

# Cisco Network Assurance Engine 4.1 v1



最終更新日 : 20-May-2020

## このデモンストレーションについて

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

<a href="#">このデモンストレーションについて</a>	<a href="#">1</a>
<a href="#">要件</a>	<a href="#">2</a>
<a href="#">このソリューションについて</a>	<a href="#">2</a>
<a href="#">トポロジ</a>	<a href="#">3</a>
<a href="#">はじめに</a>	<a href="#">4</a>
<a href="#">シナリオ 1. 変更管理</a>	<a href="#">6</a>
<a href="#">シナリオ 2. データセンター運用</a>	<a href="#">18</a>
<a href="#">シナリオ 3. 移行</a>	<a href="#">28</a>
<a href="#">シナリオ 4. エポックデルタ分析</a>	<a href="#">32</a>
<a href="#">シナリオ 5. コンプライアンス分析</a>	<a href="#">35</a>
<a href="#">付録 A : ラボ ACI ファブリックの物理/論理トポロジ</a>	<a href="#">42</a>

## 要件

次の表に、このデモンストレーションの要件の概要を示します。

必須	オプション
ラップトップ	Cisco AnyConnect®

## このソリューションについて

このデモンストレーションは、実践的なシナリオを通じて Cisco Network Assurance Engine (NAE) について学ぶ機会としてご利用いただけます。また、シスコパートナーとお客様が製品を評価し、製品の強化と将来の開発に向けた貴重なフィードバックをご提供いただく機会ともなります。

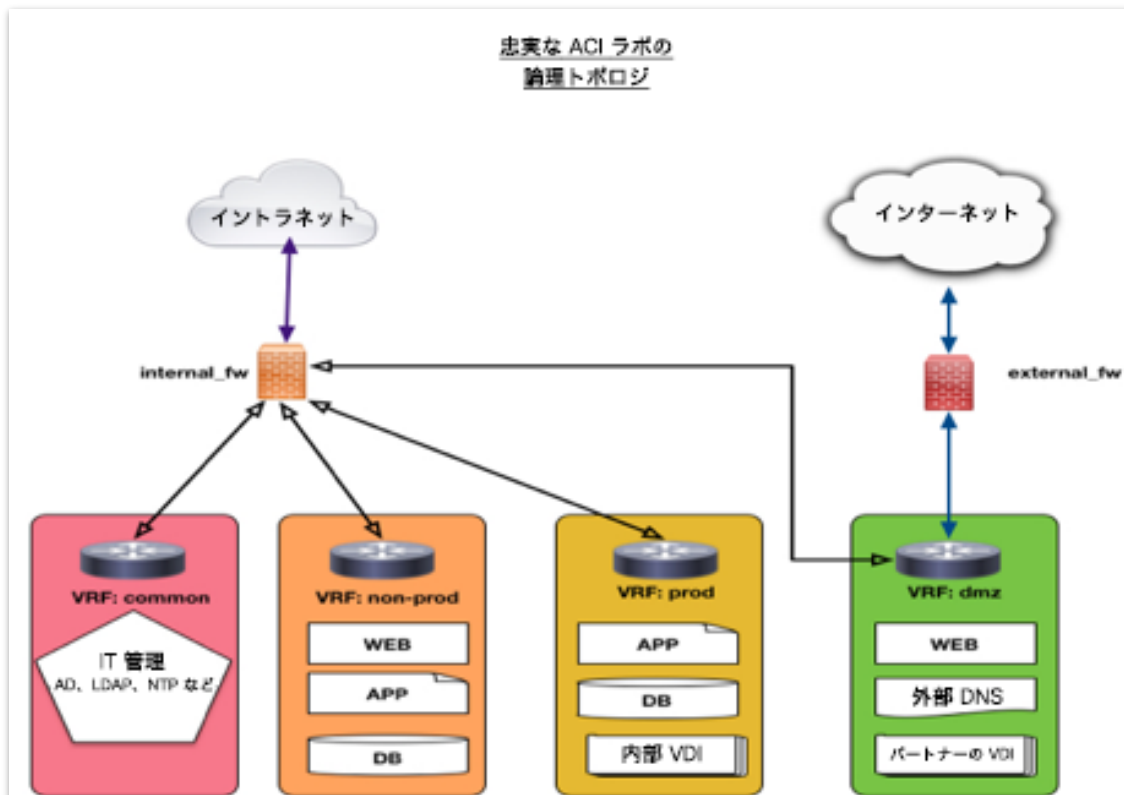
このインスタント デモンストレーションでは、複数の収集済みデータセットを使用して、オフラインモードで動作する共有 CNAE インスタンスにアクセスします。データセットは、実世界のネットワークシナリオを再現した ACI ファブリックから収集されたものです。各シナリオは、具体的な導入例を示す製品のガイド付きツアーで、変更管理やテナントエンドポイント、テナント転送、テナントセキュリティ、TCAM リソース分析などが含まれます。導入例では製品について学び、各ページの目的を知ることができます。デモンストレーションでは NAE をツールとして使い、実世界の問題を解決します。NAE の機能について学習し、その GUI に慣れることができます。

トポロジを確認し、セットアップについて理解を深めてください。これは導入例を理解するうえで役立ちます。

## トポロジ

ラボの ACI ファブリックは、6 つのリーフと 2 つのスパインで構成されます。物理トポロジの詳細については、付録 A を参照してください。

ACI ファブリックは、common、non-prod、prod および dmz を含む 4 つのテナントから成るマルチテナント データセンター ファブリックです。各テナントには、テナントと同じ名前で作成された VRF があります。VRF では、定義した EPG のブリッジドメインが作成されます。EPG はアプリケーション層と機能に基づいてセグメント化されます。テナント間のトラフィックは、内部ファイアウォールを経由します。インターネットトラフィックは、外部ファイアウォールを経由して DMZ に入り、内部ファイアウォールを経由して他のテナントにアクセスする必要があります。テナントネットワークとアプリケーション設定の詳細については、付録 A を参照してください。



注：これは共有環境なので、CNAE で独自のオフライン分析を実行しないでください。それによって、他のユーザの環境を損なうことになります。

## はじめに

### PRESNETING の前に

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

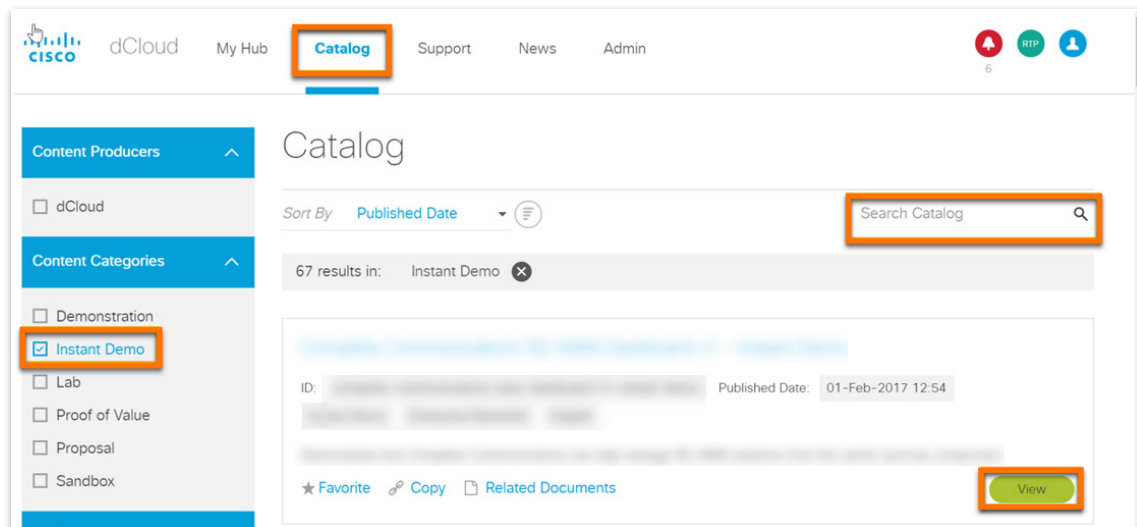
場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

**プレゼンテーションを成功させるには入念な準備が不可欠です。**

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

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

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



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

このラボには、ラボ ACI ファブリックから収集された複数のオフラインのデータセットが含まれています。ラボでの作業を簡素化するため、一部のデータセットには、オフライン分析用に独自のアシュアランスグループが設定されています。他のデータセットは、同一のアシュアランスグループ (ラボのタスクに応じて異なる) に属しています。

アシュアランスグループ間を切り替えるには、Cisco NAE GUI の右上にあるドロップダウンセレクトを使用します。

このラボには 6 つのシナリオがあります。各シナリオに適切なアシュアランスグループを使用していることを確認してください。

- **変更管理**導入例：「変更管理」アシュアランスグループを使用してください
- **データセンター運用**導入例：「データセンター運用」アシュアランスグループを使用してください
- **移行**導入例：「移行」アシュアランスグループを使用してください
- **エポックデルタ分析**導入例：「エポック分析」アシュアランスグループを使用してください
- **セグメンテーション コンプライアンス**導入例：「セグメンテーション コンプライアンス」アシュアランスグループを使用してください
- **設定コンプライアンス分析**導入例：「設定コンプライアンス分析」アシュアランスグループを使用してください

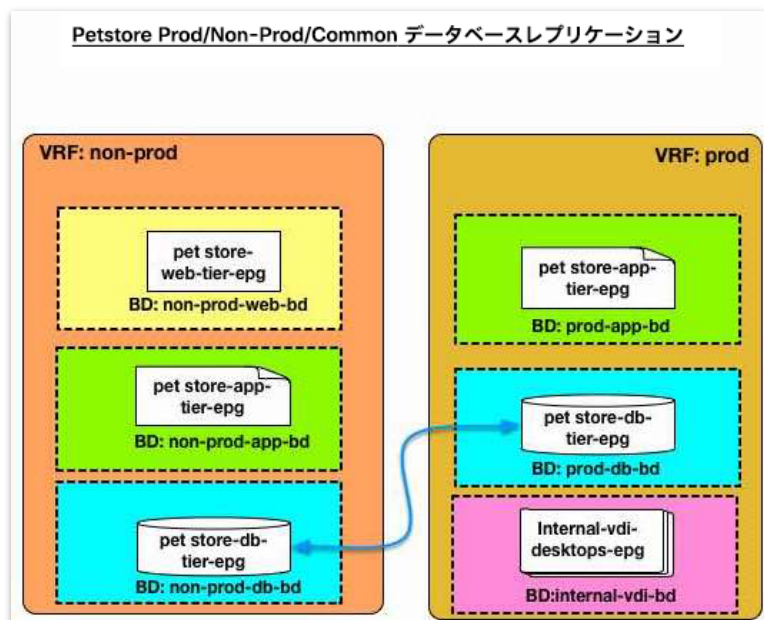
## シナリオ 1. 変更管理

### 価値提案：

Cisco NAE の主要な機能の 1 つは、ACI ファブリックの設定エラーやベストプラクティスからの逸脱についてネットワーク管理者に速やかに警告することです。

### シナリオ 1.1

DB 管理者は、ビジネスを行う上で十分な正当な理由を示して、**prod** および **non-prod** テナントの **petstore-db-tier** EPG でホストされている DB インスタンス間で、中断のない DB の複製と同期の要求を出しました。

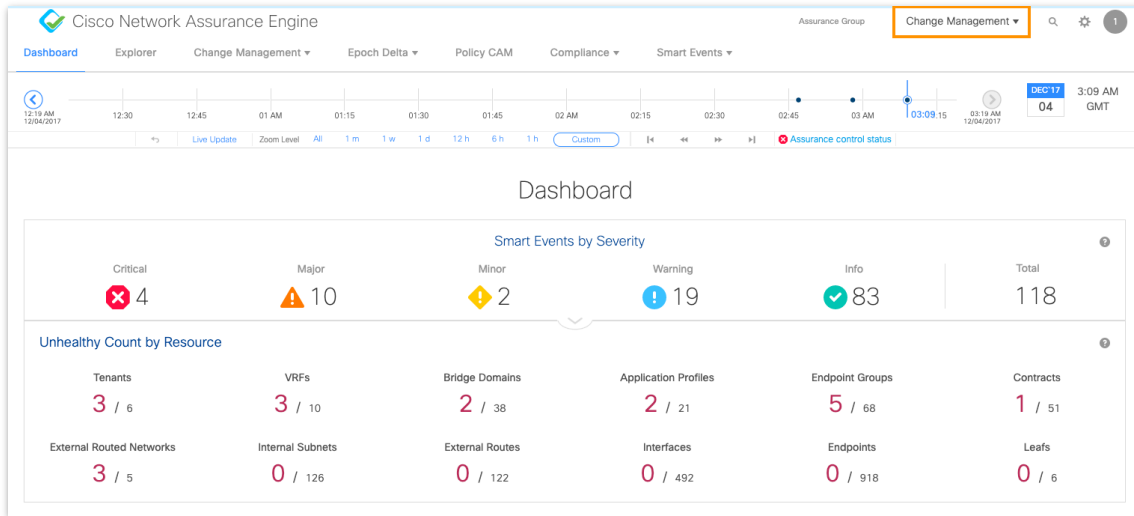


ネットワーク管理者は、このテナント間契約を作成または変更する際に、明確に指定されたセキュリティポリシーについて把握しておく必要があります。

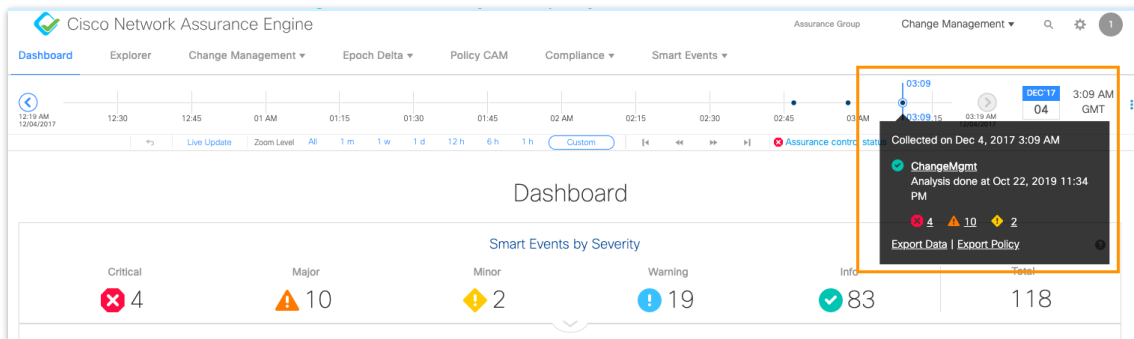
**要件：** **prod** テナントの **petstore-db-tier** EPG と **non-prod** テナントの **petstore-db-tier** EPG 間の双方向で SQL 接続 (tcp 1521) を許可します。

**設定：** テナント **non-prod** の **petstore** EPG は、契約「NP-PS\_DB-P\_PS\_DB-contract」を提供しています。この契約は、**non-prod** テナントによってエクスポートされ、**prod** テナントによってインポートされてから、**prod** の **petstore-db-tier** EPG によって利用されます。

**問題：** 管理者は、**non-prod** DB サーバが **prod** DB サーバに対する SQL 接続 (tcp、1521) を確立できないことに気がきました。



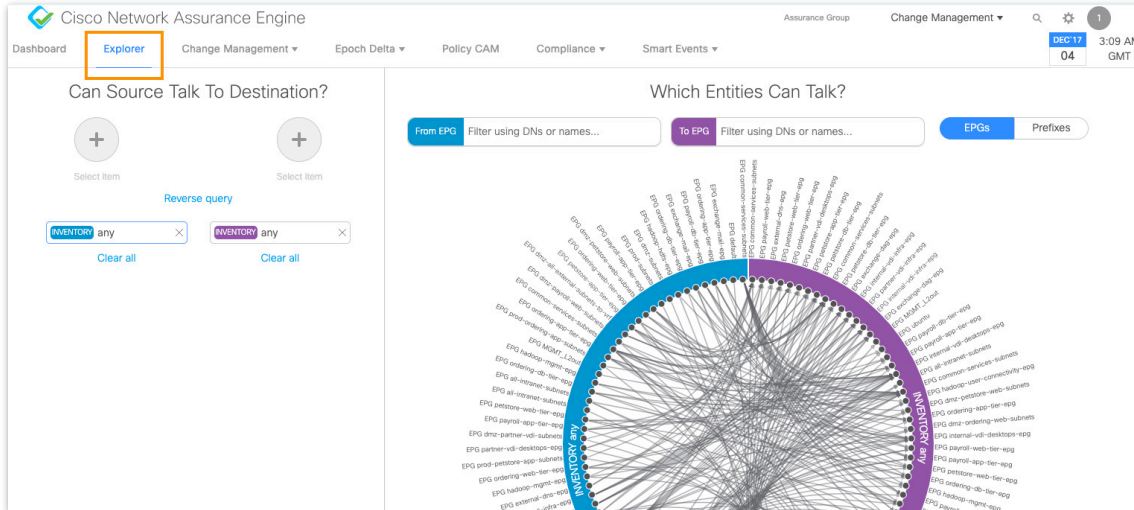
1. 上で強調表示されているように、[変更管理 (Change Management)] が選択されていることを確認します。



2. 上で強調表示されているように、[タイムライン (Timeline)] で、直近の [エポック (Epoch)] をクリックします。

**価値提案：**分析のためにエポックを選択したときに最初に表示されるものは、[CISCO NAE アプライアンスダッシュボード (Cisco NAE Appliance Dashboard)] です。ダッシュボードには、ファブリック全般の状態が迅速かつ詳細に表示されます。すべてのイベントの概要がダッシュボードに示されるため、テナントやリーフ別、および他のさまざまなカテゴリ別にイベントを分類できます。この画面でしばらく時間をとり、画面の右側にあるスクロールボタンを使用して上下方向にスクロールし、表示されるすべての情報を確認してください。

**注：**以下のスクリーンショット、およびそれ以降のすべてのスクリーンショットに表示される数字は、ラボに展開されているアプライアンスに表示される番号とは異なる場合があることに注意してください。



3. [エクスプローラ (Explorer) ] タブをクリックします。[ネットワークアシュアランスエンジン (Network Assurance Engine) ] には、通信できるエンティティを可視化したものが表示されます。

**価値提案 :** エクスプローラの機能により、Cisco APIC からのポリシースナップショットが分析され、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。

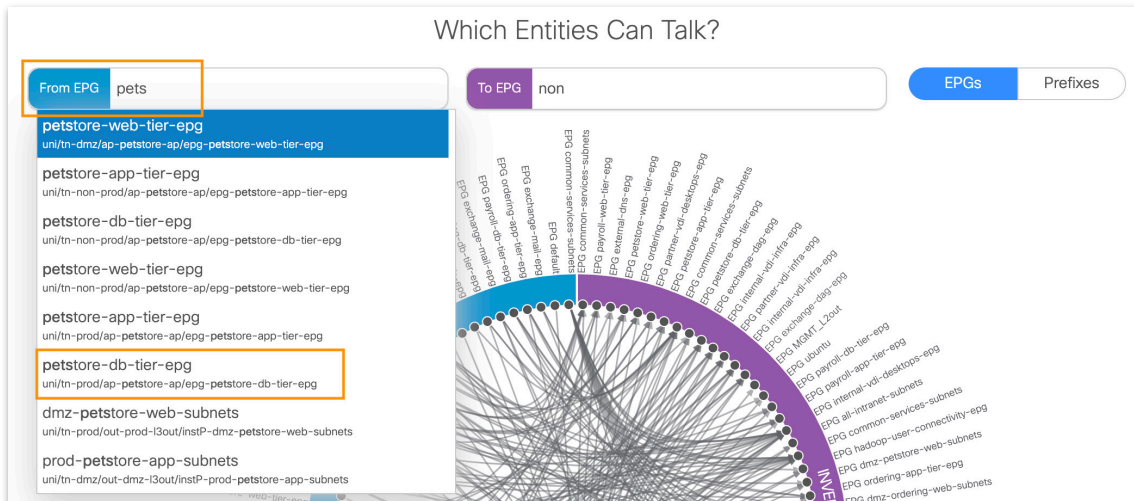
- ACI オブジェクトモデルと関連付けを調査する
- ネットワーク資産間の接続とセグメンテーションを検証する

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

**What Query :** 異なる ACI ネットワークエンティティがどのように相互に関連しているかについての情報が得られます。

**Can Query :** ACI ポリシー内のエンティティが相互に通信できるかどうかについての情報が得られます。Can queries はまた、TCP、UDP、ICMP などのプロトコル、および通信に使用される送信元と宛先ポートを使用して、ACI ポリシー内のエンティティが通信できるかどうかを判断するためにも使用されます。

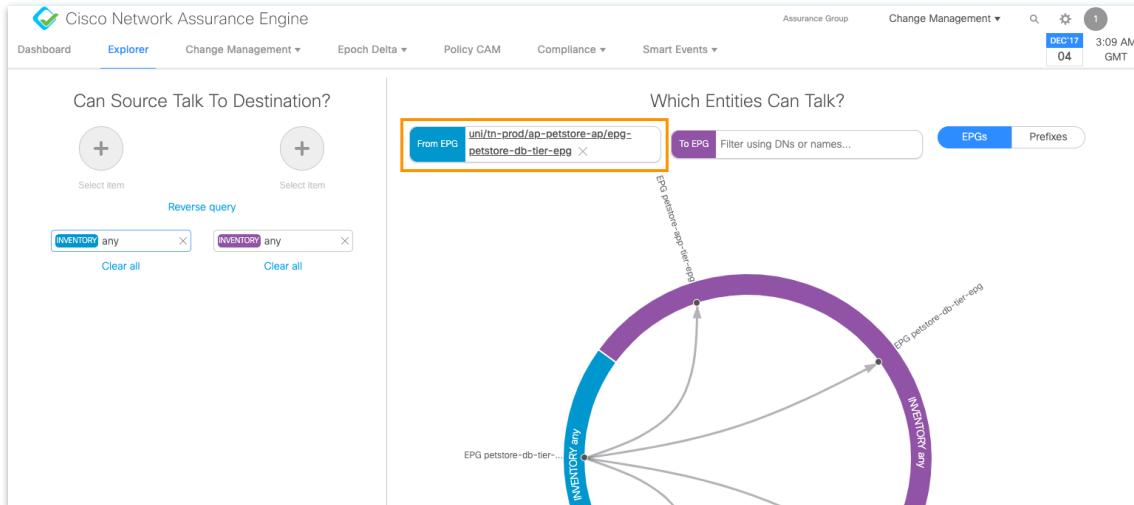
**View Query :** アシュアランスグループの任意のリーフスイッチのインターフェイスステータスを視覚的に示します。





4. [EPG から (From EPG) ] フィールドに *pets* と入力し、（開いたドロップダウンから）上で強調表示された **(tn-prod) petstore-db-tier-epg** オプションを選択します。

可視化の状態が更新され、**petstore-db-tier-epg** が通信できる EPG が表示されます。

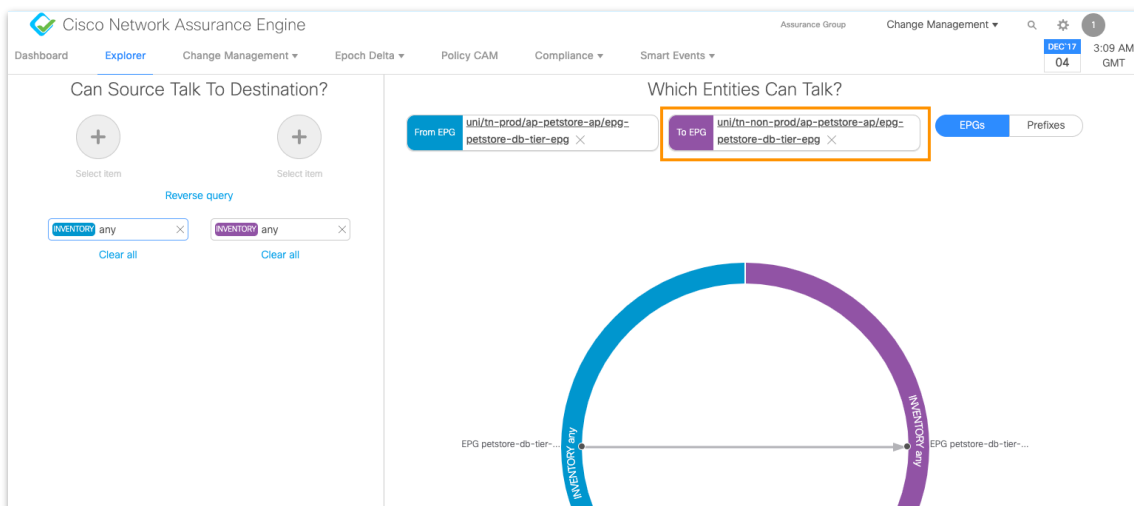


**価値** : CISCO NAE によりポリスペースを簡単に分析し、次の質問に答えることができます。EPG-A に対して必要なすべてのポリシーが正しく設定され、それらのポリシーがスイッチの TCAM テーブルで正しくプログラムされているか。

- 互いに通信できる EPG はどれか。
- 必要なすべての契約があるか、または不足しているものがあるか。
- テナントに必要な隔離が行われているか。
- 各契約の具体的な詳細情報

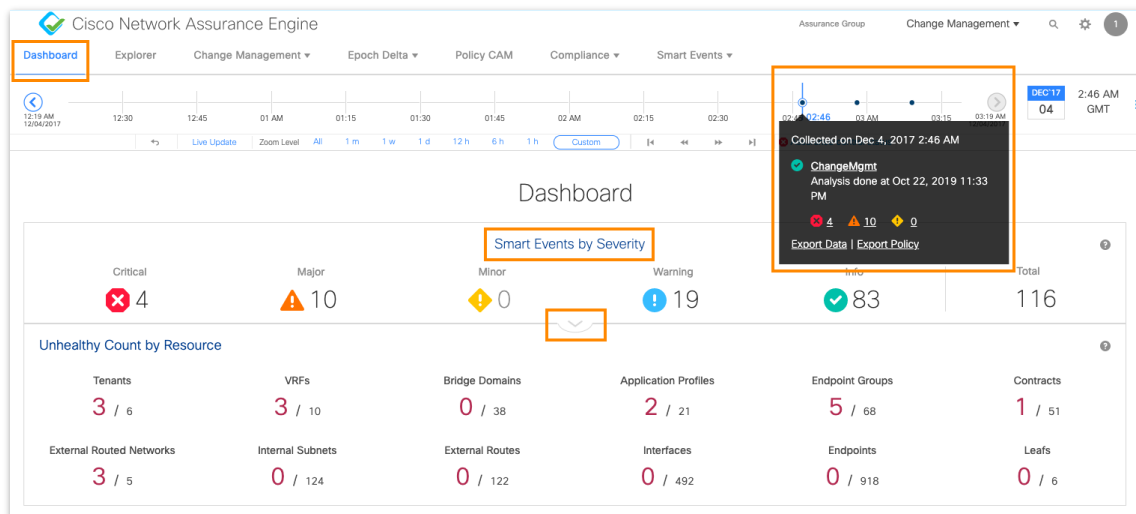
5. [EPG へ (To EPG) ] フィールドに *non* と入力し、（開いたドロップダウンから）[petstore-db-epg] オプションを選択します。

可視化の状態が更新され、**petstore-db-tier-epg** が通信できる EPG が表示されます。

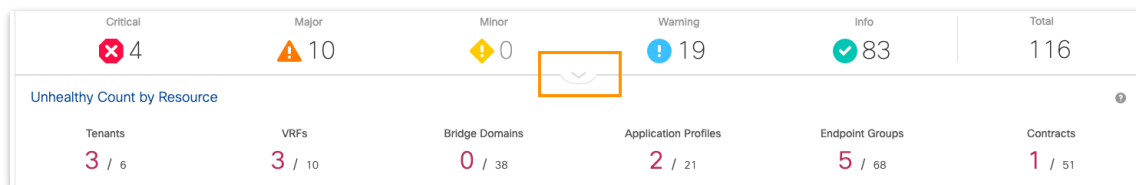


**Network Assurance Engine** がこの情報を表示する方法はいくつかあります。アプライアンスを介して移動し、イベントが特定されているかどうかを確認します。

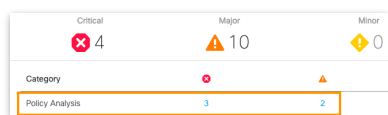
## シナリオ 1.2



1. [ダッシュボード (Dashboard) ]タブをクリックします。
2. [タイムライン (Timeline) ]で、最も古い[エポック (Epoch) ]をクリックします。



3. [重大度別のスマートイベント (Smart Events by Severity) ]パネルで、[ビューの拡張 (Expand View) ]ボタンをクリックします。



4. [ポリシー分析 (Policy Analysis) ]行で、2 をクリックします。

[イベントの説明 (Event Descriptions) ]には、**prod** の **petstore-db-tier** と **non-prod** の **petstore-db-tier** 間の問題についての説明が示されます。

Severity	Event Category	Event Subcategory	Event Name	Count	Event Description
	Filter	Filter	Filter		
▲	CHANGE_ANALYSIS	SECURITY_POLICY	<b>CONSUMER_EPG_HAS_NO_SCOPE_MATCHING_PROVIDERS</b>	1	An incorrect contract scope configuration is preventing communication between the Provider and the Consumer EPGs.
▲	CHANGE_ANALYSIS	SECURITY_POLICY	PROVIDER_EPG_HAS_NO_SCOPE_MATCHING_CONSUMERS	1	An incorrect contract scope configuration is preventing communication between the Provider and Consumer EPGs.

5. 上で強調表示されている [イベント名 (Event Name) ] をクリックします。

Smart Events of CONSUMER\_EPG\_HAS\_NO\_SCOPE\_MATCHING\_PROVIDERS

Severity ▲ Major    Event Category CHANGE\_ANALYSIS    Event Subcategory SECURITY\_POLICY  
Event Description An incorrect contract scope configuration is preventing communication between the Provider and the Consumer EPGs.

1 rows

Epochs	Event Id	EPGs
<a href="#">12/04/2017 02:46 AM GMT</a>	6bd462ab1b7b451315065064c4c446fa	petstore-db-tier-epg

Rows 10 25 50 100

Close

6. 上で強調表示されている [エポック (Epoch) ] をクリックします。

Smart Events of CONSUMER\_EPG\_HAS\_NO\_SCOPE\_MATCHING\_PROVIDERS

Severity ▲ Major    Event Category CHANGE\_ANALYSIS    Event Subcategory SECURITY\_POLICY  
Event Description An incorrect contract scope configuration is preventing communication between the Provider and the Consumer EPGs.

1 rows

Epochs	Event Id	EPGs
<a href="#">12/04/2017 02:46 AM GMT</a>	6bd462ab1b7b451315065064c4c446fa	petstore-db-tier-epg

Total Duration 22min 4sec (3 Epochs)

First Raised (1 Epochs) Last Raised Clearing Cleared

12/04/2017 02:46:59 AM 12/04/2017 02:46:59 AM 12/04/2017 02:57:59 AM 12/04/2017 03:09:03 AM

Zoom Level Lifecycle 12 h 6 h 3 h 1 h

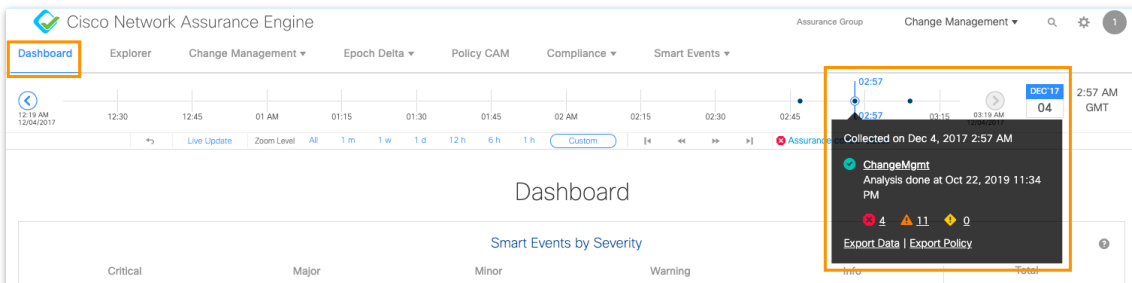
< Previous Occurrence      12/04/2017 02:46 AM GMT      Next Occurrence >

7. ページを上スクロールして、[スマートレポート (Smart Report) ] を表示します。

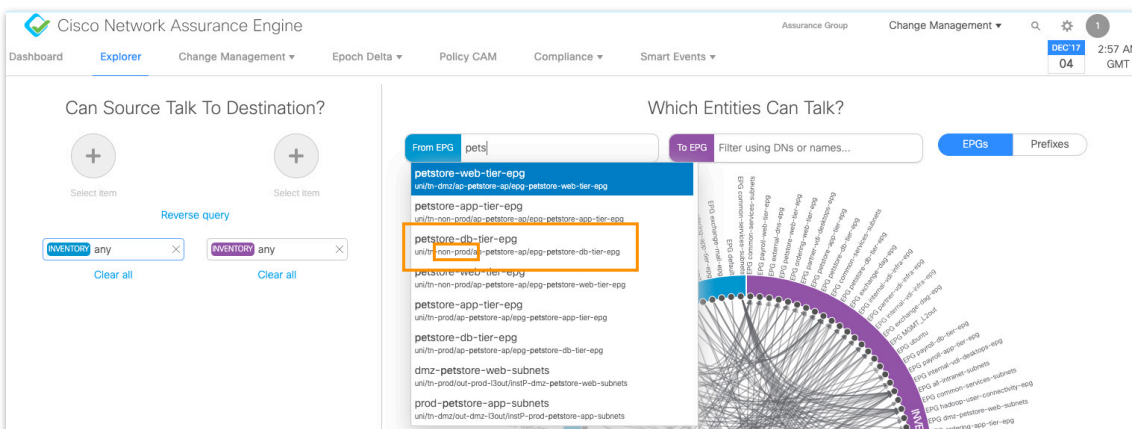
Description	An incorrect contract scope configuration is preventing communication between the Provider and the Consumer EPGs.				
Impact	No communication between the Provider and the Consumer EPGs is possible.				
Affected Objects Details	<table border="1"> <tr> <td>Consumer EPG</td> </tr> <tr> <td><b>petstore-db-tier-epg</b></td> </tr> </table>			Consumer EPG	<b>petstore-db-tier-epg</b>
Consumer EPG					
<b>petstore-db-tier-epg</b>					
Checks	Check Code	Falling Condition	Suggested Next Steps		
	83	Contract scope is not sufficient to allow communication between the Provider and the Consumer EPGs.	<p>Check to see if the Provider and the Consumer EPGs are required to communicate with each other using the listed contracts.</p> <ul style="list-style-type: none"> <li>If connectivity is required, change the contract scope to allow communication between the EPGs. The possible contract scopes are AppProfile, VRF, Tenant or Global.</li> <li>If connectivity is not required, remove the consumer (not provider) side of the contract relationship.</li> </ul>		
The following Contracts consumed by Consumer EPG : <b>petstore-db-tier-epg</b> have insufficient scope:					
Contracts	Current scope	Min. Scope needed to match atleast one Consumer	List of Provider EPGs		
NP-PS_DB-P_PS_DB-contract *	<b>tenant</b>	global	uni/tn-non-prod/ap-petstore-ap/epg-petstore-db-tier-epg		
			Max. Scope needed to match all Consumers		
			<b>global</b>		

[チェック (Checks) ] 行は、**NP-PS\_DB-P\_PS\_DB-contract** の範囲が [グローバル (global) ] であるべきときに、[テナント (tenant) ] であることを示しています。[グローバル (global) ] の範囲は、異なるテナントの EPG 間の通信を許可します。

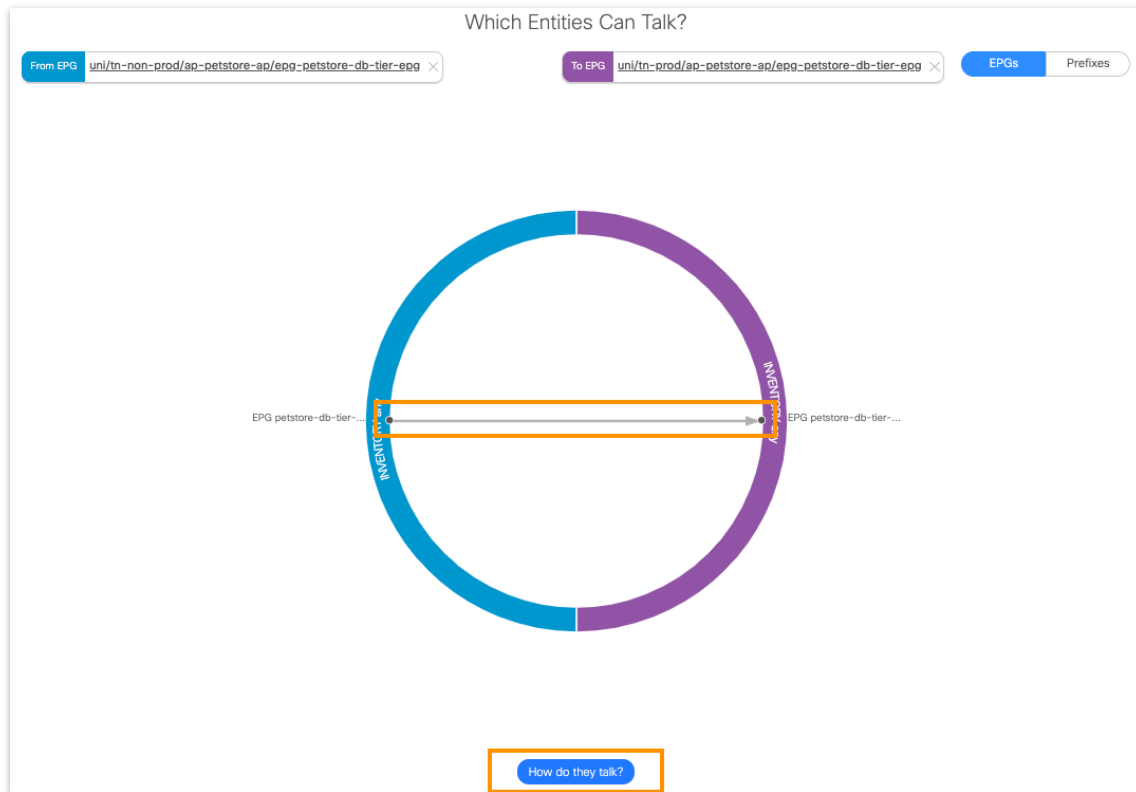
### シナリオ 1.3



1. [ダッシュボード (Dashboard) ] タブで、上で強調表示されている 2 番目の [エポック (Dashboard) ] をクリックします。
2. [エクスプローラ (Explorer) ] タブをクリックします。



- [ EPG から (From EPG) ] フィールドに *pets* と入力し、 (開いたドロップダウンから) 上で強調表示された **(tn-non-prod) petstore-db-tier-epg** オプションを選択します。
- [ EPG へ (To EPG) ] フィールドに *pets* と入力し、 (開いたドロップダウンから) **(tn-prod) petstore-db-tier-epg** オプションを選択します。



- 上で強調表示された、[ 契約 (Contract) ] 行をクリックします。
  - [ 通信方法 (How To Talk) ] ボタンをクリックします。
- [ 通信方法 (How To Talk) ] パネルには、通信の詳細が表示されます。

Source EPG	Destination EPG	Source Prefix	Destination Prefix	Source VRF	Destination VRF
petstore-db-tier-epg	petstore-db-tier-epg	10.71.0.0/24	10.65.0.0/24	non-prod-vrf	prod-vrf
petstore-db-tier-epg	petstore-db-tier-epg	10.13.0.0/24	10.65.0.0/24	non-prod-vrf	prod-vrf

Source EPG	Destination EPG	Policy Enforcement V...	Policy Owner	Ether Type	Protocol	Source Port From	Source Port To	Destination Port From	Destination Port To	TCP Rules
petstore-db-tier-epg	petstore-db-tier-epg	prod-vrf	NP-PS_DB-P_PS_DB...	ip	icmp	unspecified	unspecified	unspecified	unspecified	unspecified
petstore-db-tier-epg	petstore-db-tier-epg	prod-vrf	NP-PS_DB-P_PS_DB...	ip	tcp	1521	1521	unspecified	unspecified	unspecified

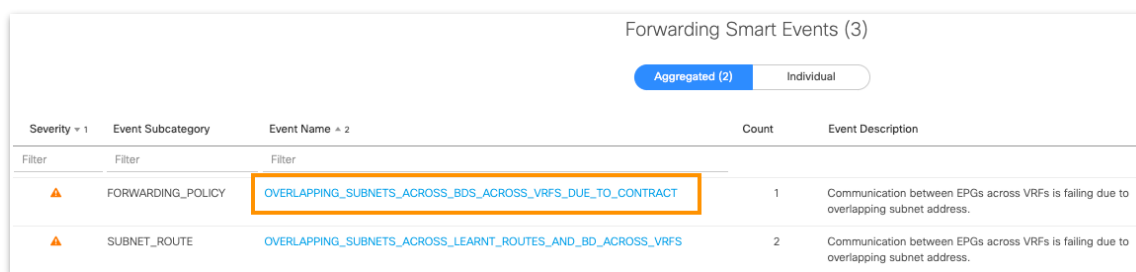
注：2 番目の [エポック (Epoch)] では、契約範囲の mis-configuration が [テナント (tenant)] から [グローバル (global)] に修正されています。

価値： 前の設定ミスが修正されたことを即座に確認できます。数回クリックするだけで、契約スペース全体を直感的かつ詳細に可視化できます。

ただし、[転送 (Forwarding)] タブにアラートが表示されているということは、修正すべき転送の問題があることを意味します。

7. [転送 (Forwarding)] タブをクリックします。

8. ページを上スクロールして、[スマートイベントの転送 (Forwarding Smart Events)] セクションを表示します。



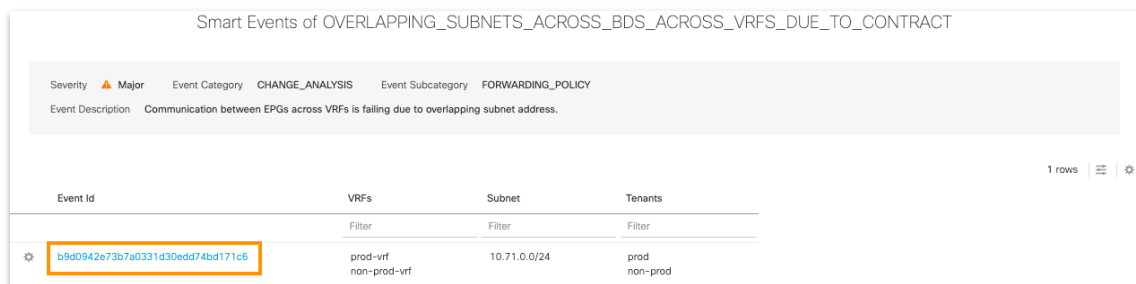
Forwarding Smart Events (3)

Aggregated (2) Individual

Severity v 1	Event Subcategory	Event Name v 2	Count	Event Description
▲	FORWARDING_POLICY	OVERLAPPING_SUBNETS_ACROSS_BDS_ACROSS_VRFs_DUE_TO_CONTRACT	1	Communication between EPGs across VRFs is failing due to overlapping subnet address.
▲	SUBNET_ROUTE	OVERLAPPING_SUBNETS_ACROSS_LEARNED_ROUTES_AND_BD_ACROSS_VRFs	2	Communication between EPGs across VRFs is failing due to overlapping subnet address.

[イベントの説明 (Event Description)] には、重複するサブネットの問題が表示されています。

9. 上で強調表示されている [イベント名 (Event Name)] をクリックします。



Smart Events of OVERLAPPING\_SUBNETS\_ACROSS\_BDS\_ACROSS\_VRFs\_DUE\_TO\_CONTRACT

Severity ▲ Major Event Category CHANGE\_ANALYSIS Event Subcategory FORWARDING\_POLICY

Event Description Communication between EPGs across VRFs is failing due to overlapping subnet address.

1 rows

Event Id	VRFs	Subnet	Tenants
b9d0942e73b7a0331d30edd74bd171c6	prod-vrf non-prod-vrf	10.71.0.0/24	prod non-prod

10. 上で強調表示されている [イベント ID (Event Id)] をクリックします。

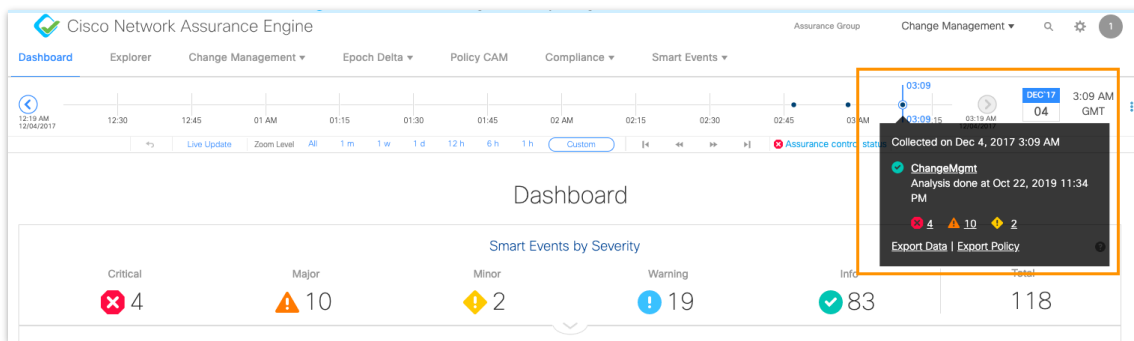
11. ページを上スクロールして、[スマートレポート (Smart Report)] を表示します。

Description	Communication between EPGs across VRFs is failing due to overlapping subnet address.						
Impact	Overlapping subnet configuration is causing intermittent connectivity problem between Provider and Consumer EPGs.						
Affected Objects Details	VRF in which overlap is seen	Prefix	VRF's Tenant				
	prod-vrf *	10.71.0.0/24 *	prod *				
Checks	Check Code	Failing Condition	Suggested Next Steps				
	39	Provider BD/EPG's subnet or Consumer BD/EPG's subnets are not unique across both VRF's	<ol style="list-style-type: none"> <li>1. Check if Provider and Consumer EPGs are required to communicate with each other using the listed contracts.</li> <li>2. If connectivity is required, ensure Provider EPG's BD subnet or Consumer EPG's BD subnet are unique across the VRF's.</li> <li>3. If connectivity is not required, determine if you can remove the consumer (not the provider) side of the imported contract relationship.</li> </ol>				
External leaked Prefix ownership information							
Leaked in Subnet	Owner EPG	Owner BD	Owner VRF				
[10.71.0.1/24]	petstore-db-tier-epg	non-prod-db-bd	non-prod-vrf				
Contract and EPG due to which Prefix leaked							
Leaked in Subnet	Affected Leaked-in VRF	EPG	EPG Type	List of Contracts	Originating Leaked-from VRF	EPG	EPG Type
10.71.0.0/24 *	prod-vrf *	petstore-db-tier-epg	Consumer	NP-PS_DB-P_PS_DB-contract	non-prod-vrf	petstore-db-tier-epg	Provider
Ownership of Subnets in the affected VRF which are impacted due to leaked Prefix							
Subnet in Affected VRF	Owner EPG	Owner BD	Owner VRF				
[10.71.0.1/24]	-	prod-internal-vdi-bd	prod-vrf *				

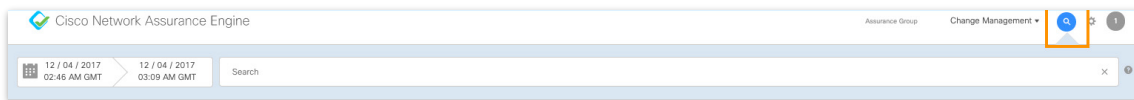
[影響を受けたオブジェクトの詳細 (Affected Objects Details) ] 行には、問題の場所が表示されます。

[チェック (Checks) ] 行には、問題を解決するうえで役立つ [推奨される次の手順 (Suggested Next Steps) ] が表示されます。

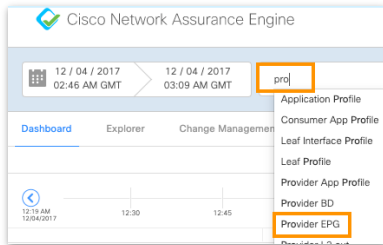
### シナリオ 1.4



1. 上で強調表示されているように、[タイムライン (Timeline) ] で、直近の [エポック (Epoch) ] をクリックします。

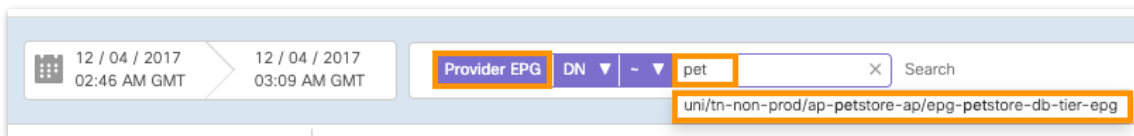


2. 上で強調表示されている [検索 (Search) ] (虫眼鏡) ボタンをクリックします。



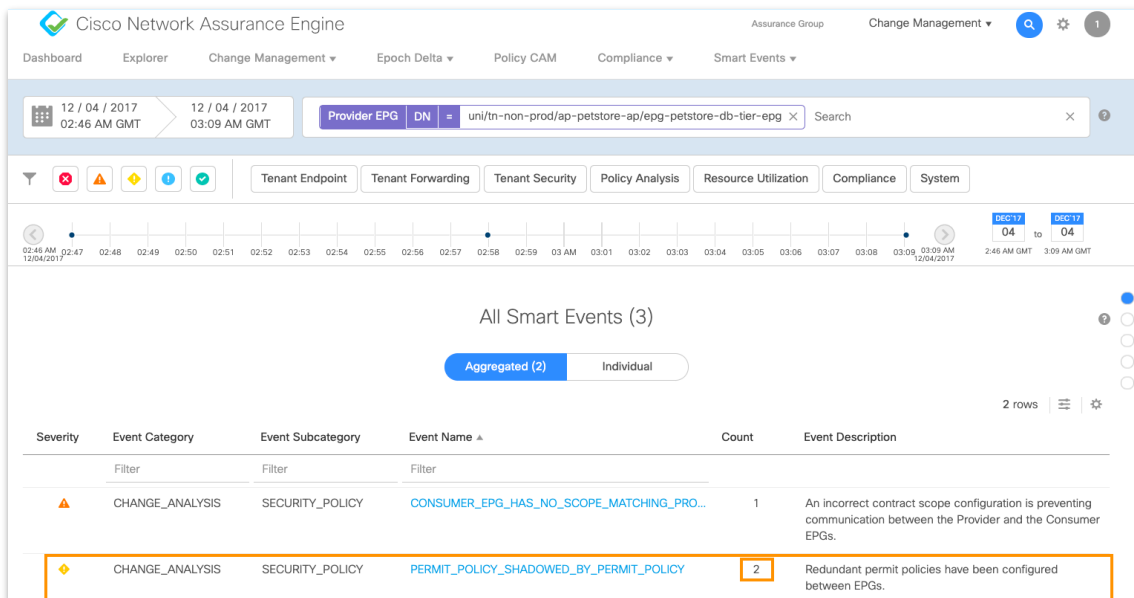
3. [検索 (Search) ] フィールドに *pro* と入力します。

4. ドロップダウンから、[プロバイダー-EPG (Provider EPG) ] オプションを選択します。



5. [=] フィールドに *pet* と入力します。

6. ドロップダウンから、**uni/tn-non-prod/ap-petstore-ap/epg-petstore-db-tier-epg** オプションを選択します。



**注 :** 2 つの「許可ポリシー」が存在します。

**価値 :** ポリシーが 10,000 以上ある場合、長年さまざまなチームや個人によってプログラミングされた結果であることがほとんどであるため、手動による検査でポリシー間の関係を理解することは不可能です。この結果、矛盾したポリシーや誤ったポリシーが発生し、ポリシーの数がますます増加しています。Cisco NAE のセキュリティポリシーモデルは、正確性、競合、および使用率に関してポリシーを継続的に監査するための強力なメカニズムをオペレータに提供します。

7. **PERMIT\_POLICY\_SHADOWED\_BY\_PERMIT\_POLICY** リンクをクリックします。



Smart Events of PERMIT\_POLICY\_SHADOWED\_BY\_PERMIT\_POLICY

Severity ◆ Minor    Event Category CHANGE\_ANALYSIS    Event Subcategory SECURITY\_POLICY

Event Description Redundant permit policies have been configured between EPGs.

2 rows | ☰ | ✖

Epochs	Event Id	Provider EPGs	Consumer EPGs	Contracts
		Filter	Filter	Filter
<span style="border: 1px solid orange; padding: 2px;">12/04/2017 03:09 AM GMT</span>	106a1a55c4af099f00a4aecee343b1d5	petstore-db-tier-epg	petstore-db-tier-epg	NP-PS_DB-P_PS_D
12/04/2017 03:09 AM GMT	c83bf3ee8e429baa6547ea678ea07ae6	petstore-db-tier-epg	petstore-db-tier-epg	NP-PS_DB-P_PS_D

8. 最初の [エポック (Epoch) ] をクリックします。

Description	Redundant permit policies have been configured between EPGs.							
Affected Objects Details	Provider EPG	Consumer EPG	Contract	Filter	Filter Entry	Directionality	Filter Entry Description	
	petstore-db-tier-epg *	petstore-db-tier-epg *	NP-PS_DB-P_PS_DB-contract *	icmp *	5_0 *	Forward *	[ icmp ] *	
Checks	Check Code	Failing Condition	Suggested Next Steps					
	118	Unique Filter entries are utilized to permit communication between EPGs.	<ol style="list-style-type: none"> <li>Determine which services are required for the Provider and Consumer EPGs.                             <ul style="list-style-type: none"> <li>Determine which permit policy, of those identified, best matches the communication requirements for the identified EPGs.</li> </ul> </li> <li>Remove the permit policy that is no longer required, ensuring that it is either a duplicate or subset of the policy identified as the correct policy.</li> </ol>					
Shadowing Policy Information								
	Provider EPG	Consumer EPG	Contract	Subject	Filter	Filter Entry	Directionality	Filter Entry Description
	petstore-db-tier-epg *	petstore-db-tier-epg *	NP-PS_DB-P_PS_DB-contract *	NP-PS_DB-P_PS_DB-subject *	oracle_default_leak	46_1	Forward *	[ icmp ]
Event ID/Code	Event ID						Code	
	23fb9488-2a315baf-0f0c-3a87-996e-c506b4e88e16-106a1a55c4af099f00a4aecee343b1d5						10020	

[説明 (Description) ] 行は、冗長ポリシーが存在することを示しています。

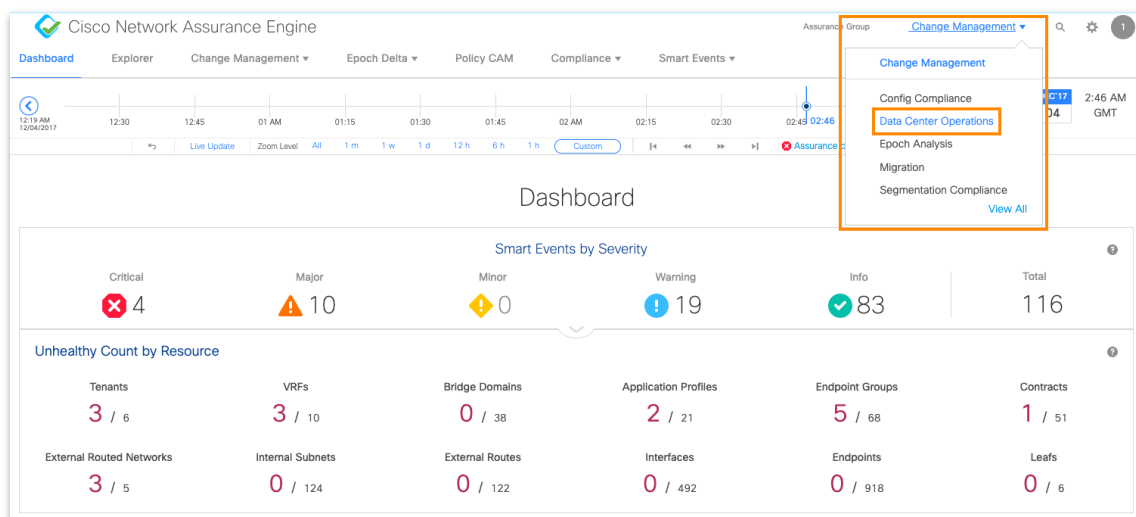
[チェック (Checks) ] 行には、冗長性の問題を解決するうえで役立つ [推奨される次の手順 (Suggested Next Steps) ] が表示されます。

**注:** 上記のイベントは、契約 **NP-PS\_DB-P\_PS\_DB-contract** 内に、どちらも ICMP を許可する 2 つのフィルタエントリがあることを説明しています。Cisco NAE は、2 つの異なるフィルタで同じプロトコルを許可してよいのかを確認しています。冗長 ICMP フィルタエントリの必要性はあると思いますか。このようなシャドーポリシーを場合の注意事項は何ですか。

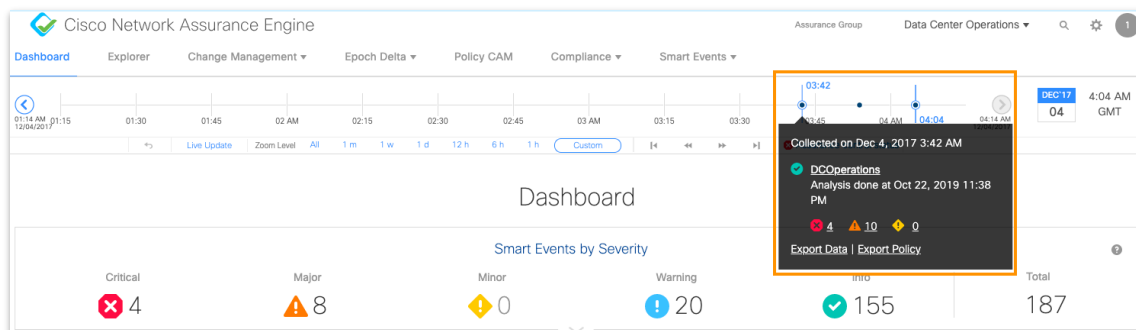
## シナリオ 2. データセンター運用

データセンター - ネットワーク オペレーション センター チームが日々直面するのは、問題レポートの一般的な性質です。たとえば、ネットワーク オペレーション センターが、アプリケーションへの到達不能に関するコールを受けるとします。Cisco **Network Assurance Engine** の継続的なネットワークアシュアランスは、問題を効率的に分析し、迅速な解決策を提供するのに役立つ洞察をネットワーク オペレーション センター チームにほぼリアルタイムで提供するように支援します。

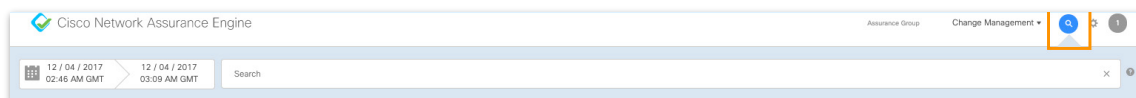
### シナリオ 2.1 : 同じ IP アドレスを持つ複数の MAC アドレス



1. [アシュアランスグループ (Assurance Group) ] ドロップダウンから、[データセンター運用 (Data Center Operations) ] オプションを選択します。



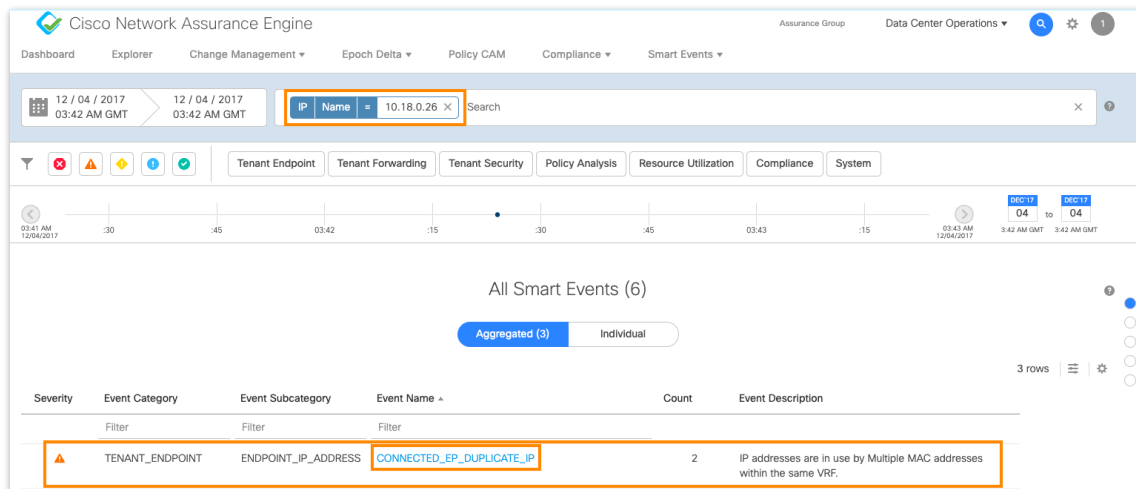
2. [タイムライン (Timeline) ] で、最初の [エポック (Epoch) ] をクリックします。



3. 上で強調表示されている [検索 (Search) ] (虫眼鏡) ボタンをクリックします。



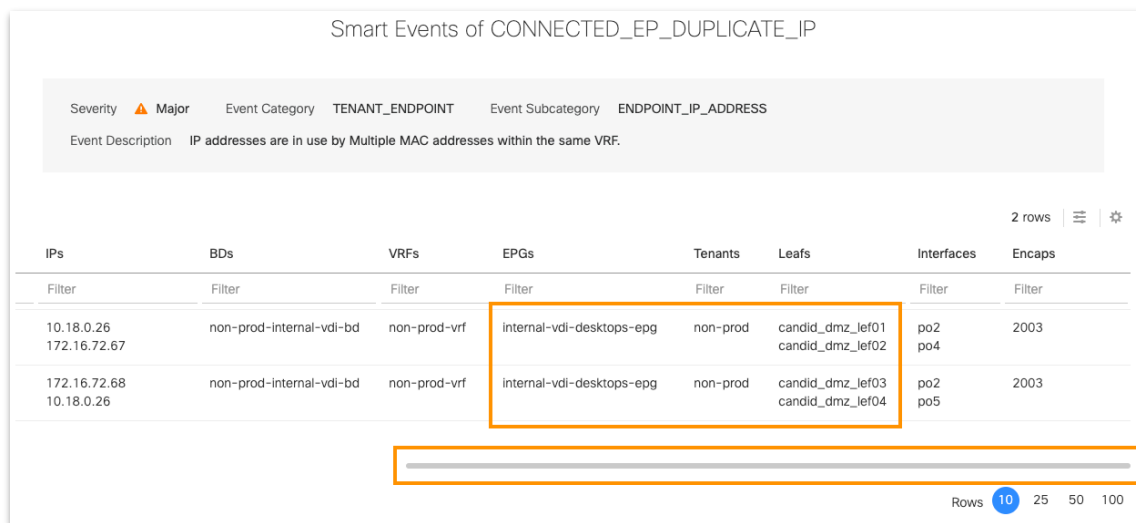
4. [検索 (Search) ] フィールドに *ip* と入力します。
5. ドロップダウンから、[IP] オプションを選択します。
6. [=] フィールドに *10.18.0.26* と入力します。
7. ドロップダウンから **10.18.0.26** オプションを選択します。



The screenshot shows the Cisco Network Assurance Engine interface. At the top, the search bar is set to "IP Name = 10.18.0.26". Below the search bar, there are several tabs: Tenant Endpoint, Tenant Forwarding, Tenant Security, Policy Analysis, Resource Utilization, Compliance, and System. The "Tenant Endpoint" tab is selected. The main content area displays "All Smart Events (6)" with a filter for "Aggregated (3)". A table shows the search results:

Severity	Event Category	Event Subcategory	Event Name	Count	Event Description
▲	TENANT_ENDPOINT	ENDPOINT_IP_ADDRESS	<a href="#">CONNECTED_EP_DUPLICATE_IP</a>	2	IP addresses are in use by Multiple MAC addresses within the same VRF.

8. **CONNECTED\_EP\_DUPLICATE\_IP** リンクをクリックします。



The screenshot shows the "Smart Events of CONNECTED\_EP\_DUPLICATE\_IP" page. It displays a table with the following columns: IPs, BDs, VRFs, EPGs, Tenants, Leafs, Interfaces, and Encaps. The table contains two rows of data:

IPs	BDs	VRFs	EPGs	Tenants	Leafs	Interfaces	Encaps
10.18.0.26 172.16.72.67	non-prod-internal-vdi-bd	non-prod-vrf	internal-vdi-desktops-epg	non-prod	candid_dmz_laf01 candid_dmz_laf02	po2 po4	2003
172.16.72.68 10.18.0.26	non-prod-internal-vdi-bd	non-prod-vrf	internal-vdi-desktops-epg	non-prod	candid_dmz_laf03 candid_dmz_laf04	po2 po5	2003

At the bottom right, there is a "Rows" dropdown menu set to 10, with options for 25, 50, and 100.

9. ページを左にスクロールします (スクロールバーを右にドラッグします)。  
明らかに、[エンドポイントグループ (Endpoint Group) ] 内に重複する **IP** アドレスがあることが分かります。

Smart Events of CONNECTED\_EP\_DUPLICATE\_IP

Severity ▲ Major Event Category TENANT\_ENDPOINT Event Subcategory ENDPOINT\_IP\_ADDRESS  
Event Description IP addresses are in use by Multiple MAC addresses within the same VRF.

IPs	BDs	VRFs	EPGs	Tenants	Leafs	Interfaces	Encaps
10.18.0.26 172.16.72.67	non-prod-internal-vdi-bd	non-prod-vrf	internal-vdi-desktops-epg	non-prod	candid_dmz_lef01 candid_dmz_lef02	po2 po4	2003
172.16.72.68 10.18.0.26	non-prod-internal-vdi-bd	non-prod-vrf	uni/tn-non-prod/ap-internal-vdi-ap/epg-internal-vdi-desktops-epg internal-vdi-desktops-epg Cross Launch to APIC	non-prod	candid_dmz_lef03 candid_dmz_lef04	po2 po5	2003

Rows 10 25 50 100

10. [X] を使用して [スマートイベント (Smart Events) ] タブを閉じます。

11. [エンドポイントグループ (Endpoint Group) ] の上にマウスポインタを置くと、「ポップアップ」で完全な [ドメイン名 (Domain Name) ] が表示されます。

**注 : Network Assurance Engine がアクティブなシステムに接続されている場合、「ポップアップ」内の [APIC へのクロスローンチ (Cross Launch to APIC) ] リンクをクリックすると、[アプリケーションポリシーインフラストラクチャ コントローラ (Application Policy Infrastructure Controller) ] が起動します。**

The screenshot shows the Cisco Network Assurance Engine Explorer interface. The 'From EPG' field is populated with 'uni/tn-non-prod/ap-internal-vdi-ap/epg-internal-vdi-desktops-epg' and the 'To EPG' field is populated with 'uni/tn-non-prod/out-prod-l3out/instP-all-intranet-subnets'. A circular diagram below shows the relationship between these two EPGs, with arrows indicating connectivity. The 'From EPG' is represented by a blue arc and the 'To EPG' by a purple arc. Two horizontal arrows connect the two arcs, representing the network path between them.

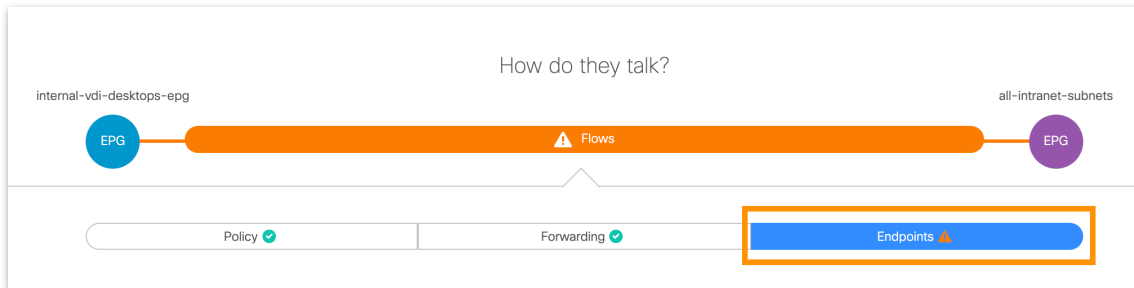
12. [エクスプローラ (Explorer) ] タブをクリックします。

13. [EPG から (From EPG) ] フィールドに **int** と入力し、(開いたドロップダウンから) **uni/tn-non-prod/ap-internal-vdi-ap/epg-internal-vdi-desktops-epg** オプションを選択します。

14. [EPG へ (To EPG) ] フィールドに *all* と入力し、（開いたドロップダウンから） **uni/tn-non-prod/out-non-prod-l3out/instP-all-intranet-subnets** オプションを選択します。

15. 上で強調表示された、[契約 (Contract) ] 行をクリックします。

16. [通信方法 (How To Talk) ] ボタンをクリックします。



17. [エンドポイント (Endpoints) ] ボタンをクリックします。

**価値：** 接続の問題を分析するために、エンドポイントの設定、転送ステート、およびセキュリティポリシーにわたって統一されたエンドポイントを可視化します。

18. ページを上スクロールして、[エンドポイントスマートイベント (Endpoint Smart Events) ] セクションを表示します。

Endpoints Smart Events (6)

Aggregated (3)     Individual

Severity ▼ 1	Event Subcategory	Event Name ▲ 2	Count	Event Description
Filter	Filter	Filter		
▲	ENDPOINT_IP_ADDRESS	<a href="#">CONNECTED_EP_DUPLICATE_IP</a>	2	IP addresses are in use by Multiple MAC addresses within the same VRF.
●	ENDPOINT_MOVE	<a href="#">CONNECTED_EP_IP_MOVED_ACROSS_LEAFS</a>	2	Possibility exists that an EP IP moved or duplicate IP addresses are found as a single IPv4 or IPv6 address may be associated with two or more MAC addresses in the VRF.
●	ENDPOINT_MOVE	<a href="#">CONNECTED_EP_MAC_MOVED_ACROSS_LEAFS</a>	2	The End Point MAC and IP address are detected on different leafs prompted by either an EP move or an IP move. IP and MAC entries exist on two leafs, as a bounce entry on one leaf, and a local learn (LST) entry on a different leaf.

19. **CONNECTED\_EP\_DUPLICATE\_IP** リンクをクリックします。

20. 最初の [イベント ID (Event Id) ] をクリックします。

Description	IP addresses are in use by Multiple MAC addresses within the same VRF.																																																																												
Impact	Multiple MACs sharing a single IP address will cause intermittent connectivity issues.																																																																												
Affected Objects Details	<table border="1"> <thead> <tr> <th>EP Type</th> <th>Mac Address</th> <th>IP Addresses</th> <th>BD</th> <th>BD's VRF</th> <th>EPGs</th> <th>EPG's Tenants</th> </tr> </thead> <tbody> <tr> <td>Connected_Internal</td> <td>00:50:56:9A:DC:82</td> <td>10.18.0.26</td> <td>non-prod-internal-<b>vdli-bd</b></td> <td>non-prod-vrf</td> <td>internal-<b>vdli</b>-desktops-<b>epg</b></td> <td>non-prod</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>TEP/VIP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> <tr> <th></th> <th></th> <th>Pod:Leaf</th> <th>Interface</th> <th>Encap VLAN/VxLAN Id</th> <th>VPC Peer Pod:Leaf</th> </tr> </thead> <tbody> <tr> <td>172.16.72.68</td> <td>Yes</td> <td>candid_dmz_leaf04</td> <td>po2</td> <td>2003</td> <td>candid_dmz_leaf03</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_leaf03</td> <td>po5</td> <td>2003</td> <td>candid_dmz_leaf04</td> </tr> </tbody> </table>					EP Type	Mac Address	IP Addresses	BD	BD's VRF	EPGs	EPG's Tenants	Connected_Internal	00:50:56:9A:DC:82	10.18.0.26	non-prod-internal- <b>vdli-bd</b>	non-prod-vrf	internal- <b>vdli</b> -desktops- <b>epg</b>	non-prod	TEP/VIP IP	is VPC	Leaf Details						Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer Pod:Leaf	172.16.72.68	Yes	candid_dmz_leaf04	po2	2003	candid_dmz_leaf03			candid_dmz_leaf03	po5	2003	candid_dmz_leaf04																																		
EP Type	Mac Address	IP Addresses	BD	BD's VRF	EPGs	EPG's Tenants																																																																							
Connected_Internal	00:50:56:9A:DC:82	10.18.0.26	non-prod-internal- <b>vdli-bd</b>	non-prod-vrf	internal- <b>vdli</b> -desktops- <b>epg</b>	non-prod																																																																							
TEP/VIP IP	is VPC	Leaf Details																																																																											
		Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer Pod:Leaf																																																																								
172.16.72.68	Yes	candid_dmz_leaf04	po2	2003	candid_dmz_leaf03																																																																								
		candid_dmz_leaf03	po5	2003	candid_dmz_leaf04																																																																								
Checks	<table border="1"> <thead> <tr> <th>Check Code</th> <th>Failing Condition</th> <th>Suggested Next Steps</th> </tr> </thead> <tbody> <tr> <td>4016</td> <td>The IPv4 or IPv6 address is associated with two or more MAC addresses.</td> <td> <ul style="list-style-type: none"> <li>Login into the APIC UI and verify the presence of the endpoints in the operational tab of the EPGs. <ul style="list-style-type: none"> <li>Tenant--Tenant Name--App Profiles--App Profile Name--App EPGs--EPG Name--Operational</li> </ul> </li> <li>Identify the EPs that actually own the IPs and change the IP address on the host/device that has the incorrect IP address.</li> <li>Clear the endpoint on the leaf by opening an SSH session to each leaf and by entering the following command: leaf1 clear system internal epm endpoint command</li> </ul> </td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Endpoint IP</th> <th>Endpoint MAC</th> <th>BD</th> <th>EPGs</th> <th>EPG's Tenants</th> <th>Owner Info</th> </tr> </thead> <tbody> <tr> <td>10.18.0.26</td> <td>00:50:56:9A:F0:36</td> <td>non-prod-internal-<b>vdli-bd</b></td> <td>internal-<b>vdli</b>-desktops-<b>epg</b></td> <td>non-prod</td> <td> <table border="1"> <thead> <tr> <th>TEP/VIP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> <tr> <th></th> <th></th> <th>Pod:Leaf</th> <th>Interface</th> <th>Encap VLAN/VxLAN Id</th> <th>VPC Peer</th> </tr> </thead> <tbody> <tr> <td>172.16.72.67</td> <td>Not Applicable</td> <td>candid_dmz_leaf01</td> <td>po2</td> <td>2003</td> <td>candid_dmz_leaf02</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_leaf0</td> <td>po4</td> <td>2003</td> <td>candid_dmz_leaf01</td> </tr> </tbody> </table> </td> </tr> <tr> <td>10.18.0.26</td> <td>00:50:56:9A:DC:82</td> <td>non-prod-internal-<b>vdli-bd</b></td> <td>internal-<b>vdli</b>-desktops-<b>epg</b></td> <td>non-prod</td> <td> <table border="1"> <thead> <tr> <th>TEP/VIP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> <tr> <th></th> <th></th> <th>Pod:Leaf</th> <th>Interface</th> <th>Encap VLAN/VxLAN Id</th> <th>VPC Peer</th> </tr> </thead> <tbody> <tr> <td>172.16.72.68</td> <td>Not Applicable</td> <td>candid_dmz_leaf04</td> <td>po2</td> <td>2003</td> <td>candid_dmz_leaf03</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_leaf0</td> <td>po5</td> <td>2003</td> <td>candid_dmz_leaf04</td> </tr> </tbody> </table> </td> </tr> </tbody> </table>					Check Code	Failing Condition	Suggested Next Steps	4016	The IPv4 or IPv6 address is associated with two or more MAC addresses.	<ul style="list-style-type: none"> <li>Login into the APIC UI and verify the presence of the endpoints in the operational tab of the EPGs. <ul style="list-style-type: none"> <li>Tenant--Tenant Name--App Profiles--App Profile Name--App EPGs--EPG Name--Operational</li> </ul> </li> <li>Identify the EPs that actually own the IPs and change the IP address on the host/device that has the incorrect IP address.</li> <li>Clear the endpoint on the leaf by opening an SSH session to each leaf and by entering the following command: leaf1 clear system internal epm endpoint command</li> </ul>	Endpoint IP	Endpoint MAC	BD	EPGs	EPG's Tenants	Owner Info	10.18.0.26	00:50:56:9A:F0:36	non-prod-internal- <b>vdli-bd</b>	internal- <b>vdli</b> -desktops- <b>epg</b>	non-prod	<table border="1"> <thead> <tr> <th>TEP/VIP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> <tr> <th></th> <th></th> <th>Pod:Leaf</th> <th>Interface</th> <th>Encap VLAN/VxLAN Id</th> <th>VPC Peer</th> </tr> </thead> <tbody> <tr> <td>172.16.72.67</td> <td>Not Applicable</td> <td>candid_dmz_leaf01</td> <td>po2</td> <td>2003</td> <td>candid_dmz_leaf02</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_leaf0</td> <td>po4</td> <td>2003</td> <td>candid_dmz_leaf01</td> </tr> </tbody> </table>	TEP/VIP IP	is VPC	Leaf Details						Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer	172.16.72.67	Not Applicable	candid_dmz_leaf01	po2	2003	candid_dmz_leaf02			candid_dmz_leaf0	po4	2003	candid_dmz_leaf01	10.18.0.26	00:50:56:9A:DC:82	non-prod-internal- <b>vdli-bd</b>	internal- <b>vdli</b> -desktops- <b>epg</b>	non-prod	<table border="1"> <thead> <tr> <th>TEP/VIP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> <tr> <th></th> <th></th> <th>Pod:Leaf</th> <th>Interface</th> <th>Encap VLAN/VxLAN Id</th> <th>VPC Peer</th> </tr> </thead> <tbody> <tr> <td>172.16.72.68</td> <td>Not Applicable</td> <td>candid_dmz_leaf04</td> <td>po2</td> <td>2003</td> <td>candid_dmz_leaf03</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_leaf0</td> <td>po5</td> <td>2003</td> <td>candid_dmz_leaf04</td> </tr> </tbody> </table>	TEP/VIP IP	is VPC	Leaf Details						Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer	172.16.72.68	Not Applicable	candid_dmz_leaf04	po2	2003	candid_dmz_leaf03			candid_dmz_leaf0	po5	2003	candid_dmz_leaf04
Check Code	Failing Condition	Suggested Next Steps																																																																											
4016	The IPv4 or IPv6 address is associated with two or more MAC addresses.	<ul style="list-style-type: none"> <li>Login into the APIC UI and verify the presence of the endpoints in the operational tab of the EPGs. <ul style="list-style-type: none"> <li>Tenant--Tenant Name--App Profiles--App Profile Name--App EPGs--EPG Name--Operational</li> </ul> </li> <li>Identify the EPs that actually own the IPs and change the IP address on the host/device that has the incorrect IP address.</li> <li>Clear the endpoint on the leaf by opening an SSH session to each leaf and by entering the following command: leaf1 clear system internal epm endpoint command</li> </ul>																																																																											
Endpoint IP	Endpoint MAC	BD	EPGs	EPG's Tenants	Owner Info																																																																								
10.18.0.26	00:50:56:9A:F0:36	non-prod-internal- <b>vdli-bd</b>	internal- <b>vdli</b> -desktops- <b>epg</b>	non-prod	<table border="1"> <thead> <tr> <th>TEP/VIP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> <tr> <th></th> <th></th> <th>Pod:Leaf</th> <th>Interface</th> <th>Encap VLAN/VxLAN Id</th> <th>VPC Peer</th> </tr> </thead> <tbody> <tr> <td>172.16.72.67</td> <td>Not Applicable</td> <td>candid_dmz_leaf01</td> <td>po2</td> <td>2003</td> <td>candid_dmz_leaf02</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_leaf0</td> <td>po4</td> <td>2003</td> <td>candid_dmz_leaf01</td> </tr> </tbody> </table>	TEP/VIP IP	is VPC	Leaf Details						Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer	172.16.72.67	Not Applicable	candid_dmz_leaf01	po2	2003	candid_dmz_leaf02			candid_dmz_leaf0	po4	2003	candid_dmz_leaf01																																																
TEP/VIP IP	is VPC	Leaf Details																																																																											
		Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer																																																																								
172.16.72.67	Not Applicable	candid_dmz_leaf01	po2	2003	candid_dmz_leaf02																																																																								
		candid_dmz_leaf0	po4	2003	candid_dmz_leaf01																																																																								
10.18.0.26	00:50:56:9A:DC:82	non-prod-internal- <b>vdli-bd</b>	internal- <b>vdli</b> -desktops- <b>epg</b>	non-prod	<table border="1"> <thead> <tr> <th>TEP/VIP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> <tr> <th></th> <th></th> <th>Pod:Leaf</th> <th>Interface</th> <th>Encap VLAN/VxLAN Id</th> <th>VPC Peer</th> </tr> </thead> <tbody> <tr> <td>172.16.72.68</td> <td>Not Applicable</td> <td>candid_dmz_leaf04</td> <td>po2</td> <td>2003</td> <td>candid_dmz_leaf03</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_leaf0</td> <td>po5</td> <td>2003</td> <td>candid_dmz_leaf04</td> </tr> </tbody> </table>	TEP/VIP IP	is VPC	Leaf Details						Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer	172.16.72.68	Not Applicable	candid_dmz_leaf04	po2	2003	candid_dmz_leaf03			candid_dmz_leaf0	po5	2003	candid_dmz_leaf04																																																
TEP/VIP IP	is VPC	Leaf Details																																																																											
		Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer																																																																								
172.16.72.68	Not Applicable	candid_dmz_leaf04	po2	2003	candid_dmz_leaf03																																																																								
		candid_dmz_leaf0	po5	2003	candid_dmz_leaf04																																																																								

[説明 (Description) ] 行に問題の原因が表示されます。

[チェック (Checks) ] 行には、問題を解決するうえで役立つ [推奨される次の手順 (Suggested Next Steps) ] が表示されます。

## シナリオ 2.2 : 到達不能な VDI インスタンス

**10.18.0.26** には到達不能な**仮想デスクトップインフラストラクチャ** インスタンスがあります。

詳細に調査するために、以下のことを実行します。

1. [変更管理 (Change Management) ] ドロップダウンから、[データセンター運用 (Data Center Operations) ] オプションを選択します。
2. [タイムライン (Timeline) ] で、最初の [エポック (Epoch) ] をクリックします。
3. 上で強調表示されている [検索 (Search) ] (虫眼鏡) ボタンをクリックします。
4. [検索 (Search) ] フィールドに *ip* と入力します。
5. ドロップダウンから、[IP] オプションを選択します。
6. [=] フィールドに *10.18.0.26* と入力します。
7. ドロップダウンから **10.18.0.26** オプションを選択します。

[スマートイベント (Smart Events) ] テーブルのエントリに、問題の原因が表示されます。

Severity	Event Category	Event Subcategory	Event Name ^	Count	Event Description
▲	TENANT_ENDPOINT	ENDPOINT_IP_ADDRE...	CONNECTED_EP_DUPLICATE_IP	2	IP addresses are in use by Multiple MAC addresses within the same VRF.
●	TENANT_ENDPOINT	ENDPOINT_MOVE	CONNECTED_EP_IP_MOVED_ACROSS_LEAFS	2	Possibility exists that an EP IP moved or duplicate IP addresses are found as a single IPv4 or IPv6 address may be associated with two or more MAC addresses in the VRF.
●	TENANT_ENDPOINT	ENDPOINT_MOVE	CONNECTED_EP_MAC_MOVED_ACROSS_LEAFS	2	The End Point MAC and IP address are detected on different leafs prompted by either an EP move or an IP move. IP and MAC entries exist on two leafs, as a bounce entry on one leaf, and a local learn (LST) entry on a different leaf.

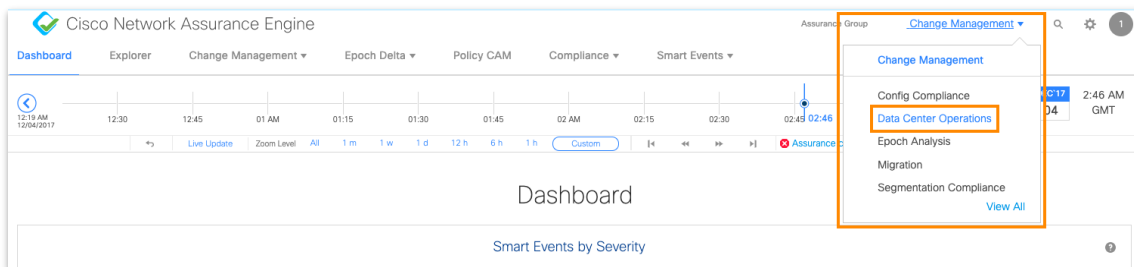
Smart Events of **CONNECTED\_EP\_DUPLICATE\_IP**

Severity ▲ Major Event Category TENANT\_ENDPOINT Event Subcategory ENDPOINT\_IP\_ADDRESS  
Event Description IP addresses are in use by Multiple MAC addresses within the same VRF.

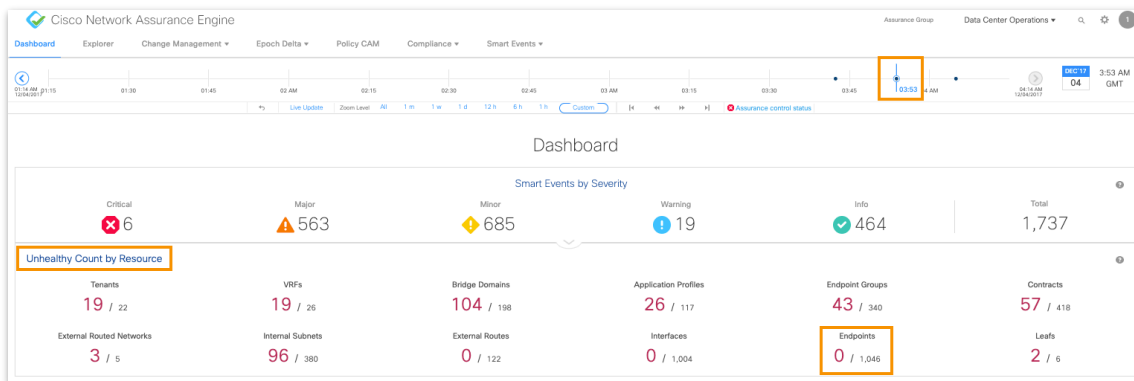
MACs	IPs	Bds	VRFs	EPGs	Tenants	Leafs	Interfaces	Encaps
00:50:56:9A:F0:36	10.18.0.26 172.16.72.67	non-prod-internal-vdi...	non-prod-vrf	internal-vdi-desktops...	non-prod	candid_dmz_leaf01 candid_dmz_leaf02	po2 po4	2003
00:50:56:9A:DC:82	172.16.72.68 10.18.0.26	non-prod-internal-vdi...	non-prod-vrf	internal-vdi-desktops...	non-prod	candid_dmz_leaf03 candid_dmz_leaf04	po2 po5	2003

**価値** : CISCO NAE は、ファブリック内のすべてのエンドポイントを分析し、静的および動的な不整合を検出します。

### シナリオ 2.3 : 到達不能な VDI インスタンスの解決を確認する



1. 上で強調表示するように、[変更管理 (Change Management)] ドロップダウンから、[データセンター運用 (Data Center Operations)] オプションを選択します。

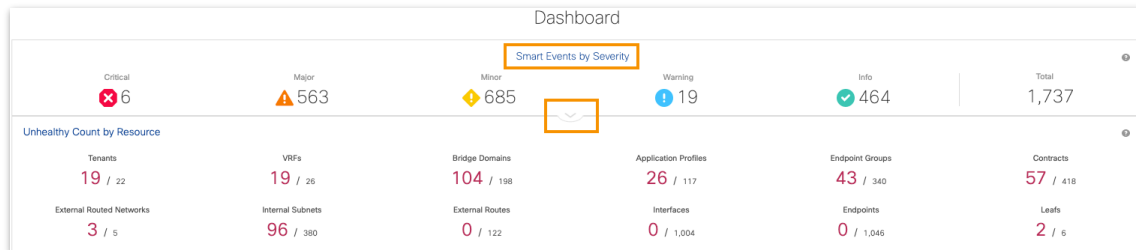


2. [タイムライン (Timeline)] で 2 番目の [エポック (Epoch)] をクリックします。

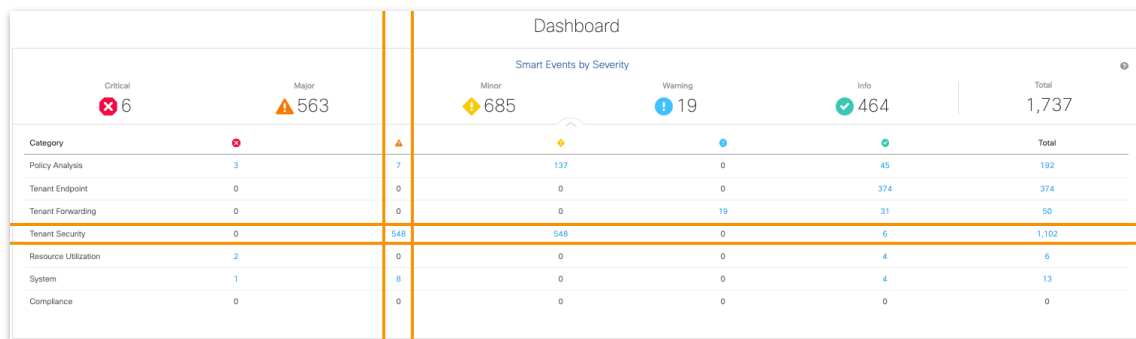
3. [リソース別の異常な数 (Unhealthy Count by Resource)] パネル (上で強調表示) で、[エンドポイント (Endpoints)] 数 (上で強調表示) が **0** であることを確認します。

### シナリオ 2.4 : 到達不能な VDI インスタンスのレポートの調査

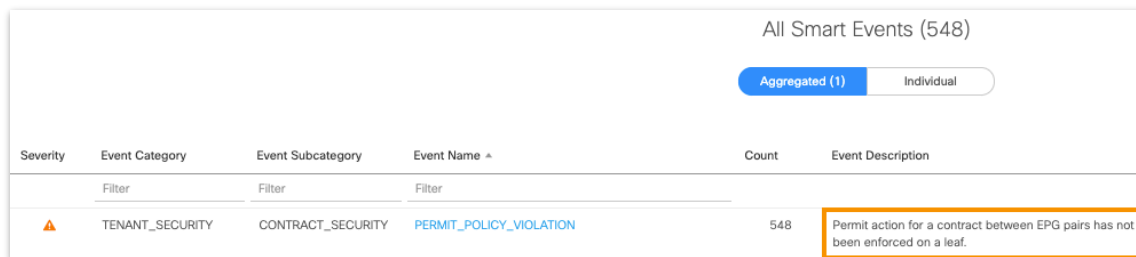
ネットワーク オペレーション センターは、仮想デスクトップ インフラストラクチャ インスタンスに到達できない複数のユーザについて、いくつかのコールを受信しました。Network Assurance Engine の一部のツールを使用することで、重点を置いている問題は non-prod テナントの VDI デスクトップ EPG にあることが分かります。



1. [重大度別のスマートイベント (Smart Events by Severity)] パネルで、[ビューの拡張 (Expand View)] ボタンをクリックします。



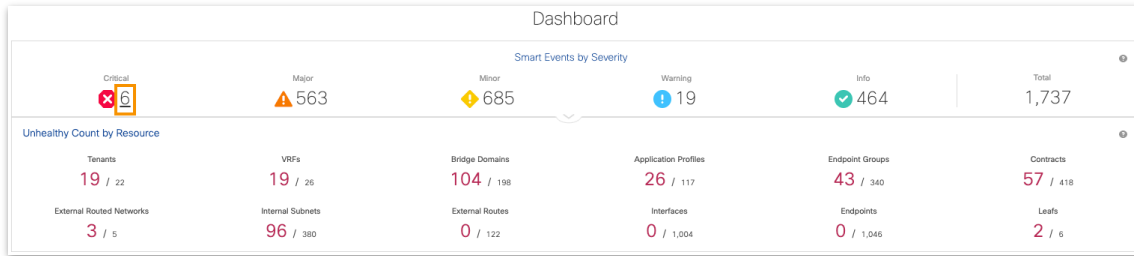
2. [テナントのセキュリティ (Tenant Security)] 行と [主なイベント (Major Event)] 列の交点にあるリンクをクリックします。



[イベントの説明 (Event Description)] の報告内容により、「許可アクション」がリーフに適用されていないことが分かります。

3. [ダッシュボード (Dashboard)] タブをクリックします。





4. [重要なイベント (Critical Events)] 数を表すリンク (上で強調表示) をクリックします。

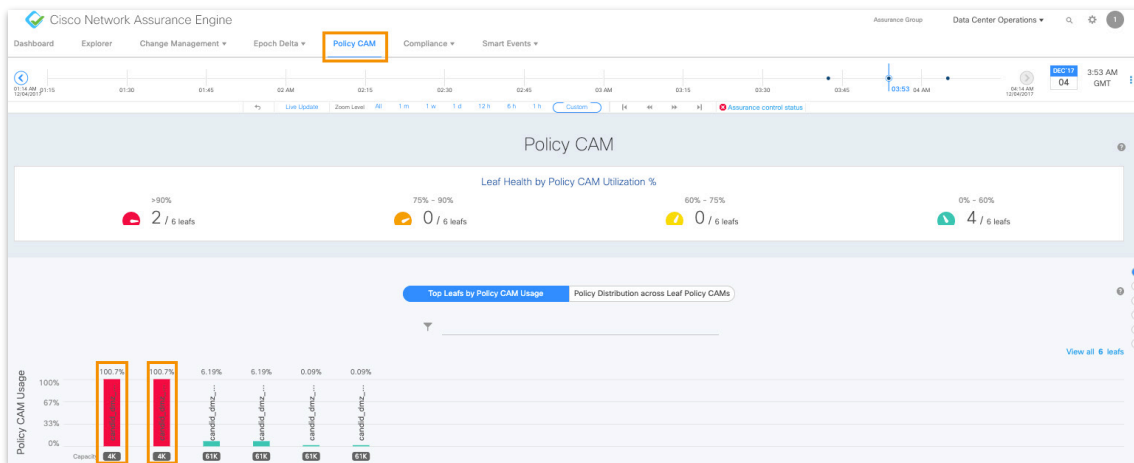
All Smart Events (6)

Aggregated (3) Individual

Severity	Event Category	Event Subcategory	Event Name	Count	Event Description
Filter	Filter	Filter	Filter		
Critical	SYSTEM	ASSURANCE_CONTROL	COLLECTION_FAILED_ON_APIC	1	NAE appliance is experiencing problem while querying the APIC for data.
Critical	CHANGE_ANALYSIS	FORWARDING_POLICY	OVERLAPPING_EXT_SUBNETS_ACROSS_L3OUT_INSTPS_IN_VRF	3	Overlapping ext subnets have been configured under L3Out EPGs belonging to the same VRF.
Critical	RESOURCE_UTILIZATION	POLICY_CAM_UTILIZATION	POLICY_CAM_UTIL_CRITICAL	2	Policy CAM is over 90% utilized on the leaf.

[イベントカテゴリ (Event Category)] : **RESOURCE\_UTILIZATION** では、[イベント名 (Event Name)] が **POLICY\_CAM\_UTIL\_CRITICAL** で、[ポリシーCAM (Policy CAM)] が「over 90% utilized on the leaf」であることに注意してください。

5. [ポリシーCAM (Policy CAM)] タブ (下で強調表示) をクリックします。 **candid\_dmz\_lef01** の TCAM 使用率を確認します。

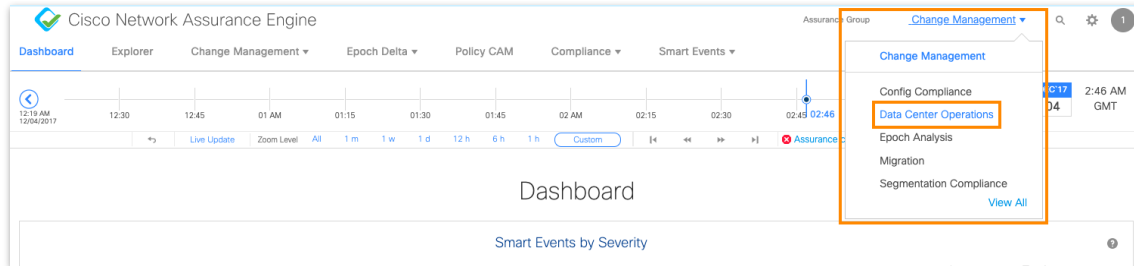


**candid\_dmz\_lef01** と **candid\_dmz\_lef02** のポリシー CAM 使用率は 100% を超えていることに注意してください。

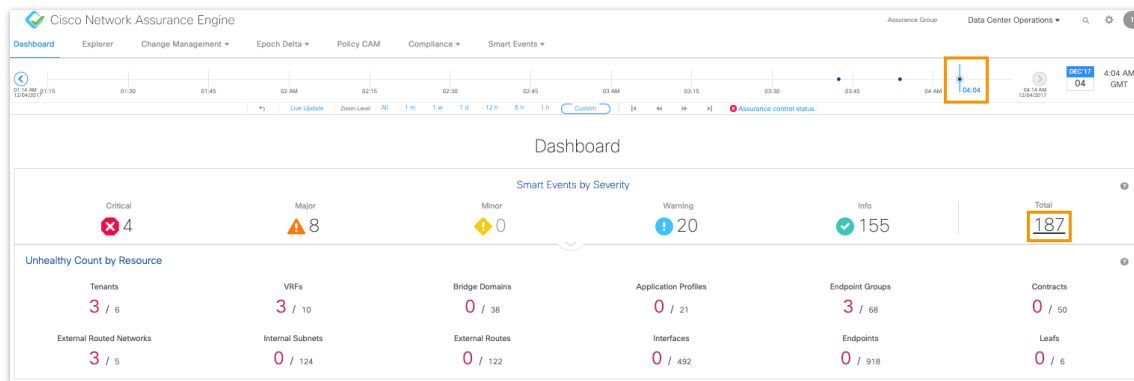
エンドポイントがリーフ X からリーフ Y に移動する際、TCAM 使用率が高いため、すべてのポリシーが正しく記述されませんでした。実際のデータプレーンの状態は、VM の移動が原因で、設定された APIC ポリシーと矛盾していました。Cisco NAE は、接続の兆候、セキュリティポリシーの整合性違反、および TCAM の使用率が上限に達する根本原因を検出できました。

## シナリオ 2.5 : 到達不能の最近展開された VDI インスタンスの調査

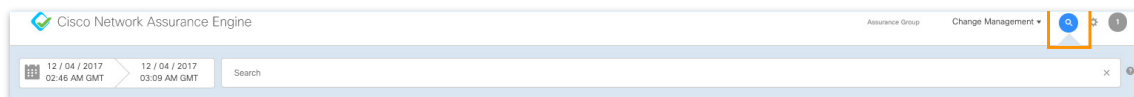
ネットワーク オペレーション センターは、最近展開され、到達不能の仮想デスクトップ インフラストラクチャ インスタンスのコールを受信しました。IP アドレスは 10.71.0.26 です。



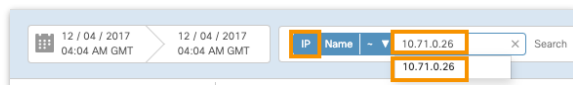
1. 上で強調表示するように、[変更管理 (Change Management) ] ドロップダウンから、[データセンター運用 (Data Center Operations) ] オプションを選択します。



2. [タイムライン (Timeline) ] で 3 番目の [エポック (Epoch) ] をクリックします。
3. [スマートイベント (Smart Events) ] の [合計 (Total) ] 数を表すリンク (上で強調表示) をクリックします。



4. 上で強調表示されている [検索 (Search) ] (虫眼鏡) ボタンをクリックします。



5. [検索 (Search) ] フィールドに *ip* と入力します。
6. ドロップダウンから、[IP] オプションを選択します。
7. [=] フィールドに 10.71.0.26 と入力します。
8. ドロップダウンから 10.71.0.26 オプションを選択します。

All Smart Events (1)

Aggregated (1)    Individual

Severity	Event Category	Event Subcategory	Event Name	Count	Event Description
<span style="color: blue;">●</span>	TENANT_ENDPOINT	ENDPOINT_IP_ADDRESS	<a href="#">CONNECTED_EP_IP_NOT_IN_BD_SUBNET_OR_BD_HAS_NO_SUBNET</a>	1	ACI Fabric is learning EPs in a BD with an IP address that does not fall under one of the subnets configured under the BD or EPG.

**価値 :** VM 管理者が VDI インスタンスを誤ったポートグループに配置したことによる従来型のエラー。Cisco NAE は、VM IP 設定と ACI で予測される設定の不一致による問題を即座に把握します。

9. **CONNECTED\_EP\_IP\_NOT\_IN\_BD\_SUBNET\_OR\_BD\_HAS\_NO\_SUBNET** リンクをクリックします。

Smart Events of [CONNECTED\\_EP\\_IP\\_NOT\\_IN\\_BD\\_SUBNET\\_OR\\_BD\\_HAS\\_NO\\_SUBNET](#)

Severity ● Warning    Event Category TENANT\_ENDPOINT    Event Subcategory ENDPOINT\_IP\_ADDRESS

Event Description ACI Fabric is learning EPs in a BD with an IP address that does not fall under one of the subnets configured under the BD or EPG.

Epochs	Event Id	MACs	IPs	BDs	VRFs	EPGs	Tenants
<a href="#">12/04/2017 04:04 AM GMT</a>	52198fc7b6776bf4bfe1557c9401d9d	00:50:56:9A:6F:BC	172.16.72.68 10.71.0.26	non-prod-internal-vdi-...	non-prod-vrf	internal-vdi-desktops-...	non-prod

10. 上に強調表示されている [エポック (Epoch) ] をクリックします。

Smart Events of [CONNECTED\\_EP\\_IP\\_NOT\\_IN\\_BD\\_SUBNET\\_OR\\_BD\\_HAS\\_NO\\_SUBNET](#)

Severity ● Warning    Event Category TENANT\_ENDPOINT    Event Subcategory ENDPOINT\_IP\_ADDRESS

Event Description ACI Fabric is learning EPs in a BD with an IP address that does not fall under one of the subnets configured under the BD or EPG.

1 rows | ☰ | ⚙

Epochs	Event Id	MACs	IPs	BDs	VRFs	EPGs
<a href="#">12/04/2017 04:04 AM GMT</a>	52198fc7b6776bf4bfe1557c9401d9d	00:50:56:9A:6F:BC	172.16.72.68 10.71.0.26	non-prod-internal-vdi-...	non-prod-vrf	internal-vdi-desktops

Total Duration (1 Epochs)

First Raised: 12/04/2017 04:04:57 AM    Last Raised: 12/04/2017 04:04:57 AM    Clearing: [⏸]    Cleared: [⏹]

Zoom Level: Lifecycle    12 h    6 h    3 h    1 h    |<    <<    >>    >

< Previous Occurrence    12/04/2017 04:04 AM GMT    Next Occurrence >

Description	ACI Fabric is learning EPs in a BD with an IP address that does not fall under one of the subnets configured under the BD or EPG.																																						
Impact	Endpoint may not be able to communicate outside the layer 2 domain.																																						
Affected Objects Details	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>EP Type</th> <th>Mac Address</th> <th>IP Addresses</th> <th>BD</th> <th>BD's VRF</th> <th>EPGs</th> <th>EPG's Tenants</th> </tr> </thead> <tbody> <tr> <td>Connected_Internal</td> <td>00:50:56:9A:6F:BC</td> <td>10.71.0.26</td> <td>non-prod-internal-vdi-bd</td> <td>non-prod-vrf</td> <td>internal-vdi-desktops-epg</td> <td>non-prod</td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>TEP/IP IP</th> <th>is VPC</th> <th colspan="4">Leaf Details</th> </tr> </thead> <tbody> <tr> <td>172.16.72.68</td> <td>Yes</td> <td>Pod:Leaf</td> <td>Interface</td> <td>Encap VLAN/VxLAN Id</td> <td>VPC Peer Pod:Leaf</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_lef04</td> <td>po2</td> <td>2003</td> <td>candid_dmz_lef03</td> </tr> <tr> <td></td> <td></td> <td>candid_dmz_lef03</td> <td>po5</td> <td>2003</td> <td>candid_dmz_lef04</td> </tr> </tbody> </table>	EP Type	Mac Address	IP Addresses	BD	BD's VRF	EPGs	EPG's Tenants	Connected_Internal	00:50:56:9A:6F:BC	10.71.0.26	non-prod-internal-vdi-bd	non-prod-vrf	internal-vdi-desktops-epg	non-prod	TEP/IP IP	is VPC	Leaf Details				172.16.72.68	Yes	Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer Pod:Leaf			candid_dmz_lef04	po2	2003	candid_dmz_lef03			candid_dmz_lef03	po5	2003	candid_dmz_lef04
EP Type	Mac Address	IP Addresses	BD	BD's VRF	EPGs	EPG's Tenants																																	
Connected_Internal	00:50:56:9A:6F:BC	10.71.0.26	non-prod-internal-vdi-bd	non-prod-vrf	internal-vdi-desktops-epg	non-prod																																	
TEP/IP IP	is VPC	Leaf Details																																					
172.16.72.68	Yes	Pod:Leaf	Interface	Encap VLAN/VxLAN Id	VPC Peer Pod:Leaf																																		
		candid_dmz_lef04	po2	2003	candid_dmz_lef03																																		
		candid_dmz_lef03	po5	2003	candid_dmz_lef04																																		

上記のイベントでは、サブネットアドレス **10.18.0.1/24** の BD 内の TEP IP 172.16.72.68 に接続された EPG **internal-vdi-desktops-epg** 内に IP **10.71.0.26/MAC 00:50:56:9A:6F:BC** があります。ブリッジドメインのサブネットアドレスは、エンドポイント IP サブネットのネットワークの外部にあります。

## シナリオ 3. 移行

ACI 環境に移行する場合、お客様は、テナント/VRF/BD/EPG に関連するすべての必要な設定を事前にプロビジョニングし、サーバポートのレイヤ 1/レイヤ 2 接続に必要で適切なポリシーをプログラムします。Cisco APIC では、次のすべてを設定する必要があります。

- インターフェイスポリシー、インターフェイスポリシー-グループ、インターフェイスプロファイル、リーフプロファイル、AAEP、VLAN プール、物理/仮想ドメインなど
- テナント/VRF/ブリッジドメイン/アプリケーションプロファイル/EPG/静的パスバインディングなど

次のステップでは、レイヤ 2 接続を古いインフラストラクチャから新しい ACI 環境に拡張し、ワークロードの ACI ファブリックへの移行を開始します。その後、カットオーバー中、複数の VLAN のデフォルトゲートウェイがレガシーインフラストラクチャから ACI に移行されます。

ACI がデフォルトゲートウェイ機能を引き継ぐようになると、たとえば DHCP リレー、契約、サブネット間ルーティングなど、いくつかの ACI 設定が有効になります。契約の正確な設定は、ファブリック内の EPG 間の接続と、ファブリック外のエンティティへの接続を提供する鍵となります。

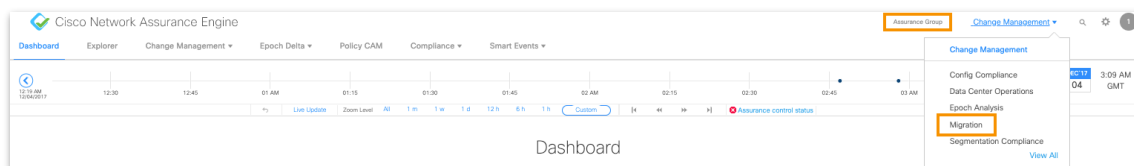
場合によっては、変更アドバイザリボードによるレビューを複数回行った後でも、人的ミスにより、移行の遅延、延期、撤回が発生します。Cisco NAE Network Assurance プラットフォームを使用することで、オペレータは、ACI ファブリック内の設定の問題も、ファブリック外の設定ミスの可能性も迅速かつ正確に特定できます。これにより、移行の実行にかかる時間を短縮でき、予想通りに動作しない場合に、複数の変更ウィンドウに関連するコストを削減できます。

### シナリオ 3.1 -

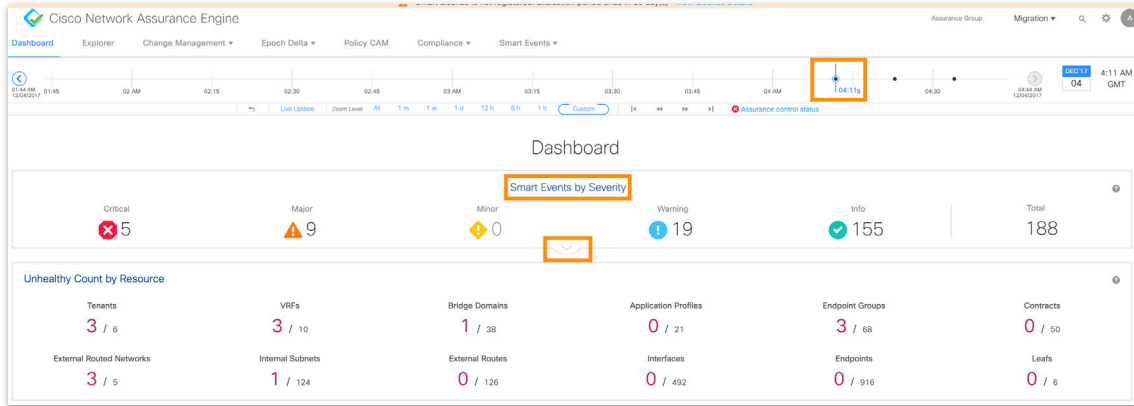
ワークロードを実稼働テナントに移行する前に、データセンターチームは、**non-prod** VRF でネットワーク接続テストを実行し、ACI ファブリックと外部ネットワーク間のルーティングとスイッチングがエンドツーエンドで動作していることを確認します。接続が機能していることを運用チームが確認したら、エンドツーエンドのワークロードが **non-prod** から **prod** テナントに移行されます。

DC オペレータは、**ブリッジドメイン (non-prod-internal-vdi-bd)** (10.18.0.0/24 サブネット) 内のリモートデスクトップアプリケーションを使用してテスト VM にログインしようとしていますが、接続は失敗します。

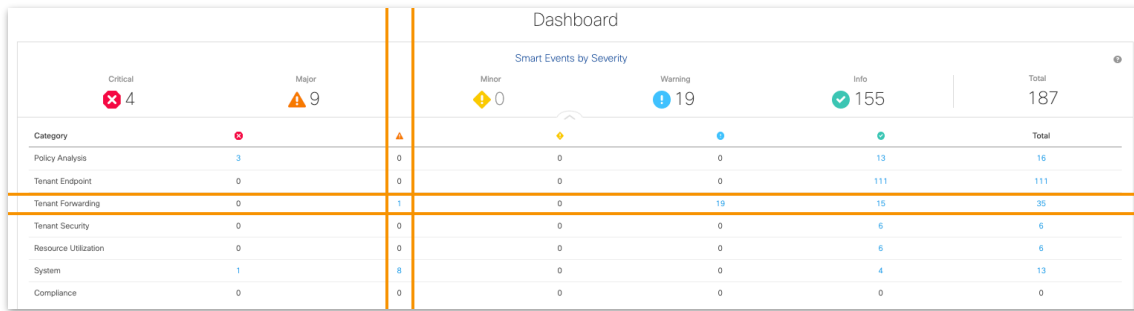
この接続障害の原因と、この問題の解決策は何でしょうか。



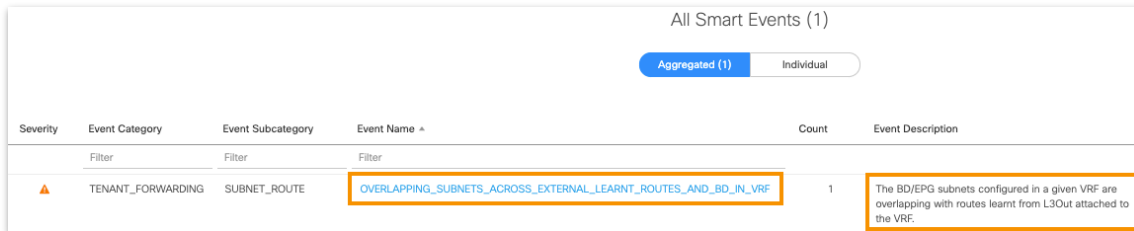
1. [アシュアランスグループ (Assurance Group)] ドロップダウンから、[移行 (Migrations)] オプションを選択します。
2. [タイムライン (Timeline)] で、最初の [エポック (Epoch)] をクリックします。



3. [重大度別のスマートイベント (Smart Events by Severity)] パネルで、[ビューの拡張 (Expand View)] ボタンをクリックします。



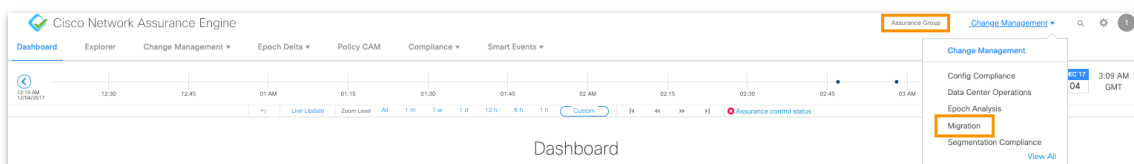
4. [テナントの転送 (Tenant Forwarding)] 行と [主なイベント (Major Event)] 列の交点にあるリンクをクリックします。



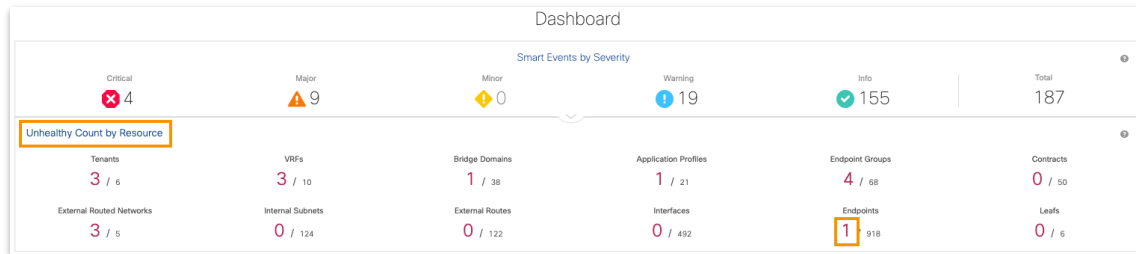
**Network Assurance Engine** は、ACI 内のサブネットが外部サブネットと重複していることを検出しました。

### シナリオ 3.2 -

**ブリッジドメイン (non-prod-internal-vdi-bd)** には、自身のネットワーク内または外部のデバイスと通信できないという不満を抱えたエンドポイントがあります。このエンドポイントへの接続が修正されない限り、このエンドポイントを **non-prod** から **prod** に移行することはできません。



1. [アシュアランスグループ (Assurance Group) ] ドロップダウンから、[移行 (Migrations) ] オプションを選択します。
2. [タイムライン (Timeline) ] で、2 番目の [エポック (Epoch) ] をクリックします。



3. [リソース別の異常な数 (Unhealthy Count by Resource) ] パネル (上で強調表示) で、[エンドポイント (Endpoints) ] の数を表すリンクをクリックします。

The screenshot shows the 'All Smart Events (1)' table. The table has columns for Severity, Event Category, Event Subcategory, Event Name, Count, and Event Description. A single event is listed with the following details:

Severity	Event Category	Event Subcategory	Event Name	Count	Event Description
Warning	TENANT_ENDPOINT	ENDPOINT_IP_ADDRESS	CONNECTED_EP_WITH_IPV4LL_MAY_HAVE_NO_DHCP_OFFER	1	The IP addresses being used by this Endpoint are self-assigned and belong to RFC 3927 IPv4 Link Local range. This usually occurs on DHCP failure.

エンドポイントは、DHCP から IP アドレスの割り当てを受信していません。

**価値 :** Cisco NAE は、このエンドポイントが DHCP サーバから IP アドレスを受信できないことを識別しました。これは、リンクのローカル IPv4 アドレスで実行されています。そのため、他のデバイスと通信できません。

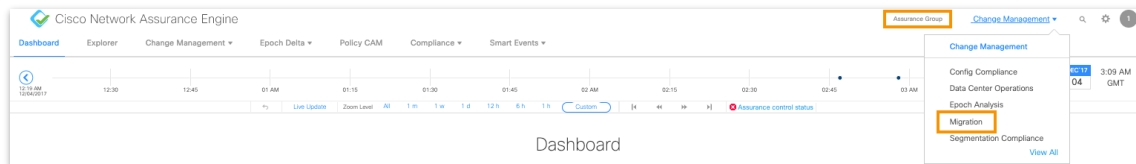
### シナリオ 3.3 - Hadoop 接続の障害

DC Ops チームは、自社の Hadoop クラスタを non-prod から prod テナントに移行する過程にあります。しかし、移行を実行する前に、Hadoop HDFS エンドポイントに到達できるよう、ネットワークとポリシーの設定が適切に行われているかどうかを確認することが重要です。

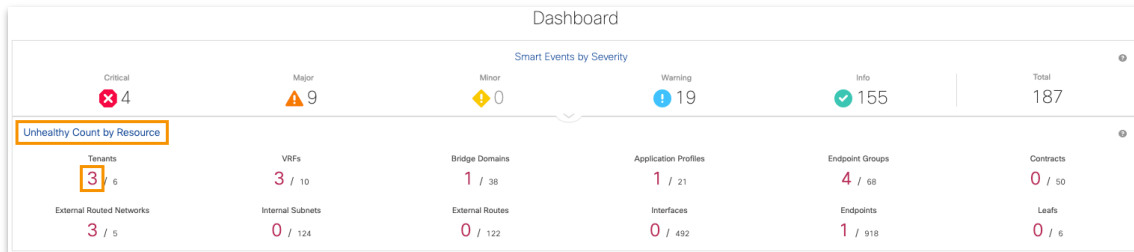
最初のテストでは、ACI ファブリック内のワークロードが Hadoop の HDFS エンドポイントに到達できるかどうかを確認しました。ファブリック内のアプリケーションは、Hadoop の HDFS エンドポイントに到達できませんでした。

2 番目のテストでは、WAN ブランチサイト内にある ACI ファブリック外のアプリケーションサーバがデータセンターの Hadoop HDFS ワークロードにアクセスできるかどうかを確認しました。2 番目の接続テストも失敗しました。

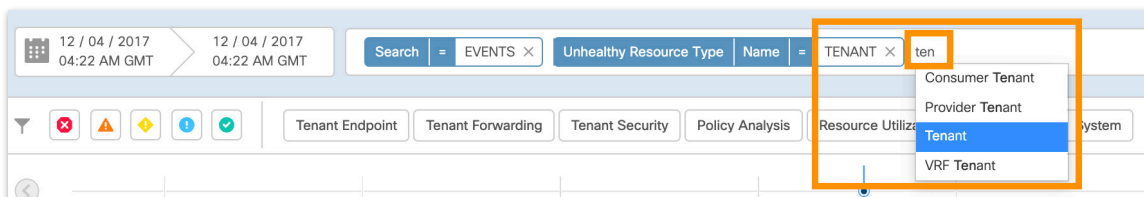
チームは両方の問題をただちに解決する必要があります。



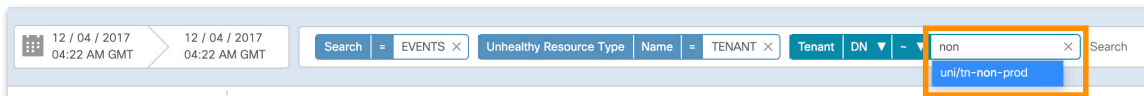
1. [アシュアランスグループ (Assurance Group) ] ドロップダウンから、[移行 (Migrations) ] オプションを選択します。
2. [タイムライン (Timeline) ] で、2 番目の [エポック (Epoch) ] をクリックします。



3. [リソース別の異常な数 (Unhealthy Count by Resource) ] パネル (上で強調表示) で、[テナント (Tenants) ] の数を表すリンクをクリックします。



4. [検索 (Search) ] フィールドに *ten* と入力します。
5. ドロップダウンから、[テナント (Tenant) ] オプションを選択します。



6. [=] フィールドに *non* と入力します。
7. ドロップダウンから、**uni/tn-non-prod** オプションを選択します。

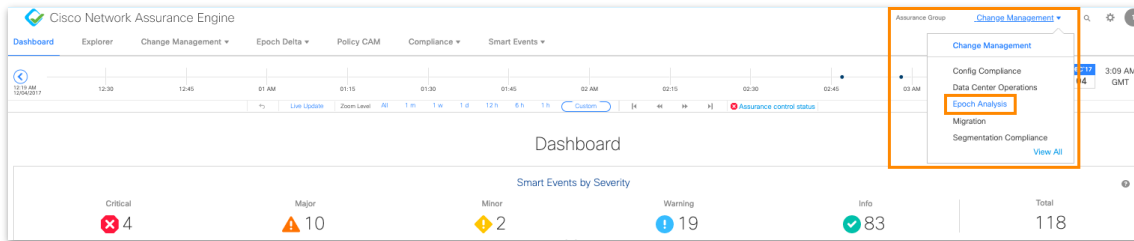
Severity	Event Category	Event Subcategory	Event Name	Count	Event Description
Critical	CHANGE_ANALYSIS	FORWARDING_POLICY	OVERLAPPING_EXT_SUBNETS_ACROSS_L3OUT_INS...	1	Overlapping ext subnets have been configured under L3Out EPGs belonging to the same VRF.
Major	TENANT_ENDPOINT	ENDPOINT_IP_ADDRE...	CONNECTED_EP_WITH_IPV4LL_MAY_HAVE_NO_DHC...	1	The IP addresses being used by this Endpoint are self-assigned and belong to RFC 3927 IPv4 Link Local range. This usually occurs on DHCP failure.

重複するサブネットが ACI ファブリックの内と外にあることに注意してください。

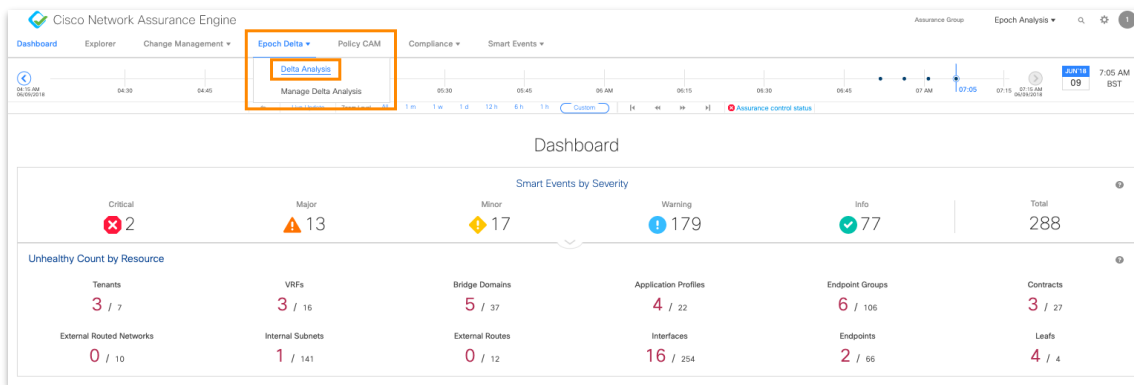
## シナリオ 4. エポックデルタ分析

Cisco NAE では、2つのエポック間の変更内容をさらにドリルダウンする機能をサポートしています。これは「エポックデルタ分析」と呼ばれています。2つのエポック間のデルタ分析には、ヘルスデルタおよびポリシーデルタの2種類があります。ヘルスデルタ分析は、2つのエポック間のネットワーク運用状態の違いを比較して表示します。ポリシーデルタ分析は、2つのエポック間のネットワーク設定の違いを比較して表示します。

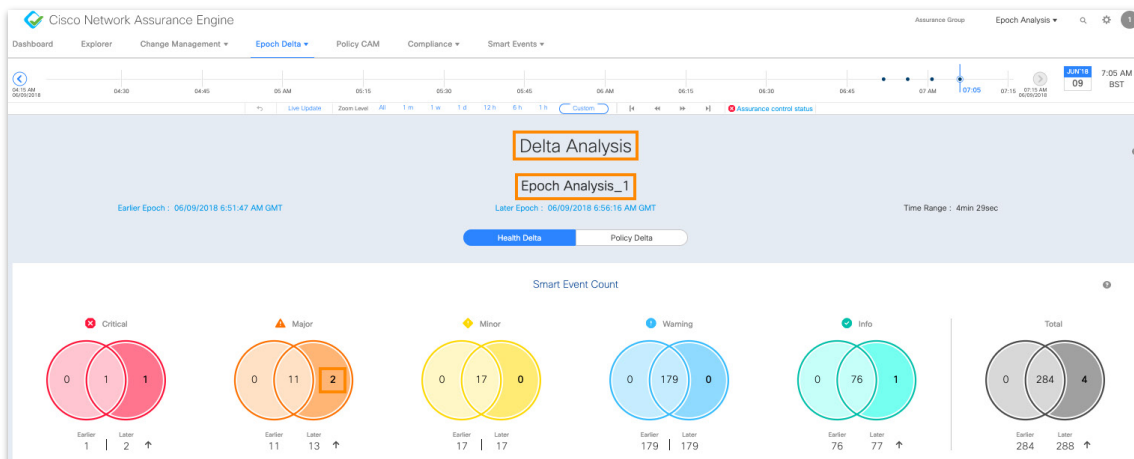
### シナリオ 4.1



1. [アシュアランスグループ (Assurance Group)] ドロップダウンから、[エポック分析 (Epoch Analysis)] オプションを選択します。



2. [エポックデルタ (Epoch Delta)] ドロップダウンから、[デルタ分析 (delta Analysis)] オプションを選択します。





Epoch Analysis\_1 という名前の完了後の分析が表示されます。

[スマートイベントカウント (Smart Event Count) ] の下の図は、両方のエポックで共通のスマートイベントと、各エポック固有のスマートイベントを表します (左側 = 以前、右側 = 後)。

後のエポックに、以前のエポックにはなかった 2 つの**主なイベント**があることに注意してください。

3. 後のエポックの**主なイベント**を示す **2** をクリックします。

Severity	Event Category	Event Subcategory	Event Name	Epoch	Count
▲	TENANT_ENDPOINT	ENDPOINT_IP_ADDRESS	CONNECTED_EP_DUPLICATE_IP	☐	2

[イベント名 (Event Name) ] と [カウント (Count) ] は、同じ IP アドレスを持つエンドポイントが 2 つあることを示しています。

4. ページを下にスクロールして、[リソース別ヘルスデルタ (Health Delta by Resource) ] パネルを表示します。

Resources	Total Earlier   Later	Unhealthy Earlier   Later	Total Unhealthy In Earlier Epoch Only	Total Unhealthy In Later Epoch Only	Total Unhealthy In Both Epochs	No Issues Earlier   Later
Tenants	7   7 -	2   3 ↑	0	1	2	5   4 ↓
App Profiles	22   22 -	3   4 ↑	0	1	3	19   18 ↓
EPGs	106   106 -	5   6 ↑	0	1	5	101   100 ↓
BDs	37   37 -	4   5 ↑	0	1	4	33   32 ↓
VRFs	16   16 -	2   3 ↑	0	1	2	14   13 ↓
Contracts	27   27 -	3   3 -	0	0	3	24   24 -
L3Outs	10   10 -	0   0 -	0	0	0	10   10 -
Internal Subnets	141   141 -	1   1 -	0	0	1	140   140 -
External Routes	12   12 -	0   0 -	0	0	0	12   12 -
Endpoints	65   66 ↑	0   2 ↑	0	2	0	65   64 ↓
Leafs	4   4 -	4   4 -	0	0	4	0   0 -
Interfaces	251   254 ↑	16   16 -	0	0	16	235   238 ↑

上向き矢印は 2 つのエポック間の増加を示し、下向き矢印は減少を示します。

[エンドポイント (Endpoint) ] 行と [合計 (Total) ] 列の交点の数が増加していることに注意してください。

5. ページを下にスクロールすると、ページの上部が表示されます。

Delta Analysis

Epoch Analysis\_1

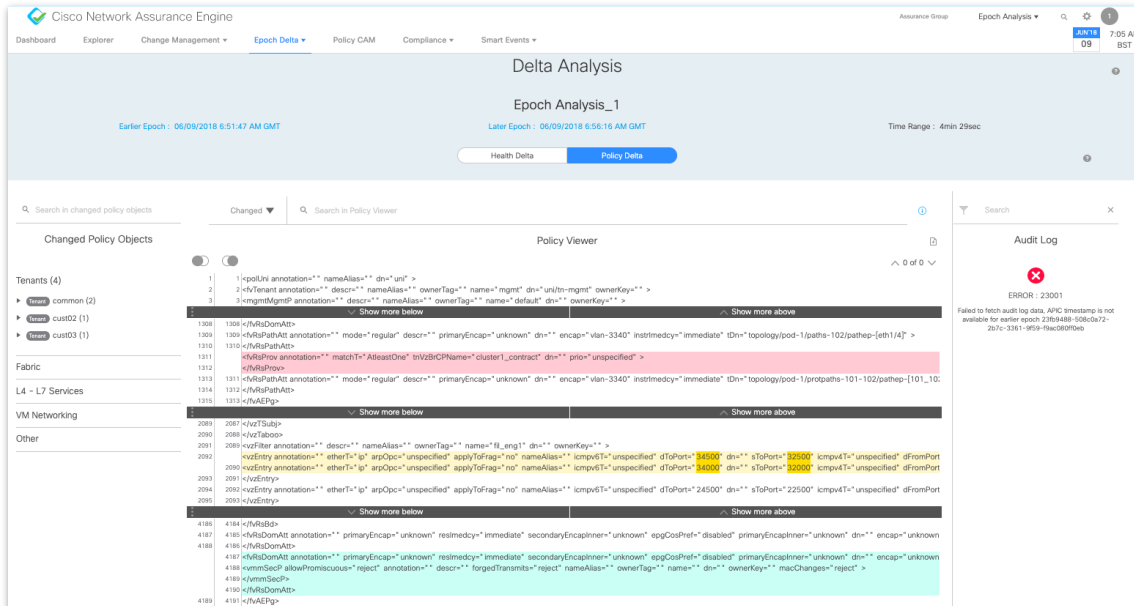
Earlier Epoch : 06/09/2018 6:51:47 AM GMT

Later Epoch : 06/09/2018 6:56:16 AM GMT

Time Range : 4min 29sec

Health Delta | **Policy Delta**

6. [ポリシーデルタ (Policy Delta) ] ボタンをクリックします。



[ポリシービューア (Policy Viewer) ]には、エポック間のポリシーの変更が表示されます。

デフォルトでは、変更箇所とその上下 3 行が表示されます。

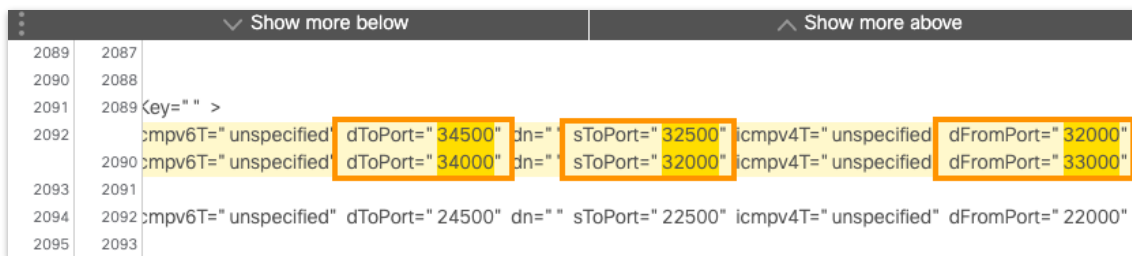
[さらに上を表示 (Show more above) ] ボタンをクリックして、さらに上を表示することも、[さらに下を表示 (Show more below) ] ボタンをクリックして、さらに下を表示することもできます。

変更は色分けされています。

- 赤色の強調表示：削除箇所を示します。
- 黄色の強調表示：変更箇所を示します。
- 青色の強調表示：追加箇所を示します。

7. (キーボードの矢印キーを使用して) [ポリシービューア (Policy Viewer) ] ウィンドウを左にスクロールして、3 つの変更をすべて表示します。

1 つの変更を拡大します。



上の行は「以前」を示し、下の行は「現在」を示します。

## シナリオ 5. コンプライアンス分析

コンプライアンス分析機能により、通信セグメンテーションと設定コンプライアンスルールを確認できます。

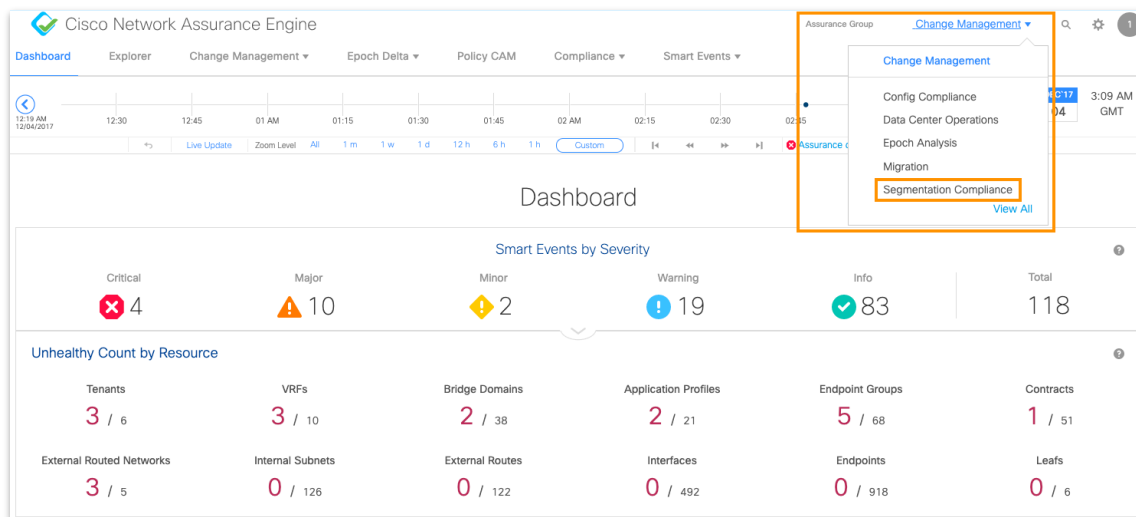
たとえば、2つの EPG が相互に通信できるかできないかを確認したり、特定の VRF が適用モードで設定されていることを確認したりできます。

### シナリオ 5.1

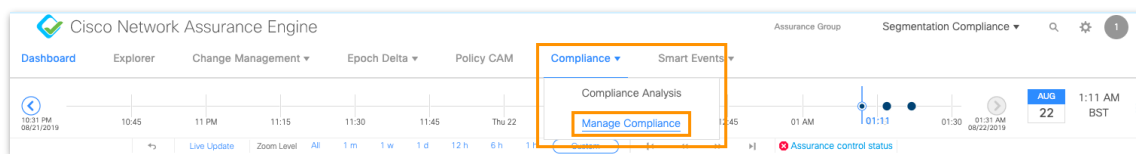
給与データベースへのセキュアなアクセスには、アプリケーションのフロントエンド層から直接アクセスできないという、通信セグメンテーションの要件があります。ACI ファブリックは、この通信関係を管理するために適切な契約を使用して設定されます。ネットワークチームは、Cisco NAE を使用して、ネットワーク内のこの要件に対するコンプライアンスを継続的に確認することを決めました。

まず、コンプライアンス要件について NAE に指定する必要があります。コンプライアンス要件を把握するため、NAE では次のエンティティとアーキテクチャが使用されます。

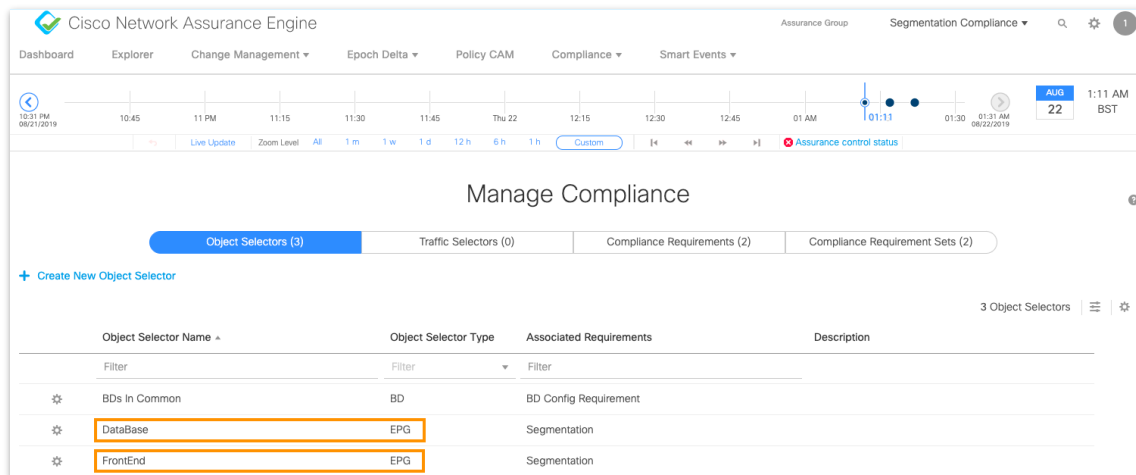
- EGP セレクタ：ルールに関連する EPG を選択します。
- コンプライアンスルール：2つの EPG セレクタ間の通信ルールを指定します。
- コンプライアンスルールセット：一連の規則をまとめてグループ化し、アシュアランスグループに関連付けます。



1. [アシュアランスグループ (Assurance Group)] ドロップダウンから、[セグメンテーションコンプライアンス (Segmentation Compliance)] オプションを選択します。
2. [タイムライン (Timeline)] で、最初の [エポック (Epoch)] をクリックします。

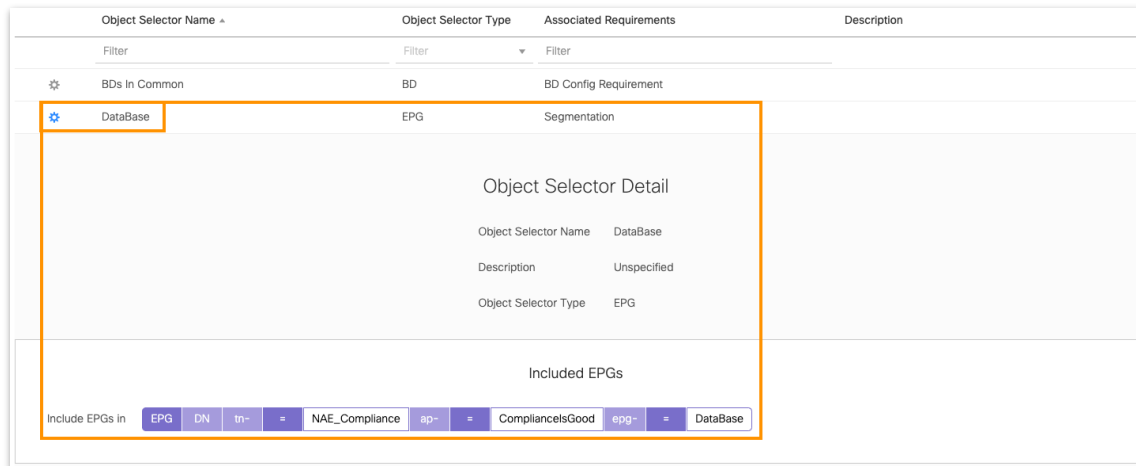


3. [コンプライアンス (Compliance) ] ドロップダウンから、[コンプライアンスの管理 (Manage Compliance) ] オプションを選択します。



事前設定された [オブジェクトセクタタイプ (Object Selector Type) ] = [EPG] の [オブジェクトセクタ (Object Selectors) ] が 2 つあることに注意してください。 [フロントエンド (FrontEnd) ] と [データベース (DataBase) ] です。

4. [データベース (Database) ] をクリックします。



5. [フロントエンド (FrontEnd) ] をクリックします。

Object Selector Name	Object Selector Type	Associated Requirements	Description
Filter	Filter	Filter	
BDs In Common	BD	BD Config Requirement	
DataBase	EPG	Segmentation	
FrontEnd	EPG	Segmentation	

Object Selector Detail

Object Selector Name: FrontEnd

Description: Unspecified

Object Selector Type: EPG

Included EPGs

Include EPGs in: EPG DN tn- = NAE\_Compliance ep- = CompliancelsGood epg- = FrontEnd

EPG は名前の完全一致に基づいて追加されます。

**Network Assurance Engine** には、次のような追加オプションがあります。

- ~ 指定した文字列を含む
- ^ 指定した文字列で始まる
- \$ 指定した文字列で終わる
- = 指定した文字列と等しい

およびその否定形。

## コンプライアンス要件

The screenshot shows the 'Manage Compliance' section of the Cisco Network Assurance Engine. It displays a table of compliance requirements with the following data:

Requirement Name	Description	Requirement Type	Communication Type
BD Config Requirement		CONFIGURATION_CO...	
Segmentation		SEGMENTATION	Must Not Talk

Below the table, the 'Compliance Requirement Detail' for 'Segmentation' is shown:

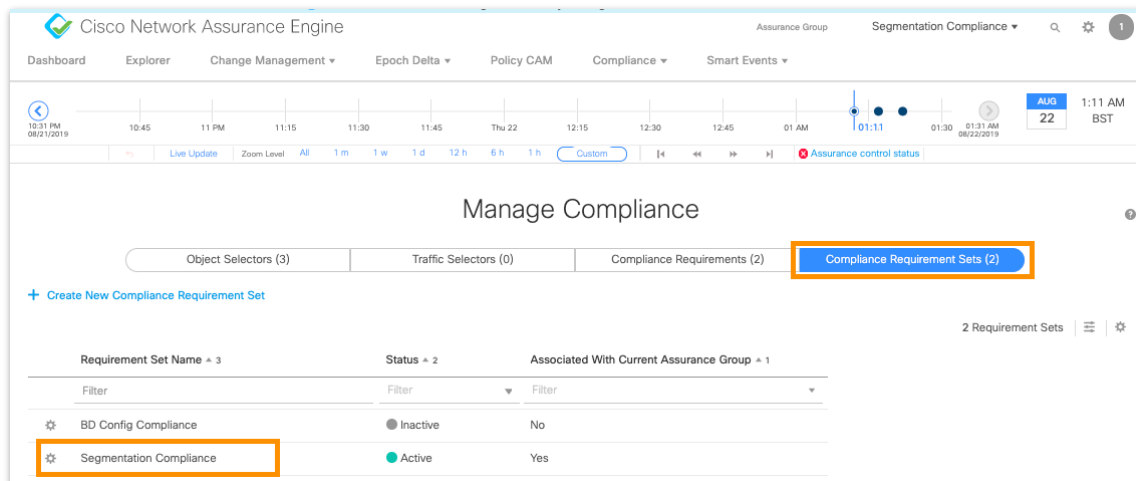
- Requirement Name: Segmentation
- Description: Unspecified
- Requirement Type: Segmentation
- Requirement: FrontEnd Must Not Talk To DataBase

1. [コンプライアンス要件 (Compliance Requirements) ] をクリックします。

**Segmentation** の要件、**Must Not Talk** に注意してください。**Segmentation** の設定を表示するには、

2. [セグメンテーション (Segmentation) ] をクリックします。

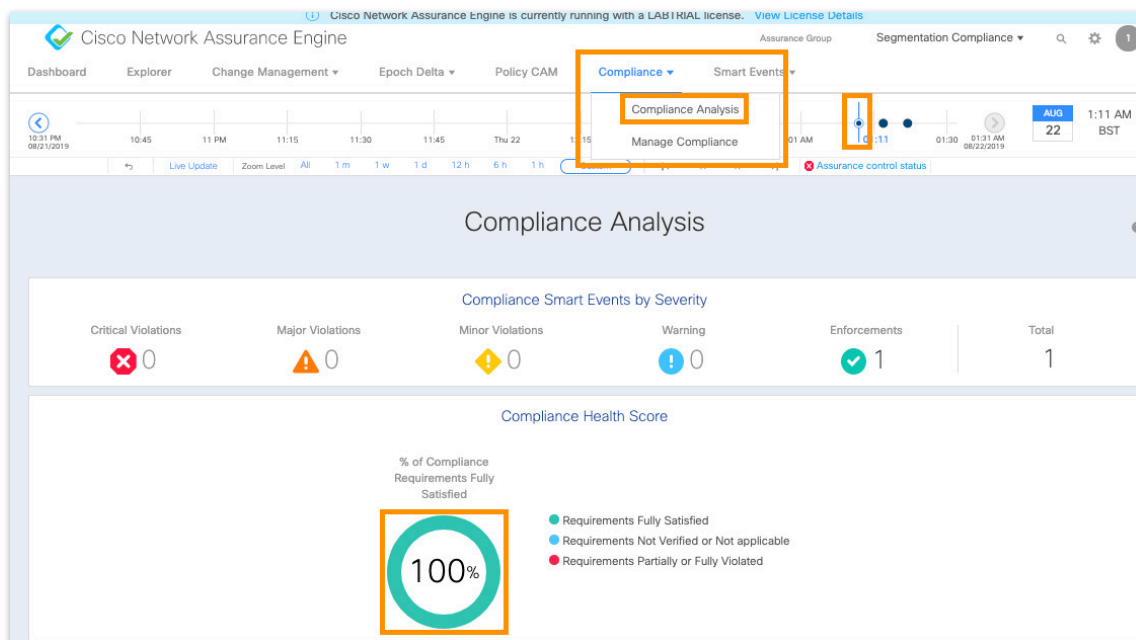
「フロントエンドはデータベースと通信してはならない」という、定義されたルールがあります。



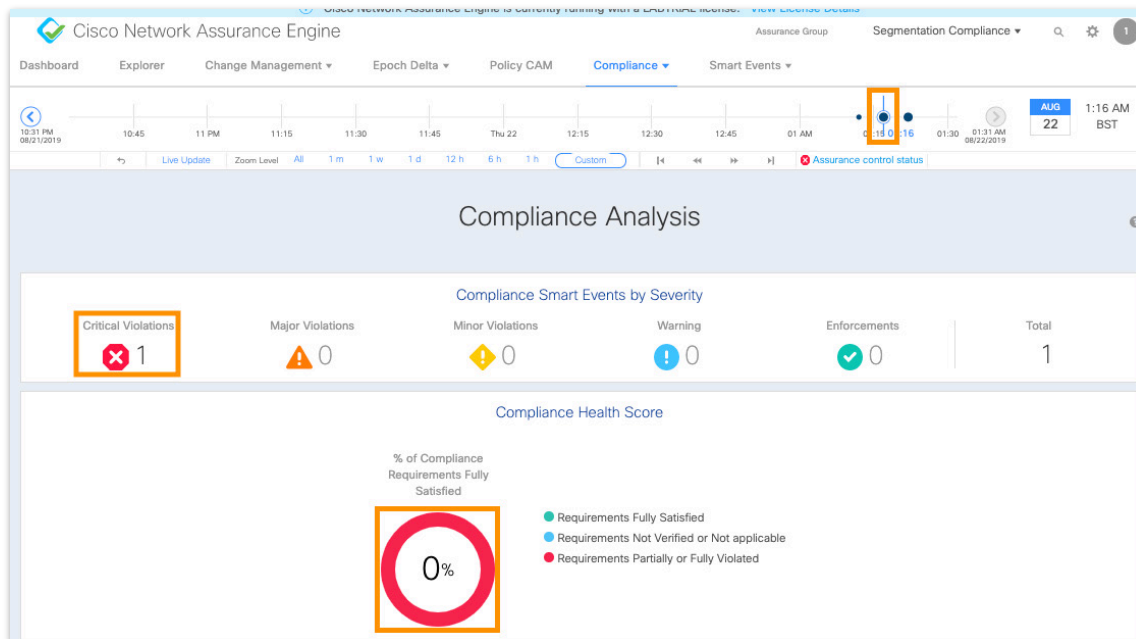
3. [コンプライアンス要件セット (Compliance Requirement Sets) ] をクリックします。

4. [セグメンテーションコンプライアンス (Segmentation Compliance) ] をクリックします。要件は、現在のアシュアランスグループに関連付けられていて、アクティブで、以前作成されたセグメンテーション要件を使用していることです。

## コンプライアンス分析



1. [タイムライン (timeline) ]で最初の [エポック (Epoch) ] を選択します。
2. [コンプライアンス (Compliance) ]ドロップダウンから、[コンプライアンス分析 (Compliance Analysis) ] を選択します。
3. ステータスが 100% であることを確認します。
4. [タイムライン (timeline) ]で 2 番目の [エポック (Epoch) ] を選択します。



問題：このエポックのコンプライアンスステータスは何ですか。

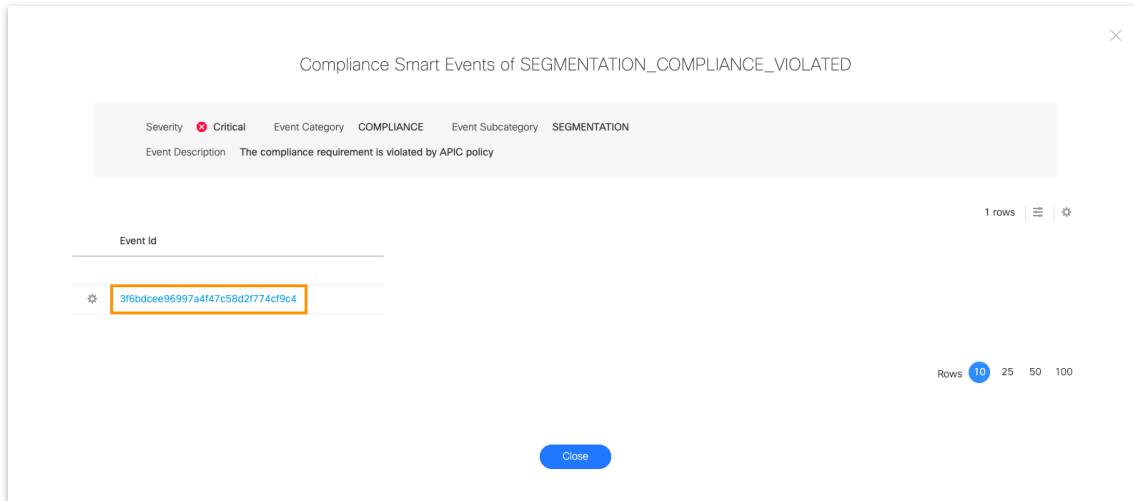
解答：重大な違反があります。

5. [重要なイベント (Critical Events) ] 数を表すリンク (上で強調表示) をクリックします。

The screenshot shows the 'Compliance Smart Events (1)' table. The table has columns for Severity, Event Subcategory, Event Name, Count, and Event Description. One event is listed with a severity of 'Critical' (indicated by a red 'x' icon) and the event name 'SEGMENTATION\_COMPLIANCE\_VIOLATED' (highlighted with a red box). The count for this event is 1. The event description is 'The compliance requirement is violated by APIC policy'.

Severity	Event Subcategory	Event Name	Count	Event Description
Critical	SEGMENTATION	SEGMENTATION_COMPLIANCE_VIOLATED	1	The compliance requirement is violated by APIC policy

6. **SEGMENTATION\_COMPLIANCE\_VIOLATED** リンクをクリックします。



7. [ イベント ID (Event Id) ] リンクをクリックします。

8. スマートイベントレポートを確認し、失敗したチェックに注意を払います。

Description	The compliance requirement is violated by APIC policy							
Impact	The EPG pair specified in the compliance requirement will be able to communicate with each other							
Affected Objects Details	Requirement	Requirement Set	EPG from Selector A	EPG from Selector B	Tenant of EPG from Selector A	Tenant of EPG from Selector B		
	Segmentation *	Segmentation Compliance *	FrontEnd *	DataBase *	NAE_Compliance *	NAE_Compliance *		
Checks	Permit Policy Check							
	Check Code	Failing Condition		Suggested Next Steps				
	135	The EPG pair is not segmented due to permit contract(s) between them		Perform one of the following steps to segment EPG pairs: <ul style="list-style-type: none"> <li>Remove the association of the permit contract(s) with one of the EPGs in the EPG pair.</li> <li>Change the scope of the permit contract(s) to prevent it from creating permit rules between EPGs below.</li> <li>Flip the action on the permit contract(s) between the EPGs.</li> </ul>				
Direction	Permit Policy							
	A to B							
	Provider	Consumer	Contract	Subject	Filter	Filter Entry	Direction	Filter Entry Description
	VRF1/any *	VRF1/any *	ssh *	ssh *	ssh *	338_0 *	Reverse *	[ tcp, src.port: 22 ] *
	VRF1/any *	VRF1/any *	ssh *	ssh *	ssh *	337_0 *	Forward *	[ tcp, dst.port: 22 ] *
	B to A							
	Provider	Consumer	Contract	Subject	Filter	Filter Entry	Direction	Filter Entry Description
	VRF1/any *	VRF1/any *	ssh *	ssh *	ssh *	338_0 *	Reverse *	[ tcp, src.port: 22 ] *
	VRF1/any *	VRF1/any *	ssh *	ssh *	ssh *	337_0 *	Forward *	[ tcp, dst.port: 22 ] *

ここで、コンプライアンスチェックが失敗した理由が分かりましたか？

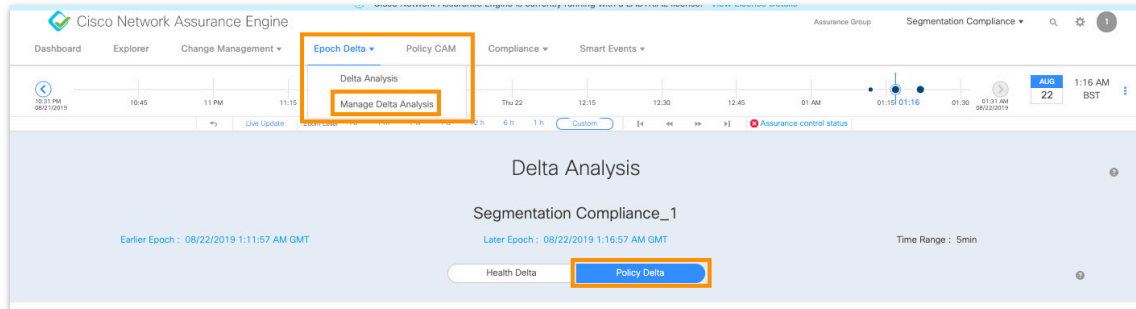
解答：

ユーザが、すべての EPG に影響を与える VRF レベルにあるポート 21 を開いた。



## エポックデルタ分析

このセクションでは、エポック 1 と 2 間の ACI 設定に加えられた変更を分析します。



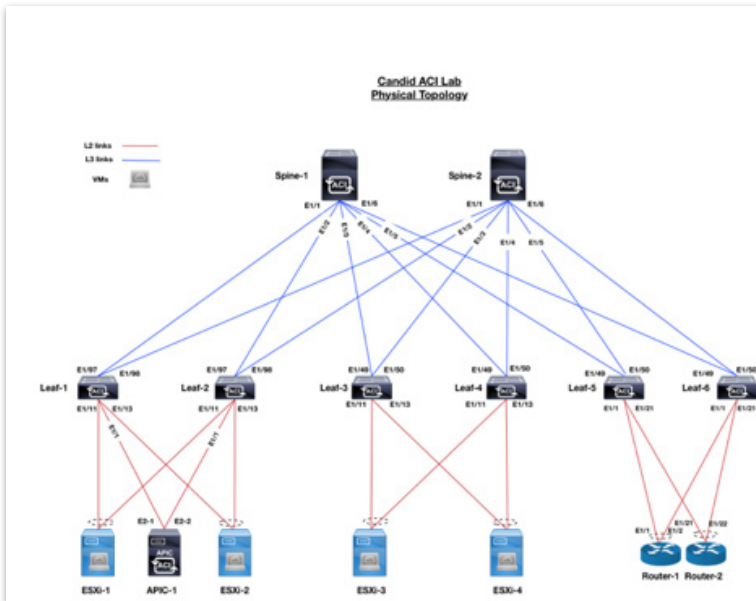
1. [エポックデルタ (Epoch Delta) ] をクリックします。
2. [デルタ分析 (Delta Analysis) ] をクリックします。
3. [ポリシーデルタ (Policy Delta) ] をクリックします。 監査ログには、2:16 am CEST GMT (2つのエポックの間に表示) に、管理者ユーザが、すべての EPG に対して ssh をコンシューマおよびプロバイダーとして許可するよう VRF を設定したことが示されていることに注意してください。



## 付録 A : ラボ ACI ファブリックの物理/論理トポロジ

このセクションでは、このラボで使用する ACI ファブリックの物理トポロジ、ルーティングトポロジ、および論理トポロジについて説明します。このラボのユーザが、ラボ演習の導入例で使用するネットワーク環境を理解するうえで役立ちます。

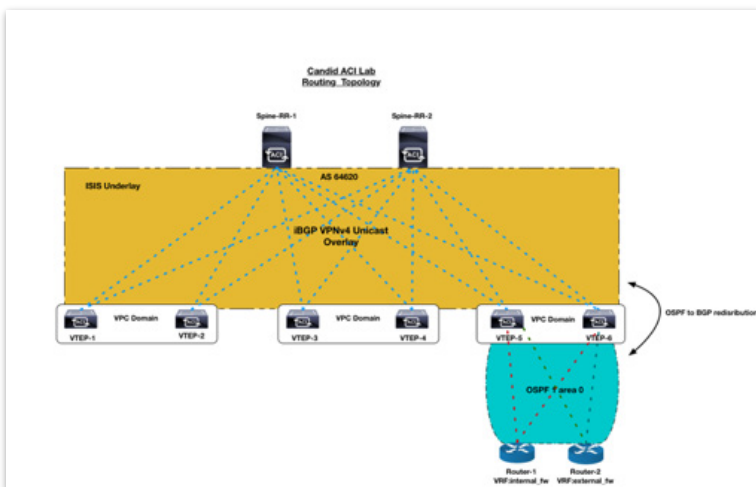
### 物理トポロジ :



ラボの ACI ファブリックは、6 つのリーフと 2 つのスパインで構成されています。Leaf-1 ~ Leaf-4 は、エンドホストが前面パネルポートに直接接続されたサーブリーフとして機能します。Leaf-5 と Leaf-6 は、一部のラボ演習で外部ルータとして機能する、またはファイアウォールをシミュレートする Nexus 3000 スイッチのペアに接続されたボーダリーフです。上記の図では、青色の線はレイヤ 3 のルーテッドリンクを示し、赤色の線はレイヤ 2 の物理接続を示します。

3 つの NAE VM が、3 つの異なる ESXi ホスト (トポロジ内の ESXi-1、2、3) にインストールされています。ESXi ホストには、異なる EPG のエンドポイントとして機能する仮想マシンもインストールされています。

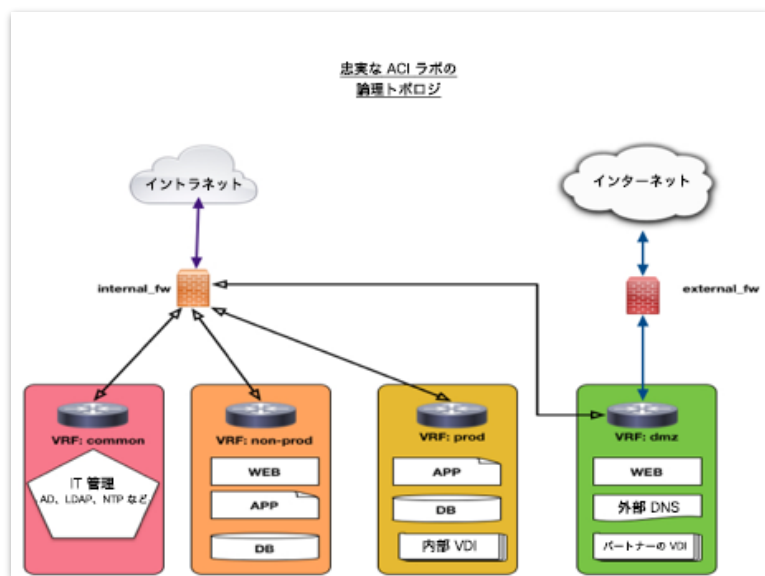
### ルーティングトポロジ :



設計では、ACI ファブリックは、外部ルートを伝搬するために、アンダーレイ IP ルーティングの IS-IS と iBGP VPNv4 を実行します。このラボファブリックは、Spine-1 と Spine-2 の両方を備えた BGP AS 64620 に、ルートリフレクタとして設定されています。ボーダーリーフ、Leaf-5、leaf-6 は、エリア 0 の OSPF を外部ルーターとともに実行します。

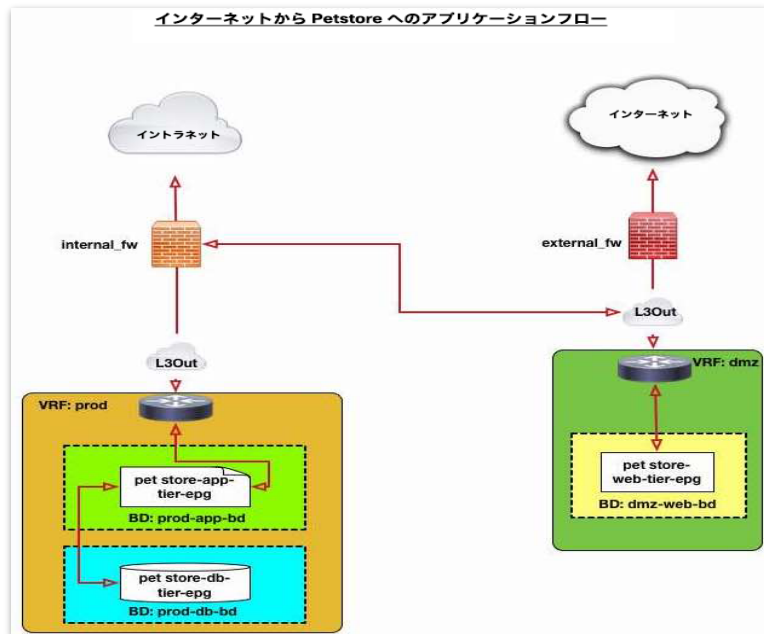
**論理トポロジ：**

論理トポロジは、多くの環境に導入された従来のファイアウォールサンドイッチ設計を表します。外部ファイアウォール (eDMZ) 環境は、パートナーおよび企業環境への外部接続に使用されます。内部ファイアウォール (iDMZ) 環境は、ミドルウェア/アプリケーション、データベース、および共通サービス、非実稼働環境への接続に使用されます。VDI はこのような環境で広く使用されており、必要に応じてデータ漏洩を防ぎ、ホストレベルのアクセスをロックダウンするセキュアなエンクレープを提供します。



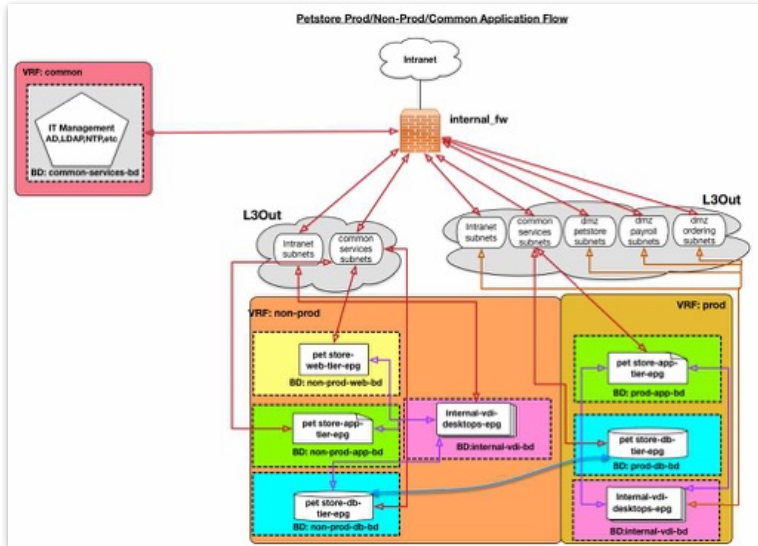
ACI ファブリックは、マルチテナントのクラウド データセンター ファブリックです。上記の論理図では、4 つのテナントが展開され、それぞれが角の丸い長方形で示されています。テナントは、common、non-prod、prod、dmz です。テナント dmz は、インターネットやイントラネットから外部ユーザがアクセスできるリソースが配置された、下位のセキュリティ層インフラストラクチャをホストします。これは 1 つのセキュリティゾーンを形成しています。その後、インターネットから内部リソースにアクセスするためにトラフィックをルーティングするには、VRF internal\_fw で示されるもう 1 つのセキュリティゾーンレベルを通過する必要があります。common、non-prod、prod のテナントは、制限付きセキュリティゾーン内でホストされます。インターネットから内部リソースに到達するには、アクセスを許可または拒否する 2 つのレベルのセキュリティルールが適用されます。

各テナントには、テナントと同じ名前で作成された VRF があります。VRF 内では、定義した EPG のブリッジドメインが作成されます。EPG はアプリケーション層と機能に基づいてセグメント化されます。仮想マシンは、トラフィックを生成し、さまざまなアプリケーション層間の通信をシミュレートするエンドポイントとして、各 EGP に展開されます。例として、アプリケーションプロファイル petstore の多数のアプリケーションフローの 1 つを以下に示します。



上記の図は、クライアントがインターネットから Web ベースのアプリケーションにアクセスする場合の従来の導入例を示します。クライアントは DMZ セキュリティ層の Web サーバにアクセスします。Web サーバへのアクセスは、外部ファイアウォールを通じて適用されるセキュリティルールによって制限されます。また、APIC には特定の L3out EPG から petstore-web-tier-epg へのトラフィックを許可する契約が必要です。クライアントがすべてのセキュリティ条件に合格して Web サーバにアクセスすると、Web サーバは、アプリケーションサーバの特定のブリッジドメイン内の実稼働テナントでホストされているアプリケーションサーバへのバックエンド接続を開始します。アプリケーションサーバは、各アプリケーションプロファイルの EPG にグループ化されます。契約は、prod-petstore-app-epg と dmz-pestore-web-epg 間に存在します。実稼働テナントは、より制限されたセキュリティゾーンの一部です。したがって、2 番目のレベルのセキュリティポリシーも internal fw を通じて適用されます。アプリケーションサーバは、契約を通じて許可されるバックエンドデータベースサーバにデータを読み書きする必要があります。これは、データベースサーバが独自の EPG 内の個別ブリッジドメインに存在するためです。

アプリケーションおよびシステム管理は、あらゆるデータセンターファブリックの重要な機能です。最新のデータセンターファブリックは、ファブリックに展開されたさまざまなシステムやアプリケーションの監視、管理、開発、テストに特化したテナントを常にホストしています。Cisco NAE ラボファブリックでは、実際の実稼働環境を複製するために同様のセットアップがプロビジョニングされます。以下に、アプリケーションプロファイル petstore 固有の論理トポロジの例を示します。



注：同様の設計は、payroll-ap や ordering-ap などの他のアプリケーションプロファイルにも適用されます。

実稼働テナントの内部システム管理者向けに EPG が作成され、非実稼働テナントの WEB、APP、DB EPG にアクセスして、実稼働テナントにプロビジョニングする前にシステムの開発と QA テストを行うことができます。また、実世界のデータセットとパラメータに対してアプリケーションコードをテストするため、青緑色の太線で示すように、非実稼働テナントと実稼働テナント内のデータベース間で定期的に同期が行われます。共通サービステナントでは、NTP、LDAP、DNS、DHCP、SNMP などのグローバルサービスがすべてのテナントによってアクセスできるように配置されています。システムおよびネットワーク管理者のマシンは管理のため、すべてのテナントに存在する任意のホストに ssh または icmp を実行できます。テナント間のすべての通信は、internal fw を通過し、契約を通じて許可される必要があります。

**APIC 命名規則：**

テナント以外のオブジェクトは、読みやすいようにオブジェクトタイプにサフィックスが付いています。これらの名前は、Cisco NAE アプライアンスにも表示されます。

例：

VRF は xxxx-vrf と呼ばれます。

ブリッジドメインは xxxx-bd と呼ばれます。

契約には次の命名規則が使用されます：

**T-fromAP-fromEPG-[toAP-toepg]-contract**

T = 送信元テナント名

fromAP = 送信元アプリケーションプロファイル

fromEPG = 送信元 EPG

toAP = 宛先アプリケーションプロファイル

toepg = 宛先 epg

From AP/ To AP は、AP の 2 つまたは 3 つの文字コードに略されます。例：PetStore (PS)、Payroll (PL)、Orderig (OR)

toepg が指定されていない場合、ターゲット AP 内のすべての EPG が契約を使用できることを意味します。

toAP が指定されていない場合、テナント内のすべての EPG が契約を使用できることを意味します。

外部契約の命名規則：

**T-e-extEPG-contrac**

APIC に設定されるこのテナントには、prod、non-prod、dmz、common が含まれます。次の表に、各テナントで設定されたアプリケーションプロファイルと EPG を示します。

テナント	AP	EPG
non-prod	internal-vdi-ap	internal-vdi-desktops-epg
non-prod	internal-vdi-ap	internal-vdi-infra-epg
non-prod	petstore-ap	petstore-web-tier-epg
non-prod	petstore-ap	petstore-app-tier-epg
non-prod	petstore-ap	petstore-db-tier-epg
non-prod	payroll-ap	payroll-web-tier-epg
non-prod	payroll-ap	payroll-app-tier-epg
non-prod	payroll-ap	payroll-db-tier-epg
non-prod	ordering-ap	ordering-web-tier-epg
non-prod	ordering-ap	ordering-app-tier-epg
non-prod	ordering-ap	ordering-db-tier-epg
non-prod	exchange-ap	exchange-mail-epg
non-prod	exchange-ap	exchange-dag-epg
non-prod	hadoop-ap	hadoop-mgmt-epg

non-prod	hadoop-ap	hadoop-user-connectivity-epg
non-prod	hadoop-ap	hadoop-hdfs-epg
prod	petstore-ap	petstore-app-tier-epg
prod	petstore-ap	petstore-db-tier-epg
prod	payroll-ap	payroll-app-tier-epg
prod	payroll-ap	payroll-db-tier-epg
prod	ordering-ap	ordering-app-tier-epg
prod	ordering-ap	ordering-db-tier-epg
prod	exchange-ap	exchange-mail-epg
prod	exchange-ap	exchange-dag-epg
prod	hadoop-ap	hadoop-mgmt-epg
prod	hadoop-ap	hadoop-user-connectivity-epg
prod	hadoop-ap	hadoop-hdfs-epg
prod	internal-vdi-ap	internal-vdi-desktops-epg
prod	internal-vdi-ap	internal-vdi-infra-epg
dmz	petstore-ap	petstore-web-tier-epg
dmz	payroll-ap	payroll-web-tier-epg
dmz	ordering-ap	ordering-web-tier-epg
dmz	partner-vdi-ap	partner-vdi-desktops-epg
dmz	partner-vdi-ap	partner-vdi-infra-epg

dmz	external-dns-ap	external-dns-epg
common	services-ap	services-management-epg





©2020 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

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

この資料の記載内容は 2020 年 5 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



#### お問い合わせ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

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