Fehlerbehebung bei Problemen mit der Suche im Cisco Jabber-Verzeichnis

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie bei der Konfiguration von Secure Socket Layer (SSL) ein Problem bei der Suche im Cisco Jabber-Verzeichnis beheben können.

Mitarbeiter: Khushbu Shaikh, Cisco TAC Engineers. Bearbeitet von Sumit Patel und Jasmeeting Sandhu

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Jabber für Windows
- Wireshark

Verwendete Komponenten

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

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.

Problem

Die Suche im Jabber-Verzeichnis funktioniert nicht, wenn SSL konfiguriert ist.

Jabber-Protokollanalyse

Jabber-Protokolle zeigen diesen Fehler an:

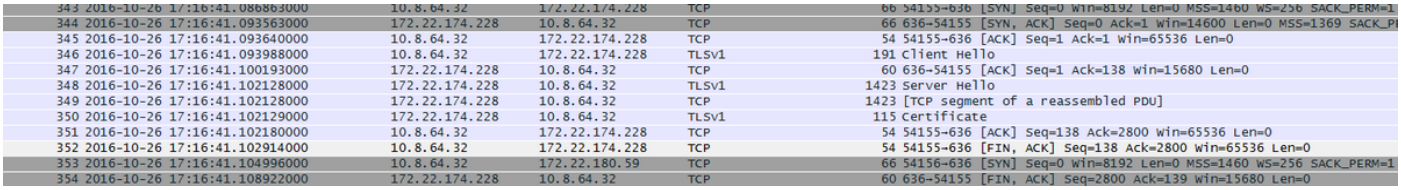
```
Directory searcher LDAP://gbllidmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not
found, adding server gbllidmauthp01.sealedair.corp to blacklist.

2016-10-21 08:35:47,004 DEBUG [0x000034ec] [rdsource\ADPersonRecordSourceLog.cpp(50)]
[csf.person.adsource] [WriteLogMessage] - ConnectionManager::GetDirectoryGroupSearcher - Using
custom credentials to connect [LDAP://gbllidmauthp02.sealedair.corp:389] with tokens [1]


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

Paketerfassungsanalyse

Bei dieser Paketerfassung ist zu erkennen, dass die TCP-Verbindung (Transmission Control Protocol) zum Active Directory (AD)-Server erfolgreich ist, der SSL-Handshake zwischen dem Client und dem Lightweight Directory Access Protocol (LDAP)-Server jedoch fehlschlägt. Dies veranlasst Jabber, eine FIN-Nachricht anstatt des verschlüsselten Sitzungsschlüssels für die Kommunikation zu senden.



343	2016-10-26 17:16:41.086863000	10.8.64.32	172.22.174.228	TCP	66	54155→636 [SYN] 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_P
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

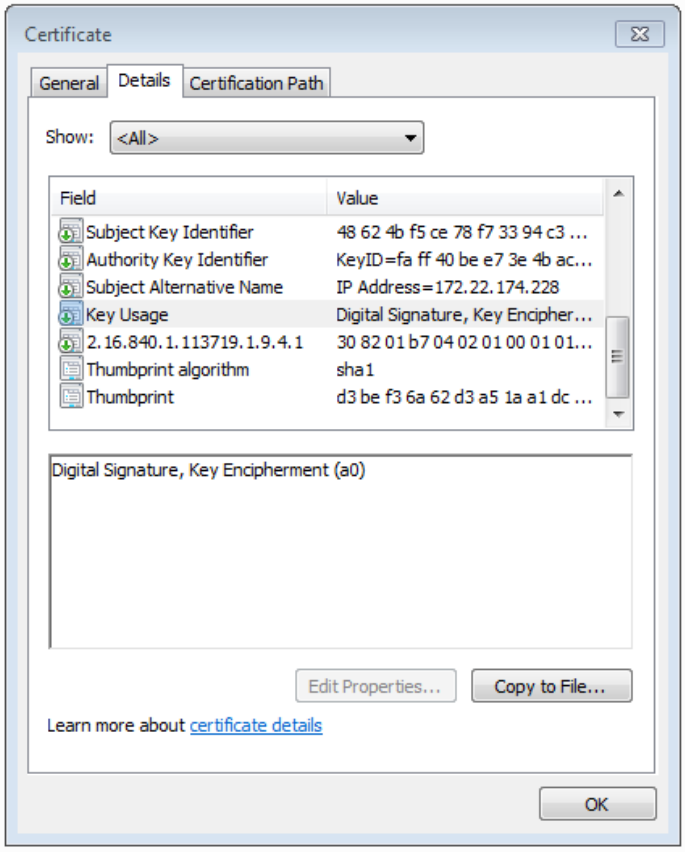
Das Problem besteht weiterhin, obwohl das signierte AD-Zertifikat in den Trust Store des Client-PCs hochgeladen wird.

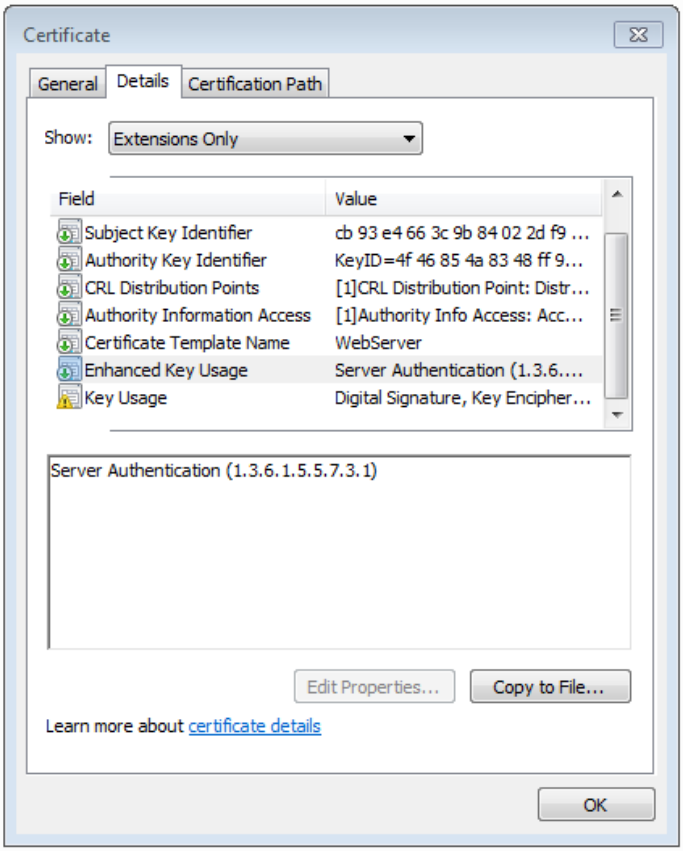
Weitere Analysen der Paketerfassung zeigen, dass die Serverauthentifizierung im Abschnitt "Enhanced Key Usage" des AD-Serverzertifikats vorkommt.

```
Certificate: 308205463082042ea0030201020224021c11ffa5290aa0e3... (id-at-commonName=gbllidmauthp01.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=gbllidmauthp01.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
```

Lösung

Ein Szenario wurde mit einem Zertifikat neu erstellt, das über die Serverauthentifizierung unter Verwendung erweiterter Schlüssel verfügt, wodurch das Problem behoben wurde. Vergleichen Sie die Bilder der Zertifikate.





Der Serverauthentifizierungsbezeichner im Zertifikat ist eine Voraussetzung für einen erfolgreichen SSL-Handshake.

Zugehörige Informationen

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