Solución de problemas de búsqueda en el directorio de Cisco Jabber

Contenido

Introducción

Este documento describe cómo resolver el problema de búsqueda del directorio Cisco Jabber cuando se configura Secure Socket Layer (SSL).

Contribuido por Khushbu Shaikh, Ingenieros del TAC de Cisco. Editado por Sumit Patel y Jasmeet Sandhu

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Jabber para Windows
- Wireshark

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

La búsqueda en el directorio Jabber no funciona cuando se configura SSL.

Análisis de registro de Jabber

Los registros de Jabber muestran este error:

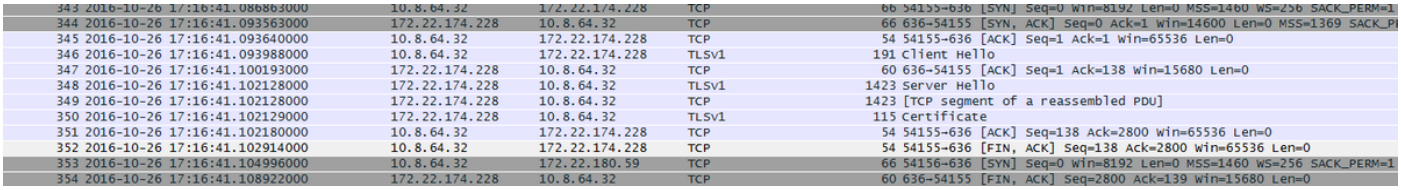
```
Directory searcher LDAP://gbllidmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not
found, adding server gbllidmauthp01.sealedair.corp to blacklist.

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]
```

Análisis de captura de paquetes

En esta captura de paquetes, se puede ver que la conexión TCP (del inglés Transmission Control Protocol, protocolo de control de transmisión) al servidor de Active Directory (AD) es correcta, pero el intercambio de señales SSL entre el cliente y el servidor LDAP (del inglés Lightweight Directory Access Protocol, protocolo ligero de acceso a directorios) falla. Esto hace que Jabber envíe un mensaje FIN en lugar de la clave de sesión cifrada para la comunicación.



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

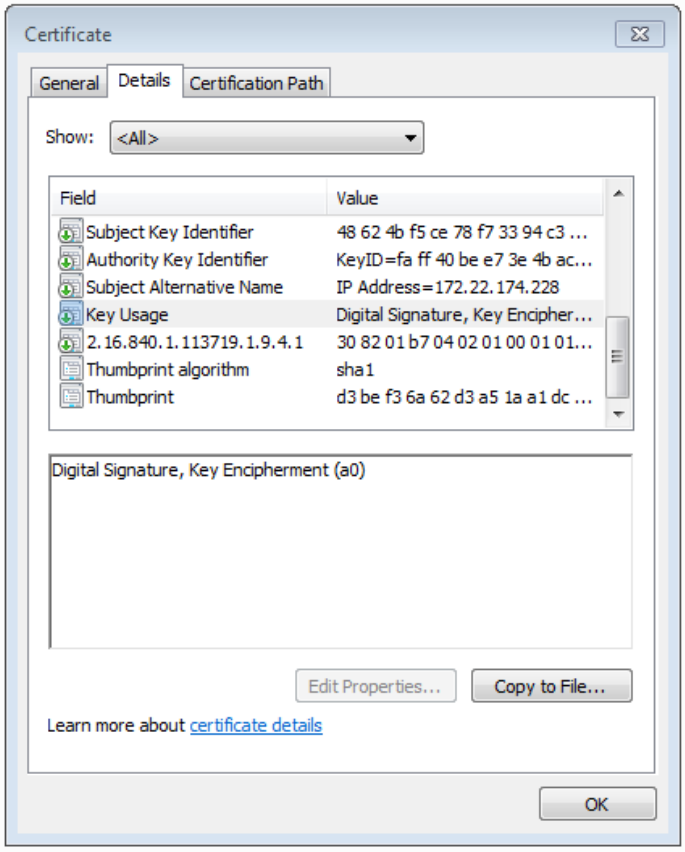
El problema persiste aunque el certificado AD firmado se carga en el almacén de confianza del equipo cliente.

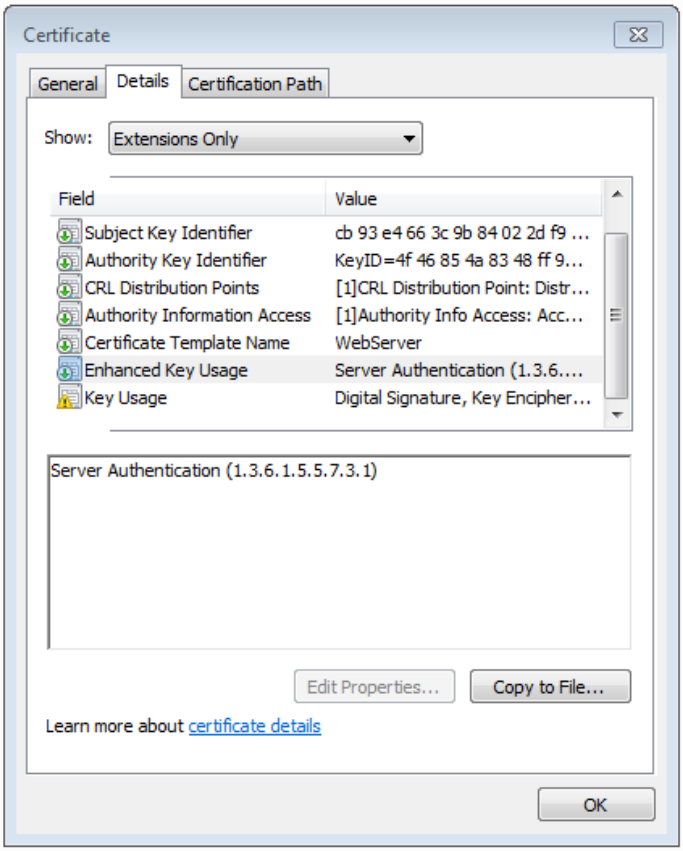
Los análisis adicionales de la captura de paquetes revelan que la autenticación del servidor ha desaparecido en la sección Uso mejorado de claves del certificado del servidor AD.

```
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
```

Solución

Se volvió a crear un escenario con un certificado que tiene la autenticación del servidor en el uso mejorado de claves que resolvió el problema. Consulte las imágenes de los certificados para su comparación.





El identificador de autenticación del servidor en el certificado es un requisito previo para un intercambio de señales SSL exitoso.

Información Relacionada

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