Cisco Stealthwatch

Guida all'installazione e alla configurazione dell'hardware di Data Store

Sommario

Introduzione all'installazione e alla configurazione dell'hardware del Data Store

Panoramica

In questa guida viene spiegato come installare il StealthwatchData Store come parte dell'implementazione di uno Stealthwatch System. Inoltre vengono descritti i componenti di Stealthwatch System e come sono collocati nel sistema, in particolare rispetto al Data Store.

Nel presente capitolo vengono trattati i seguenti argomenti:

Destinatari

La presente guida è destinata ai responsabili dell'installazione dei componenti hardware di Stealthwatch. Inoltre, si presume la conoscenza generale dei dispositivi di rete, come i Flow Collector e la Stealthwatch Management Console.

Per informazioni sulla configurazione dei prodotti Stealthwatch System, fare riferimento alla *Guida alla configurazione di Stealthwatch System*.

Come usare la guida

Oltre all'introduzione, la guida è divisa nei seguenti capitoli:

Capitolo	Descrizione
Nozioni base e architettura del Data Store	Vengono descritti i concetti fondamentali del database del Data Store e l'architettura base per l'implementazione del Data Store con una SMC e i Flow Collector.
Prerequisiti di implementazione del Data Store e suggerimenti	Viene descritto l'hardware di Stealthwatch compatibile con il Data Store e vengono forniti i requisiti e i suggerimenti per l'implementazione del Data Store, incluse le porte di comunicazione da aprire.

Capitolo	Descrizione
Panoramica dell'implementazione di Stealthwatch Data Store	Viene fornita una panoramica dettagliata per implementare le appliance Stealthwatch in modo da usarle con un Data Store.
Installazione dell'hardware del Data Store	Viene fornita una panoramica completa di come implementare le appliance Stealthwatch per l'uso con un Data Store e le istruzioni di configurazione per inizializzare il database del Data Store.
Configurazione della durata di conservazione dei dati nel Data Store	Vengono fornite informazioni su come configurare il periodo di conservazione dei dati nel Data Store.
Fasi successive dell'installazione del Data Store	Vengono descritti i passaggi successivi all'implementazione e alla configurazione del Data Store.
Manutenzione del Data Store	Vengono descritte le attività di manutenzione del Data Store.
Risoluzione dei problemi di implementazione del Data Store	Vengono descritti i problemi comuni rilevati durante il processo di installazione del Data Store e vengono suggerite le opportune soluzioni.
Appendice A. Preparazione dell'installazione	Vengono forniti per l'installazione dell'hardware.
Appendice B. Installazione dell'hardware di Stealthwatch	Viene fornita una panoramica dell'installazione delle appliance Stealthwatch, la procedura di configurazione iniziale per assegnare un indirizzo IP e altre

Capitolo	Descrizione
	informazioni sulla gestione.
Appendice C. Configurazione delle appliance	Viene fornita una panoramica dello strumento Appliance Setup Tool usato per configurare le appliance Stealthwatch.

Nozioni base e architettura del Data Store

> **Non** installare un StealthwatchData Store autonomamente. Se si pensa di acquistare StealthwatchData Store, rivolgersi ai Cisco Professional Services per consigli sulla posizione, l'implementazione e la configurazione nell'ambito del progetto complessivo di Stealthwatch.

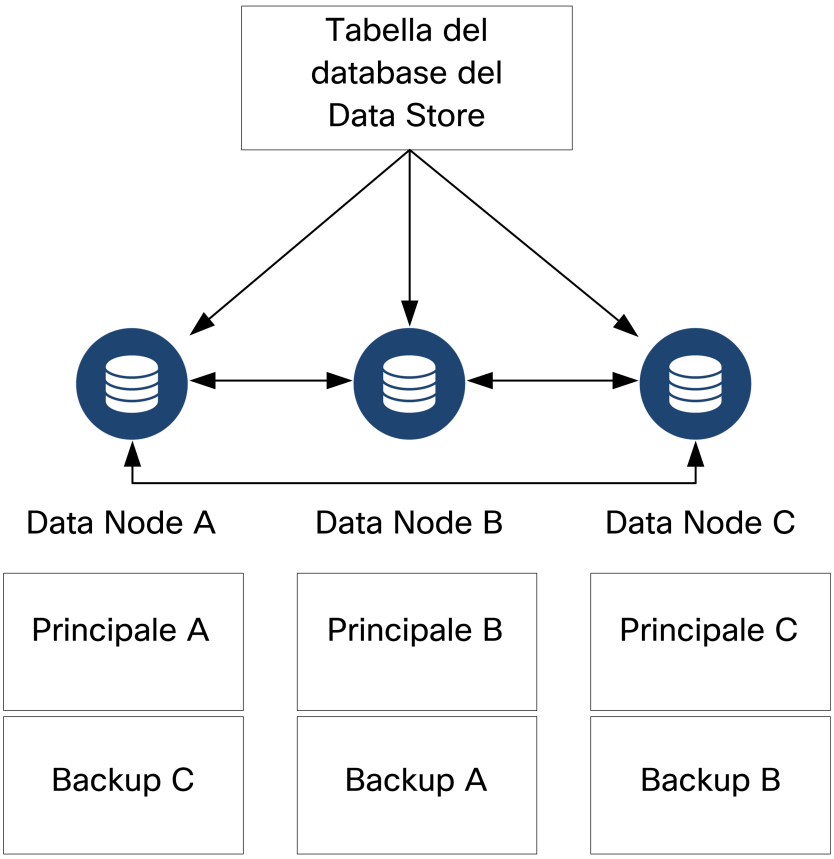
Stealthwatch Data Store fornisce un archivio centrale per memorizzare i dati di telemetria della rete raccolti dai Stealthwatch Flow Collector. Data Store è composto da un gruppo di Data Node, ciascuno dei quali contiene una parte dei dati e un backup dei dati di un altro Data Node. Mantenendo tutti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

Archiviazione e tolleranza agli errori del Data Store

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

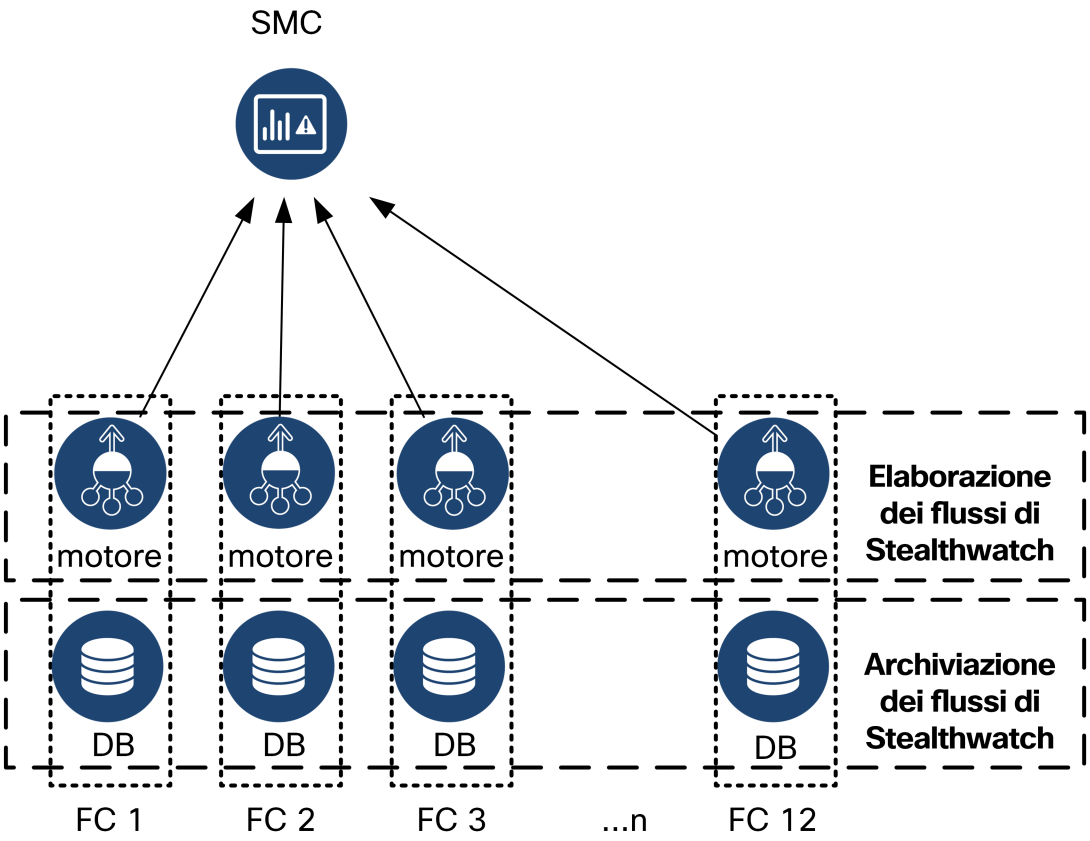
- aiuta a bilanciare i carichi
- distribuisce l'elaborazione su ciascun nodo
- garantisce che tutti i dati acquisiti nel Data Store abbiano un backup per la tolleranza agli errori
- consente di aumentare il numero di Data Node per migliorare le prestazioni complessive di archiviazione e query

Se un nodo si arresta, finché il nodo che contiene il backup è ancora disponibile e almeno la metà del numero totale di Data Node è ancora attiva, il Data Store complessivo rimane attivo. Ciò permette di riparare la connessione interrotta o l'hardware guasto; dopo aver sostituito il Data Node guasto, 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. Per un esempio di come i Data Node memorizzano i dati di telemetria, vedere lo schema seguente:

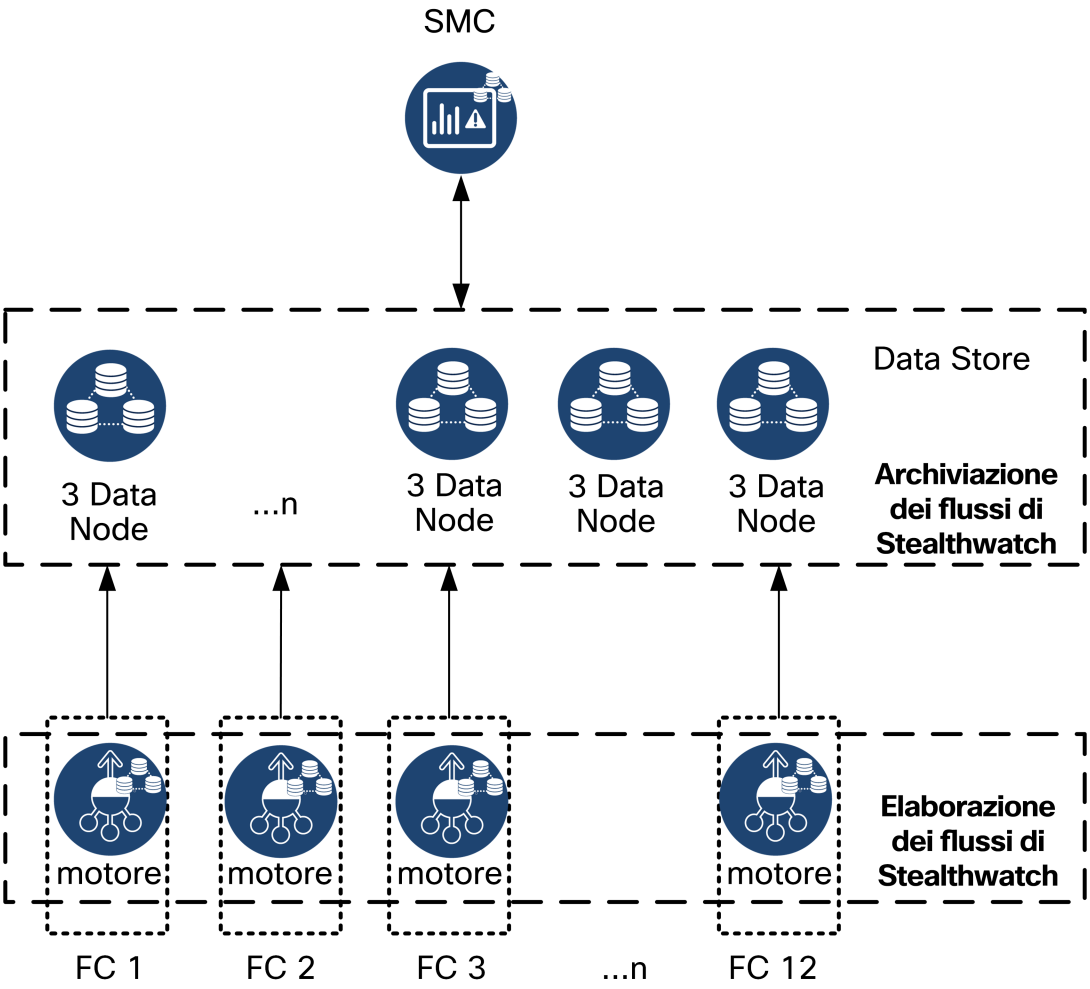


Architettura di implementazione di Stealthwatch del Data Store

In una tradizionale distribuzione di Stealthwatch senza un Data Store, uno o più Flow Collector acquisiscono e deduplicano i dati, eseguono l'analisi e comunicano dati e risultati direttamente all'SMC. Per risolvere le query inviate dall'utente, inclusi grafici e diagrammi, l'SMC interroga tutti i Flow Collector gestiti. Ciascun Flow Collector restituisce i risultati corrispondenti all'SMC. L'SMC raccoglie le informazioni dai diversi set di risultati, quindi genera un grafico. In questa distribuzione, ciascun Flow Collector memorizza i dati su un database locale. Vedere la figura seguente per un esempio.



In un'implementazione di Stealthwatch con un Data Store, il cluster del Data Store si trova tra l'SMC e i Flow Collector. I Flow Collector acquisiscono e duplicano i flussi, eseguono analisi e riportano i dati e i risultati direttamente al Data Store, distribuendoli pressappoco equamente su 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.



Per risolvere le query inviate dall'utente, inclusi i grafici, l'SMC 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 della query all'SMC. L'SMC genera il grafico senza dover raccogliere più 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.

A causa dell'architettura del Data Store, l'SMC e tutti i Flow Collector devono comunicare con il Data Store e devono essere configurati durante l'implementazione in modo da essere utilizzati con il Data Store. Non è possibile avere un ambiente "misto" con alcuni Flow Collector che comunicano direttamente con l'SMC e altri Flow Collector che comunicano con il Data Store.

Architettura di Stealthwatch Data Store

Ciascun Data Store è composto da 3 o più Data Node. Ciascun Data Node ha il proprio chassis hardware. Quando si acquista un Data Store, si ricevono più chassis hardware

per Data Node, corrispondenti al numero di nodi previsto per quel modello di Data Store. Ad esempio, un Data Store DS 6200 fornisce 3 chassis hardware per Data Node.

È possibile acquistarne più di un Data Store per la distribuzione. I Data Node possono essere raggruppati come parte del Data Store in multipli di 3, da un minimo di 3 a un massimo di 36.

> Cisco consiglia di 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. Per ulteriori informazioni, vedere Requisiti di implementazione del Data Store e suggerimenti.

Per implementare un Data Store, è necessario assegnare quanto segue a ciascun Data Node:

- un indirizzo IP indirizzabile per le comunicazioni di gestione, acquisizione e query con le appliance Stealthwatch
- un indirizzo IP non indirizzabile (blocco CIDR `169.254.42.0/24`) sulla LAN o VLAN isolata per le comunicazioni tra i Data Node che fanno parte del cluster del Data Store
- due connessioni da 10G, una per le comunicazioni di gestione, acquisizione e query, una per le comunicazioni tra i Data Node
- facoltativamente, per la ridondanza di rete e la criticità delle comunicazioni tra Data Node, un'ulteriore connessione da 10G e uno switch aggiuntivo per stabilire un port-channel sul Data Node

Per informazioni più dettagliate sull'implementazione e i prerequisiti di implementazione, vedere Prerequisiti di implementazione del Data Store e suggerimenti.

Prerequisiti di implementazione del Data Store e suggerimenti

Di seguito vengono descritti i prerequisiti di implementazione del Data Store e forniti alcuni suggerimenti.

> Se si pensa di acquistare StealthwatchData Store, rivolgersi ai Cisco Professional Services per consigli sulla posizione, l'implementazione e la configurazione nell'ambito del progetto complessivo di Stealthwatch.

Supporto della versione di Stealthwatch

Quando si implementa un Data Store, tutte le appliance Stealthwatch devono avere la stessa versione (versione 7.3+).

Licenze Stealthwatch

L'implementazione di Stealthwatch richiede una Flow Rate (FPS) Smart License; il Data Store non richiede una licenza aggiuntiva.

Compatibilità dell'hardware di Stealthwatch e requisiti di networking

Nella tabella seguente viene fornita una panoramica dei dispositivi richiesti per implementare un Data Store.

Componente hardware	**Capacità supportata**
Data Store	• Almeno 3 Data Node (DS 6200) • Set aggiuntivo di 3 Data Node per espandere il Data Store, per un massimo di 36 Data Node
Stealthwatch Management Console	• Almeno 1 console SMC (Stealthwatch Management Console)
Flow Collector	• Almeno 1 Flow Collector

Tenere presente che è necessaria una Flow Rate (FPS) Smart License per l'implementazione complessiva di Stealthwatch.

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

Se si desidera implementare un Data Store, occorre disporre di almeno 3 Data Node. 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. Il Data Store può essere ampliato aggiungendo i Data Node in multipli di 3, per un massimo di 36 Data Node.

> ℹ 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 sensore di flusso, 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 sostitutivi, in caso il Data Node principale diventi inattivo. Per assistenza e istruzioni, contattare il supporto Cisco.

Insieme al Data Store è necessario implementare una SMC e configurarla in modo che possa comunicare con il Data Store. Per assicurare che la console sia sempre disponibile, è possibile implementare anche una SMC di failover.

Inoltre, è necessario implementare almeno 1 Flow Collector con il Data Store e configurare tutti i Flow Collector in modo che possano essere utilizzati con un Data Store.

Per ciascuna SMC e Flow Collector implementati, assegnare un indirizzo IP pubblico indirizzabile alla porta di gestione `eth0`. Quando si implementa un Data Store, è possibile configurare l'uso di una porta in rame BASE-T da 1G/10G o una porta SFP+ con cablaggio biassiale da 10G come porta di gestione `eth0` dell'SMC e dei Flow Collector. Affinché la porta BASE-T in rame possa essere usata con il Data Store, è richiesta una velocità di trasmissione di 10G. Gli utenti che non stanno implementando un Data Store possono configurare solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps come `eth0`.

È inoltre possibile implementare i Flow Sensor e gli UDP Director per l'implementazione del Stealthwatch. Poiché queste appliance non comunicano direttamente con il Data Store, non è necessario configurarle per permetterne la comunicazione con un Data Store.

Per ulteriori informazioni sulle piattaforme supportate, vedere le relative Schede tecniche. Per ulteriori informazioni sulla compatibilità delle versioni, vedere Matrice di compatibilità delle versioni hardware e software di Stealthwatch.

Considerazioni sull'implementazione di Stealthwatch Enterprise

Tenere presente quanto segue:

- Se si configura un Flow Collector per la compatibilità del Data Store, sull'interfaccia di amministrazione dell'appliance (amministratore dell'appliance) alcune funzionalità risultano nascoste. Utilizzare Central Management per eseguire la configurazione del Flow Collector e altre attività correlate. Se si desidera monitorare le statistiche di archiviazione, scaricare l'app Report Builder sull'SMC.
- Utilizzare Stealthwatch Web App per monitorare e configurare l'installazione di Stealthwatch se si implementa un Data Store. Stealthwatch Desktop Client non è compatibile con il Data Store.
- Se si configura l'SMC in modo che possa essere utilizzata con un Data Store, non è possibile usare le app ETA Cryptographic Audit o Host Classifier.

Credenziali richieste per l'implementazione del Data Store

Preparare le password per i seguenti account utente:

- `root` e `sysadmin` per ciascuna SMC, Data Node e Flow Collector. Queste password devono essere assegnate durante la configurazione iniziale del sistema.
- `admin` per ciascuna SMC, Data Node e Flow Collector. Assegnare queste password con lo strumento Appliance Setup Tool.
- `dbadmin` e `readonlyuser` per il Data Store. Assegnare queste password durante l'inizializzazione del Data Store.

Considerazioni sui requisiti di networking e switching del Data Store

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

Considerazioni sulla rete	Descrizione
Credenziali necessarie	Per ciascun Data Node, Stealthwatch Management Console e Flow Collector: • Configurate durante la configurazione iniziale del sistema: `root`, `sysadmin` • Configurate con lo strumento Appliance Setup: `admin` • Configurate durante l'inizializzazione del Data Store: `dbadmin`, `readonlyuser`
Comunicazioni tra Data Node	• Stabilire una latenza RTT (Round-Trip Time) inferiore a 200 microsecondi tra i Data Node • Mantenere lo sfasamento orario al massimo a 1 secondo tra i Data Node. • Stabilire una velocità di trasmissione consigliata di almeno 6,4 Gbps (connessione commutata full duplex da 10 Gbps) tra i Data Node.
Alimentazione dell'hardware del Data Node	• Un'improvvisa interruzione dell'alimentazione su un Data Node potrebbe danneggiare i dati. Utilizzare entrambi gli alimentatori su circuiti separati alimentati da gruppi di continuità. • Quando si inizializza il cluster del Data Store (per ulteriori informazioni, vedere Inizializzazione e configurazione del Data Store), alternare la configurazione dei Data Node in base agli alimentatori usati da ciascun Data Node. In questo modo è possibile ottimizzare la tolleranza agli errori riducendo al minimo il numero di Data Node in caso di interruzione dell'alimentazione.
Switching del Data Node	• I Data Node richiedono una propria VLAN di Layer 2 per consentire le comunicazioni tra Data Node. I Data Node fisici possono essere connessi a uno switch condiviso o dedicato da 10G. • Cisco consiglia di collegare i Data Node hardware a 2 switch per garantire una connettività costante 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, in cui 2 switch sono interconnessi e supportano entrambi la VLAN di Layer 2.
Comunicazioni delle appliance Stealthwatch	• È richiesto l'accesso SSH e l'accesso SSH root per SMC, Data Node e Flow Collector, configurati dall'SMC • SMC e Flow Collector devono essere in grado di raggiungere tutti i Data Node • I Data Node devono essere in grado di raggiungere l'SMC, tutti i Flow Collector e ciascun Data Node

Assegnare i seguenti indirizzi IP a ciascun Data Node:

- Un indirizzo IP indirizzabile per comunicare con le appliance Stealthwatch (`eth0`). Collegare la porta `eth0` del Data Node alla rete per permettere la comunicazione con la SMC e i Flow Collector. È possibile configurare l'uso di una porta in rame BASE-T da 1G/10G o di una porta SFP+ con cablaggio biassiale da 10G per la porta di gestione `eth0` del Data Node.

  Durante l'implementazione e la configurazione del Data Store, gli indirizzi IP della porta `eth0` del Data Node vengono associati al nome del Data Store per permettere una distribuzione più uniforme dei dati telemetrici, delle richieste e delle risposte. Per ulteriori informazioni, vedere Inizializzazione e configurazione del database del Data Store.

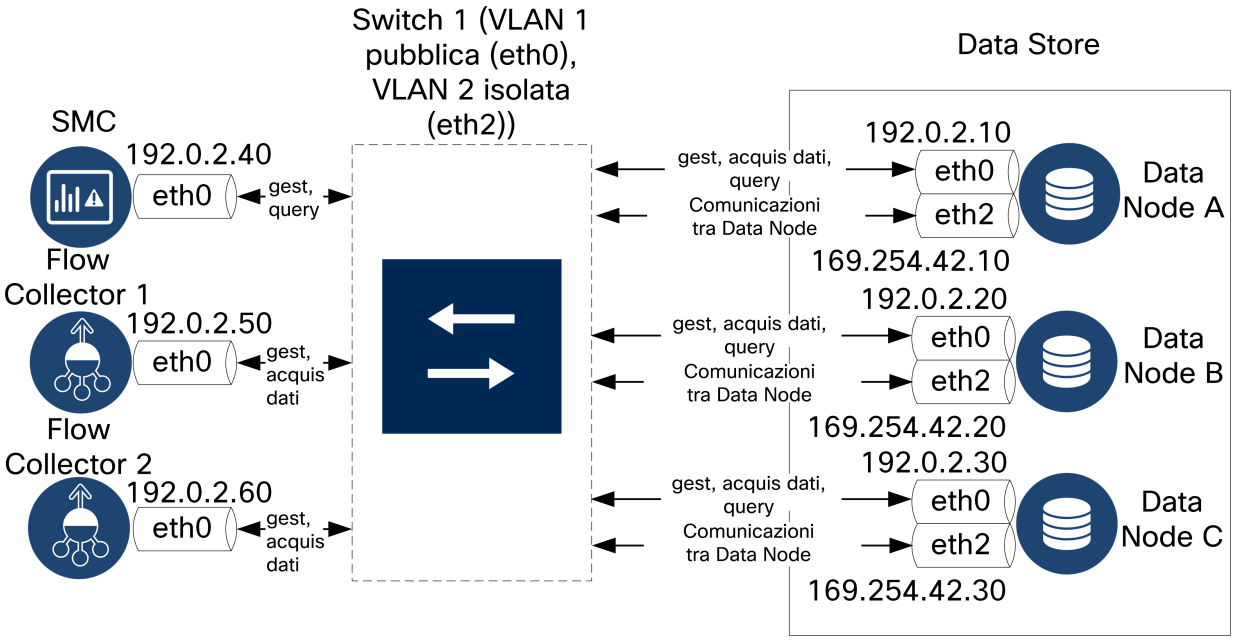
- Un indirizzo IP non indirizzabile in una LAN o VLAN privata, da usare per le comunicazioni tra Data Node (`eth2` o il port-channel contenente `eth2` e `eth3` per migliori prestazioni e velocità di trasmissione). Nell'ambito di un Data Store, i Data Node comunicano tra loro. Collegare la porta `eth2` del Data Node o il port-channel contenente `eth2` e `eth3` agli switch per permettere la comunicazione tra i Data Node.

  > Assegnare gli indirizzi IP non indirizzabili della porta `eth2` o del port-channel `eth2/eth3` dal blocco CIDR `169.254.42.0/24`.

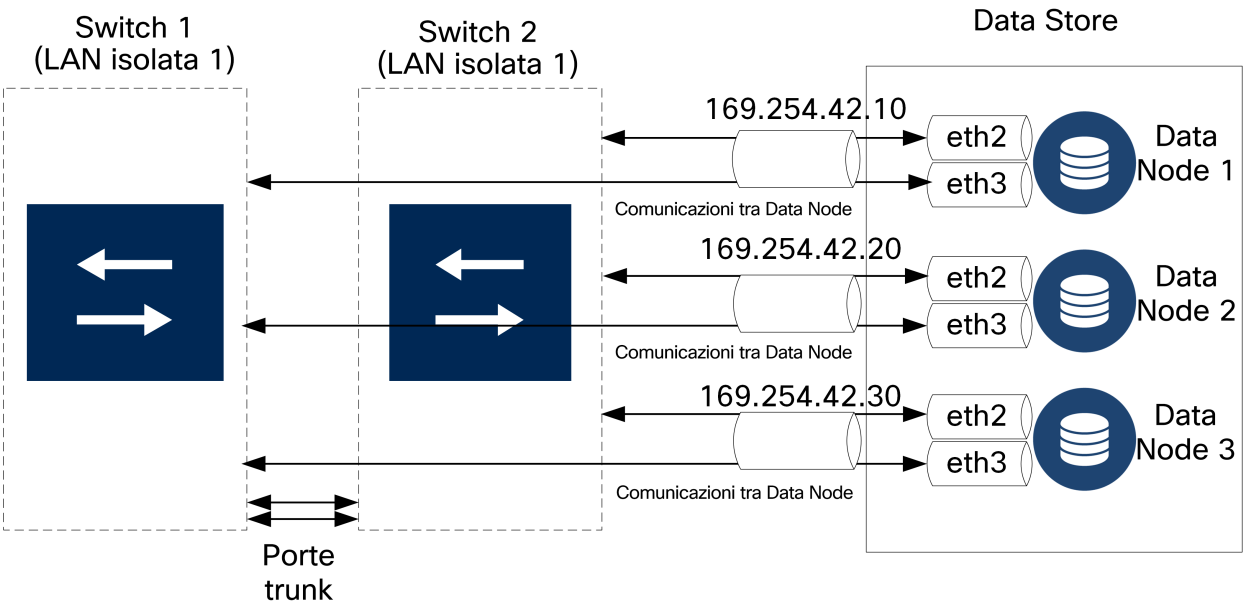
  Per consentire la comunicazione tra Data Node, è sufficiente impostare a 10G la velocità di trasmissione della porta `eth2`. La creazione di un port-channel `eth2/eth3` per una velocità di trasmissione fino a 20G permette una comunicazione più veloce tra i Data Node e una più veloce aggiunta o sostituzione

di Data Node al Data Store, in quanto ciascun nuovo Data Node riceve i dati dai Data Node adiacenti.

Per abilitare le comunicazioni tra Data Node sull'interfaccia `eth2` o sul port-channel `eth2/eth3` , implementare 1 switch che supporti velocità da 10G. Configurare una LAN o VLAN pubblica per le comunicazioni `eth0` del Data Node con l'SMC e i Flow Collector e una LAN o VLAN isolata per comunicazioni tra Data Node. È possibile condividere questi switch con altre appliance, occore 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 facenti 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, Cisco consiglia di configurare i Data Node con port-channel dedicati per le comunicazioni tra Data Node. Collegare ogni Data Node a 2 switch, con ciascuna porta fisica connessa a uno switch diverso. Per un esempio, vedere il seguente schema:



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

Requisiti di implementazione del Data Store e suggerimenti

Posizionare ciascun Data Node in modo che possa comunicare con tutti i Flow Collector, l'SMC 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 l'SMC in modo da avere la maggiore efficacia di esecuzione delle query. Cisco consiglia vivamente di posizionare i Data Node entro il perimetro del firewall, ad esempio con un NOC. Per quanto riguarda le prestazioni, tenere presente quanto segue:

- Quando si implementano i Data Node, stabilire una latenza RTT (Round-Trip Time) inferiore a 200 microsecondi.
- Mantenere lo sfasamento orario al massimo a 1 secondo tra i Data Node.
- Stabilire una velocità di trasmissione consigliata di almeno 6,4 Gbps (connessione commutata full duplex da 10 Gbps) tra i Data Node.

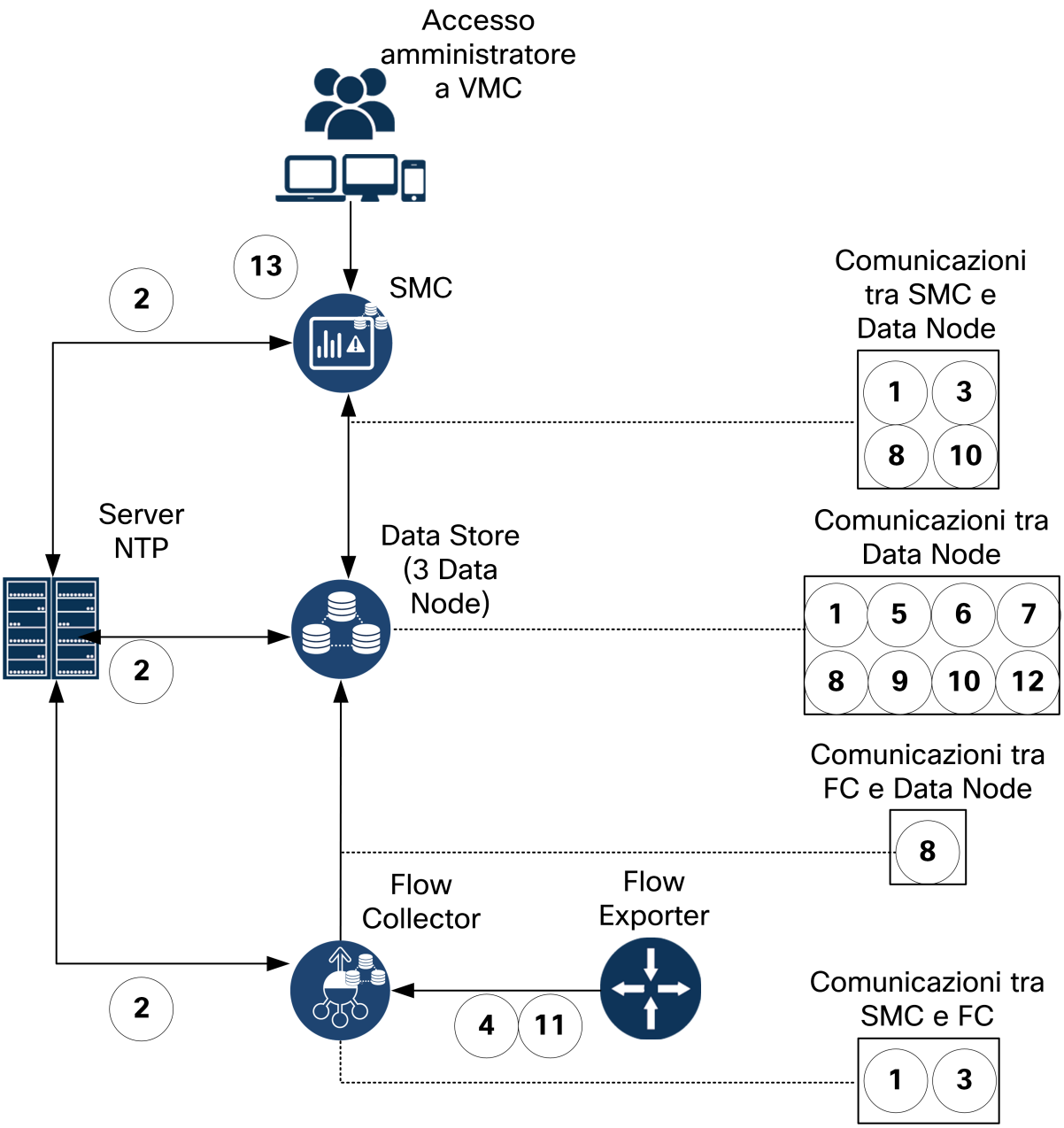
Se il Data Store diventa inattivo a causa di una perdita di alimentazione o un guasto dell'hardware, il rischio di danneggiare o perdere i dati aumenta. Cisco consiglia di installare i Data Node tenendo sempre in considerazione il tempo di attività. Tenere presente quanto segue:

- Cisco consiglia vivamente di installare alimentatori ridondanti o gruppi di continuità per ciascun Data Node, per evitare la perdita o il danneggiamento dei dati in caso di interruzioni di alimentazione.
- Verificare che la policy di ripristino dell'alimentazione del Data Node 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.
- Quando si inizializza il Data Store (per ulteriori informazioni, vedere Inizializzazione e configurazione del database del Data Store), usare entrambi gli alimentatori per configurare i Data Node. Durante la configurazione, il Data Store crea un backup di un Data Node sul Data Node successivo e un backup del Data Node configurato per ultimo sul Data Node configurato per primo. Se si implementano i Data Node su due alimentatori separati e si alterna la configurazione dei Data Node pari e dispari sui due alimentatori, in caso di guasto di un alimentatore e con un numero pari di nodi, il Data Store può ancora rimanere attivo in quanto è possibile accedere ai dati o ai dati di backup di ciascun Data Node dai Data Node alimentati.

> Se si verifica un'interruzione di alimentazione improvvisa su un Data Node e l'appliance viene riavviata, l'istanza del database su quel Data Node potrebbe non riavviarsi automaticamente. Per informazioni sul riavvio manuale dell'istanza del database, vedere Risoluzione dei problemi del Data Store.

Porte di comunicazione del Data Store

Nello schema seguente viene mostrato un esempio di architettura di Stealthwatch con le porte di comunicazione che devono essere aperte. Vedere la tabella per le porte associate con ciascun riferimento.



La tabella seguente elenca le porte di comunicazione che devono essere aperte sul firewall per implementare il Data Store. Per altre porte di comunicazione da aprire per l'implementazione complessiva di Stealthwatch, vedere Guida alla configurazione di Stealthwatch System.

#	Da (Client)	A (Server)	Porta	Protocollo o scopo
1	SMC	Flow	22/TCP	SSH, necessario per

		Collector e Data Node		inizializzare il database Data Store
1	Data Node	tutti gli altri Data Node	22/TCP	SSH, necessario per inizializzare il database Data Store e per le attività di amministrazione del database
2	SMC, Flow Collector e Data Node	Server NTP	123/UDP	NTP, richiesto per la sincronizzazione dell'ora
2	Server NTP	SMC, Flow Collector e Data Node	123/UDP	NTP, richiesto per la sincronizzazione dell'ora
3	SMC	Flow Collector e Data Node	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
3	Flow Collector	SMC	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
3	Data Node	SMC	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 comunicazione tra Data Node
6	Data Node	tutti gli altri Data Node	4803/UDP	servizio di comunicazione tra Data Node
7	Data Node	tutti gli altri Data Node	4804/UDP	servizio di comunicazione tra Data Node

8	SMC, 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	SMC	Data Node	5444/TCP	comunicazioni sicure Vertica Management Console
10	Data Node	SMC e tutti gli altri Data Node	5444/TCP	comunicazioni sicure Vertica Management Console
11	sFlow Exporter	Flow Collector – sFlow	6343/UDP	acquisizione dati in sFlow
12	Data Node	tutti gli altri Data Node	6543/UDP	servizio di comunicazione tra Data Node
13	postazioni di amministrazione per accedere a Vertica Management Console	SMC	9450/TCP	accesso al browser Web di Vertica Management Console

Panoramica dell'implementazione di Stealthwatch Data Store

> ⚠ Se si pensa di acquistare un StealthwatchData Store, rivolgersi ai Cisco Professional Services per consigli sulla posizione, l'implementazione e la configurazione nell'ambito del progetto complessivo di Stealthwatch. **Non** installare un Data Store autonomamente.

Di seguito vengono descritte le fasi principali per l'implementazione del Data Store in un'implementazione di Stealthwatch:

- Implementare le appliance Stealthwatch, tra cui i Data Node e configurare l'SMC e i Flow Collector da usare con un Data Store

  > ⓘ Accertarsi di installare la versione e la patch di rollup più recenti delle appliance dopo averle implementate, ma prima di procedere con l'inizializzazione e la configurazione del Data Store.

- Preparare l'implementazione di Stealthwatch per l'uso con il Data Store distribuendo le password utente e i certificati di identità
- Inizializza il Data Store
- Configurare la Vertica Management Console (VMC) sull'SMC e abilitare la soglia degli avvisi e le notifiche
- Configurare le impostazioni sulla conservazione dei dati del Data Store tramite l'API REST
- Installare le app di Stealthwatch sull'SMC per ulteriori funzionalità relative a Data Store

Esaminare queste attività prima di avviare l'implementazione.

Componente richiesto e attività	**Passaggi**
Installazione e configurazione dell'SMC	Per ulteriori informazioni, vedere Configurazione dell'SMC per l'utilizzo con un Data Store. 1. Implementare l'SMC nella rete. 2. Con CIMC o collegandosi direttamente all'appliance,

	accedere alla console dell'SMC come utente `root`. Eseguire lo script di configurazione del sistema `systemconfig` e utilizzare la procedura guidata di installazione iniziale per configurare le informazioni sulla gestione base, tra cui l'indirizzo IP dell'appliance, l'utilizzo con un Data Store e la configurazione della porta fisica `eth0`. 3. Da un browser Web, accedere all'indirizzo IP `eth0` dell'SMC per accedere allo strumento Appliance Setup Tool. Utilizzare lo strumento Appliance Setup Tool per configurare le password di amministrazione, il dominio di Stealthwatch, i server DNS e NTP e per installare Central Management. 4. Da un browser Web, navigare l'indirizzo IP dell'SMC dopo aver configurato l'appliance utilizzando lo strumento Appliance Setup Tool per accedere a Stealthwatch Web App. Da Central Management, abilitare l'accesso SSH e l'accesso SSH root sull'SMC. 5. Aggiornare l'SMC alla versione e alla patch più recenti. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.
Installazione e configurazione del Data Node	Per ulteriori informazioni, vedere Implementazione e configurazione iniziali dell'hardware del Data Store. 1. Implementare i Data Node sulla rete. 2. Con CIMC o collegandosi direttamente all'appliance, accedere alla console di Data Node come utente `root`. Eseguire lo script di configurazione del sistema `systemconfig` e utilizzare la procedura guidata di installazione iniziale per configurare le informazioni sulla gestione base, tra cui l'indirizzo IP di gestione dell'appliance e l'indirizzo IP non indirizzabile per la comunicazione tra i Data Node (con configurazione del port-channel facoltativo). Assegnare un indirizzo IP

	non indirizzabile a `eth2` o al port-channel `eth2/eth3` dal blocco CIDR `169.254.42.0/24`. 3. Per ciascun Data Node, da un browser Web, passare all'indirizzo IP indirizzabile `eth0` del Data Node per accedere allo strumento Appliance Setup Tool. Utilizzare lo strumento Appliance Setup Tool su ciascun Data Node per configurare le password di amministrazione, il dominio di Stealthwatch, i server DNS e NTP e per far gestire il Data Node da Central Management. 4. Dalla Stealthwatch Web App, accedere a Central Management e abilitare l'accesso SSH e l'accesso SSH root per ciascun Data Node. 5. Aggiornare i Data Node all'ultima versione e alla patch più recenti. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch. **Prima di procedere, consultare le guide all'aggiornamento dei dispositivi in uso e i file Leggimi delle patch. Il processo di aggiornamento del Data Node richiede ulteriori passaggi rispetto ad altre appliance Stealthwatch.**
Installazione e configurazione del Flow Collector	Per ulteriori informazioni, vedere Configurazione del Flow Collector per l'utilizzo con un Data Store. 1. Implementare i Flow Collector sulla rete. 2. Con CIMC o collegandosi direttamente all'appliance, accedere alla console del Flow Collector come utente `root`. Eseguire lo script di configurazione del sistema `systemconfig` e utilizzare la procedura guidata di installazione iniziale per configurare le informazioni sulla gestione base, tra cui l'indirizzo IP dell'appliance,

	l'utilizzo con un Data Store e la configurazione della porta fisica eth0. 3. Per ciascun Flow Collector, da un browser Web, passare all'indirizzo IP `eth0` del Flow Collector per accedere allo strumento Appliance Setup Tool. Utilizzare lo strumento Appliance Setup Tool su ciascun Flow Collector per configurare le password di amministrazione, il dominio di Stealthwatch, i server DNS e NTP, il numero di porta di raccolta dei flussi (`2055` per NetFlow o `6343` per sFlow) e di fare in modo che Central Management sia gestito dal Flow Collector. 4. Dalla Stealthwatch Web App, accedere a Central Management e abilitare l'accesso SSH e l'accesso SSH root per ciascun Flow Collector. 5. Aggiornare i Flow Collector all'ultima versione e alla patch più recenti. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.
Inizializzazione e configurazione del Data Store	Per ulteriori informazioni, vedere Inizializzazione e configurazione del database del Data Store. 1. Dalla Stealthwatch Web App, accedere a Central Management e verificare che tutti i Data Node e i Flow Collector siano gestiti dalla Central Management, che il collegamento sia attivo e che l'accesso SSH e l'accesso SSH root siano entrambi abilitati. 2. Accedere alla console dell'SMC principale come utente `sysadmin`. Utilizzando lo script di connessione sicura del database `setup-sw-datastore-secure-connectivity`, distribuire le password del database `dbadmin` e `readonlyuser` e i certificati di identità sull'SMC, i Data Node e i Flow Collector.

	3. In base all'output dello script di connessione sicura `setup-sw-datastore-secure-connectivity`, accedere alla console del Data Node specificato come utente `root`. Copiare il file di configurazione di esempio per l'inizializzazione del database `install_SDBN_example.cfg` come `install_SDBN.cfg` e aggiornarlo con l'indirizzo IP e la subnet del Data Node. Eseguire lo script di inizializzazione, facendo riferimento al file di configurazione di inizializzazione (`python install_SDBN_initial.py -i install_SDBN.cfg`). 4. Dal Data Node su cui è stato eseguito lo script di inizializzazione, recuperare la stringa della chiave API da `/opt/vertica/config/apikey.dat`. Questa chiave API verrà utilizzata per stabilire una connessione tra il database del Data Store e la console VMC in una fase successiva. 5. Dalla Stealthwatch Web App, andare a Central Management e per l'SMC e tutti i Flow Collector, utilizzare l'opzione di risoluzione locale per associare il nome del database del Data Store (`sw-datastore`) all'indirizzo IP indirizzabile di ciascun Data Node. Per prestazioni ottimali, mappare gli indirizzi IP di Data Node `eth0` nello stesso ordine per ciascuna appliance.
Installazione e configurazione di Vertica Management Console (VMC) sull'SMC	Per ulteriori informazioni, vedere Configurazione di Vertica Management Console Configuration. 1. Copiare il certificato del server `/lancope/var/admin/cds/ server.crt` dall'SMC alla postazione di lavoro locale. 2. Da un browser Web sulla postazione di lavoro locale, passare a `[smc-ipv4-address]:9450/webui/login` per accedere all'VMC. Eseguire la configurazione e l'impostazione iniziali della VCM. Disabilitare le connessioni che usano versioni meno sicure di TLS. Utilizzare la stringa

	della chiave API e il file del certificato `server.crt` per stabilire una connessione con il Data Store. Configurare le soglie di avviso e le notifiche per ricevere gli avvisi dell'integrità del Data Store.
Conservazione dei dati del Data Store	Per ulteriori informazioni, vedere Configurazione della durata di conservazione dei dati nel Data Store. • Utilizzare l'API REST per configurare la durata di conservazione dei dati nel Data Store.
Revisione dei passi successivi al termine dell'implementazione del Data Store	Riesaminare i passaggi di installazione successivi del Data Store: 1. Installare l'app Stealthwatch Report Builder sull'SMC per generare i report sull'implementazione di Stealthwatch e per visualizzare le statistiche di archiviazione del Data Store. Per ulteriori informazioni, vedere le note sulla versione. 2. Per ulteriori informazioni su come utilizzare Stealthwatch, consultare la guida online su Stealthwatch Web App.

Facoltativamente, è possibile effettuare anche le seguenti operazioni:

Componente opzionale e attività	**Passaggi**
Installazione e configurazione dell'UDP Director	• Implementare l'UDP Director, come descritto nella Guida all'installazione dell'hardware di Stealthwatch serie x2xx e nella Guida alla configurazione di Stealthwatch System. Aggiornare alla versione e alla patch più recenti del UDP Director. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.
Flow Sensor	• Implementare il Flow Sensor, come descritto nella

	Guida all'installazione dell'hardware di Stealthwatch serie x2xx e nella Guida alla configurazione di Stealthwatch System. Aggiornare il Flow Sensor alla versione e alla patch più recenti. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.
Installazione e configurazione dell'SMC di failover	• Implementare l'SMC di failover, come descritto nella Guida all'installazione dell'hardware di Stealthwatch serie x2xx, nella Guida alla configurazione di Stealthwatch System e nella Guida alla configurazione del failover di Stealthwatch. Aggiornare l'SMC alla versione e alla patch più recenti. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.

Installazione dell'hardware del Data Store

> Se si pensa di acquistare StealthwatchData Store, rivolgersi ai Cisco Professional Services per consigli sulla posizione, l'implementazione e la configurazione nell'ambito del progetto complessivo di Stealthwatch.

Implementazione dell'hardware di Stealthwatch e suggerimenti

Implementare e configurare le appliance di SMC, Data Node, Flow Collector e Stealthwatch in base alle istruzioni e installare gli switch del Data Store sulla rete. Quando si distribuiscono i Data Node e si connettono alla rete, consultare Requisiti di implementazione del Data Store e suggerimenti. Accertarsi che le versioni di SMC, Data Node e Flow Collector siano tutte aggiornate alla 7.3+. Per ulteriori informazioni sull'installazione e configurazione iniziali dell'appliance, vedere la Guida all'installazione dell'hardware di Stealthwatch serie x210 o l'**Appendice A. Preparazione dell'installazione** e l'**Appendice B. Installazione dell'hardware di Stealthwatch**.

> Se si desidera implementare un Data Store sulla rete come parte di un'implementazione di Stealthwatch esistente, rivolgersi a Cisco Professional Services per integrare il Data Store. Per ulteriori informazioni, contattare il supporto Cisco.

> Se si implementa un Data Store, utilizzare Stealthwatch Web App per monitorare e configurare l'installazione di Stealthwatch. Stealthwatch Desktop Client non è compatibile con il Data Store.

Configurazione dell'SMC per l'utilizzo con un Data Store

Implementare e configurare l'SMC per l'utilizzo con un Data Store e per gestire i Data Node e i Flow Collector.

> Se è presente una SMC secondaria, configurarla per prima in modo che possa comunicare con l'SMC principale. Per ulteriori informazioni su come creare una coppia di SMC per il failover, vedere la Guida alla configurazione di Stealthwatch System. Per un maggiore contesto sull'implementazione e configurazione di una SMC secondaria utilizzabile con un Data Store, vedere

Implementazione della Stealthwatch Management Console (SMC) di failover.

Effettuare quanto segue:

1. Innanzitutto, implementare l'SMC sulla rete. Quindi, connettersi all'appliance con CIMC, una tastiera e un monitor o un laptop e accedere alla console come utente `root`. Eseguire `systemconfig` e utilizzare la procedura guidata all'impostazione iniziale per aggiornare le impostazioni della porta di gestione, l'uso con un Data Store e le password utente `root` e `sysadmin`. Per ulteriori informazioni, vedere la Guida all'installazione dell'hardware di Stealthwatch serie x210 o l'**Appendice A. Preparazione dell'installazione** e l'**Appendice B. Installazione dell'hardware di Stealthwatch**.

   La prima volta che si accede alla configurazione di sistema, il sistema visualizza una procedura guidata per l'impostazione iniziale dell'appliance.

   Dopo aver scelto di configurare SMC o Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, è necessario effettuare l'RFD dell'appliance. Abilitare questa opzione solo se si intende implementare un Data Store nella rete.

2. Quindi, in un browser Web, selezionare l'indirizzo IP assegnato alla porta di gestione. Utilizzare lo strumento Appliance Setup Tool per eseguire ulteriori passaggi di configurazione, tra cui l'assegnazione della password utente `admin` (e delle password utente `root` e `sysadmin` se non sono state assegnate durante la configurazione del sistema), la configurazione del dominio di Stealthwatch e di altri parametri della rete, le impostazioni DNS e NTP e l'installazione di Central Management sull'SMC. Per ulteriori informazioni, vedere la Guida alla configurazione di Stealthwatch System o l'**Appendice C. Configurazione delle appliance**.

3. Quindi, abilitare l'accesso SSH e l'accesso SSH root sull'SMC. Per inizializzare il Data Store, come descritto in **Inizializzazione e configurazione del Data Store**, eseguire uno script basato sull'accesso SSH per ciascuna appliance.

   Quando l'accesso SSH è abilitato, il rischio che il sistema venga compromesso aumenta. È importante abilitare l'accesso SSH solo quando necessario. Quando l'accesso SSH non viene più utilizzato, disabilitarlo.

Aggiornamento dell'autorizzazione di accesso SSH dell'SMC

Operazioni preliminari

- Accedere a SMC Web App come amministratore di sistema.

Procedura

1. Accedere alla dashboard Appliance Manager (Gestione appliance). Sono disponibili le seguenti opzioni:
    - Se l'impostazione dell'appliance è stata completata, lo strumento Appliance Setup Tool apre la dashboard Appliance Manager (Gestione appliance).
    - Fare clic sull'icona **Global Settings** (Impostazioni globali). Selezionare **Central Management** (Gestione centralizzata). Viene visualizzata la dashboard Appliance Manager (Gestione appliance).
2. Per la voce dell'SMC, fare clic sul menu Actions (Azioni), quindi selezionare **Edit Appliance Configuration** (Modifica configurazione dell'appliance).
3. Selezionare la scheda Appliance.
4. Nel riquadro SSH, selezionare **Enable SSH** (Abilita SSH).
5. Selezionare **Enable Root SSH Access** (Abilita accesso SSH root).
6. Fare clic su **Apply Settings** (Applica impostazioni).

Come procedere

- Aggiornare l'SMC alla versione e alla patch più recenti, come descritto nel passaggio successivo.

1. Infine, aggiornare l'SMC alla versione e alla patch più recenti. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.

   Dopo aver aggiornato l'SMC, sono disponibili le seguenti opzioni:
    - Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
    - Implementare e configurare i Data Node come descritto nella sezione successiva.

Implementazione e configurazione iniziali dell'hardware del Data Store

Dopo aver implementato l'SMC, implementare e configurare le appliance Data Node. Quando si distribuiscono i Data Node e si connettono alla rete, consultare Requisiti di implementazione del Data Store e suggerimenti.

Per ciascun Data Node, effettuare quanto segue:

1. Innanzitutto, implementare il Data Node nella rete. Quindi, connettersi all'appliance Data Node con CIMC, una tastiera e un monitor o un laptop e accedere alla console come utente `root`. Eseguire `systemconfig` e utilizzare la procedura guidata all'impostazione iniziale per aggiornare le impostazioni della porta di gestione, le impostazioni delle porte per la comunicazione tra Data Node e le password utente `root` e `sysadmin`. Per ulteriori informazioni, vedere la Guida all'installazione dell'hardware di Stealthwatch serie x210 o l'**Appendice A. Preparazione dell'installazione** e l'**Appendice B. Installazione dell'hardware di Stealthwatch**.

   > La prima volta che si accede alla configurazione di sistema, il sistema visualizza una procedura guidata per l'impostazione iniziale dell'appliance.

2. Quindi, in un browser Web, selezionare l'indirizzo IP assegnato alla porta di gestione. Utilizzare lo strumento Appliance Setup Tool per eseguire ulteriori passaggi di configurazione, tra cui l'assegnazione della password utente `admin` (e delle password utente `root` e `sysadmin` se non sono state assegnate durante la configurazione del sistema), la configurazione del dominio di Stealthwatch e di altri parametri della rete, le impostazioni DNS e NTP e l'impostazione della gestione del Data Node tramite Central Management. Per ulteriori informazioni, vedere la Guida alla configurazione di Stealthwatch System o l'**Appendice C. Configurazione delle appliance**.

3. Quindi, abilitare l'accesso SSH e l'accesso SSH root sul Data Node. Per inizializzare il Data Store, come descritto in **Inizializzazione e configurazione del Data Store**, eseguire uno script basato sull'accesso SSH per ciascuna appliance.

   > Quando l'accesso SSH è abilitato, il rischio che il sistema venga compromesso aumenta. È importante abilitare l'accesso SSH solo quando necessario. Quando l'accesso SSH non viene più utilizzato, disabilitarlo.

Aggiornamento dell'autorizzazione di accesso SSH di un Data Node

Operazioni preliminari

- Accedere a SMC Web App come amministratore di sistema.

Procedura

1. Accedere alla dashboard Appliance Manager (Gestione appliance). Sono disponibili le seguenti opzioni:
   - Se l'impostazione dell'appliance è stata completata, lo strumento Appliance Setup Tool apre la dashboard Appliance Manager (Gestione appliance).
   - Fare clic sull'icona **Global Settings** (Impostazioni globali). Selezionare **Central Management** (Gestione centralizzata). Viene visualizzata la dashboard Appliance Manager (Gestione appliance).

   Esaminare l'elenco delle appliance e verificare che sia presente il Data Node e che lo stato dell'appliance sia **attivo**.
2. Per la voce del Data Node, fare clic sul menu Actions (Azioni), quindi selezionare **Edit Appliance Configuration (Modifica configurazione dell'appliance)**.
3. Selezionare la scheda Appliance.
4. Nel riquadro SSH, selezionare **Enable SSH** (Abilita SSH).
5. Selezionare **Enable Root SSH Access** (Abilita accesso SSH root).
6. Fare clic su **Apply Settings** (Applica impostazioni).

Come procedere

- Aggiornare il Data Node alla versione e alla patch più recenti, come descritto nel passaggio successivo.

1. Infine, aggiornare il Data Node all'ultima versione e patch. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.

   > Prima di procedere, consultare le guide all'aggiornamento dei dispositivi in uso e i file Leggimi delle patch. Il processo di aggiornamento del Data Node richiede ulteriori passaggi rispetto ad altre appliance Stealthwatch.

Dopo aver aggiornato il Data Node, sono disponibili le seguenti opzioni:

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Tornare a **Implementazione e configurazione iniziali dell'hardware del Data Store** e ripetere questo processo di installazione e configurazione iniziale del Data Node, la configurazione di Appliance Setup Tool e di Central Management per i Data Node restanti.

2. Dopo aver implementato e configurato tutti i Data Node, sono disponibili le seguenti opzioni:
   - Configurare UDP Director, se presente, come descritto nella sezione successiva.
   - Se l'UDP Director non è presente, configurare i Flow Collector come descritto in **Configurazione del Flow Collector per l'utilizzo con un Data Store**.

Implementazione di UDP Director

Se si desidera implementare un UDP Director, seguire le istruzioni fornite nella Guida all'installazione dell'hardware di Stealthwatch serie x210 e la Guida alla configurazione di Stealthwatch System. Tenere presente che il processo di installazione di UDP Director rimane invariato anche quando non si implementa il Data Store. Non è necessario configurare un UDP Director per l'uso con un Data Store.

Dopo aver implementato UDP Director, sono disponibili le seguenti opzioni.

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Implementare e configurare i Flow Collector, come descritto nella sezione successiva.

Configurazione del Flow Collector per l'utilizzo con un Data Store

Dopo aver configurato i Data Node e gli UDP Director implementati, implementare e configurare i Flow Collector.

Per ciascun Flow Collector, effettuare quanto segue:

1. Innanzitutto, implementare Flow Collector sulla rete. Quindi, connettersi al Flow Collector con CIMC, una tastiera e un monitor o un laptop e accedere alla console come utente `root`. Eseguire `systemconfig` e utilizzare la procedura guidata all'impostazione iniziale per aggiornare le impostazioni della porta di gestione, l'uso con un Data Store e le password utente `root` e `sysadmin`. Per ulteriori informazioni, vedere la Guida all'installazione dell'hardware di Stealthwatch serie x210 o l'**Appendice A. Preparazione dell'installazione** e l'**Appendice B. Installazione dell'hardware di Stealthwatch**.

   > La prima volta che si accede alla configurazione di sistema, il sistema visualizza una procedura guidata per l'impostazione iniziale dell'appliance.

   > Dopo aver scelto di configurare SMC o Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, è necessario effettuare l'RFD dell'appliance. Abilitare questa opzione solo se si intende implementare un Data Store nella rete.

2. Quindi, in un browser Web, selezionare l'indirizzo IP assegnato alla porta di gestione. Utilizzare lo strumento Appliance Setup Tool per eseguire ulteriori passaggi di configurazione, tra cui l'assegnazione della password utente `admin` (e delle password utente `root` e `sysadmin` se non sono state assegnate durante la configurazione del sistema), la configurazione del dominio di Stealthwatch e di altri parametri della rete, le impostazioni DNS e NTP, il numero di porta per la raccolta del flusso (`2055` per NetFlow o `6343` per sFlow) e l'abilitazione della gestione del Flow Collector tramite Central Management. Per ulteriori informazioni, vedere la Guida alla configurazione di Stealthwatch System o l'**Appendice C. Configurazione delle appliance**.

   > Se si configura un Flow Collector per essere usato con un Data Store, sull'interfaccia di amministrazione dell'appliance (amministratore dell'appliance) alcune funzionalità risultano nascoste. Utilizzare Central Management per eseguire la configurazione del Flow Collector e altre attività correlate. Se si desidera monitorare le statistiche di archiviazione, scaricare Data Store Storage Statistics App sull'SMC.

3. Infine, abilitare l'accesso SSH e l'accesso SSH root sui Flow Collector. Per inizializzare il Data Store, come descritto in **Inizializzazione e configurazione del Data Store**, eseguire uno script basato sull'accesso SSH per ciascuna appliance.

> ⚠ Quando l'accesso SSH è abilitato, il rischio che il sistema venga compromesso aumenta. È importante abilitare l'accesso SSH solo quando necessario. Quando l'accesso SSH non viene più utilizzato, disabilitarlo.

Aggiornamento dell'autorizzazione di accesso SSH di un Flow Collector

Operazioni preliminari

- Accedere a SMC Web App come amministratore di sistema, se non si utilizza Appliance Setup Tool.

Procedura

1. Accedere alla dashboard Appliance Manager (Gestione appliance). Sono disponibili le seguenti opzioni:
   - Se l'impostazione dell'appliance è stata completata, lo strumento Appliance Setup Tool apre la dashboard Appliance Manager (Gestione appliance).
   - Fare clic sull'icona **Global Settings** (Impostazioni globali). Selezionare **Central Management** (Gestione centralizzata). Viene visualizzata la dashboard Appliance Manager (Gestione appliance).

   Esaminare l'elenco delle appliance e verificare che sia presente il Flow Collector e che lo stato dell'appliance sia **attivo**.
2. Per la voce del Flow Collector, fare clic sul menu Actions (Azioni), quindi selezionare **Edit Appliance Configuration** (Modifica configurazione dell'appliance).
3. Selezionare la scheda Appliance.
4. Nel riquadro SSH, selezionare **Enable SSH** (Abilita SSH).
5. Selezionare **Enable Root SSH Access** (Abilita accesso SSH root).
6. Fare clic su **Apply Settings** (Applica impostazioni).

Come procedere

- Aggiornare il Flow Collector alla versione e alla patch più recenti, come descritto nel passaggio successivo.

1. Infine, aggiornare il Flow Collector alla versione e alla patch più recenti. Per ulteriori informazioni sull'aggiornamento alla versione corrente, vedere le guide

all'aggiornamento; per ulteriori informazioni sugli aggiornamenti delle patch, vedere i file Leggimi delle patch.

Dopo aver aggiornato il Flow Collector, sono disponibili le seguenti opzioni:

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Per ciascuno dei Flow Collector, ripetere il processo descritto in **Configurazione del Flow Collector per l'utilizzo con un Data Store** per l'installazione e la configurazione iniziale dei Flow Collector, la configurazione tramite lo strumento Appliance Setup Tool e la configurazione di Central Management per i Flow Collector rimanenti.

2. Dopo aver implementato e configurato tutti i Flow Collector, sono disponibili le seguenti opzioni:
   - Se presente, configurare il Flow Sensor come descritto nella sezione successiva.
   - Se presente, configurare l'SMC secondaria come descritto in **Implementazione della Stealthwatch Management Console (SMC) di failover**.
   - Se non sono presenti Flow Sensor o SMC secondarie, inizializzare e configurare il Data Store come descritto in **Inizializzazione e configurazione del Data Store**.

Implementazione di Flow Sensor

Se si desidera implementare un Flow Sensor, seguire le istruzioni fornite nella Guida all'installazione dell'hardware di Stealthwatch serie x210 e la Guida alla configurazione di Stealthwatch System. Tenere presente che il processo di installazione di Flow Sensor rimane invariato anche quando non si implementa il Data Store. Non è necessario configurare un Flow Sensor per l'uso con un Data Store.

Dopo aver implementato e configurato il Flow Sensor, sono disponibili le seguenti opzioni:

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Se presente, configurare l'SMC secondaria come SMC di failover come descritto nella sezione successiva.
- Se non è presente una SMC secondaria, inizializzare il Data Store come descritto in **Inizializzazione e configurazione del Data Store**.

Implementazione della Stealthwatch Management Console (SMC) di failover

Se una SMC secondaria deve essere configurata come SMC di failover, seguire le istruzioni fornite nella Guida all'installazione dell'hardware di Stealthwatch serie x210, la Guida alla configurazione di Stealthwatch System e la Guida alla configurazione del failover di Stealthwatch.

Dopo aver completato la configurazione dell'SMC secondaria e dopo che l'SMC principale è gestito tramite Central Management (Gestione centralizzata), sono disponibili le seguenti opzioni:

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Se è presente una SMC secondaria e la si promuove a SMC principale, sono necessari ulteriori passaggi di configurazione usando nuovamente lo script `setup-sw-datastore-secure-connectivity`. Per ulteriori informazioni, vedere Copia delle informazioni sull'attendibilità del Data Store su una SMC di failover.
- Inizializzare e configurare il Data Store, come descritto in **Inizializzazione e configurazione del Data Store**.

Inizializzazione e configurazione del Data Store

Dopo aver implementato e configurato una SMC, i Data Node e i Flow Collector, inizializzare e configurare il Data Store. Prima di procedere, accertarsi che tutte le SMC, i Data Node e i Flow Collector vengano aggiornati all'ultima versione e patch.

> Se è presente una SMC secondaria e la si promuove a SMC principale, sono necessari ulteriori passaggi di configurazione usando nuovamente lo script `setup-sw-datastore-secure-connectivity`. Per ulteriori informazioni, vedere Copia delle informazioni sull'attendibilità del Data Store su una SMC di failover.

Effettuare quanto segue:

1. Innanzitutto, accertarsi che tutti i Data Node e i Flow Collector e l'SMC secondaria, se presente, siano gestiti tramite Central Management e che l'accesso SSH e SSH root siano abilitati per tutti.

2. Dall'SMC, eseguire uno script per distribuire le password `dbadmin` del Data Store e `readonlyuser` e i certificati di identità per comunicazioni sicure tra Data Store e le appliance Stealthwatch.
3. Infine, dal Data Node specificato durante nel passaggio precedente, eseguire uno script per inizializzare il Data Store e stabilire connessioni sicure tra i Data Node e le appliance Stealthwatch.
4. Infine, in Central Management, associare un nome del Data Store interno (`sw-datastore`) agli indirizzi IP del Data Node sull'SMC e sui Flow Collector per migliorare la distribuzione dei carichi del Data Node e le prestazioni di esecuzione delle query.

Verifica della gestione dei Data Node e dei Flow Collector tramite Central Management

Operazioni preliminari

- Creare un elenco di tutti gli indirizzi IP dei Data Node e dei Flow Collector che si prevede di gestire in Central Management.
- Accedere a SMC Web App come amministratore di sistema e andare a Central Management.

Procedura

1. In Appliance Inventory (Inventario delle appliance), confrontare l'elenco di Data Node e Flow Collector, e l'SMC secondaria se presente, con l'elenco nell'inventario e accertarsi che **Appliance Status** (Stato appliance) sia **Up** (Attivo) per ciascuna appliance. **Non** proseguire con l'inizializzazione del Data Store finché tutte le appliance desiderate non sono gestite e il loro **stato** è **attivo**.

   Se lo stato dell'appliance è **Down** (Inattivo), esaminare la configurazione dell'appliance e la connessione tra l'SMC e l'appliance.

   Se un'appliance non viene visualizzata nell'inventario, aggiungerla.
2. Per ciascuna appliance, fare clic sul menu Actions (Azioni), quindi selezionare **Edit Appliance Configuration** (Modifica configurazione dell'appliance).
3. Selezionare la scheda Appliance. Accertarsi che siano selezionate le opzioni **Enable SSH** (Abilita SSH) e **Enable Root SSH Access** (Abilita accesso SSH root). **Non** proseguire con l'inizializzazione del Data Store finché tutte le appliance desiderate non hanno l'accesso SSH e l'accesso SSH root abilitati.

Se uno degli accessi non è selezionato, selezionare l'opzione e fare clic su **Apply Settings** (Applica impostazioni).

Distribuzione delle password del Data Store sull'SMC, sui Data Node e sui Flow Collector

Dall'interfaccia della riga di comando dell'SMC, è possibile eseguire uno script che prepara l'implementazione di Stealthwatch per l'inizializzazione del Data Store distribuendo le informazioni necessarie per stabilire connessioni sicure con il Data Store. La prima opzione dello script permette di creare le password per gli account utente `dbadmin` e `readonlyuser` e le distribuisce in modo sicuro all'SMC, ai Data Node e ai Flow Collector. Ciascuna password deve rispettare i seguenti requisiti:

- deve contenere almeno 1 numero
- deve contenere almeno 1 carattere minuscolo
- deve contenere almeno 1 carattere maiuscolo
- deve contenere almeno 1 carattere speciale tra i seguenti: `<>.,?/'"|:;` `~!@#$%^&*()-_+={}[]`
- deve avere almeno 8 caratteri, ma non ha limiti di lunghezza
- deve contenere solo caratteri ASCII

Quando si esegue uno script per inizializzare il Data Store, lo script utilizza queste informazioni per impostare le credenziali degli account utente `dbadmin` e `readonlyuser` e stabilire le connessioni sicure tra ciascuna appliance e il Data Store.

> Se queste password vengono perse, contattare il supporto Cisco per recuperarle.

Tenere presente che questa opzione viene utilizzata alla prima implementazione del Data Store. Se il Data Store è già stato inizializzato e si desidera aggiornare queste password, vedere Aggiornamento delle password dbadmin e readonlyuser del Data Store per ulteriori informazioni.

Operazioni preliminari

- Compilare un elenco di password root per l'SMC, i Data Node, i Flow Collector e l'SMC secondaria, se presente.
- Accedere alla console SMC come utente `root`.

Procedura

1. Dalla riga di comando, immettere `cd /lancope/admin/cds` e premere Invio per cambiare directory.
2. Immettere `./setup-sw-datastore-secure-connectivity` e premere Invio per eseguire lo script bash di connettività sicura del Data Store.
3. Dal menu principale dello script, selezionare **1. Distribute SW DataStore password to appliances** (Distribuisci SW DataStore alle appliance).

   Lo script visualizza un elenco contenente l'SMC, i Data Node gestiti dall'SMC, i Flow Collector supportati dal Data Store e gestiti dall'SMC e l'eventuale SMC secondaria supportata dal Data Store e gestita dall'SMC principale.
4. Confermare l'elenco delle appliance e selezionare **OK**. La prima volta che si esegue questo script durante la configurazione dell'implementazione di Stealthwatch per l'uso con il Data Store, vengono selezionate tutte le appliance.
5. Sulla riga di comando, quando viene chiesta la password `root` di ciascuna appliance, immettere la password e premere Invio.

   > Quando si immettono più password, accertarsi di digitare correttamente la password dell'appliance.

   Dopo aver immesso le password `root` di tutte le appliance, lo script chiede le password per `dbadmin` e `readonlyuser`.
6. Immettere la password **dbadmin**.
7. Immettere la stessa password `dbadmin` nel campo **dbadmin (confirmation)** (conferma).
8. Immettere la password **readonlyuser**.
9. Immettere la stessa password `readonlyuser` nel campo **readonlyuser (confirmation)** (conferma).

   > Non immettere la stessa password per `dbadmin` e `readonlyuser`. L'assegnazione della stessa password causa errori nello script ed entrambi gli account utente rimarranno senza password.
10. Selezionare **OK**.

    Lo script distribuisce queste password alle appliance selezionate in modo sicuro. Al termine, viene visualizzato un elenco di appliance aggiornate.
11. Selezionare **OK** per tornare al menu principale dello script.

Come procedere

- Distribuire i certificati di identità del Data Store per comunicazioni sicure, come descritto nella procedura successiva.

Distribuzione dei certificati di identità per stabilire connessioni sicure tra il Data Store e le appliance

Nello script per stabilire connessioni sicure con il Data Store, la seconda opzione consente di generare un certificato di identità e distribuirlo a SMC, i Data Node e i Flow Collector. Quando si esegue uno script per inizializzare il Data Store, lo script usa questo certificato di identità per stabilire connessioni sicure tra le appliance e i Data Store.

Il certificato di identità viene allineato automaticamente, è valido per 5 anni e viene generato con il nome comune `sw-datastore.stealthwatch.cisco.com`.

Operazioni preliminari

- Dalla riga di comando dell'SMC, eseguire lo script `setup-sw-datastore-secure-connectivity`.

Procedura

1. Dal menu principale dello script, selezionare **2. Distribute Certificates for Secure DB Connection** (Distribuisci certificati per connessioni sicure al database).
2. Lo script visualizza un elenco contenente l'SMC, i Data Node gestiti dall'SMC, i Flow Collector supportati dal Data Store e gestiti dall'SMC e l'eventuale SMC secondaria e gestita dall'SMC principale.

   Se l'elenco di appliance è già stato confermato dopo aver selezionato **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance), lo script potrebbe non essere visualizzato su questo elenco di appliance. Andare al passaggio 4.
3. Confermare l'elenco delle appliance e selezionare **OK**. La prima volta che si esegue questo script durante la configurazione dell'implementazione di Stealthwatch per l'uso con il Data Store, vengono selezionate tutte le appliance.

   Lo script genera un certificato di identità da utilizzare per le comunicazioni sicure e la chiave privata abbinata.
4. Sulla riga di comando, quando viene chiesta la password `root` di ciascuna appliance, immettere la password e premere Invio.

> Quando si immettono più password, accertarsi di digitare correttamente la password dell'appliance.

5. Quando lo script ha esito positivo, viene visualizzato un messaggio di esito positivo e l'indirizzo IP di un Data Node. Nella procedura successiva, si accede alla console del Data Node usando SSH per eseguire lo script di inizializzazione del Data Store.

> Registrare questo indirizzo IP prima di chiudere il messaggio. Non è possibile recuperarlo un volta chiuso il messaggio.

Come procedere

- Inizializzare il Data Store, come descritto nella procedura successiva.

Esecuzione di uno script per inizializzare il Data Store e stabilire connessioni sicure

Dopo aver distribuito le password utente `dbadmin` e `readonlyuser` e il certificato d'identità alle appliance, accedere al Data Node, come specificato nella procedura precedente, modificare il file di configurazione `install_SDBN.cfg` ed eseguire lo script di inizializzazione `install_SDBN.initial.py`. Questo script inizializza il Data Store, collegando i Data Node, imposta le credenziali `dbadmin` e `readonlyuser` fornite e stabilisce connessioni sicure tra le appliance Stealthwatch e il Data Store.

Dopo aver inizializzato il Data Store, copiare la chiave API principale del Data Store da questo Data Node. Usare le informazioni in **Configurazione di Vertica Management Console** per installare la console VMC (Vertica Management Console) sull'SMC.

Operazioni preliminari

- Compilare un elenco di tutti gli indirizzi IP pubblici di `eth0` del Data Node e di indirizzi IP privati del port-channel `eth2` o `eth2/eth3`.
- Accedere come utente `root` alla console del Data Node il cui indirizzo IP è stato visualizzato dopo aver distribuito i certificati di identità utilizzando lo script di connessioni sicure del Data Store, come descritto in **Distribuzione dei certificati di identità per stabilire connessioni sicure tra il Data Store e le appliance**.

Procedura

1. Dalla riga di comando, immettere `cd /lancope/database` e premere Invio per cambiare directory.
2. Immettere `cp install_SDBN_example.cfg install_SDBN.cfg` e premere Invio per effettuare una copia del file di configurazione di esempio.
3. Immettere `vi install_SDBN.cfg` e premere Invio per modificare il file di configurazione in un editor di testo.
4. Creare sezioni `[nodeN]` numerate consecutivamente, pari al numero di Data Node che si stanno implementando. Ad esempio, se sono stati implementati 6 Data Node, il file conterrà quanto segue:

```
[node1]
private = 169.254.42.30
public = 10.0.16.30
[node2]
private = 169.254.42.31
public = 10.0.16.31
[node3]
private = 169.254.42.32
public = 10.0.16.32
[node4]
private = 169.254.42.33
public = 10.0.16.33
[node5]
private = 169.254.42.34
public = 10.0.16.34
[node6]
private = 169.254.42.35
public = 10.0.16.35
[common]
subnet = 10.0.16.0
```

5. A partire dalla sezione `[node1]`, immettere l'indirizzo IP privato (`eth2` o port-channel `eth2/eth3`) e l'indirizzo IP pubblico (`eth0`) per ciascun Data Node. Tenere presente quanto segue:
    - Questo script assegna i Data Node al Data Store nell'ordine in cui sono elencati. Se i Data Node sono stati implementati con alimentatori ridondanti, assegnare i nodi alternandoli sui due alimentatori per assicurare massimi tempi di attività del Data Store e la ridondanza dei dati.

- Gli indirizzi IP privati devono essere non indirizzabili, su una LAN o VLAN privata. Assegnare gli indirizzi IP dal blocco CIDR `169.254.42.0/24`.
- Non sovrapporre gli indirizzi IP tra i Data Node.
- Aggiungere solo i Data Node che si desidera includere nel Data Store.

6. Nella sezione `[common]`, aggiornare la `subnet` con l'indirizzo IP più piccolo presente nel blocco CIDR.
7. Premere Esc, immettere `:wq` e premere Invio per salvare le modifiche, quindi uscire dall'editor di testo.
8. Dalla riga di comando, immettere `python install_SDBN_initial.py -i install_SDBN.cfg` e premere Invio per eseguire lo script python di inizializzazione del Data Store. Questo script usa il file di configurazione `install_SDBN.cfg` per inizializzare i Data Node nell'ordine specificato.

   Al termine dello script, riesaminare i messaggi di stato della CLI per accertarsi che lo script sia stato eseguito correttamente.

   > Per ciascun Data Node, la console visualizza il messaggio `Prerequisites not fully met during local (OS) configuration` ed elenca una serie di messaggi di log: `HINT (S0305)`, `HINT (S0041)`, `HINT (S0040)`, `WARN (N0010)`, `FAIL (s0180)` e `FAIL (s0311)`. Questi messaggi di log non indicano un errore di inizializzazione del Data Store. Per ulteriori informazioni su questi messaggi, vedere **Risoluzione dei problemi di implementazione del Data Store**.

   > Per ciascun Data Node, la console visualizza il messaggio `INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified`. Questi messaggi di log sono normali e non indicano che si è verificato un errore nel tentativo di stabilire una connessione sicura con il Data Store. Per ulteriori informazioni su questi messaggi, vedere **Risoluzione dei problemi di implementazione del Data Store**.

9. Immettere `cd /opt/vertica/config` per cambiare directory.
10. Immettere `cat apikeys.dat` per visualizzare la stringa della chiave API sulla console.

11. Copiare la stringa della chiave API e incollarla in un comune editor di testo. Usare questa chiave API in **Configurazione di Vertica Management Console** per configurare la console VMC sull'SMC.
12. Prendere nota dell'indirizzo IP di questo Data Node. Usare l'indirizzo IP in **Configurazione di Vertica Management Console** per configurare la console VMC sull'SMC.

Come procedere

- Usare Local Resolution (Risoluzione locale) in Central Management (Gestione centralizzata) per associare gli indirizzi IP del Data Node al nome del Data Store, come descritto nella procedura successiva.

Associazione del nome del Data Store sui Data Node con la risoluzione locale

Dopo aver inizializzato il Data Store, usare Central Management per associare il nome del Data Store (`sw-datastore`) a tutti gli indirizzi IP del Data Node per l'SMC e i Flow Collector. Poiché il Data Store contiene più Data Node, la mappatura con risoluzione locale aiuta a distribuire le richieste di archiviazione e query dei flussi in modo più uniforme tra i Data Node, migliorando le prestazioni e la risposta.

> Per prestazioni ottimali, mappare gli indirizzi IP di Data Node `eth0` nello **stesso ordine** per ciascuna appliance.

Operazioni preliminari

- Compilare un elenco di tutti gli indirizzi IP pubblici del Data Node.
- Compilare un elenco dei Flow Collector gestiti in Central Management.
- Accedere a SMC Web App come utente amministratore, quindi andare a Central Management.

Procedura

1. Dalla console SMC, fare clic sul menu Actions (Azioni), quindi selezionare **Edit Appliance Configuration** (Modifica configurazione dell'appliance).
2. Selezionare la scheda Network Services (Servizi di rete).
3. Nella sezione Local Resolution (Risoluzione locale), fare clic su **Add New** (Aggiungi nuovo).
4. Immettere `sw-datastore` nel campo **Host Name** (Nome host).

5. Immettere il primo indirizzo IP pubblico del Data Node dall'elenco.
6. Fare clic su **Add** (Aggiungi).
7. Ripetere i tre passaggi precedenti per tutti i Data Node rimanenti usando l'elenco degli indirizzi IP pubblici dei Data Node.
8. Fare clic su **Apply Settings** (Applica impostazioni), quindi confermare le modifiche apportate.
9. Ripetere questa procedura per tutti i Flow Collector nell'elenco e per l'SMC secondaria, se implementata.

> Per prestazioni ottimali, mappare gli indirizzi IP di Data Node `eth0` nello **stesso ordine** per ciascuna appliance.

Come procedere

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Configurare la console VMC (Vertica Management Console) sull'SMC. Per ulteriori informazioni, vedere la sezione successiva.

Configurazione di Vertica Management Console

Dopo aver inizializzato e configurato il Data Store, configurare la console VMC (Vertica Management Console) sull'SMC in modo che possa connettersi al Data Store. È possibile utilizzare la console VMC per monitorare l'integrità del Data Store e ricevere notifiche in base alle soglie configurate. Effettuare quanto segue:

1. Da un browser Web sulla postazione di lavoro locale, eseguire la configurazione iniziale della console VMC, tra cui configurazione della VMC per impedire l'uso dei server TLS 1.0 e 1.1 sia per l'accesso al browser Web sia per le notifiche e-mail.
2. Sulla console VMC, configurare una connessione sicura protetta con il Data Store.
3. Sulla console VMC, configurare le notifiche automatiche, ad esempio tramite e-mail, e le soglie delle notifiche.

> Se si usa l'opzione **3. Update SW DataStore password on appliances** (Aggiorna password SW DataStore sulle appliance) in `setup-sw-datastore-secure-connectivity` per aggiornare la password `dbadmin` dopo averla inizialmente impostata, accedere alla console VMC come `dbadmin` per aggiornare manualmente la password. Per ulteriori informazioni, vedere Aggiornamento delle password dbadmin e readonlyuser del Data Store dopo l'inizializzazione.

Esecuzione della configurazione iniziale della console VMC

La configurazione iniziale della console VMC viene eseguita al primo accesso.

Per impostazione predefinita, VMC consente di effettuare connessioni ai server TLS 1.0 e TLS 1.1 da un browser Web. Poiché le versioni precedenti di TLS sono meno sicure della versione TLS 1.2+, configurare la VMC in modo da impedire qualsiasi connessione sui server TLS 1.0 e TLS 1.1.

Operazioni preliminari

- Tenere a disposizione l'indirizzo IPv4 dell'SMC.
- Accertarsi che la porta di comunicazione `9450/TCP` sia aperta tra la postazione di lavoro e l'SMC.

Procedura

1. Sulla postazione di lavoro, aprire un browser Web e immettere `https://[`*`smc-ipv4-address`*`]:9450/webui/login` sulla barra degli indirizzi. Sostituire `[`*`smc-ipv4-address`*`]` con l'indirizzo IPv4 dell'SMC. Andare all'URL.
2. Accettare la licenza Vertica, quindi fare clic su **Next** (Avanti).
3. Immettere la **Password** `dbadmin`, quindi digitarla nuovamente in **Confirm password** (Conferma password).

   > Questo account utente `dbadmin` è un account VMC che viene associato successivamente all'account utente `dbadmin` del Data Store. È possibile assegnare a questo account una password diversa da quella assegnata all'account utente `dbadmin` del Data Store.

4. Immettere `dbadmin` come **Unix group name** (Nome di gruppo UNIX).
5. Lasciare invariati i percorsi dei file (`/home/dbadmin`) e la porta (`5450`), quindi fare clic su **Next** (Avanti).

   Vengono visualizzate le opzioni di archiviazione.
6. Fare clic su **Next** (Avanti).

   Vengono visualizzate le opzioni di autorizzazione della console di gestione.
7. Fare clic su **Next** (Avanti). Attendere il riavvio del servizio Vertica.

   Questa operazione potrebbe richiedere più di 20 minuti. Se la finestra del browser non si aggiorna automaticamente, riaggiornare manualmente la pagina.

8. Immettere le credenziali `dbadmin`, quindi fare clic su **Log in** (Accedi) per accedere alla console VCM.
9. Dalla pagina principale della VMC, fare clic su **MC Settings** (Impostazioni MC).
10. Fare clic sulla scheda Configuration (Configurazione).
11. Selezionare **Disable TLS 1.0 and 1.1 connections from browser** (Disabilita le connessioni TLS 1.0 e 1.1. dal browser), quindi salvare le modifiche apportate.

Configurazione di una connessione sicura del VMC al Data Store

Prima di iniziare a configurare la connessione sicura, copiare il file `/lancope/var/admin/cds/server.crt` dall'SMC sulla postazione di lavoro locale. Utilizzare questo file per stabilire una connessione sicura tra la VMC e il Data Store.

Operazioni preliminari

- Copiare il file `/lancope/var/admin/cds/server.crt` dall'SMC alla postazione di lavoro locale.
- Tenere a disposizione una copia della chiave API principale del Data Store, come descritto in **Esecuzione di uno script per inizializzare il Data Store e stabilire connessioni sicure**.
- Tenere a disposizione l'indirizzo IP del Data Node da cui è stata copiata la chiave API, come descritto in **Esecuzione di uno script per inizializzare il Data Store e stabilire connessioni sicure**.

Procedura

1. Dalla pagina principale della VMC, fare clic su **Import a Vertica Database Cluster** (Importa un cluster del database Vertica).
2. Nell'apposito campo, immettere l'**indirizzo IP** dell'interfaccia `eth0` del Data Node da cui è stata copiata la chiave API, quindi fare clic su **Next** (Avanti).
3. Facoltativamente, è possibile modificare il **nome del cluster**.
4. Immettere la **chiave API** principale del Data Store nell'apposito campo, quindi fare clic su **Continue** (Continua).

   La VMC rileva l'Data Store.
5. Immettere `dbadmin` nel campo **Username** (Nome utente), quindi specificare la password `dbadmin` nell'apposito campo.

6. Selezionare **Use TLS** (Usa TLS).
7. Fare clic su **Configure TLS and Import DB** (Configura TLS e importa database).

   Viene visualizzata la finestra Configure TLS Connection Certificates (Configura certificati di connessione TLS).
8. Fare clic su **Configure TLS Connection** (Configura connessione TLS).
9. Selezionare **Upload a new CA Certificate** (Carica un nuovo certificato CA), quindi fare clic su **Next** (Avanti).
10. Fare clic su **Browse** (Sfoglia), quindi selezionare il file `server.crt` salvato sulla postazione di lavoro locale dall'SMC.
11. Immettere `sw-datastore-cert` nel campo **CA Certificate alias** (Alias certificato CA), quindi fare clic su **Next** (Avanti).
12. Fare clic su **Review** (Rivedi).
13. Fare clic su **Configure TLS for DB** (Configura TLS per database).

    Vengono configurate connessioni sicure tra la VMC e il Data Store.
14. Fare clic su **Close** (Chiudi).

> È possibile che durante l'importazione del database venga visualizzato il messaggio "Error while importing database on MC. undefined" (Errore sconosciuto durante l'importazione del database sull'MC). Questo messaggio è normale e non indica che si è verificato un errore nel tentativo di stabilire una connessione sicura con il Data Store.

Configurazione di notifiche VMC tramite e-mail

È possibile configurare la VMC in modo che vengano inviate notifiche di avviso via e-mail.

Operazioni preliminari

- Accedere alla VMC come utente `dbadmin`.

Procedura

1. Dalla pagina MC Settings (Impostazioni MC), fare clic sulla scheda Email Gateway (Gateway e-mail).
2. Immettere un nome host per il server SMTP in **SMTP Server (Hostname)**. È possibile immettere un nome di 255 caratteri o un indirizzo IP.
3. Specificare una **porta del server SMTP** nell'apposito campo.

4. Selezionare **Use TLS** (Usa TLS) in **Session Type (SSL or TLS)** (Tipo di sessione (SSL o TLS)).
5. Immettere un **nome utente per SMTP** nell'apposito campo.
6. Immettere una **password SMTP** nell'apposito campo.
7. In **Originating Email Alias** (Alias e-mail di origine) immettere un alias per l'e-mail di origine da cui la VMC invierà gli avvisi e-mail.
8. Fare clic su **Test** (Verifica) per verificare le impostazioni.

   Aggiornare le impostazioni se non si riceve un messaggio e-mail di prova.
9. Fare clic su **Apply** (Applica).

Configurazione delle soglie di avviso VMC

È possibile configurare varie soglie minime e massime che, se superate dal Data Store, generano un avviso sulla VMC.

Operazioni preliminari

- Accedere alla VMC come utente `dbadmin`.

Procedura

1. Selezionare **Settings > Thresholds** (Impostazioni > Soglie).
2. Selezionare la casella di controllo delle soglie di avviso per abilitarle o deselezionarla per disabilitarle. Cisco consiglia di abilitare le notifiche `Node State Change` (Modifica dello stato dei nodi) per ricevere le notifiche quando un Data Node diventa inattivo.

   > Quando si configurano le soglie minime, può essere generato un numero eccessivo di notifiche di falsi positivi. Ad esempio, se si imposta la soglia minima della CPU del nodo, questo potrebbe attivarsi di frequente poiché l'utilizzo della CPU varia.
3. Selezionare *Priority 1* (Priorità 1) per ciascuna soglia di notifica che attiverà l'invio di e-mail.
4. Se si seleziona *Priority 1* (Priorità 1), fare clic sull'icona accanto a **Email Destination** (Destinazione e-mail) per sfogliare i file.
5. Immettere un indirizzo e-mail in **Entering New Field** (Immissione nuovo campo), quindi fare clic sull'icona **+**.
6. Fare clic su **OK**.

7. Specificare un intervallo di invio per le e-mail in **Email Interval** (Intervallo e-mail) per stabilire la frequenza con cui le e-mail verranno inviate quando il Data Store supera una soglia.
8. Fare clic su **Apply** (Applica).

Come procedere

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Configurare la durata di conservazione dei dati del Data Store, come descritto nella sezione successiva.

Configurazione della durata di conservazione dei dati nel Data Store

Per impostazione predefinita, il Data Store conserva i dati per almeno sette (7) giorni prima di eliminarli automaticamente. Utilizzando l'API REST di Stealthwatch, è possibile modificare il periodo di conservazione:

- in un valore diverso, fino a 3000 giorni, oppure
- archiviare i dati il più a lungo possibile, finché il Data Store non raggiunge la capacità massima.

Sulla durata di conservazione del Data Store, tenere presente quanto segue:

- Dopo aver aggiornato le impostazioni sulla conservazione dei dati, non è necessario riavviare le appliance Stealthwatch o il Data Store. Le impostazioni diventano effettive dopo alcuni minuti.
- Quando si aumenta la durata di conservazione, prima che la nuova impostazione venga effettivamente applicata, aspettare che trascorra la differenza tra la durata precedente e la nuova durata specificata. Finché non viene applicata la nuova impostazione, i dati vengono visualizzati con la risoluzione più approssimata. Ad esempio, se si modifica la durata di conservazione dei dati da 3 a 10 giorni, è necessario attendere 7 giorni prima che la nuova impostazione abbia effetto.
- I dati potrebbero essere eliminati prima del periodo selezionato, a causa della mancanza di spazio libero. Se si sceglie di archiviare i dati il più a lungo possibile, quando il Data Store raggiunge la capacità massima, il sistema inizia a eliminare i dati meno recenti.
- Se non si desidera memorizzare i dati, è possibile accedere all'interfaccia dell'utente amministratore per ciascun Flow Collector, quindi selezionare **Support > Advanced Settings** (Supporto > Impostazioni avanzate). Per ciascun Flow Collector, modificare la voce "interface_retention_days" nella colonna Option Label (Etichetta opzione) a 0 (zero), quindi riavviare Flow Collector (o il motore del Flow Collector).

Per aggiornare queste impostazioni, utilizzare l'API REST per effettuare le seguenti operazioni:

Autenticazione con l'API REST dell'SMC

Richiesta delle informazioni sulla risorsa

Risorsa	Descrizione
URI	`https://[smc-eth0-ip]/token/v2/authenticate`
Descrizione	Autenticazione con l'API REST dell'SMC.
Parametro URI	• *[smc-eth0-ip]* - Indirizzo IP di gestione eth0 dell'SMC
Metodo HTTP	POST
Tipo MIME del corpo richiesta	application/x-www-form-urlencoded
Corpo richiesta	`username=[username]&password=[password]`
Parametri del corpo della richiesta	• *[username]*- (OBBLIGATORIO) utente amministratore dell'SMC • *[password]*- (OBBLIGATORIO) password dell'account utente amministratore dell'SMC

Codice e definizione della risposta corretta

Risposta	Descrizione
Codice risposta	200 - Operazione riuscita
Corpo risposta	Il corpo della risposta contiene informazioni sui cookie, che è necessario trasferire nelle successive chiamate API REST per questa sessione. La sessione è valida per 20 minuti.

Recupero delle impostazioni corrette sulla durata di conservazione del Data Store

Richiesta delle informazioni sulla risorsa

Risorsa	Descrizione
URI	`https://[smc-eth0-ip]/smc-`

Risorsa	Descrizione
	`configuration/rest/v1/cds/retentionsettings`
Descrizione	Recuperare le impostazioni di conservazione correnti del Data Store.
Parametro URI	• *`[smc-eth0-ip]`* - Indirizzo IP di gestione eth0 dell'SMC
Metodo HTTP	RISULTATI
Tipo MIME del corpo richiesta	n/d
Corpo richiesta	n/d
Parametri del corpo della richiesta	n/d

Informazioni e codice di esito positivo

Risorsa	Descrizione
Codice risposta	200 - Operazione riuscita
Corpo risposta	Il corpo della risposta contiene le impostazioni di conservazione dei dati correnti del Data Store. Se non è stato modificato in precedenza, il valore predefinito è 7 giorni.

Aggiornamento delle impostazioni di conservazione dei dati del Data Store

Richiesta delle informazioni sulla risorsa

Risorsa	Descrizione
URI	`https://`*`[smc-eth0-ip]`*`/smc-configuration/rest/v1/cds/retentionsettings`

Risorsa	Descrizione
Descrizione	Aggiornare le impostazioni di conservazione dei dati correnti del Data Store.
Parametro URI	• *[smc-eth0-ip]* - Indirizzo IP di gestione eth0 dell'SMC
Metodo HTTP	PUT
Tipo MIME del corpo richiesta	application/json

Corpo richiesta	`{`
	`"interfaceRetentionType":"`*[type]*`",`
	`"interfaceRetentionAmount":"`*[#]*`"`
	`}`

Parametri del corpo della richiesta	• *[type]* - (OBBLIGATORIO) Il tipo di conservazione dei dati, impostato su uno dei seguenti valori di stringa:
	  • `AMOUNT` - Memorizza i dati per il numero di giorni definito in interfaceRetentionAmount prima di eliminarli
	  • `FOREVER` - Memorizza i dati il più a lungo possibile, fino al raggiungimento della capacità massima del Data Store, prima di eliminarli
	• *[#]* - (OBBLIGATORIO) La durata massima, in giorni, durante cui il Data Store conserva i dati, prima di eliminarli, espressa con un numero intero compreso tra `1-3000`.
	  Se si imposta `interfaceRetentionType` su `FOREVER`, occorre comunque superare il numero di giorni indicato da `interfaceRetentionAmount`, ignorato dal sistema. Questo valore viene memorizzato internamente su `7` per impostazione predefinita, a prescindere dal numero di giorni indicato da `interfaceRetentionAmount` e superato nella situazione specifica.

Informazioni e codice di esito positivo

Risorsa	Descrizione
Codice risposta	204 - Operazione riuscita (nessun contenuto)
Corpo risposta	Il corpo della risposta non contiene contenuti.

Per ulteriori informazioni sull'API REST, vedere Documentazione API REST di Stealthwatch Enterprise.

La procedura seguente fornisce una sintassi curl per l'aggiornamento del periodo di conservazione dei dati del Data Store.

Aggiornamento del periodo di conservazione del Data Store

Operazioni preliminari

- Accedere alla console di un'appliance basata su Linux con curl installato.

Procedura

1. Copiare il seguente comando e incollarlo in un normale editor di testo:

   ```
   curl -c cookies.txt -d "username=[username]&password=
   [password]" https://[smc-eth0-ip]/token/v2/authenticate
   ```

2. Sostituire *[username]* con il nome dell'amministratore dell'SMC.
3. Sostituire *[password]* con la password dell'amministratore dell'SMC.
4. Sostituire *[smc-eth0-ip]* con l'indirizzo IP di `eth0` dell'SMC.
5. Copiare il comando aggiornato, incollarlo nella riga di comando e premere Invio per eseguire l'autenticazione sull'SMC con l'API REST.

   La sessione è valida per 20 minuti.

6. Copiare il seguente comando e incollarlo in un normale editor di testo:

   ```
   curl -X GET -b cookies.txt https://[smc-eth0-ip]/smc-
   configuration/rest/v1/cds/retentionsettings
   ```

7. Sostituire *[smc-eth0-ip]* con l'indirizzo IP di `eth0` dell'SMC.
8. Copiare il comando aggiornato, incollarlo nella riga di comando e premere Invio per recuperare le impostazioni di conservazione correnti del Data Store.

Se è la prima volta che si esegue il controllo, il Data Store viene configurato con un periodo di conservazione predefinito di 7 giorni.

9. Copiare il seguente comando e incollarlo in un normale editor di testo:

```
curl -X PUT -b cookies.txt -H "Content-
Type:application/json" -d '{"interfaceRetentionType":"
[type]","interfaceRetentionAmount":"[#]"}' https://[smc-
eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings
```

10. Sostituire *[type]* con uno dei seguenti valori:
    - `AMOUNT` se si desidera indicare un numero di giorni specifico.
    - `FOREVER` se si desidera memorizzare i dati il più a lungo possibile.
11. Sostituire *[#]* con un valore intero compreso tra `1-3000` per il numero di giorni di conservazione dei dati.

    Questo valore deve essere definito anche se si sceglie *[type]*=`FOREVER`. In questo caso, il sistema ignora questo valore e lo imposta internamente a `7`.
12. Sostituire *[smc-eth0-ip]* con l'indirizzo IP di `eth0` dell'SMC.
13. Copiare il comando aggiornato, incollarlo nella riga di comando e premere Invio per aggiornare le impostazioni di conservazione.

> Dopo aver aggiornato le impostazioni sulla conservazione dei dati, non è necessario riavviare le appliance Stealthwatch o il Data Store. Le impostazioni diventano effettive dopo alcuni minuti. Tuttavia, quando si aumenta la durata di conservazione, prima che la nuova impostazione venga effettivamente applicata, aspettare che trascorra la differenza tra la durata precedente e la nuova durata specificata.

Come procedere

- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.
- Rivedere i passaggi successivi, come descritto nella sezione successiva.

Fasi successive dell'installazione del Data Store

Dopo aver implementato e configurato Stealthwatch in modo da poterlo usare con un Data Store:

- Installare l'app Stealthwatch Report Builder sull'SMC per generare i report sull'implementazione del Stealthwatch e per visualizzare le statistiche di archiviazione del Data Store. Per ulteriori informazioni, vedere le note sulla versione.
- Per ulteriori informazioni su come usare Stealthwatch, consultare la guida online di Stealthwatch Web App.
- Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.

Manutenzione del Data Store

Di seguito viene descritto il Data Store e le attività di manutenzione correlate per il Data Store, tra cui:

- riavvio di un Data Node e del Data Store
- backup e ripristino del Data Store
- aggiunta, rimozione e sostituzione dei Data Node
- copia delle informazioni sull'attendibilità su una SMC di failover prima di trasferirle a una SMC principale

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

Riavvio di un Data Node

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

In caso sia necessario riavviare un Data Node, immettere il comando di arresto, quindi immettere il comando di riavvio.

Arresto e riavvio del Data Node

Operazioni preliminari

- Accedere alla console del Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Copiare il seguente comando e incollarlo in un normale editor di testo:

   `/opt/vertica/bin/admintools -t stop_node -s [data-node-hostname]`

3. Prima di procedere al riavvio, sostituire `[data-node-hostname]` con il nome host del Data Node che si desidera arrestare.
4. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per arrestare il Data Node.

5. Copiare il seguente comando e incollarlo in un normale editor di testo:

   `/opt/vertica/bin/admintools -t restart_node -s [data-node-hostname]`

6. Sostituire `[data-node-hostname]` con il nome host del Data Node che si desidera riavviare.
7. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per riavviare il Data Node.

Riavvio del Data Store

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

Per riavviare il Data Store, immettere il comando per arrestarlo, quindi immettere il comando per riavviarlo.

Arresto e riavvio del Data Store

Operazioni preliminari

- Accertarsi che i Flow Collector non siano connessi al Data Store e che non vi sia trasferimento di dati.
- Accertarsi che l'SMC non sia collegata al Data Store ed eseguire le query o aggiornare il Data Store.
- Accedere alla console del Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Sono disponibili le seguenti opzioni:
   - Dal prompt dei comandi, immettere `/opt/vertica/bin/admintools -t stop_db -d sw` e premere Invio per arrestare il Data Store.
   - Dal prompt dei comandi, immettere `/opt/vertica/bin/admintools -t stop_db -d sw -F` e premere Invio per arrestare il Data Store, sovrascrivendo le connessioni Flow Collector o SMC.
3. Dal prompt dei comandi, immettere `/opt/vertica/bin/admintools -t start_db -d sw` e premere Invio per riavviare il Data Store.

Creazione del backup di un Data Store

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

Per eseguire il backup di Data Store, effettuare le seguenti operazioni:

- Stimare le dimensioni del backup
- Preparare un host di backup con una capacità di archiviazione doppia rispetto alle dimensioni dei dati di cui effettuare il backup

  > Usare un host basato su Linux distinto dalle appliance Stealthwatch.

- Installare Python 3.7 e rsync 3.0.5 sull'host di backup
- Accertarsi che tutti i Data Node possano raggiungere l'host di backup con l'accesso SSH senza uso di password
- Inizializzazione della directory di backup sull'host di backup
- Backup del Data Store

Valutazione dei requisiti di archiviazione dell'host di back-up

Operazioni preliminari

- Accedere alla console di un Data Node come utente `root`.

Procedura

1. Copiare il comando seguente, incollarlo nella riga di comando e premere Invio per connettersi al database usando vsql, quindi eseguire la query. Immettere la password quando richiesto. Prendere nota dei risultati.

   ```
   /opt/vertica/bin/vsql -U dbadmin -c "SELECT SUM(used_
   bytes) FROM storage_containers;"
   ```

2. Moltiplicare il risultato per 2 per valutare lo spazio di archiviazione che deve essere disponibile sull'host di backup.

Preparazione di un host di backup

Operazioni preliminari

- In base ai requisiti di archiviazione stimati nell'attività precedente, identificare un host Linux sulla rete in cui archiviare il backup o implementare un host Linux con i requisiti di archiviazione richiesti.

  > Usare un host basato su Linux distinto dalle appliance Stealthwatch.

- Accedere alla console dell'host di backup come utente `root`.

Procedura

1. Dal prompt dei comandi, immettere `python --version` e premere Invio per vedere la versione Python installata. Sono disponibili le seguenti opzioni:
   - Se la versione installata è Python 3.7, andare al passaggio 4.
   - In caso contrario, installare Python 3.7. Proseguire al passaggio 2.
2. Immettere `sudo apt-get update` e premere Invio per scaricare le versioni aggiornate dei pacchetti, Python incluso. Immettere la password quando richiesto.
3. Immettere `sudo apt-get install python3.7` e premere Invio per installare Python 3.7.
4. Dal prompt dei comandi, immettere rsync -version e premere Invio per vedere la versione rsync installata. Sono disponibili le seguenti opzioni:

   Se è installato rsync 3.0.5, andare al passo 7.

   In caso contrario, installare rsync 3.0.5. Proseguire al passaggio 5.
5. Immettere `sudo apt-get update` e premere Invio per scaricare le versioni aggiornate dei pacchetti, rsync incluso. Immettere la password quando richiesto.
6. Immettere `sudo apt-get install rsync` e premere Invio per installare rsync.
7. Dal prompt dei comandi, immettere `getent passwd | grep dbadmin` e premere Invio per determinare se l'account utente `dbadmin` è presente su questo host. Sono disponibili le seguenti opzioni:
   - Se l'account utente `dbadmin` è presente, l'host di backup è pronto. Andare alla sezione **Abilitazione dell'accesso SSH senza password per dbadmin**.

- In caso contrario, creare un account utente `dbadmin` su questo host. Proseguire al passaggio 5.

8. Dal prompt dei comandi, immettere `useradd dbadmin` e premere Invio per creare un account utente `dbadmin`.
9. Immettere `passwd dbadmin` e premere Invio per assegnare una password a `dbadmin`.
10. Immettere una **nuova password** e premere Invio per impostare la password `dbadmin`. Confermare la password quando richiesto.

Come procedere

- Abilitare l'accesso SSH senza password per l'account utente `dbadmin`, come descritto nella sezione successiva.

Abilitazione dell'accesso SSH senza password per dbadmin

Operazioni preliminari

- Aprire la porta 22/TCP tra l'host di backup e ciascun Data Node per SSH e la porta 50000/TCP tra l'host di backup e ciascun Data Node per rsync.
- Per ulteriori informazioni, riesaminare la documentazione OpenSSH su `ssh-copy-id`.
- Accedere al primo Data Node come utente `root`.

Procedura

1. Copiare il seguente comando e incollarlo in un normale editor di testo:

   `ssh-copy-id -i dbadmin@[`*`hostname`*`]`

2. Sostituire `[`*`hostname`*`]` con il nome dell'host di backup.
3. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per copiare la chiave SSH autorizzata `dbadmin` sull'host di backup.
4. Copiare il seguente comando e incollarlo in un normale editor di testo:

   `ssh 'dbadmin@[`*`hostname`*`]'`

5. Sostituire `[`*`hostname`*`]` con il nome dell'host di backup.
6. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per verificare che sia possibile accedere alla console dell'host remoto con SSH senza che sia necessario immettere una password da questo Data Node.

Inizializzazione della directory di backup sull'host di back-up

Operazioni preliminari

- Accedere alla console del primo Data Node come utente root.

  Prendere nota del Data Node usato per inizializzare la directory di backup. Il backup può essere eseguito anche da questo Data Node, come descritto in Backup del database del Data Store.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Copiare il comando seguente in un editor di testo: `ssh [backup-host-ip]`.
3. Sostituire `[backup-host-ip]` con l'indirizzo IP dell'host di backup.
4. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per verificare che sia possibile accedere all'interfaccia dell'host di backup come utente `dbadmin` senza dover inserire una password. Se l'host di backup richiede una password, controllare le impostazioni.
5. Immettere `cd /home/dbadmin` e premere Invio per cambiare directory.
6. Immettere `mkdir backups` e premere Invio per creare la directory `backups`.
7. Immettere `exit` e premere Invio per tornare al prompt della riga di comando del Data Node.
8. Immettere `vi pw.ini`, premere Invio per creare il file della password di backup `pw.ini` e modificarlo.

   > Se si aggiorna la password `dbadmin` con lo script `setup-sw-datastore-secure-connectivity`, aggiornare anche la password memorizzata nel file delle password di backup `pw.ini` oppure il backup non andrà a buon fine. Per ulteriori informazioni, vedere Aggiornamento delle password dbadmin e readonlyuser del Data Store dopo l'inizializzazione.

9. Copiare le seguenti righe in un normale editor di testo:

```
[Passwords]
dbPassword = [dbadmin-password]
```

10. Aggiornare `[dbadmin-password]` con la password `dbadmin` del Data Store.
11. Copiare le righe aggiornate e incollarle nel file delle password di backup `pw.ini`.
12. Premere Esc, quindi immettere `:wq` e premere Invio per uscire e salvare le modifiche.
13. Immettere `chmod 640 pw.ini` e premere Invio per modificare le autorizzazioni del file `pw.ini` e consentire all'utente `dbadmin` di leggere e modificare il file.
14. Immettere `vi config.ini` e premere Invio per creare il file di configurazione di backup `config.ini` e modificarlo.
15. Copiare le seguenti righe e incollarle in un normale editor di testo:

```
[Mapping]
v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
v_sw_node0003 = backup-host-ip:/home/dbadmin/backups

[Misc]
snapshotName = data_store_backup
passwordFile = /home/dbadmin/pw.ini
enableFreeSpaceCheck = True
retryCount = 2
retryDelay = 1

[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

16. Sostituire *`backup-host-ip`* con l'indirizzo IP dell'host di backup.
17. Se i nomi degli host in `[Mapping]` non corrispondono ai Data Node, aggiornare i nomi degli host.
18. Se implementati più di 3 volte nell'ambiente, accertarsi di avere una voce per ciascun Data Node.
19. Copiare le righe aggiornate e incollarle nel file `config.ini`.
20. Premere Esc, quindi immettere `:wq` e premere Invio per uscire e salvare le modifiche.

21. Immettere `vbr -t init -c config.ini` e premere Invio per inizializzare la directory `/home/dbadmin/backups` sull'host di backup e ricevere i backup del Data Store.

Backup del database del Data Store

Operazioni preliminari

- Accedere come utente `root` alla console del Data Node e inizializzare la directory dell'host di backup, come descritto in Inizializzazione della directory di backup sull'host di backup.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Immettere `vbr -t backup -c config.ini --debug 3 --dry-run` e premere Invio per eseguire un test senza creare il backup. Sono disponibili le seguenti opzioni:
   - Se il test di backup ha esito positivo, eseguire il backup di Data Store. Proseguire al passaggio 2.
   - Se il test di backup ha esito negativo, riesaminare i file di log del debug nella directory `/tmp/vbr`, risolvere la causa profonda, quindi eseguire nuovamente il backup. Se non è possibile risolvere il problema, contattare il supporto Cisco.
3. Immettere `vbr -t backup -c config.ini` e premere Invio per eseguire il backup del Data Store sulla directory `/home/dbadmin/backups` sull'host di backup.

Ripristino di un backup del Data Store

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

Per ripristinare il Data Store da un backup, accertarsi di quanto segue:

- Il Data Store è inattivo. È possibile arrestare il Data Store solo se i Flow Collector e SMC non sono connessi e sono state apportate le modifiche.
- Il backup e il Data Store hanno nomi dei nodi identici e lo stesso numero dei nodi.

Arresto del Data Store

Operazioni preliminari

- Accertarsi che i Flow Collector non siano connessi al Data Store e che non vi sia trasferimento di dati.
- Accertarsi che l'SMC non sia collegata al Data Store ed eseguire le query o aggiornare il Data Store.
- Accedere alla console del Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Sono disponibili le seguenti opzioni:
   - Dal prompt dei comandi, immettere `/opt/vertica/bin/admintools -t stop_db -d sw` e premere Invio per arrestare il Data Store.
   - Dal prompt dei comandi, immettere `/opt/vertica/bin/admintools -t stop_db -d sw -F` e premere Invio per arrestare il Data Store, sovrascrivendo le connessioni Flow Collector o SMC.

Ripristino del Data Store da un backup

Operazioni preliminari

- Se la password `dbadmin` è stata aggiornata con lo script `setup-sw-datastore-secure-connectivity`, aggiornare anche la password memorizzata nel file delle password di backup `pw.ini` oppure il backup non andrà a buon fine. Per ulteriori informazioni, vedere Aggiornamento delle password dbadmin e readonlyuser del Data Store dopo l'inizializzazione.
- Identificare il Data Node su cui è stato memorizzato il file di configurazione di backup `config.ini` e accedere alla console come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Dal prompt dei comandi, immettere `vbr --task restore --config-file config-file.ini` e premere Invio per ripristinare il Data Store dall'host di backup.

Avvio del Data Store

Operazioni preliminari

- Accedere alla console del Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Dal prompt dei comandi, immettere `/opt/vertica/bin/admintools -t start_db -d sw` e premere Invio per avviare il Data Store.

Come procedere

- Rimuovere l'istantanea del catalogo, come descritto nella sezione successiva.

Rimozione dell'istantanea del catalogo

Dopo aver riavviato il Data Store, rimuovere l'istantanea chiamata `catalog`. Questa istantanea non è necessaria dopo aver effettuato correttamente il ripristino e impedisce a Vertica di gestire la policy di conservazione.

Operazioni preliminari

- Accedere alla console del Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Copiare il seguente comando e incollarlo in un normale editor di testo:

   `/opt/vertica/bin/vsql -U dbadmin -w [`*`password`*`] -c "select remove_database_snapshot('catalog');"`
3. Sostituire `[password]` con la password `dbadmin`.
4. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per rimuovere l'istantanea `catalog`.

Come procedere

- Ricollegare i Flow Collector al Data Store e accertarsi che i dati vengano trasferiti.
- Ricollegare SMC al Data Store.

Aggiunta di tre Data Node al Data Store

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

È possibile espandere il Data Store in incrementi di tre Data Node o multipli di Data Node. Per espandere il numero di Data Node nel Data Store, attenersi alla seguente procedura:

Preparazione del Data Store per l'aggiunta di Data Node e il ribilanciamento

Prima di aggiungere un Data Node, effettuare quanto segue:

- Eseguire il backup del Data Store. Per ulteriori informazioni, vedere **Creazione del backup di un Data Store**.
- Accertarsi che i Flow Collector non siano connessi al Data Store e che non vi sia trasferimento di dati.
- Accertarsi che l'SMC non sia collegata al Data Store ed eseguire le query o aggiornare il Data Store.
- Eliminare le vecchie partizioni dati non utilizzate. Per identificare queste partizioni, contattare Cisco Professional Services.
- Disabilitare i segmenti locali. Da vsql, immettere `SELECT DISABLE_LOCAL_SEGMENTS();`
- Aggiornare le impostazioni del pool di risorse. Da vsql, immettere `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '70%;`

Aggiunta di Data Node al Data Store

Se questo passaggio non è stato ancora eseguito, implementare i Data Node sulla rete in multipli di 3. Per completare la configurazione iniziale, in System Configuration (Configurazione di sistema) usare l'impostazione iniziale e lo strumento Appliance Setup Tool. Per ulteriori informazioni, vedere l'**Appendice B. Installazione dell'hardware di Stealthwatch** e l'**Appendice C. Configurazione delle appliance**.

Dopo aver configurato i Data Node e assegnato un indirizzo IP indirizzabile della porta di gestione `eth0` e un indirizzo IP non indirizzabile di `eth2` o del port-channel `eth2/eth3`, attenersi a quanto segue:

- Accedere al Data Node e configurare il file `update_SDBN.cfg` per aggiungere nuovi Data Node.
- Eseguire lo script `update_SDBN.py` per aggiungere i Data Node al Data Store e, facoltativamente, aggiungerli anche al database del Data Store.

Aggiunta di Data Node al Data Store

Operazioni preliminari

- Accedere alla console di un Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Dalla riga di comando, immettere `cd /lancope/database` e premere Invio per cambiare directory.
3. Immettere `cp update_SDBN_example.cfg update_SDBN.cfg` e premere Invio per effettuare una copia del file di configurazione di esempio del Data Node da aggiungere.
4. Immettere `vi update_SDBN.cfg` e premere Invio per modificare il file di configurazione del Data Node da aggiungere in un comune editor di testo.
5. Creare sezioni `[nodeN]` numerate consecutivamente, pari al numero di Data Node che si desidera aggiungere al Data Store. Ad esempio, se sono stati implementati già 3 Data Node sulla rete, e si vogliono aggiungere altri 6 Data Node, il file deve contenere quanto segue:

```
[node1]
private = 169.254.42.30
public = 10.0.16.114
[node2]
private = 169.254.42.31
public = 10.0.16.115
[node3]
private = 169.254.42.32
public = 10.0.16.116
[node4]
private = 169.254.42.33
public = 10.0.16.117
[node5]
private = 169.254.42.34
```

```
public = 10.0.16.118
[node6]
private = 169.254.42.35
public = 10.0.16.119
[common]
subnet = 10.0.16.0
firstNode = 4
```

6. A partire dalla sezione `[node1]`, immettere gli indirizzi IP privati e pubblici per ciascun nuovo Data Node. Tenere presente quanto segue:
   - Questo script aggiunge Data Node al Data Store nell'ordine elencato, numerati consecutivamente dopo il Data Node con il numero più alto già appartenente al Data Store. Se si implementano i Data Node in rack diversi, alternare l'assegnazione dei nodi tra i rack per aumentare al massimo la ridondanza dei dati.
   - Gli indirizzi IP privati devono essere non indirizzabili, su una LAN o VLAN privata. Assegnare gli indirizzi IP dal blocco CIDR `169.254.42.0/24`.
   - Non sovrapporre gli indirizzi IP tra i Data Node.
   - Non aggiungere il Data Node sostitutivo qui, anche se è stato implementato nell'ambiente senza configurarlo. Aggiungere solo i Data Node che si desidera includere nel Data Store.
7. Nella sezione `[common]`, aggiornare la `subnet` in modo che corrisponda agli indirizzi IP pubblici.
8. Nella sezione `[common]`, aggiornare il valore `firstNode` in modo che sia superiore di uno al numero di Data Node già appartenenti al Data Store.
9. Premere Esc, immettere `:wq` e premere Invio per salvare le modifiche, quindi uscire dall'editor di testo.
10. Dalla riga di comando sono disponibili le seguenti opzioni:

    Immettere `python update_SDBN.py -i update_SDBN.cfg` e premere Invio per eseguire lo script phyton per aggiungere il Data Node. Questo script usa il file di configurazione `update_SDBN.cfg` per aggiungere i nuovi Data Node al Data Store nell'ordine specificato. Tenere presente che in questo caso **non** verranno aggiunti al database.

    Immettere `python update_SDBN.py -i update_SDBN.cfg -d` e premere Invio per eseguire lo script python per aggiungere il Data Node. Questo script usa il file di configurazione `update_SDBN.cfg` per aggiungere i nuovi Data Node al

Data Store nell'ordine specificato, quindi aggiungere i Data Node come parte del database.

Al termine dello script, riesaminare i messaggi di stato della CLI per accertarsi che lo script sia stato eseguito correttamente.

11. Immettere `cd /opt/vertica/config` per cambiare directory.
12. Immettere `vi apikeys.dat` per aprire il file delle chiavi API in un editor di testo.
13. Premere Esc, quindi immettere `q!` e premere Invio per uscire dall'editor di testo senza salvare le modifiche.
14. Prendere nota dell'indirizzo IP di questo Data Node. Usare l'indirizzo IP in **Manutenzione del Data Store** per configurare la console VMC sull'SMC.

Se i nuovi Data Node non vengono aggiunti al database con lo script `update_SDBN.py`, è possibile aggiungere i Data Node manualmente. Accedere al Data Node nel Data Store e aggiungere i Data Node al Data Store.

Aggiunta di nuovi Data Node al Data Store

Operazioni preliminari

- Accedere al Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Copiare il seguente comando e incollarlo in un normale editor di testo:

   `admintools -t db_add_node -d sw -p '[`*`dbadmin-password`*`]' -s [`*`data-node-eth0-addresses`*`]`

3. Sostituire `[`*`dbadmin-password`*`]` con la password `dbadmin`.
4. Sostituire `[`*`data-node-eth0-addresses`*`]` con un elenco separato da virgole di nuovi indirizzi IP indirizzabili della porta di gestione `eth0` del Data Node.
5. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per aggiungere i nuovi Data Node al database.

Dopo aver aggiunto i Data Node al database, ribilanciare i dati nei Data Node per creare un archivio dati bilanciato su ciascun Data Node.

Nuovo bilanciamento dei dati nel Data Store

Operazioni preliminari

- Accedere al Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Copiare il seguente comando e incollarlo in un normale editor di testo:

   ```
   /opt/vertica/bin/vsql --timing -x -c "SELECT rebalance_
   cluster()" -a -d sw -U dbadmin -w [dbadmin-password]
   ```

3. Sostituire `[dbadmin-password]` con la password `dbadmin`.
4. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per bilanciare nuovamente i dati. Tenere presente che questa operazione potrebbe richiedere del tempo, a seconda di diversi fattori, tra cui il numero di proiezioni, la quantità di dati e altro.
5. Dopo aver bilanciato nuovamente i dati, aggiornare le impostazioni del pool di risorse. Da vsql, immettere `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '0%;`

Rimozione di un Data Node dal Data Store

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

Per rimuovere un Data Node dal Data Store, attenersi a quanto segue:

- Il Data Store deve essere in esecuzione.
- Eseguire prima un backup. Per ulteriori informazioni, vedere **Creazione del backup di un Data Store**.
- È necessario avere almeno 3 nodi nel Data Store per via delle impostazioni sulla tolleranza d'errore. Per sostituire un nodo, vedere **Sostituzione di un Data Node con un Data Node sostitutivo con indirizzo IP diverso**.

Rimozione di un nodo dal Data Store

Operazioni preliminari

- Accedere alla Vertica Management Console come utente `dbadmin`.

Procedura

1. Selezionare **Manage** (Gestisci). Viene visualizzata la pagina di gestione.
2. Selezionare il nodo che si desidera rimuovere, fare clic su **Remove Node** (Rimuovi nodo).

Sostituzione di un Data Node con un Data Node sostitutivo con indirizzo IP diverso

> Per assistenza sulla pianificazione e l'implementazione di queste attività, contattare Cisco Professional Services.

Preparazione del Data Store per sostituire un Data Node guasto

- Eseguire il backup del Data Store. Per ulteriori informazioni, vedere **Creazione del backup di un Data Store**.
- Aggiungere il Data Node sostitutivo al Data Store. Per ulteriori informazioni, vedere **Aggiunta di Data Node al Data Store**.

Sostituzione del Data Node

Se Vertica è ancora in esecuzione sul Data Node che si intende sostituire, arrestare Vertica. Quindi, sostituire il Data Node precedente con il nuovo Data Node e distribuire la necessaria configurazione. Rimuovere il Data Node precedente e riavviare il nuovo Data Node.

Arresto di Vertica su un Data Node

Se Vertica è ancora in esecuzione sul Data Node, arrestare Vertica su questo Data Node. Se il Data Node è inattivo o Vertica non è in esecuzione, andare al passaggio successivo.

Operazioni preliminari

- Accedere alla console di un Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Copiare il seguente comando e incollarlo in un normale editor di testo:

```
/opt/vertica/bin/admintools -t stop_host -s [node-ip-addresses]
```

3. Sostituire `[node-ip-addresses]` con un elenco di indirizzi IP indirizzabili della porta di gestione `eth0` del Data Node che si desidera rimuovere dal Data Store.
4. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per arrestare Vertica su questo Data Node.

Sostituzione di un Data Node

Operazioni preliminari

- Accedere alla console di un Data Node come utente `root`.

Procedura

1. Immettere `su - dbadmin` e premere Invio per eseguire i comandi come utente `dbadmin`.
2. Copiare il seguente comando e incollarlo in un normale editor di testo:

   ```
   /opt/vertica/bin/admintools -t db_replace_node -d sw -o [old-data-node-hostname] -n [new-data-node-hostname]
   ```

3. Sostituire `[old-data-node-hostname]` con il nome host del Data Node che si desidera rimuovere dal Data Store.
4. Sostituire `[new-data-node-hostname]` con il nome host del Data Node che si desidera aggiungere al Data Store.
5. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per sostituire il Data Node precedente con il nuovo Data Node.
6. Copiare `/opt/vertica/bin/admintools -t distribute_config_files`, incollarlo nel prompt dei comandi e premere Invio per distribuire i file di configurazione al nuovo Data Node.
7. Copiare il seguente comando e incollarlo in un normale editor di testo:

   ```
   /opt/vertica/sbin/update_vertica --remove-hosts [old-data-node-hostname]
   ```

8. Sostituire `[old-data-node-hostname]` con il nome host del Data Node che si desidera rimuovere dal Data Store.
9. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per rimuovere il Data Node precedente dal Data Store.
10. Copiare il seguente comando e incollarlo in un normale editor di testo:

```
/opt/vertica/bin/admintools -t restart_node -s [new-data-node-hostname]
```

11. Sostituire `[new-data-node-hostname]` con il nome host del Data Node che si desidera aggiungere al Data Store.
12. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per riavviare il nuovo Data Node.

Copia delle informazioni sull'attendibilità del Data Store su una SMC di failover

Se si implementa una SMC di failover nell'ambiente, gestito dall'SMC principale, quando si esegue lo script `setup-sw-datastore-secure-connectivity`, verificare che le informazioni sull'attendibilità, incluse le password `dbadmin` e `readonlyuser`, e i certificati di identità per le comunicazioni sicure con i Data Node, non vengano copiate sull'SMC di failover. Prima di promuovere una SMC di failover a SMC principale nell'implementazione di un Data Store, copiare i file dell'SMC principale sull'SMC di failover. Se non si copiano le informazioni sull'attendibilità, SMC non può connettersi al Data Store.

Inoltre, se l'SMC di failover è già diventata SMC principale, retrocedere l'SMC principale a SMC di failover e se si desidera aggiungere nuove appliance all'implementazione del Stealthwatch, copiare le informazioni sull'attendibilità sulla nuova SMC di failover prima di eseguire lo script `setup-sw-datastore-secure-connectivity`. Se non si copiano queste informazioni sull'attendibilità, lo script potrebbe non riuscire.

Copia delle informazioni sull'attendibilità tra SMC

Operazioni preliminari

- Identificare gli indirizzi IP e le credenziali root dell'SMC principale e dell'SMC di failover.
- Se l'SMC di failover è stata appena promossa all'SMC principale, accedere alla console dell'SMC come utente `root`.

Procedura

1. Copiare il seguente comando e incollarlo in un normale editor di testo:

```
scp root@[demoted-smc-ip-address]:/lancope/var/admin/cds/sw-datastore-* /lancope/var/admin/cds
```

2. Sostituire `[demoted-smc-ip-address]` con l'indirizzo IP dell'SMC appena retrocessa a SMC di failover.
3. Copiare il comando aggiornato, incollarlo nel prompt dei comandi e premere Invio per copiare le informazioni sull'attendibilità del Data Store dall'SMC appena retrocessa a SMC di failover sull'SMC appena diventata SMC principale. Quando richiesto, immettere la password `root` dell'SMC appena retrocessa a SMC di failover.

Risoluzione dei problemi di implementazione del Data Store

Risoluzione dei problemi di implementazione dell'hardware

In caso di problemi durante l'implementazione o la configurazione dell'SMC o dei Flow Collector, consultare la Guida all'installazione dell'hardware di Stealthwatch x210 e la Guida alla configurazione di Stealthwatch System.

Risoluzione dei problemi dello script setup-sw-datastore-secure-connectivity

Se una SMC di failover è diventata una SMC principale, vedere Copia delle informazioni sull'attendibilità del Data Store su una SMC di failover per informazioni su come copiare le informazioni sull'attendibilità del Data Store sul nuovo SMC principale.

Lo script di connessione sicura `setup-sw-datastore-secure-connectivity` del Data Store registra i messaggi sui file di log in `/lancope/var/logs/containers/setup-sw-datastore-secure-connectivity.log`. Per ulteriori informazioni, consultare questi file di log.

Messaggi di errore generali di setup-sw-datastore-secure-connectivity

Nella tabella seguente sono elencati i messaggi di errore che potrebbero essere visualizzati in caso si verifichi un errore nello script `setup-sw-datastore-secure-connectivity` e le possibili soluzioni al problema.

Messaggio di errore	Descrizione	Soluzioni possibili
Error authorizing remote login for `[ip-address]`	Lo script `setup-sw-datastore-secure-connectivity` potrebbe	• Verificare di aver fornito la password root corretta per l'accesso. • Verificare che l'appliance sia al momento in esecuzione. • Verificare che la connessione tra lo script e l'appliance sia attualmente

	non accedere da remoto a un'appliance per fornire informazioni importanti.	attiva.
Error generating key pair.	Si è verificato un errore nello script `setup-sw-datastore-secure-connectivity` durante la generazione delle chiavi associate ai certificati di identità usati per le connessioni sicure del Data Store.	• Per ulteriori informazioni, contattare il supporto Cisco.
Failed to authenticate with token authority.	Lo script `setup-sw-datastore-secure-connectivity` potrebbe non stabilire correttamente una connessione con Central Management.	• Per ulteriori informazioni, contattare il supporto Cisco.

Failed to get inventory from SMC.	Lo script `setup-sw-datastore-secure-connectivity` potrebbe non recuperare correttamente le informazioni da Central Management.	• Consultare il log `/lancope/var/logs/container/svc-central-management.log` per provare a stabilire se il problema riguarda Central Management. • Per ulteriori informazioni, contattare il supporto Cisco.
No DB Clients found.	La configurazione di SMC e Flow Collector non era adeguata per permetterne l'uso con un Data Store.	• Accedere alla CLI dell'appliance, eseguire la configurazione del sistema e abilitarne l'uso con un Data Store.
Password is not available. You may want to delete /lancope/var/etc/keystore/store and rerun setup-sw-datastore-secure-connectivity.	Si è verificato un errore nello script `setup-sw-datastore-secure-connectivity` durante il salvataggio o la distribuzione delle password `dbadmin` e	• Eliminare il contenuto di `/lancope/var/etc/keystore/store`, quindi eseguire nuovamente lo script `setup-sw-datastore-secure-connectivity`.

	`readonlyuser`.	
Register the data nodes with Central Management before attempting to setup the secure connection.	I Data Node non sono gestiti da Central Management.	• Gestire i Data Node con Central Management.
SMC inventory is empty. Please add an appliance to Central Management.	Central Management non gestisce al momento nessun Data Node o Flow Collector.	• Gestire i Flow Collector e Data Node con Central Management.
sw-datastore-dbadmin-password and/or sw-datastore-readonlyuser-password not present in input	La password `dbadmin` o la password `readonlyuser` non era stata definita.	• Nello script, eseguire nuovamente **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance), se il Data Store non è ancora stato inizializzato, quindi specificare una password `dbadmin` e una password `readonlyuser`. • Se il Data Store è stato inizializzato, nello script, eseguire **3. Update SW DataStore password on appliances** (Aggiorna password SW DataStore sulle appliance) per aggiornare le password `dbadmin` e `readonlyuser`.
SW Datastore password(s) already initialized on `[ip-address]`.	Il Data Store è già inizializzato; è possibile	• Nello script, eseguire **3. Update SW DataStore password on appliances** (Aggiorna password SW DataStore sulle appliance) per aggiornare le password `dbadmin` e

	usare **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance) in `setup-sw-datastore-secure-connectivity` per modificare le password `dbadmin` o `readonlyuser`.	`readonlyuser`.
SW Datastore password(s) are not stored due to: Empty value	La password `dbadmin` o la password `readonlyuser` non era stata definita.	• Nello script, eseguire nuovamente **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance), se il Data Store non è ancora stato inizializzato, quindi specificare una password `dbadmin` e una password `readonlyuser`. • Se il Data Store è stato inizializzato, nello script, eseguire **3. Update SW DataStore password on appliances** (Aggiorna password SW DataStore sulle appliance) per aggiornare le password `dbadmin` e `readonlyuser`.

There are no data nodes currently managed.	I Data Node non sono gestiti da Central Management.	• Gestire i Data Node con Central Management.
There are no SMC/FCs currently managed.	I Flow Collector (e qualsiasi SMC di failover) non sono gestiti da Central Management.	• Gestire i Flow Collector (e l'SMC di failover) con Central Management.
Unknown error code: `[error-code]` on `[ip-address]`	Si è verificato un errore nello script durante il tentativo di distribuire le password `dbadmin` e `readonlyuser`.	• Per ulteriori informazioni, contattare il supporto Cisco.

Risoluzione dei problemi dello script install_SDBN_initial.py

Lo script di installazione `install_SDBN_initial.py` del Data Store registra i messaggi sui file di log in `/lancope/var/database/logs/db_initial_install_[datestamp].log`. Per ulteriori informazioni, consultare questi file di log.

Prerequisites not fully met during local (OS) configuration for verify-[data-node-ip-address].xml

Quando si inizializza il Data Store in Inizializzazione e configurazione del Data Store

eseguendo lo script phyton `install_SDBN_initial.py`, sulla console potrebbe essere visualizzato `Prerequisites not fully met during local (OS) configuration for verify-[data-node-ip-address].xml`, seguito da una serie di messaggi di log. Questi messaggi di log non indicano un errore di inizializzazione del Data Store. Non è necessario intervenire su nessuno di questi messaggi di log.

Nella tabella seguente viene descritto ogni messaggio.

Gravità e codice di errore	Descrizione	Spiegazione
`FAIL (s0180)`	`Insufficient swap size. Need 2.00 GB, have 1.50 GB`	Lo spazio allocato per la partizione dello swap non soddisfa i valori consigliati. **Non** modificare l'allocazione dello spazio dello swap. Cisco ha già configurato il valore corretto sul Data Store.
`FAIL (s0311)`	`root account is not in /etc/sudoers`	Il programma di installazione non ha individuato l'account root nell'elenco di autorizzazione del super utente in `/etc/sudoers` e invita ad aggiornare Vertica per risolvere il problema. **Non** aggiornare Vertica. Questa configurazione è stata progettata intenzionalmente per motivi di sicurezza.
`HINT (S0040)`	`Could not find the following tools normally provided by the pstack or gstack package: pstack/gstack`	Il programma di installazione non riesce a trovare il pacchetto `pstack` o `gstack` per registrare le tracce dello stack. Questi pacchetti non sono necessari per il Data Store.
`HINT (S0041)`	`Could not find the following tools normally provided by the mcelog package: mcelog`	Il programma di installazione non riesce a trovare il pacchetto `mcelog` per registrare i controlli della macchina. Ciò non è necessario per il Data Store.

HINT (S0305)	TZ is unsert for dbadmin. Consider updating .profile or .bashrc	Il programma di installazione non ha trovato la variabile di ambiente TZ per l'account utente dbadmin, usata per i fusi orari. La variabile non è necessaria per il Data Store, in quanto sono stati configurati i server NTP per l'implementazione del Stealthwatch.
WARN (N0010)	Linux iptables (firewall) has some non-trivial rules in tables: filter	Nell'iptables del Data Node sono già presenti delle regole. Se iptables contiene delle regole, il sistema registra un'avvertenza, ma non controlla la presenza di eventuali conflitti sulle porte di comunicazione richieste. È un comportamento previsto e non dovrebbe causare problemi con la distribuzione del Data Node.

SSLCA config parameter is not set; client certificates will not be requested or verified

Quando si inizializza il Data Store secondo quanto illustrato in Inizializzazione e configurazione del Data Store eseguendo lo script phyton install_SDBN_initial.py, sulla console potrebbe essere visualizzato il messaggio Enable SSL/TLS for remote connections, seguito da INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified per ciascun Data Node che si sta inizializzando. Questo messaggio di log è normale e non indica che si è verificato un errore nel tentativo di stabilire una connessione sicura con il Data Store. Non è necessario intervenire su nessuno di questi messaggi di log.

Il Data Store è configurato in modalità server TLS; in questa modalità, quando le appliance stabiliscono una connessione sicura al Data Store, verificano anche il certificato server del database. Al contrario, nella modalità reciproca TLS, quando le appliance stabiliscono una connessione sicura al Data Store, le appliance devono verificare il certificato server del database e il database deve verificare i certificati client delle appliance. La modalità reciproca TLS richiede la configurazione del parametro SSLCA con il file root.crt contenente l'autorità certificativa (Certificate Authority, CA) o la catena di fiducia utilizzata per firmare i certificati client. Poiché la modalità reciproca non è utilizzata, SSLCA non è configurata e il Data Store non verifica i certificati client quando stabilisce una connessione sicura. Tuttavia, la connessione tra

le appliance e il Data Store in modalità server TLS è ancora una connessione sicura su TLS.

Messaggi di errore generali di install_SDBN_initial.py

Nella seguente tabella sono elencati i messaggi di errore che potrebbero essere visualizzati in caso si verifichi un errore nello script `install_SDBN_initial.py` e le possibili soluzioni del problema.

Messaggio di errore	Descrizione	Soluzioni possibili
Config file not found or no valid sections	Lo script `install_SDBN_initial.py` non riesce a individuare il file di configurazione `install_SDBN.cfg` oppure i dati nel file di configurazione non hanno il formato previsto.	• Accertarsi di aver salvato una copia di `install_SDBN_example.cfg` nel file `/lancope/database/install_SDBN.cfg` su questo Data Node. • Accertarsi che la formattazione di `install_SDBN.cfg` corrisponda alla formattazione di `install_SDBN_example.cfg`, che a ciascuna sezione del nodo sia assegnato un nome nel formato `node#`, di aver definito sia l'indirizzo IP privato sia l'indirizzo IP pubblico per ciascuna sezione di configurazione del Data Node e di avere una subnet definita nella sezione comune.
Could not find the expected jar file to retrieve DB user passwords, check that you are running an image containing this support	Lo script `install_SDBN_initial.py` non riesce a individuare il file `sw-datastore-admin.jar` contenente le password `dbadmin` e	• Accertarsi che la versione dell'appliance sia 7.3+. • Eseguire lo script `setup-sw-datastore-secure-connectivity` in `/lancope/admin/cds` e selezionare l'opzione **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance) per distribuire le password dbadmin e readonlyuser. Dopo aver completato questa operazione, se non è già stato fatto,

	`readonlyuser`.	eseguire anche l'opzione **2. Distribute Certificates for Secure DB Connection** (Distribuisci certificati per connessioni sicure al database). • Se l'errore persiste, contattare il supporto Cisco.
each node must have a public and private address entry	Nel file di configurazione `install_SDBN.cfg` non sono stati definiti gli indirizzi IP pubblici o privati per una o più voci dei nodi.	• Accertarsi di aver definito un indirizzo IP privato e un indirizzo IP pubblico per ciascuna sezione di configurazione del Data Node nel file `/lancope/database/install_SDBN.cfg`.
Either the secret store file does not exist OR the password does not exist in the file. Please login to the SMC and run the appropriate script to set and distribute the DB passwords.	Si è verificato un errore nello script `install_SDBN_initial.py` durante il tentativo di recuperare le password `dbadmin` e `readonlyuser`.	• Dalla CLI dell'SMC, eseguire lo script `setup-sw-datastore-secure-connectivity` in `/lancope/admin/cds` e selezionare l'opzione **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance) per distribuire le password dbadmin e readonlyuser. Dopo aver completato questa operazione, se non è già stato fatto, eseguire anche l'opzione **2. Distribute Certificates for Secure DB Connection** (Distribuisci certificati per connessioni sicure al database).
Failed to retrieve the database passwords	Si è verificato un errore nello script `install_SDBN_`	• Dalla CLI dell'SMC, eseguire lo script `setup-sw-datastore-secure-connectivity` in `/lancope/admin/cds` e selezionare l'opzione **1. Distribute SW DataStore**

	`initial.py` durante il tentativo di recuperare le password `dbadmin` e `readonlyuser`.	**password to appliances** (Distribuisci password SW DataStore alle appliance) per distribuire le password dbadmin e readonlyuser. Dopo aver completato questa operazione, se non è già stato fatto, eseguire anche l'opzione **2. Distribute Certificates for Secure DB Connection** (Distribuisci certificati per connessioni sicure al database).
I/O exception while attempting to read the file	Si è verificato un errore nello script `install_SDBN_initial.py` durante il tentativo di recuperare le password `dbadmin` e `readonlyuser`.	• Contattare il supporto Cisco e fornire il messaggio di errore.
One of both of the passwords does not exists in the file. Please login to the SMC and run the appropriate script to set and distribute the DB passwords.	Si è verificato un errore nello script `install_SDBN_initial.py` durante il tentativo di recuperare le password `dbadmin` e `readonlyuser`.	• Dalla CLI dell'SMC, eseguire lo script `setup-sw-datastore-secure-connectivity` in `/lancope/admin/cds` e selezionare l'opzione **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance) per distribuire le password dbadmin e readonlyuser. Dopo aver completato questa operazione, se non è già stato fatto, eseguire anche l'opzione **2. Distribute Certificates for Secure DB Connection** (Distribuisci certificati per connessioni sicure al database).

privateAddrs must be specified	Nel file di configurazione `install_SDBN.cfg` non è stato definito un indirizzo IP privato per una o più voci dei nodi.	• Accertarsi di aver definito un indirizzo IP privato per ciascuna sezione di configurazione del Data Node nel file `/lancope/database/install_SDBN.cfg`. Tenere presente che il Data Node usa questo indirizzo IP non indirizzabile su `eth2` per comunicare con altri Data Node appartenenti al Data Store.
publicAddrs must be specified	Nel file di configurazione `install_SDBN.cfg` non è stato definito un indirizzo IP pubblico per una o più voci dei nodi.	• Accertarsi di aver definito un indirizzo IP pubblico per ciascuna sezione di configurazione del Data Node nel file `/lancope/database/install_SDBN.cfg`. Tenere presente che il Data Node usa questo indirizzo IP indirizzabile su `eth0` per comunicare con le altre appliance Stealthwatch come parte dell'implementazione di Stealthwatch.
publicSubnet must be specified	Nel file di configurazione `install_SDBN.cfg` non è stata definita una subnet per una o più voci dei nodi.	• Accertarsi di avere una subnet definita nella sezione di configurazione comune nel file `/lancope/database/install_SDBN.cfg`. Tenere presente che questa subnet usa l'indirizzo IP indirizzabile sulla porta `eth0` del Data Node per comunicare con le altre appliance Stealthwatch come parte dell'implementazione di Stealthwatch.
Unexpected exception while reading the secrets	Si è verificato un errore nello script `install_SDBN_initial.py` durante il tentativo di recuperare le	• Eseguire lo script `setup-sw-datastore-secure-connectivity` in `/lancope/admin/cds` e selezionare l'opzione **1. Distribute SW DataStore password to appliances** (Distribuisci password SW DataStore alle appliance) per distribuire le password dbadmin e readonlyuser. Dopo aver completato questa operazione, se non è già stato fatto,

	password `dbadmin` e `readonlyuser`.	eseguire anche l'opzione **2. Distribute Certificates for Secure DB Connection** (Distribuisci certificati per connessioni sicure al database). • Se l'errore persiste, contattare il supporto Cisco.
Unexpected return value	Lo script `install_SDBN_initial.py` ha ricevuto un valore e si è interrotto perché non poteva continuare.	• Contattare il supporto Cisco e fornire il messaggio di errore.

Aggiornamento delle password dbadmin e readonlyuser del Data Store dopo l'inizializzazione

Se il Data Store è già stato inizializzato, come descritto in Inizializzazione e configurazione del Data Store, e si desidera modificare le password `dbadmin` e `readonlyuser`, eseguire lo script bash di connettività sicura `setup-sw-datastore-secure-connectivity`. Dopo aver fornito la password `dbadmin` corrente, è possibile assegnare nuove password per `dbadmin` e `readonlyuser`. Lo script distribuisce le credenziali aggiornate alle appliance tramite SSH e aggiorna le credenziali degli account utente `dbadmin` e `readonlyuser`.

> Se la password `dbadmin` è andata persa, contattare il supporto Cisco per recuperarla.

Ciascuna password deve rispettare i seguenti requisiti:

- deve contenere almeno 1 numero
- deve contenere almeno 1 carattere minuscolo
- deve contenere almeno 1 carattere maiuscolo
- deve contenere almeno 1 carattere speciale tra i seguenti: `<>.,?/'"|:;`~!@#$%^&*()-_+={}[]`

- deve avere almeno 8 caratteri, ma non ha limiti di lunghezza
- deve contenere solo caratteri ASCII

Tenere presente che si utilizza questa opzione se il Data Store è già stato inizializzato. Se si stanno eseguendo le attività iniziali di implementazione e configurazione del Data Store, vedere Distribuzione delle password del Data Store su SMC, Data Node e Flow Collector per assegnare le password per `dbadmin` e `readonlyuser` e configurare le impostazioni per una connessione sicura al database del Data Store.

Se è stato effettuato il backup del database del Data Store, e successivamente è stata cambiata la password `dbadmin`, aggiornare il file delle password di backup `pw.ini` con la nuova password `dbadmin`. Per ulteriori informazioni, vedere Creazione di un backup del Data Store.

Operazioni preliminari

- Compilare un elenco di password root per l'SMC, i Data Node, i Flow Collector e l'SMC secondaria, se presente.
- Abilitare l'accesso SSH e l'accesso root SSH sulla SMC, i Data Node e i Flow Collector.

  > ⚠ Quando l'accesso SSH è abilitato, il rischio che il sistema venga compromesso aumenta. È importante abilitare l'accesso SSH solo quando necessario. Quando l'accesso SSH non viene più utilizzato, disabilitarlo.

- Accedere alla CLI della SMC come utente root.

Procedura

1. Dalla riga di comando, immettere `cd /lancope/admin/cds` e premere Invio per cambiare directory.
2. Immettere `./setup-sw-datastore-secure-connectivity` e premere Invio per eseguire lo script bash di connettività sicura del Data Store.
3. Dal menu principale dello script, selezionare **3. Update SW DataStore password on appliances** (Aggiorna password SW DataStore sulle appliance).
4. Immettere la password **dbadmin** corrente e selezionare **OK**.
5. Sulla riga di comando, quando viene chiesta la password root di ciascuna appliance, immettere la password e premere Invio.

> Quando si immettono più password, accertarsi di digitare correttamente la password dell'appliance.

Dopo aver immesso le password root di tutte le appliance, lo script chiede le password per `dbadmin` e `readonlyuser`.

6. Immettere la nuova password **dbadmin**.
7. Immettere la stessa password `dbadmin` nel campo **dbadmin (confirmation)** (conferma).
8. Immettere la nuova password **readonlyuser**.
9. Immettere la stessa password `readonlyuser` nel campo **readonlyuser (confirmation)** (conferma).

> Non immettere la stessa password per `dbadmin` e `readonlyuser`. L'assegnazione della stessa password causa errori nello script ed entrambi gli account utente rimarranno senza password.

10. Selezionare **OK**.

    Lo script distribuisce queste password alle appliance in modo sicuro. Al termine, viene visualizzato un elenco di appliance aggiornate.

11. Selezionare **OK** per tornare al menu principale dello script.

Come procedere

- Accedere alla VMC come utente `dbadmin`. Verrà richiesto di aggiornare la password.

> Se non si aggiorna la password in modo che corrisponda alla nuova password `dbadmin`, VMC non invierà notifiche di avvio sull'integrità né monitorerà adeguatamente il Data Store.

Risoluzione dei problemi dello script update_SDBN.py

Lo script `update_SDBN_initial.py` per l'aggiunta di Data Node registra i messaggi sui file di log in `/lancope/var/database/logs/db_update_[datestamp].log`. Per ulteriori informazioni, consultare questi file di log.

Messaggi di errore generali di update_SDBN_initial.py error

Nella seguente tabella sono elencati i messaggi di errore che potrebbero essere visualizzati in caso si verifichi un errore nello script `update_SDBN_initial.py` e le possibili soluzioni.

Messaggio di errore	Descrizione	Soluzioni possibili
Config file not found or no valid sections	Lo script `update_SDBN.py` non riesce a individuare il file di configurazione `update_SDBN.cfg` oppure i dati nel file di configurazione non hanno il formato previsto.	• Accertarsi di aver salvato una copia di `update_SDBN.cfg` nel file `/lancope/database/update_SDBN.cfg` su questo Data Node. • Accertarsi che la formattazione di `update_SDBN.cfg` corrisponda alla formattazione di `update_SDBN_example.cfg`, che a ciascuna sezione del nodo sia assegnato un nome nel formato `node#`, di aver definito sia l'indirizzo IP privato sia l'indirizzo IP pubblico per ciascuna sezione di configurazione del Data Node, di avere una subnet definita nella sezione comune e che il numero del primo nodo sia pari al totale dei nodi già presenti nel Data Store più uno.
each node must have a public and private address entry	Nel file di configurazione `update_SDBN.cfg` non sono stati definiti gli indirizzi IP pubblici o privati per una o più voci dei nodi.	• Accertarsi di aver definito un indirizzo IP privato e un indirizzo IP pubblico per ciascuna sezione di configurazione del Data Node nel file `/lancope/database/update_SDBN.cfg`.
Failed to retrieve the database dbadmin password	Lo script `update_SDBN.py` non riesce a individuare la password	• Accertarsi che la versione dell'appliance sia 7.3+. • Eseguire lo script `setup-sw-datastore-secure-connectivity` in `/lancope/admin/cds` e selezionare

	dbadmin.	l'opzione **3. Update SW DataStore password on appliances** (Aggiorna password SW DataStore sulle appliance) per impostare le password dbadmin e readonlyuser. • Se l'errore persiste, contattare il supporto Cisco.
firstNode must be specified	Nel file di configurazione update_SDBN.cfg non è stato specificato un valore per firstNode.	• Accertarsi di aver definito un valore per firstNode nella sezione di configurazione comune in /lancope/database/update_SDBN.cfg.
privateAddrs must be specified	Nel file di configurazione update_SDBN.cfg non sono stati definiti gli indirizzi IP privati per una o più voci dei nodi.	• Accertarsi di aver definito un indirizzo IP privato e un indirizzo IP pubblico per ciascuna sezione di configurazione del Data Node in /lancope/database/update_SDBN.cfg. Tenere presente che il Data Node usa questo indirizzo IP non indirizzabile su eth2 per comunicare con gli altri Data Node del database Data Store.
publicAddrs must be specified	Nel file di configurazione update_SDBN.cfg non è stato definito un indirizzo IP pubblico per una o più voci dei nodi.	• Accertarsi di aver definito un indirizzo IP pubblico per ciascuna sezione di configurazione del Data Node in /lancope/database/update_SDBN.cfg. Tenere presente che il Data Node usa questo indirizzo IP indirizzabile su eth0 per comunicare con le altre appliance Stealthwatch come parte dell'implementazione di Stealthwatch.
publicSubnet must be specified	Nel file di configurazione update_	• Accertarsi di aver definito una subnet nella sezione di configurazione comune in /lancope/database/update_

	`SDBN.cfg` non è stata definita una subnet per una o più voci dei nodi.	`SDBN.cfg`. Tenere presente che questa subnet usa l'indirizzo IP indirizzabile sulla porta `eth0` del Data Node per comunicare con le altre appliance Stealthwatch come parte dell'implementazione di Stealthwatch.

Risoluzione dei problemi di Vertica Management Console

Se l'istanza di VMC non si aggiorna automaticamente sul browser Web, può essere necessario aggiornarla manualmente per visualizzare le modifiche apportate al Data Store o alla configurazione.

Risoluzione dei problemi del Data Store

Notare che fino al 40% dello spazio di archiviazione disponibile sul Data Store è dedicato alla manutenzione del Data Store. Almeno il 60% dello spazio totale rimane disponibile per l'archiviazione dei flussi.

Vertica Analytics Platform non si riavvia automaticamente dopo l'interruzione di alimentazione di un Data Node e successivo riavvio

Se si verifica un'interruzione di alimentazione improvvisa su un Data Node e l'appliance viene riavviata, alcuni dati potrebbero danneggiarsi e l'istanza di Vertica Analytics Platform (Vertica) su quel Data Node potrebbe non riavviarsi automaticamente. Se il numero di Data Node attivi è sufficiente ad assicurare il funzionamento del Data Store, il Data Store continua ad acquisire dati dai Flow Collector. Tuttavia, il Data Node deve essere riavviato il prima possibile, per permettergli di ricollegarsi al Data Store, recuperare i dati persi dai Data Node adiacenti e allinearsi al resto dei Data Node.

In questo caso, accedere al Data Node e forzare un riavvio manuale di Vertica per eliminare i dati corrotti e permettere per permetterne il corretto riavvio ed eliminare i dati danneggiati.

Inoltre, potrebbe essere necessario aggiornare la policy di ripristino dell'alimentazione del Data Node prima del riavvio. Se la policy di ripristino dell'alimentazione è impostata su alimentazione disattivata, riavviare manualmente il Data Node dopo l'interruzione dell'alimentazione. Per ulteriori informazioni sulla configurazione della policy di ripristino dell'alimentazione in CIMC, vedere la Guida alla configurazione della GUI di UCS serie C.

Operazioni preliminari

- Accedere alla CLI del Data Node come utente root.

Procedura

1. Copiare il seguente comando e incollarlo in un editor di testo:

   ```
   tail /lancope/var/database/dbs/sw/v_sw_[node_name]_
   catalog/ErrorReport.txt
   ```

2. Sostituire *[node_name]* con il nome del Data Node (ad esempio, `node0001`).
3. Copiare il comando aggiornato e incollarlo sulla CLI, quindi premere Invio per riesaminare le voci più recenti nel file degli errori `ErrorReport.txt`. Se il messaggio di errore indica eventuali problemi di coerenza dei dati o dati danneggiati, procedere al passaggio successivo per forzare il riavvio di Vertica.
4. Copiare il seguente comando e incollarlo in un editor di testo:

   ```
   admintools -t restart_node --hosts=[data-node-ip-address]
   --database='sw-datastore' --password="[dbadmin-password]"
   --force
   ```

5. Sostituire *[data-node-ip-address]* con l'indirizzo IP del Data Node.
6. Sostituire *[dbadmin-password]* con la password `dbadmin` del Data Store.
7. Copiare il comando aggiornato e incollarlo nella CLI, quindi premere Invio per forzare il riavvio di Vertica sul Data Node interessato. Vertica elimina i dati danneggiati e recupera i dati corretti dai Data Node adiacenti.
8. Se il sistema chiede `Do you want to continue waiting? (yes/no) [yes]`, immettere `yes` e premere Invio per continuare ad aspettare.

   Vertica ripristina le informazioni danneggiate dei Data Node dai Data Node adiacenti, quindi se tali Data Node hanno acquisito un'elevata quantità di traffico mentre il Data Node interessato era inattivo, potrebbe volerci del tempo per permettere al Data Node di recuperare tutte le informazioni.

Come procedere

- Riesaminare i consigli Cisco sull'alimentazione dei Data Node in Requisiti di implementazione del Data Store e suggerimenti.

Appendice A. Preparazione dell'installazione

Avvertenze per l'installazione

Prima di installare le appliance Stealthwatch Data Store, leggere il documento con le Informazioni sulla conformità alle normative e sulla sicurezza.

Osservare quanto segue:

Avvertenza 1071: definizione di Avvertenza

ISTRUZIONI IMPORTANTI PER LA 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 automatico

Questo prodotto dipende dal dispositivo di protezione da cortocircuiti (sovracorrente) presente nell'impianto dell'edificio. 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 sullo scollegamento dell'alimentazione

Prima di intervenire su uno chassis o 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 indossati, quali anelli, collane e orologi. 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 causati da scariche elettrostatiche. Non toccare direttamente con la mano o con strumenti metallici il backplane per evitare il rischio di scosse elettriche.

Avvertenza 1045: protezione dai cortocircuiti

Per questo prodotto è necessario predisporre una protezione da cortocircuiti (sovracorrente) integrata nell'impianto elettrico 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 terra

Questa apparecchiatura deve essere collegata 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: avvertenza sull'alimentazione TN

Il dispositivo è progettato per funzionare con sistemi elettrici TN.

Linee guida per l'installazione

Osservare quanto segue:

Avvertenza 1047: protezione contro il surriscaldamento

Per evitare surriscaldamenti, non utilizzare il sistema in aree con temperature ambiente superiori 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 dal momento che deve essere utilizzato come dispositivo di scollegamento principale.

Avvertenza 1005: interruttore automatico

Questo prodotto dipende dal dispositivo di protezione da cortocircuiti (sovracorrente) presente nell'impianto dell'edificio. 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.

Avvertenza 371: cavo di alimentazione e adattatore CA

Per l'installazione del prodotto, utilizzare i cavi di collegamento/cavi di alimentazione/adattatori CA/batterie forniti in dotazione o espressamente indicati. 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 riparabile dall'utente

Nessun componente interno è riparabile dall'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 strumenti 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 possono implicare pericoli 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.

Mantenere la sicurezza rispetto all'elettricità

> 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 della sede 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 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 nelle 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.

Appendice B. Installazione dell'hardware di Stealthwatch

In questa sezione viene descritta la procedura di installazione delle appliance nell'ambiente in uso. Include:

- **Montaggio dell'appliance**
- **Connessione dell'appliance alla rete**
- **Connessione all'appliance**
- **Configurazione delle impostazioni di rete con la procedura di impostazione iniziale**

Montaggio dell'appliance

Le appliance Stealthwatch 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 Stealthwatch:

- 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
- 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

Connessione dell'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.

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

Per informazioni sulle specifiche di ciascuna appliance, fare riferimento alle schede tecniche di Stealthwatch.

> ⓘ Tutti i componenti hardware di Cisco x2xx utilizzano la stessa piattaforma UCS, UCSC-C220-M5SX, eccetto Flow Collector 5210 DB, che utilizza UCSC-C240-M5SX. Gli elementi che variano nelle appliance sono le schede NIC, il processore, la memoria, i sistemi di archiviazione e RAID.

> ⓘ 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 crossover SFP+ DA 10G. Quindi, connettersi 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.

   Per UDP Director HA, collegare due UDP Director tramite 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.

Osservare l'etichetta Ethernet (eth2, eth3, ecc.) di ciascuna porta. Queste etichette corrispondono alle interfacce di rete (eth2, eth3, ecc.) visualizzate e possono essere configurate dalla Home page dell'interfaccia di amministrazione dell'appliance.

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.

Connessione all'appliance

In questa sezione viene descritto come collegarsi all'appliance per poter modificare le password utente predefinite.

È possibile connettersi all'appliance in uno dei seguenti modi:

- con una tastiera e un monitor
- con un laptop (e un emulatore di terminale)

Nelle nuove appliance, SSH è disabilitato. Per abilitarlo, è necessario accedere all'interfaccia Web di amministrazione dell'appliance.

Connessione con una tastiera e un 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 alimentare i dispositivi, 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. Continuare alla sezione **Configurazione delle impostazioni di rete con la procedura di impostazione iniziale**.

Connessione con un laptop

È anche possibile collegare l'appliance al laptop con un emulatore di terminale.

Per connettersi a un'appliance con 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 alimentare i dispositivi, 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 qualsiasi 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. Continuare alla sezione seguente **Configurazione delle impostazioni di rete con la procedura di impostazione iniziale**.

Configurazione delle impostazioni di rete con la procedura di impostazione iniziale

Dopo aver effettuato il collegamento all'appliance, seguire la procedura di impostazione iniziale per configurare i parametri della rete, inclusi gli indirizzi IP. Tenere presente quanto segue:

- Se si implementa una SMC 2210 o un Flow Collector 4210 con un Data Store, oltre a configurare gli indirizzi IP, è possibile configurare l'SMC o il Flow Collector per l'uso di un Data Store ed è possibile configurare il tipo di porta fisica per la porta di gestione `eth0`.

  > ⚠ Dopo aver scelto di configurare SMC o Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, è necessario effettuare l'RFD dell'appliance. Abilitare questa opzione solo se si intende implementare un Data Store nella rete.

- Se l'appliance è un Data Node, è possibile configurare il tipo di porta fisica da utilizzare per la porta di gestione `eth0` e l'indirizzo IP e relative informazioni per `eth2` o il port-channel `eth2/eth3` per le comunicazioni con Data Node.

Per ulteriori informazioni sull'installazione di SMC 2210, FC 4210 e sulle appliance Data Node, vedere la Guida all'installazione e alla configurazione dell'hardware di Data Store Cluster.

Dopo aver configurato gli indirizzi IP e le porte, cambiare le password utente.

> ⓘ La prima volta che si accede alla configurazione del sistema, viene avviata l'impostazione guidata iniziale che guida l'utente nella configurazione iniziale

dell'appliance. Se si esce dall'impostazione iniziale prima di aver completato la procedura guidata, al successivo accesso alla configurazione di sistema, la procedura di impostazione guidata iniziale viene avviata nuovamente.

A seconda dell'appliance, passare alla sezione seguente:

- **Appliance compatibili con il Data Store (SMC 2210, FC 4210)**
- **Configurazione generale delle appliance Stealthwatch**
- **Configurazione dei Data Node**

Configurazione generale delle appliance Stealthwatch

Su tutte le appliance eccetto i Data Node, SMC 2210 e FC 4210, nell'impostazione iniziale viene visualizzato quanto segue:

- Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

L'indirizzo IP di gestione eth0 e le relative informazioni vengono specificate nell'impostazione iniziale. Sulla maggior parte delle appliance, si tratta della prima configurazione nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un Data Node, andare a Configurazione dei Data Node.
- Se si sta configurando una SMC o un Flow Collector compatibile con il Data Store, andare alla sezione Appliance compatibili con il Data Store (SMC 2210, FC 4210).
- Se si sta configurando un'altra appliance Stealthwatch, iniziare dal passaggio 1.

Procedura

1. Accedere al programma di configurazione del sistema:
    - Se si sta configurando un Data Node o un'appliance compatibile con il Data Store, digitare `root` e premere **Invio**. Se si sta configurando un'altra appliance, digitare `sysadmin` e premere **Invio**.

> Per configurare correttamente il Data Store e la compatibilità del Data Store, sono richieste autorizzazioni `root`.

- Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
- Al prompt successivo, digitare **SystemConfig** (Configurazione di sistema), quindi premere **Invio**.

2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale.

   In tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. In **IP address**, immettere l'indirizzo IP dell'appliance.
4. In **Netmask**, immettere una netmask per la rete.
5. In **Gateway**, immettere l'indirizzo gateway per l'indirizzo IP dell'appliance.
6. In **Broadcast**, immettere un indirizzo di trasmissione per l'appliance.
7. In **Hostname**, immettere un nome host per l'appliance.
8. In **Domain**, immettere un dominio per l'appliance.
9. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

   Questa è l'ultima opzione di configurazione nell'impostazione iniziale. L'appliance viene riavviata per applicare le modifiche. Al termine, viene visualizzata la pagina di accesso.

Come procedere

- Cambiare le password utente. Per ulteriori informazioni, vedere **Modifica della password utente sysadmin**.

Appliance compatibili con il Data Store (SMC 2210, FC 4210)

Sulle appliance SMC 2210 e FC 4210, nell'impostazione iniziale viene visualizzata la seguente configurazione:

1. Configurazione della porta di gestione fisica di eth0
2. Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance
3. Configurazione della compatibilità del Data Store

Configurazione della porta di gestione fisica di eth0

Se si configura una SMC o un Flow Collector compatibile con il Data Store e si sta implementando un Data Store, è possibile configurare facoltativamente `eth0` come porta SFP+ DAC al posto della porta in rame BASE-T predefinita. Su queste appliance, si tratta della prima configurazione nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un SMC o un Flow Collector compatibile con un Data Node o un Data Store, vedere la scheda tecnica di Stealthwatch relativa all'appliance per informazioni sulle porte SFP+ e BASE-T supportate.
- Se si sta configurando un Data Node, andare a Configurazione dei Data Node.
- Se si sta configurando un'appliance Stealthwatch diversa dalle appliance compatibili con il Data Store, vedere Configurazione generale delle appliance Stealthwatch.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Immettere **root**, quindi premere **Invio**.

     > Per configurare correttamente la compatibilità del Data Store, sono richieste autorizzazioni `root`.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig** (Configurazione di sistema), quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale e la configurazione dell'ordine delle porte. Andare al passaggio 5.

   In tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. Dal menu System Configuration (Configurazione di sistema), selezionare **Network** (Rete), quindi premere **Invio**.
4. Selezionare **Port Order** (Ordine delle porte), quindi premere Invio.
5. Sono disponibili le seguenti opzioni:

- Selezionare **LOM** per consentire all'appliance di utilizzare una porta in rame BASE-T per eth0.
- Selezionare **SFP+** per consentire all'appliance di utilizzare una porta in fibra SFP+ per eth0.

6. Selezionare **OK** per confermare la selezione.

Come procedere

- Configurare l'indirizzo IP e le informazioni di gestione della porta eth0. Vedere la procedura successiva.

Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

L'indirizzo IP di gestione eth0 e le relative informazioni vengono specificate nell'impostazione iniziale. Sulle appliance compatibili con il Data Store, questa configurazione viene eseguita dopo la configurazione della porta di gestione fisica eth0.

Operazioni preliminari

- Se si sta configurando una SMC o un Flow Collector compatibile con il Data Store, dopo aver configurato l'ordine delle porte, nell'impostazione guidata iniziale viene visualizzata la configurazione della gestione di `eth0`. Andare al passaggio 3.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Se si sta configurando un'appliance compatibile con il Data Store, digitare `root` e premere **Invio**.

     > Per configurare correttamente il Data Store e la compatibilità del Data Store, sono richieste autorizzazioni `root`.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig** (Configurazione di sistema), quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale.

In tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.

3. In **IP address**, immettere l'indirizzo IP dell'appliance.
4. In **Netmask**, immettere una netmask per la rete.
5. In **Gateway**, immettere l'indirizzo gateway per l'indirizzo IP dell'appliance.
6. In **Broadcast**, immettere un indirizzo di trasmissione per l'appliance.
7. In **Hostname**, immettere un nome host per l'appliance.
8. In **Domain**, immettere un dominio per l'appliance.
9. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

Come procedere

- Configurare l'appliance in modo che possa essere usata senza un Data Store. Per ulteriori informazioni, vedere la procedura seguente.

Configurazione dell'utilizzo del Data Store

Configurare SMC 2210 o FC 4210 in modo che possano essere utilizzati con un Data Store. I Flow Collector si collegheranno al Data Store e la SMC potrà eseguire delle query sul Data Store.

> ⚠ Dopo aver scelto di configurare SMC o Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, è necessario effettuare l'RFD dell'appliance. Abilitare questa opzione **solo se** si intende implementare un Data Store nella rete.

> ⓘ Se si implementa un Data Store, tutti gli SMC e i Flow Collector devono essere configurati in modo da poter essere utilizzati con un Data Store. Non è possibile configurare alcuni Flow Collector in modo che si connettano al Data Store e gli altri in modo che si connettano direttamente all'SMC.

Operazioni preliminari

- Nell'impostazione iniziale, la configurazione di sistema visualizza la configurazione del Data Store una volta specificato l'indirizzo IP dell'appliance. Andare al passaggio 3.

Procedura

1. Dal menu System Configuration (Configurazione di sistema). Selezionare **Advanced** (Avanzate), quindi premere **Invio**.
2. Selezionare **Data Store**, quindi premere Invio.
3. Selezionare **Yes** (Sì) per configurare la compatibilità dell'appliance con un Data Store.

   > ⚠ Dopo aver scelto di configurare SMC o Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, è necessario effettuare l'RFD dell'appliance. Abilitare questa opzione **solo se** si intende implementare un Data Store nella rete.

4. Selezionare **OK** per confermare la selezione.

   Questa è l'ultima opzione di configurazione nell'impostazione iniziale. L'appliance viene riavviata per applicare le modifiche. Al termine, viene visualizzata la pagina di accesso.

Come procedere

- Cambiare le password utente. Per ulteriori informazioni, vedere **Modifica della password utente sysadmin**.

Configurazione dei Data Node

Sui Data Node, nell'impostazione iniziale viene visualizzata la seguente configurazione:

1. Configurazione della porta di gestione fisica di eth0
2. Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance
3. Configurazione di eth2 ed eth3 per le comunicazioni tra Data Node

Configurazione della porta di gestione fisica di eth0

Se si configura un Data Node, è possibile facoltativamente specificare `eth0` come porta in rame BASE-T al posto della porta SFP+ DAC predefinita. Su queste appliance, si tratta della prima configurazione nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un Data Node, vedere la scheda delle specifiche Stealthwatch per l'appliance in uso per informazioni sulle porte SFP+ e BASE-T supportate.

- Se si sta configurando una SMC o un Flow Collector compatibile con il Data Store, andare alla sezione Appliance compatibili con il Data Store (SMC 2210, FC 4210).
- Se si sta configurando un'appliance Stealthwatch diversa dalle appliance compatibili con il Data Store, vedere Configurazione generale delle appliance Stealthwatch.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Immettere **root**, quindi premere **Invio**.

     > Per configurare correttamente la compatibilità del Data Store, sono richieste autorizzazioni `root`.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig** (Configurazione di sistema), quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale e la configurazione dell'ordine delle porte. Andare al passaggio 5.

   In tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. Dal menu System Configuration (Configurazione di sistema), selezionare **Network** (Rete), quindi premere **Invio**.
4. Selezionare **Port Order** (Ordine delle porte), quindi premere Invio.
5. Sono disponibili le seguenti opzioni:
   - Selezionare **SFP+** per consentire all'appliance di utilizzare una porta in fibra SFP+ per eth0.
   - Selezionare **LOM** per consentire all'appliance di utilizzare una porta in rame BASE-T per eth0.
6. Selezionare **OK** per confermare la selezione.

Come procedere

- Configurare l'indirizzo IP e le informazioni di gestione della porta eth0. Vedere la procedura successiva.

Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

L'indirizzo IP di gestione eth0 e le relative informazioni vengono specificate nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un Data Node, dopo aver configurato l'ordine delle porte, nell'impostazione iniziale guidata viene visualizzata la configurazione della gestione di `eth0`. Andare al passaggio 3.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Se si sta configurando un Data Node, digitare `root` e premere **Invio**.

     > Per configurare correttamente il Data Store e la compatibilità del Data Store, sono richieste autorizzazioni `root`.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig** (Configurazione di sistema), quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale.

   In tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. In **IP address**, immettere l'indirizzo IP dell'appliance.
4. In **Netmask**, immettere una netmask per la rete.
5. In **Gateway**, immettere l'indirizzo gateway per l'indirizzo IP dell'appliance.
6. In **Broadcast**, immettere un indirizzo di trasmissione per l'appliance.
7. In **Hostname**, immettere un nome host per l'appliance.
8. In **Domain**, immettere un dominio per l'appliance.
9. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

Come procedere

- Configurare le informazioni sulla gestione delle porte di comunicazione nel Data Node. Per ulteriori informazioni, vedere **Configurazione di eth2 ed eth3 per le comunicazioni tra Data Node**.

Configurazione di eth2 ed eth3 per le comunicazioni tra Data Node

Quando si configura un'appliance Data Node, configurare la porta per le comunicazioni tra Data Node con un indirizzo IP non indirizzabile. È possibile configurare uno dei seguenti elementi:

- `eth2`
- port-channel contenente eth2 ed eth3

> È necessario assegnare indirizzi IP non indirizzabili dal blocco CIDR `169.254.42.0/24`.

Operazioni preliminari

- Per informazioni sulle porte SFP+ `eth2` e `eth3`, vedere la scheda tecnica Stealthwatch relativa all'appliance. Notare che `eth2` e `eth3` dipendono dalla configurazione di `eth0`.
- Nell'impostazione iniziale, in System Configuration (Configurazione di sistema) viene visualizzata la configurazione di `eth2` o del port-channel `eth2/eth3` dopo aver completato la configurazione delle informazioni di gestione `eth0` dell'appliance. Andare al passaggio 3.

Procedura

1. Dal menu System Configuration (Configurazione di sistema), selezionare **Network** (Rete), quindi premere **Invio**.
2. Selezionare **Node Communications** (Comunicazioni nodi), quindi premere Invio.
3. Selezionare la configurazione della porta di comunicazione tra Data Node. Sono disponibili le seguenti opzioni:
    - Selezionare **Yes** (Sì) per aggregare `eth2` e `eth3` come port-channel per le comunicazioni tra Data Node.
    - Selezionare **No** per usare `eth2` per le comunicazioni tra Data Node.
4. Immettere un **indirizzo IP** non indirizzabile dal blocco CIDR `169.254.42.0/24` per `eth2` o il port-channel `eth2/eth3`.

5. In **Netmask**, immettere la netmask `255.255.255.0` per questo indirizzo IP.
6. In **Gateway**, immettere un indirizzo gateway per questo indirizzo IP.
7. In **Broadcast**, immettere un indirizzo di trasmissione per questo indirizzo IP.
8. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

   Questa è l'ultima opzione di configurazione nell'impostazione iniziale. L'appliance viene riavviata per applicare le modifiche. Al termine, viene visualizzata la pagina di accesso.

Come procedere

- Cambiare le password utente. Per ulteriori informazioni, vedere **Modifica della password utente sysadmin**.

Modifica della password utente sysadmin

Per garantire la sicurezza della rete, cambiare la password sysadmin predefinita delle appliance.

Modifica della password sysadmin

Operazioni preliminari

- Accedere alla console dell'appliance come **sysadmin**.
- Accedere alla configurazione di sistema.

Procedura

1. Nel menu di configurazione del sistema, selezionare **Password** e premere **Invio**.

   Se l'elenco predefinito degli host fidati è stato modificato, verificare che ciascuna appliance Stealthwatch presente nella struttura sia inclusa. In caso contrario, le appliance non potranno comunicare tra di loro.

   Sotto il menu viene visualizzato un prompt per la password corrente.
2. Digitare la password corrente e premere **Invio**.

   Viene visualizzato il prompt per una nuova password.
3. Digitare la nuova password e premere **Invio**.

   La password deve contenere da 8 a 30 caratteri alfanumerici senza spazi. È inoltre possibile utilizzare i seguenti caratteri speciali: `$.~!@#%_=?:,{}()`
4. Digitare nuovamente la password e premere **Invio**.

5. Una volta accettata la password, premere **Invio** di nuovo per tornare al menu di configurazione del sistema.
6. Continuare alla sezione successiva, **Modifica della password utente root**.

Modifica della password utente root

Dopo aver modificato la password utente sysadmin predefinita, modificare quella dell'utente root per garantire una maggiore protezione della rete.

Modifica della password utente root

Operazioni preliminari

- Accedere alla console dell'appliance come **sysadmin**.
- Accedere alla configurazione di sistema.

Procedura

1. Andare alla shell root.
2. Nel menu di configurazione del sistema, selezionare **Advanced** (Avanzate) e premere **Invio**. Viene visualizzato il menu Advanced (Avanzate).
3. Selezionare **RootShell**, quindi premere **Invio**.

   Viene visualizzato il prompt per la password root.
4. Digitare la password root corrente e premere **Invio**. Viene visualizzato il prompt per la shell root.
5. Digitare **SystemConfig**, quindi premere **Invio**.

   In questo modo, si torna al menu di configurazione del sistema da dove è possibile modificare la password root.
6. Selezionare **Password**, quindi premere **Invio**. Sotto il menu viene visualizzato il prompt per la password.
7. Digitare la nuova password root e premere **Invio**. Viene visualizzato un secondo prompt.
8. Digitare nuovamente la password root, quindi premere **Invio**.
9. Dopo aver modificato la password, premere **Invio**. A questo punto, entrambe le password sysadmin e root predefinite sono state modificate. In questo modo, si torna al menu della console di configurazione del sistema.
10. Selezionare **Cancel** (Annulla) e premere **Invio**. La console di configurazione del sistema si chiude e viene visualizzato il prompt della shell root.

11. Digitare **exit** (Esci) e premere **Invio**. Viene visualizzato il prompt di accesso.
12. Premere **Ctrl+Alt** per uscire dall'ambiente della console.

A questo punto è possibile configurare l'appliance. Per configurare l'appliance, consultare la **Guida alla configurazione di Stealthwatch System** per la versione software in uso. La serie x2xx è compatibile con le versioni software Stealthwatch 7.x.

Appendice C. Configurazione delle appliance

Quando si accede all'appliance per la prima volta, le impostazioni vengono configurate con lo strumento Appliance Setup Tool.

Requisiti dello strumento Appliance Setup Tool

- Confermare che i firewall e gli ACL (Access Control List) consentano l'accesso.
- Richiamare il nome host dell'appliance e degli indirizzi IP per i seguenti componenti:
    - Appliance
    - Subnet mask
    - Gateway predefiniti e di trasmissione
    - Server NTP e DNS
    - Indirizzo IP dell'SMC per la gestione centralizzata

Gestione

Con lo strumento Appliance Setup Tool, configurare l'appliance in modo che venga gestita dalla Stealthwatch Management Console (SMC) principale.

Quando le appliance sono gestite dalla Stealthwatch Management Console (SMC), è possibile utilizzare Central Management (Gestione centralizzata) per modificare le configurazioni delle appliance, aggiornare il software, riavviare o arrestare le appliance e molto altro.

SMC di failover

Se si dispone di più di una Stealthwatch Management Console (SMC), è possibile impostare una coppia SMC di failover in modo che una SMC funga da console di backup dell'altra.

- Utilizzare lo strumento Appliance Setup Tool per configurare ciascuna SMC.
- Pianificare quale SMC sarà la principale e quale la secondaria.
- Dopo aver configurato ciascuna SMC, utilizzare Central Management Trust Store e Stealthwatch Desktop Client per configurare la relazione di failover.

Best practice

Per configurare correttamente il sistema, accertarsi di seguire le istruzioni in questa guida.

Si consiglia quanto segue:

- **One at a Time** (Una alla volta): configurare un'appliance alla volta. Confermare che l'appliance sia **attiva** prima di avviare la configurazione sull'appliance successiva del cluster.
- **Order** (Ordine): seguire l'ordine di configurazione.
- **Multiple Central Managers** (Più gestioni centralizzate): è possibile configurare più di una gestione centralizzata nel sistema. Tuttavia, ciascuna appliance può essere gestita da una sola SMC principale o una sola gestione centralizzata.
- **Access** (Accesso): per accedere alla gestione centralizzata, è necessario disporre dei privilegi di amministratore.

Ordine di configurazione

Configurare le appliance nell'ordine seguente e prendere nota dei dettagli per ciascuna appliance:

Ordine	Appliance	Dettagli
1.	SMC principale	L'SMC principale è il Central Manager. Accertarsi che l'SMC sia visualizzata come attiva prima di iniziare a configurare l'appliance successiva nel sistema.
2.	UDP Director (chiamati anche Flow Replicator)	
3.	Data Node	
4.	Database Flow Collector serie 5000	Accertarsi che il database Flow Collector serie 5000 sia mostrato come attivo prima di avviare la configurazione del motore.

5.	Flow Collector serie 5000 Engine	Accertarsi che il database Flow Collector serie 5000 sia mostrato come attivo prima di avviare la configurazione del motore.
6.	Tutti gli altri Flow Collector (NetFlow e sFlow)	
7.	Flow Sensor	Accertarsi che Flow Collector sia visualizzato come attivo prima di avviare la configurazione del sensore di flusso.
8.	Endpoint Concentrator	
9.	SMC secondaria (se presente)	Accertarsi che l'SMC principale venga visualizzata come attiva prima di avviare la configurazione dell'SMC secondaria. L'SMC secondaria viene selezionata come Central Manager. Configurare il failover dopo aver configurato tutte le appliance.

Le appliance potrebbero non essere tutte visualizzate.

1. Accesso

Utilizzare le seguenti istruzioni per configurare ogni appliance usando lo strumento Appliance Setup Tool.

1. Nel campo dell'indirizzo del browser, immettere **https://** seguito dall'indirizzo IP dell'appliance.

   - **Primary SMC** (SMC principale): configurare prima l'SMC principale.
   - **Up** (Attiva): confermare che ciascuna appliance sia attiva prima di iniziare la configurazione dell'appliance successiva nel cluster.
   - **Order** (Ordine): accertarsi di configurare le appliance in sequenza in modo che possano comunicare correttamente.

2. Immettere le seguenti credenziali per accedere:

- **User Name** (Nome utente): admin
- **Password**: lan411cope

2. Configurazione dell'appliance

Quando si accede all'appliance per la prima volta, lo strumento Appliance Setup Tool guida l'utente in ciascuna fase della configurazione.

1. **Change Default Password** (Modifica password predefinita): immettere le nuove password per admin, root e sysadmin. Fare clic su **Next** (Avanti) per scorrere fino a ciascun utente.

   Utilizzare i seguenti criteri:

   - **Length** (Lunghezza): da 8 a 30 caratteri
   - **Change** (Modifica): accertarsi che la nuova password sia diversa dalla password predefinita per almeno 4 caratteri.

Utente	Password predefinita
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

> I menu sysadmin e root non sono disponibili se le password predefinite sono già state modificate durante l'installazione dell'hardware. Per ulteriori dettagli, fare riferimento alla Guida all'installazione dell'hardware di Stealthwatch serie x210.

2. **Management Network Interface** (Interfaccia rete di gestione): rivedere i campi dell'indirizzo IP e dell'interfaccia di rete. Verificare che le impostazioni predefinite siano corrette. Fare clic su **Next** (Avanti).

   - **Changes** (Modifiche): per modificare queste informazioni, confermarle prima con l'amministratore di rete e fare riferimento alla procedura di risoluzione dei problemi.

- **IPv6 (optional)** (facoltativo): per abilitare IPv6, fare clic su **IPv6**. Selezionare la casella di controllo **Enable IPv6** (Abilita IPv6) e completare i campi.

3. **Host Name and Domains** (Nome host e domini): immettere il nome dell'host e il nome del dominio di rete. Fare clic su **Next** (Avanti).

   - **Host Name** (Nomehost): è richiesto un nome host univoco per ciascuna appliance. Se si assegnano alle appliance gli stessi nomi, l'installazione non avrà esito positivo.
   - **Network Domain** (Dominio di rete): è richiesto un dominio dei nomi completo per ciascuna appliance.
   - **Stealthwatch Domain (SMC only)** (Dominio Stealthwatch) (solo SMC): immettere un dominio Stealthwatch per le appliance Stealthwatch.
   - **IP Address Ranges (SMC only)** (Intervalli di indirizzi IP) (solo SMC): selezionare l'intervallo degli indirizzi IP per la rete Stealthwatch.

4. **DNS Settings** (Impostazioni DNS): confermare che le impostazioni predefinite siano corrette oppure immettere l'indirizzo IP del server del dominio. Fare clic su **Next** (Avanti).

   Aggiunta o eliminazione dei server DNS (facoltativo):

   - **Add** (Aggiungi): fare clic sull'icona +.
   - **Delete** (Elimina): fare clic sulla casella di controllo per selezionare il sever DNS. Fare clic sull'icona –.

5. **NTP Settings** (Impostazioni NTP): confermare che le impostazioni predefinite siano corrette oppure fare clic sull'icona del **Menu** per selezionare il server NTP (Network Time Protocol). Fare clic su **Next** (Avanti).

   - **Multiple NTP Servers** (Più server NTP): si consiglia di impostare più server per avere ridondanza e precisione.
   - **Public Source** (Fonte pubblica): pool.ntp.org è una fonte pubblica valida per NTP.

   Aggiunta o eliminazione dei server NTP (facoltativo):

   - **Add** (Aggiungi): fare clic sull'icona +.

- **Delete** (Elimina): fare clic sulla casella di controllo per selezionare il server NTP. Fare clic sull'icona –.

6. Se l'appliance è un'SMC, passare a **3. Registrazione di Stealthwatch Management Console**.

   Se l'appliance non è un'SMC, passare a **4. Aggiunta delle appliance a Central Management**.

3. Registrazione di Stealthwatch Management Console

1. **Review Your Settings** (Rivedi impostazioni): confermare che le informazioni sull'appliance siano corrette.
2. Fare clic su **Apply** (Applica) o **Restart and Proceed** (Riavvia e prosegui).

   Seguire le istruzioni visualizzate sullo schermo mentre l'appliance si riavvia.

   Attendere alcuni minuti per rendere effettive le nuove impostazioni di sistema. Potrebbe essere necessario aggiornare la pagina.

3. Accedere alla Stealthwatch Management Console.
4. Viene nuovamente aperto lo strumento Appliance Setup Tool. Fare clic su **Continua**.
5. Sulla scheda Register Your Appliance (Registrazione appliance), riesaminare l'indirizzo IP e fare clic su **Save** (Salva).

   - In questo modo Central Management viene installato sulla Stealthwatch Management Console.
   - L'indirizzo IP dell'SMC viene rilevato automaticamente e non può essere modificato.

6. Al termine della configurazione dell'appliance, fare clic su **Go to Dashboard** (Vai alla dashboard).
7. Fare clic sull'icona **Global Settings** (Impostazioni globali). Selezionare **Central Management** (Gestione centralizzata).
8. Rivedere l'inventario. Verificare che lo stato dell'appliance SMC sia visualizzato come **attivo**.

> ⚠ Accertarsi che l'SMC principale e ciascuna appliance vengano visualizzati come attivi prima di avviare la configurazione dell'appliance successiva nel cluster utilizzando l'ordine di configurazione e i dettagli.

9. Implementare e configurare il Data Store. Per riesaminare il processo di implementazione, tornare alla Panoramica di implementazione del Data Store di Stealthwatch.

4. Aggiunta delle appliance a Central Management

Lo strumento Appliance Setup Tool continua a guidare l'utente nella configurazione dell'appliance con Central Management. Alcuni passaggi possono variare a seconda dell'appliance. Seguire i prompt visualizzati sullo schermo.

1. Sulla scheda Central Management (Gestione centralizzata), immettere l'indirizzo IP dell'SMC principale.

   L'SMC principale è il Central Manager.

2. Fare clic su **Save** (Salva).
3. Seguire le istruzioni visualizzate sullo schermo per considerare attendibile il certificato di identità dell'appliance SMC principale. Fare clic su **Yes** (Sì) per verificare il certificato e consentire che l'appliance comunichi con l'SMC.
4. Immettere le credenziali di accesso per l'SMC principale.
5. Selezionare il dominio Stealthwatch.

   - **Flow Collector**: immettere il numero di porta di Flow Collection.

     Netflow predefinito: 2055

     sFlow predefinita: 6343

   - **Flow Sensor**: selezionare un Flow Collector.

6. Fare clic su **Go to Central Management** (Vai alla gestione centralizzata). Andare a **5. Conferma dello stato dell'appliance**.

5. Conferma dello stato dell'appliance

Dopo aver configurato un'appliance nello strumento Appliance Setup Tool, confermare lo stato dell'appliance in Central Management.

1. Lo strumento Appliance Setup Tool apre l'inventario Central Management oppure è possibile aprirlo come segue:

   - Accedere alla Stealthwatch Management Console principale.
   - Fare clic sull'icona **Global Settings** (Impostazioni globali).
   - Selezionare **Central Management** (Gestione centralizzata).

2. Esaminare le appliance nell'inventario Appliance Manager.

   - Verificare che l'appliance sia visualizzata nell'inventario.
   - Verificare che lo stato dell'appliance sia visualizzato come attivo.

> ⚠ Accertarsi che l'SMC principale e ciascuna appliance vengano visualizzati come attivi prima di avviare la configurazione dell'appliance successiva nel cluster utilizzando l'ordine di configurazione e i dettagli.

3. Per configurare l'appliance successiva nel sistema, andare a **1. Accesso** e completare le procedure fino a **5. Conferma dello stato dell'appliance**.

   Se non si dispone di un'altra appliance da impostare, consultare la Guida alla configurazione di Stealthwatch System per ulteriori informazioni su come completare le configurazioni delle appliance. In alternativa, tornare alla Panoramica dell'implementazione del Data Store di Stealthwatch per riesaminare il processo di implementazione.

Informazioni sul copyright