Configurare Prime Collaboration Assurance (PCA) - Diagnostica conferenza

Sommario

Introduzione

In questo documento viene descritto come configurare e configurare l'installazione di Diagnostica conferenza in Prime Collaboration Assurance (PCA) per il monitoraggio proattivo delle statistiche relative a videoconferenze.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso amministratore di Gestione chiamate
- Accesso PCA
- Il tuo Telepresence Monitor Server (TMS)

- Credenziali di base/Expressway, se applicabili

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni 11.x - 12.x dell'APC.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Prime Collaboration 11.x supporta questi tipi di visibilità:

- Visibilità completa: è supportato il rilevamento delle chiamate con l'utilizzo di feedback JTAPI/HTTP e informazioni di monitoraggio in tempo reale, quali statistiche sulle conferenze e informazioni sulle conferenze.
- Visibilità limitata: viene eseguito il rilevamento automatico delle chiamate con l'utilizzo del feedback JTAPI/HTTP, ma le informazioni di monitoraggio in tempo reale, quali le statistiche delle conferenze e le informazioni sulle conferenze, non sono supportate. Gli endpoint con visibilità limitata sono indicati da un'icona semivuota nella topologia della conferenza.

Cisco Prime Collaboration 12.x supporta questi tipi di visibilità:

- Visibilità completa: è supportato il rilevamento delle chiamate con l'utilizzo di feedback JTAPI/HTTP e informazioni di monitoraggio in tempo reale, quali statistiche sulle conferenze e informazioni sulle conferenze.
- Nessuna visibilità - Non è supportato il rilevamento delle chiamate con feedback JTAPI/HTTP e informazioni di monitoraggio in tempo reale. Questi endpoint vengono visualizzati nella pagina Monitoraggio conferenza con un'icona completamente inattiva.

Limitazione degli endpoint impostata su Visibilità limitata o completa per ogni OAV

- Small Open Virtualization Archive (OVA) supporta fino a 500 endpoint
- OAV medio supporta fino a 1000 endpoint
- Ampio supporto di OAV fino a 1800 endpoint
- OVA molto grandi supporta fino a 2000 endpoint

Un elenco di dispositivi supportati per PCA in relazione alle conferenze e alle sessioni supportate è come mostrato nella tabella immagine qui.

Session Scenarios

The various session scenarios that are monitored in Cisco Prime Collaboration are as follows:

Table 1 Session Scenarios

Session Classification	Session Type	Session Structure	Session Topology Elements
Cisco Unified CM *intracluster* and *intercluster* sessions	Ad hoc,Scheduled	Point-to-point	Cisco TelePresence System 500, 1000, 3000, TX9000 Series.
Cisco Unified CM *intracluster* and *intercluster* sessions	Ad hoc,ScheduledStatic	Multipoint	Cisco TelePresence System 500, 1000, 3000, TX9000 Series, and CTMS.
Cisco VCS *intracluster* and *intercluster* sessions	Ad hoc,Scheduled	Point-to-point	Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20, Cisco Cius, and Cisco Jabber. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Cisco VCS *intracluster* and *intercluster* sessions (with MCU)	Ad hoc,ScheduledPermanent (displayed as static)	Multipoint	Cisco C series, EX Series, Cisco MCU, Cisco MSE[1], or Cisco TelePresence Server. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Cisco VCS *intracluster* and *intercluster* sessions (without MCU)	Ad hoc,Scheduled	Multisite	Cisco C series, EX Series, Cisco MX, Cisco MXP Series, Cisco IP Video Phone E20. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Sessions between Cisco Unified CM and Cisco VCS clusters [2]	Ad hoc	Point-to-pointMultipoint	• Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20 • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • Cisco TelePresence Server • IX 5000 series TelePresence endpoints
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) *intracluster* sessions[3]	Ad hoc	Point-to-point	• Cisco C series, EX Series, Cisco MX series • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • IX 5000 series TelePresence endpoints
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) *intracluster* sessions	Ad hoc,Scheduled **Note** Scheduler must be CTS-Manager 1.7, 1.8, or 1.9.	Multipoint	• Cisco C series, EX Series, Cisco MX series, Cisco IP Video Phone E20 • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • CTMS 1.8 or Cisco TelePresence Server
Sessions outside the enterprise firewall – Cisco VCS Expressway	Ad hocPermanent (displayed as static)	Point-to-point,Multipoint, Multisite	• Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20 • Cisco MCU or Cisco TelePresence Server • Cisco VCS Control and Cisco VCS Expressway

Endpoints in a call (with an MCU in the call) work as a conferencing bridge in Cisco Unified CM.	Ad hoc	Point-to-point When a call is put in a conference mode or when merged with another call, it becomes Multipoint. The session does not show the MCU. When the first participant leaves the call, the session shows it is connected to the MCU, while the second and third participants continue in the same call as a point-to-point call. **Note** This scenario is applicable when in-built video bridge capability is not present in the endpoint.	Multipoint conferencing devices and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.
Sessions between MRA endpoints- Cisco Jabber or Cisco TelePresence MX Series or Cisco TelePresence System EX Series or Cisco TelePresence SX Series	Ad hoc, Scheduled	Point-to-point,Multipoint, Multisite **Note** Cisco Prime Collaboration does not monitor a Multisite session where an MRA endpoint acts as a conference bridge.	Cisco Jabber, Cisco TelePresence MX Series, Cisco TelePresence System EX Series, and Cisco TelePresence SX Series.

[1] The codian software must be running on Cisco MSE.
[2] This scenario is supported on CTS 1.7.4, and TC 4.1 to 7.0.
[3] The troubleshooting workflow is supported on TC 4.2, 5.0, and above.

Note
- Cisco Cius and Cisco Jabber devices support only ad hoc sessions.

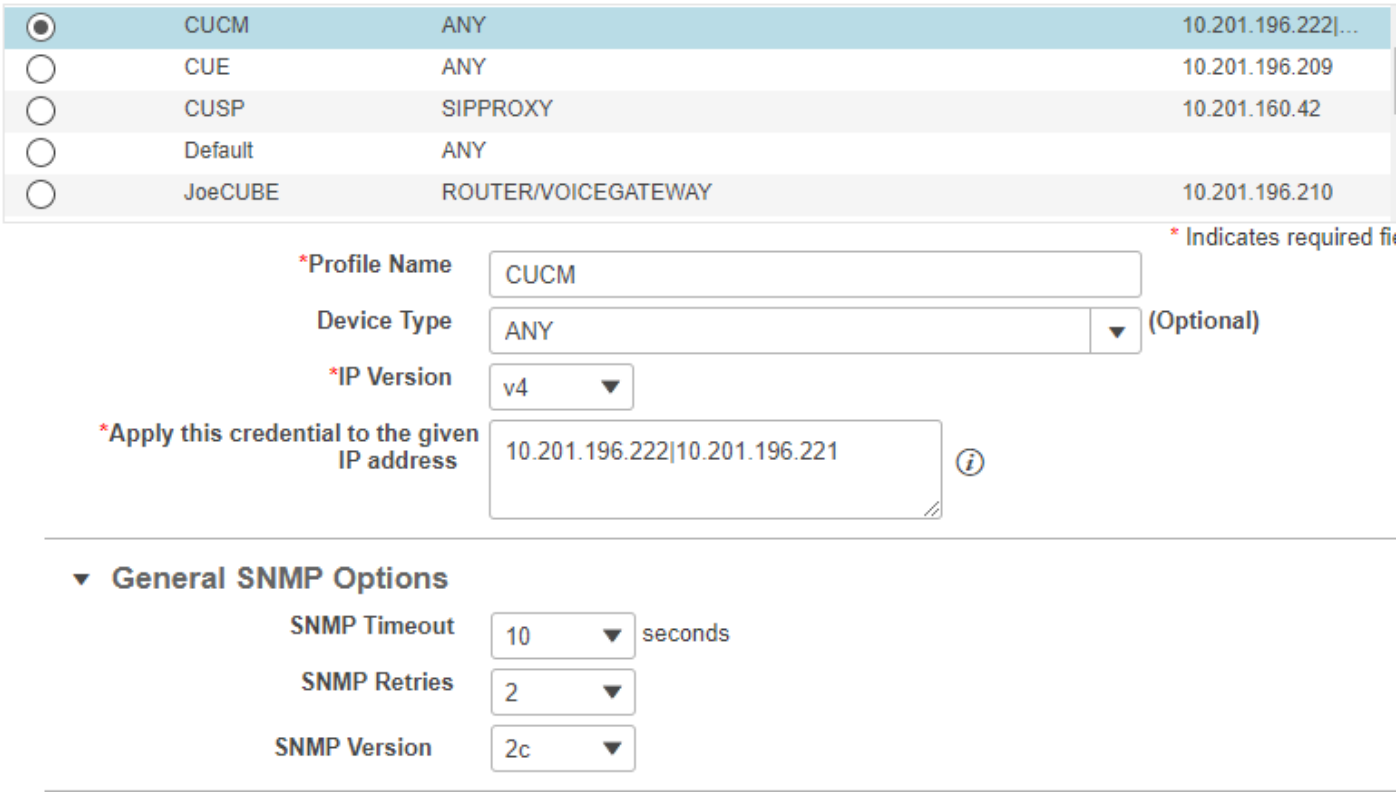
Configurazione

Scenario 1. Conferenza con endpoint video registrati in Call Manager

Passaggio 1. Innanzitutto è necessario verificare che i Call Manager siano in stato Managed.

Passare a Magazzino > Gestione articoli > Gestisci credenziali > Crea un profilo per il cluster Gestione chiamate.

Nota: ricordare che ogni profilo di credenziali utilizza le stesse credenziali per ogni IP elencato nel profilo. Pertanto, se si elencano il server di pubblicazione del gestore delle chiamate e il sottoscrittore all'interno dello stesso profilo di credenziali, verranno utilizzate le stesse credenziali per individuare entrambi gli indirizzi IP. Se nella configurazione è presente un conduttore, individuarlo prima di tutto e quindi utilizzare Cisco Call Manager, come mostrato nell'immagine.



Passaggio 2. Assicurarsi di aver impostato le credenziali HTTP (Hypertext Transfer Protocol), SNMP (Simple Name Management Protocol) e JTAPI (Java Telephony API)

Inoltre, è necessario abilitare il servizio Cisco Computer Telephony Integration (CTI) in Call Manager Serviceability.

Configurazione di Cisco Unified Communications Manager

Abilita HTTP

Non è necessario creare un nuovo utente se si desidera consentire a Cisco Prime Collaboration di utilizzare le credenziali di amministratore per eseguire l'accesso. In alternativa, se si desidera consentire a Cisco Prime Collaboration Manager di utilizzare le credenziali corrette per accedere a Cisco Unified Communications Manager, è necessario creare un nuovo gruppo di utenti HTTP e un utente corrispondente che Cisco Prime Collaboration può utilizzare per comunicare.

Per creare un utente, attenersi alla procedura descritta di seguito.

Passaggio 1. Accedere all'interfaccia Web di amministrazione di Cisco Unified CM con l'account amministratore.

Passaggio 2. Creare un gruppo di utenti con privilegi sufficienti. Passare a Gestione utenti>Impostazioni utente>Gruppo di controllo di accesso e creare un nuovo gruppo di utenti con un nome appropriato, PC_HTTP_Users in questo caso. A questo punto, selezionare Salva.

Passaggio 3. Passare a Gestione utente>Impostazioni utente>Gruppo di controllo di accesso e selezionare Trova. Individuare il gruppo definito e fare clic sull'icona a destra.

Passaggio 4. Selezionare Assegna ruolo a raggruppamento e selezionare i ruoli seguenti:

- Accesso API AXL standard
- Utenti amministratori CCM standard
- Amministrazione standard di SERVICEABILITY

Passaggio 5. Fare clic su Save (Salva).

Passaggio 6. Dal menu principale, passare aGestione utenti>Utenti applicazioni>Crea un nuovo utente.

Specificare una password appropriata nella pagina Configurazione utente applicazione. È possibile selezionare solo alcuni tipi di dispositivi dall'area di testo Dispositivi disponibili o consentire a Cisco Prime Collaboration di monitorare tutti i dispositivi

Passaggio 7. Nella sezione Informazioni autorizzazione, selezionare Aggiungi a gruppo utenti e selezionare il gruppo creato nel passaggio 1 (ad esempio, PC_HTTP_Users).

Passaggio 8. Fare clic su Salva. La pagina viene aggiornata e vengono visualizzati i privilegi appropriati.

Abilitazione SNMP

Per impostazione predefinita, il protocollo SNMP non è abilitato in Cisco Unified Communications Manager.

Per abilitare il protocollo SNMP:

Passaggio 1. Accedere alla visualizzazione Cisco Unified Servicability dall'interfaccia utente Web di Cisco Unified Communications Manager.

Passaggio 2. Selezionare Strumenti > Attivazione servizio.

Passaggio 3. Selezionare Server di pubblicazione.

Passaggio 4. Passare a Prestazioni > Servizi di monitoraggio e selezionare la casella di controllo per il servizio SNMP di Cisco Call Manager.

Passaggio 5. Selezionare Save (Salva) nella parte inferiore dello schermo.

Per creare una stringa della community SNMP:

Passaggio 1. Accedere a Cisco Unified ServiceabilityVisualizzare l'interfaccia utente Web di Cisco Unified Communications Manager.

Passaggio 2. Dal menu principale nella vista Cisco Unified Serviceability, selezionare SNMP > v1/v2c > Community String.

Passaggio 3. Selezionare un server e fare clic su Trova.
Se la stringa della community è già definita, il nome della stringa della community viene

visualizzato nei risultati della ricerca.

Passaggio 4. Fare clic su Aggiungi nuovo per aggiungere una nuova stringa se non vengono visualizzati risultati.

Passaggio 5. Specificare le informazioni SNMP richieste e salvare la configurazione.

Nota: è necessario solo l'accesso in sola lettura (RO, Read Only SNMP).

Avvia servizio CTI

Eseguire la procedura per il nodo Cisco Unified Communications Manager desiderato. È preferibile impostarlo su due nodi.

Passaggio 1. Accedere a Cisco Unified Serviceability, visualizzata nell'interfaccia utente grafica di Cisco Unified Communications Manager.

Passaggio 2. Selezionare Strumenti > Attivazione servizio.

Passaggio 3. Selezionare un server dall'elenco a discesa.

Passaggio 4. Dalla sezione CM Services, selezionare la casella di controllo Cisco CTI Manager.

Passaggio 5. Selezionare Save (Salva) nella parte superiore dello schermo

Crea utente applicazione per controllo CTI APC (utente JTAPI)

JTAPI viene utilizzato per recuperare le informazioni sullo stato della sessione dal dispositivo. È necessario creare un utente applicazione per il controllo CTI nel processore chiamate con l'autorizzazione necessaria per ricevere eventi JTAPI sugli endpoint. Prime Collaboration gestisce più cluster di processori di chiamata. È necessario verificare che gli ID cluster siano univoci. Creare un nuovo utente dell'applicazione per consentire a Cisco Prime Collaboration di ottenere le informazioni richieste.

Per creare un nuovo utente dell'applicazione JTAPI, effettuare le operazioni riportate di seguito.

Passaggio 1. Accedere all'interfaccia Web di amministrazione di Cisco Unified CM utilizzando l'account amministratore.

Passaggio 2. Creare un gruppo di utenti con privilegi sufficienti. Passare a Gestione utenti>Impostazioni utente>Gruppo di controllo di accesso e creare un nuovo gruppo di utenti con un nome appropriato, PC_HTTP_Users in questo caso. A questo punto, selezionare Salva.

Passaggio 3. Scegliere Gestione utente>Impostazioni utente>Gruppo di controllo di accesso e fare clic su Trova. Individuare il gruppo definito e selezionare l'icona a destra.

Passaggio 4. Fare clic su Assegna ruolo a raggruppamento e selezionare i ruoli seguenti:

- CTI standard per il monitoraggio delle chiamate
- CTI standard abilitata
- CTI standard per il controllo dei telefoni che supportano Connected Xfer e conf

Passaggio 5. Selezionare Salva.

Passaggio 6. Dal menu principale, passare aGestione utenti>Utenti applicazioni>Crea un nuovo utente.
Specificare una password appropriata nella pagina Configurazione utente applicazione. È possibile selezionare un determinato tipo di dispositivo dall'area di testo Dispositivi disponibili o consentire a Cisco Prime Collaboration di monitorare tutti i dispositivi.

Nota: la password non deve contenere un punto e virgola (;) o uguale (=).

Passaggio 7. Nella sezione Informazioni autorizzazione selezionare Aggiungi a gruppo di controllo di accesso e selezionare il gruppo creato nel passaggio 1, ad esempio PC_HTTP_Users.

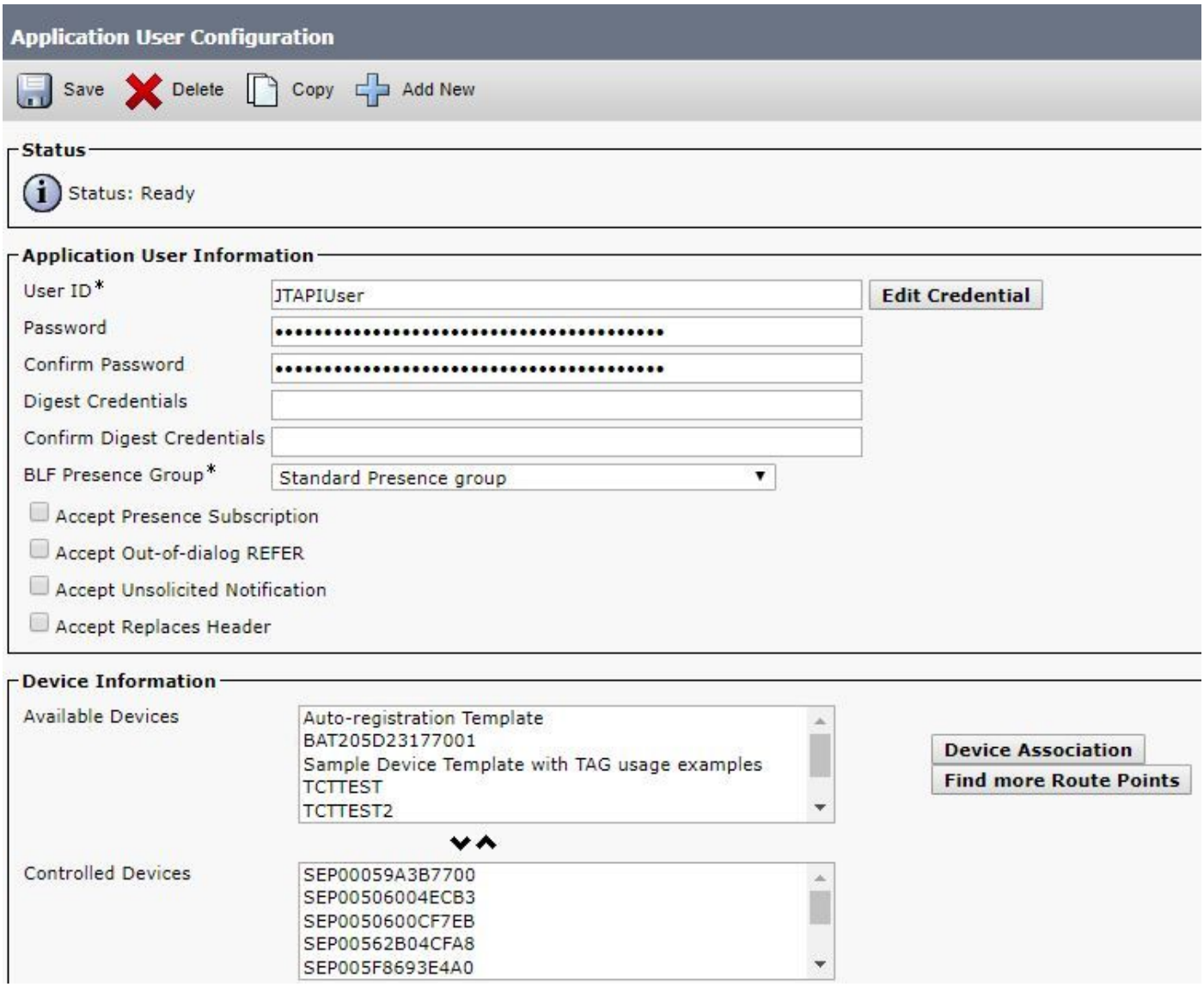
Passaggio 8. Fare clic su Salva. La pagina viene aggiornata e vengono visualizzati i privilegi appropriati.

Nota: se il gestore chiamate è stato gestito prima dell'aggiunta dell'utente JTAPI, assicurarsi che l'utente JTAPI sia stato aggiunto nel profilo credenziali per il gestore chiamate e individuarlo nuovamente.

Continuato dallo scenario 1. Passaggi:

Passaggio 3. Passare all'utente dell'applicazione JTAPI di Gestione chiamate creato e spostare gli endpoint supportati da Dispositivi disponibili a Dispositivi controllati.

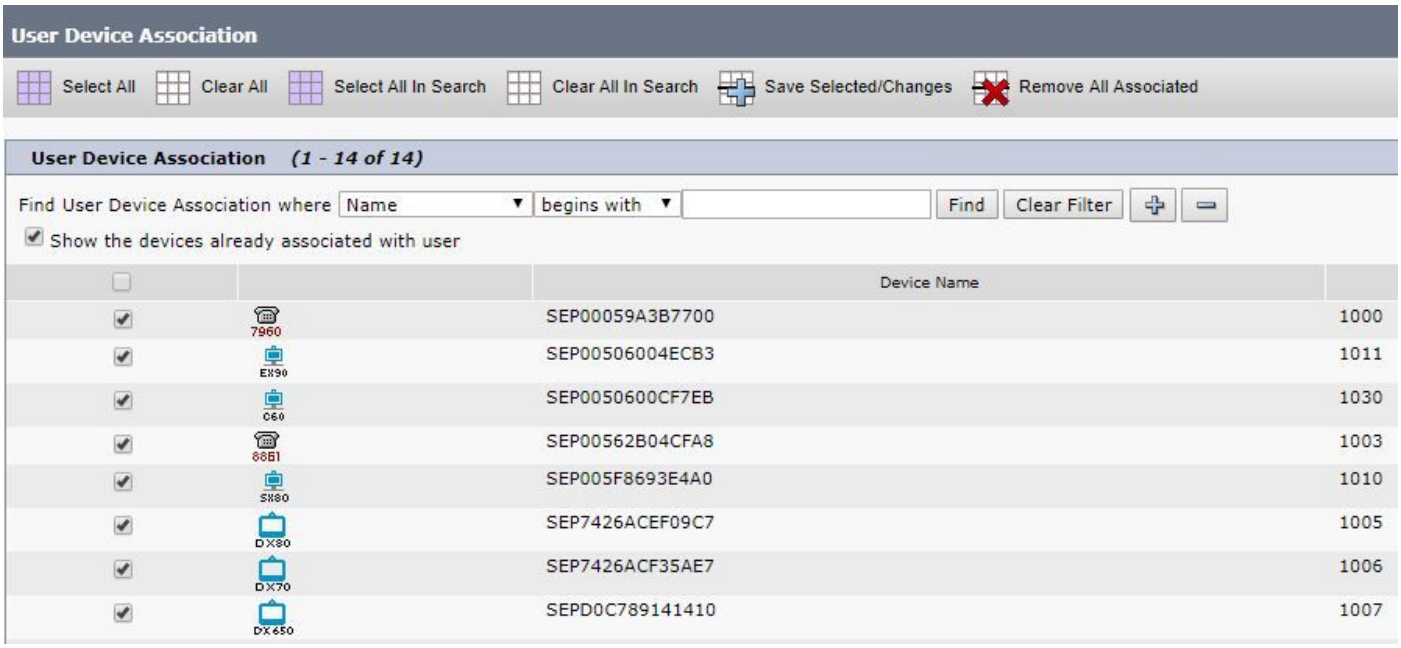
A tale scopo, è possibile utilizzare la funzione Device Association, come illustrato nell'immagine.



Se si fa riferimento alla limitazione di Endpoints Impostato su Limitato o Visibilità completa per OAV, è possibile verificare la quantità di dispositivi aggiunti alle dimensioni degli OAV.

In questa schermata è possibile filtrare i dispositivi in base al nome, alla descrizione o al numero di directory per gestire e filtrare i dispositivi, come mostrato nell'immagine.

È utile annotare questi dispositivi così come sono stati aggiunti al Passaggio 7.



Accertarsi inoltre che vengano aggiunti i ruoli utente corretti per questo utente JTAPI:

- CTI standard per il monitoraggio delle chiamate
- CTI standard abilitata
- La CTI standard permette il controllo dei telefoni che supportano Connected Xfer e conf, come mostrato nell'immagine.

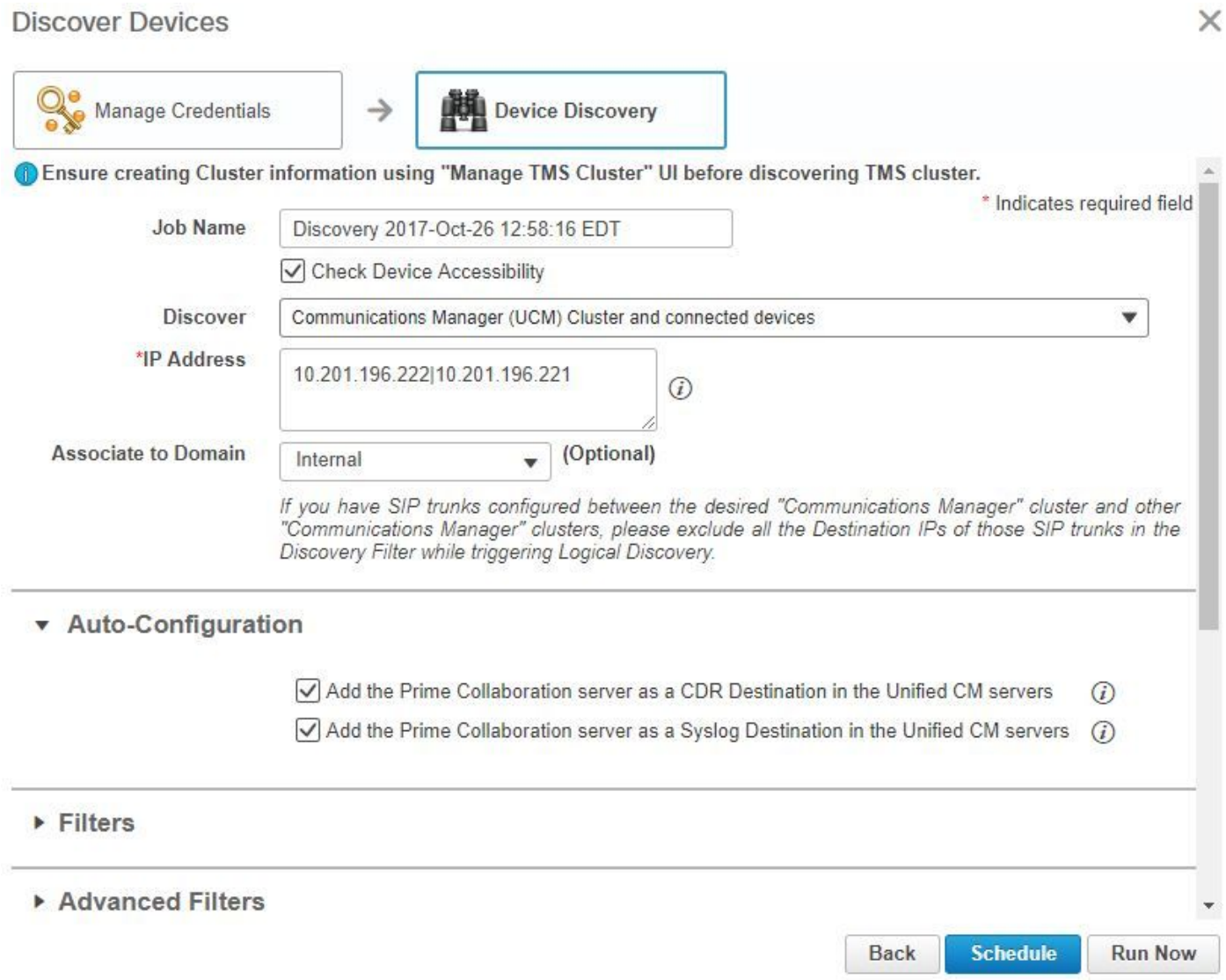
Per un elenco dei dispositivi supportati per PCA, in relazione alle conferenze e alle sessioni supportate, fare riferimento alla sezione Informazioni di base.

Nota: verificare inoltre che la casella di controllo Consenti controllo della periferica da CTI sia selezionata per le periferiche controllate dall'utente dell'applicazione CTI in Informazioni periferica, come illustrato nell'immagine.

Nota: prima di procedere, è importante notare che se gli endpoint sono registrati in Call

Manager e Call Manager è integrato con VCS/TMS, è necessario prima individuare il proprio VCS/TMS, quindi individuare per ultimo il Call Manager. In questo modo, dal punto di vista dell'inventario, tutta l'infrastruttura viene mappata alla posizione corretta. Inoltre, quando si individua il software VCS/TMS, assicurarsi di modificare la scheda di individuazione predefinita sul rispettivo dispositivo di TMS/VCS o Call Manager.

Passaggio 4. Successivamente, in APCA, selezionare Device Discovery (Rilevamento periferiche) e immettere gli indirizzi IP dei Call Manager, selezionare le due caselle di controllo Auto-Configuration (Configurazione automatica) e selezionare Run Now (Esegui ora) come mostrato nell'immagine.



Passaggio 5. Dopo che i Call Manager sono in stato Managed, procedere al passo 6.

Nota: se il Call Manager non è in uno stato gestito, nella maggior parte dei casi è dovuto a HTTP o SNMP. In caso sia necessaria ulteriore assistenza, aprire una richiesta TAC per ottenere il Call Manager in uno stato gestito.

Passaggio 6. Passare a Inventario > Programma magazzino > Programma individuazione dati

cluster e selezionare Esegui ora.

Nota: questo valore dipende dal numero di dispositivi registrati/non registrati di cui si dispone. Questo processo può richiedere da pochi minuti ad alcune ore. Aggiornare la pagina per controllare l'intera giornata. In questo modo, inoltre, viene eseguito il mapping del cluster di Gestione chiamate e vengono recuperati tutti gli endpoint. Al termine, procedere al passaggio successivo.

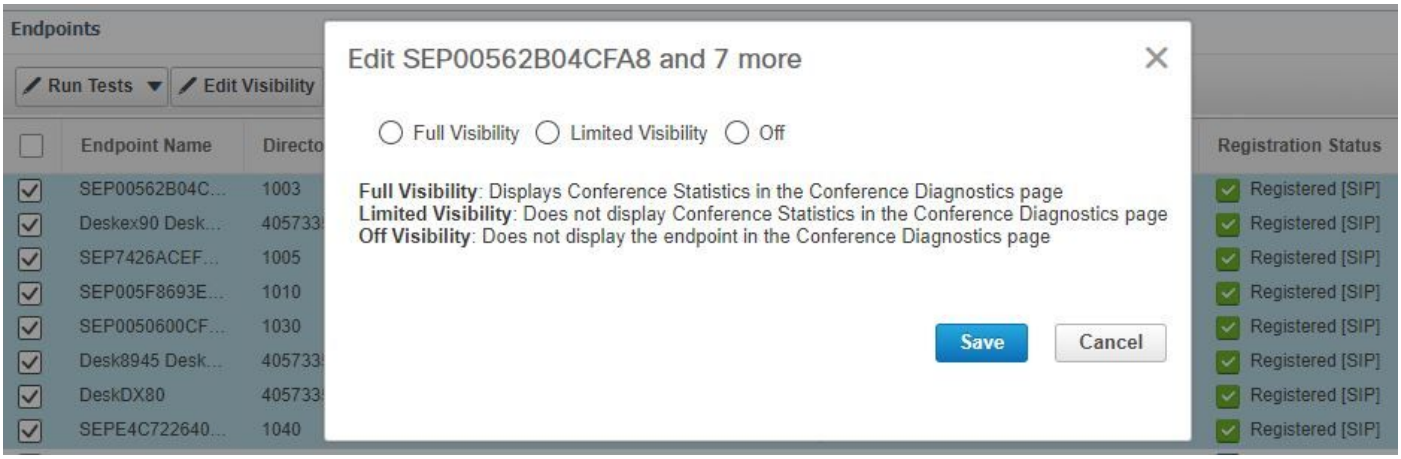
Nota: è importante indicare nell'inventario PCA se esistono endpoint in cui si desidera disporre di statistiche di conferenza supportate. Assicurarsi che siano ben gestiti per i report e tutte le statistiche, in modo da mostrare le informazioni corrette.

Passaggio 7. Passare a Diagnosi > Diagnostica endpoint.

Per ottenere statistiche aggiornate per gli endpoint della conferenza, è necessario impostare la relativa visibilità al livello massimo consentito dal sistema.

Selezionare tutti gli endpoint che si desidera monitorare in Diagnostica conferenza, quindi fare clic su Modifica visibilità e selezionare Visibilità completa come mostrato nell'immagine.

La visibilità limitata mostra solo il dispositivo all'interno della topologia, ma non fornisce statistiche e non è in grado di recuperare gli allarmi applicabili per i dispositivi correlati a Diagnostica conferenza.

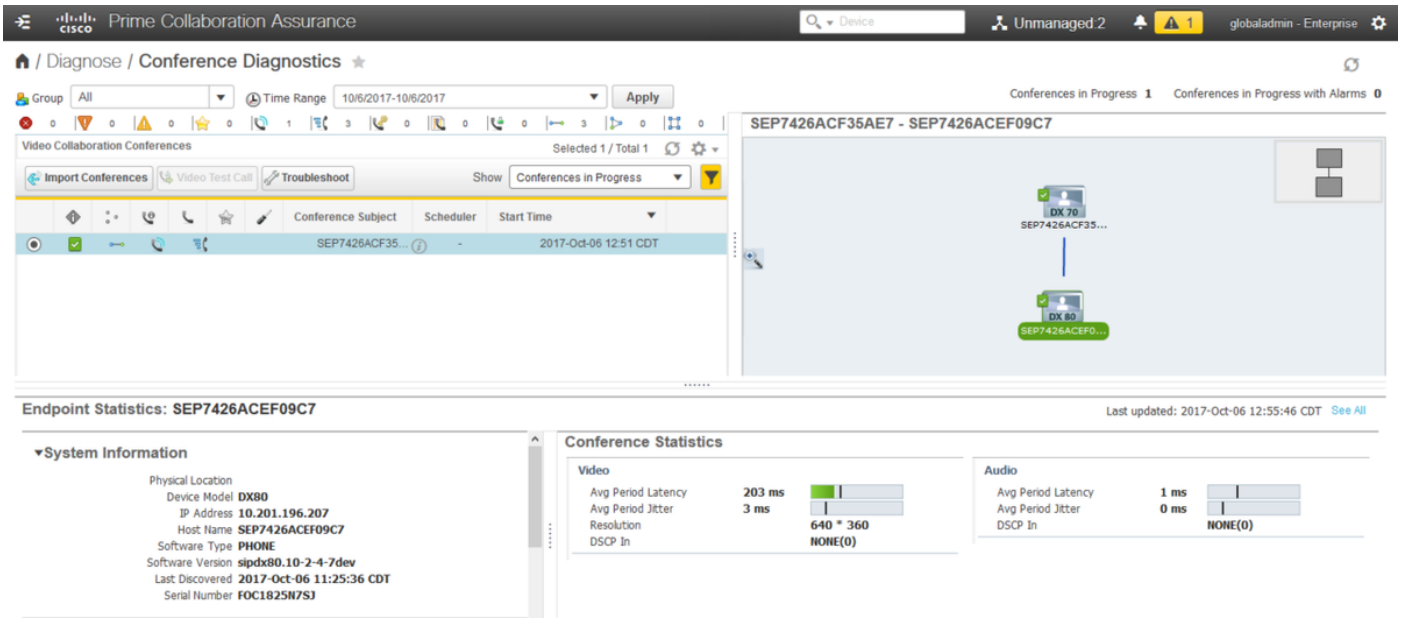


The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
• CTS 500, 1000, and 3000 Series • Cisco Codec • Cisco TelePresence SX20 • Cisco TelePresence MXP Series • Cisco IP Video Phone E20	Full	Full
• Cisco Jabber Video for TelePresence (Movi) • Polycom	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
• Cisco SX80 and Cisco SX10 • • Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: • Cisco Jabber • Cisco TelePresence MX Series • Cisco TelePresence System EX Series • Cisco TelePresence System SX Series	Limited	Limited

Nota: se si selezionano, ad esempio, 10 endpoint e si seleziona Visibilità completa, viene selezionato il livello più alto di visibilità per dispositivo.

Passaggio 8. Per eseguire il test, selezionare Diagnosi > Diagnostica conferenza e viene visualizzato Conferma in corso o Completata, come mostrato nell'immagine.



In queste conferenze è possibile visualizzare la media di perdita di pacchetti, latenza e jitter per le chiamate audio e video.

Ottenere inoltre una topologia della sessione e dei dispositivi interessati.

Attualmente, Diagnostica conferenza estrae le informazioni in base al DN e, se l'ambiente dispone di DN condivisi, Risoluzione problemi compatibilità programmi recupera il primo DN ricevuto per la conferenza.

Allarmi correlati a conferenze

Per Diagnostica conferenza è possibile ricevere tre diversi allarmi per ogni sessione e impostare le relative soglie:

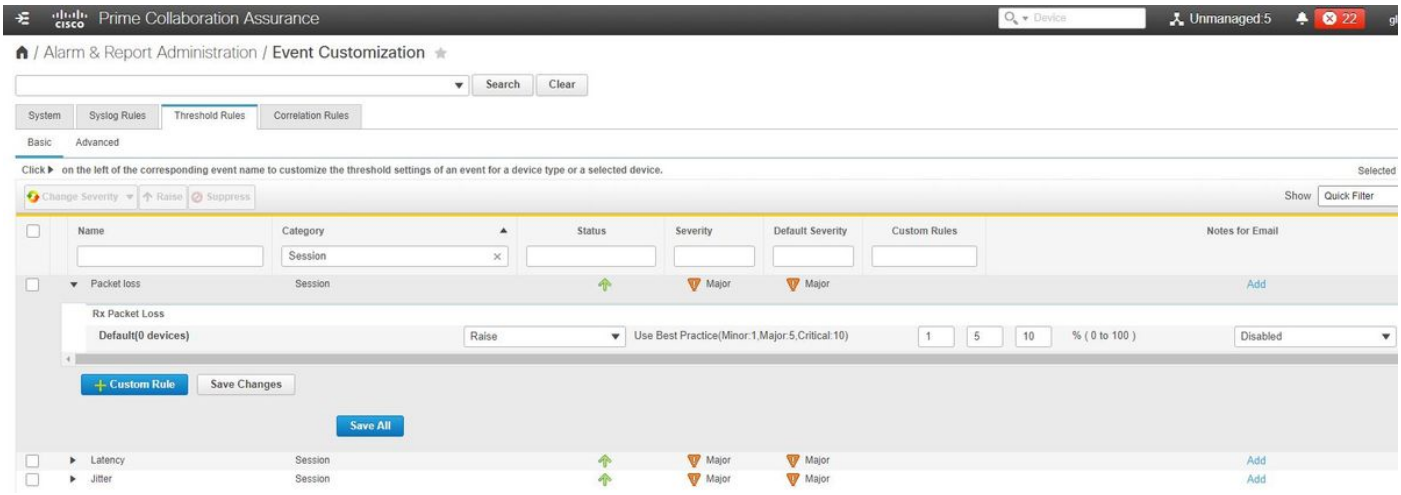
- La perdita di pacchetti
- Latenza
- Variazione

Per ciascuno di questi, è possibile modificare la soglia predefinita, sopprimerla o definire quali dispositivi si desidera associare a questo allarme.

Passaggio 1. Passare a Amministrazione avvisi e report > Personalizzazione evento.

Passaggio 2. Selezionare Regole di soglia e assicurarsi di aver selezionato Base.

Passaggio 3. Scorrere verso il basso o filtrare verso destra per la categoria Sessione con nome come mostrato nell'immagine.



Passaggio 4. Selezionare la freccia dell'elenco a discesa accanto all'avviso. È possibile modificare le percentuali Minore, Maggiore o Critica per Perdita pacchetto, Instabilità o Latenza.

Passaggio 5. Se si desidera eseguire la compressione, passare a Aumenta (Raise) a Sopprimi (Surpress).

Passaggio 6. Se si desidera definire gli endpoint associati all'allarme, è possibile selezionare Regola personalizzata.

Passaggio 7. Quindi, selezionare il Tipo di dispositivo > Seleziona tutti i dispositivi o i dispositivi selezionabili che si desidera utilizzare per questo allarme e fare clic su Salva.

Report correlati a conferenze

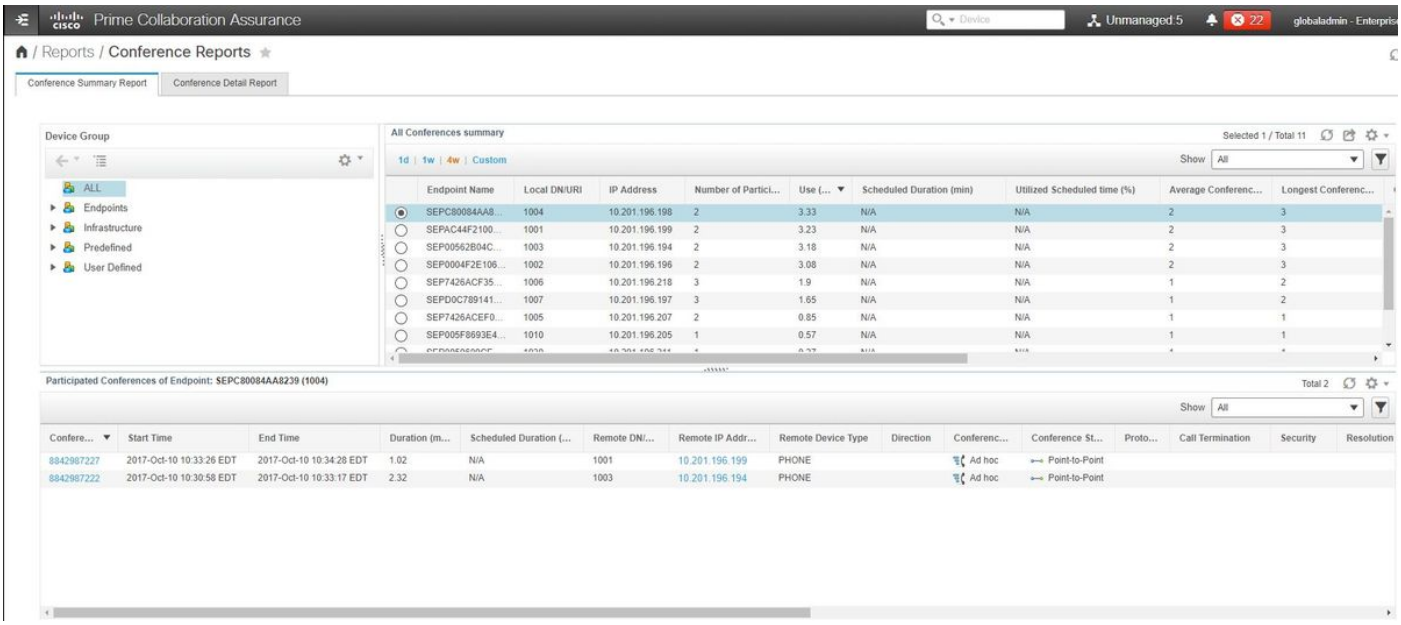
Per i rapporti di Diagnostica conferenza è possibile recuperarli e visualizzarli.

Esistono due rapporti:

- Rapporti conferenza
- Report Degli Endpoint Telepresence

Per i report delle conferenze, è possibile visualizzare un elenco di tutte le conferenze in un intervallo di tempo compreso tra una e quattro settimane oppure un periodo di tempo personalizzato in base alle esigenze.

Passaggio 1. Passare a Rapporti > Rapporti conferenza come mostrato nell'immagine.



Rapporti di riepilogo conferenza

Questo report fornisce una visualizzazione di ogni endpoint selezionato come visibilità limitata/completa e delle relative conferenze.

Le statistiche mostrate sono:

- Utilizzo medio conferenza
- Allarmi collegati alla conferenza
- Perdita media di pacchetti, jitter e latenza
- Conferenza più lunga

In questo modo è possibile ottenere una visione granulare dei problemi all'interno della rete voce/video per determinare quali endpoint presentano il maggior numero di problemi.

Inoltre, è possibile utilizzare la larghezza di banda in base all'utilizzo.

Scheda Rapporto dettagli conferenza

Se viene visualizzato un avviso relativo a una conferenza, è possibile passare alla scheda Rapporto dettagli conferenza.

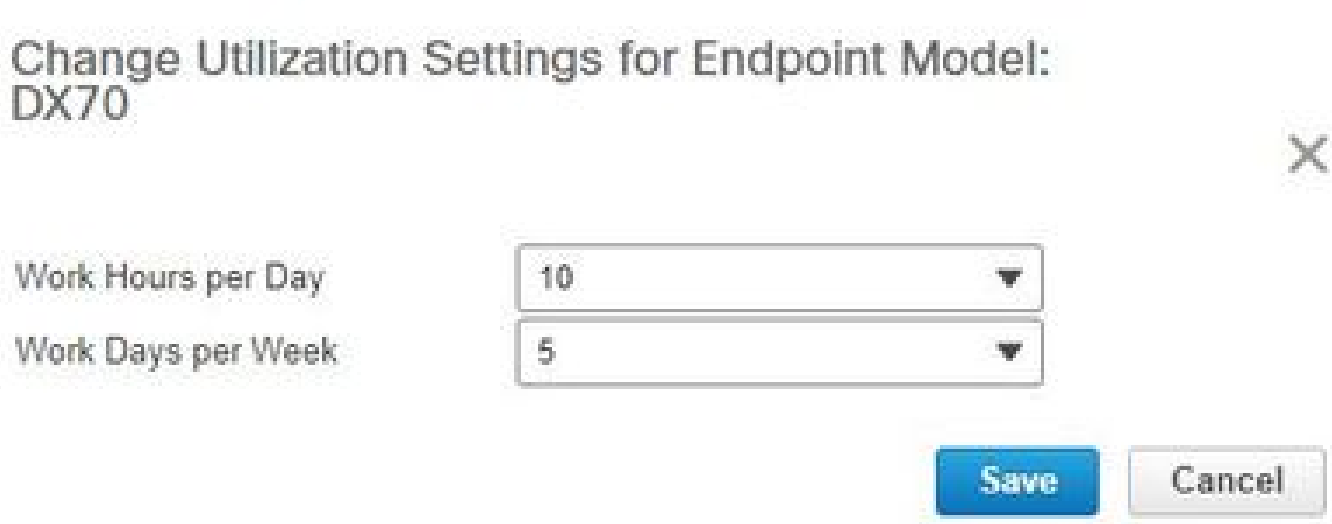
Dopo aver selezionato la conferenza, è possibile modificarla per trovare il nome dell'endpoint, la versione del software e altri dettagli utili.

Per Telepresence Endpoint Reports, è possibile visualizzare per endpoint:

- Numero di conferenze effettuate dal dispositivo
- Percentuale di utilizzo
- Modello endpoint
- Utilizzo

Inoltre, potete modificare i parametri di utilizzo mediante la scheda Cambia utilizzo (Change

Utilization), come mostrato nell'immagine.



In questo modo vengono impostati i parametri per il dispositivo in modo che il sistema possa conoscere la percentuale da visualizzare dall'utilizzo.

Nel rapporto Riepilogo endpoint non visualizzati vengono visualizzati gli endpoint per i quali le conferenze pianificate non sono state eseguite.

In questo grafico è inoltre possibile visualizzare l'endpoint, il numero totale di conferenze pianificate e il numero di conferenze effettivamente avvenute e non mostrate.

Videochiamata di test di conferenza

È possibile creare chiamate di test video point-to-point tra due endpoint video in stato gestito, per verificare la rete. È possibile visualizzare eventi e allarmi, statistiche delle sessioni, statistiche degli endpoint e topologia di rete con statistiche simili ad altre chiamate. Per questa chiamata sono supportati solo i codec delle serie CTS, C ed EX.

Inoltre, può essere utilizzato per verificare che tutto funzioni correttamente con la diagnostica della conferenza.

Prerequisiti

- Questa funzione non è supportata per la serie di codec E20.
- Per utilizzare questa funzionalità, è necessario aggiungere le credenziali CLI per gli endpoint.
- Verificare che gli endpoint siano registrati e che JTAPI sia abilitato per gli endpoint (se sono registrati in Unified CM).
- La funzione Video Test Call non è disponibile se Cisco Prime Collaboration è stato distribuito in modalità MSP.

Passaggio 1. Passare a Diagnosi > Diagnostica endpoint.

Passaggio 2. Selezionare due endpoint applicabili in base ai prerequisiti indicati.

Passaggio 3. Selezionare Esegui test > Videochiamata di test.

Passaggio 4. È possibile pianificare l'esecuzione di Video Test Call adesso o in base a una pianificazione di ripetizione delle occorrenze.

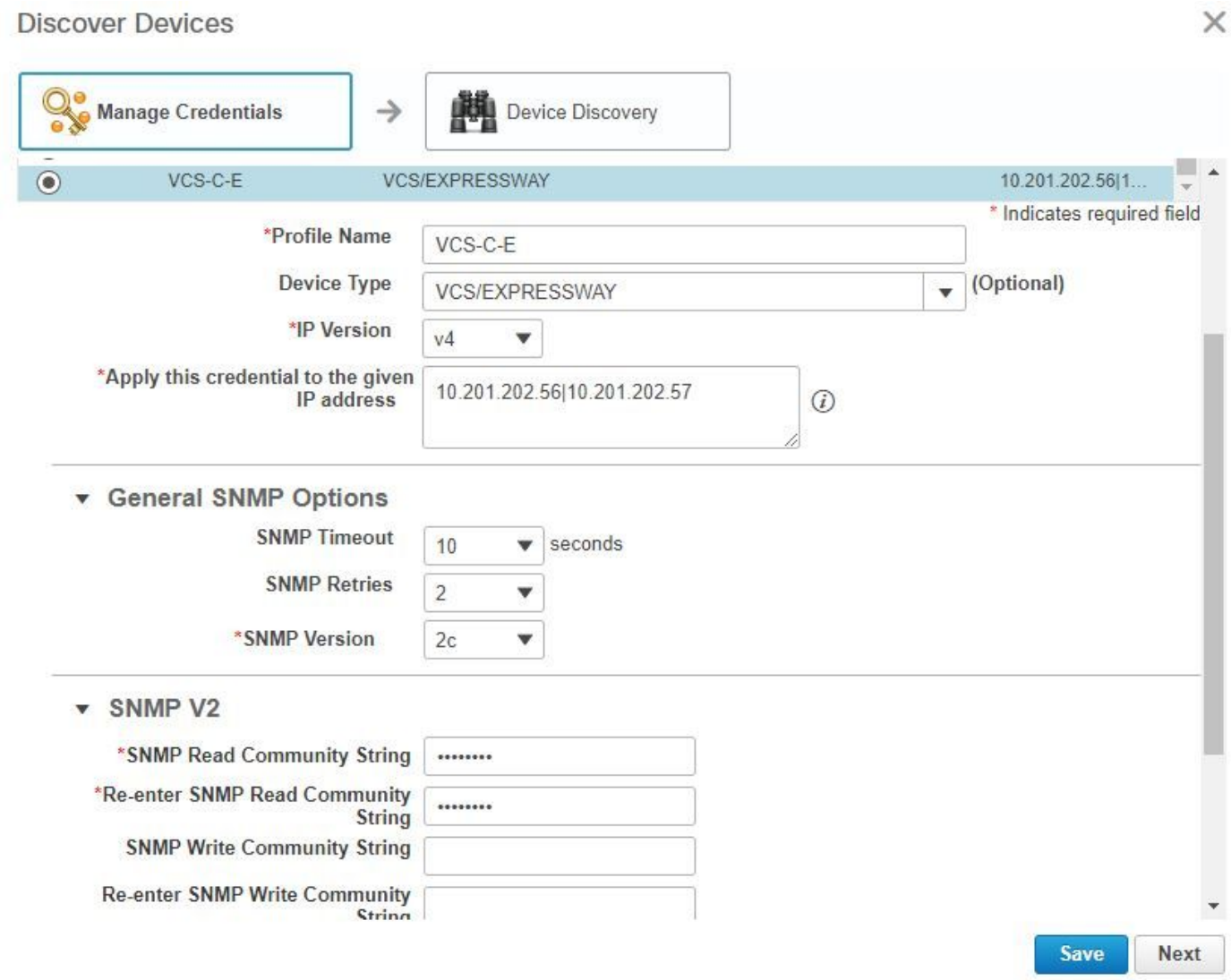
Passaggio 5. La videochiamata di test viene quindi visualizzata nella schermata Diagnostica conferenza.

Scenario 2. Conferenza con endpoint registrati non di gestione delle chiamate

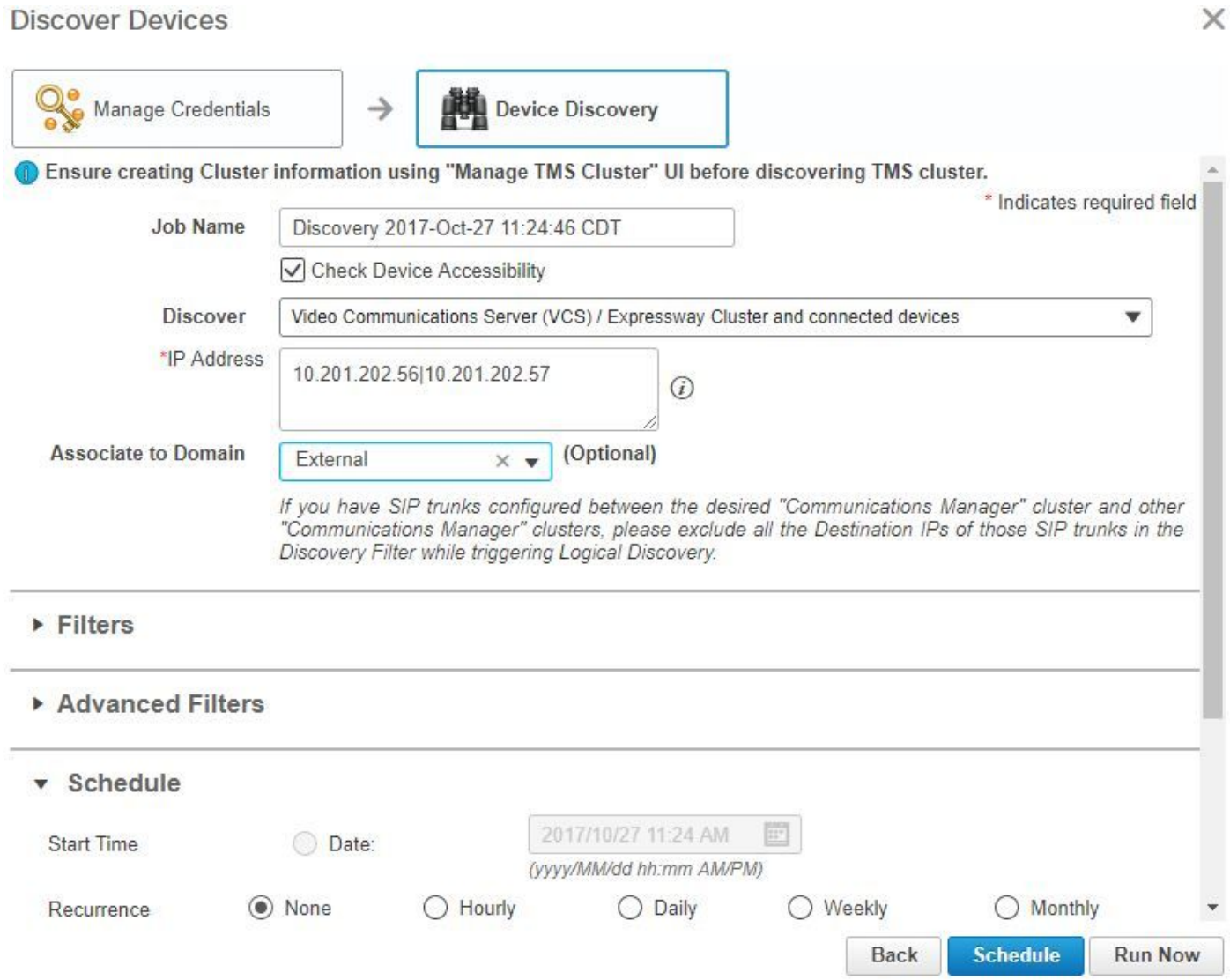
Passaggio 1. Verificare che le credenziali di Telepresence Management Suite (TMS) e Video Communications Server (VCS) siano disponibili.

Nota: quando si individua il sistema VCS/TMS in questo scenario, il processo di rilevamento è importante. Se nella configurazione è presente un gestore delle chiamate, individuare prima il conduttore e quindi il gestore delle chiamate Cisco.

Passaggio 2. Passare a Inventario > Gestione articoli > Gestisci credenziali > Seleziona Aggiungi, quindi immettere le informazioni per il TMS, mentre si crea un profilo di credenziali separato per il VCS, come mostrato nell'immagine.



Passaggio 3. Una volta creato il profilo delle credenziali, selezionare Device Discovery, immettere gli indirizzi IP, quindi selezionare VCS nella scheda Discovery e rilevare le periferiche VCS. Inoltre, selezionare TMS per il TMS e immetterne l'indirizzo IP. Fare clic su Esegui ora come illustrato nell'immagine.



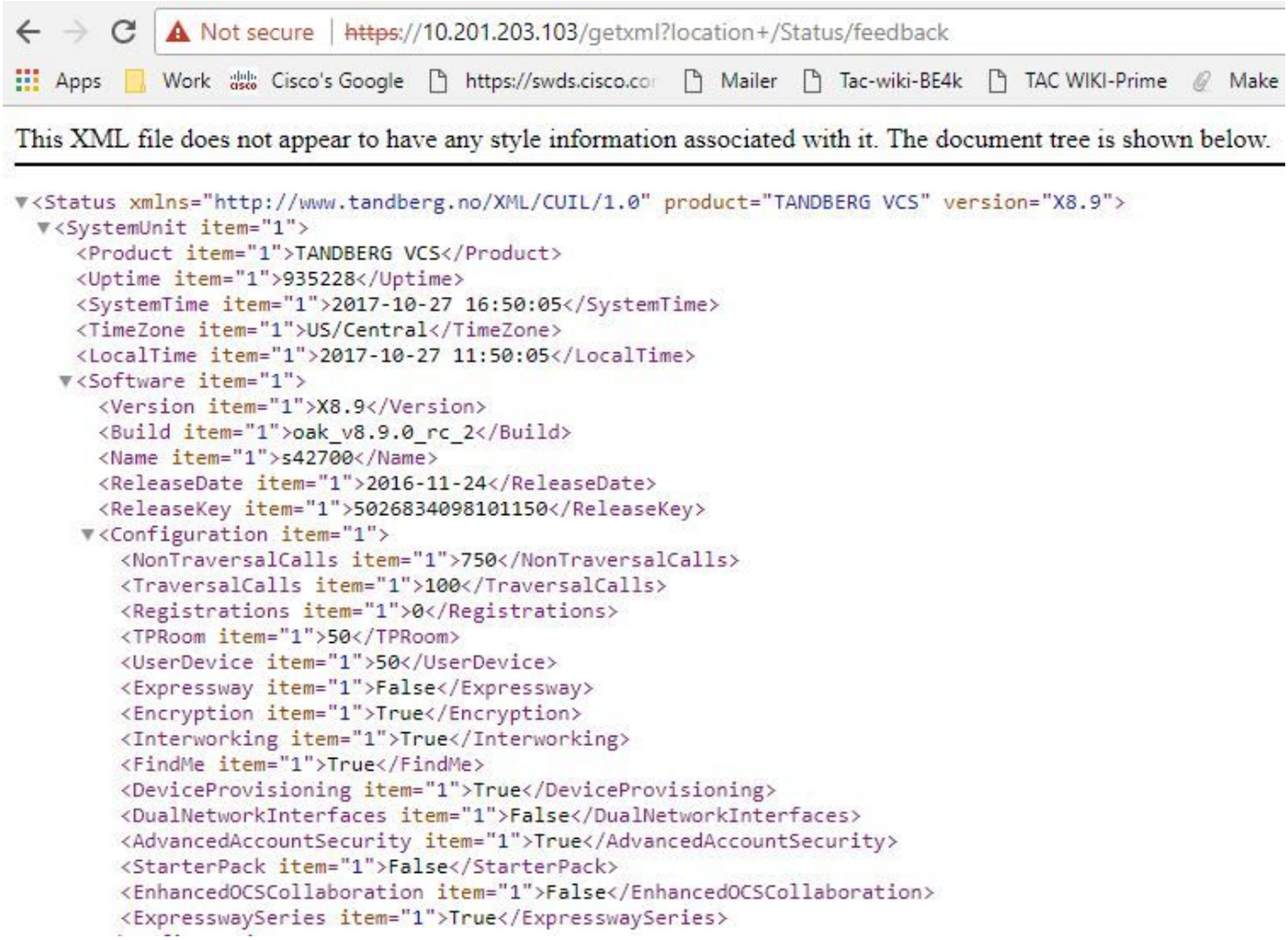
Passaggio 4. Verificare che VCS e TMS siano in stato Managed.

Nota: se il VCS o il TMS non è in uno stato gestito, nella maggior parte dei casi è dovuto a HTTP o SNMP. In caso sia necessaria ulteriore assistenza, aprire una richiesta TAC per ottenere il VCS/TMS in uno stato gestito.

Nota: utilizzare questo URL e sostituire l'indirizzo_IP _of_VCS_Server con l'indirizzo IP appropriato una volta che il VCS è in uno stato gestito. Il server PCA deve essere registrato come server di feedback per VCS. In questo modo, al termine di una sessione di conferenza, non si verificherà alcun problema con i dati che il VCS invia nuovamente all'autorità di certificazione del sistema.

https://<Indirizzo_IP_del_server_VCS>/getxml?location+/Status/feedback , vengono richieste

le credenziali http e dopo l'input è necessario ricevere una risposta come mostrato nell'immagine.



Nota: se Prime Collaboration non è sottoscritta a VCS tramite la sottoscrizione al feedback HTTP, non deve ricevere notifica da VCS quando un endpoint registrato entra o esce da una sessione o si registra o annulla la registrazione a VCS. In questo caso, impostare la visibilità di tali endpoint su completa o limitata in base alle esigenze e verificare che il software VCS sia in stato Managed.

Passaggio 5. Passare a Inventario > Programma magazzino > Programma individuazione dati cluster e selezionare Esegui ora.

Nota: l'esecuzione di questa funzione su tutti i dispositivi dell'infrastruttura può richiedere del tempo. Pertanto, se non viene completato dopo alcuni minuti, ricontrolla dopo 1-2 ore. I sistemi di grandi dimensioni possono impiegare fino a 4 ore. È importante menzionare nell'inventario PCA se ci sono endpoint in cui si desidera avere statistiche di conferenza supportate e che si assicura anche che queste siano gestite per i rapporti e tutte le statistiche per mostrare le informazioni appropriate.

Per un elenco dei dispositivi supportati in base all'APC per quanto riguarda le conferenze e le

sessioni supportate, fare riferimento alla sezione Informazioni di base.

Passaggio 6. Passare a Diagnosi > Diagnostica endpoint.

Per ottenere statistiche corrette per gli endpoint della conferenza, è necessario impostare la loro visibilità al livello massimo consentito dal sistema.

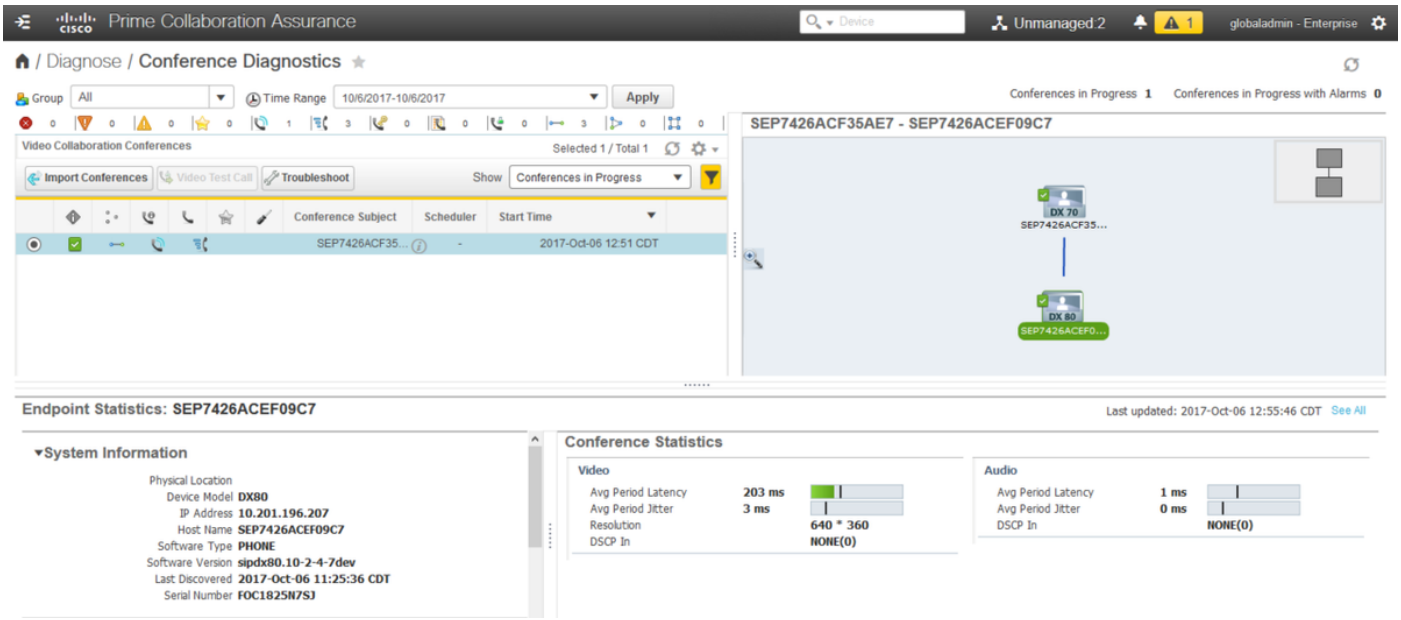
Selezionare tutti gli endpoint che si desidera monitorare in Diagnostica conferenza, quindi fare clic su Modifica visibilità e selezionare la visibilità massima.

The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
• CTS 500, 1000, and 3000 Series • Cisco Codec • Cisco TelePresence SX20 • Cisco TelePresence MXP Series • Cisco IP Video Phone E20	Full	Full
• Cisco Jabber Video for TelePresence (Movi) • Polycom	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
• Cisco SX80 and Cisco SX10 • • Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: • Cisco Jabber • Cisco TelePresence MX Series • Cisco TelePresence System EX Series • Cisco TelePresence System SX Series	Limited	Limited

Nota: se si selezionano, ad esempio, 10 endpoint e si seleziona Visibilità completa, viene selezionato il livello massimo di visibilità per dispositivo.

Passaggio 7. Per verificare, nPassare a Diagnosi > Diagnostica conferenza e una conferenza in corso o completata è come mostrato nell'immagine.



In queste conferenze è possibile visualizzare la media di perdita di pacchetti, latenza e jitter per le chiamate audio e video.

Inoltre, è possibile ottenere una topologia della sessione e dei dispositivi coinvolti.

Allarmi correlati a conferenze

Per Diagnostica conferenza, è possibile ricevere tre diversi allarmi in qualsiasi sessione e impostarne le soglie:

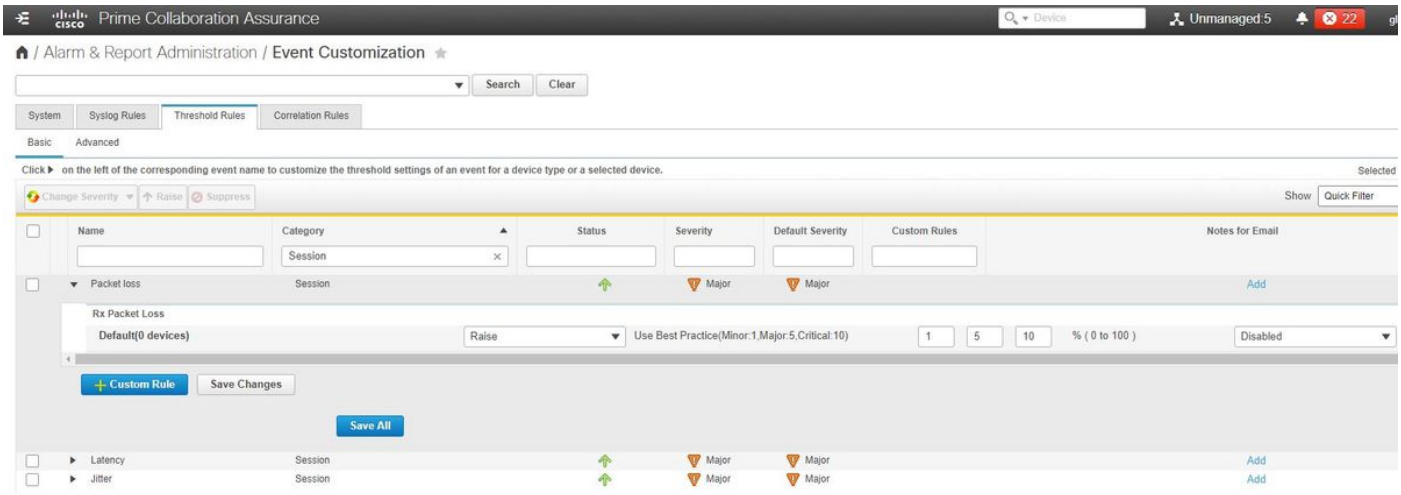
- La perdita di pacchetti
- Latenza
- Variazione

Ognuna di queste opzioni consente di modificare la soglia predefinita, disabilitarla completamente o definire quali dispositivi si desidera associare all'allarme.

Passaggio 1. Passare a Amministrazione avvisi e report >Personalizzazione evento.

Passaggio 2. Selezionare Regole di soglia e assicurarsi di aver selezionato Base.

Passaggio 3. Scorrere verso il basso o filtrare verso destra per la categoria Sessione con nome come mostrato nell'immagine.



Passaggio 4. Selezionare la freccia accanto all'allarme che si desidera modificare ed è possibile modificare le percentuali Minore, Maggiore o Critica per Perdita pacchetto, Instabilità o Latenza.

Passaggio 5. Se si desidera eseguire la compressione, passare da Raise a Surpress.

Passaggio 6. Per definire gli endpoint associati all'avviso, selezionare Regola personalizzata.

Passaggio 7. Quindi, selezionare Device Type > Select All devices o Selectable devices che si desidera vengano selezionati per questo avviso e fare clic su Save.

Report correlati a conferenze

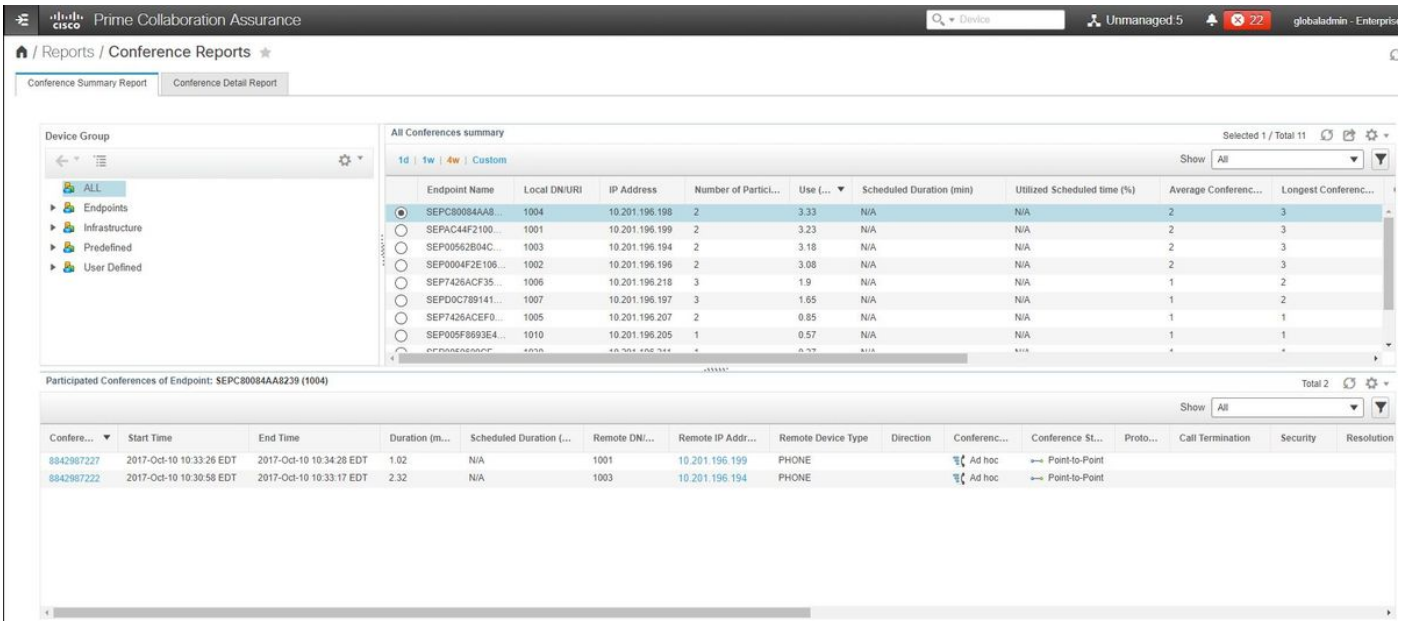
Per i rapporti di Diagnostica conferenza è possibile recuperarli e visualizzarli.

Esistono due rapporti:

- Rapporti conferenza
- Report Degli Endpoint Telepresence

Per i report delle conferenze, è possibile visualizzare un elenco di tutte le conferenze in un intervallo di tempo compreso tra una e quattro settimane oppure un periodo di tempo personalizzato in base alle esigenze.

Passaggio 1. Passare a Report > Report conferenza come mostrato nell'immagine.



Rapporti di riepilogo conferenza

Questo report offre una visualizzazione di ogni endpoint selezionato come visibilità limitata/completa e delle relative conferenze.

Le statistiche mostrate sono:

- Utilizzo medio conferenza
- Allarmi collegati alla conferenza
- Perdita media di pacchetti, jitter e latenza
- Conferenza più lunga

In questo modo è possibile ottenere una visione granulare dei problemi che possono presentarsi nella rete voce/video per determinare quali endpoint presentano il maggior numero di problemi.

Utilizza inoltre la larghezza di banda in base all'utilizzo

Scheda Rapporto dettagli conferenza

Se si verifica un allarme relativo a una conferenza, è possibile passare alla scheda Rapporto Dettagli conferenza.

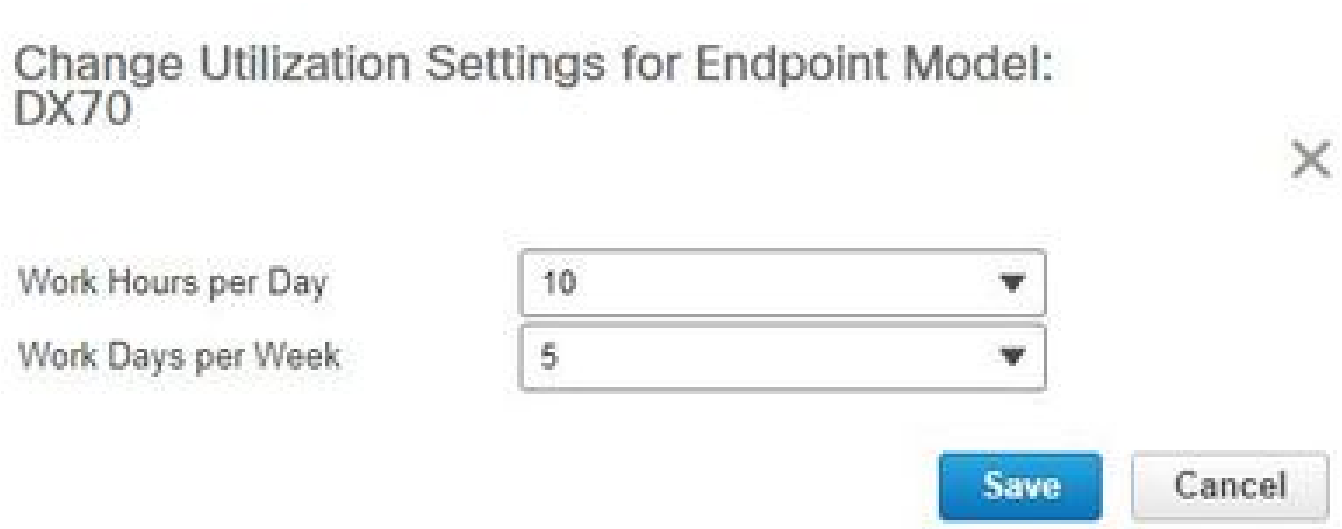
Dopo aver selezionato la conferenza, è possibile definire il nome dell'endpoint, la versione del software e altri dettagli utili.

Per i report degli endpoint di Telepresence è possibile visualizzare i seguenti

- Numero di conferenze effettuate dal dispositivo
- Percentuale di utilizzo
- Modello endpoint
- Utilizzo

Inoltre, potete modificare i parametri di utilizzo mediante la scheda Cambia utilizzo (Change

Utilization), come mostrato nell'immagine.



In questo modo vengono impostati i parametri per il dispositivo in modo che il sistema possa conoscere la percentuale da visualizzare dall'utilizzo.

Nel rapporto Riepilogo endpoint non visualizzati vengono visualizzati gli endpoint per i quali le conferenze pianificate non sono state eseguite.

In questo grafico è possibile visualizzare l'endpoint, il numero totale di conferenze pianificate e il numero di conferenze effettivamente avvenute e non mostrate.

Videochiamata di test di conferenza

È possibile creare chiamate di test video point-to-point tra due endpoint video che si trovano in uno stato gestito, per verificare la rete. È possibile visualizzare eventi e allarmi, statistiche delle sessioni, statistiche degli endpoint e topologia di rete. Per questa chiamata sono supportati solo i codec delle serie CTS, C ed EX.

Inoltre, questa funzione può essere utilizzata per verificare che tutte le funzionalità siano corrette con la diagnostica della conferenza.

Prerequisiti

- Questa funzione non è supportata per la serie di codec E20.
- Per utilizzare questa funzionalità, è necessario aggiungere le credenziali CLI per gli endpoint.
- Verificare che gli endpoint siano registrati e che JTAPI sia abilitato per gli endpoint (se sono registrati in Unified CM).
- La funzione Video Test Call non è disponibile se Cisco Prime Collaboration è stato distribuito in modalità MSP.

Passaggio 1. Passare a Diagnosi > Diagnostica endpoint.

Passaggio 2. Selezionare due endpoint applicabili in base ai prerequisiti.

Passaggio 3. Selezionare Esegui test > Videochiamata di test.

Passaggio 4. È possibile pianificare l'esecuzione di Video Test Call adesso o in base a una pianificazione di ripetizione delle occorrenze.

Passaggio 5. La videochiamata di test viene quindi visualizzata nella schermata Diagnostica conferenza.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

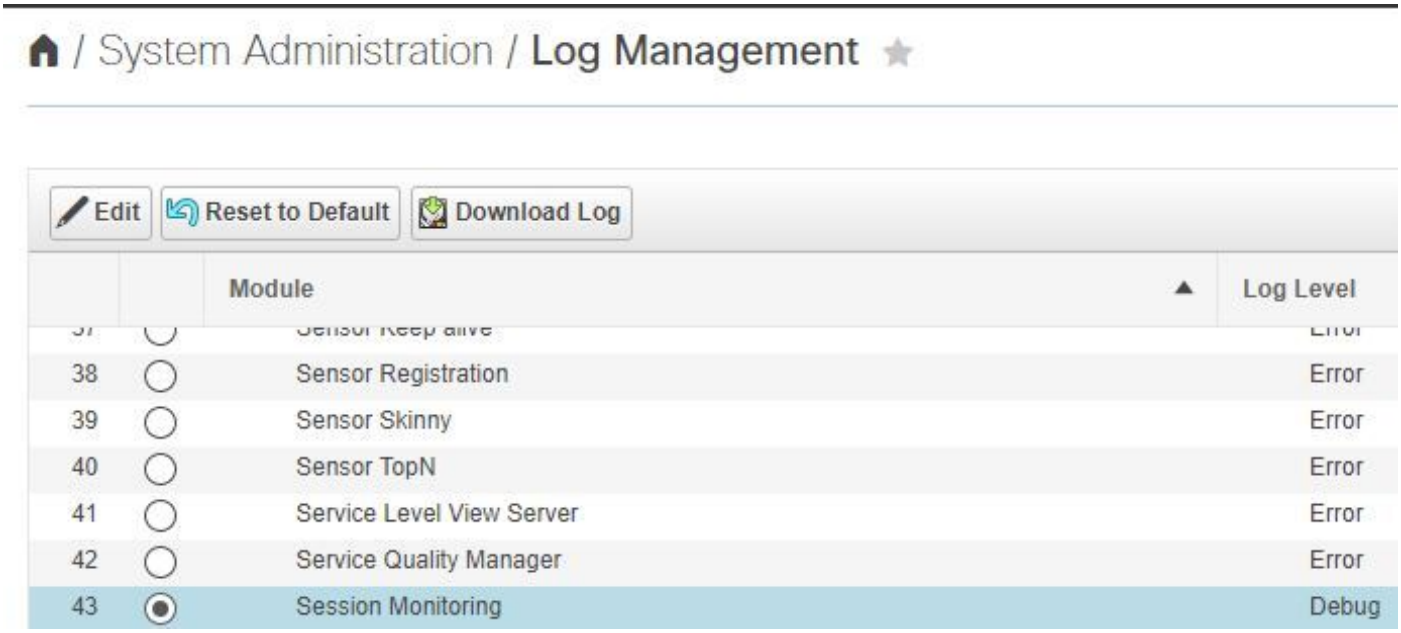
Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Registri da raccogliere per la risoluzione dei problemi

Passaggio 1. Passare a Amministrazione sistema > Gestione log.

Passaggio 2. Scorrere fino al modulo e selezionare Session Monitoring (Monitoraggio sessione), quindi selezionare Edit (Modifica), come mostrato nell'immagine.



Passaggio 3. Modificare il livello di log in debug e fare clic su Salva.

Passaggio 4. Riprodurre il problema, quindi tornare alla schermata Log Management.

Passaggio 5. Dopo aver riprodotto il problema, selezionare Monitoraggio sessione e Download log.

Passaggio 6. Dopo il download, estrarre il file zip.

Passaggio 7. Aprire il file zip e passare alle posizioni per i log utili:

/opt/emms/emsam/log/SessionMon/

- FILE.LOG.MJTAPI
- lagIDCampo.log
- CSMTracker
- CSMTrackerDiag.log
- CSMTrackerOrigineDati.log
- PostInitSessionMon.log

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).