



Cisco Telemetry Broker

Installations- och konfigurationsguide för maskinvara 2.0.1



Innehållsförteckning

Inledning	5
Översikt	5
Stödmatris för hårdvaru- och mjukvaruversion	5
Målgrupp	5
Installera virtuella broker-noder	5
Terminologi	6
Vanliga förkortningar	6
Koncept och arkitektur	8
Implementeringskrav	10
Versionsmatris för hårdvaru- och mjukvaruversion	10
Specifikationer	10
Cisco Integrated Management Controller (CIMC)	10
Migrera konfiguration till ett nytt system	11
Säkerhetskopiera CTB-konfigurationsregler	11
Återställ CTB-konfigurationsreglerna	11
1. Konfigurera din brandvägg för kommunikation	12
Öppna kommunikationsportar	12
2. Installationsvarningar och -riktlinjer	14
Installationsvarningar	14
Monteringsriktlinjer	16
Säkerhetsrekommendationer	17
Upprätthåll elsäkerheten	18
Förhindra ESD-skador	18
Platsmiljön	18
Överväganden om strömförsörjning	19
Överväganden vid rackkonfiguration	19
3. Montera dina apparater	20
Hårdvara som medföljer apparaten	20

Ytterligare nödvändig hårdvara	20
4. Anslut dina apparater till nätverket	21
1. Granska specifikationer	21
2. Anslut din apparat till nätverket	21
Bestäm nätverkskonfiguration	21
Gränssnitt tillhör samma subnät	23
Gränssnitt tillhör olika undernät	23
5. Anslut till din apparat	24
Anslutning med ett tangentbord och en bildskärm	24
Anslutning med en seriell kabel eller seriell konsol	25
Ansluta med CIMC (krävs för fjärråtkomst)	26
6. Konfigurera ditt Cisco Telemetry Broker-system	27
Webbläsarkrav	27
Systemkonfigurationskrav	27
Installera broker-noden	28
1. Logga in som installationsanvändare	28
2. Kör kommandot <code>sudo ctb-install --init</code>	28
(Valfritt) Ändra en individuell parameter	29
Mappning av portnummer-gränssnittsnamn	31
3. Kör kommandot <code>sudo ctb-manage</code>	32
4. Logga ut	32
5. Konfigurera telemetrigränssnittet	32
Hantera kluster med hög tillgänglighet	34
VIP:er och routing	35
Hantera kluster	35
Visa aktuell klusterstatus	35
Visa aktuell klusterkonfiguration	36
Aktivera och inaktivera nod-standbyläget	37
Flytta en VIP till en specifik nod	38
Slutför konfigurationen av ditt system	39

Kontakta kundtjänst	40
Tidigare ändringar	41

Inledning

Översikt

Den här guiden förklarar hur du installerar Cisco Telemetry Broker TB2300. Den här guiden beskriver även montering och installation av Cisco Telemetry Broker-hårdvaran. Observera att Cisco Telemetry Broker ibland kallas CTB i detta dokument.



Innan du installerar Broker Node TB2300 bör du läsa dokumentet med [säkerhetsinformation om föreskrifter och efterlevnad](#).

Stödmatrix för hårdvaru- och mjukvaruversion

Tillämpning	Plattform	Gen	v.2.0
Broker Node TB2300	UCSC-C220	M6	●

Använd denna förklaring när du läser stödmatrisen för hårdvaru- och mjukvaruversioner.

Symbol	Beskrivning
●	Fungerar med full kapacitet på hårdvara
○	Stöds, men prestandan är inte optimal
x	Stöds inte

Målgrupp

Den här guiden är utformad för den person som ansvarar för att installera Cisco Telemetry Broker-hårdvaran. Vi antar att du redan har en viss allmän förståelse för installation av nätverksutrustning.

Om du föredrar att arbeta med en professionell installatör ska du kontakta din lokala Cisco-partner eller [Cisco-kundtjänst](#).

Installera virtuella broker-noder

Om du vill installera virtuella broker-noder följer du instruktionerna i [Cisco Telemetry Broker Virtual Appliance Deployment och konfigurationsguiden](#).

Terminologi

Den här guiden använder ibland termen ”**apparat**” för att referera till Broker Node TB2300.

Ett ”**högt tillgänglighetskluster**” är en grupp broker-nods som hanteras av en hanteringsnod.

Vanliga förkortningar

Följande förkortningar förekommer i den här guiden:

Förkortning	Beskrivning
CIMC	Cisco Integrated Management Controller
DNS	Domännamnsserver/-tjänst
FTP	File Transfer Protocol
Gbps	Gigabits per sekund
GB	Gigabyte
HTTPS	Hypertext Transfer Protocol (Secure)
Mbit/s	Megabits per sekund
NAT	Adressöversättning
NIC	Network Interface Card (nätverkskort)
NTP	Network Time Protocol
SNMP	SNMP-protokoll (Simple Network Management Protocol)
SPAN	Switch Port Analyzer
SSH	Secure Shell
TAP	Test Access Port

Förkortning	Beskrivning
UDPD	UDP Director
UPS	Avbrottsfri strömförsörjning (Uninterruptible Power Supply)
URL	Universal Resource Locator
VLAN	Virtual Local Area Network
VM	Virtuell maskin (Virtual Machine)

Koncept och arkitektur

Cisco Telemetry Broker låter dig mata in nätverksteleometri från många ingångar, transformera telemetriformatet och vidarebefordra den telemetrin till en eller flera destinationer. Se följande tabell för exempel.

För närvarande är den enda hårdvaruapparaten som finns för Cisco Telemetry Broker en broker-nod (TB2300). Denna måste paras ihop med en VM-hanteringsnod för distribution.



Du kan distribuera en kombination av både virtuella och fysiska broker-noder, (broker-noder) eller så kan du distribuera endast alla virtuella broker-noder eller endast alla fysiska broker-noder.

Det krävs ingen installationsordning för broker-noder, även om du använder en kombination av virtuella och fysiska broker-noder.

Du kan mata in någon av följande telemetri:	Och vidarebefordra den telemetrin till någon eller alla av följande destinationer:
<ul style="list-style-type: none"> • Lokal nätverksteleometri, inklusive NetFlow, syslog och IPFIX • Molnbaserade telemetriingångar, som Amazon Web Services (AWS) Virtual Private Cloud (VPC) Flow Logs 	<ul style="list-style-type: none"> • Analysplattformar, som Secure Network Analytics eller Secure Cloud Analytics • Nätverkshantering och automationsplattformar, såsom Cisco DNA Center • Säkerhetsinformation och händelsehantering (SIEM)-plattformar

För att åstadkomma detta distribuerar du en eller flera Cisco Telemetry Broker-noder, som matar in telemetri och vidarebefordrar den till de konfigurerade destinationerna.

Cisco Telemetry Broker stöder följande transformationer från start:

Inmatat dataformat	Vidarebefordrat dataformat
VPC Flow Logs	IPFIX
Microsoft Network Security Group (NSG) Flow Logs	IPFIX
IPFIX, NetFlow v5, NetFlow v9	JSON (endast till SCA-destinationer)

Dina broker-noder hanteras alla av en Cisco Telemetry Broker-hanterare. Du kan logga in på denna hanterares webbgränssnitt och utföra olika konfigurationsuppgifter, inklusive att hantera broker-noderna, ställa in reglerna för vidarebefordran, skapa användare och granska instrumentpanelen för användning.

Implementeringskrav

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

Versionsmatris för hårdvaru- och mjukvaruversion

Granska supportmatrisen för hårdvaru- och mjukvaruversionerna för kompatibilitetsinformation. Matrisen finns dokumenterad i kapitlet **Inledning** i denna guide.

Specifikationer

Ladda ner [specifikationsbladet](#) för den Broker Node TB2300 som du planerar att installera.

Cisco Integrated Management Controller (CIMC)

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

- **Instruktioner:** se [ansluta med CIMC](#) och följ instruktionerna i konfigurationsguiden för [Cisco UCS C-Series Integrated Management Controller GUI](#).
- **Standardlösenord:** som en del av den initiala konfigurationen kommer du att logga in på CIMC som admin och skriva in **lösenordeti** fältet Lösenord.
- **Lösenordskrav:** när du loggar in bör du ändra standardlösenordet för att skydda ditt nätverks säkerhet.

Migrera konfiguration till ett nytt system

Slutför följande processer för att säkerhetskopiera och återställa CTB-konfigurationsreglerna som du ställer in i Cisco Telemetry Broker-hanteraren.

- Det är möjligt för UDPD-kunder att migrera sin befintliga UDPD-konfiguration till Cisco Telemetry Broker. Se avsnittet "Importer och exporter UDP Director-konfiguration" i Cisco Telemetry Broker-användarhandboken för mer information.

Säkerhetskopiera CTB-konfigurationsregler

Kör följande kommando på CTB-hanteringsnoden:

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

När denna process är klar kommer konfigurationsreglerna att säkerhetskopieras till filen på `~/ctb_config.json`, varefter du kan kopiera konfigurationsreglerna till en annan plats.

- VPC/NSG-flödesloggregler säkerhetskopieras inte, så du måste återskapa dina VPC-/NSG-flödesloggregler vid migrering till ett nytt system.
- Du kan endast säkerhetskopiera och återställa dina CTB-konfigurationsregler inom samma version. Om du försöker göra det på flera olika versioner kan processen misslyckas.

Återställ CTB-konfigurationsreglerna

 Du måste köra `ctb-restore-config` efter att du har slutfört `ctb-install --init` på hanteringsnoden. Om du manuellt skapar ett GUI-inloggningskonto kommer det att skrivas över av kontoinformationen från `ctb-restore-config`.

Slutför dessa steg:

1. Logga ut som *installationsanvändare*
2. Kopiera filen **ctb-config.json** från ett befintligt system.
3. Logga in på det nya systemet som *admin*.
4. Kör följande kommando på CTB-hanteringsnoden:

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

Alla indata som du lägger till i Cisco Telemetry Broker på grund av återställningen tilldelas inte till några noder eller kluster. Du måste tilldela dem efter behov.

1. Konfigurera din brandvägg för kommunikation

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

Öppna kommunikationsportar

Följande tabell ger information om alla nätverksanslutningar till och från dina Cisco Telemetry Broker-apparater. För att säkerställa att ditt nätverk tillåter dessa anslutningar måste du ändra tillämpliga åtkomstkontroller som du för närvarande använder (till exempel din brandvägg).

Klient	Server	Port	Beskrivning
användare	broker-noder och hanterarnoder	22/TCP	SSH-tillgång till konsolen
Chef	externt internet	443/TCP	HTTPS för säker extern kommunikation, såsom smart licensiering och mjukvaruuppdatering
Chef	kundens syslog-server	kunddefinierad port	Syslog-telemetri för Cisco Telemetry Broker-aviseringar
Chef	kundens SMTP-server	kunddefinierad port	SMTP-telemetri för Cisco Telemetry Broker-aviseringar
varje broker-nod	Chef	443/TCP	HTTPS för säkra hanteringsanslutningar

varje broker-nod	extern internet	443/TCP	HTTPS för att hämta VPC/NSG Flow Logs från AWS S3/Azure SAS lagringsbuckets. HTTPS för brokernod för att säkra åtkomst till SCA-server och ladda upp filer till SCA S3-bucket.
användare	Chef	443/TCP	HTTPS för säker åtkomst till webbgränssnittet
broker-noder och hanterarnoder	kundens DNS-serverar	53/UDP	DNS-telemetri
varje <i>hårdvaru</i> -broker-nod	kundens NTP-server	123	NTP-data för tidssynkronisering

Dessutom måste du öppna portar baserat på både telemetritypen som skickas till en broker-nod och telemetritypen som en broker-nod skickar till en destination. Följande tabell ger information om vanliga portar för olika telemetrityper:

Port	Beskrivning
514/UDP	syslog
2055/UDP	NetFlow v5, NetFlow v9
4739/UDP	IPFIX
6343/UDP	sFlow

2. Installationsvarningar och -riktlinjer


Installationsvarningar

Läs [dokumentet Säkerhetsinformation om föreskrifter och efterlevnad](#) innan du installerar någon Cisco Telemetry Broker-apparat.

Observera följande varningar:


Redogörelse 1071 – Varningsdefinition

VIKTIGA SÄKERHETSINSTRUKTIONER


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

SPARA DE HÄR INSTRUKTIONERNA


Redogörelse 1004 – Installationsinstruktioner

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

Redogörelse 12 – Varning: Nätaggregat urkopplat

 Innan du arbetar på ett chassi eller arbetar nära nätaggregat ska du koppla ur nätsladden på AC-enheter, och slå av strömmen till strömbrytaren på DC-enheter.

Redogörelse 43 – Varning: ta av smycken

 Innan du börjar arbeta med utrustning som är ansluten till ström ska du ta av dig eventuella smycken (inklusive ringar, halsband och klockor). Metallobjekt värms upp när de ansluts till ström och jord, och kan leda till allvarliga brännskador eller bränna fast metallföremål på terminalerna.

Redogörelse 94 – Varning: handledsrem

- ⚠ Använd jordningsarmband under denna procedur för att undvika att kortet skadas av elektrostatiska urladdningar. Rör inte bakplanet direkt med handen eller något metallverktyg, annars kan du få en stöt.

Redogörelse 1045 – Kortslutningsskydd

- ⚠ Denna produkt kräver kortslutningsskydd (överströmsskydd) som en del av byggnadsinstallationen. Montera endast i enlighet med nationella och lokala kabeldragningsregler.

Redogörelse 1021 – SELV-krets

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

Redogörelse 1024 – Jordledare

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

Redogörelse 1040 – Kassering av produkten

- ⚠ Denna produkt ska kasseras enligt nationella lagar och förordningar.

Redogörelse 19 – TN-kraftvarning

- ⚠ Enheten är designad för att fungera med TN-strömsystem.

Monteringsriktlinjer

Observera följande varningar:

Redogörelse 1047 – Överhettningsskydd

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

Redogörelse 1019 – Huvudfrånkopplingsenhet

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

Redogörelse 1005 – Kretsbytare

- ⚠ Produkten förlitar sig på byggnadens installation för kortslutningsskydd (överspänning). Se till att skyddsanordningen inte är klassad som högre än (för USA): 120, 15 A (för EU): 250 V, 16 A

Redogörelse 1074 – Följ lokala och nationella elbestämmelser

- ⚠ Montering av utrustningen måste uppfylla lokala och nationella elföreskrifter.

Redogörelse 371 – strömkabel och växelströmsadapter

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

Redogörelse 1073 – Inga delar som användaren kan utföra service på

- ⚠ Inga inre delar behöver servas av användare. Öppna inte.

När du installerar ett chassi ska du använda följande riktlinjer:

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



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

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



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

Säkerhetsrekommendationer

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

Följ dessa säkerhetsriktlinjer:

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

Upprätthåll elsäkerheten

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

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

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

Förhindra ESD-skador

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

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

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

Platsmiljön

För att undvika utrustningsfel och minska risken för avstängningar orsakade av miljön bör du planera anläggningens layout och utrustningsplatserna noggrant. Om du för närvarande upplever avstängningar eller ovanligt höga felfrekvenser med din befintliga

utrustning, kan dessa överväganden hjälpa dig att hitta orsaken till felen och förhindra framtida problem.

Överväganden om strömförsörjning

Tänk på följande när du installerar chassit:

- Kontrollera platsen innan du installerar chassit för att säkerställa att den är fritt från spikar och buller. Installera en strömconditionering om det behövs, för att säkerställa korrekta spänningar och effektnivåer i apparatens inspänning.
- Installera korrekt jordning för platsen för att undvika skador från blixtnedslag och överspänningar.
- Chassit har inget användarvalbart driftsområde. Se etiketten på chassit för rätt ingångseffekt för apparaten.
- Det finns flera olika typer av nätsladdar med AC-ingång för apparaten, så se till att du har rätt typ för din plats.
- Om du använder dubbla redundanta (1+1) nätaggregat rekommenderar vi att du använder oberoende elektriska kretsar för varje strömförsörjning.
- Installera en avbrottsfri strömkälla för din plats, om möjligt.

Överväganden vid rackkonfiguration

Tänk på följande när du planerar en rackkonfiguration:

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

3. Montera dina apparater

Du kan montera Cisco Telemetry Broker-apparater direkt i ett standard 19-tumsrack eller -skåp, vilket annat lämpligt skåp som helst eller på en plan yta. När du monterar en apparat i ett rack eller ett skåp följer du instruktionerna som ingår i monteringssetserna för skenan. När du bestämmer var du ska placera en apparat ser du till att utrymmet till de främre och bakre panelerna är som följer:

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

Hårdvara som medföljer apparaten

Följande hårdvara medföljer Cisco Telemetry Broker apparater:

- Nätsladd
- Åtkomstnycklar (för frontplattan)
- Skensats för stativmontering eller monteringsöron för mindre apparater

Ytterligare nödvändig hårdvara

Du måste tillhandahålla följande ytterligare nödvändiga hårdvara:

- Monteringsskruv för ett standard 19-tumsrack
- Avbrottsfri strömförsörjning (Uninterruptible power supply/UPS) för den Broker Node TB2300 som du installerar
- För att konfigurera lokalt (valfritt) använder du någon av följande metoder:
 - Bärbar dator med en videokabel och en USB-kabel (för tangentbordet)
 - Videomonitor med videokabel och tangentbord med USB-kabel

4. Anslut dina apparater till nätverket

1. Granska specifikationer

Använd samma procedur för att ansluta varje Broker Node TB2300 till nätverket. Den enda skillnaden för anslutningen är vilken typ av apparat du har.

- **Specifikationsblad:** för detaljerad specifikationsinformation läser du Cisco Telemetry Broker-[specifikationsbladet](#).
- **UCS-plattform:** Cisco Telemetry Broker TB2300 använder UCS-plattformen, UCSC-C225-M6SX.



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

2. Anslut din apparat till nätverket

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

1. Anslut en Ethernet-kabel till hanteringsporten enligt definitionen i specifikationsbladet.
2. Anslut en Ethernet-kabel till telemetriporten enligt definitionen i specifikationsbladet.
 - Se till att hanteringsporten är ansluten till hanteringsnätverket och att telemetriporten är ansluten till telemetrinätverket. Se nästa avsnitt, [Bestäm nätverkskonfiguration](#), för mer information.
3. Anslut den andra änden av Ethernet-kablarna till ditt nätverks switch eller switchar.
4. Anslut strömkablarna till strömförsörjningen. Vissa apparater har två strömanslutningar: strömförsörjning 1 och strömförsörjning 2.

Bestäm nätverkskonfiguration

Cisco Telemetry Broker stöder inställningar för flera noder, där en enda Cisco Telemetry Broker-hanterare kan hantera flera broker-noder. Eftersom Cisco Telemetry Broker uppdaterar varje broker-nod med alla destinationer och regler måste du noggrant planera din konfiguration för att undvika några vanliga problem, som listas nedan.

- Du kan distribuera broker-noder i olika telemetrisegment, där telemetrigränssnitten för varje broker-nod kanske inte är tillgängliga över nätverket. Du måste noggrant konstruera regler så att paket från en exportör som når en specifik nod inte

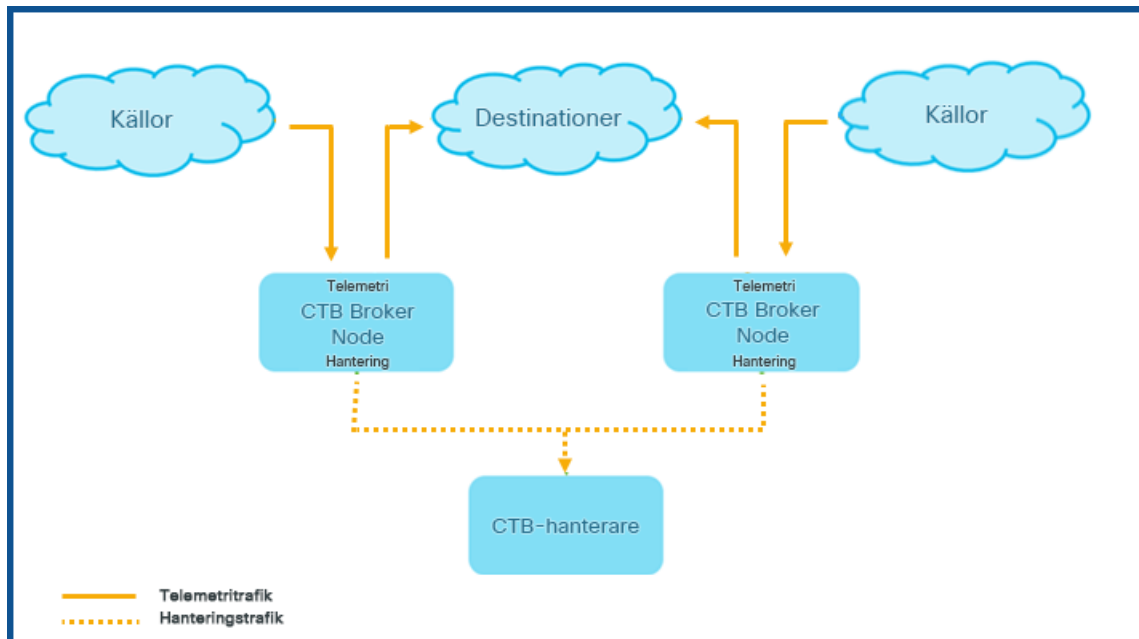
vidarebefordras till destinationer som inte är tillgängliga från den noden. För att uppnå detta måste du skapa regler som utesluter exportörer som kan orsaka detta routingproblem. Ett exempel skulle vara att inte använda några standardregler, eftersom dessa skulle matcha alla indata.

- Alla destinationer kanske inte är relevanta för varje broker-nod. Men med funktionen Kontrollera destinationens nåbarhet, och eftersom varje broker-nod försöker fastställa tillgänglighet för varje destination, kan broker-noder rapportera motstridig information tillbaka till hanteraren. Om det finns en risk att vissa broker-noder inte kommer att kunna ansluta till vissa destinationer, inaktiverar du Kontrollera destinationens nåbarhet för dessa destinationer.

Om du migrerar till Cisco Telemetry Broker från UDP- Director behöver du, innan du distribuerar hanteringsnoden och broker-noden/-noderna planera hur du ska ansluta hanteringsnoden och broker-noden/-noderna till nätverket, eftersom det finns skillnader mellan hur du konfigurerar både Cisco Telemetry Broker och UDP Director.

Cisco Telemetry Broker skiljer telemetritrafik från hanteringstrafik. Broker-noden har två gränssnitt: telemetrinätverksgränssnittet och hanteringsnätverksgränssnittet. Hanteringsnoden har bara hanteringsnätverksgränssnittet. Följande diagram visar hur man logiskt distribuerar hanteringsnoden och broker-noderna.

i Observera att exemplen i det här ämnet representerar typiska distributionsscenarioer. Kontakta en nätverksadministratör för att lära dig hur du ställer in en mer avancerad distribution (till exempel en som använder VLAN).



Cisco Telemetry Broker tar *endast* emot hanteringstrafik på hanteringsnätverksgränssnittet. Det använder detta gränssnitt för all kommunikation mellan broker-noden och hanteringsnoden. Telemetritrafik förmedlas primärt på broker-nodens telemetrinätverksgränssnitt. Det enda undantaget från detta är när Cisco Telemetry Broker hämtar AWS VPC-flödesloggar eller Azure NSG -flödesloggar, eller när Cisco Telemetry Broker skickar telemetri till SCA, som båda sker över broker-nodens hanteringsnätverksgränssnitt.

Du kan placera hanteringsnoden var som helst i nätverket på vilket subnät som helst, men du måste ha TCP-anslutning via port 443 med broker-noderna.

Du kan använda ett av följande distributionslägen med broker-noden:

1. Telemetrisubnäten och hanteringssubnäten är desamma. I det här läget hör telemetrinätverksgränssnittet och hanteringsnätverksgränssnittet på broker-noden till samma subnät. För mer information, se nästa avsnitt: [Gränssnitt tillhör samma subnät](#).
2. Telemetrisubnäten och hanteringssubnäten är olika, så broker-noden behåller sitt telemetrinätverksgränssnitt och hanteringsnätverksgränssnittet på två separata subnät. För mer information, se två avsnitt nedan: [Gränssnitt tillhör olika subnät](#).

Att tillhandahålla separata vägar för både telemetritrafik och hanteringstrafik ger följande fördelar:

- Separata vägar ökar prestandan, särskilt när den närmar sig prestandan för gränssnittshastighet, eftersom trafiken inte behöver dela resurser.
- Att separera hanteringstrafik från telemetritrafik är helt enkelt bra för en nätverkskonfiguration.

Gränssnitt tillhör samma subnät

Detta distributionsläge är mycket likt det för UDP Director, där hanteringsnätverksgränssnittet och telemetrinätverksgränssnittet är samma. Den enda skillnaden i detta första distributionsläge är att du behöver separata IP-adresser för broker-nodgränssnitten.

Du kan åstadkomma detta genom att ansluta broker-nodens telemetrinätverksgränssnitt och hanteringsnätverksgränssnitt till samma subnät.

Gränssnitt tillhör olika undernät

I det här distributionsläget finns gränssnittet för telemetrinätverk och gränssnittet för hanteringsnätverk på olika subnät.

5. Anslut till din apparat

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

Välj din anslutningsprocedur:

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

Anslutning med ett tangentbord och en bildskärm

Utför följande steg för att konfigurera IP-adressen lokalt:

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

Du kan behöva ta bort frontpanelen för att tillhandahålla ström.



Strömförsörjningsfläktarna slås på för vissa modeller när systemet inte är påslaget. Kontrollera att lysdioden på frontpanelen lyser.

Se till att ansluta apparaten till en avbrottsfri strömkälla (uninterruptible power supply/UPS). Strömförsörjningen kräver ström, annars visar systemet ett fel.

3. Anslut tangentbordet:
 - Om du har ett standardtangentbord ansluter du det till standardtangentbordskontakten.
 - Om du har ett USB-tangentbord ansluter du det till en USB-kontakt.
4. Anslut videokabeln till videokontakten. Inloggningsuppmeningen visas.
5. Gå till nästa kapitel, **6. Konfigurera ditt Cisco Telemetry Broker-system**.

Anslutning med en seriell kabel eller seriell konsol

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

1. Anslut din bärbara dator till apparaten med någon av följande metoder:
 - Anslut en RS232-kabel från den seriella portkontakten (DB9) på din bärbara dator till konsolporten på apparaten.
 - Anslut en korsad kabel från Ethernet-porten på din bärbara dator till hanteringsporten på apparaten.
2. Anslut strömkabeln till apparaten.
3. Tryck på strömknappen för att slå på apparaten. Vänta tills den har startat upp helt. Avbryt inte uppstartsprocessen.

Du kan behöva ta bort frontpanelen för att tillhandahålla ström.



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

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

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

5. Använd följande inställningar:

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

Inloggningsskärmen och inloggningssupmaningen visas.

6. Gå till nästa kapitel, **6. Konfigurera ditt Cisco Telemetry Broker-system**.

Ansluta med CIMC (krävs för fjärråtkomst)

Cisco Integrated Management Controller (CIMC) möjliggör åtkomst till serverkonfigurationen och en virtuell serverkonsol, samt övervakar hårdvarans hälsa.

1. Följ instruktionerna i [konfigurationsguiden för Cisco UCS C-Series Integrated Management Controller GUI](#).
2. Logga in på CIMC som admin och skriv in **lösenordet** i fältet Lösenord.
3. Ändra standardlösenordet för att skydda ditt nätverks säkerhet.
4. Gå till nästa kapitel, **6. Konfigurera ditt Cisco Telemetry Broker-system**.

6. Konfigurera ditt Cisco Telemetry Broker-system

Om du har installerat dina hårdvaruapparater är du redo att konfigurera Cisco Telemetry Broker till ett hanterat system.

Webbläsarkrav

Cisco Telemetry Broker stöder följande webbläsare (som testats med den senaste snabbversionen och med upplösningen 1024 x 768 px):

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Systemkonfigurationskrav

Se till att du har tillgång till apparatens konsol via [CIMC](#).

Använd följande tabell för att förbereda den information som krävs för varje Broker Node TB2300.

Konfigurationskrav	Information
IP-adress	Tilldela en routbar IP-adress till hanteringsporten.
Nätmask	Etablera subnätet för din valda IP-adress.
Gateway	Peka på ditt subnäts gateway IP-adress.
Världnamn	Ett unikt världnamn krävs för varje Broker Node TB2300. Vi kan inte konfigurera en apparat med samma världnamn som en annan broker-nod. Se också till att varje broker-nods världnamn uppfyller internetstandardkraven för internetvärdar.
DNS-servrar	Intern DNS-server för namnlösning
NTP-servrar	Intern tidsserver för synkronisering mellan servrar. Minst 1 NTP-server krävs för varje Broker Node TB2300.

Installera broker-noden

Slutför följande steg i ordning.



För närvarande är den enda hårdvaruapparaten som finns för Cisco Telemetry Broker en broker-nod (TB2300). Denna måste paras ihop med en VM-hanteringsnod för distribution.

1. Logga in som installationsanvändare

Klicka på **Starta vKVM** från CIMC-konsolen.

```

CTB-M-01
Debian GNU/Linux 10 ctb-manager-node-tagbuild tty1
ctb-manager-node-tagbuild login: install
Linux ctb-manager-node-tagbuild 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
install@ctb-manager-node-tagbuild:~$ _
  
```

2. Kör kommandot `sudo ctb-install --init`

1. Kör kommandot `sudo ctb-install --init`

2. Ange följande information:

- Lösenord för **admin**användaren

Lösenordet måste uppfylla följande krav:

- Innehålla minst 8 tecken
- Innehålla minst 1 liten bokstav
- Innehålla minst 1 stor bokstav
- Innehålla minst 1 siffra
- Innehålla minst 1 av dessa specialtecken: @ # \$ % ^ & * ! + ?
- Kan inte vara en vanligt använd fras eller sekvens
- Kan inte likna några identifierande attribut från användaren (som användarnamnet)
- Värdnamn (max 255 tecken, endast bokstäver och siffror)

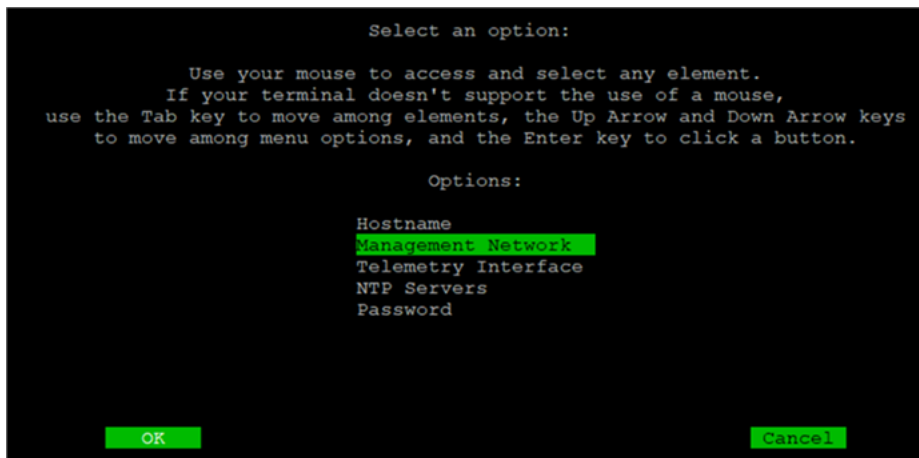
- Du kan ange en eller båda av följande IP-adressparametrar:
 - IPv4-adress, subnätmask och standardgatewayadress för hanteringsnätverksgränssnittet
 - IPv6-adress, subnätmask och standardgatewayadress för hanteringsnätverksgränssnittet
- Giltig DNS-namnserver med IP-adress som kan nås från broker-noden (du kan ange en eller två)
- Giltig NTP med IP-adress som kan nås från broker-noden.

(Valfritt) Ändra en individuell parameter

För att ändra en individuell parameter kör du kommandot `sudo ctb-install --config`.

Ändra hanteringsnätverkets gränssnitt

1. För att ändra hanteringsnätverkets gränssnitt väljer du **hanteringsnätverket** från huvudskärmen, som visas nedan:



2. Från skärmen Hanteringsnätverk som öppnas gör du eventuella ändringar i inställningarna för hanteringsnätverket, inklusive att välja ett nytt hanteringsnätverksgränssnitt. Se [tabellen Mappning av portnummer-gränssnittsnamn](#) som visas i slutet av detta avsnitt för att veta vilket gränssnittsnamn du ska välja för ett visst portnummer.

```

Management Network:

Use your mouse to access and select any element.
If your terminal doesn't support the use of a mouse,
use the Tab key to move among elements, the Up Arrow and Down Arrow keys
to move among menu options, and the Enter key to click a button.

IPV4:                                     Interface:
Address/Netmask: 10.0.17.132/22           (*) enp38s0f1
Gateway:         10.0.16.1                ( ) enp38s0f0
                                                         ( ) enp65s0f0
                                                         ( ) enp65s0f1
                                                         ( ) enp65s0f2
IPV6:                                     ( ) enp97s0f0
Address/Netmask: 2001:420:3044:2016:42a6:b7ff:feaf:cd29/64 ( ) enp97s0f1
Gateway:         2001:420:3044:2016:::    ( ) enp97s0f2
                                                         ( ) enp97s0f3

DNSs:
DNS:             10.201.21.11
DNS (optional): 2001:420:3044:2012::101

OK                                     Cancel

```

Ändra telemetrinätverkets gränssnitt

1. För att ändra gränssnittet för telemetrinätverk väljer du **Telemetrigränssnitt** från huvudskärmen, som visas nedan:

```

Select an option:

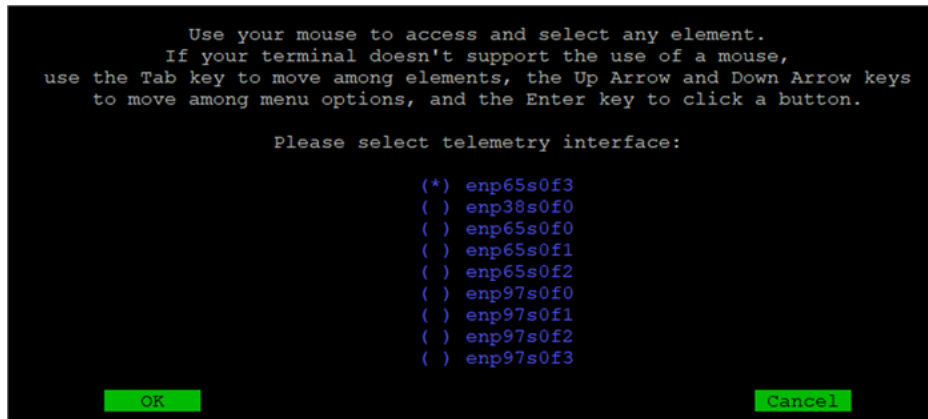
Use your mouse to access and select any element.
If your terminal doesn't support the use of a mouse,
use the Tab key to move among elements, the Up Arrow and Down Arrow keys
to move among menu options, and the Enter key to click a button.

Options:
  Hostname
  Management Network
  Telemetry Interface
  NTP Servers
  Password

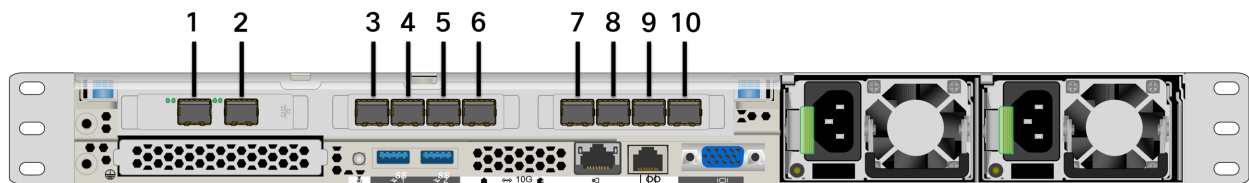
OK                                     Cancel

```

2. På skärmen som öppnas väljer du tillämpligt telemetrinätverksgränssnitt. Se [tabellen Mappning av portnummer-gränssnittsnamn](#) som visas i slutet av detta avsnitt för att veta vilket gränssnittsnamn du ska välja för ett visst portnummer.



Mapping av portnummer-gränssnittsnamn



Portnummer	Gränssnittsnamn
1	enp38s0f1
2	enp38s0f0
3	enp65s0f3
4	enp65s0f2
5	enp65s0f1
6	enp65s0f0
7	enp97s0f0
8	enp97s0f1
9	enp97s0f2
10	enp97s0f3



Dessa portnummer hänvisas även till på sidorna 2 och 3 i [specifikationsbladet till Broker Node TB2300](#).

3. Kör kommandot `sudo ctb-manage`

1. Kör kommandot `sudo ctb-manage`
2. Ange följande information:
 - IP-adress för hanteringsnoden
 - Användarnamn för superanvändarkontot du skapar i hanteringsnoden
 - Lösenordet för superanvändarkontot du skapar i hanteringsnoden


4. Logga ut

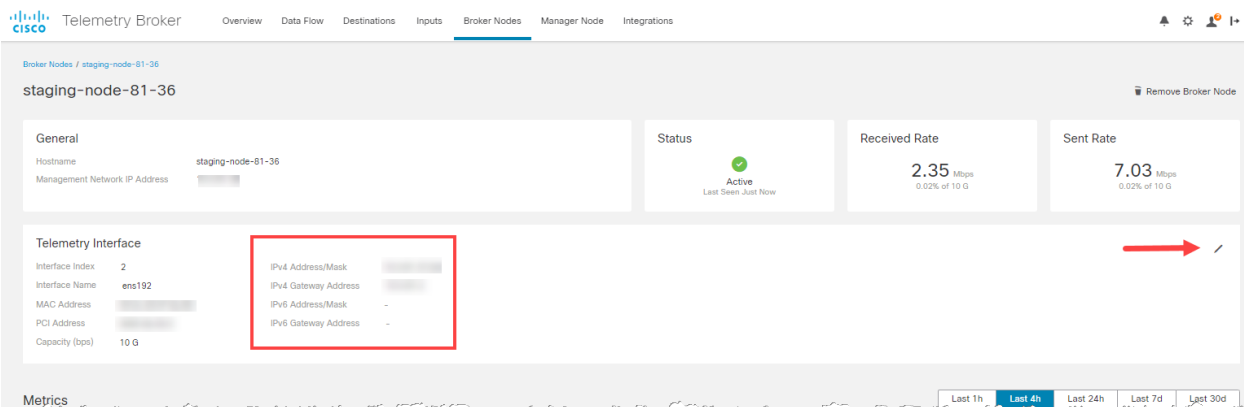
Skriv `exit` för att logga ut.

5. Konfigurera telemetrigränssnittet



Cisco Telemetry Broker är konfigurerad att fungera i pollingläge på en hårdvaruenhet.

1. Logga in på Cisco Telemetry Broker. I en webbläsare anger du hanterarens IP-adress för hanteringsgränssnittet och trycker på **Enter** för att navigera till hanterarens webbgränssnittsloggning.
2. Från huvudmenyn väljer du **Broker-noder**.
3. I tabellen för broker-noder klickar du på tillämplig broker-nod.
4. I avsnittet Telemetrigränssnitt klickar du på ikonen  (**Redigera**) (anges av pilen på följande bild).



The screenshot shows the Cisco Telemetry Broker web interface. The navigation bar includes 'Overview', 'Data Flow', 'Destinations', 'Inputs', 'Broker Nodes', 'Manager Node', and 'Integrations'. The main content area is titled 'Broker Nodes / staging-node-81-36' and 'staging-node-81-36'. It features a 'Remove Broker Node' button and several summary cards: 'General' (Hostname: staging-node-81-36, Management Network IP Address: [redacted]), 'Status' (Active, Last Seen Just Now), 'Received Rate' (2.35 Mbps, 0.02% of 10 G), and 'Sent Rate' (7.03 Mbps, 0.02% of 10 G). Below these is the 'Telemetry Interface' section, which includes fields for Interface Index (2), Interface Name (ens192), MAC Address, PCI Address, Capacity (10 G), IPv4 Address/Mask, IPv4 Gateway Address, IPv6 Address/Mask, and IPv6 Gateway Address. A red box highlights the IPv4 and IPv6 address fields, and a red arrow points to the edit icon (pencil) next to the section title.

5. Konfigurera IP- och Gateway-adresserna (omges av röd kant).

Hantera kluster med hög tillgänglighet

Cisco Telemetry Broker hög tillgänglighet ger hög tillgänglighet för IPv4 och IPv6 virtuella IP-adresser som blir målet för dina indata, vilket säkerställer tillförlitlig leverans av telemetri från indata till destinationer.

För att etablera hög tillgänglighet för broker-noder kan du skapa höga tillgänglighetskluster och tilldela flera broker-noder till var och en. I varje kluster är en broker-nod betecknad *Aktiv*, vilket betyder att den skickar telemetri och betjänar mätvärden till Cisco Telemetry Broker, och resten betecknas *Passiva*, vilket betyder att de inte skickar telemetri eller betjäningssmåt för närvarande. Om en aktiv broker-nod slutar skicka telemetri eller på annat sätt förlorar anslutningen till Telemetry Broker, flyttas en av de passiva broker-noderna upp till aktiv broker-nod och börjar skicka telemetri.

Observera följande om kluster:

- Varje broker-nod kan bara tillhöra ett kluster åt gången.
- För att skapa ett kluster måste du tilldela minst en broker-nod till det klustret.
- Tänk på att om du skapar ett kluster med endast en broker-nod och den här broker-noden misslyckas, är ingen annan broker-nod tillgänglig för att befordras till Aktiv broker-nod. Om alla broker-noder inom ett kluster på liknande sätt misslyckas, kan ingen broker-nod flyttas upp till Aktiv broker-nod. Om en broker-nod misslyckas tar du tillbaka den online så snart som möjligt.
- Du kan inte välja vilken broker-nod som är aktiv i ett givet kluster.
- Om en aktiv broker-nod för en virtuell IP-adress misslyckas, blir en av de passiva broker-noderna i samma kluster den aktiva broker-noden för den virtuella IP-adressen. När den misslyckade broker-noden kommer upp igen förblir den en passiv broker-nod. Om du vill göra den noden aktiv igen måste du göra det manuellt med hjälp av de angivna kommandona i avsnittet [Flytta en VIP till en specifik nod](#) i det här kapitlet.
- Du kan tilldela antingen en virtuell IPv4- eller virtuell IPv6-adress, eller båda, till ett kluster. Telemetry Broker använder denna virtuella IP-adress för att kommunicera med klustret och främja passiva broker-noder till aktiva broker-noder när en aktiv broker-nod förlorar anslutningen till Telemetry Broker.

För information om hur HA-kluster uppdateras under Cisco Telemetry Broker-programuppdateringsprocessen, läser du kapitlet "Programuppdatering" i Cisco Telemetry Broker användarguiden.

VIP:er och routing

Hög tillgänglighet konfigurerar VIP-adress-broker-nodens telemetrinätverksgränssnitt. Observera att gränssnittet för telemetrinätverk på varje broker-nod i klustret *redan måste vara konfigurerad* med en primär IPv4- eller IPv6-IP -adress, samt med en subnätmask och en gateway. Du kan konfigurera dessa i telemetrinätverkets gränssnitt.

Du måste konfigurera IPv4- eller IPv6 VIP IP-adresser så att de finns i samma subnät som de primära IP-adresserna **för telemetrinätverkets gränssnitt** i klustret, eftersom VIP:n också måste finnas i samma subnät. Detta säkerställer korrekt routing via den förkonfigurerade gatewayen och snabb failover.

Om VIP-adresserna inte finns i samma subnät som de primära IP-adresserna för telemetrinätverksgränssnitten, eller om telemetrinätverksgränssnitten inom ett kluster är konfigurerade med olika subnät, är det mycket troligt att hög tillgänglighet inte kommer att fungera.

Hantera kluster

Implementeringen av Cisco Telemetry Broker förlitar sig på två vanliga Linux-paket för att tillhandahålla den underliggande infrastrukturen med hög tillgänglighet:

Corosync: detta är klustermotorn på låg nivå som tillhandahåller den underliggande kommunikationen mellan klusternoder. Det ger också kворum att fatta beslut om rollen för varje nod (Aktiv eller Standby).

Pacemaker: detta är klusterresurshanteraren som hanterar alla relationer mellan maskinerna och applikationerna. Den använder Corosync för att kommunicera.

Visa aktuell klusterstatus

För att se aktuell status för klustret, inklusive status (Offline eller Online) för varje nod och platsen för IPv4 VIP (vip4) och IPv6 VIP (vip6) IP-adressen, utför du följande steg:

1. Logga in som **admin** på någon av broker-noderna i klustret via SSH. Använd lösenordet som angavs under nodinstallationen.
2. Kör kommandot `sudo crm_mon`. Detta visar en vy av de för närvarande konfigurerade attributen i klustret. Det finns mer information om detta kommando [här](#).
3. Avsluta verktyget genom att trycka på **Ctrl+C**.

```
admin@titan-8HIP2JLB: ~
Stack: corosync
Current DC: 10.0.81.31 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Tue Jan 26 16:16:24 2021
Last change: Tue Jan 26 15:45:04 2021 by root via cibadmin on 10.0.81.31

2 nodes configured
1 resource configured

Online: [ 10.0.81.31 10.0.81.32 ]

Active resources:

vip4    (ocf::titan:telemetry-vip):    Started 10.0.81.31
```

Den föregående bilden beskriver ett kluster av två noder, 10.0.81.31 och 10.0.81.32, som båda har statusen *Online*. IPv4 VIP (vip4) körs för närvarande 10.0.81.31. IPv6 VIP (vip6) är inte synlig eftersom den inte har konfigurerats.

Om 10.0.81.31 misslyckades skulle dess status se ut så här:

```
admin@titan-8HIP2JLB: ~
Stack: corosync
Current DC: 10.0.81.32 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Tue Jan 26 16:17:22 2021
Last change: Tue Jan 26 15:45:04 2021 by root via cibadmin on 10.0.81.31

2 nodes configured
1 resource configured

Online: [ 10.0.81.32 ]
OFFLINE: [ 10.0.81.31 ]

Active resources:

vip4    (ocf::titan:telemetry-vip):    Started 10.0.81.32
```

Lägg märke till hur 10.0.81.31 nu visas som *OFFLINE* och vip4 har flyttats till 10.0.81.32.

Visa aktuell klusterkonfiguration

För att se den aktuella konfigurationen av klustret för att verifiera att Corosync och Pacemaker-konfigurationen är korrekt, utför du följande steg:

1. Logga in som **admin** på någon av broker-noderna i klustret via SSH. Använd lösenordet som angavs under nodinstallationen.
2. Kör kommandot `sudo crm configure show`. Detta visar en vy av det för närvarande konfigurerade attributet i klustret. Det finns mer information om detta kommando [här](#).

```
admin@titan-8H1P2JLB: ~  
admin@titan-8H1P2JLB:~$ sudo crm configure show  
node 1: 10.0.81.31  
node 2: 10.0.81.32  
primitive vip4 ocf:titan:telemetry-vip \  
    params ip=10.0.81.63 cidr_netmask=24 nic=eth1 \  
    op monitor interval=5s  
property cib-bootstrap-options: \  
    have-watchdog=false \  
    dc-version=2.0.1-9e909a5bdd \  
    cluster-infrastructure=corosync \  
    cluster-name=debian \  
    stonith-enabled=false \  
    no-quorum-policy=ignore \  
    start-failure-is-fatal=false  
rsc_defaults rsc-options: \  
    resource-stickiness=100  
alert ctb_manager "/opt/titan/compose/bin/cluster_events.py" \  
    to localhost  
admin@titan-8H1P2JLB:~$
```

Aktivera och inaktivera nod-standbyläget

I standbyläget kan noden inte vara värd för de virtuella IPv4- eller IPv6-adresserna.

1. Logga in som **admin** på någon av broker-noderna i klustret via SSH. Använd lösenordet som angavs under nodinstallationen.
2. Kör kommandot `sudo crm node standby 10.0.81.32`. Du kan utelämna nodnamnet om du kör det här kommandot på den noden. Det finns mer information om detta kommando [här](#).
3. Kör kommandot `sudo crm node online 10.0.81.32` för att flytta noden från *Standby*-status. Det finns mer information om kommandot [här](#).

```
admin@titan-8HIP2JLB: ~
Stack: corosync
Current DC: 10.0.81.32 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Tue Jan 26 16:41:49 2021
Last change: Tue Jan 26 16:41:44 2021 by root via crm_attribute on 10.0.81.32

2 nodes configured
1 resource configured

Node 10.0.81.32: standby
Online: [ 10.0.81.31 ]

Active resources:

vip4      (ocf::titan:telemetry-vip):      Started 10.0.81.31
```

Som du märker visar *crm_mon* standby-status för noden 10.0.81.32.

Flytta en VIP till en specifik nod

Du kan stöta på omständigheter där du vill ange vilken nod som kör den virtuella IPv4- eller IPv6-adressen. Om så är fallet slutför du följande steg:

1. Logga in som **admin** på någon av broker-noderna i klustret via SSH. Använd lösenordet som angavs under nodinstallationen.
2. Kör kommandot `sudo crm resource move vip4 10.0.81.32`. Det finns mer information om detta kommando [här](#).
3. Kör kommandot `sudo crm resource unmove vip4` för att se till att VIP:n stannar på den riktade noden, annars kommer VIP:n att flytta tillbaka till noden den var på tidigare (före flytten) vid nästa tillfälle.

Slutför konfigurationen av ditt system

För att slutföra konfigurationen av ditt system ser du följande avsnitt i [Cisco Telemetry Broker-användarhandboken](#):

- Destinationer
- Indata
- Broker-noder

Kontakta kundtjänst

Om du behöver teknisk support gör du något av följande:

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

Tidigare ändringar

Dokumentversion	Publiceringsdatum	Beskrivning
1_0	April 2023	Första versionen.
1_1	maj 2023	Lade till kapitlet "Migrera konfiguration till ett nytt system".

Upphovsrättsinformation

SPECIFIKATIONER OCH INFORMATION AVSEENDE PRODUKTER I DENNA HANDBOK KAN ÄNDRAS UTAN FÖRVARNING. ALLA UTTALANDEN, INFORMATION OCH REKOMMENDATIONER I DENNA HANDBOK ANTAS VARA KORREKTA, MEN PRESENTERAS UTAN NÅGRA SOM HELST GARANTIER, VARKEN UTTALADE ELLER UNDERFÖRSTÅDDA. ANVÄNDARE MÅSTE TA FULLT ANSVAR FÖR TILLÄMPNINGEN AV PRODUKTERNA.

PROGRAMVARULICENSEN OCH DEN BEGRÄNSADE GARANTIN FÖR DEN MEDFÖLJANDE PRODUKTEN FRAMSTÄLLS I DET MEDFÖLJANDE INFORMATIONSPAKETET SOM LEVERERADES MED PRODUKTEN OCH INKLUDERAS MED DENNA REFERENS. OM DU INTE KAN HITTA PROGRAMVARULICENSEN ELLER DEN BEGRÄNSADE GARANTIN KONTAKTAR DU DIN CISCO-REPRESENTANT OCH BER OM EN KOPIA.

Ciscos implementering av TCP-huvudkomprimeringen är en anpassning av ett program som utvecklats av University of California, Berkeley (UCB) som en del av UCB:s offentliga domänversion av UNIX-operativsystemet. Med ensamrätt. Copyright © 1981, Regents of the University of California.

OAKTAT ALLA ANDRA GARANTIER HÄRMED, SÅ LEVERERAS ALLA DOKUMENTFILER OCH PROGRAMVAROR FRÅN DESSA LEVERANTÖRER I BEFINTLIGT SKICK. CISCO OCH OVANNÄMND A LEVERANTÖRER FRÅNSÄGER SIG ALLA GARANTIÅTAGANDEN, BÅDE UTTALADE OCH UNDERFÖRSTÅDDA, INKLUSIVE MEN INTE BEGRÄNSAT TILL SÅDANA SOM RÖR SÄLJBARHET, LÄMPLIGHET FÖR ETT VISST ÄNDAMÅL OCH ICKE-ÖVERTRÄDELSE AV ANDRAS RÄTTIGHETER ELLER SOM UPPSTÅR TILL FÖLJD AV HANDLANDE, BRUK ELLER HANDELSPRAXIS.

UNDER INGA OMSTÄNDIGHETER SKA CISCO ELLER DESS LEVERANTÖRER ANSES ANSVARIGA FÖR INDIREKTA SKADOR, OFÖRUTSEDDA SKADOR ELLER FÖLJDSKADOR INKLUSIVE, MEN EJ BEGRÄNSAT TILL UTEBLIVEN VINST ELLER FÖRLUSTER ELLER SKADADE DATA SOM UPPSTÅR PÅ GRUND AV ANVÄNDNINGEN ELLER UNDERLÅTENHETEN ATT ANVÄNDA DENNA HANDBOK, ÄVEN OM CISCO ELLER DESS LEVERANTÖRER HAR UNDERRÄTTATS OM RISKEN FÖR SÅDANA SKADOR.

Alla IP-adresser och telefonnummer som används i detta dokument är inte avsedda att vara verkliga adresser och telefonnummer. Alla exempel, kommandovisningsutdata, nätverkstopologidiagram och andra figurer som ingår i dokumentet visas endast i illustrativt syfte. All användning av faktiska IP-adresser eller telefonnummer i illustrativa material är oavsiktlig och endast en tillfällighet.

Alla utskrivna kopior och dubbla mjuka kopior av detta dokument anses vara okontrollerade. Se den aktuella onlineversionen för den senaste versionen.

Cisco har över 200 kontor runt om i världen. Adresser och telefonnummer finns på Ciscos webbplats på <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>.

Cisco och Cisco-logotypen är varumärken eller registrerade varumärken som tillhör Cisco och/eller dess dotterbolag i USA och i andra länder. Gå till denna webbadress för att se en lista över Ciscos varumärken: <https://www.cisco.com/go/trademarks>.

Tredjepartsvarumärken tillhör sina respektive ägare. Användningen av ordet "partner" avser inte en partnerrelation mellan Cisco och något annat företag. (1721R)