SolarWinds Orion NetFlow Traffic Analyzer

Evaluation Guide

Orion NetFlow Traffic Analyzer Evaluation Guide, Version 3.0, 08.28.2008

Über SolarWinds

SolarWinds, Inc. entwickelt und vertreibt eine Reihe von Tools für Netzwerkmanagement, -überwachung und -erkennung. Diese Tools erfüllen die mannigfaltigen Anforderungen heutiger Netzwerkmanagement- und -beratungsfachleute. SolarWinds Produkte setzen fortdauernd den Maßstab für Qualität und Leistung. Das Unternehmen hat sich dadurch als führender Anbieter von Technologie für Netzwerkmanagement- und -erkennung positioniert. Der Kundenstamm von SolarWinds umfasst mehr als 45 Prozent der Fortune 500-Unternehmen und Kunden aus über 90 Ländern. Unser globales Geschäftspartner-Händlernetz besteht aus mehr als 100 Fachhändlern und Wiederverkäufern.

Kontaktaufnahme mit SolarWinds

Sie können SolarWinds auf verschiedene Weisen kontaktieren, einschließlich:

Team	Kontaktinformationen
Verkauf	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technische Unterstützung	www.solarwinds.com/support
Benutzerforen	www.thwack.com

Konventionen

Die Dokumentation verwendet einheitliche Konventionen, sodass Sie gleichartige Elemente in der gesamten gedruckten und Online-Dokumentation einfacher erkennen können.

Konvention	Kennzeichnet
Fett	Windows-Elemente, einschließlich Schaltflächen und Felder.
Kursiv	Buch- und CD-Titel, variable Namen, neue Begriffe.
`Festbreitenschrift`	Datei- und Verzeichnisnamen, Befehle und Code-Beispiele, vom Benutzer eingegebener Text.
Eckige Klammern, wie in [*Wert*]	Optionale Befehlsparameter.
Geschweifte Klammern, wie in {*Wert*}	Erforderliche Befehlsparameter.
Logisches ODER, wie in *Wert1*|*Wert2*	Exklusive Befehlsparameter, wenn nur eine der Optionen spezifiziert werden kann.

SolarWinds Orion NetFlow Traffic Analyzer Dokumentationsbibliothek

Die folgenden Dokumente sind in der SolarWinds Orion NetFlow Traffic Analyzer Dokumentationsbibliothek enthalten:

Dokument	Zweck
Administrator Guide	Liefert ausführliche Setup-, Konfigurations- und konzeptionelle Informationen.
Seitenhilfe	Bietet Hilfe für jedes Fenster der Orion NetFlow Traffic Analyzer Benutzeroberfläche.
Evaluation Guide	Enthält eine Einführung in Funktionen von Orion Network Performance Monitor sowie Anweisungen zum Installieren und erstmaligem Konfigurieren.
Quick-Start-Anleitung	Beschreibt Installations-, Setup- und allgemeine Szenarien, für die Orion NetFlow Traffic Analyzer eine einfach, jedoch leistungsfähige Lösung bietet.
Anmerkungen zur Version	Enthält neueste Informationen, bekannte Probleme und Aktualisierungen. Die neuesten Release Notes (Anmerkungen zur Version) können unter www.solarwinds.com eingesehen werden.

Inhalt

Kapitel 1

Einführung in Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) bietet eine benutzerfreundliche, skalierbare Netzwerküberwachungslösung für IT-Fachkräfte, die NetFlow-, sFlow- bzw. J-Flow-aktivierte Netzwerke beliebiger Größen verwalten.

Gründe für die Installation von Orion NetFlow Traffic Analyzer

Wenn Unternehmen und deren Netzwerke wachsen, muss Bandbreite exponentiell wachsen. Alle modernen zusammenhängenden Branchen investieren bedeutende Mengen von Zeit uns Geld, um sicherzustellen, dass für geschäftskritische Aktivitäten und Anwendungen genügend Bandbreite vorhanden ist. Wenn Bandbreitenbedürfnisse derzeit verfügbare Kapazität übersteigt, oder wenn der Bedarf über die Fähigkeiten des Netzwerks hinausgeht, ist das Verständnis der Bandbreite nicht mehr einfach ein Gesichtspunkt, sondern wird zur einem kritischen Faktor bei der Entscheidung, ob in mehr Bandbreite investiert werden muss oder ob striktere Nutzungsfaktoren ausreichend sind, um verlorene Bandbreite zurück zu gewinnen.

Mit dem Auftreten von Streaming Media und VoIP-Technologien (Voice over IP), Onlinespielen und anderen bandbreite-intensiven Anwendungen müssen Sie als Netzwerktechniker komplexer Fragen über das Netzwerk beantworten können. Sie müssen beispielsweise beantworten, warum das Netzwerk nicht erwartungsgemäß funktioniert.

Falls Sie wissen müssen, wie und durch wen Bandbreite genutzt wird, bietet Orion NetFlow Traffic Analyzer eine einfache, integrierte Antwort. Sie können die Bandbreitennutzung einer bestimmten Anwendung oder eines bestimmten Verkehrtyps schnell verfolgen und überwachen. Wenn Sie zum Beispiel übermäßige Bandbreitennutzung auf einer bestimmten Schnittstelle sehen, können Sie Orion NetFlow Traffic Analyzer verwenden, um zu erkennen, dass die Unternehmenssitzung, die aus Streaming Video besteht, 80 % der verfügbaren Bandbreite verbraucht, die über einen bestimmten Switch verfügbar ist. Anders als zahlreiche andere NetFlow-Analyseprodukte sind die durch die Orion NetFlow Traffic Analyzer-Lösung gelieferten Netzwerk- und NetFlow-Daten nicht einfach extrapolierte Daten, sondern auf tatsächlichen Informationen basierende Daten, die durch das Orion Network Performance Monitor-Produkt erfasst wurden, das den Kern von Orion NetFlow Traffic Analyzer bildet.

Orion NetFlow Traffic Analyzer bietet eine Out-of-the-Box-Lösung mit weitgehender Überwachungs- und Charting-Funktionalität, verbunden mit detaillierten Statistiken, einschließlich:

- Bandbreitenverteilung über mehrere Verkehrstypen
- Nutzungsmuster über Zeit
- Identifizierung externen Verkehrs und Verfolgung
- Starke Integrierung mit detaillierten Schnittstellenleistungsstatistiken

Diese Überwachungsfunktionalität zusammen mit der vollständig anpassbaren Orion Web Console und Berichts-Engines machen Orion NetFlow Traffic Analyzer zur besten Option zur Überwachung Ihres NetFlow-aktivierten Netzwerks.

Gründe für die Installation von Orion NetFlow Traffic Analyzer

Mit Orion NetFlow Traffic Analyzer können Sie Netzwerkressourcen und Nutzungsmuster auf einer anpassbaren Detaillierungsebene schnell und einfach überwachen. Die folgenden Merkmale repräsentieren Kernfunktionalität von Orion NetFlow Traffic Analyzer:

Verbesserte Verfügbarkeit und Leistung

Mit Orion NetFlow Traffic Analyzer können Sie Netzwerkengpässe und Ausfälle schneller erkennen, diagnostizieren und beheben.

Analytische Kapazitätsplanung

Orion NetFlow Traffic Analyzer hebt Trends in Netzwerkverkehr hervor, sodass Sie Änderungen in der Bandbreite zu Bereichen, die Engpässe erfahren, intelligent antizipieren können.

Optimierte Netzwerkressourcenzuordnung

Durch Orion NetFlow Traffic Analyzer bereitgestellte Informationen ermöglichen es Ihnen, Bereiche des Netzwerks zu identifizieren, die begrenzte oder übermäßig ausgelastete Verbindungen aufweisen. Sie können dann vorhandenen Verkehr zu anderen Bereichen des Netzwerks umleiten, in denen Bandbreite verfügbar ist.

Ausrichtung von IT-Ressourcen auf unternehmensweite Geschäftsbedürfnisse

Da Orion NetFlow Traffic Analyzer auf der bewährten Orion Network Performance Monitor-Infrastruktur aufbaut, können Sie sowohl die Bedürfnisse des unternehmensweiten Netzwerks in einer Übersicht auf hoher Ebene als auch die Funktionsdetails spezifischer Schnittstellen und Knoten beurteilen.

Erhöhte Netzwerksicherheit

Mit Orion NetFlow Traffic Analyzer können Sie Netzwerkverkehr schnell und einfach genau untersuchen und dann mögliche Viren-, Bot- und Spyware-Infektion anzeigende sonderbare Muster, unerwünschte Verhalten und abnormale Nutzung genau feststellen.

Eine komplette NetFlow- und Netzwerkleistungs-Überwachungsanwendung

Sie müssen jetzt nicht mehr zwischen Programmen hin- und herschalten, um ein vollständiges Bild von Nutzung, Leistung und Bedarf im Netzwerk zu erhalten. Alles, was Sie zur Überwachung Ihres NetFlow-aktivierten Netzwerks benötigen, ist in Orion Network Performance Monitor und Orion NetFlow Traffic Analyzer enthalten.

Merkmale von Orion NTA Version 3.0

Orion NTA Version 3.0 bietet die folgenden Funktionen, mit denen Sie die NetFlow-aktivierten Geräte im Netzwerk noch besser überwachen können.

Suche nach IP-Adressbereich

Diese Version von Orion NTA bietet die Möglichkeit der Suche nach Endpunkten innerhalb eines spezifizierten IP-Adressbereichs (z. B. `10.10.199.1-10.10.199.50`).

Zusätzliche NetFlow-Unterstützung ist jetzt verfügbar

Orion NTA Version 3 unterstützt derzeit die Formate NetFlow v9, sFlow v5 und J-Flow zum Erfassen von Netzwerkverkehrsdaten.

Benutzerdefinierte Verkehrsansichten

Mit dem in dieser Version von Orion NTA enthaltenen Traffic View Builder können Sie erfasste NetFlow-Daten filtern, um benutzerdefinierte Ansichten zu erstellen und zu speichern. Sie können beispielsweise eine Ansicht erstellen, die Verkehr von einer ausgewählten IP-Adresse zu einer spezifischen Domain während normaler Bürozeiten (08:00-17:00 Uhr) aufzeigt.

Aktivste 10 NetFlow-Quellen nach Ressource „Prozentauslastung“

Eine neue Ressource auf der NetFlow Summary View (NetFlow-Übersichtsansicht) zeigt überwachte NetFlow-Quellen nach Prozentauslastung.

QoS-Leistungsansichten (Quality of Service = Dienstgüte)

Orion NTA Version 3 ermöglicht einfachen Einblick in den Gesamtnetzwerkverkehr, segmentiert nach CoS-Methoden (Class of Service = Dienstklasse) wie beispielsweise ToS (Type of Service = Diensttyp) oder DSCP *(*Differentiated Services Code Point). Sie können zudem die Bandbreite quantifizieren und visualisieren, die auf den festgelegten QoS-Stufen verbraucht wird, einschließlich Voice und Videodaten.

Port-Anwendungsgruppierung

Mit dieser Version von Orion NTA können Sie eine Anwendung, die mehrere Netzwerkports verwendet einer Gruppe zuordnen, um die Anwendungsleistung zu messen.

Aktivste 5 Ressourcen netzwerkweit

Die netzwerkweit aktivsten 5 Verkehrsressourcen sind jetzt verfügbar und zeigen IP-Adressgruppen. Anwendungen, Gespräche, Länder, Endpunkte, Diensttypen, Sender, Empfänger und Protokolle an.

Vollständige Integrierung von NetFlow-Ressourcen in Orion-Ansichten

NetFlow-Ressourcen können einfach automatisch zu Orion-Ansichten hinzugefügt werden.

DNS-Lookup-Funktion

Führen Sie beliebige manuelle DNS-Lookups durch, ohne auf eine ordnungsgemäße DNS-Aktualisierung zu warten.

Wie Orion NetFlow Traffic Analyzer funktioniert

NetFlow-aktivierte Geräte liefern eine große Menge IP-bezogener Verkehrsinformationen. Orion NetFlow Traffic Analyzer erfasst diese NetFlow-Daten, bringt sie in ein praktisches Format und präsentiert sie dann (mit detaillierten, durch SolarWinds Orion Network Performance Monitor erfassten Netzwerkleistungsdaten) als einfach lesbare Diagramme und Berichte über Bandbreitennutzung innerhalb Ihres Netzwerks und von Ihrem Netzwerk ausgehend. Diese Berichte helfen Ihnen, Bandbreite zu überwachen, Gespräche zwischen internen und externen Endpunkten zu verfolgen, Verkehr zu analysieren und Bandbreitenkapazität zu planen.

Kapitel 2

Installieren von Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) bietet ein assistentengesteuertes Installationsverfahren. Die Anforderungen sind für ein Produkt der Enterprise-Klasse sehr gering.

Hinweis: NetFlow-Daten sind umfassend und konsumieren in relativ kurzer Zeit große Mengen von Datenbankspeicher. Die gilt selbst für kleinere Netzwerke. SolarWinds empfiehlt demzufolge stark, dass Sie Ihre SQL Server-Datenbank und Ihre Orion-NPM/NTA-Installation auf einem physikalisch separaten Server verwalten.

Anforderungen

Der Server, den Sie als Host für Ihre NetFlow-Lösung einsetzen, muss sowohl Orion NPM als auch Orion NTA unterstützen, da Orion NTA auf Orion NPM aufbaut und Orion NPM erweitert. Die folgenden Abschnitte enthalten minimale Konfigurationsanforderungen.

Softwareanforderungen

Die folgenden Softwareanforderungen setzen voraus, dass Ihre Orion NTA-Evaluierung auf einem Server installiert ist, der Orion NPM Version 9.0 ausführt. Falls Sie Orion NTA Version 3.0 auf einer Installation von Orion NPM Version 8.5.1 evaluieren möchten, kontaktieren Sie SolarWinds unter sales@solarwinds.com.

Hinweis: SQL Express und MSDE beschränken die Datenbankgröße auf 4 GB bzw. 2 GB. Aus diesem Grund unterstützt SolarWinds deren Verwendung mit Orion NTA in Produktionsumgebungen nicht.

Software	Anforderungen
Betriebssystem	Windows Server 2003 (32-Bit oder 64-Bit) einschließlich R2, mit IIS installiert. SolarWinds empfiehlt, dass Orion NPM Administratoren lokale Administratorrechte aufweisen, um die volle Funktionalität der lokalen Orion NPM Tools zu gewährleisten. Benutzer, die auf die Web Console begrenzt sind, erfordern keine Administratorrechte. **Hinweis:** SolarWinds unterstützt Orion NTA-Installationen unter Windows XP in Produktionsumgebungen nicht. Falls Orion NTA unter Windows XP installiert wird, muss sichergestellt werden, dass Shared Memory, Named Pipes und TCP/IP auf Remote-Datenbanken aktiviert sind.

Software	Anforderungen
Web Server	Microsoft IIS Version 6.0 und neuer. DNS-Spezifikationen erfordern, dass Hostnamen aus alphanumerischen Zeichen (A-Z, 0-9), Minuszeichen (-) und Punkten (.) bestehen. Unterstriche (_) sind nicht zulässig. Für weitere Informationen siehe RFC 952. **Hinweis:** Die Installation von Orion NTA auf dem gleichen Server bzw. die Nutzung des gleichen Datenbankservers wie ein Research in Motion (RIM) Blackberry Server wird von SolarWinds weder empfohlen noch unterstützt.
.NET Framework	Version 3.5 oder neuer.
SNMP Trap Services	Windows Betriebssystemmanagement und Überwachungstoolkomponente.
SQL Server	SQL Server 2000 SP4, Standard oder Enterprise. SQL Server 2005 Standard oder Enterprise. Datenbank muss gemischten Modus oder SQL-Authentifizierung unterstützen. **Hinweis:** SQL Server Express kann Datenbanken mit mehr als 4 GB nicht verwalten. Die Software ist auf einen einzigen Prozessor begrenzt und nutzt nicht mehr als 1 GB RAM. Obwohl die Software zur Überwachung von 1-2 Schnittstellen für Evaluierungszwecke verwendet werden kann, rät SolarWinds von der Nutzung für größere Netzwerke, die größere Datenbanken erfordern, ab.
Web Console Browser	Microsoft Internet Explorer Version 6 oder neuer mit Active Scripting. Mozilla Firefox 2.0 oder neuer.

Hardwareanforderungen

Die folgenden Hardwareanforderungen setzen voraus, dass Ihre Orion NTA-Evaluierung auf einem Server installiert ist, der Orion NPM Version 9.0 ausführt. Falls Sie Orion NTA Version 3.0 auf einer anderen Version von Orion NPM evaluieren möchten, kontaktieren Sie SolarWinds unter sales@solarwinds.com.

Hinweis: Orion NTA erfordert, dass TCP-Port 17777 sowohl zum Senden als auch zum Empfangen von Verkehr zwischen Orion NPM und beliebigen Orion Modulen geöffnet ist, einschließlich Orion NTA.

Warnung: Nur die RAID-Konfigurationen 0, 1, 0+1 bzw. 1+0 sollten auf einer Orion NTA-Installation verwendet werden. Aufgrund der hohen Geschwindigkeiten und den hohen Speicheranforderungen von NetFlow-Datentransaktionen, rät SolarWinds von der Verwendung anderer RAID- oder SAN-Konfigurationen ab, da diese zu Datenverlusten und erheblichen Leistungseinbussen führen können.

Hardware	Anforderungen
CPU	3 GHz oder schneller.
RAM	2 GB oder mehr.
Festplattenspeicher	5 GB oder mehr. Unterstützt die RAID-Konfigurationen 0, 1, 0+1 bzw. 1+0. Andere RAID- oder SAN-Konfigurationen werden nicht empfohlen.
NetFlow-Geräte	Cisco-Geräte, die NetFlow Version 5 oder 9 verwenden. **Hinweis:** Orion NTA erkennt nur NetFlow Version 9-Vorlagen, die alle Felder enthalten, die durch NetFlow Version 5 genutzt werden.
J-Flow	Netzwerkgeräte, die J-Flow verwenden.
sFlow-Geräte	sFlow-Geräte, die sFlow Version 5 verwenden.

Anforderungen an Virtual Machine (Virtuelle Maschinen)

Orion NTA-Installationen auf VMware Virtual Machines und Microsoft Virtual Server werden uneingeschränkt unterstützt, falls für jede virtuelle Maschine die folgenden minimalen Konfigurationsanforderungen erfüllt sind.

Konfiguration virtuelle Maschine	Anforderungen
CPU-Geschwindigkeit	3,0 GHz
Reservierter Festplattenspeicher	5 GB **Hinweis:** RAID 1+0 wird empfohlen; aufgrund der hohen E/A-Anforderungen wird RAID 5 nicht empfohlen.
Speicher	2 GB
Netzwerkschnittstelle	Jede Installation von Orion NPM sollte ihre eigene, reservierte Netzwerkschnittstellenkarte haben. **Hinweis:** Da Orion NPM SNMP zur Überwachung Ihres Netzwerks verwendet, können Lücken in den Überwachungsdaten auftreten, falls Sie Ihrer Orion NPM Installation keine eigene Netzwerkschnittstellenkarte geben können. Diese Lücken treten auf, da SNMP-Verkehr normalerweise eine niedrige Priorität aufweist.

Für weitere Informationen über Orion NPM-Anforderungen siehe „Requirements“ in der *SolarWinds Orion Network Performance Monitor Administrator Guide*.

SQL Server und SQL Server Express mit Orion NTA

Aufgrund der Tatsache, dass NetFlow-Daten umfassend sind und in relativ kurzer Zeit große Mengen von Datenbankspeicher belegen können, rät SolarWinds von der Verwendung von SQL Server Express-Datenbankinstanzen für Orion NTA ab. Stattdessen empfiehlt SolarWinds die Verwendung einer Produktionsversion von SQL Server.

Evaluierungen von Orion NTA sind eine eingeschränkte Ausnahme. Für Evaluierungszwecke können Orion NPM and Orion NTA die Verwendung von SQL Server Express 2005-Datenbankinstanzen unterstützen. Mit SQL Express können Sie Orion NTA mit einer wirklichen Datenbank evaluieren. Zudem ist SQL Express kostenlos von Microsoft erhältlich. SolarWinds empfiehlt jedoch aus den nachfolgenden Gründen nicht, Orion NTA in Produktionsumgebungen einzusetzen:

- SQL Express kann Datenbanken mit mehr als 4 GB nicht verwalten.
- SQL Express ist auf einen einzigen Prozessor begrenzt.
- SQL Express kann nicht mehr als 1 MB RAM nutzen.

Hinweis: Für Produktionsumgebungen sollten Orion NPM- und Orion NTA-Installationen eine auf einem separaten Server installierte SQL Server-Datenbankinstanz verwenden.

Installieren von Orion NetFlow Traffic Analyzer

Führen Sie das folgende Verfahren durch, um Orion NetFlow Traffic Analyzer zu installieren. Um die Installation abzuschließen, müssen Sie den Port für NetFlow-Verkehr angeben und bestätigen, dass er aktiviert ist und NetFlow-Verkehrsdaten sendet.

Hinweis: Das folgende Verfahren setzt voraus, dass Sie Orion Network Performance Monitor Version 9.0 bereits auf dem Server installiert haben, auf dem Sie Orion NetFlow Traffic Analyzer installieren möchten. Falls Sie Orion Network Performance Monitor Version 9.0 evaluieren möchten, kontaktieren Sie SolarWinds unter sales@solarwinds.com.

Installieren von Orion NetFlow Traffic Analyzer:

1. Melden Sie sich beim Orion Network Performance Monitor-Server an, den Sie für NetFlow-Verkehrsanalysen verwenden möchten.
2. ***Falls Sie NetFlow Traffic Analyzer auf einem Terminalserver installieren,*** führen Sie, um zu gewährleisten, dass NetFlow Traffic Analyzer korrekt installiert wird, die folgenden Schritte durch, bevor Sie die Installation fortsetzen:

a. Klicken Sie auf **Start > Control Panel > Add or Remove Programs** (Start > Systemsteuerung > Software).

b. Klicken Sie auf **Add New Programs** (Neue Programme hinzufügen).

c. Klicken Sie im Fenster **Program From Floppy Disk or CD-ROM** (Programm von Diskette oder CD installieren) auf **CD or Floppy** (CD oder Diskette) und dann auf **Next** (Weiter).

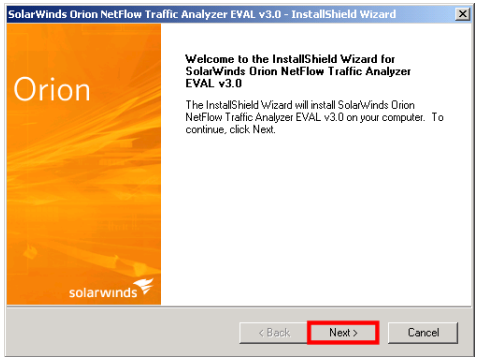
3. ***Falls Sie das Produkt von der SolarWinds Website heruntergeladen haben,*** führen Sie die folgenden Schritte durch:

   a. Navigieren Sie zum Speicherort der heruntergeladenen `.zip`-Datei und extrahieren Sie dann das Evaluierungspaket an einen geeigneten Speicherort.

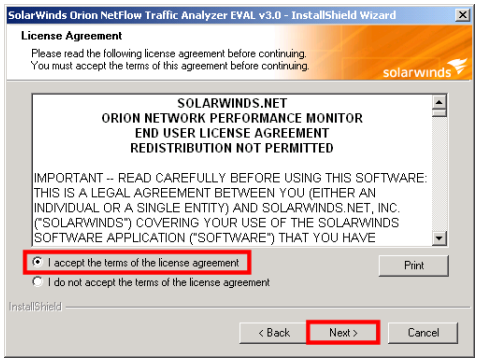
   b. Starten Sie die ausführbare Evaluierungsdatei von SolarWinds Orion NTA.

4. ***Falls Sie ein physikalisches Medium erhalten haben,*** gehen Sie zur ausführbaren Datei von SolarWinds Orion NTA und starten Sie sie.

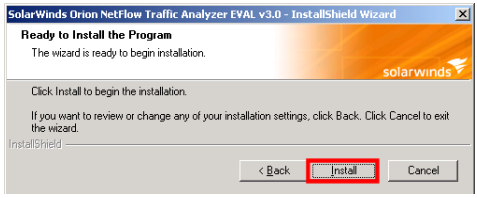
5. Lesen Sie den Begrüßungstext und klicken Sie dann auf **Next** (Weiter).



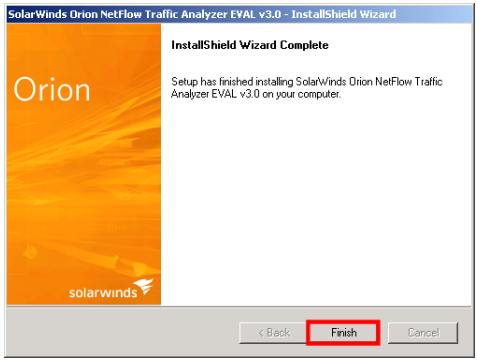
6. Wählen Sie **I accept the terms of the license agreement** (Ich stimme den Bedingungen des Lizenzvertrags zu) aus und klicken Sie dann auf **Next** (Weiter).



7. Klicken Sie im Fenster Ready to Install the Program (Das Programm kann jetzt installiert werden) auf **Install** (Installieren).



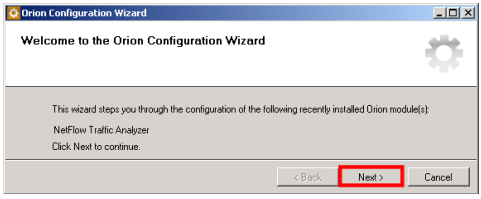
8. Wenn der InstallShield Wizard (InstallShield-Assistent) fertig ist, klicken Sie auf **Finish** (Fertig stellen), um den Assistenten zu beenden.



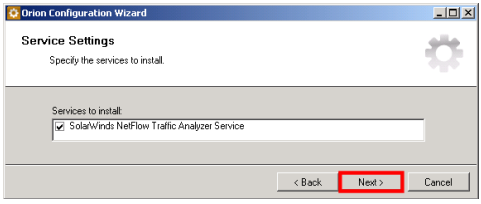
9. ***Falls Sie aufgefordert werden, den Server neu zu starten,*** wählen Sie die geeigneten Optionen aus:

- ***Falls Sie Orion NTA auf einem Terminalserver installieren,*** klicken Sie auf **No** (Nein).
- ***Falls Sie Orion NTA NICHT auf einem Terminalserver installieren,*** klicken Sie auf **Yes** (Ja).

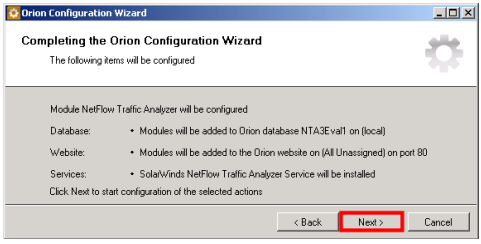
10. ***Falls der Konfigurationsassistent nicht automatisch startet,*** klicken Sie auf **Start > All Programs > SolarWinds Orion > Configuration Wizard** (Start > Alle Programme > SolarWinds Orion > Konfigurationsassistent).
11. Lesen Sie den Begrüßungstext und klicken Sie dann auf **Next** (Weiter).



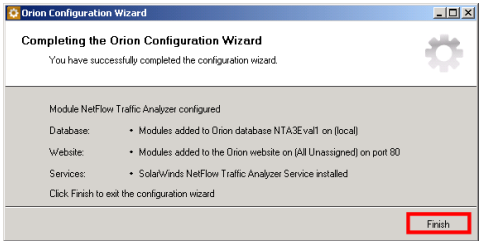
12. Stellen Sie sicher, dass **SolarWinds NetFlow Traffic Analyzer Service** (SolarWinds NetFlow-Verkehrsanalysedienst) im Fenster Service Settings (Diensteinstellungen) markiert ist, und klicken Sie dann auf **Next** (Weiter)



13. Prüfen Sie die Konfigurationsübersicht und klicken Sie dann auf **Next** (Weiter).



14. Nach Abschluss des Configuration Wizard klicken Sie auf **Finish** (Fertig stellen).



Aktivieren von NetFlow Traffic Analysis

Um zu beginnen, verfügbare NetFlow-Daten zu analysieren, die durch Geräte im Netzwerk erzeugt wurden, müssen Sie entweder eine NetFlow-aktivierte Schnittstelle zu Ihrer Orion-Datenbank hinzufügen oder eine bereits hinzugefügte Schnittstelle überwachen, die NetFlow-Daten generieren kann. NetFlow-aktivierte Geräte müssen zur Orion-Datenbank hinzugefügt werden, bevor sie in Orion NTA überwacht werden können.

Hinweis: Das Hinzufügen der NetFlow-Geräte und -Schnittstellen zur Orion-Datenbank und das Hinzufügen der NetFlow-Geräte und -Schnittstellen als NetFlow-Quellen zu Orion NTA sind separate Verfahren, die nachfolgend in separaten Abschnitten beschrieben sind.

Hinzufügen von Geräten und Schnittstellen zur Orion-Datenbank

Das folgende Verfahren fügt ein Gerät und dessen Schnittstellen unter Verwendung der Web Node Management-Funktion der Orion Web Console zur Orion-Datenbank hinzu. Falls das NetFlow-Gerät bereits zum Senden von NetFlow-Daten konfiguriert ist, beginnt Orion NTA NetFlow-Daten zu empfangen, sobald das Gerät zur Orion-Datenbank hinzugefügt wurde.

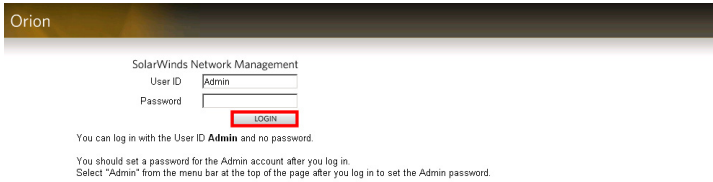
Hinweis: Für weitere Informationen über die Bestimmung von NetFlow-Quellen in Orion NTA siehe „Hinzufügen von NetFlow-Quellen zu NetFlow Traffic Analyzer“ auf Seite 19.

Hinzufügen von NetFlow-aktivierten Geräten und Schnittstellen zur Orion-Datenbank:

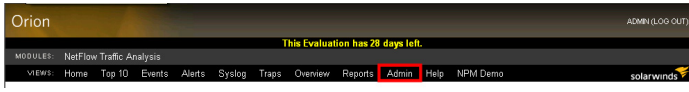
1. Melden Sie sich beim Orion NPM-Server an, der die Orion NTA-Installation hostet.

2. Klicken Sie auf **Start > SolarWinds Orion > Orion Web Console** (Start > SolarWinds Orion > Orion Web Console).
3. Melden Sie sich als Administrator bei der Orion Web Console an.

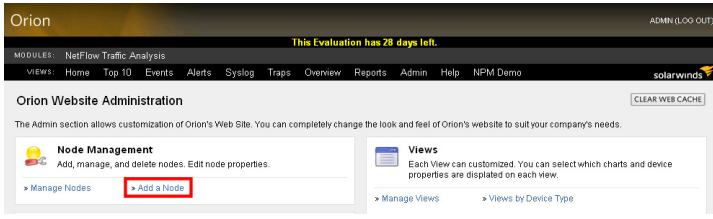
   Hinweis: Falls Sie noch kein anderes Admin-Kennwort konfiguriert haben, können Sie sich mit der **User ID** (Benutzer-ID) `Admin` ohne Kennwort anmelden.



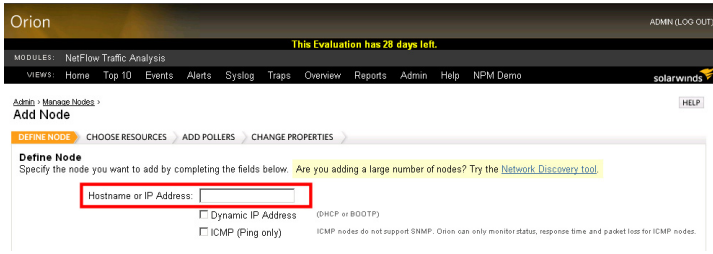
4. Klicken Sie auf der Views-Symbolleiste auf **Admin** (Verwaltung).



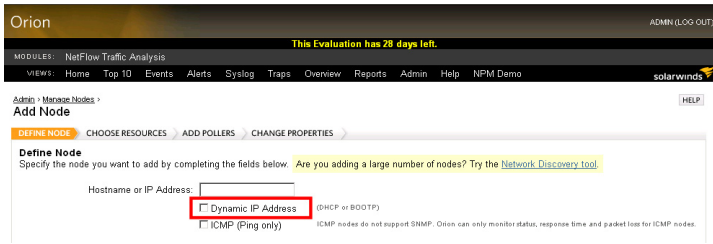
5. Klicken Sie unter Node Management (Knotenverwaltung) auf **Add a Node** (Knoten hinzufügen).



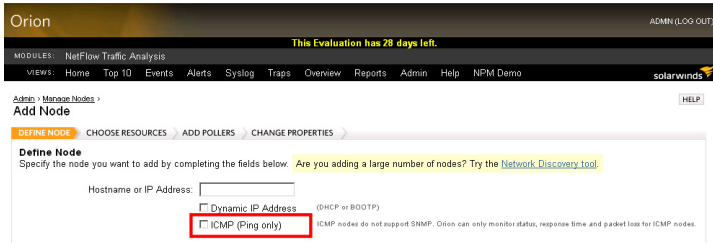
6. Geben Sie den Hostnamen oder die IP-Adresse des hinzuzufügenden NetFlow-aktivierten Geräts in das Feld **Hostname or IP Address** (Hostname oder IP-Adresse) ein.



7. ***Falls die IP-Adresse des hinzuzufügenden Geräts dynamisch zugeordnet wird (DHCP oder BOOTP),*** markieren Sie **Dynamic IP Address** (Dynamische IP-Adresse).

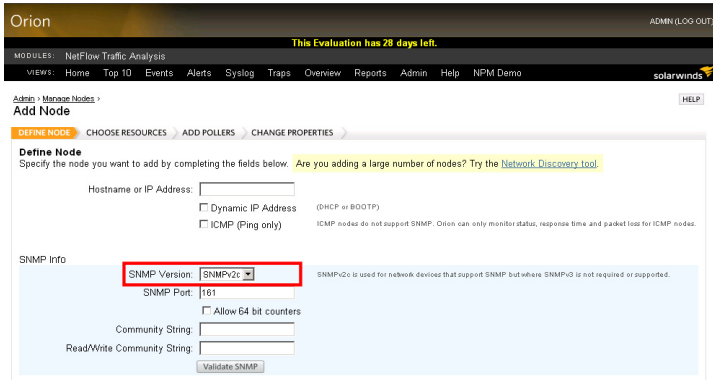


8. Stellen Sie sicher, dass **ICMP (Ping only)** (ICMP - nur Ping) nicht markiert ist.



9. Wählen Sie die **SNMP Version** für den hinzugefügten Knoten aus.

   Hinweis: Orion NPM verwendet standardmäßig **SNMPv2c**. Falls das neue Gerät die erweiterten Sicherheitsfunktionen von SNMPv3 unterstützt bzw. erfordert, wählen Sie **SNMPv3** aus.



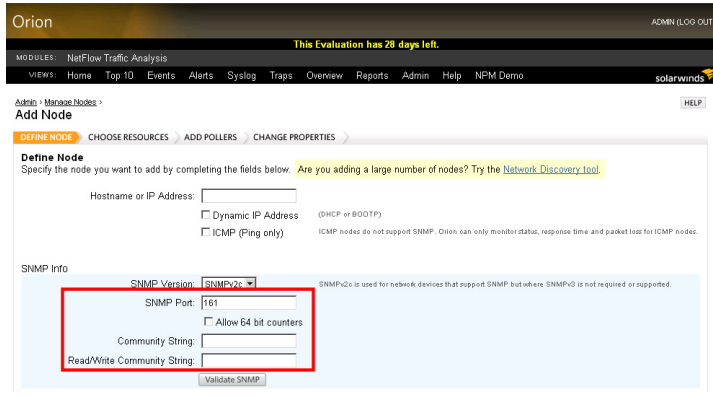
10. ***Falls Sie*** **SNMPv2c ausgewählt haben,** führen Sie die folgenden Schritte durch:

a. ***Falls der SNMP-Port auf dem hinzugefügten Knoten nicht dem Orion NPM-Standard von 161 entspricht,*** geben Sie die entsprechende Portnummer in das Feld **SNMP Port** ein.

b. ***Falls der hinzugefügte Knoten 64-Bit-Zähler unterstützt und Sie diese verwenden möchten,*** markieren Sie **Allow 64 bit counters** (64-Bit-Zähler zulassen).

c. Geben Sie gültige Community Strings für den hinzugefügten Knoten an.

Hinweis: Der **Read/Write Community String** (Lesen/Schreiben-Community-String) ist optional, doch Orion NPM erfordert mindestens den `public` **Community String**.



11. ***Falls Sie* SNMPv3 ausgewählt haben,** führen Sie die folgenden Schritte durch:

a. ***Falls der SNMP-Port auf dem hinzugefügten Knoten nicht dem Orion NPM-Standard von 161 entspricht,*** geben Sie die entsprechende Portnummer in das Feld **SNMP Port** ein.

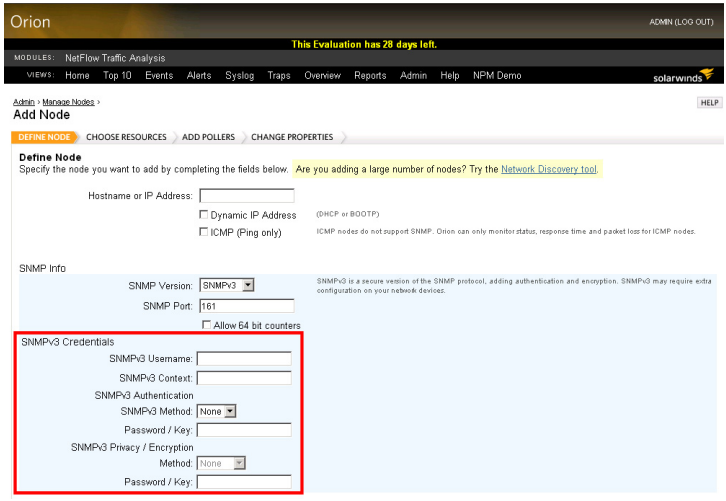
b. ***Falls der hinzugefügte Knoten 64-Bit-Zähler unterstützt und Sie diese verwenden möchten,*** markieren Sie **Allow 64 bit counters** (64-Bit-Zähler zulassen).

Hinweis: Orion NPM unterstützt die Verwendung von 64-Bit-Zählern vollständig; diese Hochleistungszähler können jedoch je nach Hersteller-implementierung zu unberechenbarem Verhalten führen. Falls Sie bei Verwendung dieser Zähler merkwürdige Ergebnisse erhalten, verwenden Sie die Ansicht Node Details (Knotendetails), um die Verwendung von 64-Bit-Zählern für das Gerät zu deaktivieren, und kontaktieren Sie den Hardwarehersteller.

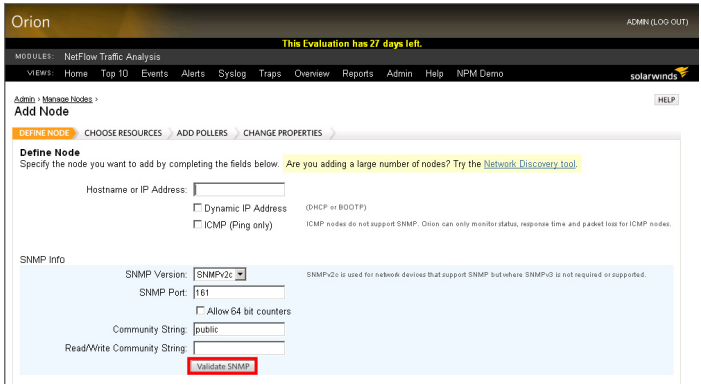
c. Geben Sie die erforderlichen Einstellungen in die Felder **SNMP Credentials** (SNMP-Anmeldeinformationen), **SNMP Authentication** (SNMP-Authentifizierung) und **SNMP Privacy/Encryption** (SNMP-Datenschutz/-Verschlüsselung) ein:

- **SNMPv3 Username** (Benutzername)
- **SNMPv3 Context** (Kontext)
- **SNMPv3 Authentication Method** (Authentifizierungsmethode)
- **SNMPv3 Authentication Password/Key** (Authentifizierungskennwort/-schlüssel)
- **SNMPv3 Privacy/Encryption Method** (Datenschutz/-Verschlüsselungsmethode)
- **SNMPv3 Privacy/Encryption Password/Key** (Datenschutz/-Verschlüsselungs-Kennwort/-Schlüssel)

Hinweis: Für die Zwecke dieser Evaluierung sind keine **Read/Write SNMPv3 Credentials** (Lesen/Schreiben SNMPv3 Anmeldeinformationen) erforderlich.



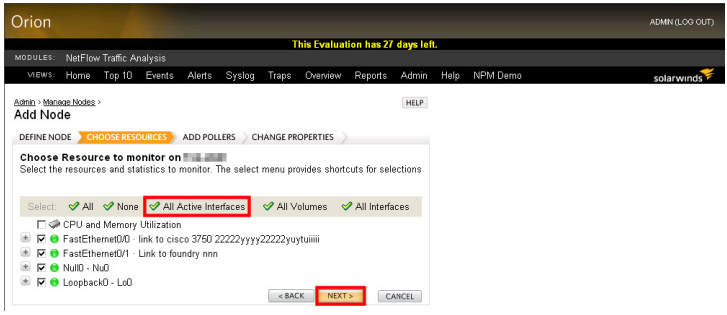
12. Klicken Sie nach der Eingabe aller SNMP-Anmeldeinformationen auf **Validate SNMP** (SNMP überprüfen).



13. Nach der Bestätigung, dass Ihre SNMP-Anmeldeinformationen gültig sind, klicken Sie auf **Next** (Weiter).

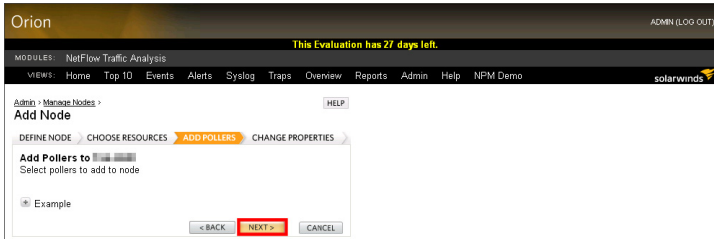
14. Markieren Sie die Schnittstellen, die Sie mit Orion NTA überwachen möchten, und klicken Sie dann auf **Next** (Weiter).

    Hinweis: Falls Sie nicht wissen, welche Schnittstellen NetFlow-aktiviert sind, klicken Sie auf **All Interfaces** (Alle Schnittstellen), um alle auszuwählen.

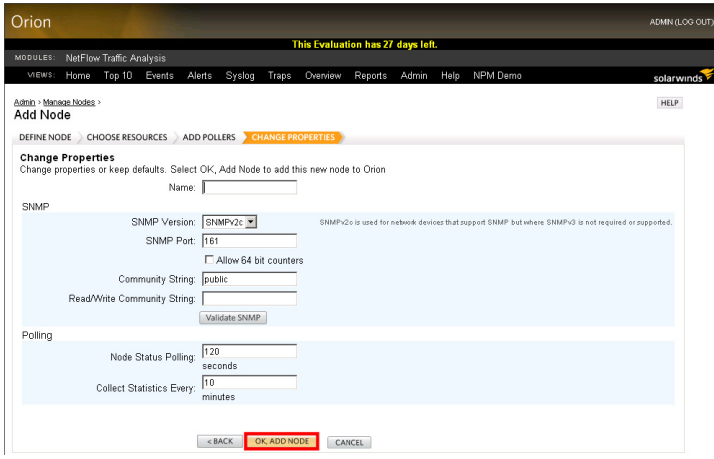


15. Für die Zwecke dieser Evaluierung, klicken Sie auf der Ansicht Add Pollers auf **Next** (Weiter).

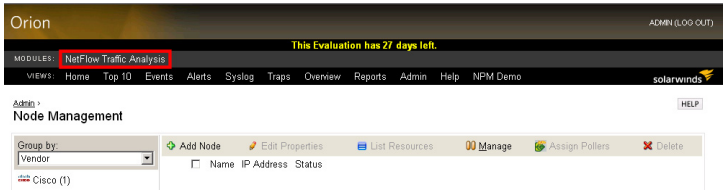
    Hinweis: Für weitere Informationen über Poller-Verwendung und -Definition von siehe die *SolarWinds Orion Network Performance Monitor Administrator Guide*.



16. Klicken Sie auf der Ansicht Change Properties (Eigenschaften ändern) auf **OK, Add Node** (OK, Knoten hinzufügen).



17. Klicken Sie auf der Modules-Symbolleiste auf **NetFlow Traffic Analysis** (NetFlow-Verkehrsanalyse).



Der folgende Abschnitt enthält die Schritte, die erforderlich sind, um zu beginnen, NetFlow-Daten von NetFlow-aktivierten Geräten im Netzwerk zu empfangen.

Hinzufügen von NetFlow-Quellen zu NetFlow Traffic Analyzer

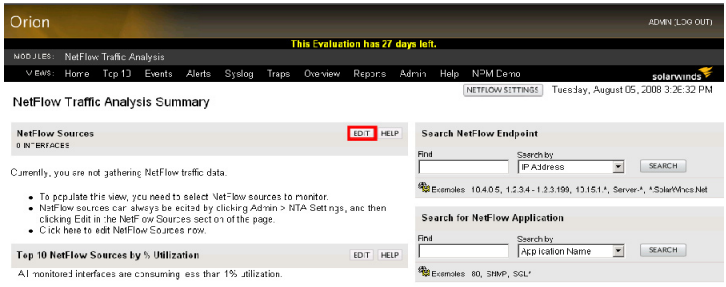
Nachdem das NetFlow-aktivierte Gerät und dessen Schnittstellen zu Orion NPM hinzugefügt wurden, müssen Sie das Gerät als NetFlow-Quelle festlegen. Das folgende Verfahren enthält die erforderliche Schritte zum Hinzufügen von NetFlow-Quellen zu Orion NTA.

Hinweis: Orion NTA erkennt nur NetFlow Version 9-Vorlagen, die alle Felder enthalten, die durch NetFlow Version 5 genutzt werden.

Hinzufügen von NetFlow-Geräten und -Schnittstellen zu NetFlow Traffic Analyzer:

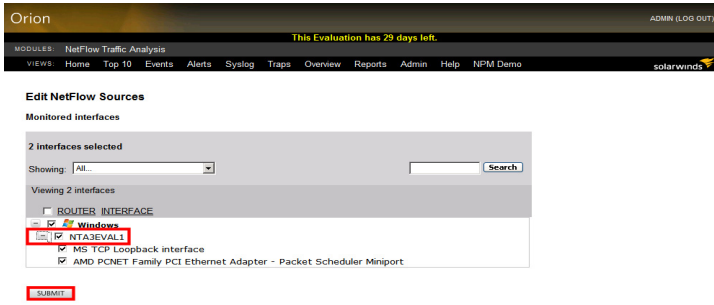
1. Melden Sie sich beim Orion NPM-Server an, der die Orion NetFlow Traffic Analyzer hostet.
2. Klicken Sie auf **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Start > Alle Programme > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console).
3. Melden Sie sich als Administrator bei der Orion Web Console an.

   Hinweis: Falls Sie noch nicht ein anderes Admin-Kennwort konfiguriert haben, können Sie sich mit der **User ID** (Benutzer-ID) `Admin` ohne Kennwort anmelden.
4. Klicken oben in der Ressource NetFlow Sources (NetFlow-Quellen) auf **Edit** (Bearbeiten).



5. Wählen Sie unter Showing (Anzeige) die Option **Exporters Only (last 15 minutes)** (Nur Exporter (letzte 15 Minuten)) aus.

6. Erweitern Sie die Gerätliste, um alle überwachten Knoten zu sehen, markieren Sie die übergeordneten Knoten der Schnittstellen, die Orion NTA überwachen soll, und klicken Sie dann auf **Submit** (Übermitteln).



Als Ergebnis davon sollte Orion NTA brauchbare Verkehrsdaten empfangen und innerhalb weniger Minuten auf der Orion Web Console anzeigen.

Kapitel 3

Orion NetFlow Traffic Analyzer Quick-Tour

Die durch Orion NetFlow Traffic Analyzer gebotenen Funktionen und die gebotene Flexibilität liefern sehr detaillierten Einblick in Quantität und Qualität von Verkehr im Netzwerk. Die Abschnitte in diesem Kapitel sind sequenziell aufgebaut und veranschaulichen die Funktionen und Merkmale von Orion NetFlow Traffic Analyzer. Dieses Kapitel ist am nützlichsten, wenn es vollständig durchgelesen und von A-Z befolgt wird. Es beginnt mit einer Übersicht der auf der Ansicht NetFlow Traffic Analysis Summary sofort verfügbaren Ressourcen, gefolgt von den Übersichten der am häufigsten verwendeten Orion NTA-Ansichten.

Hinweis: Erweiterte Nutzungsbeispiele, einschließlich Szenarien, die andere SolarWinds-Tools einschließen, befinden sich im letzten Kapitel dieser Evaluation Guide. Für weitere Informationen siehe„Verwendung von Orion NetFlow Traffic Analyzer“ auf Seite 43.

Starten von Orion NetFlow Traffic Analyzer

Um Orion NetFlow Traffic Analyzer zu starten, klicken Sie auf **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Start > Alle Programme > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console). Für weitere Informationen über die Installation und Konfiguration von Orion NTA siehe „Installieren von Orion NetFlow Traffic Analyzer“ auf Seite 5.

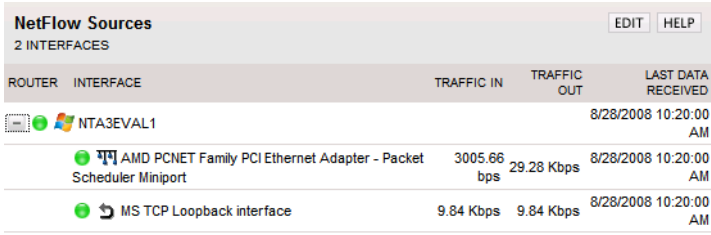
NetFlow Traffic Analysis Summary

Wenn Sie Orion NetFlow Traffic Analyzer starten wird die NetFlow Traffic Analysis Summary (Verkehrsanalyseübersicht) als erste Ansicht eingeblendet. Diese Ansicht bietet Einblick in die Datenverkehrsbedingungen im gesamten Netzwerk. Die folgenden Ressourcen sind standardmäßig in der NetFlow Traffic Analysis Summary-Ansicht enthalten.

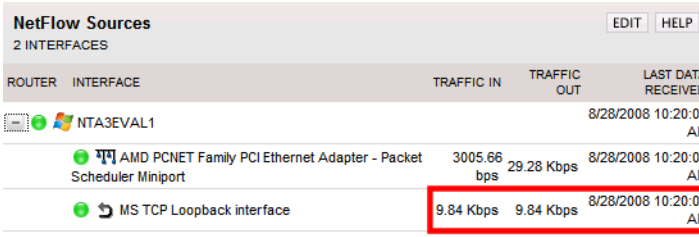
NetFlow Sources

Diese Ressource liefert eine Liste aller NetFlow-aktivierten Geräte im Netzwerk, die derzeit zum Senden von NetFlow-Daten an den Server konfiguriert sind, der die Orion NTA-Installation hostet. Für weitere Informationen über das Hinzufügen NetFlow-aktivierter Geräte siehe„Aktivieren von NetFlow Traffic Analysis“ auf Seite 12.

Klicken Sie auf das **+** neben einem beliebigen Routernamen, um NetFlow-aktivierte Schnittstellen auf dem ausgewählten Router anzuzeigen.



Schnittstellen werden zudem mit einem Statussymbol und einem Zeitstempel angezeigt, der angibt, wenn Orion NTA letztmals NetFlow-Daten von der ausgewählten Schnittstelle empfangen hat. Darüber hinaus liefert die Ressource NetFlow-Sources (NetFlow-Quelle) gemeldete Werte für eingehenden und abgehenden Verkehr auf jeder Schnittstelle.

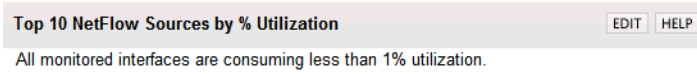


Klicken auf einen Routernamen öffnet die Ansicht NetFlow Node Details (NetFlow-Knotendetails), Klicken auf einen Schnittstellennamen öffnet die Ansicht NetFlow Interface Details (NetFlow-Schnittstellendetails). Für weitere Informationen über die NetFlow Node Details-Ansicht siehe „NetFlow Node Details-Ansicht“ auf Seite 39. Für weitere Informationen über die NetFlow Interface Details-Ansicht siehe „NetFlow Interface Details-Ansicht“ auf Seite 37.

Aktivste 10 NetFlow-Quellen nach Prozentauslastung

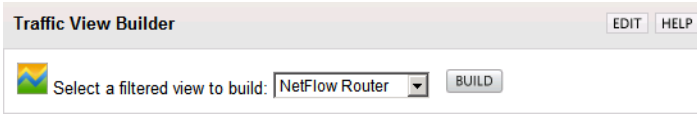
Diese Ressource liefert eine Liste aller NetFlow-Quellen im Netzwerk, die derzeit genügend Verkehr routen, um die Systemressourcen in bedeutender Weise zu beanspruchen.

Hinweis: Quellen werden nur aufgeführt, wenn sie eine Auslastung von über 1 % erzeugen.



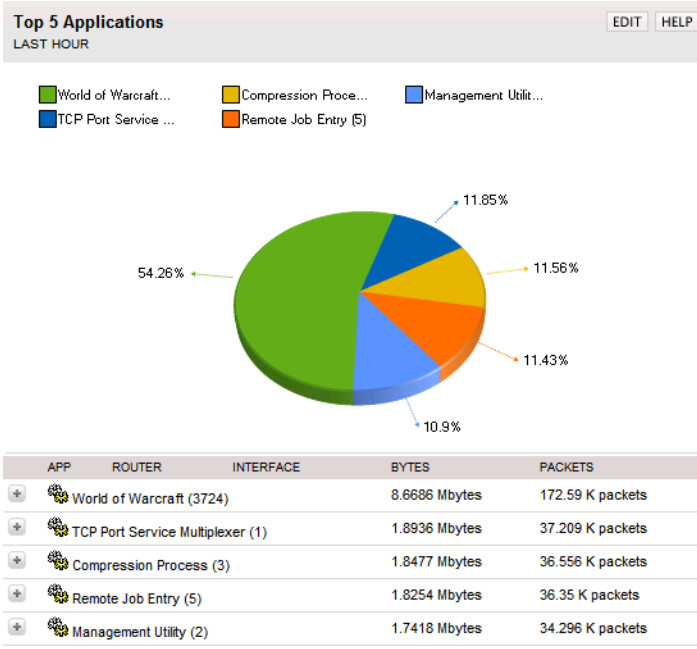
Traffic View Builder

Mit der Anwendung Traffic View Builder können Sie eigene benutzerdefinierte Orion NTA-Ansichten erstellen. Da es sich bei Orion NTA um ein webbasiertes Modul handelt, können Sie Browser-Lesezeichen für beliebige Orion NTA-Ansichten erstellen, um den Zustand von möglichen Problempunkten später einfach überprüfen zu können. Für weitere Informationen über Traffic View Builder siehe „Verwendung von Traffic View Builder“ auf Seite 43.



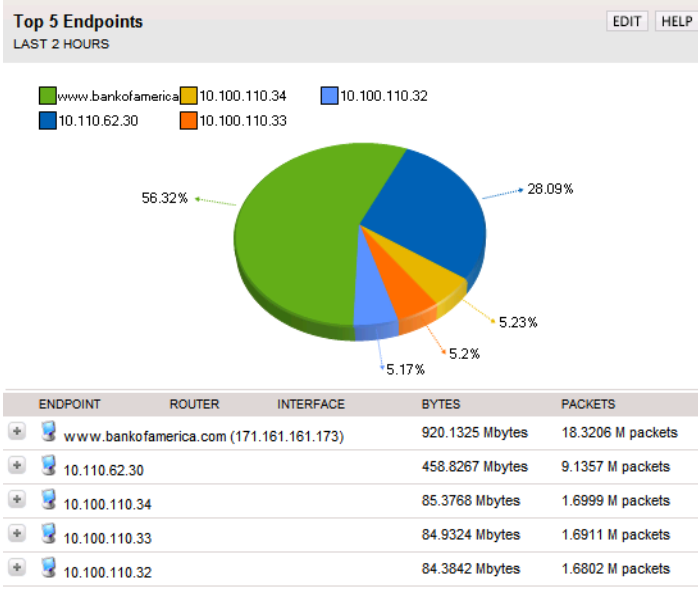
Aktivste 5 Anwendungen

Die Ressource Top 5 Applications (Aktivste 5 Anwendungen) liefert eine schnelle Ansicht der Anwendungen und Ports, die durch die Geräte im Netzwerk am meisten genutzt werden. Durch Klicken auf das **+** neben einer Anwendung können Sie die Ansicht erweitern, um den Routing-Verkehr der Netzwerkgeräte für diese Anwendung anzuzeigen.



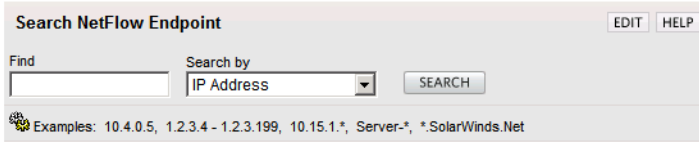
Aktivste 5 Endpunkte

Die Ressource Top 5 Endpoints (Aktivste 5 Endpunkte) liefert einen schnellen Einblick in die Endpunkte, die Quellen oder Ziele der größten Mengen von Netzwerkverkehr sind. Durch Klicken auf das **+** neben einem Endpunkt können Sie die Ansicht erweitern, um den Routing-Verkehr der Netzwerkgeräte für diesen Endpunkt anzuzeigen.



Suche nach NetFlow-Endpunkten

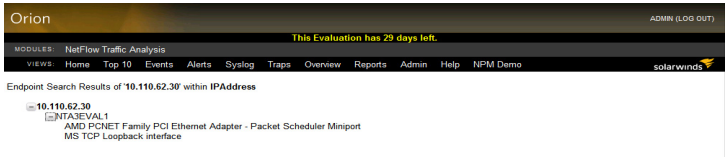
Mit dieser Ressource (Search for NetFlow Endpoints) können Sie einen beliebigen Endpunkt, der mit einem Gerät im Netzwerk kommuniziert, schnell finden.



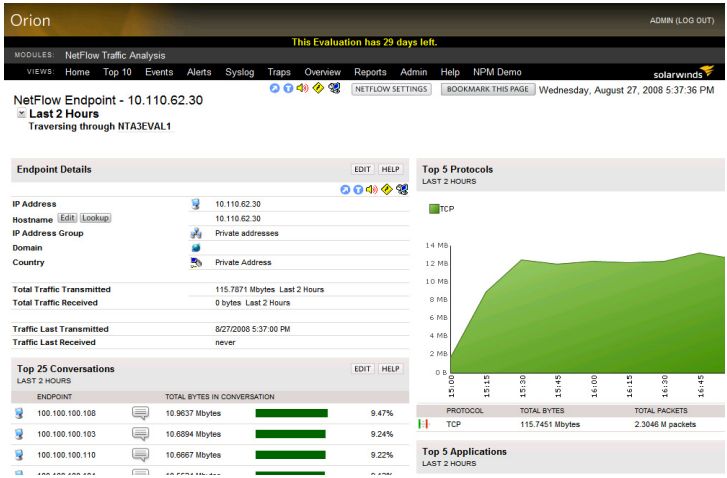
Suchen Sie einfach nach Endpunkten, indem Sie beliebige Kriterien der folgenden Tabelle verwenden:

Kriterien für die Suche nach NetFlow-Endpunkten		
Country (Land)	Domain (Domain)	Hostname (Hostname)
IP Address (IP-Adresse)	IP Address Group Name (IP-Adressgruppenname)	

Geben Sie einen geeigneten Suchbegriff an und klicken Sie dann auf **Search** (Suchen). Die Suchergebnisse liefern eine erweiterbare Liste der Geräte im Netzwerk, die entweder Verkehr zum oder Verkehr vom gesuchten Endpunkt routen.

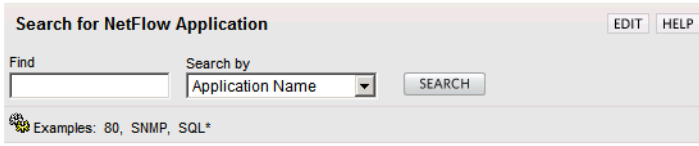


Klicken auf den Namen eines Netzwerkgeräts öffnet die Ansicht NetFlow Endpoint für jeglichen Endpunktverkehr durch das ausgewählte Gerät. Für weitere Informationen über die Ansicht NetFlow Endpoint siehe „NetFlow Endpoint-Ansicht“ auf Seite 35.

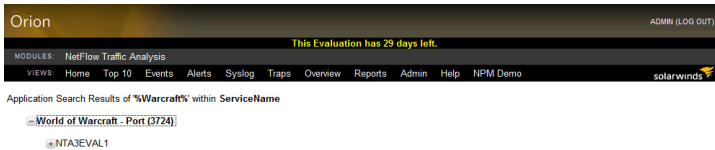


Suche nach NetFlow-Anwendung

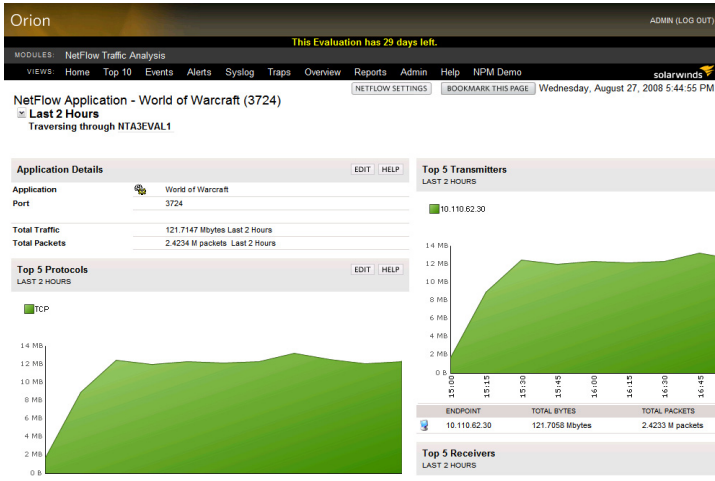
Mit der Ressource Search for NetFlow Application können Sie jederzeit schnell ermitteln, welche Geräte im Netzwerk eine bestimmte Anwendung oder einen bestimmten Port verwenden. Wählen Sie einfach Application Name (Anwendungsname) oder Port (Portnummer) aus und geben Sie einen Anwendungsnamen oder eine Portnummer ein, und klicken Sie dann auf **Search** (Suchen).



Die Suchergebnisse liefern eine erweiterbare Liste der Geräte im Netzwerk, die entweder Verkehr für die ausgewählte Anwendung oder Verkehr über den ausgewählten Port routen.

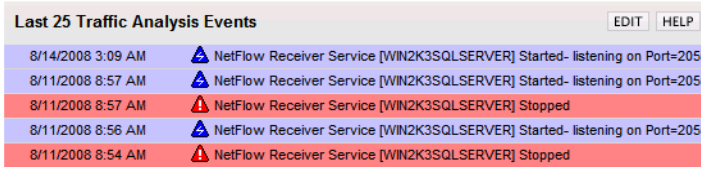


Klicken auf den Namen eines Geräts im Netzwerk öffnet die Ansicht NetFlow Application für jeglichen Verkehr durch das ausgewählte Gerät, der entweder für die gesuchte Anwendung bestimmt ist oder über den gesuchten Port geroutet wird.Für weitere Informationen über die Ansicht NetFlow Application siehe „NetFlow Application-Ansicht“ auf Seite 31.



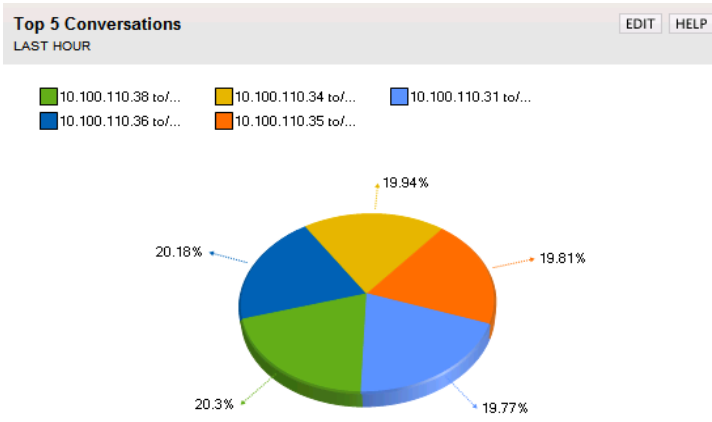
Letzte 25 Verkehrsanalyseereignisse

Diese Ressource listet die letzten 25 NetFlow-spezifischen Ereignisse, die in Geräten im überwachten Netzwerk aufgetreten sind. Diese Ressource listet normalerweise das Datum und die Uhrzeit, wenn der NetFlow Receiver Service gestartet bzw. gestoppt wird.



Aktivste 5 Gespräche

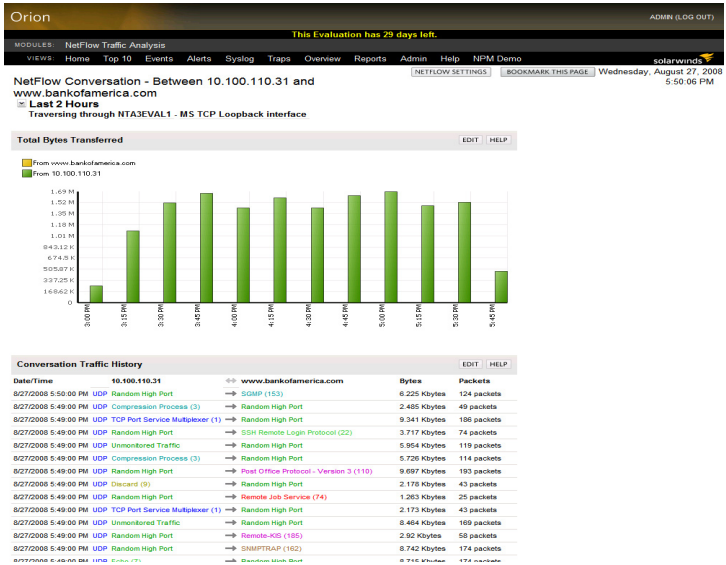
Diese Ressource liefert eine schnelle Ansicht (mit Chart und Tabelle) der Gespräche, die am meisten Bandbreite im Netzwerk verbrauchen. Jede Farbe im Chart entspricht einem einzelnen anhaltenden Gespräch zwischen zwei spezifischen Endpunkten. Die Tabelle unterhalb des Charts listet die an jedem Gespräch beteiligten Endpunkte sowie die durch das Gespräch verbrauchte Bandbreite in Bytes und Paketen. Klicken auf das **+** erweitert die Gesprächsbeschreibung und zeigt alle Geräte im Netzwerk an, über die das ausgewählte Gespräch geführt wird. Die erste Erweiterungsstufe zeigt die Netzwerkknoten an, über die Gesprächsverkehr geroutet wird. Die nächste Erweiterungsstufe zeigt die Schnittstellen an, die Verkehr für das ausgewählte Gespräch weiterleiten.



CONVERSATION ROUTER INTERFACE	BYTES	PACKETS
Between 10.100.110.38 and www.bankofamerica.com (171.161.161.173)	8.3817 Mbytes	166.891 K packets
Between 10.100.110.36 and www.bankofamerica.com (171.161.161.173)	8.3306 Mbytes	165.879 K packets
Between 10.100.110.34 and www.bankofamerica.com (171.161.161.173)	8.2335 Mbytes	163.935 K packets
Between 10.100.110.35 and www.bankofamerica.com (171.161.161.173)	8.1783 Mbytes	162.829 K packets
Between 10.100.110.31 and www.bankofamerica.com (171.161.161.173)	8.1605 Mbytes	162.464 K packets
NTA3EVAL1	8.1605 Mbytes	162.464 K packets
NTA3EVAL1 - MS TCP Loopback interface	2.9147 Mbytes	58.042 K packets
NTA3EVAL1 - AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport	2.6416 Mbytes	52.593 K packets

Sowohl auf Stufe Knoten als auch auf Stufe Schnittstelle werden die durch das ausgewählte Gespräch konsumierten Anteile der Gesamtbandbreite in Bytes und Paketen aufgeführt. Für alle Knoten entspricht der Gesprächsverkehr auf dem Knoten der Summe des Gesprächsverkehrs auf allen Schnittstellen dieses Knotens.

Klicken auf den Namen eines Netzwerkgeräts öffnet die Ansicht NetFlow Conversation für jeglichen Verkehr zwischen den zwei Endpunkten, die über das ausgewählte Gerät miteinander kommunizieren.Für weitere Informationen siehe „NetFlow Conversation-Ansicht“ auf Seite 34.



Orion NetFlow Traffic Analyzer - Ansichten

Die folgenden Abschnitte beschreiben die Typen von Informationen, die auf ausgewählten Orion NTA-Ansichten standardmäßig vorhanden sind.

Hinweise:

- Es folgt eine Auswahl der am häufigsten verwendeten Orion NTA-Ansichten. Sie sind auf der NetFlow Traffic Analysis Summary-Ansicht über Standard-Ressourcen direkt verknüpft. Weitere Ressourcen verknüpfen zusätzliche Ansichten. Für weitere Informationen siehe „Viewing NetFlow Traffic Analyzer Data in the Orion Web Console“ in der *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.
- Einige Ressourcen sind in der Standardkonfiguration einer ausgewählten Ansicht u. U. nicht vorhanden. Um alle verfügbaren Ressourcen zu sehen, müssen Sie die Ansicht über die Admin-Ansicht der Orion NPM Web Console bearbeiten. Für weitere Informationen siehe „Viewing NetFlow Traffic Analyzer Data in the Orion Web Console“ in der *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

NetFlow Application-Ansicht

Die folgenden Abschnitte enthalten kurze Beschreibungen der Ressourcen auf der standardmäßigen NetFlow-Anwendungsansicht. Weitere Informationen über die einzelnen Ressourcen, einschließlich Konfigurationsdetails, können durch Klicken auf **Help** (Hilfe) in der Ressourcen-Überschriftsleiste eingesehen werden.

Anwendungsdetails

Die Ressource Application Details (Anwendungsdetails) liefert eine Tabelle, die die folgenden Informationen über die Anwendung und den Port enthalten, die Sie gerade betrachten:

- Anwendungsname
- Durch Anwendung verwendeter Port
- Gesamtmenge von Verkehrsdaten innerhalb der ausgewählten Zeitdauer
- Gesamtanzahl von innerhalb der ausgewählten Zeitdauer gesendeten Paketen

Aktivste 5 Protokolle

Die Ressource Top 5 Protocolls (Aktivste 5 Protokolle) liefert einen schnellen Einblick in die Verkehrsprotokolle, die die ausgewählte Anwendung am häufigsten verwendet. Die Tabelle unterhalb des Charts enthält den Protokolltyp, die Menge von Daten, die Gesamtanzahl von Paketen und den Prozentanteil des Gesamtverkehrs, den die einzelnen aufgeführten Protokolle genutzt haben.

Aktivste 5 Diensttypen

Die Ressource Top 5 Types of Service (Aktivste 5 Diensttypen) liefert einen schnellen Einblick in der Form eines Charts der aktivsten Dienste, die ausgewählte Anwendung einbezieht. Die Tabelle unterhalb des Charts bietet die folgenden Informationen für jeden Diensttyp:

- Diensttyp
- Die Menge von Verkehr, die der Dienst bewältigt
- Die Anzahl von Paketen, die der Dienst bewältigt
- Der Prozentanteil des gesamten durch den ausgewählten Diensttyp bewältigten Verkehrs zur ausgewählten Anwendung

Gesamtbytes übertragen

Die Ressource Total Bytes Transferred (Gesamtbytes übertragen) zeigt ein Chart an, das die Gesamtbytemenge angibt, die die durch die ausgewählte Anwendung innerhalb einer bestimmten Zeitdauer übertragen wurden. Eine breite Palette benutzerdefinierter Charts kann für Dokumentationszwecke ausgedruckt oder exportiert werden. Klicken auf das Chart öffnet die Seite Customize Chart (Chart anpassen) für das ausgewählte Chart. Für weitere Informationen über das Anpassen von Charts siehe „Customizing Charts in NetFlow Traffic Analyzer“ in der *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Eindeutige Besucher

Die Ressource Unique Visitors (Eindeutige Besucher) liefert ein Chart, das die Anzahl eindeutiger IP-Adressen angibt, die die ausgewählte Anwendung innerhalb einer bestimmten Zeitdauer verwendet haben. Eine breite Palette benutzerdefinierter Charts kann für Dokumentationszwecke ausgedruckt oder exportiert werden. Klicken auf das Chart öffnet die Seite Customize Chart (Chart anpassen) für das ausgewählte Chart. Für weitere Informationen über das Anpassen von Charts siehe „Customizing Charts in NetFlow Traffic Analyzer“ in der *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Gesamtpakete übertragen

Die Ressource Total Packets Transferred (Gesamtpakete übertragen) zeigt ein Chart an, das die Gesamtpaketmenge angibt, die die durch die ausgewählte Anwendung innerhalb einer bestimmten Zeitdauer übertragen wurden. Eine breite Palette benutzerdefinierter Charts kann für Dokumentationszwecke ausgedruckt oder exportiert werden. Klicken auf das Chart öffnet die Seite Customize Chart (Chart anpassen) für das ausgewählte Chart. Für weitere Informationen über das Anpassen von Charts siehe „Customizing Charts in NetFlow Traffic Analyzer“ in der *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Aktivste 5 Sender

Die Ressource Top 5 Transmitters (Aktivste 5 Sender) liefert einen schnellen Einblick in der Form eines Charts der aktivsten sendenden Endpunkte, die ausgewählte Anwendung verwenden. Die Tabelle unterhalb des Charts bietet die folgenden Informationen für jeden Endpunkt:

- Name bzw. IP-Adresse des Endpunkts
- Menge von Verkehr, der durch den Endpunkt gesendet wird

- Prozentanteil (Verkehr, der auf den Endpunkt zurückgeführt werden kann) des gesamten gesendeten Verkehrs

Sie können auf einen aufgeführten Endpunkt klicken, um die Ansicht NetFlow Endpoint (NetFlow-Endpunkt) zu öffnen, die ähnliche Statistiken für jeden sendenden Endpunkt präsentiert. Für weitere Informationen siehe „NetFlow Endpoint-Ansicht“ auf Seite 35.

Aktivste 5 Empfänger

Die Ressource Top 5 Receivers (Aktivste 5 Empfänger) liefert einen schnellen Einblick in der Form eines Charts der aktivsten empfangenden Endpunkte, die ausgewählte Anwendung verwenden. Die Tabelle unterhalb des Charts bietet die folgenden Informationen für jeden Endpunkt:

- Name bzw. IP-Adresse des Endpunkts
- Menge von Verkehr, der durch den Endpunkt empfangen wird
- Prozentanteil (Verkehr, der auf den Endpunkt zurückgeführt werden kann) des gesamten empfangenen Verkehrs

Sie können auf einen aufgeführten Endpunkt klicken, um die Ansicht NetFlow Endpoint (NetFlow-Endpunkt) zu öffnen, die ähnliche Statistiken für jeden empfangenden Endpunkt präsentiert. Für weitere Informationen siehe „NetFlow Endpoint-Ansicht“ auf Seite 35.

Aktivste 5 Verkehrsquellen nach Land

Die Ressource Top 5 Traffic Sources by Country (Aktivste 5 Verkehrsquellen nach Land) liefert einen schnellen Einblick in der Form eines Charts. Es zeigt die Länder, die Ursprung des Verkehrs der ausgewählten Anwendung sind, nach Prozentanteil des Gesamtanwendungsverkehrs. Die Tabelle unterhalb des Charts bietet die folgenden Informationen für jedes Land:

- Bezeichnung des Landes
- Menge von Verkehr, der den Ursprung in diesen Land hat
- Prozentanteil (Verkehr, der auf das Land zurückgeführt werden kann) des gesamten Verkehrs

Aktivste 5 Verkehrsziele nach Land

Die Ressource Top 5 Traffic Destinations by Country (Aktivste 5 Verkehrsziele nach Land) liefert einen schnellen Einblick in der Form eines Charts. Es zeigt die Länder, die Ziele des Verkehrs der ausgewählten Anwendung sind, nach Prozentanteil des Gesamtanwendungsverkehrs. Die Tabelle unterhalb des Charts bietet die folgenden Informationen für jedes Land:

- Bezeichnung des Landes
- Menge von Anwendungsverkehr, der durch Endpunkte in diesem Land geroutet wird
- Prozentanteil (Verkehr, der auf Endpunkte in diesem Land zurückgeführt werden kann) des gesamten Anwendungsverkehrs

Aktivste 5 Gespräche

Die Ressource Top 5 Conversations (Aktivste 5 Gespräche) liefert eine Liste der bandbreiten-intensivsten Gespräche, die durch das ausgewählte Gerät geroutet werden und die ausgewählte Anwendung verwenden. Gespräche werden aufgelistet mit der Menge von Daten, die im Gespräch übertragen wurden (Bytes und Paketen), und dem durch das Gespräch erzeugten Prozentanteil des Gesamtanwendungsverkehrs. Klicken auf ein Gespräch öffnet die Ansicht NetFlow Conversation (NetFlow-Gespräch) für das ausgewählte Gespräch. Für weitere Informationen siehe „NetFlow Conversation-Ansicht“ auf Seite 34.

NetFlow Conversation-Ansicht

Die folgenden Abschnitte enthalten kurze Beschreibungen der Ressourcen auf der standardmäßigen NetFlow-Gesprächsansicht. Weitere Informationen über die einzelnen Ressourcen, einschließlich Konfigurationsdetails, können durch Klicken auf **Help** (Hilfe) in der Ressouren-Überschriftsleiste eingesehen werden.

Gesamtbytes übertragen

Die Ressource Total Bytes Transferred (Gesamtbytes übertragen) zeigt ein Chart an, das die Gesamtbytemenge angibt, die zwischen den in der Ansichtsüberschrift angegebenen zwei Knoten, IP-Adressen oder Domains innerhalb einer bestimmten Zeitdauer übertragen wurden.

Gesprächsverkehrsverlauf

Die Ressource Conversation Traffic History (Gesprächsverkehrsverlauf) liefert eine Tabelle, die die folgenden Informationen für jeden aufgeführten Gesprächsaustausch enthält:

- Datums-/Uhrzeitstempel des Austauschs
- Protokoll, das für den Austausch verwendet wurde
- Anwendung und Port, die/der für den Austausch verwendet wurde
- Richtung des Verkehrsflusses
- Menge kommunizierten Verkehrs in Bytes
- Entsprechende Anzahl kommunizierter Pakete

NetFlow Endpoint-Ansicht

Die folgenden Abschnitte enthalten kurze Beschreibungen der Ressourcen auf der standardmäßigen NetFlow-Endpunktansicht. Weitere Informationen über die einzelnen Ressourcen, einschließlich Konfigurationsdetails, können durch Klicken auf **Help** (Hilfe) in der Ressourcen-Überschriftsleiste eingesehen werden.

Endpunktdetails

Die Ressource Endpoint Details (Endpunktdetails) liefert die folgenden Informationen über einen ausgewählten Endpunkt:

- IP-Adresse
- Hostname
- IP-Adressgruppe
- Domain
- Land
- Gesamtverkehr gesendet und empfangen
- Datums-/Uhrzeitstempel der zuletzt gesendeten und zuletzt empfangenen Daten

Aktivste 5 Gespräche

Die Ressource Top 5 Conversations (Aktivste 5 Gespräche) liefert eine Liste von Endpunkten, mit denen der derzeit angezeigte Endpunkt am meisten Daten übertragen hat. Diese Ressource meldet für jedes Gespräch die Menge der im Gespräch übertragener Daten und den Prozentanteil der durch den angezeigten Endpunkt übertragenen Gesamtdaten. Klicken auf einen Endpunkt öffnet die Ansicht NetFlow Endpoint (NetFlow-Endpunkt) für den ausgewählten Endpunkt. Alle weiteren Links für einen aufgeführten Endpunkt öffnen die Ansicht NetFlow Conversation (NetFlow-Gespräch) für das Gespräch zwischen den angezeigten und ausgewählten Endpunkten. Für weitere Informationen siehe „NetFlow Conversation-Ansicht“ auf Seite 34.

Gesamtpakete übertragen

Die Ressource Total Packets Transferred (Gesamtpakete übertragen) zeigt ein Chart an, das die Gesamtpaketmenge angibt, die durch den ausgewählten Endpunkt innerhalb einer bestimmten Zeitdauer gesendet bzw. empfangen wurden.

Gesamtbytes übertragen

Die Ressource Total Bytes Transferred (Gesamtbytes übertragen) zeigt eine Tabelle an, das die Gesamtbytemenge angibt, die durch den ausgewählten Endpunkt innerhalb einer bestimmten Zeitdauer gesendet bzw. empfangen wurden.

Aktivste 5 Protokolle

Die Ressource Top 5 Protocolls (Aktivste 5 Protokolle) liefert einen schnellen Einblick in die Verkehrsprotokolle, die der ausgewählte Endpunkt am häufigsten verwendet. Die Tabelle unterhalb des Charts enthält den Protokolltyp, die Menge von Daten, die Gesamtanzahl von Paketen und den Prozentanteil des Gesamtverkehrs, den die einzelnen aufgeführten Protokolle genutzt haben.

Aktivste 5 Anwendungen

Die Ressource Top 5 Applications (Aktivste 5 Anwendungen) liefert einen schnellen Einblick in die Anwendungen, die der ausgewählte Endpunkt am häufigsten verwendet. Die Tabelle unterhalb des Charts enthält den Anwendungsnamen, die Menge von Daten (Datenfluss), die entsprechende Gesamtanzahl von Paketen und den Prozentanteil des Gesamtverkehrs, der auf die Verwendung der aufgeführten Anwendung durch den ausgewählten Endpunkt zurückgeführt werden kann. Klicken auf eine Anwendung öffnet die Ansicht NetFlow Application (NetFlow-Anwendung). Für weitere Informationen siehe „NetFlow Application-Ansicht“ auf Seite 31.

Aktivste 5 Verkehrsquellen nach Land

Die Ressource Top 5 Traffic Sources by Country (Aktivste 5 Verkehrsquellen nach Land) liefert einen schnellen Einblick in der Form eines Charts. Es zeigt die Länder, die Ursprung des Verkehrs zum ausgewählten Endpunkt sind, nach Prozentanteil des Gesamtanwendungsverkehrs zum ausgewählten Endpunkt. Die Tabelle unterhalb des Charts enthält den Namen des Landes, das Ursprung von Verkehr zum angezeigten Endpunkt ist, die Menge von Daten, die vom aufgeführten Land zum Endpunkt geroutet wurden, und den Prozentanteil des Gesamtverkehrs zum angezeigten Endpunkt, der auf das aufgeführte Land zurückgeführt werden kann.

Aktivste 5 Verkehrsziele nach Land

Die Ressource Top 5 Traffic Destinations by Country (Aktivste 5 Verkehrsziele nach Land) liefert ein Chart und eine Tabelle der Länder, die Hosting-Ziele von

Verkehr vom ausgewählten Endpunkt sind, nach Prozentanteil des Gesamtverkehrs vom ausgewählten Endpunkt. Die Tabelle unterhalb des Charts enthält den Namen des Landes, zu dem Verkehr geroutet wird, die Menge von zu Servern im aufgeführten Land geroutetem Verkehr, und den Prozentanteil von jeglichem vom angezeigten Endpunkt geroutetem Verkehr zu Servern im aufgeführten Land.

Eindeutige Besucher

Die Ressource Unique Visitors (Eindeutige Besucher) liefert ein Chart eindeutiger IP-Adressen, die innerhalb einer bestimmten Zeitdauer mit dem angezeigten Endpunkt kommuniziert haben.

Aktivste 5 Diensttypen

Die Ressource Top 5 Types of Service (Aktivste 5 Diensttypen) liefert einen schnellen Einblick in die Dienste, die durch den ausgewählten Endpunkt am häufigsten verwendet werden. Die Tabelle unterhalb des Charts bietet die folgenden Informationen für jeden Diensttyp:

- Diensttyp
- Menge von Verkehr (in Bytes und Paketen), die der Dienst bewältigt
- Prozentanteil des gesamten durch den Diensttyp bewältigten Verkehrs zum ausgewählten Endpunkt

Für weitere Informationen über Diensttypüberwachung in Orion NTA siehe „Configuring NetFlow Types of Services“ in der *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

NetFlow Interface Details-Ansicht

Die folgenden Abschnitte enthalten kurze Beschreibungen der Ressourcen auf der standardmäßigen NetFlow-Schnittstellendetail-Ansicht. Weitere Informationen über die einzelnen Ressourcen, einschließlich Konfigurationsdetails, können durch Klicken auf **Help** (Hilfe) in der Ressourcen-Überschriftsleiste eingesehen werden.

Aktivste 5 Protokolle

Die Ressource Top 5 Protocolls (Aktivste 5 Protokolle) liefert einen schnellen Einblick in die Verkehrsprotokolle, die die ausgewählte Schnittstelle am häufigsten beobachtet. Die Tabelle unterhalb des Charts enthält den Protokolltyp, die Menge von Daten, die Gesamtanzahl von Paketen und den Prozentanteil des Gesamtverkehrs über die angezeigte Schnittstelle unter Verwendung der aufgeführten Protokolle.

Aktivste 5 Endpunkte

Die Ressource Top 5 Endpoints (Aktivste 5 Endpunkte) liefert eine Chart- und eine Tabelleansicht der Endpunkte, die am meisten Verkehr über die ausgewählte Schnittstelle erzeugen. Die Tabelle unterhalb des Charts enthält den Namen oder die IP-Adresse jedes aufgeführten Endpunkts, die Menge von Verkehr von jedem aufgeführten Endpunkt (in Bytes und Paketen) und den Prozentanteil des Gesamtverkehrs über die angezeigte Schnittstelle, die zu den einzelnen Endpunkten zurückgeführt werden können. Klicken auf einen Endpunkt öffnet die Ansicht NetFlow Endpoint (NetFlow-Endpunkt) für den ausgewählten Endpunkt. Für weitere Informationen siehe „NetFlow Conversation-Ansicht“ auf Seite 34.

Aktivste 5 Anwendungen

Die Ressource Top 5 Applications (Aktivste 5 Anwendungen) liefert einen schnellen Einblick in die Anwendungen, die durch die angezeigte Schnittstelle am häufigsten verwendet werden. Die Tabelle unterhalb des Charts enthält den Anwendungsnamen, die Menge von Daten (Datenfluss), die entsprechende Gesamtanzahl von Paketen und den Prozentanteil des Gesamtverkehrs, der auf die Verwendung der aufgeführten Anwendung durch die angezeigte Schnittstelle zurückgeführt werden kann. Klicken auf eine Anwendung öffnet die Ansicht NetFlow Application (NetFlow-Anwendung). Für weitere Informationen siehe „NetFlow Conversation-Ansicht“ auf Seite 34.

Aktivste 5 Domains

Die Ressource Top 5 Domains (Aktivste 5 Domains) liefert einen schnellen Einblick in die Domains, die auf der ausgewählten Schnittstelle am meisten Verkehr erzeugen. Die Tabelle unterhalb des Charts enthält den Domain-Namen, die Menge von Verkehr in Bytes, die Gesamtanzahl kommunizierter Pakete und den Prozentanteil des Gesamtverkehrs auf der ausgewählten Schnittstelle, der auf die einzelnen Domains zurückgeführt werden kann.

Aktivste 5 Diensttypen

Die Ressource Top 5 Types of Service (Aktivste 5 Diensttypen) liefert einen schnellen Einblick in die Dienste, die durch die angezeigte Schnittstelle am häufigsten verwendet werden. Die Tabelle unterhalb des Charts bietet die folgenden Informationen für jeden Diensttyp:

- Diensttyp
- Menge von Verkehr (in Bytes und Paketen), die der Dienst über die Schnittstelle bewältigt
- Prozentanteil des über die angezeigte Schnittstelle übertragenen Verkehrs, der durch den ausgewählten Diensttyp bewältigten wurde

Für weitere Informationen über Diensttypüberwachung in Orion NTA siehe „Configuring NetFlow Types of Services“ in der *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Aktivste 5 Gespräche

Die Ressource Top 5 Conversations (Aktivste 5 Gespräche) liefert eine Liste der Gespräche, die am meisten Verkehr über die angezeigte Schnittstelle erzeugen. Diese Ressource meldet für jedes Gespräch die Menge der im Gespräch übertragener Daten und den Prozentanteil der über die angezeigte Schnittstelle übertragenen Gesamtdaten. Klicken auf ein Gespräch öffnet die Ansicht NetFlow Conversation (NetFlow-Gespräch) für das ausgewählte Gespräch. Für weitere Informationen siehe „NetFlow Conversation-Ansicht“ auf Seite 34.

NetFlow Node Details-Ansicht

Die folgenden Abschnitte enthalten kurze Beschreibungen der Ressourcen auf der standardmäßigen NetFlow-Knotendetail-Ansicht. Weitere Informationen über die einzelnen Ressourcen, einschließlich Konfigurationsdetails, können durch Klicken auf **Help** (Hilfe) in der Ressourcen-Überschriftsleiste eingesehen werden.

Aktivste 5 Protokolle

Die Ressource Top 5 Protocolls (Aktivste 5 Protokolle) liefert einen schnellen Einblick auf die Verkehrsprotokolle, die der angezeigte Knoten am häufigsten verwendet. Die Tabelle unterhalb des Charts enthält den Protokolltyp, die Menge von Daten, die Gesamtanzahl von Paketen und den Prozentanteil des Gesamtverkehrs über den angezeigten Knoten unter Verwendung der aufgeführten Protokolle.

Aktivste 5 Anwendungen

Die Ressource Top 5 Applications (Aktivste 5 Anwendungen) liefert einen schnellen Einblick in die Anwendungen, die durch den angezeigten Knoten am häufigsten verwendet werden. Die Tabelle unterhalb des Charts enthält den Anwendungsnamen, die Menge von Daten (Datenfluss), die entsprechende Gesamtanzahl von Paketen und den Prozentanteil des Gesamtverkehrs, der auf die Verwendung der aufgeführten Anwendung durch den angezeigten Knoten zurückgeführt werden kann. Klicken auf eine Anwendung öffnet die Ansicht NetFlow Application (NetFlow-Anwendung). Für weitere Informationen siehe „NetFlow Application-Ansicht“ auf Seite 31.

Aktivste 5 Gespräche

Die Ressource Top 5 Conversations (Aktivste 5 Gespräche) liefert eine Liste der Gespräche, die am meisten Verkehr über den angezeigten Knoten erzeugen. Diese Ressource meldet für jedes Gespräch die Menge der im Gespräch übertragener Daten und den Prozentanteil der über den angezeigten Knoten übertragenen Gesamtdaten. Klicken auf ein Gespräch öffnet die Ansicht NetFlow Conversation (NetFlow-Gespräch) für das ausgewählte Gespräch. Für weitere Informationen siehe „NetFlow Conversation-Ansicht“ auf Seite 34.

Aktivste 5 Endpunkte

Die Ressource Top 5 Endpoints (Aktivste 5 Endpunkte) liefert eine Chart- und eine Tabelleansicht der Endpunkte, die am meisten Verkehr über den angezeigten Knoten erzeugen. Die Tabelle unterhalb des Charts enthält den Namen oder die IP-Adresse jedes aufgeführten Endpunkts, die Menge von Verkehr von jedem aufgeführten Endpunkt (in Bytes und Paketen) und den Prozentanteil des Gesamtverkehrs über den angezeigten Knoten, die zu den einzelnen Endpunkten zurückgeführt werden können. Klicken auf einen Endpunkt öffnet die Ansicht NetFlow Endpoint (NetFlow-Endpunkt) für den ausgewählten Endpunkt. Für weitere Informationen siehe NetFlow Endpoint-Ansicht” auf Seite 35.

Aktivste 5 Domains

Die Ressource Top 5 Domains (Aktivste 5 Domains) liefert einen schnellen Einblick in die Domains, die auf dem angezeigten Knoten am meisten Verkehr erzeugen. Die Tabelle unterhalb des Charts enthält den Domain-Namen, die Menge von Verkehr in Bytes, die Gesamtanzahl kommunizierter Pakete und den Prozentanteil des Gesamtverkehrs auf dem angezeigten Knoten, der auf die einzelnen Domains zurückgeführt werden kann.

Knotenschnittstellen

Die Ressource Node Interfaces (Knotenschnittstellen) liefert eine Liste aller überwachten Schnittstellen auf dem angezeigten Knoten. Für jede Schnittstelle werden eingehender Verkehr und abgehender Verkehr gemeldet. Klicken auf eine Schnittstelle öffnet die Ansicht NetFlow Interface Details (NetFlow-Schnittstellendetails) für die ausgewählte Schnittstelle. Für weitere Informationen siehe „NetFlow Interface Details-Ansicht“ auf Seite 37.

Kapitel 4

Verwendung von Orion NetFlow Traffic Analyzer

Orion Network Performance Monitor kann die Bandbreitennutzung auf einer gegebenen Schnittstelle anzeigen. Orion NetFlow Traffic Analyzer geht einen Schritt weiter und liefert mehr Informationen über die derzeitigen Nutzer dieser Bandbreite und die Anwendungen, die sie verwenden. Die in diesem Kapitel präsentierten Szenarien veranschaulichen den Wert von Orion NetFlow Traffic Analyzer und wie das Produkt Ihnen unverzüglich in bedeutender Weise nützlich sein kann.

Verwendung von Traffic View Builder

Mit der Ressource Traffic View Builder können Sie schnell eigene benutzerdefinierte Ansichten für beliebige NetFlow-aktivierte Geräte erstellen. Traffic View Builder ermöglicht die Erstellung eigener Versionen aller in der folgenden Tabelle aufgeführten Ansichten.

Traffic View Builder - Ansichtstypen		
Application (Anwendung)	Country (Land)	Domain
Endpoint (Endpunkt)	Interface (Schnittstelle)	IP Address Group (IP-Adressgruppe)
Protocol (Protokoll)	Router	Type of Service (Diensttyp)

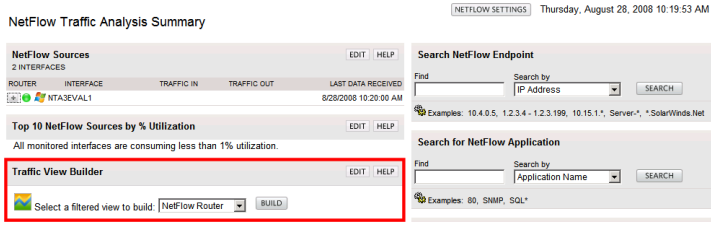
Die folgenden Abschnitte präsentieren Szenarien, die aufzeigen, wie Sie mit der Orion NTA-Ressource Traffic View Builder eigene Ansichten erstellen können.

Anzeigen von Verkehr für eine bestimmte IP-Adresse

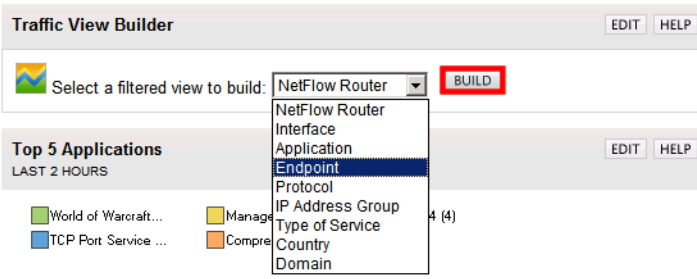
Das folgende Verfahren erstellt eine benutzerdefinierte Orion NTA-Ansicht, die sowohl eingehenden als auch abgehenden Netzwerkverkehr einer bestimmten IP-Adresse anzeigt.

Erstellen einer Ansicht für eine spezifische IP-Adresse:

1. Klicken Sie auf **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Start > Alle Programme > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console) und navigieren Sie zur Ressource Traffic View Builder.

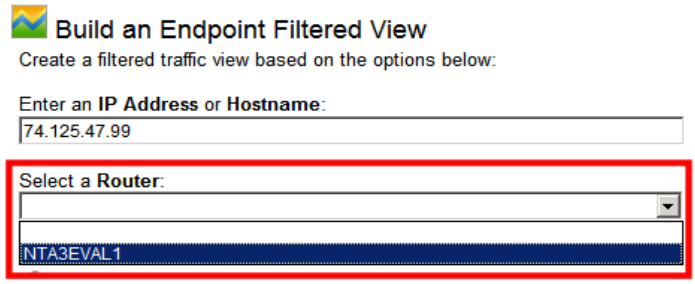


2. Wählen Sie **Endpoint** (Endpunkt) aus und klicken Sie dann auf **Build** (Erstellen).



3. Geben Sie die zu überwachende **IP address** (IP-Adresse) ein.

4. Wählen Sie den Router aus, der Verkehr zur ausgewählten IP-Adresse sendet.



5. Wählen Sie **All Interfaces** (Alle Schnittstellen) aus, wenn das Menü Select an Interface (Schnittstelle auswählen) eingeblendet wird.

   Hinweis: Sie können Ihre Ansicht weiter anpassen, um beispielsweise nur Verkehr auf einer bestimmten Schnittstelle des Routers anzuzeigen, doch für den Zweck dieser Evaluierung wählen Sie **All Interfaces** (Alle Schnittstellen) aus, um jeglichen Verkehr über den ausgewählten Router anzuzeigen.

6. Klicken Sie auf **Submit** (Übermitteln), sodass Ihre benutzerdefinierte NetFlow-Endpunkt-Ansicht eingeblendet wird.

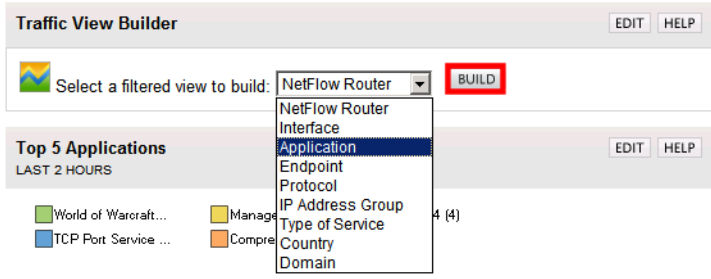
   Hinweis: Für weitere Informationen über die Ansicht NetFlow Endpoint und deren Standardressourcen siehe “NetFlow Endpoint-Ansicht” auf Seite 35.

Anzeigen von Verkehr für bestimmte Ports oder Anwendungen

Das folgende Verfahren erstellt eine benutzerdefinierte Orion NTA-Ansicht, die Netzwerkverkehr über angegebenen Ports oder zu bestimmten Anwendungen anzeigt.

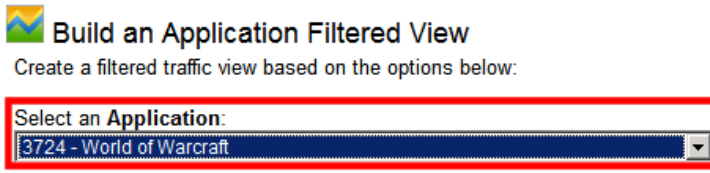
Erstellen einer Ansicht für spezifische Ports oder Anwendungen:

1. Klicken Sie auf **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Start > Alle Programme > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console) und finden Sie dann die Ressource Traffic View Builder.
2. Wählen Sie **Application** (Anwendung) aus und klicken Sie dann auf **Build** (Erstellen).



3. Wählen Sie die zu überwachende **Application** (Anwendung) bzw. den zu überwachenden Port aus.

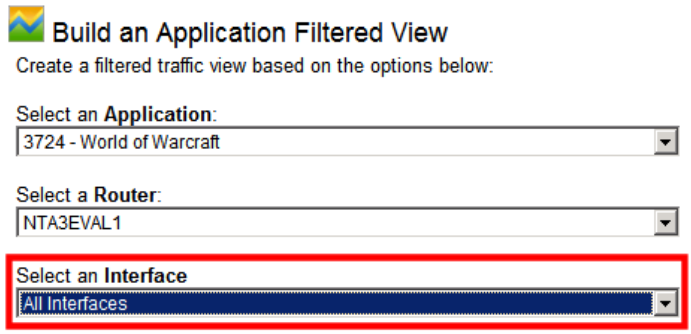
   Hinweis: Anwendungen werden nach zugeordneten Portnummern aufgelistet. Um die Zuordnungen der Anwendungsportnummern zu ermitteln, verwenden Sie die Ressource Search for NetFlow Application auf der Ansicht NetFlow Traffic Analysis Summary. Für weitere Informationen siehe “Suche nach NetFlow-Anwendung” auf Seite 27.



4. Wählen Sie den NetFlow-aktivierten Router aus, der Ihren Anwendungsverkehr routet.

5. Wählen Sie **All Interfaces** (Alle Schnittstellen) aus, wenn das Menü Select an Interface (Schnittstelle auswählen) eingeblendet wird.

   Hinweis: Sie können Ihre Ansicht weiter anpassen, um beispielsweise nur Anwendungsverkehr auf einer bestimmten Schnittstelle des Routers anzuzeigen, doch für den Zweck dieser Evaluierung wählen Sie **All Interfaces** (Alle Schnittstellen) aus, um jeglichen Verkehr über den ausgewählten Router anzuzeigen.



6. Klicken Sie auf **Submit** (Übermitteln), sodass Ihre benutzerdefinierte NetFlow-Anwendungs-Ansicht eingeblendet wird.

Hinweis: Für weitere Informationen über die Ansicht NetFlow Application und deren Standardressourcen siehe “NetFlow Application-Ansicht” auf Seite 31.

Auffinden und Absondern eines infizierten Computers

Sie können Ihre derzeit installierte Orion NPM-Instanz zusammen mit Orion NTA verwenden, um eine breite Palette sich selbst fortpflanzender Viren, die Ihr Netzwerk angreifen können, zu bestimmen und darauf zu reagieren. Ziehen Sie das folgende Szenario in Betracht:

1. Eine lokale Zweigstelle Ihres Banknetzwerks, die alle Kreditkartentransaktionen abwickelt beschwert sich über ein außerordentlich träges Netzwerk, das häufige Zeitüberschreitungen während kritischer Datenübertragungen verursacht.
2. Die Orion Web Console zeigt, dass die Verbindung zum Zweigstellennetzwerk in Betrieb ist.
3. Orion NPM Percent Utilization-Charts auf der Network Summary-Startseite zeigen, dass die erzeitige Auslastung 98 % beträgt. Die Zweigstellennetzwerkauslastung liegt jedoch normalerweise bei 15-25 %.
4. Klicken Sie auf der Modules-Symbolleiste auf **NetFlow Traffic Analysis** (Netzwerkverkehrsanalyse), und klicken Sie dann in der Ressource NetFlow Sources auf den Namen der Zweigstellen-Netzwerkverbindung, um den NetFlow-aktivierten Router im Zweigstellen-Netzwerk anzuzeigen.
5. Mit einem kurzen Blick auf die Ressource Top 5 Endpoints (Aktivste 5 Endpunkte) können Sie einen Computer im IP-Adressbereich `10.10.10.0-10.10.10.255` erkennen, der 80 % der Belastung auf der Zweigstellenverbindung erzeugt.
6. Sie wissen, dass Computer in diesem IP-Adressbereich Kunden für persönliche Transaktionen unter Verwendung des Internets zur Verfügung stehen.
7. Durch Betrachten der Ressource Top 5 Applications (Aktivste 5 Anwendungen) können Sie schnell erkennen, dass 100 % der letzen zwei Stunden von Verkehr von einem öffentlich zugänglichen Computer durch eine IBM MQSeries Messaging-Anwendung erzeugt wurde.
8. Durch Klicken auf die IBM MQSeries Messaging-Anwendung in der Ressource Top 5 Applications können Sie bestimmen, dass die IBM MQSeries Messaging-Anwendung über Port 1883 betrieben wird.

9. Da Sie wissen, dass die Geräte am kundenzugänglichen Standort weder IBM MQSeries Messaging noch einen Dienst oder ein Protokoll verwenden, der/das Port 1883 erfordert, können Sie erkennen, dass es sich um einen Virenangriff handelt.
10. Verwenden Sie ein Konfigurationsmanagementtool wie Cirrus Configuration Manager und laden Sie eine neue Konfiguration, die Port 1883 blockiert, auf Ihre Firewall.

Auffinden und Blockieren unerwünschter Nutzung

Mit Orion NTA können Sie erhöhte Nutzung auf einem Ihrer Netzwerk-Uplinks einfach feststellen und aufzeichnen. Mit Orion NPM können Sie Netzwerkauslastung aufzeichnen, doch Orion NTA geht einen Schritt weiter. Sie können damit spezifische Instanzen unerwünschter Nutzung auffinden und wie im nachfolgenden Beispiel unverzüglich Abhilfemaßnahmen durchführen:

1. Der Uplink zum Internet hat sich während der letzten 6 Monate nach und nach verlangsamt, obwohl die Anzahl der Unternehmensmitarbeiter, Anwendungsnutzung und zugeordnete Bandbreite stabil geblieben sind.
2. Wenn Sie die Orion Web Console öffnen, zeigt die Network Summary Home-Ansicht an, dass Ihre Standortverbindung zum Internet in Betrieb ist. Wenn Sie jedoch auf den spezifische Uplink klicken und die Current Percent Utilization (Derzeitige Prozentauslastung) der einzelnen Schnittstellencharts einsehen, können Sie erkennen, dass die derzeitige Auslastung Ihrer Schnittstelle zum Internet 80 % beträgt.
3. Klicken Sie auf Ihre Schnittstelle zum Internet, um die Interface Details-Ansicht zu öffnen.
4. Passen Sie das Percent Utilization-Chart an, um die letzten 6 Monate anzuzeigen. Sie sehen, dass der Verbrauch nach und nach von 15 % auf 80 % angestiegen ist. Es gibt sogar Spitzen über 90 %.
5. Klicken Sie auf die Registerkarte NetFlow Traffic Analysis (NetFlow-Verkehrsanalyse) und klicken Sie auf dann Ihre Schnittstelle zum Internet, um die NetFlow Interface Details-Ansicht zu öffnen.
6. Betrachten Sie die 50 aktivsten Endpunkte. Sie sehen, dass eine Gruppe von Computern im IP-Adressbereich `10.10.12.0-10.10.12.255` einen Großteil der Bandbreite konsumiert. Diese Computer befinden sich im IP-Adressbereich von Internal Sales.
7. Sie beginnen jede einzelne verdächtige IP-Adresse zu untersuchen und stellen fest, dass alle untersuchten Adressen Kazaa (Port 1214) und World of Warcraft (Port 3724) in den aktivsten 5 Anwendungen haben.

8. Verwenden Sie ein Konfigurationsmanagementtool wie Cirrus Configuration Manager und laden Sie eine neue Konfiguration, die Port 1214 und Port 3724 blockiert, auf Ihre Firewall.
9. Der Verkehr auf der Schnittstelle geht innerhalb von Minuten auf 25 % zurück.

Erkennen und Vereiteln von Dienstverweigerungsangriffen

Orion NTA ermöglicht, abgehenden und eingehenden Verkehr auf einfache Weise zu charakterisieren. Diese Fähigkeit wird noch bedeutender, da Unternehmensnetzwerke vermehrt Dienstverweigerungsangriffen (Denial of Service Attacks) ausgesetzt sind, die immer tückischer werden. Ziehen Sie das folgende Szenario in Betracht:

1. Ein erweiterter Orion-NPM-Alarm teilt Ihnen mit, dass Ihr Router zum Internet Probleme hat, eine stabile Verbindung zum Internet herzustellen und zu unterhalten.
2. Sie öffnen die Orion Web Console, um nach möglichen Problemen zu suchen. Alle Verbindungen sind derzeit in Betrieb und die Bandbreitenauslastung sieht gut aus. Doch dann bemerken Sie die CPU-Auslastung auf dem Firewall-Knoten. Sie liegt stetig zwischen 99 % und 100 %.
3. Klicken auf den Firewall-Knotennamen öffnet dessen Node Details-Seite, wo die derzeitige Prozentauslastung der Schnittstellenressourcen aufzeigen, dass Ihre Firewall-Schnittstellen ungewöhnlich große Mengen von Verkehr bewältigen.
4. Sie klicken auf der Modules-Symbolleiste auf **NetFlow Traffic Analysis** (NetFlow-Verkehrsanalyse), um einen schnellen Einblick in Ihre benutzerdefinierte Ressource mit den 50 aktivsten Endpunkten zu erhalten.
5. Die Ressource der 50 aktivsten Endpunkte zeigt, dass die aktivsten 6 Computer versuchen, von Übersee auf Ihr Netzwerk zuzugreifen.
6. Sie erkennen, dass Ihre Ports gescannt werden und Ihre Firewall diese Angriffe interaktiv blockiert.
7. Verwenden Sie ein Konfigurationsmanagementtool wie Cirrus Configuration Manager und laden Sie eine neue Firewall-Konfiguration, die jeglichen Verkehr über den IP-Adressbereich der Computer blockiert, die versuchen in Ihr Netzwerk einzudringen.
8. Die CPU-Auslastung Ihres Routers zum Internet geht innerhalb von Minuten auf Normalwerte zurück.

Orion NTA weiter untersuchen

Die geführte Quick-Tour durch Orion NetFlow Traffic Analyzer ist hiermit abgeschlossen. Diese *Evaluation Guide* die breite in Orion NTA verfügbare Palette von NetFlow-aktivierten Netzwerk-überwachungs- und Netzwerkmanagementfunktionen und zugehöriger Module in keiner Weise vollständig. Bitte erkunden Sie die *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*, online unter http://www.solarwinds.com/support/documentation.aspx, um noch mehr über die Leistungsfähigkeit und Eignung von Orion NetFlow Traffic Analyzer zu erfahren.