FXOS에서 LDAPS 구성

목차

소개

이 문서에서는 FCM(Secure Firewall Chassis Manager) 및 CLI를 사용하여 FXOS에서 LDAPS(Secure LDAP)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FXOS(Secure Firewall eXtensible Operating System)
- FCM(보안 방화벽 섀시 관리자)
- LDAP(Lightweight Directory Access Protocol) 개념

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Secure Firewall 9300 디바이스 버전 2.12(0.8)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설정

일반 LDAP가 보안 방화벽 디바이스에서 작동하는지 테스트하는 것이 좋습니다.

일반 LDAP 구성

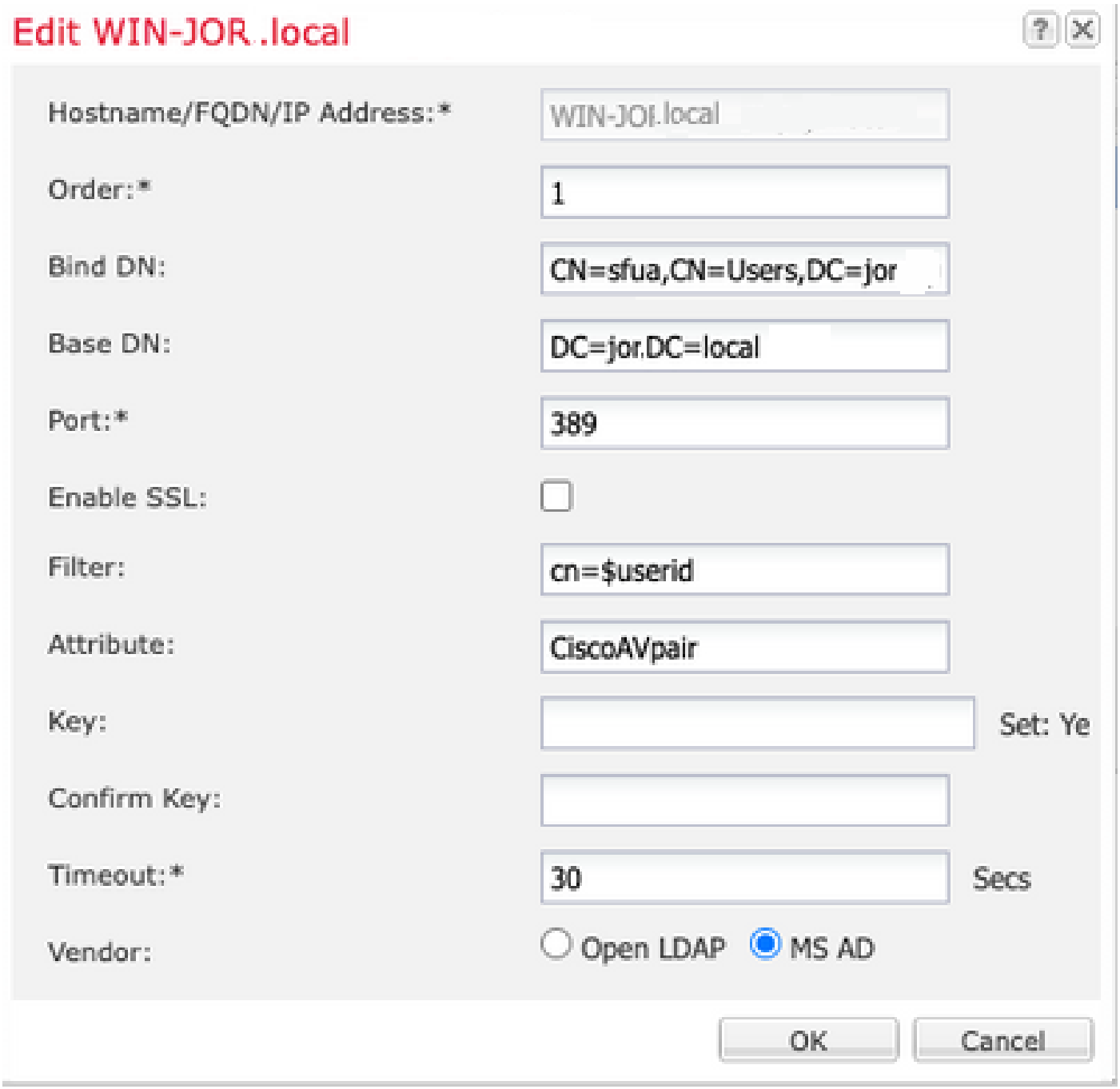
1. FCM에 로그인합니다.

2. Platform Settings(플랫폼 설정) > AAA > LDAP로 이동합니다

3. LDAP Providers(LDAP 제공자) > Add(추가)를 클릭합니다

4. LDAP 공급자를 구성하고 Microsoft Active Directory(MS AD)에 대한 바인딩 DN, 기본 DN, 특성 및 키 정보를 입력합니다.

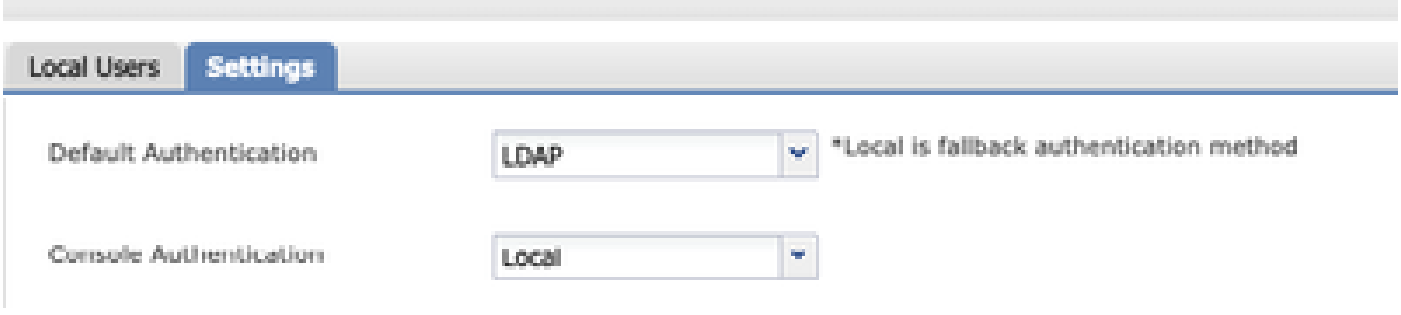
5. SSL 연결에 필요하므로 LDAP 서버의 FQDN을 사용합니다.



LDAP 컨피그레이션

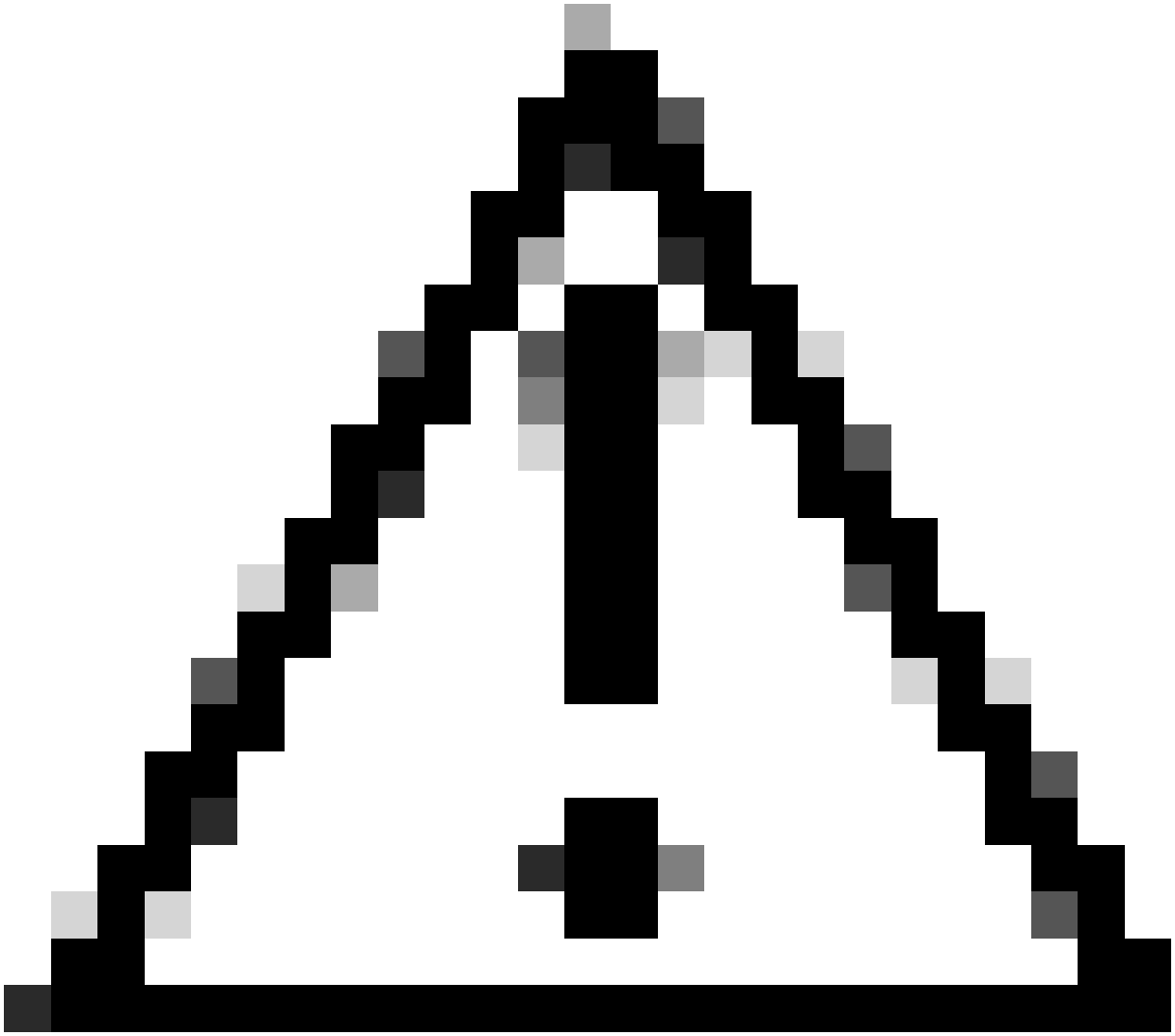
6. 시스템 > 사용자 관리 > 설정으로 이동합니다.

7. Default(기본값) 또는 Console(콘솔) 인증을 LDAP로 설정합니다.



인증 방법 선택

8. LDAP 사용자와의 인증을 테스트하려면 SSH에서 섀시로 로그인하십시오.



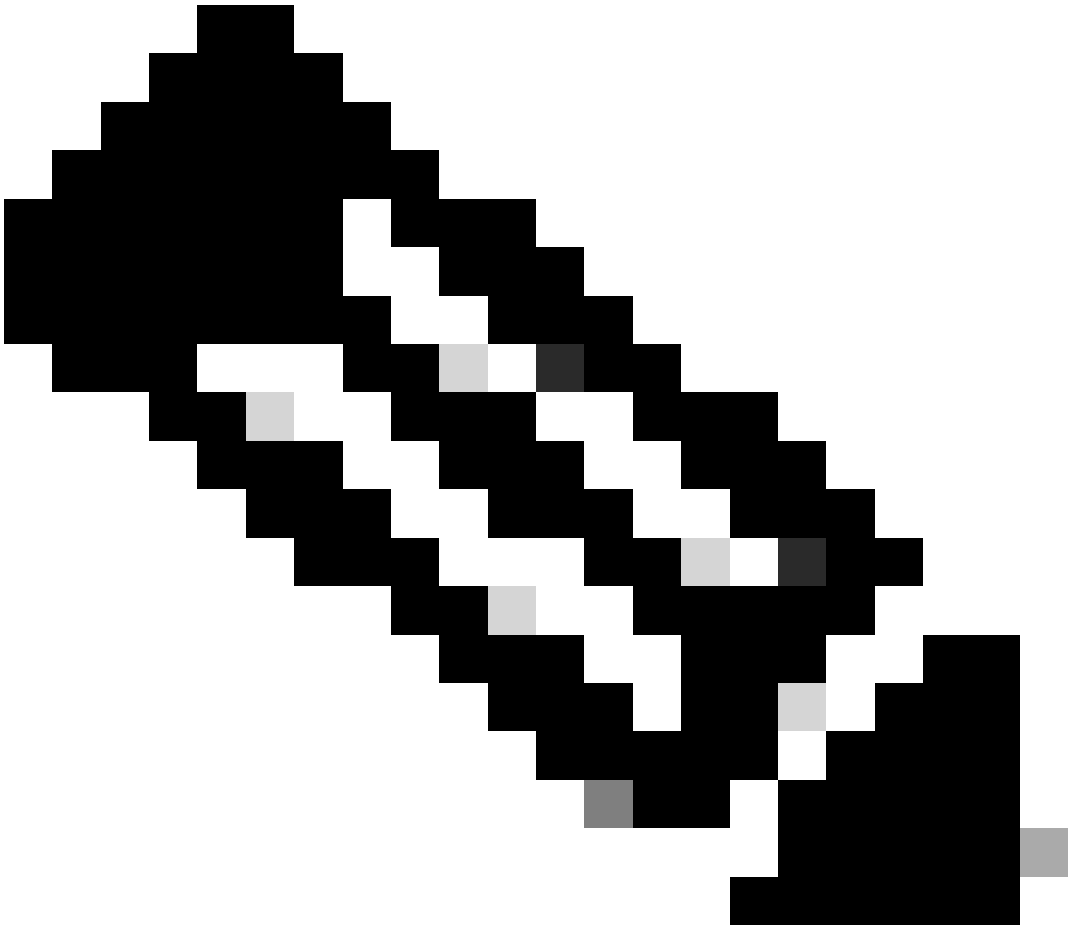
주의: LDAP 인증을 테스트할 때는 주의하십시오. 컨피그레이션에 오류가 있는 경우 이 변경으로 인해 잠길 수 있습니다. 중복 세션으로 테스트하거나 로컬 인증으로 콘솔 액세스에서 테스트하여 롤백 또는 문제 해결을 수행할 수 있습니다.

LDAPS 구성

9. 성공적인 LDAP 연결을 테스트했으면 Platform Settings(플랫폼 설정) > AAA > LDAP로 다시 이동합니다.

10. LDAP 제공자를 편집하고 SSL을 활성화합니다.

포트 선택 GUI



참고: 암호화에 포트 389를 사용해야 합니다. 포트 636이 작동하지 않습니다. 개선 사항 Cisco 버그 ID CSCwc93347이 LDAPS에 대한 맞춤형 포트를 추가하도록 제출되었습니다.

---

11. LDAP 서버의 루트 CA 인증서를 섀시로 가져와야 합니다. 중간 인증서가 있는 경우 체인을 함께 가져옵니다.

FXOS CLI에서 신뢰 지점을 생성하여 이 작업을 수행합니다.

<#root>

FPR9300-01#

scope security

FPR9300-01 /security #

create trustpoint LDAPS

>^CFPR9300-01 /security/trustpoint* #

set certchain

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:

>-----BEGIN CERTIFICATE-----

>

MIIDmTCCAoGgAwIBAgIQYPxqSJxdYLJCpz+rOqfXpjANBgkqhkiG9w0BAQsFADBT

>MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAVBgoJkiaJk/IsZAEZFgdqb3JnZWp1

>MSEwHwYDVQQDExhqb3JnZWp1LVdJTi1KT1JHRUpVLUNBLTEwHhcNMjEwMzIzMDc0

>MDAwWhcNMjYwMzIzMDc0OTU5WjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFzAV

>BgoJkiaJk/IsZAEZFgdqb3JnZWp1MSEwHwYDVQQDExhqb3JnZWp1LVdJTi1KT1JH

>RUpVLUNBLTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDmBTWU6Leu

>bPxvc+EhC7fxjowEjjL0EXlMo3x7Pe3EW6Gng2iOMB1UpBNgSObbct83P6y6EmQi

>0RCCnEFfzy4stYPz/7499wALwMLSGNQWr10rjVB64ihfugbx95iDBcwuv6XK67h/

>T1caN4GZiLtYZjURGs5mLNB2f8hLp9QR2WoZqfAvrfvFB4I5RJjx0FYKIXW1dmPT

>AAPa/Qi+1Qv1exfzvXHXx1GMDCHle2yItFgl6o7OujT0AE3oplA/qQD+mTAJmdcR

>QLUDiUptqqYKgcbrH4Hu4PMje3INLd1vw1ThAwMFn+oXjRTM0KbEQ0/JEM6xRFMv

>LqmzDwxA8IoRAgMBAAGjaTBnMBMGCSsGAQQBgjcUAgQGHgQAQwBBMA4GA1UdDwEB

>/wQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQoweZEEke7BIOd94R5

>YxjvJHdzSjAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAyGli

>n77K0OiqSljTeg+ClVLRX8VJwr7Pp5p4Mu0mRhZckmIKSUtYDla3ToVix5k4dXSU

>7MaVWDkW/1NvReaqCfis5mgfrpzoPUkqKGiz7Zhd57gA4tBU/XbP/CXpTuAR3Isa

>NKz7yy+6tisf+8vfLtRN8c3IclS6ncyrdAdJ2iJY74jJm1eUPs3muaqApPPwoRF2

>GdALD/Y+Pq36cSjK+jGP1+2rD6cW16thBp9plOOTL+qpq4DL+W6uctWeRMgGxcWn

>GsKhHysno9dZ+DnnOlx0tP+S1B9fmxF7ycCmmn328dZVEG7JXjHc8KoqwwWe+fwu

>GXLRM+rKaAICH52EEw==

>-----END CERTIFICATE-----

>ENDOFBUF

FPR9300-01 /security/trustpoint* #

commit-buffer

12. LDAP 제공자에 구성된 대로 LDAP 서버 컨피그레이션을 입력합니다. LDAP 서버의 이름을 기록해 둡니다.

13. 폐기 정책을 완화로 설정합니다.

<#root>

FPR9300-01 /security #

scope ldap

FPR9300-01 /security/ldap #

show server

```
LDAP server:
Hostname, FQDN or IP address DN to search and read Port SSL Key CRL Password
---------------------------- ---------------------- ----- ---- ----- ---- --------
WIN-JOR.jor.local CN=sfua,CN=Users,DC=jor,DC=local
```

```
389 Yes Strict ****


FPR9300-01 /security/ldap #
scope server WIN-JOR.jor.local
FPR9300-01 /security/ldap/server #
set revoke-policy relaxed

FPR9300-01 /security/ldap/server* #
commit-buffer


FPR9300-01 /security/ldap/server #
show

LDAP server:
Hostname, FQDN or IP address DN to search and read Port SSL Key CRL Password
------------------------------ ----------------------- ----- ---- ----- ---- --------
WIN-JOR.jor.local CN=sfua,CN=Users,DC=jor,DC=local
389 Yes Relaxed ****
```

14. commit-buffer를 사용하여 변경 사항을 저장합니다.

문제 해결

DNS 확인

FQDN이 올바른 IP로 확인되고 있는지 확인하십시오. 이름 확인에 문제가 있을 수 있습니다.

```
<#root>
FPR9300-01#
connect fxos

FPR9300-01(fxos)#
ethanalyzer local interface mgmt capture-filter "udp port 53" limit-captured-frames 100
Capturing on 'eth0'

1 2024-02-01 11:36:43.822089169 10.4.23.202 → 10.88.243.91 DNS 85 Standard query 0x1b86 AAAA WIN-JOR.jor.loca

2 2024-02-01 11:36:43.857989995 10.88.243.91 → 10.4.23.202 DNS 160 Standard query response 0x1b86 No such nam
```

성공적인 DNS 이름 확인은 다음과 같습니다.

<#root>

```
FPR9300-01(fxos)#
ethanalyzer local interface mgmt capture-filter "udp port 53" limit-captured-frames 100

Capturing on 'eth0'
1 2022-09-06 00:49:00.059899379 10.88.146.73 → 10.88.243.91 DNS 85 Standard query 0xc512 AAAA WIN-JOR.jor.loc
2 2022-09-06 00:49:00.061349442 10.88.243.91 → 10.88.146.73 DNS 113 Standard query response 0xc512 AAAA WIN-J
3 2022-09-06 00:49:00.061515561 10.88.146.73 → 10.88.243.91 DNS 85 Standard query 0xc513 A WIN-JOR.jor.local
4 2022-09-06 00:49:00.061727264 10.88.243.91 → 10.88.146.73 DNS 101 Standard query response 0xc513 A WIN-JOR.
```

TCP 및 SSL 핸드셰이크

LDAPS 연결을 확인하려면 포트 389에서 캡처를 설정합니다.

Unknown CA와 같은 알림이 표시되면 LDAP 서버의 루트 CA 인증서가 일치하지 않음을 의미합니다. 인증서가 실제로 서버의 루트 CA인지 확인합니다.

<#root>

```
7 2024-02-01 12:10:37.260940300 10.4.23.202 → 10.4.23.128 TLSv1 345 Client Hello
8 2024-02-01 12:10:37.264016628 10.4.23.128 → 10.4.23.202 TCP 1514 [TCP segment of a reassembled PDU]
9 2024-02-01 12:10:37.264115319 10.4.23.128 → 10.4.23.202 TLSv1.2 617 Server Hello, Certificate, Server Key E
10 2024-02-01 12:10:37.264131122 10.4.23.202 → 10.4.23.128 TCP 66 40638 → 389 [ACK] Seq=311 Ack=2046 Win=3532
11 2024-02-01 12:10:37.264430791 10.4.23.202 → 10.4.23.128 TLSv1.2 73 Alert (Level: Fatal,
Description: Unknown CA
)
12 2024-02-01 12:10:37.264548228 10.4.23.202 → 10.4.23.128 TLSv1.2 73 Ignored Unknown Record
```

성공적인 연결은 다음과 같습니다.

<#root>

```
FPR9300-01(fxos)#
ethanalyzer local interface mgmt capture-filter "tcp port 389" limit-captured-frames 100

Capturing on 'eth0'
1 2024-02-01 12:12:49.131155860 10.4.23.202 → 10.4.23.128 TCP 74 42396 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=
2 2024-02-01 12:12:49.131403319 10.4.23.128 → 10.4.23.202 TCP 74 389 → 42396 [SYN, ACK] Seq=0 Ack=1 Win=8192
3 2024-02-01 12:12:49.131431506 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [ACK] Seq=1 Ack=1 Win=29696 Len=
4 2024-02-01 12:12:49.131455795 10.4.23.202 → 10.4.23.128 LDAP 97 extendedReq(1) LDAP_START_TLS_OID
5 2024-02-01 12:12:49.131914129 10.4.23.128 → 10.4.23.202 LDAP 112 extendedResp(1) LDAP_START_TLS_OID
6 2024-02-01 12:12:49.131931868 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [ACK] Seq=32 Ack=47 Win=29696 Le
```

```
7 2024-02-01 12:12:49.133238650 10.4.23.202 → 10.4.23.128 TLSv1 345 Client Hello
8 2024-02-01 12:12:49.135557845 10.4.23.128 → 10.4.23.202 TLSv1.2 2065 Server Hello, Certificate, Server Key
9 2024-02-01 12:12:49.135595847 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [ACK] Seq=311 Ack=2046 Win=33280
10 2024-02-01 12:12:49.150071315 10.4.23.202 → 10.4.23.128 TLSv1.2 171 Certificate, Client Key Exchange, Chan
11 2024-02-01 12:12:49.150995765 10.4.23.128 → 10.4.23.202 TLSv1.2 117 Change Cipher Spec, Encrypted Handshak
12 2024-02-01 12:12:49.151218671 10.4.23.202 → 10.4.23.128 TLSv1.2 153 Application Data
13 2024-02-01 12:12:49.152638865 10.4.23.128 → 10.4.23.202 TLSv1.2 117 Application Data
14 2024-02-01 12:12:49.152782132 10.4.23.202 → 10.4.23.128 TLSv1.2 165 Application Data
15 2024-02-01 12:12:49.153310263 10.4.23.128 → 10.4.23.202 TLSv1.2 430 Application Data
16 2024-02-01 12:12:49.153463478 10.4.23.202 → 10.4.23.128 TLSv1.2 153 Application Data
17 2024-02-01 12:12:49.154673694 10.4.23.128 → 10.4.23.202 TLSv1.2 117 Application Data
18 2024-02-01 12:12:49.155219271 10.4.23.202 → 10.4.23.128 TLSv1.2 102 Application Data
19 2024-02-01 12:12:49.155254255 10.4.23.202 → 10.4.23.128 TLSv1.2 97 Encrypted Alert
20 2024-02-01 12:12:49.155273807 10.4.23.202 → 10.4.23.128 TCP 66 42396 → 389 [FIN, ACK] Seq=756 Ack=2563 Win
21 2024-02-01 12:12:49.155483352 10.4.23.128 → 10.4.23.202 TCP 60 389 → 42396 [RST, ACK] Seq=2563 Ack=725 Win
```

디버깅

더 심층적인 트러블슈팅의 경우 자세한 내용을 보려면 LDAP에 대한 디버그를 활성화할 수 있습니다.

SSL 연결이 정상적으로 수행되면 다음과 같은 심각한 오류가 발생하지 않습니다.

```
<#root>

FPR9300-01(fxos)#

debug ldap all
```

```
2024 Feb 1 11:51:16.243245 ldap: 0x00000101/111 -> 0x00000101/0 id0x2F06F sz370 [REQ] op4093 rr0x2F06F
2024 Feb 1 11:51:16.243275 ldap: mts_ldap_aaa_request_handler: session id 0, list handle is NULL
2024 Feb 1 11:51:16.243289 ldap: mts_ldap_aaa_request_handler: user :sfua:, user_len 4, user_data_len 8
2024 Feb 1 11:51:16.243298 ldap: ldap_authenticate: user sfua with server group ldap
2024 Feb 1 11:51:16.243337 ldap: ldap_authenticate:3150 the value of login_type is 0
2024 Feb 1 11:51:16.243394 ldap: ldap_global_config: entering ...
2024 Feb 1 11:51:16.243637 ldap: ldap_read_group_config:
2024 Feb 1 11:51:16.243831 ldap: ldap_server_config: GET_REQ: server index: 1 addr:
2024 Feb 1 11:51:16.244059 ldap: ldap_client_auth_init: attr_memberof not configured for server
2024 Feb 1 11:51:16.244268 ldap: ldap_client_auth_init: (user sfua) - ldap_init success for host WIN-JO
2024 Feb 1 11:51:16.244487 ldap: ldap_client_lib_init_ssl: set ldap options cipher_suite ALL:!DHE-PSK-A
SHA:!EDH-DSS-DES-CBC3-SHA:!DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDI
RSA-AES256-SHA:!ECDHE-ECDSA-AES256-SHA:!
2024 Feb 1 11:51:16.246568 ldap: ldap_do_TLS: - ldap_tls initiated
2024 Feb 1 11:51:16.246598 ldap: ldap_client_auth_init:(user sfua) - awaiting for response, isssl: 1
2024 Feb 1 11:51:16.247104 ldap: ldap_socket_ready_callback: entering...
2024 Feb 1 11:51:16.247116 ldap: ldap_process_result: entering... for user sfua
2024 Feb 1 11:51:16.247124 ldap: ldap_process_result: ldap_result sess->state: LDAP_SESS_TLS_SENT
2024 Feb 1 11:51:16.247146 ldap: ldap_process_result: (user sfua) - tls extended resp.
2024 Feb 1 11:51:16.247153 ldap: ldap_do_process_tls_resp: entering for user sfua
2024 Feb 1 11:51:16.247169 ldap: ldap_do_process_tls_resp: (user sfua) - ldap start TLS sent successful
2024 Feb 1 11:51:16.249856 ldap: ldap_app_cb: - ldap_app_ctx 0x100ad224 ldap session 0x1217a53c ssl 0x1
2024 Feb 1 12:19:20.512383 ldap: ldap_app_cb: - Check the configured hostname WIN-JORGEJU.jorgeju.local
2024 Feb 1 12:19:20.512418 ldap: ldap_app_cb: Non CC mode - hostname WIN-JORGEJU.jorgeju.local.
2024 Feb 1 12:19:20.520346 ldap: ldap_crls_http_and_local_cb: - get CRL from CRLDP
2024 Feb 1 12:19:20.520626 ldap: ldap_crls_http_and_local_cb: - crls 0x121787dc
```

```
2024 Feb 1 12:19:20.520900 ldap: ldap_load_crl_crldp: - get CRL from CRLDP
2024 Feb 1 12:19:20.521135 ldap: ldap_load_crl_crldp: - crls 0x121787dc
2024 Feb 1 12:19:20.521364 ldap: ldap_get_dp_url: - get URI from CRLDP
2024 Feb 1 12:19:20.521592 ldap: ldap_load_crl_http: - entering...
```

서버의 루트 CA 인증서가 일치하지 않을 경우 ldap_check_cert_chain_cb 프로세스에서 인증서 오류를 관찰할 수 있습니다.

```
2024 Feb 1 12:07:08.624416 ldap: ldap_app_cb: - Check the configured hostname WIN-JOR.jor.local with pe
2024 Feb 1 12:07:08.624453 ldap: ldap_app_cb: Non CC mode - hostname WIN-JOR.jor.local.
2024 Feb 1 12:08:31.274583 ldap: ldap_check_cert_chain_cb: - Enter
2024 Feb 1 12:08:31.274607 ldap: ldap_check_cert_chain_cb: - called ok flag is 0
2024 Feb 1 12:08:31.274620 ldap: ldap_check_cert_chain_cb: - ldap session 0x1217a53c, crlstrict 0.
2024 Feb 1 12:08:31.274632 ldap: ldap_check_cert_chain_cb: - get ctx error is 20
2024 Feb 1 12:08:31.274664 ldap: ldap_check_cert_chain_cb: - cert X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_
2024 Feb 1 12:08:31.274688 ldap: ldap_check_cert_chain_cb: - End ok 0
2024 Feb 1 12:08:31.274833 ldap: ldap_do_process_tls_resp: (user sfua) - TLS START failed
```

잠김에서 복구

어떤 이유로든 Chassis Manager GUI에서 잠겼지만 LDAPS가 작동하지 않는 경우 CLI 액세스 권한이 있는 경우에도 복구할 수 있습니다.

이 작업은 기본 인증 또는 콘솔 인증을 위해 인증 방법을 로컬로 다시 변경하여 수행합니다.

```
<#root>

FPR9300-01#

scope security


FPR9300-01 /security #

scope default-auth


FPR9300-01 /security/default-auth #

show


Default authentication:
Admin Realm                    Admin Authentication server group Use of 2nd factor
------------------------------ --------------------------------- -----------------
Ldap                                                             No

FPR9300-01 /security/default-auth #

set realm local
```

```
FPR9300-01 /security/default-auth* #
commit-buffer

FPR9300-01 /security/default-auth #
show

Default authentication:
Admin Realm                    Admin Authentication server group Use of 2nd factor
------------------------------ --------------------------------- -----------------
Local                                                             No
```

변경 후 다시 한 번 FCM에 로그인하십시오.

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.