

# Installation 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](http://www.vmware.com)

**VMware France SAS.**  
Tour Franklin  
100-101 Terrasse Boieldieu  
92042 Paris La Défense 8 Cedex  
France  
[www.vmware.com/fr](http://www.vmware.com/fr)

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

# Table des matières

## À propos du Guide d'installation de vRealize Network Insight 5

### 1 Préparation à l'installation 6

Recommandations et configuration système requise 6

Privilèges 10

Ports système 11

Ports de communication réseau 19

Versions et produits pris en charge 21

### 2 Installation de vRealize Network Insight 25

Workflow de l'installation 25

Déploiement de l'OVA de la plate-forme vRealize Network Insight 27

Déploiement à l'aide de vSphere Web Client 27

Déploiement à l'aide d'un client Windows vSphere natif 29

Activation de la licence 31

Générer un secret partagé 31

Configuration du collecteur Network Insight (OVA) 32

Déploiement à l'aide de vSphere Web Client 32

Déploiement à l'aide d'un client Windows vSphere natif 34

Configuration du collecteur Network Insight (AMI) dans AWS pour VMware SD-WAN 35

Déploiement de collecteurs supplémentaires dans une configuration existante 37

### 3 Accès à vRealize Network Insight à l'aide de la licence d'évaluation 38

Ajout d'une instance de vCenter Server 38

Analyse des flux de trafic 40

Génération d'un rapport 40

### 4 Planification de l'évolutivité verticale de votre déploiement 41

Planification de l'évolutivité verticale du cluster de plate-forme 41

Planification de l'évolutivité verticale du collecteur 42

Augmenter la taille de brique de votre installation 43

### 5 Mise à niveau de vRealize Network Insight 45

Mise à niveau en ligne 46

Mise à niveau hors ligne d'un simple clic 49

Mise à niveau via la CLI 52

### 6 Désinstallation de vRealize Network Insight 55

Suppression de l'adresse IP du collecteur lorsque NetFlow est activé dans le système vCenter  
56

Suppression de l'adresse IP du collecteur lorsque NetFlow est activé dans NSX 56

# À propos du Guide d'installation de vRealize Network Insight

Le Guide d'installation de *vRealize Network Insight* s'adresse aux administrateurs ou aux spécialistes chargés de l'installation de vRealize Network Insight.

## Public visé

Ces informations sont destinées aux administrateurs ou aux spécialistes responsables de l'installation de vRealize Network Insight. Elles sont destinées aux administrateurs de machines virtuelles expérimentés qui maîtrisent les applications de gestion d'entreprise et les opérations de centres de données.

# Préparation à l'installation

# 1

Avant d'installer vRealize Network Insight, préparez l'environnement de déploiement pour répondre à la configuration système requise.

Ce chapitre contient les rubriques suivantes :

- [Recommandations et configuration système requise](#)
- [Versions et produits pris en charge](#)

## Recommandations et configuration système requise

Pour obtenir des performances optimales, respectez les recommandations minimales relatives au déploiement.

### Recommandations relatives au déploiement de la plate-forme

Tableau 1-1. Spécifications pour la taille des briques de plate-forme

Taille de bloc	Cœurs requis pour CPU 2,1 GHz	Cœurs requis pour CPU 2,3 GHz	Cœurs requis pour CPU 2,6 GHz	RAM	Disque
Moyenne	10	9	8	32 Go	1 To
Grande	15	14	12	48 Go	1 To
Très grand	20	18	16	64 Go	2 To

#### Note

- La réservation de la vitesse du CPU et de la RAM pour chaque nœud doit être de 100 % de la valeur spécifiée ci-dessus.
- Pour faire correspondre votre configuration à toutes les spécifications, vous devrez peut-être ajouter les ressources (RAM, disque, CPU). Reportez-vous aux sections <https://kb.vmware.com/s/article/53550> et [Augmenter la taille de brique de votre installation](#).

Tableau 1-2. Déploiement sans cluster - Capacité maximale

Taille de bloc	Nombre de machines virtuelles (en milliers)	Flux par jour (en millions)	Nombre total de flux (en millions)	Planification des flux (en millions)
Moyenne	4 000	1 000 000	4 000 000	2 000 000
Grande	6 000	2 000 000	8 000 000	4 000 000

Tableau 1-3. Déploiement sans cluster - Capacité maximale pour VMware SD-WAN

Taille de bloc	Nombre de dispositifs Edge (en milliers)	Flux par jour (en millions)	Nombre total de flux (en millions)
Moyenne	2 000	1 000 000	4 000 000
Grande	2 000	2 000 000	8 000 000

**Note**

- Le nombre de machines virtuelles inclut également les modèles sur le vCenter.
- Le nombre total de flux correspond au nombre maximal de flux que le système peut stocker pour la période de rétention.
- La planification des flux correspond au nombre total de flux pour lesquels le système peut effectuer une planification de sécurité.

Tableau 1-4. Déploiement avec cluster - Capacité maximale

Taille de bloc	Taille du cluster	Nombre de machines virtuelles (en milliers)	Flux par jour (en millions)	Nombre total de flux (en millions)	Planification des flux (en millions)	Nombre de dispositifs Edge pour VMware SD-WAN (en milliers)
Grande	3	10 000	2 000 000	8 000 000	4 000 000	4 000
Très grand	3	18 000	6 000 000	24 000 000	4 000 000	6 000

Tableau 1-4. Déploiement avec cluster - Capacité maximale (suite)

Taille de bloc	Taille du cluster	Nombre de machines virtuelles (en milliers)	Flux par jour (en millions)	Nombre total de flux (en millions)	Planification des flux (en millions)	Nombre de dispositifs Edge pour VMware SD-WAN (en milliers)
Très grand	5	30 000	10 000 000	40 000 000	4 000 000	10 000
Très grand	10	100 000	15 000 000	55 000 000	4 000 000	10 000

**Note**

- Le nombre de machines virtuelles inclut également les modèles sur le vCenter.
- La taille du cluster correspond au nombre total de nœuds du cluster.
- Le nombre total de flux correspond au nombre de flux dans le système pour la période de rétention.
- La requête pour déterminer le nombre total de flux est `count of flows in last 31 days`, en partant du principe que la période de rétention est de 31 jours.
- La planification des flux correspond au nombre total de flux pour lesquels le système peut effectuer une planification de sécurité.

**Recommandations relatives au déploiement du collecteur**

Tableau 1-5. Spécifications pour la taille des briques du collecteur

Taille de bloc	Cœurs requis pour le CPU 2,1 GHz	Cœurs requis pour le CPU 2,3 GHz	Cœurs requis pour le CPU 2,6 GHz	RAM	Disque
Moyenne	5	5	4	12 Go	200 Go
Grande	10	9	8	16 Go	200 Go
Très grand	10	9	8	24 Go	200 Go

**Note** La réservation de la vitesse du CPU et de la RAM pour chaque nœud doit être de 100 % de la valeur spécifiée ci-dessus.



Tableau 1-6. Déploiement du collecteur - Capacité maximale

Taille de collecteur	Nombre de machines virtuelles (en milliers)	Flux par jour (en millions)	Nombre de flux dans 4 jours (en millions)	Nombre de dispositifs Edge pour VMware SD-WAN (en milliers)
Moyenne	4 000	2 500 000	3 250 000	4 000
Grande	10 000	5 000 000	6 500 000	6 000
Très grand	20 000	10 000 000	13 000 000	10 000

**Note**

- Le nombre de machines virtuelles inclut également les modèles sur le vCenter.
- Pour un déploiement unique incluant plusieurs collecteurs, la limite du nombre total de flux dans les collecteurs est basée sur la capacité de la plate-forme.

**Autres recommandations et conditions requises**

- La différence de temps maximale entre les nœuds de la plate-forme doit être inférieure à 30 secondes.
- La disponibilité du service NTP est critique pour les opérations système. Veillez à ne pas redémarrer le nœud de plate-forme ni le nœud de collecteur lorsque le service NTP n'est pas disponible.
- Lorsque les ressources de calcul existantes sont entièrement utilisées par les autres processus sur la plate-forme, vRealize Network Insight se bloque et n'est pas récupéré automatiquement. Si les services ne sont pas récupérés, redémarrez le nœud de la plate-forme.
- Si la latence réseau entre le nœud de plate-forme et le serveur de mise à niveau est supérieure à 500 ms, la mise à niveau de vRealize Network Insight peut rencontrer une erreur. Par conséquent, la latence du réseau doit être inférieure à 500 ms.
- La latence de disque recommandée pour obtenir des performances optimales est de 5 ms. Si la latence de disque est supérieure à 5 ms, les performances du système se dégradent.
- L'IOPS sur disque par seconde recommandé est de 7 500.

**Navigateur Web pris en charge**

- Google Chrome : les deux dernières versions.
- Mozilla Firefox : les deux dernières versions.

## Recommandations relatives à la prise en charge de la haute disponibilité

Vous pouvez personnaliser les options vSphere HA pour activer la haute disponibilité de vSphere.

- **Échec de l'hôte** - Redémarrer les VM
- **Isolation de l'hôte** - Désactivée
- **Invité sans signal de pulsation** - Désactivé

## Privilèges

### Privilèges requis pour les sources de données

- Privilèges requis pour la configuration et l'utilisation d'IPFIX
  - Informations d'identification vCenter Server avec privilèges :
    - Distributed Switch : Modifier
    - Groupe dvPort : Modifier
  - Les rôles prédéfinis dans vCenter Server doivent disposer des privilèges suivants, attribués au niveau racine et devant être propagés aux rôles enfants :
    - System.Anonymous
    - System.Read
    - System.View
    - global.settings

Pour en savoir plus sur les rôles dans vCenter, reportez-vous à la section Utilisation des rôles pour l'attribution de privilèges du guide de *Sécurité vSphere*.

- Privilèges requis pour le fournisseur de données NSX Manager
  - Le fournisseur de données NSX Manager requiert le rôle **Enterprise**.
  - Si l'interface de ligne de commande centrale est activée, les informations d'identification `system admin` sont requises pour le fournisseur de données NSX Manager.
- Privilèges utilisateur requis sur les commutateurs Cisco pour la collecte de mesures
  - vRealize Network Insight peut collecter des données de mesure via SNMP ainsi que la configuration via SSH à partir de commutateurs Cisco. La plate-forme UCS des commutateurs Cisco requiert l'utilisation de SSH et de l'API pour la collecte.

Tableau 1-7.

Type de données	Privilèges utilisateur
Données de configuration	Lecture seule
Données de mesure	SNMP en lecture seule

Tableau 1-7. (suite)

Type de données	Privilèges utilisateur
	Communauté SNMP en lecture seule SNMPv2
	SNMPv3 en lecture seule

## Ports système

La liste suivante répertorie les ports requis pour la communication entrante vRealize Network Insight :

### Ports pour la configuration du cluster de plate-forme

Tableau 1-8.

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Client SSH	Plate-forme	22	SSH	Accès à l'interface de ligne de commande ou à l'hôte	Non	Oui	Authentification par clé SSH ou utilisateur/mot de passe
Navigateur client Web et collecteur vRNI	Plate-forme	443	HTTPS	Accès à l'interface utilisateur/API et communication avec le collecteur vRNI	Oui	Oui	Canal SSL chiffré à l'aide du certificat SHA2 basé sur la clé 2048b RSA (ou certificat personnalisé configuré par l'utilisateur). Les messages transmis de la plate-forme vers la collecteur sur ce canal sont également chiffrés à l'aide de la fonction HMAC.

Tableau 1-8. (suite)

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Plate-forme	Plate-forme	2181	HTTP	Communication entre les serveurs ZooKeeper sur d'autres nœuds (dans le cas d'un cluster). Stocke les informations de métadonnées (données Znode)	Non	Non	
Plate-forme	Plate-forme	2888	HTTP	Utilisé pour se connecter au leader ZooKeeper	Non	Non	
Plate-forme	Plate-forme	3000	HTTP	Utilisé pour les notifications par e-mail	Oui	Non	
Plate-forme	Plate-forme	3888	HTTP	Utilisé pour la sélection du leader ZooKeeper	Oui	Non	
Plate-forme	Plate-forme	5432	jdbc	Stockage des données de configuration de VM et des métadonnées d'infrastructure	Oui	Non	
Plate-forme	Plate-forme	8020	TCP/RPC	Communication entre d'autres nœuds de nom et des nœuds de données	Oui	Non	

Tableau 1-8. (suite)

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Plate-forme	Plate-forme	8025	HTTP	Les gestionnaires de nœuds utilisent ce port pour se connecter au gestionnaire de ressources.	Non	Non	
Plate-forme	Plate-forme	8030	HTTP	Utilisé par le gestionnaire de ressources pour la planification des tâches.	Non	Non	
Plate-forme	Plate-forme	8032	HTTP	Adresse de l'interface du gestionnaire d'applications dans le gestionnaire de ressources	Non	Non	
Plate-forme	Plate-forme	8033	HTTP	Adresse de l'interface d'administration du gestionnaire de ressources	Non	Non	
Plate-forme	Plate-forme	8042	HTTP	Adresse de l'application Web du gestionnaire de nœuds	Non	Non	
Plate-forme	Plate-forme	8080	HTTP	Répond aux demandes d'interface utilisateur.	Oui	Non	

Tableau 1-8. (suite)

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Plate-forme	Plate-forme	8088	HTTP	Adresse HTTP de l'application Web du gestionnaire de ressources	Non	Non	
Plate-forme	Plate-forme	8480	TCP/RPC	Serveur HTTP JournalNod e	Non	Non	
Plate-forme	Plate-forme	8485	TCP/RPC	Répertoire de données de modifications partagées via HDFS	Non	Non	
Plate-forme	Plate-forme	9090	HTTP	Répond aux demandes du collecteur et envoie les commandes au collecteur.	Oui	Oui (protégé via Nginx)	
Plate-forme	Plate-forme	9092	Binaire via TCP	Port sur lequel d'autres intermédiaires communiquent	Oui	Non	
Plate-forme	Plate-forme	9200-9300	HTTP	Répond aux demandes de recherche. ES utilise une plage de ports à écouter ; si le port 9200 est inaccessible, il utilise le prochain port disponible.	Oui	Non	

Tableau 1-8. (suite)

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Plate-forme	Plate-forme	9300	HTTP	Répond aux demandes de recherche. ES utilise une plage de ports à écouter ; si le port 9200 est inaccessible, il utilise le prochain port disponible.	Oui	Non	
Plate-forme	Plate-forme	30000:65535	TCP	Plage de ports éphémères utilisée par divers processus pour établir la connexion TCP avec les autres processus	Non	Non	
Plate-forme	Plate-forme	60000	IPC	Utilisé pour la communication entre d'autres services HBase primaires et des serveurs de région	Oui	Non	
Plate-forme	Plate-forme	60010	HTTP	Utilisé pour l'interface utilisateur Web de HBase	Non	Non	

Tableau 1-8. (suite)

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Plate-forme	Plate-forme	60020	IPC	Communication entre le service HBase primaire et le serveur de région	Oui	Non	
Plate-forme	Plate-forme	4500-4510	TCP	Communication entre les serveurs Foundation DB s'exécutant sur différentes plates-formes	Oui	Non	



## Ports pour la configuration de plate-forme unique

Tableau 1-9.

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Client SSH	Plate-forme	22	SSH	Accès à l'interface de ligne de commande ou à l'hôte	Non	Oui	Authentification par clé SSH ou utilisateur/mot de passe
Navigateur client Web et collecteur vRNI	Plate-forme	443	HTTPS	Accès à l'interface utilisateur/API et communication avec le collecteur vRNI	Oui	Oui	Canal SSL chiffré à l'aide du certificat SHA2 basé sur la clé 2048b RSA (ou certificat personnalisé configuré par l'utilisateur). Les messages transmis de la plate-forme vers la collecteur sur ce canal sont également chiffrés à l'aide de la fonction HMAC.

## Ports pour le serveur de collecteur

Tableau 1-10.

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Client SSH	Collecteur	22	SSH	Accès à l'interface de ligne de commande ou à l'hôte	Non	Oui	Authentification par clé SSH ou utilisateur/mot de passe
Collecteur vRNI	Plate-forme	443	HTTPS	Canal de communication principale avec la plate-forme	Oui	Oui	Canal SSL chiffré à l'aide du certificat SHA2 basé sur la clé 2048b RSA (ou certificat personnalisé configuré par l'utilisateur). Les messages transmis de la plate-forme vers la collecteur sur ce canal sont également chiffrés à l'aide de la fonction HMAC.
Redirecteur de flux	Collecteur	UDP 2055	NetFlow/IPFIX	Les flux de la cible sont envoyés vers ce port.	Oui	Non	
Redirecteur de flux	Collecteur	UDP 6343	sFlow	Les flux de la cible sont envoyés vers ce port.	Oui	Non	

Tableau 1-10. (suite)

Source	Cible	Port	Protocole	Objectif	Sensible	SSL	Authentification
Hôte ESXi	Collecteur	1991	TCP	Collecte de la mesure de latence de l'infrastructure virtuelle, par exemple : latence entre vNIC et pNIC, VTEP et VTEP, TEP et TEP, etc.	Non	Non	
Dell OS10	Collecteur	50000	GRPC	Réception des informations de télémétrie des statistiques de tampon des périphériques Dell OS10	Non	Non	

## Ports de communication réseau

Le tableau suivant répertorie les ports et les protocoles utilisés pour la communication réseau dans vRealize Network Insight.

Vous pouvez également voir la liste des ports sur <https://ports.vmware.com/home/vRealize-Network-Insight>.

Tableau 1-11.

Objectif	De	Pour	Port	Protocole
Communication entre les VM de vRealize Network Insight	Collecteur	Plate-forme <b>Note</b> Le port doit être activé pour toutes les plates-formes.	443	HTTPS
Services nécessitant l'accès à Internet	Plate-forme et collecteur	svc.ni.vmware.com support2.ni.vmware.com reg.ni.vmware.com	443	HTTPS

Tableau 1-11. (suite)

Objectif	De	Pour	Port	Protocole
Communication des différents services configurés	Plate-forme	Serveur LDAP	389, 636	LDAP et LDAPS
		Serveur SNMP	Configurable	SNMP
	Plate-forme et collecteur	Serveur DNS	53	UDP
		Serveur Syslog	Configurable	
	Hôtes ESXi	Collecteur	2055	TCP
	Hôtes ESXi	Collecteur	1991	
Communication avec AWS en tant que source de données	Collecteur	AWS (*.amazonaws.com)	443	HTTPS
Communiquer avec le service de télémétrie	Navigateur	URL de télémétrie <a href="https://vcsa.vmware.com">https://vcsa.vmware.com</a>	433	HTTPS
Communication avec d'autres sources de données dans le centre de données	Collecteur	Commutateurs Arista	161 et 22	SNMP et SSH
		Azure	443	HTTPS
		Commutateurs Brocade	161 et 22	SNMP et SSH
		Pare-feu Check Point	443	HTTPS
		Cisco Nexus	161 et 22	SNMP et SSH
		Cisco UCS (Unified Computing System)	161, 22 et 443	SNMP, SSH et HTTPS
		Commutateurs Cisco Catalyst	161 et 22	SNMP et SSH
		Commutateurs Cisco ACI	161	SNMP
		Contrôleur Cisco APIC	161 et 443	HTTPS et SNMP
		Commutateurs Dell	161 et 22	SNMP et SSH
		Dell OS10	50000	TCP
		VeloCloud	443, 2055	HTTPS
		HP	22	SSH
		Commutateurs Juniper	161 et 22	SNMP et SSH
		Palo Alto Networks	443	HTTPS
		VMware vSphere	443	HTTPS

Tableau 1-11. (suite)

Objectif	De	Pour	Port	Protocole
		VMware NSX - V (tous les composants)	22 et 443	SSH et HTTPS
		NSX-T Manager	443	TCP
		serveur d'API VMware PKS	8443 et 9021	TCP
		Serveur d'API Kubernetes	8443	TCP
		vRealize Log Insight	443	HTTPS
		FortiManager Fortinet	443	HTTPS

## Versions et produits pris en charge

vRealize Network Insight prend en charge plusieurs produits et versions.

Source de données	Version/modèle	Protocole de connexion	Privilèges/autorisations
Amazon Web Services (licence d'entreprise uniquement)	Non applicable	HTTPS	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Commutateurs Arista	7050TX, 7250QX, 7050QX-32S, 7280SE-72	SSH, SNMP	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Abonnement Azure	Non applicable	HTTPS	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Commutateurs Brocade	VDX 6740, VDX 6940, MLX, MLXe	SSH, SNMP	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Pare-feu Check Point	Check Point R80, R80.10, R80.20, R80.30	HTTPS, SSH	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Cisco ACI	3.2	HTTPS (vers le contrôleur APIC) SNMP (vers le contrôleur APIC et les commutateurs ACI)	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Cisco ASA	Série X avec SE 9.4	SSH, SNMP	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Cisco Catalyst	3000, 3750, 4500, 6000, 6500	SSH, SNMP	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.

Source de données	Version/modèle	Protocole de connexion	Privilèges/autorisations
Cisco Nexus	3000, 5000, 6000, 7000, 9000	SSH, SNMP	Utilisateur en lecture seule Utilisateur SNMP en lecture seule
Cisco UCS (Unified Computing System)	Serveurs lames de série B, baie de serveurs de série C, châssis, Fabric interconnect	UCS Manager : HTTPS UCS Fabric : SSH, SNMP	Utilisateur en lecture seule Utilisateur SNMP en lecture seule
Commutateurs Dell	FORCE10 MXL 10, FORCE10 S6000, S4048, Z9100, S4810, PowerConnect 8024, Dell OS10	SSH, SNMP	Utilisateur en lecture seule Utilisateur SNMP en lecture seule
FortiManager Fortinet	6.0.1	HTTPS	L'utilisateur doit disposer : <ul style="list-style-type: none"> <li>■ au minimum du rôle <b>d'utilisateur avec accès restreint</b> autorisé à accéder à tous les domaines d'administration (ADOM) et modules de stratégie.</li> <li>■ de l'accès <b>en lecture rpc-permit</b> activé à partir de l'interface de ligne de commande (CLI).</li> </ul>
F5 BIG - IP	12.1.2 et versions ultérieures	HTTPS, SSH, SNMP	L'utilisateur doit disposer au minimum du rôle invité. De plus, l'accès TMSH doit être activé et toutes les partitions doivent être accessibles. F5 BIG-IP prend en charge le routage et l'équilibrage de charge.
HP	HP Virtual Connect Manager 4.41, HP OneView 3.0	HP OneView 3.0 : HTTPS HP Virtual Connect Manager 4.41 : SSH	Utilisateur en lecture seule
Moteur cloud d'Huawei	6800, 7800, 8800	SSH, SNMP	Utilisateur en lecture seule Utilisateur SNMP en lecture seule
Infoblox	Infoblox NIOS version 8.0, 8.1, 8.2	HTTPS	Utilisateur en lecture seule avec accès à l'interface API Autorisations en lecture seule pour les types d'objet DNS comme suit : <ul style="list-style-type: none"> <li>■ Type d'autorisation - DNS</li> <li>■ Ressources - Enregistrements A, zones DNS, vues DNS</li> </ul>
Commutateurs Juniper	EX3300, série QFX 51xx (JunOS v12 et v15, sans QFabric)	Netconf, SSH, SNMP	Utilisateur en lecture seule Utilisateur SNMP en lecture seule

Source de données	Version/modèle	Protocole de connexion	Privilèges/autorisations
Kubernetes	<ul style="list-style-type: none"> <li>■ 1.12 sur NSX-T 2.3.1</li> <li>■ 1.12 sur NSX-T 2.3.2</li> <li>■ 1.13 sur NSX-T 2.3.2</li> </ul>	HTTPS	L'utilisateur doit disposer du rôle d'administrateur de cluster avec des autorisations de lecture.
OpenShift	3.1.1	HTTPS	Consultez la section Ajouter des sources de données dans le Guide de l'utilisateur.
Palo Alto Networks	Panorama 7.0.x, 7.1, 8.x, 9.0	HTTPS	L'utilisateur doit disposer du rôle d'administrateur avec accès à l'API XML. Pour plus d'informations, consultez la section Palo Alto Networks du <i>Guide de l'utilisateur de vRealize Network Insight</i> .
ServiceNow	Londres	HTTPS	L'utilisateur doit disposer du rôle d'administrateur.
VMware SD-WAN	VeloCloud Orchestrator et Edge version 3.3.1 et versions ultérieures	HTTPS	<p>L'utilisateur doit avoir un <b>rôle de compte</b> avec l'une des autorisations suivantes :</p> <ul style="list-style-type: none"> <li>■ <b>Super utilisateur</b></li> <li>■ <b>Administrateur standard</b></li> <li>■ <b>Support client</b></li> </ul>
VMC on AWS - vCenter	<p>M8 et versions ultérieures</p> <p><b>Note</b> Seuls les SDDC VMware Cloud on AWS basés sur NSX-T sont pris en charge.</p>	HTTPS	<p>L'utilisateur doit avoir l'autorisation suivante :</p> <ul style="list-style-type: none"> <li>■ <b>Administrateur de cloud</b> : pour ajouter une source de données et activer IPFIX.</li> </ul>
VMC on AWS - NSX Manager	<p>M8 et versions ultérieures</p> <p><b>Note</b> Seuls les SDDC VMware Cloud on AWS basés sur NSX-T sont pris en charge.</p>	HTTPS	<p>L'utilisateur doit avoir l'une des autorisations suivantes :</p> <ul style="list-style-type: none"> <li>■ <b>Membre de l'organisation.Administrateur</b> : pour ajouter une source de données et activer IPFIX.</li> <li>■ <b>Membre de l'organisation.Administrateur .Administrateur NSX Cloud</b> : pour ajouter une source de données et activer IPFIX.</li> <li>■ <b>Membre de l'organisation.VMware Cloud on AWS (tous les rôles)</b> : pour ajouter une source de données et activer IPFIX.</li> <li>■ <b>Membre de l'organisation.Auditeur de NSX Cloud</b> : pour ajouter une source de données.</li> </ul>

Source de données	Version/modèle	Protocole de connexion	Privilèges/autorisations
VMware Identity Manager	3.3 et versions ultérieures	HTTPS	L'utilisateur doit disposer du rôle d'administrateur.
VMware PKS	<a href="#">Versions prises en charge</a>		L'utilisateur doit avoir les autorisations du rôle d'administrateur de cluster - <code>pks.clusters.admin</code> .
VMware NSX Manager (VMware NSX-V)	<a href="#">Versions prises en charge</a>	SSH, HTTPS	Reportez-vous à la section Collecte de données Edge du <i>Guide de l'utilisateur de vRealize Network Insight</i> .
VMware NSX-T Manager	2.4. Pour connaître les autres versions prises en charge, reportez-vous à la section <a href="#">Versions de prises en charge</a>	HTTPS	Utilisateur en lecture seule
VMware vRealize Log Insight	<a href="#">Versions prises en charge</a>	HTTPS	L'utilisateur API doit disposer d'autorisations pour installer, configurer et gérer le pack de contenu.
VMware vSphere	<a href="#">Versions prises en charge</a> Pour IPFIX, la version de VMware ESXi est requise : <ul style="list-style-type: none"> <li>■ 5.5 Update 2 (Build 2068190) et versions ultérieures</li> <li>■ 6.0 Update 1b (Build 3380124) et versions ultérieures</li> <li>■ VMware VDS 5.5 et versions ultérieures</li> </ul> <p><b>Note</b> VMware Tools doit être installé sur toutes les machines virtuelles du centre de données pour identifier le chemin de VM vers VM.</p>	HTTPS	Utilisateur en lecture seule Privilèges requis pour la configuration et l'utilisation d'IPFIX Informations d'identification vCenter Server avec privilèges : Distributed Switch: Modify dvPort group: Modify Les rôles prédéfinis dans vCenter Server doivent disposer des privilèges suivants, attribués au niveau racine et devant être propagés aux rôles enfants : System.Anonymous System.Read System.View global.settings

### Note

- Les systèmes d'exploitation pris en charge pour les périphériques Cisco ASA, ACI, Catalyst et Nexus sont iOS/NX-OS et la version UCSM pour les périphériques Cisco UCS.
- Le système d'exploitation pris en charge pour Arista est Arista EOS.



# Installation de vRealize Network Insight

## 2

Vous pouvez déployer vRealize Network Insight à l'aide de vSphere Web Client ou d'un client Windows vSphere natif.

---

**Note** Après le déploiement de l'OVA de la plate-forme vRealize Network Insight, vérifiez si l'adresse IP statique spécifiée est définie sur le système vCenter Server.

---

Pour automatiser l'installation, la configuration, la mise à niveau, les correctifs, la gestion de la configuration, la correction et la santé des décalages au sein d'une console unique, vous pouvez utiliser vRealize Suite Lifecycle Manager. Si vous êtes un nouvel utilisateur, cliquez ici pour installer [vRealize Suite Lifecycle Manager](#). Il fournit aux responsables informatiques des ressources d'administrateur de cloud afin qu'ils puissent se concentrer sur les initiatives stratégiques, tout en améliorant le retour sur investissement (TTV), la fiabilité et la cohérence.

Vous pouvez également installer et mettre à niveau vRealize Network Insight à l'aide de vRealize Suite Lifecycle Manager. Pour plus d'informations, reportez-vous au [Guide d'installation, de mise à niveau et de gestion de vRealize Suite Lifecycle Manager](#).

Ce chapitre contient les rubriques suivantes :

- [Workflow de l'installation](#)
- [Déploiement de l'OVA de la plate-forme vRealize Network Insight](#)
- [Activation de la licence](#)
- [Générer un secret partagé](#)
- [Configuration du collecteur Network Insight \(OVA\)](#)
- [Configuration du collecteur Network Insight \(AMI\) dans AWS pour VMware SD-WAN](#)
- [Déploiement de collecteurs supplémentaires dans une configuration existante](#)

## Workflow de l'installation

Pour installer vRealize Network Insight, installez l'OVA de la plate-forme, activez la licence, générez un secret partagé et configurez le fichier OVA du collecteur.

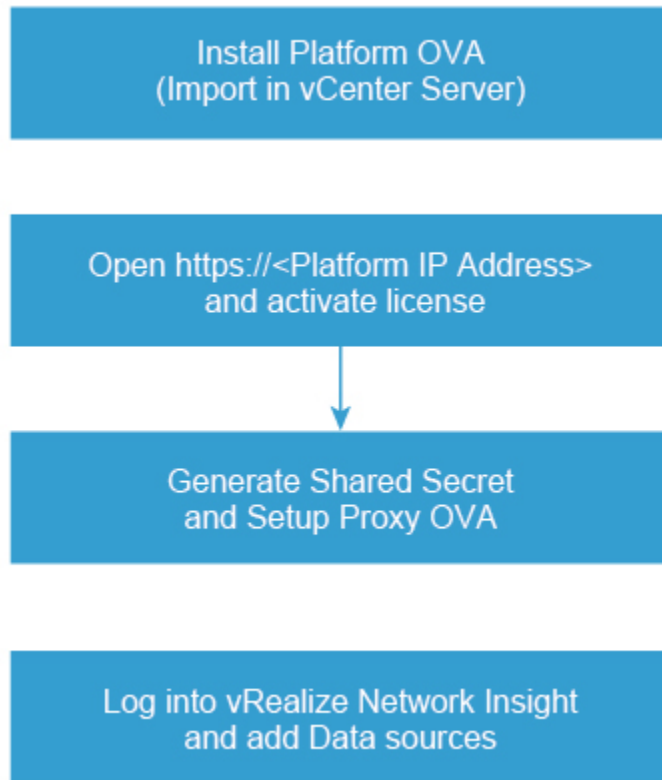
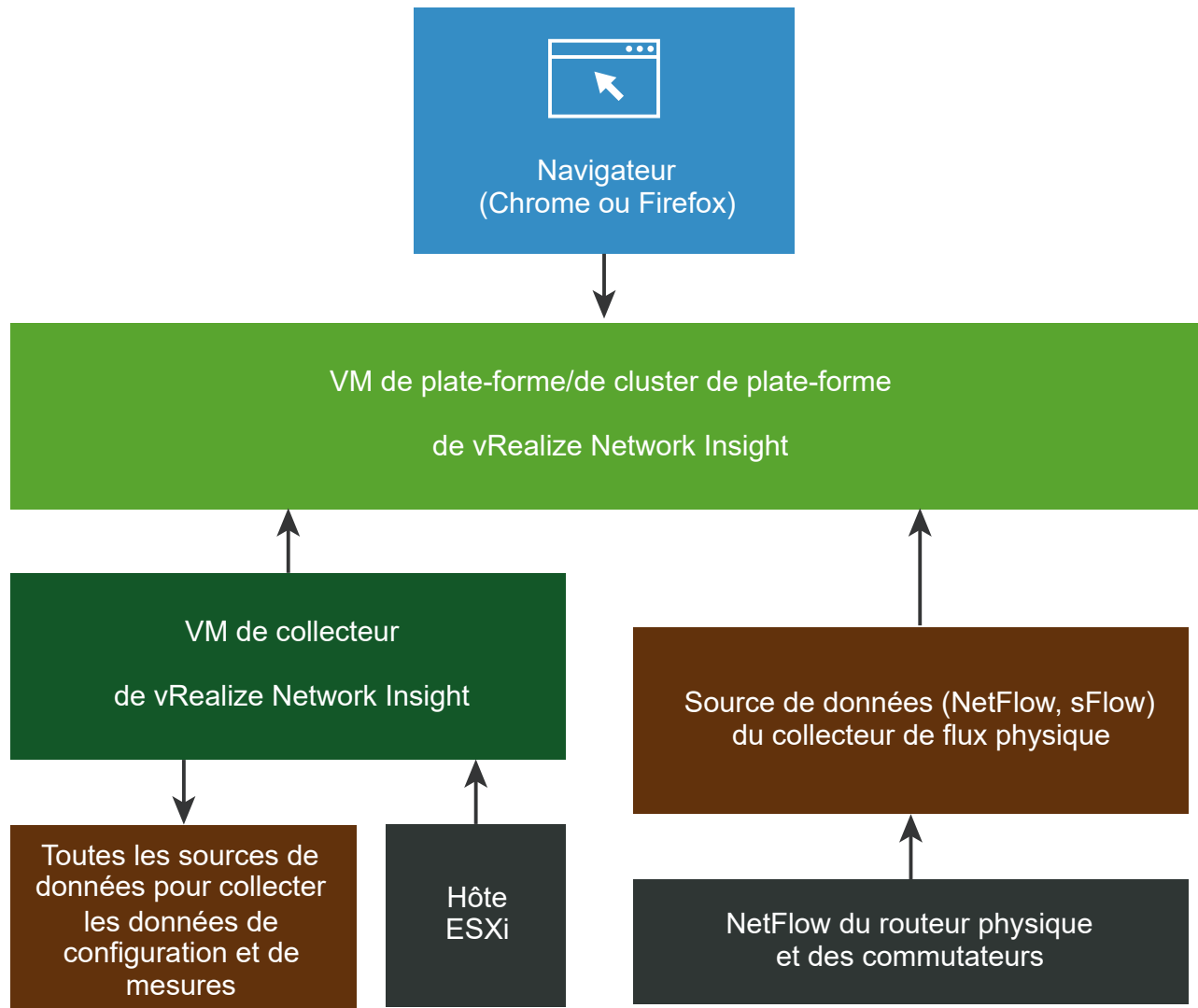


Diagramme du déploiement simplifié de vRealize Network Insight :



## Déploiement de l'OVA de la plate-forme vRealize Network Insight

Vous pouvez importer l'OVA de la plate-forme vRealize Network Insight vers votre système vCenter Server.

**Note** Le déploiement de l'OVA de la plate-forme vRealize Network Insight sur le SDDC VMC n'est pas pris en charge.

## Déploiement à l'aide de vSphere Web Client

Vous pouvez déployer vRealize Network Insight à l'aide de vSphere Web Client.

## Procédure

- 1 Cliquez avec le bouton droit sur le **centre de données** sur lequel vous souhaitez installer le dispositif et sélectionnez **Déployer le modèle OVF**.
- 2 Entrez l'URL pour télécharger et installer le module OVA ou recherchez l'emplacement source du module OVA.
- 3 Entrez le nom de l'OVA. Sélectionnez le dossier de destination pour le déploiement.
- 4 Sélectionnez un hôte, un cluster ou un pool de ressources sur lequel vous souhaitez exécuter le modèle déployé.
- 5 Vérifiez les informations du modèle OVF.
- 6 Lisez le contrat de licence d'utilisateur final et cliquez sur **Accepter**.
- 7 Sélectionnez une configuration de déploiement. Cliquez sur **Suivant**.
- 8 Sélectionnez l'emplacement pour stocker les fichiers pour le modèle de déploiement. Sélectionnez **Provisionnement dynamique** comme format de disque virtuel. Sélectionnez la banque de données ou les clusters de banques de données dans lesquels vous souhaitez stocker les fichiers. Cliquez sur **Suivant**.
- 9 Spécifiez le réseau que la VM déployée utilisera.  
  
Le réseau sélectionné doit autoriser le dispositif à accéder à Internet pour obtenir une assistance et effectuer une mise à niveau.
- 10 Pour personnaliser le modèle de déploiement, vous devrez configurer manuellement le dispositif à l'aide de la console de machine virtuelle. Cliquez sur **Suivant**.
- 11 Vérifiez les détails de la configuration et cliquez sur **Terminer**.
- 12 [Augmenter la taille de brique de votre installation](#) pour correspondre aux recommandations et exigences du système.
- 13 Une fois la plate-forme installée, démarrez la machine virtuelle et lancez la console.
- 14 Connectez-vous avec les informations d'identification de la console que vous voyez à l'écran et exécutez la commande `setup`.
- 15 Créez le mot de passe pour la connexion *support* et modifiez le mot de passe pour le compte *consoleuser*.

---

## Note

- Le mot de passer doit contenir au moins 6 caractères. Les guillemets simples (') ne sont pas autorisés.
  - Vous devez modifier régulièrement le mot de passe de *support* et de *consoleuser* pour être conforme à la stratégie de votre organisation.
-

16 Entrez les détails suivants pour configurer le réseau :

- a **Adresse IPv4** : deuxième adresse IP statique réservée
- b **Masque de réseau** : masque de sous-réseau pour l'adresse IP statique ci-dessus
- c **Passerelle par défaut** : passerelle par défaut de votre réseau
- d **DNS** : serveur DNS de votre environnement

---

**Note** Pour plusieurs serveurs DNS, assurez-vous qu'ils sont séparés par un espace.

---

- e **Liste de recherche de domaines** : domaine qui doit être ajouté pour les recherches DNS
- f Entrez `y` pour enregistrer la configuration.

17 Entrez le serveur NTP et assurez-vous qu'il peut atteindre la machine virtuelle. Les services ne parviendront pas à démarrer si l'heure NTP n'est pas synchronisée.

---

**Note** Dans le cas de plusieurs serveurs NTP, assurez-vous qu'ils sont séparés par des virgules.

---

18 (Facultatif) Pour configurer le proxy Web, entrez `y`.

19 Tous les services sont vérifiés.

20 Ajoutez de l'espace disque supplémentaire en fonction des besoins de votre configuration. Reportez-vous à la section <https://kb.vmware.com/s/article/53550>.

## Déploiement à l'aide d'un client Windows vSphere natif

Vous pouvez déployer vRealize Network Insight à l'aide d'un client Windows vSphere natif.

---

**Note** vRealize Network Insight 5.2 est la dernière version qui prend en charge le déploiement d'OVA à l'aide du client natif Windows vSphere. À partir de la version 5.3, vous pouvez continuer à utiliser vSphere Web Client pour déployer les fichiers OVA de vRealize Network Insight.

---

### Procédure

- 1 Sélectionnez **Fichier > Déployer le modèle OVF**.
- 2 Entrez l'URL pour télécharger et installer le package OVA depuis Internet ou parcourez votre ordinateur pour sélectionner l'emplacement source du module OVA.
- 3 Cliquez sur **Suivant** et vérifiez les détails du modèle OVF.
- 4 Lisez le contrat de licence d'utilisateur final et cliquez sur **Accepter**.
- 5 Fournissez un nom et un emplacement pour le modèle déployé. Cliquez sur **Suivant**.
- 6 Sélectionnez la **configuration de déploiement**.
- 7 Sélectionnez un **Hôte/cluster** sur lequel vous souhaitez exécuter le modèle déployé.
- 8 Sélectionnez le **Pool de ressources** dans lequel vous souhaitez déployer ce modèle.

- 9 Sélectionnez un stockage de destination pour les fichiers de machines virtuelles. Cliquez sur **Suivant**.
- 10 Spécifiez le format dans lequel vous souhaitez stocker les disques virtuels. Sélectionnez **Provisionnement dynamique** comme format de disque virtuel. Cliquez sur **Suivant**.
- 11 Spécifiez le réseau que le modèle déployé doit utiliser. Mappez le réseau d'OVA à votre inventaire.
- 12 Personnalisez le modèle pour le déploiement. Fournissez le secret partagé qui a été généré sur la page d'intégration. Vous devrez configurer manuellement le dispositif à l'aide de la console de machine virtuelle. Cliquez sur **Suivant**.
- 13 Vérifiez toutes les données de configuration. Sélectionnez **Mettre sous tension après le déploiement**. Cliquez sur **Terminer**.
- 14 [Augmenter la taille de brique de votre installation](#) pour correspondre à la section [Recommandations et configuration système requise](#).
- 15 Une fois le collecteur OVA installé, démarrez la machine virtuelle et lancez la console.
- 16 Connectez-vous avec les informations d'identification de la console que vous voyez à l'écran et exécutez la commande `setup`.
- 17 Créez le mot de passe pour la connexion *support* et modifiez le mot de passe pour le compte *consoleuser*.

---

#### Note

- Le mot de passer doit contenir au moins 6 caractères. Les guillemets simples (') ne sont pas autorisés.
  - Vous devez modifier régulièrement le mot de passe de *support* et de *consoleuser* pour être conforme à la stratégie de votre organisation.
- 

- 18 Entrez les détails suivants pour configurer le réseau :
  - a **Adresse IPv4** : deuxième adresse IP statique réservée
  - b **Masque de réseau** : masque de sous-réseau pour l'adresse IP statique ci-dessus
  - c **Passerelle par défaut** : passerelle par défaut de votre réseau
  - d **DNS** : serveur DNS de votre environnement

---

**Note** Pour plusieurs serveurs DNS, assurez-vous qu'ils sont séparés par un espace.

---

- e **Liste de recherche de domaine** : domaine qui doit être ajouté pour `dns lookup`.
- f Entrez `y` pour enregistrer la configuration.

- 19 Entrez le serveur NTP et assurez-vous qu'il peut atteindre la machine virtuelle. Les services ne parviendront pas à démarrer si l'heure NTP n'est pas synchronisée.

---

**Note** Dans le cas de plusieurs serveurs NTP, assurez-vous qu'ils sont séparés par des virgules.

---

- 20 (Facultatif) Pour configurer le proxy Web, entrez y.
- 21 Tous les services sont vérifiés.
- 22 Ajoutez de l'espace disque supplémentaire en fonction des besoins de votre configuration. Reportez-vous à la section <https://kb.vmware.com/s/article/53550>.

## Activation de la licence

Après l'installation de l'OVA de la plate-forme de vRealize Network Insight, ouvrez *https://<adresse IP de la plate-forme vRealize Network Insight>* dans le navigateur Web Chrome.

### Procédure

- 1 Entrez la clé de licence reçue dans l'e-mail de bienvenue.
- 2 Pour le nom de l'administrateur de l'interface utilisateur (`admin@local`), définissez le mot de passe.

---

**Note** Votre mot de passe doit être alphanumérique, contenir 8 caractères minimum et 100 caractères maximum. L'espace entre les caractères n'est pas autorisé.

---

- 3 Cliquez sur **Activer**.
- 4 Ajoutez le collecteur de vRealize Network Insight une fois la licence activée.

## Générer un secret partagé

Vous pouvez générer et importer le dispositif virtuel du collecteur vRealize Network Insight.

Générez un secret partagé et importez le dispositif virtuel du collecteur vRealize Network Insight :

### Procédure

- 1 Connectez-vous à l'interface utilisateur de vRealize Network Insight.
- 2 Développez **Infrastructure et support**, puis cliquez sur **Présentation et mises à jour**.
- 3 Faites défiler la liste vers le bas et cliquez sur **Ajouter une VM proxy**.

La boîte de dialogue **Ajouter un nouveau dispositif virtuel de collecteur de données Network Insight** s'affiche

- 4 Cliquez sur **Copier** pour copier le code secret partagé à partir de la boîte de dialogue, puis cliquez sur **Terminé**.

Vous en aurez besoin lors du déploiement de l'OVA collecteur de vRealize Network Insight.

## Configuration du collecteur Network Insight (OVA)

Vous pouvez configurer le collecteur vRealize Network Insight en important l'OVA sur votre système vCenter Server.

Suivez les étapes ci-dessous pour importer le OVA du collecteur vRealize Network Insight vers votre système vCenter Server.

### Déploiement à l'aide de vSphere Web Client

Vous pouvez importer le Collecteur OVA vRealize Network Insight à l'aide de vSphere Web Client.

#### Procédure

- 1 Cliquez avec le bouton droit sur le **centre de données** sur lequel vous souhaitez installer le dispositif et sélectionnez **Déployer le modèle OVF**.
- 2 Entrez l'URL pour télécharger et installer le module OVA depuis Internet ou parcourez pour sélectionner l'emplacement source d'OVA sur votre ordinateur.
- 3 Fournissez un nom et un emplacement pour le modèle déployé. Cliquez sur **Suivant**.
- 4 Sélectionnez une ressource (hôte ou cluster) sur laquelle vous souhaitez exécuter le modèle déployé. Cliquez sur **Suivant**.
- 5 Vérifiez tous les détails du modèle. Cliquez sur **Suivant**.
- 6 Lisez le contrat de licence d'utilisateur final et cliquez sur **Accepter**. Cliquez sur **Suivant**.
- 7 Sélectionnez une configuration de déploiement. Cliquez sur **Suivant**.
- 8 Sélectionnez l'emplacement dans lequel vous souhaitez stocker les fichiers du modèle déployé. Spécifiez le format dans lequel vous souhaitez stocker les disques virtuels. Sélectionnez **Provisionnement dynamique** comme format de disque virtuel. Sélectionnez la banque de données dans laquelle vous souhaitez installer les fichiers. Cliquez sur **Suivant**.
- 9 Spécifiez le réseau de destination pour le réseau source. Cliquez sur **Suivant**.
- 10 Personnalisez le modèle pour le déploiement. Fournissez le secret partagé généré à partir de l'interface utilisateur. Vous devrez configurer manuellement le dispositif à l'aide de la console de machine virtuelle. Cliquez sur **Suivant**.
- 11 Vérifiez toutes les données de configuration. Cliquez sur **Terminer**.
- 12 Une fois le collecteur OVA installé, démarrez la machine virtuelle et lancez la console.
- 13 Connectez-vous avec les informations d'identification de la console que vous voyez à l'écran et exécutez la commande `setup`.



- 14 Créez le mot de passe pour la connexion *support* et modifiez le mot de passe pour le compte *consoleuser*.

---

**Note**

- Le mot de passe doit contenir au moins 6 caractères. Les guillemets simples (') ne sont pas autorisés.
  - Vous devez modifier régulièrement le mot de passe de *support* et de *consoleuser* pour être conforme à la stratégie de votre organisation.
- 

- 15 Entrez les détails suivants pour configurer le réseau :

- a **Adresse IPv4** : deuxième adresse IP statique réservée
  - b **Masque de réseau** : masque de sous-réseau pour l'adresse IP statique ci-dessus
  - c **Passerelle par défaut** : passerelle par défaut de votre réseau
  - d **DNS** : serveur DNS de votre environnement
- 

**Note** Pour plusieurs serveurs DNS, assurez-vous qu'ils sont séparés par un espace.

---

- e **Liste de recherche de domaines** : domaine qui doit être ajouté pour les recherches DNS
- f Entrez *y* pour enregistrer la configuration.

- 16 Entrez le serveur NTP et assurez-vous qu'il peut atteindre la machine virtuelle. Les services ne parviendront pas à démarrer si l'heure NTP n'est pas synchronisée.

---

**Note** Dans le cas de plusieurs serveurs NTP, assurez-vous qu'ils sont séparés par des virgules.

---

- 17 (Facultatif) Pour configurer le proxy Web :

- a Entrez *y*.
- b Fournissez les détails du proxy Web.

- 18 Une vérification est effectuée pour voir si la clé secrète partagée a été configurée. Le collecteur est couplé à la plate-forme correspondante. Cette opération peut prendre quelques minutes.

- 19 Tous les services sont vérifiés.

- 20 Cliquez sur **Terminer**, une fois que le message **Proxy détecté !** s'affiche sur la page d'intégration. Il redirige vers la page de connexion.

## Déploiement à l'aide d'un client Windows vSphere natif

Vous pouvez importer le collecteur OVA vRealize Network Insight à l'aide d'un client Windows vSphere natif.

---

**Note** vRealize Network Insight 5.2 est la dernière version qui prend en charge le déploiement d'OVA à l'aide du client natif Windows vSphere. À partir de la version 5.3, vous pouvez continuer à utiliser vSphere Web Client pour déployer les fichiers OVA de vRealize Network Insight.

---

### Procédure

- 1 Sélectionnez **Fichier > Déployer le modèle OVF**.
- 2 Entrez l'URL pour télécharger et installer le package OVA depuis Internet ou parcourez votre ordinateur pour sélectionner l'emplacement source du module OVA.
- 3 Vérifiez les informations du modèle OVF. Cliquez sur **Suivant**.
- 4 Lisez le contrat de licence d'utilisateur final et cliquez sur **Accepter**. Cliquez sur **Suivant**.
- 5 Fournissez un nom et un emplacement pour le modèle déployé. Cliquez sur **Suivant**.
- 6 Sélectionnez une **Configuration de déploiement**. Cliquez sur **Suivant**.
- 7 Sélectionnez un **Hôte/cluster** sur lequel vous souhaitez exécuter le modèle déployé. Cliquez sur **Suivant**.
- 8 Sélectionnez le **Pool de ressources** dans lequel vous souhaitez déployer ce modèle. Cliquez sur **Suivant**.
- 9 Sélectionnez un stockage de destination pour les fichiers de machines virtuelles. Cliquez sur **Suivant**.
- 10 Spécifiez le format dans lequel vous souhaitez stocker les disques virtuels. Sélectionnez ensuite **Provisionnement dynamique** comme format de disque virtuel. Cliquez sur **Suivant**.
- 11 Spécifiez le réseau que le modèle déployé doit utiliser. Mappez le réseau d'OVA à votre inventaire.
- 12 Personnalisez le modèle pour le déploiement. Fournissez le secret partagé qui a été généré sur la page d'intégration. Vous devrez configurer manuellement le dispositif à l'aide de la console de machine virtuelle. Cliquez sur **Suivant**.
- 13 Vérifiez toutes les données de configuration. Sélectionnez **Mettre sous tension après le déploiement**. Cliquez sur **Terminer**.
- 14 Une fois le collecteur OVA installé, démarrez la machine virtuelle et lancez la console.
- 15 Connectez-vous avec les informations d'identification de console données. Exécutez la commande `setup`.
- 16 Créez le mot de passe pour la connexion à `support`. Modifiez le mot de passe pour `consoleuser`.

17 Entrez les détails suivants pour configurer le réseau :

- a **Adresse IPv4** : deuxième adresse IP statique réservée
- b **Masque de réseau** : masque de sous-réseau pour l'adresse IP statique ci-dessus
- c **Passerelle par défaut** : passerelle par défaut de votre réseau
- d **DNS** : serveur DNS de votre environnement

---

**Note** Pour plusieurs serveurs DNS, assurez-vous qu'ils sont séparés par un espace.

---

- e **Liste de recherche de domaine** : domaine qui doit être ajouté pour `dns lookup`.
- f Entrez `y` pour enregistrer la configuration.

18 Entrez le serveur NTP et assurez-vous qu'il peut atteindre la machine virtuelle. Les services ne parviendront pas à démarrer si l'heure NTP n'est pas synchronisée.

---

**Note** Dans le cas de plusieurs serveurs NTP, assurez-vous qu'ils sont séparés par des virgules.

---

19 (Facultatif) Pour configurer le proxy Web :

- a Entrez `y`.
- b Fournissez les détails du proxy Web.

20 Une vérification est effectuée pour voir si la clé secrète partagée a été configurée. Le collecteur est couplé à la plate-forme correspondante. Cette opération peut prendre quelques minutes.

21 Tous les services sont vérifiés.

22 Cliquez sur **Terminer**, une fois que le message **Proxy détecté !** s'affiche sur la page d'intégration. Il redirige vers la page de connexion.

## Configuration du collecteur Network Insight (AMI) dans AWS pour VMware SD-WAN

Vous pouvez configurer le collecteur vRealize Network Insight pour AWS en important l'image de machine Amazon (AMI, Amazon Machine Image) dans votre environnement AWS.

Si votre environnement ne dispose pas d'un système vCenter Server et que vous souhaitez déployer votre collecteur dans un environnement cloud, vous pouvez le déployer dans AWS.

---

**Note** Actuellement, vRealize Network Insight prend en charge le déploiement du collecteur dans AWS à l'aide d'un fichier AMI uniquement pour VMware SD-WAN.

---

La procédure et les tâches liées aux instances d'EC2 sont documentées dans <https://docs.aws.amazon.com/efs/index.html>.

## Procédure

- 1 Lancez l'instance EC2 à l'aide de l'AMI fournie par VMware dans la console Amazon EC2. Pour en savoir plus sur la procédure, reportez-vous à la section Créer des ressources EC2 et lancer votre instance d'EC2 dans la documentation d'*Amazon Elastic File System*.

**Note** Lorsque vous lancez votre instance d'EC2 dans AWS, vous devez sélectionner les éléments suivants :

Option	Action
Type d'instance	m4.xlarge (BLOC MOYEN)
Réseau	Sélectionnez un réseau et un sous-réseau appropriés.
Stockage	Stockage par défaut.
Balises	En fonction des stratégies du client.
Groupe de sécurité	Autorisez les connexions sortantes à 0.0.0.0/0 sur le port 443 (ou pour les règles restreintes, autorisez les connexions sortantes pour le nom de domaine complet de l'environnement de production SaaS de NI sur le port 443).
Clé	Sélectionnez la clé appropriée (la connexion SSH est activée pour l'AMI).

- 2 Lorsque votre instance d'EC2 est en cours d'exécution, connectez-vous à celle-ci.
- 3 Connectez-vous avec les informations d'identification de console données. Exécutez la commande `setup`.
- 4 Créez le mot de passe pour la connexion à `support`. Modifiez le mot de passe pour `consoleuser`.

**Note** Une fois que vous avez modifié le mot de passe, les options réseau seront ignorées lors de la configuration de la CLI.

Le proxy AMI ne prend pas en charge les éléments suivants :

- Modification de l'adresse IP
- IPv6
- Configuration du proxy Web.

- 5 Entrez le serveur NTP et vérifiez que vous pouvez y accéder à partir de la machine virtuelle. Les services ne parviennent pas à démarrer si l'heure NTP n'est pas synchronisée.

**Note** Dans le cas de plusieurs serveurs NTP, assurez-vous qu'ils sont séparés par des virgules.

- 6 Une vérification est effectuée pour voir si la clé secrète partagée a été configurée. Le collecteur est couplé à la plate-forme correspondante. Ce processus prend quelques minutes.
- 7 Tous les services sont vérifiés.

#### Étape suivante

Activez la collecte de flux des dispositifs Edge vers le collecteur que vous avez déployé dans AWS. Pour activer la collecte de flux, procédez comme suit :

- Définissez le collecteur que vous avez déployé dans AWS en tant que site non VeloCloud. Pour plus d'informations, contactez le support VMware.

## Déploiement de collecteurs supplémentaires dans une configuration existante

Vous pouvez ajouter un collecteur vRealize Network Insight supplémentaire à une configuration existante.

#### Procédure

- 1 Connectez-vous à l'interface utilisateur de vRealize Network Insight.
- 2 Développez **Infrastructure et support**, puis cliquez sur **Présentation et mises à jour**.
- 3 Faites défiler la liste vers le bas et cliquez sur **Ajouter une VM proxy**.  
La boîte de dialogue **Ajouter un nouveau dispositif virtuel de collecteur de données Network Insight** s'affiche
- 4 Cliquez sur **Copier** pour copier le code secret partagé à partir de la boîte de dialogue, puis cliquez sur **Terminé**.
- 5 Suivez les étapes de la section [Configuration du collecteur Network Insight \(OVA\)](#) à l'étape 3.

# Accès à vRealize Network Insight à l'aide de la licence d'évaluation

## 3

vRealize Network Insight démarre en mode d'évaluation NSX lorsque vous utilisez la licence d'évaluation.

Vous pouvez ajouter une source de données à vRealize Network Insight, analyser le flux de trafic et générer des rapports.

---

**Note** Pour passer en mode de produit complet, cliquez sur Passer à l'évaluation du produit complet dans le coin inférieur droit.

---

Ce chapitre contient les rubriques suivantes :

- [Ajout d'une instance de vCenter Server](#)
- [Analyse des flux de trafic](#)
- [Génération d'un rapport](#)

## Ajout d'une instance de vCenter Server

Vous pouvez ajouter des instances de vCenter Server en tant que source de données à vRealize Network Insight.

Plusieurs instances de vCenter Server peuvent être ajoutées à vRealize Network Insight pour commencer à surveiller les données.

### Conditions préalables

- Les rôles prédéfinis dans vCenter Server doivent disposer des privilèges suivants, attribués au niveau racine et devant être propagés aux rôles enfants :
  - **System.Anonymous**
  - **System.Read**
  - **System.View**
  - **Global.Settings**
- Les privilèges vCenter Server suivants sont requis pour configurer et utiliser IPFIX :
  - **Distributed Switch : opération de modification et de configuration de port**
  - **Groupe dvPort : opération de modification et de stratégie**

Pour en savoir plus sur les rôles dans vCenter, reportez-vous à la section *Utilisation des rôles* pour l'attribution de privilèges du guide de *Sécurité vSphere*.

### Procédure

- 1 Cliquez sur **Ajouter une instance de vCenter**.
- 2 Cliquez sur **Ajouter une nouvelle source** et personnalisez les options.

Option	Action
<b>VM de collecteur</b>	Sélectionnez une machine virtuelle de collecteur dans le menu déroulant.
<b>Adresse IP/nom de domaine complet</b>	Entrez l'adresse IP ou le nom de domaine complet de l'instance de vCenter Server.
<b>Nom d'utilisateur</b>	Entrez le nom d'utilisateur avec les privilèges suivants : <ul style="list-style-type: none"> <li>■ <b>Distributed Switch</b> : Modifier</li> <li>■ <b>Groupe dvPort</b> : Modifier</li> </ul>
<b>Mot de passe</b>	Entrez le mot de passe du logiciel vRealize Network Insight pour accéder au système vCenter Server.

- 3 Cliquez sur **Valider**.

Si le nombre de VM découvertes dépasse la capacité de la plate-forme ou d'un nœud de collecteur, la validation échoue. Vous ne serez pas autorisé à ajouter une source de données avant d'augmenter la taille de bloc de la plate-forme ou de créer un cluster.

La capacité spécifiée pour chaque taille de bloc avec et sans flux est la suivante :

Taille de bloc	Machines virtuelles	État des flux
Grande	6 000	Activé
Grande	10 000	Désactivé
Moyenne	3 000	Activé
Moyenne	6 000	Désactivé

- 4 Sélectionnez **Activer NetFlow (IPFIX) sur cette instance de vCenter** pour activer IPFIX.

Pour plus d'informations sur IPFIX, reportez-vous à la section *Activation de la configuration d'IPFIX sur VDS et DVPG* du Guide de l'utilisateur.

**Note** Si vous activez IPFIX dans vCenter et VMware NSX Manager, vRealize Network Insight détecte et supprime automatiquement les redondances de flux en désactivant IPFIX sur quelques-uns des DVPG pour les instances de vCenter associées.

- 5 Ajoutez des sources de collecte de données avancées à votre système vCenter Server.
- 6 Cliquez sur **Envoyer** pour ajouter le système vCenter Server. Les systèmes vCenter Server s'affichent sur la page d'accueil.

## Analyse des flux de trafic

Vous pouvez utiliser vRealize Network Insight pour analyser les flux dans votre centre de données.

### Conditions préalables

Avant de lancer l'analyse des flux, la collecte de données doit avoir eu lieu pendant au moins deux heures.

### Procédure

- 1 Spécifiez l'étendue de l'analyse. Par exemple, si vous êtes intéressé par les flux de toutes les VM d'un **cluster**, sélectionnez Cluster dans le menu déroulant. Vous pouvez également sélectionner toutes les VM connectées à un réseau VLAN ou VXLAN.
- 2 Sélectionnez le nom de l'entité pour laquelle vous souhaitez analyser les flux.
- 3 Sélectionnez la durée et cliquez sur **Analyser**.

## Génération d'un rapport

Vous pouvez générer un rapport sur l'évaluation des flux.

### Conditions préalables

Analysez les flux de trafic dans le centre de données. Pour obtenir des rapports complets, collectez 24 heures de données avant de lancer l'analyse.

### Procédure

- 1 En **mode d'évaluation EVAL NSX**, cliquez sur **Générer le rapport** sur la page d'analyse des flux.
- 2 En **mode non EVAL**, sur la page de **Microsegmentation**, cliquez sur **Distribution du trafic > Plus d'options > Rapport d'évaluation**.

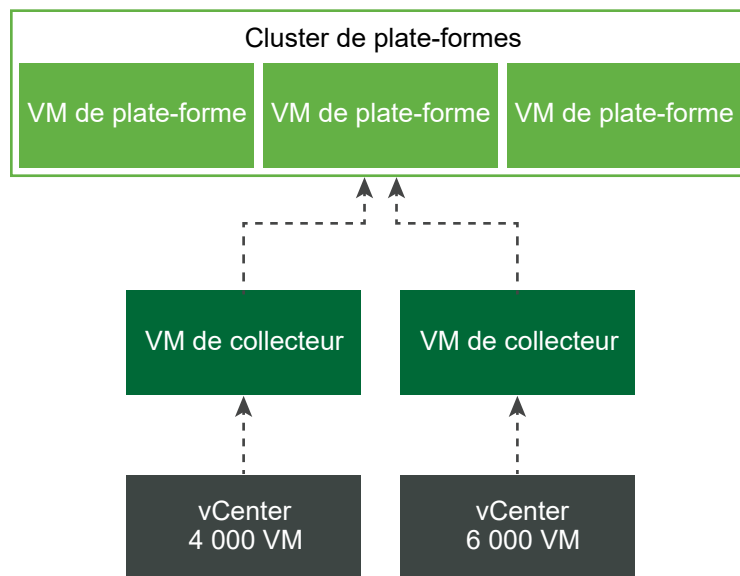


# Planification de l'évolutivité verticale de votre déploiement

## 4

Si le nombre de machines virtuelles ou le nombre de flux actifs dans votre installation est élevé ou qu'il devrait augmenter, vous pouvez augmenter la taille de la plate-forme ou du collecteur.

Vous pouvez utiliser l'architecture suivante pour mieux comprendre la distribution entre plate-forme et collecteur :



Ce chapitre contient les rubriques suivantes :

- [Planification de l'évolutivité verticale du cluster de plate-forme](#)
- [Planification de l'évolutivité verticale du collecteur](#)
- [Augmenter la taille de brique de votre installation](#)

## Planification de l'évolutivité verticale du cluster de plate-forme

Vous pouvez augmenter la capacité du cluster de plate-forme pour répondre à l'augmentation de la charge. En fonction de la charge, vous pouvez monter en puissance en augmentant la taille de brique ou en créant ou développant un cluster de plate-forme. Trois briques de plate-forme LARGE

peuvent être connectées ensemble pour former un cluster de plate-forme. Si la taille de brique d'une plate-forme est `LARGE` ou `EXTRA LARGE`, vous devez créer un cluster de plate-forme pour monter en puissance.

Pour déterminer la taille de brique de la plate-forme et le nombre de briques de plate-forme, reportez-vous à la section [Recommandations et configuration système requise](#).

---

**Note** Le cluster de plate-forme ne prend pas en charge la configuration de haute disponibilité. Tous les nœuds de plate-forme doivent être en cours d'exécution pour que le cluster fonctionne à des niveaux optimaux de performance.

---

## Scénarios d'évolutivité verticale du cluster de plate-forme

- Scénario 1 : votre plate-forme exécute 5 000 VM et 1,5 millions de flux actifs.  
Faites passer la taille de votre plate-forme de `MEDIUM` à `LARGE`. Reportez-vous à la section [Augmenter la taille de brique de votre installation](#).
- Scénario 2: votre plate-forme exécute un seul nœud `LARGE` avec 9 000 VM et 2 millions de flux actifs  
Ajoutez 2 autres nœuds de brique `LARGE` à convertir en cluster de brique `LARGE` à 3 nœuds.  
Reportez-vous à la section Extension de clusters du *Guide de l'utilisateur de vRealize Network Insight*.
- Scénario 3 : votre plate-forme exécute un cluster `LARGE` à 3 nœuds avec un ou plusieurs collecteurs, 15 000 VM et 4 millions de flux actifs.  
Faites passer la taille de vos nœuds de plate-forme existants de `LARGE` à `EXTRA-LARGE`.  
Reportez-vous à la section [Augmenter la taille de brique de votre installation](#).
- Scénario 4 : votre plate-forme exécute un cluster `EXTRA-LARGE` à 3 nœuds avec un ou plusieurs collecteurs, 25 000 VM et 8 millions de flux actifs.  
Ajoutez 2 autres nœuds de brique `EXTRA-LARGE` à convertir en cluster `EXTRA-LARGE` à 5 nœuds.  
Reportez-vous à la section Extension de clusters du *Guide de l'utilisateur de vRealize Network Insight*.

## Planification de l'évolutivité verticale du collecteur

La capacité du collecteur est basée sur la taille des briques. La source de données que vous pouvez ajouter à un collecteur dépend de la capacité de celui-ci (VM et flux).

Reportez-vous à la section [Tableau 1-6. Déploiement du collecteur - Capacité maximale](#). Lorsqu'un collecteur atteint la taille de brique `LARGE`, vous devez ajouter d'autres collecteurs. Vous pouvez augmenter la taille de chaque collecteur jusqu'à `EXTRA-LARGE`.

Vous pouvez ajouter plusieurs sources de données à un collecteur en fonction de la capacité prise en charge. Cependant, vous ne pouvez pas ajouter la même source de données à plusieurs collecteurs.

## Scénarios d'évolutivité verticale des collecteurs

- Scénario 1 : 2 000 VM dans un système vCenter.

Installez une VM de collecteur moyenne. Ajoutez le système vCenter à ce collecteur. Reportez-vous à la section [Ajout d'une instance de vCenter Server](#).

- Scénario 2 : 1 000 VM dans le système vCenter1 et 2 000 VM dans le système vCenter2 (toutes dans un centre de données).

Installez une VM de collecteur moyenne. Ajoutez les deux systèmes vCenter à ce collecteur. Reportez-vous à la section [Ajout d'une instance de vCenter Server](#).

- Scénario 3 : 1 000 machines virtuelles dans vCenter1 (centre de données 1) et 2 000 machines virtuelles dans vCenter2 (centre de données 2)

Installez une VM de collecteur moyenne dans chaque centre de données. Ajoutez le système vCenter1 à une VM de collecteur dans le même centre de données et ajoutez le système vCenter2 à une VM de collecteur dans son centre de données. Reportez-vous à la section [Ajout d'une instance de vCenter Server](#).

- Scénario 4 : le nombre de VM dépasse 4 000 ; les flux actifs dépassent 2,5 millions.

Faites passer la taille de votre VM de collecteur de `MEDIUM` à `LARGE`. Reportez-vous à la section [Augmenter la taille de brique de votre installation](#).

- Scénario 5 : 9 000 VM dans vCenter1 sans flux (centre de données 1).

Installez une grande VM de collecteur. Ajoutez ce système vCenter au collecteur. Reportez-vous à la section [Ajout d'une instance de vCenter Server](#).

- Scénario 6 : le nombre de VM est inférieur ou égal à 10 000, mais les flux actifs dépassent 5 millions.

Faites passer la taille de votre VM de collecteur de `LARGE` à `EXTRA-LARGE`. Reportez-vous à la section [Augmenter la taille de brique de votre installation](#).

- Scénario 8 : 2 systèmes vCenter, vCenter 1 comprend 10 000 VM et 9 millions flux actifs ; vCenter2 comprend 10 000 machines virtuelles et 4 millions flux actifs.

Installez un proxy `EXTRA-LARGE` et un proxy `LARGE`. Ajoutez le système vCenter1 au proxy `EXTRA-LARGE` et ajoutez le système vCenter2 au proxy `LARGE`.

- Scénario 9 : un vCenter exécute 10 000 VM et 9 millions de flux actifs.

Installez un proxy `EXTRA-LARGE` et ajoutez-y le système vCenter.

## Augmenter la taille de brique de votre installation

Pour répondre à vos besoins, vous pouvez modifier la taille de brique de votre plate-forme ou du dispositif de collecteur, de `MEDIUM` à `LARGE` ou de `LARGE` à `EXTRA-LARGE`.

## Procédure

- ◆ Réalisez les étapes relatives à votre installation.

Option	Description
<b>Pour une plate-forme à nœud unique ou un nouvel OVA indépendant</b>	<ul style="list-style-type: none"> <li>a Connectez-vous à vCenter.</li> <li>b Arrêtez la VM de plate-forme.</li> <li>c Augmentez le disque, la RAM, le nombre total de vCPU et la réservation correspondante de la VM pour qu'elle corresponde à la taille de brique. Pour plus d'informations, reportez-vous à la page Recommandations et configuration système requise.</li> <li>d Redémarrez la VM de plate-forme.</li> </ul>
<b>Pour une plate-forme de cluster</b>	<ul style="list-style-type: none"> <li>a Connectez-vous à vCenter.</li> <li>b Arrêtez la VM de plate-forme dans l'ordre chronologique inverse. Par exemple, procédez à l'arrêt du nœud 3 au nœud 1.</li> <li>c Augmentez le disque, la RAM, le nombre total de vCPU et la réservation correspondante. Pour plus d'informations, reportez-vous à Recommandations et configuration système requise.</li> <li>d Redémarrez les VM de plate-forme dans l'ordre chronologique. Par exemple, procédez au redémarrage du nœud 1 au nœud 3.</li> </ul>
<b>Pour un collecteur</b>	<ul style="list-style-type: none"> <li>a Connectez-vous à vCenter.</li> <li>b Arrêtez la VM de collecteur.</li> <li>c Augmentez le disque, la RAM, le nombre total de vCPU et la réservation correspondante de la VM pour qu'elle corresponde à la taille de brique. Pour plus d'informations, reportez-vous à la page Recommandations et configuration système requise.</li> <li>d Redémarrez la VM de collecteur.</li> </ul>

# Mise à niveau de vRealize Network Insight

# 5

Vous pouvez mettre à niveau votre environnement vRealize Network Insight actuel vers la dernière version.

Points importants à prendre en compte avant la mise à niveau :

- Après la mise à niveau, vRealize Network Insight tarde entre 12 et 24 heures pour traiter les données figurant dans le pipeline pendant l'opération de mise à niveau et les afficher dans l'interface utilisateur.
- vRealize Network Insight ne prend pas en charge la restauration ou la rétrogradation du produit. Vous devez effectuer une sauvegarde avant de procéder à la mise à niveau. Pour plus d'informations sur le processus de sauvegarde et de restauration, reportez-vous à l'article de la base de connaissances <https://kb.vmware.com/s/article/55829>.
- Dans un environnement en cluster, vous devez effectuer l'opération de mise à niveau uniquement sur le nœud de la plate-forme 1.
- Après la mise à niveau vers vRealize Network Insight 5.1, certains ID de règle de pare-feu peuvent être remplacés par les nouveaux ID renvoyés par l'API VMware Cloud on AWS 1.9. Si des règles de pare-feu de VMware Cloud on AWS 1.8 attachées aux flux existent :
  - Les règles de pare-feu de VMware Cloud on AWS 1.9 correctes ou respectives sont attachées immédiatement après la mise à niveau de tous les flux actifs.
  - Les règles de pare-feu font référence à des règles inexistantes pour les flux dont la période d'inactivité est supérieure à 24 heures avant la mise à niveau de la version 1.8 vers la version 1.9.

---

**Note** Si des problèmes tels que l'échec de téléchargement ou de l'interface utilisateur surviennent lors de l'exécution de la mise à niveau centralisée, contactez le support VMware.

---

## Migration vers la base de données Foundation

Pour distribuer les données de configuration entre les banques de données du cluster, vRealize Network Insight 5.1 remplace PostgreSQL par la base de données Foundation pour le stockage des données de configuration. Cela permet à vRealize Network Insight de :

- réduire la charge sur le nœud de la plate-forme 1
- éviter les points unitaires de panne

- améliorer la résilience
- améliorer les performances
- partager le disque uniformément entre les nœuds du cluster

Le processus de migration effectue automatiquement les opérations suivantes :

- arrêt de tous les services
- démarrage de la migration table à table de PostgreSQL vers la base de données Foundation
- affichage des informations de progression de la migration dynamique sur l'interface utilisateur de la plate-forme 1

Le temps de migration pour déplacer des données depuis PostgreSQL vers la base de données Foundation dépend de la vitesse du disque et du nombre de nœuds (un nombre de nœuds plus élevé permet un débit d'écriture plus élevé sur la base de données Foundation).

Le temps nécessaire pour terminer le processus de migration dépend de la taille de la base de données.

Taille de la configuration	Taille des données	Nombre de nœuds	Temps de migration typique
Petite	20 Go à 40 Go	1 nœud	1 à 2 heures
Moyenne	60 Go à 100 Go	3 nœuds	7 à 10 heures
Grandes configurations à cloud unique	500 Go	Cluster à 10 nœuds	15 à 20 heures
XL (Megatron)	1 To	Cluster à 10 nœuds	35 à 40 heures

Notez que la migration s'effectue dans le cadre du processus de mise à niveau de vRealize Network Insight. Par conséquent, la durée de la mise à niveau peut s'allonger, ce qui s'affiche à l'écran au cours du processus.

vRealize Network Insight prend en charge les différents modes de mise à niveau.

Ce chapitre contient les rubriques suivantes :

- [Mise à niveau en ligne](#)
- [Mise à niveau hors ligne d'un simple clic](#)
- [Mise à niveau via la CLI](#)

## Mise à niveau en ligne

Chaque fois qu'une nouvelle version de vRealize Network Insight est disponible, vous recevez une notification.

## Conditions préalables

- Les étapes de mise à niveau peuvent échouer si l'espace dans le répertoire `/tmp` n'est pas suffisant. Vérifiez que les conditions requises suivantes relatives à l'espace disque pour le serveur de plate-forme et de collecteur sont satisfaites :
  - `/tmp` - 6 Go
  - `/home` - 2 Go
- Vérifiez que les conditions requises suivantes relatives à l'espace disque pour le serveur de plate-forme sont satisfaites :
  - `/` - 6 Go (uniquement pour le nœud de la plate-forme 1)
  - `/var` - 40 Go
- Vérifiez que vous disposez de la bande passante requise minimale de 500 Ko/s pour télécharger le bundle de mise à niveau à partir du serveur. La page **Installation et prise en charge** génère un message d'erreur si la bande passante de téléchargement n'est pas suffisante.
- Assurez-vous que tous les nœuds sont en ligne. Si un nœud est inactif, vous ne serez pas autorisé à déclencher la mise à niveau.
- Effectuez des snapshots des machines virtuelles.
- Notez les valeurs suivantes à vérifier après la migration :
  - Nombre de machines virtuelles
  - Machine virtuelle sur laquelle le nombre de snapshots > 0
  - Nombre de règles de pare-feu
  - Nombre de groupes de sécurité
  - Nombre de pare-feu NSX

## Procédure

- 1 Lorsqu'une mise à jour est disponible, le message de notification **Mise à jour disponible** s'affiche.

---

### Note

- Si la notification de mise à jour n'est pas disponible, vérifiez que les machines virtuelles de plate-forme et de collecteur vRealize Network Insight disposent d'une connectivité à `svc.ni.vmware.com` sur le port 443 et à `reg.ni.vmware.com` sur le port 443 en exécutant la commande `show-connectivity-status`. Si cette connectivité requiert `http proxy`, configurez-le sur chaque VM à l'aide de la commande `set-web-proxy`. Vérifiez que la sortie contient l'état `Passed` pour la connectivité de la mise à niveau.
- Créez un ticket de support et fournissez la balise de service à partir de l'interface utilisateur du produit. La balise de service est affichée sous **Paramètres > À propos de**.
- Connectez-vous au dispositif et exécutez la commande `show-connectivity-status`. Fournissez une capture d'écran de la sortie de la commande à partir de chaque machine virtuelle de plate-forme et de collecteur vRealize Network Insight.

- 2 Dans le message de notification `Mise à jour disponible`, cliquez sur **Afficher les détails** pour afficher les détails de la mise à jour.

L'écran Mise à niveau de vRealize Network Insight s'affiche.

- 3 Lisez les instructions **Avant de commencer** et cliquez sur **Continuer**.

- 4 Attendez la fin des vérifications préalables :

- vérification de l'espace disque, y compris l'espace requis pour la migration
- vérification de la version
- vérification de l'état de synchronisation NTP
- vérification de la bande passante

Vous pouvez voir la durée approximative requise pour effectuer la mise à niveau (y compris la durée de migration) sur votre configuration.

- 5 Cliquez sur **Installer maintenant**.



- 6 Une fois le processus de mise à niveau démarré, l'écran Mise à niveau de vRealize Network Insight indique son état.

---

#### Note

- Si un nœud devient inactif, le processus de mise à niveau ne continue pas. La mise à niveau ne reprendra pas tant que le nœud ne redeviendra pas actif.
  - La plate-forme 1 devient le serveur de mise à niveau. Si elle est hors ligne, aucun autre nœud n'est mis à niveau.
  - Une fois les plates-formes mises à niveau, vous pouvez reprendre vos opérations vRealize Network Insight normales même si la mise à niveau du collecteur s'exécute en parallèle. Tant que le processus de mise à niveau n'est pas complètement terminé, le message `Node Version Mismatch detected` s'affiche sur la page Installation et prise en charge.
- 

- Une fois les services mis à niveau, Nginx redémarre pour afficher le processus de migration. Par conséquent, il se peut que vous ne puissiez pas accéder à l'interface utilisateur pendant une courte période (une à deux minutes).
- vRealize Network Insight commence à migrer les données vers la base de données Foundation. L'écran État de la migration des données affiche :
  - l'état global
  - le temps passé
  - l'état table par table
  - le nombre d'enregistrements migrés

En cas de problème, vous pouvez utiliser l'option **Exporter les journaux de migration** pour les partager avec l'équipe de support VMware.

- Les données PostgreSQL sur les collecteurs sont également migrées vers la base de données Foundation dans le cadre du processus de mise à niveau. Toutefois, l'état de la migration du collecteur ne s'affiche pas sur l'interface utilisateur.

- 7 Une fois le processus de la mise à niveau terminé, le message de confirmation s'affiche.

Toutes les plates-formes et les nœuds de collecteurs ont été mis à niveau.

#### Étape suivante

- Connectez-vous à vRealize Network Insight et effectuez les tâches appropriées.
- Après deux ou trois jours, supprimez les snapshots pour libérer de l'espace disque.

## Mise à niveau hors ligne d'un simple clic

vRealize Network Insight prend en charge d'un simple clic la mise à niveau hors ligne du produit à partir de la version 3.7 et versions ultérieures.

### Conditions préalables

- Les étapes de mise à niveau peuvent échouer si l'espace dans le répertoire `/tmp` n'est pas suffisant. Vérifiez que les conditions requises suivantes relatives à l'espace disque pour le serveur de plate-forme et de collecteur sont satisfaites :
  - `/tmp` - 6 Go
  - `/home` - 2 Go
- Vérifiez que les conditions requises suivantes relatives à l'espace disque pour le serveur de plate-forme sont satisfaites :
  - `/` - 12 Go (uniquement pour le nœud de la plate-forme 1)
  - `/var` - 40 Go

---

**Note** Les étapes de téléchargement du bundle et de mise à niveau ultérieures risquent d'échouer si l'espace dans le répertoire `/tmp` n'est pas suffisant.

---

- Pour éviter l'expiration de la session d'interface utilisateur, accédez à **Paramètres > Configuration système > Délai d'expiration de session utilisateur** et augmentez la valeur de **Délai d'expiration de session utilisateur** à au moins 2 heures. Une fois la durée du délai d'expiration de session modifiée, vous devez vous reconnecter au système.
- Assurez-vous que tous les nœuds sont en ligne. Si un nœud est inactif, vous ne serez pas autorisé à déclencher la mise à niveau.
- Effectuez des snapshots des machines virtuelles.
- Notez les valeurs suivantes à vérifier après la migration :
  - Nombre de machines virtuelles
  - Machine virtuelle sur laquelle le nombre de snapshots > 0
  - Nombre de règles de pare-feu
  - Nombre de groupes de sécurité
  - Nombre de pare-feu NSX

### Procédure

- 1 Téléchargez le fichier de bundle de mise à niveau requis à partir de [My VMware](#) et enregistrez le package de mise à jour sur votre disque local.
- 2 Vérifiez que la valeur `MD5SUM` du bundle téléchargé correspond à la valeur `MD5SUM` spécifiée sur le site Web de VMware.
- 3 Sur la page **Installation et prise en charge**, sous **Version du logiciel**, cliquez sur **Cliquez ici**.

- 4 Cliquez sur **Parcourir** pour sélectionner le fichier, puis cliquez sur **Télécharger**.

À l'issue du téléchargement, vRealize Network Insight affiche le message de notification de fin du téléchargement du bundle après 2 à 3 minutes, puis le traitement du bundle se produit en arrière-plan.

---

**Note**

- Tant que le téléchargement du module n'est pas effectué, assurez-vous que la session n'est pas fermée. Si la session se termine, vous devez redémarrer le processus de téléchargement.
  - N'actualisez pas la page après le téléchargement du bundle tant que le message de notification Mise à jour disponible n'est pas affiché.
- 

- 5 Dans le message de notification de Mise à jour disponible, cliquez sur **Afficher les détails**.

L'écran Mise à niveau de vRealize Network Insight s'affiche.

- 6 Lisez les instructions **Avant de commencer** et cliquez sur **Continuer**.

- 7 Attendez la fin des vérifications préalables :

- Vérification de l'espace disque, y compris l'espace requis pour la migration
- Vérification de la version
- Vérification de l'état de synchronisation NTP
- Vérification du bundle

- 8 Cliquez sur **Installer maintenant**.

Vous pouvez voir la durée approximative requise pour effectuer la mise à niveau sur votre configuration.

- 9 Une fois le processus de mise à niveau démarré, l'écran Mise à niveau de vRealize Network Insight indique son état.

---

#### Note

- Si un nœud devient inactif, le processus de mise à niveau ne continue pas. La mise à niveau ne reprendra pas tant que le nœud ne redeviendra pas actif.
  - La plate-forme 1 devient le serveur de mise à niveau. Si elle est hors ligne, aucun autre nœud n'est mis à niveau.
  - Une fois les plates-formes mises à niveau, vous pouvez reprendre vos opérations vRealize Network Insight normales même si la mise à niveau du collecteur s'exécute en parallèle. Tant que le processus de mise à niveau n'est pas complètement terminé, le message `Node Version Mismatch detected` s'affiche sur la page Installation et prise en charge.
- 

- Une fois les services mis à niveau, Nginx redémarre pour afficher le processus de migration. Par conséquent, il se peut que vous ne puissiez pas accéder à l'interface utilisateur pendant une courte période (une à deux minutes).
- vRealize Network Insight commence à migrer les données vers la base de données Foundation. L'écran État de la migration des données affiche :
  - L'état global
  - Le temps passé
  - L'état table par table
  - Le nombre d'enregistrements migrés

En cas de problème, vous pouvez utiliser l'option **Exporter les journaux de migration** pour les partager avec l'équipe de support VMware.

- Les données PostgreSQL sur les collecteurs sont également migrées vers la base de données Foundation dans le cadre du processus de mise à niveau. Toutefois, l'état de la migration du collecteur ne s'affiche pas sur l'interface utilisateur.

- 10 Une fois le processus de la mise à niveau terminé, le message de confirmation s'affiche.

Toutes les plates-formes et les nœuds de collecteurs ont été mis à niveau.

#### Étape suivante

- Connectez-vous à vRealize Network Insight et effectuez les tâches appropriées.
- Après deux ou trois jours, supprimez les snapshots pour libérer de l'espace disque.

## Mise à niveau via la CLI

Effectuez la mise à niveau via la CLI uniquement si la mise à niveau en ligne ou la mise à niveau hors ligne d'un simple clic ne fonctionne pas. Mettez à niveau les VM de plate-forme avant les

VM de collecteur. Cependant, vous devez contacter le support VMware avant de lancer la mise à niveau hors ligne à l'aide de l'interface de ligne de commande

Dans un environnement de cluster, vous devez effectuer l'opération de mise à niveau uniquement depuis le nœud de la plate-forme 1 (P1) et les autres nœuds de plate-forme du cluster sont mis à niveau automatiquement. Vous devez toutefois mettre à niveau chaque collecteur individuellement.

### Conditions préalables

- Les étapes de mise à niveau peuvent échouer si l'espace dans le répertoire `/tmp` n'est pas suffisant. Vérifiez que les conditions requises suivantes relatives à l'espace disque pour le serveur de plate-forme et de collecteur sont satisfaites :
  - `/tmp` - 6 Go
  - `/home` - 2 Go
  - `/var` - 40 Go
- Assurez-vous que tous les nœuds sont en ligne. Si un nœud est inactif, vous ne serez pas autorisé à déclencher la mise à niveau.
- Effectuez des snapshots des machines virtuelles.
- Notez les valeurs suivantes à vérifier après la migration :
  - Nombre de machines virtuelles
  - Machine virtuelle sur laquelle le nombre de snapshots > 0
  - Nombre de règles de pare-feu
  - Nombre de groupes de sécurité
  - Nombre de pare-feu NSX

### Procédure

- 1 Téléchargez le fichier de bundle de mise à niveau requis à partir de [My VMware](#).
- 2 Vérifiez que la valeur `MD5SUM` du bundle téléchargé correspond à la valeur `MD5SUM` spécifiée sur le site Web de VMware.
- 3 Copiez le bundle de mise à niveau sur la machine virtuelle de la plate-forme 1 vRealize Network Insight et sur toutes les machines virtuelles de collecteur.
  - Pour copier le fichier de la machine virtuelle Linux vers la machine virtuelle vRealize Network Insight, exécutez la commande `scp <filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/.`

- Pour copier le fichier de la machine virtuelle Windows vers la machine virtuelle vRealize Network Insight, exécutez la commande `pscp -scp <SOURCE_PATH>\<filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/.`

---

**Note** Utilisez l'utilitaire `pscp` à partir de <https://the.earth.li/~sgtatham/putty/latest/w64/pscp.exe>.

---

- 4 Connectez-vous à la plate-forme 1 vRealize Network Insight via la CLI à l'aide de la commande `consoleuser`, puis exécutez les commandes suivantes :

- `package-installer copy --host localhost --user consoleuser --path /home/consoleuser/<filename>.upgrade.bundle`
- `package-installer upgrade --name <filename>.upgrade.bundle`

---

**Note** Vous devez d'abord effectuer la mise à niveau de la plate-forme, puis démarrer la mise à jour du collecteur.

---

- 5 Exécutez de nouveau la commande `package-installer upgrade` après le redémarrage de la configuration dans le cadre de la mise à niveau du système d'exploitation.

---

**Important** Si vous recevez un message d'erreur d'expiration de la session SSH, consultez le fichier `/var/log/arkin/centralized_upgrade.log` pour vérifier si le redémarrage a déjà eu lieu. Si le redémarrage s'est effectué, réexécutez la commande `package-installer upgrade`.

---

- 6 Connectez-vous à chaque nœud de collecteur via l'interface de ligne de commande, puis effectuez la mise à niveau en utilisant les commandes utilisées pour la mise à niveau de la plate-forme.

---

**Note** Vous pouvez mettre à niveau tous les collecteurs simultanément.

---

- 7 Vérifiez la version mise à niveau à l'aide de la commande `show-version`.

# Désinstallation de vRealize Network Insight

# 6

Vous devez désinstaller vRealize Network Insight via vSphere Web Client.

## Procédure

- 1 Si vous pouvez accéder au portail Web de vRealize Network Insight, procédez comme suit :

- a Connectez-vous au portail Web de vRealize Network Insight.
- b Accédez à **Paramètres > Comptes et sources de données**.
- c Désactivez et supprimez toutes les sources de données.

La suppression de la source de données vCenter supprime les paramètres IPFIX (s'ils ont été configurés) sur le VDS. De même, la suppression de la source de données de NSX Manager supprime les paramètres IPFIX du moniteur de flux NSX.

- 2 Si vous ne parvenez pas à accéder au portail Web de vRealize Network Insight, procédez comme suit :

- a Si NetFlow (IPFIX) est activé sur vCenter, supprimez l'adresse IP du collecteur vRealize Network Insight des paramètres VDS/DVPG IPFIX. Reportez-vous à la section [Suppression de l'adresse IP du collecteur lorsque NetFlow est activé dans le système vCenter](#).
- b Si IPFIX est activé sur NSX, supprimez les paramètres de surveillance de flux IP du collecteur vRealize Network Insight. Reportez-vous à la section [Suppression de l'adresse IP du collecteur lorsque NetFlow est activé dans NSX](#).
- c Si NetFlow est configuré sur des commutateurs physiques pour envoyer NetFlow vers un collecteur NetFlow vRealize Network Insight, modifiez la configuration au niveau des commutateurs pour arrêter l'envoi d'informations NetFlow.

- 3 Si des règles de pare-feu ou de routage spécifiques sont créées pour autoriser ou acheminer le trafic vers et depuis des VM vRealize Network Insight, supprimez-les.
- 4 Pour des raisons de sécurité, nettoyez les informations d'identification d'accès utilisées pour configurer les sources de données dans vRealize Network Insight.
- 5 Arrêtez et supprimez l'ensemble des collecteurs et VM de plate-forme vRealize Network Insight.

## Suppression de l'adresse IP du collecteur lorsque NetFlow est activé dans le système vCenter

Si NetFlow (IPFIX) est activé dans le système vCenter, utilisez cette procédure pour supprimer l'adresse IP du collecteur de vRealize Network Insight des paramètres du serveur virtuel dédié (VDS)/IPFIX de groupe de ports virtuels distribué (DVPG).

### Procédure

- 1 Connectez-vous à vSphere Web Client.
- 2 Accédez à **Accueil > Mise en réseau**.
- 3 Dans le volet de gauche, sélectionnez **VDS** et cliquez sur **Configurer > Modifier**.
- 4 Dans le champ **Adresse IP du collecteur**, supprimez les détails de l'adresse IP du collecteur vRealize Network Insight.
- 5 Dans le champ **Port du collecteur**, supprimez les détails du port.
- 6 Cliquez sur **OK**.  
Patientez environ deux minutes avant de passer à l'étape suivante.
- 7 Sélectionnez le DVPG de ce VDS et cliquez sur **Configurer > Stratégies > Modifier**.
- 8 Dans le champ **NetFlow**, sélectionnez **Désactiver** dans le menu déroulant.
- 9 Vérifiez vos paramètres et cliquez sur **Appliquer**.

### Étape suivante

Réalisez à nouveau les étapes pour chaque VDS et ses DVPG pour lesquels IPFIX est activé et supprimez l'adresse IP du collecteur vRealize Network Insight.

## Suppression de l'adresse IP du collecteur lorsque NetFlow est activé dans NSX

Si NetFlow (IPFIX) est activé dans NSX, utilisez cette procédure pour supprimer les paramètres de surveillance de flux d'adresse IP du collecteur de vRealize Network Insight (vRealize Network Insight).

### Procédure

- 1 Connectez-vous à vSphere Web Client.
- 2 Cliquez sur **Accueil > Mise en réseau et sécurité > Outils > Surveillance de flux > Configuration**.
- 3 Dans **État de la collecte globale de flux**, cliquez sur **Désactiver**.
- 4 Pour désactiver la connexion des flux, cliquez sur **IPFIX**.
- 5 Dans l'onglet **IPFIX**, sélectionnez **Adresse IP du collecteur** et cliquez sur **Supprimer**.



- 6 S'il ne reste plus aucune adresse IP, cliquez sur **Modifier** et désactivez la case à cocher **Activer la configuration IPFIX**.
- 7 Cliquez sur **Enregistrer**.