

FAQ de vRealize Network Insight

VMware vRealize Network Insight 5.2

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

<https://docs.vmware.com/fr/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2020 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

1	À propos du Guide des FAQ vRealize Network Insight	4
2	Général	5
3	Installation et configuration	8
4	Ajout ou configuration de sources de données dans vRealize Network Insight	15
5	Micro-segmentation et flux	18
6	Mise en cluster	20
	Mise en cluster - Généralités	20
	Mise en cluster - Installation et configuration	22
	Mise en cluster - Mise à l'échelle	24
	Mise en cluster - Déploiement	25
7	Gestion et traitement des données	29
8	IPFIX	31

À propos du Guide des FAQ vRealize Network Insight

1

Le Guide des FAQ de vRealize Network Insight fournit à l'utilisateur les questions fréquemment posées sur vRealize Network Insight.

Public visé

Ces informations sont destinées aux utilisateurs qui travaillent avec vRealize Network Insight.

Comment créer un bundle de support ?

Reportez-vous à la section support-bundle *du Guide de référence de la ligne de commande de vRealize Network Insight*.

Comment créer un rôle d'administrateur en lecture seule dans Palo Alto Networks Panorama pour accéder à l'API XML ?

Pour ajouter un rôle **Admin** afin d'accéder à l'API XML :

- 1 Sélectionnez **Panorama** → **Rôles d'administrateur**.
- 2 Cliquez sur **Ajouter** pour ajouter un nouveau rôle d'administrateur et ouvrir la boîte de dialogue Profil de rôle d'administrateur.
- 3 Dans la boîte de dialogue Profil de rôle d'administrateur :
 - a Attribuez un nom au rôle (par exemple, `api-only-admin`)
 - b Sélectionnez le **Rôle Panorama**.
 - c Désactivez toutes les entrées dans l'onglet Interface utilisateur Web.
 - d Activez toutes les entrées excepté **Valider** dans l'onglet API XML.
 - e Cliquez sur **OK** pour fermer la boîte de dialogue. Un nouveau **rôle d'administrateur** et son nom apparaissent dans la liste.
 - f Cliquez sur **Valider** pour valider les modifications apportées à Panorama.
- 4 Attribuez ce rôle **Admin** à un compte d'administrateur.

Quand un service est-il considéré comme partagé ?

Les ports suivants sont configurés comme étant partagés :

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

Un événement/message d'erreur s'affiche sur la source de données indiquant que les informations d'identité de la source de données, comme le certificat ou la clé, ont été modifiées. Qu'est-ce que cela signifie ?

vRealize Network Insight a reçu un nouveau certificat d'une source de données qui n'est pas identique à celui stocké dans le produit. vRealize Network Insight accepte automatiquement le certificat présenté par les sources de données. Pendant le processus, vous recevez un événement sur les sources de données à partir desquelles vous pouvez télécharger les anciens et nouveaux certificats.

Quelle est la limite d'importation d'enregistrements DNS dans vRealize Network Insight ?

Les limites d'importation d'enregistrements DNS sont les suivantes :

- Source de données DNS Infobox : vous pouvez importer 900 000 enregistrements à partir d'une seule source de données.
- Importation manuelle d'enregistrements DNS : vous pouvez importer des enregistrements DNS à l'aide de plusieurs fichiers `.csv` ou Bind mis en package au format `.zip`. Vous pouvez importer autant d'enregistrements que vous le voulez, mais les téléchargements sont limités comme suit :
 - Nombre de fichiers dans un fichier `.zip` unique : 25
 - Taille maximale d'un fichier `.zip` unique : 10 Mo.

Installation et configuration

3

Quelles sont les besoins en ressources pour vRealize Network Insight ?

Pour connaître les besoins en ressource, reportez-vous au Guide d'installation de vRealize Network Insight.

Que se passe-t-il si j'entre une clé incorrecte lors du déploiement de l'OVA du proxy de vRealize Network Insight ?

La clé secrète n'est pas validée lors du déploiement de l'OVA du proxy de vRealize Network Insight. Le déploiement sera effectué, même avec une clé secrète incorrecte. Cependant, le couplage peut échouer et le proxy de vRealize Network Insight n'apparaît pas comme détecté dans l'interface utilisateur de vRealize Network Insight.

Pour corriger le secret partagé, connectez-vous à la CLI du proxy de vRealize Network Insight et exécutez la commande `set-proxy-shared-secret` pour définir la clé secrète correcte. Cette commande remplace l'ancienne clé par la nouvelle ; par conséquent, la plate-forme vRealize Network Insight peut détecter le proxy de vRealize Network Insight et s'y associer.

Comment configurer le DNS après le déploiement de l'OVA du proxy de vRealize Network Insight ?

Connectez-vous à la CLI du proxy de vRealize Network Insight et exécutez la commande `change-network-settings`. Cette commande interactive permet à l'utilisateur d'ajouter ou de modifier le DNS, afin de reconfigurer le proxy de vRealize Network Insight avec le nouveau DNS.

Si l'un des paramètres réseau n'est pas configuré correctement, utilisez la commande `change-network-settings` pour modifier les paramètres de configuration réseau.

Comment trouver l'adresse IP de la VM proxy de vRealize Network Insight à partir de l'interface utilisateur ?

Accédez à la page Paramètres et sélectionnez l'option de menu Infrastructure vRealize Network Insight. Les adresses IP de la plate-forme vRealize Network Insight et des machines virtuelles proxy de vRealize Network Insight s'affichent.

Que faire si le proxy de vRealize Network Insight n'est pas détecté dans les 5 minutes après le déploiement de l'OVA du proxy de vRealize Network Insight ?

Connectez-vous au proxy de vRealize Network Insight à l'aide de la commande `consoleuser` (reportez-vous au Guide de l'interface de ligne de commande de vRealize Network Insight) et vérifiez les points suivants :

- Vérifiez l'état du couplage de la plate-forme vRealize Network Insight et du proxy de vRealize Network Insight à l'aide de la CLI `show-connectivity-status`.
- Si l'état du couplage indique `Passed`, ouvrez l'interface utilisateur de la plate-forme dans une nouvelle fenêtre de navigateur et connectez-vous pour vérifier l'état.
- Si l'état du couplage indique `Failed`, la clé secrète partagée spécifiée lors du déploiement de l'OVA du proxy de vRealize Network Insight est peut-être incorrecte. Pour résoudre ce problème, utilisez la commande `set-proxy-shared-secret` pour définir la clé secrète correcte. Cette commande remplace l'ancienne clé par la nouvelle ; par conséquent, la plate-forme vRealize Network Insight peut détecter le proxy de vRealize Network Insight.
- Si `show-connectivity-status` affiche l'accessibilité du réseau à la plate-forme vRealize Network Insight avec l'état **Échec**, vérifiez que la plate-forme vRealize Network Insight est accessible depuis la machine virtuelle proxy de vRealize Network Insight à l'aide de la commande `ping`.
- Si ce n'est pas le cas, vérifiez si les paramètres NTP, DNS, de la passerelle et autres paramètres réseau sont correctement configurés à l'aide de la commande `show-config`.
- Si l'un des paramètres réseau n'est pas configuré correctement, utilisez la commande `setup` pour modifier les paramètres de configuration réseau.

Que je faire si j'oublie mes informations d'identification de connexion ?

Si vous êtes l'utilisateur local de l'interface utilisateur : contactez l'administrateur de l'interface utilisateur de vRealize Network Insight pour réinitialiser les informations d'identification de votre système.

Si vous êtes l'administrateur : dans vRealize Network Insight 3.4, les informations d'identification de l'interface utilisateur peuvent être modifiées à l'aide de la CLI `modify-password`. Pour plus de détails, consultez le Guide de l'interface de ligne de commande. Si vous utilisez une version de vRealize Network Insight antérieure à la version 3.4, contactez le support technique.

Comment modifier le mot de passe de connexion ?

Pour modifier le mot de passe de connexion :

- 1 Accédez à **Administrateur > Paramètres**, puis cliquez sur **Mon profil** dans le volet de gauche.
- 2 Sur la page **Modifier le mot de passe**, renseignez les informations requises et cliquez sur **Enregistrer**.

Que faire si l'écran de connexion s'affiche avant la détection de la VM proxy de vRealize Network Insight ?

- Ce comportement est normal lorsque le navigateur est actualisé ou que l'URL est ouverte dans une nouvelle fenêtre avant la détection du proxy.
- Connectez-vous à l'aide des informations d'identification définies lors de l'activation de la licence pour le nom d'utilisateur `admin@local`.

vRealize Network Insight prend-il en charge plusieurs instances de vCenter Server/NSX Manager ?

Oui, vRealize Network Insight prend en charge plusieurs instances de vCenter Server et NSX Manager.

Quels services de vRealize Network Insight requièrent l'accès à Internet et pourquoi ?

vRealize Network Insight prend en charge la fonctionnalité d'appel interne à distance qui nécessite l'accès à Internet. Cette fonctionnalité ou ces services permettent à l'équipe de vRealize Network Insight d'obtenir une meilleure compréhension des environnements clients et de résoudre des problèmes ou de corriger des erreurs de manière proactive. Les services suivants requièrent l'accès à Internet :

- Service de mise à jour automatique (`svc.ni.vmware.com:443`) : vRealize Network Insight utilise ce service pour contacter l'hôte de mise à niveau distant et extraire les derniers bits publiés dès qu'ils sont disponibles. L'utilisateur reçoit une notification dans l'interface utilisateur lorsque les mises à jour sont disponibles. Ce service est activé par défaut, mais vous pouvez le désactiver via l'interface utilisateur ou à l'aide de la commande `online-upgrade` via la CLI.

- Service de télémétrie des performances (`svc.ni.vmware.com:443`) : certaines mesures liées aux services et aux performances clés de vRealize Network Insight sont régulièrement collectées et téléchargées pour vRealize Network Insight. L'équipe de support surveille ces mesures et identifie toute anomalie dans l'environnement afin de pouvoir intervenir avant que les services critiques ne soient affectés. Ce service est désactivé par défaut, mais vous pouvez l'activer ou le désactiver à l'aide de la commande `telemetry` dans la CLI. Pour plus d'informations, consultez l'article : <https://kb.vmware.com/s/article/59242>
- Service de support (`support2.ni.vmware.com:443`) : ce service établit des tunnels sécurisés distants vers l'hôte vRealize Network Insight de support, qui permettent au personnel autorisé d'accéder à distance aux déploiements et de les utiliser. Ce service est désactivé par défaut et peut être activé/désactivé via l'interface utilisateur, ainsi que l'interface de ligne de commande support-tunnel.
- Service d'enregistrement (`reg.ni.vmware.com:443`) : permet d'enregistrer le dispositif auprès de tous les services externes. Il activera la communication approuvée entre les services mentionnés ci-dessus. Lorsque le programme d'installation dispose de l'accès à Internet, l'enregistrement s'effectue automatiquement. Dans un environnement isolé, il peut être effectué à l'aide de l'interface de ligne de commande `offline-registration`. Pour plus de détails, consultez le Guide de l'interface de ligne de commande. Ce service est requis pour activer le tunnel de prise en charge.

Note Si la plate-forme vRealize Network Insight se trouve derrière un proxy Internet, placez les noms de domaine et ports suivants dans la liste blanche :

Tableau 3-1.

Service	URL	Port
Service de mise à niveau/mesures	<code>svc.ni.vmware.com</code>	443
Service du tunnel de prise en charge	<code>support2.ni.vmware.com</code>	443
Service d'enregistrement	<code>reg.ni.vmware.com</code>	443

Comment désactiver l'accès à Internet depuis le dispositif ?

Les services suivants utilisent des services distants/Internet sécurisés :

- Service de mise à jour automatique
- Service de télémétrie des performances
- Service de support
- Service d'enregistrement

Pour plus d'informations sur l'activation ou la désactivation de ces services, consultez la [Quels services de vRealize Network Insight requièrent l'accès à Internet et pourquoi ?FAQ](#). Si l'un de ces services est activé, vRealize Network Insight doit disposer d'un accès à Internet.

Qu'est-ce que l'agrégation de ports et quel est le mécanisme qui permet d'effectuer cette opération ?

L'agrégation de ports est conçue pour agréger les flux de port éphémère, tels que FTP dynamique, Oracle, MS-RPC, etc. Cela permet de réduire le nombre de flux dans le système et de fournir une vue agrégée d'un nombre élevé de flux qui sont essentiellement destinés au même service.

Le mécanisme à réaliser est le suivant :

- Pendant les trois premiers jours d'observation d'une `destination_ip`, nous agrégerons les ports de destination sur cette adresse IP spécifique dans des compartiments de 10 k et commençons à créer un profil de port (port-profile) pour cette adresse IP (Nous créons un profil de port par adresse IP de destination.).
- Après trois jours, une fois le profil créé, nous commencerons à agréger des plages de ports dans lesquelles la densité de ports est élevée (reflétant le modèle d'ouverture de port éphémère). Les plages elles-mêmes seront de taille dynamique, par exemple 100, 1 000, 10 000, et seront créées selon le nombre de ports ouverts et leur étendue dans la plage d'agrégation donnée.

Note Cette décision se produit de manière indépendante pour chaque adresse IP de serveur.

- Cela permet de signaler des flux de port à numéro élevé sans agrégation lorsqu'aucune activité d'ouverture de port en bloc ne se produit et permet d'appliquer une agrégation dynamique lorsqu'une telle activité se produit.
- Le profil est continuellement mis à jour à intervalles réguliers pour prendre en compte les nouveaux ports ouverts ou les anciens désormais fermés.

Comment modifier l'adresse IP, la passerelle ou le masque de réseau après le déploiement de l'OVA de vRealize Network Insight ?

Pour modifier les paramètres réseau de la plate-forme/du proxy de vRealize Network Insight, connectez-vous à la CLI et exécutez la commande `change-network-settings`. Cette commande interactive donne à l'utilisateur la possibilité de modifier l'adresse IP, la passerelle, le masque de réseau, etc., après quoi, le dispositif vRealize Network Insight est reconfiguré avec les nouvelles informations.

Note

- Cette tâche doit être effectuée à l'aide de la session de console de machine virtuelle lorsque le dispositif redémarre finalement.
- Si l'adresse IP de la plate-forme vRNI est modifiée et couplée à des proxys, exécutez la commande de l'interface de ligne de commande suivante sur chaque VM du proxy :

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

Comment passer d'une licence d'évaluation à une licence perpétuelle ?

Reportez-vous à la section Ajouter et modifier une licence dans le Guide de l'utilisateur de vRealize Network Insight.

Comment les licences sont-elles caractérisées dans vRealize Network Insight ?

Tableau 3-2.

Nom de la licence	Type de licence	Fonctionnalités
Enterprise	Complète/de production: elle peut être perpétuelle ou limitée dans le temps.	Les fonctionnalités suivantes sont activées : <ul style="list-style-type: none"> ■ AWS en tant que fournisseur de données ■ Stratégies de rétention des données ajustables ■ Source de données Infoblox DNS ■ Adresses IP physiques et mappage DNS ■ Analyses
Avancé	Complète/de production: elle peut être perpétuelle ou limitée dans le temps.	SO

Note Toutes les licences sont dotées par socket de CPU et CCU (utilisateurs simultanés). Les licences d'évaluation peuvent être renouvelées ou converties en licence de **production** avec la clé mise à jour via **Interface utilisateur -> Paramètres -> À propos de**. Pour plus de détails, consultez le Guide de l'utilisateur.

Comment effectuer une sauvegarde des machines virtuelles dans vRealize Network Insight ?

Reportez-vous aux *Meilleures pratiques VMware* pour effectuer la sauvegarde des machines virtuelles telles que VMware VADP/VDP API. Il est recommandé d'effectuer une sauvegarde avant de créer ou d'étendre des clusters.

Ajout ou configuration de sources de données dans vRealize Network Insight

4

Que se passe-t-il si je reçois le message « La demande a expiré » lors de l'ajout d'un système vCenter Server à l'aide de l'adresse IP ?

- Vérifiez que l'adresse IP du système vCenter Server est accessible à partir de la VM proxy de vRealize Network Insight.
- Connectez-vous à l'interface de ligne de commande du proxy de vRealize Network Insight et utilisez la commande `ping` pour vérifier que l'adresse IP est accessible et `Telnet` pour vérifier que le système vCenter Server est accessible sur le port 443.
- Si le système vCenter Server est accessible, réessayez de l'ajouter.
- Si l'adresse IP n'est pas accessible, vérifiez que la passerelle est correctement configurée à partir de la VM proxy de vRealize Network Insight à l'aide de la commande `show-config`.
- Si la passerelle n'est pas correctement configurée, corrigez l'erreur à l'aide de la commande `setup`.

Que se passe-t-il si je reçois le message « L'adresse IP/le nom de domaine complet n'est pas valide » lors de l'ajout d'un système vCenter Server ?

- Vérifiez si l'adresse IP ou le nom de domaine complet fourni pour le système vCenter Server est correct.
- Vérifiez si le nom de domaine complet est accessible à partir de la VM proxy de vRealize Network Insight à l'aide de la commande `ping`.
- Si ce n'est pas le cas, vérifiez si le DNS est correctement configuré sur la VM proxy de vRealize Network Insight à l'aide des commandes `nslookup FQDN` et `show-config`.
- Si le DNS est incorrect, corrigez-le à l'aide de la commande `setup`.

Quels privilèges sont requis pour la plate-forme de sécurité et d'opérations vRealize Network Insight ?

vRealize Network Insight requiert les informations d'identification de VMware vCenter Server avec les privilèges suivants :

- Distributed Switch : Modifier
- Groupe dvPort : Modifier

Que se passe-t-il si je reçois le message d'erreur « L'utilisateur ne dispose pas des privilèges requis » lors de l'activation d'IPFIX sur la page de source de données de l'instance de vCenter Server ?

vRealize Network Insight requiert les informations d'identification de VMware vCenter Server avec les privilèges suivants pour activer IPFIX :

- Distributed Switch : Modifier
- Groupe dvPort : Modifier

Vérifiez que l'utilisateur VMware vCenter Server fourni dispose d'une autorisation d'accès au dossier racine du système vCenter Server et à toutes ses entités enfants, par exemple tous les dossiers et centres de données.

À quelle fréquence les données sont-elles extraites de l'environnement ?

Le proxy de vRealize Network Insight extrait les données toutes les 10 minutes de l'environnement.

Quand l'analyse des données démarre-t-elle après l'ajout du système vCenter Server ?

L'analyse des données démarre immédiatement après l'ajout d'un système vCenter Server. L'interface utilisateur du produit affiche une image partielle des données après quelques minutes et l'opération peut prendre deux heures.

Note Le trafic de flux de données change continuellement et inclut au moins 24 heures de données dans l'analyse.

Comment nettoyer les paramètres IPFIX dans le système vCenter Server si j'ai supprimé les OVA de vRealize Network Insight ?

- À l'aide de VMware vSphere Web Client : accédez aux paramètres **Accueil > Mise en réseau > VDS (Nom) > NetFlow**. Supprimez l'adresse IP du proxy de vRealize Network Insight des paramètres du collecteur.
- À l'aide du client Windows pour VMware vSphere : accédez aux paramètres **Accueil > Inventaire > Mise en réseau > VDS (nom) > Modifier**. Supprimez l'adresse IP du proxy de vRealize Network Insight des paramètres du collecteur dans l'onglet NetFlow. Cette étape doit être effectuée pour chaque VDS pour lequel IPFIX est activé.

Comment nettoyer la configuration IPFIX dans vRealize Network Insight ?

Dans l'interface utilisateur de vRealize Network Insight, accédez à **Paramètres > Sources de données** et supprimez l'instance de vCenter Server. Cette action supprime la configuration IPFIX effectuée par vRealize Network Insight.

Combien de temps faut-il pour afficher les règles de pare-feu correctes dans le chemin VM-VM après l'ajout de VMware NSX Manager dans vRealize Network Insight ?

Une fois que vous avez ajouté VMware NSX Manager dans vRealize Network Insight, cela peut prendre jusqu'à 24 heures pour calculer la machine virtuelle avec la relation de règle de pare-feu.

Pourquoi ne puis-je pas voir la PNIC dans le chemin VM-VM après l'ajout de VMware vCenter dans vRealize Network Insight ?

Normalement, il faut environ 2 heures pour que vRealize Network Insight calcule le chemin VM-VM après l'ajout d'une instance de VMware vCenter dans vRealize Network Insight en tant que source de données. Cependant, dans de rares situations, cela peut prendre environ 8 à 10 heures pour que la PNIC s'affiche correctement dans le chemin VM-VM après avoir ajouté l'instance de VMware vCenter dans vRealize Network Insight.

Que représentent les nombres de l'épingle de distribution du trafic ?

Le pourcentage donne un aperçu de la distribution du trafic en fonction de l'analyse des flux.

Tableau 5-1.

Trafic	Description
Est-Ouest (E-O)	Trafic Est-Ouest en pourcentage du trafic du groupe total
Commuté (% d'E-O)	Trafic commuté en pourcentage du trafic Est-Ouest
Acheminé (% d'E-O)	Trafic acheminé en pourcentage (%) du trafic Est-Ouest
Dans un hôte (% de VM vers VM)	Trafic dont la source et la destination sont sur le même hôte, en pourcentage de trafic de VM vers VM
VM vers VM (% d'E-O)	Trafic de machine virtuelle vers machine virtuelle en pourcentage du trafic Est-Ouest
Internet	Trafic Internet en pourcentage du trafic du groupe total

Comment les ports sont-ils agrégés dans les flux ?

L'agrégation de ports est conçue pour agréger les flux de port éphémère, tels que FTP dynamique, Oracle, MS-RPC, etc. Cela permet de réduire le nombre de flux dans le système et de fournir une vue agrégée d'un nombre élevé de flux qui sont essentiellement destinés au même service. Le mécanisme à réaliser est le suivant :

- Pendant les trois premiers jours d'observation d'une adresse_ip_destination, nous agrégerons les ports de destination sur cette adresse IP dans des compartiments de 10 k et commençons à créer un profil de port (port-profile) pour cette adresse IP.
- À l'issue des trois jours, nous avons créé un profil qui peut être utilisé en toute sûreté : nous commencerons à agréger des plages de ports dans lesquelles la densité de port est élevée (en d'autres termes, reflétant le modèle d'ouverture de port éphémère). Les plages elles-mêmes seront de taille dynamique (100, 1 000, 10 000) et seront créées en fonction du nombre de ports ouverts et de leur étendue dans la plage d'agrégation donnée.

- Cela permet de signaler des flux de port à numéro élevé sans agrégation lorsqu'aucune activité d'ouverture de port en bloc ne se produit et permet d'appliquer une agrégation dynamique lorsqu'une telle activité se produit.
- Le profil est continuellement mis à jour à intervalles réguliers pour prendre en compte les nouveaux ports ouverts ou les anciens désormais fermés.

Que signifie l'adresse IP 240.240.240.240 dans vRealize Network Insight ?

240.240.240.240 est l'adresse IP de l'espace réservé dans vRealize Network Insight. Cette adresse IP est utilisée lorsqu'un nombre élevé d'adresses IP (> 5 000) atteint une adresse IP particulière. Toutes les autres adresses IP Internet entrantes (à partir de la 5 001ème) avec cette adresse IP d'espace réservé 240.240.240.240 peuvent être remplacées pour ce point de terminaison de service.

Cela permet de limiter le nombre de flux dans le système, car le service publiquement exposé qui journalise chaque client Internet séparément peut générer un nombre considérable de flux, ce qui entraînerait une augmentation de la charge du système.

Pour tous les flux remplacés par cette adresse IP d'espace réservé, toutes les mesures sont agrégées sur le flux correspondant avec cette adresse IP ; aucune statistique n'est donc perdue à un niveau agrégé.

Toutes les adresses IP de destination des flux signalés dans la vue des flux sont indiquées comme provenant de l'adresse 240.240.240.240 et sont en fait atteintes par un nombre élevé d'adresses IP Internet (> 5 000).

Mise en cluster

6

Ce chapitre contient les rubriques suivantes :

- [Mise en cluster - Généralités](#)
- [Mise en cluster - Installation et configuration](#)
- [Mise en cluster - Mise à l'échelle](#)
- [Mise en cluster - Déploiement](#)

Mise en cluster - Généralités

Une VM proxy ou de collecteur peut-elle être mise en cluster ?

Non. La mise en cluster des VM proxy ou de collecteur n'est pas prise en charge.

vRealize Network Insight requiert-il un équilibrage de charge comme vRealize Log Insight ?

La mise en cluster vRealize Network Insight est une solution de montée en charge, non de haute disponibilité. Si la VM de la plate-forme principale/le nœud master échoue, l'ensemble du service devient indisponible.

Qu'arrive-t-il si la connexion entre le proxy distant et la plate-forme est interrompue ?

Si la connexion entre la plate-forme et la VM proxy est interrompue, la VM proxy stocke les données au niveau local (en fonction de l'espace disque) et les envoie dès qu'elle est reconnectée.

vRealize Log Insight est-il intégré à vRealize Network Insight ?

Oui, vRealize Log Insight a été intégré à vRealize Network Insight 3.4. Les alertes sont envoyées à Syslog, qui peut être vRealize Log Insight.

Qu'arrive-t-il lorsqu'un nœud redémarre ?

Si un nœud redémarre, il rejoint automatiquement le cluster et reste fonctionnel. S'il s'agit du nœud principal, l'ensemble du service est perdu pendant la durée d'inactivité du nœud.

Comment modifier l'adresse IP d'un nœud de plate-forme ou d'un collecteur dans un cluster ?

Dans un cluster, vous pouvez modifier l'adresse IP d'un collecteur ou d'un nœud de plate-forme à l'aide des commandes de l'interface de ligne de commande.

Note

- Contactez le support VMware avant d'effectuer cette opération.
 - Le dispositif redémarre à la fin du processus. Par conséquent, vous devez effectuer ces étapes sur la console de machine virtuelle.
-
- Pour modifier l'adresse IP du collecteur, exécutez la commande `change-network-settings`.
 - Pour modifier l'adresse IP de la plate-forme,
 - a exécutez la commande `change-network-settings`.
 - b exécutez la commande `update-IP-change` sur toutes les autres plates-formes pour refléter la nouvelle adresse IP.
 - c exécutez la commande `show-connectivity-status` sur un collecteur et recherchez **l'Adresse IP/URL de la VM de plate-forme** pour déterminer si elle est associée à cette plate-forme.
 - d exécutez la commande `vrni-proxy` pour refléter la nouvelle adresse IP de la plate-forme sur les collecteurs associés.

Cas d'utilisation 1 : dans un cluster à 3 nœuds, seule l'adresse IP de la plate-forme 2 est modifiée. Aucun collecteur ne lui est associé.

- 1 Exécutez `change-network-settings` sur la plate-forme 2.
- 2 Exécutez `update-IP-change` sur la plate-forme 1 et la plate-forme 3 pour refléter la nouvelle adresse IP de la plate-forme 2.

Cas d'utilisation 2 : dans un cluster à 3 nœuds, les adresses IP de la plate-forme 1 et la plate-forme 2 sont modifiées. Le collecteur A est associé à la plate-forme 2, les autres collecteurs sont associés à la plate-forme 3.

- 1 Exécutez `change-network-settings` sur la plate-forme 1.
- 2 Exécutez `change-network-settings` sur la plate-forme 2.
- 3 Exécutez `update-IP-change platform1-oldIP platform1-newIP` sur la plate-forme 2 et la plate-forme 3.
- 4 Exécutez `update-IP-change platform2-oldIP platform2-newIP` sur la plate-forme 1 et la plate-forme 3.
- 5 Exécutez `vrni-proxy set-platform --ip-or-fqdn platform2-newIP` sur le collecteur A.

Quelle quantité d'espace disque est nécessaire sur la plate-forme 1 ?

La plate-forme 1 requiert davantage d'espace disque que les autres nœuds du cluster, car certaines données de configuration y sont stockées uniquement.

Que se passe-t-il si l'espace disque est insuffisant sur l'un des nœuds ?

L'interface utilisateur affichera des messages d'erreur lorsque l'espace disque sur un nœud de plate-forme atteint un certain seuil. Ajoutez de l'espace disque au nœud de plate-forme en vous connectant au système vCenter.

Combien de fois les données sont-elles répliquées dans le cluster ?

Le mécanisme de réplication des données dépend des composants présents dans le nœud de plate-forme.

Mise en cluster - Installation et configuration

Toutes les VM de plate-forme doivent-elles se trouver sur le même segment L2/L3 ?

Non. Cependant, il est recommandé de conserver tous les nœuds de plate-forme sur un réseau commun avec des latences faibles entre eux. Cela est dû au fait que de nombreux composants distribués répliquent les données entre les nœuds et des latences élevées peuvent entraîner des problèmes de performances et de stabilité du système.

Un cluster peut-il être mis à niveau à l'aide de la fonctionnalité de mise à niveau intégrée au produit ?

Les mises à niveau en ligne ne sont pas prises en charge pour le cluster jusqu'à la version 3.7. À partir de la version 3.8 et versions ultérieures, un cluster peut être mis à niveau à l'aide de la méthode de mise à niveau en ligne.

Que se passe-t-il en cas de panne lors du processus de création du cluster ?

Il est recommandé d'effectuer un snapshot de la plate-forme principale et des proxys avant de lancer le processus de création de cluster. En cas de panne, supprimez les nœuds de la plate-forme secondaire et récupérez les VM proxy et de la plate-forme principale à partir des snapshots.

Qu'arrive-t-il aux données et à la configuration existantes lorsque je développe le déploiement à nœud unique dans un cluster ?

Toutes les données et la configuration sont conservées telles quelles. Les données seront accessibles après la création du cluster.

Pouvez-vous disposer d'une VM de plate-forme dans différentes régions ?

Non, les nœuds de plate-forme doivent être installés sur le même site. Les serveurs proxy peuvent être géodistribués.

La plate-forme peut-elle être hébergée dans des clusters étendus vSAN (2 centres de données, etc.) ?

Oui, les clusters vSAN dans un même ou plusieurs centres de données garantissent toujours certaines performances d'E/S, telles que le stockage local.

Pouvons-nous héberger des nœuds de cluster dans différents clusters vSAN ?

Oui, différents nœuds d'un cluster de plate-forme peuvent être hébergés dans des banques de données sous-jacentes différentes.

Devez-vous sauvegarder les nœuds de plate-forme ?

Oui, les sauvegardes doivent être effectuées à l'aide des technologies de snapshot ou de sauvegarde recommandées par VMware.

Comment estimer la bande passante entre la VM proxy de cluster dans une région et le cluster de VM de plate-forme dans une autre région ?

Dans certains déploiements étendus, ce nombre peut atteindre entre 1 Mbit/s et 20 Mbit/s. Un nombre élevé d'opérations de déduplication ou de compression se produit dans la VM proxy avant l'envoi des données vers la VM de plate-forme.

Quelle quantité le trafic réseau pourra-t-il atteindre entre les nœuds de cluster ?

Le trafic dépend généralement de la taille du cluster et du type d'environnement du centre de données.

Dans le cas d'une installation de 30 à 50 000 VM :

- Entre les clusters : 50 à 400 Mbit/s environ
- Entre le proxy et la plate-forme : 100 Kbit/s à 15 Mbit/s environ

Quelle est la latence maximale admissible entre les nœuds d'un cluster ?

Les nœuds de plate-forme doivent être situés sur le même site. Dans ce cas, la latence est minimale. Si les nœuds de plate-forme sont hébergés sur des clusters étendus vSAN (2 centres de données), les clusters vSAN dans un même ou plusieurs centres de données garantissent toujours certaines performances d'E/S, telles que le stockage local. Les applications exécutées sur des centres de données comme vRealize Network Insight fonctionnent correctement. Vous pouvez héberger différents nœuds d'un cluster de plate-forme dans différentes banques de données sous-jacentes. Vous devez toutefois vous assurer que toutes les VM de plate-forme d'un cluster sont installées sur le même site.

Quelle est la latence maximale admissible entre les VM proxy dans une région et le cluster de VM de plate-forme dans une autre région ?

Vous pouvez disposer de proxys géodistribués dans votre configuration. Une connexion HTTPS est établie entre la VM proxy et la VM de plate-forme de manière à pouvoir tolérer des latences élevées, à organiser en quelques secondes. vRealize Network Insight prend en charge 10 nœuds maximum dans un cluster (30 000 VM avec flux ou 50 000 VM sans flux).

Quelle doit être la taille de la VM proxy/de plate-forme ?

Utilisez une configuration de briques étendue. Pour cela, reportez-vous au Guide d'installation.

Mise en cluster - Mise à l'échelle

Puis-je étendre un cluster déjà créé ?

Oui, l'extension d'un cluster est prise en charge jusqu'à 10 nœuds.

Qu'arrive-t-il si une VM de plate-forme autre que principale devient indisponible ?

Les services internes ont une résilience limitée aux pannes des nœuds non principaux. En général, lors d'une panne de nœud, NI perd la puissance de calcul.

Quel type d'équilibrage de charge est pris en charge ?

Le mappage du proxy vers la plate-forme est fixe. Lorsque les données d'une VM proxy atteignent une VM de plate-forme, leur traitement est équilibré en charge en interne entre toutes les VM de la plate-forme.

La création d'un cluster de plate-forme augmentera-t-elle la consommation de bande passante ?

Les VM proxy ou de collecteur continuent de communiquer uniquement avec la VM principale ou de plate-forme. La bande passante requise pour la communication avec la VM de plate-forme dans le cluster est minime. Par conséquent, la consommation de bande passante n'augmente pas de manière significative.

Quelle est la fréquence de transmission des données entre la VM proxy et la VM de plate-forme ?

La VM proxy envoie les données dédupliquées ou compressées en continu à la VM de plate-forme.

L'optimisation des données a-t-elle lieu dans la VM proxy ?

Différentes étapes de déduplication, de compression, de réduction ou de traitement par lot se produisent dans la VM proxy. Lorsque la connexion entre la VM de plate-forme et la VM proxy est interrompue, la VM proxy stocke les données au niveau local (en fonction de l'espace disque) et les envoie dès que la connexion est restaurée.

Une optimisation est-elle effectuée pour la bande passante réseau ?

Oui, différentes étapes de déduplication/compression/réduction/traitement par lot se produisent dans la VM proxy.

La mise en cluster est-elle possible sur les serveurs proxy ?

Non. La mise en cluster n'est pas possible sur les serveurs proxy.

Comment le système vCenter envoie-t-il le trafic au serveur proxy ?

Le système vCenter n'envoie aucun trafic au serveur proxy. Les serveurs proxy se connectent au système vCenter qui leur est désigné pour extraire les informations.

Lors du déploiement d'un cluster, comment le système vCenter envoie-t-il le trafic aux différents serveurs proxy ?

En réalité, les proxys se connectent au système vCenter pour extraire les informations. Le proxy respectif se connectera au système vCenter désigné pour extraire les informations. Aucune mise en cluster n'est disponible sur le proxy.

Mise en cluster - Déploiement

Comment accéder à l'interface utilisateur après la montée en charge du cluster ?

Vous pouvez accéder à l'interface utilisateur uniquement à partir de la plate-forme 1.

Qu'est-ce que la plate-forme 1 et pourquoi dois-je mémoriser ce nœud ?

Le nœud de plate-forme à partir duquel le processus de création de cluster est lancé est traité comme **Plate-forme 1**. Accédez à l'interface utilisateur uniquement à partir de ce nœud, sur les nœuds du cluster.

Comment les données sont-elles récupérées à partir des autres nœuds d'un cluster si l'accès à l'interface utilisateur est limité à la plate-forme 1 ?

Les données du centre de données sont réparties entre tous les nœuds d'un cluster. Lorsque la couche d'interface utilisateur demande des données sur la plate-forme 1, le nœud Plate-forme 1 obtient les données stockées sur tous les nœuds et envoie une réponse à l'interface utilisateur.

Puis-je utiliser un nœud de plate-forme déployé dans un autre centre de données pour créer des clusters ?

Tous les nœuds d'un cluster échangent des données entre eux. Par conséquent, pour éviter tout problème de latence, il est recommandé d'utiliser les nœuds de plate-forme déployés dans le même centre de données pour créer un cluster.

Qu'arrive-t-il aux données de la plate-forme existante lorsque je monte en charge le nœud de plate-forme ?

Les données sur un nœud de plate-forme existant sont conservées et réparties entre tous les nœuds d'un cluster.

Le nombre de VM proxy est-il important pour déterminer le nombre de briques de plate-forme dont j'ai besoin ?

Non. Seul le nombre total de VM dans tous les systèmes vCenter et l'état des flux (activé ou désactivé) ont un impact sur le nombre de briques nécessaires. Reportez-vous au tableau de modèles de brique dans le *Guide d'installation de vRealize Network Insight*.

Le nombre de systèmes vCenter et le nombre de périphériques physiques (tels que des routeurs), ou tout autre type de sources de données, ont-ils un impact sur le nombre de briques de plate-forme dont j'ai besoin ?

Non. Seul le nombre total de VM dans tous les systèmes vCenter et l'état des flux (activé ou désactivé) ont un impact sur le nombre de briques nécessaires. Reportez-vous au tableau de modèles de brique dans le *Guide d'installation de vRealize Network Insight*.

vRNI prend-il en charge le cluster de plate-forme distribué sur 2 centres de données pour des raisons liées à la fonctionnalité HA ?

Non. Le cluster de plate-forme ne prend pas en charge la répartition entre plusieurs centres de données. Toutes les VM du cluster de plate-forme doivent être présentes sur le même site. Actuellement, le cluster de plate-forme ne prend pas en charge la fonctionnalité HA. Cette option figure sur le plan d'évolution. Les clients peuvent utiliser SRM pour la fonctionnalité HA au niveau du DR sur 2 sites.

vRNI prend-il en charge un système vCenter unique comptant plus de 6 000 VM et flux activés ?

Jusqu'à la version 3.5, les proxys vRNI ne prennent pas en charge la collecte de données à partir d'un seul système vCenter volumineux comptant plus de 6 000 VM avec flux. Cette option figure sur le plan d'évolution.

Quelle quantité d'espace disque est nécessaire sur la plate-forme 1 ?

La plate-forme 1 requiert davantage d'espace disque que les autres nœuds du cluster, car certaines données de configuration y sont stockées uniquement.

Que se passe-t-il si l'espace disque est insuffisant sur l'un des nœuds ?

L'interface utilisateur affichera des messages d'erreur lorsque l'espace disque sur un nœud de plate-forme atteint un certain seuil. Ajoutez de l'espace disque au nœud de plate-forme en vous connectant au système vCenter.

Combien de fois les données sont-elles répliquées dans le cluster ?

Le mécanisme de réplication des données dépend des composants présents dans le nœud de plate-forme.

Comment les clusters fonctionnent-ils ?

- Tous les proxys d'un déploiement se connectent à une plate-forme (plate-forme 1). La connectivité entre la plate-forme et le proxy est établie via HTTPS sur le port 443. Par conséquent, seul le port 443 est visible pour les proxys à partir de la plate-forme 1.

- Lorsqu'il reçoit les demandes du proxy, le nœud de plate-forme 1 équilibre la charge des demandes vers d'autres nœuds de plate-forme dans le cluster en mode Round Robin.
- Le nœud de plate-forme normalise les données et les place dans la file d'attente de messagerie à des fins de traitement par le moteur de calcul.
- Le moteur de calcul distribue les données sur tous les nœuds du cluster à l'aide du mécanisme de réplication des données. De cette manière, aucune donnée n'est perdue si l'un des nœuds (excepté plate-forme 1) est hors service dans le cluster.
- Certaines données de configuration sont stockées explicitement sur le nœud de plate-forme 1 qui n'est pas répliqué. C'est la raison pour laquelle la solution de haute disponibilité n'est pas prise en charge.

Comment le pipeline de traitement des données se comporte-t-il dans des conditions de limite, par exemple lorsque la communication entre le serveur proxy et la plate-forme est interrompue ?

- Quelle est la période de rétention par défaut ?

30 jours. Elle peut être prolongée dans l'interface utilisateur à l'aide de la licence d'entreprise. Remarque : si vous la prolongez, veillez à suivre les instructions relatives au disque.

- Comment les données sont-elles gérées sur le proxy ?

Toutes les données sur le proxy, y compris les données de flux, sont converties en message auto-descriptif (SDM, Self Describing Message) avant leur envoi vers la plate-forme. Cela inclut toutes les données de configuration, d'inventaire et de mesure provenant de n'importe quelle source de données. Si la plate-forme n'est pas accessible ou si le téléchargement de SDM vers la file d'attente Kafka échoue, elles sont écrites sur le disque de la VM proxy (sous `/var/BLOB_STORE`).

- À quel moment la purge des données démarre-t-elle sur le proxy ?

Dans le cas des données autres que de flux : 10 Go d'espace sont alloués au stockage des SDM sur le disque (`BLOB_STORE`). Lorsque ce magasin est rempli, le collecteur commence à supprimer les anciens SDM et ajoute les nouveaux au disque. La vitesse à laquelle cette limite est atteinte dépend de la taille des données collectées à partir de toutes les sources de données.

Dans le cas des données de flux : 15 Go d'espace sont alloués au stockage des flux bruts (sous `/var/flows/vds/nfcapd`). Une fois cet espace consommé, le processeur de flux commence à supprimer les anciens fichiers de flux. Avec un débit de flux bruts entrants d'environ 2 M/min, la rotation démarrerait après 10 heures.

- Quelle est la logique de la purge ?

Les plus anciens SDM sont supprimés en premier.

- À quel moment les nouvelles données cessent-elles d'être traitées dans le proxy ?

Jamais, le traitement continue tant que les services fonctionnent correctement.

- Supposons que la plate-forme est déconnectée du proxy et qu'aucune condition de purge n'est remplie ; toutes les données seront-elles rapprochées lors de la reconnexion de la plate-forme ?

Toutes les données stockées sur le disque seront envoyées vers la plate-forme. Elles doivent être toutes rapprochées, sauf si des conditions de perte de données existent sur la plate-forme. Vous trouverez plus d'informations sur ce point plus bas.

- Dans quelles conditions des pertes de données peuvent-elles se produire sur la plate-forme ?

La plate-forme commence à abandonner les SDM qui se trouvent dans la file d'attente Kafka depuis plus de 6 heures (18 heures dans le cas d'un cluster à 3 nœuds). Des données peuvent également être perdues si la file d'attente est saturée. Cela peut se produire lorsqu'un retard est généré dans le système et que le débit des données entrantes est élevé.

- Le premier SDM publié est-il le plus ancien ou le plus récent ?

Les plus anciens SDM sont envoyés en premier. Le produit jusqu'à la version v3.9 présente un problème qui entraîne une perte de données. Contactez GSS pour obtenir plus d'informations.

- Les données sont-elles stockées sur le disque du proxy, puis transmises à la plate-forme lorsqu'il n'existe aucun problème de communication ?

S'il n'existe aucun problème de communication, les SDM ne sont pas stockés sur le disque. Ils sont envoyés vers la plate-forme à partir de la mémoire même. Les données sont stockées sur le disque lorsque le proxy est informé d'un problème lors de l'envoi de SDM uniquement.

- En cas de problème, comment le proxy sait-il quel fichier de flux a été traité en dernier ?

Le processeur de flux gère le signet dans la base de données dans laquelle le fichier nfcapd a été traité pour la dernière fois.

- Quelle est la taille maximale d'un SDM pouvant être traitée sans problème ? Comment l'utilisateur peut-il savoir si la limite est atteinte ?

La taille du SDM est limitée à 15 Mo. À partir de la version v3.9, un événement est déclenché chaque fois que la plate-forme abandonne un SDM volumineux.

Qu'est-ce qu'IPFIX ?

IPFIX est un protocole IETF pour l'exportation d'informations de flux. Un flux est défini comme un ensemble de paquets transmis dans un intervalle de temps spécifique et partageant les valeurs 5 tuples : adresse IP source, port source, adresse IP de destination, port de destination et protocole. Les informations de flux peuvent inclure des propriétés telles que les horodatages, le nombre de paquets/d'octets, les interfaces d'entrée/sortie, les indicateurs TCP, l'ID VXLAN, les informations de flux encapsulées, etc. Le terme souvent utilisé pour le décrire est NetFlow. Toutefois, IPFIX est le protocole IETF standard.

Quelles sont les informations de flux exportées par le VDS ?

Un VDS dans un environnement vSphere peut être configuré pour exporter des informations de flux à l'aide d'IPFIX. Activez la surveillance de flux sur tous les groupes de ports connectés au VDS. Si les paquets entrent par le port X de VDS et en sortent par le port Y, un enregistrement de flux correspondant est émis si la surveillance de flux est activée sur le port Y. La direction de chaque enregistrement de flux est définie sur Egress.

Comment vRealize Network Insight utilise-t-il IPFIX ?

vRealize Network Insight utilise IPFIX VDS de VMware pour collecter des données de trafic réseau. Chaque session comprend deux chemins. Par exemple, la session A ↔ C contient des paquets A→C et des paquets C→A. Pour analyser les informations complètes d'une session, les données IPFIX sur les paquets dans les deux directions sont requises. Reportez-vous au diagramme suivant dans lequel VM-A est connecté à DVPG-A et dialogue avec VM-C. Ici, DVPG-A ne fournit que des données sur les paquets C→A, et DVPG-Uplink fournit des données sur les paquets A→C. Pour obtenir des informations complètes sur le trafic de A, IPFIX doit être activé sur DVPG-A, DVPG-uplink.

Comment dépanner la collecte de flux de vRealize Network Insight ?

- 1 Vérifiez que la surveillance NetFlow est **activée** sur le VDS spécifique et ses propriétés DVPG et Uplink, et que l'adresse IP de collecteur est celle du collecteur vRealize Network Insight.
- 2 Paquets IPFIX NetFlow abandonnés par un pare-feu (NSX, virtuel ou physique). Vérifiez que les paquets NetFlow destinés au port UDP 2055 sur l'adresse IP du collecteur vRealize Network Insight sont autorisés par tous les pare-feu présents sur le chemin entre l'hôte ESXi et le collecteur vRealize Network Insight.
- 3 L'hôte ESXi a cessé d'envoyer des paquets NetFlow IPFIX. L'hôte ESXi arrête d'envoyer des paquets NetFlow après un certain temps si le port UDP 2055 n'est pas accessible. Cela peut se produire lorsque le pare-feu abandonne les paquets.
- 4 Le collecteur vRealize Network Insight n'est pas accessible par l'hôte ESXi en raison d'un problème de routage réseau. Vérifiez qu'un chemin approprié existe entre l'hôte ESXi et le collecteur vRealize Network Insight.

Quels articles de la base de connaissances VMware liés à IPFIX dois-je connaître ?

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

Quand un service est-il considéré comme partagé ?

Protocole	Port
DNS	53
Bootpc	68
Kerberos	88
Pop3	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636

Protocole	Port
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269