

Prime Collaboration Assurance(PCA)の設定 – 会議診断

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[OVAごとに可視性を制限または完全に設定したエンドポイントの制限](#)

[設定](#)

[シナリオ 1. Call Managerに登録されたビデオエンドポイントを使用した会議](#)

[Cisco Unified Communications Managerのセットアップ](#)

[HTTPの有効化](#)

[SNMPの有効化](#)

[CTIサービスの開始](#)

[PCA CTIコントロール用アプリケーションユーザの作成 \(JTAPIユーザ\)](#)

[会議関連アラーム](#)

[会議関連レポート](#)

[会議ビデオテストコール](#)

[シナリオ 2. Call Managerに登録されていないエンドポイントとの会議](#)

[会議関連アラーム](#)

[会議ビデオテストコール](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、Prime Collaboration Assurance(PCA)内で会議診断の導入を設定およびセットアップして、音声/ビデオ会議の統計情報を予防的にモニタする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Call Manager Adminログイン
- PCAログイン
- Telepresence Monitor Server(TMS)
- Core/Expresswayクレデンシャル (該当する場合)

使用するコンポーネント

このドキュメントの情報は、PCAバージョン11.x ~ 12.xに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

Cisco Prime Collaboration 11.xは、次のタイプの可視性をサポートします。

- 完全な可視性：JTAPI/HTTPフィードバックと、会議の統計情報や会議情報などのリアルタイム監視情報を使用したコール検出がサポートされます。
- 可視性の制限：JTAPI/HTTPフィードバックを使用した自動コール検出が行われますが、会議の統計情報や会議情報などのリアルタイムのモニタリング情報はサポートされていません。可視性が限られているエンドポイントは、会議トポロジで半分グレー表示されたアイコンで示されます。

Cisco Prime Collaboration 12.xは、次のタイプの可視性をサポートします。

- 完全な可視性：JTAPI/HTTPフィードバックと、会議の統計情報や会議情報などのリアルタイム監視情報を使用したコール検出がサポートされます。
- 可視性なし：JTAPI/HTTPフィードバックおよびリアルタイムモニタリング情報を使用したコール検出はサポートされていません。これらのエンドポイントは、[会議モニタリング]ページで完全にグレー表示されたアイコンとともに表示されます。

OVAごとに可視性を制限または完全に設定したエンドポイントの制限

- スモールオープン仮想化アーカイブ(OVA)で最大500のエンドポイントをサポート
- 中規模OVAは最大1000のエンドポイントをサポート
- 大規模なOVAは最大1800のエンドポイントをサポート
- 非常に大規模なOVAは最大2000のエンドポイントをサポート

会議およびサポートされるセッションに関するPCAごとのサポート対象デバイスのリストは、次の表の図に示すとおりです。

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 <i>intracluster</i> and <i>intercluster</i> sessions	Ad hoc,Scheduled	Point-to-point	Cisco TelePresence System 500, 1000, 3000, TX9000 Series.
Cisco Unified CM <i>intracluster</i> and <i>intercluster</i> sessions	Ad hoc,ScheduledStatic	Multipoint	Cisco TelePresence System 500, 1000, 3000, TX9000 Series, and CTMS.
Cisco VCS <i>intracluster</i> and <i>intercluster</i> 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 <i>intracluster</i> and <i>intercluster</i> 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 <i>intracluster</i> and <i>intercluster</i> 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	<ul style="list-style-type: none"> • 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) <i>intracluster</i> sessions ³	Ad hoc	Point-to-point	<ul style="list-style-type: none"> • 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) <i>intracluster</i> sessions	Ad hoc,Scheduled Note Scheduler must be CTS-Manager 1.7, 1.8, or 1.9.	Multipoint	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

設定

シナリオ 1.Call Managerに登録されたビデオエンドポイントを使用した会議

ステップ 1 : まず、Call ManagerがManaged状態であることを確認する必要があります。

Inventory > Inventory Management > Manage Credentials > Create a profile for the Call Manager clusterの順に移動します。



注 : 各クレデンシャルプロファイルでは、プロファイル内にリストされているすべてのipに対して同じクレデンシャルが使用されることに注意してください。そのため、同じクレデンシャルプロファイル内にCall Managerパブリッシャとサブスクライバをリストすると、それらの同じクレデンシャルを使用して両方のIPアドレスが検出されます。セットアップにConductorがある場合は、図に示すように、最初にConductor、次にCisco Call Managerを検出します。

<input checked="" type="radio"/>	CUCM	ANY	10.201.196.222 ...
<input type="radio"/>	CUE	ANY	10.201.196.209
<input type="radio"/>	CUSP	SIPPROXY	10.201.160.42
<input type="radio"/>	Default	ANY	
<input type="radio"/>	JoeCUBE	ROUTER/VOICEGATEWAY	10.201.196.210

* Indicates required fields

*Profile Name

Device Type (Optional)

*IP Version

*Apply this credential to the given IP address ⓘ

▼ General SNMP Options

SNMP Timeout seconds

SNMP Retries

SNMP Version

ステップ 2 : ハイパーテキスト転送プロトコル(HTTP)、Simple Name Management Protocol(SNMP)、およびJava Telephony API(JTAPI)クレデンシャルが設定されていることを確認します。

さらに、Call Manager ServiceabilityでCisco Computer Telephony Integration(CTI)サービスを有効にする必要があります。

Cisco Unified Communications Managerのセットアップ

HTTPの有効化

Cisco Prime Collaborationで管理者クレデンシャルを使用してログインできるようにするには、新しいユーザを作成する必要はありません。また、Cisco Prime Collaboration Managerが適切なクレデンシャルを使用してCisco Unified Communications Managerにログインできるようにするには、新しいHTTPユーザグループと、Cisco Prime Collaborationが通信に使用できる対応するユーザを作成する必要があります。

ユーザを作成するには、次の手順を実行します。

ステップ 1 : 管理者アカウントでCisco Unified CM Administration Webインターフェイスにログインします。

ステップ 2 : 十分な権限を持つユーザグループを作成します。 User Management> User Settings> Access Control Groupedに移動し、適切な名前(この場合はPC_HTTP_Users)で新しいユーザグループを作成します。ここで、Saveを選択します。

ステップ 3 : User Management> User Settings> Access Control Groupの順に移動し、Findを選択します。定義したグループを見つけ、右側のアイコンをクリックします。

ステップ 4 : Select Assign Role to Group and select these roles (グループへのロールの割り当て):

- Standard AXL API Access
- 標準CCM管理者ユーザ
- 標準の保守管理

ステップ 5 : [Save] をクリックします。

手順 6 : メインメニューから、User Management>Application Users>Create a new userの順に移動します。

Application User Configurationページで適切なパスワードを指定します。Available Devicesテキスト領域から特定のタイプのデバイスだけを選択するか、Cisco Prime Collaborationですべてのデバイスを監視することができます

手順 7 : Permission情報セクションで、Add to User Group andを選択し、ステップ1で作成したグループ (たとえば、PC_HTTP_Users) を選択します。

ステップ 8 : Saveをクリックします。ページがリフレッシュされ、適切な権限が表示されます。

SNMPの有効化

Cisco Unified Communications Managerでは、SNMPはデフォルトでは有効になっていません。

SNMPを有効にするには、次の手順を実行します。

ステップ 1 : Cisco Unified Communications Manager Web GUIのCisco Unified Serviceabilityviewにログインします。

ステップ 2 : Tools > Service Activationの順に移動します。

ステップ 3 : Publisher Serverを選択します。

ステップ 4 : Performance > Monitoring Servicesの順に移動し、Cisco Call Manager SNMP Serviceのチェックボックスをオンにします。

ステップ 5 : 画面の下部にあるSaveを選択します。

SNMPコミュニティストリングを作成するには、次の手順を実行します。

ステップ 1 : Cisco Unified ServiceabilityCisco Unified Communications Manager Web GUIにログインします。


ステップ 2 : Cisco Unified Serviceabilityビューのメインメニューから、SNMP > v1/v2c > Community Stringの順に移動します。

ステップ 3 : サーバを選択して、Findをクリックします。

コミュニティ文字列がすでに定義されている場合、そのコミュニティ文字列名が検索結果に表示されます。

ステップ 4：結果が表示されない場合は、[新しい文字列の追加]をクリックして新しい文字列を追加します。

ステップ 5：必要なSNMP情報を指定し、設定を保存します。

 注：必要なのはSNMP読み取り専用(RO)アクセスだけです。

CTIサービスの開始

希望するCisco Unified Communications Managerノードの手順を実行します。2つのノードに設定することをお勧めします。

ステップ 1：Cisco Unified Communications Managerのグラフィカルユーザインターフェイスで表示されるCisco Unifiedサービスアビリティにログインします。

ステップ 2：Tools > Service Activationの順に移動します。

ステップ 3：ド롭ダウンリストからサーバを選択します。

ステップ 4：CM Servicesセクションから、Cisco CTI Managerチェックボックスにチェックマークを付けます。

ステップ 5：画面の上部にあるSaveを選択します

PCA CTIコントロール用アプリケーションユーザの作成 (JTAPIユーザ)

JTAPIは、デバイスからセッションステータス情報を取得するために使用されます。エンドポイントでJTAPIイベントを受信するために必要な権限を持つアプリケーションユーザを、コールプロセッサでCTI制御用に作成する必要があります。Prime Collaborationは、複数のコールプロセッサクラスタを管理します。クラスタIDが一意であることを確認する必要があります。Cisco Prime Collaborationが必要な情報を取得できるように、新しいアプリケーションユーザを作成します。

新しいJTAPIアプリケーションユーザを作成するには、次の手順を実行します。

ステップ 1：管理者アカウントでCisco Unified CM Administration Webインターフェイスにログインします。

ステップ 2：十分な権限を持つユーザグループを作成します。User Management> User Settings> Access Control Groupedに移動し、適切な名前(この場合はPC_HTTP_Users)で新しいユーザグループを作成します。ここで、Saveを選択します。

ステップ 3：User Management>User Settings>Access Control Groupの順に選択し、Findをクリックします。定義したグループを見つけ、右側のアイコンを選択します。

ステップ 4：「グループへのロールの割り当て」をクリックし、次のロールを選択します。


- Standard CTI Allow Call Monitoring
- Standard CTI Enabled

- Standard CTI Allow Control of Phones Supporting Connected Xfer and Conf

ステップ 5 : SelectSaveを選択します。


手順 6 : メインメニューから、User Management>Application Users>Create a new userの順に移動します。

Application User Configurationページで適切なパスワードを指定します。Available Devicesテキスト領域から特定のタイプのデバイスを選択するか、Cisco Prime Collaborationですべてのデバイスを監視できます。

 注 : パスワードにセミコロン(;)または等号(=)を含めることはできません。

手順 7 : Permission Informationセクションで、Add to Access Control Groupandを選択し、ステップ1で作成したグループ (たとえば、PC_HTTP_Users) を選択します。

ステップ 8 : Saveをクリックします。ページがリフレッシュされ、適切な権限が表示されます。

 注 : JTAPIユーザを追加する前にCall Managerが管理されていた場合は、Call ManagerのクレデンシャルプロファイルにJTAPIユーザが追加されていることを確認してから、再検出してください。

シナリオ1からの続き。手順 :


ステップ 3 : 作成したCall Manager JTAPIアプリケーションユーザに移動し、サポートされているエンドポイントをAvailable DevicesからControlled Devicesに移動します。

これは、図に示すように、デバイス関連付け機能によって実行できます。

Application User Configuration

 Save  Delete  Copy  Add New

Status

 Status: Ready

Application User Information

User ID*	<input type="text" value="JTAPIUser"/>	<input type="button" value="Edit Credential"/>
Password	<input type="password" value="....."/>	
Confirm Password	<input type="password" value="....."/>	
Digest Credentials	<input type="text"/>	
Confirm Digest Credentials	<input type="text"/>	
BLF Presence Group*	<input type="text" value="Standard Presence group"/>	
<input type="checkbox"/>	Accept Presence Subscription	
<input type="checkbox"/>	Accept Out-of-dialog REFER	
<input type="checkbox"/>	Accept Unsolicited Notification	
<input type="checkbox"/>	Accept Replaces Header	

Device Information

Available Devices	<input type="text" value="Auto-registration Template
BAT205D23177001
Sample Device Template with TAG usage examples
TCTTEST
TCTTEST2"/>	<input type="button" value="Device Association"/> <input type="button" value="Find more Route Points"/>
	▼ ▲	
Controlled Devices	<input type="text" value="SEP00059A3B7700
SEP00506004ECB3
SEP0050600CF7EB
SEP00562B04CFA8
SEP005F8693E4A0"/>	

エンドポイントがOVAごとに制限された、または完全な可視性に設定されている制限を再度参照すると、OVAサイズに追加したデバイスの量を確認できます。

この画面では、デバイス名、説明、または電話番号でフィルタリングして、図に示すように、これらのデバイスの管理とフィルタリングに役立てることができます。

これらのデバイスは手順7で追加されるため、注意が必要です。

User Device Association				
	Select All		Clear All	
	Clear All In Search		Save Selected/Changes	
Remove All Associated				
User Device Association (1 - 14 of 14)				
Find User Device Association where Name <input type="text"/> begins with <input type="text"/> Find Clear Filter				
<input checked="" type="checkbox"/> Show the devices already associated with user				
<input type="checkbox"/>		Device Name		
<input checked="" type="checkbox"/>		SEP00059A3B7700		1000
<input checked="" type="checkbox"/>		SEP00506004ECB3		1011
<input checked="" type="checkbox"/>		SEP0050600CF7EB		1030
<input checked="" type="checkbox"/>		SEP00562B04CFA8		1003
<input checked="" type="checkbox"/>		SEP005F8693E4A0		1010
<input checked="" type="checkbox"/>		SEP7426ACEF09C7		1005
<input checked="" type="checkbox"/>		SEP7426ACF35AE7		1006
<input checked="" type="checkbox"/>		SEPD0C789141410		1007

このJTAPIユーザに正しいユーザロールが追加されていることを確認します。

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled
- 図に示すように、Standard CTI Allow Control of Phones supporting Connected Xfer and conf。

Permissions Information

Groups [View Details](#)


Roles [View Details](#)

会議およびサポートされるセッションに関して、PCAごとにサポートされるデバイスのリストについては、「背景説明」セクションを参照してください。

注：さらに、図に示すように、CTIアプリケーションユーザによって制御されるデバイスのデバイス情報の下に、Allow Control of Device from CTIチェックボックスがオンになっていることを確認してください。


Allow Control of Device from CTI

注：先に進む前に、エンドポイントがCall Managerに登録されており、Call Managerが


 VCS/TMSと統合されている場合は、最初にVCS/TMSを検出し、次にCall Managerを最後に検出する点に注意してください。このように、インベントリの観点から見ると、すべてのインフラストラクチャが正しい場所にマッピングされます。また、VCS/TMSを検出する場合は、デフォルトの検出タブをTMS/VCSまたはCall Managerのそれぞれのデバイスに変更してください。


ステップ 4 : 次に、PCAでDevice Discoveryを選択し、Call ManagerのIPアドレスを入力して、図に示すようにAuto-Configurationの2つのチェックボックスをオンにし、Run Nowを選択します。


Discover Devices ✕

 Manage Credentials

→



 Device Discovery

 Ensure creating Cluster information using "Manage TMS Cluster" UI before discovering TMS cluster. * Indicates required field

Job Name	<input type="text" value="Discovery 2017-Oct-26 12:58:16 EDT"/>
	<input checked="" type="checkbox"/> Check Device Accessibility
Discover	<input type="text" value="Communications Manager (UCM) Cluster and connected devices"/>
*IP Address	<input type="text" value="10.201.196.222 10.201.196.221"/> 
Associate to Domain	<input type="text" value="Internal"/> (Optional)

If you have SIP trunks configured between the desired "Communications Manager" cluster and other "Communications Manager" clusters, please exclude all the Destination IPs of those SIP trunks in the Discovery Filter while triggering Logical Discovery.


▼ Auto-Configuration

- Add the Prime Collaboration server as a CDR Destination in the Unified CM servers 
- Add the Prime Collaboration server as a Syslog Destination in the Unified CM servers 


▶ Filters


▶ Advanced Filters

ステップ 5 : Call ManagerがManaged状態になった後、ステップ6に進みます。

 注 : Call Managerが管理状態ではない場合、それ以上の支援が必要な場合は、TACケースを開いてCall Managerを管理状態にする必要があり、ほとんどの場合はHTTPまたはSNMPが原因です。

手順 6 : Inventory > Inventory Schedule > Cluster Data Discovery Scheduleの順に移動し、Run Nowを選択します。

 注：これは、登録済み/未登録のデバイスの数によって異なります。このプロセスには、数分から数時間かかる場合があります。ページを更新して、1日を通して確認してください。同様に、Call Managerクラスタをまとめてマッピングし、すべてのエンドポイントを取得します。これが完了したら、次の手順に進みます。

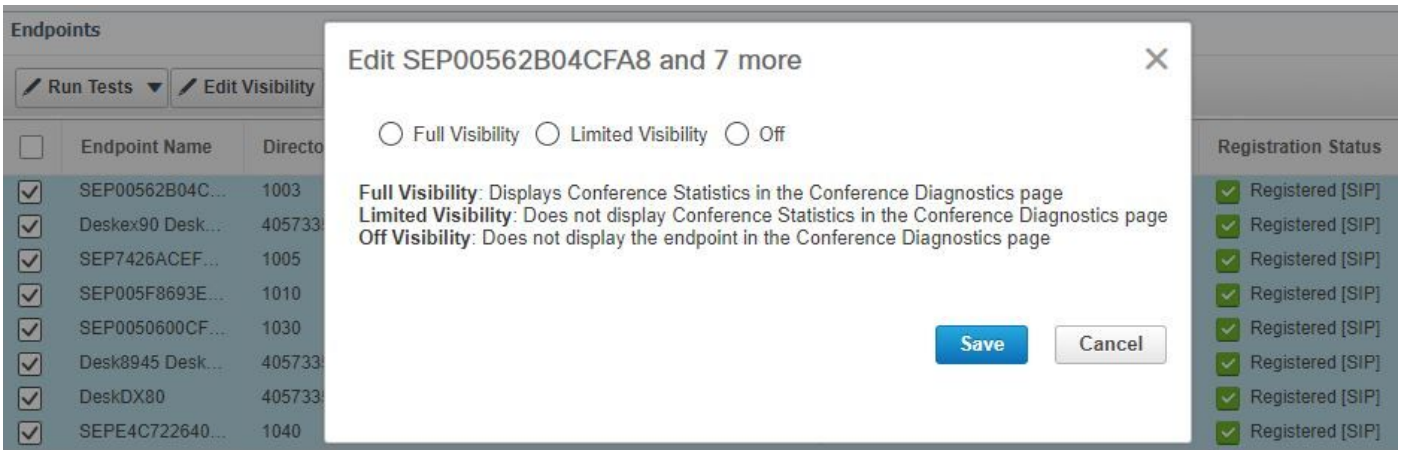
 注：サポートされている会議統計情報を必要とするエンドポイントがある場合は、PCAインベントリで言及することが重要です。正しい情報を表示するために、レポートとすべての統計情報が適切に管理されていることを確認します。

手順 7： Diagnose > Endpoint Diagnosticsの順に移動します。

会議エンドポイントの最新の統計情報を取得するには、システムで許可されている最高レベルに可視性を設定する必要があります。

図に示すように、会議診断でモニタするすべてのエンドポイントを選択し、Edit VisibilityをクリックしてからFull Visibilityを選択します。

可視性が制限されている場合、トポロジ内のデバイスのみが表示され、統計情報は表示されません。また、会議診断に関連するデバイスの該当するアラームを取得できません。




The screenshot shows the 'Endpoints' management interface. A dialog box titled 'Edit SEP00562B04CFA8 and 7 more' is open, allowing the user to set the visibility for the selected endpoints. The dialog has three radio button options: 'Full Visibility', 'Limited Visibility', and 'Off'. Below the options, there are explanatory text blocks for each visibility level. The 'Save' button is highlighted in blue, and the 'Cancel' button is in grey. In the background, a table lists endpoints with their names and direct numbers, and a 'Registration Status' column on the right shows that all endpoints are 'Registered [SIP]' with a green checkmark.

Endpoint Name	Directo	Registration Status
SEP00562B04C...	1003	Registered [SIP]
Deskex90 Desk...	405733	Registered [SIP]
SEP7426ACEF...	1005	Registered [SIP]
SEP005F8693E...	1010	Registered [SIP]
SEP0050600CF...	1030	Registered [SIP]
Desk8945 Desk...	405733	Registered [SIP]
DeskDX80	405733	Registered [SIP]
SEPE4C722640...	1040	Registered [SIP]

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

Endpoint Type	Default Visibility	Maximum Visibility
<ul style="list-style-type: none">CTS 500, 1000, and 3000 SeriesCisco CodecCisco TelePresence SX20Cisco TelePresence MXP SeriesCisco IP Video Phone E20	Full	Full
<ul style="list-style-type: none">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
<ul style="list-style-type: none">Cisco SX80 and Cisco SX10Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: <ul style="list-style-type: none">Cisco JabberCisco TelePresence MX SeriesCisco TelePresence System EX SeriesCisco TelePresence System SX Series	Limited	Limited

 注：たとえば、10個のエンドポイントを選択して[完全な可視性]を選択すると、デバイスごとに最高レベルの可視性サポートが選択されます。

ステップ 8：テストするには、図に示すように、診断>会議診断に移動し、会議が進行中または完了したことが表示されます。

The screenshot displays the Cisco Prime Collaboration Assurance interface for conference diagnostics. At the top, there is a navigation bar with the Cisco logo and 'Prime Collaboration Assurance' text. Below this, a search bar and 'Unmanaged:2' are visible. The main content area is titled 'Diagnose / Conference Diagnostics' and shows a table of 'Video Collaboration Conferences'. The table has columns for 'Conference Subject', 'Scheduler', and 'Start Time'. One conference is listed with subject 'SEP7426ACF35...' and start time '2017-Oct-06 12:51 CDT'. To the right of the table is a network diagram showing two devices, 'DX 70' and 'DX 80', connected to each other. Below the table, there are sections for 'Endpoint Statistics: SEP7426ACEF09C7' and 'System Information' (Physical Location, Device Model, IP Address, Host Name, Software Type, Software Version, Last Discovered, Serial Number). To the right of this is a 'Conference Statistics' section with 'Video' and 'Audio' metrics. The 'Video' section shows 'Avg Period Latency' as 203 ms and 'Avg Period Jitter' as 3 ms. The 'Audio' section shows 'Avg Period Latency' as 1 ms and 'Avg Period Jitter' as 0 ms. The resolution is listed as 640 * 360 and DSCP In as NONE(0).

これらの会議では、音声およびビデオコールの平均パケット損失、遅延、およびジッターを確認できます。

また、セッションのトポロジと関連するデバイスを取得します。

現在、会議診断はDNに基づいて情報を取得します。環境でDNが共有されている場合、PCAは会議のために最初に受信した情報を取得します。

会議関連アラーム

会議診断では、セッションごとに3つの異なるアラームを受信し、それらのしきい値を設定できます。

- パケット損失
- 遅延
- ジッター

これらの各アラームに対して、デフォルトのしきい値を変更したり、これを抑制したり、このアラームに関連付けるデバイスを定義したりすることができます。

ステップ 1 : Alarm & Report Administration > Event Customizationの順に移動します。

ステップ 2 : Threshold Rulesを選択して、Basicが選択されていることを確認します。

ステップ 3 : 下にスクロールするか、図に示すようにSessionという名前のカテゴリを右にフィルタします。

The screenshot shows the Cisco Prime Collaboration Assurance interface for Alarm & Report Administration / Event Customization. The 'Threshold Rules' tab is selected. A table lists event rules with columns for Name, Category, Status, Severity, Default Severity, Custom Rules, and Notes for Email. The 'Rx Packet Loss' rule is expanded, showing a configuration for 'Default(0 devices)' with a 'Raise' severity and 'Use Best Practice' settings. There are buttons for '+ Custom Rule', 'Save Changes', and 'Save All'.

ステップ 4 : アラームの横にあるドロップダウン矢印を選択します。パケット損失、ジッター、または遅延のマイナー、メジャー、またはクリティカルのパールセンテージを変更できます。

ステップ 5 : Suppressしたい場合は、Raise to Suppressを切り替えてください。

手順 6 : アラームに関連付けるエンドポイントを定義する場合は、Custom Ruleを選択します。

手順 7 : 次に、このアラームを設定するDevice Type > Select All DevicesまたはSelectable Devicesを選択し、Saveをクリックします。

会議関連レポート

会議診断レポートを取得して表示できます。

次の2つのレポートがあります。

- 会議レポート
- Telepresenceエンドポイントレポート

会議レポートでは、必要に応じて、1 ~ 4週間の期間またはカスタム期間の期間内のすべての会議のリストを表示できます。

ステップ 1 : 図に示すように、Reports > Conference Reportsの順に移動します。

The screenshot shows the Cisco Prime Collaboration Assurance interface for Conference Reports. It is divided into two main sections:

All Conferences summary

Endpoint Name	Local DNURI	IP Address	Number of Partic...	Use (...)	Scheduled Duration (min)	Utilized Scheduled time (%)	Average Conferenc...	Longest Conferenc...
SEPC80084AA8	1004	10.201.196.198	2	3.33	N/A	N/A	2	3
SEPAC44F2100	1001	10.201.196.199	2	3.23	N/A	N/A	2	3
SEP00562B04C	1003	10.201.196.194	2	3.18	N/A	N/A	2	3
SEP0004F2E106	1002	10.201.196.196	2	3.08	N/A	N/A	2	3
SEP7428ACF35	1006	10.201.196.218	3	1.9	N/A	N/A	1	2
SEPD0C789141	1007	10.201.196.197	3	1.65	N/A	N/A	1	2
SEP7428ACEF0	1005	10.201.196.207	2	0.85	N/A	N/A	1	1
SEP005F8693E4	1010	10.201.196.205	1	0.57	N/A	N/A	1	1

Participated Conferences of Endpoint: SEPC80084AA8239 (1004)

Confere...	Start Time	End Time	Duration (m...	Scheduled Duration (...)	Remote DN...	Remote IP Addr...	Remote Device Type	Direction	Conferenc...	Conference St...	Proto...	Call Termination	Security	Resolution
8842987227	2017-Oct-10 10:33:26 EDT	2017-Oct-10 10:34:28 EDT	1.02	N/A	1001	10.201.196.199	PHONE		Ad hoc	Point-to-Point				
8842987222	2017-Oct-10 10:30:58 EDT	2017-Oct-10 10:33:17 EDT	2.32	N/A	1003	10.201.196.194	PHONE		Ad hoc	Point-to-Point				

会議サマリーレポート

このレポートには、限定/完全な可視性として選択したすべてのエンドポイントとその会議が表示されます。

ここに示す統計情報は次のとおりです。

- 会議の平均利用率
- 会議に関連するアラーム
- 平均パケット損失、ジッター、および遅延
- 最長会議

これにより、音声/ビデオネットワーク内で発生する可能性のある問題を詳細に把握し、最も問題のあるエンドポイントを特定できます。

また、帯域幅を使用量に応じて使用できます。

会議の詳細レポートタブ

会議でアラームが発生した場合は、会議詳細レポートタブに移動できます。

会議を選択したら、会議を調整して、エンドポイント名、ソフトウェアバージョン、その他の詳細を確認できます。

Telepresenceエンドポイントレポートでは、エンドポイントごとに次の情報を表示できます。

- このデバイスの会議数
- 利用率
- エンドポイントモデル
- 用途

また、図に示すように、Change Utilizationタブで使用率パラメータを変更できます。

Change Utilization Settings for Endpoint Model: DX70



Work Hours per Day	<input type="text" value="10"/>
Work Days per Week	<input type="text" value="5"/>

これにより、そのデバイスのパラメータが設定され、システムは使用率から表示するパーセンテージを知ることができます。

No Show Endpoint Summaryレポートには、スケジュールされた会議に参加できなかったエンドポイントが表示されます。

このグラフ内では、エンドポイントと、スケジュール済み会議合計の数、およびこれらのうち発生し、発生しなかった数も表示できます。

会議ビデオテストコール

マネージド状態の2つのビデオエンドポイント間にポイントツーポイントビデオテストコールを作成して、ネットワークをテストできます。イベントとアラーム、セッションの統計情報、エンドポイントの統計情報、およびネットワークトポロジを、他のコールと同様の統計情報で表示できます。このコールでは、CTS、C、およびEXシリーズのコーデックのみがサポートされています。

さらに、これを使用して、すべての機能が会議診断で機能することを検証できます。

前提条件

- この機能は、E20コーデックシリーズではサポートされていません。
- この機能を使用するには、エンドポイントにCLIクレデンシャルを追加する必要があります。
- エンドポイントが登録され、エンドポイントでJTAPIが有効になっていることを確認します（エンドポイントがUnified CMに登録されている場合）。
- Cisco Prime CollaborationをMSPモードで展開している場合、ビデオテストコール機能は使用できません。

ステップ 1 : Diagnose > Endpoint Diagnosticsの順に移動します。

ステップ 2 : 前述の前提条件に従って、該当するエンドポイントを2つ選択します。


ステップ 3 : Run Tests > Video Test Callの順に選択します。

ステップ 4 : ビデオテストコールを今すぐ実行するか、再スケジュールで実行するかをスケジュールできます。

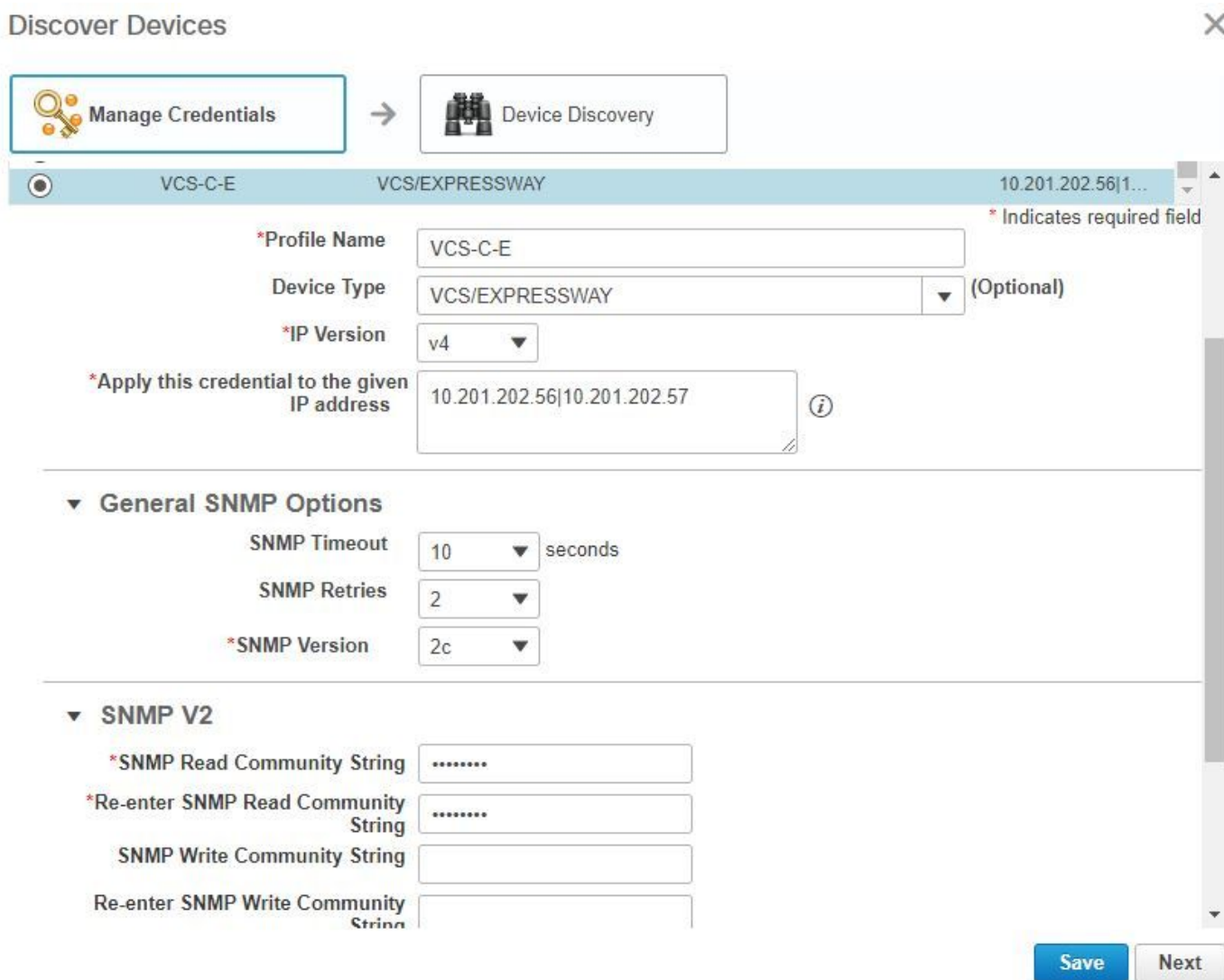
ステップ 5 : このビデオテストコールが会議診断画面に表示されます。

シナリオ 2. Call Managerに登録されていないエンドポイントとの会議

ステップ 1 : Telepresence Management Suite(TMS)およびVideo Communications Server(VCS)のクレデンシャルが使用可能であることを確認します。

 注 : このシナリオでVCS/TMSを検出する場合、検出プロセスが重要です。セットアップに Call Managerがある場合は、最初にConductorを検出し、次にCisco Call Managerを検出します。

ステップ 2 : 図に示すように、VCS用に個別のクレデンシャルプロファイルを作成しながら、Inventory > Inventory Management > Manage Credentials > の順に移動し、Addを選択してからTMSの情報を入力します。



Discover Devices

Manage Credentials → Device Discovery

VCS-C-E VCS/EXPRESSWAY 10.201.202.56|10.201.202.57

*Profile Name VCS-C-E

Device Type VCS/EXPRESSWAY (Optional)

*IP Version v4

*Apply this credential to the given IP address 10.201.202.56|10.201.202.57

* Indicates required field

▼ General SNMP Options

SNMP Timeout 10 seconds

SNMP Retries 2

*SNMP Version 2c

▼ SNMP V2

*SNMP Read Community String

*Re-enter SNMP Read Community String

SNMP Write Community String

Re-enter SNMP Write Community String



Save Next

ステップ 3 : クレデンシャルプロファイルを作成したら、Device Discoveryを選択し、IPアドレスを入力して、DiscoveryタブでVCSを選択し、VCSデバイスを検出します。また、TMSにTMSを

選択し、そのIPアドレスを入力します。図に示すように、Run Nowをクリックします。

Discover Devices



 Manage Credentials →  Device Discovery

i Ensure creating Cluster information using "Manage TMS Cluster" UI before discovering TMS cluster. * Indicates required field

Job Name

Check Device Accessibility

Discover

*IP Address **i**

Associate to Domain (Optional)

If you have SIP trunks configured between the desired "Communications Manager" cluster and other "Communications Manager" clusters, please exclude all the Destination IPs of those SIP trunks in the Discovery Filter while triggering Logical Discovery.

▶ Filters


▶ Advanced Filters


▼ Schedule


Start Time Date:
(yyyy/MM/dd hh:mm AM/PM)

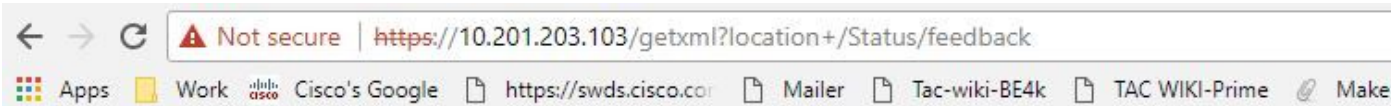
Recurrence None Hourly Daily Weekly Monthly

ステップ 4 : VCSとTMSが管理状態であることを確認します。

 注 : VCSまたはTMSが管理状態ではない場合、さらなる支援が必要な場合は、TACケースを開いてVCS/TMSを管理状態にする必要があります。ほとんどの場合はHTTPまたはSNMPが原因です。


 注:VCSが管理状態になったら、このURLを使用して、IP_Address_of_VCS_Serverを適切なIPアドレスに置き換えます。PCAサーバをフィードバックサーバとしてVCSに登録する必要があります。これにより、会議セッション終了時に、VCSがPCAに返信するデータに問題が発生しなくなります。

 https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedbackを入力すると、httpクレデンシャルが要求され、次の図に示すように応答を受信する必要があります。




This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Status xmlns="http://www.tandberg.no/XML/CUIL/1.0" product="TANDBERG VCS" version="X8.9">
  <SystemUnit item="1">
    <Product item="1">TANDBERG VCS</Product>
    <Uptime item="1">935228</Uptime>
    <SystemTime item="1">2017-10-27 16:50:05</SystemTime>
    <TimeZone item="1">US/Central</TimeZone>
    <LocalTime item="1">2017-10-27 11:50:05</LocalTime>
  <Software item="1">
    <Version item="1">X8.9</Version>
    <Build item="1">oak_v8.9.0_rc_2</Build>
    <Name item="1">s42700</Name>
    <ReleaseDate item="1">2016-11-24</ReleaseDate>
    <ReleaseKey item="1">5026834098101150</ReleaseKey>
  <Configuration item="1">
    <NonTraversalCalls item="1">750</NonTraversalCalls>
    <TraversalCalls item="1">100</TraversalCalls>
    <Registrations item="1">0</Registrations>
    <TPRoom item="1">50</TPRoom>
    <UserDevice item="1">50</UserDevice>
    <Expressway item="1">False</Expressway>
    <Encryption item="1">True</Encryption>
    <Interworking item="1">True</Interworking>
    <FindMe item="1">True</FindMe>
    <DeviceProvisioning item="1">True</DeviceProvisioning>
    <DualNetworkInterfaces item="1">False</DualNetworkInterfaces>
    <AdvancedAccountSecurity item="1">True</AdvancedAccountSecurity>
    <StarterPack item="1">False</StarterPack>
    <EnhancedOCSCollaboration item="1">False</EnhancedOCSCollaboration>
    <ExpresswaySeries item="1">True</ExpresswaySeries>
  </Configuration>
</SystemUnit>
</Status>
```

 注:Prime CollaborationがHTTPフィードバックサブスクリプションによってVCSにサブスクライブされていない場合、登録済みエンドポイントがセッションに参加または脱退したとき、またはVCSへの登録または登録解除されたときに、VCSから通知されません。この場合、必要に応じてこれらのエンドポイントの可視性をfullまたはlimitedに設定し、VCSがManaged状態になっていることを確認します。

ステップ 5 : Inventory > Inventory Schedule > Cluster Data Discovery Scheduleの順に移動し、Run Nowを選択します。

 注 : このプロセスは、すべてのインフラストラクチャデバイスでこの機能を実行するため、しばらく時間がかかる場合があります。したがって、数分後に完了しない場合は、1~2時間後に再確認してください。非常に大規模なシステムでは、最大4時間かかる場合があります。適切な情報を表示するために、会議の統計情報をサポートし、これらのエンドポイントがレポートおよびすべての統計情報に対して確実に管理されるようにする必要のあるエンドポイントがある場合は、PCAインベントリで言及することが重要です。

会議およびサポートされるセッションに関するPCAによるサポート対象デバイスのリストについては、「背景説明」セクションを参照してください。


手順 6 : Diagnose > Endpoint Diagnosticsの順に移動します。

会議エンドポイントの正確な統計情報を取得するには、システムで許可されている最高レベルにエンドポイントの可視性を設定する必要があります。

会議の診断で監視するすべてのエンドポイントを選択し、Edit Visibilityをクリックして、最大の可視性を選択します。

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

Endpoint Type	Default Visibility	Maximum Visibility
<ul style="list-style-type: none">CTS 500, 1000, and 3000 SeriesCisco CodecCisco TelePresence SX20Cisco TelePresence MXP SeriesCisco IP Video Phone E20	Full	Full
<ul style="list-style-type: none">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
<ul style="list-style-type: none">Cisco SX80 and Cisco SX10Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: <ul style="list-style-type: none">Cisco JabberCisco TelePresence MX SeriesCisco TelePresence System EX SeriesCisco TelePresence System SX Series	Limited	Limited

 注：たとえば、10個のエンドポイントを選択して[完全な可視性]を選択した場合、デバイスごとに最高レベルの可視性サポートが選択されます。

手順 7：テストするには、n図のように、「診断(Diagnose)」>「会議診断(Conference Diagnostics)」に移動し、「会議中」または「完了」を確認します。

The screenshot displays the Cisco Prime Collaboration Assurance interface for conference diagnostics. At the top, the navigation bar shows 'Diagnose / Conference Diagnostics'. Below this, there are filters for 'Group' (All) and 'Time Range' (10/6/2017-10/6/2017). A table lists 'Video Collaboration Conferences' with columns for 'Conference Subject', 'Scheduler', and 'Start Time'. The selected conference is 'SEP7426ACF35AE7 - SEP7426ACEF09C7'. To the right, a network diagram shows two endpoints: 'DX 70 SEP7426ACF35...' and 'DX 80 SEP7426ACEF09...'. Below the diagram, 'Endpoint Statistics: SEP7426ACEF09C7' are shown, including 'System Information' (Physical Location, Device Model DX80, IP Address 10.201.196.207, Host Name SEP7426ACEF09C7, Software Type PHONE, Software Version sipdx80.10-2-4-7dev, Last Discovered 2017-Oct-06 11:25:36 CDT, Serial Number FOC1825N7S3) and 'Conference Statistics' for Video (Avg Period Latency 203 ms, Avg Period Jitter 3 ms, Resolution 640 * 360, DSCP In NONE(0)) and Audio (Avg Period Latency 1 ms, Avg Period Jitter 0 ms, DSCP In NONE(0)).

これらの会議では、音声およびビデオコールの平均パケット損失、遅延、およびジッターを確認できます。

また、セッションのトポロジと関連するデバイスを取得します。

会議関連アラーム

会議診断では、セッションごとに3つの異なるアラームを受信し、しきい値を設定できます。

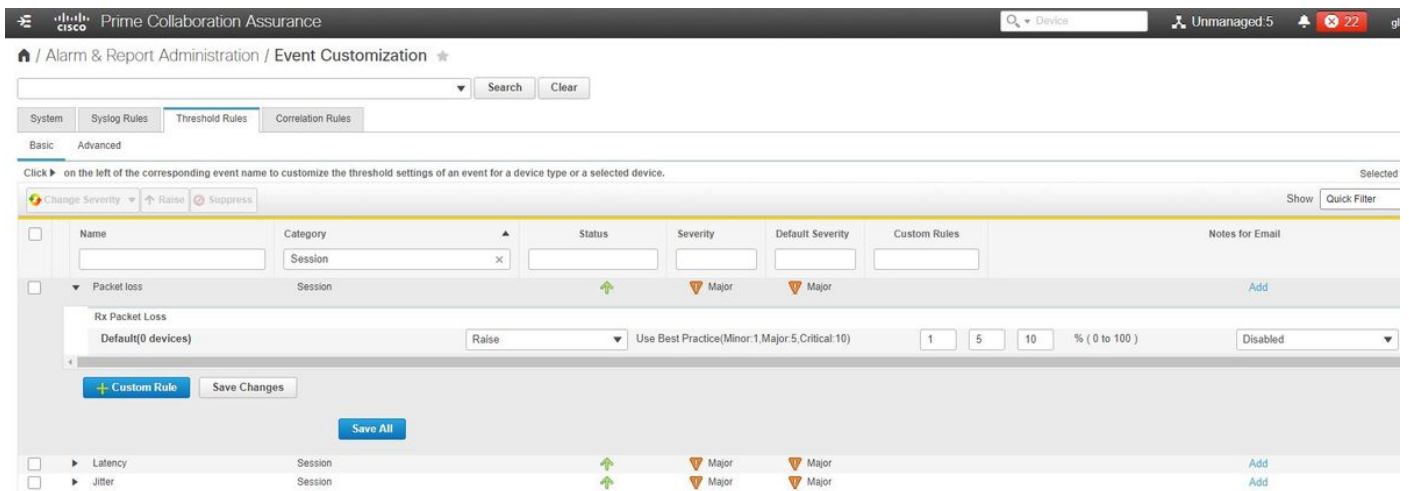
- パケット損失
- 遅延
- ジッター

これらのそれぞれについて、デフォルトのしきい値を変更したり、すべてを無効にしたり、このアラームに関連付けるデバイスを定義したりできます。

ステップ 1 : Alarm & Report Administration >Event Customizationの順に移動します。

ステップ 2 : Threshold Rulesを選択して、Basicが選択されていることを確認します。

ステップ 3 : 下にスクロールするか、図に示すようにSessionという名前のカテゴリを右にフィルタします。



ステップ 4 : 変更するアラームの横にあるドロップダウン矢印を選択すると、パケット損失、ジッター、または遅延のマイナー、メジャー、またはクリティカルの割合を変更できます。

ステップ 5 : Suppressしたい場合は、Raise to Suppressを切り替えてください。

手順 6 : アラームに関連付けるエンドポイントを定義する場合は、Custom Ruleを選択します。

手順 7 : 次に、このアラームを設定するDevice Type > Select All devicesまたはSelectable devices を選択し、Saveをクリックします。

会議関連レポート

会議診断レポートを取得して表示できます。

次の2つのレポートがあります。

- 会議レポート
- Telepresenceエンドポイントレポート

会議レポートでは、必要に応じて、1 ~ 4週間の期間またはカスタム期間の期間内のすべての会議のリストを表示できます。

ステップ 1 : 図に示すように、Report > Conference Reportsの順に移動します。

会議サマリーレポート

このレポートには、限定/完全な可視性として選択したすべてのエンドポイントとその会議が表示されます。

ここに示す統計情報は次のとおりです。

- 会議の平均使用率
- 会議に関連するアラーム
- 平均パケット損失、ジッター、および遅延
- 最長会議

これにより、音声/ビデオネットワーク内で発生する可能性のある問題を詳細に把握し、最も問題のあるエンドポイントを特定できます。

また、帯域幅を使用量に応じて使用できます

会議の詳細レポートタブ

会議でアラームが発生した場合は、[会議の詳細レポート(Conference Detail Report)]タブに移動できます。

会議を選択すると、エンドポイント名、ソフトウェアバージョン、その他の詳細を確認できます。

Telepresenceエンドポイントレポートでは、エンドポイントごとに

- このデバイスの会議数
- 使用率
- エンドポイントモデル
- 用途

また、図に示すように、[使用率の変更]タブで使用率パラメータを変更できます。

Change Utilization Settings for Endpoint Model: DX70



Work Hours per Day	<input type="text" value="10"/>
Work Days per Week	<input type="text" value="5"/>

これにより、そのデバイスのパラメータが設定され、システムは使用率から表示するパーセンテージを知ることができます。

No Show Endpoint Summaryレポートには、スケジュールされた会議に参加できなかったエンドポイントが表示されます。

このグラフ内では、エンドポイントと、スケジュール済み会議の合計数、およびこれらのうち発生したものの表示されなかった会議の数を確認できます。

会議ビデオテストコール

マネージド状態にある2つのビデオエンドポイント間にポイントツーポイントビデオテストコールを作成して、ネットワークをテストできます。イベントとアラーム、セッション統計情報、エンドポイント統計情報、およびネットワークトポロジを表示できます。このコールでは、CTS、C、およびEXシリーズのコーデックのみがサポートされています。

さらに、これを使用して、会議の診断ですべての機能が正しいことを確認できます。

前提条件

- この機能は、E20コーデックシリーズではサポートされていません。
- この機能を使用するには、エンドポイントにCLIクレデンシャルを追加する必要があります。
- エンドポイントが登録され、エンドポイントでJTAPIが有効になっていることを確認します（エンドポイントがUnified CMに登録されている場合）。
- Cisco Prime CollaborationをMSPモードで導入している場合、ビデオテストコール機能は使用できません。

ステップ 1 : Diagnose > Endpoint Diagnosticsの順に移動します。

ステップ 2 : 前提条件に従って、該当するエンドポイントを2つ選択します。

ステップ 3 : Run Tests > Video Test Callの順に選択します。

ステップ 4 : ビデオテストコールを今すぐ実行するか、再スケジュールで実行するかをスケジュー

ールできます。

ステップ 5 : このビデオテストコールが会議診断画面に表示されます。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのために収集するログ

ステップ 1 : System Administration > Log Managementの順に移動します。

ステップ 2 : モジュールまでスクロールダウンし、図に示すようにSession Monitoringを選択して、Editを選択します。

🏠 / System Administration / Log Management ★

		Module	▲	Log Level
37	<input type="radio"/>	Sensor Keep alive		Error
38	<input type="radio"/>	Sensor Registration		Error
39	<input type="radio"/>	Sensor Skinny		Error
40	<input type="radio"/>	Sensor TopN		Error
41	<input type="radio"/>	Service Level View Server		Error
42	<input type="radio"/>	Service Quality Manager		Error
43	<input checked="" type="radio"/>	Session Monitoring		Debug

ステップ 3 : ログレベルをdebugに変更して、Saveをクリックします。

ステップ 4 : 問題を再現し、Log Management画面に戻ります。

ステップ 5 : 問題を再現したら、Session Monitoringを選択し、Download Logを選択します。

手順 6 : ダウンロードしたら、zipファイルを展開します。

手順 7 : zipファイルを開き、有用なログの場所に移動します。

/opt/emms/emsam/log/SessionMon/

- CUCMJTAPIログ
- CUCMJTAPIDiag.logです。

- CSMTTracker
- CSMTTrackerDiag.log (登録ユーザ専用)
- CSMTTrackerDataSource.logです。
- PostInitSessionMon.log

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。