Allgemeine Informationen für die Registrierung von CUCM-IP-Telefonen/Fehlerbehebung bei der Registrierung von Registrierungssystemen

Inhalt

Einführung

In diesem Dokument werden allgemeine Informationen zur Erfassung von Cisco IP-Telefonen beschrieben, bei denen bei der Integration in Cisco Unified Communications Manager (CUCM) Registrierungsprobleme auftreten. In diesem Dokument werden die Schritte zur Behebung bestimmter Probleme nicht erläutert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Internetprotokoll (IP)
- Voice over Internet Protocol (VOIP)-Signalisierungsprotokolle
- Der Registrierungsprozess für Cisco IP-Telefone

HINWEIS: Der Registrierungsprozess für IP-Telefone, SCCP und SIP-Telefone mit CUCM ist ein hervorragendes Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Wichtige Fragen

- Können sie bei Telefonen, die nicht registriert sind, Anrufe tätigen und entgegennehmen? Wenn ja, überprüfen Sie den Registrierungsstatus auf der Webseite der anderen CUCM-Knoten und den Status des Telefons in RIS DC.

  HINWEIS: Wenn die Telefone Anrufe tätigen und empfangen können, verwenden Sie den folgenden Befehl für jeden Knoten, um den Status des Telefons im RIS DC anzuzeigen.

  Display-Risdabfragetelefon

  Wenn das Problem als falscher Status nicht registriert eingestuft wird, starten Sie den RIS DC-Dienst neu. Aufgrund der Architektur des RIS-Rechenzentrums kann es auch erforderlich sein, den CallManager-Dienst neu zu starten.

- Wie viele Telefone sind davon betroffen, und wie viele Telefone gibt es insgesamt?
- Wenn nur ein Teil der Telefone betroffen ist, was haben sie gemeinsam (d. h. Modell, Protokoll, Firmware-Version, auf demselben Switch/Blade, am gleichen Standort usw.)?
- Verfügt das Telefon über eine gemeinsame Leitung?
- Sind die Telefone über ein Virtual Private Network (VPN) mit dem Netzwerk verbunden?
- Tritt das Problem jedes Mal zur gleichen Tageszeit auf?
- Werden im Netzwerk Sicherheitsüberprüfungen durchgeführt (d. h. Port-Scanner)?
- Gibt es Firewalls zwischen dem Telefon und dem CUCM?
- Führen Sie eine SIP-Prüfung auf allen Geräten im Pfad zwischen Telefon und CUCM durch?
- Wie viele Telefone sind im gleichen Subnetz, und wie viele IP-Adressen stehen für das Leasing in dieses Subnetz zur Verfügung?
- Sind Sie für die Verwendung von Session Initiation Protocol (SIP) over Transmission Control Protocol (TCP) oder User Datagram Protocol (UDP) neu konfiguriert?
- Verwenden die Telefone ein sicheres oder nicht sicheres Gerätesicherheitsprofil? Haben die Telefone über ein sicheres Profil verfügen, wurde ein LSC (Locally Significant Certificate) installiert, bevor das sichere Profil auf die Telefonkonfiguration angewendet wurde?

  HINWEIS: Telefone können sich nicht registrieren, wenn sie ein sicheres Sicherheitsprofil ohne installiertes LSC verwenden. Weitere Informationen finden Sie im Dokument CUCM Generating LSC Certificates for Secure Phones (CUCM-Zertifikate für sichere Telefone erstellen).

- Ist jemand über Durchwahlmobilität an den problematischen Telefonen angemeldet? Wenn ja, stimmt das Protokoll (SCCP/SIP) des Geräteprofils mit dem des Telefons überein, und existiert dasselbe Verhalten auch nach dem Abmelden?
- Hat sich etwas geändert? Alles in allem, egal wie bedeutsam der Wandel sein mag und

unabhängig davon, wie tief er war. Alle neuen Änderungen (neue Konfigurationen, neue Software, neue Hardware) sollten bestätigt werden.

Daten vom Telefon

- Dokumentieren Sie die Meldung auf dem Telefonbildschirm, wenn das Problem auftritt. Es ist typisch, dass eine Nachricht auf dem Telefon-Bildschirm angezeigt wird. Achten Sie also darauf, dies zu überprüfen.
- Überprüfen Sie, ob ein LSC auf dem Telefon installiert ist, da dies erforderlich ist, wenn der Kunde ein sicheres Gerätesicherheitsprofil verwendet.
  79XX

  Drücken Sie die Einstellungstaste auf dem Telefon > drücken Sie die Tastenfeld Nr. 4 > drücken Sie erneut die Tastenfeld Nr. 4 > und dokumentieren Sie, ob das LSC laut Installation installiert ist oder nicht.

  78XX/88XX/99XX

  Drücken Sie die Einstellungstaste auf dem Telefon > wählen Sie Admin Settings (Admin-Einstellungen) > drücken Sie die Tastenfolge Nr. 2 > Dokument, ob das LSC laut Installation oder Installation installiert ist.

- Paketerfassung (pcap) vom Telefon abrufen

  TIPP: Bei vielen der Informationen unter diesem Punkt muss der **Internetzugriff** am Telefon aktiviert sein. Auch wenn ein Telefon nicht registriert ist, kann es möglich sein, die Einstellungen auf dem Telefon so zu ändern, dass **Webzugriff**, **span zu PC-Port** und **SSH-Zugriff** dann versuchen, auf die Webseite zuzugreifen.

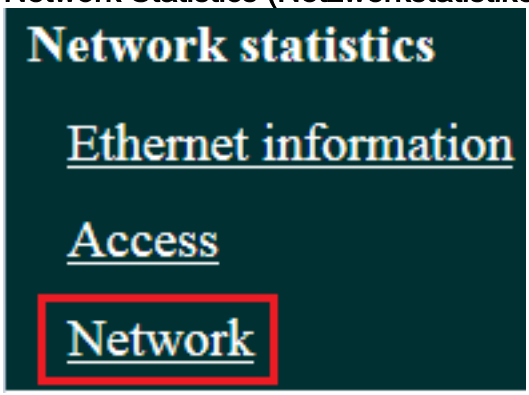
  HINWEIS: Überprüfen Sie das Feld "**Expires**" in der SIP-Registernachricht im pcap, wenn die Telefone SIP verwenden.

  Der Standardwert für das Feld **Expires (Abgelaufen)**, wenn die **REGISTER-**Nachricht vom Telefon an den primären CallManager gesendet wird, beträgt 120 Sekunden. Wenn das Telefon eine REGISTER-Nachricht sendet, die als "Keep-Alive"-Nachricht bezeichnet wird. Wenn es sich um einen sekundären CallManager-Server handelt, lautet das Feld "0" (Ablauf).

- Dokumentieren der Debug-Meldungen auf dem Telefon
- Überprüfen Sie, ob die Kerne am Telefon vorhanden sind, und laden Sie sie herunter, falls sie vorhanden sind. Stellen Sie sicher, dass Sie auch die Ausgabe von show **show core-dump** von der CLI des Telefons erfassen, wenn auf der Webschnittstelle des Telefons Kerne gefunden wurden.

  HINWEIS: Ab dem 9. November 2016 haben nur die Entwickler von Telefonen Zugriff auf das Tool zum Überprüfen von Telefonkerndateien. Wenn eine weitere Analyse des Kerns erforderlich ist, erstellen Sie ein TAC-Ticket, um die Telefonentwickler einzubinden.

- Holen Sie die **CDP-Nachbarinformationen** von der Seite **Network (Netzwerk)** im Abschnitt **Network Statistics (Netzwerkstatistiken) ein.**



CDP Neighbor device ID	**rtp12-pkinane-sw.cisco.com**
CDP Neighbor IP address	**14.48.38.251**
CDP Neighbor IPv6 address	
CDP Neighbor port	**FastEthernet0/5**

- Rufen Sie die Konsolenprotokolle vom Telefon ab. Wenn das Telefon die PRT-Funktion (Problem Report Tool) unterstützt, wird die Verwendung des PRT empfohlen.

  HINWEIS: In diesem Support-Forumsdokument wird die Verwendung von **Strace** zum Drucken der Debuggen in das Terminal erläutert. Möglicherweise müssen Sie jedoch **show strace** verwenden.

  Einige Telefone verwenden **sdump** anstatt **strace** oder **show strace**.

  Befehle für Strace oder **sdump** entsprechen der Eingabe von **Terminalmonitor** auf einem Cisco Router.

  TIPP: Es empfiehlt sich, die Konsolenprotokolle über die Befehlszeilenschnittstelle (CLI) des Telefons zu sammeln, da viele Telefone nur über begrenzten Speicherplatz verfügen und deren Protokolle schnell überschrieben werden.

  Wenn das Telefon über einen AUX-Anschluss verfügt, stecken Sie ein Konsolenkabel in das Telefon, um Debug-Aufgaben zu erfassen, selbst wenn das Telefon neu gestartet wird.

  TIPP: Am besten protokollieren Sie Ihre Terminalsitzung in einer Textdatei. Hier finden Sie Informationen dazu, wie Sie sich bei einer Textdatei mit putty anmelden und wie Sie dies mit SecureCRT tun.

Daten vom Switch

Das Telefon greift über einen Switch auf das Netzwerk zu. Identifizieren Sie den Switch, an den das Telefon angeschlossen ist, und erfassen Sie die unten aufgeführten Daten.

- Erfassen Sie **die aktuelle Konfiguration** mit **show run**
- Sammeln Sie **show proc cpu hist**
- Erfassen der Ausgabe des **Anzeigeprotokolls**

Daten aus dem CUCM

- Rufen Sie die Verzeichnisnummer (DN) des Telefons ab.

  HINWEIS: Wenn kein DN vorhanden ist und das Telefon das Session Initiation Protocol (SIP) verwendet, wird das Telefon nicht registriert.

- Rufen Sie die Konfigurationsdatei des Telefons ab.
- Pcaps von den CUCM-Servern abrufen
- Verwenden Sie das Real Time Monitoring Tool (RTMT) zum Erfassen von Protokollen und des Pcap von den CUCM-Servern. Achten Sie beim Erfassen der Protokolle darauf, alle Server auszuwählen.

  TIPP: Je nach Umgebung/Symptomatik können Sie einige oder alle der folgenden Protokolltypen sammeln:

  Cisco CallManager, Cisco Certificate Authority Proxy Function, Cisco TFTP, Cisco Trust Verification Service, Event Viewer-Application Log, Event Viewer-System Log und Packet Capture Logs.

- Erfassen Sie die Ausgabe von **show itl** und **show ctl** von allen TFTP-Servern im CUCM-Cluster.
- Erfassen Sie die Ausgabe dieser Befehle vom CUCM-Publisher:
  Stellen Sie fest, ob sich der Cluster im gemischten Modus befindet:

  sql select paramname,paramvalue from processing config, wobei paramname='ClusterSecurityMode'

  Stellen Sie fest, ob der Rollback-Parameter auf true festgelegt ist:

  sql select paramname,paramvalue from processing config, where paramname='RollBackToPreGrayback'

  Stellen Sie fest, ob die Datenbankreplikation fehlerfrei ist:

  utils dbreplication runtime state

  HINWEIS: Wenn sich der Cluster nicht im gemischten Modus befindet, sieht die Ausgabe wie folgt aus:

  admin:run sql select paramname,paramvalue from processing config where paramname='ClusterSecurityMode'

paramname paramame
==========
ClusterSecurityMode 0

HINWEIS: Wenn der Rollback-Parameter auf false festgelegt ist, sieht die Ausgabe wie folgt aus:

admin:run sql select paramname,paramvalue from processing config where paramname='RollBackToPreGrayback'
paramname paramame
==========
RollBackToPreGrayback F

TIPP: Eine Erklärung der Ausgabe aus utils dbreplication runtime state finden Sie im Understanding the output of utils dbreplication runtime state for CUCM document.

Überprüfen Sie die Telefonprotokolle

- Suchen Sie die Telefonprotokolle nach diesen Zeichenfolgen:
  Fehlgeschlagen
  Fehler
  Fehler
  Ausnahme
  newUnregReason=
  Lastoutofservice
  Fallback
  Socket error=
  opvlan
  JAVA-Sipio-
  REGISTRIERT
  Network_detect_change_task
  tftpAddr1=
  Gesperrt:
  VPN: (HINWEIS: Stellen Sie sicher, dass Sie mit regex nach diesem oder dem "" suchen. werden als Literal und nicht als Sonderzeichen analysiert)

Überprüfen Sie die CUCM-Protokolle

Suchen Sie in den CUCM-Protokollen nach folgenden Informationen:

- Die MAC-Adresse des Telefons
- Die IP-Adresse des Telefons

  TIPP: Wenn Sie Fehlermeldungen sehen, werden die Ursachencodes möglicherweise in den Dokumenten Fehler und Systemmeldungen erläutert.

Weitere Links

Häufig gestellte Fragen zu Endgeräten

Sicherheit standardmäßig

Richtlinien zur Unterstützung von Cisco IP-Telefon-Firmware

Durchsuchen Sie das Cisco Live-Repository

Protokolle und PCAP für praktische Anwendungen

Ich habe bereits einige Telefone registriert und die Protokolle/Pcaps gesammelt. Um die Dateien zu überprüfen, klicken Sie hier.