

# Solucionar problemas de pesquisa do Cisco Jabber Directory

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Análise de log do Jabber](#)

[Análise de Captura de Pacotes](#)

[Solução](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como solucionar problemas de pesquisa de diretório do Cisco Jabber quando o Secure Socket Layer (SSL) está configurado.

Contribuído por Khushbu Shaikh, engenheiros do TAC da Cisco. Editado por Sumit Patel e Jasmeet Sandhu

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Jabber para Windows
- Wireshark

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Problema

A pesquisa de diretório Jabber não funciona quando o SSL está configurado.

# Análise de log do Jabber

Os registros do Jabber mostram este erro:

```
Directory searcher LDAP://gblldmauthp01.sealedair.corp:389/ou=Internal,ou=Users,o=SAC not found, adding server gblldmauthp01.sealedair.corp to blacklist.
```

```
2016-10-21 08:35:47,004 DEBUG [0x000034ec] [rds\source\ADPersonRecordSourceLog.cpp(50)] [csf.person.ads\source] [WriteLogMessage] - ConnectionManager::GetDirectoryGroupSearcher - Using custom credentials to connect [LDAP://gblldmauthp02.sealedair.corp:389] with tokens [1]
```

```
2016-10-21 08:35:47,138 DEBUG [0x000034ec] [rds\source\ADPersonRecordSourceLog.cpp(50)] [csf.person.ads\source] [WriteLogMessage] - ConnectionManager::GetDirectoryGroupSearcher - failed to get a searcher - COMException [0x80072027]
```

## Análise de Captura de Pacotes

Nesta captura de pacote, pode-se ver que a conexão TCP (Transmission Control Protocol) com o servidor do Active Directory (AD) foi bem-sucedida, mas o handshake SSL entre o cliente e o servidor Lightweight Directory Access Protocol (LDAP) falha. Isso faz com que o Jabber envie uma mensagem FIN em vez da chave de sessão criptografada para a comunicação.

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		

O problema ainda persiste, embora o certificado do AD assinado seja carregado no armazenamento confiável do PC cliente.

Análises adicionais da captura de pacotes revelam que a Autenticação do Servidor foi removida na seção Uso Avançado de Chave do certificado do servidor AD.

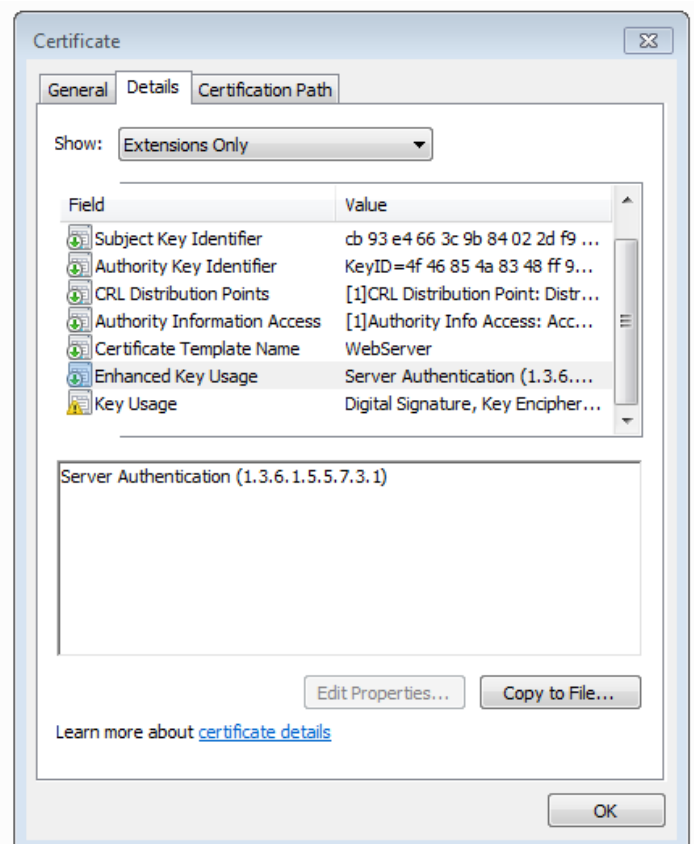
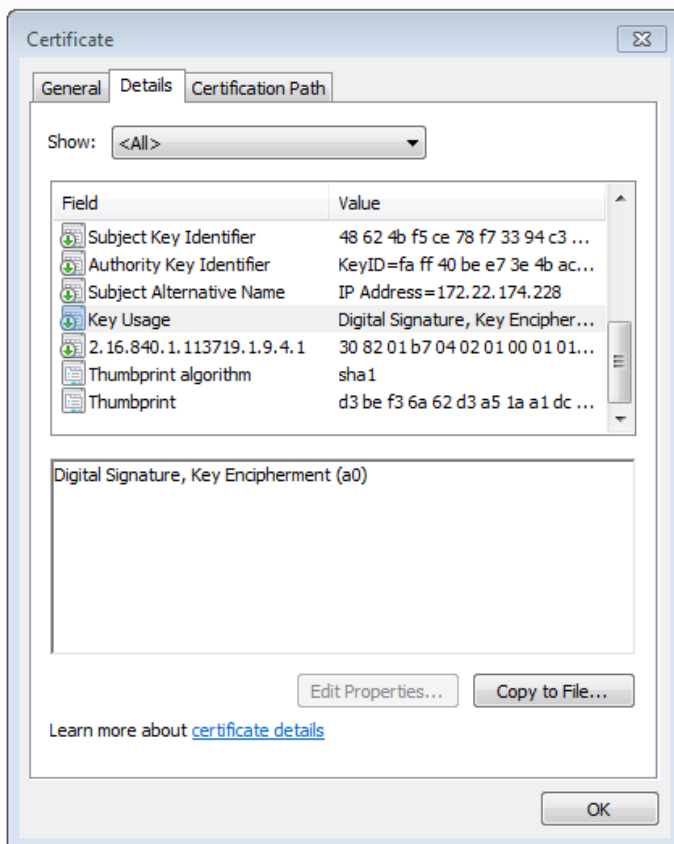
```

Certificate: 308205463082042ea0030201020224021c11ffa5290aa0e3... (id-at-commonName=gblldmauthp01.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=gblldmauthp01.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
        gLBEExtensions
    algorithmIdentifier (sha1WithRSAEncryption)
    Padding: 0

```

## Solução

Um cenário foi recriado com um certificado que tem a Autenticação de Servidor em Uso Avançado de Chave que resolveu o problema. Veja as imagens dos certificados para comparação.



O identificador de autenticação de servidor no certificado é um pré-requisito para um handshake SSL bem-sucedido.

## Informações Relacionadas

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