排除Cisco Jabber目录搜索问题

目录

简介

本文档介绍如何在配置安全套接字层(SSL)时排除Cisco Jabber目录搜索问题。

作者：Khushbu Shaikh，Cisco TAC工程师。苏米特·帕特尔、贾斯梅特·桑杜编辑

先决条件

要求

Cisco 建议您了解以下主题：

- Windows 版 Jabber
- Wireshark

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

配置SSL时，Jabber目录搜索不起作用。

Jabber日志分析

Jabber日志显示以下错误：

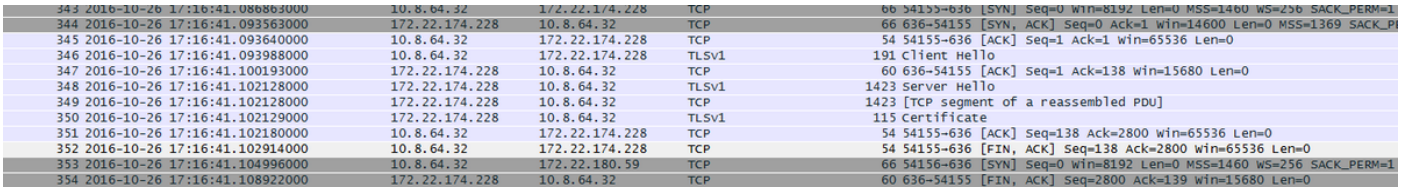
```
Directory searcher LDAP://gbllidmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not
found, adding server gbllidmauthp01.sealedair.corp to blacklist.

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]
```

数据包捕获分析

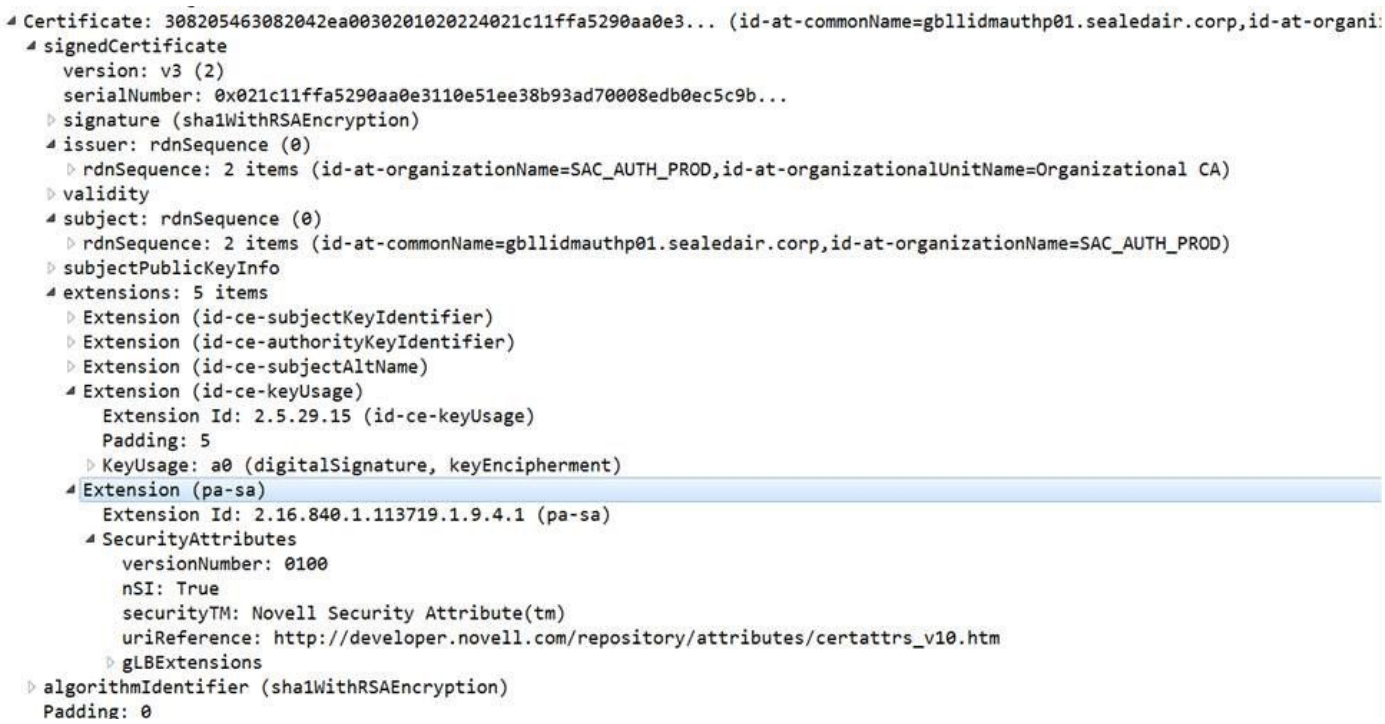
在此数据包捕获中，可以看到到Active Directory(AD)服务器的传输控制协议(TCP)连接成功，但客户端与轻量目录访问协议(LDAP)服务器之间的SSL握手失败。这会导致Jabber发送FIN消息，而不是用于通信的加密会话密钥。



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

即使已签名的AD证书上传到客户端PC的信任存储，问题仍然存在。

对数据包捕获的进一步分析显示，AD服务器证书的“增强密钥使用”(Enhanced Key Usage)部分中的“服务器身份验证”(Server Authentication)已消失。

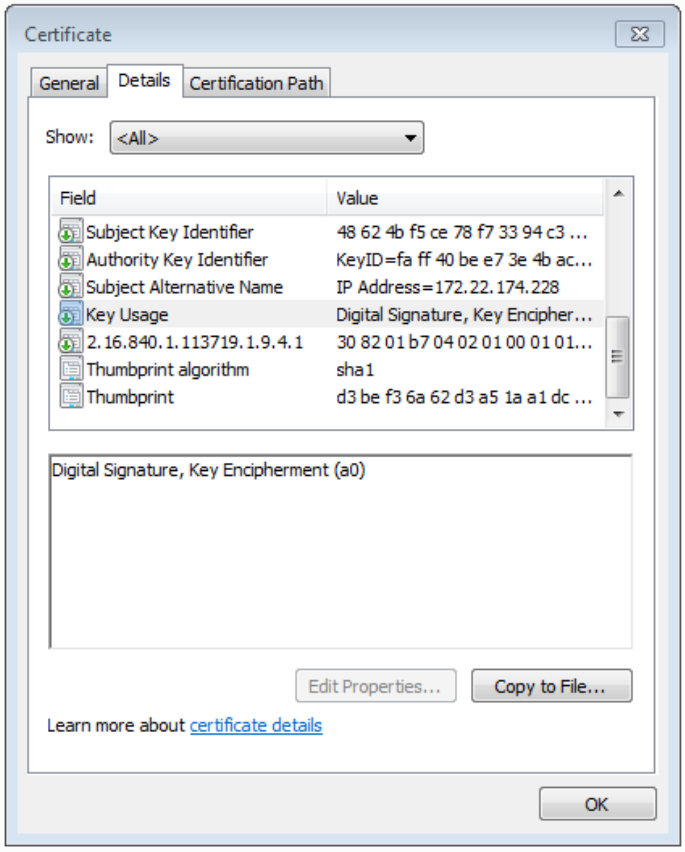


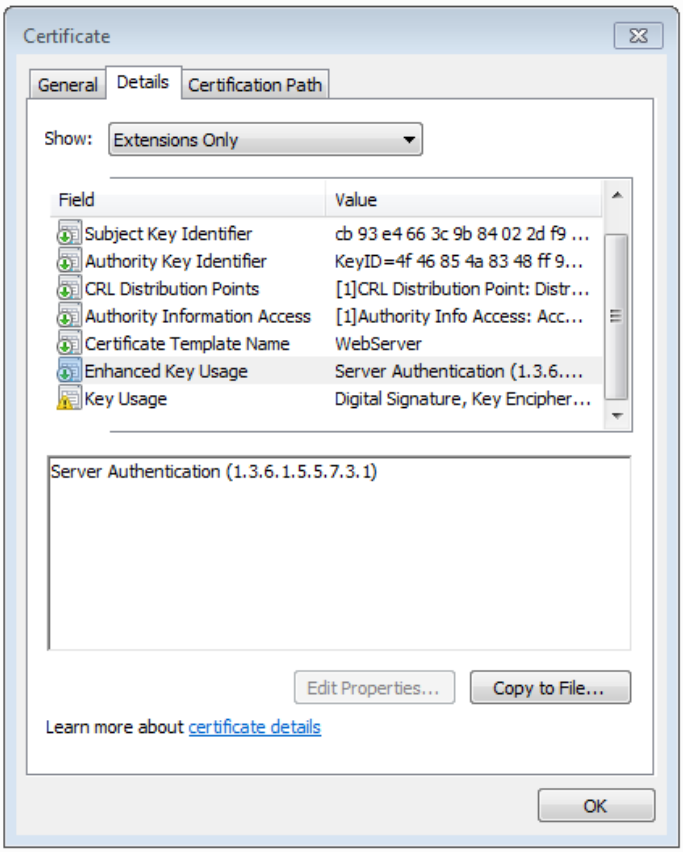
```
▲ Certificate: 308205463082042ea003020102022021c11ffa5290aa0e3... (id-at-commonName=gbllidmauthp01.sealedair.corp,id-at-organi
  ▲ signedCertificate
      version: v3 (2)
      serialNumber: 0x021c11ffa5290aa0e3110e51ee38b93ad70008edb0ec5c9b...
    ▷ signature (sha1WithRSAEncryption)
    ▲ issuer: 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
```

解决方案

已使用“增强密钥使用”中的服务器身份验证解决了该问题的证书重新创建方案。请参阅证书的映像

以进行比较。





证书中的服务器身份验证标识符是成功SSL握手的先决条件。

相关信息

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