Cisco Jabberディレクトリ検索の問題のトラブルシューティング

内容

概要

このドキュメントでは、Secure Socket Layer(SSL)が設定されている場合に、Cisco Jabberディレクトリ検索の問題をトラブルシューティングする方法について説明します。

著者：Cisco TACエンジニア、Khusbu Shaikh編集：Sumit Patel、Jasmeet Sandhu

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Jabber for Windows
- Wireshark

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

SSLが設定されている場合、Jabberディレクトリ検索は機能しません。

Jabber口グ分析

Jabber口グに次のエラーが表示されます。

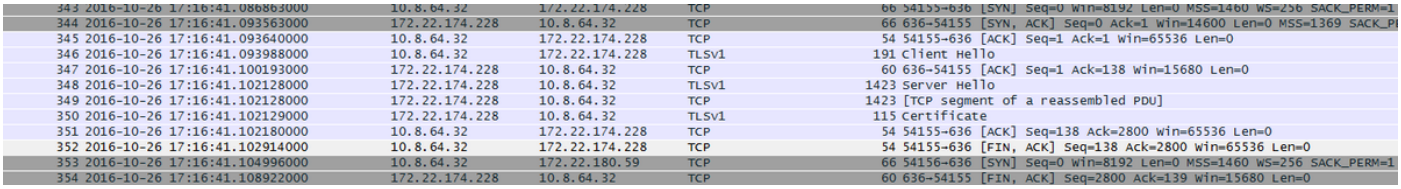
```
Directory searcher LDAP://gbllidmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not
found, adding server gbllidmauthp01.sealedair.corp to blacklist.

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]
```

パケットキャプチャ分析

このパケットキャプチャでは、Active Directory(AD)サーバへのTransmission Control Protocol(TCP)接続は成功していますが、クライアントとLightweight Directory Access Protocol(LDAP)サーバ間のSSLハンドシェイクが失敗していることが分かります。これにより、Jabberは通信の暗号化されたセッションキーの代わりにFINメッセージを送信します。



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

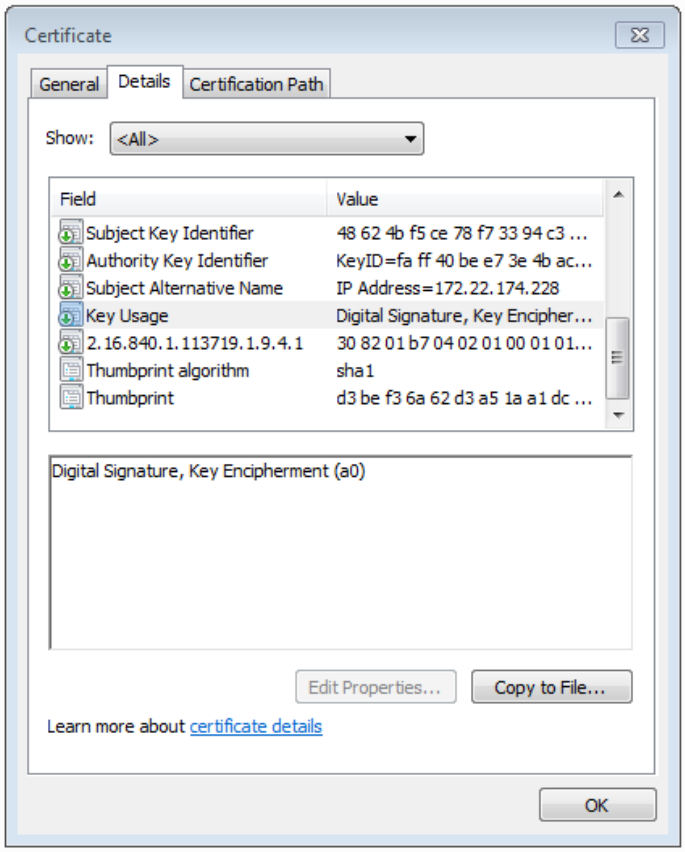
署名付きAD証明書がクライアントPCの信頼ストアにアップロードされても、問題は解決しません。

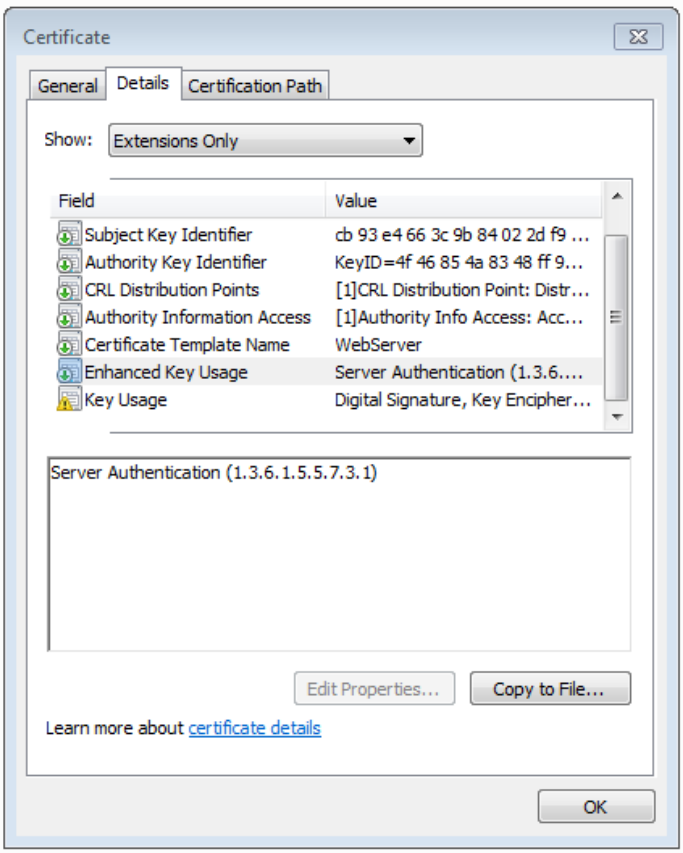
パケットキャプチャの詳細な分析により、ADサーバ証明書の[Enhanced Key Usage]セクションにサーバ認証が含まれていることが明らかになります。

```
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
```

解決方法

拡張キー使用法のサーバ認証を持つ証明書でシナリオが再作成され、問題が解決されました。比較については、証明書のイメージを参照してください。





証明書のサーバ認証識別子(SSID)は、SSLハンドシェイクが成功するための前提条件です。

関連情報

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