Problemas de Búsqueda de directorio del Jabber de Cisco del Troubleshooting

Contenido

Introducción

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

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

Prerrequisitos

Requisitos

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.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Problema

La Búsqueda de directorio del Jabber no trabaja cuando se configura el SSL.

Análisis del registro del Jabber

Los registros del Jabber muestran este error:

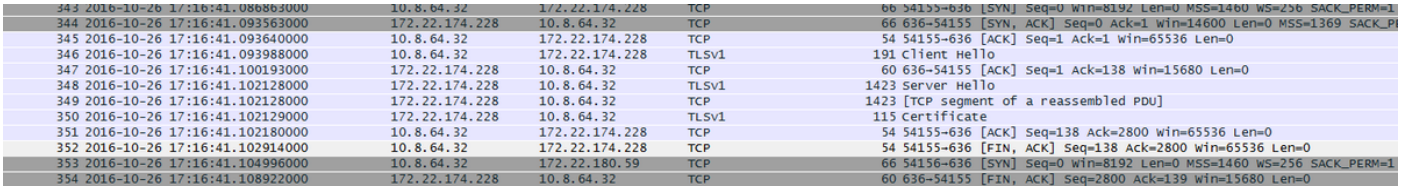
```
Directory searcher LDAP://gbllidmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not
found, adding server gbllidmauthp01.sealedair.corp to blacklist.

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 la captura de paquetes

En esta captura de paquetes, puede ser visto que la conexión del (TCP) de Protcol del control de transmisión al servidor del Active Directory (AD) es acertado pero el contacto SSL entre el cliente y el servidor del Lightweight Directory Access Protocol (LDAP) falla. Esto hace el Jabber enviar un mensaje FIN en vez de la clave de sesión encriptada 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

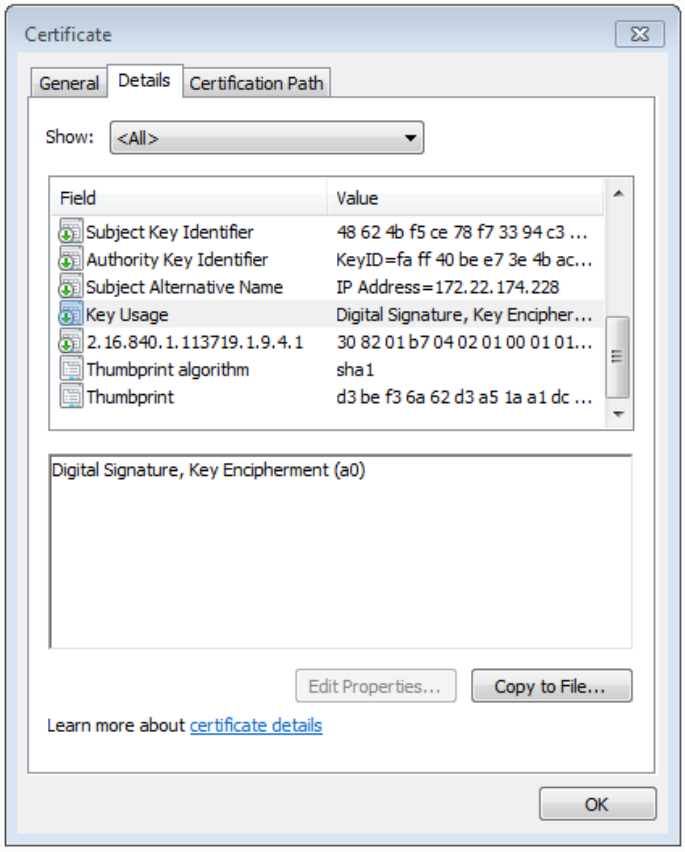
El problema todavía persiste aunque el certificado firmado AD está cargado al almacén de la confianza del cliente el PC.

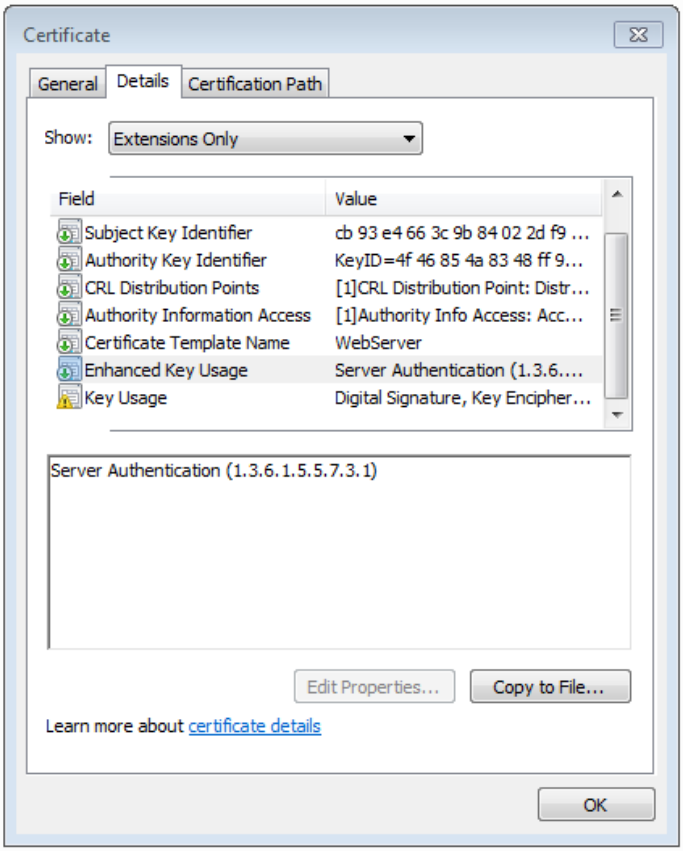
Analiza más lejos de la captura de paquetes revela que la autenticación de servidor está entrada en la sección del Enhanced Key Usage del certificado de servidor AD.

```
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
```

Solución

Un escenario fue reconstruido con un certificado que tiene la autenticación de servidor en el Enhanced Key Usage que resolvieron el problema. Vea las imágenes de los Certificados para la comparación.





El identificador de la autenticación de servidor en el certificado es un requisito previó para un contacto SSL acertado.

Información Relacionada

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