排除Cisco Jabber目錄搜尋問題

目錄

簡介

本文描述如何在配置安全套接字層(SSL)時排除Cisco Jabber目錄搜尋問題。

作者：Khushbu Shaikh，思科TAC工程師。Sumitt Patel和Jasmeet Sandhu編輯

必要條件

需求

思科建議您瞭解以下主題：

- Windows 版 Jabber
- Wireshark

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

配置SSL時，Jabber目錄搜尋不起作用。

Jabber日誌分析

Jabber日誌顯示以下錯誤：

```
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]
```

封包擷取分析

在此封包擷取中，可以看到與Active Directory(AD)伺服器的傳輸控制通訊協定(TCP)連線成功，但使用者端和輕量型目錄存取通訊協定(Lightweight Directory Access Protocol, LDAP)伺服器之間的SSL交握失敗。這導致Jabber傳送FIN報文而不是通訊的加密會話金鑰。

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

即使已簽名的AD證書已上載到客戶端PC的信任儲存，此問題仍然存在。

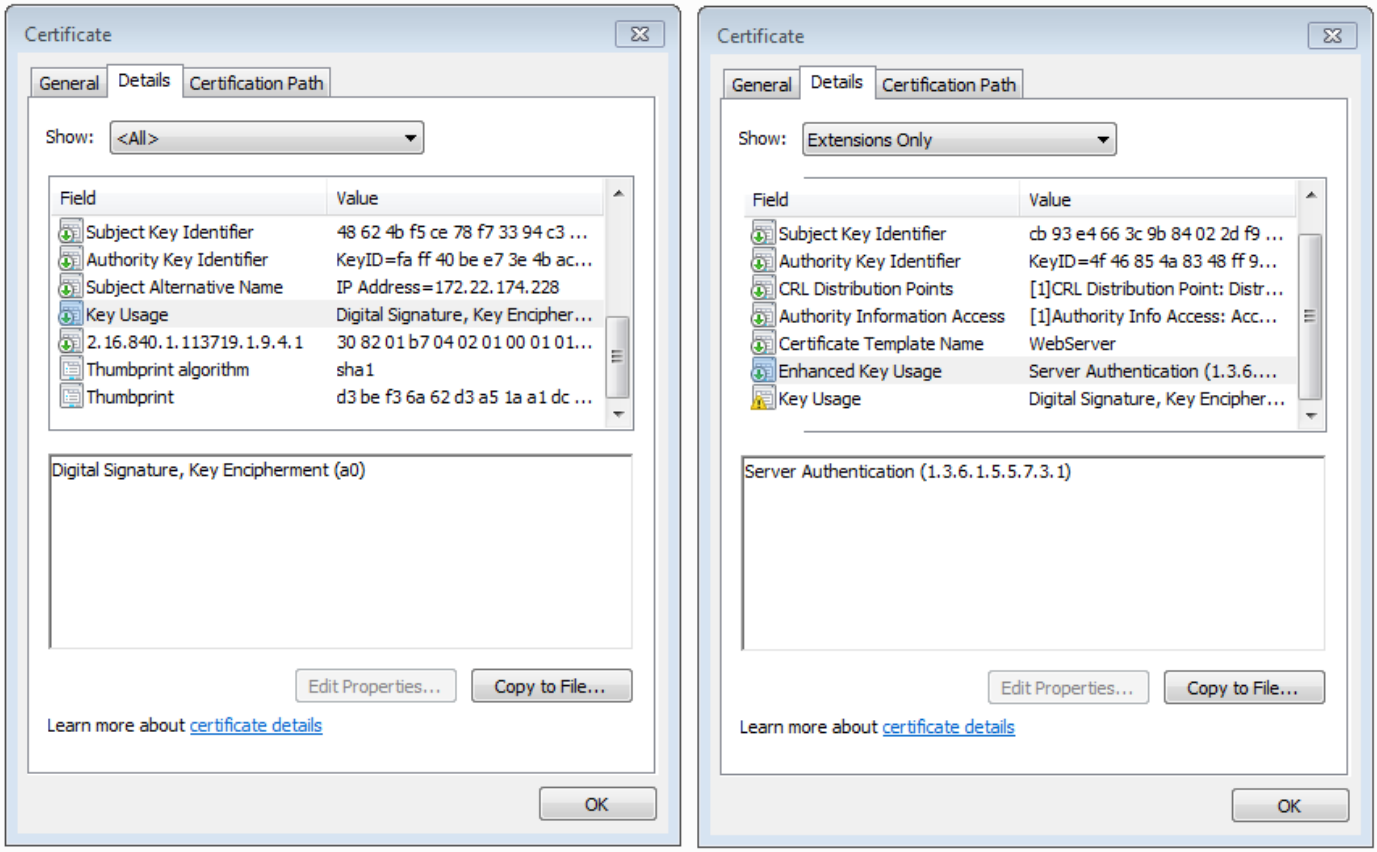
對資料包捕獲的進一步分析顯示，AD伺服器證書的「增強型金鑰使用」部分中的「伺服器身份驗證」已丟失。

```
▲ Certificate: 308205463082042ea003020102022402 1c11ffa5290aa0e3... (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
```

解決方案

使用增強型金鑰使用中的伺服器身份驗證解決了問題的證書重新建立了一個方案。請參閱證書影象

進行比較。



證書中的伺服器身份驗證識別符號是成功的SSL握手的前提條件。

相關資訊

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