

Installieren 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

Info zum Installationshandbuch für vRealize Network Insight 5

1 Vorbereitung für die Installation 6

Systemempfehlungen und -anforderungen 6

Berechtigungen 10

Systemports 11

Netzwerkkommunikationsports 19

Unterstützte Produkte und Versionen 21

2 Installieren von vRealize Network Insight 25

Installations-Workflow 25

Bereitstellen der vRealize Network Insight-Plattform-OVA 27

Bereitstellung mithilfe von vSphere Web Client 27

Bereitstellung mithilfe des nativen vSphere Windows Clients 29

Aktivieren der Lizenz 31

Erstellen eines gemeinsamen geheimen Schlüssels 31

Einrichten des Network Insight-Collector (OVA) 31

Bereitstellung mithilfe von vSphere Web Client 32

Bereitstellung mithilfe des nativen vSphere Windows Clients 34

Einrichten eines Network Insight-Collectors (AMI) in AWS für VMware SD-WAN 35

Bereitstellen eines zusätzlichen Collectors in einer vorhandenen Anordnung 37

3 Zugreifen auf vRealize Network Insight unter Verwendung der Evaluierungslizenz 38

Hinzufügen von vCenter Server 38

Analysieren von Datenverkehrs-Flows 40

Generieren eines Berichts 40

4 Planen der vertikalen Hochskalierung Ihrer Bereitstellung 41

Planen der vertikalen Hochskalierung des Plattform-Clusters 41

Planen der vertikalen Hochskalierung des Collectors 42

Vergrößern der Brick-Größe Ihrer Anordnung 43

5 Upgrade von vRealize Network Insight 45

Online-Upgrade 46

Einzelklick-Offline-Upgrade 49

CLI-Upgrade 52

6 Deinstallieren von vRealize Network Insight 55

Collector-IP entfernen, wenn Netflow in vCenter aktiviert ist 56

Collector-IP entfernen, wenn Netflow in NSX aktiviert ist 56

Info zum Installationshandbuch für vRealize Network Insight

Das *Installationshandbuch für vRealize Network Insight* ist für Administratoren oder Spezialisten bestimmt, die für die Installation von vRealize Network Insight verantwortlich sind.

Zielgruppe

Diese Informationen sind für Administratoren oder Spezialisten bestimmt, die für die Installation von vRealize Network Insight verantwortlich sind. Die Informationen wurden für erfahrene Administratoren von virtuellen Maschinen verfasst, die mit Enterprise Management-Anwendungen sowie mit Datacenter-Vorgängen vertraut sind.

Vorbereitung für die Installation

1

Bevor Sie vRealize Network Insight installieren, bereiten Sie die Bereitstellungsumgebung vor, um die Systemanforderungen zu erfüllen.

Dieses Kapitel enthält die folgenden Themen:

- [Systemempfehlungen und -anforderungen](#)
- [Unterstützte Produkte und Versionen](#)

Systemempfehlungen und -anforderungen

Um eine optimale Leistung zu erzielen, müssen Sie die Mindestempfehlungen für die Bereitstellung erfüllen.

Empfehlungen für die Plattformbereitstellung

Tabelle 1-1. Spezifikationen für die Plattform-Brick-Größe

Brick-Größe	Erforderliche Kerne für CPU mit 2,1 GHz	Erforderliche Kerne für CPU mit 2,3 GHz	Erforderliche Kerne für CPU mit 2,6 GHz	RAM	Festplatte
Mittel	10	9	8	32 GB	1 TB
Groß	15	14	12	48 GB	1 TB
Besonders groß	20	18	16	64 GB	2 TB

Hinweis

- Die Reservierung für die CPU-Geschwindigkeit und den RAM-Speicher für jeden Knoten muss 100 % des oben angegebenen Werts betragen.
- Um Ihre Einrichtung mit allen Spezifikationen abzugleichen, müssen Sie möglicherweise die Ressourcen (RAM, Festplatte, CPU) hinzufügen. Weitere Informationen finden Sie unter <https://kb.vmware.com/s/article/53550> und [Vergrößern der Brick-Größe Ihrer Anordnung](#).

Tabelle 1-2. Nicht-Cluster-Bereitstellung – Maximale Kapazität

Brick-Größe	Anzahl der VMs (in Tausenden)	Flows pro Tag (in Millionen)	Gesamt-Flows (in Millionen)	Flow-Planung (in Millionen)
Mittel	4	1	4	2
Groß	6	2	8	4

Tabelle 1-3. Nicht-Cluster-Bereitstellung – Maximale Kapazität für VMware SD-WAN

Brick-Größe	Anzahl von Edges (in Tausenden)	Flows pro Tag (in Millionen)	Gesamt-Flows (in Millionen)
Mittel	2	1	4
Groß	2	2	8

Hinweis

- Die Anzahl der VMs enthält auch die Vorlagen auf dem vCenter.
- Bei „Gesamt-Flows“ handelt es sich um die maximale Anzahl an Flows, die vom System für den Aufbewahrungszeitraum gespeichert werden können.
- Bei „Flow-Planung“ handelt es sich um alle Flows, für die das System eine Sicherheitsplanung durchführen kann.

Tabelle 1-4. Cluster-Bereitstellung – Maximale Kapazität

Brick-Größe	Clustergröße	Anzahl der VMs (in Tausenden)	Flows pro Tag (in Millionen)	Gesamt-Flows (in Millionen)	Flow-Planung (in Millionen)	Anzahl von Edges für VMware SD-WAN (in Tausenden)
Groß	3	10	2	8	4	4
Besonders groß	3	18	6	24	4	6

Tabelle 1-4. Cluster-Bereitstellung – Maximale Kapazität (Fortsetzung)

Brick-Größe	Clustergröße	Anzahl der VMs (in Tausenden)	Flows pro Tag (in Millionen)	Gesamt-Flows (in Millionen)	Flow-Planung (in Millionen)	Anzahl von Edges für VMware SD-WAN (in Tausenden)
Besonders groß	5	30	10	40	4	10
Besonders groß	10	100	15	55	4	10

Hinweis

- Die Anzahl der VMs enthält auch die Vorlagen auf dem vCenter.
- Bei „Clustergröße“ handelt es sich um die Gesamtanzahl der Knoten im Cluster.
- Bei „Gesamt-Flows“ handelt es sich um die Anzahl an Flows im System für den Aufbewahrungszeitraum.
- Die Abfrage zur Ermittlung der Gesamt-Flows lautet `count of flows in last 31 days`, wobei als Aufbewahrungszeitraum ein Wert von 31 Tagen angenommen wird.
- Bei „Flow-Planung“ handelt es sich um alle Flows, für die das System eine Sicherheitsplanung durchführen kann.

Empfehlung für die Collector-Bereitstellung

Tabelle 1-5. Spezifikationen für Collector-Brick-Größe

Brick-Größe	Erforderliche Kerne für CPU mit 2,1 GHz	Erforderliche Kerne für CPU mit 2,3 GHz	Erforderliche Kerne für CPU mit 2,6 GHz	RAM	Festplatte
Mittel	5	5	4	12 GB	200 GB
Groß	10	9	8	16 GB	200 GB
Besonders groß	10	9	8	24 GB	200 GB

Hinweis Die Reservierung für die CPU-Geschwindigkeit und den RAM-Speicher für jeden Knoten muss 100 % des oben angegebenen Werts betragen.

Tabelle 1-6. Collector-Bereitstellung – Maximale Kapazität

Collector-Größe	Anzahl der VMs (in Tausenden)	Flows pro Tag (in Millionen)	Anzahl der Flows in 4 Tagen (in Millionen)	Anzahl von Edges für VMware SD-WAN (in Tausenden)
Mittel	4	2,5	3,25	4
Groß	10	5	6,5	6
Besonders groß	20.000	10	13	10

Hinweis

- Die Anzahl der VMs enthält auch die Vorlagen auf dem vCenter.
- Bei einer einzelnen Bereitstellung mit mehr als einem Collector basiert die Beschränkung für die Gesamt-Flows in allen Collectors auf der Kapazität der Plattform.

Andere Anforderungen und Überlegungen

- Die maximale Zeitabweichung zwischen den Plattformknoten muss weniger als 30 Sekunden betragen.
- Die Verfügbarkeit des NTP-Diensts ist für Systemvorgänge entscheidend. Stellen Sie sicher, dass Sie den Plattformknoten oder den Collector-Knoten nicht neu starten, wenn der NTP-Dienst nicht verfügbar ist.
- Wenn die vorhandenen Computing-Ressourcen vollständig von den anderen Prozessen auf der Plattform genutzt werden, stürzt vRealize Network Insight ab und wird nicht automatisch wiederhergestellt. Wenn die Dienste nicht wiederhergestellt werden können, starten Sie den Plattformknoten neu.
- Wenn die Netzwerklatenz zwischen dem Plattformknoten und dem Upgrade-Server mehr als 500 ms beträgt, kann beim Upgrade von vRealize Network Insight ein Fehler auftreten. Daher muss die Netzwerklatenz weniger als 500 ms betragen.
- Die empfohlene Festplattenlatenz für eine optimale Leistung beträgt bis zu 5 ms. Wenn die Festplattenlatenz mehr als 5 ms beträgt, verschlechtert sich die Systemleistung.
- Der empfohlene Festplatten-IOPS-Wert beträgt 7500.

Unterstützter Webbrowser

- Google Chrome: Die beiden neuesten Versionen.
- Mozilla Firefox: Die beiden neuesten Versionen.

Empfehlungen zur Unterstützung von Hochverfügbarkeit

Sie können vSphere HA-Optionen anpassen, um die Hochverfügbarkeit von vSphere zu aktivieren.

- **Hostversagen** - VMs neu starten

- **Hostisolierung** - Deaktiviert
- **Gast ohne Taktsignal** - Deaktiviert

Berechtigungen

Erforderliche Berechtigungen für Datenquellen

- Erforderliche Berechtigungen zum Konfigurieren und Verwenden von IPFIX
 - vCenter Server-Anmeldedaten mit Berechtigungen:
 - Distributed Switch: Ändern
 - dvPort-Gruppe: Ändern
 - 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

Weitere Informationen zu Rollen in vCenter finden Sie unter „Verwenden von Rollen zum Zuweisen von Berechtigungen“ im Handbuch *vSphere-Sicherheit*.
- Erforderliche Berechtigungen für NSX Manager Data Provider
 - NSX Manager Data Provider erfordert die **Enterprise**-Rolle.
 - Wenn die zentrale CLI aktiviert ist, sind die `system admin`-Anmeldeinformationen für NSX Manager Data Provider erforderlich.
- Erforderliche Benutzerrechte für Cisco-Switches für die Metrikerfassung
 - vRealize Network Insight ist in der Lage, Metrikdaten über SNMP und die Konfiguration über SSH von Cisco-Switches zu erfassen. Die Cisco Switches UCS-Plattform erfordert die Verwendung von SSH und API für die Erfassung.

Tabelle 1-7.

Datentyp	Benutzerrechte
Konfigurationsdaten	Schreibgeschützt
Metrikdaten	SNMP-schreibgeschützt
	SNMPv2-schreibgeschützte SNMP-Community
	SNMPv3-schreibgeschützt

Systemports

Im Folgenden finden Sie eine Liste der Ports, die für die eingehende vRealize Network Insight-Kommunikation erforderlich sind:

Ports für das Plattform-Cluster-Setup

Tabelle 1-8.

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
SSH-Client	Plattform	22	SSH	CLI- oder Hostzugriff	Nein	Ja	Benutzer-/Kennwort- oder SSH-Schlüssel-basierte Authentifizierung
Client-Webbrowser und vRNI-Collector	Plattform	443	HTTPS	Zugriff auf die Benutzeroberfläche/API und Kommunikation mit vRNI Collector	Ja	Ja	SSL-Kanal verschlüsselt mit auf dem 2048b-RSA-Schlüssel basierendem SHA2-Zertifikat (oder benutzerkonfiguriertem Zertifikat). Nachrichten von Collector zu Plattform auf diesem Kanal werden auch mit HMAC weiter verschlüsselt.

Tabelle 1-8. (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
Plattform	Plattform	2181	HTTP	Kommunikation zwischen Zookeeper-Servern auf anderen Knoten (im Falle eines Clusters). Und speichert Metadateninformationen (znode-Daten)	Nein	Nein	
Plattform	Plattform	2888	HTTP	Wird zum Herstellen einer Verbindung mit dem Zookeeper-Leader verwendet.	Nein	Nein	
Plattform	Plattform	3000	HTTP	Wird für E-Mail-Benachrichtigungen verwendet.	Ja	Nein	
Plattform	Plattform	3888	HTTP	Wird für Zookeeper Leader-Wahl verwendet.	Ja	Nein	
Plattform	Plattform	5432	jdbc	Speichern von VM-Konfigurationsdaten und Infra-Metadaten	Ja	Nein	
Plattform	Plattform	8020	TCP/RPC	Kommunizieren zwischen anderen Name-Knoten und Datenknoten	Ja	Nein	

Tabelle 1-8. (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
Plattform	Plattform	8025	HTTP	Knotenmanager verwenden diesen Port zum Herstellen einer Verbindung mit dem Ressourcenmanager.	Nein	Nein	
Plattform	Plattform	8030	HTTP	Wird vom Ressourcenmanager verwendet, um die Aufgaben zu planen.	Nein	Nein	
Plattform	Plattform	8032	HTTP	Adresse der Anwendungsmanager-Schnittstelle im RM	Nein	Nein	
Plattform	Plattform	8033	HTTP	Adresse der RM-Admin-Schnittstelle	Nein	Nein	
Plattform	Plattform	8042	HTTP	Adresse der Web-App für Knotenmanager	Nein	Nein	
Plattform	Plattform	8080	HTTP	Reicht Benutzeroberflächenanforderungen weiter.	Ja	Nein	
Plattform	Plattform	8088	HTTP	HTTP-Adresse der Webanwendung für Ressourcenmanager	Nein	Nein	
Plattform	Plattform	8480	TCP/RPC	JournalNode-HTTP-Server	Nein	Nein	

Tabelle 1-8. (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
Plattform	Plattform	8485	TCP/RPC	Datenverzeichnis für HDFS-verteilte Bearbeitungen	Nein	Nein	
Plattform	Plattform	9090	HTTP	Reicht Anforderungen von Collector weiter und sendet Befehle an Collector	Ja	Ja (über nginx geschützt)	
Plattform	Plattform	9092	Binär über TCP	Port, auf dem andere Broker kommunizieren	Ja	Nein	
Plattform	Plattform	9200-9300	HTTP	Reicht Suchanforderungen weiter. ES verwendet einen Bereich von Ports, die überwacht werden sollen, wenn 9200 besetzt ist, wird der nächste Port verwendet.	Ja	Nein	

Tabelle 1-8. (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
Plattform	Plattform	9300	HTTP	Reicht Suchanforderungen weiter. ES verwendet einen Bereich von Ports, die überwacht werden sollen, wenn 9200 besetzt ist, wird der nächste Port verwendet.	Ja	Nein	
Plattform	Plattform	30000:65535	TCP	Flüchtiger Portbereich, der von verschiedenen Prozessen verwendet wird, um die TCP-Verbindung mit den anderen Prozessen herzustellen	Nein	Nein	
Plattform	Plattform	60000	IPC	Wird für die Kommunikation zwischen anderen primären HBase-Servern und Regionsservern verwendet.	Ja	Nein	
Plattform	Plattform	60010	HTTP	Wird für die HBase-Web-UI verwendet.	Nein	Nein	

Tabelle 1-8. (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
Plattform	Plattform	60020	IPC	Kommunikation zwischen dem primären hbase-Server und dem Regionsserver	Ja	Nein	
Plattform	Plattform	4500-4510	TCP	Kommunikation zwischen Foundation DB-Servern, die auf unterschiedlichen Plattformen ausgeführt werden	Ja	Nein	

Ports für die Anordnung mit einer einzelnen Plattform

Tabelle 1-9.

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
SSH-Client	Plattform	22	SSH	CLI- oder Hostzugriff	Nein	Ja	Benutzer-/ Kennwort- oder SSH-Schlüssel-basierte Authentifizierung
Client-Webbrowser und vRNI-Collector	Plattform	443	HTTPS	Zugriff auf die Benutzeroberfläche/API und Kommunikation mit vRNI Collector	Ja	Ja	SSL-Kanal verschlüsselt mit auf dem 2048b-RSA-Schlüssel basiertem SHA2-Zertifikat (oder benutzerkonfiguriertem Zertifikat). Nachrichten von Collector zu Plattform auf diesem Kanal werden auch mit HMAC weiter verschlüsselt.

Ports für den Collector-Server

Tabelle 1-10.

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
SSH-Client	Collector	22	SSH	CLI- oder Hostzugriff	Nein	Ja	Benutzer-/Kennwort- oder SSH-Schlüssel-basierte Authentifizierung
vRNI-Collector	Plattform	443	HTTPS	Primärer Kommunikationskanal mit Plattform	Ja	Ja	SSL-Kanal verschlüsselt mit auf dem 2048b-RSA-Schlüssel basierendem SHA2-Zertifikat (oder benutzerkonfiguriertem Zertifikat). Nachrichten von Collector zu Plattform auf diesem Kanal werden auch mit HMAC weiter verschlüsselt.
Flow-Weiterleitungen	Collector	UDP 2055	Netflow/IPFIX	Flows von Ziel werden an diesen Port übertragen.	Ja	Nein	
Flow-Weiterleitungen	Collector	UDP 6343	sFlow	Flows von Ziel werden an diesen Port übertragen.	Ja	Nein	

Tabelle 1-10. (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Vertraulich	SSL	Authentifizierung
ESXi-Host	Collector	1991	TCP	Erfassen der Latenzmessung der virtuellen Infrastruktur, Beispiel: Latenz von vNIC zu pNIC, VTEP zu VTEP, TEP zu TEP usw.	Nein	Nein	
Dell OS10	Collector	50000	GRPC	Empfangen von Telemetrieinformationen von Dell OS10-Geräten bezüglich Pufferstatistiken	Nein	Nein	

Netzwerkkommunikationsports

In der folgenden Tabelle sind die Ports und Protokolle aufgeführt, die für die Netzwerkkommunikation in vRealize Network Insight verwendet werden.

Sie können die Liste der Ports auch unter <https://ports.vmware.com/home/vRealize-Network-Insight> anzeigen.

Tabelle 1-11.

Zweck	Von	Bis	Port	Protokoll
Kommunikation zwischen den VMs von vRealize Network Insight	Collector	Plattform Hinweis Der Port muss für alle Plattformen aktiviert sein.	443	HTTPS
Dienste, die Internetzugriff erfordern	Plattform und Collector	svc.ni.vmware.com support2.ni.vmware.com reg.ni.vmware.com	443	HTTPS

Tabelle 1-11. (Fortsetzung)

Zweck	Von	Bis	Port	Protokoll
Konfigurierte Kommunikation für verschiedene Dienste	Plattform	LDAP-Server	389, 636	LDAP und LDAPS
		SNMP-Server	Konfigurierbar	SNMP
	Plattform und Collector	DNS-Server	53	UDP
		Syslog-Server	Konfigurierbar	
	ESXi-Hosts	Collector	2055	
	ESXi-Hosts	Collector	1991	TCP
Kommunikation mit AWS als Datenquelle	Collector	AWS (*.amazonaws.com)	443	HTTPS
Kommunikation mit Telemetriedienst	Browser	Telemetrie-URL https://vcsa.vmware.com	433	HTTPS
Kommunikation mit anderen Datenquellen innerhalb des Datencenters	Collector	Arista-Switches	161 und 22	SNMP und SSH
		Azure	443	HTTPS
		Brocade-Switches	161 und 22	SNMP und SSH
		Check Point-Firewall	443	HTTPS
		Cisco Nexus	161 und 22	SNMP und SSH
		Cisco UCS (Unified Computing-System)	161, 22 und 443	SNMP, SSH und HTTPS
		Cisco Catalyst-Switches	161 und 22	SNMP und SSH
		Cisco ACI-Switches	161	SNMP
		Cisco APIC-Controller	161 und 443	HTTPS und SNMP
		Dell-Switches	161 und 22	SNMP und SSH
		Dell OS10	50000	TCP
		VeloCloud	443, 2055	HTTPS
		HP	22	SSH
		Juniper-Switches	161 und 22	SNMP und SSH
		Palo Alto-Netzwerke	443	HTTPS
		VMware vSphere	443	HTTPS
		VMware NSX - V (alle Komponenten)	22 und 443	SSH und HTTPS
		NSX-T Manager	443	TCP

Tabelle 1-11. (Fortsetzung)

Zweck	Von	Bis	Port	Protokoll
		VMware PKS-API-Server	8443 und 9021	TCP
		Kubernetes-API-Server	8443	TCP
		vRealize Log Insight	443	HTTPS
		Fortinet FortiManager	443	HTTPS

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.
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

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
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
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.

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
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 Kontorolle 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.
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.

Datenquelle	Version/Modell	Konnektivitätsprotokoll	Berechtigungen/Rechte
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
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.

Installieren von vRealize Network Insight

2

Sie können vRealize Network Insight mithilfe des vSphere Web Client oder des nativen vSphere Windows-Clients bereitstellen.

Hinweis Nachdem Sie die vRealize Network Insight-Plattform-OVA erfolgreich bereitgestellt haben, überprüfen Sie, ob die angegebene statische IP-Adresse auf vCenter Server festgelegt ist.

Um Installation, Konfiguration, Upgrades, Patches, Konfigurationsverwaltung, Drift Remediation und Integrität über eine zentrale Oberfläche zu automatisieren, können Sie vRealize Suite Lifecycle Manager verwenden. Als neuer Benutzer klicken Sie hier, um den [vRealize Suite Lifecycle Manager](#) zu installieren. Dadurch profitieren die IT-Verantwortlichen der Cloud von Verwaltungsressourcen, mit denen sie sich auf geschäftskritische Maßnahmen konzentrieren und gleichzeitig Wertschöpfung, Zuverlässigkeit und Konsistenz optimieren können.

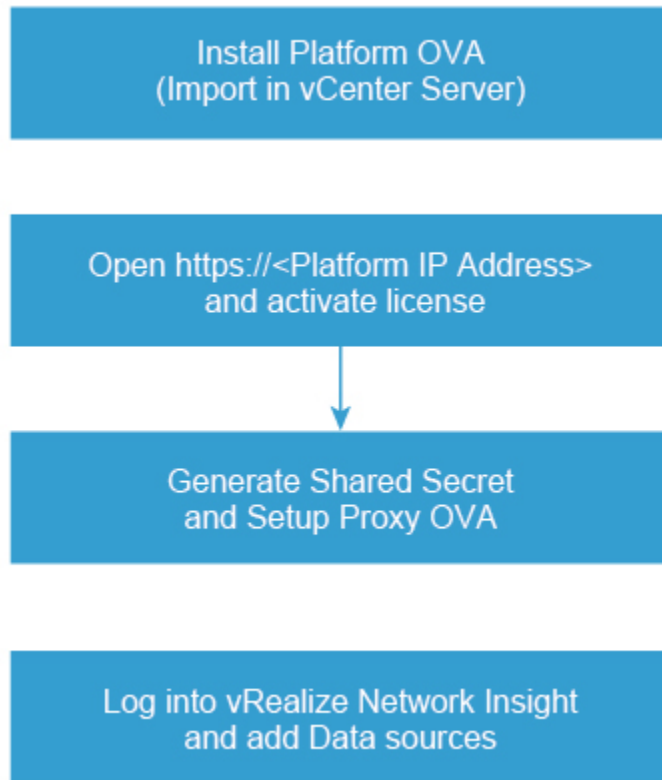
Sie können vRealize Network Insight auch mithilfe von vRealize Suite Lifecycle Manager installieren und aktualisieren. Weitere Informationen finden Sie im Handbuch [vRealize Suite Lifecycle Manager Installation, Upgrade, and Management](#).

Dieses Kapitel enthält die folgenden Themen:

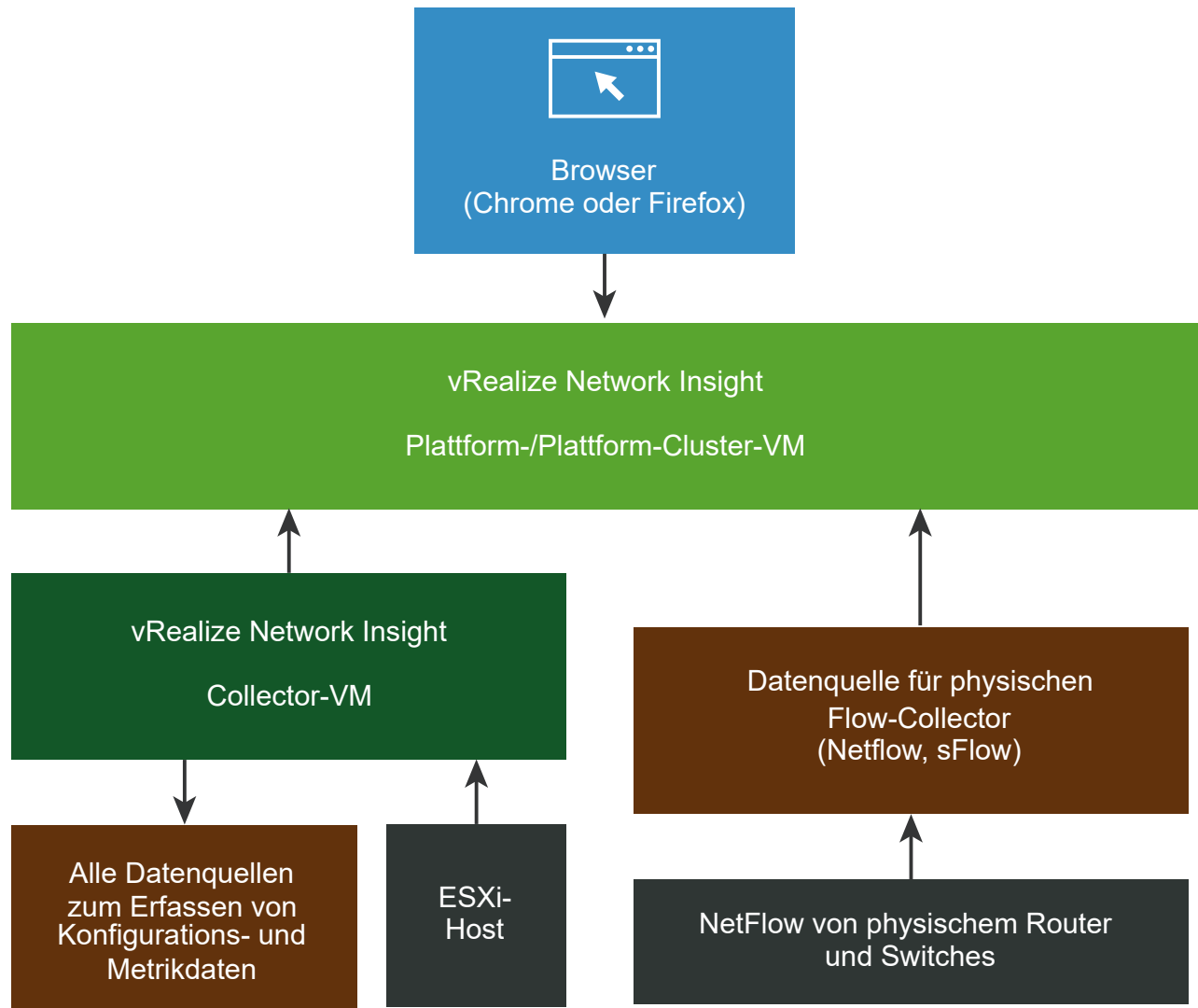
- [Installations-Workflow](#)
- [Bereitstellen der vRealize Network Insight-Plattform-OVA](#)
- [Aktivieren der Lizenz](#)
- [Erstellen eines gemeinsamen geheimen Schlüssels](#)
- [Einrichten des Network Insight-Collector \(OVA\)](#)
- [Einrichten eines Network Insight-Collectors \(AMI\) in AWS für VMware SD-WAN](#)
- [Bereitstellen eines zusätzlichen Collectors in einer vorhandenen Anordnung](#)

Installations-Workflow

Um vRealize Network Insight zu installieren, installieren Sie die Plattform-OVA, aktivieren die Lizenz, generieren einen gemeinsamen geheimen Schlüssel und richten die Collector-OVA ein.



Ein vereinfachtes Bereitstellungsdiagramm von vRealize Network Insight sieht wie folgt aus:



Bereitstellen der vRealize Network Insight-Plattform-OVA

Sie können die vRealize Network Insight-Plattform-OVA in ihren vCenter Server importieren.

Hinweis Die Bereitstellung der vRealize Network Insight-Plattform-OVA im VMC-SDDC wird nicht unterstützt.

Bereitstellung mithilfe von vSphere Web Client

Sie können vRealize Network Insight mithilfe von vSphere Web Client bereitstellen.

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf das **Datencenter**, in dem Sie die Appliance installieren möchten, und wählen Sie **OVF-Vorlage bereitstellen** aus.

- 2 Geben Sie die URL zum Herunterladen und Installieren des OVA-Pakets ein oder wählen Sie den Quellspeicherort des OVA-Pakets aus.
- 3 Geben Sie den OVA-Namen ein. Wählen Sie den Zielordner für die Bereitstellung aus.
- 4 Wählen Sie einen Host oder Cluster oder einen Ressourcenpool aus, in dem die bereitgestellte Vorlage ausgeführt werden soll.
- 5 Überprüfen Sie die Details der OVF-Vorlage.
- 6 Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Akzeptieren**.
- 7 Wählen Sie eine Bereitstellungskonfiguration aus. Klicken Sie auf **Weiter**.
- 8 Wählen Sie den Speicherort aus, an dem die Dateien für die bereitgestellte Vorlage gespeichert werden. Wählen Sie **Thin Provisioning** als das Format der virtuellen Festplatte aus. Wählen Sie den Datenspeicher oder die Datenspeicher-Cluster aus, in denen die Dateien gespeichert werden sollen. Klicken Sie auf **Weiter**.
- 9 Geben Sie das Netzwerk an, das die bereitgestellte VM nutzen wird.
Das ausgewählte Netzwerk sollte es der Appliance ermöglichen, das Internet für Support und Upgrade zu erreichen.
- 10 Um die Vorlage für die Bereitstellung anzupassen, müssen Sie die-Appliance mithilfe der VM-Konsole manuell konfigurieren. Klicken Sie auf **Weiter**.
- 11 Überprüfen Sie die Konfigurationsdetails und klicken Sie auf **Beenden**.
- 12 Befolgen Sie die Schritte unter [Vergrößern der Brick-Größe Ihrer Anordnung](#), um die Systemempfehlungen und -anforderungen zu erfüllen.
- 13 Sobald die Plattform installiert ist, starten Sie die VM und dann die Konsole.
- 14 Melden Sie sich mit den Konsolenanmeldedaten an, die auf dem Bildschirm angezeigt werden, und führen Sie den `setup`-Befehl aus.
- 15 Erstellen Sie das Kennwort für die *support*-Anmeldung und ändern Sie das Kennwort für den *consoleuser*.

Hinweis

- Ihr Kennwort muss mindestens 6 Zeichen lang sein. Ein einzelnes Anführungszeichen (') ist nicht zulässig.
- Sie müssen die Kennwörter für *support* und *consoleuser* in regelmäßigen Abständen ändern, um Ihre Organisationsrichtlinie einzuhalten.

-
- 16 Geben Sie die folgenden Details ein, um das Netzwerk zu konfigurieren:
 - a **IPv4-Adresse**: Zweite reservierte statische IP-Adresse
 - b **Netzmaske**: Subnetzmaske für die obige statische IP-Adresse
 - c **Standard-Gateway**: Standard-Gateway Ihres Netzwerks

- d **DNS:** DNS-Server Ihrer Umgebung

Hinweis Stellen Sie für mehrere DNS-Server sicher, dass sie durch Leerzeichen getrennt sind.

- e **Domänensuchliste** : Die Domäne, die für DNS-Lookups angehängt werden muss.

- f Geben Sie **y** ein, um die Konfiguration zu speichern.

- 17 Geben Sie den NTP-Server ein und stellen Sie sicher, dass er von der VM aus erreicht werden kann. Die Dienste können nicht gestartet werden, wenn die NTP-Zeit nicht synchronisiert ist.

Hinweis Stellen Sie bei Angabe mehrerer NTP-Server sicher, dass sie durch Kommata getrennt sind.

- 18 (Optional) Um den Webproxy zu konfigurieren, geben Sie **y** ein.

- 19 Alle Dienste werden überprüft.

- 20 Fügen Sie basierend auf Ihrer Einrichtungsanforderung zusätzlichen Festplattenspeicher hinzu. Weitere Informationen hierzu finden Sie unter <https://kb.vmware.com/s/article/53550>.

Bereitstellung mithilfe des nativen vSphere Windows Clients

Sie können vRealize Network Insight mithilfe des nativen vSphere Windows-Clients bereitstellen.

Hinweis vRealize Network Insight 5.2 ist die letzte Version, die die OVA-Bereitstellung mit dem nativen vSphere Windows-Client unterstützt. Ab Version 5.3 können Sie weiterhin den vSphere Web Client zum Bereitstellen von vRealize Network Insight OVA verwenden.

Verfahren

- 1 Klicken Sie auf **Datei > OVF-Vorlage bereitstellen**.
- 2 Geben Sie die URL zum Herunterladen und Installieren des OVA-Pakets aus dem Internet ein oder wählen Sie den Quellspeicherort des OVA-Pakets in Ihrem Computer aus.
- 3 Klicken Sie auf **Weiter** und überprüfen Sie die Details der OVF-Vorlage.
- 4 Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Akzeptieren**.
- 5 Geben Sie einen Namen und einen Speicherort für die bereitgestellte Vorlage an. Klicken Sie auf **Weiter**.
- 6 Wählen Sie die **Bereitstellungskonfiguration** aus.
- 7 Wählen Sie einen **Host/Cluster** aus, auf dem die bereitgestellte Vorlage ausgeführt werden soll.
- 8 Wählen Sie den **Ressourcenpool** aus, in dem Sie die Vorlage bereitstellen möchten.
- 9 Wählen Sie den Zielspeicher für die VM-Dateien aus. Klicken Sie auf **Weiter**.
- 10 Geben Sie das Format an, in dem Sie die virtuellen Festplatten speichern möchten. Wählen Sie **Thin Provisioning** als das Format der virtuellen Festplatte aus. Klicken Sie auf **Weiter**.

- 11 Geben Sie das Netzwerk an, das von der bereitgestellten Vorlage verwendet werden soll. Ordnen Sie das Netzwerk von dem OVA-Paket zu Ihrer Bestandsliste zu.
- 12 Passen Sie die Vorlage für die Bereitstellung an. Geben Sie den gemeinsamen geheimen Schlüssel an, der auf der Onboarding-Seite generiert wurde. Sie müssen die Appliance mithilfe der VM-Konsole manuell konfigurieren. Klicken Sie auf **Weiter**.
- 13 Überprüfen Sie alle Konfigurationsdaten. Aktivieren Sie **Nach der Bereitstellung einschalten**. Klicken Sie auf **Beenden**.
- 14 Befolgen Sie die Schritte unter [Vergrößern der Brick-Größe Ihrer Anordnung](#), um die [Systemempfehlungen und -anforderungen](#) zu erfüllen.
- 15 Sobald die Collector-OVA installiert ist, starten Sie die VM und dann die Konsole.
- 16 Melden Sie sich mit den Konsolenanmeldedaten an, die auf dem Bildschirm angezeigt werden, und führen Sie den `setup`-Befehl aus.
- 17 Erstellen Sie das Kennwort für die *support*-Anmeldung und ändern Sie das Kennwort für den *consoleuser*.

Hinweis

- Ihr Kennwort muss mindestens 6 Zeichen lang sein. Ein einzelnes Anführungszeichen (') ist nicht zulässig.
 - Sie müssen die Kennwörter für *support* und *consoleuser* in regelmäßigen Abständen ändern, um Ihre Organisationsrichtlinie einzuhalten.
-

- 18 Geben Sie die folgenden Details ein, um das Netzwerk zu konfigurieren:

- a **IPv4-Adresse:** Zweite reservierte statische IP-Adresse
- b **Netzmaske:** Subnetzmaske für die obige statische IP-Adresse
- c **Standard-Gateway:** Standard-Gateway Ihres Netzwerks
- d **DNS:** DNS-Server Ihrer Umgebung

Hinweis Stellen Sie für mehrere DNS-Server sicher, dass sie durch Leerzeichen getrennt sind.

- e **Domänensuchliste:** die Domäne, die für `dns lookup` angehängt werden muss.
- f Geben Sie `y` ein, um die Konfiguration zu speichern.

- 19 Geben Sie den NTP-Server ein und stellen Sie sicher, dass er von der VM aus erreicht werden kann. Die Dienste können nicht gestartet werden, wenn die NTP-Zeit nicht synchronisiert ist.

Hinweis Stellen Sie bei Angabe mehrerer NTP-Server sicher, dass sie durch Kommata getrennt sind.

- 20 (Optional) Um den Webproxy zu konfigurieren, geben Sie `y` ein.
- 21 Alle Dienste werden überprüft.

- 22 Fügen Sie basierend auf Ihrer Einrichtungsanforderung zusätzlichen Festplattenspeicher hinzu. Weitere Informationen hierzu finden Sie unter <https://kb.vmware.com/s/article/53550>.

Aktivieren der Lizenz

Öffnen Sie nach der Installation der vRealize Network Insight-Plattform-OVA *https://<iP-Adresse der vRealize Network Insight-Plattform>* im Chrome-Webbrowser.

Verfahren

- 1 Geben Sie den in der Begrüßungs-E-Mail erhaltenen Lizenzschlüssel ein.
- 2 Legen Sie für den Benutzernamen des UI-Administrators (`admin@local`) das Kennwort fest.

Hinweis Ihr Kennwort muss alphanumerisch sein und mindestens 8 und maximal 100 Zeichen haben. Leerzeichen zwischen den Zeichen sind nicht zulässig.

- 3 Klicken Sie auf **Aktivieren**.
- 4 Fügen Sie nach dem Aktivieren der Lizenz den vRealize Network Insight-Collector hinzu.

Erstellen eines gemeinsamen geheimen Schlüssels

Sie können die virtuelle Collector-Appliance von vRealize Network Insight generieren und importieren.

Erzeugen Sie einen gemeinsamen geheimen Schlüssel und importieren Sie die virtuelle Collector-Appliance von vRealize Network Insight:

Verfahren

- 1 Melden Sie sich bei der vRealize Network Insight-Benutzeroberfläche an.
- 2 Erweitern Sie **Infrastruktur und Support** und klicken Sie auf **Übersicht und Updates**.
- 3 Scrollen Sie nach unten und klicken Sie auf **Proxy-VM hinzufügen**.

Das Dialogfeld **Neue virtuelle Appliance für Network Insight-Datenerfassung hinzufügen** wird angezeigt.

- 4 Klicken Sie auf **Kopieren**, um den gemeinsamen geheimen Schlüssel aus dem Dialogfeld zu kopieren, und klicken Sie auf **Fertig**.

Dieser wird während der Bereitstellung der Collector-OVA für vRealize Network Insight benötigt.

Einrichten des Network Insight-Collector (OVA)

Sie können den vRealize Network Insight-Collector einrichten, indem Sie OVA in Ihren vCenter Server importieren.

Führen Sie die folgenden Schritte aus, um die vRealize Network Insight-Collector-OVA in ihren vCenter Server zu importieren.

Bereitstellung mithilfe von vSphere Web Client

Sie können die vRealize Network Insight-Collector-OVA mithilfe von vSphere Web Client importieren.

Verfahren

- 1 Klicken Sie mit der rechten Maustaste auf das **Datencenter**, in dem Sie die Appliance installieren möchten, und wählen Sie **OVF-Vorlage bereitstellen** aus.
- 2 Geben Sie die URL zum Herunterladen und Installieren des OVA-Pakets aus dem Internet ein oder wählen Sie den Quellspeicherort der OVA-Datei in Ihrem Computer aus.
- 3 Geben Sie einen Namen und einen Speicherort für die bereitgestellte Vorlage an. Klicken Sie auf **Weiter**.
- 4 Wählen Sie eine Ressource (Host oder Cluster) aus, auf der die bereitgestellte Vorlage ausgeführt werden soll. Klicken Sie auf **Weiter**.
- 5 Überprüfen Sie alle Details der Vorlage. Klicken Sie auf **Weiter**.
- 6 Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Akzeptieren**. Klicken Sie auf **Weiter**.
- 7 Wählen Sie eine Bereitstellungsconfiguration aus. Klicken Sie auf **Weiter**.
- 8 Wählen Sie den Speicherort aus, an dem die Dateien für die bereitgestellte Vorlage gespeichert werden sollen. Geben Sie das Format an, in dem Sie die virtuellen Festplatten speichern möchten. Wählen Sie **Thin Provisioning** als das Format der virtuellen Festplatte aus. Wählen Sie den Datenspeicher aus, in dem Sie die Dateien installieren möchten. Klicken Sie auf **Weiter**.
- 9 Geben Sie das Zielnetzwerk für das Quellnetzwerk an. Klicken Sie auf **Weiter**.
- 10 Passen Sie die Vorlage für die Bereitstellung an. Geben Sie den gemeinsamen geheimen Schlüssel an, der von der Benutzeroberfläche generiert wurde. Sie müssen die Appliance mithilfe der VM-Konsole manuell konfigurieren. Klicken Sie auf **Weiter**.
- 11 Überprüfen Sie alle Konfigurationsdaten. Klicken Sie auf **Beenden**.
- 12 Sobald die Collector-OVA installiert ist, starten Sie die VM und dann die Konsole.
- 13 Melden Sie sich mit den Konsolenanmeldedaten an, die auf dem Bildschirm angezeigt werden, und führen Sie den `setup`-Befehl aus.

- 14 Erstellen Sie das Kennwort für die *support*-Anmeldung und ändern Sie das Kennwort für den *consoleuser*.

Hinweis

- Ihr Kennwort muss mindestens 6 Zeichen lang sein. Ein einzelnes Anführungszeichen (') ist nicht zulässig.
 - Sie müssen die Kennwörter für *support* und *consoleuser* in regelmäßigen Abständen ändern, um Ihre Organisationsrichtlinie einzuhalten.
-

- 15 Geben Sie die folgenden Details ein, um das Netzwerk zu konfigurieren:

- a **IPv4-Adresse:** Zweite reservierte statische IP-Adresse
- b **Netzmaske:** Subnetzmaske für die obige statische IP-Adresse
- c **Standard-Gateway:** Standard-Gateway Ihres Netzwerks
- d **DNS:** DNS-Server Ihrer Umgebung

Hinweis Stellen Sie für mehrere DNS-Server sicher, dass sie durch Leerzeichen getrennt sind.

- e **Domänensuchliste :** Die Domäne, die für DNS-Lookups angehängt werden muss.
- f Geben Sie *y* ein, um die Konfiguration zu speichern.

- 16 Geben Sie den NTP-Server ein und stellen Sie sicher, dass er von der VM aus erreicht werden kann. Die Dienste können nicht gestartet werden, wenn die NTP-Zeit nicht synchronisiert ist.

Hinweis Stellen Sie bei Angabe mehrerer NTP-Server sicher, dass sie durch Kommata getrennt sind.

- 17 (Optional) So konfigurieren Sie den Webproxy:

- a Geben Sie *y* ein.
- b Geben Sie die Details zum Webproxy an.

- 18 Es wird geprüft, ob der gemeinsame geheime Schlüssel konfiguriert wurde. Der Collector wird mit der entsprechenden Plattform gekoppelt. Dies kann einige Minuten in Anspruch nehmen.

- 19 Alle Dienste werden überprüft.

- 20 Klicken Sie auf **Beenden**, sobald eine **Proxy erkannt!**-Meldung auf der Onboarding-Seite angezeigt wird. Sie werden zur Anmeldeseite weitergeleitet.

Bereitstellung mithilfe des nativen vSphere Windows Clients

Sie können die Collector-OVA von vRealize Network Insight mithilfe des nativen vSphere Windows Clients importieren.

Hinweis vRealize Network Insight 5.2 ist die letzte Version, die die OVA-Bereitstellung mit dem nativen vSphere Windows-Client unterstützt. Ab Version 5.3 können Sie weiterhin den vSphere Web Client zum Bereitstellen von vRealize Network Insight OVA verwenden.

Verfahren

- 1 Klicken Sie auf **Datei > OVF-Vorlage bereitstellen**.
- 2 Geben Sie die URL zum Herunterladen und Installieren des OVA-Pakets aus dem Internet ein oder wählen Sie den Quellspeicherort des OVA-Pakets in Ihrem Computer aus.
- 3 Überprüfen Sie die Details der OVF-Vorlage. Klicken Sie auf **Weiter**.
- 4 Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Akzeptieren**. Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und einen Speicherort für die bereitgestellte Vorlage an. Klicken Sie auf **Weiter**.
- 6 Wählen Sie eine **Bereitstellungskonfiguration** aus. Klicken Sie auf **Weiter**.
- 7 Wählen Sie einen **Host/Cluster** aus, auf dem die bereitgestellte Vorlage ausgeführt werden soll. Klicken Sie auf **Weiter**.
- 8 Wählen Sie den **Ressourcenpool** aus, in dem Sie die Vorlage bereitstellen möchten. Klicken Sie auf **Weiter**.
- 9 Wählen Sie den Zielspeicher für die VM-Dateien aus. Klicken Sie auf **Weiter**.
- 10 Geben Sie das Format an, in dem Sie die virtuellen Festplatten speichern möchten. Wählen Sie **Thin Provisioning** als das Format der virtuellen Festplatte aus. Klicken Sie auf **Weiter**.
- 11 Geben Sie das Netzwerk an, das von der bereitgestellten Vorlage verwendet werden soll. Ordnen Sie das Netzwerk von dem OVA-Paket zu Ihrer Bestandsliste zu.
- 12 Passen Sie die Vorlage für die Bereitstellung an. Geben Sie den gemeinsamen geheimen Schlüssel an, der auf der Onboarding-Seite generiert wurde. Sie müssen die Appliance mithilfe der VM-Konsole manuell konfigurieren. Klicken Sie auf **Weiter**.
- 13 Überprüfen Sie alle Konfigurationsdaten. Aktivieren Sie **Nach der Bereitstellung einschalten**. Klicken Sie auf **Beenden**.
- 14 Sobald die Collector-OVA installiert ist, starten Sie die VM und dann die Konsole.
- 15 Melden Sie sich mit den angegebenen Konsolenanmeldedaten an. Führen Sie den Befehl `setup` aus.
- 16 Erstellen Sie das Kennwort für die `support`-Anmeldung. Ändern Sie das Kennwort für den `consoleuser`.

17 Geben Sie die folgenden Details ein, um das Netzwerk zu konfigurieren:

- a **IPv4-Adresse:** Zweite reservierte statische IP-Adresse
- b **Netzmaske:** Subnetzmaske für die obige statische IP-Adresse
- c **Standard-Gateway:** Standard-Gateway Ihres Netzwerks
- d **DNS:** DNS-Server Ihrer Umgebung

Hinweis Stellen Sie für mehrere DNS-Server sicher, dass sie durch Leerzeichen getrennt sind.

- e **Domänensuchliste:** die Domäne, die für `dns lookup` angehängt werden muss.
- f Geben Sie `y` ein, um die Konfiguration zu speichern.

18 Geben Sie den NTP-Server ein und stellen Sie sicher, dass er von der VM aus erreicht werden kann. Die Dienste können nicht gestartet werden, wenn die NTP-Zeit nicht synchronisiert ist.

Hinweis Stellen Sie bei Angabe mehrerer NTP-Server sicher, dass sie durch Kommata getrennt sind.

19 (Optional) So konfigurieren Sie den Webproxy:

- a Geben Sie `y` ein.
- b Geben Sie die Details zum Webproxy an.

20 Es wird geprüft, ob der gemeinsame geheime Schlüssel konfiguriert wurde. Der Collector wird mit der entsprechenden Plattform gekoppelt. Dies kann einige Minuten in Anspruch nehmen.

21 Alle Dienste werden überprüft.

22 Klicken Sie auf **Beenden**, sobald eine **Proxy erkannt!**-Meldung auf der Onboarding-Seite angezeigt wird. Sie werden zur Anmeldeseite weitergeleitet.

Einrichten eines Network Insight-Collectors (AMI) in AWS für VMware SD-WAN

Sie können einen vRealize Network Insight-Collector für AWS einrichten, indem Sie das Amazon-Maschinen-Image (AMI) in Ihre AWS-Umgebung importieren.

Wenn Ihre Umgebung keinen vCenter Server enthält und Sie Ihren Collector in einer Cloud-Umgebung bereitstellen möchten, können Sie Ihren Collector in AWS bereitstellen.

Hinweis Derzeit unterstützt vRealize Network Insight die Collector-Bereitstellung in AWS, wobei AMI nur für VMware SD-WAN verwendet wird.

Der Vorgang und die Aufgabe im Zusammenhang mit EC2-Instanzen sind unter <https://docs.aws.amazon.com/efs/index.html> dokumentiert.

Verfahren

- 1 Starten Sie Ihre EC2-Instanz mit dem von VMware bereitgestellten AMI in der Amazon EC2-Konsole. Weitere Informationen zur Vorgehensweise finden Sie unter dem Thema „Erstellen Sie Ihre EC2-Ressourcen, und starten Sie Ihre EC2-Instance“ in der Dokumentation zu *Amazon Elastic File System*.

Hinweis Wenn Sie Ihre EC2-Instanz in AWS starten, müssen Sie Folgendes auswählen:

Option	Aktion
Instanztyp	m4.xlarge (MITTELGROSSER BRICK)
Netzwerk	Wählen Sie ein geeignetes Netzwerk und Subnetz aus.
Speicher	Standardspeicher.
Tags	Gemäß Kundenrichtlinien.
Sicherheitsgruppe	Lassen Sie „Ausgehend“ zu 0.0.0.0/0 für Port 443 (oder bei eingeschränkten Regeln „Ausgehend“ für NI SaaS-Prod-FQDN für Port 443) zu.
Schlüssel	Wählen Sie den geeigneten Schlüssel aus (SSH-Anmeldung ist für das AMI aktiviert).

- 2 Wenn sich Ihre EC2-Instanz im Status „Wird ausgeführt“ befindet, melden Sie sich bei Ihrer EC2-Instanz an.
- 3 Melden Sie sich mit den angegebenen Konsolenanmeldedaten an. Führen Sie den Befehl `setup` aus.
- 4 Erstellen Sie das Kennwort für die `support`-Anmeldung. Ändern Sie das Kennwort für den `consoleuser`.

Hinweis Nachdem Sie das Kennwort geändert haben, werden die Netzwerkoptionen während der Einrichtung der Befehlszeilenschnittstelle übersprungen.

Proxy-AMI unterstützt Folgendes nicht:

- Änderung der IP
- IPv6
- Webproxy-Konfiguration

- 5 Geben Sie den NTP-Server ein und stellen Sie sicher, dass er von der VM aus erreicht werden kann. Die Dienste können nicht gestartet werden, wenn die NTP-Zeit nicht synchronisiert ist.

Hinweis Stellen Sie bei Angabe mehrerer NTP-Server sicher, dass sie durch Kommata getrennt sind.

- 6 Es wird geprüft, ob der gemeinsame geheime Schlüssel konfiguriert wurde. Der Collector wird mit der entsprechenden Plattform gekoppelt. Dieser Vorgang kann einige Minuten in Anspruch nehmen.
- 7 Alle Dienste werden überprüft.

Nächste Schritte

Aktivieren Sie die Flow-Erfassung von Edges zu dem Collector, den Sie in AWS bereitgestellt haben. Gehen Sie zum Aktivieren der Flow-Erfassung wie folgt vor:

- Machen Sie den Collector, den Sie in AWS bereitgestellt haben, zu einer Nicht-VeloCloud-Site. Weitere Informationen erhalten Sie vom VMware Support.

Bereitstellen eines zusätzlichen Collectors in einer vorhandenen Anordnung

Sie können einer vorhandenen Anordnung einen zusätzlichen vRealize Network Insight-Collector hinzufügen.

Verfahren

- 1 Melden Sie sich bei der vRealize Network Insight-Benutzeroberfläche an.
- 2 Erweitern Sie **Infrastruktur und Support** und klicken Sie auf **Übersicht und Updates**.
- 3 Scrollen Sie nach unten und klicken Sie auf **Proxy-VM hinzufügen**.
Das Dialogfeld **Neue virtuelle Appliance für Network Insight-Datenerfassung hinzufügen** wird angezeigt.
- 4 Klicken Sie auf **Kopieren**, um den gemeinsamen geheimen Schlüssel aus dem Dialogfeld zu kopieren, und klicken Sie auf **Fertig**.
- 5 Befolgen Sie die Schritte in Abschnitt [Einrichten des Network Insight-Collector \(OVA\)](#) in Schritt 3.

Zugreifen auf vRealize Network Insight unter Verwendung der Evaluierungslizenz

3

vRealize Network Insight wird im NSX-Bewertungsmodus gestartet, wenn Sie die Evaluierungslizenz verwenden.

Sie können eine Datenquelle zu vRealize Network Insight hinzufügen, den Datenverkehrs-Flows analysieren und Berichte generieren.

Hinweis Um zum vollständigen Produktmodus zu wechseln, klicken Sie in der unteren rechten Ecke auf [Zur vollständigen Produktbewertung wechseln](#).

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen von vCenter Server](#)
- [Analysieren von Datenverkehrs-Flows](#)
- [Generieren eines Berichts](#)

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 DVPG* 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 DVPGs 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.

Analysieren von Datenverkehrs-Flows

Sie können mit vRealize Network Insight Flows in Ihrem Datencenter analysieren.

Voraussetzungen

Vor dem Starten der Flow-Analyse müssen mindestens zwei Stunden lang Daten erfasst werden.

Verfahren

- 1 Geben Sie den Geltungsbereich der Analyse an. Wenn Sie sich beispielsweise für Flows aller virtuellen Maschinen in einem **Cluster** interessieren, wählen Sie im Dropdown-Menü „Cluster“ aus. Sie können alternativ alle virtuellen Maschinen auswählen, die mit einem VLAN oder einer VXLAN verbunden sind.
- 2 Wählen Sie den Namen der Einheit, für die Sie die Flows analysieren möchten.
- 3 Wählen Sie die Dauer aus und klicken Sie auf **Analysieren**.

Generieren eines Berichts

Sie können einen Bericht über die Flow-Bewertung generieren.

Voraussetzungen

Analysieren Sie die Datenverkehrsflüsse im Datencenter. Erfassen Sie für umfassende Berichte 24 Stunden an Daten vor der Analyse.

Verfahren

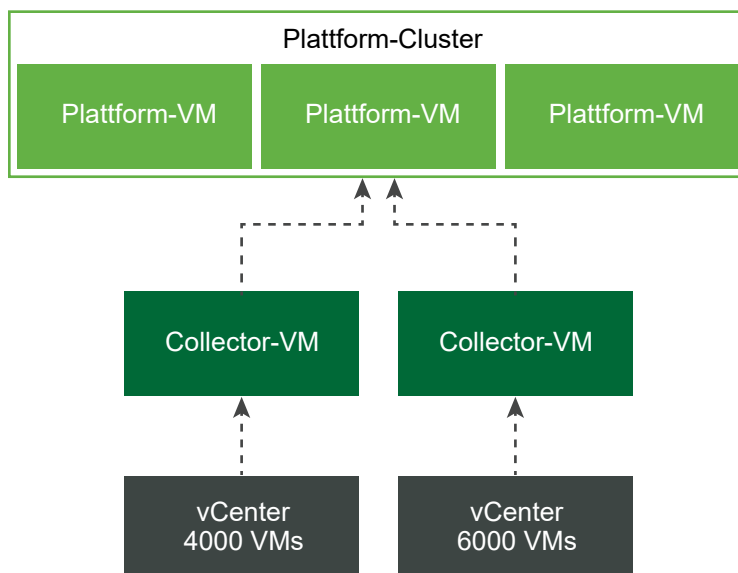
- 1 Klicken Sie in **EVAL NSX-Bewertungsmodus** auf **Bericht erstellen** auf der Seite „Flows analysieren“.
- 2 Klicken Sie im **Nicht-EVAL-Modus** auf der Seite **Mikrosegmentierung** auf **Datenverkehrsverteilung > Weitere Optionen > Bewertungsbericht**.

Planen der vertikalen Hochskalierung Ihrer Bereitstellung

4

Wenn die VM-Anzahl oder die Anzahl der aktiven Flows in Ihrer Anordnung hoch ist oder wahrscheinlich wachsen wird, können Sie die Größe der Plattform oder des Collectors erhöhen.

Sie können zum besseren Verständnis der Plattform und der Collector-Verteilung die folgende Architektur verwenden:



Dieses Kapitel enthält die folgenden Themen:

- [Planen der vertikalen Hochskalierung des Plattform-Clusters](#)
- [Planen der vertikalen Hochskalierung des Collectors](#)
- [Vergrößern der Brick-Größe Ihrer Anordnung](#)

Planen der vertikalen Hochskalierung des Plattform-Clusters

Sie können den Plattform-Cluster vertikal hochskalieren, um die steigende Auslastung zu erfüllen. Je nach Last können Sie entweder vertikal hochskalieren oder einen Plattform-Cluster erstellen oder erweitern. Drei `LARGE`-Plattform-Bricks können miteinander zu einem Plattform-Cluster

verbunden werden. Wenn eine Plattform eine Brick-Größe `LARGE` oder `EXTRA LARGE` aufweist, müssen Sie vertikal hochskalieren, indem Sie einen Plattform-Cluster erstellen.

Informationen zur Entscheidung über die Plattform-Brick-Größe und die Anzahl der Plattform-Bricks finden Sie unter [Systemempfehlungen und -anforderungen](#).

Hinweis Der Plattform-Cluster unterstützt die Hochverfügbarkeitskonfiguration nicht. Alle Plattformknoten müssen betriebsbereit sein, damit der Cluster mit optimaler Leistung funktioniert.

Hochskalieren von Szenarien für den Plattform-Cluster

- Szenario 1: Auf Ihrer Plattform werden 5000 VMs und 1,5 Millionen aktive Flows ausgeführt
Konvertieren Sie Ihre Plattform von `MEDIUM` in `LARGE`. Weitere Informationen hierzu finden Sie unter [Vergrößern der Brick-Größe Ihrer Anordnung](#).
- Szenario 2: Ihre Plattform führt einen einzelnen `LARGE`-Knoten mit 9000 VMs und 2 Millionen aktiven Flows aus
Fügen Sie zwei weitere `LARGE`-Brick-Knoten hinzu, um sie in einen `LARGE`-Brick-Cluster mit 3 Knoten zu konvertieren. Weitere Informationen finden Sie unter *Erweitern von Clustern im vRealize Network Insight-Benutzerhandbuch*.
- Szenario 3: Auf Ihrer Plattform wird ein `LARGE`-Cluster mit 3 Knoten mit mindestens einem Collector, 15000 VMs und 4 Millionen aktiven Flows betrieben.
Konvertieren Sie Ihre vorhandenen Plattformknoten von `LARGE` in `EXTRA-LARGE`. Weitere Informationen hierzu finden Sie unter [Vergrößern der Brick-Größe Ihrer Anordnung](#).
- Szenario 4: Auf Ihrer Plattform wird ein `EXTRA-LARGE`-Cluster mit 3 Knoten mit mindestens einem Collector, 25000 VMs und 8 Millionen aktiven Flows betrieben.
Fügen Sie zwei weitere `EXTRA-LARGE`-Brick-Knoten hinzu, die in einen `EXTRA-LARGE`-Cluster mit 5 Knoten konvertiert werden sollen. Weitere Informationen finden Sie unter *Erweitern von Clustern im vRealize Network Insight-Benutzerhandbuch*.

Planen der vertikalen Hochskalierung des Collectors

Die Collector-Kapazität basiert auf der Brick-Größe. Die Datenquelle, die Sie einem Collector hinzufügen können, hängt von der Kapazität des Collectors (VMs und Flows) ab.

Weitere Informationen hierzu finden Sie unter [Tabelle 1-6. Collector-Bereitstellung – Maximale Kapazität](#). Nachdem ein Collector eine Brick-Größe `LARGE` hat, müssen Sie weitere Collectors hinzufügen. Sie können jeden Collector auf die Größe `EXTRA-LARGE` vertikal hochskalieren.

Sie können einem Collector mehrere Datenquellen basierend auf der unterstützten Collector-Kapazität hinzufügen. Sie können jedoch dieselbe Datenquelle nicht mehreren Collectors hinzufügen.

Vertikale Hochskalieren von Szenarien für die Collectors

- Szenario1: 2000 VMs in einem vCenter

Installieren Sie eine mittelgroße Collector-VM. Fügen Sie das vCenter zu diesem Collector hinzu. Weitere Informationen hierzu finden Sie unter [Hinzufügen von vCenter Server](#).

- Szenario 2: 1000 VMs in vCenter1 und 2000 VMs in vCenter2 (alle befinden sich in einem Datacenter)

Installieren Sie eine mittelgroße Collector-VM. Fügen Sie beide vCenter diesem Collector hinzu. Weitere Informationen hierzu finden Sie unter [Hinzufügen von vCenter Server](#).

- Szenario 3: 1.000 VMs in vCenter1 (Datacenter 1) und 2.000 VMs in vCenter2 (Datacenter 2)

Installieren Sie eine mittelgroße Collector-VM in jedem Datacenter. Fügen Sie vCenter1 einer Collector-VM im selben Datacenter hinzu und fügen Sie vCenter2 zu einer Collector-VM in seinem Datacenter hinzu. Weitere Informationen hierzu finden Sie unter [Hinzufügen von vCenter Server](#).

- Szenario 4: VM-Anzahl überschreitet 4000, aktive Flows überschreiten 2,5 Millionen.

Konvertieren Sie Ihre Collector-VM von `MEDIUM` in `LARGE`. Weitere Informationen hierzu finden Sie unter [Vergrößern der Brick-Größe Ihrer Anordnung](#).

- Szenario 5: 9000 VMs in vCenter1 ohne Flows (Datacenter1)

Installieren Sie eine große Collector-VM. Fügen Sie dieses vCenter zum Collector hinzu. Weitere Informationen hierzu finden Sie unter [Hinzufügen von vCenter Server](#).

- Szenario 6: VM-Anzahl ist kleiner oder gleich 10000, aber der aktive Flow überschreitet 5 Millionen.

Konvertieren Sie Ihre Collector-VM von `LARGE` in `EXTRA-LARGE`. Weitere Informationen hierzu finden Sie unter [Vergrößern der Brick-Größe Ihrer Anordnung](#).

- Szenario 8: zwei vCenter, vCenter1 hat 10000 VMs und 9 Millionen aktive Flows und vCenter2 hat 10000 VMs und 4 Millionen aktive Flows.

Installieren Sie einen `EXTRA-LARGE`- und einen `LARGE`-Proxy. Fügen Sie vCenter1 zu Proxy `EXTRA-LARGE` hinzu und fügen Sie vCenter2 zu Proxy `LARGE` hinzu.

- Szenario 9: ein vCenter, das 10000 VMs und 9 Millionen aktive Flows ausführt.

Installieren Sie einen Proxy `EXTRA-LARGE` und fügen Sie das vCenter dem Proxy hinzu.

Vergrößern der Brick-Größe Ihrer Anordnung

Um Ihren Anforderungen gerecht zu werden, können Sie die Brick-Größe Ihrer Plattform oder die Collector-Appliance von `MEDIUM` auf `LARGE` oder `LARGE` auf `EXTRA-LARGE` ändern.

Verfahren

- ◆ Führen Sie die für Ihre Anordnung relevanten Schritte aus.

Option	Bezeichnung
Für eine Plattform mit einem einzelnen Knoten oder eine neue unabhängige OVA	<ul style="list-style-type: none"> a Melden Sie sich beim vCenter an. b Fahren Sie die Plattform-VM herunter. c Erhöhen Sie die Festplattengröße, den Arbeitsspeicher, die Gesamt-vCPU und die entsprechende Reservierung der VM, um die gleiche Brick-Größe zu erreichen. Weitere Informationen finden Sie auf der Seite „Systemempfehlungen und -anforderungen“. d Starten Sie die Plattform-VM neu.
Für eine Cluster-Plattform	<ul style="list-style-type: none"> a Melden Sie sich beim vCenter an. b Fahren Sie die Plattform-VM in umgekehrter chronologischer Reihenfolge herunter. Beispiel: Herunterfahren von Knoten 3 zu Knoten 1. c Erhöhen Sie die Festplattengröße, den Arbeitsspeicher, die Gesamt-vCPU und die entsprechende Reservierung. Weitere Informationen finden Sie in den Systemempfehlungen und -anforderungen. d Starten Sie die Plattform-VMs in chronologischer Reihenfolge neu. Beispiel: Neustart von Knoten 1 auf Knoten 3.
Für einen Collector	<ul style="list-style-type: none"> a Melden Sie sich beim vCenter an. b Fahren Sie die Collector-VM herunter. c Erhöhen Sie die Festplattengröße, den Arbeitsspeicher, die Gesamt-vCPU und die entsprechende Reservierung der VM, um die gleiche Brick-Größe zu erreichen. Weitere Informationen finden Sie auf der Seite „Systemempfehlungen und -anforderungen“. d Starten Sie die Collector-VM neu.

Upgrade von vRealize Network Insight

5

Sie können ein Upgrade Ihrer aktuellen vRealize Network Insight-Umgebung auf die neueste Version durchführen.

Wichtige Punkte, die vor dem Upgrade berücksichtigt werden sollten:

- Nach dem Upgrade benötigt vRealize Network Insight ca. 12 bis 24 Stunden, um die Daten zu verarbeiten, die sich während des Upgrade-Vorgangs in der Pipeline befanden, und dies auf der Benutzeroberfläche darzustellen.
- vRealize Network Insight unterstützt weder eine Wiederherstellung noch ein Produkt-Downgrade. Sie müssen eine Sicherung durchführen, bevor Sie mit dem Upgrade fortfahren. Weitere Informationen zum Sicherungs- und Wiederherstellungsvorgang finden Sie im KB-Artikel <https://kb.vmware.com/s/article/55829>.
- In einer Cluster-Umgebung müssen Sie den Upgrade-Vorgang nur auf dem Platform1-Knoten durchführen.
- Nach dem Upgrade auf vRealize Network Insight 5.1 werden einige Firewall-Regel-IDs möglicherweise zu den neuen IDs geändert, die von der VMware Cloud on AWS 1.9-API zurückgegeben wurden. Wenn VMware Cloud on AWS 1.8-Firewallregeln vorhanden sind, die an die Flows angehängt sind, kann Folgendes eintreten:
 - Die korrekten oder entsprechenden VMware Cloud on AWS 1.9-Firewallregeln werden unmittelbar nach dem Upgrade für alle aktiven Flows angehängt.
 - Die Firewallregeln beziehen sich auf für die Flows nicht vorhandene Regeln, deren Zeitraum der Inaktivität 24 Stunden vor dem Upgrade von Version 1.8 auf 1.9 übersteigt.

Hinweis Wenn bei der Durchführung des zentralisierten Upgrades Probleme wie z. B. Uploadfehler oder Fehler bei der Benutzeroberfläche auftreten, wenden Sie sich an den VMware Support.

Migration zu FoundationDB

Um Konfigurationsdaten über Datenspeicher im Cluster zu verteilen, ersetzt vRealize Network Insight 5.1 zum Speichern der Konfigurationsdaten PostgreSQL durch FoundationDB. Dadurch kann vRealize Network Insight Folgendes gewährleisten:

- Verringerung der Last auf Platform1-Knoten

- Vermeidung von einzelner Fehlerquelle
- Verbesserung der Robustheit
- Verbesserung der Leistung
- Gleichmäßige Aufteilung der Festplatte über die Clusterknoten hinweg

Im Rahmen des Migrationsvorgangs werden automatisch folgende Aktionen ausgeführt:

- Herunterfahren aller Dienste
- Starten der tabellenweisen Migration von PostgreSQL zu FoundationDB
- Anzeigen der Fortschrittsinformationen zur dynamischen Migration auf der Platform1-Benutzeroberfläche

Die Migrationszeit für das Verschieben von Daten von PostgreSQL zu FoundationDB hängt von der Festplattengeschwindigkeit und der Anzahl der Knoten ab (mehr Knoten bieten mehr Schreibdurchsatz in FoundationDB)

Die Zeit, die zum Abschließen des Migrationsvorgangs benötigt wird, hängt von der Größe der Datenbank ab.

Setupgröße	Datengröße	Knotenanzahl	Typische Migrationszeit
Klein	20 GB bis 40 GB	1 Knoten	1 bis 2 Stunden
Mittel	60 GB bis 100 GB	3 Knoten	7 bis 10 Stunden
Einrichtungen mit einer großen Cloud	500GB	10-Knoten-Cluster	15 bis 20 Stunden
XL (Megatron)	1 TB	10-Knoten-Cluster	35 bis 40 Stunden

Beachten Sie, dass die Migration im Rahmen des vRealize Network Insight-Upgrades erfolgt. Das Upgrade dauert somit möglicherweise länger, was während des Vorgangs auf dem Bildschirm zu sehen ist.

vRealize Network Insight bietet unterschiedliche Upgrade-Modi.

Dieses Kapitel enthält die folgenden Themen:

- [Online-Upgrade](#)
- [Einzelklick-Offline-Upgrade](#)
- [CLI-Upgrade](#)

Online-Upgrade

Wenn eine neue Version von vRealize Network Insight verfügbar ist, erhalten Sie eine Benachrichtigung.

Voraussetzungen

- Die Upgrade-Schritte schlagen möglicherweise fehl, wenn im Verzeichnis `/tmp` nicht genügend Speicherplatz vorhanden ist. Stellen Sie sicher, dass Sie die folgenden Festplattenspeicheranforderungen für Plattform- und Collector-Server erfüllen:
 - `/tmp` – 6 GB
 - `/home` – 2 GB
- Stellen Sie sicher, dass Sie die folgenden Festplattenspeicheranforderungen für Plattform-Server erfüllen:
 - `/` – 6 GB (nur für den Plattform1-Knoten)
 - `/var` – 40 GB
- Stellen Sie sicher, dass Sie die Mindestbandbreitenanforderung von 500 KB/s erfüllen, um das Upgrade-Paket vom Server herunterzuladen. Die Seite **Installation und Support** löst einen Fehler aus, wenn die Download-Bandbreite nicht ausreicht.
- Stellen Sie sicher, dass alle Knoten online sind. Wenn ein Knoten inaktiv ist, dürfen Sie das Upgrade nicht auslösen.
- Erstellen Sie die Snapshots der VMs.
- Beachten Sie die folgenden Werte, die nach der Migration überprüft werden sollten:
 - Anzahl der VMs
 - VM, bei der die Anzahl der Snapshots > 0 ist
 - Anzahl der Firewallregeln
 - Anzahl der Sicherheitsgruppen
 - Anzahl der NSX-Firewalls

Verfahren

- 1 Wenn ein Update verfügbar ist, sehen Sie die Benachrichtigung **Update verfügbar**.

Hinweis

- Wenn die Update-Benachrichtigung nicht verfügbar ist, stellen Sie sicher, dass sowohl die vRealize Network Insight-Plattform- als auch die -Collector-VMs über Konnektivität mit `svc.ni.vmware.com` auf Port 443 und `reg.ni.vmware.com` auf Port 443 verfügen, indem Sie den Befehl `show-connectivity-status` ausführen. Wenn für diese Konnektivität `http proxy` erforderlich ist, konfigurieren Sie es auf jeder VM mithilfe des Befehls `set-web-proxy`. Stellen Sie sicher, dass die Ausgabe den Upgrade-Konnektivitätsstatus `Passed` enthält.
 - Eröffnen Sie ein Support-Ticket und geben Sie das Service-Tag aus der Produkt-Benutzeroberfläche an. Das Service-Tag wird unter **Einstellungen > Info** angezeigt.
 - Melden Sie sich bei der Appliance an und führen Sie den Befehl `show-connectivity-status` aus. Übermitteln Sie einen Screenshot der Befehlsausgabe von jeder vRealize Network Insight-Plattform- und -Collector-VM.
-

- 2 Klicken Sie in der Benachrichtigung `Update verfügbar` auf **Details anzeigen**, um die Update-Details anzuzeigen.

Der Bildschirm „vRealize Network Insight-Upgrade“ wird angezeigt.

- 3 Lesen Sie Anweisungen unter **Bevor Sie fortfahren** und klicken Sie auf **Weiter**.
- 4 Warten Sie bis zum Abschluss der Vorabprüfungen, bei denen Folgendes überprüft wird:
 - Festplattenspeicher, einschließlich des für die Migration erforderlichen Speicherplatzes
 - Version
 - NTP-Synchronisierungsstatus
 - Bandbreite

Sie können in Ihrem Setup die ungefähr erforderliche Zeit bis zum Abschluss des Vorgangs sehen (einschließlich der Migrationsdauer).

- 5 Klicken Sie auf **Jetzt installieren**.

- 6 Nach Beginn des Upgrade-Vorgangs wird im Fenster „vRealize Network Insight-Upgrade“ der Status des Upgrade-Vorgangs angezeigt.

Hinweis

- Wenn ein Knoten inaktiv wird, wird der Upgrade-Vorgang nicht fortgesetzt. Das Upgrade wird erst dann fortgesetzt, wenn der Knoten wieder aktiv ist.
 - Platform1 wird zum Upgrade-Server. Wenn Platform1 offline ist, wird kein anderer Knoten aktualisiert.
 - Nach der Aktualisierung der Plattformen können Sie Ihre normalen vRealize Network Insight-Vorgänge fortsetzen, obwohl das Collector-Upgrade parallel erfolgt. Bis der Upgrade-Vorgang vollständig abgeschlossen ist, wird die `Node Version Mismatch detected`-Meldung auf der Seite „Installation und Support“ angezeigt.
-
- Nach dem Upgrade der Dienste wird Nginx neu gestartet, um den Migrationsvorgang anzuzeigen. Daher ist es möglich, dass Sie für einen kurzen Zeitraum (ein bis zwei Minuten) nicht auf die Benutzeroberfläche zugreifen können.
 - vRealize Network Insight beginnt mit der Migration von Daten zur Foundation-Datenbank. Auf dem Bildschirm „Datenmigrationsstatus“ wird Folgendes angezeigt:
 - Gesamtstatus
 - Vergangene Zeit
 - Status für jede einzelne Tabelle
 - Anzahl der migrierten Datensätze

Bei Problemen können Sie die Option **Migrationsprotokolle exportieren** zur Freigabe für den VMware Support-Team verwenden.
 - Die PostgreSQL-Daten auf den Collectors werden auch als Teil des Upgrade-Vorgangs zu FoundationDB migriert. Der Collector-Migrationsstatus wird jedoch auf der Benutzeroberfläche nicht angezeigt.

- 7 Bei Abschluss des Upgrade-Vorgangs sehen Sie eine Bestätigungsmeldung.

Alle Plattformen und die Collector-Knoten wurden aktualisiert.

Nächste Schritte

- Melden Sie sich bei vRealize Network Insight an und führen Sie Ihre Aufgaben aus.
- Löschen Sie die Snapshots nach zwei oder drei Tagen, um Festplattenspeicher zu sparen.

Einzelklick-Offline-Upgrade

vRealize Network Insight unterstützt das Einzelklick-Offline-Upgrade des Produkts ab Version 3.7 und höher.

Voraussetzungen

- Die Upgrade-Schritte schlagen möglicherweise fehl, wenn im Verzeichnis `/tmp` nicht genügend Speicherplatz vorhanden ist. Stellen Sie sicher, dass Sie die folgenden Festplattenspeicheranforderungen für Plattform- und Collector-Server erfüllen:
 - `/tmp` – 6 GB
 - `/home` – 2 GB
- Stellen Sie sicher, dass Sie die folgenden Festplattenspeicheranforderungen für Plattform-Server erfüllen:
 - `/` – 12 GB (nur für den Plattform1-Knoten)
 - `/var` – 40 GB

Hinweis Der Paket-Upload und die nachfolgenden Upgrade-Schritte schlagen möglicherweise fehl, wenn im Verzeichnis `/tmp` nicht genügend Speicherplatz vorhanden ist.

- Um eine Zeitüberschreitung der UI-Sitzung zu vermeiden, wechseln Sie zu **Einstellungen > Systemkonfiguration > Zeitüberschreitung der Benutzersitzung** und erhöhen Sie den Wert für **Zeitüberschreitung der Benutzersitzung** auf mindestens 2 Stunden. Nachdem Sie die Zeitüberschreitungsdauer für Sitzungen geändert haben, müssen Sie sich erneut beim System anmelden.
- Stellen Sie sicher, dass alle Knoten online sind. Wenn ein Knoten inaktiv ist, dürfen Sie das Upgrade nicht auslösen.
- Erstellen Sie die Snapshots der VMs.
- Beachten Sie die folgenden Werte, die nach der Migration überprüft werden sollten:
 - Anzahl der VMs
 - VM, bei der die Anzahl der Snapshots > 0 ist
 - Anzahl der Firewallregeln
 - Anzahl der Sicherheitsgruppen
 - Anzahl der NSX-Firewalls

Verfahren

- 1 Laden Sie die erforderliche Upgrade-Paketdatei von [My VMware](#) herunter und speichern Sie das Update-Paket auf Ihrer lokalen Festplatte.
- 2 Stellen Sie sicher, dass der `MD5SUM`-Wert des heruntergeladenen Pakets mit dem `MD5SUM`-Wert übereinstimmt, der auf der VMware-Website angegeben ist.
- 3 Wählen Sie auf der Seite **Installation und Support** unter **Softwareversion Hier klicken**.

- 4 Klicken Sie auf **Durchsuchen**, um die Datei auszuwählen und klicken Sie anschließend auf **Hochladen**.

Nach Abschluss des Uploads wird innerhalb von 2–3 Minuten in vRealize Network Insight die Meldung `Paket-Upload abgeschlossen` angezeigt, während die Paketverarbeitung im Hintergrund erfolgt.

Hinweis

- Stellen Sie sicher, dass bis zum Hochladen des Pakets die Sitzung nicht geschlossen wird. Wenn die Sitzung endet, müssen Sie den Upload-Vorgang neu starten.
 - Aktualisieren Sie die Seite nach dem Hochladen des Pakets erst, wenn die Meldung `Update verfügbar` angezeigt wird.
-

- 5 Klicken Sie in der Fehlermeldung `Update verfügbar` auf **Details anzeigen**.

Der Bildschirm „vRealize Network Insight-Upgrade“ wird angezeigt.

- 6 Lesen Sie Anweisung **Bevor Sie fortfahren** und klicken Sie auf **Weiter**.

- 7 Warten Sie bis zum Abschluss der Vorabprüfungen, bei denen Folgendes überprüft wird:

- Festplattenspeicher, einschließlich des für die Migration erforderlichen Speicherplatzes
- Version
- NTP-Synchronisierungsstatus
- Paket

- 8 Klicken Sie auf **Jetzt installieren**.

Sie können in Ihrem Setup die ungefähre Zeit sehen, die zum Abschließen des Upgrade-Vorgangs erforderlich ist.

- 9 Nach Beginn des Upgrade-Vorgangs wird im Fenster „vRealize Network Insight-Upgrade“ der Status des Upgrade-Vorgangs angezeigt.

Hinweis

- Wenn ein Knoten inaktiv wird, wird der Upgrade-Vorgang nicht fortgesetzt. Das Upgrade wird erst dann fortgesetzt, wenn der Knoten wieder aktiv ist.
 - Platform1 wird zum Upgrade-Server. Wenn Platform1 offline ist, wird kein anderer Knoten aktualisiert.
 - Nach der Aktualisierung der Plattformen können Sie Ihre normalen vRealize Network Insight-Vorgänge fortsetzen, obwohl das Collector-Upgrade parallel erfolgt. Bis der Upgrade-Vorgang vollständig abgeschlossen ist, wird die `Node Version Mismatch detected`-Meldung auf der Seite „Installation und Support“ angezeigt.
-
- Nach dem Upgrade der Dienste wird Nginx neu gestartet, um den Migrationsvorgang anzuzeigen. Daher ist es möglich, dass Sie für einen kurzen Zeitraum (ein bis zwei Minuten) nicht auf die Benutzeroberfläche zugreifen können.

- vRealize Network Insight beginnt mit der Migration von Daten zur Foundation-Datenbank. Auf dem Bildschirm „Datenmigrationsstatus“ wird Folgendes angezeigt:

- Gesamtstatus
- Vergangene Zeit
- Status für jede einzelne Tabelle
- Anzahl der migrierten Datensätze

Bei Problemen können Sie die Option **Migrationsprotokolle exportieren** zur Freigabe für den VMware Support-Team verwenden.

- Die PostgreSQL-Daten auf den Collectors werden auch als Teil des Upgrade-Vorgangs zu FoundationDB migriert. Der Collector-Migrationsstatus wird jedoch auf der Benutzeroberfläche nicht angezeigt.

10 Bei Abschluss des Upgrade-Vorgangs sehen Sie eine Bestätigungsmeldung.

Alle Plattformen und die Collector-Knoten wurden aktualisiert.

Nächste Schritte

- Melden Sie sich bei vRealize Network Insight an und führen Sie Ihre Aufgaben aus.
- Löschen Sie die Snapshots nach zwei oder drei Tagen, um Festplattenspeicher zu sparen.

CLI-Upgrade

Ziehen Sie das CLI-Upgrade nur dann in Betracht, wenn weder das Online-Upgrade noch das Ein-Klick-Offline-Upgrade funktionieren. Sie müssen Plattform-VMs vor Collector-VMs aktualisieren. Sie müssen sich jedoch an den VMware-Support wenden, bevor Sie ein Offline-Upgrade mit CLI initiieren.

In einer Cluster-Umgebung müssen Sie den Upgrade-Vorgang nur vom P1-Knoten (Plattform 1) aus durchführen, und die anderen Plattformknoten im Cluster werden automatisch aktualisiert. Sie müssen jedoch für jeden Collector einzeln ein Upgrade durchführen.

Voraussetzungen

- Die Upgrade-Schritte schlagen möglicherweise fehl, wenn im Verzeichnis `/tmp` nicht genügend Speicherplatz vorhanden ist. Stellen Sie sicher, dass Sie die folgenden Festplattenspeicheranforderungen für Plattform- und Collector-Server erfüllen:
 - `/tmp` – 6 GB
 - `/home` – 2 GB
 - `/var` – 40 GB
- Stellen Sie sicher, dass alle Knoten online sind. Wenn ein Knoten inaktiv ist, dürfen Sie das Upgrade nicht auslösen.
- Erstellen Sie die Snapshots der VMs.

- Beachten Sie die folgenden Werte, die nach der Migration überprüft werden sollten:
 - Anzahl der VMs
 - VM, bei der die Anzahl der Snapshots > 0 ist
 - Anzahl der Firewallregeln
 - Anzahl der Sicherheitsgruppen
 - Anzahl der NSX-Firewalls

Verfahren

- 1 Laden Sie die erforderliche Upgrade-Paketdatei von [My VMware](#) herunter.
- 2 Stellen Sie sicher, dass der MD5SUM-Wert des heruntergeladenen Pakets mit dem MD5SUM-Wert übereinstimmt, der auf der VMware-Website angegeben ist.
- 3 Kopieren Sie das Upgrade-Paket auf die Plattform 1-VM und alle Collector-VMs in vRealize Network Insight.

- Um die Datei von der Linux-VM auf die vRealize Network Insight-VM zu kopieren, führen Sie den Befehl `scp <filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/` aus.
- Um die Datei von der Windows-VM auf die vRealize Network Insight-VM zu kopieren, führen Sie den Befehl `pscp -scp <SOURCE_PATH>\<filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/` aus.

Hinweis Verwenden Sie das Dienstprogramm pscp von <https://the.earth.li/~sgtatham/putty/latest/w64/pscp.exe>.

- 4 Melden Sie sich über die Befehlszeilenschnittstelle mit der Rolle `consoleuser` bei Plattform 1 in vRealize Network Insight an und führen Sie die folgenden Befehle aus:
 - `package-installer copy --host localhost --user consoleuser --path /home/consoleuser/<filename>.upgrade.bundle`
 - `package-installer upgrade --name <filename>.upgrade.bundle`

Hinweis Sie müssen zuerst das Plattform-Upgrade durchführen und dann die Collector-Aktualisierung starten.

- 5 Führen Sie den Befehl `package-installer upgrade` erneut aus, nachdem das Setup im Rahmen des Betriebssystem-Upgrades neu gestartet wurde.

Wichtig Wenn Sie einen Zeitüberschreitungsfehler bei der SSH-Sitzung erhalten, müssen Sie das `/var/log/arkin/centralized_upgrade.log` überprüfen, um zu erfahren, ob der Neustart schon durchgeführt wurde. Wenn der Neustart erfolgreich ist, müssen Sie den Befehl `package-installer upgrade` erneut ausführen.

- 6 Melden Sie sich über die Befehlszeilenschnittstelle bei allen Collector-Knoten an und führen Sie das Upgrade mithilfe derselben Befehle durch, die für das Plattform-Upgrade verwendet wurden.

Hinweis Sie können für alle Collectors gleichzeitig ein Upgrade durchführen.

- 7 Überprüfen Sie die aktualisierte Version mit dem Befehl `show-version`.

Deinstallieren von vRealize Network Insight

6

Sie müssen vRealize Network Insight über vSphere Web Client deinstallieren.

Verfahren

- 1 Wenn Sie auf das vRealize Network Insight-Webportal zugreifen können, gehen Sie wie folgt vor:
 - a Melden Sie sich beim Webportal von vRealize Network Insight an.
 - b Wechseln Sie zu **Einstellungen > Konten und Datenquellen**.
 - c Deaktivieren Sie alle Datenquellen und löschen Sie sie.

Durch das Löschen der vCenter-Datenquelle werden IPFIX-Einstellungen (sofern konfiguriert) auf VDS entfernt. Ebenso werden durch das Löschen der NSX Manager-Datenquelle IPFIX-Einstellungen aus dem NSX Flow Monitor entfernt.
- 2 Wenn Sie nicht auf das Webportal von vRealize Network Insight zugreifen können, führen Sie die folgenden Schritte aus:
 - a Wenn Netflow (IPFIX) auf vCenter aktiviert ist, entfernen Sie die Collector-IP-Adresse von vRealize Network Insight aus den VDS/DVPG-IPFIX-Einstellungen. Weitere Informationen hierzu finden Sie unter [Collector-IP entfernen, wenn Netflow in vCenter aktiviert ist](#).
 - b Wenn IPFIX auf NSX aktiviert ist, entfernen Sie die Flow-Überwachungseinstellungen zur Collector-IP von vRealize Network Insight. Weitere Informationen hierzu finden Sie unter [Collector-IP entfernen, wenn Netflow in NSX aktiviert ist](#).
 - c Wenn Netflow auf physischen Switches zum Senden von Netflow an vRealize Network Insight Netflow Collector konfiguriert ist, ändern Sie die Konfiguration bei Switches, um das Senden von Netflow-Informationen zu beenden.
- 3 Wenn bestimmte Firewall- oder Routing-Regeln erstellt wurden, um den Datenverkehr zu und von vRealize Network Insight VMs zu ermöglichen, entfernen Sie diese Firewall-/Routing-Regeln.
- 4 Bereinigen Sie aus Sicherheitsgründen die Anmeldedaten, die zum Konfigurieren von Datenquellen in vRealize Network Insight verwendet werden.
- 5 Fahren Sie alle vRealize Network Insight-Collectors und -Plattform-VMs herunter und löschen Sie sie.

Collector-IP entfernen, wenn Netflow in vCenter aktiviert ist

Wenn Netflow (IPFIX) in vCenter aktiviert ist, verwenden Sie diese Vorgehensweise, um die vRealize Network Insight-Collector-IP aus den IPFIX-Einstellungen für virtuelle dedizierte Server (VDS)/Distributed Virtual Port Group (DVPG) zu entfernen.

Verfahren

- 1 Melden Sie sich bei vSphere Web Client an.
- 2 Wechseln Sie zu **Start > Netzwerk**.
- 3 Wählen Sie im linken Bereich den **VDS** aus und klicken Sie auf **Konfigurieren > Bearbeiten**.
- 4 Entfernen Sie im Feld **Collector-IP-Adresse** die Collector-IP-Details für vRealize Network Insight.
- 5 Entfernen Sie im Feld **Collector-Port** die Port-Details.
- 6 Klicken Sie auf **OK**.
Sie müssen etwa zwei Minuten warten, bevor Sie mit dem nächsten Schritt fortfahren können.
- 7 Wählen Sie den DVPG dieses VDS aus und klicken Sie auf **Konfigurieren > Richtlinien > Bearbeiten**.
- 8 Wählen Sie im Feld **Netflow** die Option **Deaktivieren** aus dem Dropdown-Menü aus.
- 9 Überprüfen Sie Ihre Einstellungen und klicken Sie auf **Anwenden**.

Nächste Schritte

Führen Sie die Schritte für jeden VDS und dessen DVPGs, für den IPFIX zum Entfernen der Collector-IP-Adresse für vRealize Network Insight aktiviert ist, erneut aus.

Collector-IP entfernen, wenn Netflow in NSX aktiviert ist

Wenn Netflow (IPFIX) in NSX aktiviert ist, verwenden Sie dieses Verfahren zum Entfernen von Collector IP Flow Monitoring-Einstellungen in vRealize Network Insight (vRealize Network Insight).

Verfahren

- 1 Melden Sie sich bei vSphere Web Client an.
- 2 Klicken Sie auf **Start > Netzwerk und Sicherheit > Tools > Flow-Überwachung > Konfiguration**.
- 3 Klicken Sie im **Globaler Flow-Erfassungstatus** auf **Deaktivieren**.
- 4 Um die Flow-Verbindung zu deaktivieren, klicken Sie auf **IPFIX**.
- 5 Wählen Sie auf der Registerkarte **IPFIX** die **Collector-IP** aus und klicken Sie auf **Löschen**.
- 6 Wenn keine weiteren IP-Adressen mehr vorhanden sind, klicken Sie auf **Bearbeiten** und deaktivieren Sie das Kontrollkästchen **IPFIX-Konfiguration aktivieren**.

7 Klicken Sie auf **Speichern**.