XMPP Federation auf Expressway konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Schritt 1: Aktivieren Sie XMPP Federation auf Expressway E Überprüfen der XMPP-Konfiguration auf Expressway Fehlerbehebung: XMPP Federation auf Expressway C und Expressway E Schritt 2: Dialback-geheim konfigurieren Überprüfen des DFÜ-Geheimhaltungsgrades Schritt 3: Sicherheitsmodus konfigurieren Fehlerbehebung im Sicherheitsmodus Häufige Fragen: Symptom 1: unidirektionales Messaging Das Internet zu extern funktioniert nicht. IM&P-Status ist aktiv Symptom 2: Föderation schlägt fehl, XCP-Router auf CUP bounce-Pakete Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument werden die Konfigurationsschritte für die XMPP-Föderation (Extensible Messaging and Presence Protocol) auf Expressway beschrieben.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Expressway X8.2 oder höher
- Unified Call Manager (CM) Instant Messanger (IM) und Presence Service 9.1.1 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen



Dieses Diagramm veranschaulicht die Kommunikation auf höchster Ebene:

Wenn Sie XMPP Federation auf Expressway aktivieren, wechselt der aktive Server zu Server (S2S) von Cisco Unified Presence (CUP) zum Expressway Edge (Expressway E). Diese Komponente verwaltet die gesamte XMPP-Kommunikation zwischen den verbundenen Domänen.

- S2S verwendet Port 5269 für die Kommunikation mit den verbundenen Domänen
- Interner XMPP-Datenverkehr zwischen XCP-Routern auf ExpresswayE, C und CUP wird auf Port 7400 ausgeführt.
- XMPP-Bereitstellungsinformationen von Expressway E werden über den SSH-Tunnel an Port 2222 an Expressway C gesendet
- Expressway C aktualisiert CUP mit den erforderlichen Routing-Informationen über den AXL-Port 8443

Konfigurieren

Schritt 1: Aktivieren Sie XMPP Federation auf Expressway E

Konfiguration > Unified Communication > Unterstützung der XMPP-Föderation > Ein

սիսիս	
CISCO	Cisco Expressway-E

status	System	Configuration	Applications	Users	Maintenance	
nified	Commu	nications				
Config	uration					
Unified	Communicatio	ons mode				Mobile and remote access ‡
XMPP 1	federation					
XMPP f	ederation sup	port				On : ()
Use sta	tic routes					Off : 1 Configure static routes for federated XMPP domains
Dialbac	k secret					*
Security	/ mode					No TLS ;
Dia	mode					Off : (i)

Save

Wenn Sie die XMPP-Föderation aktivieren, wird Folgendes beachtet:

1. Expressway-E aktualisiert die lokale Konfiguration und repliziert diese Einstellung mit Expressway Core (Expressway C).

Expressway E-Protokolle werden angezeigt: "Detail="xconfiguration xcpConfiguration is_Federation_enabled - geändert von: 0 bis: 1 Zoll

2. Expressway-C aktualisiert die Tabelle "xmpps2sknoten" in der CUP-Datenbank mit den Realms der Expressway E S2S Komponente.

Expressway C-Protokolle werden angezeigt: "Module="network.axl" Level="INFO" Action="Senden" URL="<u>https://cups.ciscotac.net:8443/axl/</u>" Function="executeSQLQuery"

3. Stellen Sie sicher, dass der öffentliche DNS mit den SRV-Datensätzen des XMPP-Servers für alle Domänen aktualisiert wird, für die eine Föderation erforderlich ist.

_xmpp-server._tcp.domain.com auf Port 5269

Überprüfen der XMPP-Konfiguration auf Expressway

Schritt 1: Überprüfen Sie, ob die Datenbankänderungen erfolgreich vom IM&P-Server übernommen wurden, indem Sie diese Abfrage über die CUP-Befehlszeilenschnittstelle (CLI) ausführen:

admin:run sql select * from xmpps2sknoten pchild cp_id

055c13d9-943d-459d-a3c6-af1d176936d cm-2_s2scp-1.eft-xwye-a-coluc-com Administrator:

Schritt 2: Überprüfen Sie, ob der XMPP-Verbund auf dem IM&P-Server deaktiviert ist:

Presence > Inter-Domain Federation > XMPP Federation > Settings > XMPP Federation Node Status > Off

Fehlerbehebung: XMPP Federation auf Expressway C und Expressway E

Schritt 1: .Enable the DEBUG level log:

Auf Expressway-E:

Wartung > Diagnose > Erweitert > Support-Protokollkonfiguration > developer.clusterdb.restapi

Auf Expressway-C:

Wartung > Diagnose > Erweitert > Support-Protokollkonfiguration > developer.clusterdb.restapi

Wartung > Diagnose > Erweitert > Netzwerkprotokollkonfiguration > network.axl

Schritt 2: Starten Sie das Diagnoseprotokoll und TCP-Dumps auf Expressway-C und Expressway-E:

Wenn ein Netzwerkproblem vermutet wird, führen Sie die Paketerfassung auf IM&P-Seite von der CLI aus:

"utils network capture eth0 file axl_inject.pcap count 1000000 size all"

Schritt 3: Aktivieren Sie die XMPP-Föderation auf Expressway-E.

Warten Sie 30 Sekunden. Gehen Sie anschließend die Schritte durch, die unter "Überprüfen der XMPP-Konfiguration auf Expressway" beschrieben sind.

Schritt 2: Dialback-geheim konfigurieren

Konfiguration > Unified Communication > Dialback Secret

1111111	
CISCO	Cisco Expressway-E

itatus System Configuration Application	ons Users Maintenance	() Help. Og Logout
nified Communications		You are here: Configuration > Unified Communications > Configuratio
Juccess: Saved		
Configuration		
Unified Communications mode	Mobile and remote access 🗧 🧃	
XMPP federation		
XMPP federation support	On ; ()	
Use static routes	Off : Configure static routes f	or federated XMPP domains
Dialback secret	*	
Security mode	No TLS 📫	
Privacy mode	(Off :)	
Save		
Unified Communications service configuration status		
SIP registrations and provisioning on Unified CM	Configur	ed (See Unified Communications status)
IM and Presence services on Unified CM	Configur	red (See Unified Communications status)
KMPP federation	Configur	ed (See Unified Communications status)
Related tasks		
View XMPP federation activity in the event log		

Wie funktioniert die Rückwahl?



Schritt 1: Der initiierende Server berechnet auf Basis des geheimen konfigurierten Wählergebnisses und sendet ihn an den empfangenden Server.

Schritt 2: Der empfangende Server validiert diese Ergebnisse mit dem autoritativen Server der

initiierenden Domäne.

Schritt 3: Da der autoritative Server denselben Wählgeheimnis teilt, kann das Ergebnis validiert werden.

Schritt 4: Nach der Validierung akzeptiert der empfangende Server XMPP vom initiierenden Server.

Schritt 5: Der initiierende Server führt eine Suche nach dem Empfänger-Server "_xmpp-server._tcp.<target domain>" durch.

Schritt 6: Der empfangende Server sucht nach dem autoritativen Server _xmppserver._tcp.<orginating domain>

Schritt 7: Der autoritative Server kann mit dem initiierenden Server identisch sein.

Überprüfen des DFÜ-Geheimhaltungsgrades

Expressway zeigt dieses Debuggen an, wenn es sich um den initiierenden Server handelt:

XCP_CM2[12122]:.. Level="INFO" CodeLocation="stanza.Component.out" Detail="xcoder=34A9B60C8 Senden: <db:result from='coluc.com' to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762ef52ea9b03</db:result>"

XCP_CM2[12122]:.. Level="INFO" CodeLocation="ConnInfoHistory" Detail="Verbindungsstatusänderung: AUSSTEHEND->VERBUNDEN: ...

Expressway zeigt dieses Debuggen an, wenn es sich um den empfangenden Server handelt:

XCP_CM2[22992]:.. Level="VBOSE" CodeLocation="stanza.Component.in" Detail="xcoder=05E295A2B erhalten: <db:result from='coluc.com' to='vngtp.lab'>d780f198ac34a6dbd795fcdaf8762ef52ea9b03</db:result>"

XCP_CM2[22992]:.. Level="INFO" CodeLocation="Resolver.cpp:128" Detail= "Starting Resolver Lookup for 'coluc.com:puny=coluc.com:service=_xmpp-server._tcp:defport=0""

XCP_CM2[22992]:.. Level="INFO " CodeLocation="debug" Detail="(e5b18d01-fe24-4290-bba1a57788a76468, vngtp.lab:coluc.com, IN) gelöste Dialback-Adresse für host=coluc.com method=SRV dns-timings=(TOTAL:0.003157 SRV:0.002885)"

XCP_CM2[22992]:.. Level="INFO " CodeLocation="DBVerify.cpp:270" Detail="(e5b18d01-fe24-4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN) Der DBVerify-Stream ist offen. Senden von db:Paket überprüfen: <db:verify from='vngtp.lab' id='05E295A2B' to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03</db:verify>"

XCP_CM2[22992]:.. Level="INFO " CodeLocation="DBVerify.cpp:282" Detail="(e5b18d01-fe24-

4290-bba1-a57788a76468, vngtp.lab:coluc.com, IN) DBVerfy Received <db:verify from='coluc.com' id='05E295A2B' to='vngtp.lab' type='valide'>d780f198ac34a6d795fcdaf8762eaf52ea9b03</db:verify>

Expressway zeigt dieses Debuggen an, wenn es sich um den autoritativen Server handelt

XCP_CM2[5164]:..Level="INFO" CodeLocation="debug" Detail="xcoder=94A9B60C8 onStreamOpen: <stream:stream from='vngtp.lab' id='1327B794B' to='coluc.com' version='1.0' xml:lang='en-US.UTF-8' xmlns='jabber:server' xmlns:db='jabber:server:dialback' xmlns stream='http://etherx.jabber.org/streams'/>"

XCP_CM2[5164]:..Level="VBOSE" CodeLocation="stanza.Component.in" Detail="xcoder=94A9B60C8 erhalten: <db:verify from='vngtp.lab' id='05E295A2B' to='coluc.com'>d780f198ac34a6dbd795fcdaf8762eaf52ea9b03< /db:verify>"

XCP_CM2[5164]:..Level="INFO" CodeLocation="stream.in" Detail="xcoder=94A9B60C8-Abschlussstream wird nur für die Rückwahl verwendet"

Schritt 3: Sicherheitsmodus konfigurieren

Status System Configuration	Applications Users Maintenance	? ~
Inified Communications	You are here: Configurati	on Unified Communications Configuratio
Configuration		
Unified Communications mode	Mobile and remote access ;	
XMPP federation		
XMPP federation support	On ; ()	
Use static routes	Off : Configure static routes for federated XMPP domains	
Dialback secret	*	
Security mode	No TLS :	
Privacy mode	TLS required TLS optional	

Fehlerbehebung im Sicherheitsmodus

- Wireshark kann zur Fehlerbehebung verwendet werden.
- Die Funktionen zeigen an, ob TLS (Transport Layer Security), OPTIONAL oder kein TLS erforderlich ist.

Dieses Extra zur Paketerfassung zeigt ein Beispiel dafür, wann TLS erforderlich ist:

				Y XMPP Protocol
Source	Destination	Protocollie	angth Info	▼ FEATURES(stream) []
Joouree	Descinación	111000001120	ingen inno	▼ STARTTLS [xmlns="urn:ietf:params:xml:ns:xmpp-tls"]
10.48.36.1/1	10.48.55.113	TCP	74 30353 > xmpp-	
10.48.55.113	10.48.36.171	TCP	/4 xmpp-server >	xmuns: urn:retr:params:xmu:ns:xmpp-uts
10.48.36.171	10.48.55.113	TCP	66 30353 > xmpp-:	REQUIRED
10.48.36.171	10.48.55.113	XMPP/XML	269 STREAM > colu	
10.48.55.113	10.48.36.171	TCP	66 xmpp-server	30353 [ACK] Seq=1 Ack=204 Win=30080 Len=0 TSval=1119100130 TSecr=1119103044
10.48.55.113	10.48.36.171	XMPP/XML	254 STREAM Scoluc	c.com
10.48.36.171	10.48.55.113	TCP	66 30353 S xmpp-s	server [ACK] Seg=204 Ack=189 Win=30336 Len=0 TSval=1119103044 TSecr=1119100130
10.48.55.113	10.48.36.171	XMPP/XML	173 FEATURES	
10.48.36.171	10.48.55.113	TCP	66 30353 > xmpp-s	server [ACK] Seg=204 Ack=296 Win=30336 Len=0 TSval=1119103046 TSecr=1119100131
10.48.36.171	10.48.55.113	XMPP/XML	117 STARTTLS	
10.48.55.113	10.48.36.171	XMPP/XML	116 PROCEED	
10.48.36.171	10.48.55.113	TCP	5 [ICP segment o	of a ssembled PDU)
10.48.55.113	10.48.36.171	TCP	434 [TCP segment of	of a reavery XMPP Protocol
10.48.55.113	10.48.36.171	ТСР	🖊 1369 [TCP segment d	of a rea
10.48.36.171	10.48.55.113	TCP	66 30353 > xmpp-s	server [
10.48.36.171	10.48.55.113	TCP	640 [TCP segment of	of a rea Xmins: urn:letT:params:Xml:ns:Xmpp-tis
10.48.55.113	10.48.36.171	TCP	292 [TCP segment of	of a rea
10.48.36.171	10.48.55.113	TCP	298 [TCP segment of	of a reassempted PDOI
10.48.55.11	VMDD Destas			
10,48,36,17	AMPP Protoc	01		Ack=3460 Win=41600 Len=0 TSval=1119103110 TSecr=111910015
10 48 55 11	▼ PROCEED [xmlns="urn	:ietf:params:xml	.:ns:xmpp-tls"]
101.0000111	xmlns:	urn:ietf:n	params:xml:ns:xmr	pp-tls
L	aireno.	a		

Beim Debuggen als SSL wird der TLS-Handshake angezeigt

Source	Destination	Protocol	Length I	Info
10.48.36.171	10.48.55.113	TCP	74 3	30353 > xmpp.servar [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1119103043 TSacr=0 W
10.48.55.113	10.48.36.171	TCP	74 x	xmpp-server > 30353 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=111910017
10.48.36.171	10.48.55.113	TCP	66 3	30353 > xmpp-server [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1119103043 TSecr=1119100129
10.48.36.171	10.48.55.113	TLSv1.2	269 0	Continuation Data
10.48.55.113	10.48.36.171	TCP	66 x	xmpp-server > 30353 [ACK] Seq=1 Ack=204 Win=30080 Len=0 TSval=1119100130 TSecr=1119103044
10.48.55.113	10.48.36.171	TLSv1.2	254 0	Continuation Data
10.48.36.171	10.48.55.113	TCP	66 3	30353 > xmpp-server [ACK] Seq=204 Ack=189 Win=30336 Len=0 TSval=1119103044 TSecr=1119100130
10.48.55.113	10.48.36.171	TLSv1.2	173 0	Continuation Data
10.48.36.171	10.48.55.113	TCP	66 3	30353 > xmpp-server [ACK] Seq=204 Ack=296 Win=30336 Len=0 TSval=1119103046 TSecr=1119100131
10.48.36.171	10.48.55.113	TLSv1.2	117 0	Continuation Data
10.48.55.113	10.48.36.171	TLSv1.2	116 0	Continuation Data
10.48.36.171	10.48.55.113	TLSv1.2	275 0	Client Hello
10.48.55.113	10.48.36.171	TLSv1.2	1434 5	Server Hello
10.48.55.113	10.48.36.171	TLSv1.2	1369 0	Certificate, Server Hello Done
10.48.36.171	10.48.55.113	TCP	66 3	30353 > xmpp-server [ACK] Seq=464 Ack=3017 Win=36096 Len=0 TSval=1119103049 TSecr=1119100134
10.48.36.171	10.48.55.113	TLSv1.2	640 0	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10.48.55.113	10.48.36.171	TLSv1.2	292 N	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
10.48.36.171	10.48.55.113	TLSv1.2	298 A	Application Data
10.48.55.113	10.48.36.171	TLSv1.2	283 A	Application Data
10.48.36.171	10.48.55.113	TCP	66 3	30353 > xmpp-server [ACK] Seq=1270 Ack=3460 Win=41600 Len=0 TSval=1119103110 TSecr=1119100156
10.48.55.113	10.48.36.171	TLSv1.2	113 A	Application Data
10.48.36.171	10.48.55.113	TCP	66 3	30353 > xmpp-server [ACK] Seq=1270 Ack=3507 Win=41600 Len=0 TSval=1119103110 TSecr=1119100195
10.48.36.171	10.48.55.113	TLSv1.2	190 A	Application Data
10.48.55.113	10.48.36.171	TCP	66 x	xmpp-server > 30353 [ACK] Seq=3507 Ack=1394 Win=33408 Len=0 TSval=1119100236 TSecr=1119103110
10.48.55.113	10.48.36.171	TLSv1.2	218 A	Application Data

Häufige Fragen:

Symptom 1: unidirektionales Messaging Das Internet zu extern funktioniert nicht. IM&P-Status ist aktiv

Auf Expressway-C-Protokollen:

"Function="executeSQLQuery" status="401" Grund="Keine"

Ursache 1: Falsche Anmeldeinformationen für den IM&P-Benutzer auf Expressway-C Seite.

Dies kann auch überprüft werden, indem Sie diese URL ausführen und sich mit den Anmeldeinformationen anmelden, die auf Expressway C konfiguriert sind.

Konfiguration > Unified Communications > IM und Presence Server

https://cups_address.domain.com:8443/axl

Lösung 1: Kennwort aktualisieren, CUP-Servererkennung aktualisieren

Symptom 2: Föderation schlägt fehl, XCP-Router auf CUP bounce-Pakete

Ursache 2: Der XCP-Router auf dem CUP wurde nicht neu gestartet.

Dies kann in der CUP-Verwaltung auf der Seite "Benachrichtigungen" überprüft werden.

ababa Cis	In Cisco Unified CM IM and Presence Administration				stration : Go
CISCO For (Cisco Unifi	3 ccmadmin	Search	Logout About	
System - Pres	esence 🕶	essaging + Application + Bulk Administration + Diagnostics + Help +			
Find and List N	otification				
Select All	Clea	All 💥 Delete Selected			
Status					
i 5 records	s found				
Notifications	(1-50	5)		Rows p	per Page 50 ÷
Find Notification	ins where O	gin begins with : Find Clear Filter			
Severity	Count	Description	Origin		Created
Δ	5	Cisco XCP Router : (ecup10s.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service here. Once the service is restarted, this notification will be deleted automatically.	Cisco XCP Config M	lanager J.	an 5, 2015 3:10:43 PM
Δ	5	Cisco XCP Router : (ecup10.coluc.com) requires a restart in order for recent configuration changes to take effect. You can restart this service here. Once the service is restarted, this notification will be deleted automatically.	Cisco XCP Config M	lanager J.	an 5, 2015 3:10:42 PM

Lösung 2: XCP-Router auf CUP neu starten

Manchmal gibt es keine Benachrichtigung, aber die XCP-Router-Anmeldung beim CUP bounce-Pakete. Wenn das Neustarten des XCP-Routerdiensts dies nicht behebt, wird der IM&P-Cluster neu gestartet.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

<u>Technischer Support und Dokumentation - Cisco Systems</u>