SolarWinds Orion NetFlow Traffic Analyzer

Evaluation Guide

Orion NetFlow Traffic Analyzer Evaluation Guide, Version 3.0, 08.28.2008

Chi è SolarWinds

SolarWinds, Inc. sviluppa e commercializza un'ampia gamma di strumenti di rilevazione, monitoraggio e gestione di rete per rispondere ai diversi requisiti di consulenti e specialisti di gestione delle reti. I prodotti SolarWinds continuano a stabilire gli standard di qualità e prestazioni e hanno fatto dell'azienda il leader nella tecnologia della rilevazione e gestione di reti. Tra i clienti SolarWinds figura oltre il 45 percento delle aziende Fortune 500 e clienti in oltre 90 paesi. La nostra rete globale di partner commerciali è composta da oltre 100 distributori e rivenditori.

Per contattare SolarWinds

È possibile contattare SolarWinds in vari modi:

Uffici o siti	Recapiti
Vendite	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Assistenza tecnica	www.solarwinds.com/support
Forum utenti	www.thwack.com

Convenzioni

Nei vari documenti si utilizzano in modo coerente le seguenti convenzioni, che facilitano l'identificazione degli elementi sia nella documentazione cartacea che in quella online.

Convenzione	Elementi specificati
Grassetto	Elementi Windows, inclusi pulsanti e campi.
Corsivo	Titoli di libri e CD, nomi di variabili, nuovi termini.
`Caratteri a spaziatura fissa`	Nomi di file e directory, esempi di comandi e istruzioni di programmazione, testo digitato dall'utente.
Parentesi quadre, come in [*valore*]	Parametri di comando opzionali.
Parentesi graffe, come in {*valore*}	Parametri di comando necessari.
OR logico, come in *valore1*|*valore2*	Parametri di comando esclusivi, in cui è possibile specificare solo una delle opzioni.

SolarWinds Orion NetFlow Traffic Analyzer – Documentazione

La documentazione SolarWinds Orion NetFlow Traffic Analyzer include i seguenti documenti:

Documento	Scopo
Guida dell'amministratore	Fornisce informazioni dettagliate di tipo concettuale, sulle impostazioni e sulla configurazione.
Guida in linea	Visualizza pagine pertinenti della guida per ogni finestra dell'interfaccia utente Orion NetFlow Traffic Analyzer.
Evaluation Guide (Guida alla valutazione)	Introduce le caratteristiche di Orion Network Performance Monitor e presenta le istruzioni per l'installazione e la configurazione iniziale.
Guida di avviamento rapido	Presenta le istruzioni per l'installazione e la configurazione nonché scenari in cui Orion NetFlow Traffic Analyzer offre una soluzione semplice ed efficace.
Note di rilascio	Informazioni aggiornate e su problemi noti. Le note di rilascio più recenti sono reperibili sul sito www.solarwinds.com.

Indice

Capitolo 1

Introduzione a Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) rappresenta per gli specialisti IT una soluzione di semplice uso e scalabile per il monitoraggio di reti NetFlow-, sFlow- o J-Flow, indipendentemente dalle loro dimensioni.

Vantaggi generali di Orion NetFlow Traffic Analyzer

A mano a mano che un'azienda cresce e si sviluppa la sua rete, aumenta esponenzialmente la larghezza di banda necessaria. Tutte le moderne aziende collegate in rete investono risorse umane e capitali notevoli per assicurare la disponibilità di una larghezza di banda sufficiente per le attività e le applicazioni essenziali. Quando la larghezza di banda supera la capacità attualmente disponibile o quando la richiesta sembra eccedere le capacità della rete, occorre prendere una decisione complessa: stabilire se è necessario investire in una maggiore larghezza di banda o se linee guida più rigorose sull'utilizzo sono sufficienti a recuperare la larghezza di banda persa.

Con l'avvento dei media in streaming, delle tecnologie VoIP (Voice over IP), dei giochi online e di altre applicazioni che richiedono notevoli larghezze di banda, un ingegnere di rete deve rispondere a domande ben più complesse della semplice: la rete al momento è in funzione o no? Deve poter spiegare perché la rete non funziona ai livelli prestazionali che ci si aspetta.

Se occorre sapere come e da chi viene utilizzata la larghezza di banda della rete, Orion NetFlow Traffic Analyzer offre una risposta semplice e integrata, permettendo di rilevare rapidamente e monitorare l'utilizzo della larghezza di banda fatto da una particolare applicazione o da un certo tipo di traffico. Ad esempio, se si osserva un utilizzo eccessivo della larghezza di banda su una certa interfaccia, si può adoperare Orion NetFlow Traffic Analyzer per determinare che una riunione aziendale, attuata in video streaming, sta consumando l'80% della larghezza di banda disponibile attraverso un certo switch. A differenza di numerosi altri prodotti di analisi NetFlow, i dati di rete e NetFlow forniti dalla soluzione Orion NetFlow Traffic Analyzer non sono dati puramente estrapolati, bensì basati su informazioni reali sulla rete acquisite da Orion Network Performance Monitor, il modulo alla base di Orion NetFlow Traffic Analyzer.

Senza bisogno di configurazioni complesse, Orion NetFlow Traffic Analyzer offre ampie funzionalità di monitoraggio e creazione di grafici e tabelle, insieme con statistiche basate su dettagli importanti:

- Distribuzione della larghezza di banda tra i vari tipi di traffico
- Schemi di utilizzo nel corso del tempo
- Identificazione e monitoraggio del traffico esterno
- Stretta integrazione con statistiche dettagliate sulle prestazioni delle interfacce.

Queste funzionalità di monitoraggio, unitamente alla console web Orion Network Performance Monitor e ai motori di reporting, fa di Orion NetFlow Traffic Analyzer la scelta ideale per il monitoraggio di una NetFlow.

Vantaggi dettagliati di Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer consente di monitorare velocemente e agevolmente risorse e schemi di utilizzo della rete con un livello di dettagli personalizzabile. Le seguenti sono le funzionalità più importanti di Orion NetFlow Traffic Analyzer:

Prestazioni e disponibilità migliori

Con Orion NetFlow Traffic Analyzer è possibile rilevare, diagnosticare e risolvere più velocemente rallentamenti e interruzioni della funzionalità delle rete.

Pianificazione della capacità analitica

Orion NetFlow Traffic Analyzer evidenzia tendenze nel traffico di rete, consentendo di anticipare in modo intelligente variazioni della larghezza di banda nelle aree in cui si verificano ingorghi.

Assegnazione ottimizzata delle risorse di rete

Le informazioni fornite da Orion NetFlow Traffic Analyzer consentono di individuare le aree della rete in cui sono presenti connessioni limitate o sovraccaricate. Si può quindi reinstradare il traffico su altre aree della rete che abbiano la larghezza di banda disponibile.

Allineamento delle risorse IT alle necessità aziendali

Poiché Orion NetFlow Traffic Analyzer è basato sulla comprovata infrastruttura di Orion Network Performance Monitor, è possibile valutare sia le esigenze della rete aziendale a livello generale sia i dettagli funzionali di interfacce e nodi specifici.

Maggiore sicurezza della rete

Orion NetFlow Traffic Analyzer permette di esaminare velocemente e con precisione il traffico di rete e quindi individuare e analizzare schemi insoliti, funzionamenti indesiderati e utilizzi anomali che potrebbero indicare la presenza di virus, bot o spyware.

Un'applicazione integrata di monitoraggio delle prestazioni della rete e NetFlow

Finalmente non è più necessario passare da un programma all'altro per ottenere un quadro completo dell'utilizzo, delle prestazioni e delle esigenze della rete. Orion Network Performance Monitor e Orion NetFlow Traffic Analyzer offrono tutte le funzionalità necessarie per il monitoraggio di una rete.

Funzionalità di Orion NTA versione 3.0

Orion NTA versione 3.0 offre le seguenti funzionalità per consentire di monitorare meglio le periferiche NetFlow della rete.

Ricerca secondo l'intervallo di indirizzi IP

Questa versione di Orion NTA permette di cercare punti terminali in un intervallo specifico di indirizzi IP (ad esempio, `10.10.199.1-10.10.199.50`).

Supporto per ulteriori flussi

Orion NTA versione 3 attualmente supporta i formati NetFlow v9, sFlow v5 e J-flow per la raccolta dei dati del traffico di rete.

Viste del traffico personalizzate

Grazie a Traffic View Builder, incluso in questa versione di Orion NTA, è possibile filtrare i dati NetFlow acquisiti per creare viste personalizzate accessibili. Ad esempio, si può creare una vista che mostri il traffico diretto verso un certo dominio, generato durante il normale orario di ufficio (8 - 17) da un indirizzo IP selezionato.

Risorsa di elencazione delle 10 sorgenti NetFlow più attive in base all'utilizzo percentuale

Una nuova risorsa sulla vista riepilogativa NetFlow Summary elenca le sorgenti NetFlow monitorate secondo l'utilizzo percentuale.

Viste prestazionali QoS (**Quality of Service**)

Orion NTA versione 3 permette di visualizzare facilmente il traffico di rete complessivo segmentato secondo metodi basati sulla Classe di servizio, come Tipo di servizio o DSCP. È possibile anche quantificare e visualizzare la percentuale della larghezza di banda consumata da ciascuno dei livelli QoS designati, inclusi i dati voce e video.

Assegnazione a un gruppo di applicazioni per più porte

Questa versione di Orion NTA permette di assegnare un'applicazione che utilizzi numerose porte di rete a un gruppo, per valutare le prestazioni dell'applicazione.

Disponibilità delle cinque risorse di rete più attive

Adesso sono disponibili le cinque risorse più attive a livello dell'intero rete per l'analisi del traffico, elencanti i gruppi di indirizzi IP, le applicazioni, le conversazioni, i Paesi, gli endpoint, i tipi di servizio, i trasmettitori, i ricevitori e i protocolli.

Integrazione completa delle risorse NetFlow nelle viste di Orion

Le risorse NetFlow possono essere aggiunte facilmente e automaticamente alle viste di Orion.

Funzione di ricerca immediata nel DNS

Si possono eseguire ricerche manuali nel DNS senza bisogno di attendere un aggiornamento del DNS programmato a una certa ora.

Modalità operativa di Orion NetFlow Traffic Analyzer

Le periferiche NetFlow generano una miniera di informazioni sul traffico IP. Orion NetFlow Traffic Analyzer raccoglie questi dati NetFlow, li correla in un formato utilizzabile e li presenta, insieme a dettagliati dati prestazionali sulla rete acquisiti da SolarWinds Orion Network Performance Monitor, sotto forma di grafici e rapporti di facile lettura che mostrano l'utilizzo della larghezza di banda in entrata nella rete, all'interno della stessa e in uscita. Questi rapporti facilitano il monitoraggio della larghezza di banda, la rilevazione di conversazione tra endpoint interni ed esterni, l'analisi del traffico e la pianificazione delle esigenze di capacità della larghezza di banda.

Capitolo 2

Installazione di Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) è installabile mediante una semplice procedura guidata. Per un prodotto di livello aziendale, i requisiti sono nominali.

Nota: i dati NetFlow hanno grande capacità e possono consumare grandi quantità della memoria di una database in un periodo di tempo relativamente breve, anche in reti abbastanza piccole. Quindi SolarWinds suggerisce vivamente di mantenere il database del server SQL e l'installazione di Orion NPM/NTA su server fisici separati.

Requisiti

Il server impiegato come host della soluzione NetFlow deve supportare sia Orion NPM sia Orion NTA in quanto Orion NTA è basato su Orion NPM e ne amplia le funzionalità. Le seguenti sezioni illustrano i requisiti minimi per la configurazione.

Requisiti software

I seguenti requisiti software presuppongono che la versione di valutazione di Orion NTA sia installata su un server in cui viene eseguito Orion NPM versione 9.0. Se si desidera valutare Orion NTA versione 3.0 su un'installazione di Orion NPM versione 8.5.1, contattare SolarWinds all'indirizzo sales@solarwinds.com.

Nota: SQL Express e MSDE limitano la capacità del database a 4 GB e 2 GB, rispettivamente. Per questo motivo, SolarWinds non ne supporta l'utilizzo con Orion NTA in ambienti di produzione.

Software	Requisiti
Sistema operativo	Windows Server 2003 (32 bit o 64 bit) incluso R2, con IIS installato. SolarWinds suggerisce che gli amministratori Orion NPM abbiano privilegi locali di amministratore per assicurare la completa funzionalità degli strumenti Orion NPM locali. Gli utenti limitati alla console web non hanno bisogno di privilegi di amministratore. **Nota:** SolarWinds non supporta l'installazione di Orion NTA su Windows XP in ambienti di produzione. Se si installerà Orion NTA su Windows XP, è necessario confermare che Shared Memory, Named Pipes e TCP/IP siano abilitati sui database remoti.

Software	Requisiti
Server web	Microsoft IIS versione 6.0 o successiva. Le specifiche DNS richiedono che i nomi degli host siano composti da caratteri alfanumerici (A–Z, 0–9), dal segno meno (-) e da punti (.). Il carattere di sottolineatura (_) non è consentito. Per ulteriori informazioni vedi *RFC 952*. **Nota:** SolarWinds non suggerisce né supporta l'installazione di Orion NTA sullo stesso server o l'utilizzo dello stesso server del database come un server Blackberry Research in Motion (RIM).
.NET Framework	Versione 3.5 o successiva.
Servizi Trap SNMP	Componente degli strumenti di monitoraggio e gestione del sistema operativo Windows
SQL Server	SQL Server 2000 SP4, Standard o Enterprise. SQL Server 2005 Standard o Enterprise. Il database deve supportare la modalità mista o l'autenticazione SQL. **Nota:** SQL Server Express non è in grado di gestire database di capacità superiore a 4 GB; è limitato a un solo processore e non utilizza più di 1 GB di RAM. Sebbene possa essere utilizzato per il monitoraggio di una o due interfacce a scopo di valutazione, SolarWinds ne sconsiglia l'uso per reti di grandi dimensioni che richiedono database di notevole capacità.
Browser Web Console	Microsoft Internet Explorer versione 6 o successiva con funzionalità Active Scripting. Firefox 2.0 o versione successiva.

Requisiti hardware

I seguenti requisiti hardware presuppongono che la versione di valutazione di Orion NTA sia installata su un server in cui viene eseguito Orion NPM versione 9.0. Se si desidera valutare Orion NTA versione 3.0 su un'altra versione di Orion NPM, contattare SolarWinds all'indirizzo sales@solarwinds.com.

Nota: Orion NTA richiede che la porta TCP 17777 sia aperta sia per l'invio che per la ricezione dei dati tra Orion NPM e qualunque modulo Orion, incluso Orion NTA.

Attenzione: le sole configurazioni RAID che devono essere impiegate su un'installazione Orion NTA sono 0, 1, 0+1 o 1+0. A causa della velocità elevata e della grande capacità di memoria richiesta dai trasferimenti di dati NetFlow, SolarWinds sconsiglia l'utilizzo di altre configurazioni RAID o SAN, che potrebbero causare perdite di dati e ridurre notevolmente le prestazioni.

Hardware	Requisiti
CPU	Velocità uguale o maggiore di 3 GHz
RAM	Almeno 2 GB
Spazio sul disco rigido	Almeno 5 GB. Configurazioni RAID suggerite: 0, 1, 0+1 e 1+0. Si sconsigliano altre configurazioni RAID o SAN.
Periferiche NetFlow	Le periferiche Cisco utilizzano NetFlow versione 5 o 9. **Nota:** Orion NTA riconosce solo i modelli NetFlow versione 9 che includono tutti i campi utilizzati da NetFlow versione 5.
J-Flow	Periferiche di rete che utilizzano J-Flow.
Periferiche sFlow	Periferiche sFlow che utilizzano sFlow versione 5.

Requisiti della Virtual Machine (Macchina virtuale)

Le installazioni di Orion NTA su VMware Virtual Machines e Microsoft Virtual Servers sono interamente supportate se per ciascuna macchina virtuale sono soddisfatti i seguenti requisiti minimi di configurazione.

Configurazione della macchina virtuale	Requisiti
Velocità della CPU	3,0 GHz
Spazio sul disco rigido assegnato	5 GB **Nota:** si suggerisce RAID 1+0 ; si sconsiglia RAID 5 a causa dei gravosi requisiti I/O.
Memoria	2 GB
Interfaccia di rete	Ciascuna installazione di Orion NPM deve avere la propria scheda di rete dedicata. **Nota:** poiché Orion NPM utilizza SNMP per monitorare la rete, se non è possibile impiegare una scheda di rete dedicata per l'installazione di Orion NPM si possono perdere dati di monitoraggio a causa della bassa priorità che in genere viene assegnata al traffico SNMP.

Per ulteriori informazioni sulla configurazione di Orion NPM, vedi "Requirements" nel documento *SolarWinds Orion Network Performance Monitor Administrator Guide*.

SQL Server e SQL Server Express con Orion NTA

Poiché i dati NetFlow hanno una grande capacità e consumano notevoli quantità della memoria del database in un tempo relativamente breve, SolarWinds sconsiglia l'utilizzo di istanze del database SQL Server Express per Orion NTA. SolarWinds suggerisce invece l'uso di una versione di produzione di SQL Server.

Le versioni di valutazione di Orion NTA costituiscono un'eccezione limitata. A scopo di valutazione, Orion NPM e Orion NTA possono supportare l'utilizzo di istanze del database SQL Server Express 2005. SQL Express permette di valutare Orion NTA con una database reale ed è disponibile, gratuitamente, presso Microsoft. Tuttavia, SolarWinds non ne suggerisce l'utilizzo con Orion NTA in nessun ambiente di produzione per i seguenti motivi:

- SQL Express non è in grado di gestire database di capacità superiore a 4 GB;
- SQL Express è limitato a un solo processore;
- SQL Express non è in grado di utilizzare più di 1 MB di RAM.

Nota: per ambienti di produzione, le installazioni di Orion NPM e Orion NTA devono usare un'istanza del database SQL Server installato su un server separato.

Installazione di Orion NetFlow Traffic Analyzer

Procedere come segue per installare Orion NetFlow Traffic Analyzer. Per completare l'installazione occorre specificare la porta impiegata per il traffico NetFlow e confermare che è abilitata e sta inviando i dati NetFlow.

Nota: la seguente procedura presuppone che sia stato già installato Orion Network Performance Monitor versione 9.0 sul server su cui si desidera installare Orion NetFlow Traffic Analyzer. Se si desidera valutare Orion Network Performance Monitor versione 9.0, contattare SolarWinds all'indirizzo sales@solarwinds.com.

Per installare Orion NetFlow Traffic Analyzer:

1. Accedere al server Orion Network Performance Monitor che si desidera utilizzare per l'analisi del traffico NetFlow.
2. ***Se si sta installando NetFlow Traffic Analyzer su un server terminale,*** procedere come segue prima di continuare l'installazione, per accertarsi che NetFlow Traffic Analyzer è installato correttamente:
   a. Fare clic su **Start > Control Panel > Add or Remove Programs** (Avvio > Pannello di controllo > Installazione applicazioni).
   b. Fare clic su **Add New Programs** (Aggiungi nuovi programmi).
   c. Fare clic su **CD-ROM o Floppy**, quindi fare clic su **Next** (Avanti) nella finestra Install Program From Floppy Disk or CD-ROM (Installazione del programma da floppy o da CD-ROM).

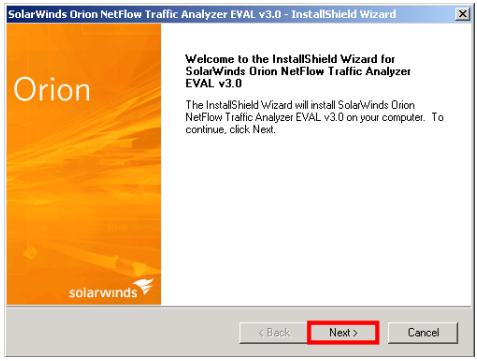
3. ***Se si è scaricato il prodotto dal sito web SolarWinds,*** procedere come segue:

   a. Andare alla directory in cui si è salvato il file `.zip` scaricato e quindi estrarre il pacchetto della versione di valutazione in una directory appropriata.

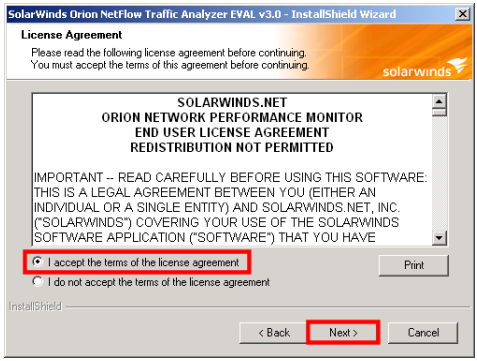
   b. Avviare l'eseguibile della versione di valutazione SolarWinds Orion NTA.

4. ***Se si sono ricevuti supporti fisici,*** andare alla directory in cui risiede l'eseguibile della versione di valutazione SolarWinds Orion NTA e avviarlo.

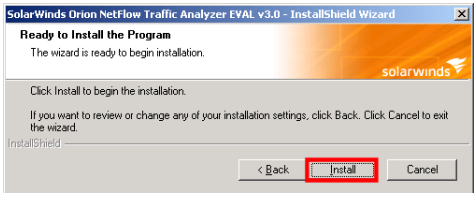
5. Sulla schermata iniziale, fare clic su **Next** (Avanti).



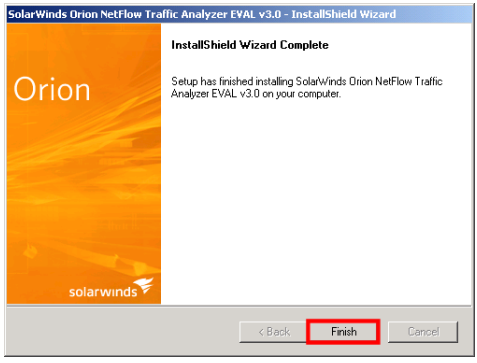
6. Selezionare **I accept the terms of the license agreement** (Accetto i termini del Contratto di Licenza Microsoft), quindi fare clic su **Next** (Avanti).



7. Fare clic su **Install** (Installa) sulla finestra Ready to Install the Program (Installazione del programma).

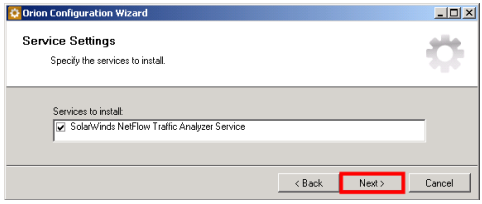


8. Una volta completata InstallShield Wizard (Procedura guidata InstallShield), fare clic su **Finish** (Fine) per terminare la procedura.

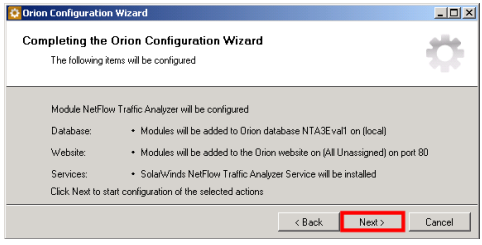


9. ***Se viene richiesto di riavviare il server,*** selezionare tra le seguenti opzioni, come appropriato:
   - ***Se si sta installando Orion NTA su un server terminale,*** fare clic su **No**.
   - ***Se NON si sta installando Orion NTA su un server terminale,*** fare clic su **Yes** (Sì).
10. ***Se Configuration Wizard non si avvia automaticamente,*** fare clic su **Start > All Programs > SolarWinds Orion > Configuration Wizard** (Avvio > Tutti i programmi > SolarWinds Orion > Procedura di configurazione guidata).
11. Sulla schermata iniziale, fare clic su **Next** (Avanti).

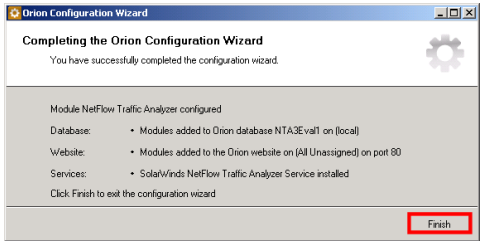
12. Verificare che **SolarWinds NetFlow Traffic Analyzer Service** (Servizio SolarWinds NetFlow Traffic Analyzer) sia selezionato nella finestra Service Settings (Impostazioni servizio), quindi fare clic su **Next** (Avanti).



13. Esaminare il sommario della configurazione, quindi fare clic su **Next** (Avanti).



14. Una volta completata Configuration Wizard (Procedura di configurazione guidata), fare clic su **Finish** (Fine).



Abilitazione dell'analisi del traffico NetFlow

Per iniziare ad analizzare i dati NetFlow disponibili generati da periferiche della rete, occorre aggiungere un'interfaccia NetFlow al database Orion oppure monitorare un'interfaccia aggiunta in precedenza che sia in grado di generare dati NetFlow. Affinché sua possibile monitorare periferiche NetFlow in Orion NTA, occorre aggiungerle al database Orion.

Nota: l'aggiunta di interfacce e periferiche NetFlow al database Orion e a Orion NTA come sorgenti NetFlow sono procedure separate, descritte dettagliatamente in sezioni separate, come segue.

Aggiunta di periferiche e interfacce al database Orion

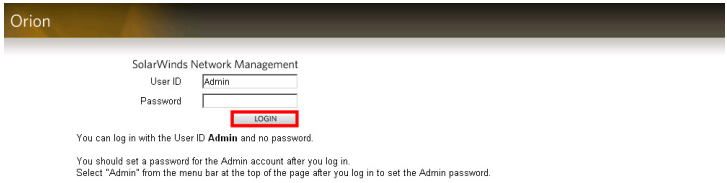
La seguente procedura mostra come aggiungere una periferica e le sue interfacce al database Orion mediante la funzionalità Web Node Management (Gestione nodi web) della Orion Web Console. Se la periferica NetFlow è già configurata per l'invio di dati NetFlow, Orion NTA inizia a ricevere dati NetFlow non appena si aggiunge la periferica al database Orion.

Nota: per ulteriori informazioni sulla designazione di sorgenti NetFlow in Orion NTA, vedi "Aggiunta di sorgenti NetFlow a NetFlow Traffic Analyzer" a pagina 18.

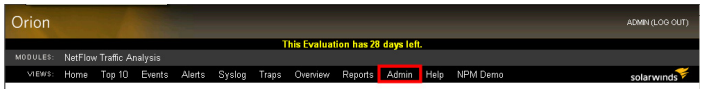
Per aggiungere periferiche e interfacce NetFlow al database Orion:

1. Accedere al server Orion NPM su cui si è istallato Orion NTA.
2. Fare clic su **Start > SolarWinds Orion > Orion Web Console** (Avvio > SolarWinds Orion > Console web Orion).
3. Accedere a Orion Web Console eseguendo il login come amministratore.

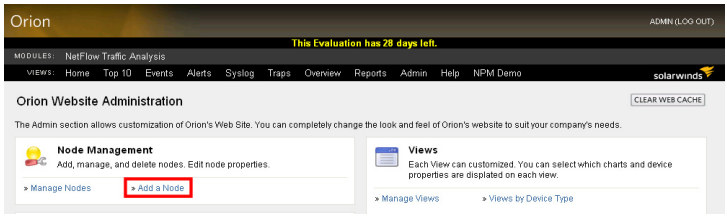
   Nota: se non si è già configurata un'altra password di amministratore, si può eseguire il login utilizzando `Admin` per **User ID** (ID utente) e nessuna password.



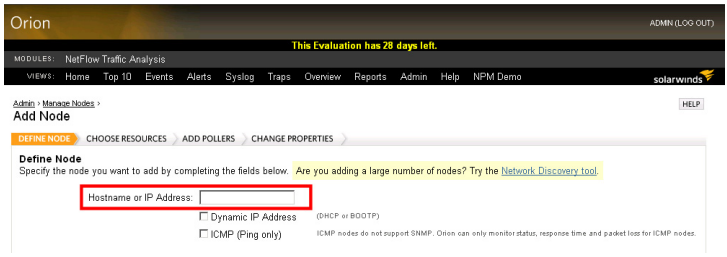
4. Fare clic su **Admin** (Ammin.) nella barra strumenti Views (Viste).



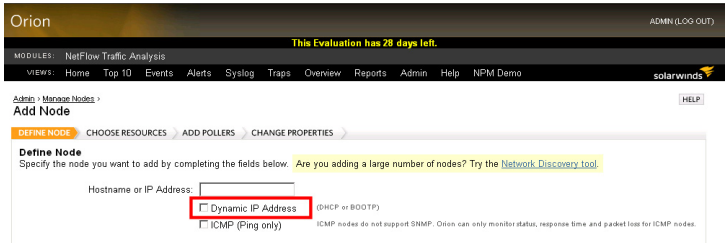
5. Fare clic su **Add a Node** (Aggiungi nodo) sul riquadro Node Management (Gestione nodi).



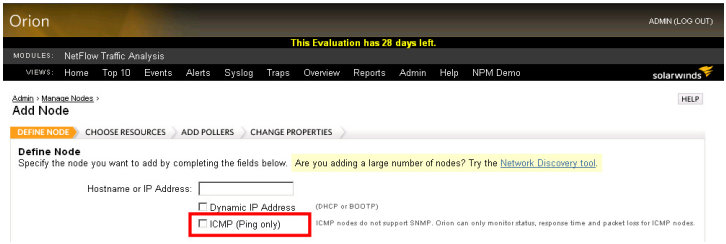
6. Immettere nel campo **Hostname or IP Address** (Nome host o indirizzo IP) il nome host o l'indirizzo IP della periferica che si desidera aggiungere.



7. ***Se l'indirizzo IP della periferica che si sta aggiungendo viene assegnato dinamicamente (DHCP o BOOTP),*** selezionare **Dynamic IP Address** (Indirizzo IP dinamico).

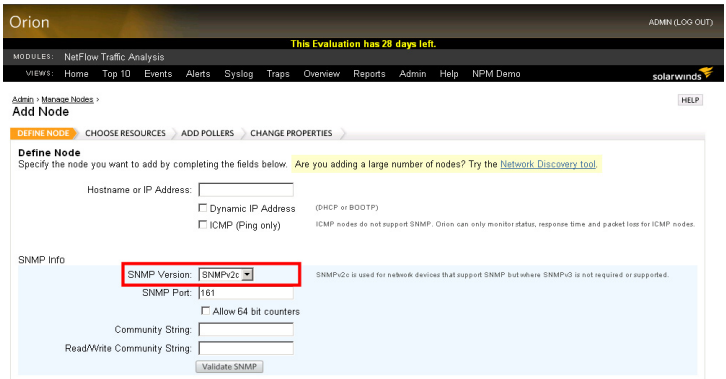


8. Verificare che l'opzione **ICMP** (**Ping only**) [ICMP (solo ping)] non sia selezionata.



9. Selezionare **SNMP Version** (Versione SNMP) per il nodo aggiunto.

   Nota: Orion NPM utilizza **SNMPv2c** come impostazione predefinita. Se la nuova periferica supporta o richiede le funzionalità di sicurezza avanzate di SNMPv3, selezionare **SNMPv3**.



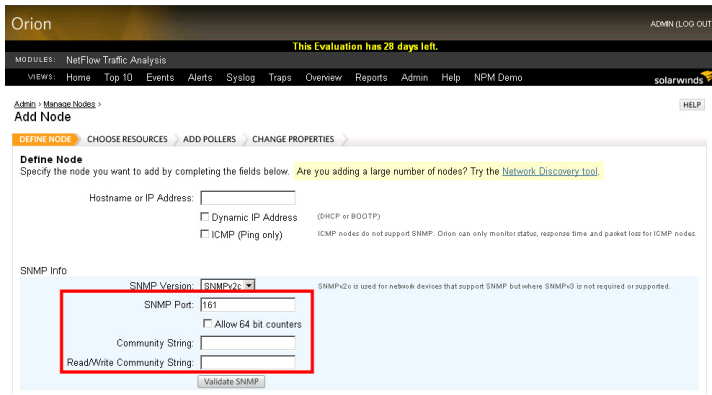
10. ***Se si è selezionato*** **SNMPv2c,** procedere come segue:

    a. ***Se la porta SNMP sul nodo aggiunto non è quella predefinita di Orion NPM, ossia 161,*** immettere il numero della porta effettiva nel campo **SNMP Port** (Porta SNMP).

    b. ***Se il nodo aggiunto supporta contatori a 64 bit e si desidera utilizzarli,*** selezionare **Allow 64 bit counters** (Autorizza contatori a 64 bit).

    c. Immettere stringhe di comunità valide per il nodo aggiunto.

       Nota: Read/Write Community String (Stringa di comunità di lettura/scrittura) è opzionale, ma Orion NPM richiede almeno `public` per **Community String** (Stringa di comunità).



11. ***Se si è selezionato* SNMPv3,** procedere come segue:

    a. ***Se la porta SNMP sul nodo aggiunto non è quella predefinita di Orion NPM, ossia 161,*** immettere il numero della porta effettiva nel campo **SNMP Port** (Porta SNMP).

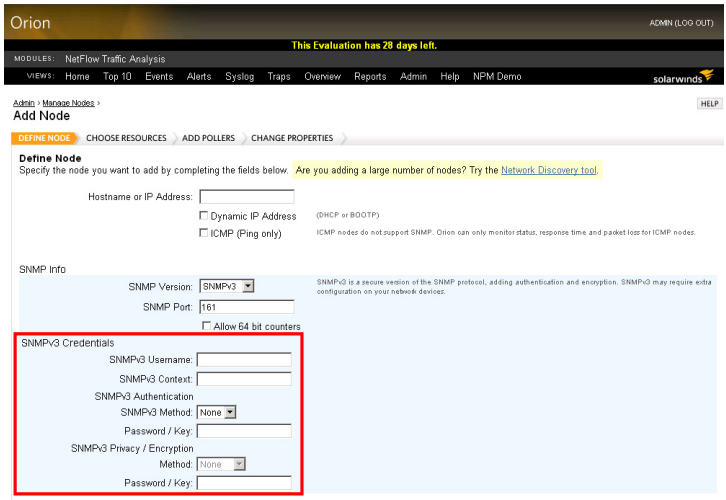
    b. ***Se il nodo aggiunto supporta contatori a 64 bit e si desidera utilizzarli,*** selezionare **Allow 64 bit counters** (Autorizza contatori a 64 bit).

       Nota: Orion NPM supporta completamente l'utilizzo di contatori a 64 bit; tuttavia questi contatori di grande capacità possono funzionare in modo irregolare, a seconda dell'implementazione attuata dal produttore. Se si osservano risultati strani quando si adoperano questi contatori, utilizzare la vista Node Details (Dettagli nodo) per disattivare l'uso dei contatori a 64 bit per la periferica e rivolgersi al produttore dell'hardware.

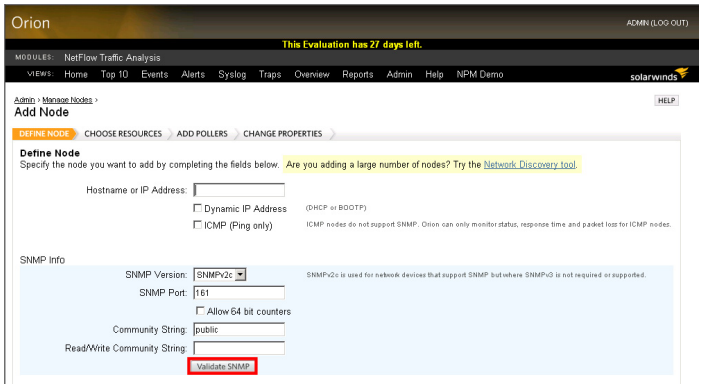
    c. Immettere le seguenti impostazioni **SNMP Credentials** (Credenziali SNMP)**, Authentication** (Autenticazione) e **Privacy/Encryption** (Privacy/Criptazione):

       - **SNMPv3 Username** (Nome utente SNMPv3)
       - **SNMPv3 Context** (Contesto SNMPv3)
       - **SNMPv3 Authentication Method** (Metodo di autenticazione SNMPv3)
       - **SNMPv3 Authentication Password/Key** (Chiave/password di autenticazione SNMPv3)
       - **SNMPv3 Privacy/Encryption Method** (Metodo di criptazione/privacy SNMPv3)
       - **SNMPv3 Privacy/Encryption Method** (Chiave/password di criptazione/privacy SNMPv3)

Nota: ai fini di questa valutazione, non sono necessarie le impostazioni **Read/Write SNMPv3 Credentials** (Credenziali SNMPv3 di lettura/scrittura).



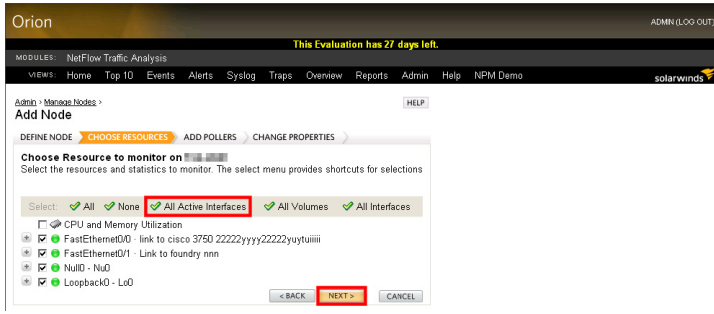
12. Fare clic su **Validate SNMP** (Valida SNMP) una volta immesse tutte le credenziali SNMP necessarie.



13. Una volta confermata la validità delle credenziali SNMP, fare clic su **Next** (Avanti).

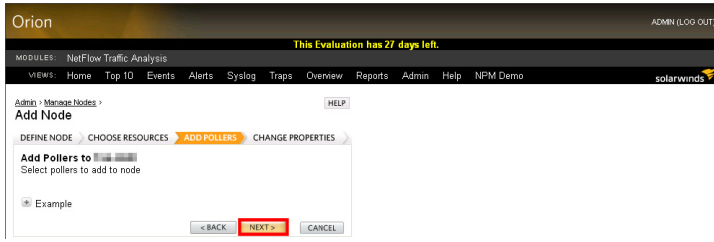
14. Selezionare le periferiche che si desidera monitorare con Orion NTA, quindi fare clic su **Next** (Avanti).

Nota: se non si sa quali sono le intrfacce NetFlow, fare clic su **All Interfaces** (Tutte le interfacce) per selezionarle tutte.

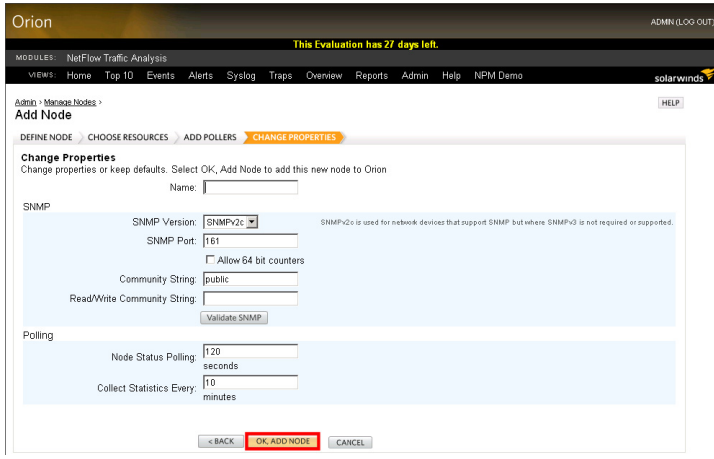


15. Ai fini di questa valutazione, fare clic su **Next** (Avanti) nella vista Add Pollers (Aggiungi polling).

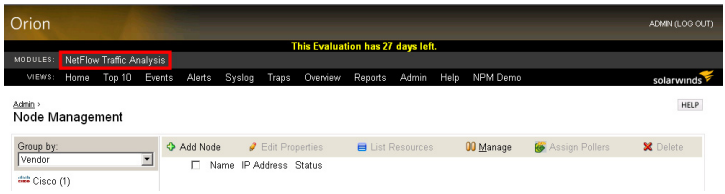
Nota: per ulteriori informazioni sull'utilizzo o sulla definizione del polling, consultare il documento *SolarWinds Orion Network Performance Monitor Administrator Guide*.



16. Fare clic su **OK, Add Node** (OK, Aggiungi nodo) sulla vista Change Properties (Modifica proprietà).



17. Fare clic su **NetFlow Traffic Analysis** (Analisi del traffico NetFlow) nella barra strumenti Modules (Moduli).



La seguente sezione illustra come iniziare a ricevere dati NetFlow dalle periferiche NetFlow della rete.

Aggiunta di sorgenti NetFlow a NetFlow Traffic Analyzer

Una volta aggiunte le periferiche NetFlow e le interfacce corrispondenti a Orion NPM, occorre designare ciascuna periferica come sorgente NetFlow. La seguente procedura mostra come aggiungere sorgenti NetFlow a Orion NTA.

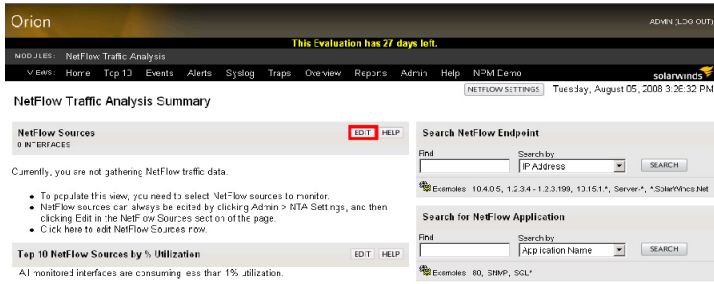
Nota: Orion NTA riconosce solo i modelli NetFlow versione 9 che includono tutti i campi utilizzati da NetFlow versione 5.

Per aggiungere periferiche e interfacce NetFlow a NetFlow Traffic Analyzer:

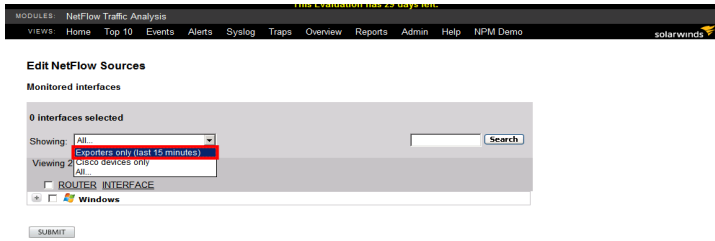
1. Accedere al server Orion NPM su cui si è istallato Orion NetFlow Traffic Analyzer.
2. Fare clic su **Start > All Programs > SolarWinds Orion > Orion Web Console** (Avvio > Tutti i programmi > SolarWinds Orion > Console web Orion).
3. Accedere a Orion Web Console eseguendo il login come amministratore.

   Nota: se non si è già configurata un'altra password di amministratore, si può eseguire il login utilizzando `Admin` per **User ID** (ID utente) e nessuna password.

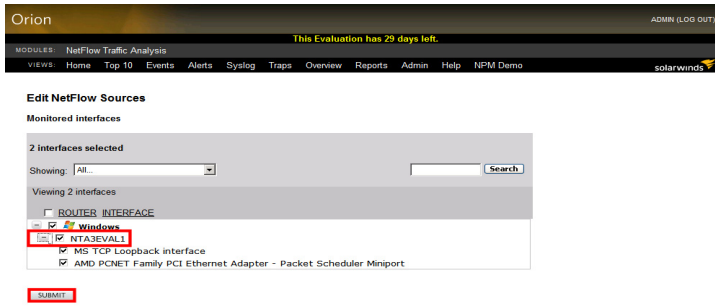
4. Fare clic su **Edit** (Modifica) nell'intestazione della risorsa NetFlow Sources (Sorgenti NetFlow).



5. Selezionare **Exporters Only** (**last 15 minutes**) [Solo periferiche di esportazione (ultimi 15 minuti)] dal menu Showing (Visualizzazione).



6. Espandere l'elenco delle periferiche per visualizzare tutti i nodi monitorati, controllare i nodi di livello superiore (nodi "padre") delle interfacce che si desidera vengano monitorate da Orion NTA, quindi fare clic su **Submit** (Invia).



In base a queste impostazioni, dopo alcuni minuti Orion NTA riceverà dati significativi sul traffico e li visualizzerà su Orion Web Console.

Capitolo 3

Orion NetFlow Traffic Analyzer – Panoramica

Le funzionalità e la flessibilità offerte da Orion NetFlow Traffic Analyzer permettono di analizzare con elevata accuratezza la quantità e la qualità del traffico della rete. le sezioni di questo capitolo sono strutturate in modo sequenziale, per illustrare come utilizzare le caratteristiche chiave di Orion NetFlow Traffic Analyzer. Questo capitolo è particolarmente utile se letto dall'inizio alla fine; inizia con una descrizione generale delle risorse immediatamente disponibili sulla vista NetFlow Traffic Analysis Summary (Sommario dell'analisi del traffico NetFlow), e continua descrivendo le viste di Orion NTA utilizzate più spesso.

Nota: nel capitolo finale della presente Evaluation Guide sono presentati vari casi di utilizzo, inclusi scenari che incorporano altri strumenti SolarWinds. Per ulteriori informazioni, vedi "Utilizzo di Orion NetFlow Traffic Analyzer" a pagina 41.

Avvio di Orion NetFlow Traffic Analyzer

Fare clic su **Start > All Programs > SolarWinds Orion > Orion Web Console** (Avvio > Tutti i programmi > SolarWinds Orion > Console web Orion). Per ulteriori informazioni sull'installazione e sulla configurazione di Orion NTA, vedi "Installazione di Orion NetFlow Traffic Analyzer" a pagina 5.

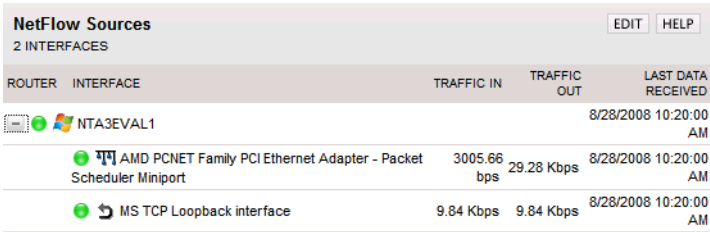
Sommario dell'analisi del traffico NetFlow

Quando si avvia Orion NetFlow Traffic Analyzer, NetFlow Traffic Analysis Summary (Sommario dell'analisi del traffico NetFlow) è la prima vista visualizzata e mostra le condizioni del traffico sull'intera rete. Le seguenti risorse sono incluse nella vista NetFlow Traffic Analysis Summary View per impostazione predefinita.

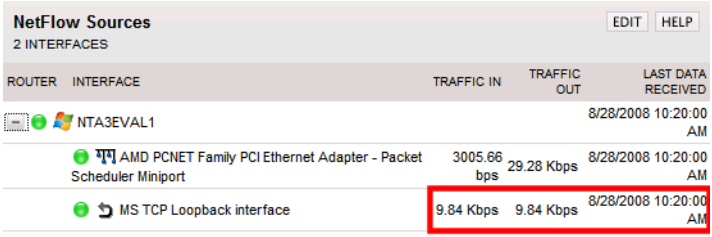
NetFlow Sources (Sorgenti NetFlow)

Questa risorsa fornisce un elenco di tutte le periferiche NetFlow della rete attualmente configurate in modo da inviare dati NetFlow al server su cui è installato Orion NTA. Per ulteriori informazioni sulla vista NetFlow Endpoint, vedi "Abilitazione dell'analisi del traffico NetFlow" a pagina 12.

Fare clic su **+** accanto al nome di un router qualsiasi per visualizzare le interfacce NetFlow sul router selezionato.



Le interfacce sono contrassegnate da un'icona dello stato e una marcatura temporale che indica quando Orion NTA ha ricevuto per l'ultima volta i dati NetFlow dall'interfaccia selezionata. Inoltre, la risorsa NetFlow Sources presenta i valori rilevati sia per il traffico in entrata che per quello in uscita su ciascuna interfaccia.

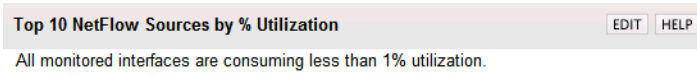


Facendo clic sul nome di un router si apre la vista NetFlow Node Details (Dettagli nodo NetFlow), e facendo clic sul nome di un'interfaccia si apre la vista NetFlow Interface Details (Dettagli interfaccia NetFlow). Per ulteriori informazioni sulla vista NetFlow Node Details vedi "Vista NetFlow Node Details" a pagina 37. Per ulteriori informazioni sulla vista NetFlow Interface Details vedi "Vista NetFlow Interface Details" a pagina 36.

Top 10 NetFlow Sources by % Utilization (Elenco delle 10 sorgenti NetFlow più attive in base all'utilizzo percentuale)

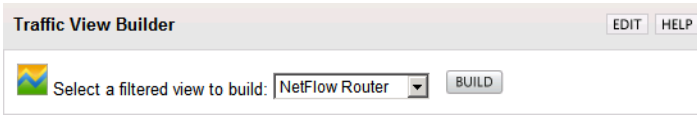
Questa risorsa presenta un elenco delle risorse NetFlow sulla rete che attualmente instradano un volume di traffico che le impegna notevolmente.

Nota: nell'elenco figurano solo le risorse con utilizzo superiore a 1%.



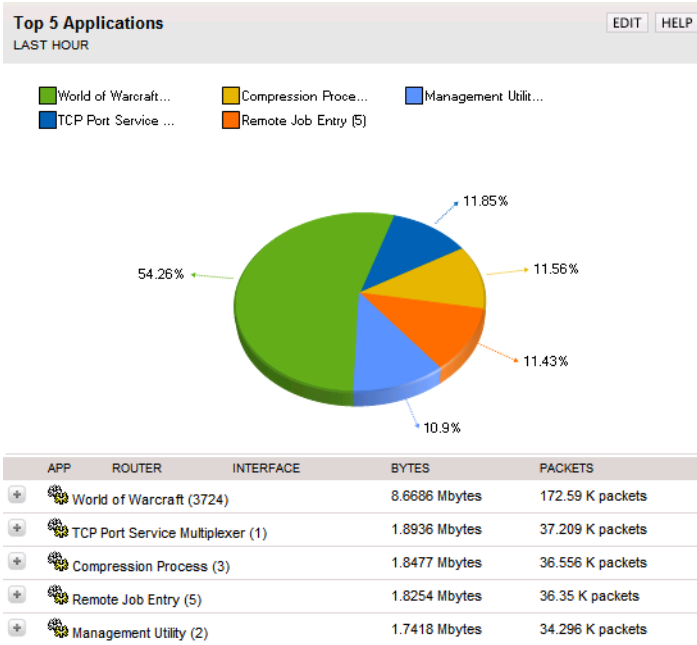
Traffic View Builder

L'applicazione Traffic View Builder permette di creare viste Orion NTA personalizzate. Poiché Orion NTA è un modulo basato su web, si possono creare segnalibri nel browser per qualsiasi vista Orion NTA per controllare agevolmente in un secondo tempo lo stato di potenziali punti problematici. Per ulteriori informazioni su Traffic View Builder, vedi "Utilizzo di Traffic View Builder" a pagina 41.



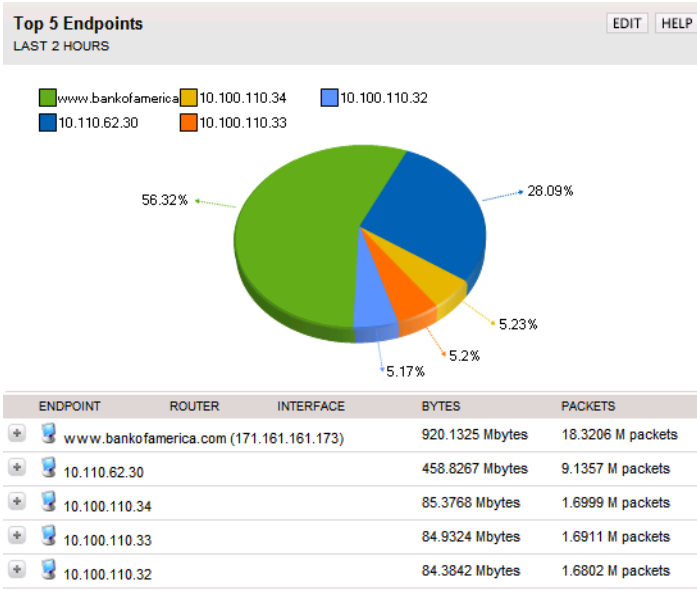
Top 5 Applications (Le cinque risorse più attive)

La risorsa Top 5 Applications permette di esaminare a colpo d'occhio le applicazioni e le porte maggiormente utilizzate dalle periferiche della rete. Facendo clic **+** si può espandere ciascuna applicazione per vederne il traffico instradato dalle periferiche della rete.



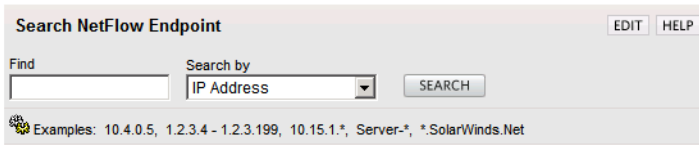
Top 5 Endpoints (I cinque endpoint più attivi)

La risorsa Top 5 Endpoints permette di esaminare a colpo d'occhio gli endpoint da cui si genera o a cui arriva la maggior parte del traffico della rete. Facendo clic **+** si può espandere ciascun endpoint per vedere le periferiche della rete che instradano il traffico per ciascun endpoint.



Search for NetFlow Endpoints (Ricerca di endpoint NetFlow)

Mediante questa risorsa è possibile individuare velocemente qualsiasi endpoint che comunichi con qualsiasi periferica della rete.

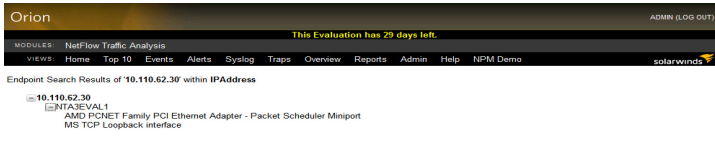


È sufficiente cercare endpoint secondo uno qualsiasi dei criteri riportati nella seguente tabella:

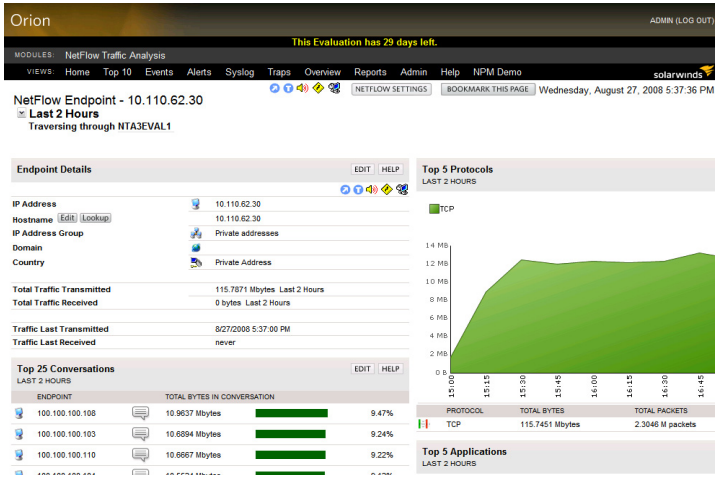
Criteri di ricerca degli endpoint NetFlow		
Paese	Dominio	Nome host

Criteri di ricerca degli endpoint NetFlow		
Indirizzo IP	Nome gruppo indirizzo IP	

Digitare un termine di ricerca appropriato, quindi fare clic su **Search** (Cerca). I risultati della ricerca si presentano sotto forma di un elenco espandibile delle periferiche della rete che stanno instradando traffico in entrata o in uscita dall'endpoint cercato.

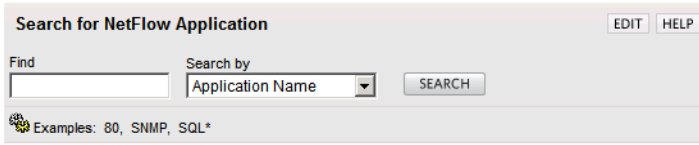


Facendo clic sul nome delle periferiche della rete si apre la vista NetFlow Endpoint relativa al traffico di tutti gli endpoint attraverso la periferica selezionata. Per ulteriori informazioni sulla vista NetFlow Endpoint, vedi "Vista NetFlow Endpoint" a pagina 33.

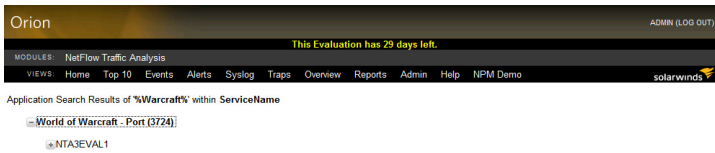


Search for NetFlow Application (Ricerca di applicazioni NetFlow)

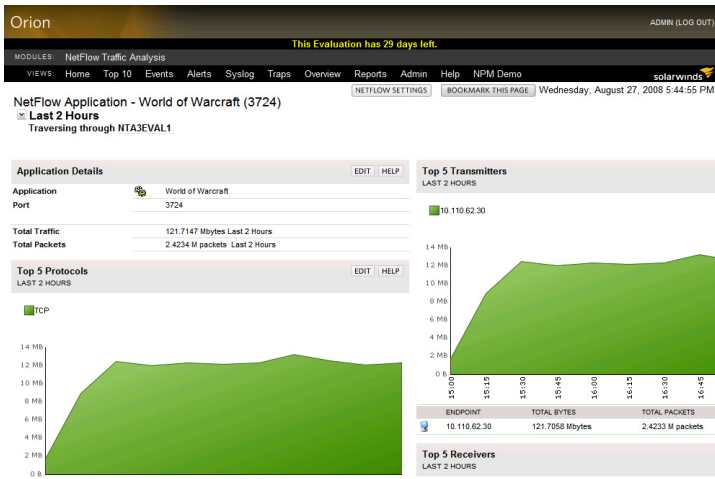
Tramite la risorsa Search for NetFlow Application è possibile vedere rapidamente, in qualsiasi momento, quali periferiche della rete stanno usando una certa applicazione o porta. Selezionare il criterio di ricerca, Application Name o Port, digitare un appropriato nome di applicazione o numero di porta, quindi fare clic su **Search** (Cerca).



I risultati della ricerca si presentano sotto forma di un elenco espandibile delle periferiche della rete che stanno instradando per l'applicazione o attraverso la porta selezionata.

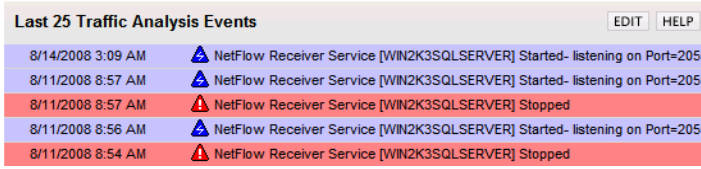


Facendo clic sul nome di una periferica della rete si apre la vista NetFlow Application (Applicazione NetFlow) per tutto il traffico attraverso la periferica selezionata instradato per l'applicazione o attraverso la porta cercata. Per ulteriori informazioni sulla vista NetFlow Application, vedi "Vista NetFlow Application" a pagina 30.



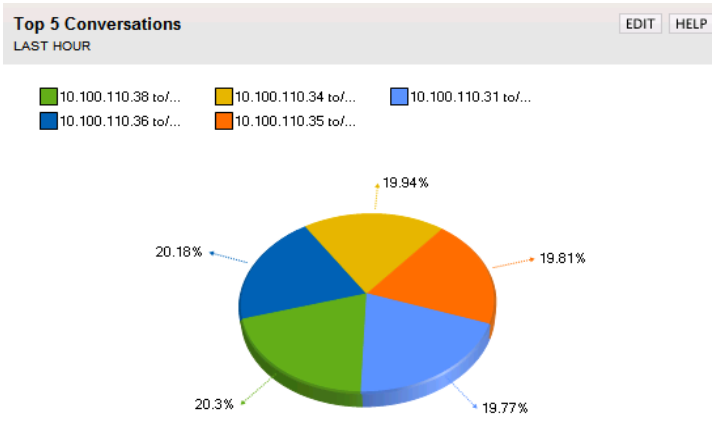
Last 25 Traffic Analysis Events (Ultimi 25 eventi di analisi del traffico)

Questa risorsa elenca gli ultimi 25 eventi NetFlow che hanno avuto luogo sulle periferiche della rete monitorata. Normalmente questa risorsa elenca data e ora degli avvii e arresti di NetFlow Receiver Service.



Top 5 Conversations (Le cinque conversazioni più attive)

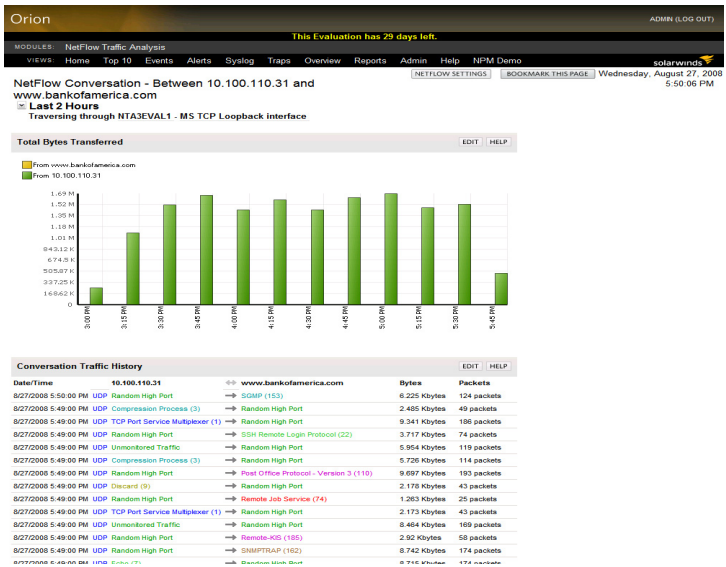
Questa risorsa permette di esaminare a colpo d'occhio, tramite un diagramma e una tabella, le conversazioni che utilizzano la maggior parte della larghezza di banda della rete. Ciascun colore del diagramma corrisponde a una singola conversazione ininterrotta tra due endpoint specifici. La tabella sotto il diagramma elenca gli endpoint relativi a ciascuna conversazione, con la larghezza di banda consumata sia in termini di byte che di pacchetti. Fare clic su **+** per espandere la descrizione della conversazione allo scopo di vedere tutte le periferiche della rete attraverso le quali viene condotta la conversazione stessa. Il primo livello di espansione mostra i nodi della rete attraverso cui viene instradato il traffico della conversazione. Il livello successivo di espansione mostra le interfacce che stanno trasferendo traffico per la conversazione selezionata.



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

Sia a livello di nodo che a livello di interfaccia, sono elencate le rispettive parti della larghezza di banda totale consumata dalla conversazione selezionata, sia in byte che in pacchetti. Per un nodo qualsiasi, il traffico della conversazione su di esso è uguale alla somma del traffico della conversazione su tutte le interfacce con tale nodo.

Facendo clic sul nome di una qualsiasi periferica della rete si apre la vista NetFlow Conversation relativa a tutto il traffico esistente tra i due endpoint che conversano attraverso la periferica selezionata. Per ulteriori informazioni, vedi “Vista NetFlow Conversation” a pagina 33.



Orion NetFlow Traffic Analyzer – Viste

Le seguenti sezioni descrivono in dettaglio i tipi di informazioni disponibili per impostazione predefinita su viste Orion NTA selezionate.

Note:

- Le seguenti sono alcune delle viste Orion NTA più utilizzate. Sono accessibili attraverso link diretti dalle risorse predefinite sulla vista NetFlow Traffic Analysis Summary. Da altre risorse si raggiungono ulteriori viste. Per ulteriori informazioni, vedi “Viewing NetFlow Traffic Analyzer Data in the Orion Web Console” nel documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.
- Alcune risorse possono non essere presenti nella configurazione predefinita di una vista selezionata. Per visualizzare tutte le risorse disponibile occorre modificare la vista dalla vista Admin della console web Orion NPM. Per ulteriori informazioni, vedi “Viewing NetFlow Traffic Analyzer Data in the Orion Web Console” nel documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Vista NetFlow Application

Le seguenti sezioni descrivono brevemente le risorse disponibili sulla vista NetFlow Application predefinita. Per ulteriori informazioni su ciascuna risorsa, inclusi i dettagli della configurazione, fare clic su **Help** (Guida) nella barra del titolo della risorsa.

Application Details (Dettagli applicazione)

La risorsa Application Details fornisce una tabella contenente le seguenti informazioni sull'applicazione e sulla porta attualmente visualizzate:

- Nome dell'applicazione
- Porta utilizzata dall'applicazione
- Quantità totale dei dati del traffico nel periodo di tempo selezionato
- Numero totale di pacchetti inviati nel periodo di tempo selezionato

Top 5 Protocols (Le cinque protocolli più attivi)

La risorsa Top 5 Protocols permette di esaminare a colpo d'occhio i protocolli utilizzati in misura maggiore dall'applicazione selezionata. La tabella seguente mostra il tipo di protocollo, la quantità di dati, il numero totale di pacchetti e la percentuale del traffico totale che utilizza ciascun protocollo elencato.

Top 5 Types of Service (I cinque tipi di servizio più attivi)

La risorsa Top 5 Types of Service permette di esaminare a colpo d'occhio, tramite un diagramma, i servizi più attivi utilizzati dall'applicazione selezionata. La tabella sotto il diagramma riporta le seguenti informazioni per ciascun tipo di servizio:

- Il tipo di servizio
- Il volume del traffico gestito dal servizio
- Il numero di pacchetti gestiti dal servizio
- La percentuale di tutto il traffico relativo all'applicazione selezionata che viene gestito dal tipo di servizio selezionato

Total Bytes Transferred (Totale byte trasferiti)

La risorsa Total Bytes Transferred visualizza un diagramma che mostra il numero totale di byte trasferiti dall'applicazione selezionata durante un intervallo specificato. È disponibile un'ampia gamma di diagrammi personalizzati che possono essere stampati o esportati ai fini della documentazione. Facendo clic sul diagramma si apre la pagine Customize Chart (Personalizza diagramma) relativa al diagramma selezionato. Per ulteriori informazioni sulla

personalizzazione dei diagrammi, vedi “Customizing Charts in NetFlow Traffic Analyzer” nel documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Unique Visitors (Visitatori unici)

La risorsa Unique Visitors visualizza un diagramma che mostra il numero di indirizzi IP unici che hanno utilizzato l’applicazione selezionata durante un intervallo specificato. È disponibile un’ampia gamma di diagrammi personalizzati che possono essere stampati o esportati ai fini della documentazione. Facendo clic sul diagramma si apre la pagine Customize Chart (Personalizza diagramma) relativa al diagramma selezionato. Per ulteriori informazioni sulla personalizzazione dei diagrammi, vedi “Customizing Charts in NetFlow Traffic Analyzer” nel documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Total Packets Transferred (Totale pacchetti trasferiti)

La risorsa Total Packets Transferred visualizza un diagramma che mostra il numero totale di pacchetti trasferiti dall’applicazione selezionata durante un intervallo specificato. È disponibile un’ampia gamma di diagrammi personalizzati che possono essere stampati o esportati ai fini della documentazione. Facendo clic sul diagramma si apre la pagine Customize Chart (Personalizza diagramma) relativa al diagramma selezionato. Per ulteriori informazioni sulla personalizzazione dei diagrammi, vedi “Customizing Charts in NetFlow Traffic Analyzer” nel documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Top 5 Transmitters (I cinque trasmettitori più attivi)

La risorsa Top 5 Transmitters permette di esaminare a colpo d’occhio, tramite un diagramma, gli endpoint di trasmissione più attivi utilizzati dall'applicazione selezionata. La tabella sotto il diagramma riporta le seguenti informazioni per ciascun endpoint:

- Il nome o l’indirizzo IP dell’endpoint
- Il volume del traffico trasmesso dall’endpoint
- La percentuale di tutto il traffico trasmesso che può essere fatto risalire all’endpoint

Si può fare clic su ciascun endpoint elencato per aprire la vista NetFlow Endpoint, che presenta statistiche analoghe per ciascun endpoint trasmittente. Per ulteriori informazioni, vedi “Vista NetFlow Endpoint” a pagina 33.

Top 5 Receivers (I cinque ricevitori più attivi)

La risorsa Top 5 Receivers permette di esaminare, tramite un diagramma, gli endpoint di ricezione più attivi utilizzati dall'applicazione selezionata. La tabella sotto il diagramma riporta le seguenti informazioni per ciascun endpoint:

- Il nome o l'indirizzo IP dell'endpoint
- Il volume del traffico ricevuto dall'endpoint
- La percentuale di tutto il traffico ricevuto che può essere fatto risalire all'endpoint

Si può fare clic su ciascun endpoint elencato per aprire la vista NetFlow Endpoint, che presenta statistiche analoghe per ciascun endpoint trasmittente. Per ulteriori informazioni, vedi "Vista NetFlow Endpoint" a pagina 33.

Top 5 Traffic Sources by Country (I cinque sorgenti di traffico più attive secondo il Paese)

La risorsa Top 5 Traffic Sources by Country permette di esaminare a colpo d'occhio, tramite un diagramma, i Paesi da cui ha origine il traffico sull'applicazione selezionata, classificati secondo la percentuale del traffico totale sull'applicazione stessa. La tabella sotto il diagramma riporta le seguenti informazioni per ciascun Paese:

- Il nome del Paese
- Il volume del traffico che ha origine dal Paese
- La percentuale di tutto il traffico che può essere fatto risalire al Paese

Top 5 Traffic Destinations by Country (Le cinque destinazioni del traffico più attive secondo il Paese)

La risorsa Top 5 Traffic Destinations by Country permette di esaminare a colpo d'occhio, tramite un diagramma, i Paesi di destinazione del traffico sull'applicazione selezionata, classificati secondo la percentuale del traffico totale sull'applicazione stessa. La tabella sotto il diagramma riporta le seguenti informazioni per ciascun Paese:

- Il nome del Paese
- Il volume del traffico che viene instradato verso gli endpoint del Paese
- La percentuale di tutto il traffico dell'applicazione che può essere fatto risalire agli endpoint del Paese

Top 5 Conversations (Le cinque conversazioni più attive)

La risorsa Top 5 Conversations fornisce un elenco delle conversazioni che consumano la maggior parte della larghezza di banda e instradate attraverso la periferica selezionata mediante l'applicazione selezionata. Le conversazioni sono elencate con la quantità di dati trasferiti nella conversazione, sia in termini di byte che di pacchetti, e la percentuale del traffico totale dell'applicazione generato dalla conversazione. Facendo clic su una conversazione se ne apre la vista NetFlow Conversation. Per ulteriori informazioni, vedi "Vista NetFlow Conversation" a pagina 33.

Vista NetFlow Conversation

Le seguenti sezioni descrivono brevemente le risorse disponibili sulla vista NetFlow Conversation predefinita. Per ulteriori informazioni su ciascuna risorsa, inclusi i dettagli della configurazione, fare clic su **Help** (Guida) nella barra del titolo della risorsa.

Total Bytes Transferred (Totale byte trasferiti)

La risorsa Total Bytes Transferred visualizza un diagramma che mostra il numero totale di byte trasferiti, durante un certo intervallo, tra i due nodi, indirizzi IP o domini indicati nel titolo della vista.

Conversation Traffic History (Cronologia del traffico della conversazione)

La risorsa Conversation Traffic History fornisce una tabella che visualizza le seguenti informazioni per ciascuno scambio di dati elencato:

- Data/marcatura temporale del trasferimento di dati
- Protocollo utilizzato per il trasferimento dei dati
- L'applicazione e la porta utilizzati per il trasferimento dei dati
- La direzione del flusso dei dati
- La quantità di dati trasmessa in byte
- Il numero equivalente di pacchetti trasferiti

Vista NetFlow Endpoint

Le seguenti sezioni descrivono brevemente le risorse disponibili sulla vista NetFlow Endpoint predefinita. Per ulteriori informazioni su ciascuna risorsa, inclusi i dettagli della configurazione, fare clic su **Help** (Guida) nella barra del titolo della risorsa.

Endpoint Details (Dettagli sull'endpoint)

La risorsa Endpoint Details fornisce le seguenti informazioni su un endpoint selezionato:

- Indirizzo IP
- Nome host
- Gruppo dell'indirizzo IP
- Dominio
- Paese
- Traffico totale trasmesso e ricevuto
- Marcature temporali (data-ora) dei dati trasmessi e ricevuti per ultimi

Top 5 Conversations (Le cinque conversazioni più attive)

Questa risorsa fornisce un elenco degli endpoint con i quali l'endpoint attualmente visualizzato ha trasferito la maggior parte dei dati Per ciascuna conversazione, questa risorsa fornisce la quantità di dati trasferiti e la percentuale della conversazione elencata rappresenta la quantità totale di dati trasferiti dall'endpoint visualizzato. Facendo clic su un endpoint se ne apre la vista NetFlow Endpoint. Tutti gli altri link relativi a un endpoint elencato aprono la vista NetFlow Conversation relativa al trasferimento di dati tra gli endpoint visualizzati e quelli selezionati. Per ulteriori informazioni, vedi "Vista NetFlow Conversation" a pagina 33.

Total Packets Transferred (Totale pacchetti trasferiti)

La risorsa Total Packets Transferred visualizza un diagramma che mostra il numero totale di pacchetti trasmessi e ricevuti dall'endpoint visualizzato durante un intervallo specificato.

Total Bytes Transferred (Totale byte trasferiti)

La risorsa Total Bytes Transferred visualizza un diagramma che mostra il numero totale di byte trasmessi e ricevuti dall'endpoint visualizzato durante un intervallo specificato.

Top 5 Protocols (I cinque protocolli più attivi)

La risorsa Top 5 Protocols permette di esaminare a colpo d'occhio i protocolli utilizzati in misura maggiore dall'endpoint selezionato. La tabella seguente mostra il tipo di protocollo, la quantità di dati, il numero totale di pacchetti e la percentuale del traffico totale che utilizza ciascun protocollo elencato.

Top 5 Applications (Le cinque risorse più attive)

La risorsa Top 5 Applications permette di esaminare a colpo d'occhio le applicazioni utilizzate in misura maggiore dall'endpoint selezionato. La tabella sotto il diagramma mostra il nome dell'applicazione, la quantità di dati che viene trasferita, il numero totale equivalente di pacchetti e la percentuale del traffico totale che può essere fatta risalire all'utilizzo dell'applicazione elencata da parte del protocollo selezionato. Facendo clic su un'applicazione se ne apre la vista NetFlow Application. Per ulteriori informazioni, vedi "Vista NetFlow Application" a pagina 30.

Top 5 Traffic Sources by Country (I cinque sorgenti di traffico più attive secondo il Paese)

La risorsa Top 5 Traffic Sources by Country permette di esaminare a colpo d'occhio, tramite un diagramma, i Paesi da cui ha origine il traffico sull'endpoint selezionato, classificati secondo la percentuale del traffico totale sull'endpoint stesso. La tabella sotto il diagramma riporta il nome del Paese da cui ha origine il traffico verso l'endpoint visualizzato, il volume del traffico instradato e la percentuale di tutto il traffico instradato all'endpoint visualizzato che può essere fatto risalire al Paese elencato.

Top 5 Traffic Destinations by Country (Le cinque destinazioni del traffico più attive secondo il Paese)

La risorsa Top 5 Traffic Destinations by Country fornisce un diagramma e una tabella dei Paesi verso cui è diretto il traffico dall'endpoint selezionato, classificati secondo la percentuale del traffico totale proveniente dall'endpoint stesso. La tabella sotto il diagramma riporta il nome del Paese verso cui è instradato il traffico, il volume del traffico instradato verso i server nel Paese elencato e la percentuale di tutto il traffico instradato dall'endpoint visualizzato verso i server nel Paese elencato.

Unique Visitors (Visitatori unici)

La risorsa Unique Visitors visualizza un diagramma degli indirizzi IP unici che hanno comunicato con l'endpoint visualizzato durante un intervallo specificato.

Top 5 Types of Service (I cinque tipi di servizio più attivi)

La risorsa Top 5 Types of Service permette di esaminare a colpo d'occhio i servizi utilizzati in misura maggiore dall'endpoint selezionato. La tabella sotto il diagramma riporta le seguenti informazioni per ciascun tipo di servizio:

- Il tipo di servizio
- Il volume del traffico, in byte e pacchetti, gestito dal servizio
- La percentuale di tutto il traffico instradato verso l'endpoint selezionato che viene gestito dal tipo di servizio selezionato

Per ulteriori informazioni sul monitoraggio del tipo di servizio in Orion NTA, vedi "Configuring NetFlow Types of Services" nel documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Vista NetFlow Interface Details

Le seguenti sezioni descrivono brevemente le risorse disponibili sulla vista NetFlow Interface Details predefinita. Per ulteriori informazioni su ciascuna risorsa, inclusi i dettagli della configurazione, fare clic su **Help** (Guida) nella barra del titolo della risorsa.

Top 5 Protocols (I cinque protocolli più attivi)

La risorsa Top 5 Protocols permette di esaminare a colpo d'occhio i protocolli del traffico che l'interfaccia visualizzata rileva in misura maggiore. La tabella seguente mostra il tipo di protocollo, la quantità di dati, il numero totale di pacchetti e la percentuale del traffico totale attraverso l'interfaccia visualizzata e che utilizza ciascun protocollo elencato.

Top 5 Endpoints (I cinque endpoint più attivi)

La risorsa Top 5 Endpoints fornisce un diagramma e una tabella degli endpoint che generano la maggior parte del traffico attraverso l'interfaccia selezionata. La tabella sotto il diagramma riporta il nome o l'indirizzo IP di ciascun endpoint visualizzato, il volume del traffico generato da ciascun endpoint elencato, sia in byte che in pacchetti, e la percentuale di tutto il traffico attraverso l'interfaccia visualizzata che può essere fatto risalire a ciascun endpoint elencato. Facendo clic su un endpoint se ne apre la vista NetFlow Endpoint. Per ulteriori informazioni, vedi "Vista NetFlow Endpoint" a pagina 33.

Top 5 Applications (Le cinque risorse più attive)

La risorsa Top 5 Applications permette di esaminare a colpo d'occhio le applicazioni utilizzate in misura maggiore dall'interfaccia visualizzata. La tabella sotto il diagramma mostra il nome dell'applicazione, la quantità di dati che viene trasferita, il numero totale equivalente di pacchetti e la percentuale del traffico totale che può essere fatta risalire all'utilizzo dell'applicazione elencata da parte dell'interfaccia visualizzata. Facendo clic su un'applicazione se ne apre la vista NetFlow Application. Per ulteriori informazioni, vedi "Vista NetFlow Application" a pagina 30.

Top 5 Domains (I cinque domini più attivi)

Questa risorsa permette di esaminare a colpo d'occhio i domini che stanno generano la maggior parte del traffico sull'interfaccia selezionata. La tabella seguente mostra il nome del dominio, il volume del traffico in byte, il numero totale di pacchetti trasferito e la percentuale del traffico totale attraverso l'interfaccia selezionata che può essere fatto risalire a ciascun dominio.

Top 5 Types of Service (I cinque tipi di servizio più attivi)

La risorsa Top 5 Types of Service permette di esaminare a colpo d'occhio i servizi utilizzati in misura maggiore dall'interfaccia visualizzata. La tabella sotto il diagramma riporta le seguenti informazioni per ciascun tipo di servizio:

- Il tipo di servizio
- Il volume del traffico, in byte e pacchetti, gestito dal servizio attraverso l'interfaccia visualizzata
- La percentuale di tutto il traffico instradato attraverso l'interfaccia visualizzata che viene gestito dal tipo di servizio selezionato

Per ulteriori informazioni sul monitoraggio del tipo di servizio in Orion NTA, vedi "Configuring NetFlow Types of Services" nel documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Top 5 Conversations (Le cinque conversazioni più attive)

Questa risorsa fornisce un elenco delle conversazioni che creano la maggior parte del traffico attraverso l'interfaccia visualizzata. Per ciascuna conversazione, questa risorsa fornisce la quantità di dati trasferiti e la percentuale della conversazione elencata rappresenta la quantità totale di dati trasferiti attraverso l'interfaccia visualizzata. Facendo clic su una conversazione se ne apre la vista NetFlow Conversation. Per ulteriori informazioni, vedi "Vista NetFlow Conversation" a pagina 33.

Vista NetFlow Node Details

Le seguenti sezioni descrivono brevemente le risorse disponibili sulla vista NetFlow Node Details predefinita. Per ulteriori informazioni su ciascuna risorsa, inclusi i dettagli della configurazione, fare clic su **Help** (Guida) nella barra del titolo della risorsa.

Top 5 Protocols (I cinque protocolli più attivi)

La risorsa Top 5 Protocols permette di esaminare a colpo d'occhio i protocolli utilizzati in misura maggiore dal nodo visualizzato. La tabella seguente mostra il tipo di protocollo, la quantità di dati, il numero totale di pacchetti e la percentuale

del traffico totale attraverso il nodo visualizzato e che utilizza ciascun protocollo elencato.

Top 5 Applications (Le cinque risorse più attive)

La risorsa Top 5 Applications permette di esaminare a colpo d'occhio le applicazioni utilizzate in misura maggiore dal nodo visualizzato.

La tabella sotto il diagramma mostra il nome dell'applicazione, la quantità di dati che viene trasferita, il numero totale equivalente di pacchetti e la percentuale del traffico totale che può essere fatta risalire all'utilizzo dell'applicazione elencata da parte del nodo visualizzato. Facendo clic su un'applicazione se ne apre la vista NetFlow Application. Per ulteriori informazioni, vedi "Vista NetFlow Application" a pagina 30.

Top 5 Conversations (Le cinque conversazioni più attive)

Questa risorsa fornisce un elenco delle conversazioni che creano la maggior parte del traffico attraverso il nodo visualizzato. Per ciascuna conversazione, questa risorsa fornisce la quantità di dati trasferiti e la percentuale della conversazione elencata rappresenta la quantità totale di dati trasferiti attraverso il nodo visualizzato. Facendo clic su una conversazione se ne apre la vista NetFlow Conversation. Per ulteriori informazioni, vedi "Vista NetFlow Conversation" a pagina 33.

Top 5 Endpoints (I cinque endpoint più attivi)

La risorsa Top 5 Endpoints fornisce un diagramma e una tabella degli endpoint che generano la maggior parte del traffico attraverso il nodo visualizzato. La tabella sotto il diagramma riporta il nome o l'indirizzo IP di ciascun endpoint visualizzato, il volume del traffico generato da ciascun endpoint elencato, sia in byte che in pacchetti, e la percentuale di tutto il traffico attraverso il nodo visualizzato che può essere fatto risalire a ciascun endpoint elencato. Facendo clic su un endpoint se ne apre la vista NetFlow Endpoint. Per ulteriori informazioni, vedi "Vista NetFlow Endpoint" a pagina 33.

Top 5 Domains (I cinque domini più attivi)

Questa risorsa permette di esaminare a colpo d'occhio i domini che stanno generano la maggior parte del traffico sul nodo visualizzato. La tabella seguente mostra il nome del dominio, il volume del traffico in byte, il numero totale di pacchetti trasferito e la percentuale del traffico totale attraverso il nodo visualizzato che può essere fatto risalire a ciascun dominio.

Node Interfaces (Interfacce del nodo)

Questa risorsa fornisce un elenco di tutte le interfacce monitorate sul nodo visualizzato. Per ciascun interfaccia sono forniti sia il traffico in entrata che quello in uscita. Facendo clic su un endpoint se ne apre la vista NetFlow Interface Details. Per ulteriori informazioni, vedi “Vista NetFlow Interface Details” a pagina 36.

Capitolo 4

Utilizzo di Orion NetFlow Traffic Analyzer

Orion Network Performance Monitor è in grado di rilevare l'utilizzo della larghezza di banda attraverso una data interfaccia; Orion NetFlow Traffic Analyzer amplia questa funzionalità, fornendo ulteriori informazioni sull'utente effettivo di tale larghezza di banda e sulle applicazioni utilizzate. Gli scenari presentati in questo capitolo illustrano l'utilità di Orion NetFlow Traffic Analyzer e come possa offrire un'immediata e notevole redditività dell'investimento effettuato.

Utilizzo di Traffic View Builder

Mediante la risorsa Traffic View Builder si possono generare rapidamente viste personalizzate per ogni periferica NetFlow. Traffic View Builder permette di creare versioni personalizzate delle viste riportate nella seguente tabella.

Tipi di viste personalizzabili con Traffic View Builder		
Applicazione	Paese	Dominio
Endpoint	Interfaccia	Gruppo dell'indirizzo IP
Protocollo	Router	Tipo di servizio

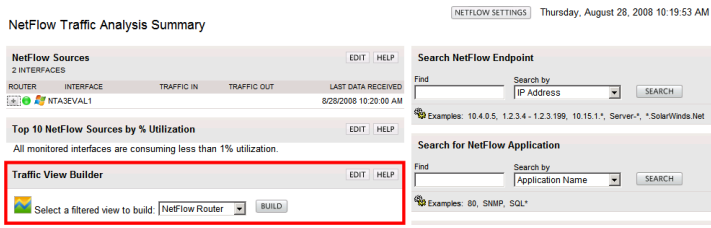
Le seguenti sezioni presentano scenari che mostrano come la risorsa Orion NTA Traffic View Builder permetta di creare viste personalizzate.

Visualizzazione del traffico per un indirizzo IP designato

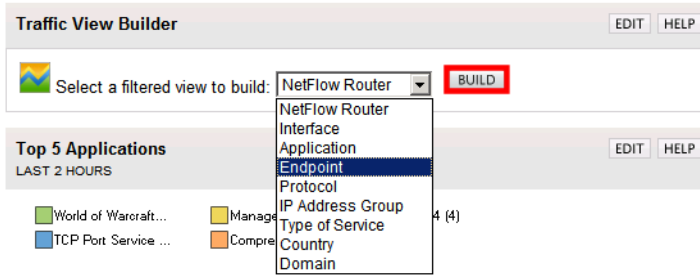
La seguente procedura mostra come creare una vista Orion NTA personalizzata che visualizzi sia il traffico in entrata che quello in uscita corrispondente a un indirizzo IP designato.

Per creare una vista per un indirizzo IP designato:

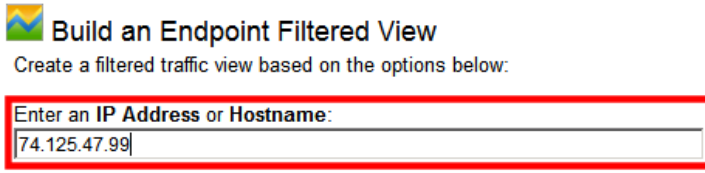
1. Fare clic su **Start > All Programs > SolarWinds Orion > Orion Web Console** (Avvio > Tutti i programmi > SolarWinds Orion > Console web Orion), quindi individuare la risorsa Traffic View Builder.



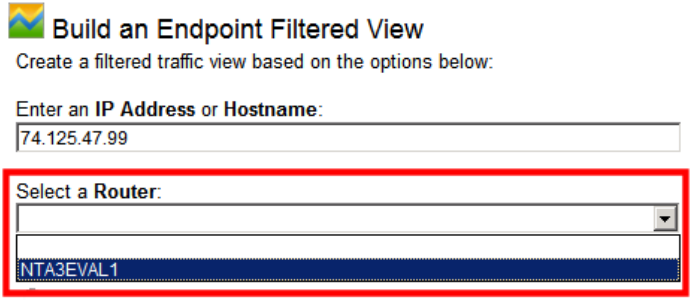
2. Selezionare **Endpoint**, quindi fare clic su **Build** (Crea).



3. Digitare l'**IP address** (Indirizzo IP) che si desidera monitorare.



4. Selezionare il router che invia il traffico all'indirizzo IP selezionato.



5. Selezionare **All Interfaces** (Tutte le interfacce) quando compare il menu Select an Interface (Selezionare un'interfaccia).

   Nota: è possibile personalizzare ulteriormente la vista in modo che mostri solo il traffico attraverso un'interfaccia specifica del router, ma ai fini di questa valutazione, selezionare **All Interfaces** (Tutte le interfacce) per visualizzare tutto il traffico attraverso il router selezionato.

6. Fare clic su **Submit** (Invia); compare la vista NetFlow Endpoint personalizzata.

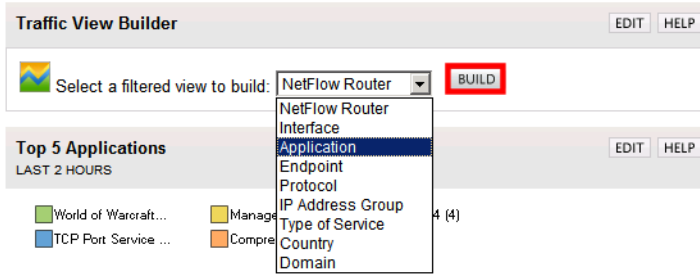
   Nota: Per ulteriori informazioni sulla vista NetFlow Endpoint, vedi “Vista NetFlow Endpoint” a pagina 33.

Visualizzazione del traffico relativo a porte o applicazioni specifiche

La seguente procedura illustra come creare una vista Orion NTA personalizzata che mostra il traffico della rete attraverso porte specifiche o ad applicazioni designate.

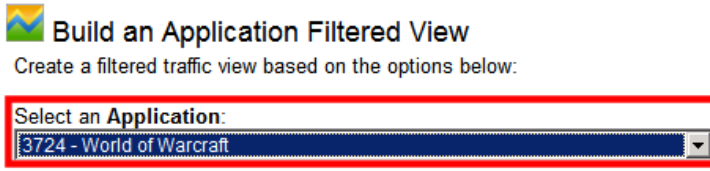
Per creare una vista per porte o applicazioni specifiche:

1. Fare clic su **Start > All Programs > SolarWinds Orion > Orion Web Console** (Avvio > Tutti i programmi > SolarWinds Orion > Console web Orion), quindi individuare la risorsa Traffic View Builder.
2. Selezionare **Application** (Applicazioni), quindi fare clic su **Build** (Crea).



3. Digitare l’**Application** (Applicazioni) o la porta che si desidera monitorare.

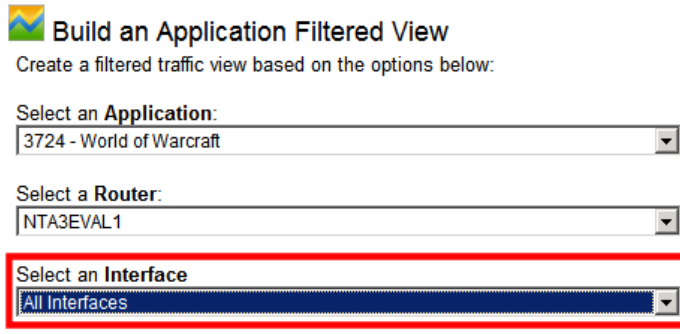
   Nota: le applicazioni sono elencate secondo i numeri delle porte corrispondenti. Per determinare i numeri delle porte corrispondenti alle applicazioni, usare la funzione di ricerca della risorsa NetFlow Application o la vista NetFlow Traffic Analysis Summary. Per ulteriori informazioni, vedi “Search for NetFlow Application (Ricerca di applicazioni NetFlow)” a pagina 25.



4. Selezionare il router NetFlow che sta instradando il traffico dell'applicazione.

5. Selezionare **All Interfaces** (Tutte le interfacce) quando compare il menu Select an Interface (Selezionare un'interfaccia).

   Nota: è possibile personalizzare ulteriormente la vista in modo che mostri solo il traffico dell'applicazione attraverso un'interfaccia specifica del router, ma ai fini di questa valutazione, selezionare **All Interfaces** (Tutte le interfacce) per visualizzare tutto il traffico attraverso il router selezionato.



6. Fare clic su **Submit** (Invia); compare la vista NetFlow Application personalizzata.

Nota: per ulteriori informazioni sulla vista NetFlow Endpoint, vedi "Vista NetFlow Application" a pagina 30.

Individuazione e isolamento di un computer infetto

È possibile impiegare l'istanza di Orion NPM attualmente installata, insieme con Orion NTA, per individuare velocemente un'ampia gamma di virus autopropaganti che possono attaccare la rete e intervenire tempestivamente. Si consideri il seguente scenario:

1. In una filiale della banca che impiega la rete per la gestione di tutte le transazioni relative a carte di credito la rete funziona con estrema lentezza, causando timeout frequenti durante i trasferimenti di dati sensibili.
2. Orion Web Console mostra che il collegamento con la filiale è funzionante.
3. I diagrammi di utilizzo percentuale di Orion NPM, nella home page Network Summary, mostrano che l'utilizzo attuale è pari al 98%, mentre il normale utilizzo da parte della filiale è pari a 15-25%.
4. Facendo clic su **NetFlow Traffic Analysis** (Analisi del traffico NetFlow) nella barra strumenti Modules (Moduli) e quindi sul nome del collegamento alla filiale nella risorsa NetFlow Sources (Sorgenti NetFlow) si visualizza il router NetFlow che instrada il traffico alla filiale.
5. Un colpo d'occhio alla risorsa Top 5 Endpoints (I cinque endpoint più attivi) mostra che un solo computer nell'intervallo di indirizzi IP `10.10.10.0-10.10.10.255` genera l'80% del carico sul link della filiale.
6. È noto che i computer con indirizzo IP compreso in questo intervallo sono accessibili ai clienti che desiderano eseguire transazioni online.
7. Esaminando la risorsa Top 5 Applications (Le cinque applicazioni più attive), si scopre rapidamente che il 100% delle ultime due ore di traffico proveniente da un computer accessibile pubblicamente è stato generato da un'applicazione di messaggeria IBM MQSeries.
8. Facendo clic sul nome dell'applicazione IBM MQSeries di cui sopra nella risorsa Top 5 Applications è possibile determinare che i messaggi IBM MQSeries vengono trasmessi attraverso la porta 1883.
9. Sapendo che non esiste nessuna periferica che utilizza l'applicazione IBM MQSeries sul computer accessibile al cliente né alcun altro servizio o protocollo che richiede la porta 1883, risulta evidente che si è in presenza di un virus.
10. Tramite uno strumento di gestione della configurazione, come Cirrus Configuration Manager, si stabilisce una nuova configurazione del firewall in modo da bloccare la porta 1883.

Individuazione e bloccaggio di utilizzi indesiderati

Con Orion NTA è possibile diagrammare agevolmente un aumento di utilizzo su uno qualsiasi dei vari uplink della rete. Orion NPM permette già di diagrammare l'utilizzo, ma aggiungendo Orion NTA è possibile individuare istanze specifiche di utilizzo indesiderato, in modo da poter intervenire immediatamente, come nel seguente scenario:

1. L'uplink a Internet ha rallentato progressivamente nel corso degli ultimi 6 mesi anche se il numero di utenti, l'utilizzo delle applicazioni e la larghezza di banda dedicata sono rimasti invariati.
2. Quando si apre la console web Orion, la vista Network Summary Home (Pagina iniziale riepilogo rete) mostra che il link del sito a Internet è funzionale, ma quando si fa clic su di esso e si consulta il diagramma Current Percent Utilization of each Interface (Utilizzo percentuale attuale di ciascuna interfaccia), si scopre che l'utilizzo attuale dell'interfaccia con il web è pari a 80%.
3. Facendo clic sull'interfaccia con il web si apre la vista Interface Details (Dettagli interfaccia).
4. Personalizzando il diagramma di utilizzo percentuale in modo da esaminare gli ultimi 6 mesi, si osserva che nel corso del tempo il consumo è aumentano costantemente, dal 15% all'80%, con picchi transitori che vanno anche oltre il 90%.
5. Facendo clic sulla scheda NetFlow Traffic Analysis (Analisi del traffico NetFlow) e quindi sull'interfaccia con il web si apre la vista NetFlow Interface Details (Dettagli interfaccia NetFlow).
6. Osservando i 50 endpoint più attivi, si rileva che un gruppo di computer con indirizzo IP nell'intervallo `10.10.12.0-10.10.12.255` consuma la maggior parte della larghezza di banda. Questi computer risiedono nell'intervallo di indirizzi IP vendite interne.
7. Esaminando in maggiori dettagli ciascuno degli indirizzi IP causa del problema, si scopre che tale indirizzo mostra Kazaa (porta 1214) e World of Warcraft (porta 3724) nelle cinque applicazioni più attive.
8. Tramite uno strumento di gestione della configurazione, come Cirrus Configuration Manager, si stabilisce una nuova configurazione del firewall in modo da bloccare le porte 1214 e 3724.
9. Nell'arco di minuti il traffico attraverso l'interfaccia scende al 25%.

Individuazione e bloccaggio di attacchi "Denial of Service" ("Rifiuto del servizio")

Orion NTA permette di caratterizzare facilmente sia il traffico in entrata che quello in uscita. Questa funzionalità è ancora più importante in quanto le reti aziendali sono esposte sempre di più agli attacchi di rifiuto del servizio. Si consideri il seguente scenario:

1. Un allarme avanzato di Orion NPM segnala che il router che s'interfaccia con il web ha problemi a creare e mantenere una connessione stabile con Internet.
2. Aprendo la console web Orion per indagare sulle cause, si osserva che tutte le connessioni sono funzionali e l'utilizzo della larghezza di banda appare soddisfacente. Si nota invece che l'utilizzo della CPU sul nodo del firewall è sempre compreso tra il 99% e il 100%.
3. Facendo clic sul nodo del firewall se ne apre la pagine Node Details (Dettagli nodo) in cui la risorsa Current Percent Utilization of Each Interface (Utilizzo percentuale attuale di ciascuna interfaccia) mostra che le interfacce del firewall ricevono livelli insolitamente alti di traffico.
4. Facendo clic su **NetFlow Traffic Analysis** (Analisi del traffico NetFlow) nella barra strumenti Modules (Moduli) si può esaminare a colpo d'occhio la risorsa Top 50 Endpoints (I 50 endpoint più attivi) personalizzata.
5. La risorsa Top 50 Endpoints mostra che i sei computer più attivi che tentano di accedere alla rete sono situati oltreoceano.
6. A questo punto è evidente che le porte sono soggette ad accessi ciclici e che il firewall sta bloccando interattivamente questi attacchi.
7. Tramite uno strumento di gestione della configurazione, come Cirrus Configuration Manager, si stabilisce una nuova configurazione del firewall in che blocca tutto il traffico nell'intervallo di indirizzi IP dei computer che tentano di accedere alla rete.
8. Nell'arco di minuti, l'utilizzo della CPU sul router che s'interfaccia con il web ritorna al livello normale.

Ulteriori funzionalità di Orion NTA

Nelle sezioni precedenti sono state illustrate solo alcune della miniera di funzionalità di monitoraggio delle reti offerta da Orion NetFlow Traffic Analyzer. Consultare il documento *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*, disponibile sul sito web SolarWinds, http://www.solarwinds.com/support/documentation.aspx, per scoprire ulteriori funzionalità di Orion NetFlow Traffic Analyzer.