Cisco Secure Network Analytics

Guida all'installazione dell'appliance hardware serie x3xx 7.4.2

Sommario

Introduzione

Panoramica

In questa guida viene illustrato come installare le appliance fisiche Cisco Secure Network Analytics serie x3xx (precedentemente Stealthwatch). Viene descritto inoltre come montare e installare i componenti hardware di Secure Network Analytics.

> ⚠ Prima di installare le appliance Secure Network Analytics serie x3xx, leggere il documento Informazioni sulla conformità alle normative e sulla sicurezza.

Componenti hardware della serie x3xx:

Appliance	**Codice prodotto**
Manager 2300 (precedentemente Stealthwatch Management Console)	ST-SMC-2300-K9
Data Node 6300	ST-DN6300-K9
Flow Collector 4300	ST-FC4300-K9
Telemetry Broker 2300	ST-TB2300-K9
Flow Sensor 1300	ST-FS1300-K9
Flow Sensor 3300	ST-FS3300-K9
Flow Sensor 4300	ST-FS4300-K9

Destinatari

La presente guida è destinata ai responsabili dell'installazione dei componenti hardware Secure Network Analytics. Inoltre, si presume la conoscenza generale delle procedure di installazione dei dispositivi di rete.

Per richiedere il supporto di un installatore professionista, contattare il partner Cisco di riferimento o il supporto Cisco.

Installazione delle appliance e configurazione del sistema

Prendere nota del flusso di lavoro generale per l'installazione e la configurazione di Secure Network Analytics.

1. **Installazione delle appliance:** installare le appliance fisiche Secure Network Analytics serie x3xx facendo riferimento alla presente guida all'installazione. Per installare le appliance Virtual Edition, seguire le istruzioni della Guida all'installazione delle appliance Virtual Edition.
2. **Configurazione di Secure Network Analytics:** dopo aver installato le appliance fisiche e virtuali, è possibile configurare Secure Network Analytics in un sistema gestito. Seguire le istruzioni nella Guida alla configurazione del sistema Secure Network Analytics v7.4.2.

Informazioni correlate

Per ulteriori informazioni su Secure Network Analytics, fare riferimento alle risorse online seguenti:

- **Informazioni sulla conformità alle normative e sulla sicurezza:** leggere il documento Informazioni sulla conformità alle normative e sulla sicurezza prima di installare le appliance Secure Network Analytics serie x3xx.
- **Panoramica:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **Guida alla progettazione del Data Store:** https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **Matrice di compatibilità delle versioni hardware e software:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **Specifiche dell'appliance:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

Terminologia

In questa guida viene usato il termine "**appliance**" per tutti i prodotti Secure Network Analytics.

Un "**cluster**" è un gruppo di appliance Secure Network Analytics che sono gestite dal Manager.

Acronimi di uso comune

Nella guida sono presenti i seguenti acronimi:

Acronimo	Descrizione
DMZ	Demilitarized Zone (zona demilitarizzata) (una rete perimetrale)
HTTPS	Hypertext Transfer Protocol (Secure) (protocollo di trasferimento di un ipertesto)
ISE	Identity Services Engine
NIC	Network Interface Card (scheda di rete)
NTP	Network Time Protocol
PCIe	Peripheral Component Interconnect Express
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
TAP	Test Access Port
UPS	Uninterruptible Power Supply (gruppo statico di continuità)
VLAN	Virtual Local Area Network (LAN virtuale)

Informazioni sulle appliance Secure Network Analytics

Secure Network Analytics comprende diverse appliance hardware che raccolgono, analizzano e presentano informazioni relative alla rete al fine di migliorarne le prestazioni e la sicurezza. In questa sezione vengono descritte le appliance Secure Network Analytics serie x3xx.

Manager 2300

Manager gestisce, coordina, configura e organizza tutti i diversi componenti del sistema. Il software Secure Network Analytics consente di accedere all'interfaccia utente Web della console da qualsiasi computer dotato di accesso a un browser Web. È possibile accedere alle informazioni sulla sicurezza e sulla rete in tempo reale per i segmenti critici dell'azienda. Basato su una piattaforma Java indipendente, Manager offre:

- Gestione, configurazione e reporting centralizzati per un massimo di 25 Secure Network Analytics Flow Collector
- Grafici per la visualizzazione del traffico
- Analisi dettagliate per la risoluzione dei problemi
- Report consolidati e personalizzabili
- Analisi delle tendenze
- Monitoraggio delle prestazioni
- Notifica immediata delle violazioni alla sicurezza

Data Node 6300

Il Data Store fornisce un archivio centrale per memorizzare i dati di telemetria della rete raccolti dai Flow Collector. Il Data Store comprende un gruppo di Data Node, ciascuno dei quali contiene una parte dei dati e un backup dei dati di un altro Data Node. Mantenendo tutti i dati in un database centralizzato, anziché averli dispersi su più Flow Collector, il Manager può richiamare i risultati delle query più velocemente dal Data Store anziché dover interrogare separatamente tutti i Flow Collector. Il gruppo di Data Store offre una migliore tolleranza agli errori, una migliore risposta alle query e permette di popolare i grafici e le tabelle più rapidamente.

Per ulteriori informazioni, fare riferimento a **Secure Network Analytics con Data Store**.

Flow Collector 4300

Flow Collector raccoglie i dati di NetFlow, cFlow, J-Flow, Packeteer 2, NetStream e IPFIX per proteggere la rete sulla base dei comportamenti.

Flow Collector aggrega i dati sui comportamenti delle reti ad alta velocità provenienti da più reti o segmenti di rete per offrire protezione end-to-end e per migliorare le prestazioni delle reti che coprono diverse aree geografiche.

> Mano a mano che riceve i dati, Flow Collector identifica attacchi noti o sconosciuti, uso interno improprio e dispositivi di rete configurati in modo errato, a prescindere dalla crittografia o della frammentazione dei pacchetti. Una volta che Secure Network Analytics ha identificato il comportamento, il sistema può intraprendere l'azione configurata, se disponibile, per quel tipo di comportamento.

Telemetry Broker 2300

Cisco Telemetry Broker fornisce le seguenti funzionalità principali:

- Gestione dei dati: la capacità di indirizzare e replicare i dati di telemetria da una posizione di origine a più utenti di destinazione. Onboarding rapido di nuovi strumenti basati sulla telemetria.
- Filtraggio dei dati: la capacità di filtrare i dati replicati per un controllo granulare su ciò che gli utenti possono vedere e analizzare.
- Trasformazione dei dati: la capacità di trasformare i dati nel protocollo dell'esportatore in modo che siano utilizzabili dal protocollo preferito dell'utente. Permette l'uso di formati di dati diversi nei vari strumenti.

L'obiettivo di Cisco Telemetry Broker è:

1. Offrire maggiore visibilità negli ambienti di cloud ibrido negli strumenti on-premises (come Secure Network Analytics) tramite la conversione del log di flusso di AWS VPC in IPFIX.
2. Maggiore affidabilità nel monitoraggio, nel rilevamento dello stato di inattività degli utenti e nei servizi ad alta disponibilità. Maggiore affidabilità nel monitoraggio, nel rilevamento dello stato di inattività degli utenti e nei servizi ad alta disponibilità.

Flow Sensor 1300, 3300 e 4300

Flow Sensor è un'appliance di rete che funziona in modo simile a un'appliance di acquisizione di pacchetti tradizionale o IDS, ossia si collega a uno Switch Port Analyzer (SPAN), una porta di mirroring o una porta TAP (Test Access Port) Ethernet. Flow Sensor aumenta la visibilità delle seguenti aree di rete:

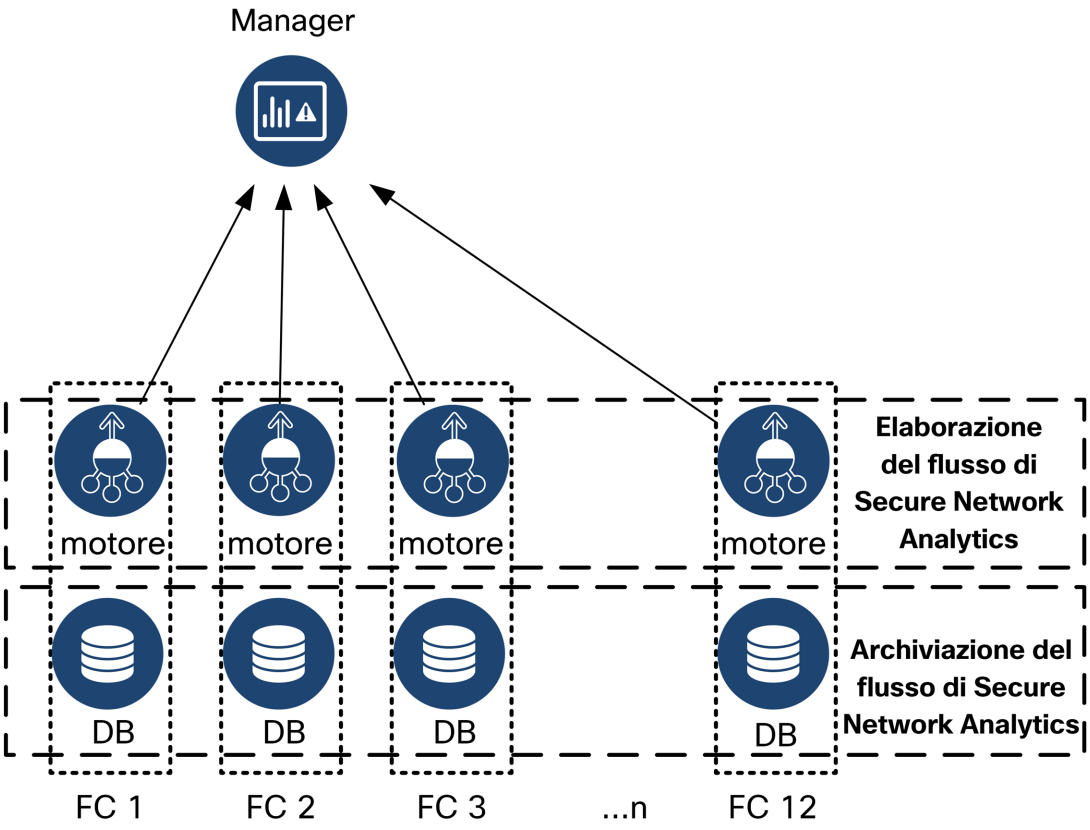
- Dove non è disponibile NetFlow.
- Dove NetFlow è disponibile, ma si desidera una visibilità più approfondita delle metriche delle prestazioni e dei dati del pacchetto.

Indirizzando il Flow Sensor verso un Flow Collector con NetFlow v9, è possibile ottenere statistiche dettagliate sul traffico da NetFlow. Insieme a Secure Network Analytics Flow Collector, Flow Sensor offre informazioni approfondite sulle prestazioni misurate e sugli indicatori comportamentali. Questi indicatori delle prestazioni di flusso offrono informazioni sulla latenza di round-trip introdotta dalla rete o dall'applicazione lato server.

Poiché il Flow Sensor può vedere i dati a livello di pacchetto, può calcolare il tempo di round-trip (RTT), il tempo di risposta del server (SRT) e la perdita di pacchetti per le sessioni TCP. Sono inclusi tutti quei campi nei record NetFlow che vengono inviati al Flow Collector.

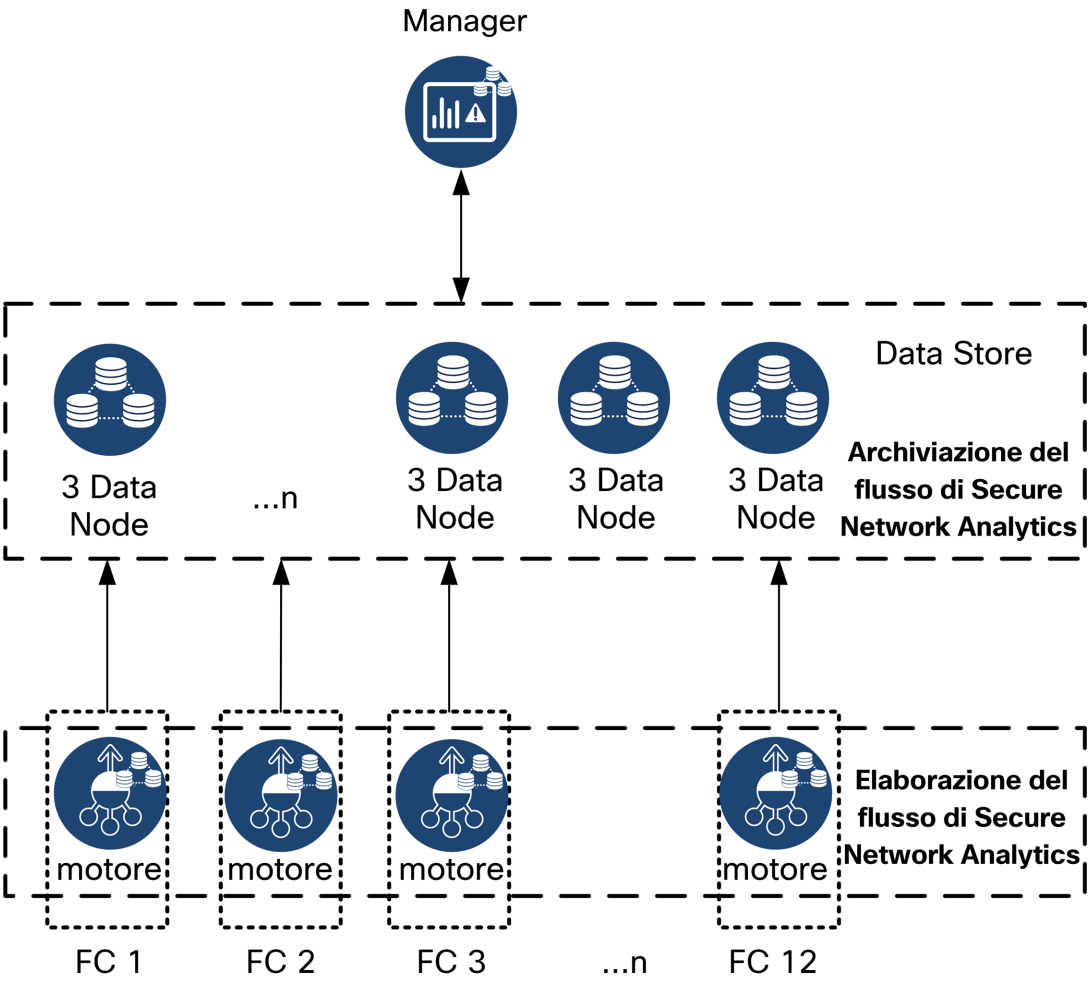
Secure Network Analytics senza Data Store

Nelle implementazioni di Secure Network Analytics senza Data Store, uno o più Flow Collector acquisiscono e deduplicano i dati, eseguono l'analisi e comunicano dati e risultati direttamente al Manager. Per risolvere le query inviate dall'utente, inclusi i grafici e i diagrammi, il Manager interroga tutti i Flow Collector gestiti. Ciascun Flow Collector restituisce i risultati trovati al Manager. Il Manager raccoglie le informazioni dai diversi set di risultati e genera un grafico. In questa implementazione, ciascun Flow Collector memorizza i dati su un database locale. Vedere la figura seguente per un esempio.



Secure Network Analytics con Data Store

In un'implementazione di Secure Network Analytics con Data Store, il cluster del Data Store si trova tra il Manager e i Flow Collector. Uno o più Flow Collector acquisiscono e deduplicano i flussi, eseguono l'analisi e comunicano dati e risultati direttamente al Data Store, distribuendoli all'incirca allo stesso modo a tutti i Data Node. Il Data Store facilita l'archiviazione dei dati e mantiene tutto il traffico centralizzato anziché distribuirlo sui vari Flow Collector, offrendo una maggiore capacità di archiviazione. Vedere la figura seguente per un esempio.



Il Data Store fornisce un archivio centrale per memorizzare i dati di telemetria della rete raccolti dai Flow Collector. Il Data Store comprende un gruppo di Data Node, ciascuno dei quali contiene una parte dei dati e un backup dei dati di un altro Data Node. Mantenendo tutti i dati in un database centralizzato, anziché averli dispersi su più Flow Collector, il Manager può richiamare i risultati delle query più velocemente dal Data Store anziché dover interrogare separatamente tutti i Flow Collector. Il gruppo di Data Store offre una

migliore tolleranza agli errori, una migliore risposta alle query e permette di popolare i grafici e le tabelle più rapidamente.

Query

Per risolvere le query inviate dall'utente, inclusi i grafici e i diagrammi, il Manager interroga il Data Store. Il Data Store trova i risultati corrispondenti nelle colonne pertinenti alla query, quindi recupera le righe corrispondenti e restituisce i risultati al Manager. Il Manager genera il grafico senza dover raccogliere i set di risultati da più Flow Collector. In questo modo si riducono i costi, rispetto a dover interrogare più Flow Collector, e si migliorano le prestazioni.

Archiviazione e tolleranza di errore del Data Store

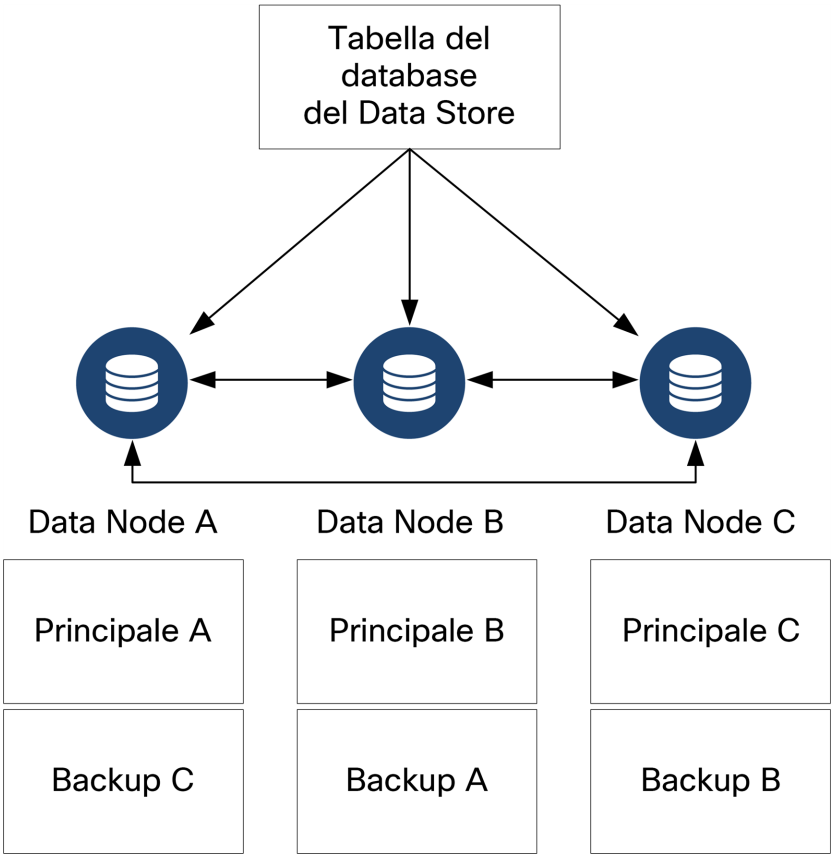
Il Data Store raccoglie i dati dai Flow Collector e li distribuisce in modo uniforme tra i Data Node all'interno del cluster. Ciascun Data Node, oltre a memorizzare una parte dei dati telemetrici complessivi, memorizza anche il backup dei dati di telemetria di un altro Data Node. In questo modo:

- aiuta a bilanciare i carichi,
- distribuisce l'elaborazione tra i vari nodi,
- garantisce che tutti i dati acquisiti nel Data Store abbiano un backup per la tolleranza degli errori,
- consente di aumentare il numero di Data Node per migliorare le prestazioni complessive di archiviazione e interrogazione del database.

Se un Data Node si arresta nel Data Store con 3 o più Data Node, finché il Data Node che contiene il backup resta disponibile e almeno la metà dei Data Node totali è ancora attiva, il Data Store rimane nel suo complesso attivo. Ciò consente di ripristinare la connessione interrotta o il dispositivo guasto. Dopo aver sostituito il Data Node difettoso, il Data Store ne ripristina i dati dal backup esistente memorizzato sul Data Node adiacente e crea un backup di dati su quel Data Node.

Esempio di archiviazione dei dati di telemetria

Per un esempio di come 3 Data Node memorizzano i dati di telemetria, vedere lo schema seguente:



Requisiti di implementazione generali

Prima di iniziare, leggere questa guida per conoscere le procedure, la preparazione, il tempo e le risorse necessari per pianificare l'installazione.

Matrice di compatibilità delle versioni hardware e software

Per informazioni sulla compatibilità, consultare la Matrice di compatibilità delle versioni hardware e software. La matrice è disponibile sul sito Web: https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html.

Specifiche

Scarica la scheda tecnica di ciascuna appliance che deve essere installata. Le specifiche sono disponibili sul sito Web: https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.

Cisco Integrated Management Controller (CIMC)

Dopo aver installato le appliance, accertarsi di configurare Cisco Integrated Management Controller (CIMC) per abilitare l'accesso alla configurazione del server e a una console del server virtuale. È inoltre possibile utilizzare CIMC per monitorare l'integrità dell'hardware.

- **Istruzioni:** fare riferimento a **Connessione al CIMC** e seguire le istruzioni nella Guida alla configurazione della GUI di Cisco UCS serie C Integrated Management Controller.
- **Password predefinita:** durante la configurazione iniziale, accedere a CIMC come admin e digitare **password** nel campo Password.
- **Requisiti della password:** una volta effettuato l'accesso, modificare la password predefinita per proteggere la rete.

Requisiti dell'appliance standard (senza Data Store)

Se si esegue l'installazione di Secure Network Analytics senza un Data Store, installare le appliance seguenti:

Appliance	**Requisiti**
Manager	• Almeno 1 Manager
Flow Collector	• Almeno 1 Flow Collector
Flow Sensor	Facoltativo
Cisco Telemetry Broker	Facoltativo

Per rivedere i requisiti di installazione dell'appliance per Secure Network Analytics con Data Store, fare riferimento a **Requisiti di implementazione del Data Store**.

Requisiti di implementazione di Manager e Flow Collector

Per ciascun Manager e Flow Collector implementati, assegnare un indirizzo IP instradabile alla porta di gestione `eth0`.

Requisiti di implementazione del Data Store

Per implementare Secure Network Analytics con un Data Store, rivedere i seguenti requisiti e suggerimenti per l'implementazione.

Requisiti dell'appliance (con Data Store)

Nella tabella seguente viene fornita una panoramica delle appliance richieste per implementare Secure Network Analytics con Data Store.

Appliance	**Requisiti**
Manager	• Almeno 1 Manager
Data Store	• Almeno 1 o 3 Data Node • Set aggiuntivi di 3 Data Node per espandere il Data Store, per un massimo di 36 Data Node • L'implementazione di 2 soli Data Node in un cluster non è supportata.
Flow Collector	• Almeno 1 Flow Collector
Flow Sensor	Facoltativo
Cisco Telemetry Broker	Facoltativo

⚠ Non aggiornare il BIOS dell'appliance in quanto potrebbe causare problemi di funzionalità.

Requisiti di implementazione di Manager e Flow Collector

Per ciascun Manager e Flow Collector implementati, assegnare un indirizzo IP instradabile alla porta di gestione `eth0`.

- **Configurazione della porta eth0:** è possibile configurare l'uso di una porta o di una porta da 10G con cavo ricetrasmettitore compatibile come porta di gestione `eth0` di Manager e Flow Collector.

- **Throughput:** considerare un throughput da 10G per il ricetrasmettitore se utilizzato con Data Store. Se non si implementa alcun Data Store, è possibile utilizzare qualsiasi ricetrasmettitore compatibile.

Requisiti di implementazione del Data Node

Ogni Data Store è composto da Data Node.

- **Nodi fisici:** ogni Data Node fisico corrisponde allo chassis dello stesso Data Node. È possibile implementare 1, 3 o più Data Node (in set di 3).
- **Nodi virtuali:** quando si scarica un Data Store virtuale, è possibile implementare 1, 3 o più Data Node Virtual Edition (in set di 3).

> Accertarsi che i Data Node siano tutti fisici o tutti virtuali. La combinazione di Data Node fisici e virtuali non è supportata e i dispositivi fisici devono appartenere alla stessa generazione (tutti DS 6200 o tutti DN 6300).

Implementazione di più Data Node

L'implementazione di più Data Node fornisce i massimi risultati in termini di prestazioni. Ad esempio, un'implementazione di Data Store 6300 con 3 Data Node può gestire all'incirca 1,5 milioni di flussi al secondo per circa 90 giorni.

Tenere presente quanto segue:

- **Set di tre:** è possibile raggruppare i Data Node in cluster all'interno del Data Store in multipli di 3, da un minimo di 3 a un massimo di 36. L'implementazione di 2 soli Data Node in un cluster non è supportata.
- **Tutti nodi fisici o tutti nodi virtuali:** accertarsi che i Data Node siano tutti fisici (della stessa generazione) o tutti virtuali. La combinazione di Data Node fisici e virtuali o la combinazione di Data Store 6200 e Data Node 6300 non è supportata.

Metriche hardware supportate (con Analytics abilitato)

Numero di nodi	Flussi al secondo (FPS)	Host interni univoci
1	600.000	1,3 milioni
Almeno 3	600.000	1,3 milioni
Almeno 3	850.000	700.000

> I suggerimenti forniti si basano esclusivamente su considerazioni telemetriche. Le prestazioni effettive possono variare in base ad altri fattori, tra cui il numero di host, l'utilizzo del Flow Sensor, i profili di traffico e altre caratteristiche della rete. Per assistenza sulle dimensioni ottimali, contattare Supporto Cisco.

Metriche hardware supportate (senza Analytics abilitato)

Numero di nodi	Flussi al secondo (FPS)	Host interni univoci
1	Fino a 1 milione	Fino a 33 milioni
Almeno 3	Fino a 3 milioni	Fino a 33 milioni

> Questi numeri vengono generati nei nostri ambienti di test, basandosi su una media di dati degli utenti provenienti da 1,3 milioni di host univoci. Le prestazioni possono subire l'influenza di diversi fattori, quali il numero di host, le dimensioni medie dei flussi e molto altro. Per assistenza sulle dimensioni ottimali, contattare Supporto Cisco.

Implementazione di un singolo Data Node

Se si sceglie di implementare un (1) solo Data Node:

- **Flow Collector:** sono supportati al massimo 4 Flow Collector.
- **Aggiunta di Data Node:** se si implementa un solo Data Node, è possibile aggiungerli all'implementazione in un secondo momento. Per ulteriori informazioni, fare riferimento a **Implementazione di più Data Node**.

> I suggerimenti forniti si basano esclusivamente su considerazioni telemetriche. Le prestazioni effettive possono variare in base ad altri fattori, tra cui il numero di host, l'utilizzo del Flow Sensor, i profili di traffico e altre caratteristiche della rete. Per assistenza sulle dimensioni ottimali, contattare il supporto Cisco.

> Al momento, il Data Store non supporta l'implementazione automatica di Data Node di riserva in caso il Data Node principale diventi inattivo. Per assistenza e istruzioni, contattare il supporto Cisco.

Requisiti di configurazione del Data Node

Per implementare un Data Store, assegnare quanto segue a ciascun Data Node. Le informazioni preparate verranno configurate nell'impostazione iniziale facendo riferimento alla Guida alla configurazione del sistema.

- **Indirizzo IP instradabile (eth0):** per la gestione, l'acquisizione e l'invio di query alle appliance Secure Network Analytics.
- **Configurazione della porta eth0:** è possibile configurare la porta di gestione `eth0` con qualsiasi ricetrasmettitore compatibile.
- **Throughput:** per prestazioni ottimali, si consiglia la connettività 10G per l'uso del Data Store.
- **Comunicazioni tra Data Node:** configurare un indirizzo IP non instradabile dal blocco CIDR `169.254.42.0/24` all'interno di una LAN privata o di una VLAN da usare per le comunicazioni tra Data Node.

  Per prestazioni di throughput migliori, collegare la porta `eth2` del Data Node (o il port-channel contenente le interfacce `eth2` e `eth3`) agli switch per la comunicazione tra Data Node. In quanto parte del Data Store, i Data Node comunicano tra loro.
- **Connessioni di rete:** sono necessarie due connessioni di rete, una connessione da 10G per le comunicazioni di gestione, acquisizione dati e query, una connessione da 10G per le comunicazioni tra Data Node.
- **Connessione aggiuntiva:** il Data Node può facoltativamente supportare il protocollo 802.3ad LACP per la ridondanza di rete e per gestire le criticità nelle comunicazioni tra Data Node. Per abilitarlo, installare una connessione aggiuntiva compatibile con il ricetrasmettitore esistente e un altro switch per stabilire un port-channel sul Data Node.

> Configurare i Data Node in modo che i Data Node adiacenti siano alimentati con alimentatori ridondanti separati. Questa configurazione migliora la ridondanza dei dati e il tempo di attività complessivo del Data Store.

Considerazioni sui requisiti di networking e switching

Nella tabella seguente viene fornita una panoramica delle considerazioni sui requisiti di networking e switching da tenere presenti quando si implementa Secure Network Analytics con un Data Store.

Considerazioni sulla rete	Descrizione
Comunicazioni tra Data Node	• Stabilire una latenza RTT (Round-Trip Time) consigliata inferiore a 200 microsecondi tra i Data Node. • Mantenere lo sfasamento orario tra i Data Node al massimo a 1 secondo. • Stabilire un throughput consigliato di almeno 6,4 Gbps (connessione commutata full duplex da 10 Gbps) tra i Data Node. • Per i Data Node fisici, è sufficiente impostare a 10G il throughput della porta `eth2` per consentire la comunicazione tra i Data Node. La creazione di un port-channel LACP `eth2/eth3` per un throughput fino a 20G permette una comunicazione più veloce tra i Data Node e consente di aggiungere o sostituire rapidamente il Data Node al Data Store, in quanto ciascun Data Node nuovo riceve i dati dai Data Node adiacenti. Tenere presente che il port-channel sulla porta LACP è l'unica opzione di aggregazione disponibile per i Data Node fisici.
Alimentazione del Data Node fisico	• Un'interruzione improvvisa dell'alimentazione su un Data Node fisico potrebbe danneggiare i dati. Utilizzare entrambi gli alimentatori su circuiti separati da gruppi di continuità. • Quando si inizializza il cluster del Data Store, configurare i Data Node alternati in base agli alimentatori usati da ciascuno di essi. In questo modo è possibile ottimizzare la tolleranza d'errore, riducendo al minimo il numero di Data Node inattivi in caso di interruzione dell'alimentazione.

Switching dei Data Node	• È necessario che i Data Node dispongano di una propria VLAN di Layer 2 per comunicare tra loro. È possibile connettere i Data Node fisici a uno switch condiviso o dedicato da 10G. • Consigliamo di collegare i Data Node fisici a due switch per garantire la connettività anche durante le interruzioni e gli aggiornamenti degli switch. A causa della bassa latenza richiesta per la comunicazione tra Data Node, Cisco consiglia una coppia di switch ridondanti, che sono interconnessi e supportano entrambi la VLAN di Layer 2.
Comunicazioni delle appliance Secure Network Analytics	• Manager e i Flow Collector devono essere in grado di raggiungere tutti i Data Node. • I Data Node devono essere in grado di raggiungere il Manager, tutti i Flow Collector e ciascun Data Node.

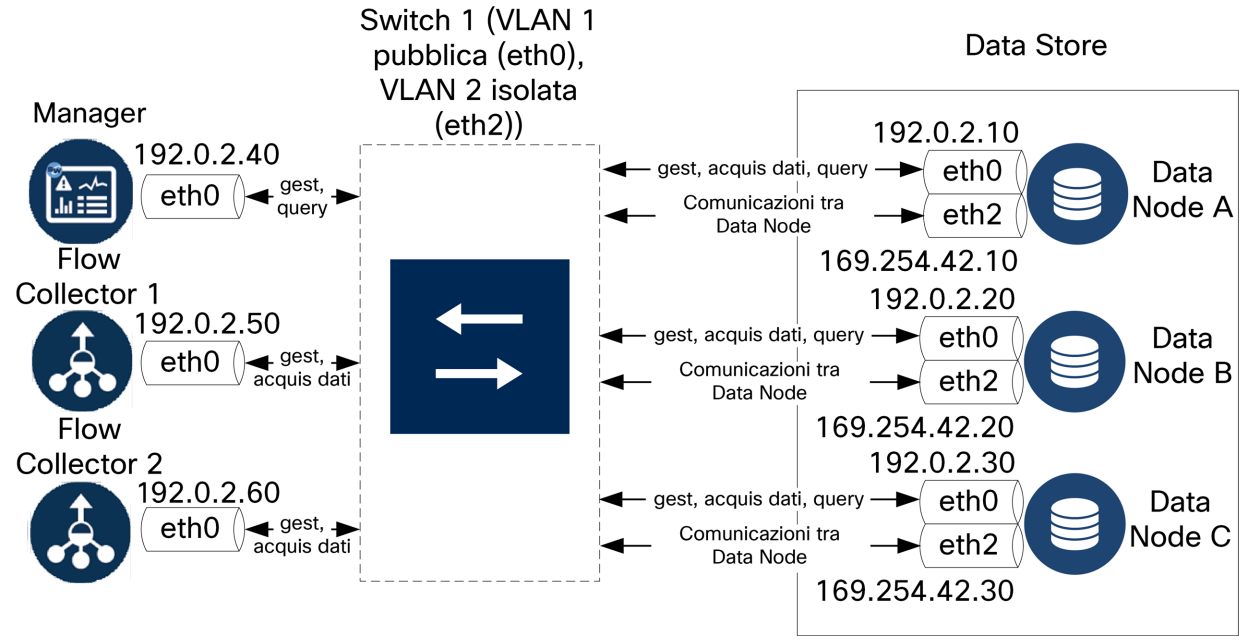
Al momento, il Data Store non supporta l'implementazione automatica di Data Node di riserva in caso il Data Node principale diventi inattivo. Per assistenza e istruzioni, contattare il supporto Cisco.

Esempio di switch fisico

Per abilitare le comunicazioni tra Data Node su `eth2` o sul port-channel `eth2/eth3`, implementare uno switch che supporti velocità di 10G.

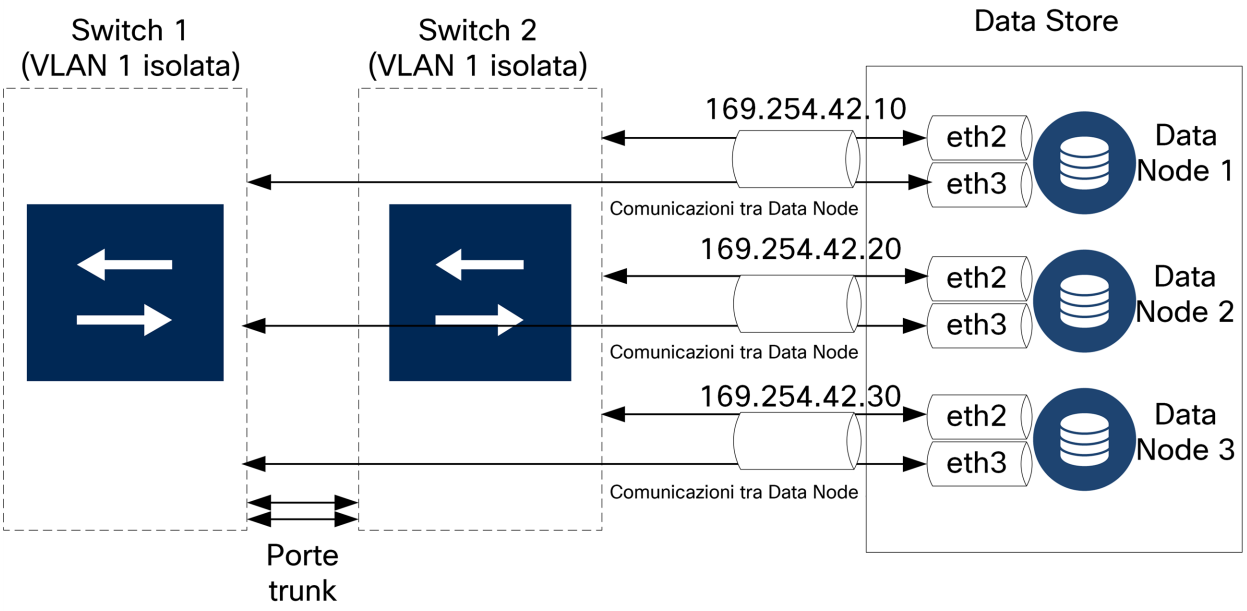
Configurare una LAN o VLAN per le comunicazioni sulla porta `eth0` dei Data Node con Manager e i Flow Collector e una LAN o VLAN isolata per le comunicazioni tra Data Node.

È possibile condividere questi switch con altre appliance, occorre tuttavia creare LAN o VLAN separate per il traffico aggiuntivo delle appliance. Per un esempio, vedere il seguente schema:



Il cluster del Data Store richiede un heartbeat continuo tra i nodi che fanno parte della VLAN isolata. Senza questo heartbeat, i Data Node potrebbero scollegarsi, aumentando il rischio che il Data Store diventi inattivo.

Se si desidera una maggiore ridondanza della rete per pianificare gli aggiornamenti degli switch e le interruzioni pianificate, accertarsi di configurare i Data Node con port-channel dedicati per le comunicazioni tra Data Node. Collegare ogni Data Node a due switch, connettendo ciascuna porta fisica a uno switch diverso. Per un esempio, vedere il seguente schema:



Per assistenza sulla pianificazione e l'implementazione, contattare Cisco Professional Services.

Considerazioni sul posizionamento del Data Store

Posizionare ciascun Data Node in modo che possa comunicare con tutti i Flow Collector, il Manager e tutti gli altri Data Node. Per prestazioni ottimali, posizionare i Data Node e i Flow Collector in modo da ridurre al minimo la latenza di comunicazione e i Data Node e il Manager in modo da avere la maggiore efficacia di esecuzione delle query.

- **Firewall:** consigliamo vivamente di posizionare i Data Node entro il perimetro del firewall, ad esempio in un NOC.
- **Alimentatore:** se il Data Store diventa inattivo a causa di una perdita di alimentazione o un guasto dell'hardware, il rischio di danneggiare o perdere i dati aumenta. Installare i Data Node tenendo sempre in considerazione il tempo di attività.

Se si verifica un'interruzione imprevista dell'alimentazione su un Data Node e l'appliance viene riavviata, l'istanza del database su quel Data Node potrebbe non riavviarsi automaticamente. Per la risoluzione dei problemi e il riavvio manuale del database, fare riferimento alla Guida alla configurazione del sistema.

- **Policy:** verificare che la policy di ripristino dell'alimentazione del Data Node fisico sia impostata su **Restore Last State** (Ripristina ultimo stato), in modo che il Data Node si riavvii automaticamente dopo un'interruzione di alimentazione e cerchi di ripristinare i processi in esecuzione. Per ulteriori informazioni sulla configurazione della policy di ripristino dell'alimentazione in CIMC, vedere la Guida alla configurazione della GUI di UCS serie C.

Requisiti di implementazione di Analytics

Secure Network Analytics usa la modellazione dinamica delle entità per monitorare lo stato della rete. In Secure Network Analytics, per entità si intende qualsiasi oggetto che possa essere monitorato nel tempo, ad esempio un host o un endpoint della rete. La modellazione dinamica delle entità raccoglie informazioni sulle entità in base al traffico trasmesso e alle attività effettuate sulla rete. Per ulteriori informazioni, consultare la guida Analytics: rilevamenti, avvisi e osservazioni.

Per abilitare Analytics, l'implementazione deve essere configurata:

- in un Data Store fisico o virtuale con un numero qualsiasi di Flow Collector,
- con 1 solo dominio Secure Network Analytics Data Store.

1. Configurazione del firewall per le comunicazioni

Affinché le appliance comunichino correttamente, è necessario configurare la rete in modo che i firewall o gli elenchi di controllo degli accessi non blocchino le connessioni richieste. Per configurare la rete in modo che le appliance possano comunicare, attenersi alle informazioni mostrate in questa sezione.

Porte aperte (tutte le appliance)

Rivolgersi all'amministratore di rete per accertarsi che le seguenti porte siano disponibili e abbiano accesso illimitato alle appliance (Manager, Flow Collector, Data Node, Flow Sensor e 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

Porte aperte aggiuntive per Data Node

Inoltre, se si implementano Data Node sulla rete, assicurarsi che le porte seguenti siano aperte e abbiano accesso illimitato:

- TCP 5433
- TCP 5444
- TCP 9450

Porte e protocolli di comunicazione

Nella tabella seguente viene mostrato l'uso delle porte in Secure Network Analytics:

Da (Client)	A (Server)	Porta	Protocollo
PC utente amministratore	Tutte le appliance	TCP/443	HTTPS
Tutte le appliance	Origine ora rete	UDP/123	NTP
Active Directory	Manager	TCP/389, UDP/389	LDAP
Cisco ISE	Manager	TCP/443	HTTPS
Cisco ISE	Manager	TCP/8910	XMPP
Origini log esterni	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	Sistemi di gestione eventi di terze parti	UDP/514	SYSLOG
Flow Sensor	Manager	TCP/443	HTTPS
Flow Sensor	Flow Collector (NetFlow)	UDP/2055	NetFlow
NetFlow Exporter	Flow Collector (NetFlow)	UDP/2055*	NetFlow
sFlow Exporter	Flow Collector (sFlow)	UDP/6343*	sFlow
Manager	UDP Director	TCP/443	HTTPS
Manager	Cisco ISE	TCP/443	HTTPS

Da (Client)	A (Server)	Porta	Protocollo
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 Exporter	UDP/161	SNMP
Manager	LDAP	TCP/636	TLS
Manager	Punti di distribuzione CRL	TCP/80	HTTP
Manager	Risponditori OCSP	TCP/80	OCSP
PC utente	Manager	TCP/443	HTTPS

* Questa è la porta predefinita, ma è possibile configurare qualsiasi porta UDP sull'esportatore.

Porte aperte aggiuntive per Data Store

La tabella seguente elenca le porte di comunicazione che devono essere aperte sul firewall per implementare il Data Store.

N°	**Da (Client)**	**A (Server)**	**Porta**	**Protocollo o scopo**
1	Manager	Flow Collector e Data Node	22/TCP	SSH, necessario per inizializzare il database del Data Store
1	Data Node	Tutti gli altri Data Node	22/TCP	SSH, necessario per inizializzare il database del Data Store e per le attività di amministrazione del database
2	Manager, Flow Collector e Data Node	Server NTP	123/UDP	NTP, richiesto per la sincronizzazione dell'ora
2	Server NTP	Manager, Flow Collector e Data Node	123/UDP	NTP, richiesto per la sincronizzazione dell'ora
3	Manager	Flow Collector e Data Node	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
3	Flow Collector	Manager	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
3	Data Node	Manager	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
4	NetFlow Exporter	Flow Collector – NetFlow	2055/UDP	Acquisizione dati in NetFlow

5	Data Node	Tutti gli altri Data Node	4803/TCP	Servizio di messaggistica tra Data Node
6	Data Node	Tutti gli altri Data Node	4803/UDP	Servizio di messaggistica tra Data Node
7	Data Node	Tutti gli altri Data Node	4804/UDP	Servizio di messaggistica tra Data Node
8	Manager, Flow Collector e Data Node	Data Node	5433/TCP	Connessioni client Vertica
9	Data Node	Tutti gli altri Data Node	5433/UDP	Monitoraggio del servizio di messaggistica Vertica
10	sFlow Exporter	Flow Collector (sFlow)	6343/UDP	Acquisizione dati in sFlow
11	Data Node	Tutti gli altri Data Node	6543/UDP	Servizio di messaggistica tra Data Node

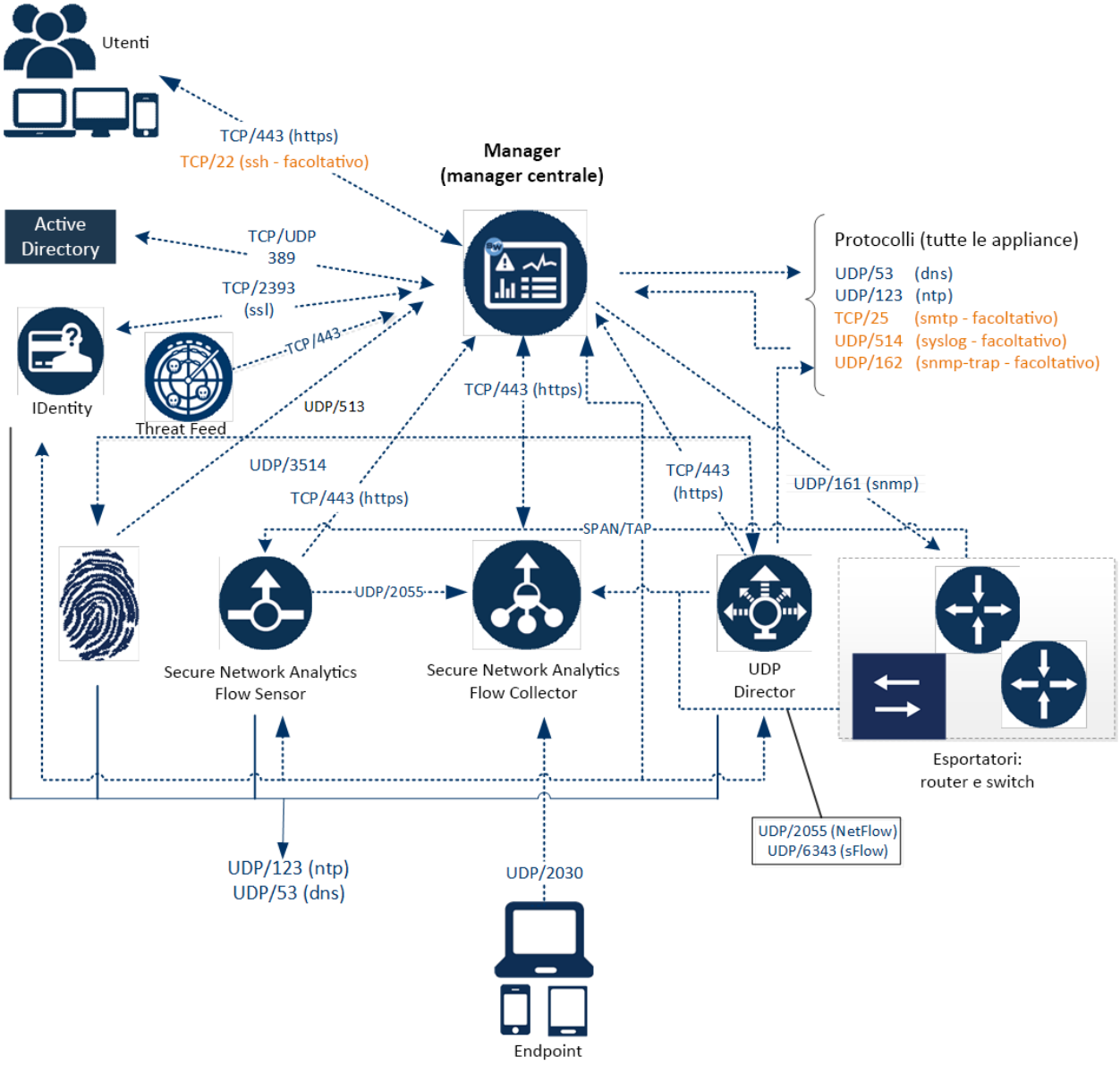
Porte di comunicazione facoltative

La tabella seguente riguarda le configurazioni facoltative determinate dalle esigenze di rete:

Da (Client)	**A (Server)**	**Porta**	**Protocollo**
Tutte le appliance	PC utente	TCP/22	SSH
Manager	Sistemi di gestione eventi di terze parti	UDP/162	Trap SNMP
Manager	Sistemi di gestione eventi di terze parti	UDP/514	SYSLOG
Manager	Gateway e-mail	TCP/25	SMTP
Manager	Threat Feed	TCP/443	SSL
PC utente	Tutte le appliance	TCP/22	SSH

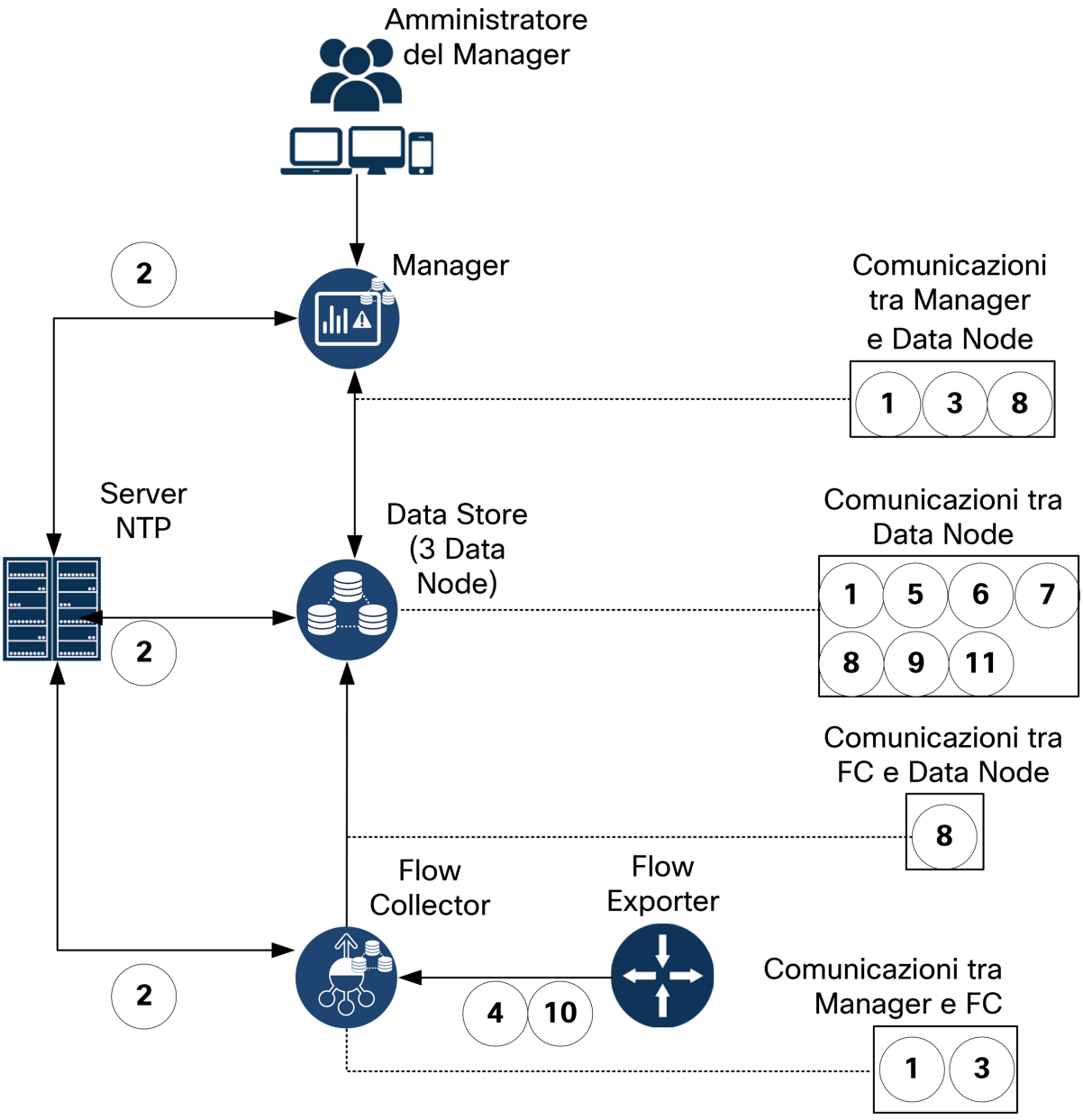
Esempio di implementazione di Secure Network Analytics

Nello schema seguente vengono mostrate le varie connessioni utilizzate da Secure Network Analytics. Alcune di queste porte sono facoltative.



Esempio di implementazione di Secure Network Analytics con Data Store

Come mostrato nella figura seguente, è possibile implementare le appliance Secure Network Analytics in modo strategico per fornire una copertura ottimale dei segmenti di rete principali all'interno della rete, sul suo perimetro o nella zona DMZ.



2. Avvertenze e linee guida per l'installazione

Avvertenze per l'installazione

Prima di installare le appliance Secure Network Analytics serie x3xx, leggere il documento Informazioni sulla conformità alle normative e sulla sicurezza.

Osservare quanto segue:

Avvertenza 1071: definizione delle avvertenze

ISTRUZIONI IMPORTANTI SULLA SICUREZZA

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di utilizzare qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze di sicurezza fornite con il dispositivo.

CONSERVARE QUESTE ISTRUZIONI

Avvertenza 1004: istruzioni per l'installazione

Leggere le istruzioni per l'installazione prima di usare, installare o collegare il sistema all'alimentazione.

Avvertenza 1005: interruttore

Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente).

Avvertenza 1006: avvertenza sullo chassis per il montaggio in rack e la manutenzione

Per evitare infortuni fisici durante il montaggio o la manutenzione di questa unità in un rack, occorre osservare speciali precauzioni per garantire che il sistema rimanga stabile. Le seguenti direttive sono atte a garantire la sicurezza personale:
- Se questa è l'unica unità da montare nel rack, posizionarla sul piano inferiore.
- Se l'unità deve essere montata in un rack parzialmente pieno, caricare il rack

dal basso verso l'alto, con il componente più pesante posizionato sul piano inferiore.

⚠ • Se l'unità deve essere montata in un rack parzialmente pieno, caricare il rack dal basso verso l'alto, con il componente più pesante posizionato sul piano inferiore.

Avvertenza 1015: gestione della batteria

Per ridurre il rischio di incendi, esplosioni o perdite di liquidi o gas infiammabili:

• Sostituire la batteria solo con il modello consigliato dall'azienda produttrice o con un modello equivalente.

⚠ • Non smontare, schiacciare o forare la batteria, né utilizzare strumenti affilati per rimuoverla, non mettere in cortocircuito i contatti esterni e non gettarla nel fuoco.

• Non utilizzare la batteria se deformata o gonfia.

• Non conservare né utilizzare la batteria a temperature maggiori di 60 °C.

• Non conservare né utilizzare la batteria in ambienti con bassa pressione atmosferica inferiore a 69,7 kPa.

Avvertenza 1017: area ad accesso limitato

⚠ L'installazione di questa unità è prevista per aree ad accesso limitato. Solo personale esperto, addestrato o qualificato può entrare in un'area ad accesso limitato.

Avvertenza 191: avvertenza di classe A del Voluntary Control Council for Interference (VCCI) per il Giappone

⚠ Questo è un prodotto di classe A basato sullo standard del VCCI Council. Se l'apparecchiatura viene utilizzata in un ambiente domestico, potrebbero verificarsi interferenze radio, nel qual caso potrebbe essere necessario adottare misure correttive.

Avvertenza 164: requisiti per il sollevamento

⚠ Per sollevare le parti pesanti del prodotto, sono necessarie due persone. Per evitare infortuni, tenere la schiena dritta e sollevarlo piegandosi sulle gambe, non con la schiena.

Avvertenza 256: avvertenza per i dispositivi di classe A in Ungheria

Questa apparecchiatura di classe A deve essere utilizzata e installata correttamente secondo le norme ungheresi applicabili ai dispositivi di classe A EMC (MSZEN55022). L'apparecchiatura di classe A è stata concepita per l'impiego in ambienti commerciali standard in cui sono previste condizioni di installazione e distanze di sicurezza specifiche.

Avvertenza 294: avvertenza per i dispositivi di classe A in Corea

Questo è un dispositivo di Classe A conforme ai requisiti di compatibilità elettromagnetica (ECM) per l'utilizzo in ambito industriale. È necessario che il venditore o l'acquirente ne sia al corrente. Se si vende o si acquista per sbaglio questo tipo di dispositivo, sostituirlo con uno per l'utilizzo in ambito residenziale.

Avvertenza 340: avvertenza per i dispositivi di classe A per CISPR22/EN55022/CISPR32/EN55032

Questo dispositivo è un prodotto di Classe A. Negli ambienti domestici il prodotto può causare interferenze radio; in questo caso può essere necessario prendere misure adeguate.

Avvertenza 1021: circuito SELV

Per evitare shock elettrici, non collegare i circuiti a bassissima tensione di sicurezza (SELV) ai circuiti telefonici (TNV). Le porte LAN includono circuiti SELV, mentre le porte WAN utilizzano circuiti TNV. Alcune porte LAN e WAN utilizzano connettori RJ-45. Prestare attenzione durante il collegamento dei cavi.

Avvertenza 1024: conduttore di messa a terra

Questa apparecchiatura deve essere dotata di messa a terra. Non escludere mai il conduttore di protezione né usare l'apparecchiatura in assenza di un conduttore di protezione installato in modo corretto. Se non si è certi della disponibilità di un adeguato collegamento di messa a terra, richiedere un controllo alle autorità competenti o rivolgersi a un elettricista.

Avvertenza 1028: presenza di più connessioni all’alimentazione

L'unità può avere più di una connessione all'alimentazione elettrica. Per ridurre il rischio di scosse elettriche, scollegare tutti i collegamenti per diseccitare l'unità.

Avvertenza 1029: coprislot e pannelli di copertura

I coprislot e i pannelli di chiusura svolgono tre funzioni importanti: riducono il rischio di scosse elettriche e incendi, limitano le interferenze elettromagnetiche (EMI) che potrebbero causare il malfunzionamento di altre apparecchiature e consentono di convogliare l'aria di raffreddamento nello chassis. Non utilizzare l'apparecchiatura se non sono state installate tutte le schede, i coprislot e i pannelli di chiusura frontali e posteriori.

Avvertenza 1030: installazione dell'apparecchiatura

L'installazione, la sostituzione e la manutenzione dell'apparecchiatura devono essere affidate solo a personale specializzato e qualificato.

Avvertenza 1032: sollevamento dello chassis

Per evitare lesioni personali o danni allo chassis, non tentare mai di sollevare o inclinare lo chassis utilizzando le impugnature sui moduli, come alimentatori, ventole o schede. Questi tipi di maniglie non sono progettati per sostenere il peso dell'unità.

Avvertenza 9001: smaltimento del prodotto

Il prodotto deve essere smaltito in ottemperanza alle normative nazionali vigenti.

Avvertenza 1051: radiazioni laser

Le fibre o i connettori scollegati possono emettere radiazioni laser invisibili. Non fissare lo sguardo sui raggi laser né osservarli direttamente tramite strumenti ottici.

Avvertenza 1055: laser di classe 1/1M

Presenza di radiazioni laser invisibili. Non esporre agli utenti di ottiche telescopiche. Si applica ai prodotti laser di classe 1/1M.

Avvertenza 1008: prodotto laser di classe 1

Questo prodotto è un prodotto laser di classe 1.

Avvertenza 1056: cavo in fibra senza terminazione

L'estremità del connettore o del cavo ottico senza terminazione può emettere radiazioni laser invisibili. Non osservarle direttamente con l'impiego di strumenti ottici. L'osservazione del fascio laser con determinati strumenti ottici (come monocoli, lenti di ingrandimento o microscopi) entro una distanza di 100 mm può provocare danni alla vista.

Tipo di fibra e diametro nucleo (µm)	Lunghezza d'onda (nm)	Potenza massima (mW)	Divergenza di fascio (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

Avvertenza 1089: definizioni di persona addestrata e persona esperta

La persona addestrata è un soggetto istruito e formato da una persona esperta in grado di adottare le precauzioni necessarie quando lavora sulle apparecchiature.

Per persona esperta/qualificata si intende una persona con formazione o esperienza specifica sulla tecnologia delle apparecchiature utilizzate e che ne comprenda i pericoli potenziali.

Avvertenza 1090: installazione effettuata da personale esperto

L'installazione, la sostituzione e la manutenzione dell'apparecchiatura devono essere affidate solo a persone esperte. Per la definizione di persone esperte, vedere l'avvertenza 1089.

Avvertenza 1091: installazione effettuata da personale addestrato

L'installazione, la sostituzione e la manutenzione dell'apparecchiatura devono essere affidate solo a persone addestrate o esperte. Per la definizione di persone addestrate o esperte, vedere l'avvertenza 1089.

Avvertenza 1074: conformità alle normative elettriche locali e nazionali

L'installazione dell'apparecchiatura deve essere conforme alle normative elettriche locali e nazionali.

Avvertenza 2017: avviso di Classe A per FCC

Se l'apparecchiatura viene modificata senza autorizzazione di Cisco, può venire meno la conformità ai requisiti FCC per i dispositivi digitali di classe A. In tal caso, il diritto a utilizzare l'apparecchiatura può risultare limitato dalle norme FCC e l'utente potrà essere tenuto a correggere a proprie spese eventuali interferenze con le comunicazioni radiotelevisive.
Questa apparecchiatura è stato collaudata e rispetta i limiti per i dispositivi digitali di Classe A, ai sensi della normativa FCC, parte 15. Tali limiti sono studiati per garantire un grado di protezione sufficiente contro le interferenze dannose quando l'apparecchiatura viene utilizzata in ambienti commerciali. L'apparecchiatura genera, impiega e può irradiare energia in radiofrequenza e, se non è installata e utilizzata nel rispetto di quanto previsto dal manuale di istruzioni, può essere causa di interferenze dannose per le comunicazioni radio. È probabile che l'utilizzo dell'apparecchiatura in aree residenziali determini interferenze dannose. In tal caso, gli utenti dovranno porvi rimedio a proprie spese.

Avvertenza 2021: avviso di Classe A per il Canada

Questo apparecchio digitale di Classe A è conforme alle norme canadesi ICES-003/NMB-003.

Avvertenza 7001: mitigazione ESD

Questa apparecchiatura potrebbe essere sensibile alle scariche elettrostatiche. Utilizzare sempre un bracciale antistatico alla caviglia o al polso prima di maneggiare l'apparecchiatura. Collegare l'estremità dell'apparecchiatura della fascetta antistatica a una superficie non finita dello chassis dell'apparecchiatura o al connettore antistatico sull'apparecchiatura, se presente.

Avvertenza 7003: requisiti dei cavi schermati per sovratensioni da fulmini all'interno degli edifici

Le porte dell'apparecchiatura o del sottogruppo installate all'interno di edifici devono utilizzare cablaggi e conduttori schermati dotati di connessione a terra su entrambe le estremità.
Su questa apparecchiatura le seguenti porte sono considerate porte per interni:

Avvertenza 7005: sovratensioni da fulmini all'interno degli edifici e guasto dell'alimentazione CA

Le porte dell'apparecchiatura o del sottogruppo installate all'interno di edifici sono adatte al collegamento a cavi interni o comunque non esposti o al solo cablaggio. Le porte dell'apparecchiatura o del sottogruppo installate all'interno di edifici NON DEVONO essere collegate attraverso il metallo alle interfacce connesse alla centrale esterna (OSP) o al suo cablaggio per oltre 6 metri (circa 20 piedi). Queste interfacce sono progettate per l'uso esclusivo all'interno di edifici (porte di tipo 2, 4 o 4a come descritto in GR-1089) e richiedono l'isolamento dal cablaggio dell'OSP esposto. L'aggiunta di dispositivi di protezione primari non è una protezione sufficiente per il collegamento metallico di queste interfacce al cablaggio dell'OSP.
Su questa apparecchiatura le seguenti porte sono considerate porte per interni:

Linee guida per l'installazione

Osservare quanto segue:

> Avvertenza 1047: prevenzione del surriscaldamento
>
> Per evitare che il sistema si surriscaldi, non utilizzarlo in un'area in cui la temperatura ambiente è superiore alla temperatura massima consigliata di 5 - 35 °C.

> Avvertenza 1019: dispositivo di scollegamento principale
>
> Il gruppo spina-presa deve essere sempre accessibile in quanto serve da sistema di disconnessione principale.

> Avvertenza 1075: cavo di alimentazione e adattatore CA
>
> Per l'installazione del prodotto, utilizzare i cavi di collegamento, i cavi di alimentazione, gli adattatori CA e le batterie in dotazione o indicati nelle istruzioni. Se si dovessero usare cavi o adattatori diversi, potrebbero verificarsi guasti e incendi. Le norme giapponesi in materia di sicurezza dei materiali e degli apparecchi elettrici vietano l'utilizzo di cavi con certificazione UL (sui quali è riportato il marchio UL o CSA), in quanto non disciplinati dalle disposizioni di legge che prevedono invece il marchio PSE sul cavo, per tutti i dispositivi elettrici diversi da quelli indicati da CISCO.

> Avvertenza 1073: nessun componente soggetto a manutenzione da parte dell'utente
>
> Non vi sono all'interno componenti soggetti a manutenzione da parte dell'utente. Non aprire.

Per l'installazione di uno chassis, utilizzare le seguenti linee guida:

- Assicurarsi che vi sia spazio sufficiente intorno allo chassis per consentire la manutenzione e un flusso d'aria adeguato. L'aria nello chassis fluisce dalla parte anteriore a quella posteriore.

> Per garantire un corretto flusso d'aria è necessario montare lo chassis in rack per mezzo dei kit guide. Se le unità vengono installate una sopra all'altra o impilate senza kit guide, le prese d'aria sulla parte superiore dello chassis vengono

> ostruite causando il surriscaldamento, l'aumento di velocità delle ventole e un maggiore consumo energetico. Si consiglia di montare lo chassis in rack con kit guide in quanto queste offrono la distanza minima richiesta. L'uso dei kit guide per il montaggio dello chassis non richiede l'uso di distanziatori aggiuntivi.

- Verificare che il climatizzatore possa mantenere lo chassis a una temperatura di 5 - 35 °C.
- Assicurarsi che il rack o l'armadio soddisfi i requisiti di montaggio in rack.
- Assicurarsi che l'alimentazione del sito sia conforme ai requisiti indicati nella scheda tecnica dell'appliance. Se disponibile, è possibile utilizzare un UPS come protezione da possibili guasti nell'alimentazione.

> Evitare i tipi di UPS che utilizzano tecnologia ferro-risonante. Questi tipi di UPS possono diventare instabili con questi sistemi, che possono avere fluttuazioni notevoli in termini di assorbimento di corrente a causa di pattern di traffico dati oscillanti.

Raccomandazioni per la sicurezza

Utilizzare le seguenti informazioni per garantire la propria sicurezza e proteggere lo chassis. Queste informazioni potrebbero non comprendere tutte le situazioni potenzialmente rischiose nell'ambiente di lavoro, quindi prestare attenzione e prendere sempre decisioni ponderate.

Osservare queste linee guida sulla sicurezza:

- Mantenere l'area pulita e priva di polvere prima, durante e dopo l'installazione.
- Tenere gli attrezzi lontani dalle aree di passaggio per evitare che qualcuno possa inciamparvi.
- Non indossare abiti molto larghi o gioielli, come orecchini, braccialetti o collane, che potrebbero restare impigliati nello chassis.
- Indossare gli occhiali protettivi se le condizioni di lavoro potrebbero essere pericolose per gli occhi.
- Non compiere azioni che possono generare eventuali pericoli per le persone o rendere l'apparecchiatura pericolosa.
- Non tentare mai di sollevare un oggetto troppo pesante per una persona sola.

Misure di sicurezza per gli interventi su apparecchiature sotto tensione

> ⚠ Prima di intervenire su uno chassis, assicurarsi che il cavo di alimentazione sia scollegato.

Quando si utilizzano apparecchiature con alimentazione elettrica, attenersi alle seguenti linee guida:

- Non lavorare da soli se sussistono condizioni di potenziale pericolo nella propria area di lavoro.
- Non dare per scontato che l'alimentazione sia scollegata; controllare sempre.
- Verificare attentamente la presenza di eventuali pericoli nell'area di lavoro, ad esempio superfici bagnate, prolunghe di alimentazione senza messa a terra, cavi di alimentazione consumati e assenza di messa a terra.
- In caso di incidente elettrico:
    - Agire con cautela per evitare di subire danni.
    - Scollegare l'alimentazione dal sistema.
    - Se possibile, mandare un'altra persona a chiamare il soccorso medico. Altrimenti, valutare le condizioni della vittima e chiedere aiuto.
    - Stabilire se è necessario praticare la respirazione bocca a bocca o il massaggio cardiaco, quindi intervenire in maniera adeguata.
- Utilizzare lo chassis rispettando le specifiche elettriche indicate e le istruzioni per l’uso del prodotto.

Prevenzione dei danni da scariche elettrostatiche

Le scariche elettrostatiche si verificano quando i componenti elettronici vengono gestiti in modo improprio. Possono danneggiare l'apparecchiatura e compromettere i circuiti elettrici, causando il guasto sporadico o definitivo dell'apparecchiatura.

Attenersi sempre alle procedure di prevenzione delle scariche elettrostatiche quando si rimuovono o si sostituiscono i componenti. Verificare che lo chassis sia collegato alla messa a terra. Indossare un bracciale antistatico, controllando che aderisca alla pelle. Collegare il morsetto della messa a terra a una parte non verniciata del telaio dello chassis in modo da scaricare a terra le tensioni elettrostatiche in totale sicurezza. Per evitare danni e shock elettrostatici, utilizzare il bracciale e il cavo in modo corretto. Se non è disponibile un bracciale antistatico, toccare la parte in metallo dello chassis per scaricare a terra l'eventuale elettricità statica accumulata.

Per operare in sicurezza, controllare periodicamente che il valore di resistenza del bracciale antistatico sia compreso tra 1 e 10 megaohm.

Ambiente di installazione

Per evitare guasti alle apparecchiature e ridurre la possibilità di arresti causati da condizioni ambientali, pianificare la disposizione del sito e il posizionamento delle apparecchiature. In caso di arresto o di un numero insolitamente elevato di errori delle apparecchiature esistenti, queste considerazioni possono servire per individuarne la causa ed evitare problemi futuri.

Considerazioni sull’alimentazione

Quando si installa lo chassis, tenere in considerazione quanto segue:

- Controllare l'alimentazione prima di installare lo chassis per assicurarsi che la sede di installazione sia priva di picchi di corrente e interferenze. Installare uno stabilizzatore di tensione, se necessario, per garantire i voltaggi e i livelli di alimentazione adeguati nella tensione di ingresso dell’appliance.
- Installare la messa a terra adeguata per la sede in modo da evitare danni derivati da fulmini e sbalzi di corrente.
- Lo chassis non ha un intervallo operativo selezionabile dall’utente. Fare riferimento all'etichetta sullo chassis per i corretti requisiti di alimentazione in ingresso dell’appliance.
- Sono disponibili diversi tipi di cavi di alimentazione CA in ingresso per l'appliance; assicurarsi di disporre del tipo corretto per il proprio impianto.
- In caso di utilizzo di alimentatori doppi ridondanti (1+1), si consiglia di utilizzare circuiti elettrici indipendenti per ogni alimentatore.
- Se possibile, installare un gruppo di continuità nella propria sede.

Considerazioni sulla configurazione in rack

Quando si pianifica la configurazione in rack, è opportuno tenere presente alcune considerazioni:

- Se si installa uno chassis in un rack aperto, verificare che il telaio del rack non blocchi le porte di aspirazione o di sfiato.
- Assicurarsi che i rack chiusi godano di un'adeguata ventilazione. Assicurarsi che il rack non contenga un numero eccessivo di apparecchiature poiché tutti gli chassis generano calore. Un rack chiuso deve avere i pannelli laterali finestrati e una ventola per il raffreddamento.

- In un rack chiuso con una ventola nella parte superiore, il caldo generato dalle apparecchiature nella parte inferiore del rack può salire verso l'alto e le porte di aspirazione delle apparecchiature presenti nella parte alta del rack. Assicurarsi di fornire una ventilazione adeguata alle apparecchiature sulla parte bassa del rack.
- L'uso di deflettori contribuisce a separare il flusso d'aria in uscita da quello in entrata e a convogliare l'aria all'interno dello chassis per raffreddarlo. La collocazione ottimale dei deflettori dipende dal percorso del flusso d'aria all’interno del rack. Provando diverse soluzioni, si può determinare come posizionare i deflettori in modo efficace.

3. Montaggio delle appliance

Le appliance Secure Network Analytics possono essere montate direttamente su un rack o un armadio da 19'' standard, su altro armadio disponibile o su una superficie piana. Per il montaggio dell'appliance in un rack o armadio, seguire le istruzioni incluse nei kit di montaggio guide. Quando si sceglie il luogo in cui installare l'appliance, assicurarsi che ci sia una distanza sufficiente dai pannelli anteriore e posteriore per consentire quanto segue:

- Sia possibile vedere chiaramente le spie del pannello anteriore.
- L'accesso alle porte sul pannello posteriore sia sufficiente per un cablaggio senza alcuna restrizione.
- La presa di alimentazione sul pannello posteriore sia raggiungibile da una sorgente di alimentazione CA condizionata.
- Il flusso d'aria intorno all'appliance e attraverso le feritoie non incontri ostruzioni.

Hardware incluso con l'appliance

I seguenti componenti hardware sono forniti con le appliance Secure Network Analytics:

- Cavo di alimentazione CA
- Chiavi di accesso (per piastra anteriore)
- Kit di guide per il montaggio in rack o per il montaggio di piastrine per appliance più piccole
- Ricetrasmettitori compatibili

Hardware aggiuntivo richiesto

Sono richiesti i seguenti componenti hardware aggiuntivi:

- Viti di montaggio per rack da 19" standard
- UPS (Uninterruptible Power Supply) per ciascuna appliance da installare
- Per la configurazione in locale (facoltativo), procedere in uno dei seguenti modi:
    - Laptop con cavo video e cavo USB (per la tastiera)
    - Monitor con cavo video e tastiera con cavo USB

4. Connessione delle appliance alla rete

Utilizzare la stessa procedura per connettere ogni appliance alla rete. L'unica differenza per la connessione consiste nel tipo di appliance di cui si dispone.

1. Revisione delle specifiche

Utilizzare la stessa procedura per connettere ogni appliance alla rete. L'unica differenza per la connessione consiste nel tipo di appliance di cui si dispone.

- **Schede tecniche:** per informazioni dettagliate sulle specifiche di ciascuna appliance, fare riferimento alle Schede tecniche di Secure Network Analytics.
- **Piattaforma UCS:** i dispositivi Cisco x3xx utilizzano tutti la stessa piattaforma UCS, UCSC-C225-M6SX, mentre usano schede NIC, processori, memorie, storage e RAID diversi.
- Quando si configura il sistema, accertarsi di configurare il database e il motore nell'ordine specificato nella Guida alla configurazione del sistema.

2. Connessione dell'appliance alla rete

Per collegare l'appliance alla rete:

1. Collegare un cavo Ethernet alla porta di gestione, nella parte posteriore dell'appliance.
2. Collegare l'altra estremità dei cavi Ethernet allo switch di rete.
3. Collegare i cavi di alimentazione all'alimentatore. Alcune appliance dispongono di due alimentazioni: alimentatore 1 e alimentatore 2.

5. Connessione all'appliance

In questa sezione viene descritto come connettersi all'appliance per la configurazione del sistema.

Scegliere la procedura di connessione:

- **Connessione con tastiera e monitor**
- **Connessione con cavo seriale o console seriale**
- **Connessione con CIMC (richiesto per l'accesso remoto)** Per connettersi all'appliance per l'accesso remoto, adottare questa procedura.

Connessione con tastiera e monitor

Per configurare l'indirizzo IP locale, procedere come segue:

1. Collegare il cavo di alimentazione all'appliance.
2. Premere il pulsante di accensione per attivare l'appliance. Attendere il completamento dell'avvio. Non interrompere il processo di avvio.

> Per fornire alimentazione, potrebbe essere necessario rimuovere il pannello anteriore.
>
> In alcuni modelli, le ventole dell'alimentatore si attivano con il sistema spento. Verificare che il LED sul pannello anteriore sia acceso.
>
> Collegare l'appliance a un UPS. In assenza di alimentazione, il sistema riporta un errore.

3. Collegare la tastiera:
    - Se si dispone di una tastiera standard, collegarla al connettore della tastiera standard.
    - Se si dispone di una tastiera USB, collegarla a un connettore USB.
4. Collegare il cavo video al connettore video. Viene visualizzato il prompt di accesso.
5. Passare alla sezione **6. Configurazione del sistema Secure Network Analytics**.

Connessione con cavo seriale o console seriale

È possibile collegare l'appliance anche con un cavo seriale o una console seriale, ad esempio un laptop con un emulatore di terminale. Nelle istruzioni ad esempio viene usato un laptop.

1. Collegare il laptop all'appliance in uno dei seguenti modi:

    - Collegare un cavo RS232 tra il connettore della porta seriale (DB9) sul laptop e la porta console sull'appliance.
    - Collegare un cavo crossover tra la porta Ethernet del laptop e la porta di gestione dell'appliance.

2. Collegare il cavo di alimentazione all'appliance.
3. Premere il pulsante di accensione per attivare l'appliance. Attendere il completamento dell'avvio. Non interrompere il processo di avvio.

    Per fornire alimentazione, potrebbe essere necessario rimuovere il pannello anteriore.

    In alcuni modelli, le ventole dell'alimentatore si attivano con il sistema spento. Verificare che il LED sul pannello anteriore sia acceso. Collegare l'appliance a un UPS. In assenza di alimentazione, il sistema riporta un errore.

4. Stabilire una connessione con l'appliance dal laptop.

    Utilizzare un emulatore di terminale disponibile per comunicare con l'appliance.

5. Applicare le seguenti impostazioni:

    - BPS: 115200
    - Bit di dati: 8
    - Bit di stop: 1
    - Parità: Nessuna
    - Controllo del flusso: Nessuno

    Vengono visualizzati la schermata e il prompt di accesso.

6. Passare alla sezione **6. Configurazione del sistema Secure Network Analytics**.

Connessione con CIMC (richiesto per l'accesso remoto)

Cisco Integrated Management Controller (CIMC) consente l'accesso alla console di configurazione del server, alla console del server virtuale e ai sistemi di monitoraggio dell'integrità dell'hardware. CIMC viene utilizzato anche nella configurazione del sistema Secure Network Analytics.

1. Seguire le istruzioni nella Guida alla configurazione della GUI di Cisco UCS serie C Integrated Management Controller.
2. Accedere a CIMC come admin e digitare la **password** nel campo Password.
3. Modificare la password predefinita per garantire una maggiore protezione della rete.
4. Passare alla sezione **6. Configurazione del sistema Secure Network Analytics**.

6. Configurazione del sistema Secure Network Analytics

Se l'installazione delle appliance Virtual Edition e/o delle appliance fisiche è stata completata, è possibile configurare Secure Network Analytics in un sistema gestito.

> ⚠ Per configurare Secure Network Analytics, seguire le istruzioni nella Guida alla configurazione del sistema Secure Network Analytics v7.4.2. Questo passaggio è fondamentale per la corretta configurazione e comunicazione del sistema.
>
> Accertarsi di configurare le appliance nell'ordine specificato nella Guida alla configurazione del sistema.

Requisiti di configurazione del sistema

Accertarsi di poter accedere alla console dell'appliance tramite CIMC.

Utilizzare la tabella seguente per preparare le informazioni necessarie per ciascuna appliance.

Requisiti per la configurazione	Dettagli	Appliance
Indirizzo IP	Assegna un indirizzo IP instradabile alla porta di gestione `eth0`.	
Netmask		
Gateway		
Nome host	È richiesto un nome host univoco per ciascuna appliance. Non è possibile configurare un'appliance con lo stesso nome host di un'altra appliance. Inoltre, assicurarsi che i nomi host delle appliance soddisfino i requisiti standard per gli host Internet.	

Nome di dominio	È richiesto un nome di dominio completo per ciascuna appliance. Non è possibile installare un'appliance con un dominio vuoto.	
Server DNS	Server DNS interno per la risoluzione dei nomi	
Server NTP	Server di riferimento ora interno per la sincronizzazione tra i server. Almeno 1 server NTP per ciascuna appliance. Rimuovere il server NTP 130.126.24.53 se presente nell'elenco dei server. Questo server causa problemi e non è più supportato nell'elenco predefinito dei server NTP.	
Mail Relay Server	Server di posta SMTP per l'invio di avvisi e notifiche	
Porta di esportazione di Flow Collector	Obbligatorio solo per i Flow Collector. NetFlow predefinito: 2055	
Indirizzo IP non instradabile all'interno di una LAN privata o di una VLAN (per la comunicazione tra Data Node)	Richiesto solo per i Data Node. • Interfaccia eth2 fisica o port-channel eth2/eth3. La creazione di un port-channel LACP `eth2/eth3` per un throughput fino a 20G permette una comunicazione più veloce tra i Data Node e consente di aggiungere o sostituire rapidamente i Data Node al Data Store. Tenere presente che il port-channel sulla porta LACP è l'unica opzione di aggregazione disponibile per i Data Node fisici. • Interfaccia eth1 virtuale	

	Indirizzo IP: è possibile usare l'indirizzo IP fornito o immettere un valore che soddisfi i seguenti requisiti per le comunicazioni tra Data Node. • **Indirizzo IP non instradabile** dal **blocco CIDR 169.254.42.0/24**, tra 169.254.42.2 e 169.254.42.254. • **Primi tre ottetti:** 169.254.42 • **Subnet:** /24 • **Sequenziale:** per facilitare la manutenzione, selezionare gli indirizzi IP sequenziali (ad esempio, 169.254.42.10, 169.254.42.11 e 169.254.42.12). **Netmask:** La netmask è codificata sull'indirizzo 255.255.255.0 e non può essere modificata.	
Porta di connessione hardware eth0	Richiesto solo per le appliance Secure Network Analytics con Data Store fisiche: • Manager 2300 • Flow Collector 4300 • Data Node Opzioni della porta di connessione fisica eth0: • **SFP+**: ricetrasmettitori supportati	

Supporto tecnico

In caso di necessità, contattare il supporto tecnico:

- Contattare il partner Cisco locale
- Contattare il supporto Cisco
- Per creare una richiesta di assistenza via Web: http://www.cisco.com/c/en/us/support/index.html
- Per creare una richiesta di assistenza tramite e-mail: tac@cisco.com
- Per contattare il supporto telefonico chiamare il numero: 1-800-553-2447 (USA)
- Per conoscere i numeri dell'assistenza in tutto il mondo: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Cronologia delle modifiche

Versione documento	Data di pubblicazione	Descrizione
1_0	11 maggio 2023	Versione iniziale.
1_1	12 maggio 2023	Aggiornato il link alle Informazioni sulla conformità alle normative e sulla sicurezza per i dispositivi serie x3xx.

Informazioni sul copyright