Cisco Stealthwatch

Guide d'installation et de configuration matérielle du data store

Sommaire

Introduction au guide d'installation et de configuration matérielle du data store

Présentation

Ce guide explique comment installer le Stealthwatch data store dans le cadre du déploiement d'un système Stealthwatch. Il décrit les composants du système Stealthwatch et la manière dont ils sont placés dans le système, en particulier par rapport au data store.

Ce chapitre comprend les rubriques suivantes :

Public

Ce guide s'adresse au technicien chargé de l'installation des composants matériels du système Stealthwatch. Nous supposons que vous disposez déjà des connaissances générales nécessaires pour installer l'équipement réseau (collecteur de flux et console de gestion Stealthwatch).

Pour plus d'informations sur la configuration des produits système Stealthwatch, consultez le *Guide de configuration du système Stealthwatch*.

Utilisation du présent guide

En plus de l'introduction, ce guide comprend les chapitres suivants :

Chapitre	Description
Concepts et architecture du data store	Décrit les concepts de base qui sous-tendent la base de données data store, ainsi que l'architecture de base liée au déploiement du data store en relation avec une console SMC et des collecteurs de flux.
Exigences et recommandations	Décrit les composants matériels Stealthwatch compatibles avec le data

Chapitre	Description
relatives au déploiement du data store	store, spécifie la configuration requise et fournit des recommandations relatives au déploiement de votre data store, y compris les ports de communication à ouvrir.
Présentation du déploiement du data store Stealthwatch	Fournit une vue d'ensemble du déploiement des appliances Stealthwatch à utiliser avec un data store.
Installation matérielle du data store	Fournit une présentation de bout en bout du déploiement des appliances Stealthwatch à utiliser avec un data store, ainsi que des instructions de configuration pour initialiser la base de données data store.
Configuration de la conservation du data store	Fournit des informations sur la configuration de la période de conservation des données du data store.
Étapes postérieures à l'installation du data store	Décrit les étapes qui suivent le déploiement et la configuration de votre data store.
Maintenance du data store	Décrit les tâches de maintenance du data store.
Résoudre les problèmes liés au déploiement du data store	Décrit les problèmes courants rencontrés au cours du processus d'installation du data store et propose des solutions.
Annexe A. Préparation de l'installation	Fournit des avertissements pour l'installation des composants matériels.
Annexe B. Installation du matériel	Fournit une présentation de l'installation des appliances Stealthwatch et de la

Chapitre	Description
Stealthwatch	configuration initiale en vue d'attribuer une adresse IP et d'autres informations de gestion connexes.
Annexe C. Configuration de vos appliances	Fournit une présentation de l'utilisation de l'outil de configuration de l'appliance pour configurer vos appliances Stealthwatch.

Concepts et architecture du data store

> Veillez à ne **pas** installer vous-même un Stealthwatch data store. Si vous envisagez d'acheter un Stealthwatch data store, contactez les services professionnels Cisco pour obtenir de l'aide concernant le placement, le déploiement et la configuration dans le cadre de votre déploiement Stealthwatch global.

Le Stealthwatch data store fournit un référentiel central pour stocker les données de télémétrie de votre réseau collectées par vos collecteurs de flux Stealthwatch. Le data store se compose d'un cluster de nœuds de données, contenant chacun une partie de vos données, ainsi qu'une sauvegarde des données d'un nœud de données distinct. Étant donné que toutes vos données se trouvent dans une base de données centralisée au lieu d'être réparties sur plusieurs collecteurs de flux, votre console de gestion Stealthwatch peut récupérer les résultats de la requête auprès de data store plus rapidement que si elle interrogeait tous vos collecteurs de flux séparément. Le cluster data store offre une meilleure tolérance aux pannes, une réponse améliorée aux requêtes et un remplissage plus rapide des graphiques.

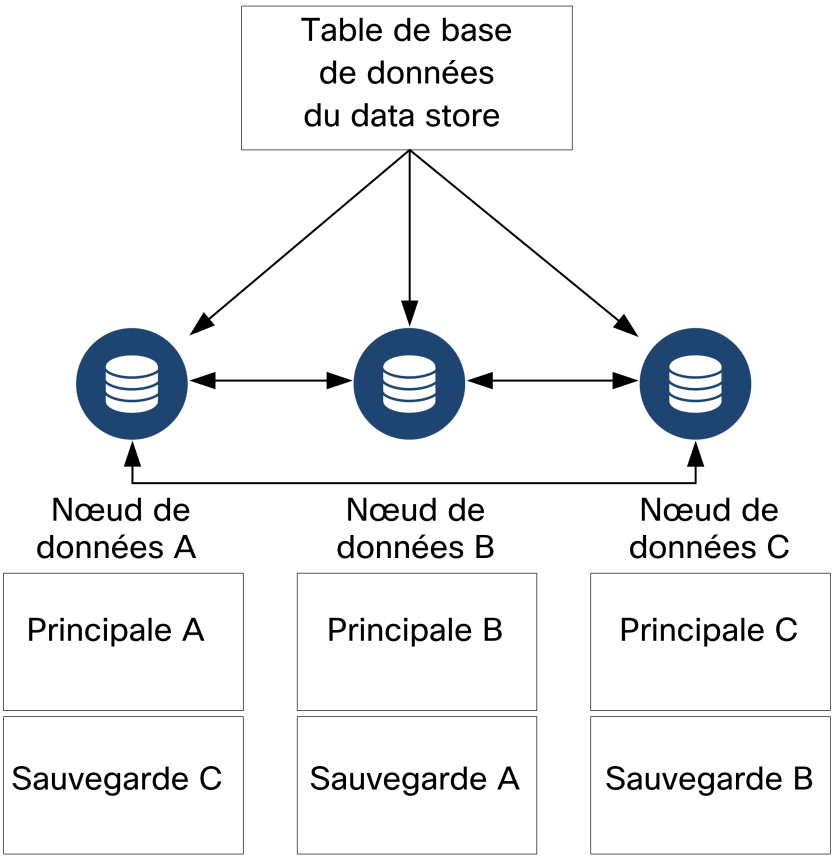
Stockage du data store et tolérance aux pannes

Le data store collecte des données auprès des collecteurs de flux et les distribue de façon équitable sur les nœuds de données dans le cluster. Chaque nœud de données, en plus de stocker une partie de votre télémétrie globale, stocke également une sauvegarde de la télémétrie d'un autre nœud de données. Ce mode de stockage des données permet :

- de faciliter l'équilibrage de la charge ;
- de répartir le traitement sur chaque nœud ;
- de s'assurer que toutes les données intégrées dans le data store disposent d'une sauvegarde en cas de panne ;
- d'augmenter le nombre de nœuds de données en vue d'améliorer les performances globales de stockage et de consultation.

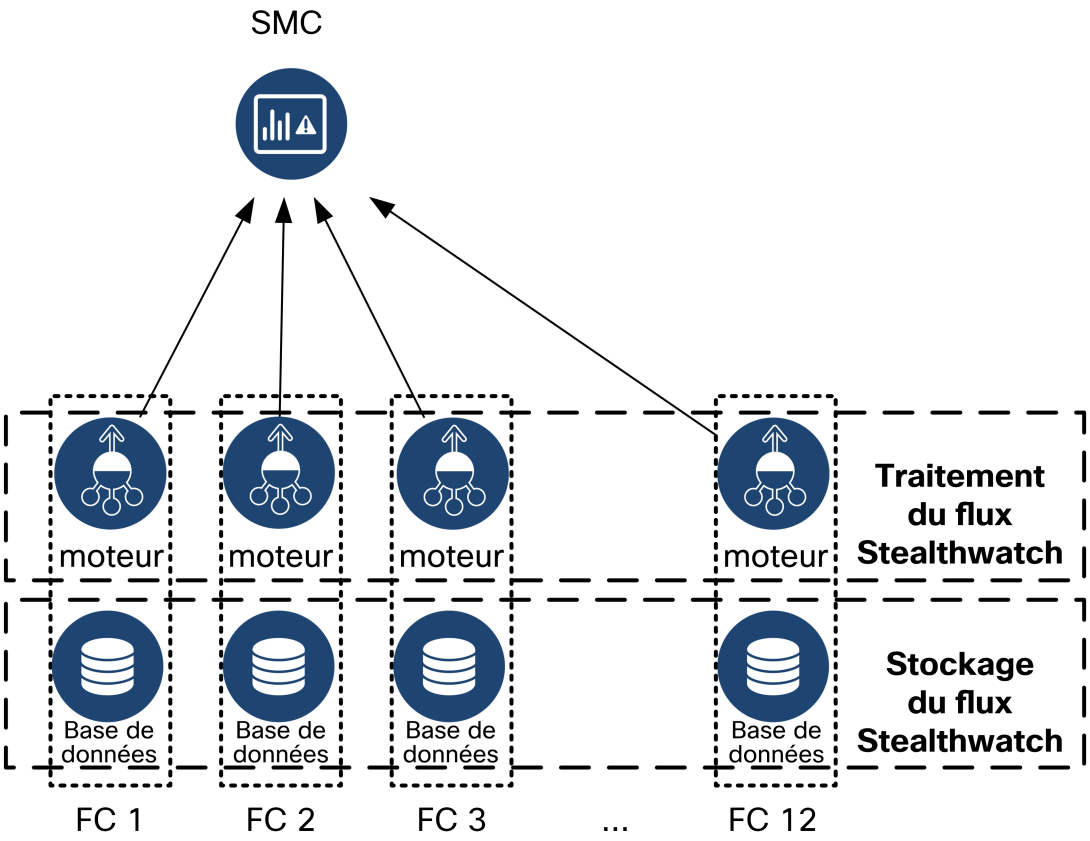
Si un nœud tombe en panne, tant que le nœud contenant sa sauvegarde est toujours disponible et qu'au moins la moitié du nombre total de nœuds de données est toujours active, l'ensemble du data store reste actif. Vous avez ainsi le temps de rétablir la connexion défaillante ou de réparer le matériel défectueux ; après avoir remplacé le nœud de données défectueux, le data store restaure les données de ce nœud à partir de la sauvegarde existante stockée sur le nœud de données adjacent et crée une

sauvegarde des données sur ce nœud de données. Reportez-vous au schéma suivant pour savoir comment les nœuds de données stockent la télémétrie :

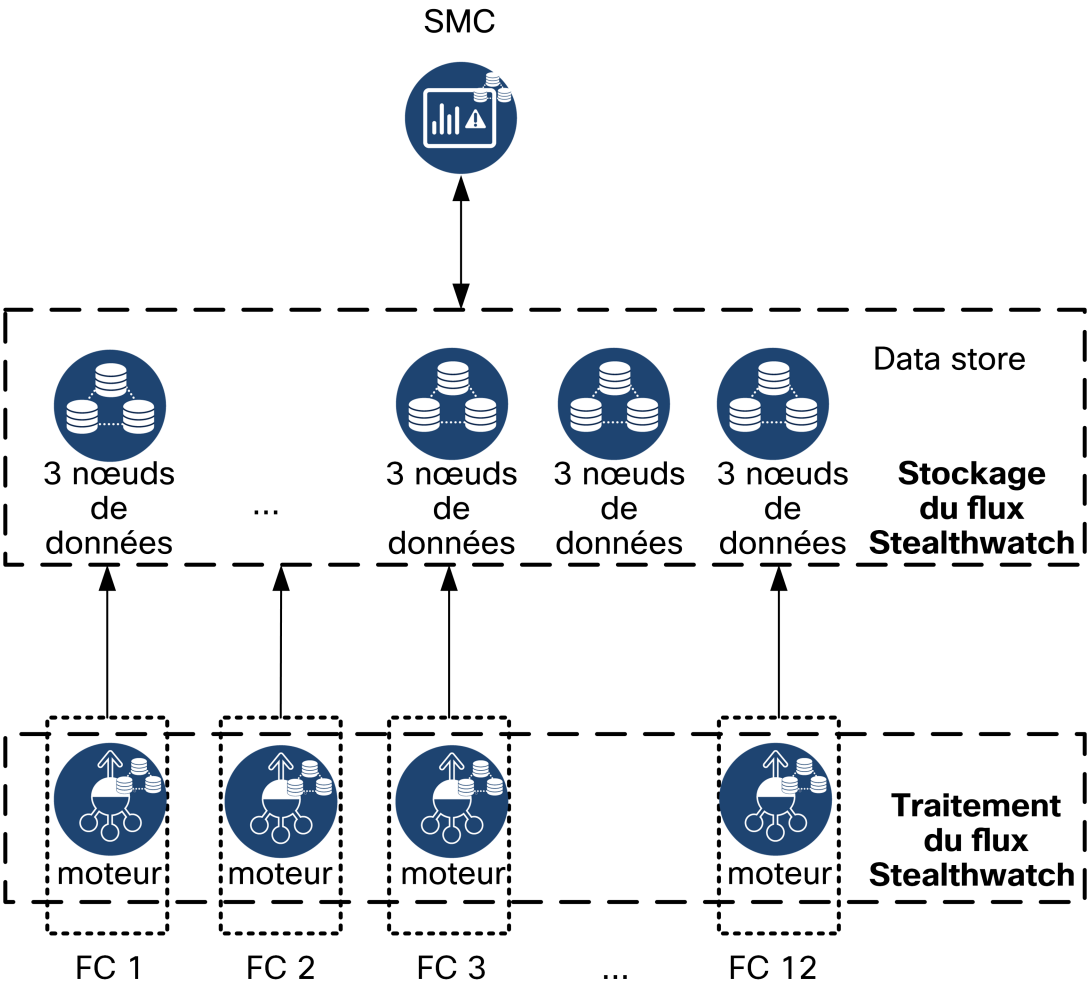


Stealthwatch Architecture de déploiement du data store

Dans un déploiement Stealthwatch classique sans data store, un ou plusieurs collecteurs de flux intègrent et dédupliquent les données, effectuent des analyses, et consignent les données et les résultats directement sur la console SMC. Pour résoudre les requêtes envoyées par l'utilisateur, y compris les graphiques et les diagrammes, la console SMC interroge tous les collecteurs de flux gérés. Chaque collecteur de flux renvoie les résultats correspondants à la console SMC. La console SMC collecte les informations des différents jeux de résultats, puis génère un graphique ou un diagramme affichant les résultats. Dans ce déploiement, chaque collecteur de flux stocke les données dans une base de données locale. Reportez-vous au schéma suivant pour voir un exemple.



Dans un déploiement Stealthwatch avec un data store, le cluster data store se trouve entre votre console SMC et vos collecteurs de flux. Un ou plusieurs collecteurs de flux intègrent et dédupliquent les flux, effectuent des analyses, et transmettent les données et les résultats directement au data store, en les distribuant de façon plus ou moins équitable à l'ensemble des nœuds de données. Le data store facilite le stockage des données, conserve l'ensemble de votre trafic dans cet emplacement centralisé et non sur plusieurs collecteurs de flux, et offre une capacité de stockage supérieure à celle de plusieurs collecteurs de flux. Reportez-vous au schéma suivant pour voir un exemple.



Pour résoudre les requêtes envoyées par l'utilisateur, y compris les graphiques et les diagrammes, la console SMC interroge le data store. Le data store recherche les résultats connexes dans les colonnes correspondant à la requête, puis récupère les lignes correspondantes et renvoie les résultats de la requête à la console SMC. La console SMC génère le graphique ou le diagramme sans avoir à assembler plusieurs jeux de résultats à partir de plusieurs collecteurs de flux. Cela réduit le coût des requêtes et améliore les performances d'interrogation.

Étant donné l'architecture du data store, la console SMC et tous les collecteurs de flux doivent communiquer avec le data store, et doivent être configurés pendant le déploiement pour fonctionner avec le data store. Vous ne pouvez pas créer un environnement « mixte », parmi lequel certains collecteurs de flux relèvent directement de la console SMC et d'autres du data store.

Architecture du data store Stealthwatch

Chaque data store est composé d'au moins 3 nœuds de données. Chaque nœud de données constitue son propre châssis matériel. Lorsque vous achetez un data store, vous recevez plusieurs châssis matériels de nœuds de données, qui correspondent au nombre de nœuds indiqué par ce modèle de data store. Par exemple, un data store DS 6200 fournit 3 châssis matériels de nœuds de données.

Vous pouvez acheter plusieurs data store pour votre déploiement. Il est possible de mettre en cluster les nœuds de données dans le cadre de votre data store en plusieurs multiples de 3, de 3 minimum à 36 maximum.

> Cisco vous recommande de configurer votre nœud de données de sorte à alimenter les nœuds de données numérotés adjacents par des modules d'alimentation redondante distincts. Cette configuration améliore la redondance des données et la disponibilité globale du data store. Reportez-vous à la section Exigences et considérations relatives au déploiement du data store pour plus d'informations.

Pour déployer un data store, vous devez attribuer les éléments suivants à chaque nœud de données :

- Une adresse IP routable pour la gestion, l'intégration et l'interrogation des communications avec vos appliances Stealthwatch
- Une adresse IP non routable (bloc CIDR `169.254.42.0/24`) sur un LAN ou un VLAN isolé pour les communications entre les nœuds de données dans le cadre du cluster de data store
- Deux connexions 10G, une pour les communications de gestion, d'intégration et d'interrogation, une pour les communications entre les nœuds de données
- Éventuellement, pour assurer la redondance du réseau et la criticité des communications entre les nœuds de données, une connexion 10G supplémentaire et un commutateur supplémentaire pour établir un canal de port sur le nœud de données

Reportez-vous à la section Exigences et recommandations relatives au déploiement du data store pour plus d'informations sur le déploiement et les conditions préalables au déploiement.

Exigences et recommandations relatives au déploiement du data store

Vous trouverez ci-après des informations sur les exigences et les recommandations relatives au déploiement de votre data store.

> Si vous envisagez d'acheter un Stealthwatch data store, contactez les services professionnels Cisco pour obtenir de l'aide concernant le placement, le déploiement et la configuration dans le cadre de votre déploiement Stealthwatch global.

Version Stealthwatch prise en charge

Lorsque vous déployez un data store, toutes vos appliances Stealthwatch doivent disposer de la même version (version 7.3+).

Licence Stealthwatch

Le déploiement de votre Stealthwatch nécessite une licence Smart Flow Rate (FPS) ; le data store proprement dit ne nécessite aucune licence supplémentaire.

Compatibilité matérielle Stealthwatch et configuration réseau requise

Le tableau suivant présente le matériel requis pour déployer un data store.

Composant matériel	**Capacité prise en charge**
data store	• 3 nœuds de données minimum (DS 6200) • Jeux supplémentaires de 3 nœuds de données pour étendre le data store, avec un maximum 36 nœuds de données
Console de gestion Stealthwatch	• 1 console de gestion Stealthwatch minimum
Collecteur de flux	• 1 collecteur de flux minimum

Notez que vous devez obtenir une licence Smart Flow Rate (FPS) pour votre déploiement Stealthwatch global.

> ⚠ Ne mettez pas à jour le BIOS de l'appliance, car cela pourrait entraîner un dysfonctionnement.

Si vous souhaitez déployer un data store, vous devez disposer d'au moins 3 nœuds de données. Un data store 6200 avec 3 nœuds de données peut gérer environ 500 000 flux par seconde et conserver ces données pendant environ 90 jours. Vous pouvez étendre votre data store avec des nœuds de données supplémentaires, par multiples de 3, jusqu'à un maximum de 36 nœuds de données.

> ⓘ Ces recommandations ne prennent en compte que la télémétrie. Vos performances peuvent varier en fonction d'autres facteurs, notamment du nombre d'hôtes, de l'utilisation de capteurs de flux, des profils de trafic et d'autres caractéristiques du réseau. Contactez l'assistance Cisco pour obtenir de l'aide sur le dimensionnement.

> ⓘ À l'heure actuelle, le data store ne prend pas en charge le déploiement de nœuds de données de rechange dans le cadre de remplacements automatiques en cas de panne d'un nœud de données principal. Contactez l'assistance Cisco pour obtenir de l'aide.

Vous devez déployer une console SMC avec votre data store, et la configurer pour l'utiliser avec un data store. Pour disposer d'une console SMC haute disponibilité, vous pouvez également déployer une console SMC de basculement.

En outre, vous devez déployer au moins 1 collecteur de flux avec votre data store, et configurer les collecteurs de flux en vue de les utiliser avec un data store.

Pour chaque console SMC et collecteur de flux que vous déployez, vous devez attribuer une adresse IP publique routable au port de gestion `eth0`. Lors du déploiement d'un data store, vous pouvez configurer l'utilisation d'un port cuivre 1G/10G BASE-T ou d'un port câble Twinax SFP+ 10G pour le port de gestion `eth0` de la console SMC et du collecteur de flux. Pour utiliser un data store, vous devez disposer d'un port cuivre BASE-T d'un débit de 10G. Les utilisateurs qui ne déploient pas de data store peuvent uniquement configurer l'interface cuivre 100 Mbit/s/1 Gbit/s/10 Gbit/s sur `eth0`.

Vous pouvez également déployer des capteurs de flux et des solutions UDP Director dans le cadre du déploiement de votre Stealthwatch. Étant donné que ces appliances ne communiquent pas directement avec le data store, il est inutile de les configurer pour les utiliser avec un data store.

Reportez-vous aux fiches techniques correspondantes pour plus d'informations sur les plateformes prises en charge. Reportez-vous à la section Matrice de compatibilité des versions matérielles et logicielles de Stealthwatch pour plus d'informations sur la compatibilité des versions.

Considérations relatives au déploiement en entreprise Stealthwatch

Notez les éléments suivants :

- Si vous configurez un collecteur de flux pour la compatibilité du data store, l'interface d'administration de l'appliance (administrateur de l'appliance) masque certaines fonctionnalités. Utilisez Central Management pour configurer le collecteur de flux et effectuer d'autres tâches connexes. Si vous souhaitez surveiller les statistiques de stockage, téléchargez l'application Report Builder sur votre console SMC.
- Utilisez l'application web Stealthwatch pour surveiller et configurer votre installation Stealthwatch si vous déployez un data store. Le client de bureau Stealthwatch n'est pas compatible avec un data store.
- Si vous configurez votre console SMC pour une utilisation avec un data store, vous ne pouvez pas utiliser les applications Audit cryptographique ETA ou Classificateur d'hôtes.

Informations d'identification requises pour le déploiement du data store

Préparez les mots de passe pour les comptes utilisateur suivants :

- `root` et `sysadmin` pour chaque console SMC, nœud de données et collecteur de flux. Vous attribuez ces mots de passe lors de la configuration initiale du système.
- `admin` pour chaque console SMC, nœud de données et collecteur de flux. Vous pouvez attribuer ce mot de passe à l'aide de l'outil de configuration de l'appliance.
- `dbadmin` et `readonlyuser` pour le data store. Vous attribuez ces mots de passe lors de l'initialisation du data store.

Considérations relatives aux réseaux et à la commutation du data store

Le tableau suivant fournit un aperçu des considérations relatives aux réseaux et à la commutation lors du déploiement d'un data store.

Considérations relatives au réseau	**Description**
Informations d'identification requises	Pour chaque nœud de données, console de gestion Stealthwatch et collecteur de flux : • Configuré lors de la configuration initiale du système : `root`, `sysadmin` • Configuré à l'aide de l'outil de configuration de l'appliance : `admin` • Configuré au cours de l'initialisation de data store : `dbadmin`, `readonlyuser`
Communications entre nœud de données	• Spécifiez une latence RTT (durée aller-retour) recommandée inférieure à 200 microsecondes entre les nœuds de données. • Conservez une distorsion d'horloge de 1 seconde ou inférieure entre vos nœuds de données. • Spécifiez un débit recommandé de 6,4 Gbit/s ou supérieur (connexion commutée duplex intégral de 10 Gbit/s) entre vos nœuds de données.
Alimentation du nœud de données matériel	• Si un nœud de données matériel tombe en panne de façon inattendue, les données peuvent être endommagées. Utilisez les deux modules d'alimentation sur des circuits distincts des modules d'alimentation sans coupure. • Lorsque vous initialisez le cluster de data store (reportez-vous à la section Initialisation et configuration du data store pour plus d'informations), modifiez la configuration du nœud de données en fonction des modules d'alimentation que chaque nœud de données utilise. Cela vous permettra d'optimiser la tolérance aux pannes en réduisant le nombre

	de nœuds de données qui cessent de fonctionner en cas de panne d'alimentation.
Commutation des nœuds de données	• Les nœuds de données nécessitent leur propre VLAN de couche 2 pour permettre la communication entre les nœuds de données. Il est possible de connecter les nœuds de données matériels à un commutateur 10G partagé ou dédié. • Cisco recommande de connecter les nœuds de données matériels à 2 commutateurs pour garantir une connectivité constante en cas de panne et de mise à niveau des commutateurs. En raison de la faible latence requise pour la communication entre les nœuds de données, Cisco recommande une paire de commutateurs redondants, où les 2 commutateurs sont interconnectés et transportent le VLAN de couche 2 sur les deux commutateurs.
Communications de l'appliance Stealthwatch	• Accès SSH et SSH racine requis pour la console SMC, les nœuds de données et les collecteurs de flux, et configurés à partir de la console SMC. • La console SMC et les collecteurs de flux doivent pouvoir accéder à tous les nœuds de données. • Les nœuds de données doivent pouvoir accéder à la console SMC, à tous les collecteurs de flux et à chaque nœud de données

Vous devez attribuer les adresses IP suivantes à chaque nœud de données :

- Une adresse IP routable pour la communication avec vos appliances Stealthwatch (`eth0`). Connectez le port `eth0` du nœud de données à votre réseau pour permettre la communication avec votre console SMC et vos collecteurs de flux. Vous pouvez configurer l'utilisation d'un port cuivre 1G/10G BASE-T ou d'un port câble Twinax 10G SFP+ pour le port de gestion `eth0` du nœud de données .

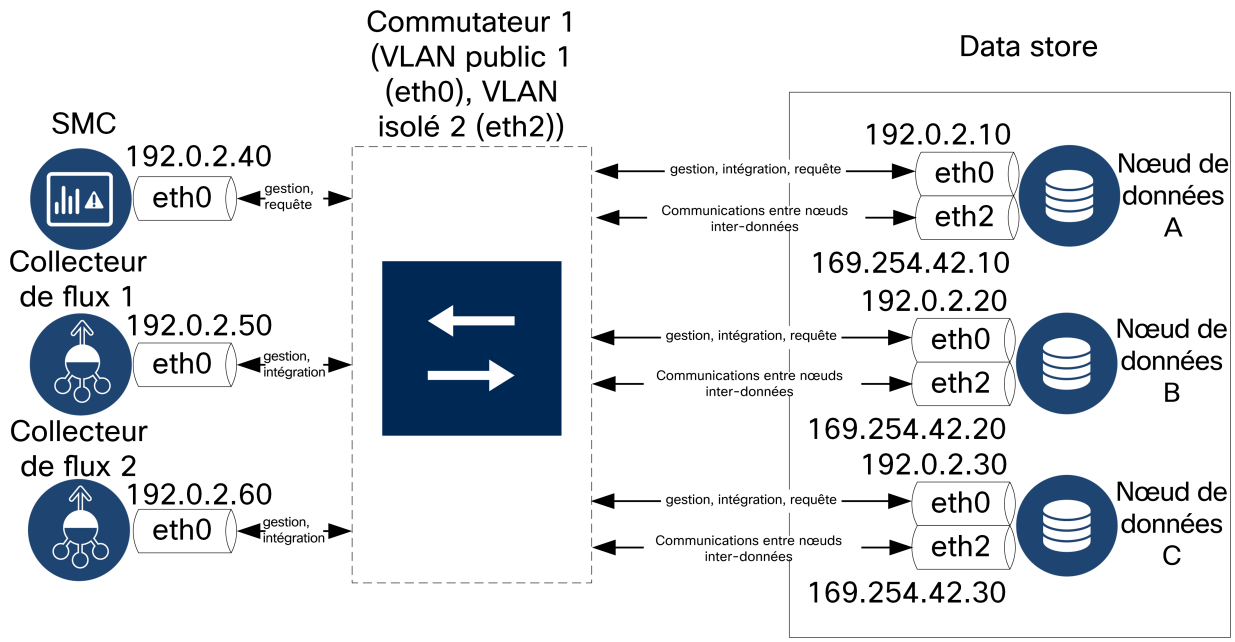
  Au cours du déploiement et de la configuration du data store, vous mappez les adresses IP `eth0` du nœud de données sur le nom du data store pour permettre une distribution plus équitable du stockage de télémétrie, ainsi que des requêtes et des réponses. Reportez-vous à la section Initialisation et configuration de la base de données du data store pour plus d'informations.
- Une adresse IP non routable dans un LAN ou un VLAN privé, à utiliser pour la

communication entre les nœuds de données (`eth2`, ou canal de port contenant `eth2` et `eth3` pour améliorer le débit et les performances). Dans le cadre du data store, vos nœuds de données communiquent entre eux. Connectez le port `eth2` du nœud de données ou le canal de port contenant `eth2` et `eth3` aux commutateurs pour assurer la communication entre les nœuds de données.

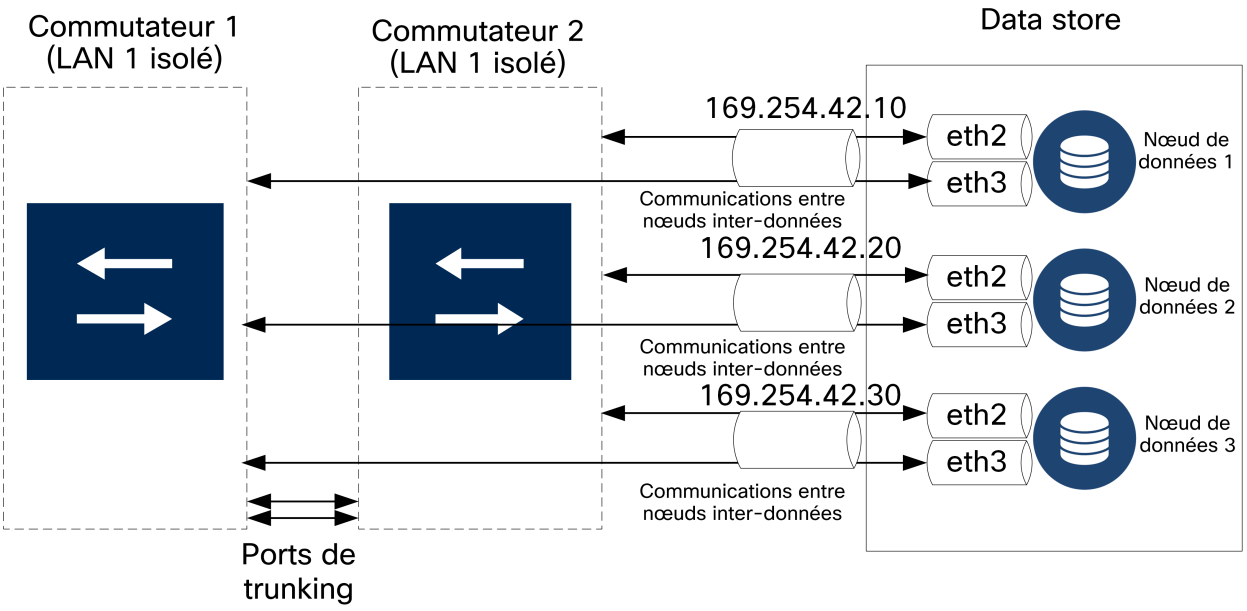
> Vous devez attribuer les adresses IP non routables du port `eth2` ou du canal de port `eth2/eth3` à partir du bloc CIDR `169.254.42.0/24`.

La configuration d'un port `eth2` pour le débit 10G est suffisante pour une communication normale entre les nœuds de données. La création d'un canal de port `eth2/eth3` pour un débit allant jusqu'à 20G permet d'assurer une communication plus rapide entre les nœuds de données, et d'ajouter ou de remplacer un nœud de données plus rapidement sur le data store, car chaque nouveau nœud de données reçoit le trafic des nœuds de données adjacents afin d'alimenter ses données.

Pour activer les communications entre les nœuds de données via `eth2` ou le canal de port `eth2/eth3`, vous devez déployer 1 commutateur prenant en charge les débits 10G. Configurez un LAN ou un VLAN public pour les communications `eth0` des nœuds de données avec la console SMC et les collecteurs de flux, et un LAN ou un VLAN isolé pour les communications entre les nœuds de données. Vous pouvez partager ces commutateurs avec d'autres appliances, mais créer des LAN ou des VLAN distincts pour le trafic supplémentaire de l'appliance. Reportez-vous au schéma suivant pour obtenir un exemple :



Le cluster de data store nécessite une pulsation continue entre les nœuds au sein du VLAN isolé. Sans cette pulsation, les nœuds de données risquent de se déconnecter, ce qui augmente le risque de panne du data store. Si vous souhaitez disposer d'une redondance réseau supplémentaire pour planifier les mises à jour des commutateurs et les interruptions, Cisco vous recommande de configurer vos nœuds de données avec des canaux de port pour la communication dédiée entre les nœuds de données. Connectez chaque nœud de données à 2 commutateurs, chaque port physique étant connecté à un commutateur différent. Reportez-vous au schéma suivant pour obtenir un exemple :



Contactez les services professionnels Cisco pour vous aider à planifier votre déploiement.

Exigences et considérations relatives au déploiement du data store

Placez chaque nœud de données de façon à ce qu'il puisse communiquer avec tous vos collecteurs de flux, votre console SMC et tous les autres nœuds de données. Pour optimiser les performances, placez ensemble les nœuds de données et les collecteurs de flux afin de minimiser la latence des communications, et ensemble les nœuds de données et la console SMC pour optimiser les performances des requêtes. Cisco recommande vivement de placer les nœuds de données dans votre pare-feu, par exemple dans un centre d'exploitation du réseau. Tenez compte des éléments suivants pour améliorer les performances :

- Spécifiez une latence RTT (durée aller-retour) recommandée inférieure à 200 microsecondes entre les nœuds de données lorsque vous les déployez.
- Conservez une distorsion d'horloge de 1 seconde ou inférieure entre vos nœuds de données.
- Établissez un débit recommandé de 6,4 Gbit/s ou supérieur (connexion commutée duplex intégral de 10 Gbit/s) entre vos nœuds de données.

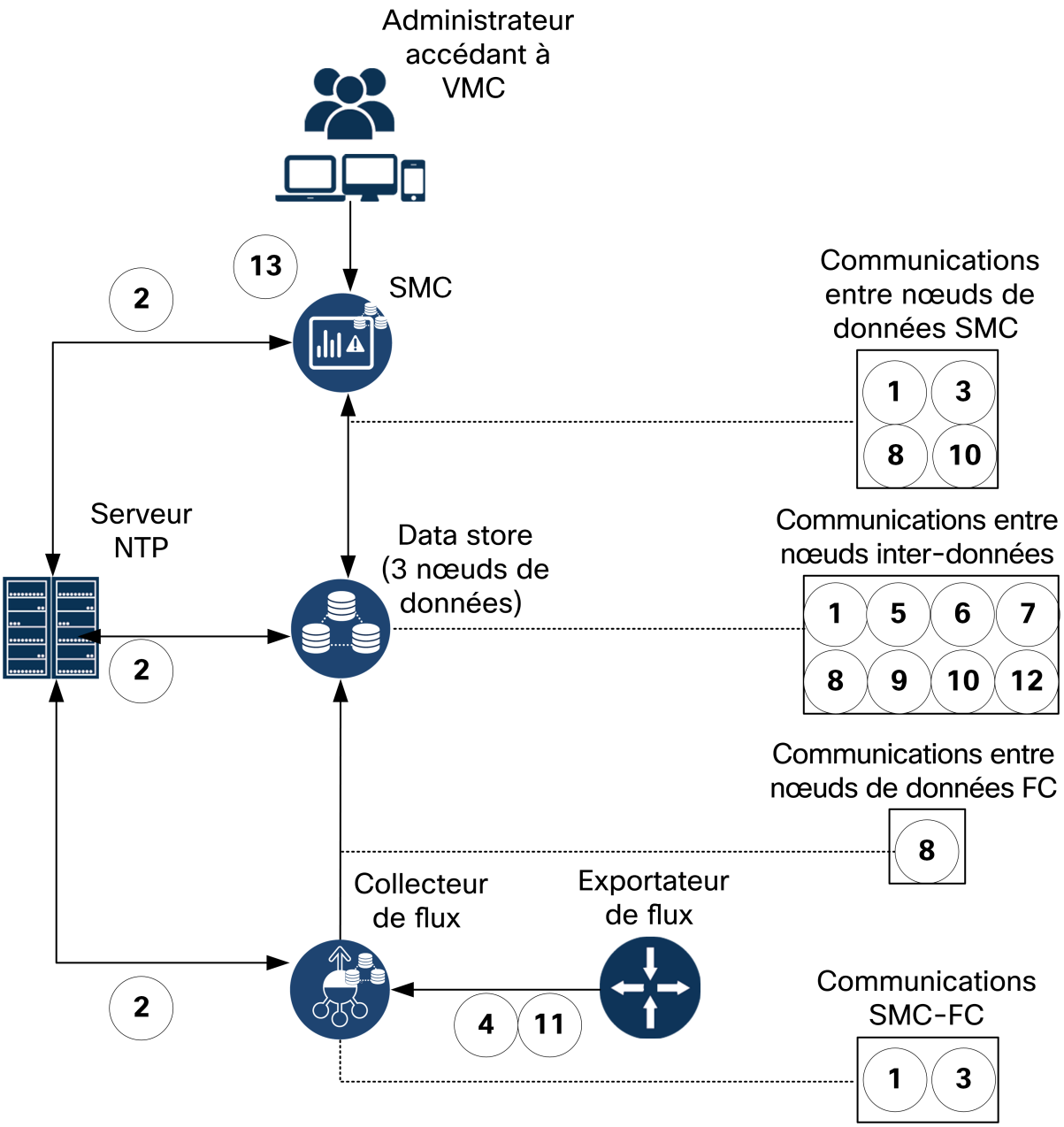
L'arrêt du data store suite à une panne d'alimentation ou à une panne matérielle implique un risque accru de corruption ou de perte des données. Cisco recommande d'installer vos nœuds de données de sorte à assurer une disponibilité constante. Analysons les faits suivants :

- Cisco recommande vivement d'installer des modules d'alimentation redondants ou sans coupure pour tous les nœuds de données, afin d'éviter toute perte ou corruption de données en cas de panne d'alimentation.
- Vérifiez que la politique de restauration de l'alimentation du nœud de données est définie sur l'option **Restaurer le dernier état**, qui permet de redémarrer automatiquement le nœud de données après une panne d'alimentation et de tenter de restaurer les processus en cours d'exécution. Reportez-vous au Guide de configuration de l'interface utilisateur graphique des systèmes UCS C pour plus d'informations sur la configuration de la politique de restauration de l'alimentation dans CIMC.
- Lorsque vous initialisez le data store (reportez-vous à la section Initialisation et configuration de la base de données du data store pour en savoir plus), alternez la configuration du nœud de données en fonction de l'alimentation. Le data store crée une sauvegarde du nœud de données sur le nœud de données suivant dans la séquence lors de la configuration et une sauvegarde du dernier nœud de données configuré sur le premier nœud de données configuré. Si vous déployez vos nœuds de données sur deux modules d'alimentation distincts et utilisez en alternance des nœuds de données pairs et impairs en fonction du bloc d'alimentation, si un bloc d'alimentation tombe en panne et que vous disposez d'un nombre pair de nœuds, le data store reste actif, car les données ou les données de sauvegarde de chaque nœud de données sont accessibles depuis le nœud de données alimenté.

> Si un nœud de données tombe en panne de manière inattendue et que vous redémarrez l'appliance, l'instance de base de données sur ce nœud de données risque de ne pas redémarrer automatiquement. Reportez-vous à la section Résolution des problèmes liés au data store pour plus d'informations sur le redémarrage manuel de l'instance de base de données.

Ports de communication du data store

Le schéma suivant présente un exemple d'architecture de Stealthwatch, avec les ports de communication à ouvrir. Reportez-vous au tableau pour connaître les ports associés à chaque légende.



La liste suivante répertorie les ports de communication à ouvrir sur votre pare-feu pour déployer le data store. Consultez le Guide de configuration du système Stealthwatch pour connaître les ports de communication supplémentaires à ouvrir pour votre déploiement Stealthwatch global.

N°	De (client)	À (serveur)	Port	Protocole ou objectif
1	SMC	Collecteurs	22/TCP	SSH, requis pour initialiser la

		de flux et nœuds de données		base de données data store
1	Nœuds de données	Tous les autres nœuds de données	22/TCP	SSH, requis pour initialiser la base de données data store et pour exécuter les tâches d'administration de la base de données
2	SMC, collecteurs de flux et nœuds de données	Serveur NTP	123/UDP	NTP, requis pour la synchronisation de l'heure
2	Serveur NTP	SMC, collecteurs de flux et nœuds de données	123/UDP	NTP, requis pour la synchronisation de l'heure
3	SMC	Collecteurs de flux et nœuds de données	443/TCP	HTTPS, requis pour sécuriser les communications entre les appliances
3	Collecteurs de flux	SMC	443/TCP	HTTPS, requis pour sécuriser les communications entre les appliances
3	Nœuds de données	SMC	443/TCP	HTTPS, requis pour sécuriser les communications entre les appliances
4	Exportateurs NetFlow	Collecteurs de flux – NetFlow	2055/UDP	Intégration NetFlow
5	Nœuds de données	Tous les autres	4803/TCP	Service de messagerie entre les nœuds de données

		nœuds de données		
6	Nœuds de données	Tous les autres nœuds de données	4803/UDP	Service de messagerie entre les nœuds de données
7	Nœuds de données	Tous les autres nœuds de données	4804/UDP	Service de messagerie entre les nœuds de données
8	SMC, collecteurs de flux et nœuds de données	Nœuds de données	5433/TCP	Connexions client Vertica
9	Nœuds de données	Tous les autres nœuds de données	5433/UDP	Surveillance du service de messagerie Vertica
10	SMC	Nœuds de données	5444/TCP	Communications sécurisées de la console de gestion Vertica
10	Nœuds de données	SMC et tous les autres nœuds de données	5444/TCP	Communications sécurisées de la console de gestion Vertica
11	Exportateurs sFlow	Collecteur de flux – sFlow	6343/UDP	Intégration sFlow
12	Nœuds de données	Tous les autres nœuds de données	6543/UDP	Service de messagerie entre les nœuds de données

13	Postes de travail d'administrateur pour accéder à la console de gestion Vertica	SMC	9450/TCP	Accès au navigateur web de la console de gestion Vertica

Présentation du déploiement du data store Stealthwatch

> ⚠ Si vous envisagez d'acheter un data store, contactez les services professionnels Cisco pour obtenir de l'aide concernant le placement, le déploiement et la configuration dans le cadre de votre déploiement Stealthwatch global. Veillez à ne **pas** installer un data store vous-même.

Voici les étapes générales du déploiement d'un data store dans le cadre d'un déploiement Stealthwatch :

- Déployez vos appliances Stealthwatch, y compris vos nœuds de données, et configurez vos consoles SMC et vos collecteurs de flux pour les utiliser avec un data store

  > ⓘ Veillez à installer la dernière version et le correctif cumulatif pour vos appliances après les avoir déployées, mais avant de procéder à l'initialisation et à la configuration du data store.

- Préparez votre déploiement Stealthwatch pour le data store en distribuant les mots de passe et les certificats d'identité des utilisateurs
- Initialisez le data store
- Configurez la console de gestion Vertica (VMC) sur votre console SMC, et activez le seuil d'alerte et les notifications
- Configurez les paramètres de conservation du data store via l'API REST
- Installez des applications Stealthwatch sur votre console SMC pour utiliser d'autres fonctionnalités liées au data store

Passez en revue ces tâches avant de commencer votre déploiement.

Composant requis et tâche	**Étapes**
Installation et configuration de la console	Reportez-vous à la section Configuration de la console SMC en vue de l'utiliser avec un data store pour plus d'informations. 1. Déployez votre console SMC sur votre réseau.

SMC	2. En utilisant CIMC ou en vous connectant directement à l'appliance, connectez-vous à la console SMC en tant qu'utilisateur `root`. Exécutez le script de configuration système `systemconfig` et utilisez l'assistant de configuration initiale pour configurer les informations de gestion de base, notamment l'adresse IP de l'appliance, l'utilisation avec un data store et la configuration du port physique `eth0`. 3. À partir d'un navigateur web, accédez à l'adresse IP `eth0` de la console SMC pour accéder à l'outil de configuration de l'appliance. Utilisez l'outil de configuration de l'appliance pour configurer les mots de passe de l'administrateur, le domaine du Stealthwatch et les serveurs DNS et NTP, et pour installer Central Management. 4. À partir d'un navigateur web, accédez à l'adresse IP de la console SMC après avoir configuré l'appliance à l'aide de l'outil de configuration de l'appliance pour accéder à l'application web Stealthwatch. Dans Central Management, activez l'accès SSH et l'accès SSH racine à la console SMC. 5. Mettez à jour votre console SMC vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.
Installation et configuration du nœud de données	Consultez le Guide de déploiement et de configuration matérielle du data store pour en savoir plus. 1. Déployez vos nœuds de données sur votre réseau. 2. En utilisant CIMC ou en vous connectant directement à l'appliance, connectez-vous à la console de chaque nœud de données en tant qu'utilisateur `root`. Exécutez le script de configuration système `systemconfig` et utilisez l'assistant de configuration initiale pour configurer les informations de gestion de base, notamment l'adresse IP de gestion de l'appliance et l'adresse IP non routable de communication entre les nœuds de données (avec la configuration facultative du canal de port). Attribuez une adresse IP non routable au canal de port `eth2` ou `eth2/eth3` à partir du bloc CIDR `169.254.42.0/24`.

	3. Pour chaque nœud de données, accédez à l'adresse IP routable `eth0` du nœud de données à partir d'un navigateur web pour accéder à l'outil de configuration de l'appliance. Utilisez l'outil de configuration de l'appliance sur chaque nœud de données pour configurer les mots de passe de l'administrateur, le domaine du Stealthwatch et les serveurs DNS et NTP, et pour demander à Central Management de gérer le nœud de données. 4. À partir de l'application web Stealthwatch, accédez à Central Management, puis activez l'accès SSH et l'accès SSH racine à chaque nœud de données. 5. Mettez à jour vos nœuds de données vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs. **Consultez les guides de mise à jour et les fichiers Lisez-moi des correctifs pertinents avant de continuer. Le processus de mise à jour du nœud de données nécessite des étapes supplémentaires par rapport aux autres appliances Stealthwatch.**
Installation et configuration du collecteur de flux	Reportez-vous à la section Configuration du collecteur de flux en vue de l'utiliser avec un data store pour plus d'informations. 1. Déployez vos collecteurs de flux sur votre réseau. 2. En utilisant CIMC ou en vous connectant directement à l'appliance, connectez-vous à la console de chaque collecteur de flux en tant qu'utilisateur `root`. Exécutez le script de configuration système `systemconfig` et utilisez l'assistant de configuration initiale pour configurer les informations de gestion de base, notamment l'adresse IP de l'appliance, l'utilisation avec un data store et la configuration du port physique eth0. 3. Pour chaque collecteur de flux, accédez à l'adresse IP `eth0` du collecteur de flux à partir d'un navigateur web pour accéder à l'outil de configuration de l'appliance. Utilisez l'outil de configuration de l'appliance sur chaque collecteur de flux pour

	configurer les mots de passe de l'administrateur, le domaine du Stealthwatch, les serveurs DNS et NTP et le numéro de port de collecte de flux (`2055` pour NetFlow ou `6343` pour sFlow), et pour demander à Central Management de gérer le collecteur de flux. 4. À partir de l'application web Stealthwatch, accédez à Central Management et activez l'accès SSH et l'accès SSH racine sur chaque collecteur de flux. 5. Mettez à jour vos collecteurs de flux vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.
Initialisation et configuration du data store	Consultez la section Initialisation et configuration de la base de données du data store pour en savoir plus. 1. À partir de l'application web Stealthwatch, accédez à Central Management et vérifiez que tous vos nœuds de données et collecteurs de flux sont gérés dans Central Management, que la connexion est active, et que l'accès SSH et l'accès SSH racine sont activés. 2. Connectez-vous à la console SMC principale en tant qu'utilisateur `sysadmin`. À l'aide du script de connectivité sécurisée à la base de données `setup-sw-datastore-secure-connectivity`, distribuez les mots de passe `dbadmin` et `readonlyuser` de la base de données et les certificats d'identité à vos consoles SMC, vos nœuds de données et vos collecteurs de flux. 3. En fonction du résultat du script de connectivité sécurisée `setup-sw-datastore-secure-connectivity`, connectez-vous à la console du nœud de données spécifié en tant qu'utilisateur `root`. Copiez le fichier d'exemple de configuration d'initialisation de la base de données `install_SDBN_example.cfg` en tant que fichier `install_SDBN.cfg` et mettez-le à jour avec les adresses IP et le sous-réseau de votre nœud de données. Exécutez le script d'initialisation en vous référant au fichier de configuration d'initialisation (`python`

	`install_SDBN_initial.py -i install_SDBN.cfg`). 4. À partir du nœud de données sur lequel vous avez exécuté le script d'initialisation, récupérez la chaîne de clé d'API auprès de `/opt/vertica/config/apikey.dat`. Vous utiliserez cette clé d'API pour établir ultérieurement une connexion entre la base de données du data store et la console VMC. 5. À partir de l'application web Stealthwatch, accédez à Central Management et, pour la console SMC et tous les collecteurs de flux, utilisez la résolution locale pour mapper le nom de la base de données du data store (`sw-datastore`) sur l'adresse IP routable de chaque nœud de données. Pour des performances optimales, mappez les adresses IP `eth0` du nœud de données dans le même ordre pour chaque appliance.
Installation et configuration de la console de gestion Vertica (VMC) sur la console SMC	Reportez-vous à la section Configuration de la console de gestion Vertica pour plus d'informations. 1. Copiez le certificat du serveur `/lancope/var/admin/cds/server.crt` de votre console SMC sur votre poste de travail local. 2. Sur votre poste de travail local, accédez à `[smc-ipv4-address]:9450/webui/login` à partir d'un navigateur web pour accéder à la console VMC. Effectuez la configuration initiale de la console VMC. Désactivez les connexions qui utilisent des versions moins sécurisées de TLS. Utilisez la chaîne de clé d'API et le fichier de certificat `server.crt` pour établir une connexion avec le data store. Configurez les seuils d'alerte et les notifications d'alerte pour recevoir les alertes d'intégrité du data store.
Conservation des données du data store	Reportez-vous à la section Configuration de la conservation du data store pour plus d'informations. • Utilisez l'API REST pour configurer la période de conservation de votre data store.
Passer en revue les étapes	Passez en revue les étapes postérieures à l'installation du data store :

postérieures au déploiement du data store	1. Installez l'application Stealthwatch Report Builder sur votre console SMC pour exécuter des rapports sur votre déploiement Stealthwatch et afficher les statistiques de stockage du data store. Reportez-vous aux notes de version pour plus d'informations. 2. Consultez l'aide en ligne de l'application web Stealthwatch pour en savoir plus sur l'utilisation du Stealthwatch.

Vous pouvez également procéder comme suit :

Composant en option et tâche	**Étapes**
Installation et configuration de UDP Director	• Déployez UDP Director en suivant les instructions du Guide d'installation matérielle des appliances Stealthwatch x2xx et du Guide de configuration du système Stealthwatch. Mettez à jour votre UDP Director vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.
Capteur de flux	• Déployez le capteur de flux en suivant les instructions du Guide d'installation matérielle des appliances Stealthwatch x2xx et du Guide de configuration du système Stealthwatch. Mettez à jour votre capteur de flux vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.
Installation et configuration de la console SMC de	• Déployez la console SMC de basculement en suivant les instructions du Guide d'installation matérielle des appliances Stealthwatch x2xx, du Guide de configuration du système Stealthwatch et du Guide de configuration du basculement Stealthwatch. Mettez à jour votre console SMC vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise

basculement	à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.

Installation matérielle du data store

> Si vous envisagez d'acheter un Stealthwatch data store, contactez les services professionnels Cisco pour obtenir de l'aide concernant le placement, le déploiement et la configuration dans le cadre de votre déploiement Stealthwatch global.

Considérations relatives au déploiement du matériel Stealthwatch

Déployez et configurez vos consoles SMC, vos nœuds de données et vos collecteurs de flux Stealthwatch en suivant les instructions ci-dessous, puis installez les commutateurs pour le data store correspondant à votre réseau. Lorsque vous déployez vos nœuds de données et les connectez à votre réseau, consultez la section Exigences et considérations relatives au déploiement du data store. Assurez-vous que vos consoles SMC, vos nœuds de données et vos collecteurs de flux sont de la même version (7.3+). Reportez-vous au Guide d'installation matérielle des appliances Stealthwatch x210 ou à l'**Annexe A. Préparation de l'installation** et à l'**Annexe B. Installation du matériel Stealthwatch** pour plus d'informations sur l'installation et la configuration initiales des appliances.

> Si vous souhaitez déployer un data store sur votre réseau dans le cadre d'un déploiement Stealthwatch existant, utilisez les services professionnels Cisco pour intégrer le data store. Contactez le service d'assistance Cisco pour plus d'informations.

> Utilisez l'application web Stealthwatch pour contrôler et configurer votre installation Stealthwatch si vous déployez un data store. Le client de bureau Stealthwatch n'est pas compatible avec un data store.

Configuration de la console SMC en vue de l'utiliser avec un data store

Déployez et configurez votre console SMC pour l'utiliser avec un data store, mais aussi pour gérer vos nœuds de données et collecteurs de flux.

> Si vous disposez d'une console SMC secondaire, configurez-la en premier afin que la console SMC principale puisse communiquer avec elle. Reportez-vous

au Guide de configuration du système Stealthwatch pour plus d'informations sur l'établissement d'une paire de basculement SMC. Reportez-vous à la section **Déployer la console de gestion Stealthwatch de basculement** pour en savoir plus sur le déploiement et la configuration d'une console SMC secondaire avec un data store.

Procédez comme suit :

1. Commencez par déployer votre console SMC sur le réseau. Connectez-vous ensuite à votre appliance avec CIMC, un clavier et un écran (ou un ordinateur portable) et connectez-vous à la console en tant qu'utilisateur `root`. Exécutez `systemconfig` et utilisez l'assistant de configuration initiale pour mettre à jour les paramètres du port de gestion, l'utilisation avec un data store, et les mots de passe utilisateur `root` et `sysadmin`. Reportez-vous au Guide d'installation matérielle des appliances Stealthwatch x210 ou à l'**Annexe A. Préparation de l'installation** et l'**Annexe B. Installation du matériel Stealthwatch** pour plus d'informations.

   La première fois que vous accédez à la configuration du système, celui-ci vous dirige vers l'assistant de configuration initiale, qui vous guide automatiquement au cours du processus de configuration initiale de l'appliance.

   Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez pas mettre à jour la configuration de l'appliance en vue de la modifier. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option uniquement si vous prévoyez de déployer un data store sur votre réseau.

2. Ouvrez ensuite un navigateur web et accédez à l'adresse IP que vous avez attribuée au port de gestion. Utilisez l'outil de configuration de l'appliance pour effectuer une configuration supplémentaire, notamment l'attribution du mot de passe de l'utilisateur `admin` (et des mots de passe utilisateur `root` et `sysadmin` si vous ne les avez pas attribués lors de la configuration du système), la configuration du domaine Stealthwatch, une autre configuration réseau, les paramètres DNS et NTP, ainsi que l'installation de Central Management sur la console SMC. Reportez-vous au Guide de configuration du système Stealthwatch ou à l'**Annexe C. Configuration de vos appliances** pour plus d'informations.

3. Activez ensuite l'accès SSH et l'accès racine SSH sur votre console SMC. Pour initialiser le data store conformément aux instructions de la section **Initialisation et configuration du data store**, vous devez exécuter un script basé sur l'accès SSH sur chaque appliance.

   > ⚠ Une fois la console SSH activée, le risque de compromission du système augmente. Il est important d'activer SSH uniquement lorsque vous en avez besoin. Lorsque vous avez terminé d'utiliser l'accès SSH, désactivez-le.

Mettre à jour l'autorisation d'accès SSH de la console SMC

Avant de commencer

- Connectez-vous à l'application web SMC en tant qu'administrateur système.

Procédure

1. Accédez au tableau de bord du gestionnaire d'appliances. Les options suivantes sont disponibles :
   - L'outil de configuration de l'appliance s'ouvre sur le tableau de bord du gestionnaire des appliances si vous avez terminé la configuration de l'appliance.
   - Cliquez sur l'icône **Paramètres généraux**. Sélectionnez **Central Management**. Le tableau de bord du gestionnaire d'appliances s'affiche.
2. Pour l'entrée de l'élément de ligne SMC, cliquez sur le menu Actions, puis sélectionnez **Modifier la configuration de l'appliance**.
3. Sélectionnez l'onglet Appliance.
4. Dans le volet SSH, sélectionnez **Activer SSH**.
5. Sélectionnez **Activer l'accès SSH racine**.
6. Cliquez sur **Appliquer les paramètres**.

Étape(s) suivante(s)

- Mettez à jour votre console SMC vers la dernière version et le dernier correctif, comme décrit à l'étape suivante.

1. Enfin, mettez à jour votre console SMC vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.

   Après avoir mis à jour votre console SMC, vous pouvez :

   - Revenez à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.
   - déployer et configurez vos nœuds de données, comme décrit à la section suivante.

Configuration et déploiement initiaux du matériel du data store

Après avoir déployé votre console SMC, déployez et configurez vos appliances de nœuds de données. Lorsque vous déployez vos nœuds de données et les connectez à votre réseau, consultez la section Exigences et considérations relatives au déploiement du data store.

Pour chaque nœud de données, procédez comme suit :

1. Commencez par déployer le nœud de données sur le réseau. Connectez-vous ensuite à votre appliance de nœuds de données avec CIMC, un clavier et un écran (ou un ordinateur portable) et connectez-vous à la console en tant qu'utilisateur `root`. Exécutez `systemconfig` et utilisez l'assistant de configuration initiale pour mettre à jour les paramètres du port de gestion, les paramètres du port de communication entre les nœuds de données, ainsi que les mots de passe utilisateur `root` et `sysadmin`. Reportez-vous au Guide d'installation matérielle des appliances Stealthwatch x210 ou à l'**Annexe A. Préparation de l'installation** et à l'**Annexe B. Installation du matériel Stealthwatch** pour plus d'informations.

   > La première fois que vous accédez à la configuration du système, celui-ci vous dirige vers l'assistant de configuration initiale, qui vous guide automatiquement au cours du processus de configuration initiale de l'appliance.

2. Ouvrez ensuite un navigateur web et accédez à l'adresse IP que vous avez attribuée au port de gestion. Utilisez l'outil de configuration de l'appliance pour effectuer une configuration supplémentaire, notamment l'attribution du mot de passe de l'utilisateur `admin` (et des mots de passe utilisateur `root` et `sysadmin`

si vous ne les avez pas attribués lors de la configuration du système), la configuration du domaine Stealthwatch, une autre configuration réseau, les paramètres DNS et NTP, ainsi que la gestion du nœud de données par Central Management. Reportez-vous au Guide de configuration du système Stealthwatch ou à l'**Annexe C. Configuration de vos appliances** pour plus d'informations.

3. Enfin, activez l'accès SSH et l'accès SSH racine sur votre nœud de données. Pour initialiser le data store conformément aux instructions de la section **Initialisation et configuration du data store**, vous devez exécuter un script basé sur l'accès SSH sur chaque appliance.

> ⚠ Une fois la console SSH activée, le risque de compromission du système augmente. Il est important d'activer SSH uniquement lorsque vous en avez besoin. Lorsque vous avez terminé d'utiliser l'accès SSH, désactivez-le.

Mettre à jour l'autorisation d'accès SSH d'un nœud de données

Avant de commencer

- Connectez-vous à l'application web SMC en tant qu'administrateur système.

Procédure

1. Accédez au tableau de bord du gestionnaire d'appliances. Les options suivantes sont disponibles :
   - L'outil de configuration de l'appliance s'ouvre sur le tableau de bord du gestionnaire des appliances si vous avez terminé la configuration de l'appliance.
   - Cliquez sur l'icône **Paramètres généraux**. Sélectionnez **Central Management**. Le tableau de bord du gestionnaire d'appliances s'affiche.

   Examinez la liste des appliances, puis vérifiez que votre nœud de données est répertorié et que l'option État de l'appliance est définie sur **Activé**.
2. Pour l'entrée de l'élément de ligne du nœud de données, cliquez sur le menu Actions, puis sélectionnez **Modifier la configuration de l'appliance**.
3. Sélectionnez l'onglet Appliance.
4. Dans le volet SSH, sélectionnez **Activer SSH**.

5. Sélectionnez **Activer l'accès SSH racine**.
6. Cliquez sur **Appliquer les paramètres**.

Étape(s) suivante(s)

- Mettez à jour votre nœud de données vers la dernière version et le dernier correctif, comme décrit à l'étape suivante.

1. Enfin, mettez à jour votre nœud de données vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.

   > Consultez les guides de mise à jour et les fichiers Lisez-moi des correctifs pertinents avant de continuer. Le processus de mise à jour du nœud de données nécessite des étapes supplémentaires par rapport aux autres appliances Stealthwatch.

   Après avoir mis à jour votre nœud de données, vous pouvez :

   - Revenez à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.
   - revenir à la configuration initiale du matériel **Configuration et déploiement initiaux du matériel du data store** et répéter ce processus d'installation et de configuration initiales du nœud de données, de configuration de l'outil de configuration de l'appliance et de configuration de Central Management pour les autres nœuds de données.

2. Après avoir déployé et configuré tous vos nœuds de données, vous pouvez :
   - configurer votre solution UDP Director, si vous en avez une, conformément aux instructions de la section suivante ;
   - configurer vos collecteurs de flux si vous ne disposez pas de solution UDP Director, conformément aux instructions de la section **Configurer un collecteur de flux en vue de l'utiliser avec un data store**.

Déployer une solution UDP Director

Si vous souhaitez déployer une solution UDP Director, suivez les instructions du Guide d'installation matérielle des appliances Stealthwatch x210 et du Guide de configuration du système Stealthwatch. Notez que le processus d'installation de UDP Director est le même, que vous déployiez ou non un data store. Il n'est pas nécessaire de configurer une solution UDP Director pour l'utiliser avec un data store.

Après avoir déployé votre solution UDP Director, vous pouvez :

- revenir à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement ;
- déployer et configurer vos collecteurs de flux, comme décrit à la section suivante.

Configurer un collecteur de flux en vue de l'utiliser avec un data store

Après avoir configuré vos nœuds de données (et votre solution UDP Director si vous en avez déployé une), déployez et configurez vos collecteurs de flux.

Pour chaque collecteur de flux, procédez comme suit :

1. Commencez par déployer le collecteur de flux sur votre réseau. Connectez-vous ensuite à votre collecteur de flux avec CIMC, un clavier et un écran (ou un ordinateur portable) et connectez-vous à la console en tant qu'utilisateur `root`. Exécutez `systemconfig` et utilisez l'assistant de configuration initiale pour mettre à jour les paramètres du port de gestion, l'utilisation avec un data store, et les mots de passe utilisateur `root` et `sysadmin`. Reportez-vous au Guide d'installation matérielle des appliances Stealthwatch x210 ou à l'**Annexe A. Préparation de l'installation** et à l'**Annexe B. Installation du matériel Stealthwatch** pour plus d'informations.

   > La première fois que vous accédez à la configuration du système, celui-ci vous dirige vers l'assistant de configuration initiale, qui vous guide automatiquement au cours du processus de configuration initiale de l'appliance.

   > Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez pas mettre à jour la configuration de l'appliance en vue de la modifier. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option uniquement si vous prévoyez de déployer un data store sur votre réseau.

2. Ouvrez ensuite un navigateur web et accédez à l'adresse IP que vous avez attribuée au port de gestion. Utilisez l'outil de configuration de l'appliance pour effectuer une configuration supplémentaire, notamment l'attribution du mot de passe de l'utilisateur `admin` (et des mots de passe utilisateur `root` et `sysadmin` si vous ne les avez pas attribués lors de la configuration du système), la sélection

du domaine Stealthwatch, une autre configuration réseau, les paramètres DNS et NTP, le numéro de port de collecte des flux (`2055` pour NetFlow ou `6343` pour sFlow), ainsi que la gestion du collecteur de flux par Central Management. Reportez-vous au Guide de configuration du système Stealthwatch ou à l'**Annexe C. Configuration de vos appliances** pour plus d'informations.

> Si vous configurez un collecteur de flux en vue de l'utiliser avec un data store, l'interface d'administration de l'appliance (administrateur de l'appliance) masque certaines fonctionnalités. Utilisez Central Management pour configurer le collecteur de flux et effectuer d'autres tâches connexes. Si vous souhaitez contrôler les statistiques de stockage, téléchargez l'application Statistiques de stockage du data store sur votre console SMC.

3. Enfin, activez l'accès SSH et l'accès SSH racine sur vos collecteurs de flux. Pour initialiser le data store conformément aux instructions de la section **Initialisation et configuration du data store**, vous devez exécuter un script basé sur l'accès SSH sur chaque appliance.

> ⚠ Une fois la console SSH activée, le risque de compromission du système augmente. Il est important d'activer SSH uniquement lorsque vous en avez besoin. Lorsque vous avez terminé d'utiliser l'accès SSH, désactivez-le.

Mettre à jour l'autorisation d'accès SSH d'un collecteur de flux

Avant de commencer

- Connectez-vous à l'application web SMC en tant qu'administrateur système si vous n'utilisez pas l'outil de configuration de l'appliance.

Procédure

1. Accédez au tableau de bord du gestionnaire d'appliances. Les options suivantes sont disponibles :
    - L'outil de configuration de l'appliance s'ouvre sur le tableau de bord du gestionnaire des appliances si vous avez terminé la configuration de l'appliance.

- Cliquez sur l'icône **Paramètres généraux**. Sélectionnez **Central Management**. Le tableau de bord du gestionnaire d'appliances s'affiche.

Examinez la liste des appliances, puis vérifiez que votre collecteur de flux est répertorié et que l'option État de l'appliance est définie sur **Activé**.

2. Pour l'entrée de l'élément de ligne du collecteur de flux, cliquez sur le menu Actions, puis sélectionnez **Modifier la configuration de l'appliance**.
3. Sélectionnez l'onglet Appliance.
4. Dans le volet SSH, sélectionnez **Activer SSH**.
5. Sélectionnez **Activer l'accès SSH racine**.
6. Cliquez sur **Appliquer les paramètres**.

Étape(s) suivante(s)

- Mettez à jour votre collecteurs de flux vers la dernière version et le dernier correctif, comme décrit à l'étape suivante.

1. Enfin, mettez à jour votre collecteurs de flux vers la dernière version et le dernier correctif. Reportez-vous aux guides de mise à jour pour plus d'informations sur la mise à jour vers la version actuelle et sur les fichiers Lisez-moi des correctifs pour plus d'informations sur les mises à jour des correctifs.

   Après avoir mis à jour votre collecteurs de flux, vous pouvez :

   - revenir à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement ;
   - pour chacun de vos collecteurs de flux, répétez le processus décrit à la section **Configurer un collecteur de flux en vue de l'utiliser avec un data store** pour l'installation et la configuration initiale du collecteur de flux, la configuration via l'outil de configuration de l'appliance et la configuration de Central Management pour vos autres collecteurs de flux.
2. Après avoir déployé et configuré tous vos collecteurs de flux, vous pouvez :
   - configurer votre capteur de flux, si vous en avez un, conformément aux instructions de la section suivante ;
   - configurer votre console SMC secondaire, si vous en avez une, conformément aux instructions de la section **Déployer la console de gestion Stealthwatch de basculement** ;
   - si vous ne disposez pas d'un capteur de flux ou d'une console SMC secondaire, initialisez et configurez le data store, comme décrit à la section **Initialisation et configuration du data store**.

Déployer un capteur de flux

Si vous souhaitez déployer un capteur de flux, suivez les instructions du Guide d'installation matérielle des appliances Stealthwatch x210 et du Guide de configuration du système Stealthwatch. Notez que le processus d'installation d'un capteur de flux est le même, que vous déployiez ou non un data store. Il n'est pas nécessaire de configurer un capteur de flux pour l'utiliser avec un data store.

Après avoir déployé et configuré votre capteur de flux, vous pouvez :

- revenir à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement ;
- configurer votre console SMC secondaire, si vous en avez une, conformément aux instructions de la section suivante ;
- si vous ne disposez pas de console SMC secondaire, initialiser le data store, conformément aux instructions de la section **Initialisation et configuration du data store**.

Déployer la console de gestion Stealthwatch de basculement

Si vous disposez d'une console SMC secondaire que vous souhaitez configurer en tant que console SMC de basculement, suivez les instructions du Guide d'installation matérielle des appliances Stealthwatch x210, du Guide de configuration du système Stealthwatch et du Guide de configuration du basculement Stealthwatch.

Après avoir terminé la configuration de la console SMC secondaire et avoir vérifié qu'elle est gérée par la console SMC principale via Central Management, vous pouvez :

- revenir à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement ;
- si vous disposez d'une console SMC secondaire et que vous promouvez votre console SMC secondaire en console SMC principale, une configuration supplémentaire est nécessaire avant de réutiliser le script `setup-sw-datastore-secure-connectivity` ; reportez-vous à la section Copier les informations de confiance du data store sur une console SMC de basculement pour plus d'informations ;
- initialiser et configurer le data store, conformément aux instructions de la section **Initialisation et configuration du data store**.

Initialisation et configuration du data store

Après avoir déployé et configuré votre console SMC, vos nœuds de données et vos collecteurs de flux, initialisez et configurez le data store. Assurez-vous que l'ensemble de vos consoles SMC, nœuds de données et collecteurs de flux sont mis à jour vers la dernière version et le dernier correctif avant de continuer.

> Si vous disposez d'une console SMC secondaire et que vous promouvez votre console SMC secondaire en console SMC principale, une configuration supplémentaire est nécessaire avant de réutiliser le script `setup-sw-datastore-secure-connectivity`. Reportez-vous à la section Copier les informations de confiance du data store sur une console SMC de basculement pour plus d'informations.

Procédez comme suit :

1. Assurez-vous tout d'abord que tous les nœuds de données et collecteurs de flux, ainsi que la console SMC secondaire (si vous en avez déployé une) sont gérés via Central Management, et que tous les accès SSH et SSH racine sont activés.
2. Ensuite, à partir de la console SMC, exécutez un script pour distribuer les mots de passe `dbadmin` et `readonlyuser` du data store et les certificats d'identité en vue de sécuriser les communications du data store avec vos appliances Stealthwatch.
3. À partir du nœud de données spécifié à l'étape précédente, exécutez un script pour initialiser le data store et établir des connexions sécurisées entre les nœuds de données et vos appliances Stealthwatch.
4. Enfin, dans Central Management, mappez un nom de data store interne (`sw-datastore`) sur les adresses IP du nœud de données de votre console SMC et de vos collecteurs de flux afin d'améliorer la répartition de la charge et les performances des requêtes sur le nœud de données.

Vérifier que les nœuds de données et les collecteurs de flux sont gérés via Central Management

Avant de commencer

- Dressez une liste des adresses IP et noms d'hôte du nœud de données et du collecteur de flux que vous prévoyez de gérer dans Central Management.
- Connectez-vous à l'application web SMC en tant qu'administrateur système, puis accédez à Central Management.

Procédure

1. Dans l'inventaire des appliances, comparez votre liste de nœuds de données et de collecteurs de flux (ainsi que la console SMC secondaire si vous en avez déployé une) à la liste de l'inventaire, puis assurez-vous que l'option **État de l'appliance** est définie sur **Activé** pour chacun d'eux. Ne poursuivez **pas** l'initialisation du data store tant que toutes les appliances attendues ne sont pas gérées et activées.

   Si l'une des appliances est **en panne**, vérifiez la configuration de votre appliance et la connexion entre la console SMC et cette appliance.

   Si une appliance n'apparaît pas dans l'inventaire, ajoutez-la.
2. Pour chaque appliance, cliquez sur le menu Actions, puis sélectionnez **Modifier la configuration de l'appliance**.
3. Sélectionnez l'onglet Appliance. Assurez-vous que les options **Activer SSH** et **Activer l'accès SSH racine** sont sélectionnées. Ne poursuivez **pas** l'initialisation du data store tant que vous n'avez pas activé l'accès SSH et l'accès racine SSH sur toutes vos appliances.

   Si ces options ne sont pas sélectionnées, sélectionnez-les, puis cliquez sur **Appliquer les paramètres**.

Distribuer les mots de passe du data store à vos consoles SMC, vos nœuds de données et vos collecteurs de flux

Dans l'interface de ligne de commande de la console SMC, vous pouvez exécuter un script qui prépare le déploiement de votre Stealthwatch à l'initialisation du data store en distribuant les informations nécessaires pour établir des connexions data store sécurisées. La première option du script vous permet de créer des mots de passe pour les comptes utilisateur `dbadmin` et `readonlyuser`, et de les distribuer de manière sécurisée aux consoles SMC, aux nœuds de données et aux collecteurs de flux. Chaque mot de passe doit respecter les conditions suivantes :

- contenir au moins un nombre
- contenir au moins un caractère en minuscules
- contenir au moins un caractère en majuscules
- contenir au moins un caractère spécial parmi la liste suivante : `<>.,? / '"|:;` ~! @ # $% ^ & * () -_ + = {} []`

- contenir au moins 8 caractères (aucune restriction de longueur maximum)
- contenir uniquement des caractères codés ASCII

Lorsque vous exécutez un script pour initialiser le data store, le script utilise ces informations pour configurer les informations d'identification du compte utilisateur `dbadmin` et `readonlyuser`, et pour établir des connexions sécurisées entre chaque appliance et le data store.

> Si vous définissez ces mots de passe et que vous les perdez, contactez le service d'assistance Cisco pour les récupérer.

Notez que vous utilisez cette option lorsque vous déployez le data store. Si vous avez déjà initialisé le data store et souhaitez mettre à jour ces mots de passe, reportez-vous à la section Mettre à jour les mots de passe dbadmin et readonlyuser du data store pour plus d'informations.

Avant de commencer

- Compilez une liste de mots de passe racines pour votre console SMC, vos nœuds de données, vos collecteurs de flux et votre console SMC secondaire si vous en avez déployé une.
- Connectez-vous à la console SMC en tant qu'utilisateur `root`.

Procédure

1. Dans la ligne de commande, saisissez `cd /lancope/admin/cds` et appuyez sur la touche Entrée pour modifier les répertoires.
2. Saisissez la commande `./setup-sw-datastore-secure-connectivity` et appuyez sur la touche Entrée pour exécuter le script bash de connectivité sécurisée au data store.
3. Dans le menu principal du script, sélectionnez **1. Distribuer le mot de passe du data store logiciel aux appliances**.

   Le script affiche une liste des consoles SMC, des nœuds de données gérés par la console SMC, des collecteurs de flux pris en charge par le data store et gérés par la console SMC, ainsi que des consoles SMC secondaires prises en charge par le data store et gérées par la console SMC principale.
4. Confirmez la liste des appliances et sélectionnez **OK**. La première fois que vous exécutez ce script lors de la configuration de votre déploiement Stealthwatch en vue de l'utiliser avec le data store, toutes les appliances sont sélectionnées.
5. Sur la ligne de commande, lorsque vous êtes invité à saisir le mot de passe `root`

pour chaque appliance, saisissez-le et appuyez sur la touche Entrée.

> Étant donné que vous saisissez plusieurs mots de passe, veillez à saisir le mot de passe correspondant à cette appliance.

Après avoir saisi tous les mots de passe `root` des appliances, le script vous invite à saisir les mots de passe `dbadmin` et `readonlyuser`.

6. Saisissez le mot de passe **dbadmin**.
7. Saisissez le même mot de passe `dbadmin` dans le champ **dbadmin (confirmation)**.
8. Saisissez le mot de passe **readonlyuser**.
9. Saisissez le même mot de passe `readonlyuser` dans le champ **readonlyuser (confirmation)**.

> Veillez à ne pas saisir le même mot de passe pour `dbadmin` que pour `readonlyuser`. L'attribution du même mot de passe entraîne l'échec du script, et aucun mot de passe ne sera affecté aux comptes utilisateur.

10. Cliquez sur **OK**.

    Le script distribue ces mots de passe de manière sécurisée aux appliances sélectionnées. Lorsque vous avez terminé, la liste des appliances mises à jour s'affiche.
11. Sélectionnez **OK** pour revenir au menu principal du script.

Étape(s) suivante(s)

- Distribuez les certificats d'identité du data store pour les communications sécurisées, comme décrit dans la procédure suivante.

Distribuer les certificats d'identité du data store pour établir des communications sécurisées avec vos appliances

Dans le script permettant d'établir des connexions sécurisées au data store, la deuxième option vous permet de générer un certificat d'identité et de le distribuer à la console SMC, aux nœuds de données et aux collecteurs de flux. Lorsque vous exécutez un script pour initialiser le data store, le script utilise ce certificat d'identité pour établir des connexions sécurisées entre vos appliances et le data store.

Le certificat d'identité est autosigné, valide pendant 5 ans, et a pour nom commun `sw-datastore.stealthwatch.cisco.com`.

Avant de commencer

- Dans la ligne de commande de la console SMC, exécutez le script `setup-sw-datastore-secure-connectivity`.

Procédure

1. Dans le menu principal du script, sélectionnez **2. Distribuer les certificats pour la connexion sécurisée à la base de données**.
2. Le script affiche une liste des consoles SMC, des nœuds de données gérés par la console SMC, des collecteurs de flux gérés par la console SMC et des consoles SMC secondaires gérées par la console SMC principale.

   Si vous avez confirmé la liste des appliances après avoir sélectionné **1. Distribuer le mot de passe du data store logiciel aux appliances**, il est possible que le script n'affiche pas cette liste d'appliances. Passez à l'étape 4.
3. Confirmez la liste des appliances et sélectionnez **OK**. La première fois que vous exécutez ce script lors de la configuration de votre déploiement Stealthwatch en vue de l'utiliser avec le data store, toutes les appliances sont sélectionnées.

   Le script génère un certificat d'identité, à utiliser pour les communications sécurisées, et la clé privée associée.
4. Sur la ligne de commande, lorsque vous êtes invité à saisir le mot de passe `root` pour chaque appliance, saisissez-le et appuyez sur la touche Entrée.

   > Étant donné que vous saisissez plusieurs mots de passe, veillez à saisir le mot de passe correspondant à cette appliance.
5. Une fois le script correctement exécuté, un message de confirmation et l'adresse IP d'un nœud de données s'affichent. Dans la procédure suivante, vous vous connectez à la console de ce nœud de données à l'aide de SSH pour exécuter le script d'initialisation du data store.

   > Enregistrez cette adresse IP avant de quitter ce message. Vous ne pourrez pas la récupérer après avoir fermé le message.

Étape(s) suivante(s)

- Initialisez le data store, comme décrit dans la procédure suivante.

Exécuter un script pour initialiser le data store et appliquer les connexions sécurisées

Après avoir distribué les mots de passe utilisateur `dbadmin` et `readonlyuser` et le certificat d'identité à vos appliances, connectez-vous au nœud de données en suivant les instructions de la procédure précédente, modifiez le fichier de configuration `install_SDBN.cfg` et exécutez le script d'initialisation `install_SDBN.initial.py`. Ce script initialise le data store en connectant vos nœuds de données, définit les informations d'identification `dbadmin` et `readonlyuser`, et met en place des connexions sécurisées entre vos appliances Stealthwatch et le data store.

Après avoir initialisé le data store, copiez la clé d'API du data store principal à partir de ce nœud de données. Vous utilisez ces informations dans l'étape **Configurer la console de gestion Vertica** pour installer la console de gestion Vertica (VMC) sur votre console SMC.

Avant de commencer

- Compilez une liste de toutes vos adresses IP publiques `eth0` de nœud de données et de vos adresses IP privées de canal de port `eth2` ou `eth2/eth3`.
- En tant qu'utilisateur `root`, connectez-vous à la console du nœud de données dont l'adresse IP a été affichée après la distribution des certificats d'identité à l'aide du script de connexion sécurisée du data store, comme décrit à la section **Distribuer les certificats d'identité du data store pour établir des communications sécurisées avec vos appliances**.

Procédure

1. Dans la ligne de commande, saisissez `cd /lancope/database` et appuyez sur la touche Entrée pour changer de répertoire.
2. Saisissez `cp install_SDBN_example.cfg install_SDBN.cfg` et appuyez sur la touche Entrée pour copier le fichier de configuration d'exemple.
3. Saisissez `vi install_SDBN.cfg` et appuyez sur la touche Entrée pour modifier le fichier de configuration dans un éditeur de texte.
4. Créez des sections `[nodeN]` numérotées consécutivement en fonction du nombre de nœuds de données que vous avez déployés. Par exemple, si vous avez déployé 6 nœuds de données, votre fichier contient les éléments suivants :

```
[node1]
private = 169.254.42.30
```

```
public = 10.0.16.30
[node2]
private = 169.254.42.31
public = 10.0.16.31
[node3]
private = 169.254.42.32
public = 10.0.16.32
[node4]
private = 169.254.42.33
public = 10.0.16.33
[node5]
private = 169.254.42.34
public = 10.0.16.34
[node6]
private = 169.254.42.35
public = 10.0.16.35
[common]
subnet = 10.0.16.0
```

5. En commençant par la section `[node1]`, saisissez les adresses IP privées (canal de port `eth2` ou `eth2/eth3`) et publiques (`eth0`) pour chaque nœud de données. Notez les éléments suivants :
    - Ce script attribue les nœuds de données au data store dans l'ordre dans lequel ils sont répertoriés. Si vous avez déployé vos nœuds de données avec plusieurs modules d'alimentation redondants, modifiez l'affectation des nœuds en fonction du module d'alimentation pour optimiser la disponibilité globale et la redondance des données du data store.
    - Les adresses IP privées ne doivent pas être routables, sur un LAN ou un VLAN privé. Vous devez attribuer les adresses IP dans le bloc CIDR `169.254.42.0/24`.
    - Veillez à ne pas faire se chevaucher les adresses IP entre ou parmi les nœuds de données.
    - Ajoutez uniquement les nœuds de données devant appartenir au data store.
6. Dans la section `[common]`, mettez à jour le `sous-réseau` de façon à ce qu'il dispose de l'adresse IP la plus faible dans le bloc CIDR d'adresses IP publiques.
7. Appuyez sur la touche Échap, saisissez `:wq`, puis appuyez sur la touche Entrée pour enregistrer vos modifications et quitter l'éditeur de texte.
8. Dans de la ligne de commande, saisissez `python install_SDBN_`

`initial.py -i install_SDBN.cfg` et appuyez sur la touche Entrée pour exécuter le script Python d'initialisation du data store. Ce script utilise le fichier de configuration `install_SDBN.cfg` pour initialiser les nœuds de données dans l'ordre que vous avez spécifié.

Une fois le script terminé, vérifiez les messages d'état de la CLI pour vous assurer que le script a réussi.

> Pour chaque nœud de données, la console affiche le message `Prerequisites not fully met during local (OS) configuration` (Conditions préalables non satisfaites lors de la configuration locale (SE)) et affiche une série de messages de journalisation : `HINT (S0305)`, `HINT (S0041)`, `HINT (S0040)`, `WARN (N0010)`, `FAIL (s0180)` et `FAIL (s0311)`. Ces messages de journalisation s'affichent par anticipation ; ils n'indiquent pas l'échec de l'initialisation de data store. Reportez-vous à la section **Résoudre les problèmes liés au déploiement du data store** pour plus d'informations sur ces messages.

> Pour chaque nœud de données, la console affiche le message `INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified` (INFO 6403 : le paramètre de configuration SSLCA de la console n'est pas défini. Les certificats clients ne seront ni demandés ni vérifiés). Ces messages de journalisation s'affichent par anticipation ; ils n'indiquent pas l'échec de l'établissement des connexions sécurisées avec le data store. Reportez-vous à la section **Résoudre les problèmes liés au déploiement du data store** pour plus d'informations sur ces messages.

9. Saisissez `cd /opt/vertica/config` pour modifier les répertoires.
10. Saisissez `cat apikeys.dat` pour afficher la chaîne de la clé d'API dans la console.
11. Copiez la chaîne de la clé d'API et collez-la dans un éditeur de texte brut. Vous utilisez cette clé d'API à l'étape **Configurer la console de gestion Vertica** pour configurer la console VMC sur votre console SMC.
12. Notez l'adresse IP de ce nœud de données. Vous utilisez cette adresse IP à l'étape **Configurer la console de gestion Vertica** pour configurer la console VMC sur votre console SMC.

Étape(s) suivante(s)

- Utilisez la résolution locale dans Central Management pour mapper les adresses IP du nœud de données sur le nom du data store, comme décrit dans la procédure suivante.

Mapper le nom du data store sur vos nœuds de données à l'aide de la résolution locale

Après avoir initialisé le data store, utilisez Central Management pour mapper le nom du data store (`sw-datastore`) sur les adresses IP de tous vos nœuds de données pour votre console SMC et vos collecteurs de flux. Étant donné que le data store contient plusieurs nœuds de données, ce mappage de résolution locale permet de répartir le stockage de flux et les demandes de requête de manière plus homogène dans vos nœuds de données, améliorant ainsi les performances et la réponse.

> Pour des performances optimales, mappez les adresses IP `eth0` du nœud de données dans le **même ordre** pour chaque appliance.

Avant de commencer

- Compilez une liste des adresses IP publiques de tous vos nœuds de données.
- Compilez une liste de vos collecteurs de flux gérés dans Central Management.
- Connectez-vous à l'application web SMC en tant qu'administrateur et accédez à Central Management.

Procédure

1. En commençant par la console SMC, cliquez sur le menu Actions, puis sélectionnez **Modifier la configuration de l'appliance**.
2. Sélectionnez l'onglet Services réseau.
3. Dans la section Résolution locale, cliquez sur **Ajouter**.
4. Saisissez `sw-datastore` dans le champ **Nom d'hôte**.
5. Saisissez la première adresse IP publique du nœud de données de votre liste.
6. Cliquez sur **Ajouter**.
7. Répétez les trois étapes précédentes pour tous les autres nœuds de données, en utilisant la liste des adresses IP publiques du nœud de données.
8. Cliquez sur **Appliquer les paramètres**, puis confirmez vos modifications.
9. Répétez cette procédure pour tous les collecteurs de flux de votre liste, et sur

votre console SMC secondaire si vous en avez déployé une.

> Pour des performances optimales, mappez les adresses IP `eth0` du nœud de données dans le **même ordre** pour chaque appliance.

Étape(s) suivante(s)

- Revenez à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.
- Configurez la console de gestion Vertica (VMC) sur votre console SMC. Reportez-vous à la section suivante pour obtenir plus d'informations.

Configurer la console de gestion Vertica

Après avoir initialisé et configuré le data store, configurez la console de gestion Vertica (VMC) sur votre console SMC pour vous connecter au data store. Vous pouvez utiliser la console VMC pour contrôler l'intégrité du data store et recevoir des notifications en fonction de seuils configurables. Procédez comme suit :

1. À partir d'un navigateur web sur votre poste de travail local, effectuez la configuration initiale de la console VMC, notamment la configuration de la VMC pour interdire l'utilisation de TLS 1.0 et 1.1 pour l'accès au navigateur web et les notifications par e-mail.
2. Dans la console VMC, configurez une connexion sécurisée avec votre data store.
3. Dans la console VMC, configurez les notifications automatiques (telles que les e-mails) et les seuils de notification.

> Si vous utilisez l'option **3. Mettre à jour le mot de passe du data store logiciel sur les appliances** dans `setup-sw-datastore-secure-connectivity` pour mettre à jour le mot de passe `dbadmin` après l'avoir défini, vous devez vous connecter à la console VMC en tant qu'utilisateur `dbadmin` pour mettre à jour manuellement le mot de passe. Pour plus d'informations, reportez-vous à la section Mettre à jour les mots de passe dbadmin et readonlyuser du data store après l'initialisation.

Effectuer la configuration initiale de la console VMC

Vous effectuez la configuration initiale de la console VMC la première fois que vous accédez à cette dernière.

Par défaut, la console VMC autorise les connexions TLS 1.0 et TLS 1.1 à partir d'un navigateur web. Étant donné que ces anciennes versions de TLS sont moins sécurisées que TLS 1.2+, configurez la console VMC de sorte à interdire toute connexion sur TLS 1.0 et TLS 1.1.

Avant de commencer

- Tenez prête l'adresse IPv4 de votre console SMC.
- Assurez-vous que le port de communication `9450/TCP` est ouvert entre votre poste de travail et la console SMC.

Procédure

1. Sur votre poste de travail, ouvrez un navigateur web et saisissez `https://[smc-ipv4-address]:9450/webui/login` dans la barre d'adresse. Remplacez `[smc-ipv4-address]` par l'adresse IPv4 de votre console SMC. Accédez à cette URL.
2. Acceptez la licence Vertica, puis cliquez sur **Suivant**.
3. Saisissez le **mot de passe** `dbadmin` et confirmez-le dans **Confirmer le mot de passe**.

   > Ce compte utilisateur `dbadmin` est un compte utilisateur VMC qui est ensuite mappé sur votre compte utilisateur `dbadmin` du data store. Vous pouvez attribuer à ce compte un mot de passe différent de celui que vous avez attribué à votre compte utilisateur `dbadmin` du data store.

4. Saisissez `dbadmin` comme **nom de groupe Unix**.
5. Laissez tels quels les chemins de fichiers par défaut (`/home/dbadmin`) et le port par défaut (`5450`), et cliquez sur **Suivant**.

   Les options de stockage s'affichent.
6. Cliquez sur **Suivant**.

   Les options d'autorisation de la console de gestion s'affichent.
7. Cliquez sur **Suivant**. Attendez que le service Vertica redémarre.

   Cette opération peut prendre 20 minutes ou plus. Si la fenêtre du navigateur ne s'actualise pas automatiquement, actualisez manuellement la page.
8. Saisissez vos informations d'identification `dbadmin` et cliquez sur **Se connecter** pour vous connecter à la console VMC.
9. Sur la page principale de la console VMC, cliquez sur **Paramètres MC**.

10. Cliquez sur l'onglet Configuration.
11. Sélectionnez **Désactiver les connexions TLS 1.0 et 1.1 dans le navigateur**, puis enregistrez vos modifications.

Configurer une connexion sécurisée VMC au data store

Avant de commencer à configurer cette connexion sécurisée, copiez le fichier `/lancope/var/admin/cds/server.crt` de votre console SMC sur votre poste de travail local. Vous utilisez ce fichier pour établir une connexion sécurisée entre la console VMC et le data store.

Avant de commencer

- Copiez le fichier `/lancope/var/admin/cds/server.crt` de votre console SMC sur votre poste de travail local.
- Effectuez une copie de la clé d'API de votre data store principal en suivant les instructions de la section **Exécuter un script pour initialiser le data store et appliquer les connexions sécurisées**.
- Obtenez l'adresse IP du nœud de données à partir duquel vous avez copié la clé d'API, en suivant les instructions de la section **Exécuter un script pour initialiser le data store et appliquer les connexions sécurisées**.

Procédure

1. Sur la page principale de la console VMC, cliquez sur **Importer un cluster de bases de données Vertica**.
2. Saisissez l'**adresse IP** de l'adresse IP `eth0` du nœud de données à partir duquel vous avez copié la clé d'API, puis cliquez sur **Suivant**.
3. Vous pouvez également modifier le **nom du cluster**.
4. Saisissez la **clé d'API** du data store principal, puis cliquez sur **Continuer**.

   La console VMC localise le data store.
5. Saisissez le **nom d'utilisateur** `dbadmin` et le **mot de passe** `dbadmin`.
6. Sélectionnez **Utiliser TLS**.
7. Cliquez sur **Configurer TLS et importer la base de données**.

   La fenêtre Configurer les certificats de connexion TLS s'affiche.
8. Cliquez sur **Configurer la connexion TLS**.
9. Sélectionnez **Charger un nouveau certificat CA**, puis cliquez sur **Suivant**.

10. Cliquez sur **Parcourir**, puis sélectionnez le fichier `server.crt` que vous avez enregistré sur votre poste de travail local à partir de la console SMC.
11. Saisissez `sw-datastore-cert` comme **alias du certificat CA**, puis cliquez sur **Suivant**.
12. Cliquez sur **Vérifier**.
13. Cliquez sur **Configurer TLS pour la base de données**.

    La console VMC configure les connexions sécurisées au data store.
14. Cliquez sur **Fermer**.

> Le message « Erreur lors de l'importation de la base de données sur MC. non défini » peut s'afficher. Ce message s'affiche par anticipation ; il n'indique pas l'échec de l'établissement d'une connexion sécurisée avec le data store.

Configurer les notifications d'alerte VMC par e-mail

Vous pouvez configurer la console VMC de sorte à envoyer des notifications d'alerte par e-mail.

Avant de commencer

- Connectez-vous à la console VMC en tant qu'utilisateur `dbadmin`.

Procédure

1. Sur la page Paramètres MC, cliquez sur l'onglet Passerelle de messagerie.
2. Spécifiez un **Serveur SMTP (nom d'hôte)**. Vous pouvez saisir un nom de 255 caractères maximum ou une adresse IP.
3. Spécifiez un **Port de serveur SMTP**.
4. Sélectionnez **Utiliser TLS** pour **Type de session (SSL ou TLS)**.
5. Spécifiez un **Nom d'utilisateur SMTP**.
6. Spécifiez un **Mot de passe SMTP**.
7. Spécifiez l'**Alias de l'adresse e-mail d'envoi** à partir duquel la console VMC enverra les alertes par e-mail.
8. Cliquez sur **Tester** pour tester vos paramètres.

   Mettez à jour les paramètres si vous ne recevez pas d'e-mail de test.
9. Cliquez sur **Apply (Appliquer).**

Configurer les seuils des alertes VMC

Vous pouvez configurer divers seuils minimum et maximum à partir desquels la console VMC génère une alerte si le data store dépasse une valeur de seuil.

Avant de commencer

- Connectez-vous à la console VMC en tant qu'utilisateur `dbadmin`.

Procédure

1. Sélectionnez **Paramètres > Seuils**.
2. Cochez la case d'un élément de seuil de notification d'alerte pour l'activer, ou décochez la case pour le désactiver. Cisco recommande d'activer la notification `Changement d'état du nœud` pour recevoir des notifications en cas de panne du nœud de données.

   > Lorsque vous configurez des seuils minimaux, des notifications de faux-positifs excessives peuvent être générées. Par exemple, si vous définissez le seuil minimal de CPU du nœud, le nœud risque de se déclencher fréquemment en raison d'une utilisation fluctuante du CPU.

3. Sélectionnez *Priorité 1* pour chaque seuil de notification pour lequel vous souhaitez recevoir des e-mails.
4. Si vous sélectionnez *Priorité 1*, cliquez sur l'icône de navigation en regard de **Destination de l'e-mail**.
5. Saisissez une adresse e-mail dans le champ **Saisie d'un nouveau champ**, puis cliquez sur l'icône **+**.
6. Cliquez sur **OK**.
7. Sélectionnez un **intervalle d'envoi des e-mails** pour déterminer la fréquence d'envoi des e-mails si le data store dépasse un certain seuil.
8. Cliquez sur **Apply (Appliquer).**

Étape(s) suivante(s)

- Revenez à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.
- Configurez la conservation des données de votre data store, comme décrit dans la section suivante.

Configuration de la conservation du data store

Par défaut, le data store conserve les données pendant sept (7) jours maximum avant de les supprimer automatiquement. Utilisez l'API REST du Stealthwatch pour modifier cette période de conservation :

- sur un nombre de jours différent (jusqu'à 3 000), ou
- stocker les données le plus longtemps possible, jusqu'à ce que le data store atteigne la capacité maximale.

Notez les points suivants concernant la conservation du data store :

- Après avoir mis à jour les paramètres de conservation des données, il n'est plus nécessaire de redémarrer les appliances Stealthwatch ou le data store. Les paramètres prennent effet au bout de quelques minutes.
- Lorsque vous définissez une période de conservation plus longue, vous devez attendre l'expiration du délai précédent avant que les données en cours de stockage correspondent exactement aux paramètres de conservation. Dans l'intervalle, les données s'affichent à l'aide de la résolution la plus faible disponible. Par exemple, si vous modifiez la conservation de 3 jours sur 10 jours, vous devez maintenant attendre 7 jours avant que les données stockées correspondent exactement aux paramètres de conservation.
- Il est possible que vos données soient supprimées plus tôt en raison de la réduction critique des données selon l'utilisation du disque. Si vous choisissez de stocker les données le plus longtemps possible, lorsque la capacité maximale du data store est atteinte, le système commence à supprimer les données les plus anciennes.
- Si vous ne souhaitez pas stocker de données, vous pouvez accéder à l'interface utilisateur d'administration de chacun de vos collecteurs de flux et sélectionner **Assistance > Paramètres avancés**. Pour chaque collecteur de flux, modifiez l'entrée « interface_retention_days » dans la colonne Libellé de l'option sur 0 (zéro) et redémarrez votre collecteur de flux (ou le moteur du collecteur de flux, si possible).

Pour mettre à jour ces paramètres, utilisez l'API REST pour effectuer les opérations suivantes :

Authentification auprès de l'API REST de la console SMC

Demande d'informations sur les ressources

Ressource	Description
URI	`https://[smc-eth0-ip]/token/v2/authenticate`
Description	Authentifiez-vous auprès de l'API REST de la console SMC.
Paramètres de l'URI	• *[smc-eth0-ip]* – SMC Adresse IP de gestion eth0 de la console SMC
Méthode HTTP	POST
Type MIME du corps de la demande	application/x-www-form-urlencoded
Corps de la demande	`username=[username]&password=[password]`
Paramètres du corps de la demande	• *[username]* - (OBLIGATOIRE) Utilisateur Admin de la console SMC • *[password]* - (OBLIGATOIRE) Mot de passe du compte de l'utilisateur Admin de la console SMC

Code de réponse de réussite et définition

Réponse	Description
Code de réponse	200 – Réussite
Corps de la réponse	Le corps de la réponse contient des informations sur les cookies, que vous devez transmettre lors des appels suivants à l'API REST pour cette session. Votre session est valide pendant 20 minutes.

Récupérer les paramètres actuels de conservation des données du data store

Demande d'informations sur les ressources

Ressource	Description
URI	`https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings`

Ressource	Description
Description	Récupérez les paramètres actuels de conservation des données du data store.
Paramètres de l'URI	• *[smc-eth0-ip]* – SMC Adresse IP de gestion eth0 de la console SMC
Méthode HTTP	GET
Type MIME du corps de la demande	s.o.
Corps de la demande	s.o.
Paramètres du corps de la demande	s.o.

Informations et code de la réponse de réussite

Ressource	Description
Code de réponse	200 – Réussite
Corps de la réponse	Le corps de la réponse contient les paramètres actuels de conservation des données du data store. Si vous ne les avez pas modifiés précédemment, la valeur par défaut est de 7 jours.

Mettre à jour les paramètres de conservation des données du data store

Demande d'informations sur les ressources

Ressource	Description
URI	`https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings`
Description	Mettez à jour les paramètres actuels de conservation des données du data store.

Ressource	Description
Paramètres de l'URI	• *[smc-eth0-ip]* – SMC Adresse IP de gestion eth0 de la console SMC
Méthode HTTP	PUT
Type MIME du corps de la demande	application/json
Corps de la demande	`{ "interfaceRetentionType":"[type]", "interfaceRetentionAmount":"[#]" }`

Paramètres du corps de la demande	• *[type]* : (OBLIGATOIRE) type de conservation des données, défini sur l'une des valeurs de chaîne suivantes :
	  • `AMOUNT` : les données sont stockées pendant le nombre de jours maximum défini dans interfaceRetentionAmount avant leur suppression.
	  • `FOREVER` : les données sont stockées le plus longtemps possible, jusqu'à ce que la capacité maximale du data store soit atteinte, avant leur suppression.
	• *[#]* : (OBLIGATOIRE) nombre maximal de jours pendant lesquels le data store conserve les données, avant leur suppression, défini sur un nombre entier compris `entre 1 et 3 000`.
	  Si vous définissez `interfaceRetentionType` sur `FOREVER`, vous devez toujours transmettre une valeur `interfaceRetentionAmount`, que le système ignore. Il stocke cette valeur en interne en tant que valeur par défaut `7`, quelle que soit la valeur `interfaceRetentionAmount` que vous transmettez dans ce cas.

Informations et code de la réponse de réussite

Ressource	Description
Code de réponse	204 – Réussite (aucun contenu)
Corps de la réponse	Le corps de la réponse ne possède aucun contenu.

Reportez-vous à la documentation de l'API REST d'entreprise Stealthwatch pour en savoir plus sur l'API REST.

La procédure suivante fournit la syntaxe curl pour la mise à jour de la période de conservation des données du data store :

Mettre à jour la période de conservation du data store

Avant de commencer

- Connectez-vous à la console d'une appliance Linux sur laquelle la syntaxe curl est installée.

Procédure

1. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   curl -c cookies.txt -d "username=[username]&password=
   [password]" https://[smc-eth0-ip]/token/v2/authenticate
   ```

2. Remplacez *[username]* par le nom d'utilisateur admin de la console SMC.
3. Remplacez *[password]* par le mot de passe admin de la console SMC.
4. Remplacez *[smc-eth0-ip]* par l'adresse IP `eth0` de la console SMC.
5. Copiez la commande mise à jour, collez-la dans la ligne de commande, puis appuyez sur la touche Entrée pour vous authentifier auprès de la console SMC en vue d'utiliser l'API REST.

   Votre session est valide pendant 20 minutes.

6. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   curl -X GET -b cookies.txt https://[smc-eth0-ip]/smc-
   configuration/rest/v1/cds/retentionsettings
   ```

7. Remplacez *[smc-eth0-ip]* par l'adresse IP `eth0` de la console SMC.
8. Copiez la commande mise à jour, collez-la dans la ligne de commande, puis

appuyez sur la touche Entrée pour récupérer les paramètres actuels de conservation du data store.

S'il s'agit de votre première vérification, le data store est par défaut configuré avec une période de conservation de 7 jours.

9. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

```
curl -X PUT -b cookies.txt -H "Content-
Type:application/json" -d '{"interfaceRetentionType":"
[type]","interfaceRetentionAmount":"[#]"}' https://[smc-
eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings
```

10. Remplacez *[type]* par l'une des valeurs suivantes :
    - `AMOUNT` si vous souhaitez définir un nombre de jours de conservation.
    - `FOREVER` si vous souhaitez stocker des données aussi longtemps que possible.
11. Remplacez *[#]* par un nombre entier compris `entre 1 et 3 000` pour la durée de conservation.

    Vous devez le définir même si vous sélectionnez *[type]*=FOREVER. Dans ce cas, le système ignore cette valeur et la définit sur `7` en interne.
12. Remplacez *[smc-eth0-ip]* par l'adresse IP `eth0` de la console SMC.
13. Copiez la commande mise à jour, collez-la dans la ligne de commande, puis appuyez sur la touche Entrée pour mettre à jour les paramètres de conservation.

> Après avoir mis à jour les paramètres de conservation, il n'est plus nécessaire de redémarrer les appliances Stealthwatch ou le data store. Les paramètres prennent effet au bout de quelques minutes. Lorsque vous définissez une période de conservation plus longue, vous devez attendre l'expiration du délai précédent avant que les données en cours de stockage correspondent exactement aux paramètres de conservation.

Étape(s) suivante(s)

- Revenez à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.
- Passez en revue les étapes décrites dans la section suivante.

Étapes postérieures à l'installation du data store

Après avoir déployé et configuré Stealthwatch pour une utilisation avec un data store :

- Installez l'application Stealthwatch Report Builder sur votre console SMC pour exécuter des rapports sur votre déploiement Stealthwatch et afficher les statistiques de stockage du data store. Reportez-vous aux notes de version pour plus d'informations.
- Consultez l'aide en ligne de l'application web Stealthwatch pour en savoir plus sur l'utilisation de Stealthwatch.
- Revenez à la section Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.

Maintenance du data store

Ce chapitre décrit le data store et les tâches de maintenance liées au data store, notamment :

- Redémarrer un nœud de données et le data store
- Sauvegarder et restaurer un data store
- Ajouter, supprimer et remplacer des nœuds de données
- Copier les informations d'approbation sur une console SMC de basculement avant de promouvoir cette dernière en tant que console SMC principale

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Redémarrer un nœud de données

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Si vous devez redémarrer un nœud de données, exécutez la commande permettant de l'arrêter, puis la commande permettant de le redémarrer.

Arrêter, puis redémarrer le nœud de données

Avant de commencer

- Connectez-vous à une console de nœuds de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   `/opt/vertica/bin/admintools -t stop_node -s [data-node-hostname]`

3. Remplacez `[data-node-hostname]` par le nom d'hôte du nœud de données que vous souhaitez arrêter avant de le redémarrer.
4. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour arrêter le nœud de données.

5. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   `/opt/vertica/bin/admintools -t restart_node -s [data-node-hostname]`

6. Remplacez `[data-node-hostname]` par le nom d'hôte du nœud de données que vous souhaitez redémarrer.
7. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour redémarrer le nœud de données.

Redémarrer le data store

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Pour redémarrer un data store, exécutez la commande permettant de l'arrêter, puis la commande permettant de le redémarrer.

Arrêter, puis redémarrer le data store

Avant de commencer

- Assurez-vous que vos collecteurs de flux ne sont pas connectés au data store et ne transmettent pas de données.
- Assurez-vous que votre console SMC n'est pas connectée au data store, et qu'elle n'interroge pas ou ne met pas à jour le data store.
- Connectez-vous à une console de nœuds de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Les options suivantes sont disponibles :
   - Dans l'invite de commande, saisissez `/opt/vertica/bin/admintools -t stop_db -d sw`, puis appuyez sur la touche Entrée pour arrêter le data store.
   - Dans l'invite de commande, saisissez `/opt/vertica/bin/admintools -t stop_db -d sw -F`, puis appuyez sur la touche Entrée pour arrêter le data store et remplacer les connexions au collecteur de flux ou à la console SMC.

3. Dans l'invite de commande, saisissez `/opt/vertica/bin/admintools -t start_db -d sw`, puis appuyez sur la touche Entrée pour redémarrer le data store.

Créer une sauvegarde du data store

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Pour sauvegarder votre data store, vous devez suivre la procédure ci-après :

- Estimer la taille de la sauvegarde
- Préparer un hôte de sauvegarde avec une capacité de stockage deux fois supérieure à la taille de la sauvegarde

  > Utilisez un hôte Linux distinct de celui de vos appliances Stealthwatch.

- Installer Python 3.7 et rsync 3.0.5 sur l'hôte de sauvegarde
- Vérifier que tous les nœuds de données peuvent communiquer avec l'hôte de sauvegarde à l'aide d'un accès SSH sans mot de passe
- Initialiser le répertoire de sauvegarde sur l'hôte de sauvegarde
- Sauvegarder le data store

Estimer les besoins de stockage de l'hôte de sauvegarde

Avant de commencer

- Connectez-vous à la console du nœud de données en tant qu'utilisateur `root`.

Procédure

1. Copiez la commande suivante, collez-la dans la ligne de commande, puis appuyez sur la touche Entrée pour vous connecter à la base de données à l'aide de vsql et exécuter la requête. Saisissez votre mot de passe, si vous y êtes invité. Notez les résultats.

   ```
   /opt/vertica/bin/vsql -U dbadmin -c "SELECT SUM(used_bytes) FROM storage_containers;"
   ```

2. Multipliez la somme par deux pour estimer l'espace de stockage dont a besoin votre hôte de sauvegarde.

Préparer un hôte de sauvegarde

Avant de commencer

- En fonction des besoins de stockage estimés lors de la tâche précédente, identifiez un hôte exécutant Linux sur votre réseau pour stocker la sauvegarde ou déployez un hôte exécutant Linux avec les exigences de stockage nécessaires.

  > Utilisez un hôte Linux distinct de celui de vos appliances Stealthwatch.

- Connectez-vous à la console de l'hôte de sauvegarde en tant qu'utilisateur `root`.

Procédure

1. Dans l'invite de commande, saisissez `python --version`, puis appuyez sur la touche Entrée pour connaître la version de Python dont vous disposez. Les options suivantes sont disponibles :
   - Si vous disposez de Python 3.7, passez à l'étape 4.
   - Sinon, installez Python 3.7. Passez à l'étape 2.
2. Saisissez `sudo apt-get update`, puis appuyez sur la touche Entrée pour télécharger les versions mises à jour des packages, y compris Python. Saisissez votre mot de passe, si vous y êtes invité.
3. Saisissez `sudo apt-get install python3.7`, puis appuyez sur la touche Entrée pour installer Python 3.7.
4. Dans l'invite de commande, saisissez rsync -version, puis appuyez sur la touche Entrée pour connaître la version de rsync dont vous disposez. Les options suivantes sont disponibles :

   Si vous disposez de rsync 3.0.5, passez à l'étape 7.

   Sinon, installez rsync 3.0.5. Passez à l'étape 5.
5. Saisissez `sudo apt-get update`, puis appuyez sur la touche Entrée pour télécharger les versions mises à jour des packages, y compris rsync. Saisissez votre mot de passe, si vous y êtes invité.
6. Saisissez `sudo apt-get install rsync`, puis appuyez sur la touche Entrée pour installer rsync.
7. Dans l'invite de commande, saisissez `getent passwd | grep dbadmin`, puis appuyez sur la touche Entrée afin de déterminer si un compte utilisateur `dbadmin` existe sur cet hôte. Les options suivantes sont disponibles :

- S'il existe un compte utilisateur `dbadmin`, l'hôte de sauvegarde est prêt. Passez à l'étape **Activer l'accès SSH sans mot de passe pour dbadmin**.
- Sinon, créez un compte utilisateur `dbadmin` sur cet hôte. Passez à l'étape 5.

8. Dans l'invite de commande, saisissez `useradd dbadmin`, puis appuyez sur la touche Entrée pour créer un compte utilisateur `dbadmin`.
9. Saisissez `passwd dbadmin`, puis appuyez sur la touche Entrée pour attribuer un mot de passe à `dbadmin`.
10. Saisissez un **nouveau mot de passe**, puis appuyez sur la touche Entrée pour définir le mot de passe `dbadmin`. Confirmez le mot de passe lorsque vous y êtes invité.

Étape(s) suivante(s)

- Activez l'accès SSH sans mot de passe pour le compte utilisateur `dbadmin`, comme décrit dans la section suivante.

Activer l'accès SSH sans mot de passe pour dbadmin

Avant de commencer

- Ouvrez le port 22/TCP entre l'hôte de sauvegarde et chaque nœud de données pour SSH, et le port 50000/TCP entre l'hôte de sauvegarde et chaque nœud de données pour rsync.
- Consultez la documentation OpenSSH sur `ssh-copy-id` pour plus d'informations.
- Connectez-vous au premier nœud de données en tant qu'utilisateur `root`.

Procédure

1. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   ssh-copy-id -i dbadmin@[hostname]
   ```

2. Remplacez `[hostname]` par le nom d'hôte de l'hôte de sauvegarde.
3. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour copier la clé autorisée SSH de l'utilisateur `dbadmin` sur l'hôte de sauvegarde.
4. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   ssh 'dbadmin@[hostname]'
   ```

5. Remplacez `[hostname]` par le nom d'hôte de l'hôte de sauvegarde.

6. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour vérifier que vous pouvez vous connecter à la console de l'hôte distant via SSH sans saisir le mot de passe de ce nœud de données.

Initialiser le répertoire de sauvegarde sur l'hôte de sauvegarde

Avant de commencer

- Connectez-vous à la console du premier nœud de données en tant qu'utilisateur root.

  Notez le nœud de données que vous utilisez pour initialiser le répertoire de sauvegarde. Vous effectuez également la sauvegarde à partir de ce nœud de données, comme décrit à la section Sauvegarder le data store.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Copiez la commande suivante dans un éditeur de texte : `ssh [backup-host-ip]`
3. Remplacez `[backup-host-ip]` par l'adresse IP de votre hôte de sauvegarde.
4. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour vérifier que vous pouvez vous connecter à l'interface de l'hôte de sauvegarde en tant qu'utilisateur `dbadmin` sans saisir de mot de passe. Si l'hôte de sauvegarde vous demande un mot de passe, vérifiez vos paramètres.
5. Saisissez `cd /home/dbadmin`, puis appuyez sur la touche Entrée pour modifier les répertoires.
6. Saisissez `mkdir backups`, puis appuyez sur la touche Entrée pour créer le répertoire `backups`.
7. Saisissez `exit`, puis appuyez sur la touche Entrée pour revenir à l'invite de ligne de commande du nœud de données.
8. Saisissez `vi pw.ini`, appuyez sur la touche Entrée pour créer le fichier de mots de passe de sauvegarde `pw.ini`, puis modifiez-le.

   > Si vous mettez à jour le mot de passe `dbadmin` à l'aide du script `setup-sw-datastore-secure-connectivity`, vous devez également

> mettre à jour le mot de passe stocké dans le fichier de mots de passe de sauvegarde `pw.ini`, auquel cas votre sauvegarde échouera. Pour plus d'informations, reportez-vous à la section Mettre à jour les mots de passe dbadmin et readonlyuser du data store après l'initialisation.

9. Copiez les lignes suivantes dans un éditeur de texte brut :

```
[Passwords]
dbPassword = [dbadmin-password]
```

10. Mettez à jour `[dbadmin-password]` avec le mot de passe `dbadmin` du data store.
11. Copiez les lignes mises à jour et collez-les dans le fichier de mots de passe de sauvegarde `pw.ini`.
12. Appuyez sur la touche Échap, puis saisissez `:wq` et appuyez sur la touche Entrée pour quitter et enregistrer vos modifications.
13. Saisissez `chmod 640 pw.ini`, puis appuyez sur la touche Entrée pour modifier les autorisations du fichier `pw.ini` afin de permettre à l'utilisateur `dbadmin` d'accéder au fichier et de le modifier.
14. Saisissez `vi config.ini`, puis appuyez sur la touche Entrée pour créer le fichier de configuration de sauvegarde `config.ini` et le modifier.
15. Copiez les lignes suivantes et collez-les dans un éditeur de texte brut :

```
[Mapping]
v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
v_sw_node0003 = backup-host-ip:/home/dbadmin/backups

[Misc]
snapshotName = data_store_backup
passwordFile = /home/dbadmin/pw.ini
enableFreeSpaceCheck = True
retryCount = 2
retryDelay = 1

[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

16. Remplacez *backup-host-ip* par l'adresse IP de l'hôte de sauvegarde.
17. Si les noms d'hôte sous `[Mapping]` ne correspondent pas à ceux de vos nœuds de données, mettez à jour ces noms d'hôte.
18. Assurez-vous de disposer d'une entrée pour chaque nœud de données si vous en avez déployé plus de 3 dans votre environnement.
19. Copiez les lignes mises à jour et collez-les dans le fichier `config.ini`.
20. Appuyez sur la touche Échap, puis saisissez `:wq` et appuyez sur la touche Entrée pour quitter et enregistrer vos modifications.
21. Saisissez `vbr -t init -c config.ini`, puis appuyez sur la touche Entrée pour initialiser le répertoire `/home/dbadmin/backups` sur l'hôte de sauvegarde afin de recevoir les sauvegardes du data store.

Sauvegarder la base de données du data store

Avant de commencer

- En tant qu'utilisateur `root`, connectez-vous à la console du nœud de données à partir de laquelle vous avez initialisé le répertoire de l'hôte de sauvegarde, selon les instructions de la section Initialiser le répertoire de sauvegarde sur l'hôte de sauvegarde.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Saisissez `vbr -t backup -c config.ini --debug 3 --dry-run`, puis appuyez sur la touche Entrée pour effectuer un test de sauvegarde sans créer la sauvegarde. Les options suivantes sont disponibles :
    - Si le test de sauvegarde réussit, sauvegardez le data store. Passez à l'étape 2.
    - Si la résolution du test de sauvegarde échoue, examinez les fichiers journaux de débogage dans le répertoire `/tmp/vbr`, résolvez la cause première, puis testez à nouveau la sauvegarde. Contactez l'assistance Cisco si vous ne parvenez pas à résoudre le problème.
3. Saisissez `vbr -t backup -c config.ini`, puis appuyez sur la touche Entrée pour sauvegarder le data store dans le répertoire `/home/dbadmin/backups` sur l'hôte de sauvegarde.

Restaurer la sauvegarde d'un data store

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Pour restaurer le data store à partir d'une sauvegarde, vous devez vérifier les points suivants :

- Le data store est éteint. Vous pouvez arrêter le data store uniquement si vos collecteurs de flux et votre console SMC ne sont pas connectés et n'effectuent pas de modifications.
- Les noms de nœuds et le nombre de nœuds sont identiques sur la sauvegarde et sur le data store.

Arrêter le data store

Avant de commencer

- Assurez-vous que vos collecteurs de flux ne sont pas connectés au data store et ne transmettent pas de données.
- Assurez-vous que votre console SMC n'est pas connectée au data store, et qu'elle n'interroge pas ou ne met pas à jour le data store.
- Connectez-vous à une console de nœuds de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Les options suivantes sont disponibles :
    - Dans l'invite de commande, saisissez `/opt/vertica/bin/admintools -t stop_db -d sw`, puis appuyez sur la touche Entrée pour arrêter le data store.
    - Dans l'invite de commande, saisissez `/opt/vertica/bin/admintools -t stop_db -d sw -F`, puis appuyez sur la touche Entrée pour arrêter le data store et remplacer les connexions au collecteur de flux ou à la console SMC.

Restaurer le data store à partir d'une sauvegarde

Avant de commencer

- Si vous avez mis à jour le mot de passe `dbadmin` à l'aide du script `setup-sw-datastore-secure-connectivity`, vous devez également mettre à jour le mot de passe stocké dans le fichier de mots de passe de sauvegarde `pw.ini`, auquel cas la restauration échouera. Pour plus d'informations, reportez-vous à la section Mettre à jour les mots de passe dbadmin et readonlyuser du data store après l'initialisation.
- Identifiez le nœud de données sur lequel vous avez stocké le fichier de configuration de sauvegarde `config.ini` et connectez-vous à sa console en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Dans l'invite de commande, saisissez `vbr --task restore --config-file config-file.ini`, puis appuyez sur la touche Entrée pour restaurer le data store à partir de l'hôte de sauvegarde.

Démarrer le data store

Avant de commencer

- Connectez-vous à une console de nœuds de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Dans l'invite de commande, saisissez `/opt/vertica/bin/admintools -t start_db -d sw`, puis appuyez sur la touche Entrée pour démarrer le data store.

Étape(s) suivante(s)

- Supprimez l'instantané du catalogue, comme décrit dans la section suivante.

Supprimer l'instantané du catalogue

Après avoir redémarré le data store, supprimez l'instantané portant le nom `catalog`. Cet instantané n'est pas nécessaire une fois la restauration résolue et empêche Vertica d'exécuter la gestion de la conservation.

Avant de commencer

- Connectez-vous à une console de nœuds de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   /opt/vertica/bin/vsql -U dbadmin -w [password] -c "select
   remove_database_snapshot('catalog');"
   ```

3. Remplacez `[password]` par votre mot de passe `dbadmin`.
4. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour supprimer l'instantané `catalog`.

Étape(s) suivante(s)

- Reconnectez vos collecteurs de flux au data store et vérifiez qu'ils transmettent les données.
- Reconnectez votre console SMC au data store.

Ajouter trois nœuds de données au data store

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Vous pouvez étendre votre data store par incréments de trois nœuds de données, ou multiples de trois nœuds de données. Pour augmenter le nombre de nœuds de données dans votre data store, procédez comme suit :

Préparer le data store pour l'ajout de nœuds de données et le rééquilibrage de charge

Avant d'ajouter un nœud de données, suivez la procédure ci-après :

- Sauvegardez le data store. Reportez-vous à la section **Créer une sauvegarde du data store** pour plus d'informations.
- Assurez-vous que vos collecteurs de flux ne sont pas connectés au data store et ne transmettent pas de données.
- Assurez-vous que votre console SMC n'est pas connectée au data store, et qu'elle n'interroge pas ou ne met pas à jour le data store.
- Supprimez les anciennes partitions de données inutilisées. Contactez les services professionnels Cisco pour vous aider à identifier ces partitions.
- Désactivez les segments locaux. À partir de vsql, exécutez la commande `SELECT DISABLE_LOCAL_SEGMENTS();`
- Mettez à jour les paramètres de votre pool de ressources. À partir de vsql, exécutez la commande `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '70%;`

Ajouter des nœuds de données au data store

Ensuite, si ce n'est pas déjà fait, déployez les nœuds de données sur votre réseau, par multiples de 3. Procédez à la configuration initiale dans Configuration du système à l'aide de l'assistant de configuration initiale et de l'outil de configuration de l'appliance pour terminer la configuration initiale. Reportez-vous à l'**Annexe B. Installation du matériel Stealthwatch** et à l'**Annexe C. Configuration de vos appliances** pour plus d'informations.

Après avoir configuré les nœuds de données, notamment après avoir attribué une adresse IP de gestion `eth0` routable et une adresse IP de canal de port `eth2` ou `eth2/eth3` non routable, procédez comme suit :

- Connectez-vous à un nœud de données et configurez le fichier de configuration `update_SDBN.cfg` pour ajouter vos nouveaux nœuds de données.
- Exécutez le script `update_SDBN.py` pour ajouter les nœuds de données au data store, et éventuellement les ajouter à la base de données du data store.

Ajouter les nœuds de données au data store

Avant de commencer

- Connectez-vous à la console du nœud de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Dans la ligne de commande, saisissez `cd /lancope/database` et appuyez sur la touche Entrée pour changer de répertoire.
3. Saisissez la commande `cp update_SDBN_example.cfg update_SDBN.cfg`, puis appuyez sur la touche Entrée pour créer une copie du fichier de configuration d'exemple d'ajout d'un nœud de données.
4. Saisissez `vi update_SDBN.cfg`, puis appuyez sur la touche Entrée pour modifier le fichier de configuration d'ajout d'un nœud de données dans un éditeur de texte.
5. Créez des sections `[nodeN]` numérotées consécutivement pour qu'elles correspondent au nombre de nouveaux nœuds de données que vous souhaitez ajouter au data store. Par exemple, si vous avez déjà déployé 3 nœuds de données sur votre réseau et que vous souhaitez ajouter 6 nœuds de données, votre fichier contiendra les éléments suivants :

```
[node1]
private = 169.254.42.30
public = 10.0.16.114
[node2]
private = 169.254.42.31
public = 10.0.16.115
[node3]
private = 169.254.42.32
public = 10.0.16.116
[node4]
private = 169.254.42.33
public = 10.0.16.117
[node5]
private = 169.254.42.34
public = 10.0.16.118
[node6]
private = 169.254.42.35
public = 10.0.16.119
[common]
subnet = 10.0.16.0
firstNode = 4
```

6. En commençant par la section `[node1]`, saisissez les adresses IP privées et publiques de chaque nouveau nœud de données. Notez les éléments suivants :
    - Ce script ajoute les nœuds de données au data store dans l'ordre dans lequel ils sont répertoriés, et les numérote consécutivement à partir du nœud de données possédant le numéro le plus élevé et faisant déjà partie du data store. Si vous avez déployé vos nœuds de données dans différents racks, alternez l'affectation des nœuds entre les racks pour optimiser la redondance des données.
    - Les adresses IP privées ne doivent pas être routables, sur un LAN ou un VLAN privé. Vous devez attribuer les adresses IP dans le bloc CIDR `169.254.42.0/24`.
    - Veillez à ne pas faire se chevaucher les adresses IP entre ou parmi les nœuds de données.
    - N'ajoutez pas votre nœud de données de rechange ici, même si vous l'avez déployé dans votre environnement sans le configurer. Ajoutez uniquement les nœuds de données devant appartenir au data store.
7. Dans la section `[common]`, mettez à jour le `sous-réseau` pour qu'il corresponde à vos adresses IP publiques.
8. Dans la section `[common]`, mettez à jour la valeur `firstNode` pour qu'elle soit supérieure d'une unité par rapport au nombre de nœuds de données qui font déjà partie de votre déploiement data store.
9. Appuyez sur la touche Échap, saisissez `:wq`, puis appuyez sur la touche Entrée pour enregistrer vos modifications et quitter l'éditeur de texte.
10. Dans la ligne de commande, vous disposez des options suivantes :

    Saisissez `python update_SDBN.py -i update_SDBN.cfg`, puis appuyez sur la touche Entrée pour exécuter le script python d'ajout d'un nœud de données. Ce script utilise le fichier de configuration `update_SDBN.cfg` pour ajouter les nouveaux nœuds de données au data store dans l'ordre que vous avez spécifié. Notez qu'ils ne sont **pas** ajoutés à la base de données dans ce cas.

    Saisissez `python update_SDBN.py -i update_SDBN.cfg -d`, puis appuyez sur la touche Entrée pour exécuter le script python d'ajout d'un nœud de données. Ce script utilise le fichier de configuration `update_SDBN.cfg` pour ajouter les nouveaux nœuds de données au data store dans l'ordre que vous avez spécifié, et ajoute également les nœuds de données dans la base de données.

    Une fois le script terminé, vérifiez les messages d'état de la CLI pour vous assurer que le script a réussi.

11. Saisissez `cd /opt/vertica/config` pour modifier les répertoires.
12. Saisissez `vi apikeys.dat` pour ouvrir le fichier de clés d'API dans un éditeur de texte.
13. Appuyez sur la touche Échap, puis saisissez `q!` et appuyez sur la touche Entrée pour quitter l'éditeur de texte sans enregistrer les modifications.
14. Notez l'adresse IP de ce nœud de données. Vous utilisez cette adresse IP à l'étape **Maintenance du data store** pour configurer la console VMC sur votre console SMC.

Si vous n'ajoutez pas les nouveaux nœuds de données à la base de données à l'aide du script `update_SDBN.py`, vous pouvez ajouter manuellement les nœuds de données. Connectez-vous à un nœud de données dans votre data store et ajoutez les nœuds de données au data store.

Ajouter de nouveaux nœuds de données au data store

Avant de commencer

- Connectez-vous à un nœud de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   `admintools -t db_add_node -d sw -p '[`*`dbadmin-password`*`]' -s [`*`data-node-eth0-addresses`*`]`

3. Remplacez `[`*`dbadmin-password`*`]` par votre mot de passe `dbadmin`.
4. Remplacez `[`*`data-node-eth0-address`*`]` par une liste séparée par des virgules des nouvelles adresses IP routables `eth0` du nœud de données.
5. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour ajouter les nouveaux nœuds de données à la base de données.

Après avoir ajouté les nœuds de données à votre base de données, rééquilibrez les données entre les nœuds de données pour créer un stockage équilibré des données sur chaque nœud de données.

Rééquilibrer les données dans le data store

Avant de commencer

- Connectez-vous à un nœud de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   /opt/vertica/bin/vsql --timing -x -c "SELECT rebalance_
   cluster()" -a -d sw -U dbadmin -w [dbadmin-password]
   ```

3. Remplacez `[dbadmin-password]` par le mot de passe `dbadmin`.
4. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour lancer le rééquilibrage des données. Notez que cette opération peut prendre un certain temps et dépend de plusieurs facteurs, notamment du nombre de projections et de la quantité de données.
5. Une fois le rééquilibrage terminé, mettez à jour les paramètres de votre pool de ressources. À partir de vsql, exécutez la commande `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '0%;`

Supprimer un nœud de données du data store

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Si vous souhaitez supprimer un nœud de données du data store, notez les points suivants :

- Le data store doit être en cours d'exécution.
- Exécutez d'abord une sauvegarde. Reportez-vous à la section **Créer une sauvegarde du data store** pour plus d'informations.
- Vous devez disposer d'au moins 3 nœuds dans le data store en raison des paramètres de tolérance aux pannes. Si vous souhaitez remplacer un nœud, reportez-vous à la section **Remplacer un nœud de données par un nœud de données de rechange avec une adresse IP différente** pour plus d'informations.

Supprimer un nœud du data store

Avant de commencer

- Connectez-vous à la console de gestion Vertica en tant qu'utilisateur `dbadmin`.

Procédure

1. Sélectionnez **Gérer**. La page correspondante s'affiche.
2. Sélectionnez le nœud que vous souhaitez supprimer, puis cliquez sur **Supprimer le nœud**.

Remplacer un nœud de données par un nœud de données de rechange avec une adresse IP différente

> Contactez les services professionnels Cisco pour obtenir de l'aide concernant la planification et la mise en œuvre de ces tâches.

Préparer le data store pour remplacer un nœud de données en panne

- Sauvegardez le data store. Reportez-vous à la section **Créer une sauvegarde du data store** pour plus d'informations.
- Ajoutez le nœud de données de rechange au data store. Consultez la section **Ajouter les nœuds de données au data store** pour plus d'informations.

Remplacer le nœud de données

Si Vertica fonctionne toujours sur le nœud de données que vous souhaitez remplacer, arrêtez Vertica. Ensuite, remplacez l'ancien nœud de données par le nouveau nœud de données et distribuez la configuration nécessaire au nouveau nœud de données. Supprimez l'ancien nœud de données et redémarrez le nouveau nœud de données.

Arrêter Vertica sur un nœud de données

Si le nœud de données que vous souhaitez supprimer exécute toujours Vertica, arrêtez Vertica sur ce nœud de données. Si ce nœud de données est éteint ou n'exécute pas Vertica, passez à l'étape suivante.

Avant de commencer

- Connectez-vous à la console du nœud de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   /opt/vertica/bin/admintools -t stop_host -s [node-ip-addresses]
   ```

3. Remplacez `[node-ip-address]` par une liste séparée par des virgules des adresses IP routables `eth0` de nœud de données que vous souhaitez supprimer du data store.
4. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour arrêter Vertica sur ce nœud de données.

Remplacer un nœud de données

Avant de commencer

- Connectez-vous à la console du nœud de données en tant qu'utilisateur `root`.

Procédure

1. Saisissez `su - dbadmin`, puis appuyez sur la touche Entrée pour exécuter les commandes suivantes en tant qu'utilisateur `dbadmin`.
2. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   /opt/vertica/bin/admintools -t db_replace_node -d sw -o [old-data-node-hostname] -n [new-data-node-hostname]
   ```

3. Remplacez `[old-data-node-hostname]` par le nom d'hôte du nœud de données que vous souhaitez supprimer du data store.
4. Remplacez `[new-data-node-hostname]` par le nom d'hôte du nœud de données que vous souhaitez ajouter au fichier en remplacement du data store.
5. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour remplacer l'ancien nœud de données par le nouveau nœud de données.
6. Copiez `/opt/vertica/bin/admintools -t distribute_config_files`, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour distribuer les fichiers de configuration dans le nouveau nœud de données.

7. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   `/opt/vertica/sbin/update_vertica --remove-hosts [old-data-node-hostname]`

8. Remplacez `[old-data-node-hostname]` par le nom d'hôte du nœud de données que vous souhaitez supprimer du data store.
9. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour supprimer l'ancien nœud de données du data store.
10. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

    `/opt/vertica/bin/admintools -t restart_node -s [new-data-node-hostname]`

11. Remplacez `[new-data-node-hostname]` par le nom d'hôte du nœud de données que vous souhaitez ajouter au fichier en remplacement du data store.
12. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour redémarrer le nouveau nœud de données.

Copier les informations d'approbation du data store sur une console SMC de basculement

Si vous déployez une console SMC de basculement dans votre environnement et que celle-ci est gérée par votre console SMC principale, lorsque vous exécutez le script `setup-sw-datastore-secure-connectivity`, certaines informations d'approbation, notamment les mots de passe `dbadmin` et `readonlyuser` et les certificats d'identité pour les communications sécurisées avec les nœuds de données, ne sont pas copiées sur la console SMC de basculement. Avant de pouvoir promouvoir la console SMC de basculement en console SMC principale dans un déploiement data store, vous devez copier les fichiers de votre console SMC principale sur la console SMC de basculement. Si vous ne copiez pas ces informations d'approbation, votre console SMC ne peut pas se connecter au data store.

En outre, si vous avez déjà promu votre console SMC de basculement en console SMC principale, rétrogradé votre console SMC principale en console SMC de basculement et souhaitez ajouter de nouvelles appliances à votre déploiement Stealthwatch, vous devez copier les informations d'approbation sur la nouvelle console SMC de basculement avant d'exécuter le script `setup-sw- datastore-secure-connectivity`. Si vous ne copiez pas ces informations d'approbation, le script risque d'échouer.

Copier les informations d'approbation entre les consoles SMC

Avant de commencer

- Identifiez les adresses IP et les informations d'identification de l'utilisateur root de la console SMC principale et de la console SMC de basculement.
- Si vous venez de promouvoir votre console SMC de basculement en console SMC principale, connectez-vous à cette console en tant qu'utilisateur `root`.

Procédure

1. Copiez la commande suivante et collez-la dans un éditeur de texte brut :

   ```
   scp root@[demoted-smc-ip-address]:/lancope/var/admin/cds/sw-datastore-* /lancope/var/admin/cds
   ```

2. Remplacez `[demote-smc-ip-address]` par l'adresse IP de votre console SMC nouvellement rétrogradée (c'est-à-dire la console SMC de basculement actuelle).

3. Copiez la commande mise à jour, collez-la dans l'invite de commande, puis appuyez sur la touche Entrée pour copier les informations d'approbation du data store de votre console SMC nouvellement rétrogradée (console de basculement actuelle) vers votre console SMC nouvellement promue (console principale actuelle). Saisissez le mot de passe `root` correspondant à la console SMC nouvellement rétrogradée (console de basculement actuelle) lorsque vous y êtes invité.

Résoudre les problèmes liés au déploiement du data store

Résoudre les problèmes liés au déploiement du matériel

En cas de problèmes de déploiement ou de configuration de votre console SMC ou de vos collecteurs de flux, consultez le Guide d'installation matérielle des appliances Stealthwatch x210 et le Guide de configuration du système Stealthwatch pour plus d'informations.

Résoudre les problèmes liés au script setup-sw-datastore-secure-connectivity

Si vous avez promu une console SMC de basculement en console SMC principale, reportez-vous à la section Copier les informations de confiance du data store sur une console SMC de basculement pour en savoir plus sur la copie des informations de confiance du data store sur votre console SMC nouvellement promue (c'est-à-dire, la console principale actuelle).

Le script de connexion sécurisée `commande setup-sw-datastore-secure-connectivity` du data store consigne les messages dans les fichiers journaux à l'adresse `/lancope/var/logs/containers/setup-sw-datastore-secure-connectivity.log`. Consultez ces messages pour obtenir des informations supplémentaires.

Messages d'erreur généraux liés au script setup-sw-datastore-secure-connectivity

Le tableau suivant répertorie les messages d'erreur qui peuvent s'afficher si le script `setup-sw-datastore-secure-connectivity` rencontre une erreur, ainsi que les solutions possibles au problème.

Message d'erreur	Description	Solutions possibles
Erreur lors de l'autorisation de la connexion à distance pour `[ip-address]`.	Le script `setup-sw-datastor`	• Vérifiez que vous avez fourni le mot de passe racine correct pour l'accès. • Vérifiez que l'appliance est en cours

	`e-secure-connectivity` n'a pas pu se connecter à distance à une appliance pour fournir des informations clés.	d'exécution. • Vérifiez que la connexion entre le script et l'appliance est actuellement active.
Erreur lors de la génération de la paire de clés.	Le script `setup-sw-datastore-secure-connectivity` a rencontré une erreur lors de la génération des clés associées aux certificats d'identité utilisés pour les connexions sécurisées du data store.	• Contactez le service d'assistance Cisco pour plus d'informations.
Échec de l'authentification avec l'autorité de jeton.	Le script `setup-sw-datastore-secure-connectivity` n'a pas	• Contactez le service d'assistance Cisco pour plus d'informations.

	pu établir une connexion avec Central Management.	
Échec de l'obtention de l'inventaire auprès de la console SMC.	Le script `setup-sw-datastore-secure-connectivity` n'a pas pu récupérer correctement les informations de Central Management.	• Examinez le fichier `/lancope/var/logs/container/svc-central-management.log` pour essayer de déterminer s'il existe un problème avec Central Management. • Contactez le service d'assistance Cisco pour plus d'informations.
Aucun client de base de données trouvé.	La console SMC et les collecteurs de flux n'ont pas été correctement configurés pour être utilisés avec un data store.	• Connectez-vous à l'interface de ligne de commande de l'appliance, exécutez la configuration système, puis activez l'utilisation avec un data store.
Le mot de passe n'est pas disponible. Vous pouvez supprimer /lancope/var/etc/keystore/store et réexécuter le script setup-sw-datastore-secure-connectivity.	Le script `setup-sw-datastore-secure-connectivity` a rencontré un problème lors de	• Supprimez le contenu de `lancope/var/etc/keystore/store`, puis réexécutez le script `setup-sw-datastore-secure-connectivity`.

	l'enregistrement ou de la distribution des mots de passe `dbadmin` et `readonlyuser`.	
Enregistrez les nœuds de données auprès de Central Management avant de tenter de configurer la connexion sécurisée.	Vos nœuds de données ne sont pas gérés par Central Management.	• Gérez vos nœuds de données avec Central Management.
L'inventaire SMC est vide. Ajoutez une appliance à Central Management.	Central Management ne gère aucun nœud de données ou collecteur de flux.	• Gérez vos collecteurs de flux et vos nœuds de données avec Central Management.
sw-datastore-dbadmin-password et/ou sw-datastore-readonlyuser-password non présents dans l'entrée.	Le mot de passe `dbadmin` ou le mot de passe `readonlyuser` n'a pas été défini.	• Dans le script, renouvelez l'étape **1. Distribuer le mot de passe du data store logiciel aux appliances**, si vous n'avez pas encore initialisé le data store, et définissez à la fois un mot de passe `dbadmin` et un mot de passe `readonlyuser`. • Si vous avez initialisé le data store, dans le script, exécutez l'étape **3. Mettre à jour le mot de passe du data store logiciel sur les appliances** pour mettre à jour les mots de passe `dbadmin` et

		`readonlyuser`.
Le ou les mots de passe du data store logiciel ont déjà été initialisés sur `[ip-address]`.	Le data store est déjà initialisé ; vous ne pouvez pas utiliser l'étape **1. Distribuer le mot de passe du data store logiciel aux appliances** dans le script `setup-sw-datastore-secure-connectivity` pour modifier les mots de passe `dbadmin` ou `readonlyuser`.	• Dans le script, exécutez l'étape **3. Mettre à jour le mot de passe du data store logiciel sur les appliances** pour mettre à jour les mots de passe `dbadmin` et `readonlyuser`.
Le ou les mots de passe du data store logiciel ne sont pas stockés pour la raison suivante : Valeur vide.	Le mot de passe `dbadmin` ou le mot de passe `readonlyuser` n'a pas été défini.	• Dans le script, renouvelez l'étape **1. Distribuer le mot de passe du data store logiciel aux appliances**, si vous n'avez pas encore initialisé le data store, et définissez à la fois un mot de passe `dbadmin` et un mot de passe `readonlyuser`. • Si vous avez initialisé le data store,

		dans le script, exécutez l'étape **3. Mettre à jour le mot de passe du data store logiciel sur les appliances** pour mettre à jour les mots de passe `dbadmin` et `readonlyuser`.
Aucun nœud de données n'est actuellement géré.	Vos nœuds de données ne sont pas gérés par Central Management.	• Gérez vos nœuds de données avec Central Management.
Aucune console SMC/FC n'est actuellement gérée.	Vos collecteurs de flux (et toutes les consoles SMC de basculement) ne sont pas gérés par Central Management.	• Gérez vos collecteurs de flux (et les consoles SMC de basculement) avec Central Management.
Code d'erreur inconnu : `[error-code]` sur `[ip-address]`.	Le script a rencontré une erreur lors de la tentative de distribution des mots de passe `dbadmin` et `readonlyuser`.	• Contactez le service d'assistance Cisco pour plus d'informations.

Résoudre les problèmes liés au script install_SDBN_initial.py

Le script d'initialisation `install_SDBN_initial.py` data store consigne les messages dans les fichiers journaux à l'adresse `/lancope/var/database/logs/db_initial_install_[datestamp].log`. Consultez ces messages pour obtenir des informations supplémentaires.

Les conditions préalables ne sont pas entièrement respectées lors de la configuration locale (système d'exploitation) pour verify-[data-node-ip-address].xml

Lors de l'initialisation du data store à l'étape Initialisation et configuration du data store via l'exécution du script python `install_SDBN_initial.py`, vous remarquerez peut-être que la console affiche le message `Prerequisites not fully met during local (OS) configuration for verify-[data-node-ip-address].xml`, puis une série de messages de journalisation. Ces messages de journalisation s'affichent par anticipation ; ils n'indiquent pas l'échec de l'initialisation de data store. Aucune intervention de votre part n'est requise lors de l'affichage de ces messages de journalisation.

Le tableau suivant décrit chaque message.

Niveau de journalisation et code d'erreur	**Description**	**Explication**
`ÉCHEC (s0180)`	`Taille d'échange insuffisante. Capacité nécessaire : 2 Go, capacité actuelle : 1,50 Go`	L'espace alloué à la partition d'échange n'est pas conforme aux recommandations. Veillez à ne **pas** modifier l'espace d'échange alloué. Cisco a configuré votre data store en allouant l'espace d'échange adéquat.
`ÉCHEC (s0311)`	`Le compte racine ne se trouve pas`	Le programme d'installation n'a pas trouvé le compte racine dans la liste des autorisations de super utilisateur

	dans /etc/sudoers	/etc/sudoers et vous recommande de mettre à niveau Vertica pour résoudre le problème. Veillez à ne **pas** mettre à niveau Vertica. Cette configuration est intentionnelle pour des raisons de sécurité.
CONSEIL (S0040)	Les outils suivants, normalement fournis par le package pstack ou gstack, sont introuvables : pstack/gstack	Le programme d'installation ne trouve pas les packages pstack ou gstack pour la journalisation des traces de pile. Ils ne sont pas nécessaires pour votre data store.
CONSEIL (S0041)	Les outils suivants, normalement fournis par le package mcelog, sont introuvables : mcelog	Le programme d'installation ne trouve pas le package mcelog pour la journalisation des contrôles de la machine. Celui-ci n'est pas nécessaire pour votre data store.
CONSEIL (S0305)	TZ est unsert pour dbadmin. Envisagez de mettre à jour .profile ou .bashrc	Le programme d'installation n'a pas trouvé de variable d'environnement TZ pour le compte utilisateur dbadmin, utilisée pour les fuseaux horaires. Celle-ci n'est pas nécessaire pour votre data store, car vous configurez des serveurs NTP pour votre déploiement Stealthwatch.
AVERTISSEMENT (N0010)	Le pare-feu iptables Linux contient des règles non triviales dans les tables : filtre	Le pare-feu iptables du nœud de données contient des règles préexistantes. Le système indique un avertissement si le pare-feu iptables contient des règles, mais ne vérifie pas les collisions avec les ports de communication requis. Ce

		comportement est normal et ne devrait pas poser de problème lors du déploiement du nœud de données.

Le paramètre de configuration SSLCA n'est pas défini ; les certificats clients ne seront ni demandés ni vérifiés

Lors de l'initialisation du data store à l'étape Initialisation et configuration du data store via l'exécution du script python `install_SDBN_initial.py`, vous remarquerez peut-être que la console affiche une fois le message `Enable SSL/TLS for remote connections`, puis le message `INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified` pour chaque nœud de données que vous initialisez. Ce message de journalisation s'affiche par anticipation ; il n'indique pas un échec de l'établissement des connexions sécurisées avec le data store. Aucune intervention de votre part n'est requise lors de l'affichage de ces messages de journalisation.

Le data store est configuré en mode Serveur TLS, ce qui signifie que lorsque les appliances établissent une connexion sécurisée avec le data store, elles vérifient également le certificat de serveur de la base de données. Comparez cela avec la configuration du mode TLS mutuel, qui exige que, lorsque les appliances établissent une connexion sécurisée avec le data store, les appliances vérifient le certificat de serveur de la base de données et que la base de données vérifie les certificats clients des appliances. Le mode TLS mutuel nécessite la configuration du paramètre `SSLCA` avec le fichier `root.crt` contenant l'autorité de certification (CA) ou la chaîne de confiance de l'autorité de certification servant à signer les certificats clients. Étant donné que le mode Mutuel n'est pas activé, le paramètre `SSLCA` n'est pas configuré et le data store ne vérifie pas les certificats clients lors de l'établissement d'une connexion sécurisée. Cependant, la connexion entre les appliances et le data store en mode Serveur TLS reste une connexion sécurisée sur TLS.

Messages d'erreur généraux liés au script install_SDBN_initial.py

Le tableau suivant répertorie les messages d'erreur qui peuvent s'afficher si le script `install_SDBN_initial.py` rencontre une erreur, ainsi que les solutions possibles au problème.

Message d'erreur	Description	Solutions possibles
Fichier de configuration introuvable ou aucune section valide.	Le script `install_SDBN_initial.py` ne trouve pas le fichier de configuration `install_SDBN.cfg`, ou les données du fichier de configuration ne correspondent pas au format attendu.	• Assurez-vous de disposer d'une copie de `install_SDBN_example.cfg` enregistrée dans `/lancope/database/install_SDBN.cfg` sur ce nœud de données. • Assurez-vous que la mise en forme du fichier `install_SDBN.cfg` correspond à la mise en forme du fichier `install_SDBN_example.cfg`, que vous nommez chaque section de nœud au format `node#`, que vous avez défini une adresse IP privée et une adresse IP publique pour chaque section de configuration du nœud de données, et que vous disposez d'un sous-réseau défini dans la section commune.
Le fichier .jar attendu pour récupérer les mots de passe des utilisateurs de la base de données est introuvable, vérifiez que vous exécutez une image contenant cette prise en charge.	Le script `install_SDBN_initial.py` ne peut pas localiser le fichier `sw-datastore-admin.jar` qui contient les mots de passe `dbadmin` et `readonlyuser`.	• Assurez-vous que votre appliance dispose de la version 7.3+. • Exécutez le script `setup-sw-datastore-secure-connectivity` sur `/lancope/admin/cds` et sélectionnez l'option **1. Distribuer le mot de passe du data store logiciel aux appliances** pour distribuer les mots de passe dbadmin et readonlyuser. Une fois cette opération terminée, si ce n'est pas déjà fait, exécutez également l'option **2. Distribuer les certificats pour la connexion sécurisée à la base de données**. • Contactez le service d'assistance Cisco

		si l'erreur persiste.
Chaque nœud doit posséder une entrée d'adresse publique et privée.	Le fichier de configuration `install_SDBN.cfg` comporte une ou plusieurs entrées de nœud pour lesquelles aucune adresse IP privée et publique n'est définie.	• Vérifiez que vous avez défini une adresse IP privée et une adresse IP publique pour chaque section de configuration du nœud de données dans `/lancope/database/install_SDBN.cfg`.
Le fichier de magasin des secrets n'existe pas OU le mot de passe n'existe pas dans le fichier. Connectez-vous à la console SMC et exécutez le script approprié pour définir et distribuer les mots de passe de la base de données.	Le script `install_SDBN_initial.py` a rencontré un problème lors de la tentative de récupération des mots de passe `dbadmin` et `readonlyuser`.	• Dans l'interface de ligne de commande de la console SMC, exécutez le script `setup-sw-datastore-secure-connectivity` sur `/lancope/admin/cds` et sélectionnez l'option **1. Distribuer le mot de passe du data store logiciel aux appliances** pour distribuer les mots de passe dbadmin et readonlyuser. Une fois cette opération terminée, si ce n'est pas déjà fait, exécutez également l'option **2. Distribuer les certificats pour la connexion sécurisée à la base de données**.
Impossible de récupérer les mots de passe de la base de données.	Le script `install_SDBN_initial.py` a rencontré un	• Dans l'interface de ligne de commande de la console SMC, exécutez le script `setup-sw-datastore-secure-connectivity` sur `/lancope/admin/cds` et

	problème lors de la tentative de récupération des mots de passe `dbadmin` et `readonlyuser`.	sélectionnez l'option **1. Distribuer le mot de passe du data store logiciel aux appliances** pour distribuer les mots de passe dbadmin et readonlyuser. Une fois cette opération terminée, si ce n'est pas déjà fait, exécutez également l'option **2. Distribuer les certificats pour la connexion sécurisée à la base de données**.
Exception d'E/S lors de la lecture du fichier.	Le script `install_SDBN_initial.py` a rencontré un problème lors de la tentative de récupération des mots de passe `dbadmin` et `readonlyuser`.	• Contactez le service d'assistance Cisco et spécifiez le message d'erreur.
L'un des deux mots de passe n'existe pas dans le fichier. Connectez-vous à la console SMC et exécutez le script approprié pour définir et distribuer les mots de passe de la base de données.	Le script `install_SDBN_initial.py` a rencontré un problème lors de la tentative de récupération des mots de passe `dbadmin` et `readonlyuser`.	• Dans l'interface de ligne de commande de la console SMC, exécutez le script `setup-sw-datastore-secure-connectivity` sur `/lancope/admin/cds` et sélectionnez l'option **1. Distribuer le mot de passe du data store logiciel aux appliances** pour distribuer les mots de passe dbadmin et readonlyuser. Une fois cette opération terminée, si ce n'est pas déjà fait, exécutez également l'option **2. Distribuer les certificats pour la connexion sécurisée à la base de**

		données.
Il est nécessaire de spécifier la valeur privateAddrs.	Le fichier de configuration `install_SDBN.cfg` comporte une ou plusieurs entrées de nœud pour lesquelles aucune adresse IP privée n'est définie.	• Vérifiez que vous avez défini une adresse IP privée pour chaque section de configuration du nœud de données dans `/lancope/database/install_SDBN.cfg`. Notez que le nœud de données utilise cette adresse IP non routable sur `eth2` pour communiquer avec d'autres nœuds de données dans le cadre du data store.
Il est nécessaire de spécifier la valeur publicAddrs.	Le fichier de configuration `install_SDBN.cfg` comporte une ou plusieurs entrées de nœud pour lesquelles aucune adresse IP publique n'est définie.	• Vérifiez que vous avez défini une adresse IP publique pour chaque section de configuration du nœud de données dans `/lancope/database/install_SDBN.cfg`. Notez que le nœud de données utilise cette adresse IP routable sur `eth0` pour communiquer avec d'autres appliances Stealthwatch dans le cadre de votre déploiement Stealthwatch.
Il est nécessaire de spécifier la valeur publicSubnet.	Le fichier de configuration `install_SDBN.cfg` contient une ou plusieurs entrées de nœud pour	• Vérifiez que vous avez défini un sous-réseau dans la section de configuration commune dans `/lancope/database/install_SDBN.cfg`. Notez que ce sous-ensemble est associé aux adresses IP routables sur les `eth0` nœud de données pour communiquer avec

	lesquelles aucun sous-réseau n'est défini.	d'autres appliances Stealthwatch dans le cadre de votre déploiement Stealthwatch.
Exception inattendue lors de la lecture des secrets.	Le script `install_SDBN_initial.py` a rencontré un problème lors de la tentative de récupération des mots de passe `dbadmin` et `readonlyuser`.	• Exécutez le script `setup-sw-datastore-secure-connectivity` sur `/lancope/admin/cds` et sélectionnez l'option **1. Distribuer le mot de passe du data store logiciel aux appliances** pour distribuer les mots de passe dbadmin et readonlyuser. Une fois cette opération terminée, si ce n'est pas déjà fait, exécutez également l'option **2. Distribuer les certificats pour la connexion sécurisée à la base de données**. • Contactez le service d'assistance Cisco si l'erreur persiste.
Valeur de retour inattendue.	Le script `install_SDBN_initial.py` a reçu une valeur et s'est arrêté, car il ne pouvait pas continuer.	• Contactez le service d'assistance Cisco et spécifiez le message d'erreur.

Mettre à jour les mots de passe dbadmin et readonlyuser du data store après l'initialisation

Si vous avez déjà initialisé le data store conformément aux instructions de la section Initialisation et configuration du data store et souhaitez modifier les mots de passe `dbadmin` et `readonlyuser`, exécutez le script bash de connectivité sécurisée `setup-sw-datastore-secure-connectivity`. Après avoir fourni le mot de passe `dbadmin` actuel, vous pouvez attribuer de nouveaux mots de passe pour

`dbadmin` et `readonlyuser`. Le script distribue les informations d'identification mises à jour à vos appliances via SSH et met à jour les informations d'identification des comptes utilisateur `dbadmin` et `readonlyuser`.

> Si vous avez perdu le mot de passe `dbadmin`, contactez le service d'assistance Cisco pour le récupérer.

Chaque mot de passe doit respecter les conditions suivantes :

- contenir au moins un nombre
- contenir au moins un caractère en minuscules
- contenir au moins un caractère en majuscules
- contenir au moins un caractère spécial parmi la liste suivante : `<>.,? / '"|:;` ~! @ # $% ^ & * () -_ + = {} []`
- contenir au moins 8 caractères (aucune restriction de longueur maximum)
- contenir uniquement des caractères codés ASCII

Notez que vous devez utiliser cette option si vous avez déjà initialisé le data store. Si vous effectuez le déploiement et la configuration initiaux du data store, reportez-vous à la section Distribuer les mots de passe du data store à votre console SMC, vos nœuds de données et vos collecteurs de flux pour attribuer des mots de passe aux comptes utilisateur `dbadmin` et `readonlyuser` et configurer les paramètres de connexion sécurisée avec la base de données du data store.

Si vous avez sauvegardé la base de données du data store, puis modifié le mot de passe `dbadmin`, mettez à jour le fichier de mots de passe de sauvegarde `pw.ini` avec le nouveau mot de passe `dbadmin`. Reportez-vous à la section Créer une sauvegarde du data store pour plus d'informations.

Avant de commencer

- Compilez une liste de mots de passe racines pour votre console SMC, vos nœuds de données, vos collecteurs de flux et votre console SMC secondaire si vous en avez déployé une.
- Activez l'accès SSH et l'accès SSH racine sur votre console SMC, vos nœuds de données et vos collecteurs de flux.

> ⚠ Une fois la console SSH activée, le risque de compromission du système augmente. Il est important d'activer SSH uniquement lorsque vous en avez besoin. Lorsque vous avez terminé d'utiliser l'accès SSH, désactivez-le.

- Connectez-vous à l'interface de ligne de commande de votre console SMC en tant qu'utilisateur racine.

Procédure

1. Dans la ligne de commande, saisissez `cd /lancope/admin/cds` et appuyez sur la touche Entrée pour modifier les répertoires.
2. Saisissez la commande `./setup-sw-datastore-secure-connectivity` et appuyez sur la touche Entrée pour exécuter le script bash de connectivité sécurisée au data store.
3. Dans le menu principal du script, sélectionnez **3. Mettre à jour le mot de passe du data store logiciel sur les appliances**.
4. Saisissez le mot de passe **dbadmin** actuel et sélectionnez **OK**.
5. Sur la ligne de commande, lorsque vous êtes invité à saisir le mot de passe root pour chaque appliance, saisissez-le et appuyez sur la touche Entrée.

   > ⓘ Étant donné que vous saisissez plusieurs mots de passe, veillez à saisir le mot de passe correspondant à cette appliance.

   Après avoir saisi tous les mots de passe root des appliances, le script vous invite à saisir les mots de passe `dbadmin` et `readonlyuser`.
6. Saisissez le nouveau mot de passe **dbadmin**.
7. Saisissez le même mot de passe `dbadmin` dans le champ **dbadmin (confirmation)**.
8. Saisissez le nouveau mot de passe **readonlyuser**.
9. Saisissez le même mot de passe `readonlyuser` dans le champ **readonlyuser (confirmation)**.

   > ⓘ Veillez à ne pas saisir le même mot de passe pour `dbadmin` que pour `readonlyuser`. Si vous attribuez le même mot de passe, le script échoue et aucun mot de passe n'est attribué aux comptes utilisateur.
10. Cliquez sur **OK**.

Le script distribue ces mots de passe de manière sécurisée à vos appliances. Lorsque vous avez terminé, la liste des appliances mises à jour s'affiche.

11. Sélectionnez **OK** pour revenir au menu principal du script.

Étape(s) suivante(s)

- Connectez-vous à la console VMC en tant qu'utilisateur `dbadmin`. Vous êtes invité à mettre à jour votre mot de passe.

> Si vous ne mettez pas à jour le mot de passe pour qu'il corresponde au nouveau mot de passe `dbadmin`, la console VMC n'envoie pas de notifications d'alerte d'intégrité ou ne contrôle pas correctement votre data store.

Résoudre les problèmes liés au script update_SDBN.py

Le script du nœud de données `update_SDBN_initial.py` consigne les messages dans les fichiers journaux à l'adresse `/lancope/var/database/logs/db_update_[datestamp].log`. Consultez ces messages pour obtenir des informations supplémentaires.

Messages d'erreur généraux liés au script update_SDBN_initial.py

Le tableau suivant répertorie les messages d'erreur qui peuvent s'afficher si le script `update_SDBN_initial.py` rencontre une erreur, et les solutions possibles au problème.

Message d'erreur	Description	Solutions possibles
Fichier de configuration introuvable ou aucune section valide	Le script `update_SDBN.py` ne trouve pas le fichier de configuration `update_SDBN.cfg`, ou	• Assurez-vous de conserver une copie du script `update_SDBN.cfg` dans `/lancope/database/update_SDBN.cfg` sur ce nœud de données. • Assurez-vous que la mise en forme du fichier `update_SDBN.cfg` correspond à la mise en forme du fichier `update_SDBN_example.cfg`, que vous nommez chaque

	les données du fichier de configuration ne correspondent pas au format attendu.	section de nœud au format `node#`, que vous avez défini une adresse IP privée et une adresse IP publique pour chaque section de configuration du nœud de données, que vous avez défini un sous-réseau dans la section commune, et que vous avez défini le premier nœud comme un nœud supplémentaire par rapport au nombre total de nœuds déjà présents dans votre data store.
Chaque nœud doit posséder une entrée d'adresse publique et privée	Le fichier de configuration `update_SDBN.cfg` comporte une ou plusieurs entrées de nœud pour lesquelles aucune adresse IP privée et publique n'est définie.	• Vérifiez que vous avez défini une adresse IP privée et une adresse IP publique pour chaque section de configuration du nœud de données dans `/lancope/database/update_SDBN.cfg`.
Impossible de récupérer le mot de passe dbadmin de la base de données	Le script `update_SDBN.py` ne trouve pas le mot de passe `dbadmin`.	• Assurez-vous que votre appliance dispose de la version 7.3+. • Exécutez le script `setup-sw-datastore-secure-connectivity` sur `/lancope/admin/cds` et sélectionnez l'option **3. Mettre à jour le mot de passe du data store logiciel sur les appliances** pour définir les mots de passe `dbadmin` et `readonlyuser`. • Contactez le service d'assistance Cisco si l'erreur persiste.
Il est	La valeur	• Vérifiez que vous avez défini une valeur

nécessaire de spécifier la valeur firstNode	`firstNode` n'est pas définie sur le fichier de configuration `update_SDBN.cfg`.	firstNode dans la section de configuration commune de `/lancope/database/update_SDBN.cfg`.
Il est nécessaire de spécifier la valeur privateAddrs	Le fichier de configuration `update_SDBN.cfg` contient une ou plusieurs entrées de nœud pour lesquelles aucune adresse IP privée n'est définie.	• Vérifiez que vous avez défini une adresse IP privée pour chaque section de configuration du nœud de données dans `/lancope/database/update_SDBN.cfg`. Notez que le nœud de données utilise cette adresse IP non routable sur `eth2` pour communiquer avec d'autres nœuds de données dans le cadre de la base de données du data store.
Il est nécessaire de spécifier la valeur publicAddrs	Le fichier de configuration `update_SDBN.cfg` comporte une ou plusieurs entrées de nœud pour lesquelles aucune adresse IP publique n'est définie.	• Vérifiez que vous avez défini une adresse IP publique pour chaque section de configuration du nœud de données dans `/lancope/database/update_SDBN.cfg`. Notez que le nœud de données utilise cette adresse IP routable sur `eth0` pour communiquer avec d'autres appliances Stealthwatch dans le cadre de votre déploiement Stealthwatch.
Il est nécessaire	Le fichier de configuration	• Vérifiez que vous avez défini un sous-réseau dans la section de configuration commune du

de spécifier la valeur publicSubnet	`update_SDBN.cfg` contient une ou plusieurs entrées de nœud pour lesquelles aucun sous-réseau n'est défini.	fichier `/lancope/database/update_SDBN.cfg`. Notez que ce sous-ensemble est associé aux adresses IP routables sur les nœuds de données `eth0` pour communiquer avec d'autres appliances Stealthwatch dans le cadre de votre déploiement Stealthwatch.

Résoudre les problèmes liés à la console de gestion Vertica

Si votre instance de la console VMC ne s'actualise pas automatiquement dans votre navigateur web, vous devrez peut-être l'actualiser manuellement pour afficher les modifications apportées à votre data store ou à votre configuration.

Résolution des problèmes au data store

Notez que le data store réserve jusqu'à 40 % de l'espace de stockage disponible pour maintenir le data store. Au minimum, 60 % de l'espace total est disponible pour le stockage de flux.

La plateforme analytique Vertica ne redémarre pas automatiquement après la mise hors tension et le redémarrage d'un nœud de données

Si le nœud de données se met hors tension de manière inattendue et que vous redémarrez l'appliance, l'instance de la plateforme analytique Vertica (Vertica) sur ce nœud de données risque de ne pas redémarrer automatiquement, sans doute parce que certaines données ont été endommagées. Si le nombre de nœuds de données en cours d'exécution est suffisant pour poursuivre l'exécution du data store, le data store continue d'intégrer les données via des collecteurs de flux. Cependant, vous devez redémarrer le nœud de données dès que possible pour lui permettre de se connecter au data store, de récupérer les données manquantes des nœuds de données adjacents et de revenir au niveau des autres nœuds de données.

Dans ce cas, connectez-vous au nœud de données et forcez manuellement le redémarrage de Vertica, afin de supprimer les données endommagées et de permettre à Vertica de redémarrer correctement.

En outre, vous devrez peut-être mettre à jour la politique de restauration de l'alimentation du nœud de données avant de le redémarrer. Si la politique de restauration de l'alimentation est désactivée, vous devez redémarrer manuellement le nœud de données après la coupure d'alimentation. Reportez-vous au Guide de configuration de l'interface utilisateur graphique des systèmes UCS C pour plus d'informations sur la configuration de la politique de restauration de l'alimentation dans CIMC.

Avant de commencer

- Connectez-vous à l'interface de ligne de commande du nœud de données en tant qu'utilisateur racine.

Procédure

1. Copiez la commande suivante et collez-la dans un éditeur de texte :

   ```
   tail /lancope/var/database/dbs/sw/v_sw_[node_name]_
   catalog/ErrorReport.txt
   ```

2. Remplacez *[note_name]* par le nom de votre nœud de données (par exemple, `node0001`).
3. Copiez la commande mise à jour et collez-la dans l'interface de ligne de commande, puis appuyez sur la touche Entrée pour examiner les entrées les plus récentes du fichier d'erreurs `ErrorReport.txt`. Si le message d'erreur signale des problèmes de cohérence ou de corruption des données, passez à l'étape suivante pour forcer le redémarrage de Vertica.
4. Copiez la commande suivante et collez-la dans un éditeur de texte :

   ```
   admintools -t restart_node --hosts=[data-node-ip-address]
   --database='sw-datastore' --password="[dbadmin-password]"
   --force
   ```

5. Remplacez *[data-node-ip-address]* par l'adresse IP du votre nœud de données concerné.
6. Remplacez *[dbadmin-password]* par votre mot de passe `dbadmin` du data store.
7. Copiez la commande mise à jour et collez-la dans l'interface de ligne de

commande, puis appuyez sur la touche Entrée pour forcer le redémarrage de Vertica sur le nœud de données concerné. Vertica supprime toutes les données endommagées et les récupère à partir des nœuds de données adjacents.

8. Si le système affiche le message `Do you want to continue waiting? (yes/no) [yes]`, saisissez `yes` et appuyez sur la touche Entrée pour continuer à attendre.

   Étant donné que Vertica restaure les informations du nœud de données correspondant à partir des nœuds de données adjacents, si ces nœuds de données ont intégré une grande quantité de trafic de flux alors que le nœud de données concerné était en panne, la récupération du nœud de données concerné peut prendre un certain temps.

Étape(s) suivante(s)

- Passez en revue les recommandations de Cisco relatives à l'alimentation de vos nœuds de données dans la section Exigences et considérations relatives au déploiement du data store.

Annexe A. Préparation de l'installation

Avertissements relatifs à l'installation

Lisez le document Informations relatives à la conformité et à la sécurité avant d'installer les appliances Stealthwatch data store.

Prenez en compte les avertissements suivants :

Consigne 1 071 – Définition de l'avertissement

CONSIGNES DE SÉCURITÉ IMPORTANTES

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Utilisez le numéro indiqué après chaque consigne de sécurité pour pouvoir retrouver sa traduction parmi les consignes relatives à ce périphérique.

CONSERVEZ CES INSTRUCTIONS.

Consigne 1 005 – Disjoncteur

Un système de protection contre les risques de court-circuit (surintensité) doit être installé dans le bâtiment. Assurez-vous que la puissance nominale du dispositif de protection n'est pas supérieure à : 120 V, 15 A (USA), 250 V, 16 A (UE).

Consigne 1 004 – Instructions d'installation

Avant d'utiliser, d'installer ou de brancher le système sur la source d'alimentation, consultez les instructions d'installation.

Consigne 12 – Avertissement relatif à la déconnexion de la source d'alimentation

Avant de travailler sur un châssis ou à proximité de modules d'alimentation, débranchez le câble d'alimentation des unités CA. Sur les unités CC, coupez l'alimentation au niveau du disjoncteur.

Consigne 43 – Avertissement relatif au retrait des bijoux

Avant d'utiliser un appareil raccordé au réseau électrique, retirez vos bijoux (bagues, colliers, montre, etc.). En cas de contact avec l'alimentation électrique et la mise à la terre, les objets métalliques peuvent chauffer et provoquer de graves brûlures ou se souder aux bornes.

Consigne 94 – Avertissement relatif au port de bracelets de mise à la terre

Au cours de cette procédure, portez des bracelets de mise à la terre pour éviter d'endommager la carte par choc électrostatique. Pour éviter les risques d'électrocution, ne touchez pas le fond de panier directement avec les mains ni avec un outil métallique.

Consigne 1 045 – Protection contre les courts-circuits

Un système de protection contre les courts-circuits (surintensité) doit être installé dans le bâtiment accueillant ce produit. Installez-le uniquement conformément aux réglementations nationales et locales.

Consigne 1 021 – Circuit SELV

Pour prévenir tout risque de décharge électrique, ne connectez pas les circuits de sécurité de très basse tension (SELV) aux circuits de tension du réseau téléphonique (TNV). Les ports LAN comportent des circuits SELV et les ports WAN sont équipés de circuits TNV. Certains ports LAN et WAN utilisent des connecteurs RJ-45. Soyez prudent lors du branchement des câbles.

Consigne 1 024 – Conducteur de terre

Cet équipement doit être relié à la terre. N'endommagez jamais le conducteur de terre et n'utilisez pas l'équipement sans avoir préalablement installé un

conducteur de terre adéquat. Contactez l'autorité de contrôle compétente ou un électricien si vous n'êtes pas sûr qu'une mise à la terre correcte a été effectuée.

Consigne 1 040 – Mise au rebut du produit

La mise au rebut de ce produit doit être effectuée conformément aux réglementations nationales.

Consigne 1 074 – Respect des réglementations électriques locales et nationales

L'installation de l'équipement doit être conforme aux réglementations électriques locales et nationales en vigueur.

Consigne 19 – Avertissement d'alimentation TN

Cet équipement est conçu pour fonctionner avec des systèmes d'alimentation TN.

Consignes d'installation

Prenez en compte les avertissements suivants :

Consigne 1 047 – Prévention des surchauffes

Afin d'éviter toute surchauffe du système, ne l'utilisez pas dans une pièce dont la température ambiante dépasse la valeur maximale recommandée de 5 à 35 °C (41 à 95 °F).

Consigne 1 019 – Principal dispositif de déconnexion

Dans la mesure où il constitue le principal dispositif de déconnexion, l'ensemble fiche-prise doit être accessible à tout moment.

Consigne 1 005 – Disjoncteur

Un système de protection contre les risques de court-circuit (surintensité) doit être installé dans le bâtiment. Assurez-vous que la puissance nominale du

dispositif de protection n'est pas supérieure à : 120 V, 15 A (USA), 250 V, 16 A (UE).

Consigne 1 074 – Respect des réglementations électriques locales et nationales

L'installation de l'équipement doit être conforme aux réglementations électriques locales et nationales en vigueur.

Consigne 371 – Cordon d'alimentation et adaptateur CA

Lors de l'installation du produit, utilisez les câbles de connexion/cordons d'alimentation/adaptateurs CA fournis ou indiqués. L'utilisation d'un autre câble/adaptateur peut entraîner un dysfonctionnement ou un incendie. La réglementation sur les matériaux et les appareils électriques interdit l'utilisation des câbles certifiés UL (portant le sigle « UL » ou « CSA »), mais non conformes aux normes en vigueur si le sigle « PSE » n'est pas apposé sur le cordon, pour tout autre appareil électrique que les produits conçus par CISCO.

Consigne 1 073 – Aucune pièce remplaçable par l'utilisateur

Aucune pièce interne ne peut être remplacée par l'utilisateur. Ne l'ouvrez pas.

Lorsque vous installez un châssis, suivez les instructions ci-dessous :

- Assurez-vous qu'il y a suffisamment d'espace autour du châssis pour permettre les opérations de maintenance et la circulation de l'air. La circulation de l'air dans le châssis s'effectue de l'avant à l'arrière.

  Pour garantir une circulation d'air adéquate, placez vos châssis dans un rack en utilisant les kits de rails. Si vous placez physiquement les unités l'une au-dessus de l'autre ou les empilez sans utiliser les kits de rails, cela risque de bloquer les orifices de ventilation sur le dessus de chaque châssis, ce qui peut entraîner une surchauffe, et par conséquent une accélération des ventilateurs et une plus grande consommation électrique. Nous vous recommandons de monter vos châssis sur les kits de rails lorsque vous les installez dans le rack, car les kits de rails assurent l'espacement minimal nécessaire entre les châssis.

> Aucun espacement supplémentaire entre les châssis n'est requis lorsque vous les montez en utilisant les kits de rails.

- Veillez à ce que la climatisation maintienne les châssis à une température de 5 à 35 °C (41 à 95 °F).
- Assurez-vous que l'armoire ou le rack respecte les conditions relatives à l'utilisation de racks.
- Assurez-vous que l'alimentation du site respecte les conditions relatives à l'alimentation indiquées dans la notice technique de votre appliance. Le cas échéant, vous pouvez utiliser un UPS pour protéger votre installation contre les pannes de courant.

> Évitez les types de systèmes UPS qui utilisent la technologie ferrorésonante. Ces types d'UPS risquent de devenir instables avec les systèmes qui présentent d'importantes variations de consommation électrique en raison d'un trafic de données fluctuant.

Consignes de sécurité

Lisez les informations suivantes pour assurer votre sécurité et protéger le châssis. Étant donné que ces informations ne couvrent pas toutes les situations potentiellement dangereuses dans votre environnement de travail, soyez vigilant et faites preuve de bon sens en toutes circonstances.

Respectez les consignes de sécurité suivantes :

- Maintenez la zone dégagée et exempte de poussière avant, pendant et après l'installation.
- Tenez les outils à l'écart des zones de passage afin d'éviter de trébucher.
- Ne portez pas de vêtements amples ou de bijoux, notamment des boucles d'oreille, des bracelets ou des colliers susceptibles de se coincer dans le châssis.
- Portez des lunettes de sécurité si vous travaillez dans des conditions présentant un risque pour les yeux.
- Ne faites rien qui soit susceptible de présenter un danger pour autrui ou qui puisse rendre le matériel dangereux.
- Ne tentez pas de soulever seul un objet trop lourd pour une personne.

Précautions de sécurité en présence d'électricité

> ⚠ Avant de travailler sur un châssis, assurez-vous que le câble d'alimentation est débranché.

Respectez les consignes suivantes lorsque vous travaillez sur un équipement alimenté électriquement :

- Ne travaillez pas seul s'il existe des dangers potentiels sur votre lieu de travail.
- Vérifiez systématiquement que l'alimentation est déconnectée.
- Repérez les éventuels dangers présents dans votre zone de travail, tels que des sols humides, des câbles de rallonge non mis à la terre, des câbles d'alimentation endommagés et des prises de terre de sécurité manquantes.
- En cas d'accident électrique :
  - Soyez extrêmement prudent, ne devenez pas une victime vous-même.
  - Mettez le système hors tension.
  - Si possible, envoyez une autre personne demander de l'assistance médicale. Si cela s'avère impossible, évaluez l'état de la victime et demandez de l'aide.
  - Déterminez si vous devez pratiquer un bouche-à-bouche ou un massage cardiaque et donnez les soins requis.
- Utilisez le châssis conformément à ses caractéristiques électriques et respectez les instructions d'utilisation.

Éviter tout dommage par choc électrostatique

Les décharges électrostatiques se produisent en cas de manipulation incorrecte des composants électroniques. Elles peuvent endommager l'équipement et les circuits électriques, ce qui risque d'entraîner des dysfonctionnements ou une panne généralisée de votre équipement.

Suivez toujours les procédures de protection contre les décharges électrostatiques lorsque vous retirez ou remplacez des composants. Veillez à raccorder électriquement le châssis à une prise de terre. Portez un bracelet antistatique et vérifiez qu'il est bien en contact avec votre peau. Connectez la pince de mise à la terre à une surface non peinte du cadre du châssis afin de diriger en toute sécurité les tensions de décharge électrostatique vers la terre. Pour obtenir une bonne protection contre les chocs ou dommages causés par les décharges électrostatiques, vous devez vérifier que le bracelet de protection et le câble fonctionnent correctement. Si aucun bracelet de

protection n'est disponible, reliez-vous à la terre en touchant la partie en métal du châssis.

Pour des raisons de sécurité, vérifiez régulièrement la valeur de résistance du bracelet de protection, qui doit être comprise entre 1 et 10 mégohms (Mohm).

Environnement du site

Pour éviter les défaillances matérielles et réduire les risques de pannes liés aux facteurs environnementaux, planifiez soigneusement l'agencement du site et l'emplacement des équipements. Si votre équipement subit des pannes ou des erreurs graves dont la fréquence est particulièrement élevée, les observations qui suivent peuvent vous aider à isoler leur cause et à prévenir de futurs problèmes.

Considérations en matière d'alimentation électrique

Lorsque vous installez le châssis, tenez compte des points suivants :

- Vérifiez l'alimentation sur le site avant d'installer le châssis pour vous assurer qu'elle ne présente aucun pic de tension et n'émet aucun bruit. Le cas échéant, installez un conditionneur d'énergie pour garantir une tension d'alimentation et des niveaux de puissance électrique adéquats en entrée de l'appliance.
- Mettez le site à la terre afin d'éviter les dommages causés par la foudre et les surtensions.
- L'utilisateur ne peut pas sélectionner de plage de fonctionnement sur le châssis. Consultez l'étiquette sur le châssis pour connaître la puissance d'entrée de l'équipement.
- Plusieurs types de câbles d'alimentation CA sont disponibles pour l'appliance ; vérifiez que vous disposez du type adapté à votre site.
- Si vous utilisez deux modules d'alimentation redondants (1+1), nous vous recommandons d'utiliser des circuits électriques indépendants pour chacun d'eux.
- Dans la mesure du possible, installez une source d'alimentation sans interruption sur votre site.

Conditions à prendre en compte pour la configuration en rack

Tenez compte de ce qui suit pour planifier une configuration en rack :

- Si vous montez un châssis dans un rack ouvert, assurez-vous que le cadre du rack ne bloque pas les orifices d'entrée et d'évacuation d'air.
- Assurez-vous que les racks fermés disposent d'une ventilation adéquate. Veillez également à ne pas surcharger le rack, car chaque unité génère de la chaleur. Un bâti fermé doit être doté de fentes d'aérations sur les côtés et d'un ventilateur pour permettre la circulation d'air de refroidissement.
- Dans un rack fermé doté d'un ventilateur supérieur, la chaleur générée par l'équipement situé dans la partie inférieure du rack peut remonter vers les ports d'entrée de l'équipement situé juste au-dessus. Assurez-vous que la circulation d'air est suffisante dans la partie inférieure du rack.
- Des déflecteurs peuvent aider à isoler l'air évacué de l'air entrant, ce qui permet également de faire circuler l'air de refroidissement dans le châssis. Le placement idéal des déflecteurs dépend de la circulation de l'air dans le rack. Essayez différentes dispositions pour positionner correctement les déflecteurs.

Annexe B. Installation du matériel Stealthwatch

Cette section concerne l'installation des appliances dans votre environnement. Elle comprend :

- **Montage de votre appliance**
- **Connexion de votre appliance au réseau**
- **Connexion à l'appliance**
- **Définition des paramètres réseau à l'aide de l'assistant de configuration initiale**

Montage de votre appliance

Vous pouvez monter des appliances Stealthwatch directement dans une armoire ou un rack de 19 pouces standard, dans une autre armoire appropriée ou sur une surface plane. Lorsque vous installez une appliance dans une armoire ou un rack, suivez les instructions incluses dans les kits de montage de rails. Pour déterminer où placer une appliance, prévoyez suffisamment d'espace à l'avant et l'arrière de l'appliance en tenant compte de ce qui suit :

- Les indicateurs en façade doivent être clairement lisibles.
- L'accès aux ports à l'arrière est suffisant et permet d'effectuer un câblage sans restrictions.
- La prise d'alimentation du panneau arrière est à proximité d'une source d'alimentation AC conditionnée.
- L'air circule librement autour de l'appliance et à travers les orifices.

Matériel fourni avec l'appliance

Le matériel suivant est fourni avec les appliances Stealthwatch :

- Cordon d'alimentation CA
- Touches d'accès (pour la plaque de la face avant)
- Kit de rails pour le montage en rack ou étriers de montage pour les plus petites appliances
- Pour le collecteur de flux modèle 5210 un câble SFP de 10 Gbit

Matériel supplémentaire requis

Prévoyez le matériel supplémentaire suivant :

- Vis de fixation pour un rack standard de 19 pouces
- Source d'alimentation sans interruption (UPS) pour chaque appliance que vous installez
- Pour une configuration locale (facultatif), utilisez l'une des méthodes suivantes :
  - Ordinateur portable avec un câble vidéo et un câble USB (pour le clavier)
  - Moniteur vidéo avec un câble vidéo et un clavier avec un câble USB

Connexion de votre appliance au réseau

Utilisez la même procédure pour connecter chaque appliance au réseau. La connexion diffère selon le type d'appliance dont vous disposez.

> ⚠ Ne mettez pas à jour le BIOS de l'appliance, car cela pourrait entraîner un dysfonctionnement.

Pour obtenir des informations spécifiques sur chaque appliance, reportez-vous aux notices techniques Stealthwatch.

> ⓘ L'ensemble du matériel de la gamme Cisco x2xx utilise la même plateforme UCS (UCSC-C220-M5SX), à l'exception du collecteur de flux 5210 (base de données), qui utilise la plateforme UCSC-C240-M5SX. Les variations dans les appliances sont la carte réseau, le processeur, la mémoire, le stockage et le niveau RAID.

> ⓘ Le collecteur de flux 5210 se compose de deux serveurs connectés (moteur et base de données) afin qu'ils fonctionnent comme une même appliance. De ce fait, l'installation diffère légèrement d'autres appliances. Tout d'abord, connectez-les ensemble directement avec un câble d'interconnexion à attache directe SFP+ 10G. Ensuite, connectez-les à votre réseau.

Pour connecter votre appliance à votre réseau :

1. Connectez un câble Ethernet au port de gestion, à l'arrière de l'appliance.
2. Connectez au moins un port de moniteur pour les capteurs de flux et les appliances UDP Director.

   Pour la haute disponibilité des appliances UDP Director, reliez celles-ci avec des

câbles croisés. Connectez le port eth2 d'une des deux appliances UDP Director au port eth2 de la seconde appliance UDP Director. De même, connectez les ports eth3 des deux appliances UDP Director avec un second câble croisé. Il peut s'agir d'un câble fibre ou cuivre.

Tenez compte de l'étiquette Ethernet (eth2, eth3, etc.) pour chaque port. Ces étiquettes correspondent aux interfaces réseau (eth2, eth3, etc.) qui sont indiquées sur la page d'accueil de l'interface d'administration de l'appliance où vous pouvez les configurer.

3. Connectez l'autre extrémité des câbles Ethernet au commutateur de votre réseau.
4. Branchez les cordons d'alimentation au module d'alimentation. Certaines appliances ont deux connexions d'alimentation : module d'alimentation 1 et module d'alimentation 2.

Connexion à l'appliance

Cette section décrit comment vous connecter à votre appliance afin de modifier les mots de passe utilisateur par défaut.

Vous pouvez vous connecter à l'appliance de deux manières :

- avec un clavier et un moniteur
- avec un ordinateur portable (et un émulateur de terminal)

Pour les nouvelles appliances, SSH est désactivé. Vous devez vous connecter à l'interface web d'administration de l'appliance pour l'activer.

Se connecter avec un clavier et un moniteur

Pour configurer l'adresse IP localement, procédez comme suit :

1. Branchez le câble d'alimentation à l'appliance.
2. Poussez le bouton d'alimentation pour allumer l'appliance. Attendez qu'elle démarre complètement. N'interrompez pas le processus de démarrage.

> Vous devrez peut-être retirer la façade pour permettre l'alimentation.
>
> Les ventilateurs d'alimentation s'activent sur certains modèles alors que le système n'est pas sous tension. Vérifiez que le voyant sur la façade est allumé.

> Veillez à connecter l'appliance à un module d'alimentation sans interruption (UPS). Le module d'alimentation nécessite du courant, sinon le système affiche une erreur.

3. Connectez le clavier :

- Si vous disposez d'un clavier standard, branchez-le au connecteur de clavier standard.
- Si vous disposez d'un clavier USB, branchez-le à un connecteur USB.

4. Branchez le câble vidéo au connecteur vidéo. L'invite de connexion s'affiche.
5. Passez à la section, **Définition des paramètres réseau à l'aide de l'assistant de configuration initiale**.

Se connecter avec un ordinateur portable

Vous pouvez également vous connecter à l'appliance avec un ordinateur portable équipé d'un émulateur de terminal.

Pour vous connecter à une appliance avec un ordinateur portable :

1. Connectez votre ordinateur portable à l'appliance en utilisant l'une des méthodes suivantes :

- Connectez un câble RS232 du connecteur du port série (DB9) sur votre ordinateur portable au port de console sur l'appliance.
- Connectez un câble croisé du port Ethernet sur votre ordinateur portable au port de gestion sur l'appliance.

2. Branchez le câble d'alimentation à l'appliance.
3. Poussez le bouton d'alimentation pour allumer l'appliance. Attendez qu'elle démarre complètement. N'interrompez pas le processus de démarrage.

> Vous devrez peut-être retirer la façade pour permettre l'alimentation.
>
> Les ventilateurs d'alimentation s'activent sur certains modèles alors que le système n'est pas sous tension. Vérifiez que le voyant sur la façade est allumé. Veillez à connecter l'appliance à un module d'alimentation sans interruption (UPS). Le module d'alimentation nécessite du courant, sinon le système affiche une erreur.

4. Sur l'ordinateur portable, établissez une connexion à l'appliance.

   Vous pouvez utiliser tout émulateur de terminal disponible pour communiquer avec l'appliance.

5. Appliquez les paramètres suivants :

- BPS : 115200
- Bits de données : 8
- Bit d'arrêt : 1
- Parité : aucune
- Contrôle de flux : aucun

   L'écran de connexion et l'invite de connexion sont affichés.

6. Passez à la section suivante, **Définition des paramètres réseau à l'aide de l'assistant de configuration initiale**.

Définition des paramètres réseau à l'aide de l'assistant de configuration initiale

Après vous être connecté à l'appliance, utilisez l'assistant de configuration initiale pour configurer les paramètres réseau, notamment les adresses IP. Notez les éléments suivants :

- Si vous déployez un SMC 2210 ou un collecteur de flux 4210 avec un data store, vous pouvez non seulement configurer les adresses IP, mais également le SMC ou le collecteur de flux pour une utilisation avec le data store, ainsi que le type de port physique dont il se sert pour le port de gestion `eth0`.

  > ⚠ Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez pas mettre à jour la configuration de l'appliance en vue de la modifier. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option uniquement si vous prévoyez de déployer un data store sur votre réseau.

- Si votre appliance est un nœud de données, vous pouvez configurer le type de port physique qu'il utilise pour le port de gestion `eth0`, ainsi que l'adresse IP et les informations connexes pour le canal de port `eth2` ou `eth2`/`eth3` pour les communications du nœud de données.

Consultez le Guide d'installation et de configuration matérielle du cluster de data store pour en savoir plus sur l'installation des appliances SMC 2210, FC 4210 et nœuds de données.

Après avoir configuré les adresses IP et les ports, modifiez les mots de passe utilisateur.

> La première fois que vous accédez à la configuration du système, l'assistant de configuration initiale démarre et vous guide tout au long de la configuration initiale de l'appliance. Si vous quittez la configuration initiale avant la fin de l'assistant, la prochaine fois que vous accéderez à la configuration du système, l'assistant de configuration initiale s'ouvrira de nouveau.

En fonction de votre appliance, accédez à la section suivante :

- **Appliances compatibles avec le data store (SMC 2210, FC 4210)**
- **Configuration générale de l'appliance Stealthwatch**
- **Configuration du nœud de données**

Configuration générale de l'appliance Stealthwatch

Pour toutes les appliances, à l'exception des nœuds de données, de la console SMC 2210 et de la console FC 4210, la configuration initiale affiche la configuration suivante :

- Configurer l'adresse IP et les informations de gestion de l'appliance

Configurer l'adresse IP et les informations de gestion de l'appliance :

Configurez l'adresse IP de gestion eth0 de votre appliance et les informations connexes dans l'assistant de configuration initiale. Pour la plupart des appliances, il s'agit de la première configuration de l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, accédez à la section Configuration du nœud de données.
- Si vous configurez une console SMC ou un collecteur de flux compatible avec le data store, accédez à la section Appliances compatibles avec le data store (SMC 2210, FC 4210).
- Si vous configurez une autre appliance Stealthwatch, commencez par l'étape 1.

Procédure

1. Connectez-vous au programme de configuration du système :
   - Si vous configurez une appliance compatible avec un nœud de données ou un data store, saisissez `root`, puis appuyez sur la touche **Entrée**. Si vous configurez toute autre appliance, saisissez `sysadmin`, puis appuyez sur la touche **Entrée**.

     > Les autorisations `root` sont requises pour configurer correctement la compatibilité du data store et du data store.

   - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
   - À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.
2. S'il s'agit de la configuration initiale du système sur cette appliance, l'assistant de configuration initiale démarre.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Spécifiez l'**adresse IP** de cette appliance.
4. Spécifiez le **masque réseau** du réseau.
5. Saisissez une adresse de **passerelle** comme adresse IP de cette appliance.
6. Spécifiez l'adresse de **diffusion** de l'appliance.
7. Spécifiez le **nom d'hôte** de l'appliance.
8. Spécifiez le **domaine** de l'appliance.
9. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

   Il s'agit de la dernière option de configuration de l'assistant de configuration initiale. Votre appliance redémarre et les modifications sont appliquées. Une fois que c'est fait, la page de connexion s'ouvre.

Étape(s) suivante(s)

- Modifiez les mots de passe utilisateur. Reportez-vous à la section **Modification du mot de passe de l'utilisateur Sysadmin** pour en savoir plus.

Appliances compatibles avec le data store (SMC 2210, FC 4210)

Pour le SMC 2210 et le FC 4210, l'assistant de configuration initiale affiche la configuration suivante :

1. Configurer le port physique de gestion eth0
2. Configurer l'adresse IP et les informations de gestion de l'appliance
3. Configurer la compatibilité du data store

Configurer le port physique de gestion eth0

Si vous configurez une console SMC ou un collecteur de flux compatible avec un data store et déployez un data store, vous pouvez éventuellement configurer `eth0` en tant que port DAC SFP+ plutôt que le port cuivre BASE-T par défaut. Pour ces appliances, il s'agit de la première configuration de l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, ou un SMC ou un collecteur de flux compatible avec un data store, consultez la notice technique Stealthwatch de votre appliance pour obtenir des informations sur les ports SFP+ et BASE-T pris en charge.
- Si vous configurez un nœud de données, accédez à la section Configuration du nœud de données.
- Si vous configurez une autre appliance Stealthwatch outre les appliances compatibles avec un data store, reportez-vous à la section Configuration générale de l'appliance Stealthwatch.

Procédure

1. Connectez-vous au programme de configuration du système :
   - Tapez **root**, puis appuyez sur **Entrée**.

     > Les autorisations `root` sont requises pour configurer correctement la compatibilité du data store.

   - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
   - À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.
2. Si vous accédez pour la première fois à la configuration du système sur cette appliance, l'assistant de configuration initiale démarre et la configuration de l'ordre des ports s'affiche. Passez à l'étape 5.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.

3. Dans le menu de configuration du système, sélectionnez **Network** (Réseau), puis appuyez sur **Entrée**.
4. Sélectionnez **Port Order** (Ordre des ports), puis appuyez sur Entrée.
5. Les options suivantes sont disponibles :
    - Sélectionnez **LOM** pour configurer votre appliance pour qu'elle utilise un port cuivre BASE-T pour eth0.
    - Sélectionnez **SFP+** pour configurer votre appliance afin qu'elle utilise un port fibre SFP+ pour eth0.
6. Sélectionnez **OK** pour confirmer la sélection.

Étape(s) suivante(s)

- Configurez l'adresse IP et les informations de gestion du port de gestion eth0. Reportez-vous à la procédure suivante.

Configurer l'adresse IP et les informations de gestion de l'appliance :

Configurez l'adresse IP de gestion eth0 de votre appliance et les informations connexes dans l'assistant de configuration initiale. Pour les appliances compatibles avec un data store, cette configuration a lieu après la configuration du port de gestion physique eth0.

Avant de commencer

- Si vous configurez une console SMC ou un collecteur de flux compatible avec un data store, après avoir configuré l'ordre des ports, l'assistant de configuration initiale affiche la configuration de gestion `eth0`. Passez à l'étape 3.

Procédure

1. Connectez-vous au programme de configuration du système :
    - Si vous configurez une appliance compatible avec un data store, saisissez `root`, puis appuyez sur la touche **Entrée**.

      > Les autorisations `root` sont requises pour configurer correctement la compatibilité du data store et du data store.

    - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis

appuyez sur **Entrée**.

- À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.

2. S'il s'agit de la configuration initiale du système sur cette appliance, l'assistant de configuration initiale démarre.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Spécifiez l'**adresse IP** de cette appliance.
4. Spécifiez le **masque réseau** du réseau.
5. Saisissez une adresse de **passerelle** comme adresse IP de cette appliance.
6. Spécifiez l'adresse de **diffusion** de l'appliance.
7. Spécifiez le **nom d'hôte** de l'appliance.
8. Spécifiez le **domaine** de l'appliance.
9. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

Étape(s) suivante(s)

- Configurez l'appliance pour une utilisation sans data store. Reportez-vous à la procédure suivante pour plus d'informations.

Configurer l'utilisation du data store

Configurez votre console SMC 2210 ou FC 4210 pour qu'elle fonctionne avec un data store. Vos collecteurs de flux se connecteront au data store, et votre console SMC interrogera le data store.

Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez pas mettre à jour la configuration de l'appliance en vue de la modifier. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option **uniquement si** vous prévoyez de déployer un data store sur votre réseau.

Vous devez configurer tous vos SMC et collecteurs de flux pour une utilisation avec un data store si vous déployez un data store. Vous ne pouvez pas configurer certains de vos collecteurs de flux pour qu'ils se connectent au data store et d'autres pour qu'ils se connectent directement au SMC.

Avant de commencer

- Si vous vous trouvez dans l'assistant de configuration initiale, la configuration du système indique la configuration du data store une fois terminée la configuration de l'adresse IP de l'appliance. Passez à l'étape 3.

Procédure

1. Dans le menu de configuration du système. Sélectionnez **Advanced** (Avancé), puis appuyez sur **Entrée**.
2. Sélectionnez **Data Store**, puis appuyez sur Entrée.
3. Sélectionnez **Yes** (Oui) pour configurer la compatibilité de votre appliance avec un data store.

   > ⚠ Après avoir choisi de configurer votre SMC ou collecteur de flux pour une utilisation avec un data store, vous ne pouvez pas mettre à jour la configuration de l'appliance en vue de la modifier. Vous devez rétablir les paramètres par défaut de l'appliance si vous effectuez le mauvais choix. Activez cette option **uniquement si** vous prévoyez de déployer un data store sur votre réseau.

4. Sélectionnez **OK** pour confirmer la sélection.

   Il s'agit de la dernière option de configuration de l'assistant de configuration initiale. Votre appliance redémarre et les modifications sont appliquées. Une fois que c'est fait, la page de connexion s'ouvre.

Étape(s) suivante(s)

- Modifiez les mots de passe utilisateur. Reportez-vous à la section **Modification du mot de passe de l'utilisateur Sysadmin** pour en savoir plus.

Configuration du nœud de données

Pour les nœuds de données, l'assistant de configuration initiale affiche la configuration suivante :

1. Configurer le port physique de gestion eth0
2. Configurer l'adresse IP et les informations de gestion de l'appliance
3. Configurer eth2 et eth3 pour les communications entre les nœuds de données

Configurer le port physique de gestion eth0

Si vous configurez un nœud de données, vous pouvez éventuellement configurer `eth0` en tant que port cuivre BASE-T plutôt que le port DAC SFP+ par défaut. Pour ces appliances, il s'agit de la première configuration de l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, consultez la fiche technique Stealthwatch de votre appliance pour obtenir des informations sur les ports SFP+ et BASE-T pris en charge.
- Si vous configurez une console SMC ou un collecteur de flux compatible avec le data store, accédez à la section Appliances compatibles avec le data store (SMC 2210, FC 4210).
- Si vous configurez une autre appliance Stealthwatch outre les appliances compatibles avec un data store, reportez-vous à la section Configuration générale de l'appliance Stealthwatch.

Procédure

1. Connectez-vous au programme de configuration du système :
   - Tapez **root**, puis appuyez sur **Entrée**.

     > Les autorisations `root` sont requises pour configurer correctement la compatibilité du data store.

   - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
   - À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.
2. Si vous accédez pour la première fois à la configuration du système sur cette appliance, l'assistant de configuration initiale démarre et la configuration de l'ordre des ports s'affiche. Passez à l'étape 5.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Dans le menu de configuration du système, sélectionnez **Network** (Réseau), puis appuyez sur **Entrée**.
4. Sélectionnez **Port Order** (Ordre des ports), puis appuyez sur Entrée.
5. Les options suivantes sont disponibles :

- Sélectionnez **SFP+** pour configurer votre appliance afin qu'elle utilise un port fibre SFP+ pour eth0.
- Sélectionnez **LOM** pour configurer votre appliance pour qu'elle utilise un port cuivre BASE-T pour eth0.

6. Sélectionnez **OK** pour confirmer la sélection.

Étape(s) suivante(s)

- Configurez l'adresse IP et les informations de gestion du port de gestion eth0. Reportez-vous à la procédure suivante.

Configurer l'adresse IP et les informations de gestion de l'appliance :

Configurez l'adresse IP de gestion eth0 de votre appliance et les informations connexes dans l'assistant de configuration initiale.

Avant de commencer

- Si vous configurez un nœud de données, après avoir configuré l'ordre des ports, l'assistant de configuration initiale affiche la configuration de gestion `eth0`. Passez à l'étape 3.

Procédure

1. Connectez-vous au programme de configuration du système :
   - Si vous configurez un nœud de données, saisissez `root`, puis appuyez sur la touche **Entrée**.

     > Les autorisations `root` sont requises pour configurer correctement la compatibilité du data store et du data store.

   - Dans l'invite de mot de passe qui s'affiche, saisissez **lan1cope**, puis appuyez sur **Entrée**.
   - À l'invite suivante, saisissez **SystemConfig**, puis appuyez sur **Entrée**.
2. S'il s'agit de la configuration initiale du système sur cette appliance, l'assistant de configuration initiale démarre.

   Sinon, le menu de configuration du système s'ouvre. Sélectionnez **Management** (Gestion), puis appuyez sur **Entrée**.
3. Spécifiez l'**adresse IP** de cette appliance.

4. Spécifiez le **masque réseau** du réseau.
5. Saisissez une adresse de **passerelle** comme adresse IP de cette appliance.
6. Spécifiez l'adresse de **diffusion** de l'appliance.
7. Spécifiez le **nom d'hôte** de l'appliance.
8. Spécifiez le **domaine** de l'appliance.
9. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

Étape(s) suivante(s)

- Configurez les informations de gestion des ports de communication du nœud de données. Reportez-vous à la section **Configurer eth2 et eth3 pour les communications entre les nœuds de données :** pour en savoir plus.

Configurer eth2 et eth3 pour les communications entre les nœuds de données :

Lors de la configuration d'une appliance nœud de données, configurez le port de communication entre les nœuds de données avec une adresse IP non routable. Vous pouvez configurer l'une des options suivantes :

- `eth2`
- canal de port contenant `eth2` et `eth3`

> Vous devez attribuer des adresses IP non routables à partir du bloc CIDR `169.254.42.0/24`.

Avant de commencer

- Consultez la notice technique Stealthwatch de votre appliance pour plus d'informations sur les ports SFP+ `eth2` et `eth3`. Notez que `eth2` et `eth3` dépendent de la configuration de `eth0`.
- Si vous vous trouvez dans l'assistant de configuration initiale, la configuration du système affiche la configuration du canal de port `eth2` ou `eth2/eth3` une fois que vous avez terminé de configurer les informations de gestion `eth0` de l'appliance. Passez à l'étape 3.

Procédure

1. Dans le menu de configuration du système, sélectionnez **Network** (Réseau), puis appuyez sur **Entrée**.
2. Sélectionnez **Node Communications** (Communications du nœud), puis appuyez sur Entrée.
3. Sélectionnez la configuration du port de communication entre les nœuds de données. Les options suivantes sont disponibles :
   - Sélectionnez **Yes** (Oui) pour ajouter `eth2` et `eth3` en tant que canal de port pour les communications entre les nœuds de données.
   - Sélectionnez **No** (Non) pour utiliser `eth2` pour les communications entre les nœuds de données.
4. Saisissez une **adresse IP** non routable à partir du bloc CIDR `169.254.42.0/24` pour `eth2` ou le canal de port `eth2/eth3`.
5. Spécifiez un **masque réseau** de `255.255.255.0` pour cette adresse IP.
6. Saisissez une adresse de **passerelle** pour cette adresse IP.
7. Saisissez une adresse de **diffusion** pour cette adresse IP.
8. Cliquez sur **Select** (Sélectionner), puis sur **Yes** (Oui) pour valider vos saisies.

   Il s'agit de la dernière option de configuration de l'assistant de configuration initiale. Votre appliance redémarre et les modifications sont appliquées. Une fois que c'est fait, la page de connexion s'ouvre.

Étape(s) suivante(s)

- Modifiez les mots de passe utilisateur. Reportez-vous à la section **Modification du mot de passe de l'utilisateur Sysadmin** pour en savoir plus.

Modification du mot de passe de l'utilisateur Sysadmin

Pour que votre réseau soit sécurisé, modifiez le mot de passe sysadmin par défaut pour les appliances.

Modifier le mot de passe sysadmin :

Avant de commencer

- Connectez-vous à la console de l'appliance en tant que **sysadmin**.
- Accédez à la configuration du système.

Procédure

1. Dans le menu de configuration du système, sélectionnez **Password** (Mot de passe), puis appuyez sur **Entrée**.

   Si vous modifiez la liste des hôtes approuvés par défaut, veillez à ce que chaque appliance Stealthwatch dans votre déploiement soit incluse dans cette liste. Si ce n'est pas le cas, les appliances ne seront pas en mesure de communiquer entre elles.

   Une invite pour le mot de passe actuel s'affiche sous le menu.
2. Saisissez le mot de passe actuel et appuyez sur **Entrée**.

   L'invite pour un nouveau mot de passe s'affiche.
3. Saisissez le nouveau mot de passe et appuyez sur **Entrée**.

   Le mot de passe doit comporter entre 8 et 30 caractères alphanumériques sans espaces. Vous pouvez également utiliser les caractères spéciaux suivants : `$.~!@#%_=?:,{}()`
4. Saisissez de nouveau le mot de passe et appuyez sur **Entrée**.
5. Lorsque votre mot de passe est accepté, appuyez de nouveau sur **Entrée** pour revenir au menu de configuration du système.
6. Passez à la section suivante, **Modification du mot de passe de l'utilisateur root**.

Modification du mot de passe de l'utilisateur root

Après avoir modifié le mot de passe par défaut de l'utilisateur sysadmin, vous devez modifier le mot de passe de l'utilisateur root par défaut pour renforcer la sécurité de votre réseau.

Modifier le mot de passe de l'utilisateur root :

Avant de commencer

- Connectez-vous à la console de l'appliance en tant que **sysadmin**.
- Accédez à la configuration du système.

Procédure

1. Accédez au shell root.
2. Dans le menu Configuration du système, sélectionnez **Advanced** (Avancé), puis appuyez sur **Entrée**. Le menu Advanced s'affiche.

3. Sélectionnez **RootShell**, puis appuyez sur **Entrée**.

   Une invite de mot de passe pour l'utilisateur root s'affiche.

4. Saisissez le mot de passe de l'utilisateur root actuel et appuyez sur **Entrée**. L'invite du shell root s'affiche.
5. Saisissez **SystemConfig**, puis appuyez sur **Entrée**.

   Vous retournez au menu de configuration du système pour modifier le mot de passe de l'utilisateur root.

6. Sélectionnez **Password** (Mot de passe), puis appuyez sur **Entrée**. L'invite du mot de passe s'affiche sous le menu.
7. Saisissez le nouveau mot de passe de l'utilisateur root et appuyez sur **Entrée**. Une deuxième invite s'affiche.
8. Saisissez à nouveau le nouveau mot de passe de l'utilisateur root et appuyez sur **Entrée**.
9. Une fois que votre mot de passe est modifié, appuyez sur **Entrée**. Vous avez désormais modifié les mots de passe sysadmin et root par défaut. Vous retournez au menu de la console de configuration du système.
10. Cliquez sur **Cancel** (Annuler), puis appuyez sur **Entrée**. La console de configuration du système se ferme et l'invite du shell root s'affiche.
11. Saisissez **exit** et appuyez sur **Entrée**. L'invite de connexion s'affiche.
12. Appuyez sur **Ctrl + Alt** pour quitter l'environnement de la console.

Vous êtes maintenant prêt à configurer votre appliance. Pour configurer votre appliance, reportez-vous au **Guide de configuration Stealthwatch** correspondant à votre version logicielle. L'appliance x2xx est compatible avec les versions logicielles Stealthwatch 7.x.

Annexe C. Configuration de vos appliances

La première fois que vous vous connectez à l'appliance, vous utilisez l'outil de configuration de l'appliance pour configurer les paramètres.

Configuration requise pour l'outil de configuration de l'appliance

- Vérifiez que vos pare-feu et listes de contrôle d'accès autorisent l'accès.
- Collectez le nom d'hôte de l'appliance et les adresses IP des composants suivants :
    - appliance
    - masque de sous-réseau
    - passerelles par défaut et de diffusion
    - serveurs NTP et DNS
    - adresse IP de la console SMC pour Central Management

Gestion

Dans le cadre de l'outil de configuration de l'appliance, vous allez configurer votre appliance pour qu'elle soit gérée par votre console de gestion Stealthwatch (SMC) principale.

Lorsque vos appliances sont gérées par votre console SMC, vous pouvez utiliser Central Management pour modifier les configurations des appliances, mettre à jour le logiciel, redémarrer les appliances, les arrêter, etc.

Basculement SMC

Si vous disposez de plusieurs consoles de gestion Stealthwatch (SMC), vous pouvez configurer une paire de basculement SMC de sorte que l'une des consoles serve de console de sauvegarde à l'autre.

- Utilisez l'outil de configuration de l'appliance pour configurer chaque console SMC individuelle.
- Prévoyez à l'avance quelle sera votre console SMC principale et votre console SMC secondaire.

- Après avoir configuré chaque console SMC, vous utiliserez le magasin de confiance de Central Management et le client de bureau Stealthwatch pour configurer la relation du basculement SMC.

Bonnes pratiques

Pour configurer correctement votre système, suivez les instructions de ce guide.

Nous vous recommandons de procéder comme suit :

- **Une par une :** configurez une appliance à la fois. Vérifiez que l'appliance est **active** avant de configurer l'appliance suivante dans votre cluster.
- **Ordre :** suivez l'ordre de configuration.
- **Plusieurs gestionnaires centralisés :** vous pouvez configurer plusieurs gestionnaires centralisés dans votre système. Cependant, chaque appliance peut être gérée par une seule console SMC/un seul gestionnaire centralisé.
- **Accès :** vous devez disposer de privilèges d'administrateur pour accéder à Central Management.

Ordre de configuration

Configurez vos appliances dans l'ordre suivant et notez les informations relatives à chaque appliance :

Commande	Appliance	Détails
1.	Console SMC principale	Votre console SMC principale correspond à votre gestionnaire centralisé. Assurez-vous que la console SMC est active avant de commencer à configurer l'appliance suivante dans le système.
2.	Solutions UDP Director (également appelées FlowReplicators)	
3.	Nœuds de données	
4.	Base de données du	Assurez-vous que la base de

	collecteur de flux 5000	données du collecteur de flux 5000 est active avant de démarrer la configuration du moteur.
5.	Moteur du collecteur de flux 5000	Assurez-vous que la base de données du collecteur de flux 5000 est active avant de démarrer la configuration du moteur.
6.	Tous les autres collecteurs de flux (NetFlow et sFlow)	
7.	Capteurs de flux	Assurez-vous que votre collecteur de flux est actif avant de commencer la configuration du capteur de flux.
8.	Concentrateur de terminaux	
9.	Console SMC secondaire (si elle est présente)	Assurez-vous que la console SMC principale est active avant de démarrer la configuration de la console SMC secondaire. La console SMC secondaire est automatiquement sélectionnée comme gestionnaire centralisé. Configurez le basculement une fois toutes les appliances configurées.

Il est possible que votre système ne dispose pas de toutes les appliances indiquées ici.

1. Se connecter

Procédez comme suit pour configurer chaque appliance à l'aide de l'outil de configuration de l'appliance.

1. Dans le champ d'adresse de votre navigateur, saisissez **https://** suivi de l'adresse IP de l'appliance.

- **Console SMC principale :** configurez tout d'abord la console SMC principale.
- **Active :** vérifiez que chaque appliance est active avant de configurer l'appliance suivante dans votre cluster.
- **Ordre :** veillez à configurer vos appliances dans l'ordre afin qu'elles communiquent correctement.

2. Saisissez les informations d'identification suivantes pour vous connecter :

   - **Nom d'utilisateur :** admin
   - **Mot de passe :** lan411cope

2. Configurer l'appliance

La première fois que vous vous connectez à l'appliance, l'outil de configuration de l'appliance vous guide au cours de chaque étape de configuration.

1. **Modifier le mot de passe par défaut :** saisissez de nouveaux mots de passe pour les utilisateurs suivants : admin, root et sysadmin. Cliquez sur **Suivant** pour accéder à chaque utilisateur.

   Utilisez les critères suivants :

   - **Longueur :** de 8 à 30 caractères
   - **Modification :** assurez-vous que le nouveau mot de passe diffère du mot de passe par défaut d'au moins 4 caractères.

Utilisateur	Mot de passe par défaut
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

Les menus sysadmin et root ne sont pas disponibles si vous avez déjà modifié les mots de passe par défaut lors de l'installation du matériel. Reportez-vous au Guide d'installation matérielle des appliances Stealthwatch x210 pour en savoir plus.

2. **Interface réseau de gestion :** vérifiez les champs de l'adresse IP et de l'interface réseau. Vérifiez que les paramètres par défaut sont corrects. Cliquez sur **Suivant**.

    - **Modifications :** pour modifier ces informations, consultez votre administrateur réseau et reportez-vous à la section Résolution des problèmes.
    - **IPv6 (facultatif) :** pour activer le paramètre IPv6, cliquez sur **IPv6**. Cochez la case **Activer IPv6** et renseignez les champs.

3. **Nom d'hôte et domaines :** saisissez le nom d'hôte et le nom de domaine du réseau. Cliquez sur **Suivant**.

    - **Nom d'hôte :** un nom d'hôte unique est requis pour chaque appliance. Si vous attribuez les mêmes noms d'hôte à vos appliances, celles-ci ne seront pas installées correctement.
    - **Domaine réseau :** un nom de domaine complet est requis pour chaque appliance.
    - **Domaine Stealthwatch (SMC uniquement) :** saisissez un domaine Stealthwatch pour vos appliances Stealthwatch.
    - **Plages d'adresses IP (SMC uniquement) :** sélectionnez la plage d'adresses IP de votre réseau Stealthwatch.

4. **Paramètres DNS :** vérifiez que la valeur par défaut est correcte ou saisissez l'adresse IP de votre serveur de domaine. Cliquez sur **Suivant**.

    Ajouter ou supprimer des serveurs DNS (facultatif) :

    - **Ajouter :** cliquez sur l'icône +.
    - **Supprimer :** cochez cette case pour sélectionner le serveur DNS. Cliquez sur l'icône -.

5. **Paramètres NTP :** vérifiez que la valeur par défaut est correcte ou cliquez sur l'icône **Menu** pour sélectionner votre serveur NTP (Network Time Protocol). Cliquez sur **Suivant**.

    - **Plusieurs serveurs NTP :** nous vous recommandons de configurer plusieurs serveurs NTP pour assurer la redondance et la précision.

- **Source publique :** pool.ntp.org est une source publique adéquate pour NTP.

Ajouter ou supprimer des serveurs NTP (facultatif) :

- **Ajouter :** cliquez sur l'icône +.
- **Supprimer :** cochez cette case pour sélectionner le serveur NTP. Cliquez sur l'icône –.

6. Si l'appliance est une console SMC, passez à l'étape **3. Enregistrer la console de gestion Stealthwatch**.

   Si l'appliance n'est pas une console SMC, passez à l'étape **4. Ajouter des appliances à Central Management**.

3. Enregistrer la console de gestion Stealthwatch

1. **Vérifier vos paramètres :** vérifiez que les informations de l'appliance sont exactes.
2. Cliquez sur **Appliquer** ou sur **Redémarrer et continuer**.

   Suivez les instructions à l'écran pendant le redémarrage de l'appliance.

   Attendez quelques minutes que les nouveaux paramètres système prennent effet. Il est possible que vous deviez actualiser la page.

3. Connectez-vous à la console de gestion Stealthwatch.
4. L'outil de configuration de l'appliance s'ouvre à nouveau. Cliquez sur **Continuer**.
5. Sous l'onglet Enregistrer votre appliance, vérifiez l'adresse IP et cliquez sur **Enregistrer**.

   - Central Management est installé sur la console de gestion Stealthwatch.
   - L'adresse IP de la console SMC est automatiquement détectée et il est impossible de la modifier.

6. Une fois la configuration de l'appliance terminée, cliquez sur **Accéder au tableau de bord**.
7. Cliquez sur l'icône **Paramètres généraux**. Sélectionnez **Central Management**.

8. Vérifiez l'inventaire. Vérifiez que l'appliance SMC est **active**.

> ⚠ Assurez-vous que la console SMC principale et que chaque appliance sont actives avant de commencer à configurer l'appliance suivante dans votre cluster en vous reportant à la rubrique concernant l'ordre et les détails de configuration.

9. Déployez et configurez votre data store. Revenez à la rubrique Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.

4. Ajouter des appliances à Central Management

L'outil de configuration de l'appliance continue de vous guider au cours de la configuration de l'appliance avec Central Management. Certaines étapes peuvent varier en fonction de l'appliance. Suivez les invites affichées à l'écran.

1. Sous l'onglet Central Management, saisissez l'adresse IP de votre console SMC principale.

   Votre console SMC principale correspond à votre gestionnaire centralisé.

2. Cliquez sur **Enregistrer**.
3. Suivez les instructions à l'écran pour approuver le certificat d'identité de l'appliance SMC principale. Cliquez sur **Oui** pour approuver le certificat et autoriser l'appliance à communiquer avec la console SMC.
4. Saisissez les informations d'identification de votre console SMC principale.
5. Sélectionnez votre domaine Stealthwatch.

   - **Collecteurs de flux :** saisissez le numéro de port de collecte de flux.

     Netflow par défaut : 2055

     sFlow par défaut : 6343

   - **Capteurs de flux :** sélectionnez un collecteur de flux.

6. Cliquez sur **Accéder à Central Management**. Passez à l'étape **5. Confirmer l'état de l'appliance**.

5. Confirmer l'état de l'appliance

Après avoir configuré une appliance dans l'outil de configuration de l'appliance, confirmez l'état de l'appliance dans Central Management.

1. L'outil de configuration de l'appliance s'ouvre dans l'inventaire Central Management ; si ce n'est pas le cas, vous pouvez l'ouvrir comme suit :

   - Connectez-vous à votre console de gestion Stealthwatch principale.
   - Cliquez sur l'icône **Paramètres généraux**.
   - Sélectionnez **Central Management**.

2. Examinez les appliances dans l'inventaire du gestionnaire d'appliances.

   - Vérifiez que l'appliance figure dans l'inventaire.
   - Vérifiez que l'appliance est active.

> ⚠ Assurez-vous que la console SMC principale et que chaque appliance sont actives avant de commencer à configurer l'appliance suivante dans votre cluster en vous reportant à la rubrique concernant l'ordre et les détails de configuration.

3. Pour configurer l'appliance suivante dans votre système, accédez à l'étape **1. Se connecter** et suivez la procédure décrite jusqu'à l'étape **5. Confirmer l'état de l'appliance**.

   Si vous n'avez pas d'autre appliance à configurer, consultez le Guide de configuration du système Stealthwatch pour en savoir plus sur la configuration des appliances. Vous pouvez également revenir à l'étape Présentation du déploiement du data store Stealthwatch pour passer en revue le processus de déploiement.

Informations de copyright