームに組み込まれているデバイスコネクタを介して Cisco Intersight Cloud に接続し、更新されたメタデータを定期的にプルします。Nexus Dashboard が Cisco Intersight Cloud に接続されていない場合、エアギャップ環境のメタデータ サポートを使用し、ユーザーは手動で、安全で信頼できる方法により最新のメタデータを Nexus Dashboard Insights にアップロードできます。バンドルの更新は、[Cisco DC App Center](#) からダウンロードできます。

[管理 (Admin) ] > [システム設定 (System Settings) ] > [メタデータ (Metadata) ] に移動して、メタデータ バージョンを表示します。

- ・ [全般 (General) ] エリアで、メタデータ バージョンが表示されます。
- ・ [メタデータ バージョンの更新 (Update Metadata Version) ] エリアで、エアギャップ環境のメタデータを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

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

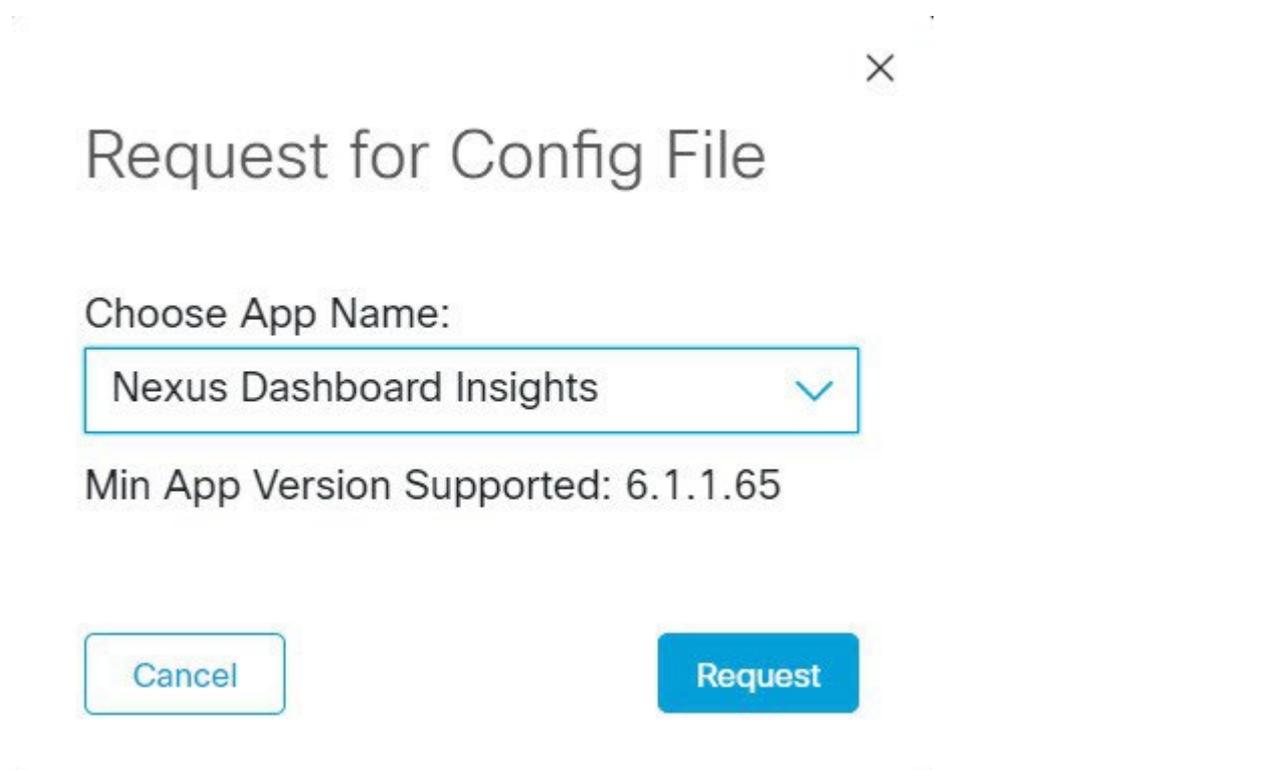
ない場合、安全で信頼できる方法で最新のメタデータをNexus Dashboard Insightsに定期的にアップロードできます。

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 にアップロードすると、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 (User) ] ドロップダウンメニューから [マイアカウント (My Account) ] を選択します。
3. [構成ファイルのリクエスト (Config Files Requests) ] タブをクリックします。
4. [構成ファイルのリクエスト (Request Config File) ] をクリックします。
5. [アプリIDの選択 (Choose App ID) ] ドロップダウンリストから、[Nexus Dashboard] を選択します。



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

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

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

Request Id	App Name	Created At	Last Update	Status	Version	Link
2	<a href="#">Nexus Dashboard Insights</a>	2022-02-25 17:47:16	2022-02-25 17:48:26	Processed	22	<a href="#">Download</a>

8. Cisco Nexus Dashboard Insightsにログインします。
9. [管理 (Admin) ] > [システム設定 (System Settings) ] > [メタデータ (Metadata) ] に移動して、

メタデータ バージョンを表示します。

10. [メタデータ バージョンの更新 (Update Metadata Version) ] 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。
11. [アップロードの開始 (**Begin Upload**) ] をクリックして、最新のメタデータをアップロードします。

# 著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。

商標または登録商標です。シスコの商標の一覧は、<http://www.cisco.com/go/trademarks> でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。(1110R)。

© 2017-2024 Cisco Systems, Inc. All rights reserved.