Configurar o Prime Collaboration Assurance (PCA) - Diagnóstico de Conferência

Contents

Introdução

Este documento descreve como configurar e configurar sua implantação para o Conference Diagnostics no Prime Collaboration Assurance (PCA) para monitorar de forma proativa as estatísticas de conferência de voz/vídeo.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Logon do administrador do Call Manager
- Fazer login no APC
- Seu TMS (Telepresence Monitor Server, servidor de monitoramento de telepresença)

- Credenciais do Core/Expressway, se aplicável

Componentes Utilizados

As informações neste documento são baseadas nas versões 11.x - 12.x do APC.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Prime Collaboration 11.x oferece suporte aos seguintes tipos de visibilidade:

- Visibilidade total - A detecção de chamadas com o uso de feedback JTAPI/HTTP e informações de monitoramento em tempo real, como estatísticas de conferência e informações de conferência, é suportada.
- Visibilidade limitada - Ocorre a detecção automática de chamadas com o uso de feedback JTAPI/HTTP, mas não há suporte para informações de monitoramento em tempo real, como estatísticas de conferência e informações de conferência. Endpoints com visibilidade limitada são indicados com um ícone de meio esmaecido na topologia de conferência.

O Cisco Prime Collaboration 12.x oferece suporte aos seguintes tipos de visibilidade:

- Visibilidade total - A detecção de chamadas com o uso de feedback JTAPI/HTTP e informações de monitoramento em tempo real, como estatísticas de conferência e informações de conferência, é suportada.
- Sem visibilidade - A detecção de chamadas com o uso de feedback JTAPI/HTTP e informações de monitoramento em tempo real não são suportadas. Esses pontos finais são exibidos na página Monitoramento de Conferência com um ícone totalmente esmaecido.

Limitação de endpoints definidos para visibilidade limitada ou total por OVA

- O Small Open Virtualization Archive (OVA) suporta até 500 endpoints
- OVA médio suporta até 1000 endpoints
- OVA grande suporta até 1800 endpoints
- OVA muito grande comporta até 2000 endpoints

Uma lista de dispositivos suportados por PCA em relação a conferências e nossas sessões suportadas é mostrada na imagem da tabela aqui.

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.

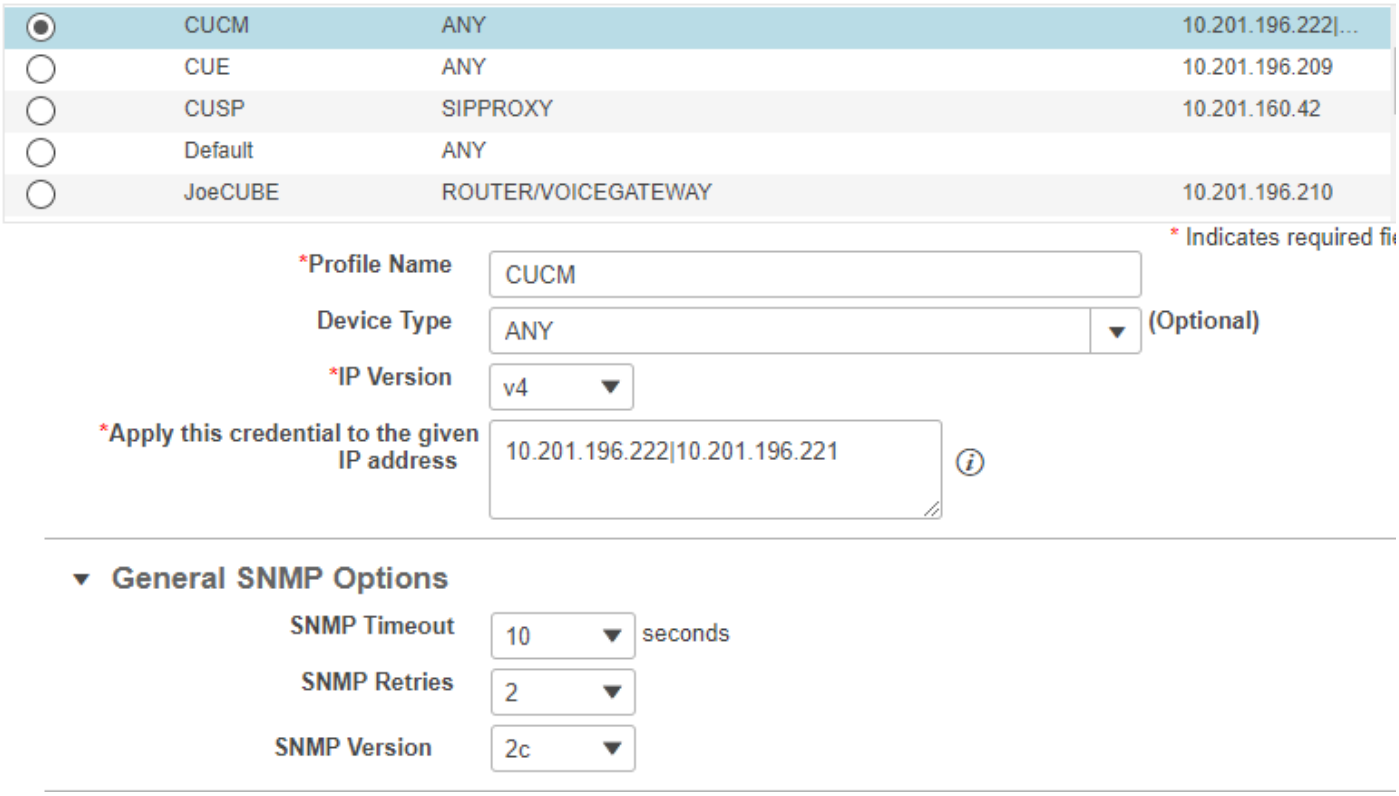
Configurar

Cenário 1. Conferência com endpoints de vídeo registrados no Call Manager

Etapa 1. Primeiro, você precisa garantir que os gerenciadores de chamadas estejam em um estado Gerenciado.

Navegue para Inventário > Gerenciamento de inventário > Gerenciar credenciais > Criar um perfil para o cluster do Call Manager.

Observação: lembre-se de que cada perfil de credencial usa as mesmas credenciais para cada ip listado no perfil. Assim, se você listar o editor e o assinante do Call Manager dentro do mesmo perfil de credencial, ele usará essas mesmas credenciais para descobrir os dois endereços ip. Se você tiver um condutor em sua configuração, descubra primeiro o condutor e depois o Cisco Call Manager, como mostrado na imagem.



Etapa 2. Verifique se você configurou o HTTP (Hypertext Transfer Protocol), o SNMP (Simple Name Management Protocol) e as credenciais da API de telefonia Java (JTAPI)

Além disso, você deve habilitar o serviço Cisco Computer Telephony Integration (CTI) no Call Manager Serviceability.

Configuração do Cisco Unified Communications Manager

Habilitar HTTP

Você não precisa criar um novo usuário se quiser permitir que o Cisco Prime Collaboration use credenciais de administrador para fazer login. Como alternativa, se quiser permitir que o Cisco Prime Collaboration Manager use as credenciais corretas para fazer login no Cisco Unified Communications Manager, você deverá criar um novo grupo de usuários HTTP e um usuário correspondente que o Cisco Prime Collaboration possa usar para se comunicar.

Para criar um usuário, siga estas etapas:

Etapa 1. Faça login na interface da Web do Cisco Unified CM Administration com sua conta de administrador.

Etapa 2. Crie um grupo de usuários com privilégios suficientes. Navegue para Gerenciamento de usuário>Configurações do usuário>Grupo de controle de acesso e crie um novo grupo de usuários com um nome adequado, PC_HTTP_Users nesse caso. Agora, selecioneSalvar.

Etapa 3. Navegue até Gerenciamento de usuários>Configurações do usuário>Grupo de controle de acesso e selecioneLocalizar. Localize o grupo que você definiu e clique no ícone à direita.

Etapa 4. Selecione Atribuir função ao grupo e selecione estas funções:

- Acesso à API AXL padrão
- Usuários padrão do CCM Admin
- Administração de FACILIDADE DE MANUTENÇÃO padrão

Etapa 5. Click Save.

Etapa 6. No menu principal, navegue atéGerenciamento de usuários>Usuários de aplicativos>Criar um novo usuário.

Especifique uma senha adequada na página Application User Configuration. Você pode selecionar apenas determinados tipos de dispositivos na área de texto Dispositivos disponíveis ou permitir que o Cisco Prime Collaboration monitore todos os dispositivos

Passo 7. Na seção Permission Information, selecione Add to User Group e selecione o grupo criado na Etapa 1. (por exemplo, PC_HTTP_Users).

Etapa 8. Clique em Salvar. A página é atualizada e os privilégios corretos são exibidos.

Habilitar SNMP

O SNMP não está habilitado no Cisco Unified Communications Manager por padrão.

Para habilitar o SNMP:

Etapa 1. Faça login na exibição Cisco Unified Serviceabilityna GUI da Web do Cisco Unified Communications Manager.

Etapa 2. Navegue até Ferramentas > Ativação de serviço.

Etapa 3. Selecione Publisher Server.

Etapa 4. Navegue para Performance > Monitoring Services e marque a caixa de seleção para Cisco Call Manager SNMP Service.

Etapa 5. Selecione Save na parte inferior da tela.

Para criar uma série de comunidade SNMP:

Etapa 1. Faça login noCisco Unified Serviceabilityexibir a GUI da Web do Cisco Unified Communications Manager.

Etapa 2. No menu principal na exibição Cisco Unified Serviceability, navegue para SNMP > v1/v2c > Community String.

Etapa 3. Selecione um servidor e clique emLocalizar.
Se a string de comunidade já estiver definida, o Nome da String de Comunidade será exibido nos Resultados da Pesquisa.

Etapa 4. Clique em Adicionar novo para adicionar uma nova string se nenhum resultado for exibido.

Etapa 5. Especifique as informações SNMP necessárias e salve a configuração.

Observação: somente o acesso somente leitura (RO) SNMP é necessário.

Iniciar Serviço CTI

Execute o procedimento desejado para o nó do Cisco Unified Communications Manager, que é preferível definir em dois nós.

Etapa 1. Faça login no Cisco Unified Serviceability, exibido na interface gráfica do usuário do Cisco Unified Communications Manager.

Etapa 2. Navegue até Ferramentas > Ativação de serviço.

Etapa 3. Selecione um servidor na lista suspensa.

Etapa 4. Na seção CM Services, marque a caixa de seleção Cisco CTI Manager.

Etapa 5. Selecione Save na parte superior da tela

Criar usuário de aplicativo para controle CTI PCA (usuário JTAPI)

JTAPI é usado para recuperar as informações de status da sessão do dispositivo. Você deve criar um usuário de aplicativo para o Controle CTI no processador de chamadas com a permissão necessária para receber eventos JTAPI em pontos de extremidade. O Prime Collaboration gerencia vários clusters de processadores de chamadas. Você deve garantir que as IDs de cluster sejam exclusivas. Crie um novo usuário do aplicativo para ajudar o Cisco Prime Collaboration a obter as informações necessárias.

Para criar um novo aplicativo JTAPI, siga estas etapas:

Etapa 1. Faça login na interface da Web do Cisco Unified CM Administration por meio da sua conta de administrador.

Etapa 2. Crie um grupo de usuários com privilégios suficientes. Navegue para Gerenciamento de usuário>Configurações do usuário>Grupo de controle de acesso e crie um novo grupo de usuários com um nome adequado, PC_HTTP_Users nesse caso. Agora, selecioneSalvar.

Etapa 3. Selecione Gerenciamento de usuários>Configurações do usuário>Grupo de controle de acesso e clique emLocalizar. Localize o grupo que você definiu e selecione o ícone à direita.

Etapa 4. Clique em Atribuir função ao grupo e selecione estas funções:

- CTI Padrão Permitir Monitoramento de Chamadas
- CTI padrão habilitado

- CTI padrão permite controle de telefones que suportam Xfer e conf conectados

Etapa 5. Selecione Salvar.

Etapa 6. No menu principal, navegue atéGerenciamento de usuários>Usuários de aplicativos>Criar um novo usuário.
Especifique uma senha adequada na página Application User Configuration. Você pode selecionar determinados tipos de dispositivos na área de texto Dispositivos disponíveis ou permitir que o Cisco Prime Collaboration monitore todos os dispositivos.

Observação: a senha não deve conter um ponto-e-vírgula (;) ou igual a (=).

Passo 7. Na seção Permission Information, selecione Add to Access Control Group e selecione o grupo criado na Etapa 1. (por exemplo, PC_HTTP_Users).

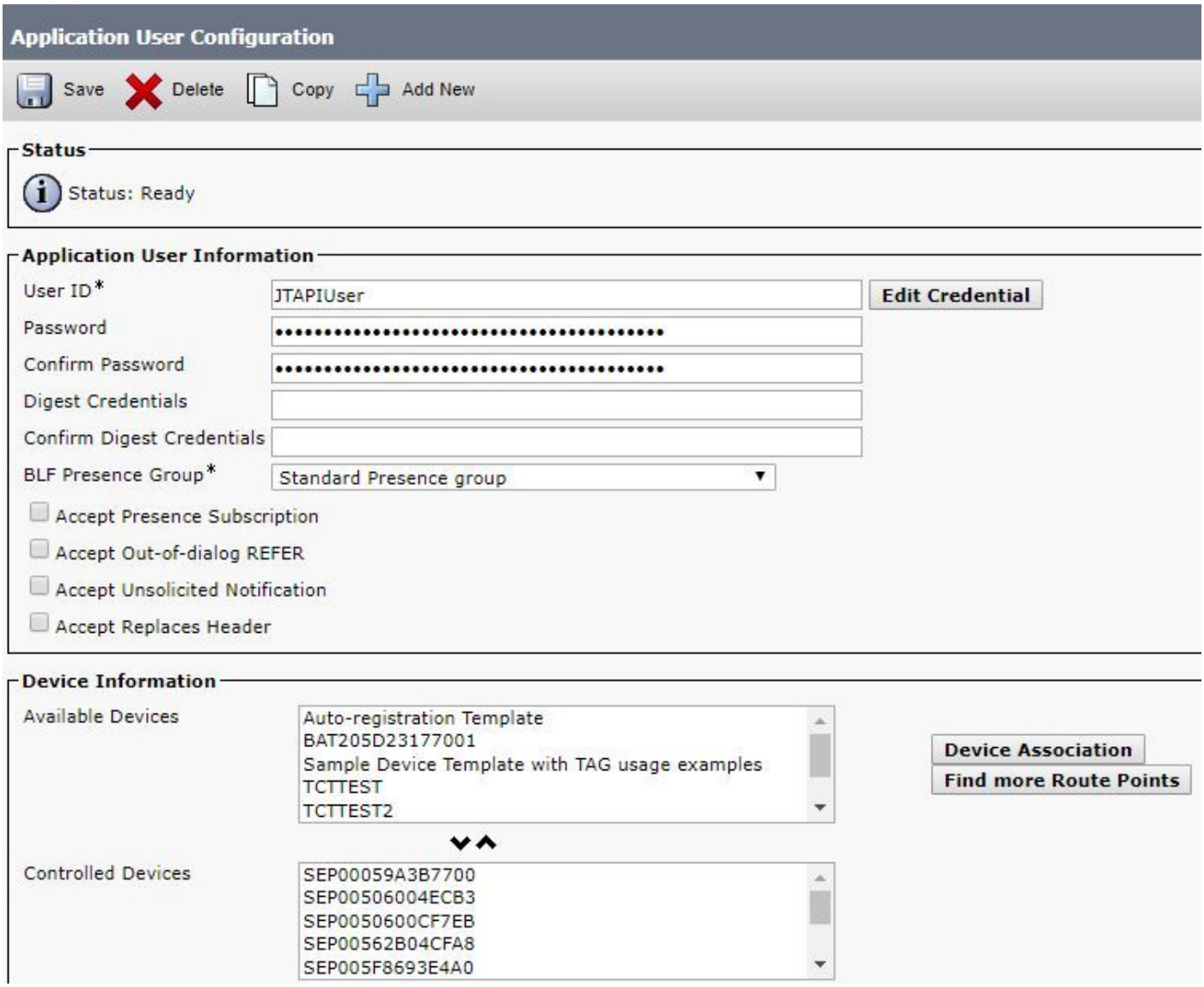
Etapa 8. Clique em Salvar. A página é atualizada e os privilégios corretos são exibidos.

Observação: se o Call Manager foi gerenciado antes da adição do usuário JTAPI, verifique se o usuário JTAPI foi adicionado ao Perfil de credencial do Call Manager e redescubra-o.

Continuação do cenário 1. Etapas:

Etapa 3. Navegue até o usuário do aplicativo JTAPI do Call Manager que você criou e mova os endpoints com suporte de Dispositivos Disponíveis para Dispositivos Controlados.

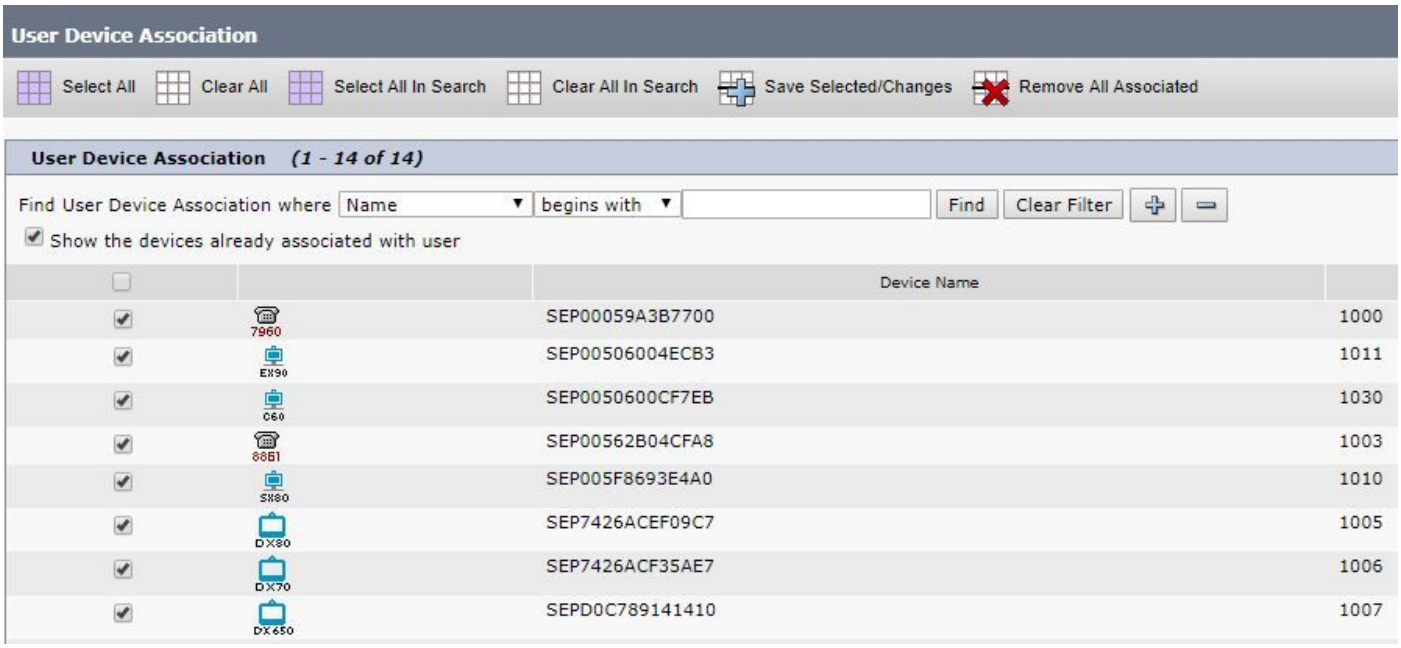
Você pode executar isso pela função Device Association, conforme mostrado na imagem.



Se você consultar a limitação de endpoints definidos como limitada ou visibilidade total por OVA, poderá verificar a quantidade de dispositivos adicionados ao tamanho do OVA.

Nesta tela, você pode filtrar por Nome do dispositivo, Descrição ou Número do diretório para ajudá-lo a gerenciar e filtrar esses dispositivos como mostrado na imagem.

É útil observar esses dispositivos à medida que são adicionados na Etapa 7.



Certifique-se também de que as funções de usuário corretas sejam adicionadas para este usuário JTAPI:

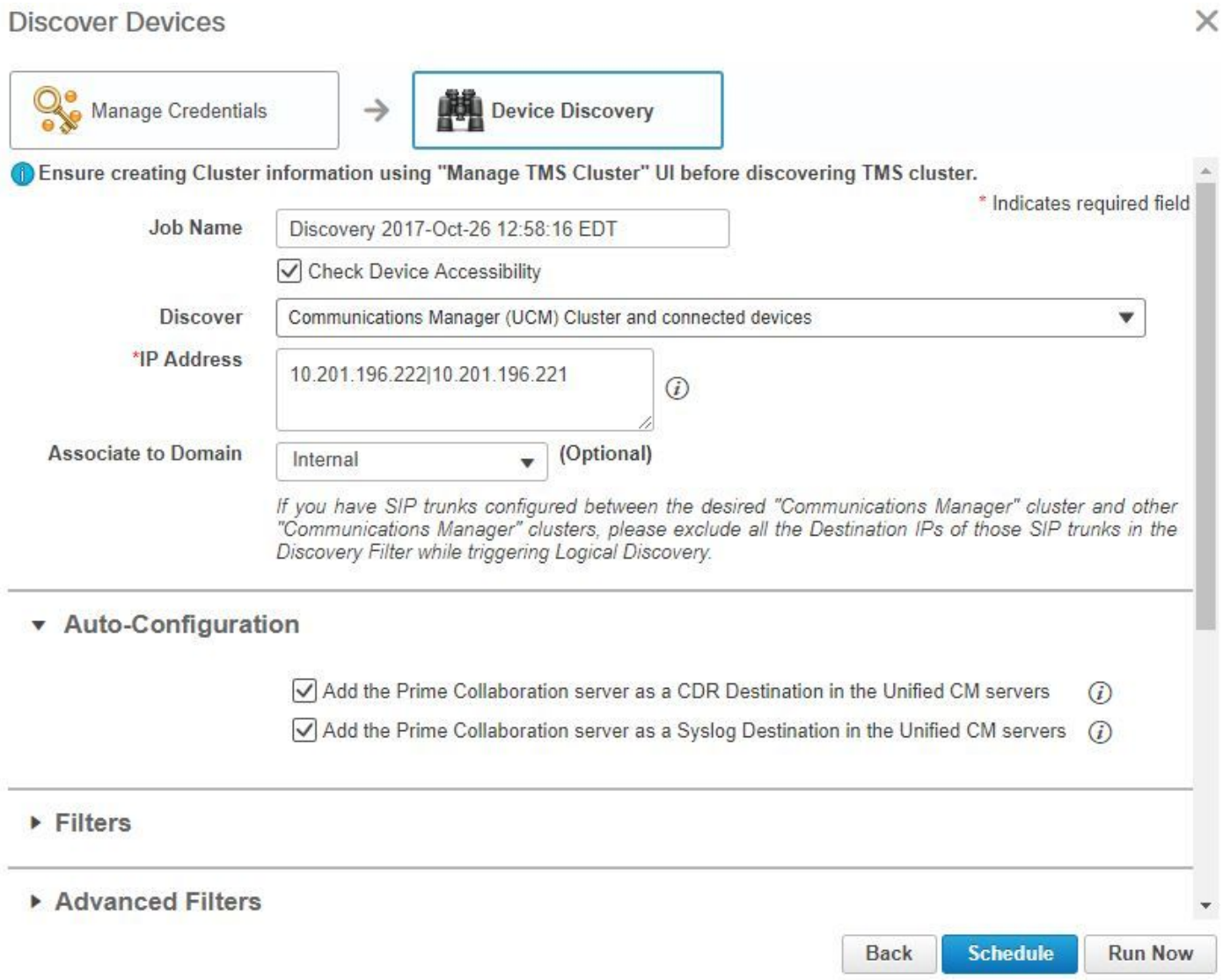
- CTI Padrão Permitir Monitoramento de Chamadas
- CTI padrão habilitado
- O CTI padrão permite o controle de telefones que suportam Xfer conectado e conf como mostrado na imagem.

Para obter uma lista de dispositivos suportados por PCA, com relação às conferências e nossas sessões suportadas, consulte a seção Informações de Fundo.

Observação: além disso, certifique-se de que os dispositivos controlados pelo usuário do aplicativo CTI tenham a caixa de seleção Permitir controle do dispositivo do CTI marcada nas informações do dispositivo, conforme mostrado na imagem.

Observação: antes de continuar, é importante observar que, se você tiver os endpoints registrados no Call Manager e o Call Manager estiver integrado ao VCS/TMS, você descobrirá primeiro o VCS/TMS e, em seguida, descobrirá o Call Manager por último. Dessa forma, do ponto de vista do inventário, toda a sua infraestrutura é mapeada para o local correto. Além disso, quando você descobre o VCS/TMS, certifique-se de alterar a guia Discover (Detectar) padrão para o respectivo dispositivo do TMS/VCS ou Call Manager.

Etapa 4. Em seguida, no PCA, selecione Device Discovery e insira os endereços IP dos seus Call Managers, marque as duas caixas de seleção em AutoConfiguration e selecione Run Now, como mostrado na imagem.



Etapa 5. Depois que os Call Managers estiverem em um estado Gerenciado, continue na etapa 6.

Observação: se o Call Manager não estiver em um estado gerenciado, na maioria das vezes é devido a HTTP ou SNMP, se for necessária mais assistência, abra um caso no TAC para colocar o call manager em um estado Gerenciado.

Etapa 6. Navegue para Inventory > Inventory Schedule > Cluster Data Discovery Schedule e

selecione Run Now.

Observação: isso depende de quantos dispositivos registrados/não registrados você tem. Esse processo pode levar de alguns minutos a algumas horas. Verifique durante o dia com uma atualização da página. Além disso, isso mapeia o cluster do Call Manager e recupera todos os endpoints. Depois que isso estiver concluído, vá para a próxima etapa.

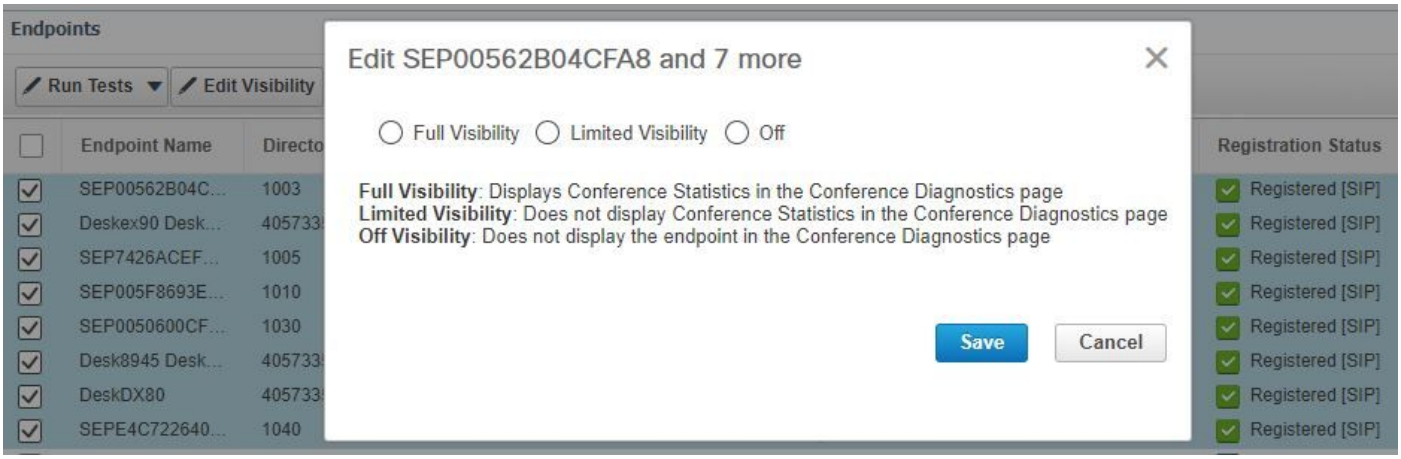
Nota: É importante mencionar no inventário de PCA se houver endpoints nos quais você deseja ter estatísticas de conferência suportadas. Certifique-se de que eles sejam bem gerenciados para relatórios e todas as estatísticas, para mostrar as informações corretas.

Passo 7. Navegue até Diagnostics > Endpoint Diagnostics.

Para obter estatísticas atualizadas para seus endpoints de conferência, você precisa definir sua visibilidade para o nível mais alto possível permitido pelo sistema.

Selecione todos os pontos de extremidade que deseja monitorar no Diagnóstico de Conferência, clique em Editar Visibilidade e selecione Visibilidade Total como mostrado na imagem.

A visibilidade limitada mostra apenas o dispositivo na topologia, mas não mostra estatísticas e não pode recuperar alarmes aplicáveis para os dispositivos relacionados ao Diagnóstico de Conferência.

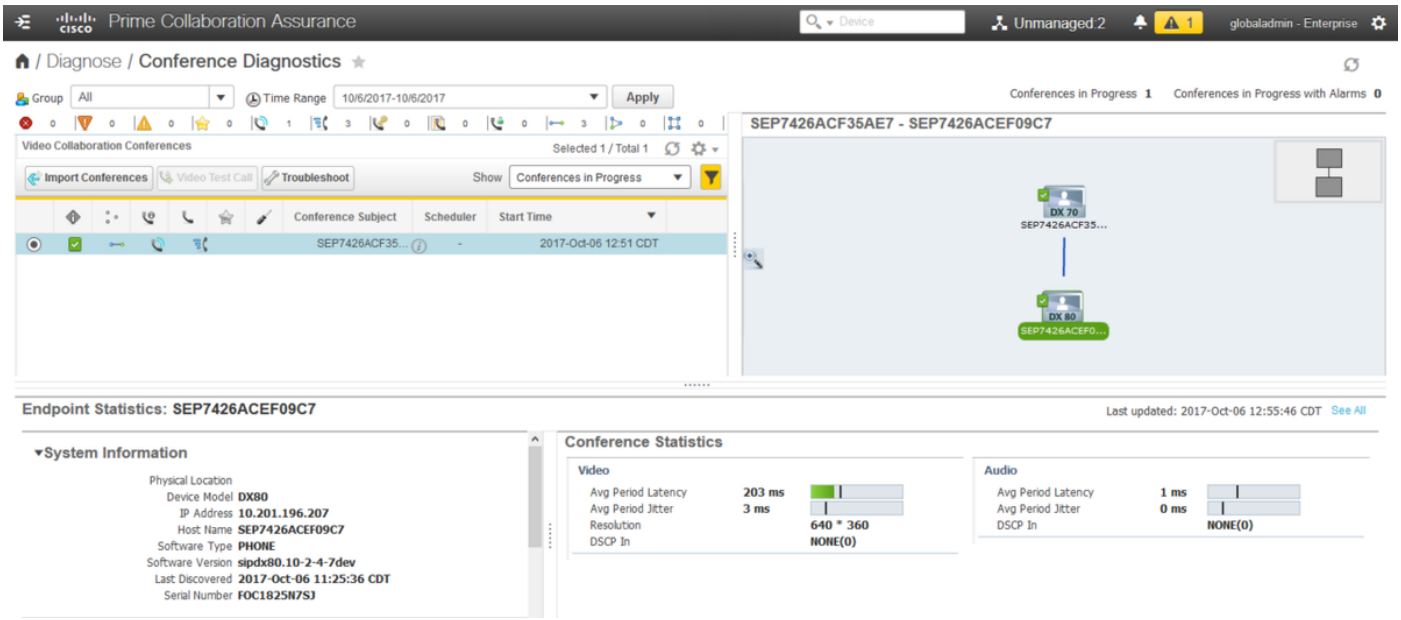


The following table lists the default and maximum visibility details for the endpoints:

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

Observação: se você selecionar, por exemplo, 10 pontos finais e selecionar Visibilidade total, ele selecionará o nível mais alto de suporte de visibilidade por dispositivo.

Etapa 8. Para testar, navegue até Diagnostics > Conference Diagnostics e uma exibição Conference In progress ou completed, conforme mostrado na imagem.



Nessas conferências, você pode exibir a perda média de pacotes, a latência e o jitter para chamadas de áudio e vídeo.

Além disso, obtenha uma topologia da sessão e dos dispositivos envolvidos.

Atualmente, o Diagnóstico de Conferência extrai as informações com base no DN e, se o seu ambiente tiver DNs compartilhados, o PCA recupera o primeiro que receber para a conferência.

Alarmes Relacionáveis à Conferência

Para o Diagnóstico de Conferência, você pode receber três alarmes diferentes para qualquer sessão e definir seus limites:

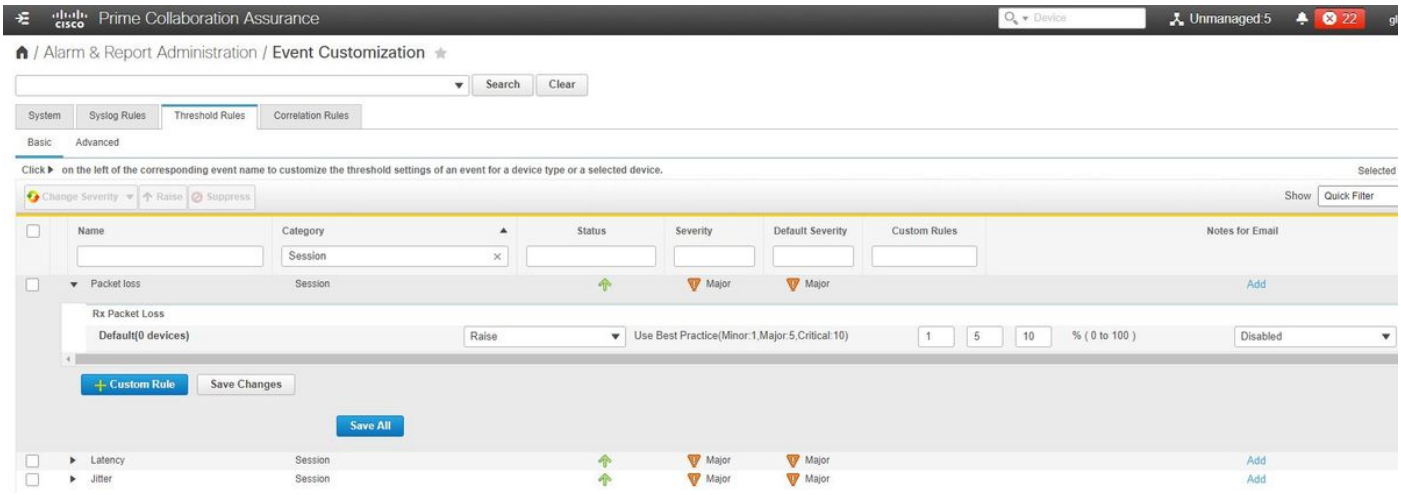
- Perda de pacote
- Latência
- Tremulação

Para cada um deles, você pode modificar o limite padrão, suprimi-lo ou definir quais dispositivos você gostaria de associar a este alarme.

Etapa 1. Navegue até Alarm & Report Administration > Event Customization.

Etapa 2. Selecione Threshold Rules e certifique-se de que Basic esteja selecionado.

Etapa 3. Role para baixo ou filtre para a direita para a Categoria Sessão Nomeada como mostrado na imagem.



Etapa 4. Selecione a seta suspensa ao lado do alarme. Você deseja modificar e pode modificar as porcentagens Secundária, Principal ou Crítica para Perda de Pacote, Instabilidade ou Latência.

Etapa 5. Se você quiser suprimir, alterne Raise para Surpress.

Etapa 6. Se quiser definir os pontos finais associados ao alarme, você poderá selecionar a opção Regra Personalizada.

Passo 7. Em seguida, selecione o Tipo de dispositivo > Selecionar todos os dispositivos ou Dispositivos selecionáveis que você deseja para este alarme e clique em Salvar.

Relatórios Relacionáveis à Conferência

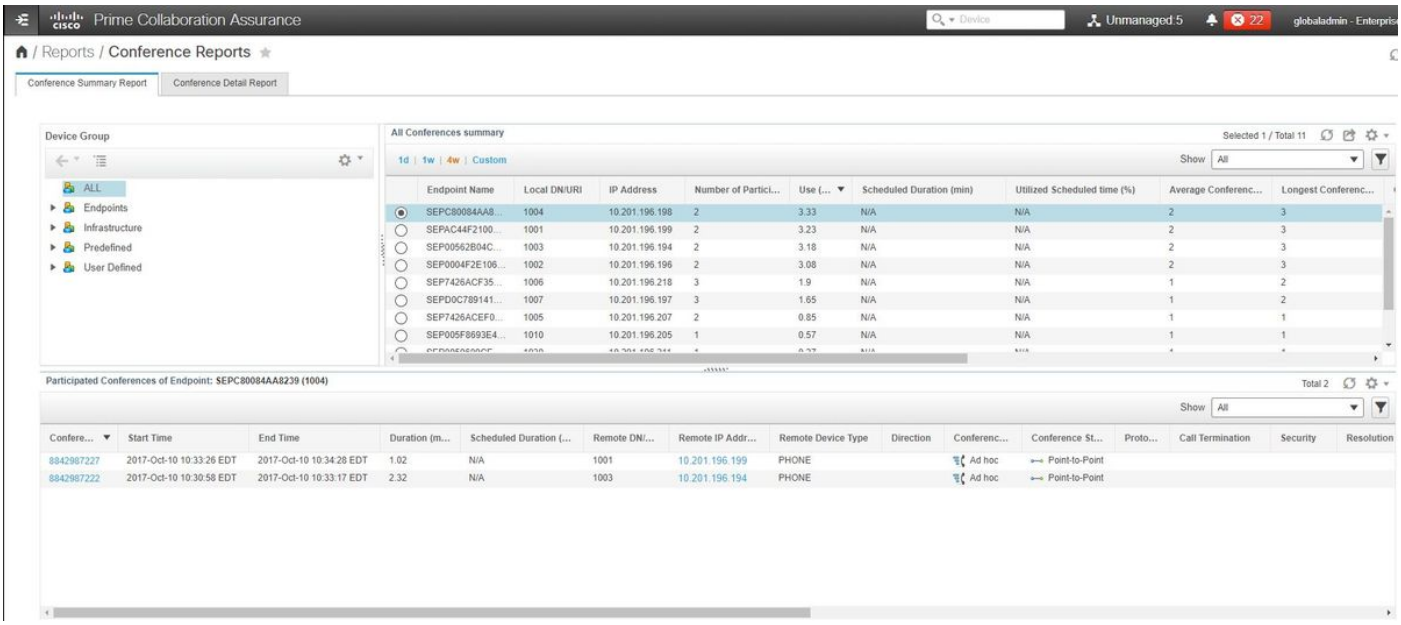
Os relatórios de Diagnóstico de Conferência podem ser recuperados e exibidos.

Há dois relatórios:

- Relatórios de conferência
- Relatórios de endpoint de telepresença

Para Relatórios de Conferência, você pode exibir uma lista de todas as conferências em um período de uma a quatro semanas ou em um período personalizado, conforme necessário.

Etapa 1. Navegue até Relatórios > Relatórios de conferência conforme mostrado na imagem.



Relatórios de Resumo de Conferências

Este relatório fornece uma exibição de cada endpoint selecionado como visibilidade limitada/total e suas conferências.

As estatísticas mostradas aqui são:

- Uso Médio da Conferência
- Alarmes relacionados à conferência
- Perda média de pacotes, instabilidade e latência
- Conferência Mais Longa

Isso pode ajudá-lo a obter uma visão granular dos problemas que você pode ter em sua rede de voz/vídeo para determinar quais endpoints têm mais problemas.

Além disso, você pode utilizar sua largura de banda em correspondência por uso.

Guia Relatório de detalhes de conferências

Se você encontrar um alarme para uma Conferência, poderá navegar até a guia Relatório de detalhes da conferência.

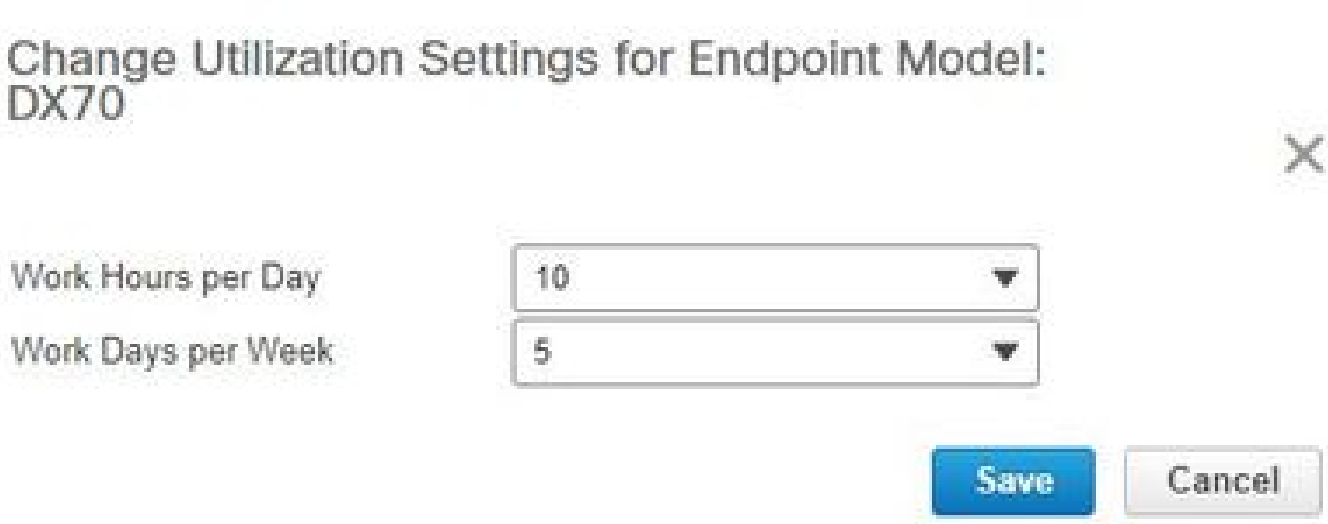
Depois de selecionar a Conferência, você poderá refiná-la para encontrar o nome do endpoint, a versão do software e outros detalhes nos quais possa estar interessado.

Para Relatórios de endpoint de telepresença, você pode exibir por endpoint:

- Número de conferências que este dispositivo tinha
- Porcentagem de utilização
- Modelo de endpoint
- Uso

Além disso, você pode alterar os Parâmetros de Utilização pela guia Alterar Utilização, conforme

mostrado na imagem.



Isso define os parâmetros desse dispositivo para que o sistema saiba, com base no uso, qual porcentagem exibir.

O Relatório de resumo de endpoints não exibidos exibe os endpoints que perderam conferências agendadas.

Neste gráfico, você também pode exibir o Ponto de Extremidade e quantas Conferências Total Agendadas e quantas delas ocorreram e não foram mostradas.

Chamada de Teste de Vídeo de Conferência

Você pode criar chamadas de teste de vídeo ponto a ponto entre dois endpoints de vídeo no estado gerenciado para testar sua rede. Você pode ver eventos e alarmes, estatísticas de sessão, estatísticas de endpoint e topologia de rede com estatísticas como outras chamadas. Somente os codecs das séries CTS, C e EX são suportados para esta chamada.

Além disso, isso pode ser usado para validar se tudo está funcionando com o diagnóstico de conferência.

Pré-requisitos

- Este recurso não é suportado para a série de codecs E20.
- Para usar esse recurso, as credenciais da CLI devem ser adicionadas para os endpoints.
- Verifique se os pontos de extremidade estão registrados e se JTAPI está habilitado para pontos de extremidade (se estiverem registrados no Unified CM).
- O recurso Video Test Call não está disponível se você tiver implantado o Cisco Prime Collaboration no modo MSP.

Etapa 1. Navegue até Diagnostics > Endpoint Diagnostics.

Etapa 2. Selecione dois endpoints aplicáveis de acordo com os pré-requisitos mencionados.

Etapa 3. Selecione Run Tests > Video Test Call.

Etapa 4. Você pode agendar a chamada de teste de vídeo para ser executada agora ou em um cronograma de recorrência.

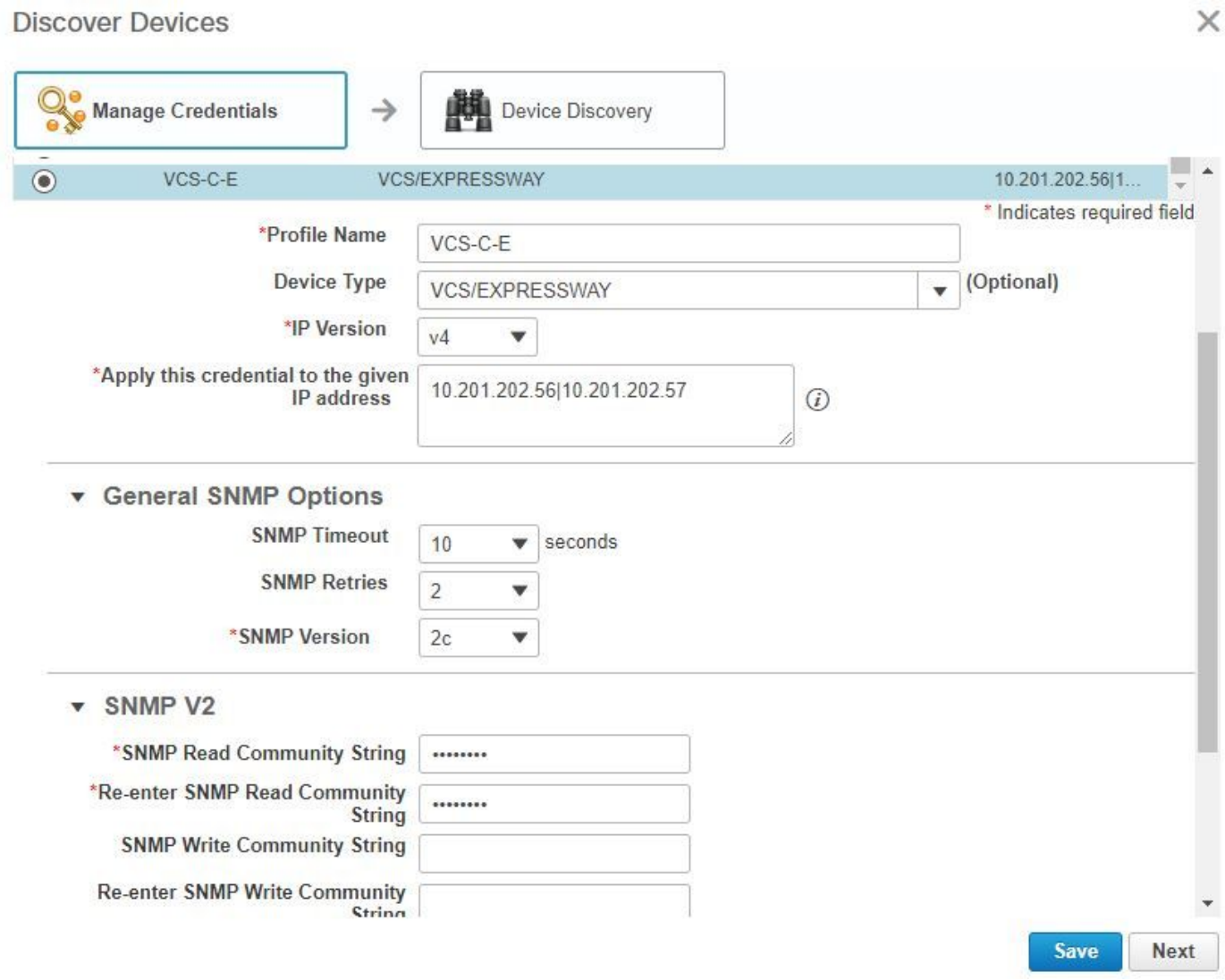
Etapa 5. Esta chamada de teste de vídeo é exibida na tela Diagnóstico de conferência.

Cenário 2. Conferência com pontos finais registrados fora do Call Manager

Etapa 1. Verifique se as credenciais do TMS (Telepresence Management Suite) e do VCS (Video Communications Server) estão disponíveis.

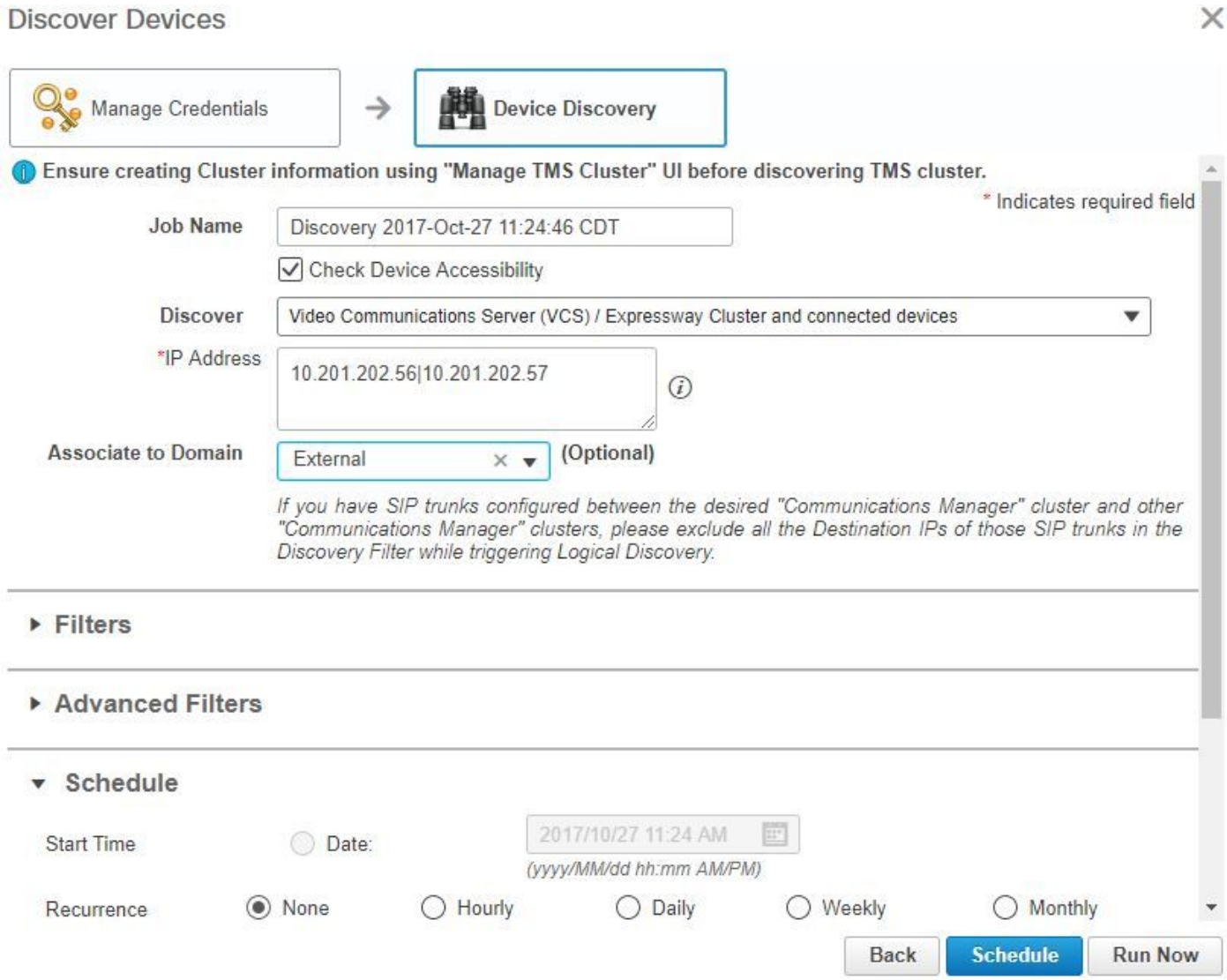
Observação: quando você descobre o VCS/TMS nesse cenário, o processo de descoberta é importante. Se você tiver um gerenciador de chamadas em sua configuração, descubra primeiro o condutor e depois o Cisco Call Manager.

Etapa 2. Navegue para Inventory > Inventory Management > Manage Credentials > Selecione Add e insira as informações para seu TMS, enquanto cria um perfil de credencial separado para seus VCSs, como mostrado na imagem.



Etapa 3. Depois que o perfil de credencial for criado, selecione Device Discovery, insira os endereços ip e, na guia Discovery, selecione VCS e descubra os dispositivos VCS. Além disso,

selecione TMS para o TMS e insira seu endereço IP. Clique em Executar agora como mostrado na imagem.

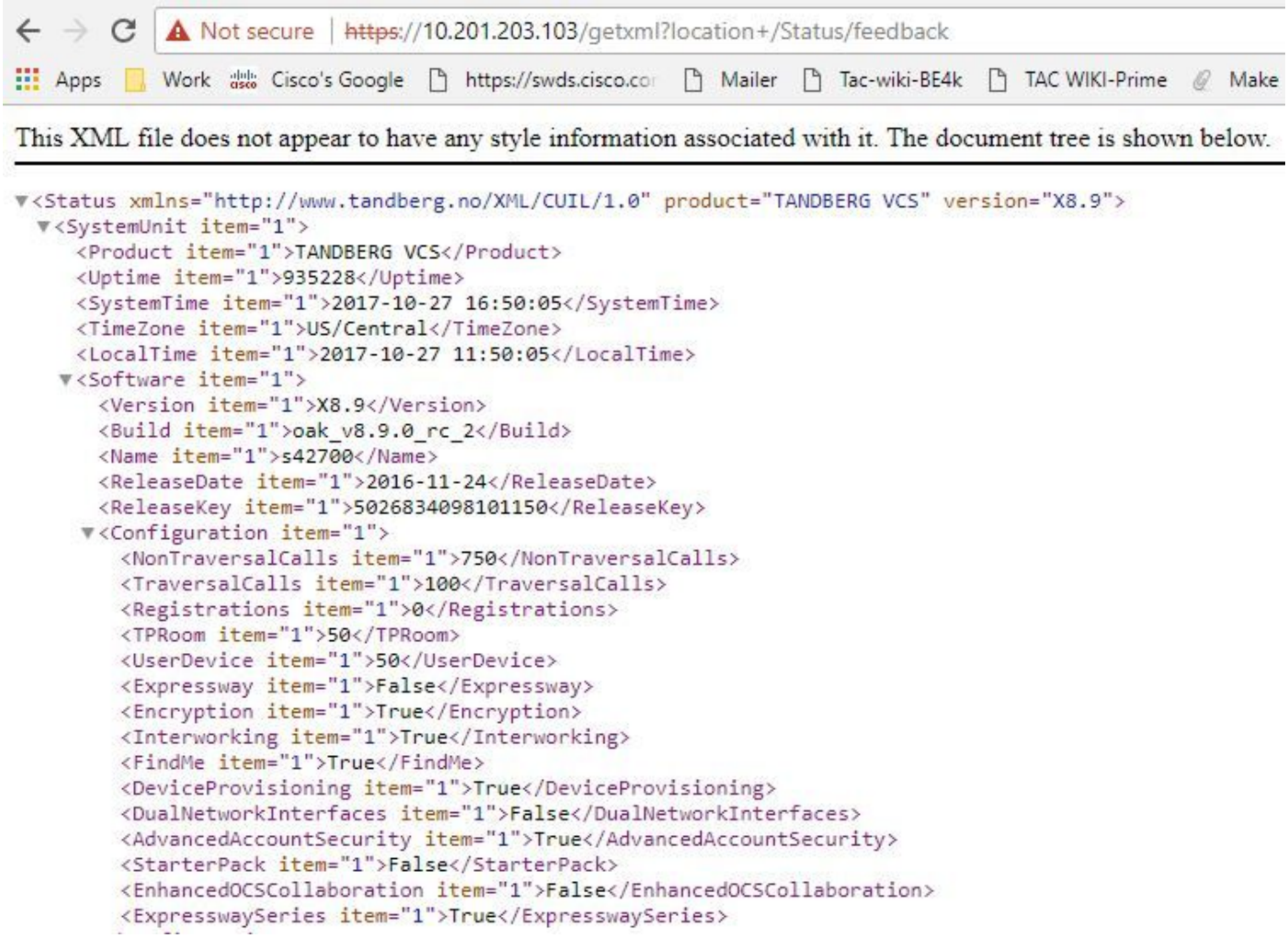


Etapa 4. Verifique se o VCS e o TMS estão em um estado Gerenciado.

Observação: se o VCS ou TMS não estiver em um estado gerenciado, na maioria das vezes é devido ao HTTP ou SNMP, se for necessária mais assistência, abra um caso de TAC para colocar o VCS/TMS em um estado Gerenciado.

Observação: use esta url e substitua o IP_Address _of_VCS_Server pelo endereço IP apropriado quando o VCS estiver em um estado Gerenciado.O servidor PCA deve ser registrado como um servidor de feedback para o VCS, isso garante que quando uma sessão de conferência termina, não há nenhum problema com os dados que o VCS envia de volta para o PCA.

https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedback , as credenciais http são solicitadas e, depois de inseridas, você deve receber uma resposta como mostrado na imagem.



Observação: se o Prime Collaboration não estiver inscrito no VCS por meio da assinatura de feedback de HTTP, ele não deverá ser notificado pelo VCS quando um endpoint registrado ingressar ou sair de uma sessão, ou se registrar ou cancelar o registro no VCS. Nesse caso, defina a visibilidade desses endpoints como completa ou limitada, conforme necessário, e verifique se o VCS está em um estado Gerenciado.

Etapa 5. Navegue para Inventory > Inventory Schedule > Cluster Data Discovery Schedule e selecione Run Now.

Observação: esse processo pode levar algum tempo, pois executa essa função em todos os dispositivos de infraestrutura. Portanto, se ele não for concluído após alguns minutos, verifique novamente após 1 a 2 horas. Sistemas muito grandes podem levar até 4 horas. É importante mencionar no inventário de PCA se há endpoints nos quais você deseja ter estatísticas de conferência suportadas e se você também garante que elas sejam gerenciadas para que relatórios e todas as estatísticas mostrem as informações apropriadas.

Para obter uma lista de dispositivos suportados de acordo com o APC com relação às conferências e nossas sessões suportadas, consulte a seção Informações de Apoio.

Etapa 6. Navegue até Diagnostics > Endpoint Diagnostics.

Para obter estatísticas corretas para os endpoints de conferência, você precisa definir sua visibilidade para o nível mais alto possível permitido pelo sistema.

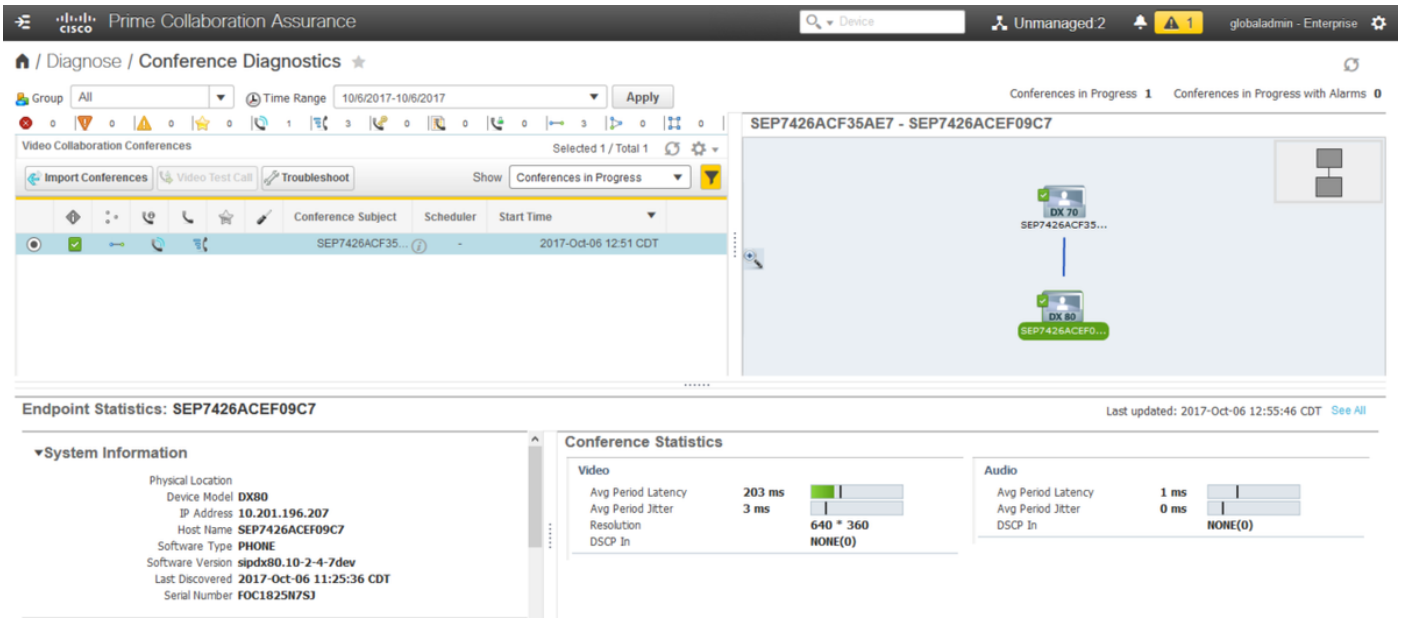
Selecione todos os pontos de extremidade que deseja monitorar no Diagnóstico de Conferência, clique em Editar Visibilidade e selecione a visibilidade máxima.

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

Observação: se você selecionar, por exemplo, 10 pontos finais e selecionar Visibilidade total, ele selecionará o nível mais alto de suporte de visibilidade por dispositivo.

Passo 7. Para testar, nNavegue até Diagnostics > Conference Diagnostics e uma conferência em andamento ou concluída será como mostrado na imagem.



Nessas conferências, você pode exibir a perda média de pacotes, a latência e o jitter para chamadas de áudio e vídeo.

Além disso, você obtém uma topologia da sessão e dos dispositivos envolvidos.

Alarmes Relacionáveis à Conferência

Para o Diagnóstico de Conferência, você pode receber três alarmes diferentes em qualquer sessão e definir seus limites:

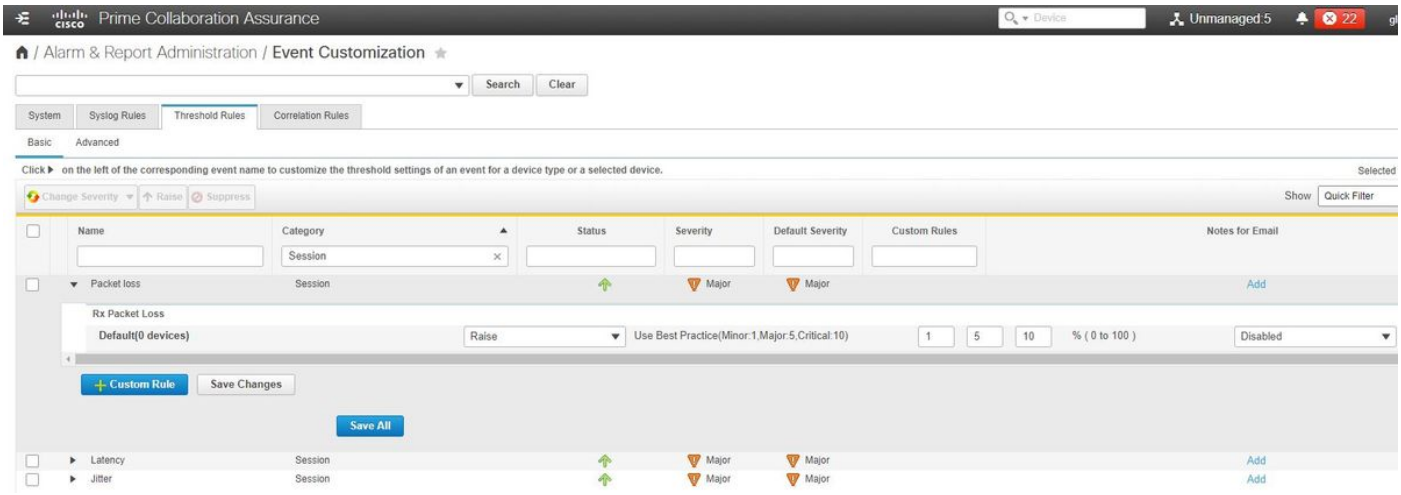
- Perda de pacote
- Latência
- Tremulação

Cada um deles você pode modificar o limite padrão, desativá-lo totalmente ou definir quais dispositivos você gostaria de associar a este alarme.

Etapa 1. Navegue até Alarm & Report Administration >Event Customization.

Etapa 2. Selecione Threshold Rules e certifique-se de que Basic esteja selecionado.

Etapa 3. Role para baixo ou filtre para a direita para a Categoria Sessão Nomeada como mostrado na imagem.



Etapa 4. Selecione a seta suspensa ao lado do alarme que deseja modificar e você poderá modificar as porcentagens Secundária, Principal ou Crítica para Perda de Pacotes, Instabilidade ou Latência.

Etapa 5. Se quiser suprimi-lo, alterne Raise para Surpress.

Etapa 6. Se quiser definir os pontos finais associados ao alarme, você deverá selecionar a opção Regra Personalizada.

Passo 7. Em seguida, selecione Tipo de dispositivo > Selecione Todos os dispositivos ou Dispositivos selecionáveis que você deseja para este alarme e clique em Salvar.

Relatórios Relacionáveis à Conferência

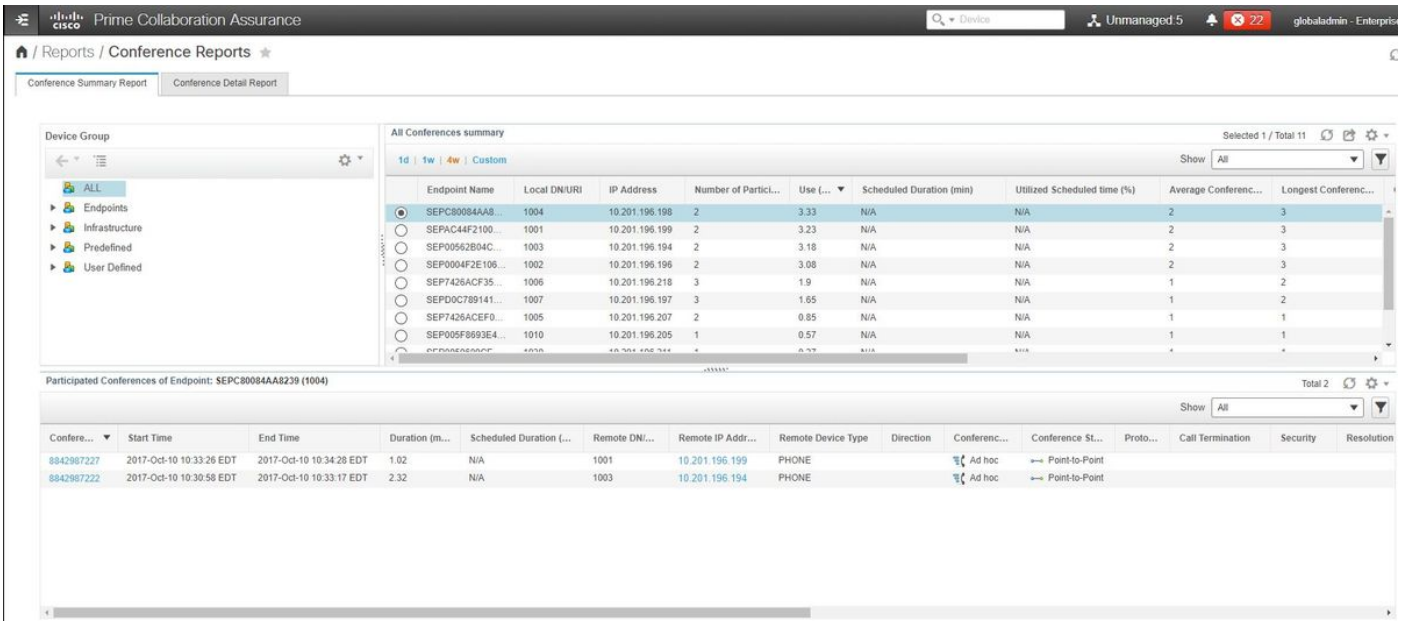
Os relatórios de Diagnóstico de Conferência podem ser recuperados e exibidos.

Há dois relatórios:

- Relatórios de conferência
- Relatórios de endpoint de telepresença

Para Relatórios de Conferência, você pode exibir uma lista de todas as conferências em um período de uma a quatro semanas ou em um período personalizado, conforme necessário.

Etapa 1. Navegue até Relatório > Relatórios de conferência conforme mostrado na imagem.



Relatórios de Resumo de Conferências

Este relatório fornece uma exibição de cada endpoint selecionado como visibilidade limitada/total e suas conferências.

As estatísticas mostradas aqui são:

- Uso Médio da Conferência
- Alarmes relacionados à conferência
- Perda média de pacotes, instabilidade e latência
- Conferência Mais Longa

Isso pode ajudá-lo a obter uma visão granular dos problemas que você pode ter em sua rede de voz/vídeo para determinar quais endpoints têm mais problemas.

Além disso, utilize sua largura de banda em correspondência por uso

Guia Relatório de detalhes de conferências

Se você encontrar um alarme para uma Conferência, poderá navegar até a guia Conference Detail Report (Relatório de detalhes da conferência).

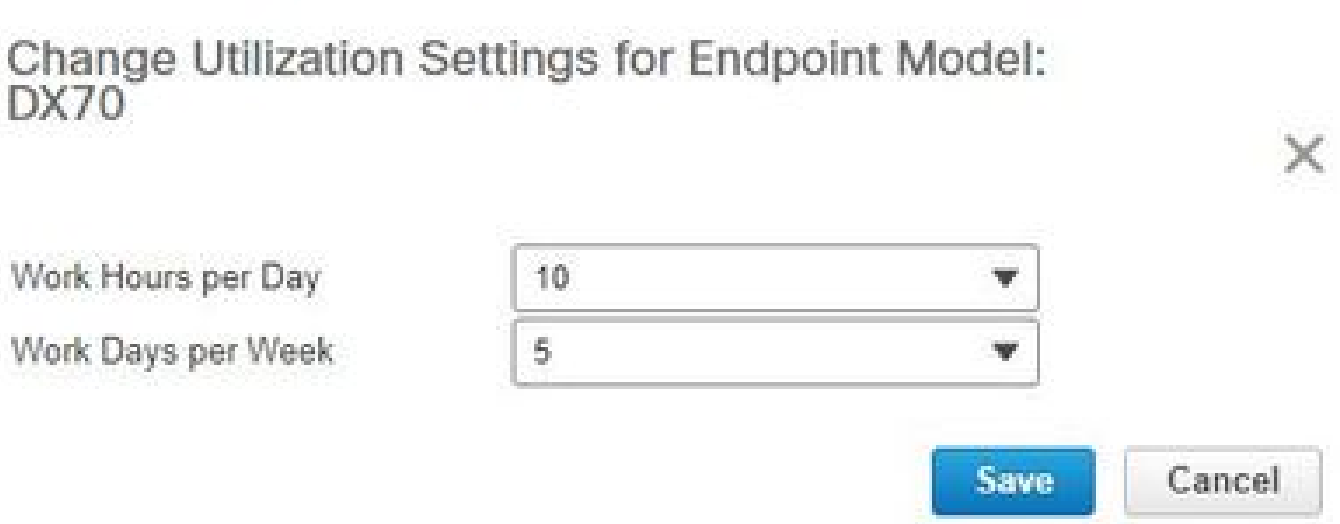
Depois de selecionar a conferência, você poderá refinar para encontrar o nome do endpoint, a versão do software e outros detalhes nos quais possa estar interessado.

Para relatórios de endpoint de telepresença, você pode exibir por endpoint o-

- Número de conferências que este dispositivo tinha
- Porcentagem de utilização
- Modelo de endpoint
- Uso

Além disso, você pode alterar os Parâmetros de Utilização pela Guia Alterar Utilização, conforme

mostrado na imagem.



Isso define os parâmetros desse dispositivo para que o sistema saiba, com base no uso, qual porcentagem exibir.

O Relatório de resumo de endpoints não exibidos exibe os endpoints que perderam conferências agendadas.

Neste gráfico, você pode exibir o Ponto de Extremidade e o Total de Conferências Agendadas, bem como o número delas que ocorreram e não foram mostradas.

Chamada de Teste de Vídeo de Conferência

Você pode criar chamadas de teste de vídeo ponto a ponto entre dois endpoints de vídeo que estão em um estado gerenciado, para testar sua rede. Você pode ver eventos e alarmes, estatísticas de sessão, estatísticas de endpoint e topologia de rede. Somente os codecs das séries CTS, C e EX são suportados para esta chamada.

Além disso, isso pode ser usado para validar se toda a funcionalidade está correta com o diagnóstico de conferência.

Pré-requisitos

- Este recurso não é suportado para a série de codecs E20.
- Para usar esse recurso, as credenciais da CLI devem ser adicionadas para os endpoints.
- Verifique se os pontos de extremidade estão registrados e se JTAPI está habilitado para pontos de extremidade (se estiverem registrados no Unified CM).
- O recurso Video Test Call não estará disponível se você tiver implantado o Cisco Prime Collaboration no modo MSP.

Etapa 1. Navegue até Diagnostics > Endpoint Diagnostics.

Etapa 2. Selecione dois endpoints aplicáveis de acordo com os pré-requisitos.

Etapa 3. Selecione Run Tests > Video Test Call.

Etapa 4. Você pode agendar a chamada de teste de vídeo para ser executada agora ou em um cronograma de recorrência.

Etapa 5. Esta chamada de teste de vídeo é exibida na tela Diagnóstico de conferência.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

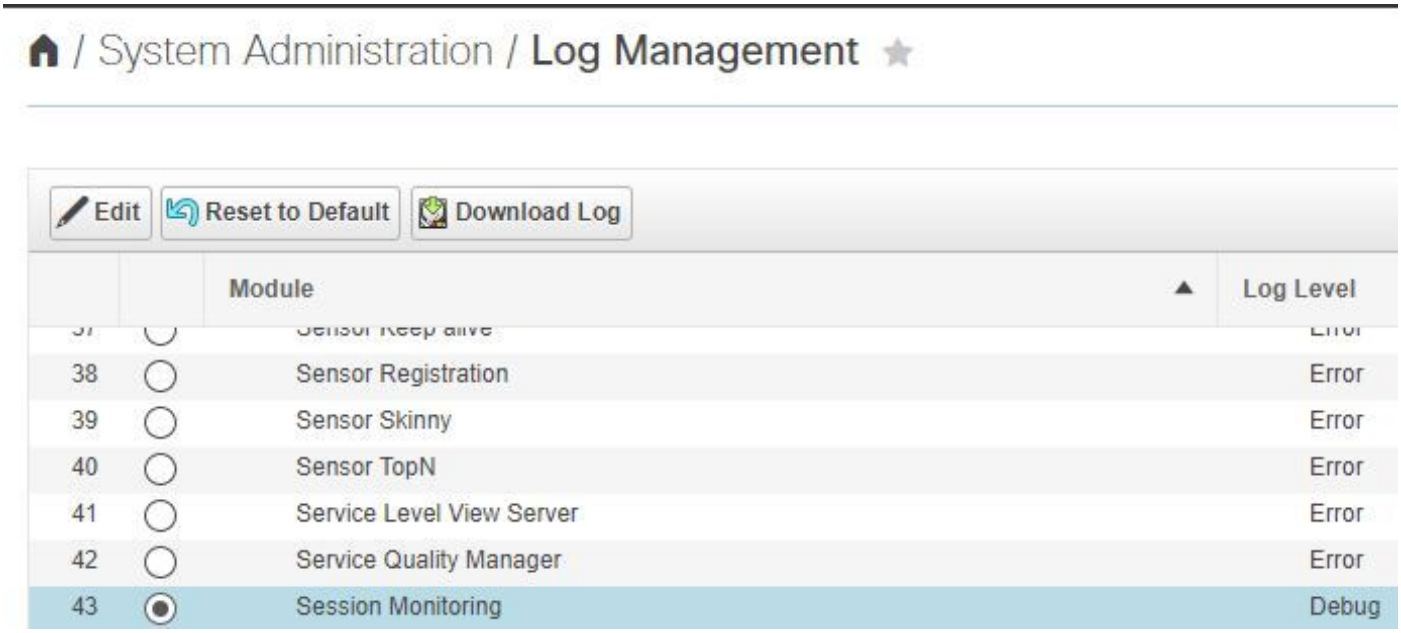
Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Registros a serem coletados para solução de problemas

Etapa 1. Navegue até System Administration > Log Management.

Etapa 2. Role para baixo até o módulo e selecione Monitoramento de sessão e selecione Editar como mostrado na imagem.



Etapa 3. Altere o nível de log para depurar e clique em Salvar.

Etapa 4. Reproduza o problema e, em seguida, volte para a tela Gerenciamento de logs.

Etapa 5. Depois de reproduzir o problema, selecione Monitoramento de sessão e Log de download.

Etapa 6. Depois de fazer o download, extraia o arquivo zip.

Passo 7. Abra o arquivo zip e navegue até os locais para obter logs úteis:

/opt/emms/emsam/log/SessionMon/

- CUCMJTAPI.log
- CUCMJTAPIDiag.log
- CSMTracker
- CSMTrackerDiag.log
- CSMTrackerDataSource.log
- PostInitSessionMon.log

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.