SolarWinds Orion NetFlow Traffic Analyzer

Evaluation Guide

Orion NetFlow Traffic Analyzer Evaluation Guide, Version 3.0, 08.28.2008

À propos de SolarWinds

SolarWinds Inc développe et commercialise une série d'outils de gestion, de surveillance et de détection de réseau en réponse aux diverses exigences actuelles de la gestion de réseau et des spécialistes du conseil. Les produits SolarWinds continuent à définir la norme en matière de qualité et de performances ; ils ont fait de la société le leader des technologies de gestion et de détection de réseau. La clientèle de SolarWinds inclut plus de 45 pour cent des sociétés Fortune 500 et s'étend sur plus de 90 pays. Notre réseau mondial de distributeurs et partenaires commerciaux compte plus de 100 distributeurs et revendeurs.

Pour prendre contact avec SolarWinds

Plusieurs moyens permettent de prendre contact avec SolarWinds :

Équipe	Coordonnées
Ventes	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Assistance technique	www.solarwinds.com/support
Forums d'utilisateurs	www.thwack.com

Conventions de mise en forme

Des conventions de mise en forme cohérentes permettent de repérer des passages précis dans tous les documents imprimés et en ligne.

Convention	Indique
Caractères gras	Éléments de Windows, y compris les boutons et les champs
Caractères italiques	Titre des ouvrages et des CD, nom des variables, nouveaux termes
`Police à espacement fixe`	Nom des fichiers et répertoires, commandes et exemples de code, texte saisi par l'utilisateur
Crochets, comme dans [*valeur*]	Paramètres de commande facultatifs
Accolades, comme dans {*valeur*}	Paramètres de commande obligatoires
OU logique, comme dans *valeur1*|*valeur2*	Paramètres de commande exclusifs, pour lesquels on ne peut spécifier qu'une seule option

Bibliothèque de documents de SolarWinds Orion NetFlow Traffic Analyzer

Les documents suivants sont inclus dans la bibliothèque de documents de SolarWinds Orion NetFlow Traffic Analyzer :

Document	Objectif
Guide de l'administrateur	Contient des informations relatives à l'installation, à la configuration et à différents concepts.
Aide détaillée	Fournit l'aide relative à chaque fenêtre de l'interface utilisateur d'Orion NetFlow Traffic Analyzer.
Evaluation Guide	Présentation des fonctionnalités et instructions d'Orion Network Performance Monitor en vue de l'installation et de la configuration initiale.
Guide de prise en main	Scénarios d'installation, de configuration et de situations fréquentes pour lesquels Orion NetFlow Traffic Analyzer fournit une solution simple mais performante.
Notes de publication	Détaillent les toutes dernières informations, les problèmes connus et les mises à jour. Les dernières notes de publication se trouvent sur www.solarwinds.com.

Table des matières

Chapitre 1

Introduction à Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer (Orion NTA) offre une solution de surveillance de réseau -simple et évolutive- aux professionnels de l'informatique qui gèrent un réseau NetFlow, sFlow ou J-Flow de n'importe quelle taille.

Pourquoi installer Orion NetFlow Traffic Analyzer

Au fur et à mesure de la croissance des entreprises et de leurs réseaux, les besoins en bande passante augmentent de manière exponentielle. Tous les secteurs d'activité modernes connectés en réseau investissent beaucoup de temps et d'argent pour disposer d'une bande passante suffisante pour les activités et applications indispensables à l'entreprise. Lorsque les besoins en bande passante excèdent la capacité disponible ou quand la demande semble dépasser les possibilités du réseau, la bonne connaissance de cette bande passante cesse d'être saugrenue et devient essentielle pour décider s'il est nécessaire d'investir dans plus de bande passante ou si des consignes d'utilisation plus restrictives seront suffisantes pour récupérer la bande passante perdue.

L'essor des médias diffusés en continu, des technologies de voix sur IP (VoIP), des jeux en ligne et d'autres applications gourmandes en bande passante, oblige les ingénieurs réseau, vous, en l'occurrence, à répondre à des questions plus complexes que de savoir si le réseau est fonctionnel ou non. Vous devez pouvoir expliquer pourquoi le réseau n'est pas aussi performant qu'on s'y attendrait.

Si vous avez besoin de savoir qui utilise la bande passante, et comment, Orion NetFlow Traffic Analyzer vous apporte une réponse simple et intégrée. Ainsi, vous pouvez rapidement assurer le suivi et surveiller l'utilisation de la bande passante consommée par une application particulière ou un certain type de trafic. Si, par exemple, vous constatez qu'une interface particulière consomme beaucoup de bande passante, Orion NetFlow Traffic Analyzer vous permettra de voir qu'une vidéoconférence d'entreprise consomme 80 % de la bande passante disponible sur un commutateur donné. À la différence de nombreux autres produits d'analyse NetFlow, les données réseau et NetFlow fournies par la solution Orion NetFlow Traffic Analyzer ne sont pas seulement des données extrapolées, mais sont basées sur des informations réelles collectées sur le réseau par le produit Orion Network Performance Monitor qui est au cœur de Orion NetFlow Traffic Analyzer.

Prêt à l'emploi, Orion NetFlow Traffic Analyzer offre d'importantes capacités de surveillance et de tracé de diagrammes associées à des statistiques détaillées, dont :

- La répartition de la bande passante en fonction des différents types de trafic
- Les schémas d'utilisation au fil du temps
- L'identification et le suivi du trafic externe
- L'intégration étroite avec les statistiques détaillées sur les performances des interfaces.

Ces capacités de surveillance, associées à la Web Console personnalisable d'Orion Network Performance Monitor et aux moteurs de création de rapports, font de Orion NetFlow Traffic Analyzer votre option de choix pour la surveillance de votre réseau compatible NetFlow.

Pourquoi utiliser Orion NetFlow Traffic Analyzer

Orion NetFlow Traffic Analyzer permet de surveiller rapidement et facilement les ressources du réseau et les schémas d'utilisation avec un niveau de détail entièrement personnalisable. Ces fonctionnalités essentielles de Orion NetFlow Traffic Analyzer sont une aide précieuse :

Meilleures disponibilité et performances

Orion NetFlow Traffic Analyzer permet de détecter, diagnostiquer et résoudre plus rapidement les ralentissements et les pannes du réseau.

Planification analytique de la capacité

Orion NetFlow Traffic Analyzer met en évidence les tendances du trafic réseau, ce qui vous permet d'anticiper avec intelligence les variations de la bande passante dans des secteurs embouteillés.

Allocation optimisée des ressources réseau

Les informations fournies par Orion NetFlow Traffic Analyzer permettent de repérer les secteurs du réseau dont les connexions sont limitées ou surexploitées. Vous pouvez alors rediriger le trafic existant vers un autre segment du réseau disposant de bande passante inutilisée.

Alignement des ressources informatiques sur les besoins de l'entreprise

Orion NetFlow Traffic Analyzer est basé sur l'infrastructure éprouvée d'Orion Network Performance Monitor, ce qui permet d'évaluer tant les besoins du réseau d'entreprise dans sa globalité que les détails fonctionnels d'interfaces et de nœuds spécifiques.

Meilleure sécurité du réseau

Orion NetFlow Traffic Analyzer permet d'examiner rapidement et précisément le trafic réseau, puis de repérer et démasquer les schémas suspects, les comportements non souhaités et toute utilisation anormale révélateurs d'une infection par un virus, un robot ou un logiciel espion.

Application multifonctionnelle de surveillance NetFlow et performances réseau

Arrêtez de passer d'un programme à l'autre pour vous faire une idée complète de l'utilisation, des performances et des besoins du réseau. Tout ce dont vous avez besoin pour surveiller votre réseau compatible NetFlow se trouve dans Orion Network Performance Monitor et Orion NetFlow Traffic Analyzer.

Fonctionnalités de Orion NTA version 3.0

Orion NTA version 3.0 met à votre disposition les fonctionnalités suivantes pour mieux surveiller les dispositifs compatibles NetFlow sur votre réseau.

Recherche par plage d'adresse IP

Cette version de Orion NTA permet de rechercher des points de terminaison dans une plage d'adresses IP spécifiée (`10.10.199.1–10.10.199.50`, par exemple).

Maintenant disponible, la prise en charge de flux supplémentaires

Orion NTA version 3 prend actuellement en charge les formats de flux NetFlow v9, sFlow v5, et J pour la collecte des données du réseau.

Vues personnalisées du trafic

L'utilitaire Traffic View Builder inclus dans cette version de Orion NTA permet de filtrer les données NetFlow collectées afin de créer des vues personnalisées facilement accessibles. Vous pouvez, par exemple, construire une vue affichant le trafic vers un domaine spécifique généré pendant les heures ouvrées standard (8 h – 17 h) à partir d'une adresse IP sélectionnée.

Ressource Top 10 NetFlow Sources by Percent Utilization (Dix principales sources NetFlow par pourcentage d'utilisation)

Une nouvelle ressource de la vue résumée NetFlow répertorie les sources NetFlow surveillées par pourcentage d'utilisation.

Vues des performances de qualité de service

Orion NTA version 3 facilite la visualisation du trafic réseau total segmenté par méthode de classe de service, telle que TOS ou DSCP. Il est également possible de quantifier et de visualiser la bande passante consommée par chacun des niveaux de qualité de service y compris la voix et les données vidéo.

Regroupement des ports des applications

Cette version de Orion NTA permet d'affecter une application utilisant plusieurs ports réseau à un groupe afin d'en jauger les performances.

Cinq principales ressources de la totalité du réseau

Une nouvelle liste des cinq principales ressources pour le trafic au niveau du réseau répertorie les groupes d'adresse IP, les applications, les conversations, les pays, les points de terminaison, les types de service, les émetteurs, récepteurs et protocoles.

Intégration complète des ressources NetFlow avec les vues d'Orion

Il est facile d'ajouter automatiquement les ressources NetFlow aux vues d'Orion.

Fonctionnalité de recherche immédiate de DNS

Lancez des recherches manuelles de DNS sans attendre la mise à jour de DNS planifiée.

Fonctionnement de Orion NetFlow Traffic Analyzer

Les dispositifs compatibles NetFlow fournissent une grande quantité d'informations sur le trafic sur IP. Orion NetFlow Traffic Analyzer collecte ces données NetFlow, les corrèle sous un format utilisable, puis les présente, avec les données détaillées sur les performances réseau collectées par SolarWinds Orion Network Performance Monitor, dans des graphiques et des rapports sur l'utilisation entrante, sortante et interne au réseau, de la bande passante. Ces rapports permettent de surveiller la bande passante, d'assurer le suivi des conversations entre les points de terminaison internes et externes, d'analyser le trafic et de planifier les besoins en capacité de bande passante.

Chapitre 2

Installation de Orion NetFlow Traffic Analyzer

La procédure d'installation de Orion NetFlow Traffic Analyzer (Orion NTA) est guidée par un assistant. Pour un produit de qualité professionnelle, les exigences sont nominales.

Remarque : les données NetFlow sont volumineuses et peuvent consommer beaucoup de mémoire de base de données en relativement peu de temps. Cette remarque concerne également les petits réseaux. SolarWinds vous conseille donc vivement d'installer la base de données SQL Server et Orion NPM/NTA sur des serveurs matériels distincts.

Conditions requises

Le serveur utilisé pour héberger la solution NetFlow doit prendre en charge aussi bien Orion NPM que Orion NTA, car Orion NTA est basé sur Orion NPM et en étend les fonctionnalités. Les sections suivantes indiquent quelles sont les configurations minimales requises.

Configuration logicielle

La configuration logicielle suivante suppose que la version d'évaluation de Orion NTA est installée sur un serveur exécutant Orion NPM version 9.0. Pour évaluer Orion NTA version 3.0 sur une installation d'Orion NPM version 8.5.1, veuillez contacter SolarWinds à l'adresse sales@solarwinds.com.

Remarque : SQL Express et MSDE restreignent respectivement la taille de la base de données à 4 Go et 2 Go. C'est pourquoi SolarWinds ne prend pas en charge leur utilisation avec Orion NTA dans les environnements de production.

Logiciels	Conditions requises
Système d'exploitation	Windows Server 2003 (32 ou 64 bits) avec R2, et IIS installé. SolarWinds recommande aux administrateurs d'Orion NPM de disposer des privilèges d'administrateur local pour l'utilisation de toutes les fonctionnalités des outils locaux d'Orion NPM. Les utilisateurs limités à la console Web n'ont pas besoin des privilèges d'administrateur. **Remarque :** SolarWinds ne prend pas en charge l'installation de Orion NTA sous Windows XP dans les environnements de production. Si vous installez Orion NTA sous Windows XP, vous devez vérifier que la mémoire partagée, les tubes nommés et TCP/IP sont activés sur les bases de données distantes.

Logiciels	Conditions requises
Serveur Web	Microsoft IIS version 6.0 et versions ultérieures. Les spécifications DNS exigent que le nom des hôtes soit composé de caractères alphanumériques (A à Z, 0 à 9), du signe moins (-) et de points (.). Le caractère de soulignement (_) n'est pas autorisé. Pour plus d'informations, consultez *RFC 952*. **Remarque :** SolarWinds déconseille d'installer Orion NTA sur le même serveur ou pour utiliser le même serveur de base de donnée qu'un serveur Blackberry RIM (Research in Motion) et ne fournit pas d'assistance dans ce cas.
.NET Framework	Version 3.5 ou version ultérieure
Services SNMP Trap (interruptions SNMP)	Composant de gestion et de surveillance du système d'exploitation Windows
SQL Server	SQL Server 2000 SP4, Standard ou Entreprise SQL Server 2005 Standard ou Entreprise La base de données doit prendre en charge le mode mixte ou l'authentification SQL. **Remarque :** SQL Express ne gère pas les bases de données de taille supérieure à 4 Go. Il est limité à un seul processeur et n'utilise pas plus de 1 Go de RAM. Bien qu'il soit possible de l'utiliser pour surveiller une ou plusieurs interfaces aux fins d'évaluation, SolarWinds déconseille son utilisation pour les grands réseaux exigeant des bases de données plus volumineuses.
Navigateur Web Console	Microsoft Internet Explorer version 6 ou version ultérieure avec Active Scripting Mozilla Firefox 2.0 ou version ultérieure

Configuration matérielle

La configuration matérielle suivante suppose que la version d'évaluation de Orion NTA est installée sur un serveur exécutant Orion NPM version 9.0. Pour évaluer Orion NTA version 3.0 sur une autre version d'Orion NPM, veuillez contacter SolarWinds à l'adresse sales@solarwinds.com.

Remarque : Orion NTA exige que le port TCP 17777 soit ouvert, tant pour envoyer que pour recevoir le trafic entre Orion NPM et tout module Orion, dont Orion NTA.

Avertissement : Les seules configurations RAID utilisables pour l'installation de Orion NTA sont 0, 1, 0+1 et 1+0. En raison de la vitesse élevée et des exigences de mémoire des transactions de données NetFlow, SolarWinds déconseille l'utilisation d'autres configurations RAID ou SAN qui pourraient entraîner la perte de données et une importante dégradation des performances.

Matériel	Conditions requises
Processeur	3 GHz ou plus
RAM	2 Go ou plus
Espace libre sur le disque dur	5 Go ou plus Configurations RAID 0, 1, 0+1 et 1+0 conseillées. Les autres configurations RAID ou SAN sont déconseillées
Dispositifs NetFlow	Dispositifs Cisco utilisant NetFlow version 5 ou 9 **Remarque :** Orion NTA ne reconnaît que les modèles NetFlow version 9 incluant tous les champs utilisés par NetFlow version 5
J-Flow	Dispositifs réseau utilisant J-Flow
Dispositifs sFlow	Dispositifs sFlow utilisant sFlow version 5

Conditions requises pour Virtual Machine (les machines virtuelles)

L'installation d'Orion NTA sur les machines virtuelles VMWare et Serveurs virtuels Microsoft est totalement prise en charge si les exigences de configuration minimale sont satisfaites par chaque machine virtuelle.

Configuration de machine virtuelle	Conditions requises
Vitesse du processeur	3,0 GHz
Allocation d' espace libre sur le disque dur	5 Go **Remarque :** il est conseillé d'utiliser des disques RAID 1+0 ; l'utilisation de RAID 5 est déconseillée en raison des importants besoins en E/S.
Mémoire	2 Go
Interface réseau	Chaque installation d'Orion NPM doit disposer de sa propre carte d'interface réseau dédiée. **Remarque :** Orion NPM utilisant SNMP pour surveiller le réseau, s'il est impossible de réserver une carte d'interface réseau à l'installation d'Orion NPM, il peut se produire des interruptions du flux des données de surveillance en raison de la faible priorité accordée en général au trafic SNMP.

Pour plus d'informations sur les conditions requises par Orion NPM, veuillez consulter la section « Requirements » du manuel *SolarWinds Orion Network Performance Monitor Administrator Guide*.

SQL Server et SQL Server Express avec Orion NTA

Les données NetFlow sont volumineuses et peuvent consommer beaucoup de mémoire de base de données en relativement peu de temps, c'est pourquoi SolarWinds déconseille d'utiliser une base de données SQL Server Express pour Orion NTA. Il est plutôt conseillé d'utiliser une version de production de SQL Server.

La seule exception concerne la version d'évaluation de Orion NTA. Pour l'évaluation, Orion NPM et Orion NTA peuvent utiliser la version de base de données SQL Server Express 2005. Disponible gratuitement auprès de Microsoft, SQL Express permet d'évaluer Orion NTA sur une base de données réelle. Cependant, SolarWinds déconseille de l'utiliser avec Orion NTA dans un environnement de production pour les raisons suivantes :

- SQL Express ne gère pas les bases de données de taille supérieure à 4 Go.
- SQL Express est limité à un processeur unique.
- SQL Express ne peut pas utiliser plus de 1 Go de RAM.

Remarque : pour les environnement de production, Orion NPM et Orion NTA doivent utiliser une instance de base de données SQL Server installée sur un serveur distinct.

Installation de Orion NetFlow Traffic Analyzer

La procédure suivante permet d'installer Orion NetFlow Traffic Analyzer. Pour terminer l'installation, vous devez indiquer le port du trafic NetFlow et vérifier qu'il est activé et transmet bien les données du trafic NetFlow.

Remarque : la procédure suivante suppose que vous avez déjà installé Orion Network Performance Monitor version 9.0 sur le serveur sur lequel vous souhaitez installer Orion NetFlow Traffic Analyzer. Pour évaluer Orion Network Performance Monitor version 9.0, adressez-vous à SolarWinds, à l'adresse sales@solarwinds.com.

Pour installer Orion NetFlow Traffic Analyzer :

1. Connectez-vous au serveur d'Orion Network Performance Monitor à utiliser pour l'analyse du trafic NetFlow.
2. ***En cas d'installation de NetFlow Traffic Analyzer sur un serveur terminal,*** procédez comme suit avant de poursuivre l'installation pour que l'application soit correctement installée :

a. Cliquez sur **Start > Control Panel > Add or Remove Programs** (Démarrer > Panneau de configuration > Ajout/Suppression de programmes).

b. Cliquez sur **Add New Programs** (Ajouter de nouveaux programmes).

c. Cliquez sur **CD or Floppy** (CD ou disquette), puis sur **Next** (Suivant) pour installer le programme à partir d'une disquette ou d'un cédérom.

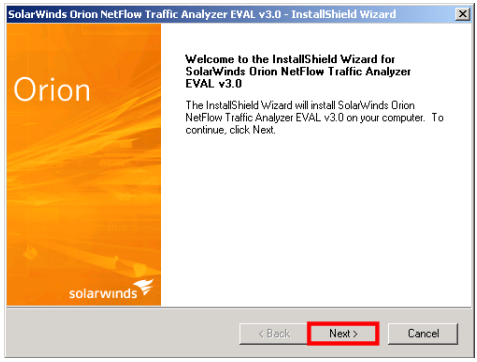
3. ***Si vous avez téléchargé le produit depuis le site Web SolarWinds,*** suivez les étapes ci-dessous :

   a. Naviguez jusqu'à l'emplacement de téléchargement du fichier `.zip`, puis décompressez le logiciel d'évaluation dans un répertoire approprié.

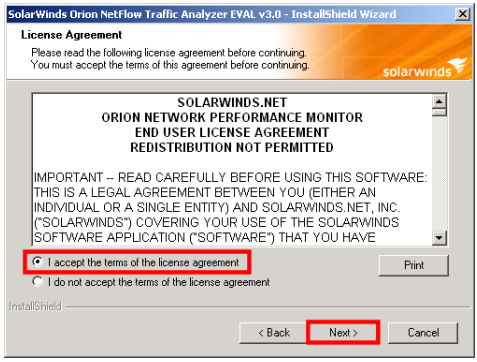
   b. Lancez l'exécutable d'évaluation de SolarWinds Orion NTA.

4. ***Si vous avez reçu un support physique,*** recherchez dessus l'exécutable d'évaluation de SolarWinds Orion NTA puis lancez-le.

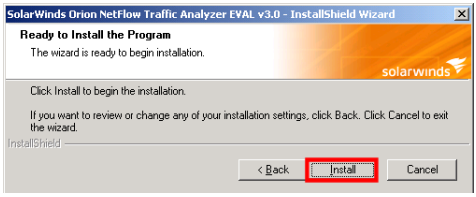
5. Lisez le texte de bienvenue, puis cliquez sur **Next** (Suivant).



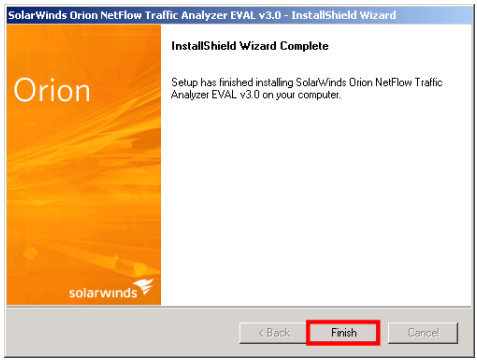
6. Sélectionnez **I accept the terms of the license agreement** (J'accepte les termes de cet accord de licence), puis cliquez sur **Next** (Suivant).



7. Cliquez sur **Install** (Installer) sur la fenêtre Ready to Install the Program (Prêt à installer le programme).

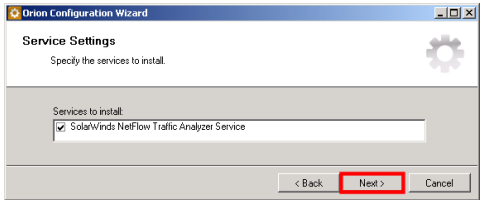


8. À la fin de l'assistant InstallShield, cliquez sur **Finish** (Terminer) pour le refermer.

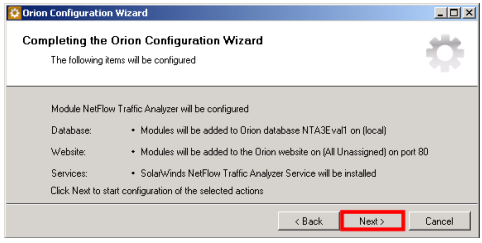


9. ***Si le système vous demande de redémarrer le serveur,*** choisissez l'option qui convient parmi les deux suivantes :
   - ***En cas d'installation de Orion NTA sur un serveur terminal,*** cliquez sur **No** (Non).
   - ***En cas d'installation de Orion NTA sur un autre type de serveur,*** cliquez sur **Yes** (Oui).
10. ***Si l'assistant de configuration ne démarre pas automatiquement,*** cliquez sur **Start > All Programs > SolarWinds Orion > Configuration Wizard** (Démarrer > Tous les programmes > SolarWinds Orion > Configuration Wizard).
11. Lisez le texte de bienvenue, puis cliquez sur **Next** (Suivant).

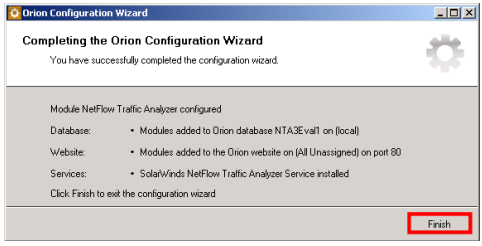
12. Vérifiez que le service **SolarWinds NetFlow Traffic Analyzer Service** (SolarWinds NetFlow Traffic Analyzer) est coché dans la fenêtre Service Settings (Paramètre du service), puis cliquez sur **Next** (Suivant).



13. Prenez connaissance du résumé de la configuration, puis cliquez sur **Next** (Suivant).



14. À la fin de l'assistant de configuration, cliquez sur **Finish** (Terminer).



Activation de l'analyse du trafic NetFlow

Pour lancer l'analyse des données NetFlow disponibles produites par les dispositifs du réseau, vous devez, soit ajouter une interface compatible NetFlow à la base de données Orion, soit surveiller une interface déjà existante capable de générer des données NetFlow. Il est nécessaire d'ajouter les dispositifs compatibles NetFlow à la base de données Orion avant de pouvoir les surveiller dans Orion NTA.

Remarque : l'ajout des dispositifs et interfaces Netflow à la base de données Orion et l'ajout des dispositifs et interfaces NetFlow à Orion NTA en tant que sources NetFlow sont des procédures distinctes qui sont détaillées ci-dessous dans des sections différentes.

Ajout de dispositifs et d'interfaces à la base de données Orion

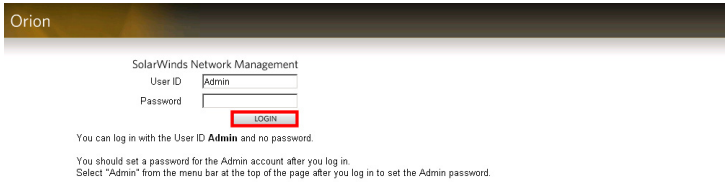
La procédure suivante permet d'ajouter un dispositif et ses interfaces à la base de données Orion grâce à la fonctionnalité Web Node Management d'Orion Web Console. Si le dispositif NetFlow est déjà configuré pour envoyer des données NetFlow, Orion NTA reçoit les premières données NetFlow dès qu'il est ajouté à la base de données Orion.

Remarque : pour plus d'informations sur la désignation des sources NetFlow dans Orion NTA, veuillez consulter « Ajout de sources NetFlow à NetFlow Traffic Analyzer », page 19.

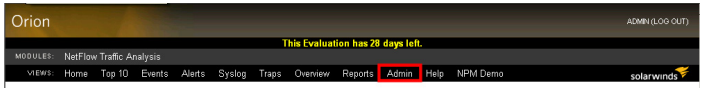
Pour ajouter des périphériques et interfaces- compatibles NetFlow à la base de données Orion :

1. Connectez-vous au serveur Orion NPM qui héberge l'installation de Orion NTA.
2. Cliquez sur **Start > All Programs > SolarWinds Orion > Orion Web Console** (Démarrer > > SolarWinds Orion > Orion Web Console).
3. Identifiez-vous en tant qu'administrateur dans Orion Web Console.

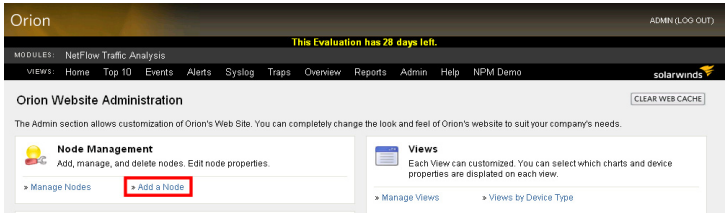
   Remarque : si vous n'avez pas encore configuré d'autre mot de passe d'administration, vous pouvez vous identifier avec **User ID** (Identifiant utilisateur) `Admin`, sans mot de passe.



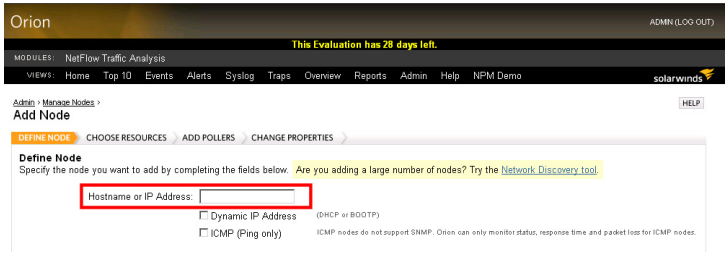
4. Cliquez sur **Admin** sur la barre d'outils Views (Vues).



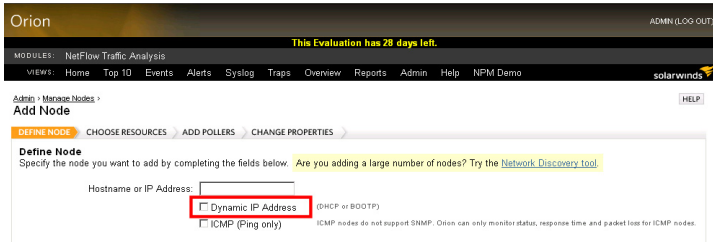
5. Cliquez sur **Add a Node** (Ajouter un nœud) dans le groupe Node Management (Gestion des nœuds).



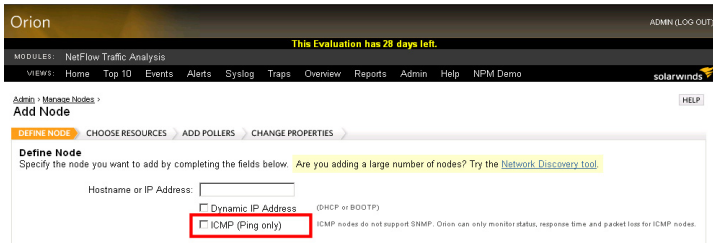
6. Indiquez le nom d'hôte ou l'adresse IP du dispositif compatible Netflow à ajouter dans le champ **Hostname or IP Address** (Nom d'hôte ou adresse IP).



7. ***Si l'adresse IP du dispositif à ajouter est allouée de manière dynamique (DHCP ou BOOTP),*** cochez l'option **Dynamic IP Address** (Adresse IP dynamique).

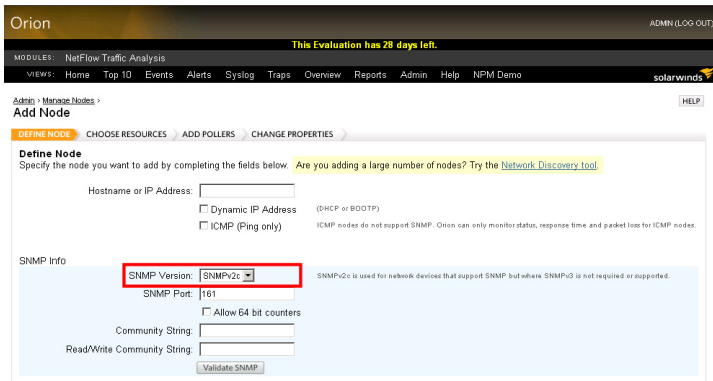


8. Vérifiez que **ICMP (Ping only)** (ICMP 'Ping uniquement') n'est pas coché.



9. Sélectionnez la **SNMP Version** (Version SNMP) pour le nœud ajouté.

   Remarque : Orion NPM utilise par défaut **SNMPv2c**. Si le nouveau dispositif prend en charge ou nécessite des fonctionnalités de sécurité propres à SNMPv3, sélectionnez **SNMPv3.**



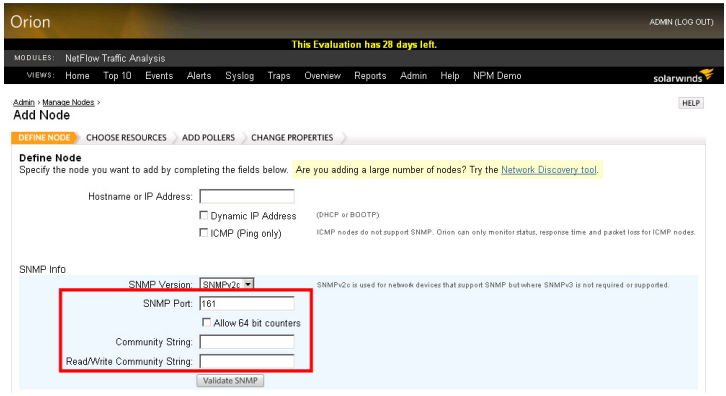
10. ***Si vous avez sélectionné* SNMPv2c,** suivez les étapes ci-dessous :

a. ***Si le port SNMP du nœud ajouté n'est pas le port Orion NMP par défaut (161),*** indiquez le numéro de port réel dans le champ **SNMP Port** (Le port SNMP).

b. ***Si le nœud ajouté prend en charge les compteurs 64 bits,*** cochez **Allow 64 bit counters** (Autoriser les compteurs 64 bits) pour les utiliser.

c. Indiquez les chaînes de communauté pour le nœud ajouté.

Remarque : le paramètre **Read/Write Community String** (Chaîne de communauté de lecture/écriture) est facultatif, mais Orion NPM a besoin au minimum du paramètre de **Community String** (Chaîne de communauté) `public`.



11. ***Si vous avez sélectionné*** **SNMPv3c,** suivez les étapes ci-dessous :

a. ***Si le port SNMP du nœud ajouté n'est pas le port Orion NMP par défaut (161),*** indiquez le numéro de port réel dans le champ **SNMP Port** (Le port SNMP).

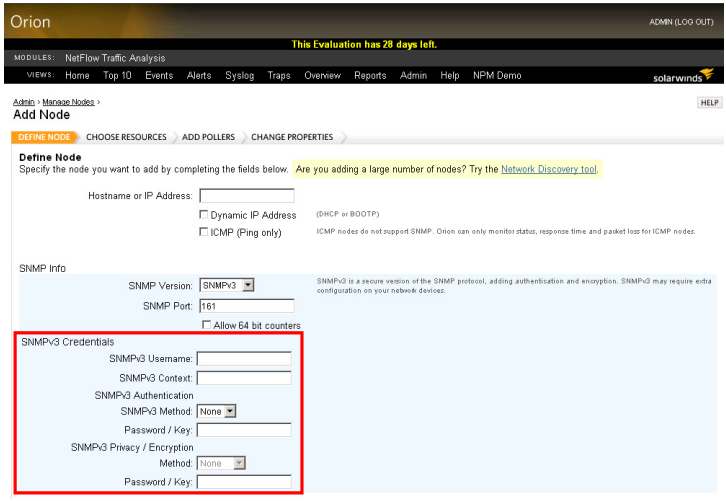
b. ***Si le nœud ajouté prend en charge les compteurs 64 bits,*** cochez **Allow 64 bit counters** (Autoriser les compteurs 64 bits) pour les utiliser.

Remarque : Orion NPM prend totalement en charge l'utilisation des compteurs 64 bits ; cependant, ces compteurs de grande capacité peuvent avoir un comportement erratique en fonction de leur mise en œuvre par le fabricant. Si vous remarquez des résultats particuliers lors de l'utilisation de ces compteurs, utilisez la vue Node Details (Détails du nœud) pour désactiver l'utilisation des compteurs 64 bits pour ce dispositif et prenez contact avec le fabricant du matériel.

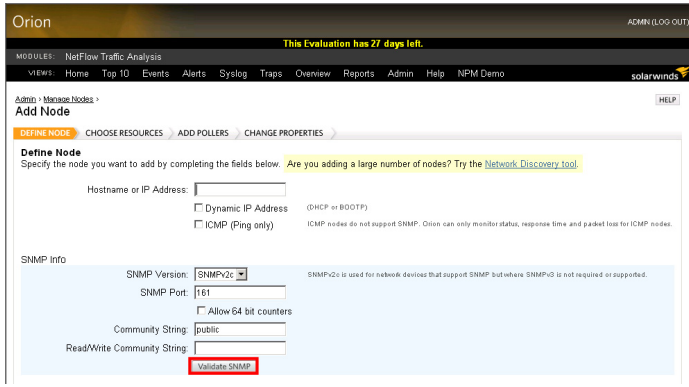
c. Indiquez les paramètres suivants pour **SNMP Credentials** (Informations d'identification), **Authentification** (Authentification) et **Privacy/Encryption** (Confidentialité/Chiffrement) :

- **SNMPv3 Username** (Nom d'utilisateur SNMPv3)
- **SNMPv3 Context** (Contexte SNMPv3)
- **SNMPv3 Authentication Method** (Méthode d'authentification SNMPv3)
- **SNMPv3 Authentication Password/Key** (Mot de passe/Clé d'authentification)
- **SNMPv3 Privacy/Encryption Method** (Méthodes de Confidentialité/ Chiffrement SNMPv3)
- **SNMPv3 Privacy/Encryption Password/Key** (Mot de passe/Clé de Confidentialité/ Chiffrement SNMPv3)

Remarque : les informations d'identification **Read/Write SNMPv3 Credentials** (Informations d'identification SNMPv3 de lecture/écriture) ne sont pas nécessaires pour cette évaluation.



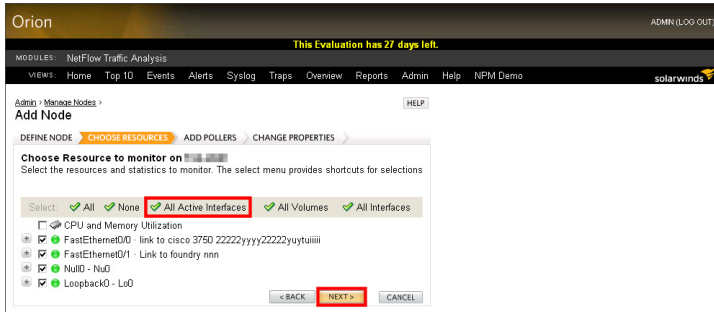
12. Cliquez sur **Validate SNMP** (Valider SNMP) après avoir saisi toutes les informations d'identification SNMP requises.



13. Après avoir vérifié la validité des informations d'identification SNMP, cliquez sur **Next** (Suivant).

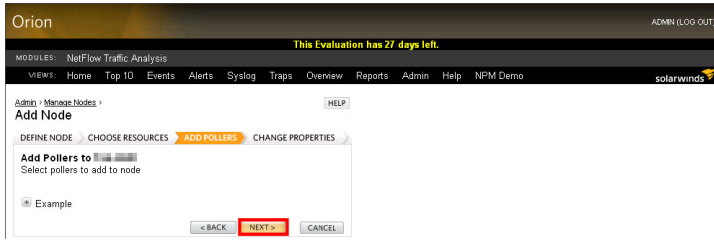
14. Cochez les interfaces à surveiller avec Orion NTA, puis cliquez sur **Next** (Suivant).

Remarque : si vous ignorez quelles sont les interfaces compatibles NetFlow, cliquez sur **All Interfaces** (Toutes les interfaces) pour sélectionner toutes les interfaces.

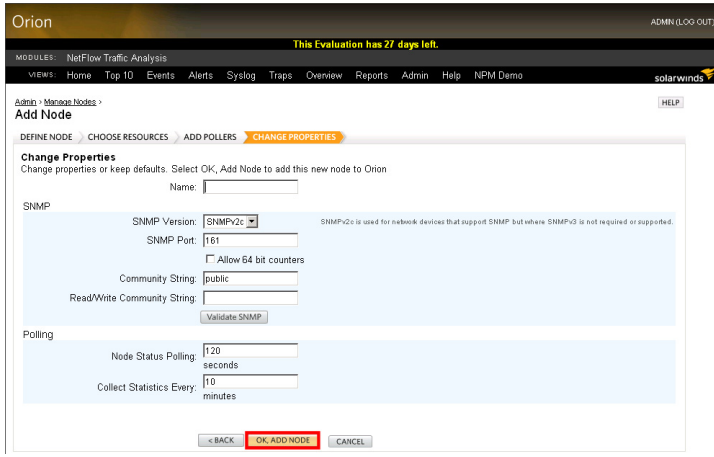


15. Pour cette évaluation, cliquez sur **Next** (Suivant) dans la vue Add Pollers (Ajouter des enquêteurs).

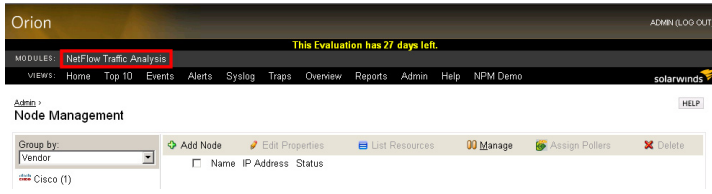
Remarque : pour plus d'informations sur l'utilisation ou la définition des pollers (enquêteurs), veuillez consulter le manuel *SolarWinds Orion Network Performance Monitor Administrator Guide*.



16. Cliquez sur **OK, Add Node** (OK, ajouter un nœud) dans la vue Change Properties (Modification des propriétés).



17. Cliquez sur **NetFlow Traffic Analysis** (Analyse du trafic NetFlow) sur la barre d'outils Modules.



La section suivante décrit les étapes permettant de recevoir les données NetFlow depuis les dispositifs compatibles NetFlow du réseau.

Ajout de sources NetFlow à NetFlow Traffic Analyzer

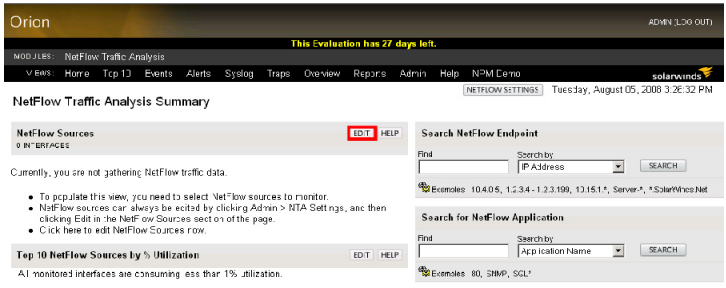
Après l'ajout du dispositif compatible NetFlow et de ses interfaces à Orion NPM, vous devez le désigner comme source NetFlow. La procédure suivante décrit les étapes requises pour ajouter des sources NetFlow à Orion NTA.

Remarque : Orion NTA ne reconnaît que les modèles NetFlow version 9 incluant tous les champs utilisés par NetFlow version 5.

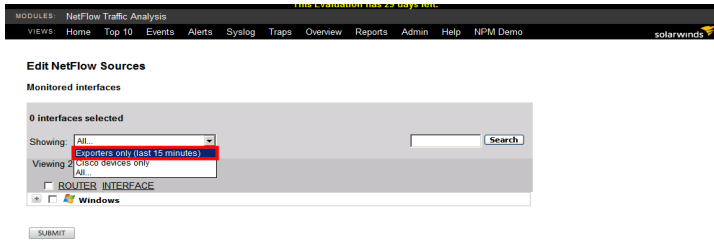
Pour ajouter des dispositifs et interfaces Netflow à NetFlow Traffic Analyzer :

1. Identifiez-vous sur le serveur Orion NPM qui héberge NetFlow Traffic Analyzer.
2. Cliquez sur **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Démarrer > Tous les programmes > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console).
3. Identifiez-vous en tant qu'administrateur dans Orion Web Console.

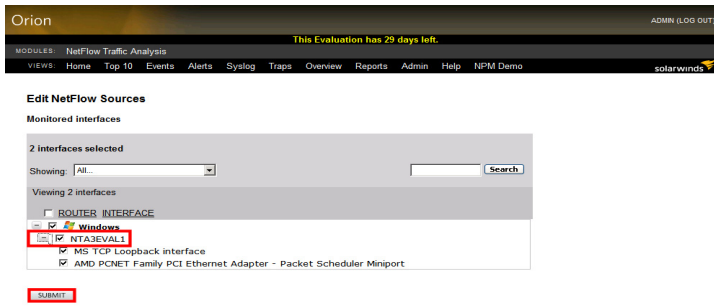
   Remarque : si vous n'avez pas encore configuré d'autre mot de passe d'administration, vous pouvez vous identifier avec **User ID** (Identifiant utilisateur) `Admin`, sans mot de passe.
4. Cliquez sur **Edit** (Modifier) dans l'en-tête de la ressource NetFlow Sources (Sources NetFlow).



5. Sélectionnez **Exporters Only (last 15 minutes)** (Exportateurs uniquement ‘15 dernières minutes’) dans le menu Showing (Affichage).



6. Développez la liste des dispositifs pour afficher tous les nœuds surveillés, cochez le nœud parent des interfaces à surveiller avec Orion NTA, puis cliquez sur **Submit** (Envoyer).



En réponse, Orion NTA doit alors recevoir des données compréhensibles sur le trafic et les afficher dans Orion Web Console dans les quelques minutes qui suivent.

Chapitre 3

Présentation rapide de Orion NetFlow Traffic Analyzer

Les fonctionnalités et la flexibilité de Orion NetFlow Traffic Analyzer permettent de disposer d'informations très détaillées sur le volume et la qualité du trafic du réseau. Les sections de ce chapitre indiquent comment utiliser certaines fonctionnalités importantes de Orion NetFlow Traffic Analyzer et doivent être parcourues dans l'ordre de ce manuel Ce chapitre est le plus utile lorsqu'on le lit d'un bout à l'autre ; il commence par un aperçu des ressources immédiatement disponibles dans la vue résumée NetFlow Traffic Analysis Summary, et se poursuit avec la description sommaire des vues de Orion NTA les plus utilisées.

Remarque : le dernier chapitre de cet Evaluation Guide inclut des études de cas détaillées, y compris des scénarios mettant en œuvre d'autres outils SolarWinds. Pour plus d'informations, veuillez consulter « Utilisation de Orion NetFlow Traffic Analyzer », page 41.

Lancement de Orion NetFlow Traffic Analyzer

Pour démarrer Orion NetFlow Traffic Analyzer, Cliquez sur **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Démarrer > Tous les programmes > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console). Pour plus d'informations sur l'installation et la configuration de Orion NTA, veuillez consulter « Installation de Orion NetFlow Traffic Analyzer », page 5.

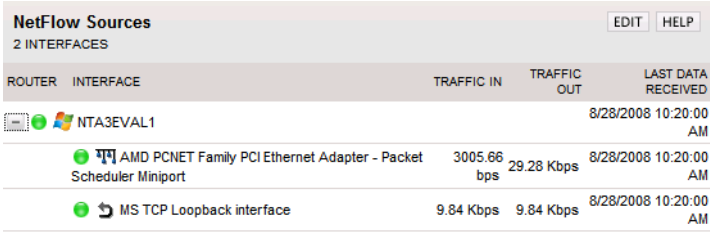
Vue NetFlow Traffic Analysis Summary

La vue NetFlow Traffic Analysis Summary (Résumé de l'analyse du trafic NetFlow) est la première à s'afficher au démarrage de Orion NetFlow Traffic Analyzer. Cette vue offre un aperçu des conditions du trafic de données sur la totalité du réseau. La vue NetFlow Traffic Analysis Summary inclut par défaut les ressources suivantes.

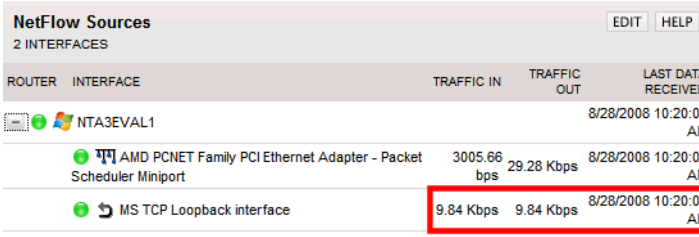
NetFlow Sources (Sources NetFlow)

Cette ressource répertorie tous les dispositifs compatibles NetFlow du réseau actuellement configurés pour envoyer des données NetFlow au serveur qui héberge l'installation de Orion NTA. Pour plus d'informations sur l'ajout de dispositifs compatibles NetFlow, veuillez consulter « Activation de l'analyse du trafic NetFlow », page 12.

Cliquez sur **+** en regard du nom de chaque routeur pour afficher les interfaces compatibles NetFlow activées sur le routeur sélectionné.



Les interfaces sont également répertoriées avec une icône d'état et l'heure et la date de réception par Orion NTA des dernières données NetFlow en provenance de l'interface sélectionnée. De plus, la ressource NetFlow Sources indique les valeurs du trafic entrant et sortant sur chaque interface.

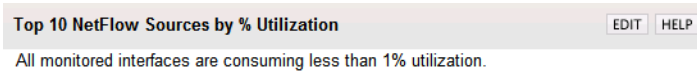


Cliquez sur le nom d'un routeur pour ouvrir la vue Netflow Node Details (Détails du nœud NetFlow) ; cliquez sur le nom d'une interface pour ouvrir la vue NetFlow Interface Details (Détails de l'interface NetFlow). Pour plus d'informations sur la vue NetFlow Node Details, veuillez consulter « Vue NetFlow Node Details », page 37. Pour plus d'informations sur la vue NetFlow Interface Details, veuillez consulter « Vue NetFlow Interface Details », page 36.

Top 10 NetFlow Sources by % Utilization (Dix principales sources NetFlow par pourcentage d'utilisation)

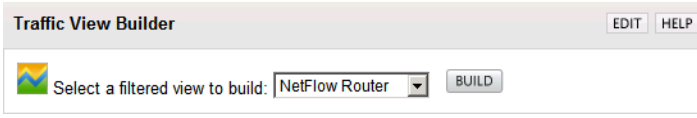
Cette ressource répertorie les sources NetFlow du réseau qui acheminent actuellement assez de trafic pour consommer beaucoup de ressources système.

Remarque : les sources ne sont répertoriées que si leur pourcentage d'utilisation dépasse 1 %.



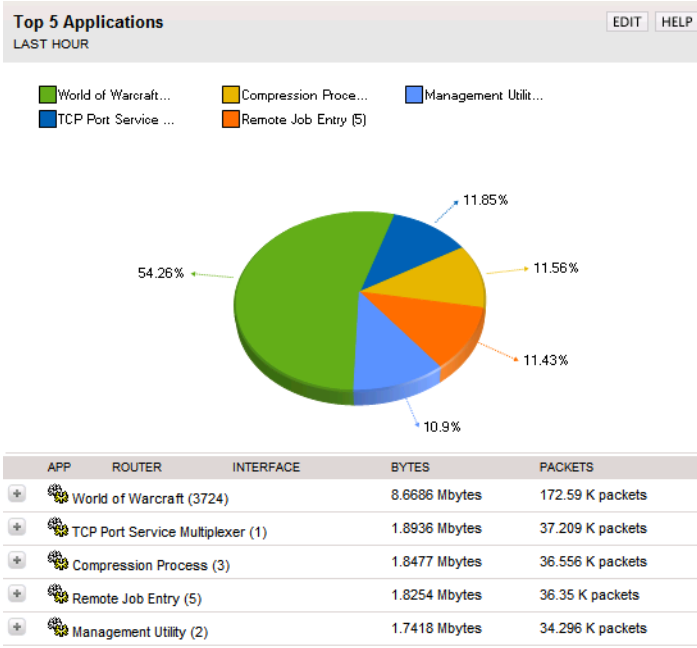
Traffic View Builder (Constructeur de vues du trafic)

L'application Traffic View Builder permet de créer ses propres vues Orion NTA personnalisées. Orion NTA étant un module à interface Web, il est possible de créer un signet de navigateur pour n'importe quelle vue Orion NTA afin de revenir ultérieurement vérifier les points à problèmes potentiels. Pour plus d'informations sur Traffic View Builder, veuillez consulter « Utilisation de Traffic View Builder », page 41.



Top 5 Applications (Cinq principales applications)

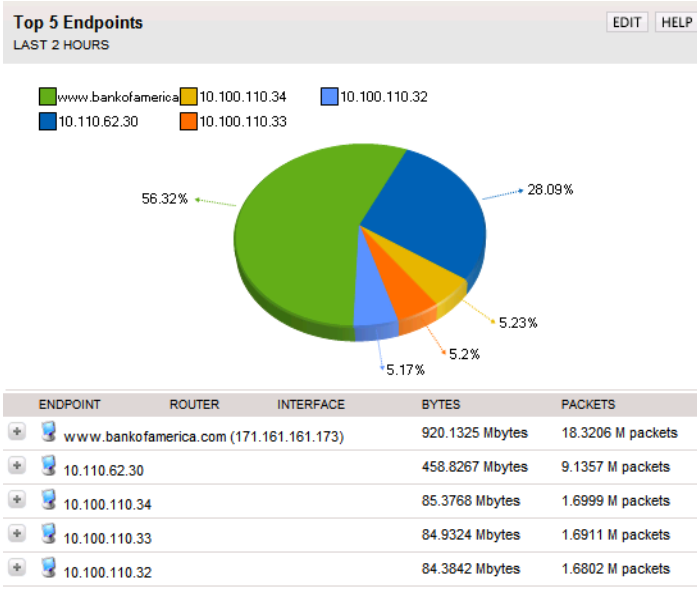
Cette ressource offre un instantané des applications et des ports les plus utilisés par les dispositifs en réseau. Cliquez sur **+** pour développer chaque application et afficher les dispositifs du réseau qui acheminent le trafic lui appartenant.



APP	ROUTER	INTERFACE	BYTES	PACKETS
World of Warcraft (3724)			8.6686 Mbytes	172.59 K packets
TCP Port Service Multiplexer (1)			1.8936 Mbytes	37.209 K packets
Compression Process (3)			1.8477 Mbytes	36.556 K packets
Remote Job Entry (5)			1.8254 Mbytes	36.35 K packets
Management Utility (2)			1.7418 Mbytes	34.296 K packets

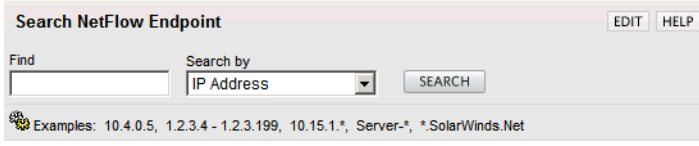
Top 5 Endpoints (Cinq principaux points de terminaison)

Cette ressource offre un instantané des points de terminaison qui sont la source ou la cible du plus gros volume de trafic sur le réseau. Cliquez sur **+** pour développer chaque point de terminaison, vous verrez alors les dispositifs en réseau qui acheminent le trafic pour chaque point de terminaison.



Search for NetFlow Endpoints (Recherche des points de terminaison NetFlow)

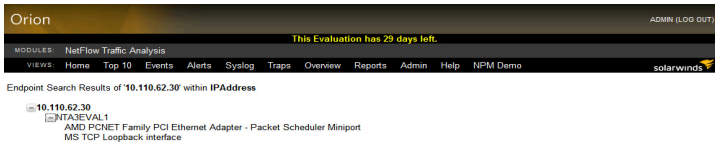
Cette ressource permet de repérer rapidement tout point de terminaison communiquant avec tout dispositif du réseau.



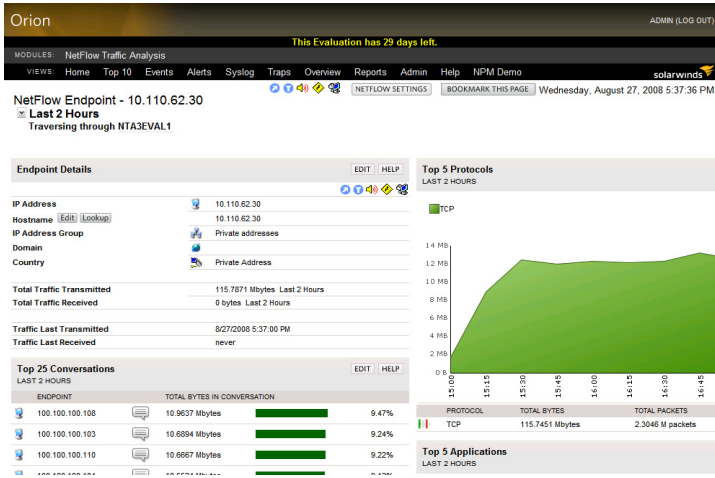
Il suffit de rechercher les points de terminaison en utilisant l'un des critères du tableau suivant :

Critères de recherche des points de terminaison NetFlow		
Country (Pays)	Domain (Domaine)	Hostname (Nom d'hôte)
IP Address (Adresse IP)	IP Address Groupe Name (Nom de groupe d'adresses IP)	

Indiquez un terme de recherche approprié, puis cliquez sur **Search** (Rechercher). Les résultats de la recherche s'affichent sous la forme d'une liste développable de dispositifs en réseau qui acheminent le trafic en direction ou en provenance du point de terminaison recherché.

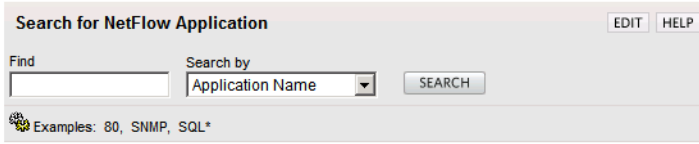


Cliquez sur le nom de l'un des dispositifs du réseau pour ouvrir la vue NetFlow Endpoint (Point de terminaison NetFlow) et voir tout le trafic du point de terminaison passant par le dispositif sélectionné. Pour plus d'informations sur la vue NetFlow Endpoint, veuillez consulter « Vue NetFlow Endpoint », page 33.

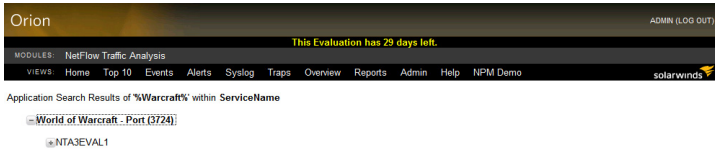


Search for NetFlow Application (Recherche d'application Netflow)

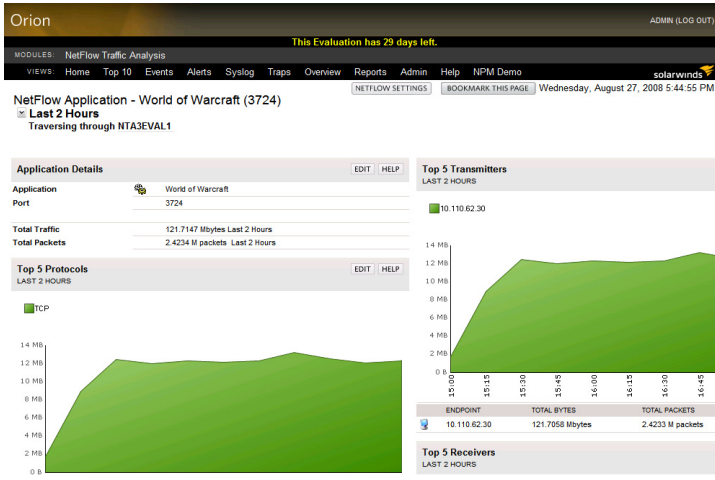
Cette ressource permet d'afficher rapidement les dispositifs du réseau qui utilisent une application ou un port spécifique à tout moment. Il suffit de sélectionner la recherche par nom d'application (Application Name) ou par port, de fournir un nom d'application ou un numéro de port approprié, puis de cliquer sur **Search** (Rechercher).



Les résultats de la recherche s'affichent sous la forme d'une liste développable de dispositifs en réseau qui acheminent le trafic à destination de l'application sélectionnée ou par le port sélectionné.

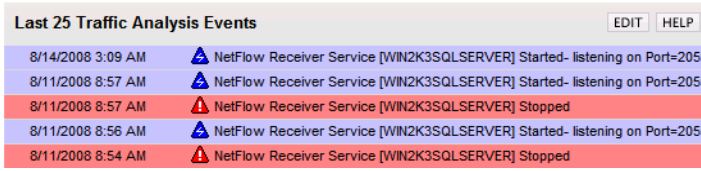


Cliquez sur le nom d'un dispositif du réseau pour ouvrir la vue NetFlow Application (Application NetFlow) et voir tout le trafic passant par le dispositif sélectionné à destination de l'application recherchée ou acheminé par le port recherché. Pour plus d'informations sur la vue NetFlow Application, veuillez consulter « Vue NetFlow Application », page 30.



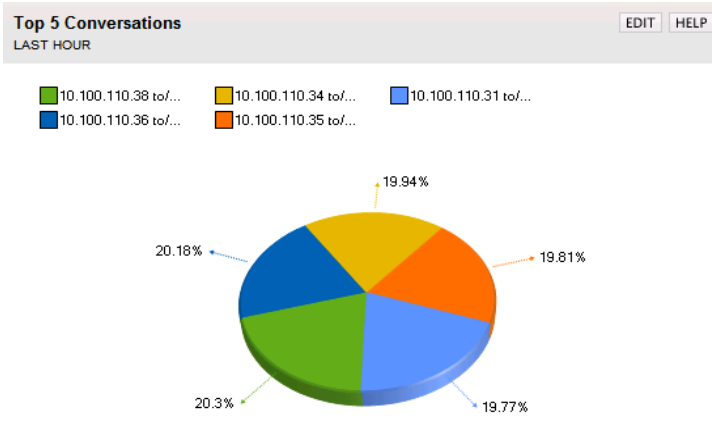
Last 25 Traffic Analysis Events (Vingt-cinq derniers événements d'analyse du trafic)

Cette ressource répertorie les 25 derniers événements spécifiques à NetFlow survenus sur les dispositifs du réseau surveillé. Elle répertorie habituellement la date et l'heure de démarrage et d'arrêt du service NetFlow Receiver (Récepteur NetFlow).



Top 5 Conversations (Cinq principales conversations)

Cette ressource offre un instantané, avec tableau et diagramme, des conversations qui utilisent le plus de bande passante sur le réseau. Chaque couleur du diagramme correspond à une conversation continue unique entre deux points de terminaison spécifiques. Le tableau situé sous le diagramme répertorie les points de terminaison participant à chaque conversation, ainsi que la bande passante consommée par chaque conversation, exprimée à la fois en octets et en paquets. Cliquez sur **+** pour développer la description de la conversation et afficher tous les dispositifs du réseau par lesquels passe la conversion sélectionnée. Le premier niveau de développement affiche les nœuds du réseau par lesquels la conversation est acheminée. Le niveau suivant affiche les interfaces qui relaient le trafic de la conversation sélectionnée.

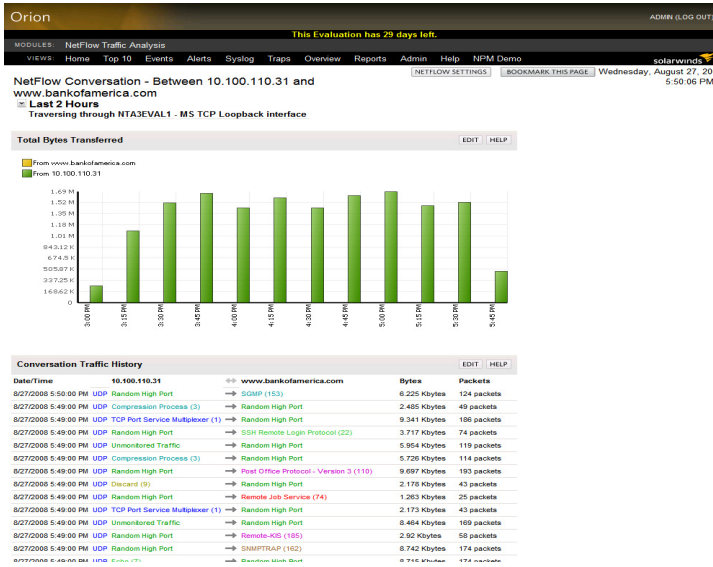


CONVERSATION ROUTER INTERFACE	BYTES	PACKETS
+ Between 10.100.110.38 and www.bankofamerica.com (171.161.161.173)	8.3817 Mbytes	166.891 K packets
+ Between 10.100.110.36 and www.bankofamerica.com (171.161.161.173)	8.3306 Mbytes	165.879 K packets
+ Between 10.100.110.34 and www.bankofamerica.com (171.161.161.173)	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

La part respective de bande passante totale consommée par la conversation sélectionnée est affichée en octets et en paquets aux deux niveaux du nœud et

de l'interface. Le trafic de la conversation sur chaque nœud est égal à la somme du trafic de la conversation sur toutes les interfaces de ce nœud.

Cliquez sur le nom d'un dispositif du réseau pour ouvrir la vue NetFlow Conversation (Conversation NetFlow) pour tout le trafic entre les deux points de terminaison en conversation passant par le dispositif sélectionné. Pour plus d'informations, veuillez consulter « Vue NetFlow Conversation », page 33.



Orion NetFlow Traffic Analyzer Vues

Les sections suivantes détaillent le type d'informations disponibles par défaut sur les vues Orion NTA sélectionnées.

Remarques :

- Voici quelques-unes des vues Orion NTA les plus utilisées. Elles sont directement accessibles à partir des ressources par défaut de la vue NetFlow Traffic Analysis Summary (Résumé de l'analyse du trafic NetFlow). D'autres ressources conduisent à des vues supplémentaires. Pour plus d'informations, veuillez consulter « Viewing NetFlow Traffic Analyzer Data in the Orion Web Console » dans le manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.
- Il se peut que certaines ressources soient absentes de la configuration par défaut d'une vue sélectionnée. Pour afficher toutes les ressources disponibles, modifiez la vue à partir de l'écran Admin d'Orion NPM Web

Console. Pour plus d'informations, veuillez consulter « Viewing NetFlow Traffic Analyzer Data in the Orion Web Console » dans le manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Vue NetFlow Application

Les sections suivantes offrent une courte description des ressources disponibles sur la vue NetFlow Application (Application NetFlow). D'autres informations sur chaque ressource, y compris les détails de la configuration, sont accessibles en cliquant sur **Help** (Aide) dans la barre de titre de la ressource.

Application Details (Détails de l'application)

Cette ressource affiche un tableau des informations suivantes sur l'application et le port actuellement sélectionnés :

- Nom de l'application
- Port utilisé par l'application
- Volume total de données du trafic au cours de la période sélectionnée
- Nombre total de paquets envoyés au cours de la période sélectionnée

Top 5 Protocols (Cinq principaux protocoles)

Cette ressource offre un instantané des protocoles de trafic les plus utilisés par l'application. Le tableau situé sous le diagramme indique le type de protocole, le volume de données, le nombre total de paquets et le pourcentage du trafic total utilisant ce protocole.

Top 5 Types of Service (Cinq principaux types de service)

Cette ressource offre un instantané sous forme de diagramme des services les plus actifs utilisés par l'application sélectionnée. Le tableau situé sous le diagramme fournit les informations suivantes sur chaque type de service :

- Type de service
- Volume de trafic géré par le service
- Nombre de paquets gérés par le service

- Pourcentage du trafic total en direction de l'application sélectionnée géré par ce type de service

Total Bytes Transferred (Nombre total d'octets transférés)

Cette ressource affiche un diagramme qui détaille le nombre total d'octets transférés par l'application sélectionnée pendant une période donnée. Un grand

choix de diagrammes personnalisés permettent l'impression ou l'exportation aux fins d'archivage. Cliquez sur le diagramme pour ouvrir la page Customize Chart (Personnaliser le diagramme) correspondante. Pour plus d'informations sur la personnalisation des diagrammes, veuillez consulter la section « Customizing Charts in NetFlow Traffic Analyzer » du manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Unique Visitors (Visiteurs uniques)

Cette ressource affiche un diagramme détaillant le nombre d'adresses IP uniques qui ont utilisé l'application sélectionnée pendant une période donnée. Un grand choix de diagrammes personnalisés permettent l'impression ou l'exportation aux fins d'archivage. Cliquez sur le diagramme pour ouvrir la page Customize Chart (Personnaliser le diagramme) correspondante. Pour plus d'informations sur la personnalisation des diagrammes, veuillez consulter la section « Customizing Charts in NetFlow Traffic Analyzer » du manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Total Packets Transferred (Nombre total de paquets transférés)

Cette ressource affiche un diagramme qui détaille le nombre total de paquets transférés par l'application sélectionnée pendant une période donnée. Un grand choix de diagrammes personnalisés permettent l'impression ou l'exportation aux fins d'archivage. Cliquez sur le diagramme pour ouvrir la page Customize Chart (Personnaliser le diagramme) correspondante. Pour plus d'informations sur la personnalisation des diagrammes, veuillez consulter la section « Customizing Charts in NetFlow Traffic Analyzer » du manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Top 5 Transmitters (Cinq principaux émetteurs)

Cette ressource offre un instantané, sous forme de diagramme, des points de terminaison les plus actifs quant à l'envoi de données qui utilisent l'application sélectionnée. Le tableau situé sous le diagramme fournit les informations suivantes sur chaque point de terminaison :

- Le nom ou l'adresse IP du point de terminaison
- Le volume de trafic émis depuis le point de terminaison
- Le pourcentage du total de trafic émis qui peut être « tracé » vers le point de terminaison

Cliquez sur un point de terminaison de la liste pour ouvrir la vue NetFlow Endpoint (Point de terminaison Netflow) qui présente des statistiques similaires pour chaque point de terminaison émetteur. Pour plus d'informations, veuillez consulter « Vue NetFlow Endpoint », page 33.

Top 5 Receivers (Cinq principaux récepteurs)

Cette ressource offre un instantané, sous forme de diagramme, des points de terminaison les plus actifs quant à la réception de données qui utilisent l'application sélectionnée. Le tableau situé sous le diagramme fournit les informations suivantes sur chaque point de terminaison :

- Le nom ou l'adresse IP du point de terminaison
- Le volume de trafic reçu par le point de terminaison
- Le pourcentage du total de trafic reçu qui peut être « tracé » vers le point de terminaison

Cliquez sur un point de terminaison de la liste pour ouvrir la vue NetFlow Endpoint (Point de terminaison NetFlow) qui présente des statistiques similaires pour chaque point de terminaison récepteur. Pour plus d'informations, veuillez consulter « Vue NetFlow Endpoint », page 33.

Top 5 Traffic Sources by Country (Cinq principales sources de trafic par pays)

Cette ressource offre un instantané, sous forme de diagramme, des pays d'où provient le trafic sur l'application sélectionnée, par ordre de pourcentage du trafic total sur cette application. Le tableau situé sous le diagramme fournit les informations suivantes sur chaque pays :

- Le nom du pays
- Le volume du trafic émanant du pays
- Le pourcentage du total de trafic reçu qui peut être « tracé » vers le pays

Top 5 Traffic Destinations by Country (Cinq principales destinations du trafic par pays)

Cette ressource offre un instantané, sous forme de diagramme, des pays vers lequels est dirigé le trafic sur l'application sélectionnée, par ordre de pourcentage du trafic total sur cette application. Le tableau situé sous le diagramme fournit les informations suivantes sur chaque pays :

- Le nom du pays
- Le volume du trafic total sur l'application qui est acheminé vers les points de terminaisons de ce pays
- Le pourcentage du total de trafic émis qui peut être « tracé » vers le pays.

Top 5 Conversations (Cinq principales conversations)

Cette ressource répertorie les conversations les plus gourmandes en bande passante acheminées au travers du dispositif sélectionné en utilisant l'application sélectionnée. Les conversations figurent avec le volume des données transférées, exprimé en octets et en paquets, et le pourcentage du trafic total sur l'application généré par la conversation. Cliquez sur une conversation pour ouvrir la vue Netflow Conversation (Conversation NetFlow) correspondante. Pour plus d'informations, veuillez consulter « Vue NetFlow Conversation », page 33.

Vue NetFlow Conversation

Les sections suivantes offrent une courte description des ressources disponibles sur la vue NetFlow Conversation (Conversation NetFlow). D'autres informations sur chaque ressource, y compris les détails de la configuration, sont accessibles en cliquant sur **Help** (Aide) dans la barre de titre de la ressource.

Total Bytes Transferred (Nombre total d'octets transférés)

Cette ressource affiche un diagramme détaillant le nombre total d'octets transférés pendant une période donnée entre les deux nœuds, adresses IP ou domaines indiqués dans le titre de la vue.

Conversation Traffic History (Historique du trafic des conversations)

Cette ressource affiche un tableau résumant les informations suivantes pour chaque échange de conversation de la liste :

- L'horodatage de l'échange
- Le protocole utilisé par l'échange
- L'application et le port utilisés par l'échange
- Le sens du flux de trafic
- Le volume de trafic exprimé en octets
- Le nombre équivalent de paquets envoyés

Vue NetFlow Endpoint

Les sections suivantes offrent une courte description des ressources disponibles sur la vue NetFlow Endpoint (Point de terminaison NetFlow). D'autres informations sur chaque ressource, y compris les détails de la configuration, sont accessibles en cliquant sur **Help** (Aide) dans la barre de titre de la ressource.

Endpoint Details (Détails du point de terminaison)

Cette ressource offre les informations suivantes sur un point de terminaison sélectionné :

- Adresse IP
- Nom d'hôte
- Groupe d'adresses IP
- Domaine
- Pays
- Trafic total émis et reçu
- Horodatage des dernières données émises et reçues-

Top 5 Conversations (Cinq principales conversations)

Cette ressource répertorie les points de terminaison avec lesquels le point de terminaison actuellement affiché a échangé le plus de données. Elle indique le volume de données transférées au cours de la conversation et le pourcentage que représente cette conversation par rapport au total des données transférées par le point de terminaison affiché. Cliquez sur un point de terminaison pour ouvrir la vue NetFlow Endpoint correspondante. Tous les autres liens concernant un point de terminaison de la liste ouvrent la vue NetFlow Conversation (Conversation NetFlow) pour la conversation entre les points de terminaison affichés et sélectionnés. Pour plus d'informations, veuillez consulter « Vue NetFlow Conversation », page 33.

Total Packets Transferred (Nombre total de paquets transférés)

Cette ressource affiche un diagramme du nombre total de paquets émis et reçus par le point de terminaison affiché pendant une période donnée.

Total Bytes Transferred (Nombre total d'octets transférés)

Cette ressource affiche un diagramme du nombre total d'octets émis et reçus par le point de terminaison affiché pendant une période donnée.

Top 5 Protocols (Cinq principaux protocoles)

Cette ressource offre un instantané des protocoles de trafic les plus utilisés par le point de terminaison. Le tableau situé sous le diagramme indique le type de protocole, le volume de données, le nombre total de paquets et le pourcentage du trafic total utilisant ce protocole.

Top 5 Applications (Cinq principales applications)

Cette ressource offre un instantané des applications les plus utilisées par le point de terminaison sélectionné. Le tableau situé sous le diagramme indique le nom de l'application, la quantité de données qu'elle met en circulation, le nombre total équivalent de paquets et le pourcentage du trafic total pouvant être « tracé » vers l'application de la liste par le point de terminaison sélectionné. Cliquez sur une application pour ouvrir la vue NetFlow Application (Application NetFlow). Pour plus d'informations, veuillez consulter « Vue NetFlow Application », page 30.

Top 5 Traffic Sources by Country (Cinq principales sources de trafic par pays)

Cette ressource offre un instantané, sous forme de diagramme, des pays d'où provient le trafic vers le point de terminaison sélectionné, par ordre de pourcentage du trafic total sur ce point de terminaison. Le tableau situé sous le diagramme indique le nom du pays émetteur du trafic vers le point de terminaison affiché, le volume de trafic acheminé vers ce point de terminaison depuis le pays de la liste et le pourcentage du trafic total acheminé vers le point de terminaison affiché pouvant être « tracé » vers ce pays.

Top 5 Traffic Destinations by Country (Cinq principales destinations du trafic par pays)

Cette ressource offre un diagramme et un tableau des pays hébergeant les destinations du trafic émanant du point de terminaison sélectionné, classés par pourcentage du trafic total émanant de ce point de terminaison. Le tableau situé sous le diagramme indique le nom du pays vers lequel le trafic est acheminé, le volume du trafic acheminé vers les serveurs du pays de la liste et le pourcentage de la totalité du trafic acheminé à partir du point de terminaison affiché en direction des serveurs de ce pays.

Unique Visitors (Visiteurs uniques)

Cette ressource offre un diagramme des adresses IP uniques qui ont communiqué avec le point de terminaison affiché pendant une période donnée.

Top 5 Types of Service (Cinq principaux types de service)

Cette ressource offre un instantané des services les plus utilisés par le point de terminaison sélectionné. Le tableau situé sous le diagramme fournit les informations suivantes sur chaque type de service :

- Type de service
- Volume du trafic, en octets et en paquets, géré par le service
- Pourcentage du trafic total en direction du point de terminaison sélectionné géré par ce type de service

Pour plus d'informations sur la surveillance du type de service dans Orion NTA, veuillez consulter « Configuring NetFlow Types of Services » dans le manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Vue NetFlow Interface Details

Les sections suivantes offrent une courte description des ressources disponibles sur la vue NetFlow Interface Details (Détails de l'interface NetFlow). D'autres informations sur chaque ressource, y compris les détails de la configuration, sont accessibles en cliquant sur **Help** (Aide) dans la barre de titre de la ressource.

Top 5 Protocols

Cette ressource offre un instantané (Aide) des protocoles de trafic les plus vus par l'interface affichée. Le tableau situé sous le diagramme indique le type de protocole, le volume de données, le nombre total de paquets et le pourcentage du trafic total utilisant ce protocole sur l'interface affichée.

Top 5 Endpoints (Cinq principaux points de terminaison)

Cette ressource affiche un diagramme et un tableau des points de terminaison émettant le plus de trafic sur l'interface sélectionnée. Le tableau situé sous le diagramme indique le nom ou l'adresse IP de chaque point de terminaison de la liste, le volume de trafic émis par chaque point de terminaison, exprimé en octets et en paquets, et le pourcentage du trafic total sur l'interface affichée qui peut être « tracé » jusqu'à chaque point de terminaison de la liste. Cliquez sur un point de terminaison pour ouvrir la vue NetFlow Endpoint (Points de terminaison NetFlow) correspondante. Pour plus d'informations, veuillez consulter « Vue NetFlow Endpoint », page 33.

Top 5 Applications (Cinq principales applications)

Cette ressource offre un instantané des applications les plus utilisées par l'interface affichée. Le tableau situé sous le diagramme indique le nom de l'application, la quantité de données qu'elle met en circulation, le nombre total équivalent de paquets et le pourcentage du trafic total pouvant être « tracé » vers l'application de la liste par l'interface affichée. Cliquez sur une application pour ouvrir la vue NetFlow Application (Application NetFlow). Pour plus d'informations, veuillez consulter « Vue NetFlow Application », page 30.

Top 5 Domains (Cinq principaux domaines)

Cette ressource offre un instantané des domaines qui émettent le plus de trafic sur l'interface sélectionnée. Le tableau situé sous le diagramme indique le nom du domaine, le volume du trafic en octets, le nombre total de paquets envoyés et le pourcentage du trafic total sur l'interface sélectionnée qui peut être « tracé » vers chaque domaine.

Top 5 Types of Service (Cinq principaux types de service)

Cette ressource offre un instantané des services les plus utilisés par l'interface sélectionnée. Le tableau situé sous le diagramme fournit les informations suivantes sur chaque type de service :

- Type de service
- Volume du trafic, en octets et en paquets, géré par le service sur l'interface affichée.
- Pourcentage du trafic total sur l'interface affichée géré par ce type de service

Pour plus d'informations sur la surveillance du type de service dans Orion NTA, veuillez consulter « Configuring NetFlow Types of Services » dans le manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Top 5 Conversations (Cinq principales conversations)

Cette ressource affiche la liste des conversations qui créent le plus de trafic sur l'interface affichée. Elle indique le volume de données transférées au cours de la conversation et le pourcentage que représente cette conversation par rapport au total des données transférées sur l'interface affichée. Cliquez sur une conversation pour ouvrir la vue Netflow Conversation correspondante. Pour plus d'informations, veuillez consulter « Vue NetFlow Conversation », page 33.

Vue NetFlow Node Details

Les sections suivantes offrent une courte description des ressources disponibles sur la vue NetFlow Node Details (Détails du nœud NetFlow). D'autres informations sur chaque ressource, y compris les détails de la configuration, sont accessibles en cliquant sur **Help** (Aide) dans la barre de titre de la ressource.

Top 5 Protocols (Cinq principaux protocoles)

Cette ressource offre un instantané des protocoles de trafic les plus utilisés par le nœud affiché. Le tableau situé sous le diagramme indique le type de protocole, le volume de données, le nombre total de paquets et le pourcentage du trafic total utilisant chaque protocole sur le nœud affiché.

Top 5 Applications (Cinq principales applications)

Cette ressource offre un instantané des applications les plus utilisées par le nœud affiché. Le tableau situé sous le diagramme indique le nom de l'application, la quantité de données qu'elle met en circulation, le nombre total équivalent de paquets et le pourcentage du trafic total pouvant être « tracé » vers l'application de la liste par le nœud affiché. Cliquez sur une application pour ouvrir la vue NetFlow Application (Application NetFlow). Pour plus d'informations, veuillez consulter « Vue NetFlow Application », page 30.

Top 5 Conversations (Cinq principales conversations)

Cette ressource affiche la liste des conversations qui créent le plus de trafic sur le nœud affiché. Elle indique le volume de données transférées au cours de la conversation et le pourcentage que représente cette conversation par rapport au total des données transférées sur le nœud affiché. Cliquez sur une conversation pour ouvrir la vue Netflow Conversation (Conversation NetFlow) correspondante. Pour plus d'informations, veuillez consulter « Vue NetFlow Conversation », page 33.

Top 5 Endpoints (Cinq principaux points de terminaison)

Cette ressource affiche un diagramme et un tableau des points de terminaison émettant le plus de trafic sur le nœud affiché. Le tableau situé sous le diagramme indique le nom ou l'adresse IP de chaque point de terminaison de la liste, le volume de trafic émis par chaque point de terminaison, exprimé en octets et en paquets, et le pourcentage du trafic total sur le nœud affiché qui peut être « tracé » jusqu'à chaque point de terminaison de la liste. Cliquez sur un point de terminaison pour ouvrir la vue NetFlow Endpoint (Point de terminaison NetFlow) correspondante. Pour plus d'informations, veuillez consulter « Vue NetFlow Endpoint », page 33.

Top 5 Domains (Cinq principaux domaines)

Cette ressource offre un instantané des domaines qui émettent le plus de trafic sur le nœud affiché. Le tableau situé sous le diagramme indique le nom du domaine, le volume du trafic en octets, le nombre total de paquets envoyés et le pourcentage du trafic total sur le nœud affiché qui peut être « tracé » vers chaque domaine.

Node Interfaces (Interfaces du nœud)

Cette ressource répertorie toutes les interfaces surveillées sur le nœud affiché. Le trafic entrant et sortant y figure pour chaque interface. Cliquez sur une interface pour ouvrir la vue NetFlow Interface Details (Détails de l'interface NetFlow) correspondante. Pour plus d'informations, veuillez consulter « Vue NetFlow Interface Details », page 36.

Chapitre 4

Utilisation de Orion NetFlow Traffic Analyzer

Tandis qu'Orion Network Performance Monitor peut indiquer l'utilisation qui est faite de la bande passante sur une interface donnée, Orion NetFlow Traffic Analyzer pousse un peu plus loin cette capacité en offrant des informations supplémentaires sur l'utilisateur réel de cette bande passante et les applications utilisées. Les scénarios décrits dans ce chapitre illustrent la valeur de Orion NetFlow Traffic Analyzer et en quoi il peut représenter un important retour immédiat sur investissement.

Utilisation de Traffic View Builder

La ressource Traffic View Builder (Constructeur de vues du trafic) permet de générer rapidement des vues personnalisées pour tout dispositif compatible NetFlow. Traffic View Builder permet de créer votre propre version de n'importe laquelle des vues du tableau suivant.

Types de vues de Traffic View Builder		
Application	Pays	Domaine
Point de terminaison	Interface	Groupe d'adresses IP
Protocole	Routeur	Type de service

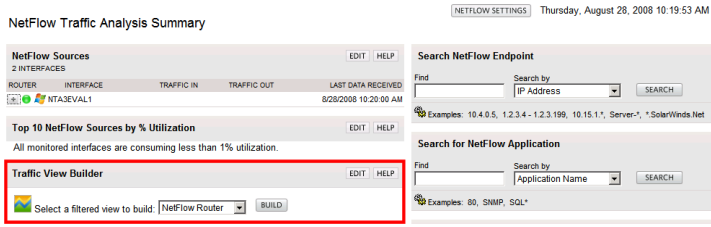
Les sections suivantes présente des scénarios montrant comment Orion NTA Traffic View Builder permet de créer vos propres vues.

Affichage du trafic pour une adresse IP désignée

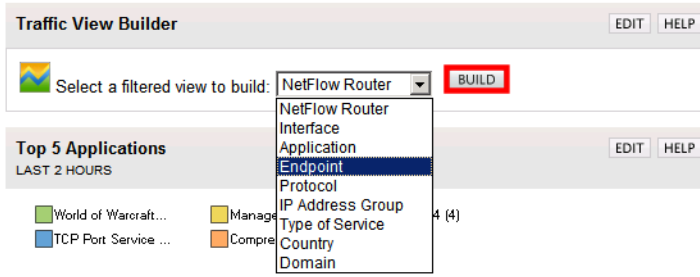
La procédure suivante permet de créer une vue Orion NTA personnalisée montrant le trafic entrant et sortant pour une adresse IP désignée.

Pour créer une vue pour une adresse IP spécifique :

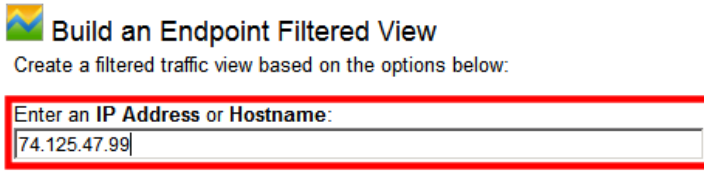
1. Cliquez sur **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Démarrer > Tous les programmes > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console), puis recherchez la ressource Traffic View Builder.



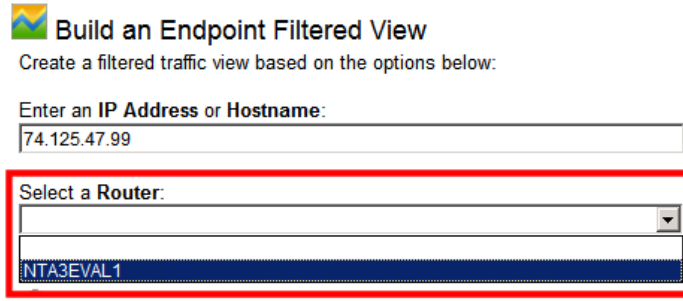
2. Sélectionnez **Endpoint** (Point de terminaison), puis cliquez sur **Build** (Construire).



3. Entrez l'**IP address** (Adresse IP) à surveiller.



4. Sélectionnez le routeur qui envoie le trafic vers l'adresse IP sélectionnée.



5. Sélectionnez **All Interfaces** (Toutes les interfaces) dans le menu Select an Interface (Sélectionner une interface).

   Remarque : il est naturellement possible de personnaliser la vue de manière à n'afficher que le trafic d'une interface spécifique sur le routeur mais, pour cette évaluation, sélectionnez **All Interfaces** (Toutes les interfaces) pour afficher tout le trafic passant par le routeur sélectionné.

6. Cliquez sur **Submit** (Envoyer) ; la vue NetFlow personnalisée s'affiche alors.

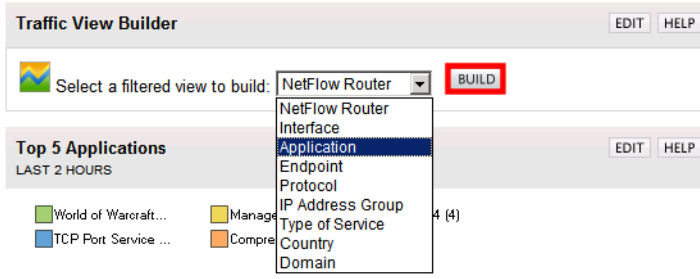
   Remarque : pour plus d'informations sur la vue NetFlow Endpoint (Point de terminaison NetFlow) et ses ressources par défaut, veuillez consulter « Vue NetFlow Endpoint », page 33.

Affichage du trafic pour des ports ou applications spécifiques

La procédure suivante permet de créer une vue Orion NTA personnalisée montrant le trafic passant par des ports spécifiés ou en direction d'applications spécifiées.

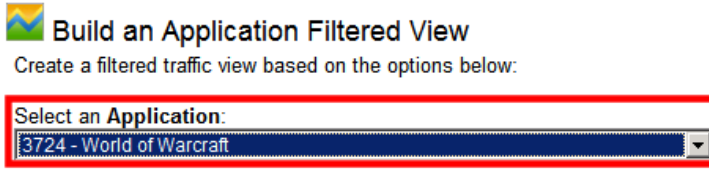
Pour créer une vue pour des ports ou applications spécifiques :

1. Cliquez sur **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console** (Démarrer > Tous les programmes > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console), puis recherchez la ressource Traffic View Builder.
2. Sélectionnez **Application**, puis cliquez sur **Build** (Construire).



3. Sélectionnez l'**Application** ou le Port à surveiller.

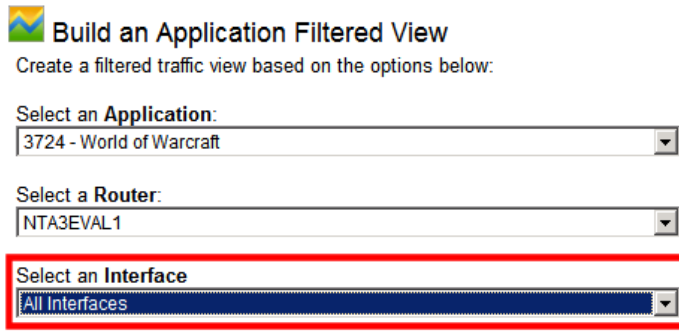
   Remarque : les applications sont répertoriées par numéro de port associé. Pour déterminer les associations entre numéros de port et applications, utilisez la ressource Search for NetFlow Application (Recherche d'application NetFlow) sur la vue NetFlow Traffic Analysis Summary (Résumé de l'analyse du trafic NetFlow). Pour plus d'informations, veuillez consulter « Search for NetFlow Application **(Recherche d'application Netflow)** », page 26.



4. Sélectionnez le routeur compatible NetFlow qui achemine le trafic de l'application.

5. Sélectionnez **All Interfaces** (Toutes les interfaces) dans le menu Select an Interface (Sélectionner une interface).

   Remarque : là encore, il est possible de personnaliser la vue de manière à n'afficher que le trafic d'une interface spécifique sur le routeur mais, pour cette évaluation, sélectionnez **All Interfaces** (Toutes les interfaces) pour afficher tout le trafic passant par le routeur sélectionné.



6. Cliquez sur **Submit** (Envoyer) ; la vue NetFlow personnalisée s'affiche alors.

Remarque : pour plus d'informations sur la vue NetFlow Application et ses ressources par défaut, veuillez consulter « Vue NetFlow Application », page 30.

Recherche et isolement d'un ordinateur infecté

Il est possible d'utiliser l'instance actuellement installée d'Orion NPM, en y associant Orion NTA pour repérer et réagir rapidement à une grande diversité de virus auto-propagateurs qui peuvent attaquer le réseau. Parcourez le scénario suivant :

1. Une agence locale du réseau de votre banque qui gère toutes les transactions par carte bancaire se plaint d'un réseau extrêmement lent qui provoque de fréquents dépassements de délai lors des transferts de données sensibles.

2. Orion Web Console montre que la liaison avec le réseau de l'agence est fonctionnelle.
3. Les diagrammes Orion NPM Percent Utilization (Utilisation en pourcentage) de la page d'accueil Network Summary (Résumé du réseau) montrent que l'utilisation actuelle atteint 98 %, bien que le taux d'utilisation normal soit de l'ordre de 15 % à 25 %.
4. Cliquez sur **NetFlow Traffic Analysis** (Analyse du trafic NetFlow) sur la barre d'outils Modules, puis sur le nom de la liaison réseau de l'agence dans la ressource NetFlow Sources Sources NetFlow) pour afficher le routeur compatible NetFlow présent sur ce réseau.
5. Un coup d'œil rapide à la ressource Top 5 Endpoints (Cinq principaux points de terminaison) et vous constatez qu'un ordinateur de la plage d'adresses IP `10.10.10.0-10.10.10.255` génère à lui seul 80 % de la charge sur cette liaison.
6. Vous savez que les ordinateurs de cette plage d'adresses IP sont accessibles aux clients sur le Web pour leurs transactions personnelles.
7. Dans la ressource Top 5 Applications (Cinq principales applications), vous voyez rapidement que la totalité des deux dernières heures de trafic à partir d'un ordinateur accessible au public a été générée par une application de messagerie IBM MQSeries.
8. Cliquez sur le nom de l'application de messagerie IBM MQSeries dans la ressource Top 5 Applications ; vous voyez alors que le trafic de l'application de messagerie IBM MQSeries passe par le port 1883.
9. Vous ne disposez d'aucun dispositif utilisant la messagerie IBM MQSeries dans la zone accessible aux clients, ni aucun autre service ou protocole utilisant le port 1883, vous savez donc qu'il s'agit d'une attaque virale.
10. Utilisez un outil de gestion de configuration, tel que Cirrus Configuration Manager, pour envoyer vers le pare-feu une nouvelle configuration bloquant le port 1883.

Recherche et blocage d'une utilisation non souhaitée

Orion NTA permet de tracer rapidement le diagramme de l'augmentation de l'utilisation sur n'importe laquelle des différentes liaisons réseau. Orion NPM permet lui aussi de tracer le diagramme de l'utilisation mais lorsque vous lui associez Orion NTA, vous pouvez repérer des instances spécifiques d'utilisation non souhaitée, et décider immédiatement de l'action de correction à y apporter, comme dans le scénario suivant :

1. La liaison ascendante vers Internet a ralenti progressivement au cours des six derniers mois, bien que le nombre d'employés, l'utilisation des applications et la bande passante dédiée soient restés stables.
2. Lorsque vous ouvrez Orion Web Console, la vue Network Summary Home (Résumé de l'analyse du trafic NetFlow) montre que la liaison du site vers Internet est opérationnelle mais, lorsque vous cliquez sur la liaison ascendante et consultez la vue Current Percent Utilization (Utilisation actuelle en pourcentage) de chaque diagramme Interface, vous constatez que l'utilisation actuelle de l'interface avec le Web atteint 80 %.
3. Cliquez sur l'interface avec le Web pour ouvrir la vue Interface Details (Détails de l'interface).
4. En personnalisant le diagramme Percent Utilisation (Utilisation en pourcentage) pour afficher les 6 derniers mois, vous voyez une augmentation régulière de la consommation de 15 % à 80 % au fil du temps. On constate aussi des pics à 90 % et plus.
5. Cliquez sur l'onglet NetFlow Traffic Analysis (Analyse du trafic NetFlow), puis sur l'interface avec le Web- pour ouvrir la vue NetFlow Interface Details (Détails de l'interface NetFlow).
6. En examinant les 50 premiers points de terminaison, vous voyez qu'un groupe d'ordinateurs dans la plage d'adresse IP `10.10.12.0-10.10.12.255` consomme la majeure partie de la bande passante. Ces ordinateurs se trouvent dans la plage d'adresses IP des ventes internes.
7. Analysez chacune des adresses IP en cause ; chacune d'elle montre la présence de Kazaa (port 1214) et World of Warcraft (port 3724) parmi les cinq principales applications.
8. Utilisez un outil de gestion de configuration, tel que Cirrus Configuration Manager, pour envoyer vers le pare-feu une nouvelle configuration bloquant les ports 1214 et 3724.
9. En quelques minutes, vous voyez le trafic de l'interface revenir à 25 %.

Détection et mise en échec des attaques de type déni de service

Orion NTA permet de caractériser facilement le trafic entrant et sortant. Cette capacité est encore plus importante dès lors que les réseaux d'entreprise sont de plus en plus exposés à des attaques malveillantes par déni de service. Parcourez le scénario suivant :

1. Une alerte avancée d'Orion NPM vous avertit des difficultés rencontrées par le routeur tourné vers le Web pour établir et conserver une connexion stable avec Internet.
2. Ouvrez Orion Web Console pour rechercher les problèmes potentiels. Toutes les connexions sont actuellement opérationnelles et l'utilisation de la bande passante paraît correcte. Mais vous remarquez l'utilisation du processeur sur le nœud du pare-feu. Elle reste stable à 99 % à 100 %.
3. Cliquez sur le nom du nœud du pare-feu pour ouvrir la page Node Details (Détails du nœud) correspondante ; la ressource Current Percent Utilization of Each Interface (Utilisation actuelle en pourcentage de chaque interface) montre que les interfaces du pare-feu reçoivent un trafic anormalement élevé.
4. Cliquez sur **NetFlow Traffic Analysis** (Analyse du trafic NetFlow) sur la barre d'outils Modules pour jeter un coup d'œil à la ressource personnalisée Top 50 Endpoints.
5. Cette ressource montre que les six principaux ordinateurs qui tentent d'accéder au réseau se trouvent outre-mer.
6. Vous vous rendez compte que les ports sont balayés et que le pare-feu bloque ces attaques à la volée.
7. Utilisez un outil de gestion de configuration, tel que Cirrus Configuration Manager, pour envoyer vers le pare-feu une nouvelle configuration bloquant tout le trafic sur la plage d'adresses IP des ordinateurs qui essaient d'accéder au réseau.
8. En quelques minutes, l'utilisation processeur sur le routeur tourné vers le Web redevient normale.

En savoir plus sur Orion NTA

Ceci termine la découverte de Orion NetFlow Traffic Analyzer, mais cet *Evaluation Guide* est loin d'avoir traité de la pléthore de fonctionnalités de surveillance des réseaux compatibles Netflow offerte par Orion NTA. Pour en savoir plus sur la puissance et la commodité de Orion NetFlow Traffic Analyzer, ne manquez pas de parcourir le manuel *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide* disponible sur le site Web de SolarWinds, à l'adresse http://www.solarwinds.com/support/documentation.aspxOrion NetFlow Traffic Analyzer.