# Cisco Secure Network Analytics

Guide d'installation matérielle des appliances x2xx 7.4.2

# Sommaire

# Introduction

## Présentation

Ce guide explique comment installer les appliances matérielles Cisco Secure Network Analytics (anciennement Stealthwatch) x2xx. Ce guide explique également comment monter et installer le matériel Secure Network Analytics.

> ⚠ Lisez le document Informations relatives à la réglementation, à la conformité et à la sécurité avant d'installer les appliances Secure Network Analytics x2xx.

Le matériel des appliances x2xx inclut :

| **Appliance** | **Référence** |
|---|---|
| Gestionnaire 2210<br>(anciennement Console de gestion Stealthwatch) | ST-SMC2210-K9 |
| Data store 6200 (trois nœuds de données) | ST-DS6200-K9<br>(trois ST-DNODE-G1) |
| Collecteur de flux 4210 | ST-FC4210-K9 |
| Collecteur de flux 5210 - Moteur | ST-FC5210-E |
| Collecteur de flux 5210 - Base de données | ST-FC5210-D |
| UDP Director 2210 | ST-UDP2210-K9 |
| Capteur de flux 1210 | ST-FS1210-K9 |
| Capteur de flux 3210 | ST-FS3210-K9 |
| Capteur de flux 4240 | ST-FS4240-K9 |

## Public

Ce guide est destiné au technicien chargé de l'installation du matériel Secure Network Analytics. Nous supposons que vous disposez déjà des connaissances générales nécessaires pour installer l'équipement réseau.

Si vous préférez faire appel à un installateur professionnel, contactez votre partenaire Cisco local ou le service d'assistance Cisco.

## Installation des appliances et configuration de votre système

Prenez note du flux d'installation et de configuration global de Secure Network Analytics.

1. **Installer les appliances :** installez vos appliances matérielles (physiques) Secure Network Analytics x2xx à l'aide de ce guide d'installation. Pour installer des appliances Édition virtuelle, suivez les instructions du Guide d'installation de l'appliance Édition virtuelle.
2. **Configurer Secure Network Analytics :** après avoir installé les appliances matérielles et virtuelles, vous êtes prêt à configurer Secure Network Analytics dans un système géré. Suivez les instructions du Guide de configuration de Secure Network Analytics v7.4.2.

## Informations connexes

Pour en savoir plus sur Secure Network Analytics, consultez les ressources en ligne suivantes :

- **Informations relatives à la réglementation, à la conformité et à la sécurité :** lisez le document Informations relatives à la réglementation, à la conformité et à la sécurité avant d'installer les appliances Secure Network Analytics x2xx.
- **Présentation :** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Guide de conception du data store :** https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **Matrice de prise en charge des versions matérielles et logicielles :** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **Caractéristiques de l'appliance :** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

## Terminologie

Ce guide utilise le terme « **appliance** » pour tous les produits Secure Network Analytics.

Un « **cluster** » est votre groupe d'appliances Secure Network Analytics gérées par le Gestionnaire.

## Abréviations courantes

Les abréviations suivantes peuvent apparaître dans ce guide :

| Abréviation | Description |
|---|---|
| DMZ | Zone démilitarisée (un réseau de périmètre) |
| HTTPS | Protocole HTTPS (Hypertext Transfer Protocol Secure) |
| ISE | Cisco ISE (Identity Services Engine) |
| NIC | Carte réseau |
| NTP | Protocole Network Time (NTP) |
| PCIe | Standard Peripheral Component Interconnect Express |
| SNMP | Protocole SNMP (Simple Network Management Protocol) |
| Classes SPAN | Analyseur de port commuté |
| TAP | Port d'accès de test |
| UPS | Onduleur |
| VLAN | Réseau local virtuel |

# À propos des appliances Secure Network Analytics

Secure Network Analytics comporte plusieurs appliances matérielles qui recueillent, analysent et présentent des informations sur votre réseau pour améliorer ses performances et sa sécurité. Cette section décrit chaque appliance Secure Network Analytics  x2xx.

## Gestionnaire  2210

Le Gestionnaire gère, coordonne, configure et organise les différents composants du système. Le logiciel Secure Network Analytics vous permet d'accéder à l'interface utilisateur web de la console depuis un ordinateur muni d'un navigateur web. Vous pouvez facilement accéder en temps réel aux informations de sécurité et de réseau concernant les segments essentiels de votre entreprise. Indépendant de toute plateforme grâce à Java, le Gestionnaire permet ce qui suit :

- Gestion, configuration et création de rapports centralisées pour 25 collecteurs de flux Secure Network Analytics
- Création de graphiques pour visualiser le trafic
- Analyse approfondie pour le dépannage
- Rapports consolidés et personnalisables
- Analyse des tendances
- Surveillance des performances
- Notification immédiate des failles de sécurité

Si vous déployez un data store, vous pouvez configurer un Gestionnaire  2210  avec une interface DAC SFP+ 10 Gbit/s sur eth0 pour un débit accru. Si vous ne déployez pas de data store, vous pouvez uniquement configurer l'interface 1 Gbit/s-10 Gbit/s sur eth0.

## Data store 6200

Le data store fournit un référentiel central pour stocker les données de télémétrie de votre réseau récoltées par vos collecteurs de flux. 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. Comme toutes vos données se trouvent dans une base de données centralisée au lieu d'être réparties sur plusieurs collecteurs de flux, votre Gestionnaire peut récupérer les résultats de la requête auprès du data store plus rapidement que s'il interrogeait tous vos collecteurs de flux

séparément. Le cluster du data store offre une meilleure tolérance aux pannes, une réponse améliorée aux requêtes et un remplissage plus rapide des graphiques.

Pour plus d'informations, reportez-vous à **Secure Network Analytics avec data store**.

## Collecteurs de flux 4210 et 5210

Le collecteur de flux collecte des données NetFlow, cFlow, J-Flow, Packeteer 2, NetStream et IPFIX pour assurer la protection du réseau basée sur le comportement.

Le collecteur de flux regroupe les données sur les comportements de plusieurs réseaux ou segments de réseau haut débit pour garantir une protection complète et améliorer les performances sur l'ensemble des réseaux répartis dans différentes zones géographiques.

Si vous déployez un data store, vous pouvez configurer un collecteur de flux 4210 avec une interface DAC  SFP+ 10 Gbit/s  sur eth0 pour un débit accru. Si vous ne déployez pas de data store, vous pouvez uniquement configurer l'interface cuivre 100 Mbit/s-1 Gbit/s-10 Gbit/s sur eth0.

> À partir des données qu'il reçoit, le collecteur de flux identifie les attaques connues ou inconnues, les utilisations frauduleuses internes et les périphériques réseau mal configurés, quel que soit le chiffrement ou la fragmentation des paquets. Dès que Secure Network Analytics identifie un comportement suspect, le système exécute l'action que vous avez configurée, le cas échéant, pour ce type de comportement.

## UDP Director 2210

L'appliance UDP Director est un réplicateur de paquets UDP haut débit ultraperformant. L'appliance UDP Director est très utile, car elle envoie les déroutements NetFlow, sFlow, syslog ou SNMP (Simple Network Management Protocol) à divers collecteurs. Elle reçoit des données des applications UDP hors connexion, puis les retransmet à plusieurs destinataires en dupliquant les données le cas échéant.

Lorsque vous utilisez la configuration UDP Director haute disponibilité (HA), veillez à connecter deux appliances UDP Director avec des câbles croisés. Pour obtenir des instructions, reportez-vous à la section **2. Connexion de votre appliance au réseau**.

## Capteurs de flux 1210, 3210 et 4240

Le capteur de flux est une appliance réseau qui fonctionne de la même manière qu'une appliance de capture de paquets classique ou qu'un IDS du fait qu'il se branche à un port SPAN (switch port analyzer), à un port miroir ou à un port TAP Ethernet. Le capteur de flux augmente la visibilité sur les zones de réseau suivantes :

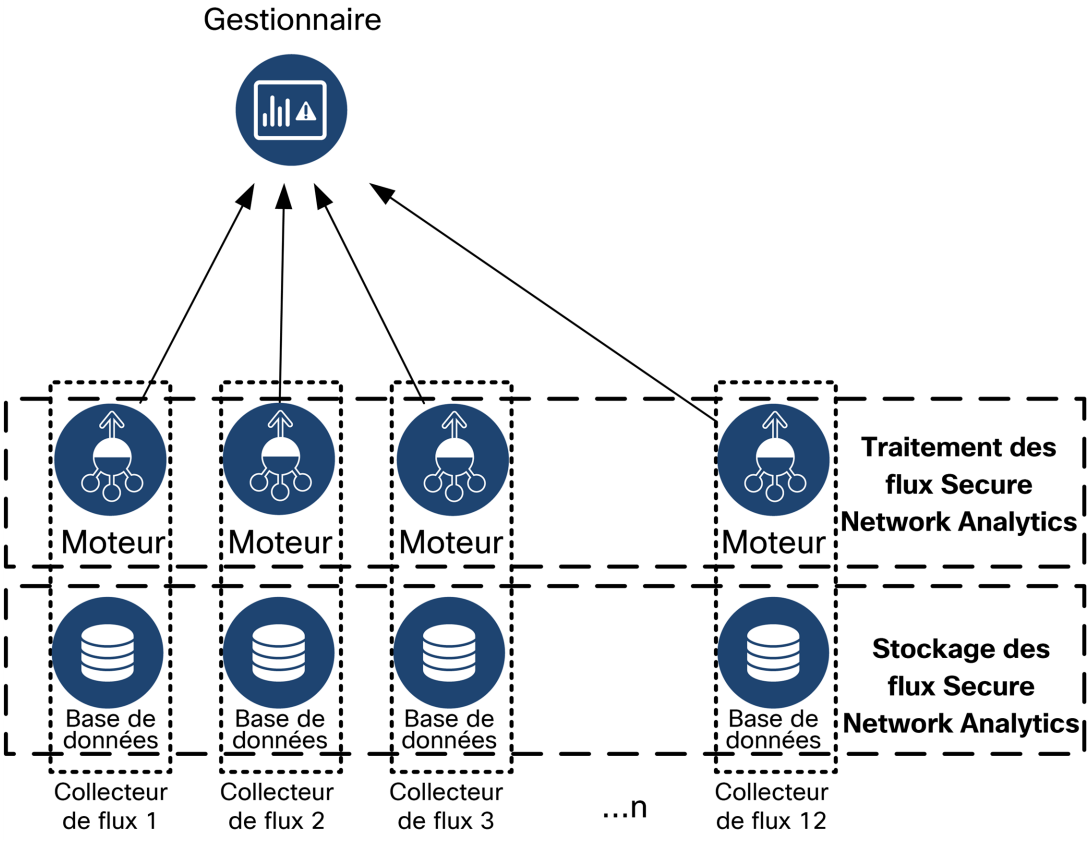
- Où NetFlow n'est pas disponible.
- Où NetFlow est disponible, mais vous voulez une meilleure visibilité sur les indicateurs de performance et les données des paquets.

En orientant le capteur de flux vers un collecteur de flux NetFlow v9, vous pouvez obtenir des statistiques détaillées et utiles sur le trafic à partir de NetFlow. Associé au collecteur de flux Secure Network Analytics, le capteur de flux fournit également des informations détaillées sur les indicateurs de performance et de comportement. Les indicateurs de performance, quant à eux, donnent des informations sur la latence aller-retour introduite par le réseau ou par l'application côté serveur.

Étant donné que le capteur de flux bénéficie d'une visibilité sur les paquets, il peut calculer le délai de retransmission (RTT), le délai de réponse du serveur (SRT) et la perte de paquets pour les sessions TCP. Il inclut tous les champs supplémentaires dans les enregistrements NetFlow qu'il envoie au collecteur de flux.

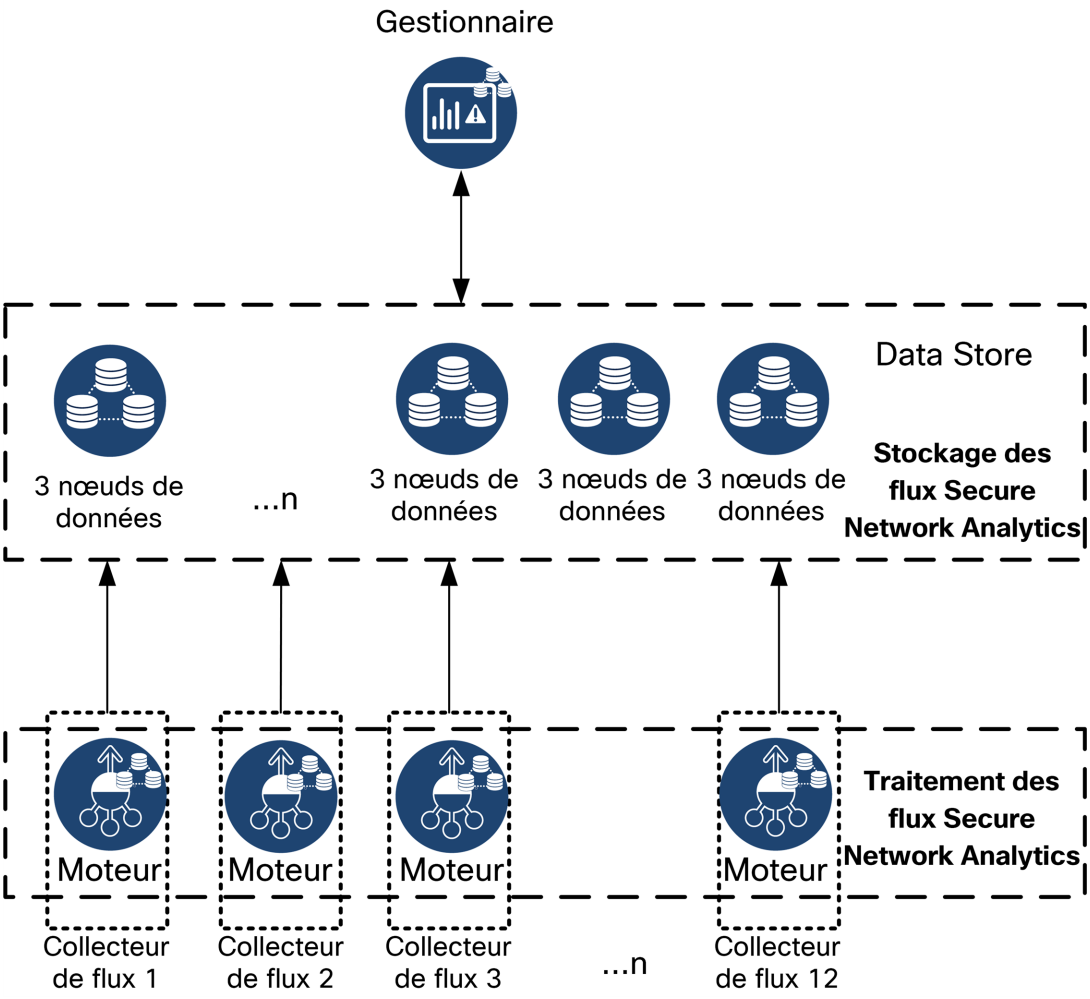
# Secure Network Analytics sans data store

Dans un déploiement Secure Network Analytics sans data store, un ou plusieurs collecteurs de flux intègrent et dédupliquent les données, effectuent des analyses, et transmettent les données et les résultats directement au Gestionnaire. Pour résoudre les requêtes envoyées par l'utilisateur, y compris les graphiques et les diagrammes, le Gestionnaire interroge tous les collecteurs de flux gérés. Chaque collecteur de flux renvoie les résultats correspondants au Gestionnaire. Le Gestionnaire collecte les informations des différents jeux de résultats, puis génère un graphique ou un tableau 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.



# Secure Network Analytics avec data store

Dans un déploiement Secure Network Analytics avec un data store, le cluster du data store se trouve entre votre Gestionnaire 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 répartissant de manière à peu près égale entre tous les 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.




Le data store fournit un référentiel central pour stocker les données de télémétrie de votre réseau récoltées par vos collecteurs de flux. 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. Comme toutes vos données se

trouvent dans une base de données centralisée au lieu d'être réparties sur plusieurs collecteurs de flux, votre Gestionnaire peut récupérer les résultats de la requête auprès du data store plus rapidement que s'il interrogeait tous vos collecteurs de flux séparément. Le cluster du data store offre une meilleure tolérance aux pannes, une réponse améliorée aux requêtes et un remplissage plus rapide des graphiques.

## Requêtes

Pour résoudre les requêtes envoyées par l'utilisateur, notamment les graphiques et les tableaux, le Gestionnaire 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 au Gestionnaire. Le Gestionnaire génère le graphique ou le tableau 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.

## Stockage et tolérance aux pannes du data store

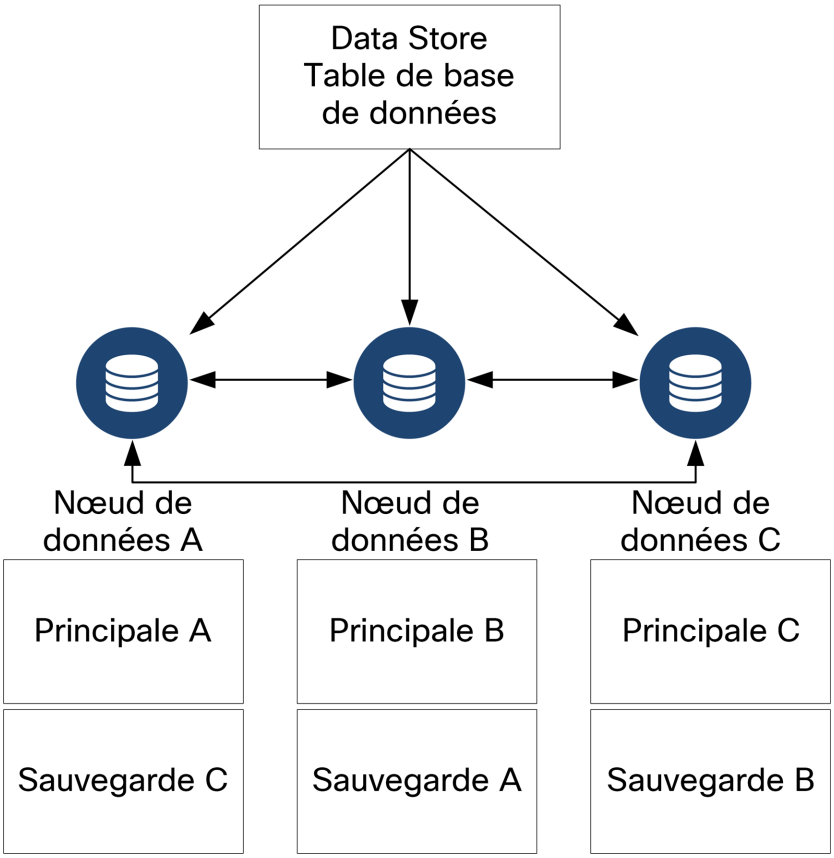
Le data store collecte des données auprès des collecteurs de flux et les distribue de façon équitable sur les nœuds de données dans le cluster. Chaque nœud de données, en plus de stocker une partie de votre télémétrie globale, stocke également une sauvegarde de la télémétrie d'un autre nœud de données. 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 votre data store possède 3 nœuds de données ou plus et qu'un nœud de données tombe en panne, tant que le nœud de données 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.

## Exemple de stockage de télémétrie

Reportez-vous au schéma suivant pour savoir comment ces trois nœuds de données stockent la télémétrie :



# Configuration générale requise pour un déploiement

Avant de démarrer, consultez ce guide pour comprendre le processus ainsi que la préparation, le temps et les ressources dont vous aurez besoin pour planifier l'installation.

## Matrice des versions matérielles et logicielles

Reportez-vous à la section Matrice des versions matérielles et logicielles pour plus d'informations sur la compatibilité. La matrice est disponible à l'adresse https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html.

## Caractéristiques techniques

Téléchargez la fiche technique de chaque appliance que vous prévoyez d'installer. Les caractéristiques techniques sont disponibles à l'adresse https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.

## Cisco Integrated Management Controller (CIMC)

Après avoir installé vos appliances, veillez à configurer Cisco Integrated Management Controller (CIMC) pour permettre l'accès à la configuration du serveur et à une console de serveur virtuel. Vous pouvez également utiliser CIMC pour surveiller l'intégrité du matériel.

- **Instructions :** reportez-vous à la section **Se connecter avec CIMC (requis pour l'accès à distance)** et suivez les instructions du Guide de configuration de l'interface utilisateur de Cisco Integrated Management Controller UCS C-Series.
- **Mot de passe par défaut :** dans le cadre de la configuration initiale, vous devez vous connecter à CIMC en tant qu'administrateur et saisir **password** dans le champ du mot de passe.
- **Critères de sécurité obligatoires du mot de passe :** une fois connecté, modifiez le mot de passe par défaut pour protéger la sécurité de votre réseau.

## Configuration requise pour les appliances standard (sans data store)

Si vous installez Secure Network Analytics sans data store, installez les appliances suivantes :

| Appliance | Besoin |
|---|---|
| Gestionnaire | • Minimum 1 Gestionnaire |
| Collecteur de flux | • 1 collecteur de flux minimum |
| Capteur de flux | En option |
| UDP Director | En option |

Pour connaître la configuration requise pour l'installation de Secure Network Analytics avec un data store, reportez-vous à la section **Configuration requise pour le déploiement du data store**.

## Configuration requise pour le déploiement du gestionnaire et du collecteur de flux

Pour chaque Gestionnaire et collecteur de flux que vous déployez, affectez une adresse IP routable au port de gestion `eth0`.

# Configuration requise pour le déploiement du data store

Pour déployer Secure Network Analytics avec un data store, passez en revue la configuration requise et les recommandations suivantes pour votre déploiement.

## Configuration requise pour l'appliance (avec data store)

Le tableau suivant présente les appliances requises pour déployer Secure Network Analytics avec un data store.

| Appliance | Besoin |
|---|---|
| Gestionnaire | • Minimum 1 Gestionnaire |
| Data store | • 1 ou 3 nœuds de données minimum<br>• Jeux supplémentaires de 3 nœuds de données pour étendre le data store, avec un maximum 36 nœuds de données<br>• Le déploiement de 2 nœuds de données seulement dans un cluster n'est pas pris en charge. |
| Collecteur de flux | • 1 collecteur de flux minimum |
| UDP Director | En option |
| Capteur de flux | En option |

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

## Configuration requise pour le déploiement du gestionnaire et du collecteur de flux

Pour chaque Gestionnaire et collecteur de flux que vous déployez, affectez une adresse IP routable au port de gestion `eth0`.

- **Configuration du port eth0 :** 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`

du Gestionnaire et du collecteur de flux.

- **Débit :** vous obtenez un débit de 10G pour le port cuivre BASE-T pour utiliser le data store. Si vous ne déployez pas de data store, vous pouvez uniquement configurer l'interface cuivre 100 Mbit/s, 1 Gbit/s, 10 Gbit/s sur `eth0`.

## Configuration requise pour le déploiement du nœud de données

Chaque data store comprend des nœuds de données.

- **Matériel :** chaque nœud de données matériel possède son propre châssis. Lorsque vous achetez un data store matériel, vous recevez plusieurs châssis matériels de nœud 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 nœud de données.
- **Édition virtuelle** : lorsque vous téléchargez un data store virtuel, vous pouvez déployer 1 ou 3 nœuds de données (ou plus, par lots de 3).

> Assurez-vous que vos nœuds de données sont tous des nœuds matériels ou virtuels. La combinaison de nœuds de données virtuels et matériels n'est pas prise en charge, et le matériel doit appartenir à la même génération matérielle (tous des DS 6200 ou des DN 6300).

### Déploiement de plusieurs nœuds de données

Un déploiement de plusieurs nœuds de données offre des performances maximales. Par exemple, un data store 6200 avec 3 nœuds de données peut gérer environ 1 million de flux par seconde et conserver ces données pendant environ 90 jours.

Notez les éléments suivants :

- **Ensembles de trois :** il est possible de mettre en cluster les nœuds de données dans votre data store par ensembles de 3, de 3 minimum à 36 maximum. Le déploiement de 2 nœuds de données seulement dans un cluster n'est pas pris en charge.
- **Tous matériels ou Tous virtuels** : assurez-vous que vos nœuds de données sont tous des nœuds matériels ou tous des nœuds virtuels. La combinaison de nœuds de données matériels et virtuels, ou la combinaison de nœuds de données du data store 6200 et du data store 6300, ne sont pas prises en charge.

### Déploiement d'un seul nœud de données

Si vous choisissez de déployer un seul (1) nœud de données :

- **Collecteurs de flux** : un maximum de 4 Collecteur de flux collecteurs de flux sont pris en charge.
- **Ajout de nœuds de données :** si vous déployez un seul nœud de données, vous pouvez ajouter des nœuds de données à votre déploiement ultérieurement. Reportez-vous à la section **Déploiement de plusieurs nœuds de données** pour plus d'informations.

> 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 le service d'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 le service d'assistance Cisco pour obtenir de l'aide.

## Configuration requise du nœud de données

Pour déployer un data store, attribuez les éléments suivants à chaque nœud de données. Les informations que vous préparez seront configurées lors de la première installation à l'aide du Guide de configuration du système.

- **Adresse IP routable (eth0) :** pour la gestion, l'intégration et l'interrogation des communications avec vos appliances Secure Network Analytics.
- **Configuration du port eth0 :** vous pouvez configurer l'utilisation d'un port cuivre **BASE-T** 1G/10G ou d'un port câble Twinax SFP+ 10G pour le port de gestion `eth0`.
- **Débit :** vous obtenez un débit de 10G pour le port cuivre BASE-T pour utiliser le data store.
- **Communications entre les nœuds de données :** configurez une adresse IP non routable à partir du bloc CIDR `169.254.42.0/24` dans un LAN ou un VLAN privé à utiliser pour la communication entre les nœuds de données.

  Pour optimiser le débit, connectez le port `eth2` du nœud de données (ou le canal de port contenant `eth2` et `eth3`) aux commutateurs pour la communication entre les

nœuds de données. Dans le cadre du data store, vos nœuds de données communiquent entre eux.

- **Connexions réseau :** vous devez disposer de deux connexions réseau 10G, une pour les communications de gestion, d'intégration et d'interrogation, une autre pour les communications entre les nœuds de données.
- **Connexion et commutateur supplémentaires :** éventuellement, uniquement pour les nœuds de données matériels, pour assurer la redondance du réseau et la criticité des communications entre les nœuds de données, installez une connexion 10G supplémentaire et un commutateur supplémentaire pour établir un canal de port sur le nœud de données.

> Configurez vos nœuds 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.

## Considérations relatives aux réseaux et à la commutation

Le tableau suivant fournit un aperçu des considérations relatives aux réseaux et à la commutation pour le déploiement de Secure Network Analytics avec un data store.

| Considérations relatives au réseau | Description |
|---|---|
| Communications entre les nœuds de données | • Spécifiez une latence RTT (durée aller-retour) recommandée inférieure à 200 microsecondes entre les nœuds de données.<br>• Conservez une distorsion d'horloge de 1 seconde ou moins entre vos nœuds de données.<br>• Spécifiez un débit recommandé de 6,4 Gbit/s ou supérieur (connexion commutée duplex intégral de 10 Gbit/s) entre vos nœuds de données.<br>• La configuration d'un port `eth2` pour le débit 10G est suffisante pour une communication normale entre les nœuds de données matériels. La création d'un canal de port LACP `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 dans le data store, car chaque nouveau nœud de données reçoit le trafic des nœuds adjacents afin d'alimenter ses données. Notez que la liaison de port LACP est la seule option de liaison disponible pour les nœuds de données matériels. |
| Alimentation matérielle du nœud de données | • 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.<br>• Lorsque vous initialisez le cluster de data store, 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 ont besoin de 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.<br>• Nous vous recommandons 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. |
| Secure Network Analytics Communications de l'appliance | • Gestionnaire et les collecteurs de flux doivent pouvoir accéder à tous les nœuds de données.<br>• Les nœuds de données doivent pouvoir accéder au Gestionnaire, à tous les collecteurs de flux et à chaque nœud de données. |

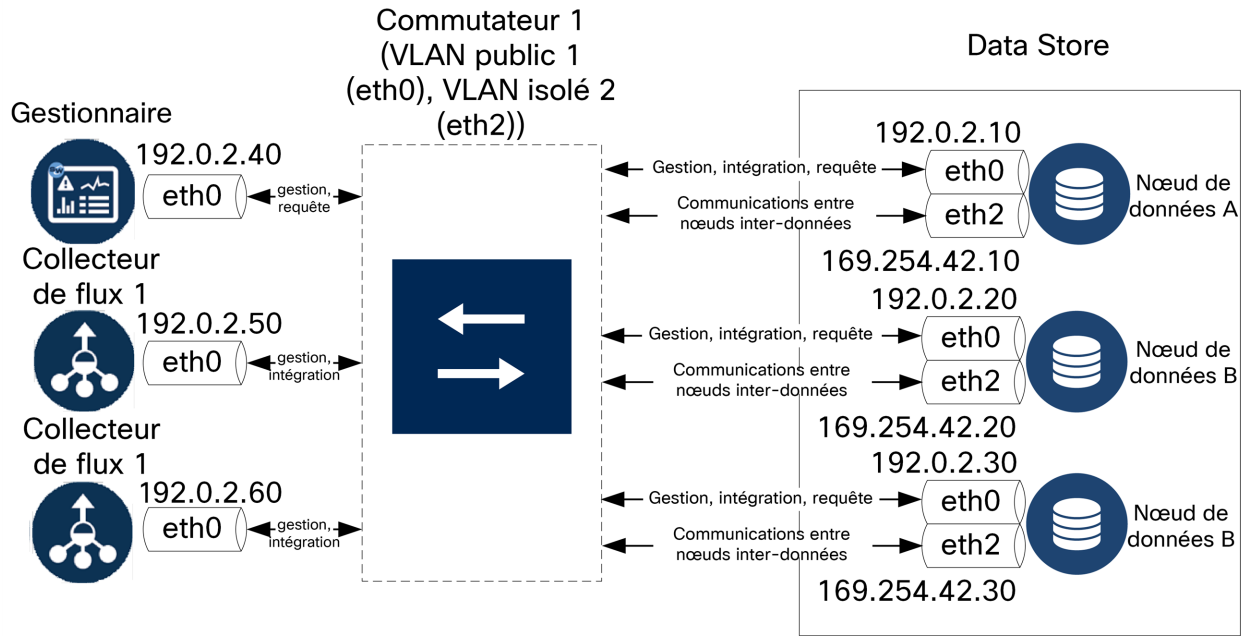
> À l'heure actuelle, le data store ne prend pas en charge le déploiement de nœuds de données de rechange dans le cadre de remplacements automatiques en cas de panne d'un nœud de données principal. Contactez le service d'assistance Cisco pour obtenir de l'aide.

## Exemple de commutateur matériel

Pour activer les communications entre les nœuds de données via `eth2` ou le canal de port `eth2/eth3`, déployez 1 commutateur prenant en charge les débits 10G.

Configurez un LAN ou un VLAN public pour les communications `eth0` des nœuds de données avec le Gestionnaire et les collecteurs de flux, et un LAN ou un VLAN isolé pour les communications entre les nœuds de données.

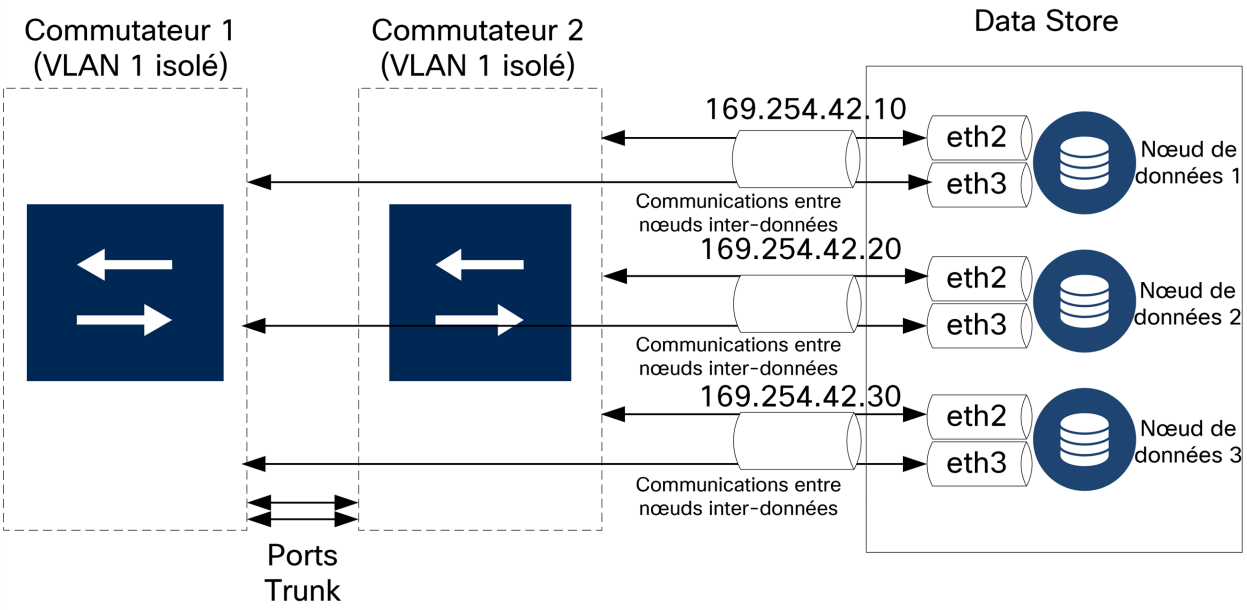
Vous pouvez partager ces commutateurs avec d'autres appliances, mais créer des LAN ou des VLAN distincts pour le trafic supplémentaire de l'appliance. Reportez-vous au schéma suivant pour obtenir un exemple :




Le cluster de data store nécessite une pulsation continue entre les nœuds sur le 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, veillez à 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.

## Considérations relatives au positionnement du data store

Positionnez chaque nœud de données de façon à ce qu'il puisse communiquer avec tous vos collecteurs de flux, votre Gestionnaire 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 le Gestionnaire pour optimiser les performances des requêtes.

- **Pare-feu :** nous vous recommandons vivement de placer les nœuds de données dans votre pare-feu, par exemple dans un centre d'exploitation du réseau.
- **Alimentation :** 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. Installez vos nœuds de données de sorte à assurer une disponibilité constante.

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 risque de ne pas redémarrer automatiquement. Consultez le Guide de configuration du système pour le dépannage et le redémarrage manuel de la base de données.

- **Politique :** vérifiez que la politique de restauration de l'alimentation du nœud de données matériel 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.

## Exigences en termes de déploiement d'outils d'analyse

Secure Network Analytics utilise la modélisation dynamique des entités pour suivre l'état de votre réseau. Dans le contexte de Secure Network Analytics, une entité est un élément qui peut être suivi sur le long cours, comme un hôte ou un terminal sur votre réseau. La modélisation dynamique collecte des informations sur les entités en fonction du trafic qu'elles transmettent et des activités qu'elles effectuent sur votre réseau. Pour en savoir plus, reportez-vous au guide Analyses : détections, alertes et observations.

Pour activer l'outil d'analyse, votre déploiement doit être configuré

- sur un déploiement de data store virtuel ou matériel avec un nombre illimité de collecteurs de flux.
- avec un seul domaine de data store Secure Network Analytics.

# 1. Configurer votre pare-feu pour les communications

Pour que les appliances puissent communiquer correctement, vous devez configurer le réseau de façon à ce que les pare-feu ou les listes de contrôle d'accès ne bloquent pas les connexions nécessaires. Utilisez les informations présentées dans cette section pour configurer votre réseau de façon à ce que les appliances puissent communiquer sur celui-ci.

## Ports ouverts (toutes les appliances)

Vérifiez auprès de votre administrateur réseau que les ports suivants sont ouverts et ont un accès illimité sur vos appliances (Gestionnaires, Collecteurs de flux, Nœuds de données, Capteurs de flux et UDP Director) :

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 8910
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

## Ports ouverts supplémentaires pour les nœuds de données

En outre, si vous déployez des nœuds de données sur votre réseau, assurez-vous que les ports suivants sont ouverts et ont un accès illimité :

- TCP 5433
- TCP 5444

- TCP 9450

## Ports et protocoles de communication

Le tableau suivant montre comment les ports sont utilisés dans Secure Network Analytics :

| De (client) | À (serveur) | Port | Protocole |
|---|---|---|---|
| Ordinateur de l'utilisateur admin | Tous les appareils | TCP/443 | HTTPS |
| Tous les appareils | Source d'heure réseau | UDP/123 | NTP |
| Active Directory | Gestionnaire | TCP/389, UDP/389 | LDAP |
| Cisco ISE | Gestionnaire | TCP/443 | HTTPS |
| Cisco ISE | Gestionnaire | TCP/8910 | XMPP |
| Sources de journalisation externes | Gestionnaire | UDP/514 | SYSLOG |
| Collecteur de flux | Gestionnaire | TCP/443 | HTTPS |
| UDP Director | Gestionnaire | TCP/443 | HTTPS |
| UDP Director | Collecteur de flux (sFlow) | UDP/6343* | sFlow |
| UDP Director | Collecteur de flux (NetFlow) | UDP/2055* | NetFlow |
| UDP Director | Systèmes de gestion d'événements tiers | UDP/514 | SYSLOG |
| Capteur de flux | Gestionnaire | TCP/443 | HTTPS |
| Capteur de flux | Collecteur de flux (NetFlow) | UDP/2055 | NetFlow |
| Exportateurs NetFlow | Collecteur de flux (NetFlow) | UDP/2055* | NetFlow |
| Exportateurs sFlow | Collecteur de flux (sFlow) | UDP/6343* | sFlow |

| De (client) | À (serveur) | Port | Protocole |
|---|---|---|---|
| Gestionnaire | UDP Director | TCP/443 | HTTPS |
| Gestionnaire | Cisco ISE | TCP/443 | HTTPS |
| Gestionnaire | Cisco ISE | TCP/8910 | XMPP |
| Gestionnaire | DNS | UDP/53 | DNS |
| Gestionnaire | Collecteur de flux | TCP/443 | HTTPS |
| Gestionnaire | Capteur de flux | TCP/443 | HTTPS |
| Gestionnaire | Exportateurs de flux | UDP/161 | SNMP |
| Gestionnaire | LDAP | TCP/636 | TLS |
| Gestionnaire | Points de distribution des CRL | TCP/80 | HTTP |
| Gestionnaire | Répondeurs OCSP | TCP/80 | OCSP |
| PC utilisateur | Gestionnaire | TCP/443 | HTTPS |

*C'est le port par défaut, mais tout port UDP peut être configuré sur l'exportateur.

## Ports ouverts supplémentaires pour le data store

La liste suivante répertorie les ports de communication à ouvrir sur votre pare-feu pour déployer le data store.

| N° | De (client) | À (serveur) | Port | Protocole ou objectif |
|---|---|---|---|---|
| 1 | Gestionnaire | Collecteurs de flux et nœuds de données | 22/TCP | SSH, requis pour initialiser la base de données du data store |
| 1 | Nœuds de données | Tous les autres nœuds de données | 22/TCP | SSH, requis pour initialiser la base de données du data store et pour exécuter les tâches d'administration de la base de données |
| 2 | Gestionnaire, collecteurs de flux et nœuds de données | Serveur NTP | 123/UDP | NTP, requis pour la synchronisation de l'heure |
| 2 | Serveur NTP | Gestionnaire, collecteurs de flux et nœuds de données | 123/UDP | NTP, requis pour la synchronisation de l'heure |
| 3 | Gestionnaire | Collecteurs de flux et nœuds de données | 443/TCP | HTTPS, requis pour sécuriser les communications entre les appliances |
| 3 | Collecteurs de flux | Gestionnaire | 443/TCP | HTTPS, requis pour sécuriser les communications entre les appliances |
| 3 | Nœuds de données | Gestionnaire | 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 nœuds de données | 4803/TCP | Service de messagerie inter-nœuds de données |
| 6 | Nœud de données | Tous les autres nœuds de données | 4803/UDP | Service de messagerie inter-nœuds de données |
| 7 | Nœuds de données | Tous les autres nœuds de données | 4804/UDP | Service de messagerie inter-nœuds de données |
| 8 | Gestionnaire, collecteurs de flux et nœuds de données | Nœuds de données | 5433/TCP | Connexions client Vertica |
| 9 | Nœud de données | Tous les autres nœuds de données | 5433/UDP | Surveillance du service de messagerie Vertica |
| 10 | Exportateurs sFlow | Collecteur de flux (sFlow) | 6343/UDP | Intégration sFlow |
| 11 | Nœuds de données | Tous les autres nœuds de données | 6543/UDP | Service de messagerie inter-nœuds de données |

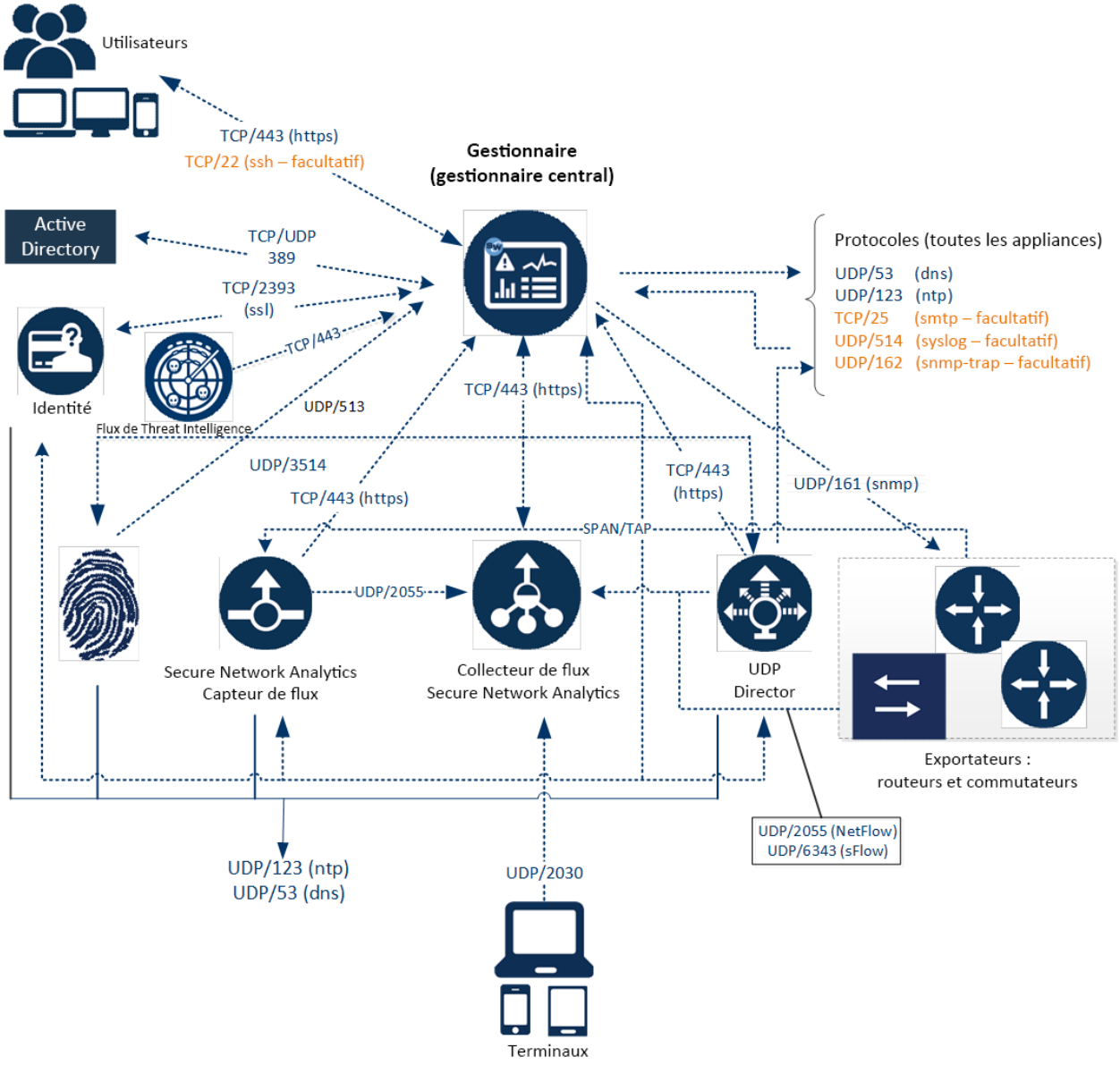
## Ports de communication facultatifs

Le tableau suivant concerne les configurations facultatives en fonction des besoins de votre réseau :

| De (client) | À (serveur) | Port | Protocole |
|---|---|---|---|
| Tous les appareils | PC utilisateur | TCP/22 | SSH |
| Gestionnaire | Systèmes de gestion d'événements tiers | UDP/162 | SNMP-trap |
| Gestionnaire | Systèmes de gestion d'événements tiers | UDP/514 | SYSLOG |
| Gestionnaire | Passerelle de messagerie | TCP/25 | SMTP |
| Gestionnaire | Flux de Threat Intelligence | TCP/443 | SSL |
| PC utilisateur | Tous les appareils | TCP/22 | SSH |

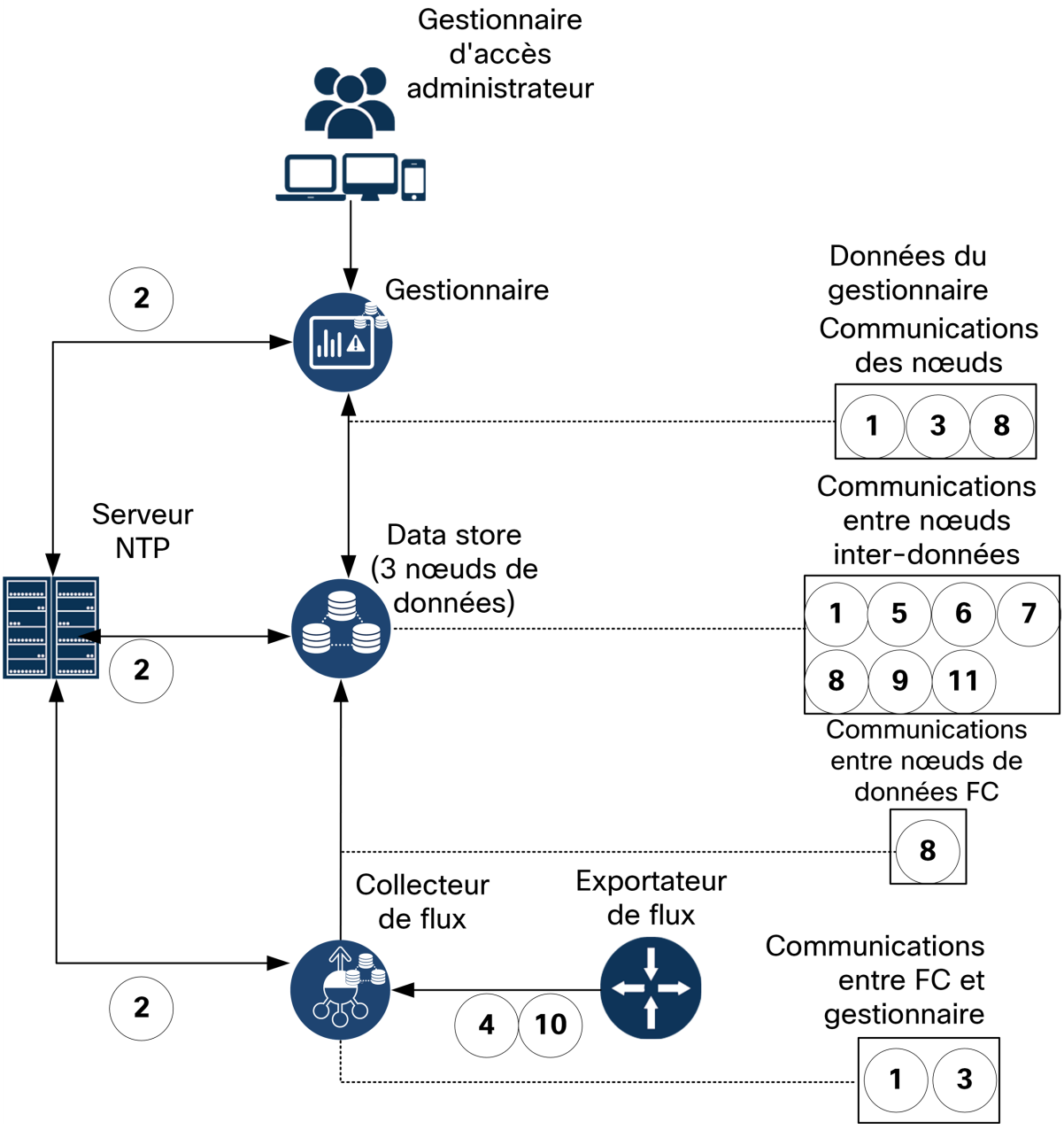
# Secure Network Analytics Exemple de déploiement

Le diagramme suivant montre les diverses connexions utilisées par Secure Network Analytics. Certains de ces ports sont facultatifs.



## Secure Network Analytics Exemple de déploiement avec data store

Comme le montre la figure ci-dessous, vous pouvez déployer stratégiquement des appliances Secure Network Analytics pour assurer une couverture optimale des segments clés du réseau, dans le réseau interne, au niveau du périmètre ou dans la DMZ.



# 2. Avertissements et consignes d'installation

## Avertissements d'installation

Lisez le document Informations relatives à la réglementation, à la conformité et à la sécurité avant d'installer les appliances Secure Network Analytics x2xx.

Prenez en compte les avertissements suivants :

Consigne 1071 : définition du symbole « Attention »

CONSIGNES DE SÉCURITÉ IMPORTANTES

Ce symbole indique un risque de 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 cet appareil.

CONSERVEZ CES INSTRUCTIONS.

Consigne 1004 : consignes d'installation

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

Consigne 1005 : disjoncteur

Un système de protection contre les risques de court-circuit (surintensité) doit être installé dans le bâtiment.

Consigne 1006 : consigne de sécurité relative au châssis pendant le montage en rack et les tâches de maintenance

Pour prévenir les blessures corporelles lors de la fixation ou des opérations de maintenance du produit dans le rack, prenez les mesures qui s'imposent pour garantir la stabilité du système. Les consignes suivantes sont fournies dans le but d'assurer votre sécurité :
- Cette unité doit être fixée au fond du rack s'il s'agit de la seule unité du rack.
- Lorsque vous fixez cette unité dans un rack partiellement rempli, allez du bas

vers le haut et veillez à placer les composants les plus lourds dans la partie inférieure du rack.

⚠ • Lorsque vous fixez cette unité dans un rack partiellement rempli, allez du bas vers le haut et veillez à placer les composants les plus lourds dans la partie inférieure du rack.

Consigne 1015 : manipulation de la batterie

Pour réduire les risques d'incendie, d'explosion ou de fuite de liquide ou de gaz inflammable :

• Remplacer la batterie que par une batterie de même type ou d'un type équivalent recommandé par le fabricant.

⚠ • Ne pas démonter, écraser, percer ou utiliser un outil pointu pour enlever ou court-circuiter les contacts externes, et ne pas jeter la batterie au feu.

• Ne pas utiliser si la batterie est déformée ou gonflée.

• Ne pas stocker ni utiliser la batterie à une température supérieure à 60 °C (140 °F).

• Ne pas stocker ni utiliser la batterie si la pression atmosphérique est inférieure à 69,7 kPa.

Consigne 1017 : zone d'accès limité

⚠ Cet équipement a été conçu pour être installé dans des endroits dont l'accès est contrôlé. Seul le personnel qualifié, formé ou compétent peut accéder aux zones dont l'accès est contrôlé.

Consigne 191 : mise en garde relative à la classe A du Voluntary Control Council for Interference (VCCI) pour le Japon

⚠ Ce produit appartient à la classe A selon la norme définie par le VCCI Council. L'utilisation de l'équipement dans un environnement domestique peut entraîner des perturbations radioélectriques, auquel cas vous devrez éventuellement prendre des mesures adéquates.

Consigne 164 : soulever les composants

⚠ Il faut deux personnes pour soulever les éléments lourds du produit. Pour éviter de vous blesser, gardez le dos droit et soulevez en poussant sur vos jambes. Ne faites pas reposer tout le poids du châssis sur votre dos.

Consigne 256 : consigne de sécurité relative aux appareils de classe A (Hongrie)

Cet équipement est un produit de classe A. Il doit être utilisé et installé correctement et conformément aux exigences de classe A de la norme CEM en Hongrie (MSZEN55022). L'équipement de classe A est conçu pour des établissements commerciaux types pour lesquels des conditions spéciales d'installation et de distance de protection s'appliquent.

Consigne 294 : consigne de sécurité relative aux appareils de classe A (Corée)

Il s'agit d'un équipement de classe A conforme aux exigences de compatibilité électromagnétique (CEM) relatives à une utilisation industrielle. L'acheteur et le vendeur doivent avoir connaissance de ce fait. Si ce type d'appareil a été vendu ou acheté par erreur, il doit être remplacé par un appareil à usage résidentiel.

Consigne 340 : consigne de sécurité relative à la classe A pour CISPR22/EN55022/CISPR32/EN55032

Il s'agit d'un produit de classe A. Dans un environnement domestique, ce produit peut entraîner des perturbations radioélectriques, auquel cas vous devrez éventuellement prendre des mesures adéquates.

Consigne 1021 : 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 1024 : conducteur de mise à la terre

Cet équipement doit être mis 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 1028 : plusieurs modules d'alimentation

Cette unité peut présenter plus d'un connecteur de module d'alimentation. Afin de réduire le risque de choc électrique, débranchez tous les câbles pour mettre l'unité hors tension.

Consigne 1029 : plaques vierges et capots

Les plaques vierges et les capots du châssis remplissent trois fonctions importantes : ils réduisent le risque de choc électrique et d'incendie ; ils aident à contenir les interférences électromagnétiques qui pourraient perturber d'autres équipements ; enfin, ils dirigent le flux d'air de refroidissement dans le châssis. Avant d'utiliser le système, vérifiez que toutes les cartes, toutes les plaques et tous les capots avant et arrière sont en place.

Consigne 1030 : installation des équipements

Seul le personnel spécialisé et qualifié est habilité à effectuer l'installation, le remplacement et l'entretien de cet équipement.

Consigne 1032 : soulever le châssis

Pour éviter de vous blesser et d'endommager le châssis, n'essayez pas de soulever ni d'incliner le châssis à l'aide des poignées des modules (tels que les blocs d'alimentation, les ventilateurs et les cartes). Ces types de poignées ne sont pas conçus pour supporter le poids de l'unité.

Consigne 9001 : mise au rebut du produit

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

Consigne 1051 : rayonnement laser

Une fois débranchés, les câbles à fibre optique et certains connecteurs sont susceptibles d'émettre un rayonnement laser invisible. Ne regardez pas les faisceaux à l'œil nu ni à l'aide d'instruments optiques.

Consigne 1055 : laser de classe 1/1M

Présence de radiations laser invisibles. Ne pas exposer les utilisateurs de composants optiques télescopiques. Cette consigne s'applique aux produits laser de classe 1/1M.

Consigne 1008 : produit laser de classe 1

Il s'agit d'un produit laser de classe 1.

Consigne 1056 : câble de fibre optique sans terminaison

Des radiations laser invisibles peuvent être générées à l'extrémité d'un câble de fibre optique ou d'un connecteur sans terminaison. Ne regardez pas directement à l'aide d'instruments d'optique. Si vous regardez un laser à l'aide de certains instruments d'optique (par exemple une loupe ou un microscope) à une distance de 100 mm ou moins, vous risquez des dommages oculaires.

| Type de fibre et diamètre de cœur (µm) | Longueur d'onde (nm) | Puissance maximale (mW) | Divergence de faisceau (rad) |
|---|---|---|---|
| SM 11 | 1200–1400 | 39–50 | 0,1–0,11 |
| MM 62,5 | 1200–1400 | 150 | 0,18 NA |
| MM 50 | 1200–1400 | 135 | 0,17 NA |
| SM 11 | 1400–1600 | 112–145 | 0,11–0,13 |

Consigne 1089 : définitions de personne formée et personne qualifiée

Une personne formée est une personne qui a suivi une formation dispensée par une personne qualifiée et qui prend les précautions nécessaires lors de l'utilisation de l'équipement.

Une personne qualifiée/compétente est une personne qui dispose d'une formation ou d'une expérience relative à la technologie de l'équipement, et qui comprend les risques potentiels lorsqu'elle travaille avec l'équipement concerné.

Consigne 1090 : installation par une personne formée

Seule une personne qualifiée est habilitée à effectuer l'installation, le remplacement et l'entretien de cet équipement. Reportez-vous à la consigne 1 089 pour connaître la définition d'une personne qualifiée.

Consigne 1091 : installation par une personne formée

Seule une personne formée ou qualifiée est habilitée à effectuer l'installation, le remplacement et l'entretien de cet équipement. Reportez-vous à la consigne 1089 pour connaître la définition d'une personne qualifiée ou compétente.

Consigne 1074 : conformité aux codes de réglementation électrique régionaux et nationaux

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

Consigne 2017 : avis relatif aux appareils de classe A (FCC)

Toute modification de l'équipement sans l'autorisation de Cisco peut entraîner sa non-conformité aux exigences de la FCC concernant les appareils numériques de classe A. Le cas échéant, vos droits d'utilisation de l'équipement seront susceptibles d'être limités par les règlements de la FCC et vous pourrez être amené à remédier, à vos frais, aux éventuelles interférences avec des dispositifs radiophoniques ou télévisuels.
Cet équipement a été testé et jugé conforme aux limites imposées pour un périphérique numérique de classe A en vertu de la partie 15 des règlements de

la FCC. Ces limites ont pour but de fournir une protection raisonnable contre les interférences nuisibles susceptibles de se produire lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radioélectrique. S'il n'est pas installé ni utilisé conformément au manuel d'instructions, il peut provoquer des interférences nuisibles aux communications radio. L'utilisation de cet équipement en zone résidentielle est susceptible de causer des interférences, auquel cas les utilisateurs devront corriger ces interférences à leurs propres frais.

Consigne 2021 : avis relatif aux appareils de classe A (Canada)

Cet appareil numérique de classe A est conforme à la norme ICES-003/NMB-003 du Canada.

Consigne 7001 : protection contre les chocs électrostatiques

Cet équipement peut être sensible aux décharges électrostatiques. Avant d'intervenir sur l'équipement, portez systématiquement un bracelet antistatique au poignet ou à la cheville et vérifiez qu'il est suffisamment en contact avec la peau. Raccordez l'extrémité du bracelet antistatique à une surface non peinte du châssis de l'équipement ou à la prise antistatique, si l'équipement en est pourvu.

Consigne 7003 : exigences relatives à la résistance à la foudre à l'intérieur des bâtiments pour les câbles blindés

Les ports intrabâtiments de l'équipement ou du sous-ensemble doivent utiliser des câbles ou des fils intérieurs blindés reliés à la terre aux deux extrémités. Sur cet équipement, les ports suivants sont considérés comme des ports intrabâtiments :

Consigne 7005 : surtension et coupure de courant dans les bâtiments

Les ports intrabâtiments de l'équipement ou du sous-ensemble sont uniquement adaptés aux connexions dont le câblage est installé à l'intérieur d'un bâtiment ou dont le câblage est non exposé. Les ports intrabâtiments de l'équipement ou du sous-ensemble ne doivent PAS entrer en contact avec des pièces métalliques des interfaces connectées au réseau extérieur ni à son câblage sur plus de 6 mètres (environ 20 pieds). Ces interfaces ne doivent être utilisées qu'à l'intérieur (ports de type 2, de type 4 ou de type 4a tels que décrits dans GR-

1089) et doivent être isolées du câblage exposé du réseau extérieur. L'ajout de dispositifs de protection primaires n'offre pas de protection suffisante lorsque ces interfaces sont reliées au câblage du réseau extérieur par leur partie métallique.
Les ports suivants sont considérés comme des ports intrabâtiments sur l'équipement :

## Consignes d'installation

Prenez en compte les avertissements suivants :

Consigne 1047 : prévention de la surchauffe

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 1019 : périphérique de déconnexion principal

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

Consigne 1075 : câble d'alimentation et adaptateur CA

Lors de l'installation du produit, utilisez les câbles de connexion, les cordons d'alimentation et les adaptateurs ou batteries 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 1073 : aucune pièce réparable ni remplaçable par l'utilisateur

L'appareil ne contient aucune pièce réparable ni remplaçable 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.

## Considérations relatives à 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.

# 3. Montage de vos appliances

Vous pouvez monter des appliances Secure Network Analytics 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 Secure Network Analytics :

- 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

# 4. Connexion de vos appliances au réseau

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

## 1. Vérification des caractéristiques techniques

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

- **Fiches techniques :** pour obtenir des informations spécifiques sur chaque appliance, reportez-vous aux Fiches techniques Secure Network Analytics.
- **Plateforme UCS :** 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 (NIC), le processeur, la mémoire, le stockage et le niveau RAID.
- **Gestionnaire 2210 :** si vous déployez un data store, vous pouvez configurer un Gestionnaire 2210 avec une interface DAC SFP+ 10 Gbit/s sur eth0 pour un débit accru. Si vous ne déployez pas de data store, vous pouvez uniquement configurer l'interface cuivre 100 Mbit/s, 1 Gbit/s, 10 Gbit/s sur eth0.
- **Collecteur de flux 4210 :** si vous déployez un data store, vous pouvez configurer un collecteur de flux 4210 avec une interface DAC SFP+ 10 Gbit/s sur eth0 pour un débit accru. Si vous ne déployez pas de data store, vous pouvez uniquement configurer l'interface cuivre 100 Mbit/s, 1 Gbit/s, 10 Gbit/s sur eth0.
- **Collecteur de flux 5210 :** 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.

  Lorsque vous configurez votre système, veillez à configurer la base de données et le moteur dans l'ordre spécifié dans le Guide de configuration du système.

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

## 2. Connexion de votre appliance au 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.

    - **Haute disponibilité 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.
    - **Étiquette Ethernet :** tenez compte de l'étiquette Ethernet (eth2, eth3, etc.) pour chaque port. Ces étiquettes correspondent aux interfaces réseau (eth2, eth3, etc.) qui sont utilisées dans la configuration du système.

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.

# 5. Connexion à l'appliance

Dans cette section, nous vous expliquons comment vous connecter à votre appliance pour la configuration du système.

Choisissez votre procédure de connexion :

- **Se connecter avec un clavier et un moniteur**
- **Se connecter avec un câble série ou une console série**
- **Se connecter avec CIMC (requis pour l'accès à distance)** Pour vous connecter à l'appliance pour un accès à distance, procédez comme suit.

## 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. Accédez à la section **6. Configuration de votre système Cisco Secure Network Analytics**.

## Se connecter avec un câble série ou une console série

Vous pouvez également vous connecter à l'appliance avec un câble série ou une console série, par exemple un ordinateur portable équipé d'un émulateur de terminal. Nous utilisons un ordinateur portable comme exemple dans ces instructions.

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. Accédez à la section **6. Configuration de votre système Cisco Secure Network Analytics**.

## Se connecter avec CIMC (requis pour l'accès à distance)

Le contrôleur CIMC (Cisco Integrated Management Controller) permet d'accéder à la configuration du serveur, à une console de serveur virtuel et aux moniteurs surveillant l'intégrité du matériel. Vous utiliserez également CIMC dans la configuration système de Secure Network Analytics.

1. Suivez les instructions du Guide de configuration de l'interface utilisateur de Cisco Integrated Management Controller UCS C-Series.
2. Connectez-vous à CIMC en tant qu'administrateur et saisissez **password** dans le champ du mot de passe.
3. Modifiez le mot de passe par défaut pour protéger la sécurité de votre réseau.
4. Accédez à la section **6. Configuration de votre système Cisco Secure Network Analytics**.

# 6. Configurer votre système Secure Network Analytics

Si vous avez terminé l'installation de vos appliances Édition virtuelle et/ou matérielles, vous êtes prêt à configurer Secure Network Analytics dans un système géré.

> ⚠ Pour configurer Secure Network Analytics, suivez les instructions du Guide de configuration du système v7.4.2. Cette étape est essentielle à la configuration et à la communication de votre système.
>
> Veillez à configurer vos appliances dans l'ordre spécifié dans le Guide de configuration du système.

## Configuration système requise

Assurez-vous d'avoir accès à la console de l'appliance via CIMC.

Utilisez le tableau suivant pour préparer les informations requises pour chaque appliance.

| Configuration requise | Détails | Appliance |
|---|---|---|
| Adresse IP | Attribuez une adresse IP routable au port de gestion `eth0`. | |
| Masque réseau | | |
| Passerelle | | |
| Nom d'hôte | Un nom d'hôte unique est requis pour chaque appliance. Nous ne pouvons pas configurer une appliance portant le même nom d'hôte qu'une autre appliance. En outre, assurez-vous que le nom d'hôte de chaque appliance répond aux exigences du standard Internet pour les hôtes Internet. | |

| | | |
|---|---|---|
| Nom de domaine | Un nom de domaine complet est requis pour chaque appliance. Nous ne pouvons pas installer une appliance avec un domaine vide. | |
| Serveurs DNS | Serveur DNS interne pour la résolution de noms | |
| Serveurs NTP | Serveur de temps interne pour la synchronisation entre les serveurs. Au moins 1 serveur NTP est obligatoire pour chaque appliance.<br>Supprimez le serveur NTP 130.126.24.53 s'il figure dans votre liste de serveurs. Ce serveur est connu pour poser problème et n'est plus pris en charge dans notre liste de serveurs NTP par défaut. | |
| Serveur relais de messagerie | Serveur de messagerie SMTP pour envoyer des alertes et des notifications | |
| Collecteur de flux<br>Port d'exportation | Requis pour les collecteurs de flux uniquement.<br>NetFlow par défaut : 2055 | |
| Adresse IP non routable dans un LAN ou un VLAN privé (pour la communication entre les nœuds de données) | Requis pour les nœuds de données uniquement.<br>• Port matériel eth2, ou liaison entre eth2 et eth3. La création d'un canal de port lié LACP `eth2/eth3` pour un débit allant jusqu'à 20G permet une communication plus rapide entre et parmi les nœuds de données, ainsi qu'un ajout ou un remplacement plus rapide des nœuds de données dans le data store. Notez que la liaison de port LACP est la seule option de | |

| | | |
|---|---|---|
| | liaison disponible pour les nœuds de données matériels.<br>• eth1 virtuel<br><br>**Adresse IP :** vous pouvez utiliser l'adresse IP fournie ou saisir une valeur qui répond aux exigences suivantes pour les communications entre les nœuds de données.<br>• **Adresse IP non routable** du **bloc CIDR 169.254.42.0/24**, entre 169.254.42.2 et 169.254.42.254.<br>• **Trois premiers octets :** 169.254.42<br>• **Sous-réseau :** /24<br>• **Séquentielle :** pour faciliter la maintenance, sélectionnez des adresses IP séquentielles (telles que 169.254.42.10, 169.254.42.11 et 169.254.42.12).<br><br>**Masque de réseau :**<br>Le masque de réseau est codé en dur sur 255.255.255.0 et ne peut pas être modifié. | |

| | | |
|---|---|---|
| Port de connexion matérielle eth0 | Requis pour les appliances matérielles Secure Network Analytics avec data store uniquement :<br>• Gestionnaire 2210<br>• Collecteur de flux 4210<br>• Nœuds de données<br><br>Options de port de connexion matérielle eth0 :<br>• **SFP+** : SFP+ : port fibre DAC/SFP+ 10G pour eth0.<br>• **BASE-T** : 100 Mbit/s/1GbE/10GbE<br>Port cuivre BASE-T pour eth0. BASE-T est la valeur par défaut. | |

# Contacter l'assistance

Si vous avez besoin d'une assistance technique, procédez comme suit :

- Contactez votre partenaire Cisco local
- Contactez l'assistance Cisco
- Pour faire une demande d'assistance par Internet : http://www.cisco.com/c/en/us/support/index.html
- Pour faire une demande d'assistance par e-mail : tac@cisco.com
- Pour une assistance téléphonique : 1-800-553-2447 (États-Unis)
- Pour connaître les numéros d'assistance dans le monde entier : https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

# Informations de copyright

# Historique des modifications

| Version du document : | Date de publication | Description |
|---|---|---|
| 1_0 | 27 février 2023 | Version initiale. |
| 1_1 | 16 mars 2023 | Correction d'un problème lié au chapitre sur les exigences générales de déploiement. |
| 1_2 | 27 mars 2023 | Mise à jour du tableau des ports et protocoles de communication. |
| 1_3 | 27 mars 2023 | Correction d'une faute de frappe. |
| 1_4 | 29 mars 2023 | Ajout des informations de liaison de port LACP. |
| 1_5 | 7 juin 2023 | Mise à jour de la section des avertissements et les consignes d'installation. |