Cisco Telemetry Broker

Guida alla configurazione e all'installazione dell'appliance hardware 2.0.1

Sommario

Introduzione

Panoramica

In questa guida viene spiegato come installare l'appliance Cisco Telemetry Broker TB2300. Viene descritto inoltre come montare e installare i componenti hardware di Cisco Telemetry Broker. A volte, Cisco Telemetry Broker viene denominato con l'acronimo CTB nel presente documento.

> ⚠ Prima di installare il nodo broker TB2300, leggere il documento Informazioni sulla conformità alle normative e sulla sicurezza.

Matrice di compatibilità delle versioni hardware e software

Appliance	Piattaforma	Gen	v.2.0
Nodo broker TB2300	UCSC-C220	M6	●

Fare riferimento a questa legenda per la Matrice di compatibilità delle versioni hardware e software.

Simbolo	Descrizione
●	Supportato con massima funzionalità sull'hardware
o	Supportato, con prestazioni non ottimali
x	Non supportato

Destinatari

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

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

Installazione dei nodi broker virtuali

Per installare i nodi broker virtuali, seguire le istruzioni riportate nella Guida all'implementazione e alla configurazione dell'appliance Cisco Telemetry Broker virtuale.

Terminologia

In questa guida il nodo broker TB2300 viene chiamato a volte "**appliance**".

Un "**cluster ad alta disponibilità**" è un gruppo di nodi broker gestiti da un nodo manager.

Acronimi di uso comune

Nella guida sono presenti i seguenti acronimi:

Acronimo	Descrizione
CIMC	Cisco Integrated Management Controller
DNS	Domain Name Server/Service
FTP	File Transfer Protocol
Gbps	Gigabit al secondo
GB	Gigabyte
HTTPS	Hypertext Transfer Protocol (Secure) (protocollo di trasferimento di un ipertesto)
Mbps	Megabit al secondo
NAT	Network Address Translation
NIC	Network Interface Card (scheda di rete)
NTP	Network Time Protocol
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SSH	Secure Shell

Acronimo	Descrizione
TAP	Test Access Port
UDPD	UDP Director
UPS	Uninterruptible Power Supply (gruppo statico di continuità)
URL	Universal Resource Locator
VLAN	Virtual Local Area Network (LAN virtuale)
VM	Virtual Machine (macchina virtuale)

Nozioni base e architettura

Cisco Telemetry Broker consente di acquisire i dati di telemetria della rete provenienti da fonti diverse, trasformarne il formato e inoltrarli a una o più destinazioni. Fare riferimento alla tabella seguente per alcuni esempi.

Attualmente, l'unica appliance hardware esistente per Cisco Telemetry Broker è un nodo broker (TB2300). Ai fini dell'implementazione, il nodo broker deve essere associato a un nodo VM Manager.

È possibile implementare una combinazione di nodi broker fisici e virtuali oppure è possibile implementare solo tutti nodi broker virtuali o solo tutti nodi broker fisici.

Non occorre rispettare un ordine di installazione per i nodi broker, anche quando si implementa una combinazione di nodi broker fisici e virtuali.

È possibile acquisire i seguenti dati di telemetria:	**E inoltrare i dati di telemetria a una o tutte le seguenti destinazioni:**
• Dati di telemetria della rete on-premises, inclusi NetFlow, syslog e IPFIX • Input di telemetria basati su cloud, ad esempio i log di flusso di Amazon Web Services (AWS) Virtual Private Cloud (VPC)	• Piattaforme di analisi, come Secure Network Analytics o Secure Cloud Analytics • Piattaforme di automazione e gestione della rete, come Cisco DNA Center • Piattaforme Security Information and Event Management (SIEM)

A tal fine, implementare uno o più nodi Cisco Telemetry Broker con l'obiettivo di acquisire i dati di telemetria e inoltrarli alle destinazioni configurate.

Per impostazione predefinita, Cisco Telemetry Broker supporta i seguenti processi:

Formato dati acquisiti	**Formato dati inoltrati**
Log di flusso di VPC	IPFIX
Log di flusso di Microsoft Network Security Group (NSG)	IPFIX
IPFIX, NetFlow v5, NetFlow v9	JSON (solo per destinazioni SCA)

I nodi broker sono tutti gestiti da un unico Cisco Telemetry Broker Manager. È possibile accedere all'interfaccia Web di questo Manager ed eseguire varie attività di configurazione, tra cui la gestione dei nodi broker, l'impostazione delle regole di inoltro, la creazione di utenti e la verifica dell'utilizzo sulla dashboard.

Requisiti di implementazione

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

Matrice di compatibilità delle versioni hardware e software

Per informazioni sulla compatibilità, consultare la Matrice di compatibilità delle versioni hardware e software. La matrice è riportata nel capitolo **Introduzione** di questa guida.

Specifiche

Scaricare la scheda tecnica del nodo broker TB2300 che si desidera installare.

Cisco Integrated Management Controller (CIMC)

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

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

Migrazione della configurazione a un nuovo sistema

Completare i seguenti processi per eseguire il backup e ripristinare le regole di configurazione di CTB impostate in Cisco Telemetry Broker Manager.

- I clienti UDPD possono migrare la configurazione UDPD esistente in Cisco Telemetry Broker. Per ulteriori informazioni, vedere la sezione "Importazione ed esportazione della configurazione di UDP Director" nella Guida per l'utente di Cisco Telemetry Broker.

Backup delle regole di configurazione di CTB

Eseguire questo comando sul nodo CTB Manager:

```
$ sudo ctb-backup-config -v -f ctb_config.json
```

Al termine del processo, il backup delle regole di configurazione viene salvato nel file ~/.ctb_config.json; sarà possibile quindi copiare le regole di configurazione in un'altra posizione.

- Le regole del log di flusso VPC/NSG non vengono incluse nel processo di backup, quindi è necessario ricrearle quando si migra a un nuovo sistema.
- È possibile eseguire il backup e ripristinare le regole di configurazione di CTB solo se si usa la stessa versione. Se si tenta di eseguire questa operazione tra versioni diverse, il processo potrebbe non riuscire.

Ripristino delle regole di configurazione di CTB

> ⚠ Eseguire il comando `ctb-restore-config` dopo aver completato il comando `ctb-install --init` sul nodo Manager. Se si crea un account di accesso alla GUI manualmente, verrà sovrascritto dalle informazioni sull'account restituite dal comando `ctb-restore-config`.

Seguire questa procedura:

1. Disconnettersi come utente *install*.
2. Copiare il file **ctb-config.json** da un sistema esistente.
3. Accedere al nuovo sistema come *admin*.
4. Eseguire questo comando sul nodo CTB Manager:

```
$ sudo ctb-restore-config -v -f ctb_config.json
```

Tutti gli input aggiunti durante il ripristino di Cisco Telemetry Broker non sono assegnati ad alcun nodo o cluster. Sarà necessario assegnarli manualmente secondo necessità.

1. Configurazione del firewall per le comunicazioni

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

Porte di comunicazione aperte

Nella tabella seguente vengono forniti i dettagli di tutte le connessioni di rete da e verso le appliance Cisco Telemetry Broker. Per garantire che la rete consenta queste connessioni, è necessario modificare i controlli di accesso applicabili attualmente in uso (ad esempio, il firewall).

Client	Server	Porta	Descrizione
utenti	nodi broker e nodo Manager	22/TCP	accesso SSH alla console
Manager	Internet esterno	443/TCP	HTTPS per comunicazioni esterne sicure, ad esempio licenze Smart e aggiornamento software
Manager	server syslog del cliente	porta definita dal cliente	telemetria syslog per le notifiche di Cisco Telemetry Broker
Manager	server SMTP del cliente	porta definita dal cliente	telemetria SMTP per le notifiche di Cisco Telemetry Broker
ciascun nodo broker	Manager	443/TCP	HTTPS per connessioni di gestione sicure

ciascun nodo broker	Internet esterno	443/TCP	HTTPS per il recupero dei log di flusso di VPC/NSG dai bucket di archiviazione AWS S3/Azure SAS, rispettivamente. HTTPS per il nodo broker per proteggere l'accesso al server SCA e caricare i file nel bucket SCA S3.
utenti	Manager	443/TCP	HTTPS per l'accesso sicuro all'interfaccia Web
nodi broker e nodo Manager	server DNS del cliente	53/UDP	telemetria DNS
ciascun nodo broker *hardware*	server NTP del cliente	123	dati NTP per la sincronizzazione

Inoltre, è necessario aprire le porte in base al tipo di dati di telemetria inviati a un nodo broker e al tipo di dati di telemetria trasmessi dal nodo broker a una destinazione. Nella tabella seguente vengono forniti i dettagli sulle porte comuni per i vari tipi di telemetria:

Porta	**Descrizione**
514/UDP	syslog
2055/UDP	NetFlow v5, NetFlow v9
4739/UDP	IPFIX
6343/UDP	sFlow

2. Avvertenze e linee guida per l'installazione

Avvertenze per l'installazione

Prima di installare le appliance Cisco Telemetry Broker, leggere il documento Informazioni sulla conformità alle normative e sulla sicurezza.

Osservare quanto segue:

> Avvertenza 1071: definizione delle avvertenze
>
> ISTRUZIONI IMPORTANTI SULLA SICUREZZA
>
> ⚠ Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di utilizzare qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze di sicurezza fornite con il dispositivo.
>
> CONSERVARE QUESTE ISTRUZIONI

> Avvertenza 1004: istruzioni per l’installazione
>
> ⚠ Leggere le istruzioni per l'installazione prima di usare, installare o collegare il sistema all'alimentazione.

> Avvertenza 12: avvertenza sulla disconnessione dell’alimentazione
>
> ⚠ Prima di intervenire su uno chassis o di lavorare vicino agli alimentatori, scollegare il cavo di alimentazione sulle unità CA; scollegare l'alimentazione all’interruttore automatico sulle unità CC.

> Avvertenza 43: avvertenza per la rimozione degli oggetti preziosi
>
> ⚠ Prima di utilizzare apparecchiature collegate alle linee elettriche, rimuovere eventuali gioielli e accessori in metallo (anelli, collane e orologi) indossati. Poiché gli oggetti metallici si riscaldano se collegati all'alimentazione e alla messa a terra, si rischia di subire gravi ustioni oppure l'oggetto stesso può saldarsi ai terminali.

Avvertenza 94: avvertenza sul bracciale antistatico

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

Avvertenza 1045: protezione contro cortocircuiti

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

Avvertenza 1021: circuito SELV

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

Avvertenza 1024: conduttore di messa a terra

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

Avvertenza 1040: smaltimento del prodotto

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

Avvertenza 19: avviso di alimentazione TN

Il dispositivo è progettato per funzionare con sistemi elettrici TN.

Linee guida per l'installazione

Osservare quanto segue:

Avvertenza 1047: prevenzione del surriscaldamento

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

Avvertenza 1019: dispositivo di scollegamento principale

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

Avvertenza 1005: interruttore

Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia una classe superiore a 120 V, 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, i cavi di alimentazione, gli adattatori CA e le batterie in dotazione o indicati nelle istruzioni. Se si dovessero usare cavi o adattatori diversi, potrebbero verificarsi guasti e incendi. Le norme giapponesi in materia di sicurezza dei materiali e degli apparecchi elettrici vietano l'utilizzo di cavi con certificazione UL (sui quali è riportato il marchio UL o CSA), in quanto non disciplinati dalle disposizioni di legge che prevedono invece il marchio PSE sul cavo, per tutti i dispositivi elettrici diversi da quelli indicati da CISCO.

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

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

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

> ⓘ Per garantire un corretto flusso d'aria è necessario montare lo chassis in rack per mezzo dei kit guide. Se le unità vengono installate una sopra all'altra o impilate senza kit guide, le prese d'aria sulla parte superiore dello chassis vengono ostruite causando il surriscaldamento, l'aumento di velocità delle ventole e un maggiore consumo energetico. Si consiglia di montare lo chassis in rack con kit guide in quanto queste offrono la distanza minima richiesta. L'uso dei kit guide per il montaggio dello chassis non richiede l'uso di distanziatori aggiuntivi.

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

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

Raccomandazioni per la sicurezza

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

Osservare queste linee guida sulla sicurezza:

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

Misure di sicurezza per gli interventi su apparecchiature sotto tensione

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

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

- Non lavorare da soli se sussistono condizioni di potenziale pericolo nella propria area di lavoro.
- Non dare per scontato che l'alimentazione sia scollegata; controllare sempre.
- Verificare attentamente la presenza di eventuali pericoli nell'area di lavoro, ad esempio superfici bagnate, prolunghe di alimentazione senza messa a terra, cavi di alimentazione consumati e assenza di messa a terra.
- In caso di incidente elettrico:
    - Agire con cautela per evitare di subire danni.
    - Scollegare l'alimentazione dal sistema.

    - Se possibile, mandare un'altra persona a chiamare il soccorso medico. Altrimenti, valutare le condizioni della vittima e chiedere aiuto.
    - Stabilire se è necessario praticare la respirazione bocca a bocca o il massaggio cardiaco, quindi intervenire in maniera adeguata.
- Utilizzare lo chassis rispettando le specifiche elettriche indicate e le istruzioni per l'uso del prodotto.

Prevenzione dei danni da scariche elettrostatiche

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

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

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

Ambiente di installazione

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

Considerazioni sull'alimentazione

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

- Controllare l'alimentazione prima di installare lo chassis per assicurarsi che la sede di installazione sia priva di picchi di corrente e interferenze. Installare uno stabilizzatore di tensione, se necessario, per garantire i voltaggi e i livelli di alimentazione adeguati nella tensione di ingresso dell'appliance.
- Installare la messa a terra adeguata per la sede in modo da evitare danni derivati da fulmini e sbalzi di corrente.

- Lo chassis non ha un intervallo operativo selezionabile dall'utente. Fare riferimento all'etichetta sullo chassis per i corretti requisiti di alimentazione in ingresso dell'appliance.
- Sono disponibili diversi tipi di cavi di alimentazione CA in ingresso per l'appliance; assicurarsi di disporre del tipo corretto per il proprio impianto.
- In caso di utilizzo di alimentatori doppi ridondanti (1+1), si consiglia di utilizzare circuiti elettrici indipendenti per ogni alimentatore.
- Se possibile, installare un gruppo di continuità nella propria sede.

Considerazioni sulla configurazione in rack

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

- Se si installa uno chassis in un rack aperto, verificare che il telaio del rack non blocchi le porte di aspirazione o di sfiato.
- Assicurarsi che i rack chiusi godano di un'adeguata ventilazione. Assicurarsi che il rack non contenga un numero eccessivo di apparecchiature poiché tutti gli chassis generano calore. Un rack chiuso deve avere i pannelli laterali finestrati e una ventola per il raffreddamento.
- In un rack chiuso con una ventola nella parte superiore, il caldo generato dalle apparecchiature nella parte inferiore del rack può salire verso l'alto e le porte di aspirazione delle apparecchiature presenti nella parte alta del rack. Assicurarsi di fornire una ventilazione adeguata alle apparecchiature sulla parte bassa del rack.
- L'uso di deflettori contribuisce a separare il flusso d'aria in uscita da quello in entrata e a convogliare l'aria all'interno dello chassis per raffreddarlo. La collocazione ottimale dei deflettori dipende dal percorso del flusso d'aria all'interno del rack. Provando diverse soluzioni, si può determinare come posizionare i deflettori in modo efficace.

3. Montaggio delle appliance

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

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

Hardware incluso con l'appliance

I seguenti componenti hardware sono forniti con le appliance Cisco Telemetry Broker:

- 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

Hardware aggiuntivo richiesto

Sono richiesti i seguenti componenti hardware aggiuntivi:

- Viti di montaggio per rack da 19" standard
- Gruppo statico di continuità (UPS) per ciascun nodo broker TB2300 da installare
- Per la configurazione in locale (facoltativo), procedere in uno dei seguenti modi:
    - Laptop con cavo video e cavo USB (per la tastiera)
    - Monitor con cavo video e tastiera con cavo USB

4. Connessione delle appliance alla rete

1. Revisione delle specifiche

Per connettere ciascun nodo broker TB2300 alla rete è possibile adottare la stessa procedura. L'unica differenza per la connessione consiste nel tipo di appliance di cui si dispone.

- **Scheda tecnica:** per informazioni dettagliate sulle specifiche, fare riferimento alle Schede tecniche di Cisco Telemetry Broker .
- **Piattaforma UCS:** l'appliance Cisco Telemetry Broker TB2300 usa la piattaforma UCS, UCSC-C225-M6SX.

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

2. Connessione dell'appliance alla rete

Per collegare l'appliance alla rete:

1. Collegare un cavo Ethernet alla porta di gestione come descritto nella scheda tecnica.
2. Collegare un cavo Ethernet alla porta di telemetria come descritto nella scheda tecnica.
    - Accertarsi che la porta di gestione sia connessa alla rete di gestione e che la porta di telemetria sia connessa alla rete di telemetria. Per ulteriori informazioni, vedere la sezione successiva Introduzione alla configurazione di rete.
3. Collegare l'altra estremità dei cavi Ethernet agli switch della rete.
4. Collegare i cavi di alimentazione all'alimentatore. Alcune appliance dispongono di due alimentazioni: alimentatore 1 e alimentatore 2.

Introduzione alla configurazione di rete

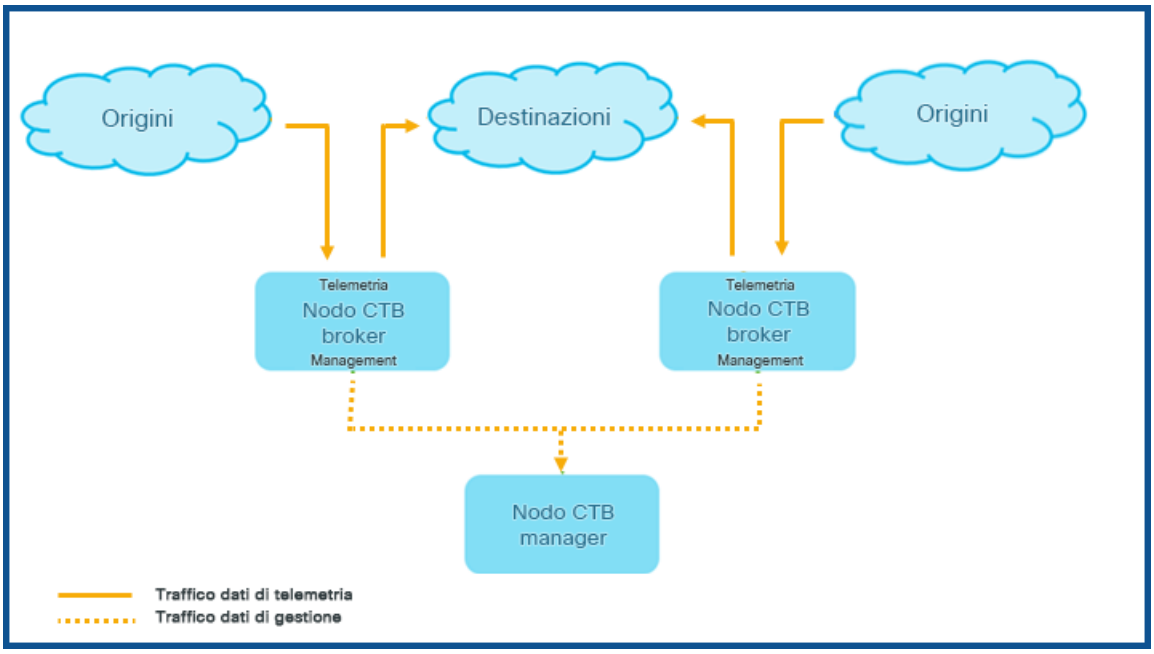
Cisco Telemetry Broker supporta una configurazione multinodo con un unico Cisco Telemetry Broker Manager che gestisce più nodi broker. Poiché Cisco Telemetry Broker aggiorna ogni nodo broker con tutte le destinazioni e le regole, occorre pianificare attentamente la configurazione per evitare gli errori più comuni descritti di seguito.

- I nodi broker possono essere implementati in segmenti di telemetria diversi e potrebbe quindi non essere possibile accedere alle interfacce di telemetria di ciascun nodo sulla rete. È necessario quindi creare attentamente le regole in modo che i pacchetti trasmessi da un dispositivo di esportazione a un determinato nodo non siano inoltrati alle destinazioni a cui non è possibile accedere da quel nodo. A tal fine, è necessario creare regole che escludano i dispositivi di esportazione che potrebbero causare questo problema di routing. Ad esempio, si sconsiglia l'uso di regole predefinite, in quanto finirebbero per restituire risultati per qualsiasi input.
- Le destinazioni potrebbero non essere tutte rilevanti per ciascun nodo broker. La funzione di verifica della raggiungibilità delle destinazioni prevede che ciascun nodo broker controlli se sia possibile accedere a ciascuna destinazione e potrebbe portare i nodi broker a segnalare informazioni contrastanti al nodo Manager. Se si prevede che alcuni nodi broker potrebbero non essere in grado di connettersi ad alcune destinazioni, disabilitare la funzione di verifica della raggiungibilità per tali destinazioni.

Se si esegue la migrazione a Cisco Telemetry Broker da UDP Director, prima di implementare il nodo Manager e i nodi broker, è necessario pianificarne la modalità di connessione, considerate le differenze nella configurazione di Cisco Telemetry Broker e UDP Director.

Cisco Telemetry Broker differenzia il traffico di telemetria dal traffico di gestione. Il nodo broker ha due interfacce: l'interfaccia della rete di telemetria e l'interfaccia della rete di gestione. Il nodo Manager ha solo l'interfaccia della rete di gestione. Nel diagramma seguente viene mostrato un esempio di logica di implementazione per il nodo Manager e i nodi broker.

> Si noti che gli esempi in questo argomento fanno riferimento a scenari di implementazione comuni. Per informazioni su come configurare un'implementazione più avanzata (ad esempio, con presenza di VLAN), contattare un amministratore di rete.



Cisco Telemetry Broker riceve il traffico di gestione *solo* sull'interfaccia della rete di gestione e usa questa interfaccia per tutte le comunicazioni tra il nodo broker e il nodo Manager. Il traffico di telemetria viene negoziato principalmente sull'interfaccia della rete di telemetria del nodo broker. L'unica eccezione si verifica quando Cisco Telemetry Broker richiama i log di flusso di AWS VPC o di Azure NSG o quando Cisco Telemetry Broker invia i dati di telemetria a SCA. In entrambi i casi, viene usata l'interfaccia della rete di gestione.

È possibile posizionare il nodo Manager in qualsiasi punto della rete su qualsiasi subnet, a condizione che la connettività TCP ai nodi broker sia disponibile sulla porta 443.

È possibile adottare una delle seguenti modalità di implementazione con il nodo broker:

1. Le subnet di telemetria e di gestione coincidono. In questa modalità, l'interfaccia della rete di telemetria e della rete di gestione sul nodo broker appartengono alla stessa subnet. Per ulteriori informazioni, vedere la sezione successiva Interfacce appartenenti alla stessa subnet.
2. Le subnet di telemetria e le subnet di gestione sono diverse, quindi il nodo broker gestisce l'interfaccia della rete di telemetria e l'interfaccia della rete di gestione su due subnet separate. Per ulteriori informazioni, vedere più avanti Interfacce appartenenti a subnet diverse.

Specificare percorsi separati per il traffico di telemetria e per il traffico di gestione ha i seguenti vantaggi:

- I percorsi separati aumentano le prestazioni, in particolare la velocità di linea dell'interfaccia, poiché il traffico non deve condividere le stesse risorse.
- Separare il traffico di gestione dal traffico di telemetria è una buona prassi per la configurazione della rete.

Interfacce appartenenti alla stessa subnet

Questa modalità di implementazione è molto simile a quella di UDP Director; in questo caso l'interfaccia della rete di gestione e l'interfaccia della rete di telemetria coincidono. L'unica differenza in questa prima modalità di implementazione è che le interfacce dei nodi broker richiedono indirizzi IP separati.

A tal fine, collegare l'interfaccia della rete di telemetria e l'interfaccia della rete di gestione del nodo broker alla stessa subnet.

Interfacce appartenenti a subnet diverse

In questa modalità di implementazione, l'interfaccia della rete di telemetria e l'interfaccia della rete di gestione si trovano su subnet diverse.

5. Connessione all'appliance

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

Scegliere la procedura di connessione:

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

Connessione con tastiera e monitor

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

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

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

3. Collegare la tastiera:
    - Se si dispone di una tastiera standard, collegarla al connettore della tastiera standard.
    - Se si dispone di una tastiera USB, collegarla a un connettore USB.
4. Collegare il cavo video al connettore video. Viene visualizzato il prompt di accesso.
5. Andare al capitolo successivo, **6. Configurazione del sistema Cisco Telemetry Broker**.

Connessione con cavo seriale o console seriale

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

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

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

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

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

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

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

5. Applicare le seguenti impostazioni:

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

    Vengono visualizzati la schermata e il prompt di accesso.

6. Andare al capitolo successivo, **6. Configurazione del sistema Cisco Telemetry Broker**.

Connessione con CIMC (richiesto per l'accesso remoto)

Cisco Integrated Management Controller (CIMC) consente l'accesso alla console di configurazione del server, alla console del server virtuale e ai sistemi di monitoraggio dell'integrità dell'hardware.

1. Seguire le istruzioni nella Guida alla configurazione della GUI di Cisco UCS serie C Integrated Management Controller.
2. Accedere a CIMC come admin e digitare la **password** nel campo Password.
3. Modificare la password predefinita per garantire una maggiore protezione della rete.
4. Andare al capitolo successivo, **6. Configurazione del sistema Cisco Telemetry Broker**.

6. Configurazione del sistema Cisco Telemetry Broker

Se l'installazione delle appliance fisiche è stata completata, è possibile configurare Cisco Telemetry Broker in un sistema gestito.

Requisiti del browser

Cisco Telemetry Broker supporta i seguenti browser (testati con l'ultima release rapida e con risoluzione a 1024 x 768 pixel):

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Requisiti di configurazione del sistema

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

Utilizzare la tabella seguente per preparare le informazioni necessarie per ciascun nodo broker TB2300.

Requisiti per la configurazione	Dettagli
Indirizzo IP	Assegnare un indirizzo IP instradabile alla porta di gestione.
Netmask	Stabilire la subnet per l'indirizzo IP scelto.
Gateway	Puntare all'indirizzo IP del gateway della subnet.
Nome host	È richiesto un nome host univoco per ciascun nodo broker TB2300. Non è possibile configurare un'appliance con lo stesso nome host di un altro nodo broker. Inoltre, accertarsi che i nomi host dei nodi broker soddisfino i requisiti standard degli host Internet.
Server DNS	Server DNS interno per la risoluzione dei nomi

Server NTP	Server di riferimento ora interno per la sincronizzazione tra i server. È necessario predisporre almeno 1 server NTP per ciascun nodo broker TB2300.

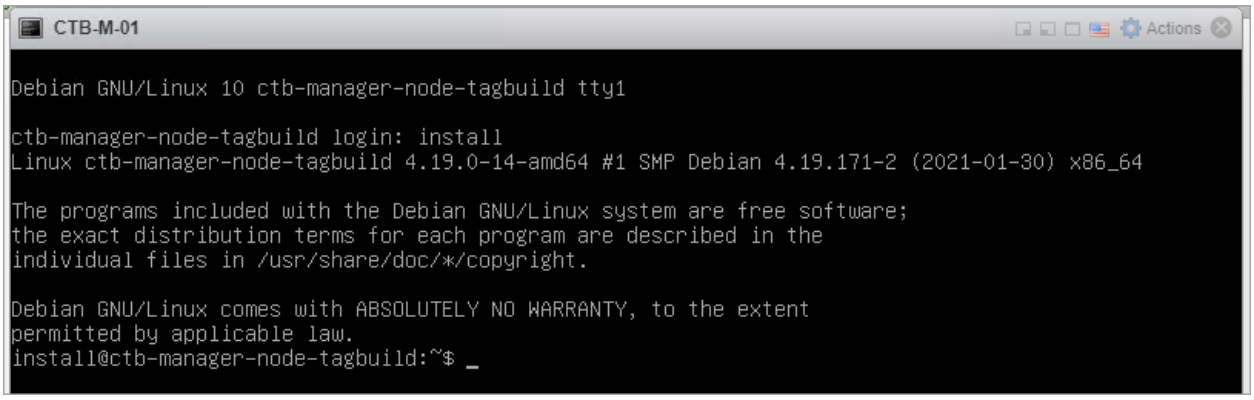
Installazione del nodo broker

Completare la procedura seguente secondo la sequenza indicata.

> Attualmente, l'unica appliance hardware esistente per Cisco Telemetry Broker è un nodo broker (TB2300). Ai fini dell'implementazione, il nodo broker deve essere associato a un nodo VM Manager.

1. Accedere come utente di installazione

Dalla console CIMC, fare clic su **Launch vKVM** (Avvia vKVM).



2. Eseguire il comando sudo ctb-install --init

1. Eseguire il comando `sudo ctb-install --init`.
2. Immettere le seguenti informazioni:
    - Password per l'utente **admin**

      La password deve soddisfare i seguenti requisiti:
        - Deve contenere almeno 8 caratteri
        - Deve contenere almeno 1 lettera minuscola
        - Deve contenere almeno 1 lettera maiuscola
        - Deve contenere almeno 1 cifra

- Deve contenere almeno 1 tra i seguenti caratteri speciali: @ # $ % ^ & * ! + ?
- Non può essere una frase o una sequenza di uso comune
- Non può essere simile ad alcun attributo identificativo dell'utente (ad esempio, il nome utente)

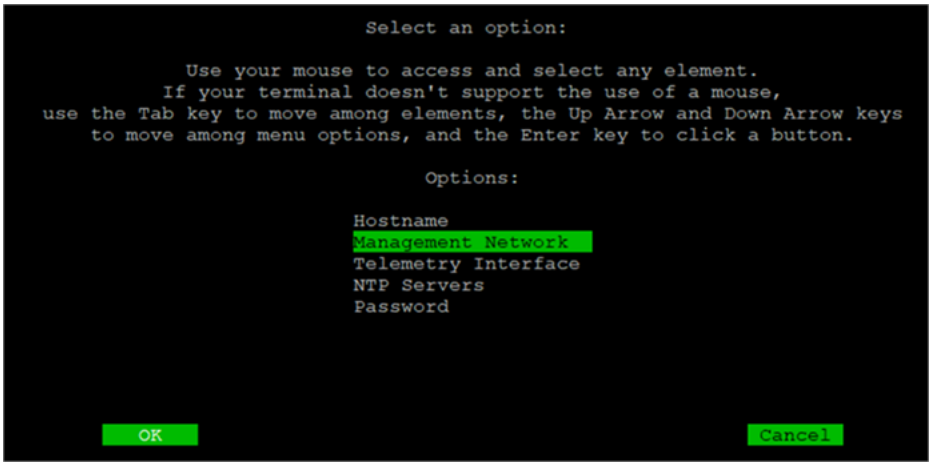
- Nome host (massimo 255 caratteri, solo lettere e numeri)
- È possibile immettere uno o entrambi i seguenti parametri dell'indirizzo IP:
  - Indirizzo IPv4, subnet mask e indirizzo gateway predefinito per l'interfaccia della rete di gestione
  - Indirizzo IPv6, subnet mask e indirizzo gateway predefinito per l'interfaccia della rete di gestione
- Indirizzo IP del server dei nomi DNS valido raggiungibile dal nodo broker (è possibile inserirne uno o due)
- Indirizzo IP NTP valido raggiungibile dal nodo broker.

(Facoltativo) Modifica di un singolo parametro

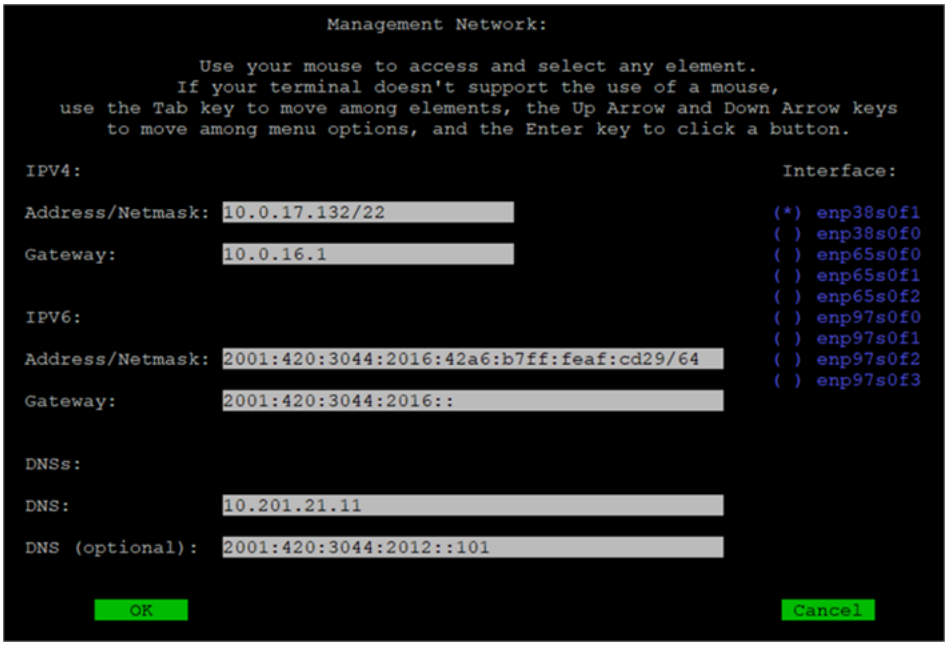
Per modificare un singolo parametro, eseguire il comando `sudo ctb-install --config`.

Modifica dell'interfaccia della rete di gestione

1. Per modificare l'interfaccia della rete di gestione, selezionare **Management Network** (Rete di gestione) dalla schermata principale, come mostrato di seguito:

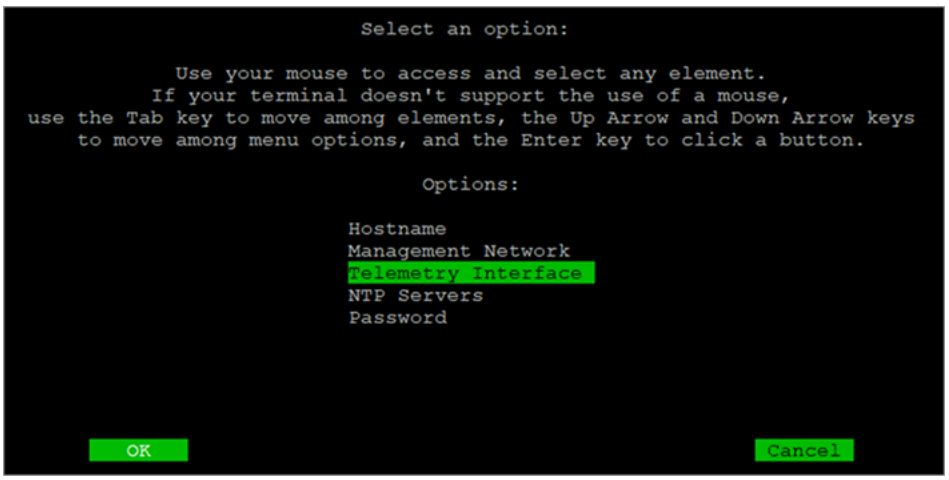


2. Nella schermata Management Network (Rete di gestione) visualizzata modificare le impostazioni secondo necessità, inclusa la selezione di una nuova interfaccia della rete di gestione. Fare riferimento alla Tabella delle corrispondenze tra numeri di porta e nomi di interfaccia alla fine di questa sezione per capire quale nome di interfaccia scegliere per un determinato numero di porta.



Modifica dell'interfaccia della rete di telemetria

1. Per modificare l'interfaccia della rete di telemetria, selezionare **Telemetry Interface** (Interfaccia di telemetria) dalla schermata principale, come mostrato di seguito:



2. Dalla schermata visualizzata, selezionare l'interfaccia della rete di telemetria interessata. Fare riferimento alla Tabella delle corrispondenze tra numeri di porta e nomi di interfaccia alla fine di questa sezione per capire quale nome di interfaccia scegliere per un determinato numero di porta.

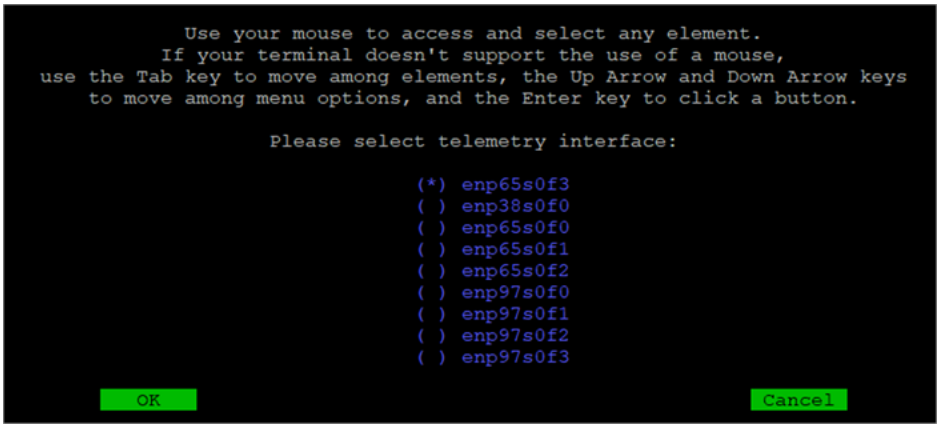
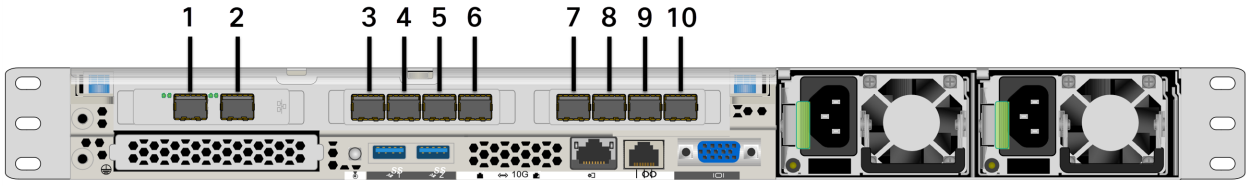


Tabella delle corrispondenze tra numeri di porta e nomi di interfaccia



Numero porta	Nome interfaccia
1	enp38s0f1
2	enp38s0f0
3	enp65s0f3
4	enp65s0f2
5	enp65s0f1
6	enp65s0f0
7	enp97s0f0

Numero porta	Nome interfaccia
8	enp97s0f1
9	enp97s0f2
10	enp97s0f3

I numeri di porta sono menzionati anche a pagina 2 e a pagina 3 della Scheda tecnica del nodo broker TB2300.

3. Eseguire il comando sudo ctb-manage

1. Eseguire il comando `sudo ctb-manage`.
2. Immettere le seguenti informazioni:
   - Indirizzo IP del nodo Manager
   - Nome utente dell'account con privilegi avanzati creato nel nodo Manager
   - Password dell'account con privilegi avanzati creato nel nodo Manager

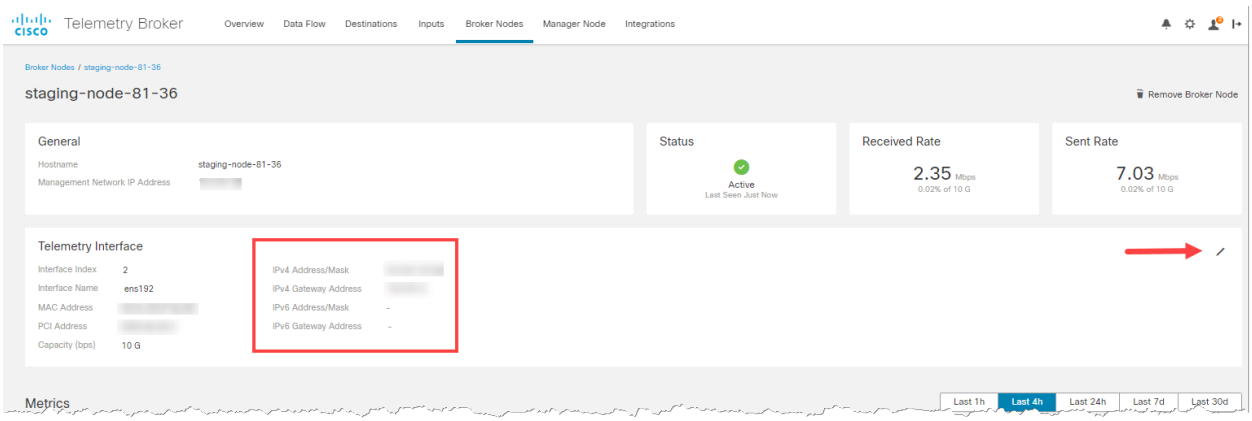
4. Disconnettersi

Per disconnettersi, digitare `exit`.

5. Configurare l'interfaccia di telemetria

Cisco Telemetry Broker è configurato per funzionare in modalità polling su un'appliance hardware.

1. Accedere a Cisco Telemetry Broker. In un browser Web, accedere all'indirizzo IP dell'interfaccia di gestione del nodo Manager, quindi premere **Invio** per accedere all'interfaccia Web del nodo Manager.
2. Dal menu principale, selezionare **Broker Nodes** (Nodi broker).
3. Nella tabella Broker Nodes (Nodi broker), fare clic sul nodo broker interessato.
4. Nella sezione Telemetry Interface (Interfaccia di telemetria), fare clic sull'icona **(Modifica)** (indicata dalla freccia nell'immagine seguente).



5. Configurare gli indirizzi IP e Gateway (evidenziati dal riquadro rosso).

Gestione dei cluster ad alta disponibilità

La funzionalità di alta disponibilità di Cisco Telemetry Broker fornisce indirizzi IPv4 e IPv6 virtuali come destinazioni degli input, garantendo l'inoltro affidabile dei dati di telemetria dalle fonti che li hanno generati alle destinazioni.

Per configurare l'alta disponibilità del nodo broker, è possibile creare cluster ad alta disponibilità e assegnare più nodi broker a ciascun cluster. In ogni cluster, un nodo broker è designato come *Attivo* per indicare che trasmette i dati di telemetria ed elabora le metriche per Cisco Telemetry Broker, mentre gli altri nodi sono considerati *Passivi*, ossia in quel momento non inviano dati di telemetria né elaborano metriche. Se un nodo broker attivo smette di trasmettere i dati di telemetria o perde la connettività con l'appliance Telemetry Broker, uno dei nodi broker passivi prende il suo posto come nodo attivo e inizia a trasmettere i dati di telemetria.

Tenere presente quanto segue sui cluster:

- Ogni nodo broker può appartenere a un solo cluster alla volta.
- Per creare un cluster, è necessario che gli sia stato assegnato almeno un nodo broker.
- Tenere presente che se si crea un cluster con un solo nodo broker e tale nodo broker non funziona, nessun altro nodo broker può prenderne il posto come nodo attivo. Analogamente, in caso di errore di tutti i nodi broker di un cluster, nessun nodo broker può diventare nodo attivo. In caso di guasto su un nodo broker, ripristinarne la connessione il prima possibile.
- Non è possibile scegliere il nodo broker attivo in un determinato cluster.
- In caso di guasto di un nodo broker attivo per un indirizzo IP virtuale, uno dei nodi broker passivi nello stesso cluster diventa il nodo broker attivo per l'indirizzo IP virtuale. Quando viene ripristinato il collegamento, il nodo broker precedentemente guasto continua a essere un nodo passivo. Se si desidera riattivare il nodo, è necessario farlo manualmente usando i comandi forniti nella sezione Spostamento di un indirizzo VIP su un nodo specifico in questo capitolo.
- È possibile assegnare un indirizzo IPv4 o IPv6 virtuale, o entrambi, a un cluster. Telemetry Broker usa questo indirizzo IP virtuale per comunicare con il cluster e far diventare attivi i nodi broker passivi in caso di problemi di connettività del nodo broker precedentemente attivo.

Per informazioni su come i cluster ad alta disponibilità vengono gestiti durante il processo di aggiornamento software di Cisco Telemetry Broker, consultare il capitolo "Aggiornamento del software" nella Guida per l'utente di Cisco Telemetry Broker.

VIP e routing

L'alta disponibilità configura l'indirizzo VIP per l'interfaccia della rete di telemetria del nodo broker. Notare che l'interfaccia della rete di telemetria di ciascun nodo broker nel cluster *deve sempre essere configurata* con un indirizzo IPv4 o IPv6 principale, con una subnet mask e un gateway. È possibile configurare questi parametri nell'interfaccia della rete di telemetria.

Gli indirizzi VIP IPv4 or IPv6 devono appartenere alla stessa subnet degli indirizzi IP principali **delle interfacce della rete di telemetria** nel cluster, in quanto anche l'indirizzo VIP deve appartenere alla stessa subnet. Ciò garantisce il corretto routing tramite il gateway preconfigurato e un rapido failover.

Se gli indirizzi VIP non si trovano nella stessa subnet degli indirizzi IP principali delle interfacce della rete di telemetria o se le interfacce della rete di telemetria di un cluster sono configurate con subnet diverse, è molto probabile che l'alta disponibilità non sia utilizzabile.

Gestione dei cluster

L'implementazione di Cisco Telemetry Broker si basa su due pacchetti Linux di uso comune che permettono di fornire l'infrastruttura sottostante per l'alta disponibilità:

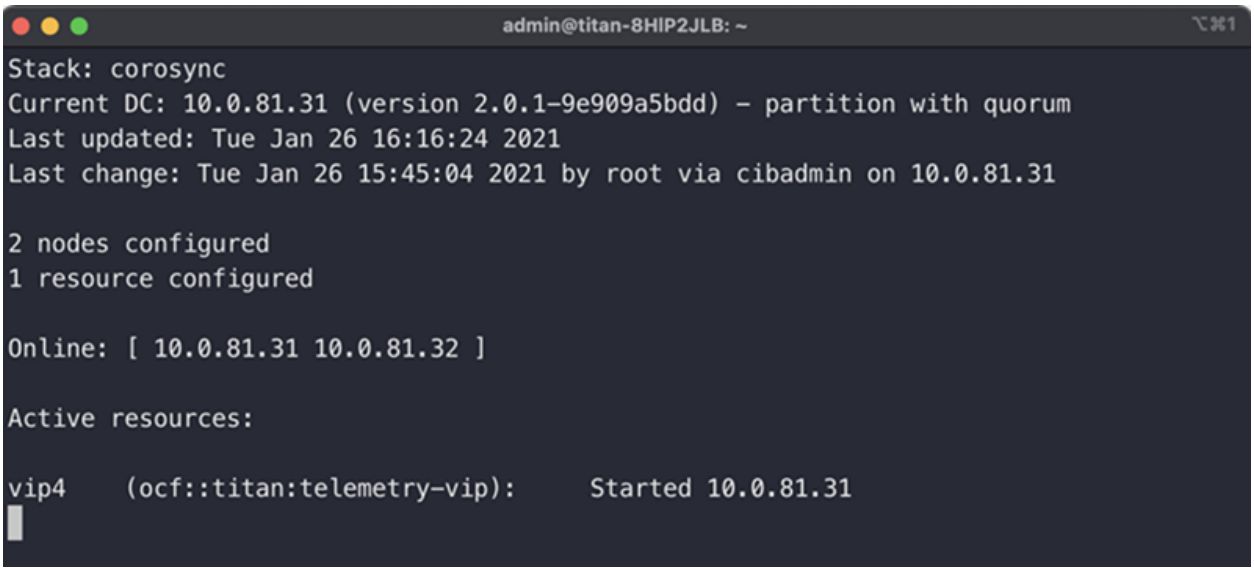
Corosync: motore del cluster di primo livello, permette la comunicazione sottostante tra i nodi del cluster. Fornisce inoltre la modalità quorum per prendere decisioni sul ruolo che deve avere ciascun nodo, attivo o in standby.

Pacemaker: gestisce le risorse del cluster, ossia tutte le relazioni tra le macchine e le applicazioni. Usa Corosync per comunicare.

Visualizzazione dello stato corrente del cluster

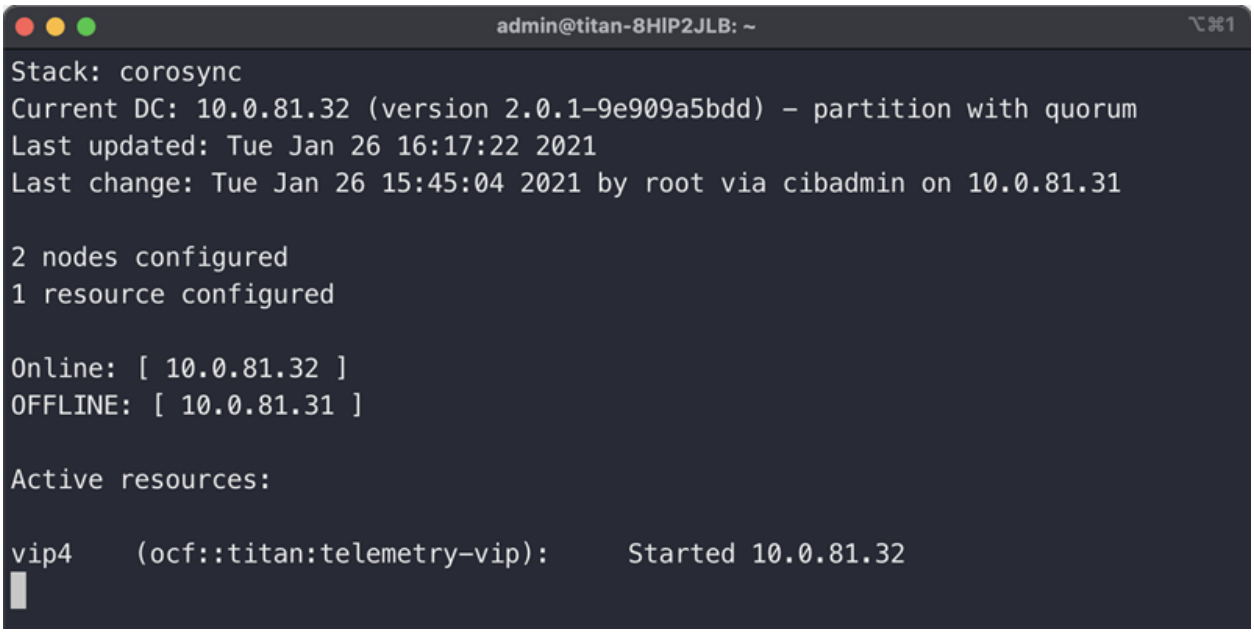
Per visualizzare lo stato corrente del cluster, incluso lo stato (offline o online) di ciascun nodo e la posizione degli indirizzi VIP IPv4 (vip4) e IPv6 (vip6), completare la seguente procedura:

1. Accedere in modalità SSH come **admin** a un nodo broker del cluster. Usare la password fornita durante l'installazione del nodo.
2. Eseguire il comando `sudo crm_mon`. Viene visualizzata una vista degli attributi attualmente configurati nel cluster. Per visualizzare altri dettagli su questo comando, fare clic qui.
3. Uscire dallo strumento premendo **Ctrl+C**.



L'immagine precedente descrive un cluster di due nodi, 10.0.81.31 e 10.0.81.32, entrambi con stato *Online*. L'indirizzo VIP IPv4 (vip4) è al momento in esecuzione su 10.0.81.31. L'indirizzo VIP IPv6 (vip6) non è visibile perché non è stato configurato.

Se l'indirizzo 10.0.81.31 non risponde, il suo stato sarà simile al seguente:



Notare come l'indirizzo 10.0.81.31 risulti ora *OFFLINE* e l'indirizzo vip4 sia stato spostato su 10.0.81.32.

Visualizzazione della configurazione corrente del cluster

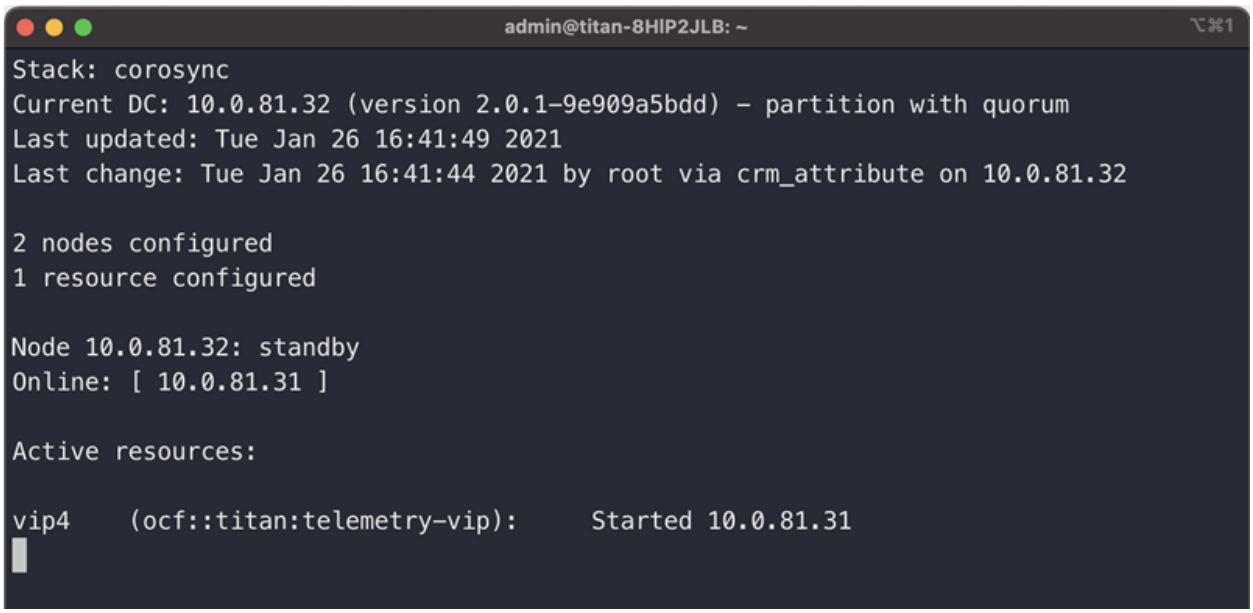
Per visualizzare la configurazione corrente del cluster e verificare che la configurazione di Corosync e Pacemaker sia corretta, completare la seguente procedura:

1. Accedere in modalità SSH come **admin** a un nodo broker del cluster. Usare la password fornita durante l'installazione del nodo.
2. Eseguire il comando `sudo crm configure show`. Viene visualizzata una vista dell'attributo attualmente configurato nel cluster. Per visualizzare altri dettagli su questo comando, fare clic qui.

Abilitazione e disabilitazione della modalità standby del nodo

In modalità standby, il nodo non può ospitare gli indirizzi IP virtuali IPv4 o IPv6.

1. Accedere in modalità SSH come **admin** a un nodo broker del cluster. Usare la password fornita durante l'installazione del nodo.
2. Eseguire il comando `sudo crm node standby 10.0.81.32`. È possibile omettere il nome del nodo se si esegue questo comando su quel nodo. Per visualizzare altri dettagli su questo comando, fare clic qui.
3. Eseguire il comando `sudo crm node online 10.0.81.32` per spostare il nodo dallo stato *Standby*. Per visualizzare altri dettagli sul comando, fare clic qui.



Come si può vedere, il comando *crm_mon* restituisce lo stato di standby del nodo 10.0.81.32.

Spostamento di un indirizzo VIP su un nodo specifico

In alcune circostanze, potrebbe essere necessario distinguere i nodi in esecuzione sugli indirizzi IP virtuali IPv4 o IPv6. A tal fine, adottare la seguente procedura:

1. Accedere in modalità SSH come **admin** a un nodo broker del cluster. Usare la password fornita durante l'installazione del nodo.
2. Eseguire il comando `sudo crm resource move vip4 10.0.81.32`. Per visualizzare altri dettagli su questo comando, fare clic qui.
3. Eseguire il comando `sudo crm resource unmove vip4` per verificare che l'indirizzo VIP sia sul nodo target, altrimenti l'indirizzo VIP verrà spostato di nuovo sul nodo su cui si trovava prima dello spostamento alla prima occasione.

Passaggi finali per la configurazione del sistema

Per completare la configurazione del sistema, fare riferimento alle seguenti sezioni della Guida per l'utente di Cisco Telemetry Broker:

- Destinazioni
- Input
- Nodi broker

Supporto tecnico

In caso di necessità, contattare il supporto tecnico:

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

Cronologia delle modifiche

Versione documento	Data di pubblicazione	Descrizione
1_0	Aprile 2023	Versione iniziale.
1_1	Maggio 2023	Aggiunto il capitolo "Migrazione della configurazione a un nuovo sistema".

Informazioni sul copyright

LE SPECIFICHE E LE INFORMAZIONI SUI PRODOTTI RIPORTATE DEL PRESENTE MANUALE SONO SOGGETTE A MODIFICHE SENZA PREAVVISO. TUTTE LE DICHIARAZIONI, LE INFORMAZIONI E LE RACCOMANDAZIONI FORMULATE NEL MANUALE SONO DA RITENERSI PRECISE, MA VENGONO FORNITE SENZA ALCUNA GARANZIA ESPLICITA O IMPLICITA. L'UTENTE SI ASSUME OGNI RESPONSABILITÀ IN MERITO ALL'UTILIZZO DEI PRODOTTI.

LA LICENZA SOFTWARE E LA GARANZIA LIMITATA RELATIVE AL PRODOTTO VENGONO FORNITE NEL PACCHETTO INFORMATIVO IN DOTAZIONE CON IL PRODOTTO STESSO E SONO INCORPORATE NELLA PRESENTE TRAMITE QUESTO RIFERIMENTO. IN CASO DI DIFFICOLTÀ A INDIVIDUARE LA LICENZA O LA GARANZIA LIMITATA DEL SOFTWARE, RICHIEDERNE UNA COPIA AL RAPPRESENTANTE CISCO DI RIFERIMENTO.

L'implementazione Cisco della compressione delle intestazioni TCP è un adattamento di un programma sviluppato dalla University of California (UCB) di Berkeley nell'ambito della versione pubblica del sistema operativo UNIX. Tutti i diritti sono riservati. Copyright © 1981, Regents of the University of California.

SENZA PREGIUDIZIO PER OGNI ALTRA GARANZIA, TUTTI I FILE DELLA DOCUMENTAZIONE E IL SOFTWARE DEI SUDDETTI FORNITORI SONO RESI DISPONIBILI "COSÌ COME SONO", CON EVENTUALI DIFETTI. CISCO E I FORNITORI SOPRA INDICATI NON RICONOSCONO ALCUNA GARANZIA, ESPLICITA O IMPLICITA, INCLUSE SENZA LIMITAZIONE LE GARANZIE DI COMMERCIABILITÀ, IDONEITÀ PER UNO SCOPO SPECIFICO, DI NON VIOLAZIONE DEI DIRITTI ALTRUI O DERIVANTI DA CONSUETUDINE, USO O PRASSI COMMERCIALE.

IN NESSUN CASO CISCO O I SUOI FORNITORI POTRANNO ESSERE RITENUTI RESPONSABILI DI EVENTUALI DANNI INDIRETTI, SPECIALI, CONSEQUENZIALI O INCIDENTALI, INCLUSI, A TITOLO ESEMPLIFICATIVO, MANCATI PROFITTI OPPURE PERDITA O DANNEGGIAMENTO DI DATI DERIVANTI DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE IL PRESENTE MANUALE, ANCHE QUALORA CISCO O I SUOI FORNITORI SIANO STATI INFORMATI DELLA POSSIBILITÀ DI TALI DANNI.

Nel presente documento vengono utilizzati indirizzi IP e numeri di telefono fittizi. Gli esempi, la visualizzazione dei comandi, i diagrammi di topologia di rete e le altre immagini contenute nel documento hanno scopo puramente illustrativo. L'utilizzo di indirizzi IP o numeri di telefono reali nei contenuti delle illustrazioni non è voluto ed è del tutto casuale.

Tutte le copie stampate e tutti i duplicati elettronici del presente documento sono da considerarsi non controllati. Per la versione più recente, vedere l'ultima versione online.

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono sono disponibili nel sito Web Cisco all'indirizzo https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.