Mise à niveau des meilleures pratiques SNA (Secure Network Analytics)

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Téléchargements de logiciels et guides de mise à niveau
- Matrice de support matériel
  - Gestionnaire et collecteur de flux (moteur et base de données inclus)
  - Magasin de données
  - Capteur De Débit
  - Réplicateur de flux/Directeur UDP
- Matrice de compatibilité des applications
  - audit cryptographique ETA
  - Classificateur d'hôte
  - Diagrammes de réseau et Report Builder (Report Builder est intégré au produit depuis la version 7.4.0)
  - Security Analytics and Logging on Prem (intégré au produit à partir de la version 7.5.1) et Visibility Assessment
- Mises à niveau par version
  - Mise à niveau version 7.3.x vers 7.4.x
  - Mise à niveau version 7.4.x vers 7.5.x
  - Mise à niveau version 7.5.x vers 7.6.0
- Calendrier d'assistance logicielle
- Avis de fin de vie (EOL)
  - FlexNet en fin de vie
  - Global Threat Analytics (GTA) en fin de vie
  - Licence de terminal (intégration du module AnyConnect Network Visibility)
  - Licence SAL-OP EOL
  - UDP Director EOL virtuel
- Mise à niveau des informations et avertissements

Introduction

Ce document décrit certaines informations sur les meilleures pratiques relatives aux mises à niveau vers Secure Network Analytics (SNA) (anciennement appelé StealthWatch).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

SNA ne prend en charge que les mises à niveau d'une version principale à la suivante. Par exemple, de 7.3.x à 7.4.x ou de 7.4.x à 7.5.x. Les sauts de version ne sont pas pris en charge. Si l'utilisateur est à l'aise avec la réinitialisation de toutes les données à un état par défaut d'usine, alors un appareil matériel peut être réimagé, une nouvelle machine virtuelle peut être installée.

Téléchargements de logiciels et guides de mise à niveau

- Les logiciels et les guides pour les versions 7.3.2 et ultérieures sont disponibles sur le site Téléchargement de logiciels
- Les logiciels et les guides des versions antérieures à 7.3.2 ne sont plus disponibles

Matrice de support matériel

Les informations de cette section sont tirées du guide Cisco Secure Network Analytics Hardware and Software Version Support Matrix à partir de la version 7.6.0.

Gestionnaire et collecteur de flux (moteur et base de données inclus)

● - Performs at full capacity on hardware	○ - Supported, but performance not optimal	x - Not supported

Manager

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
Manager 2200	UCSC-C220	M4S	●	●	●	●	x	x	x	x
Manager 2210	UCSC-C220	M5SX	●	●	●	●	●	●	●	●
Manager 2300	UCSC-C225	M6SX	x	x	●	●	●	●	●	●

Flow Collector

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
FC 4200	UCSC-C220	M4S	●	●	●	●	x	x	x	x
FC 4210	UCSC-C220	M5SX	●	●	●	●	●	●	●	●
FC 4300	UCSC-C225	M6SX	x	x	●	●	●	●	●	●
FC 5200 Engine	UCSC-C220	M4S	●	●	●	●	x	x	x	x

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
FC 5200 Database	UCSC-C240	M4S2	●	●	●	●	x	x	x	x
FC 5210 Engine	UCSC-C220	M5SX	●	●	●	●	●	●	●	●
FC 5210 Database	UCSC-C240	M5SX	●	●	●	●	●	●	●	●

Magasin de données

Data Store

v7.4.1 and Earlier Releases

Users deploying a Data Store for v7.4.1 or earlier can configure the Manager and Flow Collector 10Gbps SFP+ interface as eth0 for increased throughput. Users not deploying a Data Store for v7.4.1 or earlier can only configure the Manager and Flow Collector 100Mbps/1Gbps/10Gbps copper interface as eth0.

v7.4.2 and Later Releases

Users deploying a Data Store for v7.4.2 can configure a Manager 2300 with a 10Gbps SFP+ DAC interface as eth0 for increased throughput. Users not deploying a Data Store for v7.4.2 can only configure the 1 Gbps/10 Gbps interface as eth0.

Appliance	Data Nodes	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
DS 6200	3	UCSC-C240	M5SX	●	●	●	●	●	●	●	●
DN 6300	1	UCSC-C225	M6SX	x	x	●	●	●	●	●	●

The following table describes Data Store appliance support:

Appliance	Required?	Supported Models
Data Store	yes	• DS 6200 multi node (v7.4.0 or greater) or single node (v7.4.1 or greater), Virtual Edition • DN 6300 multi node or single node (v7.4.2 or greater), Virtual Edition
Manager	yes	• Manager 2210 or Manager Virtual Edition (v7.4.0 or greater). Four models available for virtual edition • Manager 2300 or Manager Virtual Edition (v7.4.2 or greater).
Flow Collector	yes	• Flow Collector 4210s or Flow Collector Virtual Edition (v7.4.0 or greater)* • Flow Collector 4300s or Flow Collector Virtual Edition (v7.4.2 or greater)* • Flow Collector 5210s or Flow Collector Virtual Edition (v7.4.0 or greater)* * Four models available for Virtual Edition
Flow Sensor	no	• For M5SX generations, any model at v7.4.0 or greater. • For the M6SX generation, Flow Sensors are only supported at v7.4.2 or greater.
UDP Director	no	• UD 2210 • There are no M6 UDPDs.

Mix and match of Data Nodes is not supported. Data Nodes must be either all virtual or all hardware and they must be from the same hardware generation (all DS 6200, all DN 6300).

Capteur De Débit

Flow Sensor

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3	v7.6.0
FS 1200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 1210	UCSC-C220	M5SX	•	•	•	•	•	•	•	•
FS 1300	UCSC-C225	M6SX	x	x	•	•	•	•	•	•
FS 2200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 3200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 3210	UCSC-C220	M5SX	•	•	•	•	•	•	•	•
FS 3300	UCSC-C225	M6SX	x	x	•	•	•	•	•	•
FS 4200	UCSC-C220	M4S	•	•	•	•	x	x	x	x
FS 4210	UCSC-C220	M5SX	•	•	•	•	•	•	•	x
FS 4240	UCSC-C220	M5SX	•	•	•	•	•	•	•	•
FS 4300	UCSC-C225	M6SX	x	x	•	•	•	•	•	•

Réplicateur de flux/Directeur UDP

Flow Replicator/UDP Director

Appliance	Platform	Gen	v7.4.0	v7.4.1	v7.4.2	v7.5.0	v7.5.1	v7.5.2	v7.5.3
UD 2200	UCSC-C220	M4S	•	•	•	•	x	x	x
UD 2210	UCSC-C220	M5SX	•	•	•	•	•	•	•

NOTE: UDPD 2210 est EOL. Les utilisateurs UDPD sont encouragés à migrer vers CTB, cependant la mise à niveau vers UDPD 7.6.0 est possible. Le fichier swu est disponible sur Software Download.

Matrice de compatibilité des applications

Les informations de cette section sont extraites de la [matrice de compatibilité des versions des applications Secure Network Analytics]

audit cryptographique ETA

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
ETA Cryptographic Audit	1.0.27	7.0.0, 7.0.2, 7.0.3, 7.1.1, 7.1.2, 7.1.3	None
	2.0.2	7.2.1, 7.3.0	None
	2.0.3	7.3.0	None
	3.0.0	7.3.1	None
	3.1.0	7.3.2	7.3.2 (Audit Report only)
	3.2.0	7.4.0	7.4.0 (Audit Report only)
	3.2.1	7.4.1	7.4.1 (Audit Report only)
	3.2.2	7.4.2	7.4.2 (Audit Report only)
	3.3.1	7.5.0	7.5.0 (Audit Report only)
	3.3.2	7.5.1	7.5.1 (Audit Report only)
	3.3.3	7.5.2	7.5.2 (Audit Report only)

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
	3.3.4	7.5.3	7.5.3 (Audit Report only)
	3.3.5	7.6.0	7.6.0 (Audit Report only)

Classificateur d'hôte

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
Host Classifier	1.0.9, 1.0.11, 1.0.13	7.0.0, 7.0.2, 7.0.3, 7.1.1, 7.1.2, 7.1.3	None
	2.0.3	7.2.1	None
	2.0.4	7.2.1, 7.3.0, 7.3.1	None
	2.0.6	7.3.0, 7.3.1, 7.3.2	None
	3.0.0	7.4.0	None
	3.1.1	7.4.0, 7.4.1	None
	4.0.2	7.4.2	None
	4.1.1	7.5.0	None
	4.2.1	7.5.1	None
	4.2.2	7.5.2	None

	4.3.0	7.5.3	None
	4.4.0	7.6.0	None

Diagrammes de réseau et Report Builder (Report Builder est intégré au produit depuis la version 7.4.0)

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
Network Diagrams	1.0.3	7.1.1, 7.1.2, 7.1.3	None
	2.0.2	7.2.1, 7.3.0	7.3.0
	2.0.3, 2.0.4	7.3.0, 7.3.1	7.3.0, 7.3.1
	2.0.5	7.3.2	7.3.2
	2.1.0	7.4.0	7.4.0
	2.1.1	7.4.1	7.4.1
	2.2.1	7.4.2	7.4.2
Report Builder	1.1.2, 1.1.5, 1.1.6	7.3.0	7.3.0
	1.2.1, 1.3.1, 1.3.2, 1.3.4	7.3.1	7.3.1
	1.4.1, 1.4.4, 1.4.5	7.3.2	7.3.2

Security Analytics and Logging on Prem (intégré au produit à partir de la version 7.5.1) et Visibility Assessment

App Name	Version Number	Compatible Secure Network Analytics Versions	Compatible Secure Network Analytics Data Store Versions
Security Analytics and Logging On Prem	1.0.0	7.3.0, 7.3.1	None
	2.0.1, 2.0.2	7.3.1, 7.3.2	7.3.2
	3.0.0	7.4.0	7.4.0
	3.1.0	7.4.0, 7.4.1	7.4.0, 7.4.1
	3.2.0	7.4.2	7.4.2
	3.3.0	7.5.0	7.5.0
Visibility Assessment	1.0.4	7.0.0	None
	1.0.7, 1.0.11, 1.0.14	7.0.0, 7.0.2, 7.0.3, 7.1.1, 7.1.2, 7.1.3	None

Mises à niveau par version

Mise à niveau version 7.3.x vers 7.4.x

Mises à niveau vers les versions : 7.4.0, 7.4.1 et 7.4.2

Téléchargements de logiciels : Le logiciel est disponible sur Téléchargement de logiciel

Guide de mise à niveau : Guide de mise à jour de 7.3.x vers 7.4.0 ou 7.4.1

Guide de mise à niveau : Guide de mise à jour de 7.3.x vers 7.4.2

Mise à niveau version 7.4.x vers 7.5.x

Mises à niveau vers les versions : 7.5.0, 7.5.1, 7.5.2, 7.5.3

Téléchargements de logiciels : Le logiciel est disponible sur Téléchargement de logiciel

Guide de mise à niveau : Guide de mise à jour de 7.4.x vers 7.5.0

Guide de mise à niveau : Guide de mise à jour pour 7.4.x et 7.5.0 vers 7.5.1
Guide de mise à niveau : Guide de mise à jour pour 7.4.x et 7.5.x vers 7.5.2
Guide de mise à niveau : Guide de mise à jour de 7.4.x et 7.5.x vers 7.5.3

Mise à niveau version 7.5.x vers 7.6.0

Mise à niveau vers la version 7.6.0

Téléchargements de logiciels : Le logiciel est disponible sur Téléchargement de logiciel

Guide de mise à niveau : Guide de mise à jour de 7.5.x vers 7.6.0

Calendrier d'assistance logicielle

En général, une version est couverte par la maintenance logicielle pendant 12 mois après sa publication et reçoit des correctifs de vulnérabilité et de sécurité pendant 18 mois après sa publication. Pour plus d'informations sur le modèle de version du logiciel SNA et le calendrier de prise en charge des versions, consultez le bulletin de produit Modèle de version du logiciel Cisco StealthWatch® et Calendrier de prise en charge des versions.

Ce tableau répertorie les délais de prise en charge à partir de la version 7.1.1.

Libérer	Date de sortie	Fin de la maintenance logicielle (EoS)	Fin de la prise en charge des vulnérabilités et de la sécurité (EoVSS)
7.6.0*	23 mars 2026	23 mars 2027	23 septembre 2027

7.5.3	25 août 2025	25 août 2026	25 février 2027
7.5.2	24 février 2025	24 février 2026	24 août 2026
7.5.1	19 août 2024	19 août 2025	19 février 2026
7.5.0	22 janvier 2024	22 janvier 2025,	22 juillet 2025
7.4.2	26 Marchaoût 2023	26 mars 2024,	26 septembre 2024
7.4.1	09 May, 2022	09 2023May,	09 novembre 2023
7.4.0	02 novembre 2021	02 novembre 2022	02 May, 2023
7.3.2	01 juin 2021	01 juin 2022	01 décembre 2022
7.3.1	04 fév. 2021	04 février 2022	04 août 2022
7.3.0	03 septembre 2020	03 septembre 2021	03 mars 2022
7.2.1	17 juin 2020	17 juin 2021	01 juillet 2022
7.1.1	16 août 2019	16 août 2020	01 juillet 2022

* indique la version actuellement recommandée

Avis de fin de vie (EOL)

FlexNet en fin de vie

Les licences FlexNet ont pris fin le 31 décembre 2022. Toutes les licences SNA sont passées à Cisco Smart Licensing.

Global Threat Analytics (GTA) en fin de vie

La fin de vie de GTA est prévue pour le 31 juillet 2024. La note de fin de vie traite également des options de migration.

Licence de terminal (intégration du module AnyConnect Network Visibility)

Avec Secure Network Analytics version 7.5.1, la licence Endpoint n'est plus nécessaire pour l'intégration de Secure Network Analytics au module Network Visibility de Cisco Secure Client (AnyConnect). Au lieu de cela, la consommation est prise en compte dans la licence de débit d'un client afin de simplifier les conditions d'autorisation.

Licence SAL-OP EOL

À partir de la version 7.5.3 de Secure Network Analytics, la licence SAL-OP (Secure Analytics Logging - On Prem) n'est plus nécessaire pour intégrer Secure Network Analytics à la journalisation Secure Analytics On Prem à partir des pare-feu Cisco. Au lieu de cela, l'utilisation contribue désormais à la licence de débit d'un client, simplifiant ainsi le processus d'autorisation.

UDP Director EOL virtuel

L'avis de fin de vie indique que la dernière date d'assistance est le 31 octobre 2028. UDP Director est remplacé par Cisco Telemetry Broker.

Mise à niveau des informations et avertissements

Numéro 1 : Basculement du gestionnaire : Une fois que vous avez commencé une mise à niveau, n'effectuez PAS un basculement de Manager tant que TOUTES les appliances ne sont pas mises à niveau, cela pourrait entraîner l'indisponibilité du système.

Numéro 2 : Avant de commencer la mise à jour (par exemple, vers la version 7.6.0), assurez-vous que vos appliances fonctionnent sur la même version (dans ce cas, 7.5.0, 7.5.1, 7.5.2 ou 7.5.3) depuis plus d'un mois (30 jours). Si vous avez mis à jour votre système vers plusieurs versions dans un court laps de temps, la planification initiale de votre système peut être affectée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.