

Probleemoplossing voor Cisco Jabber-zoekproblemen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Jabber-loganalyse](#)

[Packet Capture Analysis](#)

[Oplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij het zoeken naar een directory Cisco Jabber wanneer Secure Socket Layer (SSL) is ingesteld.

Bijgedragen door Khushbu Shaikh, Cisco TAC-engineers. Bewerkt door Sumit Patel en Jasmeet Sandhu

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Jabber voor Windows
- Wireshark

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

Jabber folder search werkt niet als SSL is ingesteld.

Jabber-loganalyse

Jabber-logbestanden tonen deze fout:

```
Directory searcher LDAP://gblidmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not found, adding server gblidmauthp01.sealedair.corp to blacklist.
```

```
2016-10-21 08:35:47,004 DEBUG [0x000034ec] [rdsresource\ADPersonRecordSourceLog.cpp(50)] [csf.person.adsourc] [WriteLogMessage] - ConnectionManager::GetDirectoryGroupSearcher - Using custom credentials to connect [LDAP://gblidmauthp02.sealedair.corp:389] with tokens [1]
```

```
2016-10-21 08:35:47,138 DEBUG [0x000034ec] [rdsresource\ADPersonRecordSourceLog.cpp(50)] [csf.person.adsourc] [WriteLogMessage] - ConnectionManager::GetDirectoryGroupSearcher - failed to get a searcher - COMException [0x80072027]
```

Packet Capture Analysis

Bij deze pakketvastlegging kan worden gezien dat de TCP-verbinding (Transmission Control Protocol) met de AD-server (Active Directory) succesvol is, maar dat de SSL-handdruk tussen de client en de LDAP-server lichtgewicht Directory Access Protocol (LDAP) mislukt. Dit zorgt ervoor dat Jabber een FIN-bericht verstuurt in plaats van de versleutelde sessie-sleutel voor de communicatie.

343	2016-10-26	17:16:41.086863000	10.8.64.32	172.22.174.228	TCP	66 54155-636 [SYN, ACK] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
344	2016-10-26	17:16:41.093563000	172.22.174.228	10.8.64.32	TCP	66 636-54155 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1
345	2016-10-26	17:16:41.093640000	10.8.64.32	172.22.174.228	TCP	54 54155-636 [ACK] Seq=1 Ack=1 Win=65536 Len=0
346	2016-10-26	17:16:41.093988000	10.8.64.32	172.22.174.228	TLSv1	191 Client Hello
347	2016-10-26	17:16:41.100193000	172.22.174.228	10.8.64.32	TCP	60 636-54155 [ACK] Seq=1 Ack=138 Win=15680 Len=0
348	2016-10-26	17:16:41.102128000	172.22.174.228	10.8.64.32	TLSv1	1423 Server Hello
349	2016-10-26	17:16:41.102128000	172.22.174.228	10.8.64.32	TCP	1423 [TCP segment of a reassembled PDU]
350	2016-10-26	17:16:41.102129000	172.22.174.228	10.8.64.32	TLSv1	115 Certificate
351	2016-10-26	17:16:41.102180000	10.8.64.32	172.22.174.228	TCP	54 54155-636 [ACK] Seq=138 Ack=2800 Win=65536 Len=0
352	2016-10-26	17:16:41.102914000	10.8.64.32	172.22.174.228	TCP	54 54155-636 [FIN, ACK] Seq=138 Ack=2800 Win=65536 Len=0
353	2016-10-26	17:16:41.104996000	10.8.64.32	172.22.180.59	TCP	66 54156-636 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
354	2016-10-26	17:16:41.108922000	172.22.174.228	10.8.64.32	TCP	60 636-54155 [FIN, ACK] Seq=2800 Ack=139 Win=15680 Len=0

De kwestie blijft bestaan, ook al wordt het ondertekende AD-certificaat geüpload naar de trustwinkel van de klant PC.

Uit verdere analyses van de pakketvastlegging blijkt dat de serververificatie niet is verricht in het vak Uitgebreide sleutel voor gebruik van het AD-servercertificaat.

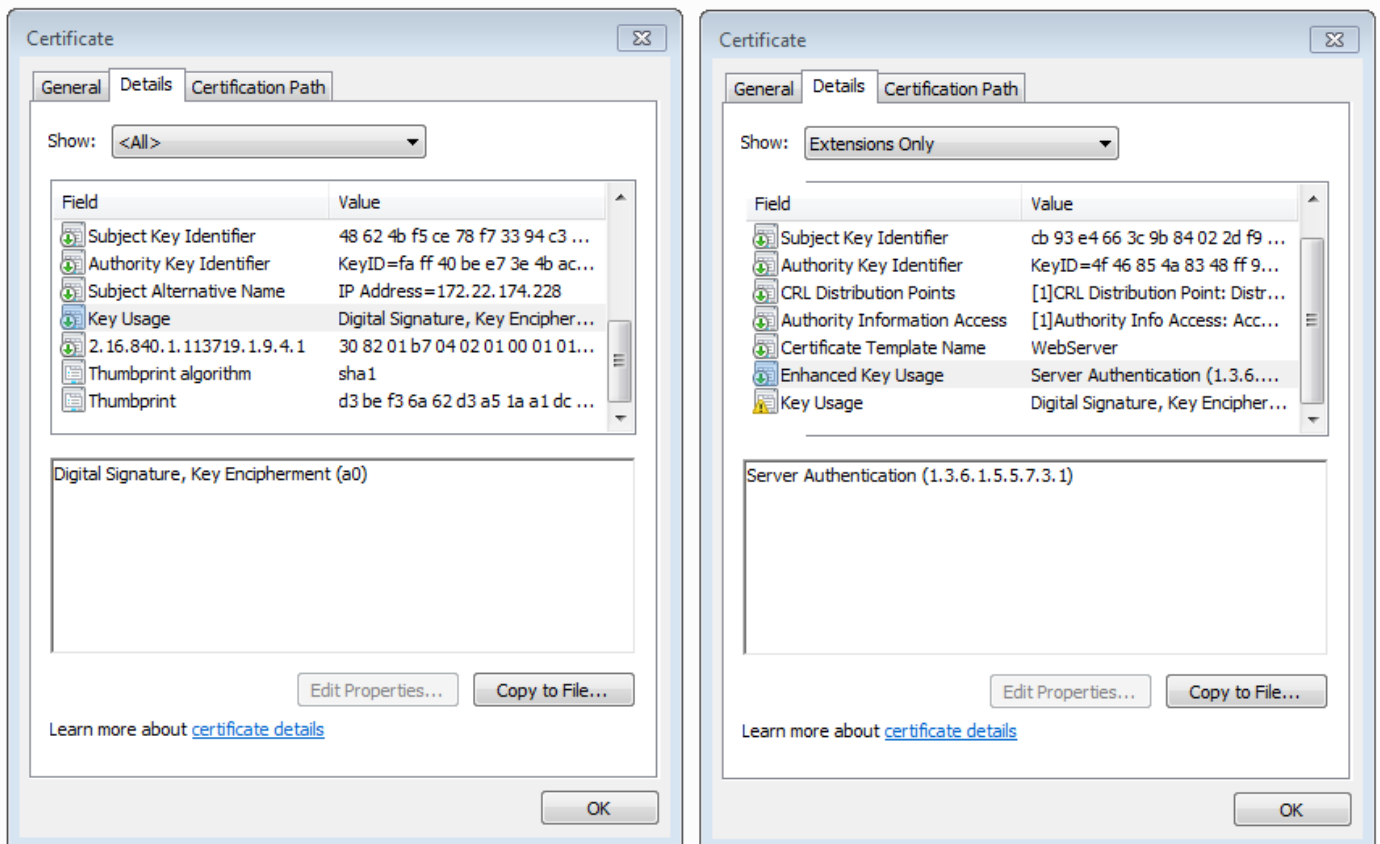
```

Certificate: 308205463082042ea0030201020224021c11ffa5290aa0e3... (id-at-commonName=gblldmauthp01.sealedair.corp,id-at-organi:
  signedCertificate
    version: v3 (2)
    serialNumber: 0x021c11ffa5290aa0e3110e51ee38b93ad70008edb0ec5c9b...
    signature (sha1WithRSAEncryption)
  issuer: rdnSequence (0)
    rdnSequence: 2 items (id-at-organizationName=SAC_AUTH_PROD,id-at-organizationalUnitName=Organizational CA)
  validity
  subject: rdnSequence (0)
    rdnSequence: 2 items (id-at-commonName=gblldmauthp01.sealedair.corp,id-at-organizationName=SAC_AUTH_PROD)
  subjectPublicKeyInfo
  extensions: 5 items
    Extension (id-ce-subjectKeyIdentifier)
    Extension (id-ce-authorityKeyIdentifier)
    Extension (id-ce-subjectAltName)
    Extension (id-ce-keyUsage)
      Extension Id: 2.5.29.15 (id-ce-keyUsage)
      Padding: 5
      KeyUsage: a0 (digitalSignature, keyEncipherment)
    Extension (pa-sa)
      Extension Id: 2.16.840.1.113719.1.9.4.1 (pa-sa)
      SecurityAttributes
        versionNumber: 0100
        nSI: True
        securityTM: Novell Security Attribute(tm)
        uriReference: http://developer.novell.com/repository/attributes/certattrs_v10.htm
      gLBExtensions
  algorithmIdentifier (sha1WithRSAEncryption)
  Padding: 0

```

Oplossing

Een scenario werd gecreëerd met een certificaat dat de Verificatie van de Server in Uitgebreid Gebruik heeft dat de kwestie oplost. Zie de afbeeldingen van de certificaten voor vergelijking.



De identificatie van de serververificatie in het certificaat is een voorwaarde voor een succesvolle SSL-handdruk.

Gerelateerde informatie

<https://www.petri.com/enable-secure-ldap-windows-server-2008-2012-dc>