Configuration de Prime Collaboration Assurance (PCA) - Diagnostics de conférence

Table des matières

Introduction

Ce document décrit comment configurer et configurer votre déploiement pour les diagnostics de conférence dans Prime Collaboration Assurance (PCA) afin de surveiller de manière proactive les statistiques de conférence vocale/vidéo.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connexion à Call Manager Admin
- Connexion PCA
- Votre serveur de surveillance Telepresence (TMS)

- Identifiants Core/Expressway, le cas échéant

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions 11.x - 12.x de PCA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Cisco Prime Collaboration 11.x prend en charge les types de visibilité suivants :

- Visibilité totale : la détection d'appels avec l'utilisation de commentaires JTAPI/HTTP et d'informations de surveillance en temps réel, telles que les statistiques et les informations de conférence, est prise en charge.
- Visibilité limitée : la détection automatique des appels s'effectue à l'aide des commentaires JTAPI/HTTP, mais les informations de surveillance en temps réel telles que les statistiques et les informations de conférence ne sont pas prises en charge. Les terminaux dont la visibilité est limitée sont indiqués par une icône semi-grisée dans la topologie de conférence.

Cisco Prime Collaboration 12.x prend en charge les types de visibilité suivants :

- Visibilité totale : la détection d'appels avec l'utilisation de commentaires JTAPI/HTTP et d'informations de surveillance en temps réel, telles que les statistiques et les informations de conférence, est prise en charge.
- Aucune visibilité : la détection d'appels avec l'utilisation de commentaires JTAPI/HTTP et d'informations de surveillance en temps réel n'est pas prise en charge. Ces points de terminaison sont affichés sur la page Surveillance des conférences avec une icône entièrement grisée.

Limitation des terminaux définis sur une visibilité limitée ou complète par OVA

- Small Open Virtualization Archive (OVA) prend en charge jusqu'à 500 terminaux
- OVA moyen prend en charge jusqu'à 1 000 terminaux
- Grand OVA prend en charge jusqu'à 1 800 terminaux
- OVA très grand prend en charge jusqu'à 2 000 terminaux

La liste des périphériques pris en charge par PCA en ce qui concerne les conférences et nos sessions prises en charge est indiquée dans le tableau ci-dessous.

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.

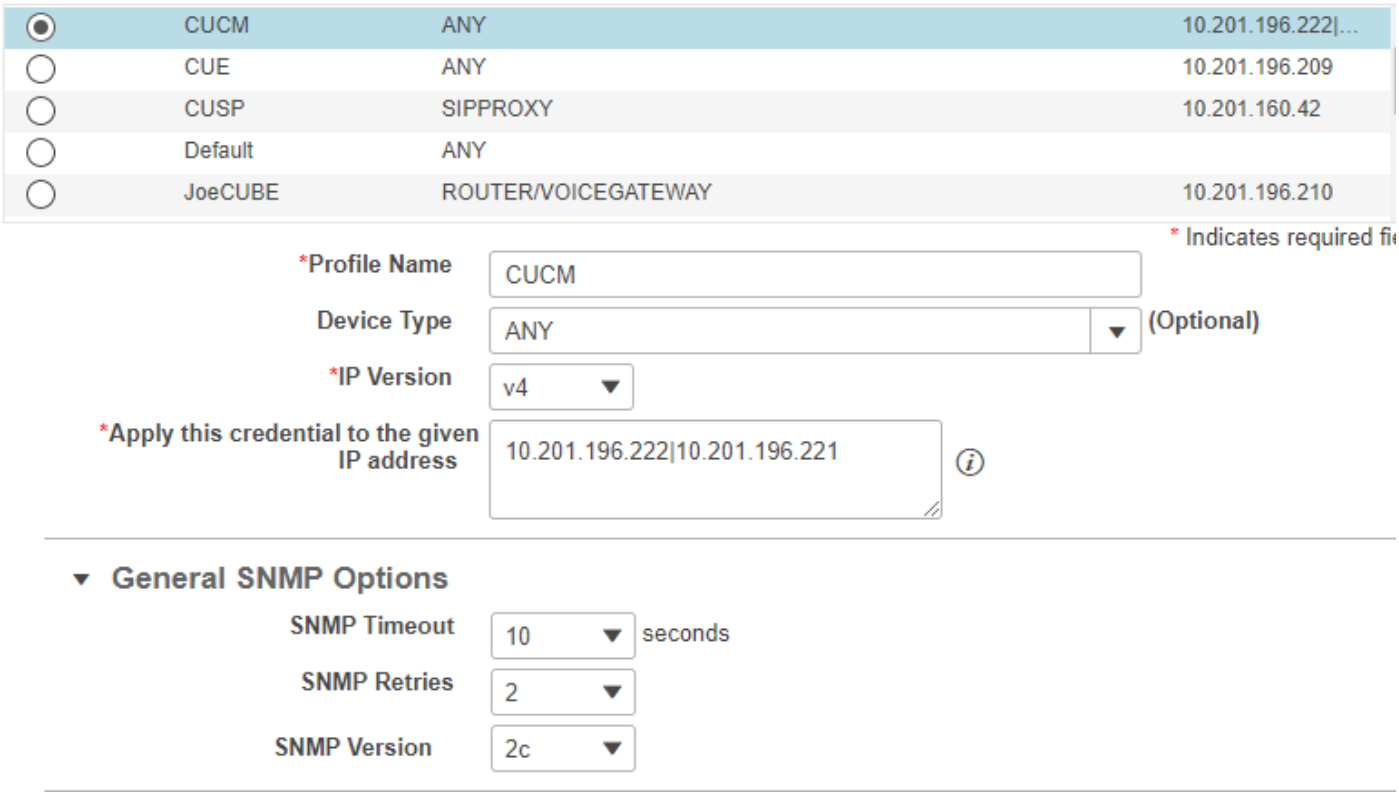
Configurer

Scénario 1. Conférence avec terminaux vidéo enregistrés auprès du gestionnaire d'appels

Étape 1. Vous devez d'abord vous assurer que les gestionnaires d'appels sont à l'état Géré.

Accédez à Inventory > Inventory Management > Manage Credentials > Create a profile for the Call Manager cluster.

Remarque : n'oubliez pas que chaque profil d'informations d'identification utilise les mêmes informations d'identification pour chaque adresse IP répertoriée dans le profil. Ainsi, si vous répertoriez le serveur de publication et l'abonné Call Manager dans le même profil d'informations d'identification, il utilise ces mêmes informations d'identification pour découvrir les deux adresses IP. Si vous avez un conducteur dans votre configuration, découvrez d'abord le conducteur, puis Cisco Call Manager, comme illustré dans l'image.



Étape 2. Vérifiez que vous avez configuré les informations d'identification HTTP (Hypertext Transfer Protocol), SNMP (Simple Name Management Protocol) et JTAPI (Java Telephony API)

En outre, vous devez activer le service Cisco Computer Telephony Integration (CTI) dans Call Manager Serviceability.

Configuration de Cisco Unified Communications Manager

Activer HTTP

Vous n'avez pas besoin de créer un nouvel utilisateur si vous souhaitez autoriser Cisco Prime Collaboration à utiliser les informations d'identification d'administrateur pour vous connecter. Par ailleurs, si vous souhaitez autoriser Cisco Prime Collaboration Manager à utiliser les informations d'identification appropriées pour vous connecter à Cisco Unified Communications Manager, vous devez créer un groupe d'utilisateurs HTTP et un utilisateur correspondant que Cisco Prime Collaboration peut utiliser pour communiquer.

Pour créer un utilisateur, procédez comme suit :

Étape 1. Connectez-vous à l'interface Web Administration de Cisco Unified CM avec votre compte administrateur.

Étape 2. Créez un groupe d'utilisateurs avec des privilèges suffisants. Accédez à User Management>User Settings>Access Control Group et créez un nouveau groupe d'utilisateurs avec un nom approprié, PC_HTTP_Users dans ce cas. Maintenant, sélectionnezEnregistrer.

Étape 3. Accédez à Gestion des utilisateurs>Paramètres utilisateur>Groupe de contrôle d'accès et sélectionnezRechercher. Recherchez le groupe que vous avez défini et cliquez sur l'icône à droite.

Étape 4. Sélectionnez Affecter un rôle au groupe et sélectionnez les rôles suivants :

- Accès API AXL standard
- Utilisateurs admin CCM standard
- Administration de la FACILITÉ de MAINTENANCE standard

Étape 5. Cliquez sur Save.

Étape 6. Dans le menu principal, accédez à Gestion des utilisateurs>Utilisateurs de l'application>Créer un nouvel utilisateur.

Spécifiez un mot de passe approprié sur la page Configuration utilisateur de l'application. Vous pouvez sélectionner uniquement certains types de périphériques dans la zone de texte Périphériques disponibles ou autoriser Cisco Prime Collaboration à surveiller tous les périphériques

Étape 7. Dans la section Informations d'autorisation, sélectionnez Ajouter au groupe d'utilisateurs et sélectionnez le groupe créé à l'étape 1 (par exemple, PC_HTTP_Users).

Étape 8. Cliquez sur Enregistrer. La page est actualisée et les privilèges appropriés s'affichent.

Activer SNMP

SNMP n'est pas activé par défaut dans Cisco Unified Communications Manager.

Afin d'activer SNMP :

Étape 1. Connectez-vous à la vue Cisco Unified Serviceabilityview dans l'interface utilisateur graphique Web de Cisco Unified Communications Manager.

Étape 2. Accédez à Outils > Activation de service.

Étape 3. Sélectionnez Serveur Publisher.

Étape 4. Accédez à Performance > Monitoring Services et activez la case à cocher Cisco Call Manager SNMP Service.

Étape 5. Sélectionnez Save en bas de l'écran.

Afin de créer une chaîne de communauté SNMP :

Étape 1. Connectez-vous à Cisco Unified Serviceabiliséconsultez l'interface utilisateur graphique Web de Cisco Unified Communications Manager.

Étape 2. Dans le menu principal de la vue Cisco Unified Serviceability, accédez à SNMP > v1/v2c > Community String.

Étape 3. Sélectionnez un serveur et cliquez sur Rechercher.
Si la chaîne de communauté est déjà définie, le nom de la chaîne de communauté s'affiche dans les résultats de la recherche.

Étape 4. Cliquez sur Ajouter nouveau pour ajouter une nouvelle chaîne si aucun résultat n'est affiché.

Étape 5. Spécifiez les informations SNMP requises et enregistrez la configuration.

Remarque : seul l'accès en lecture seule (RO) SNMP est nécessaire.

Démarrer le service CTI

Exécutez la procédure pour le noeud Cisco Unified Communications Manager que vous souhaitez, il est préférable de définir sur deux noeuds.

Étape 1. Connectez-vous à Cisco Unified Serviceability, affiché dans l'interface utilisateur graphique de Cisco Unified Communications Manager.

Étape 2. Accédez à Outils > Activation de service.

Étape 3. Sélectionnez un serveur dans la liste déroulante.

Étape 4. Dans la section CM Services, cochez la case Cisco CTI Manager.

Étape 5. Sélectionnez Save en haut de l'écran

Créer un utilisateur d'application pour le contrôle CTI PCA (utilisateur JTAPI)

JTAPI est utilisé pour récupérer les informations d'état de session à partir du périphérique. Vous devez créer un utilisateur Application pour le contrôle CTI dans le processeur d'appels avec l'autorisation requise pour recevoir des événements JTAPI sur les terminaux. Prime Collaboration gère plusieurs clusters de traitement des appels. Vous devez vous assurer que les ID de cluster sont uniques. Créez un nouvel utilisateur Application pour aider Cisco Prime Collaboration à obtenir les informations requises.

Pour créer un nouvel utilisateur d'application JTAPI, procédez comme suit :

Étape 1. Connectez-vous à l'interface Web Administration de Cisco Unified CM via votre compte d'administrateur.

Étape 2. Créez un groupe d'utilisateurs avec des privilèges suffisants. Accédez à User Management>User Settings>Access Control Group et créez un nouveau groupe d'utilisateurs avec un nom approprié, PC_HTTP_Users dans ce cas. Maintenant, sélectionnezEnregistrer.

Étape 3. Choisissez User Management>User Settings>Access Control Group et cliquez sur Find. Recherchez le groupe que vous avez défini et sélectionnez l'icône à droite.

Étape 4. Cliquez sur Attribuer un rôle au groupe et sélectionnez les rôles suivants :

- CTI standard permettant la surveillance des appels
- CTI standard activé

- CTI standard permettant le contrôle des téléphones prenant en charge Connected Xfer et conf

Étape 5. Sélectionnez Enregistrer.

Étape 6. Dans le menu principal, accédez à Gestion des utilisateurs>Utilisateurs de l'application>Créer un nouvel utilisateur.
Spécifiez un mot de passe approprié sur la page Configuration utilisateur de l'application. Vous pouvez sélectionner certains types de périphériques dans la zone de texte Périphériques disponibles ou autoriser Cisco Prime Collaboration à surveiller tous les périphériques.

Remarque : le mot de passe ne doit pas contenir de point-virgule (;) ni être égal à (=).

Étape 7. Dans la section Informations d'autorisation, sélectionnez Ajouter au groupe de contrôle d'accès et sélectionnez le groupe qui a été créé à l'étape 1. (par exemple, PC_HTTP_Users).

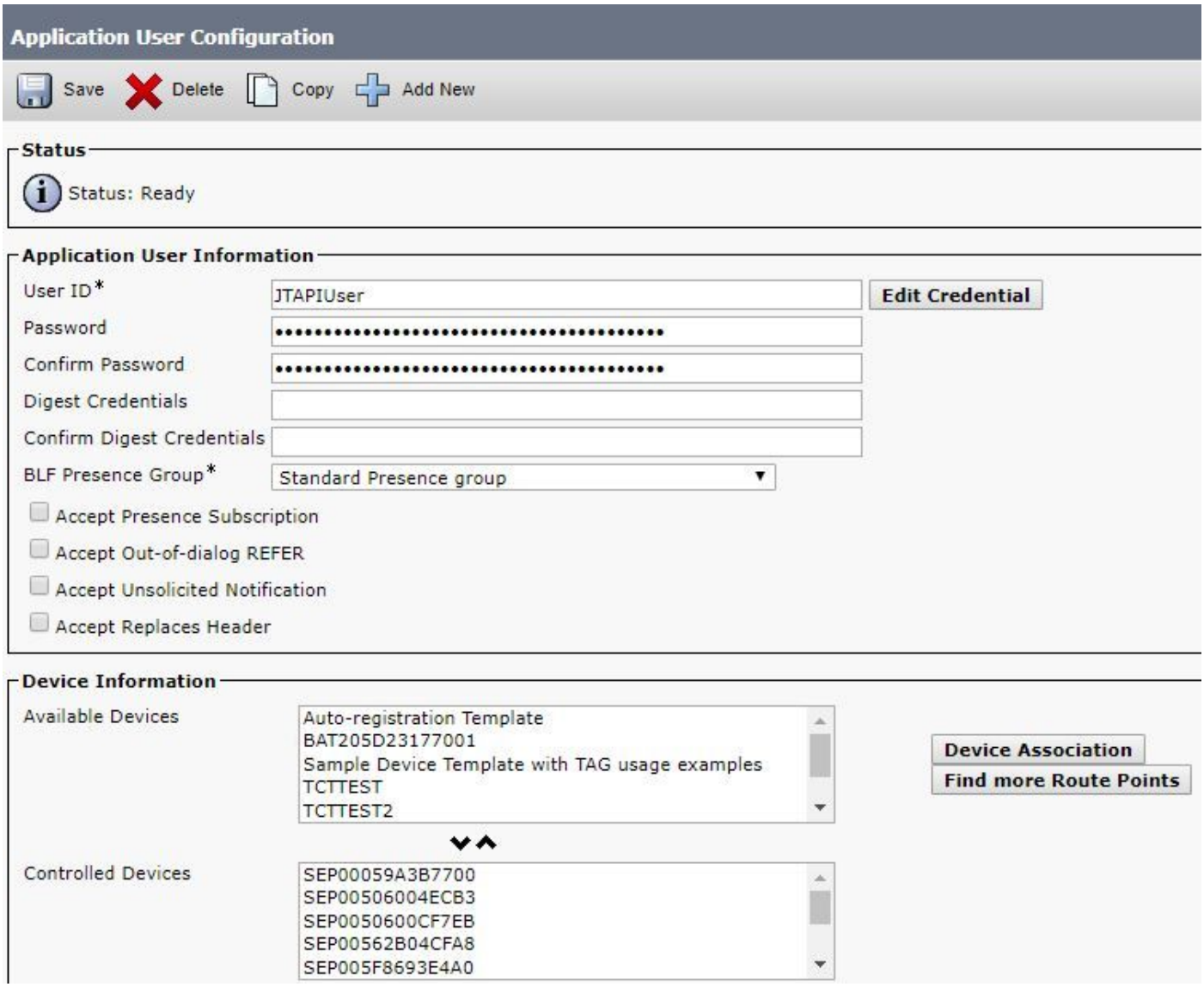
Étape 8. Cliquez sur Enregistrer. La page est actualisée et les privilèges appropriés s'affichent.

Remarque : si le gestionnaire d'appels a été géré avant l'ajout de l'utilisateur JTAPI, assurez-vous que l'utilisateur JTAPI est ajouté dans le profil d'informations d'identification du gestionnaire d'appels et redécouvrez-le.

Suite du scénario 1. Étapes :

Étape 3. Accédez à l'utilisateur de l'application JTAPI Call Manager que vous avez créé et déplacez les terminaux pris en charge de Périphériques disponibles vers Périphériques contrôlés.

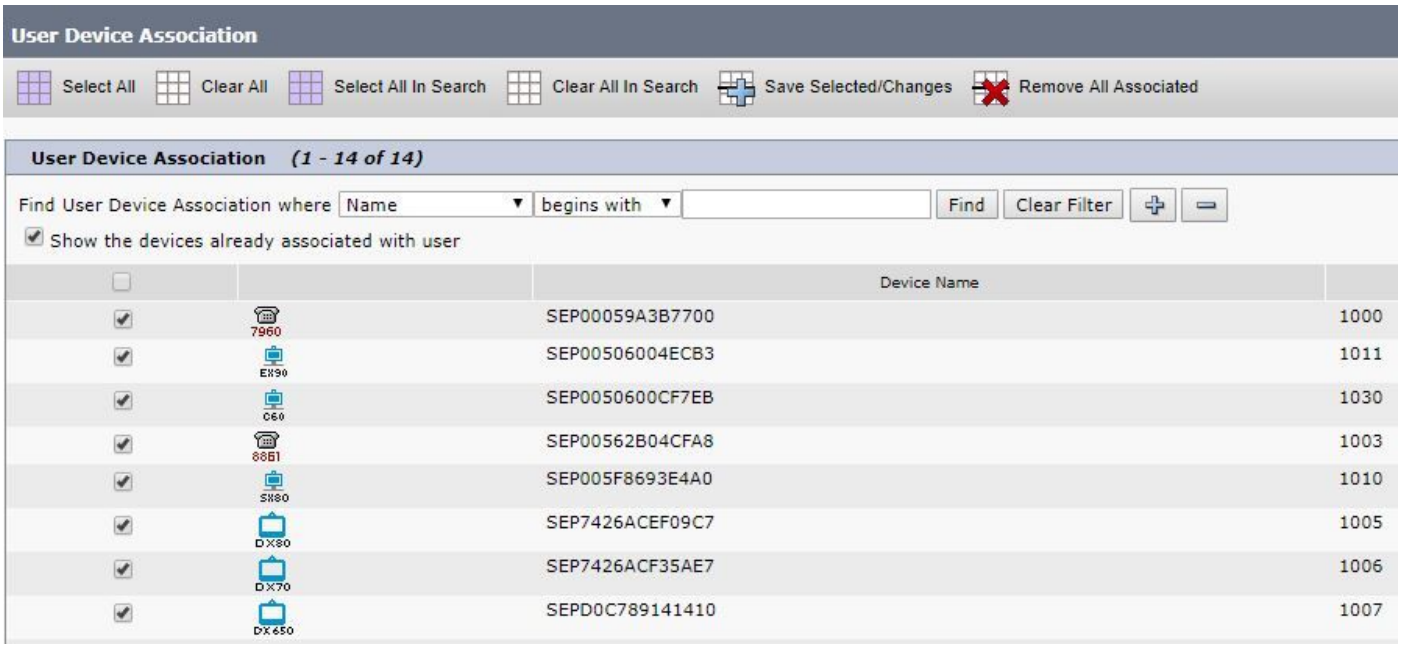
Pour ce faire, utilisez la fonction Association de périphériques, comme illustré dans l'image.



Si vous vous référez à la limitation des terminaux définis sur une visibilité limitée ou complète par OVA, vous pouvez vérifier la quantité de périphériques que vous avez ajoutée à la taille OVA.

Dans cet écran, vous pouvez filtrer par nom de périphérique, description ou numéro de répertoire pour vous aider à gérer et à filtrer ces périphériques comme illustré dans l'image.

Il est utile de noter ces périphériques tels qu'ils sont ajoutés à l'étape 7.



Assurez-vous également que les rôles utilisateur corrects sont ajoutés pour cet utilisateur JTAPI :

- CTI standard permettant la surveillance des appels
- CTI standard activé
- CTI standard Autorise le contrôle des téléphones prenant en charge Connected Xfer et conf, comme illustré dans l'image.

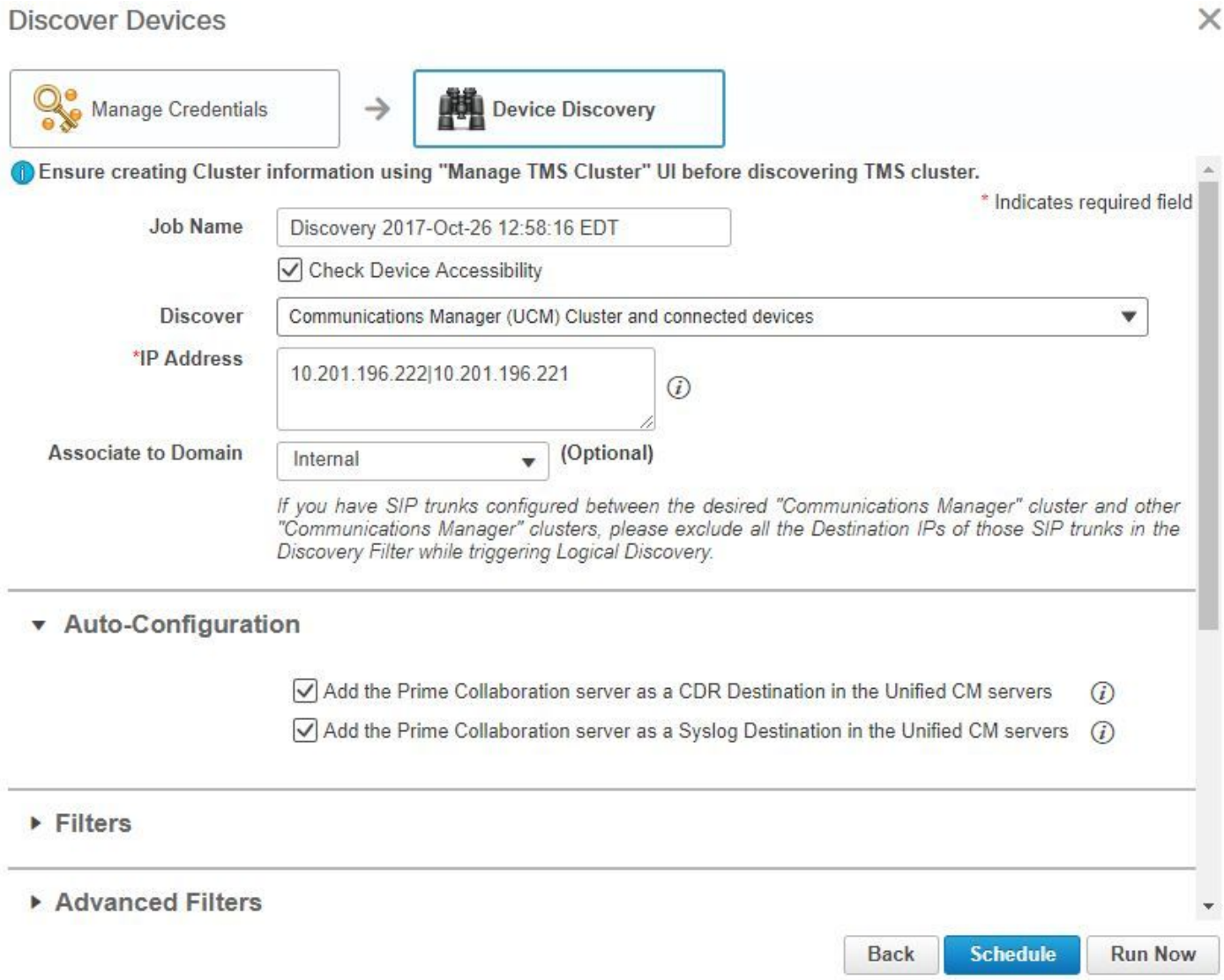
Pour obtenir la liste des périphériques pris en charge par PCA, en ce qui concerne les conférences et nos sessions prises en charge, reportez-vous à la section Informations générales.

Remarque : assurez-vous également que la case Autoriser le contrôle du périphérique à partir de CTI est cochée sur les périphériques contrôlés par l'utilisateur de l'application CTI, sous Informations sur le périphérique, comme illustré dans l'image.

Remarque : il est important de noter avant de continuer que si vous avez enregistré les

terminaux auprès de Call Manager et que Call Manager est intégré à VCS/TMS, vous découvrez d'abord votre VCS/TMS, puis votre Call Manager en dernier. Ainsi, du point de vue de l'inventaire, l'ensemble de votre infrastructure est mappé au bon emplacement. En outre, lorsque vous détectez le VCS/TMS, assurez-vous de remplacer l'onglet de détection par défaut par le périphérique correspondant de TMS/VCS ou Call Manager.

Étape 4. Ensuite, dans PCA, sélectionnez Device Discovery et entrez les adresses IP de vos Call Managers, activez les deux cases à cocher sur Auto-Configuration et sélectionnez Run Now comme indiqué dans l'image.



Étape 5. Une fois que les Call Managers sont à l'état Géré, passez à l'étape 6.

Remarque : si le Call Manager n'est pas dans un état géré, c'est la plupart du temps dû à HTTP ou SNMP, si une assistance supplémentaire est nécessaire, ouvrez un dossier TAC pour obtenir le Call Manager dans un état Managed.

Étape 6. Accédez à Inventory > Inventory Schedule > Cluster Data Discovery Schedule et sélectionnez Run Now.

Remarque : cela dépend du nombre d'appareils enregistrés/non enregistrés dont vous disposez. Ce processus peut prendre de quelques minutes à quelques heures. Vérifiez tout au long de la journée en actualisant la page. En outre, cela permet de mapper votre cluster Call Manager et de récupérer tous vos terminaux. Une fois cette opération terminée, passez à l'étape suivante.

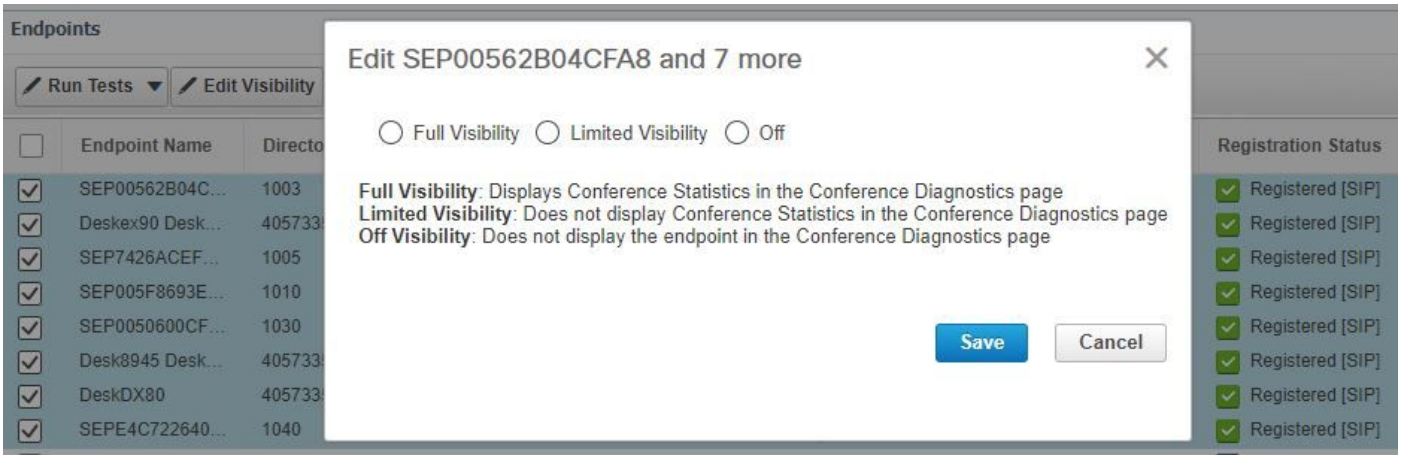
Remarque : il est important de mentionner dans l'inventaire PCA s'il existe des terminaux pour lesquels vous souhaitez que les statistiques de conférence soient prises en charge. Assurez-vous qu'ils sont bien gérés pour les rapports et toutes les statistiques, afin d'afficher les informations correctes.

Étape 7. Naviguez jusqu'à Diagnose > Endpoint Diagnostics.

Afin d'obtenir des statistiques à jour pour vos terminaux de conférence, vous devez définir leur visibilité au niveau le plus élevé possible autorisé par le système.

Sélectionnez tous les points d'extrémité que vous souhaitez surveiller dans les Diagnostics de conférence, puis cliquez sur Modifier la visibilité et sélectionnez Visibilité complète comme illustré dans l'image.

La section Visibilité limitée affiche uniquement le périphérique dans la topologie, mais pas de statistiques. Elle ne peut pas récupérer les alarmes applicables aux périphériques associés aux diagnostics de conférence.

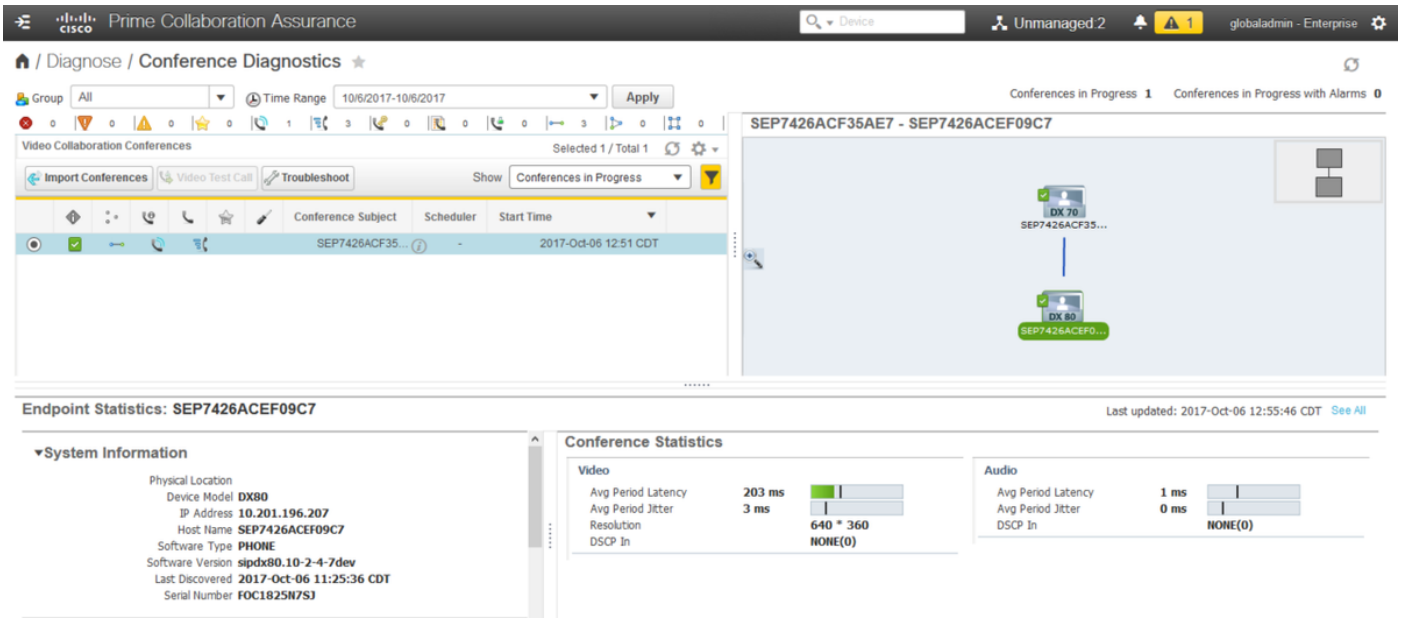


The following table lists the default and maximum visibility details for the endpoints:

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

Remarque : si vous sélectionnez, par exemple, 10 terminaux et que vous sélectionnez une visibilité totale, vous sélectionnez le niveau le plus élevé de visibilité prise en charge par périphérique.

Étape 8. Pour tester, accédez à Diagnostiquer > Diagnostics de conférence et une conférence en cours ou terminée s'affiche, comme illustré dans l'image.



Dans ces conférences, vous pouvez afficher la perte moyenne de paquets, la latence et la gigue pour les appels audio et vidéo.

Obtenez également une topologie de la session et des périphériques concernés.

Actuellement, les diagnostics de conférence extraient les informations basées sur les DN et si votre environnement a des DN partagés, PCA récupère le premier qu'il reçoit pour la conférence.

Alarmes relatives aux conférences

Pour les diagnostics de conférence, vous pouvez recevoir trois alarmes différentes pour chaque session et définir leurs seuils :

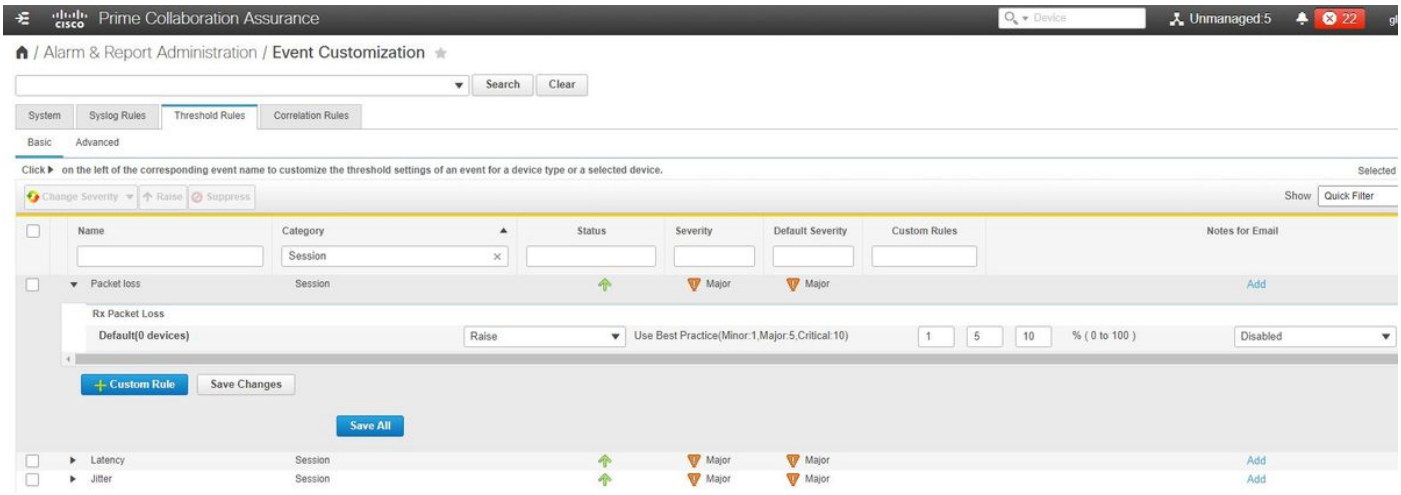
- La perte de paquets
- Latence
- Gigue

Pour chacun d'entre eux, vous pouvez modifier le seuil par défaut, le dépasser ou définir les périphériques que vous souhaitez associer à cette alarme.

Étape 1. Accédez à Administration des alarmes et des rapports > Personnalisation des événements.

Étape 2. Sélectionnez Threshold Rules et assurez-vous que Basic est sélectionné.

Étape 3. Faites défiler vers le bas ou filtrez vers la droite pour afficher la session nommée par catégorie, comme illustré dans l'image.



Étape 4. Sélectionnez la flèche de la liste déroulante en regard de l'alarme. Vous souhaitez modifier et vous pouvez modifier les pourcentages Mineur, Majeur ou Critique pour Perte de paquets, Gigue ou Latence.

Étape 5. Si vous souhaitez surpresser, sélectionnez l'option Surpresser (Raise).

Étape 6. Si vous souhaitez définir les points d'extrémité associés à l'alarme, vous pouvez sélectionner Règle personnalisée.

Étape 7. Sélectionnez ensuite Device Type > Select All Devices ou Selectable Devices que vous souhaitez pour cette alarme et cliquez sur Save.

Rapports relatifs aux conférences

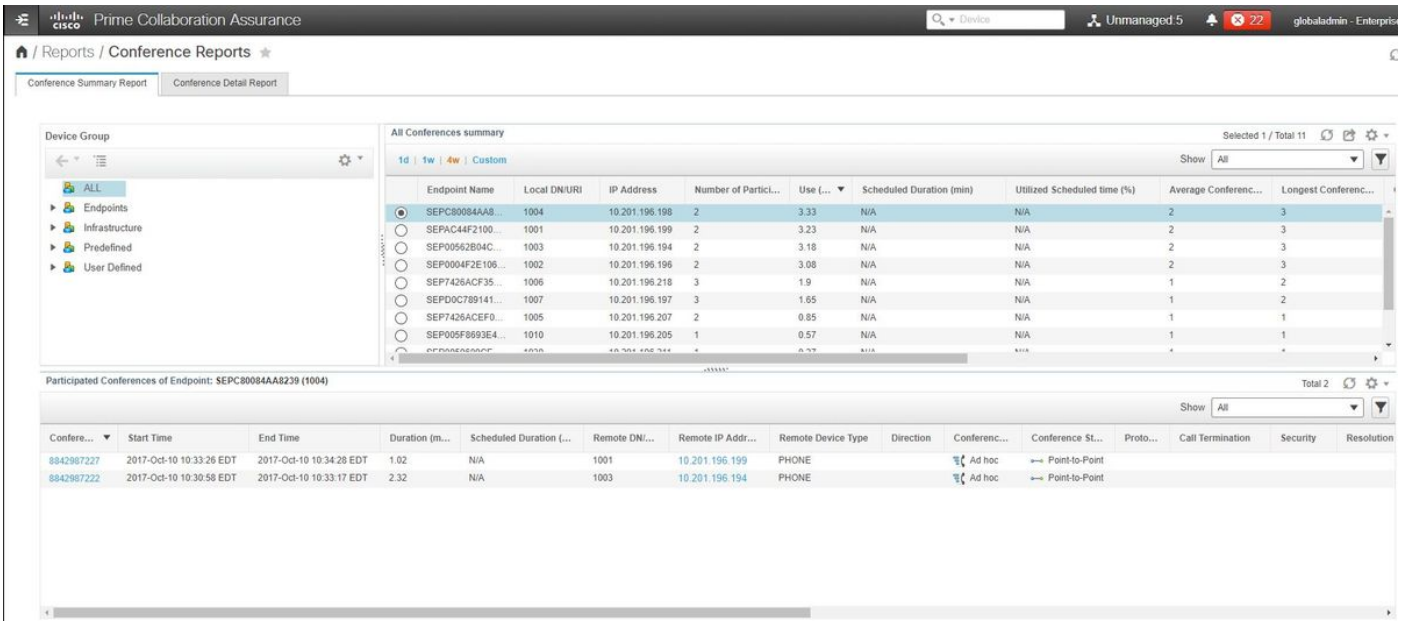
Pour les rapports de diagnostics de conférence peuvent être récupérés et affichés.

Il existe deux rapports :

- Rapports de conférence
- Rapports sur les terminaux Telepresence

Pour les rapports de conférence, vous pouvez afficher la liste de toutes les conférences dans un délai compris entre une et quatre semaines ou une période personnalisée, le cas échéant.

Étape 1. Accédez à Rapports > Rapports de conférence comme indiqué dans l'image.



Rapports récapitulatifs de conférence

Ce rapport fournit une vue de chaque terminal que vous avez sélectionné comme étant à visibilité limitée/complète et de leurs conférences.

Les statistiques présentées ici sont les suivantes :

- Utilisation moyenne des conférences
- Alarmes liées à la conférence
- Perte moyenne de paquets, gigue et latence
- Conférence la plus longue

Cela peut vous aider à obtenir une vue granulaire des problèmes que vous pouvez rencontrer au sein de votre réseau voix/vidéo afin de déterminer quels terminaux présentent le plus de problèmes.

Vous pouvez également utiliser votre bande passante pour la correspondance par utilisation.

Onglet Rapport détaillé sur la conférence

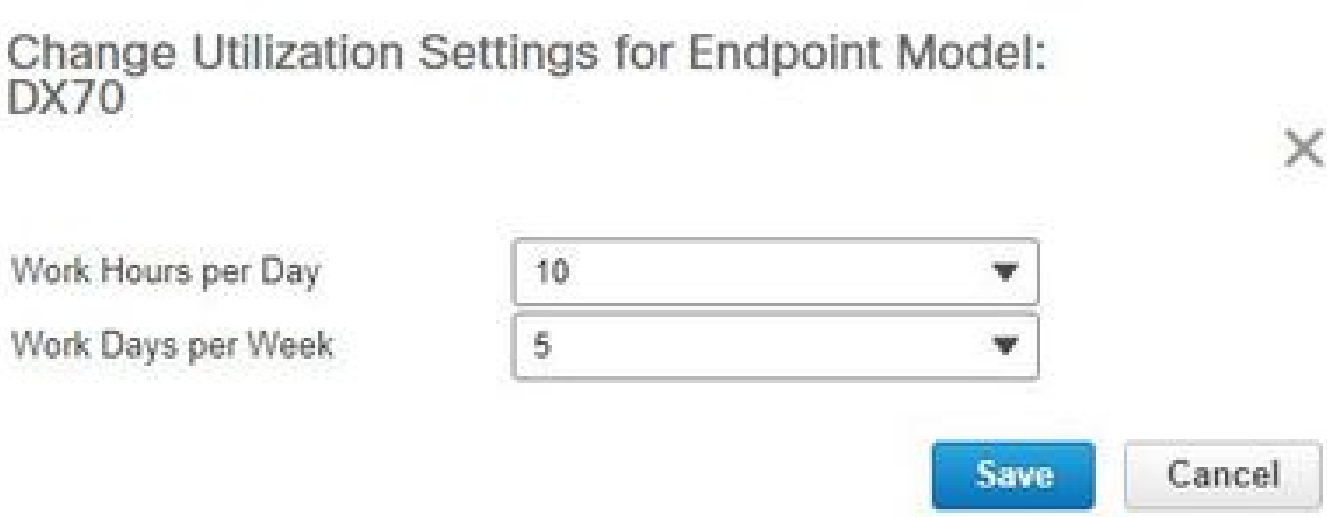
Si vous rencontrez une alarme pour une conférence, vous pouvez accéder à l'onglet Rapport détaillé de la conférence.

Une fois que vous avez sélectionné la conférence, vous pouvez l'affiner pour trouver le nom du terminal, la version du logiciel et d'autres détails susceptibles de vous intéresser.

Pour les rapports sur les terminaux de téléprésence, vous pouvez afficher les éléments suivants par terminal :

- Nombre de conférences de ce périphérique
- Pourcentage d'utilisation
- Modèle de terminal
- Utilisation

En outre, vous pouvez modifier les paramètres d'utilisation en utilisant l'onglet Modifier l'utilisation comme illustré dans l'image.



Cette option définit les paramètres de ce périphérique de sorte que le système sache quel pourcentage afficher à partir de l'utilisation.

Le rapport de synthèse No Show Endpoint affiche les terminaux qui ont manqué les conférences planifiées.

Dans ce graphique, vous pouvez également afficher le point de terminaison et le nombre total de conférences planifiées, ainsi que le nombre de conférences qui ont eu lieu et qui n'ont pas été présentées.

Appel de test vidéo de conférence

Vous pouvez créer des appels de test vidéo point à point entre deux points d'extrémité vidéo à l'état géré, pour tester votre réseau. Vous pouvez voir les événements et les alarmes, les statistiques de session, les statistiques de point de terminaison et la topologie du réseau avec des statistiques comme les autres appels. Seuls les codecs des séries CTS, C et EX sont pris en charge pour cet appel.

En outre, vous pouvez l'utiliser pour vérifier que tout fonctionne avec les diagnostics de conférence.

Conditions préalables

- Cette fonctionnalité n'est pas prise en charge pour la gamme de codecs E20.
- Pour utiliser cette fonctionnalité, des informations d'identification CLI doivent être ajoutées pour les terminaux.
- Assurez-vous que les terminaux sont enregistrés et que JTAPI est activé pour les terminaux (s'ils sont enregistrés dans Unified CM).
- La fonction Appel de test vidéo n'est pas disponible si vous avez déployé Cisco Prime Collaboration en mode MSP.

Étape 1. Naviguez jusqu'à Diagnose > Endpoint Diagnostics.

Étape 2. Sélectionnez deux points d'extrémité applicables, conformément aux conditions préalables mentionnées.

Étape 3. Sélectionnez Run Tests > Video Test Call.

Étape 4. Vous pouvez programmer l'appel de test vidéo pour qu'il s'exécute maintenant ou selon un calendrier de réoccurrence.

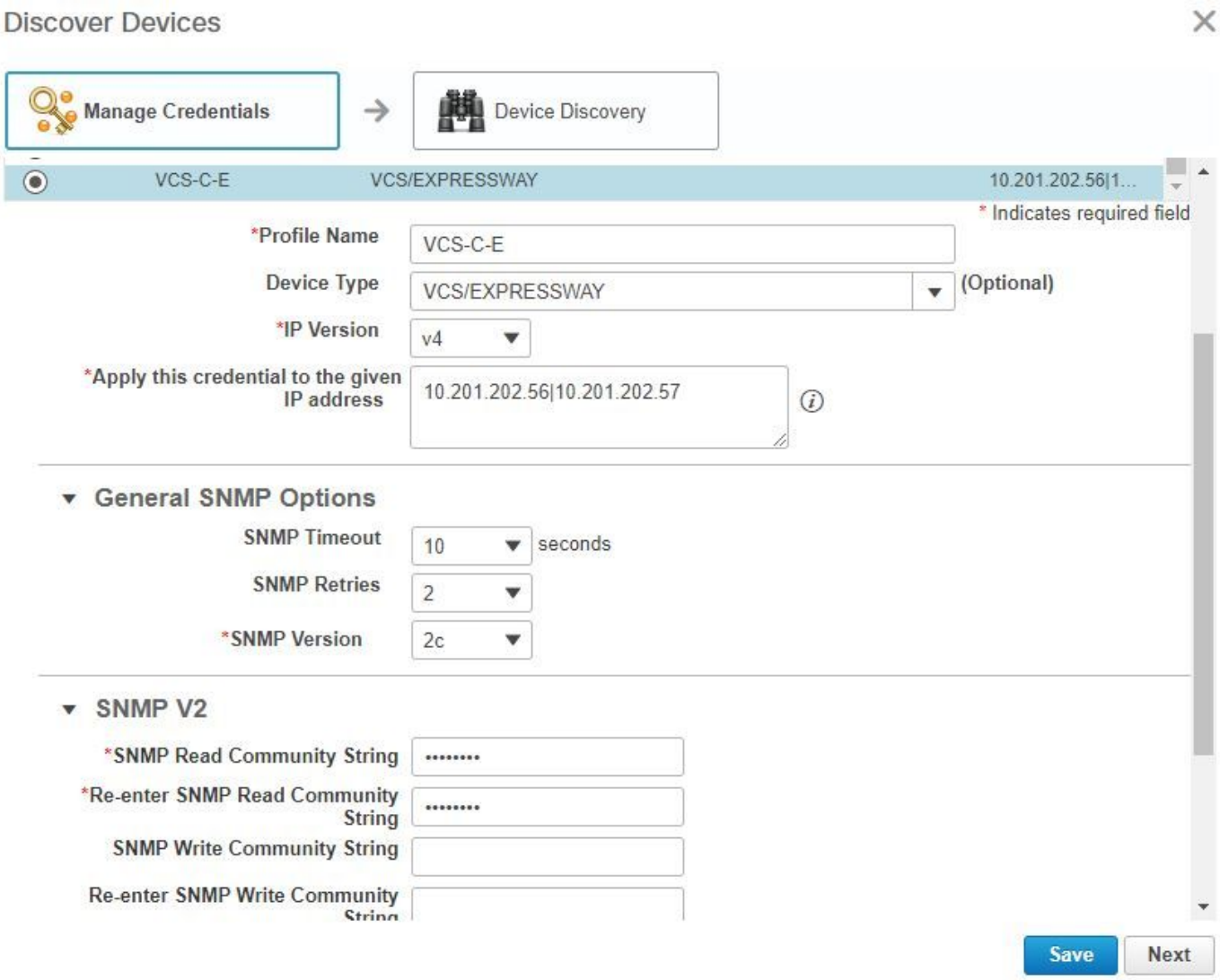
Étape 5. Cet appel de test vidéo s'affiche ensuite dans l'écran Diagnostics de la conférence.

Scénario 2. Conférence avec des terminaux enregistrés non Call Manager

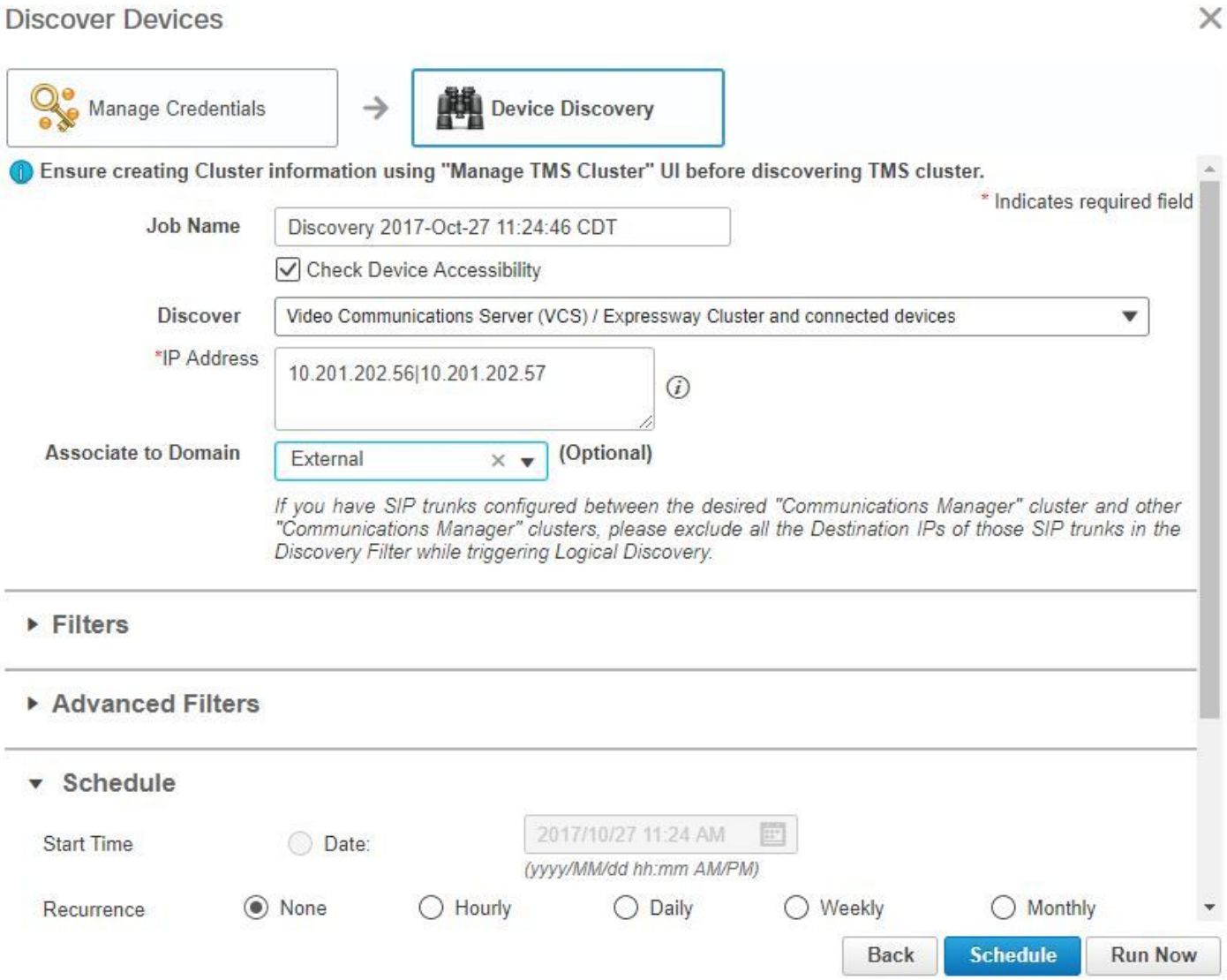
Étape 1. Assurez-vous que les informations d'identification de Telepresence Management Suite (TMS) et Video Communications Server(s) (VCS) sont disponibles.

Remarque : lorsque vous détectez votre VCS/TMS dans ce scénario, le processus de détection est important. Si vous disposez d'un gestionnaire d'appels dans votre configuration, identifiez d'abord le conducteur, puis le gestionnaire d'appels Cisco.

Étape 2. Accédez à Inventory > Inventory Management > Manage Credentials et sélectionnez Add, puis entrez les informations pour votre TMS, tandis que vous créez un profil d'informations d'identification distinct pour vos VCS, comme illustré dans l'image.



Étape 3. Une fois le profil d'informations d'identification créé, sélectionnez Device Discovery, entrez les adresses IP et dans l'onglet Discovery, sélectionnez VCS et détectez les périphériques VCS. Sélectionnez également TMS pour le TMS et entrez son adresse IP. Cliquez sur Exécuter maintenant comme indiqué dans l'image.

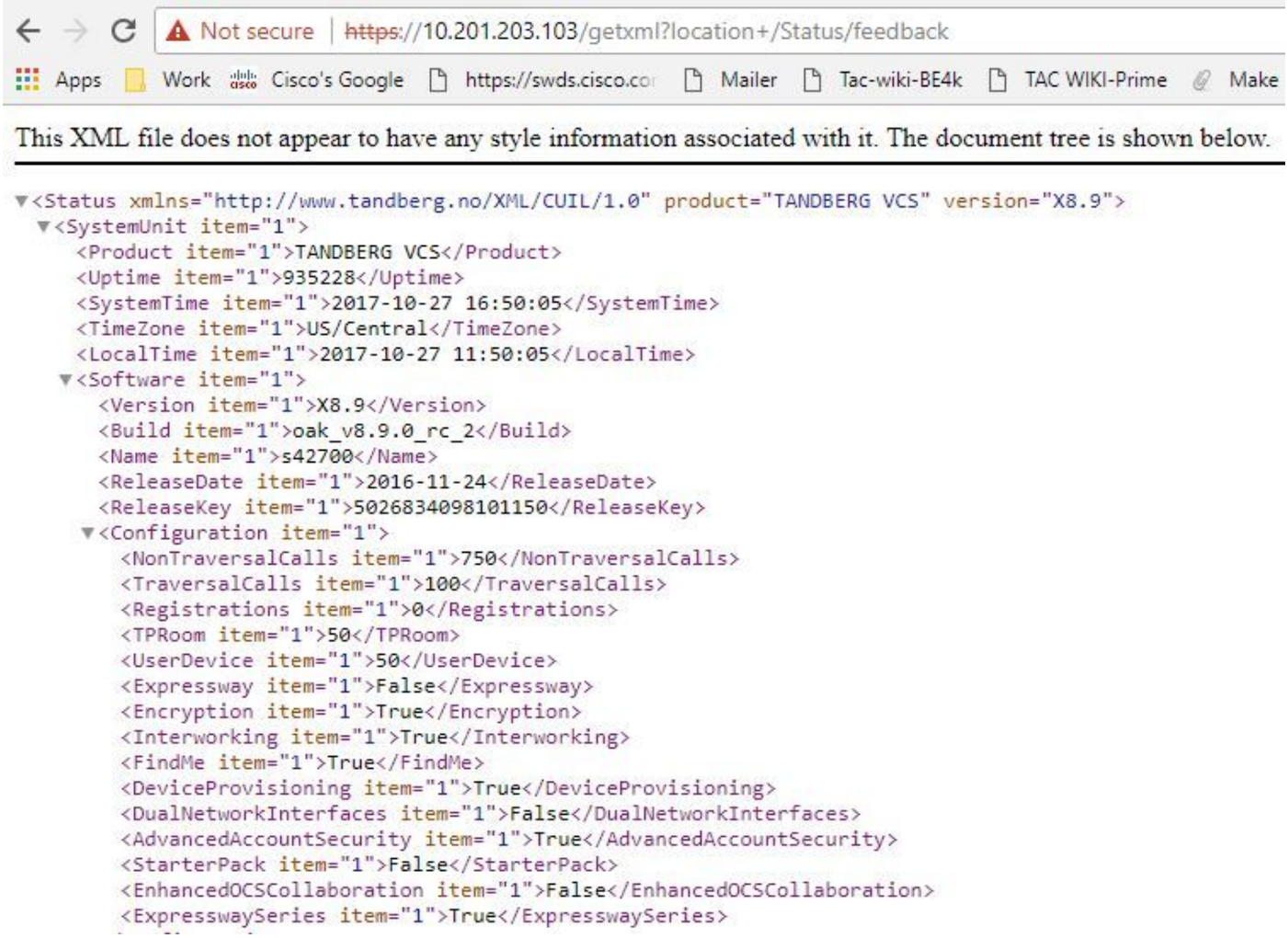


Étape 4. Assurez-vous que VCS et TMS sont à l'état Géré.

Remarque : si le VCS ou le TMS n'est pas dans un état géré, c'est la plupart du temps dû à HTTP ou SNMP, si une assistance supplémentaire est nécessaire, ouvrez un dossier TAC pour obtenir le VCS/TMS dans un état géré.

Remarque : utilisez cette URL et remplacez IP_Address_of_VCS_Server par l'adresse IP appropriée une fois que le serveur VCS est dans un état Géré.Le serveur PCA doit être enregistré en tant que serveur de commentaires sur VCS, ce qui garantit que lorsqu'une session de conférence se termine, il n'y a aucun problème avec les données que VCS renvoie à PCA.

https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedback , les informations d'identification http sont demandées et une fois entrées, vous devez recevoir une réponse, comme indiqué dans l'image.



Remarque : si Prime Collaboration n'est pas abonné à VCS via l'abonnement aux commentaires HTTP, il ne doit pas être averti par le VCS lorsqu'un terminal inscrit rejoint ou quitte une session, ou s'inscrit ou se désinscrit auprès de VCS. Dans ce cas, définissez la visibilité de ces points d'extrémité sur complète ou limitée, selon les besoins, et assurez-vous que votre VCS est à l'état Géré.

Étape 5. Accédez à Inventory > Inventory Schedule > Cluster Data Discovery Schedule et sélectionnez Run Now.

Remarque : ce processus peut prendre un certain temps car il exécute cette fonction sur tous les périphériques de l'infrastructure. Par conséquent, si elle ne se termine pas après quelques minutes, revérifiez après 1-2 heures. Les très grands systèmes peuvent prendre jusqu'à 4 heures. Il est important de mentionner dans l'inventaire PCA s'il y a des points d'extrémité où vous voulez avoir des statistiques de conférence qui sont prises en charge et que vous vous assurez également que ceux-ci sont également gérés pour les rapports et toutes les statistiques pour montrer les informations appropriées.

Pour obtenir la liste des périphériques pris en charge par PCA en ce qui concerne les conférences et nos sessions prises en charge, reportez-vous à la section Informations générales.

Étape 6. Naviguez jusqu'à Diagnose > Endpoint Diagnostics.

Afin d'obtenir des statistiques correctes pour les terminaux de conférence, vous devez définir leur visibilité au niveau le plus élevé possible autorisé par le système.

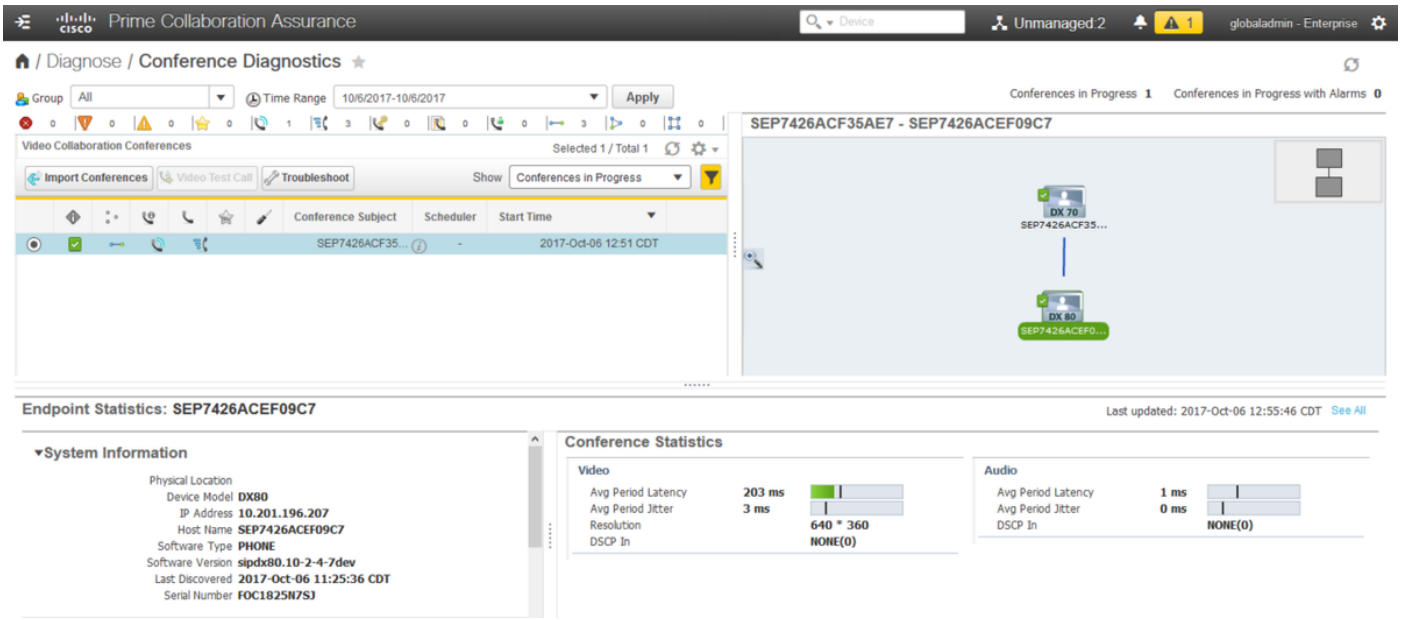
Sélectionnez tous les points d'extrémité que vous souhaitez surveiller dans les Diagnostics de conférence, puis cliquez sur Modifier la visibilité et sélectionnez la visibilité maximale.

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

Remarque : si vous sélectionnez, par exemple, 10 terminaux et que vous sélectionnez une visibilité totale, le niveau le plus élevé de visibilité est pris en charge par périphérique.

Étape 7. Afin de tester, nNaviguez jusqu'à Diagnostiquer > Diagnostics de conférence et une conférence en cours ou terminée est comme indiqué dans l'image.



Dans ces conférences, vous pouvez afficher la perte moyenne de paquets, la latence et la gigue pour les appels audio et vidéo.

Vous obtenez également une topologie de la session et des périphériques concernés.

Alarmes relatives aux conférences

Pour les diagnostics de conférence, vous pouvez recevoir trois alarmes différentes par session et définir leurs seuils :

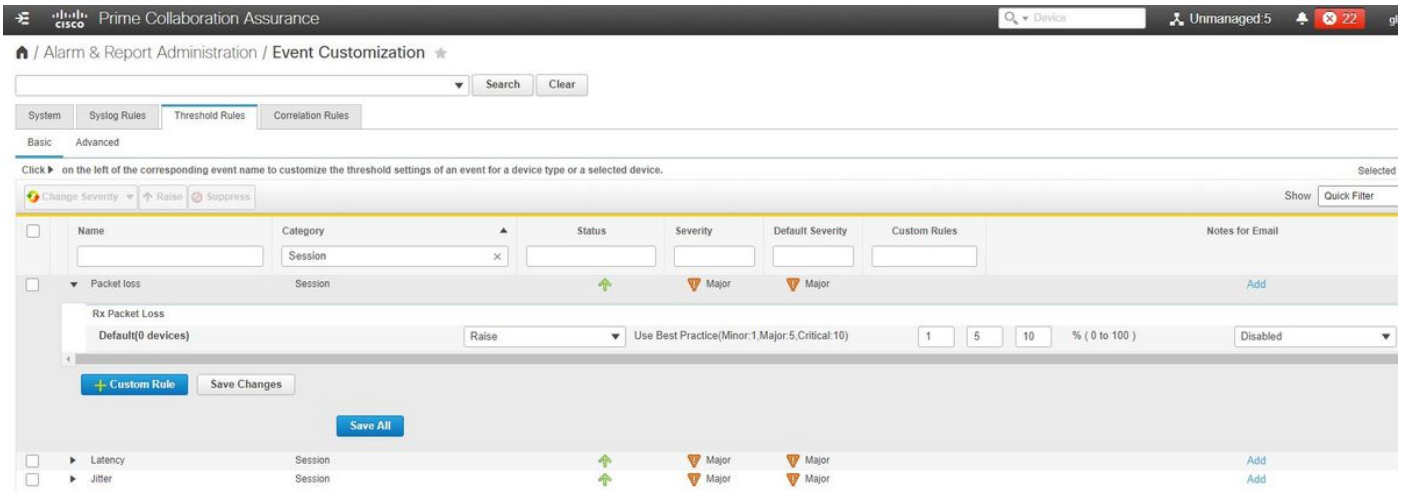
- La perte de paquets
- Latence
- Gigue

Vous pouvez modifier le seuil par défaut, le désactiver entièrement ou définir les périphériques que vous souhaitez associer à cette alarme.

Étape 1. Accédez à Administration des alarmes et des rapports > Personnalisation des événements.

Étape 2. Sélectionnez Threshold Rules et assurez-vous que Basic est sélectionné.

Étape 3. Faites défiler vers le bas ou filtrez vers la droite pour afficher la session nommée par catégorie, comme illustré dans l'image.



Étape 4. Sélectionnez la flèche de la liste déroulante en regard de l'alarme que vous souhaitez modifier et vous pouvez modifier les pourcentages Mineur, Majeur ou Critique pour Perte de paquets, Gigue ou Latence.

Étape 5. Si vous souhaitez la supprimer, passez de l'option Augmenter à la supprimer.

Étape 6. Si vous souhaitez définir les points d'extrémité associés à l'alarme, sélectionnez Règle personnalisée.

Étape 7. Sélectionnez ensuite Device Type > Select All devices ou Selectable devices que vous souhaitez pour cette alarme et cliquez sur Save.

Rapports relatifs aux conférences

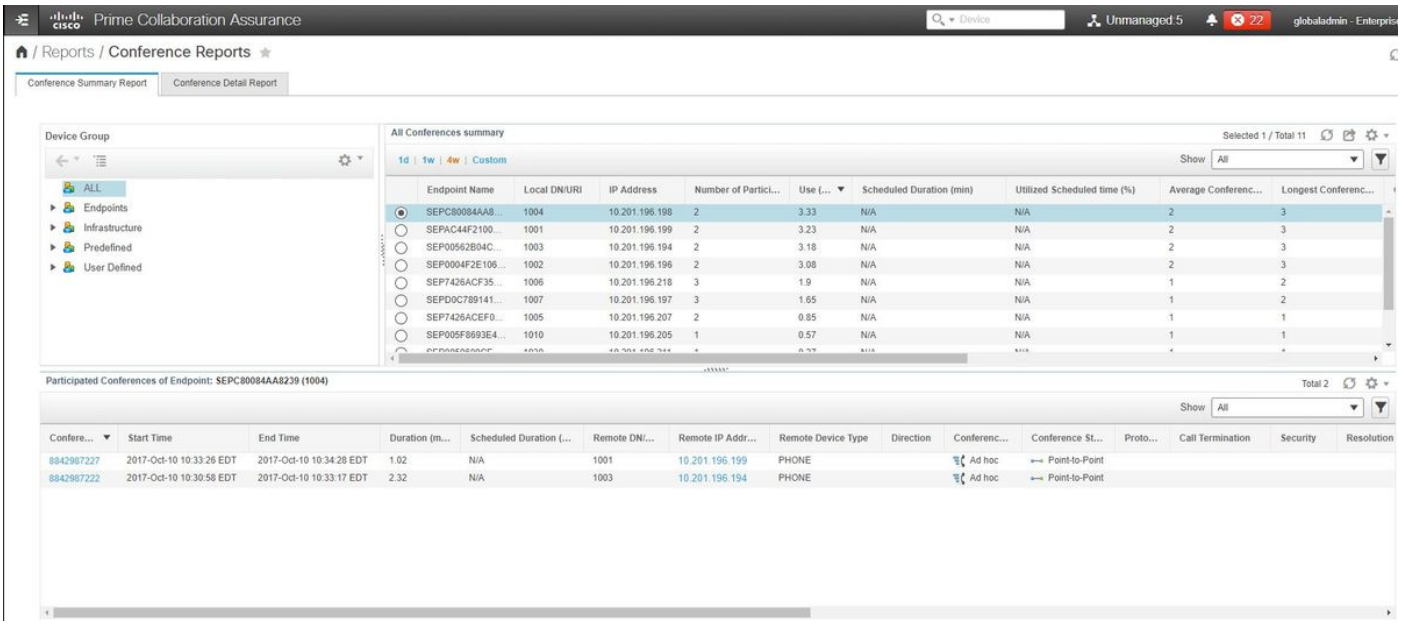
Pour les rapports de diagnostics de conférence peuvent être récupérés et affichés.

Il existe deux rapports :

- Rapports de conférence
- Rapports sur les terminaux Telepresence

Pour les rapports de conférence, vous pouvez afficher la liste de toutes les conférences dans un délai compris entre une et quatre semaines ou une période personnalisée, le cas échéant.

Étape 1. Accédez à Rapport > Rapports de conférence comme indiqué dans l'image.



Rapports récapitulatifs de conférence

Ce rapport fournit une vue de chaque terminal que vous avez sélectionné comme étant à visibilité limitée/complète et de leurs conférences.

Les statistiques présentées ici sont les suivantes :

- Utilisation moyenne des conférences
- Alarmes liées à la conférence
- Perte moyenne de paquets, gigue et latence
- Conférence la plus longue

Cela peut vous aider à obtenir une vue granulaire des problèmes que vous pouvez rencontrer au sein de votre réseau voix/vidéo afin de déterminer quels terminaux présentent le plus de problèmes.

En outre, utilisez votre bande passante en correspondance par utilisation

Onglet Rapport détaillé sur la conférence

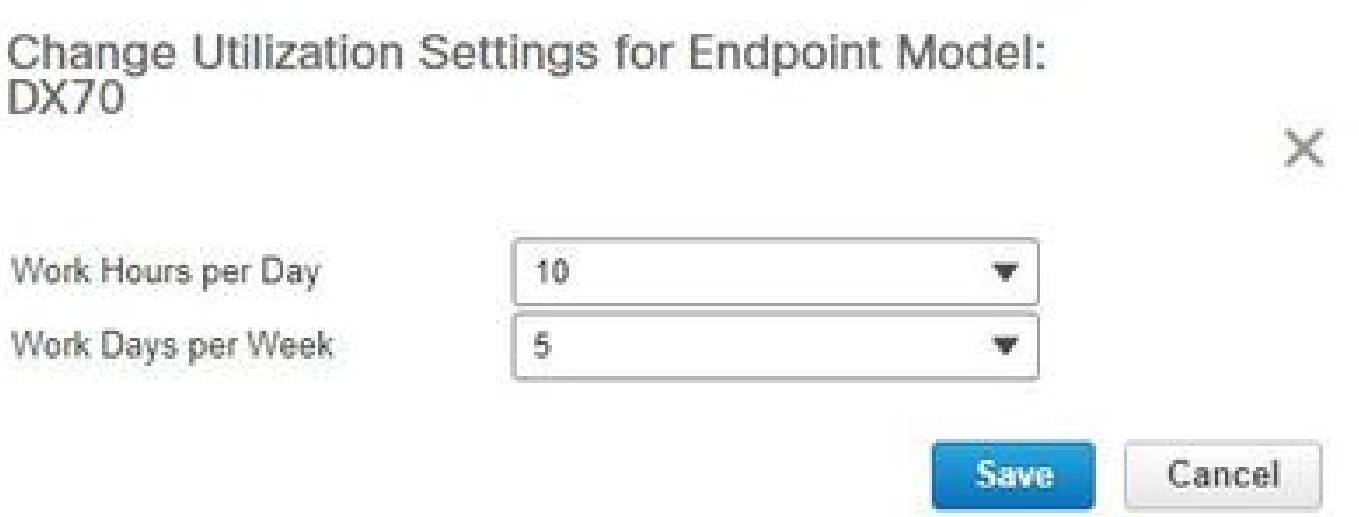
Si vous rencontrez une alarme pour une conférence, vous pouvez accéder à l'onglet Rapport détaillé de la conférence.

Une fois que vous avez sélectionné la conférence, vous pouvez l'affiner pour trouver le nom du terminal, la version du logiciel et d'autres détails qui pourraient vous intéresser.

Pour les rapports sur les terminaux TelePresence, vous pouvez afficher par terminal le-

- Nombre de conférences de ce périphérique
- Pourcentage d'utilisation
- Modèle de terminal
- Utilisation

En outre, vous pouvez modifier les paramètres d'utilisation à l'aide de l'onglet Modifier l'utilisation, comme illustré dans l'image.



Cette option définit les paramètres de ce périphérique de sorte que le système sache quel pourcentage afficher à partir de l'utilisation.

Le rapport de synthèse No Show Endpoint affiche les terminaux qui ont manqué les conférences planifiées.

Dans ce graphique, vous pouvez afficher le point de terminaison et le nombre total de conférences planifiées, ainsi que le nombre de conférences qui ont eu lieu et qui n'ont pas été présentées.

Appel de test vidéo de conférence

Vous pouvez créer des appels de test vidéo point à point entre deux points d'extrémité vidéo qui sont dans un état géré, pour tester votre réseau. Vous pouvez voir les événements et les alarmes, les statistiques de session, les statistiques de point de terminaison et la topologie du réseau. Seuls les codecs des séries CTS, C et EX sont pris en charge pour cet appel.

En outre, vous pouvez l'utiliser pour valider que toutes les fonctionnalités sont correctes avec les diagnostics de conférence.

Conditions préalables

- Cette fonctionnalité n'est pas prise en charge pour la gamme de codecs E20.
- Pour utiliser cette fonctionnalité, des informations d'identification CLI doivent être ajoutées pour les terminaux.
- Assurez-vous que les terminaux sont enregistrés et que JTAPI est activé pour les terminaux (s'ils sont enregistrés dans Unified CM).
- La fonction Appel de test vidéo n'est pas disponible si vous avez déployé Cisco Prime Collaboration en mode MSP.

Étape 1. Naviguez jusqu'à Diagnose > Endpoint Diagnostics.

Étape 2. Sélectionnez deux points d'extrémité applicables, conformément aux conditions requises.

Étape 3. Sélectionnez Run Tests > Video Test Call.

Étape 4. Vous pouvez programmer l'appel de test vidéo pour qu'il s'exécute maintenant ou selon un calendrier de réoccurrence.

Étape 5. Cet appel de test vidéo s'affiche ensuite dans l'écran Diagnostics de la conférence.

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

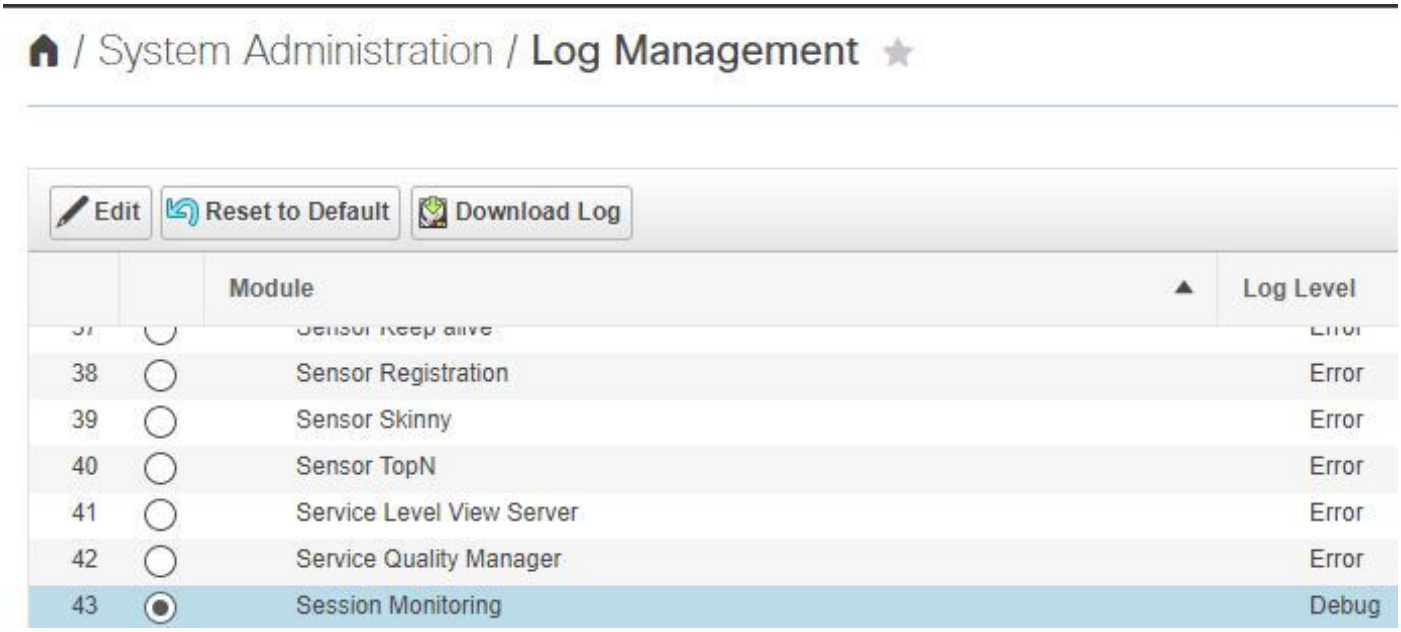
Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Journaux à collecter pour le dépannage

Étape 1. Accédez à Administration système > Gestion des journaux.

Étape 2. Faites défiler jusqu'au module et sélectionnez Session Monitoring et sélectionnez Edit comme indiqué dans l'image.



Étape 3. Modifiez le niveau du journal en debug et cliquez sur Save.

Étape 4. Reproduisez le problème, puis revenez à l'écran Log Management.

Étape 5. Après avoir reproduit le problème, sélectionnez Session Monitoring et sélectionnez Download Log.

Étape 6. Après le téléchargement, extrayez le fichier zip.

Étape 7. Ouvrez le fichier zip et accédez aux emplacements des journaux utiles :

/opt/emms/emsam/log/SessionMon/

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.