升级安全网络分析(SNA)最佳实践

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 软件下载和升级指南

硬件支持表

- 管理器和流量收集器（包括引擎和数据库）
- 数据存储
- 流量传感器
- Flow Replicator/UDP Director

应用程序兼容性矩阵

- ETA加密审计
- 主机分类器
- 网络图和报告生成器（从7.4.0开始，将报告生成器集成到产品中）
- 安全分析和登录Prem（从7.5.1开始集成到产品中）和可见性评估

按版本升级

- 将版本7.3.x升级到7.4.x
- 将版本7.4.x升级到7.5.x
- 将版本7.5.x升级到7.6.0

软件支持时间表

生命周期终止(EOL)通知

- FlexNet停产
- 全球威胁分析(GTA)停产
- 终端许可证（AnyConnect网络可视性模块集成）
- SAL-OP许可证停产
- UDP Director虚拟EOL

升级陷阱和警告

简介

本文档介绍有关升级至安全网络分析(SNA)（以前称为Stealthwatch）的一些最佳实践信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

SNA仅支持从一个主要版本升级到下一个主要版本。例如，从7.3.x到7.4.x或7.4.x到7.5.x。不支持发布跳过。如果用户愿意将所有数据重置为出厂默认状态，则可以重新映像硬件设备，可以安装新的VM。

软件下载和升级指南

- 软件下载和版本7.3.2及更高版本的指南位于Software Download
- 7.3.2之前版本的软件和指南不再提供

硬件支持表

从7.6.0版本开始，本节信息摘自Cisco安全网络分析硬件和软件版本支持表指南。

管理器和流量收集器（包括引擎和数据库）

● - 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	●	●	●	●	●	●	●	●

数据存储

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).

流量传感器

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	•	•	•	•	•	•

Flow Replicator/UDP Director

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为EOL。我们鼓励UDPD用户迁移到CTB，但是可以进行7.6.0 UDPD升级。swu文件在软件下载中提供。

应用程序兼容性矩阵

此部分中的信息来自安全网络分析应用版本兼容性列表

ETA加密审计

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)

主机分类器

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

网络图和报告生成器（从7.4.0开始，将报告生成器集成到产品中）

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

安全分析和登录Prem（从7.5.1开始集成到产品中）和可见性评估

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

按版本升级

将版本7.3.x升级到7.4.x

升级到版本：7.4.0、7.4.1和7.4.2

软件下载:软件下载中提供了软件

升级指南：7.3.x到7.4.0或7.4.1的更新指南

升级指南：7.3.x到7.4.2的更新指南

将版本7.4.x升级到7.5.x

升级到版本：7.5.0、7.5.1、7.5.2、7.5.3

软件下载:软件下载中提供了软件

升级指南：7.4.x到7.5.0的更新指南

升级指南：7.4.x和7.5.0到7.5.1的更新指南
升级指南：7.4.x和7.5.x更新指南到7.5.2
升级指南：7.4.x和7.5.x更新指南到7.5.3

将版本7.5.x升级到7.6.0

升级到版本7.6.0

软件下载:软件下载中提供了软件

升级指南：7.5.x到7.6.0的更新指南

软件支持时间表

通常，一个版本在发布后12个月内在“软件维护”下受保护，并在发布后18个月内接收漏洞和安全修复。有关SNA软件版本模型和版本支持时间表的详细信息，请参阅Cisco Stealthwatch®软件版本模型和版本支持时间线产品公告。

此表列出了从版本7.1.1开始的支持时间表。

版本	发布日期	软件维护(EoS)结束	漏洞和安全支持终止(EoVSS)
7.6.0*	2026年3月23日	2027年3月23日	2027年9月23日
7.5.3	2025年8月25日	2026年8月25日	2027年2月25日
7.5.2	2025年2月24日	2026年2月24日	2026年8月24日
7.5.1	2024年8月19日	2025年8月19日	2026年2月19日

7.5.0	2024年1月22日	2025年1月,22日	2025年7月22日
7.4.2	26、2023March	2024年3月,26日	2024年9月26日
7.4.1	09、2022May	09 2023May,	2023年11月09日
7.4.0	2021年11月02日	2022年11月02日	02、2023May
7.3.2	2021年6月01日	2022年6月01日	2022年12月01日
7.3.1	2021年2月04日	2022年2月04日	2022年8月04日
7.3.0	2020年9月03日	2021年9月03日	2022年3月03日
7.2.1	2020年6月17日	2021年6月17日	2022年7月01日
7.1.1	2019-8-16	2020年8月16日	2022年7月01日

*表示当前推荐的版本

生命周期终止(EOL)通知

FlexNet停产

FlexNet许可于2022年12月31日停产。所有SNA许可都移至思科智能许可。

全球威胁分析(GTA)停产

GTA定于2024年7月31日停产。EOL通知还讨论了迁移选项。

终端许可证（AnyConnect网络可视性模块集成）

使用安全网络分析版本7.5.1，安全网络分析与思科安全客户端(AnyConnect)中的网络可视性模块集成不再需要终端许可证。 相反，消费会计入客户的流量许可证，以简化授权要求。

SAL-OP许可证停产

从安全网络分析版本7.5.3开始，SAL-OP（安全分析日志记录 — 内部部署）许可证不再适用于从思科防火墙将安全网络分析与安全分析内部部署日志记录相集成。相反，使用现在有助于提高客户的流量许可证，简化授权流程。

UDP Director虚拟EOL

EOL通知告知最后支持日期为2028年10月31日。UDP Director正在被思科遥测代理替换。

升级陷阱和警告

第一:管理器故障切换：一旦开始升级，请在所有设备升级之前不要执行Manager故障切换，否则可能会导致系统无法运行。

第二:开始更新（例如，到7.6.0）之前，请确保设备已在相同版本（本例中为7.5.0、7.5.1、7.5.2或7.5.3）上运行了一个多月（30天）。 如果您在短时间内将系统更新到多个版本，则您的系统基线可能会受到影响。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。