

Häufig gestellte Fragen zu 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** Info zum Leitfaden mit häufig gestellten Fragen zu vRealize Network Insight 4
- 2** Allgemein 5
- 3** Installation und Konfiguration 8
- 4** Hinzufügen oder Konfigurieren von Datenquellen in vRealize Network Insight 15
- 5** Mikrosegmentierung und Flows 18
- 6** Clustering 20
 - Clustering – Allgemein 20
 - Clustering – Installation und Konfiguration 22
 - Clustering – Skalierung 24
 - Clustering – Bereitstellung 25
- 7** Datenverwaltung und -verarbeitung 29
- 8** IPFIX 31

Info zum Leitfaden mit häufig gestellten Fragen zu vRealize Network Insight

1

Der Leitfaden mit häufig gestellten Fragen zu vRealize Network Insight bietet dem Benutzer häufig gestellte Fragen zu vRealize Network Insight.

Zielgruppe

Diese Informationen sind für Benutzer bestimmt, die mit vRealize Network Insight arbeiten.

Wie erstelle ich ein Support-Paket?

Informationen finden Sie im Abschnitt „Support-Bundle“ *Befehlszeilen-Referenzhandbuch von vRealize Network Insight*.

Wie erstelle ich eine schreibgeschützte Admin-Rolle in Palo Alto Networks Panorama für XML-API-Zugriff?

So fügen Sie eine **Admin**-Rolle für den XML-API-Zugriff hinzu:

- 1 Wählen Sie **Panorama** → **Admin-Rollen** aus.
- 2 Klicken Sie auf **Hinzufügen**, um eine neue Administratorrolle zum Öffnen des Dialogfelds „Admin-Rollenprofil“ hinzuzufügen.
- 3 Im Dialogfeld „Admin-Rollenprofil“
 - a Geben Sie einen Namen für die Rolle ein (z. B. `api-only-admin`).
 - b Wählen Sie die **Rolle** als **Panorama** aus.
 - c Deaktivieren Sie alle Einträge auf der Registerkarte „Web-UI“.
 - d Aktivieren Sie alle Einträge außer **Commit** auf der Registerkarte „XML-API“.
 - e Klicken Sie auf **OK**, um das Dialogfeld zu schließen. Daraufhin wird eine neue **Admin-Rolle** in der Liste mit dem Namen angezeigt.
 - f Klicken Sie auf **Übergeben**, um die Änderungen an Panorama zu übergeben.
- 4 Weisen Sie diese **Admin**-Rolle einem Administratorkonto zu.

Wann wird ein Dienst als freigegeben angesehen?

Die folgenden Ports sind als gemeinsam genutzt konfiguriert:

Protokoll	Port
DNS	53
Bootpc	68
Kerberos	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269

Ich sehe ein Ereignis bzw. einen Fehler in der Datenquelle als „Die Identitätsinformationen der Datenquelle wie z. B. ein Zertifikat oder der Schlüssel haben sich geändert.“ Was bedeutet das?

vRealize Network Insight hat ein neues Zertifikat von einer Datenquelle erhalten, die nicht mit dem im Produkt gespeicherten Zertifikat identisch ist. vRealize Network Insight akzeptiert automatisch das von Datenquellen bereitgestellte Zertifikat. Während des Vorgangs erhalten Sie ein Ereignis in den Datenquellen, in dem Sie alte und neue Zertifikate herunterladen können.

Was ist der Grenzwert für den Import von DNS-Datensätzen in vRealize Network Insight?

Die Grenzwerte für den Import von DNS-Datensätzen sind:

- Infobox-DNS-Datenquelle: Sie können 900.000 Datensätze aus einer einzelnen Datenquelle importieren.
- Manueller DNS-Datensatzimport: Sie können DNS-Datensätze mit mehreren CSV- oder Bind-Dateien importieren, die als ZIP-Datei verpackt sind. Es gibt keine Beschränkung für die Anzahl der Datensätze, die Sie importieren können. es gibt jedoch folgende Upload-Grenzwerte:
 - Anzahl der Dateien in einer einzelnen ZIP-Datei – 25
 - Maximale Größe einer einzelnen ZIP-Datei – 10 MB

Welches sind die Ressourcenanforderungen für vRealize Network Insight?

Informationen zu den Ressourcenanforderungen finden Sie im Installationshandbuch für vRealize Network Insight.

Was passiert, wenn ich während der Proxy-OVA-Bereitstellung für vRealize Network Insight den falschen Schlüssel eingebe?

Der geheime Schlüssel wird während der Proxy-OVA-Bereitstellung für vRealize Network Insight nicht validiert. Die Bereitstellung wird auch mit einem falschen geheimen Schlüssel abgeschlossen. Die Paarbildung kann jedoch fehlschlagen, und der vRealize Network Insight-Proxy wird auf der vRealize Network Insight-Benutzeroberfläche nicht als erkannt angezeigt.

Um den gemeinsamen geheimen Schlüssel zu korrigieren, melden Sie sich bei der Proxy-CLI von vRealize Network Insight an und führen Sie den Befehl „set-proxy-shared-secret“ aus, um den korrekten geheimen Schlüssel festzulegen. Dieser Befehl ersetzt den alten Schlüssel durch den neuen. Die vRealize Network Insight-Plattform erkennt daher den vRealize Network Insight-Proxy und führt die Paarbildung durch.

Wie konfiguriere ich DNS, nachdem die Proxy-OVA von vRealize Network Insight bereitgestellt wurde?

Melden Sie sich bei der Proxy-CLI von vRealize Network Insight an und führen Sie den Befehl „change-network-settings“ aus. Mit diesem interaktiven Befehl wird dem Benutzer eine Option zum Hinzufügen oder Ändern des DNS zur Verfügung gestellt. Danach wird der vRealize Network Insight-Proxy mit dem neuen DNS neu konfiguriert.

Wenn einer der Netzwerkparameter nicht ordnungsgemäß konfiguriert ist, verwenden Sie den Befehl change-network-settings, um die Netzwerkkonfigurationsparameter zu ändern.

Wie finde ich IP-Adresse der Proxy-VM von vRealize Network Insight über die Benutzeroberfläche heraus?

Wechseln Sie zur Seite „Einstellungen“ und wählen Sie die Menüoption „vRealize Network Insight-Infrastruktur“ aus. Die IP-Adresse der vRealize Network Insight-Plattform und der vRealize Network Insight-Proxy-VMs wird angezeigt.

Was soll ich tun, wenn der vRealize Network Insight-Proxy nach der Bereitstellung die Proxy-OVA von vRealize Network Insight in 5 Minuten nicht erkannt wird?

Melden Sie sich bei dem vRealize Network Insight-Proxy mit `consoleuser` an (weitere Informationen finden Sie im Befehlszeilenschnittstellen-Handbuch für vRealize Network Insight) und überprüfen Sie Folgendes:

- Überprüfen Sie den Status der Paarbildung der vRealize Network Insight-Plattform mit dem vRealize Network Insight-Proxy mithilfe des CLI-Befehls `show-connectivity-status`.
- Wenn der Paarbildungsstatus `Passed` angezeigt wird, öffnen Sie die Plattform-Benutzeroberfläche in einem neuen Browserfenster und melden Sie sich zum Überprüfen des Status an.
- Wenn der Paarbildungsstatus `Failed` angezeigt wird, ist der gemeinsame geheime Schlüssel, der während der Bereitstellung der Proxy-OVA von vRealize Network Insight angegeben wurde, möglicherweise falsch. Um dieses Problem zu beheben, verwenden Sie den Befehl `set-proxy-shared-secret`, um den korrekten geheimen Schlüssel festzulegen. Dieser Befehl ersetzt den alten Schlüssel durch den neuen. Die vRealize Network Insight-Plattform erkennt daher den vRealize Network Insight-Proxy.
- Wenn der Befehl `show-connectivity-status` die Netzwerkerreichbarkeit der vRealize Network Insight-Plattform als **Fehlgeschlagen** anzeigt, überprüfen Sie, ob die vRealize Network Insight-Plattform von der vRealize Network Insight-Proxy-VM aus mithilfe des `ping`-Befehls erreichbar ist.
- Wenn es nicht erreichbar ist, überprüfen Sie mit dem Befehl `show-config`, ob NTP, DNS, Gateway und andere Netzwerkparameter ordnungsgemäß konfiguriert sind.
- Wenn einer der Netzwerkparameter nicht ordnungsgemäß konfiguriert ist, verwenden Sie den Befehl `setup`, um die Netzwerkkonfigurationsparameter zu ändern.

Was soll ich tun, wenn ich meine Anmeldedaten vergesse?

Wenn Sie der lokale Benutzer der Benutzeroberfläche sind: Wenden Sie sich an den Administrator der Benutzeroberfläche von vRealize Network Insight, um die Anmeldedaten für Sie zurückzusetzen.

Wenn Sie der Administrator sind: Ab vRealize Network Insight 3.4 können die Anmeldedaten der Benutzeroberfläche mithilfe von `modify-password` in der CLI geändert werden. Weitere Informationen finden Sie im CLI-Handbuch. Wenn Sie mit vRealize Network Insight-Versionen vor 3.4 arbeiten, wenden Sie sich an den Support.

Wie ändere ich das Anmeldekennwort?

So ändern Sie das Anmeldekennwort:

- 1 Wechseln Sie zu **Administrator > Einstellungen** und klicken Sie dann im linken Bereich auf **Mein Profil**.
- 2 Geben Sie auf der Seite **Kennwort ändern** die erforderlichen Informationen ein und klicken Sie auf **Speichern**.

Was soll ich tun, wenn ich den Anmeldebildschirm erhalte, bevor die vRealize Network Insight-Proxy-VM erkannt wird?

- Dies soll so sein, wenn der Browser aktualisiert wird oder die URL in einem neuen Fenster geöffnet wird, bevor der Proxy erkannt wird.
- Melden Sie sich mit den während der Lizenzaktivierung festgelegten Anmeldedaten für den Benutzernamen `admin@local an`.

Unterstützt vRealize Network Insight mehrere vCenter Server/NSX Manager?

Ja, vRealize Network Insight unterstützt mehrere vCenter Server und NSX Manager.

Welche Dienste von vRealize Network Insight benötigen Internetzugang und warum?

vRealize Network Insight unterstützt die Funktion für Remote-Home-Telefonie, die Internetzugang erfordert. Diese Funktion oder Dienste ermöglichen es dem vRealize Network Insight-Team, ein besseres Verständnis der Kundenumgebungen zu erlangen und Probleme proaktiv zu beheben oder zu reparieren. Die folgenden Dienste benötigen Internetzugang:

- Dienst für die automatische Aktualisierung (`svc.ni.vmware.com:443`): vRealize Network Insight verwendet diesen Dienst, um den Remote-Upgrade-Host zu kontaktieren und neu freigegebene Paketarten abzurufen, sobald diese verfügbar sind, und der Benutzer erhält eine Benutzeroberflächen-Benachrichtigung, wenn die Updates verfügbar sind. Dieser Dienst ist standardmäßig aktiviert, Sie können ihn jedoch über die Benutzeroberfläche oder über die CLI mithilfe des Befehls `online-upgrade` deaktivieren.

- **Leistungstelemetriedienst** (`svc.ni.vmware.com:443`): Bestimmte Metriken im Zusammenhang mit wichtigen Diensten und der Leistung von vRealize Network Insight werden in regelmäßigen Abständen erfasst und für vRealize Network Insight hochgeladen. Das Support-Team überwacht diese Metriken und identifiziert alle Anomalien in der Umgebung, damit das Supportteam handeln kann, bevor sie sich auf kritische Dienste auswirken. Dieser Dienst ist standardmäßig deaktiviert, Sie können ihn jedoch über die CLI mit dem Befehl `telemetry` aktivieren/deaktivieren. Weitere Informationen finden Sie hier: <https://kb.vmware.com/s/article/59242>
- **Support-Dienst** (`support2.ni.vmware.com:443`): Dieser Dienst richtet remote gesicherte Tunnel zum vRealize Network Insight-Support-Host ein, mit dem autorisierte Mitarbeiter remote auf Bereitstellungen zugreifen und mit diesen arbeiten können. Er ist standardmäßig deaktiviert und kann über die Benutzeroberfläche sowie die CLI „support-tunnel“ aktiviert/deaktiviert werden.
- **Registrierungsdienst** (`reg.ni.vmware.com:443`): für die Registrierung der-Appliance bei allen externen Diensten. Damit wird die vertrauenswürdige Kommunikation zwischen den oben genannten Diensten aktiviert. Wenn das Setup Zugang zum Internet hat, erfolgt die Registrierung automatisch. In einer isolierten Umgebung kann es mit der CLI „offline-registration“ geschehen (Weitere Informationen finden Sie im CLI-Handbuch). Er ist erforderlich, um den Support-Tunnel zu aktivieren.

Hinweis Wenn sich die vRealize Network Insight-Plattform hinter einem Internet-Proxy befindet, setzen Sie die folgenden Domännennamen und Ports auf die Whitelist:

Tabelle 3-1.

Dienst	URL	Port
Upgrade-Dienst/Metrikdienst	<code>svc.ni.vmware.com</code>	443
Support-Tunnel-Dienst	<code>support2.ni.vmware.com</code>	443
Registrierungsdienst	<code>reg.ni.vmware.com</code>	443

Wie kann der Internetzugriff auf die Appliance deaktiviert werden?

Die folgenden Dienste verwenden sichere Remote-/Internetdienste:

- Dienst für die automatische Aktualisierung
- Leistungstelemetriedienst
- Support-Dienst
- Registrierungsdienst

Informationen zum Aktivieren oder Deaktivieren dieser Dienste finden Sie in den [Welche Dienste von vRealize Network Insight benötigen Internetzugang und warum?](#)FuA. vRealize Network Insight benötigt Internetzugang, wenn einer oder mehrere dieser Dienste aktiviert sind.

Was ist die Portzusammenfassung und welcher Mechanismus wird dafür verwendet?

Die Portzusammenfassung ist integriert, um die flüchtigen Port-Flows zu aggregieren – wie beispielsweise Dynamic FTP, Oracle, MS-RPC usw. Dies hilft bei der Verringerung der Anzahl der Flows im System und bietet eine aggregierte Ansicht für eine hohe Anzahl von Flows, die im Wesentlichen für denselben Dienst gelten.

Der Mechanismus dafür ist wie folgt:

- Für die ersten drei Tage nach dem Erkennen einer `destination_ip` werden wir Zielports auf dieser speziellen IP-Adresse in Buckets von 10.000 zusammenfassen und mit der Erstellung eines port-profile für diese IP-Adresse (Erstellen eines port-profile pro Ziel-IP) beginnen.
- Nach drei Tagen, nachdem wir ein Profil erstellt haben, beginnen wir mit der Zusammenfassung von Portbereichen, bei denen die Portdichte hoch ist (reflektieren Sie das flüchtige Portöffnungsmuster). Die Bereiche selbst sind dynamisch, z. B. 100, 1000, 10.000, und werden erstellt, je nachdem, wie viele Ports geöffnet werden und wie weit verbreitet sie sich im angegebenen Zusammenfassungsbereich befinden.

Hinweis Diese Entscheidung erfolgt unabhängig von jeder Server-IP-Adresse.

- Auf diese Weise können Flows mit hohen Ports ohne Zusammenfassung gemeldet werden, wenn keine offene Aktivität von Massenports stattfindet, und es kann auch eine dynamische Zusammenfassung angewandt werden, wenn eine solche Aktivität stattfindet.
- Das Profil wird ständig zeitlich abgedämpft aktualisiert, um zu berücksichtigen, dass neue Ports geöffnet werden oder ältere nicht mehr verwendet werden.

Wie ändere ich die IP-Adresse, das Gateway oder die Netzmaske, nachdem die vRealize Network Insight-OVA bereitgestellt wurde?

Um die Netzwerkeinstellungen der vRealize Network Insight-Plattform bzw. des -Proxy zu ändern, melden Sie sich bei der CLI an und führen Sie den Befehl `change-network-settings` aus. Dieser interaktive Befehl bietet dem Benutzer die Möglichkeit, die IP-Adresse, das Gateway, die Netzmaske usw. zu ändern, nach der die vRealize Network Insight-Appliance mit neuen Details neu konfiguriert wird.

Hinweis

- Diese Aufgabe muss mithilfe der VM-Konsolensitzung durchgeführt werden, wenn die Appliance am Ende neu gestartet wird.
- Wenn die vRNI-Plattform-IP-Adresse geändert wird und mit Proxys gekoppelt ist, führen Sie auf jeder Proxy-VM diesen CLI-Befehl aus:

```
vrni-proxy set-platform --ip-or-fqdn <New_Platform_IP>
```

Wie wechsele ich von einer Evaluierungslizenz zu einer unbefristeten Lizenz?

Weitere Informationen finden Sie im Abschnitt „Hinzufügen und Ändern einer Lizenz“ im vRealize Network Insight-Benutzerhandbuch.

Wie sind die Lizenzen in vRealize Network Insight gekennzeichnet?

Tabelle 3-2.

Lizenzname	Lizenztyp	Funktionen
Enterprise	Vollständig/Produktion: Sie kann unbefristet oder zeitgebunden sein.	Die folgenden Funktionen sind aktiviert: <ul style="list-style-type: none"> ■ AWS als Datenanbieter ■ Anpassbare Datenaufbewahrungsrichtlinien ■ Infoblox-DNS-Datenquelle ■ Physische IP- und DNS-Zuordnung ■ Analyse
Advanced	Vollständig/Produktion: Sie kann unbefristet oder zeitgebunden sein.	NA

Hinweis Alle Lizenzen sind pro CPU-Socket und CCU (gleichzeitige Benutzer) ermächtigt. Die Evaluierungslizenzen können erneuert oder in **Produktion** mit dem aktualisierten Schlüssel über **Benutzeroberfläche -> Einstellungen-> Info** konvertiert werden. Weitere Informationen finden Sie im Benutzerhandbuch.

Wie kann ich eine Sicherung der VMs in vRealize Network Insight durchführen?

In *VMware Best Practices* können Sie die Sicherung von VMs wie VMware VADP/VDP-API durchführen. Es wird empfohlen, vor dem Erstellen oder Erweitern von Clustern eine Sicherung durchführen.

Hinzufügen oder Konfigurieren von Datenquellen in vRealize Network Insight

4

Was passiert, wenn die Meldung „Zeitüberschreitung bei Anforderung“ beim Hinzufügen von vCenter Server mithilfe der IP-Adresse angezeigt wird?

- Stellen Sie sicher, dass die vCenter Server-IP-Adresse über die vRealize Network Insight-Proxy-VM erreichbar ist.
- Melden Sie sich bei der Proxy-CLI von vRealize Network Insight an und verwenden Sie den Ping-Befehl, um sicherzustellen, dass die IP erreichbar ist, und Telnet, um sicherzustellen, dass der vCenter Server auf Port 443 erreichbar ist.
- Wenn vCenter Server erreichbar ist, wiederholen Sie das Hinzufügen.
- Wenn die IP-Adresse nicht erreichbar ist, überprüfen Sie anhand des Befehls `show-config`, ob das Gateway ordnungsgemäß über die Proxy-VM von vRealize Network Insight konfiguriert wurde.
- Wenn das Gateway falsch ist, korrigieren Sie es mit dem Befehl `setup`.

Was passiert, wenn beim Hinzufügen von vCenter Server die Meldung „IP/FQDN ist ungültig“ angezeigt wird?

- Überprüfen Sie, ob die angegebenen Werte für IP/FQDN für vCenter Server korrekt sind.
- Überprüfen Sie mithilfe des Befehls `ping`, ob der FQDN von der Proxy-VM von vRealize Network Insight aus erreichbar ist.
- Wenn er nicht erreichbar ist, überprüfen Sie, ob der DNS auf der Proxy-VM von vRealize Network Insight mit dem Befehl `nslookup FQDN` und `show-config` ordnungsgemäß konfiguriert ist.
- Wenn der DNS falsch ist, korrigieren Sie ihn mit dem Befehl `setup`.

Welche Rechte benötigt die vRealize Network Insight-Sicherheits- und -Betriebsplattform?

vRealize Network Insight erfordert die VMware vCenter Server-Anmeldedaten mit den folgenden Berechtigungen:

- Distributed Switch: Ändern
- dvPort-Gruppe: Ändern

Was passiert, wenn der Fehler „Benutzer verfügt nicht über die erforderlichen Berechtigungen.“ beim Aktivieren von IPFIX auf der vCenter Server-Datenquellenseite angezeigt wird?

vRealize Network Insight erfordert die VMware vCenter Server-Anmeldedaten mit den folgenden Berechtigungen, um IPFIX zu aktivieren:

- Distributed Switch: Ändern
- dvPort-Gruppe: Ändern

Stellen Sie sicher, dass bereitgestellte VMware vCenter Server-Benutzer über die Berechtigung für den Root-Ordner der vCenter Servers und alle seine untergeordneten Entitäten verfügen, z. B. alle Ordner und alle Datencenter.

Wie häufig werden die Daten aus der Umgebung abgerufen?

Der vRealize Network Insight-Proxy ruft Daten alle 10 Minuten aus der Umgebung ab.

Wie schnell wird die Analyse der Daten nach dem Hinzufügen des vCenter Servers gestartet?

Die Analyse der Daten beginnt sofort, nachdem ein vCenter Server hinzugefügt wurde. Die Produkt-Benutzeroberfläche zeigt ein partielles Bild der Daten innerhalb weniger Minuten. Es kann aber zwei Stunden dauern, bis es abgeschlossen ist.

Hinweis Die Daten des Flow-Datenverkehrs ändern sich kontinuierlich und umfassen mindestens 24 Stunden an Daten in der Analyse.

Wie bereinige ich IPFIX-Einstellungen in vCenter Server, wenn ich vRealize Network Insight-OVAs gelöscht habe?

- Mithilfe von VMware vSphere Web Client: Wechseln Sie zu **Start > Netzwerk > VDS (Name) > Netflow** Einstellungen. Entfernen Sie die Proxy-IP von vRealize Network Insight aus den Collector-Einstellungen.
- Mithilfe des VMware vSphere Windows-Clients: Wechseln Sie zu **Start > Bestand > Netzwerk > VDS (Name) > Einstellungen bearbeiten**. Entfernen Sie die Proxy-IP von vRealize Network Insight aus den Collector-Einstellungen auf der Registerkarte „Netflow“. Dieser Schritt muss für jeden VDS durchgeführt werden, für den IPFIX aktiviert ist.

Wie bereinige ich die IPFIX-Konfiguration in vRealize Network Insight?

Wechseln Sie auf der vRealize Network Insight-Benutzeroberfläche zu **Einstellungen > Datenquellen** und löschen Sie den vCenter Server. Dadurch wird die von vRealize Network Insight vorgenommene IPFIX-Konfiguration entfernt.

Wie lange dauert es, bis nach dem Hinzufügen von VMware NSX Manager in vRealize Network Insight die korrekten Firewallregeln im VM-VM-Pfad angezeigt werden?

Nachdem Sie VMware NSX Manager in vRealize Network Insight hinzugefügt haben, kann es bis zu 24 Stunden dauern, bis die VM in der Firewallregelbeziehung berechnet wird.

Warum kann ich die PNIC im VM-VM-Pfad nicht sehen, nachdem ich VMware vCenter in vRealize Network Insight hinzugefügt habe?

Normalerweise dauert es ca. 2 Stunden, bis vRealize Network Insight den VM-VM-Pfad berechnet hat, nachdem Sie ein VMware vCenter in vRealize Network Insight als Datenquelle hinzugefügt haben. In seltenen Fällen kann es jedoch etwa 8-10 Stunden dauern, bis die PNIC korrekt im VM-VM-Pfad angezeigt wird, nachdem Sie VMware vCenter in vRealize Network Insight hinzugefügt haben.

Was stellen die Zahlen im Pin zur Datenverkehrsverteilung dar?

Der Prozentsatz gibt einen Überblick über die Datenverkehrsverteilung basierend auf der Flow-Analyse.

Tabelle 5-1.

Datenverkehr	Beschreibung
Ost-West (OW)	Ost-West-Datenverkehr als Prozentsatz des Datenverkehrs der gesamten Gruppe
Umgeschaltet (% von OW)	Umgeschalteter Datenverkehr als Prozentsatz des Ost-West-Datenverkehrs
Weitergeleitet (% von OW)	Weitergeleiteter Datenverkehr als Prozentsatz (%) des Ost-West-Datenverkehrs
Innerhalb Host (% von VM-VM)	Datenverkehr mit Quelle und Ziel auf demselben Host als prozentualer Anteil des Datenverkehrs zwischen virtuellen Maschinen
VM zu VM (% von OW)	Datenverkehr von virtueller Maschine zu virtueller Maschine als Prozentsatz des Ost-West-Datenverkehrs
Internet	Internet-Datenverkehr als Prozentsatz des Datenverkehrs der gesamten Gruppe

Wie werden Ports in Flows aggregiert?

Die Portzusammenfassung ist integriert, um die flüchtigen Port-Flows zu aggregieren – wie beispielsweise Dynamic FTP, Oracle, MS-RPC usw. Dies hilft bei der Verringerung der Anzahl der Flows im System und bietet eine aggregierte Ansicht für eine hohe Anzahl von Flows, die im Wesentlichen für denselben Dienst gelten. Der Mechanismus hierfür lautet wie folgt:

- Für die ersten drei Tage nach dem Erkennen einer „destination_ip“ werden wir Zielports auf dieser speziellen IP-Adresse in Buckets von 10.000 zusammenfassen und mit der Erstellung eines port-profile für diese IP-Adresse beginnen.

- Sobald drei Tage vorüber sind – und wir ein Profil erstellt haben, das ruhigen Gewissens verwendet werden kann – werden wir mit der Zusammenfassung von Portbereichen beginnen, bei denen die Portdichte hoch ist (d. h., das flüchtige Portöffnungsmuster berücksichtigt wird). Die Bereiche selbst sind dynamisch, z. B. 100, 1000, 10.000, und werden erstellt, je nachdem, wie viele Ports geöffnet werden und wie weit verbreitet sie sich im angegebenen Zusammenfassungsbereich befinden.
- Auf diese Weise können Flows mit hohen Ports ohne Zusammenfassung gemeldet werden, wenn keine offene Aktivität von Massenports stattfindet, und es kann auch eine dynamische Zusammenfassung angewandt werden, wenn eine solche Aktivität stattfindet.
- Das Profil wird ständig zeitlich abgedämpft aktualisiert, um zu berücksichtigen, dass neue Ports geöffnet werden oder ältere nicht mehr verwendet werden.

Was bedeutet die IP-Adresse 240.240.240.240 in vRealize Network Insight?

240.240.240.240 ist eine Platzhalter-IP-Adresse in vRealize Network Insight. Diese IP-Adresse wird verwendet, wenn eine sehr große Anzahl von IP-Adressen (> 5000) auf eine bestimmte IP-Adresse trifft. Alle weiteren eingehenden Internet-IP-Adressen (ab der 5001. aufwärts) mit dieser Platzhalter-IP-Adresse 240.240.240.240 können für diesen Dienstendpunkt ersetzt werden.

Dadurch wird die Anzahl der Flows im System begrenzt, da der öffentlich offen gelegte Dienst, der jeden Internet-Client einzeln protokolliert, zu einer sehr großen Anzahl von Flows führen kann, was zu einer erhöhten Systemlast führen würde.

Für alle Flows, die durch diese Platzhalter-IP-Adresse ersetzt wurden, werden alle Metriken auf dem entsprechenden Flow mit dieser IP-Adresse aggregiert, sodass Statistiken auf aggregierter Ebene nicht verloren gehen.

Alle Ziel-IP-Adressen für die in der Flow-Ansicht gemeldeten Flows werden als ausgehend von 240.240.240.240 angezeigt und sind tatsächlich von einer großen Anzahl von Internet-IP-Adressen (> 5000) betroffen.

Dieses Kapitel enthält die folgenden Themen:

- [Clustering – Allgemein](#)
- [Clustering – Installation und Konfiguration](#)
- [Clustering – Skalierung](#)
- [Clustering – Bereitstellung](#)

Clustering – Allgemein

Kann eine Proxy- oder Collector-VM geclustert werden?

Nein. Clustering für Collector-/Proxy-VMs wird nicht unterstützt.

Benötigt vRealize Network Insight einen Lastausgleichsdienst wie vRealize Log Insight?

vRealize Network Insight-Clustering ist eine skalierbare Lösung und keine HA-Lösung. Wenn die primäre Plattform-VM bzw. der Master-Knoten ausfällt, ist der gesamte Dienst nicht mehr verfügbar.

Was passiert, wenn die Verbindung zwischen dem Remote-Proxy und der Plattform ausfällt?

Wenn die Verbindung zwischen der Plattform- und der Proxy-VM ausgefallen ist, speichert die Proxy-VM Daten lokal (je nach Festplattenspeicher) und sendet sie, sobald Sie wieder verbunden ist.

Ist vRealize Log Insight in vRealize Network Insight integriert?

Ja, vRealize Log Insight wurde in vRealize Network Insight 3.4 integriert. Die Warnungen werden an Syslog gesendet, die von vRealize Log Insight kommen können.

Was passiert, wenn ein Knoten neu gestartet wird?

Wenn ein Knoten neu gestartet wird, wird er automatisch dem Cluster hinzugefügt und ist weiterhin betriebsbereit. Wenn es sich um den primären Knoten handelt, ist der Dienst während der Zeit, in der er ausgefallen ist, vollständig verloren.

Wie kann die IP-Adresse eines beliebigen Plattformknotens oder eines Collectors in einem Cluster geändert werden?

In einem Cluster können Sie mithilfe der Befehlszeilenbefehle die IP-Adresse jedes beliebigen Collectors oder Plattformknotens ändern.

Hinweis

- Wenden Sie sich vor dem Durchführen dieses Vorgang an den VMware Support.
 - Die Appliance wird am Ende des Prozesses neu gestartet. Daher müssen Sie diese Schritte auf der VM-Konsole durchführen.
-
- Führen Sie zum Ändern der IP-Adresse des Collectors den Befehl `change-network-settings` aus.
 - So ändern Sie die IP der Plattform:
 - a Führen Sie den Befehl `change-network-settings` aus.
 - b Führen Sie den Befehl `update-IP-change` auf allen anderen Plattformen aus, damit die neue IP angezeigt wird.
 - c Führen Sie den Befehl `show-connectivity-status` auf einem Collector aus und suchen Sie nach **IP/URL der Plattform-VM**, um herauszufinden, ob sie mit dieser Plattform verknüpft ist.
 - d Führen Sie `vrni-proxy` aus, damit die neue Plattform-IP auf den zugehörigen Collectors angezeigt wird.

Anwendungsbeispiel 1: In einem Cluster mit drei Knoten wird nur die IP von platform2 geändert. Es wird kein Collector als zugehörig angezeigt.

- 1 Führen Sie `change-network-settings` auf platform2 aus.
- 2 Führen Sie `update-IP-change` auf platform1 und platform3 aus, damit die neue IP-Adresse von platform2 berücksichtigt wird.

Anwendungsbeispiel 2: In einem Cluster mit drei Knoten werden die IPs von platform1 und platform2 geändert. CollectorA ist platform2 zugeordnet, der Rest ist platform3 zugeordnet.

- 1 Führen Sie `change-network-settings` auf platform1 aus.
- 2 Führen Sie `change-network-settings` auf platform2 aus.
- 3 Führen Sie `update-IP-change platform1-oldIP platform1-newIP` auf platform2 und platform3 aus.

- 4 Führen Sie `update-IP-change platform2-oldIP platform2-newIP` auf `platform1` und `platform3` aus.
- 5 Führen Sie `vrni-proxy set-platform --ip-or-fqdn platform2-newIP` auf `CollectorA` aus.

Wie viel Festplattenspeicher wird auf Platform1 benötigt?

Platform1 benötigt im Vergleich zu anderen Knoten im Cluster mehr Festplattenspeicher, da einige Konfigurationsdaten nur auf Platform1 gespeichert werden.

Was passiert, wenn auf einem der Knoten nicht genügend Festplattenspeicher zur Verfügung steht?

Die Benutzeroberfläche beginnt mit der Anzeige von Fehlermeldungen, wenn der Festplattenspeicher auf einem bestimmten Plattformknoten einen bestimmten Schwellenwert erreicht. Fügen Sie dem Plattformknoten mehr Festplattenspeicher hinzu, indem Sie sich bei vCenter anmelden.

Wie oft werden Daten im Cluster repliziert?

Der Datenreplizierungsmechanismus hängt von den Komponenten ab, die im Plattformknoten vorhanden sind.

Clustering – Installation und Konfiguration

Müssen sich alle Plattform-VMs im selben L2/L3-Segment befinden?

Nein. Es ist jedoch am besten, alle Plattformknoten in einem gemeinsamen Netzwerk mit niedrigen Latenzen zwischen Knoten zu behalten. Dies liegt daran, dass viele der verteilten Komponenten Daten auf den Knoten replizieren und hohe Latenzen zu Problemen bei der Systemleistung und Stabilität führen können.

Kann für ein Cluster mithilfe einer produktbezogenen Upgrade-Funktion ein Upgrade durchgeführt werden?

Online-Upgrades werden für Cluster bis 3.7 nicht unterstützt. Ab 3.8 und den nachfolgenden Versionen kann ein Cluster mithilfe der Online-Upgrade-Methode aktualisiert werden.

Was passiert, wenn während des Cluster-Erstellungsvorgangs ein Fehler auftritt?

Es wird empfohlen, primäre Plattform- und Proxy-Snapshots vor dem Starten des Cluster-Erstellungsvorgangs zu erstellen. Wenn ein Fehler auftritt, löschen Sie die sekundären Plattformknoten und stellen Sie die primären Plattform- und Proxy-VMs aus den Snapshots wieder her.

Was geschieht mit den vorhandenen Daten und der Konfiguration, wenn ich die Bereitstellung mit einem einzelnen Knoten auf einen Cluster ausweite?

Alle Daten und die Konfigurationen werden ohne Änderungen beibehalten. Die Daten kann nach der Erstellung des Clusters abgerufen werden.

Können Sie Plattform-VMs in unterschiedlichen Regionen haben?

Nein, die-Plattformknoten müssen sich an derselben Site befinden. Die Proxy-Server können geografisch verteilt sein.

Kann die Plattform auf vSAN Stretch-Clustern gehostet werden (2 Datacenter...)?

Ja, vSAN-Cluster innerhalb derselben Datacenter oder über mehrere Datacenter hinweg würden weiterhin eine gewisse E/A-Leistung wie lokaler Speicher sicherstellen.

Können wir Clusterknoten auf unterschiedlichen vSAN-Clustern hosten?

Ja, verschiedene Knoten eines Plattform-Clusters können auf unterschiedlichen, zugrunde liegenden Datenspeichern gehostet werden.

Müssen Plattformknoten gesichert werden?

Ja, Sicherungen müssen mit von VMware empfohlenen Snapshot/Backup-Technologien erstellt werden.

Wie kann die Bandbreite zwischen der Cluster-Proxy-VM in einer Region und dem Plattform-VM-Cluster in einer anderen Region geschätzt werden?

In einigen großen Bereitstellungen haben wir bemerkt, dass diese Zahl von 1 MBit/s bis 20 MBit/s reicht. Ein Großteil der Deduplizierung oder Komprimierung wird in der Proxy-VM durchgeführt, bevor Daten an die Plattform-VM gesendet werden.

Wie viel Netzwerkdatenverkehr wird zwischen Clusterknoten stattfinden?

Der Datenverkehr hängt in der Regel von der Größe des Clusters und des Typs der Datacenter-Umgebung ab.

Für Installationen mit 30.000 bis 50.000 VMs:

- Zwischen Clustern: ca. 50–400 MBit/s
- Zwischen Proxy und Plattform: ca. 100 KBit/s–15 MBit/s

Was ist die maximal zulässige Latenz zwischen Knoten in einem Cluster?

Die Plattformknoten müssen sich auf derselben Site befinden. In solchen Fällen ist die Latenz minimal. Wenn die Plattformknoten auf vSAN-Stretch-Clustern (zwei Datacentern) gehostet werden, stellen die vSAN-Cluster innerhalb der Cluster oder über die Cluster hinweg eine gewisse E/A-Leistung wie lokaler Speicher sicher. Die Anwendungen, die auf Datacentern ausgeführt werden, wie z. B. vRealize Network Insight, funktionieren gut. Sie können verschiedene Knoten eines Plattform-Clusters auf unterschiedlichen, zugrunde liegenden Datenspeichern hosten. Sie müssen jedoch sicherstellen, dass sich alle Plattform-VMs in einem Cluster innerhalb derselben Site befinden.

Was ist die maximal zulässige Latenz zwischen den Proxy-VMs in einer Region und dem Plattform-VM-Cluster in einer anderen Region?

Sie können geografisch verteilte Proxys in Ihrem Setup haben. Es ist eine HTTPS-Verbindung von der Proxy-VM zu einer Plattform-VM vorhanden, sodass hohe Latenzen in einer Reihenfolge von wenigen Sekunden toleriert werden können. vRealize Network Insight unterstützt maximal 10 Knoten in einem Cluster (30.000 VMs mit Flows oder 50.000 VMs ohne Flows).

Welche Größe sollte die Proxy-/Plattform-VM haben?

Verwenden Sie eine umfangreiche Brick-Konfiguration: siehe Installationshandbuch.

Clustering – Skalierung

Kann ich einen bereits erstellten Cluster erweitern?

Ja, die Erweiterung eines Clusters wird auf bis zu 10 Knoten unterstützt.

Was passiert, wenn eine nicht primäre Plattform-VM nicht mehr verfügbar ist?

Interne Dienste haben eine eingeschränkte Widerstandsfähigkeit gegenüber nicht primären Knotenfehlern. Im Allgemeinen büßt NI aufgrund eines Knotenfehlers Rechenleistung ein.

Welche Art Lastausgleich wird unterstützt?

Die Zuordnung von Proxy zu Plattform ist fest. Sobald Daten von einer beliebigen Proxy-VM eine beliebige Plattform-VM erreicht haben, wird ihre Verarbeitung lastenmäßig intern auf alle Plattform-VMs verteilt.

Erhöht sich durch die Erstellung eines Plattform-Clusters der Bandbreitenverbrauch?

Die Proxy- oder Collector-VMs kommunizieren weiterhin nur mit der primären oder der Plattform-VM. Die Bandbreitenanforderung für die Plattform-VM-Clustering-Kommunikation ist minimal. Daher wird der Bandbreitenverbrauch nicht deutlich erhöht.

Wie hoch ist die Häufigkeit der Datenübertragung zwischen der Proxy-VM und der Plattform-VM?

Die Proxy-VM sendet die deduplizierten oder komprimierten Daten kontinuierlich an die Plattform-VM.

Erfolgt eine Optimierung der Daten in der Proxy-VM?

Verschiedene Deduplizierungen, Komprimierungen, Verkürzungen oder Batch-Schritte werden in der Proxy-VM durchgeführt. Wenn die Verbindung zwischen der Plattform-VM und der Proxy-VM unterbrochen wurde, speichert die Proxy-VM Daten lokal (je nach Festplattenspeicher) und sendet sie, wenn die Verbindung wiederhergestellt wird.

Wird für die Netzwerkbandbreite eine Optimierung durchgeführt?

Ja, verschiedene Schritte zur Deduplizierung/Komprimierung/Reduzierung/Batchverarbeitung werden auf der Proxy-VM durchgeführt.

Ist das Clustering auf den Proxy-Servern möglich?

Nein. Das Clustering ist auf den Proxy-Servern nicht möglich.

Wie sendet vCenter den Datenverkehr an den Proxy-Server?

vCenter senden keinen Datenverkehr an den Proxy-Server. Die Proxy-Server stellen tatsächlich eine Verbindung mit Ihrem festgelegten vCenter her, um die Informationen abzurufen.

Wie sendet vCenter bei der Bereitstellung eines Clusters Datenverkehr an die verschiedenen Proxy-Server?

Tatsächlich werden Proxys mit vCenter verbunden, um die Informationen abzurufen. Der entsprechende Proxy stellt eine Verbindung zu dem angegebenen vCenter her und ruft die Informationen ab. Auf dem Proxy ist kein Clustering verfügbar.

Clustering – Bereitstellung

Wie kann ich nach der horizontalen Skalierung des Clusters auf die Benutzeroberfläche zugreifen?

Der Zugriff auf die Benutzeroberfläche ist nur von Plattform1 beschränkt.

Was ist Plattform1 und warum muss ich mich an diesen Knoten erinnern?

Der Plattformknoten, von dem der Cluster-Erstellungsprozess initiiert wird, wird als **Plattform1** behandelt. Auf die Benutzeroberfläche sollte nur von diesem Knoten aus den n Knoten im Cluster zugegriffen werden.

Wie werden Daten von den anderen Knoten in einem Cluster abgerufen, wenn der Zugriff auf die Benutzeroberfläche auf Plattform1 beschränkt ist?

Die Daten des Datencenters werden auf alle Knoten in einem Cluster verteilt. Und wenn die Benutzeroberflächenebene Daten auf Plattform1 anfordert, ruft der Plattform1-Knoten die auf allen Knoten gespeicherten Daten ab und sendet eine Antwort an die Benutzeroberfläche.

Kann ich einen Plattformknoten verwenden, der in einem anderen Datacenter zum Erstellen von Clustern bereitgestellt wird?

Alle Knoten in einem Cluster tauschen Daten untereinander aus. Um Latenzprobleme zu vermeiden, wird daher empfohlen, die im selben Datacenter bereitgestellten Plattformknoten zum Erstellen eines Clusters zu verwenden.

Was geschieht mit Daten auf einer vorhandenen Plattform, wenn ich den Plattformknoten horizontal skaliere?

Die Daten auf einem vorhandenen Plattformknoten werden beibehalten und über alle Knoten in einem Cluster verteilt.

Spielt die Anzahl der Proxy-VMs eine Rolle bei der Bestimmung, wie viele Plattform-Bricks ich benötige?

Nein. Nur die Gesamtzahl der VMs in allen vCenter-Instanzen und der Status der Flows (aktiviert oder deaktiviert) haben Auswirkungen auf die Anzahl der benötigten Bricks. Weitere Informationen dazu erhalten Sie in der Brick-Modelltabelle im *Installationshandbuch zu vRealize Network Insight*.

Hat die Anzahl der vCenter oder die Anzahl der physischen Geräte (wie z. B. Router) oder anderer Datenquellen einen Einfluss auf die Anzahl der benötigten Plattform-Bricks?

Nein. Nur die Gesamtzahl der VMs in allen vCenter-Instanzen und der Status der Flows (aktiviert oder deaktiviert) haben Auswirkungen auf die Anzahl der benötigten Bricks. Weitere Informationen dazu erhalten Sie in der Brick-Modelltabelle im *Installationshandbuch zu vRealize Network Insight*.

Unterstützt vRNI Plattform-Cluster, die über 2 Datacenter verteilt sind, aus HA-Gründen?

Nein. Der Plattform-Cluster unterstützt nicht das Splitten zwischen Datacentern. Alle Plattform-Cluster-VMs müssen sich auf derselben Site befinden. Der Plattform-Cluster unterstützt HA derzeit nicht. Die Funktion befindet sich in der Roadmap. Die Kunden können SRM für HA in Verbindung mit DR über 2 Sites hinweg verwenden.

Unterstützt vRNI ein einzelnes vCenter mit mehr als 6000 VMs und aktivierten Flows?

Bis zu Version 3.5 unterstützen die vRNI-Proxys nicht die Erfassung von Daten aus einem einzelnen großen vCenter mit über 6000 VMs mit Flows. Diese Funktion befindet sich in der Roadmap.

Wie viel Festplattenspeicher wird auf Plattform1 benötigt?

Plattform1 benötigt im Vergleich zu anderen Knoten im Cluster mehr Festplattenspeicher, da einige Konfigurationsdaten nur auf Plattform1 gespeichert werden.

Was passiert, wenn auf einem der Knoten nicht genügend Festplattenspeicher zur Verfügung steht?

Die Benutzeroberfläche beginnt mit der Anzeige von Fehlermeldungen, wenn der Festplattenspeicher auf einem bestimmten Plattformknoten einen bestimmten Schwellenwert erreicht. Fügen Sie dem Plattformknoten mehr Festplattenspeicher hinzu, indem Sie sich bei vCenter anmelden.

Wie oft werden Daten im Cluster repliziert?

Der Mechanismus für die Datenreplikation hängt von den Komponenten ab, die im Plattformknoten vorhanden sind.

Wie funktionieren die Cluster?

- Alle Proxys in einer Bereitstellung stellen eine Verbindung mit einer Plattform (Plattform1) her. Die Konnektivität zwischen Plattform und Proxy erfolgt über HTTPS auf Port 443. Daher ist nur Port 443 für Proxys von Plattform1 aus sichtbar.
- Nach dem Empfang der Anforderungen vom Proxy verteilt der Plattform1-Knoten die Last der Anforderungen an andere Plattformknoten im Cluster in Round-Robin-Manier.
- Der Plattformknoten normalisiert die Daten und platziert Sie in der Messaging-Warteschlange für die Verarbeitung durch die Berechnungs-Engine.
- Die Berechnungs-Engine verteilt die Daten mithilfe des Datenreplizierungsmechanismus über alle Knoten im Cluster. Auf diese Weise tritt kein Datenverlust auf, wenn einer der Knoten (außer Plattform1) im Cluster ausfällt.

- Einige Konfigurationsdaten werden explizit auf Platform1-Knoten gespeichert, die nicht repliziert werden. Aus diesem Grund wird die Hochverfügbarkeitslösung nicht unterstützt.

Wie verhält sich die Datenverarbeitungs-Pipeline in Randbedingungen, z. B. wenn die Kommunikation des Plattform-Proxy-Servers unterbrochen wird?

- Wie lange ist der Standard-Aufbewahrungszeitraum?

30 Tage. Er kann über die Benutzeroberfläche mit der Enterprise-Lizenz erweitert werden.
Hinweis: Achten Sie beim Erweitern darauf, die Festplattenrichtlinien zu befolgen.

- Wie werden die Daten auf dem Proxy verarbeitet?

Alle Daten auf dem Proxy werden in SDM (Selbstbeschreibende Meldung) konvertiert, bevor sie an die Plattform einschließlich der Flow-Daten gesendet werden. Sie enthalten alle Konfigurations-, Bestandslisten- und Metrikdaten aus jeder Datenquelle. Wenn die Plattform nicht erreichbar ist oder der SDM-Upload in die Kafka-Warteschlange fehlschlägt, werden sie auf der Proxy-VM (unter /var/BLOB_STORE) auf die Festplatte geschrieben.

- Wann beginnt die Bereinigung von Daten auf dem Proxy?

Für Nicht-Flow-Daten: Es sind 10 GB an Speicherplatz für die Speicherung von SDMs auf der Festplatte (BLOB_STORE) zugeteilt. Wenn dieser Speicher gefüllt wird, beginnt der Collector mit dem Löschen älterer SDMs und fügt der Festplatte neue SDMs hinzu. Es hängt von der Größe der Daten ab, die von allen Datenquellen erfasst werden, wie schnell dieser Grenzwert überschritten wird.

Für Flow-Daten: Es sind 15 GB an Speicherplatz für die Speicherung von Raw-Flows (unter /var/flows/vds/nfcapd) zugeteilt. Sobald dieser Speicherplatz belegt ist, beginnt der Flow-Prozessor mit dem Löschen älterer Flow-Dateien. Bei eingehender Raw-Flow-Rate von etwa 2M/min würde es ungefähr 10 Stunden dauern, bis mit der Rotation begonnen wird.

- Was ist die Bereinigungslogik?

Die ältesten SDMs werden zuerst gelöscht.

- Wann werden neue Daten nicht mehr im Proxy verarbeitet?

Niemals, solange die Dienste ordnungsgemäß ausgeführt werden.

- Würden unter der Annahme einer Trennung zwischen Plattform und Proxy und dass keine Bereinigungsbedingung erfüllt wird, alle Daten auf der Plattform bei der erneuten Verbindung abgeglichen?

Alle auf der Festplatte gespeicherten Daten werden an die Plattform gesendet. Sie sollten vollständig abgestimmt werden, außer wenn Datenverlustbedingungen auf der Plattform vorhanden sind (Weitere Informationen unten).

- Welche Bedingungen können zu Datenverlusten auf der Plattform führen?

Die Plattform beginnt damit, SDMs abzulegen, die sich für mehr als 6 Stunden (18 Stunden, wenn es sich um einen Cluster mit 3 Knoten handelt) in der Kafka-Warteschlange befinden. Eine weitere Möglichkeit besteht, wenn die Warteschlange gesättigt ist. Es kann passieren, wenn im System eine Verzögerung aufgebaut wird und die Rate der eingehenden Daten hoch ist.

- Wird die neueste SDM zuerst oder die früheste in dieser Reihenfolge veröffentlicht?

Die ältesten SDMs werden zuerst gesendet. Es gibt ein bekanntes Problem bis v3.9, das zu einem Datenverlust führt. Wenden Sie sich an GSS, um weitere Informationen zu erhalten.

- Werden Daten auf der Festplatte im Proxy gespeichert und dann auf die Plattform verschoben, wenn kein Kommunikationsproblem vorliegt?

Wenn kein Kommunikationsproblem vorliegt, werden SDMs nicht auf der Festplatte gespeichert. Sie werden aus dem Arbeitsspeicher selbst an die Plattform gesendet. Wenn der Proxy informiert wird, dass ein Problem beim Senden von SDM aufgetreten ist, werden sie nur auf der Festplatte gespeichert.

- Wie erkennt der Proxy bei einem Problem, welche Flow-Datei zuletzt verarbeitet wurde?

Der Flow-Prozessor verwaltet Lesezeichen in der DB, in der die zuletzt verarbeitete nfcapd-Datei war.

- Was ist die maximale Größe von SDM, die ohne Probleme verarbeitet werden kann? Wie kann der Benutzer von dieser Überschreitung erfahren?

Es gibt einen Grenzwert von 15 MB für die SDM-Größe. Ab v3.9 wird ein Ereignis ausgelöst, wenn die Plattform ein großes SDM ablegt.

Was ist IPFIX?

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 der 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. Dies wird häufig als Netflow bezeichnet. IPFIX ist jedoch das Standard-IETF-Protokoll.

Welche Flow-Informationen werden vom VDS exportiert?

Ein VDS in einer vSphere-Umgebung kann für den Export von Flow-Informationen mithilfe von IPFIX konfiguriert werden. Aktivieren Sie die Flow-Überwachung für alle Portgruppen, die an den VDS angehängt sind. Wenn Pakete auf Port X eines VDS ankommen und Port Y verlassen, wird ein entsprechender Flow-Datensatz ausgegeben, wenn die Flow-Überwachung auf Port Y aktiviert ist. Die Richtung jedes Flow-Datensatzes wird auf „Egress“ festgelegt.

Wie verwendet vRealize Network Insight IPFIX?

vRealize Network Insight verwendet VMware VDS IPFIX, um Daten zum Netzwerkdatenverkehr zu erfassen. Jede Sitzung verfügt über zwei Pfade. Beispiel: Session A ↔ C hat A → C-Pakete und C → A-Pakete. Um die vollständigen Informationen einer Sitzung zu analysieren, werden 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.

Wie behebe ich Probleme bei der vRealize Network Insight Flow-Erfassung?

- 1 Stellen Sie sicher, dass für den spezifischen VDS und seine DVPGs- und Uplink-Eigenschaften Netflow-Überwachung **aktiviert** ist und die IP-Adresse des Collectors die des vRealize Network Insight Collector ist.
- 2 IPFIX Netflow-Pakete werden zwischendurch eine Firewall (NSX, virtuell oder physisch) verworfen. Stellen Sie sicher, dass die Netflow-Pakete, die für UDP-Port 2055 auf vRealize Network Insight Collector-IP bestimmt sind, von jeder Firewall zugelassen werden, die möglicherweise auf der Route zwischen dem ESXi-Host und dem vRealize Network Insight Collector vorhanden ist.
- 3 Der ESXi-Host hat keine IPFIX-Netflow-Pakete mehr gesendet. Der ESXi-Host sichert das Senden der Netflow-Pakete nach einiger Zeit ab, wenn der UDP-Port 2055 nicht erreichbar ist. Dies kann darauf zurückzuführen sein, dass die Pakete von der Firewall gelöscht werden.
- 4 Der vRealize Network Insight Collector ist aufgrund eines Netzwerkrouting-Problems nicht über den ESXi-Host erreichbar. Stellen Sie sicher, dass zwischen dem ESXi-Host und dem vRealize Network Insight Collector die richtige Route vorhanden ist.

Welche VMware-KB-Artikel sollte ich bezogen auf IPFIX beachten?

VMware ESXi 6.0 Update 1: [2135956](#) .

Wann wird ein Dienst als freigegeben angesehen?

Protokoll	Port
DNS	53
Bootpc	68
Kerberos	88
Pop3	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587

Protokoll	Port
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269