

Verwenden von vRealize Network Insight

VMware vRealize Network Insight 5.2

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

<https://docs.vmware.com/de/>

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

- 1 Informationen zum vRealize Network Insight-Benutzerhandbuch 10**

- 2 Erste Schritte 11**
 - Einführung 11
 - Startseite 13
 - Navigation 15
 - Einstellungen 16

- 3 Hinzufügen einer Datenquelle in vRealize Network Insight 17**
 - Unterstützte Produkte und Versionen 19
 - Hinzufügen von vCenter Server 23
 - Hinzufügen von VMware NSX Manager 25
 - Hinzufügen von VMware NSX-T Manager 27
 - Hinzufügen von VMware SD-WAN 32
 - Hinzufügen von Cisco ASR/ISR für SD-WAN-Bewertung 33
 - Hinzufügen von VMware Cloud on AWS 34
 - Einrichten des vRealize Network Insight-Collectors für VMware Cloud on AWS 34
 - Erstellen von VMware Cloud on AWS-Firewallregeln für vRealize Network Insight 35
 - Hinzufügen eines VMware Cloud on AWS-vCenters 37
 - Hinzufügen von VMware Cloud on AWS – NSX Manager 38
 - Hinzufügen von Amazon Web Services 39
 - Hinzufügen eines primären AWS-Kontos 40
 - Hinzufügen einer AWS-Standarddatenquelle 46
 - AWS: Unterstützung für Geo-Blockierung 49
 - Hinzufügen eines Azure-Abonnements 49
 - Aktivieren des NSG-Flow-Protokolls 50
 - Hinzufügen von VMware PKS 51
 - Hinzufügen von Kubernetes 52
 - Hinzufügen von OpenShift 53
 - Hinzufügen von Palo Alto Networks Panorama 54
 - Hinzufügen eines Check Point-Verwaltungsservers 55
 - Hinzufügen von Cisco ASA 56
 - Hinzufügen von Fortinet FortiManager 57
 - Hinzufügen von Arista-Switch-SSH 58
 - Hinzufügen von Dell OS10-Switches 59
 - Aktivieren von Telemetrie auf Dell OS10-Switches 60
 - Hinzufügen der Serien 6800/7800/8800 von Huawei 61
 - Hinzufügen von Cisco ACI 63

Hinzufügen eines physischen Flow-Collectors für NetFlow und sFlow	64
Hinzufügen von vRealize Log Insight	65
Hinzufügen von Infoblox	66
Hinzufügen von F5 BIG-IP	68
Hinzufügen von ServiceNow	70
Hinzufügen von ServiceNow	72
Hinzufügen eines neuen generischen Routers oder Switches	87
Bearbeiten eines generischen Routers oder Switches	88
4 Migrieren von Datenquellen	89
5 Löschen einer Datenquelle aus vRealize Network Insight	91
6 Konfigurieren der Einstellungen für vRealize Network Insight	92
Anzeigen des Systemzustands	93
Konfigurieren des Datenaufbewahrungsintervalls	93
Konfigurieren von IP-Eigenschaften und Subnetzen	94
Importieren der DNS-Zuordnungsdatei	94
Konfigurieren der Zuordnung zwischen Subnetz und einem VLAN	95
Konfigurieren von Ost-West-IPs	95
Konfigurieren von Nord-Süd-IPs	96
Konfigurieren von Ereignissen und Benachrichtigungen	96
Liste „Systemereignisse“	96
Anzeigen und Bearbeiten von Systemereignissen	162
Bearbeiten von benutzerdefinierten Ereignissen	166
Anzeigen von Plattformzustandseignissen	167
NSX-T-Ereignisse	167
Kubernetes-Ereignisse	183
Benachrichtigungen	184
Konfigurieren der Identitäts- und Zugriffsverwaltung	188
Konfigurieren der Benutzerverwaltung	188
Konfigurieren von Protokollen	200
Anzeigen und Exportieren von Überwachungsprotokollen	200
Einrichten der Syslog-Konfiguration	200
E-Mail-Server konfigurieren	201
Ziel des SNMP-Traps konfigurieren	202
Löschen eines SNMP-Trap-Ziels	203
Verwalten von Lizenzen	203
Vergleichen der Funktionen basierend auf der Lizenzedition	205
Hinzufügen und Ändern einer Lizenz	206
Konfigurieren des Intervalls für die automatische Aktualisierung	207

- Konfigurieren der Zeitüberschreitung für Benutzersitzungen 208
- Hinzufügen eines Google Maps-API-Schlüssels 209
- Konfigurieren der Validierung von Datenquellenzertifikaten 209
 - Manuelles Akzeptieren eines Datenquellenzertifikats 210
- Anzeigen von Überwachungsprotokollen 211
- Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit oder Verlassen des Programms 212
- Anzeigen des Systemzustands Ihrer Einrichtung 212
- Aktivieren des Support-Tunnels 213
- Verwalten der Festplattennutzung 213
- Anzeigen von Details zu Knoten 214
- Erstellen eines Support-Pakets 214
- Grundlegendes zur Kapazität für Collector- und Plattformlasten 215

- 7 Direct Connect-Unterstützung in vRealize Network Insight 217**
 - Anzeigen von Details zu Direct Connect von VMC 218
 - Anzeigen von Flows über Direct Connect 219
 - Direct Connect-Suchabfragen 219

- 8 vRealize Operations Manager-Integration 221**

- 9 Erstellen und Erweitern von Clustern 222**
 - Erstellen von Clustern 222
 - Erweitern von Clustern 223

- 10 Konfigurieren von Flows in vRealize Network Insight 224**
 - Aktivieren der IPFIX-Konfiguration 224
 - IPFIX-Konfiguration auf VDS und DVPG 224
 - IPFIX-Konfiguration für VMware NSX 226
 - Flow-Unterstützung für physische Server 228
 - Konfigurieren eines NetFlow-Collectors in einem physischen Gerät 228
 - Anreicherung von Flows und IP-Endpoints 233
 - Suchen nach physischen zu physischen Flows 234
 - Blockierte und geschützte Flows anzeigen 235
 - Netzwerkadressübersetzung (NAT) 236
 - Unterstützung für NAT-Flow – Beispiele 238
 - VMware Cloud on AWS Flows 239
 - Erstellen eines VPC-Flow-Protokolls 239
 - Senden von Flow-Datensätzen von F5 an vRealize Network Insight-Collectors 240
 - Erstellen eines Pools mit IPFIX-Collectors 241
 - Erstellen eines IPFIX-Protokollziels 242
 - Erstellen eines Protokollherausgebers 242

- Erstellen von iRules 243
- Hinzufügen der iRule zu einem virtuellen Server 247
- Erstellen eines Routeneintrags 248

11 Informationen zu Geltungsbereichen und Flows in Kubernetes und VMware PKS 249

12 Anzeigen von Details zu Einheiten 251

- Anzeigen von Details zum vRealize Network Insight-System (NI-System) 252
- Anzeigen der Details zur Plattform-VM 253
- Anzeigen von Details der Collector-VM 253
- Anzeigen der Details zu VMware vCenter-Datenquellen 254
- Anzeigen der PCI-Übereinstimmungsdetails 254
 - Als PDF exportieren 256
- Anzeigen von Kubernetes-Details 256
- Anzeigen von Details zum Lastausgleichsdienst 258
- Anzeigen von VM-Details 259
- Anzeigen der Details für Edge-Geräte 260
- Anzeigen von NSX Manager-Details 261
- Anzeigen der Details für **VMware NSX-T Manager** 261
- Anzeigen von Details zum **NSX-T-Verwaltungsknoten** 262
- Anzeigen von NSX-T-Transportdetails 263
- Anzeigen von Details zum virtuellen Server 265
- Anzeigen der Details zu Poolmitgliedern 266
- Anzeigen von Details zu Microsoft Azure 267
- Anzeigen von VeloCloud Enterprise-Details 269
 - Anzeigen von VeloCloud Edge-Details 271
- Anzeigen von Details zur SD-WAN- und Edge-SD-WAN-Anwendung 272
- Anzeigen von Details zur **SD-WAN-Bewertung** 273
 - Generieren eines Bewertungsberichts 274
- Anzeigen der Details zur **VeloCloud-Link-Anwendung** 274
- Anzeigen von Details zu **VeloCloud-Geschäftsrichtlinien** 274
- Anzeigen der VMC-SDDC-Details 275
- Anzeigen der Details für **Arista-Hardware-Gateway** und **Gateway-Bindung der Arista-Hardware** 275
- Anzeigen von Details zum **Cisco-Nexus-Gerät** 276
- Anzeigen von Flow-Erkennnisdetails 276
- Anzeigen der Details zur Mikrosegmentierung 281
- Anzeigen von Anwendungsdetails 282
- Analyse – Ausreißerererkennung 283
 - Erkennen von Ausreißer-VMs 283
- Analyse: statische und dynamische Schwellenwerte 285

Konfigurieren von Schwellenwerten und Warnungen 286

Anzeigen der Seite „Schwellenwertkonfiguration“ 288

13 Anzeigen der Topologie der Einheit 290

Topologie der virtuellen Maschine 290

Host-Topologie 290

VXLAN-Topologie 291

VLAN-Topologie 292

NSX Manager-Topologie 292

Anzeigen von Überwachungsinformationen von NSX-Objekten in vRealize Network Insight
293

14 Arbeiten mit Pins 297

Pins 297

Pintypen 297

Pinnwände 300

Gemeinsame Nutzung und Zusammenarbeit mit Pinnwänden 303

Festlegen einer Pinnwand als Startseite 305

Duplizieren einer Pinnwand 306

15 Unterstützung für Lastausgleichsdienst vRealize Network Insight 307

F5 als Lastausgleichsdienst 307

Anzeigen von Details zum Lastausgleichsdienst 309

Anzeigen von Details zum virtuellen Server 309

Anzeigen der Details zu Poolmitgliedern 310

Beispiele für Suchabfragen im Zusammenhang mit dem Lastausgleichsdienst 311

NSX-V als Lastausgleichsdienst 312

16 Netzwerksichtbarkeit 313

Pfadtopologie 313

VM-VM-Pfad für AWS 314

NSX-T 316

VM-zu-VM-Pfad über die NSX-V Edge Trunk-Schnittstelle 318

NAT-Unterstützung in vRealize Network Insight 318

VM-zu-VM-Pfad für VMware SD-WAN 320

VM-VM-Pfad für Arista-Hardware-VTEP 321

VMware Cloud on AWS: VM-zu-VM-Pfad 323

VM-VM-Pfad für Cisco ACI 324

Unterstützung für den Cisco BGP-EVPN-Modus 324

Unterstützung für ECMP-Route (Equal-Cost Multi-Path) 325

Unterstützung für die L2-Bridges 326

Anzeigen von Details zu BGP-Nachbarn 327

Pfad zum Internet 328

17 Sicherheit 329

Cross-vCenter NSX 329

Palo Alto-Netzwerke 330

Cisco-ASA-Firewall 333

Check Point-Firewall 335

Sicherheitsgruppen 337

Richtlinienbasiertes VPN 338

Inaktive Regeln für verteilte NSX-Firewall 339

Fortinet-Firewall 340

18 Arbeiten mit der Mikrosegmentierung 341

Analysieren der Anwendung 341

Anzeigen von Mikrosegmentierungs- und Flow-Daten in der Donut-Ansicht 341

Anzeigen von Mikrosegmentierungs- und Flow-Daten in der Rasteransicht 345

Manuelles Erstellen einer Anwendung 346

Anwendungsermittlung 348

Hinzufügen von ermittelten Anwendungen 349

VMware Cloud on AWS: Planung und Mikrosegmentierung 354

19 Empfohlene Firewallregeln 356

Exportregeln 359

Globale NSX DFW-Artefakte 359

Speichern der Konfiguration für CSV-Export als Eigenschaftsvorlage 360

Exportieren und Anwenden von Kubernetes-Netzwerkrichtlinien 362

20 Arbeiten mit Suchabfragen 365

Speichern und Löschen von Suchabfragen 366

Suchabfragen 367

Azure-Suchabfragen 373

Cisco-ACI-Einheiten 374

Fortinet-Suchabfragen 377

Anreicherung von Flows mit Infoblox-DNS-Daten 378

Häufige Suchabfragen für Kubernetes-Einheiten 379

Beispiele für Suchabfragen im Zusammenhang mit dem Lastausgleichsdienst 382

Suchabfragen für NSX-Firewallregeln 382

VMware SD-WAN-Suchabfragen 383

VMC-SDDC-Suchabfragen 384

VMware Cloud on AWS für AWS-Einheiten 385

Erweiterte Abfragen 386

- Zeitsteuerung 390
- Suchergebnisse 391
- Filter 391
- vCenter-Tags 392

21 Planen der Notfallwiederherstellung für vRealize Network Insight 395

- Beispiel für ein Notfallwiederherstellungsszenario 396

22 Fehlerbehebung 399

- Häufige Datenquellenfehler 399
- Aktivierung von DFW-IPFIX nicht möglich 401

23 Planen der Migration von Anwendungen auf VMware Cloud on AWS mithilfe von vRealize Network Insight 404

- Erhalten des CSP-Aktualisierungstokens für NSX Manager 405
- Abrufen von vCenter-Anmeldedaten 408
- Firewallregel für Computing-Gateway 411

Informationen zum vRealize Network Insight- Benutzerhandbuch

1

Im *vRealize Network Insight-Benutzerhandbuch* finden Sie Informationen zur Verwendung von vRealize Network Insight.

Zielgruppe

Diese Informationen richten sich an Administratoren oder Spezialisten, die für die Verwendung von vRealize Network Insight zuständig sind. Die Informationen wurden für erfahrene Administratoren von virtuellen Maschinen verfasst, die mit Enterprise Management-Anwendungen sowie mit Datacenter-Vorgängen vertraut sind.

Erste Schritte

2

Dieses Kapitel enthält die folgenden Themen:

- Einführung
- Startseite
- Navigation
- Einstellungen

Einführung

vRealize Network Insight bietet intelligente Vorgänge für softwaredefinierte Vernetzung und Sicherheit. Es unterstützt Kunden dabei, eine optimierte, hochverfügbare und sichere Netzwerkinfrastruktur über Multi-Cloud-Umgebungen hinweg zu erstellen. Es beschleunigt die Planung und Bereitstellung für die Mikrosegmentierung, ermöglicht Einblicke in alle virtuellen und physischen Netzwerke und bietet Betriebsansichten für die Verwaltung und Skalierung der VMware NSX-Bereitstellungen.

Stellen Sie sich vor, dass Ihr gesamtes Datacenter aus Einheiten den Beziehungen dieser Einheiten untereinander besteht. Eine virtuelle Maschine beispielsweise ist eine Einheit, und die virtuelle Maschine ist Teil eines Hosts, der wiederum eine andere Einheit ist. vRealize Network Insight bietet Einblicke und Informationen zu zahlreichen Einheiten, die Teil Ihres Datacenters sind.

Tabelle 2-1.

Elemente	Beschreibung
	Host
	Problem
	NSX-Firewall

Tabelle 2-1. (Fortsetzung)

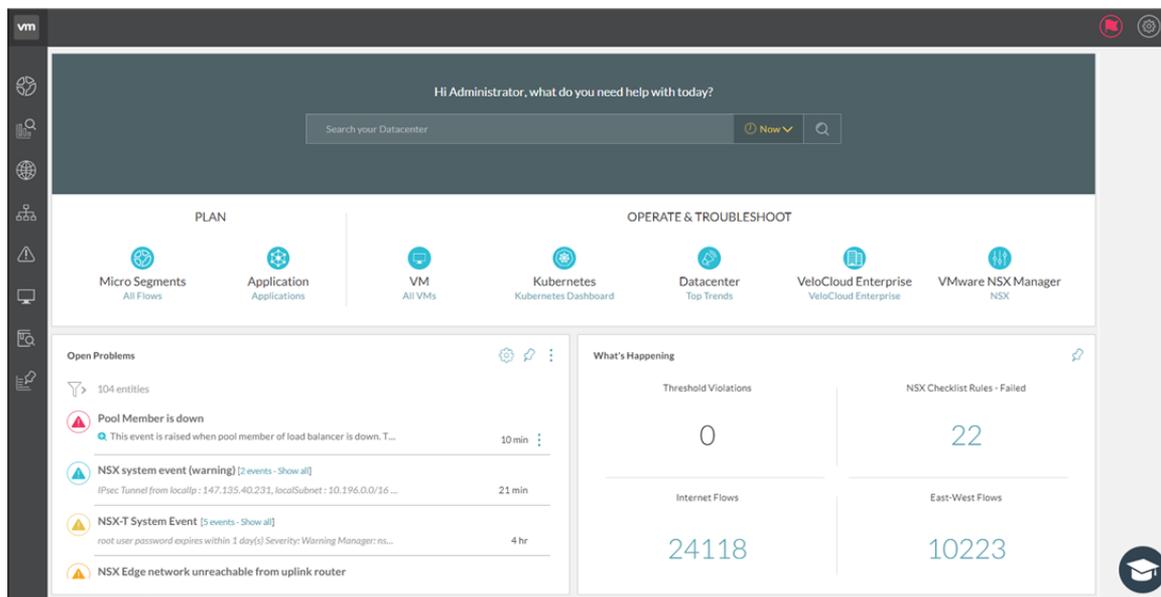
Elemente	Beschreibung
	Virtuelle Maschine
	vSphere Distributed Switch
	Physischer Switch
	Virtuelle Portgruppe
	Cisco Fabric Extender
	Logischer Switch
	Datenspeicher
	Physische Netzwerkschnittstellenkarte
	Sicherheitsgruppe
	Blade
	Router
	VLAN
	Gruppe von VMs
	Konfigurationsänderungen
	Routerschnittstelle
	Fehlerbehebung

Tabelle 2-1. (Fortsetzung)

Elemente	Beschreibung
	Netzwerkadressübersetzung (NAT)
	E-Mail-Server

Startseite

Auf der Startseite von VMware vRealize Network Insight erhalten Sie eine kurze Übersicht über die Vorgänge in Ihrem gesamten Datacenter. Sie bietet Ihnen einen schnellen Zugriff auf die wichtigen Komponenten von vRealize Network Insight in Ihrem Datacenter.



Die Startseite ist in folgende Abschnitte unterteilt:

Suchleiste

Über die Suchleiste können Sie Ihr gesamtes Datacenter-Netzwerk (und seine entsprechenden Einheiten) durchsuchen. Beispielsweise können Sie über die Suchleiste nach den Einheiten in Ihrem Datacenter suchen, die verfügbar sind. Die Suchleiste befindet sich oben auf der Startseite.

Je nach Bedarf können Sie die Suche nach den folgenden Zeitachsenoptionen durchführen:

- **Voreinstellungen:** Mit dieser Option können Sie die Suchergebnisse eingrenzen, z. B. nach last week, last 3 days, last 24 hours, yesterday, today, last 2 hours, last hour und now (aktuelle Zeit).
- **Am/um:** Mit dieser Option können Sie die Suchergebnisse auf ein bestimmtes Datum und eine bestimmte Uhrzeit eingrenzen.

- **Zwischen:** Mit dieser Option können Sie nach Daten in einem bestimmten Zeitintervall suchen.

Abschnitt „Plan“

- **Mikrosegmente:** Sie können die Mikrosegmentierung des Netzwerks anhand der Flows zwischen allen VMs planen.
- **Anwendung:** Sie können Ihre Anwendungen definieren und deren Flows analysieren sowie ihre Sicherheit planen.

Abschnitt „Betrieb und Fehlerbehebung“

Der Abschnitt **Betrieb und Fehlerbehebung** enthält Einblicke, Metriken und Analysen für die folgenden Komponenten:

- Virtuelle Maschine (VM)
- VLAN-Netzwerk
- Datacenter
- NSX-Sicherheitsgruppe
- VMware NSX

Offene Probleme

Der Abschnitt **Offene Probleme** bietet einen schnellen Überblick über die kritischen Ereignisse, die die Plattform in Ihrem Datacenter findet. Alle derartigen ähnlichen Ereignisse sind gruppiert. Mit der Option **Alle anzeigen** können Sie alle Ereignisse anzeigen. Um weitere Details zu einem Ereignis anzuzeigen, klicken Sie auf  (**Details anzeigen**). Über das Symbol „Ereignisse konfigurieren“ können Sie zu der Seite „Systemereignisse“ navigieren und die Ereignisse konfigurieren.

Wenn Sie unter **Weitere Optionen** für ein bestimmtes Ereignis auf die Option **Ereignis konfigurieren** klicken, können Sie direkt zur Bearbeitungsansicht für das jeweilige Ereignis navigieren, um die Konfigurationen zu ändern.

Was geschieht

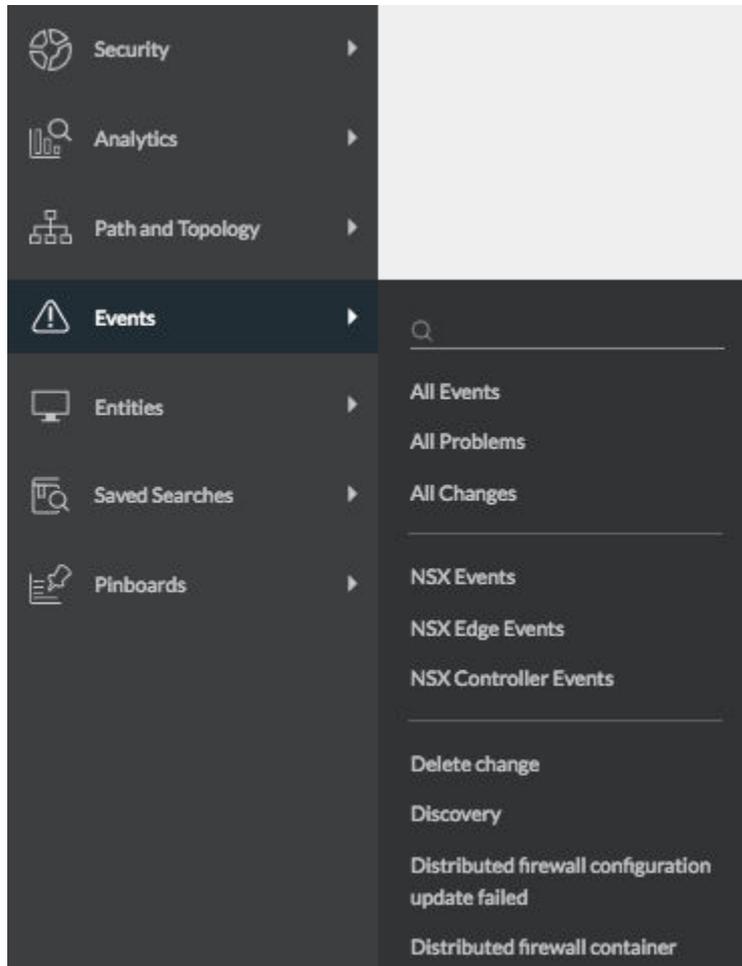
Der Abschnitt **Was geschieht** bietet einen schnellen Überblick über Eigenschaften mit sehr hohen Werten aus Ihrem Datacenter. Um die Eigenschaftsdetails anzuzeigen, klicken Sie auf die Anzahl einer bestimmten Eigenschaft. Auf der linken Seite enthält dieser Abschnitt auch Filter, mit denen Sie alle Ereignisse filtern können, und die Schaltflächen „Alle erweitern“ und „Alle reduzieren“, über die Sie die Details zu den Ereignissen anzeigen können.

Navigation

vRealize Network Insight enthält auf der linken Seite einen Navigationsbereich, mit dem Benutzer schnell zu den wichtigsten Produktfunktionen wie Sicherheit, Topologien, Einheiten, Ereignissen und gespeicherten Suchabfragen navigieren können, ohne Suchabfragen eingeben zu müssen.

Der Navigationsbereich enthält die folgenden Optionen:

- Sicherheit: Hier finden Sie die folgenden Optionen:
 - Sicherheit planen: Hiermit können Sie die Flows in der Umgebung analysieren und die Mikrosegmente innerhalb der Umgebung planen. Sie können erst alle Einheiten oder eine bestimmte Einheit und dann die Analysedauer für die ausgewählte Einheit auswählen.
 - Anwendungen: Hier können Sie Anwendungen in vRealize Network Insight mithilfe der benutzerdefinierten Suche erstellen. Nachdem Sie eine Anwendung erstellt haben, können Sie sie entsprechend planen.
 - PCI-Übereinstimmung: Das Dashboard „PCI-Übereinstimmung“ hilft bei der Bewertung der Konformität mit den PCI-Anforderungen nur in der NSX-Umgebung.
- Pfad und Topologie: Hier können Sie alle VM-zu-VM-Pfade oder -Topologien für mehrere Einheiten des Datacenters anzeigen.
- Ereignisse: Hier können Sie die Ereignisse (Änderungen und Probleme) in Ihrer Umgebung anzeigen. Außerdem finden Sie hier eine Liste der Ereignistypen, sodass Sie schnell einen bestimmten Ereignistyp anzeigen können.
- Einheiten: Hier finden Sie eine Liste aller Arten von Einheiten, die in Ihrer Umgebung vorhanden sind. Klicken Sie in der angegebenen Liste auf einen Einheitstyp, um eine Liste aller Einheiten dieses Typs anzuzeigen. In das Textfeld oberhalb der Liste der Einheiten können Sie Text eingeben, um die Liste weiter einzugrenzen.
- Gespeicherte Suchvorgänge: Hier werden die zuvor gespeicherten Suchvorgänge angezeigt.



Einstellungen

Die Seite **Einstellungen** enthält Steuerelemente zum Verwalten von Datenanbietern, Benutzern und Benachrichtigungen.

So wechseln Sie zur Seite **Einstellungen**:

- 1 Klicken Sie in der oberen rechten Ecke der Startseite auf das Symbol „Profil“.
- 2 Klicken Sie auf **Einstellungen**. Die Seite **Einstellungen** wird angezeigt.

Hinzufügen einer Datenquelle in vRealize Network Insight

3

Datenquellen ermöglichen es der Anwendung, Daten aus bestimmten Aspekten Ihres Datencenters zu erfassen. Diese reichen von Ihrer NSX-Installation bis hin zu physischen Geräten wie z. B. Cisco™ Chassis 4500 und Cisco™ N5K.

So fügen Sie eine Datenquelle hinzu:

- 1 Klicken Sie auf der Seite **Installieren und unterstützen** unter **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Neue Quelle hinzufügen**.
- 3 Wählen Sie ein Konto oder einen Quellentyp aus.
- 4 Geben Sie die erforderlichen Informationen in das Formular ein.
- 5 Klicken Sie auf **Validieren**.
- 6 Geben Sie den Spitznamen und (bei Bedarf) Notizen für die Datenquelle ein.
- 7 Klicken Sie auf **Absenden**, um die Datenquelle zur Umgebung hinzuzufügen.

Für jede Datenquelle können Sie die folgenden Details anzeigen:

Eigenschaften	Beschreibung
Typ (Spitzname)	Zeigt den Namen der Datenquelle an.
IP-Adresse/FQDN	Zeigt die IP-Adresse oder die FQDN-Details für die Datenquelle an.
Letzte Erfassung	Zeigt die letzte Erfassungszeit an, zu der die Daten erfasst wurden.
Ermittelte VMs	Zeigt die Anzahl der VMs an, die für diese Datenquelle ermittelt wurden. Hinweis Die Spalte „Ermittelte VMs“ wird nur dann aufgefüllt, wenn es sich bei der Datenquelle um vCenter oder AWS-Quelle handelt.
Collector-VM	Zeigt den Namen des Collectors an, dem die Datenquelle hinzugefügt wurde. Diese Spalte ist nicht sichtbar, wenn alle aufgelisteten Datenquellen auf demselben Collector hinzugefügt wurden. Sie können diese Spalte nur anzeigen, wenn die Datenquellen auf unterschiedlichen Collectors vorhanden sind.

Eigenschaften	Beschreibung
Aktiviert	Gibt an, ob die Datenquelle aktiviert ist.
Aktionen	Zeigt Optionen zum Bearbeiten und Löschen der Datenquelle an.

vRealize Network Insight bietet die folgenden Funktionen, um einfachen Zugriff auf die Informationen von Datenquellen zu ermöglichen.

- Sie können die Suche nach einer Datenquelle anhand des Namens, der IP-Adresse oder des Namens der Collector-VM durchführen, indem Sie die Suchleiste oberhalb der Spaltenüberschriften verwenden.
- Sie können Informationen nach unterschiedlichen Datenquellen in der Spalte **Typ (Spitzname)** filtern.
- Sie können Informationen nach verschiedenen Collector-VMs in der Spalte **Collector-VM** filtern.
- Die Datenquellen werden nach ihren Typen und Spitznamen in alphabetischer Reihenfolge sortiert.

Für jede hinzugefügte Datenquelle können Sie die folgenden Informationen anzeigen:

- **Alle:** Zeigt alle verfügbaren Datenquellen an.
- **Mit Problemen:** Zeigt die Datenquellen an, in denen vRealize Network Insight ein Problem festgestellt hat.
- **Mit Empfehlungen:** Zeigt automatisch generierte Empfehlungen von vRealize Network Insight für die Datenquellen an, die zusätzliche Informationen benötigen.
- **Deaktiviert:** Zeigt die deaktivierten Datenquellen an.

Dieses Kapitel enthält die folgenden Themen:

- [Unterstützte Produkte und Versionen](#)
- [Hinzufügen von vCenter Server](#)
- [Hinzufügen von VMware NSX Manager](#)
- [Hinzufügen von VMware NSX-T Manager](#)
- [Hinzufügen von VMware SD-WAN](#)
- [Hinzufügen von Cisco ASR/ISR für SD-WAN-Bewertung](#)
- [Hinzufügen von VMware Cloud on AWS](#)
- [Hinzufügen von Amazon Web Services](#)
- [Hinzufügen eines Azure-Abonnements](#)
- [Hinzufügen von VMware PKS](#)
- [Hinzufügen von Kubernetes](#)

- Hinzufügen von OpenShift
- Hinzufügen von Palo Alto Networks Panorama
- Hinzufügen eines Check Point-Verwaltungsservers
- Hinzufügen von Cisco ASA
- Hinzufügen von Fortinet FortiManager
- Hinzufügen von Arista-Switch-SSH
- Hinzufügen von Dell OS10-Switches
- Hinzufügen der Serien 6800/7800/8800 von Huawei
- Hinzufügen von Cisco ACI
- Hinzufügen eines physischen Flow-Collectors für NetFlow und sFlow
- Hinzufügen von vRealize Log Insight
- Hinzufügen von Infoblox
- Hinzufügen von F5 BIG-IP
- Hinzufügen von ServiceNow
- Hinzufügen eines neuen generischen Routers oder Switches

Unterstützte Produkte und Versionen

vRealize Network Insight unterstützt mehrere Produkte und Versionen.

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
Amazon Web Services (nur Enterprise-Lizenz)	Nicht anwendbar	HTTPS	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Arista-Switches	7050TX, 7250QX, 7050QX-32S, 7280SE-72	SSH, SNMP	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Azure-Abonnement	Nicht anwendbar	HTTPS	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Brocade-Switches	VDX 6740, VDX 6940, MLX, MLXe	SSH, SNMP	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Check Point-Firewall	Check Point R80, R80.10, R80.20, R80.30	HTTPS, SSH	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
Cisco	ASR 1K, ISR4K, CSR1Kv, ISR1K Hinweis Nur für SD-WAN-Bewertung unterstützt.	<ul style="list-style-type: none"> ■ Unterstütztes Betriebssystem: Cisco IOS XE-Software ■ Betriebssystemversion: 16.07.01 	Unterstützt nicht die Funktion zur Überprüfung und Sicherung von Netzwerken (Netzwerkzuordnung und Absichten).
Cisco ACI	3.2	HTTPS (zu APIC-Controller) SNMP (zu APIC-Controller und ACI-Switches)	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Cisco ASA	X Series mit OS 9.4	SSH, SNMP	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Cisco Catalyst	3000, 3750, 4500, 6000, 6500	SSH, SNMP	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Cisco Nexus	3000, 5000, 6000, 7000, 9000	SSH, SNMP	Benutzer mit Leseberechtigung SNMP-Benutzer mit Leseberechtigung
Cisco UCS (Unified Computing-System)	Blade-Server der Serie B, Rack-Server der Serie C, Chassis, Fabric Interconnect	UCS Manager: HTTPS UCS Fabric: SSH, SNMP	Benutzer mit Leseberechtigung SNMP-Benutzer mit Leseberechtigung
Dell-Switches	FORCE10 MXL 10, FORCE10 S6000, S4048, Z9100, S4810, PowerConnect 8024, Dell OS10	SSH, SNMP	Benutzer mit Leseberechtigung SNMP-Benutzer mit Leseberechtigung
Fortinet FortiManager	6.0.1	HTTPS	Der Benutzer muss über Folgendes verfügen: <ul style="list-style-type: none"> ■ mindestens die Rolle Eingeschränkter Benutzer mit Zugriff auf alle ADOMs- und Richtlinienpakete ■ Zugriff rpc-permit read, der über die Befehlszeilenschnittstelle (CLI) aktiviert wird
F5 BIG - IP	12.1.2 und höher	HTTPS, SSH, SNMP	Der Benutzer muss mindestens über die Gastrolle verfügen. Außerdem muss TMSH aktiviert sein und Zugriff auf alle Partitionen haben. F5 BIG-IP unterstützt sowohl Routing als auch Lastausgleich.
HP	HP Virtual Connect Manager 4.41, HP OneView 3.0	HP OneView 3.0: HTTPS HP Virtual Connect Manager 4.41: SSH	Benutzer mit Leseberechtigung

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
Huawei Cloud Engine	6800, 7800, 8800	SSH, SNMP	Benutzer mit Leseberechtigung SNMP-Benutzer mit Leseberechtigung
Infoblox	Infoblox NIOS-Version 8.0, 8.1, 8.2	HTTPS	Benutzer mit Lesezugriff mit API-Schnittstellenzugriff Leseberechtigungen für DNS-Objekttypen wie folgt: <ul style="list-style-type: none"> ■ Berechtigungstyp – DNS ■ Ressource – A-Datensätze, DNS-Zonen, DNS-Ansichten
Juniper-Switches	EX3300, QFX 51xx Series (JunOS v12 und v15, ohne QFabric)	Netconf, SSH, SNMP	Benutzer mit Leseberechtigung SNMP-Benutzer mit Leseberechtigung
Kubernetes	<ul style="list-style-type: none"> ■ 1.12 auf NSX-T 2.3.1 ■ 1.12 auf NSX-T 2.3.2 ■ 1.13 auf NSX-T 2.3.2 	HTTPS	Der Benutzer muss über eine Cluster-Administratorrolle mit Leseberechtigungen verfügen.
OpenShift	3.1.1	HTTPS	Siehe Abschnitt „Hinzufügen von Datenquellen“ im Benutzerhandbuch.
Palo Alto-Netzwerke	Panorama 7.0.x, 7.1, 8.x, 9.0	HTTPS	Der Benutzer muss über eine Administratorrolle mit XML-API-Zugriff verfügen. Weitere Informationen finden Sie im Abschnitt „Palo Alto Networks“ im <i>Benutzerhandbuch zu vRealize Network Insight</i> .
ServiceNow	London	HTTPS	Benutzer muss über Administratorrolle verfügen
VMware SD-WAN	VeloCloud Orchestrator und Edge Version 3.3.1 und höher	HTTPS	Der Benutzer muss über die Kontrolle mit einer der folgenden Berechtigungen verfügen: <ul style="list-style-type: none"> ■ Superuser ■ Standardadministrator ■ Kundensupport
VMC on AWS – vCenter	M8 und höher Hinweis Nur NSX-T-basierte VMware Cloud on AWS-SDDCs werden unterstützt.	HTTPS	Der Benutzer muss über die folgende Berechtigung verfügen: <ul style="list-style-type: none"> ■ Cloud-Administrator: Zum Hinzufügen einer Datenquelle und Aktivieren von IPFIX.

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
VMC on AWS – NSX Manager	M8 und höher Hinweis Nur NSX-T-basierte VMware Cloud on AWS-SDDCs werden unterstützt.	HTTPS	Der Benutzer muss über eine der folgenden Berechtigungen verfügen: <ul style="list-style-type: none"> ■ Organisationsmitglied.Administrator: Zum Hinzufügen einer Datenquelle und Aktivieren von IPFIX. ■ Organisationsmitglied.Administrator.NSX Cloud Admin: Zum Hinzufügen einer Datenquelle und Aktivieren von IPFIX. ■ Organisationsmitglied.VMware Cloud on AWS (alle Rollen): Zum Hinzufügen einer Datenquelle und Aktivieren von IPFIX. ■ Organisationsmitglied.NSX Cloud Auditor: Zum Hinzufügen einer Datenquelle.
VMware Identity Manager	3.3 und höher	HTTPS	Der Benutzer muss über eine Administratorrolle verfügen.
VMware PKS	Unterstützte Versionen		Der Benutzer muss über die Berechtigungen der Cluster-Administratorrolle – <code>pks.clusters.admin</code> – verfügen.
VMware NSX Manager (VMware NSX-V)	Unterstützte Versionen	SSH, HTTPS	Weitere Informationen finden Sie im Abschnitt „Edge-Datenerfassung“ im <i>Benutzerhandbuch zu vRealize Network Insight</i> .
VMware NSX-T Manager	2.4. Weitere unterstützte Versionen finden Sie unter Unterstützte Versionen .	HTTPS	Benutzer mit Leseberechtigung

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
VMware vRealize Log Insight	Unterstützte Versionen	HTTPS	API-Benutzer mit Berechtigungen zum Installieren, Konfigurieren und Verwalten des Inhaltspakets
VMware vSphere	Unterstützte Versionen Für IPFIX ist die folgende VMware ESXi-Version erforderlich: <ul style="list-style-type: none"> ■ 5.5 Update 2 (Build 2068190) und höher ■ 6.0 Update 1b (Build 3380124) und höher ■ VMware VDS 5.5 und höher <hr/> Hinweis VMware Tools sollte auf allen VMs im Datacenter installiert sein, um den VM-zu-VM-Pfad zu identifizieren.	HTTPS	Benutzer mit Leseberechtigung Erforderliche Berechtigungen zum Konfigurieren und Verwenden von IPFIX vCenter Server-Anmeldedaten mit Berechtigungen: Distributed Switch: Modify dvPort group: Modify Die vordefinierten Rollen in vCenter Server müssen über die folgenden Berechtigungen verfügen, die auf der Root-Ebene zugewiesen sind und an die untergeordneten Rollen weitergegeben werden müssen: System.Anonymous System.Read System.View global.settings

Hinweis

- Die unterstützten Betriebssysteme für Cisco ASA-, ACI-, Catalyst- und Nexus-Geräte sind iOS/NX-OS, für Cisco UCS die Version UCSM.
- Das unterstützte Betriebssystem für Arista ist Arista EOS.

Hinzufügen von vCenter Server

Sie können vCenter Server als Datenquelle zu vRealize Network Insight hinzufügen.

Mehrere vCenter Server können zu vRealize Network Insight hinzugefügt werden, um mit der Überwachung von Daten zu beginnen.

Voraussetzungen

- Die vordefinierten Rollen in vCenter Server müssen über die folgenden Berechtigungen verfügen, die auf der Root-Ebene zugewiesen sind und an die untergeordneten Rollen weitergegeben werden müssen:
 - **System.Anonymous**
 - **System.Read**
 - **System.View**
 - **Global.Settings**

- Zum Konfigurieren und Verwenden von IPFIX sind die folgenden vCenter Server-Berechtigungen erforderlich:
 - **Distributed Switch: Ändern und Portkonfigurationsvorgang**
 - **dvPort-Gruppe: Ändern und Richtlinienvorgang**

Weitere Informationen zu Rollen in vCenter finden Sie unter „Verwenden von Rollen zum Zuweisen von Berechtigungen“ im Handbuch *vSphere-Sicherheit*.

Verfahren

- 1 Klicken Sie auf **vCenter hinzufügen**.
- 2 Klicken Sie auf **Neue Quelle hinzufügen** und passen Sie die Optionen an.

Option	Aktion
Collector-VM	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder den vollqualifizierten Domännennamen (FQDN) des vCenter Server ein.
Benutzername	Geben Sie den Benutzernamen mit den folgenden Rechten ein: <ul style="list-style-type: none"> ■ Distributed Switch: Ändern ■ dvPort-Gruppe: Ändern
Kennwort	Geben Sie das Kennwort für die vRealize Network Insight-Software ein, um auf das vCenter Server-System zuzugreifen.

- 3 Klicken Sie auf **Validieren**.

Wenn die Anzahl der erkannten VMs die Kapazität der Plattform oder eines Collector-Knotens oder beides überschreitet, schlägt die Validierung fehl. Sie können erst dann eine Datenquelle hinzufügen, wenn Sie die Brick-Größe der Plattform erhöhen oder ein Cluster erstellen.

Die angegebene Kapazität für jede Brick-Größe mit und ohne Flows lautet wie folgt:

Brick-Größe	VMs	Status der Flows
Groß	6k	Aktiviert
Groß	10k	Deaktiviert
Mittel	3k	Aktiviert
Mittel	6k	Deaktiviert

- 4 Wählen Sie **Netflow (IPFIX) auf diesem vCenter aktivieren** aus, um IPFIX zu aktivieren.

Weitere Informationen zu IPFIX finden Sie im Abschnitt *Aktivieren der IPFIX-Konfiguration auf VDS und DVPD* des Benutzerhandbuchs.

Hinweis Wenn Sie IPFIX sowohl in vCenter als auch in VMware NSX Manager aktivieren, erkennt und entfernt vRealize Network Insight automatisch die Flow-Redundanzen durch Deaktivierung von IPFIX auf wenigen DVPDs für das zugehörige vCenter.

- 5 Fügen Sie Ihrem vCenter Server-System erweiterte Datenerfassungsquellen hinzu.
- 6 Klicken Sie auf **Absenden**, um das vCenter Server-System hinzuzufügen. Die vCenter Server-Systeme werden auf der Startseite angezeigt.

Hinzufügen von VMware NSX Manager

Sie können NSX-V als Datenquelle in vRealize Network Insight hinzufügen.

Voraussetzungen

Überprüfen Sie Folgendes:

- Sie haben bereits ein vCenter als Datenquelle hinzugefügt.
- Die **Enterprise**-Rolle.
- Wenn Central CLI aktiviert ist, werden die Anmeldedaten des **Systemadministrators**
- **Tabelle 3-1.**

NSX-Version	Benutzer
NSX 6.4 und weitere Versionen	<ul style="list-style-type: none"> ■ Um NSX Manager als Datenquelle hinzuzufügen, müssen Sie ein Super-Benutzer, ein Enterprise-Administrator, ein Auditor oder ein NSX-Sicherheitsadministrator sein. ■ Ein Enterprise-Administrator, ein Super-Benutzer, ein NSX-Sicherheitsadministrator oder ein Auditor können die von vRealize Network Insight erforderlichen NSX Central CLI-Befehle ausführen. <p>Hinweis Ein NSX-Netzwerkadministrator kann keine NSX Manager als Datenquelle hinzufügen.</p>
NSX 6.2 und weitere Versionen vor NSX 6.4	<ul style="list-style-type: none"> ■ Der Benutzer sollte ein Administrator sein, um die Edge-Datenauffüllung aktivieren zu können. ■ Ein Auditor, ein Super-Benutzer oder ein NSX-Sicherheitsadministrator kann die von vRealize Network Insight erforderlichen NSX Central CLI-Befehle ausführen. ■ Die Benutzeranmeldedaten, die beim Hinzufügen von NSX Manager als Datenquelle angegeben werden müssen, müssen die eines Enterprise-Administrators oder eines Super-Benutzers sein.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter **VMware Manager** auf **VMware NSX Manager**.
- 4 Geben Sie auf der Seite **Neues VMware NSX Manager-Konto oder Quelle hinzufügen** die erforderlichen Informationen ein:

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
Primäres VMware vCenter	Wählen Sie das vCenter aus, das Sie in vRealize Network Insight hinzufügen möchten. Hinweis Stellen Sie sicher, dass das vCenter und die zugehörige NSX Manager-Datenquelle demselben Collector hinzugefügt werden. Andernfalls werden die verweigerten Flows nicht angezeigt (wenn NSX IPFIX aktiviert ist) und die angewendete Firewallregel in einigen Flows ist möglicherweise nicht verfügbar.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Benutzername	Geben Sie einen Benutzernamen ein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.
- 6 (Optional) Wenn Sie NSX Controller-Daten erfassen möchten, aktivieren Sie das Kontrollkästchen **NSX Controller-Datenerfassung aktivieren**.

Wenn Sie diese Option auswählen, erfasst vRealize Network Insight Controller-Daten wie z. B. logische Router-Schnittstelle, Routen, Mac-Tabelle für logische Switches, VTEP-Datensätze, Controller-Clusterstatus und Rolle. Die Datenerfassung wird von NSX Central CLI oder der Controller-SSH-Sitzung durchgeführt.

- 7 (Optional) Wenn Sie NSX Edge-Daten erfassen möchten, aktivieren Sie das Kontrollkästchen **NSX Edge-Datenerfassung aktivieren**.

Die Edge-Datenerfassung erfolgt über NSX Central CLI. Daher werden unter NSX Manager keine Edge-Datenanbieter erstellt. Beim Aktivieren der Edge-Auffüllung werden die NSX-Benutzerrechte validiert.

Angenommen, ein Benutzer verfügt über die Berechtigung „Enterprise-Administrator“ in NSX 6.3 und arbeitet mit der aktuellen Version von vRealize Network Insight. Auf der Seite **Konten und Datenquellen** für **VMware NSX Manager** wird ein `Insufficient Privileges`-Fehler angezeigt. Der Fehler wird angezeigt, weil der Benutzer ein Super-Benutzer sein muss, um NSX Central CLI-Befehle in NSX 6.3 auszuführen.

- 8 (Optional) Wenn Sie IPFIX-Flows erfassen möchten, aktivieren Sie das Kontrollkästchen **IPFIX aktivieren**.

Wenn Sie diese Option auswählen, empfängt vRealize Network Insight DFW-IPFIX-Flows von NSX-V.

Hinweis Wenn Sie IPFIX in vCenter und in VMware NSX Manager aktivieren, erkennt und entfernt vRealize Network Insight automatisch Flow-Redundanzen durch Deaktivierung von IPFIX auf wenigen DVPGs für das zugehörige vCenter.

Weitere Informationen zur Aktivierung von IPFIX finden Sie unter [Aktivieren von VMware NSX-V IPFIX](#).

- 9 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 10 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 11 Klicken Sie auf **Absenden**.

Hinzufügen von VMware NSX-T Manager

VMware NSX-T wurde entwickelt, um auf die neuen Anwendungs-Frameworks und -Architekturen einzugehen, die über heterogene Endpoints und Technologie-Stacks verfügen. Zusätzlich zu vSphere können diese Umgebungen auch andere Hypervisoren, Container, Bare Metal und Public Clouds enthalten. vRealize Network Insight unterstützt NSX-T-Bereitstellungen, bei denen die VMs von vCenter verwaltet werden.

Überlegungen

- vRealize Network Insight unterstützt nur die NSX-T-Einrichtungen, in denen vCenter die ESXi-Hosts verwaltet.
- vRealize Network Insight unterstützt NSGroups, NSX-T-Firewallregeln, IPSets, logische Ports und logische Switches von NSX-T sowie verteilte NSX-T-Firewall-IPFIX-Flows, Segment, Gruppe und Richtlinie auf der Basis des VPN.
- vRealize Network Insight unterstützt sowohl NSX-V als auch NSX-T-Bereitstellungen. Wenn Sie NSX in Ihren Abfragen verwenden, enthalten die Ergebnisse sowohl NSX-V- als auch NSX-T-Einheiten. NSX Manager enthält sowohl NSX-V- als auch NSX-T Manager. NSX-Sicherheitsgruppen enthalten sowohl NSX-T- als auch NSX-V-Sicherheitsgruppen. Wenn NSX-V oder NSX-T anstelle von NSX verwendet wird, werden nur diese Einheiten angezeigt. Dieselbe Logik gilt für Einheiten wie z. B. Firewallregeln, IPSets und logische Switches.

- Mit der Version NSX-T 2.4 unterstützt vRealize Network Insight die deklarative Richtlinienverwaltung von NSX, die Netzwerk- und Sicherheitskonfigurationen über ergebnisgesteuerte Richtlinienanweisungen vereinfacht und automatisiert.

Hinweis Die Mikrosegmentierung für die Sicherheitsgruppe erfolgt auf der Grundlage der Daten der NSX-Richtlinie. Wenn jedoch keine entsprechende NSX-Richtliniengruppe vorhanden ist, ist die eigenständige NS-Gruppe in der Mikrosegmentierungsanalyse enthalten. Weitere Informationen zur NS-Gruppe finden Sie in der [NSX-T-Produktdokumentation](#).

Hinzufügen eines NSX-T Managers als Datenquelle

Hier sind die Voraussetzungen für das Hinzufügen eines NSX-T Managers als Datenquelle:

- Es wird empfohlen, alle vCenter, die NSX-T Manager zugeordnet sind, als Datenquellen in vRealize Network Insight hinzuzufügen.
- Wenn Sie vor dem Hinzufügen des vCenter NSX-T Manager hinzufügen, benötigt vRealize Network Insight etwa 4 Stunden für die Stabilisierung.
- Stellen Sie sicher, dass in der Ausschlussliste der verteilten Firewall (Distributed Firewall, DFW) keine logischen Switches vorhanden sind. Wenn in dieser Liste logische Switches vorhanden sind, werden für keine der VMs Flows gemeldet, die mit diesen logischen Switches verknüpft sind.

So fügen Sie einen NSX-T Manager hinzu:

- 1 Klicken Sie auf der Seite **Konten und Datenquelle** unter **Einstellungen** auf **Quelle hinzufügen**.
- 2 Wählen Sie unter **VMware Manager** auf der Seite **Konto oder Datentyp auswählen VMware NSX-T Manager** aus.
- 3 Geben Sie die Anmeldedaten an.

Hinweis

- Wenn Sie mehrere Verwaltungsknoten in einer einzelnen NSX-T-Bereitstellung haben, müssen Sie nur einen Knoten als Datenquelle in vRealize Network Insight hinzufügen oder die virtuelle IP (VIP) (dieser Knoten) verwenden. Wenn Sie mehr als einen Verwaltungsknoten hinzufügen, funktioniert vRealize Network Insight möglicherweise nicht ordnungsgemäß.
 - Es wird empfohlen, eine VIP zu verwenden, wenn Sie NSX-T als Datenquelle hinzufügen. Wenn Sie eine Verwaltungsknoten-IP anstelle einer VIP hinzufügen, und später eine VIP- oder eine andere Verwaltungsknoten-IP hinzufügen möchten, müssen Sie die vorhandene Datenquelle löschen, um die neue VIP oder Verwaltungs-IP hinzuzufügen.
 - Wenn IPFIX nicht erforderlich ist, muss der Benutzer ein lokaler Benutzer mit den Berechtigungen für die Überwachungsebene sein. Wenn IPFIX erforderlich ist, muss der Benutzer über eine der folgenden Berechtigungen für die Überwachungsebene verfügen: **enterprise_admin**, **network_engineer** oder **security_engineer**.
-

- 4 (Optional) Klicken Sie auf **DFW-IPFIX aktivieren**, um die IPFIX-Einstellungen von NSX-T zu aktualisieren. Wenn Sie diese Option auswählen, empfängt vRealize Network Insight DFW-IPFIX-Flows von NSX-T. Weitere Informationen zum Aktivieren von IPFIX finden Sie unter [Aktivieren von VMware NSX-T DFW IPFIX](#).

Hinweis

- DFW IPFIX wird in der Standard Edition von NSX-T nicht unterstützt.
- vRealize Network Insight unterstützt keine IPFIX-Flows für NSX-T-Switches.

- 5 (Optional) Für die Erfassung von Latenzmetrikdaten aktivieren Sie das Kontrollkästchen **Erfassung von Latenzmetrik aktivieren**. Bei Auswahl dieser Option empfängt vRealize Network Insight Latenzmetriken (VTEP - VTEP) von NSX-T. Diese Option ist nur für NSX-T 2.5 und höher verfügbar. Stellen Sie sicher, dass Port 1991 auf dem Collector geöffnet ist, um die Latenzdaten vom ESXi-Knoten zu empfangen.

Beispiele für Abfragen

Im Folgenden finden Sie einige Beispiele für Abfragen im Zusammenhang mit NSX-T:

Tabelle 3-2. Abfragen für NSX-T

Abfragen	Suchergebnisse
<code>NSX-T Manager where VC Manager=10.197.53.214</code>	NSX-T Manager, bei dem dieser bestimmte VC Manager als Compute Manager hinzugefügt wurde.
<code>NSX-T Logical Switch</code>	Listet alle logischen NSX-T-Switches auf, die in der Instanz von vRealize Network Insight vorhanden sind, einschließlich Details dazu, ob es sich um einen vom System von einem Benutzer erstellten Switch handelt.
<code>NSX-T Logical Ports where NSX-T Logical Switch = 'DB-Switch'</code>	Enthält die logischen NSX-T-Ports, die zu diesem speziellen logischen NSX-T-Switch, DB-Switch, gehören.
<code>VMs where NSX-T Security Group = 'Application-Group'</code> Or <code>VMs where NSGroup = 'Application-Group'</code>	Enthält alle VMs in dieser bestimmten Sicherheitsgruppe, Application-Group.
<code>NSX-T Firewall Rule where Action='ALLOW'</code>	Enthält alle NSX-T-Firewallregeln, deren Aktion als „ALLOW“ festgelegt ist.
<code>NSX-T Firewall Rule where Destination Security Group = 'CRM-Group'</code>	Enthält Firewallregeln, bei denen CRM-Group die Zielsicherheitsgruppe ist. Die Ergebnisse beinhalten sowohl direkte Zielsicherheitsgruppen als auch indirekte Zielsicherheitsgruppen.
<code>NSX-T Firewall Rule where Direct Destination Security Group = 'CRM-Group'</code>	Enthält Firewallregeln, bei denen CRM-Group die Zielsicherheitsgruppe ist. Die Ergebnisse beinhalten nur die direkten Zielsicherheitsgruppen.
<code>VMs where NSX-T Logical Port = 'App_Port-Id-1'</code>	Enthält alle VMs, die über diesen speziellen logischen NSX-T-Port verfügen.

Tabelle 3-2. Abfragen für NSX-T (Fortsetzung)

Abfragen	Suchergebnisse
NSX-T Transport Zone	Enthält das VLAN und die Overlay-Transportzone sowie die entsprechenden zugehörigen Details, einschließlich des Typs des Transportknotens. Hinweis vRealize Network Insight bietet keine Unterstützung für KVM als Datenquelle.
NSX-T Router	Enthält die Router der Tier 1 und Tier 0. Klicken Sie auf den in den Ergebnissen angezeigten Router, um weitere Details dazu anzuzeigen, einschließlich des NSX-T-Edge-Clusters und des HA-Modus.

Tabelle 3-3. Abfragen für NSX-Richtlinie

NSX-Richtliniensegment	Listet alle NSX-Richtliniensegmente auf, die in der Instanz von vRealize Network Insight vorhanden sind.
NSX Policy Manager	Listet alle NSX Policy Manager-Instanzen auf, die in der Instanz von vRealize Network Insight vorhanden sind.
NSX Policy Group	Listet alle NSX-Richtliniengruppen auf, die in der Instanz von vRealize Network Insight vorhanden sind.
NSX Policy Firewall	Listet alle Firewalls der NSX-Richtlinie auf, die in der Instanz von vRealize Network Insight vorhanden sind.
NSX Policy Firewall Rule	Listet alle Firewallregeln der NSX-Richtlinie auf, die in der Instanz von vRealize Network Insight vorhanden sind.
NSX Policy Firewall Rule where Action = 'ALLOW'	Listet alle NSX-Firewallregeln auf, deren Aktion als „ALLOW“ festgelegt ist.
NSX Policy Based VPN	Listet alle auf der NSX-Richtlinie basierenden VPNs auf, die in der Instanz von vRealize Network Insight vorhanden sind.

Hinweis Wenn NSX-T 2.4 und VMware Cloud on AWS als Datenquellen in Ihrem vRealize Network Insight hinzugefügt werden, müssen Sie zum Abrufen der NSX-T-Einheiten den Filter **SDDC type = ONPREM** in Ihrer Abfrage hinzufügen. Beispiel: **NSX Policy Based VPN where Tier0 = '' and SDDC Type = 'ONPREM'**.

Unterstützung für NSX-T-Metriken

In der folgenden Tabelle werden die vRealize Network Insight-Einheiten angezeigt, die gegenwärtig die NSX-T-Metriken unterstützen, sowie die Widgets, die diese Metriken auf den entsprechenden Einheiten-Dashboards anzeigen.

Tabelle 3-4.

Elemente	Widgets auf dem Einheiten-Dashboard	Unterstützte NSX-T-Metriken
Logischer Switch	Paketmetriken für logische Switches Byte-Metriken für logische Switches	Multicast and Broadcast Rx Multicast and Broadcast Tx Unicast Rx Unicast Tx Dropped Rx Dropped Tx Rx Packets (Total) Tx Packets (Total)
Logischer Port	Paketmetriken für logische Ports Byte-Metriken für logische Ports	Multicast and Broadcast Rx Multicast and Broadcast Tx Unicast Rx Unicast Tx Rx Packets (Total) Tx Packets (Total)
Routerschnittstelle	Metriken für Routerschnittstellen	Rx Packets Tx Packets Dropped Rx Packets Dropped Tx Packets Rx Bytes Tx Bytes
Firewallregel	Metriken für Firewallregeln	Hit Count Flow Bytes Flow Packets

Im Folgenden finden Sie einige Beispielabfragen für NSX-T-Metriken:

- `nsx-t logical switch where Rx Packet Drops > 0`

Diese Abfrage enthält alle logischen Switches, bei denen die Anzahl der verworfenen empfangenen Pakete größer als 0 ist.

- `nsx-t logical port where Tx Packet Drops > 0`

Diese Abfrage enthält alle logischen Ports, bei denen die Anzahl der verworfenen übertragenen Pakete größer als 0 ist.

- `top 10 nsx-t firewall rules order by Connection count`

Diese Abfrage enthält die 10 wichtigsten Firewallregeln, basierend auf der Anzahl der Verbindungen (Hit Count).

Hinzufügen von VMware SD-WAN

Sie können VMware SD-WAN von VeloCloud als Datenquelle in vRealize Network Insight hinzufügen.

Voraussetzungen

Stellen Sie Folgendes sicher:

- Sie verfügen über die korrekte Berechtigung zum Hinzufügen der Datenquelle. Informationen zu Berechtigungen finden Sie unter [Unterstützte Produkte und Versionen](#).
- Sie verwenden VeloCloud Orchestrator und Edge der Version 3.3.1 oder höher.
- Sie haben mindestens eine VMware SD-WAN-Lizenz hinzugefügt.
- Es wurde keine andere VMware SD-WAN-Instanz als Datenquelle hinzugefügt.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter **SD-WAN** auf **VeloCloud**.
- 4 Geben Sie auf der Seite **Neues VeloCloud-Konto oder neue Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
VCO-URL	Geben Sie die VCO-URL ein, die Sie als Datenquelle hinzufügen möchten.
Benutzername	Geben Sie einen Benutzernamen ein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.
- 6 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 7 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 8 Klicken Sie auf **Absenden**.

Nächste Schritte

Sie müssen NetFlow für alle Profile und Edges auf Port 2055 aktivieren. Um zu erfahren, wie Sie die NetFlow-Erfassung aktivieren, klicken Sie auf der Seite **Datenquelle bearbeiten** für VMware SD-WAN auf **Anweisungen anzeigen**.

Hinweis Die Option **Anweisungen anzeigen** wird unter **Hinweis: Die NetFlow-Erfassung sollte für alle Profile und Edges aktiviert sein** angezeigt.

Hinzufügen von Cisco ASR/ISR für SD-WAN-Bewertung

Sie können Cisco ASR/ISR-Router als Datenquelle in vRealize Network Insight ausschließlich für die SD-WAN-Bewertung hinzufügen. vRealize Network Insight unterstützt keine Cisco ASR/ISR-Router als Datenquelle für andere Zwecke.

vRealize Network Insight unterstützt nur die folgende Version für die Cisco ASR/ISR für SD-WAN-Bewertung:

Version/Modell	Unterstütztes Betriebssystem	OS-Version
ASR 1K, ISR4K, CSR1Kv, ISR1K	Cisco IOS XE Software	16.07.01

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter **WAN** auf **Cisco ASR/ISR (SD-WAN-Bewertung)**.
- 4 Geben Sie auf der Seite **Neues Cisco ASR/ISR-Konto oder Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse	Geben Sie die IP-Adressdetails ein. Hinweis Sie können diese Datenquelle nicht mithilfe eines beliebigen FQDN hinzufügen. Sie müssen zum Hinzufügen dieser Datenquelle die IP-Adressdetails eingeben.
Benutzername	Geben Sie einen Benutzernamen ein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.
- 6 Wählen Sie im Dropdown-Menü **SNMP-Version 2C** aus.
- 7 Geben Sie im Textfeld **Community-Zeichenfolge** eine Community-Zeichenfolge ein.
- 8 Ordnen Sie jede Uplink-Schnittstelle entweder MPLS oder Internet zu. Um die Uplink-Schnittstelle zuzuordnen, klicken Sie auf das Dropdown-Menü für jeden **Schnittstellennamen** und wählen Sie eine entsprechende Option aus.

Standardmäßig ruft vRealize Network Insight alle Uplink-Schnittstellen ab und listet sie auf.
- 9 Geben Sie im Textfeld **Spitzname** einen neuen Spitznamen für die Datenquelle ein.
- 10 Geben Sie in den Textfeldern **Site** und **Region** einen geeigneten Namen für die Site und die Region ein.
- 11 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.

12 Klicken Sie auf **Absenden**.

Nächste Schritte

- 1 [Hinzufügen eines physischen Flow-Collectors für NetFlow und sFlow](#).
- 2 Konfigurieren Sie Cisco ASR/ISR so, dass die NetFlow-Informationen an den vRealize Network Insight-Collector gesendet werden. Informationen zum Konfigurieren eines NetFlow finden Sie unter [Konfigurieren eines NetFlow-Collectors in einem physischen Gerät](#).

Hinweis Es dauert etwa vier Stunden, bis genügend Flow-Informationen für die SD-WAN-Bewertung erfasst sind.

- 3 Wechseln Sie zur Seite „Anzeigen von SD-WAN-Bewertungsdetails“, um Ihre SD-WAN-Bewertungsdetails abzurufen.

Hinzufügen von VMware Cloud on AWS

vRealize Network Insight unterstützt VMware Cloud on AWS nur für die Enterprise-Lizenzbenutzer. Sie können VMware Cloud on AWS (vCenter) oder VMware Cloud on AWS (NSX Policy Manager) als Datenquelle hinzufügen.

Einrichten des vRealize Network Insight-Collectors für VMware Cloud on AWS

Sie müssen den vRealize Network Insight-Collector einrichten, um Daten von VMware Cloud on AWS erfassen zu können.

Voraussetzungen

Stellen Sie in jedem SDDC, das als Datenquelle hinzugefügt werden muss, einen vRealize Network Insight-Collector bereit.

Hinweis

- Die Verwendung eines vRealize Network Insight-Collectors, der in einem VMware Cloud on AWS-SDDC zur Erfassung von Daten aus einem anderen VMware Cloud on AWS-SDDC bereitgestellt wurde, wird nicht unterstützt.
 - Sie müssen den vRealize Network Insight-Collector auf einem nativen VMware Cloud on AWS-Segment bereitstellen. Das Bereitstellen eines Collectors in erweiterten Segmenten wird nicht unterstützt.
-

Verfahren

- 1 Melden Sie sich bei vRealize Network Insight an.
- 2 Navigieren Sie zu **Einstellungen > Installation und Support > Collector-VM hinzufügen**.
- 3 Kopieren Sie den Inhalt des gemeinsamen geheimen Schlüssels.
Dieser wird während der Bereitstellung der vRealize Network Insight-Collector-OVA benötigt.

- 4 Stellen Sie die vRealize Network Insight-Collector-OVA im Computing-Ressourcenpool des VMware Cloud on AWS-vCenters bereit.

Verwenden Sie den gemeinsamen geheimen Schlüssel, den Sie generiert haben.

Hinweis Bei einem SDDC mit einem Knoten muss in VMware Cloud on AWS die CPU-Ressourcenreservierung für die Proxy-VM mindestens 1251 MHz betragen.

- 5 Starten Sie die Collector-VM und befolgen Sie den Assistenten, um den Collector mit der vRealize Network Insight-Plattform zu koppeln.
- 6 Prüfen Sie, ob der Collector erfolgreich mit der Plattform gekoppelt werden kann.

Erstellen von VMware Cloud on AWS-Firewallregeln für vRealize Network Insight

Sie müssen VMware Cloud on AWS-Gruppen und -Firewallregeln erstellen, um die Kommunikation mit vRealize Network Insight aufzubauen.

Voraussetzungen

- Stellen Sie die vRealize Network Insight-Plattform und den -Collector (für die lokale Verwendung) bereit oder holen Sie sich das gültige Abonnement (für den Cloud-Dienst).
- Sie müssen über die erforderlichen Rechte verfügen. Weitere Informationen finden Sie unter [Unterstützte Produkte und Versionen](#).
- Stellen Sie ein VMware Cloud on AWS-SDDC (Software-Defined Data Center) 1.8 oder höher mit NSX-T-Netzwerk bereit.
- [Konfigurieren von Firewallregeln für die Kommunikation zwischen vRealize Network Insight-Plattform und -Collector](#).
- Informationen zu den Portanforderungen des eingehenden Datenverkehrs finden Sie in der Tabelle „Ports für die Collector Server“ auf der Seite „Systemports“.
- Öffnen Sie den HTTPS-Port 443 für ausgehenden Datenverkehr zu den folgenden Domänen:
 - *.vmwareidentity.com
 - gaz.csp-vidm-prod.com
 - *.vmware.com
 - *.ni-onsaas.com

Konfigurieren von Firewallregeln für die Kommunikation zwischen vRealize Network Insight-Plattform und -Collector

Zur Konfiguration von Firewallregeln in VMware Cloud on AWS gehört Folgendes:

- Erstellen einer VMware Cloud on AWS-Gruppe für den vRealize Network Insight-Collector
 - a Melden Sie sich unter <https://vmc.vmware.com> bei VMware Cloud on AWS an.

- b Klicken Sie auf der Registerkarte **Netzwerk und Sicherheit** auf **Bestand > Gruppen**.
- c Klicken Sie auf der Karte **Gruppen** auf **COMPUTING-GRUPPEN**, klicken Sie dann auf **GRUPPE HINZUFÜGEN** und legen Sie für die Gruppe einen **Namen** und eine optionale **Beschreibung** fest.
- d Klicken Sie auf **Mitglieder festlegen**, um die Seite **Mitglieder auswählen** zu öffnen.
- e Geben Sie die Details der vRealize Network Insight-Collector-VM an.

Sie verwenden diese Gruppe in den Firewallregeln, die Sie später erstellen, um die Kommunikation zwischen VMware Cloud on AWS NSX Manager und vRealize Network Insight zuzulassen.

- Erstellen Sie eine Firewallregel.
 - a Melden Sie sich unter <https://vmc.vmware.com> bei der VMC-Konsole an.
 - b Klicken Sie auf der Registerkarte **Netzwerk und Sicherheit** auf **Gateway-Firewall**.
 - c Klicken Sie auf der Karte **Gateway-Firewall** auf **Computing-Gateway**, dann auf **REGEL HINZUFÜGEN**, und geben Sie unter **Name** einen neuen Namen für die Regel ein.
 - d Geben Sie die Parameter für die neue Regel ein.
 - **Quellen:** Geben Sie den Namen der VMware Cloud on AWS-Gruppe ein, die die IP-Adresse des vRealize Network Insight-Collectors enthält.
 - **Ziele:** Wählen Sie **Beliebig** aus.
 - **Dienste:** Wählen Sie **HTTPS, DNS, DNS-UDP, NTP** oder **ICMP** aus.
 - **Aktion:** Wählen Sie **Zulassen** aus.
 - **Angewendet auf:** Wählen Sie **Internetschnittstelle** aus.
 - **Protokollierung:** Aktivieren Sie bei Bedarf die Protokollierung. Ansonsten bleibt dieses Feld unverändert.

Die neue Regel wird standardmäßig aktiviert. Schieben Sie den Umschalter nach links, um sie zu deaktivieren.
 - e Klicken Sie auf **Veröffentlichen**.

Konfigurieren von Firewallregeln für die Kommunikation zwischen Collector und NSX Manager sowie Collector und vCenter

- 1 Melden Sie sich unter <https://vmc.vmware.com> bei der VMC-Konsole an.
- 2 Klicken Sie auf der Registerkarte **Netzwerk und Sicherheit** auf **Gateway-Firewall**.
- 3 Klicken Sie auf der Karte **Gateway-Firewall** auf **Verwaltungs-Gateway**, dann auf **REGEL HINZUFÜGEN** und geben Sie unter **Name** einen neuen Namen für die Regel ein.

4 Geben Sie die Parameter für die neue Regel ein.

- **Quellen:** Geben Sie den Namen der VMware Cloud on AWS-Gruppe ein, die die IP-Adresse des vRealize Network Insight-Collectors enthält.
- **Ziele:** Wählen Sie **Systemdefinierte Gruppen** aus, suchen Sie nach NSX Manager und wählen Sie dann den NSX Manager-Eintrag aus.
- **Dienste:** Wählen Sie **HTTPS (443)** aus.
- **Aktion:** Wählen Sie **Zulassen** aus.
- **Protokollierung:** Aktivieren Sie bei Bedarf die Protokollierung.

Die neue Regel wird standardmäßig aktiviert. Schieben Sie den Umschalter, um sie zu deaktivieren.

5 Klicken Sie auf **Veröffentlichen**.

6 Führen Sie dieselben Schritte aus, um eine Regel für den vCenter Server zu konfigurieren.

Hinweis Stellen Sie sicher, dass Sie in Schritt 4 für das Feld „Ziele“ das vCenter auswählen.

Hinzufügen eines VMware Cloud on AWS-vCenters

Sie können VMware Cloud on AWS vCenter als Datenquelle hinzufügen.

Voraussetzungen

- Anmeldeinformationen abrufen, um VMware Cloud on AWS – vCenter als Datenquelle hinzuzufügen
 - a Melden Sie sich bei ihrer VMware Cloud Services-Konsole an.
 - b Klicken Sie auf **VMware Cloud auf AWS** unter **Meine Dienste**.
 - c Klicken Sie auf den Namen des gewünschten SDDC.
 - d Wählen Sie die Registerkarte **Einstellungen** aus und führen Sie die folgenden Aufgaben aus:
 - Erweitern Sie den Bereich **vCenter-FQDN** und kopieren oder notieren Sie den **vCenter-FQDN**.
 - Erweitern Sie den Bereich **Standard-vCenter-Benutzerkonto** und kopieren oder notieren Sie die Benutzeranmeldeinformationen.
- Sie benötigen mindestens das Recht **Nur Lesen** für das VMware Cloud on AWS-vCenter.

Verfahren

- 1 Navigieren Sie in der vRealize Network Insight-Benutzeroberfläche zu **Einstellungen > Konten und Datenquellen > Quelle hinzufügen**.
- 2 Klicken Sie unter **VMware Cloud on AWS** auf **VMware Cloud on AWS – vCenter**.

3 Fügen Sie auf der Seite **VMware Cloud on AWS – VMware vCenter hinzufügen**

- Wählen Sie die Collector-VM aus.
- Geben Sie den vCenter-FQDN an, den Sie aus VMware Cloud Services abgerufen haben.
- Geben Sie die Benutzeranmeldedaten an, die Sie aus VMware Cloud Services abgerufen haben.

4 Klicken Sie auf **Validieren**.

5 Geben Sie **Spitzname** und **Notizen** (sofern vorhanden) für die Datenquelle ein und klicken Sie auf **Absenden**.

6 [Hinzufügen von VMware Cloud on AWS – NSX Manager](#).

Hinzufügen von VMware Cloud on AWS – NSX Manager

Sie können VMware Cloud on AWS – NSX Manager als Datenquelle hinzufügen.

Voraussetzungen

- [Generieren Sie API-Token](#).
- Um alle verfügbaren vRealize Network Insight-Funktionen zu nutzen und DFW IPFIX auf VMware Cloud on AWS Policy Manager zu aktivieren, müssen Sie über die Rollen **Administrator** und **NSX Cloud Admin** verfügen. Ihr Zugriff auf die Funktionen ist jedoch auch mit der **NSX Cloud Auditor**-Rolle (nur Leseberechtigung) möglich. Weitere Informationen finden Sie in der folgenden Tabelle:

Organisationsrolle	Dienstrolle	Zulässige Aktionen
Organisationsmitglied	Administrator	Datenquelle hinzufügen, IPFIX aktivieren
Organisationsmitglied	Administrator und NSX Cloud Admin	Datenquelle hinzufügen, IPFIX aktivieren
Organisationsmitglied	VMware Cloud on AWS (alle Rollen)	Datenquelle hinzufügen, IPFIX aktivieren
Organisationsmitglied	NSX Cloud Auditor	Nur Datenquelle hinzufügen

Verfahren

1 Führen Sie einen der folgenden Schritte durch:

- Wenn Sie VMware Cloud on AWS – vCenter nicht hinzugefügt haben,
 - a [Hinzufügen eines VMware Cloud on AWS-vCenters](#).
 - b Klicken Sie auf **NSX Manager hinzufügen**.
- Wenn Sie VMware Cloud on AWS – vCenter bereits hinzugefügt haben,
 - a Klicken Sie auf **Einstellungen > Konten und Datenquellen > Quelle hinzufügen**.
 - b Klicken Sie unter **VMware Cloud on AWS** auf **VMware Cloud on AWS – NSX Manager**.

2 Auf der Seite **Neues VMC NSX Manager-Konto hinzufügen**:

- Wählen Sie das entsprechende vCenter aus.

Der Collector wird automatisch basierend auf der Auswahl des vCenter ausgewählt. VMware Cloud on AWS. Sie müssen den NSX Manager zu derselben Collector-VM hinzufügen wie der des entsprechenden vCenter.

- Geben Sie die IP-Adresse und das generierte API-Token an.

Die IP des NSX Managers ist auf der Registerkarte **Support** im VMware Cloud on AWS-SDDC verfügbar.

3 Klicken Sie auf **Validieren**.

4 Wenn Sie IPFIX-Flows für DFW erfassen möchten, wählen Sie **DFW IPFIX aktivieren** aus.

Hinweis Die Fehlermeldungen werden in den folgenden Fällen angezeigt:

- Sie verfügen nicht über das Recht `NSX Cloud Admin`.
- Sie haben bereits vier Collectors zum DFW-IPFIX-Collector-Profil hinzugefügt. Weitere Informationen finden Sie auch unter [Aktivierung von DFW-IPFIX nicht möglich](#).

5 Geben Sie **Spitzname** und **Notizen** (sofern vorhanden) für die Datenquelle ein und klicken Sie auf **Absenden**.

Hinzufügen von Amazon Web Services

Sie können Amazon Web Services (AWS) als Datenquelle in vRealize Network Insight hinzufügen.

Die folgenden beiden Arten von AWS-Konten können Sie als Datenquelle hinzufügen.

- Primäre AWS-Konten und verknüpfte AWS-Konten
- AWS-Standardkonto

Primäre AWS-Konten und verknüpfte AWS-Konten

Das primäre AWS-Konto (Organisations- oder Payer-Konto) verfügt über Zugriff auf Organisationsebene, um alle verknüpften AWS-Konten in Ihrer Organisation über API-Aufrufe zu ermitteln und aufzulisten.

Alle AWS-Konten in Ihrer Organisation, die dem primären Konto hinzugefügt werden, werden als „verknüpfte Konten“ bezeichnet. Weitere Informationen finden Sie unter [ListAccount](#).

Das primäre AWS-Konto muss eine Rolle bezüglich der verknüpften AWS-Konten übernehmen, um auf die Ressourcen des verknüpften AWS-Kontos zuzugreifen und diese zu steuern.

Alle verknüpften AWS-Konten müssen das primäre AWS-Konto über einen Rollen-ARN als vertrauenswürdig einstufen. Weitere Informationen zu Rollen finden Sie unter [AssumeRole](#).

Wenn Sie ein primäres AWS-Konto als Datenquelle hinzufügen, werden alle verknüpften AWS-Konten automatisch als Datenquelle hinzugefügt.

AWS-Standardkonto

Ein AWS-Standardkonto hat keine Primär/Verknüpft-Beziehung.

Hinzufügen eines primären AWS-Kontos

Durch Hinzufügen eines primären AWS-Kontos können Sie automatisch alle verknüpften AWS-Konten in Ihrer Organisation in vRealize Network Insight hinzufügen.

Voraussetzungen

- Konfigurieren der Firewall für den AWS-API-Zugriff.
- Erstellen einer Richtlinie für primäre und verknüpfte Konten.
- Erstellen einer Rolle in AWS.
- Erstellen eines Benutzers im primären AWS-Konto.
- Rufen Sie Ihre Amazon-Zugriffsschlüssel-ID ab, die Sie in der AWS-Konsole erstellt haben. Nähere Informationen finden Sie unter <http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html>.
- Rufen Sie die „Amazon-Ressourcennamen“ (ARN) aus dem verknüpften AWS-Konto ab. Weitere Informationen finden Sie unter [Amazon-Ressourcennamen \(ARNs\) und AWS-Dienst-Namespace](#).

Verfahren

- 1 Melden Sie sich bei vRealize Network Insight an.
- 2 Navigieren Sie zu **Einstellungen > Konten und Datenquellen > Quelle hinzufügen**.
- 3 Klicken Sie unter dem Abschnitt „Public Clouds“ auf **Amazon Web Services**.
- 4 Wählen Sie die Collector (Proxy)-VM aus.
- 5 Geben Sie Ihre Amazon-Zugriffsschlüssel-ID und den zugehörigen geheimen Zugriffsschlüssel ein.

vRealize Network Insight braucht 15 bis 20 Minuten zum Erfassen Ihrer AWS-Kontodaten.

- 6 Klicken Sie auf **Validieren**.

Wenn die Anzahl der erkannten VMs die Kapazität der Plattform oder eines Collector-Knotens oder beides überschreitet, schlägt die Validierung fehl. Sie können erst dann eine Datenquelle hinzufügen, wenn Sie die Brick-Größe der Plattform erhöhen oder ein Cluster erstellen. Die angegebene Kapazität für jede Brick-Größe mit und ohne Flows lautet wie folgt:

Brick-Größe	VMs	Status der Flows
Groß	6k	Aktiviert
Groß	10k	Deaktiviert

Brick-Größe	VMs	Status der Flows
Mittel	3k	Aktiviert
Mittel	6k	Deaktiviert

- 7 Nachdem die Validierung Ihres AWS-Kontos abgeschlossen ist, wählen Sie die Option **Automatisch verknüpfte Konten hinzufügen**.
- 8 Geben Sie in **ARN der Rolle** die Rolle „Amazon-Ressourcennamen“ aus dem verknüpften AWS-Konto ein, um dem primären AWS-Konto zu vertrauen.
- 9 Geben Sie den **Spitznamen** und **Notizen** für die Datenquelle ein.
- 10 Klicken Sie auf **Absenden**.

vRealize Network Insight validiert den Rollen-ARN und fügt das Konto hinzu.

Erstellen einer Richtlinie für primäre und verknüpfte Konten

Sie müssen eine Richtlinie für primäre Konten für das primäre AWS-Konto (Amazon Web Service) sowie eine Richtlinie für verknüpfte Konten erstellen, die für alle verknüpfte AWS-Konten gelten soll. Sie können diese Richtlinien verwenden, um den Zugriff in AWS zu verwalten.

Sie können die AWS-Richtlinie an eine IAM-Identität anhängen, z. B. Benutzer oder Rollen. Weitere Informationen finden Sie unter [Richtlinien und Berechtigungen](#).

Verfahren

- 1 Klicken Sie in der AWS-Konsole auf **IAM > Richtlinien > Richtlinie erstellen**.
- 2 Klicken Sie auf der Seite **Richtlinie erstellen** auf die Registerkarte **JSON**.

3 Geben Sie im Textfeld **JSON** eine Richtlinie ein.

Option	Bezeichnung
<p>Richtlinie für primäre Konten hinzufügen</p> <hr/> <p>Hinweis Sie müssen die Richtlinie für primäre Konten im primären AWS-Konto hinzufügen.</p>	<pre data-bbox="651 304 1399 1442"> { "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>Verknüpftes Konto hinzufügen</p> <hr/> <p>Hinweis Sie müssen die Richtlinie für verknüpfte Konten in allen verknüpften Konten hinzufügen, die im primären AWS-Konto hinzugefügt wurden.</p>	<pre data-bbox="651 1501 1399 1881"> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": [</pre>

Option	Bezeichnung
	<pre data-bbox="638 220 1412 651"> "ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }] } </pre>

- 4 Klicken Sie auf **Richtlinie überprüfen**.
- 5 Geben Sie unter dem Abschnitt **Richtlinie überprüfen** einen Namen für die Richtlinie ein und klicken Sie auf **Richtlinie erstellen**.

Nächste Schritte

Melden Sie sich der Reihe nach bei allen verknüpften Konten an und fügen Sie eine Rolle hinzu, um das primäre AWS-Konto, das Sie vRealize Network Insight hinzufügen möchten, als vertrauenswürdig einzustufen und die Richtlinie für verknüpfte Konten anzuhängen. Informationen zum Erstellen einer Rolle und zum Anhängen der Richtlinie für verbundene Konten finden Sie unter [Erstellen einer Rolle in AWS](#).

Hinweis Wenn eine in allen verknüpften Konten erstellte Rolle bereits die Berechtigungen für die Standardrichtlinie enthält und dem primären Konto vertraut, überspringen Sie diesen Schritt.

Erstellen einer Rolle in AWS

Sie können eine AWS-Rolle erstellen, um die Konten, die Sie vRealize Network Insight hinzufügen möchten, als vertrauenswürdig einzustufen.

Voraussetzungen

Erstellen Sie eine Liste aller in [Erstellen einer Richtlinie für primäre und verknüpfte Konten](#) erstellten Richtlinien für verknüpfte Konten.

Verfahren

- 1 Klicken Sie in der AWS-Konsole auf **Dienste > IAM > Rollen > Rolle erstellen**.
- 2 Klicken Sie auf der Seite **Rolle erstellen** auf **Weiteres AWS-Konto**.
- 3 Geben Sie im Textfeld **Konto-ID** die ID des primären Kontos ein, das Sie als vertrauenswürdig einstufen möchten, und klicken Sie auf **Weiter:Berechtigung**.

- 4 Suchen Sie alle Richtlinien für verbundene Konten und wählen Sie sie aus. Klicken Sie dann auf **Weiter:Tags**.
- 5 Geben Sie im Abschnitt **Überprüfen** einen **Rollennamen** ein und klicken Sie auf **Rolle erstellen**.

Nächste Schritte

[Erstellen eines Benutzers im primären AWS-Konto](#).

Erstellen eines Benutzers im primären AWS-Konto

Sie müssen einen Benutzer im AWS-Konto erstellen, um die Amazon-Zugriffsschlüssel-ID und den entsprechenden geheimen Zugriffsschlüssel zu erhalten, die Sie während der Hinzufügung von Datenquellen in vRealize Network Insight verwenden.

Verfahren

- 1 Melden Sie sich bei der AWS-Konsole an.
- 2 Klicken Sie auf **Dienste > IAM > Benutzer > Benutzer hinzufügen**.
- 3 Geben Sie auf der Seite **Benutzer hinzufügen** einen **Benutzernamen** ein, aktivieren Sie das Kontrollkästchen **Programmgesteuerter Zugriff** und klicken Sie auf **Nächste Berechtigung**.
- 4 Klicken Sie unter der Gruppe **Berechtigung festlegen** auf **Vorhandene Richtlinien direkt angehängt**, suchen Sie eine Kontorichtlinie, die Sie zuvor erstellt haben, und wählen Sie sie aus.
 - Wählen Sie für ein primäres AWS-Konto die Richtlinie für primäre Konten aus.
 - Wählen Sie für ein AWS-Standardkonto die Richtlinie für Standardkonten aus.
- 5 Klicken Sie auf **Next-Tags > Next:Review**.
- 6 Klicken Sie auf **Benutzer erstellen**.
- 7 Notieren Sie die **Zugriffsschlüssel-ID** und den **geheimen Zugriffsschlüssel**.

Nächste Schritte

- [Hinzufügen eines primären AWS-Kontos](#).
- [Hinzufügen einer AWS-Standarddatenquelle](#).

Konfigurieren der Firewall für den AWS-API-Zugriff

Die Collector-VM benötigt eine Liste von URLs, um Zugriff auf die AWS zu erhalten.

- Die AWS kann in mehreren Regionen bereitgestellt werden. Es gibt separate URLs, die verschiedenen Regionen zugeordnet sind. Wenn Sie die Region oder den Dienst nicht kennen, nutzen Sie einen Platzhaltereintrag für die URL, z. B. *.amazonaws.com.

Hinweis Der Platzhaltereintrag funktioniert nicht für die Region China.

Wenn Sie einen differenzierten Zugriff auf separate URLs gewähren möchten, gibt es vier Dienste, basierend auf der Region:

- Regionen mit Ausnahme von GovCloud und China

- `ec2.<REGION>.amazonaws.com`
- `logs.<REGION>.amazonaws.com`
- `sts.<REGION>.amazonaws.com`
- `iam.amazonaws.com`

GovCloud-Region

- `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`

Region China (Peking)

- `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`

Sie können einen der folgenden Werte für `REGION` basierend auf der AWS-Region verwenden:

Name der Region	Region
US-Osten (Ohio)	<code>us-east-2</code>
US-Osten (N. Virginia)	<code>us-east-1</code>
US-Westen (N. California)	<code>us-west-1</code>
US-Westen (Oregon)	<code>us-west-2</code>
Asien-Pazifik (Mumbai)	<code>ap-south-1</code>
Asien-Pazifik (Seoul)	<code>ap-northeast-2</code>
Asien-Pazifik (Singapur)	<code>ap-southeast-1</code>
Asien-Pazifik (Sydney)	<code>ap-southeast-2</code>
Asien-Pazifik (Tokio)	<code>ap-northeast-1</code>
Kanada (Zentral)	<code>ca-central-1</code>
EU (Frankfurt)	<code>eu-central-1</code>
EU (Irland)	<code>eu-west-1</code>

EU (London)	eu-west-2
Südamerika (São Paulo)	sa-east-1
GovCloud	us-gov-west-1
China (Peking)	cn-north-1

Hinzufügen einer AWS-Standarddatenquelle

So fügen Sie eine AWS-Datenquelle hinzu:

Voraussetzungen

- Konfigurieren Sie die Organisations-Firewall für den AWS-API-Zugriff. Siehe [Konfigurieren der Firewall für den AWS-API-Zugriff](#).
- Erstellen Sie eine Standardkontorichtlinie für das AWS-Konto, das Sie in vRealize Network Insight hinzufügen möchten. Informationen zum Erstellen einer Richtlinie finden Sie unter [Erstellen einer Standard-Kontorichtlinie](#).
- Erstellen Sie einen Benutzer im AWS-Standardkonto. Informationen zum Erstellen eines Benutzers in AWS finden Sie unter [Erstellen eines Benutzers im primären AWS-Konto](#).

Verfahren

- 1 Navigieren Sie zu **Einstellungen > Konten und Datenquellen > Quelle hinzufügen**.
- 2 Klicken Sie unter **Public Clouds** auf **Amazon Web Services**.
- 3 Wählen Sie die Collector (Proxy)-VM aus.
- 4 Geben Sie Ihre Amazon-Zugriffsschlüssel-ID und den zugehörigen geheimen Zugriffsschlüssel ein.

Hinweis Ihre Amazon-Zugriffsschlüssel-ID ist eine 20-stellige Zeichenfolge mit einem entsprechenden geheimen Zugriffsschlüssel. Nähere Informationen finden Sie unter <http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html>.

Hinweis Um die AWS Gov Cloud Region als Datenquelle hinzuzufügen, erstellen Sie einen AWS-IAM-Benutzer unter Verwendung der empfohlenen Richtlinie im AWS-Konto mit Zugriff auf die Gov-Cloud-Region. Verwenden Sie den Zugriffsschlüssel und den geheimen Schlüssel für das neu erstellte Konto, um die Datenquelle zu vRealize Network Insight hinzuzufügen.

Dieser Vorgang zum Hinzufügen und Anzeigen Ihrer Kontodaten kann 15 bis 20 Minuten in Anspruch nehmen.

5 Klicken Sie auf **Validieren**.

Wenn die Anzahl der ermittelten VMs die Kapazität der Plattform oder eines Proxy-Knotens oder von beidem überschreitet, schlägt die Validierung fehl. Sie können erst dann eine Datenquelle hinzufügen, wenn Sie die Brick-Größe der Plattform erhöhen oder ein Cluster erstellen.

Die angegebene Kapazität für jede Brick-Größe mit und ohne Flows lautet wie folgt:

Brick-Größe	VMs	Status der Flows
Groß	6k	Aktiviert
Groß	10k	Deaktiviert
Mittel	3k	Aktiviert
Mittel	6k	Deaktiviert

6 Nachdem Sie Ihr AWS-Konto validiert haben, können Sie **Flows-Datenerfassung aktivieren** auswählen, um tiefere Einblicke zu erhalten.

Erstellen eines Benutzers im primären AWS-Konto

Sie müssen einen Benutzer im AWS-Konto erstellen, um die Amazon-Zugriffsschlüssel-ID und den entsprechenden geheimen Zugriffsschlüssel zu erhalten, die Sie während der Hinzufügung von Datenquellen in vRealize Network Insight verwenden.

Verfahren

- 1 Melden Sie sich bei der AWS-Konsole an.
- 2 Klicken Sie auf **Dienste > IAM > Benutzer > Benutzer hinzufügen**.
- 3 Geben Sie auf der Seite **Benutzer hinzufügen** einen **Benutzernamen** ein, aktivieren Sie das Kontrollkästchen **Programmgesteuerter Zugriff** und klicken Sie auf **Nächste Berechtigung**.
- 4 Klicken Sie unter der Gruppe **Berechtigung festlegen** auf **Vorhandene Richtlinien direkt angehängt**, suchen Sie eine Kontorichtlinie, die Sie zuvor erstellt haben, und wählen Sie sie aus.
 - Wählen Sie für ein primäres AWS-Konto die Richtlinie für primäre Konten aus.
 - Wählen Sie für ein AWS-Standardkonto die Richtlinie für Standardkonten aus.
- 5 Klicken Sie auf **Next-Tags > Next:Review**.
- 6 Klicken Sie auf **Benutzer erstellen**.
- 7 Notieren Sie die **Zugriffsschlüssel-ID** und den **geheimen Zugriffsschlüssel**.

Nächste Schritte

- [Hinzufügen eines primären AWS-Kontos](#).

- [Hinzufügen einer AWS-Standarddatenquelle.](#)

Erstellen einer Standard-Kontorichtlinie

Für die AWS-Standardkonten müssen Sie eine Standard-Kontorichtlinie erstellen. Mit dieser Richtlinie können Sie den Zugriff in AWS verwalten.

Sie können die AWS-Richtlinie an eine IAM-Identität anhängen, z. B. Benutzer oder Rollen. Weitere Informationen finden Sie unter [Richtlinien und Berechtigungen](#).

Verfahren

- 1 Klicken Sie in der AWS-Konsole auf **IAM > Richtlinien > Richtlinie erstellen**.
- 2 Klicken Sie auf der Seite **Richtlinie erstellen** auf die Registerkarte **JSON**.
- 3 Geben Sie im Textfeld **JSON** die folgende Kontorichtlinie ein:

Option	Bezeichnung
<p>So fügen Sie eine Standard-Kontorichtlinie hinzu</p> <hr/> <p>Hinweis Sie müssen die Standard-Kontorichtlinie im AWS-Standardkonto hinzufügen, das Sie als Datenquelle hinzufügen möchten.</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": "*" }] }</pre>

- 4 Klicken Sie auf **Richtlinie überprüfen**.
- 5 Geben Sie unter dem Abschnitt **Richtlinie überprüfen** einen Namen für die Richtlinie ein und klicken Sie auf **Richtlinie erstellen**.

Nächste Schritte

- [Erstellen eines Benutzers im primären AWS-Konto.](#)

AWS: Unterstützung für Geo-Blockierung

Da die Geo-Blockierungsrichtlinie streng auf die Unternehmensfirewall angewendet wird, sind die AWS-API-Aufrufe auf bestimmte AWS-Regionen beschränkt. vRealize Network Insight unterstützt die Geo-Blockierungsrichtlinie für AWS-Umgebungen.

So aktivieren Sie die Geo-Blockierungsrichtlinie in vRealize Network Insight:

Verfahren

- 1 Geben Sie auf der Seite **AWS-Datenquelle hinzufügen** den AWS-Zugriff und die geheimen Schlüssel ein. Klicken Sie auf **Validieren**.
- 2 Wählen Sie **Zugriff nur für bestimmte AWS-Regionen erlauben**. Wählen Sie die **AWS-Regionen** aus der Liste aus, um die automatische Erfassung aus den Regionen zu aktivieren. Wenn diese Option nicht ausgewählt ist, wird die automatische Erfassung nicht durchgeführt.
- 3 Klicken Sie auf **Absenden**.

Hinzufügen eines Azure-Abonnements

Sie können ein Microsoft Azure-Abonnement als Datenquelle in vRealize Network Insight hinzufügen.

Sie müssen über die folgende Berechtigung verfügen:

- `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`

Alternativ können Sie für mehr Benutzerfreundlichkeit die Dienstrolche **Speicherkonto-Schlüsseloperator**, die Rolle **Network Contributor** und die Berechtigung **Reader** hinzufügen.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter der Gruppe **Public Clouds** auf **Microsoft Azure**.
- 4 Geben Sie auf der Seite **Neues Azure-Abonnement hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
Mandanten-ID	Geben Sie die Mandanten-ID von Azure Active Directory (AD) ein.
Anwendungs-ID	Geben Sie die Anwendungs-ID ein.
Geheimer Schlüssel der Anwendung	Geben Sie den geheimen Schlüssel der Anwendung ein.
Abonnement-ID	Geben Sie die Abonnement-ID ein.

- 5 Klicken Sie auf **Validieren**.
Für eine erfolgreiche Validierung müssen Sie über mindestens eine VM, eine Netzwerksicherheitsgruppe (NSG), eine Netzwerkkarte (NIC) und ein VNet verfügen.
- 6 (Optional) Wenn Sie die NSG-Flow-Protokolle erfassen möchten, um Details zu Flows zu erhalten, aktivieren Sie das Kontrollkästchen **NSG-Flow-Datenerfassung aktivieren**.
- 7 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 8 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 9 Klicken Sie auf **Absenden**.

Aktivieren des NSG-Flow-Protokolls

Um die NSG-Flow-Datenerfassung in vRealize Network Insight zu aktivieren, müssen Sie das NSG-Flow-Protokoll in Ihrer Azure-Umgebung aktivieren.

Der Vorgang und die Aufgabe im Zusammenhang mit Azure sind unter <https://docs.microsoft.com/en-us/azure/network-watcher/> dokumentiert.

Voraussetzungen

Vergewissern Sie sich, dass Sie über die korrekte Berechtigung verfügen. Informationen zu Berechtigungen finden Sie unter [Unterstützte Produkte und Versionen](#).

Verfahren

- 1 Aktivieren Sie Network Watcher in ihrer Azure-Umgebung. Weitere Informationen finden Sie in den Lernprogrammen zum Protokollieren von VM-Netzwerkdatenverkehr in der *Network Watcher-Dokumentation* von Azure.
- 2 Registrieren Sie Insights Provider in Ihrer Azure-Umgebung. Weitere Informationen finden Sie in den Lernprogrammen zum Protokollieren von VM-Netzwerkdatenverkehr in der *Network Watcher-Dokumentation* von Azure.
- 3 Aktivieren Sie das NSG-Flow-Protokoll in ihrer Azure-Umgebung. Weitere Informationen finden Sie in den Lernprogrammen zum Protokollieren von VM-Netzwerkdatenverkehr in der *Network Watcher-Dokumentation* von Azure.
- 4 Klicken Sie im **Microsoft Azure**-Portal auf **Speicherkonto > Blob**.
- 5 Wählen Sie den Container aus, in dem Sie die Flow-Protokolle speichern, klicken Sie dann auf **Zugriffsebene ändern** und wählen Sie **Container (anonymer Lesezugriff für Container und Blobs)** aus.

Sie müssen diesen Schritt für alle Container durchführen, in denen Sie die Flow-Protokolle speichern.

Hinzufügen von VMware PKS

Sie können VMware PKS als Datenquelle hinzufügen und Ihre PKS-Clusterdetails in vRealize Network Insight abrufen.

Voraussetzungen

Sie müssen den entsprechenden NSX-T Manager hinzufügen.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Wählen Sie unter „Container“ **VMware PKS** aus.
- 4 Geben Sie auf der Seite „Datenquelle hinzufügen“ die folgenden Details an:

Feldname	Beschreibung
NSX-T Manager	Wählen Sie den NSX-T Manager aus, der das zugrunde liegende Netzwerk für die VMware PKS-Bereitstellung unterstützt.
Collector-VM (Proxy)	vRealize Network Insight wählt automatisch die entsprechende Collector-VM aus, die dem ausgewählten NSX-T Manager zugeordnet ist. Hinweis Die Collector-VMs, die als NetFlow-Collector hinzugefügt werden, sind in der Liste nicht verfügbar.
API-Hostname (FQDN)	Geben Sie die FQDN-Details des PKS-API-Servers ein.

Feldname	Beschreibung
Benutzername	Geben Sie den PKS-Benutzernamen ein, der Zugriff auf die Cluster hat. Hinweis Der Benutzer muss über <code>pkc.clusters.admin</code> -Rechte verfügen.
Kennwort	Geben Sie das Kennwort ein. Hinweis Derzeit werden Kennwörter mit Sonderzeichen wie <code>&</code> , <code>(,)</code> , <code> </code> , <code><</code> , <code>></code> , <code>`</code> nicht unterstützt.

5 Klicken Sie auf **Validieren**.

Die Meldung `Validierung erfolgreich` wird angezeigt.

6 Geben Sie den Spitznamen für die Datenquelle ein und fügen Sie nach Bedarf Notizen zur Beschreibung hinzu.

7 Klicken Sie auf **Absenden**.

Wenn die Fehlermeldung `Mindestens ein Master-Host des Kubernetes-Clusters ist von der Collector-VM aus nicht erreichbar` angezeigt wird, führen Sie die folgenden Befehle auf der Collector-VM aus:

a `pkc login -a PKC_API_Server - u username -p password -k`

b `pkc clusters`

Stellen Sie sicher, dass der Clusterstatus `Erfolgreich` lautet.

c `pkc cluster Kubernetes_Cluster_Name`

d `telnet Kubernetes_Master_Host Kubernetes_Master_Port`

Stellen Sie sicher, dass der Master-Host eine Verbindung herstellen kann.

e Wiederholen Sie `step c` und `step d` für jeden Kubernetes-Cluster, der in `step b` erkannt wurde.

Hinzufügen von Kubernetes

Sie können Kubernetes als Datenquelle hinzufügen und Ihre Kubernetes-Clusterdetails in vRealize Network Insight abrufen.

Hinweis Der Kubernetes-Cluster und der entsprechende NSX-T Manager müssen derselben Collector-VM hinzugefügt werden.

Voraussetzungen

- Fügen Sie NSX-T Manager in vRealize Network Insight hinzu.
- Stellen Sie sicher, dass über die Collector-VM auf den Kubernetes-API-Server zugegriffen werden kann.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Wählen Sie unter „Container“ **Kubernetes** aus.
- 4 Geben Sie auf der Seite „Datenquelle hinzufügen“ die folgenden Details an:

Feldname	Beschreibung
NSX-T Manager	Wählen Sie den NSX-T Manager aus, der das zugrunde liegende Netzwerk für Kubernetes unterstützt.
Collector-VM (Proxy)	vRealize Network Insight wählt automatisch die entsprechende Collector-VM aus, die dem ausgewählten NSX-T Manager zugeordnet ist. Hinweis Die Collector-VMs, die als NetFlow-Collector hinzugefügt werden, sind in der Liste nicht verfügbar.
Kubeconfig	Klicken Sie auf Durchsuchen und laden Sie die Kubernetes-Konfigurationsdatei mit Kubernetes-Clusterdetails hoch. Weitere Informationen zum Format der Kubeconfig-Konfigurationsdatei finden Sie in der Kubernetes-Dokumentation . Hinweis Der in der Kubeconfig-Datei konfigurierte Benutzer muss über die Rechte Auflisten und Überwachen verfügen.

- 5 Klicken Sie auf **Validieren**.

Die Meldung `Validierung erfolgreich` wird angezeigt.

- 6 Geben Sie den Spitznamen für die Datenquelle ein und fügen Sie nach Bedarf Notizen zur Beschreibung hinzu.
- 7 Klicken Sie auf **Absenden**.

Ergebnisse

vRealize Network Insight kann jetzt die Kubernetes-Clusterdetails abrufen.

Nächste Schritte

Wechseln Sie zum Kubernetes-Dashboard und zeigen Sie die Details an. Siehe [Anzeigen von Kubernetes-Details](#).

Hinzufügen von OpenShift

Sie können OpenShift als Datenquelle hinzufügen und Ihre OpenShift-Details in vRealize Network Insight abrufen.

Hinweis OpenShift und der entsprechende NSX-T Manager müssen derselben Collector-VM hinzugefügt werden.

Voraussetzungen

- Fügen Sie NSX-T Manager in vRealize Network Insight hinzu.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Wählen Sie unter „Container“ **OpenShift** aus.
- 4 Geben Sie auf der Seite „Datenquelle hinzufügen“ die folgenden Details an:

Feldname	Beschreibung
NSX-T Manager	Wählen Sie den NSX-T Manager aus, der das zugrunde liegende Netzwerk für OpenShift unterstützt.
Collector-VM (Proxy)	vRealize Network Insight wählt automatisch die entsprechende Collector-VM aus, die dem ausgewählten NSX-T Manager zugeordnet ist. Hinweis Die Collector-VMs, die als NetFlow-Collector hinzugefügt werden, sind in der Liste nicht verfügbar.
Kubeconfig	Klicken Sie auf Durchsuchen und laden Sie die Kubernetes-Konfigurationsdatei mit Kubernetes-Clusterdetails hoch. Weitere Informationen zum Format der Kubeconfig-Konfigurationsdatei finden Sie in der Kubernetes-Dokumentation . Hinweis Der in der Kubeconfig-Datei konfigurierte Benutzer muss über die Rechte Auflisten und Überwachen verfügen.

- 5 Klicken Sie auf **Validieren**.
Die Meldung `Validierung erfolgreich` wird angezeigt.
- 6 Geben Sie den Spitznamen für die Datenquelle ein und fügen Sie nach Bedarf Notizen zur Beschreibung hinzu.
- 7 Klicken Sie auf **Absenden**.

Ergebnisse

vRealize Network Insight kann jetzt die OpenShift-Details abrufen.

Nächste Schritte

Siehe die Details für weitere Informationen zum [Anzeigen von Kubernetes-Details](#).

Hinzufügen von Palo Alto Networks Panorama

Sie können Palo Alto Networks Panorama als Datenquelle in vRealize Network Insight hinzufügen.

Voraussetzungen

Stellen Sie sicher, dass Sie über eine **Administratorrolle** mit XML-API-Zugriff verfügen. Weitere Informationen finden Sie unter [Palo Alto-Netzwerke](#).

Hinweis vRealize Network Insight ruft derzeit keine lokalen Palo Alto-Netzwerkrichtlinien ab, die direkt in den Geräten definiert sind und in Panorama nicht sichtbar sind.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter **Firewalls** auf **Palo Alto Networks Panorama**.
- 4 Geben Sie auf der Seite **Neues Palo Alto Networks Panorama-Konto** oder **Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Benutzername	Geben Sie einen Benutzernamen ein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.
- 6 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 7 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 8 Klicken Sie auf **Absenden**.

Hinzufügen eines Check Point-Verwaltungsservers

vRealize Network Insight unterstützt Verwaltungsserver des Typs Check Point Security Manager (SmartCenter) und Check Point Multi-Domain Security (MDS).

Voraussetzungen

Stellen Sie sicher, dass Sie über die korrekte Berechtigung verfügen. Informationen zu Berechtigungen finden Sie unter [Check Point-Firewall](#).

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter der Gruppe **Firewall** auf **Check Point-Verwaltungsserver**.

- 4 Geben Sie auf der Seite **Neues Check Point-Verwaltungsserver-Konto oder Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein. Hinweis Wenn Sie den Check Point MDS-Verwaltungsserver hinzufügen, müssen Sie die IP-Adresse des MDS-Servers angeben. Sie können die IP-Adresse eines Domänenverwaltungsservers nicht als einzelne Datenquelle hinzufügen.
Benutzername	Geben Sie einen Benutzernamen ein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.
- 6 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 7 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 8 Klicken Sie auf **Absenden**.

Hinzufügen von Cisco ASA

Sie können Cisco ASA als Datenquelle in vRealize Network Insight hinzufügen.

Voraussetzungen

Sie müssen über Rechte für den Switch im Aktivierungsmodus verfügen. Das Kennwort des Benutzers muss mit dem für den Aktivierungsmodus von Cisco ASA verwendeten identisch sein.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter **Firewall** auf **Cisco ASA**.
- 4 Geben Sie auf der Seite **Neues Cisco ASA-Konto oder Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.

Option	Aktion
Benutzername	Geben Sie einen Benutzernamen ein. Hinweis Der Benutzer sollte über das Aktivierungsmodusrecht verfügen, um die Terminallänge auf 0 festlegen und den Sicherheitskontext wechseln zu können.
Kennwort	Geben Sie das Kennwort ein. Hinweis Stellen Sie sicher, dass Sie dasselbe Kennwort eingeben, das Sie für den Aktivierungsmodus von Cisco ASA verwendet haben.

- 5 (Optional) Um die umfassendere Datenerfassung zu aktivieren, klicken Sie auf das Kontrollkästchen **SNMP verwenden (erforderlich für umfassendere Datenerfassung)**.
- 6 Klicken Sie auf **Validieren**.
- 7 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 8 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 9 Klicken Sie auf **Absenden**.

Hinzufügen von Fortinet FortiManager

In vRealize Network Insight können Sie Fortinet FortiManager als Datenquelle hinzufügen.

Voraussetzungen

Überprüfen Sie Folgendes:

- Sie verwenden FortiManager Version 6.0.1.
- Sie haben mindestens die Rolle **Eingeschränkter Benutzer** mit Zugriff auf alle ADOMs und Richtlinienpakete.
- Sie haben den **rpc-permit read-write**-Zugriff über die Befehlszeilenschnittstelle (CLI) aktiviert.

Um die **rpc**-Berechtigung zu konfigurieren, verwenden Sie den folgenden Befehl in der Befehlszeilenschnittstelle von FortiManager:

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

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen > Quelle hinzufügen**.
- 2 Klicken Sie im Abschnitt **Firewall** auf **Fortinet FortiManager**.

- 3 Geben Sie auf der Seite **Neues Fortinet FortiManager-Konto oder Quelle hinzufügen** die erforderlichen Informationen ein:

Option	Aktion
Collector-VM (Proxy)	Wählen Sie die Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Benutzername	Geben Sie den Benutzernamen ein, den Sie für diese Datenquelle verwenden möchten.
Kennwort	Geben Sie das Kennwort ein.

- 4 Klicken Sie auf **Validieren**.
- 5 Geben Sie im Textfeld **Spitzname** einen neuen Spitznamen für die Datenquelle ein.
- 6 (Optional) Im Textfeld **Notiz** können Sie bei Bedarf eine Notiz hinzufügen.
- 7 Klicken Sie auf **Absenden**.

Hinzufügen von Arista-Switch-SSH

Sie können Arista-Switch-SSH als Datenquelle in vRealize Network Insight hinzufügen.

Voraussetzungen

Stellen Sie sicher, dass Sie über die folgende Berechtigung verfügen:

- Schreibgeschützter Benutzer.
- Schreibgeschützter SNMP-Benutzer.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter **Router und Switches** auf **Arista-Switch-SSH**.
- 4 Geben Sie auf der Seite **Neues Arista-Switch-SSH-Konto oder Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein. Hinweis Sie müssen zum Konfigurieren dieses Switches dieselbe IP bzw. denselben FQDN eingeben, die bzw. den Sie in VMware NSX Manager verwendet haben.
Benutzername	Geben Sie einen Benutzernamen ein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.
- 6 (Optional) Um die umfassendere Datenerfassung zu aktivieren, klicken Sie auf das Kontrollkästchen **SNMP verwenden (erforderlich für umfassendere Datenerfassung)**.
- 7 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 8 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 9 Klicken Sie auf **Absenden**.

Hinzufügen von Dell OS10-Switches

Sie können Dell OS10-Switches als Datenquelle in vRealize Network Insight hinzufügen.

Voraussetzungen

Informationen zu unterstützten Dell-Switches finden Sie unter [Unterstützte Produkte und Versionen](#).

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter der Gruppe **Router und Switches** auf **Dell OS10**.
- 4 Geben Sie auf der Seite **Neues Konto oder neue Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Benutzername	Geben Sie einen Benutzernamen ein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.
Die Meldung `Validierung erfolgreich` wird angezeigt.
- 6 Wählen Sie zum Aktivieren von SNMP oder der Datenerfassung die Option **SNMP verwenden** aus.
- 7 Geben Sie im Textfeld **Spitzname** einen Spitznamen ein.
- 8 Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 9 Klicken Sie auf **Absenden**.

Nächste Schritte

[Aktivieren von Telemetrie auf Dell OS10-Switches](#)

Aktivieren von Telemetrie auf Dell OS10-Switches

Sie können Telemetrie auf Dell OS10-Switches aktivieren, um Pufferstatistiken und Nachverfolgung auf Dell-Switches zu integrieren.

Voraussetzungen

Hinzufügen von Dell OS10-Switches

Wenn Anforderungen vom Switch eingeht, speichert oder puffert der vRealize Network Insight-Collector das Paket auf dem definierten Port.

Wenn die Puffergröße zunimmt, weil die Eingaberate im Vergleich zur Ausgaberate ansteigt, werden die Anforderungen möglicherweise langsamer oder es kommt zu einer Zeitüberschreitung. Dell OS10-Switches verwenden gRPC zur Erfassung dieser Metrikinformationen, die in vRealize Network Insight angezeigt werden können. Auf diese Weise können Sie Probleme bei der Anwendungsleistung diagnostizieren, die möglicherweise aufgrund einer Netzwerküberlastung verursacht wurden, und gleichzeitig proaktiv die Auswirkungen der Überlastung auf die Anwendung und das Netzwerk bereitstellen.

Verfahren

- ◆ Führen Sie die folgenden Befehle auf dem Dell OS10-Switch aus:

```
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
```

Ergebnisse

Der vRealize Network Insight-Collector erfasst die folgenden Telemetrieinformationen von den Dell OS10-Switches.

- 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`

Nächste Schritte

Führen Sie eine der folgenden Abfragen durch:

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

Das entsprechende Ereignis wird ausgelöst. Beispiel: `SwitchPort Buffer Threshold Exceeded` Event.

Sie können auch nach der Metrik Maximale Puffernutzung der Schnittstelle suchen und den Grund für die Verlangsamung der Anforderungen angeben.

Hinzufügen der Serien 6800/7800/8800 von Huawei

vRealize Network Insight unterstützt mehrere Serien der Huawei Cloud Engine.

Voraussetzungen

Der Benutzer muss zumindest über Schreibschutzberechtigungen verfügen.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Wählen Sie unter **Router und Switches** die Option **Serie 6800/7800/8800 von Huawei** aus.
- 4 Geben Sie die folgenden Informationen ein:

Eigenschaften	Beschreibung
Collector-VM (Proxy)	Wählen Sie die Proxy-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Username	Geben Sie den Benutzernamen ein, den Sie für diese Datenquelle verwenden möchten.
Password	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.

- 6 Wenn Sie SNMP für die Datenerfassung aktivieren, wählen Sie **SNMP-Version** aus.
 - a Geben Sie für **2c** die zugehörige Community-Zeichenfolge ein.
 - b Geben Sie für **3** Folgendes ein:
 - Username
 - Context Name
 - Authentication Type
- 7 Geben Sie nach Bedarf **Spitzname** und **Notizen** ein.
- 8 Klicken Sie auf **Absenden**.

Nächste Schritte

Sie können die folgenden Funktionen von vRealize Network Insight mit Huawei-Geräten oder -Routern verwenden.

- VM-zu-VM-Pfad
- VM-Underlay-Topologie
- Huawei-Router oder Switch-Dashboard
- Metriken: Metriken für Switch-Ports und Router-Schnittstellen
- Dashboards
 - Huawei-Router oder -Switch
 - Routerschnittstellen
 - Portkanäle
 - Switch-Ports
 - Routen
- Hochverfügbarkeit: Unterstützt M-LAG (Multi-Chassis Link Aggregation) und VRRP (Virtual Router Redundancy Protocol)
- Suche
 - VRF (Virtual Routing and Forwarding) von Huawei
 - Router-Schnittstelle von Huawei
 - Switch-Port von Huawei
 - Portkanal von Huawei
 - Routen in Huawei
- Huawei NetStream-Datenüberwachung

Hinzufügen von Cisco ACI

Sie können Cisco ACI als Datenquelle hinzufügen. Diese Funktion ist nur für die Benutzer der Enterprise-Lizenz verfügbar.

Voraussetzungen

- Um über HTTPS eine Verbindung zur Rest-API des APIC-Controllers herzustellen, müssen Sie Zugriff auf alle Mandanten haben und über die Berechtigung „Nur Lesen“ verfügen.
- Für SNMP müssen Sie die Berechtigung „Nur Lesen“ haben.
- Stellen Sie sicher, dass Sie über eine lokale Benutzerrolle mit dem folgenden Recht verfügen:
 - Sicherheitsdomäne: Alle
 - Rolle: Admin
 - Zugriff: Lesen

Weitere Informationen zum Erstellen eines lokalen Benutzers in Cisco ACI finden Sie im Abschnitt zu Zugriff, Authentifizierung und Ressourcenerfassung im *Cisco APIC-Sicherheitskonfigurationshandbuch*.

Verfahren

- 1 Klicken Sie auf der Seite **Konten und Datenquelle** unter **Einstellungen** auf **Quelle hinzufügen**.
- 2 Klicken Sie unter **Sonstige** auf **Cisco ACI**.
- 3 Geben Sie auf der Seite **Neues Cisco ACI-Konto oder Quelle hinzufügen** die erforderlichen Informationen ein.

Option	Aktion
Collector-VM (Proxy)	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Benutzername	Geben Sie einen Benutzernamen ein. Hinweis Wenn es sich bei dem Benutzer um einen Domänenbenutzer handelt, müssen Sie dem Benutzernamen apic: voranstellen. Wenn beispielsweise der Benutzername user1 lautet und der Benutzer zur Domäne domain1 gehört, geben Sie den Benutzernamen wie folgt an: apic:domain1\user1 . Beim Domänennamen wird die Groß- und Kleinschreibung berücksichtigt.
Kennwort	Geben Sie das Kennwort ein.

- Wählen Sie die Collector-VM aus.
- Geben Sie die IP-Adresse eines beliebigen APIC-Controllers im Cluster an.

Hinweis Sie müssen die einzelnen Switches nicht im ACI-Fabric hinzufügen.

- Geben Sie die Anmeldedaten an.

- vRealize Network Insight erfasst die Metrikdaten von den einzelnen Switches über SNMP. Um diese Aufgabe zu aktivieren, wählen Sie **SNMP verwenden**.
- 4 Klicken Sie auf **Validieren**.
 - 5 Geben Sie **Spitzname** und **Anmerkungen** (sofern vorhanden) für die Datenquelle ein und klicken Sie auf **Absenden**.

Hinzufügen eines physischen Flow-Collectors für NetFlow und sFlow

Sie können einen physischen Flow-Collector hinzufügen und die Switches so konfigurieren, dass sFlow- und NetFlow-Datensätze im Push-Verfahren an den Collector weitergegeben werden. Die Collector-VM, die für NetFlow oder sFlow verwendet wird, ist ein dedizierter Collector. Sie kann nicht für andere Datenquellen verwendet werden. Wird außerdem eine weitere Datenquelle auf dem Proxy-Server hinzugefügt, ist sie nicht als physischer Flow-Collector für sFlow und NetFlow verfügbar.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter **Flows**, auf **Physischer Flow-Collector (NetFlow, sFlow)**.
sFlows werden nur auf dem physischen Collector akzeptiert.
- 4 Geben Sie **Spitzname** und nach Bedarf **Notizen** ein.
- 5 Klicken Sie auf **Absenden**.

Ergebnisse

Hinweis vRealize Network Insight erfasst die Paketbeispiele für sFlow und kann daher die vollständigen Metriken für die Flows nicht anzeigen.

Nächste Schritte

Konfigurieren Sie die Switches, um die Flows an den physischen Flow-Collector weiterzugeben.

- Definieren Sie das Ziel (Collector-IP-Adresse, die Sie in vRealize Network Insight hinzugefügt haben).
- Legen Sie den Port für den Flow-Collector fest.
- Weisen Sie das Abfrageintervall zu.

Hinweis Die zu konfigurierende Vorgehensweise hängt von dem Switch ab, den Sie konfigurieren möchten. Weitere Informationen dazu finden Sie in der spezifischen Dokumentation zum Switch.

Hinzufügen von vRealize Log Insight

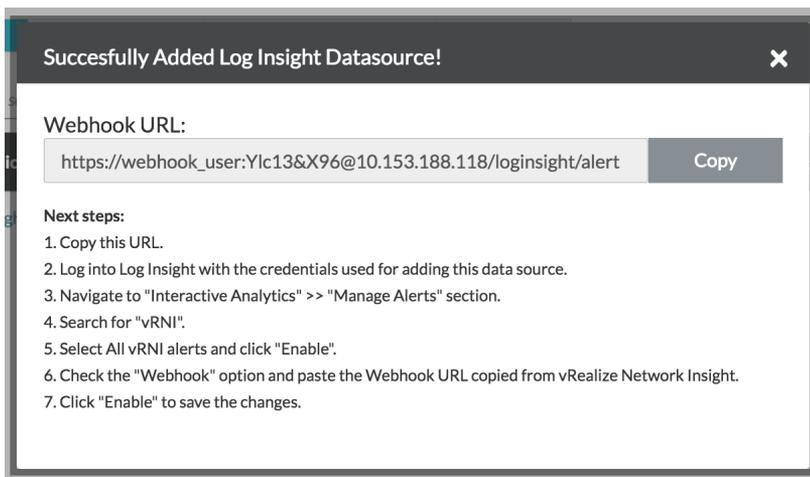
vRealize Log Insight erfasst NSX-Protokolle dynamisch, wenn ein NSX-Ereignis eintritt. vRealize Network Insight erfasst allerdings alle 10 Minuten Daten von NSX. Wenn Sie also vRealize Log Insight in vRealize Network Insight hinzufügen, können Sie Ereignisinformationen schneller abrufen, anstatt darauf zu warten.

In der Integration von vRealize Network Insight und vRealize Log Insight werden die von vRealize Log Insight generierten Warnungen von vRealize Network Insight verbraucht. Wenn eine Sicherheitsgruppe erstellt oder geändert wird, werden die Protokolle von NSX an vRealize Log Insight gesendet, das wiederum eine Warnung sendet. Nach dem Erhalt der Warnung fragt vRealize Network Insight den NSX Manager ab, auf dem die Sicherheitsgruppe erstellt wurde, und ruft die entsprechenden Daten für die geänderten Sicherheitsgruppen ab. Derzeit unterstützt diese Integration nur die CRUD-bezogenen Warnungen der Sicherheitsgruppe.

Eine Liste der unterstützten Versionen von vRealize Log Insight in vRealize Network Insight finden Sie in der [VMware-Produkt-Interoperabilitätmatrix](#).

Verfahren

- 1 Erstellen Sie einen vRealize Log Insight-Benutzer mit Zugriff auf die APIs von vRealize Log Insight oder verwenden Sie einen solchen wieder.
- 2 Klicken Sie auf der Seite **Installation und Unterstützung** auf **Konten und Datenquellen**.
- 3 Klicken Sie auf **Quelle hinzufügen**.
- 4 Klicken Sie auf **Log Insight** unter **Protokollserver**.
- 5 Klicken Sie auf der Seite **Neues Log Insight-Serverkonto oder Quelle hinzufügen** auf **Anweisungen** neben der Seitenüberschrift. Ein Pop-up-Fenster wird angezeigt, das die Voraussetzungen für das Hinzufügen der vRealize Log Insight-Datenquelle und der Anweisungen zum Aktivieren der Webhook-URL auf vRealize Log Insight bereitstellt.

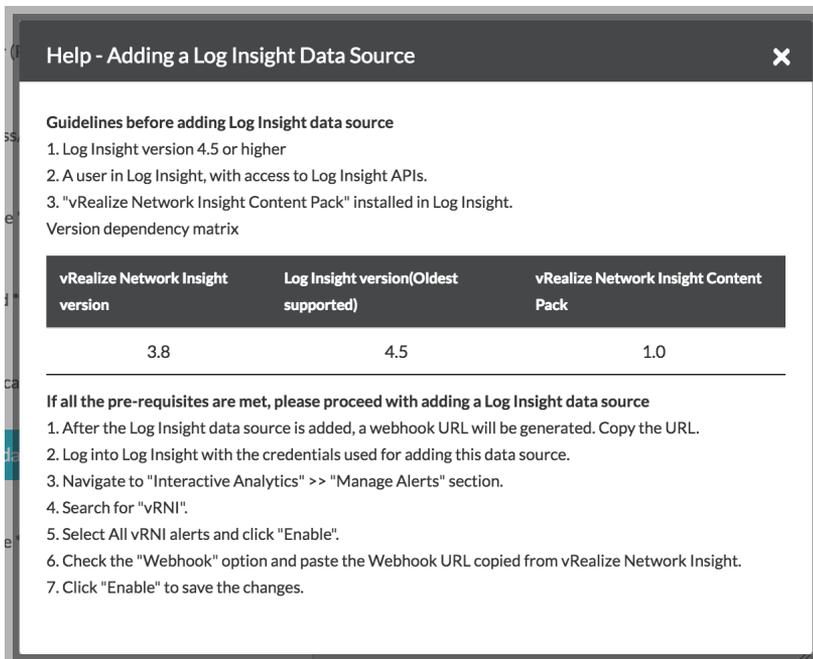


Hinweis Die Webhook-URL, die nach dem Hinzufügen der Datenquelle generiert wird, wird in vRealize Log Insight verwendet.

6 Geben Sie die erforderlichen Details ein.

Name	Beschreibung
Collector-VM (Proxy)	Wählen Sie die IP-Adresse der Datenerfassung aus, die Sie für den Datenerfassungsprozess bereitgestellt haben.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder den FQDN der Datenquelle ein.
Benutzername	Geben Sie den Benutzernamen ein, den Sie für diese bestimmte Datenquelle verwenden möchten.
Kennwort	Geben Sie das Kennwort für die Datenquelle an.
Authentifizierungsanbieter	Wählen Sie den entsprechenden Authentifizierungsanbieter für die von Ihnen bereitgestellten Anmeldedaten aus.

7 Nachdem die Datenquelle erstellt wurde, wird ein Pop-up-Fenster angezeigt, das die Webhook-URL und die Schritte bereitstellt, die ausgeführt werden müssen, um diese URL auf vRealize Log Insight zu aktivieren. Kopieren Sie die Webhook-URL. Melden Sie sich mit den Anmeldedaten an, die zum Hinzufügen dieser Datenquelle verwendet wurden. Aktivieren Sie Warnungen in der vRealize Log Insight-Anwendung und konfigurieren Sie diese Webhook-URL. Senden Sie eine Testwarnung, um sicherzustellen, dass die Integration erfolgreich ist.



Hinweis Jede auf der vRealize Log Insight-Datenquelle in vRealize Network Insight angezeigte Warnung wird innerhalb von einer Stunde gelöst.

Hinzufügen von Infoblox

Mit vRealize Network Insight können Sie Infoblox Grid als DNS-Datenanbieter hinzufügen.

Infoblox-DNS bietet eine erweiterte Lösung für die Verwaltung und Steuerung von DNS. Es verwendet Infoblox Grid, um sicherzustellen, dass das DNS im gesamten Netzwerk hochverfügbar ist. Die DNS-Daten von Infoblox werden nur zur Anreicherung der Flows verwendet, bei denen entweder die Quell- oder die Ziel-IP-Adresse mit den physischen Geräten verknüpft ist.

Die Infoblox-DNS-Daten sind zusammen mit den DNS-Daten vorhanden, die mithilfe von CSV importiert werden.

Wenn Sie eine Infoblox-DNS-Datenquelle auf einem Collector konfigurieren, können Sie auch andere Datenquellen auf demselben Collector konfigurieren. Sie benötigen keinen dedizierten Collector für Infoblox.

Überlegungen

- vRealize Network Insight unterstützt nur den Einzelnetzmodus für Infoblox in der aktuellen Version.
- In der aktuellen Version werden nur A-Datensätze unterstützt. Freigegebene A-Datensätze werden derzeit nicht unterstützt.
- Die DNS-Anreicherung wird nur für die IP-Adressen unterstützt, die in der aktuellen Version als physisch markiert sind.
- Wenn mehrere FQDNs für eine einzelne physische IP-Adresse vorhanden sind, werden alle FQDNs zurückgegeben.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen auf Konten und Datenquellen**.
- 2 Klicken Sie auf **Neue Quelle hinzufügen**.
- 3 Klicken Sie auf **Infoblox** unter **DNS**.
- 4 Geben Sie folgende Informationen ein:

Tabelle 3-5.

Eigenschaften	Beschreibung
Collector VM	Wählen Sie die Collector-VM aus dem Dropdown-Menü aus.
IP Address/FQDN	Geben Sie die IP-Adresse/den FQDN von Infoblox Grid ein.
Username	Geben Sie den Benutzernamen ein, den Sie für diese bestimmte Datenquelle verwenden möchten.
Password	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.

Hinweis Stellen Sie sicher, dass Sie über die `API Privilege` für den Zugriff auf die Infoblox-APIs verfügen.

- 6 Geben Sie **Spitzname** und **Anmerkungen** (falls vorhanden) für die Datenquelle ein und klicken Sie auf **Absenden**, um die Datenquelle des Infoblox-DNS zur Umgebung hinzuzufügen.

Hinzufügen von F5 BIG-IP

vRealize Network Insight unterstützt die Router- und die Lastausgleichsfunktion von F5 BIG-IP. Die Funktionen wie VM-VM-Pfad, Hochverfügbarkeit, VRFs, Weiterleitungen, Router-Schnittstellen, Switch-Ports, Portkanäle, Switch-Port-Metriken, VRF-Dashboard, Switch-Dashboard und Router-Dashboard werden unterstützt. Verwenden Sie für die Suche nach den Einheiten F5 BIG IP die Abfragezeichenfolge `F5 BIG-IP Data Source`. vRealize Network Insight unterstützt keine LLDP-Nachbarn oder benachbarte Geräte im VM-VM-Pfad.

So fügen Sie F5 BIG-IP als Datenquelle hinzu:

Voraussetzungen

- Der Benutzer muss über Folgendes verfügen:
 - Die Rolle `Guest` oder Schreibschutzrechte mit Zugriff auf alle Partitionen.
 - Zugriff auf die REST-API.
 - Zugriff auf das TMSH-Terminal.
- Aktivieren Sie SSH auf dem Gerät.

Aktivieren Sie `password authentication` für SSH wie folgt:

Hinweis

- Verwenden Sie die Berechtigung `root` oder die Administratorrolle, um die SSHD-Konfiguration zu ändern.
- Verwenden Sie beim Hinzufügen der F5-BIG-IP-Datenquelle in vRealize Network Insight nicht die `root`-Benutzerberechtigung.
- Der Root-Benutzer verfügt über keinen HTTP-Zugriff. Die `root`-Benutzerberechtigung wird für den administrativen Zweck verwendet.

```
[root@bigip:Active] config # tmsht
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) (tmsh) # save sys config

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

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Wählen Sie unter **Router und Switches F5 BIG-IP** aus.
- 4 Geben Sie folgende Informationen ein:

Eigenschaften	Beschreibung
Collector-VM (Proxy)	Wählen Sie die Proxy-VM aus dem Dropdown-Menü aus.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Username	Geben Sie den Benutzernamen ein, den Sie für diese Datenquelle verwenden möchten.
Password	Geben Sie das Kennwort ein.

- 5 Nachdem Sie die Informationen in die Textfelder eingegeben haben, klicken Sie auf **Validieren**.
- 6 Wenn Sie SNMP für die Datenerfassung aktivieren, wählen Sie **SNMP-Version** aus.
 - a Wenn Sie 2c auswählen, geben Sie die zugehörige Community-Zeichenfolge ein.
 - b Wenn Sie 3 auswählen, geben Sie Folgendes ein:
 - Username
 - Context Name

- Authentication Type

Hinweis Achten Sie darauf, dass Sie SNMP in der Konsole der F5 BIG-IP-Benutzeroberfläche konfigurieren.

- Melden Sie sich bei F5 an.
- Navigieren Sie zu **System > SNMP**.
- Klicken Sie auf **SNMP > Agent > Zugriff (v1, v2c)**.
- Geben Sie die Community-Zeichenfolge ein.
- Geben Sie die Quell-IP-Adresse ein.
- Wählen Sie den Zugriff **Schreibgeschützt** aus.
- Klicken Sie auf **Fertigstellen**.

7 Geben Sie nach Bedarf **Spitzname** und **Anmerkungen** an. Klicken Sie auf **Absenden**.

Hinzufügen von ServiceNow

Über die ServiceNow-Konfigurationsverwaltungsdatenbank (CMDB) erhalten Sie vollständigen Einblick in die Software- und Hardwareinfrastruktur und die Beziehung zwischen beiden in Ihrem Datacenter. Diese Informationen sind hilfreich bei der Verwaltung Ihrer Bestandsliste. Mit der ServiceNow-Integration kann vRealize Network Insight Anwendungen erkennen, die in ServiceNow CMDB verfügbar sind, damit Sie sie direkt zu vRealize Network Insight hinzufügen können.

Begriffe rund um CMDB

Eine CMDB besteht im Wesentlichen aus:

- **Konfigurationselement:** Eine Einheit oder Komponente in einem System. Beispiel: ein Computer, ein Switch, ein Dienst, eine Anwendung, ein Server oder eine VM.
- **Beziehung:** Ein Link oder eine Art der Kommunikation zwischen Konfigurationselementen. Beispiel: Ist abhängig von, wird aufgeführt auf, tauscht Daten aus.

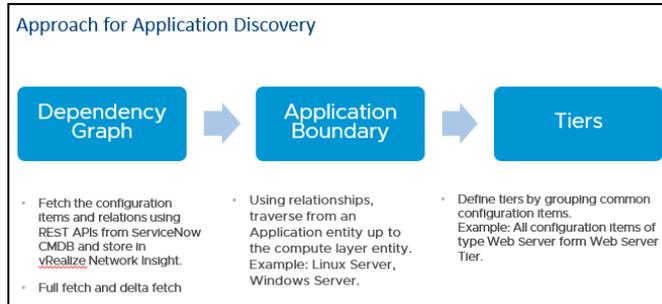
Jedes Konfigurationselement verfügt über ein definiertes Schema.

- **Konfigurationselementklasse:** Jedes Konfigurationselement muss einer Klasse zugeordnet sein, die seine Eigenschaften definiert.
- **Beziehungsklasse:** Definiert die Art der Beziehung zwischen Konfigurationselementen.

Sie können beide Klassen erweitern, um zusätzliche Eigenschaften hinzuzufügen oder die Eigenschaften anzupassen.

ServiceNow unterstützt den Anwendungsdienst, bei dem es sich um eine Gruppe untereinander verbundener Anwendungen und Hosts handelt, die einen Dienst anbieten. Mit ServiceNow können Sie einen Anwendungsdienst mithilfe einer API manuell erstellen oder automatisch durch die Dienstzuordnung ermitteln lassen. Alle diese Anwendungen werden in ServiceNow CMDB gespeichert.

Wenn Sie eine ServiceNow-Datenquelle zu vRealize Network Insight hinzufügen, ruft vRealize Network Insight die Konfigurationselemente und die Beziehungen aus der ServiceNow-CMDB-Konfigurationsdatei ab.



vRealize Network Insight ruft Daten standardmäßig in regelmäßigen Abständen ab.

- Der vollständige Datenabruf erfolgt alle 12 Stunden, wodurch alle Datensätze der Klassen abgerufen werden, die die CMDB-Konfiguration definiert haben. Darüber hinaus erfolgt der vollständige Datenabruf, wenn Sie die Datenquelle hinzufügen oder aktualisieren.
- Der Delta-Abruf erfolgt alle 2 Minuten. Dabei werden alle neuen, geänderten und gelöschten Datensätze der in der CMDB-Konfiguration definierten Klassen abgerufen. Es dauert etwa 12 Minuten, bis diese Details in der Benutzeroberfläche von vRealize Network Insight zu sehen sind.

Hinweis vRealize Network Insight ruft die Klassenhierarchie und die Beziehungstypen nur beim vollständigen Abruf ab.

Standardwerte für Einschränkungen

Grenzwertname	Beschreibung	Standardwert	Auswirkungen für das Überschreiten des Grenzwerts
maxAppsPerDataSource	Maximale Anzahl von Anwendungen pro Datenquelle.	500	Die Datenquelle beendet das Abrufen von Daten mit einem Fehler auf der Seite „Datenquelle und Ereignisse“ und die Anwendungen werden nicht aktualisiert.
maxTiersPerApp	Maximale Anzahl von Ebenen, die pro Anwendung gespeichert werden können.	150	Die Anwendungen werden erst aktualisiert, wenn die Anzahl der Ebenen reduziert wird, sodass sie in den Grenzwert passen.
maxMembersPerApp	Maximale Anzahl von Mitgliedern, die pro Anwendung gespeichert werden können.	500	Die Anwendungen werden erst aktualisiert, wenn die Anzahl der Mitglieder reduziert wird, sodass sie in den Grenzwert passen.

Grenzwertname	Beschreibung	Standardwert	Auswirkungen für das Überschreiten des Grenzwerts
maxGraphTraversalStackSize	Maximale Größe des im Diagrammdurchlauf verwendeten Stacks.	10000	Die Anwendung wird nicht erstellt und löst <code>SizeLimitExceededException</code> aus.
maxResponseAppCount	Maximale Anzahl an Apps, die in der API-Antwort zurückgegeben werden können.	5000	Nur die Anzahl der Anwendungen, die in den Grenzwert passen, wird zurückgegeben, und auf der Benutzeroberfläche wird ein Fehler angezeigt.

Hinzufügen von ServiceNow

Sie können ServiceNow als Datenquelle zu vRealize Network Insight hinzufügen und die Anwendungs- und Ebenendetails abrufen.

Voraussetzungen

Zum Hinzufügen einer Datenquelle benötigen Sie Administratorrechte.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Wählen Sie unter „CMDB“ **ServiceNow** aus.
- 4 Geben Sie auf der Seite „Datenquelle hinzufügen“ die folgenden Details an:

Feldname	Beschreibung
Collector-VM (Proxy)	Die Host-URL von ServiceNow
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.
Benutzername	Geben Sie den Benutzernamen ein, den Sie für diese Datenquelle verwenden möchten. Hinweis Der Benutzer, den Sie hinzufügen möchten, muss ein Administrator oder Schreibgeschützter Administrator in ServiceNow sein.
Kennwort	Geben Sie das Kennwort ein.

- 5 Klicken Sie auf **Validieren**.

Die Meldung `Validierung erfolgreich` wird angezeigt.

- 6 Um eine angepasste CMDB-Konfiguration hinzuzufügen,
 - a klicken Sie auf **CMDB-Konfiguration anpassen**.
 - b klicken Sie auf **Download**, um die Standardkonfigurationsdatei herunterzuladen.

- c Aktualisieren Sie die Dateieigenschaften. Weitere Informationen hierzu finden Sie unter [Anpassen der CMDB-Konfiguration](#).
 - d Navigieren Sie auf der Seite „Datenquelle hinzufügen“ zur Auswahl der aktualisierten JSON-Datei.
- 7 Geben Sie den Spitznamen für die Datenquelle ein und fügen Sie gegebenenfalls Notizen zur Beschreibung hinzu.
- 8 Klicken Sie auf **Absenden**.

Nächste Schritte

Nachdem Sie eine ServiceNow-Datenquelle hinzugefügt haben, ermittelt vRealize Network Insight die in der ServiceNow-CMDB verfügbaren Anwendungen, die Sie zu vRealize Network Insight hinzufügen. Weitere Informationen finden Sie unter [Hinzufügen von ermittelten Anwendungen](#).

Standard-CMDB-Konfigurationsdatei

vRealize Network Insight unterstützt ServiceNow-Anpassungen mithilfe der Konfigurationsdatei im JSON-Format.

```
{
  "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",

```

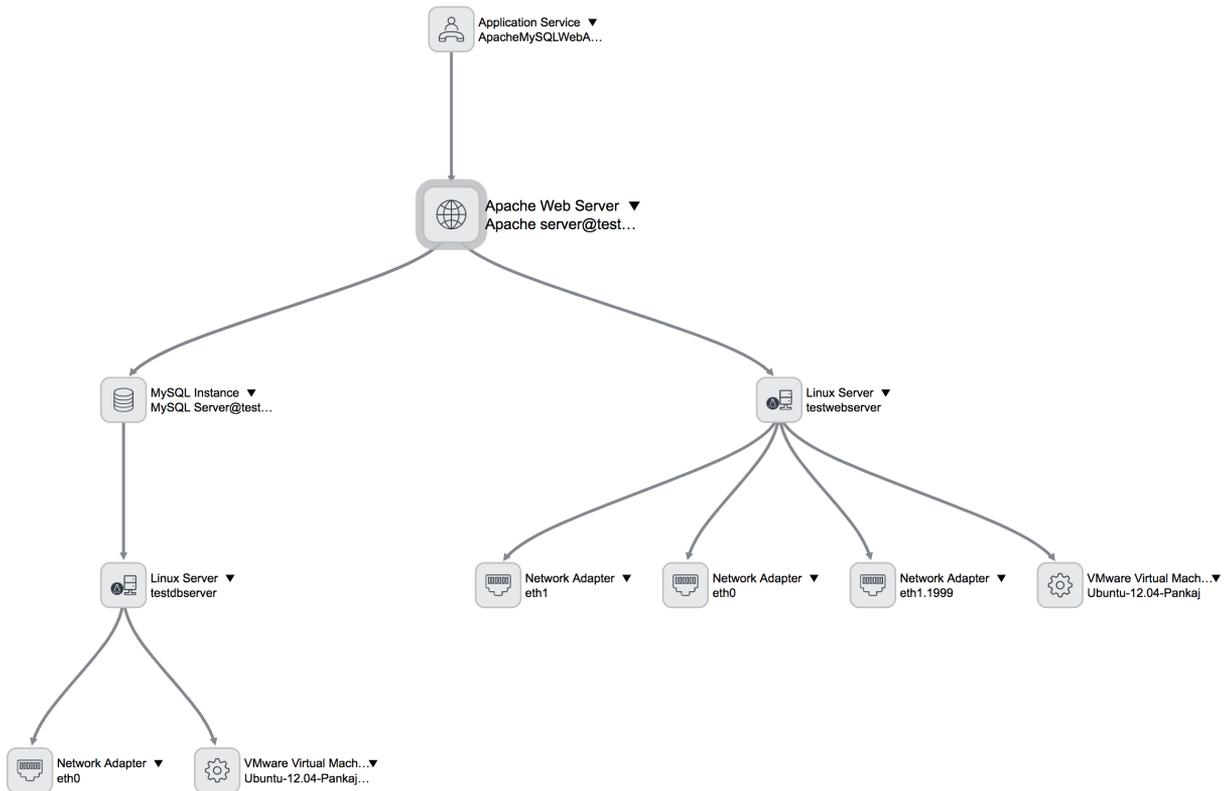
```
    "systemGenerated": true,  
    "expandCIClass": true  
  }  
],  
"traversalRule": [  
  {  
    "fromNode": [  
      "applicationClasses"  
    ],  
    "toNode": [  
      "trackedCIClasses",  
      "workloadCIClasses"  
    ],  
    "relationship": [  
      "relationshipTypeClasses"  
    ],  
    "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": [  
      "trackedCIClasses",  
      "workloadCIClasses"  
    ],  
    "relationship": [  
      "relationshipTypeClasses"  
    ],  
    "priority": 5  
  }  
]
```

```
"workloadCIClasses"  
],  
"relationship": [  
  "workloadRelationshipTypeClasses"  
],  
"priority": 5  
}  
]  
}
```

vRealize Network Insight Wenn die Konfigurationsänderung auftritt, kann es 30 Minuten dauern, bis der vollständige Datenabruf und die Neuberechnung aller Anwendungen abgeschlossen sind.

Beispiel: Beispiel für eine ServiceMap und eine ermittelte Anwendung mit der Standard-CMDB-Konfiguration

Beispiel: Die aktualisierte Seite auf vRealize Network Insight zum Hinzufügen einer Anwendung
Dadurch kann vRealize Network Insight die Anwendungen ServiceNow ermitteln.



Modify Application



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

▼ Tier		Tier Total: 1 VMs 0 Physical IPs
Name *	<u>ApacheMySQLWebApp_apache_web_server</u>	
Virtual Machines / IP Addresses *	VM Names ▼ <u>'Ubuntu-12.04-Pankaj'</u>	1 Vms
Add another Condition		
▼ Tier		Tier Total: 1 VMs 0 Physical IPs
Name *	<u>ApacheMySQLWebApp_db_mysql_instance</u>	
Virtual Machines / IP Addresses *	VM Names ▼ <u>'Ubuntu-12.04-Dark--Pankaj-1'</u>	1 Vms
Add another Condition		

[Add Tier](#) Analyze Flows[Save](#)[Cancel](#)

Anpassen der CMDB-Konfiguration

Zur Unterstützung verschiedener Anpassungen unterstützt die Integration von ServiceNow und vRealize Network Insight eine generische Konfiguration. Die CMDB-Konfiguration muss im JSON-Format vorliegen.

Die Konfiguration umfasst:

- Die Konfigurationselemente
- Die Beziehung zwischen den Konfigurationselementen
- Die Regeln für den Abhängigkeitsdiagramm-Durchlauf.

Sie können die CMDB-Konfiguration basierend auf Ihren Implementierungen anpassen.

Hinweis Wenn Sie die Konfiguration ändern, erfolgt ein vollständiger Abruf, und alle Anwendungen werden neu berechnet. Daher kann dieser Vorgang mindestens 30 Minuten dauern, bis er im Dashboard „Ermittelte Anwendung“ angezeigt wird.

Feldname	Beschreibung
fetchOnlyApprovedApplications	Lässt zu, dass der boolesche Wert nur genehmigte Anwendungen von ServiceNow abrufen. Dieser Wert ist standardmäßig auf False festgelegt.
nameBasedSearchForVm	<p>Lässt zu, dass der boolesche Wert angibt, ob ein benutzerdefiniertes VM-Suchkriterium mit dem VM-Namen erstellt wird, wenn die ServiceNow-VM in vRealize Network Insight nicht vorhanden ist. Wenn der Wert auf True festgelegt ist, wird ein benutzerdefiniertes VM-Namenskriterium erstellt und die Anzahl wird ohne Neuberechnung der Anwendung wiedergegeben, wenn die entsprechende VM in vRealize Network Insight erkannt wird.</p> <p>Dies kann verwendet werden, wenn Sie die Abhängigkeitsdiagramme oder die Dienstzuordnung manuell ohne Verwenden der Dienstzuordnung erstellen. Dieser Wert ist standardmäßig auf False festgelegt.</p>
ignoreWorkloadCheck	<p>Lässt zu, dass ein boolescher Wert angibt, ob eine Einheit zu der Ebene hinzugefügt wird, selbst wenn keine zugeordnete Arbeitslasteinheit vorhanden ist.</p> <p>Dies kann verwendet werden, wenn Sie die Abhängigkeitsdiagramme oder die Dienstzuordnung manuell ohne Verwendung der Dienstzuordnung erstellen und wenn die Beziehungen erst in der Arbeitslastschicht definiert werden. Dieser Wert ist standardmäßig auf False festgelegt.</p>
ciGroup	<p>Definiert Konfigurationselemente und Beziehungen, die von ServiceNow abgerufen werden sollen. Dieses Feld ermöglicht die folgenden Eigenschaften:</p> <ul style="list-style-type: none"> ■ Name: Name für die Konfigurationselementgruppe. ■ Value: Liste der ServiceNow-Klassennamen, die Teil dieser Gruppe sind. ■ ValueType: Lässt CI_CLASS (den abzurufenden Klassennamen) und CI_VALUE zu. <ul style="list-style-type: none"> ■ CI_CLASS: Zum Abrufen der Klasse. ■ CI_VALUE <p>Hinweis vRealize Network Insight ruft immer <code>applicationClasses</code>, <code>workloadCIClasses</code>, <code>trackedCIClasses</code>, <code>workloadCIClasses</code> und <code>relationClasses</code> ab.</p> ■ systemGenerated: Lässt zu, dass der boolesche Wert angibt, ob es sich bei der Klasse um eine benutzerdefinierte Klasse oder um eine Standardklasse handelt. ■ expandCIClass: Lässt zu, dass das boolesche Feld angibt, ob die Unterklassen der Konfigurationselementklasse, die in <code>Value</code> aufgelistet sind, abgerufen werden sollen.

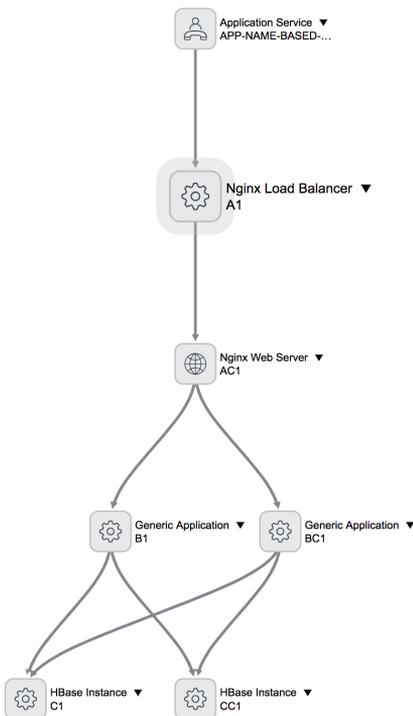
Feldname	Beschreibung
Rules for graph traversal	<p>Unterstützt drei Arten von Durchlaufregeln:</p> <ul style="list-style-type: none"> ■ <code>traversalRule</code>: Alle zulässigen oder gültigen Durchläufe. ■ <code>traversalStopRule</code>: Nicht zulässige Durchläufe. <p>Hinweis Die Regeln in <code>traversalStopRule</code> haben eine höhere Priorität als die Regeln in <code>traversalRule</code>.</p> <ul style="list-style-type: none"> ■ <code>associationRule</code>: Durchläufe, die für die der Einheit zugeordnete Arbeitslast zulässig sind. <p>Eigenschaften einer Regel:</p> <ul style="list-style-type: none"> ■ <code>fromNode</code>: Liste von <code>ciGroup</code>, die die Quelle für den Durchlauf sind. ■ <code>toNode</code>: Liste von <code>ciGroup</code>, die das Ziel für den Durchlauf sind. ■ <code>relationship</code>: Liste von <code>ciGroup</code>, die eine Beziehung in einer Art von Durchlauf aufweisen. ■ <code>priority</code>: Wenn eine <code>ciGroup</code> mit zwei Regeln übereinstimmt, wird die Regel für die <code>ciGroup</code> auf der Basis der <code>priority</code> festgelegt. Je höher die Prioritätszahl, desto höher der Prioritätswert.
applicationClasses	<p>Listet alle Einstiegspunkt-Konfigurationselementklassen für den Diagrammdurchlauf auf. Diese Klassen stellen die Konfigurationselementtypen dar, die als Anwendungsklassen in der CMDB verwendet werden.</p> <p>Die Standardkonfiguration verwendet die <code>cmdb_ci_service_discovered</code>-Klasse. Diese Klasse stellt Anwendungen dar, die von der <code>ServiceMapping</code>-Funktion von ServiceNow erstellt wurden.</p>
workloadCIClasses	<p>Listet alle Konfigurationselemente auf, die entweder einen softwarebasierten Dienst oder ein Betriebssystem wie Linux Server oder Windows Server hosten. Beispiel: VMs, AWS-Instanzen, physische Server.</p> <p>In der Regel werden Arbeitslast-Konfigurationselemente am Ende des Abhängigkeitsdiagramms platziert. Für die in dieser Gruppe genannten Konfigurationselementklassen werden keine Ebenen erstellt.</p> <p>Die Standardkonfiguration enthält die folgenden Konfigurationselementklassen:</p> <ul style="list-style-type: none"> ■ <code>cmdb_ci_computer</code>: stellt alle Computing-bezogenen Konfigurationselemente dar. Dies ist eine Superklasse für alle Linux- und Windows-Server. ■ <code>cmdb_ci_vm_instance</code>: stellt virtuelle Computing-Einheiten wie VMs und AWS-Instanzen dar. ■ <code>cmdb_ci_vmware_instance</code>: stellt VMware-VMs dar.
trackedCIClasses	<p>Listet alle Konfigurationselemente auf, die Teil der Abhängigkeitsdiagramme sein können, aber nicht unter die Klassen <code>applicationClass</code> oder <code>workloadCIClass</code> fallen. Die Konfigurationselemente in dieser Gruppe müssen für das Diagramm von <code>applicationClasses</code> bis <code>workloadCIClasses</code> vervollständigt werden.</p> <p>vRealize Network Insight erstellt Ebenen für alle in <code>trackedCIClasses</code> genannten Klassen, es sei denn, die Klasse wird unter <code>ignoredTierCiClasses</code> genannt.</p>
relationshipTypeClasses	<p>Listet alle verwandten Konfigurationselemente auf, die von Relations-Konfigurationselementklassen oder Relationstypen dargestellt werden.</p> <p>Die Standardkonfiguration verwendet * zum Abrufen aller Relationstypen.</p>

Feldname	Beschreibung
workloadRelationshipTypeClasses:	<p>Listet Relationstypen auf, die in der Regel die Relationen zu Arbeitslasteinheiten darstellen. Im Folgenden finden Sie die Relationen, die standardmäßig in ServiceNow unterstützt werden:</p> <ul style="list-style-type: none"> ■ Hosted on::Hosts ■ Instantiates::Instantiated by ■ Runs on::Runs ■ Virtualized by::Virtualizes
ignoredCiClasses	<p>Listet alle Konfigurationselemente auf, die von vRealize Network Insight ignoriert werden müssen, um von ServiceNow CMDB abgerufen zu werden.</p> <p>Dies ist nützlich beim Abrufen einer Superklasse, damit die unnötigen Unterklassen ignoriert werden.</p> <p>Standardmäßig ist <code>cmdb_ci_vcenter_server_obj</code> unter <code>ignoredCiClasses</code> aufgeführt, da vCenter Server für die Anwendungsermittlung nicht erforderlich ist.</p>
ignoredTierCiClasses	<p>Listet alle Konfigurationselemente auf, für die keine Ebenen erstellt werden dürfen.</p>

Beispiel für das Ermitteln von Anwendungen ohne Arbeitslastrelationen

In einer angepassten CMDB-Konfigurationsdatei ist `nameBasedSearchForVm` für das Ermitteln von Anwendungen definiert, wobei die `cmdb_ci_service_discovered`-Klasse der Einstiegspunkt ist und die Arbeitslastrelationen nicht definiert sind.

Topologie



Angepasste CMDB-Konfigurationsdatei

```
{
  "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
  },
  {

```

```

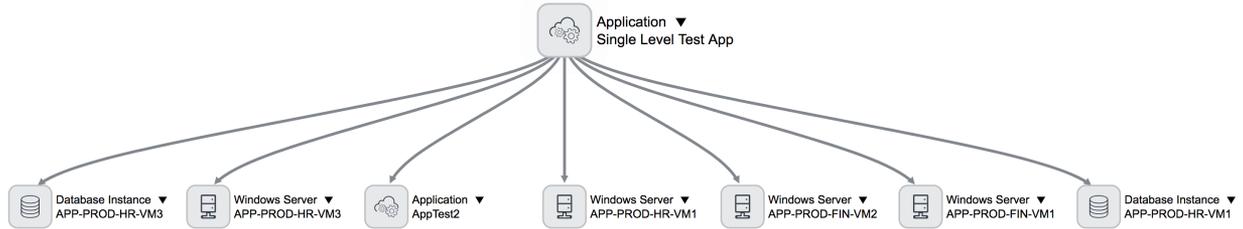
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 3
  }
],
"traversalStopRule": [
  {
    "fromNode": [
      "trackedCIClasses",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

```

Ein Beispiel für die Ermittlung von Anwendungen auf einer Ebene

In einer angepassten CMDB-Konfigurationsdatei ist `nameBasedSearchForVm` für die Ermittlung von Anwendungen auf einer Ebene definiert, wobei die `cmdb_ci_service_discovered`-Klasse der Einstiegspunkt ist und die Arbeitslastrelationen nicht definiert sind.

Topologie



Angepasste CMDB-Konfigurationsdatei

```

{
  "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
  }
]
}

```

Hinzufügen eines neuen generischen Routers oder Switches

Wenn der Router oder Switch, den Sie hinzufügen möchten, in vRealize Network Insight nicht unterstützt wird, können Sie diesen nicht unterstützten Router oder Switch als generischen Router oder Switch hinzufügen, indem Sie eine Gerätekonfigurationsdatei hochladen. vRealize Network Insight liefert anhand der Informationen in der Gerätekonfigurationsdatei Erkenntnisse für den Router bzw. Switch. Nachdem Sie eine Gerätekonfigurationsdatei in vRealize Network Insight hochgeladen haben, können Sie die Informationen der hochgeladenen Gerätekonfigurationsdatei nicht ändern.

Voraussetzungen

Erstellen Sie eine Gerätekonfigurationsdatei im `.zip`-Format und verwenden Sie dazu das von vRealize Network Insight bereitgestellte SDK. Eine Gerätekonfigurationsdatei enthält Informationen zu Einheiten wie Router-Schnittstellen, Routen, Switch-Ports, VRFs, Switch-Geräteinformationen usw. Informationen zum Erstellen einer Gerätekonfigurationsdatei finden Sie unter <https://github.com/vmware/network-insight-sdk-generic-datasources>.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf **Quelle hinzufügen**.
- 3 Klicken Sie unter „Router und Switches“ auf **Generische Router und Switches**.
- 4 Ändern Sie auf der Seite **Neuen generischen Router/Switch hinzufügen** die erforderlichen Informationen.

Option	Aktion
Collector-VM	Wählen Sie eine Collector-VM aus dem Dropdown-Menü aus.
Gerätekonfigurationsdatei	Wählen Sie die Konfigurationsdatei (<code>.zip</code>) aus, die mithilfe des SDK erstellt wurde, und laden Sie sie hoch.
IP-Adresse/FQDN	Geben Sie die IP-Adresse oder die FQDN-Details ein.

- 5 Klicken Sie auf **Validieren**.
- 6 Geben Sie im Textfeld **Spitzname** einen Spitznamen für den Switch oder Router ein, den Sie hinzufügen möchten.
- 7 (Optional) Im Textfeld **Notizen** können Sie bei Bedarf eine Notiz hinzufügen.
- 8 Klicken Sie auf **Absenden**.

Bearbeiten eines generischen Routers oder Switches

In vRealize Network Insight können Sie die Konfiguration eines vorhandenen generischen Routers oder Switches ändern, indem Sie eine neue Konfigurationsdatei hochladen.

Voraussetzungen

Erstellen Sie eine Gerätekonfigurationsdatei im `.zip`-Format und verwenden Sie dazu das von vRealize Network Insight bereitgestellte SDK. Eine Gerätekonfigurationsdatei enthält Informationen zu Einheiten wie Router-Schnittstellen, Routen, Switch-Ports, VRFs, Switch-Geräteinformationen usw. Informationen zum Erstellen einer Gerätekonfigurationsdatei finden Sie unter <https://github.com/vmware/network-insight-sdk-generic-datasources>.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Konten und Datenquellen**.
- 2 Klicken Sie auf das Symbol **Datenquelle bearbeiten** neben der Datenquelle des generischen Routers oder Switches, die Sie bearbeiten möchten.
- 3 Klicken Sie auf **Datei ersetzen** und laden Sie die neue Gerätekonfigurationsdatei hoch.
- 4 (Optional) Um die hochgeladene Gerätekonfigurationsdatei anzuzeigen, klicken Sie auf **Upload-Verlauf**.

Sie können die letzten fünf hochgeladenen Geräte Konfigurationsdateien anzeigen, herunterladen und löschen.
- 5 Klicken Sie auf **Validieren**.
- 6 (Optional) Ändern Sie im Textfeld **Spitzname** den Spitznamen.
- 7 Klicken Sie auf **Absenden**.

Migrieren von Datenquellen

4

Wenn eine Proxy-VM ausgefallen ist oder gelöscht wurde, können Sie eine neue Proxy-VM hinzufügen und die Datenquelle von der alten Proxy-VM auf die neue Proxy-VM migrieren.

So migrieren Sie eine Datenquelle:

Verfahren

- 1 Klicken Sie auf der Seite **Installation und Unterstützung** unter dem Abschnitt **Collector-VMs (Proxy)** auf das Symbol „Bearbeiten“.

Wenn eine Proxy-VM ausgefallen ist, wird die Fehlermeldung angezeigt, dass die Proxy-VM im selben Abschnitt nicht verfügbar ist.

- 2 Auf der Seite **Collector-VM (Proxy) bearbeiten** können Sie der Proxy-VM einen Spitznamen zuweisen.
- 3 Auf der Seite „Collector (Proxy) bearbeiten“ werden alle dem Proxy hinzugefügten Datenquellen aufgelistet. Um eine Datenquelle zu migrieren, klicken Sie auf **Migrieren** für eine bestimmte Datenquelle.
- 4 Die Seite „Konto oder Quelle bearbeiten“ wird angezeigt. Stellen Sie sicher, dass Sie die folgenden Informationen eingeben:

Tabelle 4-1.

Felder	Beschreibung
Collector-VM (Proxy)	Name der neuen Proxy-VM, zu der die Datenquelle migriert werden muss
IP-Adresse	Vorab ausgefüllte IP-/FQDN-Adresse der Datenquelle
Benutzername	Benutzername für die Datenquelle
Kennwort	Kennwort für die Datenquelle

- 5 Klicken Sie auf **Validieren**. Klicken Sie auf **Absenden**. Die Datenquelle wird dann in der alten Proxy-VM gelöscht und der neuen Proxy-VM hinzugefügt.

- 6 Sobald die Migration erfolgreich war, wird die neue Proxy-VM anhand der Datenquelle in der Spalte **Aktiviert** auf der Seite **Konten und Datenquellen** angezeigt.

Hinweis

- Wenn Sie vCenter auf eine andere Proxy-VM migrieren, müssen Sie sicherstellen, dass Sie die entsprechenden NSX Manager auch auf dieselbe Proxy-VM migrieren.
 - Wenn Sie NSX Manager auf eine andere Proxy-VM migrieren, werden auch die untergeordneten Datenanbieter wie NSX Controller und NSX Edge auf die neue Proxy-VM migriert.
-

Löschen einer Datenquelle aus vRealize Network Insight

5

Wenn Sie keine Daten aus einer Datenquelle anzeigen möchten oder eine Datenquelle nicht verwendet wird, können Sie die Datenquelle aus vRealize Network Insight löschen.

Hinweis Wenn eine Datenquelle in Ihrer Umgebung nicht mehr verfügbar ist, müssen Sie das Datenquellenformular vRealize Network Insight löschen.

Verfahren

- 1 Melden Sie sich bei der Webkonsole von vRealize Network Insight an.
- 2 Klicken Sie auf **Einstellungen > Konten und Datenquellen**.
- 3 Klicken Sie neben der Datenquelle die Sie löschen möchten, auf das Symbol **Datenquelle löschen**.
vRealize Network Insight fordert Sie auf, den Vorgang zu bestätigen.
- 4 Klicken Sie auf **Ja**.

Hinweis Nachdem Sie eine Datenquelle aus dem System entfernt haben, können Sie denselben Datenanbieter frühestens nach zwei Stunden wieder hinzufügen.

Konfigurieren der Einstellungen für vRealize Network Insight

6

Auf der Seite vRealize Network Insight-Einstellungen können Sie diverse Einstellungen für konfigurieren. Auf die Seite **Einstellungen** gelangen Sie mit einem Klick auf **Profil > Einstellungen**.

Dieses Kapitel enthält die folgenden Themen:

- Anzeigen des Systemzustands
- Konfigurieren des Datenaufbewahrungsintervalls
- Konfigurieren von IP-Eigenschaften und Subnetzen
- Konfigurieren von Ereignissen und Benachrichtigungen
- Konfigurieren der Identitäts- und Zugriffsverwaltung
- Konfigurieren von Protokollen
- E-Mail-Server konfigurieren
- Ziel des SNMP-Traps konfigurieren
- Verwalten von Lizenzen
- Konfigurieren des Intervalls für die automatische Aktualisierung
- Konfigurieren der Zeitüberschreitung für Benutzersitzungen
- Hinzufügen eines Google Maps-API-Schlüssels
- Konfigurieren der Validierung von Datenquellenzertifikaten
- Anzeigen von Überwachungsprotokollen
- Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit oder Verlassen des Programms
- Anzeigen des Systemzustands Ihrer Einrichtung
- Aktivieren des Support-Tunnels
- Verwalten der Festplattennutzung
- Anzeigen von Details zu Knoten
- Erstellen eines Support-Pakets
- Grundlegendes zur Kapazität für Collector- und Plattformlasten

Anzeigen des Systemzustands

In vRealize Network Insight können Sie den Systemzustand Ihres Systems anzeigen. Der Zustand Ihres Systems wird durch Prozessverzögerung, Indexer-Verzögerung und Rasternutzung bestimmt. Wenn alle diese Parameter den Status „Grün“ aufweisen, ist der Systemzustand gut. Wenn einer dieser drei Parameter den Status „Rot“ aufweist, ist der Systemzustand schlecht.

Verfahren

- ◆ Klicken Sie auf der Seite **Einstellungen auf Installation und Unterstützung**.

Auf der Seite **Installation und Unterstützung** wird der Abschnitt **Systemzustand** angezeigt.

Hinweis Wenn der Systemzustand mehr als sechs Stunden schlecht ist, müssen Sie sich an den vRealize Network Insight-Support wenden.

Konfigurieren des Datenaufbewahrungsintervalls

In vRealize Network Insight können Sie angeben, wie lange Sie Ihre Daten aufbewahren möchten.

Hinweis vRealize Network Insight unterstützt konfigurierbares Datenmanagement ausschließlich auf einer Enterprise-Lizenz. In der Advanced License Edition ist die Datenaufbewahrung standardmäßig auf 1 Monat eingestellt.

Die Daten sind in folgende Kategorien unterteilt:

Tabelle 6-1.

Kategorie	Minimalwert	Maximalwert
Ereignisse	1 Monat	13 Monate
Einheiten und Konfigurationsdaten	1 Monat	3 Monate
Metriken	1 Monat	13 Monate
Flows	NA	1 Monat
Sonstige Daten	NA	100 GB zusätzlicher Festplattenspeicher

Hinweis Für alle Kategorien ist der Minimalwert der Standardwert.

Für jede Kategorie können verschiedene Richtlinien konfiguriert und gesteuert werden. Sie können die Richtlinie gemäß Ihren Anforderungen konfigurieren.

So konfigurieren Sie Datenmanagement:

- 1 Klicken Sie in der oberen rechten Ecke der Startseite auf  und dann auf **Einstellungen**.
- 2 Klicken Sie im Abschnitt **Einstellungen auf Datenmanagement**.

- 3 Wenn Sie sich zum ersten Mal anmelden, werden auf dieser Seite die Standarddaten angezeigt.
- 4 Klicken Sie auf das Informationssymbol, um weitere Informationen darüber zu erhalten, wie Daten die Festplatte belegen.
- 5 Klicken Sie auf **Richtlinie ändern**, um den Datenaufbewahrungszeitraum für die verschiedenen Datenkategorien zu ändern. Sobald Sie die Änderungen vorgenommen haben, werden die Informationen in der Datenbank aufgezeichnet.
- 6 Klicken Sie auf **Absenden**.

Hinweis Der Aufbewahrungszeitraum für Metriken mit niedriger Auflösung ist länger als für die hochauflösenden Metriken.

Konfigurieren von IP-Eigenschaften und Subnetzen

In vRealize Network Insight können Sie verschiedene IP-Eigenschaften für eine bessere Sicherheitsplanung und -kennung konfigurieren.

Importieren der DNS-Zuordnungsdatei

Um die Informationen für die Flows zwischen physischen Geräten bereitzustellen, können Sie die DNS-Zuordnungsdatei importieren. Die unterstützten Formate für die DNS-Zuordnungsdatei sind das Bind- und das CSV-Dateiformat. Stellen Sie sicher, dass Sie diese Dateien in einer einzelnen ZIP-Datei platziert haben.

Hinweis vRealize Network Insight unterstützt keine kennwortgeschützten ZIP-Dateien.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** auf **IP-Eigenschaften und Subnetze**.
- 2 Klicken Sie auf **Physische IP- und DNS-Zuordnung**.
- 3 Klicken Sie auf **Hochladen und ersetzen**, um Ihre DNS-Zuordnungsdatei hochzuladen. Nachdem Sie die Datei ausgewählt und hochgeladen haben, klicken Sie auf **Validieren**. Die Anzahl der DNS-Datensätze wird nach der Validierung angezeigt.

Der Vorgang **Hochladen und ersetzen** entfernt alle vorhandenen DNS-Zuordnungen und ersetzt diese durch die Zuordnungen, die importiert werden. Die DNS-Zuordnungsdatei besteht aus den folgenden drei Feldern:

- Hostname
- IP-Adresse
- Domänenname

Konfigurieren der Zuordnung zwischen Subnetz und einem VLAN

Sie können eine Zuordnung zwischen Subnetz und einem VLAN definieren.

Sie können diese Zuordnung für Folgendes verwenden:

- Anreicherung der Informationen zu den IP-Einheiten, die von physischen zu physischen Flows erlernt werden, durch Hinzufügen der Quell- und Ziel-Subnetze und der Layer2-Netzwerke, die dem Flow zugeordnet sind.
- Planen der Netzwerktopologie basierend auf dem Subnetz und dem VLAN für physische Adressen.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** auf **IP-Eigenschaften und Subnetze**.
- 2 Klicken Sie auf **Physische IP- und DNS-Zuordnung**.
- 3 Klicken Sie auf der Seite **Einstellungen** unter **IP-Eigenschaften und Subnetze** auf **Physische Subnetze und VLANs**.
Auf dieser Seite werden alle Subnetze und die zugehörigen VLAN-IDs aufgelistet.
- 4 Klicken Sie auf **Hinzufügen**, um das Subnetz und die VLAN-Informationen hinzuzufügen.
- 5 Nach der Definition der Zuordnungsinformationen können Sie nur die VLAN-ID bearbeiten, die dem Subnetz zugeordnet ist. Es ist nicht möglich, das mit der VLAN-ID verknüpfte CIDR-Subnetz zu ändern. Um ein Subnetz zu bearbeiten, das mit der VLAN-ID verknüpft ist, löschen Sie das zu bearbeitende Subnetz und erstellen Sie eine Subnetz-VLAN-Zuordnung mit den erforderlichen Werten.

Wenn die Subnetz-VLAN-Zuordnungsinformationen aktualisiert werden, wird ein neues VLAN für die angegebene VLAN-ID erstellt und die Subnetzinformationen werden mit diesem VLAN verknüpft.

- 6 Um die Subnetz-VLAN-ID-Zuordnung zu löschen, klicken Sie auf das Symbol „Löschen“.

Hinweis Alle Erstellungs-, Aktualisierungs- und Löschvorgänge für VLAN treten nicht unmittelbar nach der Erstellung der Subnetz- und VLAN-Zuordnungen auf. Es dauert einige Zeit, bis die Änderungen übernommen und das entsprechende VLAN erstellt oder geändert wurde.

Konfigurieren von Ost-West-IPs

Die IPs, die sich im Bereich von RFC1918-Standard befinden, gelten als private IPs. Die IPs, die sich außerhalb von RFC1918 befinden, werden als Internet-IPs behandelt. Benutzer können jedoch ihre Ost-West-IPs (öffentliche Datacenter-IPs) angeben, die sie beim Tagging von Flows und Mikrosegmentierung als Nicht-Internet-IPs behandeln möchten, selbst wenn diese außerhalb des privaten IP-Adressbereichs liegen, das von RFC1918 definiert wird.

Angeben öffentlicher IPs, die als Nicht-Internet-IPs behandelt werden sollen

- 1 Klicken Sie in der oberen rechten Ecke der Startseite auf das Symbol „Profil“ und anschließend auf **Einstellungen**.
- 2 Klicken Sie im Abschnitt „Einstellungen“ auf **Ost-West-IPs**.
- 3 Geben Sie im Feld „IP-Adressen“ bestimmte IPs oder IP-Bereiche oder Subnetze ein, die als Nicht-Internet-IPs behandelt werden sollen.
- 4 Klicken Sie auf **Speichern**. Die Bestätigungsmeldung „IP-Adressen gespeichert“ wird nach erfolgreichem Speichern angezeigt.

Konfigurieren von Nord-Süd-IPs

Die IPs, die sich im RFC1918-Speicherplatz befinden, werden als Nord-Süd-IPs kategorisiert. Die Benutzer können ihre Nord-Süd-IPs beim Tagging von Flows und der Mikrosegmentierung angeben.

So geben Sie Nord-Süd-IPs an:

- 1 Klicken Sie in der oberen rechten Ecke der Startseite auf das Symbol Profil  und anschließend auf **Einstellungen**.
- 2 Klicken Sie im Abschnitt „Einstellungen“ auf **Nord-Süd-IPs**.
- 3 Geben Sie im Feld „IP-Adressen“ bestimmte IPs oder IP-Bereiche oder Subnetze ein.
- 4 Klicken Sie auf **Speichern**. Die Bestätigungsmeldung „IP-Adressen gespeichert“ wird nach erfolgreichem Speichern angezeigt.

Konfigurieren von Ereignissen und Benachrichtigungen

In vRealize Network Insight können Sie verschiedene Arten von Ereignissen und Benachrichtigungen konfigurieren. vRealize Network Insight erstellt ein Ereignis, wenn das System eine voreingestellte Regel erfüllt.

Klicken Sie auf der Seite **Einstellungen** auf **Ereignisse**, um die verschiedenen Ereignistypen anzuzeigen:

- **Systemereignisse**
- **Benutzerdefinierte Ereignisse**
- **Plattformzustand: Ereignisse**

Liste „Systemereignisse“

Hier finden Sie eine Liste aller Systemereignisse, die in vRealize Network Insight definiert sind. Um eine Benachrichtigung über diese Systemereignisse zu erhalten, müssen Sie Benachrichtigungen für das betreffende Ereignis aktivieren.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.100001	vmwNSXVLatencyNoDataEvent	Warnung	NSXVLatencyNoDataEvent	Netzwerklatenz-Erfassung angehalten
1.3.6.1.4.1.6876.100.1.0.100051	vmwVMCVMLimitExceededEvent	Kritisch	VMCVMLimitExceededEvent	Die Anzahl der VMs im VMC-SDDC überschreitet den Grenzwert.
1.3.6.1.4.1.6876.100.1.0.100052	vmwVMCHostLimitExceededEvent	Kritisch	VMCHostLimitExceededEvent	Die Anzahl der Hosts im VMC-SDDC überschreitet den Grenzwert.
1.3.6.1.4.1.6876.100.1.0.1510	vmwKubernetesBaseEvent	Moderat	KubernetesBaseEvent	Vom Kubernetes-Cluster gemeldetes Ereignis
1.3.6.1.4.1.6876.100.1.0.20001	vmwEntityDiscoveryChangeEvent	Info	Erkennung	Dieses Ereignis wird ausgelöst, wenn eine neue Einheit erkannt wird.
1.3.6.1.4.1.6876.100.1.0.20002	vmwEntityPropertiesChangeEvent	Info	Konfigurationsänderung	Dieses Ereignis wird ausgelöst, wenn eine Eigenschaft der Einheit geändert wird.
1.3.6.1.4.1.6876.100.1.0.20003	vmwFirewallNotInstalledOnHostEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20004	vmwHostWithStaleFirewallRulesEvent	Warnung	Keine Übereinstimmung der Firewallregeltabelle von Host und NSX Manager	Die Regeltabelle der verteilten Firewall ist für Host und NSX Manager unterschiedlich.
1.3.6.1.4.1.6876.100.1.0.20005	vmwIpAddressChangeEvent	Info	Änderung der IP-Adresse	Dieses Ereignis wird ausgelöst, wenn die IP-Adresse der VM geändert wird.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20006	vmwL2GatewayAnomalyEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20007	vmwL2NetworkAddressAnomalyEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20008	vmwL2NetworkDiameterExceededEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20009	vmwL2NetworkUplinkMissingEvent	Info	Uplink für verteilte virtuelle Portgruppe nicht gefunden	VXLAN hat keinen Uplink auf dem angegebenen Host
1.3.6.1.4.1.6876.100.1.0.20010	vmwL2NetworkWithNoVMsEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20011	vmwLayer2NetworkDiameterChangedEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20012	vmwMTUMismatchEvent	Warnung	Keine MTU-Übereinstimmung bei VTEP und physischem Switch-Port	Im Pfad zwischen einem VTEP und seinem physischen Switch-Port wurde eine MTU-Nichtübereinstimmung gefunden.
1.3.6.1.4.1.6876.100.1.0.20013	vmwNetworkIsolationEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20014	vmwNoPathEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20015	vmwSpoofGuardDisabledEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20018	vmwVMotionEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20019	vmwVMWithDisconnectedVnicEvent	n. z.	n. z.	n. z.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20020	vmwVMWithMultipleVnicsOnDifferentVxlansEvent	n. z.	n. z.	VM %s ist mit mehr als einem VXLAN [% s] verbunden
1.3.6.1.4.1.6876.100.1.0.20021	vmwVMWithMultipleVnicsOnSameL2Event	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20022	vmwVMWithNoIpAddressEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20023	vmwVTEPMissingEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20024	vmwL2Event	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20025	vmwMembershipChangeEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20026	vmwSecurityGroupMembershipChangeEvent	Info	Änderung der VM-Mitgliedschaft der Sicherheitsgruppe	Dieses Ereignis wird ausgelöst, wenn die Mitgliedschaft der Sicherheitsgruppe geändert wird.
1.3.6.1.4.1.6876.100.1.0.20027	vmwFirewallRuleMembershipChangeEvent	Info	Änderung der VM-Mitgliedschaft der Firewallregel	Dieses Ereignis wird ausgelöst, wenn die Mitgliedschaft der Firewallregel geändert wird.
1.3.6.1.4.1.6876.100.1.0.20028	vmwVlanMembershipChangeEvent	Info	VLAN-VM-Mitgliedschaftsänderung	Dieses Ereignis wird ausgelöst, wenn die Mitgliedschaft des VLAN geändert wird.
1.3.6.1.4.1.6876.100.1.0.20029	vmwVxlanMembershipChangeEvent	Info	VXLAN-VM-Mitgliedschaftsänderung	Dieses Ereignis wird ausgelöst, wenn die Mitgliedschaft des VXLAN geändert wird.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20030	vmwDeleteChangeEvent	Info	Änderung löschen	Dieses Ereignis wird ausgelöst, wenn eine Einheit gelöscht wird.
1.3.6.1.4.1.6876.100.1.0.20031	vmwVtepFailedPingEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20034	vmwEmptySearchStreamChangeEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20035	vmwSearchStreamMembershipChangeEvent	n. z.	Benutzerdefiniertes Änderungsereignis	Benutzerdefiniertes Änderungsereignis
1.3.6.1.4.1.6876.100.1.0.20036	vmwEmptySearchStreamProblemEvent	n. z.	Fehler bei benutzerdefiniertem Nullergebnis	Benutzerdefiniertes Problem, wenn das Suchergebnis leer ist
1.3.6.1.4.1.6876.100.1.0.20037	vmwSearchStreamMembershipProblemEvent	n. z.	Benutzerdefiniertes Änderungsproblem	Benutzerdefiniertes Problem bei Änderungen des Suchergebnisses
1.3.6.1.4.1.6876.100.1.0.20038	vmwOspfConfigurationMismatchEvent	Moderrat	Keine Übereinstimmung der OSPF-Bereichs-ID von DLR und Edge-Router	Die OSPF-Bereichs-ID unterscheidet sich von den verbundenen Router-Schnittstellen.
1.3.6.1.4.1.6876.100.1.0.20039	vmwServiceVMNotHealthyEvent	n. z.	n. z.	n. z.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20040	vmwServiceVMNotPoweredOnEvent	Kritisch	NSX-Infrastruktur-VM nicht eingeschaltet	Die NSX-Infrastruktur-VM befindet sich im ausgeschalteten Zustand. Die von ihr bereitgestellten Dienste können beeinträchtigt werden. Die NSX-Infrastruktur umfasst Controller-Cluster.
1.3.6.1.4.1.6876.100.1.0.20041	vmwServiceVMHighCPUUsageEvent	Warnung	Hohe CPU-Auslastung für NSX-Infrastruktur-VM gemeldet	Eine NSX-Infrastruktur-VM weist eine hohe CPU-Auslastung auf. Dieser Zustand kann zu einer Dienstunterbrechung führen.
1.3.6.1.4.1.6876.100.1.0.20042	vmwServiceVMHighMemoryUsageEvent	Warnung	Hohe Arbeitsspeichernutzung für NSX-Infrastruktur-VM gemeldet	Eine Infrastruktur-VM weist einen Zustand mit hohem Speicherbedarf auf. Diese Bedingung kann zur Unterbrechung des NSX-Diensts führen.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20043	vmwServiceVMHighDiskUsageEvent	Warnung	Hohe Festplattennutzung für NSX-Infrastruktur-VM gemeldet	Der Großteil des zugeteilten Festplattenspeichers für eine Infrastruktur-VM wurde verbraucht. Auf die Infrastruktur-VM kann möglicherweise nicht mehr zugegriffen werden, oder es kann eine Dienstunterbrechung eintreten.
1.3.6.1.4.1.6876.100.1.0.20050	vmwIPSetPropertiesChangeEvent	Info	Änderung der IP Set-Eigenschaften	Dieses Ereignis wird ausgelöst, wenn eine Eigenschaft von IPSet geändert wird.
1.3.6.1.4.1.6876.100.1.0.20051	vmwFirewallRulePropertiesChangeEvent	Info	Änderung von Firewallregel-Eigenschaften	Dieses Ereignis wird ausgelöst, wenn eine Eigenschaft der Firewallregel geändert wird.
1.3.6.1.4.1.6876.100.1.0.20052	vmwSecurityGroupPropertiesChangeEvent	Info	Änderung der Eigenschaften der Sicherheitsgruppe	Dieses Ereignis wird ausgelöst, wenn eine Eigenschaft der Sicherheitsgruppe geändert wird.
1.3.6.1.4.1.6876.100.1.0.20053	vmwIPSetMembershipChangeEvent	Info	Änderung der IP Set-Mitgliedschaft	Dieses Ereignis wird ausgelöst, wenn die Mitgliedschaft von IPSet geändert wird.

OID	Ereignisname	Standardshwergrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20054	vmwFirewallRuleMaskEvent	Warnung	Regel für die verteilte Firewall durch vorhergehende Regel verdeckt	Eine Regel der verteilten Firewall wird durch eine oder mehrere vorangehende Regeln maskiert. Dieser Zustand weist möglicherweise auf einen Konfigurationsfehler hin.
1.3.6.1.4.1.6876.100.1.0.20056	vmwSecurityMembershipChangeEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20057	vmwSecurityTagPropertiesChangeEvent	Info	Änderung der Sicherheits-Tag-Eigenschaften	Dieses Ereignis wird ausgelöst, wenn eine Eigenschaft des Sicherheits-Tags geändert wird.
1.3.6.1.4.1.6876.100.1.0.20058	vmwSecurityTagMembershipChangeEvent	Info	Änderung der VM-Mitgliedschaft des Sicherheits-Tags	Dieses Ereignis wird ausgelöst, wenn die Mitgliedschaft des Sicherheits-Tags geändert wird.
1.3.6.1.4.1.6876.100.1.0.20059	vmwHostDatastoreChangeEvent	Info	Datenspeicher des Hosts geändert	Dieses Ereignis wird ausgelöst, wenn der Datenspeicher des Hosts geändert wird.
1.3.6.1.4.1.6876.100.1.0.20060	vmwVMDatastoreChangeEvent	Info	Datenspeicher der VM geändert	Dieses Ereignis wird ausgelöst, wenn der VM-Datenspeicher geändert wird.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20061	vmwVMSnapshotChangeEvent	Info	Snapshots der VM geändert	Dieses Ereignis wird ausgelöst, wenn der Snapshot der VM geändert wird.
1.3.6.1.4.1.6876.100.1.0.20062	vmwVMVirtualDiskChangeEvent	Info	Virtuelle Festplatten der VM geändert	Dieses Ereignis wird ausgelöst, wenn die virtuelle Festplatte der VM geändert wird.
1.3.6.1.4.1.6876.100.1.0.20063	vmwIPSetDefinitionMismatchEvent	Info	Keine Übereinstimmung der IPSet-Definition von NSX Managern	Ein IPSet mit demselben Namen und unterschiedlichen Geltungsbereichen ist in zwei NSX Managern definiert. Dieser Zustand weist möglicherweise auf einen Konfigurationsfehler hin.
1.3.6.1.4.1.6876.100.1.0.20064	vmwSegmentMismatchEvent	Info	Segment-ID-Bereiche von zwei NSX Managern überschneiden sich	Die in unterschiedlichen NSX Managern definierten VXLAN-Segment-ID-Bereiche weisen überlappende Bereiche auf
1.3.6.1.4.1.6876.100.1.0.20065	vmwVtepEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20066	vmwVtepConfigurationFaultEvent	n. z.	n. z.	n. z.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20067	vmwDLRNetworksNotReachableEvent	Kritisch	DLR-Netzwerke sind von NSX Edge oder externem Router aus nicht erreichbar	Ein oder mehrere DLR-Netzwerke können nicht über die Uplink-Schnittstelle auf dem NSX Edge-Router erreicht werden. Diese Bedingung deutet entweder auf einen OSPF-Konfigurationsfehler auf dem Edge-Router/DLR oder auf eine Route hin, die im Uplink-Router nicht konfiguriert ist.
1.3.6.1.4.1.6876.100.1.0.20068	vmwVtepSubnetMismatchEvent	Moderat	Keine Übereinstimmung des VTEP-IP-Subnetzes bei Host(s) und vorbereitetem NSX-Cluster	Mindestens eine IP-Adresse des Host-VTEPs befindet sich nicht im selben Subnetz wie andere VTEPs im selben Cluster. Dieser Zustand kann zu Problemen bei der Netzwerkkonnektivität führen.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20069	vmwVtepCountMismatchEvent	Kritisch	Keine Übereinstimmung der VTEP-Anzahl von Host und Cluster	Die VTEP-Anzahl des Hosts stimmt nicht mit der VTEP-Anzahl anderer Hosts im selben Cluster überein. VMs auf diesem Host, die mit einem logischen Switch verbunden sind, können möglicherweise nicht kommunizieren.
1.3.6.1.4.1.6876.100.1.0.20070	vmwEdgeNetworksNotReachableEvent	Moderat	NSX Edge-Netzwerk vom Uplink-Router aus nicht erreichbar	Mindestens ein Netzwerk, das mit einem NSX Edge-Router verbunden ist, ist von einem Uplink-Router aus nicht erreichbar.
1.3.6.1.4.1.6876.100.1.0.20089	vmwNilInfraChangeEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.20090	vmwDataSourceEnabledChangeEvent	Info	Datenquelle wurde aktiviert.	Dieses Ereignis wird ausgelöst, wenn die Datenquelle aktiviert ist.
1.3.6.1.4.1.6876.100.1.0.20091	vmwDataSourceDisabledChangeEvent	Info	Datenquelle wurde deaktiviert.	Dieses Ereignis wird ausgelöst, wenn die Datenquelle deaktiviert ist.
1.3.6.1.4.1.6876.100.1.0.20092	vmwDataSourceCreatedEvent	Info	Datenquelle wurde hinzugefügt.	Dieses Ereignis wird ausgelöst, wenn eine Datenquelle hinzugefügt wird.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20093	vmwPlatformCpuCoreChangeEvent	Info	Plattform-CPU-Kerne (Änderungsereignis)	Dieses Ereignis wird ausgelöst, wenn die CPU-Kerne auf der Plattform geändert werden.
1.3.6.1.4.1.6876.100.1.0.20094	vmwPlatformDiskChangeEvent	Info	Plattformfestplatte (Änderungsereignis)	Dieses Ereignis wird ausgelöst, wenn die Festplatte auf der Plattform geändert wird.
1.3.6.1.4.1.6876.100.1.0.20095	vmwPlatformMemoryChangeEvent	Info	Plattform-Arbeitsspeicher (Änderungsereignis)	Dieses Ereignis wird ausgelöst, wenn der Arbeitsspeicher auf der Plattform geändert wird.
1.3.6.1.4.1.6876.100.1.0.20096	vmwPlatformRebootedEvent	Info	Plattform neu gestartet (Ereignis)	Dieses Ereignis wird ausgelöst, wenn die Plattform neu gestartet wird.
1.3.6.1.4.1.6876.100.1.0.20097	vmwProxyCpuCoreChangeEvent	Info	Proxy-CPU-Kerne (Änderungsereignis)	Dieses Ereignis wird ausgelöst, wenn CPU-Kerne auf dem Collector geändert werden.
1.3.6.1.4.1.6876.100.1.0.20098	vmwProxyDiskChangeEvent	Info	Proxy-Festplatten-Änderungsereignis	Dieses Ereignis wird ausgelöst, wenn die Festplatte auf dem Collector geändert wird.
1.3.6.1.4.1.6876.100.1.0.20099	vmwProxyMemoryChangeEvent	Info	Proxy-Arbeitsspeicher (Änderungsereignis)	Dieses Ereignis wird ausgelöst, wenn der Speicher auf dem Collector geändert wird.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.20100	vmwProxyRebootedEvent	Info	Proxy neu gestartet (Ereignis)	Dieses Ereignis wird ausgelöst, wenn der Collector neu gestartet wird.
1.3.6.1.4.1.6876.100.1.0.20101	vmwNICClusterChangeEvent	Info	Cluster wurde erweitert	Dieses Ereignis wird ausgelöst, wenn eine Plattform zum System hinzugefügt wird.
1.3.6.1.4.1.6876.100.1.0.20102	vmwNISystemProxyChangeEvent	Info	Proxy wurde hinzugefügt/entfernt	Dieses Ereignis wird ausgelöst, wenn der Proxy hinzugefügt oder entfernt wird.
1.3.6.1.4.1.6876.100.1.0.20103	vmwNICClusterCreateEvent	Info	Cluster wurde erstellt.	Dieses Ereignis wird ausgelöst, wenn ein Cluster erstellt wird.
1.3.6.1.4.1.6876.100.1.0.30001	vmwThresholdExceededEventCpuReady	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30002	vmwThresholdExceededEventCpuCoStop	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30003	vmwThresholdExceededEventDiskCommandAbortRule	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30004	vmwThresholdExceededEventIODEviceLatencyRule	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30005	vmwThresholdExceededEventIOKernelLatencyRule	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30006	vmwThresholdExceededEventMemorySwapInRule	n. z.	n. z.	n. z.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.30007	vmwThresholdExceededEventMemorySwapOutRule	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30008	vmwThresholdExceededEventNetworkRxDropRule	Warnung	Auf der Host-Schnittstelle erkannte Paketverluste empfangen	Auf einer Hostschnittstelle wurde einen Schwellenwert überschreitende Menge an Paketverlusten auf der Empfangsseite erkannt.
1.3.6.1.4.1.6876.100.1.0.30009	vmwThresholdExceededEventNetworkTxDropRule	Warnung	Auf Hostschnittstelle erkannte Paketverluste übertragen	Auf einer Hostschnittstelle wurde einen Schwellenwert überschreitende Menge an Paketverlusten auf der Übermittlungseite erkannt.
1.3.6.1.4.1.6876.100.1.0.30010	vmwAWSRegionSGLimitEvent	Kritisch	Verfügbare AWS-Sicherheitsgruppen mit AWS-Region.	Verfügbare AWS-Sicherheitsgruppen mit AWS-Region.
1.3.6.1.4.1.6876.100.1.0.30011	vmwAWSVPCSGLimitEvent	Kritisch	AWS-Sicherheitsgruppen, die mit AWS VPC verfügbar sind.	AWS-Sicherheitsgruppen, die mit AWS VPC verfügbar sind.
1.3.6.1.4.1.6876.100.1.0.30012	vmwAWSSGInboundRuleLimitEvent	Kritisch	Eingehende Regeln, die mit der AWS-Sicherheitsgruppe verfügbar sind.	Eingehende Regeln, die mit der AWS-Sicherheitsgruppe verfügbar sind.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.30013	vmwAWSSGOutboundRuleLimitEvent	Kritisch	Ausgehende Regeln, die mit der AWS-Sicherheitsgruppe verfügbar sind.	Ausgehende Regeln, die mit der AWS-Sicherheitsgruppe verfügbar sind.
1.3.6.1.4.1.6876.100.1.0.30014	vmwAWSInterfaceSGLimitEvent	Kritisch	Verfügbare AWS-Sicherheitsgruppen mit AWS-Schnittstelle.	Verfügbare AWS-Sicherheitsgruppen mit AWS-Schnittstelle.
1.3.6.1.4.1.6876.100.1.0.30100	vmwPacketDropEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30101	vmwSwitchPortPacketDropEvent	Warnung	Paketverluste auf Switch-Port	Erhebliche Anzahl Paketverluste am angegebenen Switch-Port erkannt
1.3.6.1.4.1.6876.100.1.0.30102	vmwRouterInterfacePacketDropEvent	Warnung	Paketverluste auf NSX Edge Gateway-Schnittstelle	Auf der vNIC-Schnittstelle eines NSX Edge Gateways wurde eine den Schwellenwert überschreitende Menge an Paketverlusten erkannt.
1.3.6.1.4.1.6876.100.1.0.30103	vmwVnicPacketDropEvent	Warnung	Bei VM verloren gegangene Pakete	Auf einer VM-Schnittstelle wurde eine den Schwellenwert überschreitende Menge an Paketverlusten erkannt.
1.3.6.1.4.1.6876.100.1.0.30104	vmwVTEPUnderlayPacketDropEvent	Moderat	VTEP-Underlay-Paketverluste	Erhebliche Anzahl Paketverluste in VTEP-Underlay erkannt

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.30105	vmwPnicUnderlyingSwitchPortPacketDropEvent	Warnung	Paketverluste am zugrunde liegenden Switch-Port für pNIC	Auf dem Switch-Port, der der angegebenen physischen Netzwerkkarte zugeordnet ist, wurde eine den Schwellenwert überschreitende Menge an Paketverlusten erkannt.
1.3.6.1.4.1.6876.100.1.0.30106	vmwDevicePacketDropEvent	Warnung	Am Hardware-Gateway-Port erkannte Paketverluste	Auf dem angegebenen Gerät wurde eine den Schwellenwert überschreitende Menge an Paketverlusten erkannt.
1.3.6.1.4.1.6876.100.1.0.30110	vmwSwitchPortUptimeThresholdRecededEvent	Warnung	SwitchPortUptimeThresholdRecededEvent	Betriebszeit verkürzt
1.3.6.1.4.1.6876.100.1.0.30111	SwitchPortOperationalDownEvent	Warnung	Switch-Port ist ausgefallen	Switch-Port ist ausgefallen.
1.3.6.1.4.1.6876.100.1.0.30112	RouterInterfaceOperationalDownEvent	Warnung	Router-Schnittstelle ist ausgefallen	Router-Schnittstelle ist ausgefallen.
1.3.6.1.4.1.6876.100.1.0.30116	UnderlayDeviceFanMalFunctionEvent	Warnung	Ereignis: Underlay-Gerätelüfter wurde entfernt oder funktioniert nicht.	Ereignis: Underlay-Gerätelüfter wurde entfernt oder funktioniert nicht.
1.3.6.1.4.1.6876.100.1.0.30117	UnderlayDeviceTemperatureThresholdExceededEvent	Warnung	Der Schwellenwert für die Underlay-Gerätetemperatur hat das Ereignis überschritten.	Der Schwellenwert für die Underlay-Gerätetemperatur hat das Ereignis überschritten.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.30118	UnderlayDeviceFexFanMalFunctionEvent	Warnung	Ereignis: FEX-Lüfter wurde entfernt oder funktioniert nicht	Ereignis: FEX-Lüfter wurde entfernt oder funktioniert nicht.
1.3.6.1.4.1.6876.100.1.0.30119	UnderlayDeviceFexPsMalFunctionEvent	Warnung	Ereignis: FEX-Netzteil wurde entfernt oder funktioniert nicht	Ereignis: FEX-Netzteil wurde entfernt oder funktioniert nicht.
1.3.6.1.4.1.6876.100.1.0.30120	UnderlayDeviceModuleMalFunctionEvent	Warnung	Ereignis: Underlay-Gerätemodul wurde entfernt oder funktioniert nicht	Ereignis: Underlay-Gerätemodul wurde entfernt oder funktioniert nicht.
1.3.6.1.4.1.6876.100.1.0.30121	UnderlayDevicePsMalFunctionEvent	Warnung	Ereignis: Underlay-Gerätenetzteil wurde entfernt oder funktioniert nicht	Ereignis: Underlay-Gerätenetzteil wurde entfernt oder funktioniert nicht.
1.3.6.1.4.1.6876.100.1.0.30122	UnderlayDeviceBfdSessionRemovedEvent	Warnung	Ereignis: BFD-Sitzung des Underlay-Geräts wurde gelöscht	Ereignis: BFD-Sitzung des Underlay-Geräts wurde gelöscht.
1.3.6.1.4.1.6876.100.1.0.30123	UnderlayDeviceLldpNeighbourRemovedEvent	Warnung	Ereignis: LLDP-Nachbar des Underlay-Geräts wurde entfernt	Ereignis: LLDP-Nachbar des Underlay-Geräts wurde entfernt
1.3.6.1.4.1.6876.100.1.0.30203	vmwThresholdExceededEventDatastoreFreeSpaceWarning	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30204	vmwThresholdExceededEventDatastoreFreeSpaceCritical	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.30205	vmwThresholdExceededEventDatastoreReadLatency	n. z.	n. z.	n. z.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.30206	vmwThresholdExceededEventDatastoreWriteLatency	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.35001	vmwDistributedFirewallApplyHostEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.35002	vmwDistributedFirewallApplyVMEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.35003	vmwNsxEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.35004	vmwFeatureImpactedEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.35221	vmwNSXComponentEvent	Kritisch	NSX-Verwaltungsdienst wird nicht ausgeführt	Ein NSX-Verwaltungs-Appliance-Dienst ist nicht aktiv.
1.3.6.1.4.1.6876.100.1.0.35222	vmwNSXBackupEvent	Info	NSX Manager-Sicherungen nicht konfiguriert	NSX Manager-Sicherungen sind nicht konfiguriert. Die ordnungsgemäße Sicherung aller NSX-Komponenten ist entscheidend, um das System im Falle eines Fehlers wieder in den Betriebszustand zu versetzen.
1.3.6.1.4.1.6876.100.1.0.35223	vmwNSXBackupAuditLogExcludedEvent	Info	Von der NSX Manager-Sicherung ausgeschlossene Überwachungsprotokolle	Überwachungsprotokolle sind derzeit von der Sicherung ausgeschlossen
1.3.6.1.4.1.6876.100.1.0.35224	vmwNSXUnsecureBackupEvent	Info	NSX Manager-Sicherungen nicht für SFTP konfiguriert	Sicheres FTP wird derzeit nicht für Sicherungen verwendet

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.35225	vmwNSXBackupSystemEventsExcludedEvent	Info	Von NSX Manager-Sicherung ausgeschlossene Systemereignisse	Systemereignisse sind derzeit von der Sicherung ausgeschlossen
1.3.6.1.4.1.6876.100.1.0.35226	vmwNSXBackupNotScheduledEvent	Info	Geplante NSX Manager-Sicherungen nicht aktiviert	Geplante Sicherungen der Umgebung wurden nicht konfiguriert.
1.3.6.1.4.1.6876.100.1.0.35227	vmwNSXBackupNotRecordedEvent	Info	NSX Manager-Sicherung nicht aufgezeichnet	Es wurde keine Sicherung der Umgebung durchgeführt. Die ordnungsgemäße Sicherung aller NSX-Komponenten ist entscheidend, um das System im Falle eines Fehlers wieder in den Betriebszustand zu versetzen.
1.3.6.1.4.1.6876.100.1.0.35228	vmwNSXNtpServerEvent	Info	NTP-Server nicht für NSX Manager konfiguriert	Auf dem NSX Manager ist kein NTP-Server konfiguriert

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.35229	vmwNSXSysLogServerEvent	Info	Syslog-Server nicht für NSX Manager konfiguriert	Für den NSX Manager ist kein Syslog-Server konfiguriert. Syslog-Daten sind nützlich für die Fehlerbehebung und Überprüfung der während der Installation und Konfiguration protokollierten Daten.
1.3.6.1.4.1.6876.100.1.0.35230	vmwControllerSysLogServerEvent	Info	Syslog-Server nicht für NSX Controller konfiguriert	Für den Syslog-Server ist kein NSX Controller konfiguriert. Syslog-Daten sind nützlich für die Fehlerbehebung und Überprüfung der während der Installation und Konfiguration protokollierten Daten.
1.3.6.1.4.1.6876.100.1.0.35231	vmwNSXIPv6EnabledEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.35232	vmwNSXospfNeighborDownEvent	Warnung	Mindestens ein OSPF-Nachbar ist vom NSX Edge-Router aus nicht erreichbar	Mindestens ein mit NSX Edge verbundener OSPF-Nachbar ist ausgefallen

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.36022	vmwClusterFeatureVersionMismatchEvent	Info	Keine Übereinstimmung der Version der NSX-Funktion mit der Version des ESXi-Clusters	Die Version der NSX-Funktion des vorbereiteten Clusters stimmt nicht mit der von NSX Manager überein.
1.3.6.1.4.1.6876.100.1.0.36023	vmwHostFeatureVersionMismatchEvent	Info	Keine Übereinstimmung der NSX-Funktionsversion von Host und Cluster	Die Version des Fabric-Status der Ressourcenfunktion dieses Hosts entspricht nicht der des Clusters oder NSX Managers.
1.3.6.1.4.1.6876.100.1.0.36024	vmwFeatureVersionMismatchEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.36025	vmwHostFeatureEnabledMismatchEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.36026	vmwHostFeatureInstalledMismatchEvent	Info	Funktionsstatus des Netzwerk-Fabric von Host und Cluster stimmt nicht überein	Der Status der Netzwerk-Fabric-Funktion für einen Host stimmt nicht mit dem Status anderer Hosts im Cluster überein.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.36027	vmwHostVtepNotFoundEvent	Kritisch	Keinen VTEP auf vorbereitetem Host gefunden	Auf einem Host in einem für NSX vorbereiteten Cluster fehlt mindestens ein VTEP. VMs auf diesem Host, die mit einem logischen Switch verbunden sind, können möglicherweise nicht kommunizieren.
1.3.6.1.4.1.6876.100.1.0.36028	vmwHostVtepDisconnectedEvent	Warnung	VTEP des Hosts ist für die Verwaltung deaktiviert	Der VTEP des Hosts wurde deaktiviert und hat den Status „Nicht verbunden“.
1.3.6.1.4.1.6876.100.1.0.36029	vmwHostVtepEvent	Kritisch	Host-VTEP getrennt	Host-VTEP getrennt
1.3.6.1.4.1.6876.100.1.0.36030	vmwClusterHostsVtepMTUMismatchEvent	Warnung	Keine Übereinstimmung der VTEP-MTU bei Host und vorbereitetem NSX-Cluster	Die VTEP-MTU zwischen einem Host und dem vorbereiteten NSX-Cluster stimmt nicht überein.
1.3.6.1.4.1.6876.100.1.0.36031	vmwFeatureUnhealthyEvent	Warnung	Status der Netzwerk-Fabric-Funktion im Fehlerzustand	Die installierte NSX-Funktion wird von NSX Manager gemeldet, da ein Problem aufgetreten ist.
1.3.6.1.4.1.6876.100.1.0.36032	vmwEdgeHANTotConfiguredEvent	Info	Hochverfügbarkeit für NSX Edge nicht aktiviert	Hochverfügbarkeit ist auf NSX Edge nicht aktiviert
1.3.6.1.4.1.6876.100.1.0.36033	vmwEdgeInterfacesDownEvent	Warnung	Mindestens eine Schnittstelle des logischen NSX Edge-Routers ist ausgefallen	Mindestens eine NSX Edge-Schnittstelle ist ausgefallen.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.36041	vmwModuleUnhealthyEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.36042	vmwModuleNotLoadedEvent	Kritisch	NSX-VIB- oder Host-Modul wurde auf dem Host nicht erkannt	Mindestens ein NSX-VIB- oder Host-Modul wurde auf dem Host nicht erkannt
1.3.6.1.4.1.6876.100.1.0.36043	vmwModuleNetworkConnectionFailureEvent	Kritisch	Nachrichtenbus- und/oder Steuerebenenverbindung zwischen NSX Manager und Host nicht hergestellt	Der Nachrichtenbus- und/oder der Steuerungsebenen-Agent-Daemon auf diesem Host weist Verbindungsfehler mit NSX Controller oder NSX Manager auf.
1.3.6.1.4.1.6876.100.1.0.36044	vmwHostNetworkControlPlaneMismatchEvent	Moderat	Keine Übereinstimmung der Tabelle logischer Switches für Host und NSX Controller	Informationen zum logischen Switch zwischen dem primären NSX-Controller und allen Hosts, auf denen der logische Switch verwendet wird, stimmen nicht überein. Dieses Ereignis kann darauf hindeuten, dass nach einer Sharding-Änderung ein Fehlerzustand auftritt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.36045	vmwHostNetworkControlPlaneConnectionFailureEvent	Kritisch	Für mindestens einen logischen Switch besteht keine Verbindung zwischen der Host-Steuerungsebene und dem Controller	Die Verbindung zwischen dem Steuerungsebenen-Agenten auf einem NSX-Host und dessen primärem NSX Controller für einen oder mehrere logische Switches wurde nicht hergestellt. Diese Bedingung kann zu veralteten Informationen auf dem Host und den NSX Controllern führen.
1.3.6.1.4.1.6876.100.1.0.36046	vmwHostNetworkControlPlaneNotSyncedEvent	Moderat	Logisches Netzwerk außerhalb der Synchronisierung zwischen Host und NSX Controller	Die logischen Switching- und Routing-Informationen auf einem Host sind nicht mit den NSX Controller-Informationen synchronisiert. Zur Bestätigung dieses Zustands
1.3.6.1.4.1.6876.100.1.0.36047	vmwNSXControllerClusterMajorityEvent	Moderat	Keine NSX Controller-Mehrheit	Einige der NSX Controller im Cluster kommunizieren nicht mit NSX Manager
1.3.6.1.4.1.6876.100.1.0.36048	vmwNSXControllersVMOnSameHostEvent	Info	Alle Controller-VMs, die auf demselben Host bereitgestellt werden	Alle NSX Controller im Cluster werden auf demselben Host bereitgestellt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.36049	vmwVxLanRangeExhaustEvent	Warnung	ID-Bereich für VXLAN-Segment ist erschöpft	Mehr als 90 % der VXLAN-Segment-IDs wurden verwendet.
1.3.6.1.4.1.6876.100.1.0.36050	vmwNSXFirewallDefaultAllowAllRulesEvent	Info	Gesamter nach Standard-Firewallregel zulässiger Datenverkehr	Die verteilte Firewall ist so konfiguriert, dass sie sämtlichen Datenverkehr standardmäßig zulässt
1.3.6.1.4.1.6876.100.1.0.36051	vmwLogicalRouterNoUplinkEvent	Info	NSX-DLR ohne Uplink-Schnittstelle bereitgestellt	Für den NSX-DLR ist keine Uplink-Schnittstelle konfiguriert
1.3.6.1.4.1.6876.100.1.0.36052	vmwEdgeNotHAEvent	Info	NSX Edge ist konfiguriert, aber nicht hochverfügbar	Wenn zwei Edge-VMs für Edge-Hochverfügbarkeit konfiguriert wurden
1.3.6.1.4.1.6876.100.1.0.36053	vmwEdgeNotDeployedEvent	Info	Fehler bei der NSX Edge-Bereitstellung	Eine NSX Edge konnte nicht bereitgestellt werden. Dieser Zustand kann darauf hindeuten, dass eine NSX Edge konfiguriert wurde, ohne tatsächlich bereitgestellt zu werden.
1.3.6.1.4.1.6876.100.1.0.36054	vmwEcmpIsEnabledAndStatefulServicesAreUpEvent	Info	Mit ECMP und statusbehafteten Edge-Diensten konfigurierte NSX Edge	Eine Firewall

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.36055	vmwLogicalRouterDeployedOnEcmpEdgeHostEvent	Info	NSX-DLR wird auf demselben Host wie eine oder mehrere NSX-ECMP-Edges bereitgestellt	Der NSX Distributed Logical Router der Steuerungs-VM wird auf demselben Host bereitgestellt wie ein oder mehrere NSX Edges, die für ECMP konfiguriert sind.
1.3.6.1.4.1.6876.100.1.0.36056	vmwEdgeMissingInterfaceOSPFAreaMappingEvent	Info	Zuordnung der NSX Edge-Schnittstelle zum OSPF-Bereich fehlt	OSPF ist auf NSX Edge aktiviert
1.3.6.1.4.1.6876.100.1.0.36057	vmwOspfInsecureAuthRouterEvent	Info	Unsichere Authentifizierung in einem oder mehreren OSPF-Bereichen verwendet	Mindestens ein OSPF-Bereich auf dem NSX Edge-Dienstgateway oder DLR ist nicht für die MD5-Authentifizierung konfiguriert.
1.3.6.1.4.1.6876.100.1.0.36058	vmwNSXControllersDeployedCountEvent	Info	Falsche Anzahl der bereitgestellten NSX Controller	Es sind weniger als drei Controller bereitgestellt
1.3.6.1.4.1.6876.100.1.0.36059	vmwNSXControllerNotActiveCountEvent	Moderrat	Weniger als drei aktive NSX Controller	Es sind weniger als drei aktive Controller vorhanden
1.3.6.1.4.1.6876.100.1.0.36060	vmwNSXControllerEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.36061	vmwNSXEdgeDownEvent	Info	Eine oder mehrere NSX Edges im ECMP-Cluster sind derzeit ausgefallen	Eine oder mehrere NSX Edges im ECMP-Cluster sind derzeit ausgefallen

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.36062	vmwNSXMajorityEcmpEdgesDownEvent	Warnung	Die Mehrheit der NSX Edges im ECMP-Cluster ist derzeit inaktiv	Die Mehrheit der NSX Edges im ECMP-Cluster ist derzeit inaktiv
1.3.6.1.4.1.6876.100.1.0.36063	vmwNSXAllEcmpEdgesDownEvent	Kritisch	Alle NSX Edges im ECMP-Cluster sind derzeit nicht verfügbar	Alle NSX Edges im ECMP-Cluster sind derzeit nicht verfügbar
1.3.6.1.4.1.6876.100.1.0.36064	vmwNSXEdgeMtuMismatchEvent	Info	Die auf einer oder mehreren Schnittstellen an der Edge konfigurierte MTU stimmt nicht mit der MTU auf dem nächsten Hop-Router überein	Die MTU, die für eine oder mehrere Schnittstellen auf den Edges im selben Layer-2-Netzwerk konfiguriert ist, stimmt nicht überein.
1.3.6.1.4.1.6876.100.1.0.36065	vmwNSXEdgesSplitBrainEvent	Kritisch	Beide NSX Edge-HA-VMs im aktiven Zustand	Beide VMs von Edge HA befinden sich im aktiven Zustand. Das häufigste Problem ist Split-Brain.
1.3.6.1.4.1.6876.100.1.0.36066	vmwVirtualDistributedRoutingEvent	Warnung	VDR-Port wurde auf dem Host für das VXLAN-Routing nicht gefunden	Der VDR-Port wurde auf dem Host für das angegebene VXLAN nicht gefunden
1.3.6.1.4.1.6876.100.1.0.36067	vmwNSXEdgeBGPNeighbourDownEvent	Kritisch	Mindestens ein BGP-Nachbar befindet sich nicht im Status „Eingerichtet“	Mindestens ein BGP-Nachbar befindet sich nicht im Status „Eingerichtet“.
1.3.6.1.4.1.6876.100.1.0.37001	vmwAnalyticsEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.37002	vmwAnalyticsOutlierEvent	n. z.	n. z.	n. z.

OID	Ereignisname	Standardsehwergrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.37003	vmwAnalyticsThresholdEvent	Kritisch	Schwellenwertverstoß (Ereignis)	Das als Ergebnis der angegebenen Metrik generierte Ereignis überschreitet die in der Konfiguration angegebene obere oder untere Grenze.
1.3.6.1.4.1.6876.100.1.0.38001	vmwVMCEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.40001	vmwCriticalHostNotAccessibleEvent	Kritisch	Zugriff auf Host mit Infrastruktur-VMs nicht möglich	Zugriff auf Host mit Infrastruktur-VMs nicht möglich
1.3.6.1.4.1.6876.100.1.0.568	vmwArkinApplicationMemberLimitEvent	Info	Grenzwert für Anwendungsmitgliedschaft überschritten	Die Anzahl der Mitglieder in der Anwendung überschreitet den unterstützten Grenzwert.
1.3.6.1.4.1.6876.100.1.0.70000	vmwGenericNSXSystemEvent	Moderrat	NSX-Systemereignis (Warnung)	NSX-Systemereignisse mit hohem oder schwerwiegenden Schweregrad
1.3.6.1.4.1.6876.100.1.0.70001	vmwFilterConfigApplyOnHostFailedEvent	Warnung	Fehler beim Anwenden der Aktualisierung der verteilten Firewall für Host-vNIC	Ein Konfigurations-Update der verteilten Firewall konnte nicht auf eine vNIC auf einem für NSX vorbereiteten Host angewendet werden.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.70002	vmwRulesetLoadOnHostFailedEvent	Warnung	Fehler beim Anwenden der Aktualisierung der verteilten Firewall auf den Host	Ein Regelsatz der verteilten Firewall wurde nicht auf einen Host angewendet.
1.3.6.1.4.1.6876.100.1.0.70003	vmwConfigUpdateOnHostFailedEvent	Warnung	Fehler beim Aktualisieren der Konfiguration für die verteilte Firewall	Bei der Aktualisierung der Firewallkonfiguration auf einen NSX-Host ist eine Zeitüberschreitung aufgetreten. Der Host wird nicht mit der neuesten Version der Firewallkonfiguration synchronisiert.
1.3.6.1.4.1.6876.100.1.0.70004	vmwSpoofguardConfigUpdateOnHostFailedEvent	Info	Fehler beim Aktualisieren der SpoofGuard-Konfiguration	Für den Host ist ein Update der SpoofGuard-Konfiguration fehlgeschlagen.
1.3.6.1.4.1.6876.100.1.0.70005	vmwApplyRuleToVnicFailedEvent	Warnung	Regel für die verteilte Firewall nicht auf Host-vNIC angewendet	Eine Regel für die verteilte Firewall wurde nicht auf die vNIC eines Hosts angewendet.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.70006	vmwContainerConfigUpdateOnVnicFailedEvent	Warnung	Fehler beim Aktualisieren des Containers für verteilte Firewall auf Host	Netzwerk- und Sicherheitscontainter-Informationen, die mit der verteilten NSX-Firewall oder mit Service Composer verwendet werden, konnten auf einem NSX-Host nicht aktualisiert werden.
1.3.6.1.4.1.6876.100.1.0.70007	vmwSpoofguardApplyToVnicFailedEvent	Info	Fehler bei SpoofGuard-Erstkonfiguration	Die SpoofGuard-Konfiguration wurde nicht auf die angegebene vNIC auf dem Host angewendet.
1.3.6.1.4.1.6876.100.1.0.70008	vmwHostMessagingConfigurationFailedEvent	Warnung	Fehler beim Aktualisieren der Host-Messaging-Konfiguration	Ein Konfigurations-Update, das über den NSX-Messaging-Kanal an Hosts übertragen wurde, wurde nicht abgeschlossen.
1.3.6.1.4.1.6876.100.1.0.70009	vmwHostMessagingConnectionReconfigurationFailedEvent	Warnung	Fehler beim Neukonfigurieren der Host-Messaging-Verbindung	Aktualisierte Informationen zum Host-Messaging-Kanal konnten nicht an den NSX-Host gesendet werden.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.70010	vmwHostMessagingConfigurationFailedNotificationSkippedEvent	Warnung	Fehler beim erneuten Einrichten des Host-Messaging-Kanals zwischen Host und NSX Manager	NSX Manager versucht, den Nachrichtenbuskanal wieder einzurichten, wenn der vorbereitete Host wieder mit vCenter Server verbunden ist. Diese Verbindung ist erneut fehlgeschlagen.
1.3.6.1.4.1.6876.100.1.0.70011	vmwHostMessagingInfrastructureDownEvent	Warnung	Host-Messaging-Infrastruktur ist auf dem Host nicht aktiv	Mindestens zwei Messaging-Channel-Taktsignalmeldungen zwischen NSX Manager und einem NSX-Host wurden ausgelassen.
1.3.6.1.4.1.6876.100.1.0.70012	vmwEdgeVMNotRespondingEvent	Moderrat	Taktsignal von NSX Edge an NSX Manager fehlgeschlagen	Eine NSX Edge-VM reagiert nicht auf die Integritätsprüfung durch NSX Manager.
1.3.6.1.4.1.6876.100.1.0.70013	vmwEdgeUnhealthyEvent	Kritisch	NSX Edge-VM nicht im Status „Aktiv/Selbst“	NSX Edge-VM meldet einen problematischen Zustand und funktioniert möglicherweise nicht ordnungsgemäß.
1.3.6.1.4.1.6876.100.1.0.70014	vmwEdgeVMCommunicationFailureEvent	Kritisch	Fehler bei der Kommunikation zwischen NSX Manager und Edge-VM	Kommunikationsfehler zwischen NSX Manager und Edge-VM erkannt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.70015	vmwNSXEdgeEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.71000	vmwOtherCriticalNSXEvent	Kritisch	Kritisches NSX-Systemereignis	NSX-Systemereignisse mit kritischem Schweregrad.
1.3.6.1.4.1.6876.100.1.0.80001	vmwPanNsxNotInRegisteredStateEvent	Kritisch	Palo Alto Panorama ist bei NSX Manager nicht registriert	Panorama ist nicht bei NSX Manager registriert.
1.3.6.1.4.1.6876.100.1.0.80002	vmwPanNsxDynamicUpdateDelayedEvent	Warnung	Dynamische Aktualisierung der Mitgliedschaftsdefinition in Panorama verzögert	Aktualisierung der dynamischen Panorama-Mitgliedschaftsdefinition von NSX Manager verzögert. Dieser Zustand weist möglicherweise auf ein Problem mit der Netzwerkkonnektivität oder ein Problem mit dem NetX-Dienst von NSX Manager hin.
1.3.6.1.4.1.6876.100.1.0.80003	vmwPanDeviceInDisconnectedStateEvent	Warnung	Palo Alto-Dienst-VM ist nicht mit Panorama verbunden	Eine Dienst-VM oder ein Gerät für Palo Alto-Netzwerke befindet sich in einem nicht verbundenen Zustand mit Panorama.
1.3.6.1.4.1.6876.100.1.0.80004	vmwPanNsxServiceApplianceViewMismatchEvent	Kritisch	Keine Übereinstimmung des Status der Dienst-VM bei Panorama und NSX Manager	Nichtübereinstimmung bei Dienst-Appliance-Informationen zwischen NSX Manager und Panorama.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80005	vmwPanNsxFabricAgentNotFoundOnHostEvent	Kritisch	NSX-Fabric-Agent auf dem Host nicht gefunden	Sicherheits-Fabric-Agent wird von NSX für einen Host, auf dem der Cluster vorbereitet wird, nicht gemeldet.
1.3.6.1.4.1.6876.100.1.0.80006	vmwPanNsxServiceVMNotFoundOnHostEvent	Kritisch	Palo Alto-Dienst-VM wurde auf dem Host nicht gefunden	Eine Sicherheits-Appliance-VM von Palo Alto Networks wurde auf einem Host in einem vorbereiteten NSX-Cluster nicht gefunden.
1.3.6.1.4.1.6876.100.1.0.80100	vmwCheckpointEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.80102	vmwCheckpointNsxFabricAgentNotFoundOnHostEvent	Kritisch	CheckpointNsxFabricAgentNotFoundOnHostEvent	Sicherheits-Fabric-Agent wird von NSX für einen Host, auf dem der Cluster vorbereitet wird, nicht gemeldet.
1.3.6.1.4.1.6876.100.1.0.80103	vmwCheckpointNsxServiceVMNotFoundOnHostEvent	Kritisch	CheckpointNsxServiceVMNotFoundOnHostEvent	Eine Check Point-Sicherheits-Appliance-VM wurde auf einem Host in einem vorbereiteten NSX-Cluster nicht gefunden.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80104	vmwCheckpointGatewaySicStatusNotCommunicatingEvent	Kritisch	CheckpointGatewaySicStatusNotCommunicatingEvent	Eine Dienst-VM oder ein Gateway für Check Point weist nicht den SIC-Status „Kommuniziert“ auf.
1.3.6.1.4.1.6876.100.1.0.80105	vmwCheckpointNsxServiceApplianceViewMismatchEvent	Kritisch	Status der Dienst-VMs von Check Point und NSX Manager stimmen nicht überein	Nichtübereinstimmung bei Dienst-Appliance-Informationen zwischen NSX Manager und Check Point.
1.3.6.1.4.1.6876.100.1.0.80200	NSXTEvent	n. z.	NSX-T-Systemereignis	Von der NSX-T-Plattform generierte Alarme/ Ereignisse
1.3.6.1.4.1.6876.100.1.0.80201	NSXTVcNotAddedEvent	Warnung	Mindestens ein vCenter Server wurde nicht als Datenquelle in vRNI hinzugefügt	NSX-T verfügt über einen oder mehrere Berechnungsmanager, die nicht als Datenquellen in vRNI mit derselben IP bzw. demselben FQDN hinzugefügt werden.
1.3.6.1.4.1.6876.100.1.0.80202	NSXTStandaloneHostsEvent	Warnung	Mindestens ein Fabric-Knoten wird als eigenständiger Host in NSX-T hinzugefügt	Einer oder mehrere Fabric-Knoten werden als eigenständige Hosts in NSX-T hinzugefügt. Virtuelle Maschinen auf diesen Hosts sind in vRNI nicht sichtbar.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80203	vmwNSXSystemEvent	n. z.	n. z.	n. z.
1.3.6.1.4.1.6876.100.1.0.80205	NSXNoUplinkConnectivityEvent	Warnung	Logischer NSX-T-Ebene-1-Router getrennt (Ereignis)	Der logische NSX-T-Ebene-1-Router ist vom Ebene-0-Router getrennt. Netzwerke unter diesem Router sind von außerhalb nicht erreichbar und umgekehrt.
1.3.6.1.4.1.6876.100.1.0.80206	NSXRoutingAdvertisementEvent	Warnung	Routing-Ankündigung deaktiviert	Die Routing-Ankündigung ist für den logischen NSX-T-Ebene-1-Router deaktiviert. Netzwerke unter diesem Router sind von außerhalb nicht erreichbar.
1.3.6.1.4.1.6876.100.1.0.80207	NSXManagerConnectivityDownEvent	Kritisch	NSX-T Edge-Knoten verfügt über keine Manager-Konnektivität	Manager-Konnektivität des NSX-T Edge-Knotens wurde getrennt.
1.3.6.1.4.1.6876.100.1.0.80208	NSXControllerConnectivityDegradedEvent	Warnung	Controller-Konnektivität für NSX-T Edge-Knoten herabgestuft	Der NSX-T Edge-Knoten kann nicht mit einem oder mehreren Controllern kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80209	NSXControllerConnectivityDownEvent	Kritisch	NSX-T Edge-Knoten verfügt über keine Controller-Konnektivität	Der NSX-T Edge-Knoten ist nicht in der Lage, mit einem der Controller zu kommunizieren.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtumismatchEvent	Warnung	MTU-Nichtübereinstimmung zwischen NSX-T-Ebene-0- und Uplink-Switch/Router	Die auf den Schnittstellen des logischen Tier-0-Routers konfigurierte MTU stimmt nicht mit den Schnittstellen des Uplink-Switch/-Routers aus demselben L2-Netzwerk überein. Dies kann sich auf die Netzwerkleistung auswirken.
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	Info	Eine oder mehrere VMs sind von der NSX-T DFW-Firewall ausgeschlossen.	Eine oder mehrere VMs sind nicht durch die NSX-T DFW-Firewall geschützt. vRealize Network Insight erhält keine IPFIX-Flows für diese VMs.
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	Warnung	Fehlkonfiguration des Uplink-VLAN	Die Kommunikation wird unterbrochen, da sich das VLAN auf dem Uplink-Port des Tier-0-Routers vom VLAN auf dem externen Gateway unterscheidet.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	Warnung	An den Transportknoten ist keine Transportzone angehängt.	Dem Transportknoten wurde keine Transportzone hinzugefügt. Daher verlieren VMs möglicherweise die Konnektivität.
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	Warnung	Kein VTEP auf dem Transportknoten verfügbar.	Alle VTEPs werden aus dem Transportknoten gelöscht. VMs verlieren möglicherweise aus diesem Grund die Konnektivität.
1.3.6.1.4.1.6876.100.1.0.80215	vmwDuplicateL3SwitchEvent	Kritisch	Gleicher Switch oder Router hinzugefügt (Ereignis)	Derselbe Switch oder Router wird mit unterschiedlichen IPs hinzugefügt. VM-zu-VM-Pfad kann nicht generiert werden.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80216	vmwLBPoolMemberDownEvent	Kritisch	Poolmitglied nicht verfügbar	Dieses Ereignis wird ausgelöst, wenn das Poolmitglied des Lastausgleichsdienstes nicht verfügbar ist. Um zu ermitteln, welche Poolmitglieder nicht verfügbar sind, suchen Sie nach „Pool Member where state = DISABLED“ (Poolmitglied mit Status = DEAKTIVIERT).
1.3.6.1.4.1.6876.100.1.0.80217	vmwLBPoolDownEvent	Kritisch	Pool inaktiv	Dieses Ereignis wird ausgelöst, wenn der Pool des Lastausgleichsdienstes nicht verfügbar ist.
1.3.6.1.4.1.6876.100.1.0.80218	vmwLBPoolEmptyEvent	Kritisch	Pool leer	Dieses Ereignis wird ausgelöst, wenn der Pool des Lastausgleichsdienstes leer ist. Um herauszufinden, welche Pools leer sind, suchen Sie nach „Pool where PoolMembers Count = 0“ (Pool mit PoolMembers-Anzahl = 0).

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80219	vmwLBPoolMemberVMDownEvent	Kritisch	VM des Poolmitglieds nicht verfügbar	Dieses Ereignis wird ausgelöst, wenn die VM, die dem Poolmitglied des Lastausgleichsdienstes zugeordnet ist, nicht bereit ist.
1.3.6.1.4.1.6876.100.1.0.80220	vmwLBVirtualServerDisableEvent	Kritisch	Virtueller Server des Lastausgleichsdienstes deaktiviert	Dieses Ereignis wird ausgelöst, wenn der virtuelle Server des Lastausgleichsdienstes deaktiviert ist.
1.3.6.1.4.1.6876.100.1.0.80221	vmwLBServiceNodeIPNotFoundEvent	Kritisch	IP des Dienstknotens nicht gefunden	Dieses Ereignis wird ausgelöst, wenn keine der IP-Adresse des Dienstknotens des Lastausgleichsmodus zugeordnete Netzwerkkarte gefunden wurde.
1.3.6.1.4.1.6876.100.1.0.80222	vmwLBServiceNodeMultipleNICFoundEvent	Kritisch	Mehrere Netzwerkkarten des Dienstknotens gefunden	Dieses Ereignis wird ausgelöst, wenn mehrere Netzwerkkarten, die mit der IP des Dienstknotens des Lastausgleichsdienstes verknüpft sind, gefunden werden.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80223	NSXSwitchIpflixEnabledEvent	Warnung	NSX-T-Switch-IPFIX ist aktiviert und weist ein Collector-Profil auf, das auf einen der vRNI-Collectors verweist.	Network Insight unterstützt die IPFIX-Flow-Daten von NSX-T-Switches nicht. Gemäß der Konfiguration werden IPFIX-Daten an Network Insight Collector-VM gesendet. Möglicherweise wurden vorhandene Flow-Daten im System beschädigt.
1.3.6.1.4.1.6876.100.1.0.80224	NSXStandaloneHostsWithoutVcEvent	Kritisch	Ein vCenter, das einen oder mehrere Fabric-Knoten in NSX-T verwaltet, wird nicht als Datenquelle in vRNI hinzugefügt	Ein vCenter, das einen oder mehrere Fabric-Knoten in NSX-T verwaltet, wird nicht als Datenquelle in vRNI hinzugefügt. Virtuelle Maschinen auf diesen Hosts werden in vRNI nicht angezeigt.
1.3.6.1.4.1.6876.100.1.0.80225	NSXControllerNodeToControlClusterConnectivityEvent	Kritisch	Der NSX-T-Controller-Knoten ist nicht mit dem Steuerungscluster verbunden	Der NSX-T-Controller-Knoten hat die Verbindung zum Steuerungscluster verloren.
1.3.6.1.4.1.6876.100.1.0.80226	NSXControllerNodeToMgmtPlaneConnectivityEvent	Kritisch	NSX-T-Controller-Knoten ist nicht mit der Managementebene verbunden	Der NSX-T-Controller-Knoten hat die Verbindung zur Managementebene verloren.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	Kritisch	NSX-T-Verwaltungsknoten ist nicht mit dem Verwaltungscluster verbunden	Der NSX-T-Verwaltungsknoten hat die Verbindung zum Verwaltungscluster verloren.
1.3.6.1.4.1.6876.100.1.0.80228	NSXHostNodePnicStatusDownEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80229	NSXHostNodePnicStatusDegradedEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80230	NSXHostNodePnicStatusUnknownEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80231	NSXHostNodeTunnelStatusDownEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80232	NSXHostNodeTunnelStatusDegradedEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80233	NSXHostNodeTunnelStatusUnknownEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80234	NSXHostNodeStatusDownEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80235	NSXHostNodeStatusDegradedEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.	Der Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80236	NSXHostNodeStatusUnknownEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der Status des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Unbekannt“.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradedEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der Status des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	Warnung	NSX-T-Hostknoten verfügt über keine Manager-Konnektivität	Desynchronisierung des Konnektivitätsstatus von NSX Manager mit Hosttransportknoten

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	Kritisch	Controller-Konnektivität für NSX-T Edge-Knoten ist „Unbekannt“.	Die Controller-Konnektivität des NSX-T Edge-Knotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	Warnung	NSX-T-Hostknoten verfügt über keine Controller-Konnektivität	Der NSX-T-Hostknoten ist nicht in der Lage, mit einem der Controller zu kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	Warnung	Controller-Konnektivität für NSX-T-Hostknoten herabgestuft	Der NSX-T-Hostknoten kann nicht mit einem oder mehreren Controllern kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	Warnung	Controller-Konnektivität für NSX-T-Hostknoten ist „Unbekannt“.	Die Controller-Konnektivität des NSX-T-Hostknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	Warnung	Der Administratorstatus des logischen NSX-T-Switches ist „Nicht verfügbar“	Der Administratorstatus des logischen NSX-T-Switches ist „Nicht verfügbar“

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	Kritisch	Der Betriebsstatus des logischen NSX-T-Ports ist „Nicht verfügbar“	Der Betriebsstatus des logischen NSX-T-Ports ist „Nicht verfügbar“. Dies kann zu einem Kommunikationsfehler zwischen zwei virtuellen Schnittstellen (VIFs) führen, die mit demselben logischen Switch verbunden sind, z. B. können Sie eine VM nicht von einer anderen Maschine aus anpingen.
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	Warnung	Der Betriebsstatus des logischen NSX-T-Ports ist „Unbekannt“	Der Betriebsstatus des logischen NSX-T-Ports ist „Unbekannt“. Dies kann zu einem Kommunikationsfehler zwischen zwei virtuellen Schnittstellen (VIFs) führen, die mit demselben logischen Switch verbunden sind, z. B. können Sie eine VM nicht von einer anderen Maschine aus anpingen.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	Warnung	Verbindungsstatus von NSX-T-Berechnungsmanager ist nicht „Verfügbar“.	Verbindungsstatus von NSX-T-Berechnungsmanager ist nicht „Verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackupDisabledEvent	Warnung	NSX-T Manager-Sicherung ist nicht geplant.	NSX-T Manager-Sicherung ist nicht geplant.
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	Kritisch	Die NSX-T DFW-Firewall ist deaktiviert.	Die verteilte Firewall ist im NSX-T Manager deaktiviert.
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	Warnung	Vom logischen NSX-T-Port empfangene Pakete gehen verloren.	Empfangene Pakete gehen auf dem logischen NSX-T-Port verloren und zugehörige Einheiten werden möglicherweise davon betroffen.
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	Warnung	Vom logischen NSX-T-Port übertragene Pakete gehen verloren.	Übertragene Pakete gehen auf dem logischen NSX-T-Port verloren, und zugehörige Einheiten werden möglicherweise davon betroffen.
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	Warnung	Vom logischen NSX-T-Switch empfangene Pakete gehen verloren.	Empfangene Pakete gehen auf dem logischen NSX-T-Switch verloren, und zugehörige Einheiten werden möglicherweise davon betroffen.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	Warnung	Vom logischen NSX-T-Switch übertragene Pakete gehen verloren.	Übertragene Pakete gehen auf dem logischen NSX-T-Switch verloren, und zugehörige Einheiten werden möglicherweise davon betroffen.
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	Warnung	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren.	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren. Dies kann sich auf den Netzwerkdatenverkehr im Zusammenhang mit dem NSX-T-Verwaltungscluster auswirken.
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	Kritisch	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren. Dies kann sich auf den Edge-Cluster-Netzwerkdatenverkehr auswirken.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	Warnung	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren. Dies kann sich auf den Netzwerkdatenverkehr auf ESXi-Hosts auswirken.
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	Warnung	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren. Dies kann sich auf den Netzwerkdatenverkehr im Zusammenhang mit dem NSX-T-Verwaltungscluster auswirken.
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	Kritisch	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren. Dies kann sich auf den Edge-Cluster-Netzwerkdatenverkehr auswirken.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	Warnung	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren. Dies kann sich auf den Netzwerkdatenverkehr auf ESXi-Hosts auswirken.
1.3.6.1.4.1.6876.100.1.0.80301	vmwHardwareVTEPMismatchEvent	Kritisch	HardwareVTEPMismatchEvent	Hardware-Gateway-Bindungen stimmen nicht überein
1.3.6.1.4.1.6876.100.1.0.80302	vmwHardwareVTEPPortDownEvent	Kritisch	HardwareVTEPPortDownEvent	Hardware-Gateway-Port ausgefallen
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmInventoryStatusEvent	Warnung	Die Ausführung des CM-Bestandsdiensts wurde beendet	Der Status des CM-Bestandsdiensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmInventoryStatusEvent	Kritisch	CM-Bestandsdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der CM-Inventory-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	Warnung	Die Ausführung des Controller-Diensts wurde beendet.	Der Status des Controller-Diensts wurde in „Angehalten“ geändert.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	Kritisch	Controller-Dienst wurde beendet	Einer der Dienste des NSX-T Verwaltungsknotens, nämlich der Controller-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	Warnung	Die Ausführung des DataStore-Diensts wurde beendet.	Der Status des DataStore-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	Kritisch	DataStore-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der DataStore-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	Warnung	Die Ausführung des HTTP-Diensts wurde beendet.	Der Status des HTTP-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	Kritisch	HTTP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der HTTP-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	Warnung	Die Ausführung des Diensts für die Installation von Upgrades wurde beendet.	Der Status des Diensts für die Installation von Upgrades wurde in „Angehalten“ geändert.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	Warnung	Dienst für die Installation von Upgrades wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Dienst für die Installation von Upgrades, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	Warnung	Die Ausführung des liagent-Diensts wurde beendet.	Der Status des liagent-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	Warnung	liagent-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der LI-Agent-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	Warnung	Die Ausführung des Manager-Diensts wurde beendet.	Der Status des Manager-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	Kritisch	Manager-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich Managerdienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Warnung	Die Ausführung des Management Plane-Diensts wurde beendet.	Der Status des Management Plane-Diensts wurde in „Angehalten“ geändert.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Warnung	Management Plane-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Busdienst der Verwaltungsebene, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Warnung	Die Ausführung des Migrationskoordinator-Diensts wurde beendet.	Der Status des Migrationskoordinator-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Warnung	Migrationskoordinator-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Migrationskoordinator-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	Warnung	Die Ausführung des Knotenverwaltungsdiensts wurde beendet.	Der Status des Knotenverwaltungsdiensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	Kritisch	Knotenverwaltungsdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Knotenverwaltungsdienst, wird nicht mehr ausgeführt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatusEvent	Warnung	Die Ausführung des Knotenstatistikdiensts wurde beendet.	Der Status des Knotenstatistikdiensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatusEvent	Kritisch	Knotenstatistikdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich die Knotenstatistik, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	Warnung	Die Ausführung des Nachrichtenbus-Diensts wurde beendet.	Der Status des Nachrichtenbus-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	Warnung	Nachrichtenbusdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Nachrichtenbusdienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	Warnung	Die Ausführung des Plattform-Client-Diensts wurde beendet.	Der Status des Plattform-Client-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	Kritisch	Plattform-Client-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Plattform Client Service, wird nicht mehr ausgeführt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	Warnung	Die Ausführung des Upgrade-Agent-Diensts wurde beendet.	Der Status des Upgrade-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	Warnung	Upgrade-Agent-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich Upgrade-Agent-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	Warnung	Die Ausführung des NTP-Diensts wurde beendet.	Der Status des NTP-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	Kritisch	NTP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der NTP-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	Warnung	Die Ausführung des Richtliniendienstes wurde beendet.	Der Status des Richtliniendienstes wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	Kritisch	Richtliniendienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Richtliniendienst, wird nicht mehr ausgeführt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	Warnung	Die Ausführung des Suchdiensts wurde beendet.	Der Status des Suchdiensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	Kritisch	Suchdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Suchdienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	Warnung	Die Ausführung des SNMP-Diensts wurde beendet.	Der Status des SNMP-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	Warnung	SNMP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der SNMP-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	Warnung	Die Ausführung des SSH-Diensts wurde beendet.	Der Status des SSH-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	Kritisch	SSH-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der SSH-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	Warnung	Die Ausführung des Syslog-Diensts wurde beendet.	Der Status des Syslog-Diensts wurde in „Angehalten“ geändert.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	Kritisch	Syslog-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Syslog-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	Warnung	Die Ausführung des Telemetriediensts wurde beendet.	Der Status des Telemetriediensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	Warnung	Telemetriedienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Telemetrie-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	Warnung	Die Ausführung des UI-Diensts wurde beendet.	Der Status des UI-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	Kritisch	UI-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der UI-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeServiceClusterManagerStatusEvent	Kritisch	Cluster Manager-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Clustermanager-Dienst, wird nicht mehr ausgeführt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80501	vmwIndexerLagEvent	Kritisch	Indexer-Verzögerung (Ereignis)	Die Indizierung der aktuellen Daten wird noch ausgeführt. Die Suchergebnisse sind möglicherweise ungenau.
1.3.6.1.4.1.6876.100.1.0.80502	vmwIPFIXFlowDPPausedEvent	Kritisch	IPFIX-Flow-Datenquelle angehalten (Ereignis)	Die IPFIX-Flow-Datenquelle wurde aufgrund einer großen Anzahl von Flows angehalten.
1.3.6.1.4.1.6876.100.1.0.80503	vmwGridProcessingStoppedEvent	Kritisch	Tabellenverarbeitung wurde angehalten (Ereignis)	Die Tabellenverarbeitung wurde angehalten.
1.3.6.1.4.1.6876.100.1.0.80504	vmwUnableToSendEmailsEvent	Kritisch	E-Mail-Ereignis kann nicht gesendet werden	E-Mail-Nachricht kann nicht gesendet werden.
1.3.6.1.4.1.6876.100.1.0.80505	vmwSMTPNotConfiguredEvent	Kritisch	SMTP nicht konfiguriert (Ereignis)	SMTP nicht konfiguriert
1.3.6.1.4.1.6876.100.1.0.80506	vmwSNMPNotConfiguredEvent	Kritisch	Systemzustand (Ereignis)	Es sind keine SNMP-Ziele konfiguriert.
1.3.6.1.4.1.6876.100.1.0.80507	vmwReindexingInProgressEvent	Kritisch	Neuindizierung in Bearbeitung (Ereignis)	Daten werden zurzeit neu indiziert. Nach Abschluss dieser Migrationsaktivität ist der Suchdienst verfügbar.
1.3.6.1.4.1.6876.100.1.0.80508	vmwNodesVersionMismatchEvent	Kritisch	Nichtübereinstimmung der Knotenversion (Ereignis)	Nichtübereinstimmung der Knotenversion erkannt

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80509	vmwNotAllServicesRunningEvent	Kritisch	Es werden nicht alle Dienste ausgeführt (Ereignis)	Mindestens ein wichtiger Dienst wird nicht ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80510	vmwNotAllServicesHealthyEvent	Kritisch	Nicht alle Dienste sind fehlerfrei (Ereignis)	Mindestens ein wichtiger Dienst ist nicht fehlerfrei.
1.3.6.1.4.1.6876.100.1.0.80511	vmwExpandPartitionFailedEvent	Kritisch	Erweitern der Partition fehlgeschlagen (Ereignis)	Fehler beim Erweitern der Festplattenpartition.
1.3.6.1.4.1.6876.100.1.0.80512	vmwDiskCleanupFailedEvent	Kritisch	Datenträgerbereinigung fehlgeschlagen (Ereignis)	Der Datenträgerbereinigungsdienst ist fehlerhaft.
1.3.6.1.4.1.6876.100.1.0.80513	vmwVacuumFailedEvent	Kritisch	Fehler bei Vacuum (Ereignis)	Der PostgreSQL Vacuum-Dienst ist fehlerhaft.
1.3.6.1.4.1.6876.100.1.0.80514	vmwConfigStorageCleanupFailedEvent	Kritisch	Fehler bei der Bereinigung des Konfigurationsspeichers (Ereignis)	Der Dienst für die Datenaufbewahrung (Wartung des Konfigurationsspeichers) ist fehlerhaft.
1.3.6.1.4.1.6876.100.1.0.80515	vmwHBaseRetentionToolFailedEvent	Kritisch	Fehler bei HBase-Aufbewahrungstool (Ereignis)	Der Dienst für die Datenaufbewahrung (Konfiguration der Metrik-Aufbewahrung) ist fehlerhaft.
1.3.6.1.4.1.6876.100.1.0.80516	vmwMetricStorageUpdaterFailedEvent	Kritisch	Fehler bei Metrikspeicher-Updater (Ereignis)	Der Dienst für die Datenaufbewahrung (Wartung des Metrik-Speichers) ist fehlerhaft.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80517	vmwCollectorLagEvent	Kritisch	Verzögerung bei Collector (Ereignis)	Letzte Datenerfassung auf Collector liegt länger zurück als der Schwellenwert
1.3.6.1.4.1.6876.100.1.0.80518	vmwCollectionLagEvent	Kritisch	Erfassungsverzögerung (Ereignis)	Die letzte Datenerfassung in der Datenquelle liegt länger zurück als der Schwellenwert
1.3.6.1.4.1.6876.100.1.0.80519	vmwGridProcessingLagEvent	Kritisch	Verzögerung bei der Tabellenverarbeitung (Ereignis)	Die Tabellenverarbeitung ist um mehr als den Schwellenwert verzögert.
1.3.6.1.4.1.6876.100.1.0.80520	vmwConnectionErrorEvent	Kritisch	Verbindungsfehler (Ereignis)	Fehler bei der Verbindung zur Datenquelle
1.3.6.1.4.1.6876.100.1.0.80521	vmwNodeNotActiveEvent	Kritisch	Knoten nicht aktiv (Ereignis)	Knoten nicht aktiv
1.3.6.1.4.1.6876.100.1.0.80522	vmwHighDiskUtilizationEvent	Kritisch	Hohe Festplattennutzung (Ereignis)	Hohe Festplattennutzung
1.3.6.1.4.1.6876.100.1.0.80523	vmwIndexingAbortedEvent	Kritisch	Indizierung abgebrochen (Ereignis)	Indizierung abgebrochen
1.3.6.1.4.1.6876.100.1.0.80524	vmwUpgradeFailedEvent	Kritisch	Upgrade fehlgeschlagen (Ereignis)	Upgrade fehlgeschlagen
1.3.6.1.4.1.6876.100.1.0.80525	vmwFlowProcessingSuspendedEvent	Kritisch	Flow-Verarbeitung angehalten (Ereignis)	Flow-Verarbeitung angehalten
1.3.6.1.4.1.6876.100.1.0.80526	vmwLargeSdmsDroppedEvent	Kritisch	Fehler bei der Datenverarbeitung	Großer SDMS verworfen
1.3.6.1.4.1.6876.100.1.0.80527	vmwApplianceNotConfiguredEvent	Kritisch	Appliance nicht konfiguriert (Ereignis)	Die Konfiguration der Collector-VM ist unvollständig.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80531	vmwFdbConfigStoreCleanupFailedEvent		FDB_CONFIG_STORE_CLEANUP_FAILED_EVENT	Fehler bei der Bereinigung des FDB-Konfigurationsspeichers (Ereignis)
1.3.6.1.4.1.6876.100.1.0.80531	vmwDiskAllocationInsufficientEvent	Info	DISK_ALLOCATION_INSUFFICIENT_EVENT	Datenträger nicht konfiguriert (Ereignis)
1.3.6.1.4.1.6876.100.1.0.80601	vmwFailedEvent	Kritisch	Fehler bei Datenquelle (Ereignis)	Fehler bei Datenquelle
1.3.6.1.4.1.6876.100.1.0.80602	vmwTimeoutEvent	Kritisch	Zeitüberschreitung bei Datenquelle (Ereignis)	Zeitüberschreitung bei Datenquelle
1.3.6.1.4.1.6876.100.1.0.80603	vmwConnectionRefusedEvent	Kritisch	Verbindung abgelehnt (Ereignis)	Verbindung abgelehnt
1.3.6.1.4.1.6876.100.1.0.80605	vmwIncorrectConnectionStringEvent	Kritisch	Falsche Verbindungszeichenfolge (Ereignis)	Falsche Verbindungszeichenfolge
1.3.6.1.4.1.6876.100.1.0.80606	vmwInvalidCredentialsEvent	Kritisch	Ungültige Anmeldedaten (Ereignis)	Ungültige Anmeldedaten
1.3.6.1.4.1.6876.100.1.0.80608	vmwUnknownHostEvent	Kritisch	Unbekannter Host (Ereignis)	Unbekannter Host
1.3.6.1.4.1.6876.100.1.0.80609	vmwSNMPConnectionInvalidEvent	Kritisch	Ungültiges SNMP-Verbindungsereignis	Ungültige SNMP-Verbindung
1.3.6.1.4.1.6876.100.1.0.80610012	vmwPwAuthModeDisabledAristaEvent	Kritisch	Kennwortauthentifizierung deaktiviert (Ereignis)	Kennwortauthentifizierung deaktiviert
1.3.6.1.4.1.6876.100.1.0.80610018	vmwUnsupportedNSXVersionEvent	Kritisch	Nicht unterstützte NSX-Version (Ereignis)	Nicht unterstützte NSX-Version
1.3.6.1.4.1.6876.100.1.0.80611	vmwFailedCredentialsEncryptEvent	Kritisch	Fehler bei der Verschlüsselung der Anmeldedaten (Ereignis)	Verschlüsselung der Anmeldedaten fehlgeschlagen
1.3.6.1.4.1.6876.100.1.0.80612	vmwPwAuthModeDisabledEvent	Kritisch	Kennwortauthentifizierungsmodus deaktiviert (Ereignis)	Kennwortauthentifizierungsmodus deaktiviert
1.3.6.1.4.1.6876.100.1.0.80613	vmwInsufficientPrivilegesEvent	Kritisch	Nicht genügend Rechte (Ereignis)	Unzureichende Rechte

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.8061313	vmwFlowCollectionErrorEvent	Kritisch	Fehler bei Flow-Erfassung (Ereignis)	Flow-Erfassungsfehler
1.3.6.1.4.1.6876.100.1.0.8061314	vmwAWSThrottlingExceptionEvent	Kritisch	AWS-Einschränkungs Ausnahme (Ereignis)	AWS-Drosselung (Ausnahme)
1.3.6.1.4.1.6876.100.1.0.8061315	vmwAWSFlowLogAccessDeniedExceptionEvent	Kritisch	Zugriff auf AWS-Flow-Protokoll verweigert (Ausnahmeereignis)	Zugriff auf AWS-Flow-Protokoll verweigert (Ausnahme). Dieses Ereignis wird ausgelöst, wenn der Benutzer nicht über die erforderlichen Berechtigungen zum Erfassen von Flow-Protokollen verfügt.
1.3.6.1.4.1.6876.100.1.0.80614	vmwNotFoundEvent	Kritisch	Nicht gefunden (Ereignis)	Nicht gefunden
1.3.6.1.4.1.6876.100.1.0.80616	vmwInvalidConfigEvent	Kritisch	Ungültige Datenquellenkonfiguration (Ereignis)	Ungültige Datenquellenkonfiguration
1.3.6.1.4.1.6876.100.1.0.80617	vmwWarnConfigEvent	Kritisch	Ungültige Datenquellenkonfiguration (Ereignis)	Ungültige Datenquellenkonfiguration
1.3.6.1.4.1.6876.100.1.0.80618	vmwUnexpectedDSTypeOrVersionEvent	Kritisch	Unerwarteter Datenquellentyp oder unerwartete Version (Ereignis)	Unerwartete(r) Datenquellentyp oder -version
1.3.6.1.4.1.6876.100.1.0.80619	vmwNSXControllerNotFoundEvent	Kritisch	NSX Controller nicht gefunden (Ereignis)	NSX Controller nicht gefunden
1.3.6.1.4.1.6876.100.1.0.80620	vmwHostNotReachableEvent	Kritisch	Host nicht erreichbar (Ereignis)	Host nicht erreichbar
1.3.6.1.4.1.6876.100.1.0.80621	vmwInvalidResponseFromDataSourceEvent	Kritisch	Ungültige Antwort von Datenquelle (Ereignis)	Ungültige Antwort von Datenquelle
1.3.6.1.4.1.6876.100.1.0.80622	vmwDataProviderNotRunningEvent	Kritisch	Datenquelle wird nicht ausgeführt (Ereignis)	Datenquelle wird nicht ausgeführt

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80623	vmwPrimaryNSXNotAddedEvent	Kritisch	Primäres NSX-Ereignis nicht hinzugefügt	Primärer NSX nicht hinzugefügt
1.3.6.1.4.1.6876.100.1.0.80624	vmwHostnameResolutionErrorEvent	Kritisch	Hostnamen-Auflösungsfehler (Ereignis)	Hostnamen-Auflösungsfehler
1.3.6.1.4.1.6876.100.1.0.80625	vmwNumVMsOrHostsNotFoundEvent	Kritisch	Anzahl der VMs oder Hosts, die nicht gefunden wurden (Ereignis)	Anzahl der VMs oder Hosts nicht gefunden
1.3.6.1.4.1.6876.100.1.0.80626	vmwNSXIPFIXStatusMismatchEvent	Kritisch	Nichtübereinstimmung bei NSX IPFIX-Status (Ereignis)	Nichtübereinstimmung bei NSX IPFIX-Status
1.3.6.1.4.1.6876.100.1.0.80627	vmwFlowPhysicalNodeEvent	Kritisch	Physischer Flow-Knoten (Ereignis)	Physischer Flow-Knoten
1.3.6.1.4.1.6876.100.1.0.80628	vmwNotEmptyNodeEvent	Kritisch	Knoten nicht leer (Ereignis)	Knoten nicht leer
1.3.6.1.4.1.6876.100.1.0.80629	vmwUnsupportedNSXTVersionEvent	Kritisch	Nicht unterstützte NSX-T-Version (Ereignis)	Nicht unterstützte NSX-T-Version
1.3.6.1.4.1.6876.100.1.0.80630	vmwComputeManagersNotFoundEvent	Kritisch	Berechnungsmanager nicht gefunden (Ereignis)	Berechnungsmanager nicht gefunden
1.3.6.1.4.1.6876.100.1.0.80631	vmwComputeManagersNotAddedEvent	Kritisch	Berechnungsmanager nicht hinzugefügt (Ereignis)	Berechnungsmanager nicht hinzugefügt
1.3.6.1.4.1.6876.100.1.0.80632	vmwUnsupportedLogInsightVersionEvent	Kritisch	Log Insight-Version wird nicht unterstützt (Ereignis)	Log Insight-Version wird nicht unterstützt
1.3.6.1.4.1.6876.100.1.0.80633	vmwUnsupportedVRNIContentPackVersionEvent	Kritisch	Die Version des vRealize Network Insight-Inhaltspakets wird nicht unterstützt (Ereignis)	Die Version des vRealize Network Insight-Inhaltspakets wird nicht unterstützt.
1.3.6.1.4.1.6876.100.1.0.80634	vmwVRNIContentPackNotInstalledEvent	Kritisch	vRealize Network Insight-Inhaltspaket in Log Insight nicht gefunden (Ereignis)	vRealize Network Insight-Inhaltspaket in Log Insight nicht gefunden

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80635	vmwWebhookNotEnabledOnAlertEvent	Kritisch	Webhook ist in einer Network Insight-Warnung nicht aktiviert (Ereignis)	Webhook für eine oder mehrere Warnungen des vRealize Network Insight-Inhaltspakets nicht in Log Insight aktiviert
1.3.6.1.4.1.6876.100.1.0.80636	vmwIncorrectWebhookConfiguredOnAlertEvent	Kritisch	Falsche Webhook-URL für eine Log Insight-Warnung konfiguriert (Ereignis)	Falsche Webhook-Konfiguration für eine oder mehrere Warnungen von vRealize Network Insight-Inhaltspaket in Log Insight gefunden
1.3.6.1.4.1.6876.100.1.0.80637	vmwWebhookNotRunningEvent	Kritisch	Webhook wird auf der Collector-VM (Proxy) nicht ausgeführt (Ereignis)	Webhook wird auf der Collector-VM (Proxy) nicht gestartet
1.3.6.1.4.1.6876.100.1.0.80638	vmwInfobloxRecordLimitExceededEvent	Kritisch	Die Anzahl der Datensätze von Infoblox überschreitet den aktuellen Grenzwert.	Die Anzahl der Datensätze von Infoblox überschreitet den aktuellen Grenzwert.
1.3.6.1.4.1.6876.100.1.0.80639	vmwIncorrectInfobloxCredentialsEvent	Kritisch	Falsche Infoblox-Anmeldedaten (Ereignis)	Infoblox-Anmeldedaten sind ungültig oder der Benutzer verfügt nicht über die „API-Berechtigung“ für den Zugriff auf Infoblox-Daten.
1.3.6.1.4.1.6876.100.1.0.80640	vmwUnsupportedInfobloxVersionEvent	Kritisch	Nicht unterstützte Infoblox-Version (Ereignis)	Die Version von NIOS wird nicht unterstützt.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80641	vmwUnknownInfobloxVersionEvent	Kritisch	Unbekannte Infoblox-Version (Ereignis)	NIOS-Version konnte nicht ermittelt werden.
1.3.6.1.4.1.6876.100.1.0.80642	vmwNoDVSAvailableEvent	Kritisch	IPFIX kann nicht aktiviert werden (Ereignis)	IPFIX kann nicht aktiviert werden, da kein DVS gefunden wurde
1.3.6.1.4.1.6876.100.1.0.80643	vmwVCNotOnSameProxyEvent	Kritisch	NSX Manager und die vCenter-Datenquelle befinden sich nicht auf derselben Collector-VM (Ereignis)	NSX Manager und die verknüpften vCenter-Datenquellen befinden sich nicht auf derselben Collector-VM.
1.3.6.1.4.1.6876.100.1.0.80644	vmwNSXTIPFixNoCollectorProfileEvent	Kritisch	NSX-T IPFIX: Kein Collector-Profil (Ereignis)	NSX-T IPFIX: Kein Collector-Profil
1.3.6.1.4.1.6876.100.1.0.80645	vmwNSXTIPFixNoNewCollectorProfileCanBeAddedEvent	Kritisch	NSX-T IPFIX: Es kann kein neues Collector-Profil hinzugefügt werden (Ereignis)	NSX-T IPFIX: Es kann kein neues Collector-Profil hinzugefügt werden.
1.3.6.1.4.1.6876.100.1.0.80646	vmwNSXTIPFixNoIPFixProfileEvent	Kritisch	NSX-T IPFIX: Kein IPFIX-Profil (Ereignis)	NSX-T IPFIX: Kein IPFIX-Profil
1.3.6.1.4.1.6876.100.1.0.80647	vmwNSXTIPFixIPFixProfilePriorityNotZeroEvent	Kritisch	NSX-T IPFIX: Priorität des IPFIX-Profiles nicht Null (Ereignis)	NSX-T IPFIX: Priorität des IPFIX-Profiles nicht Null
1.3.6.1.4.1.6876.100.1.0.80648	vmwNSXTIPFixCollectorAndIPFixProfileMismatchEvent	Kritisch	NSX-T IPFIX: Collector- und IPFIX-Profil stimmen nicht überein (Ereignis)	NSX-T IPFIX: Nichtübereinstimmung bei Collector-IPFIX-Profil
1.3.6.1.4.1.6876.100.1.0.80649	vmwNSXTIPFixPortIncorrectEvent	Kritisch	NSX-T IPFIX: Collector-Port falsch (Ereignis)	Collector-Port im Collector-Profil ist falsch.
1.3.6.1.4.1.6876.100.1.0.80650	vmwNSXTIPFixDFWStatusNotEnabledEvent	Kritisch	NSX-T-IPFIX: DFW ist nicht aktiviert (Ereignis)	NSX-T-IPFIX: DFW ist nicht aktiviert

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80651	vmwPolicyManagerNoDfwIPFixProfile	Kritisch	Das DFW-IPFIX-Profil ist auf NSX Policy Manager nicht vorhanden. (Ereignis)	DFW-IPFIX-Profil wurde auf NSX Policy Manager nicht gefunden.
1.3.6.1.4.1.6876.100.1.0.80652	vmwPolicyManagerVrniDfwIPFixCollectorAbsent	Kritisch	Die Konfiguration des IPFIX-Collectors für Network Insight ist auf NSX Policy Manager nicht vorhanden. (Ereignis)	Network-Insight-IPFIX-Collector-IP und -Port sind im DFW-IPFIX-Collector-Profil auf NSX Policy Manager nicht vorhanden.
1.3.6.1.4.1.6876.100.1.0.80653	vmwDataSourceIdentificationChangedEvent	Info	Identitätsinformationen für Datenquelle geändert	Die Identitätsinformationen der Datenquelle, wie z. B. das Zertifikat oder der Schlüssel, wurden geändert.
1.3.6.1.4.1.6876.100.1.0.80654	vmwPKSKubernetesUnknownHostEvent	Kritisch	Kubernetes-Cluster-API-Server nicht erreichbar (Ereignis)	Mindestens eine Kubernetes-Konfigurationsdatei eines Kubernetes-Clusters in PKS ist nicht gültig.
1.3.6.1.4.1.6876.100.1.0.80655	vmwKubernetesInsufficientPrivilegesEvent	Kritisch	Kubernetes-Cluster-Dienstknoten verfügen nicht über ausreichende Rechte.	Mindestens ein Kubernetes-Cluster-Dienstkonto verfügt nicht über ausreichende Rechte.
1.3.6.1.4.1.6876.100.1.0.80657	vmwUANIFileNotProvidedEvent	Kritisch	Von der Datenquelle für generische Router und Switches benötigte Datei nicht angegeben	Von der Datenquelle für generische Router und Switches benötigte Datei nicht angegeben

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80658	vmwUANIFileDoesNotExistEvent	Kritisch	Die von der Datenquelle für generische Router und Switches benötigte Datei ist nicht vorhanden	Die von der Datenquelle für generische Router und Switches benötigte Datei ist nicht vorhanden
1.3.6.1.4.1.6876.100.1.0.80659	vmwNSXTLatencyNotEnabledEvent	Kritisch	NSXT_LATENCY_NOT_ENABLED_EVENT	NSX-T-Latenzerfassung ist nicht aktiviert
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	Kritisch	NSXT_LATENCY_COLLECTOR_MISMATCH_EVENT	NSX-T-Latenz-Collector nicht konfiguriert
1.3.6.1.4.1.6876.100.1.0.80663	vmwBigIpInsufficientShellAccessEvent	Kritisch	BIGIP_INSUFFICIENT_SHELL_ACCESS_EVENT	Kein Zugriff auf Shell
1.3.6.1.4.1.6876.100.1.0.80664	vmwBigIpInsufficientPartitionAccessEvent	Kritisch	BIGIP_INSUFFICIENT_PARTITION_ACCESS_EVENT	Unzureichender Partitionszugriff
1.3.6.1.4.1.6876.100.1.0.80665	vmwBigIpInsufficientRoleEvent	Kritisch	BIGIP_INSUFFICIENT_ROLE_EVENT	Unzureichende Rolle
1.3.6.1.4.1.6876.100.1.0.90001	vmwVeloCloudEdgeDownEvent	Warnung	VeloCloud Edge ist nicht fehlerfrei	Edge-Zustand von VeloCloud Edge ist „Nicht verbunden“.
1.3.6.1.4.1.6876.100.1.0.90002	vmwVeloCloudLinkDownEvent	Warnung	VeloCloud-Link ist nicht fehlerfrei	Verbindungsstatus von VeloCloud Edge ist „Nicht verbunden“.
1.3.6.1.4.1.6876.100.1.0.90005	vmwVeloCloudLinkLostPacketEventTx	Kritisch	VeloCloud-Link-Upstream-Paketverlust überschreitet den Schwellenwert.	VeloCloud-Link-Paketverlustereignis Tx.
1.3.6.1.4.1.6876.100.1.0.90007	vmwVeloCloudLinkDegradedVoiceQoeEvent	Kritisch	Sprachqualität von VeloCloud-Link beeinträchtigt.	VeloCloud-Link-Ereignis aufgrund beeinträchtigter Sprachqualität.

OID	Ereignisname	Standardseveregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.90008	vmwVeloCloudLinkDegradedVideoQoeEvent	Kritisch	Videoqualität von VeloCloud-Link beeinträchtigt.	VeloCloud-Link-Ereignis aufgrund beeinträchtigter Videoqualität.
1.3.6.1.4.1.6876.100.1.0.90009	vmwVeloCloudLinkDegradedTransQoeEvent	Kritisch	Transaktionsqualität von VeloCloud-Link beeinträchtigt.	VeloCloud-Link-Ereignis aufgrund beeinträchtigter Transaktionsqualität (Ereignis).
1.3.6.1.4.1.6876.100.1.0.90010	vmwVeloCloudEdgeDegradedVoiceQoeEvent	Kritisch	Sprachqualität von VeloCloud Edge beeinträchtigt.	VeloCloud Edge-Ereignis aufgrund beeinträchtigter Sprachqualität.
1.3.6.1.4.1.6876.100.1.0.90011	vmwVeloCloudEdgeDegradedVideoQoeEvent	Kritisch	Videoqualität von VeloCloud Edge beeinträchtigt.	VeloCloud Edge-Ereignis aufgrund beeinträchtigter Videoqualität.
1.3.6.1.4.1.6876.100.1.0.90012	vmwVeloCloudEdgeDegradedTransQoeEvent	Kritisch	Transaktionsqualität von VeloCloud Edge beeinträchtigt.	VeloCloud Edge-Ereignis aufgrund beeinträchtigter Transaktionsqualität.
1.3.6.1.4.1.6876.100.1.0.90013	vmwVeloCloudLinkLostPacketEventRx	Kritisch	VeloCloud-Link-Downstream-Paketverlust überschreitet den Schwellenwert.	VeloCloud-Link-Paketverlustereignis Rx.

Anzeigen und Bearbeiten von Systemereignissen

Das Ereignis wird entweder vom System oder vom Benutzer definiert. Bei den Systemereignissen handelt es sich um vordefinierte Ereignisse.

Die Systemereignisse werden auf der Seite **Systemereignisse** unter **Einstellungen** aufgeführt. Folgende Felder werden für jedes Ereignis angegeben. Sie können die Informationen basierend auf Ihren Anforderungen in allen folgenden Spalten mit Ausnahme der Spalte „Ereignis“ filtern.

Tabelle 6-2.

Spalte	Beschreibung
Ereignis	Dieses Feld gibt den Namen des Ereignisses an.
Schweregrad	Dieses Feld gibt den Schweregrad des Ereignisses an. Sie können sie auf die folgenden Werte festlegen: <ul style="list-style-type: none"> ■ Kritisch ■ Moderat ■ Warnung ■ Info
Typ	Dieses Feld gibt an, ob das Ereignis auf ein Problem oder eine Änderung hinweist. Hinweis Alle Ereignisse des Typs Problem werden in Syslog protokolliert.
Elemente	Dieses Feld gibt an, dass das Ereignis so konfiguriert ist, dass Einheiten für die Ereignisgenerierung entweder aufgenommen oder ausgeschlossen werden. Standardmäßig ist der Wert <code>ALL</code> .
Benachrichtigungen	Dieses Feld gibt die Benachrichtigungstypen an, die gesendet werden. Die Benachrichtigungen können per E-Mail, SNMP-Trap oder auf beiden Wegen gesendet werden. Hinweis Sie müssen die Benachrichtigung für alle kritischen vom System definierten Ereignisse aktivieren. Um die Liste aller kritischen Systemereignisse zu erhalten, sortieren Sie die Systemereignisse nach Schweregrad.
Aktiviert	Diese Option wird ausgewählt, wenn das Ereignis aktiviert ist.

Wenn Sie mit dem Cursor auf jedes Ereignis zeigen, werden **Weitere Informationen** angezeigt. Durch Klicken auf diese Option werden die Beschreibung, die Ereignis-Tags und der Einheitstyp für dieses Ereignis angezeigt.

Sie können die folgenden Aufgaben für die Systemereignisse durchführen:

- Ein Ereignis bearbeiten
- Massenbearbeitung durchführen
- Ein Ereignis für eine bestimmte Einheit deaktivieren

Bearbeiten der Systemereignisse

Sie können Systemereignisse bearbeiten und Benachrichtigungen für die bevorzugten Systemereignisse definieren.

Verfahren

- 1 Klicken Sie auf das Symbol „Bearbeiten“ neben der Spalte **Aktiviert** für ein bestimmtes Ereignis.
- 2 Bei Bedarf können Sie Ereignis-Tags hinzufügen oder entfernen.
- 3 Ändern Sie den Schweregrad.
- 4 Klicken Sie auf „Einheiten aufnehmen/ausschließen“, wenn das Ereignis für ausgewählte Einheiten aktiviert oder deaktiviert werden soll.
 - So erstellen Sie Aufnahmeregeln:
 - a Wählen Sie **Aufnahmeliste** aus.
 - b Geben Sie die Einheiten an, die Sie für das Ereignis aufnehmen möchten, unter **Bedingungen** ein.
 - So erstellen Sie Ausschlussregeln:
 - a Wählen Sie **Ausschlussliste** aus.
 - b Geben Sie die Einheiten, die Sie für das Ereignis ausschließen möchten, unter **Bedingungen** ein.

Hinweis

- Sie können mehrere Regeln in Aufnahme- und Ausschlusslisten erstellen.
 - Wenn Sie *NSX Manager* auswählen, können Sie in beiden Listen Ausnahmen hinzufügen. Sie können eine Ausnahme definieren, wenn die Aufnahme- oder die Ausschlussregel eine Ausnahme für eine bestimmte Einheit enthalten soll.
 - Sie können auch *Custom Search* angeben, indem Sie Ihre eigene Abfrage schreiben, um Einheiten einzubeziehen oder auszuschließen.
-
- 5 Aktivieren Sie das Kontrollkästchen **Benachrichtigungen aktivieren**, um zu konfigurieren, wann die Benachrichtigungen gesendet werden müssen. Gehen Sie je nach Ihrer Konfiguration folgendermaßen vor:

Option	Aktion
Wenn Sie keinen E-Mail-Server konfiguriert haben	Klicken Sie auf E-Mail-Server konfigurieren . Informationen zum Konfigurieren des E-Mail-Servers finden Sie unter E-Mail-Server konfigurieren .
Wenn Sie kein SNMP-Trap konfiguriert haben	Klicken Sie auf SNMP-Trap konfigurieren . Informationen zum Konfigurieren eines SNMP-Traps finden Sie unter Ziel des SNMP-Traps konfigurieren .
Wenn Sie bereits einen E-Mail-Server konfiguriert haben	Geben Sie die Häufigkeit für den Erhalt von E-Mails im Dropdown-Menü E-Mail-Häufigkeit und die E-Mail-Adresse unter Benachrichtigungs-E-Mails senden an an.
Wenn Sie bereits ein SNMP-Trap konfiguriert haben	Wählen Sie ein oder mehrere SNMP-Trap-Ziel im Dropdown-Menü SNMP-Trap senden an aus. Sie können bis zu vier SNMP-Trap-Ziele auswählen.

6 Klicken Sie auf **Absenden**.

Durchführen einer Massенbearbeitung für ein Ereignis

- 1 Wenn Sie auf der Seite **Systemereignisse** mehrere Ereignisse auswählen, werden die Optionen **Aktivieren**, **Deaktivieren** und **Bearbeiten** oberhalb der Liste angezeigt.
- 2 Klicken Sie auf **Bearbeiten**.
- 3 Auf der Seite **Bearbeiten** haben Sie die folgenden Optionen:
 - **Vorhandene Werte überschreiben:** Bei dieser Option werden nur die Felder, die Sie bearbeiten, überschrieben.
 - **Zu vorhandenen hinzufügen:** Bei dieser Option können Sie zu den vorhandenen Werten wie z. B. E-Mail-Adressen und Ereignis-Tags hinzufügen.
- 4 Klicken Sie auf **Absenden**.

Deaktivieren eines Ereignisses

- 1 Sie können ein Ereignis im Widget **Offene Probleme** auf der Startseite auswählen. Sie können auch **Probleme** in der Suchleiste eingeben und ein Ereignis aus der Liste auswählen.
- 2 Wählen Sie ein bestimmtes Ereignis aus und klicken Sie auf **Archivieren**.
- 3 Wählen Sie **Alle Ereignisse dieses Typs in Zukunft deaktivieren für** und wählen Sie eine Einheit oder alle Einheiten aus.
- 4 Klicken Sie auf **Speichern**.

Hinweis Die Änderungen, die in den Regeln „Schweregrad“, „Tags“ oder „Aufnahme/Ausschluss“ vorgenommen werden, werden in zukünftigen Ereignissen widergespiegelt. Die bestehenden Ereignisse zeigen weiterhin die alte Konfiguration an.

Einschränkungen für Ereignisse

Dieser Abschnitt enthält die Einschränkungen für die diversen vom System definierten Ereignisse.

Regel für die verteilte Firewall durch vorhergehende Regelereignisbeschränkung maskiert

Dieses Ereignis weist die folgenden Beschränkungen auf:

- Dieses Ereignis wird nur für Regeln für verteilte NSX-V-Firewalls unterstützt. Andere Firewallanbieter werden nicht unterstützt.
- Die folgenden Eigenschaften für Firewallregeln werden derzeit für die Ermittlung der Maskierung unterstützt:
 - Quelle
 - Ziel
 - Angewendet auf

- Dienstprotokoll und Portbereiche
- Pakettyt
- Layer-7-Anwendungs-IDs
- Regeln mit Inversion von Quelle oder Ziel werden nicht unterstützt.
- Deaktivierte Regeln werden ignoriert.
- Regeln mit Sicherheitsgruppen, die ausgeschlossene Mitglieder direkt oder indirekt in „Quelle“/„Ziel“ oder „Angewendet auf“ enthalten, werden nicht unterstützt.
- Die Maskierungsermittlung für die Eigenschaften von „Quelle“, „Ziel“ und „Angewendet auf“ basiert auf der statischen Mitgliedschaft und der IP-Bereichsüberlappung der Mitglieder-IPSets. Die dynamische Mitgliedschaft einer Sicherheitsgruppe wird für Maskierungen nicht berücksichtigt.

Bearbeiten von benutzerdefinierten Ereignissen

Die benutzerdefinierten Ereignisse basieren auf der Suche.

Alle benutzerdefinierten Ereignisse werden auf der Seite **Benutzerdefinierte Ereignisse** unter **Einstellungen** aufgeführt. Folgende Felder werden für jedes Ereignis angegeben.

Tabelle 6-3.

Feld	Beschreibung
Name (Suchkriterien)	Dieses Feld gibt den Namen des Ereignisses und die Suchkriterien für das Ereignis an.
Schweregrad	Dieses Feld gibt den Schweregrad der Warnung an. Sie können sie auf die folgenden Werte festlegen: <ul style="list-style-type: none"> ■ Kritisch ■ Moderat ■ Warnung ■ Info
Typ	Dieses Feld gibt an, ob das Ereignis auf ein Problem oder eine Änderung hinweist.
Benachrichtigen, wenn	Dieses Feld gibt an, wann die Benachrichtigung gesendet werden muss.
Erstellt von	Dieses Feld gibt an, wer das Ereignis erstellt hat.
Aktiviert	Diese Option wird ausgewählt, wenn das Ereignis aktiviert ist.

Sie können das Ereignis bearbeiten oder löschen. Während der Bearbeitung können Sie die E-Mail-Adresse und die Häufigkeit der E-Mail-Benachrichtigungen angeben.

Konfigurieren eines benutzerdefinierten Ereignisses

Über die Suche können Sie ein benutzerdefiniertes Ereignis erstellen.

Verfahren

- 1 Klicken Sie im Suchergebnisfenster auf das Benachrichtigungssymbol.
Die Seite „Benutzerdefiniertes Ereignis konfigurieren“ wird geöffnet.
- 2 Geben Sie einen eindeutigen Namen für das Ereignis ein.
- 3 Aktivieren Sie das Kontrollkästchen, um das Ereignis als Problem zu kennzeichnen, und wählen Sie den Schweregrad aus.
- 4 Geben Sie die eindeutigen Suchkriterien ein.
- 5 Die Bedingung auswählen, unter der Sie die Benachrichtigungen erhalten möchten.
- 6 Als Benachrichtigungshäufigkeit können Sie **Sofort** oder **Als tägliche Übersicht** angeben.
- 7 Geben Sie die E-Mail-Adresse an.
- 8 Um den SNMP-Server zu konfigurieren, klicken Sie auf **SNMP-Trap konfigurieren**.
Wenn Sie den SNMP-Server bereits konfiguriert haben, wählen Sie die Option **SNMP-Trap an IP-Adresse senden** aus.
Mit einem Klick auf **Ändern** können Sie die SNMP-Konfiguration ändern.
- 9 Klicken Sie auf **Speichern**.

Anzeigen von Plattformzustandseignissen

Die Seite „Systemzustandseignisse“ ist Ihre Übersichtsseite, um alle Ereignisse anzuzeigen, die Details zum allgemeinen Zustand des Systems bereitstellen. Diese Ereignisse sind möglicherweise auf einer Datenquelle oder einem Knoten in der Infrastruktur aufgetreten. Sie können diese Ereignisse auch über die Suche anzeigen.

Tabelle 6-4.

Feld	Beschreibung
Ereignis	Dieses Feld gibt den Namen des Ereignisses an.
Schweregrad	Dieses Feld gibt den Schweregrad des Ereignisses an. Sie können den Schweregrad des Ereignisses nicht ändern.
Typ	Dieses Feld gibt an, ob das Ereignis auf ein Problem oder eine Änderung hinweist.
Benachrichtigungen	Dieses Feld gibt die Benachrichtigungstypen an, die gesendet werden. Die Benachrichtigungen können per E-Mail, SNMP-Trap oder auf beiden Wegen gesendet werden.

NSX-T-Ereignisse

vRealize Network Insight löst mehrere selbstberechnete NSX-T-Ereignisse aus. Darüber hinaus werden alle von NSX-T generierten Systemereignisse (für NSX-T-Versionen 2.2 bis 2.5) und NSX-T-Alarme (für NSX-T-Version 3.0) auch in vRealize Network Insight sichtbar.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	Warnung	Logischer NSX-T-Ebene-1-Router getrennt (Ereignis)	Der logische NSX-T-Ebene-1-Router ist vom Ebene-0-Router getrennt. Netzwerke unter diesem Router sind von außerhalb nicht erreichbar und umgekehrt.
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	Warnung	Routing-Ankündigung deaktiviert	Die Routing-Ankündigung ist für den logischen NSX-T-Ebene-1-Router deaktiviert. Netzwerke unter diesem Router sind von außerhalb nicht erreichbar.
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	Kritisch	NSX-T Edge-Knoten verfügt über keine Manager-Konnektivität	Manager-Konnektivität des NSX-T Edge-Knotens wurde getrennt.
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	Warnung	Controller-Konnektivität für NSX-T Edge-Knoten herabgestuft	Der NSX-T Edge-Knoten kann nicht mit einem oder mehreren Controllern kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	Kritisch	NSX-T Edge-Knoten verfügt über keine Controller-Konnektivität	Der NSX-T Edge-Knoten ist nicht in der Lage, mit einem der Controller zu kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtumismatchEvent	Warnung	MTU-Nichtübereinstimmung zwischen NSX-T-Ebene-0- und Uplink-Switch/Router	Die auf den Schnittstellen des logischen Tier-0-Routers konfigurierte MTU stimmt nicht mit den Schnittstellen des Uplink-Switch/-Routers aus demselben L2-Netzwerk überein. Dies kann sich auf die Netzwerkleistung auswirken.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	Info	Eine oder mehrere VMs sind von der NSX-T DFW-Firewall ausgeschlossen.	Eine oder mehrere VMs sind nicht durch die NSX-T DFW-Firewall geschützt. vRealize Network Insight erhält keine IPFIX-Flows für diese VMs.
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	Warnung	Fehlkonfiguration des Uplink-VLAN	Die Kommunikation wird unterbrochen, da sich das VLAN auf dem Uplink-Port des Tier-0-Routers vom VLAN auf dem externen Gateway unterscheidet.
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	Warnung	An den Transportknoten ist keine Transportzone angehängt.	Dem Transportknoten wurde keine Transportzone hinzugefügt. Daher verlieren VMs möglicherweise die Konnektivität.
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	Warnung	Kein VTEP auf dem Transportknoten verfügbar.	Alle VTEPs werden aus dem Transportknoten gelöscht. VMs verlieren möglicherweise aus diesem Grund die Konnektivität.
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	Kritisch	Der NSX-T-Controller-Knoten ist nicht mit dem Steuerungscluster verbunden	Der NSX-T-Controller-Knoten hat die Verbindung zum Steuerungscluster verloren.
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	Kritisch	NSX-T-Controller-Knoten ist nicht mit der Managementebene verbunden	Der NSX-T-Controller-Knoten hat die Verbindung zur Managementebene verloren.
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	Kritisch	NSX-T-Verwaltungsknoten ist nicht mit dem Verwaltungscluster verbunden	Der NSX-T-Verwaltungsknoten hat die Verbindung zum Verwaltungscluster verloren.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	Warnung	NSX-T-Hostknoten verfügt über keine Manager-Konnektivität	Desynchronisierung des Konnektivitätsstatus von NSX Manager mit Hosttransportknoten
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	Kritisch	Controller-Konnektivität für NSX-T Edge-Knoten ist „Unbekannt“.	Die Controller-Konnektivität des NSX-T Edge-Knotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	Warnung	NSX-T-Hostknoten verfügt über keine Controller-Konnektivität	Der NSX-T-Hostknoten ist nicht in der Lage, mit einem der Controller zu kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	Warnung	Controller-Konnektivität für NSX-T-Hostknoten herabgestuft	Der NSX-T-Hostknoten kann nicht mit einem oder mehreren Controllern kommunizieren.
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	Warnung	Controller-Konnektivität für NSX-T-Hostknoten ist „Unbekannt“.	Die Controller-Konnektivität des NSX-T-Hostknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	Warnung	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der pNIC-Status des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	Kritisch	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der pNIC-Status des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	Warnung	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der Tunnelstatus des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradeEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	Kritisch	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der Tunnelstatus des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.	Der Status des NSX-T-Host-Transportknotens ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.	Der Status des NSX-T-Host-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	Warnung	Der Status des NSX-T-Host-Transportknotens ist „Unbekannt“.	Der Status des NSX-T-Host-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.	Der Status des NSX-T Edge-Transportknotens ist „Nicht verfügbar“.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.	Der Status des NSX-T Edge-Transportknotens ist „Beeinträchtigt“.
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	Kritisch	Der Status des NSX-T Edge-Transportknotens ist „Unbekannt“.	Der Status des NSX-T Edge-Transportknotens ist „Unbekannt“.
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	Warnung	Der Administratorstatus des logischen NSX-T-Switches ist „Nicht verfügbar“.	Der Administratorstatus des logischen NSX-T-Switches ist „Nicht verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	Kritisch	Der Betriebsstatus des logischen NSX-T-Ports ist „Nicht verfügbar“.	Der Betriebsstatus des logischen NSX-T-Ports ist „Nicht verfügbar“. Dies kann zu einem Kommunikationsfehler zwischen zwei virtuellen Schnittstellen (VIFs) führen, die mit demselben logischen Switch verbunden sind, z. B. können Sie eine VM nicht von einer anderen Maschine aus anpingen.
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	Warnung	Der Betriebsstatus des logischen NSX-T-Ports ist „Unbekannt“.	Der Betriebsstatus des logischen NSX-T-Ports ist „Unbekannt“. Dies kann zu einem Kommunikationsfehler zwischen zwei virtuellen Schnittstellen (VIFs) führen, die mit demselben logischen Switch verbunden sind, z. B. können Sie eine VM nicht von einer anderen Maschine aus anpingen.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	Warnung	Verbindungsstatus von NSX-T-Berechnungsmanager ist nicht „Verfügbar“.	Verbindungsstatus von NSX-T-Berechnungsmanager ist nicht „Verfügbar“.
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackUpDisabledEvent	Warnung	NSX-T Manager-Sicherung ist nicht geplant.	NSX-T Manager-Sicherung ist nicht geplant.
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	Kritisch	Die NSX-T DFW-Firewall ist deaktiviert.	Die verteilte Firewall ist im NSX-T Manager deaktiviert.
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	Warnung	Vom logischen NSX-T-Port empfangene Pakete gehen verloren.	Empfangene Pakete gehen auf dem logischen NSX-T-Port verloren und zugehörige Einheiten werden möglicherweise davon betroffen.
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	Warnung	Vom logischen NSX-T-Port übertragene Pakete gehen verloren.	Übertragene Pakete gehen auf dem logischen NSX-T-Port verloren, und zugehörige Einheiten werden möglicherweise davon betroffen.
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	Warnung	Vom logischen NSX-T-Switch empfangene Pakete gehen verloren.	Empfangene Pakete gehen auf dem logischen NSX-T-Switch verloren, und zugehörige Einheiten werden möglicherweise davon betroffen.
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	Warnung	Vom logischen NSX-T-Switch übertragene Pakete gehen verloren.	Übertragene Pakete gehen auf dem logischen NSX-T-Switch verloren, und zugehörige Einheiten werden möglicherweise davon betroffen.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	Warnung	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren.	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren. Dies kann sich auf den Netzwerkdatenverkehr im Zusammenhang mit dem NSX-T-Verwaltungscluster auswirken.
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	Kritisch	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren. Dies kann sich auf den Edge-Cluster-Netzwerkdatenverkehr auswirken.
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	Warnung	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren	Empfangene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren. Dies kann sich auf den Netzwerkdatenverkehr auf ESXi-Hosts auswirken.
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	Warnung	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Verwaltungsknotens verloren. Dies kann sich auf den Netzwerkdatenverkehr im Zusammenhang mit dem NSX-T-Verwaltungscluster auswirken.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	Kritisch	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T Edge-Knotens verloren. Dies kann sich auf den Edge-Cluster-Netzwerkdatenverkehr auswirken.
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	Warnung	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren	Übertragene Pakete gehen an der Netzwerkschnittstelle des NSX-T-Host-Knotens verloren. Dies kann sich auf den Netzwerkdatenverkehr auf ESXi-Hosts auswirken.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmlInventoryStatusEvent	Warnung	Die Ausführung des CM-Bestandsdiensts wurde beendet	Der Status des CM-Bestandsdiensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	Warnung	Die Ausführung des Controller-Diensts wurde beendet.	Der Status des Controller-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	Warnung	Die Ausführung des DataStore-Diensts wurde beendet.	Der Status des DataStore-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	Warnung	Die Ausführung des HTTP-Diensts wurde beendet.	Der Status des HTTP-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	Warnung	Die Ausführung des Diensts für die Installation von Upgrades wurde beendet.	Der Status des Diensts für die Installation von Upgrades wurde in „Angehalten“ geändert.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	Warnung	Die Ausführung des liagent-Diensts wurde beendet.	Der Status des liagent-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	Warnung	Die Ausführung des Manager-Diensts wurde beendet.	Der Status des Manager-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Warnung	Die Ausführung des Management Plane-Diensts wurde beendet.	Der Status des Management Plane-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Warnung	Die Ausführung des Migrationskoordinator-Diensts wurde beendet.	Der Status des Migrationskoordinator-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	Warnung	Die Ausführung des Knotenverwaltungsdiens wurde beendet.	Der Status des Knotenverwaltungsdiens wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	Warnung	Die Ausführung des Knotenstatistikdiensts wurde beendet.	Der Status des Knotenstatistikdiensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	Warnung	Die Ausführung des Nachrichtenbus-Diensts wurde beendet.	Der Status des Nachrichtenbus-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	Warnung	Die Ausführung des Plattform-Client-Diensts wurde beendet.	Der Status des Plattform-Client-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	Warnung	Die Ausführung des Upgrade-Agent-Diensts wurde beendet.	Der Status des Upgrade-Diensts wurde in „Angehalten“ geändert.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	Warnung	Die Ausführung des NTP-Diensts wurde beendet.	Der Status des NTP-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	Warnung	Die Ausführung des Richtliniendienstes wurde beendet.	Der Status des Richtliniendienstes wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	Warnung	Die Ausführung des Suchdiensts wurde beendet.	Der Status des Suchdiensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	Warnung	Die Ausführung des SNMP-Diensts wurde beendet.	Der Status des SNMP-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	Warnung	Die Ausführung des SSH-Diensts wurde beendet.	Der Status des SSH-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	Warnung	Die Ausführung des Syslog-Diensts wurde beendet.	Der Status des Syslog-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	Warnung	Die Ausführung des Telemetriedienstes wurde beendet.	Der Status des Telemetriedienstes wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	Warnung	Die Ausführung des UI-Diensts wurde beendet.	Der Status des UI-Diensts wurde in „Angehalten“ geändert.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmInventoryStatusEvent	Kritisch	CM-Bestandsdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der CM-Inventory-Dienst, wird nicht mehr ausgeführt.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	Kritisch	Controller-Dienst wurde beendet	Einer der Dienste des NSX-T Verwaltungsknotens, nämlich der Controller-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	Kritisch	DataStore-Dienst wurde beendet	Einer der Dienste des NSX-T Verwaltungsknotens, nämlich der DataStore-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	Kritisch	HTTP-Dienst wurde beendet	Einer der Dienste des NSX-T Verwaltungsknotens, nämlich der HTTP-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	Warnung	Dienst für die Installation von Upgrades wurde beendet	Einer der Dienste des NSX-T Verwaltungsknotens, nämlich der Dienst für die Installation von Upgrades, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	Warnung	liagent-Dienst wurde beendet	Einer der Dienste des NSX-T Verwaltungsknotens, nämlich der LI-Agent-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	Kritisch	Manager-Dienst wurde beendet	Einer der Dienste des NSX-T Verwaltungsknotens, nämlich Managerdienst, wird nicht mehr ausgeführt.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Warnung	Management Plane-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Busdienst der Verwaltungsebene, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Warnung	Migrationskoordinatordienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Migrationskoordinatordienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	Kritisch	Knotenverwaltungsdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Knotenverwaltungsdienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	Kritisch	Knotenstatistikdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich die Knotenstatistik, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeServiceNSXMessageBusStatusEvent	Warnung	Nachrichtenbusdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Nachrichtenbusdienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	Kritisch	Plattform-Client-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Platform Client Service, wird nicht mehr ausgeführt.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	Warnung	Upgrade-Agent-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich Upgrade-Agent-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	Kritisch	NTP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der NTP-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	Kritisch	Richtliniendienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Richtliniendienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	Kritisch	Suchdienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Suchdienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	Warnung	SNMP-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der SNMP-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	Kritisch	SSH-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der SSH-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	Kritisch	Syslog-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Syslog-Dienst, wird nicht mehr ausgeführt.

Tabelle 6-5. Von vRealize Network Insight berechnete NSX-T-Ereignisse (Fortsetzung)

OID	Ereignisname	Standardschweregrad	Benutzeroberflächenname	Beschreibung
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	Warnung	Telemetriedienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Telemetrie-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	Kritisch	UI-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der UI-Dienst, wird nicht mehr ausgeführt.
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeServiceClusterManagerStatusEvent	Kritisch	Cluster Manager-Dienst wurde beendet	Einer der Dienste des NSX-T-Verwaltungsknotens, nämlich der Clustermanager-Dienst, wird nicht mehr ausgeführt.

NSX-T-Systemereignisse

Die folgenden Ereignisse von NSX-T 2.2 bis 2.5 werden in vRealize Network Insight unterstützt. Die Objekt-ID (OID) für all diese NSX-T-Systemereignisse lautet

1.3.6.1.4.1.6876.100.1.0.80203.

Tabelle 6-6. NSX-T-Systemereignisse

Ereignisname	Beschreibung
vmwNSXPlatformSysCpuUsage	CPU-Auslastung auf Manager- und Edge-Appliances (NSX-T 2.2)
vmwNSXPlatformSysDiskUsage	Festplattenspeichernutzung auf Manager- und Edge-Appliance für Partition „/var/log“ (NSX-T 2.2)
vmwNSXPlatformSysMemUsage	Arbeitsspeichernutzung auf Manager- und Edge-Appliance (NSX-T 2.2)
vmwNSXPlatformSysConfigDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/config“ (NSX-T 2.4)
vmwNSXPlatformSysVarDumpDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/var/dump“ (NSX-T 2.5)
vmwNSXPlatformSysRepositoryDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/repository“ (NSX-T 2.5)
vmwNSXPlatformSysRootDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/root“ (NSX-T 2.5)

Tabelle 6-6. NSX-T-Systemereignisse (Fortsetzung)

Ereignisname	Beschreibung
vmwNSXPlatformSysTmpDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/tmp“ (NSX-T 2.5)
vmwNSXPlatformSysImageDiskUsage	Festplattennutzung auf Manager- und Edge-Appliances für die Partition „/image“ (NSX-T 2.5)
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP-Pool überlastet/normal (NSX-T 2.5)
vmwNSXDhcpPoolLeaseAllocationFailedEvent	Lease-Zuteilung für DHCP-Pool fehlgeschlagen/erfolgreich (NSX-T 2.5)
vmwNSXPlatformPasswordExpiryStatus	Kennwortablauf für Manager (NSX-T 2.4)
vmwNSXPlatformCertificateExpiryStatus	Zertifikatsablauf für Manager (NSX-T 2.4)
vmwNSXRoutingBgpNeighborStatus	BGP-Nachbarstatus (NSX-T 2.2)
vmwNSXVpnTunnelState	VPN-Tunnel aktiv/inaktiv (NSX-T 2.2)
vmwNSXVpnL2TunnelStatus	L2 VPN-Sitzung aktiv/inaktiv (NSX-T 2.2)
vmwNSXVpnIkeSessionStatus	IKE-Sitzung aktiv/inaktiv (NSX-T 2.2)
vmwNSXDnsForwarderStatus	DNS-Weiterleitungsstatus (NSX-T 2.4)
vmwNSXClusterNodeStatus	Cluster-Knotenstatus (NSX-T 2.4)
vmwNSXFabricCryptoStatus	Edge Crypto MUX-Treiber hat Known_Answer_Tests(KAT) bestanden/nicht bestanden (NSX-T 2.4)
Manager-Festplattennutzung ist nicht OK	
BGP-Nachbar nicht verfügbar	Eine Warnung ist erforderlich, wenn der BGP-Nachbar nicht verfügbar ist.
BGP-Nachbar verfügbar	Alarm löschen, wenn ein Nachbar zur Verfügung steht.
Speichernutzung über X	Alarm für Speicher über X – Ereignis wird für alle Appliance-VMs (MP, CCP) oder Transportknoten (Edge, Host) ausgelöst.
Arbeitsspeichernutzung über X	Alarm für Arbeitsspeicher über X – Ereignis wird für alle Appliance-VMs (MP, CCP) oder Transportknoten (Edge, Host) ausgelöst.
CPU-Nutzung über X	Alarm für CPU über X – Ereignis wird für alle Appliance-VMs (MP, CCP) oder Transportknoten (Edge, Host) ausgelöst.

NSX-T-Systemalarne

Hinweis Zusätzlich zu diesen Ereignissen werden alle NSX-T 3.0-Alarne als NSX-T-Systemereignisse in vRealize Network Insight 5.2 und höher angezeigt. Sie können die vollständige Liste der von NSX-T generierten Alarne unter https://NSX-T_IP_Address/nsx/#/app/home/alarms/alarm-definitions anzeigen.

Kubernetes-Ereignisse

Die folgenden Kubernetes-Ereignisse werden in vRealize Network Insight unterstützt. Die Objekt-ID (OID) für alle Kubernetes-Ereignisse lautet 1.3.6.1.4.1.6876.100.1.0.1510.

Ereignisname	Schweregrad	Beschreibung
FailedToCreateContainer	Kritisch	Fehler beim Erstellen des Containers
FailedToStartContainer	Kritisch	Fehler beim Starten des Containers
PreemptContainer	Warnung	Andere Pods werden getrennt.
BackOffStartContainer	Warnung	Der Back-Off-Neustart des Containers ist fehlgeschlagen.
ExceededGracePeriod	Warnung	Die Container-Laufzeit hat den Pod innerhalb des angegebenen Kulanzeitraums nicht angehalten.
FailedToKillPod	Warnung	Ein Pod konnte nicht angehalten werden.
FailedToCreatePodContainer	Moderat	Fehler beim Erstellen eines Pod-Containers.
FailedToMakePodDataDirectories	Moderat	Fehler beim Erstellen der Pod-Datenverzeichnisse.
NetworkNotReady	Warnung Kritisch	Netzwerk ist nicht bereit.
FailedScheduling	Kritisch	Pod kann nicht geplant werden
FailedToPullImage	Warnung Kritisch	Das Image konnte nicht abgerufen werden.
FailedToInspectImage	Warnung	Das Image konnte nicht überprüft werden.
ErrImageNeverPullPolicy	Warnung	Die NeverPull-Richtlinie des Images wird verletzt.
ImagePullBackOff	Kritisch	Fehler beim Abrufen des Container-Images, Kubelet sichert Image-Pull
ImageInspectError	Warnung	Image kann nicht überprüft werden
ErrImagePull	Kritisch	Image-Pull-Fehler
ErrImageNeverPull	Kritisch	Das erforderliche Image ist auf dem Host nicht vorhanden und PullPolicy ist NeverPullImage
RegistryUnavailable	Kritisch	HTTP-Fehler beim Abrufen des Images aus der Registrierung
InvalidImageName	Kritisch	Der Image-Name kann nicht analysiert werden

Ereignisname	Schweregrad	Beschreibung
KubeletSetupFailed	Moderat	Kubelet-Setup fehlgeschlagen.
FailedAttachVolume	Kritisch	Fehler beim Anhängen des Volumes.
FailedMountVolume	Kritisch	Fehler beim Mounten des Volumes.
VolumeResizeFailed	Warnung	Fehler beim Erweitern/Reduzieren des Volumes.
FileSystemResizeFailed	Warnung	Fehler beim Erweitern/Reduzieren des Dateisystems.
FailedMapVolume	Kritisch	Fehler beim Zuordnen eines Volumes.
WarnAlreadyMountedVolume	Warnung	Das Volume wurde bereits gemountet.
ContainerGCFailed	Warnung	Garbage Collection des Containers fehlgeschlagen.
ImageGCFailed	Warnung	Garbage Collection des Images fehlgeschlagen.
FailedNodeAllocatableEnforcement	Warnung	Vom System reservierter Cgroup-Grenzwert konnte nicht erzwungen werden.
FailedCreatePodSandBox	Warnung	Fehler beim Erstellen der Pod-Sandbox.
FailedStatusPodSandBox	Warnung	Fehler beim Pod-Sandbox-Status.
InvalidDiskCapacity	Moderat	Ungültige Festplattenkapazität.
FreeDiskSpaceFailed	Moderat	Freigabe von Festplattenspeicher fehlgeschlagen.
ContainerUnhealthy	Kritisch	Container ist fehlerhaft.
ContainerProbeWarning	Warnung	Container-Test erfolgreich mit einer Warnung.
FailedSync	Warnung	Pod-Synchronisierung fehlgeschlagen.
FailedValidation	Warnung	Fehler bei der Validierung der Pod-Konfiguration.
FailedPostStartHook	Warnung	Handler für Pod-Start fehlgeschlagen.
FailedPreStopHook	Warnung	Handler für Pre-Stop fehlgeschlagen.
NodeNotReady	Kritisch	Knoten ist nicht bereit.
NodeNotSchedulable	Kritisch	Knoten ist nicht planbar.
NodeRebooted	Moderat	Knoten neu gestartet.

Benachrichtigungen

Suchbasierte Benachrichtigungen

Die suchbasierten Benachrichtigungen können wie folgt kategorisiert werden:

- Systembasierte Benachrichtigung

■ Benutzerdefinierte Benachrichtigung

Systembasierte Benachrichtigungsparameter sind vordefiniert, und die Benachrichtigungen in Form von E-Mails werden beim Aktivieren der Benachrichtigungswarnung gesendet. Benutzerdefinierte Benachrichtigungen werden von Benutzern basierend auf ihren Anforderungen festgelegt. Sie können E-Mail-Benachrichtigungen basierend auf Ihrer Suchabfrage erstellen. Nachdem Sie eine Suche ausgeführt haben, wird auf der Seite „Ergebnisse“ die Option **Benachrichtigung erstellen** angezeigt. Für jede Suche können Sie:

- Die Bedingung auswählen, unter der Sie die Benachrichtigungen erhalten möchten.
- Festlegen, wie häufig die Benachrichtigungen empfangen werden sollen.
- Geben Sie die E-Mail-Empfänger für jede Benachrichtigung ein (standardmäßig ist Ihre E-Mail-ID in der Empfängerliste enthalten; Sie können auch mehrere E-Mail-IDs hinzufügen).

Für eine benutzerdefinierte Suche:

- Es ist zwingend erforderlich, dass Sie der suchbasierten Benachrichtigung einen Namen zuweisen.
- Es ist zwingend erforderlich, den Schweregrad eines suchbasierten Ereignisses auszuwählen, das als Problem markiert ist.
- Die benutzerdefinierten Ereignisse werden durch die Suchkriterien eindeutig identifiziert.
- Sie können die Benachrichtigungshäufigkeit als **Sofort** oder **Als tägliche Übersicht** angeben.

Sie können Ihre Benachrichtigungen über die Seite **Einstellungen > Suchbasierte Benachrichtigungen** verwalten. Auf der Seite **Suchbasierte Benachrichtigungen** können Sie die vorhandenen Benachrichtigungen anzeigen, bearbeiten, aktivieren oder deaktivieren und unerwünschte Benachrichtigungen löschen.

Konfigurieren der Ereignisbenachrichtigung

Die Benachrichtigungen werden in Form von E-Mails gesendet.

Um eine Benachrichtigung einzurichten, müssen Sie zuerst den Mailserver konfigurieren. Informationen zum Konfigurieren des Mailservers finden Sie unter [E-Mail-Server konfigurieren](#).

Angeben von Benachrichtigungsereignissen für E-Mails, die gesendet werden sollen

Benutzer können Ereignisse angeben, für die E-Mail-Benachrichtigungen gesendet werden sollen.

Angeben der Ereignisse

- 1 Klicken Sie auf der Seite **Einstellungen** auf **Suchbasierte Benachrichtigungen** oder suchen Sie einfach im Suchfeld nach Informationen.
- 2 Klicken Sie auf der Seite „Suchbasierte Benachrichtigungen“ auf das Symbol **Benachrichtigung erstellen**. Ein Benachrichtigungsdialogfeld wird angezeigt.
- 3 Wählen Sie im Feld **Benachrichtigung empfangen bei** das Ereignis aus, bei dem die Benachrichtigungen gesendet werden sollen.

- 4 Wählen Sie im Feld **Benachrichtigen** die Häufigkeit aus, mit der die Benachrichtigungen gesendet werden sollen.
- 5 Wenn das Ereignis nicht erwünscht ist, aktivieren Sie das Kontrollkästchen **Als Problem markieren**.
- 6 Geben Sie die E-Mail-Adressen ein, an die die Benachrichtigungen gesendet werden sollen, und klicken Sie anschließend auf **Speichern**.

Hinweis Um zu überprüfen, ob die Benachrichtigungs-E-Mail ordnungsgemäß eingerichtet ist, klicken Sie auf **Test-E-Mail senden**.

Ereignisbenachrichtigungen

vRealize Network Insight enthält eine Liste vordefinierter Systemereignisse (Systemprobleme und Systemänderungen), für die Sie alle vier Stunden automatische E-Mail-Benachrichtigungen erhalten können. Sie können diese Einstellungen ändern.

Sie können die Liste der Benachrichtigungen auf der Seite **Einstellungen > Systembenachrichtigungen** anzeigen.

Hinweis Ein Admin-Benutzer kann die abonnierten Plattformen und Systemereignisse eines anderen Admin-Benutzers oder Mitglied-Benutzers nicht sehen.

Wenn Sie keine E-Mail- oder SNMP-Benachrichtigungen für ein Ereignis konfiguriert haben, wird auf der Startseite eine Warnmeldung angezeigt, die Sie daran erinnert und über die Sie Benachrichtigungen definieren können. Sie können in der Warnmeldung auf **Benachrichtigungen aktivieren** klicken, um direkt zur Seite „Systemereignisse“ zu navigieren und Benachrichtigungen für die bevorzugten Ereignisse zu abonnieren.

Um die Erinnerung zu deaktivieren, wählen Sie die Option **Diese Meldung nicht mehr anzeigen** aus. Die Warnmeldung wird für den betreffenden Benutzer nicht angezeigt. Um Benachrichtigungen zu einem späteren Zeitpunkt zu definieren, navigieren Sie zu **Einstellungen > Ereignisse**.

Archivieren von Problemen

Archivieren eines Problems

- 1 Klicken Sie auf den Link „Alle anzeigen“ (falls mehr als eine Instanz eines Ereignisses vorhanden ist), um alle Instanzen des Ereignisses anzuzeigen.
- 2 Bewegen Sie den Mauszeiger über die Instanz des Ereignisses, das Sie archivieren möchten, um einen Satz von Symbolen anzuzeigen, und klicken Sie dann auf das Symbol „Archiv“.
- 3 Im ereignisspezifischen Dialogfeld
 - a Wählen Sie dieses Ereignis aus der Liste „Sie sind im Begriff zu archivieren“, wenn Sie nur dieses Ereignis archivieren möchten.

- b Wählen Sie „Alle Ereignisse dieses Typs“ aus der Liste „Sie sind im Begriff zu archivieren“ aus, wenn Sie alle Ereignisse desselben Typs im System archivieren möchten.

4 Klicken Sie auf **Speichern**.

Anzeigen aller archivierten Ereignisse

- 1 Geben Sie auf der Startseite „Ereignisse“ in das Suchfeld ein und drücken Sie **Eingabe**. Es wird eine Liste der Ereignisse angezeigt.
- 2 Aktivieren Sie im linken Fensterbereich, im Facet „Archiviert“, das Kontrollkästchen „Wahr“ (im Screenshot unten hervorgehoben).

Sie können alle archivierten Ereignisse hier anzeigen.

Wiederherstellen eines archivierten Ereignisses

- 1 Klicken Sie im archivierten Ereignis auf das Symbol „Archiviert“. (Weitere Informationen zum Wechseln auf die Seite „Archivierte Ereignisse“ finden Sie im vorherigen Abschnitt „Anzeigen eines archivierten Ereignisses“).
- 2 Im ereignisspezifischen Dialogfeld
 - a Wählen Sie dieses Ereignis aus der Liste „Sie sind im Begriff wiederherzustellen“, wenn Sie nur dieses Ereignis wiederherstellen möchten.
 - b Wählen Sie „Alle Ereignisse dieses Typs“ aus der Liste „Sie sind im Begriff wiederherzustellen“ aus, wenn Sie alle Ereignisse desselben Typs wiederherstellen möchten.
 - c Klicken Sie auf „Speichern“, um die Wiederherstellung abzuschließen.

Deaktivieren von Ereignissen

Benutzer können Ereignisse selektiv deaktivieren und verhindern, dass Benachrichtigungen zukünftig gesendet werden.

Deaktivieren von Ereignisbenachrichtigungen

Methode 1

- 1 Klicken Sie in dem Ereignis auf den Link **Alle anzeigen** (falls mehr als eine Instanz eines Ereignisses vorhanden ist), um alle Instanzen des Ereignisses anzuzeigen.
- 2 Bewegen Sie den Mauszeiger über die Instanz des Ereignisses, dessen Benachrichtigung Sie deaktivieren möchten. Es wird ein Satz von Symbolen angezeigt, klicken Sie auf das Archivsymbol.
- 3 Aktivieren Sie im Dialogfeld „Ereignisspezifisch“ das Kontrollkästchen **Alle Ereignisse dieses Typs in Zukunft deaktivieren** und klicken Sie dann auf **Speichern**.

Methode 2

- 1 Klicken Sie in der oberen rechten Ecke der **Startseite** auf das Symbol **Profil** und anschließend auf **Einstellungen**.

- 2 Klicken Sie im Abschnitt **Einstellungen** auf **Ereignisbenachrichtigungen**, um eine Liste aller aktivierten und deaktivierten Ereignisse anzuzeigen.
- 3 Klicken Sie auf dem aktivierten Ereignis, das Sie deaktivieren möchten, in der Spalte **Aktiviert** auf den linken Bereich des entsprechenden Schiebereglers.
- 4 Klicken Sie im Dialogfeld **Aktion bestätigen** auf **Ja**.

Konfigurieren des Ereignisbenachrichtigungsdiensts

Benutzer können Kundenbenachrichtigungen für verschiedene Ereignisse aktivieren.

Einrichten der Benachrichtigungsdienste

- 1 Wechseln Sie unter „Einstellungen“ zu „Ereignisbenachrichtigung“ und klicken Sie auf das Symbol „Bearbeiten“, das dem Problem entspricht, für das Sie E-Mail-Benachrichtigungen und SNMP aktivieren möchten.
- 2 Geben Sie im Dialogfeld „Systembenachrichtigung bearbeiten“ die E-Mail-Adresse ein, an die die E-Mail-Benachrichtigung gesendet werden soll. Wählen Sie im Feld „E-Mail-Häufigkeit“ die Häufigkeit aus, in der Sie Benachrichtigungen erhalten möchten.
- 3 Aktivieren Sie das Kontrollkästchen „SNMP-Trap für dieses Ereignis aktivieren“, um SNMP-Benachrichtigungen einzurichten.
- 4 Klicken Sie auf **Speichern**.
- 5 Nach erfolgreicher Aktivierung werden die entsprechenden Mail- und SNMP-Symbole angezeigt, wie im folgenden Screenshot hervorgehoben.

Konfigurieren der Identitäts- und Zugriffsverwaltung

In vRealize Network Insight können Sie einen Benutzer erstellen oder den Zugriff von LDAP-Benutzern und VMware Identity Manager-Benutzern konfigurieren. Sie können den Benutzern auch verschiedene Rollen zuweisen.

Konfigurieren der Benutzerverwaltung

vRealize Network Insight unterstützt drei Typen von Benutzerrollen für einen Benutzer. Benutzer können entsprechend den ihnen zugewiesenen Rollen auf vRealize Network Insight-Funktionen zugreifen.

- **Administrator:** Ein Administrator hat vollständigen Zugriff.
- **Mitglied:** Ein Mitglied hat eingeschränkten Zugriff.
- **Auditor:** Ein Auditor hat nur Lesezugriff und ist von allen Erstellungs-, Hinzufügungs-, Bearbeitungs- oder Löschaktionen ausgeschlossen. Benutzer können nur den Zustand anzeigen.

Tabelle 6-7. Unterstützte Funktionen für jede Rolle

Seite	Aktionen	Administrator
[Einstellungen] Protokolle: Überwachungsprotokolle	Anzeigen: Seite/Registerkarte „Überwachungsprotokolle“	Zulässig
	Aktivieren/Deaktivieren: Personenbezogene Daten	Zulässig
	Anzeigen/Filtern: Überwachungsprotokolle	Zulässig
	Als CSV exportieren	Zulässig
[Einstellungen] Protokolle: Syslog-Konfiguration	Anzeigen: Seite/Registerkarte „Syslog-Konfiguration“	Zulässig
	Syslog aktivieren/deaktivieren	Zulässig
	Hinzufügen: Syslog-Server	Zulässig
	Bearbeiten/Löschen: Syslog-Server	Zulässig
	Anzeigen: Syslog-Server	Zulässig
	Anzeigen: Quellserverzuordnung	Zulässig
	Bearbeiten: Quellserverzuordnung	Zulässig
[Einstellungen] Info über	Anzeigen von Details zum Produkt (Name, Version, Service-Tag)	Zulässig
[Einstellungen] Systemkonfiguration	Anzeigen: Seite/Registerkarte „Systemkonfiguration“	Zulässig
	Anzeigen: Zeitüberschreitung der Benutzersitzung	Zulässig
	Bearbeiten: Zeitüberschreitung der Benutzersitzung	Zulässig
	Anzeigen: Validierung von Datenquellenzertifikaten	Zulässig
	Bearbeiten: Validierung von Datenquellenzertifikaten	Zulässig
	Anzeigen: Google Maps-API-Schlüssel	Zulässig
	Bearbeiten: Google Maps-API-Schlüssel	Zulässig
[Einstellungen] Meine Einstellungen	Anzeigen/Bearbeiten: Meine Einstellungen	Zulässig
[Einstellungen] Lizenz und Nutzung	Anzeigen: Seite/Registerkarte „Lizenz und Nutzung“	Zulässig

Tabelle 6-7. Unterstützte Funktionen für jede Rolle (Fortsetzung)

Seite	Aktionen	Administrator
	Anzeigen: Lizenzdetails	Zulässig
	Hinzufügen/Validieren: Lizenzschlüssel	Zulässig
	Löschen: Lizenzschlüssel	Zulässig
	Option: „Möchten Sie die Datenquellen verwalten?“	Zulässig
	Option (Link zur Seite „Konten und Datenquellen“): „Datenquelle hinzufügen, um die aktuelle Nutzung anzuzeigen“	Zulässig
[Einstellungen] SNMP-Trap-Ziele	Anzeigen: Seite/Registerkarte „SNMP-Trap-Ziel“	Zulässig
	Anzeigen: Liste der vorhandenen SNMP-Ziele (mit konfigurierter Anzahl der Ereignisse)	Zulässig
	Anzeigen: Liste der für jedes SNMP-Ziel konfigurierten Ereignisse	Zulässig
	Hinzufügen/Bearbeiten/Löschen/Migrieren/Send-TestTRAP: SNMP-Ziele	Zulässig
[Einstellungen] E-Mail-Server	Anzeigen: Seite/Registerkarte „E-Mail-Server“	Zulässig
	Anzeigen: Vorhandene Konfiguration des E-Mail-Servers	Zulässig
	Hinzufügen/Bearbeiten/Löschen: E-Mail-Serverkonfiguration	Zulässig
	Test-E-Mail senden	Zulässig
[Einstellungen] Identitäts- und Zugriffsverwaltung	Anzeigen: Seite/Registerkarte „Identitäts- und Zugriffsverwaltung“	Zulässig
[Einstellungen] Identitäts- und Zugriffsverwaltung: LDAP	Anzeigen: Seite/Registerkarte „LDAP“	Zulässig
	Anzeigen: Vorhandene Konfiguration für LDAP	Zulässig
	Hinzufügen/Bearbeiten/Löschen: LDAP-Konfiguration	Zulässig
[Einstellungen] Identitäts- und Zugriffsverwaltung: VIDM	Anzeigen: Seite/Registerkarte „VIDM“	Zulässig
	Anzeigen: Vorhandene Konfiguration für VIDM	Zulässig

Tabelle 6-7. Unterstützte Funktionen für jede Rolle (Fortsetzung)

Seite	Aktionen	Administrator
	Hinzufügen/Bearbeiten/Löschen: VIDM-Konfiguration	Zulässig
	Umschalten: VIDM-Konfiguration	Zulässig
[Einstellungen] Identitäts- und Zugriffsverwaltung: Benutzerverwaltung	Anzeigen: Seite/Registerkarte „Benutzerverwaltung“	Zulässig
	Anzeigen: Lokale/LDAP-/VIDM-Benutzer	Zulässig
	Hinzufügen/Bearbeiten/Löschen: Lokaler Benutzer	Zulässig
	Hinzufügen/Bearbeiten/Löschen: LDAP-Benutzer	Zulässig
	Hinzufügen/Bearbeiten/Löschen: VIDM-Benutzer	Zulässig
[Einstellungen] Ereignisse	Anzeigen: Seite/Registerkarte „Ereignisse“	Zulässig
[Einstellungen] Ereignisse: Systemereignisse	Anzeigen: Seite/Registerkarte „Systemereignisse“	Zulässig
	Anzeigen: Liste der Systemereignisse	Zulässig
	Bearbeiten: Systemereignisse	Zulässig
	Aktivieren/Deaktivieren: Systemereignisse	Zulässig
	Massenbearbeitung/Aktivieren/Deaktivieren: Systemereignisse	Zulässig
[Einstellungen] Ereignisse: Plattformzustand: Ereignisse	Anzeigen: Seite/Registerkarte „Plattformzustand: Ereignisse“	Zulässig
	Anzeigen: Liste der Plattformzustandereignisse	Zulässig
	Bearbeiten: Plattformzustand: Ereignisse	Zulässig
	Massenbearbeitung: Plattformzustand: Ereignisse	Zulässig
[Einstellungen] Ereignisse: Benutzerdefinierte Ereignisse	Anzeigen: Seite/Registerkarte „Benutzerdefinierte Ereignisse“	Zulässig
	Anzeigen: Liste der benutzerdefinierten Ereignisse	Zulässig
	Bearbeiten/Löschen: Benutzerdefinierte Ereignisse	Zulässig
	Aktivieren/Deaktivieren: Benutzerdefinierte Ereignisse	Zulässig
[Einstellungen] IP-Eigenschaften und Subnetze	Anzeigen: Seite/Registerkarte „IP-Eigenschaften und Subnetze“	Zulässig
[Einstellungen] Zuordnung von physischer IP und DNS	Anzeigen: Seite/Registerkarte „Zuordnung von physischer IP und DNS“	Zulässig
	Anzeigen: Zuletzt importierte Zuordnung von physischer IP und DNS	Zulässig

Tabelle 6-7. Unterstützte Funktionen für jede Rolle (Fortsetzung)

Seite	Aktionen	Administrator
	Herunterladen: Datei für Zuordnung von physischer IP und DNS	Zulässig
	Hochladen/Ersetzen: Zuordnung von physischer IP und DNS	Zulässig
	Löschen: Vorhandene Zuordnung von physischer IP und DNS	Zulässig
[Einstellungen] Physische Subnetze und VLANs	Anzeigen: Seite/Registerkarte „Physische Subnetze und VLANs“	Zulässig
	Anzeigen: Vorhandene Liste der konfigurierten physischen Subnetze und VLANs	Zulässig
	Hinzufügen/Bearbeiten/Löschen: Physische Subnetze und VLANs	Zulässig
[Einstellungen] Ost-West-IPs	Anzeigen: Seite/Registerkarte „Ost-West-IPs“	Zulässig
	Anzeigen: Vorhandene Ost-West-IP-Tags	Zulässig
	Hinzufügen/Aktualisieren/Löschen: Ost-West-IP-Tags	Zulässig
[Einstellungen] Nord-Süd-IPs	Anzeigen: Seite/Registerkarte „Nord-Süd-IPs“	Zulässig
	Anzeigen: Vorhandene Nord-Süd-IP-Tags	Zulässig
	Hinzufügen/Aktualisieren/Löschen: Nord-Süd-IP-Tags	Zulässig
[Einstellungen] Konten und Datenquellen	Anzeigen: Seite/Registerkarte „Konten und Datenquellen“	Zulässig
	Anzeigen: Vorhandene Datenquellen	Zulässig
	Hinzufügen/Bearbeiten/Löschen: Datenquellen	Zulässig
	Aktivieren/Deaktivieren: Vorhandene Datenquellen	Zulässig
[Einstellungen] Datenverwaltung	Anzeigen: Seite/Registerkarte „Datenverwaltung“	Zulässig
	Anzeigen: Details zu Datenaufbewahrungsintervall	Zulässig
	Bearbeiten: Details zu Datenaufbewahrungsintervall	Zulässig
[Einstellungen] Infrastruktur und Support	Anzeigen: Seite/Registerkarte „Infrastruktur und Support“	Zulässig

Tabelle 6-7. Unterstützte Funktionen für jede Rolle (Fortsetzung)

Seite	Aktionen	Administrator
[Einstellungen] Infrastruktur und Support: Übersicht und Updates	Anzeigen: Seite/Registerkarte „Übersicht und Support“	Zulässig
	Anzeigen: Details zu Übersicht und Updates	Zulässig
	Aktivieren/Deaktivieren: Online-Update-Status	Zulässig
	Details anzeigen/Upgrade starten: Online-Update	Zulässig
	Anzeigen: Offline-Update	Zulässig
	Hochladen: Offline-Paket	Zulässig
	Anzeigen: Systemzustand	Zulässig
	Anzeigen: Plattform-VMs	Zulässig
	Cluster erstellen	Zulässig
	Herunterladen: Support-Paket	Zulässig
	Anzeigen: Collector-VMs	Zulässig
[Einstellungen] Infrastruktur und Support: Support	Hinzufügen/Bearbeiten/Löschen: Collector-VMs	Zulässig
	Anzeigen: Seite/Registerkarte „Support“	Zulässig
	Anzeigen: Details zum Produktsupport	Zulässig
	Aktivieren/Deaktivieren: Support-Tunnel	Zulässig
	Anzeigen: Programm zur Verbesserung der Benutzerfreundlichkeit	Zulässig
	Bearbeiten: Programm zur Verbesserung der Benutzerfreundlichkeit	Zulässig
	Erstellen: Support-Paket	Zulässig
Herunterladen: Support-Pakete	Zulässig	
[Einstellungen] Vorlagen	Anzeigen: Seite/Registerkarte „Vorlagen“	Zulässig
[Einstellungen] Vorlagen: Eigenschaftsvorlagen	Anzeigen: Seite/Registerkarte „Eigenschaftsvorlagen“	Zulässig

Tabelle 6-7. Unterstützte Funktionen für jede Rolle (Fortsetzung)

Seite	Aktionen	Administrator
	Anzeigen: Vorhandene Eigenschaftsvorlagen	Zulässig
	Klonen/Bearbeiten/Löschen: Vorhandene Eigenschaftsvorlagen	Zulässig
[Einstellungen] Vorlagen: App-Erkennungsvorlagen	Anzeigen: Seite/Registerkarte „App-Erkennungsvorlagen“	Zulässig
	Anzeigen: Vorhandene App-Erkennungsvorlagen	Zulässig
	Klonen/Bearbeiten/Löschen: Vorhandene App-Erkennungsvorlagen	Zulässig
[Dashboard] Planen und bewerten	Anzeigen: Registerkarte „Planen und bewerten“	Zulässig
[Dashboard] Planen und bewerten: Sicherheitsplanung	Anzeigen: Seite „Sicherheitsplanung“ (Mikro-Segmente, Datenverkehrsverteilung, Top-Ports nach Byte)	Zulässig
	Analysieren: Sicherheitsplanung	Zulässig
	Pin-Widgets	Zulässig
	Bewertungsbericht	Zulässig
	Ringdiagramm-/Listenansicht: Mikrosegmente	Zulässig
	Als CSV exportieren	Zulässig
[Dashboard] Planen und bewerten: PCI-Übereinstimmung	Anzeigen: Seite/Registerkarte „PCI-Übereinstimmung“	Zulässig
	Bewerten: PCI-Übereinstimmung	Zulässig
	Pin-Widgets/Benachrichtigungen erstellen	Zulässig
	CSV/PDF exportieren	Zulässig
	Hilfe	Zulässig
[Dashboard] Planen und bewerten: Anwendungen	Anzeigen: Seite/Registerkarte „Anwendungen“	Zulässig
	Hinzufügen: Anwendungen	Zulässig
	Bearbeiten/Löschen: Vorhandene Anwendungen	Zulässig
	Exportieren	Zulässig
Anwendungsermittlung	Anzeigen: Registerkarte „Ermitteln“	Zulässig
	Anwendungen ermitteln	Zulässig
[Dashboard] Analyse	Anzeigen: Seite/Registerkarte „Analyse“	Zulässig
[Dashboard] Analyse: Ausreißer	Anzeigen: Seite/Registerkarte „Ausreißer“	Zulässig
	Anzeigen: Konfigurationen für vorhandene Ausreißer	Zulässig

Tabelle 6-7. Unterstützte Funktionen für jede Rolle (Fortsetzung)

Seite	Aktionen	Administrator
	Hinzufügen/Bearbeiten/Löschen: Konfiguration für vorhandene Ausreißer	Zulässig
	Aktivieren/Deaktivieren: Konfiguration für vorhandenen Ausreißer	Zulässig
	Pin-Widget	Zulässig
[Dashboard] Analyse: Schwellenwerte	Anzeigen: Seite/Registerkarte „Schwellenwerte“	Zulässig
	Anzeigen: Konfigurationen für vorhandene Schwellenwerte	Zulässig
	Hinzufügen/Bearbeiten/Löschen: Konfiguration für vorhandene Schwellenwerte	Zulässig
	Aktivieren/Deaktivieren: Konfiguration für vorhandene Schwellenwerte	Zulässig
	Pin-Widget	Zulässig
[Dashboard] Analyse: Flow-Einblicke	Anzeigen: Seite/Registerkarte „Flow-Einblicke“	Zulässig
	Analysieren: Flow-Einblicke	Zulässig
	Pin-Widgets	Zulässig
	Als CSV exportieren/Maximieren/Hilfe	Zulässig
Gespeicherte Suchvorgänge	Anzeigen: Gespeicherte Standardsuche	Zulässig
	Hinzufügen/Löschen: Neue gespeicherte Suche	Zulässig

Hinzufügen von lokalen Benutzern

vRealize Network Insight ermöglicht es Ihnen, Benutzer hinzuzufügen und jedem Benutzer eine Rolle zuzuweisen.

Verfahren

- 1 Erweitern Sie auf der Seite **Einstellungen** in vRealize Network Insight die Option **Identitäts- und Zugriffsverwaltung**.
- 2 Klicken Sie auf **Benutzerverwaltung** und wählen Sie die Registerkarte „Benutzer“ in VMware Identity Manager aus.
- 3 Klicken Sie auf **BENUTZER HINZUFÜGEN** und geben Sie die erforderlichen Details ein.

Eigenschaften	Beschreibung
Name	Geben Sie den Namen des Benutzers ein.
E-Mail (Anmelde-ID)	Geben Sie ggf. Ihre E-Mail-Adresse oder Anmelde-ID ein.

Eigenschaften	Beschreibung
Rolle	Wählen Sie eine Rolle aus der Dropdown-Liste.
Kennwort	Geben Sie das Kennwort ein.
Geben Sie das neue Kennwort erneut ein.	Geben Sie das Kennwort zur Bestätigung erneut ein.

- 4 Klicken Sie auf **Benutzer hinzufügen**, um die Benutzerinformationen zu speichern.

Zuweisen von Rollen zu LDAP-Benutzern

Sie können beliebigen LDAP-Benutzern Rollen zuweisen, um ihnen Zugriff auf vRealize Network Insight zu gewähren.

Voraussetzungen

[Konfigurieren des Lightweight Directory Access Protocol \(LDAP\)](#)

Verfahren

- 1 Erweitern Sie auf der Seite **Einstellungen** in vRealize Network Insight die Option **Identitäts- und Zugriffsverwaltung**.
- 2 Klicken Sie auf **Benutzerverwaltung** und wählen Sie die Registerkarte **LDAP-Benutzer** aus.
- 3 Klicken Sie auf **BENUTZER HINZUFÜGEN**.
- 4 Geben Sie die Anmelde-ID des Benutzers an, dem Sie eine Rolle zuweisen möchten.
- 5 Wählen Sie eine Rolle aus der Liste aus. Weitere Informationen finden Sie unter [Konfigurieren der Benutzerverwaltung](#).
- 6 Klicken Sie auf **BENUTZER HINZUFÜGEN**.

Konfigurieren des Lightweight Directory Access Protocol (LDAP)

Damit sich die LDAP-Benutzer bei vRealize Network Insight anmelden können, müssen Sie den LDAP-Dienst auf der vRealize Network Insight-Plattform wie folgt konfigurieren:

Voraussetzungen

Sie müssen über das Recht **Administrator** verfügen.

Verfahren

- 1 Melden Sie sich bei vRealize Network Insight an und klicken Sie auf **Einstellungen**.
- 2 Klicken Sie unter **Identitäts- und Zugriffsverwaltung** auf **LDAP**.
- 3 Klicken Sie auf **Konfigurieren**.

4 Geben Sie folgende Informationen ein:

Feld	Beschreibung
Domäne	Geben Sie den Domänennamen ein. Dies ist in der Regel der letzte Teil der E-Mail-Adresse des Benutzers nach dem Zeichen „@“. Beispiel: Für einen Benutzer, der sich als johndoe@example.com anmeldet, ist dieses Feld <code>example.com</code> .
LDAP-Host-URLs	Geben Sie den Hostnamen ein. Sie können mehrere durch Komma getrennte LDAP-Host-URLs angeben.
Gruppenbasierte Zugriffssteuerung	<p>Wählen Sie diese Option aus, um eine Gruppe zu konfigurieren und den Mitgliedern dieser Gruppe eine Rolle zuzuweisen.</p> <ol style="list-style-type: none"> Geben Sie unter Basis-DN den Basis-DN ein, d. h. den Punkt, von dem aus der Server die Suche nach Benutzern startet. Geben Sie das Suchattribut an. Wählen Sie unter Gruppen-DN die Rolle des Benutzers für jede Gruppe aus. <p>Wenn Sie die Administratorrolle für eine bestimmte Gruppe auswählen, verfügen alle Mitglieder dieser Gruppe über das Administratorrecht. Wenn Sie die Mitgliedsrolle für eine bestimmte Gruppe auswählen, verfügen alle Mitglieder dieser Gruppe über das Mitgliederrecht. Wenn diese Option nicht ausgewählt wird, wird die Gruppeneinstellung verwendet, um die Rechte zuzuweisen. Aber andere gültige LDAP-Benutzer, die nicht zu den von Ihnen hinzugefügten Gruppen gehören, können sich beim Produkt anmelden.</p> Klicken Sie auf Weitere hinzufügen, um Gruppen in der Einschlussliste hinzuzufügen. Wählen Sie die Option Zugriff nur auf Mitglieder der oben genannten Gruppen beschränken aus, um den Zugriff auf die Benutzer nur über die von Ihnen hinzugefügten LDAP-Gruppen (direkte oder geerbte Mitgliedschaft) zuzulassen.
Benutzername	Benutzer mit den erforderlichen Berechtigungen zur Anmeldung mit den bereitgestellten Einstellungen.
Kennwort	Das Kennwort des Benutzers.

5 Klicken Sie auf **ABSENDEN**.

Nach der Konfiguration sehen Sie die **LDAP**-Details, die Sie konfiguriert haben.

Importieren von Benutzern aus VMware Identity Manager

Sie können VMware Identity Manager-Benutzerkonten importieren, damit diese vRealize Network Insight verwenden können, und Sie können ihnen Rollen zuweisen.

Voraussetzungen

[Konfigurieren von VMware Identity Manager](#) .

Verfahren

- 1 Erweitern Sie auf der Seite **Einstellungen** in vRealize Network Insight die Option **Identitäts- und Zugriffsverwaltung**.
- 2 Klicken Sie auf **Benutzerverwaltung** und wählen Sie die Registerkarte „Benutzer“ in VMware Identity Manager aus.
- 3 Klicken Sie auf **BENUTZER HINZUFÜGEN** und geben Sie die erforderlichen Details ein.

Feldname	Beschreibung
Domänenname	Geben Sie den VMware Identity Manager-Domännennamen für den Import ein.
Benutzer/Gruppen suchen	Geben Sie eine Suchzeichenfolge ein und wählen Sie das Benutzerkonto aus der Liste „Automatisch vervollständigen“ aus. Sie können entweder einen einzelnen Benutzer oder eine Benutzergruppe auswählen. Wenn Sie eine Gruppe auswählen, können alle Mitglieder in der Gruppe auf vRealize Network Insight zugreifen.
Rolle	Weisen Sie dem Benutzerkonto eine Rolle zu. Weitere Informationen finden Sie unter Konfigurieren der Benutzerverwaltung .

- 4 Klicken Sie auf **Benutzer hinzufügen**.

Hinweis

- Wenn Sie eine Gruppe ausgewählt haben, wird allen Mitgliedern in der Gruppe dieselbe Rolle zugewiesen. Wenn Sie einem bestimmten Benutzer in der Gruppe eine andere Rolle zuweisen möchten, müssen Sie den Benutzer einzeln hinzufügen und ihm die gewünschte Rolle zuweisen.

Beispiel: Um die **Administrator**-Rolle nur dem Benutzer *user1* in der Gruppe *Mygroup* zuzuweisen, gehen Sie wie folgt vor:

- Fügen Sie *Mygroup* hinzu und weisen Sie ihr die Rolle **Mitglied** zu.
- Fügen Sie *user1* hinzu und weisen Sie diesem Benutzer die **Administrator**-Rolle zu.

Die dem Benutzer zugewiesene Rolle überschreibt unmittelbar die Rolle, die dem Benutzer als Mitglied der Gruppe zugewiesen ist.

- Wenn ein Benutzer mehreren Gruppen mit unterschiedlichen Rollen angehört, wird dem Benutzer die Rolle mit dem höchsten Recht zugewiesen.

Beispiel: Wenn ein Benutzer zu *Group A* gehört, die die **Administrator**-Rolle hat, und zugleich zu *Group B* und *Group C* gehört, die die **Mitglied**-Rolle haben, übernimmt der Benutzer die **Administrator**-Rolle.

Ergebnisse

Dieser VMware Identity Manager-Benutzer bzw. die Mitglieder dieser Gruppe können sich jetzt bei vRealize Network Insight anmelden und die Funktionen verwenden, zu denen die ihnen zugewiesene Rolle berechtigt ist.

Konfigurieren von VMware Identity Manager

Administratoren können für VMware Identity Manager-Benutzer den Zugriff auf vRealize Network Insight-Funktionen basierend auf ihren Rollen autorisieren.

Voraussetzungen

Registrieren Sie vRealize Network Insight als OAuth-Client für den VMware Identity Manager-Host. Weitere Informationen finden Sie in der [Dokumentation zu VMware Workspace ONE Access](#).

Verfahren

- 1 Melden Sie sich bei vRealize Network Insight an und klicken Sie auf **Einstellungen**.
- 2 Klicken Sie unter „Identitäts- und Zugriffsverwaltung“ auf VMware Identity Manager.
- 3 Klicken Sie auf **Konfigurieren**.
- 4 Geben Sie folgende Informationen ein:

Parameter	Beschreibung
VMware Identity Manager-Appliance	Den vollqualifizierten Domänennamen (FQDN) des VMware Identity Manager-Hosts.
OAuth-Client-ID	Die ID, die beim Registrieren von vRealize Network Insight auf dem VMware Identity Manager-Host erstellt wird.
Geheimer OAuth-Clientschlüssel	Den geheimen Schlüssel, der beim Registrieren von vRealize Network Insight auf dem VMware Identity Manager-Host erstellt wird.
SHA-256-Fingerabdruck	Dies ist ein optionales Feld. Den Zertifikatfingerabdruck des VMware Identity Manager-Hosts. Weitere Informationen finden Sie unter Abrufen des Zertifikatfingerabdrucks vom VMware Identity Manager-Host .

- 5 Klicken Sie auf **Absenden**.
Nach der Konfiguration sehen Sie die VMware Identity Manager-Appliance und die Client-Details, die Sie konfiguriert haben.
- 6 Klicken Sie auf die Umschaltfläche, um VMware Identity Manager zu aktivieren oder zu deaktivieren. Wenn Sie es deaktivieren, können Sie die VMware Identity Manager-Authentifizierung in vRealize Network Insight nicht verwenden.

Abrufen des Zertifikatfingerabdrucks vom VMware Identity Manager-Host

Für die Validierung des SSL-Zertifikats können Sie den SHA-256-Fingerabdruck vom VMware Identity Manager-Host abrufen.

Verfahren

- 1 Um das SSL/TLS-Zertifikat abzurufen, führen Sie den folgenden Befehl aus:

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

Kopieren Sie das Serverzertifikat von -----BEGIN CERTIFICATE----- bis -----END CERTIFICATE----- in eine Datei namens `cert.pem` und speichern Sie die Datei.

2 Um den Fingerabdruck zu aktualisieren, führen Sie den folgenden Befehl aus:

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

Ergebnisse

Der Fingerabdruck wird im folgenden Format angezeigt:

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
```

Nächste Schritte

Kopieren Sie den Fingerabdruck und fügen Sie ihn auf der Seite „VMware Identity Manager konfigurieren“ ein.

Konfigurieren von Protokollen

In vRealize Network Insight können Sie verschiedene Protokolltypen anzeigen und konfigurieren.

Anzeigen und Exportieren von Überwachungsprotokollen

Überwachungsprotokolle erfassen administrative Aktionen, die im System durchgeführt werden. Dies sind reguläre CRUD-Vorgänge sowie Anmelde- und Abmeldeereignisse. Die administrativen Aktionen, die über die Benutzeroberfläche, die CLI oder die API durchgeführt werden, werden protokolliert.

Die Überwachungsprotokolle erfassen die Aktionen von API, Benutzeroberfläche und CLI.

Funktionen

- Die Überwachungsprotokollfunktion ist immer aktiviert.
- vRealize Network Insight unterstützt das UTC-Format für die Überwachungsprotokolle.
- Das Überwachungsprotokoll ist in den Syslog integriert. Sie können den Syslog-Collector so konfigurieren, dass alle Überwachungsprotokolle erfasst werden.
- Sie können alle Überwachungsprotokolldaten in eine CSV-Datei exportieren.

Einrichten der Syslog-Konfiguration

Sie können Remote-Syslog-Server für vRealize Network Insight mithilfe der Seite **Syslog-Konfiguration** konfigurieren.

Während jeder Proxy-Server potenziell einen anderen Remote-Syslog-Server haben kann, verwenden alle Plattformservers in einem Cluster denselben Remote-Syslog-Server.

In der aktuellen Version werden die vRealize Network Insight-Problemeereignisse und die Syslogs des Plattform-/Proxy-Servers an den Remote-Syslog-Server gesendet.

Derzeit unterstützt vRealize Network Insight nur UDP für die Kommunikation zwischen vRealize Network Insight-Servern und Remote-Syslog-Servern. Stellen Sie also sicher, dass Ihre Remote-Syslog-Server so konfiguriert sind, dass Sie Syslog-Datenverkehr über UDP akzeptieren.

So konfigurieren Sie Syslogs:

- 1 Klicken Sie auf der Seite **Einstellungen** auf **Syslog-Konfiguration**. Die **Syslog-Konfiguration** enthält die konfigurierten Syslog-Server und deren Zuordnungen zu den aufgeführten virtuellen Appliances. Wenn Sie zum ersten Mal auf diese Seite zugreifen, ist das Syslog standardmäßig deaktiviert, und die Liste der Server auf dieser Seite wird nicht angezeigt.
- 2 So fügen Sie einen Syslog-Server hinzu:
 - a Klicken Sie auf **Syslog-Server hinzufügen**.
 - b Geben Sie die IP-Adresse, den Spitznamen und die Portnummer des Servers ein. Die Standard-Portnummer für UDP lautet 514.
 - c Um die Konfiguration zu testen, klicken Sie auf **Testprotokoll senden**.
 - d Klicken Sie auf **Absenden**.
 - e Wenn es sich um den ersten Server handelt, den Sie hinzugefügt haben, aktivieren Sie Syslog oben auf der Seite.
- 3 So ordnen Sie Server Plattformen und Proxys zu:
 - a Klicken Sie auf **Zuordnungen bearbeiten**.
 - b Wählen Sie den Syslog-Server für alle Plattformen und Proxy-Server aus.
 - c Wenn Sie Syslog nicht auf einem Proxy-Server oder auf der Plattform aktivieren möchten, wählen Sie die Option **Keine Server** aus.
 - d Klicken Sie auf **Absenden**.

Hinweis Nachdem Sie die Änderungen vorgenommen haben, kann es einige Minuten dauern, bis Sie wirksam sind.

E-Mail-Server konfigurieren

In vRealize Network Insight können Sie einen Mailserver so konfigurieren, dass Ereignisbenachrichtigungen per E-Mail empfangen werden.

So konfigurieren Sie den Mail-Server:

- 1 Klicken Sie in der oberen rechten Ecke der Startseite auf das Symbol **Profil** und anschließend auf **Einstellungen**.
- 2 Klicken Sie auf **Mail-Server**.

- 3 Aktivieren Sie das Kontrollkästchen "SMTP-Server".
- 4 Geben Sie die entsprechenden Werte in die Felder ein.

Tabelle 6-8.

Feld	Beschreibung
Sender-E-Mail	E-Mail-Adresse des Senders
SMTP-Hostname/IP-Adresse	Hostname oder IP-Adresse des SMTP-Servers.
Verschlüsselung	Die folgenden Verschlüsselungsoptionen sind verfügbar: keine, TLS und SSL.
SMTP-Portnummer	Portnummer des SMTP-Servers (Standard 25).

Hinweis Um den Gmail-Server als E-Mail-Server zu verwenden, sind zusätzliche Konfigurationseinstellungen erforderlich. Diese sind im Google-Support aufgeführt.

Aktivieren Sie optional das Kontrollkästchen „Authentifizierung“ und geben Sie den Benutzernamen und das Kennwort ein, um zusätzliche Sicherheit zu erhalten.

Hinweis Um zu überprüfen, ob die Benachrichtigungs-E-Mail ordnungsgemäß eingerichtet ist, klicken Sie auf **Test-E-Mail senden**.

- 5 Klicken Sie auf **Absenden**, um die Konfiguration abzuschließen.

Ziel des SNMP-Traps konfigurieren

In vRealize Network Insight können Sie maximal vier SNMP-Trap-Agenten (Simple Network Management Protocol) für den Empfang von Benachrichtigungen konfigurieren. Das Produkt unterstützt die Versionen v2c und v3 von SNMP:

- 1 Klicken Sie auf der Seite **Einstellungen** auf **SNMP-Trap-Ziele > ZIEL HINZUFÜGEN**.
- 2 Wählen Sie auf der Seite **SNMP-Trap-Ziel hinzufügen** im Dropdown-Feld **Version** das Protokoll **SNMPv2c** oder **SNMPv3** aus.

Hinweis Das SNMP v2c-Protokoll erfordert keine Authentifizierung. Das SNMP v3-Protokoll unterstützt die Authentifizierung.

- 3 Geben Sie im Textfeld **Ziel-IP-Adresse/FQDN** die IP-Adresse des SNMP-Agenten oder den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) ein.
- 4 Geben Sie im Textfeld **Zielport** eine Portnummer des SNMP-Agenten ein.

- 5 Führen Sie je nach der von Ihnen ausgewählten Version von SNMP eine der folgenden Aktionen aus:

Option	Aktion
Für SNMP v2c	Geben Sie im Textfeld Community-Zeichenfolge eine Community-Zeichenfolge ein.
Für SNMP v3	<ol style="list-style-type: none"> 1 Geben Sie im Textfeld Benutzername den Namen des Benutzers ein, den Sie im SNMP-Agent erstellt haben. 2 (Optional) Aktivieren Sie das Kontrollkästchen Authentifizierung verwenden. 3 (Optional) Wählen Sie ein Authentifizierungsprotokoll aus und geben Sie dann das Kennwort ein, das Sie für den jeweiligen Benutzer im SNMP-Agenten festgelegt haben. 4 (Optional) Aktivieren Sie das Kontrollkästchen Datenschutz verwenden, wählen Sie ein Datenschutzprotokoll aus und geben Sie einen entsprechenden Satz für den Datenschutz ein.

- 6 Geben Sie im Feld **Spitzname** einen Spitznamen ein.
- 7 (Optional) Um zu überprüfen, ob die Konfiguration korrekt durchgeführt wurde, klicken Sie auf **SNMP-Trap testen** und ermitteln Sie dann, ob das Trap an den SNMP-Agenten gesendet wurde.
- 8 Klicken Sie auf **Absenden**.

Löschen eines SNMP-Trap-Ziels

Sie können ein SNMP-Trap-Ziel aus vRealize Network Insight löschen. Wenn Sie über mehrere SNMP-Trap-Ziele verfügen, können Sie beim Löschen eines SNMP-Trap-Ziels die gesamte Benachrichtigung in Bezug auf dieses Trap-Ziel auf ein anderes verfügbares Trap-Ziel migrieren.

Verfahren

- 1 Klicken Sie neben der Datenquelle, die Sie löschen möchten, auf das Symbol **Löschen**.
Ein Popup-Fenster des Typs **Aktion bestätigen** wird geöffnet.
- 2 Wenn Sie das Ereignis vom aktuellen Trap-Ziel zu einem anderen Trap-Ziel migrieren möchten, klicken Sie auf die Dropdown-Liste **Mehrere Ziele auswählen** und wählen Sie das Trap-Ziel aus, auf das Sie die Ereignisse migrieren möchten.
- 3 Klicken Sie auf **Bestätigen**.

Verwalten von Lizenzen

Bei der Lizenzierung von vRealize Network Insight verlässt sich VMware auf die Ehrlichkeit. Das bedeutet, dass Sie bei einem Verstoß gegen die Anzahl der Lizenzen zwar eine Warnmeldung auf der Benutzeroberfläche sehen, die verfügbaren Funktionen jedoch unbeschränkt nutzen können.

In den folgenden Szenarien wird auf allen Seiten der Benutzeroberfläche eine Lizenz-Warnmeldung angezeigt:

- Lizenznutzung für Socket (CPU)-Lizenz überschritten.
Sie müssen eine weitere Lizenz hinzufügen, damit Ihre Anforderungen unterstützt werden.
- Gemischter Lizenztyp
 - Wenn Sie sowohl eine Advanced-Lizenz als auch eine Enterprise-Lizenz hinzugefügt haben.
Nach einem Upgrade von der Advanced-Edition auf die Enterprise-Edition müssen Sie die Advanced-Lizenz manuell löschen (**Einstellungen > Lizenz und Nutzung**). Stellen Sie sicher, dass Sie über eine ausreichende Anzahl von Enterprise-Lizenzen zur Verwendung der Enterprise-Funktionen verfügen.
 - Wenn Sie eine Socket-Lizenz und eine Core-Lizenz hinzugefügt haben.
Löschen Sie je nach Ihren Anforderungen einen der Lizenztypen.

Berechnung der Lizenznutzung

Die Nutzung der vRealize Network Insight-Lizenzen wird auf der Grundlage des folgenden Verhältnisses berechnet:

Objekt	Beschreibung	Anzahl zulässiger Objekte pro Socket-Lizenz
VMware vSphere-CPU	Gesamtzahl der CPU-Sockets von lokalen Host-Maschinen	1
VMware Cloud on AWS-Hosts	Gesamtzahl der VMware Cloud on AWS-Hosts	0,5 Hinweis One VMC host requires two socket licenses.
AWS-vCPUs oder Azure	Gesamtzahl der vCPUs von AWS-Instanzen oder Azure	16
VMware-fremde Endpoints	Gesamtzahl der in Flows angezeigten Endpoints außerhalb des Internets und außerhalb von VMware, die ausschließlich durch VMware-fremde Flow-Berichtsfunktionen gemeldet werden (z. B. ein NetFlow, der von einem physischen Switch kommt)	15

Hinweis vRealize Network Insight berücksichtigt deaktivierte Datenquellen auch bei der Berechnung der Lizenznutzung. Löschen Sie die Datenquellen, wenn Sie möchten, dass vRealize Network Insight diese beim Zählen ignoriert.

SD-WAN-Lizenz

Um VMware SD-WAN als Datenquelle hinzuzufügen und Ihre VMware SD-WAN-Bereitstellung in vRealize Network Insight anzuzeigen, müssen Sie eine VMware SD-WAN-Lizenz hinzufügen. Sie können die VMware SD-WAN-Lizenz als eigenständige Lizenz hinzufügen oder in Verbindung mit einer Enterprise-Lizenz verwenden. Sie können eine VMware SD-WAN-Lizenz jedoch nicht in Verbindung mit einer Advance-Lizenz verwenden. Sie können zur Unterstützung von Edges mit unterschiedlichen Bandbreiten mehrere VMware SD-WAN-Lizenzschlüssel verwenden.

Mit der VMware SD-WAN-Lizenz können Sie zusätzlich zur VMware SD-WAN-Datenquelle, können Sie auch vCenter ohne IPFIX, Switches und Router sowie Infoblox hinzufügen.

Vergleichen der Funktionen basierend auf der Lizenzedition

Die Funktionen von vRealize Network Insight variieren je nach verwendeter Lizenz.

Die folgende Tabelle zeigt den Funktionsvergleich zwischen den verschiedenen für vRealize Network Insight angebotenen Lizenzen:

Funktion	Advanced-Lizenz	Enterprise-Lizenz	Cloud-Dienst	SD-WAN lokal	SD-WAN-SKU (Cloud-Dienst)
Virtuelle Flows (VDS IPFIX, V2V, V2P)	Ja	Ja	Ja	Nein	Nein
M-Seg-Planung und -Vorgänge für NSX-Firewall (NSX IPFIX)	Ja	Ja	Ja	Nein	Nein
Sichtbarkeit in Switches, Routern, Firewalls und Lastausgleichsdiensten von Drittanbietern	Ja	Ja	Ja	Nein	Nein
Öffentliche API	Ja	Ja	Ja	Nein	Nein
DNS-Zuordnung (Bind-Datei importieren)	Ja	Ja	Ja	Nein	Nein
NSX-Dashboard „PCI-Übereinstimmung“	Nein	Ja	Ja	Nein	Nein
Sicherheitsplanung und Sichtbarkeit für VMware Cloud on AWS	Nein	Ja	Ja	Nein	Nein
Sicherheitsplanung und Sichtbarkeit für AWS und Azure	Nein	Ja	Ja	Nein	Nein
DNS-Auflösung mit Infoblox	Nein	Ja	Ja	Nein	Nein
Physische Flows (NetFlow v7 und v9 und sFlow)	Nein	Ja	Ja	Nein	Nein
Sichtbarkeit für VMware Enterprise PKS, Kubernetes und OpenShift	Nein	Ja	Ja	Nein	Nein

Funktion	Advanced-Lizenz	Enterprise-Lizenz	Cloud-Dienst	SD-WAN lokal	SD-WAN-SKU (Cloud-Dienst)
Netzwerk- und Sicherheitsanalyse (Top-Kommunizierer, Anomalien, Ausreißerererkennung usw.)	Nein	Ja	Ja	Nein	Nein
Konfigurierbarer und erweiterter Aufbewahrungszeitraum für Daten	Nein	Ja	Ja	Nein	Nein
Underlay-Sichtbarkeit für Cisco ACI und BGP-EVPN	Nein	Ja	Ja	Nein	Nein
Dashboard „Anwendungserkennung“ (Namen, Tags, Regex)	Ja	Ja	Ja	Nein	Nein
ServiceNow-Integration für Anwendungserkennung	Nein	Ja	Ja	Nein	Nein
Flow-basierte Anwendungserkennung	Nein	Nein	Ja	Nein	Nein
VMware Cloud on AWS Direct Connect	Nein	Ja	Ja	Nein	Nein
VMware SD-WAN by VeloCloud	Nein	Nein	Nein	Ja	Ja
vRealize Operations Manager-Integration	Ja	Ja	Ja	Nein	Nein

Hinzufügen und Ändern einer Lizenz

Sie können die Lizenznutzungszahlen und auch die zugehörigen Details anzeigen, indem Sie auf der Seite „Lizenz und Nutzung“ auf den jeweiligen Link für jede Einheit klicken. Auf dieser Seite können Sie auch einen Lizenztyp hinzufügen oder den Lizenztyp ändern. vRealize Network Insight unterstützt das Hinzufügen mehrerer Lizenzen.

Lizenz hinzufügen

So fügen Sie eine Lizenz hinzu:

- 1 Klicken Sie auf der Seite „Lizenz und Nutzung“ auf **Lizenz hinzufügen**.
- 2 Geben Sie den Lizenzschlüssel im Feld **Neuer Lizenzschlüssel** an.
- 3 Klicken Sie auf **Validieren**.

Sie sehen den Lizenztyp, die Anzahl der mit der Lizenz verfügbaren Sockets oder Kerne und die Ablaufdetails.

- 4 Klicken Sie auf **Aktivieren**.
- 5 Sie können die Liste der Lizenzen auf der Seite anzeigen.

- 6 Sie können die Lizenz auch löschen, indem Sie auf das Symbol „Löschen“ neben der Spalte „Ablauf“ klicken. Wenn die Lizenz zu einer Enterprise-Edition gehört und die letzte verbleibende Enterprise-Edition im System ist, stellen Sie sicher, dass Sie das AWS-Konto gelöscht haben, bevor Sie die Enterprise-Lizenz löschen.

Lizenz ändern

Bei Ablauf der Evaluierungslizenz wird bei der Anmeldung im Produkt eine Meldung angezeigt, die besagt, dass die Lizenz abgelaufen ist und Sie Ihre Lizenz verlängern müssen. Führen Sie die folgenden Schritte aus, um eine Lizenz zu ändern.

So ändern Sie eine Lizenz:

- 1 Klicken Sie auf den Link in der Meldung über den Ablauf, um zur Seite „Lizenz ändern“ zu wechseln. Alternativ können Sie in **Einstellungen** auf **Lizenz und Nutzung** und dann auf **Lizenz ändern** klicken.
- 2 Geben Sie auf der Seite **Lizenz ändern** in **Neuer Lizenzschlüssel** den neuen Lizenzschlüssel ein, den Sie von VMware erhalten haben.
- 3 Klicken Sie auf **Validieren**.
- 4 Klicken Sie auf **Aktivieren**.

Hinweis Nach Ablauf der Evaluierungslizenz werden die Datenanbieter deaktiviert und erfassen keine Daten mehr. Nach der Verlängerung der Lizenz müssen die Datenanbieter von der Benutzeroberfläche aus erneut aktiviert werden, um die Datenerfassung zu starten.

Konfigurieren des Intervalls für die automatische Aktualisierung

In vRealize Network Insight können Sie das Intervall für die automatische Aktualisierung der Seiten und Pinnwände für Einheiten konfigurieren.

vRealize Network Insight enthält die Funktion zum automatischen Aktualisieren von Dashboards und Pinnwänden für Einheiten. Das Dashboard wird gemäß der Angabe in der Kopfzeile automatisch alle n Minuten aktualisiert.

Sie können das Zeitintervall angeben, in dem alle Ihre Dashboards automatisch aktualisiert werden sollen. Nach dem angegebenen Zeitintervall (n Minuten) werden alle geöffneten Widgets auf dem Dashboard automatisch neu geladen.

Hinweis

- Das Zeitintervall für die automatische Aktualisierung eines bestimmten Dashboards können Sie nicht ändern.
 - Die automatische Aktualisierung wird angehalten, wenn Sie mit dem Schieberegler der Zeitachse ein vergangenes Zeitintervall auswählen.
-

Sie können die automatische Aktualisierung anhalten, wenn Sie sie für ein bestimmtes Dashboard nicht benötigen. Wählen Sie in der Kopfzeile für **Anhalten** die Einstellung **EIN** aus. Der Zähler für die automatische Aktualisierung wird zurückgesetzt, sobald Sie die Einstellung für **Anhalten** zu **AUS** ändern.

Wenn Sie eine Pinnwand anzeigen und ein anderer Benutzer Änderungen daran vornimmt, z. B. das Layout der Pinnwand ändert, aktualisiert die Funktion zur automatischen Aktualisierung nicht nur den Inhalt, sondern auch die gesamte Pinnwand. Dieser Fall tritt nur ein, wenn Sie und der andere Benutzer die Pinnwand gemeinsam nutzen und daran zusammenarbeiten.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** auf **Meine Einstellungen**. Oder klicken Sie im entsprechenden Dashboard neben „Automatische Aktualisierung“ in der Kopfzeilenleiste auf **Ändern**.
- 2 Klicken Sie auf **Bearbeiten**, um das Zeitintervall für die automatische Aktualisierung zu ändern. Wählen Sie das Zeitintervall aus dem Dropdown-Menü aus. Klicken Sie auf **Speichern**.
- 3 Um die Option für die automatische Aktualisierung zu deaktivieren, wählen Sie **Deaktiviert** aus dem Dropdown-Menü aus. Die automatische Aktualisierung wird dann für alle Dashboards deaktiviert.

Konfigurieren der Zeitüberschreitung für Benutzersitzungen

Standardmäßig ist für Benutzersitzungen eine Zeitüberschreitung von 15 Minuten festgelegt. Sie können diesen Wert nach Wunsch ändern.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** auf **Systemkonfiguration**.

Hinweis Die Registerkarte **Systemkonfiguration** ist nur für `admin` user sichtbar.

- 2 Klicken Sie auf das Symbol „Bearbeiten“, um Ihre Präferenz für die Zeitüberschreitung der Benutzersitzung zu ändern.
- 3 Ziehen Sie den Schieberegler, um den Zeitüberschreitungswert für die Sitzung festzulegen. Der Wert reicht von 15 Minuten bis 24 Stunden.
- 4 Sie können auch die Details dazu anzeigen, wer den Zeitüberschreitungswert und im Feld **Zuletzt geändert** geändert hat.
- 5 Klicken Sie auf **Absenden**. Die Erfolgsmeldung wird angezeigt, um zu bestätigen, dass die aktualisierte Sitzungsdauer ab der nächsten Anmeldung wirksam wird.

Hinweis Der neue Wert für die Zeitüberschreitung der Benutzersitzung wird erst wirksam, nachdem Sie sich abgemeldet und erneut angemeldet haben.

Hinzufügen eines Google Maps-API-Schlüssels

Zum Abrufen der Kartenansicht Ihrer SD-WAN-Bereitstellung müssen Sie einen Google Maps-API-Schlüssel in vRealize Network Insight hinzufügen.

Voraussetzungen

Stellen Sie Folgendes sicher:

- Sie sind Mitglied der Google Cloud Platform und Abrechnung ist in Ihrem Konto aktiviert.
- Sie verfügen über den Google Maps-API-Schlüssel. Informationen zum Abrufen des API-Schlüssels finden Sie im Verfahren „Abrufen eines API-Schlüssels“ in der *Dokumentation zur Google Maps Platform*.
- Sie haben den API-Schlüssel eingeschränkt, um Missbrauch zu verhindern. Weitere Informationen finden Sie unter „Einschränken des API-Schlüssels“ in der *Dokumentation zur Google Maps Platform*.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** auf **Systemkonfiguration**.
- 2 Geben Sie unter **Google Maps-API-Schlüssel** den API-Schlüssel ein und klicken Sie auf **Speichern**.

Konfigurieren der Validierung von Datenquellenzertifikaten

Wenn Sie in vRealize Network Insight eine Datenquelle hinzufügen, werden alle Zertifikate (HTTPS-Zertifikate oder öffentliche SSH-Schlüssel), die sich auf diese Datenquelle beziehen, automatisch als bei der ersten Verwendung vertrauenswürdig hinzugefügt. Nach dem Hinzufügen der Datenquelle in vRealize Network Insight wird bei jeder Änderung an einem Zertifikat das Zertifikat vom System validiert.

Sie haben zwei Möglichkeiten, die Validierung von Zertifikaten zu konfigurieren: **Automatische Akzeptanz** und **Manuelle Akzeptanz**. Bei **Automatische Akzeptanz** akzeptiert das System automatisch alle erkannten Änderungen des Zertifikats. Bei **Manuelle Akzeptanz** stoppt das System die Datenquelle und zeigt eine Warnmeldung zum manuellen Akzeptieren des Zertifikats an. Wenn Sie das Zertifikat akzeptieren, startet das System die Datenquelle.

Verfahren

- 1 Gehen Sie zu **Einstellungen > Systemkonfiguration**.
- 2 Wählen Sie im Dropdown-Menü **Validierung von Datenquellenzertifikaten** eine der Validierungsmethoden für die Datenquelle aus:
 - **Automatische Akzeptanz**
 - **Manuelle Akzeptanz**

3 Klicken Sie auf **Speichern**.

Hinweis Wenn Sie die Zertifikatvalidierungsmethode von **Manuelle Akzeptanz** in **Automatische Akzeptanz** ändern, müssen Sie alle verfügbaren Zertifikatänderungen manuell akzeptieren, bevor Sie die Zertifikatvalidierungsmethode ändern.

Wenn Sie die **Validierung von Datenquellenzertifikaten** von **Manuelle Akzeptanz** in **Automatische Akzeptanz** ändern, ohne die ausstehenden erkannten Zertifikatänderungen zu akzeptieren, müssen Sie alle Datenquellen, die ein ausstehendes Zertifikat aufweisen, löschen und erneut hinzufügen, um Einsicht in diese Datenquellen zu erhalten.

Manuelles Akzeptieren eines Datenquellenzertifikats

Wenn Sie für **Validierung von Datenquellenzertifikaten** die Option **Manuelle Akzeptanz** konfiguriert haben, müssen Sie für jede Datenquelle, bei der das System eine Zertifikatänderung feststellt, das neue Zertifikat (HTTPS-Zertifikat oder öffentlicher SSH-Schlüssel) akzeptieren.

Wenn Sie **Validierung von Datenquellenzertifikaten** als **Manuelle Akzeptanz** konfiguriert haben, wird eine Warnmeldung angezeigt, wenn vRealize Network Insight eine Änderung des Zertifikats erkennt. Sie können die Zertifikatänderungswarnung auch auf der Seite **Konten und Datenquellen** sehen. Verwenden Sie dieses Verfahren, um das Zertifikat zu akzeptieren.

Verfahren

- ◆ Klicken Sie in der Warnmeldung **Aktualisierung des Datenquellenzertifikats verfügbar auf ÜBERPRÜFEN**.

<p>Wenn bis zu zwei aktualisierte Zertifikate verfügbar sind:</p>	<p>a Es wird ein Fenster für das Datenquellenzertifikat angezeigt, das Details zum aktuellen und zum neuen Zertifikat enthält.</p> <p>b Überprüfen Sie das neue Zertifikat und klicken Sie auf AKZEPTIEREN.</p>
<p>Wenn mehr als zwei aktualisierte Zertifikate verfügbar sind, gehen Sie wie folgt vor:</p>	<p>a Auf der Seite Konten und Datenquellen sehen Sie die Meldung</p> <div data-bbox="671 1331 1430 1415" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Zertifikataktualisierung verfügbar. Hier klicken, um zu überprüfen und zu akzeptieren</p> </div> <p>unter der Datenquelle, in der die Zertifikataktualisierung verfügbar ist.</p> <p>b Klicken Sie auf Hier klicken, um zu überprüfen und zu akzeptieren für die Datenquelle, die Sie überprüfen und deren aktualisiertes Zertifikat Sie akzeptieren möchten.</p> <p>c Es wird ein Fenster für das Datenquellenzertifikat angezeigt, das Details zum aktuellen und zum neuen Zertifikat enthält.</p> <p>d Überprüfen Sie das neue Zertifikat und klicken Sie auf AKZEPTIEREN.</p>

Ergebnisse

Wenn Sie das neue Zertifikat akzeptieren, wird die Meldung `Zertifikat erfolgreich aktualisiert` angezeigt.

Anzeigen von Überwachungsprotokollen

Überwachungsprotokolle erfassen administrative Aktionen, die im System durchgeführt werden. Diese Aktionen sind reguläre CRUD-Vorgänge, Anmelde- und Abmeldeereignisse. Die Überwachungsprotokolle erfassen die Aktionen von API, Benutzeroberfläche und CLI.

- Die Überwachungsprotokollfunktion ist immer aktiviert.
- vRealize Network Insight unterstützt das UTC-Format für die Überwachungsprotokolle.
- Das Überwachungsprotokoll ist in den Syslog integriert. Sie können den Syslog-Collector so konfigurieren, dass alle Überwachungsprotokolle erfasst werden.
- Sie können alle Überwachungsprotokolldaten in eine CSV-Datei exportieren.

Derzeit werden die folgenden administrativen Aktionen nicht in Überwachungsprotokollen erfasst:

- SSH-Anmeldeprotokolle. Sie können die SSH-Protokolle in `/var/log/auth.log` finden.
- Änderungen bei „Physische IP- und DNS-Zuordnung“.
- Änderungen bei „Physische Subnetze und VLANs“.

Verfahren

- 1 Klicken Sie auf der Seite **Einstellungen** unter **Protokolle** auf **Überwachungsprotokolle**.
- 2 Die folgenden Details werden auf der Seite **Überwachungsprotokolle** angezeigt:

Informationen	Beschreibung
Date & Time	Zeitstempel der ausgeführten Aktion.
IP Address	IP-Adresse des Clients, von dem aus die Verbindung hergestellt wird, z. B. die CLI oder der Browser.
User Name	Benutzer, der die Aktion ausführt.
Object Type	Das Objekt, für das die Aktion durchgeführt wird.
Operation	Verschiedene Aktionen, die der Benutzer für das Objekt ausführt.
Object Identifier	Eindeutiger Bezeichner für das jeweilige Objekt, für das die Aktion ausgeführt wird.
Response	Indikator für Erfolg oder Fehlschlagen des Vorgangs.
Details	Details zu den Einstellungen, die geändert wurden, z. B. der Spitzname oder eine Eigenschaft.

- 3 Um die Erfassung von Informationen zu ermöglichen, wenn sich der Benutzer über einen Browser oder eine CLI anmeldet, aktivieren Sie **Erfassung von persönlich identifizierbaren Informationen zulassen**. Diese Option ist standardmäßig deaktiviert.

Hinweis Die Spalten `IP Address` und `User Name` sind leer, wenn diese Option deaktiviert ist.

- 4 Klicken Sie auf **Als CSV exportieren**, um die Überwachungsprotokolldaten im CSV-Format zu exportieren.

Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit oder Verlassen des Programms

Das Produkt ist Teil des Programms zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) von VMware. Mit dem CEIP werden Informationen für VMware bereitgestellt, mit denen es VMware ermöglicht wird seine Produkte und Dienste zu verbessern, Probleme zu beheben und Benutzern Hinweise zur optimalen Bereitstellung und Verwendung unserer Produkte zu geben. Im Rahmen des CEIP erfasst VMware regelmäßig technische Daten über die Verwendung von Produkten und Diensten von VMware durch Ihre Organisation in Verbindung mit den VMware-Lizenzschlüsseln Ihrer Organisation. Mit diesen Informationen können keine Einzelpersonen persönlich identifiziert werden.

Die Einzelheiten im Hinblick auf die durch das CEIP erfassten Daten und die Zwecke, für die sie von VMware verwendet werden, werden im Trust & Assurance Center unter <https://www.vmware.com/solutions/trustvmware/ceip.html> erläutert.

Sie können am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für vRealize Network Insight teilnehmen oder es verlassen.

- 1 Klicken Sie auf der Seite **Über das Programm** unter dem Programm zur Verbesserung der Benutzerfreundlichkeit auf **Ändern**.
- 2 Das CEIP-Fenster wird eingeblendet. Um dem CEIP beizutreten, aktivieren Sie **Aktivieren**. Diese Aktion aktiviert das CEIP und sendet Daten an <https://vmware.com>.
- 3 Um CEIP zu verlassen, deaktivieren Sie **Aktivieren**.
- 4 Klicken Sie auf **Absenden**.

Anzeigen des Systemzustands Ihrer Einrichtung

Der Indikator **Integrität** ist im Abschnitt **Übersicht** auf der Seite **Installation und Unterstützung** verfügbar.

Der Indikator **Integrität** wird rot angezeigt, wenn eine der folgenden Fehlfunktionen auftritt:

- Proxy stoppt die Erfassung von Flow-Daten
- Plattform stoppt die Verarbeitung von Daten aus irgendeinem Grund; Beispiel: unzureichender Festplattenspeicher
- Such-Indexer liegt zurück, was zu einem veralteten Suchergebnis führt

Die allgemeine Systemzustandsanzeige zeigt die Anzahl der Unregelmäßigkeiten mit einer roten Ampel an. Die einzelnen Unregelmäßigkeiten werden mit ihren Details aufgelistet, wenn Sie auf die Anzahl der Probleme im Zusammenhang mit der gesamten Integrität klicken. Bei normaler Funktion leuchtet die Systemzustandsanzeige grün.

Hinweis Es kann gelegentlich vorkommen, dass vRealize Network Insight eine nicht synchronisierte Systemuhr nicht erkennt. Wenn die Uhr nicht mit NTP synchronisiert ist, können einige Dienste fehlerhaft werden oder funktionieren möglicherweise nicht mehr.

Aktivieren des Support-Tunnels

Über den Support-Tunnel kann VMware für die erweiterte Fehlerbehebung extern eine Verbindung mit Ihrer Plattform und Collector-VMs auf der SSL-geschützten Verbindung herstellen.

Um den erweiterten Support anzufordern, klicken Sie auf der Seite **Installation und Support** im Abschnitt **Übersicht** auf den Schalter für die Option **Support-Tunnel**.

Hinweis Stellen Sie sicher, dass der Datenverkehr zu `support2.ni.vmware.com` auf Port 443 zugelassen ist.

Verwalten der Festplattennutzung

Wenn die Festplattennutzung für eine Plattform oder einen Collector hoch ist, wird ein Ereignis ausgelöst, um den Benutzer zu warnen. Darüber hinaus wird eine Empfehlung dafür bereitgestellt, wie viel mehr Festplattenspeicher hinzugefügt werden muss. Sie können das Ereignis in dem Plattform- oder dem Collector-Dashboard anzeigen. Die Warnung wird auch im entsprechenden Collector- oder Plattformabschnitt auf der Seite **Installation und Unterstützung** angezeigt.

Plattform VMs

IP Address (Name)	Last Activity	Status
<div style="display: flex; align-items: center;"> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc; margin-right: 10px;"> [Redacted] </div> <div style="color: #0070c0;">(vrni-platform)</div> </div> <div style="border: 2px solid #e91e63; padding: 5px; margin-top: 5px; display: flex; align-items: center;"> ! Critical: Disk Utilization is high i </div>		<div style="background-color: #333; color: #fff; padding: 10px; border-radius: 5px; width: fit-content;"> <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> </div>

Sie können Festplatten zu den Knoten hinzufügen, indem Sie die folgenden Schritte ausführen:

Hinweis Erweitern Sie die vorhandene Festplatte nicht.

Verfahren

- 1 Melden Sie sich über den Web-Client bei vCenter mit ausreichenden Rechten an.
- 2 Klicken Sie mit der rechten Maustaste auf den Knoten und klicken Sie auf **Einstellungen bearbeiten**.
- 3 Fügen Sie die Festplatte gemäß der in der Warnung bereitgestellten Empfehlung hinzu.
vRealize Network Insight benötigt einige Minuten, um die Appliance zu erkennen und zur /var-Partition hinzuzufügen.

Anzeigen von Details zu Knoten

Sie können die Details jedes Knotens in einer Plattform oder einem Collector anzeigen.

Verfahren

- 1 Um die Details eines bestimmten Plattformknotens anzuzeigen, klicken Sie auf den Namen, der unter **Plattform-VMs** auf der Seite **Installation und Unterstützung** aufgeführt ist.
Das NI-Plattform-Dashboard wird angezeigt.
- 2 Um die Details eines bestimmten Collector-Knotens anzuzeigen, klicken Sie auf den Namen, der unter **Collector-VMs (Proxy)** auf der Seite **Installation und Unterstützung** aufgeführt ist.
Das NI-Collector-Dashboard wird angezeigt.

Erstellen eines Support-Pakets

Sie können ein Support-Paket erstellen, das Diagnosedaten wie produktspezifische Protokolle oder Konfigurationsdateien von Ihrer Einrichtung erfasst. Wenn Sie eine Support-Anfrage einreichen, nutzt der Technische Support von VMware diese Informationen, um die Probleme in Ihrer Einrichtung zu identifizieren und zu beheben.

Verfahren

- 1 Klicken Sie auf der Seite „Einstellungen“ auf **Installation und Unterstützung**.
- 2 Klicken Sie auf **Support-Paket erstellen**.
- 3 Wählen Sie die Plattform-VMs und die Collector-VMs aus, für die Sie das Support-Paket erstellen möchten.
Um alle VMs auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Plattform-VM- und der Collector-VM-Tabellen.
- 4 Klicken Sie auf **Erstellen**.

5 Klicken Sie auf **Ja**, um die Erstellung eines neuen Support-Pakets zu bestätigen.

vRealize Network Insight benötigt einige Zeit, um die Erstellung des Pakets abzuschließen.

Ergebnisse

Ein neues Support-Paket wird erstellt, und Datum und Uhrzeit werden angezeigt. Um den Download des Support-Pakets zu initiieren, klicken Sie neben der jeweiligen VM auf den Link **Herunterladen**.

Hinweis

- Die Erstellung des Support-Pakets auf einem mittelgroßen System kann über fünfzehn Minuten dauern.
- Zu einem bestimmten Zeitpunkt können jeweils nur zwei Support-Pakete vorhanden sein. Wenn bereits zwei Support-Pakete vorhanden sind und ein neues Support-Paket erstellt wird, wird das ältere der beiden vorhandenen Support-Pakete gelöscht.

Nächste Schritte

Hängen Sie das Support-Paket an Ihre Dienstanforderung für VMware an, um auf die Details zuzugreifen.

Grundlegendes zur Kapazität für Collector- und Plattformlasten

vRealize Network Insight bietet die ungefähre Kapazitäts- und Auslastungsinformationen eines Collector-Knotens und einer Plattform. Diese grenzwertbasierten Informationen helfen Ihnen, zukünftige Leistungs- und Erfahrungsprobleme zu vermeiden.

Grundlegendes zur Kapazität

Es gibt zwei Arten von Kapazitäten:

- VM-Kapazität: Sie ist definiert als die Anzahl der erkannten VMs, die ein Knoten oder eine Einrichtung verarbeiten können.
- Flow-Kapazität: Sie ist definiert als die Anzahl der Flows, die ein Knoten oder eine Einrichtung verarbeiten können.

Die Kapazität ist wie folgt definiert:

- Einzelne Plattform mit einem oder mehreren Proxy-Knoten: Die Kapazität eines Proxy-Knotens oder der Plattform ist die Anzahl der erkannten VMs, die ohne Leistungseinbußen verarbeitet werden können.
- Cluster-Einrichtung: Die Kapazität der Plattform in einer Cluster-Einrichtung ist die Aggregation aller Kapazitäten aller Plattformknoten, während die Kapazität von Proxy-Knoten auf der Ebene eines einzelnen Knotens berücksichtigt wird.

Zugreifen auf die Kapazitätsinformationen

Sie können **VM-Kapazität** und **Flow-Kapazität** auf der Seite **Installation und Unterstützung** anzeigen.

Für jeden Collector-Knoten, der unter Collector-VMs (Proxy) aufgeführt ist, werden nur die VM-Kapazitätsinformationen bereitgestellt.

Hinweis Wenn die Anzahl der erkannten VMs aus den Datenquellen in der Bereitstellung die Kapazität des Systems, des Collectors oder von beiden überschreitet, werden Sie das Upgrade nicht auslösen können.

So zeigen Sie die ermittelten VMs für eine Datenquelle an:

- 1 Auf der Seite **Konten und Datenquellen** können Sie die Anzahl der VMs sehen, die für eine bestimmte Datenquelle ermittelt wurden, die bereits hinzugefügt wurde und derzeit aktiv ist. Diese Spalte hat nur dann einen Wert, wenn es sich bei der Datenquelle um vCenter oder AWS handelt.

Hinweis Die Anzahl der ermittelten VMs umfasst Platzhalter- und Vorlagen-VMs. Sie kann sich also von der Anzahl der VMs im Produkt unterscheiden.

Direct Connect-Unterstützung in vRealize Network Insight

7

Direct Connect ist ein Mechanismus, um die Datenübertragungsverbindung zwischen einem lokalen Speicherort und Public Cloud-Diensten bereitzustellen. Ab Version 5.2 unterstützt vRealize Network Insight die Direct Connect-Funktion für VMware Cloud on AWS.

Die Direct Connect-Unterstützung ermöglicht Folgendes:

- Identifizieren der Flows über Direct Connect zwischen dem lokalen Datacenter und dem VMware Cloud on AWS-SDDC
- Ausführen der Flow-Analyse zum Ermitteln der Flow-Bandbreite und der Paketrate
- Anzeigen der detaillierten Pfadtopologie zwischen virtuellen Maschinen, die über Direct Connect kommunizieren
- Anzeigen der Details zu Direct Connect und zugehörigen Ereignissen

Datenabrufmechanismus von Direct Connect

vRealize Network Insight ruft Direct Connect-Informationen mithilfe der VMware Cloud on AWS-NSX-APIs ab. Daher müssen Sie die auf VMware Cloud on AWS bezogenen Datenquellen (vCenter und NSX Manager) hinzufügen, um die Direct Connect-Informationen zu erhalten.

Hinweis Sie müssen für die Direct Connect-Unterstützung kein AWS-Konto oder andere zusätzliche Datenquellen hinzufügen.

Um jedoch die Informationen zur Pfadtopologie zu erhalten, müssen Sie Colocation-Router wie Cisco N9k und Cisco ASR 9k (generischer Router) hinzufügen.

Mit Direct Connect-Unterstützung erfasste Daten

- Konfigurationsdetails zu Direct Connect im VMware Cloud on AWS SDDC.
- Angekündigte und erlernte Subnetze für Direct Connect auf der Ebene des SDDC.
- Konfigurationsinformationen von Direct Connect-Schnittstellen (VIFs), die mit dem SDDC verknüpft sind.

- Flows, die von der verteilten Firewall (DFW) in VMware Cloud on AWS gemeldet werden.

Hinweis

- Die Aktivierung von NetFlow ist auf den Colocation-Routern nicht erforderlich.
- Routenbasiertes VPN wird für Direct Connect nicht unterstützt. Selbst wenn Sie die Option „VPN als Sicherung für Direct Connect verwenden“ aktiviert haben, schlägt die VPN-Sicherung fehl.
- Die Metriken und die Informationen zu angekündigten oder erlernten Subnetzen sind auf individueller VIF-Ebene nicht verfügbar.

Direct Connect-Einheiten

- *VMware Cloud on AWS Direct Connect*: Dies ist die übergeordnete Einheit für alle Direct Connect-Einheiten in vRealize Network Insight, die die Konfigurationsinformationen von Direct Connect innerhalb des VMware Cloud on AWS SDDC modelliert.
- *Direct Connect-Schnittstelle*: Hiermit werden die von VMware Cloud on AWS bereitgestellten AWS Direct Connect-VIF-Informationen modelliert. Diese Einheit ermöglicht den Austausch von angekündigten und erlernten Routen zwischen VMware Cloud on AWS und dem lokalen Datacenter.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen von Details zu Direct Connect von VMC](#)
- [Anzeigen von Flows über Direct Connect](#)
- [Direct Connect-Suchabfragen](#)

Anzeigen von Details zu Direct Connect von VMC

Sie können die Seite **Direct Connect von VMC** aufrufen, um einen Überblick über die zugehörigen Eigenschaften und die Einheiten anzuzeigen, die mit Direct Connect verknüpft sind. Diese Angaben basieren auf den von VMware Cloud on AWS gesammelten Informationen.

Tabelle 7-1. Direct Connect-Dashboard

Abschnitt	Details
Eigenschaften	Primäre Direct Connect-Eigenschaften, einschließlich des zugehörigen SDDC, der lokalen ASN, der erlernten und angekündigten Routen und der fehlgeschlagenen angekündigten Routen.
Direct Connect-Schnittstellen	Die Liste aller virtuellen Direct Connect-Schnittstellen, die mit Direct Connect verknüpft sind
Ereignisse	Liste der mit Direct Connect verknüpften Ereignisse.

Anzeigen von Flows über Direct Connect

Sie können die Liste aller Flows anzeigen, die auf Direct Connect ausgeführt werden. So kann der Datenverkehr über Direct Connect angezeigt werden. Damit können Sie den Nutzungsgrad von Direct Connect analysieren und verstehen.

Wenn Sie eine Suche mithilfe der `Flows where connection = Direct Connect-ID`-Abfrage ausführen, sehen Sie die Liste der über Direct Connect laufenden Flows und Informationen wie die Bandbreitennutzung und die Netzwerkdatenverkehrsrate für eine bestimmte Direct Connect-Instanz. Diese Zeile aktualisieren – Unter dem Flow-Typ können Sie sehen, ob der Flow auf dem VPN, Direct Connect oder auf dem hybriden Netzwerk stattfindet.

Um nur die Direct Connect-Flows anzuzeigen, können Sie die folgende Abfrage ausführen:

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

Um die Anzahl der Flows und die Datenmenge für jede Direct Connect-Verbindung anzuzeigen, führen Sie die folgende Abfrage aus:

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

Um die Anzahl der Flows und die Paketanzahl für jede Direct Connect-Schnittstelle anzuzeigen, führen Sie die folgende Abfrage aus:

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

Weitere Informationen zu Abfragen finden Sie unter [Direct Connect-Suchabfragen](#).

Direct Connect-Suchabfragen

Sie können auf VMware Cloud on AWS Direct Connect- und Direct Connect-Schnittstelleneinheiten in vRealize Network Insight suchen.

Tabelle 7-2. Suchabfragen

Beschreibung	Abfrage
Abrufen einer Liste von VMware Cloud on AWS Direct Connect-Einheiten, auf deren Basis Sie die Informationen filtern können	<code>VMC Direct Connect where</code>
Abrufen der VMware Cloud on AWS Direct Connect-Listenansicht	<code>VMC Direct Connect</code>
Abrufen der maximal zulässigen Datenmenge über Direct Connect	<code>max(series(sum(bytes))) of flows where connection = 'Verbindungs-ID' and flow type = 'Different Dc' and source vm is set and destination vm is set and flow type = 'Direct Connect'</code>

Tabelle 7-2. Suchabfragen (Fortsetzung)

Beschreibung	Abfrage
Abrufen der maximal zulässigen Paketanzahl über Direct Connect	<code>max(series(sum(packets))) of flows where connection = 'Verbindungs-ID' and flow type = 'Different Dc' and source vm is set and destination vm is set and flow type = 'Direct Connect'</code>
Abrufen der maximal zulässigen Paketanzahl über Direct Connect zum Internet	<code>max(series(sum(packets))) of flows where connection = 'Verbindungs-ID' and flow type = 'Destination is internet' and flow type = 'Direct Connect'</code>
Abrufen der maximal zulässigen Datenmenge über Direct Connect zum Internet	<code>max(series(sum(bytes))) of flows where connection = 'Verbindungs-ID' and flow type = 'Destination is internet' and flow type = 'Direct Connect'</code>
Abrufen der maximal zulässigen Paketanzahl zwischen Datencentern über Direct Connect	<code>max(series(sum(packets))) of flows where connection = 'Verbindungs-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>
Abrufen der maximal zulässigen Datenmengen zwischen Datencentern über Direct Connect	<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-Integration



Mit vRealize Operations Manager können Sie die vRealize Network Insight-Warnungen in vRealize Operations Manager anzeigen. Darüber hinaus können Sie die Netzwerkinformationen in vRealize Operations Manager über vRealize Network Insight anzeigen.

vRealize Operations Manager verbraucht einen Satz von vRealize Network Insight-APIs und zeigt Listen von Warnungen im Dashboard „Warnungen“ an. Sie können die Warnungen aus vRealize Network Insight anhand des Präfix „vrni-“ in den Namen der Warnungen identifizieren. Darüber hinaus können Sie sehen, in welcher Einheit die Warnung ausgelöst wurde.

Eine Liste der vRealize Network Insight-APIs finden Sie im [vRealize Network Insight-API-Handbuch](#).

Sie können die Option **Launch-in-vRNI-context** von den Einheitsseiten wie VMs, Hosts, NSX-V und NSX-T verwenden, um das Dashboard der jeweiligen Einheit anzuzeigen. Dies ermöglicht es Ihnen, den Netzwerkzustand anzuzeigen und ein gegebenenfalls vorliegendes Netzwerkproblem zu beheben.

Informationen zum Integrieren von vRealize Network Insight in vRealize Operations Manager finden Sie im [VMware vRealize Operations Management Pack for vRealize Network Insight](#). Informationen zu unterstützten vRealize Operations Manager-Versionen finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).

Hinweis Sie müssen den vRealize Operations Manager-Benutzer in vRealize Network Insight hinzufügen, und der Benutzer muss mindestens über das Recht **Mitglied** verfügen, um die Funktion in vRealize Operations Manager verwenden zu können.

Erstellen und Erweitern von Clustern

9

Dieses Kapitel enthält die folgenden Themen:

- Erstellen von Clustern
- Erweitern von Clustern

Erstellen von Clustern

Sie können Cluster auf der Seite **Installation und Unterstützung** erstellen.

Voraussetzungen

Mindestens zwei zusätzliche Plattformen sind erforderlich. Die zusätzlichen Plattform-VMs sollten bereitgestellt und eingeschaltet sein.

Erstellen eines Clusters

- 1 Klicken Sie auf **Cluster erstellen** für **Plattform-VMs**.
- 2 Geben Sie auf der Seite **Cluster erstellen** die folgenden Informationen ein:
 - **IP-Adresse**: Geben Sie die IP-Adresse der neuen Plattform ein, die Sie hinzufügen möchten.
 - **Kennwort**: Geben Sie das Kennwort des Support-Benutzers der Plattform-VM ein. Wenn Sie das Kennwort noch nicht geändert haben, lesen Sie dazu den Abschnitt *Standardmäßige Anmeldedaten* im *vRealize Network Insight-Installationshandbuch*.
- 3 Um weitere Plattformen hinzuzufügen, klicken Sie auf **Weitere hinzufügen** und geben Sie die IP-Adresse und das Support-Benutzerkennwort ein.
- 4 Klicken Sie auf **Absenden**. Klicken Sie auf **Ja**.

- 5 Nach dem Erstellen eines Clusters muss sich der Benutzer erneut beim Produkt anmelden.

Hinweis

- Die Option **Cluster erstellen** ist nur aktiviert, wenn die Plattform eine große Brick-Größe aufweist. Alle Plattformen sollten eine große Brick-Größe haben, um ein Cluster zu erstellen.
 - Wenn Telemetrie auf einem einzelnen Knoten aktiviert wird, wird sie auf allen Knoten aktiviert.
 - Um Cluster zu erweitern, lesen Sie den Abschnitt *Erweitern eines Clusters* im *vRealize Network Insight-Installationshandbuch*.
-

Erweitern von Clustern

Sobald der Cluster erstellt wurde, können Sie ihn erweitern, indem Sie ihm weitere Plattformknoten hinzufügen.

Hinweis Den Clustererweiterungsvorgang dürfen Sie nur vom Knoten „Plattform 1“ (P1) aus durchführen.

Verfahren

- 1 Klicken Sie auf der Seite **Installation und Unterstützung** auf **Cluster erweitern** für **Plattform-VMs**.
- 2 Die IP-Adressen der VMs, die Teil des Clusters sind, sind bereits auf der Seite „Cluster erweitern“ aufgeführt. Um einen oder mehrere Knoten zum vorhandenen Cluster hinzuzufügen, geben Sie die IP-Adresse des Knotens und das Kennwort des Support-Benutzers an.

Hinweis

- Derzeit unterstützt vRealize Network Insight 10 Knoten in einem vorhandenen Cluster. Sobald der Grenzwert erreicht ist, ist die Schaltfläche **Weitere hinzufügen** deaktiviert.
 - Stellen Sie sicher, dass alle neuen Knoten nicht bereitgestellt und über SSH erreichbar sind.
 - Stellen Sie sicher, dass Sie eine Sicherung der vorhandenen Plattform-VMs erstellt haben, bevor Sie mit der Cluster-Erweiterung fortfahren.
-

- 3 Klicken Sie auf **Absenden**.

Der schrittweise Fortschritt wird angezeigt.

- 4 Sobald der Cluster-Erweiterungslink abgeschlossen ist, wird eine Erfolgsmeldung angezeigt. Während der Cluster-Erweiterung kann die Anwendung nicht für andere Vorgänge verwendet werden.

Konfigurieren von Flows in vRealize Network Insight

10

Dieses Kapitel enthält die folgenden Themen:

- Aktivieren der IPFIX-Konfiguration
- Flow-Unterstützung für physische Server
- Blockierte und geschützte Flows anzeigen
- Netzwerkadressübersetzung (NAT)
- VMware Cloud on AWS Flows
- Erstellen eines VPC-Flow-Protokolls
- Senden von Flow-Datensätzen von F5 an vRealize Network Insight-Collectors

Aktivieren der IPFIX-Konfiguration

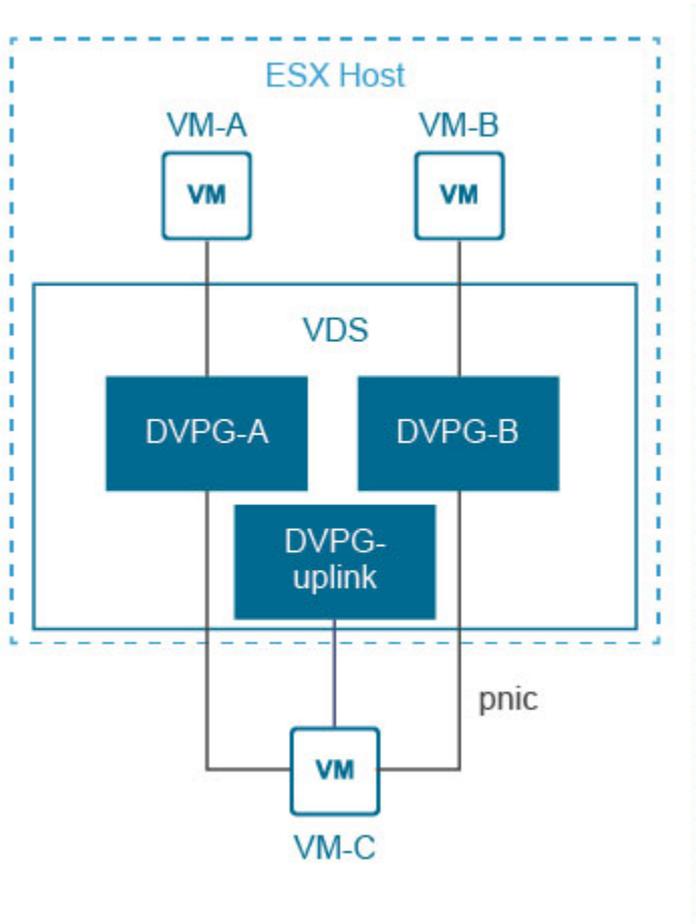
IPFIX ist ein IETF-Protokoll für den Export von Flow-Informationen.

Ein Flow wird als Satz von Paketen definiert, die in einem bestimmten Zeitfenster übertragen werden und die Nutzung derselben 5-Tupel-Werte – Quell-IP-Adresse, Quell-Port, Ziel-IP-Adresse, Zielport und Protokoll – teilen. Die Flow-Informationen können Eigenschaften wie z. B. Zeitstempel, Pakete/Byteanzahl, Eingabe-/Ausgabeschnittstellen, TCP-Flags, VXLAN-ID, gekapselte Flow-Informationen usw. enthalten.

IPFIX-Konfiguration auf VDS und DVPG

Ein VDS in einer vSphere-Umgebung kann für den Export von Flow-Informationen mithilfe von IPFIX konfiguriert werden. Die Flow-Überwachung muss für alle Portgruppen aktiviert werden, die an den VDS angehängt sind. Wenn Pakete auf Port X eines VDS ankommen und aus Port Y rausgehen, wird ein entsprechender Flow-Datensatz ausgegeben, wenn die Flow-Überwachung auf Port Y aktiviert ist.

Um die vollständigen Informationen einer Sitzung zu analysieren, werden die IPFIX-Daten über Pakete in beiden Richtungen benötigt. Beachten Sie das folgende Diagramm, in dem VM-A mit DVPG-A verbunden ist und mit VM-C kommuniziert. Hier liefert DVPG-A nur Daten über die C → A-Pakete und DVPG-Uplink liefert Daten über A → C-Pakete. Um die vollständigen Informationen über den Datenverkehr von A zu erhalten, sollte IPFIX auf DVPG-A, DVPG-Uplink aktiviert sein.



Die Proxy-VM von vRealize Network Insight verfügt über einen integrierten Collector/Receiver für IPFIX-Flow-Informationen. Sie können die IPFIX-Informationserfassung in den vCenter-Datenquelleneinstellungen auf verschiedenen Granularitätsebenen aktivieren.

Aktivieren der IPFIX-Konfiguration auf VDS und DVPG

So aktivieren Sie IPFIX-Informationen auf vCenter-Ebene:

Verfahren

- 1 Aktivieren Sie das Kontrollkästchen **NetFlow (IPFIX) in diesem vCenter aktivieren**, wenn Sie vCenter in vRealize Network Insight hinzufügen.
Sie sehen eine Liste aller verfügbaren VDS.
- 2 Wählen Sie den VDS, für den Sie IPFIX aktivieren möchten, aus der Liste der verfügbaren VDS in vCenter aus.
- 3 Es wird ein Benachrichtigungssymbol für den VDS angezeigt, in dem einer der Hosts eine nicht unterstützte Version von ESXi aufweist. Wenn vRealize Network Insight feststellt, dass IPFIX bereits für einen VDS mit einer anderen IP-Adresse außer der vRealize Network Insight-Proxy-VM konfiguriert wurde, wird die Schaltfläche **Überschreiben** angezeigt. Klicken Sie auf **Überschreiben**, um die Liste der DVPGs unter diesem VDS anzuzeigen.

- Die Liste der verfügbaren DVPGs für den ausgewählten VDS wird angezeigt. Alle DVPGs werden standardmäßig ausgewählt. Aktivieren Sie **Manuelle Auswahl**, um bestimmte DVPGs auszuwählen, für die Sie IPFIX aktivieren möchten. Wählen Sie die gewünschten DVPGs aus und klicken Sie auf **Absenden**.

Hinweis Das DVPG mit einem Benachrichtigungssymbol weist darauf hin, dass es sich um den Uplink-DVPG handelt, der ausgewählt werden muss.

IPFIX-Konfiguration für VMware NSX

IPFIX für VMware NSX stellt Netzwerküberwachungsdaten ähnlich denen von physischen Geräten bereit und bietet Administratoren eine klare Übersicht über die Bedingungen des virtuellen Netzwerks.

VMware NSX virtualisiert das Netzwerk, indem es dem Netzwerkadministrator die Möglichkeit bietet, das Netzwerk von der physischen Hardware abzukoppeln. Mit dieser Funktion können Sie das Netzwerk nach Bedarf vergrößern und verkleinern und das Netzwerk für die Anwendungen, die es durchlaufen, transparent machen.

Durch die Verwendung von NSX IPFIX in einem virtualisierten Netzwerk erhalten die Netzwerkadministratoren Einblick in das virtuelle Overlay-Netzwerk. Die VXLAN-IPFIX-Berichterstellung mithilfe von NetFlow ist auf dem Host-Uplink aktiviert. Sie bietet einen Überblick über die VTEP, die das Paket kapselt, und die Details der VM, die den Inter-Host-Datenverkehr auf einem NSX Logical Switch (VXLAN) generiert hat.

Die verteilte Firewall implementiert die statusorientierte Verfolgung von Flows. Da diese nachverfolgten Flows mehrere Zustandsänderungen durchlaufen, kann IPFIX zum Exportieren von Daten über den Status von Flows verwendet werden.

Die nachverfolgten Ereignisse umfassen Flow-Erstellung, Flow-Zurückweisung, Flow-Update und Flow-Abrüstung. Die zurückgewiesenen Ereignisse werden als Syslogs exportiert.

Aktivieren von VMware NSX-V IPFIX

So aktivieren Sie VMware NSX-V IPFIX in vRealize Network Insight:

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Anmeldedaten des Sicherheitsadministrators oder des Unternehmensadministrators verfügen.
- Es wird empfohlen, VDS-IPFIX auf allen DVS und DVPGs zu aktivieren, von denen NSX-IPFIX-Daten erfasst werden müssen. Sie können VDS IPFIX über die Seite „Details“ des zugeordneten vCenter aktivieren.

Verfahren

- ◆ Wählen Sie **IPFIX aktivieren**, wenn Sie eine NSX-V-Manager-Datenquelle hinzufügen oder bearbeiten.

Aktivieren von VMware NSX-T DFW IPFIX

So aktivieren Sie VMware NSX-T IPFIX in vRealize Network Insight:

Voraussetzungen

- Stellen Sie sicher, dass Sie über eine der folgenden Berechtigungen verfügen:
 - `enterprise_admin`
 - `network_engineer`
 - `security_engineer`
- Stellen Sie sicher, dass die verteilte Firewall (Distributed Firewall, DFW) aktiviert ist.
- Stellen Sie sicher, dass die Priorität 0 für das Network-Insight-IPFIX-Profil verfügbar ist. Wenn ein anderes IPFIX-Profil mit der Priorität 0 vorhanden ist, müssen Sie es in einen anderen Wert ändern.

Verfahren

- ◆ Wählen Sie **IPFIX aktivieren**, wenn Sie eine NSX-T Manager-Datenquelle hinzufügen oder bearbeiten.

Nächste Schritte

Nachdem Sie IPFIX aktiviert haben, erstellt vRealize Network Insight ein eigenes Network-Insight-Collector-Profil und Network-Insight-IPFIX-Profil auf NSX-T. Stellen Sie sicher, dass Sie keines dieser Profile ändern.

Wenn die Flows nach der Aktivierung von IPFIX auf NSX-T nicht in vRealize Network Insight angezeigt werden, können folgende Ereignisse auftreten:

- Network-Insight-Collector-Profil ist nicht im NSX-T Manager registriert.
- Network-Insight-IPFIX-Profil ist nicht im NSX-T Manager registriert.
- Die Portnummer des Netzwerk-Insight-IPFIX-Profiles wurde geändert.
- Das Netzwerk-Insight-Collector-Profil stimmt im Network-Insight-IPFIX-Profil im NSX-T Manager nicht überein.

Hinweis Um alle oben genannten Probleme zu beheben, aktivieren Sie NSX-T IPFIX erneut.

- Die Priorität des Network-Insight-IPFIX-Profiles ist im NSX-T Manager nicht null.
Um dieses Problem zu beheben, melden Sie sich bei NSX-T Manager an und legen Sie die Priorität des Network-Insight-IPFIX-Profiles auf null fest.
- Network Insight Collector-IP kann nicht im vorhandenen Network-Insight-Collector-Profil im NSX-T Manager hinzugefügt werden.
Löschen Sie einen der Collectors aus dem Network-Insight-Collector-Profil im NSX-T Manager und aktivieren Sie NSX-T IPFIX von der Datenquellenseite aus erneut.

- Die verteilte Firewall ist in NSX-T Manager deaktiviert.

Melden Sie sich bei NSX-T Manager an und aktivieren Sie die DFW-Firewall.

Wenn in NSX-T 2.4 die Flows in vRealize Network Insight nach dem Aktivieren von IPFIX auf NSX-T nicht sichtbar sind, können folgende Ereignisse eintreten:

- Die Konfiguration des IPFIX-Collectors für Network Insight ist im Profil des NSX-T Manager-Collectors nicht vorhanden.
- Das DFW-IPFIX-Profil ist in NSX-T Manager nicht vorhanden.

Diese Probleme können Sie durch erneutes Aktivieren von DFW-IPFIX beheben.

Hinweis Alle in NSX-T vorhandenen logischen Switches werden innerhalb von 10-15 Minuten im IPFIX-Profil angehängt.

Flow-Unterstützung für physische Server

vRealize Network Insight unterstützt das Gerät, das die NetFlow-Daten der Versionen v5, v7 und v9 sendet. Wenn die DNS-Zuordnung und die Subnetz-VLAN-Zuordnungsinformationen bereitgestellt werden, kann vRealize Network Insight die NetFlow-Daten mit DNS-Domänen, DNS-Hostnamen, Subnetzen und Schicht-2-Netzwerken anreichern. Diese Funktion ist nur für Benutzer der Enterprise-Lizenz verfügbar.

Führen Sie die folgenden Schritte aus, um NetFlow in vRealize Network Insight zu konfigurieren:

- 1 [Hinzufügen eines physischen Flow-Collectors für NetFlow und sFlow.](#)
- 2 [Konfigurieren eines NetFlow-Collectors in einem physischen Gerät.](#)
- 3 [Importieren der DNS-Zuordnungsdatei.](#)
- 4 [Konfigurieren der Zuordnung zwischen Subnetz und einem VLAN.](#)

Konfigurieren eines NetFlow-Collectors in einem physischen Gerät

Um die NetFlow-Informationen an den NetFlow-Collector von vRealize Network Insight zu senden, konfigurieren Sie das physische Gerät manuell. Im Folgenden finden Sie die Schritte für die Konfiguration in den meisten physischen Geräten:

- 1 Erstellen Sie einen Flow-Datensatz.

Die erforderlichen Felder für einen Flow-Datensatz lauten wie folgt:

- Markieren Sie die folgenden Felder als `Match`.
 - `ipv4 protocol`
 - `ipv4 source address`
 - `ipv4 destination address`
 - `transport source-port`

- `transport destination-port`
 - `interface input`
 - Markieren Sie die folgenden Felder als `Collect`.
 - `direction`
 - `counter bytes`
 - `counter packets`
 - `timestamp sys-uptime first`
 - `timestamp sys-uptime last`
 - Markieren Sie das folgende Feld als `Match` oder `Collect`. Ist dies nicht der Fall, überspringen Sie sie.
 - `transport tcp flags`
- 2 Erstellen Sie einen Flow-Exporter.
 - Geben Sie vRealize Network Insight-NetFlow-Proxy-IP und Port 2055 an.
 - 3 Konfigurieren Sie den Flow-Cache wie folgt:
 - Aktive Zeitüberschreitung: 30 Sekunden
 - Inaktive Zeitüberschreitung: 60 Sekunden
 - 4 Erstellen Sie die Flow-Überwachung unter Verwendung des erstellten Flow-Datensatzes und des Flow-Exporters.
 - 5 Konfigurieren Sie die Überwachung auf jeder Schnittstelle.

Voraussetzungen

Beispiel

Die Beispielschritte zum Konfigurieren der physischen Geräte werden in den folgenden Abschnitten bereitgestellt:

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

Hinweis Die Schritte können von Version zu Version und Gerät zu Gerät variieren.

Cisco 4500

- 1 Erstellen des Flow-Datensatzes

```
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 Erstellen des Flow-Exporters

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

3 Erstellen der Flow-Überwachung

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

4 Konfigurieren der Zeitüberschreitungen

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

- 5 Konfigurieren der Flow-Überwachung für jede Schnittstelle im Modus für eingehenden und ausgehenden Datenverkehr oder zumindest im Modus für eingehenden Datenverkehr

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

Cisco Nexus 1000v

- 1 Konfigurieren von Zeitüberschreitungen

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

- 2 Konfigurieren des Exporters

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

- 3 Konfigurieren der Flow-Überwachung für jede Schnittstelle:

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

- 4 Konfigurieren der Flow-Überwachung für jede Schnittstelle im Modus für eingehenden und ausgehenden Datenverkehr oder zumindest im Modus für eingehenden Datenverkehr

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

```
.  
.   
end
```

Cisco Nexus 9000

Hier sind einige Beispiele für Gerätebefehle für Cisco Nexus 9000:

1 Aktivieren der NetFlow-Funktion

```
configure terminal  
  
feature netflow  
  
end
```

2 Erstellen des Flow-Datensatzes

```
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 Erstellen des Flow-Exporters

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

```
source <INTERFACE_NAME>  
end
```

4 Erstellen der Flow-Überwachung für jede Schnittstelle

```
configure terminal  
flow monitor vrni-monitor  
record vrni-record  
exporter vrni-exporter  
end
```

5 Konfigurieren von Zeitüberschreitungen

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

6 Konfigurieren der Flow-Überwachung für jede Schnittstelle im Modus für eingehenden und ausgehenden Datenverkehr oder zumindest im Modus für eingehenden Datenverkehr

```
configure terminal  
interface <INTERFACE_NAME>  
ip flow monitor vrni-monitor input  
end
```

Anreicherung von Flows und IP-Endpoints

Sie können die DNS-Zuordnung und die Subnetz-VLAN-Zuordnungsinformationen über die Benutzeroberfläche importieren.

Die Flow-Informationen sind mit den folgenden Informationstypen, basierend auf dem Import der DNS-Daten und der Spezifikation der Subnetz-VLAN-Zuordnungen, angereichert.

- DNS-Quelldomäne
- DNS-Quellhostname
- DNS-Zieldomäne
- DNS-Zielhostname
- L2-Quellnetzwerk
- Subnetz-Quellnetzwerk
- L2-Zielnetzwerk

- Subnetz-Zielnetzwerk

Die IP-Endpoint-Informationen sind mit den folgenden Informationstypen, basierend auf dem Import der DNS-Daten und der Spezifikation der Subnetz-VLAN-Zuordnungen, angereichert.

- DNS-Domäne
- DNS-Hostname
- FQDN
- L2-Netzwerk
- Subnetz-Netzwerk

Weitere Informationen zur Anreicherung von Flows mit DNS-Informationen finden Sie unter [Importieren der DNS-Zuordnungsdatei](#).

Weitere Informationen zur Anreicherung von Flows mit Subnetz-VLAN-Zuordnungen finden Sie unter [Konfigurieren der Zuordnung zwischen Subnetz und einem VLAN](#).

Hinweis

- Die DNS-Zuordnungen und die Subnetz-Informationen werden nur für die physischen IPs verbessert. Keine Subnetz- oder DNS-Zuordnungsinformationen sind mit einer virtuellen Netzwerkkarte verknüpft.
- Die Informationen werden nur für Flows angereichert, die von vRNI nach dem Importieren dieser Informationen erkannt wurden.

Suchen nach physischen zu physischen Flows

Sie können anhand der folgenden Attribute nach physischen zu physischen Flows suchen:

- DNS-Quellhost
- DNS-Zielhost
- DNS-Quelldomäne
- DNS-Zieldomäne
- Subnetz-Quellnetzwerk
- Subnetz-Zielnetzwerk

Sie können anhand der folgenden Attribute nach Flows Physisch-Physisch suchen. Einige Beispiele für Flow-Suchabfragen unter Verwendung der angereicherten DNS- und Subnetz-VLAN-Zuordnungsinformationen lauten wie folgt:

```
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,12 network of flows where flow type = 'Source is Internet'  
and flow type = 'Destination is Physical'
```

Blockierte und geschützte Flows anzeigen

Die NSX-IPFIX-Integration ermöglicht die Sichtbarkeit der blockierten und geschützten Flows im System.

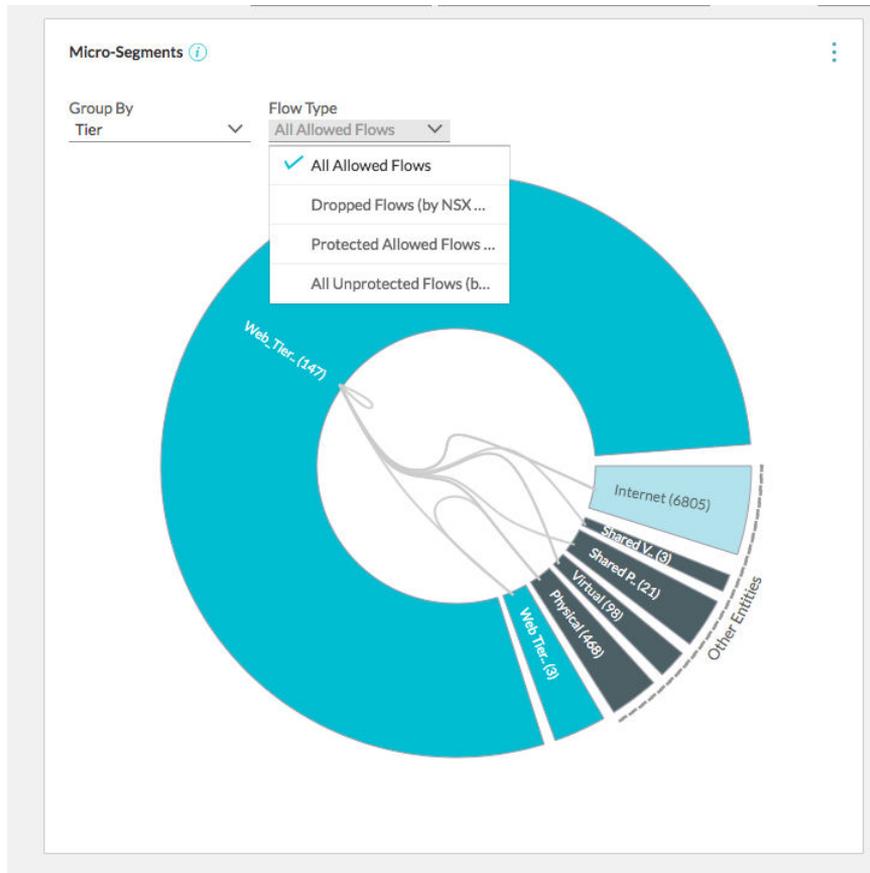
Die grundlegenden Filter auf der Seite „Mikrosegmentierungsplanung“ lauten wie folgt:

- **Alle zulässigen Flows:** Diese Option ist standardmäßig ausgewählt. Um alle Flows anzuzeigen, für die die Aktion in den Firewallregeln auf **Zugelassen** festgelegt ist, wählen Sie diese Option aus.
- **Verworfenne Flows:** Diese Option hilft, die verworfenen Flows zu erkennen und die Sicherheit in einer besseren Art und Weise zu planen.
- **Alle geschützten Flows:** Diese Option hilft dabei, alle Flows zu erkennen, denen eine andere Regel als Typ `any(source)any(dest)any(service)allow` zugeordnet wurde. Solche Flows werden als geschützte Flows bezeichnet.
- **Alle ungeschützten Flows:** Diese Option hilft, alle Flows zu erkennen, denen standardmäßig Regeln des Typs `any(source)any(dest)any(service)allow` zugeordnet wurden. Solche Flows werden als ungeschützte Flows bezeichnet.

Die Firewallregeln werden nur für die zulässigen und ungeschützten Flows angezeigt.

Wenn Sie sich beispielsweise in der Planungsphase befinden und die zulässigen Flows im System anzeigen möchten, führen Sie die folgenden Schritte aus:

- 1 Wählen Sie auf der Seite „Mikrosegmentierungsplanung“ für eine bestimmte Gruppe **Alle zulässigen Flows** aus dem Dropdown-Menü aus.
- 2 Klicken Sie auf die verworfenen Flows im Topologiediagramm, um die entsprechenden empfohlenen Firewallregeln anzuzeigen.
- 3 Implementieren Sie diese Firewallregeln, indem Sie sie in NSX Manager exportieren.



Netzwerkadressübersetzung (NAT)

vRealize Network Insight unterstützt statisches NAT (SNAT), dynamisches NAT (DNAT), reflexive Regeln in den Flows und den VM-VM-Pfad für NSX-V, NSX-T-Edges, Fortinet und Check Point.

Die NAT-Flow-Unterstützung in vRealize Network Insight ist wie folgt:

- vRealize Network Insight unterstützt die verschachtelte NAT-Hierarchie für NSX for vSphere und NSX-T und für physische Geräte, vRealize Network Insight unterstützt die einzelne Hierarchie (DNAT) nur für Fortinet.
- vRealize Network Insight unterstützt die Edges und die Ebenenrouter mit NAT-definierten Uplinks.

Hinweis Die NAT-Regeln auf der NSX Edge Version 5.5 oder den vorherigen Versionen werden nicht unterstützt.

- vRealize Network Insight unterstützt SNAT-Regeln mit Bereich. DNAT muss jedoch eine 1:1-Zuordnung zwischen den Ziel- und den übersetzten IP-Adressen (Parität mit NSX for vSphere) sein.
- Für Check Point werden sowohl automatisch als auch manuell generierte NAT-Regeln sowohl für die Quelle als auch für das Ziel als Netzwerk, Netzwerkgruppe oder Adressbereich unterstützt.

Verwenden Sie die folgenden Abfragen, um NAT-Regeln anzuzeigen:

- Um alle NAT-Regeln in NSX-T anzuzeigen, verwenden Sie die Abfrage `NSX-T Edge NAT Rule`.
- Um alle NAT-Regeln in NSX-V anzuzeigen, verwenden Sie die Abfrage `Edge NAT Rules`.
- Um alle NAT-Regeln in Fortinet anzuzeigen, verwenden Sie die Abfrage `Fortinet NAT Rule`.
- Um alle NAT-Regeln in Check Point anzuzeigen, verwenden Sie die Abfrage `Check Point NAT Rule`.
- Um alle NAT-Regeln anzuzeigen, verwenden Sie die Abfrage `NAT Rule`.

Abfragen

Verwenden Sie die folgenden Abfragen, um NAT-Regeln anzuzeigen:

- Um alle NAT-Regeln in NSX-T anzuzeigen, verwenden Sie die Abfrage `NSX-T Edge NAT Rule`.
- Um alle NAT-Regeln in NSX-V anzuzeigen, verwenden Sie die Abfrage `Edge NAT Rules`.
- Um alle NAT-Regeln in Fortinet anzuzeigen, verwenden Sie die Abfrage `Fortinet NAT Rule`.
- Um alle NAT-Regeln in Check Point anzuzeigen, verwenden Sie die Abfrage `Check Point NAT Rule`.
- Um alle NAT-Regeln anzuzeigen, verwenden Sie die Abfrage `NAT Rule`.

Überlegung

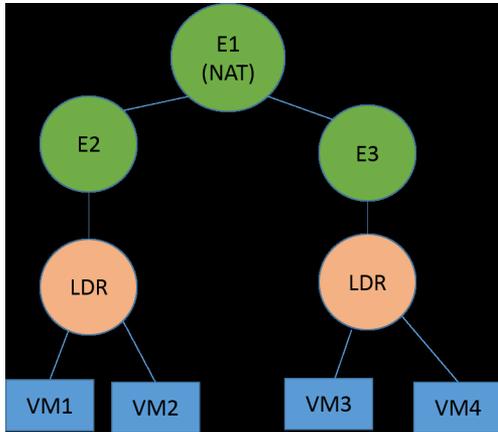
- vRealize Network Insight unterstützt die folgenden Anwendungsfälle nicht:
 - In NSX-T können NAT-Regeln auf Dienstebene angewendet werden. Beispielsweise ist in NSX-T der L4-Port-Satz ein Dienstyp und die zugehörigen Protokolle können TCP oder UDP sein. Folglich werden die Details der Dienstebene im VM-VM-Pfad nicht unterstützt.
 - Jede Übersetzung auf Portebene wird nicht unterstützt.
 - Die Zieladresse der SNAT-Übereinstimmung und die Quelladresse der DNAT-Übereinstimmung werden nicht unterstützt. Verwenden Sie die Zieladresse der SNAT-Übereinstimmung als Ziel-IP-Adresse, wenn Sie die SNAT-Regel festlegen. Verwenden Sie die Quelladresse der DNAT-Übereinstimmung als Quell-IP-Adresse, wenn Sie die DNAT-Regel angeben. Wenn beispielsweise eine in der SNAT-Regel erwähnte Ziel-IP-Adresse vorhanden ist, wendet vRealize Network Insight die SNAT-Regel an, unabhängig davon, ob das Paket die Zieladresse als Ziel-IP-Adresse aufweist.
 - Die NSX-T Edge-Firewall hat Auswirkungen auf den Datenpfad, wenn sie mit dem NAT-Dienst auf demselben logischen Router aktiviert ist. Wenn ein Flow sowohl mit der NAT- als auch der Edge-Firewall übereinstimmt, hat das NAT-Lookup-Ergebnis Vorrang vor der Firewall. Daher wird die Firewall nicht auf diesen Flow angewendet. Wenn der Flow nur mit einer Firewallregel übereinstimmt, wird das Ergebnis der Firewallsuche für diesen Flow berücksichtigt.

- Dienstübersetzung wird nicht unterstützt.
- vSEC NAT wird nicht unterstützt.

Unterstützung für NAT-Flow – Beispiele

Dieser Abschnitt enthält einige Beispiele für den unterstützten NAT-Flow in vRealize Network Insight.

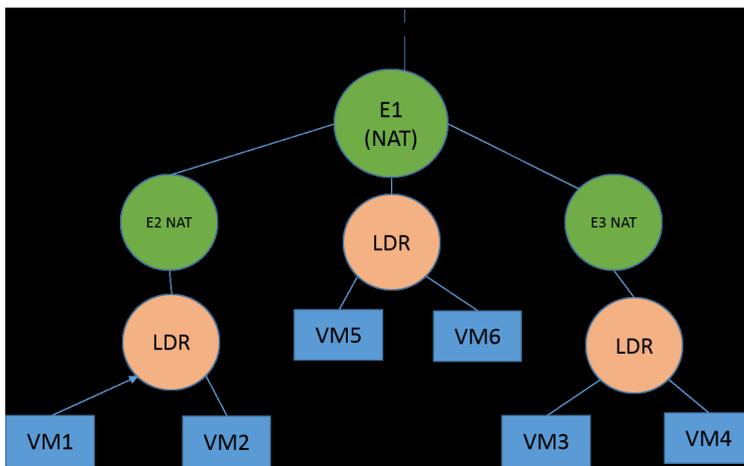
Beispiel 1



In der obigen Topologie sind E2, E3, LDRs, VMs (VM1, VM2, VM3, VM4) Teil der NAT-Domäne E1. Alles über E1, wie z. B. Uplink von E1, ist Teil der NAT-Standarddomäne. Die obige Topologie besteht aus Folgendem:

Der Flow von VM1 zu VM2 und umgekehrt wird in vRealize Network Insight berichtet. Ebenso wird der Flow von VM3 zu VM4 und umgekehrt berichtet.

Beispiel 2



Die obige Topologie besteht aus Folgendem:

- VM1 und VM2 sind Teil der E2-Domäne.

- VM3 und VM4 sind Teil der E2-Domäne.
- E2- und E3-NAT-Domänen sind untergeordnete Domänen der E1-NAT-Domäne.
- E1 ist das einzige untergeordnete Element der NAT-Standarddomäne.
- VM5 und VM6 sind Teil der E1-NAT-Domäne.

In der obigen Topologie werden die folgenden Flows in vRealize Network Insight gemeldet:

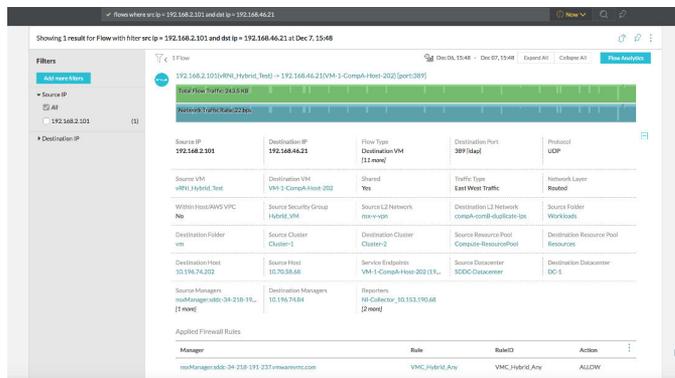
- Flow von VM5 zu VM6,
- Flow von (VM1, VM2) nach (VM3, VM4).

VMware Cloud on AWS Flows

Wenn Sie IPFIX auf der Datenquelle auf der Seite **Einstellungen** aktiviert haben, können Sie die Flow-Anzahl und die letzte Erfassungszeit anzeigen.

Sie können nach einem bestimmten Flow suchen und die mit den Einheiten verknüpften Details abrufen. Beispielsweise können Sie das Richtliniensegment und die Informationen der Richtliniengruppe in *Source L2 Network* und *Source Security Group* anzeigen. Sie können auch die Richtlinien-Firewallregel anzeigen, die mit dem Flow verknüpft ist.

vRealize Network Insight unterstützt die Hybrid-Flows über das VPN. Die Flow-Informationen sind mit den Quell- und Zieleinheiten angereichert.



Hinweis Wenn Sie VMware Cloud on AWS von Version 1.8 auf 1.9 aktualisiert haben, werden die Flows möglicherweise zweimal auf der Benutzeroberfläche angezeigt.

Erstellen eines VPC-Flow-Protokolls

Mit VPC-Flow-Protokollen (Virtual Private Cloud) können Sie Informationen über den IP-Datenverkehr zu und von den Netzwerkschnittstellen in Ihrem VPC erfassen.

Flow-Protokolle können Sie über das AWS-Portal erstellen.

Verfahren

- 1 Melden Sie sich bei der AWS-Konsole an.

- 2 Geben Sie im Textfeld **Dienst suchen CloudWatch** ein und wählen Sie es aus.
- 3 Klicken Sie auf **Protokolle > Aktion > Protokollgruppe erstellen**.
Das Fenster **Protokollgruppe erstellen** wird angezeigt.
- 4 Geben Sie im Feld **Gruppennamen erstellen** einen Gruppennamen ein und klicken Sie auf **Protokollgruppe erstellen**.
- 5 Klicken Sie im oberen Navigationsbereich auf **Dienst**. Geben Sie dann **VPC** ein und wählen Sie es aus.
- 6 Klicken Sie auf der Seite **VPC-Dashboard** auf **Ihre VPCs**.
- 7 Wählen Sie die VPC aus, die Sie ändern möchten, und klicken Sie auf **Flow-Protokolle > Flow-Protokoll erstellen**.
- 8 Konfigurieren Sie im Fenster **Flow-Protokoll erstellen** das Flow-Protokoll:

Option	Aktion
Filtern	Wählen Sie eine der folgenden Optionen aus: Akzeptieren , Ablehnen oder Alle .
Ziel	Klicken Sie auf An CloudWatch-Protokolle senden .
Zielprotokollgruppe	Wählen Sie die Protokollgruppe aus, die Sie erstellt haben.

- 9 Klicken Sie auf **Berechtigungen einrichten**.
Das System öffnet die Seite **VPC-Flow-Protokolle fordert die Berechtigung zum Verwenden der Ressourcen in Ihrem Konto an**.
- 10 IAM-Rolle erstellen.
 - a Klicken Sie auf der Seite **VPC-Flow-Protokolle fordert die Berechtigung zum Verwenden der Ressourcen in Ihrem Konto an** in der **IAM-Rolle** auf **Neue IAM-Rolle erstellen**.
 - b Geben Sie im Feld **Rollename** einen Rollennamen ein.
 - a Klicken Sie auf **Zulassen**.
- 11 Wählen Sie auf der Seite **Flow-Protokoll erstellen** im Dropdown-Menü **IAM-Rolle** die Rolle aus, die Sie erstellt haben.
- 12 Klicken Sie auf **Erstellen**.

Ergebnisse

Das Flow-Protokoll beginnt mit der Veröffentlichung in der ausgewählten Protokollgruppe. Weitere Informationen über VPC-Flow-Protokolle finden Sie in der AWS-Dokumentation unter <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#create-flow-log>.

Senden von Flow-Datensätzen von F5 an vRealize Network Insight-Collectors

Um die Flow-Datensätze zu senden, müssen Sie die folgenden Schritte ausführen:

Lfd. Nr.	Aufgabe	Link
1	Erstellen Sie einen Pool von IPFIX-Collectors, um die IPFIX-Protokollmeldungen vom BIG-IP-System zu empfangen.	Erstellen eines Pools mit IPFIX-Collectors
2	Erstellen Sie ein Protokollziel, um die Protokolle in IPFIX-Vorlagen zu formatieren.	Erstellen eines IPFIX-Protokollziels
3	Erstellen Sie einen Protokollherausgeber, um Protokolle an die angegebenen Protokollziele zu senden.	Erstellen eines Protokollherausgebers
4	Erstellen Sie eine iRule, um die Flow-Informationen an den konfigurierten vRealize Network Insight-Collector zu senden.	Erstellen von iRules
5	Fügen Sie die iRule zu einer Konfiguration des virtuellen Servers hinzu, damit die iRule den gesamten Netzwerkdatenverkehr des virtuellen Servers analysiert.	Hinzufügen der iRule zu einem virtuellen Server
6	Wenn die Collector-VM über F5 nicht erreichbar ist, müssen Sie einen Routeneintrag für den Collector erstellen, um die Flow-Datensätze zu senden.	Erstellen eines Routeneintrags

Erstellen eines Pools mit IPFIX-Collectors

Erstellen Sie einen Pool von IPFIX-Collectors. Das BIG-IP-System sendet IPFIX-Protokollmeldungen an diesen Pool.

Verfahren

- 1 Melden Sie sich bei einer F5-Konsole an.
- 2 Klicken Sie auf **Hauptmenü > Lokaler Datenverkehr > Pools > Pool-Listen > Erstellen**.
Der Bildschirm **Neuer Pool** wird geöffnet.
- 3 Geben Sie im Textfeld **Name** einen eindeutigen Namen für den Pool ein.
- 4 Wählen Sie in **Systemüberwachung** das Element **gateway_icmp** aus und verschieben Sie es in das Feld **Aktiv**.

- 5 Konfigurieren Sie im Abschnitt **Neues Mitglied** die Collector-IP-Adresse und klicken Sie auf **Hinzufügen**.

Option	Aktion
Knotenname	Geben Sie die Collector-IP-Adresse ein.
Dienstport	2055

- 6 Klicken Sie auf **Fertigstellen**.

Erstellen eines IPFIX-Protokollziels

Erstellen Sie ein Protokollziel, um die Protokolle in IPFIX-Vorlagen zu formatieren. Nach der Formatierung werden diese Protokolle an den IPFIX-Collector gesendet.

Verfahren

- 1 Klicken Sie in der F5-Konsole auf **Hauptmenü > System > Protokolle > Konfiguration > Protokollziele > Erstellen**.

Der Bildschirm **Protokollziele** wird angezeigt.

- 2 Geben Sie im Textfeld **Name** einen eindeutigen Namen ein.
- 3 Klicken Sie in der Liste **Typ** auf **IPFIX**.
- 4 Konfigurieren Sie die **IPFIX-Einstellungen**.

Option	Aktion
Protokoll	Klicken Sie auf Netflow V9 .
Poolname	Klicken Sie auf den Poolnamen, den Sie im vorherigen Schritt erstellt haben.

- 5 Klicken Sie auf **Fertigstellen**.

Erstellen eines Protokollherausgebers

Um die Protokolle an ein bestimmtes Protokollziel zu senden, müssen Sie einen Protokollherausgeber erstellen.

Verfahren

- 1 Klicken Sie in der F5-Konsole auf **Hauptmenü > System > Protokolle > Konfiguration > Protokollherausgeber > Erstellen**.

Der Bildschirm **Protokollherausgeber** wird angezeigt.

- 2 Geben Sie im Feld **Name** einen eindeutigen Namen ein.
- 3 Wählen Sie im Feld **Ziel** das Protokollziel aus, das Sie zuvor über das Feld **Verfügbar** erstellt haben, und verschieben Sie es in das Feld **Ausgewählt**.
- 4 Klicken Sie auf **Fertigstellen**.

Erstellen von iRules

Um die Flow-Informationen an den konfigurierten vRealize Network Insight-Collector zu senden, müssen Sie iRules erstellen. Sie müssen zwei iRules erstellen: eine iRule für das TCP-Protokoll und die andere für das UDP-Protokoll.

Verfahren

- 1 Klicken Sie in der F5-Konsole auf **Hauptmenü > iRules > iRule-Liste > Erstellen**.
Der Bildschirm **Neue iRule** wird angezeigt.
- 2 Geben Sie im Textfeld **Name** einen eindeutigen Namen ein.
- 3 Geben Sie im Textfeld **Definition** die TCP-Regeln für das TCP-Protokoll und die UDP-Regel für das UDP-Protokoll ein. Informationen zu Regeln finden Sie unter [iRules für TCP- und UDP-Protokoll](#).
Stellen Sie sicher, dass die iRule auf den zuvor erstellten Herausgeber verweist.
- 4 Klicken Sie auf **Fertigstellen**.

iRules für TCP- und UDP-Protokoll

Diese dienen zum Erstellen von iRules für das TCP- und das UDP-Protokoll.

TCP-Regel

Verwenden Sie die folgende Regel zum Erstellen einer iRule für das TCP-Protokoll:

Hinweis Stellen Sie sicher, dass die iRule auf den zuvor erstellten Protokollherausgeber verweist.

```
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-Regel

Verwenden Sie die folgende Regel zum Erstellen einer iRule für das UDP-Protokoll:

Hinweis Stellen Sie sicher, dass die iRule auf den zuvor erstellten Protokollherausgeber verweist.

```

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
    }
}
}

```

Hinzufügen der iRule zu einem virtuellen Server

Verfahren

- 1 Klicken Sie in der F5-Konsole auf **Hauptmenü > Virtueller Server > Virtuelle Serverliste**.
Der Bildschirm **Virtuelle Serverliste** wird angezeigt.
- 2 Wählen Sie den Server aus, dem Sie die iRule hinzufügen möchten.
- 3 Klicken Sie auf die Registerkarte **Ressourcen** und dann im Abschnitt „iRule“ auf **Verwalten**.
- 4 Wählen Sie die TCP- und UDP-iRules aus, die Sie zuvor erstellt haben, und verschieben Sie die iRules vom Feld **Verfügbar** in das Feld **Aktivieren**.
- 5 Klicken Sie auf **Fertigstellen**.

Erstellen eines Routeneintrags

Die Collector-VM muss über F5 erreichbar sein. Ist die Collector-VM nicht über F5 erreichbar, müssen Sie einen Routeneintrag für den Collector erstellen.

Um zu prüfen, ob die Collector-VM über F5 erreichbar ist, müssen Sie den folgenden Befehl über die Befehlszeilenschnittstelle (CLI) ausführen: `ping <collector-ip> -I <virtual interface>`. Wenn der Collector über F5 nicht erreichbar ist, müssen Sie einen Routeneintrag für den Collector erstellen.

Beispiel:

```
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
```

Verfahren

- 1 Klicken Sie in der F5-Konsole auf **Hauptmenü > Netzwerk > Routen > Hinzufügen**.
Der Bildschirm **Neue Route** wird angezeigt.
- 2 Konfigurieren Sie im Abschnitt **Eigenschaften** die Routeneinträge zum Senden von Flow-Datensätzen von F5 aus über den virtuellen Server an den vRealize Network Insight-Collector.

Informationen zu Geltungsbereichen und Flows in Kubernetes und VMware PKS

11

In vRealize Network Insight können Sie Geltungsbereiche für Containereinheiten definieren und die Flow-Informationen anzeigen.

Informationen zu Flows in VMware PKS und Kubernetes

vRealize Network Insight unterstützt die folgenden Flow-Typen für Kubernetes-Einheiten.

- VM zu Kubernetes-Pod
- Kubernetes-Pod zu Pod
- Ziel ist Kubernetes-Pod
- Quelle ist Kubernetes-Pod

Mithilfe dieser Flow-Typen können Sie nach bestimmten Kubernetes-Einheiten suchen.

Beispiel: `flows where flow type = x`, wobei `x` einer der Flow-Typen ist

vRealize Network Insight kann Flow-Informationen wie Metriken, Zeitreihen und Relationen für alle Einheiten bereitstellen, einschließlich der Details zu Containerquelle und -ziel und deren Einheiten.

Darüber hinaus können Sie die Flows, die die meiste Bandbreite verbrauchen, nach Kubernetes-Cluster, -Namespace, -Dienst und -Knoten auf dem Flow-Analyse-Dashboard anzeigen.

Planung und Mikrosegmentierung von Kubernetes-Einheiten

Sie können einen bestimmten Typ von Kubernetes-Einheiten planen, indem Sie auf der Seite „Sicherheit planen“ Kubernetes-Cluster, Kubernetes-Dienst, Kubernetes-Namespace oder Kubernetes-Knoten als Geltungsbereich und Mikrosegmente auswählen. Darüber hinaus können Sie Daten für die Anwendung planen oder analysieren und Gruppierungen auf der Basis von Kubernetes-Einheiten definieren, um die Informationen zum Anwendungs-Flow anzuzeigen.

Außerdem können Sie auf der Seite „Sicherheit planen“ die empfohlenen Firewallregeln im Zusammenhang mit Kubernetes-Einheiten im YAML-Format aus Mikrosegmenten exportieren.

Hinweis Den Geltungsbereich einer Anwendung können Sie nicht in das YAML-Format exportieren, wenn er VMs oder VM-Mitglieder enthält. Wenn die Anwendung nur Containereinheiten enthält, ist der Export in das YAML-Format verfügbar.

Anzeigen von Details zu Einheiten

12

Die Einheitsseiten bieten einen umfassenden Überblick über die Einheiten, die in Ihrem Datacenter vorhanden sind. Diese Informationen reichen von detaillierten Topologien zur Anzeige von Beziehungen zu anderen Einheiten Ihres Datacenters bis hin zu detaillierten Metriken für eine bestimmte Einheit.

Jede Einheitsseite besteht aus einer Sammlung von Widgets und in jedem Widget werden bestimmte Informationen im Zusammenhang mit der Einheit angezeigt. Die bereitgestellten Informationen sind sowohl in Echtzeit als auch historisch und bieten eine erschöpfende Liste mit Metriken und Eigenschaften für die Einheit.

Wenn Sie weitere Informationen zu Einheiten anzeigen möchten, klicken Sie in der oberen rechten Ecke der Seite auf **Profil > Hilfe**.

Zeitlinie

Die Zeitlinie bietet Ihnen die folgenden Informationen:

- Status des Datacenters zu einem bestimmten Zeitpunkt in der Vergangenheit.
- Gesamtüberblick über die Ereignisse, die innerhalb eines ausgewählten Zeitraums erkannt wurden.

Wählen Sie den Zeitraum innerhalb der Zeitlinie aus, die Sie anzeigen möchten.

Um eine bestimmte Zeitlinie anzuzeigen, wählen Sie den Zeitbereich mit der Option **Zeitbereich** aus.

Widget „Eigenschaft“

In den Eigenschafts-Widgets werden wichtige Attribute in einem zweispaltigen Layout angezeigt. Einige Eigenschaftspins zeigen möglicherweise auch nur einen singulären Attributwert an. Ein Beispiel für einen Eigenschaftspin ist der Pin **VM-Eigenschaften**. Der **VM-Eigenschaft**-Pin zeigt die Eigenschaften einer VM an, z. B. Betriebssystem, IP-Adresse, Standard-Gateway, logische Switches, CPU, Arbeitsspeicher, Betriebszustand usw.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen von Details zum vRealize Network Insight-System \(NI-System\)](#)

- Anzeigen der Details zur Plattform-VM
- Anzeigen von Details der Collector-VM
- Anzeigen der Details zu VMware vCenter-Datenquellen
- Anzeigen der PCI-Übereinstimmungsdetails
- Anzeigen von Kubernetes-Details
- Anzeigen von Details zum Lastausgleichsdienst
- Anzeigen von VM-Details
- Anzeigen der Details für Edge-Geräte
- Anzeigen von NSX Manager-Details
- Anzeigen der Details für **VMware NSX-T Manager**
- Anzeigen von Details zum **NSX-T-Verwaltungsknoten**
- Anzeigen von NSX-T-Transportdetails
- Anzeigen von Details zum virtuellen Server
- Anzeigen der Details zu Poolmitgliedern
- Anzeigen von Details zu Microsoft Azure
- Anzeigen von VeloCloud Enterprise-Details
- Anzeigen von Details zur SD-WAN- und Edge-SD-WAN-Anwendung
- Anzeigen von Details zur **SD-WAN-Bewertung**
- Anzeigen der Details zur **VeloCloud-Link-Anwendung**
- Anzeigen von Details zu **VeloCloud-Geschäftsrichtlinien**
- Anzeigen der VMC-SDDC-Details
- Anzeigen der Details für **Arista-Hardware-Gateway** und **Gateway-Bindung der Arista-Hardware**
- Anzeigen von Details zum **Cisco-Nexus-Gerät**
- Anzeigen von Flow-Erkennisdetails
- Anzeigen der Details zur Mikrosegmentierung
- Anzeigen von Anwendungsdetails
- Analyse – Ausreißerererkennung
- Analyse: statische und dynamische Schwellenwerte

Anzeigen von Details zum vRealize Network Insight-System (NI-System)

Die Seite „vRealize Network Insight-System (NI-System)“ enthält einen Snapshot aller Informationen im Zusammenhang mit dem System. So greifen Sie auf die Seite „vRealize Network Insight-System“ zu:

- Klicken Sie auf der Seite **Installation und Unterstützung** neben **Übersicht** auf **Details anzeigen**. Die Seite „NI-System“ wird angezeigt.
- Geben Sie `NI-System` als Suchabfrage an, um die Seite „vRealize Network Insight-System“ anzuzeigen.

Die Seite „NI-System“ ist in drei Abschnitte unterteilt:

- **Übersicht:** Dieser Abschnitt enthält Informationen zu den wichtigsten Eigenschaften, den Datenquellen, den offenen Problemen und allen Änderungen und Problemen im Zusammenhang mit dem System. Zeigen Sie die Details der einzelnen Datenquellen an, indem Sie draufklicken.
- **Ereignisse:** In diesem Abschnitt werden alle Probleme und Änderungen im System, Datenquellen, Plattformen und die Collectors aufgelistet.
- **Plattformen und Collectors:** In diesem Abschnitt werden alle Plattformen und die Collectors aufgelistet, die dem System zugeordnet sind. Um weitere Details zu einer Plattform oder einem Collector anzuzeigen, klicken Sie drauf.

Anzeigen der Details zur Plattform-VM

Auf der Seite **Plattform-VM** finden Sie einen Snapshot der Eigenschaften, Änderungen und Probleme eines bestimmten Plattformknotens.

Auf der Seite **Plattform-VM** sehen Sie Folgendes:

- Wichtige Informationen über den ausgewählten Plattformknoten, wie z. B. Name, IP-Adresse, CPU-Kerne, Arbeitsspeicher, Zeitpunkt der letzten Aktualisierung und Version.
- Offene Probleme im Zusammenhang mit den Plattformen
- Liste der Ereignisse in Bezug auf den ausgewählten Plattformknoten
- Die grafische Darstellung der Metriken wie CPU-Auslastung, Arbeitsspeichernutzung und Datenfestplattennutzung

Anzeigen von Details der Collector-VM

Auf der Seite **Collector-VM** finden Sie einen Snapshot der Eigenschaften, Änderungen und Probleme eines bestimmten Collector-Knotens.

Auf der Seite **Collector-VM** sehen Sie Folgendes:

- Wichtige Informationen über den ausgewählten Plattformknoten, wie z. B. Name, IP-Adresse, CPU-Kerne, Arbeitsspeicher, Zeitpunkt der letzten Aktualisierung und Version.

- Anzahl der offenen Probleme im Zusammenhang mit dem Collector und Details zu diesen Problemen.
- Anzahl der offenen Probleme im Zusammenhang mit den Datenquellen und Details zu diesen Problemen.
- Liste der Änderungen in der Datenquelle, die in den letzten sieben Tagen aufgetreten sind.
- Details der Datenquellen und der im Collector verfügbaren NetFlow-Reporter. Die Anzahl der Flows wird für jeden NetFlow-Reporter angezeigt. Für Datenquellen wird die Anzahl der Flows und der ermittelten VMs angezeigt.
- Die grafische Darstellung der Metriken wie CPU-Auslastung, Arbeitsspeichernutzung und Datenfestplattennutzung.

Anzeigen der Details zu VMware vCenter-Datenquellen

Die Seite **VMware vCenter-Datenquelle** enthält einen Snapshot mit Eigenschaften, Änderungen und Problemen einer bestimmten Datenquelle.

Auf der Seite „VMware vCenter-Datenquelle“ sehen Sie Folgendes:

- Wichtige Informationen zur ausgewählten VMware vCenter-Datenquelle, z. B. IP-Adresse/FQDN, Collector-Name, Aktiviert, Anzahl der erkannten VMs, Status „IPFIX aktiviert“ usw.
- Alle offenen Probleme, die der Datenquelle zugeordnet sind.
- Alle Änderungen und Probleme, die in den letzten sieben Tagen in einer bestimmten Datenquelle aufgetreten sind.

Anzeigen der PCI-Übereinstimmungsdetails

Die Seite **PCI-Übereinstimmung** ist nur für Benutzer der Enterprise-Lizenz verfügbar.

Zugriff auf die PCI-Übereinstimmung

- 1 Wählen Sie im Navigationsbereich links auf der Startseite **Sicherheit > PCI-Übereinstimmung** aus.
- 2 Das Fenster **PCI-Übereinstimmung** wird geöffnet. Wählen Sie den erforderlichen Geltungsbereich, die entsprechende Einheit und die Dauer aus, für die Sie die Daten benötigen. Klicken Sie auf **Zugreifen**.
- 3 Die Seite **PCI-Übereinstimmung** wird geöffnet.

Details zur Seite „PCI-Übereinstimmung“

Auf der Seite **PCI-Übereinstimmung** können Sie die Übereinstimmung mit den PCI-Anforderungen nur in der NSX-Umgebung bewerten. Diese Anforderungen werden unter dem ersten Pin im Dashboard erwähnt. Die restlichen Pins im Dashboard, die Daten für die Bewertung dieser Anforderungen bereitstellen, lauten wie folgt:

- **Netzwerkflussdiagramm:** Es zeigt den Datenfluss, Firewalls, Verbindungen sowie sonstige Details im Zusammenhang mit einem Netzwerk an.
- **Flows:** es listet die Flows auf, die Sie im Netzwerkflussdiagramm sehen.
- **Klartextprotokoll-Flows basierend auf dem Zielport:** Der Datenverkehr, der auf bestimmten Ports fließt, ist im Klartext. Dieser Pin zeigt die Klartextprotokoll-Flows basierend auf einem bestimmten Zielport an.
- **Virtuelle Maschinen im Geltungsbereich:** Zeigt die virtuellen Maschinen im Geltungsbereich an, den Sie für die Abfrage ausgewählt haben. Dieser Pin zeigt die ausgehenden Regeln, eingehenden Regeln und Sicherheitsgruppen für virtuelle Maschinen in diesem Bereich an.
- **Sicherheitsgruppen von virtuellen Maschinen:** Listet die Sicherheitsgruppen der virtuellen Maschinen auf.
- **Anzahl virtueller Maschinen nach Sicherheitsgruppen:** Sie können die Liste der virtuellen Maschinen in einer Sicherheitsgruppe anzeigen, indem Sie in diesem Pin auf „Anzahl“ klicken.
- **Anzahl virtueller Maschinen nach Sicherheits-Tags:** Sie können die Liste der virtuellen Maschinen mit Sicherheits-Tags anzeigen, indem Sie in diesem Pin auf „Anzahl“ klicken.
- **Auf internen Datenverkehr angewendete Firewallregeln:** Sie können die Firewallregeln für den Datenverkehr zwischen den virtuellen Maschinen innerhalb des ausgewählten Geltungsbereichs anzeigen.
- **Auf eingehenden Datenverkehr angewendete Firewallregeln:** Sie können die Firewallregeln für den Datenverkehr anzeigen, der von einer virtuellen Maschine außerhalb des Geltungsbereichs zu der virtuellen Maschine innerhalb des ausgewählten Geltungsbereichs kommt.
- **Auf ausgehenden Datenverkehr angewendete Firewallregeln:** Sie können die Firewallregeln für den Datenverkehr anzeigen, der zu einer virtuellen Maschine außerhalb des Geltungsbereichs von der virtuellen Maschine innerhalb des ausgewählten Geltungsbereichs geht.
- **Änderungen der Sicherheits-Tag-Mitgliedschaft:** Die Änderungen im Zusammenhang mit der Mitgliedschaft für Sicherheits-Tags werden in diesem Pin angezeigt.
- **Änderungen der Sicherheitsgruppenmitgliedschaft:** Die Änderungen im Zusammenhang mit der Mitgliedschaft in einer Sicherheitsgruppe werden in diesem Pin angezeigt.

- Firewall-Regeländerungen: Die Änderungen, die sich auf eine Firewallregel beziehen, werden in diesem Pin aufgeführt.

Hinweis Wenn NSX geschachtelte Sicherheitsgruppen aufweist, sollte der Geltungsbereich der PCI-Übereinstimmung nicht der Sicherheitsgruppe entsprechen.

Als PDF exportieren

Mit vRealize Network Insight können Sie die Informationen im Dashboard „PCI-Übereinstimmung“ als PDF-Bericht erstellen und exportieren.

Verfahren

- 1 Klicken Sie im Dashboard „PCI-Übereinstimmung“ auf **Als PDF exportieren** rechts oben auf der Seite. Das Fenster „In PDF exportieren“ wird angezeigt.
- 2 Im Fenster „In PDF exportieren“ werden alle Widgets und ihre jeweiligen Eigenschaften aufgelistet, die im Dashboard „PCI-Übereinstimmung“ verfügbar sind. Wählen Sie die Widgets und die Eigenschaften aus, die Sie exportieren möchten.

Hinweis

- Sie müssen mindestens eine Eigenschaft auswählen.
- Die maximale Anzahl der Eigenschaften, die ausgewählt werden können, ist 20.
- Die maximale Anzahl der Einträge in der Listenansicht, die exportiert werden können, ist 100.
- Bei bestimmten Widgets können Sie keine Eigenschaften auswählen. Geben Sie in solchen Fällen nur die Anzahl der Einträge an.

- 3 Geben Sie einen Namen für den PDF-Bericht an.

Hinweis

- Die maximal zulässige Zeichenanzahl für den Berichtsamen ist 200.
- Die maximale Anzahl der Seiten, die im Bericht erstellt werden können, ist 50.

- 4 Klicken Sie auf **Vorschau**. Sie können die Vorschau des vollständigen Berichts anzeigen.
- 5 Klicken Sie auf **PDF exportieren**.

Anzeigen von Kubernetes-Details

Über das Kubernetes-Dashboard können Sie sich einen schnellen Überblick über Ihre Kubernetes- oder VMware PKS-Bereitstellungen in vRealize Network Insight verschaffen.

Sie sehen Details zu:

- Clustern und Namespaces, die die meisten Bandbreite verbrauchen, basierend auf den Flows

- Übersicht über Kubernetes-Clustereinheiten wie z. B. Anzahl der Namespaces, Pods, Dienste und Knoten
- In vRealize Network Insight hinzugefügte Kubernetes-Cluster
- Liste der auf Pods ausgeführten Container-Images und Anzahl der Pods für jedes Container-Image
- Liste der gefundenen neuen Pods, Anzahl, Namespace- und Cluster-Details.

Darüber hinaus können Sie im Dashboard auf die Anzahl der verschiedenen Kubernetes-Einheiten klicken, um die Listenansicht anzuzeigen und zu Details der jeweiligen Einheit zu wechseln.

Tabelle 12-1. Dashboard „Kubernetes-Einheit“

Dashboard	Beschreibung
Dashboard „Cluster“	<p>Sie rufen die Bereitstellungsdetails auf der Clusterebene ab, einschließlich:</p> <ul style="list-style-type: none"> ■ Cluster-Überblick mit der Anzahl der Namespaces, Dienste, Pods und Knoten in der Bereitstellung ■ Liste der Top-Namespaces auf der Basis der Flows ■ Interaktion zwischen Namespaces
Namespace-Dashboard	<p>Sie erhalten die Namespace-Details zum Cluster, wie z. B.:</p> <ul style="list-style-type: none"> ■ Namespace-Übersicht mit der Anzahl der Pods, Dienste und Knoten, die sich im jeweiligen Namespace befinden ■ Liste der Dienste, die die meiste Bandbreite verbrauchen, auf der Basis der Flows ■ Dienstinteraktionen im Namespace ■ Netzwerkdatenverkehr nach Paketen und Byte
Dashboard „Dienste“	<p>Sie sehen die Details der Kubernetes-Dienste, wie z. B.:</p> <ul style="list-style-type: none"> ■ Dienstübersicht, die Informationen zur Anzahl für Folgendes enthält: <ul style="list-style-type: none"> ■ Offene Ereignisse in 24 Stunden ■ Eingehende und ausgehende Flows in 24 Stunden ■ Pods ■ Knoten, auf denen der Dienst bereitgestellt wird ■ Konnektivität zwischen den Kubernetes-Komponenten und NSX-T ■ Anzahl der aktiven Knoten und Pods für einen bestimmten Zeitraum ■ Dienstinteraktion im Namespace ■ Netzwerkdatenverkehr nach Paketen und Byte

Tabelle 12-1. Dashboard „Kubernetes-Einheit“ (Fortsetzung)

Dashboard	Beschreibung
Dashboard „Pods“	Sie sehen Details wie z. B.: <ul style="list-style-type: none"> Cluster, Namespace und Knoten, zu denen der Pod gehört Netzwerkdatenverkehr zwischen Pods auf Basis von Paketen und Byte
Dashboard „Knoten“	Sie sehen Details wie z. B.: <ul style="list-style-type: none"> Liste der Namespaces Liste der Dienste Liste der Container-Pods Netzwerkdatenverkehr zwischen Knoten auf Basis von Paketen und Byte

Hinweis

- vRealize Network Insight erfasst alle 10 Minuten Kubernetes-Clusterdetails von VMware PKS.
- vRealize Network Insight erfasst alle 4 Stunden alle Objekte (Namespace, Knoten, Pod, Dienst) aus dem Kubernetes-Cluster. Wenn es jedoch zu einer Änderung bei den Kubernetes-Objekten kommt, führt vRealize Network Insight die Watch API aus und aktualisiert die Änderungen sofort.
- VMware PKS liefert keine Details zu den primären Kubernetes-Knoten.
- vRealize Network Insight gibt die Details der Cluster an, die sich nur im Status „erfolgreich erstellt“ befinden.

Häufige Ereignisse oder Fehlermeldungen

- `Data Source not reachable` – Pingen Sie die IP/den FQDN des VMware PKS von der virtuellen Proxy-Maschine aus an, um sicherzustellen, dass der VMware PKS erreichbar ist.
- `Kubernetes Cluster API Servers not reachable` – Stellen Sie sicher, dass alle API-Server des Kubernetes-Clusters von der virtuellen Proxy-Maschine aus erreichbar sind.

Anzeigen von Details zum Lastausgleichsdienst

Auf der Seite „Lastausgleichsdienst“ werden alle Informationen der virtuellen Server und der Pools zusammengefasst, die auf dem Lastausgleichsdienst erstellt werden.

Sie sehen die folgenden Informationen:

- Liste der virtuellen Server auf dem Lastausgleichsdienst sowie die zugehörigen Probleme
- Liste der Pools auf dem Lastausgleichsdienst und die zugehörigen Probleme
- Dem Lastausgleichsdienst zugeordnete Ereignisse

- Liste der Flows, Anzahl und Netzwerkdatenverkehr auf verschiedenen Ziel-IPs

Hinweis Für NSX-V-Lastausgleichsdienste werden die Flow-Informationen nicht erfasst.

- Eigenschaften des Lastausgleichsdiensts, der Informationen wie z. B. Anbieter, Typ, Seriennummer, virtuelle Server und Pools bereitstellt.

Anzeigen von VM-Details

Auf der Seite „VM“ erhalten Sie einen detaillierten Überblick über Ihre in vRealize Network Insight verfügbaren VMs.

Auf der Seite „VM“ sehen Sie die folgenden Abschnitte:

Abschnitt	Details
Übersicht	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ VM-Details ■ Topologie-Informationen ■ Diverse Konfigurationsparameter ■ Sicherheitsbezogene Parameter ■ Pfad von der VM zum Internet
Nachbarn	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Grafische Ansicht diverser Metrikeigenschaften im Vergleich zu den benachbarten VMs ■ Liste der VMs, die zu demselben Host gehören
Ereignisse	<p>Sie sehen die Liste der Ereignisse in Bezug auf die ausgewählte VM.</p>
Flows	<p>Sie sehen die Liste der Flows, die entweder erzeugt werden oder versuchen, die ausgewählte VM zu erreichen, für die die Firewallaktion zugelassen und abgelehnt wird.</p>
Metriken	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Die Metrikinformationen in Bezug auf die ausgewählte VM ■ Informationen zur Netzwerknutzung von Ports im Pfad zu ToR ■ Informationen zu allen Metrik-Eigenschaften ■ Informationen zu Eingabe-Ausgabe-Metriken ■ Den Speicherplatz der virtuellen Festplatte ■ Die Datenspeicherleistung <hr/> <p>Hinweis Sie können die Datenspeicher-Metriken einer VM nicht sehen, wenn diese auf dem vSAN-Datenspeicher gehostet wird.</p> <hr/> <ul style="list-style-type: none"> ■ Details zur Latenz der virtuellen Infrastruktur <hr/> <p>Hinweis Um die Latenz der virtuellen Infrastruktur anzuzeigen, muss der Port 1991 auf dem Collector geöffnet sein, damit er Latenzdaten vom ESXi-Host empfangen kann.</p>

Anzeigen der Details für Edge-Geräte

Auf der Seite **VMware Edge-Gerät** erhalten Sie einen Überblick über die VMware Edge-Geräte, die Ihnen in vRealize Network Insight zur Verfügung stehen.

Suchen Sie für den Zugriff auf diese Seite nach **Edge-Gerät** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf der Seite **VMware Edge-Gerät** sehen Sie Folgendes:

Abschnitt	Details
Übersicht	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Eine Übersicht über Ihre Edge-Geräte, einschließlich Ereignisdiagramm, Byte, Pakete, Flows und Sitzungsnummern. ■ Eine Liste der NSX Edge-Eigenschaften, NSX Edge-Dienste und NSX Edge-Appliance-VMs. ■ Die Topologiedetails.
Ereignis	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Eine Liste mit Details zu verschiedenen Ereignissen.
Flows	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Verschiedene Flow-Analysen, z. B. Gesamtzahl der Byte, die durch NSX Edge fließen, Gesamtzahl der Pakete, die NSX Edge durchlaufen, Gesamtzahl der Flows und Gesamtzahl der Sitzungen über NSX Edge.
Metriken	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Verschiedene Metriken, wie z. B. die CPU-Auslastung und die Arbeitsspeicher- und Netzwerknutzung von NSX Edge-Appliance-VMs und die Netzwerknutzung pro vNIC von NSX Edge.

Überlegung

In seltenen Fällen kann es vorkommen, dass Sie auf der Seite **VMware Edge-Gerät** falsche Flow-Informationen erhalten, wenn Folgendes zutrifft:

- Die IP einer VM ist vRealize Network Insight unbekannt.
- Das Standard-Gateway ist in einer VM falsch konfiguriert.
- Es gibt mehr als zwei Edge Hops für den vertikalen Flow von einer VM.
- Edge gehört zu einem ECMP-Cluster (Equal Cost Multi Path Routing).
- Edge ist mit einem universellen logischen verteilten Router verbunden.

Anzeigen von NSX Manager-Details

Auf der Seite **NSX Manager** erhalten Sie einen detaillierten Überblick über Ihre in vRealize Network Insight verfügbaren NSX Manager.

Vorgehensweise zum Zugreifen auf die Seite NSX Manager

Suchen Sie für den Zugriff auf diese Seite nach `NSX Manager where SDDC Type = 'VMC'` und klicken Sie in der Suchergebnisliste auf die **NSX Manager**-Seite, die angezeigt werden soll.

Übersicht

Auf der Seite **NSX Manager** sehen Sie den folgenden Abschnitt:

Tabelle 12-2.

Abschnitt	Details
Übersicht	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Übersicht über NSX-Richtlinieneinheiten ■ In den letzten 24 Stunden geänderte Einheiten ■ Top-Flows nach Regel ■ Liste der Router <hr/> <p>Hinweis Die Anzahl der im Widget Übersicht über NSX-Richtlinieneinheiten und im Widget Einheiten in den letzten 24 Stunden angezeigten Einheiten kann voneinander abweichen. Wenn einige der in den letzten 24 Stunden erkannten Einheiten gelöscht wurden, kann die Anzahl der im Widget Einheiten in den letzten 24 Stunden angezeigten Einheiten größer sein als die Anzahl der im Widget Übersicht über NSX-Richtlinieneinheiten angezeigten Einheiten.</p>
Top-Kommunizierer	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Meistkommunizierende Einheiten in Ihrer Umgebung
Netzwerkdatenverkehr und -ereignisse	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Details zur Übersicht über Netzwerkdatenverkehr und -warnungen ■ Ereignisliste

Anzeigen der Details für VMware NSX-T Manager

Auf der Seite **VMware NSX-T Manager** erhalten Sie einen Überblick über Ihren in vRealize Network Insight verfügbaren VMware NSX-T Manager.

Suchen Sie für den Zugriff auf diese Seite nach **NSX-T Manager** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf der Seite „NSX Manager“ sehen Sie Folgendes:

Abschnitt	Details
Übersicht	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Eine Übersicht über Ihren NSX-T Manager, einschließlich Ereignisdiagramm, Anzahl der Firewallregeln, IPSET, Transportzonen, Anwendungen und ungeschützter Flows, und Flow-Volumen in den letzten 24 Stunden. ■ Liste der Eigenschaften, Firewallregeln nach Trefferanzahl, Top-Flows nach Regel und Berechnungsmanager. ■ Die Topologiedetails. Topologie bietet eine kontextbezogene Ansicht der Einheiten und zeigt auch Ereignisse an, die mit den Einheiten verknüpft sind.
Ereignis	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Liste der verschiedenen Ereignisse und Ereignisse in Bezug auf den Schwellenwert von Analysefunktionen.
Flows	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Verschiedene Flow-Analysen.
Metriken	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Details zum Systemzustand des NSX-T-Verwaltungsknotens. <p>Hinweis Die Systemzustandsdetails des NSX-T-Verwaltungsknotens sind nur für NSX-T Version 2.4.0 und höher verfügbar.</p>

Anzeigen von Details zum NSX-T-Verwaltungsknoten

Auf der Seite **NSX-T-Verwaltungsknoten** erhalten Sie einen Überblick über die in vRealize Network Insight verfügbaren Details zu VMware NSX-T-Verwaltungsknoten.

Suchen Sie für den Zugriff auf diese Seite nach **NSX-T-Verwaltungsknoten** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf dieser Seite sehen Sie Folgendes:

Abschnitt	Details
Übersicht	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Zusammenfassung Ihres NSX-T-Verwaltungsknotens, einschließlich Eigenschaftsdetails, Systemmetriken und Dienststatus.
Ereignis	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit verschiedenen Ereignissen.
Schnittstellenstatistiken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Schnittstellenstatistiken, einschließlich empfangener Pakete, übertragener Pakete, verloren gegangener empfangener und übertragener Pakete usw.
Systemstatistiken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Systemstatistiken, einschließlich Systemlast, Systemnutzung und Dateisystemnutzung.

Anzeigen von NSX-T-Transportdetails

Auf der Seite **NSX-T-Transportknoten** erhalten Sie einen Überblick über die in vRealize Network Insight verfügbaren Transportknoten-Details. Sie können sowohl Hostknoten- als auch Edge-Knoten-Details in vRealize Network Insight anzeigen.

Seite NSX-T-Transportknoten, wobei der Knotentyp „Host“ lautet

Suchen Sie für den Zugriff auf diese Seite nach **NSX-T Transport Node where Node Type = 'HostNode'** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf dieser Seite sehen Sie Folgendes:

Abschnitt	Details
Übersicht	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Übersicht über Ihren Host-Transportknoten, einschließlich Ereignisdiagramm, des eingehenden, ausgehenden und internen Datenverkehrs, der Anzahl der Netzwerkschnittstellen und der Gesamtzahl der VMs. ■ Details zu Eigenschaften, Transportknotenstatus, pNIC- und TEP-Statistiken sowie Systemmetriken in den letzten 24 Stunden. <p>Hinweis Die Systemmetriken sind nur für NSX-T Version 2.4.0 und höher verfügbar.</p>
Ereignis	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit verschiedenen Ereignissen.

Abschnitt	Details
Latenz	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Details zur TEP-zu-TEP-Latenz.
Schnittstellenstatistiken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Schnittstellenstatistiken, einschließlich empfangener Pakete, übertragener Pakete, verloren gegangener empfangener und übertragener Pakete usw.
Systemstatistiken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Systemstatistiken, einschließlich Systemlast, Systemnutzung und Dateisystemnutzung. <p>Hinweis Die Systemstatistiken sind nur für NSX-T Version 2.4.0 und höher verfügbar.</p>
Flows	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Top-VMs und Top-Regeln nach Flows (in den letzten 24 Stunden).

Seite NSX-T-Transportknoten, wobei der Knotentyp Edge ist

Suchen Sie für den Zugriff auf diese Seite nach **NSX-T Transport Node where Node Type = 'EdgeNode'** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf dieser Seite sehen Sie Folgendes:

Abschnitt	Details
Übersicht	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Übersicht über Ihren Edge-Transportknoten, einschließlich Ereignisdiagramm, Anzahl der Netzwerkschnittstellen, Tier-0-Dienstrouter, Tier-1-Dienstrouter und Routen. ■ Details zu Eigenschaften, Transportknotenstatus, Uplink- und TEP-Statistiken sowie Systemmetriken in den letzten 24 Stunden
Ereignis	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit verschiedenen Ereignissen.
NAT-Statistiken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene NAT-Statistiken, einschließlich NAT-Regelstatistik und Top-NAT-Regeln nach Gesamtzahl der Byte, nach Gesamtzahl der Pakete und nach Sitzungsanzahl.

Abschnitt	Details
Schnittstellenstatistiken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Schnittstellenstatistiken, einschließlich empfangener Pakete, übertragener Pakete, verloren gegangener empfangener und übertragener Pakete usw.
Systemstatistiken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Systemstatistiken, einschließlich Systemlast, Systemnutzung und Dateisystemnutzung.

Anzeigen von Details zum virtuellen Server

Auf der Seite „Virtueller Server“ werden die Metriken zum virtuellen Server und die Problem- und Änderungsereignisse angezeigt.

Sie sehen die folgenden Informationen:

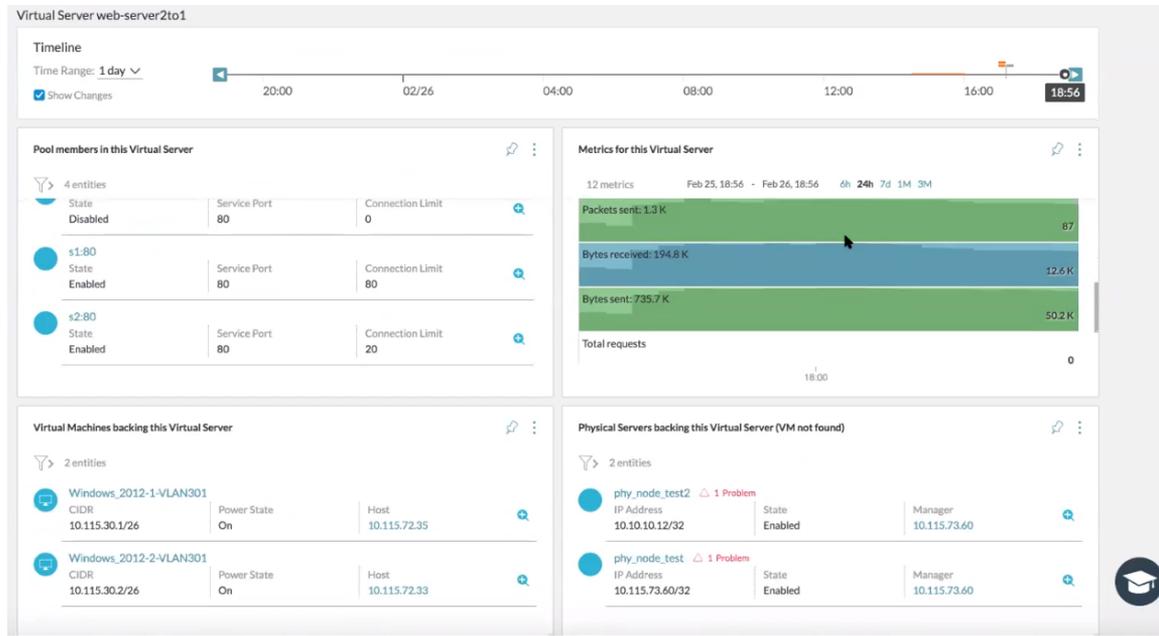
- Die Liste aller Poolmitglieder im virtuellen Server und die zugehörigen Details sowie bei Problemen jeweils eine Warnung
- Die Liste der virtuellen Maschinen
- Die Liste der physischen Server
- Die Liste der dem virtuellen Server zugeordneten Problemereignisse
- Die Liste der auf den virtuellen Server bezogenen Metriken, z. B.
 - Verbindungen (Anzahl, Dauer)
 - Netzwerkmetriken (Pakete und empfangene oder gesendete Byte)
 - CPU-Auslastung

Hinweis Eine Liste der unterstützten Metriken für den NSX-V-Lastausgleichsdienst finden Sie unter [Unterstützte NSX-V-Metriken](#).

- Die Top-Flows für die von diesem virtuellen Server verwendeten Poolmitglieder

Hinweis Für NSX-V-Lastausgleichsdienste werden die Flow-Informationen nicht erfasst.

- Die Eigenschaften des virtuellen Servers, darunter Informationen zur IP-Adresse des Lastausgleichsdiensts, zum Netzwerkdatenverkehr und zum Dienstport



Mit der folgenden Abfrage können Sie den dem Lastausgleichsdienst zugeordneten Topologie-Pfad anzeigen: *Client-VM-Name to IP des virtuellen Servers*.. Wenn mehrere virtuelle Server auf verschiedenen Dienstports vorhanden sind, wird die Liste unter dem Abschnitt „Ziel-VM auswählen“ angezeigt. Sie können einen Server aus der Liste auswählen und den Pfad des virtuellen VM-Servers mit einem Klick auf **Pfad anzeigen** anzeigen.

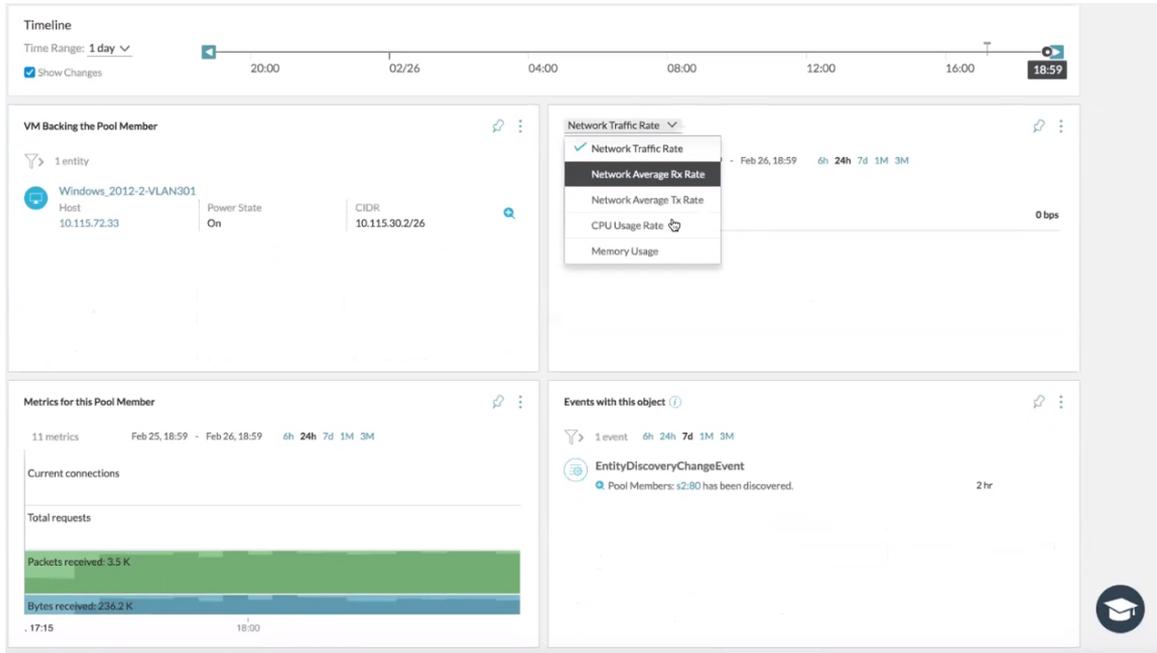
Mit einem Klick auf den virtuellen Server in der VM-Pfad-Topologie können Sie eine Gruppe von VMs im Fenster „Virtueller Server“ anzeigen. Klicken Sie auf **Pfad anzeigen**, um den Pfad vom virtuellen Server zur ausgewählten VM anzuzeigen.

Anzeigen der Details zu Poolmitgliedern

Auf der Seite „Poolmitglieder“ erhalten Sie Erkenntnisse über die Poolmitglieder, Metriken und Ereignisse im Zusammenhang mit dem jeweiligen Poolmitglied.

Sie sehen die folgenden Informationen:

- Liste der virtuellen Maschinen und zusätzliche Details zur VM
- Sie können die Metriken des Poolmitglieds mit denen der VM vergleichen. Beispielsweise Arbeitsspeicher- und CPU-Auslastung, Netzwerkdatenverkehr.
- Liste der Metriken, die sich auf das Poolmitglied beziehen, wie
 - Verbindungen (Anzahl, Dauer, Alter)
 - Netzwerkmetriken (Pakete und empfangene oder gesendete Byte)
 - CPU-Auslastung
- Eigenschaften des Poolmitglieds mit Angaben über den Lastausgleichsdienst, den Knoten, den Status und den Dienstport.



Anzeigen von Details zu Microsoft Azure

Mithilfe der Seite **Microsoft Azure** können Sie in vRealize Network Insight einen schnellen Überblick über die Details Ihrer Azure-Umgebung erhalten.

Vorgehensweise für den Zugriff

Suchen Sie nach **Azure**, um auf diese Seite zuzugreifen. Alternativ dazu können Sie auf der Startseite im Abschnitt **BETRIEB UND FEHLERBEHEBUNG** auf das **Microsoft Azure**-Symbol klicken.

Übersicht

Auf dieser Seite sehen Sie Folgendes:

- Liste der Abonnements
- Liste der virtuellen Maschinen
- Liste der Netzwerkschnittstellen, virtuellen Netzwerke, Subnetze, Routentabellen und Routen
- Liste der Netzwerksicherheitsgruppen, Anwendungssicherheitsgruppen und NSG-Regeln.

Sie können auch auf die Elemente auf dieser Seite klicken, um detaillierten Einblick in das jeweilige Element zu erhalten.

Zusätzlich zur Seite **Microsoft Azure** können Sie Details zu den folgenden Azure-Entitäten anzeigen:

Tabelle 12-3. Details zu Azure-Entitäten

Name der Entität	Beschreibung
Azure-Anwendungssicherheitsgruppe	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse, zugeordneten VMs und der in den letzten 24 Stunden zugeordneten VMs ■ Liste der eingehenden und ausgehenden NSG-Regeln ■ Liste der zulässigen Flows, verweigerten Flows und der Flows in den letzten 24 Stunden
Azure-Datenquelle	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse und Metriken
Azure NSG-Regeln	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse und Metriken
Azure-Netzwerkschnittstelle	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse und Metriken
Azure-Netzwerksicherheitsgruppe	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse, Netzwerkkarten und Subnetz ■ Liste der ausgehenden und eingehenden Regeln ■ Liste der zulässigen Flows, verweigerten Flows und der Flows in den letzten 24 Stunden
Azure-Route	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse und Metriken
Azure-Routentabelle	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse und Metriken
Azure-Subnetz	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse, VMs, Netzwerkkarten und benutzerdefinierten Routen ■ Liste der NSG-Regeln
Azure-Abonnement	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Liste der Eigenschaften und Ereignisse. ■ Liste der virtuellen Maschinen. ■ Liste der Netzwerkkarten, virtuellen Netzwerke und Routentabellen ■ Liste der Netzwerksicherheitsgruppen, Anwendungssicherheitsgruppen und NSG-Regeln.

Tabelle 12-3. Details zu Azure-Entitäten (Fortsetzung)

Name der Entität	Beschreibung
Virtuelle Azure-Maschine	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse, Netzwerkkarten und zugeordneten Anwendungssicherheitsgruppen (ASGs) ■ Liste der eingehenden und ausgehenden NSG-Regeln ■ Liste der zulässigen und verweigerten Flows
Virtuelles Azure-Netzwerk	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Liste der Eigenschaften, Ereignisse, VMs, in den letzten 24 Stunden erstellte VMs, zugeordnete ASGs, in den letzten 24 Stunden zugeordnete ASGs, Subnetze und Routentabellen ■ Liste der zulässigen Flows, verweigerten Flows und Flows in den letzten 24 Stunden

Anzeigen von VeloCloud Enterprise-Details

Sie können die Seite **VeloCloud Enterprise** anzeigen, um einen Überblick über Ihre VMware SD-WAN-Bereitstellung in vRealize Network Insight zu erhalten.

Zugriff auf die Seite VeloCloud Enterprise

Für den Zugriff auf diese Seite suchen Sie nach **veLoCloud Enterprise**. Alternativ dazu können Sie auf der Startseite im Abschnitt **BETRIEB UND FEHLERBEHEBUNG** auf das **VeloCloud Enterprise**-Symbol klicken.

Übersicht

Auf dieser Seite sehen Sie die folgenden Abschnitte:

Abschnitt	Details
Übersicht	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Eine Übersicht über Ihre VMware SD-WAN-Bereitstellung, einschließlich des Ereignisdiagramms, der Anzahl der Edges, Hubs, Gateways, Links, Edge-zu-Edge-Flows, des Internet-Flows und der Anwendungen. Sie können auch den Systemzustand dieser Elemente einsehen. ■ Eine Kartenansicht Ihrer VMware SD-WAN-Bereitstellung und eine Liste der Anwendungen auf Edges. <hr/> <p>Hinweis Zum Abrufen der Kartenansicht müssen Sie einen Google Maps-API-Schlüssel in vRealize Network Insight hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Google Maps-API-Schlüssels. Wenn Sie keinen Google Maps-API-Schlüssel hinzufügen, können Sie nur die Listenansicht der Edges anzeigen.</p>
Ereignis	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Eine Liste mit verschiedenen Ereignissen.
Analyse	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Verschiedene Datenverkehrsverteilungslisten, wie beispielsweise die Datenverkehrsverteilung nach Anwendungen, Edge, Edge-Paaren, Flow-Pfad, Datenverkehrstyp, Link-Richtlinie und Routentyp
Verfügbarkeit	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Eine Liste mit verfügbaren und nicht verfügbaren Edges/Hubs.
Metriken	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Verschiedene Metriken basierend auf dem Edge-Datenverkehr, dem Edge-Paket, der Edge-Qualität, dem Anwendungsdatenverkehr, den Anwendungspaketen, dem Link-Paket, der Link-Latenz, dem Link-Durchsatz und der Link-Qualität Sie können auf das Pluszeichen (+) klicken, um weitere Details zu erhalten.

Sie können auch auf die Elemente auf dieser Seite klicken, um detaillierten Einblick in das jeweilige Element zu erhalten.

Zusätzlich zur Seite **VeloCloud Enterprise** können Sie Details zu den folgenden VMware SD-WAN-Elementen anzeigen:

Tabelle 12-4. Details zum VMware SD-WAN-Element

Name des Elements	Beschreibung
VeloCloud-Cluster	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit Eigenschaften.
VeloCloud-Datenquelle	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit Eigenschaften, ungelösten Problemen, Änderungen und Problemen, die in den letzten 7 Tagen aufgetreten sind.
VeloCloud Edge	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Details zur VMware SD-WAN-Edge. Weitere Informationen finden Sie unter Anzeigen von VeloCloud Edge-Details.
VeloCloud-Gateway	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit Eigenschaften und Edges.
VeloCloud Layer2-Netzwerk	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit Eigenschaften und Ereignissen.
VeloCloud-Link	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit Eigenschaften und Ereignissen. ■ Metriken zu QoE, Paket, Betriebszeit, Latenz und Durchsatz.
VeloCloud-Profil	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit Eigenschaften und Edges.
VeloCloud-Segment	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste mit Eigenschaften.

Anzeigen von VeloCloud Edge-Details

Sie können die Seite **VeloCloud Edge** verwenden, um einen schnellen Überblick über VMware SD-WAN-Edge in vRealize Network Insight zu erhalten.

Suchen Sie für den Zugriff auf diese Seite nach **VeloCloud Edge** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf dieser Seite sehen Sie die folgenden Abschnitte:

Abschnitt	Details
Übersicht	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Übersicht über Ihre VMware SD-WAN-Edge, wie beispielsweise das Ereignisdiagramm, das Richtliniendiagramm, Details zur Betriebszeit sowie die Anzahl der Anwendungen, Segmente, Links, Layer-2-Netzwerke, LAN-Schnittstellen, WAN-Schnittstellen und Tunnel. ■ VMware SD-WAN-Edge-Topologie ■ Liste zu Edge-Qualität und Link-Qualität
Ereignis	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Liste der verschiedenen Ereignisse
Flows	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Liste der Flows
Analyse	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Verschiedene Datenverkehrsverteilungslisten, wie beispielsweise die Datenverkehrsverteilung nach Anwendung und Priorität, Flow-Pfad, Datenverkehrstyp, Link-Richtlinie und Routentyp
Metriken	<p>Sie sehen die folgenden Informationen:</p> <ul style="list-style-type: none"> ■ Verschiedene Metriken basierend auf dem Edge-Datenverkehr, dem Edge-Paket, dem Anwendungsdatenverkehr, den Anwendungspaketen, dem Link-Paket, der Link-Latenz, dem Link-Datenverkehr und dem Tunnel-Datenverkehr. Sie können auf das Pluszeichen (+) klicken, um weitere Details zu erhalten.

Sie können auch auf die Elemente auf dieser Seite klicken, um detaillierten Einblick in das jeweilige Element zu erhalten.

Anzeigen von Details zur SD-WAN- und Edge-SD-WAN-Anwendung

Sie können die **SD-WAN-Anwendung** und die **Edge-SD-WAN-Anwendung** verwenden, um in vRealize Network Insight einen schnellen Überblick über die SD-WAN- und die Edge-SD-WAN-Anwendung zu erhalten.

Übersicht

Auf dieser Seite sehen Sie die folgenden Abschnitte:

Tabelle 12-5. SD-WAN-Anwendung

Abschnitt	Details
Übersicht	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Eine Liste der Edges, Links, Ereignisse und Flows.
Datenverkehrsverteilung	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Details zur Datenverkehrsverteilung, z. B. Datenverkehr nach Edge und nach Client.
Metriken	Sie sehen die folgenden Informationen: <ul style="list-style-type: none"> ■ Verschiedene Metriken, wie z. B. Edge-Datenverkehr, Edge-Paket, Datenverkehr der Verknüpfung und Details zu Verknüpfungspaketen.

Sie können auch auf die Elemente auf dieser Seite klicken, um detaillierten Einblick in das jeweilige Element zu erhalten.

Zusätzlich zur Seite **SD-WAN-Anwendung** werden folgende Informationen zur **Edge-SD-WAN-Anwendung** angezeigt:

- Eine Liste mit Eigenschaften, Ereignissen und Metriken

Hinweis vRealize Network Insight unterstützt maximal 2 Segmente pro VMware SD-WAN-Edge und maximal 20.000 Layer 3-Domänen.

Anzeigen von Details zur SD-WAN-Bewertung

Sie können die Seite **SD-WAN-Bewertung** anzeigen, um einen Überblick über Ihre WAN-Bereitstellungsdetails zu erhalten. Sie können auch einen ROI-Bewertungsbericht abrufen, um die Art Ihres Datenverkehrs zu verstehen und eine Empfehlung für die SD-WAN-Bereitstellung zu erhalten. vRealize Network Insight

Wie erfolgt der Zugriff auf die Seite SD-WAN-Bewertung?

Um auf diese Seite zuzugreifen, klicken Sie im linken Navigationsbereich auf **Planen und bewerten > SD-WAN-Bewertung**.

Übersicht

Auf dieser Seite sehen Sie die Zusammenfassung des SD-WAN-Bewertungsberichts, Daten des ausgehenden und eingehenden Datenverkehrs sowie die wichtigsten Dienste für den ausgehenden und den eingehenden Datenverkehr.

Sie können den Geltungsbereich und die Dauer der Bewertung ändern. Um den Geltungsbereich und die Dauer der Bewertung zu ändern, wählen Sie in den Dropdown-Menüs **Geltungsbereich** und **Dauer** den Geltungsbereich und die Dauer aus, die Sie verwenden möchten, und klicken Sie auf **Analysieren**.

Sie können auch einen SD-WAN-Bewertungsbericht generieren. Weitere Informationen finden Sie unter [Generieren eines Bewertungsberichts](#).

Generieren eines Bewertungsberichts

In vRealize Network Insight können Sie einen SD-WAN-Bewertungsbericht generieren, um eine Schätzung der Kosteneinsparungen zu erhalten, die VMware SD-WAN über das herkömmliche WAN-Setup bieten kann. Darüber hinaus bietet der SD-WAN-Bewertungsbericht auch eine SD-WAN-Edge-Empfehlung für jede Ihrer Sites.

Verfahren

- 1 Klicken Sie auf der Seite **SD-WAN-Bewertung** auf **BERICHT GENERIEREN**.

Das Dialogfeld **Zusätzliche Daten** wird angezeigt.

- 2 Geben Sie im Textfeld **Organisationsname** den Namen der Organisation ein, für die Sie den Bericht generieren möchten.

- 3 Überprüfen Sie in der Tabelle **Regionsspezifische Eingaben** die regionsspezifischen Eingaben und klicken Sie auf **BERICHT GENERIEREN**.

Sie können die regionsspezifischen Eingaben gemäß Ihren Anforderungen ändern. Sie können auf **ZURÜCKSETZEN** klicken, um die Standardwerte für die regionsspezifischen Eingaben abzurufen.

Ergebnisse

Auf einer neuen Registerkarte können Sie den Bericht **SD-WAN-Bewertung** anzeigen.

Anzeigen der Details zur VeloCloud-Link-Anwendung

Auf der Seite **VeloCloud-Link-Anwendung** können Sie über einen Link einen Überblick über Ihre Anwendung erhalten.

Suchen Sie für den Zugriff auf diese Seite nach **SD-WAN-Link-Anwendung** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf dieser Seite sehen Sie Folgendes: Liste der Schlüsseleigenschaften, Details zu Flow-Datenverkehr und Details zu Flow-Paketen.

Anzeigen von Details zu VeloCloud-Geschäftsrichtlinien

Auf der Seite **VeloCloud-Geschäftsrichtlinie** können Sie einen Überblick über Ihre VeloCloud-Geschäftsrichtlinien erhalten.

Suchen Sie für den Zugriff auf diese Seite nach **VeloCloud-Geschäftsrichtlinie** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf dieser Seite sehen Sie Folgendes: Definition: Übereinstimmung, Definition: Aktion, Ereignisse und Flow-Details.

Hinweis Aktuell bietet vRealize Network Insight keine Unterstützung für Folgendes:

- SD-WAN-Geschäftsrichtlinie mit Nicht-VeloCloud-Site als Quelle/Ziel.
- SD-WAN-Geschäftsrichtlinie mit Objektgruppe (IP-Adresse oder Portgruppe) als Quelle/Ziel.

Anzeigen der VMC-SDDC-Details

Sie können die Seite **VMC-SDDC** verwenden, um einen Überblick über Ihren vCenter und Ihren NSX Manager in vRealize Network Insight zu erhalten.

Wie erfolgt der Zugriff auf die Seite VMC-SDDC?

Suchen Sie für den Zugriff auf diese Seite nach **VMC-SDDC** und klicken Sie in der Suchergebnisliste auf die **VMC-SDDC**-Einheit, die angezeigt werden soll.

Übersicht

Auf der Seite **VMC-SDDC** sehen Sie Folgendes:

Abschnitt	Details
Übersicht	Sie sehen eine Übersicht über Ihre NSX-Richtlinieneinheiten, Einheiten in den letzten 24 Stunden, Top-Flows nach Regel, Liste der Router und Eigenschaftendetails.
Top-Kommunizierer	Sie sehen Diagramme der Top-Kommunizierer unter Ihren VMs.
Netzwerkdatenverkehr und -ereignisse	Sie sehen eine Übersicht über den Netzwerkdatenverkehr und die Listenereignisse.

Anzeigen der Details für Arista-Hardware-Gateway und Gateway-Bindung der Arista-Hardware

Sie können die Seiten **Arista-Hardware-Gateway** und **Gateway-Bindung der Arista-Hardware** anzeigen, um eine Übersicht über Ihre Arista-Hardware-Gateways zu erhalten.

Wie erfolgt der Zugriff auf die Seite Arista-Hardware-Gateway?

Um auf die Seite **Arista-Hardware-Gateway** zuzugreifen, suchen Sie nach **Arista-Hardware-VTEP** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Um auf die Seite **Gateway-Bindung der Arista-Hardware** zuzugreifen, suchen Sie nach **Gateway-Bindung der Arista-Hardware** und klicken Sie in der Liste der Suchergebnisse auf die Einheit, die Sie anzeigen möchten.

Übersicht

Auf der Seite **Arista-Hardware-Gateway** sehen Sie Folgendes:

- Ereignisliste
- Liste der Schlüsseleigenschaften
- Liste der Gateway-Bindungen der Arista-Hardware

Auf der Seite **Gateway-Bindung der Arista-Hardware** sehen Sie Folgendes:

- Ereignisliste
- Liste mit Eigenschaften

Anzeigen von Details zum Cisco-Nexus-Gerät

Auf der Seite **Cisco-Nexus-Gerät** erhalten Sie einen Überblick über die in vRealize Network Insight verfügbaren Details zu Ihrem Cisco-Nexus-Gerät.

Übersicht

Auf dieser Seite sehen Sie Folgendes:

- Leistungsüberwachungs-Metriken

Hinweis Klicken Sie auf den einzelnen Metrikwert, um einen weiteren Einblick in die jeweilige Metrik zu erhalten.

- Ereignisliste
- Details zu Eigenschaften
- Liste der mit dem Port verbundenen Switch-Ports, Switch-Port-Peers und VMs
- Switch-Port-Metriken

Anzeigen von Flow-Erkenntnisdetails

Die Seite **Flow-Erkenntnisse** bietet einen Einblick in Datencenter, Geräte und Flows. Es handelt sich um eine kontextbasierte Seite, da sie basierend auf den Einheiten, Flows und dem ausgewählten Zeitraum eine Analyse durchführt.

Gehen Sie wie folgt vor, um die Seite „Flow-Erkenntnisse“ zu öffnen:

- 1 Klicken Sie im linken Navigationsbereich auf **Analyse > Flow-Erkenntnisse**.
- 2 Wählen Sie den **Geltungsbereich** und die **Dauer** aus.

3 Klicken Sie auf **Analysieren**.

Alternativ können Sie nach **Flows** suchen und auf der Seite mit den Suchergebnissen auf **Flow-Erkenntnisse** klicken.

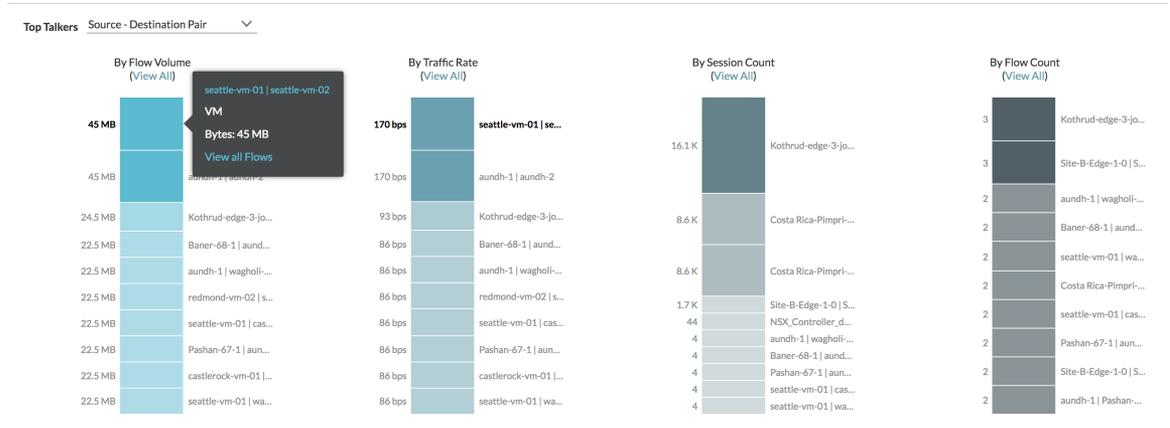
Die verschiedenen Abschnitte im Dashboard „Flow-Analyse“ sind:

- Top-Talkers
- Neuigkeiten
- Netzwerkleistung
- Ausreißer

Top-Talkers

In diesem Abschnitt können Sie erkennen, welche Einheiten in Ihrer Umgebung am meisten kommunizieren. Sie können verschiedene Arten von Einheiten auswählen, z. B. Quelle-Ziel-Paar, VM, Cluster, L2-Netzwerk, Subnetz. Dieses Widget listet die wichtigsten 10 Talkers in der von Ihnen ausgewählten Einheitenkategorie auf. Es hilft dem Kunden bei der Planung der Netzwerkoptimierung. Die Metriken, die durch Balken in diesem Widget dargestellt werden, sind wie folgt:

- Nach Flow-Volumen: gibt das Datenverkehrsvolumen an.
- Nach Datenverkehrsrate: gibt die Rate des Datenverkehrs an.
- Nach Sitzungsanzahl: gibt die Anzahl der Sitzungen an.
- Nach Flow-Anzahl: gibt die Anzahl der Flows an.



Hinweis

- Wenn eine VM in einer oder mehreren Metriken angezeigt wird und Sie auf diese VM in einer Leiste zeigen, wird Sie auch in anderen Balken hervorgehoben.
- Wenn Sie in der Metrikleiste auf eine VM klicken, wird die vollständige Liste der Flows zu dieser VM angezeigt.
- Wenn Sie VM als Einheit in der Liste der Top-Talkers auswählen, werden alle mit dieser VM verbundenen Flows, unabhängig davon, ob es sich um die Quelle oder das Ziel handelt, angezeigt. Wenn Sie Quell-VM in der Liste auswählen, werden nur die Flows berücksichtigt, die von dieser VM stammen.
- Wenn Sie die physischen Flows berücksichtigen, können Sie entweder Quell-IP oder Ziel-IP auswählen.
- Wenn Sie das Quelle-Ziel-Paar und den Punkt auf der Metrikleiste ausgewählt haben und auf den Link in der QuickInfo klicken, wird das entsprechende Dashboard angezeigt. Beispiel: Für eine VM im Quelle-Ziel-Paar wird das Dashboard VM-VM-Pfad angezeigt.
- Für eine Flow-Gruppenansicht, eine Flow-Einheitsprojektion oder eine Flows-Gruppenabfrage können Sie die Schaltfläche **Flow-Analyse** nicht sehen.

Neuigkeiten

In diesem Abschnitt können Sie nachverfolgen, welche Dienste und Einheiten im ausgewählten Zeitraum im Datacenter erkannt werden. Die Widgets in diesem Abschnitt lauten wie folgt:

- Neue virtuelle Maschinen, die auf das Internet zugreifen: Listet die neuen VMs auf, die auf das Internet zugreifen.
- Zugriff auf neue Internetdienste: Listet die neuen Internetdienste auf, die in der Umgebung erkannt wurden.
- Zugriff auf neue interne Dienste: Listet die neuen Intranet-Dienste auf, die vom Internet-Endpoint erkannt und darauf zugegriffen werden.

- Zugriff auf neue interne/E-W-Dienste: Listet die Dienste auf, die von den Maschinen innerhalb eines Datacenters offengelegt und darauf zugegriffen werden.
- Neue Dienste mit blockierten Flows: Listet Dienste auf, die blockierte Flows aufweisen. Dieser Abschnitt wird nur für IPFIX ausgefüllt.
- Neue Firewallregeltreffer: Listet die neuen Firewallregeln auf, die in Kraft gesetzt werden. Dieser Abschnitt wird nur für IPFIX ausgefüllt.

Netzwerkleistung

In diesem Abschnitt können Sie die abnormalen Flows für die verschiedenen Bereiche von TCP Round Trip Time (RTT)-Werten basierend auf den ausgewählten Kriterien suchen und visualisieren.

Hinweis vRealize Network Insight zeigt die durchschnittlichen TCP-RTT-Metriken mit einer Granularität von 5 Minuten nur für die letzten 24 Stunden an.

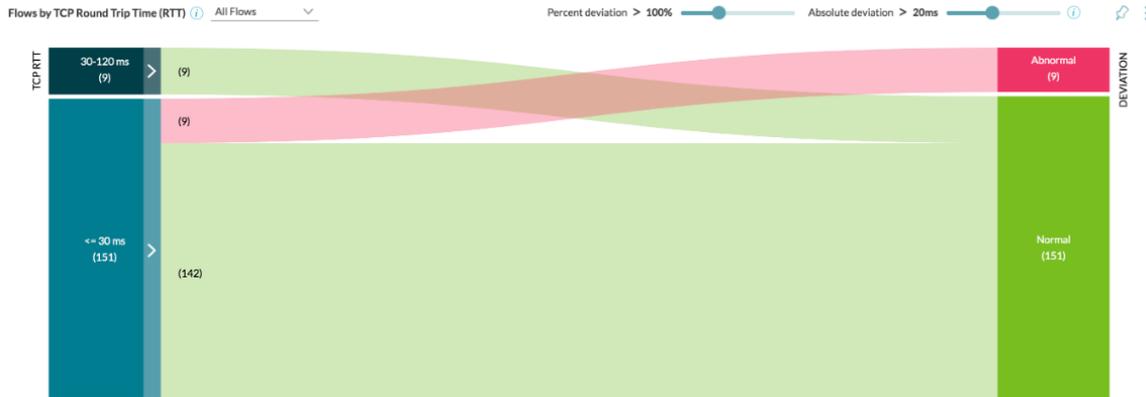
Wenn die prozentuale Flow-Abweichung 100 % und die absolute Abweichung 20 Millisekunden (ms) beträgt, stuft vRealize Network Insight diesen Flow als abnormalen Flow ein.

In der Visualisierung werden auf der linken Seite der unterschiedliche TCP-RTT-Bereich und auf der rechten Seite der Normalbereich und der Bereich der abnormalen Abweichung angezeigt. Basierend auf den Werten der prozentualen und der absoluten Abweichung werden die Flows von links (TCP-RTT) nach rechts (ABWEICHUNG) verbunden. Sie können die folgenden Arten von Flows analysieren:

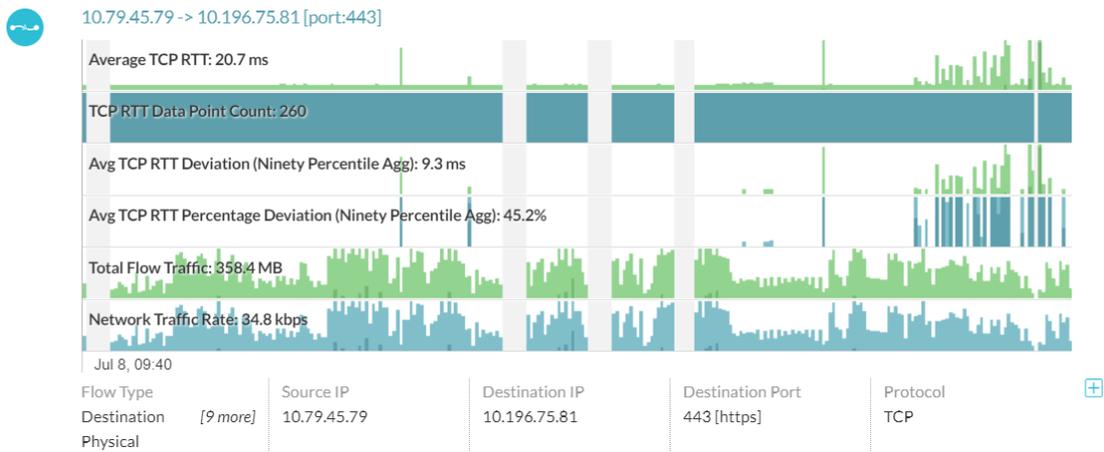
- Host-übergreifend
- Host-intern
- Internet
- Alle Flows

Die prozentuale und die absolute Abweichung können Sie auch je nach Ihrem Bedarf ändern.

Im folgenden Beispiel gibt es zwei verschiedene TCP-RTT-Bereiche. Einer ist kleiner oder gleich 30 ms und der andere ist 30–120 ms. Sie können feststellen, dass es insgesamt 151 Flows gibt, die kleiner oder gleich 30 ms sind (TCP-RTT-Bereich). Von den 151 Flows werden 9 Flows als anormaler Flow angezeigt.



Für genauere Erkenntnisse über die TCP-RTT-Verteilung und die Anzahl der Flows können Sie in der Visualisierung auf die farbige Linie klicken. Im folgenden Beispiel sehen Sie detaillierte Erkenntnisse über die TCP-RTT-Verteilung und die Anzahl der Flows:



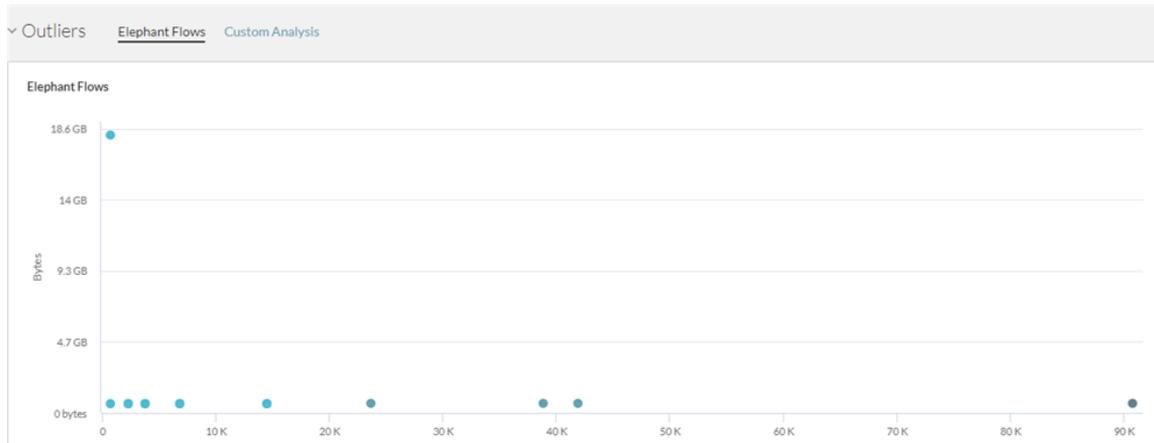
Ausreißer

Dieser Abschnitt hilft Ihnen dabei, verwandte Daten nachzuverfolgen und zu analysieren. Er besteht aus folgenden Abschnitten:

- **Elephant-Flows:** Dieser Abschnitt hilft bei der Identifizierung der Flows mit einer geringen Anzahl von Sitzungen und einem hohen Durchsatz im Vergleich zu Flows, die eine große Anzahl von Sitzungen und einen geringen Durchsatz aufweisen. In der Regel werden die Flows mit hoher Sitzungsanzahl und geringem Durchsatz auch als Mice-Flows bezeichnet. Die Analyse basiert auf dem Verhältnis von Bytes zur Anzahl der Sitzungen. Jeder Punkt im Diagramm stellt mehrere Flows dar. Wenn Sie auf einen Punkt zeigen, wird die Liste der Flows angezeigt. Um die Details eines bestimmten Flows anzuzeigen, klicken Sie in der Liste auf diesen Flow.

- Benutzerdefinierte Analyse: In diesem Abschnitt können Sie die Flow-Daten auf zwei Dimensionen Ihrer Wahl visualisieren. Diese Funktion hilft bei der Analyse der Daten, um verschiedene Arten von Ausreißern zu finden.

Hinweis Die in diesem Abschnitt dargestellten Metriken sind die ungefähren Werte und nicht die genauen Werte.



Anzeigen der Details zur Mikrosegmentierung

Sie können die Flows analysieren, indem Sie den Geltungsbereich auswählen und sie basierend auf Einheiten wie VLAN/VXLAN, Sicherheitsgruppen, Anwendung, Ebene, Ordner, Subnetz, Cluster, virtuelle Maschine (VM), Port, Sicherheits-Tag, Sicherheitsgruppe und IPSet entsprechend segmentieren.

Die Seite „Mikrosegmentierung“ enthält die Analysedetails mit dem Topologiediagramm. Diese Seite besteht aus den folgenden Abschnitten:

- Mikrosegmente: Dieses Widget stellt das Diagramm für die Topologieplanung bereit. Sie können den Gruppentyp und Flows auswählen. Basierend auf Ihren Eingaben können Sie das entsprechende Topologieplanungsdiagramm anzeigen.
- Verteilung des Datenverkehrs: Dieses Widget liefert die Details der Datenverkehrsverteilung in Bytes.
- Top-Ports nach Byte: Dieses Widget listet die wichtigsten 100 Ports auf, die den höchsten Datenverkehr verzeichnen. Die Metriken für die Flow-Anzahl und das Flow-Volumen werden angegeben. Sie können die Flows für einen bestimmten Port anzeigen, indem Sie auf die Anzahl der Flows klicken, die diesem Port entsprechen.

So greifen Sie auf die Seite „Mikrosegmentierung“ zu:

Verfahren

- 1 Klicken Sie im Navigationsbereich auf der linken Seite der Startseite auf **Sicherheit** > **Sicherheit planen**.

- 2 Wählen Sie den Geltungsbereich, den Unterbereich und die Dauer aus, für die Sie planen und analysieren möchten. Klicken Sie auf **Analysieren**.

Die Seite „Mikrosegmentierung“ wird angezeigt.

Hinweis In der Donut-Ansicht können bis zu 600 Knoten und 6000 Edges angezeigt werden. Wenn der Grenzwert überschritten wird, wird die folgende Fehlermeldung angezeigt: Zu viele Mikrosegmente für die Analyse. Wählen Sie eine andere Einheit oder andere Kriterien für die Mikrosegmentierung aus.

Anzeigen von Anwendungsdetails

Eine Anwendung ist eine Sammlung von Ebenen. Jede Ebene in einer Anwendung ist eine Sammlung von VMs und physischen IPs basierend auf den benutzerdefinierten Filterkriterien. Mit den Anwendungen können Sie eine Gruppe von Ebenen erstellen und Datenverkehr oder Flows zwischen den Ebenen derselben Anwendung und zwischen Anwendungen visualisieren.

Sie haben drei Möglichkeiten, eine Anwendung in vRealize Network Insight zu erstellen oder hinzuzufügen:

- [Manuelles Erstellen einer Anwendung](#)
- [Öffentliche API](#)
- [Anwendungsermittlung](#)

Die Anwendungsseite bietet die vollständige Sichtbarkeit einer einzelnen Anwendung in vRealize Network Insight. Auf diese Weise können Sie Probleme beheben und auch die Analyse anzeigen.

- Eine Übersicht
 - der Anwendungstopologie
 - Ebenenübersicht
 - Liste der VMs in den Anwendungen
 - der physischen IPs, von denen die Anwendung abhängt oder die sie verwendet
 - Gemeinsam genutzte Dienste
 - Anwendungen, mit denen diese bestimmte Anwendung kommuniziert
 - Ereignisse im Zusammenhang mit den Anwendungen
 - Manager für Anwendungs-VMs
- Neuigkeiten in den letzten 24 Stunden
 - Menge des ein- und ausgehenden Datenverkehrs
 - Flow-Verluste
 - Neue und ungeschützte Mitglieder
 - Dienste, auf die extern zugegriffen wird

- Dienste, auf die über das Internet zugegriffen wird
- Verwendete Anwendungspors
- Datenverkehrs-Flows oder Flow-Analyse
 - Top-Talkers
 - Top-Anwendungs-Flows nach Regel
- Mikrosegmentierung
 - Kontextbezogene Flows zwischen Einheiten, die Daten unterschiedlicher Flow-Typen bereitstellen, wie alle zulässigen Flows, und verloren gegangene Flows, geschützte und ungeschützte Flows von NSX DFW.
 - Neuheiten in einer Anwendung
- Metriken
 - die VM-Metrikinformationen, die Informationen über die Netzwerkrate, CPU, Arbeitsspeicher und Festplatte darstellen.
 - die Kubernetes-Metriken

Analyse – Ausreißerererkennung

vRealize Network Insight bietet eine Ausreißerererkennung basierend auf den Metriken, die den über die VMs und physischen IP-Adressen definierten Flows zugeordnet sind. Diese VMs/IPs sollten ähnliche Datenverkehrsmuster aufweisen, damit eine Klassifizierung einer bestimmten VM/IP als Ausreißer von Wert ist. Beispielsweise führen die VMs, die zur selben Ebene einer Anwendung gehören, in der Regel dieselbe Funktion für die Anwendung aus, z. B. die VMs einer SQL-Datenbank, die Anforderungen für eine Webanwendung bedienen. Für diese Art von VMs gehen die Anzahl der empfangenen Anforderungen, die Menge des gesendeten Datenverkehrs, die Anzahl der Sitzungen usw. durch eine Reihe ähnlicher Variationen.

Mithilfe von vRealize Network Insight können Sie über die Ausreißerererkennung eine bestimmte VM erkennen, die im Vergleich zu anderen VMs/IPs in der Gruppe sehr unterschiedliche Datenverkehrsmuster aufweisen kann. Beispiel: Wenn die VM im Vergleich zum Rest der Gruppe viel höheren/geringeren Datenverkehr sendet oder empfängt. Dies könnte auf einen falsch konfigurierten Lastausgleichsdienst, einen DDOS-Angriff usw. zurückgeführt werden. vRealize Network Insight stuft solche VMs/IPs als Ausreißer ein. Beim Betrachten dieser Ausreißer kann der Benutzer dieses unerwartete Verhalten leicht erkennen und entsprechende Maßnahmen ergreifen.

Erkennen von Ausreißer-VMs

Verfahren

- 1 Klicken Sie in der Seitenleiste auf **Analyse**. Klicken Sie auf **Ausreißer**.
- 2 Klicken Sie auf **Hinzufügen**, um eine Konfiguration hinzuzufügen.

3 Geben Sie auf der Seite **Analyse/Konfigurieren** die folgenden Details für die Konfiguration an:

Tabelle 12-6.

Feld	Beschreibung
Name	Name der Konfiguration
Geltungsbereich	<p>Name der Gruppe, die die VMs und die IPs definiert, für die die Analyse durchgeführt werden muss. Sie können Anwendungsebene oder Sicherheitsgruppe als Geltungsbereich auswählen.</p> <p>Wenn Sie Anwendungsebene auswählen, geben Sie den Namen der Anwendung und die Ebene separat an. Die Anzahl der VMs und physischen IPs, die für die Ebene definiert sind, wird neben dem Namen der Ebene angezeigt.</p> <p>Wenn Sie Sicherheitsgruppe auswählen, geben Sie den Namen der Sicherheitsgruppe an.</p> <p>Hinweis Der aktuelle Grenzwert für die Anzahl der VMs und der physischen IPs in einer Ebene liegt bei 200. Wählen Sie eine Ebene oder eine Sicherheitsgruppe mit VMs und physischen IPs aus, die unter diesem Grenzwert liegen. Der Geltungsbereich sollte auch mindestens 3 VMs/physische IPs enthalten.</p> <p>Sie können die Mikrosegmentierung für die ausgewählte Konfiguration anzeigen, indem Sie auf Mikrosegmente anzeigen klicken.</p>
Erkennungstyp	Derzeit können Sie mit vRealize Network Insight den Ausreißer im System erkennen.
Metrik	<p>Die Erkennung basiert auf dieser Flow-Metrik. Sie können folgende Optionen auswählen:</p> <ul style="list-style-type: none"> ■ Bytes ■ Pakete ■ Sitzungen ■ Datenverkehrsrate
Richtung des Datenverkehrs	Sie können Ausgehend , Eingehend oder Beide als Datenverkehrsrichtung auswählen. Wenn Sie Beide auswählen, können Sie in der Vorschau der Konfiguration „Eingehend“ oder „Ausgehend“ angeben.
Datenverkehrstyp	Sie können Internet , Ost-West oder „Alle“ basierend auf der Anforderung auswählen.

Tabelle 12-6. (Fortsetzung)

Feld	Beschreibung
Zielports	<p>Sie können entweder alle Ports auswählen, die auf den im ausgewählten Geltungsbereich ermittelten Flows erkannt wurden, oder die Zielports Ihrer Wahl manuell eingeben. Wenn Sie Alle Ports auswählen, wird die Anzahl der Zielports angezeigt. Wenn Sie Ports manuell eingeben auswählen und dann die Ports in das Textfeld „Autovervollständigung“ eingeben, bleibt die Analyse auf diese Ports beschränkt.</p> <p>Hinweis Der aktuelle Grenzwert für die Anzahl der Ports ist 20.</p>
Empfindlichkeit	Dies ist ein Maß für die Empfindlichkeit der von Ihnen benötigten Erkennung und Berichterstellung. Der Standardwert ist Mittel .
Vorschau	Dieser Abschnitt bietet eine Vorschau der jeweiligen Konfiguration basierend auf den von Ihnen bereitgestellten Eingaben und Parametern. Geben Sie die Ports und die Richtung des Datenverkehrs an, wenn Sie zuvor „Beide“ für die Datenverkehrsrichtung ausgewählt haben. Sie werden die Ausreißer-VM im Diagramm identifizieren können.

Hinweis

- Der Ausreißer wird durch die Auswertung der für die letzten 24 Stunden verfügbaren Daten ermittelt.
- Sie benötigen einen kontinuierlichen Fluss von IPFIX-Daten, um den Ausreißer zu erkennen.

- 4 Klicken Sie auf **Absenden**, um die Analysekonfiguration zu erstellen.
- 5 Sobald die Anwendung erstellt wurde, ist sie in der Listenansicht der Anwendungen auf der Seite „Analysekonfigurationen“ verfügbar. Klicken Sie auf diese bestimmte Anwendung, um ein zugehöriges Dashboard anzuzeigen.

Analyse: statische und dynamische Schwellenwerte

Mit vRealize Network Insight können Sie Schwellenwerte festlegen und konfigurieren sowie Warnungen basierend auf Aberrationen im Verhalten der Einheiten erhalten. Sie können zwei Arten von Schwellenwerten konfigurieren:

- **Statischer Schwellenwert:** Wenn ein bestimmter Metrikerwert über oder unter den konfigurierten Wert hinausgeht, wird eine statisch-schwellenwertbasierte Warnung erstellt.

- **Dynamischer Schwellenwert:** Wenn der Schwellenwert von dem System basierend auf der Analyse der Verlaufsdaten festgelegt wird, wird eine Warnung erstellt, falls gegen diesen Schwellenwert verstoßen wird. Die Daten werden für einen Zeitraum von 7 Tagen analysiert, bevor eine Warnung erstellt wird. Der Vorgang zum Erstellen einer Baseline ist auf historische Daten im Zeitraum von 21 Tagen beschränkt und die älteren Metrikwerte werden nicht als Baseline für die neuen Metrikwerte berücksichtigt.

Die Warnung wird sofort erstellt, wenn ein Verstoß gegen einen Schwellenwert vorliegt. Die Benutzer der Enterprise-Lizenz können die Anzahl der Schwellenwertverstöße auf der Startseite im Abschnitt **Was geschieht** anzeigen. Klicken Sie zum Anzeigen der Ereignisdetails auf die Zahl für die Schwellenwertverstöße. Wenn im System keine Schwellenwertkonfigurationen vorhanden sind, wird im Abschnitt **Was geschieht** der Link **+Konfigurieren** angezeigt. Sie können auf den Link **+Konfigurieren** klicken, um den Schwellenwert zu konfigurieren.

Konfigurieren von Schwellenwerten und Warnungen

Sie können eine Schwellenwertkonfiguration hinzufügen und Warnungen für den konfigurierten Schwellenwert abrufen.

So konfigurieren Sie analysebezogene Schwellenwerte und Warnungen:

Verfahren

- 1 Klicken Sie auf der Startseite im linken Navigationsbereich auf **Analyse > Schwellenwerte > Hinzufügen**.
Die Seite **Schwellenwert – Konfiguration hinzufügen** wird geöffnet.
- 2 Geben Sie im Textfeld **Name** einen eindeutigen Namen für die Konfiguration ein.
- 3 Wählen Sie aus dem Dropdown-Menü **Geltungsbereich** einen Geltungsbereich aus und geben Sie im Textfeld **Kriterien auswählen** ein Kriterium ein.
Das Dropdown-Menü **Geltungsbereich** besteht aus den Einheiten **Virtuelle Maschinen, Flows, Anwendung, SD-WAN-Link, SD-WAN-Edge** und **SD-WAN-Edge-Anwendung**. Der Geltungsbereich basiert auf dem Suchabfragesystem. Sie können eine Abfrage aus den verfügbaren Vorschlägen gemäß Ihren Anforderungen erstellen.
- 4 Legen Sie im Abschnitt **Bedingung** eine Bedingung fest, um eine Warnung zu erstellen.
Basierend auf der von Ihnen festgelegten Bedingung entscheidet das System, ob der Schwellenwert über- oder unterschritten wird.

5 Die Standardmetrik ist `network traffic rate`. Wählen Sie die Gruppierung der Einheit und den Wert aus, für den Sie den Schwellenwert überprüfen. Sie können einen Schwellenwert für eine kumulative Metrik festlegen, indem Sie die Daten über eine Gruppe von Einheiten aggregieren.

a Um den statischen Schwellenwert zu konfigurieren, wählen Sie eine der folgenden Schwellenwertbedingungen aus der Liste aus:

- **überschreitet den Schwellenwert**
- **sinkt unter**
- **liegt außerhalb des Bereichs**

Wenn Sie `Upper Bound` oder `Lower Bound` (sofern ein Geltungsbereich vorhanden ist) für `network traffic rate` oder `total traffic` oder eine andere Metrik eingeben, müssen Sie sicherstellen, dass Sie den Wert in den angegebenen Metriken für dieses Textfeld eingeben. Die folgenden Konvertierungswerte dienen als Referenz:

- 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 Um den dynamischen Schwellenwert zu konfigurieren, wählen Sie **weicht vom früheren Verhalten ab**. Wählen Sie die Empfindlichkeit basierend auf Ihren Anforderungen für die Berichterstellung aus.

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

Wenn Sie den Schwellenwert festlegen, können Sie das zugeordnete Diagramm oben auf der Seite anzeigen. Der rosafarbene Balken bezeichnet die VMs oder die Flows, die gegen den Schwellenwert verstoßen. Sie können die Liste der Einheiten anzeigen, die gegen Schwellenwerte verstoßen haben, und die Einheiten, die sich innerhalb der Schwellenwerte im System befinden.

6 Konfigurieren Sie die Benachrichtigungen oder Warnungen, indem Sie die folgenden Eigenschaften festlegen:

- **Schweregrad**

- **E-Mail-Häufigkeit**
- **Benachrichtigungs-E-Mails senden an:**

Hinweis Wählen Sie **SNMP-Trap senden** aus, wenn Sie SNMP-Traps auf Ihrem System konfiguriert haben.

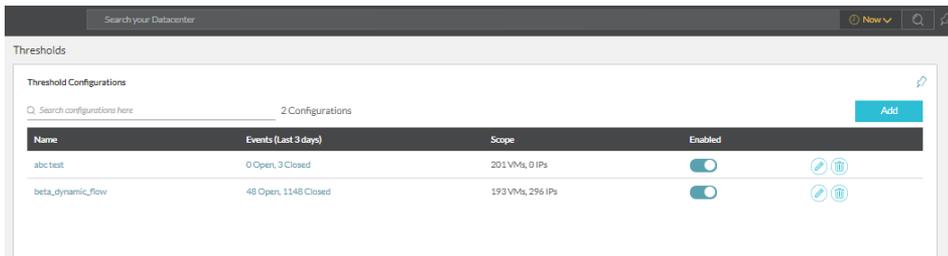
- 7 Klicken Sie auf **Absenden**, um die Schwellenwertkonfiguration zu erstellen.

Anzeigen der Seite „Schwellenwertkonfiguration“

Nachdem Sie eine Schwellenwertkonfiguration hinzugefügt haben, können Sie deren Details auf der Seite **Schwellenwertkonfiguration** anzeigen.

Verfahren

- 1 Klicken Sie im linken Navigationsbereich auf **Analyse**. Klicken Sie auf **Schwellenwerte**.

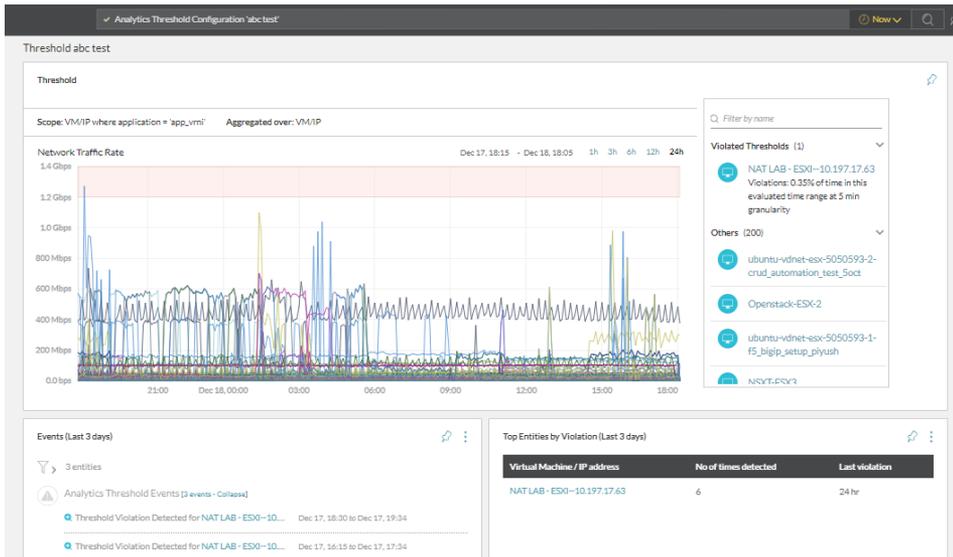


- 2 Die folgenden Details für eine Schwellenwertkonfiguration werden bereitgestellt:

- Name
- Events
- Scope

Wenn die Konfiguration deaktiviert ist, wird die Warnung für den Verstoß gegen diesen bestimmten Schwellenwert nicht generiert. Sie können auf dieser Seite auch nach einer bestimmten Schwellenwertkonfiguration suchen.

- 3 Klicken Sie in der Liste auf die gewünschte Schwellenwertkonfiguration, um das Dashboard für diese bestimmte Konfiguration anzuzeigen.



Sie können die folgenden Widgets auf dem Dashboard anzeigen:

- Diagramm: Das Schwellenwertdiagramm hilft Ihnen, die Einheiten zu erkennen, die gegen die Schwellenwerte verstoßen haben.
- Ereignisse: Dieses Widget enthält die Liste der Ereignisse, die für verletzte Schwellenwerte für die letzten drei Tage generiert wurden.
- Top-Einheiten nach Verstoß: Mit diesem Widget können Sie die wichtigsten Einheiten kennen, die die Ursache von Aberrationen für die letzten drei Tage gewesen sind.

Anzeigen der Topologie der Einheit

13

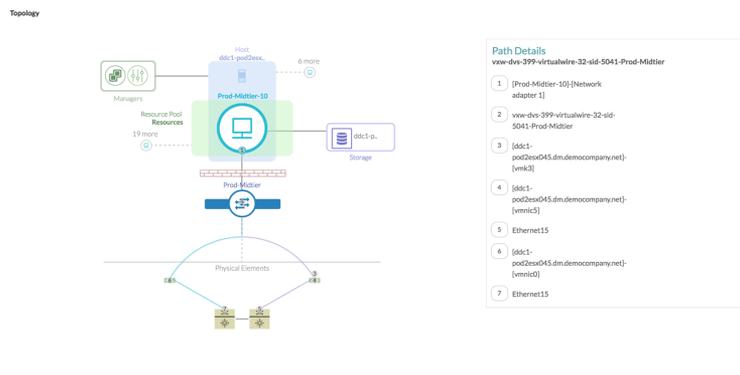
Die Topologie enthält eine umfassende bildliche Darstellung der Einheit.

Dieses Kapitel enthält die folgenden Themen:

- Topologie der virtuellen Maschine
- Host-Topologie
- VXLAN-Topologie
- VLAN-Topologie
- NSX Manager-Topologie

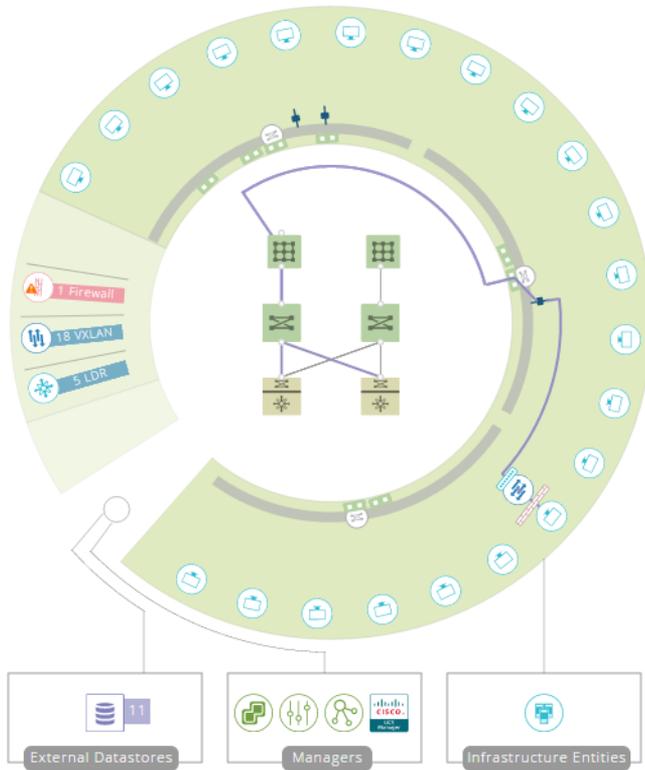
Topologie der virtuellen Maschine

Die Topologie der virtuellen Maschine bietet eine umfassende Ansicht einer einzelnen virtuellen Maschine in Bezug auf den Rest Ihres Datacenters.



Host-Topologie

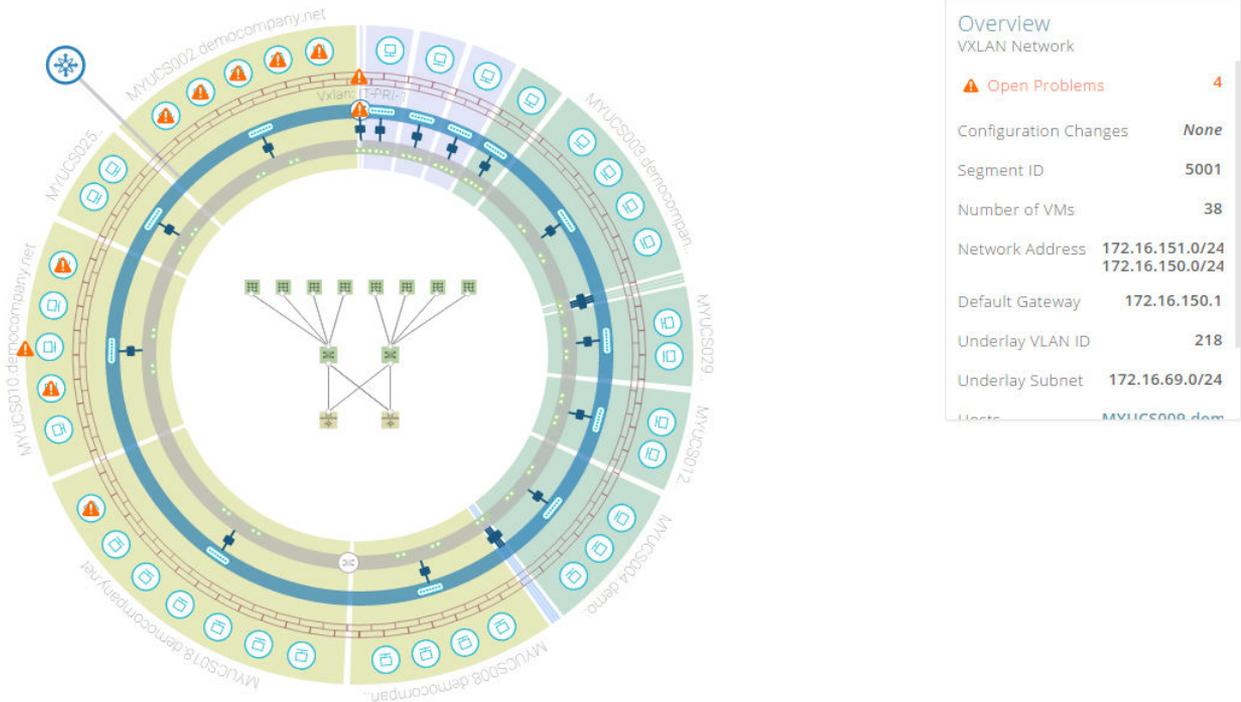
Die Host-Topologie zeigt, wie VMs eines bestimmten Hosts mit den virtuellen und physischen Komponenten Ihres Datacenters verbunden sind, und auch, wie der Host selbst mit Ihrem Datacenter verbunden ist.



VXLAN-Topologie

Die VXLAN-Overlay-Netzwerktechnologie (Virtual eXtensible Local Area Network) ist ein Industriestandard, der von VMware gemeinsam mit den wichtigsten Netzwerkanbietern entwickelt wird.

Die VXLAN-Topologie ist eine innovative Visualisierung, die Ihnen einen Überblick über die ausgewählte VXLAN bietet. Das folgende Diagramm erläutert die verschiedenen Komponenten, aus denen die Visualisierung besteht:



Hinweis Sowohl virtuelle als auch physische Komponenten können auf diese Weise visualisiert werden.

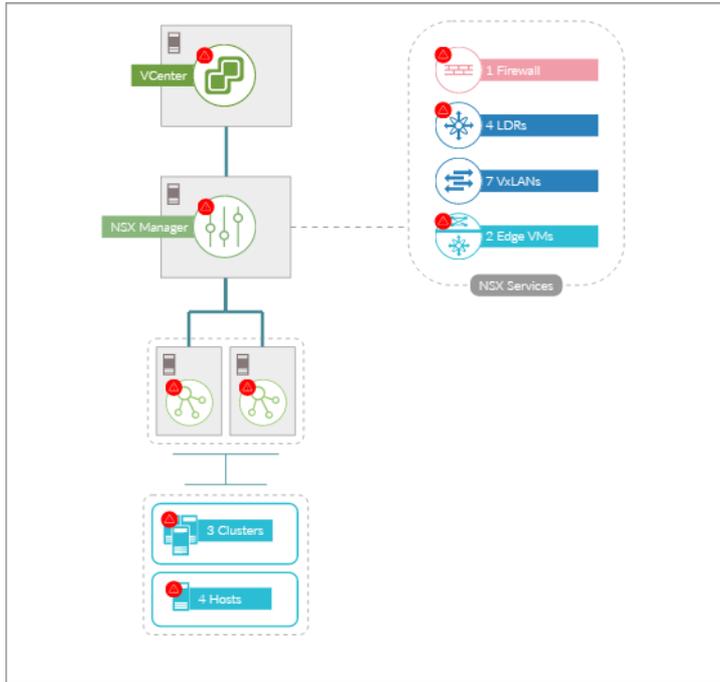
VLAN-Topologie

Virtuelle LANs (VLANs) ermöglichen die weitere Segmentierung eines einzelnen LAN-Segments, damit Portgruppen so voneinander isoliert werden können, als befänden sie sich auf unterschiedlichen physischen Segmenten.

Die VLAN-Topologie wird auf ähnliche Weise wie die VxLAN-Topologie erstellt.

NSX Manager-Topologie

In der NSX Manager-Topologie werden die Komponenten angezeigt, die mit NSX Manager verknüpft sind.



Anzeigen von Überwachungsinformationen von NSX-Objekten in vRealize Network Insight

vRealize Network Insight kann über NSX-T Manager und NSX-V Manager schnell Überwachungsinformationen von NSX-Objekten erfassen. Die Informationen umfassen den Benutzernamen, der das NSX-Objekt erstellt oder geändert hat, den Zeitpunkt, zu dem der Vorgang stattgefunden hat, und die Vorgangsdetails für das Objekt.

Wenn Sie Überwachungsprotokolle in NSX-T Manager oder NSX-V Manager aktiviert haben, kann vRealize Network Insight die Überwachungsdetails für einige der NSX-T- und NSX-V-Objekte erfassen.

NSX-V

Liste der NSX-V-Objekte, für die vRealize Network Insight Überwachungsdetails innerhalb von drei bis fünf Minuten erfasst.

- SecurityGroup
- SecurityGroupTranslation
- FirewallConfiguration
- FirewallStatus
- IPSet
- SecurityTag
- UniversalSecurityGroup
- UniversalSecurityGroupTranslation

■ UniversalIPSet

Die Überwachungsdetails der NSX-V-Objekte werden für die Ereignisse „Ermittlung“, „Eigenschaftsänderung“ und „Löschen“ erfasst:

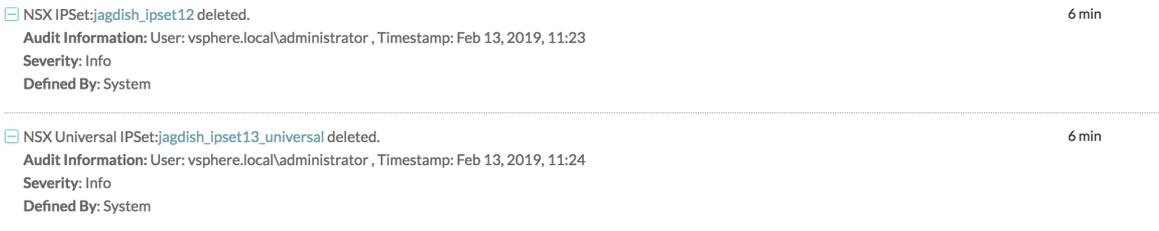
■ Discovery



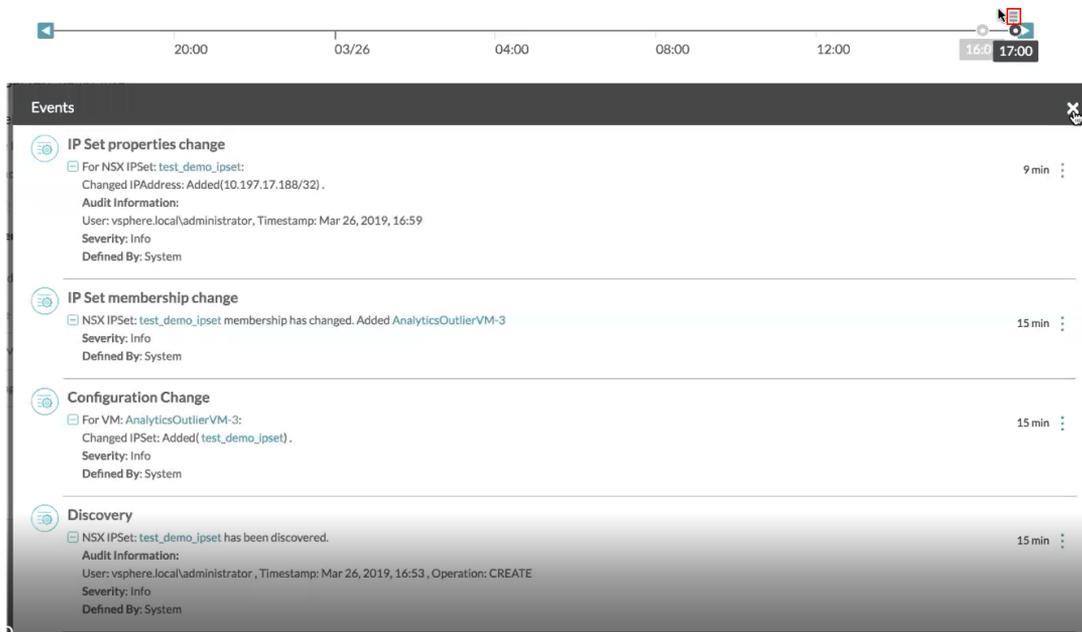
■ Properties Change



■ Delete



Sie können die Überwachungsinformationen auch auf der Zeitachse des Objekts anzeigen.



NSX-T

Liste der NSX-T-Objekte, für die vRealize Network Insight Überwachungsdetails erfasst.

Hinweis Die Überwachungsinformationen stehen für die Elemente der VMC-Richtlinie nicht zur Verfügung.

- NSGroup
- NSService
- NSServiceGroup
- NSFirewallRule

Hinweis Die Überwachungsinformationen stehen für das Ereignis „Löschen“ der NSFirewallRule nicht zur Verfügung.

- IPSet
- NSX-Richtliniengruppe
- Firewallregel der NSX-Richtlinie

Die Überwachungsdetails der NSX-T-Objekte werden für die Ereignisse „Ermittlung“, „Eigenschaftsänderung“ und „Löschen“ erfasst:

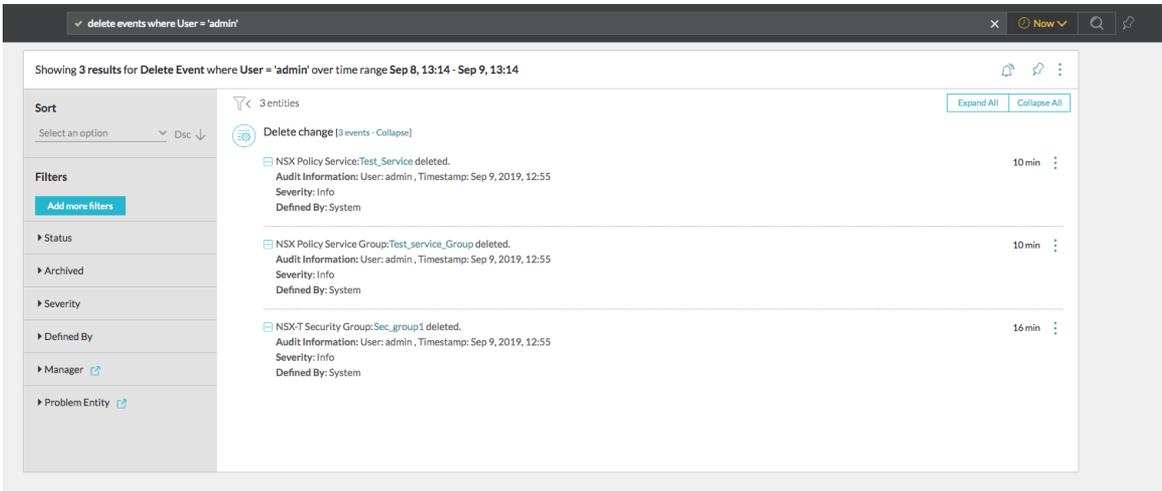
- Discovery



■ Properties Change



■ Delete



Hinweis Die Ereignisse vom Typ „Löschen“ stehen im Element-Dashboard nicht zur Verfügung. Sie können das Ereignis jedoch durchsuchen, um die Überwachungsinformationen anzuzeigen.

Beispielabfragen zum Anzeigen von Überwachungsinformationen

- `events where user = username`
- `discovery events where user = username`
- `delete events where user = username`
- `change events where user = username`

Alle Teile der Anwendung werden als Pins bezeichnet – grundlegende Einheiten, die gespeichert und in Klubdaten gruppiert werden können, die Sie für hilfreich erachten und mit anderen Mitgliedern Ihres Teams gemeinsam nutzen können. Sie können eine Suchabfrage und auch die für eine Einheit verfügbaren Pins anheften.

Um einen Pin hinzuzufügen, klicken Sie auf das Pin-Symbol. Alle gespeicherten Pins werden im Abschnitt „Pinnwände“ angezeigt, der durch Klicken auf das Pinnwandensymbol in der Kopfzeile aufgerufen werden kann.

Dieses Kapitel enthält die folgenden Themen:

- [Pins](#)
- [Pinnwände](#)

Pins

Die Informationen auf jeder Einheitsseite werden in Pins aufgetrennt. Alle Einheitsseiten bestehen aus Pins und jeder Pin enthält ein bestimmtes Bit an Informationen im Zusammenhang mit der Einheit.

Die Pins verfügen über die folgenden Funktionen:

- Sie können die Ansicht eines beliebigen Pins mit der Schaltfläche „Weitere Optionen“ () maximieren und auch weitere Informationen über den Pin mit der Option **Hilfe** anzeigen.
- Pins können auch Filter enthalten, damit Sie für die Daten, die auf dem Pin angezeigt werden, einen Drill-Down vornehmen können.
- Viele Pins enthalten auch die Option „Als CSV exportieren“, sodass Sie die Daten, die im Pin vorhanden sind, im CSV-Format exportieren können. Sie können die spezifischen Eigenschaften und die Anzahl der CSV-Zeilen, die Sie exportieren möchten, in dem angezeigten Dialogfeld auswählen.

Hinweis Wenn alle Felder ausgewählt sind, dauert die Funktion „Als CSV exportieren“ für die Flow-Daten mehr als 30 Minuten für 180.000 Flows.

Pintypen

Die meisten der in der Software verfügbaren Pins können in folgende Kategorien eingeteilt werden:

Metrik-Pins

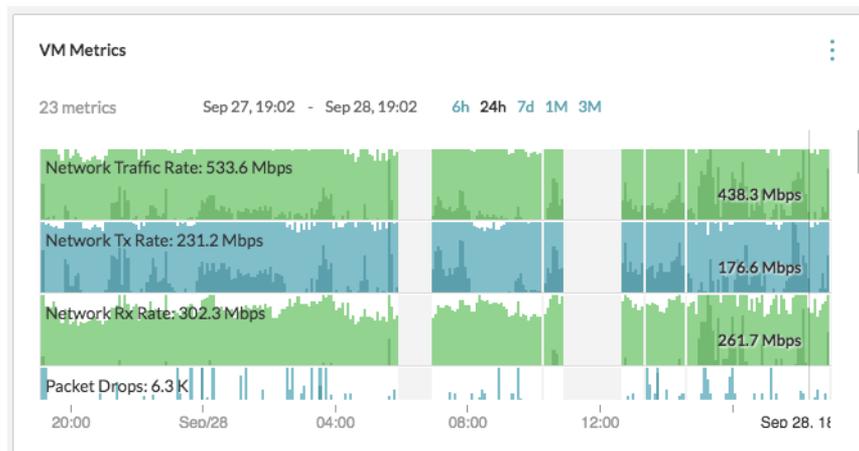
Die Metrik-Pins zeigen wichtige Metriken, die sich auf die ausgewählte Einheit beziehen.

Die Metrik-PIN verwendet das Kubismus-Diagramm zum Anzeigen von Daten, indem jedes Diagramm in zwei Bänder aufgeteilt und der höhere Wert über einen anderen verschoben wird. Die höheren Werte werden daher in dunklerer Farbe angezeigt und sind leichter zu erkennen.

Sie können die anzuzeigende Metrik in der Dropdown-Liste in der Pin-Kopfzeile auswählen und die Auswahl der anzuzeigenden Einheiten ändern.

Der Zeitraum kann geändert werden, indem entweder die Bereichsvoreinstellungen verwendet werden oder benutzerdefinierte Datum/Uhrzeit eingegeben werden.

Ein Beispiel für den Metrik-Pin ist der VM-Metrik-Pin. Dieser Pin zeigt die Netzwerkdatenverkehrsrate, die Netzwerk-TX-Rate, die Netzwerk-RX-Rate und die Paketverwerfungen der virtuellen Maschine an.

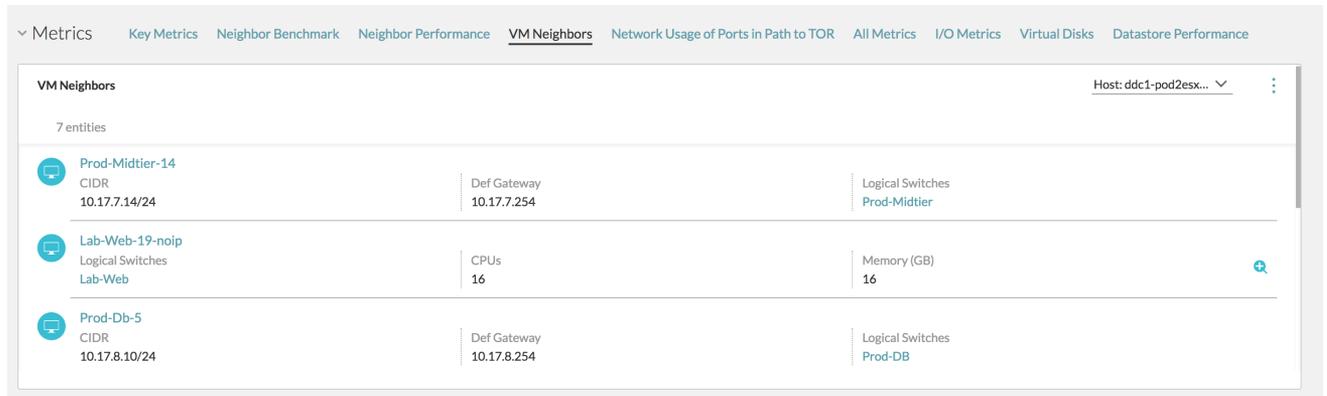


Ansichtspins der Einheitsliste

Die Ansichtspins der Einheitsliste zeigen eine Liste von Einheiten an, die nach einem gemeinsamen Thema gruppiert sind. Die Liste enthält wichtige Attribute pro Einheit.

Sie können weitere Attribute einer bestimmten Einheit anzeigen, indem Sie ganz rechts auf das Symbol „Vergrößern“ klicken. Durch Klicken auf den Einheitsnamen gelangen Sie zur Seite „Einheit“.

Wie andere Pins beherbergt das Filtersymbol verschiedene Facets, mit denen die Liste gefiltert werden kann. Ein Beispiel für den Ansichtspin der Eintragsliste ist der Pin „VM-Nachbarn“. Standardmäßig zeigt dieser Pin die VMs an, die auf demselben Host vorhanden sind. Sie können VMs auch nach Sicherheitsgruppen, VXLAN und Datenspeicher filtern.



Pins der Ereignisansichtsliste

Die Pins der Ereignislistenansicht stellen eine Liste von Ereignissen in chronologischer Reihenfolge für eine bestimmte Einheit oder eine Gruppe von Einheiten bereit (die aus der Dropdown-Liste in der Pin-Kopfzeile ausgewählt werden können).

Sie können ändern, wie weit zurück in der Zeit (ab dem aktuellen Zeitpunkt) der Pin die Ereignisse anzeigen soll, indem Sie die verfügbaren Voreinstellungen verwenden oder ein benutzerdefiniertes Datum/eine Uhrzeit eingeben. Andere Filteroptionen, z. B. **Ereignisstatus** und **Ereignistyp**, können durch Klicken auf das Filtersymbol ausgewählt werden.

Im nachfolgenden Image werden die Ereignisse im Zusammenhang mit VM Prod-db-vm21 und den zugehörigen Einheiten angezeigt. Sie können auf den Namen der Einheit klicken, um Ereignisse von anderen verwandten Einheiten anzuzeigen. Mithilfe des Filters können Sie die Ereignisse basierend auf ihrem Status und ihren Typen filtern. Ein Ereignis kann eine Änderung oder ein Problem im Zusammenhang mit einer Einheit sein.

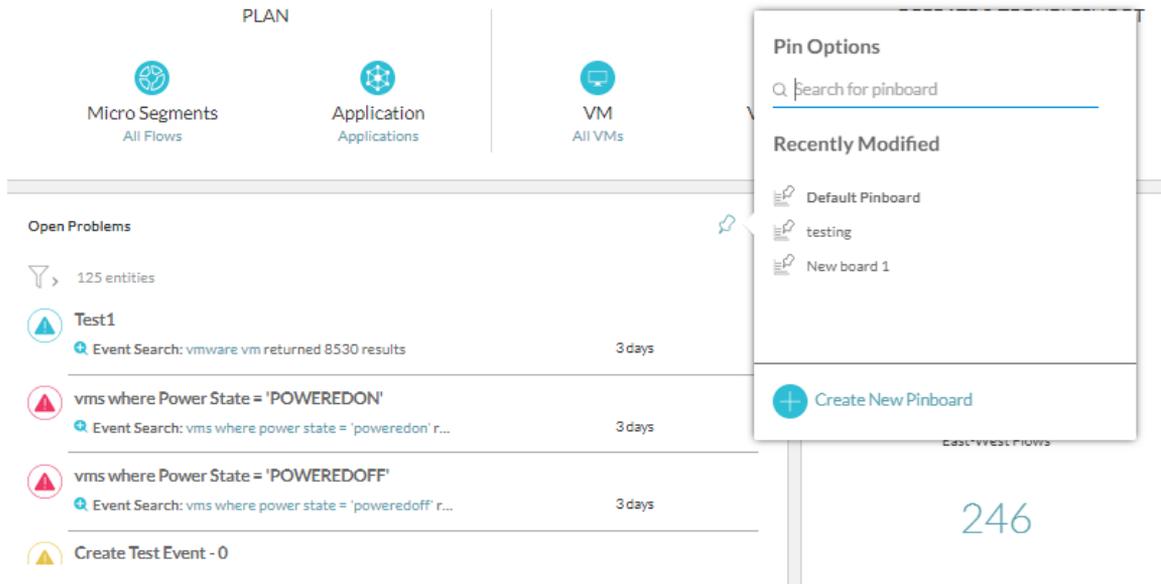


Sie können mithilfe der Ereignissuchabfrage nach den Ereignissen suchen. Sie können nach offenen oder geschlossenen Ereignissen mit Abfragen wie z. B. offene Ereignisse oder geschlossene Ereignisse suchen. Sie können auch nach Problemen mit den gleichen Modifikatoren suchen.

Pinnwände

Sie können jedes beliebige Widget von einer beliebigen Seite auf einer Pinnwand anheften, um den Zugriff auf und die gemeinsame Nutzung von Daten zu vereinfachen.

Erstellen einer Pinnwand



- 1 Klicken Sie auf das Pin-Symbol auf dem Widget, das Sie anheften möchten.
- 2 Klicken Sie im Popup-Fenster auf **Neue Pinnwand erstellen**.

Hinweis

- Wenn Sie noch keine Pinnwand erstellt haben, können Sie **Standard-Pinnwand** aus der Liste **Kürzlich geändert** auswählen.

Hinweis Die Standard-Pinnwand bietet dem erstmaligen Benutzer das Aussehen und Verhalten einer typischen Pinnwand. Sie hilft dem Benutzer, sich mit dem Layout und den Funktionen einer Pinnwand vertraut zu machen. Sie kann nicht freigegeben oder gelöscht werden. Sie können Pins von der Standard-Pinnwand auf eine beliebige benutzerdefinierte Pinnwand kopieren.

- Die maximale Anzahl von Einträgen, die in der Liste „Kürzlich geändert“ angezeigt werden können, ist 15.
- Die maximale Anzahl von Pinnwänden, die Sie für alle Benutzer erstellen können, ist 500.

Hinweis Die Gesamtzahl der Pinnwände umfasst die benutzerdefinierten Pinnwände, die freigegebenen Pinnwände und die standardmäßigen Pinnwände.

- Die maximale Anzahl der Pins pro Pinnwand ist 20.

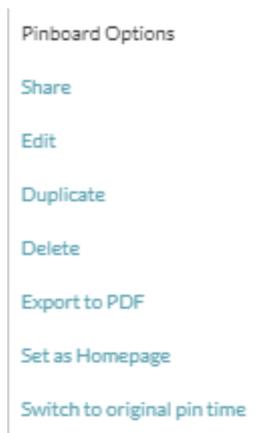
- 3 Geben Sie im Fenster **Pinwand erstellen** den Namen und die Beschreibung für die neue Pinwand ein. Klicken Sie auf **Erstellen und Pinnen**.

Hinweis

- Der Name der Pinwand muss im gesamten System eindeutig sein.
- Die maximal zulässige Zeichenanzahl für den Pinwandnamen ist 100. Sie können nur Buchstaben, Ziffern und Leerzeichen für den Namen der Pinwand verwenden.

- 4 Die Meldung **Pinwand erstellt** wird angezeigt. Klicken Sie auf **Jetzt freigeben**, um die Pinwand sofort freizugeben.
- 5 Um das Widget an eine vorhandene Pinwand anzuheften, wählen Sie die Pinwand unter **Kürzlich geändert** aus und klicken Sie auf **Pinnen**. Die Meldung **Ihr Pin wurde hinzugefügt** mit dem Link zur entsprechenden Pinwand wird angezeigt.

Zugreifen auf die Pinwandoptionen



Klicken Sie auf **Weitere Optionen** in der oberen rechten Ecke einer Pinwand, um auf die **Pinwandoptionen** zuzugreifen.

Hinweis Sie können alle Pinwandoptionen nur dann anzeigen, wenn Sie die Pinwand erstellt haben oder wenn Sie sie für einen anderen Benutzer mit den Berechtigungen **Anzeigen und Bearbeiten** freigegeben haben. Jeder andere Benutzer sieht nur die Optionen **In PDF exportieren** und **Zur ursprünglichen Pinzeit wechseln** sehen.

Auf der Pinwand können Sie die folgenden Aktionen durchführen:

- Sie können die Pinwand für alle anderen vorhandenen vRealize Network Insight-Benutzer freigeben.
- Sie können den Namen der Pinwand und den Pin auf der Pinwand bearbeiten.
- Sie können die Pins auf einer Pinwand neu anordnen. Ihre Positionen werden beibehalten.
- Klicken Sie auf **Löschen**, um diese bestimmte Pinwand zu löschen.

- Klicken Sie auf **In PDF exportieren**, um die Informationen auf der Pinnwand als PDF-Bericht zu exportieren. Weitere Informationen finden Sie unter [Als PDF exportieren](#).
- Um die Daten auf dem Pin zum Zeitpunkt des Pinnens anzuzeigen, klicken Sie auf **Zur ursprünglichen Pinnzeit wechseln**. Mit dieser Funktion können Sie die Daten für jede Pin zum Zeitpunkt der Erstellung anzeigen.

Arbeiten mit dem Schieberegler für eine Pinnwand

vRealize Network Insight unterstützt einen Zeitachsen-Schieberegler auf Pinnwänden. Um die Pinnwanddaten für jede gewünschte Zeit anzuzeigen, können Sie den Schieberegler für die Zeitachse verwenden. Wenn eine Pinnwand geladen wird, werden alle Pins für die aktuelle Zeit (**Jetzt**) geladen.

Ansicht der Pinnwandbibliothek

Wenn Sie ein Admin-Benutzer sind, können Sie die Registerkarte **Meine Pinnwände** und die Registerkarte **Alle Pinnwände** in der Pinnwandbibliothek sehen, wie in der folgenden Abbildung gezeigt. Wenn Sie ein Mitgliedsbenutzer sind, sehen Sie eine Liste der Pinnwände in der Pinnwandbibliothek.

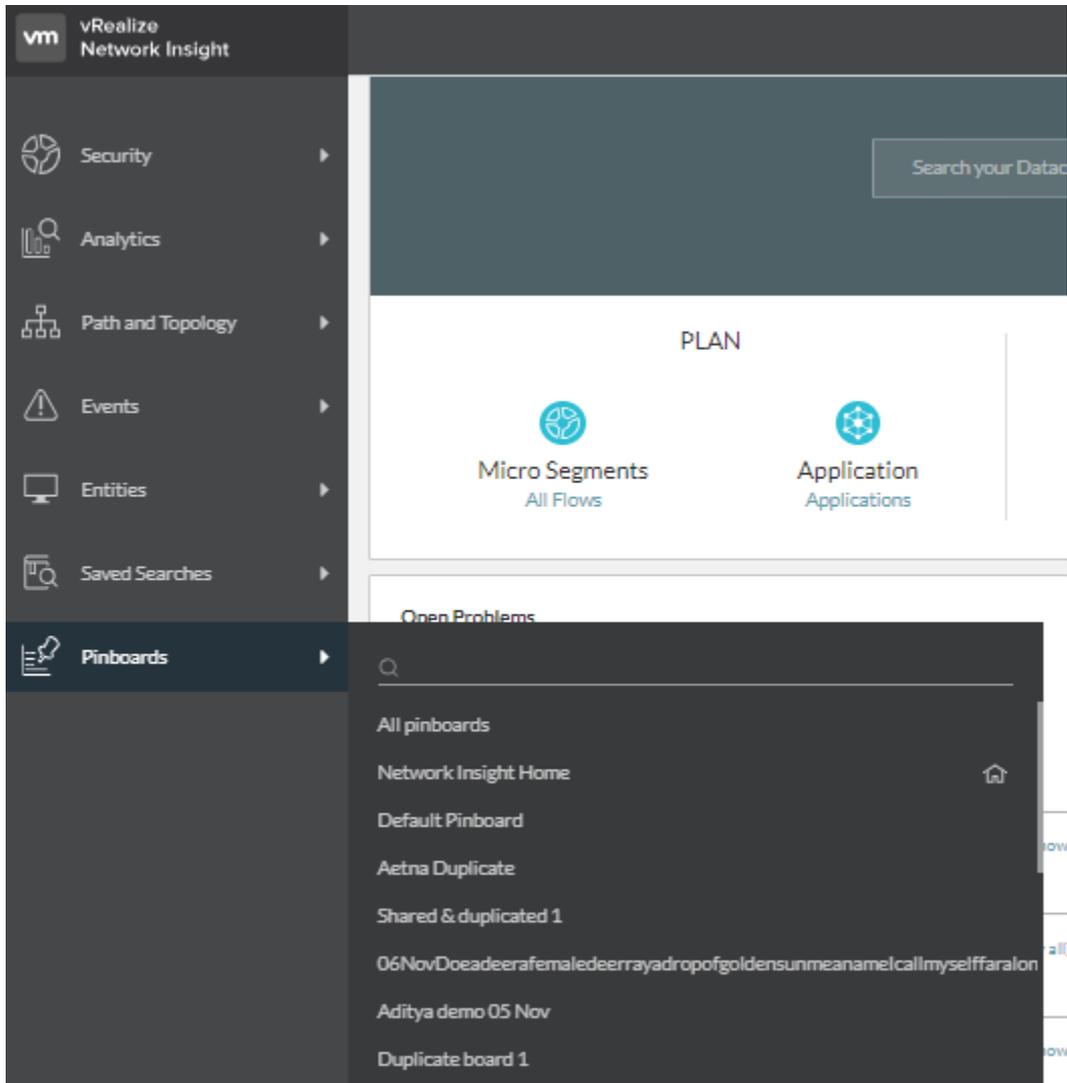
 Pinboards

Search for pinboards 17 pinboards

Pinboard name	Last modified	Owner	Shared	Actions
Network Insight Home 	--	--	--	
Default Pinboard	81 days	Guest 1	Not shared	
Aetna Duplicate	24 days	Guest 1	Not shared	  
Shared & duplicated 1	30 days	Guest 1	5 others	  

- 1 Klicken Sie in der linken Navigationsleiste der Startseite auf **Pinnwände**.
- 2 Klicken Sie auf **Alle Pinnwände**, um alle Pinnwände im System anzuzeigen.
- 3 In der Navigationsleiste können Sie die Liste der vorhandenen Pinnwände anzeigen. Die Liste enthält dieselben Elemente wie die Registerkarte **Meine Pinnwände** in der Pinnwandbibliothek. Die zuletzt geänderte Pinnwand wird oben in der Liste angezeigt. Klicken Sie auf die Pinnwand, die Sie ansehen möchten.

Hinweis Es dauert einige Zeit, bis die Pinnwand in dieser Liste angezeigt wird, nachdem sie erstellt wurde.



4 Sie können auch eine Suche nach einer Pinwand in der Bibliothek durchführen.

Kopieren eines Pins

- 1 Klicken Sie auf das Pin-Symbol im Widget.
- 2 Wählen Sie die Pinwand aus, auf die Sie den Pin kopieren möchten.
- 3 Klicken Sie auf **Hinzufügen**.

Gemeinsame Nutzung und Zusammenarbeit mit Pinwänden

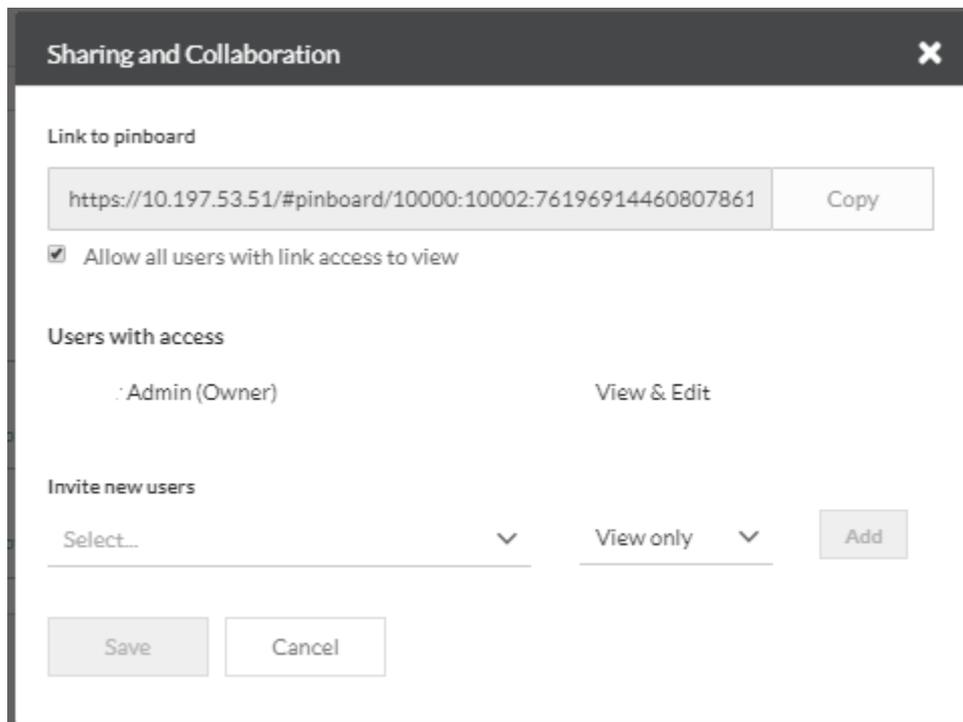
Sie können die Pinwände, die Sie erstellen, zur gemeinsamen Nutzung für andere Benutzer freigeben. Ein Admin-Benutzer kann jede Pinwand anzeigen und löschen. Im Folgenden finden Sie die Funktionen für gemeinsame Nutzung und Zusammenarbeit mit Pinwänden:

Wenn Sie eine Pinwand erstellt haben, können Sie sie anzeigen, bearbeiten oder löschen, unabhängig davon, ob Sie ein Administrator oder ein Mitgliedsbenutzer sind.

Tabelle 14-1.

Pinnwandbesitzer	Gemeinsam genutzt mit	Recht	Mögliche Aktion
Administrator	Administrator	Anzeigen und bearbeiten	Anzeigen, bearbeiten, löschen
	Administrator	Nur anzeigen	Anzeigen, löschen
	Mitglied	Anzeigen und bearbeiten	Anzeigen, bearbeiten
	Mitglied	Nur anzeigen	Anzeigen
Mitglied	Administrator	Anzeigen und bearbeiten	Anzeigen, bearbeiten, löschen
	Administrator	Nur anzeigen	Anzeigen, löschen
	Mitglied	Anzeigen und bearbeiten	Anzeigen, bearbeiten
	Mitglied	Nur anzeigen	Anzeigen

Hinweis Wenn eine Pinnwand gelöscht werden muss und der Benutzer, der sie erstellt hat, nicht verfügbar ist, kann der Admin-Benutzer sie löschen.



So geben Sie eine Pinnwand frei:

Verfahren

- 1 Klicken Sie auf der Pinnwand, die Sie freigeben möchten, auf **Weitere Optionen**.

- 2 Klicken Sie auf **Freigeben**.
- 3 Sie können auch eine Pinnwand von der **Pinnwandbibliothek** freigeben, indem Sie auf das Symbol „Freigabe“ unter **Aktionen** klicken.
- 4 Der Freigabe-Link ist standardmäßig aktiviert. Sie können den Link einer Pinnwand für jeden Benutzer freigeben, der angemeldet ist.
- 5 Sie können die Benutzer, für die Sie die Pinnwand freigeben möchten, hinzufügen. Sie können für einen bestimmten Benutzer die Berechtigungen wie z. B. `view` und `view and edit` angeben.

Hinweis Der Benutzer, der nur über die Berechtigung „Anzeigen“ verfügt, kann die Pinnwand nicht für andere Benutzer freigeben.

- 6 Klicken Sie auf **Speichern**, um die von Ihnen vorgenommenen Änderungen in Bezug auf gemeinsame Nutzung und Zusammenarbeit zu speichern.
- 7 Sie können die Informationen zur gemeinsamen Nutzung und Zusammenarbeit für jede Pinnwand über eine der folgenden Optionen anzeigen.
 - In der **Pinnwandbibliothek** können Sie die Freigabeinformationen in der Spalte **Gemeinsam genutzt** für eine bestimmte Pinnwand anzeigen.
 - Klicken Sie auf das Pin-Symbol im Widget. Zeigen Sie auf eine der Pinnwände, die unter **Kürzlich geändert** aufgeführt sind, um die Details bezüglich des Besitzers und für wen diese freigegeben wurde, anzuzeigen.

Festlegen einer Pinnwand als Startseite

Sie können eine Pinnwand Ihrer Wahl als Standard-Startseite festlegen.

Verfahren

- 1 Navigieren Sie zur gewünschten Pinnwand, die Sie als Startseite festlegen möchten.
- 2 Klicken Sie auf **Pinnwandoptionen**. Klicken Sie auf **Als Startseite festlegen**.
Diese bestimmte Pinnwand wird als Startseite festgelegt.

Hinweis Nachdem Sie eine Pinnwand als Startseite festgelegt haben, ist die Option **Als Startseite festlegen** auf dieser Pinnwand deaktiviert.

- 3 Sie können auch eine bestimmte Pinnwand als Standard-Startseite auf der Seite **Meine Einstellungen** unter **Einstellungen** festlegen.

- Wenn Sie die vorherige Startseite anzeigen möchten, klicken Sie im linken Navigationsbereich auf **Network Insight Home** unter **Pinnwände**. Die Nachricht **Möchten Sie Network Insight Home als Startseite festlegen?** wird eingeblendet. Wenn Sie die Standard-Startseite wiederherstellen möchten, klicken Sie auf **Startseite festlegen**. Klicken Sie auf **Verwerfen**.

Hinweis

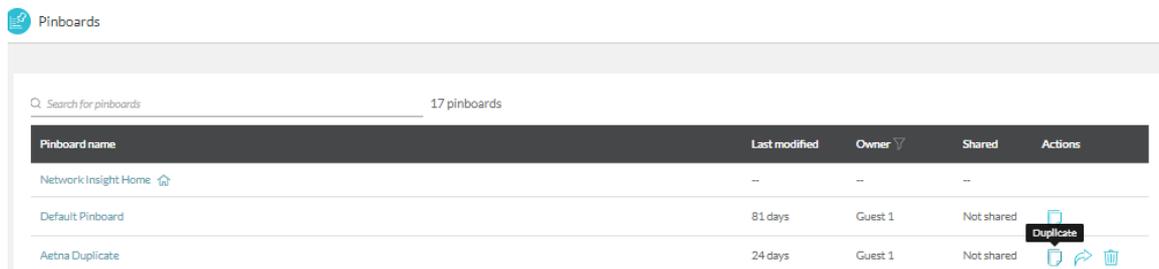
- Wenn Sie eine Pinnwand löschen, die Sie als Startseite festgelegt haben, wird die Standard-Startseite auf **Network Insight Home** zurückgesetzt. Wenn Sie der Besitzer der Pinnwand sind, die Sie löschen, wird eine Meldung zur Löschbestätigung eingeblendet.
- Wenn ein anderer Benutzer die Pinnwand, die Sie erstellt haben, als Startseite festgelegt hat, wird die Startseite, wenn Sie sie löschen, für diesen Benutzer automatisch wieder auf **Network Insight Home** zurückgesetzt.

Ergebnisse

Duplizieren einer Pinnwand

Verfahren

- Klicken Sie auf das Symbol „Duplizieren“ unter **Aktionen** für die jeweilige Pinnwand in der Liste in der Pinnwandbibliothek.



- Ein Pop-up-Fenster wird geöffnet, in dem Sie den Namen der Pinnwand eingeben müssen. Die Beschreibung entspricht der der ursprünglichen Pinnwand. Klicken Sie auf **Duplizieren**.

Hinweis Der Name der Pinnwand ist obligatorisch. Die Schaltfläche **Duplizieren** wird erst aktiviert, nachdem Sie den Namen eingegeben haben.

- Wenn Sie versuchen, eine Pinnwand zu duplizieren, die gemeinsam genutzt wird, können Sie die Benutzer und Berechtigungen der Quellpinnwand beibehalten. Wählen Sie **Benutzer und Berechtigungen der Quellpinnwand beibehalten** aus, wenn Sie diese beibehalten möchten.

Hinweis Wenn die Pinnwand, die Sie duplizieren möchten, nur schreibgeschützt für Sie freigegeben wurde, sehen Sie die Option **Benutzer und Berechtigungen der Quellpinnwand beibehalten** nicht.

Der Benutzer, der eine Pinnwand dupliziert, wird zum Besitzer der neuen Pinnwand.

Unterstützung für Lastausgleichsdienst vRealize Network Insight

15

Mit Lastausgleich können Sie eingehenden Anwendungsdatenverkehr über mehrere Back-End-Ziele verteilen. Dazu gehören auch Bereitstellungen in öffentlichen oder privaten Clouds. Es ist daher notwendig, über ein Konzept für die Sammlung von Back-End-Zielen zu verfügen.

vRealize Network Insight supports the following load balancing devices.

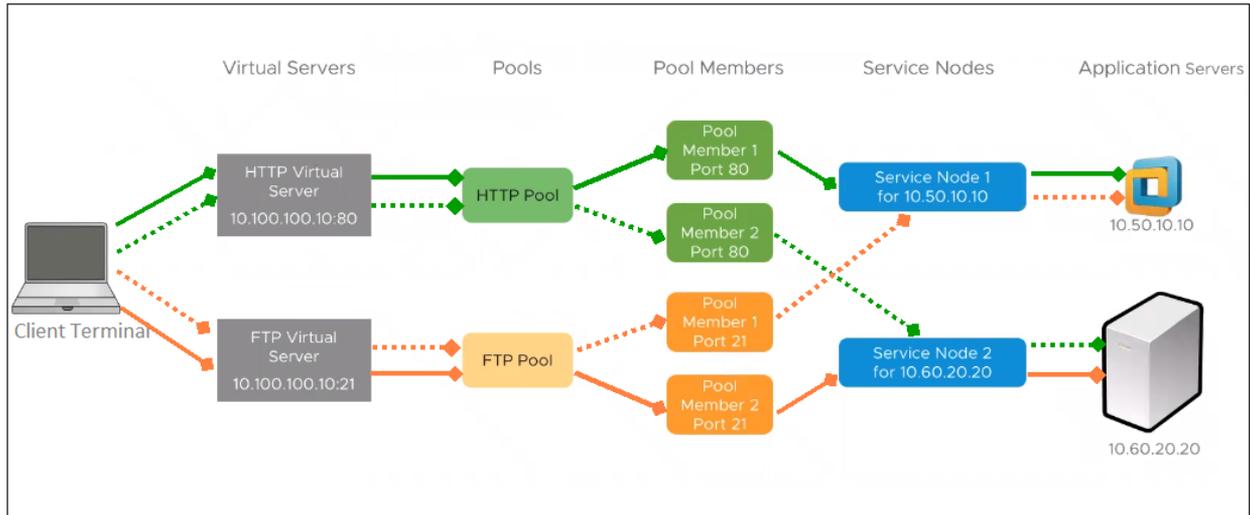
Dieses Kapitel enthält die folgenden Themen:

- [F5 als Lastausgleichsdienst](#)
- [NSX-V als Lastausgleichsdienst](#)

F5 als Lastausgleichsdienst

Um die Lastausgleichsfunktion von F5 zu unterstützen und zu aktivieren, wurden die erforderlichen Komponenten bzw. Einheiten zu vRealize Network Insight hinzugefügt.

Überblick über einen F5-Lastausgleichsdienst und seine Komponenten



- **Anwendungsserver:** Die Maschinen, auf denen die Anwendungen gehostet werden. Wenn Sie beispielsweise über einen Webserver verfügen, wird der Server auf Anwendungsservern ausgeführt (physischer oder virtueller Server).
- **Dienstknoten:** F5 stellt die Anwendungsserver als Dienstknoten dar. Daher hat der Dienstknoten dieselbe IP-Adresse bzw. denselben FQDN wie der Anwendungsserver. Jeder Dienstknoten kann über mehrere Anwendungen verfügen.
- **Poolmitglieder:** Eine logische Einheit. Jede Anwendung in einem Dienstknoten wird durch ein Poolmitglied dargestellt, das dieselbe IP-Adresse bzw. denselben FQDN hat wie der Dienstknoten. Zur Kennzeichnung verschiedener Anwendungen betten die Poolmitglieder die Portnummer in die IP-Adresse der Dienstknoten ein.
- **Pools:** Alle Poolmitglieder, die eine Anwendung bereitstellen, sind zu einem Pool gruppiert.
- **Virtuelle Server:** Eine öffentliche IP-Adresse der Anwendung. Die Clients, die eine Anwendung verwenden möchten, stellen also eine Verbindung mit der IP-Adresse (z. B. 10.100.100.10) und der Portnummer (80 oder 21) des virtuellen Servers her.
- **Client-Terminal:** Die Verbindung beginnt bei einem Client-Terminal. Dabei handelt es sich um eine virtuelle Maschine.

Die Clientanforderung stellt eine Verbindung zum virtuellen Server her, der auf der Basis des Pools über die Poolmitglieder bestimmt. Die Poolmitglieder leiten die Anforderung dann an den Anwendungsserver (VM oder physischen Server) weiter.

Hinweis Ein einzelner Anwendungsserver kann mehrere Anforderungen von unterschiedlichen Ports und unterschiedlichen Dienstknoten bereitstellen.

vRealize Network Insight bietet zusätzliche Vorteile bei der Unterstützung der Lastausgleichsfunktion:

- Sie können damit ermitteln, ob es sich bei den Anwendungsservern um physische Server oder virtuelle Maschinen handelt.
- Dank des Einblicks in Informationen zum Anwendungsserver (Host oder VM), wie z. B. Konfiguration, Leistung, Flows, ist die Fehlerbehebung damit einfach.
- Sie erhalten Einblick in die physischen oder virtuellen Netzwerkkomponenten in einer Anwendung mit verteilter Last.
- Bei Problemen in der Umgebung werden Warnungen ausgegeben; außerdem können Sie damit den Grund für das Problem ermitteln. Beispiel: Die Anwendung reagiert nicht, weil die Dienstknoten-VM ausgefallen ist.
- Sie gewinnen dadurch lückenlose Einsicht in Flows.

Anzeigen von Details zum Lastausgleichsdienst

Auf der Seite „Lastausgleichsdienst“ werden alle Informationen der virtuellen Server und der Pools zusammengefasst, die auf dem Lastausgleichsdienst erstellt werden.

Sie sehen die folgenden Informationen:

- Liste der virtuellen Server auf dem Lastausgleichsdienst sowie die zugehörigen Probleme
- Liste der Pools auf dem Lastausgleichsdienst und die zugehörigen Probleme
- Dem Lastausgleichsdienst zugeordnete Ereignisse
- Liste der Flows, Anzahl und Netzwerkdatenverkehr auf verschiedenen Ziel-IPs

Hinweis Für NSX-V-Lastausgleichsdienste werden die Flow-Informationen nicht erfasst.

- Eigenschaften des Lastausgleichsdiensts, der Informationen wie z. B. Anbieter, Typ, Seriennummer, virtuelle Server und Pools bereitstellt.

Anzeigen von Details zum virtuellen Server

Auf der Seite „Virtueller Server“ werden die Metriken zum virtuellen Server und die Problem- und Änderungsereignisse angezeigt.

Sie sehen die folgenden Informationen:

- Die Liste aller Poolmitglieder im virtuellen Server und die zugehörigen Details sowie bei Problemen jeweils eine Warnung
- Die Liste der virtuellen Maschinen
- Die Liste der physischen Server
- Die Liste der dem virtuellen Server zugeordneten Problemereignisse

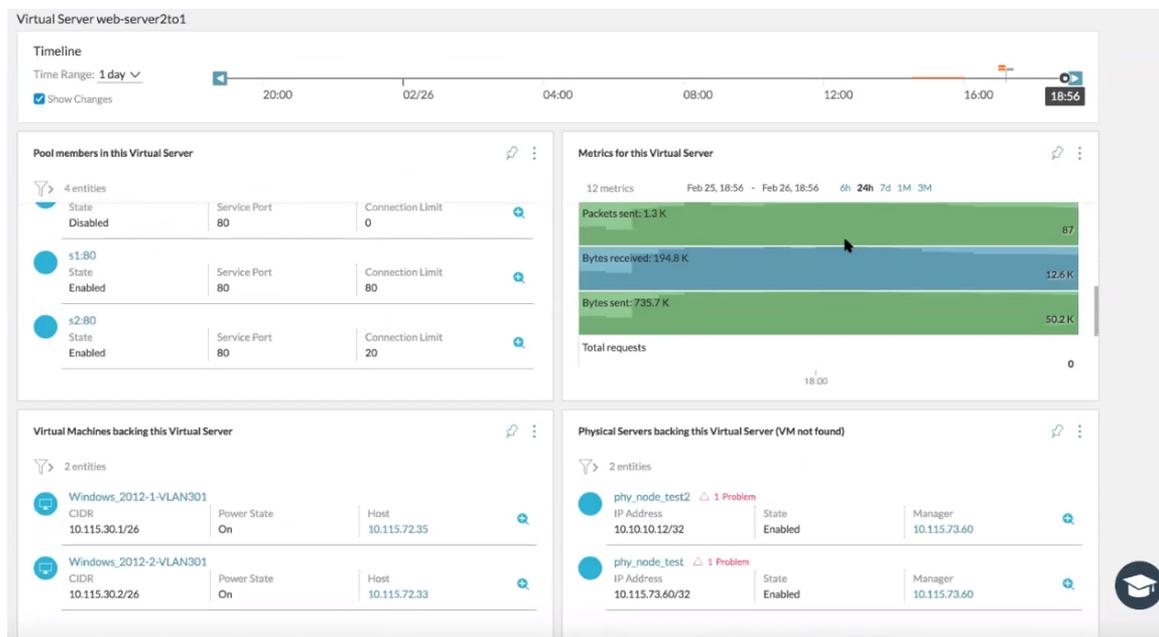
- Die Liste der auf den virtuellen Server bezogenen Metriken, z. B.
 - Verbindungen (Anzahl, Dauer)
 - Netzwerkmetriken (Pakete und empfangene oder gesendete Byte)
 - CPU-Auslastung

Hinweis Eine Liste der unterstützten Metriken für den NSX-V-Lastausgleichsdienst finden Sie unter [Unterstützte NSX-V-Metriken](#).

- Die Top-Flows für die von diesem virtuellen Server verwendeten Poolmitglieder

Hinweis Für NSX-V-Lastausgleichsdienste werden die Flow-Informationen nicht erfasst.

- Die Eigenschaften des virtuellen Servers, darunter Informationen zur IP-Adresse des Lastausgleichsdiensts, zum Netzwerkdatenverkehr und zum Dienstport



Mit der folgenden Abfrage können Sie den dem Lastausgleichsdienst zugeordneten Topologie-Pfad anzeigen: *Client-VM-Name to IP des virtuellen Servers*.. Wenn mehrere virtuelle Server auf verschiedenen Dienstports vorhanden sind, wird die Liste unter dem Abschnitt „Ziel-VM auswählen“ angezeigt. Sie können einen Server aus der Liste auswählen und den Pfad des virtuellen VM-Servers mit einem Klick auf **Pfad anzeigen** anzeigen.

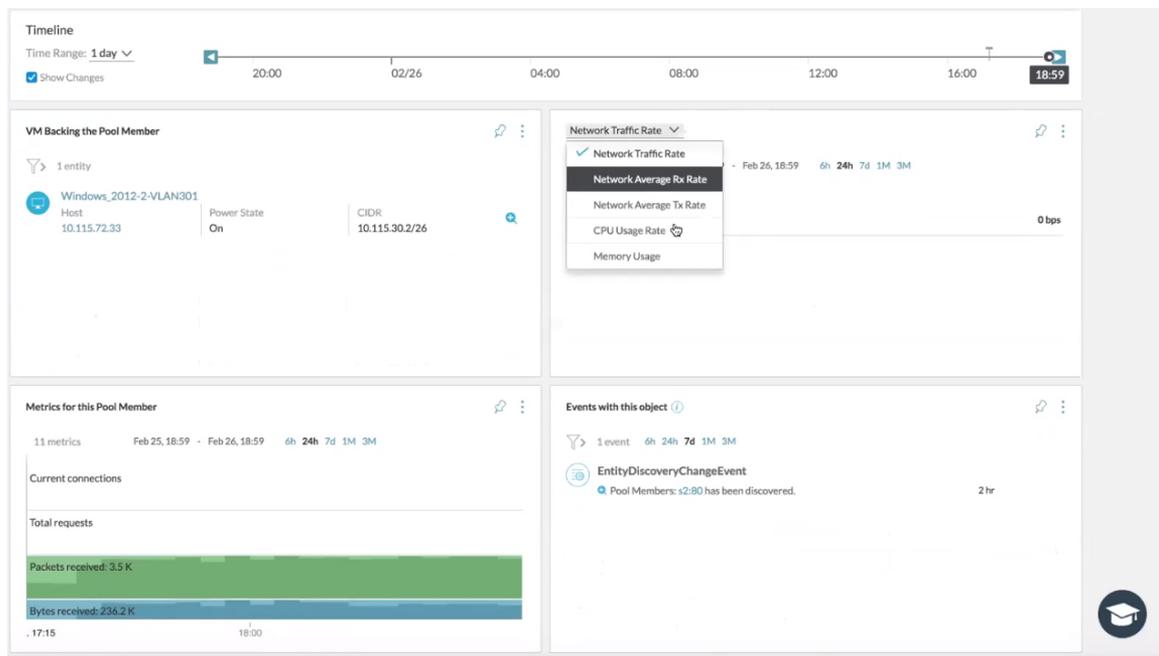
Mit einem Klick auf den virtuellen Server in der VM-Pfad-Topologie können Sie eine Gruppe von VMs im Fenster „Virtueller Server“ anzeigen. Klicken Sie auf **Pfad anzeigen**, um den Pfad vom virtuellen Server zur ausgewählten VM anzuzeigen.

Anzeigen der Details zu Poolmitgliedern

Auf der Seite „Poolmitglieder“ erhalten Sie Erkenntnisse über die Poolmitglieder, Metriken und Ereignisse im Zusammenhang mit dem jeweiligen Poolmitglied.

Sie sehen die folgenden Informationen:

- Liste der virtuellen Maschinen und zusätzliche Details zur VM
- Sie können die Metriken des Poolmitglieds mit denen der VM vergleichen. Beispielsweise Arbeitsspeicher- und CPU-Auslastung, Netzwerkdatenverkehr.
- Liste der Metriken, die sich auf das Poolmitglied beziehen, wie
 - Verbindungen (Anzahl, Dauer, Alter)
 - Netzwerkmetriken (Pakete und empfangene oder gesendete Byte)
 - CPU-Auslastung
- Eigenschaften des Poolmitglieds mit Angaben über den Lastausgleichsdienst, den Knoten, den Status und den Dienstport.



Beispiele für Suchabfragen im Zusammenhang mit dem Lastausgleichsdienst

Anhand der folgenden Beispielabfragen können Sie die Daten in Bezug auf den Lastausgleichsdienst filtern oder durchsuchen.

- `vm where lbServiceNodes is set`: Listet alle VMs auf, die eine Anwendung hosten, wobei die Last verteilt wird.
- `vm where lbServiceNodes is set and PowerState != 'POWEREDON'`: Listet alle VMs auf, die eine Anwendung mit Lastausgleich hosten, die aber derzeit nicht funktional sind.
- `pool member where state = 'DISABLED'`: Listet alle Poolmitglieder auf, die deaktiviert sind.

- `Count of Pool Memembers where Service Port = '80'`: Gibt die Anzahl aller Poolmitglieder für einen bestimmten Dienstyp an, die auf Port 80 ausgeführt werden.
- `service node where virtual machine is not set`: Listet alle Dienstknoten auf, die den physischen Server als Anwendungsserver verwenden, oder der vCenter Server, der die VMs hostet, wird in vRealize Network Insight nicht hinzugefügt.

NSX-V als Lastausgleichsdienst

Ab Version 4.2 unterstützt und ermöglicht vRealize Network Insight die Lastausgleichsfunktion von NSX-V.

Hier ist die Liste der aktuell unterstützten Metriken:

- Virtueller Server
 - Insgesamt gesendete eingehende Byte
 - Insgesamt gesendete ausgehende Byte
 - Aktuelle Sitzungen
 - Sitzungen insgesamt
- Pool
 - Insgesamt gesendete eingehende Byte
 - Insgesamt gesendete ausgehende Byte
 - Aktuelle Verbindungen
 - Max. Verbindungen
 - Verbindungen insgesamt

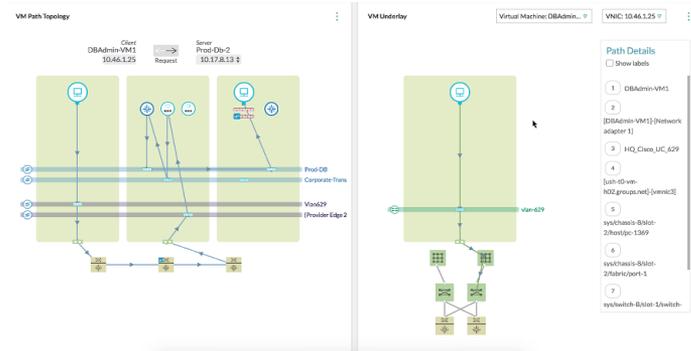
Derzeit werden in vRealize Network Insight nur VMs als Poolmitglieder unterstützt.

Dieses Kapitel enthält die folgenden Themen:

- Pfadtopologie
- Anzeigen von Details zu BGP-Nachbarn
- Pfad zum Internet

Pfadtopologie

In der Pfadtopologie wird eine detaillierte Verbindung zwischen zwei beliebigen virtuellen Maschinen in Ihrer Umgebung erstellt.



Die Topologie umfasst Komponenten der Ebene 3 und der Ebene 2. Diese Topologie kann mithilfe der Suchabfrage `vm_name_1` bis `vm_name_2` angezeigt werden. Wenn ein Pfad vorhanden ist, wird die VM-zu-VM-Pfadvisualisierung fortgesetzt, um alle zwischen `vm_name_1` und `vm_name_2` vorhandenen Komponenten zu befüllen. Darüber hinaus wird auch ein animierter Pfad gezeichnet. Wenn die Router physisch sind, werden sie außerhalb der Begrenzung angezeigt.

In der Pfadtopologie wird der VM-zu-VM-Pfad zwischen der Quelle und dem Ziel angezeigt. Wenn der Standardpfad nicht zwischen den VMs konfiguriert ist, wird eine Fehlermeldung angezeigt, die darüber informiert, dass der Pfad nicht definiert ist oder dass die Router-Schnittstelle nicht gefunden wurde.

Bei Kubernetes zeigt die Pfadtopologie den Pfad für die folgenden Szenarien an:

- Kubernetes-Dienst zu Kubernetes-Dienst
- Kubernetes-Dienst zu Kubernetes-Pod

- Kubernetes-Pod zu Kubernetes-Pod

Hinweis Der Pfad, der physische Geräte einschließt, wird nicht unterstützt.

Mit der Option **Pfad über Lastausgleichsdienst** werden alle Lastausgleichsdienste aufgelistet, die zwischen dem Pfad von der ausgewählten Quelle und der Ziel-VM verwendet werden. Um den Pfad zwischen den VMs über einen bestimmten Lastausgleichsdienst anzuzeigen, wählen Sie den Namen des Lastausgleichsdiensts aus der Liste aus. Wenn Sie die Maus auf die Lastausgleichsdienstkomponente in der Pfad-Topologie bewegen, werden die folgenden Details angezeigt:

- Name des virtuellen Servers
- IP-Adresse des Lastausgleichsdiensts
- Portnummer
- Lastausgleichsalgorithmus
- Das Standard-Gateway, das vom Lastausgleichsdienst beansprucht wurde.

Sie können auch die Routing-Komponenten in der Pfad-Topologie anzeigen.

Wenn Sie die Maus über einen der Router, Edges oder LDRs bewegen, die an dem Pfad beteiligt sind, werden die vollständigen Routing- oder NAT-Informationen angezeigt.

Der Abschnitt „VM-Underlay“ auf der rechten Seite der VM-Pfadtopologie zeigt die Underlay-Informationen der beteiligten VMs und deren Konnektivität mit dem oberen Rand der Rack-Switches und den beteiligten Ports. Bei Kubernetes-Elementen werden im Abschnitt „VM-Underlay“ Informationen für die VM oder die Kubernetes-Knoten angezeigt, auf denen sich der Pod befindet.

Im Abschnitt „VM-Underlay“ werden die Komponenten beschriftet, wenn Sie **Bezeichnungen anzeigen** unter **Pfaddetails auswählen** . In diesem Abschnitt werden in der Dropdown-Liste oben die Endpoint-VMs und an den Rändern die aktiven VMs angezeigt. Für jede Edge-VM zeigt die benachbarte Dropdown-Liste die IP-Adressen der Schnittstelle für den eingehenden und der Schnittstelle für den ausgehenden Datenverkehr an. Basierend auf der Auswahl wird der Underlay-Pfad für diese bestimmte Schnittstelle angezeigt.

Sie können die Pfadrichtung auch mit den Pfeilen oben auf der Topologiezuordnung umkehren.

Die Topologiezuordnung bietet mehr Transparenz bezüglich der Ports, die am VM-VM-Pfad beteiligt sind. Im Abschnitt **Pfaddetails** wird der Name des tatsächlichen Portkanals angezeigt.

Hinweis Es gibt keine vollständige Sichtbarkeit für Ebene 2 auf der physischen Seite. Wenn ein Paket von einem Switch zu einem anderen wechselt, sind möglicherweise mehrere Switches beteiligt. In der Topologie werden die Switches im Underlay-Netzwerk jedoch nicht angezeigt.

VM-VM-Pfad für AWS

Der VM-VM-Pfad für AWS bietet die Pfadsichtbarkeit zwischen den lokalen VMs und den AWS-EC2-Instanzen.

Derzeit unterstützt vRealize Network Insight die folgenden Szenarien:

- **AWS-Intra-VPC-VM-VM-Pfad:** Dieses Szenario beinhaltet die Kommunikation zwischen den VMs desselben Subnetzes oder verschiedenen Subnetzen in einer bestimmten VPC.
- **AWS-Inter-VPC-VM-VM-Pfad über die Peering-Verbindung:** Dieses Szenario beinhaltet die Kommunikation zwischen der VM einer VPC mit der VM einer anderen VPC über eine Peering-Verbindung.
- **AWS-VM zu Internet:** Die VM in einer VPC kommuniziert über das Internet-Gateway mit dem Internet.
- **AWS-VM zur Datacenter-VM über AWS-VPN-Verbindung:** In diesem Szenario kommuniziert die VM in einer VPC über die AWS-VPN-Verbindung mit der VM in einem Datacenter. vRealize Network Insight unterstützt für dieses Szenario SDDC sowie NSX-V- und NSX-T-Datacenter.

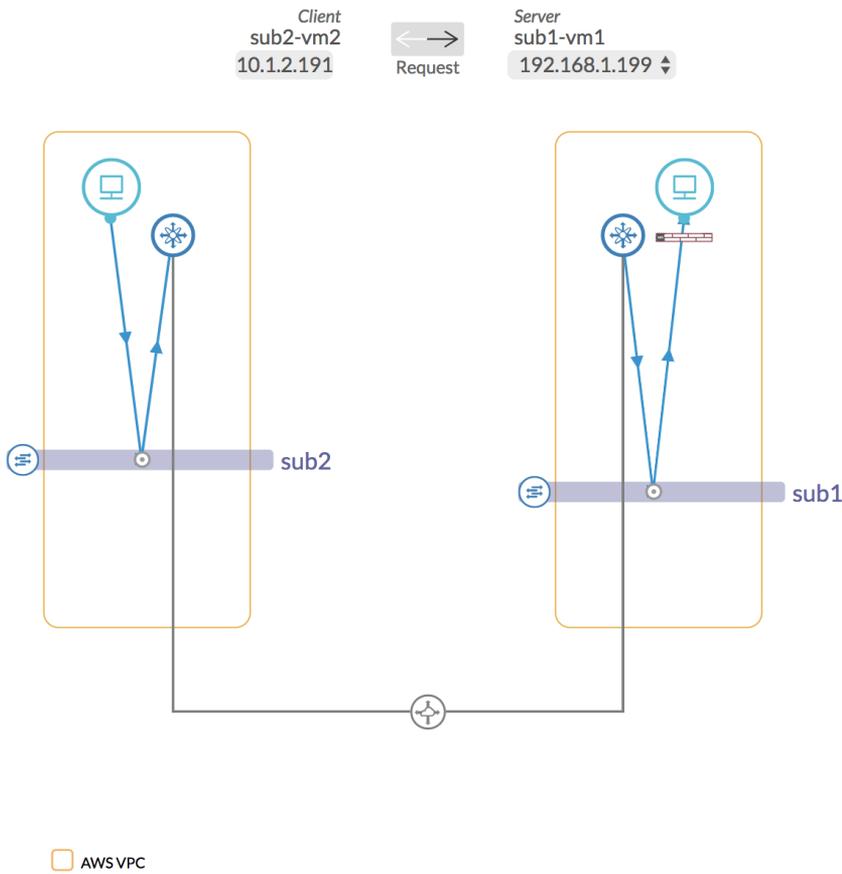
Hinweis

- Die Hybridpfad-Topologie zu NSX-T- und NSX-V-Datacentern funktioniert nur, wenn die NSX-T- und NSX-V-Edge-Router mit einer öffentlichen IP-Adresse konfiguriert sind.
 - vRealize Network Insight unterstützt nicht die VM-Underlay-Topologie für AWS.
-

Hinweis

Ein Beispiel für einen AWS-VM-VM-Pfad für den AWS-Inter-VPC-VM-VM-Pfad über die Peering-Verbindung ist wie folgt:

VM Path Topology i



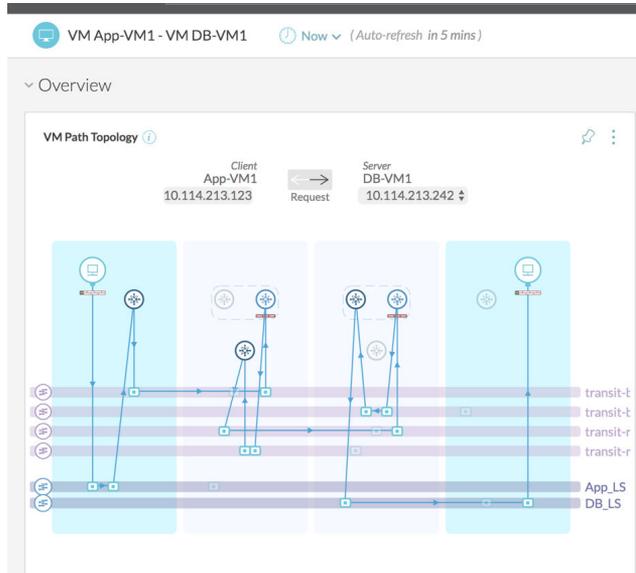
Sie können die Eigenschaften der Peering-Verbindung anzeigen, indem Sie auf das zugehörige Symbol im VM-VM-Pfad zeigen.

In Bezug auf den AWS-VM-VM-Pfad können Sie die folgenden Einheiten durchsuchen:

- AWS Subnet
- AWS Route Table
- AWS Virtual Private Gateway
- AWS Internet Gateway
- AWS VPN Connection
- AWS VPC Peering Connection

NSX-T

Ein Beispiel für einen VM-VM-Pfad für NSX-T lautet wie folgt:



Die blaue Farbe steht für den Hostknoten, und die graue Farbe stellt den Edge-Knoten dar. Die in der VM-Pfad-Topologie verwendeten Symbole werden auf der rechten Seite des Bildschirms zusammen mit den Beschriftungen unter „Pfad Details“ aufgeführt. Die verteilten Router werden unabhängig von ihren Ebenen in derselben Farbe angezeigt. Die Farbe des Dienst-Routers im Topologie-Diagramm ändert sich entsprechend der zugehörigen Ebene. Alle Ebene-1-Komponenten werden auf derselben Ebene angezeigt, und alle Ebene-0-Komponenten werden auf einer anderen Ebene angezeigt. In NSX-T werden die Edge-Firewalls im Diagramm dargestellt.

Um die Sicherheit für das NSX-T-Netzwerk zu planen, können Sie den Geltungsbereich als **NSX-T Layer2-Network** auswählen und die folgende Abfrage verwenden:

```
plan NSX-T Layer2 Network '<NAME_OF_NSX_T_LOGICAL_SEGMENT>'
```

Sie können das gleiche Ergebnis erzielen, indem Sie die folgenden Schritte ausführen:

- Wählen Sie **Sicherheit** aus der Navigationsleiste aus.
- Wählen Sie **NSX-T Layer2-Network** als Geltungsbereich aus dem Dropdown-Menü aus.

Hinweis

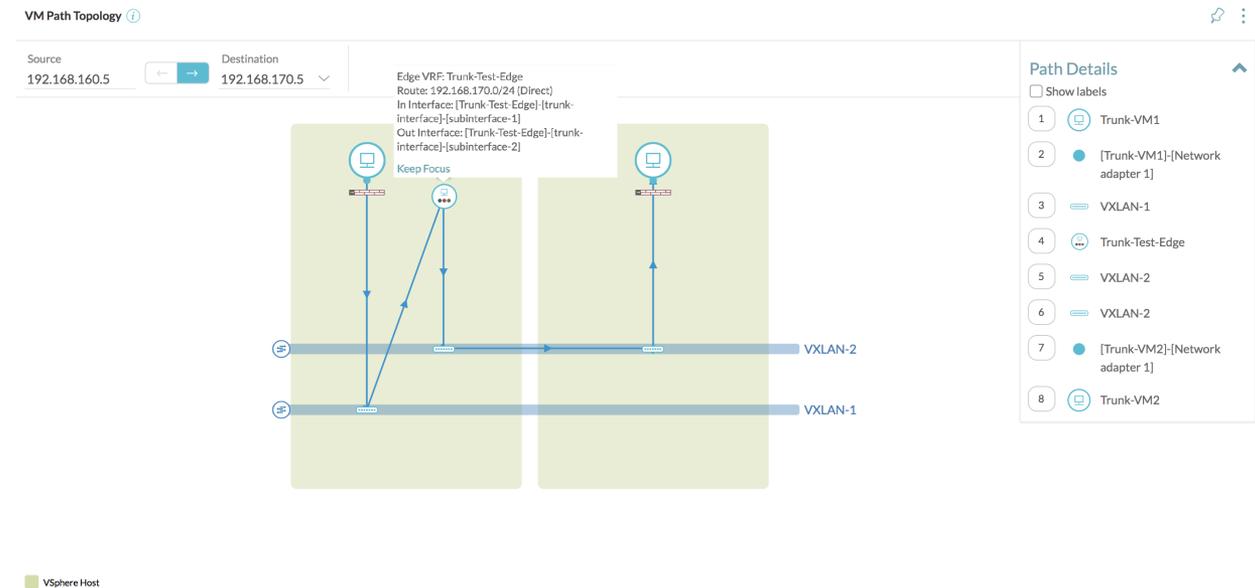
- NSX-T-bezogene Einheiten wie **NSX-T L2-Network** und **Tags** sind im Geltungsbereich verfügbar. Sie können diese NSX-T-bezogenen Einheiten für Planung, Mikrosegmentierung und Anwendungsdefinition verwenden.
- Im Dropdown-Menü **Gruppieren nach** ist **NSX-T-Sicherheitsgruppe** ein Teil von **Sicherheits-Tag** und **Logisches Segment** ist Teil von **VLAN/VXLAN**.

VM-zu-VM-Pfad über die NSX-V Edge Trunk-Schnittstelle

In vRealize Network Insight können Sie den VM-zu-VM-Pfad und den VM-zu-Internet-Pfad anzeigen, wenn das DVPG mit der Trunk-vNIC der NSX Edge verbunden ist und die Unterschnittstellen mit VLAN oder VXLAN verbunden sind.

Nachfolgend sehen Sie ein Beispiel für einen VM-zu-VM-Pfad über die NSX Edge:

Hinweis vRealize Network Insight unterstützt die Underlay-Informationen für die Trunk-Schnittstellen der Edge-VM nicht.



NAT-Unterstützung in vRealize Network Insight

vRealize Network Insight unterstützt den VM-VM-Pfad für NSX for vSphere, NSX-T Edges, Fortinet und Check Point.

VM-VM-Pfad

Ein VM-VM-Beispielpfad über NAT lautet wie folgt:

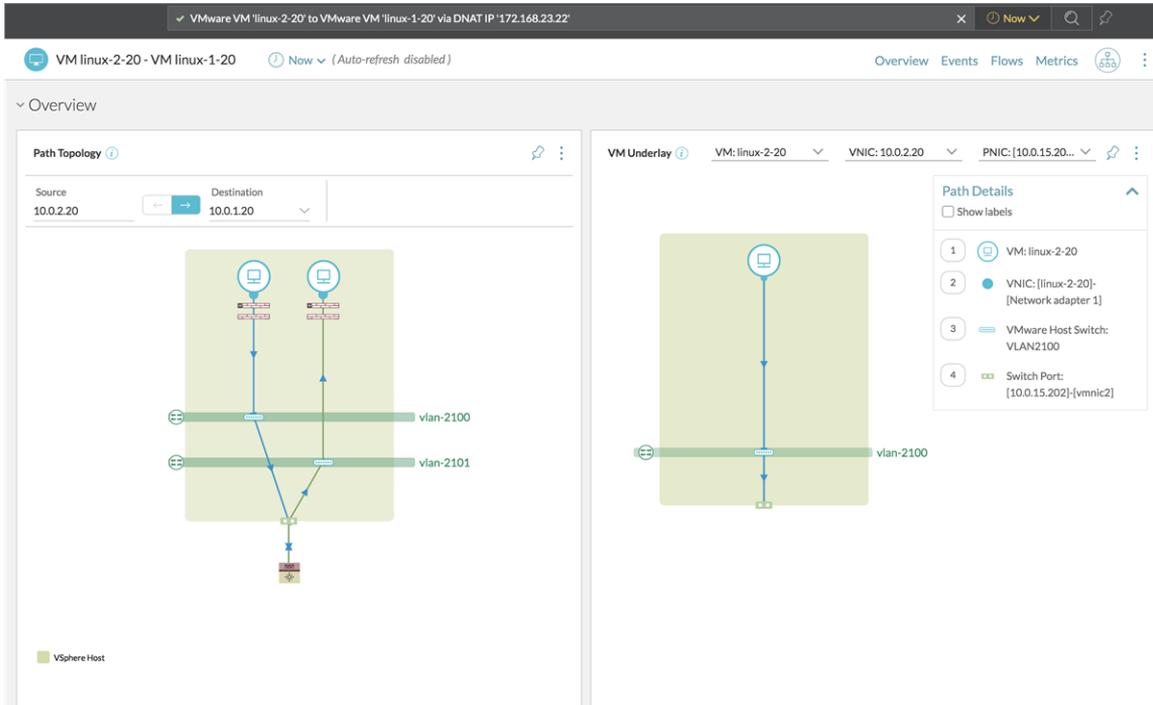
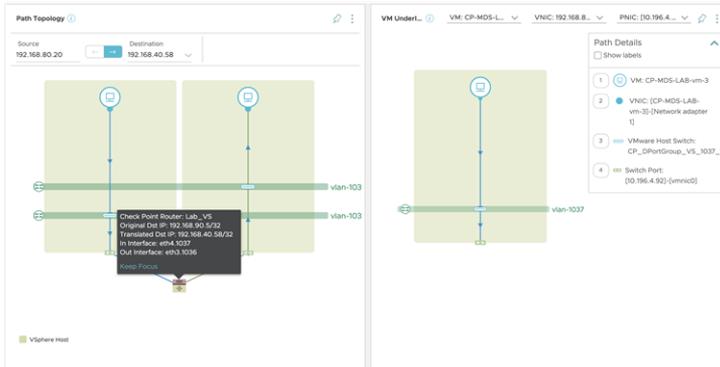


Abbildung 16-1. VM-VM-Pfad über Check Point NAT



Abfragen

Verwenden Sie die folgenden Abfragen, um den VM-VM-Pfad über NAT anzuzeigen:

- Wenn sich die Ziel-VM hinter einem Fortinet- und Check Point-Router befindet und mit NAT konfiguriert ist, verwenden Sie die Abfrage `VMware VM '<name of the VM>' to VMware VM '<name of the VM>' via DNAT`.
- Wenn sich die Ziel-VM hinter einem NSX for vSphere oder NSX-T Edge befindet und mit NAT konfiguriert ist, verwenden Sie die Abfrage `VMware VM '<name of the VM>' to VMware VM '<name of the VM>'`.

Überlegungen

- Für den VM-VM-Pfad mit den logischen NSX-T-Routern, auf denen der NAT-Dienst aktiviert ist, zeigt vRealize Network Insight die Firewallregeln für NSX-T Edge für einen solchen Pfad nicht ordnungsgemäß an.

VM-zu-VM-Pfad für VMware SD-WAN

In vRealize Network Insight können Sie den VM-VM-Pfad für Ihre VMware SD-WAN-Bereitstellung anzeigen.

vRealize Network Insight unterstützt die folgenden Szenarien:

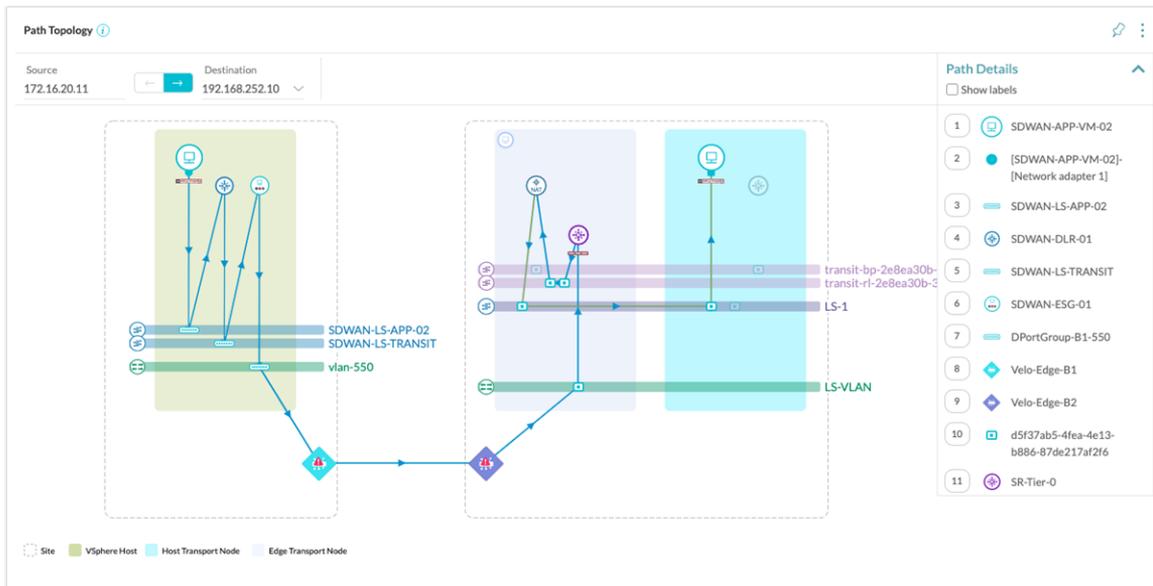
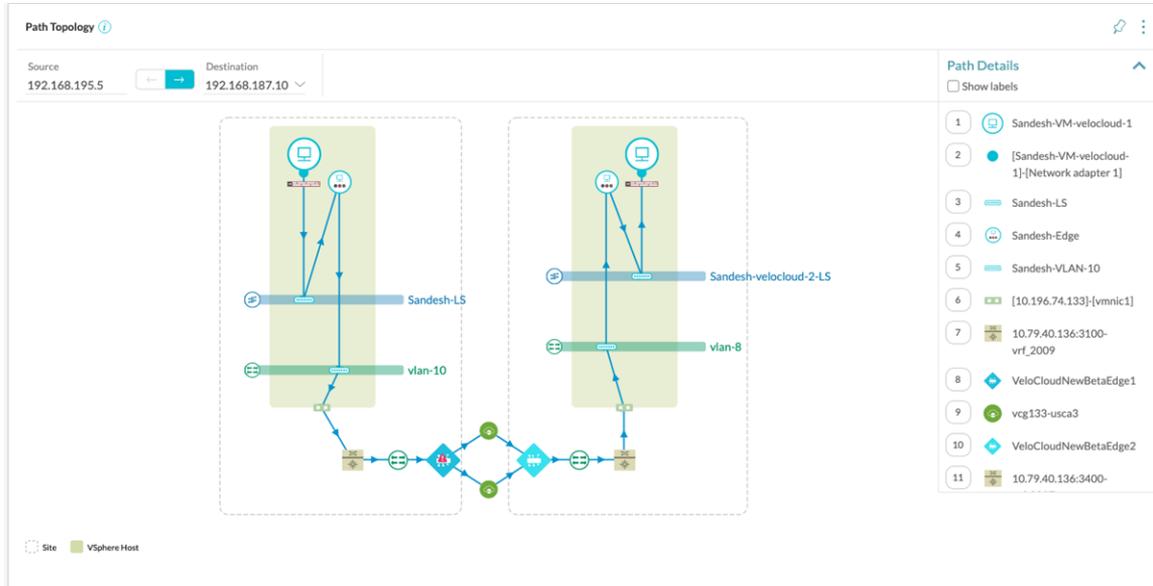
- IP-zu-IP-Pfad: Beide IPs müssen sich direkt im VLAN hinter einer VMware SD-WAN-Edge befinden.
- IP-zu-Internet/IP-zu-unbekannter-IP: Quell-IP muss sich direkt im VLAN hinter einer VMware SD-WAN-Edge befinden.

Hinweis Bei „Internet“ oder „Unbekannte IP“ handelt es sich um eine beliebige IP-Adresse, die in vRealize Network Insight nicht erkannt wird.

- VM-zu-IP-, IP-zu-VM- oder VM-zu-VM-Pfad:
 - VMs werden nur in NSX-/NSX-T-Datencentern unterstützt. VMs in VMware Cloud on AWS, Amazon Web Services und AZURE werden nicht unterstützt.
 - Die VMware SD-WAN-Edge muss über ein VLAN mit einem physischen/virtuellen Router im Datacenter verbunden sein.
- **Hinweis** Wenn die für die VMware SD-WAN-Quell-Edge und die VMware SD-WAN-Ziel-Edge konfigurierten VMware SD-WAN-Gateways nicht übereinstimmen, wird der Pfad über die Gateways der VMware SD-WAN-Quell-Edge angezeigt.

Wenn ein Zweig-zu-Zweig-VPN zwischen den VMware SD-WAN-Edges über einen VeloCloud-Cluster verläuft, werden alle Mitglieder des VMware SD-WAN-Clusters im Pfad angezeigt.

Im Folgenden finden Sie einige Beispiele für einen VM-VM-Pfad für VMware SD-WAN:



VM-VM-Pfad für Arista-Hardware-VTEP

In vRealize Network Insight können Sie einen Hardware-VTEP im VM-VM-Pfad anzeigen.

Derzeit unterstützt vRealize Network Insight die folgenden Szenarien:

- VM-VM-Pfad über Hardware-VTEP, wenn sich die Quell- und Ziel-VMs in einem anderen VXLAN und auf einem anderen Host befinden.
- VM-VM-Pfad über Hardware-VTEP, wenn sich die Quell- und Ziel-VMs auf demselben Host, aber in einem anderen VXLAN befinden.

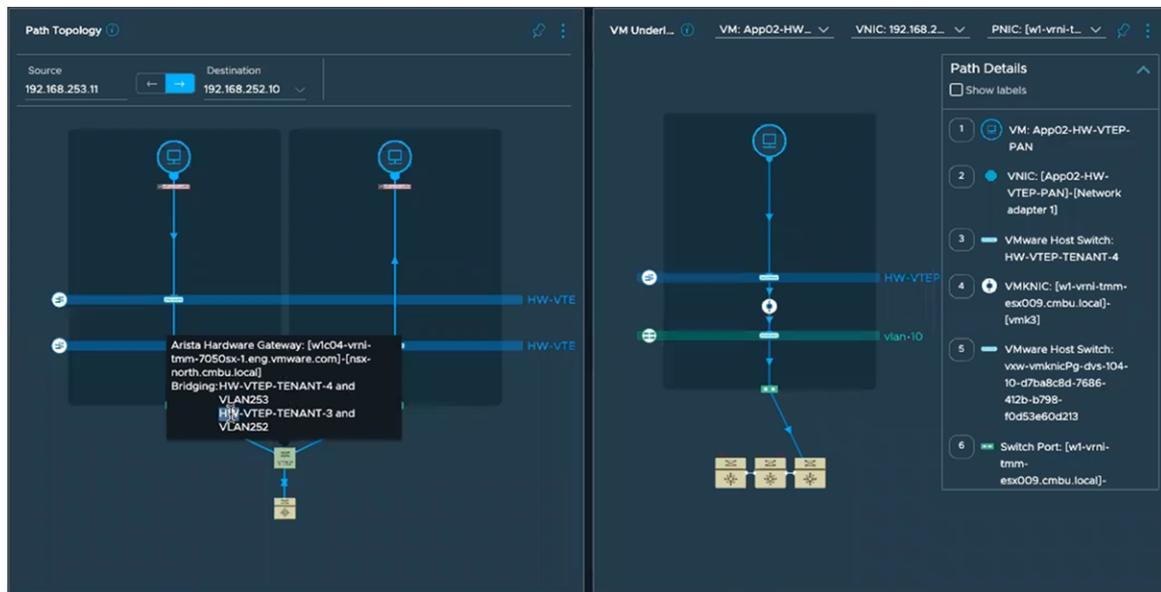
- Hardware-VTEP in der VM-Underlay-Topologie, wenn der Switch direkt mit dem Host verbunden ist.

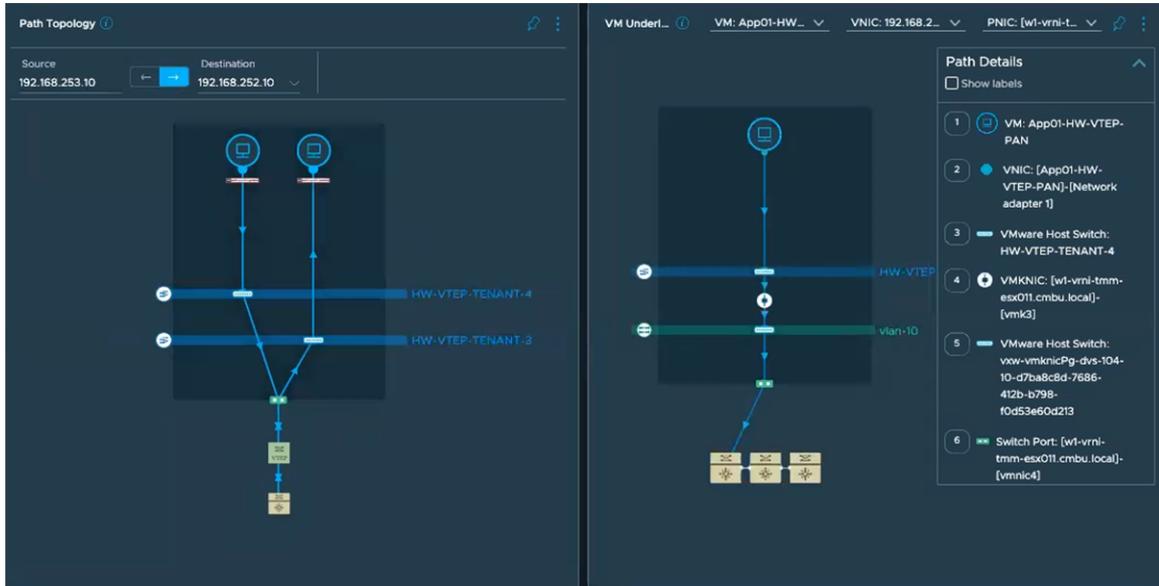
Hinweis Wenn Sie Arista-Switch-SSH in vRealize Network Insight als Datenquelle hinzufügen, müssen Sie dieselbe IP bzw. denselben FQDN verwenden, die bzw. den Sie in VMware NSX Manager zum Konfigurieren von Arista-Switch-SSH verwendet haben. Andernfalls wird der Hardware-VTEP im VM-VM-Pfad nicht angezeigt.

Sie können den Hardware-VTEP auch in der VM-Topologie und im Pfad „VM zu Internet“ anzeigen, wenn zwischen der VM und dem Internet ein Hardware-VTEP verfügbar ist.

VM-VM-Pfad über Hardware-VTEP, wenn sich die Quell- und Ziel-VMs im selben VXLAN befinden, wird nicht unterstützt.

Im Folgenden finden Sie einige Beispiele für VM-VM-Pfad über Hardware-VTEP:





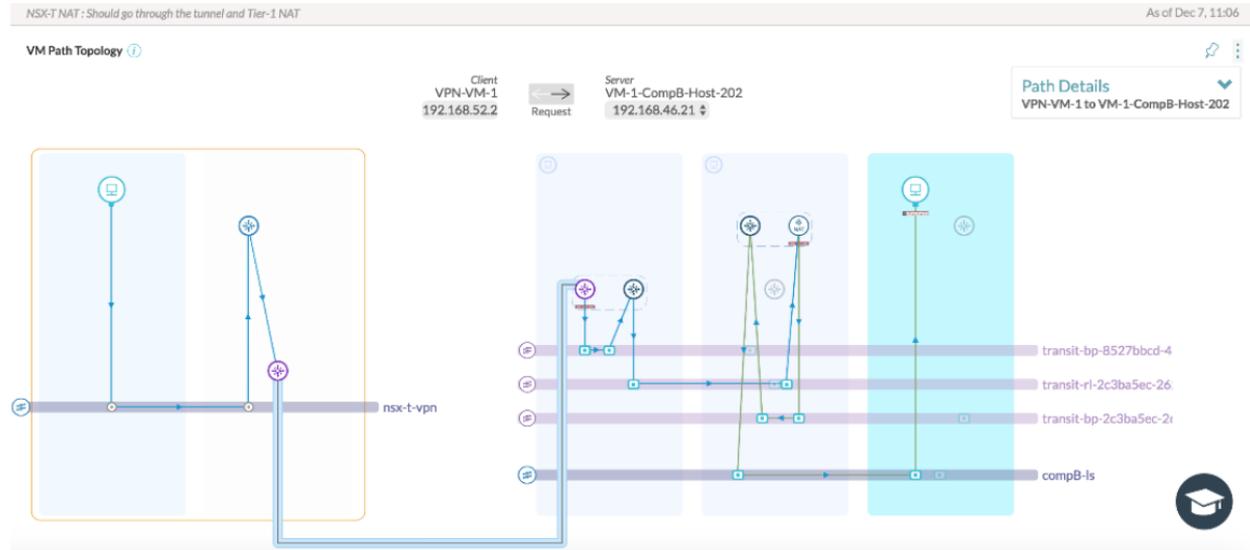
VMware Cloud on AWS: VM-zu-VM-Pfad

vRealize Network Insight unterstützt die folgenden Hybridpfade in VMware Cloud on AWS:

- VMware Cloud on AWS und VMware Cloud on AWS
- VMware Cloud on AWS und NSX-T
- VMware Cloud on AWS und NSX-V
- VMware Cloud on AWS und AWS
- VMware Cloud on AWS-intern

Für alle VMs, die in VMware Cloud on AWS vorhanden sind, werden die Underlay-Informationen nur bis zum Segment angezeigt, in dem die VM liegt, da die zugrunde liegenden physischen Elemente des Netzwerks von VMware Cloud on AWS herausabstrahiert werden und keine Sichtbarkeit auf dieser Ebene vorhanden ist.

Beispiel für einen VMware Cloud on AWS- und NSX-T-VM-VM-Pfad:



Die dunkelblaue Linie zeigt den Tunnel an.

VM-VM-Pfad für Cisco ACI

In vRealize Network Insight können Sie den VM-VM-Pfad über Cisco ACI anzeigen.

Ein Beispiel für einen VM-VM-Pfad für Cisco ACI lautet wie folgt:

Hinweis vRealize Network Insight zeigt den VM-VM-Pfad über die Leaf- und Spine-Switches an, wenn die Cisco-ACI-APIs die Details zur Switch-Ebene bereitstellen. Ist dies nicht der Fall, zeigt vRealize Network Insight ein einzelnes Cisco-ACI-VRF für den gesamten Fabric anstelle der Leaf- und Spine-Switches im VM-zu-VM-Pfad an.

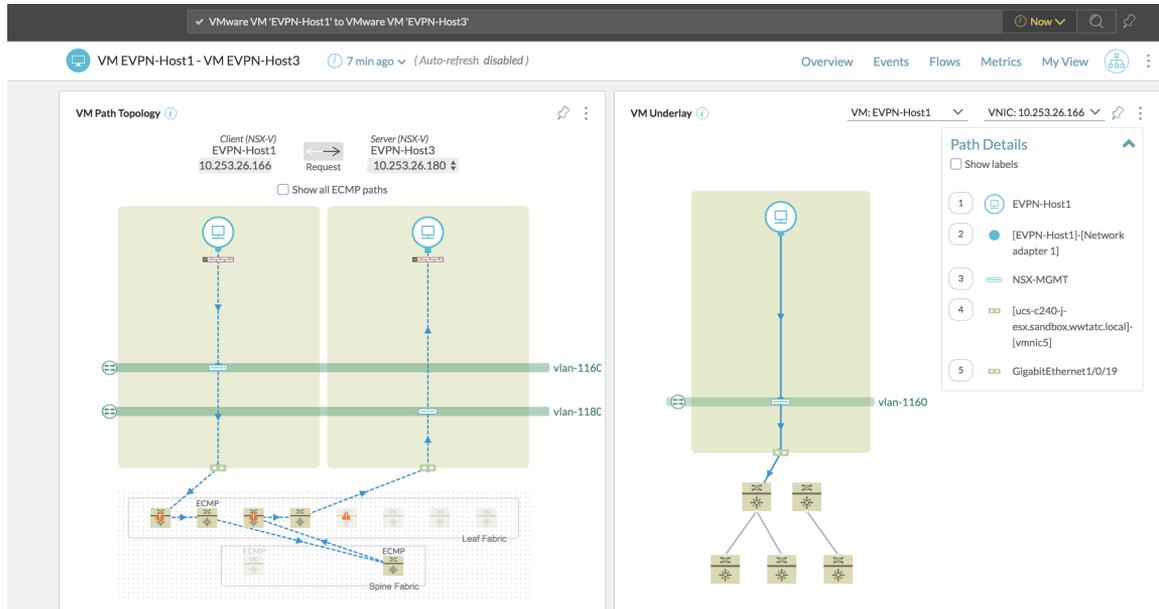


Unterstützung für den Cisco BGP-EVPN-Modus

vRealize Network Insight unterstützt das Fabric von Cisco-9000-Switches, die im BGP-EVPN-Konfigurationsmodus von Cisco für die Enterprise Edition konfiguriert sind. vRealize Network Insight unterstützt keine Switch-Modelle außer Cisco Nexus 9000 mit der Cisco BGP-EVPN-Konfiguration.

Jeder Cisco-Nexus-9000-Switch, der Teil des Fabric ist, wird einzeln als Datenquelle hinzugefügt. Verwenden Sie die `switches where role is set`-Abfrage, um alle Spine- oder Leaf-Switches im Fabric anzuzeigen.

Ein Beispiel für einen VM-VM-Pfad für den Cisco-BGP-EVPN-Modus lautet wie folgt:

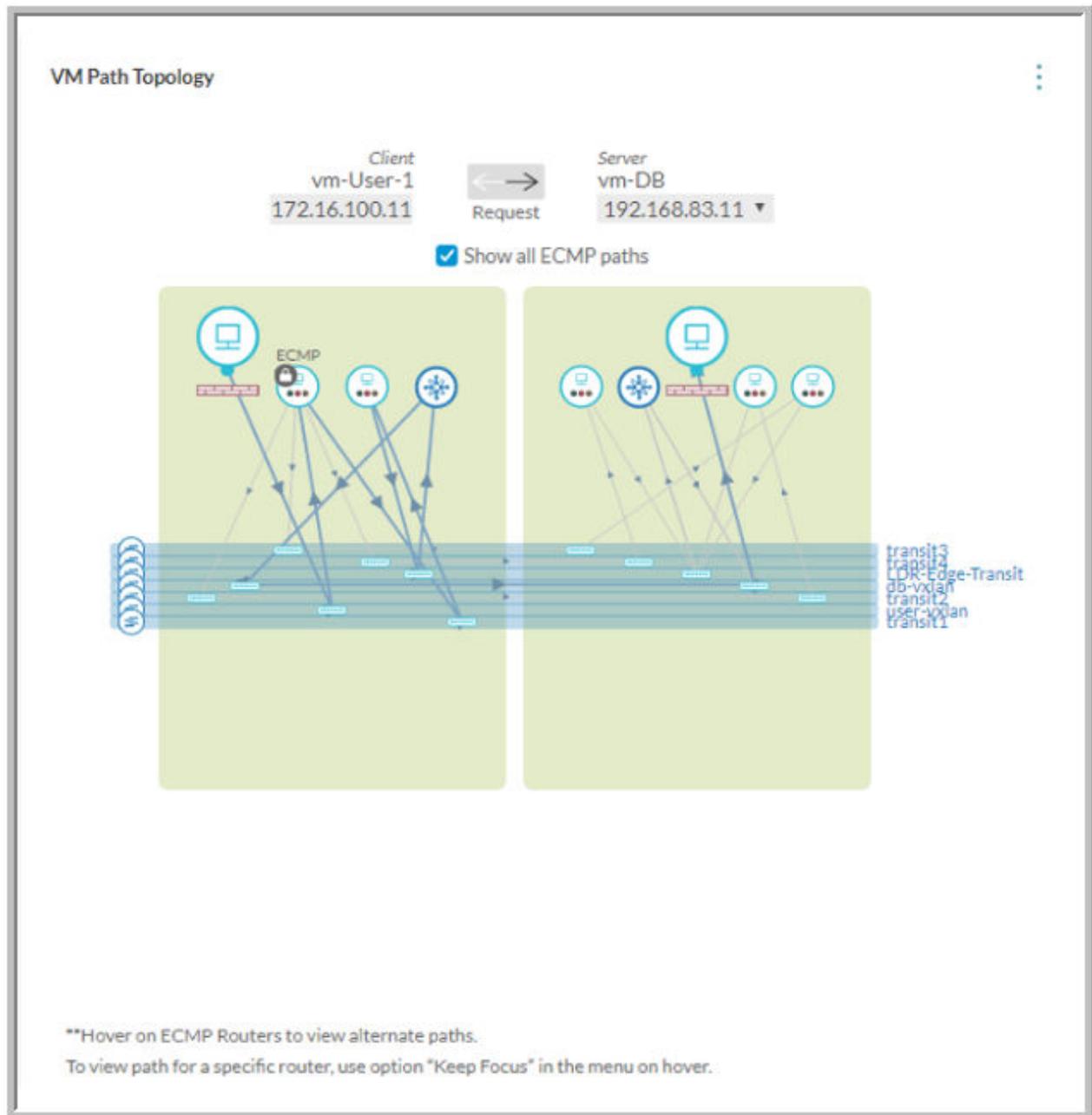


Unterstützung für ECMP-Route (Equal-Cost Multi-Path)

vRealize Network Insight bietet ECMP-Unterstützung im VM-VM-Pfad.

Der VM-VM-Pfad zeigt die folgenden Informationen zu ECMP:

- Mehrere ECMP-Pfade von Quelle zu Ziel,
- Router, auf denen ECMP ausgeführt wird,
- Mögliche ausgehende Pfade für einen bestimmten Router (VRF),
- Route für den möglichen Pfad,



In der obigen Abbildung werden die ECMP-fähigen Router angezeigt. Wenn Sie mit dem Cursor darauf zeigen, werden die zusätzlichen Pfade angezeigt. Sie können auch einen Pfad erstellen, indem Sie die Router gemäß Ihren Anforderungen auswählen und sperren. Wenn Sie alle ECMP-Pfade zwischen den beiden VMs anzeigen möchten, wählen Sie die Option **Alle ECMP-Pfade anzeigen** im Topologie-Diagramm aus.

Wenn Sie den Pfad für einen bestimmten Router anzeigen möchten, zeigen Sie auf den Router und klicken Sie auf **Fokus beibehalten**. Die für den Router spezifischen Pfade werden angezeigt.

Unterstützung für die L2-Bridges

Die L2- oder VLAN-Bridges erstellen eine einzelne Broadcast-Domäne aus mehreren VLANs. Wenn in den vorherigen Versionen der VM-VM-Pfad eine L2-Bridge zwischen zwei oder mehr VLANs umfasste, funktionierte der VM-VM-Pfad nicht. Ab dieser Version unterstützt vRealize Network Insight L2-Bridging. Derzeit wird diese Funktion nur für die Cisco-ASA-Router unterstützt.

Anzeigen von Details zu BGP-Nachbarn

In vRealize Network Insight können Sie verschiedene Informationen zu BGP-Nachbarn anzeigen. Sie können die BGP-Nachbarn eines NSX Edge oder eines logischen Routers anzeigen.

Verfahren

- 1 Geben Sie `Router where bgp= 'Disabled'` in die Suchleiste ein und drücken Sie **Eingabe**.
- 2 Erweitern Sie den bestimmten Router in der Liste, um die Details anzuzeigen.

Sie können bei NSX-V die folgenden Informationen unter „BGP-Nachbarn“ anzeigen:

- IP Address
- Remote AS
- Weight
- Keep Alive Time
- Hold Down Time
- Status

Sie können bei NSX-T die folgenden Informationen unter „BGP-Nachbarn“ anzeigen:

- IP Address
- Remote AS
- Keep Alive Time
- Hold Down Time
- Status

Hinweis

- Wenn die Informationen zu den Nachbarn nicht abgerufen werden, wird `Status` als `Unknown` angezeigt.
- Wenn `Status` nicht `Established.up` ist, wird das `One or more BGP neighbours are not in established state`-Ereignis für diesen Edge ausgelöst. Sie können dieses Ereignis auch bei der Suche nach `problems` anzeigen.

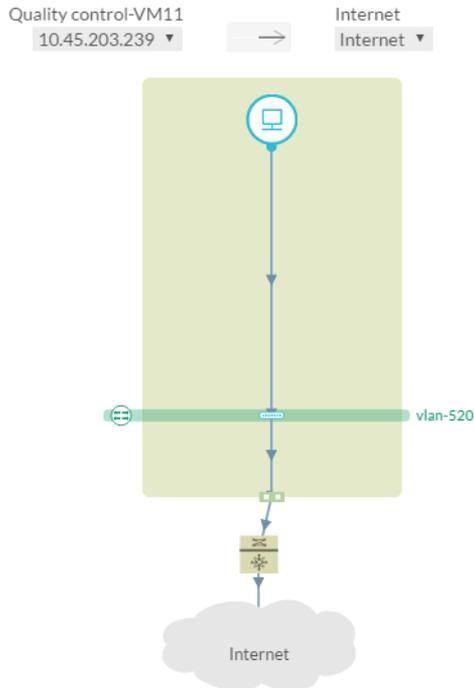
- 3 (Optional) Zum Anzeigen von Routern, auf denen der BGP-Status deaktiviert ist, suchen Sie nach `Router where bgp= 'Disabled'`.

Pfad zum Internet

Für jede virtuelle Maschine, die in Ihrer Umgebung vorhanden ist, zeigt vRealize Network Insight mithilfe eines animierten Pfades im Pin **Pfad zu Internet** an, wie die VM mit dem Internet verbunden ist.

Der Pfad füllt alle Komponenten (sowohl virtuell als auch physisch), die zwischen der virtuellen Maschine und dem Internet vorhanden sind. Er zeichnet einen animierten Pfad, der jede Komponente in einer Sequenz verbindet. Die Pfadrichtung kann auch mithilfe der Pfeile über der Visualisierung umgekehrt werden.

Zeigen Sie mit dem Mauszeiger auf die Einheitensymbole, um deren adressierbare Namen zu erhalten. Klicken Sie auf ein Symbol im Pfad, um eine zusammengefasste Aufstellung seiner primären Attribute anzuzeigen. Sie können auch den Pin maximieren, um die Pfaddetails anzuzeigen.



Dieses Kapitel enthält die folgenden Themen:

- Cross-vCenter NSX
- Palo Alto-Netzwerke
- Cisco-ASA-Firewall
- Check Point-Firewall
- Sicherheitsgruppen
- Richtlinienbasiertes VPN
- Inaktive Regeln für verteilte NSX-Firewall
- Fortinet-Firewall

Cross-vCenter NSX

In einer Cross-vCenter NSX-Umgebung können Sie mehrere vCenter-Server einrichten, die jeweils an ihrem eigenen NSX Manager gekoppelt werden müssen.

Einem NSX Manager wird die Rolle des primären NSX Manager zugewiesen, den übrigen wird die Rolle von sekundären NSX Managern zugewiesen. Der primäre NSX Manager wird verwendet, um einen universellen Controller-Cluster bereitzustellen, der die Steuerungsebene für die Cross-vCenter NSX-Umgebung bereitstellt. Die sekundären NSX Manager verfügen nicht über eigene Controller-Cluster. Der primäre NSX Manager kann globale Objekte wie globale logische Switches erstellen. Diese Objekte werden durch den globalen NSX-Synchronisierungsdienst mit den sekundären NSX Managern synchronisiert. Sie können diese Objekte in den sekundären NSX Managern anzeigen, sie jedoch nicht dort bearbeiten. Zur Verwaltung globaler Objekte müssen Sie den primären NSX Manager verwenden. Der primäre NSX Manager kann dazu verwendet werden, jeden sekundären NSX Manager in der Umgebung zu konfigurieren.

Folgende globale Objekte werden unterstützt:

- Globaler LDR,
- Globale Transportzone,
- Globaler logischer Switch,

- Globale Firewallregel,
- Globale Sicherheitsgruppe,
- Globale IPSets,
- Globaler Dienst,
- Globale Dienstgruppen,
- Globaler Segmentbereich.

Palo Alto-Netzwerke

vRealize Network Insight unterstützt die Palo Alto Panorama-Firewall.

Hinweis vRealize Network Insight unterstützt die Palo Alto Panorama-Integration in mehrere NSX-Manager nicht.

Um das Palo Alto Panorama in vRealize Network Insight hinzuzufügen, benötigt der Palo Alto Networks-Benutzer die **Administratorrolle** mit Zugriff auf die XML-API. Führen Sie auf der Benutzeroberfläche **Palo Alto-Netzwerke** die folgenden Schritte aus, um eine Administratorrolle für die XML-API hinzuzufügen.

- 1 Klicken Sie auf **Panorama > Administratorrollen**.
- 2 Klicken Sie auf **Hinzufügen**, um eine neue Administratorrolle hinzuzufügen.
- 3 Das Fenster „Admin-Rollenprofil“ wird geöffnet.
- 4 Geben Sie den Namen für die Rolle ein und klicken Sie auf **Panorama**.
- 5 Klicken Sie auf die Registerkarte **Web-UI** und deaktivieren Sie alle Einträge.
- 6 Klicken Sie auf die Registerkarte **XML-API** und deaktivieren Sie alle Einträge außer **Konfiguration** und **Betriebsanforderungen**.
- 7 Klicken Sie auf **OK**, um das Fenster zu schließen.
Die neue Administratorrolle wird in der Liste angezeigt.
- 8 Klicken Sie auf **Übernehmen**.
- 9 Weisen Sie diese Rolle einem Administratorkonto zu oder erstellen Sie einen neuen Benutzer und weisen Sie ihm diese Rolle zu.

Die Palo Alto-Netzwerkfunktionen, die von vRealize Network Insight unterstützt werden, lauten wie folgt:

- Zusammenhang zwischen Palo Alto- und NSX-Einheiten: die VM-Mitgliedschaft der Adresse und der Adressgruppe von Palo Alto-Netzwerken wird basierend auf der Zuordnung von IP-Adresse zu VM berechnet. Diese Mitgliedschaftsinformationen können wie folgt abgefragt werden:
 - `VM where Address = <>`

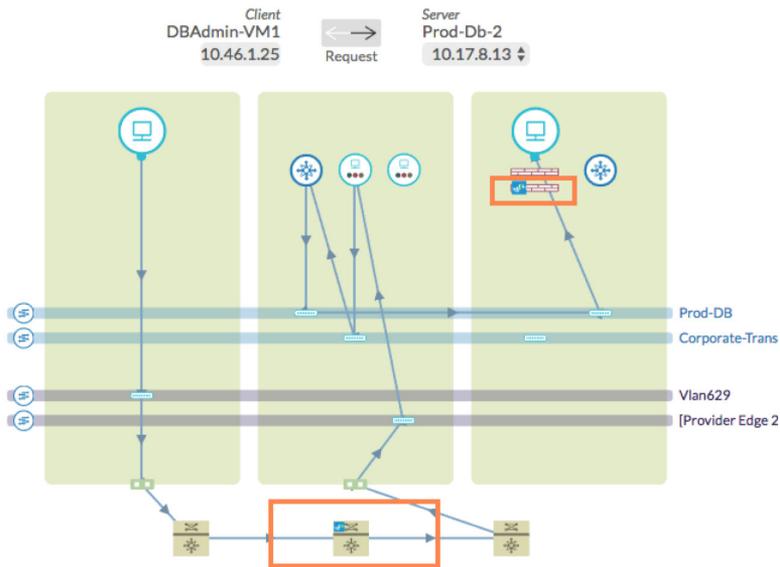
- Palo Alto address where vm = <>
 - VM where Address Group = <>
 - Palo Alto address group where vm = <>
- Abfrage: Sie können eine Abfrage für alle Palo Alto-Einheiten durchführen, die von vRealize Network Insight unterstützt werden. Allen Einheiten wird das Präfix „Palo Alto“ vorangestellt. Einige der Abfragen lauten wie folgt:

Tabelle 17-1.

Elemente	Abfragen
Palo Alto-Adresse	Palo Alto address where vm = <> VM where Address = <>
Palo Alto-Adressgruppe	Palo Alto address group where Translated VMs = <> VM where address group = <>
Palo Alto-Gerät	Palo Alto Device where Version = <> Palo Alto Device where connected = true Palo Alto Device where family = 'PA-5060'
Physisches Palo Alto-Gerät	Palo Alto Physical Device where model = 'PA-5060'
Palo Alto-VM-Gerät	Palo Alto VM Device where model = 'PA-VM'
Palo Alto-Gerätegruppe	Palo Alto Device Group where device = <> Palo Alto Device Group where address = <> Palo Alto Device Group where address group = <>
Palo Alto-Dienst	Palo Alto service where Port = <> Palo Alto service where Protocol = <>
Palo Alto-Dienstgruppe	Palo Alto service group where Member = <>
Palo Alto-Richtlinie	Palo Alto Policy where Source vm = <> and Destination vm = <> Palo Alto Policy where Source IP = <> and Destination IP = <>
Palo Alto-Firewall	Palo Alto firewall where Rule = <>
Palo Alto-Zone	Palo Alto Zone where device = <>
Virtuelles Palo Alto-System	Palo Alto Virtual System where Device = <> Palo Alto Virtual System where Device Group = <>

Hinweis Mit Ausnahme der Abfragen können Sie auch Facets zur Analyse der Suchergebnisse verwenden.

- VM-zu-VM-Pfad: Als Teil der VM-VM-Topologie zeigt vRealize Network Insight die Palo Alto VM Series-Firewall auf dem Host an. Die anwendbaren Regeln werden angezeigt, wenn Sie auf das Firewall-Symbol klicken. Wenn auch ein Firewall-Gerät (Routing-Gerät) des Palo Alto-Netzwerks im Pfad vorhanden ist, wird dieses Gerät ebenfalls angezeigt. Wenn Sie auf das Gerätesymbol klicken, werden die grundlegenden Informationen wie eine Routing-Tabelle, Schnittstellen und eine Tabelle mit den angewendeten Firewallregeln angezeigt.



- Sie können einige Systemereignisse im Zusammenhang mit den folgenden Szenarien für Palo Alto-Netzwerke anzeigen:
 - Palo Alto-Gerät ist nicht mit Panorama (Manager) verbunden.
 - NSX Manager ist nicht bei Panorama registriert.
 - NSX-Fabric-Agent wurde auf dem ESX für Palo Alto-Gerät nicht gefunden.
 - Palo Alto-Gerät wurde auf Panorama für NSX-Fabric-Agent nicht gefunden.
 - Nicht synchronisierte Daten der Sicherheitsgruppenmitgliedschaft
- Sie können mehrere Dienstdefinitionen in Panorama mit einem bestimmten NSX Manager erstellen und registrieren. Wenn verschiedene ESXi-Cluster Arbeitslasten aufweisen, die erfordern, dass die VM-Series-Firewall den Datenverkehr unterschiedlich verarbeitet, werden mehrere Dienstdefinitionen erstellt. Jede Dienstdefinition verfügt über eine zugeordnete Gerätegruppe, aus der die Richtlinien entnommen werden. Beim Anzeigen des VM-VM-Pfads in vRealize Network Insight sollte basierend auf den Cluster-Informationen der richtige Satz von Richtlinien berücksichtigt werden.

Beispiel für ein Palo Alto Manager-Dashboard

Timeline

Time Range: 1 day

Show Changes

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 Address	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 Address	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

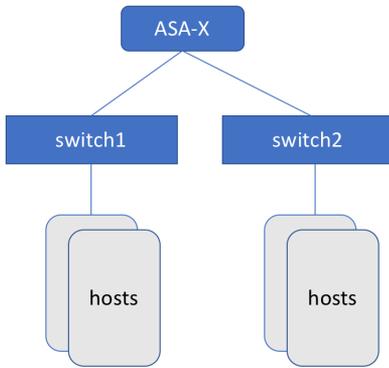
Host Name	Number of VMs	Power State	Version
ddc1-pod2esx046.dm.democompany.net	3	On	6.0.0
ddc1-pod2esx040.dm.democompany.net	3	On	6.0.0
ddc1-pod2esx037.dm.democompany.net	2	On	6.0.0

Cisco-ASA-Firewall

vRealize Network Insight unterstützt die Cisco-ASA-Firewall.

Die Funktionen für die Cisco-ASA-Firewall sind wie folgt:

- vRealize Network Insight unterstützt nur die Cisco-ASA-X-Serie.
- vRealize Network Insight unterstützt keine Firepower-Module.
- Derzeit unterstützt vRealize Network Insight die Cisco-ASA-Betriebssystemversion 9.4.
- vRealize Network Insight unterstützt nicht die Cluster-Bereitstellung von Cisco ASA.
- vRealize Network Insight unterstützt nicht die Hochverfügbarkeit von Cisco ASA.
- vRealize Network Insight unterstützt Cisco ASA nicht, wenn es direkt mit dem Host verbunden ist. Es wird eine Topologie unterstützt, die der folgenden ähnelt:



- Es werden nur die Cisco-ASA-Zugriffsregeln des Typs `Extended` unterstützt. Andere Zugriffsregeltypen wie `Standard`, `WebType`, `EtherType` usw. werden nicht unterstützt.
- Die Cisco-ASA-Firewall im VM-zu-VM-Pfad zeigt keine anwendbaren Zugriffsregeln an, wenn die Firewall im `Transparent`-Modus konfiguriert ist.

Beispiel

Sie können eine Abfrage für alle Cisco ASA-Einheiten durchführen, die von vRealize Network Insight unterstützt werden.

Tabelle 17-2.

Einheiten in Cisco ASA	Suchbegriffe	Beispielabfragen
Sicherheitskontext	ASA-Firewall ASA-Sicherheitskontext	<code>asa firewall where access group = <></code>
Zugriffsregel	ASA-Zugriffsregel	<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>
Zugriffsgruppe	ASA-Zugriffsgruppe	<code>asa access group where interface = <></code>
Netzwerkobjekt/ Netzwerkobjektgruppe	ASA-Netzwerkobjekt ASA-Netzwerkobjektgruppe	<code>asa network object where ip address = <></code> <code>asa network object group where ip address = <></code>
Dienstobjekt/Dienstobjektgruppe	ASA-Dienstobjekt ASA-Dienstobjektgruppe	<code>asa service object where port = <></code> <code>asa service where protocol = <></code> <code>asa service object group</code>

Check Point-Firewall

Der Check Point-Verwaltungsserver sollte den API-Zugriff über die Collector-IP-Adresse akzeptieren.

Sie können den Zugriff über den folgenden Menüpfad einrichten: **Verwaltung und Einstellungen > Blades > Verwaltungs-API > Erweiterte Einstellungen**.

Wenn Check Point MDS als Datenquelle hinzugefügt wird, ruft vRealize Network Insight Daten aus allen benutzerdefinierten Domänen und der globalen Domäne ab.

vRealize Network Insight verwendet die öffentliche Web-API-Schnittstelle von Check Point zum Abrufen der Daten vom Check Point-Verwaltungsserver. Wenn das VSX-Gateway mit dem Verwaltungsserver verknüpft ist, verwenden wir SSH-basierte CLI-Befehle zum Abrufen der von VSX verwalteten virtuellen System-VS-Routing-Tabelle, um die Anzeige des VS-Gateways im VM-VM-Pfad zu unterstützen.

vRealize Network Insight benötigt nur Leserechte für den Zugriff auf die Web-API-Schnittstelle, um die meisten Check Point-Daten abzurufen. Die wenigen Ausnahmen sind wie folgt:

- Wenn ein nicht-physisches VSX-Gateway mit dem Verwaltungsserver verbunden ist, sollte der Benutzer über Rechte für Lese- und Schreibzugriff für die Web-API verfügen. Dies ist erforderlich, um die Gateway-Routen für die Verwendung der `run script`-Web-API für die VM-VM-Pfadberechnung abzurufen.
- Wenn ein VSX-Gateway mit dem Verwaltungsserver verknüpft ist, sollte der Benutzer über SSH-Zugriff mit demselben Kennwort verfügen. Darüber hinaus sollte der Benutzer Zugriff auf den CLI-Befehl `vsx_util view_vs_conf` haben. Mit diesem Befehl werden die VSX-Gateway-Routen für die VM-VM-Pfadberechnung abgerufen.
- Für die MDS-Server-IP-Adresse als Datenquelle sollte der Benutzer über den Web-API-Zugriff auf alle Domänen einschließlich der MDS-Domäne und der globalen Domäne verfügen. Dies ist erforderlich, um Regeln, Richtlinienpakete und andere Daten aus allen Domänen abzurufen.

Sie können eine Abfrage für alle Check Point-Einheiten durchführen, die von vRealize Network Insight unterstützt werden. Allen Einheiten wird das Präfix `Check Point` vorangestellt. Einige der Abfragen für den Check Point lauten wie folgt:

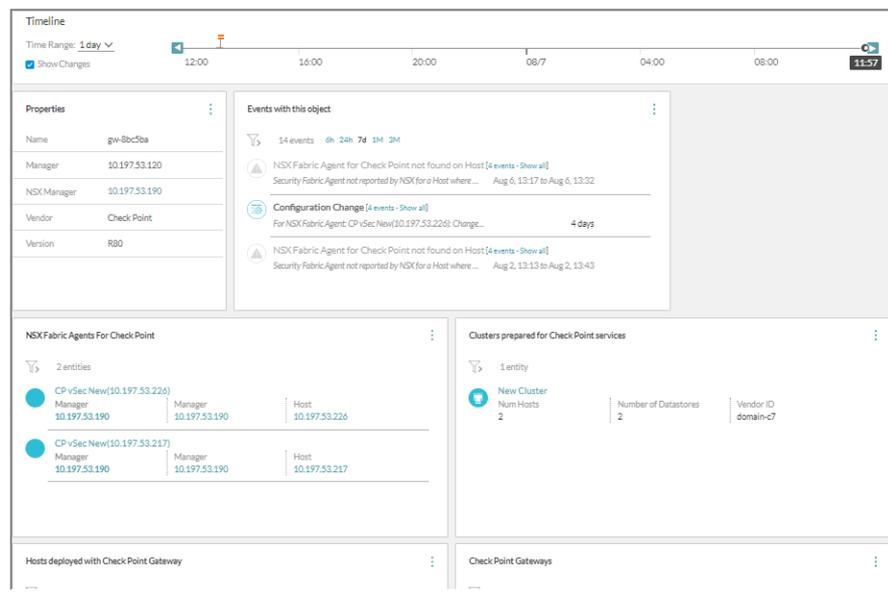
Tabelle 17-3.

Einheiten in Check Point	Suchbegriffe	Abfragen
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>
Gruppierung	Check Point Network Group	<code>Check Point Network Group where Translated VM = <></code>
		<code>vm where Network Group = <></code>

Tabelle 17-3. (Fortsetzung)

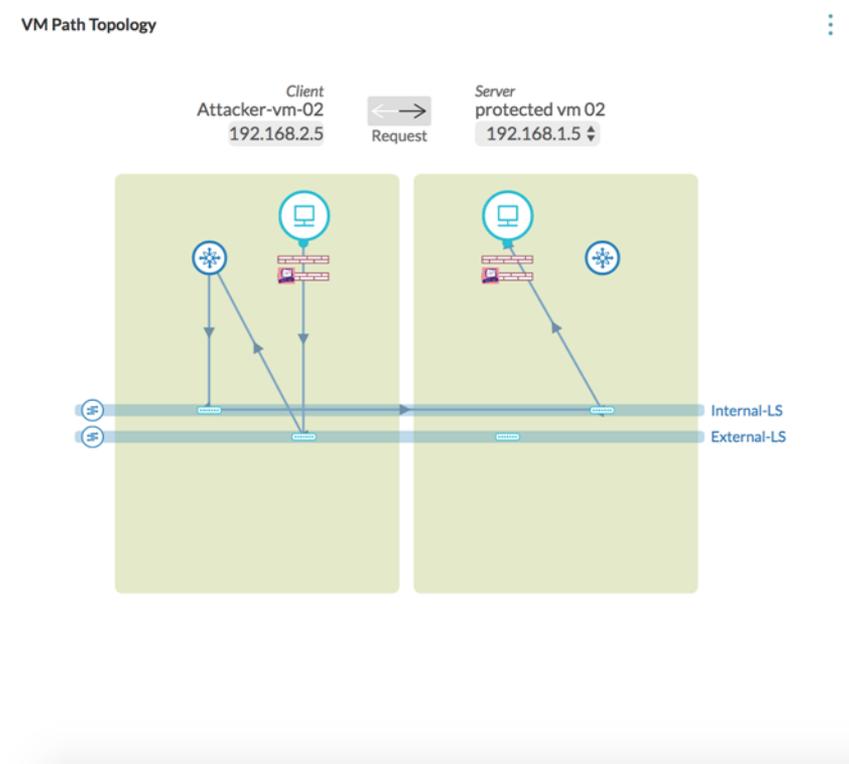
Einheiten in Check Point	Suchbegriffe	Abfragen
Dienst/Dienstgruppe	Check Point Service	Check point service where Port = <>
	Check Point Service Group	Check point service where protocol = <>
Zugriffsebene	Check Point Access Layer	Check Point Policy where Access Layer = <>
Domäne	Check Point Domain	check point domain where ip address = <>
		check point policy where domain = <>
		check point access layer where domain = <>
Gateways und Gateway-Cluster	Check Point Gateway	Check Point Gateway Cluster where Policy Package = <>
	Check Point Gateway Cluster	
Richtlinienpaket	Check Point Policy package	Check Point Policy where Policy Package = <>
		Check Point Policy Package where Rule = <>
Richtlinie	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)

Ein Beispiel für ein Check Point Manager-Dashboard wird wie folgt angezeigt:



In einem VM-VM-Topologie-Diagramm können Sie die Check Point-Dienst-VMs auf einem Host anzeigen, um die auf den jeweiligen Datenverkehr angewendeten Check Point-Regeln zu kennzeichnen. Das durch das VSX verwaltete virtuelle System-Gateway (Virtual System, VS) kann im VM-VM-Pfad als physisches Gateway angezeigt werden. Die Liste der anwendbaren Check Point-Richtlinien wird angezeigt, wenn Sie auf das Gateway-Symbol klicken.

Hinweis Für den VM-VM-Pfad unterstützt vRealize Network Insight nicht den VSX-Cluster mit virtuellem Switch und virtuellem Router.



Im Folgenden finden Sie einige Szenarien, für die die Systemereignisse für den Check Point generiert werden:

- Der NSX Fabric Agent wurde auf dem ESX für das Check Point-Gateway nicht gefunden.
- Die Check Point-Dienst-VM wurde nicht gefunden.
- Der Status des Check Point-Gateways `sic` wird nicht kommuniziert.
- Die Funktionen für Ermittlungs- und Aktualisierungsereignisse für die Check Point-Einheiten wie Adressbereich, Netzwerke, Richtlinien, Gruppen, Richtlinienpaket, Dienst, Dienstgruppe usw.

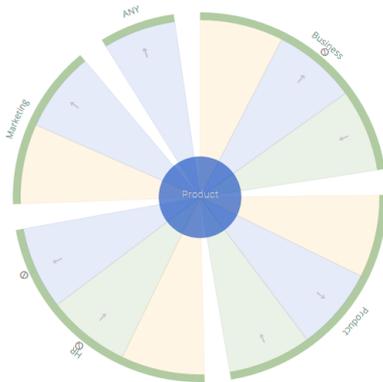
Sicherheitsgruppen

Sicherheitsgruppen sind ein Satz von Gruppen, die über einen gemeinsamen Satz von Berechtigungen verwaltet werden.

Die Sicherheitsgruppentopologie verfügt über die folgenden beiden Ansichten:

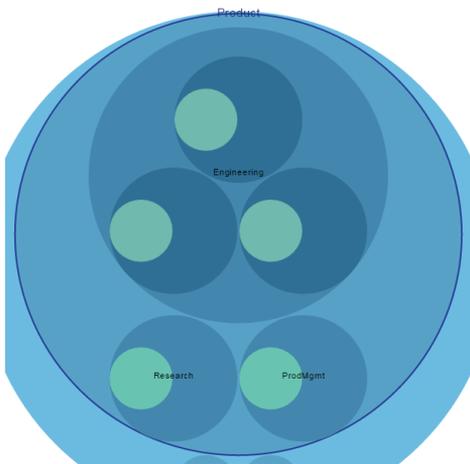
Firewallansicht

Die Firewalltopologie der Sicherheitsgruppe zeigt die Beziehung zwischen der ausgewählten Sicherheitsgruppe und anderen Sicherheitsgruppen an, indem die Firewallregeln präsentiert werden, die für die Sicherheitsgruppen anwendbar sind.



Container-Ansicht

In der Container-Topologie der Sicherheitsgruppe wird angezeigt, wie die Sicherheitsgruppe in Bezug auf ihre übergeordneten Sicherheitsgruppen oder untergeordneten Sicherheitsgruppen (Sicherheitsgruppen oder andere Einheiten) strukturiert ist.



Richtlinienbasiertes VPN

vRealize Network Insight unterstützt richtlinienbasiertes VPN in VMware Cloud on AWS, NSX-T und NSX-V. Die folgenden Szenarien werden für das richtlinienbasierte VPN unterstützt:

- VPN-Tunnel zwischen der öffentlichen IP-Adresse von VMware Cloud on AWS und der öffentlichen IP-Adresse von NSX-V/NSX-T/AWS

- VPN-Tunnel von der öffentlichen IP-Adresse von VMware Cloud on AWS und der öffentlichen IP-Adresse der Unternehmensfirewall zu einer 1:1-NAT zwischen der öffentlichen IP-Adresse der Unternehmensfirewall und der internen NSX Edge.

Hinweis vRealize Network Insight unterstützt nicht das Szenario des VPN-Tunnels von VMware Cloud on AWS, der auf einer Unternehmensfirewall endet, ohne dass eine NAT mit dem internen NSX Edge konfiguriert ist.

Richtlinienbasierte VPN-Einheiten

vRealize Network Insight ruft Daten für die `L3 VPN Session`-Einheit ab, bei der es sich um das tatsächlich im Datacenter konfigurierte VPN handelt.

Hier sind die Suchbegriffe für die richtlinienbasierten VPN-Einheiten:

Tabelle 17-4.

Suchbegriffe	Beschreibung
<code>Policy based VPN</code>	Alle richtlinienbasierten VPN-Sitzungen für VMware Cloud on AWS, NSX-V und NSX-T
<code>VMC Policy based VPN</code>	Richtlinienbasierte VPN-Sitzungen – VMware Cloud on AWS
<code>NSX-T Policy based VPN</code>	Richtlinienbasierte VPN-Sitzungen – NSX-T
<code>NSX Policy based VPN</code>	Richtlinienbasierte VPN-Sitzungen – NSX

Inaktive Regeln für verteilte NSX-Firewall

vRealize Network Insight unterstützt die Sichtbarkeit der Regeln für die verteilte NSX-Firewall, für die es seit einiger Zeit keine Flows gibt. Diese Regeln werden als inaktive Regeln bezeichnet. Diese Regeln verwenden einen Arbeitsspeicher-Heap und können Sicherheitsprobleme verursachen. Um diese inaktiven Regeln zu überwachen, stellt vRealize Network Insight die folgenden zwei Widgets im Dashboard **Sicherheit** bereit:

Hinweis Um das Sicherheits-Dashboard anzuzeigen, geben Sie **Sicherheit** in die Suchleiste ein.

- Nicht verwendete NSX-Firewallregel: Dieses Widget listet alle NSX-Firewallregeln auf, für die zum angegebenen Zeitpunkt kein Flow gemeldet wird. Sie können auch die folgende Suchabfrage verwenden, um diese Regeln abzurufen:

```
nsx firewall rule where flow is not set
```

Hinweis Stellen Sie sicher, dass Sie den verteilten NSX-Firewall-IPFIX für den angegebenen Zeitraum aktiviert haben.

Fortinet-Firewall

In vRealize Network Insight können Sie Erkenntnisse über die Fortinet-Firewall anzeigen.

vRealize Network Insight unterstützt die folgenden Fortinet-Einheiten:

- Fortinet Manager
- Fortinet ADOM: Details zur administrativen Fortinet-Domäne.
- Fortinet VDOM: Details zur virtuellen Fortinet-Domäne. vRealize Network Insight unterstützt nur Flow-basierte Filterung. Der transparente Modus wird nicht unterstützt.
- Fortinet-Adresse: Liste der ADOM-spezifischen Adressen. vRealize Network Insight unterstützen ipmask-, iprange- und NSX-Fabric-Connectors.
- Fortinet-Adressgruppen: Liste der ADOM-spezifischen Adressgruppen.
- Dynamische Fortinet-Adressen: Liste der ADOM-spezifischen dynamischen Adressen (VDOM zugeordnete Adressen)
- Dynamische Fortinet-Adressgruppen: Liste der ADOM-spezifischen dynamischen Adressgruppen (VDOM zugeordnete Adressgruppen)
- Dynamische Fortinet-Schnittstellen: Liste der ADOM-spezifischen dynamischen Schnittstellen.
- Fortinet-Zonen: Liste der ADOM-spezifischen Zonen.
- Fortinet-Dienste: Liste der manuell und automatisch generierten Dienste für jede ADOM.
- Fortinet-Dienstgruppen: Liste der Dienstgruppen für jede ADOM.
- Fortinet-Richtlinie: Fortinet-Richtlinien für jede ADOM. Derzeit unterstützen wir nur IPv4-Richtlinien, Fortinet Global Header-Richtlinien und Fortinet Global Footer-Richtlinien.
- Fortinet-Richtlinienpakete: Liste der Richtlinienpakete. Der Name der Richtlinienpakete enthält auch den Pfad zum Richtlinienpaket. Dieser ist dem Namen des Pakets vorangestellt.
- Fortinet-Geräte: Liste der dem FortiManager zugeordneten Fortinet-Geräte.
- Fortinet-Gerätegruppen: Liste der vom Benutzer angegebenen Fortinet-Gerätegruppen.

Nicht unterstützt werden:

- VM-zu-VM-Pfad im NAT-Modus.
- VM-zu-VM-Pfad für physische Geräte im transparenten Modus.
- Erweiterte (nicht-IP-basierte) Richtlinieigenschaften wie Benutzer, Benutzergruppe, Anwendung und Sicherheitsprofil.

Arbeiten mit der Mikrosegmentierung

18

vRealize Network Insight bietet Planung und Empfehlungen für die Implementierung der Sicherheit der **Mikrosegmentierung**. Es hilft dem Benutzer, die VMware-NSX-Bereitstellungen schnell und sicher zu verwalten und zu skalieren.

Dieses Kapitel enthält die folgenden Themen:

- [Analysieren der Anwendung](#)
- [Anwendungsermittlung](#)
- [VMware Cloud on AWS: Planung und Mikrosegmentierung](#)

Analysieren der Anwendung

Die Topologie der Mikrosegmentierungsplanung zeigt alle Flows an, die in Ihrer Umgebung vorhanden sind, indem die Flows in Segmente aufgeteilt werden.

In vRealize Network Insight ist ein Flow ein 4-Tupel. Dazu gehören:

- Quell-IP
- Ziel-IP
- Zielport
- Protokoll

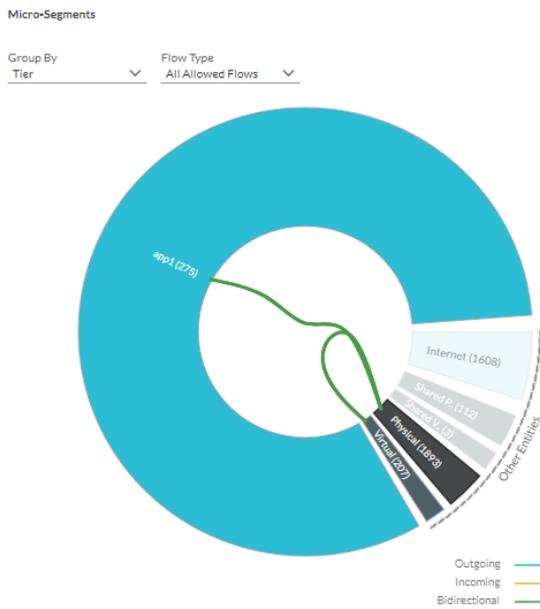
Sie können die Daten in zwei Formaten anzeigen: Donut-Ansicht und Rasteransicht.

Anzeigen von Mikrosegmentierungs- und Flow-Daten in der Donut-Ansicht

In der Donut-Ansicht bezeichnen die blauen Linien die ausgehenden Flows, die grünen Linien bezeichnen die eingehenden Flows und die gelben Linien bezeichnen die bidirektionalen Flows. Sie können auf eines der Segmente klicken, um die zugehörigen Details anzuzeigen.

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	

Jede Gruppe wird zu einem Keil erweitert. In der folgenden Topologie wird der Keil für **Physische Gruppe** angezeigt.



Der Flows-Pin zeigt an, dass die Flows für unterschiedliche Zeitintervalle durch Ports getrennt sind. Sie können entweder alle Flows oder die Flows zwischen zwei Einheiten anzeigen. Sie können die Flows nach zulässigen und blockierten Flows filtern. Sie können Flows entweder nach Gesamtbyte oder nach zulässiger Sitzungsanzahl anzeigen. Für die Flows, die durch eine Firewall geschützt werden, wird das Zeichen „Geschützt durch Firewall“ verwendet, um zu kennzeichnen, dass die Flows in diesem Port durch eine Firewall geschützt sind.

Bei der Planung für einen Geltungsbereich wie z. B. ein ganzes Datacenter oder ein Cluster werden Flows ausgewählt, die VMs oder physische Server (identifiziert durch die physischen IPs) als Quelle oder Ziel aufweisen.

Eine Topologie verfügt über zwei unterschiedliche Zonen:

- Intern: Diese Zone enthält die VMs oder die IP-Adressen im Geltungsbereich.
- Extern: diese Zone enthält die VMs oder die IP-Adressen, die außerhalb des Geltungsbereichs liegen, aber mit der VM oder den IP-Adressen in der internen Zone kommunizieren. Die externe Zone besteht aus folgenden Keilen:
 - DC virtuell: Es enthält die internen VMs des Quell- oder des Zieldatencenters, die mit VMs oder IP-Adressen in der internen Zone kommunizieren und keine bekannten gemeinsam genutzten Dienste wie LDAP, NTP usw. hosten.
 - Gemeinsam genutzt virtuell: Es enthält die internen VMs des Zieldatencenters, die bekannte gemeinsame Dienste wie LDAP, NTP usw. hosten, und mit denen die VMs oder IP-Adressen in der internen Zone kommunizieren.
 - DC physisch: Es enthält die internen physischen IP-Adressen des Quell- oder des Zieldatencenters, die mit VMs oder IP-Adressen in der internen Zone kommunizieren und keine bekannten gemeinsam genutzten Dienste wie LDAP, NTP usw. hosten.
 - Gemeinsam genutzt physisch: Es enthält die internen physischen IP-Adressen des Zieldatencenters, die bekannte gemeinsame Dienste wie LDAP, NTP usw. hosten, und mit denen die VMs oder IP-Adressen in der internen Zone kommunizieren.
 - Internet: Es enthält die externen VMs des Quell- oder des Zieldatencenters oder die physischen IP-Adressen, die mit den VMs oder IP-Adressen in der internen Zone kommunizieren.

Hinweis

- Datacenter-intern impliziert, RFC 1918 ordnete IPs standardmäßig zu + alle Überschreibungen, die in den E-W-Einstellungen definiert sind.
 - Datacenter-extern impliziert, Nicht-RFC 1918 ordnete IPs standardmäßig zu + alle Überschreibungen, die in den N-S-Einstellungen definiert sind.
-

Anzeigen von Mikrosegmentierungs- und Flow-Daten in der Rasteransicht

In vRealize Network Insight können Sie die Kommunikation zwischen Objekten in einer Tabellen- oder Rasteransicht anzeigen.

Verfahren

- 1 Navigieren Sie zu **Sicherheit > Sicherheit planen** und klicken Sie auf das Symbol für

Rasteransicht .

- 2 Wählen Sie einen Wert für die Option **Gruppieren nach** aus, z. B. **VMs**, **Anwendung**, **Sicherheitsgruppen**, um die entsprechenden Details im Tabellenformat anzuzeigen.

Feldname	Beschreibung
Quellobjekt	Name der Quelle
Zielobjekt	Name des Ziels
Verwandte Flows	Anzahl der Kommunikationen oder Flows zwischen Quelle und Ziel Klicken Sie auf den Wert für die Anzahl, um die zugehörigen Flow-Details anzuzeigen.
Byte-Summe	Gesamtzahl von Byte für alle Flows zusammen
Max. Datenverkehrsrate	Maximale Datenverkehrsrate, die bei allen zugehörigen Flows beobachtet wird
Anzahl der Sitzungen	Anzahl der aktiven Sitzungen für den jeweiligen Flow

Hinweis

- Mit einem Klick auf die einzelnen Spaltenüberschriften können Sie die Werte in aufsteigender oder absteigender Reihenfolge sortieren.
 - Sie können das Feld in der Tabellenansicht ausblenden, auf das Symbol „Mehr“ neben der Feldkopfzeile klicken und die Auswahl des Feldnamens aufheben.
- 3 Darüber hinaus können Sie auf der Seite „Rasteransicht“ diverse Aktionen ausführen.
 - Im Filterbereich auf der linken Seite des Bildschirms können Sie die folgenden Aktionen ausführen:
 - Wählen Sie eine einzelne Quelle oder ein einzelnes Ziel aus, um die Flows zu filtern, die mit dem ausgewählten Quell- oder Zielobjekt verknüpft sind.
 - Wählen Sie die Firewall-Aktion aus, um die zulässigen Flows oder die verloren gegangenen Flows anzuzeigen.
 - Wählen Sie den Schutzstatus aus, um den Flow-Status anzuzeigen.
 - Klicken Sie auf **Weitere Filter hinzufügen**, um weitere Filter hinzuzufügen.
 - Um die Tabellendaten in ein CSV-Format zu exportieren, klicken Sie oben in der Tabelle auf die Option „Mehr“ und wählen **Als CSV exportieren** aus.

Manuelles Erstellen einer Anwendung

Sie können eine Anwendung manuell in der vRealize Network Insight-Benutzeroberfläche erstellen.

Verfahren

- 1 Klicken Sie auf der vRealize Network Insight-Startseite auf **Sicherheit > Anwendungen**.
- 2 Klicken Sie auf der Registerkarte **Anwendungen** auf **Anwendung hinzufügen**.
- 3 Geben Sie auf der Seite **Anwendung hinzufügen** im Textfeld **Name der Anwendung** einen Namen für die Anwendung ein, die Sie erstellen möchten.

- 4 Geben Sie im Abschnitt **Ebene/Bereitstellung** einen eindeutigen Namen ein.

Sie können eine Ebene/Abteilung für VMs, physische Maschinen oder Dienste gemäß Ihren Anforderungen erstellen.

- 5 Wählen Sie im Feld **Mitglieder**

- a eine Bedingung aus dem Dropdown-Menü aus, um eine Ebene zu erstellen.

Sie können eine Bedingung basierend auf VM-Eigenschaften, Speicherort von VMs (Anwendung, Cluster, Ordner) und auch basierend auf den Kubernetes-Diensten (Dienstname, Cluster-IP-Adresse, Namespace, Cluster-IP oder Dienstbezeichnungen) definieren.

Um einen bestimmten Kubernetes-Dienst zu suchen, der in mehreren Clustern denselben Namen, dieselbe IP oder denselben Tag hat, zu durchsuchen, verwenden Sie die benutzerdefinierte Suche.

- b Geben Sie den Wert ein, den Sie der Ebene hinzufügen möchten, oder wählen Sie einen Wert aus.

Verwenden Sie für die Eingabe mehrerer Werte nach den einzelnen Werten jeweils ein Komma.

Um einen Dienst hinzuzufügen, der Teil der Ebene sein soll, wählen Sie **Dienstname** aus und geben den Namen in den Wert ein.

Basierend auf der definierten Bedingung sehen Sie die Anzahl zugeordneter oder verwandter VMs oder die Anzahl physischer IPs oder die Anzahl der Dienste.

- 6 Um zusätzliche Bedingungen hinzuzufügen, klicken Sie auf **Weitere Bedingung hinzufügen**.
- 7 (Optional) Um eine weitere Ebene unter einer Anwendung zu erstellen, klicken Sie auf **Ebene/Bereitstellung hinzufügen**.

Sie können mehrere Ebenen unter einer Anwendung erstellen.

Die Anwendung erstellt alle Ebenen und zeigt die Anzahl der VMs, physischen IPs und Dienste an, die allen Bedingungen entsprechen.

- 8 (Optional) Um eine dynamische Schwellenwertkonfiguration zu erstellen, aktivieren Sie das Kontrollkästchen **Schwellenwertanalyse aktivieren**.

Das System erstellt eine Schwellenwertkonfiguration auf der Seite

Schwellenwertkonfigurationen. Der von vRealize Network Insight erstellte Name der Schwellenwertkonfiguration beginnt mit dem Präfix `sys`.

Hinweis

- Wenn Sie ein Mitglied in der Anwendung hinzufügen und das Kontrollkästchen **Schwellenwertanalysen aktivieren** aktivieren, kann es etwa 20 Minuten dauern, bis das Mitglied auf der Seite „Schwellenwertkonfiguration“ angezeigt wird.
- Sie können eine vom System generierte Schwellenwertkonfiguration nicht löschen. Wenn Sie die Anwendung löschen oder das Kontrollkästchen **Schwellenwertanalysen aktivieren** deaktivieren und die Anwendung speichern, wird die vom System generierte Schwellenwertkonfiguration, die sich auf diese Anwendung bezieht, automatisch gelöscht.

- 9 Wählen Sie „Flows analysieren“ aus, um die Flows anzuzeigen, bevor Sie die Anwendung schließlich hinzufügen. Sie können die Ebenen basierend auf VMs oder physischen Adressen entsprechend anzeigen.

- 10 Klicken Sie auf **Speichern**.

Hinweis Wenn Ihre Anwendung über keine VMware-VM verfügt und Sie das Kontrollkästchen **Schwellenwertanalysen aktivieren** markieren, können Sie die Anwendung nicht speichern. Sie müssen eine VMware-VM hinzufügen oder die Auswahl des Kontrollkästchens **Schwellenwertanalysen aktivieren** aufheben, um Ihre Anwendung zu speichern.

- 11 (Optional) Um eine Vorschau der Flow-Analyse anzuzeigen, klicken Sie auf **Flow-Vorschau**.
Zeigt die Mikrosegmentansicht für die Anwendung an.

Nächste Schritte

Sie können die Anwendungsdetails unter **Gespeicherte Anwendung** anzeigen.

Erstellen von Ebenen für physische IPs

Beim Erstellen einer Anwendung können Sie **Benutzerdefinierte IP-Suche** aus der Dropdown-Liste auswählen, um Ebenen für die physischen IPs basierend auf den angereicherten Feldern zu erstellen. Weitere Informationen zu den angereicherten Feldern finden Sie unter [Anreicherung von Flows und IP-Endpoints](#).

Die angereicherten DNS-, Subnetz- und VLAN-Informationen können bei der Angabe von Ebenen wie folgt verwendet werden:

- Web

```
Query: IP Endpoint where Subnet Network = '172.16.101.0/24'
```

- App

```
Query: IP Endpoint where Dns Domain = app.example.com
```

- DB

```
Query: IP Endpoint where L2 Network = 'vlan-102'
```

- Gemeinsame Dienste

```
Query: IP Endpoint where Dns Domain = svc.example.com
```

Anwendungsermittlung

Wenn Sie über mehrere Anwendungen oder über mehrere Ebenen in einer Anwendung verfügen, wird das Erstellen von Anwendungen mithilfe der öffentlichen APIs oder der Benutzeroberfläche zu einem langen Prozess. vRealize Network Insight ermittelt automatisch die Anwendungen und aktiviert Sie für sie und ihre Ebenen automatisch. Das erspart Ihnen viel Handarbeit.

vRealize Network Insight kann die Anwendungsermittlung auf der Basis von Folgendem durchführen:

- Tags (vCenter Server- oder AWS-Tags)
- VM-Namen
- [Hinzufügen von ServiceNow](#)

Beispiel: Ein Beispiel für das Anwendungsermittlungskonstrukt

Nehmen wir an,

- Sie haben vCenter Server als Datenquelle hinzugefügt
- Sie verfügen über vier VMs in Ihrem Datacenter – VM1, VM2, VM3 und VM4.
- Sie haben Tags (Schlüssel/Wert) definiert, die die Anwendungsnamen definieren, zu denen jede VM gehört
- Sie haben Tags (Schlüssel/Wert) definiert, die die Ebene definieren, zu der jede VM gehört

Dies wird zum Beispiel in der folgenden Tabelle veranschaulicht:

VM-Name	Schlüssel-Wert-Tags
VM1	<ul style="list-style-type: none"> ■ Name der Anwendung: MyApplication1 ■ Anwendungsebene: App
VM2	<ul style="list-style-type: none"> ■ Name der Anwendung: MyApplication1 ■ Anwendungsebene: Internet
VM3	<ul style="list-style-type: none"> ■ Name der Anwendung: MyApplication2 ■ Anwendungsebene: App
VM4	<ul style="list-style-type: none"> ■ Name der Anwendung: MyApplication2 ■ Anwendungsebene: Internet

Ermitteln von Anwendungen auf der Basis von Tags

In vRealize Network Insight können Sie für diese Tags ein Gruppierungskriterium für die Anwendungsermittlung definieren.

In diesem Beispiel erkennt vRealize Network Insight basierend auf den definierten Tags und Gruppierungskriterien zwei Anwendungen (MyApplication1 und MyApplication2) mit zwei Ebenen (App und Internet) und den zugehörigen VMs.

Anwendung	Ebenen und ihre VMs
MyApplication1	■ App und VM1
	■ Internet und VM2
MyApplication2	■ App und VM3
	■ Internet und VM4

So erstellen Sie eine Anwendung und Ebenen basierend auf VM-Namen

Angenommen, die VM-Namen werden in einem bestimmten Format definiert. `ApplicationName` : `Tier` : `VMName`

```
MyApplication1 : App : VM1
MyApplication1 : Web : VM2
MyApplication2 : App : VM3
MyApplication2 : Web : VM4
```

Hinweis Zufällig definierte VM-Namen können nicht für die Anwendungsermittlung gruppiert werden.

Wenn Sie den folgenden Regex verwenden, ermittelt vRealize Network Insight zwei Anwendungen.

- App-Regex: `(.*)_(.*)_.*-.*`
- Ebenen-Regex: `(.*)_(.*)_(.*)-.*`

Anwendung	Ebenen und ihre VMs
MyApplication1	■ App und MyApplication1: App: VM1
	■ Internet und MyApplication1: Internet: VM2
MyApplication2	■ App und MyApplication2: App: VM3
	■ Internet und MyApplication2: Internet: VM4

Hinzufügen von ermittelten Anwendungen

Sie können vorhandene Anwendungen ermitteln und diese zu vRealize Network Insight hinzufügen.

Verfahren

- 1 Suchen Sie im Suchfeld nach der Zeichenfolge **Anwendungen**.
- 2 Führen Sie auf der Registerkarte **Anwendungen** eine oder alle der folgenden Aktionen aus:
 - Anwendung nach Name, Ebene oder Mitgliedern sortieren.
 - Anzahl der Anwendungen, die in der Topologie angezeigt werden (z. B. Top 10 oder Top 20) filtern. Jedes Sechseck stellt eine Anwendung dar. Je größer die Anzahl, desto dunkler die Farbe des Sechsecks.
 - Anwendungen nach Namen, Ebenen oder Mitgliedern durchsuchen.
- 3 Klicken Sie auf die Registerkarte **Ermitteln**.

Sie sehen die folgenden Registerkarten zum Hinzufügen einer Anwendung: **Tags**, **ServiceNow**, **Namen** und **Advanced**.

- 4 Klicken Sie auf die gewünschte Registerkarte und führen Sie die entsprechenden Schritte aus.

Registerkarte	Beschreibung
Tags	<ol style="list-style-type: none"> a Legen Sie den Geltungsbereich fest. <ul style="list-style-type: none"> ■ Wählen Sie Alle VMs aus, um eine Liste aller VMs aus allen Datenquellen anzuzeigen, die in vRealize Network Insight hinzugefügt werden, oder ■ klicken Sie auf Manuelle Auswahl und filtern Sie die VMs je nach Bedarf, z. B. nach Konto, Datacenter, Manager usw. b Legen Sie den Schlüssel und den Wert für das Tag fest. <ul style="list-style-type: none"> ■ Geben Sie einen Schlüssel für das Tag ein. Beispiel: <i>Automation</i>, <i>Category</i>, <i>CreatedBy</i> und <i>Owner</i>. ■ (Optional) Geben Sie einen Wert für den jeweiligen Schlüssel ein. c Klicken Sie auf den Link count Anwendungen gefunden, um die Liste der Anwendungsnamen, die VM-Namen und die Anzahl der VMs anzuzeigen, die mit den angegebenen Kriterien übereinstimmen. d Klicken Sie auf Nicht klassifizierte VMs, um eine Liste der VMs anzuzeigen, die nicht dem angegebenen Namens- oder Tag-Muster folgen. Sie können die VMs bearbeiten, um die Namens- oder Tag-Kriterien zu korrigieren. e Wählen Sie die Option Änderungen speichern unter aus, um eine neue Vorlage zu erstellen oder eine vorhandene Vorlage zu aktualisieren. <hr/> <p>Hinweis Wenn Sie Admin-Benutzer sind, können Sie alle Vorlagen aktualisieren. Wenn Sie Mitglied-Benutzer sind, können Sie nur die Vorlagen bearbeiten, die Sie selbst erstellt haben.</p> <hr/> f Klicken Sie auf Ermitteln.
ServiceNow	Sie sehen die auf ServiceNow verfügbaren Anwendungen.

Registerkarte	Beschreibung
Namen	<p>a Legen Sie den Geltungsbereich fest.</p> <ul style="list-style-type: none"> ■ Klicken Sie auf Alle VMs, um eine Liste aller VMs aus allen Datenquellen anzuzeigen, die in vRealize Network Insight hinzugefügt werden, oder ■ klicken Sie auf Manuelle Auswahl und filtern Sie die VMs je nach Bedarf, z. B. nach Konto, Datacenter, Manager usw. <p>b Klicken Sie auf Mustererstellung.</p> <p>Je nachdem, welchen Geltungsbereich Sie festgelegt haben, filtert vRealize Network Insight die Liste der VMs in der Mustererstellung.</p> <ol style="list-style-type: none"> 1 Wählen Sie den Standard-VM-Namen aus oder wählen Sie eine VM aus der Liste aus, um ein Muster oder den regulären Ausdruck (Regex) basierend auf dem VM-Namen zu erstellen. 2 Klicken Sie auf eine Position oder eine Gruppe, um ein Muster zu erstellen. <hr/> <p>Hinweis Wenn Sie nach der Auswahl einer Gruppe ein Zeichen oder eine Position auswählen, ignoriert vRealize Network Insight Ihre Gruppenauswahl für die Erstellung des Musters und umgekehrt.</p> <hr/> <p>Je nach Ihrer Auswahl sehen Sie, dass das Muster auf dem Bildschirm angezeigt wird. Außerdem wird die Liste der Anwendungen angezeigt, die mit dem Muster übereinstimmen, sowie die Anzahl der VMs in den jeweiligen Anwendungen und die VM-Namen in den jeweiligen Anwendungen.</p> <ol style="list-style-type: none"> 3 Klicken Sie auf Absenden. <p>c Klicken Sie auf den Link count Anwendungen gefunden, um die Liste der Anwendungsnamen, die VM-Namen und die Anzahl der VMs anzuzeigen, die mit dem Regex übereinstimmen.</p> <p>d Klicken Sie auf Nicht klassifizierte VMs, um eine Liste der VMs anzuzeigen, die nicht dem angegebenen Namensmuster folgen.</p> <p>e Wählen Sie die Option Änderungen speichern unter aus, um eine neue Vorlage zu erstellen oder eine vorhandene Vorlage zu aktualisieren.</p> <hr/> <p>Hinweis Wenn Sie Admin-Benutzer sind, können Sie alle Vorlagen aktualisieren. Wenn Sie Mitglied-Benutzer sind, können Sie nur die Vorlagen bearbeiten, die Sie selbst erstellt haben.</p> <hr/> <p>f Klicken Sie auf Ermitteln.</p>
Advanced	<p>a Legen Sie den Geltungsbereich fest.</p> <ul style="list-style-type: none"> ■ Klicken Sie auf Alle VMs, um eine Liste aller VMs aus allen Datenquellen anzuzeigen, die in vRealize Network Insight hinzugefügt werden, oder ■ klicken Sie auf Manuelle Auswahl und filtern Sie die VMs je nach Bedarf, z. B. nach Konto, Datacenter, Manager usw. <p>b Klicken Sie auf Mustererstellung.</p> <p>Je nachdem, welchen Geltungsbereich Sie festgelegt haben, filtert vRealize Network Insight die Liste der VMs in der Mustererstellung.</p> <ol style="list-style-type: none"> 1 Wählen Sie den Standard-VM-Namen aus oder wählen Sie eine VM aus der Liste aus, um ein Muster oder den regulären Ausdruck (Regex) basierend auf dem VM-Namen zu erstellen.

Registerkarte	Beschreibung
	<p>2 Klicken Sie auf eine Position oder eine Gruppe, um ein Muster zu erstellen.</p> <hr/> <p>Hinweis Wenn Sie nach der Auswahl einer Gruppe ein Zeichen oder eine Position auswählen, ignoriert vRealize Network Insight Ihre Gruppenauswahl für die Erstellung des Musters und umgekehrt.</p> <hr/> <p>Je nach Ihrer Auswahl sehen Sie, dass das Muster auf dem Bildschirm angezeigt wird. Außerdem wird die Liste der Anwendungen angezeigt, die mit dem Muster übereinstimmen, sowie die Anzahl der VMs und die VM-Namen in den jeweiligen Anwendungen.</p> <p>3 Klicken Sie auf Absenden.</p> <p>c Klicken Sie auf den Link count Anwendungen gefunden, um die Liste der Anwendungsnamen und die Anzahl der VMs anzuzeigen, die mit dem Regex übereinstimmen, sowie die VM-Namen.</p> <p>d Klicken Sie auf Nicht klassifizierte VMs, um eine Liste der VMs anzuzeigen, die nicht dem angegebenen Namensmuster folgen.</p> <p>e Wählen Sie die Option Änderungen speichern unter aus, um eine neue Vorlage zu erstellen oder eine vorhandene Vorlage zu aktualisieren.</p> <hr/> <p>Hinweis Wenn Sie Admin-Benutzer sind, können Sie alle Vorlagen aktualisieren. Wenn Sie Mitglied-Benutzer sind, können Sie nur die Vorlagen bearbeiten, die Sie selbst erstellt haben.</p> <hr/> <p>f Klicken Sie auf Ermitteln.</p>

Sie sehen die Tabellenansicht und die Sechseck-Zuordnungsansicht für alle Anwendungen, die den Kriterien entsprechen.

In der Zuordnungsansicht können Sie den Mauszeiger über das Sechseck bewegen, um Informationen wie den Namen der Anwendung, die Anzahl ermittelter VMs und die Anzahl der Ebenen anzuzeigen. Die Linien zwischen Anwendungen und Internet stellen die Verbindungen dar. Sie können auf die Linien klicken, um die Flow-Details anzuzeigen, wie z. B. die Anzahl der Quell- und Ziel-Flows und die Anzahl der ungeschützten Quell-Flows und ungeschützten Ziel-Flows. Das Fragezeichen auf dem Sechseck bedeutet, dass vRealize Network Insight keine Flow-Details für die Anwendung finden oder abrufen konnte, weil die Anwendung den Flow-Grenzwert überschritten hat oder ungeschützte Flows aufweist.

In der Tabellenansicht werden Anwendungsdetails angezeigt, darunter der Name der Anwendung, die Anzahl der Flows, die das Ziel nicht erreichen und verloren gehen, wenn die Firewall-Aktion verweigert wird, sowie die Anzahl der Ebenen und Mitglieder.

Die Zuordnungs- und die Tabellenansicht sind interaktiv. Wenn Sie in der Tabellenansicht auf eine Anwendung klicken, wird das Sechseck in der Zuordnungsansicht hervorgehoben oder fokussiert und alle Netzwerkverbindungen werden angezeigt.

- 5 (Optional) Führen Sie eine der folgenden Aktionen in der Zuordnungsansicht aus:
- Vergrößern und verkleinern Sie die Zuordnung oder verschieben Sie sie, um die Anwendungen anzuzeigen.
 - Zeigen Sie alle ungeschützten Anwendungen an.

- Weitere Informationen finden Sie in den Anwendungen, die mit dem Internet kommunizieren.
 - Sehen Sie sich alle Anwendungen an, die von Hosts gemeinsam genutzte Dienste verwenden.
 - Sehen Sie sich die Anwendungen mit Problemen an.
- 6 (Optional) Führen Sie eine der folgenden Aktionen in der Tabellenansicht aus:
- Bewegen Sie den Mauszeiger auf den Wert in der Spalte „Mitglied“, um die Anzahl der einzelnen VMs, physischen IPs und Dienste anzuzeigen.
 - Klicken Sie auf den Namen einer Anwendung, um das Anwendungs-Dashboard zu öffnen und die Details zu dieser spezifischen Anwendung anzuzeigen.
 - Klicken Sie auf das +-Symbol in der Tabellenansicht, um die Anwendungsdetails zu erweitern, wie z. B. die Kriterien und die Anzahl der VMs und der Ebenen.

Hinweis Das Symbol ist nur für die ermittelten Anwendungen verfügbar.

- 7 Um die ermittelte Anwendung zu speichern,
- können Sie in der Zuordnungsansicht die Maus auf das Sechseck bewegen und auf **Anwendung speichern** klicken oder
 - in der Tabellenansicht auf **Anwendung speichern** klicken.

Hinweis Sie können die Massenspeicherung der Anwendungen durchführen, indem Sie mehrere Kontrollkästchen der Anwendungen in der Tabelle auswählen und dann auf **Anwendung speichern** klicken.

- 8 Überprüfen Sie die Details auf der Seite „Anwendung hinzufügen“ und klicken Sie auf **Absenden**.

Nach dem Speichern sehen Sie in der Hoverliste zum Anwendungssechseck die Bestätigung `application:Saved`. In der Tabellenansicht wird ein Häkchen für die Anwendung angezeigt. Wenn die Anwendung bereits gespeichert wurde, können Sie den Mauszeiger über das Häkchen bewegen und auf **Speichern unter** klicken, um die Anwendung unter einem anderen Namen zu speichern.

Hinweis Wenn die Anwendungen in ServiceNow geändert werden, werden sie in vRealize Network Insight nicht automatisch aktualisiert. In vRealize Network Insight müssen Sie die Anwendung manuell aktualisieren.

Tabelle 18-1. Einschränkungen

Objekte	Empfohlene Grenzwerte
Anwendungsliste in der Zuordnungsansicht	1000
Anwendungsliste in der Tabellenansicht	NA
Gespeicherte Anwendungen	400
Gesamtzahl der Ebenen für alle Anwendungen	5000
Ebenen pro Anwendung	30
Mitglieder pro Ebene	NA
Mitglieder pro Anwendung	1 800
	Wenn eine Anwendung den Grenzwert überschreitet, werden die Flow-Informationen möglicherweise nicht in der Pinnwand der Anwendungstopologie angezeigt oder es wird eine Fehlermeldung angezeigt.
Flows pro Anwendung	300.000

Wenn Ihre Einrichtung die empfohlenen Grenzwerte für Ebenen, Anwendungen und Flows pro Anwendung überschreitet, können Sie zwar mit dem Hinzufügen der Objekte fortfahren, aber die Leistung wird möglicherweise beeinträchtigt.

Nächste Schritte

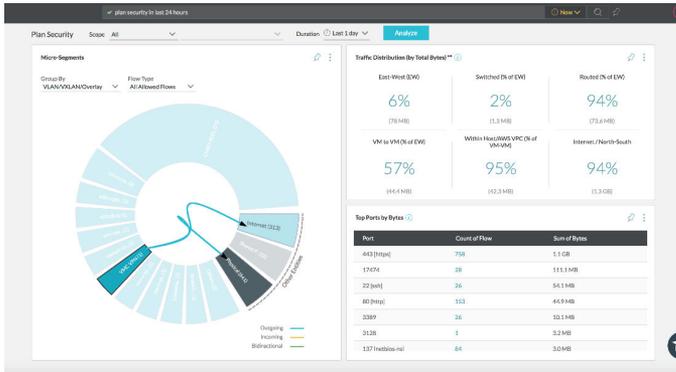
Klicken Sie auf **Als CSV exportieren**, um die Anwendungsdetails im CSV-Format zu exportieren. Sie können die Anzahl der Anwendungen und die Felder definieren, die Sie exportieren möchten. Die Felder „Name der Anwendung“ und „Name der Ebene“ werden basierend auf der Anzahl der Mitglieder (eine Zeile pro Mitglied) wiederholt. Nur die Felder, die mit der Anwendung verknüpft sind, werden ausgefüllt, sodass die restlichen Felder leer bleiben.

VMware Cloud on AWS: Planung und Mikrosegmentierung

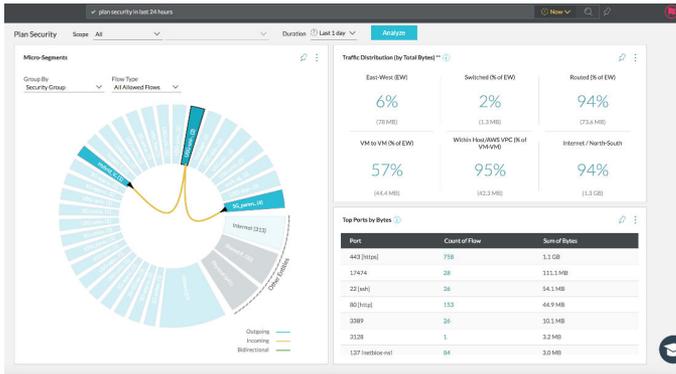
Verwenden von vRealize Network Insight

Sie können ein bestimmtes VMware Cloud on AWS-Segment planen, indem Sie auf der Seite **Sicherheit planen** als Geltungsbereich **VMC-Segment** auswählen.

Verwenden Sie für die Richtliniensegmente die **VLAN/VXLAN/Overlay**-Klausel in der Gruppe.



Verwenden Sie für die Richtliniengruppen die **Security Group**-Klausel in der Gruppe.

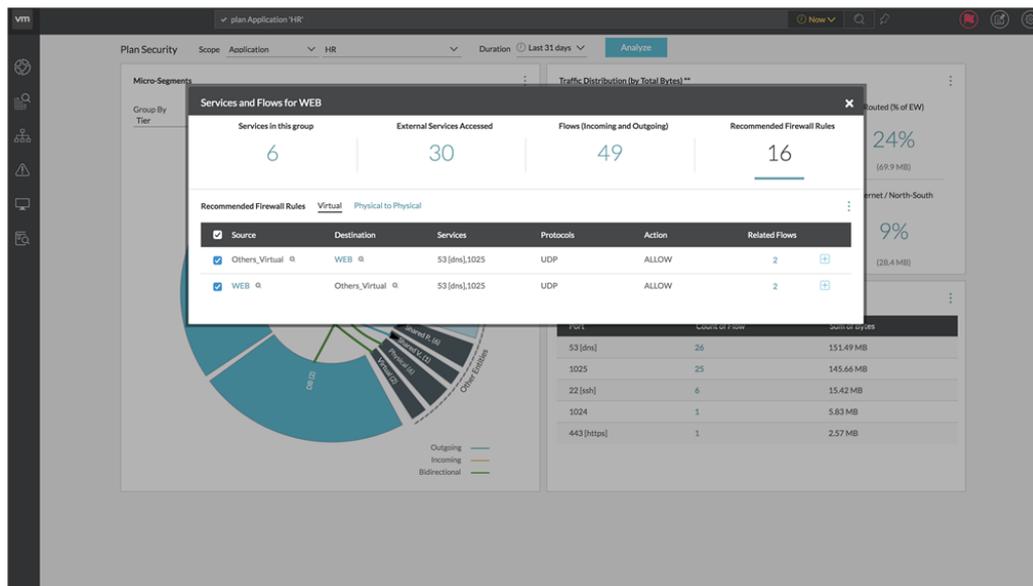


Empfohlene Firewallregeln

19

Wenn Sie auf der Seite **Sicherheitsplanung** auf den Keil oder die Kante des Topologiediagramms klicken, können Sie die Liste der Dienste und Flows für dieses bestimmte Segment anzeigen. Klicken Sie auf **Empfohlene Firewallregeln**, um die darauf definierten Regeln anzuzeigen. Die Mitglieder der Quelle oder des Ziels werden unter den folgenden Regeltypen aufgelistet:

- **Physisch-physisch:** Diese Registerkarte listet alle Regeln für physische und Internet-IPs auf. Die Regeln können für Einheiten physisch-physisch, physisch-Internet, Internet-physisch oder Internet-Internet gelten.
- **Virtuell:** Diese Registerkarte listet alle Regeln auf, bei denen mindestens einer der Endpunkte eine VM ist.



Für jede Firewallregel stehen die folgenden Details zur Verfügung:

- Mitglieder der Gruppe anzeigen: Klicken Sie auf das Symbol + neben dem Namen der Einheit, um die Mitglieder der Gruppe anzuzeigen.

Source	Destination	Services	Protocols	Action	Related Flows
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

Hinweis

- Die Mitglieder für die Gruppen, die zur Internetkategorie gehören, werden nicht angezeigt.
 - Wenn eine Sicherheitsgruppe sowohl über virtuelle als auch über physische IPs verfügt, werden die physischen und die Internet-IPs nicht in der Liste der Mitglieder dieser bestimmten Gruppe angezeigt.
 - Die Kubernetes-Dienste der Mitglieder werden auf der Registerkarte **Kubernetes-Dienste** angezeigt.
 - Wenn die Anzahl der Mitglieder oder der Eintrag für **Virtuelle Maschine, Physische und Internet-IPs** oder **Kubernetes-Dienste** null ist, wird die Registerkarte nicht angezeigt.
- Quelle
 - Ziel
 - Dienste
 - Protokolle
 - Aktion
 - Verwandte Flows: Klicken Sie auf die Anzahl der verknüpften Flows, um die Liste der Flows mit den entsprechenden Flow-Informationen anzuzeigen.
 - Angewendete Firewallregeln anzeigen: Klicken Sie auf das Symbol + neben der Spalte **Verwandte Flows**, um die angewendeten Firewallregeln anzuzeigen, die den ähnlichen Flow-Sätzen entsprechen.

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

Sie können die empfohlenen Regeln als XML- oder CSV-Datei basierend auf Ihren Anforderungen exportieren.

Hinweis Sie können empfohlene Regeln im Zusammenhang mit Kubernetes-Objekten auch in das YAML-Format exportieren.

Weitere Informationen zu diesen Artefakten finden Sie unter [Exportregeln](#).

Empfohlene Firewallregel zum Schutz gefährdeter Betriebssysteme

Mit dem folgenden Verfahren können Sie die empfohlene Firewallregel zum Schutz gefährdeter Betriebssysteme abrufen:

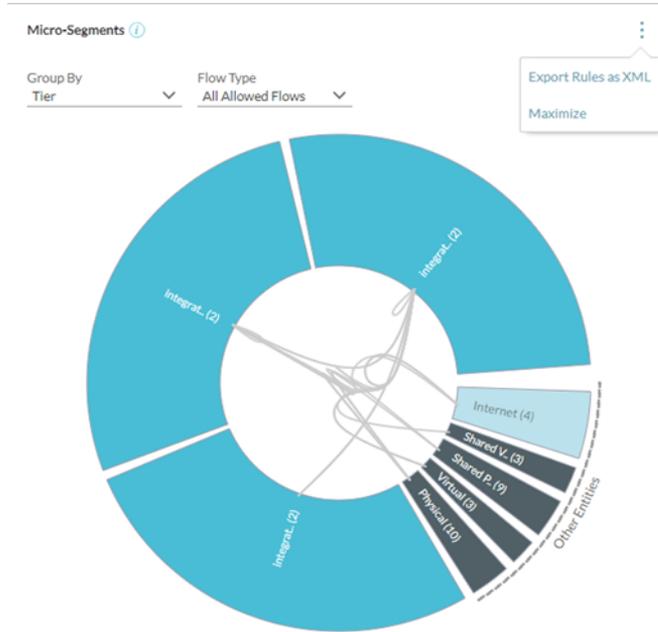
- 1 Klicken Sie auf **Sicherheit > Anwendung > Anwendung erstellen**.
- 2 Geben Sie einen Namen für die Anwendung und die Ebene/Bereitstellung ein.
- 3 Klicken Sie im Dropdown-Menü **Mitglied** auf **Benutzerdefinierte VM-Suche** und geben Sie im Textfeld unter „Qualifizierer“ die folgenden Übereinstimmungskriterien als Bedingung ein: **Betriebssystem wie 'Microsoft Windows Server 2003' oder Betriebssystem wie 'Microsoft Windows Server 2008' oder Betriebssystem wie 'Red Hat Enterprise Linux 6' oder Betriebssystem wie 'Red Hat Enterprise Linux 5' oder Betriebssystem wie 'SUSE Linux Enterprise 10'**.
- 4 Klicken Sie auf **Speichern**.
- 5 Wechseln Sie zu **Sicherheit > Sicherheit planen**.
- 6 Wählen Sie in der Dropdown-Liste **Geltungsbereich** die Option **Anwendung** und den Namen der von Ihnen erstellten Anwendung aus.
- 7 Wählen Sie im Dropdown-Menü **Dauer** die Option **Letzte 7 Tage** aus.
- 8 Um die empfohlenen Firewallregeln abzurufen, klicken Sie auf **Analysieren**.

Dieses Kapitel enthält die folgenden Themen:

- [Exportregeln](#)
- [Exportieren und Anwenden von Kubernetes-Netzwerkrichtlinien](#)

Exportregeln

Sie können alle Regeln als XML für die gesamte Topologie exportieren. Sie finden diesen Menüpunkt auf der Seite **Mikrosegmentierungsplanung** wie folgt:



Die Option „Als XML exportieren“ ist nur für die folgenden Einheiten verfügbar:

- Sicherheitsgruppe
- Anwendungsebene

Wenn der Planungsbereich nur einen einzigen NSX Manager umfasst, enthalten die generierten Artefakte die XML-Dateien, die den empfohlenen Diensten und Firewallregeln entsprechen. Wenn der Planungsbereich mehrere NSX Manager umfasst, enthalten die generierten Artefakte die XML-Dateien, die den empfohlenen Diensten, IPSets, Sicherheitsgruppen und Firewallregeln entsprechen.

Im Folgenden finden Sie die Platzhalterartefakte für Sicherheitsgruppen:

- SG-Others_Internet.xml
- SG-Other.xml

Sie können alle Regeln als XML oder CSV für einen bestimmten Keil oder Edge exportieren, der im Topologie-Diagramm dargestellt wird.

Hinweis Sie können empfohlene Regeln im Zusammenhang mit Kubernetes-Objekten auch in das YAML-Format exportieren.

Globale NSX DFW-Artefakte

Es ist einfach, Objekte in globalen Sicherheitsgruppen über die verschiedenen vCenter- und NSX-Bereitstellungen hinweg zu verwalten. vRealize Network Insight unterstützt die Generierung und den Import der globalen Artefakte ausschließlich für die Anwendungs- und Ebenengruppen. Mit den globalen Sicherheitsgruppen wird es einfach, die Firewallregeln in vCenter-übergreifenden Szenarios problemlos bereitzustellen und zu verwalten. Stellen Sie sicher, dass Sie die globalen Artefakte auf dem primären NSX Manager importieren. Sie können die Mitgliedschaft der globalen Sicherheitsgruppe nur über den primären NSX Manager verwalten.

Eine globale Sicherheitsgruppe besteht wahlweise aus:

- Anderen globalen Gruppen
- Globalen IP Sets
- Globalem Sicherheits-Tag

Wenn Sie die Regeln als XML exportieren, wird zusätzlich zu den spezifischen NSX Manager-Ordern ein globaler Ordner erstellt, der aus den globalen NSX DFW-Artefakten besteht. Die entsprechenden globalen Sicherheitsgruppen, globalen IP Sets, globalen Sicherheits-Tags und globalen DFW-Firewallregeln werden nach dem Import der globalen NSX DFW-Artefakte erstellt.

Hinweis

- Das globale Sicherheits-Tag wird nur im Aktiv/Standby-Modus unterstützt.
- Der globale IP Set wird sowohl im Aktiv/Aktiv- als auch im Aktiv/Standby-Modus unterstützt.

Sie können den globalen IP Set oder das globale Sicherheits-Tag basierend auf Ihren Anforderungen erstellen. Wenn Sie das globale Sicherheits-Tag erstellen, können Sie die Anwendungs-VM dem Sicherheits-Tag zuordnen. Andernfalls wird der globale IP Set verwendet.

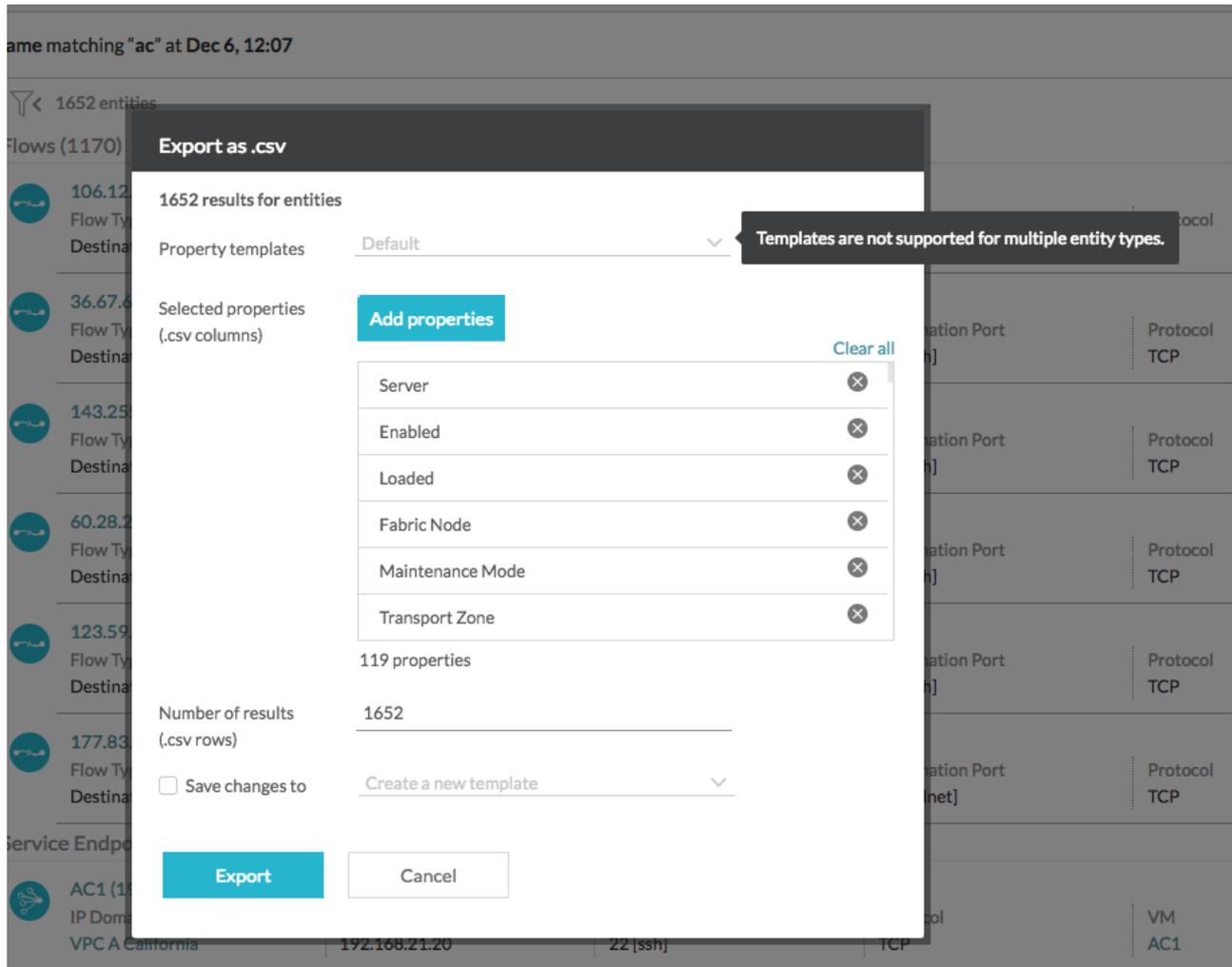
Sie können die folgenden Flags im Import-Tool verwenden:

Tabelle 19-1.

Flag-Name	Beschreibung
-uni	So importieren Sie Artefakte aus dem globalen Ordner.
-utag	So importieren Sie die globalen Artefakte mit den globalen Sicherheits-Tags in der Mitgliedschaft der globalen Sicherheitsgruppen.
-log	Zum Erstellen von Regeln, in denen die Protokollierung aktiviert ist.
	Hinweis Dieses Flag ist nicht spezifisch für die globale Option.

Speichern der Konfiguration für CSV-Export als Eigenschaftsvorlage

Beim Exportieren der Daten aus Widgets in die CSV-Dateien können Sie die Kombination der zu exportierenden Eigenschaften (oder Spalten) in den Eigenschaftsvorlagen speichern. Diese Eigenschaftsvorlagen sind für den CSV-Export aktiviert, wenn die Ergebnisse zu einem einzelnen Einheitstyp gehören. Wenn Sie mit einem Schlüsselwort suchen, das mehrere Einheitstypen auflistet, kann die Kombination der Eigenschaften nicht in den Eigenschaftsvorlagen gespeichert werden.



Wenn Sie das CSV-Exportmodell öffnen, sehen Sie die Standardauswahl der Eigenschaften für die Suchergebnisse (je nach Einheitstyp). Sie können diese Liste der ausgewählten Eigenschaften ändern und die neue Konfiguration als Referenz für Ihren zukünftigen Bedarf speichern. Alternativ können Sie auch eine vorab gespeicherte Eigenschaftsvorlage aus dem Abschnitt **Vorlagen** im CSV-Exportmodell laden oder öffnen. Wenn Sie den Wert ändern, sehen Sie die ausgewählten Eigenschaften für die ausgewählte Eigenschaftsvorlage.

Nachdem Sie Änderungen an den ausgewählten Eigenschaften für den Export vorgenommen haben, können Sie eine Eigenschaftsvorlage aus dem CSV-Exportmodell erstellen oder eine vorhandene Eigenschaftsvorlage bearbeiten. Diese Vorlage hat denselben Einheitstyp wie die aktuellen Suchergebnisse.

Sie können die Liste der vorhandenen Eigenschaftsvorlagen im System anzeigen, indem Sie zu der Seite **Einstellungen** -> **Eigenschaftsvorlagen** navigieren. Die Liste auf der Seite **Eigenschaftsvorlagen** zeigt die vorhandenen Vorlagen mit Angaben wie Einheitstyp, letzte Aktualisierung und Anzahl der Eigenschaften. Sie können Eigenschaftsvorlagen auf der Seite **Eigenschaftsvorlagen** bearbeiten oder löschen. Sie können die Eigenschaftsvorlage bearbeiten, ohne ihren Namen zu ändern.

Exportieren und Anwenden von Kubernetes-Netzwerkrichtlinien

Sie können die empfohlenen Regeln für Netzwerkrichtlinien im Zusammenhang mit Kubernetes-Objekten in das YAML-Format exportieren. vRealize Network Insight unterstützt nur das Exportieren in das YAML-Format für die Gruppe nach Namespace und das Gruppieren nach Dienstopologien.

Voraussetzungen

- [Hinzufügen von Kubernetes](#)
- [Hinzufügen von VMware PKS](#)

Verfahren

- 1 Um die empfohlenen Regeln in das YAML-Format zu exportieren, wählen Sie im Sicherheitsplanungsmodell den Kubernetes-Cluster aus, für den Sie die Sicherheit planen möchten, und führen einen der folgenden Schritte aus.
 - Erweitern Sie weitere Optionen im Widget „Mikrosegmente“ und wählen Sie **Regeln als YAML exportieren** aus.
 - Wählen Sie einen Knoten in der Donut-Ansicht des Mikrosegments aus, klicken Sie auf die Anzahl der empfohlenen Firewallregeln, erweitern Sie weitere Optionen und klicken Sie auf **Regeln als YAML exportieren**.

vRealize Network Insight lädt eine ZIP-Datei mit dem Namen „Kubernetes-Netzwerkrichtlinien“ und einen zugehörigen Zeitstempel herunter. Wenn Sie die Datei entpacken, sehen Sie die folgenden fünf CSV-Dateien und auch mehrere Ordner, je nach der Anzahl der Cluster. Jeder Ordner enthält mehrere YAML-Dateien für den Cluster.

Dateiname	Beschreibung
network-policy-others-ipaddress.csv	Enthält die IP-Adressen der physischen Server und der virtuellen Maschine, mit denen die Dienste oder Namespaces kommunizieren.
recommended-namespace-labels-to-add.csv	Enthält die Bezeichnungen, die an die dem Namespace zugeordneten Pods angehängt werden sollen. Beispiel <ul style="list-style-type: none"> ■ Cluster – pdk8s ■ Namespace – sock-shop ■ Bezeichnung – sock-shop-pdk8s

Dateiname	Beschreibung
<code>recommended-service-labels-to-add.csv</code>	<p>Enthält die Bezeichnungen, die an die dem Dienst zugeordneten Pods angehängt werden sollen.</p> <p>Beispiel</p> <ul style="list-style-type: none"> ■ Cluster – pdk8s ■ Namespace – sock-shop ■ Dienst – front-end ■ Bezeichnung – Service:front-sock-shop-pdk8s ■ Cluster – pdk8s ■ Namespace – sock-shop ■ Dienst – user ■ Bezeichnung – Service:user-sock-shop
<code>recommended-network-policy.csv</code>	Enthält alle von vRealize Network Insight empfohlenen Regeln.
<code>exported-network-policy-rule-names.csv</code>	Listet alle auf der Basis der empfohlenen Regeln exportierten Netzwerkrichtlinien auf.

2 Führen Sie die folgenden Schritte aus, um die Dienstbezeichnungen anzuwenden:

- a Führen Sie den folgenden Kubernetes-CLI-Befehl aus.

```
kubectl edit deployment service-name -n namespace-name
```

```
kubectl edit deployment redis-master -n guestbook
```

Die Bereitstellungsdatei des Diensts wird geöffnet.

- b Hängen Sie in der Liste der Dienstbezeichnungen die in der CSV-Datei vorgeschlagene Bezeichnung an die Bezeichnungen an, die im Abschnitt mit den Spezifikationen der Dienstbereitstellung aufgeführt sind.

3 Führen Sie die folgenden Schritte aus, um die Namespace-Bezeichnungen anzuwenden:

- a Führen Sie den folgenden Kubernetes-CLI-Befehl aus.

```
kubectl edit namespace namespace-name
```

```
kubectl edit namespace guestbook
```

Die Bereitstellungsdatei des Namespace wird geöffnet.

- b Hängen Sie in den Metadaten die in der CSV-Datei vorgeschlagene Bezeichnung an die Bezeichnungen an, die im Abschnitt `spec` der Namespace-Bereitstellung aufgeführt sind.

4 Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Bezeichnungen auf die Pods angewendet werden.

```
kubectl get pods -n namespace-name--show-labels
```

```
kubectl get pods guestbook--show-labels
```

Sehen Sie sich die Bezeichnungen in der Ergebnisansicht an.

Hinweis Bei der Anwendung auf Namespace werden die Bezeichnungen nicht auf Pods reflektiert.

- 5 Kopieren Sie zum Erstellen der Netzwerkrichtlinien die YAML-Dateien aus dem jeweiligen Cluster-Ordner in einen anderen Ordner und führen Sie einen der folgenden Befehle aus:
 - `kubectl apply -f <folder-name>/` – Alle Firewallregeln werden zusammen angewendet.
 - `kubectl apply -f <folder-name>/<firewall-rule>.yaml` – Firewallregeln werden nacheinander angewendet.

Arbeiten mit Suchabfragen

20

vRealize Network Insight bietet eine robuste Suche nach allen Einheiten in Ihrer Umgebung.

Im Folgenden finden Sie einige der Begriffe, die Ihnen bei der Suchfunktion in vRealize Network Insight helfen können:

- Einheiten: Ein Datacenter besteht aus physischen und logischen Bausteinen wie Host, virtuelle Maschine, Switch, Router, NSX Manager usw. Die Instanzen dieser Blöcke sind Einheiten.
- Eigenschaft: Eine Einheit besteht aus mehreren Eigenschaften. Eine Eigenschaft kann entweder eine Konfigurationseigenschaft oder eine Metrikeigenschaft sein.
 - a Konfigurationseigenschaft: Eine Einheit kann durch ihre Konfigurationseigenschaften beschrieben werden. Eine Konfigurationseigenschaft kann ein ganzer oder ein reeller Wert, eine Zeichenfolge oder ein boolescher Wert sein.
 - Name, CPU-Kerne und Betriebssystem für virtuelle Maschinen
 - Name und Anzahl der virtuellen Maschinen für Hosts
 - b Metrikeigenschaft: Jede Eigenschaft, die ein bestimmtes Merkmal einer Einheit misst, ist eine Metrikeigenschaft. Die Werte von Metrikeigenschaften werden in regelmäßigen Zeitintervallen erfasst. CPU-Auslastung, Arbeitsspeichernutzung und Netzwerknutzung für virtuelle Maschinen sind einige Beispiele für Metrikeigenschaften.
- Aggregationsfunktionen: Sie können in den Suchabfragen verwendet werden, um die Gesamtzahl der Instanzen eines bestimmten Einheitstyps oder einer maximalen Eigenschaft einer Einheit zu berechnen. vRealize Network Insight unterstützt die folgenden Aggregationsfunktionen.
 - a `sum`
 - b `max`
 - c `min`
 - d `avg`

Wenn Sie nach Einheiten suchen, zeigt die Software die Einheiten an, die mit Ihrer Suchabfrage auf der Seite **Ergebnisse** übereinstimmen.

Für jede Suchabfrage schlägt die Suchleiste den nächsten Begriff vor, den Sie zur Eingrenzung Ihrer Suchergebnisse verwenden können. Wenn Sie beispielsweise den Begriff **VM** eingeben, zeigt die Suchleiste eine mögliche Liste von Begriffen an, die Sie zu Ihrem vorhandenen Begriff hinzufügen können, um die Suchergebnisse einzugrenzen. Die Suchleiste validiert auch jede Suchabfrage. Ein Häkchen kennzeichnet eine gültige Suchabfrage und ein Kreuzzeichen kennzeichnet eine ungültige Suchabfrage. Auf der Seite **Hilfe** finden Sie Beispiele für aktuell unterstützte Abfragen.

Dieses Kapitel enthält die folgenden Themen:

- [Speichern und Löschen von Suchabfragen](#)
- [Suchabfragen](#)
- [Erweiterte Abfragen](#)
- [Zeitsteuerung](#)
- [Suchergebnisse](#)
- [Filter](#)
- [vCenter-Tags](#)

Speichern und Löschen von Suchabfragen

Mit vRealize Network Insight können Sie eine Suchabfrage ausführen und die Abfrage zur späteren Verwendung speichern. Darüber hinaus können Sie die gespeicherten Suchen löschen.

Hinweis

- vRealize Network Insight stellt die folgenden gespeicherten Standardsuchen bereit:
 - Alle Flows
 - Anwendungen
 - Azure
 - Kubernetes-Dashboard
 - Top-Trends
 - NSX
 - Die gespeicherten Standardsuchen können nicht gespeichert oder gelöscht werden.
 - Eine ungültige Suchabfrage kann nicht gespeichert werden.
 - Die gespeicherten Suchvorgänge sind benutzerspezifisch, und die gespeicherten Standardsuchen sind für alle Benutzer verfügbar.
-

Verfahren

- 1 Um eine Abfrage zu speichern, führen Sie eine Suche aus und klicken Sie auf das Lesezeichensymbol neben der Suchleiste.

Das Lesezeichensymbol wird in hervorgehobenem Stil dargestellt, sodass Sie sicherstellen können, dass die Abfrage gespeichert wurde. In der linken Navigationsleiste finden Sie die unter **Gespeicherte Suchvorgänge** gespeicherte Suche. Um alle gespeicherten Abfragen zu sehen, klicken Sie auf **Gespeicherte Suchvorgänge > Gespeicherte Suchvorgänge verwalten**.

- 2 Um die gespeicherte Suche zu löschen, klicken Sie erneut auf das Lesezeichensymbol und dann im Dialogfeld zum Bestätigen der Aktion auf **Löschen**.

Sie können die gespeicherte Suche auch im Fenster **Gespeicherte Suchvorgänge verwalten** löschen.

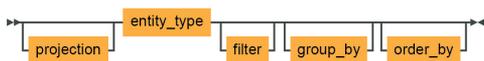
- 3 Gehen Sie zum Löschen mehrerer gespeicherte Suchabfragen zusammen wie folgt vor:
 - a Erweitern Sie die linke Navigationsleiste und klicken Sie auf **Gespeicherte Suchen > Gespeicherte Suchvorgänge verwalten**.
 - b Wählen Sie die Abfragen aus, die Sie löschen möchten.
 - c Klicken Sie auf die Option **Löschen**.
 - d Bestätigen Sie den Löschvorgang.

Suchabfragen

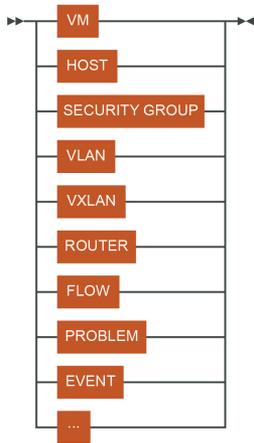
Suchabfragen können in folgende Kategorien unterteilt werden:

1 Strukturierte Abfragen

Eine strukturierte Abfrage besteht aus den folgenden Komponenten:



- **Einheitstyp:** ein Einheitstyp stellt den Objekttyp dar, den wir durchsuchen möchten. Er kann entweder in Singular- oder in Pluralform sein. Der Einheitstyp ist in einer strukturierten Abfrage obligatorisch.



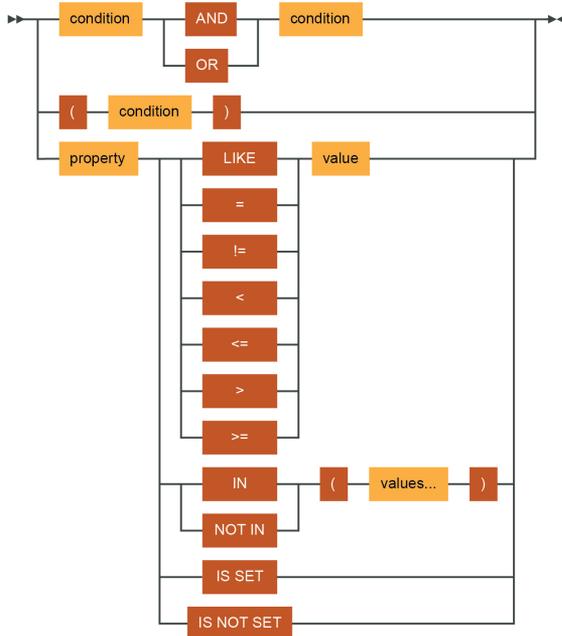
Hier sind einige Beispiele:

- 1 Virtual machines
- 2 Hosts
- 3 Flows
- 4 MTU Mismatch Events
- 5 Problems

■ **Filter:** Die Syntax für Filter lautet wie folgt:



Die Syntax für Bedingung lautet wie folgt:



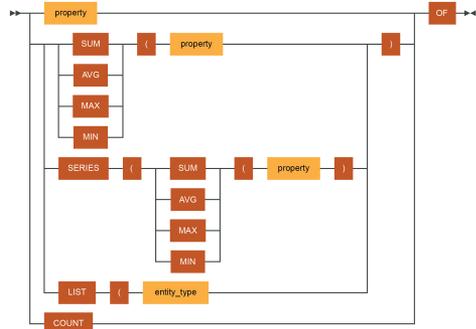
Eine Filterklausel kann zum Filtern der Suchergebnisse verwendet werden. Die Bedingung in einer Filterklausel besteht aus Eigenschaft, Vergleichsoperator und Wert. Die Bedingungen können mit logischen Operatoren kombiniert werden, um komplexe Bedingungen zu bilden. Im Folgenden finden Sie eine Liste der Operatoren, die Sie verwenden können:

Operator	Beispiele
=	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
is not set	vms where firewall rule is not set
()	flows where (src tier = 'App' and destination tier = 'DB') OR (destination tier = 'App' and source tier = 'DB')
and	flows where src tier = 'App' and destination tier = 'DB'
or	flows where flow type = 'Source is VMKNIC' or flow type = 'Destination is VMKNIC'
Übereinstimmungen	vm where name matches '.*' vm where name matches 'a.*' vm where name matches '[a-z]vm-delta[0-9]'

Operator	Beispiele
stimmt nicht überein	<pre>vm where name not matches '.*'</pre> <pre>vm where name not matches 'a.*'</pre> <pre>vm where name not matches '[a-z]vm-delta[0-9]'</pre>
geschachtelter 'in'-Operator	<pre>vm where in (vm where name = 'x')</pre> <pre>vm where in (vm of host where name = 'x')</pre> <pre>vm where host in (host of vm where name = 'x')</pre> <pre>vm where name in (name of vm where name = 'x')</pre>

- Projektionen:** Eine Projektionsklausel in einer Abfrage entscheidet, welche Felder aus den gefilterten Elementen angezeigt werden müssen. Dies ist eine optionale Bedingung. Wenn die Projektionsklausel nicht angegeben ist, wird der Standardfeldsatz in den Suchergebnissen angezeigt. Eine Projektionsklausel kann eines der folgenden Elemente enthalten:

- Eigenschaft
- Anzahl
- Liste
- Aggregation
- Serie



- Eigenschaft:** Wenn Einheiten nach Einheitstyp durchsucht werden, wird der Standardeigenschaftensatz in den Suchergebnissen angezeigt. Mithilfe von Projektionen können Sie die Felder auswählen, die in den Suchergebnissen angezeigt werden sollen. So listet `os of vms` beispielsweise alle virtuellen Maschinen mit `os property` in den Suchergebnissen auf.

Hier sind weitere Beispiele:

- `cpu cores of vms`
- `source ip address of flows`

Wenn eine Metrikeigenschaft verwendet wird, wird für jede Einheit ein Diagramm mit der Metrikeigenschaft als *y-axis* und der Zeit als *x-axis* angezeigt.

- 2 **Anzahl:** Die Abfrage „Anzahl“ kann verwendet werden, um die Anzahl der Objekte eines Einheitstyps zu berechnen. Hier sind einige Beispiele:

- `count of vms`
- `count of hosts`
- `count of flows`

- 3 **Liste:** Ein Listenoperator ist hilfreich, wenn die Filterbedingung nicht auf die Einheit angewendet werden kann, die Sie abrufen.

Beispiel:

```
List(host) of vms where memory <= 2gb
```

Diese Abfrage ruft die Liste der Hosts ab, während die Filterbedingung auf virtuelle Maschinen angewendet wird. Hier sind weitere Beispiele:

- `List(ip address) of vms where cpu cores = 1`

- 4 **Aggregationsfunktionen:** Eine Aggregationsfunktion ermöglicht es Ihnen, einen einzelnen Wert aus einer numerischen `config`- oder `metric`-Eigenschaft zu berechnen. Die Suchabfrage „Sprache“ unterstützt die folgenden Aggregationsfunktionen:

- `max`
- `sum`
- `min`
- `avg`

Hier sind einige Beispiele:

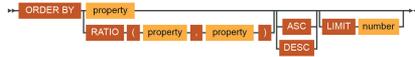
- `sum(memory) of hosts`
- `sum(memory), sum(cpu cores) of vms`
- `sum(bytes) of flows`

- 5 **Serie:** Ein Serienoperator wird zum Durchführen der Aggregation an den Metrikeigenschaften verwendet. Beispiel:

```
series(avg(cpu usage)) of vms where cpu cores = 4
```

Diese Abfrage zeigt das Diagramm mit der durchschnittlichen CPU-Auslastung aller virtuellen Maschinen mit 4 CPU-Kernen an. Hier sind einige Beispiele:

- `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`
- **Ordnen:** Die Suchergebnisse können mithilfe der `order by`-Klausel sortiert werden. In der `order by`-Klausel ist nur ein Feld zulässig. Die Ergebnisse werden standardmäßig in absteigender Reihenfolge sortiert.



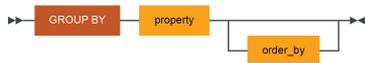
Hier sind einige Beispiele:

- 1 vms order by cpu cores
- 2 vms order by cpu cores asc
- 3 flows order by bytes

Die `limit`-Klausel kann verwendet werden, um die Anzahl der Ergebnisse zu begrenzen. Dieser muss die `order by`-Klausel vorangestellt sein. Beispiel:

```
vms order by memory limit 5
```

- **Gruppieren:** die Einheiten können nach Eigenschaft gruppiert werden. Wenn Einheiten nach einer Eigenschaft gruppiert werden, wird standardmäßig die Anzahl der Ergebnisse in jeder Gruppe angezeigt. Durch Hinzufügen einer Projektion kann `sum`/`max`/`min` jeder Eigenschaft berechnet werden. Durch das Hinzufügen der `order by`-Klausel werden die Ergebnisse sortiert. Wenn die `order by`- oder `projection`-Klausel in einer Abfrage vorhanden ist, muss die Aggregationsfunktion vorhanden sein.



```
sum(bytes) of flows group by dest vm
```

Diese Abfrage ist gültig, da die Abfrage eine Aggregationsfunktion in der Projektionsklausel aufweist. Eine Abfrage wie z. B. `bytes of flows group by dest vm` ist ungültig, da es keine Aggregationsfunktion in der Projektionsklausel gibt.

Hier sind einige Beispiele:

- 1 vms group by host
- 2 sum (bytes) of flows group by dest vm order by sum(bytes)

2 Einheitsabfragen



- a **Nach Einheitsabfrage suchen:** Alle Einheiten eines Einheitstyps können durch Durchsuchen des Einheitstyps aufgelistet werden.

Beispiele: `vms`, `hosts`, `flows`, `nsx managers`

- b **Nach Einheitsnamen suchen**

- Nach vollständigem Namen suchen: Wenn der vollständige Name einer Einheit bekannt ist, können Sie durch die Angabe des Namens in einfachen Anführungszeichen danach suchen.

Beispiele: `'prod-68-1'`, `'appl-72-1'`

- Nach teilweise Namen suchen: Eine Suche nach einem einzelnen Wort oder nach mehreren Wörtern ruft alle Elemente ab, die mit den eingegebenen Wörtern übereinstimmen.

Beispiele: `prod`, `app1`

Hinweis Wenn die Eingabe Schlüsselwörter oder Einheitstypen enthält, kann sie als Suchabfrage verarbeitet werden.

- Nach Einheitstyp und Namen suchen: Wenn der Name und der Einheitstyp bekannt sind, können Sie danach suchen, indem Sie den Einheitstyp und den Einheitsnamen zusammen abfragen.

Beispiel: Die Suchabfrage `'vm app1'` gibt alle VMs zurück, die `app1` enthalten.

3 Planungsabfragen

Diese Abfragen können verwendet werden, um mittels Flow-Analyse die Sicherheit des Datacenters zu planen.

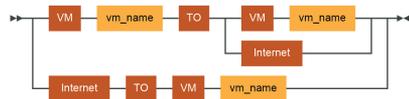


Beispiele:

- a `plan securitygroup1`
- b `plan host1`
- c `plan security`

4 Pfadabfragen

Diese Abfragen können verwendet werden, um den Pfad zwischen zwei VMs oder den Pfad von VM zu Internet anzuzeigen.



Beispiele:

- a `Vm 'vm1' to Vm 'vm2'`
- b `VM 'vm1' to Internet`

Hinweis

- Bei den Suchabfragen wird die Groß-/Kleinschreibung nicht beachtet.
 - Die Einheitstypen oder die Konfigurationseigenschaften können Synonyme aufweisen. Beispielsweise hat der Einheitstyp `'virtual machine'` das Synonym `'vm'`.
-

Azure-Suchabfragen

Sie können nach Details zu Azure-Entitäten in vRealize Network Insight suchen.

Hier sind einige Beispiele für Suchabfragen:

Azure-Entitäten	Beispielabfragen
Microsoft Azure	Azure
Azure-Anwendungssicherheitsgruppe	Azure Application Security Group where Azure Virtual Network = 'Test-vnet2'
Azure-Datenquelle	Azure Data Source
Azure NSG-Regel	Azure NSG Rule where Action = 'ALLOW'
Azure-Netzwerkschnittstelle	Azure Network Interface where Azure Virtual Network = 'Test-vnet2'
Azure-Netzwerksicherheitsgruppe	Azure Network Security Group where Subscription = 'vRNI-dev'
Azure-Route	Azure Route where Route Table = 'TestRouteTable'
Azure-Routentabelle	Azure Route Table where Azure Virtual Network = 'aks-vnet-28255566'
Azure-Subnetz	Azure Subnet where Azure Virtual Network = 'vrni-01-vnet'
Azure-Abonnement	Azure Subscription
Virtuelle Azure-Maschine	Azure Virtual Machine where Azure Application Security Group = 'TestASG'
Virtuelles Azure-Netzwerk	Azure Virtual Network where Azure Peer Virtual Network = 'vrni-01-vnet'

Cisco-ACI-Einheiten

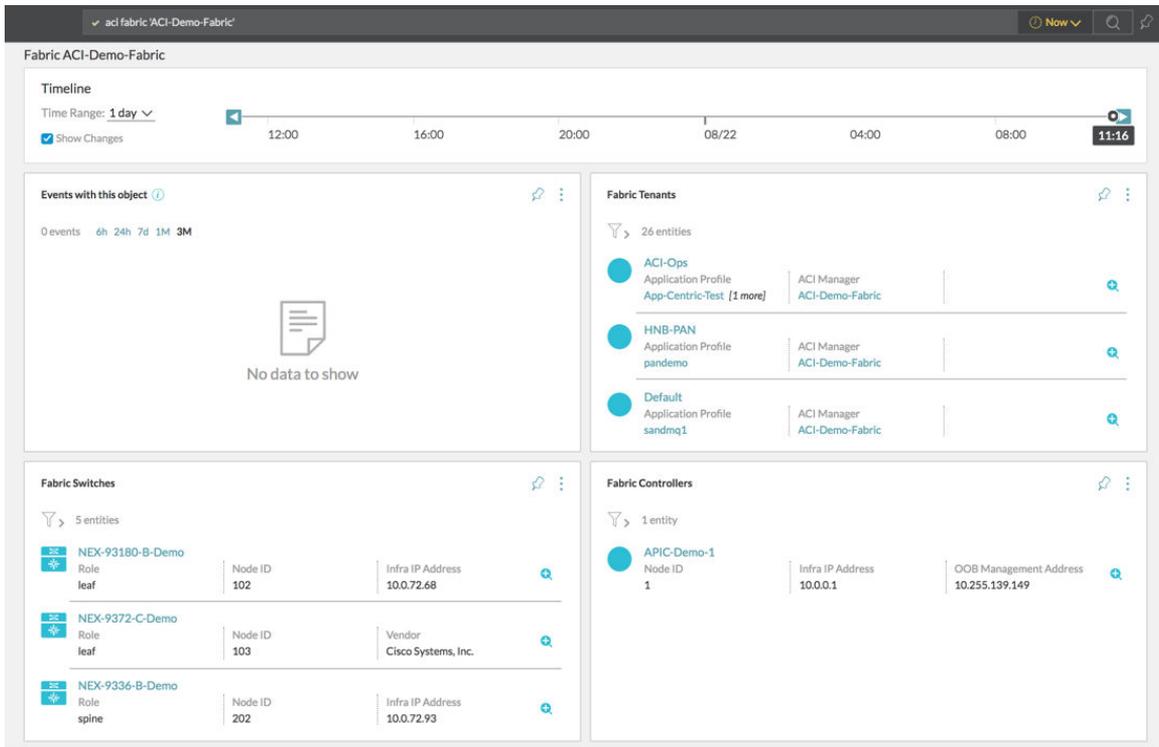
Im Folgenden finden Sie eine Liste mit einigen der Cisco-ACI-Einheiten, auf denen Sie eine Suche durchführen können:

Hinweis Den Einheiten wird das Präfix `aci` vorangestellt.

- `aci application profile`
- `aci bridge domain`
- `aci endpoint group`
- `aci fabric`
- `aci switch`
- `aci tenant`

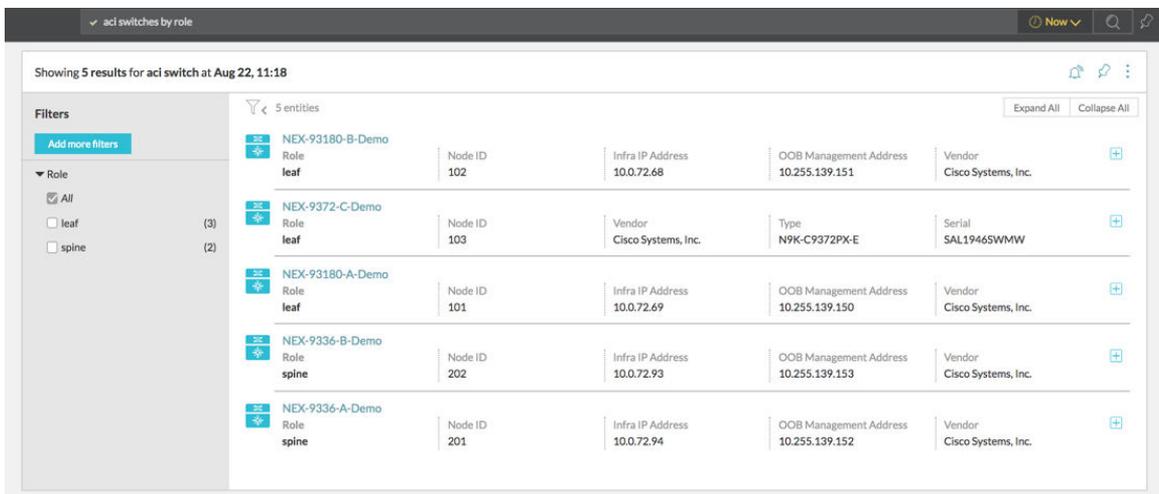
Hier sind einige Beispiele für Suchabfragen:

- `aci fabric 'ACI-Demo-Fabric'`: Diese Abfrage ruft Informationen zu den Mandanten, Switches und Controllern im ACI-Fabric ab.



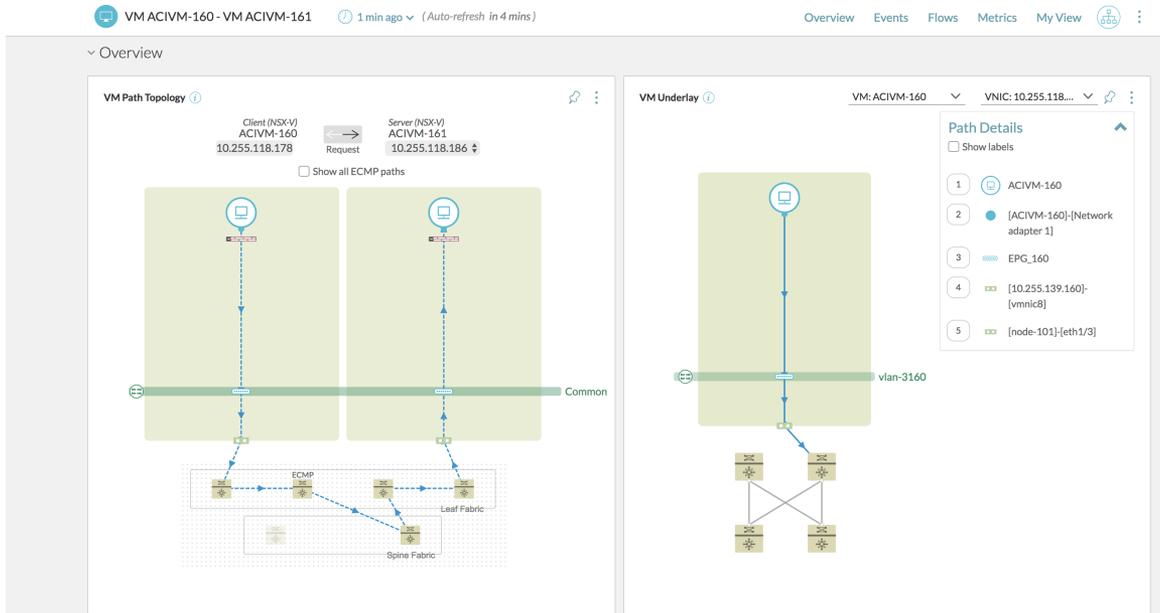
- `aci switches by role`: Diese Abfrage ruft Informationen zu den verschiedenen Leaf-Switches oder den Spine-Switches im ACI-Fabric ab.

Klicken Sie in der Switch-Liste auf einen Switch-Namen, um weitere Details dazu zu erhalten.



- `aci endpoint group`: Diese Abfrage ruft eine Liste der Endpoint-Gruppen mit den zugeordneten VMs, Bridge-Domänen und VRFs ab.

- aci application profile 'Production': Diese Abfrage ruft das Anwendungsprofil der Produktion mit den enthaltenen Endpoint-Gruppen und VMs ab.
- VMware VM 'ACIVM-160' to VMware VM 'ACIVM-161': Diese Abfrage zeigt den VM-VM-Pfad zwischen den beiden VMs an.



- Sie können mit IP-Adresse suchen, um den Port, die Endpoint-Gruppe und die Bridge-Domänendetails abzurufen.

10.114.219.158

Showing 2 results for Entities with keywords "10.114.219.158" at Mar 25, 15:10

2 entities

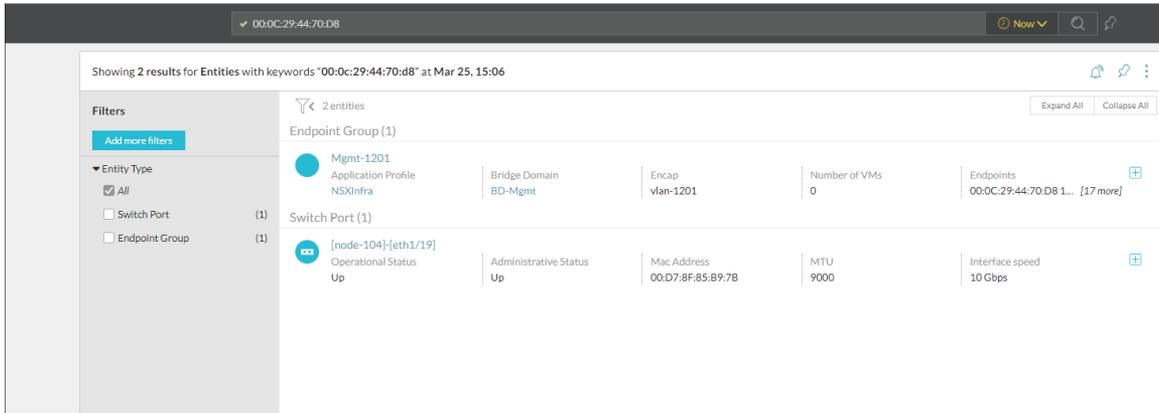
Endpoint Group (1)

Mgmt-1201	Bridge Domain BD-Mgmt	Encap vlan-1201	Number of VMs 0	Endpoints 00:0C:29:44:70:D8 10.114.21... [17 more]
-----------	--------------------------	--------------------	--------------------	---

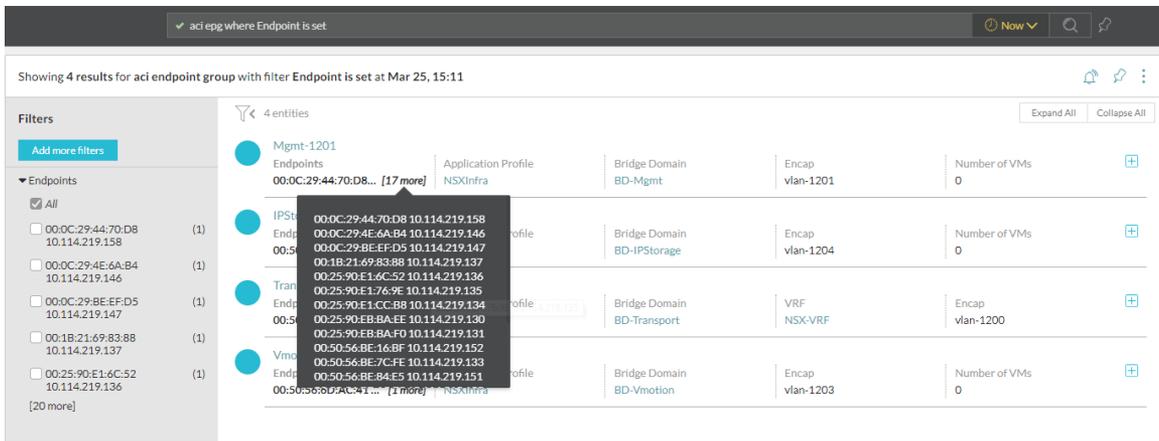
Switch Port (1)

[node-104]-[eth1/19]	Operational Status Up	Administrative Status Up	Mac Address 00:D7:8F:85:B9:7B	MTU 9000	Interface speed 10 Gbps
----------------------	--------------------------	-----------------------------	----------------------------------	-------------	----------------------------

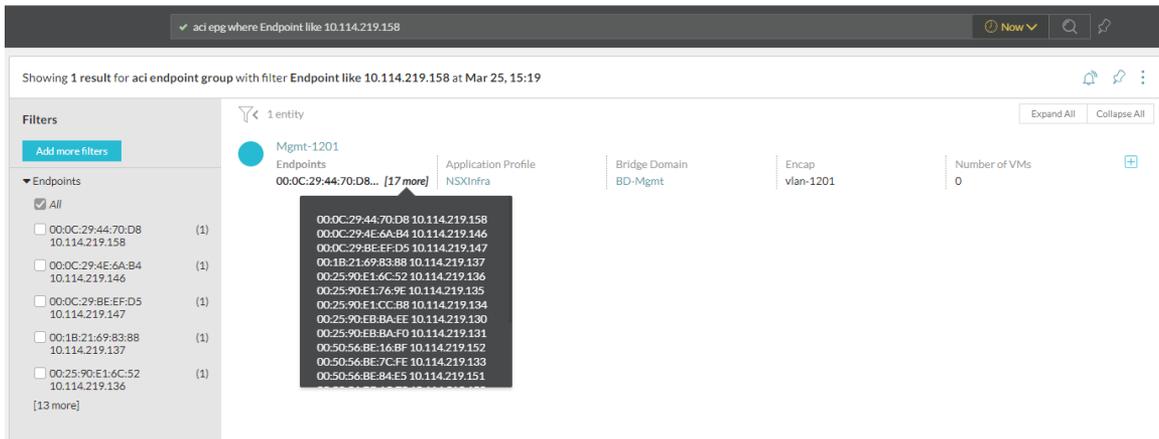
- Bei der Suche mit Mac-Adresse können Sie den Port, die Endpoint-Gruppe und die Bridge-Domänendetails abrufen.



- Sie können nach einer Endpoint-Gruppe suchen und die Liste der verknüpften Endpoints abrufen.



- Sie können nach einem Endpoint suchen.



Fortinet-Suchabfragen

Sie können Details zu Fortinet-Einheiten in vRealize Network Insight suchen.

Hier sind einige Beispiele für Suchabfragen:

Fortinet-Einheiten	Beispielabfragen
Fortinet-Richtlinienpaket	Fortinet Policy Package where Domain Manager = 'ADOM_NAME'
Fortinet-Richtlinie	Fortinet Policy where Source IP = '10.0.0.15'
Fortinet-Adresse	Fortinet Address where Address Type = 'ipmask'
Dynamische Fortinet-Adresse	Fortinet Dynamic Address where Domain Manager = 'ADOM_NAME'
Dynamische Fortinet-Adressgruppe	Fortinet Dynamic Address Group where Domain Manager = 'ADOM_NAME'
Fortinet-Dienst	Fortinet Service where port = 5900
Fortinet-Dienstgruppe	Fortinet Service Group where Manger = '10.0.15.101'
Fortinet-ADOM	Fortinet ADOM where Manager ID = '10.0.15.101'
Fortinet-VDOM	Fortinet VDOM where Domain Manager = 'ADOM_NAME'
Dynamische Fortinet-Schnittstelle	Fortinet Dynamic Interface where Domain Manager = 'ADOM_NAME'

Anreicherung von Flows mit Infoblox-DNS-Daten

vRealize Network Insight unterstützt zwei Quellen von DNS-Informationen:

- Importierte CSV-Datei
- Infoblox-DNS

Hinweis Bei einem Konflikt zwischen Infoblox-DNS und CSV-Datei hat die Information von Infoblox-DNS Vorrang.

Sie können verschiedene Suchabfragen verwenden, um mehr über die Quelle von DNS-Einträgen in einem Flow zu erfahren.

Tabelle 20-1.

Suchbegriff	Beispielsuchabfrage	Beschreibung
DNS-Anbieter	Flows where DNS Provider='Infoblox'	Stellt die Liste der Flows bereit, in denen die DNS-Daten von Infoblox abgerufen werden.
DNS-Anbieter	Flows where DNS Provider='CSV'	Stellt die Liste der Flows bereit, in denen die DNS-Daten aus CSV abgerufen werden.

Tabelle 20-1. (Fortsetzung)

Suchbegriff	Beispielsuchabfrage	Beschreibung
Quell-DNS-Quellanbieter	<code>Flows where Source DNS Provider='Infoblox'</code>	Stellt die Liste der Flows bereit, in denen der DNS-Anbieter für die Quell-IP-Adresse Infoblox ist.
Ziel-DNS-Anbieter	<code>Flows where Destination DNS provider='Infoblox'</code>	Stellt die Liste der Flows bereit, in denen der DNS-Anbieter für die Ziel-IP-Adresse Infoblox ist.

Häufige Suchabfragen für Kubernetes-Einheiten

Sie können Details zu Kubernetes-Einheiten in vRealize Network Insight suchen.

Häufige Abfragen

- Such-Flows: `flows where Kubernetes Object = Object name`
Beispiel: Flows, bei denen **Kubernetes Cluster = 'Production'**
- Anzeigen der Dienstskalierung: `kubernetes pods group by Kubernetes Services`
- Anzeigen der Knotenlast: `kubernetes Pods group by Kubernetes Node`
- Anzeigen des Knotenzustands: `MemoryPressure and PIDPressure and DiskPressure and Ready of Kubernetes Node`
- Anzeigen der Flow-Konformität: `flows from Kubernetes Object name of the object to Kubernetes Object name of the object`
Beispiel: `flows from Kubernetes Namespace 'PCI' to Kubernetes Namespace 'Non-PCI'`
- Anzeigen der Pfadtopologie:
 - Kubernetes-Dienst *Dienstname* zu Kubernetes-Dienst *Dienstname*
 - Kubernetes-Dienst *Dienstname* zu Kubernetes-Pod *Pod-Name*
 - Kubernetes-Pod *Pod-Name* zu Kubernetes-Pod *Pod-Name*

Tabelle 20-2. Abfragen zum Kubernetes-Objekt

Kubernetes-Objekt	Abfrage	Beschreibung
Namespace	<ul style="list-style-type: none"> kubernetes namespace where L2 Networks = 'a' list(Kubernetes Node) of Kubernetes Pod where Kubernetes Namespace = 'a' 	<ul style="list-style-type: none"> Gibt den Kubernetes-Namespace zurück, in dem er mit dem L2-Netzwerk „a“ verbunden ist. Gibt die Liste der Kubernetes-Knoten zurück, bei denen der Kubernetes-Namespace „a“ ist.
Pod	<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"> Gibt die Liste der mit einem Knoten verbundenen logischen Ports auf der Basis der übertragenen Pakete in absteigender Reihenfolge zurück. Gibt die Liste der mit Kubernetes-Pods verbundenen logischen Ports zurück, bei denen die Zahl verloren gegangener Rx-Pakete > 0 ist. In letzter 1 Stunde neu ermittelte Kubernetes-Pods.
Dienste	<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"> Liste der Kubernetes-Pods, die über keinen Dienst verfügen Anzahl der Pods, die auf jedem Dienst ausgeführt werden
Knoten	<ul style="list-style-type: none"> kubernetes nodes where Ready != 'True' kubernetes node where Virtual Machine = 'vm-a' 	<ul style="list-style-type: none"> Liste der fehlerhaften Kubernetes-Knoten Kubernetes-Knoten, der Teil der virtuellen Maschine „vm-a“ ist
Flows	<ul style="list-style-type: none"> flows where kubernetes service is set flows where source kubernetes node = 'a' 	<ul style="list-style-type: none"> Liste der Flows, bei denen entweder ein Quell- oder ein Ziel-Kubernetes-Dienst vorhanden ist Liste der Flows, bei denen Quell-Kubernetes-Knoten = „a“ oder Ziel-Kubernetes-Knoten = „a“

Tabelle 20-3. Zusätzliche Abfragen

Einheit/ Komponenten	Abfrage	Beschreibung
Anwendungen mit Kubernetes-Einheiten	application where virtual member = 'service-a'	Liste aller Anwendungen, bei denen der Kubernetes-Dienst „service-a“ Mitglied ist
	application where virtual member = 'service-a' and virtual member.Kubernetes Namespace = 'namespace-b'	Liste aller Anwendungen, bei denen der Kubernetes-Dienst „service-a“ und der Kubernetes-Namespace „namespace-b“ Mitglieder sind
	tier where virtual member = 'service-a' and virtual member.Kubernetes Namespace = 'namespace-b'	Liste aller Ebenen, auf denen der Kubernetes-Dienst „service-a“ und der Kubernetes-Namespace „namespace-b“ Mitglieder sind
	count of applications where Virtual Member in (kubernetes services)	Die Anzahl der Anwendungen, bei denen ein Mitglied den Typ „Kubernetes-Dienst“ aufweist

Tabelle 20-3. Zusätzliche Abfragen (Fortsetzung)

Einheit/ Komponenten	Abfrage	Beschreibung
	count of applications where virtual member in (kubernetes services where Kubernetes Namespace = 'sock-shop')	Die Anzahl der Anwendungen, bei denen ein Mitglied den Typ „Kubernetes-Dienst“ aufweist, der sich im Kubernetes-Namespace 'sock-shop' befindet
	list(virtual member) of applications where Name = 'app-1' and virtual member.Kubernetes Cluster is set	Liste aller Kubernetes-Dienste als Mitglieder für die Anwendung „app-1“
Metriken	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)	Rx-Paketverluste gruppiert nach Kubernetes-Pod
	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)	Rx-Paketverluste gruppiert nach Kubernetes-Knoten
	nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/project:' order by Rx Packet Drops	Rx-Paketverluste gruppiert nach Kubernetes-Namespace
	nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/project:<namespace name>'	Paketverluste von einem bestimmten Namespace
	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)	Paketverluste gruppiert nach Kubernetes-Diensten
	flows where firewall action = 'DROP' group by Kubernetes Service	Flow-Verluste gruppiert nach Kubernetes-Dienst
	flows where firewall action = 'DROP' group by source Kubernetes Namespace	Liste aller Flow-Verluste gruppiert nach Kubernetes-Namespace
Kubernetes-Ereignisse	Kubernetes events where Problem Entity = '<pod/namespace/node Name>'	Liste aller Kubernetes-Ereignisse für die angegebene Kubernetes-Einheit. Die Kubernetes-Einheit ist entweder ein Pod, ein Namespace oder ein Knoten.
	Kubernetes events where Event code = 'ImagePullBackOff' in last 24 hours	Liste der Kubernetes-Ereignisse des Typs „ImagePullBackOff“ in den letzten 24 Stunden
	Kubernetes events where problem entity.Kubernetes Cluster = '<cluster-a>'	Liste aller Kubernetes-Ereignisse für den angegebenen Cluster

Beispiele für Suchabfragen im Zusammenhang mit dem Lastausgleichsdienst

Anhand der folgenden Beispielabfragen können Sie die Daten in Bezug auf den Lastausgleichsdienst filtern oder durchsuchen.

- `vm where lbServiceNodes is set`: Listet alle VMs auf, die eine Anwendung hosten, wobei die Last verteilt wird.
- `vm where lbServiceNodes is set and PowerState != 'POWEREDON'`: Listet alle VMs auf, die eine Anwendung mit Lastausgleich hosten, die aber derzeit nicht funktional sind.
- `pool member where state = 'DISABLED'`: Listet alle Poolmitglieder auf, die deaktiviert sind.
- `Count of Pool Memembers where Service Port = '80'`: Gibt die Anzahl aller Poolmitglieder für einen bestimmten Diensttyp an, die auf Port 80 ausgeführt werden.
- `service node where virtual machine is not set`: Listet alle Dienstknoten auf, die den physischen Server als Anwendungsserver verwenden, oder der vCenter Server, der die VMs hostet, wird in vRealize Network Insight nicht hinzugefügt.

Suchabfragen für NSX-Firewallregeln

In vRealize Network Insight können Sie nach NSX-Firewallregeln suchen.

Tabelle 20-4. Abfragen für NSX-Firewallregeln

Suchabfrage	Beschreibung
<code>VM where incoming rules.Source Any</code>	Zeigt Regeln mit einer beliebigen Quelle an (kann mit einem bestimmten Port kombiniert werden).
<code>Firewall rule where action = allow and service any = true</code>	Zeigt Firewallregeln an, die alle Ports zulassen.
<code>Firewall Rule Masked Event</code>	Zeigt die Liste der nicht verwendeten Firewallregeln an.
<code>New firewall rules in last 24 hours</code>	Zeigt die Firewallregeln an, die in den letzten 24 Stunden erstellt wurden.
<code>New firewall rules in last 7 days</code>	Zeigt die Firewallregeln an, die in den letzten 7 Tagen erstellt wurden.
<code>New firewall rules in last 30 days</code>	Zeigt die Firewallregeln an, die in den letzten 30 Tagen erstellt wurden.
<code>Firewall rule where flow is not set</code>	Zeigt die Liste aller inaktiven Firewallregeln an.
<code>Flow group by firewall rule</code>	Zeigt die Anzahl der Flows an, die auf jede Firewallregel treffen.
<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>	Zeigt die nicht verwendete Sicherheitsgruppe an.

Tabelle 20-4. Abfragen für NSX-Firewallregeln (Fortsetzung)

Suchabfrage	Beschreibung
<code>Ipset 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>	Zeigt den IPSet an, der nicht verwendet wird.
<code>Flow where rule id in (1011, 1012, 1013)</code>	Flows, die auf eine bestimmte Regel-ID treffen.
<code>Flow where application = appl</code>	Flows, die auf die Anwendung treffen.

- Nicht verwendete Firewallregeln
- Firewallregel-Maskierungsregelereignis

VMware SD-WAN-Suchabfragen

Sie können in vRealize Network Insight nach Details zu VMware SD-WAN-Einheiten suchen.

Im Folgenden finden Sie einige Beispiele für Suchabfragen:

VMware SD-WAN-Einheiten	Beispielabfragen
VeloCloud-Cluster	<code>VeloCloud Cluster where Description = 'cluster one'</code>
VeloCloud-Datenquelle	<code>VeloCloud Data Source where Enabled = true</code>
VeloCloud Edge	<code>VeloCloud Edge where Activation State = 'Activated'</code>
VeloCloud Enterprise	<code>VeloCloud Enterprise where Name = 'VMware - vRNI'</code>
VeloCloud-Gateway	<code>VeloCloud Gateway where City = 'Ashburn'</code>
VeloCloud Layer2-Netzwerk	<code>VeloCloud Layer2 Network where Network = '172.16.40.2/24'</code>
VeloCloud-Link	<code>VeloCloud Link where Link Uptime = 100%</code>
VeloCloud-Profil	<code>VeloCloud Profile where Name = 'APProfile'</code>

VMware SD-WAN-Einheiten	Beispielabfragen
VeloCloud-Segment	<code>VeloCloud Segment where Vendor ID = '1'</code>
VeloCloud-Geschäftsrichtlinie	<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-Suchabfragen

Sie können Details zu VMC-SDDC-Einheiten in vRealize Network Insight suchen.

Im Folgenden finden Sie einige Beispiele für Suchabfragen:

VMC-SDDC-Einheiten	Beispielabfragen	Beschreibung
NSX Manager	<code>vmc sddc where NSX Manager</code>	Zeigt den NSX Manager an, der dem VMC-SDDC zugeordnet ist.
NSX Manager – FQDN	<code>vmc sddc where NSX Manager Fqdn</code>	Zeigt den NSX Manager-FQDN für das VMC-SDDC an.

VMC-SDDC-Einheiten	Beispielabfragen	Beschreibung
NSX Manager – Private IP-Adresse	<code>vmc sddc where NSX Manager Private Ip</code>	Zeigt die private IP-Adresse des NSX Manager für das VMC-SDDC an.
NSX Manager – Öffentliche IP-Adresse	<code>vmc sddc where NSX Manager Public Ip</code>	Zeigt die öffentliche IP-Adresse des NSX Manager für das VMC-SDDC an.
Name	<code>vmc sddc where Name</code>	Zeigt den Namen des VMC-SDDC an.
Organisations-ID	<code>vmc sddc where Org Id</code>	Zeigt die ID der Organisation an, zu der das SDDC gehört.
Name der Organisation	<code>vmc sddc where Org Name</code>	Zeigt den Namen der Organisation an, zu der das SDDC gehört.
Region	<code>vmc sddc where Region</code>	Zeigt die AWS-Region an, in der sich das SDDC befindet.
VC-FQDN	<code>vmc sddc where VC FQDN</code>	Zeigt den vCenter-FQDN für das VMC-SDDC an.
VC Manager	<code>vmc sddc where VC Manager</code>	Zeigt den vCenter Manager an, der dem VMC-SDDC zugeordnet ist.
Private IP-Adresse des VC	<code>vmc sddc where VC Private Ip</code>	Zeigt die private IP-Adresse des vCenter für das VMC-SDDC an.
Öffentliche IP-Adresse des VC	<code>vmc sddc where VC Public Ip</code>	Zeigt die öffentliche IP-Adresse des vCenter für das VMC-SDDC an.
Anbieter-ID	<code>vmc sddc where Vendor ID</code>	Zeigt die ID des SDDC an.

VMware Cloud on AWS für AWS-Einheiten

Einheiten im Zusammenhang mit VMware Cloud on AWS NSX Policy Manager:

- 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

Hinweis Wenn NSX-T 2.4 und VMware Cloud on AWS als Datenquellen in Ihrer vRealize Network Insight-Instanz hinzugefügt werden, müssen Sie zum Abrufen der VMware Cloud on AWS-Einheiten den Filter **SDDC type = VMC** in Ihrer Abfrage hinzufügen. Um beispielsweise die richtlinienbasierten VPNs für VMware Cloud on AWS aufzulisten, geben Sie **NSX Policy Based VPN where Tier0 = '' and SDDC Type = 'VMC'** ein.

Beispiele für Suchabfragen, die sich auf die VMware Cloud on AWS-Einheiten beziehen:

- `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 = ''`

Hinweis

- NSX Policy Manager unterstützt keine untergeordneten Gruppen oder IPSETS. Daher sind alle Suchvorgänge wie `NSX Policy firewall rule where Indirect _____ = ''` oder `NSX Policy group where Indirect _____ = ''` deaktiviert.
-

Erweiterte Abfragen

Im Folgenden finden Sie einige Beispiele für erweiterte Abfragen:

Flow-Abfragen für Kommunikationsmuster

- Gesamtdatenverkehr zwischen Datacentern oder Sites (DCI-Link-Nutzung)


```
sum(bytes) of flows where ( Dst Manager = 'abc' AND src manager = 'cba') OR ( Dst Manager = 'cba' AND src manager = 'abc')
```
- Gesamter VTEP-Datenverkehr
 - `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`
- Sonstiger Management-Datenverkehr


```
flows where Flow Type = 'Source is VMKNIC' or Flow Type = 'Destination is VMKNIC'
```

Flow-Abfragen für Aggregation und Gruppierung

- Gesamter Internet Datenverkehr nach Quell-VM


```
sum(bytes) of flows where Flow Type = 'Internet' group by src vm
```
- Top-Ports nach Gesamtbyte


```
sum(bytes) of flow group by port order by sum(bytes)
```

- Top-Subnetz-Paare nach geroutetem Datenverkehrsvolumen

```
sum(bytes) of flow where Flow Type = 'Routed' group by Source Subnet Network,  
destination subnet network order by sum(bytes)
```

- VM insgesamt nach Gesamtpaar-Byte

```
sum(bytes) of flows group by src vm , dest vm order by sum(bytes)
```

- Top-Server-VM/Port nach Gesamtbyte

```
sum(bytes) of flows group by dest vm , port order by sum(bytes)
```

Flow-Abfragen zur Kapazitätsschätzung und Größenanpassung

- Gesamtzahl der Bytes des gesamten vm-internet/internet-vm-Datenverkehrs, gruppiert nach ESX (Palo Alto Service-VM-Dimensionierung)

```
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)
```

- Aggregierte Datenverkehrsserie für übereinstimmende Flows (Palo Alto-Dienst-VM-Dimensionierung)

```
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')
```

Nützliche Abfragen für die Anwendung

- VMs in einer bestimmten Anwendung

```
VM where application = 'CRM'
```

- Geroutete Flows aus einer bestimmten Anwendung

```
Flows where source application = CRM and Flow Type = 'Routed'
```

- Flows zwischen zwei Ebenen (unidirektional)

```
Flows where src tier = 'App' and Destination Tier = 'DB'
```

- Flows zwischen zwei Ebenen (unidirektional)

```
Flows where ( src tier = 'App' and destination Tier = 'DB') OR (destination tier =  
'App' and source tier = 'DB')
```

Hilfreiche Abfragen für VM und ESX

- Eigenschaften von Prod-Midtier-1-VM (MAC, IP, Host usw.)

```
CPU Usage Rate, Network Rate, Memory Usage Rate, mac address, ip , vxlan , host of  
vm 'Quality control-VM26'
```

- Netzwerksegmente mit der höchsten VM-Anzahl

```
vm group by l2 network
```

- Datenspeicher mit der höchsten VM-Anzahl

```
vm group by datastore
```

- Hosts nach vSphere-Version

```
host group by version
```

- Hosts nach vSphere-Builds

```
host group by OS
```

- Alle VMs auf allen Hosts/Blades in einem bestimmten UCS-Chassis (geschachtelte Abfrage)

```
vm where host in (host where Blade like 'sys/chassis-1')
```

Nützliche Abfragen: Allgemeine Kapazität

- Anzahl der Datacenter:

```
count of datacenter
```

- Anzahl der Cluster

```
count of cluster
```

- Anzahl der Hosts

```
count of host
```

- Anzahl der VMs

```
count of vm
```

- Anzahl der Netzwerke

```
count of vlan
```

Nützliche Abfragen: Routen

- VNIs nach primärem Controller

```
vxlان group by Primary Controller
```

- Routen für Provider Edge 3

```
routes where vrf = 'Provider Edge 3'
```

- Routen von DMZ DLR

```
NextHop Router of routes where VRF = 'LDR-DMZ'
```

- Routen mit dem angegebenen Router als nächster Hop

```
routes where NextHop Router = 'California-Edge'
```

Hilfreiche Abfragen: Firewallregeln

- Firewallregeln zwischen zwei VMs

```
firewall rules from 'Prod-MidTier-1' to 'Prod-Db-1'
```

- Regeln mit der Quelle „ANY“

```
firewall rules where Service Any = true
```

- VMs für eine bestimmte Regel

```
vm where Firewall Rule = 'Prod MidTier to Prod DB - DBService '
```

- Firewallregeln, bei denen ein beliebiger Port zulässig ist

```
firewall rule where action = allow and service any = true
```

- Flows, die auf eine bestimmte Firewallregel treffen

```
flows where firewall rule = 'Admin to Prod and Lab - SSH'
```

- Zurückgewiesene Flows im System

```
flows where firewall action = deny
```

- Gateway-Firewall anzeigen

```
Firewall Rule where firewall type = 'GatewayFirewall'
```

- Verteilte Firewall anzeigen

```
Firewall Rule where firewall type = 'Distributed Firewall'
```

Nützliche Abfragen: Allgemeine Datenverkehrsmuster

- Menge des Ost-West- und Nord-Süd-Datenverkehrs, Menge des umgeschalteten Datenverkehrs, Menge des gerouteten Datenverkehrs und Menge des VM-zu-VM-Datenverkehrs

```
plan security in last 7 days
```

Nützliche Abfragen: Datenverkehr von einer Überwachungskamera

- Details zu VMs, die die meiste Bandbreite verbrauchen

```
top 7 vm group by name, Vlan order by sum(Total Network Traffic) in last 7 days
```

- Netzwerke, die den meisten Datenverkehr transportieren

```
top 7 vlan group by Vlan id, vm count order by sum(Total Network Traffic) in last 7 days
```

- Netzwerke, bei denen der Großteil der Kommunikation innerhalb des VLAN liegt (ohne eine physische Firewall oder L3-Grenze zu überschreiten)

```
top 7 flow where Flow Type = 'Switched' group by Subnet Network order by sum(Bytes) in last 7 days
```

- Netzwerke, bei denen der Großteil der Kommunikation über VLAN hinweg erfolgt (was zu Engpässen bei der physischen Firewall führen kann)

```
top 7 flow where Flow Type = 'Routed' group by Source Subnet Network, Destination Subnet Network order by sum(Bytes) in last 7 days
```

- VMs, die außerhalb des Landes kommunizieren

```
top 7 flow where Destination Country != 'United States' group by Source VM, Destination Country order by sum(Bytes) in last 7 days
```

- Datenspeicher mit den meisten Speicherlatenzen

```
avg(Read Latency), avg(Write Latency) of top 7 vm group by Datastore, vlan order by avg(Write Latency) in last 7 days
```

Nützliche Abfragen: Konformität/Schwachstellen

- Details zu anfälligen Betriebssystemen

```
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
```

- Anzahl der anfälligen Betriebssysteme

```
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'
```

- Gesamte Angriffsfläche aufgrund alter Betriebssysteme

```
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'))
```

Hinweis Informationen zum Abrufen der empfohlenen Firewallregel für das anfällige Betriebssystem finden Sie unter [Empfohlene Firewallregel zum Schutz gefährdeter Betriebssysteme](#).

Zeitsteuerung

Mit der Zeitsteuerung können Sie eine Suchabfrage im Kontext eines ausgewählten Zeitraums oder Zeitbereichs ausführen. Sie können aus einer Liste von Voreinstellungen auswählen, wie z. B. die letzten 24 Stunden, die letzten 3 Tage usw. Sie können auch ein bestimmtes Datum und eine Uhrzeit mit der Option **Um** oder sogar einen Bereich mit der Option **Zwischen** angeben.

Suchergebnisse

Auf der Seite „Suchergebnisse“ finden Sie eine detaillierte Liste der betroffenen Einheiten, die mit einer bestimmten Suche übereinstimmen. Die Seite selbst bietet zahlreiche Informationen, die von der Liste der Einheiten, ihren entsprechenden Eigenschaften und Facets reicht, damit Sie die Suchergebnisse zwecks Verfeinerung Ihrer Suche filtern können.

Sie können auch jeden Eintrag in den Suchergebnissen erweitern oder reduzieren, um weitere Informationen zu einem bestimmten Eintrag anzuzeigen. Sie können auch eine Benachrichtigung für jede Suche erstellen.

Hinweis Sie können auf eine bestimmte Eigenschaft in den Suchergebnissen und auch auf den Einheitsseiten verweisen, um eine QuickInfo mit weiteren Informationen zu dieser Eigenschaft anzuzeigen.

Die folgende Abbildung zeigt die Suchergebnisse für die VXLANs an, wobei `num vms > 0` eine Suchabfrage für eine Zeit in der Vergangenheit ist.

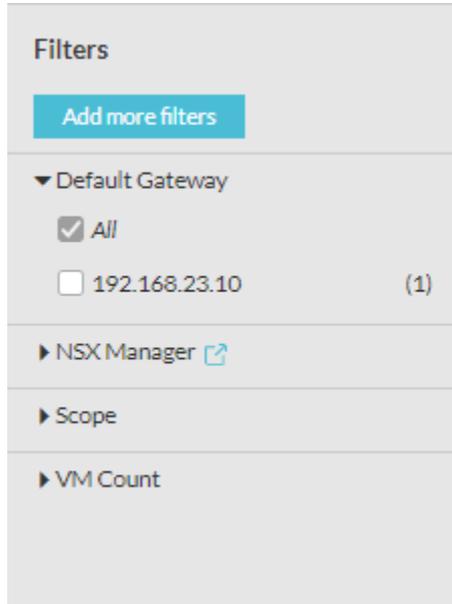
Showing 12 results for Vxlan with filter Num VMs > 0 at

Filters

- Add more filters
- VM Count
 - All
 - 1 (5)
 - 2 (5)
 - 3 (2)
- NSX Manager
- Scope

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

Filter



Nachdem Sie die Suchergebnisse abgerufen haben, klicken Sie gemäß Ihren Anforderungen im linken Fensterbereich auf „Weitere Filter hinzufügen“. Sie können eine Reihe von Filterkategorien anzeigen, die Sie verwenden können, um die Suchergebnisse einzugrenzen. Die Anzahl der verfügbaren Filter für jede Kategorie wird in einem kleinen Feld neben der Kategorie angegeben. Zeigen Sie die verfügbaren Filter für diese Kategorie an (zusammen mit einer kurzen Erläuterung für jeden Filter) und klicken Sie, um diesen Filter anzuwenden. Sie können auch das Suchfeld „Filter“ verwenden, um nach einem bestimmten Filter zu suchen. vRealize Network Insight zeigt automatisch die Filter an, die mit Ihrer Suchabfrage übereinstimmen, und Sie können klicken, um diesen Filter anzuwenden. Jeder Filter verfügt über mehrere Eigenschaften, um die Suchergebnisse zu verfeinern. Wenn Sie eine Filtereigenschaft aus einem der Filter auswählen, wird die ausgewählte Eigenschaft in den Suchergebnissen hervorgehoben.

vCenter-Tags

vRealize Network Insight stellt vCenter-Tags für Suche und Planung bereit.

Sie können VMs basierend auf den vCenter-Tags und benutzerdefinierten Attributen durchsuchen. Sie können z. B. die folgende Suchabfrage verwenden, indem Sie Tags verwenden:

```
vm where tag = '{keyname}:{value}'
```

Jedes Tag gehört einer Kategorie an. Im obigen Beispiel ist der Tastenname die Kategorie, zu der das Tag gehört, und der Wert ist der Name des Tags.

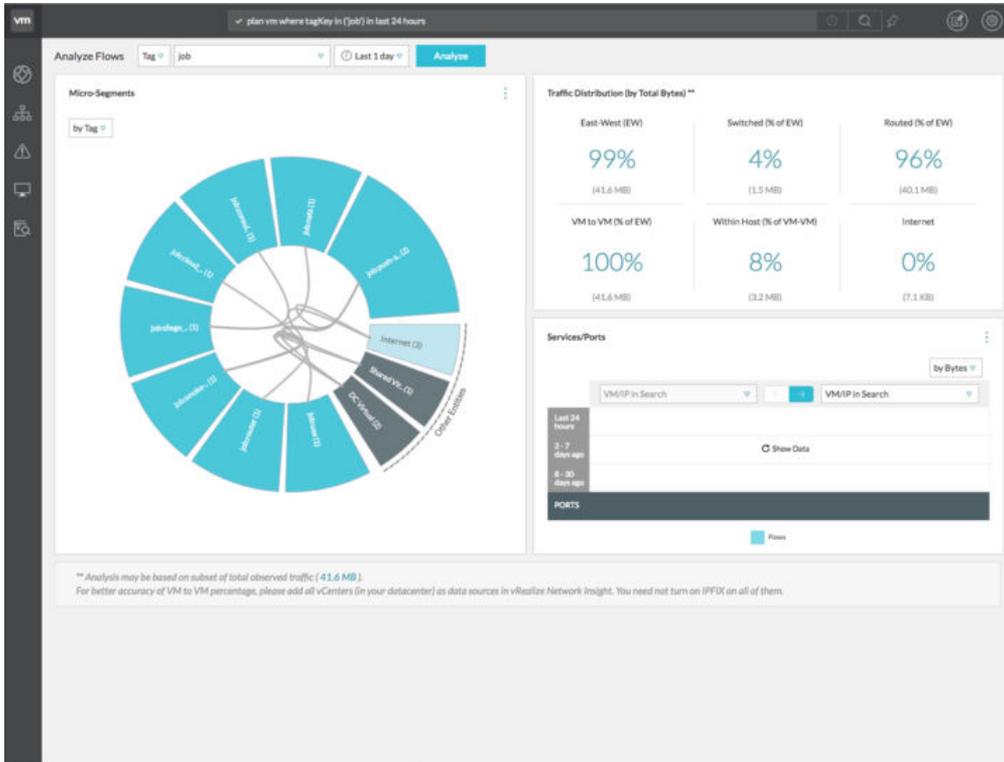
Sie können auch einen alternativen Namen für eine VM angeben, indem Sie vCenter-Tags oder benutzerdefinierte Attribute verwenden, indem Sie die `name`-Taste verwenden. Dieser alternative Name wird als `other names`-Eigenschaft angezeigt. Es ist auch möglich, mithilfe des alternativen Namens nach Pfadabfragen zu suchen und diese zu erstellen.

Die folgenden Abfragen werden unterstützt:

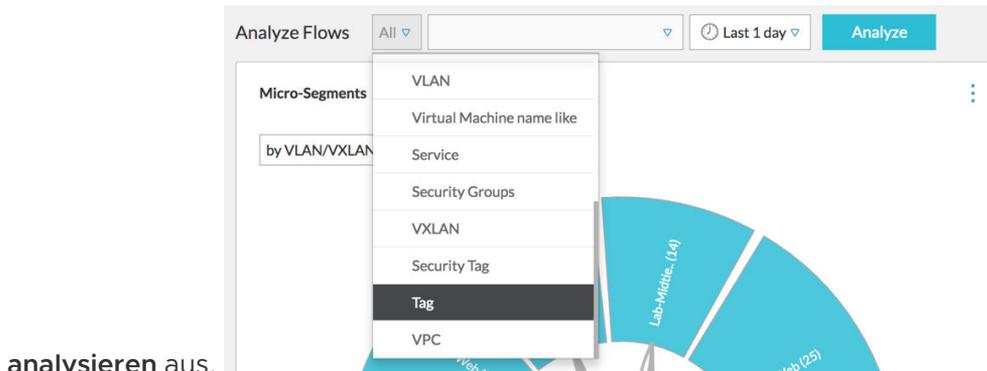
```
vm "other-name-1"  
  vm "other-name-1" to vm "other-name-2"
```

In diesem Beispiel sind `other-name-1` und `other-name-2` benutzerdefinierte Attribute mit dem `name`-Schlüssel oder den Tags, die zur Kategorie `name` gehören.

Sie können auch die Flows im Netzwerk analysieren, indem Sie die vCenter-Tags verwenden, wie in der Abbildung dargestellt.

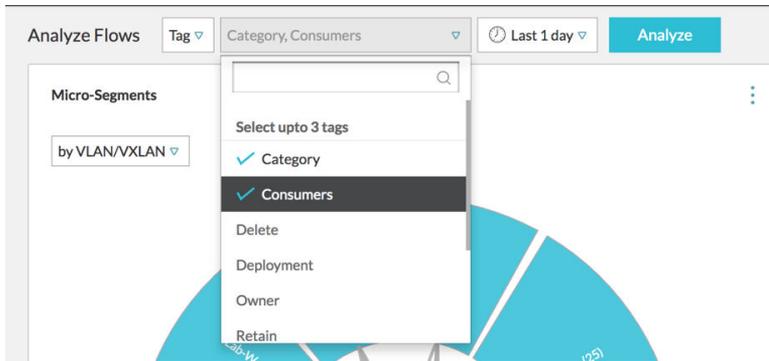


Um die vCenter-Tags zu verwenden, wählen Sie die Option **Tag** aus der Dropdown-Liste **Flows**

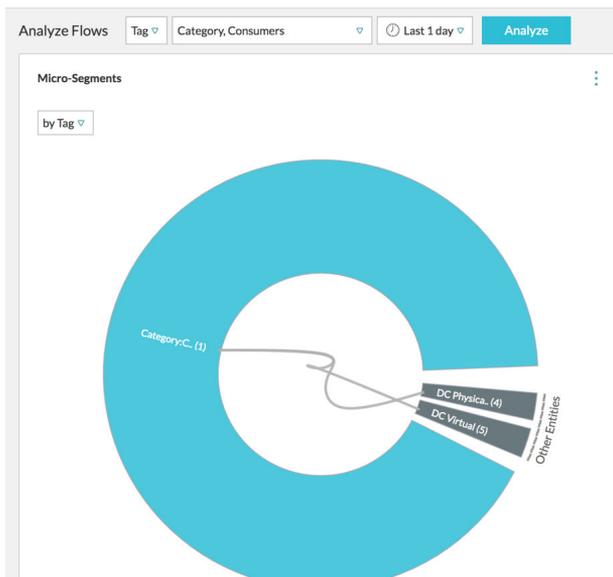


analysieren aus.

Sie können auch bis zu drei Tags auf dieser Ebene auswählen. Nachdem Sie das Tag ausgewählt haben, klicken Sie auf **Analysieren**.



In **Nach Kriterien gruppieren** ist **Tag** ausgewählt.



Planen der Notfallwiederherstellung für vRealize Network Insight

21

VMware Site Recovery Manager (SRM) ist eine Automatisierungssoftware für die Notfallwiederherstellung, die richtlinienbasierte Verwaltung, unterbrechungsfreie Tests und automatisierte Orchestrierungen bereitstellt. vRealize Network Insight unterstützt SRM 8.1 und die weiteren Versionen. Zum Schutz Ihrer vRealize Network Insight-Instanz automatisiert SRM jeden Aspekt der Ausführung eines Notfallwiederherstellungsplans, um die Wiederherstellung zu beschleunigen und die Risiken bei der Verwendung eines manuellen Prozesses zu beseitigen.

Informationen zum Installieren, Aktualisieren und Konfigurieren von SRM finden Sie in der [Dokumentation zu VMware Site Recovery Manager](#).

Voraussetzungen für den Notfallwiederherstellungsvorgang für vRealize Network Insight:

- Vergewissern Sie sich, dass vSphere Replication installiert und konfiguriert ist.
- SRM sollte sowohl auf der geschützten als auch auf der Wiederherstellungs-Site bereitgestellt und konfiguriert sein.
- Vergewissern Sie sich, dass die Site-Kopplung korrekt in der SRM-Benutzeroberfläche konfiguriert wurde, bevor Sie den Notfallwiederherstellungsplan und weitere Komponenten erstellen.
- VMware vSphere Replication sollte für jeden der geschützten Knoten der vRNI-Einrichtung im Kontext aktiviert werden. Geben Sie bei der Aktivierung von VMware vSphere Replication ein ausreichendes RPO an. Berücksichtigen Sie dabei die Größe und Nutzung der vRealize Network Insight-Knoten, sodass bei einem Notfall nur ein minimaler Datenverlust zu erwarten ist. Weitere Informationen zur Replizierung finden Sie in der [Dokumentation zu VMware vSphere Replication](#).
- Sie müssen eine gesonderte Schutzgruppe für vRealize Network Insight erstellen. Achten Sie bei kleinen und nicht verteilten Bereitstellungen darauf, dass sich alle VMs in derselben Schutzgruppe befinden. Für verteilte Bereitstellungen wird empfohlen, dass Sie alle Plattformen in einer einzigen Schutzgruppe platzieren, damit sie leicht wiederhergestellt werden können. Sie können die Collectors in verschiedenen Schutzgruppen platzieren.

- Erstellen Sie einen Wiederherstellungsplan und fügen Sie die Schutzgruppen mit den vRealize Network Insight VMs zu diesem Plan hinzu. Achten Sie darauf, dass die Schutzgruppe, die die Plattformknoten enthält, die höhere Rangfolge erhält. Stellen Sie im Wiederherstellungsplan sicher, dass der primäre Plattformknoten in eine Gruppe mit höherer Priorität gestellt wird als die anderen Plattformknoten.
- Derzeit werden alle Arten von IPv4-Anpassungen mit SRM nicht unterstützt.

Es wird empfohlen, dass Sie vRealize Network Insight-VMs auf eine identische Netzwerkkonfiguration migrieren bzw. wiederherstellen. Außerdem können Sie gemäß der SRM-Empfehlung regelmäßig einen Testlauf durchführen, um sicherzustellen, dass der vorhandene Plan mit der zugrunde liegenden Infrastruktur und dem konfigurierten RPO-Grenzwert funktioniert.

- Migrieren Sie vRealize Network Insight-VMs auf eine identische Netzwerkkonfiguration bzw. stellen Sie sie mit einer identischen Netzwerkkonfiguration wieder her.

Wenn die Wiederherstellungs-Site so konfiguriert ist, dass sie dieselbe Netzwerkkonfiguration hat wie die Schutz-Site, und eine Zuordnung zwischen den identischen Netzwerken erstellt wird, konfigurieren Sie alle replizierten vRealize Network Insight-VMs so, dass sie mit denselben IPs gestartet werden, da diese VMs die geschützten Knoten sind. Das wiederhergestellte System wird in Betrieb genommen, nachdem die geplante Migration oder die Notfallwiederherstellung erfolgreich abgeschlossen wurde.

- Geben Sie keine IP-Anpassung für einen Wiederherstellungsplan an, wenn die Wiederherstellungs-Site nicht über dasselbe Netzwerk wie die Schutz-Site verfügt. In diesem Szenario wird SRM für die Wiederherstellung der Appliance-VMs verwendet. Weisen Sie für die Konfigurierung des Netzwerks nach der Wiederherstellung manuell die folgenden Netzwerkeinstellungen zu:
 - 1 Führen Sie den Befehl `change-network-settings` gleichzeitig auf allen Plattformknoten aus.
 - 2 Führen Sie den Befehl `update-IP-change` auf den Knoten auf Plattform1, Plattform2 und Plattform3 nacheinander aus.
 - 3 Führen Sie `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Plattform1>` auf dem Collector-Knoten aus.
 - 4 Überprüfen Sie den Dienststatus. Wenn einige der Dienste auf den Plattformknoten nicht ausgeführt werden, starten Sie die Knoten in der empfohlenen Reihenfolge neu.

Hinweis Weitere Informationen über die oben genannten Befehle finden Sie im *Referenzhandbuch zur vRealize Network Insight-Befehlszeile*.

Dieses Kapitel enthält die folgenden Themen:

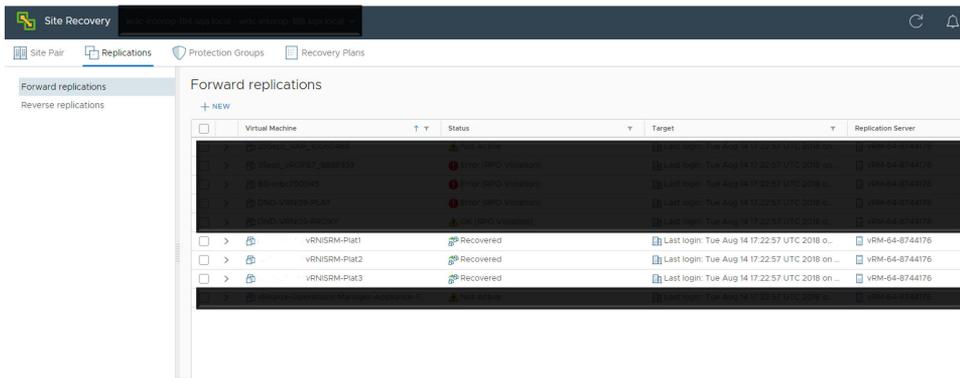
- [Beispiel für ein Notfallwiederherstellungsszenario](#)

Beispiel für ein Notfallwiederherstellungsszenario

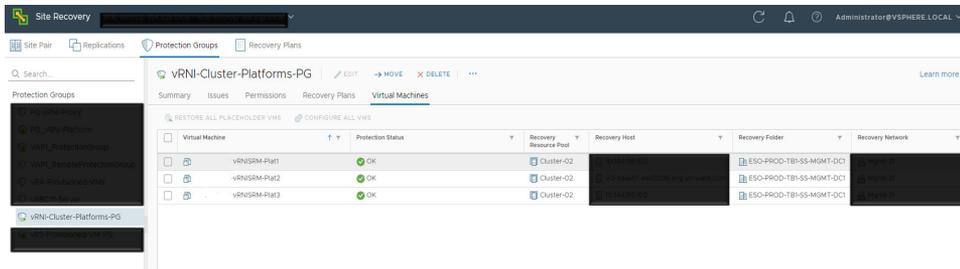
Nachfolgend sehen Sie die Schritte für ein Beispielszenario für die Notfallwiederherstellung (Disaster Recovery, DR) von vRealize Network Insight:

Verfahren

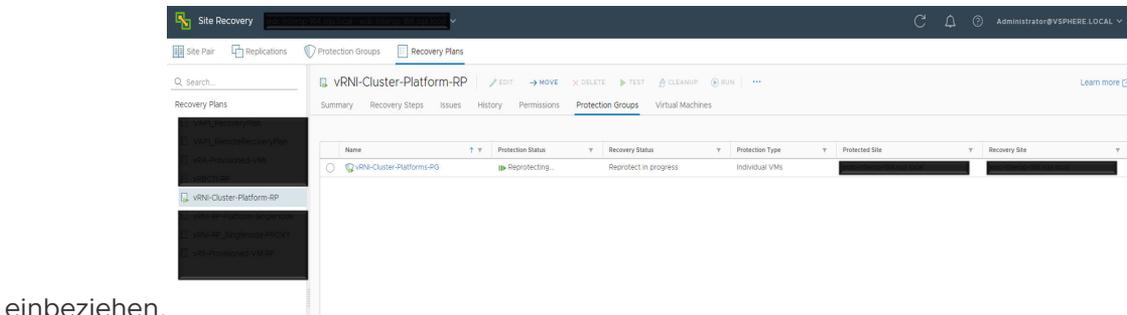
- 1 Stellen Sie sicher, dass SRM sowohl auf der Schutz- als auch auf der Wiederherstellungs-Site konfiguriert und in Betrieb ist.
- 2 Konfigurieren Sie die Replizierung für jeden der vRealize Network Insight-Knoten, die geschützt werden sollen. Geben Sie beim Konfigurieren der Replizierung eine angemessene RPO-Zeit (Recovery Point Objectives) für die vRealize Network Insight-Instanz an. Wenn es sich beispielsweise um eine vRealize Network Insight-Bereitstellung mit einer einzelnen Plattform und Collector-Knoten (mittlere Größe) handelt, ist ein RPO von 45 Minuten gut. Wenn es sich jedoch um einen Cluster mit großen Knoten handelt, sollte ein entsprechend größeres RPO angegeben werden. Die Konfiguration des Snapshot-Intervalls bezieht sich speziell auf die Umgebung und die Anforderungen des Benutzers.



- 3 Erstellen Sie eine Schutzgruppe. Schließen Sie die VMs, die Sie schützen möchten, unter einer bestimmten Schutzgruppe ein.



- 4 Erstellen Sie den Wiederherstellungsplan, in den Sie die entsprechenden Schutzgruppen



einbeziehen.

- 5 Führen Sie eine Testwiederherstellung durch. Dadurch wird sichergestellt, dass Ihr Wiederherstellungsplan wie erwartet funktioniert.
- 6 SRM empfiehlt, dass Benutzer in regelmäßigen Abständen eine geplante Migration durchführen, um die Integrität des vorhandenen DR-Plans zu validieren.
- 7 Angenommen, die Wiederherstellungs-Site verfügt über eine Netzwerkkonfiguration, die erzwingt, dass die vRealize Network Insight-VMs mit den neuen IPs bereitgestellt werden. Stellen Sie die vRealize Network Insight-VMs mit einem Wiederherstellungsplan wieder her, der keine Netzwerkkänderung für die wiederhergestellten VMs annimmt. Sobald die Wiederherstellung der VMs in vRealize Network Insight als erfolgreich gemeldet wurde, weisen Sie den vRealize Network Insight-Knoten manuell neue IP-Adressen zu, wenden Sie neue Zertifikate an und initialisieren Sie den Cluster neu.
- 8 Da die IPv4-Anpassung mit SRM derzeit nicht unterstützt wird, können Sie DR als Umgehung mit vRealize Network Insight durchführen, so als ob es keine Netzwerkkänderung gäbe.

So weisen Sie die Netzwerkeinstellungen manuell zu:

- a Führen Sie den Befehl `change-network-settings` gleichzeitig auf allen Plattformknoten aus.
- b Führen Sie den Befehl `update-IP-change` auf den Knoten auf Platform1, Platform2 und Platform3 nacheinander aus.
- c Führen Sie `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Platform1>` auf dem Collector-Knoten aus.
- d Überprüfen Sie den Dienststatus. Wenn einige der Dienste auf den Plattformknoten nicht ausgeführt werden, starten Sie die Knoten in der empfohlenen Reihenfolge neu.

Dieses Kapitel enthält die folgenden Themen:

- Häufige Datenquellenfehler
- Aktivierung von DFW-IPFIX nicht möglich

Häufige Datenquellenfehler

Wenn Sie eine Datenquelle hinzufügen, können Sie auf mehrere Fehler stoßen. Diese Tabelle enthält eine Liste häufiger Fehler nebst Ursache und Lösung für jeden Fehler.

Tabelle 22-1.

Fehlertext	Ursache	Lösung
Ungültige Antwort von Datenquelle	Proxy von vRealize Network Insight konnte die von der Datenquelle empfangenen Informationen nicht verarbeiten, da die Informationen nicht das erwartete Format aufweisen.	Bei einigen Datenanbietern wird dieses Problem zeitweise beobachtet und tritt möglicherweise beim nächsten Abrufvorgang nicht mehr auf. Falls es regelmäßig auftritt, wenden Sie sich an den Support.
Datenquelle ist von der Proxy-VM aus nicht erreichbar.	Die IP-Adresse der Datenquelle auf SSH/REST (Port 22 oder 443) kann entweder nicht von der Proxy-VM von vRealize Network Insight erreicht werden, oder die Datenquelle antwortet nicht. Dieser Fehler tritt beim Hinzufügen der Datenquelle auf.	Überprüfen Sie die Konnektivität der Proxy-VM von vRealize Network Insight mit der Datenquelle auf Port 22 oder 443. Stellen Sie sicher, dass die Datenquelle aktiviert ist und dass die Firewall die Verbindung der Proxy-VM von vRealize Network Insight zur Datenquelle nicht blockiert.
Kein NSX Controller gefunden	Auf der Seite „Datenquelle für NSX Manager“ wurde ein NSX Controller ausgewählt, aber es ist kein NSX Controller installiert.	Installieren Sie einen NSX Controller auf NSX Manager und aktivieren Sie dann das Kontrollkästchen NSX Controller auf der Seite „Datenquelle für NSX Manager“.

Tabelle 22-1. (Fortsetzung)

Fehlertext	Ursache	Lösung
Nichtübereinstimmung bei Datenquellentyp oder -Version	Die angegebene IP-Adresse/der FQDN der Datenquelle entspricht nicht dem ausgewählten Datenquellentyp.	Stellen Sie sicher, dass die angegebene IP-Adresse/der FQDN der Datenquelle dem ausgewählten Datenquellentyp entspricht und die Version von vRealize Network Insight unterstützt wird.
Fehler bei der Verbindung zur Datenquelle	Proxy-VM von vRealize Network Insight kann keine Verbindung zur Datenquelle herstellen. Dieser Fehler tritt nach dem Hinzufügen der Datenquelle auf.	Überprüfen Sie die Konnektivität der Proxy-VM von vRealize Network Insight mit der Datenquelle auf Port 22 oder 443. Stellen Sie sicher, dass die Datenquelle aktiviert ist und dass die Firewall die Verbindung der Proxy-VM von vRealize Network Insight zur Datenquelle nicht blockiert.
Nicht gefunden	Proxy VM von vRealize Network Insight wurde nicht gefunden.	Überprüfen Sie, ob die Paarbildung zwischen der Proxy-VM von vRealize Network Insight und der Plattform-VM von vRealize Network Insight zustande kommt.
Unzureichende Rechte zum Aktivieren von IPFIX	Der Benutzer, der versucht, IPFIX in vCenter zu aktivieren, verfügt nicht über die folgenden Rechte: DVSwitch.Modify; DVPortgroup.Modify.	Geben Sie dem Benutzer die entsprechenden Rechte.
IP/FQDN ist ungültig	Die auf der Seite „Datenquelle“ angegebene IP/FQDN ist ungültig oder nicht vorhanden.	Geben Sie eine gültige IP/FQDN-Adresse an.
Es werden keine Daten empfangen.	Plattform-VM von vRealize Network Insight empfängt keine Daten von der Proxy-VM von vRealize Network Insight für diese Datenquelle.	Supportkontakt.
Ungültige Anmeldedaten	Die angegebenen Anmeldedaten sind ungültig.	Geben Sie die korrekten Anmeldedaten ein.
Verbindungszeichenfolge ist ungültig.	Die/der auf der Seite „Datenquelle“ angegebene IP/FQDN hat nicht das richtige Format.	Geben Sie eine gültige IP/FQDN-Adresse an.
Aktuelle Daten sind aufgrund einer Verarbeitungsverzögerung möglicherweise nicht verfügbar.	Plattform-VM von vRealize Network Insight ist überlastet und es kommt zu Verzögerungen bei der Verarbeitung von Daten .	Supportkontakt.
Zeitüberschreitung bei Anforderung, bitte versuchen Sie es erneut.	Die Anforderung konnte nicht in der festgelegten Zeit abgeschlossen werden.	Versuchen Sie es erneut. Wenn das Problem nicht behoben ist, wenden Sie sich an den Support.

Tabelle 22-1. (Fortsetzung)

Fehlertext	Ursache	Lösung
Aus unbekanntem Grund fehlgeschlagen, versuchen Sie es erneut oder wenden Sie sich an den Support.	Die Anforderung ist aus einem unbekanntem Grund fehlgeschlagen.	Versuchen Sie es erneut. Wenn das Problem nicht behoben ist, wenden Sie sich an den Support.
Die Kennwortauthentifizierung für SSH muss auf dem Gerät aktiviert sein.	SSH-Anmeldung mit Kennwort ist auf dem hinzugefügten Gerät deaktiviert.	Aktivieren Sie die Kennwortauthentifizierung für SSH auf dem Gerät, das zur Überwachung hinzugefügt wird.
SNMP-Konnektivitätsfehler	Fehler beim Verbinden mit dem SNMP-Port	Überprüfen Sie, ob SNMP auf dem Zielgerät ordnungsgemäß konfiguriert ist.

Aktivierung von DFW-IPFIX nicht möglich

vRealize Network Insight ermöglicht es Ihnen nicht, DFW-IPFIX zu aktivieren.

Problem

Wenn Sie beim Hinzufügen eines Richtlinienmanagers oder einer Quelle von VMware Cloud on AWS versuchen, DFW-IPFIX zu aktivieren, werden möglicherweise die folgenden Fehlermeldungen angezeigt:

- `Es können keine neuen Collectors hinzugefügt werden.`
- `Der angegebene Benutzer verfügt nicht über die erforderliche Rolle. Nur Benutzer mit der folgenden Rolle können IPFIX aktivieren: Cloud-Administrator.`

Ursache

- VMware Cloud on AWS unterstützt nur vier Collectors für sein DFW-IPFIX-Collector-Profil. Wenn das vorhandene Profil bereits über vier Collectors verfügt, wird die Meldung

`Es können keine neuen Collectors hinzugefügt werden.`

angezeigt.

- Der Benutzer verfügt nicht über die Schreibberechtigung. Nur Benutzer mit der Rolle **Cloud-Administrator** können den Schreibvorgang auf dem VMware Cloud on AWS Policy Manager durchführen.

Lösung

- ◆ Um einen neuen Collector hinzuzufügen, müssen Sie wie folgt vorgehen:
 - Einen vorhandenen Collector löschen oder
 - ein neues Profil erstellen oder

- ◆ Um das Problem mit der Benutzerrolle zu vermeiden oder zu beheben, müssen Sie einen der folgenden Schritte ausführen:
 - Weisen Sie dem Benutzer die Rolle **Cloud-Administrator** zu oder
 - Melden Sie sich als Benutzer mit der Rolle **Cloud-Administrator** an.

Planen der Migration von Anwendungen auf VMware Cloud on AWS mithilfe von vRealize Network Insight

23

Mithilfe von vRealize Network Insight können Sie Ihre lokale Umgebung für die Anwendungsmigration auf VMware Cloud on AWS oder AWS bewerten.

Schritte	Verfahren	Verweise
Schritt 1	Einrichten Ihrer Umgebung	<ul style="list-style-type: none">■ Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).<ul style="list-style-type: none">a Erstellen Sie ein VMware-Benutzerkonto oder melden Sie sich beim VMware-Konto an.b Aktualisieren Sie das Registrierungsformular. Neue Benutzer erhalten eine E-Mail für die Aktivierung ihres Kontos.c Akzeptieren Sie die VMware-Nutzungsbedingungen und die EULA.■ Herunterladen der OVA-Dateien<ul style="list-style-type: none">a Melden Sie sich unter https://my.vmware.com/group/vmware/home auf der Produkt-Downloadseite von VMware an.b Suchen Sie nach vRealize Network Insight.c Laden Sie die neuesten vRealize Network Insight-Plattform- und Proxy-OVA-Dateien herunter.■ Bereiten Sie die Installation vor.<ul style="list-style-type: none">a Überprüfen Sie die Systemempfehlungen und -voraussetzungen.b Überprüfen Sie die Unterstützte Produkte und Versionen.
Schritt 2	Bereitstellung	<ol style="list-style-type: none">1 Stellen Sie die vRealize Network Insight-Plattform-OVA-Datei bereit.2 Aktivieren Sie die Lizenz.3 Generieren eines gemeinsamen geheimen Schlüssels4 Stellen Sie die vRealize Network Insight-Proxy-OVA-Datei bereit.5 Erstellen von VMware Cloud on AWS-Firewallregeln für vRealize Network Insight bereit.

Schritte	Verfahren	Verweise
Schritt 3	Datenquellen-Hinzufügung	<ol style="list-style-type: none"> 1 Melden Sie sich bei vRealize Network Insight an. 2 Hinzufügen eines VMware Cloud on AWS-vCenters. 3 Hinzufügen von VMware Cloud on AWS – NSX Manager.
Schritt 4	Modellanwendung	<ul style="list-style-type: none"> ■ Analysieren Sie Anwendungsabhängigkeiten <ol style="list-style-type: none"> a Manuelles Erstellen einer Anwendung b Erstellen von Ebenen für physische IPs c Analysieren der Anwendung d VMware Cloud on AWS: Planung und Mikrosegmentierung ■ Kapitel 19 Empfohlene Firewallregeln. ■ Kapitel 20 Arbeiten mit Suchabfragen. ■ Pinnwände.

Dieses Kapitel enthält die folgenden Themen:

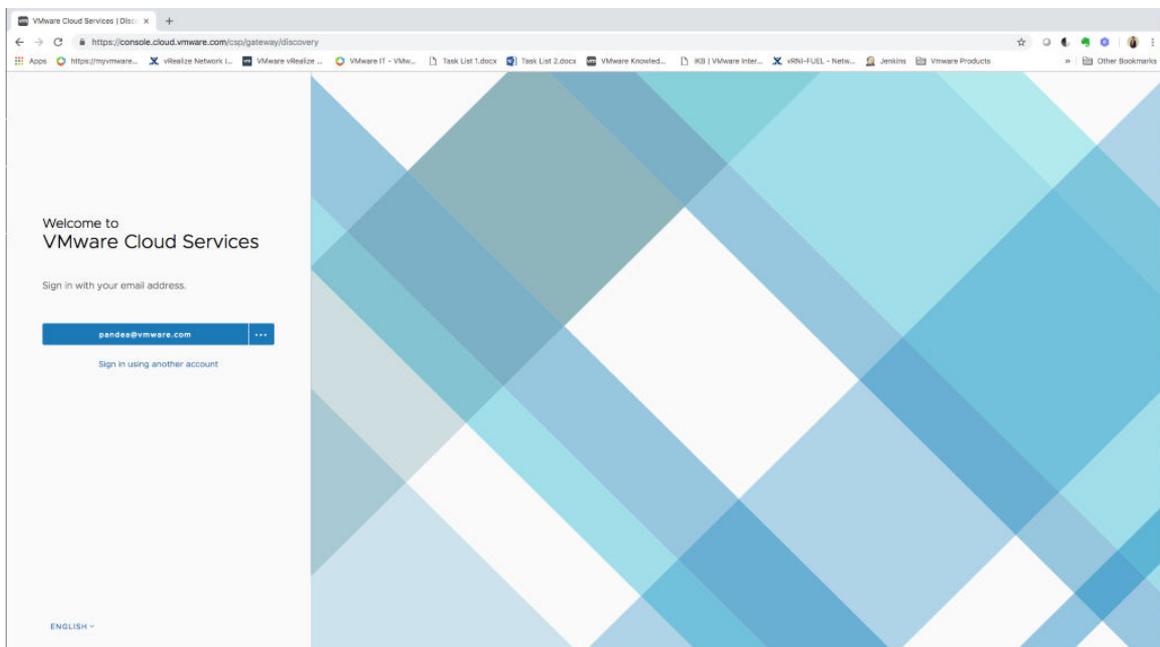
- [Erhalten des CSP-Aktualisierungstokens für NSX Manager](#)
- [Abrufen von vCenter-Anmeldedaten](#)
- [Firewallregel für Computing-Gateway](#)

Erhalten des CSP-Aktualisierungstokens für NSX Manager

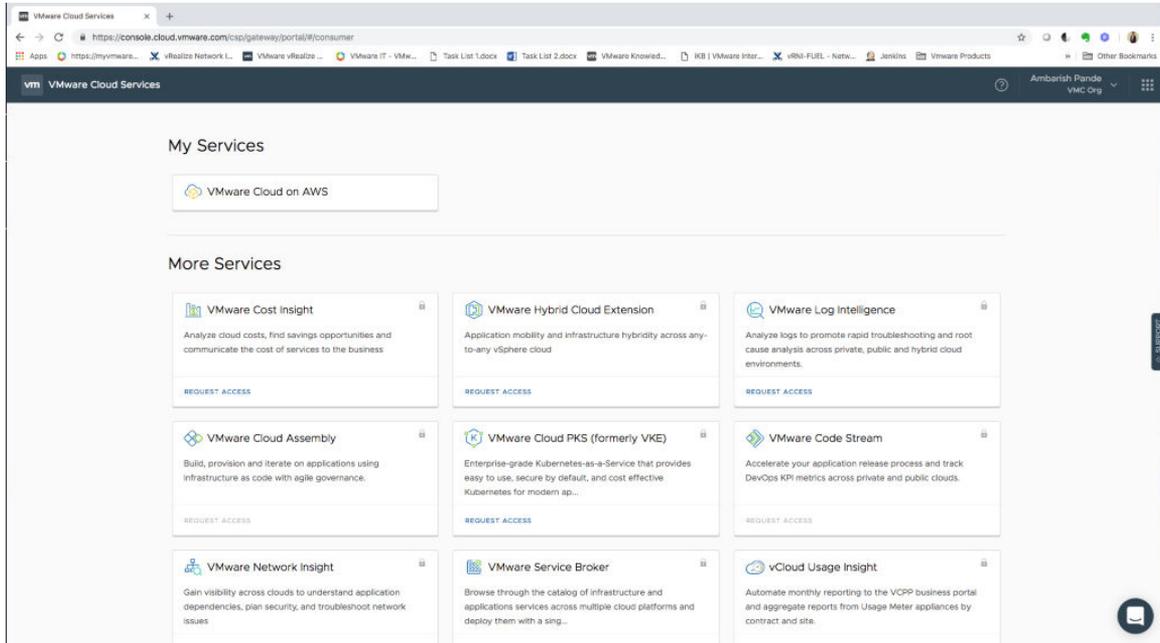
Um einen VMware Cloud on AWS NSX Manager als Datenquelle in vRealize Network Insight, hinzuzufügen, benötigen Sie ein Aktualisierungstoken.

Verfahren

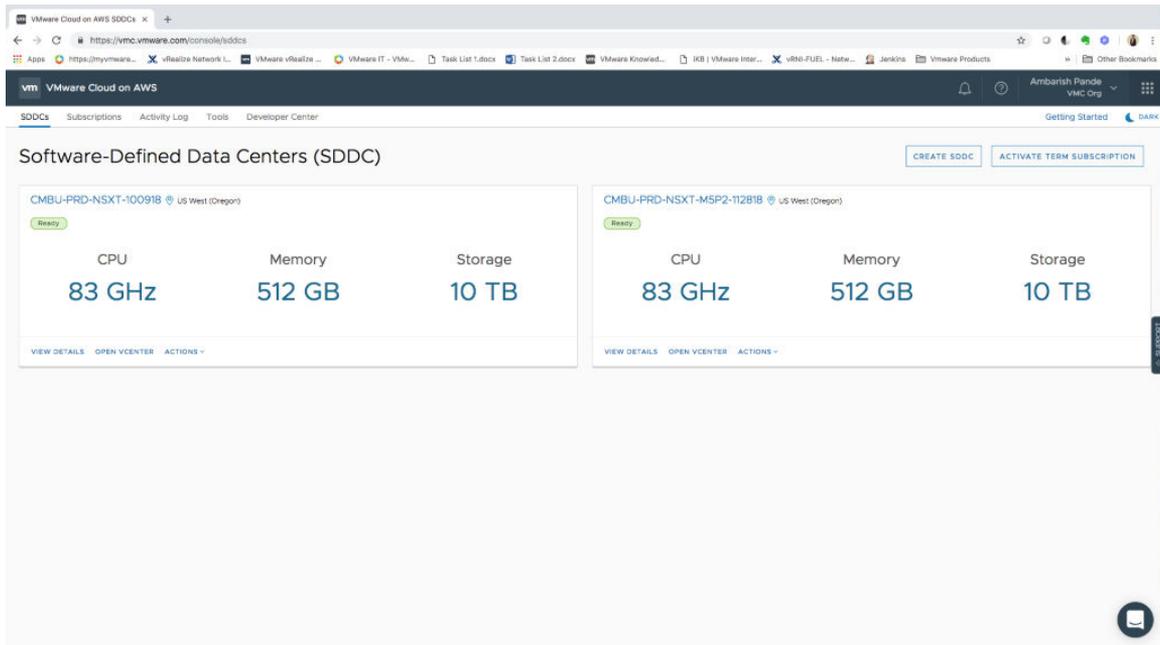
- 1 Melden Sie sich bei der VMware Cloud-Dienstkonzole an.



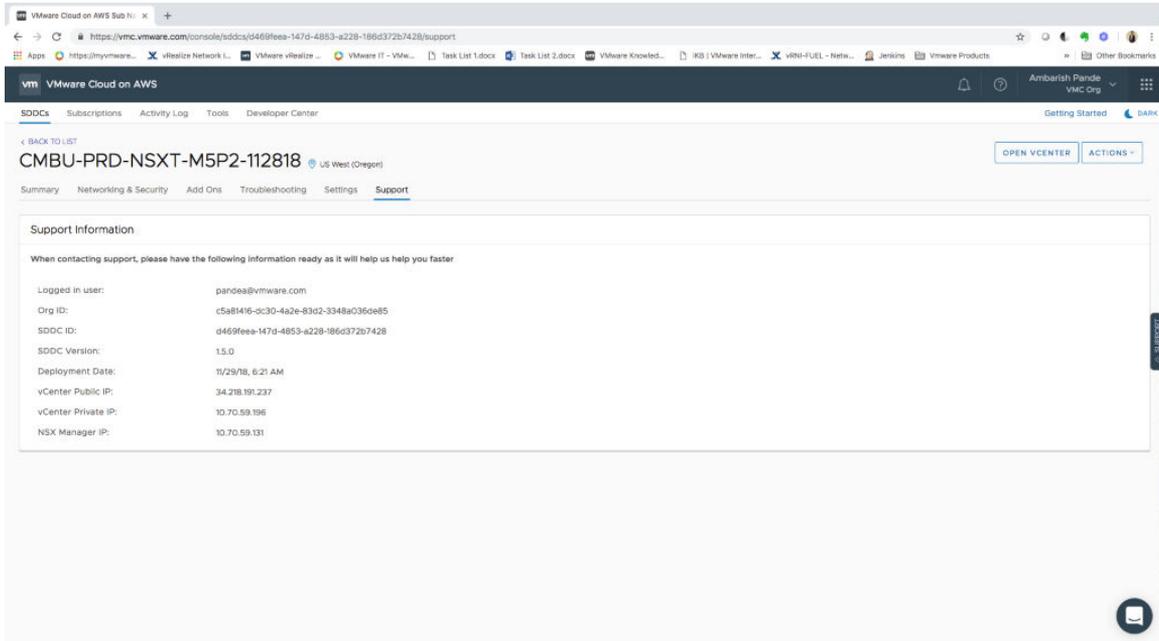
2 Klicken Sie unter „Meine Dienste“ auf VMware Cloud on AWS.



3 Wählen Sie das gewünschte Software-Defined Data Center (SDDC) aus.



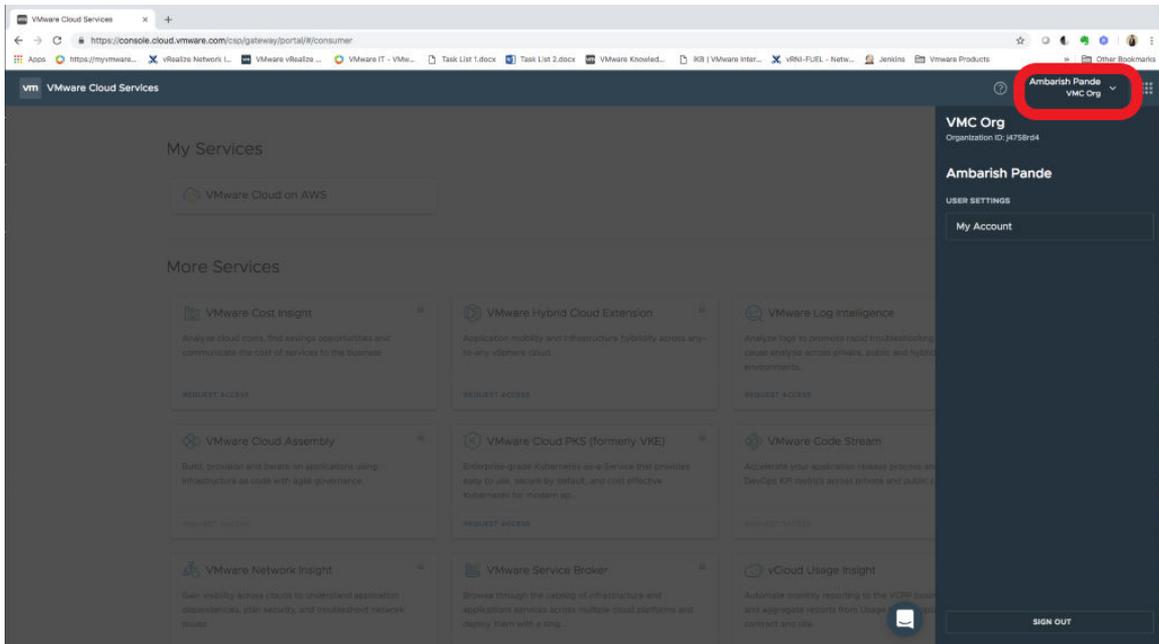
4 Klicken Sie auf die Registerkarte **Support**.



5 Notieren Sie sich die IP-Adresse von NSX Manager.

6 Klicken Sie im oberen Banner auf den Namen der Organisation.

Hinweis Achten Sie darauf, dass sich die Organisation im ausgewählten SDDC befindet.



7 Generieren Sie das API-Token.

Das entsprechende Verfahren finden Sie unter [Generieren von API-Token](#).

Hinweis Zum Generieren des API-Tokens müssen Sie über die Rechte **Administrator** und **NSX Cloud Admin** verfügen.

Ergebnisse

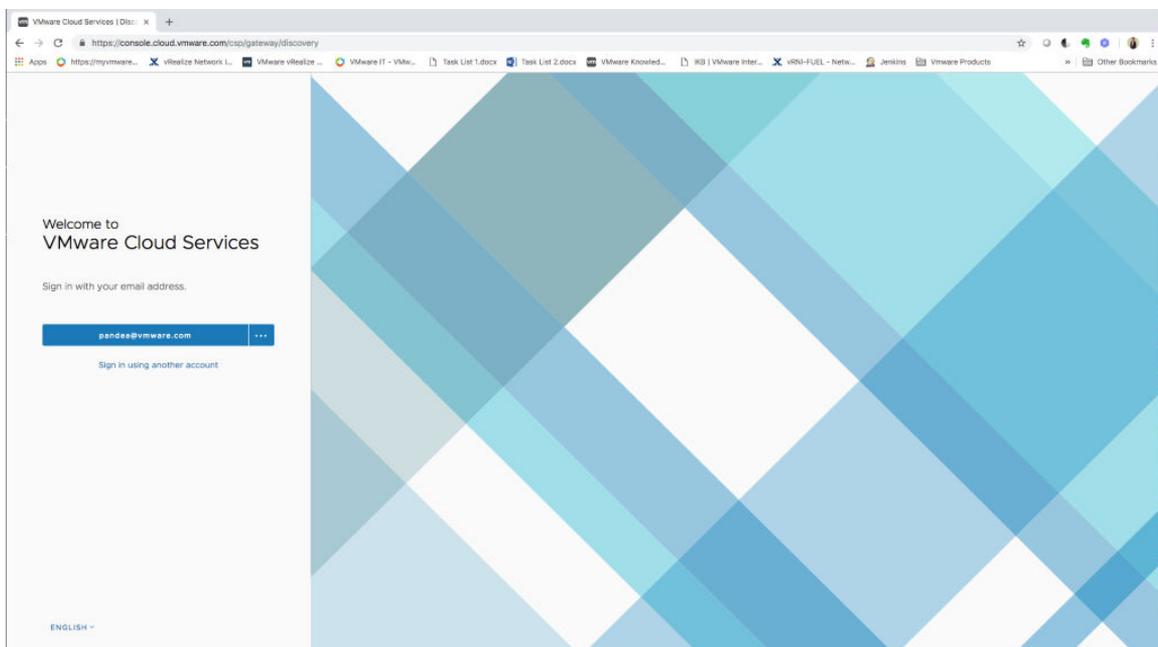
Sie können dieses Token für die Authentifizierung aller VMware Cloud on AWS-SDDCs in der Organisation verwenden.

Abrufen von vCenter-Anmeldedaten

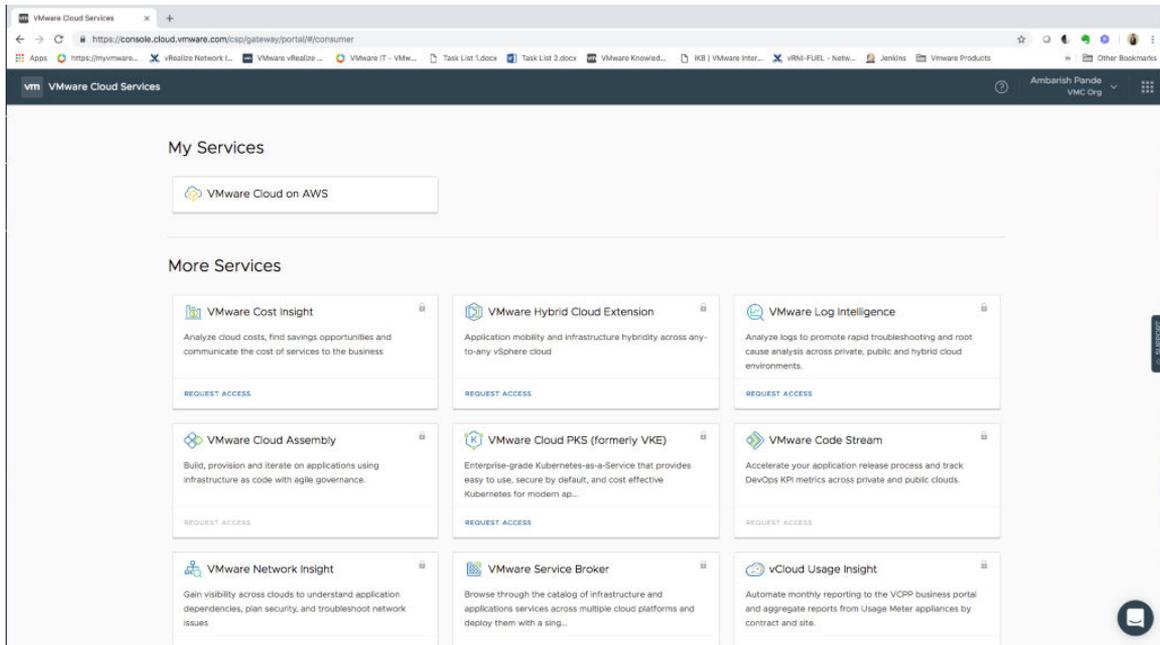
Um eine vCenter-Datenquelle zu vRealize Network Insight hinzuzufügen, benötigen Sie die vCenter-Anmeldedaten.

Verfahren

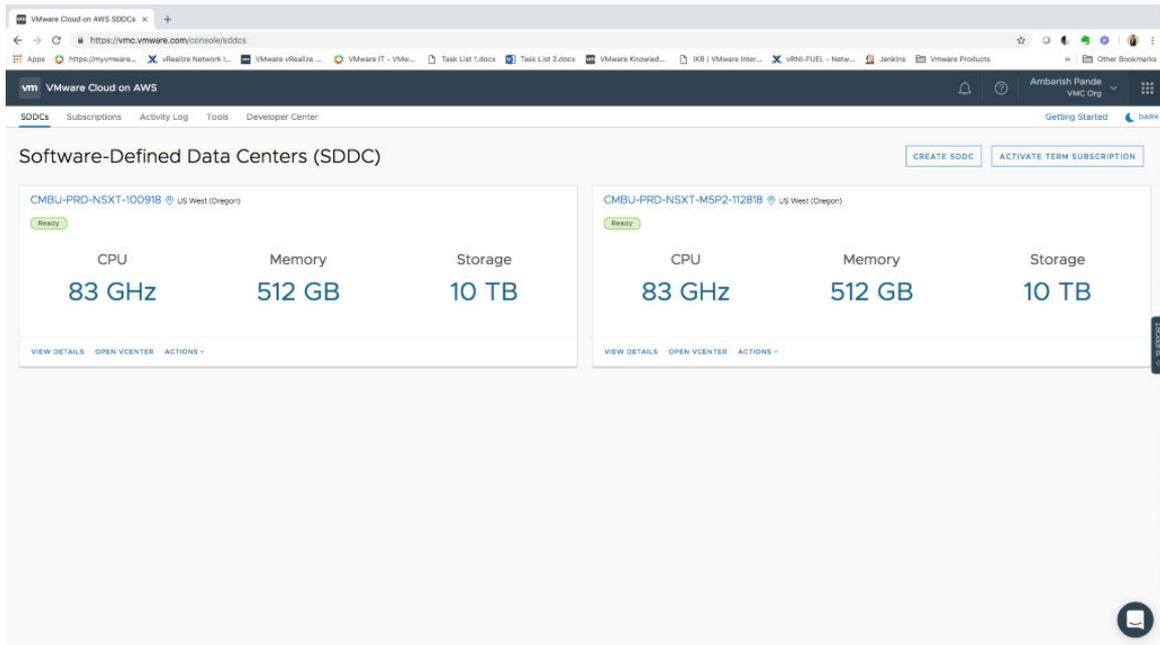
- 1 Melden Sie sich bei der VMware Cloud-Dienstkonzole an.



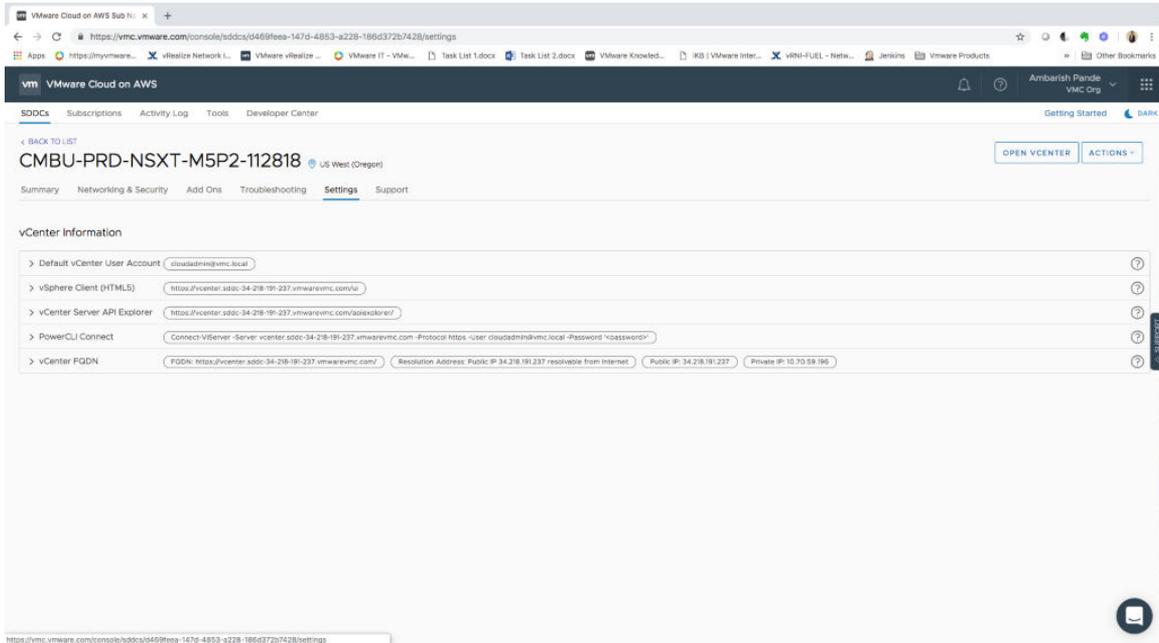
2 Klicken Sie unter „Meine Dienste“ auf VMware Cloud on AWS.



3 Wählen Sie das gewünschte Software-Defined Data Center (SDDC) aus.



4 Klicken Sie auf die Registerkarte **Einstellungen**.

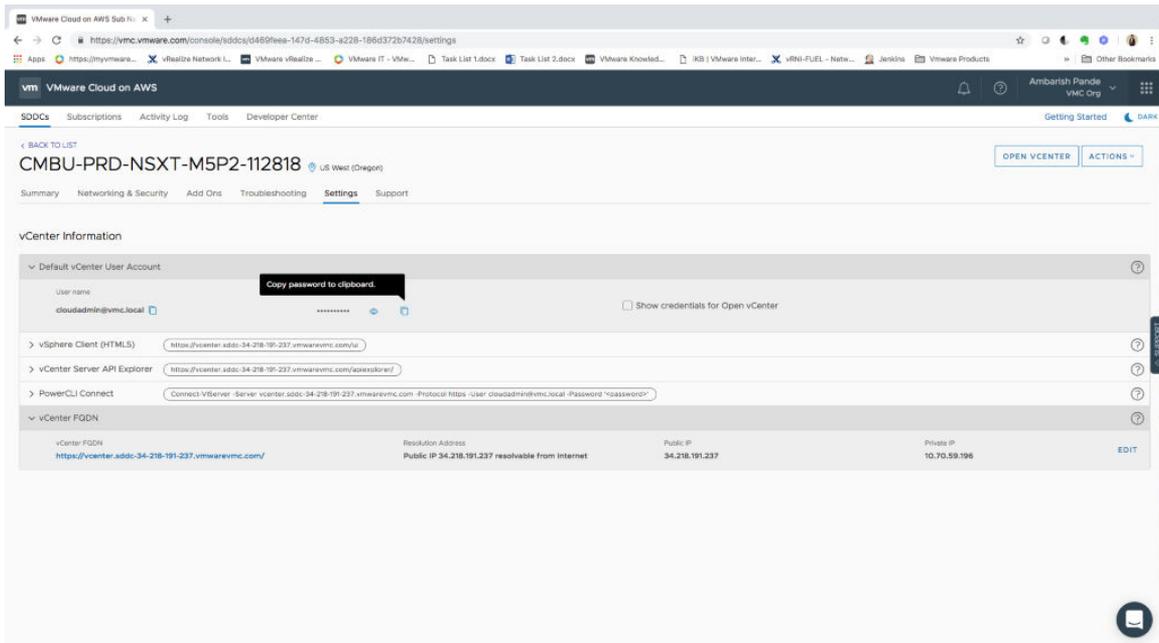


5 Erweitern Sie „vCenter-FQDN“.

Notieren Sie sich die Details zum vCenter-FQDN.

6 Erweitern Sie das standardmäßige vCenter-Benutzerkonto, um den Benutzernamen und das Kennwort abzurufen.

Kopieren Sie das Kennwort und notieren Sie sich den Benutzernamen.



Firewallregel für Computing-Gateway

Bei der Kommunikation mit der vRealize Network Insight-Plattform erfordert der Collector, dass HTTPS-Port 443 für ausgehenden Datenverkehr geöffnet ist.

Der Collector greift über die Firewall auf die folgenden von VMware gehosteten URLs zu:

- *.vmwareidentity.com
- gaz.csp-vidm-prod.com
- *.vmware.com
- *.ni-onsaas.com

Außerdem sollte der NTP- und DNS-Datenverkehr zugelassen sein, damit der vRealize Network Insight- oder vRealize Network Insight-Collector einwandfrei funktioniert.

Erstellen Sie eine Firewallregel mit den folgenden Angaben:

- Name: Ein geeigneter beschreibender Name.
- Quelle: Der Name der VMware Cloud on AWS-Gruppe, die die Collector-IP-Adresse enthält.
- Ziel: Wählen Sie **BELIEBIG** aus.
- Dienste: Wählen Sie **HTTPS, DNS, DNS-UDP, NTP, ICMP** aus.
- Aktion: **Zulassen**
- Angewendet auf: **Internet-Schnittstelle**
- Protokollierung: Aktivieren Sie bei Bedarf die Protokollierung.