



SSL/TLS发生原因secd ldap.noServers的证书已过期

https://kb-cn-stage.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/secd_ldap_noServers_in_EMS_when...

Updated: Wed, 22 Apr 2026 08:24:21 GMT

适用场景

- ONTAP
- 第三方LDAP服务器
- SSL/TLS

问题描述

- 在现有LDAP配置上启用SSL/TLS后、由于与LDAP服务器的连接失败、存储访问可能会受到影响
- EMS 日志：

```
secd.ldap.noServers: None of the LDAP servers configured for Vserver (VS1) are currently accessible via the network for LDAP service type (Service: LDAP (Active Directory), Operation: SiteDiscovery).
```

```
secd.ldap.noServers: None of the LDAP servers configured for Vserver (VS1) are
```

'NetApp provides no representations or warranties regarding the accuracy or reliability or serviceability of any information or recommendations provided in this publication or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS and the use of this information or the implementation of any recommendations or techniques herein is a customers responsibility and depends on the customers ability to evaluate and integrate them into the customers operational environment. This document and the information

currently accessible via the network for LDAP service type (Service: LDAP (Active Directory), Operation: MapNetbiosDomainToADDomain).

- **Secd**日志：

```
error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed
```

```
RESULT_ERROR_LDAPSERVER_SERVER_DOWN:7642
```

```
LDAP TLS Alert generated is 'fatal:decrypt error'
```

```
error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01
```

```
RESULT_ERROR_LDAPSERVER_CONNECT_ERROR:7652
```

```
secd: secd.unexpectedFailure:debug]: vserver (VSERVER) Unexpected failure.
```

```
Error: Get DC Info procedure failed CIFS Domain Query via
```

```
LSAR_DS_ROLE_GET_DOMAIN_INFO - Client Ip = X.X.X.X
```

```
User = DOMAIN\USER ...
```

```
[ 236] Successfully connected to ip X.X.X.X, port 389 using TCP
```

```
[ 377] Unable to start TLS: Connect error
```

```
[ 377] Additional info: error:14090086:SSL
```

```
routines:ssl3_get_server_certificate:certificate verify failed (certificate has expired)
```

```
...
```

- **Secd**日志条目将包含预期证书的主题

```
00000013.0022c89e 01eab99b Mon Apr 06 2020 14:31:44 +01:00
```

```
[kern_sec:info:14641] | [000.499.972] info : Required certificate with <CANAME> is not installed { in VerifyCertificateRevocationViaOSCP() at src/connection_manager/secd_connection.cpp:1667 }
```

- 到期日期在CLI命令中指示到期日期： `::> security certificate show`

- 数据包跟踪可以显示完整的证书链由客户端提供

LDAP服务器示例提供了一个由两个证书组成的证书链

- 一个是主机本身的证书(由颁发者**CA**颁发的**ldapservershostname**)，
- 其他，中间证书(由根**CA**颁发的颁发者**CA**)

Transport Layer Security

TLsv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages

Content Type: Handshake (22)

```

Version: TLS 1.2 (0x0303)
Length: 2911
Handshake Protocol: Server Hello
Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 2587
  Certificates Length: 2584
  Certificates (2584 bytes)
    Certificate Length: 1208
      Certificate: 308204b43082039ca0030201020213160000802cf3c5747b...
      (id-at-commonName=LDAPserverhostname)
        signedCertificate
          version: v3 (2)
          serialNumber: 0x160000802cf3c5747b5475eb2100000000802c
          signature (sha256WithRSAEncryption)
            issuer: rdnSequence (0)
              rdnSequence: 3 items (id-at-commonName=Issuer CA )
            validity
              subject: rdnSequence (0)
              subjectPublicKeyInfo
                extensions: 9 items
              algorithmIdentifier (sha256WithRSAEncryption)
              Padding: 0
              encrypted:
d403151937a2904d0405e5fe7be043a51969650e43cc27e0...
              Certificate Length: 1370
            Certificate: 308205563082033ea00302010211114500000002578509d7...
            (id-at-commonName=Issuer CA )
              signedCertificate
                version: v3 (2)
                serialNumber: 0x4500000002578509d77c523cae000000000002
                signature (sha256WithRSAEncryption)
                  issuer: rdnSequence (0)
                    rdnSequence: 3 items (id-at-commonName=Root CA)

```

- 在此示例中、Root CA 必须安装的根证书