



Cisco Secure Network Analytics

Guida all'installazione dell'appliance hardware serie x2xx 7.4.1



Sommario

Introduzione	5
Panoramica	5
Destinatari	6
Installazione delle appliance e configurazione del sistema	6
Informazioni correlate	6
Terminologia	7
Acronimi di uso comune	7
Informazioni sulle appliance Secure Network Analytics	8
Manager 2210	8
Data Store 6200	8
Flow Collector 4210 e 5210	9
UDP Director 2210	9
Flow Sensor 1210, 3210 e 4240	9
Secure Network Analytics senza Data Store	11
Secure Network Analytics con Data Store	12
Query	13
Archiviazione e tolleranza di errore del Data Store	13
Esempio di archiviazione telemetrica	14
Requisiti di implementazione generali	15
Matrice di compatibilità delle versioni hardware e software	15
Specifiche	15
Cisco Integrated Management Controller (CIMC)	15
Requisiti dell'appliance standard (senza Data Store)	16
Requisiti di implementazione di Manager e Flow Collector	16
Requisiti per l'implementazione del Data Store	17
Requisiti dell'appliance (con Data Store)	17
Requisiti di implementazione di Manager e Flow Collector	17
Requisiti di implementazione del Data Node	18

Implementazione di più Data Node	18
Implementazione di un singolo Data Node	18
Requisiti di configurazione del Data Node	19
Considerazioni sui requisiti di networking e switching	19
Esempio di switch fisico	22
Considerazioni sul posizionamento del Data Store	23
1. Configurazione del firewall per le comunicazioni	25
Porte aperte (tutte le appliance)	25
Porte aperte aggiuntive per Data Node	25
Porte e protocolli di comunicazione	26
Porte aperte aggiuntive per Data Store	28
Porte di comunicazione facoltative	30
Esempio di implementazione di Secure Network Analytics	31
Esempio di implementazione di Secure Network Analytics con Data Store	32
2. Avvertenze e linee guida per l'installazione	33
Avvertenze per l'installazione	33
Linee guida per l'installazione	35
Raccomandazioni per la sicurezza	37
Misure di sicurezza per gli interventi su apparecchiature sotto tensione	37
Prevenzione dei danni da scariche elettrostatiche	38
Ambiente del sito	38
Considerazioni sull'alimentazione	38
Considerazioni sulla configurazione del rack	39
3. Montaggio delle appliance	40
Hardware incluso con l'appliance	40
Hardware aggiuntivo richiesto	40
4. Connessione delle appliance alla rete	41
1. Revisione delle specifiche	41
2. Connessione dell'appliance alla rete	42
5. Connessione all'appliance	43

Connessione con tastiera e monitor	43
Connessione con cavo seriale o console seriale	44
Connessione con CIMC (richiesto per l'accesso remoto)	45
6. Configurazione del sistema Secure Network Analytics	46
Requisiti di configurazione del sistema	46
Supporto tecnico	49

Introduzione

Panoramica

In questa guida viene illustrato come installare le appliance fisiche Cisco Secure Network Analytics serie x2xx (precedentemente Stealthwatch). In questa guida vengono descritte anche le operazioni di montaggio e installazione dell'hardware Secure Network Analytics.



Prima di installare le appliance Secure Network Analytics serie x2xx, leggere il documento [Informazioni sulla conformità alle normative e sulla sicurezza](#).

Componenti hardware della serie x2xx:

Appliance	Codice prodotto
Manager 2210 (precedentemente Stealthwatch Management Console)	ST-SMC2210-K9
Data Store 6200 (tre Data Node)	ST-DS6200-K9 (tre ST-DNODE-G1)
Flow Collector 4210	ST-FC4210-K9
Flow Collector 5210 Engine	ST-FC5210-E
Flow Collector 5210 Database	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

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 di Secure Network Analytics serie x2xx 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 di sistema di [Secure Network Analytics v7.4.1](#).

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 x2xx.
- **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	Scheda di interfaccia 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 x2xx.

Manager 2210

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

Gli utenti che implementano un Data Store possono configurare un Manager 2210 con un'interfaccia SFP+ DAC a 10 Gbps come eth0 per avere un throughput maggiore. Gli utenti che non implementano un Data Store possono configurare come eth0 solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps.

Data Store 6200

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 4210 e 5210

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.

Gli utenti che implementano un Data Store possono configurare un Flow Collector 4210 con un'interfaccia SFP+ DAC a 10 Gbps come eth0 per avere throughput maggiore. Gli utenti che non implementano un Data Store possono configurare come eth0 solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps.



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.

UDP Director 2210

UDP Director consente la replica dei pacchetti UDP ad alta velocità e ad alte prestazioni. UDP Director è utile nella redistribuzione di trap NetFlow, sFlow, syslog o Simple Network Management Protocol (SNMP) a vari collector. Riceve i dati da qualsiasi applicazione UDP senza connessione e poi li ritrasmette a destinazioni diverse, duplicando i dati secondo necessità.

Quando si configura UDP Director con la funzionalità High Availability (HA), è necessario collegare due appliance UDP Director con cavi crossover. Per le istruzioni, vedere

[2. Connessione dell'appliance alla rete](#).

Flow Sensor 1210, 3210 e 4240

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:

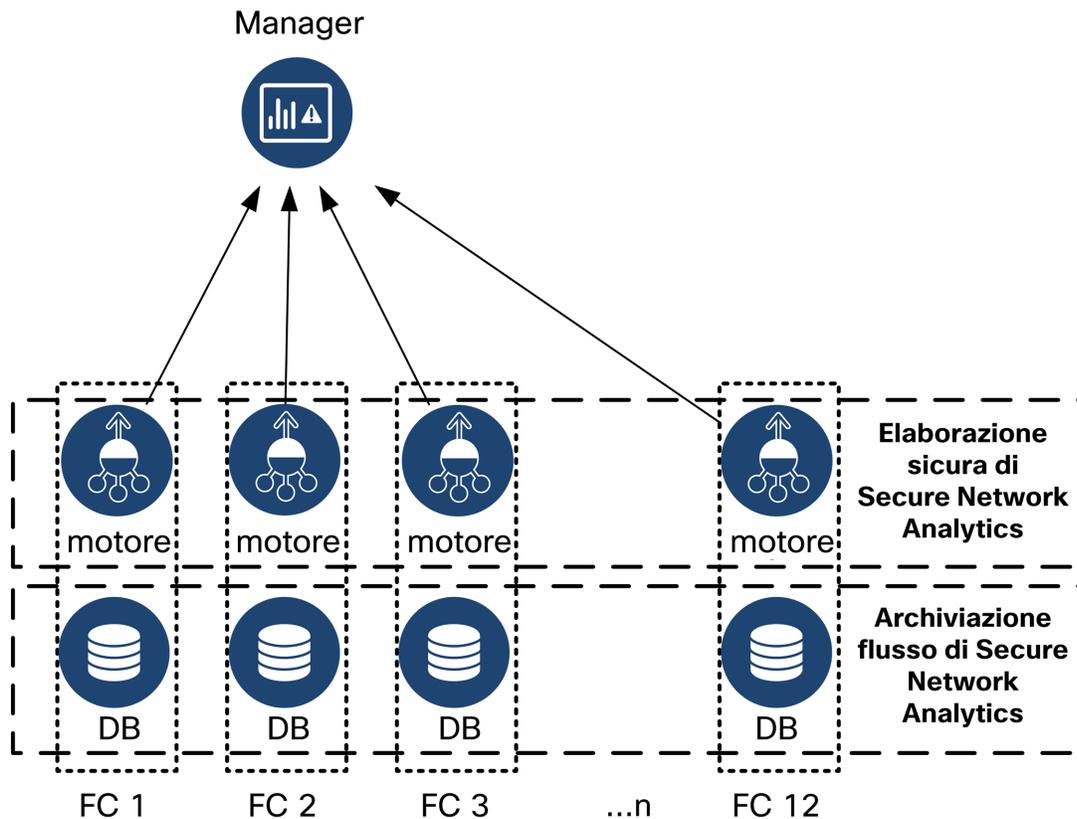
- Dove non è disponibile NetFlow.
- Dove NetFlow è disponibile, ma si desidera una visibilità più approfondita delle metriche delle prestazioni e dei dati del pacchetto.

Indirizzando il Flow Sensor verso il Flow Collector 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.

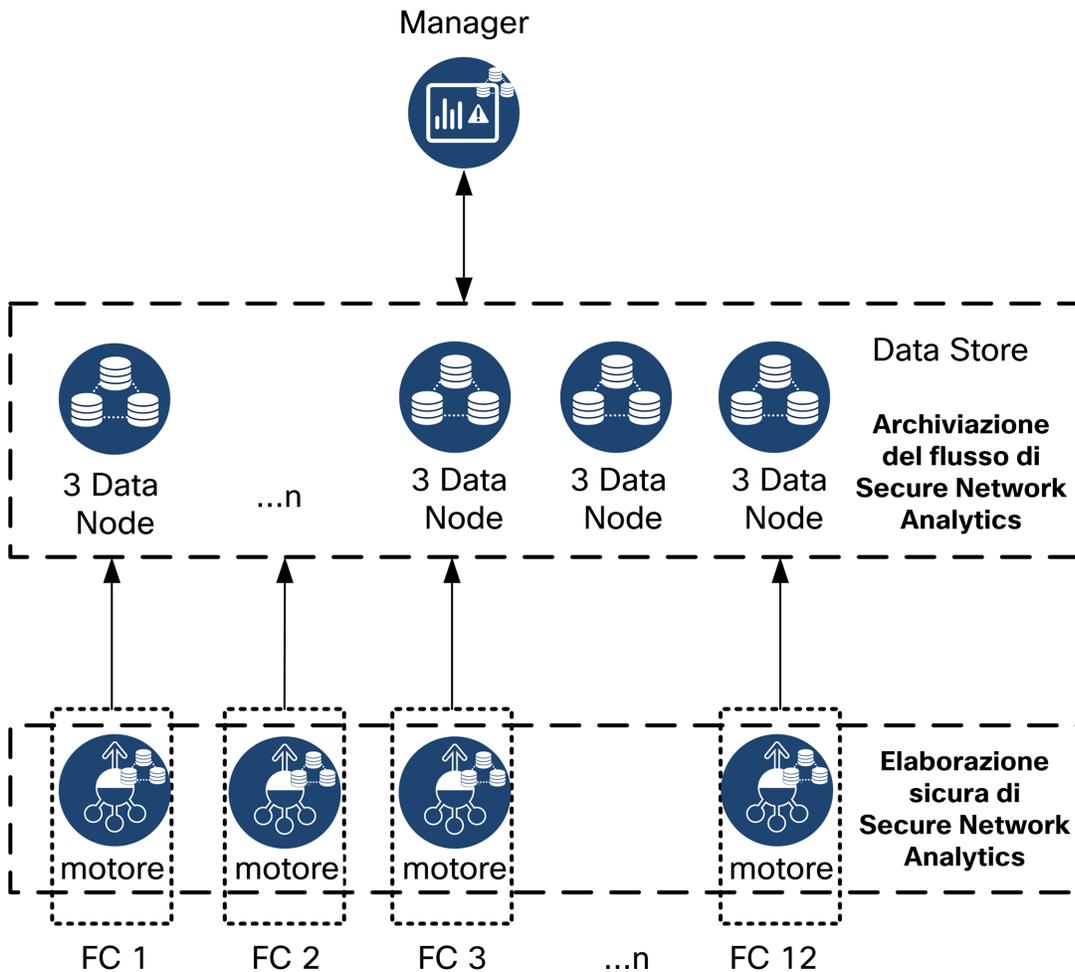
Secure Network Analytics senza Data Store

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 distribuzione, 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

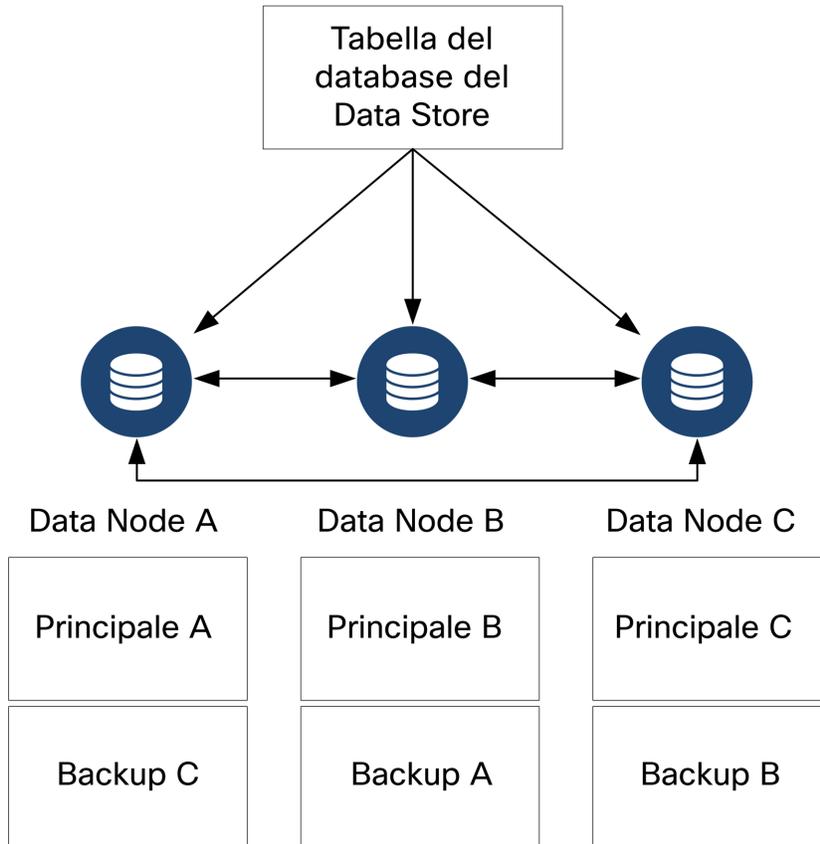
Il Data Store raccoglie i dati dai Flow Collector e li distribuisce in modo uniforme tra i Data Node all'interno del cluster. Ciascun Data Node, oltre a memorizzare una parte dei dati telemetrici complessivi, memorizza anche il backup dei dati di telemetria di un altro Data Node. In questo modo:

- aiuta a bilanciare i carichi
- distribuisce l'elaborazione su ciascun nodo
- garantisce che tutti i dati acquisiti nel Data Store abbiano un backup per la tolleranza di errore
- consente di aumentare il numero di Data Node per migliorare le prestazioni complessive di archiviazione e query

Se un Data Node si arresta nei 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 complessivo rimane 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 telemetrica

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 alla pianificazione dell'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 con CIMC (richiesto per l'accesso remoto)** 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	Requisito
Manager	<ul style="list-style-type: none">• Almeno 1 Manager
Flow Collector	<ul style="list-style-type: none">• Almeno 1 Flow Collector
Flow Sensor	Facoltativo
UDP Director	Facoltativo

Per rivedere i requisiti di installazione dell'appliance per Secure Network Analytics con Data Store, fare riferimento a [Requisiti per l'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 per l'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	Requisito
Manager	<ul style="list-style-type: none"> Almeno 1 Manager
Data Store	<ul style="list-style-type: none"> Almeno 1 o 3 Data Node Set aggiuntivi di tre 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	<ul style="list-style-type: none"> Almeno 1 Flow Collector
UDP Director	Facoltativo
Flow Sensor	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 in rame **BASE-T** da 1G/10G o una porta SFP+ con cablaggio assiale da 10G come porta di gestione `eth0` di Manager e Flow Collector.
- Throughput:** affinché la porta BASE-T in rame possa essere usata con il Data Store, è richiesto un throughput di 10G. Gli utenti che non implementano un Data Store possono configurare come `eth0` solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps.

Requisiti di implementazione del Data Node

Ogni Data Store è composto da Data Node.

- **Hardware:** ogni Data Node fisico corrisponde allo chassis dello stesso Data Node. Quando si acquista un Data Store fisico, si riceve un numero di chassis di Data Node fisici corrispondenti al numero di nodi previsto per il modello di Data Store in uso. Ad esempio, un Data Store DS 6200 fornisce tre chassis fisici per Data Node.
- **Virtual Edition:** 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.

Implementazione di più Data Node

L'implementazione di più Data Node fornisce i massimi risultati in termini di prestazioni. Ad esempio, un Data Store 6200 con 3 Data Node può gestire all'incirca 500.000 flussi al secondo e memorizzare i dati 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 o tutti virtuali. La combinazione di Data Node fisici e virtuali non è supportata.

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 di Flow Sensor, i profili di traffico e altre caratteristiche della rete. Per assistenza sul dimensionamento, contattare il [supporto Cisco](#).

- i** 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 di 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 l'uso di una porta in rame **BASE-T** da 1G/10G o di una porta SFP+ con cablaggio assiale da 10G come porta di gestione `eth0`.
- **Throughput:** affinché la porta BASE-T in rame possa essere usata con il Data Store, è richiesto un throughput di 10G.
- **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.

- **Conessioni di rete:** due connessioni di rete da 10G, una per le comunicazioni di gestione, acquisizione e query, una per le comunicazioni con i Data Node.
- **Connessione e switch aggiuntivi:** facoltativamente, solo sui Data Node fisici, per la ridondanza di rete e la criticità delle comunicazioni tra Data Node, installare un'ulteriore connessione da 10G e uno switch aggiuntivo per stabilire un port-channel sul Data Node.

- i** 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	<ul style="list-style-type: none"> • 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 <code>eth2</code> per consentire la comunicazione tra i Data Node. La creazione di un port-channel <code>eth2/eth3</code> per un throughput fino a 20G permette una comunicazione più veloce tra i Data Node e una più veloce aggiunta o sostituzione di Data Node al Data Store, in quanto ciascun Data Node nuovo riceve i dati dai Data Node adiacenti.
Alimentazione del Data Node fisico	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.



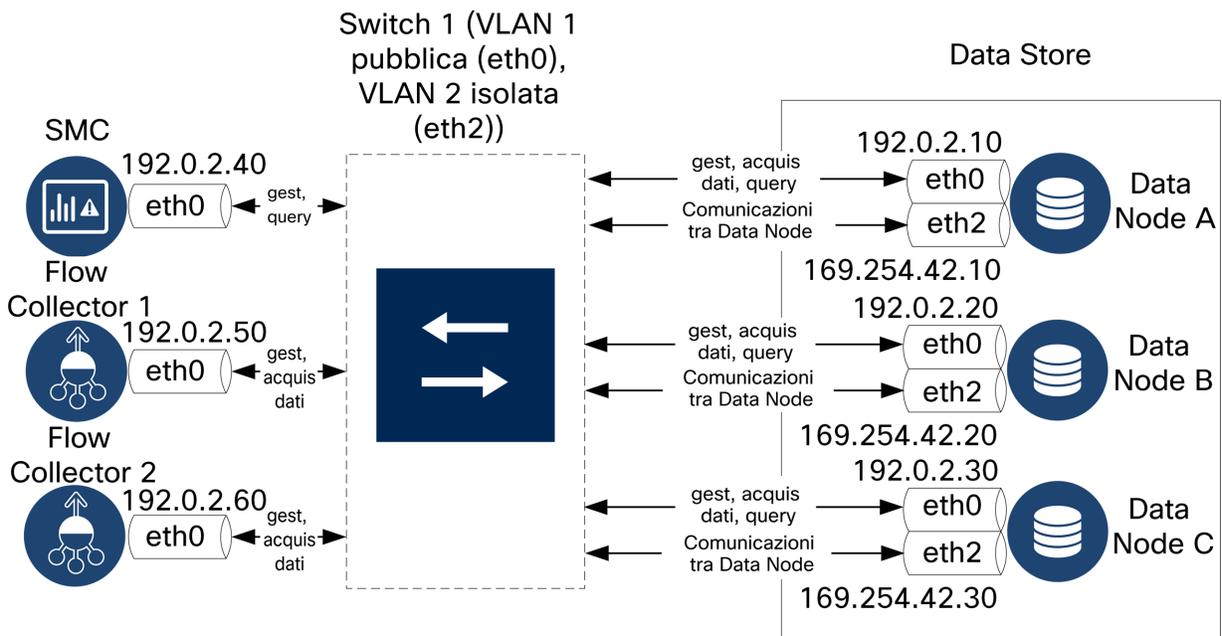
Al momento, il Data Store non supporta l'implementazione automatica di Data Node di riserva in caso il Data Node principale diventi inattivo. Per assistenza e istruzioni, contattare il [supporto Cisco](#).

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.

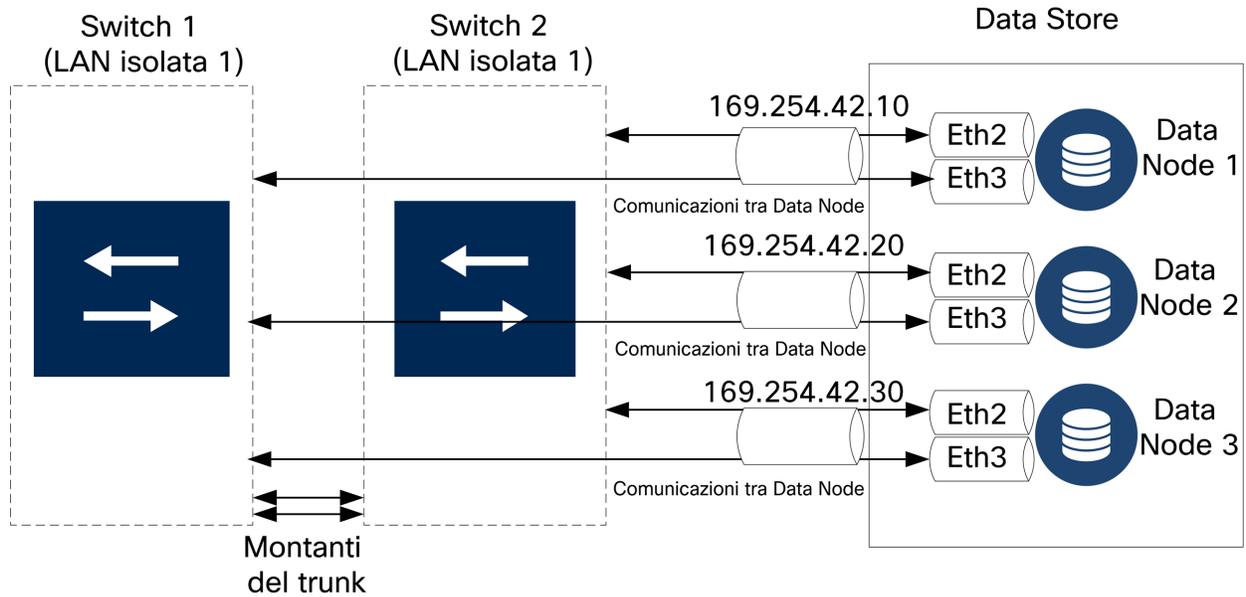
Configurare una LAN o VLAN per le comunicazioni sulla porta `eth0` dei Data Node con Manager e i Flow Collector e una LAN o VLAN isolata per le comunicazioni tra Data Node.

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 di 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 riavvia automaticamente dopo un'interruzione di alimentazione e cerca 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](#).

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 aperte 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	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
Identity	Manager	TCP/2393	SSL
Esportatori NetFlow	Flow Collector (NetFlow)	UDP/2055*	NetFlow
Esportatori sFlow	Flow Collector (sFlow)	UDP/6343*	sFlow
Manager	Cisco ISE	TCP/443	HTTPS
Manager	Cisco ISE	TCP/8910	XMPP

Da (Client)	A (Server)	Porta	Protocollo
Manager	DNS	UDP/53	DNS
Manager	Flow Collector	TCP/443	HTTPS
Manager	Flow Sensor	TCP/443	HTTPS
Manager	Identity	TCP/2393	SSL
Manager	Esportatori di flussi	UDP/161	SNMP
Manager	LDAP	TCP/636	TLS
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	Esportatori NetFlow	Flow Collector - NetFlow	2055/UDP	Inserimento 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	Esportatori sFlow	Flow Collector (sFlow)	6343/UDP	Inserimento sFlow
11	Data Node	Tutti gli altri Data Node	6543/UDP	Servizio di messaggistica tra Data Node

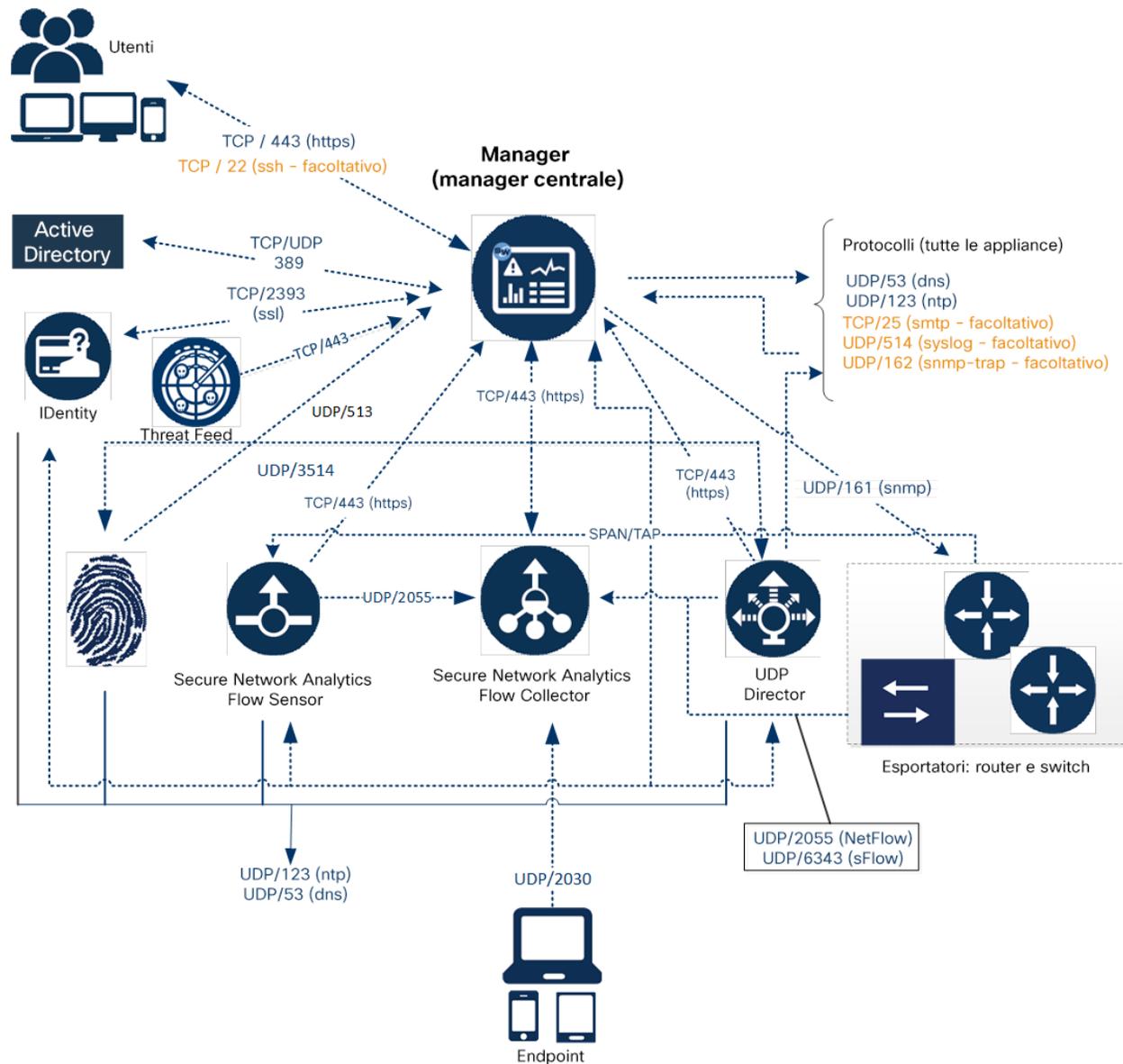
Porte di comunicazione facoltative

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

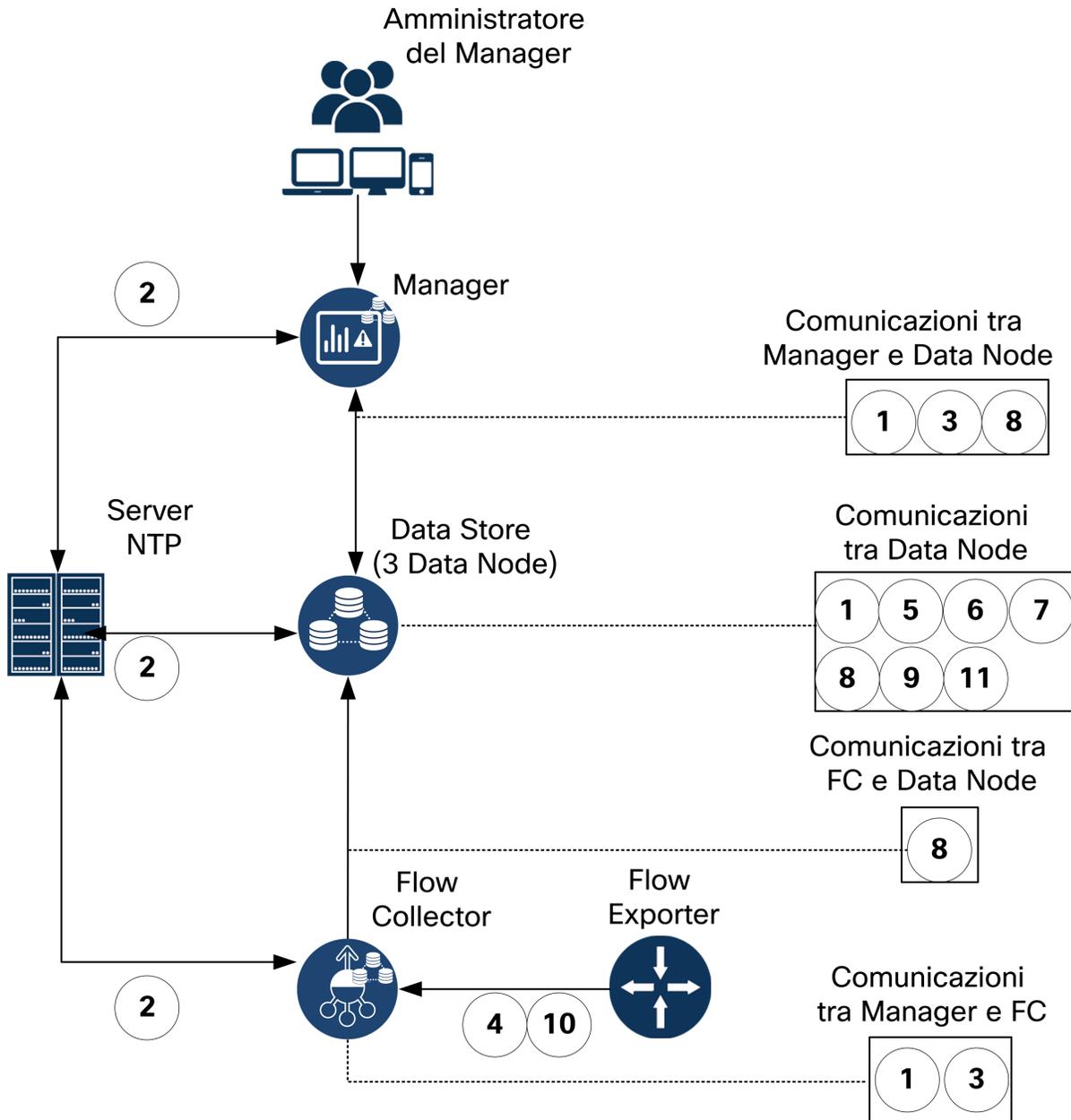
Esempio di implementazione di Secure Network Analytics

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 x2xx, 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 fornite con il dispositivo.

CONSERVARE QUESTE ISTRUZIONI

Avvertenza 1005: interruttore

 Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia una classe superiore a 120, 15 A per gli Stati Uniti (250 V, 16 A per l'Unione europea)

Avvertenza 1004: istruzioni per l'installazione

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

Avvertenza 12: avvertenza sulla disconnessione dell'alimentazione

 Prima di intervenire su uno chassis o di lavorare vicino agli alimentatori, scollegare il cavo di alimentazione sulle unità CA; scollegare l'alimentazione all'interruttore automatico sulle unità CC.

Avvertenza 43: avvertenza per la rimozione degli oggetti preziosi

- ⚠ Prima di utilizzare apparecchiature collegate alle linee elettriche, rimuovere eventuali gioielli e accessori in metallo (anelli, collane e orologi) indossati. Poiché gli oggetti metallici si riscaldano se collegati all'alimentazione e alla messa a terra, si rischia di subire gravi ustioni oppure l'oggetto stesso può saldarsi ai terminali.

Avvertenza 94: avvertenza sul bracciale antistatico

- ⚠ Durante questa procedura, indossare il bracciale antistatico per la messa a terra in modo da evitare danni alla scheda dovuti a scariche elettrostatiche. Non toccare direttamente con la mano o con strumenti metallici il backplane per evitare il rischio di scosse elettriche.

Avvertenza 1045: protezione contro cortocircuiti

- ⚠ Per questo prodotto è necessario predisporre la protezione contro i cortocircuiti (sovracorrente) nell'ambito dell'impianto dell'edificio. Installare solo in conformità con le normative nazionali e locali che regolano il cablaggio.

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 1040: smaltimento del prodotto

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

Avvertenza 1074: conformità alle normative elettriche locali e nazionali



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

Avvertenza 19: avviso di alimentazione TN



Il dispositivo è progettato per funzionare con sistemi elettrici TN.

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 (41 - 95 °F)

Avvertenza 1019: dispositivo di scollegamento principale



Il gruppo spina-presa deve essere sempre accessibile in quanto serve da sistema di disconnessione principale.

Avvertenza 1005: interruttore



Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia una classe superiore a 120, 15 A per gli Stati Uniti (250 V, 16 A per l'Unione europea)

Avvertenza 1074: conformità alle normative elettriche locali e nazionali



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

Dichiarazione 371: 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 (41 - 95 °F).
- 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 del sito

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 in ingresso CA 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 del rack

Quando si pianifica la configurazione del rack, è opportuno tenere presente alcuni punti:

- 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 essere diretto verso l'alto e nelle porte di aspirazione delle apparecchiature sovrastanti presenti nel rack. Assicurarsi di fornire una ventilazione adeguata alle apparecchiature sul fondo del rack.
- L'uso di deflettori contribuisce a separare il flusso d'aria in uscita da quello in entrata e ad aspirare l'aria per il raffreddamento nello chassis. 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 inclusi 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 piastrelle per appliance più piccole
- Per Flow Collector 5210, cavo SFP da 10 GB

Hardware aggiuntivo richiesto

Sono richiesti i seguenti componenti hardware aggiuntivi:

- Viti di montaggio per rack da 19" standard
- UPS (Uninterruptible Power Supply, gruppo statico di continuità) per ciascuna appliance da installare
- Per la configurazione in locale (opzionale), 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 delle specifiche:** per informazioni dettagliate sulle specifiche di ciascuna appliance, fare riferimento alle Schede delle specifiche di [Secure Network Analytics](#).
- **Piattaforma UCS:** tutti i componenti di Cisco x2xx utilizzano la stessa piattaforma UCS, UCSC-C220-M5SX, eccetto Flow Collector 5210 DB, che usa UCSC-C240-M5SX. Gli elementi che variano nelle appliance sono le schede NIC, il processore, la memoria, i sistemi di archiviazione e RAID.
- **Manager 2210:** gli utenti che implementano un Data Store possono configurare un Manager 2210 con un'interfaccia SFP+ DAC da 10 Gbps come eth0 per avere un throughput maggiore. Gli utenti che non implementano un Data Store possono configurare come eth0 solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps.
- **Flow Collector 4210:** gli utenti che implementano un Data Store possono configurare un Flow Collector 4210 con un'interfaccia SFP+ DAC da 10 Gbps come eth0 per avere un throughput maggiore. Gli utenti che non implementano un Data Store possono configurare come eth0 solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps.
- **Flow Collector 5210:** Flow Collector 5210 è composto da due server connessi (motore e database) che funzionano come singola appliance. Per questo motivo, l'installazione è leggermente diversa dalle altre appliance. Innanzitutto, collegarle tra loro direttamente tramite un cavo Cross Connect SFP+ DA 10G. Quindi, connettersi alla rete.



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

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 almeno una porta monitor per i Flow Sensor e gli UDP Director.
 - **UDP Director High Availability:** collegare due UDP Director con cavi crossover. Collegare la porta eth2 di un UDP Director alla porta eth2 del secondo UDP Director. Analogamente, collegare la porta eth3 di ciascun UDP Director con un secondo cavo crossover. Il cavo può essere in fibra ottica o in rame.
 - **Etichetta Ethernet:** prendere nota dell'etichetta Ethernet (eth2, eth3, ecc.) per ciascuna porta. Queste etichette corrispondono alle interfacce di rete (eth2, eth3, ecc.) utilizzate nella configurazione del sistema.
3. Collegare l'altra estremità dei cavi Ethernet allo switch di rete.
4. 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 dal connettore della porta seriale (DB9) sul laptop alla porta console dell'appliance.
 - Collegare un cavo crossover dalla porta Ethernet del laptop alla 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 di sistema di Secure Network Analytics v7.4.1](#). Questo passaggio è fondamentale per la corretta configurazione e comunicazione 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 <code>eth0</code> .	
Netmask		
Gateway		
Broadcast		
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. <ul style="list-style-type: none"> • Interfaccia eth2 fisica o port-channel eth2 / eth3 • Interfaccia eth1 virtuale <p>Indirizzo IP: è possibile usare l'indirizzo IP fornito o immettere un valore che soddisfi i seguenti requisiti per le comunicazioni tra Data Node.</p> <ul style="list-style-type: none"> • 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 	

	<ul style="list-style-type: none"> • 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). <p>Netmask:</p> <p>La netmask è codificata sull'indirizzo 255.255.255.0 e non può essere modificata.</p>	
Porta di connessione hardware eth0	<p>Richiesto solo per le appliance Secure Network Analytics con Data Store fisiche:</p> <ul style="list-style-type: none"> • Manager 2210 • Flow Collector 4210 • Data Node <p>Opzioni della porta di connessione fisica eth0:</p> <ul style="list-style-type: none"> • SFP+: porta in fibra ottica SFP+/DAC da 10G per eth0. • BASE-T: 100Mbs/1GbE/10GbE <p>Porta in rame BASE-T per eth0. BASE-T è l'impostazione predefinita.</p>	

Supporto tecnico

In caso di necessità, contattare il supporto tecnico:

- Contattare il partner Cisco locale
- Contattare il supporto Cisco
- Per aprire una richiesta di assistenza via Web:
<http://www.cisco.com/c/en/us/support/index.html>
- Per aprire 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>

Informazioni sul copyright

Cisco e il logo Cisco sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi. Per visualizzare un elenco di marchi Cisco, visitare il sito a questo indirizzo: <https://www.cisco.com/go/trademarks>. I marchi commerciali di terze parti citati sono proprietà dei rispettivi titolari. L'uso del termine "partner" non implica una relazione di partnership tra Cisco e altre aziende. (1721R)