Cisco Secure Network Analytics

Installationsguide för maskinvaruenheter i x2xx-serien 7.4.2

Innehållsförteckning

Introduktion

Översikt

I den här guiden förklarar vi hur du installerar Cisco Secure Network Analytics-maskinvaruenheter (tidigare Stealthwatch) i x2xx-serien. Den här guiden beskriver även montering och installation av Secure Network Analytics-hårdvaran.

> ⚠ Läs dokumentet Information om regelefterlevnad och säkerhet innan du installerar enheter i Secure Network Analytics x2xx-serien.

Maskinvara i x2xx-serien inkluderar följande:

Enhet	Artikelnummer
Manager 2210 (tidigare Stealthwatch hanteringskonsol)	ST-SMC2210-K9
Data Store 6200 (tre datanoder)	ST-DS6200-K9 (tre ST-DNODE-G1)
Flow Collector 4210	ST-FC4210-K9
Flow Collector 5210-motor	ST-FC5210-E
Flow Collector 5210-databas	ST-FC5210-D
UDP Director 2210	ST-UDP2210-K9
Flow Sensor 1210	ST-FS1210-K9
Flow Sensor 3210	ST-FS3210-K9
Flow Sensor 4240	ST-FS4240-K9

Målgrupp

Den här guiden är utformad för den person som ansvarar för att installera Secure Network Analytics-maskinvaran. Vi antar att du redan har en viss allmän förståelse för installation av nätverksutrustning.

Om du föredrar att arbeta med en professionell installatör ska du kontakta din lokala Cisco-partner eller Ciscos support.

Installera enheter och konfigurera ditt system

Observera det allmänna arbetsflödet för installation och konfiguration av Secure Network Analytics.

1. **Installera enheter:** Installera dina maskinvaruenheter (fysiska) i Secure Network Analytics x2xx-serien med hjälp av den här installationsguiden. Följ instruktionerna i installationsguiden för virtuella enheter för att installera virtuella enheter.
2. **Konfigurera Secure Network Analytics:** När du har installerat maskinvaruenheter och virtuella enheter är du redo att konfigurera Secure Network Analytics till ett hanterat system. Följ instruktionerna i Secure Network Analytics systemkonfigurationsguiden v7.4.2.

Relaterad information

Det finns mer information om Secure Network Analytics i följande resurser online:

- **Information om regelefterlevnad och säkerhet:** Läs dokumentet Information om regelefterlevnad och säkerhet innan du installerar enheter i Secure Network Analytics x2xx-serien.
- **Översikt:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Data Store-designguide:** https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **Matris för stöd för maskinvaru- och programvaruversion:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **Enhetsspecifikationer:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

Terminologi

Vi använder ordet ”**enhet**” för alla Secure Network Analytics-produkter i den här guiden.

Ett ”**kluster**” är en grupp Secure Network Analytics-enheter som hanteras av Manager.

Vanliga förkortningar

Följande förkortningar förekommer i den här guiden:

Förkortning	Beskrivning
DMZ	Demilitariserad zon (ett perimeternätverk)
HTTPS	Hypertext Transfer Protocol (Secure)
ISE	Identity Services Engine
NIC	Network Interface Card (nätverkskort)
NTP	Network Time Protocol
PCIe	Peripheral Component Interconnect Express
SNMP	SNMP-protokoll (Simple Network Management Protocol)
SPAN	Switch Port Analyzer
TAP	Test Access Port
UPS	Avbrottsfri strömförsörjning (Uninterruptible Power Supply)
VLAN	Virtual Local Area Network

Om Secure Network Analytics-enheter

Secure Network Analytics består av flera maskinvaruenheter som samlar in, analyserar och visar information om ditt nätverk för att förbättra nätverkets prestanda och säkerhet. I det här avsnittet beskriver vi varje enhet i Secure Network Analytics x2xx-serien.

Manager 2210

Manager hanterar, samordnar, konfigurerar och organiserar alla systemets olika komponenter. Med Secure Network Analytics-programvara kommer du åt konsolens webbanvändargränssnitt från valfri dator som har en webbläsare. Du kommer enkelt åt säkerhets- och nätverksinformation i realtid om viktiga segment i hela företaget. Manager inkluderar Java-baserat plattformsoberoende och möjliggör

- centraliserad hantering, konfiguration och rapportering för upp till 25 Secure Network Analytics Flow Collectors
- diagram med bilder så att du kan visualisera trafiken
- djupgående analys för felsökning
- sammanfattade och anpassningsbara rapporter
- trendanalys
- prestandaövervakning
- omedelbar avisering vid säkerhetsintrång.

Om du distribuerar en Data Store kan du konfigurera en Manager 2210 med ett SFP+ DAC-gränssnitt på 10 Gbit/s som eth0 för ökad genomströmning. Om du inte distribuerar en Data Store kan du bara konfigurera gränssnitt på 1 Gbit/s och 10 Gbit/s som eth0.

Data Store 6200

Data Store tillhandahåller ett centralt arkiv för att lagra ditt nätverks telemetri, insamlat av dina Flow Collectors. Data Store består av ett kluster av datanoder, som var och en innehåller en del av dina data, och en säkerhetskopia av en separat datanods data. Eftersom alla dina data finns i en centraliserad databas, i stället för spridda över flera Flow Collectors, kan Manager hämta frågeresultat från Data Store snabbare än om den frågade alla dina Flow Collectors separat. Data Store-klustret ger förbättrad feltolerans, förbättrat frågesvar och snabbare diagram- och tabellifyllning.

Det finns mer information i **Secure Network Analytics med Data Store**.

Flow Collector 4210 och 5210

Flow Collector samlar in NetFlow-, cFlow-, J-Flow, Packeteer 2-, NetStream- och IPFIX-data för att tillhandahålla beteendebaserat nätverksskydd.

Flow Collector samlar beteendedata för höghastighetsnätverk från flera nätverk eller nätverkssegment för att tillhandahålla heltäckande skydd och förbättra prestandan i fysiskt utspridda nätverk.

Om du distribuerar en Data Store kan du konfigurera en Flow Collector 4210 med ett 10 Gbit/s SFP+ DAC-gränssnitt som eth0 för ökad genomströmning. Om du inte distribuerar en Data Store kan du bara konfigurera koppargränssnitt på 100 Mbit/s, 1 Gbit/s och 10 Gbit/s som eth0.

> När Flow Collector tar emot data identifierar den kända eller okända attacker, intern felaktig användning och felkonfigurerade nätverksenheter, oavsett paketkryptering eller -fragmentering. När Secure Network Analytics identifierar beteendet kan systemet vidta åtgärder som du har konfigurerat, om du har det, för den sortens beteende.

UDP Director 2210

UDP Director är en snabb och högpresterande UDP-paketreplikator. UDP Director är till stor hjälp för att omfördela administrativa meddelanden från NetFlow, sFlow, syslog eller SNMP (Simple Network Management Protocol) till olika insamlare. Den kan ta emot data från vilken anslutningslös UDP-applikation som helst och sedan återsända den till flera destinationer, och duplicera data om det behövs.

När du använder konfigurationen UDP Director High Availability (HA), ska du se till att du ansluter två UDP Director-enheter med korsade kablar. Se **2. Ansluta din enhet till nätverket**.

Flow Sensor 1210, 3210 och 4240

Flow Sensor är en nätverksenhet som likt en traditionell paketinsamlingsenhet eller IDS kopplas till en Switch Port Analyzer (SPAN), speglad port eller Ethernet-teståtkomstport (TAP). Flow Sensor stärker insynen i följande nätverksområden:

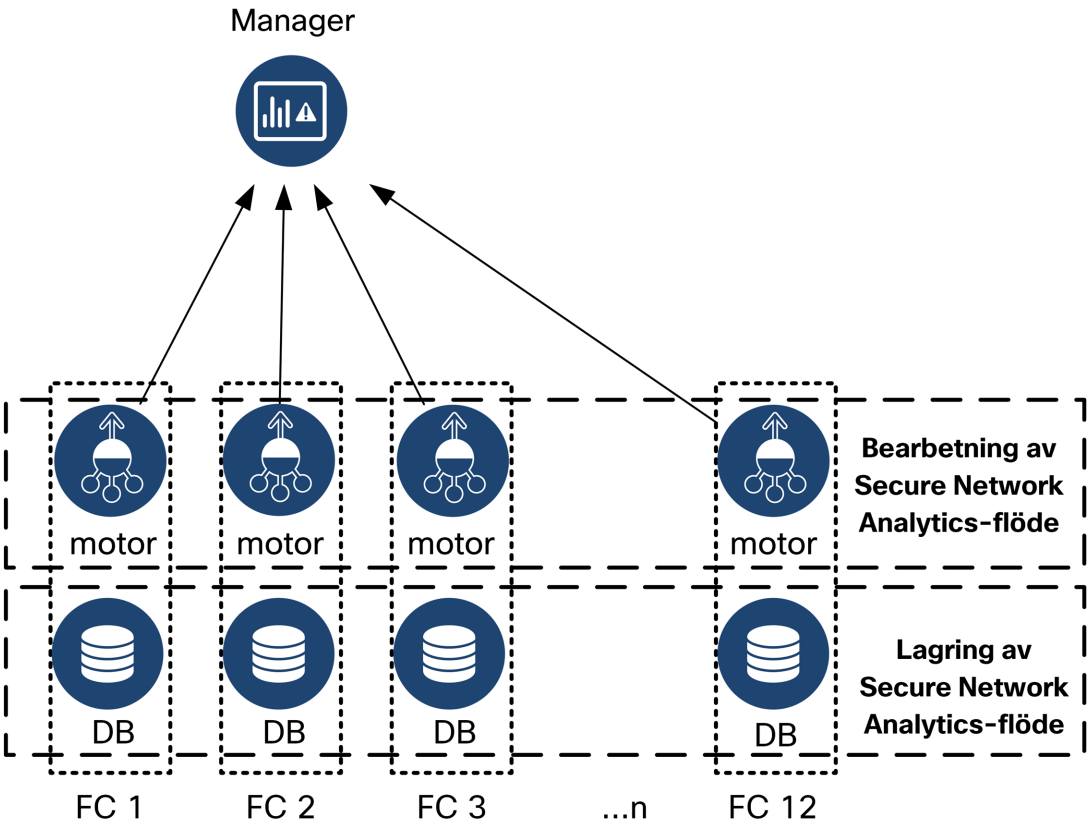
- Där NetFlow inte finns tillgängligt.
- Där NetFlow finns tillgängligt men du vill ha större insyn i prestandamätvärden och paketdata.

Genom att rikta Flow Sensor mot en Flow Collector med kapacitet för NetFlow v9 kan du få värdefull detaljerad trafikstatistik från NetFlow. Tillsammans med Secure Network Analytics Flow Collector ger Flow Sensor även djupgående insyn i prestandamätvärden och beteendeindikatorer. Dessa indikatorer på flödesprestanda ger insikt om latens fram och tillbaka som introduceras av nätverket eller programmet på serversidan.

Flow Sensor har insyn på paketnivå, så den kan beräkna överföringstid (RTT), serversvarstid (SRT) och paketförlust för TCP-sessioner. Den inkluderar alla dessa ytterligare fält i NetFlow-poster som den skickar till Flow Collector.

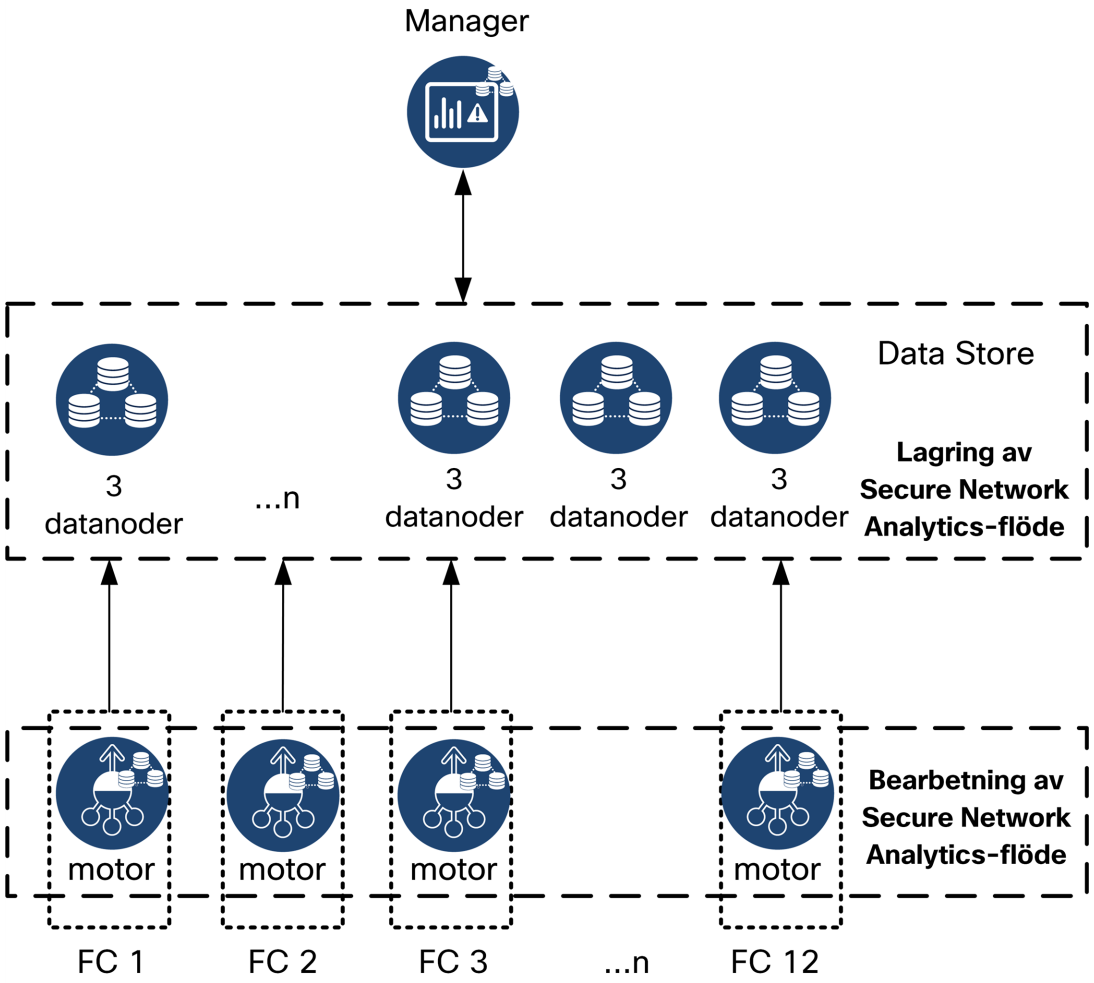
Secure Network Analytics utan Data Store

I en Secure Network Analytics-driftsättning utan Data Store tar en eller flera Flow Collectors emot data och tar bort dubbletter, analyserar och rapporterar data och resultat direkt till Manager. För att lösa frågor som har skickats in av användare, inklusive diagram och tabeller, frågar Manager alla hanterade Flow Collectors. Varje Flow Collector skickar matchande resultat till Manager. Manager sammanställer informationen från olika resultatuppsättningar och skapar ett diagram eller en tabell med resultaten. I den här driftsättningen lagrar varje Flow Collector data på en lokal databas. Följande diagram är ett exempel.



Secure Network Analytics med Data Store

I en Secure Network Analytics-distribution med en Data Store sitter Data Store-klustret mellan dina Manager och Flow Collectors. En eller flera Flow Collectors tar in och deduplicerar flöden, utför analyser och rapporterar data och resultatet går direkt till Data Store och distribuerar det ungefär lika till alla datanoder. Data Store underlättar datalagring, håller all din trafik på den centraliserade platsen istället för att vara spridd över flera Flow Collectors och erbjuder större lagringskapacitet än flera Flow Collectors. Följande diagram är ett exempel.



Data Store tillhandahåller ett centralt arkiv för att lagra ditt nätverks telemetri, insamlat av dina Flow Collectors. Data Store består av ett kluster av datanoder, som var och en innehåller en del av dina data, och en säkerhetskopia av en separat datanods data. Eftersom alla dina data finns i en centraliserad databas, i stället för spridda över flera Flow Collectors, kan Manager hämta frågeresultat från Data Store snabbare än om den frågade

alla dina Flow Collectors separat. Data Store-klustret ger förbättrad feltolerans, förbättrat frågesvar och snabbare diagram- och tabellifyllning.

Frågor

För att lösa frågor som har skickats in av användare, inklusive diagram och tabeller, frågar Manager Data Store. Data Store hittar matchande resultat i kolumner som är relevanta för frågan, hämtar matchande rader och skickar resultaten till Manager. Manager skapar diagrammet eller tabellen utan att behöva sammanställa flera resultatuppsättningar från flera Flow Collectors. Detta minskar kostnaden för frågor jämfört med att fråga flera Flow Collectors och förbättrar frågeprestandan.

Data Store-lagring och feltolerans

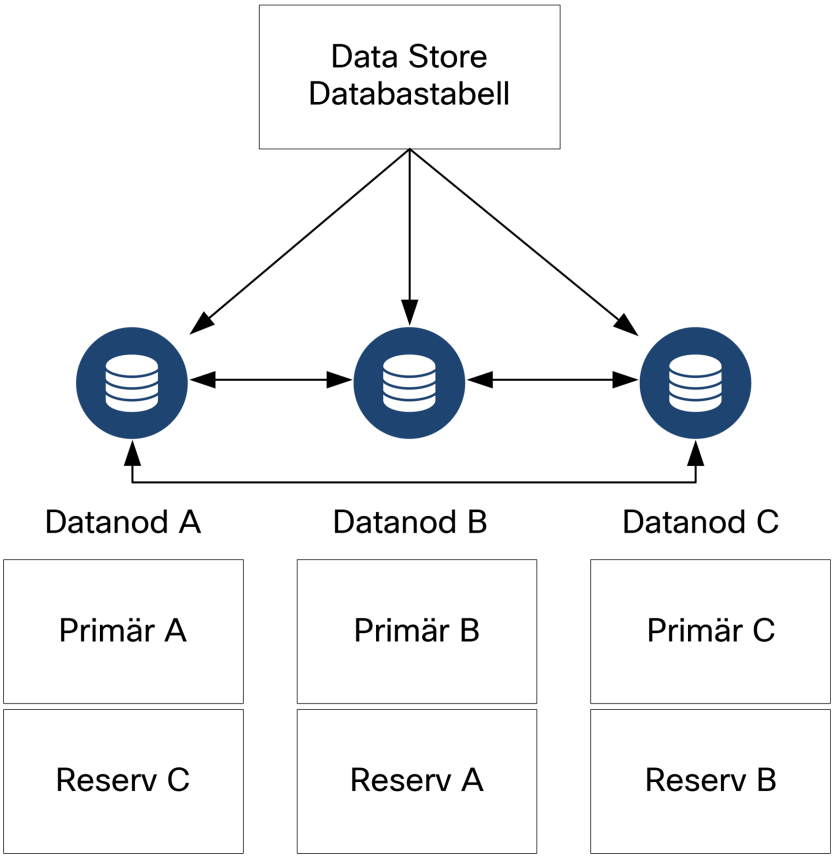
Data Store samlar in data från Flow Collectors och fördelar dem jämlikt mellan datanoder inom klustret. Varje datanod lagrar en del av din allmänna telemetri samt en säkerhetskopia av en annan datanods telemetri. Fördelar med att lagra data på det här sättet:

- bättre belastningsbalansering
- fördelade processer för varje nod
- alla data som tas emot i Data Store har en säkerhetskopia för feltolerans
- möjliggör fler datanoder för bättre generell lagring och frågeprestanda.

Om din Data Store har 3 eller fler datanoder och en datanod slutar fungera fortsätter Data Store att fungera så länge som datanoden som lagrar säkerhetskopian för datanoden som har slutat fungera fortfarande är tillgänglig och minst hälften av ditt totala antal datanoder fungerar. Det ger dig tid att reparera den förlorade anslutningen eller felaktiga maskinvaran. När du har ersatt den felaktiga datanoden återskapar Data Store dess data från den befintliga säkerhetskopian som lagras på den intilliggande datanoden och skapar en säkerhetskopia av data på den.

Exempel på telemetrilagring

Följande diagram är ett exempel på hur 3 datanoder lagrar telemetri:



Allmänna driftsättningskrav

Innan du börjar ska du gå igenom den här guiden för att förstå processen samt förberedelserna, tiden och resurserna du behöver för att planera installationen.

Versionmatris för hårdvaru- och mjukvaruversion

Granska versionsmatrisen för hårdvaru- och mjukvaruversionerna för kompatibilitetsinformation. Matrisen finns på https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html.

Specifikationer

Ladda ner specifikationsbladet för varje enhet som du planerar att installera. Specifikationerna finns på https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.

Cisco Integrated Management Controller (CIMC)

När du har installerat dina enheter ska du se till att du konfigurerar Cisco Integrated Management Controller (CIMC) för att möjliggöra åtkomst till serverkonfigurationen och en virtuell serverkonsol. Du kan också använda CIMC för att övervaka maskinvarans hälsa.

- **Instruktioner:** Läs **Ansluta med CIMC (krävs för fjärråtkomst)** och följ instruktionerna i konfigurationsguiden för Cisco UCS C-Series Integrated Management Controller GUI.
- **Standardlösenord:** Som en del av den initiala konfigurationen kommer du att logga in på CIMC som admin och skriva in **lösenordet** i fältet Lösenord.
- **Lösenordskrav:** När du loggar in ska du ändra standardlösenordet för att skydda ditt nätverks säkerhet.

Standardenhetskrav (utan Data Store)

Om du installerar Secure Network Analytics utan en Data Store ska du installera följande enheter:

Enhet	Krav
Manager	• Minst 1 Manager
Flow Collector	• Minst 1 Flow Collector
Flow Sensor	Valfritt
UDP Director	Valfritt

Du kan läsa mer om enheter som måste installeras för Secure Network Analytics med en Data Store i **Driftsättningskrav för Data Store**.

Driftsättningskrav för Manager och Flow Collector

För varje Manager och Flow Collector som du driftsätter ska du tilldela en omkopplingsbar IP-adress till `eth0`-hanteringsporten.

Driftsättningskrav för Data Store

Granska följande krav och rekommendationer om du vill driftsätta Secure Network Analytics med Data Store.

Enhetskrav (med Data Store)

Följande tabell ger en översikt över enheter som krävs för att driftsätta Secure Network Analytics med Data Store.

Enhet	Krav
Manager	• Minst 1 Manager
Data Store	• Minst 1 eller 3 datanoder • Ytterligare uppsättningar med 3 datanoder för att utöka Data Store, maximalt 36 datanoder • Det går inte att bara driftsätta 2 datanoder i ett kluster.
Flow Collector	• Minst 1 Flow Collector
UDP Director	Valfritt
Flow Sensor	Valfritt

⚠ Uppdatera inte enhetens BIOS, eftersom detta kan orsaka problem med enhetens funktionalitet.

Driftsättningskrav för Manager och Flow Collector

För varje Manager och Flow Collector som du driftsätter ska du tilldela en omkopplingsbar IP-adress till `eth0`-hanteringsporten.

- **Konfiguration av eth0-port:** Du kan konfigurera användningen av en **BASE-T** kopparport på 1 G/10 G eller SFP+-port på 10 G med twinaxkabel som Manager- och Flow Collector `eth0`-hanteringsport.
- **Genomströmning:** Vi kräver 10 G genomströmning för BASE-T-kopparporten för Data Store-användning. Om du inte driftsätter en Data Store kan du bara konfigurera koppargränssnitt på 100 Mbit/s, 1 Gbit/s eller 10 Gbit/s som `eth0`.

Driftsättningskrav för datanoder

Varje Data Store består av datanoder.

- **Maskinvara:** Varje maskinvarudatanod är dess eget chassi. När du köper en maskinvarudatanod får du flera datanodmaskinvaruchassin, som motsvarar antalet noder som anges av Data Store-modellen. En DS 6200 Data Store tillhandahåller t.ex. 3 datanodmaskinvaruchassin.
- **Virtuell version:** När du laddar ner en virtuell Data Store kan du driftsätta 1, 3 eller fler virtuella versioner av datanoder (i uppsättningar om 3).

> Se till att alla dina datanoder är maskinvara eller virtuella. Du kan inte blanda maskinvarudatanoder och virtuella datanoder och maskinvara måste komma från samma generation (alla tillhör DS 6200 eller alla tillhör DN 6300).

Driftsättning med flera datanoder

En driftsättning med flera datanoder ger bästa möjliga prestanda. En Data Store 6200 med 3 datanoder kan t.ex. hantera cirka en miljon flöden per sekund och behålla data i cirka 90 dagar.

Obs!

- **Uppsättningar om 3:** Datanoder kan indelas i kluster som en del av din Data Store i uppsättningar om 3, med minst 3 och högst 36. Det går inte att bara driftsätta 2 datanoder i ett kluster.
- **Bara maskinvarudatanoder eller bara virtuella datanoder:** Se till att alla dina datanoder är maskinvara eller virtuella. Du kan inte blanda maskinvarudatanoder och virtuella datanoder eller Data Store 6200- och Data Store 6300-datanoder.

Driftsättning med en datanod

Om du väljer att driftsätta 1 datanod:

- **Flow Collectors:** Stöd för högst 4 Flow Collectors.
- **Lägga till datanoder:** Om du bara driftsätter 1 datanod kan du lägga till datanoder i din driftsättning framöver. Det finns mer information i **Driftsättning med flera datanoder**.

> Dessa rekommendationer gäller endast telemetri. Din prestanda kan variera beroende på andra faktorer, inklusive antal värdar, Flow Sensor-användning, trafikprofiler och andra nätverksegenskaper. Kontakta Ciscos support om du behöver hjälp med storleken.

> I nuläget har inte Data Store stöd för driftsättning av reservdatanoder som automatiska ersättningar om en primär datanod slutar fungera. Kontakta Ciscos support om du behöver hjälp.

Konfigurationskrav för datanoder

För att driftsätta en Data Store ska du tilldela följande till varje datanod. Informationen du förbereder kommer att konfigureras i konfigurationen vid första användning med systemkonfigurationsguiden.

- **Omkopplingsbar IP-adress (eth0):** För kommunikation kring hantering, inmatning och frågor med dina Secure Network Analytics-enheter.
- **Konfiguration av eth0-port:** Du kan konfigurera användningen av en **BASE-T** kopparport på 1 G/10 G eller SFP+-port på 10 G med twinaxkabel som `eth0`-hanteringsport.
- **Genomströmning:** Vi kräver 10 G genomströmning för BASE-T kopparporten för Data Store-användning.
- **Kommunikation mellan datanoder:** Konfigurera en ej omkopplingsbar IP-adress från `169.254.42.0/24` CIDR-blocket inom ett privat LAN eller VLAN som ska användas för kommunikation mellan datanoder.

  För bättre genomströmning kan du ansluta datanodens `eth0`-port (eller portkanal som innehåller `eth2` och `eth3`) till switcharna för kommunikation mellan datanoder. Som en del av Data Store kommunicerar dina datanoder med varandra.
- **Nätverksanslutningar:** Du behöver två nätverksanslutningar på 10 G – en för kommunikation kring hantering, inmatning och frågor och en för kommunikation mellan datanoder.
- **Ytterligare anslutning och switch:** Som tillval endast på maskinvarudatanoder kan du för nätverksredundans och viktig kommunikation mellan datanoder installera ytterligare en anslutning på 10 G och en ytterligare switch för att etablera en portkanal på datanoden.

> Konfigurera dina datanoder så att datanoder med intilliggande nummer drivs med separat, redundant strömförsörjning. Denna konfiguration förbättrar dataredundans och allmän Data Store-drifttid.

Saker att tänka på för nätverk och switchar

Följande tabell ger en översikt över saker att tänka på för nätverk och switchar vid driftsättning av Secure Network Analytics med en Data Store.

Nätverksövervägande	Beskrivning
Kommunikation mellan datanoder	• Fastställ en rekommenderad latens för överföringstid (RTT) på under 200 mikrosekunder mellan och bland datanoder. • Håll klockförvrängningen på 1 sekund eller mindre mellan och bland dina datanoder. • Fastställ en rekommenderad genomströmning på 6,4 Gbit/s eller mer (switchanslutning på 10 Gbit/s med full duplex) mellan och bland dina datanoder. • För maskinvarunoder räcker det att konfigurera en `eth2`-port för 10 G genomströmning för normal kommunikation mellan datanoder. Att skapa en LACP `eth2/eth3`-bunden portkanal för upp till 20 G genomströmning möjliggör snabbare kommunikation mellan och bland datanoder samt snabbare tillägg eller utbyte av datanoder till Data Store, eftersom varje ny datanod tar emot trafik från intilliggande datanoder för att fylla i dess data. Observera att LACP-portens bindning är det enda bindningsalternativet som är tillgängligt för maskinvarudatanoder.
Strömförsörjning för maskinvarudatanoder	• Data kan korrumperas om strömförsörjningen till en maskinvaradatanod oväntat avbryts. Använd båda strömförsörjningar på separata kretsar så att strömförsörjningen inte kan avbrytas. • När du initierar Data Store-klustret ska du växla datanodkonfigurationen baserat på vilken strömförsörjning varje datanod använder. Detta kan optimera feltoleransen genom att minimera antalet datanoder som slutar fungera om strömförsörjningen förloras.

Datanodswitchar	• Datanoder behöver ett eget Layer 2 VLAN för att möjliggöra kommunikation mellan datanoder. Maskinvarudatanoder kan anslutas till en delad eller särskild switch på 10 G. • Vi rekommenderar att maskinvarudatanoder ansluts till två switchar för att säkerställa kontinuerlig anslutning under driftavbrott och uppgraderingar av switchar. På grund av den låga latens som krävs för kommunikation mellan datanoder rekommenderar Cisco ett redundant par switchar, där de två switcharna är sammankopplade och bär Layer 2 VLAN mellan switcharna.
Secure Network Analytics enhetskommunikation	• Manager och Flow Connectors måste kunna nå alla datanoder. • Datanoder måste kunna nå Manager, alla Flow Connectors och varje datanod.

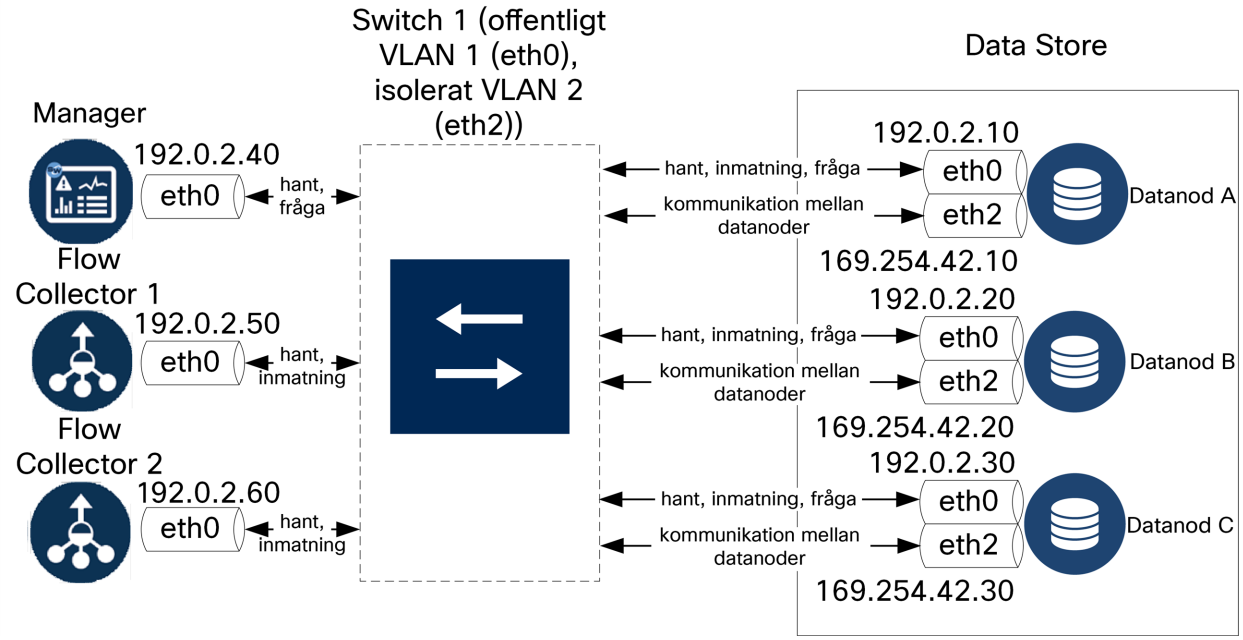
I nuläget har inte Data Store stöd för driftsättning av reservdatanoder som automatiska ersättningar om en primär datanod slutar fungera. Kontakta Ciscos support om du behöver hjälp.

Exempel på maskinvaruswitch

Driftsätt en switch som har stöd för 10 G hastighet om du vill möjliggöra kommunikation mellan datanoder via `eth2`- eller `eth2/eth3`-portkanalen.

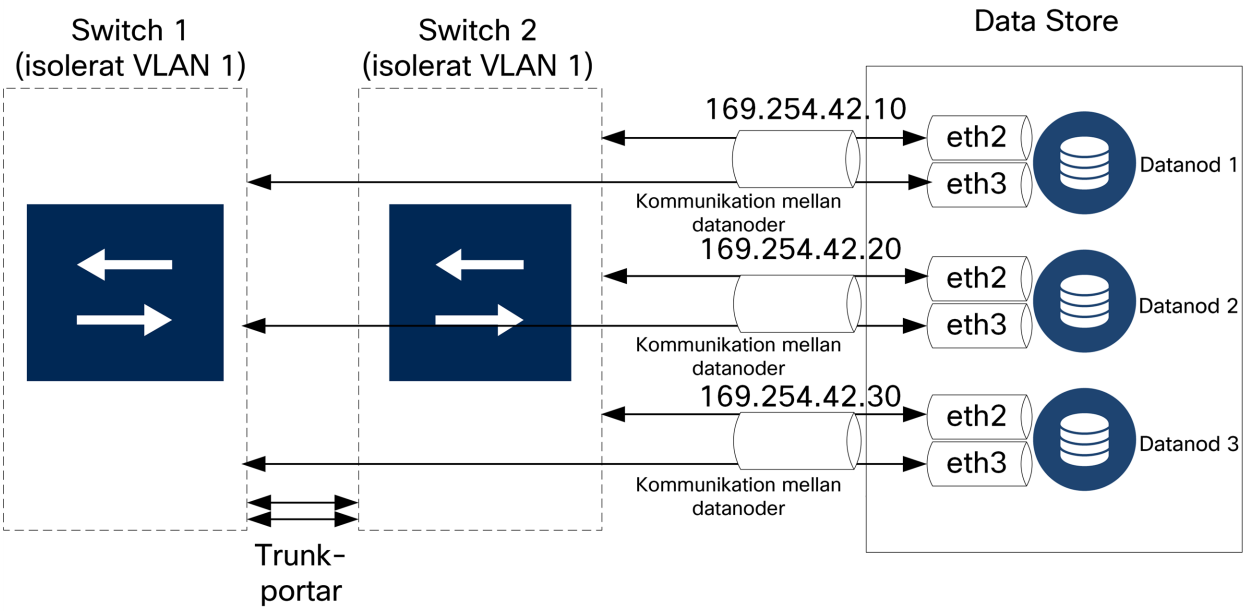
Konfigurera ett LAN eller VLAN för `eth0`-datanodkommunikation med Manager och Flow Collectors, och ett isolerat LAN eller VLAN för kommunikation mellan datanoder.

Du kan dela dessa switchar med andra enheter, men skapa separata LAN eller VLAN för den ytterligare enhetstrafiken. Följande diagram är ett exempel:



Data Store-klustret kräver en kontinuerlig puls mellan noder inom det isolerade VLAN:et. Utan denna puls kan datanoder gå offline, vilket ökar risken för Data Store-driftavbrott.

För ytterligare nätverksredundans för planering kring switchuppdateringar och planerade driftavbrott kan du konfigurera dina datanoder med portkanaler för särskild kommunikation mellan datanoder. Anslut varje datanod till två switchar, och se till att alla fysiska portar är anslutna till olika switchar. Följande diagram är ett exempel:



Kontakta Cisco Professional Services om du behöver hjälp med att planera din driftsättning.

Saker att tänka på kring placering av Data Store

Placera varje datanod så att den kan kommunicera med alla dina Flow Collectors, din Manager och alla andra datanoder. För bästa prestanda ska du samlokalisera dina datanoder och Flow Collectors för minimerad kommunikationslatens och samlokalisera datanoder och Manager för optimal frågeprestanda.

- **Brandvägg:** Vi rekommenderar starkt att du placerar datanoderna inom din brandvägg, t.ex. inom ett NOC.
- **Strömförsörjning:** Om Data Store slutar fungera på grund av förlorad strömförsörjning eller maskinvarufel ökar risken att data korrumperas eller förloras. Installera dina datanoder med kontinuerlig drifttid i åtanke.

Om strömförsörjningen till en datanod avbryts oväntat och du startar om enheten kanske inte databasinstansen på datanoden startas om automatiskt. Läs mer om felsökning och manuell omstart av databasen i systemkonfigurationsguiden.

- **Policy:** Kontrollera att en policy för återställning av strömförsörjningen till en maskinvarudatanod har ställts in för att **återställa till senaste tillstånd**, vilket startar om datanoden automatiskt efter avbruten strömförsörjning och försöker återställa

processer som körs. Det finns mer information om att konfigurera policyn för återställning av strömförsörjning i CIMC i UCS C-Series GUI-konfigurationsguiden.

Driftsättningskrav för Analytics

Secure Network Analytics använder dynamisk entitetsmodellering för att hålla koll på nätverkets status. När det gäller Secure Network Analytics är en entitet något som kan spåras med tiden, t.ex. en värd eller slutpunkt i ditt nätverk. Dynamisk entitetsmodellering samlar in information om entiteter baserat på den trafik de skickar och aktiviteter de utför i ditt nätverk. Du kan läsa mer i guiden Analytics: Detektering, aviseringar och observering.

För att du ska kunna aktivera Analytics måste din driftsättning ha konfigurerats

- på en virtuell eller maskinvarubaserad Data Store-driftsättning med valfritt antal Flow Collectors.
- med bara en Secure Network Analytics Data Store-domän.

1. Konfigurera din brandvägg för kommunikation

För att enheterna ska kunna kommunicera korrekt bör du konfigurera nätverket så att brandväggar eller åtkomstkontrollistor inte blockerar de nödvändiga anslutningarna. Använd informationen i det här avsnittet för att konfigurera ditt nätverk så att enheterna kan kommunicera via nätverket.

Öppna portar (alla enheter)

Prata med din näterksadministratör för att se till att följande portar är öppna och har obegränsad åtkomst på dina enheter (Managers, Flow Collectors, datanoder, Flow Sensors och UDP Directors):

- 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

Ytterligare öppna portar för datanoder

Om du driftsätter datanoder i ditt nätverk ska du även se till att följande portar är öppna och har obegränsad åtkomst:

- TCP 5433
- TCP 5444
- TCP 9450

Kommunikationsportar och -protokoll

I följande tabell visar vi hur portar används i Secure Network Analytics:

Från (klient)	Till (server)	Port	Protokoll
Administratörsanvändares dator	Alla enheter	TCP/443	HTTPS
Alla enheter	Nätverkstidskälla	UDP/123	NTP
Active Directory	Manager	TCP/389, UDP/389	LDAP
Cisco ISE	Manager	TCP/443	HTTPS
Cisco ISE	Manager	TCP/8910	XMPP
Externa loggkällor	Manager	UDP/514	SYSLOG
Flow Collector	Manager	TCP/443	HTTPS
UDP Director	Manager	TCP/443	HTTPS
UDP Director	Flow Collector (sFlow)	UDP/6343*	sFlow
UDP Director	Flow Collector (NetFlow)	UDP/2055*	NetFlow
UDP Director	Händelsehanteringssystem från tredje part	UDP/514	SYSLOG
Flow Sensor	Manager	TCP/443	HTTPS
Flow Sensor	Flow Collector (NetFlow)	UDP/2055	NetFlow
NetFlow-exportörer	Flow Collector (NetFlow)	UDP/2055*	NetFlow
sFlow-exportörer	Flow Collector (sFlow)	UDP/6343*	sFlow
Manager	UDP Director	TCP/443	HTTPS
Manager	Cisco ISE	TCP/443	HTTPS

Från (klient)	Till (server)	Port	Protokoll
Manager	Cisco ISE	TCP/8910	XMPP
Manager	DNS	UDP/53	DNS
Manager	Flow Collector	TCP/443	HTTPS
Manager	Flow Sensor	TCP/443	HTTPS
Manager	Flow-exportörer	UDP/161	SNMP
Manager	LDAP	TCP/636	TLS
Manager	CRL-driftsättningspunkter	TCP/80	HTTP
Manager	OCSP-svarspersoner	TCP/80	OCSP
Användares dator	Manager	TCP/443	HTTPS

*Detta är standardporten, men valfri UDP-port kan konfigureras på exportören.

Ytterligare öppna portar för Data Store

Nedan anges de kommunikationsportar som ska öppnas i din brandvägg för driftsättning av Data Store.

#	Från (klient)	Till (server)	Port	Protokoll eller syfte
1	Manager	Flow Collectors och datanoder	22/TCP	SSH, krävs för att initiera Data Store-databas
1	Datanoder	Alla andra datanoder	22/TCP	SSH, krävs för att initiera Data Store-databas eller för administrationsuppgifter i databasen
2	Manager, Flow Collectors och datanoder	NTP-server	123/UDP	NTP, krävs för tidssynkronisering
2	NTP-server	Manager, Flow Collectors och datanoder	123/UDP	NTP, krävs för tidssynkronisering
3	Manager	Flow Collectors och datanoder	443/TCP	HTTPS, krävs för säker kommunikation mellan enheter
3	Flow Collectors	Manager	443/TCP	HTTPS, krävs för säker kommunikation mellan enheter
3	Datanoder	Manager	443/TCP	HTTPS, krävs för säker kommunikation mellan enheter
4	NetFlow-exportörer	Flow Collector – NetFlow	2055/UDP	NetFlow-inmatning
5	Datanoder	Alla andra datanoder	4803/TCP	Meddelandetjänst inom datanod

6	Datanod	Alla andra datanoder	4803/UDP	Meddelandetjänst inom datanod
7	Datanoder	Alla andra datanoder	4804/UDP	Meddelandetjänst inom datanod
8	Manager, Flow Collectors och datanoder	Datanoder	5433/TCP	Vertica-klientanslutningar
9	Datanod	Alla andra datanoder	5433/UDP	Övervakning av Vertica-meddelandetjänst
10	sFlow-exportörer	Flow Collector (sFlow)	6343/UDP	sFlow-inmatning
11	Datanoder	Alla andra datanoder	6543/UDP	Meddelandetjänst inom datanod

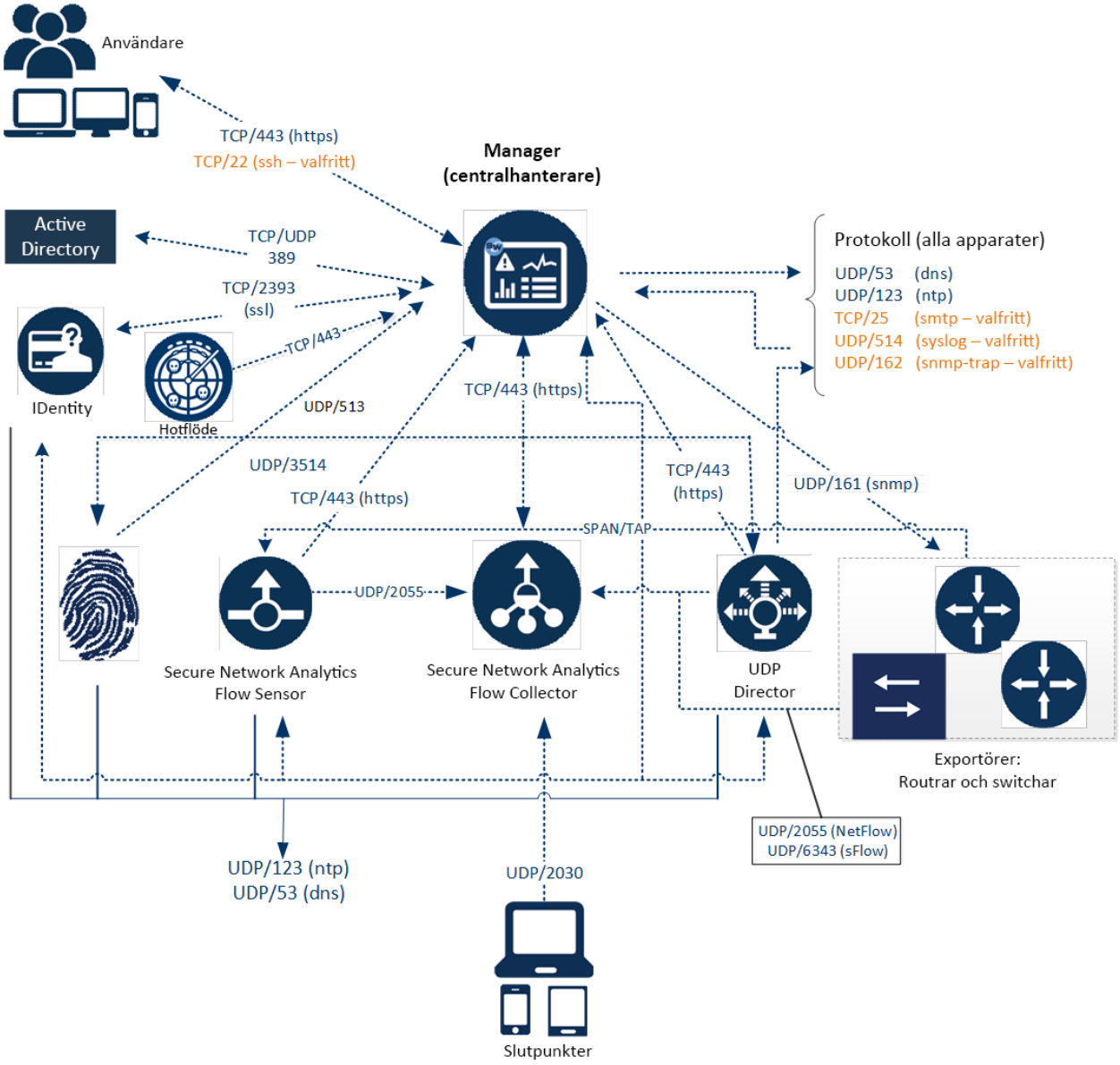
Valfria kommunikationsportar

Följande tabell är för valfria konfigurationer baserade på dina nätverksbehov:

Från (klient)	**Till (server)**	**Port**	**Protokoll**
Alla enheter	Användares dator	TCP/22	SSH
Manager	Händelsehanteringssystem från tredje part	UDP/162	SNMP-trap
Manager	Händelsehanteringssystem från tredje part	UDP/514	SYSLOG
Manager	E-postgateway	TCP/25	SMTP
Manager	Hotflöde	TCP/443	SSL
Användares dator	Alla enheter	TCP/22	SSH

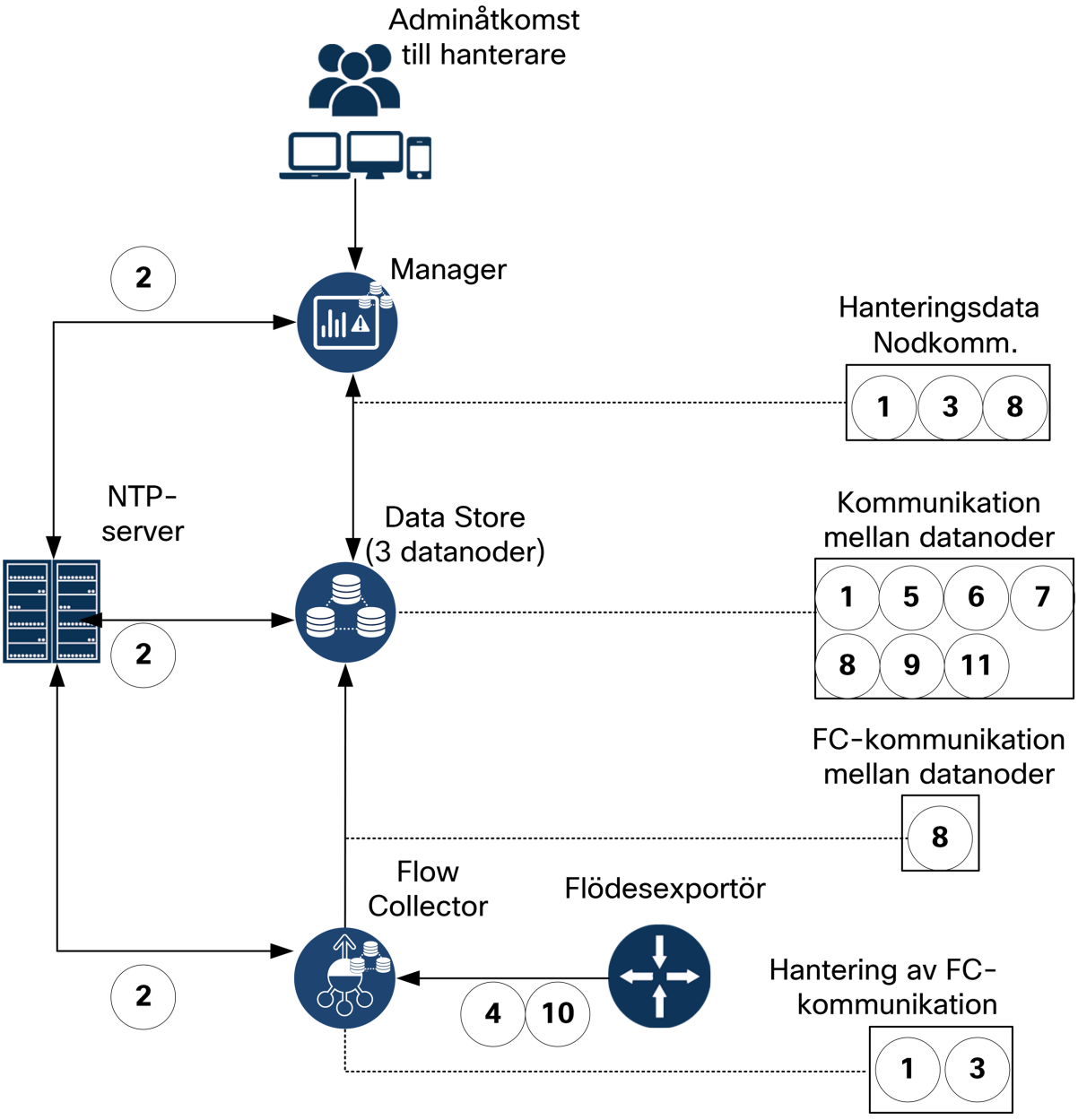
Secure Network Analytics Driftsättningsexempel

I följande diagram visar vi diverse anslutningar som används av Secure Network Analytics. Vissa av portarna är valfria.



Secure Network Analytics driftsättning med Data Store, exempel

Som du ser i bilden nedan kan du driftsätta Secure Network Analytics-enheter strategiskt för att ge optimal täckning för viktiga nätverkssegment i hela nätverket– i det interna nätverket, vid perimetern eller i DMZ.



2. Installationsvarningar och -riktlinjer

Installationsvarningar

Läs dokumentet Information om regelefterlevnad och säkerhet innan du installerar enheter i Secure Network Analytics x2xx-serien.

Observera följande varningar:

Redogörelse 1071 – Varningsdefinition

VIKTIGA SÄKERHETSINSTRUKTIONER

⚠ Den här varningssymbolen indikerar fara. Det finns risk för kroppsskador. Innan du börjar arbeta med utrustningen måste du vara medveten om riskerna med elektriska kretsar och känna till de normala förfarandena för att förhindra olyckor. Använd numret som finns angivet vid varje varning för att hitta den översatta varningen bland de översatta säkerhetsvarningarna som medföljde enheten.

SPARA DE HÄR INSTRUKTIONERNA

Redogörelse 1004 – Installationsinstruktioner

⚠ Läs monteringsinstruktionerna innan du använder, installerar eller ansluter systemet till en strömkälla.

Redogörelse 1005 – Kretsbrytare

⚠ Produkten förlitar sig på byggnadens installation för kortslutningsskydd (överspänning).

Redogörelse 1006 – Chassivarning för rackmontering och service

För att förhindra personskador vid montering eller underhåll av enheten i rack måste du vidta särskilda försiktighetsåtgärder för att säkerställa att systemet är stabilt. Följande riktlinjer tillhandahålls för att hålla dig säker:

- Enheten ska monteras längst ner på racket om den är den enda enheten i racket.
- När enheten monteras i ett delvist fullt rack ska racket lastas nedifrån och upp med de tyngsta komponenterna längst ner.
- När enheten monteras i ett delvist fullt rack ska racket lastas nedifrån och upp med de tyngsta komponenterna längst ner.

Redogörelse 1015 – Batterihantering

För att minska risken för bränder, explosioner eller läckage av lättantändliga gaser eller vätskor:

- Byt endast ut batteriet med samma eller motsvarande typ som rekommenderas av tillverkaren.
- Förbjudet att plocka isär, krossa, punktera, använda vassa verktyg för att ta bort, kortsluta externa kontakter eller kassera batteriet i eld.
- Använd inte om batteriet är förvrängt eller uppsvällt.
- Förvara eller använd inte batteriet vid temperaturer > 60 °C.
- Förvara eller använd inte batteriet i en miljö med lågt lufttryck < 69,7 kPa.

Redogörelse 1017 – Skyddsområde

Enheten är avsedd för montering i skyddsområden med begränsad åtkomst. Ett skyddsområde med begränsad åtkomst får endast beträdas av kunnig, instruerad eller kvalificerad personal.

Redogörelse 191 – Voluntary Control Council for Interference (VCCI) klass A-varning för Japan

Det här är en klass A-produkt baserat på standarden från VCCI Council. Om utrustningen används i hemmiljö kan radiostörningar uppstå och du kan behöva åtgärda dem.

Redogörelse 164 – Lyftkrav

Det krävs två personer för att lyfta de tunga delarna av produkten. För att förebygga skador, håll ryggen rakt och lyft med benen, inte ryggen.

Redogörelse 256 – Klass A-varning för Ungern

Den här utrustningen är en klass A-produkt och ska användas och installeras ordentligt i enlighet med Ungerns EMC klass A-krav (MSZEN55022). Klass A-utrustning har utformats för typiska kommersiella miljöer för vilka specifika villkor för installation och skyddsavstånd används.

Redogörelse 294 – Klass A-varning för Korea

Det här är en klass A-enhet och är registrerad för krav på elektromagnetisk kompatibilitet (EMC) för industriell användning. Säljaren eller köparen bör känna till detta. Om denna typ såldes eller köptes av misstag ska den ersättas med en typ för användning i hemmiljö.

Redogörelse 340 – Klass A-varning för CISPR22/EN55022/CISPR32/EN55032

Det här är en klass A-produkt. I en hemmiljö kan den orsaka radiostörningar som du kan behöva åtgärda.

Redogörelse 1021 – SELV-krets

Undvik elstötar genom att inte ansluta säkerhetskretsar med extra låg spänning (SELV-kretsar) till kretsar med telefonnätverksspänning (TNV-kretsar). LAN-portar innehåller SELV-kretsar, och WAN-portar innehåller TNV-kretsar. Både vissa LAN- och WAN-portar använder RJ-45-anslutningar. Var försiktig när du ansluter kablar.

Redogörelse 1024 – Markledare

Utrustningen måste vara jordad. Sätt aldrig jordledaren ur spel och använd inte utrustningen i avsaknad av lämplig monterad jordledare. Kontakta lämplig elinspektionsmyndighet eller en elektriker om du är osäker på om en lämplig jordning kan utföras.

Redogörelse 1028 – Fler än ett nätaggregat

Enheten kan ha fler än en strömanslutning. För att minska risken för elstötar måste alla anslutningar tas bort så att strömmen helt kopplas bort.

Redogörelse 1029 – Tomma täckplåtar

Tomma täckplåtar har tre viktiga funktioner: de minskar risken för elstöt och brand, de har elektromagnetiska störningar (EMI) som kan störa annan utrustning och de riktar flödet av kylluft genom chassit. Använd inte systemet om inte alla kort, täckplåtar, främre och bakre skydd är på plats.

Redogörelse 1030 – Installation av utrustning

Endast utbildad och kvalificerad personal får installera, byta eller utföra service på denna utrustning.

Redogörelse 1032 – Lyfta chassit

För att undvika personskada eller skada på chassit ska du aldrig försöka lyfta eller luta chassit med handtagen på modulen, såsom strömförsörjning, fläktar eller kort. Dessa slags handtag är inte utformade för att hantera enhetens vikt.

Redogörelse 9001 – Kassering av produkten

Denna produkt ska kasseras enligt nationella lagar och förordningar.

Redogörelse 1051 – Laserstrålning

Osynlig laserstrålning kan avges från bortkopplade fibrer eller kontakter. Titta inte in i strålar och titta inte rakt på dem med optiska instrument.

Redogörelse 1055 – Laser i klass 1/1M

Osynlig laserstrålning är närvarande. Exponera inte för användare av teleskopisk optik. Detta gäller för laserprodukter i klass 1/1M.

Redogörelse 1008 – Laserprodukt i klass 1

Den här produkten är en laserprodukt i klass 1.

Redogörelse 1056 – Öppen fiberkabel

Osynlig laserstrålning kan avges från änden av den öppna fiberkabeln eller kontakten. Titta inte rakt på den med optiska instrument. Att titta på lasern med vissa optiska instrument, till exempel ögonluppar, förstoringsglas och mikroskop, inom ett avstånd på 100 mm kan vara farligt för ögat.

Fibertyp och kärndiameter (µm)	**Våglängd (nm)**	**Maximal effekt (mW)**	**Stråldivergens (rad)**
SM 11	1 200–1 400	39–50	0,1–0,11
MM 62,5	1 200–1 400	150	0,18 NA
MM 50	1 200–1 400	135	0,17 NA
SM 11	1 400–1 600	112–145	0,11–0,13

Redogörelse 1089—Definitioner av instruerad och kunnig person

En instruerad person är någon som har instruerats och utbildats av en kunnig person och som vidtar nödvändiga försiktighetsåtgärder vid användning av utrustningen.

En kunnig person eller kvalificerad personal är personer som har utbildning i eller erfarenhet av utrustningens teknik och som förstår de faror som kan uppstå vid arbete med utrustningen.

Redogörelse 1090 – Installation av kunnig person

Endast en kunnig person får installera, byta eller utföra service på utrustningen. Se redogörelse 1089 för definitionen av en kunnig person.

Redogörelse 1091—Montering av en instruerad person

Endast en instruerad eller kunnig person får montera, byta eller utföra service på utrustningen. Se redogörelse 1089 för definitionen av en instruerad eller kunnig person.

Redogörelse 1074 – Följ lokala och nationella elbestämmelser

Monteringen av utrustningen måste uppfylla lokala och nationella elföreskrifter.

Redogörelse 2017 – Klass A-meddelande för FCC

Om utrustningen ändras utan Ciscos godkännande kanske den inte längre uppfyller FCC:s (Federal Communications Commission) krav för digitala enheter i klass A. I så fall kan din rätt att använda utrustningen begränsas av FCC-bestämmelser och du kan behöva åtgärda eventuell störning av radio- eller TV-signaler på egen bekostnad.

Den här utrustningen har testats och befunnits fungera inom gränsvärdena för en digital enhet i klass A, i enlighet med Kapitel 15 i FCC:s regelverk. Dessa gränser är utformade för att ge ett rimligt skydd mot skadliga störningar när utrustningen används i en kommersiell miljö. Utrustningen genererar, använder och kan utstråla radiofrekvensenergi och kan orsaka störningar i radiokommunikation om den inte installeras och används enligt instruktionerna. Användning av denna utrustning i ett bostadsområde kommer sannolikt att orsaka skadliga störningar, i vilket fall användaren kan behöva korrigera störningarna på egen bekostnad.

Redogörelse 2021 – Klass A-meddelande för Kanada

Denna digitala enhet i klass A uppfyller Kanadas ICES-003/NMB-003.

Redogörelse 7001 – ESD-lindring

⚠ Denna utrustning kan vara känslig för elektrostatisk urladdning. Använd alltid ett fotleds- eller armband för skydd mot elektrostatiska urladdningar. Anslut utrustningsänden på bandet till en obehandlad yta på utrustningens chassi eller till ESD-uttaget på utrustningen, om tillämpligt.

Redogörelse 7003 – Krav på skärmade kablar för blixtnedslag inom byggnaden

⚠ Utrustningens eller delmonteringens port(ar) inom byggnaden måste använda skärmade kablar/sladdar som är jordade i båda ändar.
Följande port(ar) anses vara portar inom byggnaden på denna utrustning:

Redogörelse 7005 – Blixtnedslag och växelströmsfel inom byggnaden

⚠ Utrustningens eller delmonteringens port(ar) inom byggnaden är endast lämplig(a) för anslutning till kablar eller sladdar som är inom byggnaden eller som inte är exponerade. Utrustningens eller undermonteringens portar inom byggnaden FÅR INTE vara metalliskt anslutna till gränssnitt som ansluter till OSP eller dess kablage i mer än sex meter. Dessa gränssnitt är utformade för användning endast som gränssnitt inom byggnader (Type 2-, Type 4- eller Type 4a-portar enligt beskrivning i GR-1089) och måste isoleras från exponerat OSP-kablage. Ytterligare primära skydd är inte tillräckligt skydd för att ansluta dessa gränssnitt metalliskt till ett OSP-kablagesystem.
Följande portar anses vara portar inom byggnaden på utrustningen:

Installationsriktlinjer

Observera följande varningar:

Redogörelse 1047 – Överhettningsskydd

⚠ Undvik överhettning av systemet genom att inte använda det i områden som överskrider den högsta rekommenderade omgivningstemperaturen på 5 till 35 °C.

Redogörelse 1019 – Huvudfrånkopplingsenhet

Kontakten i vägguttaget måste alltid vara åtkomlig eftersom den utgör den huvudsakliga frånkopplingsenheten.

Redogörelse 1075—Strömkabel och växelströmsadapter

Använd de tillhandahållna eller avsedda anslutningskablarna/strömkablarna/AC-adaptrarna/batterierna när du installerar produkten. Användning av andra kablar/adaptrar kan leda till fel eller brand. Lagen om säkerhetsförordningar gällande elektrisk apparatur och materiel förbjuder användning av UL-certifierade kablar (som har markeringen ”UL” eller ”CSA” på kabeln), markeringen ”PSE” på kabeln innebär att den inte regleras av tillämplig lag, för samtliga elektriska enheter som inte är designerade av CISCO.

Redogörelse 1073 – Inga delar som användaren kan utföra service på

Inga inre delar behöver servas av användare. Öppna inte.

När du installerar ett chassi ska du använda följande riktlinjer:

- Se till att det finns tillräckligt med utrymme runt chassit för att möjliggöra service och tillräckligt luftflöde. Luftflödet i chassit sker framifrån och bak.

För att säkerställa korrekt luftflöde är det nödvändigt att ställa in ditt chassi med hjälp av rälssatser. Att fysiskt placera enheterna ovanpå varandra eller stapla utan användning av rälssatserna blockerar luftventilerna ovanpå chassit, vilket kan resultera i överhettning, högre fläkthastigheter och högre strömförbrukning. Vi rekommenderar att du monterar ditt chassi på rälssatser när du installerar dem i racket, eftersom detta ger det minimala avståndet som krävs mellan chassit. Inget ytterligare avstånd mellan chassit krävs när du monterar dem med skensatser.

- Se till att luftkonditioneringen kan hålla chassit vid en temperatur på 5 till 35 °C (41 till 95 °F).
- Se till att skåpet eller ställningen uppfyller ställningskraven.
- Se till att strömförsörjningen på plats uppfyller strömkraven som anges i specifikationsbladet för din enhet. Om tillgänglig kan du använda en UPS för att skydda mot strömavbrott.

Undvik UPS-typer som använder ferroresonant teknologi. Dessa UPS-typer kan bli instabila med dessa system, som kan ha betydande fluktuationer i strömuttaget från fluktuerande datatrafikmönster.

Säkerhetsrekommendationer

Följande information hjälper till att garantera din säkerhet och att skydda chassit. Denna information kanske inte behandlar alla potentiellt farliga situationer i din arbetsmiljö, så var uppmärksam och använd sunt förnuft hela tiden.

Följ dessa säkerhetsriktlinjer:

- Håll området rent och dammfritt före, under och efter installationen.
- Håll verktyg borta från gångvägar, där du och andra kan snubbla över dem.
- Bär inte löst sittande kläder eller smycken, som örhängen, armband eller kedjor som kan fastna i chassit.
- Använd skyddsglasögon om du arbetar under förhållanden som kan vara farliga för dina ögon.
- Utför inga åtgärder som skapar en potentiell fara för människor eller gör utrustningen osäker.
- Försök aldrig att lyfta ett föremål som är för tungt för en person.

Upprätthåll elsäkerheten

Se till att nätsladden är urkopplad innan du arbetar med ett chassi.

Följ dessa riktlinjer när du arbetar med utrustning som drivs med el:

- Arbeta inte ensam om det finns potentiellt farliga förhållanden någonstans på din arbetsplats.
- Anta aldrig att strömmen är frånkopplad, utan kolla alltid först.
- Titta noga efter möjliga faror i ditt arbetsområde, såsom fuktiga golv, ojordade förlängningskablar, slitna nätsladdar och avsaknaden av säkerhetsområden.
- Om en elolycka inträffar:
    - Var försiktig och bli inte själv ett offer.
    - Koppla bort strömmen från systemet.
    - Skicka om möjligt en annan person för att få medicinsk hjälp. Bedöm annars tillståndet för offret och ring sedan efter hjälp.

    - Bestäm om personen behöver andningshjälp eller externa hjärtkompressioner, och vidta sedan lämpliga åtgärder.
- Använd chassit inom dess märkta elektriska klassificeringar och produktanvändningsinstruktioner.

Förhindra ESD-skador

ESD uppstår när elektroniska komponenter hanteras felaktigt, och detta kan skada utrustning och försämra elektriska kretsar, vilket kan resultera i tillfälligt eller fullständigt fel på din utrustning.

Följ alltid ESD-förebyggande procedurer när du tar bort och byter ut komponenter. Se till att chassit är elektriskt anslutet till jordad kontakt. Bär en ESD-förebyggande handledsrem, och se till att den har bra hudkontakt. Anslut jordklämman till en omålad yta på chassiramen för att säkert jorda ESD-spänningar. För att skydda mot ESD-skador och stötar måste handledsremmen och sladden fungera effektivt. Om ingen handledsrem finns tillgängligt jordar du dig själv genom att röra vid metalldelen av chassit.

Kontrollera för säkerhets skull med jämna mellanrum resistansvärdet för det antistatiska bandet, vilket bör vara mellan en och 10 megohm.

Platsmiljön

För att undvika utrustningsfel och minska risken för avstängningar orsakade av miljön ska du planera anläggningens layout och utrustningsplatserna noggrant. Om du för närvarande upplever avstängningar eller ovanligt höga felfrekvenser med din befintliga utrustning, kan dessa överväganden hjälpa dig att hitta orsaken till felen och förhindra framtida problem.

Överväganden om strömförsörjning

Tänk på följande när du installerar chassit:

- Kontrollera platsen innan du installerar chassit för att säkerställa att den är fritt från spikar och buller. Installera en strömkonditionering om det behövs, för att säkerställa korrekta spänningar och effektnivåer i enhetens inspänning.
- Installera korrekt jordning för platsen för att undvika skador från blixtnedslag och överspänningar.
- Chassit har inget användarvalbart arbetsområde. Se etiketten på chassit för rätt ingångseffekt för enheten.
- Det finns flera olika typer av nätsladdar med AC-ingång för enheten, så se till att du har rätt typ för din plats.

- Om du använder dubbla redundanta (1+1) nätaggregat rekommenderar vi att du använder oberoende elektriska kretsar för varje strömförsörjning.
- Installera en avbrottsfri strömkälla för din plats, om möjligt.

Saker att tänka på vid rackkonfiguration

Tänk på följande när du planerar en rackkonfiguration:

- Om du monterar ett chassi i ett öppet rack ska du se till att rackets ram inte blockerar insugnings- eller avgasportarna.
- Se till att slutna rack har tillräcklig ventilation. Se till att racket inte är överbelastat, eftersom varje chassi genererar värme. Ett slutet rack bör ha sidor med jalusier och en fläkt för att ge kylande luft.
- I ett slutet rack med en ventilationsfläkt i toppen kan värme som genereras av utrustning nära botten av racket dras uppåt och in i utrustningens intagsportar ovanför den i racket. Se till att du tillhandahåller tillräcklig ventilation för utrustningen i botten av racket.
- Bafflar kan hjälpa till att isolera frånluften från insugningsluften, vilket också hjälper till att dra kylluft genom chassit. Den bästa placeringen av bafflarna beror på luftflödesmönstren i racket. Experimentera med olika arrangemang för att placera bafflarna effektivt.

3. Montera dina enheter

Du kan montera Secure Network Analytics-enheter direkt i ett standard 19-tumsrack eller -skåp, vilket annat lämpligt skåp som helst eller på en plan yta. När du monterar en enhet i ett rack eller ett skåp följer du instruktionerna som ingår i monteringssatserna för skenan. När du bestämmer var du ska placera en enhet ser du till att utrymmet till de främre och bakre panelerna är som följer:

- Frontpanelens indikatorer kan enkelt avläsas.
- Tillgång till portar på bakpanelen är tillräcklig för obegränsad kablage.
- Strömingången på baksidan är inom räckhåll för en konditionerad växelströmskälla.
- Luftflödet runt enheten och genom ventilerna är obegränsat.

Maskinvara som medföljer enheten

Följande maskinvara medföljer Secure Network Analytics-enheter:

- Nätsladd
- Åtkomstnycklar (för frontplattan)
- Skensats för rackmontering eller monteringsöron för mindre enheter
- En 10 GB SFP-kabel för Flow Collector 5210

Ytterligare nödvändig maskinvara

Du måste tillhandahålla följande ytterligare nödvändig maskinvara:

- Monteringsskruv för ett standard 19-tumsrack
- Avbrottsfri strömförsörjning (Uninterruptible power supply/UPS) för varje enhet du installerar
- För att konfigurera lokalt (valfritt) använder du någon av följande metoder:
    - Bärbar dator med en videokabel och en USB-kabel (för tangentbordet)
    - Videomonitor med videokabel och tangentbord med USB-kabel

4. Ansluta dina enheter till nätverket

Använd samma procedur för att ansluta varje enhet till nätverket. Den enda skillnaden för anslutningen är vilken typ av enhet du har.

1. Granska specifikationer

Använd samma procedur för att ansluta varje enhet till nätverket. Den enda skillnaden för anslutningen är vilken typ av enhet du har.

- **Specifikationsblad:** Det finns detaljerad specifikationsinformation om varje enhet i Secure Network Analytics specifikationsblad.
- **UCS-plattform:** Maskinvaran från Cisco x2xx använder alla samma UCS-plattform, UCSC-C220-M5SX, förutom Flow Collector 5210 DB, som använder UCSC-C240-M5SX. Variationerna i enheterna är NIC-korten, processorerna, minnena, lagringen och RAID.
- **Manager 2210:** Om du distribuerar ett datalager kan du konfigurera en Manager 2210 med ett 10Gbps SFP+ DAC-gränssnitt som eth0 för ökad genomströmning. Om du inte distribuerar ett datalager kan du bara konfigurera 100Mbps/1 Gbps/10 Gbps koppargränssnitt som eth0.
- **Flow Collector 4210:** Om du distribuerar ett datalager kan du konfigurera en Flow Collector 4210 med ett 10 Gbps SFP+ DAC-gränssnitt som eth0 för ökad genomströmning. Om du inte distribuerar ett datalager kan du bara konfigurera 100Mbps/1 Gbps/10 Gbps koppargränssnitt som eth0.
- **Flow Collector 5210:** Flow Collector 5210 består av två anslutna servrar (databas och motor) så att de fungerar som en enda enhet. På grund av detta skiljer sig installationen något från andra enheter. Koppla först ihop dem direkt med en 10G SFP+ DA Cross Connect-kabel. Anslut sedan till ditt nätverk.

  När du konfigurerar ditt system ser du till att du konfigurerar databasen och motorn i den ordning som anges i systemkonfigurationsguiden.

> ⚠ Uppdatera inte enhetens BIOS, eftersom detta kan orsaka problem med enhetens funktionalitet.

2. Ansluta din enhet till nätverket

Gör så här för att ansluta din enhet till ditt nätverk:

1. Anslut en Ethernet-kabel till hanteringsporten på baksidan av enheten.
2. Anslut minst en monitorport för Flow Sensors och UDP Directors.

    - **UDP Director High Availability:** Anslut de två UDP Directors med korsade kablar. Anslut eth2-porten på en UDP Director till eth2-porten på den andra UDP Directorn. Anslut på samma sätt eth3-porten på varje UDP Director med en andra korsad kabel. Kabeln kan vara av fiber eller koppar.
    - **Ethernet-etikett:** Notera Ethernet-etiketten (eth2, eth3, etc.) för varje port. Dessa etiketter motsvarar nätverksgränssnitten (eth2, eth3, etc.) som används i systemkonfigurationen.

3. Anslut den andra änden av ethernet-kablarna till ditt nätverks switch.
4. Anslut strömkablarna till strömförsörjningen. Vissa enheter har två strömanslutningar: strömförsörjning 1 och strömförsörjning 2.

5. Ansluta till din enhet

Det här avsnittet beskriver hur du ansluter till din enhet för systemkonfiguration.

Välj din anslutningsprocedur:

- **Ansluta med ett tangentbord och en bildskärm**
- **Ansluta med en seriell kabel eller seriell konsol**
- **Ansluta med CIMC (krävs för fjärråtkomst)** Använd denna procedur för att ansluta till enheten för fjärråtkomst.

Ansluta med ett tangentbord och en bildskärm

Utför följande steg för att konfigurera IP-adressen lokalt:

1. Anslut strömkabeln till enheten.
2. Tryck på strömknappen för att slå på enheten. Vänta tills den har startat upp helt. Avbryt inte uppstartsprocessen.

> Du kan behöva ta bort frontpanelen för att tillhandahålla ström.
>
> Strömförsörjningsfläktarna slås på för vissa modeller när systemet inte är påslaget. Kontrollera att lysdioden på frontpanelen lyser.
>
> Se till att ansluta enheten till en avbrottsfri strömkälla (uninterruptible power supply/UPS). Strömförsörjningen kräver ström, annars visar systemet ett fel.

3. Anslut tangentbordet:
    - Om du har ett standardtangentbord ansluter du det till standardtangentbordskontakten.
    - Om du har ett USB-tangentbord ansluter du det till en USB-kontakt.
4. Anslut videokabeln till videokontakten. Inloggningsuppmaningen visas.
5. Gå till **6. Konfigurera ditt Secure Network Analytics System**.

Ansluta med en seriell kabel eller seriell konsol

Du kan också ansluta till enheten med en seriell kabel eller seriell konsol, till exempel en bärbar dator som har en terminalemulator. Vi använder en bärbar dator som exempel i instruktionerna.

1. Anslut din bärbara dator till enheten med någon av följande metoder:

    - Anslut en RS232-kabel från den seriella portkontakten (DB9) på din bärbara dator till konsolporten på enheten.
    - Anslut en korsad kabel från ethernet-porten på din bärbara dator till hanteringsporten på enheten.

2. Anslut strömkabeln till enheten.
3. Tryck på strömknappen för att slå på enheten. Vänta tills den har startat upp helt. Avbryt inte uppstartsprocessen.

    > Du kan behöva ta bort frontpanelen för att tillhandahålla ström.
    >
    > Strömförsörjningsfläktarna slås på för vissa modeller när systemet inte är påslaget. Kontrollera att lysdioden på frontpanelen lyser. Se till att ansluta enheten till en avbrottsfri strömkälla (uninterruptible power supply/UPS). Strömförsörjningen kräver ström, annars visar systemet ett fel.

4. På den bärbara datorn gör du en anslutning till enheten.

    Du kan använda vilken terminalemulator som helst för att kommunicera med enheten.

5. Använd följande inställningar:

    - BPS: 115200
    - Databits: 8
    - Stopbit: 1
    - Paritet: Ingen
    - Flow Control: Ingen

    Inloggningsskärmen och inloggningsuppmaningen visas.

6. Gå till **6. Konfigurera ditt Secure Network Analytics System**.

Ansluta med CIMC (krävs för fjärråtkomst)

Cisco Integrated Management Controller (CIMC) möjliggör åtkomst till serverkonfigurationen och en virtuell serverkonsol, samt övervakar maskinvarans hälsa. Du kommer också att använda CIMC i systemkonfigurationen för Secure Network Analytics.

1. Följ instruktionerna i konfigurationsguiden för Cisco UCS C-Series Integrated Management Controller GUI.
2. Logga in på CIMC som admin och skriv in **lösenordet** i fältet Lösenord.
3. Ändra standardlösenordet för att skydda ditt nätverks säkerhet.
4. Gå till **6. Konfigurera ditt Secure Network Analytics System**.

6. Konfigurera ditt Secure Network Analytics-system

Om du har installerat dina virtuella enheter och/eller maskinvaruenheter är du redo att konfigurera Secure Network Analytics till ett hanterat system.

> ⚠ För att konfigurera Secure Network Analytics följer du instruktionerna i systemkonfigurationsguiden v7.4.2. Detta steg är avgörande för en lyckad konfiguration och kommunikation med ditt system.
>
> Se till att du konfigurerar dina enheter i den ordning som anges i systemkonfigurationsguiden.

Systemkonfigurationskrav

Se till att du har tillgång till enhetens konsol via CIMC.

Använd följande tabell för att förbereda den information som krävs för varje enhet.

Konfigurationskrav	Information	Enhet
IP-adress	Tilldela en routbar IP-address till `eth0`-hanteringsporten.	
Nätmask		
Gateway		
Värdnamn	Ett unikt värdnamn krävs för varje enhet. Vi kan inte konfigurera en enhet med samma värdnamn som en annan enhet. Se också till att varje enhets värdnamn uppfyller internetstandardkraven för internetvärdar.	
Domännamn	Ett fullt kvalificerat domännamn krävs för varje enhet. Vi kan inte installera en enhet med en tom domän.	
DNS-servrar	Intern DNS-server för namnlösning	

NTP-servrar	Intern tidsserver för synkronisering mellan servrar. Minst 1 NTP-server krävs för varje enhet. Ta bort 130.126.24.53 NTP-servern om den finns i din lista över servrar. Denna server är känd för att vara problematisk och den stöds inte längre i vår standardlista över NTP-servrar.	
Server för att vidarebefordra e-post	SMTP e-postserver för att skicka varningar och meddelanden	
Flow Collector Exportport	Krävs endast för Flow Collectors. NetFlow-standard: 2055	
Icke-routerbar IP-adress inom ett privat LAN eller VLAN (för kommunikation mellan datanoder)	Krävs endast för datanoder. • Hårdvara eth2 eller bindning av eth2 och eth3. Att skapa en LACP `eth2/eth3`-bunden portkanal för upp till 20 G-genomströmning möjliggör snabbare kommunikation mellan och bland datanoder samt snabbare tillägg eller utbyte av datanoder till Data Store. Observera att LACP-portens bindning är det enda bindningsalternativet som är tillgängligt för hårdvarudatanoder. • Virtuell eth1 **IP-adress:** du kan använda den angivna IP-adressen eller ange ett värde som uppfyller följande krav för kommunikation mellan datanoder. • **Icke-routerbar IP-adress** från **169.254.42.0/24 CIDR-blocket**, mellan 169.254.42.2 och 169.254.42.254.	

	• **Första tre oktetter:** 169.254.42 • **Subnät:** /24 • **Sekventiell:** för att underlätta underhållet väljer du sekventiella adresser (som 169.254.42.10, 169.254.42.11 och 169.254.42.12). **Nätmask:** Nätmasken är hårdkodad till 255.255.255.0 och kan inte ändras.	
eth0 hårdvaruanslutningsport	Krävs endast för Secure Network Analytics med Data Store-hårdvara: • Manager 2210 • Flow Collector 4210 • Datanoder Alternativ för eth0 hårdvaruanslutningsport: • **SFP+**: SFP+: 10G SFP+/DAC fiberport för eth0. • **BASE-T**: 100Mbs/1GbE/10GbE BASE-T kopparport för eth0. BASE-T är standard.	

Kontakta kundtjänst

Om du behöver teknisk support gör du något av följande:

- Kontakta din lokala Cisco-partner
- Kontakta Cisco support
- Öppna ett ärende via webben: http://www.cisco.com/c/en/us/support/index.html
- Öppna ett ärende via e-post: tac@cisco.com
- Telefonsupport: 1-800-553-2447 (USA)
- För globala supportnummer: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Upphovsrättsinformation

Tidigare ändringar

Dokumentversion	Publiceringsdatum	Beskrivning
1_0	27 februari 2023	Första versionen.
1_1	16 mars 2023	Rättade till ett problem i kapitlet Allmänna distributionskrav.
1_2	27 mars 2023	Uppdaterade tabellen Kommunikationsportar och protokoll.
1_3	27 mars 2023	Rättade ett stavfel.
1_4	29 mars 2023	Lade till information om LACP-portbindning.
1_5	7 juni 2023	Uppdaterade avsnittet Installationsvarningar och riktlinjer.