

vRealize Network Insight の使用

VMware vRealize Network Insight 5.2

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2020 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

1	vRealize Network Insight ユーザー ガイドについて	10
2	はじめに	11
	概要	11
	[ホーム] 画面	13
	ナビゲーション	14
	設定	15
3	vRealize Network Insight でのデータ ソースの追加	17
	サポート対象の製品とバージョン	19
	vCenter Server を追加	22
	VMware NSX Manager の追加	23
	VMware NSX-T Manager の追加	25
	VMware SD-WAN の追加	30
	SD-WAN での Cisco ASR/ISR の追加	31
	VMware Cloud on AWS の追加	32
	VMware Cloud on AWS 用の vRealize Network Insight コレクタのセットアップ	32
	vRealize Network Insight 用の VMware Cloud on AWS ファイアウォール ルールの作成	33
	VMware Cloud on AWS vCenter Server の追加	35
	VMware Cloud on AWS NSX Manager の追加	35
	Amazon Web Services の追加	37
	プライマリ AWS アカウントの追加	37
	標準の AWS データ ソースの追加	42
	AWS : 地理的ブロッキングのサポート	45
	Azure サブスクリプションの追加	46
	NSG フロー ログの有効化	47
	VMware PKS の追加	47
	Kubernetes の追加	49
	OpenShift の追加	50
	Palo Alto Networks Panorama の追加	50
	Check Point 管理サーバの追加	51
	Cisco ASA の追加	52
	Fortinet FortiManager の追加	53
	Arista スイッチ SSH の追加	54
	Dell OS10 スイッチの追加	54
	Dell OS10 スイッチでのテレメトリの有効化	55
	Huawei 6800/7800/8800 シリーズの追加	56
	Cisco ACI の追加	58

- NetFlow および sFlow 用の物理フロー コレクタの追加 59
- vRealize Log Insight の追加 60
- Infoblox の追加 62
- F5 BIG-IP の追加 63
- ServiceNow の追加 65
 - ServiceNow の追加 67
- 新しい汎用ルーターまたはスイッチの追加 81
 - 汎用ルーターまたはスイッチの編集 82

4 データ ソースの移行 83

5 vRealize Network Insight からのデータ ソースの削除 85

6 vRealize Network Insight 設定の構成 86

- システムの健全性の表示 87
- データ保持間隔の設定 87
- IP プロパティおよびサブネットの設定 88
 - DNS マッピング ファイルのインポート 88
 - サブネットと VLAN の間のマッピングの設定 88
 - East-West IP アドレスの設定 89
 - North-South 通信用の IP アドレスの設定 89
- イベントおよび通知の設定 90
 - システム イベントのリスト 90
 - システム イベントの表示と編集 136
 - ユーザー定義イベントの編集 139
 - プラットフォームの健全性イベントの表示 140
 - NSX-T イベント 141
 - Kubernetes イベント 152
 - 通知 154
- ID およびアクセス権の管理の設定 157
 - ユーザー管理の設定 157
- ログの設定 167
 - 監査ログの表示とエクスポート 167
 - Syslog の設定 167
- メール サーバを設定 168
- SNMP トラップ先の設定 169
 - SNMP トラップ先の削除 169
- ライセンスの管理 170
 - ライセンス エディションに基づく機能の比較 171
 - ライセンスの追加と変更 172
- 自動更新間隔の設定 173

- ユーザー セッションのタイムアウトの設定 174
- Google マップ API キーの追加 174
- データ ソース証明書の検証の構成 174
 - データ ソース証明書の手動での承諾 175
- 監査ログの表示 176
- カスタマー エクスペリエンス向上プログラムへの参加または参加取り消し 177
- セットアップの健全性の表示 178
- サポート トンネルの有効化 178
- ディスク使用率の管理 178
- ノードの詳細情報の表示 179
- サポート バンドルの作成 180
- コレクタおよびプラットフォームの負荷のキャパシティの概要 180

7 vRealize Network Insight での Direct Connect サポート 182

- VMC Direct Connect の詳細の表示 183
- Direct Connect 上のフローの表示 184
- Direct Connect 検索クエリ 184

8 vRealize Operations Manager 統合 186

9 クラスタの作成と拡張 187

- クラスタの作成 187
- クラスタの拡張 188

10 vRealize Network Insight でのフローの設定 189

- IPFIX 設定の有効化 189
 - Distributed Switch および DVPG での IPFIX 設定 189
 - VMware NSX IPFIX の設定 191
- 物理サーバのフロー サポート 193
 - 物理デバイスでの NetFlow コレクタの設定 193
 - フローと IP アドレス エンドポイントの拡充 198
 - [物理から物理] フローの検索 199
- ブロックおよび保護されたフローの表示 199
- ネットワーク アドレス変換 (NAT) 200
 - NAT フローのサポート - 例 201
- VMware Cloud on AWS 個のフロー 203
- VPC フロー ログの作成 203
- F5 から vRealize Network Insight コレクタへのフロー レコードの送信 204
 - IPFIX コレクタのプールの作成 205
 - IPFIX ログの宛先の作成 205
 - ログ発行元の作成 206

- iRule の作成 206
- 仮想サーバへの iRule の追加 211
- ルート エントリの作成 211

11 Kubernetes と VMware PKS のスコーピングおよびフロー情報 213

12 エンティティの詳細の表示 214

- vRealize Network Insight システム (NI システム) の詳細の表示 215
- プラットフォーム仮想マシンの詳細の表示 216
- コレクタ仮想マシンの詳細の表示 216
- VMware vCenter データ ソースの詳細の表示 217
- PCI コンプライアンスの詳細の表示 217
 - PDF としてエクスポート 218
- Kubernetes の詳細の表示 219
- ロード バランサの詳細の表示 220
- 仮想マシンの詳細の表示 221
- Edge デバイスの詳細の表示 221
- NSX Manager の詳細の表示 222
- [VMware NSX-T Manager] の詳細の表示 223
- [NSX-T 管理ノード] 詳細の表示 224
- NSX-T トランスポートの詳細の表示 224
- 仮想サーバの詳細の表示 226
- プール メンバーの詳細の表示 227
- Microsoft Azure の詳細の表示 228
- VeloCloud Enterprise の詳細の表示 230
 - VeloCloud Edge の詳細の表示 231
- SD-WAN および Edge SD-WAN アプリケーションの詳細の表示 232
- [SD-WAN 評価] の詳細の表示 233
 - 評価レポートの生成 233
- [VeloCloud リンク アプリケーション] 詳細の表示 233
- [VeloCloud ビジネス ポリシー] の詳細の表示 234
- VMC SDDC の詳細の表示 234
- [Arista ハードウェア ゲートウェイ] および [Arista ハードウェア ゲートウェイのバインド] の詳細の表示 235
- [Cisco Nexus デバイス] の詳細の表示 235
- フロー情報の詳細の表示 236
- マイクロセグメンテーションの詳細の表示 239
- アプリケーションの詳細の表示 240
- 分析：外れ値検出 241
 - 外れ値を持つ仮想マシンの検出方法 242
- 分析：静的および動的しきい値 243
 - しきい値とアラートの設定 243

しきい値設定画面の表示 246

13 エンティティ トポロジの表示 248

仮想マシン トポロジ 248

ホスト トポロジ 248

VXLAN トポロジ 249

VLAN トポロジ 250

NSX Manager トポロジ 250

vRealize Network Insight での NSX オブジェクトの監査情報の表示 251

14 ピンの使用 255

ピン 255

ピンのタイプ 255

ピンボード 257

ピンボードの共有とコラボレーション 261

ピンボードをホーム ページとして設定するには 263

ピンボードを複製するには 264

15 vRealize Network Insight におけるロード バランサのサポート 265

ロード バランサとしての F5 265

ロード バランサの詳細の表示 266

仮想サーバの詳細の表示 267

プール メンバーの詳細の表示 268

ロード バランサに関連するサンプル検索クエリ 269

ロード バランサとしての NSX-V 269

16 ネットワークの可視性 270

バス トポロジ 270

AWS 仮想マシン間バス 271

NSX-T 273

NSX-V Edge トランク インターフェイスの仮想マシン間バス 274

vRealize Network Insight での NAT のサポート 274

VMware SD-WAN の仮想マシン間バス 276

Arista ハードウェア VTEP 仮想マシン間バス 277

VMware Cloud on AWS : 仮想マシン間バス 278

Cisco ACI 仮想マシン間のバス 279

Cisco BGP-EVPN モードのサポート 280

イコールコスト マルチパス (ECMP) ルートのサポート 281

L2 ブリッジのサポート 282

BGP ネイバーの詳細の表示 282

インターネットへのパス 283

17 セキュリティ 284

- Cross-vCenter NSX 284
- Palo Alto Networks 285
- Cisco ASA ファイアウォール 288
- Check Point ファイアウォール 290
- セキュリティ グループ 292
- ポリシーベース VPN 293
- NSX 分散ファイアウォールの非アクティブ ルール 294
- Fortinet ファイアウォール 294

18 マイクロセグメンテーションの操作 296

- アプリケーションの分析 296
 - ドーナツ ビューでのマイクロセグメンテーションおよびフロー データの表示 296
 - グリッド ビューでのマイクロセグメンテーションおよびフロー データの表示 299
 - 手動によるアプリケーションの作成 300
- アプリケーション検出 302
 - 検出されたアプリケーションの追加 304
- VMware Cloud on AWS : 計画およびマイクロセグメンテーション 308

19 推奨されるファイアウォール ルール 309

- ルールのエクスポート 311
 - NSX DFW ユニバーサル アーティファクト 312
 - CSV エクスポートの設定をプロパティ テンプレートとして保存 313
- Kubernetes ネットワーク ポリシーのエクスポートと適用 315

20 検索クエリの操作 317

- 検索クエリの保存と削除 318
- 検索クエリ 319
 - Azure 検索クエリ 324
 - Cisco ACI エンティティ 325
 - Fortinet 検索クエリ 328
 - Infoblox DNS データによるフローの強化 329
 - Kubernetes エンティティの一般的な検索クエリ 329
 - ロード バランサに関連するサンプル検索クエリ 332
 - NSX ファイアウォール ルールの検索クエリ 332
 - VMware SD-WAN 検索クエリ 333
 - VMC SDDC 検索クエリ 334
 - AWS エンティティ向け VMware Cloud on AWS 335
- 高度なクエリ 336
- 時間管理 340
- 検索結果 341

フィルタ 341

vCenter Server タグ 342

21 vRealize Network Insight のディザスタ リカバリの計画 345

ディザスタ リカバリ シナリオの例 346

22 トラブルシューティング 349

一般的なデータ ソースのエラー 349

DFW IPFIX を有効にできない 350

23 vRealize Network Insight を使用した VMware Cloud on AWS へのアプリケーションの移行の計画 353

NSX Manager の CSP 更新トークンの取得方法 354

vCenter Server の認証情報の取得方法 357

コンピューティング ゲートウェイ：ファイアウォール ルール 360

vRealize Network Insight ユーザー ガイドについて

1

『vRealize Network Insight ユーザーガイド』には、vRealize Network Insight の使用に関する情報が記載されています。

対象者

この情報は、vRealize Network Insight の使用を担当する管理者またはスペシャリストを対象としています。記載されている情報は、仮想マシンの管理者としての経験があり、エンタープライズ管理アプリケーションおよびデータセンターの運用に詳しい方を対象としています。

はじめに

2

この章には、次のトピックが含まれています。

- 概要
- [ホーム] 画面
- ナビゲーション
- 設定

概要

vRealize Network Insight は、ソフトウェア定義のネットワークとセキュリティにおいてインテリジェントな運用を実現します。複数のマルチクラウド環境にまたがる、安全かつ可用性の高い、最適化されたネットワーク インフラストラクチャを構築するのに役立ちます。マイクロセグメンテーションの計画とデプロイを促進し、仮想ネットワークと物理ネットワーク全体の可視化を実現します。また、VMware NSX 環境を管理および拡張するための運用ビューを提供します。

データセンター全体は、エンティティとその関係で構成されていると考えることができます。たとえば、仮想マシンはエンティティであり、また、別のエンティティであるホストの一部でもあります。vRealize Network Insight は、データセンターの一部である多数のエンティティを可視化し、その情報を提供します。

表 2-1.

エンティティ	説明
	ホスト
	問題
	NSX ファイアウォール
	仮想マシン

表 2-1. (続き)

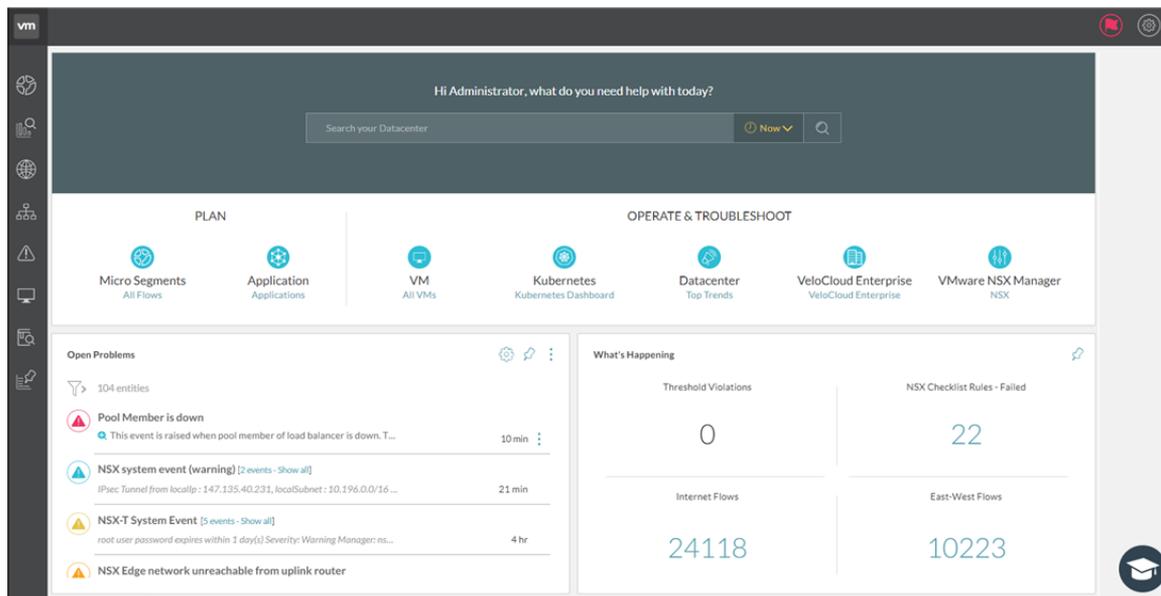
エンティティ	説明
	vSphere Distributed Switch
	物理スイッチ
	仮想ポート グループ
	Cisco ファブリック エクステンダ
	論理スイッチ
	データストア
	物理ネットワーク インターフェイス カード
	セキュリティ グループ
	ブレード
	ルーター
	VLAN
	仮想マシンのグループ
	設定の変更
	ルーター インターフェイス
	トラブルシューティング

表 2-1. (続き)

エンティティ	説明
	ネットワーク アクセス変換 (NAT)
	メール サーバ

[ホーム] 画面

VMware vRealize Network Insight の [ホーム] 画面には、データセンター全体で何が発生しているかを示す簡潔なサマリが表示されます。また、データセンターの vRealize Network Insight の重要なコンポーネントにすばやくアクセスできます。



[ホーム] 画面は以下のセクションに分類されます。

検索バー

検索バーを使用すると、データセンター ネットワーク（およびそれに対応するエンティティ）全体を検索できます。検索バーを使用して、データセンターで使用可能なエンティティを検索できます。検索バーは、[ホーム] 画面の最上部にあります。

要件に基づいて、次のタイムライン オプションに従って検索を実行できます。

- [プリセット]: このオプションを使用すると、last week、last 3 days、last 24 hours、yesterday、today、last 2 hours、last hour、now（現在時刻）などの事前設定によって検索結果を絞り込むことができます。
- [日時]: このオプションを使用すると、特定の日時によって検索結果を絞り込むことができます。
- [範囲]: このオプションを使用すると、特定の時間範囲のデータを検索できます。

[計画] セクション

- [マイクロ セグメント] : すべての仮想マシン間のフローに基づいて、ネットワークのマイクロセグメンテーションを計画できます。
- [アプリケーション] : アプリケーションを定義してフローを分析し、セキュリティを計画することができます。

[運用とトラブルシューティング] セクション

[運用とトラブルシューティング] セクションでは、以下のコンポーネントの可視性、メトリック、分析が提供されません。

- 仮想マシン (VM)
- VLAN ネットワーク
- データセンター
- NSX セキュリティ グループ
- VMware NSX

未解決の問題

[未解決の問題] セクションでは、データセンター内で検出された重大なイベントを簡単に確認できます。これらのイベントは、類似したものがすべてグループ化されます。すべてのイベントを表示するには、[すべて表示] を使用します。イベントの詳細を表示するには、 ([詳細の表示]) をクリックします。[イベントの構成] アイコンを使用すると、[システム イベント] 画面に移動してシステム イベントを構成できます。

また、特定のイベントの [詳細オプション] で [イベントの構成] オプションをクリックすると、特定のイベントの編集ビューに直接移動して構成を編集できます。

現在の状態

[現在の状態] セクションでは、データセンターのプロパティのうち値が非常に高いものを簡単に確認できます。プロパティの詳細を表示するには、特定のプロパティの値をクリックします。また、このセクションにはイベントをフィルタリングするためのフィルタが左側にあり、イベントの詳細を表示するための [すべて展開] ボタンおよび [すべて折りたたむ] ボタンもあります。

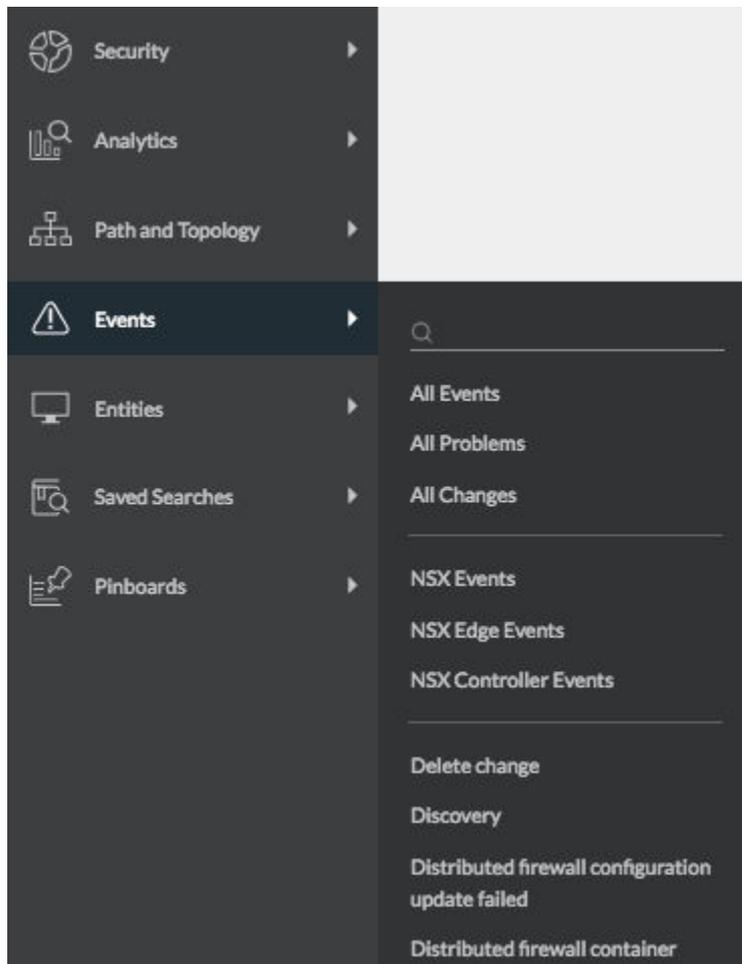
ナビゲーション

vRealize Network Insight には左側にナビゲーション パネルが表示されます。このパネルによって、ユーザーは、検索クエリを入力することなく、自分が関心のあるセキュリティ、トポロジ、エンティティ、イベント、保存された検索などの主要な製品機能にすばやく移動できます。

ナビゲーション パネルには、次のオプションがあります。

- セキュリティ : 次のオプションが用意されています。
 - セキュリティのプラン : 環境内のフローを分析し、環境内のマイクロセグメントの計画に役立てることができます。すべてのエンティティを選択するか、特定のエンティティを選択して、選択したエンティティを分析する期間を選択することができます。

- アプリケーション：カスタム検索を使用して、vRealize Network Insight でアプリケーションを作成できます。アプリケーションを作成したら、アプリケーションを適切に計画できます。
- PCI コンプライアンス：PCI コンプライアンス ダッシュボードは、NSX 環境専用の PCI 要件に対する準拠度を評価するのに役立ちます。
- パスとトポロジ：仮想マシン間のパスまたはデータセンターの複数のエンティティのトポロジを表示できます。
- イベント：環境内のイベント（変更と問題）を表示できます。また、特定のタイプのイベントをすばやく表示できるように、イベント タイプのリストも表示されます。
- エンティティ：環境内にあるさまざまなタイプのエンティティを網羅するリストを表示します。特定のリストで任意のエンティティ タイプをクリックすると、そのタイプのすべてのエンティティがリストで表示されます。エンティティ リストの上にあるテキスト ボックスを使用すると、入力したテキストに基づいてリストを絞り込むことができます。
- 保存された検索：以前に保存した検索が表示されます。



設定

[設定] 画面には、データ プロバイダ、ユーザー、および通知を管理するためのコントロールがあります。

[設定] 画面に移動するには、以下の手順に従います。

- 1 [ホーム] 画面の右上隅にある [プロフィール] アイコンをクリックします。
- 2 [設定] をクリックします。[設定] 画面が表示されます。

vRealize Network Insight でのデータソースの追加

3

データソースにより、アプリケーションは、データセンターの特定の側面からデータを収集できます。収集範囲は、NSX インストールから、Cisco™ シャーシ 4500 や Cisco™ N5K などの物理デバイスにまで及びます。

データソースを追加するには、次の操作を行います。

- 1 [設定] の [インストールとサポート] 画面で、[アカウントとデータソース] をクリックします。
- 2 [新しいソースの追加] をクリックします。
- 3 アカウントまたはソースタイプを選択します。
- 4 フォームに必須情報を入力します。
- 5 [検証] をクリックします。
- 6 データソースのニックネームとメモ（必要な場合）を入力します。
- 7 [送信] をクリックして、データソースを環境に追加します。

各データソースについて、次の詳細を表示できます。

プロパティ	説明
タイプ (ニックネーム)	データソースの名前を表示します。
IP アドレス/FQDN	データソースの IP アドレスまたは FQDN の詳細を表示します。
前回の収集	データが収集された前回の収集時間が表示されます。
検出された仮想マシン	このデータソースについて検出された仮想マシンの数が表示されます。 注: [検出された仮想マシン] 列は、データソースが vCenter Server または AWS ソースの場合にのみ表示されます。
コレクタ仮想マシン	データソースが追加されたコレクタの名前が表示されます。リストされているすべてのデータソースが同じコレクタに追加されている場合、この列は表示されません。この列は、データソースが異なるコレクタにある場合にのみ表示できます。
有効	データソースが有効かどうかを示します。
アクション	データソースを編集および削除するためのオプションを表示します。

vRealize Network Insight には、データ ソースの情報に簡単にアクセスできるようにするための次の機能があります。

- データ ソースの検索は、列ヘッダーの上の検索バーを使用して、データ ソースの名前、IP アドレス、またはコレクタ仮想マシン名で実行できます。
- [タイプ (ニックネーム)] 列では、データ ソース別に情報をフィルタリングできます。
- [コレクタ仮想マシン] 列では、さまざまなコレクタ仮想マシン別に情報をフィルタリングできます。
- データ ソースは、それらのタイプとニックネームでアルファベット順にソートされます。

追加された各データ ソースについて、次の情報を表示できます。

- すべて：使用可能なすべてのデータ ソースを表示します。
- 問題のあるデータ ソース：vRealize Network Insight が問題を検出したデータ ソースを表示します。
- 推奨事項があるデータ ソース：追加情報が必要なデータ ソースについて、vRealize Network Insight が自動生成した推奨事項を表示します。
- 無効：無効にされたデータ ソースを表示します。

この章には、次のトピックが含まれています。

- サポート対象の製品とバージョン
- vCenter Server を追加
- VMware NSX Manager の追加
- VMware NSX-T Manager の追加
- VMware SD-WAN の追加
- SD-WAN での Cisco ASR/ISR の追加
- VMware Cloud on AWS の追加
- Amazon Web Services の追加
- Azure サブスクリプションの追加
- VMware PKS の追加
- Kubernetes の追加
- OpenShift の追加
- Palo Alto Networks Panorama の追加
- Check Point 管理サーバの追加
- Cisco ASA の追加
- Fortinet FortiManager の追加
- Arista スイッチ SSH の追加
- Dell OS10 スイッチの追加

- Huawei 6800/7800/8800 シリーズの追加
- Cisco ACI の追加
- NetFlow および sFlow 用の物理フロー コレクタの追加
- vRealize Log Insight の追加
- Infoblox の追加
- F5 BIG-IP の追加
- ServiceNow の追加
- 新しい汎用ルーターまたはスイッチの追加

サポート対象の製品とバージョン

vRealize Network Insight はいくつかの製品およびバージョンをサポートしています。

データ ソース	バージョン / モデル	接続プロトコル	権限
Amazon Web Services (エンタープライズライセンスのみ)	該当なし	HTTPS	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Arista スイッチ	7050TX、7250QX、7050QX-32S、7280SE-72	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Azure サブスクリプション	該当なし	HTTPS	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Brocade スイッチ	VDX 6740、VDX 6940、MLX、MLXe	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Check Point ファイアウォール	Check Point R80、R80.10、R80.20、R80.30	HTTPS、SSH	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco	ASR 1K、ISR4K、CSR1Kv、ISR1K 注： SD-WAN 評価のためにのみサポート	<ul style="list-style-type: none"> ■ サポート対象の OS : Cisco IOS XE ソフトウェア ■ OS バージョン : 16.07.01 	ネットワークの検証と管理機能(ネットワーク マップとインテント) はサポートされません。
Cisco ACI	3.2	HTTPS (APIC コントローラ) SNMP (APIC コントローラおよび ACI スイッチ)	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco ASA	OS 9.4 の X シリーズ	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco Catalyst	3000、3750、4500、6000、6500	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco Nexus	3000、5000、6000、7000、9000	SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー

データ ソース	バージョン / モデル	接続プロトコル	権限
Cisco UCS (統合コンピューティングシステム)	シリーズ B ブレード サーバ、シリーズ C ラック サーバ、シャーシ、ファブリック相互接続	UCS Manager : HTTPS UCS ファブリック : SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー
Dell スイッチ	FORCE10 MXL 10、FORCE10 S6000、S4048、Z9100、S4810、PowerConnect 8024、Dell OS10	SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー
Fortinet FortiManager	6.0.1	HTTPS	ユーザーには次のものがが必要です。 <ul style="list-style-type: none"> ■ すべての ADOM およびポリシーパッケージへのアクセス権を持つ制限されたユーザー 以上のロール。 ■ コマンドライン インターフェイスから有効にされた rpc-permit read アクセス権。
F5 BIG - IP	12.1.2 以降	HTTPS、SSH、SNMP	ユーザーには、ロールが1つ以上必要です。また、TMSH が有効になっており、すべてのパーティションにアクセスする必要があります。F5 BIG-IP は、ルーティングとロード バランシングの両方をサポートします。
HP	HP Virtual Connect Manager 4.41、HP OneView 3.0	HP OneView 3.0 : HTTPS HP Virtual Connect Manager 4.41 : SSH	読み取り専用ユーザー
Huawei Cloud Engine	6800、7800、8800	SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー
Infoblox	Infoblox NIOS バージョン 8.0、8.1、8.2	HTTPS	API インターフェイス アクセス権を持つ読み取り専用ユーザー DNS オブジェクト タイプの読み取り専用権限は次のとおりです。 <ul style="list-style-type: none"> ■ 権限タイプ - DNS ■ リソース - A レコード、DNS ゾーン、DNS ビュー
Juniper スイッチ	EX3300、QFX 51xx シリーズ (JunOS v12 & v15、QFabric なし)	Netconf、SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー
Kubernetes	<ul style="list-style-type: none"> ■ 1.12 (NSX-T 2.3.1) ■ 1.12 (NSX-T 2.3.2) ■ 1.13 (NSX-T 2.3.2) 	HTTPS	ユーザーには、読み取り権限を持つクラスタ管理者ロールが必要です。
OpenShift	3.1.1	HTTPS	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Palo Alto Networks	Panorama 7.0.x、7.1、8.x、9.0	HTTPS	ユーザーには、XML API アクセス権限を持つ管理者ロールが必要です。詳細については、『vRealize Network Insight ユーザー ガイド』の「Palo Alto Networks」セクションを参照してください。

データ ソース	バージョン / モデル	接続プロトコル	権限
ServiceNow	London	HTTPS	ユーザーには管理者ロールが必要です
VMware SD-WAN	VeloCloud Orchestrator および Edge バージョン 3.3.1 以降	HTTPS	ユーザーには、次のいずれかの権限を持つアカウント ロールが必要です。 <ul style="list-style-type: none"> ■ スーパーユーザー ■ 標準管理者 ■ カスタム サポート
VMC on AWS - vCenter	M8 以降 注: NSX-T ベースの VMware Cloud on AWS SDDC のみがサポートされます。	HTTPS	ユーザーには次の権限が必要です。 <ul style="list-style-type: none"> ■ クラウド管理者: データ ソースを追加して、IPFIX を有効にします。
VMC on AWS - NSX Manager	M8 以降 注: NSX-T ベースの VMware Cloud on AWS SDDC のみがサポートされます。	HTTPS	ユーザーには次のいずれかの権限が必要です。 <ul style="list-style-type: none"> ■ 組織メンバー.管理者: データ ソースの追加と IPFIX の有効化。 ■ 組織メンバー.管理者.NSX Cloud 管理者: データ ソースの追加と IPFIX の有効化。 ■ 組織メンバー.VMware Cloud on AWS (すべてのロール): データ ソースの追加と IPFIX の有効化。 ■ 組織メンバー.NSX Cloud 監査者: データ ソースの追加。
VMware Identity Manager	3.3 以降	HTTPS	ユーザーには管理者ロールが必要です。
VMware PKS	サポートされているバージョン		ユーザーにはクラスタ管理者ロールの権限 - pks.clusters.admin が必要です。
VMware NSX Manager (VMware NSX-V)	サポートされているバージョン	SSH, HTTPS	『vRealize Network Insight ユーザーガイド』の「Edge データ収集」セクションを参照してください。
VMware NSX-T Manager	2.4。 その他のサポートされるバージョンについては、サポートされるバージョンを参照してください。	HTTPS	読み取り専用ユーザー

データ ソース	バージョン / モデル	接続プロトコル	権限
VMware vRealize Log Insight	サポートされているバージョン	HTTPS	コンテンツ バックをインストール、構成、管理する権限を持つ API ユーザー
VMware vSphere	サポートされているバージョン IPFIX の場合、VMware ESXi のバージョンは次のようになります。 <ul style="list-style-type: none"> ■ 5.5 Update 2 (ビルド 2068190) 以降 ■ 6.0 Update 1b (ビルド 3380124) 以降 ■ VMware VDS 5.5 以降 注： 仮想マシン間のパスを識別するには、データセンターのすべての仮想マシンに VMware Tools をインストールする必要があります。	HTTPS	読み取り専用ユーザー IPFIX の構成と使用に必要な権限 権限付きの vCenter Server 認証情報: Distributed Switch: Modify dvPort group: Modify vCenter Server の事前定義ロールには、root レベルで割り当てられた、子ロールに伝達が必要な次の権限が必要です。 System.Anonymous System.Read System.View global.settings

注：

- Cisco ASA、ACI、Catalyst、および Nexus デバイスでサポートされているオペレーティング システムは、iOS/NX-OS です。Cisco UCS の場合は、UCSM バージョンです。
- Arista でサポートされているオペレーティング システムは、Arista EOS です。

vCenter Server を追加

vCenter Servers をデータ ソースとして vRealize Network Insight に追加できます。

複数の vCenter Servers を vRealize Network Insight に追加して、データの監視を開始できます。

前提条件

- vCenter Server の事前定義ロールには、root レベルで割り当てられた、子ロールに伝達が必要な次の権限が必要です。
 - System.Anonymous
 - System.Read
 - System.View
 - Global.Settings
- IPFIX の設定と使用には、次の vCenter Server 権限が必要です。
 - Distributed Switch : 変更およびポート設定操作
 - dvPort グループ : 変更およびポリシー操作

vCenter Server でのロールの詳細については、『vSphere セキュリティ ガイド』の「ロールを使用した権限の割り当て」セクションを参照してください。

手順

- 1 [vCenter Server の追加] をクリックします。
- 2 [新しいソースの追加] をクリックし、オプションをカスタマイズします。

オプション	アクション
コレクタ仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	vCenter Server の IP アドレスまたは完全修飾ドメイン名を入力します。
ユーザー名	次の権限を持つユーザー名を入力します。 <ul style="list-style-type: none"> ■ [Distributed Switch] : 変更 ■ [dvPort グループ] : 変更
パスワード	vCenter Server システムにアクセスするための vRealize Network Insight ソフトウェアのパスワードを入力します。

- 3 [検証] をクリックします。

検出された仮想マシンの数が、プラットフォームまたはコレクタ ノードのキャパシティを超えている場合、検証に失敗します。プラットフォームのブリック サイズを増やすか、クラスタを作成するまでは、データ ソースを追加することはできません。

フローがある場合とない場合の各ブリック サイズの指定されたキャパシティは、次のようになります。

ブリック サイズ	仮想マシン	フローの状態
大	6 k	有効
大	10 k	無効
中	3 k	有効
中	6 k	無効

- 4 IPFIX を有効にするには、[この vCenter Server での Netflow (IPFIX)] を選択します。

IPFIX の詳細については、ユーザー ガイドの「Distributed Switch および DVPG での IPFIX 設定の有効化」のセクションを参照してください。

注： vCenter Server と VMware NSX Manager の両方で IPFIX を有効にすると、vRealize Network Insight は、関連付けられた vCenter Server で一部の DVPG で IPFIX を無効にして、フローの冗長性を自動的に検出して削除します。

- 5 高度なデータ収集ソースを vCenter Server システムに追加します。
- 6 vCenter Server システムを追加するには、[送信] をクリックします。vCenter Server システムがホーム画面に表示されます。

VMware NSX Manager の追加

vRealize Network Insight で NSX-V をデータ ソースとして追加できます。

前提条件

以下を確認します。

- vCenter Server をデータ ソースとして追加してあること。
- Enterprise ロール。
- システム管理者の認証情報（Central CLI が有効になっている場合）。
- 表 3-1.

NSX バージョン	ユーザー
NSX 6.4 以降のリリース	<ul style="list-style-type: none"> ■ NSX Manager をデータ ソースとして追加するには、スーパーユーザー、エンタープライズ管理者、監査者、または NSX セキュリティ管理者である必要があります。 ■ エンタープライズ管理者、スーパーユーザー、NSX セキュリティ管理者、または監査者は、vRealize Network Insight で必要な NSX Central CLI コマンドを実行できます。 <p>注： NSX ネットワーク管理者は、NSX Manager をデータ ソースとして追加できません。</p>
NSX 6.2 から NSX 6.4 までのリリース	<ul style="list-style-type: none"> ■ エッジデータのポピュレートを有効にするには、管理者である必要があります。 ■ 監査者、スーパーユーザー、または NSX セキュリティ管理者は、vRealize Network Insight で必要な NSX Central CLI コマンドを実行できます。 ■ NSX Manager をデータ ソースとして追加するときに指定する必要があるユーザー認証情報は、エンタープライズ管理者またはスーパーユーザーの情報である必要があります。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [VMware Manager] で、[VMware NSX Manager] をクリックします。
- 4 [新しい VMware NSX Manager アカウントまたはソースの追加] 画面で、次の必須情報を指定します。

オプション	アクション
コレクタ（プロキシ）仮想マシン	ドロップダウンメニューからコレクタ仮想マシンを選択します。
プライマリ VMware vCenter Server	vRealize Network Insight に追加する vCenter Server を選択します。 注： vCenter Server とそれに関連する NSX Manager のデータ ソースは、同じコレクタに追加していることを確認してください。同じプロキシ サーバに接続すると、拒否されたフローが表示されず（NSX IPFIX が有効になっている場合）、適用されたファイアウォール ルールが一部のフローで使用できなくなる可能性があります。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。

5 [検証] をクリックします。

6 (オプション) NSX Controller データを収集する場合は、[NSX Controller データ収集の有効化] チェックボックスを選択します。

このオプションを選択すると、vRealize Network Insight では、論理ルーター インターフェイス、ルート、論理スイッチ MAC テーブル、VTEP レコード、コントローラ クラスタのステータス、ロールなどのコントローラ データが収集されます。データ収集は、NSX Central CLI またはコントローラ SSH セッションによって実行されます。

7 (オプション) NSX Edge データを収集する場合は、[NSX Edge データ収集の有効化] チェックボックスを選択します。

Edge データ収集は NSX Central CLI によって実行されます。そのため、NSX Manager にエッジ データ プロバイダは作成されません。Edge のポピュレートが有効な場合、NSX ユーザーの権限が検証されます。

NSX 6.3 のエンタープライズ管理者権限を持つユーザーが、最新リリースの vRealize Network Insight を使用している場合、[VMware NSX Manager] の [アカウントとデータ ソース] ページには `Insufficient Privileges` エラーが表示されます。NSX 6.3 で NSX Central CLI コマンドを実行するにはスーパー ユーザーであることが必要なため、このエラーが表示されます。

8 (オプション) IPFIX フローを収集する場合は、[IPFIX の有効化] チェックボックスを選択します。

このオプションを選択すると、vRealize Network Insight は NSX-V から DFW IPFIX フローを受信しません。

注： vCenter Server と VMware NSX Manager で IPFIX を有効にすると、vRealize Network Insight は、関連付けられた vCenter Server で一部の DVPG で IPFIX を無効にして、フローの冗長性を自動的に検出して削除します。

IPFIX の有効化の詳細については、[VMware NSX-V IPFIX の有効化](#)を参照してください。

9 [ニックネーム] テキスト ボックスにニックネームを入力します。

10 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。

11 [送信] をクリックします。

VMware NSX-T Manager の追加

VMware NSX-T は、異種のエンドポイントとテクノロジー スタックを備えた、新しいアプリケーション フレームワークとアーキテクチャに対応するように設計されています。これらの環境には、vSphere に加えて、他のハイパーバイザー、コンテナ、ヘアメタル、パブリック クラウドも含まれることがあります。vRealize Network Insight は、vCenter Server によって仮想マシンが管理される NSX-T 展開をサポートします。

考慮事項

- vRealize Network Insight は、vCenter Server が ESXi ホストを管理する NSX-T セットアップのみをサポートします。

- vRealize Network Insight は、NSGroup、NSX-T ファイアウォール ルール、IPSet、NSX-T 論理ポート、NSX-T 論理スイッチ、NSX-T 分散ファイアウォールの IPFIX フロー、セグメント、グループ、およびポリシーベースの VPN をサポートします。
- vRealize Network Insight は、NSX-V と NSX-T の両方の展開をサポートしています。クエリで NSX を使用する場合、結果には NSX-V と NSX-T の両方のエンティティが含まれます。NSX Manager には、NSX-V Manager と NSX-T Manager の両方が一覧表示されます。NSX セキュリティ グループには、NSX-T と NSX-V の両方のセキュリティ グループが表示されます。NSX-V または NSX-T が NSX の代わりに使用されている場合は、これらのエンティティのみが表示されます。ファイアウォール ルール、IPSet、論理スイッチなどのエンティティにも、同じ論理が当てはまります。
- NSX-T 2.4 リリースでは、vRealize Network Insight は NSX 宣言型ポリシー管理をサポートしており、これにより、結果主導型のポリシー ステートメントを使用して、ネットワークおよびセキュリティの構成を簡素化および自動化できます。

注： セキュリティ グループのマイクロセグメンテーションは、NSX ポリシー データに基づいて実行されます。ただし、対応する NSX ポリシー グループがない場合は、スタンドアロン NS グループがマイクロセグメンテーション分析に含まれます。NS グループの詳細については、[NSX-T の製品ドキュメント](#)を参照してください。

NSX-T Manager をデータ ソースとして追加するには

NSX-T Manager をデータ ソースとして追加するための前提条件は次のとおりです。

- NSX-T Manager に関連付けられているすべての vCenter Server をデータ ソースとして vRealize Network Insight に追加することをお勧めします。
- vCenter Server を追加する前に NSX-T Manager を追加すると、vRealize Network Insight は安定化するまで約 4 時間かかります。
- 分散ファイアウォール (DFW) の除外リストに論理スイッチがないことを確認します。このリストに論理スイッチがある場合、これらの論理スイッチに接続されている仮想マシンのフローは報告されません。

NSX-T Manager を追加するには、次のように行います。

- 1 [設定] の [アカウントとデータ ソース] 画面で、[ソースの追加] をクリックします。
- 2 [アカウントまたはデータ タイプの選択] 画面の [VMware Manager] で、[VMware NSX-T Manager] を選択します。

3 ユーザー認証情報を指定します。

注：

- 1つの NSX-T 展開に複数の管理ノードがある場合は、1台のノードのみをデータソースとして vRealize Network Insight に追加するか、(これらのノードの) 仮想 IP アドレス (VIP) を使用する必要があります。複数の管理ノードを追加すると、vRealize Network Insight が適切に機能なくなる可能性があります。
- NSX-T をデータソースとして追加する場合は、VIP の使用を推奨します。VIP ではなく管理ノードの IP アドレスを追加する場合に、後で VIP または他の管理ノードの IP アドレスを追加する場合は、既存のデータソースを削除して、新しい VIP または管理 IP アドレスを追加する必要があります。
- IPFIX が必要ない場合、ユーザーは監査レベルの権限を持つローカルユーザーである必要があります。一方、IPFIX が必要な場合は、ユーザーは、enterprise_admin、network_engineer、または security_engineer のいずれかの監査レベル権限を持っている必要があります。

- 4 (オプション) [DFW IPFIX を有効にする] を選択して、NSX-T で IPFIX 設定を更新します。このオプションを選択すると、vRealize Network Insight は NSX-T から DFW IPFIX フローを受け取ります。IPFIX の有効化の詳細については、[VMware NSX-T DFW IPFIX の有効化](#)を参照してください。

注：

- DFW IPFIX は、NSX-T の Standard エディションではサポートされていません。
- vRealize Network Insight は NSX-T スイッチの IPFIX フローをサポートしていません。

- 5 (オプション) 遅延メトリックデータを収集する場合は、[遅延メトリックの収集を有効にする] チェックボックスを選択します。このオプションを選択すると、vRealize Network Insight は NSX-T から遅延メトリック (VTEP-VTEP) を受信します。このオプションを使用できるのは、NSX-T 2.5 以降のみです。ESXi ノードから遅延データを受信するために、コレクタのポート 1991 が開いていることを確認します。

クエリの例

NSX-T に関連するクエリの例を示します。

表 3-2. NSX-T のクエリ

クエリ	検索結果
<code>NSX-T Manager where VC Manager=10.197.53.214</code>	この特定の VC Manager がコンピュータ マネージャとして追加された NSX-T Manager です。
<code>NSX-T Logical Switch</code>	vRealize Network Insight のインスタンスにあるすべての NSX-T 論理スイッチが一覧表示されます。スイッチの作成元がシステムであるか、またはユーザーであるかについての詳細も含まれています。
<code>NSX-T Logical Ports where NSX-T Logical Switch = 'DB-Switch'</code>	特定の NSX-T 論理スイッチ (DB-Switch) に属する NSX-T 論理ポートを一覧表示します。
<code>VMs where NSX-T Security Group = 'Application-Group'</code> または <code>VMs where NSGGroup = 'Application-Group'</code>	特定のセキュリティグループ (Application-Group) 内のすべての仮想マシンを一覧表示します。

表 3-2. NSX-T のクエリ (続き)

クエリ	検索結果
<code>NSX-T Firewall Rule where Action='ALLOW'</code>	アクションが ALLOW として設定されているすべての NSX-T ファイアウォール ルールを一覧表示します。
<code>NSX-T Firewall Rule where Destination Security Group = 'CRM-Group'</code>	CRM-Group がターゲット セキュリティ グループであるファイアウォール ルールを一覧表示します。結果には、直接的なターゲット セキュリティ グループと間接的なターゲット セキュリティ グループの両方が含まれます。
<code>NSX-T Firewall Rule where Direct Destination Security Group = 'CRM-Group'</code>	CRM-Group がターゲット セキュリティ グループであるファイアウォール ルールを一覧表示します。結果には、直接的なターゲット セキュリティ グループのみが含まれます。
<code>VMs where NSX-T Logical Port = 'App_Port-Id-1'</code>	特定の NSX-T 論理ポートを持つすべての仮想マシンが一覧表示されます。
<code>NSX-T Transport Zone</code>	VLAN およびオーバーレイ トランスポート ゾーンと、それに関連付けられている詳細 (トランスポート ノードのタイプを含む) を一覧表示します。 注: vRealize Network Insight はデータ ソースとして KVM をサポートしていません。
<code>NSX-T Router</code>	TIER-1 と TIER-0 のルーターを一覧表示します。結果に表示されるルーターをクリックすると、NSX-T Edge クラスターや HA モードなどのより詳細な情報が表示されます。

表 3-3. NSX ポリシーのクエリ

<code>NSX Policy Segment</code>	vRealize Network Insight のインスタンスにあるすべての NSX ポリシー セグメントが一覧表示されます。
<code>NSX Policy Manager</code>	vRealize Network Insight のインスタンスにあるすべての NSX Policy Manager が一覧表示されます。
<code>NSX Policy Group</code>	vRealize Network Insight のインスタンスにあるすべての NSX ポリシー グループが一覧表示されます。
<code>NSX Policy Firewall</code>	vRealize Network Insight のインスタンスにあるすべての NSX ポリシー ファイアウォールが一覧表示されます。
<code>NSX Policy Firewall Rule</code>	vRealize Network Insight のインスタンスにあるすべての NSX ポリシー ファイアウォール ルールを一覧表示します。
<code>NSX Policy Firewall Rule where Action = 'ALLOW'</code>	アクションが ALLOW として設定されているすべての NSX ポリシー ファイアウォール ルールを一覧表示します。
<code>NSX Policy Based VPN</code>	vRealize Network Insight のインスタンスにあるすべての NSX ポリシー ベース VPN を一覧表示します。

注: NSX-T 2.4 および VMware Cloud on AWS が vRealize Network Insight のデータ ソースとして追加されている場合、NST-T エンティティを取得するには、クエリで `SDDC type = ONPREM` というフィルタを追加する必要があります。たとえば、

`NSX Policy Based VPN where Tier0 = '' and SDDC Type = 'ONPREM'` のようにします。

NSX-T メトリックのサポート

次の表に、現在 NSX-T メトリックをサポートしている vRealize Network Insight エンティティと、対応するエンティティ ダッシュボードにこれらのメトリックを表示するウィジェットを示します。

表 3-4.

エンティティ	エンティティ ダッシュボードのウィジェット	サポートされる NSX-T メトリック
論理スイッチ	論理スイッチのバケット メトリック	Multicast and Broadcast Rx
	論理スイッチのバイト メトリック	Multicast and Broadcast Tx Unicast Rx Unicast Tx Dropped Rx Dropped Tx Rx Packets (Total) Tx Packets (Total)
論理ポート	論理ポートのバケット メトリック	Multicast and Broadcast Rx
	論理ポートのバイト メトリック	Multicast and Broadcast Tx Unicast Rx Unicast Tx Rx Packets (Total) Tx Packets (Total)
ルーター インターフェイス	ルーター インターフェイス メトリック	Rx Packets Tx Packets Dropped Rx Packets Dropped Tx Packets Rx Bytes Tx Bytes
ファイアウォール ルール	ファイアウォール ルール メトリック	Hit Count Flow Bytes Flow Packets

NSX-T メトリックのサンプル クエリを次に示します。

- `nsx-t logical switch where Rx Packet Drops > 0`
このクエリは、ドロップし受信パケット数が 0 より大きい、すべての論理スイッチを一覧表示します。
- `nsx-t logical port where Tx Packet Drops > 0`
このクエリは、ドロップした転送パケット数が 0 より大きい、すべての論理ポートを一覧表示します。
- `top 10 nsx-t firewall rules order by Connection count`
このクエリは、接続数 (Hit Count) に基づいた上位 10 個のファイアウォール ルールを一覧表示します。

VMware SD-WAN の追加

vRealize Network Insight に、VMware SD-WAN by VeloCloud をデータ ソースとして追加することができます。

前提条件

以下の条件を確認します。

- データ ソースを追加するための適切な権限がある。権限の詳細については、「サポート対象の製品とバージョン」を参照してください。
- VeloCloud Orchestrator と Edge バージョン 3.3.1 以降を使用している。
- 1 つ以上の VMware SD-WAN ライセンスを追加した。
- データ ソースとして追加された別の VMware SD-WAN がない。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [SD-WAN] で、[VeloCloud] をクリックします。
- 4 [新しい VeloCloud アカウントまたはソースの追加] 画面で、次の必須情報を指定します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
VCO URL	データ ソースとして追加する VCO の URL を入力します。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。

- 5 [検証] をクリックします。
- 6 [ニックネーム] テキスト ボックスにニックネームを入力します。
- 7 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 8 [送信] をクリックします。

次のステップ

ポート 2055 で、すべてのプロファイルと Edge に対して NetFlow を有効にする必要があります。NetFlow の収集を有効にする方法については、VMware SD-WAN の [データ ソースの編集] 画面で、[手順の表示] をクリックします。

注： [手順の表示] オプションは「注：すべてのプロファイルと Edge で Netflow 収集を有効にする必要があります。」メッセージに表示されます。

SD-WAN での Cisco ASR/ISR の追加

Cisco ASR/ISR ルーターは、SD-WAN 評価の目的でのみ vRealize Network Insight データ ソースとして追加が可能です。vRealize Network Insight は、Cisco ASR/ISR ルーターを他の目的でのデータ ソースとしてサポートしません。

vRealize Network Insight は、SD-WAN 評価の目的でのみ、次のバージョンの Cisco ASR/ISR をサポートしています。

バージョン / モデル	サポートされる OS	OS バージョン
ASR 1K, ISR4K, CSR1Kv, ISR1K	Cisco IOS XE Software	16.07.01

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [WAN] で [Cisco ASR/ISR (SD-WAN 評価)] をクリックします。
- 4 [新しい Cisco ASR/ISR アカウントまたはソースの追加] 画面で、次の情報を指定します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス	IP アドレスの詳細を入力します。 注: このデータ ソースは、FQDN を使用して追加することはできません。このデータ ソースを追加するには、IP アドレスの詳細を入力する必要があります。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。

- 5 [検証] をクリックします。
- 6 [SNMP バージョン] ドロップダウン メニューから、[2C] を選択します。
- 7 [コミュニティ スtring] テキスト ボックスに、コミュニティ文字列を入力します。
- 8 各アップリンク インターフェイスを MPLS またはインターネットにマッピングします。アップリンク インターフェイスをマッピングするには、各 [インターフェイス名] に対するドロップダウン メニューをクリックし、適切なオプションを選択します。

デフォルトでは、vRealize Network Insight はすべてのアップリンク インターフェイスを取得してリストします。

- 9 [ニックネーム] テキスト ボックスに、データ ソースのニックネームを入力します。
- 10 [サイト] と [リージョン] テキスト ボックスに適切なサイトとリージョン名を入力します。
- 11 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 12 [送信] をクリックします。

次のステップ

- 1 NetFlow および sFlow 用の物理フロー コレクタの追加。
- 2 Cisco ASR/ISR を構成して vRealize Network Insight Collector に NetFlow 情報を送信するようにします。NetFlow の構成の詳細については、[物理デバイスでの NetFlow コレクタの設定](#)を参照してください。

注： SD-WAN 評価のための十分なフロー情報を収集するには、約 4 時間かかります。

- 3 「SD-WAN 評価の詳細の表示」ページに移動し、SD-WAN 評価の詳細を確認します。

VMware Cloud on AWS の追加

vRealize Network Insight による VMware Cloud on AWS のサポートは、Enterprise ライセンスのユーザーに限定されます。VMware Cloud on AWS (vCenter) または VMware Cloud on AWS (NSX Policy Manager) をデータ ソースとして追加できます。

VMware Cloud on AWS 用の vRealize Network Insight コレクタのセットアップ

VMware Cloud on AWS からデータを収集するには、vRealize Network Insight コレクタをセットアップする必要があります。

前提条件

データ ソースとして追加する必要があるすべての SDDC 内に vRealize Network Insight コレクタを展開します。

注：

- VMware Cloud on AWS SDDC に展開された vRealize Network Insight コレクタを使用して、別の VMware Cloud on AWS SDDC からデータを収集することはサポートされません。
 - vRealize Network Insight コレクタは、ネイティブの VMware Cloud on AWS セグメントに展開する必要があります。拡張セグメントへのコレクタの展開はサポートされていません。
-

手順

- 1 vRealize Network Insight にログインします。
- 2 [設定] - [インストールとサポート] - [コレクタ仮想マシンの追加] の順に移動します。
- 3 共有シークレットの内容をコピーします。
これは vRealize Network Insight コレクタ OVA の展開時に必要になります。
- 4 vRealize Network Insight コレクタ OVA を VMware Cloud on AWS vCenter Server のコンピューティング リソース プールに展開します。
生成した共有シークレットを使用します。

注： VMware Cloud on AWS の単一ノード SDDC の場合、プロキシ仮想マシンの CPU リソース予約は 1251 MHz 以上にする必要があります。

- 5 コレクタ仮想マシンを起動し、ウィザードに従ってコレクタと vRealize Network Insight プラットフォームをペアリングします。
- 6 コレクタがプラットフォームと正常にペアリングされていることを確認します。

vRealize Network Insight 用の VMware Cloud on AWS ファイアウォールルールの作成

vRealize Network Insight との通信を構築するには、VMware Cloud on AWS グループとファイアウォールルールを作成する必要があります。

前提条件

- オンプレミスの場合、vRealize Network Insight プラットフォームとコレクタを展開します。クラウドサービスの場合、有効なサブスクリプションを取得します。
- 必要な権限を持っていること。サポート対象の製品とバージョンを参照してください。
- NSX-T のネットワークを使用する VMware Cloud on AWS の Software-Defined Data Center (SDDC) バージョン 1.8 以降を展開します。
- vRealize Network Insight プラットフォームとコレクタ間の通信用ファイアウォールルールの構成。
- 受信トラフィックのポート要件については、[システム ポート] 画面の [コレクタ サーバのポート] テーブルを参照してください。
- 次のドメインへの送信トラフィック用に HTTPS ポート 443 を開きます。
 - *.vmwareidentity.com
 - gaz.csp-vidm-prod.com
 - *.vmware.com
 - *.ni-onsaas.com

vRealize Network Insight プラットフォームとコレクタ間の通信用ファイアウォールルールの構成

VMware Cloud on AWS でのファイアウォールルールの構成では、次の作業を実行します。

- vRealize Network Insight コレクタ用に VMware Cloud on AWS グループを作成します。
 - a <https://vmc.vmware.com> から VMware Cloud on AWS にログインします。
 - b [ネットワークとセキュリティ] タブで、[インベントリ] > [グループ] の順にクリックします。
 - c [グループ] カードで [コンピューティング グループ] をクリックしてから、[グループの追加] をクリックしてグループの [名前] を指定し、任意で [説明] を入力します。
 - d [メンバーを設定] をクリックし、[メンバーを選択] 画面を開きます。
 - e vRealize Network Insight コレクタ仮想マシンの詳細を指定します。

後で作成するファイアウォールルールでこのグループを使用して、VMware Cloud on AWS NSX Manager と vRealize Network Insight 間の通信を許可します。

- ファイアウォール ルールを作成します。
 - a <https://vmc.vmware.com> から VMC コンソールにログインします。
 - b [ネットワークとセキュリティ] タブで、[ゲートウェイ ファイアウォール] をクリックします。
 - c [ゲートウェイ ファイアウォール] カードで、[コンピューティング ゲートウェイ] をクリックしてから、[ルールの追加] をクリックし、新しいルールの [名前] を入力します。
 - d 新しいルールのパラメータを入力します。
 - [ソース] : vRealize Network Insight コレクタの IP アドレスを含む VMware Cloud on AWS グループの名前を入力します。
 - [宛先] : [任意] を選択します。
 - [サービス] : [HTTPS]、[DNS]、[DNS-UDP]、[NTP]、[ICMP] を選択します。
 - [アクション] : [許可] を選択します。
 - [適用先] : [インターネット インターフェイス] を選択します。
 - [ログ] : 必要に応じてログを有効にします。必要でない場合、このフィールドは変更しません。
新しいルールはデフォルトで有効になります。切り替えボタンを左にスライドして無効にします。
 - e [公開] をクリックします。

コレクタと NSX Manager、およびコレクタと vCenter Server 間の通信のためのファイアウォール ルールの構成

- 1 <https://vmc.vmware.com> から VMC コンソールにログインします。
- 2 [ネットワークとセキュリティ] タブで、[ゲートウェイ ファイアウォール] をクリックします。
- 3 [ゲートウェイ ファイアウォール] カードで、[管理ゲートウェイ] をクリックしてから、[ルールの追加] をクリックし、新しいルールの [名前] を入力します。
- 4 新しいルールのパラメータを入力します。
 - [ソース] : vRealize Network Insight コレクタの IP アドレスを含む VMware Cloud on AWS グループの名前を入力します。
 - [宛先] : [システム定義のグループ] を選択し、NSX Manager を検索して NSX Manager エントリを選択します。
 - [サービス] : [HTTPS (443)] を選択します。
 - [アクション] : [許可] を選択します。
 - [ログ] : 必要に応じてログを有効にします。
新しいルールはデフォルトで有効になります。切り替えボタンをスライドして無効にします。
- 5 [公開] をクリックします。
- 6 同じ手順を実行して、vCenter Server のルールを設定します。

注： 手順 4 の [宛先] フィールドでは [vCenter Server] を選択します。

VMware Cloud on AWS vCenter Server の追加

VMware Cloud on AWS - vCenter Server をデータ ソースとして追加できます。

前提条件

- VMware Cloud on AWS - vCenter Server をデータ ソースとして追加するための認証情報を取得します。
 - a VMware Cloud Services コンソールにログインします。
 - b [マイ サービス] の [VMware Cloud on AWS] をクリックします。
 - c 目的の Software-Defined Data Center (SDDC) の名前をクリックします。
 - d [設定] タブを選択し、次のタスクを実行します。
 - [vCenter Server FQDN] パネルを展開し、[vCenter Server FQDN] をコピーするか、メモします。
 - [デフォルトの vCenter Server ユーザー アカウント] パネルを展開し、ユーザー認証情報をコピーするか、メモします。
- 少なくとも、VMware Cloud on AWS vCenter Server に対する読み取り専用権限が必要です。

手順

- 1 vRealize Network Insight ユーザー インターフェイスで、[設定] - [アカウントとデータ ソース] - [ソースの追加] の順に移動します。
- 2 [VMware Cloud on AWS] で、[VMware Cloud on AWS - vCenter Server] をクリックします。
- 3 [VMware Cloud on AWS - VMware vCenter の追加] 画面で、
 - コレクタ仮想マシンを選択します。
 - VMware Cloud Services から取得した vCenter Server の FQDN を指定します。
 - VMware Cloud Services から取得したユーザー認証情報を指定します。
- 4 [検証] をクリックします。
- 5 データ ソースの [ニックネーム] と [メモ] (ある場合) を入力し、[送信] をクリックします。
- 6 [VMware Cloud on AWS NSX Manager の追加](#)。

VMware Cloud on AWS NSX Manager の追加

VMware Cloud on AWS - NSX Manager をデータ ソースとして追加できます。

前提条件

- [API トークンを生成](#)します。

- 使用可能なすべての vRealize Network Insight 機能を使用し、VMware Cloud on AWS Policy Manager で DFW IPFIX を有効にするには、管理者ロールと NSX Cloud 管理者ロールが必要です。ただし、NSX Cloud 監査者（読み取り専用）ロールがあれば、機能にアクセスできます。詳細については、次の表を参照してください。

組織ロール	サービス ロール	許可されるアクション
組織メンバー	管理者	データ ソースの追加、IPFIX の有効化
組織メンバー	管理者と NSX Cloud 管理者	データ ソースの追加、IPFIX の有効化
組織メンバー	VMware Cloud on AWS（すべてのロール）	データ ソースの追加、IPFIX の有効化
組織メンバー	NSX Cloud 監査者	データ ソースの追加のみ

手順

- 1 次のいずれかの手順を実行します。

- VMware Cloud on AWS - vCenter Server を追加していない場合
 - a [VMware Cloud on AWS vCenter Server の追加](#)。
 - b [NSX Manager を追加] をクリックします。
- すでに VMware Cloud on AWS - vCenter Server を追加している場合
 - a [設定] - [アカウントとデータ ソース] - [ソースの追加] の順にクリックします。
 - b [VMware Cloud on AWS] で、[VMware Cloud on AWS - NSX Manager] をクリックします。

- 2 [新しい VMC NSX Manager アカウントの追加] 画面で、以下の操作を実行します。

- 対応する vCenter Server を選択します。
コレクタは、vCenter Server の選択に基づいて自動的に選択されます。VMware Cloud on AWS。対応する vCenter Server のコレクタ仮想マシンと同じコレクタ仮想マシンに NSX Manager を追加する必要があります。
- 生成した IP アドレスと API トークンを指定します。
NSX Manager の IP アドレスは、VMware Cloud on AWS SDDC の [サポート] タブで確認できます。

- 3 [検証] をクリックします。

- 4 分散ファイアウォール (DFW) の IPFIX フローを収集する場合は、[DFW IPFIX の有効化] を選択します。

注： 次のシナリオでは、エラー メッセージがポップアップ表示されます。

- NSX Cloud Admin 権限がない。
- DFW IPFIX コレクタ プロファイルにすでにコレクタを 4 つ追加している。[DFW IPFIX を有効にできない](#)も参照してください。

- 5 データ ソースの [ニックネーム] と [メモ]（ある場合）を入力し、[送信] をクリックします。

Amazon Web Services の追加

vRealize Network Insight では、Amazon Web Services (AWS) をデータ ソースとして追加できます。

次の 2 種類の AWS アカウントをデータ ソースとして追加できます。

- プライマリおよびリンクされた AWS アカウント
- 標準 AWS アカウント

プライマリおよびリンクされた AWS アカウント

プライマリ AWS アカウント（組織アカウントまたは支払人アカウント）は、組織内のすべてのリンクされた AWS アカウントを API 呼び出しを通じて検出および一覧表示できる組織レベルのアクセス権を持っています。

プライマリ アカウントに追加された組織内の AWS アカウントはすべて、リンクされたアカウントと呼ばれます。詳細については、[ListAccount](#) を参照してください。

プライマリ AWS アカウントには、リンクされた AWS アカウントのリソースにアクセスして制御するために、リンクされた AWS アカウントに対するロールが必要です。すべてのリンクされた AWS アカウントは、ロール ARN を介してプライマリ AWS アカウントを信頼する必要があります。ロールの詳細については、[AssumeRole](#) を参照してください。

プライマリ AWS アカウントをデータ ソースとして追加すると、すべてのリンクされた AWS アカウントがデータ ソースとして自動的に追加されます。

標準 AWS アカウント

標準 AWS アカウントには、プライマリおよびリンクされた関係はありません。

プライマリ AWS アカウントの追加

プライマリ AWS アカウントを追加することにより、組織内のすべてのリンクされた AWS アカウントを自動的に vRealize Network Insight に追加できます。

前提条件

- AWS API アクセス用のファイアウォールの構成。
- プライマリおよびリンクされたアカウント ポリシーの作成。
- AWS でのロールの作成。
- プライマリ AWS アカウントでのユーザーの作成。
- AWS コンソールで作成した Amazon アクセス キー ID を取得します。詳細については、<http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html> を参照してください。
- リンクされた AWS アカウントのロール Amazon リソース ネーム (ARN) を取得します。[Amazon リソース ネーム \(ARN\)](#) と [AWS サービス名前空間](#) を参照してください。

手順

- 1 vRealize Network Insight にログインします。

- 2 [設定] - [アカウントとデータ ソース] - [ソースの追加] の順に移動します。
- 3 [パブリック クラウド] セクションで、[Amazon Web Services] をクリックします。
- 4 コレクタ（プロキシ）仮想マシンを選択します。
- 5 Amazon アクセス キー ID と、それに対応するプライベート アクセス キーを入力します。
vRealize Network Insight では、AWS アカウント データの収集に 15 ～ 20 分かかります。
- 6 [検証] をクリックします。

検出された仮想マシンの数が、プラットフォームまたはコレクタ ノードのいずれかまたは両方のキャパシティを超えている場合、検証は失敗します。プラットフォームのブリック サイズを増やすか、クラスタを作成するまでは、データ ソースを追加することはできません。フローがある場合とない場合の各ブリック サイズの指定されたキャパシティは、次のようになります。

ブリック サイズ	仮想マシン	フローの状態
大	6 k	有効
大	10 k	無効
中	3 k	有効
中	6 k	無効

- 7 AWS アカウントの検証が完了したら、[リンクされたアカウントを自動的に追加] オプションを選択します。
- 8 [ロール ARN] で、プライマリ AWS アカウントを信頼するために、リンクされている AWS アカウントのロール Amazon リソース ネームを入力します。
- 9 データ ソースの [ニックネーム] と [メモ] を入力します。
- 10 [送信] をクリックします。

vRealize Network Insight によってロール ARN が検証され、アカウントが追加されます。

プライマリおよびリンクされたアカウント ポリシーの作成

プライマリ Amazon Web Services (AWS) アカウント用にプライマリ アカウント ポリシーを、リンクされたすべての AWS アカウント用にリンクされたアカウント ポリシーをそれぞれ作成する必要があります。これらのポリシーを使用して、AWS でのアクセスを管理できます。

AWS ポリシーは、ユーザーやロールなどの IAM ID に関連付けることができます。詳細については、[ポリシーとアクセス許可](#)を参照してください。

手順

- 1 AWS コンソールで、[IAM] - [ポリシー] - [ポリシーの作成] の順に移動します。
- 2 [ポリシーの作成] 画面で、[JSON] タブをクリックします。

3 [JSON] テキスト ボックスにポリシーを入力します。

オプション	説明
<p>プライマリ アカウント ポリシーの追加</p> <hr/> <p>注: プライマリ アカウント ポリシーは、プライマリ AWS アカウントに追加する必要があります。</p>	<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": ["ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }, { "Effect": "Allow", "Action": ["organizations:ListAccounts"], "Resource": "*" }, { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<Role ARNs>" }] }</pre>
<p>リンクされたアカウントの追加</p> <hr/> <p>注: リンクされたアカウント ポリシーは、プライマリ AWS アカウントに追加されたすべてのリンクされたアカウントに追加する必要があります。</p>	<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": [</pre>

オプション	説明
	<pre> "ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }] } </pre>

- 4 [ポリシーの確認] をクリックします。
- 5 [ポリシーの確認] セクションで、ポリシー名を入力し、[ポリシーの作成] をクリックします。

次のステップ

すべてのリンクされたアカウントに1つずつログインし、ロールを追加して vRealize Network Insight に追加するプライマリ AWS アカウントを信頼して、リンクされたアカウント ポリシーを適用します。ロールを作成し、リンクされたアカウント ポリシーを関連付けるには、[AWS でのロールの作成](#)を参照してください。

注: すべてのリンク アカウントで作成されたロールがすでに標準のポリシー権限を含んでいて、プライマリ アカウントを信頼している場合は、この手順をスキップします。

AWS でのロールの作成

vRealize Network Insight に追加するアカウントを信頼するために、AWS ロールを作成できます。

前提条件

[プライマリおよびリンクされたアカウント ポリシーの作成](#)で作成したすべてのリンクされたアカウント ポリシーのリストを作成します。

手順

- 1 AWS コンソールで、[サービス] - [IAM] - [ロール] - [ロールの作成] の順に移動します。
- 2 [ロールの作成] 画面で、[別の AWS アカウント] をクリックします。
- 3 [アカウント ID] テキスト ボックスに信頼するプライマリ アカウント ID を入力し、[次: 権限] をクリックします。
- 4 すべてのリンクされたアカウント ポリシーを検索して選択し、[次: タグ] をクリックします。
- 5 [確認] セクションで、[ロール名] を入力し、[ロールの作成] をクリックします。

次のステップ

[プライマリ AWS アカウントでのユーザーの作成](#)。

プライマリ AWS アカウントでのユーザーの作成

vRealize Network Insight にデータ ソースを追加する際に使用する Amazon アクセス キー ID とそれに対応するシークレット アクセス キーを取得するには、AWS アカウントでユーザーを作成する必要があります。

手順

- 1 AWS コンソールにログインします。
- 2 [サービス] - [IAM] - [ユーザー] - [ユーザーの追加] の順に移動します。
- 3 [ユーザーの追加] 画面で、[ユーザー名] を入力し、[プログラムによるアクセス] チェックボックスを選択して、[次の権限] をクリックします。
- 4 [権限の設定] グループで、[直接接続されている既存のポリシー] をクリックし、作成済みのポリシーを検索して選択します。
 - プライマリ AWS アカウントの場合は、プライマリ アカウント ポリシーを選択します。
 - 標準 AWS アカウントの場合は、標準アカウント ポリシーを選択します。
- 5 [次のタグ] - [次: レビュー] の順にクリックします。
- 6 [ユーザーの作成] をクリックします。
- 7 [アクセス キー ID] と [シークレット アクセス キー] をメモします。

次のステップ

- [プライマリ AWS アカウントの追加](#)。
- [標準の AWS データ ソースの追加](#)。

AWS API アクセス用のファイアウォールの構成

コレクタ仮想マシンには、AWS へのアクセスを取得するための URL のリストが必要です。

- AWS は複数のリージョンに展開できます。異なるリージョンに関連付けられた個別の URL があります。リージョンまたはサービスを把握していない場合は、*.amazonaws.com などの URL のワイルドカード エントリを指定します。

注： ワイルドカード エントリは、中国リージョンでは動作しません。

個別の URL にアクセスできるようにする場合、リージョンに基づく 4 つのサービスがあります。

- GovCloud と中国を除くリージョン
 - ec2.<REGION>.amazonaws.com
 - logs.<REGION>.amazonaws.com
 - sts.<REGION>.amazonaws.com
 - iam.amazonaws.com

GovCloud リージョン

- ec2.us-gov-west-1.amazonaws.com

- logs.us-gov-west-1.amazonaws.com
- sts.us-gov-west-1.amazonaws.com
- iam.us-gov.amazonaws.com

中国（北京）リージョン

- ec2.cn-north-1.amazonaws.com.cn
- logs.cn-north-1.amazonaws.com.cn
- sts.cn-north-1.amazonaws.com.cn
- iam.cn-north-1.amazonaws.com.cn

AWS リージョンに基づいて、次のいずれかの値を REGION に使用できます。

[リージョン名]	[リージョン]
米国東部（オハイオ）	us-east-2
米国東部（北バージニア）	us-east-1
米国西部（北カリフォルニア）	us-west-1
米国西部（オレゴン）	us-west-2
アジア太平洋（ムンバイ）	ap-south-1
アジア太平洋（ソウル）	ap-northeast-2
アジア太平洋（シンガポール）	ap-southeast-1
アジア太平洋（シドニー）	ap-southeast-2
アジア太平洋（東京）	ap-northeast-1
カナダ（中部）	ca-central-1
EU（フランクフルト）	eu-central-1
EU（アイルランド）	eu-west-1
EU（ロンドン）	eu-west-2
南米（サンパウロ）	sa-east-1
GovCloud	us-gov-west-1
中国（北京）	cn-north-1

標準の AWS データ ソースの追加

AWS データ ソースを追加するには、次の必要があります。

前提条件

- AWS API アクセス用の組織ファイアウォールを設定します。[AWS API アクセス用のファイアウォールの構成](#)を参照してください。
- vRealize Network Insight に追加する AWS アカウント向けの標準アカウント ポリシーを作成します。ポリシーを作成するには、[標準アカウント ポリシーの作成](#)を参照してください。
- 標準 AWS アカウントでユーザーを作成します。AWS でユーザーを作成するには、[プライマリ AWS アカウントでのユーザーの作成](#)を参照してください。

手順

- 1 [設定] - [アカウントとデータ ソース] - [ソースの追加] の順に移動します。
- 2 [パブリック クラウド] の [Amazon Web Services] をクリックします。
- 3 コレクタ（プロキシ）仮想マシンを選択します。
- 4 Amazon アクセス キー ID と、それに対応するプライベート アクセス キーを入力します。

注： Amazon アクセス キー ID は、対応するプライベート アクセス キーを含む 20 桁の文字列です。詳細については、<http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html> を参照してください。

注： AWS GovCloud リージョンをデータ ソースとして追加するには、GovCloud リージョンへのアクセス権限を持つ AWS アカウントの推奨ポリシーを使用して、AWS IAM ユーザーを作成します。新しく作成したアカウントのアクセス キーとプライベート キーを使用して、データ ソースを vRealize Network Insight に追加します。

このプロセスは、アカウント データの追加と表示に 15~20 分かかります。

- 5 [検証] をクリックします。

検出された仮想マシンの数がプラットフォームまたはプロキシ ノードの少なくともいずれかの容量を超えていると、検証は失敗します。プラットフォームのブリック サイズを増やすか、クラスタを作成するまでは、データ ソースを追加することはできません。

フローがある場合とない場合の各ブリック サイズの指定されたキャパシティは、次のようになります。

ブリック サイズ	仮想マシン	フローの状態
大	6 k	有効
大	10 k	無効
中	3 k	有効
中	6 k	無効

- 6 AWS アカウントを検証したら、[フロー データ収集の有効化] を選択して、より詳細な情報を取得できます。

プライマリ AWS アカウントでのユーザーの作成

vRealize Network Insight にデータ ソースを追加する際に使用する Amazon アクセス キー ID とそれに対応するシークレット アクセス キーを取得するには、AWS アカウントでユーザーを作成する必要があります。

手順

- 1 AWS コンソールにログインします。
- 2 [サービス] - [IAM] - [ユーザー] - [ユーザーの追加] の順に移動します。
- 3 [ユーザーの追加] 画面で、[ユーザー名] を入力し、[プログラムによるアクセス] チェックボックスを選択して、[次の権限] をクリックします。
- 4 [権限の設定] グループで、[直接接続されている既存のポリシー] をクリックし、作成済みのポリシーを検索して選択します。
 - プライマリ AWS アカウントの場合は、プライマリ アカウント ポリシーを選択します。
 - 標準 AWS アカウントの場合は、標準アカウント ポリシーを選択します。
- 5 [次のタグ] - [次: レビュー] の順にクリックします。
- 6 [ユーザーの作成] をクリックします。
- 7 [アクセス キー ID] と [シークレット アクセス キー] をメモします。

次のステップ

- [プライマリ AWS アカウントの追加](#)。
- [標準の AWS データ ソースの追加](#)。

標準アカウント ポリシーの作成

標準 AWS アカウントに適用される標準アカウント ポリシーを作成する必要があります。このポリシーを使用して AWS でのアクセスを管理できます。

AWS ポリシーは、ユーザーやロールなどの IAM ID に関連付けることができます。詳細については、[ポリシーとアクセス許可](#)を参照してください。

手順

- 1 AWS コンソールで、[IAM] - [ポリシー] - [ポリシーの作成] の順に移動します。
- 2 [ポリシーの作成] 画面で、[JSON] タブをクリックします。

3 [JSON] テキスト ボックスに、次のアカウント ポリシーを入力します。

オプション	説明
<p>標準アカウント ポリシーを追加する方法</p> <hr/> <p>注： データ ソースとして追加する標準 AWS アカウントに標準アカウント ポリシーを追加する必要があります。</p>	<pre data-bbox="638 294 1412 1134"> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": ["ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }] }</pre>

4 [ポリシーの確認] をクリックします。

5 [ポリシーの確認] セクションで、ポリシー名を入力し、[ポリシーの作成] をクリックします。

次のステップ

- [プライマリ AWS アカウントでのユーザーの作成。](#)

AWS：地理的ブロッキングのサポート

企業のファイアウォールでは地理的ブロッキング ポリシーが厳密に実装されているため、AWS API の呼び出しは特定の AWS 領域に制限されます。vRealize Network Insight は、AWS 環境の地理的ブロッキング ポリシーをサポートします。

vRealize Network Insight で地理的ブロッキング ポリシーを有効にするには、次のように行います。

手順

- 1 [AWS データ ソースの追加] 画面で、AWS アクセス キーとプライベート キーを入力します。[検証] をクリックします。

- 2 [特定の AWS 領域へのアクセスのみを許可] を選択します。[AWS 領域] をリストから選択して、領域からの自動収集を有効にします。このオプションが選択されていない場合、自動収集は行われません。
- 3 [送信] をクリックします。

Azure サブスクリプションの追加

Microsoft Azure サブスクリプションを vRealize Network Insight のデータ ソースとして追加することができます。

次の権限が必要です。

- Microsoft.Resources/subscriptions/read
- Microsoft.Compute/virtualMachines/read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/applicationSecurityGroups/read
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Network/networkWatchers/queryFlowLogStatus/*
- Microsoft.Network/networkWatchers/read
- Microsoft.Network/publicIPAddresses/read

または、利便性を考慮して、ストレージ アカウント キー オペレーターのサービス ロール、ネットワーク共同作成者、および閲覧者権限も追加できます。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [パブリック クラウド] グループで、[Microsoft Azure] をクリックします。
- 4 [新しい Azure サブスクリプションの追加] 画面で必要な情報を入力します。

オプション	アクション
コレクタ仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
テナント ID	Azure Active Directory (AD) のテナント ID を入力します。
アプリケーション ID	アプリケーション ID を入力します。

オプション	アクション
アプリケーションのシークレット キー	アプリケーションのシークレット キーを入力します。
サブスクリプション ID	サブスクリプション ID を入力します。

- 5 [検証] をクリックします。

検証が成功するには、1 台以上の仮想マシン、ネットワーク セキュリティ グループ (NSG)、NIC、および VNET が必要です。

- 6 (オプション) NSG フロー ログを収集して、フローに関する詳細情報を取得する場合は、[NSG フロー データ 収集を有効にする] チェック ボックスを選択します。
- 7 [ニックネーム] テキスト ボックスにニックネームを入力します。
- 8 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 9 [送信] をクリックします。

NSG フロー ログの有効化

vRealize Network Insight でネットワーク セキュリティ グループ (NSG) のフロー データの収集を有効にするには、Azure 環境で NSG フロー ログを有効にする必要があります。

Azure に関連する手順とタスクは、<https://docs.microsoft.com/en-us/azure/network-watcher/>に記載されています。

前提条件

適切な権限があることを確認します。権限については、[サポート対象の製品とバージョン](#)を参照してください。

手順

- 1 Azure 環境で Network Watcher を有効にします。詳細については、Azure の「Network Watcher Documentation」の「Log VM network traffic」でチュートリアルを参照してください。
- 2 Azure 環境に vRealize Network Insights プロバイダを登録します。詳細については、Azure の「Network Watcher Documentation」の「Log VM network traffic」でチュートリアルを参照してください。
- 3 Azure 環境で NSG フロー ログを有効にします。詳細については、Azure の「Network Watcher Documentation」の「Log VM network traffic」でチュートリアルを参照してください。
- 4 [Microsoft Azure] ポータルで [ストレージ アカウント] - [Blob] の順に選択します。
- 5 フロー ログを保存するコンテナを選択し、[アクセス レベルの変更] をクリックして、[Container (anonymous read access for container and blobs)] を選択します。

この手順は、フロー ログを格納しているすべてのコンテナに対して実行する必要があります。

VMware PKS の追加

VMware PKS をデータ ソースとして追加して、PKS クラスタの詳細を vRealize Network Insight に取り込むことができます。

前提条件

対応する NSX-T Manager を追加する必要があります。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [コンテナ] で、[VMware PKS] を選択します。
- 4 [データ ソースの追加] 画面で、以下の詳細を指定します。

フィールド名	説明
NSX-T Manager	VMware PKS の展開の基盤となるネットワークをサポートする NSX-T Manager を選択します。
コレクタ (プロキシ) 仮想マシン	<p>選択した NSX-T Manager に関連付けられている、対応するコレクタ仮想マシンが、vRealize Network Insight によって自動的に選択されます。</p> <p>注： NetFlow コレクタとして追加されたコレクタ仮想マシンは、リストには表示されません。</p>
API ホスト名 (FQDN)	PKS API サーバの FQDN の詳細を入力します。
ユーザー名	<p>クラスタにアクセスできる PKS ユーザーの名前を入力します。</p> <p>注： ユーザーには <code>pks.clusters.admin</code> 権限が必要です。</p>
パスワード	<p>パスワードを入力します。</p> <p>注： 現在、<code>&</code>、<code>(</code>、<code>)</code>、<code> </code>、<code><</code>、<code>></code>、<code>`</code> などの特殊文字を含むパスワードはサポートされていません。</p>

- 5 [検証] をクリックします。
検証が成功しました というメッセージが表示されます。
- 6 必要に応じて、データ ソースのニックネームを入力し、説明のメモを追加します。
- 7 [送信] をクリックします。

「コレクタ仮想マシンから 1 つ以上の Kubernetes クラスタ マスター ホストにアクセスできません」というエラー メッセージが表示された場合は、コレクタ仮想マシンで次のコマンドを実行します。

a `pks login -a PKS_API_Server - u username -p password -k`

b `pks clusters`

クラスタの状態が 成功 になっていることを確認します。

c `pks cluster Kubernetes_Cluster_Name`

d `telnet Kubernetes_Master_Host Kubernetes_Master_port`

マスター ホストが接続可能であることを確認します。

e step b で検出された各 Kubernetes クラスタに対して、step c と step d を繰り返します。

Kubernetes の追加

Kubernetes をデータ ソースとして追加して、Kubernetes の詳細を vRealize Network Insight に取り込むことができます。

注： Kubernetes クラスタとそれに対応する NSX-T Manager は、同じコレクタ仮想マシンに追加する必要があります。

前提条件

- vRealize Network Insight に NSX-T Manager を追加します。
- Kubernetes API サーバがコレクタ仮想マシンからアクセスできることを確認します。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [コンテナ] で [Kubernetes] を選択します。
- 4 [データ ソースの追加] 画面で、以下の詳細を指定します。

フィールド名	説明
NSX-T Manager	Kubernetes の基盤となるネットワークをサポートする NSX-T Manager を選択します。
コレクタ (プロキシ) 仮想マシン	選択した NSX-T Manager に関連付けられている、対応するコレクタ仮想マシンが、vRealize Network Insight によって自動的に選択されます。 注： NetFlow コレクタとして追加されたコレクタ仮想マシンは、リストには表示されません。
Kubeconfig	[参照] をクリックし、Kubernetes クラスタの詳細を含む Kubernetes 構成ファイルをアップロードします。Kubeconfig 構成ファイルの形式の詳細については、 Kubernetes のドキュメント を参照してください。 注： Kubeconfig ファイルで設定されたユーザーには、一覧表示 と 監視 の権限が必要です。

- 5 [検証] をクリックします。
検証が成功しました というメッセージが表示されます。
- 6 必要に応じて、データ ソースのニックネームを入力し、説明のメモを追加します。
- 7 [送信] をクリックします。

結果

vRealize Network Insight は Kubernetes クラスタの詳細を取得できるようになりました。

次のステップ

Kubernetes ダッシュボードに移動し、詳細を表示するには、[Kubernetes の詳細の表示](#)を参照してください。

OpenShift の追加

OpenShift をデータ ソースとして追加して、OpenShift の詳細を vRealize Network Insight に取り込むことができます。

注： OpenShift とそれに対応する NSX-T Manager は、同じコレクタ仮想マシンに追加する必要があります。

前提条件

- vRealize Network Insight に NSX-T Manager を追加します。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [コンテナ] で [OpenShift] を選択します。
- 4 [データ ソースの追加] 画面で、以下の詳細を指定します。

フィールド名	説明
NSX-T Manager	OpenShift の基盤となるネットワークをサポートする NSX-T Manager を選択します。
コレクタ (プロキシ) 仮想マシン	選択した NSX-T Manager に関連付けられている、対応するコレクタ仮想マシンが、vRealize Network Insight によって自動的に選択されます。 注： NetFlow コレクタとして追加されたコレクタ仮想マシンは、リストには表示されません。
Kubeconfig	[参照] をクリックし、Kubernetes クラスタの詳細を含む Kubernetes 構成ファイルをアップロードします。Kubeconfig 構成ファイルの形式の詳細については、 Kubernetes のドキュメント を参照してください。 注： Kubeconfig ファイルで設定されたユーザーには、一覧表示 と 監視 の権限が必要です。

- 5 [検証] をクリックします。
検証が成功しました というメッセージが表示されます。
- 6 必要に応じて、データ ソースのニックネームを入力し、説明のメモを追加します。
- 7 [送信] をクリックします。

結果

vRealize Network Insight は OpenShift の詳細を取得できるようになりました。

次のステップ

詳細については、[Kubernetes の詳細の表示](#)を参照してください。

Palo Alto Networks Panorama の追加

vRealize Network Insight では、Palo Alto Networks Panorama をデータ ソースとして追加することができます。

前提条件

ユーザーに、XML API アクセス権限を持つ管理者ロールがあることを確認します。詳細については、[Palo Alto Networks](#) を参照してください。

注： vRealize Network Insight は現在、デバイスで直接定義されているローカル Palo Alto Network ポリシーを取得しないため、Panorama には表示されません。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [ファイアウォール] で、[Palo Alto Networks Panorama] をクリックします。
- 4 [新しい Palo Alto Networks Panorama アカウントまたはソースの追加] 画面で、次の必須情報を指定します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。

- 5 [検証] をクリックします。
- 6 [ニックネーム] テキスト ボックスにニックネームを入力します。
- 7 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 8 [送信] をクリックします。

Check Point 管理サーバの追加

vRealize Network Insight は、Check Point Security Manager (SmartCenter) および Check Point Multi-Domain Security (MDS) 管理サーバをサポートしています。

前提条件

適切な権限があることを確認します。権限の詳細については、[Check Point ファイアウォール](#)を参照してください。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [ファイアウォール] グループで、[Check Point 管理サーバ] をクリックします。

- 4 [新しい Check Point 管理サーバ アカウントまたはソースの追加] 画面で、次の必須情報を指定します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。 注: Check Point MDS 管理サーバを追加する場合は、MDS サーバの IP アドレスを指定する必要があります。MDS サーバのドメイン管理サーバの IP アドレスは、個別のデータソースとして追加することはできません。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。

- 5 [検証] をクリックします。
- 6 [ニックネーム] テキスト ボックスにニックネームを入力します。
- 7 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 8 [送信] をクリックします。

Cisco ASA の追加

vRealize Network Insight では、Cisco ASA をデータ ソースとして追加できます。

前提条件

有効化モードでの切り替え権限が必要です。ユーザーのパスワードは、Cisco ASA の有効化モードで使用されるものと同じである必要があります。

手順

- [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- [ソースの追加] をクリックします。
- [ファイアウォール] グループで [Cisco ASA] をクリックします。
- [新しい Cisco ASA アカウントまたはソースの追加] 画面で、次の情報を指定します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
ユーザー名	ユーザー名を入力します。 注: ユーザーは、ターミナルの長さを 0 に設定し、セキュリティ コンテキストを切り替えるための有効化モード権限を持っている必要があります。
パスワード	パスワードを入力します。 注: Cisco ASA の有効化モードで使用したパスワードと同じパスワードを確実に入力します。

- 5 (オプション) より高度なデータ収集を有効にするには、[SNMP の使用 (高度なデータ収集に推奨)] チェックボックスをクリックします。
- 6 [検証] をクリックします。
- 7 [ニックネーム] テキスト ボックスにニックネームを入力します。
- 8 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 9 [送信] をクリックします。

Fortinet FortiManager の追加

vRealize Network Insight では、Fortinet FortiManager をデータ ソースとして追加できます：

前提条件

以下を確認します。

- FortiManager バージョン 6.0.1 を使用している。
- すべての ADOM およびポリシー パッケージにアクセスできる 制限ユーザー 以上のロールを持っている。
- コマンド ライン インターフェイス (CLI) から rpc-permit read-write アクセスを有効にしてある。

rpc 権限を設定するには、FortiManager の CLI で次のコマンドを使用します。

```
config system admin user
edit "<administrator name>"
set rpc-permit [none | read | read-write ]
end
```

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] - [ソースの追加] の順にクリックします。
- 2 [ファイアウォール] セクションで、[Fortinet FortiManager] をクリックします。
- 3 [新しい Fortinet FortiManager アカウントまたはソースの追加] 画面で、以下の必須情報を入力します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	コレクタ仮想マシンをドロップダウン メニューから選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
ユーザー名	このデータ ソースに使用するユーザー名を入力します。
パスワード	パスワードを入力します。

- 4 [検証] をクリックします。
- 5 [ニックネーム] テキスト ボックスに、データ ソースのニックネームを入力します。
- 6 (オプション) 必要に応じて [注] テキスト ボックスにメモを追加できます。
- 7 [送信] をクリックします。

Arista スイッチ SSH の追加

vRealize Network Insight では、Arista スイッチ SSH をデータ ソースとして追加できます。

前提条件

以下の権限があることを確認します。

- 読み取り専用ユーザー。
- 読み取り専用 SNMP ユーザー。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [ルーターとスイッチ] で、[Arista スイッチ SSH] をクリックします。
- 4 [新しい Arista スイッチ SSH アカウントまたはソースの追加] 画面で、次の情報を指定します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。 注: このスイッチを構成するには、VMware NSX Manager で使用したのと同じ IP アドレス/FQDN を入力する必要があります。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。

- 5 [検証] をクリックします。
- 6 (オプション) より高度なデータ収集を有効にするには、[SNMP の使用 (高度なデータ収集に推奨)] チェックボックスをクリックします。
- 7 [ニックネーム] テキスト ボックスにニックネームを入力します。
- 8 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 9 [送信] をクリックします。

Dell OS10 スイッチの追加

vRealize Network Insight に Dell OS10 をデータ ソースとして追加できます。

前提条件

サポート対象の Dell スイッチの詳細については、「[サポート対象の製品とバージョン](#)」を参照してください。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。

- 2 [ソースの追加] をクリックします。
- 3 [ルーターおよびスイッチ] グループで、[Dell OS10] をクリックします。
- 4 [新しいアカウントまたはソースの追加] 画面で、次の必須情報を指定します。

オプション	アクション
コレクタ仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。

- 5 [検証] をクリックします。
検証が成功しました というメッセージが表示されます。
- 6 SNMP またはデータ収集を有効にするには、[SNMP を使用] を選択します。
- 7 [ニックネーム] テキスト ボックスにニックネームを入力します。
- 8 [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 9 [送信] をクリックします。

次のステップ

[Dell OS10 スイッチでのテレメトリの有効化](#)

Dell OS10 スイッチでのテレメトリの有効化

Dell OS10 スイッチでテレメトリを有効にすると、Dell スイッチでバッファ統計情報とトラッキングを統合することができます。

前提条件

[Dell OS10 スイッチの追加](#)

スイッチから要求を受信すると、vRealize Network Insight コレクタは定義されたポート上でパケットを保存するか、バッファリングします。

出力速度と比較して入力速度が大きいためバッファ サイズが増加している場合は、要求の速度が低下するか、タイムアウトになることがあります。Dell OS10 スイッチは、gRPC を使用してこのようなメトリック情報を取得します。この情報は vRealize Network Insight で確認できます。これにより、ネットワークの輻輳が原因で発生した可能性があるアプリケーションのパフォーマンスの問題を診断できるようになり、輻輳がアプリケーションとネットワークに与える影響もプロアクティブに確認できます。

手順

- ◆ Dell OS10 スイッチで次のコマンドを実行します。

```
telemetry
enable
!
```

```

destination-group dg03
  destination vRNI Collector IP 50000
!
subscription-profile sp03
  sensor-group bgp
  sensor-group buffer
  sensor-group device
  sensor-group environment
  sensor-group interface
  sensor-group lag
  sensor-group system
  destination-group dg03
  encoding gpb
  transport grpc no-tls
  source-interface ethernet1/1/1

```

結果

vRealize Network Insight コレクタは、Dell OS10 スイッチから次のテレメトリ情報を収集します。

- per-port egress unicast queues
- per-port egress multicast queues
- per-port egress service pool
- per priority group ingress shared headroom
- per service pool ingress

次のステップ

次のいずれかのクエリを実行します。

- `show ports where metric > X in time range`
- `show switches where metric > X in time range`
- `port show metrics in time range`
- `swicth show metrics in time range`
- `show switches where at least one port metric > X in time range`

それぞれのイベントがトリガされます。例：SwitchPort Buffer Threshold Exceeded Event。

また、Interface Peak Buffer Utilization メトリックを検索して、要求速度が低下した理由を特定することもできます。

Huawei 6800/7800/8800 シリーズの追加

vRealize Network Insight は複数の Huawei Cloud Engine シリーズをサポートしています。

前提条件

ユーザーは、少なくとも読み取り権限が必要です。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [ルーターおよびスイッチ] で、[Huawei 6800/7800/8800 シリーズ] を選択します。
- 4 次の情報を入力します。

プロパティ	説明
コレクタ (プロキシ) 仮想マシン	プロキシ仮想マシンをドロップダウン メニューから選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
Username	このデータ ソースに使用するユーザー名を入力します。
Password	パスワードを入力します。

- 5 [検証] をクリックします。
- 6 データ収集のために SNMP を有効にする場合は、[SNMP バージョン] を選択します。
 - a [2c] の場合は、関連するコミュニティ文字列を入力します。
 - b [3] の場合は、次のように入力します。
 - Username
 - Context Name
 - Authentication Type
- 7 必要に応じて、[ニックネーム] と [メモ] を指定します。
- 8 [送信] をクリックします。

次のステップ

Huawei デバイスまたはルーターでは、vRealize Network Insight の次の機能を使用できます。

- 仮想マシン間パス
- 仮想マシン アンダーレイ トポロジ
- Huawei ルーターまたはスイッチ ダッシュボード
- メトリック：スイッチ ポートおよびルーター インターフェイス メトリック
- ダッシュボード
 - Huawei ルーターまたはスイッチ
 - ルーター インターフェイス
 - ポート チャンネル
 - スイッチ ポート

- ルート
- 高可用性：M-LAG（マルチシャーシ リンク集約）と VRRP（仮想ルーター冗長プロトコル）をサポート
- 検索
 - Huawei の VRF（仮想ルーティングおよび転送）
 - Huawei のルーター インターフェイス
 - Huawei のスイッチ ポート
 - Huawei のポート チャンネル
 - Huawei 内のルート
- Huawei NetStream データの監視

Cisco ACI の追加

Cisco ACI をデータ ソースとして追加できます。この機能は、Enterprise ライセンス ユーザーのみが使用できません。

前提条件

- HTTPS 経由の APIC コントローラ REST API に接続するために、すべてのテナントへのアクセス権と、読み取り専用権限が必要です。
- SNMP の場合、読み取り専用権限が必要です。
- 次の権限を持つローカル ユーザー ロールがあることを確認します。
 - セキュリティ ドメイン：すべて
 - ロール：管理者
 - アクセス：読み取り

Cisco ACI でのローカル ユーザーの作成方法については、『Cisco APIC Security Configuration Guide』の「Access, Authentication, and Accounting」セクションを参照してください。

手順

- 1 [設定] の [アカウントとデータ ソース] 画面で、[ソースの追加] をクリックします。
- 2 [その他] で、[Cisco ACI] をクリックします。
- 3 [新しい Cisco ACI アカウントまたはソースの追加] 画面で、必要な情報を指定します。

オプション	アクション
コレクタ (プロキシ) 仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。

オプション	アクション
ユーザー名	ユーザー名を入力します。 注： ユーザーがドメイン ユーザーの場合は、ユーザー名の前に apic: を追加する必要があります。たとえば、ユーザー名が user1 で、ユーザーがドメイン domain1 に属している場合は、ユーザー名を apic:domain1\user1 のように指定します。ドメイン名では大文字と小文字が区別されます。
パスワード	パスワードを入力します。

- コレクタ仮想マシンを選択します。
- クラスタ内の APIC コントローラの IP アドレスを指定します。

注： ACI ファブリックの個別のスイッチを追加する必要はありません。

- ユーザー認証情報を指定します。
- vRealize Network Insight は、個別のスイッチから SNMP を介してメトリック データを収集します。このタスクを有効にするには、[SNMP を使用] を選択します。

4 [検証] をクリックします。

5 データ ソースの [ニックネーム] と [メモ] (ある場合) を入力し、[送信] をクリックします。

NetFlow および sFlow 用の物理フロー コレクタの追加

物理フロー コレクタを追加し、sFlow および NetFlow レコードをコレクタにプッシュするようにスイッチを設定することができます。NetFlow または sFlow に使用されるコレクタ仮想マシンは、専用のコレクタです。他のデータ ソースに使用することはできません。他のデータ ソースをさらにプロキシ サーバに追加しても、sFlow と NetFlow の物理フロー コレクタとしては使用できません。

手順

- 1 [設定] 画面の [アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [フロー] で、[物理フロー コレクタ (Netflow、sFlow)] をクリックします。
sFlow は、物理コレクタでのみ受け入れられます。
- 4 必要に応じて、[ニックネーム] と [メモ] を入力します。
- 5 [送信] をクリックします。

結果

注： vRealize Network Insight は sFlow のバケット サンプルを収集するため、フローの完全なメトリックは表示できません。

次のステップ

フローを物理フロー コレクタにプッシュするようにスイッチを設定します。

- 宛先（vRealize Network Insight で追加したコレクタ IP アドレス）を定義します。
- フロー コレクタのポートを設定します。
- ポーリング間隔を割り当てます。

注： 設定手順は、設定するスイッチによって異なります。詳細については、実際のスイッチのドキュメントを参照してください。

vRealize Log Insight の追加

vRealize Log Insight は、NSX イベントが発生したときに NSX ログを動的に収集します。ただし、vRealize Network Insight は、NSX から 10 分ごとにデータを収集します。したがって、vRealize Network Insight に vRealize Log Insight を追加すると、イベント情報を待機せずに迅速にイベント情報を取得できるようになります。

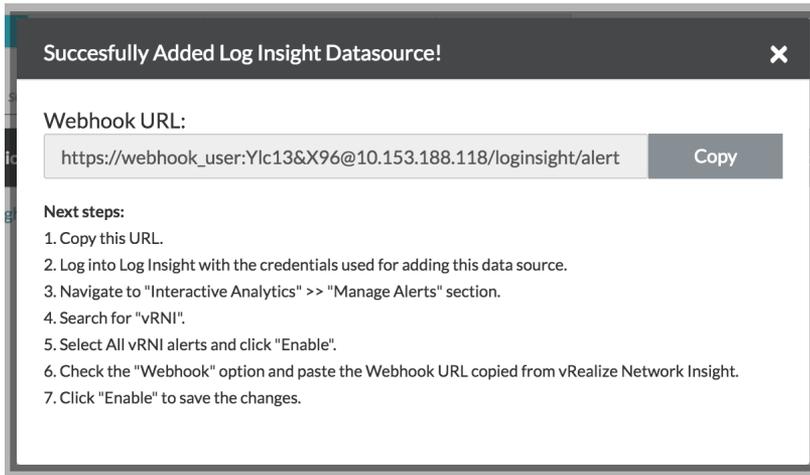
vRealize Network Insight と vRealize Log Insight の統合環境では、vRealize Log Insight によって生成されるアラートが vRealize Network Insight で使用されます。セキュリティ グループが作成または変更されるたびに、NSX のログが vRealize Log Insight に送信され、対応したアラートが送信されます。アラートを受信した vRealize Network Insight は、セキュリティ グループが作成された NSX Manager をポーリングし、変更されたセキュリティ グループについて対応するデータを取得します。現在この統合では、セキュリティ グループの CRUD 関連アラートのみがサポートされます。

vRealize Network Insight でサポートされている vRealize Log Insight のバージョンのリストについては、[VMware 製品の相互運用性マトリックス](#)を参照してください。

手順

- 1 vRealize Log Insight の API へのアクセス権を持つ vRealize Log Insight ユーザーを作成するか、再利用します。
- 2 [インストールとサポート] 画面で、[アカウントとデータ ソース] をクリックします。
- 3 [ソースの追加] をクリックします。
- 4 [ログ サーバ] の下の [Log Insight] をクリックします。

- 5 [新しい Log Insight サーバのアカウントまたはソースを追加] 画面で、画面タイトルの横にある [手順] をクリックします。ポップアップ ウィンドウに、vRealize Log Insight データ ソースを追加する際の前提条件と、vRealize Log Insight で Webhook URL を有効にする手順が表示されます。

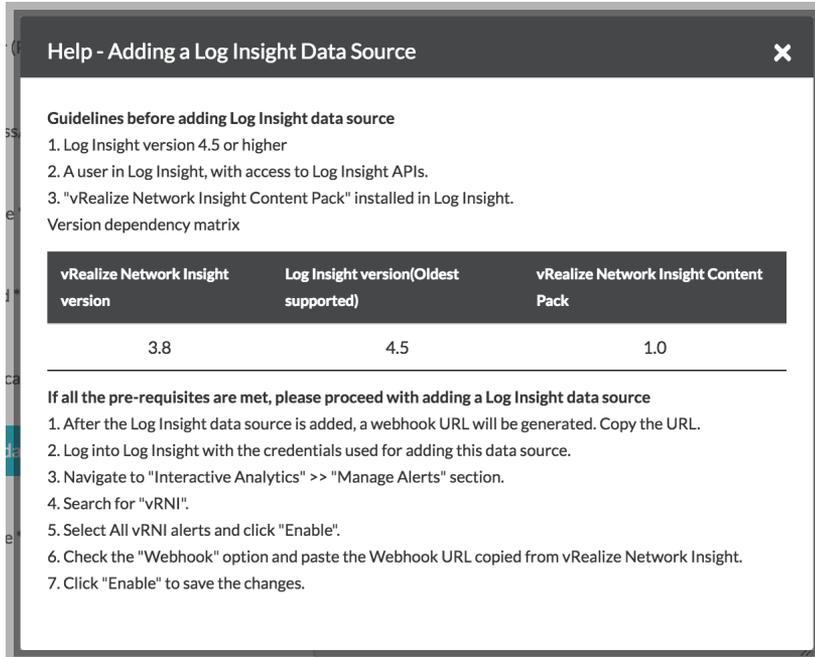


注： データ ソースの追加後に生成される Webhook URL は vRealize Log Insight で使用されます。

- 6 必要な詳細情報を入力します。

名前	説明
コレクタ (プロキシ) 仮想マシン	データ収集プロセス用に展開したデータ コレクタの IP アドレスを選択します。
IP アドレス/FQDN	データ ソースの IP アドレスまたは FQDN を入力します。
ユーザー名	特定のデータ ソースに使用するユーザー名を入力します。
パスワード	データ ソースのパスワードを入力します。
認証プロバイダ	指定した認証情報に対応する認証プロバイダを選択します。

- 7 データソースが作成されると、ポップアップウィンドウに、Webhook URL と、この URL を vRealize Log Insight で有効にするために実行する必要がある手順が表示されます。Webhook URL をコピーします。このデータソースの追加に使用された認証情報を使用してログインします。vRealize Log Insight アプリケーションでアラートを有効にし、この Webhook URL を設定します。テストアラートを送信して、統合が成功したことを確認します。



注： vRealize Network Insight の vRealize Log Insight データソースに表示されるアラートは、1時間で解決されます。

Infoblox の追加

vRealize Network Insight では、Infoblox Grid を DNS データ プロバイダとして追加できます。

Infoblox DNS は、DNS を管理および制御するための高度なソリューションを提供します。また、Infoblox Grid を使用して、ネットワーク全体にわたり可用性の高い DNS を実現します。Infoblox からの DNS データは、ソースまたはターゲットの IP アドレスが物理デバイスに関連付けられている場合に、フローを強化する目的でのみ使用されます。

Infoblox の DNS データは、CSV を使用してインポートされた DNS データと共存します。

コレクタで Infoblox の DNS データソースを設定する場合は、同じコレクタ上にある他のデータソースも設定できます。Infoblox 専用のコレクタは必要ありません。

[考慮事項]

- vRealize Network Insight の最新リリースでは、Infoblox に対してシングルグリッドモードのみをサポートします。
- 最新リリースでは、A レコードのみがサポートされています。共有 A レコードは現在サポートされていません。
- DNS の強化は、現在のリリースで物理としてマークされている IP アドレスに対してのみサポートされます。

- 単一の物理 IP アドレスに対して複数の FQDN がある場合は、すべての FQDN が返されます。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [新しいソースの追加] をクリックします。
- 3 [DNS] の下の [Infoblox] をクリックします。
- 4 次の情報を入力します。

表 3-5.

プロパティ	説明
Collector VM	コレクタ仮想マシンをドロップダウン メニューから選択します。
IP Address/FQDN	Infoblox Grid の IP アドレス/FQDN を入力します。
Username	特定のデータ ソースに使用するユーザー名を入力します。
Password	パスワードを入力します。

- 5 [検証] をクリックします。

注： Infoblox API にアクセスするための API Privilege があることを確認します。

- 6 データ ソースの [ニックネーム] と [メモ] (ある場合) を入力し、[送信] をクリックして、Infoblox の DNS データ ソースを環境に追加します。

F5 BIG-IP の追加

vRealize Network Insight では、F5 BIG-IP のルーターおよびロード バランサの機能がサポートされます。仮想マシン間パス、高可用性、VRF、ルート、ルーター インターフェイス、スイッチ ポート、ポート チャネル、スイッチ ポート メトリック、VRF ダッシュボード、スイッチ ダッシュボード、ルーター ダッシュボードなどの機能をサポートします。F5 BIG-IP エンティティを検索する場合は、クエリ文字列 F5 BIG-IP Data Source を使用します。vRealize Network Insight は、仮想マシン間パスの LLDP ネイバーまたは隣接デバイスをサポートしません。F5 BIG-IP をデータ ソースとして追加するには、次の手順を実行します。

前提条件

- ユーザーには次のものがが必要です。
 - Guest ロール、またはすべてのパーティションに対する読み取り専用権限。
 - REST API へのアクセス。
 - TMSH ターミナル アクセスへのアクセス。
- デバイスで SSH を有効にします。

SSH の password authentication を次のように有効にします。

注：

- SSHD 構成を変更するには、root または管理者ロールの権限を使用します。
- vRealize Network Insight で F5 BIG-IP データ ソースを追加するときは、root ユーザー権限を使用しないでください。
- root ユーザーには HTTP アクセス権はありません。root ユーザー権限は、管理目的で使用されます。

```
[root@bigip:Active] config # tmsh
root@bigip(Active) (/Common) (tmos) # edit sys sshd

## Adding the following configuration ##

modify sshd {
    include "
    ChallengeResponseAuthentication no
    PasswordAuthentication yes"
}
#####
Save changes? (y/n/e) y
root@bigip(Active) (/Common) (tmos) #
root@bigip(Active) (/Common) (tmos) # save sys config

root@bigip(Active) (/Common) (tmos) # show running-config sys sshd
sys sshd {
    include "
    ChallengeResponseAuthentication no
    PasswordAuthentication yes"
}
```

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [ルーターおよびスイッチ] で [F5 BIG-IP] を選択します。
- 4 次の情報を入力します。

プロパティ	説明
コレクタ (プロキシ) 仮想マシン	プロキシ仮想マシンをドロップダウン メニューから選択します。
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
Username	このデータ ソースに使用するユーザー名を入力します。
Password	パスワードを入力します。

- 5 テキスト ボックスに情報を入力したら、[検証] をクリックします。

6 データ収集のために SNMP を有効にする場合は、[SNMP バージョン] を選択します。

- a 2c を選択した場合は、関連するコミュニティ文字列を入力します。
- b 3 を選択した場合は、次のように入力します。
 - Username
 - Context Name
 - Authentication Type

注： F5 BIG-IP ユーザー インターフェイス コンソールで SNMP を設定してあることを確認します。

- a F5 にログインします。
 - b [システム] - [SNMP] の順に移動します。
 - c [SNMP] - [エージェント] - [アクセス (v1、v2c)] の順に移動します。
 - d コミュニティの文字列を入力します。
 - e 送信元 IP アドレスを入力します。
 - f 読み取り専用 アクセスを選択します。
 - g [終了] をクリックします。
-

7 必要に応じて、[ニックネーム] と [メモ] を指定します。[送信] をクリックします。

ServiceNow の追加

ServiceNow 構成管理データベース (CMDB) は、ソフトウェアおよびハードウェア インフラストラクチャに関する情報や、データセンター内のアイテム間の関係に関する詳細なデータを提供するもので、インベントリの管理に有用です。ServiceNow 統合を使用すると、vRealize Network Insight によって ServiceNow CMDB で使用可能なアプリケーションが検出され、直接 vRealize Network Insight に追加することができます。

CMDB の概念

基本的に、CMDB の構成は次のとおりです。

- 構成アイテム：システム内のエンティティまたはコンポーネント。例：コンピュータ、スイッチ、サービス、アプリケーション、サーバ、仮想マシンなど。
- 関係：構成アイテム間のリンクまたは通信のタイプ。例：依存先、実行先、データの交換など。

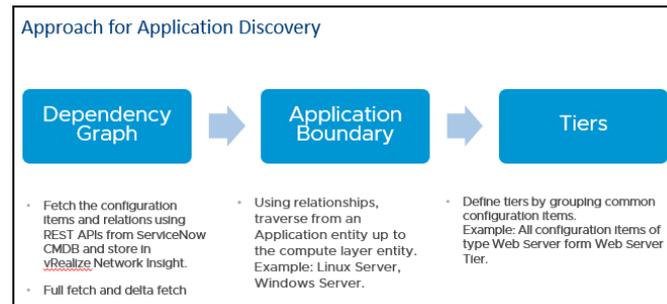
各構成アイテムには定義済みのスキーマがあります。

- 構成アイテム クラス：各構成アイテムは、そのプロパティを定義するクラスに関連付けられている必要があります。
- 関係クラス：構成アイテム間の関係のタイプを定義します。

両方のクラスを拡張して、プロパティを追加したり、プロパティをカスタマイズしたりすることができます。

ServiceNow は、アプリケーション サービスをサポートします。アプリケーション サービスとは、アプリケーションとホストが相互接続され、セットとしてサービスを提供するものをいいます。ServiceNow では、アプリケーション サービスを API を使用して手動で作成したり、サービス マッピングによって自動的に検出したりすることができます。これらのアプリケーションはすべて、ServiceNow CMDB に保存されます。

ServiceNow データソースを vRealize Network Insight に追加すると、vRealize Network Insight により ServiceNow CMDB 構成ファイルから構成アイテムと関係がフェッチされます。



デフォルトで vRealize Network Insight は一定の間隔でデータをフェッチします。

- 完全なデータのフェッチは 12 時間ごとに行われ、これにより、CMDB 構成で定義されたクラスのすべてのレコードがフェッチされます。また、データソースを追加または更新するときにも完全なフェッチが行われます。
- 差分フェッチは 2 分ごとに実行され、CMDB 構成で定義されているクラスのすべての新しいレコード、変更されたレコードと削除されたレコードがフェッチされます。vRealize Network Insight では、ユーザー インターフェイスにこれらの詳細が反映されるまで、約 12 分かかります。

注： vRealize Network Insight は、完全なフェッチの時点に限り、クラス階層と関係タイプを取得します。

制限のデフォルト値

制限名	説明	デフォルト値	制限を超えた場合の影響
maxAppsPerDataSource	データソース 1 件当たりの最大アプリケーション数。	5,000	データソースがデータのフェッチを停止し、データソースとイベントの画面にエラーが表示されて、アプリケーションが更新されなくなります。
maxTiersPerApp	アプリケーション 1 件あたりの保存できる階層の最大数。	150	階層の数が制限に収まるまで、アプリケーションが更新されなくなります。
maxMembersPerApp	アプリケーション 1 件あたりの保存できるメンバーの最大数。	5,000	メンバーの数が制限に収まるまで、アプリケーションが更新されなくなります。
maxGraphTraversalStackSize	グラフ トラバーサルで使用されるスタックの最大サイズ。	10,000	アプリケーションが作成されなくなり、SizeLimitExceededException をスローします。
maxResponseAppCount	API 応答で返すことのできる最大アプリケーション数。	5,000	制限に適合するアプリケーションの数のみが返され、ユーザー インターフェイスにエラーが表示されます。

ServiceNow の追加

データ ソースとして ServiceNow を vRealize Network Insight に追加して、アプリケーションと階層の詳細を取得できます。

前提条件

データ ソースを追加するには、管理者権限が必要です。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [CMDB] で、[ServiceNow] を選択します。
- 4 [データ ソースの追加] 画面で、以下の詳細を指定します。

フィールド名	説明
コレクタ (プロキシ) 仮想マシン	ServiceNow のホスト URL
IP アドレス/FQDN	IP アドレスまたは FQDN の詳細を入力します。
ユーザー名	このデータ ソースに使用するユーザー名を入力します。 注: 追加する予定のユーザーは、ServiceNow の 管理者 または 読み取り専用管理者 である必要があります。
パスワード	パスワードを入力します。

- 5 [検証] をクリックします。
検証が成功しました というメッセージが表示されます。
- 6 カスタマイズされた CMDB 設定を追加するには、以下の手順を実行します。
 - a [CMDB 設定のカスタマイズ] を選択します。
 - b [ダウンロード] をクリックして、デフォルトの構成ファイルをダウンロードします。
 - c ファイルのプロパティを更新します。[CMDB 構成のカスタマイズ](#)を参照してください。
 - d [データ ソースの追加] 画面で、更新された JSON ファイルを参照して選択します。
- 7 データ ソースのニックネームを入力し、必要に応じて説明のメモを追加します。
- 8 [送信] をクリックします。

次のステップ

ServiceNow データ ソースを追加すると、ServiceNow CMDB で使用可能なアプリケーションが vRealize Network Insight によって検出されるので、これを vRealize Network Insight に追加します。詳細については、[検出されたアプリケーションの追加](#)を参照してください。

デフォルトの CMDB 構成ファイル

vRealize Network Insight は、JSON 形式の構成ファイルを使用して、ServiceNow のカスタマイズをサポートします。

```
{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": false,
  "ignoreWorkloadCheck": false,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_service_discovered"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "relationshipTypeClasses",
      "value": [
        "*"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": false
    },
    {
      "name": "workloadRelationshipTypeClasses",
      "value": [
        "Hosted on::Hosts",
        "Instantiates::Instantiated by",
        "Runs on::Runs",
        "Virtualized by::Virtualizes"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": false
    },
    {
      "name": "workloadCIClasses",
      "value": [
        "cmdb_ci_computer",
        "cmdb_ci_vm_instance",
        "cmdb_ci_vmware_instance"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "relationClasses",
      "value": [
        "cmdb_rel_ci"
      ]
    }
  ]
}
```

```

    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "ignoredCIClasses",
    "value": [
      "cmdb_ci_vcenter_server_obj"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "ignoredTierCIClasses",
    "value": [
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "trackedCIClasses",
    "value": [
      "cmdb_ci_appl",
      "cmdb_ci_cluster",
      "cmdb_ci_cluster_node",
      "cmdb_ci_database",
      "cmdb_ci_lb_service",
      "cmdb_ci_spkg",
      "cmdb_ci_qualifier_manual_connection",
      "cmdb_ci_endpoint",
      "cmdb_ci_network_adapter",
      "cmdb_ci_translation_rule"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  }
],
"traversalRule": [
  {
    "fromNode": [
      "applicationClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  }
],

```

```

{
  "fromNode": [
    "trackedCIClasses",
    "workloadCIClasses"
  ],
  "toNode": [
    "trackedCIClasses",
    "workloadCIClasses"
  ],
  "relationship": [
    "relationshipTypeClasses"
  ],
  "priority": 3
}
],
"traversalStopRule": [
{
  "fromNode": [
    "trackedCIClasses",
    "workloadCIClasses"
  ],
  "toNode": [
    "applicationClasses"
  ],
  "relationship": [
    "relationshipTypeClasses"
  ],
  "priority": 5
}
],
"associationRule": [
{
  "fromNode": [
    "trackedCIClasses",
    "workloadCIClasses"
  ],
  "toNode": [
    "workloadCIClasses"
  ],
  "relationship": [
    "workloadRelationshipTypeClasses"
  ],
  "priority": 5
}
]
}

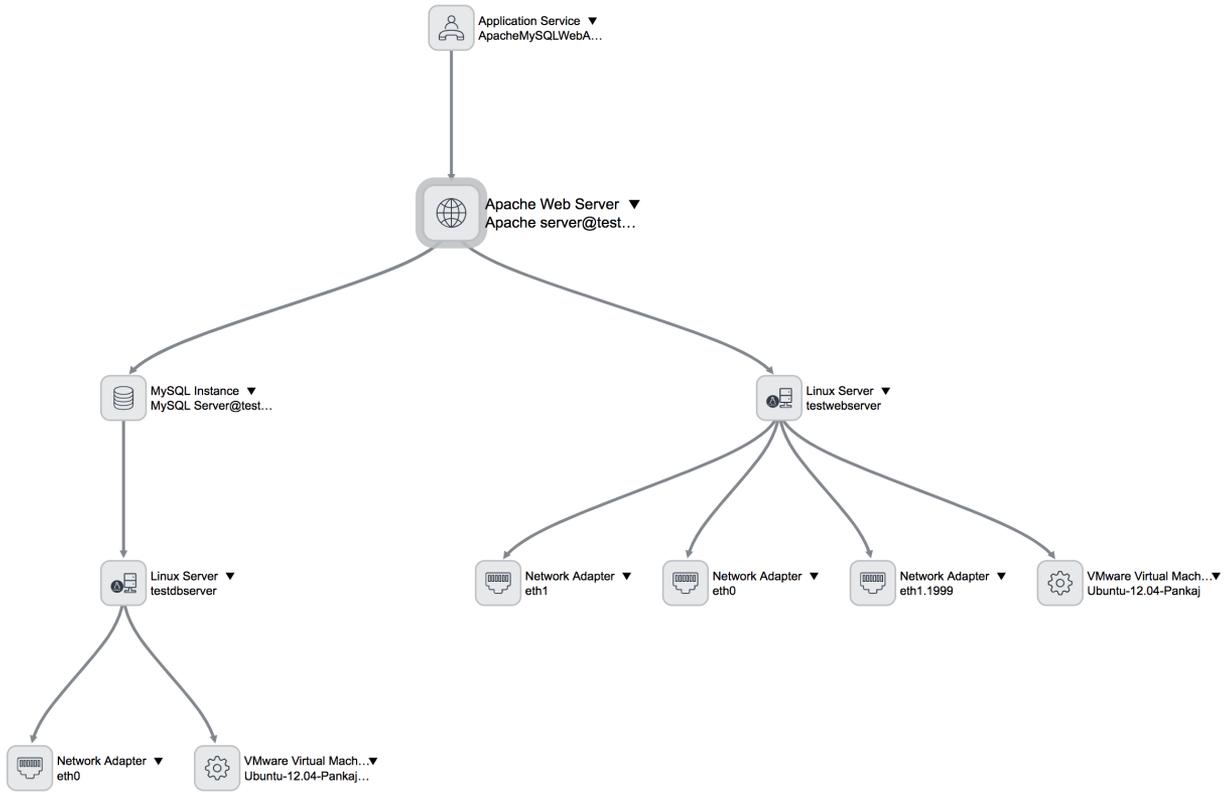
```

vRealize Network Insight 構成の変更が発生すると、すべてのアプリケーションの完全なデータのフェッチと再計算に 30 分かかることがあります。

例：デフォルトの CMDB 構成を使用した、サービスマップおよび検出されたアプリケーションの例

例：アプリケーションの追加用の vRealize Network Insight の更新された画面

これにより、vRealize Network Insight が ServiceNow でアプリケーションを検出できます。



Modify Application



Application Name * ApacheMySQLWebApp Application Total: 2 VMs | 0 Physical IPs

▼ Tier Tier Total: 1 VMs | 0 Physical IPs

Name * ApacheMySQLWebApp_apache_web_server

Virtual Machines / IP Addresses * VM Names ▼ 'Ubuntu-12.04-Pankaj' 1 VMs

[Add another Condition](#)

▼ Tier Tier Total: 1 VMs | 0 Physical IPs

Name * ApacheMySQLWebApp_db_mysql_instance

Virtual Machines / IP Addresses * VM Names ▼ 'Ubuntu-12.04-Dark--Pankaj-1' 1 VMs

[Add another Condition](#)

Add Tier

 Analyze Flows

Save

Cancel

CMDB 構成のカスタマイズ

さまざまなカスタマイズに対応するために、ServiceNow と vRealize Network Insight の統合は一般的な構成をサポートしています。CMDB 構成は JSON 形式である必要があります。

構成には以下の内容が含まれます。

- 構成項目
- 構成項目間の関係
- 依存関係グラフをスキャンするルール

CMDB 構成は、実装に基づいてカスタマイズできます。

注： 構成を変更すると、全体に対してフェッチが実行され、すべてのアプリケーションが再計算されます。そのため、このプロセスによって [検出されたアプリケーション] ダッシュボードにアプリケーションが表示されるまで 30 分以上かかる場合があります。

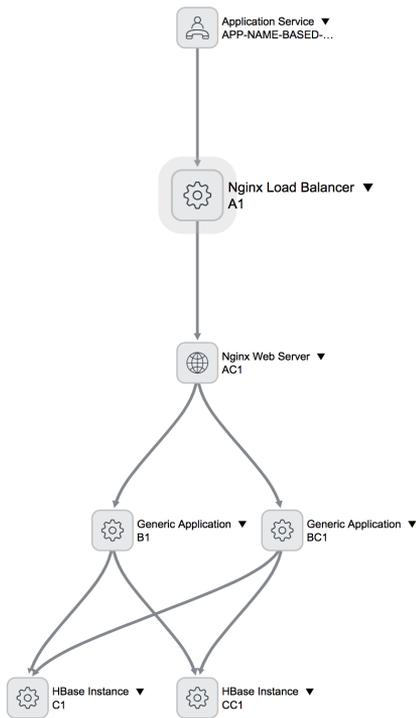
フィールド名	説明
fetchOnlyApprovedApplications	このブール値により、ServiceNow から承認済みアプリケーションのみを取得することができます。デフォルトでは、この値は False に設定されています。
nameBasedSearchForVm	このブール値により、ServiceNow 仮想マシンが vRealize Network Insight 内にない場合に、仮想マシン名を使用してカスタムの仮想マシン検索条件を作成するかどうかを指定できます。値が True に設定されている場合、カスタムの仮想マシン名条件が作成されます。該当する仮想マシンが vRealize Network Insight 内で検出されるとカウント数に反映され、アプリケーションの再計算は行われません。 これは、サービス マッピングを使用せずに、依存関係グラフまたはサービス マップを手動で作成するときに使用できます。デフォルトでは、この値は False に設定されています。
ignoreWorkloadCheck	このブール値により、関連付けられているワークロード エンティティが存在しない場合でも階層にエンティティを追加するかどうかを指定できます。 これは、関係がワークロード レイヤーまで定義されていないときに、サービス マッピングを使用せずに依存関係グラフまたはサービス マップを手動で作成するときに使用できます。デフォルトでは、この値は False に設定されています。
ciGroup	ServiceNow から取得する構成項目と関係を定義します。このフィールドでは、以下のプロパティが許可されます。 <ul style="list-style-type: none"> ■ Name : 構成項目グループの名前 ■ Value : このグループの一部である ServiceNow クラス名のリスト。 ■ ValueType : CI_CLASS (取得するクラスの名前) および CI_VALUE を使用できます。 <ul style="list-style-type: none"> ■ CI_CLASS : クラスを取得します。 ■ CI_VALUE <p>注 : vRealize Network Insight は常に applicationClasses、workloadCIClasses、trackedCIClasses、workloadCIClasses、relationClasses を取得します。</p> ■ systemGenerated : このブール値を使用すると、クラスがユーザー定義クラスであるかデフォルト クラスであるかを示すことができます。 ■ expandCIClass : このブール値フィールドを使用すると、Value に一覧表示されている構成項目クラスのサブクラスを取得するかどうかを指定できます。
Rules for graph traversal	次の 3 種類のスキャン ルールがサポートされます。 <ul style="list-style-type: none"> ■ traversalRule : 許可されている、または有効なすべてのスキャン。 ■ traversalStopRule : 許可されていないスキャン。 <p>注 : traversalStopRule のルールには、traversalRule のルールよりも高い優先順位が設定されます。</p> <ul style="list-style-type: none"> ■ associationRule : エンティティに関連付けられたワークロードに対して許可されているスキャン。 <p>ルールのプロパティは次のとおりです。</p> <ul style="list-style-type: none"> ■ fromNode : スキャン元の ciGroup のリスト。 ■ toNode : スキャン先の ciGroup のリスト。 ■ relationship : あるタイプのスキャンで、関係がある ciGroup のリスト。 ■ priority : ciGroup が 2 つのルールに一致する場合、ciGroup のルールは priority に基づいて設定されます。優先度の値が大きいほど優先度は高くなります。

フィールド名	説明
applicationClasses	<p>グラフ スキャンのすべてのエントリ ポイント構成項目クラスを一覧表示します。これらのクラスは、CMDB でアプリケーション クラスとして使用される構成項目タイプを表します。</p> <p>デフォルトの構成では、cmdb_ci_service_discovered クラスが使用されます。このクラスは、ServiceNow の ServiceMapping 機能によって作成されたアプリケーションを表します。</p>
workloadCIClasses	<p>ソフトウェア ベースのサービス、または Linux サーバ、Windows Server などのオペレーティング システムをホストするすべての構成項目が表示されます。たとえば、仮想マシン、AWS インスタンス、物理サーバです。</p> <p>通常、ワークロード構成項目は依存関係グラフの末尾に配置されます。このグループに記載された構成項目クラスについては、階層が作成されません。</p> <p>デフォルトの構成には、以下の構成項目クラスが含まれています。</p> <ul style="list-style-type: none"> ■ cmdb_ci_computer: コンピューティング関連のすべての構成項目を表します。これは、すべての Linux および Windows Server のスーパー クラスです。 ■ cmdb_ci_vm_instance: 仮想マシンや AWS インスタンスなどの仮想コンピューティング エンティティを表します。 ■ cmdb_ci_vmware_instance: VMware 仮想マシンを表します。
trackedCIClasses	<p>依存関係グラフに含めることができるが applicationClass でも workloadCIClass でもない、すべての構成項目が一覧表示されます。このグループの構成項目は、applicationClasses から workloadCIClasses までのグラフを完成させるために必要です。</p> <p>vRealize Network Insight は、ignoredTierCiClasses に記述されているクラスを除く、trackedCIClasses に記述されているすべてのクラスの階層を作成します。</p>
relationshipTypeClasses	<p>リレーション構成項目のクラスまたは関係タイプで表される、関連するすべての構成項目が一覧表示されます。</p> <p>デフォルトの構成では、* を使用してすべての関係タイプを取得できます。</p>
workloadRelationshipTypeClasses :	<p>関係タイプが一覧表示されます。これは通常、ワークロード エンティティとの関係を表します。ServiceNow でデフォルトでサポートされる関係は次のとおりです。</p> <ul style="list-style-type: none"> ■ Hosted on::Hosts ■ Instantiates::Instantiated by ■ Runs on::Runs ■ Virtualized by::Virtualizes
ignoredCiClasses	<p>ServiceNow CMDB から取得する際に vRealize Network Insight が無視する必要のあるすべての構成項目を一覧表示します。</p> <p>これを使用すると、スーパー クラスを取得するときに不要なサブクラスを無視できます。</p> <p>アプリケーション検出に vCenter Server は不要なので、デフォルトでは cmdb_ci_vcenter_server_obj が ignoredCiClasses の下に一覧表示されます。</p>
ignoredTierCiClasses	<p>階層を作成しないすべての構成項目を一覧表示します。</p>

ワークロードの関係を持たないアプリケーションを検出する例

ここでは、アプリケーションを検出するように nameBasedSearchForVm が定義された、カスタマイズされた CMDB 構成ファイルを示します。cmdb_ci_service_discovered クラスがエントリ ポイントで、ワークロードの関係は定義されていません。

トポロジ



カスタマイズされた CMDB 構成ファイル

```

{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": true,
  "ignoreWorkloadCheck": true,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_service_discovered"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "relationshipTypeClasses",
      "value": [
        "*"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": false
    },
    {
      "name": "workloadRelationshipTypeClasses",
      "value": [

```

```

    "Hosted on::Hosts",
    "Instantiates::Instantiated by",
    "Runs on::Runs",
    "Virtualized by::Virtualizes"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": false
},
{
  "name": "workloadCIClasses",
  "value": [
    "cmdb_ci_computer",
    "cmdb_ci_vm_instance",
    "cmdb_ci_vmware_instance"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "relationClasses",
  "value": [
    "cmdb_rel_ci"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredCIClasses",
  "value": [
    "cmdb_ci_vcenter_server_obj"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredTierCIClasses",
  "value": [
    "cmdb_ci_qualifier_manual_connection",
    "cmdb_ci_endpoint"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "trackedCIClasses",
  "value": [
    "cmdb_ci_appl",
    "cmdb_ci_cluster",
    "cmdb_ci_cluster_node",
    "cmdb_ci_database",

```

```

    "cmdb_ci_lb_service",
    "cmdb_ci_spkg",
    "cmdb_ci_qualifier_manual_connection",
    "cmdb_ci_endpoint",
    "cmdb_ci_network_adapter",
    "cmdb_ci_translation_rule"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
}
],
"traversalRule": [
  {
    "fromNode": [
      "applicationClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  },
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 3
  }
],
"traversalStopRule": [
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "applicationClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  }
]

```

```

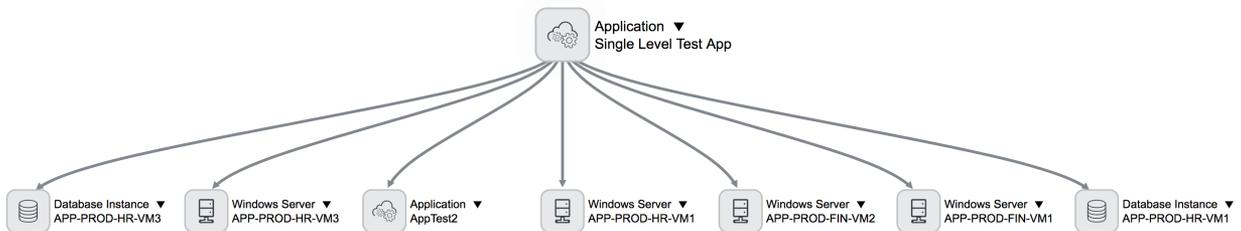
],
"associationRule": [
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "workloadCIClasses"
    ],
    "relationship": [
      "workloadRelationshipTypeClasses"
    ],
    "priority": 5
  }
]
}

```

1つのレベルのアプリケーションを検出する例

ここでは、1つのレベルのアプリケーションを検出するように nameBasedSearchForVm が定義された、カスタマイズされた CMDB 構成ファイルを示します。cmdb_ci_service_discovered クラスがエントリ ポイントで、ワークロードの関係は定義されていません。

トポロジ



カスタマイズされた CMDB 構成ファイル

```

{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": true,
  "ignoreWorkloadCheck": true,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_appl"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": false
    }
  ],
  {
    "name": "relationshipTypeClasses",

```

```

    "value": [
      "*"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": false
  },
  {
    "name": "workloadRelationshipTypeClasses",
    "value": [
      "Hosted on::Hosts",
      "Instantiates::Instantiated by",
      "Runs on::Runs",
      "Virtualized by::Virtualizes"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": false
  },
  {
    "name": "workloadCIClasses",
    "value": [
      "cmdb_ci_computer",
      "cmdb_ci_vm_instance",
      "cmdb_ci_vmware_instance"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "relationClasses",
    "value": [
      "cmdb_rel_ci"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "ignoredCIClasses",
    "value": [
      "cmdb_ci_vcenter_server_obj"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "ignoredTierCIClasses",
    "value": [
      "cmdb_ci_qualifier_manual_connection",
      "cmdb_ci_endpoint"
    ],
    "valueType": "CI_VALUE",

```

```

    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "trackedCIClasses",
    "value": [
      "cmdb_ci_appl",
      "cmdb_ci_cluster",
      "cmdb_ci_cluster_node",
      "cmdb_ci_database",
      "cmdb_ci_lb_service",
      "cmdb_ci_spkg",
      "cmdb_ci_qualifier_manual_connection",
      "cmdb_ci_endpoint",
      "cmdb_ci_network_adapter",
      "cmdb_ci_translation_rule"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  }
],
"traversalRule": [
  {
    "fromNode": [
      "applicationClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  },
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 3
  }
],
"traversalStopRule": [
  {
    "fromNode": [
      "trackedCIClasses",

```

```

        "workloadCIClasses"
    ],
    "toNode": [
        "applicationClasses"
    ],
    "relationship": [
        "relationshipTypeClasses"
    ],
    "priority": 5
    }
],
"associationRule": [
    {
        "fromNode": [
            "trackedCIClasses",
            "workloadCIClasses"
        ],
        "toNode": [
            "workloadCIClasses"
        ],
        "relationship": [
            "workloadRelationshipTypeClasses"
        ],
        "priority": 5
    }
]
}

```

新しい汎用ルーターまたはスイッチの追加

追加するルーターまたはスイッチが vRealize Network Insight でサポートされていない場合は、デバイス構成ファイルをアップロードすることで、そのルーターまたはスイッチを汎用ルーターまたは汎用スイッチとして追加できます。vRealize Network Insight では、デバイス構成ファイルの情報を使用して、ルーターまたはスイッチに関する判断材料を提供します。vRealize Network Insight にデバイス構成ファイルをアップロードした後、アップロードされたデバイス構成ファイルの情報を変更することはできません。

前提条件

デバイス構成ファイルは、vRealize Network Insight で提供されている SDK を使用して .zip 形式で作成します。デバイス構成ファイルには、ルーター インターフェイス、ルート、スイッチ ポート、VRF、スイッチ デバイスなどのエンティティに関する情報が含まれています。デバイス構成ファイルを作成するには、<https://github.com/vmware/network-insight-sdk-generic-datasources> を参照してください。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 [ソースの追加] をクリックします。
- 3 [ルーターおよびスイッチ] の下で、[汎用ルーターおよびスイッチ] をクリックします。

- 4 [新しい汎用ルーターまたはスイッチの追加] 画面で、必要な情報を変更します。

オプション	アクション
[コレクタ仮想マシン]	ドロップダウン メニューからコレクタ仮想マシンを選択します。
[デバイス構成ファイル]	SDK を使用して作成された構成ファイル (.zip) を選択してアップロードします。
[IP アドレス/FQDN]	IP アドレスまたは FQDN の詳細を入力します。

- 5 [検証] をクリックします。
- 6 [ニックネーム] テキスト ボックスに、追加するスイッチまたはルーターのニックネームを入力します。
- 7 (オプション) [ノート] テキスト ボックスには、必要に応じてメモを追加できます。
- 8 [送信] をクリックします。

汎用ルーターまたはスイッチの編集

vRealize Network Insight では、新しい構成ファイルをアップロードして、既存の汎用ルーターまたはスイッチの構成を変更できます。

前提条件

デバイス構成ファイルは、vRealize Network Insight で提供されている SDK を使用して .zip 形式で作成します。デバイス構成ファイルには、ルーター インターフェイス、ルート、スイッチ ポート、VRF、スイッチ デバイス 情報など、エンティティに関する情報が含まれています。デバイス構成ファイルを作成するには、<https://github.com/vmware/network-insight-sdk-generic-datasources> を参照してください。

手順

- 1 [設定] 画面で、[アカウントとデータ ソース] をクリックします。
- 2 編集する汎用ルーターまたはスイッチ データ ソースの横にある [データ ソースの編集] アイコンをクリックします。
- 3 [ファイルの置き換え] をクリックして、新しいデバイス構成ファイルをアップロードします。
- 4 (オプション) アップロードしたデバイス構成ファイルを表示するには、[アップロード履歴] をクリックします。直近にアップロードされた 5 つのデバイス構成ファイルを表示、ダウンロード、および削除できます。
- 5 [検証] をクリックします。
- 6 (オプション) [ニックネーム] テキスト ボックスで、ニックネームを変更します。
- 7 [送信] をクリックします。

データ ソースの移行

4

プロキシ仮想マシンが停止または削除された場合は、新しいプロキシ仮想マシンを追加して、古いプロキシ仮想マシンから新しいプロキシ仮想マシンにデータ ソースを移行できます。

データ ソースを移行するには、次の手順を実行します。

手順

- 1 [インストールとサポート] 画面の [コレクタ (プロキシ) 仮想マシン] セクションの下にある編集アイコンをクリックします。

プロキシ仮想マシンが停止している場合は、プロキシ仮想マシンを使用できないことを示すエラー メッセージが同じセクションに表示されます。
- 2 [コレクタ (プロキシ) 仮想マシンの編集] 画面では、プロキシ仮想マシンにニックネームを割り当てることができます。
- 3 [コレクタ (プロキシ) 仮想マシンの編集] 画面には、プロキシに追加されたすべてのデータ ソースが一覧表示されます。データ ソースを移行するには、特定のデータ ソースについて [移行] をクリックします。
- 4 アカウントまたはソースの編集画面が表示されます。次の情報が入力されていることを確認します。

表 4-1.

フィールド	説明
コレクタ (プロキシ) 仮想マシン	データ ソースの移行先とする新しいプロキシ仮想マシンの名前
IP アドレス	事前入力されたデータ ソースの IP アドレス/FQDN
ユーザー名	データ ソースのユーザー名
パスワード	データ ソースのパスワード

- 5 [検証] をクリックします。[送信] をクリックします。データ ソースが古いプロキシ仮想マシンから削除され、新しいプロキシ仮想マシンに追加されます。

- 6 移行が成功すると、[アカウントとデータ ソース] 画面の [有効] 列にあるデータ ソースに対して新しいプロキシ仮想マシンが表示されます。

注：

- vCenter Server を別のプロキシ仮想マシンに移行する場合は、対応する NSX Manager も同じプロキシ仮想マシンに移行してください。
 - NSX Manager を別のプロキシ仮想マシンに移行すると、NSX Controller や NSX Edge などの子データ プロバイダも新しいプロキシ仮想マシンに移行されます。
-

vRealize Network Insight からのデータソースの削除

5

データソースのデータを表示しない場合や、データソースが使用されていない場合は、データソースを vRealize Network Insight から削除できます。

注： 環境で使用できなくなったデータソースがある場合は、vRealize Network Insight からそのデータソースを削除する必要があります。

手順

- 1 vRealize Network Insight Web コンソールにログインします。
- 2 [設定] - [アカウントとデータソース] の順に移動します。
- 3 削除するデータソースの横にある [データソースの削除] アイコンをクリックします。
vRealize Network Insight によって、確認を求めるプロンプトが表示されます。
- 4 [はい] をクリックします。

注： システムからデータソースを削除してから 2 時間以上経過すると、同じデータプロバイダをもう一度追加することができます。

vRealize Network Insight 設定の構成

6

vRealize Network Insight のさまざまな要素を [設定] 画面で構成できます。[設定] 画面にアクセスするには、[プロフィール] - [設定] の順にクリックします。

この章には、次のトピックが含まれています。

- システムの健全性の表示
- データ保持間隔の設定
- IP プロパティおよびサブネットの設定
- イベントおよび通知の設定
- ID およびアクセス権の管理の設定
- ログの設定
- メール サーバを設定
- SNMP トラップ先の設定
- ライセンスの管理
- 自動更新間隔の設定
- ユーザー セッションのタイムアウトの設定
- Google マップ API キーの追加
- データ ソース証明書の検証の構成
- 監査ログの表示
- カスタマー エクスペリエンス向上プログラムへの参加または参加取り消し
- セットアップの健全性の表示
- サポート トンネルの有効化
- ディスク使用率の管理
- ノードの詳細情報の表示
- サポート バンドルの作成
- コレクタおよびプラットフォームの負荷のキャパシティの概要

システムの健全性の表示

vRealize Network Insight では、システムの健全性ステータスを表示できます。システムの健全性はプロセスの遅延、インデクサの遅延、グリッドの使用状況によって判断されます。これらのすべてのパラメータが緑色の状態になっている場合は、システムの健全性が良好です。これらの 3 つのパラメータのいずれかが赤色の状態になっている場合は、システムの健全性が不良です。

手順

- ◆ [設定] 画面で、[インストールとサポート] をクリックします。

[インストールとサポート] 画面に [システムの健全性] セクションが表示されます。

注： システムの健全性が不良な状態が 6 時間以上続いている場合は、vRealize Network Insight サポートに問い合わせる必要があります。

データ保持間隔の設定

vRealize Network Insight では、データを保持する期間を指定できます。

注： vRealize Network Insight は、Enterprise ライセンスでのみ、設定可能なデータ管理をサポートします。Advanced ライセンス エディションでは、データ保持のデフォルトは 1 か月です。

データは次のカテゴリに分類されます。

表 6-1.

カテゴリ	最小値	最大値
イベント	1 か月	13 か月
エンティティと設定データ	1 か月	3 か月
メトリック	1 か月	13 か月
フロー	なし	1 か月
その他のデータ	なし	100 GB の追加のディスク容量

注： すべてのカテゴリについて、最小値がデフォルト値になります。

カテゴリごとに異なるポリシーを設定および制御できます。ポリシーは、要件に合わせて設定できます。

データ管理を設定するには、次の手順を実行します。

- 1 ホーム ページの右上隅にある  をクリックし、[設定] をクリックします。
- 2 [設定] セクションで、[データ管理] をクリックします。
- 3 初回ログイン時、この画面にはデフォルトのデータが表示されます。
- 4 情報アイコンをクリックすると、データがディスクをどのように占有しているかに関する詳細が表示されます。

- 5 [ポリシーの変更] をクリックして、データのさまざまなカテゴリのデータ保持期間を変更します。変更を加えると、情報がデータベースに記録されます。
- 6 [送信] をクリックします。

注： 低解像度のメトリックの保持期間は、高解像度のメトリックよりも長くなります。

IP プロパティおよびサブネットの設定

vRealize Network Insight では、セキュリティ計画と識別を強化するために各種の IP プロパティを設定できません。

DNS マッピング ファイルのインポート

物理デバイス間のフローに関する情報を提供するには、DNS マッピング ファイルをインポートします。DNS マッピング ファイルでサポートされる形式は、バインド形式および CSV ファイル形式です。これらのファイルは、単一の ZIP ファイルに配置してください。

注： vRealize Network Insight は、パスワード保護された ZIP ファイルをサポートしません。

手順

- 1 [設定] 画面で、[IP プロパティおよびサブネット] をクリックします。
- 2 [物理 IP アドレスおよび DNS マッピング] をクリックします。
- 3 [アップロードおよび置換] をクリックして、DNS マッピング ファイルをアップロードします。ファイルを選択してアップロードしたら、[検証] をクリックします。検証後に DNS レコードの数が表示されます。

[アップロードおよび置換] 操作により、既存の DNS マッピングがすべて削除され、インポートされるマッピングに置き換えられます。DNS マッピング ファイルは、次の 3 つのフィールドで構成されます。

- ホスト名
- IP アドレス
- ドメイン名

サブネットと VLAN の間のマッピングの設定

サブネットと VLAN 間のマッピングを定義できます。

このマッピングは、次の目的で使用できます。

- ソースとターゲットのサブネット、およびフローに関連付けられたレイヤー 2 ネットワークを追加することによって、物理/物理フローから判明した IP エンティティに関する情報を強化する。
- 物理アドレスのサブネットと VLAN に基づいてネットワーク トポロジを計画する。

手順

- 1 [設定] 画面で、[IP プロパティおよびサブネット] をクリックします。
- 2 [物理 IP アドレスおよび DNS マッピング] をクリックします。
- 3 [設定] 画面の [IP プロパティおよびサブネット] で、[物理サブネットおよび VLAN] をクリックします。
この画面には、すべてのサブネットおよび関連付けられた VLAN ID が一覧表示されます。
- 4 [追加] をクリックして、サブネットと VLAN の情報を追加します。
- 5 マッピング情報を定義した後は、サブネットに関連付けられている VLAN ID のみを編集できます。VLAN ID に関連付けられたサブネット CIDR を変更することはできません。VLAN ID に関連付けられたサブネットを編集するには、編集するサブネットを削除し、必要な値を指定してサブネット VLAN マッピングを作成します。
サブネットと VLAN 間のマッピング情報が更新されると、指定した VLAN ID の新しい VLAN が作成され、サブネット情報がこの VLAN に関連付けられます。
- 6 サブネットと VLAN ID のマッピングを削除するには、削除アイコンをクリックします。

注： サブネットと VLAN のマッピングが作成されても、VLAN の作成、更新、削除の全処理がすぐに行われるわけではありません。変更が伝達され、対応する VLAN が作成または変更されるまでにはしばらく時間がかかります。

East-West IP アドレスの設定

RFC1918 標準の範囲内にある IP アドレスは、プライベート IP アドレスと見なされます。RFC1918 の範囲外にある IP アドレスは、インターネット IP アドレスとして扱われます。ただしユーザーは、RFC1918 が定義するプライベート IP アドレスの範囲外であっても、タグ付けフローやマイクロセグメンテーションの際に、非インターネット IP アドレスとして扱う独自の East-West 通信用の IP アドレス（データセンター パブリック IP アドレス）を指定できます。

非インターネット IP アドレスとして扱うパブリック IP アドレスを指定するには、次の手順を実行します。

- 1 [ホーム] 画面の右上隅にある [プロフィール] アイコンをクリックし、[設定] をクリックします。
- 2 [設定] セクションで、[East-West 通信用の IP アドレス] をクリックします。
- 3 [IP アドレス] ボックスに、非インターネット IP アドレスとして扱う特定の IP アドレス、IP アドレス範囲、またはサブネットを入力します。
- 4 [保存] をクリックします。保存に成功すると、「IP アドレスが保存されました」メッセージが表示されます。

North-South 通信用の IP アドレスの設定

RFC1918 空間にある IP アドレスは、North-South 通信用の IP アドレスとして分類されます。ユーザーは、フローとマイクロセグメンテーションをタグ付けするときに、North-South 通信用の IP アドレスを指定できます。

North-South 通信用の IP アドレスを指定するには、次の手順を実行します。

- 1 [ホーム] 画面の右上隅にある [プロフィール] アイコン  をクリックし、[設定] をクリックします。

- 2 [設定] セクションで、[North-South 通信用の IP アドレス] をクリックします。
- 3 [IP アドレス] ボックスに、特定の IP アドレス、IP アドレス範囲、またはサブネットを入力します。
- 4 [保存] をクリックします。保存に成功すると、「IP アドレスが保存されました」メッセージが表示されます。

イベントおよび通知の設定

vRealize Network Insight では、さまざまなタイプのイベントおよび通知を設定できます。事前設定したルールが満たされるたびに、vRealize Network Insight によってイベントが作成されます。

[設定] 画面では、[イベント] をクリックしてさまざまなタイプのイベントを表示できます。

- [システム イベント]
- [ユーザー定義イベント]
- [プラットフォームの健全性イベント]

システム イベントのリスト

vRealize Network Insight で定義されているすべてのシステム イベントのリストを次に示します。そのいずれかのシステム イベントに関する通知を受信するには、その特定のイベントの通知を有効にする必要があります。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.100001	vmwNSXVLate ncyNoDataEve nt	警告	NSXVLatencyNoDataEvent	ネットワーク遅延の収集が停止しました
1.3.6.1.4.1.6876.100.1.0.100051	vmwVMCVMLi mitExceededEv ent	最重要	VMCVMLimitExceededEvent	VMC SDDC 内の仮想マシンの数が制限を超えています。
1.3.6.1.4.1.6876.100.1.0.100052	vmwVMCHostLi mitExceededEv ent	最重要	VMCHostLimitExceededEvent	VMC SDDC 内のホスト数が制限を超えています。
1.3.6.1.4.1.6876.100.1.0.1510	vmwKubernete sBaseEvent	中程度	KubernetesBaseEvent	Kubernetes クラスタによって報告されるイベント
1.3.6.1.4.1.6876.100.1.0.20001	vmwEntityDisco veryChangeEve nt	情報	検出	このイベントは、新しいエンティティが検出された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20002	vmwEntityProp ertiesChangeEv ent	情報	設定の変更	このイベントは、エンティティのいずれかのプロパティが変更された場合に発生します

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20003	vmwFirewallNotInstalledOnHostEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20004	vmwHostWithStaleFirewallRulesEvent	警告	ホストと NSX Manager 間のファイアウォール ルール テーブルが一致しません	ホストと NSX Manager で、分散ファイアウォール ルールのテーブルが異なります。
1.3.6.1.4.1.6876.100.1.0.20005	vmwIpAddressChangeEvent	情報	IP アドレスの変更	このイベントは、仮想マシンの IP アドレスが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20006	vmwL2GatewayAnomalyEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20007	vmwL2NetworkAddressAnomalyEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20008	vmwL2NetworkDiameterExceededEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20009	vmwL2NetworkUplinkMissingEvent	情報	分散仮想ポート グループのアップリンクが見つかりません	VXLAN には指定したホストのアップリンクがありません
1.3.6.1.4.1.6876.100.1.0.20010	vmwL2NetworkWithNoVMsEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20011	vmwLayer2NetworkDiameterChangedEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20012	vmwMTUMismatchEvent	警告	VTEP と物理スイッチ ポート間で MTU が一致しません	VTEP とその物理スイッチ ポートを結ぶバスで、MTU の不一致が検出されました
1.3.6.1.4.1.6876.100.1.0.20013	vmwNetworkIsolationEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20014	vmwNoPathEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20015	vmwSpoofguardDisabledEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20018	vmwVMotionEvent	該当なし	該当なし	該当なし

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20019	vmwVMWithDisconnectedVnicsEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20020	vmwVMWithMultipleVnicsOnDifferentVxlansEvent	該当なし	該当なし	仮想マシン %s が複数の VXLAN [%s] に接続されています
1.3.6.1.4.1.6876.100.1.0.20021	vmwVMWithMultipleVnicsOnSameL2Event	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20022	vmwVMWithNoIpAddressEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20023	vmwVTEPMissingEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20024	vmwL2Event	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20025	vmwMembershipChangeEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20026	vmwSecurityGroupMembershipChangeEvent	情報	セキュリティ グループの仮想マシン メンバーシップの変更	このイベントは、セキュリティ グループのメンバーシップが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20027	vmwFirewallRuleMembershipChangeEvent	情報	ファイアウォール ルールの仮想マシン メンバーシップの変更	このイベントは、ファイアウォール ルールのメンバーシップが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20028	vmwVlanMembershipChangeEvent	情報	VLAN 仮想マシン メンバーシップの変更	このイベントは、VLAN のメンバーシップが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20029	vmwVxlanMembershipChangeEvent	情報	VXLAN 仮想マシン メンバーシップの変更	このイベントは、VXLAN のメンバーシップが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20030	vmwDeleteChangeEvent	情報	変更の削除	このイベントは、エンティティが削除された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20031	vmwVtepFailedPingEvent	該当なし	該当なし	該当なし

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20034	vmwEmptySearchStreamChangeEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20035	vmwSearchStreamMembershipChangeEvent	該当なし	ユーザー定義の変更イベント	ユーザー定義の変更イベント
1.3.6.1.4.1.6876.100.1.0.20036	vmwEmptySearchStreamProblemEvent	該当なし	ユーザー定義のゼロ結果の問題	検索結果が空の場合のユーザー定義問題
1.3.6.1.4.1.6876.100.1.0.20037	vmwSearchStreamMembershipProblemEvent	該当なし	ユーザー定義の変更の問題	検索結果が変更された場合のユーザー定義問題
1.3.6.1.4.1.6876.100.1.0.20038	vmwOspfConfigurationMismatchEvent	中程度	DLR と Edge ルーター間で OSPF エリア ID が一致しない	OSPF エリア ID が、接続先のルーター インターフェイスによって異なります。
1.3.6.1.4.1.6876.100.1.0.20039	vmwServiceVMNotHealthyEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20040	vmwServiceVMNotPoweredOnEvent	最重要	NSX インフラストラクチャ仮想マシンがパワーオンされていません	NSX インフラストラクチャ仮想マシンがパワーオフ状態になっています。この仮想マシンで提供されるサービスが影響を受ける可能性があります。NSX インフラストラクチャには、コントローラ クラスタが含まれます。
1.3.6.1.4.1.6876.100.1.0.20041	vmwServiceVMHighCPUUsageEvent	警告	NSX インフラストラクチャ仮想マシンで高 CPU 使用率が報告されました	NSX インフラストラクチャ仮想マシンで CPU 使用率が高くなっています。この状態になると、サービスが中断する可能性があります。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20042	vmwServiceVMHighMemoryUsageEvent	警告	NSX インフラストラクチャ仮想マシンに対して高メモリ使用率が報告されました	インフラストラクチャ仮想マシンでメモリ使用率が高くなっています。この状態になると、NSX サービスが中断する可能性があります。
1.3.6.1.4.1.6876.100.1.0.20043	vmwServiceVMHighDiskUsageEvent	警告	NSX インフラストラクチャ仮想マシンに対して高ディスク使用率が報告されました	インフラストラクチャ仮想マシンに割り当てられたディスク容量がほとんど使用されています。インフラストラクチャ仮想マシンにアクセスできなくなるか、サービスが中断される可能性があります。
1.3.6.1.4.1.6876.100.1.0.20050	vmwIPSetPropertiesChangeEvent	情報	IP セットのプロパティの変更	このイベントは、IPSet のいずれかのプロパティが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20051	vmwFirewallRulePropertiesChangeEvent	情報	ファイアウォール ルールのプロパティの変更	このイベントは、ファイアウォール ルールのいずれかのプロパティが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20052	vmwSecurityGroupPropertiesChangeEvent	情報	セキュリティ グループのプロパティの変更	このイベントは、セキュリティ グループのいずれかのプロパティが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20053	vmwIPSetMembershipChangeEvent	情報	IP セット メンバーシップの変更	このイベントは、IPSet のメンバーシップが変更された場合に発生します

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20054	vmwFirewallRuleMaskEvent	警告	先行するルールによってマスクされた分散ファイアウォール ルール	分散ファイアウォール ルールは、前述の1つ以上のルールによってマスクされます。この状態は、設定エラーを示していることがあります
1.3.6.1.4.1.6876.100.1.0.20056	vmwSecurityMembershipChangeEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20057	vmwSecurityTagPropertiesChangeEvent	情報	セキュリティ タグのプロパティの変更	このイベントは、セキュリティ タグのいずれかのプロパティが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20058	vmwSecurityTagMembershipChangeEvent	情報	セキュリティ タグ仮想マシンのメンバーシップの変更	このイベントは、セキュリティ タグのメンバーシップが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20059	vmwHostDatastoreChangeEvent	情報	ホストのデータストアが変更されました	このイベントは、ホストのデータストアが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20060	vmwVMDatastoreChangeEvent	情報	仮想マシンのデータストアが変更されました	このイベントは、仮想マシンのデータストアが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20061	vmwVMSnapshotChangeEvent	情報	変更された仮想マシンのスナップショット	このイベントは、仮想マシンのスナップショットが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20062	vmwVMVirtualDiskChangeEvent	情報	仮想マシンの仮想ディスクが変更されました	このイベントは、仮想マシンの仮想ディスクが変更された場合に発生します

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20063	vmwIPSetDefinitionMismatchEvent	情報	NSX Manager 間の IPSet 定義の不一致	名前が同じで、範囲が異なる IPSet が 2 つの NSX Manager で定義されています。この状態は設定エラーを示している可能性があります。
1.3.6.1.4.1.6876.100.1.0.20064	vmwSegmentMismatchEvent	情報	2 つの NSX Manager 間でセグメント ID の範囲が重複しています	複数の NSX Manager で定義されている VXLAN セグメント ID の範囲が重複しています
1.3.6.1.4.1.6876.100.1.0.20065	vmwVtepEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20066	vmwVtepConfigurationFaultEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20067	vmwDLRNetworksNotReachableEvent	最重要	NSX Edge または外部ルーターから DLR ネットワークにアクセスできません	NSX Edge ルーターのアップリンク インターフェイスから 1 つ以上の DLR ネットワークにアクセスできません。この状態は、Edge ルーター/DLR に OSPF 構成エラーがあること、またはアップリンク ルーターでルートが設定されていないことを示します。
1.3.6.1.4.1.6876.100.1.0.20068	vmwVtepSubnetMismatchEvent	中程度	ホストと NSX を使用するクラスタ間で VTEP IP サブネットが一致しません	1 台以上のホストの VTEP の IP アドレスが、同じクラスタ内の他の VTEP と同じサブネット上にありません。この状態になると、ネットワーク接続問題が発生する可能性があります

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20069	vmwVtepCountMismatchEvent	最重要	ホストの VTEP カウントがクラスタと一致しません	ホストの VTEP 数が、同じクラスタ内の他のホストの VTEP 数と一致しません。論理スイッチに接続されているこのホスト上の仮想マシンは通信できない可能性があります。
1.3.6.1.4.1.6876.100.1.0.20070	vmwEdgeNetworksNotReachableEvent	中程度	アップリンク ルーターから NSX Edge ネットワークにアクセスできません	NSX Edge ルーターに接続された 1 つ以上のネットワークにアップリンク ルーターからアクセスできません。
1.3.6.1.4.1.6876.100.1.0.20089	vmwNilInfraChangeEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.20090	vmwDataSourceEnabledChangeEvent	情報	データ ソースが有効になりました	このイベントは、データ ソースが有効な場合に発生します
1.3.6.1.4.1.6876.100.1.0.20091	vmwDataSourceDisabledChangeEvent	情報	データ ソースが無効になりました	このイベントは、データ ソースが無効になっている場合に発生します
1.3.6.1.4.1.6876.100.1.0.20092	vmwDataSourceCreatedEvent	情報	データ ソースが追加されました	このイベントは、データ ソースが追加された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20093	vmwPlatformCpuCoreChangeEvent	情報	プラットフォーム CPU コア変更イベント	このイベントは、プラットフォームの CPU コアが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20094	vmwPlatformDiskChangeEvent	情報	プラットフォーム ディスク変更イベント	このイベントは、プラットフォームのディスクが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20095	vmwPlatformMemoryChangeEvent	情報	プラットフォーム メモリ変更イベント	このイベントは、プラットフォームのメモリが変更された場合に発生します

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.20096	vmwPlatformRebootedEvent	情報	プラットフォームが再起動されたというイベント	このイベントは、プラットフォームが再起動された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20097	vmwProxyCpuCoreChangeEvent	情報	プロキシ CPU コア変更イベント	このイベントは、コレクタの CPU コアが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20098	vmwProxyDiskChangeEvent	情報	プロキシ ディスク変更イベント	このイベントは、コレクタのディスクが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20099	vmwProxyMemoryChangeEvent	情報	プロキシ メモリ変更イベント	このイベントは、コレクタのメモリが変更された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20100	vmwProxyRebootedEvent	情報	プロキシが再起動されたというイベント	このイベントは、コレクタが再起動された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20101	vmwNICClusterChangeEvent	情報	クラスタが拡張されました	このイベントは、プラットフォームがシステムに追加された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20102	vmwNISystemProxyChangeEvent	情報	プロキシが追加/削除されました	このイベントは、プロキシが追加または削除された場合に発生します
1.3.6.1.4.1.6876.100.1.0.20103	vmwNICClusterCreateEvent	情報	クラスタが作成されました	このイベントは、クラスタが作成された場合に発生します
1.3.6.1.4.1.6876.100.1.0.30001	vmwThresholdExceededEventCpuReady	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30002	vmwThresholdExceededEventCpuCoStop	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30003	vmwThresholdExceededEventDiskCommandAbortRule	該当なし	該当なし	該当なし

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.30004	vmwThresholdExceededEventIODeviceLatencyRule	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30005	vmwThresholdExceededEventIOKernelLatencyRule	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30006	vmwThresholdExceededEventMemorySwapInRule	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30007	vmwThresholdExceededEventMemorySwapOutputRule	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30008	vmwThresholdExceededEventNetworkRxDropRule	警告	ホスト インターフェイスで受信パケット ドロップが検出されました	ホスト インターフェイスの受信側で、しきい値を超える量のパケット ドロップが検出されました。
1.3.6.1.4.1.6876.100.1.0.30009	vmwThresholdExceededEventNetworkTxDropRule	警告	ホスト インターフェイスで転送パケット ドロップが検出されました	ホスト インターフェイスの送信側で、しきい値を超える量のパケット ドロップが検出されました。
1.3.6.1.4.1.6876.100.1.0.30010	vmwAWSRegionSGLimitEvent	最重要	AWS リージョンで使用可能な AWS セキュリティ グループ。	AWS リージョンで使用可能な AWS セキュリティ グループ。
1.3.6.1.4.1.6876.100.1.0.30011	vmwAWSVPCSGLimitEvent	最重要	Amazon VPC で使用可能な AWS セキュリティ グループ。	Amazon VPC で使用可能な AWS セキュリティ グループ。
1.3.6.1.4.1.6876.100.1.0.30012	vmwAWSSGInboundRuleLimitEvent	最重要	AWS セキュリティ グループで使用可能な受信ルール。	AWS セキュリティ グループで使用可能な受信ルール。
1.3.6.1.4.1.6876.100.1.0.30013	vmwAWSSGOutboundRuleLimitEvent	最重要	AWS セキュリティ グループで使用可能な送信ルール。	AWS セキュリティ グループで使用可能な送信ルール。
1.3.6.1.4.1.6876.100.1.0.30014	vmwAWSInterfaceSGLimitEvent	最重要	AWS インターフェイスで使用可能な AWS セキュリティ グループ。	AWS インターフェイスで使用可能な AWS セキュリティ グループ。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.30100	vmwPacketDropEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30101	vmwSwitchPortPacketDropEvent	警告	スイッチ ポートでドロップされたパケット	指定したスイッチ ポートで大量のパケット ドロップが検出されました
1.3.6.1.4.1.6876.100.1.0.30102	vmwRouterInterfacePacketDropEvent	警告	NSX Edge ゲートウェイ インターフェイスでドロップされたパケット	NSX Edge Gateway の vNIC インターフェイスで、しきい値を超える量のパケット ドロップが検出されました。
1.3.6.1.4.1.6876.100.1.0.30103	vmwVnicPacketDropEvent	警告	仮想マシンでドロップされたパケット数	仮想マシン インターフェイスで、しきい値を超える量のパケット ドロップが検出されました。
1.3.6.1.4.1.6876.100.1.0.30104	vmwVTEPUnderlayPacketDropEvent	中程度	VTEP アンダーレイ パケット ドロップ	VTEP アンダーレイで大量のパケット ドロップが検出されました
1.3.6.1.4.1.6876.100.1.0.30105	vmwPnicUnderlyingSwitchPortPacketDropEvent	警告	物理 NIC の基盤となるスイッチ ポートでドロップされたパケット	指定した物理 NIC に関連付けられたスイッチ ポートで、しきい値を超える量のパケット ドロップが検出されました。
1.3.6.1.4.1.6876.100.1.0.30106	vmwDevicePacketDropEvent	警告	ハードウェア ゲートウェイ ポートでパケット ドロップが検出されました	指定したデバイスで、しきい値を超える量のパケット ドロップが検出されました。
1.3.6.1.4.1.6876.100.1.0.30110	vmwSwitchPortUptimeThresholdRecededEvent	警告	SwitchPortUptimeThresholdRecededEvent	アップタイムの後退
1.3.6.1.4.1.6876.100.1.0.30111	SwitchPortOperationalDownEvent	警告	スイッチ ポートが動作を停止しています	スイッチ ポートが動作を停止しています。
1.3.6.1.4.1.6876.100.1.0.30112	RouterInterfaceOperationalDownEvent	警告	ルーター インターフェイスが動作を停止しています	ルーター インターフェイスが動作を停止しています。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.30116	UnderlayDeviceFanMalFunctionEvent	警告	アンダーレイ デバイス ファン削除イベントまたは非動作イベント。	アンダーレイ デバイス ファン削除イベントまたは非動作イベント。
1.3.6.1.4.1.6876.100.1.0.30117	UnderlayDeviceTemperatureThresholdExceededEvent	警告	アンダーレイ デバイス温度のしきい値超過イベント	アンダーレイ デバイス温度のしきい値超過イベント。
1.3.6.1.4.1.6876.100.1.0.30118	UnderlayDeviceFexFanMalFunctionEvent	警告	Fex ファン削除イベントまたは非動作イベント	Fex ファン削除イベントまたは非動作イベント。
1.3.6.1.4.1.6876.100.1.0.30119	UnderlayDeviceFexPsMalFunctionEvent	警告	Fex 電源削除イベントまたは非動作イベント	Fex 電源削除イベントまたは非動作イベント。
1.3.6.1.4.1.6876.100.1.0.30120	UnderlayDeviceModuleMalFunctionEvent	警告	アンダーレイ デバイス モジュール削除イベントまたは非動作イベント	アンダーレイ デバイス モジュール削除イベントまたは非動作イベント。
1.3.6.1.4.1.6876.100.1.0.30121	UnderlayDevicePsMalFunctionEvent	警告	アンダーレイ デバイス電源削除イベントまたは非動作イベント	アンダーレイ デバイス電源削除イベントまたは非動作イベント。
1.3.6.1.4.1.6876.100.1.0.30122	UnderlayDeviceBfdSessionRemovedEvent	警告	アンダーレイ デバイス BFD セッション削除イベント	アンダーレイ デバイス BFD セッションの削除イベント。
1.3.6.1.4.1.6876.100.1.0.30123	UnderlayDeviceLldpNeighbourRemovedEvent	警告	アンダーレイ デバイス LLDP ネイバー削除イベント	アンダーレイ デバイス LLDP ネイバー削除イベント
1.3.6.1.4.1.6876.100.1.0.30203	vmwThresholdExceededEventDatastoreFreeSpaceWarning	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30204	vmwThresholdExceededEventDatastoreFreeSpaceCritical	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30205	vmwThresholdExceededEventDatastoreReadLatency	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.30206	vmwThresholdExceededEventDatastoreWriteLatency	該当なし	該当なし	該当なし

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.35001	vmwDistributedFirewallApplyHostEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.35002	vmwDistributedFirewallApplyVMEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.35003	vmwNsxEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.35004	vmwFeatureIm pactedEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.35221	vmwNSXComp onentEvent	最重要	NSX 管理サービスが実行されていません	NSX 管理アプライアンス サービスが停止しています
1.3.6.1.4.1.6876.100.1.0.35222	vmwNSXBacku pEvent	情報	NSX Manager バックアップが構成されていません	NSX Manager のバックアップが設定されていません。すべての NSX コンポーネントを正しくバックアップすることは、障害が発生した場合にシステムを正常動作の状態にリストアするために重要です
1.3.6.1.4.1.6876.100.1.0.35223	vmwNSXBacku pAuditLogExclu dedEvent	情報	NSX Manager のバックアップから除外される監査ログ	監査ログは現在バックアップから除外されています
1.3.6.1.4.1.6876.100.1.0.35224	vmwNSXUnsec ureBackupEven t	情報	NSX Manager バックアップが SFTP 用に構成されていません	現在、セキュアな FTP がバックアップに使用されていません
1.3.6.1.4.1.6876.100.1.0.35225	vmwNSXBacku pSystemEvents ExcludedEvent	情報	NSX Manager バックアップから除外されるシステム イベント	システム イベントは現在バックアップから除外されています
1.3.6.1.4.1.6876.100.1.0.35226	vmwNSXBacku pNotScheduled Event	情報	スケジュール設定された NSX Manager バックアップが有効になっていません	環境のスケジュール バックアップが設定されていません

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.35227	vmwNSXBackupNotRecordedEvent	情報	NSX Manager バックアップが記録されていません	環境のバックアップが実行されませんでした。すべての NSX コンポーネントを正しくバックアップすることは、障害が発生した場合にシステムを正常動作の状態にリストアするために重要です
1.3.6.1.4.1.6876.100.1.0.35228	vmwNSXNtpServerEvent	情報	NTP サーバが NSX Manager 用に構成されていません	NSX Manager に NTP サーバが構成されていません
1.3.6.1.4.1.6876.100.1.0.35229	vmwNSXSysLogServerEvent	情報	Syslog サーバが NSX Manager 用に構成されていません	NSX Manager に設定された Syslog サーバがありません。Syslog データは、インストールおよび設定中にログに記録されたデータをトラブルシューティングする場合や、取得する場合に役立ちます
1.3.6.1.4.1.6876.100.1.0.35230	vmwControllerSysLogServerEvent	情報	NSX Controller に対して Syslog サーバが構成されていません	NSX Controller に設定された Syslog サーバがありません。Syslog データは、インストールおよび設定中にログに記録されたデータをトラブルシューティングする場合や、取得する場合に役立ちます
1.3.6.1.4.1.6876.100.1.0.35231	vmwNSXIPv6EnabledEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.35232	vmwNSXOspfNeighborDownEvent	警告	NSX Edge ルーターから 1 つ以上の OSPF ネイバーにアクセスできません	NSX Edge に接続されている 1 つ以上の OSPF ネイバーが停止しています

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.36022	vmwClusterFeatureVersionMismatchEvent	情報	NSX 機能のバージョンが ESXi クラスタのバージョンと一致しません	準備されたクラスタの NSX 機能のバージョンが NSX Manager のバージョンと一致しません。
1.3.6.1.4.1.6876.100.1.0.36023	vmwHostFeatureVersionMismatchEvent	情報	ホストとクラスタ間の NSX 機能のバージョンが一致しません	ホストのファブリック ステータス リソース機能のバージョンが、クラスタまたは NSX Manager のバージョンと同じではありません
1.3.6.1.4.1.6876.100.1.0.36024	vmwFeatureVersionMismatchEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.36025	vmwHostFeatureEnabledMismatchEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.36026	vmwHostFeatureInstalledMismatchEvent	情報	ネットワーク ファブリック 機能のステータスがホストとクラスタ間で一致しません	ホストのネットワーク ファブリック 機能のステータスが、クラスタ内の他のホストのステータスと一致しません。
1.3.6.1.4.1.6876.100.1.0.36027	vmwHostVtepNotFoundEvent	最重要	準備されたホストに VTEP が見つかりません	NSX 用に準備されたクラスタ内のホストに、1つ以上の VTEP がありません。このホストの仮想マシンがいずれかの論理スイッチに接続されている場合、これらの仮想マシンが通信できない可能性があります。
1.3.6.1.4.1.6876.100.1.0.36028	vmwHostVtepDisconnectedEvent	警告	ホストの VTEP が管理上無効になっています	ホストの VTEP が無効になり、接続されていない状態になっています。
1.3.6.1.4.1.6876.100.1.0.36029	vmwHostVtepEvent	最重要	ホストの VTEP が切断されました	ホストの VTEP が切断されました

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.36030	vmwClusterHostsVtepMTUMismatchEvent	警告	ホストと NSX を使用するクラスタ間で VTEP MTU が一致しません	ホストと NSX 対応クラスタの間で VTEP MTU が一致しません。
1.3.6.1.4.1.6876.100.1.0.36031	vmwFeatureUnhealthyEvent	警告	ネットワーク ファブリック機能がエラー状態です	問題によっては、インストールされている NSX の機能が NSX Manager から報告されることがあります。
1.3.6.1.4.1.6876.100.1.0.36032	vmwEdgeHANOtConfiguredEvent	情報	NSX Edge 高可用性が有効になっていません	NSX Edge で高可用性が有効になっていません
1.3.6.1.4.1.6876.100.1.0.36033	vmwEdgeInterfacesDownEvent	警告	1つ以上の NSX Edge 論理ルーター インターフェイスが停止しています	1つ以上の NSX Edge インターフェイスが停止しています。
1.3.6.1.4.1.6876.100.1.0.36041	vmwModuleUnhealthyEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.36042	vmwModuleNotLoadedEvent	最重要	NSX VIB またはホスト モジュールがホストで検出されませんでした	1つ以上の NSX VIB またはホスト モジュールがホストで検出されませんでした
1.3.6.1.4.1.6876.100.1.0.36043	vmwModuleNetworkConnectionFailureEvent	最重要	NSX Manager とホスト間で、メッセージ バスまたは制御プレーンの接続が確立されていません	このホスト上のメッセージ バスおよび制御プレーン エージェント デモンには、NSX Controller または NSX Manager との接続エラーが発生しています

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.36044	vmwHostNetworkControlPlaneMismatchEvent	中程度	論理スイッチテーブルがホストと NSX Controller 間で一致しません	プライマリ NSX Controller と、論理スイッチが使用されているすべてのホストの間で論理スイッチ情報が一致しません。このイベントは、シャードニングの変更後にエラー状態になっていることを示している場合があります。
1.3.6.1.4.1.6876.100.1.0.36045	vmwHostNetworkControlPlaneConnectionFailureEvent	最重要	1 台以上の論理スイッチに対して、ホスト制御プレーンからコントローラへの接続が確立されていません	1 台以上の論理スイッチで、NSX ホストの制御プレーンエージェントとそのプライマリ NSX Controller の間に接続が確立されていません。この状態になると、ホストと NSX Controller の情報が古くなる可能性があります。
1.3.6.1.4.1.6876.100.1.0.36046	vmwHostNetworkControlPlaneNotSyncedEvent	中程度	ホストと NSX Controller 間の論理ネットワークの同期が取れていません	ホスト上の論理スイッチングおよびルーティングに関する情報が、NSX Controller の情報と同期していません。この状況が発生していることを確認するには
1.3.6.1.4.1.6876.100.1.0.36047	vmwNSXControllerClusterMajorityEvent	中程度	NSX Controller マジョリティがありません	クラスタ内の一部の NSX Controller が NSX Manager と通信していません
1.3.6.1.4.1.6876.100.1.0.36048	vmwNSXControllersVMOnSameHostEvent	情報	すべてのコントローラ仮想マシンが同じホストに展開されました	クラスタ内のすべての NSX Controller が同じホストに展開されています

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.36049	vmwVxLanRangeExhaustEvent	警告	VXLAN セグメント ID 範囲が枯渇しています	VXLAN セグメント ID の使用率が 90% を超えています
1.3.6.1.4.1.6876.100.1.0.36050	vmwNSXFirewallDefaultAllowAllRulesEvent	情報	デフォルトのファイアウォール ルールで許可されるすべてのトラフィック	分散ファイアウォールは、デフォルトですべてのトラフィックを許可するように設定されています
1.3.6.1.4.1.6876.100.1.0.36051	vmwLogicalRouterNoUplinkEvent	情報	アップリンク インターフェイスを使用せずに展開した NSX DLR	NSX DLR にアップリンク インターフェイスが設定されていません
1.3.6.1.4.1.6876.100.1.0.36052	vmwEdgeNotHAAEvent	情報	NSX Edge が設定されていますが、高可用性ではありません	Edge の高可用性を実現するために 2 台の Edge 仮想マシンが設定されています
1.3.6.1.4.1.6876.100.1.0.36053	vmwEdgeNotDeployedEvent	情報	NSX Edge の展開に失敗しました	NSX Edge の展開に失敗しました。この状態は、NSX Edge が設定されているにもかかわらず、実際には展開されていないことを示している場合があります。
1.3.6.1.4.1.6876.100.1.0.36054	vmwEcmpIsEnabledAndStatefulServicesAreUpEvent	情報	ECMP サービスとステートフル Edge サービスの両方で構成された NSX Edge	ファイアウォール
1.3.6.1.4.1.6876.100.1.0.36055	vmwLogicalRouterDeployedOnEcmpEdgeHostEvent	情報	NSX DLR が 1 つ以上の NSX ECMP Edge と同じホストに展開されています	NSX 分散論理ルーター制御仮想マシンは、ECMP 用に設定された 1 つ以上の NSX Edge と同じホストに展開されています。
1.3.6.1.4.1.6876.100.1.0.36056	vmwEdgeMissingInterfaceOSPFAreaMappingEvent	情報	NSX Edge インターフェイスから OSPF エリアへのマッピングがありません	NSX Edge で OSPF が有効になっています

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.36057	vmwOspfInsecureAuthRouterEvent	情報	1つ以上の OSPF エリアで安全でない認証が使用されています	NSX Edge Services Gateway または DLR 上の1つ以上の OSPF エリアが MD5 認証を使用するように設定されていません
1.3.6.1.4.1.6876.100.1.0.36058	vmwNSXControllersDeployedCountEvent	情報	展開された NSX Controller の数が正しくありません	展開されているコントローラが3台未満です
1.3.6.1.4.1.6876.100.1.0.36059	vmwNSXControllerNotActiveCountEvent	中程度	3台未満のアクティブな NSX Controller	アクティブなコントローラが3台未満です
1.3.6.1.4.1.6876.100.1.0.36060	vmwNSXControllerEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.36061	vmwNSXEcmpEdgeDownEvent	情報	ECMP クラスタ内の1つ以上の NSX Edges が現在停止しています	ECMP クラスタ内の1つ以上の NSX Edges が現在停止しています
1.3.6.1.4.1.6876.100.1.0.36062	vmwNSXMajorityEcmpEdgesDownEvent	警告	ECMP クラスタ内の大多数の NSX Edges が現在停止しています	ECMP クラスタ内の大多数の NSX Edges が現在停止しています
1.3.6.1.4.1.6876.100.1.0.36063	vmwNSXAllEcmpEdgesDownEvent	最重要	ECMP クラスタ内のすべての NSX Edge が現在停止しています	ECMP クラスタ内のすべての NSX Edge が現在停止しています
1.3.6.1.4.1.6876.100.1.0.36064	vmwNSXEdgeMtuMismatchEvent	情報	Edge 上の1つ以上のインターフェイスで構成された MTU が、ネクスト ホップ ルーターの MTU と一致しません	同じレイヤー 2 ネットワーク内にある複数の Edge 上の1つ以上のインターフェイスに設定された MTU が一致しません
1.3.6.1.4.1.6876.100.1.0.36065	vmwNSXEdgesSplitBrainEvent	最重要	両方の NSX Edge HA 仮想マシンがアクティブな状態です	Edge HA の両方の仮想マシンがアクティブな状態です。最も一般的な問題はスプリット ブレインです
1.3.6.1.4.1.6876.100.1.0.36066	vmwVirtualDistributedRoutingEvent	警告	VXLAN ルーティング用の VDR ポートがホストにありません	指定した VXLAN のホストに VDR ポートがありません

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.36067	vmwNSXEdgeBGPNeighbourDownEvent	最重要	1つ以上の BGP ネイバーが確立された状態ではありません	1つ以上の BGP ネイバーが確立された状態ではありません。
1.3.6.1.4.1.6876.100.1.0.37001	vmwAnalyticsEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.37002	vmwAnalyticsOutlierEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.37003	vmwAnalyticsThresholdEvent	最重要	しきい値違反イベント	指定したメトリックの結果として生成されたイベントが、設定で指定された上限または下限を超えています
1.3.6.1.4.1.6876.100.1.0.38001	vmwVMCEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.40001	vmwCriticalHostNotAccessibleEvent	最重要	インフラストラクチャ仮想マシンを含むホストにアクセスできない	インフラストラクチャ仮想マシンを含むホストにアクセスできない
1.3.6.1.4.1.6876.100.1.0.568	vmwArkinApplicationMembershipLimitEvent	情報	アプリケーション メンバーシップの制限を超えました	アプリケーションのメンバー数がサポートされている制限を超えています
1.3.6.1.4.1.6876.100.1.0.70000	vmwGenericNSXSystemEvent	中程度	NSX システム イベント (警告)	重要度が高または重大である NSX システム イベント
1.3.6.1.4.1.6876.100.1.0.70001	vmwFilterConfigApplyOnHostFailedEvent	警告	ホスト vNIC の分散ファイアウォールの更新の適用に失敗しました	分散ファイアウォール設定の更新を NSX 対応ホストの vNIC に適用できませんでした。
1.3.6.1.4.1.6876.100.1.0.70002	vmwRulesetLoadOnHostFailedEvent	警告	分散ファイアウォールの更新をホストに適用できませんでした	分散ファイアウォールのルールセットがホストに適用されませんでした。
1.3.6.1.4.1.6876.100.1.0.70003	vmwConfigUpdateOnHostFailedEvent	警告	分散ファイアウォールの構成の更新に失敗しました	NSX ホストへのファイアウォール設定の更新がタイムアウトになりました。ホストと最新版のファイアウォール設定が同期していません。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.70004	vmwSpoofguardConfigUpdateOnHostFailedEvent	情報	SpoofGuard 構成の更新に失敗しました	ホストの SpoofGuard 設定の更新に失敗しました。
1.3.6.1.4.1.6876.100.1.0.70005	vmwApplyRuleToVnicFailedEvent	警告	分散ファイアウォールルールがホスト vNIC に適用されていません	分散ファイアウォールルールがホストの vNIC に適用されませんでした。
1.3.6.1.4.1.6876.100.1.0.70006	vmwContainerConfigUpdateOnVnicFailedEvent	警告	ホストでの分散ファイアウォール コンテナの更新に失敗しました	NSX 分散ファイアウォールまたは Service Composer で使用されるネットワークおよびセキュリティ コンテナの情報が、NSX ホストで更新されませんでした。
1.3.6.1.4.1.6876.100.1.0.70007	vmwSpoofguardApplyToVnicFailedEvent	情報	SpoofGuard の初期構成に失敗しました	ホスト上の指定した vNIC に SpoofGuard の設定が適用されませんでした。
1.3.6.1.4.1.6876.100.1.0.70008	vmwHostMessagingConfigurationFailedEvent	警告	ホストのメッセージング構成の更新に失敗しました	NSX メッセージングチャンネルを介してホストにプッシュされた設定の更新が完了しませんでした。
1.3.6.1.4.1.6876.100.1.0.70009	vmwHostMessagingConnectionReconfigurationFailedEvent	警告	ホストのメッセージング接続の再設定に失敗しました	ホスト メッセージングチャンネルに関する最新情報を NSX ホストに送信できませんでした。
1.3.6.1.4.1.6876.100.1.0.70010	vmwHostMessagingConfigurationFailedNotificationSkippedEvent	警告	ホストと NSX Manager 間のホストのメッセージングチャンネルの再確立に失敗しました	準備済みホストが vCenter Server に再び接続したときに、NSX Manager がメッセージバスチャンネルの再確立を試行しました。この接続が再度失敗しました

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.70011	vmwHostMessagingInfrastructureDownEvent	警告	ホスト上でホスト メッセージング インフラストラクチャが停止しています	NSX Manager と NSX ホスト間の 2 つ以上のメッセージングチャネル ハートビートメッセージが失われました。
1.3.6.1.4.1.6876.100.1.0.70012	vmwEdgeVMNotRespondingEvent	中程度	NSX Edge から NSX Manager へのハートビートに障害が発生しました	NSX Edge 仮想マシンが NSX Manager による健全性チェックに応答していません
1.3.6.1.4.1.6876.100.1.0.70013	vmwEdgeUnhealthyEvent	最重要	NSX Edge 仮想マシンがアクティブ/セルフ状態ではありません	NSX Edge 仮想マシンが問題のある状態を報告していて、正しく機能していない可能性があります。
1.3.6.1.4.1.6876.100.1.0.70014	vmwEdgeVMCommunicationFailureEvent	最重要	NSX Manager と Edge 仮想マシンの通信障害	NSX Manager と Edge 仮想マシン間で通信エラーが検出されました。
1.3.6.1.4.1.6876.100.1.0.70015	vmwNSXEdgeEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.71000	vmwOtherCriticalNSXEvent	最重要	重大な NSX システム イベント	重要度が重大である NSX システム イベントです。
1.3.6.1.4.1.6876.100.1.0.80001	vmwPanNsxNotInRegisteredStateEvent	最重要	Palo Alto Panorama が NSX Manager に登録されていません	Panorama は NSX Manager に登録された状態ではありません。
1.3.6.1.4.1.6876.100.1.0.80002	vmwPanNsxDynamicUpdateDelayedEvent	警告	Panorama 動的メンバーシップ定義の更新が遅延しています	NSX Manager で行った Panorama メンバーシップ定義の動的な更新が遅延しています。この状態は、ネットワーク接続に問題があること、または NSX Manager の NetX サービスに問題があることを示している可能性があります。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80003	vmwPanDeviceInDisconnectedStateEvent	警告	Palo Alto サービス仮想マシンが Panorama に接続されていません	Palo Alto Networks 用のサービス仮想マシンまたはデバイスが、Panorama と接続された状態になっていません
1.3.6.1.4.1.6876.100.1.0.80004	vmwPanNsxServiceApplianceViewMismatchEvent	最重要	Panorama と NSX Manager 間のサービス仮想マシンのステータスが一致しません	NSX Manager と Panorama の間でサービス アプライアンス情報が一致しません。
1.3.6.1.4.1.6876.100.1.0.80005	vmwPanNsxFabricAgentNotFoundOnHostEvent	最重要	NSX ファブリック エージェントがホストに見つかりませんでした	クラスタが準備されているホストでは、NSX からセキュリティ ファブリック エージェントに報告されません
1.3.6.1.4.1.6876.100.1.0.80006	vmwPanNsxServiceVMNotFoundOnHostEvent	最重要	ホストに Palo Alto サービス仮想マシンが見つかりません	Palo Alto のセキュリティ アプライアンス仮想マシンが、NSX 対応クラスタ内のホスト上に見つかりませんでした。
1.3.6.1.4.1.6876.100.1.0.80100	vmwCheckpointEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.80102	vmwCheckpointNsxFabricAgentNotFoundOnHostEvent	最重要	CheckpointNsxFabricAgentNotFoundOnHostEvent	クラスタが準備されているホストでは、NSX からセキュリティ ファブリック エージェントに報告されません
1.3.6.1.4.1.6876.100.1.0.80103	vmwCheckpointNsxServiceVMNotFoundOnHostEvent	最重要	CheckpointNsxServiceVMNotFoundOnHostEvent	Check Point のセキュリティ アプライアンス仮想マシンが、NSX 対応クラスタ内のホスト上に見つかりませんでした。
1.3.6.1.4.1.6876.100.1.0.80104	vmwCheckpointGatewaySicStatusNotCommunicatingEvent	最重要	CheckpointGatewaySicStatusNotCommunicatingEvent	Check Point のサービス仮想マシンまたはゲートウェイの SIC ステータスが「通信中」ではありません

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80105	vmwCheckpointNsxServiceApplianceViewMismatchEvent	最重要	Check Point と NSX Manager 間のサービス仮想マシンのステータスが一致しません	NSX Manager と Check Point の間でサービス アプライアンス情報が一致しません。
1.3.6.1.4.1.6876.100.1.0.80200	NSXTEvent	該当なし	NSX-T システム イベント	NSX-T プラットフォームで生成されたアラーム/イベント
1.3.6.1.4.1.6876.100.1.0.80201	NSXTVcNotAddedEvent	警告	1 台以上の vCenter Server が vRNI にデータ ソースとして追加されていません	NSX-T に、同じ IP アドレスまたは同じ FQDN で vRNI にデータ ソースとして追加されていないコンピュータ マネージャが少なくとも 1 つ存在します。
1.3.6.1.4.1.6876.100.1.0.80202	NSXTStandaloneHostsEvent	警告	1 台以上のファブリック ノードがスタンドアローン ホストとして NSX-T に追加されました	1 台以上のファブリック ノードが、NSX-T にスタンドアローン ホストとして追加されています。これらのホスト上の仮想マシンは、vRNI では表示されません。
1.3.6.1.4.1.6876.100.1.0.80203	vmwNSXTSysystemEvent	該当なし	該当なし	該当なし
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	警告	NSX-T Tier-1 論理ルーターの切断イベント	NSX-T Tier-1 論理ルーターが Tier-0 ルーターから切断されています。このルーターの下位のネットワークに外部からアクセスすることはできず、その逆方向にアクセスすることもできません。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	警告	ルーティングのアドバタイズが無効です	NSX-T Tier-1 論理ルーターでは、ルーティングのアドバタイズが無効になっています。このルーターの下位のネットワークには外部からアクセスできません。
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	最重要	NSX-T Edge ノードにマネージャが接続されていません	NSX-T Edge ノードにマネージャが接続されていません。
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	警告	NSX-T Edge ノードのコントローラの接続が低下しました	NSX-T Edge ノードが 1 台以上のコントローラと通信できません。
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	最重要	NSX-T Edge ノードにコントローラが接続されていません	NSX-T Edge ノードは、どのコントローラとも通信できません。
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtuMismatchEvent	警告	NSX-T Tier-0 とアップリンク スイッチ / ルーター間で MTU が一致しません	Tier-0 論理ルーターのインターフェイスに設定された MTU が、同じ L2 ネットワーク内のアップリンク スイッチ / ルーターのインターフェイスと一致しません。これは、ネットワークのパフォーマンスに影響を与える可能性があります。
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	情報	1 台以上の仮想マシンが NSX-T DFW ファイアウォールから除外されました。	NSX-T DFW ファイアウォールで保護されていない仮想マシンが 1 台以上あります。vRealize Network Insight は、これらの仮想マシンの IPFIX フローを受信しません。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	警告	アップリンク VLAN の設定が正しくありません	Tier-0 ルーターのアップリンク ポートの VLAN が外部ゲートウェイの VLAN と異なるため、通信は中断されます。
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	警告	トランスポート ノードに接続されているトランスポート ゾーンがありません。	トランスポート ノードに接続されたトランスポート ゾーンがありません。これが原因で、仮想マシンは接続に失敗した可能性があります。
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	警告	トランスポート ノードで使用できる VTEP がありません。	すべての VTEP がトランスポート ノードから削除されています。これが原因で、仮想マシンは接続に失敗した可能性があります。
1.3.6.1.4.1.6876.100.1.0.80215	vmwDuplicateL3SwitchEvent	最重要	同じスイッチまたはルーターが追加されたというイベント	異なる IP アドレスを持つ同じスイッチまたはルーターが追加されました。仮想マシン間のパスが生成されない可能性があります。
1.3.6.1.4.1.6876.100.1.0.80216	vmwLBPoolMemberDownEvent	最重要	プール メンバーが停止しています	このイベントは、ロード バランサのプール メンバーが停止している場合に発生します。停止しているプール メンバーを確認するには、「Pool Member where state = DISABLED」で検索します
1.3.6.1.4.1.6876.100.1.0.80217	vmwLBPoolDownEvent	最重要	プールが停止しています	このイベントは、ロード バランサのプールが停止したときに発生します

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80218	vmwLBPoolEmptyEvent	最重要	プールが空です	このイベントは、ロード バランサのプールが空の場合に発生します。空のプールを確認するには、「Pool where PoolMembers Count = 0」で検索します。
1.3.6.1.4.1.6876.100.1.0.80219	vmwLBPoolMemberVMDownEvent	最重要	プール メンバーの仮想マシンが停止しています	このイベントは、ロード バランサのプール メンバーに関連付けられた仮想マシンが停止した場合に発生します
1.3.6.1.4.1.6876.100.1.0.80220	vmwLBVirtualServerDisableEvent	最重要	ロード バランサの仮想サーバが無効です	このイベントは、ロード バランサの仮想サーバが無効になっている場合に発生します
1.3.6.1.4.1.6876.100.1.0.80221	vmwLBServiceNodeIPNotFoundEvent	最重要	サービス ノードの IP アドレスが見つかりません	このイベントは、ロード バランサのサービス ノードの IP アドレスに関連付けられた NIC が見つからない場合に発生します
1.3.6.1.4.1.6876.100.1.0.80222	vmwLBServiceNodeMultipleNICFoundEvent	最重要	サービス ノードの複数の NIC が検出されました	このイベントは、ロード バランサのサービス ノードの IP アドレスに関連付けられた NIC が複数見つかった場合に発生します

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80223	NSXSwitchIpfixEnabledEvent	警告	NSX-T スイッチの IPFIX が有効になっていて、いずれかの vRNI コレクタを参照するコレクタ プロファイルが用意されています。	Network Insight は、NSX-T スイッチからの IPFIX フロー データをサポートしていません。Network Insight は、Network Insight Collector 仮想マシンの 1 つに IPFIX データを送信するように設定されています。システム内の既存のフロー データが破損している可能性があります。
1.3.6.1.4.1.6876.100.1.0.80224	NSXSTandaloneHostsWithoutVcEvent	最重要	NSX-T で 1 台以上のファブリック ノードを管理している vCenter Server は vRNI でデータ ソースとして追加しない	NSX-T で 1 台以上のファブリック ノードを管理している vCenter Server は、vRNI でデータ ソースとして追加されません。これらのホスト上の仮想マシンは、vRNI では表示されません。
1.3.6.1.4.1.6876.100.1.0.80225	NSXControllerNodeToControlClusterConnectivityEvent	最重要	NSX-T コントローラ ノードにコントロール クラスタが接続されていません	NSX-T コントローラ ノードでコントロール クラスタへの接続が失われました。
1.3.6.1.4.1.6876.100.1.0.80226	NSXControllerNodeToMgmtPlaneConnectivityEvent	最重要	NSX-T コントローラ ノードに管理プレーンが接続されていません	NSX-T コントローラ ノードで管理プレーンへの接続が失われました。
1.3.6.1.4.1.6876.100.1.0.80227	NSXMPNodeToMgmtClusterConnectivityEvent	最重要	NSX-T 管理ノードに管理クラスタが接続されていません	NSX-T 管理ノードで管理クラスタへの接続が失われました。
1.3.6.1.4.1.6876.100.1.0.80228	NSXHostNodePnicStatusDownEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「切断」です。	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「切断」です。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80229	NSXHostNodePnicStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「劣化」です	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80230	NSXHostNodePnicStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「不明」です。	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80231	NSXHostNodeTunnelStatusDownEvent	警告	NSX-T ホスト トランスポート ノードのトンネルのステータスが「停止」です。	NSX-T ホスト トランスポート ノードのトンネルのステータスが「停止」です。
1.3.6.1.4.1.6876.100.1.0.80232	NSXHostNodeTunnelStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードのトンネルのステータスが「劣化」です。	NSX-T ホスト トランスポート ノードのトンネルのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80233	NSXHostNodeTunnelStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードのトンネルのステータスが「不明」です。	NSX-T ホスト トランスポート ノードのトンネルのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80234	NSXHostNodeStatusDownEvent	警告	NSX-T ホスト トランスポート ノードのステータスが「切断」です。	NSX-T ホスト トランスポート ノードのステータスが「切断」です。
1.3.6.1.4.1.6876.100.1.0.80235	NSXHostNodeStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードのステータスが「劣化」です。	NSX-T ホスト トランスポート ノードのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80236	NSXHostNodeStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードのステータスが「不明」です。	NSX-T ホスト トランスポート ノードのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	最重要	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「切断」です。	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「切断」です。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	最重要	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「劣化」です。	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	最重要	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「不明」です。	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	最重要	NSX-T Edge トランスポート ノードのトンネルのステータスが「停止」です。	NSX-T Edge トランスポート ノードのトンネルのステータスが「停止」です。
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradeEvent	最重要	NSX-T Edge トランスポート ノードのトンネルのステータスが「劣化」です。	NSX-T Edge トランスポート ノードのトンネルのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	最重要	NSX-T Edge トランスポート ノードのトンネルのステータスが「不明」です。	NSX-T Edge トランスポート ノードのトンネルのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	最重要	NSX-T Edge トランスポート ノードのステータスが「切断」です。	NSX-T Edge トランスポート ノードのステータスが「切断」です。
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	最重要	NSX-T Edge トランスポート ノードのステータスが「劣化」です。	NSX-T Edge トランスポート ノードのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	最重要	NSX-T Edge トランスポート ノードのステータスが「不明」です。	NSX-T Edge トランスポート ノードのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	警告	NSX-T ホスト ノードにマネージャが接続されていません	ホスト トランスポート ノードと NSX Manager の接続状態の同期が失われました
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	最重要	NSX-T Edge ノードのコントローラ接続が不明です。	NSX-T Edge ノードのコントローラ接続が不明です。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	警告	NSX-T ホスト ノードにコントローラが接続されていません	NSX-T ホスト ノードは、どのコントローラとも通信できません。
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	警告	NSX-T ホスト ノードのコントローラの接続が低下しました	NSX-T ホスト ノードが 1 台以上のコントローラと通信できません。
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	警告	NSX-T ホスト ノードのコントローラ接続が不明です。	NSX-T ホスト ノードのコントローラ接続が不明です。
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	警告	NSX-T 論理スイッチの管理ステータスが「切断」です	NSX-T 論理スイッチの管理ステータスが「切断」です
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	最重要	NSX-T 論理ポートの動作ステータスが「切断」です	NSX-T 論理ポートの動作ステータスが「切断」です。これにより、同じ論理スイッチに接続された 2 つの仮想インターフェイス (VIF) 間で、仮想マシンから別の仮想マシンに ping を実行できなくなるなどの通信障害が発生する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	警告	NSX-T 論理ポートの動作ステータスが「不明」です	NSX-T 論理ポートの動作ステータスが「不明」です。これにより、同じ論理スイッチに接続された 2 つの仮想インターフェイス (VIF) 間で、仮想マシンから別の仮想マシンに ping を実行できなくなるなどの通信障害が発生する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	警告	NSX-T コンピュート マネージャの接続ステータスが接続中ではありません	NSX-T コンピュート マネージャの接続ステータスが接続中ではありません

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackupDisabledEvent	警告	NSX-T Manager のバックアップがスケジュール設定されていません。	NSX-T Manager のバックアップがスケジュール設定されていません
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	最重要	NSX-T DFW ファイアウォールが無効になっています。	分散ファイアウォールが NSX-T Manager で無効になっています
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	警告	NSX-T 論理ポートで受信パケットがドロップされています。	NSX-T 論理ポートで受信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	警告	NSX-T 論理ポートで送信パケットがドロップされています。	NSX-T 論理ポートで送信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	警告	NSX-T 論理スイッチで受信パケットがドロップされています	NSX-T 論理スイッチで受信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	警告	NSX-T 論理スイッチで送信パケットがドロップされています	NSX-T 論理スイッチで送信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	警告	NSX-T 管理ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T 管理ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは NSX-T 管理クラスタに関連するネットワーク トラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	最重要	NSX-T Edge ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T Edge ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは、Edge クラスタのネットワーク トラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	警告	NSX-T ホスト ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T ホスト ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは ESXi ホストのネットワーク トラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	警告	NSX-T 管理ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T 管理ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは NSX-T 管理クラスタに関連するネットワーク トラフィックに影響する可能性があります。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	最重要	NSX-T Edge ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T Edge ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは、Edge クラスターのネットワーク トラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	警告	NSX-T ホスト ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T ホスト ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは ESXi ホストのネットワーク トラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80301	vmwHardwareVTEPMismatchEvent	最重要	HardwareVTEPMismatchEvent	ハードウェア ゲートウェイのバインドが一致しません
1.3.6.1.4.1.6876.100.1.0.80302	vmwHardwareVTEPPortDownEvent	最重要	HardwareVTEPPortDownEvent	ハードウェア ゲートウェイのポートが停止しています
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmInventoryStatusEvent	警告	CM インベントリ サービスが実行を停止しました	CM インベントリ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmInventoryStatusEvent	最重要	CM インベントリ サービスが停止しました	NSX-T 管理ノードのサービスの 1 つである CM インベントリ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	警告	コントローラ サービスが実行を停止しました。	コントローラ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	最重要	コントローラ サービスが停止しました	NSX-T 管理ノードのサービスの 1 つであるコントローラ サービスが実行を停止しました。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	警告	データストア サービスが実行を停止しました。	データストア サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	最重要	データストア サービスが停止しました	NSX-T 管理ノードのサービスの1つであるデータストア サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	警告	HTTP サービスが実行を停止しました。	HTTP サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	最重要	HTTP サービスが停止しました	NSX-T 管理ノードのサービスの1つである HTTP サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	警告	アップグレード インストール サービスが実行を停止しました。	アップグレード インストール サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	警告	インストール アップグレード サービスが停止しました	NSX-T 管理ノードのサービスの1つであるインストール アップグレード サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	警告	Liagent サービスが実行を停止しました。	Liagent サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	警告	Liagent サービスが停止しました	NSX-T 管理ノードのサービスの1つである LI エージェント サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	警告	マネージャ サービスが実行を停止しました。	マネージャ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	最重要	マネージャ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるマネージャ サービスが実行を停止しました。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	警告	管理プレーン サービスが実行を停止しました。	管理サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	警告	管理プレーン サービスが停止しました	NSX-T 管理ノードのサービスの1つである管理プレーン バス サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	警告	移行コーディネータ サービスが実行を停止しました。	移行コーディネータ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	警告	移行コーディネータ サービスが停止しました	NSX-T 管理ノードのサービスの1つである移行コーディネータ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	警告	ノード管理サービスが実行を停止しました。	ノード管理 サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	最重要	ノード管理サービスが停止しました	NSX-T 管理ノードのサービスの1つであるノード管理サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	警告	ノード統計サービスが実行を停止しました。	ノード統計サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	最重要	ノード統計サービスが停止しました	NSX-T 管理ノードのサービスの1つであるノード統計サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	警告	メッセージ バス サービスが実行を停止しました。	メッセージ バス クライアント サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	警告	メッセージ バス サービスが停止しました	NSX-T 管理ノードのサービスの1つであるメッセージ バス サービスが実行を停止しました。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	警告	プラットフォーム クライアント サービスが実行を停止しました。	プラットフォーム クライアント サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	最重要	プラットフォーム クライアント サービスが停止しました	NSX-T 管理ノードのサービスの1つであるプラットフォーム クライアント サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	警告	エージェント アップグレード サービスが実行を停止しました。	アップグレード サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	警告	アップグレード エージェント サービスが停止しました	NSX-T 管理ノードのサービスの1つであるアップグレード エージェント サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	警告	NTP サービスが実行を停止しました。	NTP サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	最重要	NTP サービスが停止しました	NSX-T 管理ノードのサービスの1つである NTP サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	警告	ポリシー サービスが実行を停止しました。	ポリシー サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	最重要	ポリシー サービスが停止しました	NSX-T 管理ノードのサービスの1つであるポリシー サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	警告	検索サービスが実行を停止しました。	検索サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	最重要	検索サービスが停止しました	NSX-T 管理ノードのサービスの1つである検索サービスが実行を停止しました。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	警告	SNMP サービスが実行を停止しました。	SNMP サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	警告	SNMP サービスが停止しました	NSX-T 管理ノードのサービスの1つである SNMP サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	警告	SSH サービスが実行を停止しました。	SSH サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	最重要	SSH サービスが停止しました	NSX-T 管理ノードのサービスの1つである SSH サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	警告	Syslog サービスが実行を停止しました。	Syslog サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	最重要	Syslog サービスが停止しました	NSX-T 管理ノードのサービスの1つである Syslog サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	警告	テレメトリ サービスが実行を停止しました。	テレメトリ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	警告	テレメトリ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるテレメトリ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	警告	ユーザー インターフェイス サービスが実行を停止しました。	ユーザー インターフェイス サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	最重要	ユーザー インターフェイス サービスが停止しました	NSX-T 管理ノードのサービスの1つであるユーザー インターフェイス サービスが実行を停止しました。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeServiceClusterManagerStatusEvent	最重要	クラスター マネージャ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるクラスター マネージャ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80501	vmwIndexerLagEvent	最重要	インデクサ遅延イベント	最新のデータはまだインデックス処理中です。検索結果が不正確になることがあります。
1.3.6.1.4.1.6876.100.1.0.80502	vmwIPFIXFlowDPPausedEvent	最重要	IPFIX フロー データ ソースが一時停止したというイベント	フロー数が多いため、IPFIX フロー データ ソースが一時停止しました。
1.3.6.1.4.1.6876.100.1.0.80503	vmwGridProcessingStoppedEvent	最重要	グリッド処理が停止しているというイベント	グリッド処理が停止しました。
1.3.6.1.4.1.6876.100.1.0.80504	vmwUnableToSendEmailsEvent	最重要	E メールを送信できないというイベント	E メール メッセージを送信できません。
1.3.6.1.4.1.6876.100.1.0.80505	vmwSMTPNotConfiguredEvent	最重要	SMTP が設定されていないというイベント	SMTP が設定されていない
1.3.6.1.4.1.6876.100.1.0.80506	vmwSNMPNotConfiguredEvent	最重要	システム健全性イベント	SNMP ターゲットが設定されていません。
1.3.6.1.4.1.6876.100.1.0.80507	vmwReindexingInProgressEvent	最重要	インデックス処理が進行中であるというイベント	データは現在、再インデックス処理中です。検索サービスは、この移行アクティビティの完了後に使用できるようになります。
1.3.6.1.4.1.6876.100.1.0.80508	vmwNodesVersionMismatchEvent	最重要	ノード バージョン不一致イベント	ノード バージョンの不一致が検出されました
1.3.6.1.4.1.6876.100.1.0.80509	vmwNotAllServicesRunningEvent	最重要	実行中でないサービスあるというイベント	1つ以上の重要なサービスが実行されていません。
1.3.6.1.4.1.6876.100.1.0.80510	vmwNotAllServicesHealthyEvent	最重要	良好でないサービスがあるというイベント	1つ以上の重要なサービスが良好な状態ではありません。
1.3.6.1.4.1.6876.100.1.0.80511	vmwExpandPartitionFailedEvent	最重要	パーティションの拡張に失敗したというイベント	ディスク パーティションの拡張に失敗しました。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80512	vmwDiskCleanupFailedEvent	最重要	ディスク クリーンアップに失敗したというイベント	ディスク クリーンアップ サービスが不良な状態です。
1.3.6.1.4.1.6876.100.1.0.80513	vmwVacuumFailedEvent	最重要	vacuum に失敗したというイベント	PostgreSQL Vacuum サービスが不良な状態です。
1.3.6.1.4.1.6876.100.1.0.80514	vmwConfigStoreCleanupFailedEvent	最重要	ストアのクリーンアップの設定に失敗したというイベント	データ保持 (設定ストアのメンテナンス) サービスが不良な状態です。
1.3.6.1.4.1.6876.100.1.0.80515	vmwHBaseRetentionToolFailedEvent	最重要	HBASE 保持ツールに失敗したというイベント	データ保持 (メトリック保持設定) サービスが不良な状態です。
1.3.6.1.4.1.6876.100.1.0.80516	vmwMetricStoreUpdaterFailedEvent	最重要	メトリック ストア更新機能に失敗したというイベント	データ保持 (メトリック ストアのメンテナンス) サービスが不良な状態です。
1.3.6.1.4.1.6876.100.1.0.80517	vmwCollectorLagEvent	最重要	コレクタ遅延イベント	コレクタの前のデータ収集がしきい値より前に行われました
1.3.6.1.4.1.6876.100.1.0.80518	vmwCollectionLagEvent	最重要	収集遅延イベント	データ ソースの前のデータ収集がしきい値よりも前に行われました
1.3.6.1.4.1.6876.100.1.0.80519	vmwGridProcessingLagEvent	最重要	グリッド処理遅延イベント	グリッド処理の遅れがしきい値を超えています
1.3.6.1.4.1.6876.100.1.0.80520	vmwConnectionErrorEvent	最重要	接続エラー イベント	データ ソースへの接続中にエラーが発生しました
1.3.6.1.4.1.6876.100.1.0.80521	vmwNodeNotActiveEvent	最重要	ノードがアクティブでないというイベント	ノードがアクティブではありません
1.3.6.1.4.1.6876.100.1.0.80522	vmwHighDiskUtilizationEvent	最重要	ディスク使用率が高いというイベント	ディスク使用率が高くなっています
1.3.6.1.4.1.6876.100.1.0.80523	vmwIndexingAbortedEvent	最重要	インデックスが中止されたというイベント	インデックスが中止されました
1.3.6.1.4.1.6876.100.1.0.80524	vmwUpgradeFailedEvent	最重要	アップグレードに失敗したというイベント	アップグレードに失敗しました
1.3.6.1.4.1.6876.100.1.0.80525	vmwFlowProcessingSuspendedEvent	最重要	フロー処理がサスペンドされているというイベント	フロー処理がサスペンドされました

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80526	vmwLargeSdmsDroppedEvent	最重要	データ処理中のエラー	SDMS が大量にドロップされました
1.3.6.1.4.1.6876.100.1.0.80527	vmwApplianceNotConfiguredEvent	最重要	アプライアンスが構成されていないイベント	コレクタ仮想マシンの構成が不完全です。
1.3.6.1.4.1.6876.100.1.0.80531	vmwFdbConfigStoreCleanupFailedEvent		FDB_CONFIG_STORE_CLEANUP_FAILED_EVENT	FDB 構成ストアのクリーンアップに失敗したというイベント
1.3.6.1.4.1.6876.100.1.0.80531	vmwDiskAllocationInsufficientEvent	情報	DISK_ALLOCATION_INSUFFICIENT_EVENT	ディスクが構成されていないイベント
1.3.6.1.4.1.6876.100.1.0.80601	vmwFailedEvent	最重要	データ ソースに失敗したというイベント	データ ソースに失敗しました
1.3.6.1.4.1.6876.100.1.0.80602	vmwTimeoutEvent	最重要	データ ソース タイムアウト イベント	データ ソースのタイムアウト
1.3.6.1.4.1.6876.100.1.0.80603	vmwConnectionRefusedEvent	最重要	接続が拒否されたというイベント	接続が拒否されました
1.3.6.1.4.1.6876.100.1.0.80605	vmwIncorrectConnectionStringEvent	最重要	接続文字列が不正であるというイベント	接続文字列が正しくありません
1.3.6.1.4.1.6876.100.1.0.80606	vmwInvalidCredentialsEvent	最重要	認証情報が無効であるというイベント	無効な認証情報
1.3.6.1.4.1.6876.100.1.0.80608	vmwUnknownHostEvent	最重要	ホストが不明であるというイベント	不明なホスト
1.3.6.1.4.1.6876.100.1.0.80609	vmwSNMPConnectionInvalidEvent	最重要	SNMP 接続が無効であるというイベント	SNMP 接続が無効です
1.3.6.1.4.1.6876.100.1.0.80610012	vmwPwdAuthModeDisabledAristaEvent	最重要	パスワード認証が無効であるというイベント	パスワード認証が無効です
1.3.6.1.4.1.6876.100.1.0.80610018	vmwUnsupportedNSXVersionEvent	最重要	NSX バージョンがサポートされていないというイベント	NSX バージョンがサポートされていません
1.3.6.1.4.1.6876.100.1.0.80611	vmwFailedCredentialsEncryptEvent	最重要	認証情報の暗号化に失敗したというイベント	認証情報の暗号化に失敗しました
1.3.6.1.4.1.6876.100.1.0.80612	vmwPwdAuthModeDisabledEvent	最重要	パスワード認証モードが無効であるというイベント	パスワード認証モードが無効です
1.3.6.1.4.1.6876.100.1.0.80613	vmwInsufficientPrivilegesEvent	最重要	権限不足イベント	権限が適切ではありません
1.3.6.1.4.1.6876.100.1.0.8061313	vmwFlowCollectionErrorEvent	最重要	フロー収集エラー イベント	フロー収集エラー

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.8061314	vmwAWSThrottlingExceptionEvent	最重要	AWS スロットリングの例外イベント	AWS スロットリングの例外
1.3.6.1.4.1.6876.100.1.0.8061315	vmwAWSFlowLogAccessDeniedExceptionEvent	最重要	AWS フロー ログへのアクセス拒否の例外というイベント	AWS フロー ログのアクセス拒否の例外が発生しました。このイベントは、フロー ログを収集するために必要な権限がユーザーにない場合に発生します。
1.3.6.1.4.1.6876.100.1.0.80614	vmwNotFoundEvent	最重要	見つからないというイベント	見つかりません
1.3.6.1.4.1.6876.100.1.0.80616	vmwInvalidConfigEvent	最重要	データ ソース構成が無効であるというイベント	データ ソース構成が無効です
1.3.6.1.4.1.6876.100.1.0.80617	vmwWarnConfigEvent	最重要	データ ソース構成が無効であるというイベント	データ ソース構成が無効です
1.3.6.1.4.1.6876.100.1.0.80618	vmwUnexpectedDSTypeOrVersionEvent	最重要	予期しないデータソース タイプまたはバージョンのイベント	予期しないデータソース タイプまたはバージョン
1.3.6.1.4.1.6876.100.1.0.80619	vmwNSXControllerNotFoundEvent	最重要	NSX Controller が見つからないというイベント	NSX Controller が見つかりません
1.3.6.1.4.1.6876.100.1.0.80620	vmwHostNotReachableEvent	最重要	ホストにアクセスできないというイベント	ホストにアクセスできません
1.3.6.1.4.1.6876.100.1.0.80621	vmwInvalidResponseFromDataSourceEvent	最重要	データ ソースからの応答が無効であるというイベント	データ ソースからの応答が無効です
1.3.6.1.4.1.6876.100.1.0.80622	vmwDataProviderNotRunningEvent	最重要	データ ソースが実行されていないというイベント	データ ソースが実行されていません
1.3.6.1.4.1.6876.100.1.0.80623	vmwPrimaryNSXNotAddedEvent	最重要	プライマリ NSX が追加されていないというイベント	プライマリ NSX が追加されていません
1.3.6.1.4.1.6876.100.1.0.80624	vmwHostnameResolutionErrorEvent	最重要	ホスト名解決エラー イベント	ホスト名解決エラー
1.3.6.1.4.1.6876.100.1.0.80625	vmwNumVMsOrHostsNotFoundEvent	最重要	見つからなかった仮想マシンまたはホストの数のイベント	見つからなかった仮想マシンまたはホストの数
1.3.6.1.4.1.6876.100.1.0.80626	vmwNSXIPFIXStatusMismatchEvent	最重要	NSX IPFIX: ステータスが一致しないというイベント	NSX IPFIX のステータスが一致しません

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80627	vmwFlowPhysicalNodeEvent	最重要	フロー物理ノード イベント	フロー物理ノード
1.3.6.1.4.1.6876.100.1.0.80628	vmwNotEmptyNodeEvent	最重要	空でないノードというイベント	空でないノード
1.3.6.1.4.1.6876.100.1.0.80629	vmwUnsupportedNSXTVersionEvent	最重要	NSXT バージョンがサポートされていないというイベント	NSXT バージョンがサポートされていない
1.3.6.1.4.1.6876.100.1.0.80630	vmwComputeManagersNotFoundEvent	最重要	コンピューター マネージャーが見つからないというイベント	コンピューター マネージャーが見つかりません
1.3.6.1.4.1.6876.100.1.0.80631	vmwComputeManagersNotAddedEvent	最重要	コンピューター マネージャーが追加されていないというイベント	コンピューター マネージャーが追加されていません
1.3.6.1.4.1.6876.100.1.0.80632	vmwUnsupportedLogInsightVersionEvent	最重要	Log Insight のバージョンがサポートされていないというイベント	Log Insight のバージョンはサポートされていません
1.3.6.1.4.1.6876.100.1.0.80633	vmwUnsupportedVRNICContentPackVersionEvent	最重要	vRealize Network Insight Content Pack のバージョンがサポートされていないというイベント	vRealize Network Insight Content Pack のバージョンはサポートされていません
1.3.6.1.4.1.6876.100.1.0.80634	vmwVRNICContentPackNotInstalledEvent	最重要	vRealize Network Insight Content Pack が Log Insight イベントに見つからないというイベント	vRealize Network Insight Content Pack が Log Insight に見つかりません
1.3.6.1.4.1.6876.100.1.0.80635	vmwWebhookNotEnabledOnAlertEvent	最重要	Network Insight アラートに関して Webhook が有効でないというイベント	Log Insight 内の vRealize Network Insight Content Pack の 1 つまたは複数のアラートに対する webhook が有効ではありません
1.3.6.1.4.1.6876.100.1.0.80636	vmwIncorrectWebhookConfiguredOnAlertEvent	最重要	Log Insight アラートに設定されている Webhook URL が不正であるというイベント	Log Insight 内の vRealize Network Insight Content Pack の 1 つまたは複数のアラートに対して、不正な webhook 構成が見つかりました

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80637	vmwWebhookNotRunningEvent	最重要	Webhook がコレクタ (プロキシ) 仮想マシン上で実行されていないというイベント	Webhook がコレクタ (プロキシ) 仮想マシン上で実行されていません
1.3.6.1.4.1.6876.100.1.0.80638	vmwInfobloxRecordLimitExceededEvent	最重要	Infoblox のレコード数が現在の制限を超えています	Infoblox のレコード数が現在の制限を超えています
1.3.6.1.4.1.6876.100.1.0.80639	vmwIncorrectInfobloxCredentialEvent	最重要	Infoblox 認証情報不正イベント	Infoblox の認証情報が無効であるか、Infoblox データにアクセスするための「API 権限」をユーザーが持っていない
1.3.6.1.4.1.6876.100.1.0.80640	vmwUnsupportedInfobloxVersionEvent	最重要	Infoblox バージョンがサポートされていないというイベント	NIOS のバージョンがサポートされていません。
1.3.6.1.4.1.6876.100.1.0.80641	vmwUnknownInfobloxVersionEvent	最重要	Infoblox バージョンが不明であるというイベント	NIOS のバージョンを特定できません。
1.3.6.1.4.1.6876.100.1.0.80642	vmwNoDVSAvailableEvent	最重要	IPFIX を有効にできないというイベント	DVS が見つからないため、IPFIX を有効にできません
1.3.6.1.4.1.6876.100.1.0.80643	vmwVCNotOnSameProxyEvent	最重要	NSX Manager と vCenter Server データソースが同じコレクタ仮想マシン上になしイベント	NSX Manager および関連付けられた vCenter Server のデータソースが同じコレクタ仮想マシン上にありません。
1.3.6.1.4.1.6876.100.1.0.80644	vmwNSXTIPFixNoCollectorProfileEvent	最重要	NSX-T IPFIX: コレクタ プロファイルがないというイベント	NSXT IPFIX: コレクタ プロファイルがありません
1.3.6.1.4.1.6876.100.1.0.80645	vmwNSXTIPFixNoNewCollectorProfileCanBeAddedEvent	最重要	NSX-T IPFIX: 追加できる新しいコレクタ プロファイルがないというイベント	NSXT IPFIX: 追加できる新しいコレクタ プロファイルがありません
1.3.6.1.4.1.6876.100.1.0.80646	vmwNSXTIPFixNoIPFixProfileEvent	最重要	NSX-T IPFIX: IPFIX プロファイルがないというイベント	NSXT IPFIX: Ipfix プロファイルがありません
1.3.6.1.4.1.6876.100.1.0.80647	vmwNSXTIPFixIpfixProfilePriorityNotZeroEvent	最重要	NSX-T IPFIX: Ipfix プロファイルの優先順位がゼロでないというイベント	NSXT IPFIX の Ipfix プロファイルの優先順位がゼロではありません

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80648	vmwNSXTIPFixCollectorAndIPFixProfileMismatchEvent	最重要	NSX-T IPFIX: コレクタおよび IPFIX プロファイルが一致しないというイベント	NSXT IPFIX コレクタと Ipfix プロファイルが一致しません
1.3.6.1.4.1.6876.100.1.0.80649	vmwNSXTIPFixPortIncorrectEvent	最重要	NSX-T IPFIX コレクタ ポートが正しくないというイベント	コレクタ プロファイルのコレクタ ポートが正しくありません
1.3.6.1.4.1.6876.100.1.0.80650	vmwNSXTIPFixDFWStatusNotEnabledEvent	最重要	NSX-T IPFIX: DFW が有効でないというイベント	NSX-T IPFIX: DFW が有効になっていません
1.3.6.1.4.1.6876.100.1.0.80651	vmwPolicyManagerNoDfwIPFixProfile	最重要	DFW IPFIX プロファイルが NSX Policy Manager 上にないというイベント。	NSX Policy Manager に DFW IPFIX プロファイルが見つかりません
1.3.6.1.4.1.6876.100.1.0.80652	vmwPolicyManagerVrniDfwIPFixCollectorAbsent	最重要	Network Insight IPFIX コレクタの設定が NSX Policy Manager がないというイベントです。	Network Insight IPFIX コレクタの IP アドレスとポートが、NSX Policy Manager の DFW IPFIX コレクタ プロファイルに含まれていません。
1.3.6.1.4.1.6876.100.1.0.80653	vmwDataSourceIdentificationChangedEvent	情報	データ ソースの ID 情報が変更されました	証明書やキーなどのデータ ソース ID 情報が変更されました。
1.3.6.1.4.1.6876.100.1.0.80654	vmwPKSKubernetesUnknownHostEvent	最重要	Kubernetes クラスター API サーバにアクセスできないというイベント	PKS 内の 1 つ以上の Kubernetes クラスターの Kube 構成ファイルが有効ではありません。
1.3.6.1.4.1.6876.100.1.0.80655	vmwKubernetesInsufficientPrivilegesEvent	最重要	Kubernetes クラスター サービス アカウントに適切な権限がありません	1 つ以上の Kubernetes クラスター サービス アカウントに適切な権限がありません。
1.3.6.1.4.1.6876.100.1.0.80657	vmwUANIFileNotProvidedEvent	最重要	汎用ルーターと汎用スイッチのデータ ソースに必要なファイルが指定されていません	汎用ルーターと汎用スイッチのデータ ソースに必要なファイルが指定されていません

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80658	vmwUANIFileDoesNotExistEvent	最重要		汎用ルーターと汎用スイッチのデータ ソースに必要なファイルがありません
1.3.6.1.4.1.6876.100.1.0.80659	vmwNSXTLatencyNotEnabledEvent	最重要	NSXT_LATENCY_NOT_ENABLED_EVENT	NSX-T 遅延の収集が有効ではありません
1.3.6.1.4.1.6876.100.1.0.80660	vmwNSXTLatencyMoreBFDProfileEvent		NSXT_LATENCY_MORE_BFD_PROFILE_EVENT	
1.3.6.1.4.1.6876.100.1.0.80662	vmwNSXTLatencyCollectorMismatchEvent	最重要	NSXT_LATENCY_COLLECTOR_MISMATCH_EVENT	NSX-T 遅延コレクタが設定されていません
1.3.6.1.4.1.6876.100.1.0.80663	vmwBigIplInsufficientShellAccessEvent	最重要	BIGIP_INSUFFICIENT_SHELL_ACCESS_EVENT	シェルにアクセスできません
1.3.6.1.4.1.6876.100.1.0.80664	vmwBigIplInsufficientPartitionAccessEvent	最重要	BIGIP_INSUFFICIENT_PARTITION_ACCESS_EVENT	パーティション アクセス権が不十分です
1.3.6.1.4.1.6876.100.1.0.80665	vmwBigIplInsufficientRoleEvent	最重要	BIGIP_INSUFFICIENT_ROLE_EVENT	ロールが不十分です
1.3.6.1.4.1.6876.100.1.0.90001	vmwVeloCloudEdgeDownEvent	警告	VeloCloud Edge が健全ではありません	VeloCloud Edge の Edge 状態は未接続です。
1.3.6.1.4.1.6876.100.1.0.90002	vmwVeloCloudLinkDownEvent	警告	VeloCloud リンクが健全ではありません	VeloCloud Edge のリンク状態は未接続です。
1.3.6.1.4.1.6876.100.1.0.90005	vmwVeloCloudLinkLostPacketEventTx	最重要	VeloCloud リンクのアップストリームでのパケット ロスがしきい値を超えています。	VeloCloud リンクのパケット ロス イベント Tx。
1.3.6.1.4.1.6876.100.1.0.90007	vmwVeloCloudLinkDegradedVoiceQoeEvent	最重要	VeloCloud リンクの音声 QOE が劣化しました。	VeloCloud リンクの音声 QOE 劣化イベント。
1.3.6.1.4.1.6876.100.1.0.90008	vmwVeloCloudLinkDegradedVideoQoeEvent	最重要	VeloCloud リンクのビデオ QOE が劣化しました。	VeloCloud リンクのビデオ QoE 劣化イベント。
1.3.6.1.4.1.6876.100.1.0.90009	vmwVeloCloudLinkDegradedTransactionsQoeEvent	最重要	VeloCloud リンクのトランザクション QOE が劣化しました。	VeloCloud リンクのトランザクション QOE 劣化イベント。

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.90010	vmwVeloCloudEdgeDegradedVoiceQoeEvent	最重要	VeloCloud Edge の音声 QOE が劣化しました。	VeloCloud Edge のボイス QoE 劣化イベント。
1.3.6.1.4.1.6876.100.1.0.90011	vmwVeloCloudEdgeDegradedVideoQoeEvent	最重要	VeloCloud Edge のビデオ QOE が劣化しました。	VeloCloud Edge のビデオ QoE 劣化イベント。
1.3.6.1.4.1.6876.100.1.0.90012	vmwVeloCloudEdgeDegradedTransQoeEvent	最重要	VeloCloud Edge のトランザクション QOE が劣化しました。	VeloCloud Edge のトランザクション QoE 劣化イベント。
1.3.6.1.4.1.6876.100.1.0.90013	vmwVeloCloudLinkLostPacketEventRx	最重要	VeloCloud リンクのダウンストリームでのパケット ロスがしきい値を超えています。	VeloCloud リンクのパケット ロス イベント Rx。

システム イベントの表示と編集

イベントは、システムまたはユーザーのいずれかによって定義されます。システム イベントは、事前定義されたイベントです。

システム イベントは、[設定] の [システム イベント] 画面に一覧表示されます。各イベントには、次のフィールドが指定されます。イベント列を除いた次のすべての列で、要件に基づいて情報をフィルタできます。

表 6-2.

列	説明
イベント	このフィールドは、イベントの名前を指定します。
重大度	このフィールドは、イベントの重大度を指定します。次の値を設定できます。 <ul style="list-style-type: none"> ■ 最重要 ■ 中程度 ■ 警告 ■ 情報
タイプ	このフィールドは、イベントが [問題] を示すか [変更] を示すかを指定します。 注： タイプが [問題] のすべてのイベントが Syslog に記録されます。
エンティティ	このフィールドは、対象のイベントがイベント生成で包含エンティティとして設定されるか、除外エンティティとして設定されるかを指定します。デフォルトの値は All です。

表 6-2. (続き)

列	説明
通知	このフィールドは、送信される通知のタイプを指定します。通知は、Eメールか SNMP トラップ、または両方を使用して送信できます。 注： すべての重要なシステム定義のイベントに対して通知を有効にする必要があります。すべての重要なシステム イベントのリストを取得するには、システム イベントを重大度でソートします。
有効	このオプションは、イベントが有効な場合に選択されます。

各イベント上にマウス ポインタを置くと、[詳細情報] が表示されます。このオプションをクリックすると、そのイベントの説明、イベント タグ、およびエンティティ タイプが表示されます。

システム イベントでは、次のタスクを実行できます。

- イベントの編集
- 一括編集の実行
- 特定のエンティティでのイベントの無効化

システム イベントの編集

システム イベントを編集したり、指定したシステム イベントの通知を定義したりできます。

手順

- 1 特定のイベントの [有効] 列の隣にある編集アイコンをクリックします。
- 2 必要に応じて、イベント タグを追加または削除します。
- 3 重大度を変更します。
- 4 選択したエンティティでイベントを有効または無効にする場合は、エンティティの包含/除外を選択します。
 - 包含ルールを作成するには、次のようにします。
 - a [包含リスト] を選択します。
 - b イベント用に含めるエンティティを [条件] で指定します。
 - 除外ルールを作成するには、次のようにします。
 - a [除外リスト] を選択します。
 - b イベント用に除外するエンティティを [条件] で指定します。

注：

- 包含リストおよび除外リストの両方に複数のルールを作成できます。
- NSX Manager を選択した場合、両方のリストに例外を追加できます。包含または除外のルールで特定のエンティティに対する例外を保持する場合は、例外を定義できます。
- また、エンティティを包含または除外するための独自のクエリを記述して、Custom Search を指定することもできます。

- 5 通知の送信が必要な場合は、[通知の有効化] チェック ボックスを選択します。設定に応じて、次の操作を行います。

オプション	アクション
メール サーバを構成していない場合	[メール サーバを設定] をクリックします。メール サーバの構成方法については、 メール サーバを設定 を参照してください。
SNMP トラップを構成していない場合	[SNMP トラップの構成] をクリックします。SNMP トラップの構成方法については、 SNMP トラップ先の設定 を参照してください。
メール サーバをすでに構成している場合	[E メールの頻度] ドロップダウン メニューで E メールを受信する頻度を指定し、[通知メールの送信先] テキスト ボックスにメール アドレスを指定します。
SNMP トラップをすでに構成している場合	[SNMP トラップの送信先] ドロップダウン メニューで 1 つ以上の SNMP トラップ先を選択します。SNMP トラップ先は 4 つまで選択できます。

- 6 [送信] をクリックします。

イベントでの一括編集の実行

- [システム イベント] 画面で複数のイベントを選択すると、[有効化]、[無効化]、[編集] のオプションがリストの上に表示されます。
- [編集] をクリックします。
- [編集] 画面には、次のオプションがあります。
 - [既存の値のオーバーライド]：このオプションでは、編集したフィールドのみが上書きされます。
 - [既存に追加]：このオプションでは、メール アドレスやイベント タグなどの既存の値に追加できます。
- [送信] をクリックします。

イベントの無効化

- ホームページの [未解決の問題] ウィジェットでイベントを選択できます。また、検索バーに「問題」[] と入力して、リストからイベントを選択することもできます。
- 特定のイベントを選択し、[アーカイブ] をクリックします。
- [今後このタイプのすべてのイベントを無効にする] を選択して、1 つのエントリまたはすべてのエントリを選択します。
- [保存] をクリックします。

注： 重要度、タグ、または包含/除外ルールに加えた変更は、今後のイベントに反映されます。既存のイベントでは、引き続き古い設定が表示されます。

イベントの制限事項

このセクションでは、さまざまなシステム定義イベントの制限について説明します。

先行するルールによってマスクされた分散ファイアウォール ルールのイベントの制限事項

このイベントには次の制限事項があります。

- このイベントは、NSX-V 分散ファイアウォール ルールでのみサポートされます。他のファイアウォール ベンダーはサポートされていません。
- 現在、以下のファイアウォール ルール プロパティがマスキング計算でサポートされています。
 - ソース
 - ターゲット
 - 適用先
 - サービス プロトコルとポート範囲
 - パケット タイプ
 - レイヤー 7 アプリケーション ID
- ソースまたはターゲットの反転を含むルールはサポートされていません。
- 無効にしたルールは無視されます。
- 除外されたメンバーが直接的または間接的に [ソース]、[ターゲット]、または [適用先] に含まれるセキュリティ グループを使用するルールはサポートされません。
- [ソース]、[ターゲット]、[適用先] の各プロパティのマスキング計算は、メンバー IPSet の固定メンバーシップと IP アドレス範囲の重なりに基づきます。セキュリティ グループの動的メンバーシップは、マスキングの対象と見なされません。

ユーザー定義イベントの編集

ユーザー定義のイベントは、検索に基づきます。

すべてのユーザー定義のイベントは、[設定] の [ユーザー定義のイベント] 画面に一覧表示されます。各イベントには、次のフィールドが指定されます。

表 6-3.

フィールド	説明
名前 (検索条件)	このフィールドでは、イベントの名前と、イベントの検索条件を指定します。
重大度	このフィールドでは、アラートの重要度を指定します。次の値を設定できます。 <ul style="list-style-type: none"> ■ 最重要 ■ 中程度 ■ 警告 ■ 情報
タイプ	このフィールドは、イベントが問題と変更のどちらを示しているかを指定します。
通知のタイミング	このフィールドでは、通知をいつ送信するかを指定します。

表 6-3. (続き)

フィールド	説明
作成者	このフィールドでは、イベントの作成者を指定します。
有効	このオプションは、イベントが有効な場合に選択されます。

イベントは編集または削除できます。編集の際に、Eメール通知のメールアドレスと頻度を指定できます。

ユーザー定義のイベントの構成

検索を利用して、ユーザー定義のイベントを作成できます。

手順

- 1 検索結果ウィンドウで、[通知の作成] アイコンをクリックします。
[ユーザー定義イベントの構成] 画面が開きます。
- 2 イベントの一意の名前を入力します。
- 3 チェック ボックスを選択してイベントを問題としてマークし、重要度を選択します。
- 4 一意の検索条件を入力します。
- 5 通知を受信する場合はその条件を選択する。
- 6 通知の頻度として、[即座] または [デイリー ダイジェストとして] を選択します。
- 7 メールアドレスを指定します。
- 8 SNMP サーバを設定するには、[SNMP トラップの構成] をクリックします。
SNMP サーバがすでに構成されている場合は、[SNMP トラップを IP アドレスに送信] を選択します。
[変更] をクリックして SNMP 設定を変更できます。
- 9 [保存] をクリックします。

プラットフォームの健全性イベントの表示

[プラットフォームの健全性イベント] 画面には、システム全体の健全性に関する詳細を示す全イベントがまとめて表示されます。これらのイベントは、インフラストラクチャ内のデータ ソースまたはノードで発生したイベントです。これらのイベントは、検索して確認することもできます。

表 6-4.

フィールド	説明
イベント	このフィールドは、イベントの名前を指定します。
重大度	このフィールドは、イベントの重大度を指定します。イベントの重大度を変更することはできません。

表 6-4. (続き)

フィールド	説明
タイプ	このフィールドは、イベントが問題と変更のどちらを示しているかを指定します。
通知	このフィールドは、送信される通知のタイプを指定します。通知は、Eメールか SNMP トラップ、または両方を使用して送信できます。

NSX-T イベント

vRealize Network Insight では、自己計算された NSX-T イベントが発生します。この他に、vRealize Network Insight には NSX-T によって生成されたすべてのシステム イベント (NSX-T バージョン 2.2 ~ 2.5) と NSX-T アラーム (NSX-T バージョン 3.0 以降) も表示されます。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	警告	NSX-T Tier-1 論理ルーターの切断イベント	NSX-T Tier-1 論理ルーターが Tier-0 ルーターから切断されています。このルーターの下位のネットワークに外部からアクセスすることはできず、その逆方向にアクセスすることもできません。
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	警告	ルーティングのアドバタイズが無効です	NSX-T Tier-1 論理ルーターでは、ルーティングのアドバタイズが無効になっています。このルーターの下位のネットワークには外部からアクセスできません。
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	最重要	NSX-T Edge ノードにマネージャが接続されていません	NSX-T Edge ノードにマネージャが接続されていません。
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	警告	NSX-T Edge ノードのコントローラの接続が低下しました	NSX-T Edge ノードが 1 台以上のコントローラと通信できません。
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	最重要	NSX-T Edge ノードにコントローラが接続されていません	NSX-T Edge ノードは、どのコントローラとも通信できません。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtuMismatchEvent	警告	NSX-T Tier-0 とアップリンク スイッチ / ルーター間で MTU が一致しません	Tier-0 論理ルーターのインターフェイスに設定された MTU が、同じ L2 ネットワーク内のアップリンク スイッチ/ルーターのインターフェイスと一致しません。これは、ネットワークのパフォーマンスに影響を与える可能性があります。
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	情報	1 台以上の仮想マシンが NSX-T DFW ファイアウォールから除外されました。	NSX-T DFW ファイアウォールで保護されていない仮想マシンが 1 台以上あります。vRealize Network Insight は、これらの仮想マシンの IPFIX フローを受信しません。
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	警告	アップリンク VLAN の設定が正しくありません	Tier-0 ルーターのアップリンク ポートの VLAN が外部ゲートウェイの VLAN と異なるため、通信は中断されます。
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	警告	トランスポート ノードに接続されているトランスポート ゾーンがありません。	トランスポート ノードに接続されたトランスポート ゾーンがありません。これが原因で、仮想マシンは接続に失敗した可能性があります。
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	警告	トランスポート ノードで使用できる VTEP がありません。	すべての VTEP がトランスポート ノードから削除されています。これが原因で、仮想マシンは接続に失敗した可能性があります。
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	最重要	NSX-T コントローラ ノードにコントロール クラスタが接続されていません	NSX-T コントローラ ノードでコントロール クラスタへの接続が失われました。
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	最重要	NSX-T コントローラ ノードに管理プレーンが接続されていません	NSX-T コントローラ ノードで管理プレーンへの接続が失われました。
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	最重要	NSX-T 管理ノードに管理クラスタが接続されていません	NSX-T 管理ノードで管理クラスタへの接続が失われました。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	警告	NSX-T ホスト ノードにマネージャが接続されていません	ホスト トランスポート ノードと NSX Manager の接続状態の同期が失われました
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	最重要	NSX-T Edge ノードのコントローラ接続が不明です。	NSX-T Edge ノードのコントローラ接続が不明です。
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	警告	NSX-T ホスト ノードにコントローラが接続されていません	NSX-T ホスト ノードは、どのコントローラとも通信できません。
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	警告	NSX-T ホスト ノードのコントローラの接続が低下しました	NSX-T ホスト ノードが 1 台以上のコントローラと通信できません。
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	警告	NSX-T ホスト ノードのコントローラ接続が不明です。	NSX-T ホスト ノードのコントローラ接続が不明です。
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「切断」です。	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「切断」です。
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「劣化」です	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「不明」です。	NSX-T ホスト トランスポート ノードの物理 NIC のステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	最重要	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「切断」です。	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「切断」です。
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	最重要	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「劣化」です。	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	最重要	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「不明」です。	NSX-T Edge トランスポート ノードの物理 NIC のステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	警告	NSX-T ホスト トランスポート ノードのトンネルのステータスが「停止」です。	NSX-T ホスト トランスポート ノードのトンネルのステータスが「停止」です。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードのトンネルのステータスが「劣化」です。	NSX-T ホスト トランスポート ノードのトンネルのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードのトンネルのステータスが「不明」です。	NSX-T ホスト トランスポート ノードのトンネルのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	最重要	NSX-T Edge トランスポート ノードのトンネルのステータスが「停止」です。	NSX-T Edge トランスポート ノードのトンネルのステータスが「停止」です。
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradeEvent	最重要	NSX-T Edge トランスポート ノードのトンネルのステータスが「劣化」です。	NSX-T Edge トランスポート ノードのトンネルのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	最重要	NSX-T Edge トランスポート ノードのトンネルのステータスが「不明」です。	NSX-T Edge トランスポート ノードのトンネルのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	警告	NSX-T ホスト トランスポート ノードのステータスが「切断」です。	NSX-T ホスト トランスポート ノードのステータスが「切断」です。
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	警告	NSX-T ホスト トランスポート ノードのステータスが「劣化」です。	NSX-T ホスト トランスポート ノードのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	警告	NSX-T ホスト トランスポート ノードのステータスが「不明」です。	NSX-T ホスト トランスポート ノードのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	最重要	NSX-T Edge トランスポート ノードのステータスが「切断」です。	NSX-T Edge トランスポート ノードのステータスが「切断」です。
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	最重要	NSX-T Edge トランスポート ノードのステータスが「劣化」です。	NSX-T Edge トランスポート ノードのステータスが「劣化」です。
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	最重要	NSX-T Edge トランスポート ノードのステータスが「不明」です。	NSX-T Edge トランスポート ノードのステータスが「不明」です。
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	警告	NSX-T 論理スイッチの管理ステータスが「切断」です。	NSX-T 論理スイッチの管理ステータスが「切断」です。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	最重要	NSX-T 論理ポートの動作ステータスが「切断」です	NSX-T 論理ポートの動作ステータスが「切断」です。これにより、同じ論理スイッチに接続された 2 つの仮想インターフェイス (VIF) 間で、仮想マシンから別の仮想マシンに ping を実行できなくなるなどの通信障害が発生する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	警告	NSX-T 論理ポートの動作ステータスが「不明」です	NSX-T 論理ポートの動作ステータスが「不明」です。これにより、同じ論理スイッチに接続された 2 つの仮想インターフェイス (VIF) 間で、仮想マシンから別の仮想マシンに ping を実行できなくなるなどの通信障害が発生する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	警告	NSX-T コンピュートマネージャの接続ステータスが接続中ではありません	NSX-T コンピュートマネージャの接続ステータスが接続中ではありません
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackupDisabledEvent	警告	NSX-T Manager のバックアップがスケジュール設定されていません。	NSX-T Manager のバックアップがスケジュール設定されていません
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	最重要	NSX-T DFW ファイアウォールが無効になっています。	分散ファイアウォールが NSX-T Manager で無効になっています
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	警告	NSX-T 論理ポートで受信パケットがドロップされています。	NSX-T 論理ポートで受信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	警告	NSX-T 論理ポートで送信パケットがドロップされています。	NSX-T 論理ポートで送信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	警告	NSX-T 論理スイッチで受信パケットがドロップされています	NSX-T 論理スイッチで受信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	警告	NSX-T 論理スイッチで送信パケットがドロップされています	NSX-T 論理スイッチで送信パケットがドロップされています。関連付けられたエンティティが影響を受ける可能性があります
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	警告	NSX-T 管理ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T 管理ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは NSX-T 管理クラスタに関連するネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	最重要	NSX-T Edge ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T Edge ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは、Edge クラスタのネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	警告	NSX-T ホスト ノードのネットワーク インターフェイスで受信パケットがドロップされています	NSX-T ホスト ノードのネットワーク インターフェイスで受信パケットがドロップされています。これは ESXi ホストのネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	警告	NSX-T 管理ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T 管理ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは NSX-T 管理クラスタに関連するネットワークトラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	最重要	NSX-T Edge ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T Edge ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは、Edge クラスタのネットワークトラフィックに影響する可能性があります。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	警告	NSX-T ホスト ノードのネットワーク インターフェイスで送信パケットがドロップされています	NSX-T ホスト ノードのネットワーク インターフェイスで送信パケットがドロップされています。これは ESXi ホストのネットワーク トラフィックに影響する可能性があります。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmlInventoryStatusEvent	警告	CM インベントリ サービスが実行を停止しました	CM インベントリ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	警告	コントローラ サービスが実行を停止しました。	コントローラ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	警告	データストア サービスが実行を停止しました。	データストア サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	警告	HTTP サービスが実行を停止しました。	HTTP サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	警告	アップグレード インストール サービスが実行を停止しました。	アップグレード インストール サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	警告	Liagent サービスが実行を停止しました。	Liagent サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	警告	マネージャ サービスが実行を停止しました。	マネージャ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	警告	管理プレーン サービスが実行を停止しました。	管理サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	警告	移行コーディネータ サービスが実行を停止しました。	移行コーディネータ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	警告	ノード管理サービスが実行を停止しました。	ノード管理 サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	警告	ノード統計サービスが実行を停止しました。	ノード統計サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	警告	メッセージ バス サービスが実行を停止しました。	メッセージ バス クライアント サービスのステータスが停止になりました。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	警告	プラットフォーム クライアント サービスが実行を停止しました。	プラットフォーム クライアント サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	警告	エージェント アップグレード サービスが実行を停止しました。	アップグレード サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	警告	NTP サービスが実行を停止しました。	NTP サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	警告	ポリシー サービスが実行を停止しました。	ポリシー サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	警告	検索サービスが実行を停止しました。	検索サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP サービスが実行を停止しました。	SNMP サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	警告	SSH サービスが実行を停止しました。	SSH サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	警告	Syslog サービスが実行を停止しました。	Syslog サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	警告	テレメトリ サービスが実行を停止しました。	テレメトリ サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	警告	ユーザー インターフェイス サービスが実行を停止しました。	ユーザー インターフェイス サービスのステータスが停止になりました。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmInventoryStatusEvent	最重要	CM インベントリ サービスが停止しました	NSX-T 管理ノードのサービスの1つである CM インベントリ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	最重要	コントローラ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるコントローラ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	最重要	データストア サービスが停止しました	NSX-T 管理ノードのサービスの1つであるデータストア サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	最重要	HTTP サービスが停止しました	NSX-T 管理ノードのサービスの1つである HTTP サービスが実行を停止しました。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	警告	インストール アップグレード サービスが停止しました	NSX-T 管理ノードのサービスの1つであるインストール アップグレード サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	警告	Liagent サービスが停止しました	NSX-T 管理ノードのサービスの1つである LI エージェント サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	最重要	マネージャ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるマネージャ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatus Event	警告	管理プレーン サービスが停止しました	NSX-T 管理ノードのサービスの1つである管理プレーン バス サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinator StatusEvent	警告	移行コーディネータ サービスが停止しました	NSX-T 管理ノードのサービスの1つである移行コーディネータ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEvent	最重要	ノード管理サービスが停止しました	NSX-T 管理ノードのサービスの1つであるノード管理サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEvent	最重要	ノード統計サービスが停止しました	NSX-T 管理ノードのサービスの1つであるノード統計サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	警告	メッセージ バス サービスが停止しました	NSX-T 管理ノードのサービスの1つであるメッセージ バス サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	最重要	プラットフォーム クライアント サービスが停止しました	NSX-T 管理ノードのサービスの1つであるプラットフォーム クライアント サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	警告	アップグレード エージェント サービスが停止しました	NSX-T 管理ノードのサービスの1つであるアップグレード エージェント サービスが実行を停止しました。

表 6-5. vRealize Network Insight NSX-T コンピューティング イベント (続き)

OID	イベント名	デフォルトの重要度	ユーザー インターフェイス名	説明
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	最重要	NTP サービスが停止しました	NSX-T 管理ノードのサービスの1つである NTP サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	最重要	ポリシー サービスが停止しました	NSX-T 管理ノードのサービスの1つであるポリシー サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	最重要	検索サービスが停止しました	NSX-T 管理ノードのサービスの1つである検索サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP サービスが停止しました	NSX-T 管理ノードのサービスの1つである SNMP サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	最重要	SSH サービスが停止しました	NSX-T 管理ノードのサービスの1つである SSH サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	最重要	Syslog サービスが停止しました	NSX-T 管理ノードのサービスの1つである Syslog サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	警告	テレメトリ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるテレメトリ サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	最重要	ユーザー インターフェイス サービスが停止しました	NSX-T 管理ノードのサービスの1つであるユーザー インターフェイス サービスが実行を停止しました。
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeService ClusterManagerStatusEvent	最重要	クラスター マネージャ サービスが停止しました	NSX-T 管理ノードのサービスの1つであるクラスター マネージャ サービスが実行を停止しました。

NSX-T システム イベント

以下に、vRealize Network Insight でサポートされている NSX-T 2.2 ~ 2.5 のイベントのリストを示します。これらのすべての NSX-T システム イベントのオブジェクト ID (OID) は、1.3.6.1.4.1.6876.100.1.0.80203 です。

表 6-6. NSX-T システム イベント

イベント名	説明
vmwNSXPlatformSysCpuUsage	マネージャと Edge アプライアンスの両方の CPU 使用率 (NSX-T 2.2)。
vmwNSXPlatformSysDiskUsage	マネージャと Edge アプライアンスの両方のディスク容量使用率 (/var/log パーティション) (NSX-T 2.2)。
vmwNSXPlatformSysMemUsage	マネージャと Edge アプライアンスの両方のメモリ使用率 (NSX-T 2.2)。
vmwNSXPlatformSysConfigDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (/config パーティション) (NSX-T 2.4)。
vmwNSXPlatformSysVarDumpDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (/var/dump パーティション) (NSX-T 2.5)。
vmwNSXPlatformSysRepositoryDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (/repository パーティション) (NSX-T 2.5)。
vmwNSXPlatformSysRootDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (ルート パーティション) (NSX-T 2.5)。
vmwNSXPlatformSysTmpDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (tmp パーティション) (NSX-T 2.5)。
vmwNSXPlatformSysImageDiskUsage	マネージャと Edge アプライアンスのディスク使用率 (/image パーティション) (NSX-T 2.5)。
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP プールの overloaded/normal (NSX-T 2.5)。
vmwNSXDhcpPoolLeaseAllocationFailedEvent	DHCP プールのリース割り当て失敗/成功 (NSX-T 2.5)。
vmwNSXPlatformPasswordExpiryStatus	マネージャのパスワード期限切れ (NSX-T 2.4)。
vmwNSXPlatformCertificateExpiryStatus	マネージャの証明書期限切れ (NSX-T 2.4)。
vmwNSXRoutingBgpNeighborStatus	BGP ネイバーのステータス (NSX-T 2.2)。
vmwNSXVpnTunnelState	VPN トンネルが動作/停止 (NSX-T 2.2)。
vmwNSXVpnL2TunnelStatus	L2 VPN セッションが動作/停止 (NSX-T 2.2)。
vmwNSXVpnIkeSessionStatus	IKE セッションが動作/停止 (NSX-T 2.2)。
vmwNSXDnsForwarderStatus	DNS フォワーダのステータス (NSX-T 2.4)。
vmwNSXClusterNodeStatus	クラスター ノードのステータス (NSX-T 2.4)。
vmwNSXFabricCryptoStatus	Edge 暗号化 MUX ドライバが Known_Answer_Tests (KAT) に失敗/合格 (NSX-T 2.4)。
マネージャのディスク使用率が良好ではありません	
BGP ネイバーが停止しています	BGP ネイバーが停止している場合はアラートが必要です。
BGP ネイバーが動作しています	ネイバーが起動するときに、アラームをクリアします。

表 6-6. NSX-T システム イベント (続き)

イベント名	説明
ストレージ使用率が X を超過	ストレージのアラームが X を超過 - すべてのアプライアンス仮想マシン (MP、CCP) またはトランスポート ノード (Edge、ホスト) でイベントが発生します。
メモリ使用率が X を超過	メモリのアラームが X を超過 - すべてのアプライアンス仮想マシン (MP、CCP) またはトランスポート ノード (Edge、ホスト) でイベントが発生します。
CPU 使用率が X を超過	CPU のアラームが X を超過 - すべてのアプライアンス仮想マシン (MP、CCP) またはトランスポート ノード (Edge、ホスト) でイベントが発生します。

NSX-T システム アラーム

注： これらのイベントに加えて、vRealize Network Insight 5.2 以降では、NSX-T 3.0 のすべてのアラームが NSX-T システム イベントとして表示されます。NSX-T によって生成されるアラームの完全なリストについては、https://NSX-T_IP_Address/nsx/#/app/home/alarms/alarm-definitions を参照してください。

Kubernetes イベント

vRealize Network Insight でサポートされている Kubernetes イベントのリストは次のとおりです。すべての Kubernetes イベントのオブジェクト ID (OID) は 1.3.6.1.4.1.6876.100.1.0.1510 です。

イベント名	重大度	説明
FailedToCreateContainer	最重要	コンテナの作成に失敗しました
FailedToStartContainer	最重要	コンテナの開始に失敗しました
PreemptContainer	警告	他のポッドを切断します。
BackOffStartContainer	警告	バックオフの再起動でコンテナが失敗しました。
ExceededGracePeriod	警告	コンテナのランタイムは、指定された猶予期間内にポッドを停止しませんでした。
FailedToKillPod	警告	ポッドの停止に失敗しました。
FailedToCreatePodContainer	中程度	ポッド コンテナの作成に失敗しました。
FailedToMakePodDataDirectories	中程度	ポッド データ ディレクトリの作成に失敗しました。
NetworkNotReady	警告 最重要	ネットワークの準備ができていません。
FailedScheduling	最重要	ポッドをスケジューリングすることができません
FailedToPullImage	警告 最重要	イメージのプルに失敗しました。
FailedToInspectImage	警告	イメージの検査に失敗しました。
ErrImageNeverPullPolicy	警告	イメージの NeverPull ポリシーに違反しています。

イベント名	重大度	説明
ImagePullBackOff	最重要	コンテナ イメージのプルに失敗しました。Kubelet はイメージ プルをバックオフしています
ImageInspectError	警告	イメージを検証できません
ErrImagePull	最重要	イメージ プル エラー
ErrImageNeverPull	最重要	ホストに必要なイメージがないため、PullPolicy は NeverPullImage です
RegistryUnavailable	最重要	レジストリからイメージをプルするときに HTTP エラーが発生します
InvalidImageName	最重要	イメージ名を解析できません
KubeletSetupFailed	中程度	Kubelet のセットアップに失敗しました。
FailedAttachVolume	最重要	ボリュームの接続に失敗しました。
FailedMountVolume	最重要	ボリュームのマウントに失敗しました。
VolumeResizeFailed	警告	ボリュームの拡張または縮小に失敗しました。
FileSystemResizeFailed	警告	ファイル システムの拡張または縮小に失敗しました。
FailedMapVolume	最重要	ボリュームのマッピングに失敗しました。
WarnAlreadyMountedVolume	警告	ボリュームはすでにマウントされています。
ContainerGCFailed	警告	コンテナのガーベジ コレクションに失敗しました。
ImageGCFailed	警告	イメージのガーベジ コレクションに失敗しました。
FailedNodeAllocatableEnforcement	警告	システムで予約済みの Cgroup の制限を適用できませんでした。
FailedCreatePodSandBox	警告	ポッド サンドボックスの作成に失敗しました。
FailedStatusPodSandBox	警告	ポッド サンドボックスのステータスが失敗しました。
InvalidDiskCapacity	中程度	ディスク容量が無効です。
FreeDiskSpaceFailed	中程度	ディスクの空き容量に障害が発生しました。
ContainerUnhealthy	最重要	コンテナが不良な状態です。
ContainerProbeWarning	警告	コンテナのプロブは完了しましたが、警告が発生しました。
FailedSync	警告	ポッドの同期に失敗しました。
FailedValidation	警告	ポッド構成の検証に失敗しました。
FailedPostStartHook	警告	ポッド開始のハンドラが失敗しました。
FailedPreStopHook	警告	事前停止のハンドラが失敗しました。
NodeNotReady	最重要	ノードの準備ができていません。

イベント名	重大度	説明
NodeNotSchedulable	最重要	ノードはスケジュール可能ではありません。
NodeRebooted	中程度	ノードが再起動されました。

通知

検索ベースの通知

検索ベースの通知は、次のように分類できます。

- システムベースの通知
- ユーザー定義の通知

システムベースの通知のパラメータは事前定義されており、通知アラートを有効にすると、メール形式の通知が送信されます。ユーザー定義の通知は、ユーザーが要件に基づいて設定します。E メール通知は、検索クエリに基づいて作成できます。検索を実行すると、[結果] 画面に [通知の作成] オプションが表示されます。各検索では次を実行できます。

- 通知を受信する場合はその条件を選択する。
- 通知を受信する頻度を定義する。
- 各通知の E メール受信者を入力する（デフォルトでは、受信者のリストに自分のメール アドレスが表示されています。複数のメール アドレスを追加することもできます）。

ユーザー定義の検索の場合は、以下が適用されます。

- 検索ベースの通知には、名前を割り当てる必要があります。
- 問題としてマークされた検索ベースのイベントについては、問題の重要度を選択する必要があります。
- ユーザー定義のイベントは、検索条件によって一意に識別されます。
- 通知の頻度として、[即座] または [デイリー ダイジェストとして] を指定できます。

通知は [設定] > [検索ベースの通知] 画面から管理できます。[検索ベースの通知] 画面では、既存の通知の表示、編集、有効化、無効化を行えるほか、不要な通知の削除を行うこともできます。

イベント通知の設定

通知は E メール形式で送信されます。

通知を設定するには、まずメール サーバを構成する必要があります。メール サーバの構成方法については、[メールサーバを設定](#)を参照してください。

E メールを送信するための通知イベントの指定

ユーザーは、E メール通知を送信するイベントを指定できます。

イベントを指定するには、次の手順を実行します。

- 1 [設定] 画面で [検索ベースの通知] をクリックするか、単純に [検索] ボックスを使用して情報を検索します。

- 2 [検索ベースの通知] 画面で、[通知の作成] アイコンをクリックします。通知ダイアログ ボックスが表示されま
す。
- 3 [通知を受信するタイミング] ボックスで、発生時に通知を送信するイベントを選択します。
- 4 [通知] ボックスで、通知を送信する頻度を選択します。
- 5 望ましくないイベントの場合は、[問題としてマーク] チェック ボックスを選択します。
- 6 通知の送信先メール アドレスを入力し、[保存] をクリックします。

注： 通知メールが正しく設定されているかどうかを確認するには、[テスト メールを送信] をクリックします。

イベント通知

vRealize Network Insight には、4 時間ごとに自動メール通知を受信できる、事前定義済みシステム イベント（シ
ステムの問題とシステムの変更）のリストが含まれています。

通知のリストは、[設定] > [システム通知] 画面で確認できます。

注： 管理者ユーザーは、別の管理者ユーザーまたはメンバー ユーザーの登録済みのプラットフォームやシステム イ
ベントを表示することはできません。

イベントに対して電子メール通知も SNMP 通知も設定していない場合は、ホーム画面にアラート メッセージが表示
され、通知を定義することができます。このアラート メッセージに対して [通知の有効化] をクリックすると、[シス
テム イベント] 画面に直接移動して、指定したイベントの通知を登録できます。

このリマインダを無効にするには、[今後はこのメッセージを表示しない] オプションを選択します。そのユーザーに
対してはアラート メッセージが表示されなくなります。後で通知を定義するには、[設定] - [イベント] の順に移動し
ます。

問題のアーカイブ

問題のアーカイブ

- 1 イベントのインスタンスが複数ある場合、[すべて表示] リンクをクリックして、イベントのすべてのインスタン
スを表示します。
- 2 アーカイブするイベントのインスタンスの上にマウスを移動して、一連のアイコンを表示し、アーカイブ アイコ
ンをクリックします。
- 3 [イベント固有] ダイアログ ボックスで、次の手順を実行します。
 - a このイベントのみをアーカイブする場合、[アーカイブしようとしています] リストから [このイベント] を
選択します。
 - b システム内の同じ種類のすべてのイベントをアーカイブする場合、[アーカイブしようとしています] リスト
から [この種類のすべてのイベント] を選択します。
- 4 [保存] をクリックします。

アーカイブされたすべてのイベントの表示

- 1 [ホーム] 画面で、[検索] ボックスに「イベント」と入力し、[Enter] キーを押します。イベントのリストが表示されます。
- 2 左側のペインのアーカイブされたファセットで、[真] チェックボックスを選択します。以下のスクリーンショットでハイライトされています。

ここでアーカイブされたすべてのイベントを表示できます。

アーカイブされたイベントをリストアするには

- 1 アーカイブされたイベントで、アーカイブ済みアイコンをクリックします。アーカイブされたイベントの画面への移動方法については、前のセクションのアーカイブされたイベントの表示方法に関する記述を参照してください。
- 2 [イベント固有] ダイアログ ボックスで、次の手順を実行します。
 - a このイベントのみをリストアする場合、[アーカイブからリストアしようとしています] リストから [このイベント] を選択します。
 - b すべての類似の種類イベントをリストアする場合、[アーカイブからリストアしようとしています] リストから [すべてのイベント] を選択します。
 - c [保存] をクリックして、リストアを完了します。

イベントの無効化

ユーザーは、イベントを選択的に無効にし、今後通知が送信されないようにできます。

イベント通知を無効にするには

方法 1

- 1 イベントで、イベントのインスタンスが複数ある場合、[すべて表示] リンクをクリックして、イベントのすべてのインスタンスを表示します。
- 2 無効にする通知を持つイベントのインスタンスの上にマウスを移動します。アイコンのセットが表示されたら、アーカイブ アイコンをクリックします。
- 3 [イベント固有] ダイアログ ボックスで、[今後このタイプのすべてのイベントを無効にする] チェックボックスを選択し、[保存] をクリックします。

方法 2

- 1 [ホーム] 画面の右上隅にある [プロフィール] アイコンをクリックし、[設定] をクリックします。
- 2 [設定] セクションで、[イベント通知] をクリックして、有効および無効なすべてのイベントのリストを表示します。
- 3 無効にする有効なイベントの [有効] 列で、それぞれのスライダの左側の領域をクリックします。
- 4 [アクションの確認] ダイアログ ボックスで、[はい] をクリックします。

イベント通知サービスの設定

ユーザーは、さまざまなイベントに関するお客様の通知を有効にできます。

通知サービスを設定するには

- 1 [設定] の [イベント通知] に移動し、E メール通知と SNMP を有効にする問題に対応する編集アイコンをクリックします。
- 2 [システム通知の編集] ダイアログ ボックスで、E メール通知を送信するメールアドレスを入力します。[E メールの頻度] ボックスで、通知を受信する時間の頻度を選択します。
- 3 SNMP 通知を設定するには、[このイベントの SNMP トラップを有効にする] チェックボックスを選択します。
- 4 [保存] をクリックします。
- 5 有効にすると、次のスクリーンショットに示されているように、それぞれのメールと SNMP アイコンが表示されます。

ID およびアクセス権の管理の設定

vRealize Network Insight では、ユーザーの作成や、LDAP ユーザーおよび VMware Identity Manager ユーザーのアクセス権の設定を行うことができます。また、ユーザーにさまざまなロールを割り当てることもできます。

ユーザー管理の設定

vRealize Network Insight のユーザーには、3 タイプのユーザー ロールがサポートされています。ユーザーは、割り当てられたロールに基づいて vRealize Network Insight の機能にアクセスできます。

- 管理者：管理者は完全なアクセス権を持ちます。
- メンバー：メンバー ユーザーのアクセス権には制限があります。
- 監査者：監査者には読み取り専用のアクセス権があり、作成、追加、編集、削除のすべてのアクションは制限されています。ユーザーは状態の表示のみが可能です。

表 6-7. 各ロールでサポートされる機能

画面	アクション	管理者
[設定] ログ：監査ログ	表示：[監査ログ] 画面/タブ	許可
	有効化/無効化：個人の特定が可能な情報	許可
	表示/フィルタ：監査ログ	許可
	CSV としてエクスポート	許可
[設定] ログ：Syslog 設定	表示：[Syslog 設定] 画面/タブ	許可
	Syslog の有効化/無効化	許可
	追加：Syslog サーバ	許可
	編集/削除：Syslog サーバ	許可
	表示：Syslog サーバ	許可
	表示：ソース サーバのマッピング	許可

表 6-7. 各ロールでサポートされる機能（続き）

画面	アクション	管理者
	編集：ソース サーバのマッピング	許可
[設定] バージョン情報	製品に関する詳細（製品名、バージョン、サービス タグ）を表示	許可
[設定] システム設定	表示：[システム設定] 画面/タブ	許可
	表示：ユーザー セッションのタイムアウト	許可
	編集：ユーザー セッションのタイムアウト	許可
	表示：データ ソース証明書の検証	許可
	編集：データ ソース証明書の検証	許可
	表示：Google マップ API キー	許可
	編集：Google マップ API キー	許可
[設定] 自分の環境設定	表示/編集：自分の環境設定	許可
[設定] ライセンスと使用量	表示：[ライセンスと使用量] 画面/タブ	許可
	表示：ライセンスの詳細	許可
	追加/検証：ライセンス キー	許可
	削除：ライセンス キー	許可
	オプション：「データ ソースを管理する」	許可
	オプション（[アカウントとデータソース] 画面へのリンク）：「現在の使用量にデータ ソースを追加」	許可
[設定] SNMP トラップ先	表示：[SNMP トラップ先] 画面/タブ	許可
	表示：既存の SNMP ターゲットのリスト（構成されたイベント数を含む）	許可
	表示：SNMP ターゲットごとに構成されたイベントのリスト	許可
	テスト トラップの追加/編集/削除/移行/送信：SNMP ターゲット	許可
[設定] メール サーバ	表示：[メール サーバ] 画面/タブ	許可
	表示：メール サーバの既存の構成	許可
	追加/編集/削除：メール サーバの構成	許可
	テスト メールを送信	許可
[設定] ID およびアクセス権の管理	表示：[ID およびアクセス権の管理] 画面/タブ	許可
[設定] ID およびアクセス権の管理：LDAP	表示：[LDAP] 画面/タブ	許可
	表示：LDAP の既存の構成	許可

表 6-7. 各ロールでサポートされる機能 (続き)

画面	アクション	管理者
	追加/編集/削除: LDAP の構成	許可
[設定] ID およびアクセス権の管理: vIDM	表示: [vIDM] 画面/タブ	許可
	表示: vIDM の既存の構成	許可
	追加/編集/削除: vIDM の構成	許可
	切り替え: vIDM の構成	許可
[設定] ID およびアクセス権の管理: ユーザー管理	表示: [ユーザー管理] 画面/タブ	許可
	表示: ローカル/LDAP/vIDM ユーザー	許可
	追加/編集/削除: ローカル ユーザー	許可
	追加/編集/削除: LDAP ユーザー	許可
	追加/編集/削除: vIDM ユーザー	許可
[設定] イベント	表示: [イベント] 画面/タブ	許可
[設定] イベント: システム イベント	表示: [システム イベント] 画面/タブ	許可
	表示: システム イベントのリスト	許可
	編集: システム イベント	許可
	有効化/無効化: システム イベント	許可
	一括編集/有効化/無効化: システム イベント	許可
[設定] イベント: プラットフォームの健全性イベント	表示: [プラットフォームの健全性イベント] 画面/タブ	許可
	表示: プラットフォームの健全性イベントのリスト	許可
	編集: プラットフォームの健全性イベント	許可
	一括編集: プラットフォームの健全性イベント	許可
[設定] イベント: ユーザー定義イベント	表示: [ユーザー定義イベント] 画面/タブ	許可
	表示: ユーザー定義イベントのリスト	許可
	編集/削除: ユーザー定義イベント	許可
	有効化/無効化: ユーザー定義イベント	許可
[設定] IP プロパティおよびサブネット	表示: [IP プロパティおよびサブネット] 画面/タブ	許可
[設定] 物理 IP アドレスおよび DNS マッピング	表示: [物理 IP アドレスおよび DNS マッピング] 画面/タブ	許可
	表示: 前回インポートした物理 IP アドレスおよび DNS マッピング	許可
	ダウンロード: 物理 IP アドレスおよび DNS マッピング ファイル	許可

表 6-7. 各ロールでサポートされる機能 (続き)

画面	アクション	管理者
	アップロード/置換: 物理 IP アドレスおよび DNS マッピング	許可
	削除: 既存の物理 IP アドレスおよび DNS マッピング	許可
[設定] 物理サブネットおよび VLAN	表示: [物理サブネットおよび VLAN] 画面/タブ	許可
	表示: 構成されている物理サブネットおよび VLAN の既存のリスト	許可
	追加/編集/削除: 物理サブネットおよび VLAN	許可
[設定] East-West 通信用の IP アドレス	表示: [East-West 通信用の IP アドレス] 画面/タブ	許可
	表示: 既存の East-West IP アドレス タグ	許可
	追加/更新/削除: East-West IP アドレス タグ	許可
[設定] North-South 通信用の IP アドレス	表示: [North-South 通信用の IP アドレス] 画面/タブ	許可
	表示: 既存の North-South IP アドレス タグ	許可
	追加/更新/削除: North-South IP アドレス タグ	許可
[設定] アカウントとデータ ソース	表示: [アカウントとデータ ソース] 画面/タブ	許可
	表示: 既存のデータ ソース	許可
	追加/編集/削除: データ ソース	許可
	有効化/無効化: 既存のデータ ソース	許可
[設定] データ管理	表示: [データ管理] 画面/タブ	許可
	表示: データ保持間隔の詳細	許可
	編集: データ保持間隔の詳細	許可
[設定] インフラストラクチャおよびサポート	表示: [インフラストラクチャおよびサポート] 画面/タブ	許可
[設定] インフラストラクチャおよびサポート: 概要と更新	表示: [概要と更新] 画面/タブ	許可
	表示: 概要と更新の詳細	許可
	有効化/無効化: オンライン更新のステータス	許可
	詳細の表示/アップグレードの開始: オンライン更新	許可
	表示: オフライン更新	許可
	アップロード: オフライン バンドル	許可
	表示: システムの健全性	許可
	表示: プラットフォーム仮想マシン	許可
	クラスタの作成	許可

表 6-7. 各ロールでサポートされる機能 (続き)

画面	アクション	管理者
	ダウンロード：サポート バンドル	許可
	表示：コレクタ仮想マシン	許可
	追加/編集/削除：コレクタ仮想マシン	許可
[設定] インフラストラクチャおよびサポート：サポート	表示：[サポート] 画面/タブ	許可
	表示：製品サポートの詳細	許可
	有効化/無効化：サポート トンネル	許可
	表示：カスタマー エクスペリエンス向上プログラム	許可
	編集：カスタマー エクスペリエンス向上プログラム	許可
	作成：サポート バンドル	許可
	ダウンロード：サポート バンドル	許可
[設定] テンプレート	表示：[テンプレート] 画面/タブ	許可
[設定] テンプレート：プロパティ テンプレート	表示：[プロパティ テンプレート] 画面/タブ	許可
	表示：既存のプロパティ テンプレート	許可
	クローン作成/編集/削除：既存のプロパティ テンプレート	許可
[設定] テンプレート：アプリケーション検出テンプレート	表示：[アプリケーション検出テンプレート] 画面/タブ	許可
	表示：既存のアプリケーション検出テンプレート	許可
	クローン作成/編集/削除：既存のアプリケーション検出テンプレート	許可
[ダッシュボード] プランと評価	表示：[プランと評価] タブ	許可
[ダッシュボード] プランと評価：セキュリティ計画	表示：[セキュリティ計画] 画面（マイクロセグメント、トラフィックの分布、バイト数別の上位ポート）	許可
	分析：セキュリティ計画	許可
	ウィジェットの固定	許可
	評価レポート	許可
	ドーナツ/リスト表示：マイクロセグメント	許可
	CSV としてエクスポート	許可
[ダッシュボード] プランと評価：PCI コンプライアンス	表示：[PCI コンプライアンス] 画面/タブ	許可
	評価：PCI コンプライアンス	許可
	ウィジェットの固定/通知の作成	許可

表 6-7. 各ロールでサポートされる機能 (続き)

画面	アクション	管理者
	CSV/PDF のエクスポート	許可
	ヘルプ	許可
[ダッシュボード] ブランと評価: アプリケーション	表示: [アプリケーション] 画面/タブ	許可
	追加: アプリケーション	許可
	編集/削除: 既存のアプリケーション	許可
	エクスポート	許可
アプリケーション検出	表示: [検出] タブ	許可
	アプリケーションの検出	許可
[ダッシュボード] 分析	表示: [分析] 画面/タブ	許可
[ダッシュボード] 分析: 外れ値	表示: [外れ値] 画面/タブ	許可
	表示: 既存の外れ値の設定	許可
	追加/編集/削除: 既存の外れ値の設定	許可
	有効化/無効化: 既存の外れ値の設定	許可
	ウィジェットの固定	許可
[ダッシュボード] 分析: しきい値	表示: [しきい値] 画面/タブ	許可
	表示: 既存のしきい値の設定	許可
	追加/編集/削除: 既存のしきい値の設定	許可
	有効化/無効化: 既存のしきい値の設定	許可
	ウィジェットの固定	許可
[ダッシュボード] 分析: フロー インサイト	表示: [フロー インサイト] 画面/タブ	許可
	分析: フロー インサイト	許可
	ウィジェットの固定	許可
	CSV としてエクスポート/最大化/ヘルプ	許可
保存された検索	表示: デフォルトで保存された検索	許可
	追加/削除: 新規で保存された検索	許可

ローカル ユーザーの追加

vRealize Network Insight を使用すると、ユーザーを追加し、各ユーザーにロールを割り当てることができます。

手順

- 1 vRealize Network Insight の [設定] 画面で、[ID およびアクセス権の管理] を展開します。
- 2 [ユーザー管理] をクリックし、VMware Identity Manager ユーザー タブを選択します。
- 3 [ユーザーの追加] をクリックして、必要な詳細を入力します。

プロパティ	説明
名前	ユーザーの名前を入力します。
E メール (ログイン ID)	E メールまたはログイン ID があれば入力します。
ロール	ロールをドロップダウン リストから選択します。
パスワード	パスワードを入力します。
新しいパスワードの再入力	確認のためにパスワードを再入力します。

- 4 [ユーザーの追加] をクリックして、ユーザー情報を保存します。

LDAP ユーザーへのロールの割り当て

任意の LDAP ユーザーにロールを割り当てて、vRealize Network Insight へのアクセスを可能にすることができます。

前提条件**Lightweight Directory Access Protocol (LDAP) の設定****手順**

- 1 vRealize Network Insight の [設定] 画面で、[ID およびアクセス権の管理] を展開します。
- 2 [ユーザー管理] をクリックし、[LDAP ユーザー] タブを選択します。
- 3 [ユーザーの追加] をクリックします。
- 4 ロールの割り当て先となるユーザーのログイン ID を指定します。
- 5 リストからロールを選択します。詳細については、[ユーザー管理の設定](#)を参照してください。
- 6 [ユーザーの追加] をクリックします。

Lightweight Directory Access Protocol (LDAP) の設定

LDAP ユーザーが vRealize Network Insight にログインできるようにするには、vRealize Network Insight プラットフォームで LDAP サービスを設定する必要があります。

前提条件

管理者権限が必要です。

手順

- 1 vRealize Network Insight にログインし、[設定] をクリックします。

- 2 [ID およびアクセス権の管理] で、[LDAP] を選択します。
- 3 [設定] をクリックします。
- 4 次の情報を入力します。

フィールド	説明
ドメイン	ドメイン名を入力します。通常、これはユーザー メール アドレスで「@」記号の後にある最後の部分です。例 : johndoe@example.com としてログインしているユーザーの場合、このフィールドは example.com です。
LDAP ホストの URL	ホスト名を入力します。複数の LDAP ホストの URL をカンマで区切って指定できます。
[グループ ベースのアクセス コントロール]	<p>このオプションを選択してグループを設定し、そのグループのメンバーにロールを提供します。</p> <ol style="list-style-type: none"> a [ベース DN] でベース DN を入力します。サーバはここからユーザーの検索を開始します。 b 検索属性を指定します。 c [グループ DN] で、各グループのユーザーのロールを選択します。 <p>特定のグループに対して管理者ロールを選択すると、そのグループのすべてのメンバーに管理者権限が付与されます。同様に、特定のグループに対してメンバー ロールを選択すると、そのグループのすべてのメンバーにメンバー権限が付与されます。このオプションが選択されていない場合、権限の割り当てにはグループ設定が使用されます。ただし、追加したグループに属していないその他の有効な LDAP ユーザーは、製品にログインできません。</p> <ol style="list-style-type: none"> d [さらに追加] をクリックして、包含リストにグループを追加します。 e アクセスの許可対象を、追加した LDAP グループ（直接または継承されたメンバーシップ）のみに制限するには、[上記グループのメンバーのみにアクセスを制限] オプションを選択します。
ユーザー名	指定された設定を使用してログインするために必要な権限を持つユーザーです。
パスワード	ユーザーのパスワードです。

- 5 [送信] をクリックします。

設定が完了すると、設定した [LDAP] の詳細が表示されます。

VMware Identity Manager からのユーザーのインポート

VMware Identity Manager ユーザー アカウントをインポートして、vRealize Network Insight を使用できるようにし、ロールを割り当てることができます。

前提条件

VMware Identity Manager の構成。

手順

- 1 vRealize Network Insight の [設定] 画面で、[ID およびアクセス権の管理] を展開します。
- 2 [ユーザー管理] をクリックし、VMware Identity Manager ユーザー タブを選択します。

3 [ユーザーの追加] をクリックして、必要な詳細を入力します。

フィールド名	説明
ドメイン名	インポートする VMware Identity Manager ドメイン名を入力します。
ユーザー/グループの検索	検索文字列を入力し、オートコンプリート リストからユーザー アカウントを選択します。単一のユーザーを選択するか、またはユーザー グループを選択できます。グループを選択すると、グループ内のすべてのメンバーが vRealize Network Insight にアクセスできるようになります。
ロール	ロールをユーザー アカウントに割り当てます。詳細については、 ユーザー管理の設定 を参照してください。

4 [ユーザーの追加] をクリックします。

注：

- グループを選択した場合は、グループ内のすべてのメンバーが同じロールを取得します。グループ内の特定のユーザーに別のロールを割り当てる場合は、そのユーザーを個別に追加し、必要なロールを割り当てる必要があります。

たとえば、管理者ロールを *Mygroup* の *user1* にのみ割り当てるには、次のことを行います。

- *Mygroup* を追加し、メンバーロールを割り当てます。
- *user1* を追加し、管理者ロールを割り当てます。

ユーザーに割り当てられたロールは、グループの一部としてユーザーに割り当てられたロールを直接上書きします。

- 異なるロールを持つ複数のグループにユーザーが属している場合、最も高い権限ロールがユーザーに割り当てられます。

たとえば、ユーザーが、管理者ロールを持つグループ A に属していて、メンバー ロールを持つグループ B とグループ C にも属している場合、このユーザーは管理者ロールを継承します。

結果

これで、この VMware Identity Manager ユーザーまたはグループ メンバーが vRealize Network Insight にログインし、割り当てられたロールに基づいて機能を使用できるようになりました。

VMware Identity Manager の構成

管理者は VMware Identity Manager ユーザーに対して、それぞれのロールに基づいて vRealize Network Insight 機能へのアクセスを許可できます。

前提条件

vRealize Network Insight を OAuth クライアントとして VMware Identity Manager ホストに登録します。詳細については、[VMware Workspace ONE Access のドキュメント](#)を参照してください。

手順

- 1 vRealize Network Insight にログインし、[設定] をクリックします。
- 2 [ID およびアクセス権の管理] で、VMware Identity Manager を選択します。
- 3 [設定] をクリックします。

4 次の情報を入力します。

パラメータ	説明
VMware Identity Manager アプライアンス	VMware Identity Manager ホストの完全修飾ドメイン名 (FQDN)。
OAuth クライアント ID	VMware Identity Manager ホストに vRealize Network Insight を登録するときに作成される ID。
OAuth クライアント シークレット	vRealize Network Insight を VMware Identity Manager ホストに登録するときに作成されるシークレット。
SHA-256 サムプリント	これはオプションのフィールドです。VMware Identity Manager ホストの証明書サムプリント。詳細については、 VMware Identity Manager ホストからの証明書サムプリントの取得 を参照してください。

5 [送信] をクリックします。

設定が完了すると、設定した VMware Identity Manager アプライアンスとクライアントの詳細が表示されません。

6 切り替えボタンをクリックして、VMware Identity Manager を有効または無効にします。無効にすると、vRealize Network Insight で VMware Identity Manager 認証を使用できません。

VMware Identity Manager ホストからの証明書サムプリントの取得

SSL 証明書の検証では、VMware Identity Manager ホストから SHA-256 サムプリントを取得できます。

手順

1 SSL/TLS 証明書を取得するには、次のコマンドを実行します。

```
openssl s_client -connect <FQDN of vIDM host>:443
```

サーバ証明書の -----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- までを cert.pem という名前のファイルにコピーして、ファイルを保存します。

2 サムプリントを取得するには、次のコマンドを実行します。

```
openssl x509 -fingerprint -noout -sha256 -in cert.pem
```

結果

サムプリントが次の形式で表示されます。

```
SHA256
```

```
Fingerprint=3D:E8:4C:CD:19:D6:AD:23:30:86:E4:A1:72:D5:22:08:F9:72:6D:D3:E7:6E:99:32:C8:C7:3D:F8:E2:91:91:AE
```

次のステップ

サムプリントをコピーし、[VMware Identity Manager の構成] 画面に貼り付けます。

ログの設定

vRealize Network Insight では、さまざまなタイプのログを表示および設定できます。

監査ログの表示とエクスポート

監査ログには、システムで実行される管理アクションがキャプチャされます。これらは、通常の CRUD 操作、およびログインとログアウトのイベントです。ユーザー インターフェイス、CLI、または API 経由で実行される管理アクションがログに記録されます。

監査ログには、API、ユーザー インターフェイス、および CLI からのアクションがキャプチャされます。

機能

- 監査ログ機能は常に有効です。
- vRealize Network Insight は、監査ログで UTC 形式をサポートしています。
- 監査ログは、Syslog に統合されます。すべての監査ログを収集するように Syslog コレクタを設定できます。
- すべての監査ログ データを CSV ファイルにエクスポートできます。

Syslog の設定

vRealize Network Insight のリモート Syslog サーバは、[Syslog 設定] 画面を使用して設定できます。

プロキシ サーバのリモート Syslog サーバはそれぞれ異なる可能性があります。クラスタ内のすべてのプラットフォーム サーバは同じリモート Syslog サーバを使用します。

最新リリースでは、vRealize Network Insight の問題イベントとプラットフォーム/プロキシ サーバ Syslog は、リモート Syslog サーバに送信されます。

現在 vRealize Network Insight は、vRealize Network Insight サーバとリモート Syslog サーバ間の通信で UDP のみをサポートしています。そのため、リモート Syslog サーバが、UDP 経由の Syslog トラフィックを受け入れるように設定されていることを確認してください。

Syslog を設定するには

- 1 [設定] 画面で、[Syslog 設定] をクリックします。[Syslog 設定] 画面には、設定済みの Syslog サーバと、仮想アライアンスへのマッピングが表示されています。この画面に初めてアクセスする際、Syslog はデフォルトで無効になっており、この画面のサーバ リストは表示されません。
- 2 Syslog サーバを追加するには、次の手順を実行します。
 - a [Syslog サーバ の追加] をクリックします。
 - b サーバの IP アドレス、ニックネーム、およびポート番号を入力します。UDP の標準ポート番号は 514 です。
 - c 設定をテストするには、[テストログの送信] をクリックします。
 - d [送信] をクリックします。
 - e これが、初めて追加するサーバである場合は、画面の最上部にある Syslog を有効にします。

- 3 サーバをプラットフォームとプロキシにマッピングするには、次の手順を実行します。
 - a [マッピングの編集] をクリックします。
 - b すべてのプラットフォームとプロキシサーバに対する Syslog サーバを選択します。
 - c どのプロキシサーバまたはプラットフォームでも Syslog を有効にしない場合は、[サーバなし] オプションを選択します。
 - d [送信] をクリックします。

注： 変更を行った後、それらが有効になるまで数分かかる場合があります。

メールサーバを設定

vRealize Network Insight では、メールでイベント通知を受信するようにメールサーバを設定できます。

メールサーバを構成するには、次の手順を実行します。

- 1 [ホーム] 画面の右上隅にある [プロファイル] アイコンをクリックし、[設定] をクリックします。
- 2 [メールサーバ] をクリックします。
- 3 [SMTP サーバ] チェックボックスを選択します。
- 4 各ボックスに適切な値を入力します。

表 6-8.

フィールド	説明
送信者の E メール	送信者のメール アドレス。
SMTP ホスト名/IP アドレス	SMTP サーバのホスト名または IP アドレス。
暗号化	使用できる暗号化オプションは、[なし]、[TLS]、[SSL] です。
SMTP ポート番号	SMTP サーバのポート番号 (デフォルトは 25)。

注： メールサーバとして Gmail サーバを使用するには、Google サポートに記載されている設定が追加で必要になります。

必要に応じ、セキュリティを強化するために [認証] チェックボックスを選択し、ユーザー名とパスワードを入力します。

注： 通知メールが正しく設定されているかどうかを確認するには、[テスト メールを送信] をクリックします。

- 5 [送信] をクリックして構成を完了します。

SNMP トラップ先の設定

vRealize Network Insight では、Simple Network Management Protocol (SNMP) トラップ エージェントを 4 つまで設定して通知を受信することができます。この製品では、v2c および v3 バージョンの SNMP がサポートされています。

- 1 [設定] 画面で [SNMP トラップ先] - [宛先の追加] の順にクリックします。
- 2 [SNMP トラップ先の設定] 画面の [バージョン] ドロップダウン ボックスで、[SNMPv2c] または [SNMPv3] プロトコルを選択します。

注： SNMP v2c プロトコルは認証を必要としません。SNMP v3 プロトコルは認証をサポートします。

- 3 [ターゲット IP アドレス/FQDN] テキスト ボックスに、SNMP エージェントの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
- 4 [宛先ポート] テキストボックスに、SNMP エージェントのポート番号を入力します。
- 5 選択した SNMP のバージョンに応じて、次のいずれかの操作を実行します。

オプション	アクション
SNMP v2c の場合	[コミュニティ スtring] テキスト ボックスに、コミュニティ文字列を入力します。
SNMP v3 の場合	<ol style="list-style-type: none"> 1 [ユーザー名] テキストボックスに、SNMP エージェントで作成したユーザーの名前を入力します。 2 (オプション) [認証の使用] チェック ボックスを選択します。 3 (オプション) 認証プロトコルを選択し、SNMP エージェントで特定のユーザー用に設定したパスワードを入力します。 4 (オプション) [プライバシーの使用] チェック ボックスをオンにして、プライバシー プロトコルを選択し、プライバシー フレームをそれぞれ入力します。

- 6 [ニックネーム] フィールドにニックネームを入力します。
- 7 (オプション) 設定が正しく行われているかどうかを確認するには、[SNMP トラップのテスト] をクリックし、トラップが SNMP エージェントに送信されたかどうかを確認します。
- 8 [送信] をクリックします。

SNMP トラップ先の削除

vRealize Network Insight から SNMP トラップ先を削除することができます。SNMP トラップ先が複数ある場合、SNMP トラップ先を削除すると、そのトラップ先に関連するすべての通知を、使用可能な別のトラップ先に移行することができます。

手順

- 1 削除するトラップ先の横にある [削除] アイコンをクリックします。
[アクションの確認] ポップアップが表示されます。

- 2 現在のトラップ先から別のトラップ先にイベントを移行する場合は、[複数の宛先を選択します...] ドロップダウンをクリックして、イベントを移行するトラップ先を選択します。
- 3 [確認] をクリックします。

ライセンスの管理

VMware では、vRealize Network Insight ライセンスを自主管理制としています。つまり、ライセンス数の違反があるとユーザー インターフェイスに警告メッセージが表示されますが、機能の使用は制限されません。

以下のシナリオでは、ユーザー インターフェイスのすべてのページにライセンス警告メッセージが表示されます。

- ライセンスの使用量がソケット (CPU) ライセンスを超えている。
要件を満たすには、ライセンスを追加する必要があります。
- ライセンス タイプの混在
 - Advanced ライセンスと Enterprise ライセンスの両方を追加してある場合。
Advanced Edition から Enterprise Edition にアップグレードした後、手動で Advanced ライセンスを削除する必要があります ([設定] - [ライセンスと使用量])。Enterprise の機能を使用するために十分な数の Enterprise ライセンスがあることを確認します。
 - ソケット ライセンスとコア ライセンスを追加してある場合。
要件に基づいて、どちらかのライセンス タイプを削除します。

ライセンス使用量の計算

vRealize Network Insight ライセンス使用量は、次の比率に基づいて計算されます。

オブジェクト	説明	ソケット ライセンスあたりの許可されるオブジェクト数
VMware vSphere CPU 数	オンプレミス ホスト マシンの CPU ソケット数の合計	1
AWS VMware Cloud のホスト数	VMware Cloud on AWS ホストの総数	0.5 <small>注: One VMC host requires two socket licenses.</small>
AWS vCPU または Azure	AWS インスタンスまたは Azure の vCPU の総数	16
非 VMware のエンドポイント	非 VMware フロー レポート機能によってのみ報告されるフローに表れる、非インターネットおよび非 VMware のエンドポイントの総数 (物理スイッチからのネット フローなど)	15

注: vRealize Network Insight のライセンス使用量の計算では、無効にされているデータ ソースも対象になります。カウント時に vRealize Network Insight によって無視されるようにするには、データ ソースを削除します。

SD-WAN ライセンス

VMware SD-WAN をデータソースとして追加して vRealize Network Insight に VMware SD-WAN 展開を表示するには、VMware SD-WAN ライセンスを追加する必要があります。VMware SD-WAN ライセンスは、スタンドアローンのライセンスとして追加することも、Enterprise ライセンスと併用することもできます。ただし、VMware SD-WAN ライセンスは Advance ライセンスと併用することはできません。複数の VMware SD-WAN ライセンス キーを使用することで、バンド幅の異なる Edge をサポートすることもできます。

VMware SD-WAN ライセンスでは、VMware SD-WAN データソースのほかに、IPFIX なしの vCenter Server、スイッチとルーター、Infoblox を追加できます。

ライセンス エディションに基づく機能の比較

vRealize Network Insight の機能は、使用するライセンスによって異なります。

次の表に、vRealize Network Insight によって提供されるさまざまなライセンスの機能の比較を示します。

機能	Advanced ライセンス	Enterprise ライセンス	クラウドサービス	SD-WAN オンプレミス	SD-WAN SKU (クラウドサービス)
仮想フロー (VDS IPFIX、V2V、V2P)	はい	はい	はい	なし	なし
NSX ファイアウォール M-Seg の計画と操作 (NSX IPFIX)	はい	はい	はい	なし	なし
サードパーティ製スイッチ、ルータ、ファイアウォール、ロード バランサ全体にわたる可視性	はい	はい	はい	なし	なし
パブリック API	はい	はい	はい	なし	なし
DNS マッピング (バインド ファイルのインポート)	はい	はい	はい	なし	なし
NSX PCI コンプライアンス ダッシュボード	なし	はい	はい	なし	なし
VMware Cloud on AWS 向けのセキュリティの計画と可視性	なし	はい	はい	なし	なし
AWS および Azure 向けのセキュリティの計画と可視性	なし	はい	はい	なし	なし
Infoblox による DNS 解決	なし	はい	はい	なし	なし
物理フロー (NetFlow v7 および v9、sFlow)	なし	はい	はい	なし	なし
VMware Enterprise PKS、Kubernetes、OpenShift に対する可視性	なし	はい	はい	なし	なし
ネットワークとセキュリティ分析 (上位の発信者、アノマリ、異常値検出など)	なし	はい	はい	なし	なし
データの設定と拡張保持期間	なし	はい	はい	なし	なし

機能	Advanced ライセンス	Enterprise ライセンス	クラウドサービス	SD-WAN オンプレミス	SD-WAN SKU (クラウドサービス)
Cisco ACI、BGP-EVPN アンダレイの可視性	なし	はい	はい	なし	なし
アプリケーション検出ダッシュボード (名前、タグ、正規表現)	はい	はい	はい	なし	なし
アプリケーション検出のための ServiceNow 統合	なし	はい	はい	なし	なし
フロー ベースのアプリケーション検出	なし	なし	はい	なし	なし
VMware Cloud on AWS Direct Connect	なし	はい	はい	なし	なし
VMware SD-WAN by VeloCloud	なし	なし	なし	はい	はい
vRealize Operations Manager の統合	はい	はい	はい	なし	なし

ライセンスの追加と変更

[ライセンスと使用量] 画面で各エンティティの数への個別のリンクをクリックすると、ライセンスの使用数と詳細が表示されます。この画面でライセンス タイプを追加および変更することもできます。vRealize Network Insight は複数のライセンスの追加をサポートしています。

ライセンスを追加

ライセンスを追加するには、次の手順を実行します。

- 1 [ライセンスと使用量] 画面で、[ライセンスの追加] をクリックします。
- 2 [新しいライセンス キー] フィールドにライセンス キーを指定します。
- 3 [検証] をクリックします。

ライセンスのタイプ、ライセンスで使用可能なソケット数またはコア数、および有効期限の詳細が表示されます。

- 4 [有効化] をクリックします。
- 5 画面にライセンスのリストが表示されます。
- 6 [有効期限] 列の横にある削除アイコンをクリックして、ライセンスを削除することもできます。ライセンスが Enterprise エディションに属していて、それがシステム内に残る最後の Enterprise エディションである場合は、Enterprise ライセンスを削除する前に AWS アカウントの削除を確実に実行します。

ライセンスの変更

評価版ライセンスの有効期限が切れた場合、製品にログインすると、ライセンスの有効期限が切れており、ライセンスの更新が必要であることを示すメッセージが表示されます。次の手順に従って、ライセンスを変更します。

ライセンスを変更するには、次の手順を実行します。

- 1 期限切れメッセージに含まれるリンクをクリックして [ライセンスの変更] 画面に移動します。または、[設定] で [ライセンスと使用量] をクリックし、[ライセンスの変更] をクリックします。
- 2 [ライセンスの変更] 画面の [新しいライセンス キー] で、VMware から受け取った新しいライセンス キーを入力します。
- 3 [検証] をクリックします。
- 4 [有効化] をクリックします。

注： 評価版ライセンスの有効期限が切れると、データ プロバイダが無効になり、データの収集が停止します。ライセンスの更新後、ユーザー インターフェイスからデータ プロバイダを再度有効にして、データ収集を開始する必要があります。

自動更新間隔の設定

vRealize Network Insight では、エンティティ ページとピンボードの自動更新間隔を設定できます。

vRealize Network Insight では、エンティティ ダッシュボードとピンボードに自動更新機能が提供されています。ダッシュボードは、ヘッダー バーで指定された n 分ごとに 1 回、自動的に更新されます。

すべてのダッシュボードの自動更新が実行される時間間隔を指定できます。指定された時間間隔 (n 分) が経過すると、ダッシュボード上のすべての開いているウィジェットが自動的に再ロードされます。

注：

- 特定のダッシュボードの自動更新間隔を変更することはできません。
- タイムライン スライダで過去の時間間隔を選択すると、自動更新が一時停止します。

特定のダッシュボードで自動更新が不要な場合は、一時停止できます。ヘッダー バーで、[一時停止] を [オン] に設定します。[一時停止] を [オフ] に設定すると、自動更新カウンタがリセットされます。

ピンボードを表示しているとき、別のユーザーがレイアウト変更などの変更をそのピンボードに対して行くと、自動更新機能によってコンテンツだけでなくピンボード全体が更新されます。これは、他のユーザーとの間で共有と共同作業が設定されている場合にのみ発生します。

手順

- 1 [設定] 画面で、[自分の環境設定] をクリックします。または、それぞれのダッシュボードのヘッダー バーで、自動更新の横にある [更新] をクリックします。
- 2 自動更新の時間間隔を変更するには、[編集] をクリックします。時間間隔はドロップダウン メニューから選択します。[保存] をクリックします。
- 3 自動更新オプションを無効にするには、ドロップダウン メニューから [無効] を選択します。このオプションを選択すると、すべてのダッシュボードが自動的に更新されなくなります。

ユーザー セッションのタイムアウトの設定

デフォルトでは、ユーザー セッションのタイムアウトが 15 分に設定されています。この値は、希望に合わせて変更できます。

手順

- 1 [設定] 画面で、[システム設定] をクリックします。

注： [システム設定] タブは、admin user のみに表示されます。

- 2 編集アイコンをクリックして、ユーザー セッションのタイムアウトのプリファレンスを変更します。
- 3 スライダーをドラッグして、セッションのタイムアウト値を設定します。値の範囲は 15 分から 24 時間です。
- 4 また、いつ、誰がタイムアウト値を変更したかについての詳細を、[最終変更] フィールドで確認することもできます。
- 5 [送信] をクリックします。正常に完了したことを示すメッセージが表示されて、更新されたセッション期間が次回ログインから有効になることが確認されます。

注： ユーザー セッションのタイムアウトに設定した新しい値は、ログアウトして再度ログインした後にのみ有効になります。

Google マップ API キーの追加

SD-WAN 展開のマップ ビューを取得するには、vRealize Network Insight に Google マップ API キーを追加する必要があります。

前提条件

以下の条件を確認します。

- Google Cloud Platform のメンバーであり、アカウントで課金が有効になっている。
- Google マップ API キーがある。API キーを取得するには、Google Maps Platform のドキュメントで API キーを取得する手順を参照してください。
- 誤使用を防止するために API キーが制限されている。詳細については、Google Maps Platform のドキュメントで API キーを制限する手順を参照してください。

手順

- 1 [設定] 画面で、[システム設定] をクリックします。
- 2 [Google マップ API キー] で API キーを入力し、[保存] をクリックします。

データ ソース証明書の検証の構成

vRealize Network Insight にデータ ソースを追加すると、最初の使用の際にそのデータ ソースに関連するすべての証明書（HTTPS 証明書または SSH パブリック キー）が、信頼された証明書として自動的に追加されます。

vRealize Network Insight にデータ ソースを追加した後は、証明書が変更されるたびに証明書はシステムによって検証されます。

証明書の検証を設定するには、[自動で承諾] と [手動で承諾] の 2 つの方法があります。[自動で承諾] の場合は、検出されたすべての証明書の変更がシステムで自動的に承諾されます。[手動で承諾] の場合、システムはデータ ソースを停止し、証明書の手動承諾を要求するアラート メッセージ通知が表示されます。証明書を承諾すると、システムによりデータ ソースが起動されます。

手順

- 1 [設定] - [システム設定] に移動します。
- 2 [データ ソース証明書の検証] ドロップダウン メニューで、いずれかのデータ ソース検証方法を選択します。
 - [自動で承諾]
 - [手動で承諾]
- 3 [保存] をクリックします。

注： 証明書の検証方法を [手動で承諾] から [自動で承諾] に変更する場合は、証明書の検証方法を変更する前に、使用可能なすべての証明書の変更を手動で承諾する必要があります。

保留中の検出された証明書の変更を承諾せずに [データ ソース証明書の検証] を [手動で承諾] から [自動で承諾] に変更した場合、保留中の証明書を含むデータ ソースに関するインサイトを取得するには、これらのデータ ソースをすべて削除してから再度追加する必要があります。

データ ソース証明書の手動での承諾

[データ ソース証明書の検証] を [手動で承諾] に設定している場合は、システムによって証明書の変更が検出されたデータ ソースごとに、新しい証明書 (HTTPS 証明書または SSH パブリック キー) を承諾する必要があります。

[データ ソース証明書の検証] を [手動で承諾] に設定している場合に、vRealize Network Insight が証明書内の変更を検出すると、アラート メッセージ通知が表示されます。また、[アカウントとデータ ソース] 画面で証明書の変更アラートを確認することもできます。証明書を承諾するには、次の手順を使用します。

手順

- ◆ [データ ソース証明書の更新が利用可能です] というアラート メッセージ通知内の[確認] をクリックします。

利用可能な証明書の更新の数が 2 以下の場合	<p>a 現在の証明書と新しい証明書の詳細が示された [データ ソース証明書] ウィンドウが表示されます。</p> <p>b 新しい証明書を確認し、[同意] をクリックします。</p>
利用可能な証明書の更新の数が 2 を超える場合：	<p>a [アカウントとデータ ソース] 画面の、証明書の更新が利用可能なデータ ソースの下に、</p> <div data-bbox="678 478 1425 537" style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin: 5px 0;"> <p style="text-align: center;">証明書の更新が利用可能です。確認して同意するには、こちらをクリック</p> </div> <p>のようなメッセージが表示されます。</p> <p>b 確認するデータ ソースの [確認して同意するには、こちらをクリック] をクリックして、更新された証明書を承諾します。</p> <p>c 現在の証明書と新しい証明書の詳細が示された [データ ソース証明書] ウィンドウが表示されます。</p> <p>d 新しい証明書を確認し、[同意] をクリックします。</p>

結果

新しい証明書を承諾すると、「証明書が正常に更新されました」というメッセージが表示されます。

監査ログの表示

監査ログには、システムで実行される管理アクションがキャプチャされます。これらのアクションには、通常の CRUD 処理、ログイン、ログアウト イベントがあります。監査ログには、API、ユーザー インターフェイス、および CLI からのアクションがキャプチャされます。

- 監査ログ機能は常に有効です。
- vRealize Network Insight は、監査ログで UTC 形式をサポートしています。
- 監査ログは、Syslog に統合されます。すべての監査ログを収集するように Syslog コレクタを設定できます。
- すべての監査ログ データを CSV ファイルにエクスポートできます。

現在、次の管理アクションは監査ログにキャプチャされません。

- SSH ログイン ログ。SSH ログは `/var/log/auth.log` で確認できます。
- 物理 IP アドレスと DNS マッピングの変更。
- 物理サブネットと VLAN の変更。

手順

- 1 [設定] 画面で、[ログ] の下にある [監査ログ] をクリックします。

- 2 [監査ログ] 画面には次の詳細が表示されます。

情報	説明
Date & Time	実際に実行したアクションのタイムスタンプ。
IP Address	CLI やブラウザなど、接続の確立元となるクライアントの IP アドレス。
User Name	アクションを実行しているユーザー。
Object Type	アクションが実行されているオブジェクト。
Operation	ユーザーがオブジェクトに対して実行するさまざまなアクション。
Object Identifier	アクションが実行されている特定のオブジェクトの一意の識別子。
Response	操作の成功または失敗を示すインジケータ。
Details	ニックネームやプロパティなど、変更された設定の詳細。

- 3 ユーザーがブラウザまたは CLI を使用してログインしたときに情報の収集を許可するには、[個人識別情報の収集を許可] を有効にします。このオプションはデフォルトで無効です。

注： このオプションが無効な場合、IP Address 列と User Name 列は空白です。

- 4 [CSV としてエクスポート] をクリックして、監査ログ データを CSV 形式でエクスポートします。

カスタマー エクスペリエンス向上プログラムへの参加または参加取り消し

この製品は、VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加しています。CEIP で収集される情報は、VMware 製品およびサービスの向上、問題の解決、各製品のデプロイおよび使用に関する最適な方法をお客様に提案するために役立てられます。CEIP の一環として、VMware は、お客様の組織の VMware ライセンス キーと関連付けて、組織における VMware 製品およびサービスの使用に関する技術的な情報を定期的に収集します。この情報は、お客様個人を特定するものではありません。

CEIP を介して収集されるデータと、VMware がそのデータを使用する目的についての詳細は、<https://www.vmware.com/solutions/trustvmware/ceip.html> の Trust & Assurance センターで説明されています。

vRealize Network Insight のカスタマー エクスペリエンス向上プログラム (CEIP) は、以下の手順によって参加または離脱できます。

- 1 [バージョン情報] 画面で、[カスタマー エクスペリエンス向上プログラム] の [変更] をクリックします。
- 2 CEIP ウィンドウがポップアップ表示されます。CEIP に参加するには、[有効化] を選択します。この操作を実行すると、CEIP が有効になり、データが <https://vmware.com> に送信されます。
- 3 CEIP から離脱するには、[有効化] を選択解除します。
- 4 [送信] をクリックします。

セットアップの健全性の表示

[健全性] インジケータは、[インストールとサポート] 画面の [概要] セクションから利用できます。

次の不良イベントのいずれかが発生すると、[健全性] インジケータは赤になります。

- プロキシがフロー データの収集を停止した場合
- プラットフォームが何らかの理由によりデータの処理を停止した場合（ディスク容量の不足など）
- 検索のインデксаで遅延が発生していて、そのために検索結果が古くなる場合

全体的な健全性インジケータには、赤のライトと一緒に異常の数が表示されます。全体的な健全性に対する問題の数をクリックすると、個別の異常が詳細とともに一覧表示されます。正常に動作している場合、健全性インジケータには緑色のライトが表示されます。

注： vRealize Network Insight は、同期されていないシステム クロックを検出できない場合があります。クロックが NTP と同期していない場合、一部のサービスが正常に動作しなくなったり停止したりする可能性があります。

サポート トンネルの有効化

サポート トンネルにより、VMware は、SSL で保護された接続を使ってプラットフォームおよびコレクタ仮想マシンにリモート接続し、高度なトラブルシューティングやデバッグを行うことができます。

高度なサポートをリクエストするには、[インストールとサポート] 画面の [概要] セクションで、[トンネルのサポート] オプションを切り替えます。

注： ポート 443 の support2.ni.vmware.com へのトラフィックが許可されていることを確認します。

ディスク使用率の管理

プラットフォームまたはコレクタのディスク使用率が高い場合、ユーザーに警告するイベントがトリガされます。さらに、追加する必要があるディスク容量の推奨事項も提示されます。イベントは、プラットフォームまたはコレクタダッシュボードで確認できます。このアラートは、[インストールとサポート] 画面の対応するコレクタまたはプラットフォーム セクションにも表示されます。

Platform VMs

IP Address (Name)	Last Activity	Status
 Critical: Disk Utilization is high 		<p>Disk utilization is at 85%. The Platform might run out of disk in 2 days. Add 100 GB more disk space to avoid any service interruption.</p>

ノードにディスクを追加するには、次の手順を実行します。

注： 既存のハード ディスクを拡張しないでください。

手順

- 1 適切な権限を持つ Web クライアントを介して vCenter Server にログインします。
- 2 ノードを右クリックして、[設定の編集] をクリックします。
- 3 アラートで指定されている推奨事項に合わせてハード ディスクを追加します。

vRealize Network Insight は、アプライアンスを検出して /var パーティションに追加するのに数分かかります。

ノードの詳細情報の表示

プラットフォームまたはコレクタ内の各ノードの詳細を表示できます。

手順

- 1 特定のプラットフォーム ノードの詳細を表示するには、[インストールとサポート] 画面の [プラットフォーム仮想マシン] に一覧表示されている名前をクリックします。
NI プラットフォーム ダッシュボードが表示されます。
- 2 特定のコレクタ ノードの詳細を表示するには、[インストールとサポート] 画面の [コレクタ (プロキシ) 仮想マシン] に一覧表示されている名前をクリックします。
NI コレクタ ダッシュボードが表示されます。

サポート バンドルの作成

製品固有のログ、セットアップの構成ファイルなどの診断情報を収集するサポート バンドルを作成できます。サポート リクエストを発行すると、VMware のテクニカルサポートはその情報を使用して、セットアップの問題をトラブルシューティングします。

手順

- 1 [設定] 画面で、[インストールとサポート] をクリックします。
- 2 [サポート バンドルの作成] をクリックします。
- 3 サポート バンドルの作成対象となるプラットフォーム仮想マシンおよびコレクタ仮想マシンを選択します。
すべての仮想マシンを選択するには、プラットフォーム仮想マシンとコレクタ仮想マシンのテーブルのヘッダーにあるチェック ボックスをクリックします。
- 4 [作成] をクリックします。
- 5 [はい] をクリックして、新しいサポート バンドルの作成を確認します。
vRealize Network Insight によるバンドルの作成が完了するまで、多少時間がかかります。

結果

新しいサポート バンドルが作成され、日時が表示されます。サポート バンドルのダウンロードを開始するには、それぞれの仮想マシンの横にある [ダウンロード] リンクをクリックします。

注：

- 中規模システムでのサポート バンドルの作成には、15 分以上かかる場合があります。
 - 同時に使用できるサポート バンドルは 2 つまでです。そのため、新しいサポート バンドルがすでに作成されている場合は古いバージョンが削除されます。
-

次のステップ

VMware が詳細にアクセスできるように、サポート バンドルをサービス申請に添付します。

コレクタおよびプラットフォームの負荷のキャパシティの概要

vRealize Network Insight は、コレクタ ノードおよびプラットフォームのおおよそのキャパシティと負荷情報を提供します。この制限ベースの情報は、パフォーマンスや操作性の問題が後から発生することを防止するのに役立ちます。

キャパシティの概要

キャパシティには 2 つの種類があります。

- 仮想マシンのキャパシティ：ノードまたはセットアップで処理できる、検出済み仮想マシンの数を意味します。
- フローのキャパシティ：ノードまたはセットアップで処理できる、フローの数を意味します。

キャパシティは次のように定義されます。

- 1つ以上のプロキシ ノードを持つ単一プラットフォーム：プロキシ ノードまたはプラットフォームのキャパシティは、パフォーマンスが低下せずに処理できる、検出済み仮想マシンの数です。
- クラスタ セットアップ：クラスタ セットアップのプラットフォームのキャパシティは、すべてのプラットフォーム ノードのすべてのキャパシティを集約したもので、プロキシ ノードのキャパシティは、個別のノードのレベルで考慮されます。

キャパシティ情報へのアクセス

[仮想マシンのキャパシティ] および [フローのキャパシティ] は、[インストールとサポート] 画面で参照できます。

コレクタ（プロキシ）仮想マシンの下に一覧表示される各コレクタ ノードでは、仮想マシンのキャパシティ情報のみが提供されます。

注： 環境全体のデータ ソースから検出された仮想マシンの数が、システムとコレクタの両方、またはそのいずれかのキャパシティを超えると、アップグレードをトリガできなくなります。

データ ソースで検出された仮想マシンを表示するには、次のように行います。

- 1 [アカウントとデータ ソース] 画面では、すでに追加されてアクティブになっている特定のデータ ソースについて検出された仮想マシンの数を確認できます。データ ソースが vCenter Server または AWS ソースの場合にのみ、この列に値が設定されます。

注： 検出された仮想マシンの数には、ブレースホルダとテンプレート仮想マシンが含まれます。そのため、製品内の仮想マシン数とは異なる場合があります。

vRealize Network Insight での Direct Connect サポート

7

Direct Connect は、オンプレミスの場所とパブリック クラウド サービスとの間でデータ転送接続を提供するメカニズムです。5.2 リリース以降、vRealize Network Insight は VMware Cloud on AWS の Direct Connect 機能をサポートしています。

Direct Connect のサポートにより、次のことが可能になります。

- オンプレミス データセンターと VMware Cloud on AWS SDDC の間で Direct Connect を経由して送信されるフローを識別します。
- フローのバンド幅やパケット速度を特定するためのフロー分析を実行する。
- Direct Connect を経由して仮想マシン間で送信される詳細なパス トポロジを表示します。
- Direct Connect および関連付けられたイベントに関する詳細を表示します。

Direct Connect のデータ取得メカニズム

vRealize Network Insight は VMware Cloud on AWS NSX API を使用して Direct Connect の情報を取得します。したがって、Direct Connect の情報を取得するには、VMware Cloud on AWS 関連のデータ ソース (vCenter Server と NSX Manager) を追加する必要があります。

注： Direct Connect のサポートのために、AWS アカウントやその他のデータ ソースを追加する必要はありません。

ただし、パス トポロジ情報を取得するには、Cisco N9k や Cisco ASR 9k (汎用ルーター) などのコロケーションルーターを追加する必要があります。

Direct Connect のサポートによって収集されるデータ

- VMware Cloud on AWS の SDDC 内の Direct Connect に関連した設定の詳細。
- SDDC レベルで Direct Connect 用にアドバイズおよび学習されたサブネット。
- SDDC に関連付けられた Direct Connect インターフェイス (VIF) の設定情報。

- VMware Cloud on AWS の分散ファイアウォール (DFW) によって報告されるフロー。

注：

- コロケーション ルーターでは、NetFlow を有効にすることが必須ではありません。
- Direct Connect では、ルート ベースの VPN はサポートされていません。そのため、[Direct Connect へのバックアップとして VPN を使用する] オプションを有効にした場合でも、VPN によるバックアップは失敗します。
- メトリックと、アドバタイズまたは学習されたサブネットの情報は、個々の VIF レベルでは取得されません。

Direct Connect のエンティティ

- VMware Cloud on AWS Direct Connect : これは vRealize Network Insight のすべての Direct Connect エンティティの親エンティティであり、VMware Cloud on AWS の SDDC 内の Direct Connect の設定情報をモデル化します。
- Direct Connect インターフェイス : VMware Cloud on AWS によって提供される AWS Direct Connect の VIF 情報をモデル化します。このエンティティにより、VMware Cloud on AWS とオンプレミス データセンターの間で、アドバタイズおよび学習されたルートの交換が可能になります。

この章には、次のトピックが含まれています。

- [VMC Direct Connect の詳細の表示](#)
- [Direct Connect 上のフローの表示](#)
- [Direct Connect 検索クエリ](#)

VMC Direct Connect の詳細の表示

[VMC Direct Connect] 画面では、VMware Cloud on AWS から収集された情報に基づいて、Direct Connect のプロパティや関連付けられたエンティティの概要を確認できます。

表 7-1. Direct Connect のダッシュボード

セクション	詳細
プロパティ	関連付けられた Software-Defined Data Center (SDDC)、ローカル ASN、学習およびアドバタイズされたルート、アドバタイズされたルートの障害などを含む、Direct Connect のプライマリ プロパティ。
Direct Connect インターフェイス	Direct Connect に関連付けられたすべての Direct Connect 仮想インターフェイスのリスト
イベント	Direct Connect に関連付けられたイベントのリスト。

Direct Connect 上のフローの表示

Direct Connect で実行されているすべてのフローのリストを表示することで、Direct Connect のトラフィックを確認できます。これにより、Direct Connect の利用率レベルを分析して理解することができます。

Flows where connection = **Direct Connection ID** クエリを使用して検索すると、Direct Connect を経由して送信されるフローのリストと、特定の Direct Connect のバンド幅使用率やネットワークトラフィック速度などの情報が表示されます。この行を更新します。[フロータイプ] で、フローのタイプが VPN、Direct Connect、ハイブリッドネットワークのいずれであるかを確認できます。

Direct Connect フローのみを表示するには、次のクエリを実行します。

```
flows where flow type = Direct Connect group by Connection
```

各 Direct Connect 接続で実行されているフローの数とデータボリュームを表示するには、次のクエリを実行します。

```
max(series(sum(Bytes))) of Flows where flow type = Direct Connect and group by Connection
```

各 Direct Connect インターフェイスでのフロー数とパケット数を表示するには、次のクエリを実行します。

```
max(series(sum(packets))) of Flows where flow type = Direct Connect and group by Connection
```

その他のクエリについては、[Direct Connect 検索クエリ](#)を参照してください。

Direct Connect 検索クエリ

vRealize Network Insight で、VMware Cloud on AWS Direct Connect と Direct Connect インターフェイスのエンティティを検索できます。

表 7-2. 検索クエリ

説明	クエリ
情報をフィルタリングできる項目に基づいて VMware Cloud on AWS Direct Connect エンティティのリストを取得する	VMC Direct Connect where
VMware Cloud on AWS Direct Connect リスト表示を取得する	VMC Direct Connect
Direct Connect を経由する最大データ ボリュームを取得する	max(series(sum(bytes))) of flows where connection = ' Connection-ID ' and flow type = 'Different Dc' and source vm is set and destination vm is set and flow type = 'Direct Connect'
Direct Connect を経由する最大パケット数を取得する	max(series(sum(packets))) of flows where connection = ' Connection-ID ' and flow type = 'Different Dc' and source vm is set and destination vm is set and flow type = 'Direct Connect'
Direct Connect を経由してインターネットに送信される最大パケット数を取得する	max(series(sum(packets))) of flows where connection = ' Connection-ID ' and flow type = 'Destination is internet' and flow type = 'Direct Connect'

表 7-2. 検索クエリ (続き)

説明	クエリ
Direct Connect を経由してインターネットに送信される最大データボリュームを取得する	<code>max(series(sum(bytes))) of flows where connection = 'Connection-ID' and flow type = 'Destination is internet' and flow type = 'Direct Connect'</code>
Direct Connect を経由してデータセンター間で送信される最大パケット数を取得する	<code>max(series(sum(packets))) of flows where connection = 'Connection-ID' and flow type = 'Different Dc' and source vm is set and destination vm is set group by Source Dc, Destination Dc and flow type = 'Direct Connect'</code>
Direct Connect を経由してデータセンター間で送信される最大データボリュームを取得する	<code>max(series(sum(bytes))) of flows where connection = '64638-10.63.229.131' and flow type = 'Different Dc' and source vm is set and destination vm is set group by Source Dc, Destination Dc and flow type = 'Direct Connect'</code>

vRealize Operations Manager 統合



vRealize Operations Manager を使用すると、vRealize Operations Manager に vRealize Network Insight のアラートを表示できます。また、vRealize Network Insight からのネットワーク情報を vRealize Operations Manager に表示することもできます。

vRealize Operations Manager は一連の vRealize Network Insight API を使用して、アラート ダッシュボードにアラートのリストを表示します。アラート名の `vrni-` プリフィックスによって vRealize Network Insight アラートを識別できます。また、アラートがトリガされたエンティティを表示することもできます。

vRealize Network Insight API のリストについては、『[vRealize Network Insight API ガイド](#)』を参照してください。

仮想マシン、ホスト、NSX-V、NSX-T などのエンティティ画面で [vRNI のコンテキストで起動] オプションを使用して、この特定のエンティティのダッシュボードを表示できます。これにより、ネットワークの健全性を確認し、ネットワークの問題をデバッグできます。

vRealize Network Insight を vRealize Operations Manager と統合する方法については、[VMware vRealize Operations Management Pack for vRealize Network Insight](#) を参照してください。vRealize Operations Manager のサポート対象バージョンの詳細については、[VMware 製品の相互運用性マトリックス](#)を参照してください。

注： vRealize Operations Manager ユーザーを vRealize Network Insight に追加する必要があります。また、この機能を vRealize Operations Manager で使用するには、ユーザーにメンバー以上の権限が必要です。

クラスタの作成と拡張

9

この章には、次のトピックが含まれています。

- クラスタの作成
- クラスタの拡張

クラスタの作成

[インストールとサポート] 画面からクラスタを作成できます。

前提条件

2 つ以上の追加のプラットフォームが必要です。追加のプラットフォーム仮想マシンは、展開してパワーオンする必要があります。

クラスタを作成するには

- 1 [プラットフォーム仮想マシン] の [クラスタの作成] をクリックします。
- 2 [クラスタの作成] 画面で、次の情報を入力します。
 - [IP アドレス]: 追加する新しいプラットフォームの IP アドレスを入力します。
 - [パスワード]: プラットフォーム仮想マシンのサポート ユーザー パスワードを入力します。パスワードをまだ変更していない場合は、『vRealize Network Insight Installation Guide』の「Default Login Credentials」セクションを参照してください。
- 3 さらに多くのプラットフォームを追加するには、[さらに追加] をクリックして、IP アドレスとサポート ユーザー パスワードを入力します。
- 4 [送信] をクリックします。[はい] をクリックします。

5 クラスタの作成後、ユーザーは製品に再度ログインする必要があります。

注：

- [クラスタの作成] オプションは、プラットフォームのブリック サイズが大きい場合にのみ有効になります。クラスタを作成するには、すべてのプラットフォームが大きいブリックである必要があります。
 - 1つのノードでテレメトリを有効にすると、すべてのノードでテレメトリが有効になります。
 - クラスタを拡張するには、『vRealize Network Insight Installation Guide』の「Expanding a Cluster」セクションを参照してください。
-

クラスタの拡張

クラスタが作成されたら、そのクラスタにプラットフォーム ノードを追加してクラスタを拡張できます。

注： クラスタの拡張操作は、Platform 1 (P1) ノードからのみ実行する必要があります。

手順

- 1 [インストールとサポート] 画面で、[プラットフォーム仮想マシン] の [クラスタの拡張] をクリックします。
- 2 クラスタに属する仮想マシンの IP アドレスは、[クラスタの拡張] 画面にすでにリストされています。1 台以上のノードを既存のクラスタに追加するには、ノードの IP アドレスとサポート ユーザーのパスワードを指定します。

注：

- 現在、vRealize Network Insight は既存のクラスタで 10 台のノードをサポートしています。この制限に達すると、[さらに追加] ボタンが無効になります。
 - すべての新しいノードがプロビジョニングされていないこと、および SSH を介して到達可能であることを確認します。
 - クラスタの拡張に進む前に、既存のプラットフォーム仮想マシンのバックアップを作成しておく必要があります。
-

- 3 [送信] をクリックします。

ステップバイステップの進行状況が表示されます。

- 4 クラスタ拡張リンクが完了すると、成功を示すメッセージが表示されます。

クラスタ拡張の進行中は、他の処理でアプリケーションを使用することはできません。

vRealize Network Insight でのフロー 一の設定

10

この章には、次のトピックが含まれています。

- IPFIX 設定の有効化
- 物理サーバのフロー サポート
- ブロックおよび保護されたフローの表示
- ネットワーク アドレス変換 (NAT)
- VMware Cloud on AWS 個のフロー
- VPC フロー ログの作成
- F5 から vRealize Network Insight コレクタへのフロー レコードの送信

IPFIX 設定の有効化

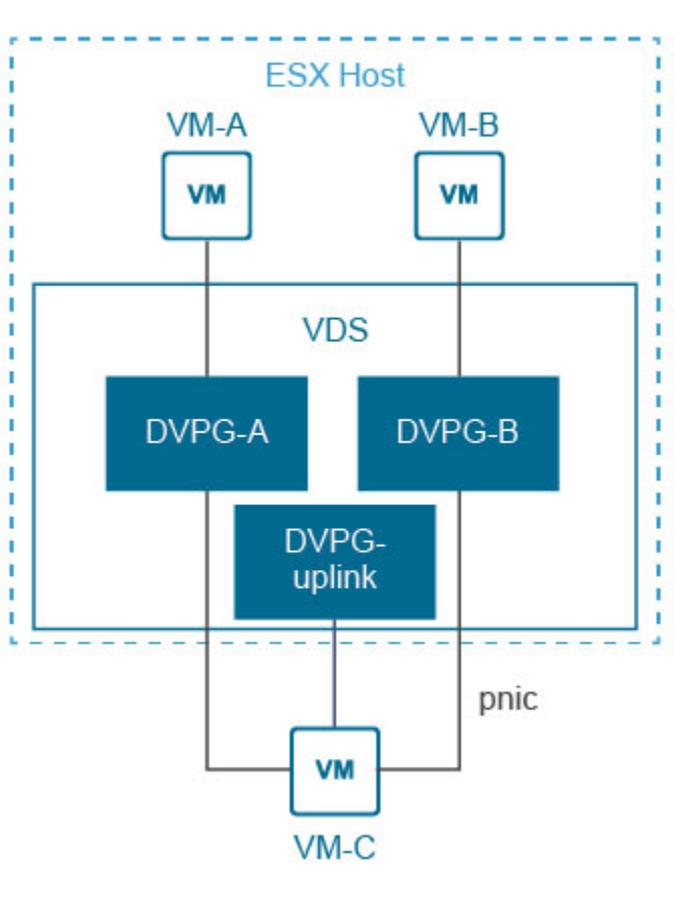
IPFIX は、フロー情報をエクスポートするための IETF プロトコルです。

フローは、特定のタイムスロットで転送されるパケットのセットとして定義され、同じ 5 組の値（送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、プロトコル）を共有します。フロー情報には、タイムスタンプ、パケット/バイト数、入力/出カインターフェイス、TCP フラグ、VXLAN ID、カプセル化されたフロー情報などのプロパティが含まれます。

Distributed Switch および DVPG での IPFIX 設定

vSphere 環境の Distributed Switch は、IPFIX を使用してフロー情報をエクスポートするように設定できます。フロー監視は、Distributed Switch に接続されたすべてのポート グループで有効にする必要があります。パケットが Distributed Switch のポート X に到着し、ポート Y から送信されると、ポート Y でフロー監視が有効な場合は対応するフロー レコードが生成されます。

セッションの完全な情報を分析するには、両方向のパケットに関する IPFIX データが必要です。次の図では、仮想マシン-A が DVPG-A との接続を介して 仮想マシン-C と通信しています。DVPG-A が提供するのは C→A パケットに関するデータのみで、DVPG-Uplink は A→C パケットに関するデータを提供します。A のトラフィックの完全な情報を取得するには、IPFIX を DVPG-A と DVPG-Uplink で有効にする必要があります。



vRealize Network Insight プロキシ仮想マシンには、IPFIX フロー情報用の組み込みのコレクタ/レシーバがあります。IPFIX の情報収集は、vCenter Server のデータ ソース設定で、さまざまな詳細度レベルを使用して有効にできます。

Distributed Switch および DVPG での IPFIX 設定の有効化

vCenter Server レベルで IPFIX 情報を有効にするには、次の手順を実行します。

手順

- 1 vRealize Network Insight で vCenter Server を追加する際に [この vCenter Server で NetFlow (IPFIX) を有効にする] チェック ボックスを選択します。
使用可能なすべての Distributed Switch のリストが表示されます。
- 2 vCenter Server で使用可能な Distributed Switch のリストから、IPFIX を有効にする Distributed Switch を選択します。
- 3 いずれかのホストにサポートされていないバージョンの ESXi がある場合は、Distributed Switch の通知アイコンが表示されます。vRealize Network Insight によって、IPFIX が vRealize Network Insight のプロキシ仮想マシンとは別の IP アドレスを持つ Distributed Switch 用にすでに設定されていることを検出した場合、[オーバーライド] ボタンが表示されます。[オーバーライド] をクリックして、その Distributed Switch の下にある DVPG のリストを表示します。

- 4 選択した Distributed Switch について使用可能な DVPG のリストが表示されます。デフォルトでは、すべての DVPG が選択されています。[手動選択] を有効にして、IPFIX を有効にする特定の DVPG を選択します。目的の DVPG を選択し、[送信] をクリックします。

注： 通知アイコンが付いた DVPG は、それがアップリンク DVPG であり、選択する必要があることを示しています。

VMware NSX IPFIX の設定

VMware NSX IPFIX は、物理デバイスの場合と同様のネットワーク監視データを提供します。これにより管理者は、仮想ネットワークの状態を明確に把握できます。

VMware NSX は、ネットワーク管理者がネットワークを物理ハードウェアから分離できるようにすることで、ネットワークを仮想化します。この機能により、必要に応じてネットワークを拡張および縮小し、そのネットワークを通過するアプリケーションに対してネットワークを透過的にすることができます。

NSX IPFIX を仮想ネットワークで使用することで、ネットワーク管理者は仮想オーバーレイ ネットワークを把握できます。Netflow を使用した VXLAN IPFIX は、ホストのアップリンクで有効です。これにより、パケットをカプセル化している VTEP を把握し、NSX 論理スイッチ (VXLAN) 上でホスト間トラフィックを生成した仮想マシンの詳細を確認できます。

分散ファイアウォールは、フローのステートフルな追跡を実装します。これらの追跡対象フローが一連の状態変化をたどる際、IPFIX を使用して、そのフローのステータスに関するデータをエクスポートできます。

追跡対象イベントには、フロー作成、フロー拒否、フロー更新、およびフロー分解が含まれます。拒否されたイベントは、Syslog としてエクスポートされます。

VMware NSX-V IPFIX の有効化

vRealize Network Insight で VMware NSX-V IPFIX を有効にするには、次の手順を実行します。

前提条件

- セキュリティ管理者またはエンタープライズ管理者の認証情報があることを確認します。
- NSX IPFIX データの収集が必要なすべての Distributed Switch と DVPG で、Distributed Switch IPFIX を有効にすることをお勧めします。Distributed Switch IPFIX は、関連付けられている vCenter Server の詳細ページから有効にすることができます。

手順

- ◆ NSX-V Manager データ ソースを追加または編集するときは、[IPFIX の有効化] を選択します。

VMware NSX-T DFW IPFIX の有効化

vRealize Network Insight で VMware NSX-T IPFIX を有効にするには、次の手順を実行します。

前提条件

- 次のいずれかの権限があることを確認します。
 - enterprise_admin

- network_engineer
- security_engineer
- 分散ファイアウォール (DFW) ファイアウォールを有効にします。
- Network Insight IPFIX プロファイルで優先順位 0 を使用できるようにします。優先順位 0 の別の IPFIX プロファイルがある場合は、別の値に変更する必要があります。

手順

- ◆ NSX-T Manager データ ソースを追加または編集するときは、[IPFIX の有効化] を選択します。

次のステップ

IPFIX を有効にすると、vRealize Network Insight が独自の Network Insight Collector プロファイルと Network Insight IPFIX プロファイルを NSX-T に作成します。これらのプロファイルは変更しないでください。

NSX-T で IPFIX を有効にした後でフローが vRealize Network Insight に表示されない場合、次のイベントが発生する可能性があります。

- Network Insight Collector プロファイルが NSX-T Manager に登録されていない。
- Network Insight IPFIX プロファイルが NSX-T Manager に登録されていない。
- Network Insight IPFIX プロファイルのポート番号が変更された。
- Network Insight Collector プロファイルが、NSX-T Manager の Network Insight IPFIX プロファイルと一致しない。

注： 上記の問題をすべて解決するには、NSX-T IPFIX を再度有効にします。

- NSX-T Manager で Network Insight IPFIX プロファイルの優先順位がゼロではない。
この問題を解決するには、NSX-T Manager にログインし、Network Insight IPFIX プロファイルの優先順位をゼロに設定します。
- Network Insight Collector の IP アドレスを NSX-T Manager の既存の Network Insight Collector プロファイルに追加できない。
NSX-T Manager の Network Insight Collector プロファイルからいずれかのコレクタを削除し、データ ソース ページから NSX-T IPFIX を再度有効にします。
- 分散ファイアウォールが NSX-T Manager で無効になっている。
NSX-T Manager にログインし、DFW ファイアウォールを有効にします。

NSX-T 2.4 では、NSX-T で IPFIX を有効にした後で vRealize Network Insight にフローが表示されない場合、以下のイベントが発生する可能性があります。

- Network Insight IPFIX コレクタの設定が NSX-T Manager のコレクタ プロファイルにない。
- NSX-T Manager に DFW IPFIX プロファイルがない。

これらの問題を解決するには、DFW IPFIX を再度有効にします。

注： NSX-T にあるすべての論理スイッチは、10 ~ 15 分以内に IPFIX プロファイルに追加されます。

物理サーバのフロー サポート

vRealize Network Insight は、バージョン v5、v7、および v9 の NetFlow データを送信するデバイスをサポートしています。DNS マッピングおよびサブネット VLAN マッピング情報が指定されている場合、vRealize Network Insight は DNS ドメイン、DNS ホスト名、サブネット、およびレイヤー 2 ネットワークを使用して、NetFlow データを強化できます。この機能は、Enterprise ライセンス ユーザーのみ使用できます。

vRealize Network Insight で NetFlow を設定するには、次の手順を実行します。

- 1 NetFlow および sFlow 用の物理フロー コレクタの追加。
- 2 物理デバイスでの NetFlow コレクタの設定。
- 3 DNS マッピング ファイルのインポート。
- 4 サブネットと VLAN の間のマッピングの設定。

物理デバイスでの NetFlow コレクタの設定

NetFlow 情報を vRealize Network Insight NetFlow コレクタに送信するには、物理デバイスを手動で設定します。ほとんどの物理デバイスでの設定手順は次のとおりです。

- 1 フロー レコードを作成します。

フロー レコードの必須フィールドは次のとおりです。

- 次のフィールドを Match としてマークします。
 - `ipv4 protocol`
 - `ipv4 source address`
 - `ipv4 destination address`
 - `transport source-port`
 - `transport destination-port`
 - `interface input`
- 次のフィールドを Collect としてマークします。
 - `direction`
 - `counter bytes`
 - `counter packets`
 - `timestamp sys-uptime first`
 - `timestamp sys-uptime last`
- 次のフィールドを Match または Collect としてマークします。そうでない場合はスキップします。
 - `transport tcp flags`

- 2 フロー エクスポーターを作成します。
 - vRealize Network Insight NetFlow プロキシ IP アドレスとポート 2055 を指定します。
- 3 フロー キャッシュを次のように設定します。
 - アクティブ タイムアウト : 30 秒
 - 非アクティブ タイムアウト : 60 秒
- 4 作成されたフロー レコードとフロー エクスポートを使用して、フロー モニターを作成します。
- 5 各インターフェイスでモニターを設定します。

前提条件

例

物理デバイスを設定するためのサンプル手順は、次のセクションで提供されています。

- [Cisco 4500](#)
- [Cisco Nexus 1000v](#)
- [Cisco Nexus 9000](#)

注： 手順は、バージョンおよびデバイスによって異なる場合があります。

Cisco 4500

- 1 フロー レコードを作成するには、次を実行します。

```
configure terminal

flow record netflow-original

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match interface input

collect transport tcp flags

collect counter bytes

collect counter packets

collect timestamp sys-uptime first

collect timestamp sys-uptime last

End
```

- 2 フロー エクスポーターを作成するには、次を実行します。

```
configure terminal
flow exporter e1
destination <PROXY_IP>
transport udp 2055
end
```

- 3 フロー モニターを作成するには、次を実行します。

```
configure terminal
flow monitor m1
record netflow-original
exporter e1
end
```

- 4 タイムアウトを設定するには、次を実行します。

```
configure terminal
cache timeout inactive 30
cache timeout active 60
end
```

- 5 Egress モードと Ingress モード、または少なくとも Ingress モードで各インターフェイスに対するフロー モニターを設定するには、次を実行します。

```
configure terminal
interface <INTERFACE_NAME>
ip flow monitor m1 unicast input
end
```

Cisco Nexus 1000v

- 1 タイムアウトを設定するには、次を実行します。

```
configure terminal
Active timeout 60
Inactive timeout 15
end
```

- 2 エクスポートを設定するには、次を実行します。

```
configure terminal
```

```

flow exporter <EXPORTER_NAME>
destination <PROXY_IP>
transport udp 2055
source <VSM_IP_OR_SUBNET>
end

```

- 3 各インターフェイスに対してフロー モニターを設定するには、次を実行します。

```

configure terminal
flow monitor <MONITOR_NAME>
record netflow-original
exporter <EXPORTER_NAME>
end

```

- 4 Egress モードと Ingress モード、または少なくとも Ingress モードで各インターフェイスに対するフロー モニターを設定するには、次を実行します。

```

configure terminal
port-profile type vethernet <IF_NAME>
ip flow monitor <MONITOR_NAME> input
ip flow monitor <MONITOR_NAME> output
.
.
end

```

Cisco Nexus 9000

次に、Cisco Nexus 9000 のデバイス コマンドの例をいくつか示します。

- 1 NetFlow 機能を有効にするには、次を実行します。

```

configure terminal
feature netflow
end

```

- 2 フロー レコードを作成するには、次を実行します。

```

configure terminal
flow record vrni-record
match ipv4 protocol
match ipv4 source address

```

```
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
collect transport tcp flags
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
End
```

- 3 フロー エクスポーターを作成するには、次を実行します。

```
configure terminal
flow exporter vrni-exporter
destination <PROXY_IP>
transport udp 2055
version 9
source <INTERFACE_NAME>
end
```

- 4 各インターフェイスに対してフロー モニターを作成するには、次を実行します。

```
configure terminal
flow monitor vrni-monitor
record vrni-record
exporter vrni-exporter
end
```

- 5 タイムアウトを設定するには、次を実行します。

```
configure terminal
cache timeout inactive 30
cache timeout active 60
end
```

- 6 Egress モードと Ingress モード、または少なくとも Ingress モードで各インターフェイスに対するフロー モニターを設定するには、次を実行します。

```

configure terminal

interface <INTERFACE_NAME>

ip flow monitor vrni-monitor input

end

```

フローと IP アドレス エンドポイントの拡充

ユーザー インターフェイスから DNS マッピングとサブネット VLAN (仮想ローカル エリア ネットワーク) マッピング情報をインポートできます。

このフロー情報は、DNS データのインポートおよびサブネット VLAN (仮想ローカル エリア ネットワーク) マッピングの仕様に基づいて、次のタイプの情報を使用して拡充されます。

- ソース DNS ドメイン
- ソース DNS ホスト名
- ターゲット DNS ドメイン
- ターゲット DNS ホスト名
- ソース L2 ネットワーク
- ソース サブネット ネットワーク
- ターゲット L2 ネットワーク
- ターゲット サブネット ネットワーク

IP アドレス エンドポイント情報は、DNS データのインポートおよびサブネットと VLAN (仮想ローカル エリア ネットワーク) 間のマッピングの仕様に基づいて、次のタイプの情報を使用して拡充されます。

- DNS ドメイン
- DNS ホスト名
- FQDN
- L2 ネットワーク
- サブネット ネットワーク

DNS 情報によるフローの追加の詳細については、[DNS マッピング ファイルのインポート](#)を参照してください。

サブネットと VLAN (仮想ローカル エリア ネットワーク) 間のマッピングを介したフローの拡充の詳細については、[サブネットと VLAN の間のマッピングの設定](#)を参照してください。

注：

- DNS マッピングとサブネットの情報は、物理 IP アドレスについてのみ拡充されます。サブネットまたは DNS マッピング情報は、仮想 NIC とは関連付けられません。
 - この情報は、この情報がインポートされた後に vRNI に表示されたフローについてのみ拡充されます。
-

[物理から物理] フローの検索

[物理から物理] フローは、次の属性に基づいて検索できます。

- ソース DNS ホスト
- ターゲット DNS ホスト
- ソース DNS ドメイン
- ターゲット DNS ドメイン
- ソース サブネット ネットワーク
- ターゲット サブネット ネットワーク

[物理から物理] フローは、次の属性に基づいて検索できます。強化された DNS およびサブネット VLAN マッピング情報を使用したフロー検索クエリの例は、次のとおりです。

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Physical-Physical'
```

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Source is VM' and  
flow type = 'Destination is Physical'
```

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Source is Internet'  
and flow type = 'Destination is Physical'
```

ブロックおよび保護されたフローの表示

NSX と IPFIX の連携により、システム内のブロックおよび保護されたフローを表示できます。

[マイクロセグメンテーションの計画] 画面の基本的なフィルタは、次のとおりです。

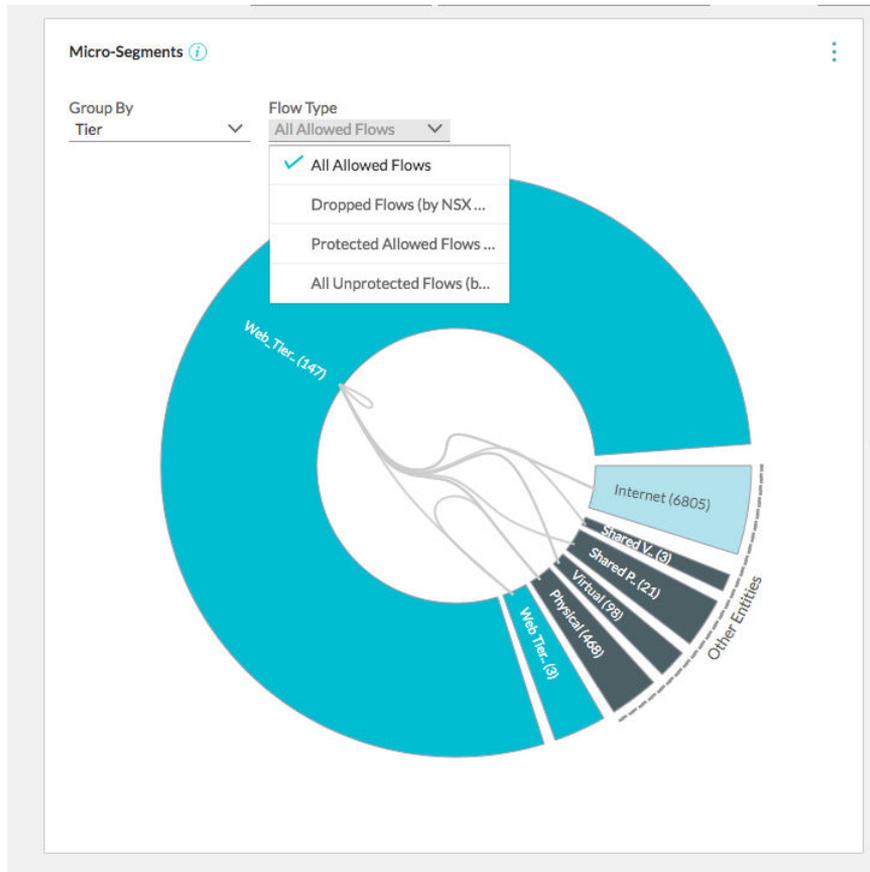
- 許可されたすべてのフロー：デフォルトでは、このオプションが選択されています。ファイアウォール ルールのアクションが [許可] に設定されているすべてのフローを表示するには、このオプションを選択します。
- ドロップしたフロー：このオプションは、ドロップしたフローを検出し、セキュリティをより適切に計画するのに役立ちます。
- 保護されたすべてのフロー：このオプションは、any(source)any(dest)any(service)allow 以外のタイプのルールが関連付けられているすべてのフローを検出するのに役立ちます。前述のタイプ以外のルールが関連付けられているフローは、保護されたフローと呼ばれます。
- 保護されていないすべてのフロー：このオプションは、タイプが any(source)any(dest)any(service)allow のデフォルト ルールを持つすべてのフローを検出するのに役立ちます。前述のタイプがデフォルト ルールになっているフローは、保護されていないフローと呼ばれます。

ファイアウォール ルールは、許可されたフローと保護されていないフローに対してのみ表示されます。

たとえば、計画の段階で、システムで許可されているフローを確認する場合は、次の手順を実行します。

- 1 [マイクロセグメンテーションの計画] 画面の特定のグループで、ドロップダウン メニューから [許可されたすべてのフロー] を選択します。
- 2 トポロジ図でドロップしたフローをクリックすると、対応する推奨ファイアウォール ルールが表示されます。

3 これらのファイアウォール ルールを NSX Manager にエクスポートして実装します。



ネットワーク アドレス変換 (NAT)

vRealize Network Insight は、フロー内の静的 NAT (SNAT)、動的 NAT (DNAT)、再帰ルールと、NSX-V、NSX-T Edge、Fortinet、および Check Point で仮想マシン間パスをサポートします。

vRealize Network Insight での NAT フローのサポートは次のとおりです。

- vRealize Network Insight は、NSX for vSphere および NSX-T の場合に、ネストされた NAT 階層をサポートします。物理デバイスについては、vRealize Network Insight は Fortinet の場合のみ、単一の階層 (DNAT) をサポートします。
- vRealize Network Insight は、NAT で定義されたアップリンクを使用して Edge と階層ルーターをサポートします。

注： NSX Edge バージョン 5.5 またはそれ以前のバージョンに対する NAT ルールはサポートされていません。

- vRealize Network Insight は範囲がある SNAT ルールをサポートしています。ただし、DNAT は、宛先と変換された IP アドレス (NSX for vSphere とのパリティ) 間の 1 対 1 のマッピングである必要があります。
- Check Point の場合、自動または手動で生成された NAT ルールは、ネットワーク、ネットワークグループ、またはアドレス範囲と同様に、ソースとターゲットの両方でサポートされます。

NAT ルールを表示するには、次のクエリを使用します。

- NSX-T のすべての NAT ルールを表示するには、NSX-T Edge NAT Rule クエリを使用します。
- NSX-v のすべての NAT ルールを表示するには、Edge NAT Rules クエリを使用します。
- Fortinet のすべての NAT ルールを表示するには、Fortinet NAT Rule クエリを使用します。
- Check Point のすべての NAT ルールを表示するには、Check Point NAT Rule クエリを使用します。
- すべての NAT ルールを表示するには、NAT Rule クエリを使用します。

クエリ

NAT ルールを表示するには、次のクエリを使用します。

- NSX-T のすべての NAT ルールを表示するには、NSX-T Edge NAT Rule クエリを使用します。
- NSX-v のすべての NAT ルールを表示するには、Edge NAT Rules クエリを使用します。
- Fortinet のすべての NAT ルールを表示するには、Fortinet NAT Rule クエリを使用します。
- Check Point のすべての NAT ルールを表示するには、Check Point NAT Rule クエリを使用します。
- すべての NAT ルールを表示するには、NAT Rule クエリを使用します。

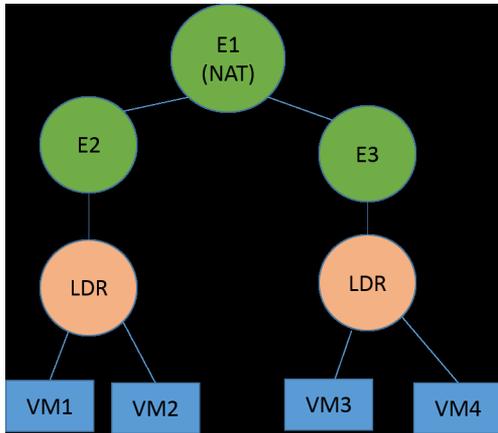
考慮事項

- vRealize Network Insight は次の使用方法をサポートしていません。
 - NSX-T では、サービス レベルで NAT ルールを適用できます。たとえば、NSX-T では、L4 ポート セットはサービスの一種であり、関連付けられたプロトコルは TCP または UDP になります。そのため、仮想マシン間パスでは、サービス レベルの詳細はサポートされません。
 - ポート レベルの変換はサポートされません。
 - SNAT 照合先のアドレスと DNAT 照合元のアドレスはサポートされません。SNAT ルールを指定するときに、SNAT 照合先アドレスを宛先 IP アドレスとして使用します。DNAT ルールを指定するときに、DNAT 照合元アドレスを送信元 IP アドレスとして使用します。たとえば、SNAT ルールに宛先 IP アドレスが記載されている場合、パケットに宛先のアドレスが宛先 IP アドレスとしてあるかどうかに関係なく、vRealize Network Insight は SNAT ルールを適用します。
 - NSX-T Edge ファイアウォールでは、同じ論理ルーターで NAT サービスが有効になっている場合、データパスに影響を及ぼします。フローが NAT と Edge ファイアウォールの両方に一致する場合、NAT ルックアップ結果がファイアウォールよりも優先されます。そのため、ファイアウォールはそのフローに適用されません。フローがファイアウォール ルールのみ一致する場合、そのフローに対するファイアウォールの検索結果が受け入れられます。
 - サービス変換はサポートされていません。
 - vSEC NAT はサポートされていません。

NAT フローのサポート - 例

このセクションでは、vRealize Network Insight でサポートされている NAT フローの例がいくつか示します。

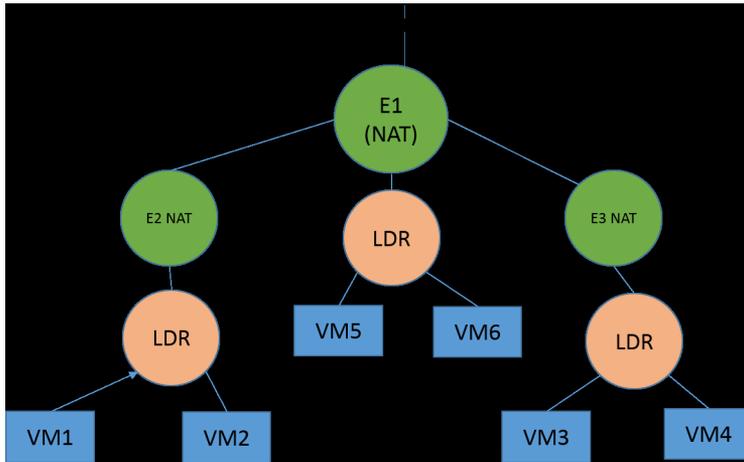
例 1



上のトポロジでは、E2、E3、LDR、仮想マシン（VM1、VM2、VM3、VM4）は NAT ドメイン E1 に含まれます。E1 より上位にあるもの（E1 のアップリンクなど）は、デフォルトの NAT ドメインに含まれます。上のトポロジは、次の要素で構成されています。

VM1 から VM2 のフローと VM2 から VM1 のフローが vRealize Network Insight で報告されます。同様に、VM3 から VM4 のフローと VM4 から VM3 のフローが報告されます。

例 2



上のトポロジは、次の要素で構成されています。

- VM1 および VM2 は、E2 ドメインの一部です。
- VM3 および VM4 は、E2 ドメインの一部です。
- E2 および E3 の NAT ドメインは、E1 NAT ドメインの子ドメインです。
- E1 は、デフォルトの NAT ドメインの単一の子です。
- VM5 および VM6 は、E1 NAT ドメインの一部です。

上のトポロジでは、次のフローが vRealize Network Insight で報告されます。

- VM5 から VM6 へのフロー

- (VM1、VM2) から (VM3、VM4) へのフロー

VMware Cloud on AWS 個のフロー

[設定] 画面で、データ ソースに対して IPFIX を有効にしている場合、フロー カウントと前回の収集時間を表示できます。

特定のフローを検索して、エンティティに関連付けられている詳細を取得できます。たとえば、ポリシー セグメントとポリシー グループの情報を Source L2 Network と Source Security Group でそれぞれ確認できます。フローに添付されたポリシー ファイアウォール ルールを表示することもできます。

vRealize Network Insight は、VPN 経由のハイブリッド フローをサポートします。フロー情報は、ソースとターゲットのエンティティによって拡充されます。

The screenshot shows a flow log entry with the following details:

Source IP	Destination IP	Flow Type	Destination Port	Protocol
192.168.2.101	192.168.46.21	Destination VM [11 more]	389 [tcp]	UDP
Source VM	Destination VM	Shared	Traffic Type	Network Layer
vms1-japan01-test	vms1-computehost-202	Yes	East-West Traffic	Router
Within Host/AWS VPC	Source Security Group	Source L2 Network	Destination L2 Network	Source Folder
No	sg-14062-vm	ns-vpn	comp-conf-duplicate-ss	Workloads
Destination Folder	Source Cluster	Destination Cluster	Source ResourcePool	Destination Resource Pool
vm	Cluster-1	Cluster-2	Compute-ResourcePool	Resources
Destination Host	Source Host	Service Endpoints	Source Datacenter	Destination Datacenter
10.196.74.202	10.70.38.48	VM-1-Comp-Host-202 (1 more)	SDDC-Datacenter	DC-1
Source Managers	Destination Managers	Repositories	NS-Collector	NS-Collector
nsManager-02b-34-218-131-237.vmw.com	10.196.74.81	nsCollector [2 more]		

Applied Firewall Rules:

Manager	Rule	RuleID	Action
nsManager-02b-34-218-131-237.vmw.com	VMC_Hybrid_Any	VMC_Hybrid_Any	ALLOW

注： VMware Cloud on AWS をバージョン 1.8 から 1.9 にアップデートした場合、ユーザー インターフェイスにこのフローが 2 回表示されることがあります。

VPC フロー ログの作成

Virtual Private Cloud (VPC) のフロー ログを使用すると、VPC 内のネットワーク インターフェイスで送受信される IP トラフィックに関する情報を取得できます。

フロー ログは、AWS ポータルから作成できます。

手順

- 1 AWS コンソールにログインします。
- 2 [サービスの検索] テキスト ボックスで、**CloudWatch** と入力して選択します。
- 3 [ログ] - [アクション] - [ログ グループの作成] の順に移動します。
[ログ グループの作成] ウィンドウが表示されます。
- 4 [グループ名の作成] フィールドにグループ名を入力し、[ログ グループの作成] をクリックします。
- 5 上部のナビゲーション ペインで、[サービス] をクリックしてから、**VPC** と入力して選択します。
- 6 [VPC ダッシュボード] 画面で、[現在の VPC] をクリックします。

- 7 変更する VPC を選択し、[フロー ログ] - [フロー ログの作成] の順にクリックします。
- 8 [フロー ログの作成] ウィンドウで、以下のようにフロー ログを設定します。

オプション	アクション
フィルタ	[承諾]、[拒否]、[すべて] のいずれかを選択します。
ターゲット	[CloudWatch ログに送る] を選択します。
宛先ログ グループ	作成したログ グループを選択します。

- 9 [権限の設定] をクリックします。
[VPC フロー ログがアカウント内のリソースを使用する権限を要求しています] 画面が表示されます。
- 10 IAM ロールを作成します。
 - a [VPC フロー ログがアカウント内のリソースを使用する権限を要求しています] 画面の [IAM ロール] で、[新しい IAM ロールの作成] を選択します。
 - b [ロール名] テキスト ボックスにロールの名前を入力します。
 - a [許可] をクリックします。
- 11 [フロー ログの作成] 画面の [IAM ロール] ドロップダウンで、作成したロールを選択します。
- 12 [作成] をクリックします。

結果

選択されたログ グループでフロー ログの発行が開始されます。VPC フロー ログの詳細については、<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#create-flow-log> にある AWS ドキュメントを参照してください。

F5 から vRealize Network Insight コレクタへのフロー レコードの送信

フロー レコードを送信するには、次の操作を実行する必要があります。

SI 番号	タスク	リンク
1	IPFIX コレクタのプールを作成して、BIG-IP システムから IPFIX ログ メッセージを受信します。	IPFIX コレクタのプールの作成
2	ログの宛先を作成して、IPFIX テンプレートでログをフォーマットします。	IPFIX ログの宛先の作成
3	ログ発行元を作成して、指定したログの宛先にログを送信します。	ログ発行元の作成
4	iRule を作成して、設定された vRealize Network Insight コレクタにフロー情報を送信します。	iRule の作成

SI 番号	タスク	リンク
5	仮想サーバ構成に iRule を追加して、iRule がすべての仮想サーバのネットワーク トラフィックを解析できるようにします。	仮想サーバへの iRule の追加
6	コレクタ仮想マシンが F5 からアクセスできない場合は、フロー レコードを送信するためにコレクタのルート エントリを作成する必要があります。	ルート エントリの作成

IPFIX コレクタのプールの作成

IPFIX コレクタのプールを作成します。BIG-IP システムは、このプールに IPFIX ログ メッセージを送信します。

手順

- 1 F5 コンソールにログインします。
- 2 [メイン] - [ローカル トラフィック] - [プール] - [プール リスト] - [作成] の順にクリックします。
[新しいプール] 画面が開きます。
- 3 [名前] テキスト ボックスに、プールの一意の名前を入力します。
- 4 [健全性モニター] で、[gateway_icmp] を選択して [アクティブ] ボックスに移動します。
- 5 [新しいメンバー] セクションで、コレクタ IP アドレスを設定し、[追加] をクリックします。

オプション	アクション
ノード名	コレクタ IP アドレスを入力します。
サービス ポート	2055

- 6 [終了] をクリックします。

IPFIX ログの宛先の作成

ログの宛先を作成して、IPFIX テンプレートでログをフォーマットします。フォーマットされたログは IPFIX コレクタに送信されます。

手順

- 1 F5 コンソールで、[メイン] - [システム] - [ログ] - [設定] - [ログの宛先] - [作成] の順にクリックします。
[ログの宛先] 画面が表示されます。
- 2 [名前] テキスト ボックスに一意の名前を入力します。
- 3 [タイプ] リストで、[IPFIX] をクリックします。

- 4 [IPFIX 設定] を調整します。

オプション	アクション
プロトコル	[Netflow V9] をクリックします。
プール名	前の手順で作成したプールの名前をクリックします。

- 5 [終了] をクリックします。

ログ発行元の作成

指定された宛先にログを送信するには、ログ発行元を作成する必要があります。

手順

- 1 F5 コンソールで、[メイン] - [システム] - [ログ] - [設定] - [ログ発行元] - [作成] の順にクリックします。
[ログ発行元] 画面が表示されます。
- 2 [名前] フィールドに、一意の名前を入力します。
- 3 [宛先] ボックスで、以前に作成したログの宛先を [使用可能] ボックスから選択し、[選択済み] ボックスに移動します。
- 4 [終了] をクリックします。

iRule の作成

設定した vRealize Network Insight コレクタにフロー情報を送信するには、iRule を作成する必要があります。2 つの iRules を作成します。1 つの iRule は TCP プロトコル用、もう 1 つの iRule は UDP プロトコル用です。

手順

- 1 F5 コンソールで、[メイン] - [iRule] - [iRule リスト] - [作成] の順にクリックします。
[新しい iRule] 画面が表示されます。
- 2 [名前] テキスト ボックスに一意の名前を入力します。
- 3 [定義] テキスト ボックスに、TCP プロトコル用の TCP ルールと UDP プロトコル用の UDP ルールを入力します。ルールの詳細については、[TCP および UDP プロトコル用の iRule](#) を参照してください。
iRule で、作成済みの発行元が指定されていることを確認します。
- 4 [終了] をクリックします。

TCP および UDP プロトコル用の iRule

以下を使用して、TCP および UDP プロトコルの iRule を作成します。

TCP ルール

次のルールを使用して、TCP プロトコルの iRule を作成します。

注： iRule が、以前に作成したログ発行元を参照していることを確認します。

```

when RULE_INIT {
    set static::http_rule1_dest ""
    set static::http_rule1_tmplt ""
}

# CLIENT_ACCEPTED event to initiate IPFIX destination and template
when CLIENT_ACCEPTED {
    set start [clock clicks -milliseconds]
    if { $static::http_rule1_dest == "" } {
        # open the logging destination if it has not been opened yet
        set static::http_rule1_dest [IPFIX::destination open -publisher /Common/<Log Publisher>]
    }
    if { $static::http_rule1_tmplt == "" } {
        # if the template has not been created yet, create the template
        set static::http_rule1_tmplt [IPFIX::template create "flowStartMilliseconds \
            sourceIPv4Address \
            sourceIPv6Address \
            destinationIPv4Address \
            destinationIPv6Address \
            sourceTransportPort \
            destinationTransportPort \
            protocolIdentifier \
            octetTotalCount \
            packetTotalCount \
            octetDeltaCount \
            packetDeltaCount \
            postNATSourceIPv4Address \
            postNATSourceIPv6Address \
            postNATDestinationIPv4Address \
            postNATDestinationIPv6Address \
            postNAPTSourceTransportPort \
            postNAPTDestinationTransportPort \
            postOctetTotalCount \
            postPacketTotalCount \
            postOctetDeltaCount \
            postPacketDeltaCount \
            flowEndMilliseconds"]
    }
}

# SERVER_CONNECTED event to initiate flow data to vrni and populate 5 tuples
when SERVER_CONNECTED {
    set rule1_msg1 [IPFIX::msg create $static::http_rule1_tmplt]
    set client_closed_flag 0
    set server_closed_flag 0
    IPFIX::msg set $rule1_msg1 flowStartMilliseconds $start
    IPFIX::msg set $rule1_msg1 protocolIdentifier [IP::protocol]

    # Clientside

```

```

if { [clientside {IP::version}] equals "4" } {
    # Client IPv4 address
    IPFIX::msg set $rule1_msg1 sourceIPv4Address [IP::client_addr]
    # BIG-IP IPv4 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv4Address [clientside {IP::local_addr}]
} else {
    # Client IPv6 address
    IPFIX::msg set $rule1_msg1 sourceIPv6Address [IP::client_addr]
    # BIG-IP IPv6 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv6Address [clientside {IP::local_addr}]
}
# Client port
IPFIX::msg set $rule1_msg1 sourceTransportPort [TCP::client_port]
# BIG-IP VIP port
IPFIX::msg set $rule1_msg1 destinationTransportPort [clientside {TCP::local_port}]

# Serverside
if { [serverside {IP::version}] equals "4" } {
    # BIG-IP IPv4 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv4Address [IP::local_addr]
    # Server IPv4 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv4Address [IP::server_addr]
} else {
    # BIG-IP IPv6 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv6Address [IP::local_addr]
    # Server IPv6 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv6Address [IP::server_addr]
}
# BIG-IP self IP port
IPFIX::msg set $rule1_msg1 postNAPTSourceTransportPort [TCP::local_port]
# Server port
IPFIX::msg set $rule1_msg1 postNAPTDestinationTransportPort [TCP::server_port]
}

# SERVER_CLOSED event to collect IP pkts and bytes count on serverside
when SERVER_CLOSED {
    set server_closed_flag 1
    # when flow is completed, BIG-IP to server REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetTotalCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 packetTotalCount [IP::stats pkts out]
    # when flow is completed, server to BIG-IP RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetDeltaCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 packetDeltaCount [IP::stats pkts in]
    if { $client_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

# CLIENT_CLOSED event to collect IP pkts and bytes count on clientside
when CLIENT_CLOSED {
    set client_closed_flag 1
    # when flow is completed, client to BIG-IP REQUEST pkts and bytes octetDeltaCount
    IPFIX::msg set $rule1_msg1 postOctetTotalCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 postPacketTotalCount [IP::stats pkts in]
}

```

```

# when flow is completed, BIG-IP to client RESPONSE pkts and bytes count
IPFIX::msg set $rule1_msg1 postOctetDeltaCount [IP::stats bytes out]
IPFIX::msg set $rule1_msg1 postPacketDeltaCount [IP::stats pkts out]
# record the client closed time in ms
IPFIX::msg set $rule1_msg1 flowEndMilliseconds [clock click -milliseconds]
if { $server_closed_flag == 1 } {
    # send the IPFIX log
    IPFIX::destination send $static::http_rule1_dest $rule1_msg1
}
}

```

UDP ルール

次のルールを使用して、UDP プロトコルの iRule を作成します。

注： iRule が、以前に作成したログ発行元を参照していることを確認します。

```

when RULE_INIT {
    set static::http_rule1_dest ""
    set static::http_rule1_tmplt ""
}

# CLIENT_ACCEPTED event to initiate IPFIX destination and template
when CLIENT_ACCEPTED {
    set start [clock clicks -milliseconds]
    if { $static::http_rule1_dest == "" } {
        # open the logging destination if it has not been opened yet
        set static::http_rule1_dest [IPFIX::destination open -publisher /Common/<Log Publisher>]
    }
    if { $static::http_rule1_tmplt == "" } {
        # if the template has not been created yet, create the template
        set static::http_rule1_tmplt [IPFIX::template create "flowStartMilliseconds \
            sourceIPv4Address \
            sourceIPv6Address \
            destinationIPv4Address \
            destinationIPv6Address \
            sourceTransportPort \
            destinationTransportPort \
            protocolIdentifier \
            octetTotalCount \
            packetTotalCount \
            octetDeltaCount \
            packetDeltaCount \
            postNATSourceIPv4Address \
            postNATSourceIPv6Address \
            postNATDestinationIPv4Address \
            postNATDestinationIPv6Address \
            postNAPTSourceTransportPort \
            postNAPTDestinationTransportPort \
            postOctetTotalCount \
            postPacketTotalCount \
            postOctetDeltaCount \
            postPacketDeltaCount \
            flowEndMilliseconds"]
    }
}

```

```

}
}

# SERVER_CONNECTED event to initiate flow data to vrni and populate 5 tuples
when SERVER_CONNECTED {
  set rule1_msg1 [IPFIX::msg create $static::http_rule1_tmplt]
  set client_closed_flag 0
  set server_closed_flag 0
  IPFIX::msg set $rule1_msg1 flowStartMilliseconds $start
  IPFIX::msg set $rule1_msg1 protocolIdentifier [IP::protocol]

  # Clientside
  if { [clientside {IP::version}] equals "4" } {
    # Client IPv4 address
    IPFIX::msg set $rule1_msg1 sourceIPv4Address [IP::client_addr]
    # BIG-IP IPv4 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv4Address [clientside {IP::local_addr}]
  } else {
    # Client IPv6 address
    IPFIX::msg set $rule1_msg1 sourceIPv6Address [IP::client_addr]
    # BIG-IP IPv6 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv6Address [clientside {IP::local_addr}]
  }
  # Client port
  IPFIX::msg set $rule1_msg1 sourceTransportPort [UDP::client_port]
  # BIG-IP VIP port
  IPFIX::msg set $rule1_msg1 destinationTransportPort [clientside {UDP::local_port}]

  # Serverside
  if { [serverside {IP::version}] equals "4" } {
    # BIG-IP IPv4 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv4Address [IP::local_addr]
    # Server IPv4 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv4Address [IP::server_addr]
  } else {
    # BIG-IP IPv6 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv6Address [IP::local_addr]
    # Server IPv6 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv6Address [IP::server_addr]
  }
  # BIG-IP self IP port
  IPFIX::msg set $rule1_msg1 postNAPTSourceTransportPort [UDP::local_port]
  # Server port
  IPFIX::msg set $rule1_msg1 postNAPTDestinationTransportPort [UDP::server_port]
}

# SERVER_CLOSED event to collect IP pkts and bytes count on serverside
when SERVER_CLOSED {
  set server_closed_flag 1
  # when flow is completed, BIG-IP to server REQUEST pkts and bytes count
  IPFIX::msg set $rule1_msg1 octetTotalCount [IP::stats bytes out]
  IPFIX::msg set $rule1_msg1 packetTotalCount [IP::stats pkts out]
  # when flow is completed, server to BIG-IP RESPONSE pkts and bytes count
  IPFIX::msg set $rule1_msg1 octetDeltaCount [IP::stats bytes in]
  IPFIX::msg set $rule1_msg1 packetDeltaCount [IP::stats pkts in]
}

```

```

if { $client_closed_flag == 1 } {
    # send the IPFIX log
    IPFIX::destination send $static::http_rule1_dest $rule1_msg1
}
}

# CLIENT_CLOSED event to collect IP pkts and bytes count on clientside
when CLIENT_CLOSED {
    set client_closed_flag 1
    # when flow is completed, client to BIG-IP REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetTotalCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 postPacketTotalCount [IP::stats pkts in]
    # when flow is completed, BIG-IP to client RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetDeltaCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 postPacketDeltaCount [IP::stats pkts out]
    # record the client closed time in ms
    IPFIX::msg set $rule1_msg1 flowEndMilliseconds [clock click -milliseconds]
    if { $server_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}
}

```

仮想サーバへの iRule の追加

手順

- 1 F5 コンソールで、[メイン] - [仮想サーバ] - [仮想サーバリスト] の順にクリックします。
[仮想サーバリスト] 画面が表示されます。
- 2 iRule を追加するサーバを選択します。
- 3 [リソース] タブをクリックし、iRule セクションで [管理] をクリックします。
- 4 作成済みの TCP iRule および UDP iRule を選択して、[使用可能] ボックスから [有効] ボックスに移動します。
- 5 [終了] をクリックします。

ルート エントリの作成

コレクタ仮想マシンは、F5 からアクセスできる必要があります。コレクタ仮想マシンが F5 からアクセスできない場合は、コレクタのルート エントリを作成する必要があります。

コレクタ仮想マシンが F5 からアクセスできるかどうかを確認するには、コマンドライン インターフェイス (CLI) から ping <collector-ip> -I <virtual interface> コマンドを実行する必要があります。コレクタが F5 からアクセスできない場合は、コレクタのルート エントリを作成する必要があります。

次に例を示します。

```
admin@(localhost) (cfg-sync Standalone) (Active) (/Common) (tmos)# ping 10.153.191.116 -I VLAN301
PING 10.153.191.116 (10.153.191.116) from 10.115.30.50 VLAN301: 56(84) bytes of data.
From 10.115.30.50 icmp_seq=1 Destination Host Unreachable
From 10.115.30.50 icmp_seq=2 Destination Host Unreachable
```

手順

- 1 F5 コンソールで、[メイン] - [ネットワーク] - [ルート] - [追加] の順にクリックします。
[新しいルート] 画面が表示されます。
- 2 [プロパティ] セクションで、F5 から vRealize Network Insight コレクタに仮想サーバを介してフロー レコードを送信するためのルート エントリを設定します。

Kubernetes と VMware PKS のスコ ーピングおよびフロー情報

11

コンテナ エンティティのスコーピングを実行して、vRealize Network Insight でフロー情報を表示できます。

VMware PKS および Kubernetes のフロー情報

vRealize Network Insight は、Kubernetes エンティティに関する次のフロー タイプをサポートしています。

- 仮想マシンから Kubernetes ポッド
- Kubernetes ポッドからポッドへ
- 宛先が Kubernetes ポッド
- 送信元が Kubernetes ポッド

これらのフロー タイプを使用して、特定の Kubernetes エンティティを検索できます。

たとえば、`flows where flow type = x` で、`x` にいずれかのフロー タイプを指定します。

vRealize Network Insight は、コンテナの送信元と宛先の詳細、およびそのエンティティの詳細を含む、すべてのエンティティのメトリック、時系列、関係などのフロー情報を提供できます。

また、[フロー分析] ダッシュボードで Kubernetes クラスタ、名前空間、サービス、およびノード別に上位エンティティを表示できます。

Kubernetes エンティティの計画とマイクロセグメンテーション

[セキュリティのプラン] 画面で、スコープおよびマイクロセグメントとして Kubernetes クラスタ、Kubernetes サービス、Kubernetes 名前空間、または Kubernetes ノードを選択すると、特定の Kubernetes エンティティタイプについて計画できます。また、アプリケーションのデータを計画または分析し、Kubernetes エンティティに基づいてグループ分けを定義して、アプリケーションのフロー情報を表示することもできます。

さらに、[セキュリティのプラン] 画面では、Kubernetes エンティティに関連する推奨ファイアウォール ルールをマイクロセグメントから YAML 形式でエクスポートすることもできます。

注： アプリケーション スコープに仮想マシンまたは仮想マシン メンバーが含まれている場合は、YAML 形式でアプリケーション スコープをエクスポートすることはできません。アプリケーションにコンテナ エンティティのみが含まれている場合は、YAML 形式へのエクスポートを使用できます。

エンティティの詳細の表示

12

エンティティ ページは、データセンター内のエンティティに関する情報を包括的に示します。データセンター内のエンティティ間の関係を示す詳細なトポロジから、特定のエンティティに関する詳細なメトリックに至るまで、さまざまな情報を提供します。

各エンティティ画面は複数のウィジェットで構成され、各ウィジェットにはエンティティに関連する特定の情報が表示されます。リアルタイム情報と履歴情報が両方とも表示されるほか、エンティティに関するあらゆるメトリックとプロパティのリストが提供されます。

エンティティに関する詳細情報を表示するには、画面の右上隅で [プロファイル] - [ヘルプ] の順にクリックします。

タイムライン

タイムラインでは、次の情報が提供されます。

- 過去の特定時点でのデータセンターの状態。
- 選択した時間範囲について検出されたイベントの概観図。

表示するタイムラインの時間範囲を選択します。

特定のタイムラインを表示するには、[時間範囲] オプションを使用して時間範囲を選択します。

プロパティ ウィジェット

プロパティ ウィジェットには、重要な属性が 2 列形式で表示されます。一部のプロパティ ピンには、さらに単一の属性値のみが表示される場合もあります。プロパティ ピンの一例は、[仮想マシンのプロパティ] ピンです。[仮想マシンのプロパティ] ピンには、オペレーティング システム、IP アドレス、デフォルト ゲートウェイ、論理スイッチ、CPU、メモリ、電源状態などの仮想マシンのプロパティが表示されます。

この章には、次のトピックが含まれています。

- [vRealize Network Insight システム \(NI システム\) の詳細の表示](#)
- [プラットフォーム仮想マシンの詳細の表示](#)
- [コレクタ仮想マシンの詳細の表示](#)
- [VMware vCenter データ ソースの詳細の表示](#)
- [PCI コンプライアンスの詳細の表示](#)
- [Kubernetes の詳細の表示](#)

- ロード バランサの詳細の表示
- 仮想マシンの詳細の表示
- Edge デバイスの詳細の表示
- NSX Manager の詳細の表示
- [VMware NSX-T Manager] の詳細の表示
- [NSX-T 管理ノード] 詳細の表示
- NSX-T トランスポートの詳細の表示
- 仮想サーバの詳細の表示
- プール メンバーの詳細の表示
- Microsoft Azure の詳細の表示
- VeloCloud Enterprise の詳細の表示
- SD-WAN および Edge SD-WAN アプリケーションの詳細の表示
- [SD-WAN 評価] の詳細の表示
- [VeloCloud リンク アプリケーション] 詳細の表示
- [VeloCloud ビジネス ポリシー] の詳細の表示
- VMC SDDC の詳細の表示
- [Arista ハードウェア ゲートウェイ] および [Arista ハードウェア ゲートウェイのバインド] の詳細の表示
- [Cisco Nexus デバイス] の詳細の表示
- フロー情報の詳細の表示
- マイクロセグメンテーションの詳細の表示
- アプリケーションの詳細の表示
- 分析：外れ値検出
- 分析：静的および動的しきい値

vRealize Network Insight システム（NI システム）の詳細の表示

vRealize Network Insight システム（NI システム）画面には、システムに関連するすべての情報のスナップショットが表示されます。[vRealize Network Insight システム] 画面にアクセスするには、次の手順を実行します。

- [インストールとサポート] 画面で、[概要] の横にある [詳細の表示] をクリックします。[NI システム] 画面が表示されます。
- [vRealize Network Insight システム] 画面を表示するには、検索クエリに `NI-System` を指定します。

[NI システム] 画面は、次の 3 つのセクションに分かれています。

- 概要：このセクションには、キー プロパティ、データ ソース、未解決の問題、およびシステムに関連するすべての変更と問題についての情報が示されます。各データ ソースをクリックして、詳細を表示します。
- イベント：このセクションには、システム、データ ソース、プラットフォーム、およびコレクタのすべての問題と変更が一覧表示されます。
- プラットフォームとコレクタ：このセクションには、システムに関連付けられているすべてのプラットフォームとコレクタが一覧表示されます。任意のプラットフォームまたはコレクタの詳細を表示するには、そのプラットフォームまたはコレクタをクリックします。

プラットフォーム仮想マシンの詳細の表示

[プラットフォーム仮想マシン] 画面には、特定のプラットフォーム ノードのプロパティ、変更、および問題のスナップショットが表示されます。

[プラットフォーム仮想マシン] 画面には、次の情報が表示されます。

- IP アドレス、CPU コア、メモリ、前回のアップグレード時刻、およびバージョンなど、選択したプラットフォーム ノードに関する重要な情報。
- プラットフォームに関連する未解決の問題。
- 選択したプラットフォーム ノードに関連するイベントのリスト。
- CPU 使用率、メモリ使用量、データ ディスク使用量などのメトリックのグラフィカルな表示。

コレクタ仮想マシンの詳細の表示

[コレクタ仮想マシン] 画面には、特定のコレクタ ノードのプロパティ、変更、および問題のスナップショットが表示されます。

[コレクタ仮想マシン] 画面には、次の情報が表示されます。

- IP アドレス、CPU コア、メモリ、前回のアップグレード時刻、およびバージョンなど、選択したプラットフォーム ノードに関する重要な情報。
- コレクタに関連する未解決の問題の数と問題の詳細。
- データ ソースに関連する未解決の問題の数と問題の詳細。
- 過去 7 日間にデータ ソースで発生した変更のリスト。
- データ ソースの詳細と、コレクタで使用可能な NetFlow レポート。各 NetFlow レポートに、フローの数が表示されます。データ ソースの場合は、フローの数と検出された仮想マシンの数が表示されます。
- CPU 使用率、メモリ使用量、データ ディスク使用量などのメトリックのグラフィカルな表示。

VMware vCenter データ ソースの詳細の表示

[VMware vCenter データ ソース] 画面には、特定のデータ ソースのプロパティ、変更、および問題のスナップショットが表示されます。

[VMware vCenter データ ソース] 画面には、以下の情報が表示されます。

- 選択されている VMware vCenter データ ソースに関する重要な情報 (IP アドレス/FQDN、コレクタ名、有効、検出された仮想マシンの数、IPFIX の有効ステータスなど)。
- データ ソースに関連するすべての未解決の問題。
- 過去 7 日間に特定のデータ ソースで発生したすべての変更と問題。

PCI コンプライアンスの詳細の表示

[PCI コンプライアンス] 画面は、Enterprise ライセンス ユーザーのみ使用できます。

[PCI コンプライアンス] へのアクセス

- 1 ホームページの左側にあるナビゲーション パネルで、[セキュリティ] > [PCI コンプライアンス] の順に選択します。
- 2 [PCI コンプライアンス] ウィンドウが表示されます。必要な範囲、対応するエンティティ、およびデータを必要とする期間を選択します。[評価] をクリックします。
- 3 [PCI コンプライアンス] 画面が表示されます。

[PCI コンプライアンス] 画面の詳細

[PCI コンプライアンス] 画面は、NSX 環境専用の PCI 要件に対する準拠度を評価するのに役立ちます。これらの要件は、ダッシュボードの最初のピンの下に記載されています。それ以外のダッシュボード内のピンには、要件を評価するための次のようなデータが表示されます。

- ネットワーク フロー図：データ フロー、ファイアウォール、接続、およびネットワークに関連付けられているその他の詳細情報が表示されます。
- フロー：ネットワーク フロー図に表示されるフローが一覧表示されます。
- ターゲット ポートに基づくクリア テキスト プロトコル フロー：特定のポートを流れるトラフィックはクリア テキストです。このピンには、特定のターゲット ポートに基づくクリア テキスト プロトコル フローが表示されます。
- 範囲内の仮想マシン：クエリで選択した範囲内の仮想マシンが表示されます。このピンには、送信ルール、受信ルール、およびその範囲内の仮想マシンのセキュリティ グループが表示されます。
- 仮想マシンのセキュリティ グループ：仮想マシンのセキュリティ グループが一覧表示されます。
- セキュリティ グループ別の仮想マシン数：このピンのカウントをクリックすると、セキュリティ グループ内の仮想マシンのリストが表示されます。
- セキュリティ タグ別の仮想マシン数：このピンのカウントをクリックすると、セキュリティ タグの付いた仮想マシンのリストが表示されます。

- 内部トラフィックに適用されるファイアウォール ルール: 選択した範囲にある仮想マシン間のトラフィックについて、ファイアウォール ルールを表示できます。
- 受信トラフィックに適用されるファイアウォール ルール: 選択範囲外の仮想マシンから選択範囲内の仮想マシンへのトラフィックに関するファイアウォール ルールを表示できます。
- 送信トラフィックに適用されるファイアウォール ルール: 選択範囲内の仮想マシンから選択範囲外の仮想マシンへのトラフィックに関するファイアウォール ルールを表示できます。
- セキュリティ タグ メンバーシップの変更: セキュリティ タグのメンバーシップに関する変更がこのピンに表示されます。
- セキュリティ グループ メンバーシップの変更: セキュリティ グループのメンバーシップに関する変更がこのピンに表示されます。
- ファイアウォール ルールの変更: ファイアウォール ルールに関連する変更がこのピンに表示されます。

注: ネストされたセキュリティ グループが NSX にある場合、PCI コンプライアンスの範囲はセキュリティ グループ以外であることが必要です。

PDF としてエクスポート

vRealize Network Insight を使用すると、[PCI コンプライアンス] ダッシュボードで情報を作成し、それらを PDF レポートとしてエクスポートできます。

手順

- 1 [PCI コンプライアンス] ダッシュボードで、画面の右上にある [PDF としてエクスポート] をクリックします。[PDF にエクスポート] ウィンドウが表示されます。
- 2 [PDF にエクスポート] ウィンドウには、[PCI コンプライアンス] ダッシュボードで使用可能なすべてのウィジェットとそれぞれのプロパティが一覧表示されます。エクスポートするウィジェットとプロパティを選択します。

注:

- 1 つ以上のプロパティを選択する必要があります。
- 選択可能なプロパティの最大数は 20 個です。
- リスト表示でエクスポート可能な最大エントリ数は 100 個です。
- 一部のウィジェットでは、プロパティを選択できません。この場合はエントリ数のみを指定します。

- 3 PDF レポートのタイトルを入力します。

注:

- タイトルに使用できる最大文字数は 200 文字です。
- レポートで生成できる最大ページ数は 50 ページです。

- 4 [プレビュー] をクリックします。完全なレポートのプレビューが表示されます。

5 [PDF にエクスポート] をクリックします。

Kubernetes の詳細の表示

Kubernetes ダッシュボードを使用して、vRealize Network Insight の Kubernetes 環境または VMware PKS 環境の概要をすばやく把握できます。

次の詳細を確認できます。

- フローに基づく上位の通信中クラスタおよび名前空間
- 名前空間、ポッド、サービスおよびノードの数など、Kubernetes クラスタ エンティティの概要
- vRealize Network Insight に追加された Kubernetes クラスタ
- ポッドで実行されているコンテナ イメージおよび各コンテナ イメージのポッド数のリスト
- 検出された新しいポッド、その数、名前空間およびクラスタの詳細のリスト

また、ダッシュボードでさまざまな Kubernetes エンティティの数をクリックしてリストを表示し、その特定のエンティティの詳細に移動することもできます。

表 12-1. Kubernetes エンティティ ダッシュボード

ダッシュボード	説明
クラスタ ダッシュボード	<p>以下のような、クラスタ レベルでの環境の詳細を取得します。</p> <ul style="list-style-type: none"> ■ 環境内の名前空間、サービス、ポッドおよびノードの数を含むクラスタの概要。 ■ フローに基づく上位の名前空間のリスト。 ■ 名前空間どうしの相互作用。
名前空間ダッシュボード	<p>以下のような、クラスタの名前空間に関する詳細を取得します。</p> <ul style="list-style-type: none"> ■ 特定の名前空間にあるポッド、サービスおよびノードの数を含む名前空間の概要。 ■ フローに基づく上位の通信中名前空間のリスト。 ■ 名前空間内のサービス相互作用。 ■ ネットワーク トラフィック (パケット数およびバイト数)
サービス ダッシュボード	<p>以下のような、Kubernetes サービスの詳細が表示されます。</p> <ul style="list-style-type: none"> ■ 次の数を含むサービスの概要： <ul style="list-style-type: none"> ■ 24 時間以内に開いていたイベント ■ 24 時間の送受信フロー ■ ポッド ■ サービスが展開されたノード ■ kubernetes コンポーネントと NSX-T の間の接続 ■ 指定された期間内にアクティブだったノードとポッドの数 ■ 名前空間内でのサービスのやりとり ■ ネットワーク トラフィック (パケット数およびバイト数)

表 12-1. Kubernetes エンティティ ダッシュボード (続き)

ダッシュボード	説明
ポッド ダッシュボード	<p>以下のような詳細が表示されます。</p> <ul style="list-style-type: none"> ■ ポッドが属しているクラスター、名前空間およびノード ■ パケットとバイトに基づくポッド間のネットワーク トラフィック
ノード ダッシュボード	<p>以下のような詳細が表示されます。</p> <ul style="list-style-type: none"> ■ 名前空間の詳細のリスト ■ サービスのリスト ■ コンテナ ポッドのリスト ■ パケットとバイトに基づくノード間のネットワーク トラフィック

注：

- vRealize Network Insight は、10 分ごとに VMware PKS から Kubernetes クラスターの詳細を収集します。
- vRealize Network Insight は、4 時間ごとに Kubernetes クラスターからすべてのオブジェクト（名前空間、ノード、ポッド、サービス）を収集します。ただし、Kubernetes オブジェクトに変更があった場合は、vRealize Network Insight は Watch API を実行し、変更をただちに更新します。
- VMware PKS では、Kubernetes プライマリ ノードに関する詳細は提供されません。
- vRealize Network Insight では、正常に作成された状態にあるクラスターについてのみ詳細が提供されます。

よくあるイベントまたはエラー メッセージ

- `Data Source not reachable` - プロキシ仮想マシンから Ping で VMware PKS の IP アドレスまたは FQDN を送信し、VMware PKS に到達可能であることを確認します。
- `Kubernetes Cluster API Servers not reachable` - すべての Kubernetes クラスター API サーバがプロキシ仮想マシンからアクセス可能であることを確認します。

ロード バランサの詳細の表示

[ロード バランサ] 画面には、ロード バランサに作成された仮想サーバおよびプールに関する情報の概要が表示されます。

表示される情報は次のとおりです。

- ロード バランサ上の仮想サーバのリストと仮想サーバの問題
- ロード バランサ上のプールのリストとプールに関連する問題
- ロード バランサに関連付けられているイベント
- さまざまな宛先 IP アドレスでのフロー、数およびフローのネットワーク トラフィックのリスト。

注： NSX-V ロード バランサについては、フロー情報がキャプチャされません。

- ベンダー、タイプ、シリアル番号、仮想サーバ、プールなどの情報を提供するロード バランサのプロパティ。

仮想マシンの詳細の表示

[仮想マシン] 画面を使用して、vRealize Network Insight で使用可能な仮想マシンの概要について詳しい情報を取得できます。

[仮想マシン] 画面には、次のセクションが表示されます。

セクション	詳細
[概要]	<p>表示される情報は次のとおりです。</p> <ul style="list-style-type: none"> ■ 仮想マシンの詳細。 ■ トポロジの情報。 ■ さまざまな構成パラメータ。 ■ セキュリティ関連のパラメータ。 ■ 仮想マシンからインターネットへのパス。
[ネイバー]	<p>表示される情報は次のとおりです。</p> <ul style="list-style-type: none"> ■ ネイバー仮想マシンと比較したさまざまなメトリック プロパティのグラフィカル表示 ■ 同じホストに属している仮想マシンのリスト。
[イベント]	<p>選択した仮想マシンに関連するイベントのリストが表示されます。</p>
[フロー]	<p>選択した仮想マシンのうち、ファイアウォール アクションが許可または拒否されているものから送信されたフロー、またはそのような仮想マシンに到達しようとしているフローのリストが表示されます。</p>
[メトリック]	<p>表示される情報は次のとおりです。</p> <ul style="list-style-type: none"> ■ 選択した仮想マシンに関連するメトリック情報。 ■ ToR へのパス内のポートのネットワーク使用量に関する情報。 ■ すべてのメトリック プロパティに関する情報。 ■ 入力 - 出力メトリック情報。 ■ 仮想ディスク容量。 ■ データストアのパフォーマンス。 <p>注： 仮想マシンが vSAN データストア上でホストされている場合、仮想マシンのデータストア メトリックは表示できません。</p> <ul style="list-style-type: none"> ■ 仮想インフラストラクチャの遅延の詳細。 <p>注： 仮想インフラストラクチャの遅延を確認するには、ESXi ホストからの遅延データを受信できるように、コレクタでポート 1991 が開いている必要があります。</p>

Edge デバイスの詳細の表示

[VMware Edge デバイス] 画面を使用して、vRealize Network Insight で使用可能な VMware Edge デバイスの概要を取得することができます。

この画面にアクセスするには、**Edge デバイス**を検索し、検索結果リストで、表示するエンティティをクリックします。

概要

[VMware Edge デバイス] 画面には、以下が表示されます。

セクション	詳細
[概要]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ イベント チャート、バイト、パケット、フロー、セッション番号を含む、Edge デバイスの概要。 ■ NSX Edge のプロパティ、NSX Edge サービス、および NSX Edge アプライアンス仮想マシンのリスト。 ■ トポロジの詳細。
[イベント]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ さまざまなイベントの詳細のリスト。
[フロー]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ NSX Edge を通過する合計バイト数、NSX Edge を通過する合計パケット数、合計フロー数、および NSX Edge を通過する合計セッション数など、さまざまなフロー分析。
[メトリック]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ NSX Edge アプライアンス仮想マシンの CPU 使用率、NSX Edge アプライアンス仮想マシンのメモリ使用率、NSX Edge アプライアンス仮想マシンのネットワーク使用率、NSX Edge の vNIC ごとのネットワーク使用率など、さまざまなメトリック。

考慮事項

以下の条件下では、[VMware Edge デバイス] 画面にまれに誤ったフロー情報が表示されることがあります。

- 仮想マシンの IP アドレスが vRealize Network Insight で認識されていない。
- 仮想マシンでデフォルト ゲートウェイが正しく設定されていない。
- 仮想マシンからの North-South フローで Edge ホップ数が 2 つを超えている。
- Edge が ECMP (Equal Cost Multi Path ルーティング) に属している。
- Edge がユニバーサル分散論理ルーターに接続されている。

NSX Manager の詳細の表示

[NSX Manager] 画面を使用して、vRealize Network Insight で使用可能な NSX Manager の概要について詳細を取得できます。

[NSX Manager] 画面へのアクセス方法

この画面にアクセスするには、NSX Manager where SDDC Type = 'VMC' で検索し、検索結果リストで、表示する [NSX Manager] 画面をクリックします。

概要

[NSX Manager] 画面には、次のセクションが表示されます。

表 12-2.

セクション	詳細
[概要]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ NSX ポリシー エンティティの概要の詳細。 ■ 直近 24 時間に変更されたエンティティ。 ■ 上位のルール別フロー。 ■ ルーターのリスト。 <p>注： [NSX ポリシー エンティティの概要] ウィジェットと [直近 24 時間のエンティティ数] ウィジェットに表示されるエンティティ数は異なることがあります。直近 24 時間に検出された一部のエンティティが削除された場合、[直近 24 時間以内のエンティティ数] に表示されるエンティティ数が、[NSX ポリシー エンティティの概要] ウィジェットに表示されるエンティティの数よりも大きくなる場合があります。</p>
[上位エンティティ]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ 環境内の主要エンティティ。
[ネットワーク トラフィックおよびイベント]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ ネットワーク トラフィックとアラートの概要。 ■ イベントのリスト。

[VMware NSX-T Manager] の詳細の表示

[VMware NSX-T Manager] 画面を使用して、vRealize Network Insight で使用可能な VMware NSX-T Manager の概要を取得できます。

この画面にアクセスするには、**NSX-T Manager** を検索し、検索結果リストで、表示するエンティティをクリックします。

概要

NSX Manager 画面には、次の情報が表示されます。

セクション	詳細
[概要]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ イベント チャート、ファイアウォール ルールの数、IPSET、トランスポート ゾーン、アプリケーション、保護されていないフロー、および直近 24 時間のフロー ボリュームを含む、NSX-T Manager のサマリ。 ■ プロパティ、ヒット数別のファイアウォール ルール、ルールごとの上位フロー、およびコンピュート マネージャのリスト。 ■ トポロジの詳細。トポロジでは、エンティティのコンテキストビューが提供され、エンティティに関連付けられたイベントも表示されます。
[イベント]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ さまざまなイベントおよび分析しきい値イベントのリスト。

セクション	詳細
[フロー]	以下が表示されます。 <ul style="list-style-type: none"> ■ さまざまなフロー分析。
[メトリック]	以下が表示されます。 <ul style="list-style-type: none"> ■ NSX-T 管理ノードの健全性の詳細。 <p>注： NSX-T 管理ノードの健全性の詳細は、NSX-T のバージョン 2.4.0 以降でのみ使用できます。</p>

[NSX-T 管理ノード] 詳細の表示

[NSX-T 管理ノード] 画面を使用して、vRealize Network Insight で使用可能な VMware NSX-T 管理ノードの詳細についての概要を取得できます。

この画面にアクセスするには、**NSX-T Management Node** を検索し、検索結果リストで、表示するエンティティをクリックします。

概要

この画面には、以下の項目が表示されます。

セクション	詳細
[概要]	以下が表示されます。 <ul style="list-style-type: none"> ■ プロパティの詳細、システム メトリック、サービス ステータスなど、NSX-T 管理ノードのサマリ。
[イベント]	以下が表示されます。 <ul style="list-style-type: none"> ■ さまざまなイベントのリスト。
[インターフェイスの統計情報]	以下が表示されます。 <ul style="list-style-type: none"> ■ 受信パケット、送信パケット、ドロップされた受信パケット、ドロップされた送信パケットなど、さまざまなインターフェイス統計情報。
[システムの統計情報]	以下が表示されます。 <ul style="list-style-type: none"> ■ システム負荷、システム使用量、ファイル システム使用量など、さまざまなシステム統計情報。

NSX-T トランスポートの詳細の表示

[NSX-T トランスポート ノード] 画面を使用して、vRealize Network Insight で使用可能なトランスポート ノードの詳細についての概要を取得できます。vRealize Network Insight では、ホスト ノードの詳細と Edge ノードの詳細を表示できます。

ノード タイプが「ホスト」の場合の [NSX-T トランスポート ノード] 画面

この画面にアクセスするには、**NSX-T Transport Node where Node Type = 'HostNode'** を入力して検索し、検索結果リストで、表示するエンティティをクリックします。

概要

この画面には、以下の項目が表示されます。

セクション	詳細
[概要]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ イベント チャート、受信トラフィック、送信トラフィック、内部トラフィック、ネットワーク インターフェイスの数、仮想マシンの合計数など、ホスト トランスポート ノードのサマリ。 ■ プロパティの詳細、トランスポート ノードのステータス、直近 24 時間の物理 NIC の統計情報、直近 24 時間の TEP の統計情報、および直近 24 時間のシステム メトリック。 <p>注： システム メトリックは NSX-T バージョン 2.4.0 以降でのみ使用可能です。</p>
[イベント]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ ささまざまなイベントのリスト。
[遅延]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ TEP 間の遅延の詳細。
[インターフェイスの統計情報]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ 受信パケット、送信パケット、ドロップされた受信パケット、ドロップされた送信パケットなど、さまざまなインターフェイス統計情報。
[システムの統計情報]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ システム負荷、システム使用量、ファイル システム使用量など、さまざまなシステム統計情報。 <p>注： [システムの統計情報] 画面は、NSX-T バージョン 2.4.0 以降でのみ使用可能です。</p>
[フロー]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ フロー別の上位仮想マシン（直近 24 時間） およびフロー別の上位ルール（直近 24 時間）。

ノード タイプが「Edge」の場合の [NSX-T トランスポート ノード] 画面

この画面にアクセスするには、**NSX-T Transport Node where Node Type = 'EdgeNode'** を入力して検索し、検索結果リストで、表示するエンティティをクリックします。

概要

この画面には、以下の項目が表示されます。

セクション	詳細
[概要]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ イベント チャート、ネットワーク インターフェイスの数、tier-0 サービス ルーター、tier-1 サービス ルーター、ルーティングなど、Edge トランスポート ノードのサマリ。 ■ プロパティの詳細、トランスポート ノードのステータス、直近 24 時間のアップリンクの統計情報、直近 24 時間の TEP の統計情報、および直近 24 時間のシステム メトリック。
[イベント]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ さまざまなイベントのリスト。
[NAT 統計情報]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ NAT ルールの統計情報、合計バイト数で上位の NAT ルール、合計パケット数で上位 NAT ルール、セッション数で上位の NAT ルールなど、さまざまな NAT の統計情報。
[インターフェイスの統計情報]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ 受信パケット、送信パケット、ドロップされた受信パケット、ドロップされた送信パケットなど、さまざまなインターフェイス統計情報。
[システムの統計情報]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ システム負荷、システム使用量、ファイル システム使用量など、さまざまなシステム統計情報。

仮想サーバの詳細の表示

[仮想サーバ] 画面には、仮想サーバのメトリックと、問題および変更イベントが表示されます。

表示される情報は次のとおりです。

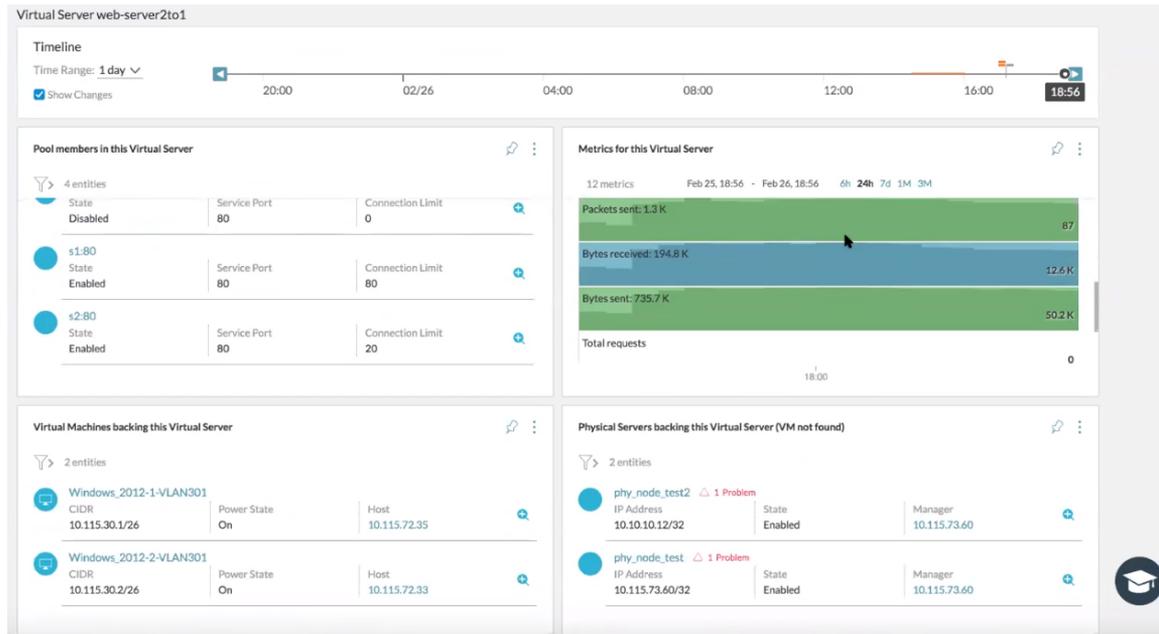
- 仮想サーバのすべてのプール メンバーのリストとその詳細、および問題のアラート
- 仮想マシンのリスト
- 物理サーバのリスト
- 仮想サーバに関連付けられている問題イベントのリスト
- 次のような、仮想サーバに関連するメトリックのリスト。
 - 接続（数、期間）
 - ネットワーク メトリック（受信済みまたは送信済みのパケットおよびバイト数）
 - CPU 使用率

注： サポートされている NSX-V ロード バランサのメトリックのリストについては、[サポートされている NSX-V メトリック](#)を参照してください。

- 仮想サーバで使用されるプール メンバーの上位フロー

注： NSX-V ロード バランサについては、フロー情報がキャプチャされません。

- ロード バランサの IP アドレス、ネットワーク トラフィック、サービス ポートに関する情報を提供する仮想サーバのプロパティ。



ロード バランサに関連付けられているトポロジ パスを表示するには、`client VM name to Virtual server IP`、というクエリを使用できます。異なるサービス ポートに複数の仮想サーバがある場合、[宛先仮想マシンを選択] セクションにそのリストが表示されます。リストからサーバを選択し、[パスを表示] をクリックすると、仮想マシンから仮想サーバへのパスが表示されます。

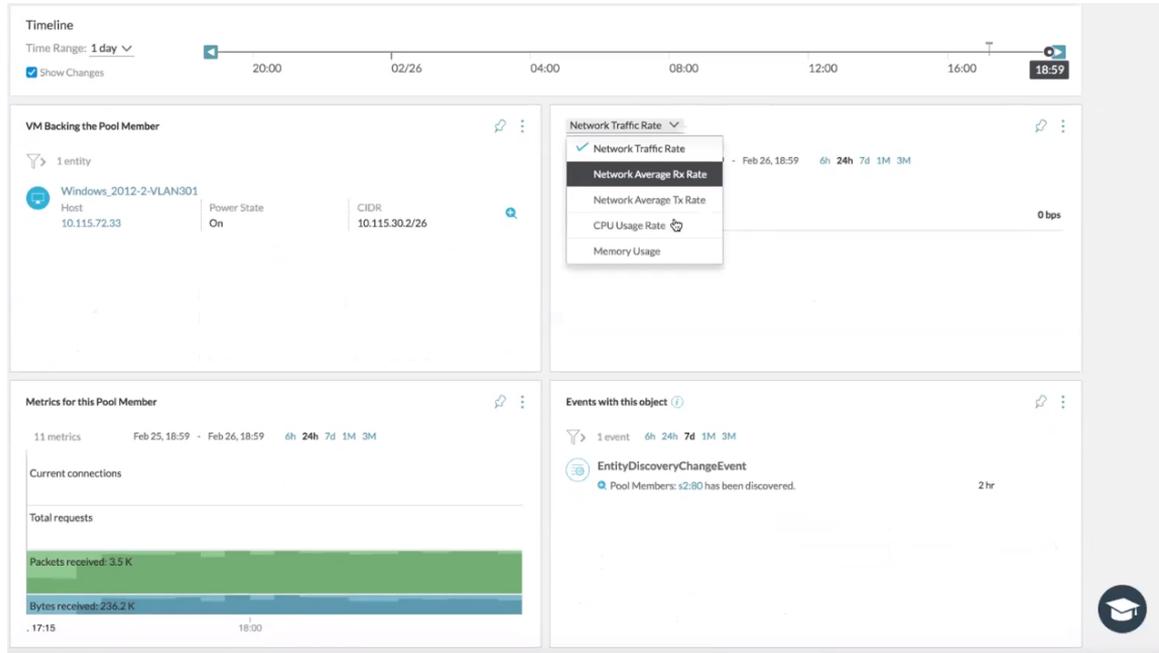
仮想マシンのパス トポロジで仮想サーバをクリックすると、[仮想サーバ] ウィンドウに一連の仮想マシンが表示されます。[パスの表示] をクリックすると、仮想サーバから選択した仮想マシンへのパスが表示されます。

プール メンバーの詳細の表示

[プール メンバー] 画面には、プール メンバー、メトリック、およびプール メンバーに関連付けられているイベントに関する情報が表示されます。

以下が表示されます。

- 仮想マシンのリストと仮想マシンに関する追加の詳細
- プール メンバーのメトリックと仮想マシンのメトリックを比較できる情報。たとえば、メモリと CPU の使用率、ネットワーク トラフィックなど。
- 次のような、プール メンバーに関連するメトリックのリスト。
 - 接続（数、期間、存続時間）
 - ネットワーク メトリック（受信済みまたは送信済みのパケットおよびバイト数）
 - CPU 使用率
- ロード バランサ、ノード、状態、サービス ポートに関する情報を提供するプール メンバーのプロパティ。



Microsoft Azure の詳細の表示

[Microsoft Azure] 画面を使用して vRealize Network Insight で Azure 環境の概要を確認することができます。

アクセス方法

この画面にアクセスするには、**Azure** を検索します。または、[ホーム] 画面の [運用とトラブルシューティング] セクションで、[Microsoft Azure] アイコンをクリックします。

概要

この画面には、以下の項目が表示されます。

- サブスクリプションのリスト
- 仮想マシンのリスト
- ネットワーク インターフェイス、仮想ネットワーク、サブネット、ルート テーブル、およびルートのリスト
- ネットワーク セキュリティ グループ、アプリケーション セキュリティ グループ、および NSG ルールのリスト。

また、この画面のエンティティをクリックして、特定のエンティティに関する詳細を表示することもできます。

[Microsoft Azure] 画面では、以下の Azure エンティティの詳細について確認できます。

表 12-3. Azure エンティティの詳細

エンティティ名	説明
[Azure アプリケーション セキュリティ グループ]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、関連付けられた仮想マシン、直近 24 時間で関連付けられた仮想マシンのリスト。 ■ 受信 NSG ルールと送信 NSG ルールのリスト。 ■ 許可されたフロー、拒否されたフロー、直近 24 時間のフローのリスト。
[Azure データ ソース]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、メトリックのリスト。
[Azure NSG ルール]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、メトリックのリスト。
[Azure ネットワーク インターフェイス]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、メトリックのリスト。
[Azure ネットワーク セキュリティ グループ]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、NIC、サブネットのリスト。 ■ 送信ルールと受信ルールのリスト。 ■ 許可されたフロー、拒否されたフロー、直近 24 時間のフローのリスト。
[Azure ルート]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、メトリックのリスト。
[Azure ルート テーブル]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、メトリックのリスト。
[Azure サブネット]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、仮想マシン、NIC、カスタム ルートのリスト。 ■ NSG ルールのリスト。
[Azure サブスクリプション]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティとイベントのリスト。 ■ 仮想マシンのリスト。 ■ NIC、仮想ネットワーク、およびルート テーブルのリスト。 ■ ネットワーク セキュリティ グループ、アプリケーション セキュリティ グループ、および NSG ルールのリスト。
[Azure 仮想マシン]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、NIC、関連付けられたアプリケーション セキュリティ グループ (ASG) のリスト。 ■ 受信 NSG ルールと送信 NSG ルールのリスト。 ■ 許可されたフローと拒否されたフローのリスト。
[Azure 仮想ネットワーク]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ プロパティ、イベント、仮想マシン、直近の 24 時間に作成された仮想マシン、関連付けられている ASG、直近の 24 時間で関連付けられた ASG、サブネット、ルート テーブルのリスト。 ■ 許可されたフロー、拒否されたフロー、直近 24 時間のフローのリスト。

VeloCloud Enterprise の詳細の表示

vRealize Network Insight の [VeloCloud エンタープライズ] 画面で VMware SD-WAN 展開環境の概要を確認することができます。

[VeloCloud エンタープライズ] 画面にアクセスします。

この画面にアクセスするには、**VeloCloud エンタープライズ** を検索します。または、[ホーム] 画面の [運用とトラブルシューティング] セクションで、[VeloCloud Enterprise] アイコンをクリックします。

概要

この画面には、次のセクションが表示されます。

セクション	詳細
[概要]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ イベント チャート、Edge の数、ハブ、ゲートウェイ、リンク、Edge から Edge へのフロー、インターネット フロー、アプリケーションなどの、VMware SD-WAN 展開環境のサマリ。これらのエンティティの健全性状態も表示されます。 ■ VMware SD-WAN 展開環境のマップ ビューと、Edge 上のアプリケーションのリスト。 <p>注: マップ ビューを取得するには、vRealize Network Insight に Google マップ API キーを追加する必要があります。詳細については、『Google マップ API キーの追加』を参照してください。Google マップ API キーを追加しない場合は、Edge のリスト ビューのみが表示されます。</p>
[イベント]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ さまざまなイベントのリスト。
[分析]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ アプリケーション、Edge、Edge ペア、フロー バス、トラフィック タイプ、リンク ポリシー、ルート タイプ別のトラフィック分布など、さまざまなトラフィック分布のリスト。
[可用性]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ 利用可能な Edge/ハブと利用不可の Edge/ハブのリスト。
[メトリック]	<p>以下が表示されます。</p> <ul style="list-style-type: none"> ■ Edge トラフィック、Edge パケット、Edge QoE、アプリケーショントラフィック、アプリケーションパケット、リンクパケット、リンク遅延、リンクスループットおよびリンク QoE に基づくさまざまなメトリック。プラス (+) アイコンをクリックして、詳細が表示できます。

また、この画面のエンティティをクリックして、特定のエンティティに関する詳細を表示することもできます。

[VeloCloud Enterprise] 画面では、以下の VMware SD-WAN エンティティの詳細について確認できます。

表 12-4. VMware SD-WAN エンティティの詳細

エンティティ名	説明
[VeloCloud クラスタ]	以下が表示されます。 ■ プロパティのリスト。
[VeloCloud データ ソース]	以下が表示されます。 ■ プロパティ、未解決の問題、直近 7 日間に発生した変更および問題のリスト。
[VeloCloud Edge]	以下が表示されます。 ■ VMware SD-WAN Edge の詳細。詳細については、 VeloCloud Edge の詳細の表示 を参照してください。
[VeloCloud ゲートウェイ]	以下が表示されます。 ■ プロパティと Edge のリスト。
[VeloCloud レイヤー 2 ネットワーク]	以下が表示されます。 ■ プロパティとイベントのリスト。
[VeloCloud リンク]	以下が表示されます。 ■ プロパティとイベントのリスト。 ■ QoE、パケット、アップタイム、遅延、スループットに関するメトリック。
[VeloCloud プロファイル]	以下が表示されます。 ■ プロパティと Edge のリスト。
[VeloCloud セグメント]	以下が表示されます。 ■ プロパティのリスト。

VeloCloud Edge の詳細の表示

[VeloCloud Edge] 画面を使用して vRealize Network Insight で VMware SD-WAN Edge の概要を利用することができます。

この画面にアクセスするには、**VeloCloud Edge** を検索し、検索結果リストで、表示するエンティティをクリックします。

概要

この画面には、次のセクションが表示されます。

セクション	詳細
[概要]	以下が表示されます。 ■ VMware SD-WAN Edge のサマリ。イベントチャート、ポリシーチャート。アップタイムの詳細、アプリケーションの数、セグメント、リンク、レイヤー 2 ネットワーク、LAN インターフェイス、WAN インターフェイス、トンネルなど。 ■ VMware SD-WAN Edge トポロジ。 ■ Edge QoE とリンク QoE のリスト
[イベント]	以下が表示されます。 ■ さまざまなイベントのリスト。

セクション	詳細
[フロー]	以下が表示されます。 ■ フローのリスト。
[分析]	以下が表示されます。 ■ アプリケーションおよび優先順位別、フロー バス別、トラフィックタイプ別、リンク ポリシー別、ルート タイプ別のトラフィック分布など、さまざまなトラフィック分布のリスト。
[メトリック]	以下が表示されます。 ■ Edge トラフィック、Edge パケット、アプリケーション トラフィック、アプリケーション パケット、リンク パケット、リンク 遅延、リンク トラフィック、トンネル トラフィックに基づく、さまざまなメトリック。プラス (+) アイコンをクリックして、詳細が表示できます。

また、この画面のエンティティをクリックして、特定のエンティティに関する詳細を表示することもできます。

SD-WAN および Edge SD-WAN アプリケーションの詳細の表示

vRealize Network Insight の [SD-WAN アプリケーション] 画面と [Edge SD-WAN アプリケーション] 画面を使用して、SD-WAN アプリケーションと Edge SD-WAN アプリケーションの概要を確認できます。

概要

この画面には、次のセクションが表示されます。

表 12-5. [SD-WAN アプリケーション]

セクション	詳細
[概要]	以下が表示されます。 ■ Edge、リンク、イベント、フローのリスト。
[トラフィックの分布]	以下が表示されます。 ■ Edge 別のトラフィックやクライアント別のトラフィックなど、さまざまなトラフィック分布の詳細。
[メトリック]	以下が表示されます。 ■ Edge トラフィック、Edge パケット、リンク トラフィック、リンク パケットの詳細など、さまざまなメトリック。

また、この画面のエンティティをクリックして、特定のエンティティに関する詳細を表示することもできます。

[SD-WAN アプリケーション] 画面のほかに、[Edge SD-WAN アプリケーション] に関する次の詳細も表示されます。

- プロパティ、イベント、メトリックのリスト。

注： vRealize Network Insight は、VMware SD-WAN Edge ごとに最大 2 つのセグメントと、最大 20,000 のレイヤー 3 ドメインをサポートします。

[SD-WAN 評価] の詳細の表示

[SD-WAN 評価] 画面を表示して、WAN 展開の概要を確認できます。また、投資回収率 (ROI) 評価レポートを取得して、トラフィックの性質を理解し、SD-WAN 環境の推奨事項を確認することもできます。vRealize Network Insight

[SD-WAN 評価] 画面へのアクセス方法

この画面にアクセスするには、左側のナビゲーション ペインで [プランと評価] - [SD-WAN 評価] の順にクリックします。

概要

この画面には、SD-WAN 評価レポートのサマリ、出力方向と入力方向のトラフィック データ、出力方向と入力方向のトラフィックの上位のサービスが表示されます。

評価の範囲と期間を変更できます。評価の範囲と期間を変更するには、[範囲] と [期間] ドロップダウン メニューから、使用する範囲と期間を選択し、[分析] をクリックします。

また、SD-WAN 評価レポートを生成することもできます。詳細については、[評価レポートの生成](#)を参照してください。

評価レポートの生成

vRealize Network Insight では、SD-WAN 評価レポートを生成し、VMware SD-WAN が従来の WAN セットアップ経由で提供可能なコスト節約の見積もりを取得できます。さらに、SD-WAN 評価レポートでは、各サイトに対する SD-WAN Edge の推奨事項も提供されます。

手順

- 1 [SD-WAN 評価] 画面で、[レポートの生成] をクリックします。
[追加データ] ダイアログ ボックスが表示されます。
- 2 [組織名] テキスト ボックスに、レポートを生成する組織名を入力します。
- 3 [リージョン固有の入力] テーブルで、リージョン固有の入力を確認し、[レポートの生成] をクリックします。
リージョン固有の入力は、現在使用中の要件に応じて変更が可能です。[リセット] をクリックすると、リージョン固有の入力のデフォルト値を取得できます。

結果

[SD-WAN 評価] レポートが新しいタブで表示されます。

[VeloCloud リンク アプリケーション] 詳細の表示

[VeloCloud リンク アプリケーション] 画面を使用して、リンク上のアプリケーションの概要を取得できます。

この画面にアクセスするには、**SD-WAN Link Application** を検索し、検索結果リストで、表示するエンティティをクリックします。

概要

この画面には、キー プロパティのリスト、フロー トラフィックの詳細、およびフロー パケットの詳細が表示されます。

[VeloCloud ビジネス ポリシー] の詳細の表示

[VeloCloud ビジネス ポリシー] 画面を使用して、VeloCloud ビジネス ポリシーの概要を確認できます。

この画面にアクセスするには、**VeloCloud Business Policy** を検索し、検索結果リストで、表示するエンティティをクリックします。

概要

この画面には、定義：一致、定義：アクション、イベント、およびフローの詳細が表示されます。

注： 現在、vRealize Network Insight は以下をサポートしていません。

- 送信元/宛先が非 VeloCloud サイトである SD-WAN ビジネス ポリシー。
- 送信元/宛先がオブジェクト グループ (IP アドレス グループまたはポート グループ) である SD-WAN ビジネス ポリシー。

VMC SDDC の詳細の表示

[VMC SDDC] 画面を使用して、vCenter Server と NSX Manager の概要を vRealize Network Insight で確認することができます。

[VMC SDDC] 画面へのアクセス方法

この画面にアクセスするには、**VMC Sddc** で検索し、検索結果リストで、表示する [VMC SDDC] 画面をクリックします。

概要

[VMC SDDC] 画面には、次の情報が表示されます。

セクション	詳細
[概要]	NSX ポリシー エンティティ、過去 24 時間のエンティティ、上位のルール別フロー、ルーターのリスト、およびプロパティ詳細の概要が表示されます。
[上位エンティティ]	上位の通信仮想マシンのグラフが表示されます。
[ネットワーク トラフィックおよびイベント]	ネットワーク トラフィックの概要とイベントのリストが表示されます。

[Arista ハードウェア ゲートウェイ] および [Arista ハードウェア ゲートウェイのバインド] の詳細の表示

[Arista ハードウェア ゲートウェイ] および [Arista ハードウェア ゲートウェイのバインド] 画面を表示して、Arista ハードウェア ゲートウェイの概要を確認できます。

[Arista ハードウェア ゲートウェイ] 画面にアクセスする方法

[Arista ハードウェア ゲートウェイ] 画面にアクセスするには、**Arista ハードウェア VTEP** を検索し、検索結果リストで、表示するエンティティをクリックします。

[Arista ハードウェア ゲートウェイのバインド] 画面にアクセスするには、**Arista ハードウェア ゲートウェイのバインド** を検索し、検索結果リストで、表示するエンティティをクリックします。

概要

[Arista ハードウェア ゲートウェイ] 画面には、以下が表示されます。

- イベントのリスト
- 主要なプロパティのリスト
- Arista ハードウェア ゲートウェイのバインドのリスト。

[Arista ハードウェア ゲートウェイのバインド] 画面には、以下が表示されます。

- イベントのリスト
- プロパティのリスト。

[Cisco Nexus デバイス] の詳細の表示

[Cisco Nexus デバイス] 画面を使用して、vRealize Network Insight で使用可能な Cisco Nexus デバイスの概要を取得できます。

概要

この画面には、以下の項目が表示されます。

- パフォーマンス監視メトリック。

注： 各メトリックのインサイトを表示するには、各メトリック値をクリックします。

- イベント リスト。
- プロパティの詳細。
- スイッチ ポート、スイッチ ポートのピア、ポートに接続されている仮想マシンのリスト。
- スイッチ ポート メトリック。

フロー情報の詳細の表示

[フロー情報] 画面は、データセンター、デバイス、およびフローに関する判断材料を提供します。これは、選択したエンティティ、フロー、および時間範囲に基づいて分析を実行する、コンテキストベースの画面です。

[フロー情報] 画面にアクセスするには、以下の手順を実行します。

- 1 左側のナビゲーション ペインで、[分析] - [フロー情報] の順にクリックします。
- 2 [範囲] と [期間] を選択します。
- 3 [分析] をクリックします。

または、**フロー** を検索し、[検索結果] 画面で [フロー情報] をクリックします。

[フロー分析] ダッシュボードには、次のセクションがあります。

- 上位エンティティ
- 最新情報
- ネットワーク パフォーマンス
- 外れ値

上位エンティティ

このセクションでは、環境内で測定値の値が大きいエンティティを確認できます。ソースとターゲットのペア、仮想マシン、クラスタ、L2 ネットワーク、サブネットなど、さまざまな種類のエンティティを選択できます。このウィジェットには、選択したエンティティ カテゴリのうち、上位 10 件のエンティティが一覧表示されます。これは、ネットワーク最適化の計画に役立ちます。このウィジェットにあるバーで示されたメトリックは、次を示しています。

- フロー ボリューム別：トラフィック ボリュームを示します。
- トラフィック レート別：トラフィック レートを示します。
- セッション数別：セッション数を示します。
- フロー数別：フロー数を示します。

**注：**

- 1つ以上のメトリックに仮想マシンが表示される場合は、あるバー内でその仮想マシンをポイントすると、他のバーでもハイライトされます。
- メトリックバーで仮想マシンをクリックすると、その仮想マシンに送信されるフローの完全なリストが表示されます。
- [上位エンティティ] リストで仮想マシンをエンティティとして選択すると、ソースかターゲットかを問わず、この仮想マシンに関連するすべてのフローが表示されます。リストでソース仮想マシンを選択すると、この仮想マシンから送信されるフローのみが考慮されます。
- 物理フローを考慮している場合は、送信元 IP アドレスか宛先 IP アドレスのいずれかを選択できます。
- ソースとターゲットのペアを選択してメトリックバーをポイントした後、ツールチップのリンクをクリックすると、対応するダッシュボードが表示されます。たとえば、ソースとターゲットのペアの仮想マシンについては、仮想マシン間パスのダッシュボードが表示されます。
- フローグループビュー、フローエンティティプロジェクション、またはフローグループクエリについては、[フロー分析] ボタンは表示されません。

最新情報

このセクションは、選択した時間範囲内にデータセンターで検出されたサービスとエンティティを追跡するのに役立ちます。このセクションのウィジェットは次のとおりです。

- インターネットにアクセスしている新しい仮想マシン：インターネットにアクセスしている新しい仮想マシンを一覧表示します。
- アクセスされた新しいインターネットサービス：環境内で検出された新しいインターネットサービスを一覧表示します。
- アクセスされた新しい内部サービス：検出され、インターネットのエンドポイントからアクセスされた新しいイントラネットサービスを一覧表示します。
- アクセスされた新しい内部/E-W サービス：公開され、データセンター内のマシンからアクセスされたサービスを一覧表示します。

- ブロックされたフローがある新しいサービス：ブロックされたフローがあるサービスを一覧表示します。このセクションは、IPFIX についてのみポピュレートされます。
- 新しいファイアウォール ルールのヒット：有効な新しいファイアウォール ルールを一覧表示します。このセクションは、IPFIX についてのみポピュレートされます。

ネットワーク パフォーマンス

このセクションでは、選択した基準に基づいて、さまざまな範囲の TCP ラウンド トリップ時間 (RTT) 値から異常フローを見つけて可視化できます。

注： vRealize Network Insight には、5 分間隔で測定された過去 24 時間のみの平均 TCP RTT が表示されません。

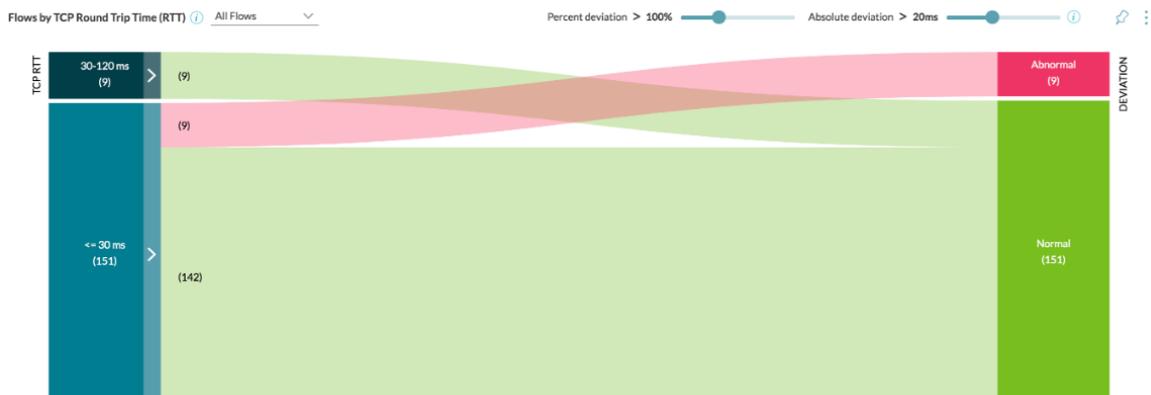
フローの偏差の割合が 100% で、絶対偏差が 20 ミリ秒 (ms) の場合、vRealize Network Insight ではこのフローが異常フローと判断されます。

視覚化では、左側に TCP RTT のさまざまな範囲が表示され、右側には正常と異常の範囲が表示されます。偏差と絶対偏差のパーセント値に基づいて、フローが左 (TCP RTT) から右 (偏差) に関連付けられます。以下のタイプのフローを分析できます。

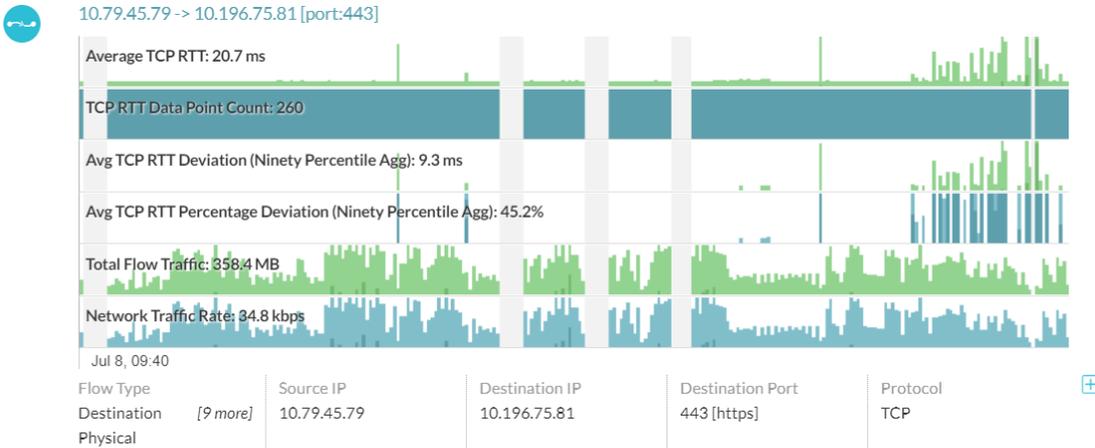
- ホスト間
- ホスト内
- インターネット
- すべてのフロー

要件に基づいて、偏差のパーセント値や絶対偏差を変更することもできます。

次の例では、TCP RTT の範囲を 2 種類示しています。1つは 30 ミリ秒以下、もう1つは 30 ~ 120 ミリ秒です。30 ミリ秒以下の TCP RTT 範囲には、合計 151 件のフローが発生していることがわかります。この 151 件のフローのうち、9 件のフローが異常なフローとして示されています。



TCP RTT 分布情報およびフロー数の詳細な判断材料を得るには、表示の中で色が設定されている行をクリックします。次の例では、TCP RTT 分布情報とフロー数に関する詳細な判断材料を確認できます。

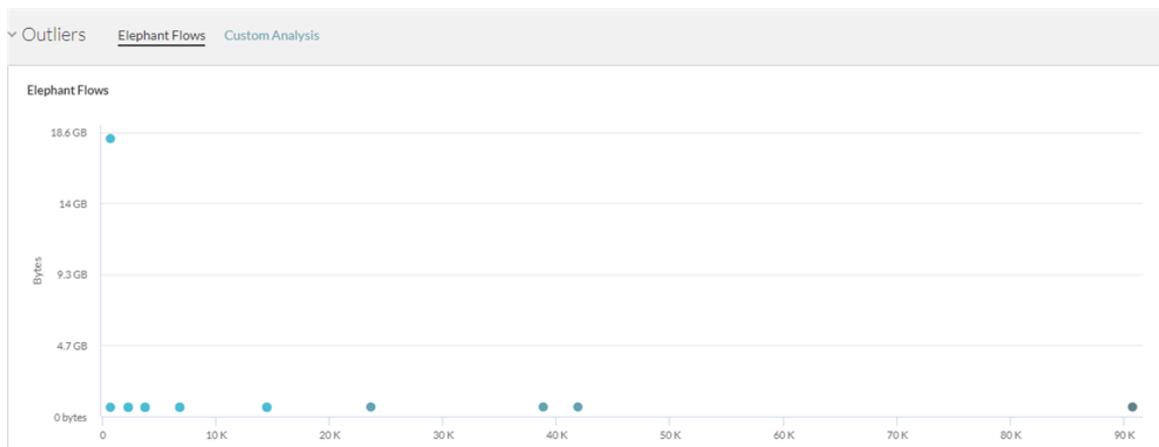


外れ値

このセクションは、関連データの追跡と分析に役立ちます。次のセクションで構成されています。

- エレファントフロー：このセクションは、セッション数が少なくスループットが大きいフローと、セッション数が多くスループットが小さいフローを識別するのに役立ちます。通常、セッション数が多くスループットが小さいフローは「マウスフロー」とも呼ばれます。分析は、セッション数に対するバイト数の比率に基づきます。グラフ内のそれぞれの点は、複数のフローを表します。点をポイントすると、フローのリストが表示されます。特定のフローの詳細を表示するには、リスト内でそのフローをクリックします。
- カスタム分析：このセクションでは、選択した2つのディメンションでフローデータを視覚的に表示できます。データを分析して外れ値をさまざまな方法で見つけるのに役立ちます。

注： このセクションに示すメトリックは概数値であり、正確な値ではありません。



マイクロセグメンテーションの詳細の表示

フローを分析するには、範囲を選択し、エンティティに基づいてフローをセグメント化します。このエンティティには、VLAN/VXLAN、セキュリティグループ、アプリケーション、階層、フォルダ、サブネット、クラスター、仮想マシン (VM)、ポート、セキュリティタグ、セキュリティグループ、IPSet があります。

マイクロセグメンテーション画面に、分析の詳細がトポロジ図と一緒に表示されます。この画面は、次のセクションで構成されています。

- **マイクロセグメント**：このウィジェットは、トポロジ計画の図を提供します。グループのタイプとフローを選択できます。入力内容に基づいて、対応するトポロジ計画図を表示できます。
- **トラフィックの分布**：このウィジェットは、トラフィック分布の詳細をバイト単位で提供します。
- **バイト数の上位ポート**：このウィジェットは、トラフィックが最も多い上位 100 個のポートを一覧表示します。フロー カウントとフロー ボリュームのメトリックが提供されます。特定のポートのフローを表示するには、そのポートに対応するフローの数をクリックします。

マイクロセグメンテーション画面にアクセスするには、次のようにします。

手順

- 1 ホーム ページの左側にあるナビゲーション パネルで、[セキュリティ] > [セキュリティの計画] をクリックします。
- 2 計画と分析の対象範囲、サブスコープ、および期間を選択します。[分析] をクリックします。

マイクロセグメンテーション画面が表示されます。

注： ドーナツ ビューでは、ノードは 600 台、エッジは 6,000 個まで表示できます。制限を超えると、「分析対象のマイクロセグメントが多すぎます。別のエンティティまたはマイクロセグメントの条件を選択してください」というエラーが表示されます。

アプリケーションの詳細の表示

アプリケーションは階層の集合体です。アプリケーションの各階層は、ユーザー定義のフィルタ基準に基づいた仮想マシンと物理 IP アドレスの集合です。アプリケーションを使用すると、階層のグループを作成し、同じアプリケーションの階層間、またはアプリケーション間のトラフィックやフローを視覚化できます。

vRealize Network Insight にアプリケーションを作成または追加するには、次の 3 つの方法があります。

- [手動によるアプリケーションの作成](#)
- [パブリック API](#)
- [アプリケーション検出](#)

[アプリケーション] 画面では、vRealize Network Insight の 1 つのアプリケーションの全体を把握できます。これにより、問題をトラブルシューティングしたり分析を表示したりすることができます。

- **概要**
 - アプリケーション トポロジ
 - 階層の概要
 - アプリケーション内の仮想マシンのリスト
 - アプリケーションが依存または使用する物理 IP アドレス
 - 共有サービス

- この特定のアプリケーションの通信対象となっているアプリケーション
- アプリケーションに関連するイベント
- アプリケーション仮想マシン マネージャ
- 直近 24 時間の最新情報
 - 受信および送信トラフィック数
 - ドロップされたフロー
 - 新規および保護されていないメンバー
 - 外部からアクセスされるサービス
 - インターネットからアクセスされるサービス
 - 使用されるアプリケーション ポート
- トラフィック フローまたはフロー分析
 - 上位エンティティ
 - 上位のルール別アプリケーション フロー
- マイクロセグメンテーション
 - エンティティ間のコンテキスト フローについて、すべての許可されたフロー、ドロップされたフロー、NSX DFW によって保護されているフロー、保護されていないフローなど、さまざまなフロー タイプのデータが得られます。
 - アプリケーションの最新情報
- メトリック
 - ネットワーク速度、CPU、メモリ、ディスクの情報を表す仮想マシン メトリック情報。
 - Kubernetes メトリック

分析：外れ値検出

vRealize Network Insight は、複数の仮想マシンと物理 IP アドレスに対して定義されたフローに関連付けられたメトリックに基づく、外れ値の検出機能を備えています。この場合の仮想マシンと IP アドレスは、特定の仮想マシンまたは IP アドレスを意味ある外れ値として分類できるように、トラフィック パターンが似ていることが必要です。たとえば、あるアプリケーションの同じ階層に属する複数の仮想マシンは通常、そのアプリケーションに対して同じ機能を実行します (Web アプリケーションに対して要求を処理する SQL データベースの仮想マシンなど)。これらの種類の仮想マシンでは、受信した要求の数、送信されたトラフィックの量、セッション数などの値が似たような傾向を示します。

vRealize Network Insight の外れ値検出により、グループ内の他の仮想マシンや IP アドレスと比べてトラフィックパターンが大きく異なる特定の仮想マシンを検出できます。たとえば、ある仮想マシンが送受信しているトラフィックが、グループの他の仮想マシンと比較して大幅に多い、または少ないことがあります。原因として、ロードバランサの設定が正しくないことや、DDOS 攻撃が考えられます。vRealize Network Insight は、これらの仮想マシンまたは IP アドレスを外れ値として分類します。これらの外れ値を調べることで、ユーザーは予期しない動作を簡単に把握し、適切な措置を講じることができます。

外れ値を持つ仮想マシンの検出方法

手順

- 1 サイドバーで、[分析] をクリックします。[外れ値] をクリックします。
- 2 [追加] をクリックして設定を追加します。
- 3 [分析/設定] 画面で、設定について次の詳細情報を指定します。

表 12-6.

フィールド	説明
名前	設定の名前
範囲	<p>分析を実行する必要がある仮想マシンと IP アドレスを定義するグループの名前。範囲には [アプリケーション層] または [セキュリティグループ] を選択できます。</p> <p>[アプリケーション層] を選択した場合は、アプリケーションと階層の名前を個別に指定します。階層名の横には、その階層に対して定義されている仮想マシンと物理 IP アドレスの数が表示されます。</p> <p>[セキュリティグループ] を選択した場合は、セキュリティグループの名前を指定します。</p> <p>注: 階層内の仮想マシンと物理 IP アドレスの数の上限は現在のところ 200 です。この制限を下回る仮想マシンと物理 IP アドレスを持つ階層またはセキュリティグループを選択してください。範囲には、3 台以上の仮想マシンと物理 IP アドレスを含める必要があります。</p> <p>選択した設定のマイクロセグメンテーションを表示するには、[マイクロセグメントの表示] をクリックします。</p>
検出タイプ	現在、vRealize Network Insight ではシステム内の外れ値を検出できます。
メトリック	<p>検出は、このフローメトリックに基づいています。次のオプションを選択できます。</p> <ul style="list-style-type: none"> ■ [バイト] ■ [パケット] ■ [セッション] ■ [トラフィックレート]
トラフィック方向	トラフィックの方向として、[送信]、[受信]、または [両方] を選択できます。[両方] を選択した場合は、設定のプレビューで [受信] または [送信] を指定できます。
トラフィックタイプ	要件に基づき、[インターネット]、[East-West]、または [すべて] を選択できます。

表 12-6. (続き)

フィールド	説明
ターゲット ポート	<p>選択した範囲で見つかったフロー上で検出されたすべてのポートを選択するか、特定のターゲット ポートを手動で入力できます。[すべてのポート]を選択すると、ターゲット ポートの数が表示されます。[ポートを手動で入力]を選択し、オートコンプリート テキスト ボックスにポートを入力すると、分析はこれらのポートのみに制限されます。</p> <p>注： 現在、最大ポート数は 20 です。</p>
感度	<p>必要とされる検出とレポートの感度を測る尺度です。デフォルト値は [中] です。</p>
プレビュー	<p>このセクションは、指定した入力とパラメータに基づいた、特定の設定のプレビューを表示します。すでに [トラフィック方向] で [両方] を選択している場合は、ポートとトラフィック方向を指定します。これで、外れ値のある仮想マシンをグラフ内で識別できます。</p>

注：

- 外れ値は、過去 24 時間の使用可能なデータを評価することで検出されます。
- 外れ値を検出するには、IPFIX データの連続フローが必要です。

- 4 [送信] をクリックして、分析設定を作成します。
- 5 アプリケーションが作成されると、[分析設定] 画面のアプリケーションのリスト表示で使用できるようになります。特定のアプリケーションをクリックすると、関連付けられたダッシュボードが表示されます。

分析：静的および動的しきい値

vRealize Network Insight を使用すると、しきい値を設定および構成し、エンティティの動作の逸脱に基づいてアラートを受け取ることができます。次の 2 種類のしきい値を設定できます。

- 静的しきい値：特定のメトリック値が設定値を超えた場合、またはそれを下回っている場合、静的しきい値ベースのアラートが生成されます。
- 動的しきい値：しきい値が履歴データの分析に基づいてシステムによって決定されたものである場合、このしきい値に違反するとアラートが生成されます。アラートが生成される前に、データは 7 日間分析されます。ベースラインの作成プロセスは履歴データの 21 日間に制限されており、古いメトリック値は、新しいメトリック値のベースラインの作成に組み込まれません。

アラートは、しきい値に違反した直後に生成されます。Enterprise ライセンス ユーザーは、しきい値違反の数を [ホーム] 画面の [現在の状態] セクションで確認できます。イベントの詳細を表示するには、しきい値違反の数をクリックします。システム内にしきい値設定がない場合は、[現在の状態] セクションに [+ 設定] リンクが表示されます。[+ 設定] リンクをクリックして、しきい値を設定できます。

しきい値とアラートの設定

しきい値設定を追加して、設定したしきい値のアラートを取得できます。

分析に関連するしきい値とアラートを設定するには、次の手順を実行します。

手順

- 1 [ホーム] 画面の左側のナビゲーション パネルで、[分析] - [しきい値] - [追加] の順にクリックします。

[しきい値 - 設定の追加] 画面が表示されます。

- 2 [名前] テキスト ボックスに、設定の一意の名前を入力します。

- 3 [範囲] ドロップダウン メニューから範囲を選択し、[基準の選択] テキスト ボックスに基準を入力します。

[範囲] ドロップダウンは、[仮想マシン]、[フロー]、[アプリケーション]、[SD-WAN リンク]、[SD-WAN Edge]、[SD-WAN Edge アプリケーション] の各エンティティで構成されます。範囲は、検索クエリ システムに基づきます。要件に従って、用意されている提案からクエリを作成できます。

- 4 [条件] セクションで、アラートを作成するための条件を設定します。

設定した条件に基づいて、しきい値を超えたかどうかシステムによって決定されます。

5 デフォルトのメトリックは、`network traffic rate` です。エンティティのグループ分けと、しきい値を確認する値を選択します。エンティティ グループ全体のデータを集約することで、累積メトリックのしきい値を設定できます。

a 静的しきい値を設定するには、リストから次のしきい値条件のいずれかを選択します。

- [しきい値を超過]
- [しきい値以下]
- [範囲外]

`network traffic rate` か `total traffic` またはその他のメトリックについて Upper Bound または Lower Bound (範囲がある場合) を入力する場合は、その特定のテキスト ボックスの指定されたメトリックに値を確実に入力します。次の変換値が参考になります。

- 1 Kbps = 1000 bps
- 1 Mbps = 1000 kbps
- 1 Gbps = 1000 mbps
- 1 KB = 1024 B
- 1 MB = 1024 KB
- 1 GB = 1024 MB

b 動的しきい値を設定するには、[過去の動作からの逸脱] を選択します。レポートの要件に基づいて感度を選択します。

Condition ⓘ

For metric `network traffic rate` aggregated over `virtual machine` when `any value` `deviates from past behavior`

Sensitivity `Medium (2.5 standard deviation)`

- exceeds threshold
- drops below
- is outside range
- deviates from past behavior

しきい値を設定すると、関連付けられたグラフが画面の上部に表示されます。ピンクのバーは、しきい値に違反している仮想マシンまたはフローを示します。しきい値に違反したエンティティのリストと、システムのしきい値内にあるエンティティのリストを表示できます。

6 次のプロパティを設定して、通知またはアラートを設定します。

- [重大度]
- [Eメールの頻度]
- [通知メールの送信先:]

注： システムで SNMP トラップを設定した場合は、[SNMP トラップの送信] を選択します。

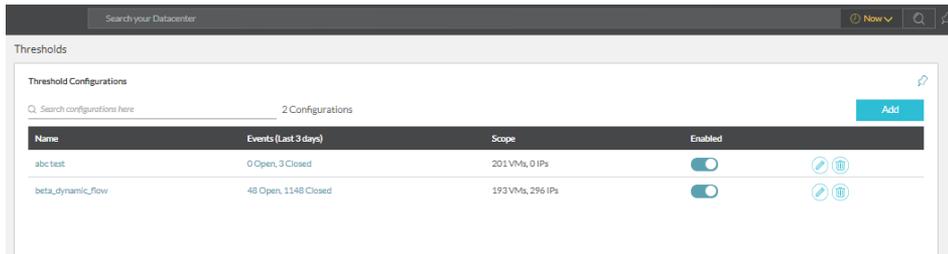
7 [送信] をクリックして、しきい値設定を作成します。

しきい値設定画面の表示

しきい値設定を追加した後、その詳細を [しきい値設定] 画面に表示できます。

手順

- 1 左側のナビゲーション パネルで、[分析] をクリックします。[しきい値] をクリックします。

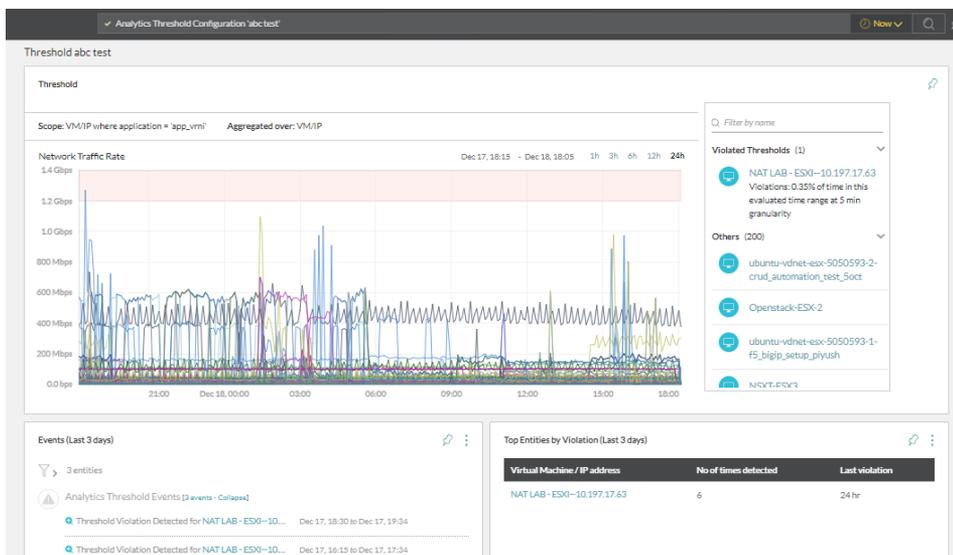


- 2 しきい値設定について、次の詳細情報が提供されます。

- Name
- Events
- Scope

設定が無効になっている場合、その特定のしきい値の違反に関するアラートは生成されません。この画面では、特定のしきい値設定を検索することもできます。

- 3 特定のしきい値設定のダッシュボードを表示するには、リストから目的の設定をクリックします。



ダッシュボードには、次のウィジェットを表示できます。

- グラフ：しきい値グラフは、しきい値に違反したエンティティを検出するのに役立ちます。
- イベント：このウィジェットには、過去 3 日間に違反したしきい値に対して生成されたイベントのリストが表示されます。

- 違反別の上位エンティティ：このウィジェットには、過去 3 日間の逸脱の原因となった上位のエンティティが表示されます。

エンティティ トポロジの表示

13

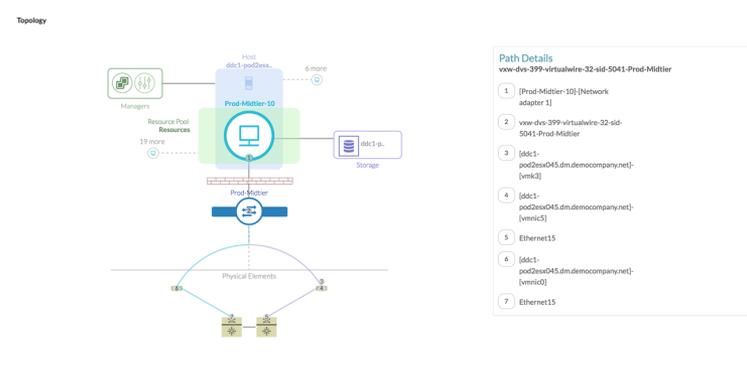
トポロジを使用すると、エンティティ全体を視覚的に把握できます。

この章には、次のトピックが含まれています。

- 仮想マシン トポロジ
- ホスト トポロジ
- VXLAN トポロジ
- VLAN トポロジ
- NSX Manager トポロジ

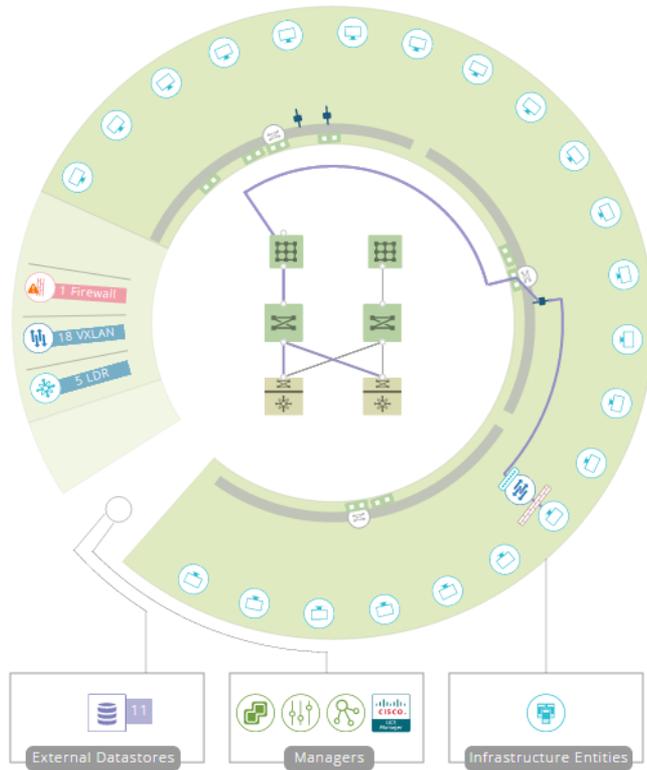
仮想マシン トポロジ

仮想マシン トポロジは、単一の仮想マシンと、データセンターの他の部分との関連性を包括的に示します。



ホスト トポロジ

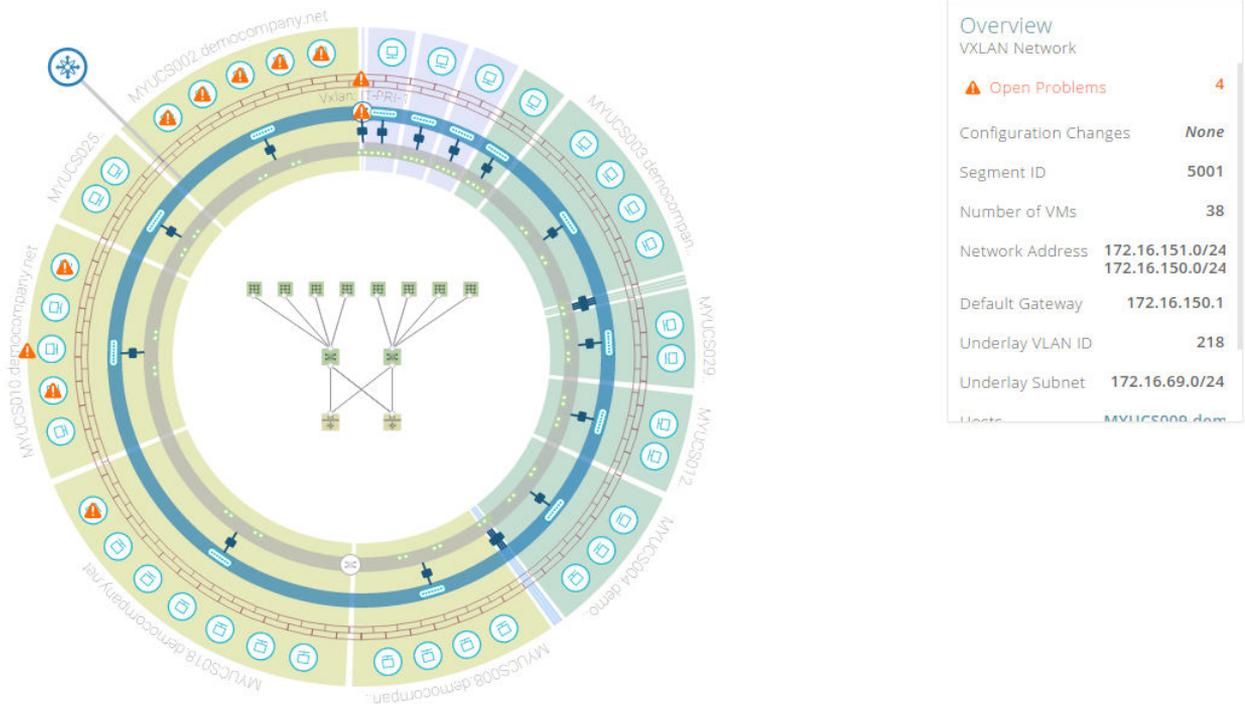
ホスト トポロジは、特定のホストの仮想マシンがデータセンターの仮想および物理コンポーネントにどのように接続されているか、およびホスト自体がデータセンターに接続されているかどうかを示します。



VXLAN トポロジ

VXLAN (Virtual eXtensible Local Area Network) のオーバーレイ ネットワーク テクノロジーは、VMware が主要なネットワーク ベンダーと共同で開発した業界標準です。

VXLAN トポロジは、選択した VXLAN の概要を提示する革新的な視覚化手法です。次の図は、視覚化を構成するさまざまなコンポーネントを示しています。



注： この手法では、仮想コンポーネントと物理コンポーネントの両方を視覚化できます。

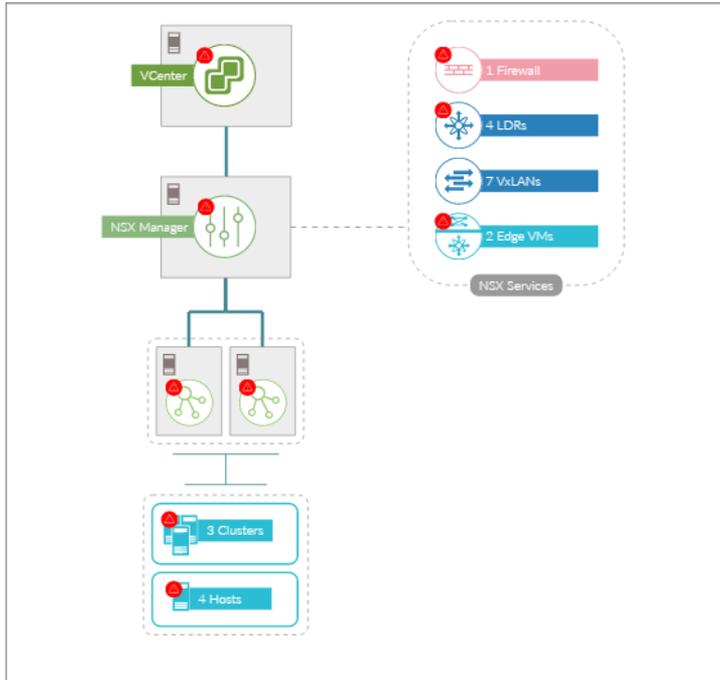
VLAN トポロジ

仮想 LAN (VLAN) は、単一の物理 LAN セグメントをさらに分離して、ポート グループが物理的に別々のセグメントにあるかのように、互いに分離できます。

VLAN トポロジは、VXLAN トポロジと同様の方法で構築されます。

NSX Manager トポロジ

NSX Manager トポロジには、NSX Manager に関連付けられているコンポーネントが表示されます。



vRealize Network Insight での NSX オブジェクトの監査情報の表示

vRealize Network Insight を使用すると、NSX-T Manager および NSX-V Manager から NSX オブジェクトの監査情報をすばやくキャプチャできます。この情報には、NSX オブジェクトを作成または変更したユーザー名、その操作が行われた日時、およびオブジェクトに対する操作の詳細が含まれます。

NSX-T Manager または NSX-V Manager で監査ログを有効にしている場合、vRealize Network Insight によって一部の NSX-T オブジェクトおよび NSX-V オブジェクトの監査の詳細を収集できます。

NSX-V

vRealize Network Insight によって 3 ~ 5 分以内に監査の詳細が収集される NSX-V オブジェクトのリスト。

- SecurityGroup
- SecurityGroupTranslation
- FirewallConfiguration
- FirewallStatus
- IPSet
- SecurityTag
- UniversalSecurityGroup
- UniversalSecurityGroupTranslation
- UniversalIPSet

NSX-V オブジェクトの監査の詳細は、次のように検出イベント、プロパティの変更イベント、および削除イベントについてキャプチャされます。

■ Discovery



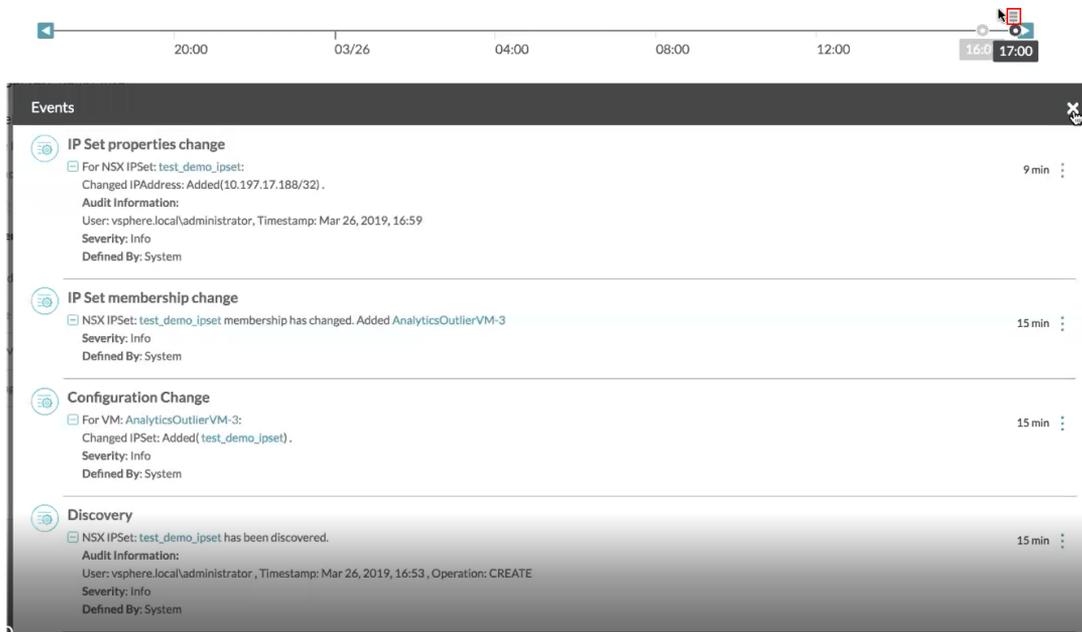
■ Properties Change



■ Delete

<p>NSX IPSet:jagdish_ipset12 deleted.</p> <p>Audit Information: User: vsphere.local\administrator, Timestamp: Feb 13, 2019, 11:23</p> <p>Severity: Info</p> <p>Defined By: System</p>	6 min
<p>NSX Universal IPSet:jagdish_ipset13_universal deleted.</p> <p>Audit Information: User: vsphere.local\administrator, Timestamp: Feb 13, 2019, 11:24</p> <p>Severity: Info</p> <p>Defined By: System</p>	6 min

オブジェクトのタイムラインで監査情報を表示することもできます。



NSX-T

vRealize Network Insight によって監査の詳細が収集される NSX-T オブジェクトのリスト。

注： VMC ポリシー エンティティには、監査情報を使用できません。

- NSGroup
- NSService
- NSServiceGroup
- NSFirewallRule

注： NSFirewallRule の削除イベントには、監査情報を使用できません。

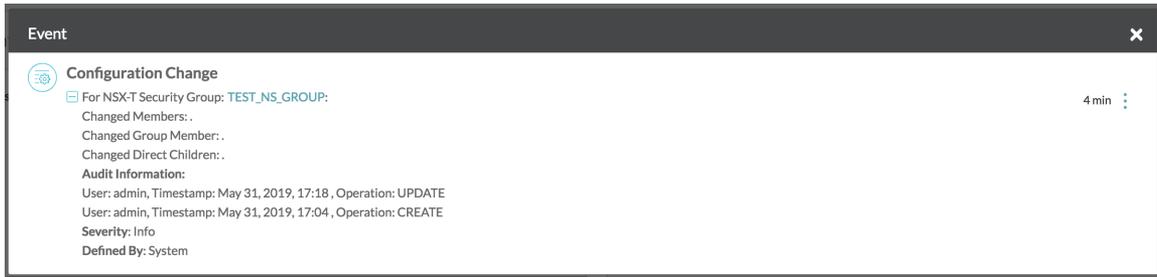
- IPSet
- NSX ポリシー グループ
- NSX ポリシー ファイアウォール ルール

NSX-T オブジェクトの監査の詳細は、次のように検出イベント、プロパティの変更イベント、および削除イベントが発生した場合にキャプチャされます。

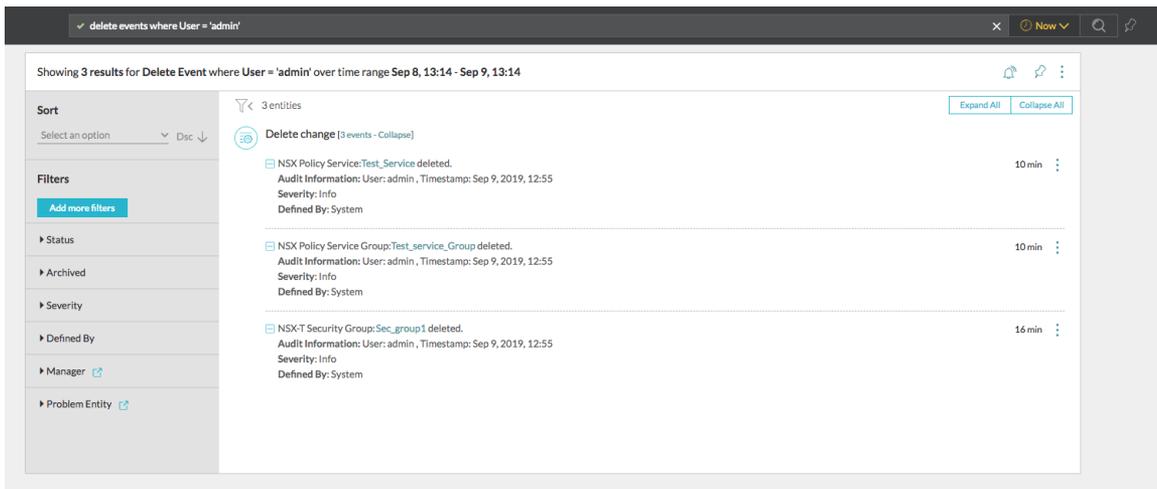
- Discovery



■ Properties Change



■ Delete



注： エンティティ ダッシュボードでは削除イベントを使用できません。ただし、イベントを検索して監査情報を表示することはできます。

監査情報を表示するサンプル クエリ

- `events where user = username`
- `discovery events where user = username`
- `delete events where user = username`
- `change events where user = username`

アプリケーションのあらゆる部分はピンで表されます。ピンは基本単位であり、保存できるうえ、組み合わせると便利なデータをグループにまとめてチームの他のメンバーと共有できます。検索クエリをピンに固定できるほか、エンティティに使用できるピンもあります。

ピンを追加するには、ピン アイコンをクリックします。保存済みのすべてのピンは、ヘッダーのピンボード アイコンをクリックすると起動する [ピンボード] セクションに表示されます。

この章には、次のトピックが含まれています。

- [ピン](#)
- [ピンボード](#)

ピン

各エンティティ ページの情報は複数のピンに分かれています。すべてのエンティティ ページはピンで構成され、各ピンにはエンティティに関連する特定の情報が含まれています。

ピンの機能は次のとおりです。

- [その他のオプション] ボタンを使用すると、ピン表示を最大化できます。また、[ヘルプ] オプションを使用して、ピンに関する詳細情報を表示することもできます。
- ピンには、ピンに表示されるデータをドリルダウンするためのフィルタを含めることもできます。
- 多くのピンには [CSV としてエクスポート] オプションもあり、これを使用して、ピンのデータを CSV 形式でエクスポートできます。表示されるダイアログで、エクスポートする特定のプロパティと CSV 行の数を選択できます。

注： すべてのフィールドが選択されている場合、フロー データの CSV へのエクスポート機能では、180,000 個のフローのエクスポートに 30 分以上かかります。

ピンのタイプ

ソフトウェアで使用できるほとんどのピンは、次のように分類できます。

メトリック ピン

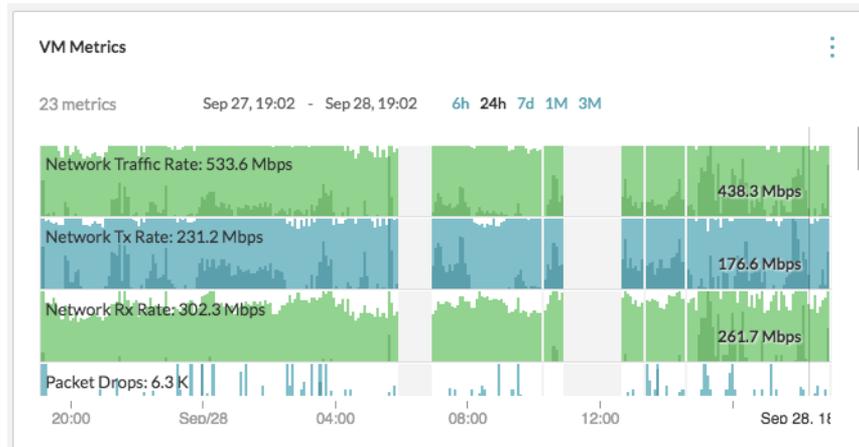
メトリック ピンには、選択したエンティティに関連する重要なメトリックが表示されます。

メトリック ピンは、立体的なグラフを使用しており、各グラフを2つの帯に分けて大きい方の値をもう一方の上に配置してデータを表示します。これにより、大きい方の値が濃い色で表示され、わかりやすくなります。

ピン ヘッダーにあるドロップダウンから、表示する特定のメトリックを選択したり、表示するエンティティの選択肢を変更することもできます。

時間範囲は、範囲のプリセットを使用するか、カスタムの日時を入力することで変更できます。

メトリック ピンの一例は、[仮想マシン メトリック] ピンです。このピンには、仮想マシンのネットワークトラフィック レート、ネットワーク Tx レート、ネットワーク Rx レート、およびパケットのドロップが表示されます。



エンティティのリスト表示ピン

エンティティのリスト表示ピンには、共通のテーマによってグループ化されたエンティティのリストが表示されます。リストには、エンティティごとの重要な属性が表示されます。

右端の拡大アイコンをクリックすると、特定のエンティティの属性をさらに表示できます。エンティティ名をクリックすると、エンティティ画面に移動します。

他のピンと同じく、フィルタ アイコンには、リストのフィルタリングに使用できるさまざまなファセットが含まれています。エントリのリスト表示ピンの例として、仮想マシンのネイバー ピンが挙げられます。デフォルトでは、このピンには同じホスト上にある仮想マシンが表示されます。また、セキュリティ グループ、VXLAN、およびデータストアごとに仮想マシンをフィルタリングすることもできます。

The screenshot shows the 'VM Neighbors' dashboard for host 'ddc1-pod2esx...'. It displays a list of 7 entities. The following table shows the first three entities and their key attributes:

Entity Name	Attributes
Prod-Midtier-14	CIDR: 10.17.7.14/24, Def Gateway: 10.17.254, Logical Switches: Prod-Midtier
Lab-Web-19-noip	Logical Switches: Lab-Web, CPUs: 16, Memory (GB): 16
Prod-Db-5	CIDR: 10.17.8.10/24, Def Gateway: 10.17.8.254, Logical Switches: Prod-DB

イベント表示リストのピン

イベント リスト表示のピンには、特定のエンティティまたはエンティティ グループ（ピン ヘッダーのドロップダウンから選択可能）に関するイベントのリストが時系列で表示されます。

現時点からどこまで遡ってイベントをピンに表示するかは、用意されている事前設定を使用するか、カスタムの日時を入力して変更できます。[イベント ステータス] や [イベント タイプ] などの他のフィルタ オプションは、フィルタ アイコンをクリックして選択できます。

次の図では、仮想マシン Prod-db-vm21 に関連するイベントとその関連エンティティが表示されます。エンティティ名をクリックすると、他の関連エンティティのイベントを表示できます。フィルタを使用すると、状態とタイプに基づいてイベントをフィルタできます。イベントとは、特定のエンティティに関する変更または問題です。

The screenshot shows the 'Events' section for the entity 'VM: SITED-ESX-01'. It displays a list of events with the following details:

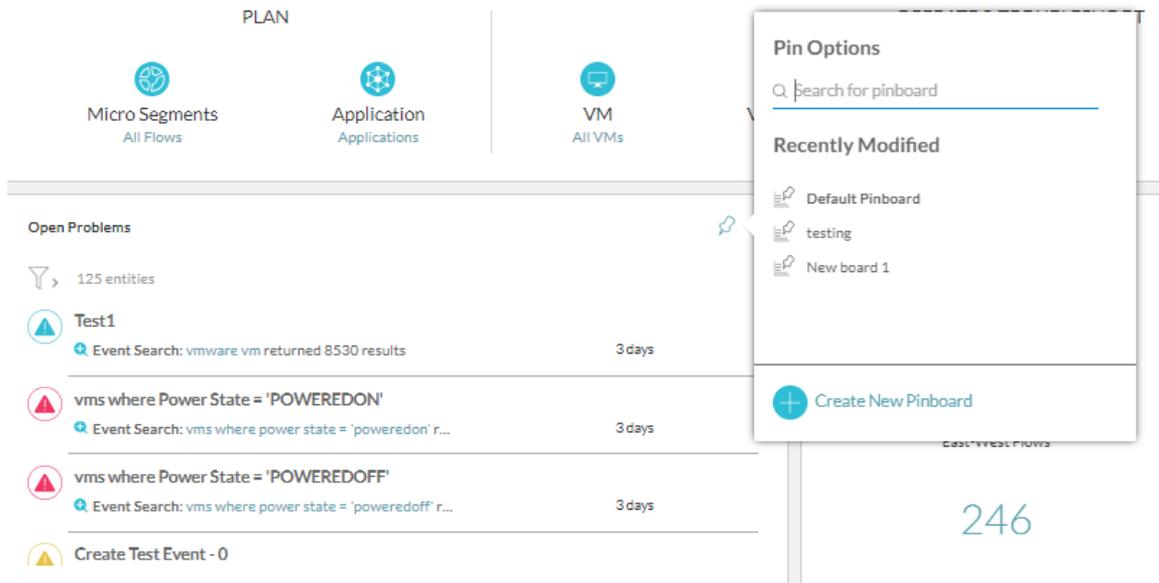
- Configuration change [5 - Show all]**: For Host: 192.168.0.218: VMs has changed. Added 122, deleted 0. 4 days
- Discovery**: Virtual Machine: SITED-ESX-01 has been discovered. 4 days
- Delete change**: Virtual Machine: SITED-ESX-01 deleted. 8 days
- Configuration change [2 - Show all]**: For Virtual Machine: SITED-ESX-01: VDS has changed. Added VDS-Priv-Netw... 8 days

イベントは、イベント検索クエリを使用して検索できます。未解決イベントや解決済みイベントなどのクエリを使用して、これらのイベントを検索できます。同じ修飾子を使用して問題を検索することもできます。

ピンボード

ピンボードのページからウィジェットをピン留めして、データへのアクセスや共有を容易にすることができます。

ピンボードを作成するには



- 1 ピン留めするウィジェットのピンアイコンをクリックします。
- 2 ポップアップウィンドウで [ピンボードの新規作成] をクリックします。

注：

- ピンボードを初めて作成する場合は、[最近変更された項目] リストから [デフォルトのピンボード] を選択します。

注： [デフォルトのピンボード] には、初めて使用するユーザー向けの一般的なピンボードのルックアンドフィールが設定されています。ユーザーがピンボードのレイアウトと機能に慣れるのに適しています。共有または削除することはできません。ピン留めした内容は、デフォルトピンボードからカスタムピンボードにコピーできます。

- [最近変更された項目] リストに表示できるエントリの最大数は 15 個です。
- すべてのユーザーに対して作成できるピンボードの最大数は 500 個です。

注： ピンボードの総数には、カスタムピンボード、共有ピンボード、およびデフォルトピンボードが含まれます。

- ピンボードあたりのピンの最大数は、20 個です。

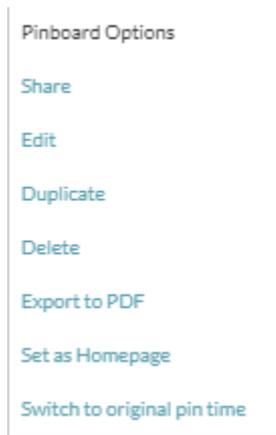
- 3 [ピンボードの作成] ウィンドウで、新しいピンボードの名前と説明を入力します。[作成してピン留め] をクリックします。

注：

- ピンボードの名前は、システム全体で一意である必要があります。
- ピンボード名に使用できる最大文字数は 100 文字です。ピンボードの名前に使用できるのは、文字、数字、スペースのみです。

- 4 [ピンボードが作成されました] というメッセージが表示されます。[今すぐ共有] をクリックすると、ピンボードをただちに共有できます。
- 5 ウィジェットを既存のピンボードにピン留めするには、[最近変更された項目] の下にあるピンボードを選択し、[ピン] をクリックします。[ピンが追加されました] というメッセージが、対応するピンボードへのリンクとともに表示されます。

ピンボード オプションにアクセスするには



[ピンボード オプション] にアクセスするには、ピンボードの右上隅にある [その他のオプション] をクリックします。

注： すべてのピンボード オプションを表示できるのは、自分でピンボードを作成した場合、または [表示および編集] 権限をもつ他のユーザーと共有した場合のみです。それ以外のユーザーに表示されるのは、[PDF にエクスポート] オプションと [元のピン時間に切り替え] オプションのみです。

ピンボードでは、次の操作を実行できます。

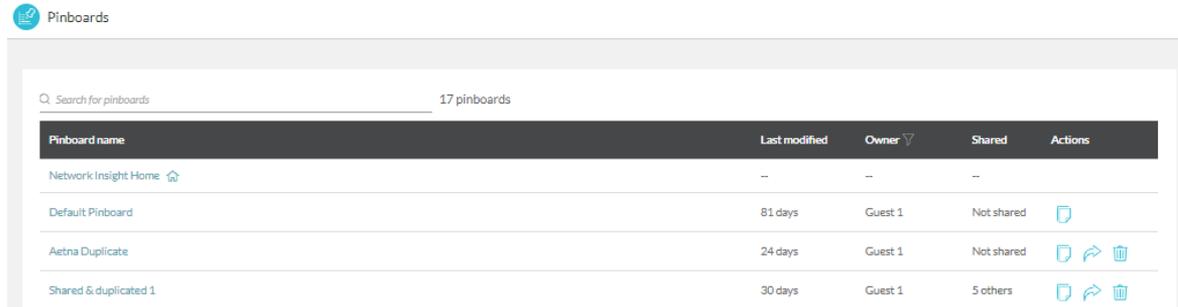
- ピンボードは他の既存の vRealize Network Insight ユーザーと共有できます。
- ピンボードの名前とピンボード上のピンは、編集できます。
- ピンはピンボード上で並べ替えることができます。ピンの位置は保持されます。
- 特定のピンボードを削除するには、[削除] をクリックします。
- [PDF にエクスポート] をクリックすると、ピンボード上の情報を PDF レポートとしてエクスポートできます。詳細については、[PDF としてエクスポート](#)を参照してください。
- ピンがピン留めされたときのデータを表示するには、[元のピン時間に切り替え] をクリックします。この機能を使用すると、ピン作成時のデータを表示できます。

ピンボードのタイムライン スライダを使用するには

vRealize Network Insight は、ピンボードでタイムライン スライダをサポートしています。特定の時間のピンボード データを表示するには、タイムライン スライダを使用します。ピンボードがロードされると、現在時刻 ([今]) のすべてのピンがロードされます。

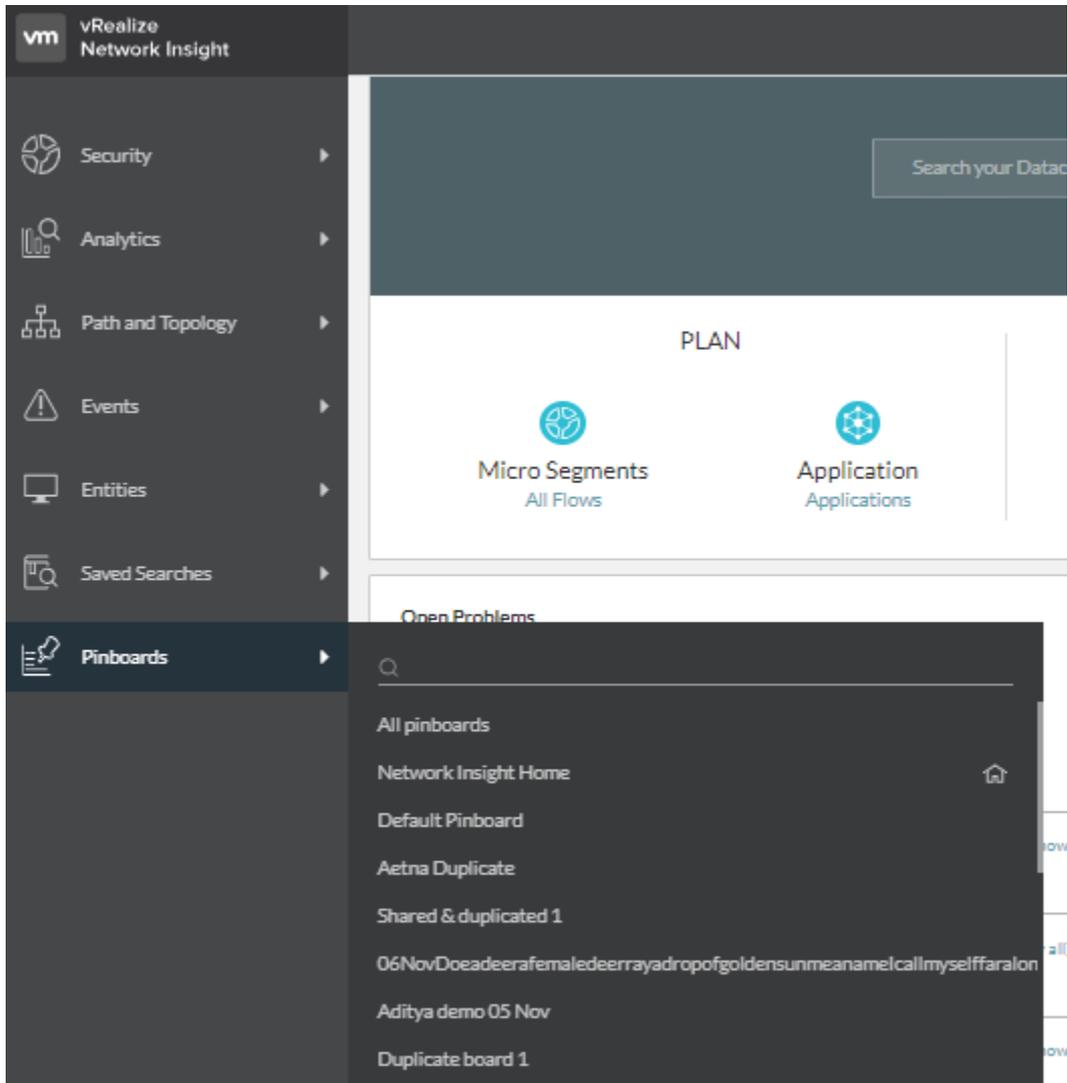
ピンボード ライブラリを表示するには

管理者ユーザーのピンボード ライブラリには、次の図に示すように、[マイ ピンボード] タブと [すべてのピンボード] タブが表示されます。メンバー ユーザーのピンボード ライブラリには、ピンボードのリストが表示されます。



- 1 ホーム画面の左側のナビゲーション バーで、[ピンボード] をクリックします。
- 2 システム内のすべてのピンボードを表示するには、[すべてのピンボード] をクリックします。
- 3 ナビゲーション バーでは、既存のピンボードのリストを表示できます。このリストには、ピンボード ライブラリの [マイ ピンボード] タブと同じ項目が含まれています。前回変更したピンボードがリストの最上部に表示されます。表示するピンボードをクリックします。

注： ピンボードが作成後にこのリストに表示されるまでには、しばらく時間がかかります。



4 ライブラリ内のピンボードを検索することもできます。

ピンをコピーするには

- 1 ウィジェットのピンアイコンをクリックします。
- 2 ピンのコピー先のピンボードを選択します。
- 3 [追加] をクリックします。

ピンボードの共有とコラボレーション

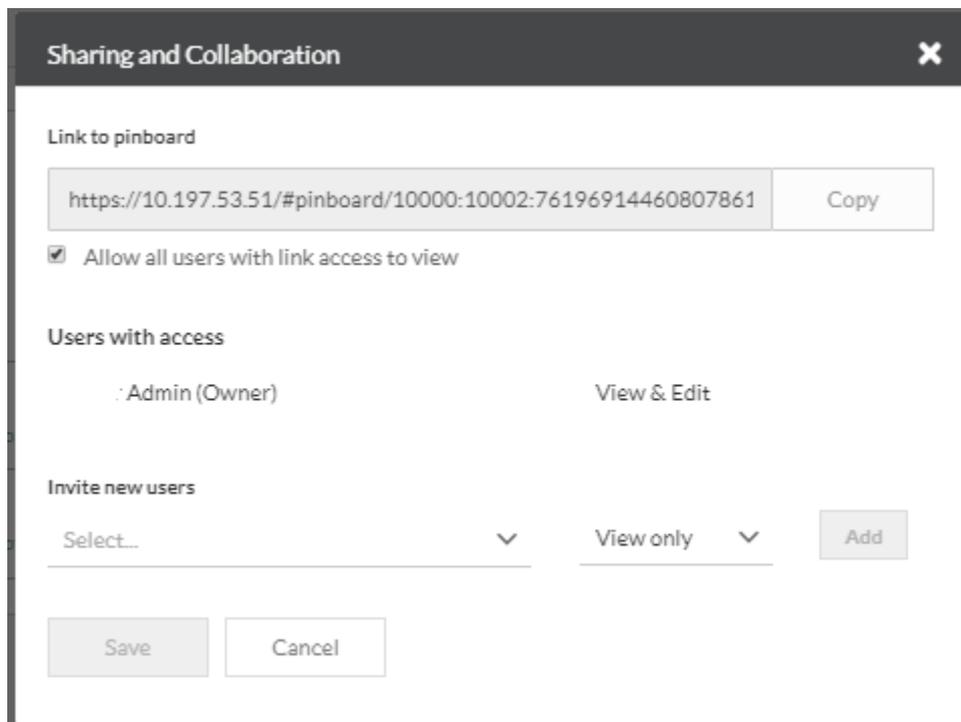
作成したピンボードは他のユーザーと共有できます。管理者ユーザーは、どのピンボードも表示および削除できます。ピンボードの共有とコラボレーションに関する機能を次に示します。

自分でピンボードを作成した場合は、管理者ユーザーかメンバーユーザーかは関係なく、ピンボードの表示、編集、削除を行うことができます。

表 14-1.

ピンボードの所有者	共有可能な相手	権限	実行可能な操作
管理者	管理者	表示、編集	表示、編集、削除
	管理者	表示のみ	表示、削除
	メンバー	表示、編集	表示、編集
	メンバー	表示のみ	表示
メンバー	管理者	表示、編集	表示、編集、削除
	管理者	表示のみ	表示、削除
	メンバー	表示、編集	表示、編集
	メンバー	表示のみ	表示

注： ピンボードを削除する必要があるが、作成したユーザーがない場合、管理者ユーザーが削除を実行できます。



ピンボードを共有するには

手順

- 共有するピンボードで [その他のオプション] をクリックします。
- [共有] をクリックします。

- 3 [アクション] の下にある共有アイコンをクリックして、[ピンボード ライブラリ] からピンボードを共有することもできます。
- 4 デフォルトでは、リンク共有は有効です。ピンボードのリンクは、ログイン中のユーザーであれば誰とでも共有できます。
- 5 ピンボードを共有するユーザーを追加できます。特定のユーザーに対して、[view] や [view and edit] などの権限を指定します。

注： 表示権限のみを持つユーザーは、他のユーザーとピンボードを共有できません。

- 6 [保存] をクリックして、共有とコラボレーションの変更を保存します。
- 7 次のいずれかの方法で、ピンボードの共有とコラボレーションの情報を表示できます。
 - [ピンボード ライブラリ] にある特定のピンボードの [共有] 列で、共有情報を確認できます。
 - ウィジェットのピン アイコンをクリックします。[最近変更された項目] の下に一覧表示されているピンボードをポイントすると、所有者と共有相手に関する詳細が表示されます。

ピンボードをホーム ページとして設定するには

選択したピンボードをデフォルトのホーム ページとして設定できます。

手順

- 1 ホーム ページとして設定するピンボードに移動します。
- 2 [ピンボード オプション] をクリックします。[ホーム ページとして設定] をクリックします。

この特定のピンボードがホーム ページとして設定されます。

注： ピンボードをホーム ページとして設定すると、そのピンボードの [ホーム ページとして設定] オプションは無効になります。

- 3 [設定] の [マイ プリファレンス] 画面から、特定のピンボードをデフォルトのホーム ページとして設定することもできます。
- 4 以前のホーム ページを表示するには、左側のナビゲーション パネルにある [ピンボード] の下にある [Network Insight ホーム] をクリックします。[Network Insight ホームをホーム ページとして設定しますか?] というメッセージが表示されます。デフォルトのホーム ページに戻すには、[ホームページの設定] をクリックします。[終了] をクリックしてメッセージを閉じます。

注：

- ホーム ページとして設定したピンボードを削除すると、デフォルトのホーム ページが [Network Insight ホーム] 画面にリセットされます。削除するピンボードの所有者である場合は、削除の確認を求めるメッセージが表示されます。
 - 作成したピンボードを別のユーザーがホーム ページとして設定している場合にホーム ページを削除すると、そのユーザーの [Network Insight ホーム] に自動的に戻ります。
-

結果

ピンボードを複製するには

手順

- 1 ピンボード ライブラリのリストにある特定のピンボードについて、[アクション] の複製アイコンをクリックしま



- 2 ポップアップが表示され、ここにピンボードの名前を入力する必要があります。説明は元のピンボードと同じです。[複製] をクリックします。

注： ピンボードの名前は必須です。[複製] ボタンは、名前を入力するまで有効になりません。

- 3 共有されているピンボードを複製する場合は、ソースのピンボード ユーザーと権限を保持することを選択できます。それらを保持するには、[ソースのピンボード ユーザーと権限を保持する] を選択します。

注： 複製するピンボードが読み取り専用アクセスで共有されている場合、[ソースのピンボード ユーザーと権限を保持する] オプションは表示されません。

ピンボードを複製するユーザーは、新しいピンボードの所有者になります。

vRealize Network Insight における ロード バランサのサポート

15

ロード バランシングを使用すると、バックエンドの複数の宛先に対して受信アプリケーション トラフィック（パブリック クラウドまたはプライベート クラウドへのデプロイを含む）を分散させることができます。そのため、バックエンドの宛先のコレクションという概念を理解しておく必要があります。

vRealize Network Insight supports the following load balancing devices.

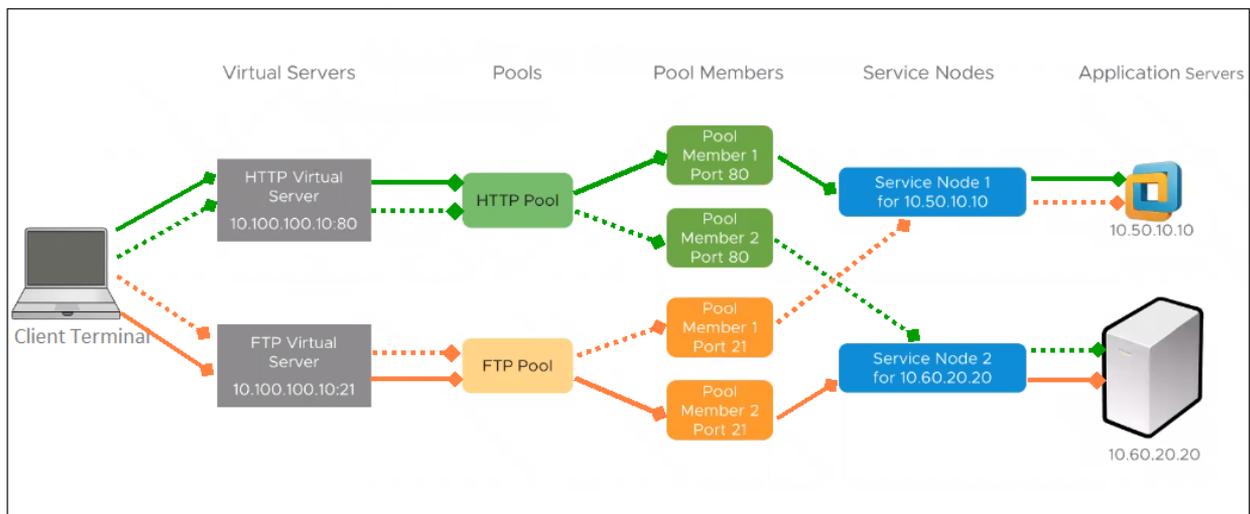
この章には、次のトピックが含まれています。

- ロード バランサとしての F5
- ロード バランサとしての NSX-V

ロード バランサとしての F5

F5 でロード バランシング機能をサポートして有効にするために、vRealize Network Insight には必要なコンポーネントやエンティティが追加されています。

F5 ロード バランサとそのコンポーネントの概要



- アプリケーション サーバ：アプリケーションがホストされるマシン。たとえば、Web サーバがある場合、サーバはアプリケーション サーバ（物理サーバまたは仮想サーバ）で実行されます。

- サービス ノード：F5 では、アプリケーション サーバがサービス ノードとして表されます。そのため、サービス ノードの IP アドレスまたは FQDN はアプリケーション サーバと同じです。各サービス ノードには複数のアプリケーションを含めることができます。
- プール メンバー：論理エンティティ。サービス ノード内の各アプリケーションは、サービス ノードと同じ IP アドレスまたは FQDN を持つプール メンバーによって表されます。各アプリケーションを識別するために、プール メンバーがサービス ノードの IP アドレスにポート番号を埋め込みます。
- プール：特定のアプリケーションを扱うすべてのプール メンバーが1つのプールとしてグループ化されます。
- 仮想サーバ：アプリケーションのパブリック側 IP アドレス。アプリケーションを使用するクライアントは、仮想サーバの IP アドレス（たとえば、10.100.100.10）とポート番号（80 または 21）に接続します。
- クライアント ターミナル：接続の開始点は仮想マシンであるクライアント ターミナルです。

クライアント要求は仮想サーバに接続され、仮想サーバによってプールに基づくプール メンバーが決定されます。次に、プール メンバーによって要求がアプリケーション サーバ（仮想マシンまたは物理サーバ）に転送されます。

注： 1つのアプリケーション サーバで、複数のポートと複数のサービス ノードからの複数の要求を処理できます。

vRealize Network Insight には、ロード バランシング機能のサポートによる次のようなメリットもあります。

- アプリケーション サーバが物理サーバか仮想マシンかを識別できます。
- アプリケーション サーバ（ホストまたは仮想マシン）の設定、パフォーマンス、フローなどの情報が提供され、問題のデバッグやトラブルシューティングを容易に行うことができます。
- 負荷が分散されているアプリケーションの物理または仮想ネットワーク ポートメントの情報が提供されます。
- 環境内の問題に関するアラートを発生させ、問題の原因の検出にも役立ちます。たとえば、サービス ノードの仮想マシンがダウンしているためアプリケーションが応答しない状況などに対応できます。
- フローの可視性をエンド ツー エンドで提供します。

ロード バランサの詳細の表示

[ロード バランサ] 画面には、ロード バランサに作成された仮想サーバおよびプールに関する情報の概要が表示されます。

表示される情報は次のとおりです。

- ロード バランサ上の仮想サーバのリストと仮想サーバの問題
- ロード バランサ上のプールのリストとプールに関連する問題
- ロード バランサに関連付けられているイベント
- さまざまな宛先 IP アドレスでのフロー、数およびフローのネットワーク トラフィックのリスト。

注： NSX-V ロード バランサについては、フロー情報がキャプチャされません。

- ベンダー、タイプ、シリアル番号、仮想サーバ、プールなどの情報を提供するロード バランサのプロパティ。

仮想サーバの詳細の表示

[仮想サーバ] 画面には、仮想サーバのメトリックと、問題および変更イベントが表示されます。

表示される情報は次のとおりです。

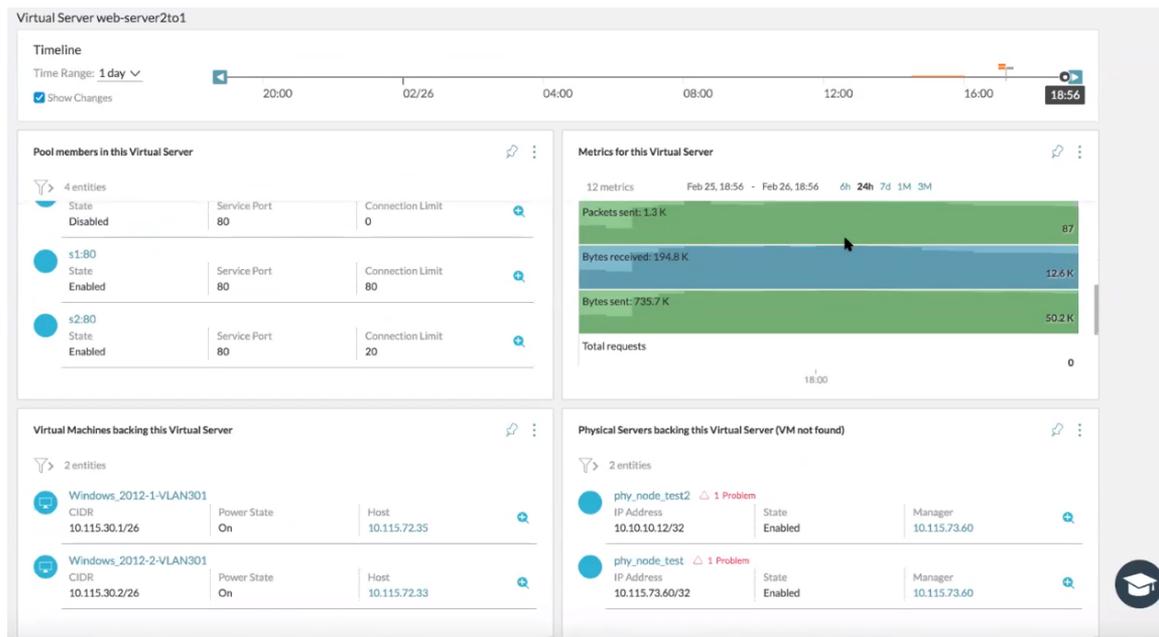
- 仮想サーバのすべてのプール メンバーのリストとその詳細、 および問題のアラート
- 仮想マシンのリスト
- 物理サーバのリスト
- 仮想サーバに関連付けられている問題イベントのリスト
- 次のような、仮想サーバに関連するメトリックのリスト。
 - 接続（数、期間）
 - ネットワーク メトリック（受信済みまたは送信済みのパケットおよびバイト数）
 - CPU 使用率

注： サポートされている NSX-V ロード バランサのメトリックのリストについては、[サポートされている NSX-V メトリック](#)を参照してください。

- 仮想サーバで使用されるプール メンバーの上位フロー

注： NSX-V ロード バランサについては、フロー情報がキャプチャされません。

- ロード バランサの IP アドレス、ネットワーク トラフィック、サービス ポートに関する情報を提供する仮想サーバのプロパティ。



ロード バランサに関連付けられているトポロジ パスを表示するには、`client VM name to Virtual server IP`、というクエリを使用できます。異なるサービス ポートに複数の仮想サーバがある場合、[宛先仮想マシンを選択] セクションにそのリストが表示されます。リストからサーバを選択し、[パスを表示] をクリックすると、仮想マシンから仮想サーバへのパスが表示されます。

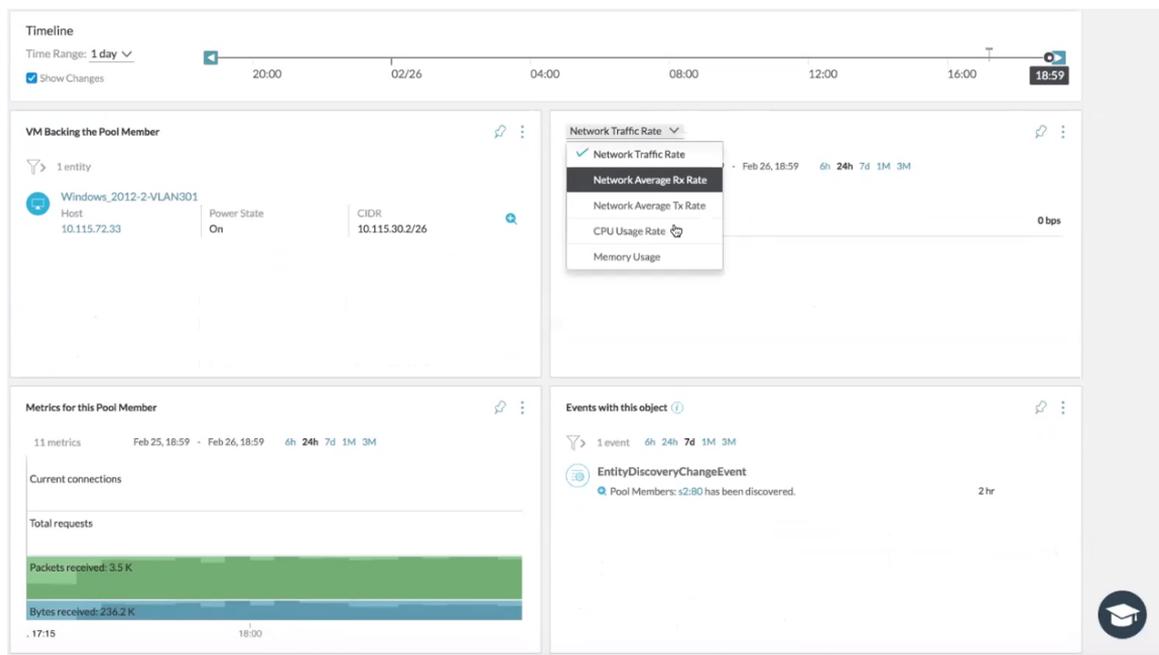
仮想マシンのパス トポロジで仮想サーバをクリックすると、[仮想サーバ] ウィンドウに一連の仮想マシンが表示されます。[パスの表示] をクリックすると、仮想サーバから選択した仮想マシンへのパスが表示されます。

プール メンバーの詳細の表示

[プール メンバー] 画面には、プール メンバー、メトリック、およびプール メンバーに関連付けられているイベントに関する情報が表示されます。

以下が表示されます。

- 仮想マシンのリストと仮想マシンに関する追加の詳細
- プール メンバーのメトリックと仮想マシンのメトリックを比較できる情報。たとえば、メモリと CPU の使用率、ネットワーク トラフィックなど。
- 次のような、プール メンバーに関連するメトリックのリスト。
 - 接続（数、期間、存続時間）
 - ネットワーク メトリック（受信済みまたは送信済みのパケットおよびバイト数）
 - CPU 使用率
- ロード バランサ、ノード、状態、サービス ポートに関する情報を提供するプール メンバーのプロパティ。



ロード バランサに関連するサンプル検索クエリ

次のサンプル クエリを使用すると、ロード バランサに関連するデータをフィルタまたは検索できます。

- `vm where lbServiceNodes is set` - 負荷が分散されているアプリケーションをホストしているすべての仮想マシンを一覧表示します。
- `vm where lbServiceNodes is set and PowerState != 'POWEREDON'` - ロード バランシングされたアプリケーションをホストしているものの、現在機能していないすべての仮想マシンを一覧表示します。
- `pool member where state = 'DISABLED'` - 無効になっているすべてのプール メンバーを表示します。
- `Count of Pool Memembers where Service Port = '80'` - ポート 80 で実行されている特定のタイプのサービスについて、すべてのプール メンバーの数を示します。
- `service node where virtual machine is not set` - アプリケーション サーバとして物理サーバを使用しているすべてのサービス ノード、または仮想マシンをホストして vRealize Network Insight に追加されていない vCenter Server を一覧表示します。

ロード バランサとしての NSX-V

4.2 リリース以降、vRealize Network Insight では NSX-V のロード バランシング機能を利用できます。

現在サポートされているメトリックのリストは次のとおりです。

- 仮想サーバ
 - 受信したバイト数の合計
 - 送信したバイト数の合計
 - 現在のセッション数
 - 合計セッション数
- プール
 - 受信したバイト数の合計
 - 送信したバイト数の合計
 - 現在の接続数
 - 最大接続数
 - 合計接続数

現在、vRealize Network Insight でプール メンバーとしてサポートされているのは仮想マシンのみです。

ネットワークの可視性

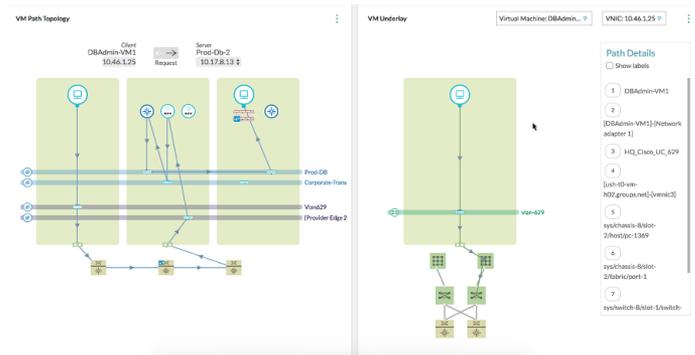
16

この章には、次のトピックが含まれています。

- パス トポロジ
- BGP ネイバーの詳細の表示
- インターネットへのパス

パス トポロジ

パス トポロジは、環境内にある任意の 2 台の仮想マシン間の接続を詳細に表示します。



トポロジには、レイヤー 3 とレイヤー 2 の両方のコンポーネントが関与します。このトポロジは、`vm_name_1` から `vm_name_2` の検索クエリを使用して表示できます。パスがある場合は、仮想マシン間パスの視覚化により、`vm_name_1` と `vm_name_2` の間のすべてのコンポーネントがポップアップされ、アニメーション化されたパスが描画されます。ルーターが物理の場合、それらのルーターは境界の外に表示されます。

パス トポロジでは、送信元と宛先間の仮想マシン間パスが表示されます。仮想マシン間にデフォルトのパスが設定されていない場合、パスが定義されていない、またはルーター インターフェイスが見つからないことを通知するエラーメッセージが表示されます。

Kubernetes の場合、次のシナリオでパス トポロジにパスが表示されます。

- Kubernetes サービスと Kubernetes サービスの間
- Kubernetes サービスと Kubernetes ポッドの間

■ Kubernetes ポッドと Kubernetete ポッドの間

注： 物理デバイスを含むパスはサポートされません。

[ロード バランサを介したパス] オプションには、選択した送信元仮想マシンと宛先仮想マシンのパスの間で使用されるすべてのロード バランサが一覧表示されます。特定のロード バランサを介した仮想マシン間パスを表示するには、リストからロード バランサの名前を選択します。パス トポロジのロード バランサ コンポーネントの上にマウスを置くと、次の詳細が表示されます。

- 仮想サーバ名
- ロード バランサ IP アドレス
- ポート番号
- ロード バランサのアルゴリズム
- ロード バランサから取得されたデフォルト ゲートウェイ

ルーティング コンポーネントをパス トポロジで確認することもできます。

パスに関係するルーター、エッジ、または LDR にマウスを置くと、完全なルーティングまたは NAT の情報が表示されます。

仮想マシン パス トポロジの右側にある仮想マシンのアンダーレイ セクションには、関連する仮想マシンのアンダーレイ情報と、関連するラック スイッチおよびポートの上部への接続が表示されます。Kubernetes エンティティの場合は、仮想マシンのアンダーレイに、ポッドが配置されている仮想マシンまたは Kubernetes ノードの情報が表示されます。

仮想マシンのアンダーレイ セクションでは、コンポーネントがラベル付けされます ([ラベルを表示] ([パスの詳細] の下) を選択した場合)。このセクションでは、上部のドロップダウン リストに、エンドポイントの仮想マシンと、エッジのアクティブな仮想マシンが表示されます。各エッジ仮想マシンについて、隣接するドロップダウン リストに入力方向と出力方向のインターフェイス IP アドレスが表示されます。選択内容に基づいて、その特定のインターフェイスのアンダーレイ パスが表示されます。

また、トポロジ マップ上部の矢印を使用して、パスの方向を反転することもできます。

トポロジ マップを使用すると、仮想マシン間パスに含まれるポートに関する可視性を高めることができます。[パスの詳細] セクションには、実際のポート チャネルの名前が表示されます。

注： 物理フロントでレイヤー 2 を完全に可視化することはできません。あるスイッチから別のスイッチにパケットが移動している場合は、複数のスイッチが関与している可能性があります。ただし、トポロジには、アンダーレイ ネットワークのスイッチは表示されません。

AWS 仮想マシン間パス

AWS の仮想マシン間パスは、オンプレミスの仮想マシンと AWS EC2 インスタンスとの間のパスの可視性を提供します。

現在、vRealize Network Insight は次のシナリオをサポートしています。

- AWS VPC 内の仮想マシン間パス：このシナリオでは、特定の VPC における、同一サブネット内の仮想マシン間、または異なるサブネットにある仮想マシン間での通信が関与します。

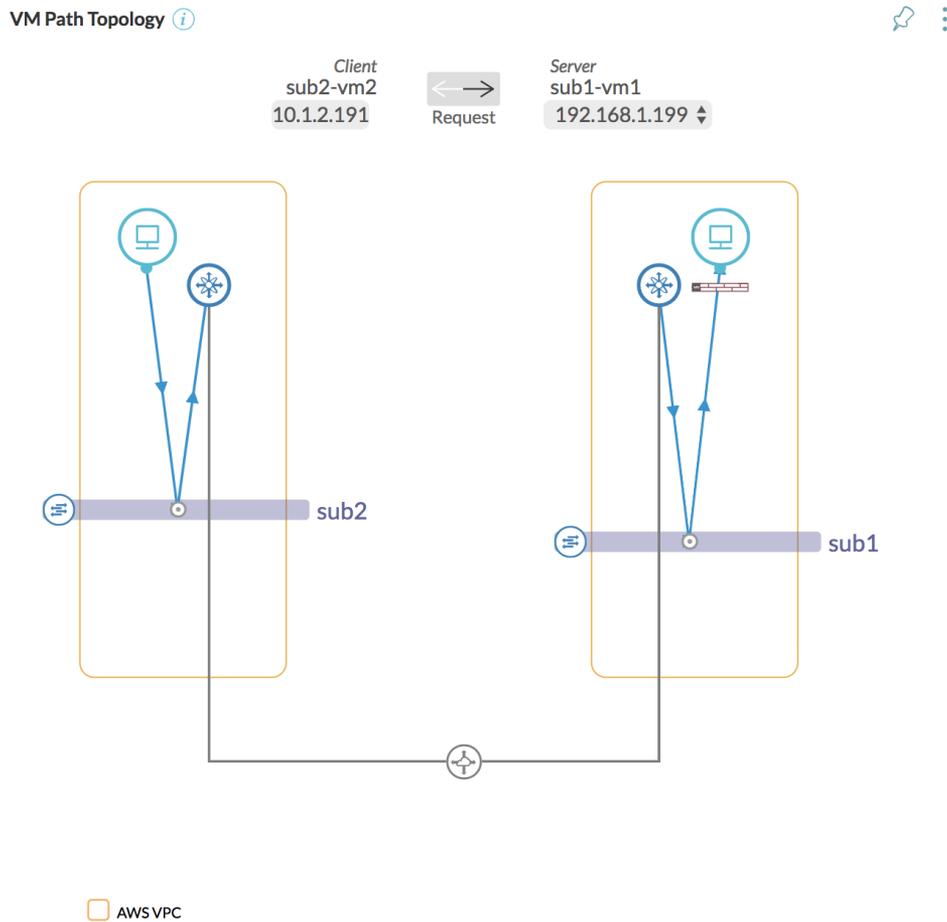
- ピア接続を介した AWS VPC 間の仮想マシン間パス：このシナリオでは、1 台の VPC の仮想マシンと、ピア接続を介した別の VPC の仮想マシンとの間の通信が関与します。
- AWS 仮想マシンからインターネットへの通信：VPC の仮想マシンが、インターネット ゲートウェイを介してインターネットに通信します。
- AWS 仮想マシンからデータセンター仮想マシンへの AWS VPN 接続を介した通信：このシナリオでは、VPC 内の仮想マシンが、AWS VPN 接続を介して、データセンター内の仮想マシンに通信します。vRealize Network Insight は、このシナリオで Software-Defined Data Center (SDDC)、NSX-V データセンター、および NSX-T データセンターをサポートします。

注：

- NSX-T および NSX-V データセンターへのハイブリッドパス トポロジは、NSX-T および NSX-V の Edge ルーターがパブリック IP アドレスを使用して設定されている場合のみ機能します。
- vRealize Network Insight は、AWS の仮想マシン アンダーレイ トポロジをサポートしていません。

注：

ピア接続を介した AWS VPC 間の仮想マシン間パスの AWS 仮想マシン間パスの例は次のとおりです。



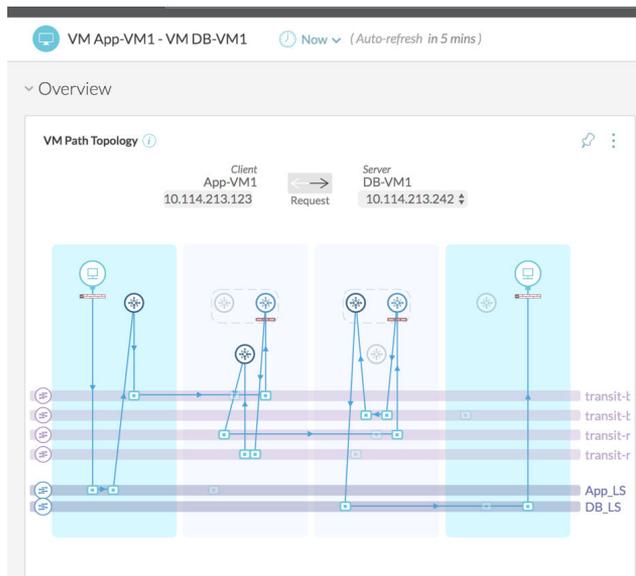
仮想マシン間パス内のアイコンをポイントすると、ピア接続のプロパティを表示できます。

AWS 仮想マシン間パスに関する次のエンティティを検索できます。

- AWS Subnet
- AWS Route Table
- AWS Virtual Private Gateway
- AWS Internet Gateway
- AWS VPN Connection
- AWS VPC Peering Connection

NSX-T

NSX-T の仮想マシン間パスの例を次に示します。



青色はホスト ノードを表し、灰色はエッジ ノードを表します。仮想マシン パス トポロジで使用されるアイコンは、画面の右側の [パスの詳細] の下に、ラベルとともに表示されます。分散ルーターは、その階層に関係なく同じ色で表示されます。トポロジ図内のサービス ルーターの色は、関連付けられている階層によって変わります。階層 1 の全コンポーネントは同じレベルに表示され、階層 0 の全コンポーネントは別のレベルに表示されます。NSX-T では、Edge ファイアウォールが図に示されています。

NSX-T ネットワークのセキュリティを計画するには、範囲として [NSX-T レイヤー 2 ネットワーク] を選択し、次のクエリを使用します。

```
plan NSX-T Layer2 Network '<NAME_OF_NSX_T_LOGICAL_SEGMENT>'
```

次の手順を実行すると、同じ結果を得ることができます。

- ナビゲーション サイド バーから [セキュリティ] を選択します。

- ドロップダウン メニューから [NSX-T レイヤー 2 ネットワーク] を範囲として選択します。

注：

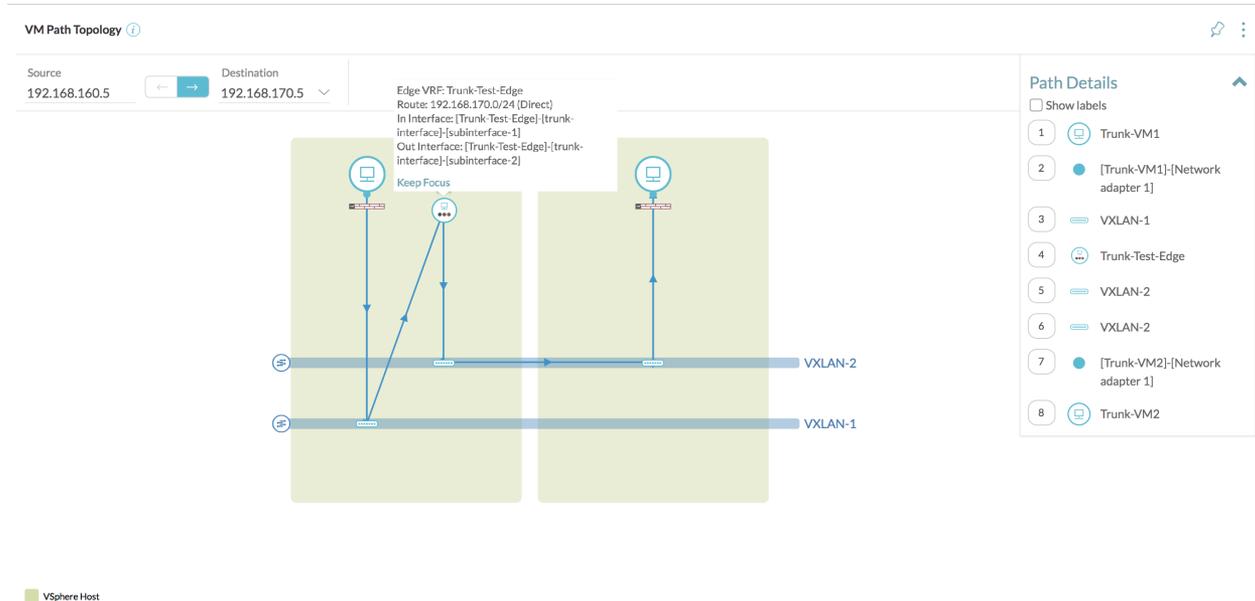
- 範囲では [NSX-T L2 ネットワーク] や [タグ] などの NSX-T に関連するエンティティを使用できます。NSX-T に関連するこれらのエンティティは、計画、マイクロセグメンテーション、およびアプリケーション定義で使用できます。
- [グループ別] ドロップダウン メニューでは、[NSX-T セキュリティ グループ] は [セキュリティ タグ] の一部であり、[論理セグメント] は [VLAN/VXLAN] の一部です。

NSX-V Edge トランク インターフェイスの仮想マシン間パス

vRealize Network Insight では、DVPG が NSX Edge のトランク vNIC に接続されていて、サブ インターフェイスが VLAN または VXLAN に接続されている場合に、仮想マシン間パスおよび仮想マシンとインターネットの間のパスを表示できます。

次に、NSX Edge を使用した仮想マシン間パスの例を示します。

注： vRealize Network Insight は Edge 仮想マシンのトランク インターフェイスのアンダーレイ情報をサポートしていません。



vRealize Network Insight での NAT のサポート

vRealize Network Insight は NSX for vSphere、NSX-T Edge、Fortinet、および Check Point の仮想マシン間パスをサポートしています。

仮想マシン間パス

NAT を介した仮想マシン間パスの例を以下に示します。

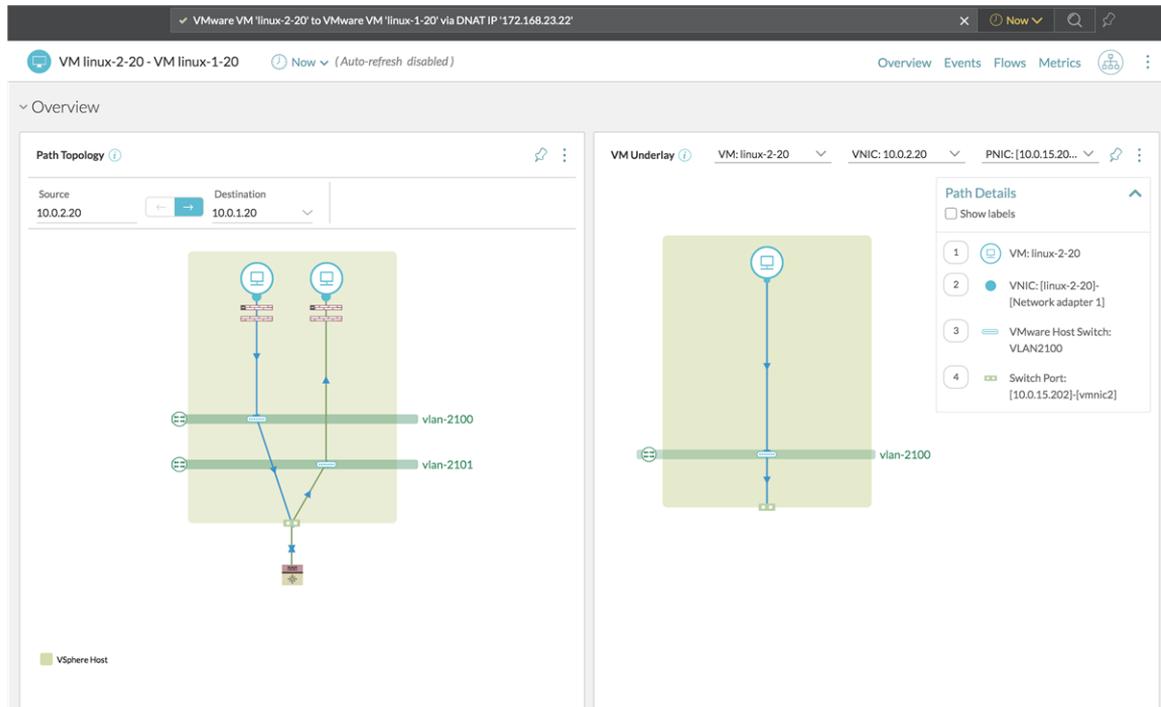
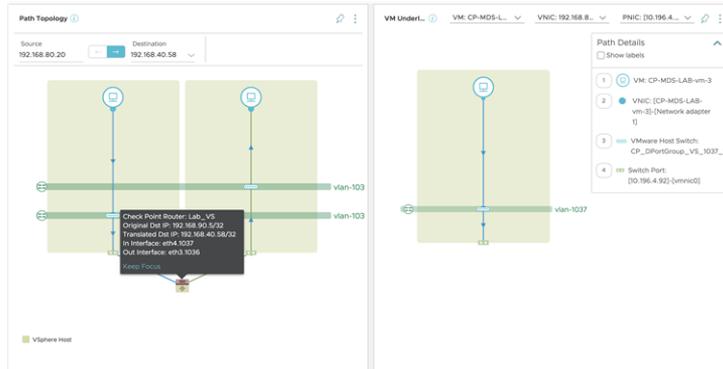


図 16-1. Check Point NAT を介した仮想マシン間パス



クエリ

NAT を介した仮想マシン間パスを表示するには、次のクエリを使用します。

- 宛先の仮想マシンが Fortinet および Check Point ルーターの背後にあり、NAT で構成されている場合は、VMware VM '<name of the VM>' to VMware VM '<name of the VM>' via DNAT クエリを使用します。
- 宛先の仮想マシンが NSX for vSphere または NSX-T Edge の背後にあり、NAT が構成されている場合は、VMware VM '<name of the VM>' to VMware VM '<name of the VM>' クエリを使用します。

考慮事項

- NAT サービスが有効になっている NSX-T 論理ルーターを使用した仮想マシン間パスの場合、vRealize Network Insight は、これらのパスについての NSX-T Edge ファイアウォール ルールを適切に表示しません。

VMware SD-WAN の仮想マシン間パス

vRealize Network Insight では、VMware SD-WAN 環境の仮想マシン間パスを表示できます。

vRealize Network Insight は次のシナリオをサポートしています。

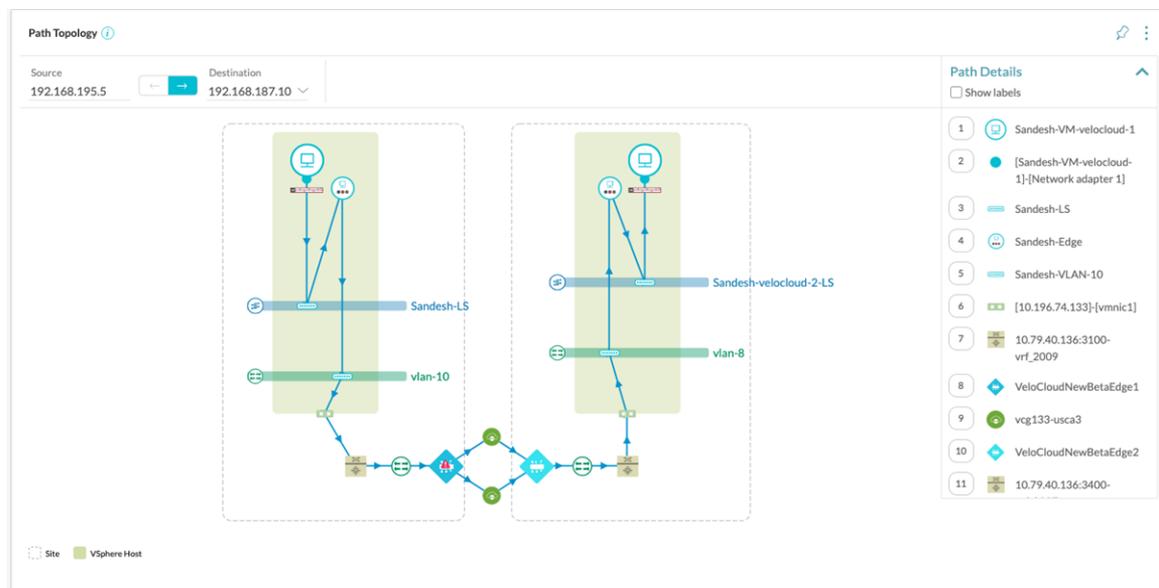
- IP アドレス間のパス：両方の IP アドレスを VMware SD-WAN Edge の背後の VLAN に直接配置する必要があります。
- IP アドレスからインターネット/IP アドレスから不明な IP アドレス：送信元 IP アドレスを VMware SD-WAN Edge の背後の VLAN に直接配置する必要があります。

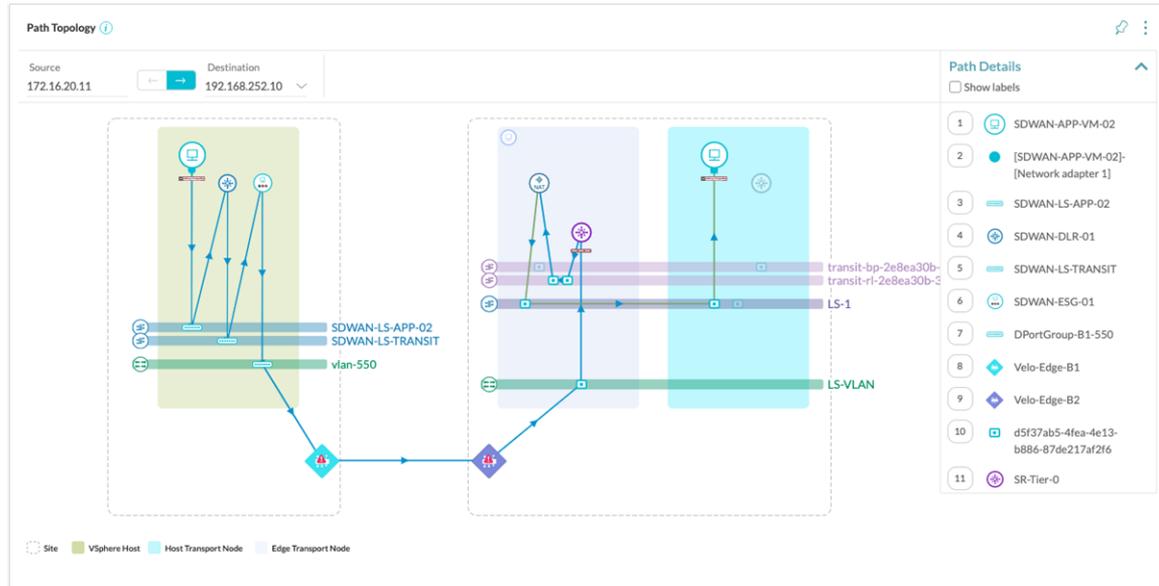
注： インターネット IP アドレスまたは不明な IP アドレスは、vRealize Network Insight で検出されない IP アドレスです。

- 仮想マシンから IP アドレス、IP アドレスから仮想マシン、または仮想マシン間のパス：
 - サポートされるのは、NSX/NSX-T データセンター内の仮想マシンのみです。VMware Cloud on AWS、Amazon Web Services、Azure 内の仮想マシンはサポートされません。
 - VMware SD-WAN Edge は、VLAN を介してデータセンター内の物理/仮想ルーターに接続する必要があります。
- **注：** ソース VMware SD-WAN Edge とターゲット VMware SD-WAN Edge に設定された VMware SD-WAN Gateway が異なる場合は、ソース VMware SD-WAN Edge のゲートウェイ経由でパスが表示されます。

VMware SD-WAN Edge 間のブランチとブランチを接続する VPN が VMware SD-WAN クラスタを経由する場合、このクラスタのすべてのメンバーがパスに表示されます。

次に、VMware SD-WAN の仮想マシン間パスの例をいくつか示します。





Arista ハードウェア VTEP 仮想マシン間パス

vRealize Network Insight では、仮想マシン間パスにハードウェア VTEP を表示できます。

現在、vRealize Network Insight は次のシナリオをサポートしています。

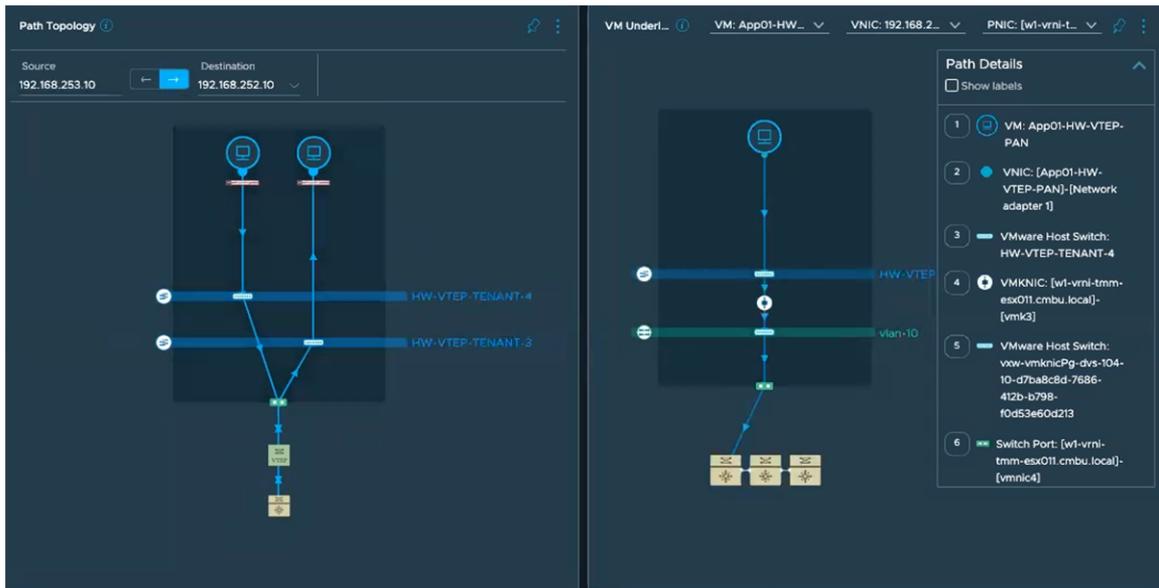
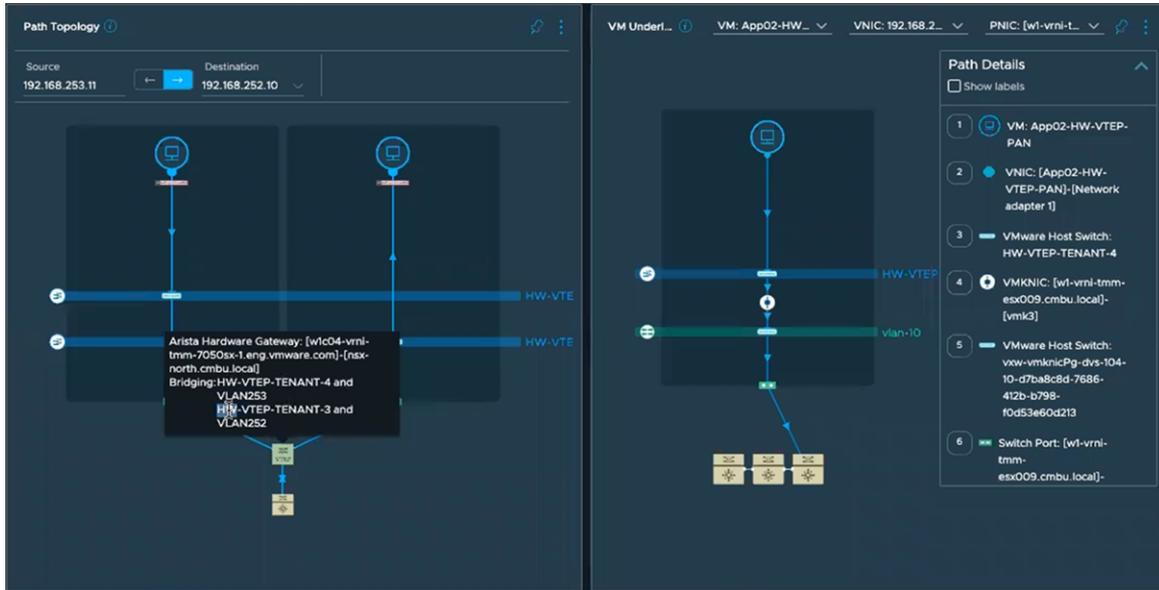
- 送信元仮想マシンと宛先仮想マシンが異なる VXLAN および異なるホストに配置されている場合の、ハードウェア VTEP を経由する仮想マシン間パス。
- 送信元仮想マシンと宛先仮想マシンが同じホストで異なる VXLAN に配置されている場合の、ハードウェア VTEP を経由する仮想マシン間パス。
- スイッチがホストに直接接続されている場合の、仮想マシンのアンダーレイ トポロジ内にあるハードウェア VTEP。

注： Arista スイッチ SSH をデータ ソースとして vRealize Network Insight に追加する場合は、Arista スイッチの SSH を設定するために VMware NSX Manager を使用したときと同じ IP/FQDN を使用する必要があります。そうしないと、仮想マシン間パスにハードウェア VTEP が表示されません。

また、仮想マシンとインターネットの間でハードウェア VTEP が使用可能な場合は、仮想マシン トポロジ、および仮想マシンからインターネットへのパスにもハードウェア VTEP を表示できます。

送信元仮想マシンと宛先仮想マシンが同じ VXLAN に配置されている場合、ハードウェア VTEP 経由の仮想マシン間パスはサポートされません。

ハードウェア VTEP を経由する仮想マシン間パスの例を以下に示します。



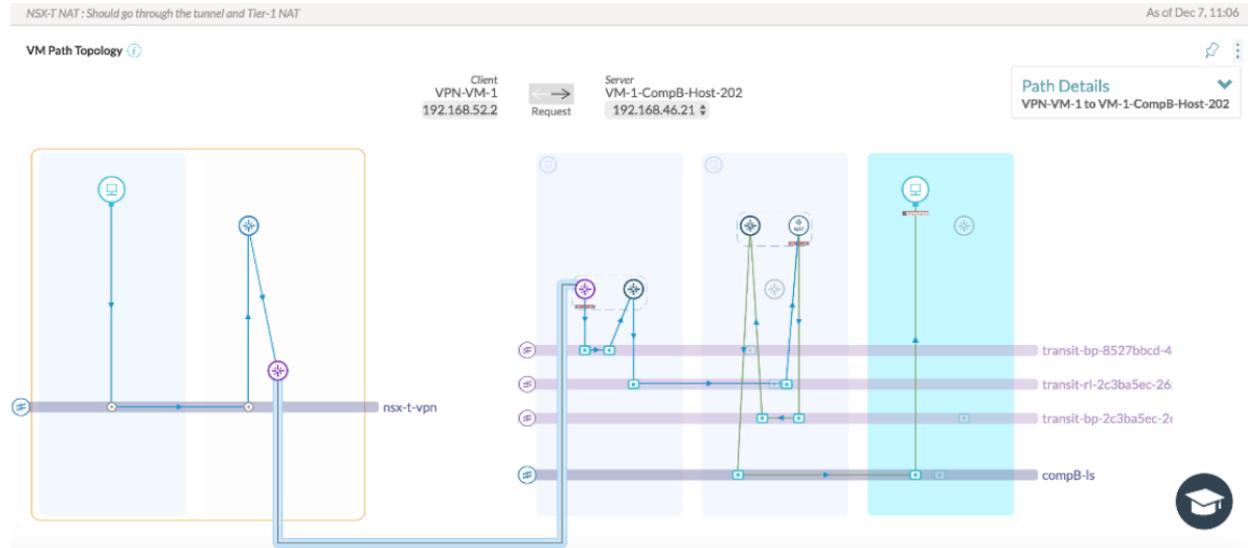
VMware Cloud on AWS : 仮想マシン間パス

vRealize Network Insight は、VMware Cloud on AWS で次のハイブリッドパスをサポートしています。

- VMware Cloud on AWS および VMware Cloud on AWS
- VMware Cloud on AWS および NSX-T
- VMware Cloud on AWS および NSX-V
- VMware Cloud on AWS および AWS
- VMware Cloud on AWS 内部

VMware Cloud on AWS 内のどの仮想マシンについても、アンダーレイ情報が表示されるのは、仮想マシンがあるセグメントまでです。これは、ネットワークの基盤となる物理要素が VMware Cloud on AWS で抽象化され、そのレベルでは可視性がないためです。

次に示すのは、VMware Cloud on AWS および NSX-T の仮想マシン間パスの例です。



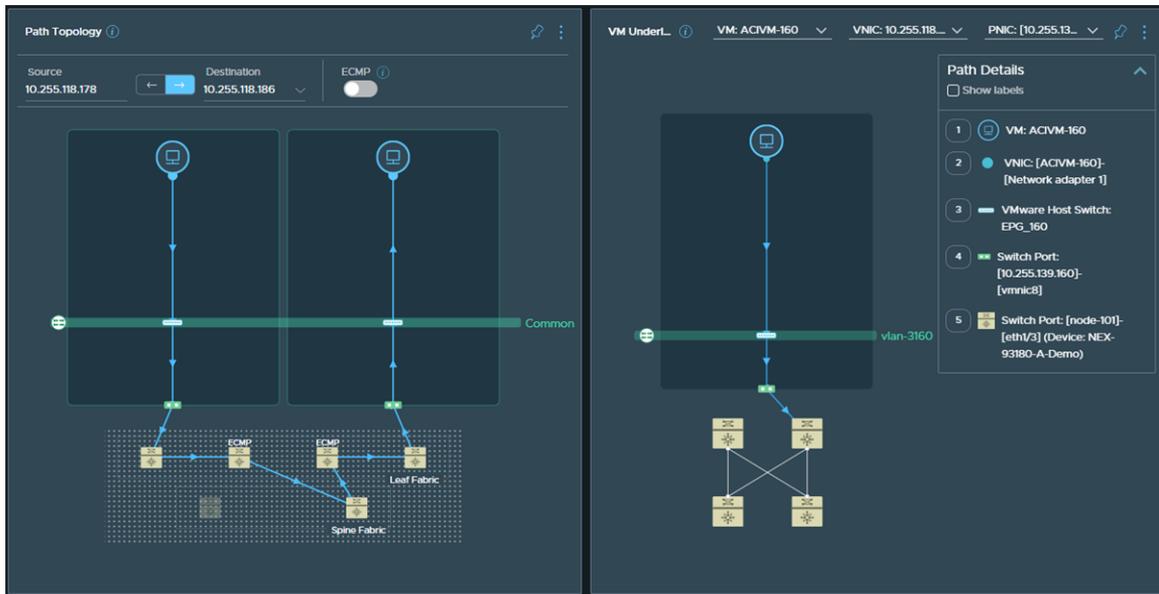
暗い青色の線はトンネルを示しています。

Cisco ACI 仮想マシン間のパス

vRealize Network Insight では、Cisco ACI を経由する仮想マシン間パスを表示できます。

Cisco ACI での仮想マシン間パスの例は、次のとおりです。

注： Cisco ACI API でスイッチ レベルの詳細が提供されている場合、vRealize Network Insight では、リーフおよびスパインのスイッチを経由する仮想マシンのパスが示されます。そうでない場合、vRealize Network Insight では、仮想マシン間パス上にあるリーフおよびスパインのスイッチではなく、ファブリック全体に対応する 1 つの Cisco ACI VRF が示されます。

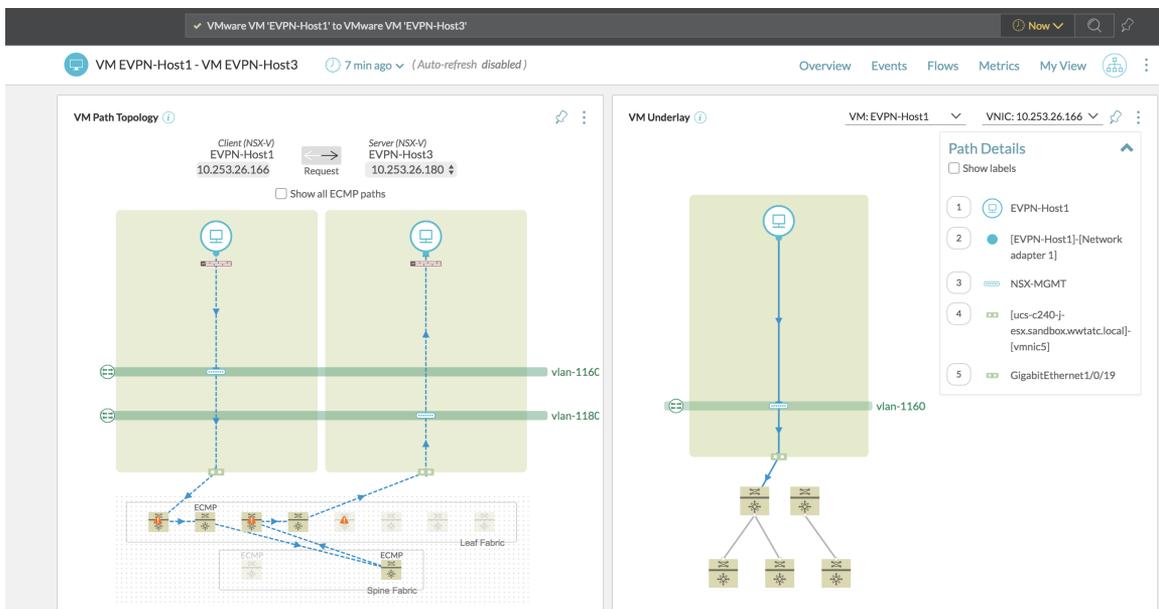


Cisco BGP-EVPN モードのサポート

vRealize Network Insight は、Enterprise エディション限定の Cisco BGP-EVPN 設定モードで設定された Cisco 9000 スイッチのファブリックをサポートします。vRealize Network Insight は、Cisco BGP-EVPN 構成を使用した Cisco Nexus 9000 以外のスイッチ モデルはサポートしていません。

ファブリックの一部である各 Cisco Nexus 9000 スイッチは、データ ソースとして個別に追加されます。ファブリック内のすべてのスパインまたはリーフスイッチを表示するには、switches where role is set クエリを使用します。

Cisco BGP-EVPN モードのサンプルの仮想マシン間パスは次のとおりです。

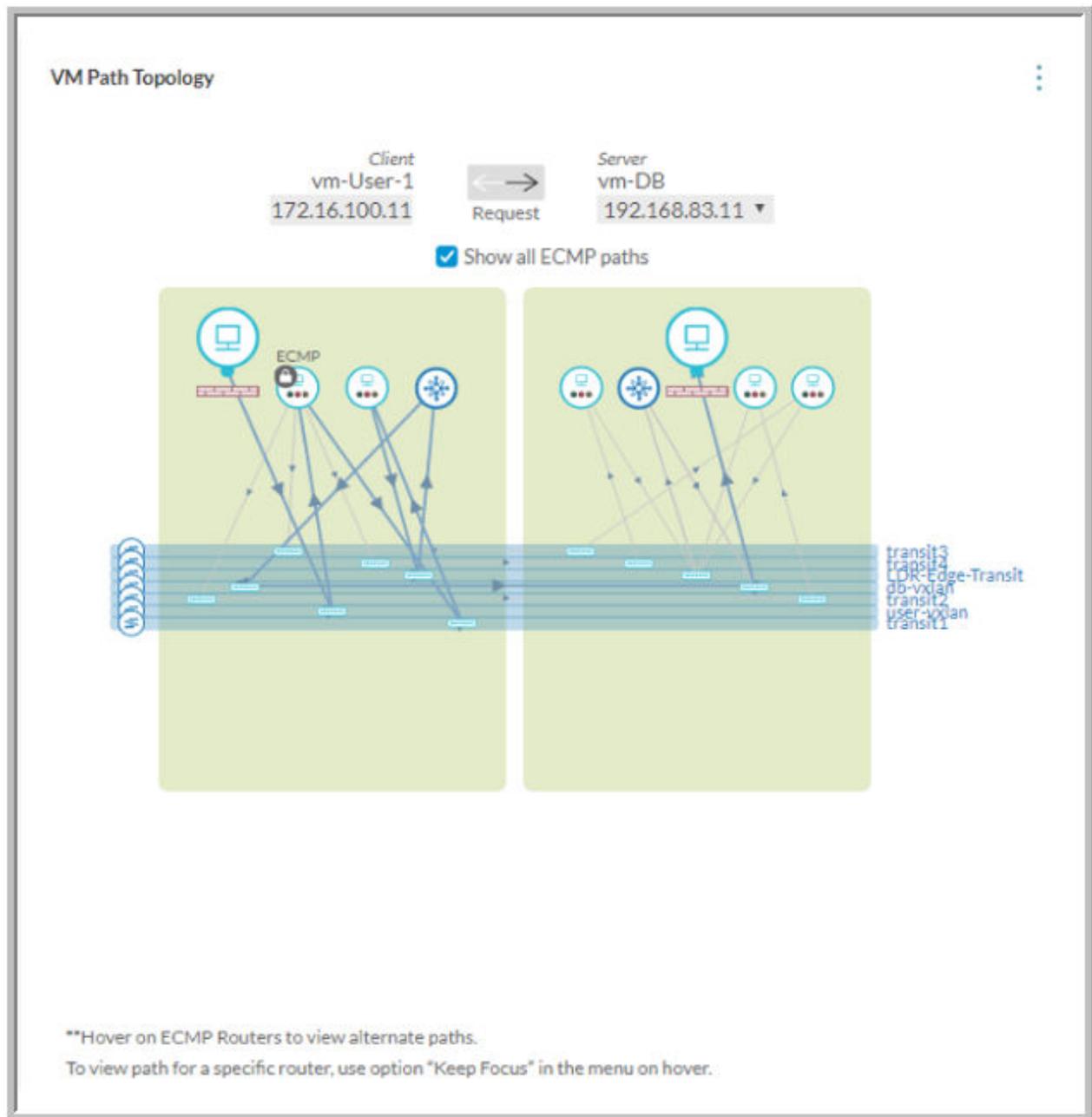


イコールコスト マルチパス (ECMP) ルートのサポート

vRealize Network Insight は、仮想マシン間パスで ECMP をサポートします。

仮想マシン間パスには、ECMP に関する次の情報が表示されます。

- ソースからターゲットへの複数の ECMP パス
- ECMP が発生するルーター
- 指定されたルーター (VRF) について可能な送信パス
- 可能なパスのルート



前の図では、ECMP が有効なルーターを確認できます。これらをポイントすると、追加のパスが表示されます。また、要件に基づいてルーターを選択し、ロックすることで、パスを作成できます。2 台の仮想マシン間のすべての ECMP パスを表示する場合は、トポロジ図で [すべての ECMP パスの表示] オプションを選択します。

特定のルーターのパスを表示する場合は、ルーターをポイントし、[フォーカスを維持] をクリックします。ルーター固有のパスが表示されます。

L2 ブリッジのサポート

L2 または VLAN ブリッジは、複数の VLAN から 1 つのブロードキャスト ドメインを作成します。以前のリリースでは、仮想マシン間パスに 2 つ以上の VLAN 間の L2 ブリッジが関与している場合、仮想マシン間パスは機能しませんでした。このリリース以降、vRealize Network Insight は L2 ブリッジをサポートするようになりました。現在、この機能は Cisco ASA ルーターでのみサポートされています。

BGP ネイバーの詳細の表示

BGP ネイバーに関するさまざまな情報は、vRealize Network Insight で表示できます。NSX Edge または論理ルーターの BGP ネイバーを表示できます。

手順

- 1 検索バーに Router where bgp= 'Disabled' と入力し、[Enter] キーを押します。
- 2 リストから特定のルーターを展開して詳細を表示します。

NSX-V では、BGP ネイバーの次の情報を表示できます。

- IP Address
- Remote AS
- Weight
- Keep Alive Time
- Hold Down Time
- Status

NSX-T では、BGP ネイバーの次の情報を表示できます。

- IP Address
- Remote AS
- Keep Alive Time
- Hold Down Time

- Status

注：

- ネイバーに関する情報が取得されない場合、Status は Unknown として表示されます。
 - Status が Established.up でない場合、そのエッジの One or more BGP neighbours are not in established state イベントが発生します。このイベントは、problems を検索した場合も表示できません。
-

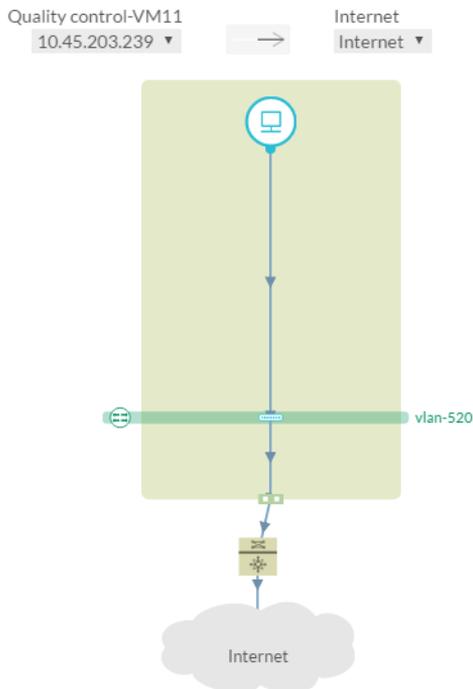
- 3 (オプション) BGP ステータスが無効になっているルーターを表示するには、Router where bgp='Disabled' を検索します。

インターネットへのパス

環境内の各仮想マシンについて、vRealize Network Insight は、[インターネットへのパス] ピン内のアニメーション化されたパスを使用して、仮想マシンをインターネットに接続する方法を示します。

パスによって、仮想マシンとインターネット間のすべてのコンポーネント（仮想および物理）が設定されます。シーケンス内の各コンポーネントを接続する、アニメーション化されたパスが描画されます。パスの方向は、表示の上にある矢印を使用して逆向きにもできます。

エンティティのアイコンにマウス ポインタをポイントすると、アドレス指定可能な名前が表示されます。パスのアイコンをクリックすると、そのプライマリ属性の要約されたアカウントが表示されます。ピンを最大化して、パスの詳細を表示することもできます。



この章には、次のトピックが含まれています。

- Cross-vCenter NSX
- Palo Alto Networks
- Cisco ASA ファイアウォール
- Check Point ファイアウォール
- セキュリティ グループ
- ポリシーベース VPN
- NSX 分散ファイアウォールの非アクティブ ルール
- Fortinet ファイアウォール

Cross-vCenter NSX

Cross-vCenter NSX 環境では、複数の vCenter Server を設定できます。各 vCenter Server は、それぞれの NSX Manager とペアリングされている必要があります。

1 つの NSX Manager にプライマリ NSX Manager のロールが割り当てられ、その他の NSX Manager にセカンダリ NSX Manager のロールが割り当てられます。プライマリ NSX Manager は、Cross-vCenter NSX 環境の制御プレーンを提供するユニバーサル コントローラ クラスタの展開に使用されます。セカンダリ NSX Manager には、独自のコントローラ クラスタはありません。プライマリ NSX Manager は、ユニバーサル論理スイッチなどのユニバーサル オブジェクトを作成できます。これらのオブジェクトは、NSX ユニバーサル同期サービスによってセカンダリ NSX Manager に同期されます。セカンダリ NSX Manager では、これらのオブジェクトを表示できますが、編集することはできません。ユニバーサル オブジェクトを管理するには、プライマリ NSX Manager を使用する必要があります。プライマリ NSX Manager を使用して、環境内の任意のセカンダリ NSX Manager を設定できます。

次のユニバーサル オブジェクトがサポートされています。

- ユニバーサル LDR
- ユニバーサル トランスポート ゾーン
- ユニバーサル論理スイッチ
- ユニバーサル ファイアウォール ルール

- ユニバーサル セキュリティ グループ
- ユニバーサル IPSet
- ユニバーサル サービス
- ユニバーサル サービス グループ
- ユニバーサル セグメント範囲

Palo Alto Networks

vRealize Network Insight は Palo Alto Panorama ファイアウォールをサポートしています。

注： vRealize Network Insight は、複数の NSX Manager との Palo Alto Panorama 統合をサポートしていません。

vRealize Network Insight に Palo Alto Panorama を追加するには、Palo Alto Networks のユーザーに、XML API アクセス権限を持つ管理者ロールが必要です。[Palo Alto Networks] ユーザー インターフェイスで、次の手順を実行して XML API の管理者ロールを追加します。

- 1 [Panorama] - [管理者ロール] の順に選択します。
- 2 [追加] をクリックして新しい管理者ロールを追加します。
- 3 [管理者ロール プロファイル] ウィンドウが開きます。
- 4 ロールに名前を入力し、[Panorama] を選択します。
- 5 [Web ユーザー インターフェイス] タブをクリックし、すべてのエントリを無効にします。
- 6 [XML API] タブをクリックし、[設定] と [操作要求] を除くすべてのエントリを無効にします。
- 7 [OK] をクリックしてウィンドウを閉じます。

新しい管理者ロールがリストに表示されます。

- 8 [コミット] をクリックします。
- 9 このロールを管理者アカウントに割り当てるか、新しいユーザーを作成して、このロールを新しいユーザーに割り当てます。

vRealize Network Insight でサポートされている Palo Alto Networks の機能は次のとおりです。

- Palo Alto と NSX エンティティの相互関係：Palo Alto Networks のアドレスとアドレス グループの仮想マシン メンバーシップは、IP アドレスと仮想マシンのマッピングに基づいて計算されます。このメンバーシップ情報は、次のように照会できます。
 - `VM where Address = <>`
 - `Palo Alto address where vm = <>`
 - `VM where Address Group = <>`
 - `Palo Alto address group where vm = <>`

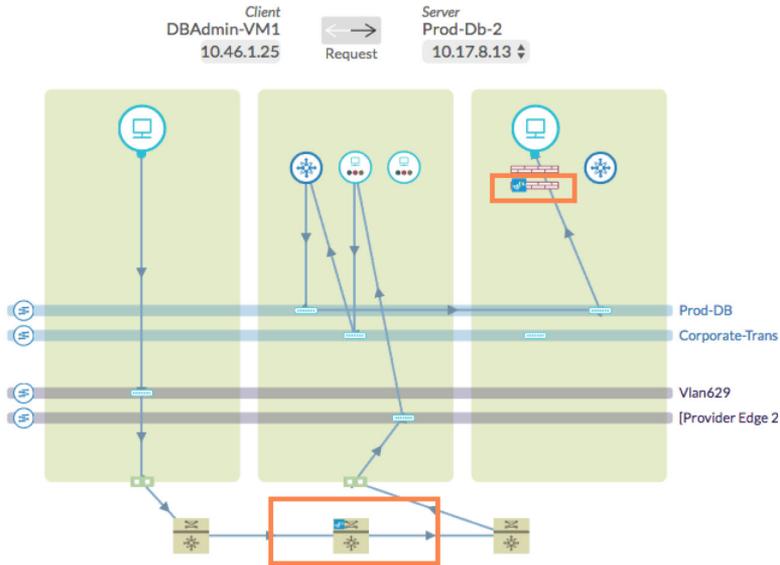
- クエリ：vRealize Network Insight でサポートされるすべての Palo Alto エンティティに対してクエリを実行できます。すべてのエンティティには、Palo Alto というプリフィックスが付きます。クエリの一部を次に示します。

表 17-1.

エンティティ	クエリ
Palo Alto アドレス	Palo Alto address where vm = <> VM where Address = <>
Palo Alto アドレス グループ	Palo Alto address group where Translated VMs = <> VM where address group = <>
Palo Alto デバイス	Palo Alto Device where Version = <> Palo Alto Device where connected = true Palo Alto Device where family = 'PA-5060'
Palo Alto 物理デバイス	Palo Alto Physical Device where model = 'PA-5060'
Palo Alto 仮想マシン デバイス	Palo Alto VM Device where model = 'PA-VM'
Palo Alto デバイス グループ	Palo Alto Device Group where device = <> Palo Alto Device Group where address = <> Palo Alto Device Group where address group = <>
Palo Alto サービス	Palo Alto service where Port = <> Palo Alto service where Protocol = <>
Palo Alto サービス グループ	Palo Alto service group where Member = <>
Palo Alto ポリシー	Palo Alto Policy where Source vm = <> and Destination vm = <> Palo Alto Policy where Source IP = <> and Destination IP = <>
Palo Alto ファイアウォール	Palo Alto firewall where Rule = <>
Palo Alto ゾーン	Palo Alto Zone where device = <>
Palo Alto 仮想システム	Palo Alto Virtual System where Device = <> Palo Alto Virtual System where Device Group = <>

注： クエリ以外にも、ファセットを使用して検索結果を分析できます。

- 仮想マシン間パス：仮想マシン-仮想マシンのトポロジの一環として、vRealize Network Insight は、ホストの Palo Alto VM-Series ファイアウォールを表示します。該当するルールは、ファイアウォールアイコンをクリックすると表示されます。Palo Alto Networks のファイアウォール デバイス（ルーティング デバイス）もパスに含まれている場合は、そのデバイスも表示されます。デバイスアイコンをクリックすると、ルーティング テーブル、インターフェイス、適用されているファイアウォール ルールを含むテーブルなどの基本的な情報を確認できます。



- Palo Alto Networks の次のシナリオに関連するいくつかのシステムイベントを確認できます。
 - Palo Alto デバイスが Panorama (マネージャ) に接続されていない
 - NSX Manager が Panorama に登録されていない
 - NSX ファブリック エージェントが Palo Alto 用 ESX デバイスに見つからない
 - Palo Alto デバイスが NSX ファブリック エージェント用 Panorama に見つからない
 - セキュリティ グループ メンバーシップ データが同期していない
- 指定した NSX Manager を使用して、複数のサービス定義を Panorama に作成し、登録できます。異なる ESXi クラスタに、トラフィックをそれぞれ別の方法で処理するための VM-Series ファイアウォールを必要とするワークロードがある場合、複数のサービス定義が作成されます。各サービス定義には、関連付けられたデバイス グループがあり、ここからポリシーが選択されます。vRealize Network Insight で仮想マシン間パスを表示している間は、仮想マシンのクラスタ情報に基づく正しいポリシー セットを考慮する必要があります。

Palo Alto Manager ダッシュボードの例

Timeline

Time Range: 1 day

Show Changes

12:00 16:00 20:00 10/26 04:00 8:28

Properties

Name	10.16.128.200
NSX Manager	10.16.128.170
Device Group (NSX)	PAN_VM_Series_Device_G...
Last Dynamic Update with NSX	Mar 29, 16:57
FQDN	10.16.128.200

Palo Alto Checklist Rules - All

#	Rule
1	Palo Alto Panorama not registered with NSX Manager
2	Panorama dynamic membership definition update delayed
3	Palo Alto service VM not connected to Panorama
4	Palo Alto service VM not found on host
5	Palo Alto Service Device view mismatch with NSX

Events with this object

19 events 6h 24h 7d 1M 3M

- Panorama dynamic membership definition update delayed**
Panorama dynamic membership definition update from ... 63 days
- Palo Alto service VM not connected to Panorama (2 events - Show all)**
A service VM or device for Palo Alto Networks is in a not connect... 65 days
- NSX Fabric Agent not found on Host (9 events - Show all)**
Security Fabric Agent not reported by NSX for a Host where as L... 65 days
- Service VM's status mismatched between Panorama and NSX Manager**

Palo Alto Virtual Devices

16 entities

IP	Manager	Device Family	Name
10.16.128.13	10.16.128.200	VM	10.16.128.13
10.16.128.14	10.16.128.200	VM	10.16.128.14
10.8.201.3	10.16.128.200	VM	10.8.201.3

Palo Alto Physical Devices

1 entity

IP	Manager	Device Family	Name
10.16.21.2	10.16.128.200	PA-5060	10.16.21.2

Clusters prepared for Palo Alto services

4 entities

Cluster Name	Num Hosts	Number of Datastores	Vendor ID
ddc-pod2-compute1	9	5	domain-c11610
ddc-pod2-compute2	4	4	domain-c8791
pod2-compute1	16	117	domain-c376

Hosts deployed with Palo Alto Device

17 entities

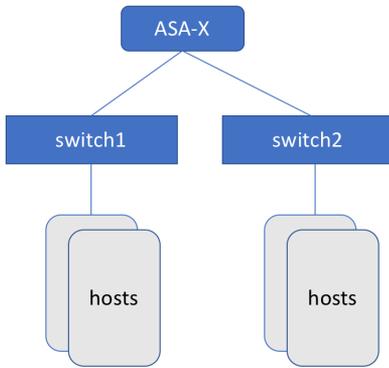
Host Name	Number of VMs	Power State	Version
ddc1-pod2esx046.dm.democompany.net	3	On	6.0.0
ddc1-pod2esx040.dm.democompany.net	3	On	6.0.0
ddc1-pod2esx037.dm.democompany.net	2	On	6.0.0

Cisco ASA ファイアウォール

vRealize Network Insight は Cisco ASA ファイアウォールをサポートしています。

Cisco ASA ファイアウォールの機能は次のとおりです。

- vRealize Network Insight は Cisco ASA-X シリーズのみをサポートします。
- vRealize Network Insight は Firepower モジュールをサポートしていません。
- 現在、vRealize Network Insight は Cisco ASA オペレーティング システム バージョン 9.4 をサポートしています。
- vRealize Network Insight は Cisco ASA のクラスタ展開をサポートしていません。
- vRealize Network Insight は、Cisco ASA の高可用性をサポートしていません。
- vRealize Network Insight は、ホストに直接接続されている場合、Cisco ASA をサポートしません。次のようなトポロジがサポートされます。



- Extended タイプの Cisco ASA アクセス ルールのみがサポートされます。Standard、WebType、EtherType などの他のタイプのアクセス ルールはサポートされません。
- ファイアウォールが Transparent モードで設定されている場合、仮想マシン間パスにある Cisco ASA ファイアウォールは、適用可能なアクセス ルールを表示しません。

例

vRealize Network Insight でサポートされているすべての Cisco ASA エンティティに対してクエリを実行できます。

表 17-2.

Cisco ASA のエンティティ	キーワード	サンプル クエリ
セキュリティ コンテキスト	ASA ファイアウォール ASA セキュリティ コンテキスト	<code>asa firewall where access group = <></code>
アクセス ルール	ASA アクセス ルール	<code>asa access rule where source ip = <></code> <code>asa access rule where destination ip = '192.168.2.2'</code> <code>asa access rule where port = <></code> <code>asa access rule where interface = <></code>
アクセス グループ	ASA アクセス グループ	<code>asa access group where interface = <></code>
ネットワーク オブジェクト/ネットワーク オブジェクト グループ	ASA ネットワーク オブジェクト ASA ネットワーク オブジェクト グループ	<code>asa network object where ip address = <></code> <code>asa network object group where ip address = <></code>
サービス オブジェクト/サービス オブジェクト グループ	ASA サービス オブジェクト ASA サービス オブジェクト グループ	<code>asa service object where port = <></code> <code>asa service where protocol = <></code> <code>asa service object group</code>

Check Point ファイアウォール

Check Point 管理サーバは、コレクタ IP アドレスからの API アクセスを受け入れる必要があります。

アクセスをセットアップするには、[管理と設定] > [ブレード] > [管理 API] > [高度な設定] の順に選択します。

Check Point MDS がデータ ソースとして追加されている場合、vRealize Network Insight はすべてのユーザー定義ドメインおよびグローバルドメインからデータを取得します。

vRealize Network Insight は Check Point 管理サーバからデータを取得するために、Check Point のパブリック Web API を使用します。VSX ゲートウェイが管理サーバに接続されている場合は、SSH ベースの CLI コマンドを使用して VSX 管理対象仮想システム VS ルーティング テーブルを取得し、仮想マシン間パスでの VS ゲートウェイの表示をサポートします。

vRealize Network Insight には、ほとんどの Check Point データを取得するために、Web-API アクセスに対する読み取り専用権限が必要です。例外は次のとおりです。

- 管理サーバに VSX 以外の物理ゲートウェイが接続されている場合、ユーザーは Web API に対する読み取り/書き込みアクセス権限を持っている必要があります。これは、仮想マシン間パス計算で `run script Web API` を使用するためのゲートウェイ ルートの取得に必要です。
- VSX ゲートウェイが管理サーバに接続されている場合、ユーザーには、同じパスワードを使用する SSH アクセス権限が必要です。さらに、CLI コマンド `vsx_util view_vs_conf` へのアクセス権限がユーザーに付与されている必要があります。このコマンドは、仮想マシン間パス計算の VSX ゲートウェイ ルートの取得に使用されます。
- MDS サーバの IP アドレスをデータ ソースとして使用する場合、ユーザーには、MDS ドメインとグローバルドメインを含むすべてのドメインへの Web API アクセス権限が必要です。これは、すべてのドメインからルール、ポリシー パッケージ、およびその他のデータを取得するために必要です。

vRealize Network Insight でサポートされているすべての Check Point エンティティに対してクエリを実行できます。すべてのエンティティの先頭に Check Point が付けられます。Check Point のクエリには、次のようなものがあります。

表 17-3.

Check Point のエンティティ	キーワード	クエリ
IPset	Check Point Address Range	<code>vm where Address Range = <></code>
	Check Point Network	<code>vm where Address Range = <></code>
		<code>Check Point Address Range where Translated VM = <></code>
グループ化	Check Point Network Group	<code>Check Point Network Group where Translated VM = <></code>
		<code>vm where Network Group = <></code>
サービス/サービス グループ	Check Point Service	<code>Check point service where Port = <></code>
	Check Point Service Group	<code>Check point service where protocol = <></code>
アクセス レイヤー	Check Point Access Layer	<code>Check Point Policy where Access Layer = <></code>

表 17-3. (続き)

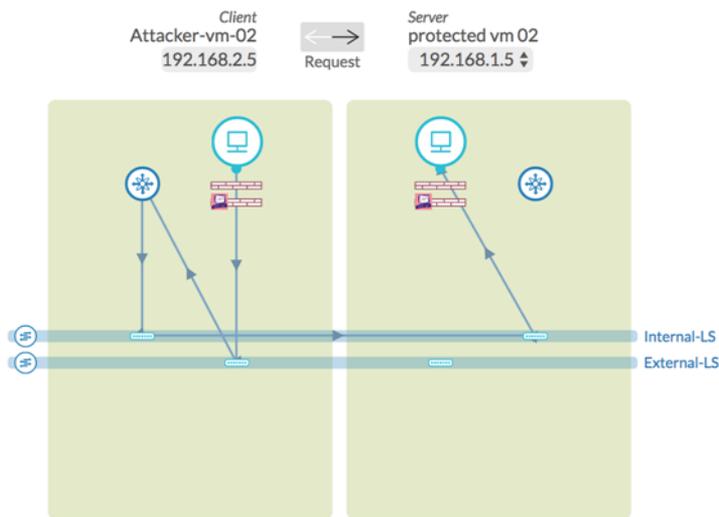
Check Point のエンティティ	キーワード	クエリ
ドメイン	Check Point Domain	check point domain where ip address = <> check point policy where domain = <> check point access layer where domain = <>
ゲートウェイとゲートウェイ クラスタ	Check Point Gateway Check Point Gateway Cluster	Check Point Gateway Cluster where Policy Package = <>
ポリシー パッケージ	Check Point Policy package	Check Point Policy where Policy Package = <> Check Point Policy Package where Rule = <>
ポリシー	Check Point Policy	Check point policy where source ip = <> and Destination IP = <> Rule where source ip = <> and Destination IP = <> (will display other rules- nsx, redirect along with check point policies in the system)

サンプルの Check Point マネージャ ダッシュボードは次のように表示されます。

仮想マシン間トポロジ図では、ホスト上の Check Point サービス仮想マシンを表示して、特定のトラフィックに適用された Check Point ルールを示すことができます。VSX 管理対象仮想システム (VS) ゲートウェイは、仮想マシン間パス内で物理ゲートウェイとして表示されます。ゲートウェイ アイコンをクリックすると、該当する Check Point ポリシーのリストが表示されます。

注： 仮想マシン間パスでは、vRealize Network Insight は仮想スイッチと仮想ルーターを含む VSX クラスタをサポートしません。

VM Path Topology



次に、Check Point 用のシステム イベントが生成されるシナリオをいくつか示します。

- NSX ファブリック エージェントが Check Point ゲートウェイの ESX で見つからない。
- Check Point サービス仮想マシンが見つからない。
- Check Point ゲートウェイの `sic` 状態が通信していない。
- アドレス範囲、ネットワーク、ポリシー、グループ、ポリシー パッケージ、サービス、サービス グループなどの、Check Point エンティティの検出イベントおよび更新イベントがある。

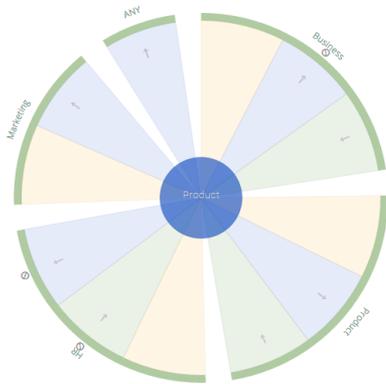
セキュリティ グループ

セキュリティ グループは、共通の権限セットを使用して管理されるグループのセットです。

セキュリティ グループ トポロジには、次の 2 つのビューがあります。

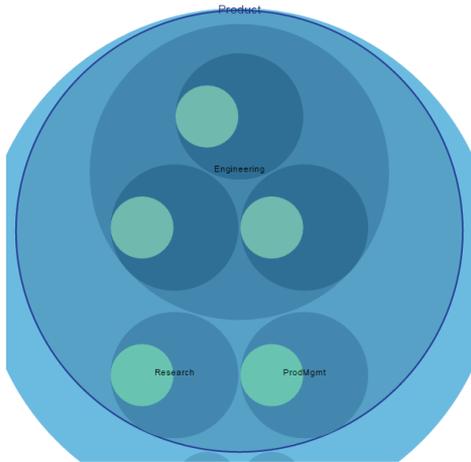
ファイアウォール ビュー

セキュリティ グループ ファイアウォール トポロジは、セキュリティ グループ間で適用可能なファイアウォール ルールを示すことで、選択したセキュリティ グループと他のセキュリティ グループとの関係を表示します。



コンテナ ビュー

セキュリティ グループ コンテナ トポロジは、セキュリティ グループが、その親セキュリティ グループまたは子（セキュリティ グループまたはその他のエンティティ）に対してどのように構造化されているかを表示します。



ポリシーベース VPN

vRealize Network Insight は、VMware Cloud on AWS、NSX-T、NSX-V でポリシーベース VPN をサポートします。ポリシーベース VPN では、次のシナリオがサポートされています。

- VMware Cloud on AWS パブリック IP アドレスと NSX-V/NSX-T/AWS パブリック IP アドレス間の VPN トンネル
- 企業ファイアウォールのパブリック IP アドレスと内部 NSX Edge 間の、VMware Cloud on AWS パブリック IP アドレスおよび企業ファイアウォール パブリック IP アドレスから 1:1 NAT への VPN トンネル

注： vRealize Network Insight は、企業のファイアウォールでの VMware Cloud on AWS からの VPN トンネルのシナリオをサポートしておらず、内部 NSX Edge では NAT が設定されていません。

ポリシーベース VPN エンティティ

vRealize Network Insight は、データセンターで設定された実際の VPN である L3 VPN Session エンティティのデータを取得します。

次に、ポリシーベース VPN エンティティの検索語を示します。

表 17-4.

検索語	説明
Policy based VPN	VMware Cloud on AWS、NSX-V、および NSX-T のすべてのポリシーベース VPN セッション
VMC Policy based VPN	VMware Cloud on AWS ポリシーベース VPN セッション
NSX-T Policy based VPN	NSX-T ポリシーベース VPN セッション
NSX Policy based VPN	NSX ポリシーベース VPN セッション

NSX 分散ファイアウォールの非アクティブ ルール

vRealize Network Insight は、しばらくの間フローがない場合の NSX 分散ファイアウォール ルールの可視性をサポートしています。これらのルールは、非アクティブルールとして知られています。これらのルールはメモリ ヒープを使用し、セキュリティの問題につながる可能性があります。これらの非アクティブルールを監視するため、vRealize Network Insight は [セキュリティ] ダッシュボードで次の 2 つのウィジェットを提供しています。

注： [セキュリティ] ダッシュボードを表示するには、検索バーに [セキュリティ] と入力します。

- 未使用の NSX ファイアウォール ルール：このウィジェットには、指定した期間にフローが報告されない場合のすべての NSX ファイアウォール ルールが一覧表示されます。これらのルールは、次の検索クエリを使用して取得することもできます。

```
nsx firewall rule where flow is not set
```

注： 指定した時間に NSX 分散ファイアウォール IPFIX を有効にしてください。

Fortinet ファイアウォール

vRealize Network Insight では、Fortinet ファイアウォールに関する判断材料を表示できます。

vRealize Network Insight では、以下の Fortinet エンティティがサポートされます。

- Fortinet マネージャ
- Fortinet ADOM：Fortinet 管理ドメインの詳細
- Fortinet VDOM：Fortinet 仮想ドメインの詳細。vRealize Network Insight では、フローベースのフィルタリングのみがサポートされます。透過モードはサポートされません。
- Fortinet アドレス：ADOM 固有のアドレスのリスト。vRealize Network Insight では、ipmask、iprange、NSX の各ファブリック コネクタがサポートされます。

- Fortinet アドレス グループ : ADOM 固有のアドレス グループのリスト
- Fortinet 動的アドレス : ADOM 固有の動的アドレス (VDOM でマッピングされたアドレス) のリスト
- Fortinet 動的アドレス グループ : ADOM 固有の動的アドレス グループ (VDOM でマッピングされたアドレス グループ) のリスト
- Fortinet 動的インターフェイス : ADOM 固有の動的インターフェイスのリスト。
- Fortinet ゾーン : ADOM 固有のゾーンのリスト。
- Fortinet サービス : 各 ADOM で手動および自動により生成されたサービスのリスト。
- Fortinet サービス グループ : 各 ADOM のサービス グループのリスト。
- Fortinet ポリシー : 各 ADOM の Fortinet ポリシー。現在サポートされているのは、IPv4 ポリシー、Fortinet グローバル ヘッダー ポリシー、Fortinet グローバル フッター ポリシーのみです。
- Fortinet ポリシー パッケージ : ポリシー パッケージのリスト。ポリシー パッケージ名には、パッケージ名の前にポリシー パッケージへのパスも含まれています。
- Fortinet デバイス : FortiManager に関連付けられている Fortinet デバイスのリスト。
- Fortinet デバイス グループ : ユーザーが指定した Fortinet デバイス グループのリスト。

以下はサポートされません。

- NAT モードでの仮想マシンから仮想マシンへのパス。
- 透過モードの物理デバイスの仮想マシンから仮想マシンへのパス。
- ユーザー、ユーザー グループ、アプリケーション、セキュリティ プロファイルなどの詳細な (IP アドレスを使用しない) ポリシー プロパティ。

マイクロセグメンテーションの操作

18

vRealize Network Insight は、**マイクロセグメンテーション** セキュリティを実装するための計画と推奨事項を提供します。これは、ユーザーが VMware NSX 環境を迅速かつ確実に管理および拡張するのに役立ちます。

この章には、次のトピックが含まれています。

- アプリケーションの分析
- アプリケーション検出
- VMware Cloud on AWS : 計画およびマイクロセグメンテーション

アプリケーションの分析

マイクロセグメンテーション プラニング トポロジは、フローをセグメントに分割することで、環境内にあるすべてのフローを表示します。

vRealize Network Insight では、1つのフローは 4 組で構成されます。次の内容が含まれます。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 宛先ポート
- プロトコル

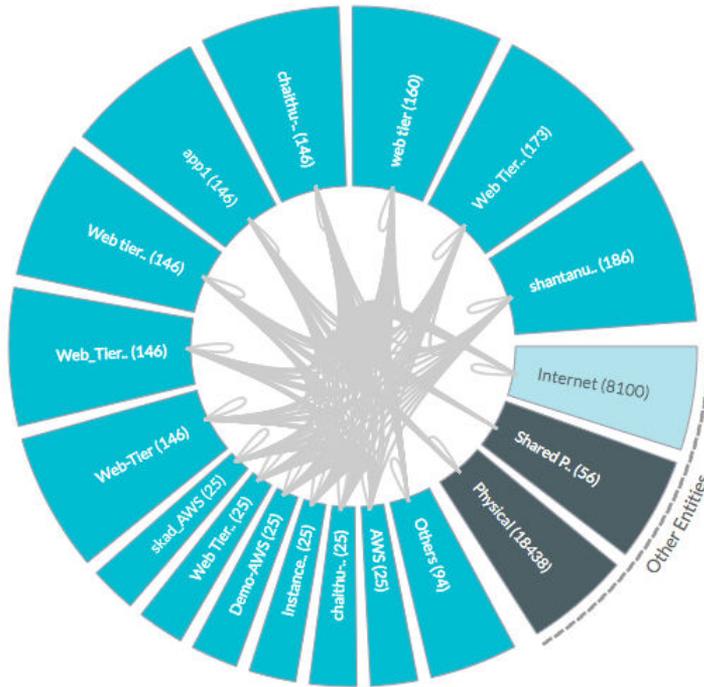
データは、ドーナツ ビューとグリッド ビューという 2 つの形式で表示できます。

ドーナツ ビューでのマイクロセグメンテーションおよびフロー データの表示

ドーナツ ビューでは、青色の線は送信フロー、緑色の線は受信フロー、黄色の線は送受信フローを表します。セグメントをクリックすると、その詳細が表示されます。

Micro-Segments i

Group By Tier v Flow Type All Allowed Flows v

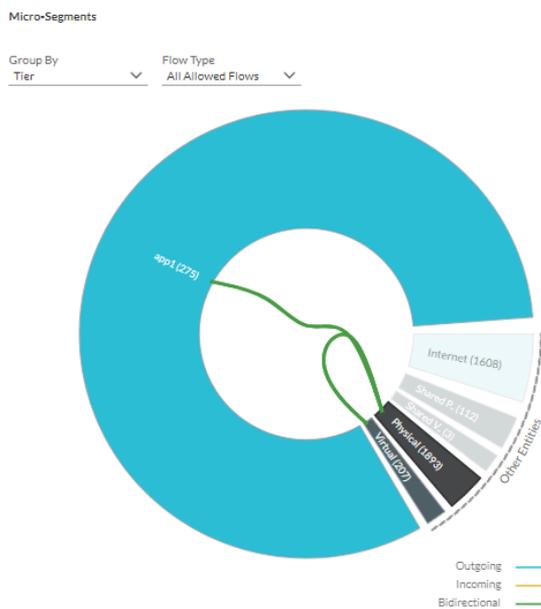


選択した範囲外の仮想マシンは、マイクロセグメンテーション プランニング トポロジ内の [他のエンティティ] としてグループ化されます。

カテゴリ別（物理、他の仮想、インターネット）にサブグループを作成してフローを分析することもできます。

Group By	Also show groups for
VLAN/VXLAN	All
Application	Physical
✓ Tier	Virtual
Subnet	Internet
Folder	✓ None
Cluster	
VM	
Port	
Security Tag	
Security Group	
IPSet	
VPC	

各グループはウェッジに展開されます。次に示すトポロジには、[物理グループ]のウェッジが表示されています。



[フロー] ピンは、ポート別に分けられた、異なる時間間隔のフローを示します。すべてのフローを表示するか、2つのエンティティ間のフローを表示できます。許可されたフローやブロックされたフロー別に、フローをフィルタリングすることもできます。フローは、合計バイト数または許可されたセッション数のいずれかで表示できます。ファイアウォールで保護されているフローの場合は、そのことを示す印を使用して、ポート内のフローがファイアウォールで保護されていることが示されます。

範囲（データセンター全体またはクラスタなど）の計画では、ソースまたはターゲットとして仮想マシンまたは物理サーバ（物理 IP アドレス識別）を含むフローが選択されます。

トポロジには 2 つの異なるゾーンがあります。

- 内部：このゾーンには、範囲内の仮想マシンまたは IP アドレスが含まれます。
- 外部：このゾーンには、範囲外だが内部ゾーンの仮想マシンまたは IP アドレスと通信する、仮想マシンまたは IP アドレスが含まれます。外部ゾーンは、次のウェッジで構成されます。
 - DC 仮想：内部ゾーン内の仮想マシンまたは IP アドレスと通信していて、LDAP や NTP などの既知の共有サービスをホストしていない、ソースまたはターゲットのデータセンターの内部仮想マシンが含まれます。
 - 共有仮想：LDAP や NTP などの既知の共有サービスをホストしており、内部ゾーン内の仮想マシンまたは IP アドレスが通信している、ターゲット データセンターの内部仮想マシンが含まれます。
 - DC 物理：内部ゾーン内の仮想マシンまたは IP アドレスと通信していて、LDAP や NTP などの既知の共有サービスをホストしていない、ソースまたはターゲットのデータセンターの内部物理 IP アドレスが含まれます。
 - 共有物理：LDAP や NTP などの既知の共有サービスをホストしており、内部ゾーン内の仮想マシンまたは IP アドレスが通信している、ターゲット データセンターの内部物理 IP アドレスが含まれます。
 - インターネット：内部ゾーン内の仮想マシンまたは IP アドレスと通信する、ソースまたはターゲットのデータセンターの外部仮想マシンまたは物理 IP アドレスが含まれます。

注：

- データセンターの内部とは、RFC 1918 が規定する IP アドレス（デフォルト）と、E-W 設定で定義されたオーバーライドを意味します。
- データセンターの外部とは、RFC 1918 で規定されない IP アドレス（デフォルト）と、N-S 設定で定義されたオーバーライドを意味します。

グリッド ビューでのマイクロセグメンテーションおよびフロー データの表示

vRealize Network Insight を使用すると、表形式またはグリッド形式でオブジェクト間の通信を表示できます。

手順

- 1 [セキュリティ] - [セキュリティのプラン] の順に移動し、グリッド ビュー  アイコンをクリックします。
- 2 **仮想マシン、アプリケーション、セキュリティ グループ**など、[グループ化の基準] オプションの値を選択すると、対応する詳細が表形式で表示されます。

フィールド名	説明
送信元オブジェクト	送信元の名前
宛先オブジェクト	宛先の名前
関連フロー	送信元と宛先間の通信またはフローの数 数値をクリックすると、関連フローの詳細が表示されます。
バイト数の合計	すべてのフローの間の合計バイト数

フィールド名	説明
最大トラフィック速度	すべての関連フロー間で観察された最大トラフィック速度
セッションの数	特定のフローのアクティブなセッションの数

注：

- 各列のヘッダーをクリックして、昇順または降順でデータをソートすることができます。
- 表形式ビューからフィールドを非表示にするには、フィールドヘッダーの横にある [その他] アイコンをクリックし、フィールド名の選択を解除します。

3 グリッドビューの画面では、ほかにもいくつかのアクションを実行できます。

- 画面左側のフィルタペインでは、次の操作を実行できます。
 - 個々の送信元または宛先を選択して、選択した送信元オブジェクトまたは宛先オブジェクトに関連するフローをフィルタします。
 - 許可されたフローまたはドロップされたフローを表示するには、ファイアウォールアクションを選択します。
 - フローの状態を表示するには、保護ステータスを選択します。
- [フィルタの追加] をクリックして、フィルタを追加します。
- 表形式のデータを CSV 形式でエクスポートするには、表の上部にある [その他] オプションをクリックして、[CSV としてエクスポート] を選択します。

手動によるアプリケーションの作成

vRealize Network Insight ユーザーインターフェイスでは、アプリケーションを手動で作成できます。

手順

- 1 vRealize Network Insight の [ホーム] 画面で、[セキュリティ] - [アプリケーション] の順にクリックします。
- 2 [アプリケーション] タブで、[アプリケーションの追加] をクリックします。
- 3 [アプリケーションの追加] 画面の [アプリケーション名] テキストボックスに、作成するアプリケーションの名前を入力します。
- 4 [階層/展開] セクションで、一意の名前を入力します。

要件に従って、仮想マシン、物理マシン、またはサービスの階層/部門を作成できます。

5 [メンバー] フィールドで、

- a ドロップダウンメニューから、階層を作成するための条件を選択します。

条件は、仮想マシンのプロパティ、仮想マシンの場所（アプリケーション、クラスタ、フォルダ）に加えて、Kubernetes サービス（サービス名、クラスタの IP アドレス、名前空間、クラスタ IP アドレス、サービスラベル）にも基づいて定義できます。

複数のクラスタで名前、IP アドレス、またはタグが同一の特定の Kubernetes サービスを検索するには、カスタム検索を使用します。

- b 階層に追加する値を入力または選択します。

複数の値を入力するには、個々の値の後にカンマを使用します。

サービスを層の一部として追加するには、[サービス名] を選択し、値に名前を入力します。

定義された条件に基づいて、関連付けられた仮想マシンの数、物理 IP アドレスの数、またはサービスの数を確認できます。

- 6 さらに条件を追加するには、[別の条件を追加] をクリックします。

- 7 （オプション）1つのアプリケーションの下に別の階層を作成するには、[階層/展開の追加] をクリックします。

1つのアプリケーションの下に複数の階層を作成できます。

アプリケーションによってすべての階層が作成され、すべての条件に一致する仮想マシン、物理 IP アドレス、およびサービスの数が表示されます。

- 8 （オプション）動的しきい値設定を作成するには、[しきい値分析の有効化] チェックボックスを選択します。

システムによって [しきい値の設定] 画面にしきい値設定が作成されます。vRealize Network Insight によって作成されるしきい値設定の名前は、Sys で始まります。

注：

- アプリケーションにメンバーを追加し [しきい値分析の有効化] チェックボックスを選択してから、[しきい値設定] 画面にメンバーが反映されるまで、20 分ほどかかる場合があります。
- システム生成のしきい値設定は削除できません。アプリケーションを削除するか、[しきい値分析の有効化] チェックボックスをクリアしてからアプリケーションを保存すると、そのアプリケーションに関連するシステム生成のしきい値設定は自動的に削除されます。

- 9 最終的にアプリケーションを追加する前に、フローを表示するには、[フローの分析] を選択します。仮想マシンまたは物理アドレスに基づいて階層を表示できます。

- 10 [保存] をクリックします。

注： アプリケーションに VMware 仮想マシンがない場合に [しきい値分析の有効化] チェックボックスを選択すると、アプリケーションを保存できません。アプリケーションを保存するには、VMware 仮想マシンを追加するか [しきい値分析の有効化] をクリアする必要があります。

- 11 （オプション）フロー分析をプレビューするには、[フローのプレビュー] をクリックします。

アプリケーションのマイクロセグメントビューが表示されます。

次のステップ

アプリケーションの詳細は、[保存されたアプリケーション] で確認できます。

物理 IP アドレスの階層の作成

アプリケーションを作成する際、ドロップダウン リストから [カスタム IP アドレス検索] を選択し、拡充フィールドに基づいて物理 IP アドレスの階層を作成できます。拡充フィールドの詳細については、[フローと IP アドレス エンドポイントの拡充](#)を参照してください。

強化された DNS、サブネット、VLAN 情報は、次のように階層を指定する場合に使用できます。

- Web

```
Query: IP Endpoint where Subnet Network = '172.16.101.0/24'
```

- アプリケーション

```
Query: IP Endpoint where Dns Domain = app.example.com
```

- データベース

```
Query: IP Endpoint where L2 Network = 'vlan-102'
```

- 共通サービス

```
Query: IP Endpoint where Dns Domain = svc.example.com
```

アプリケーション検出

複数のアプリケーションがある場合、または 1 つのアプリケーションに複数の階層がある場合、パブリック API またはユーザー インターフェイスを使用してアプリケーションを作成すると手間がかかります。vRealize Network Insight では、アプリケーションとその階層を自動的に検出することで、手動による作業を大幅に削減できます。

vRealize Network Insight では、以下に基づいてアプリケーション検出を実行できます。

- タグ (vCenter Server タグまたは AWS タグ)
- 仮想マシン名
- [ServiceNow](#) の追加

例：アプリケーション検出の構造の例

次のように想定します。

- データ ソースとして vCenter Server を追加しました。
- データセンターには、VM1、VM2、VM3、VM4 の 4 台の仮想マシンがあります。
- 各仮想マシンが属するアプリケーションの名前を定義するタグ (キーと値) を定義してあります。
- 各仮想マシンが属する階層を定義するタグ (キーと値) を定義してあります。

次の表の例を参照してください。

仮想マシン名	キーと値のタグ
VM1	<ul style="list-style-type: none"> ■ アプリケーション名 : MyApplication1 ■ アプリケーション階層 : App
VM2	<ul style="list-style-type: none"> ■ アプリケーション名 : MyApplication1 ■ アプリケーション階層 : Web
VM3	<ul style="list-style-type: none"> ■ アプリケーション名 : MyApplication2 ■ アプリケーション階層 : App
VM4	<ul style="list-style-type: none"> ■ アプリケーション名 : MyApplication2 ■ アプリケーション階層 : Web

タグに基づいてアプリケーションを検出する方法

vRealize Network Insight では、アプリケーション検出のグループ化基準をこれらのタグで定義できます。

この例では、定義済みのタグとグループ化条件に基づいて、vRealize Network Insight で 2 つの階層（App および Web）とそれに関連する仮想マシンを持つ 2 つのアプリケーション（MyApplication1 および MyApplication2）を検出しています。

アプリケーション	階層とその仮想マシン
MyApplication1	<ul style="list-style-type: none"> ■ App、VM1 ■ Web、VM2
MyApplication2	<ul style="list-style-type: none"> ■ App、VM3 ■ Web、VM4

仮想マシン名に基づいてアプリケーションと階層を作成する方法

仮想マシン名が次の形式で定義されていると仮定します。ApplicationName : Tier : VMName

```
MyApplication1 : App : VM1
MyApplication1 : Web : VM2
MyApplication2 : App : VM3
MyApplication2 : Web : VM4
```

注： ランダムに定義された仮想マシン名は、アプリケーション検出用にグループ化することはできません。

以下の正規表現を使用すると、vRealize Network Insight によってそれぞれ 2 つのアプリケーションが検出されます。

- アプリケーションの正規表現 : `(.*)_(.*)_.*.*`
- 階層の正規表現 : `(.*)_(.*)_(.*)-.*`

アプリケーション	階層とその仮想マシン
MyApplication1	<ul style="list-style-type: none"> ■ App および MyApplication1 : App : VM1 ■ Web および MyApplication1 : Web : VM2
MyApplication2	<ul style="list-style-type: none"> ■ App および MyApplication2 : App : VM3 ■ Web および MyApplication2 : Web : VM4

検出されたアプリケーションの追加

既存のアプリケーションを検出して、vRealize Network Insight に追加することができます。

手順

- 1 [検索] ボックスに **applications** という文字列を指定して検索します。
- 2 [アプリケーション] タブで、次のいずれか、またはすべてを実行します。
 - アプリケーションを名前、階層、またはメンバーでソートします。
 - トポロジに表示できるアプリケーションの数をフィルタリングします（上位 10、上位 20 など）。各六角形はアプリケーションを表します。数が多いほど、六角形の色が濃くなります。
 - 名前、階層、またはメンバーでアプリケーションを検索します。
- 3 [検出] タブをクリックします。

以下に示す [タグ]、[ServiceNow]、[名前]、[詳細] の各タブが表示され、アプリケーションを追加できます。
- 4 適切なタブを選択し、それぞれの手順を実行します。

タブ	説明
タグ	<ol style="list-style-type: none"> a 範囲を定義します。 <ul style="list-style-type: none"> ■ [すべての仮想マシン] を選択すると、vRealize Network Insight に追加されているすべてのデータ ソースに含まれるすべての仮想マシンのリストが表示されます。 ■ [手動で選択] を選択すると、アカウント、データセンター、マネージャなどの要件に基づいて仮想マシンをフィルタリングできます。 b タグのキーと値を定義します。 <ul style="list-style-type: none"> ■ タグのキーを入力します。たとえば、<i>Automation</i>、<i>Category</i>、<i>CreatedBy</i>、<i>Owner</i> です。 ■ (オプション) それぞれのキーの値を入力します。 c [<i>count</i> 個のアプリケーションが見つかりました] リンクをクリックすると、指定された条件に一致するアプリケーション名、仮想マシン名、および仮想マシンの数のリストが表示されます。 d [未分類の仮想マシン] をクリックして、指定された名前パターンまたはタグ パターンに従っていない仮想マシンのリストを表示します。仮想マシンを編集することにより、名前またはタグの条件を修正できます。 e [変更の保存先] オプションを選択して、新しいテンプレートを作成するか、既存のテンプレートを更新します。 <p>注： 管理者ユーザーは、すべてのテンプレートを更新できます。メンバー ユーザーは、自分が作成したテンプレートのみを編集できます。</p> f [検出] をクリックします。
ServiceNow	ServiceNow で使用可能なアプリケーションが表示されます。

タブ	説明
名前	<p>a 範囲を定義します。</p> <ul style="list-style-type: none"> ■ [すべての仮想マシン] を選択すると、vRealize Network Insight に追加されているすべてのデータ ソースに含まれるすべての仮想マシンのリストが表示されます。 ■ [手動で選択] を選択すると、アカウント、データセンター、マネージャなどの要件に基づいて仮想マシンをフィルタリングできます。 <p>b [Pattern Builder] をクリックします。</p> <p>vRealize Network Insight は、定義された範囲に基づいて、Pattern Builder 内の仮想マシンのリストをフィルタリングします。</p> <ol style="list-style-type: none"> 1 デフォルトの仮想マシン名を選択するか、リスト内の仮想マシンを選択し、仮想マシン名に基づいてパターンまたは正規表現 (regex) を構築します。 2 パターンを作成する場所またはグループをクリックします。 <hr/> <p>注： グループを選択した後で文字または場所を選択すると、そのグループ選択は vRealize Network Insight によってパターンを構築するために使用されません。逆も同様です。</p> <hr/> <p>選択に基づいて、画面にパターンが表示されます。また、パターンに一致するアプリケーションと、それぞれのアプリケーションの仮想マシンの数、および各アプリケーションの仮想マシンの名前が表示されます。</p> <ol style="list-style-type: none"> 3 [送信] をクリックします。 <p>c [count 個のアプリケーションが見つかりました] リンクをクリックすると、正規表現に一致するアプリケーション名、仮想マシン名、および仮想マシンの数のリストが表示されます。</p> <p>d [未分類の仮想マシン] をクリックすると、指定された名前パターンに従っていない仮想マシンのリストが表示されます。</p> <p>e [変更の保存先] オプションを選択して、新しいテンプレートを作成するか、既存のテンプレートを更新します。</p> <hr/> <p>注： 管理者ユーザーは、すべてのテンプレートを更新できます。メンバー ユーザーは、自分が作成したテンプレートのみを編集できます。</p> <hr/> <p>f [検出] をクリックします。</p>
Advanced	<p>a 範囲を定義します。</p> <ul style="list-style-type: none"> ■ [すべての仮想マシン] を選択すると、vRealize Network Insight に追加されているすべてのデータ ソースに含まれるすべての仮想マシンのリストが表示されます。 ■ [手動で選択] を選択すると、アカウント、データセンター、マネージャなどの要件に基づいて仮想マシンをフィルタリングできます。 <p>b [Pattern Builder] をクリックします。</p> <p>vRealize Network Insight は、定義された範囲に基づいて、Pattern Builder 内の仮想マシンのリストをフィルタリングします。</p> <ol style="list-style-type: none"> 1 デフォルトの仮想マシン名を選択するか、リスト内の仮想マシンを選択し、仮想マシン名に基づいてパターンまたは正規表現 (regex) を構築します。 2 パターンを作成する場所またはグループをクリックします。 <hr/> <p>注： グループを選択した後で文字または場所を選択すると、そのグループ選択は vRealize Network Insight によってパターンを構築するために使用されません。逆も同様です。</p> <hr/> <p>選択に基づいて、画面にパターンが表示されます。また、パターンに一致するアプリケーションと、それぞれのアプリケーションの仮想マシンの数および名前が表示されます。</p> <ol style="list-style-type: none"> 3 [送信] をクリックします。

タブ	説明
	c [count 個のアプリケーションが見つかりました] リンクをクリックすると、正規表現および仮想マシン名に一致するアプリケーション名と仮想マシンの数のリストが表示されます。
	d [未分類の仮想マシン] をクリックすると、指定された名前パターンに従っていない仮想マシンのリストが表示されます。
	e [変更の保存先] オプションを選択して、新しいテンプレートを作成するか、既存のテンプレートを更新します。
	注： 管理者ユーザーは、すべてのテンプレートを更新できます。メンバー ユーザーは、自分が作成したテンプレートのみを編集できます。
	f [検出] をクリックします。

条件に一致するすべてのアプリケーションが表形式ビューと六角形マップ ビューで表示されます。

マップ ビューで六角形の上にマウス ポインタを置くと、アプリケーション名、検出された仮想マシンの数、階層数などの情報を確認できます。アプリケーションとインターネットの間の線は、接続を表します。行をクリックすると、送信元フローと宛先フローの数、保護されていない送信元フローと宛先フローの数など、フローの詳細が表示されます。六角形に疑問符が付いている場合は、vRealize Network Insight でアプリケーションのフローの詳細のいずれかが見つからなかった、または取得できなかったことを示しています。この原因としては、アプリケーションがフローの制限を超えたか、保護されていないフローが含まれていることが考えられます。

表形式ビューには、アプリケーション名、宛先に到達しないフローの数、ファイアウォール アクションが拒否されたためにドロップされたフローの数、階層とメンバーの数など、アプリケーションの詳細が表示されます。

マップ ビューと表形式ビューの間では対話が行われます。表形式ビューでアプリケーションをクリックすると、マップ ビューで六角形がハイライトされて選択状態になり、すべてのネットワーク接続が表示されます。

5 (オプション) マップ ビューで、次のいずれかのアクションを実行します。

- ズーム インやズーム アウト、またはマップの移動によってアプリケーションを表示します。
- 保護されていないすべてのアプリケーションを表示します。
- インターネットに接続されているアプリケーションを表示します。
- ホスト共有サービスを使用するすべてのアプリケーションを表示します。
- 問題が発生しているアプリケーションを表示します。

6 (オプション) 表形式ビューで、次のいずれかのアクションを実行します。

- メンバー列の値にマウスを置くと、それぞれの仮想マシン、物理 IP アドレス、サービスの数が表示されます。
- アプリケーション名をクリックしてアプリケーション ダッシュボードを開き、その特定のアプリケーションの詳細を表示します。
- 表形式ビューの [+] アイコンをクリックして展開し、条件、仮想マシン数、階層数などのアプリケーションの詳細を表示します。

注： このアイコンは、検出されたアプリケーションでのみ使用できます。

7 検出されたアプリケーションを保存するには、以下の手順を実行します。

- マップビューで、六角形の上にマウス ポインタを置いて、[アプリケーションの保存] をクリックするか、
- 表形式ビューで、[アプリケーションの保存] をクリックします。

注： 表内のアプリケーションに対応するチェック ボックスを複数選択して、[アプリケーションの保存] をクリックすると、アプリケーションを一括保存できます。

8 [アプリケーションの追加] 画面で詳細を確認し、[送信] をクリックします。

保存が完了すると、アプリケーションの六角形の上にマウス ポインタを置いたときに表示されるリストに application:Saved と表示され、表形式ビューでそのアプリケーションにチェック マークが表示されます。アプリケーションがすでに保存されている場合は、チェック マークにマウス ポインタを置いて [名前を付けて保存] をクリックすると、アプリケーションを別の名前でも保存できます。

注： アプリケーションが ServiceNow で変更された場合、vRealize Network Insight による自動更新は実行されません。ユーザーが vRealize Network Insight でアプリケーションを手動で更新する必要があります。

表 18-1. 制限

オブジェクト	推奨される制限
マップビューのアプリケーション リスト	1,000
表形式ビューのアプリケーション リスト	なし
保存されたアプリケーション	400
すべてのアプリケーションの階層数合計	5,000
アプリケーションごとの階層数	30
階層ごとのメンバー数	なし
アプリケーションごとのメンバー数	1,800
	アプリケーションが制限を超えると、アプリケーション トポロジのピンボードにフロー情報が表示されなくなったり、エラー メッセージが表示されたりする可能性があります。
アプリケーションごとのフロー数	300,000

セットアップがアプリケーションごとに推奨されている階層、アプリケーション、およびフローの制限を超えている場合でもオブジェクトを追加することはできますが、パフォーマンスが低下する可能性があります。

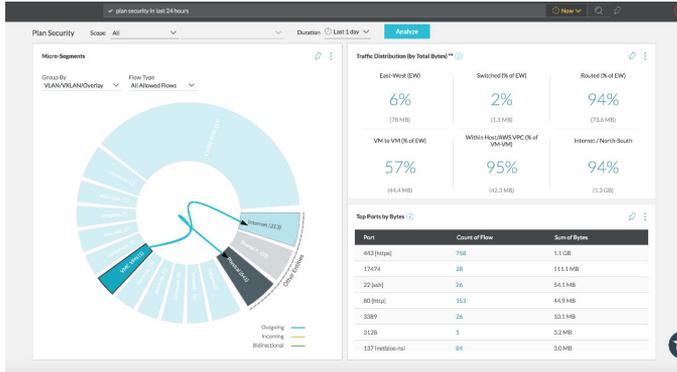
次のステップ

[CSV としてエクスポート] をクリックして、アプリケーションの詳細を .csv 形式でエクスポートします。エクスポートするアプリケーションの数とフィールドを定義できます。アプリケーション名と階層名のフィールドは、メンバー数に応じて繰り返されます（メンバーごとに 1 行）。アプリケーションに関連するフィールドのみが入力され、残りのフィールドは空のままになります。

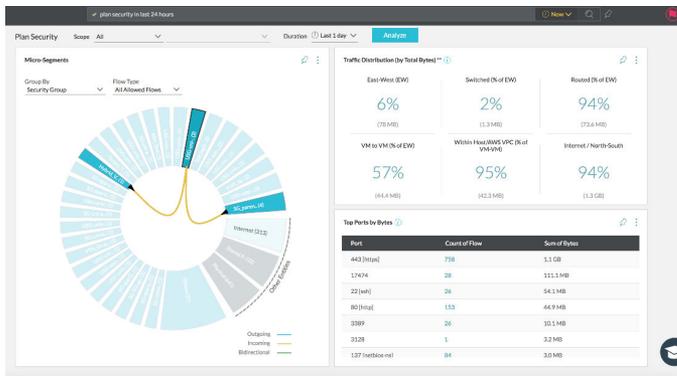
VMware Cloud on AWS : 計画およびマイクロセグメンテーション

[セキュリティのプラン] 画面で [VMC セグメント] を範囲として選択して、特定の VMware Cloud on AWS セグメントを計画できます。

ポリシー セグメントの場合は、グループ内で VLAN/VXLAN/Overlay 句を使用します。



ポリシー グループの場合は、グループ内で Security Group 句を使用します。

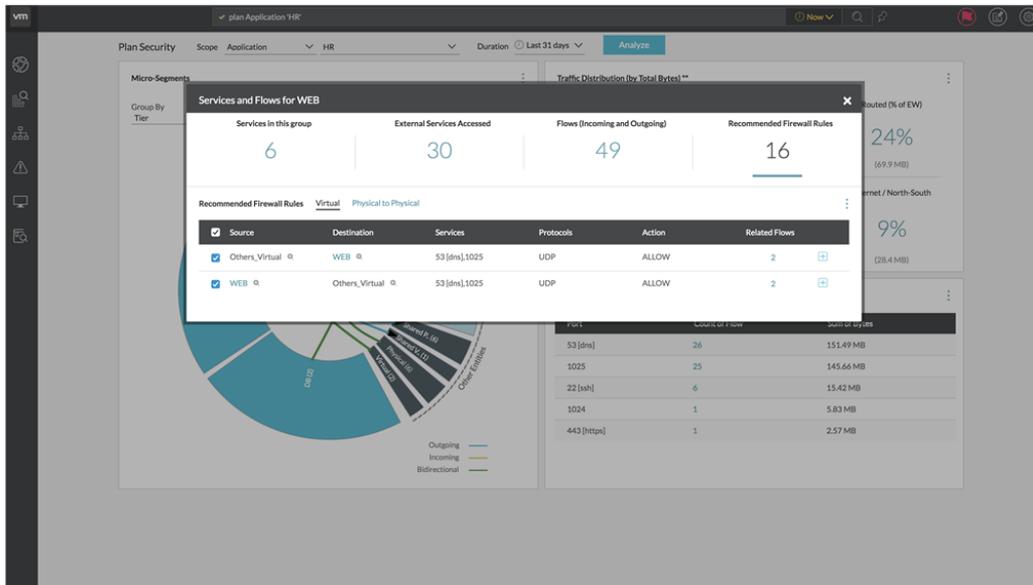


推奨されるファイアウォールルール

19

[セキュリティの計画] 画面で、トポロジ図のウェッジまたはエッジをクリックすると、その特定セグメントのサービスとフローのリストを表示できます。[推奨されるファイアウォールルール] をクリックすると、定義されているルールが表示されます。ソースまたはターゲットのメンバーは、次のタイプのルールの下に表示されます。

- 物理から物理：このタブには、物理およびインターネット IP アドレスに関連付けられているすべてのルールが一覧表示されます。ルールは、物理/物理、物理/インターネット、インターネット/物理、またはインターネット/インターネットの各エンティティについて設定できます。
- 仮想：このタブには、1 台以上のエンドポイントが仮想マシンである場合のすべてのルールが一覧表示されます。



各ファイアウォール ルールについて、次の詳細を確認できます。

- グループのメンバーを表示：エンティティ名の横にある + 記号をクリックすると、グループのメンバーが表示されます。

Services and Flows for integration.tier2

Services in this group: 7 | External Services Accessed: 22 | Flows (Incoming and Outgoing): 32 | Recommended Firewall Rules: 7

Recommended Firewall Rules: Virtual Physical to Physical

<input checked="" type="checkbox"/>	Source	Destination	Services	Protocols	Action	Related Flows
<input checked="" type="checkbox"/>	integration.tier2	integration.tier1	53 [dns],1025	UDP	ALLOW	2
<input checked="" type="checkbox"/>	integration.tier1	integration.tier2	53 [dns],1025	UDP	ALLOW	2
<input checked="" type="checkbox"/>	integration.tier1	integration.tier2	22 [ssh]	TCP	ALLOW	2

注：

- インターネット カテゴリに属するグループのメンバーは表示されません。
 - セキュリティ グループに仮想 IP アドレスと物理 IP アドレスの両方がある場合、その特定グループのメンバーのリストには、物理 IP アドレスとインターネット IP アドレスは表示されません。
 - メンバーの Kubernetes サービスは、[Kubernetes サービス] タブの下に表示されます。
 - [仮想マシン]、[物理およびインターネット IP アドレス]、または [Kubernetes サービス] のメンバー数またはエントリがゼロの場合、タブは表示されません。
-
- ソース
 - ターゲット
 - サービス
 - プロトコル
 - アクション
 - 関連フロー：関連フローの番号をクリックすると、対応するフロー情報を含むフローのリストが表示されます。
 - 適用されたファイアウォール ルールの表示：[関連フロー] 列の横にある + 記号をクリックすると、同様のフローセットに対応する適用済みのファイアウォール ルールが表示されます。

Source	Destination	Services	Protocols	Action	Related Firewall Rules
integration.tier2	integration.tier1	53 [dns], 1025	UDP	ALLOW	2
integration.tier1	integration.tier2	53 [dns], 1025	UDP	ALLOW	2
integration.tier1	integration.tier2	22 [ssh]	TCP	ALLOW	2

必要に応じて、推奨ルールを XML または CSV としてエクスポートできます。

注： また、Kubernetes オブジェクトに関連する推奨されたルールを YAML 形式でエクスポートできます。

これらのアーティファクトの詳細については、[ルールのエクスポート](#)を参照してください。

脆弱な OS を保護するために推奨されるファイアウォールルール

次の手順に従って、脆弱な OS を保護するために推奨されるファイアウォールルールを取得します。

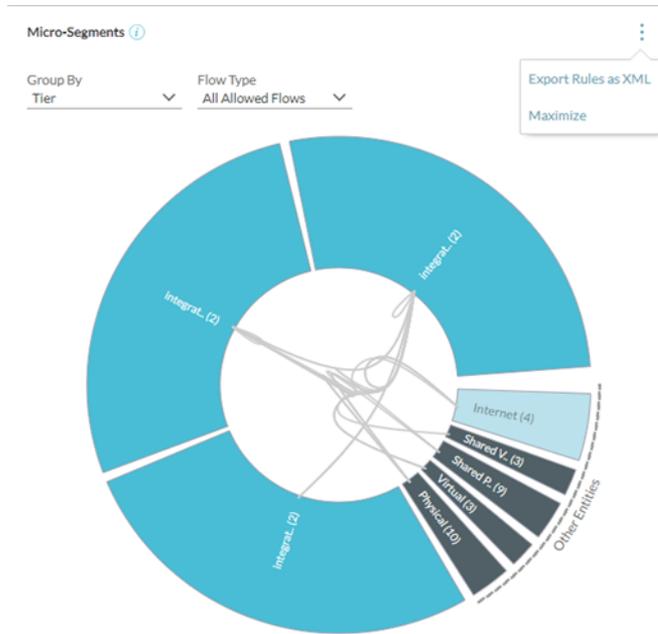
- 1 [セキュリティ] - [アプリケーション] - [アプリケーションの作成]の順に移動します。
- 2 アプリケーションおよび階層/展開の名前を入力します。
- 3 [メンバー] ドロップダウンで、[カスタム仮想マシンの検索]を選択し、テキストボックスに **in the qualifier put the matching criteria as: Operating System like 'Microsoft Windows Server 2003' or Operating System like 'Microsoft Windows Server 2008' or Operating System like 'Red Hat Enterprise Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or Operating System like 'SUSE Linux Enterprise 10'** という条件を入力します。
- 4 [保存] をクリックします。
- 5 [セキュリティ] - [セキュリティのプラン] の順に移動します。
- 6 [範囲] ドロップダウンで、[アプリケーション] と作成したアプリケーションの名前を選択します。
- 7 [期間] ドロップダウンで、[過去 7 日] を選択します。
- 8 推奨されるファイアウォールルールを取得するには、[分析] をクリックします。

この章には、次のトピックが含まれています。

- [ルールのエクスポート](#)
- [Kubernetes ネットワーク ポリシーのエクスポートと適用](#)

ルールのエクスポート

すべてのルールを、トポロジ全体の XML としてエクスポートできます。このメニュー項目は、[マイクロセグメンテーションの計画] 画面に次のように表示されます。



[XML としてエクスポート] オプションは、次のエンティティでのみ使用できます。

- セキュリティ グループ
- アプリケーション層

計画範囲が 1 つの NSX Manager のみにわたる場合、生成されるアーティファクトには、推奨されるサービスおよびファイアウォール ルールに対応する XML ファイルが含まれます。計画範囲が複数の NSX Manager にまたがる場合、生成されるアーティファクトには、推奨サービス、IPset、セキュリティ グループ、およびファイアウォール ルールに対応する XML ファイルが含まれます。

セキュリティ グループのプレースホルダ アーティファクトを次に示します。

- SG-Others_Internet.xml
- SG-Other.xml

トポロジ図に表示される特定のウェッジまたはエッジのすべてのルールを XML または CSV としてエクスポートできます。

注： また、Kubernetes オブジェクトに関連する推奨されたルールを YAML 形式でエクスポートできます。

NSX DFW ユニバーサル アーティファクト

さまざまな vCenter Server 環境や NSX 環境を対象に、ユニバーサル セキュリティ グループのオブジェクトを簡単に管理できます。vRealize Network Insight は、アプリケーションおよび階層グループについてのみ、ユニバーサル アーティファクトの生成とインポートをサポートします。ユニバーサル セキュリティ グループを使用すると、vCenter Server 間のシナリオでのファイアウォール ルールの展開および管理が簡単になります。ユニバーサル アーティファクトのインポートは、プライマリ NSX Manager で実行します。ユニバーサル セキュリティ グループのメンバーシップの管理は、プライマリ NSX Manager を介してのみ行えます。

ユニバーサル セキュリティ グループは次で構成されます。

- 他のユニバーサル グループ
- ユニバーサル IP セット
- ユニバーサル セキュリティ タグ

ルールを XML としてエクスポートすると、NSX Manager 固有のフォルダに加え、NSX DFW ユニバーサル アーティファクトで構成されるユニバーサル フォルダが作成されます。NSX DFW ユニバーサル アーティファクトのインポート後、対応するユニバーサル セキュリティ グループ、ユニバーサル IP セット、ユニバーサル セキュリティ タグ、およびユニバーサル DFW ファイアウォール ルールが作成されます。

注：

- ユニバーサル セキュリティ タグは、アクティブ/スタンバイ モードでのみサポートされます。
- ユニバーサル IP セットは、アクティブ/アクティブ モードとアクティブ/スタンバイ モードの両方でサポートされます。

ユニバーサル IP セットまたはユニバーサル セキュリティ タグは、要件に基づいて作成できます。ユニバーサル セキュリティ タグを作成すると、アプリケーション仮想マシンをセキュリティ タグにマッピングできます。それ以外の場合は、ユニバーサル IP セットが使用されます。

インポート ツールでは、次のフラグを使用できます。

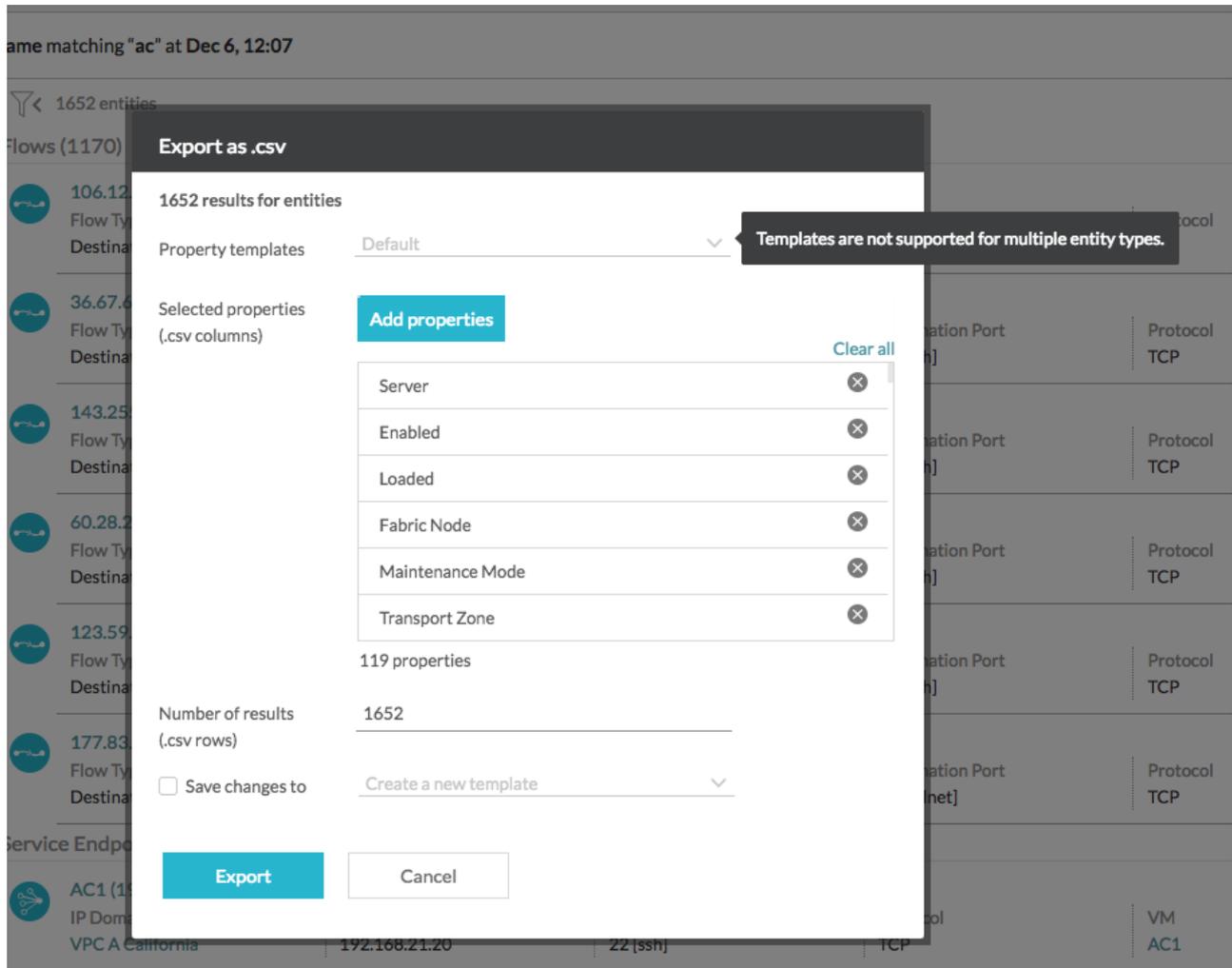
表 19-1.

フラグ名	説明
-uni	ユニバーサル フォルダからアーティファクトをインポートします。
-utag	ユニバーサル セキュリティ タグの付いたユニバーサル アーティファクトをユニバーサル セキュリティ グループのメンバーシップにインポートします。
-log	ログ作成が有効なルールを作成します。

注： これは、ユニバーサル オプション固有のフラグではありません。

CSV エクスポートの設定をプロパティ テンプレートとして保存

CSV ファイルのウィジェットからデータをエクスポートするときに、エクスポートするプロパティ（または列）の組み合わせをプロパティ テンプレートに保存できます。このプロパティ テンプレートは、結果のエンティティ タイプが 1 種類だけの場合に、CSV エクスポートで有効になります。複数のエンティティ タイプが一覧表示されるキーワードを使用して検索する場合、プロパティの組み合わせをプロパティ テンプレートに保存することはできません。



CSV エクスポートのモーダル ウィンドウを開くと、検索結果を得るためにデフォルトで（エンティティ タイプに基づいて）選択されているプロパティが表示されます。選択されているプロパティのリストを変更し、新しい設定として保存すると、後から参照できます。または、CSV エクスポートのモーダル ウィンドウの [テンプレート] セクションから、事前に保存されたプロパティ テンプレートをロードする、または開くこともできます。値を変更すると、選択したプロパティ テンプレートで選択されているプロパティが表示されます。

エクスポート用に選択されているプロパティを変更した後は、CSV エクスポートのモーダル ウィンドウからプロパティ テンプレートを作成したり、既存のプロパティ テンプレートを編集したりできます。このテンプレートは、現在の検索結果と同じエンティティ タイプです。

システム内の既存のプロパティ テンプレートのリストを表示するには、[設定] -> [プロパティ テンプレート] 画面の順に移動します。[プロパティ テンプレート] 画面のリストには、既存のテンプレートがエンティティ タイプ、最終更新日、プロパティ数などの詳細と共に表示されます。プロパティ テンプレートは、[プロパティ テンプレート] 画面で編集または削除できます。プロパティ テンプレートは、名前の変更以外の編集が可能です。

Kubernetes ネットワーク ポリシーのエクスポートと適用

Kubernetes オブジェクトに関連する推奨ネットワーク ポリシー ルールを YAML 形式でエクスポートできます。vRealize Network Insight による YAML 形式へのエクスポートでは、名前空間によるグループ化と、サービス トポロジによるグループ化のみがサポートされます。

前提条件

- [Kubernetes の追加](#)
- [VMware PKS の追加](#)

手順

- 1 推奨ルールを YAML 形式にエクスポートするには、[セキュリティのプラン] モデルで、セキュリティを計画する Kubernetes クラスタを選択し、次のいずれかの手順を実行します。
 - マイクロ セグメント ウィジェットで詳細オプションを展開し、[ルールを YAML としてエクスポート] を選択します。
 - マイクロ セグメントのドーナツ表示でノードを選択し、[推奨されるファイアウォール ルール] の数をクリックし、詳細オプションを展開して、[ルールを YAML としてエクスポート] を選択します。

Kubernetes ネットワーク ポリシーに基づいて名前が付けられ、タイムスタンプが設定された ZIP ファイルが、vRealize Network Insight によってダウンロードされます。このファイルを解凍すると、次の 5 つの CSV ファイルと、クラスタの数に応じて複数のフォルダが表示されます。各フォルダには、クラスタに対応する YAML ファイルが複数含まれています。

ファイル名	説明
network-policy-others-ipaddress.csv	サービスまたは名前空間の通信相手となっている物理サーバおよび仮想マシンの IP アドレスが含まれます。
recommended-namespace-labels-to-add.csv	名前空間に関連付けられたポッドに付けるラベルが含まれます。 例 <ul style="list-style-type: none"> ■ [クラスタ] : pdk8s ■ [名前空間] : sock-shop ■ [ラベル] : sock-shop-pdk8s
recommended-service-labels-to-add.csv	サービスに関連付けられたポッドに付けるラベルが含まれます。 例 <ul style="list-style-type: none"> ■ [クラスタ] : pdk8s ■ [名前空間] : sock-shop ■ [サービス] : front-end ■ [ラベル] : Service:front-sock-shop-pdk8s ■ [クラスタ] : pdk8s ■ [名前空間] : sock-shop ■ [サービス] : user ■ [ラベル] : Service:user-sock-shop

ファイル名	説明
recommended-network-policy.csv	vRealize Network Insight で推奨されるすべてのルールが含まれています。
exported-network-policy-rule-names.csv	推奨ルールに基づいてエクスポートされたすべてのネットワーク ポリシーを一覧表示します。

2 サービス ラベルを適用するには、以下の手順を実行します。

- a 以下の Kubernetes CLI コマンドを実行します。

```
kubectl edit deployment service-name -n namespace-name
```

```
kubectl edit deployment redis-master -n guestbook
```

サービスの展開ファイルが開きます。

- b サービス ラベル リストで、CSV ファイルで提案されたラベルをサービス展開の仕様セクションに示されているラベルに追加します。

3 名前空間ラベルを適用するには、次の手順を実行します。

- a 以下の Kubernetes CLI コマンドを実行します。

```
kubectl edit namespace namespace-name
```

```
kubectl edit namespace guestbook
```

名前空間の展開ファイルが開きます。

- b メタデータで、CSV ファイルで提案されたラベルを名前空間展開の spec セクションに示されているラベルに追加します。

4 以下のコマンドを実行して、ラベルがポッドに適用されているかどうかを確認します。

```
kubectl get pods -n namespace-name--show-labels
```

```
kubectl get pods guestbook--show-labels
```

結果ビューでラベルを確認します。

注： 名前空間に適用すると、ラベルはポッドに反映されません。

5 ネットワーク ポリシーを作成するには、それぞれのクラスタ フォルダから別のフォルダに YAML ファイルをコピーして、次のどちらかのコマンドを実行します。

- `kubectl apply -f <folder-name>/` : すべてのファイアウォール ルールをまとめて適用します。
- `kubectl apply -f <folder-name>/<firewall-rule>.yaml` : ファイアウォール ルールを1つずつ適用します。

vRealize Network Insight は、環境内のすべてのエンティティを対象とした堅牢な検索機能を備えています。

次に、vRealize Network Insight の検索機能に役立つ用語の一部を示します。

- エンティティ：データセンターは、ホスト、仮想マシン、スイッチ、ルーター、NSX Manager などの物理的および論理的なビルディング ブロックで構成されます。これらのブロックのインスタンスがエンティティです。
- プロパティ：エンティティは複数のプロパティで構成されます。プロパティは、構成プロパティまたはメトリック プロパティのいずれかです。
 - a 構成プロパティ：エンティティは、その構成プロパティによって記述できます。構成プロパティは、整数値か実数値、または文字列かブール値です。
 - 仮想マシンの名前、CPU コア、およびオペレーティング システム
 - ホストの仮想マシンの名前と数
 - b メトリック プロパティ：エンティティの特定の特性を測定するプロパティはメトリック プロパティです。メトリック プロパティの値は、一定の間隔でキャプチャされます。メトリック プロパティの例として、仮想マシンの CPU 使用量、メモリ使用量、およびネットワーク使用量があります。
- 集約関数：これらを検索クエリで使用して、特定のエンティティ タイプのインスタンス合計数の計算や、エンティティの最大プロパティの計算を行えます。vRealize Network Insight は次の集計機能をサポートします。
 - a sum
 - b max
 - c min
 - d avg

エンティティを検索する際、検索クエリに一致したエンティティが [結果] 画面に表示されます。

検索クエリを実行するたびに、検索バーには、検索結果の絞り込みに使用できる語句の候補が表示されます。たとえば、[仮想マシン] という語を入力すると、検索バーには、検索結果を絞り込むために追加できる用語の候補リストが表示されます。検索バーは、各検索クエリも検証します。チェックマークは有効な検索クエリを示し、クロスマークは無効な検索クエリを示します。[ヘルプ] 画面には、現在サポートされているクエリの例が示されています。

この章には、次のトピックが含まれています。

- [検索クエリの保存と削除](#)
- [検索クエリ](#)

- 高度なクエリ
- 時間管理
- 検索結果
- フィルタ
- vCenter Server タグ

検索クエリの保存と削除

vRealize Network Insight を使用すると、検索クエリを実行し、後で使用するためにクエリを保存することができます。また、保存された検索を削除することもできます。

注：

- vRealize Network Insight では、次のデフォルトの保存された検索を実行できます。
 - すべてのフロー
 - アプリケーション
 - Azure
 - Kubernetes ダッシュボード
 - 上位のトレンド
 - NSX
- デフォルトの保存された検索には保存または削除ができません。
- 無効な検索クエリは保存できません。
- 保存された検索はユーザーに対して固有ですが、デフォルトの保存された検索はすべてのユーザーが使用できます。

手順

- 1 クエリを保存するには、検索を実行し、検索バーの横にあるブックマーク アイコンをクリックします。

ブックマーク アイコンがハイライト表示され、クエリが保存されます。左側のナビゲーション バーの [保存された検索] に検索が表示されます。保存されているすべてのクエリを表示するには、[保存された検索] - [保存された検索の管理] の順にクリックします。
- 2 保存された検索を削除するには、ブックマーク アイコンを再度クリックし、[アクションの確認] ダイアログ ボックスで [削除] をクリックします。

[保存された検索の管理] ウィンドウから保存された検索を削除することもできます。
- 3 複数の保存された検索クエリをまとめて削除するには、次の操作を実行します。
 - a 左側のナビゲーション バーを展開し、[保存された検索] - [保存された検索の管理] の順にクリックします。
 - b 削除するクエリを選択します。

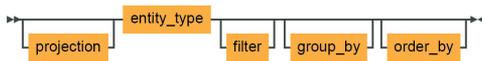
- c [削除] オプションをクリックします。
- d 削除を確認します。

検索クエリ

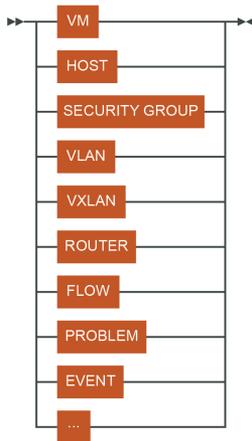
検索クエリは、次のカテゴリに分類できます。

1 [構造化クエリ]

構造化クエリは、次のコンポーネントから構成されます。



- [エンティティ タイプ]: エンティティ タイプは、検索するオブジェクトのタイプを表します。これは、単数形または複数形の形式のいずれかで指定できます。構造化クエリでは、エンティティ タイプは必須です。

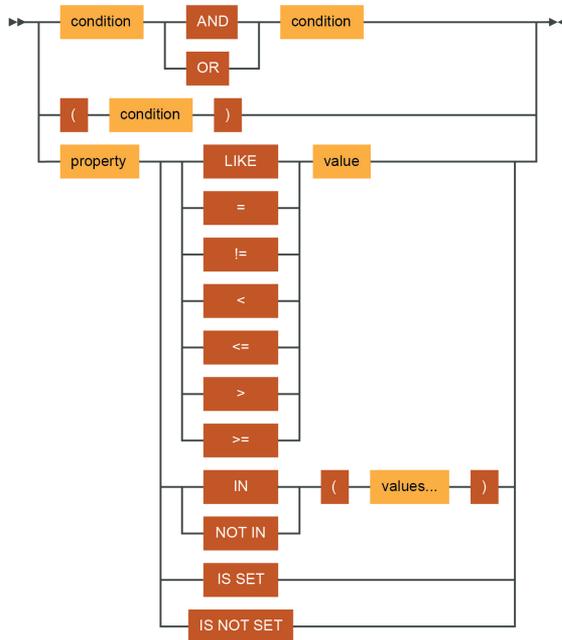


次に例を示します。

- 1 Virtual machines
 - 2 Hosts
 - 3 Flows
 - 4 MTU Mismatch Events
 - 5 Problems
- [フィルタ]: フィルタの構文は次のとおりです。



条件の構文は次のとおりです。



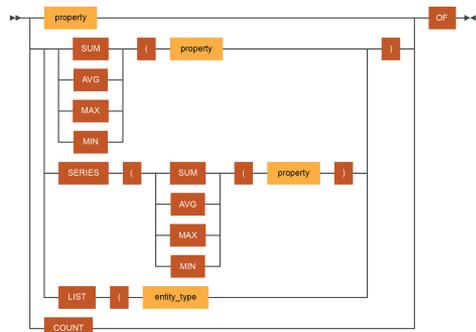
フィルタ句を使用して、検索結果をフィルタできます。フィルタ句の条件は、プロパティ、比較演算子、および値で構成されます。条件を論理演算子と組み合わせて、複雑な条件を形成できます。以下に、使用できる演算子の一覧を示します。

演算子	例
=	flows where source ip address = '10.16.240.0/24' flows where flow type = 'Source is VM'
!=	vms where ip address != '10.17.0.0/16'
>	vms where memory > 4096 mb
<	vms where cpu usage rate < 70%
>=	vms where memory >= 4096 mb
<=	vms where cpu usage rate <= 70%
like	vms where name like 'app'
not like	vms where name not like 'app'
in	flows where port in (22, 23, 80, 443) vm where ip address in (192.168.91.11, 192.168.91.10)
not in	flows where port not in (22, 23, 80, 443) vm where ip address not in (192.168.91.11, 192.168.91.10)
is set	vms where firewall rule is set

演算子	例
is not set	<code>vms where firewall rule is not set</code>
()	<code>flows where (src tier = 'App' and destination tier = 'DB') OR (destination tier = 'App' and source tier = 'DB')</code>
and	<code>flows where src tier = 'App' and destination tier = 'DB'</code>
or	<code>flows where flow type = 'Source is VMKNIC' or flow type = 'Destination is VMKNIC'</code>
一致	<code>vm where name matches '.*'</code> <code>vm where name matches 'a.*'</code> <code>vm where name matches '[a-z]vm-delta[0-9]'</code>
一致しない	<code>vm where name not matches '.*'</code> <code>vm where name not matches 'a.*'</code> <code>vm where name not matches '[a-z]vm-delta[0-9]'</code>
ネストされた「in」演算子	<code>vm where in (vm where name = 'x')</code> <code>vm where in (vm of host where name = 'x')</code> <code>vm where host in (host of vm where name = 'x')</code> <code>vm where name in (name of vm where name = 'x')</code>

- [射影]: クエリ内の射影句は、フィルタリングされたエンティティからどのフィールドを表示する必要があるかを決定します。これはオプションの句です。射影句が指定されていない場合は、デフォルトのフィールドセットが検索結果に表示されます。射影句には、次のいずれかの項目を含めることができます。

- 1 プロパティ
- 2 カウント
- 3 リスト
- 4 集計
- 5 系列



- 1 [プロパティ]: エンティティをエンティティ タイプで検索すると、デフォルトのプロパティ セットが検索結果に表示されます。射影を使用すると、検索結果に表示するフィールドを選択できます。たとえば、`os of vms` は、`OS property` が含まれるすべての仮想マシンを検索結果に一覧表示します。

次にいくつかの例を示します。

- `cpu cores of vms`
- `source ip address of flows`

メトリック プロパティが使用されている場合、メトリック プロパティが y-axis で時刻が x-axis のグラフが、エンティティごとに表示されます。

- 2 [カウント]: カウント クエリを使用すると、あるエンティティ タイプのオブジェクト数を計算できます。次に例を示します。

- `count of vms`
- `count of hosts`
- `count of flows`

- 3 [リスト]: 取得するエンティティにフィルタ条件を適用できない場合は、リスト演算子が役立ちます。次に例を示します。

```
List(host) of vms where memory <= 2gb
```

このクエリは、ホストのリストを取得しますが、仮想マシンにフィルタ条件が適用されています。次にいくつかの例を示します。

- `List(ip address) of vms where cpu cores = 1`

- 4 [集計関数]: 集計関数を使用すると、数値の config または metric プロパティから単一の値を計算できます。検索クエリ言語では、次の集計関数がサポートされています。

- `max`
- `sum`
- `min`
- `avg`

次に例を示します。

- `sum(memory) of hosts`
- `sum(memory), sum(cpu cores) of vms`
- `sum(bytes) of flows`

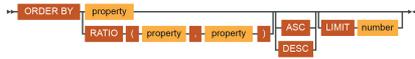
- 5 [系列]: 系列演算子は、メトリック プロパティでの集計の実行に使用します。次に例を示します。

```
series(avg(cpu usage)) of vms where cpu cores = 4
```

このクエリは、4 つの CPU コアを持つすべての仮想マシンの、平均 CPU 使用率を含むグラフを表示します。次に例を示します。

- `series(sum(network usage)) of vms where name like 'app'`
- `series(sum(memory usage)) of vms where name like 'db'`

- `series(avg(cpu usage)), series(avg(memory usage)) of vms`
- [並べ替え]: `order by` 句を使用して検索結果を並べ替えることができます。`order by` 句で使用できるフィールドは1つだけです。デフォルトでは、結果は降順でソートされます。



次に例を示します。

- 1 `vms order by cpu cores`
- 2 `vms order by cpu cores asc`
- 3 `flows order by bytes`

`limit` 句を使用すると、結果の数を制限できます。これは、`order by` 句の後に指定する必要があります。次に例を示します。

```
vms order by memory limit 5
```

- [グループ分け]: エンティティをプロパティごとにグループ化できます。エンティティをプロパティでグループ化すると、デフォルトでは、各グループの結果の数が表示されます。射影を追加することで、任意のプロパティの合計/最大/最小の値を計算できます。`order by` 句を追加すると、結果がソートされます。`order by` または `projection` 句がクエリに含まれる場合は、集計関数が必要です。



```
sum(bytes) of flows group by dest vm
```

このクエリは、射影句に集計関数があるため、有効です。`bytes of flows group by dest vm` のようなクエリは、射影句に集計関数がないため、無効になります。

次に例を示します。

- 1 `vms group by host`
- 2 `sum (bytes) of flows group by dest vm order by sum(bytes)`

2 [エンティティ クエリ]



- a [エンティティ タイプによる検索]: エンティティ タイプを検索することで、あるエンティティ タイプのすべてのエンティティを一覧表示できます。

例: `vms`、`hosts`、`flows`、`nsx managers`

- b [エンティティ名で検索]

- フルネームで検索: エンティティの完全な名前が分かっている場合は、名前を一重引用符で囲んで検索できます。

例: `'prod-68-1'`、`'app1-72-1'`

- 名前の一部で検索：1つの単語または複数の単語で検索すると、入力した単語に一致するすべてのエンティティが取得されます。

例：prod、app1

注： 入力内容にキーワードまたはエンティティ タイプが含まれる場合、検索クエリとして処理される可能性があります。

- エンティティ タイプと名前で検索：エンティティの名前とタイプの両方が分かっている場合、エンティティ タイプとエンティティ名を一緒に使用して検索できます。

例：検索クエリ 'vm app1' は app1 を含むすべての仮想マシンを返します。

3 [計画クエリ]

これらのクエリは、フローの分析による、データセンターのセキュリティ計画に使用できます。

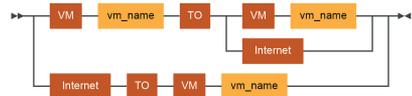


例：

- plan securitygroup1
- plan host1
- plan security

4 [パスクエリ]

これらのクエリを使用して、2 台の仮想マシン間のパス、または仮想マシンからインターネットへのパスを表示できます。



例：

- Vm 'vm1' to Vm 'vm2'
- VM 'vm1' to Internet

注：

- 検索クエリでは、大文字と小文字は区別されません。
 - エンティティ タイプまたは設定プロパティに同義語を使用できます。たとえば、エンティティタイプ 'virtual machine' には、'vm' の同義語があります。
-

Azure 検索クエリ

vRealize Network Insight では Azure エンティティの詳細を検索できます。

次に、いくつかの検索クエリの例を示します。

Azure エンティティ	サンプル クエリ
Microsoft Azure	Azure
Azure アプリケーション セキュリティ グループ	Azure Application Security Group where Azure Virtual Network = 'Test-vnet2'
Azure データ ソース	Azure Data Source
Azure NSG ルール	Azure NSG Rule where Action = 'ALLOW'
Azure ネットワーク インターフェイス	Azure Network Interface where Azure Virtual Network = 'Test-vnet2'
Azure ネットワーク セキュリティ グループ	Azure Network Security Group where Subscription = 'vRNI-dev'
Azure ルート	Azure Route where Route Table = 'TestRouteTable'
Azure ルート テーブル	Azure Route Table where Azure Virtual Network = 'aks-vnet-28255566'
Azure サブネット	Azure Subnet where Azure Virtual Network = 'vrni-01-vnet'
Azure サブスクリプション	Azure Subscription
Azure 仮想マシン	Azure Virtual Machine where Azure Application Security Group = 'TestASG'
Azure 仮想ネットワーク	Azure Virtual Network where Azure Peer Virtual Network = 'vrni-01-vnet'

Cisco ACI エンティティ

次に、検索を実行できる Cisco ACI エンティティのいくつかを示します。

注： エンティティの先頭に `aci` が付けられます。

- `aci application profile`
- `aci bridge domain`
- `aci endpoint group`
- `aci fabric`
- `aci switch`
- `aci tenant`

次に、いくつかの検索クエリの例を示します。

- `aci fabric 'ACI-Demo-Fabric'` : このクエリは、ACI ファブリック内のテナント、スイッチ、およびコントローラに関する情報を取得します。

The screenshot displays the vRealize Network Insight interface for a Fabric ACI-Demo-Fabric. The top navigation bar shows the current view and time. The main content area is divided into several sections:

- Timeline:** Shows a time range of 1 day, with a 'Show Changes' checkbox and a timeline from 12:00 to 11:16 on 08/22.
- Events with this object:** Displays 0 events for the selected time range, with a 'No data to show' message.
- Fabric Tenants:** Lists 26 entities, including:
 - ACI-Ops (Application Profile: App-Centric-Test [1 more], ACI Manager: ACI-Demo-Fabric)
 - HNB-PAN (Application Profile: pandemo, ACI Manager: ACI-Demo-Fabric)
 - Default (Application Profile: sandmq1, ACI Manager: ACI-Demo-Fabric)
- Fabric Switches:** Lists 5 entities:
 - NEX-93180-B-Demo (Role: leaf, Node ID: 102, Infra IP Address: 10.0.72.68)
 - NEX-9372-C-Demo (Role: leaf, Node ID: 103, Vendor: Cisco Systems, Inc.)
 - NEX-9336-B-Demo (Role: spine, Node ID: 202, Infra IP Address: 10.0.72.93)
- Fabric Controllers:** Lists 1 entity:
 - APIC-Demo-1 (Node ID: 1, Infra IP Address: 10.0.0.1, OOB Management Address: 10.255.139.149)

- aci switches by role : このクエリは、ACI ファブリック内のさまざまなリーフ スイッチまたはスパイン スイッチに関する情報を取得します。

スイッチ リストからスイッチ名をクリックすると、その詳細が表示されます。

The screenshot shows the 'aci switches by role' query results in vRealize Network Insight. The interface includes a filters sidebar and a main results table:

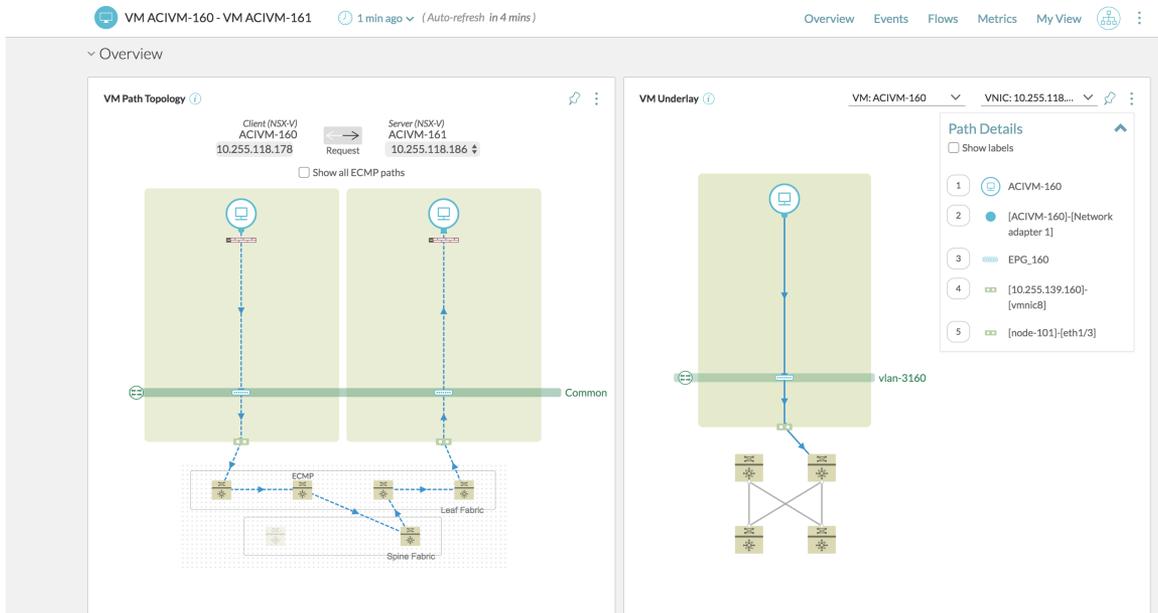
Filters:

- Role:
 - All
 - leaf (3)
 - spine (2)

Results Table:

Entity Name	Role	Node ID	Infra IP Address	OOB Management Address	Vendor
NEX-93180-B-Demo	leaf	102	10.0.72.68	10.255.139.151	Cisco Systems, Inc.
NEX-9372-C-Demo	leaf	103			Cisco Systems, Inc.
NEX-93180-A-Demo	leaf	101	10.0.72.69	10.255.139.150	Cisco Systems, Inc.
NEX-9336-B-Demo	spine	202	10.0.72.93	10.255.139.153	Cisco Systems, Inc.
NEX-9336-A-Demo	spine	201	10.0.72.94	10.255.139.152	Cisco Systems, Inc.

- aci endpoint group : このクエリは、関連付けられた仮想マシン、ブリッジ ドメイン、および VRF を持つ エンドポイント グループのリストを取得します。
- aci application profile 'Production' : このクエリは、含まれているエンドポイント グループと仮想 マシンを持つ本番環境のアプリケーション プロファイルを取得します。
- VMware VM 'ACIVM-160' to VMware VM 'ACIVM-161' : このクエリは、2 台の仮想マシン間の仮想マシ ン間パスを示します。



- IP アドレスを使用して検索することにより、ポート、エンドポイント グループ、ブリッジ ドメインの詳細を取得できます。

Showing 2 results for Entities with keywords "10.114.219.158" at Mar 25, 15:10

2 entities

Endpoint Group (1)

Mgmt-1201	Application Profile NSXInfra	Bridge Domain BD-Mgmt	Encap vlan-1201	Number of VMs 0	Endpoints 00:0C:29:44:70:D8 10.114.21... [17 more]
-----------	---------------------------------	--------------------------	--------------------	--------------------	---

Switch Port (1)

[node-104]-[eth1/19]	Operational Status Up	Administrative Status Up	Mac Address 00:D7:8F:85:89:7B	MTU 9000	Interface speed 10 Gbps
----------------------	--------------------------	-----------------------------	----------------------------------	-------------	----------------------------

- MAC アドレスを使用して検索することにより、ポート、エンドポイント グループ、ブリッジ ドメインの詳細を取得できます。

Showing 2 results for Entities with keywords "00:0c:29:44:70:d8" at Mar 25, 15:06

2 entities

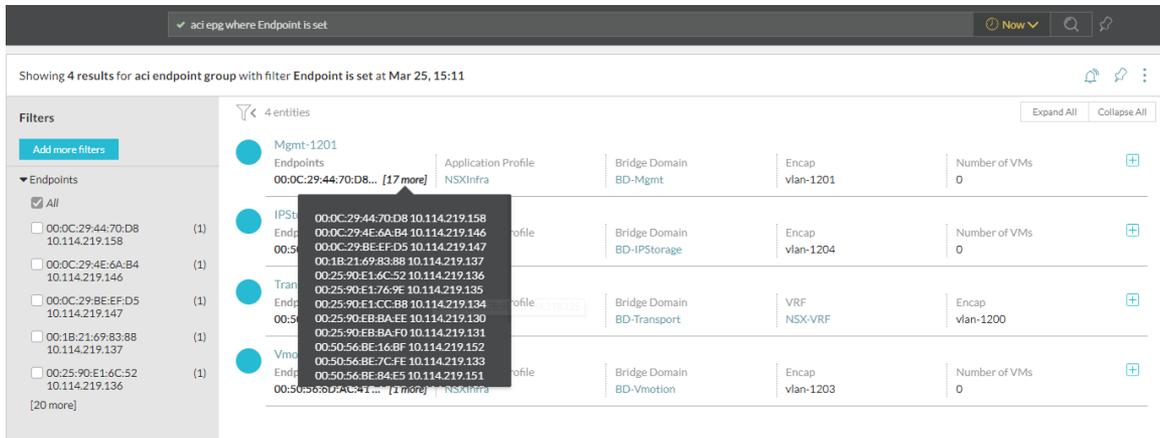
Endpoint Group (1)

Mgmt-1201	Application Profile NSXInfra	Bridge Domain BD-Mgmt	Encap vlan-1201	Number of VMs 0	Endpoints 00:0C:29:44:70:D8 1... [17 more]
-----------	---------------------------------	--------------------------	--------------------	--------------------	---

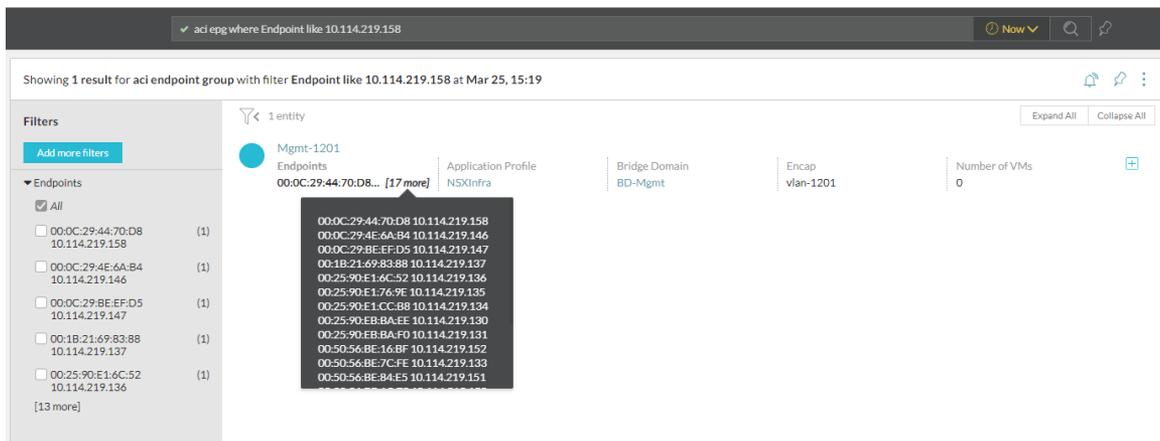
Switch Port (1)

[node-104]-[eth1/19]	Operational Status Up	Administrative Status Up	Mac Address 00:D7:8F:85:89:7B	MTU 9000	Interface speed 10 Gbps
----------------------	--------------------------	-----------------------------	----------------------------------	-------------	----------------------------

- エンドポイント グループを検索することにより、関連付けられたエンドポイントのリストを取得できます。



- エンドポイントを検索できます。



Fortinet 検索クエリ

vRealize Network Insight では Fortinet エンティティの詳細を検索できます。

次に、いくつかの検索クエリの例を示します。

Fortinet エンティティ	サンプル クエリ
Fortinet ポリシー パッケージ	Fortinet Policy Package where Domain Manager = 'ADOM_NAME'
Fortinet ポリシー	Fortinet Policy where Source IP = '10.0.0.15'
Fortinet アドレス	Fortinet Address where Address Type = 'ipmask'
Fortinet 動的アドレス	Fortinet Dynamic Address where Domain Manager = 'ADOM_NAME'
Fortinet 動的アドレス グループ	Fortinet Dynamic Address Group where Domain Manager = 'ADOM_NAME'
Fortinet サービス	Fortinet Service where port = 5900
Fortinet サービス グループ	Fortinet Service Group where Manger = '10.0.15.101'

Fortinet エンティティ	サンプル クエリ
Fortinet ADOM	Fortinet ADOM where Manager ID = '10.0.15.101'
Fortinet VDOM	Fortinet VDOM where Domain Manager = 'ADOM_NAME'
Fortinet 動的インターフェイス	Fortinet Dynamic Interface where Domain Manager = 'ADOM_NAME'

Infoblox DNS データによるフローの強化

vRealize Network Insight は、DNS 情報の 2 つのソースをサポートします。

- インポートされた CSV ファイル
- Infoblox DNS

注： Infoblox DNS と CSV ファイルの間に競合がある場合は、Infoblox DNS からの情報が優先されます。

さまざまな検索クエリを使用して、フロー内の DNS エントリのソースに関する詳細を確認できます。

表 20-1.

キーワード	サンプル検索クエリ	説明
DNS Provider	Flows where DNS Provider='Infoblox'	DNS データが Infoblox から取得されるフローのリストを提供します。
DNS Provider	Flows where DNS Provider='CSV'	DNS データが CSV から取得されるフローのリストを提供します。
Source DNS Provider	Flows where Source DNS Provider='Infoblox'	ソース IP アドレスの DNS プロバイダが Infoblox であるフローのリストを提供します。
Destination DNS Provider	Flows where Destination DNS provider='Infoblox'	ターゲット IP アドレスの DNS プロバイダが Infoblox であるフローのリストを提供します。

Kubernetes エンティティの一般的な検索クエリ

vRealize Network Insight で Kubernetes エンティティの詳細を検索できます。

一般的なクエリ

- フローの検索：`flows where Kubernetes オブジェクト = オブジェクト名`
例：`flows where Kubernetes Cluster = 'Production'`
- サービス スケールの表示：`kubernetes pods group by Kubernetes Services`
- ノードの負荷の表示：`kubernetes Pods group by Kubernetes Node`
- ノードの健全性の表示：`MemoryPressure and PIDPressure and DiskPressure and Ready of Kubernetes Node`

- フローのコンプライアンスの表示 : flows from Kubernetes Object *オブジェクトの名前* to Kubernetes Object *オブジェクトの名前*

例 : flows from Kubernetes Namespace '*PCI*' to Kubernetes Namespace '*Non-PCI*'

- バス トポロジの表示 :
 - Kubernetes サービス *service name* から Kubernetes サービス *service name*
 - Kubernetes サービス *service name* から Kubernetes ポッド *pod name*
 - Kubernetes ポッド *pod name* から Kubernetes ポッド *pod name*

表 20-2. Kubernetes オブジェクトに対するクエリ

Kubernetes オブジェクト	クエリ	説明
名前空間	<ul style="list-style-type: none"> ■ kubernetes namespace where L2 Networks = '<i>a</i>' ■ list(Kubernetes Node) of Kubernetes Pod where Kubernetes Namespace = '<i>a</i>' 	<ul style="list-style-type: none"> ■ L2 ネットワーク 「<i>a</i>」 に接続されている Kubernetes 名前空間を返します ■ Kubernetes 名前空間が 「<i>a</i>」 である Kubernetes ノードのリストを返します
ポッド	<ul style="list-style-type: none"> ■ NSX-T Logical port where connectedto.modelKey in (modelKey of kubernetes nodes) order by Tx Packets desc ■ NSX-T Logical port where connectedto.modelKey in (modelKey of kubernetes pods) and Rx Packet Drops > 0 ■ new kubernetes pod in last 1 hour 	<ul style="list-style-type: none"> ■ 転送されたパケットに基づいて、ノードに接続されている論理ポートのリストを降順で返します ■ Kubernetes ポッドに接続され、かつドロップされた受信パケットが 0 よりも多い論理ポートのリストを返します ■ 直近の 1 時間で検出された新しい Kubernetes ポッド
サービス	<ul style="list-style-type: none"> ■ kubernetes pods where kubernetes services is not set ■ kubernetes pods group by Kubernetes Services, Kubernetes Cluster 	<ul style="list-style-type: none"> ■ サービスがない Kubernetes ポッドのリスト ■ 各サービスで実行されているポッドの数
ノード	<ul style="list-style-type: none"> ■ kubernetes nodes where Ready != 'True' ■ kubernetes node where Virtual Machine = 'vm-<i>a</i>' 	<ul style="list-style-type: none"> ■ 不良な Kubernetes ノードのリスト ■ 「vm-<i>a</i>」 仮想マシンの一部となっている Kubernetes ノード
フロー	<ul style="list-style-type: none"> ■ flows where kubernetes service is set ■ flows where source kubernetes node = '<i>a</i>' 	<ul style="list-style-type: none"> ■ 送信元または宛先の Kubernetes サービスがあるフローのリスト ■ 送信元 Kubernetes ノードが 「<i>a</i>」 または宛先 Kubernetes ノードが 「<i>a</i>」 のフローのリスト

表 20-3. 追加クエリ

エンティティ/コンポーネント	クエリ	説明
Kubernetes エンティティを持つアプリケーション	application where virtual member = 'service- <i>a</i> '	Kubernetes サービス 「service- <i>a</i> 」 がメンバーになっている、すべてのアプリケーションのリスト
	application where virtual member = 'service- <i>a</i> ' and virtual member.Kubernetes Namespace = 'namespace- <i>b</i> '	Kubernetes サービスが 「service- <i>a</i> 」 かつ Kubernetes 名前空間 「namespace- <i>b</i> 」 がメンバーである、すべてのアプリケーションのリスト

表 20-3. 追加クエリ (続き)

エンティティ/コンポーネント	クエリ	説明
	tier where virtual member = 'service-a' and virtual member.Kubernetes Namespace = 'namespace-b'	Kubernetes サービスが「service-a」および Kubernetes 名前空間「namespace-b」がメンバーである、すべての階層のリスト
	count of applications where Virtual Member in (kubernetes services)	メンバーが Kubernetes サービス タイプのアプリケーションの数
	count of applications where virtual member in (kubernetes services where Kubernetes Namespace = 'sock-shop')	Kubernetes 名前空間「sock-shop」下にある Kubernetes サービス タイプのメンバーであるアプリケーションの数
	list(virtual member) of applications where Name = 'app-1' and virtual member.Kubernetes Cluster is set	アプリケーション「app-1」メンバーとしてすべての Kubernetes サービスのリスト
メトリック	nsx-t logical port where (ConnectedTo in (Kubernetes Pods where kubernetes cluster is set)) and Rx Packet Drops > 0 group by ConnectedTo order by max(Rx Packet Drops)	Kubernetes ポッドごとの受信パケット ドロップのグループ
	nsx-t logical port where (ConnectedTo in (Kubernetes Nodes where kubernetes cluster is set)) and Rx Packet Drops > 0 group by ConnectedTo order by max(Rx Packet Drops)	Kubernetes ノードごとの受信パケット ドロップのグループ
	nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/project:' order by Rx Packet Drops	Kubernetes 名前空間ごとの受信パケット ドロップのグループ
	nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/project:<namespace name>'	特定の名前空間ごとのパケット ドロップ
	nsx-t logical port where (ConnectedTo in (Kubernetes Pods where kubernetes cluster is set)) and Rx Packet Drops > 0 group by ConnectedTo.Kubernetes service order by max(Rx Packet Drops)	Kubernetes サービスごとのパケット ドロップのグループ
	flows where firewall action = 'DROP' group by Kubernetes Service	Kubernetes サービスごとのドロップ フローのグループ
	flows where firewall action = 'DROP' group by source Kubernetes Namespace	Kubernetes 名前空間ごとのドロップしたすべてのフロー グループのリスト
Kubernetes イベント	Kubernetes events where Problem Entity = '<pod/namespace/node Name>'	指定された Kubernetes エンティティのすべての Kubernetes イベントのリスト。Kubernetes エンティティは、ポッド、名前空間、ノードのいずれかになります
	Kubernetes events where Event code = 'ImagePullBackOff' in last 24 hours	過去 24 時間のタイプが「ImagePullBackOff」の Kubernetes イベントのリスト
	Kubernetes events where problem entity.Kubernetes Cluster = '<cluster-a>'	指定されたクラスタに対するすべての Kubernetes イベントのリスト

ロード バランサに関連するサンプル検索クエリ

次のサンプル クエリを使用すると、ロード バランサに関連するデータをフィルタまたは検索できます。

- `vm where lbServiceNodes is set` - 負荷が分散されているアプリケーションをホストしているすべての仮想マシンを一覧表示します。
- `vm where lbServiceNodes is set and PowerState != 'POWEREDON'` - ロード バランシングされたアプリケーションをホストしているものの、現在機能していないすべての仮想マシンを一覧表示します。
- `pool member where state = 'DISABLED'` - 無効になっているすべてのプール メンバーを表示します。
- `Count of Pool Memebbers where Service Port = '80'` - ポート 80 で実行されている特定のタイプのサービスについて、すべてのプール メンバーの数を示します。
- `service node where virtual machine is not set` - アプリケーション サーバとして物理サーバを使用しているすべてのサービス ノード、または仮想マシンをホストして vRealize Network Insight に追加されていない vCenter Server を一覧表示します。

NSX ファイアウォール ルールの検索クエリ

vRealize Network Insight では、NSX ファイアウォール ルールを検索できます。

表 20-4. NSX ファイアウォール ルール クエリ

検索クエリ	説明
<code>VM where incoming rules.Source Any</code>	任意の送信元を含むルールを表示します (特定のポートと組み合わせることが可能です)。
<code>Firewall rule where action = allow and service any = true</code>	すべてのポートを許可するファイアウォール ルールを表示します。
<code>Firewall Rule Masked Event</code>	未使用のファイアウォール ルールのリストを表示します。
<code>New firewall rules in last 24 hours</code>	過去 24 時間に作成されたファイアウォール ルールを表示します。
<code>New firewall rules in last 7 days</code>	過去 7 日に作成されたファイアウォール ルールを表示します。
<code>New firewall rules in last 30 days</code>	過去 30 日に作成されたファイアウォール ルールを表示します。
<code>Firewall rule where flow is not set</code>	すべての非アクティブなファイアウォール ルールのリストを表示します。
<code>Flow group by firewall rule</code>	各ファイアウォール ルールにヒットするフローの数を表示します。
<code>Security group where Indirect Incoming Rules is not set and Indirect Outgoing Rules is not set and Direct Incoming Rules is not set and Direct Outgoing Rules is not set</code>	使用されていないセキュリティ グループを表示します。
<code>Ipsset where Indirect Incoming Rules is not set and Indirect Outgoing Rules is not set and Direct Incoming Rules is not set and Direct Outgoing Rules is not set</code>	使用されていない IPSet を表示します。

表 20-4. NSX ファイアウォール ルール クエリ (続き)

検索クエリ	説明
Flow where rule id in (1011, 1012, 1013)	特定のルール ID にヒットするフロー。
Flow where application = appl	アプリケーションにヒットするフロー。

- 未使用のファイアウォール ルール
- ルール イベントをマスキングするファイアウォール ルール

VMware SD-WAN 検索クエリ

vRealize Network Insight で VMware SD-WAN エンティティの詳細を検索できます。

次に、いくつかの検索クエリの例を示します。

VMware SD-WAN エンティティ	サンプル クエリ
VeloCloud クラスタ	VeloCloud Cluster where Description = 'cluster one'
VeloCloud データ ソース	VeloCloud Data Source where Enabled = true
VeloCloud Edge	VeloCloud Edge where Activation State = 'Activated'
VeloCloud エンタープライズ	VeloCloud Enterprise where Name = 'VMWare - vRNI'
VeloCloud ゲートウェイ	VeloCloud Gateway where City = 'Ashburn'
VeloCloud レイヤー 2 ネットワーク	VeloCloud Layer2 Network where Network = '172.16.40.2/24'
VeloCloud リンク	VeloCloud Link where Link Uptime = 100%
VeloCloud プロファイル	VeloCloud Profile where Name = 'APProfile'

VMware SD-WAN エンティティ	サンプル クエリ
VeloCloud セグメント	<code>VeloCloud Segment where Vendor ID = '1'</code>
VeloCloud ビジネス ポリシー	<code>VeloCloud Business Policy where Application = 'skype'</code> <code>VeloCloud Business Policy where scope = 'Edge'</code> <code>VeloCloud Business Policy where Source IP = 10.79.46.0</code> <code>VeloCloud Business Policy where OS = 'Linux'</code> <code>VeloCloud Business Policy where Source VLAN ID = '1'</code> <code>VeloCloud Business Policy where Link Policy = 'Fixed'</code> <code>VeloCloud Business Policy where Priority = 'High'</code> <code>VeloCloud Business Policy where Service Class = 'Real Time'</code> <code>VeloCloud Business Policy where Route Policy = 'Gateway'</code> <code>VeloCloud Business Policy where Route Type = 'edge2cloud'</code> <code>flows where Velocloud business policy = 'EdgeToInternet'</code>

VMC SDDC 検索クエリ

vRealize Network Insight で VMC SDDC エンティティの詳細を検索できます。

次に、いくつかの検索クエリの例を示します。

VMC SDDC エンティティ	サンプル クエリ	説明
NSX Manager	<code>vmc sddc where NSX Manager</code>	VMC SDDC に関連付けられている NSX Manager を示します。
NSX Manager の FQDN	<code>vmc sddc where NSX Manager Fqdn</code>	VMC SDDC 用の NSX Manager の FQDN を示します。

VMC SDDC エンティティ	サンプル クエリ	説明
NSX Manager のプライベート IP アドレス	<code>vmc sddc where NSX Manager Private Ip</code>	VMC SDDC 用の NSX Manager のプライベート IP アドレスを示します。
NSX Manager のパブリック IP アドレス	<code>vmc sddc where NSX Manager Public Ip</code>	VMC SDDC 用の NSX Manager のパブリック IP アドレスを示します。
名前	<code>vmc sddc where Name</code>	VMC SDDC の名前を示します。
組織 ID	<code>vmc sddc where Org Id</code>	SDDC が属する組織 ID を示します。
組織名	<code>vmc sddc where Org Name</code>	SDDC が属する組織名を示します。
リージョン	<code>vmc sddc where Region</code>	SDDC が配置されている AWS リージョンを示します。
vCenter Server の FQDN	<code>vmc sddc where VC FQDN</code>	VMC SDDC 用の vCenter Server の FQDN を示します。
vCenter Server Manager	<code>vmc sddc where VC Manager</code>	VMC SDDC に関連付けられている vCenter Server Manager を示します。
vCenter Server のプライベート IP アドレス	<code>vmc sddc where VC Private Ip</code>	VMC SDDC 用の vCenter Server のプライベート IP アドレスを示します。
vCenter Server のパブリック IP アドレス	<code>vmc sddc where VC Public Ip</code>	VMC SDDC 用の vCenter Server のパブリック IP アドレスを示します。
ベンダー ID	<code>vmc sddc where Vendor ID</code>	VMC SDDC の ID を示します。

AWS エンティティ向け VMware Cloud on AWS

VMware Cloud on AWS NSX Policy Manager に関連するエンティティは、次のとおりです。

- NSX Policy Manager Data Source
- NSX Policy Manager
- NSX Policy Firewall
- NSX Policy Firewall Rule
- NSX Policy Segment
- NSX Policy Based VPN
- NSX Policy Group

注： NSX-T 2.4 および VMware Cloud on AWS が vRealize Network Insight のデータ ソースとして追加されている場合、VMware Cloud on AWS エンティティを取得するには、クエリで **SDDC type = VMC** というフィルタを追加する必要があります。たとえば、VMware Cloud on AWS のポリシー ベース VPN を一覧表示するには、**NSX Policy Based VPN where Tier0 = '' and SDDC Type = 'VMC'** を入力します。

VMware Cloud on AWS エンティティに関連するサンプル検索クエリには、次のようなものがあります。

- `Vms where L2 Network = '' (L2 Network -> NSX Policy Segment)`

- NSX Policy Based VPN where Tier0 = ''
- NSX Policy Based VPN where Local Network = '' (Local Network of Policy Based VPN Rule)
- NSX Policy Based VPN where Remote Network = '' (Remote Network of Policy Based VPN Rule)
- NSX Policy Group where Translated VM = ''
- VM where NSX Policy Group = ''

注:

- NSX Policy Manager は、子グループまたは IPSETS をサポートしていません。そのため、NSX Policy firewall rule where Indirect _____ = '' または NSX Policy group where Indirect _____ = '' などの検索はすべて無効です。
-

高度なクエリ

ここでは、高度なクエリの例をいくつか示します。

各通信パターンのフロー クエリ

- データセンターまたはサイト全体の合計トラフィック (DCI リンク使用)


```
sum(bytes) of flows where ( Dst Manager = 'abc' AND src manager = 'cba') OR ( Dst Manager = 'cba' AND src manager = 'abc')
```
- 合計 VTEP トラフィック
 - sum(bytes) of flows where Flow Type = 'Src is VTEP' or flow type = 'Dst is VTEP' VTEP traffic grouped by VMKNIC
 - sum(bytes) of flows where Flow Type = 'Src is VTEP' or Flow Type = 'Dst is VTEP' group by ip
- その他の管理トラフィック


```
flows where Flow Type = 'Source is VMKNIC' or Flow Type = 'Destination is VMKNIC'
```

集計とグループ分けに関するフロー クエリ

- ソース仮想マシンごとの合計インターネットトラフィック


```
sum(bytes) of flows where Flow Type = 'Internet' group by src vm
```
- 合計バイト数ごとの上位ポート


```
sum(bytes) of flow group by port order by sum(bytes)
```
- ルーティングが設定されたトラフィック ボリュームごとの上位サブネット ペア

```
sum(bytes) of flow where Flow Type = 'Routed' group by Source Subnet Network,
destination subnet network order by sum(bytes)
```

- 合計ペア バイト数ごとの仮想マシンの合計

```
sum(bytes) of flows group by src vm , dest vm order by sum(bytes)
```

- 合計バイト数ごとの上位サーバ仮想マシン/ポート

```
sum(bytes) of flows group by dest vm , port order by sum(bytes)
```

キャパシティの見積もりとサイジングに関するフロー クエリ

- ESX でグループ化されたすべての vm-internet/internet-vm トラフィックの合計バイト数 (Palo Alto サービス仮想マシンのサイジング)

```
sum(bytes) of flows where flow type = 'internet' and (flow type = ' src is vm ' OR
flow type = 'destination is vm ') group by host order by sum(bytes)
```

- 一致するフローに対して集計されたトラフィックの系列 (Palo Alto サービス仮想マシンのサイジング)

```
series( sum(byte rate)) of flows where host = 'ddc1-pod2esx012.dm.democompany.net'
and (Flow Type = 'Source is VM' OR flow type = 'Destination is VM')
```

アプリケーションで役立つクエリ

- 特定のアプリケーションの仮想マシン

```
VM where application = 'CRM'
```

- 特定のアプリケーションからルーティングが設定されたフロー

```
Flows where source application = CRM and Flow Type = 'Routed'
```

- 2 階層間のフロー (一方向)

```
Flows where src tier = 'App' and Destination Tier = 'DB'
```

- 2 階層間のフロー (一方向)

```
Flows where ( src tier = 'App' and destination Tier = 'DB') OR (destination tier =
'App' and source tier = 'DB')
```

仮想マシンと ESX で役立つクエリ

- Prod -Midtier-1 仮想マシンのプロパティ (MAC、IP アドレス、ホストなど)

```
CPU Usage Rate, Network Rate, Memory Usage Rate, mac address, ip , vxlan , host of
vm 'Quality control-VM26'
```

- 仮想マシン数が最大のネットワーク セグメント

```
vm group by l2 network
```

- 仮想マシン数が最大のデータストア

```
vm group by datastore
```

- vSphere バージョンごとのホスト

```
host group by version
```

- vSphere ビルドごとのホスト

```
host group by OS
```

- 特定の UCS シャーシのスロットに配備されたすべてのホスト/ブレード上の全仮想マシン（ネストされたクエリ）

```
vm where host in (host where Blade like 'sys/chassis-1')
```

便利なクエリ：一般的なキャパシティ

- データ ソース数：

```
count of datacenter
```

- クラスタ数

```
count of cluster
```

- ホスト数

```
count of host
```

- 仮想マシン数

```
count of vm
```

- ネットワーク数

```
count of vlan
```

便利なクエリ：ルート

- プライマリ コントローラごとの VNI

```
vxlan group by Primary Controller
```

- プロバイダ エッジ 3 のルート

```
routes where vrf = 'Provider Edge 3'
```

- DMZ DLR のルート

```
NextHop Router of routes where VRF = 'LDR-DMZ'
```

- 指定されたルーターをネクスト ホップとして持つルート

```
routes where NextHop Router = 'California-Edge'
```

便利なクエリ：ファイアウォール ルール

- 2 台の仮想マシン間のファイアウォール ルール

```
firewall rules from 'Prod-Midtier-1' to 'Prod-Db-1'
```

- ANY ソースを持つルール

```
firewall rules where Service Any = true
```

- 特定のルールの仮想マシン

```
vm where Firewall Rule = 'Prod MidTier to Prod DB - DBService '
```

- 任意のポートが許可されるファイアウォール ルール

```
firewall rule where action = allow and service any = true
```

- 特定のファイアウォール ルールにヒットするフロー

```
flows where firewall rule = 'Admin to Prod and Lab - SSH'
```

- システム内の拒否されたフロー

```
flows where firewall action = deny
```

- ゲートウェイ ファイアウォールの表示

```
Firewall Rule where firewall type = 'GatewayFirewall'
```

- 分散ファイアウォールの表示

```
Firewall Rule where firewall type = 'Distributed Firewall'
```

便利なクエリ：一般的なトラフィック パターン

- East-West および North-South のトラフィック数、スイッチされたトラフィックの数、経路指定されたトラフィックの数、および仮想マシン間のトラフィック数

```
plan security in last 7 days
```

便利なクエリ：セキュリティ レンズからのトラフィック

- 上位エンティティ仮想マシンの詳細

```
top 7 vm group by name, Vlan order by sum(Total Network Traffic) in last 7 days
```

- トラフィック量が上位のネットワーク

```
top 7 vlan group by Vlan id, vm count order by sum(Total Network Traffic) in last 7 days
```

- ほとんどの通信が VLAN 内で完結する（物理ファイアウォールまたは L3 境界を越えない）ネットワーク

```
top 7 flow where Flow Type = 'Switched' group by Subnet Network order by sum(Bytes) in last 7 days
```

- ほとんどの通信が VLAN をまたぐ（物理ファイアウォールでボトルネックの問題を生じさせる可能性がある）ネットワーク

```
top 7 flow where Flow Type = 'Routed' group by Source Subnet Network, Destination Subnet Network order by sum(Bytes) in last 7 days
```

- 国外と通信する仮想マシン

```
top 7 flow where Destination Country != 'United States' group by Source VM,
Destination Country order by sum(Bytes) in last 7 days
```

- ストレージ遅延の主な発生源となっているデータストア

```
avg(Read Latency), avg(Write Latency) of top 7 vm group by Datastore, vlan order by
avg(Write Latency) in last 7 days
```

便利なクエリ：コンプライアンス/脆弱性

- 脆弱性のある OS の詳細

```
vm where Operating System like 'Microsoft Windows Server 2003' or Operating System
like 'Microsoft Windows Server 2008' or Operating System like 'Red Hat Enterprise
Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or Operating System
like 'SUSE Linux Enterprise 10' group by vlan, Operating System
```

- 脆弱性のある OS の数

```
count of vm where Operating System like 'Microsoft Windows Server 2003' or
Operating System like 'Microsoft Windows Server 2008' or Operating System like 'Red
Hat Enterprise Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or
Operating System like 'SUSE Linux Enterprise 10'
```

- 古い OS による攻撃対象領域の合計

```
vm where vlan in (vlan of vm where os in ('Microsoft Windows Server 2003',
'Microsoft Windows Server 2008', 'Red Hat Enterprise Linux 6', 'Red Hat Enterprise
Linux 5', 'SUSE Linux Enterprise 10')) group by Vlan

count of vm where vlan in (vlan of vm where os in ('Microsoft Windows Server 2003',
'Microsoft Windows Server 2008', 'Red Hat Enterprise Linux 6', 'Red Hat Enterprise
Linux 5', 'SUSE Linux Enterprise 10'))
```

注： 脆弱性のある OS で推奨されるファイアウォール ルールを取得するには、[脆弱な OS を保護するために推奨されるファイアウォール ルール](#)を参照してください。

時間管理

時間管理により、選択した時間または時間範囲のコンテキスト内で検索クエリを実行できます。過去 24 時間、過去 3 日間などの事前設定のリストから選択できます。さらに、[日時] オプションを使用して特定の日時を指定できるほか、[範囲] オプションを使用して範囲を指定できます。

検索結果

検索結果画面には、特定の検索に一致する、目的のエンティティの詳細リストが表示されます。画面自体には、エンティティのリスト、対応するプロパティ、検索結果を絞り込むためのファセットなどの多岐にわたる情報が含まれています。

検索結果の各エントリを展開したり折りたたんだりして、特定のエントリに関する詳細情報を表示することもできます。また、検索ごとに通知を作成することも可能です。

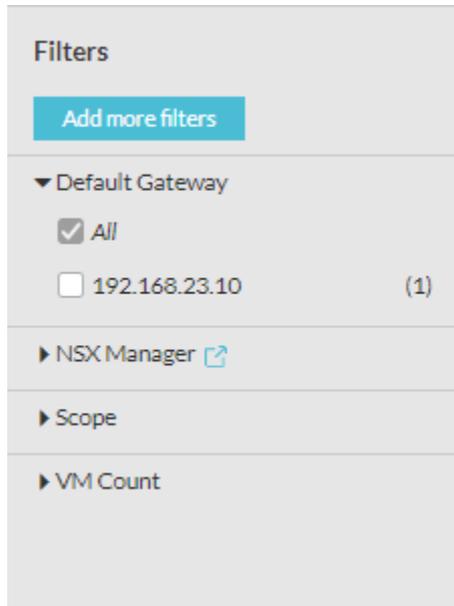
注： 検索結果やエンティティの画面内の特定のプロパティをポイントすると、そのプロパティに関する詳細情報のツールチップを表示できます。

次の図は、過去のある時点に対する `num vms > 0` 検索クエリによる、VXLAN の検索結果を示しています。

Showing 12 results for Vxlan with filter Num VMs > 0 at

Entity Name	Number of VMs	NSX Manager	Scope	Segment ID	Network Address
Siteb-Aundh-LS	3	10.197.17.114	Global	5006	192.168.23.0/24
Siteb_P-seattle-vxlan	3	10.197.17.229	Global	5000	172.17.1.0/24
Siteb_P-redmond-vxlan	2	10.197.17.229	Global	5001	172.17.2.0/24
Siteb-Wagholi-LS	2	10.197.17.114	Global	5005	192.168.26.0/24
Siteb-pashan-ls-1	2	10.197.17.114	Global	5002	192.168.24.0/24
Siteb_P-transit-vxlan-2	2	10.197.17.229	Global	5005	172.17.6.0/24
Siteb_P-transit-vxlan-1	2	10.197.17.229	Global	5004	172.17.5.0/24
Siteb-Transit-LS-1	1	10.197.17.114	Global	5003	192.168.21.0/24

フィルタ



検索結果が表示されたら、必要に応じて左側のペインの [フィルタの追加] をクリックします。検索結果を絞り込むために使用できる一連のフィルタ カテゴリが表示されます。各カテゴリで使用できるフィルタの数は、カテゴリの横にある小さなボックスに記載されています。カテゴリで適用可能なフィルタとフィルタの概要を確認し、適用するフィルタをクリックします。フィルタ検索ボックスを使用して特定のフィルタを検索することも可能で、検索クエリに一致するフィルタが vRealize Network Insight によって自動的に表示されたら、そのフィルタをクリックして適用できます。各フィルタには、検索結果を絞り込むためのプロパティがいくつかあります。フィルタのいずれかのフィルタ プロパティを選択すると、選択したプロパティが検索結果で強調表示されます。

vCenter Server タグ

vRealize Network Insight は、検索と計画用に vCenter Server タグを提供します。

vCenter Server タグとカスタム属性に基づいて、仮想マシンの検索を実行できます。たとえば、次のクエリを使用して、タグを使用した検索を行えます。

```
vm where tag = '{keyname}:{value}'
```

各タグは特定のカテゴリに属します。上記の例では、keyname はタグが属するカテゴリで、value はタグの名前です。

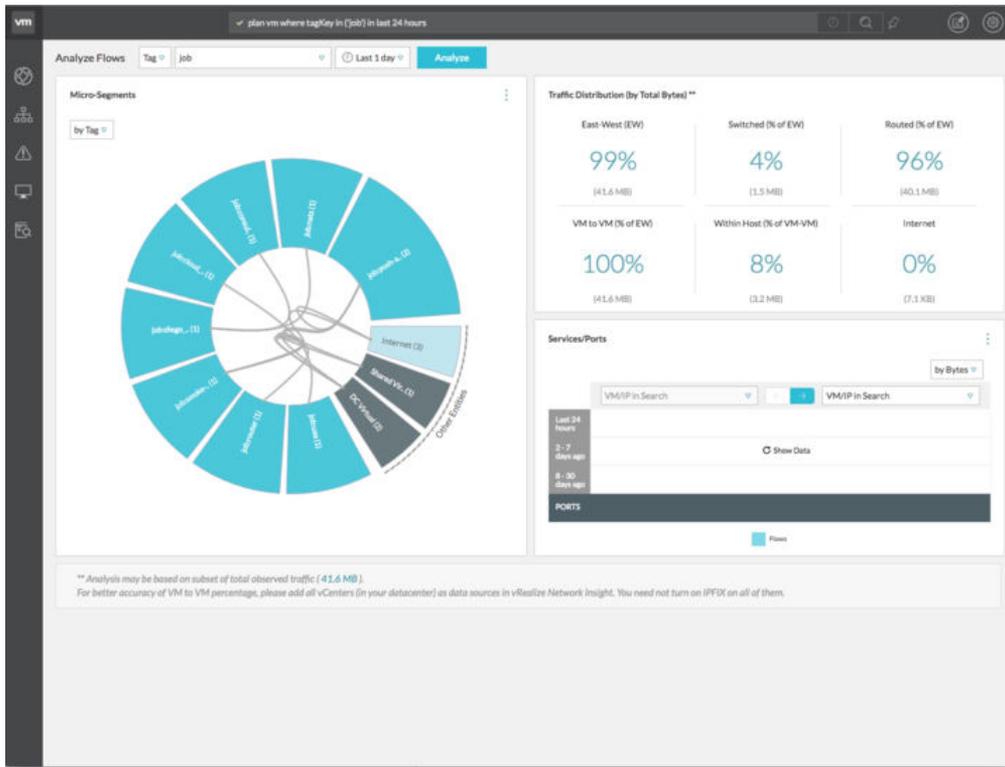
また、name キーを使用し、vCenter Server タグまたはカスタム属性を使用して、仮想マシンに代替名を指定することもできます。この代替名は、other names プロパティとして表示されます。また、代替名を使用して、検索やパス クエリを行うこともできます。

たとえば、次のクエリがサポートされます。

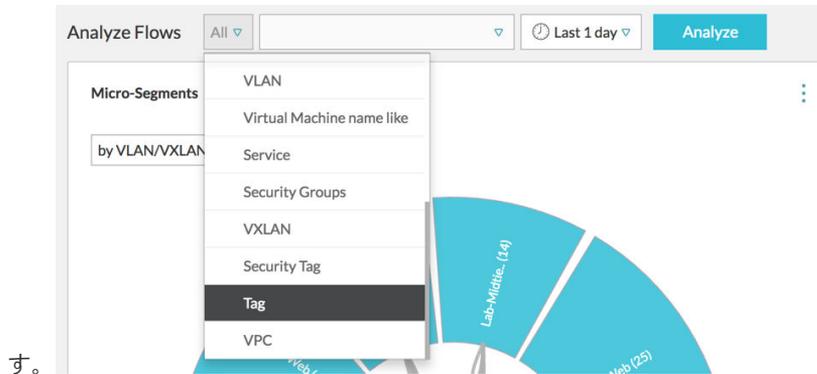
```
vm "other-name-1"
  vm "other-name-1" to vm "other-name-2"
```

この例では、other-name-1 と other-name-2 は、name キーまたは name カテゴリに属するタグを持つカスタム属性です。

図に示すように、vCenter Server タグを使用してネットワーク内のフローを分析することもできます。

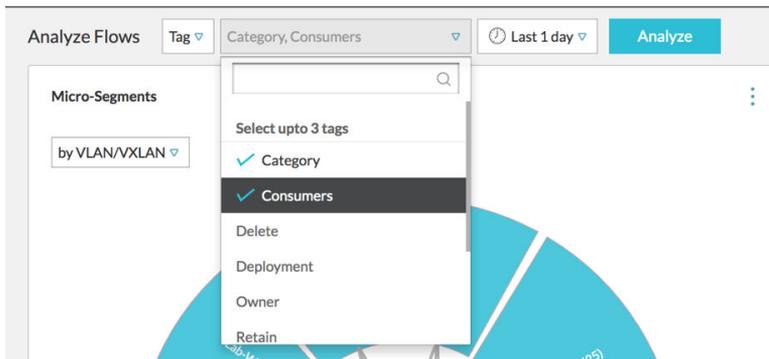


vCenter Server タグを使用するには、[フローの分析] ドロップダウン リストから [タグ] オプションを選択しま

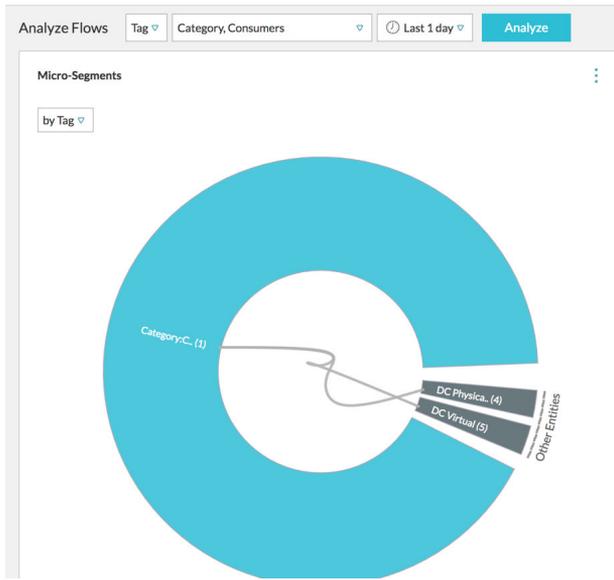


す。

このレベルで、最大 3 つのタグを選択することもできます。タグを選択したら、[分析] をクリックします。



[グループ化基準] で、[タグ] が選択されています。



vRealize Network Insight のディザスタ リカバリの計画

21

VMware Site Recovery Manager (SRM) は、ポリシーベースの管理、無停止のテスト、および自動オーケストレーションを提供する、ディザスタ リカバリ自動化ソフトウェアです。vRealize Network Insight は SRM 8.1 以降のバージョンをサポートします。vRealize Network Insight を保護するために、SRM はディザスタ リカバリプランを実行するすべての側面を自動化してリカバ리를高速化し、手動プロセスの使用に伴うリスクを排除します。

SRM のインストール、アップグレード、および設定の詳細については、[VMware Site Recovery Manager のドキュメント](#)を参照してください。

vRealize Network Insight のディザスタ リカバリ操作の前提条件は次のとおりです。

- vSphere Replication がインストールされ、設定されていることを確認します。
- SRM は、保護サイトとリカバリ サイトの両方にデプロイして設定する必要があります。
- リカバリ プランおよびその他のコンポーネントの作成を進める前に、SRM ユーザー インターフェイス内からサイトのペアリングが適切に設定されていることを確認します。
- VMware vSphere Replication は、コンテキスト内の vRNI 環境の保護されている各ノードに対して有効にする必要があります。VMware vSphere Replication を有効にするときは、障害発生時のデータ消失が最小になるように vRealize Network Insight のノード サイズと使用状況を考慮して、十分な目標復旧ポイント (RPO) を指定します。レプリケーションの詳細については、[VMware vSphere Replication のドキュメント](#)を参照してください。
- vRealize Network Insight の個別の保護グループを作成していることを確認します。小規模環境および非分散型環境の場合は、すべての仮想マシンが同じ保護グループに含まれていることを確認します。分散型環境の場合は、リカバ리를円滑に行えるように、すべてのプラットフォームを単一の保護グループに配置することをお勧めします。コレクタは、異なる保護グループに配置できます。
- リカバリ プランを作成し、このプランに vRealize Network Insight 仮想マシンを含む保護グループを追加します。プラットフォーム ノードを含む保護グループの優先順位が高くなっていることを確認します。リカバリプランで、プライマリ プラットフォーム ノードが他のプラットフォーム ノードよりも高い優先順位のグループに配置されていることを確認します。
- 現在、SRM を使用したどのタイプの IPv4 カスタマイズもサポートされていません。

vRealize Network Insight 仮想マシンは、同一のネットワーク構成に移行またはリカバリすることをお勧めします。SRM の推奨に従って、テスト実行を定期的に行い、基盤となるインフラストラクチャと設定された RPO 制限に既存のプランが対応していることも確認できます。

- vRealize Network Insight 仮想マシンを同一のネットワーク構成に移行またはリカバリします。

リカバリ サイトのネットワーク構成が保護サイトと同じで、同一構成のネットワーク間でマッピングが作成されている場合、すべてのレプリケートされた vRealize Network Insight 仮想マシンが同じ IP アドレスで起動するように設定します。この理由は、これらの仮想マシンが、保護されたノードになっているためです。リカバリされたシステムは、計画した移行またはディザスタ リカバリが正常に完了した後に動作します。

- リカバリ サイトに保護サイトと同じネットワークがない場合は、リカバリ プランの IP アドレスのカスタマイズを指定しないでください。このシナリオでは、アプライアンス仮想マシンのリカバリに SRM を使用します。リカバリ後のネットワークを構成するには、次のように手動でネットワーク設定を割り当てます。
- 1 すべてのプラットフォームノードで、`change-network-settings` コマンドを同時に実行します。
 - 2 Platform1、Platform2、および Platform3 のノードで `update-IP-change` コマンドを連続して実行します。
 - 3 コレクタ ノードで `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Platform1>` を実行します。
 - 4 サービスの状態を確認します。プラットフォーム ノードの一部のサービスが実行されていない場合は、推奨されている順序でノードを再起動します。

注： 上記のコマンドの詳細については、「vRealize Network Insight Command Line Reference Guide」を参照してください。

この章には、次のトピックが含まれています。

- [ディザスタ リカバリ シナリオの例](#)

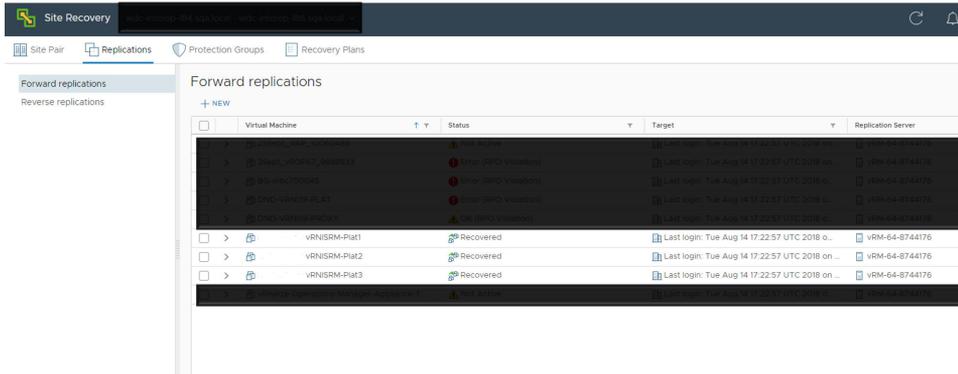
ディザスタ リカバリ シナリオの例

ここでは、vRealize Network Insight のディザスタ リカバリ (DR) に関するサンプルシナリオの手順を示します。

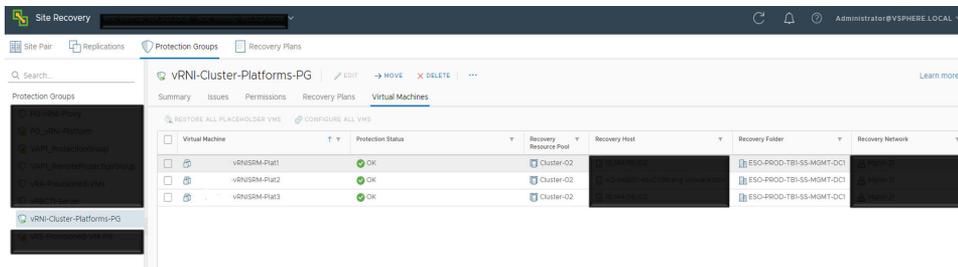
手順

- 1 保護サイトとリカバリ サイトの両方で SRM が設定されていることを確認します。

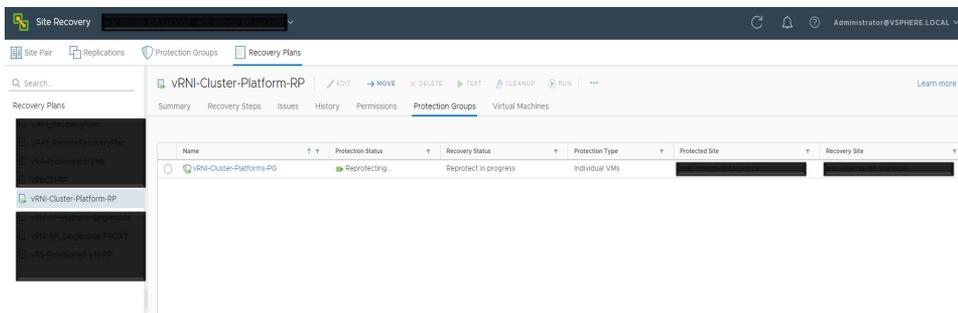
- 2 保護対象の各 vRealize Network Insight ノードのレプリケーションを設定します。レプリケーションの設定中に、vRealize Network Insight インスタンスの適切な目標復旧ポイント (RPO) 時間を指定します。たとえば、単一のプラットフォームとコレクタ ノード (中サイズ) で構成される vRealize Network Insight 環境の場合、45 分の目標復旧ポイントが適切です。ただし、大きなサイズのブリックを使用するノードがあるクラスタの場合、それに合わせて適切な目標復旧ポイントを指定する必要があります。スナップショット間隔の設定は、ユーザー環境と要件によって異なります。



- 3 保護グループを作成します。保護の対象とする仮想マシンを特定の保護グループに入れます。



- 4 それぞれの保護グループを含むリカバリ プランを作成します。



- 5 テスト リカバリを実行します。これは、リカバリ プランが予期したとおりに機能することを確認することを目的としています。
- 6 SRM では、計画した移行を一定の間隔で実行して、既存の DR プランの整合性を検証することをお勧めしています。

- 7 ここで仮に、リカバリ サイトが、vRealize Network Insight 仮想マシンに強制的に新しい IP アドレスを設定するネットワーク構成になっているとします。この場合、リカバリされた仮想マシンのネットワークに変更が発生することを想定していないリカバリ プランを使用して、vRealize Network Insight 仮想マシンをリカバリします。仮想マシンのリカバリが vRealize Network Insight で成功と報告されたら、新しい IP アドレスを vRealize Network Insight ノードに手動で割り当て、新しい証明書を適用して、クラスタを再初期化します。
- 8 SRM での IPv4 カスタマイズは現在サポートされていないため、回避策として、ネットワークに変更がないかのように、vRealize Network Insight で DR を実行できます。

ネットワーク設定を手動で割り当てるには、次の手順に従います。

- a すべてのプラットフォームノードで、`change-network-settings` コマンドを同時に実行します。
- b Platform1、Platform2、および Platform3 のノードで `update-IP-change` コマンドを連続して実行します。
- c コレクタ ノードで `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Platform1>` を実行します。
- d サービスの状態を確認します。プラットフォーム ノードの一部のサービスが実行されていない場合は、推奨されている順序でノードを再起動します。

この章には、次のトピックが含まれています。

- 一般的なデータ ソースのエラー
- DFW IPFIX を有効にできない

一般的なデータ ソースのエラー

データ ソースを追加すると、いくつかのエラーが発生する場合があります。この表に、それぞれの原因と解決策に関する一般的なエラーのリストを示します。

表 22-1.

エラー テキスト	原因	解決方法
データ ソースからの応答が無効です	vRealize Network Insight プロキシは、データ ソースから受信した情報が想定された形式でないため、情報を処理できません。	一部のデータ プロバイダでは、この問題が断続的に発生し、次のポーリング サイクルでなくなる場合があります。継続して発生する場合は、サポートにお問い合わせください。
プロキシ仮想マシンからデータ ソースにアクセスできません	SSH/REST 上のデータ ソース IP アドレス (ポート 22 または 443) が vRealize Network Insight プロキシ仮想マシンからアクセスできないか、データ ソースが応答していません。このエラーは、データ ソースの追加中に発生します。	ポート 22 または 443 の vRealize Network Insight プロキシ仮想マシンからデータ ソースへの接続を確認してください。データ ソースが実行中で、ファイアウォールが vRealize Network Insight プロキシ仮想マシンからデータ ソースへの接続をブロックしていないことを確認してください。
NSX Controller が見つかりません	[NSX Manager データ ソース] 画面で NSX Controller が選択されていますが、NSX Controller がインストールされていません。	NSX Manager に NSX Controller をインストールし、[NSX Manager データ ソース] 画面で NSX Controller のチェック ボックスを選択します。
データ ソースのタイプまたはバージョンが一致しません	指定されたデータ ソースの IP アドレス/FQDN が、選択されたデータ ソース タイプではありません。	指定されたデータ ソースの IP アドレス/FQDN が選択されたデータ ソース タイプであり、バージョンが vRealize Network Insight でサポートされているバージョンであることを確認します。

表 22-1. (続き)

エラー テキスト	原因	解決方法
データ ソースへの接続中にエラーが発生しました	vRealize Network Insight プロキシ仮想マシンはデータ ソースに接続できません。このエラーは、データ ソースを追加した後に発生します。	ポート 22 または 443 の vRealize Network Insight プロキシ仮想マシンからデータ ソースへの接続を確認してください。データ ソースが実行中で、ファイアウォールが vRealize Network Insight プロキシ仮想マシンからデータ ソースへの接続をブロックしていないことを確認します。
見つかりません	vRealize Network Insight プロキシ仮想マシンが見つかりません。	vRealize Network Insight プロキシ仮想マシンと vRealize Network Insight プラットフォーム仮想マシンとの間でペアリングが実行されているかどうかを確認します。
IPFIX を有効にするための適切な権限がありません	vCenter Server で IPFIX の有効化を試みているユーザーに、DVSwitch.Modify、DVPortgroup.Modify の権限がありません。	ユーザーに適切な権限を付与します。
IP アドレス/FQDN が無効です	データ ソース ページで指定された IP アドレス/FQDN が有効でないか、ありません。	有効な IP アドレス/FQDN アドレスを指定します。
データを受信していません	vRealize Network Insight プラットフォーム仮想マシンは、このデータ ソースの vRealize Network Insight プロキシ仮想マシンからデータを受信していません。	サポートにお問い合わせください。
認証情報が無効です	指定された認証情報が無効です。	正しい認証情報を指定してください。
接続文字列が無効です	データ ソース画面で指定された IP アドレス/FQDN が適切な形式ではありません。	有効な IP アドレス/FQDN アドレスを指定します。
処理の遅れのために最近のデータを使用できない可能性があります	vRealize Network Insight プラットフォーム仮想マシンは、データの処理中に過負荷状態になり、遅れています。	サポートにお問い合わせください。
要求がタイムアウトになりました。やり直してください。	指定された時間内に要求を完了できませんでした。	やり直してください。問題が解決しない場合は、サポートにお問い合わせください。
不明な理由により失敗しました。再試行するか、サポートにお問い合わせください。	不明な理由で要求が失敗しました。	やり直してください。問題が解決しない場合は、サポートにお問い合わせください。
SSH のパスワード認証がデバイスで有効になっている必要があります	追加されたデバイスで、パスワードを使用した SSH ログインが無効になっています。	監視用に追加されたデバイス上の SSH のパスワード認証を有効にします。
SNMP 接続エラー	SNMP ポートへの接続中にエラーが発生しました。	SNMP がターゲット デバイス上で正しく設定されていることを確認します。

DFW IPFIX を有効にできない

vRealize Network Insight では、DFW IPFIX を有効にすることはできません。

問題

Policy Manager または VMware Cloud on AWS のソースを追加するときに、DFW IPFIX を有効にしようとすると、次のエラーメッセージが表示されることがあります。

- 新しいコレクタを追加することはできません。
- 指定されたユーザーには必要なロールがありません。クラウド管理者のロールを持つユーザーのみが IPFIX を有効にできます。

原因

- VMware Cloud on AWS は、DFW IPFIX コレクタ プロファイルに対して 4 つのコレクタのみをサポートします。そのため、既存のプロファイルにすでに 4 つのコレクタがある場合は、

新しいコレクタを追加することはできません

というメッセージが表示されます。

The screenshot shows the 'Settings' page for 'Add a New Policy Manager Account or Source of VMware Cloud on AWS'. The left sidebar contains navigation options like 'Install and Support', 'Accounts and Data Sources', 'Data Management', etc. The main content area shows configuration fields for VCenter, Collector (Proxy) VM, IP Address/FQDN, and CSP Refresh Token. A 'Validate' button has been clicked, resulting in a green 'Validation Successful' message. Below this, there is a checkbox for 'Enable DFW IPFIX' with a warning message: 'No new collectors can be added.' The 'Submit' and 'Cancel' buttons are visible at the bottom.

- ユーザーには書き込み権限がありません。クラウド管理者のロールを持つユーザーのみが、VMware Cloud on AWS Policy Manager で書き込み操作を実行できます。

Settings

- Install and Support
- Accounts and Data Sources
- Data Management
- IP Properties and Subnets >
- Events >
- User Management
- Logs >
- LDAP
- Mail Server
- SNMP Service
- Property Templates
- My Preferences
- System Configuration
- About

Edit Account or Source

VCenter * ⓘ

Collector (Proxy) VM *
Tip: Want to increase capacity of your collector? [Click here](#)

IP Address/FQDN *

CSP Refresh Token * ⓘ

✔ Validation Successful

Enable DFw IPFIX
 Selecting this option will enable distributed firewall to send IPFIX flow record to the collector

! Provided user does not have the required role. Only users with the following role can enable IPFIX: Enterprise Administrator, Cloud Administrator.

Nickname *

Notes

解決方法

- ◆ 新しいコレクタを追加するには、以下を実行する必要があります。
 - 既存のコレクタを削除します。
 - または、新しいプロファイルを作成します。
- ◆ または、ユーザー ロールの問題の回避や修正を行うために、次のいずれかの手順を実行します。
 - クラウド管理者ロールをユーザーに割り当てます。
 - クラウドの管理者のロールを持つユーザーとしてログインします。

vRealize Network Insight を使用した VMware Cloud on AWS へのアプリケーションの移行の計画

23

vRealize Network Insight を使用して、VMware Cloud on AWS または AWS へのアプリケーションの移行に備えて、オンプレミス環境を評価できます。

ステップ	手順	参照
ステップ 1	環境の設定	<ul style="list-style-type: none">■ エンドユーザー使用許諾契約書 (EULA) への同意<ol style="list-style-type: none">a VMware ユーザー アカウントを作成するか、VMware アカウントにログインします。b 登録フォームを更新します。 新しいユーザーは、自分のアカウントを有効にするための E メールを受信します。c VMware の利用条件と EULA に同意します。■ OVA ファイルのダウンロード<ol style="list-style-type: none">a https://my.vmware.com/group/vmware/home で VMware 製品ダウンロード ページにログインします。b vRealize Network Insight を検索します。c 最新の vRealize Network Insight プラットフォームおよびプロキシ OVA ファイルをダウンロードします。■ インストールの準備<ol style="list-style-type: none">a システムの推奨事項および要件を確認してください。b サポート対象の製品とバージョンを確認してください。
ステップ 2	展開	<ol style="list-style-type: none">1 vRealize Network Insight プラットフォーム OVA ファイルを展開します。2 ライセンスを有効にします。3 共有シークレットを生成します。4 vRealize Network Insight プロキシ OVA ファイルを展開します。5 vRealize Network Insight 用の VMware Cloud on AWS ファイアウォール ルールの作成。
ステップ 3	データの追加	<ol style="list-style-type: none">1 vRealize Network Insight にログインします。2 VMware Cloud on AWS vCenter Server の追加。3 VMware Cloud on AWS NSX Manager の追加。
ステップ 4	モデルアプリケーション	<ul style="list-style-type: none">■ アプリケーションの依存関係の分析<ol style="list-style-type: none">a 手動によるアプリケーションの作成b 物理 IP アドレスの階層の作成c アプリケーションの分析d VMware Cloud on AWS : 計画およびマイクロセグメンテーション■ 19 章 推奨されるファイアウォール ルール■ 20 章 検索クエリの操作■ ピンボード

この章には、次のトピックが含まれています。

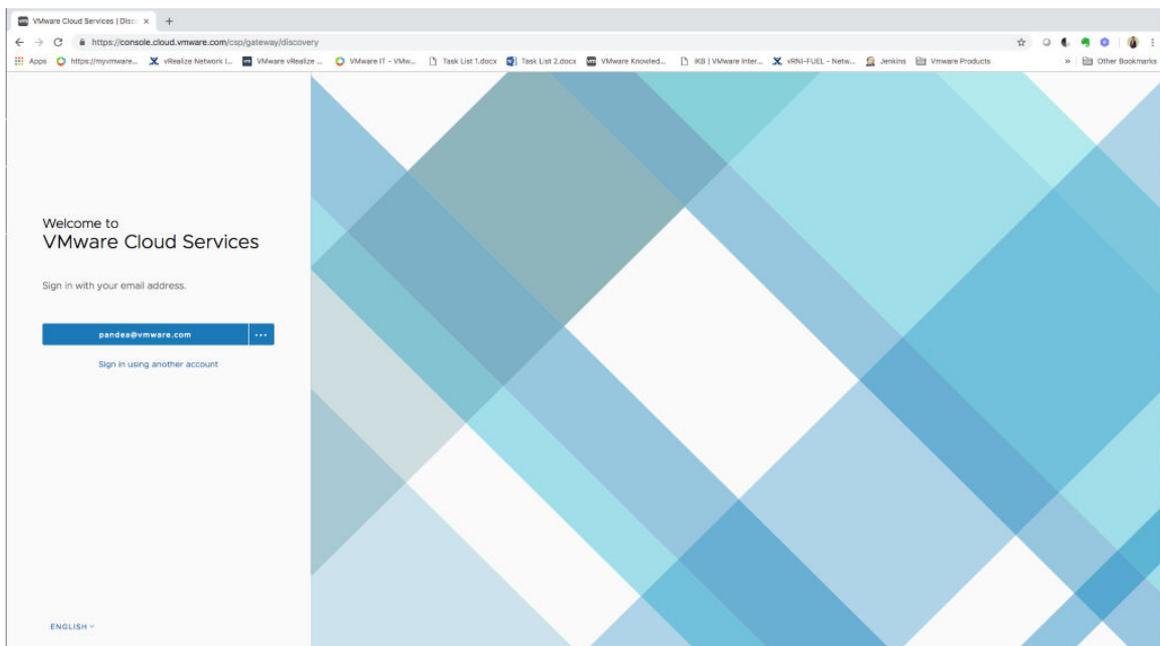
- NSX Manager の CSP 更新トークンの取得方法
- vCenter Server の認証情報の取得方法
- コンピューティング ゲートウェイ：ファイアウォール ルール

NSX Manager の CSP 更新トークンの取得方法

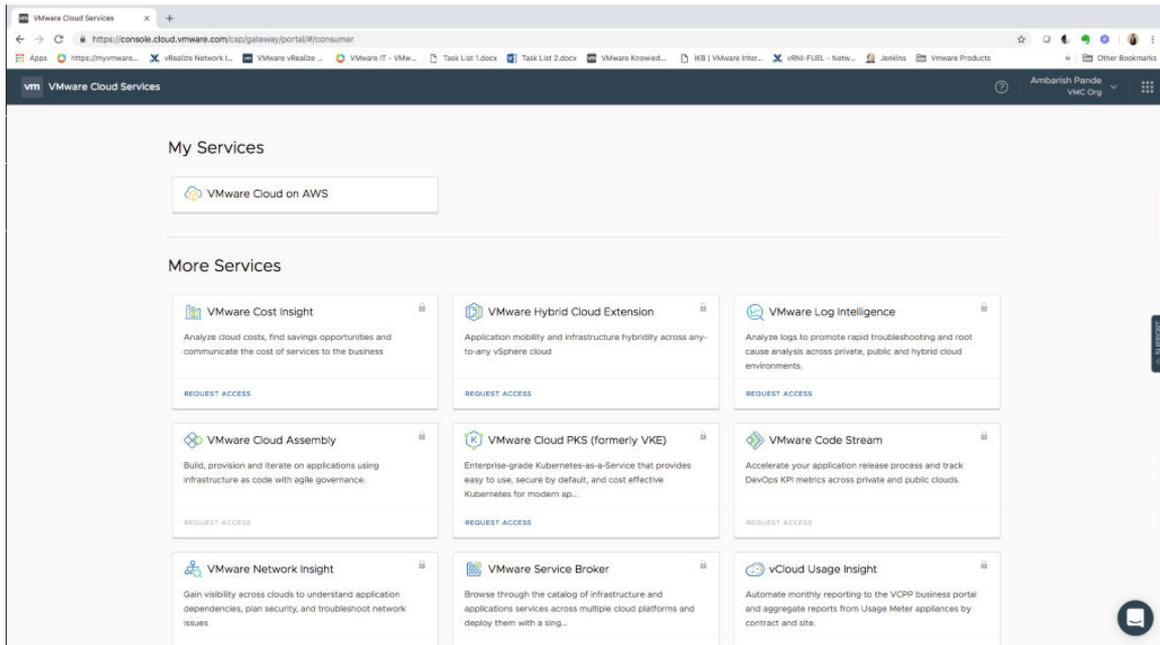
VMware Cloud on AWS NSX Manager を vRealize Network Insight にデータ ソースとして追加するには、更新トークンが必要です。

手順

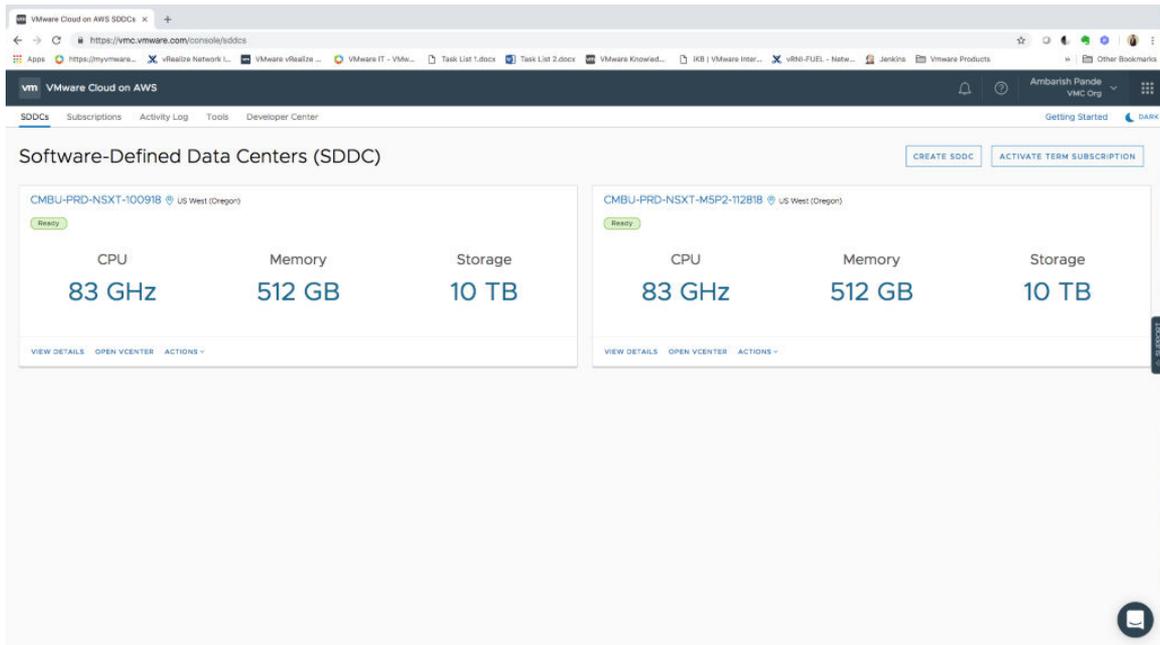
- 1 VMware Cloud Services コンソールにログインします。



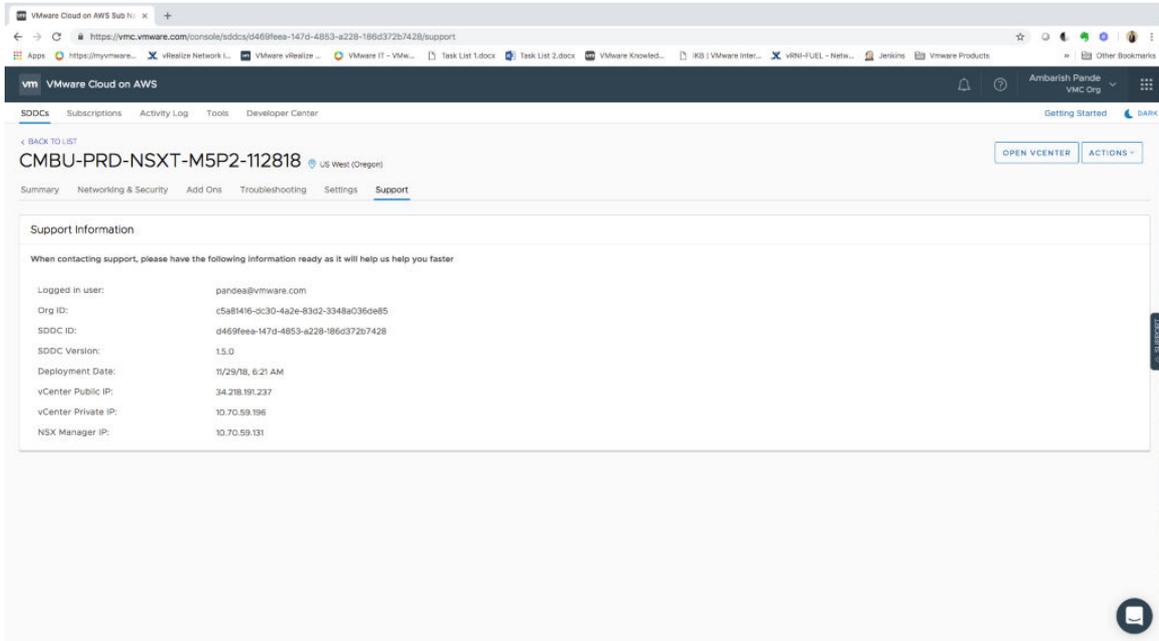
2 [マイサービス] で VMware Cloud on AWS をクリックします。



3 目的の Software-Defined Data Center (SDDC) を選択します。



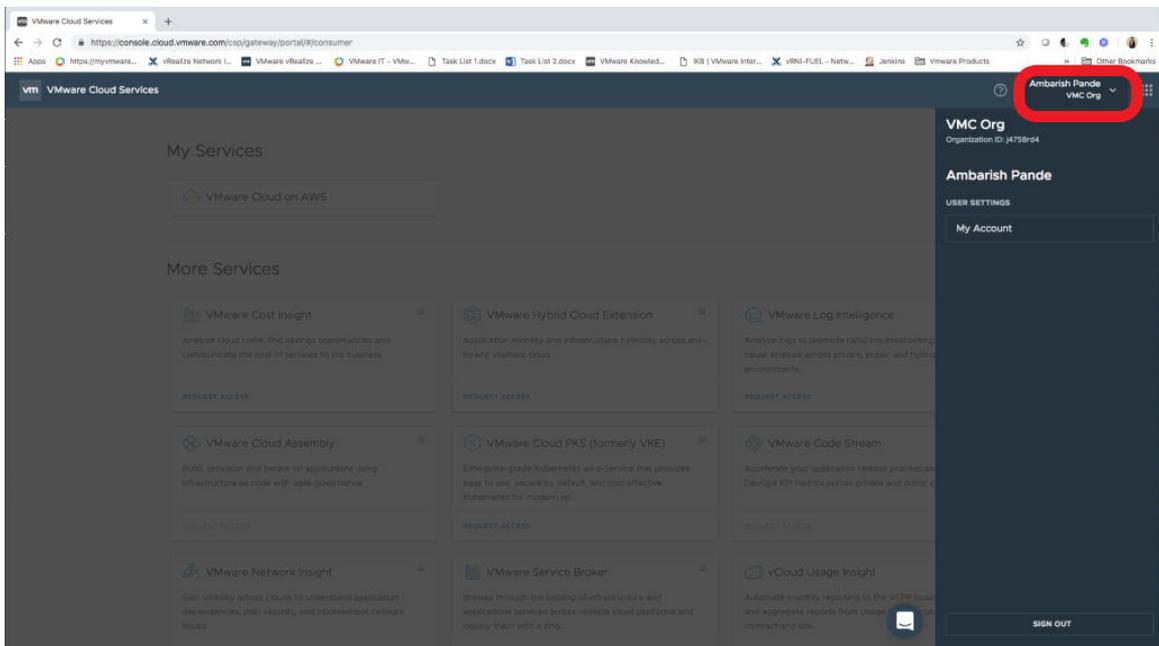
4 [サポート] タブをクリックします。



5 NSX Manager の IP アドレスをメモします。

6 上部のバナーで組織名をクリックします。

注： 選択した SDDC に組織が配置されていることを確認します。



7 API トークンを生成します。

手順については、[API トークンの生成](#)を参照してください。

注： API トークンを生成するには、管理者権限と NSX Cloud 管理者権限が必要です。

結果

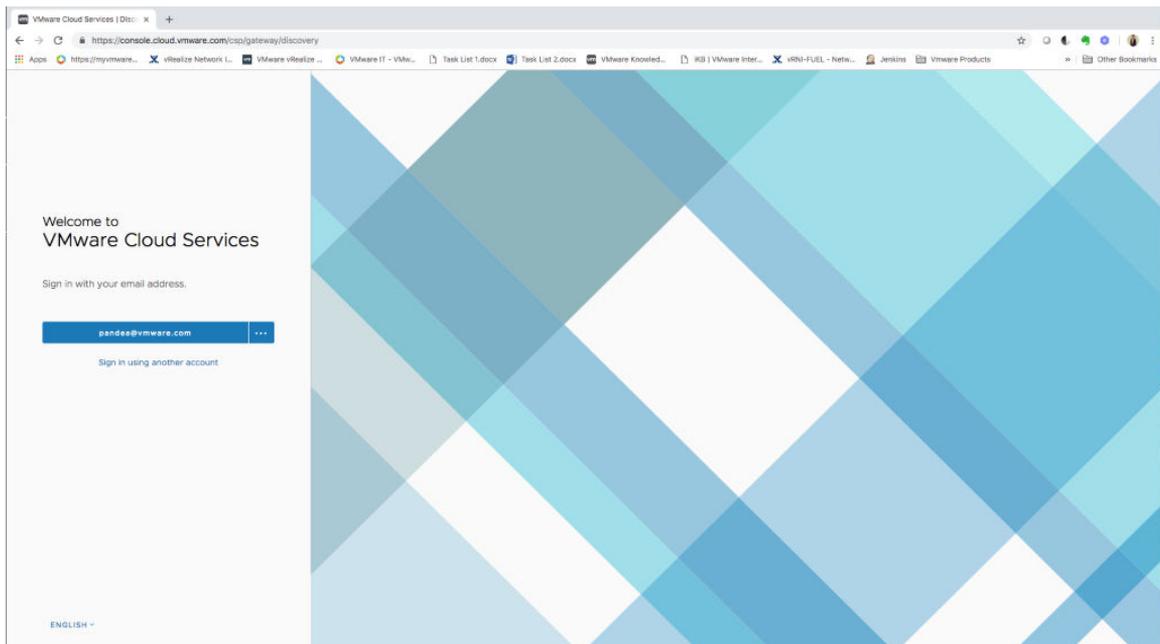
このトークンを使用して、組織内のすべての VMware Cloud on AWS の SDDC を認証できます。

vCenter Server の認証情報の取得方法

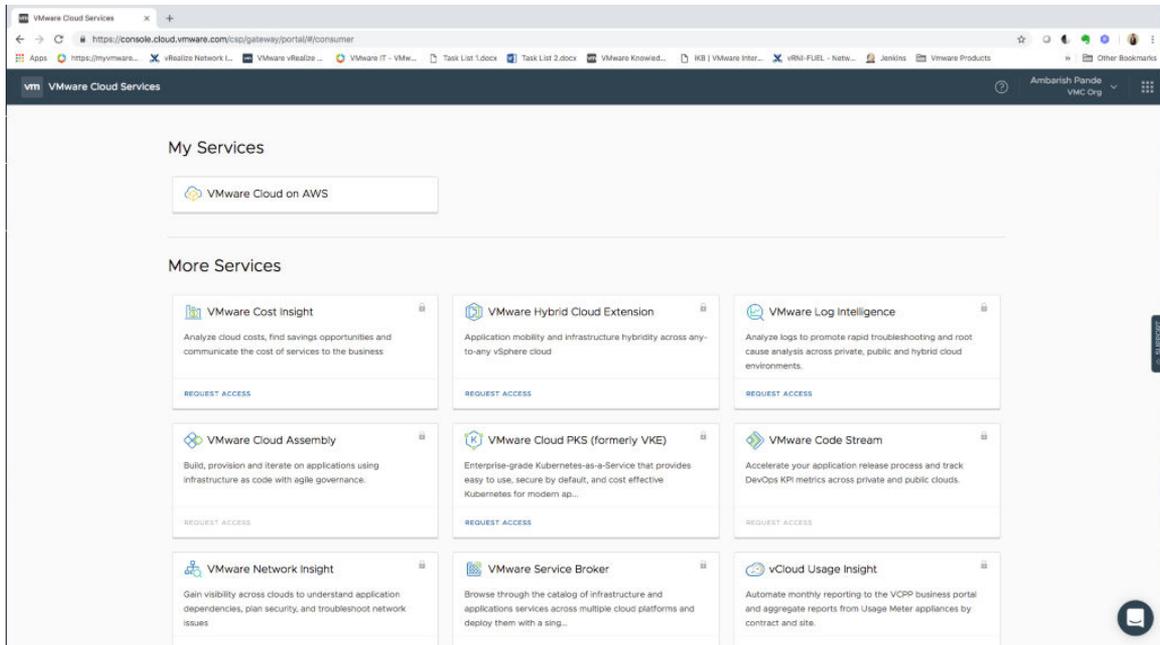
vCenter Server のデータソースを vRealize Network Insight に追加するには、vCenter Server の認証情報が必要です。

手順

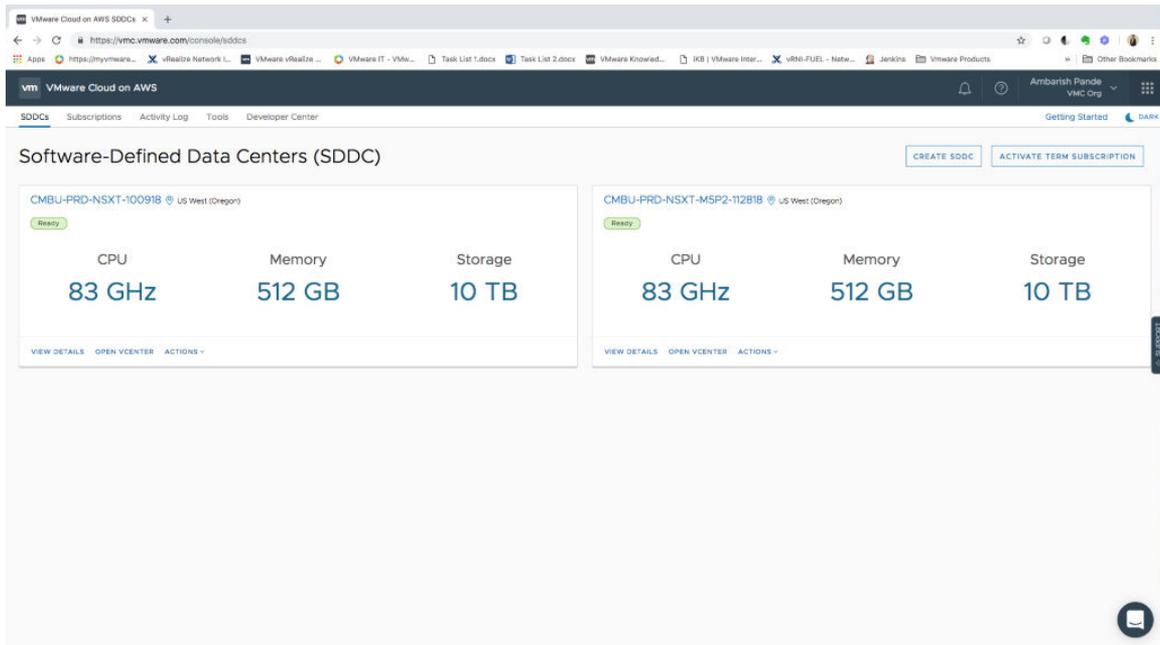
1 VMware Cloud Services コンソールにログインします。



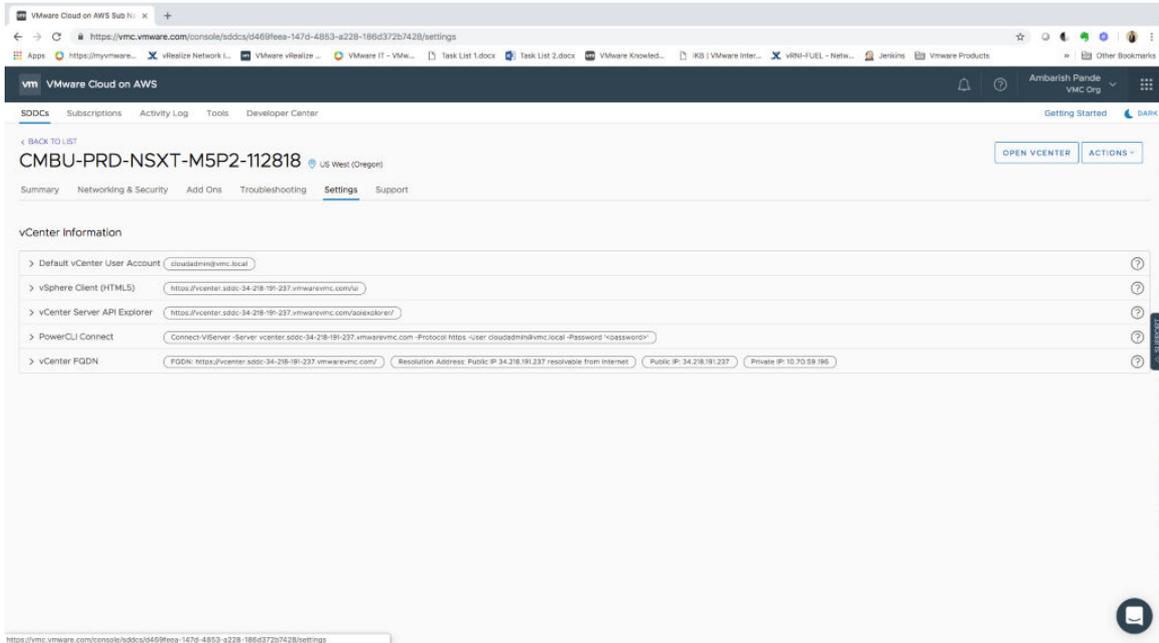
2 [マイサービス] で VMware Cloud on AWS をクリックします。



3 目的の Software-Defined Data Center (SDDC) を選択します。

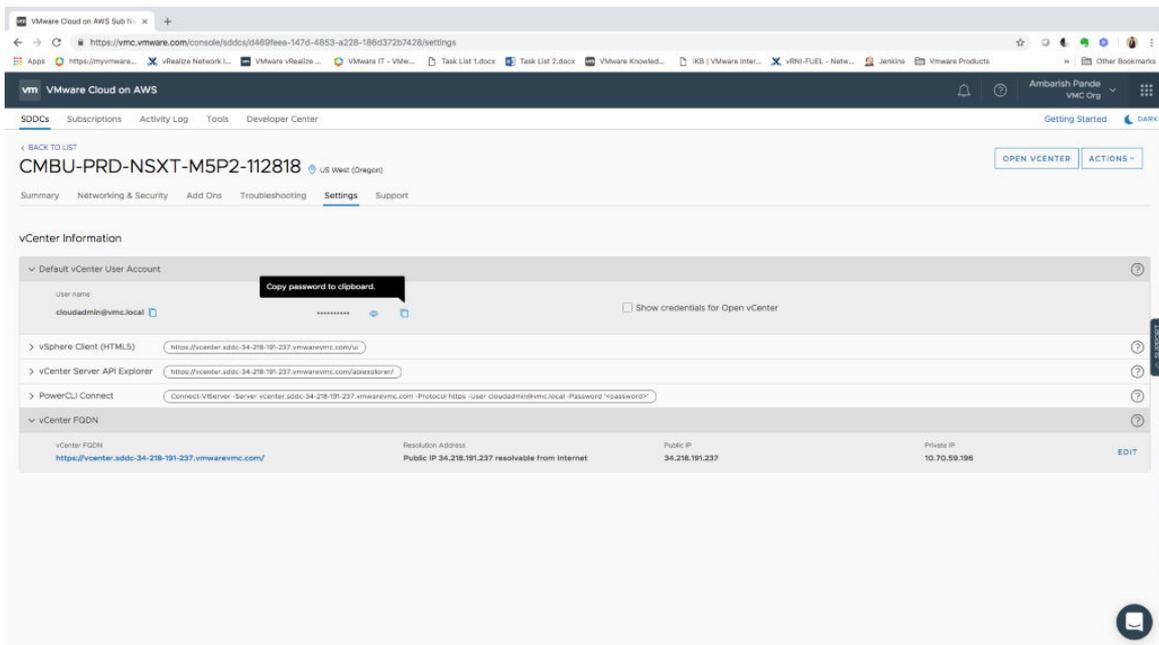


4 [設定] タブをクリックします。



5 vCenter Server の FQDN を展開します。

vCenter Server の FQDN の詳細をメモします。

6 デフォルトの vCenter Server ユーザー アカウントを展開して、ユーザー名とパスワードを取得します。
パスワードをコピーし、ユーザー名をメモします。

コンピューティング ゲートウェイ：ファイアウォール ルール

コレクタが vRealize Network Insight プラットフォームと通信するためには、送信トラフィック用に HTTPS ポート 443 が開かれている必要があります。

以下の VMware ホスト URL は、コレクタからファイアウォールを通じてアクセスされます。

- *.vmwareidentity.com
- gaz.csp-vidm-prod.com
- *.vmware.com
- *.ni-onsaas.com

また、vRealize Network Insight または vRealize Network Insight コレクタが正しく機能するためには、NTP および DNS トラフィックを許可する必要があります。

以下の詳細を持つファイアウォール ルールを作成します。

- 名前：内容を表す適切な名前
- 送信元：コレクタ IP アドレスを含む VMware Cloud on AWS グループの名前
- 宛先：[任意] を選択
- サービス：[HTTPS、DNS、DNS-UDP、NTP、ICMP] から選択
- アクション：[許可]
- 適用先：[インターネット インターフェイス]
- ログ：必要に応じてログを有効にします。