LDAPS in FXOS configureren

Inhoud

Inleiding

Dit document beschrijft hoe u Secure LDAP (LDAPS) op FXOS kunt configureren met Secure Firewall Chassis Manager (FCM) en CLI.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Firewall eXtensible Operating System (FXOS)
- Secure Firewall Chassis Manager (FCM)
- Lichtgewicht Directory Access Protocol (LDAP)-concepten

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Secure Firewall 9300 versie van het apparaat 2.12(0.8)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie

Het is aan te raden om te testen dat effen LDAP werkt op uw Secure Firewall-apparaat.

Platte LDAP configureren

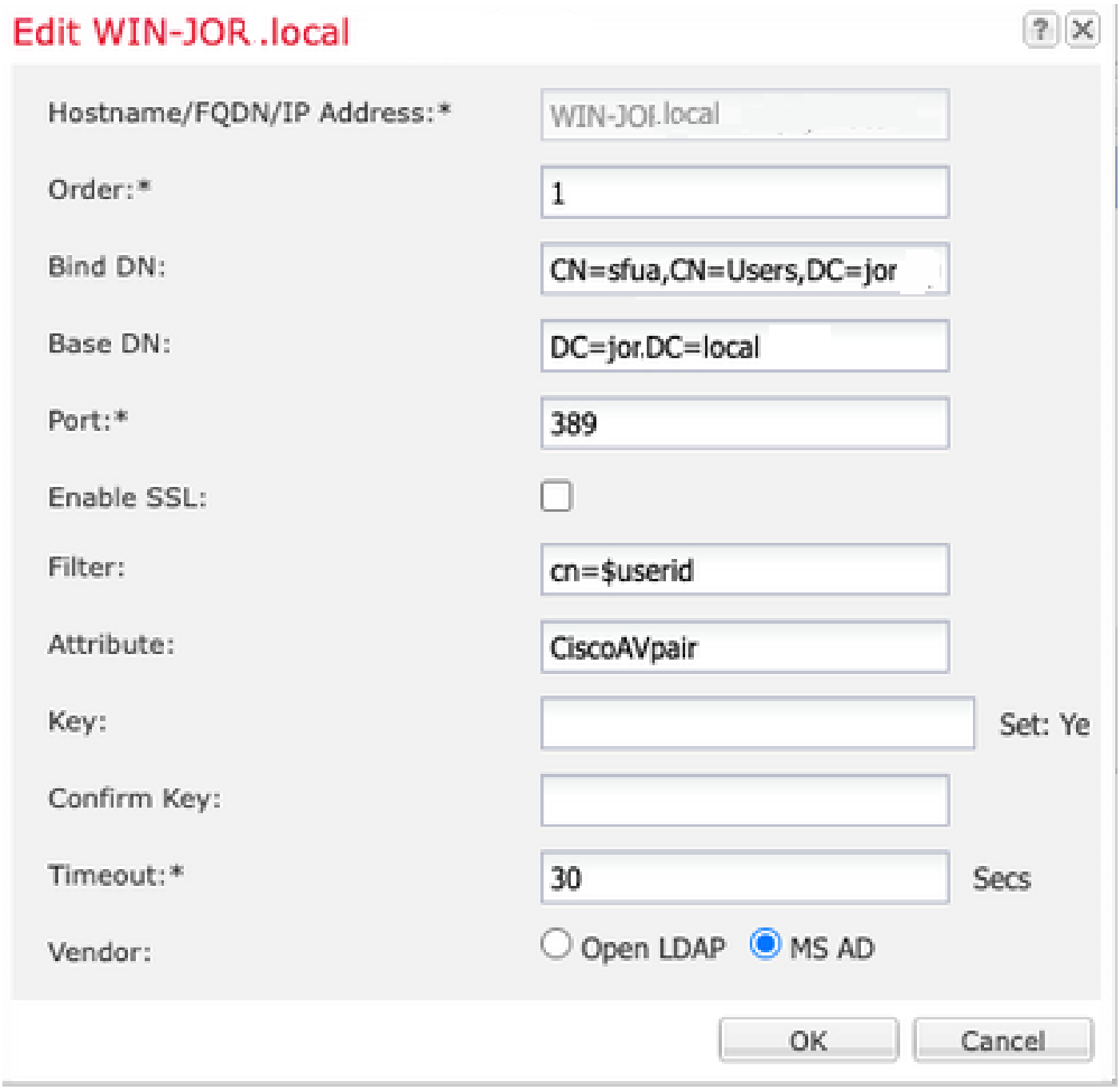
1. Log in op FCM.

2. Navigeren naar platforminstellingen > AAA > LDAP

3. Klik op LDAP Providers > Add

4. Configureer LDAP-provider en voer bind-DN, basis-DN, kenmerk- en sleutelinformatie voor Microsoft Active Directory (MS AD) in.

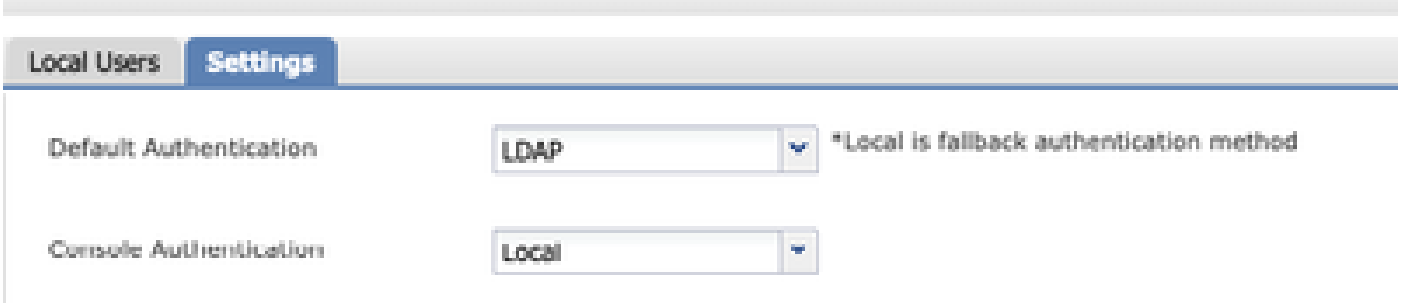
5. Gebruik de FQDN van de LDAP-server, omdat dit nodig is voor SSL-verbinding.



LDAP-configuratie

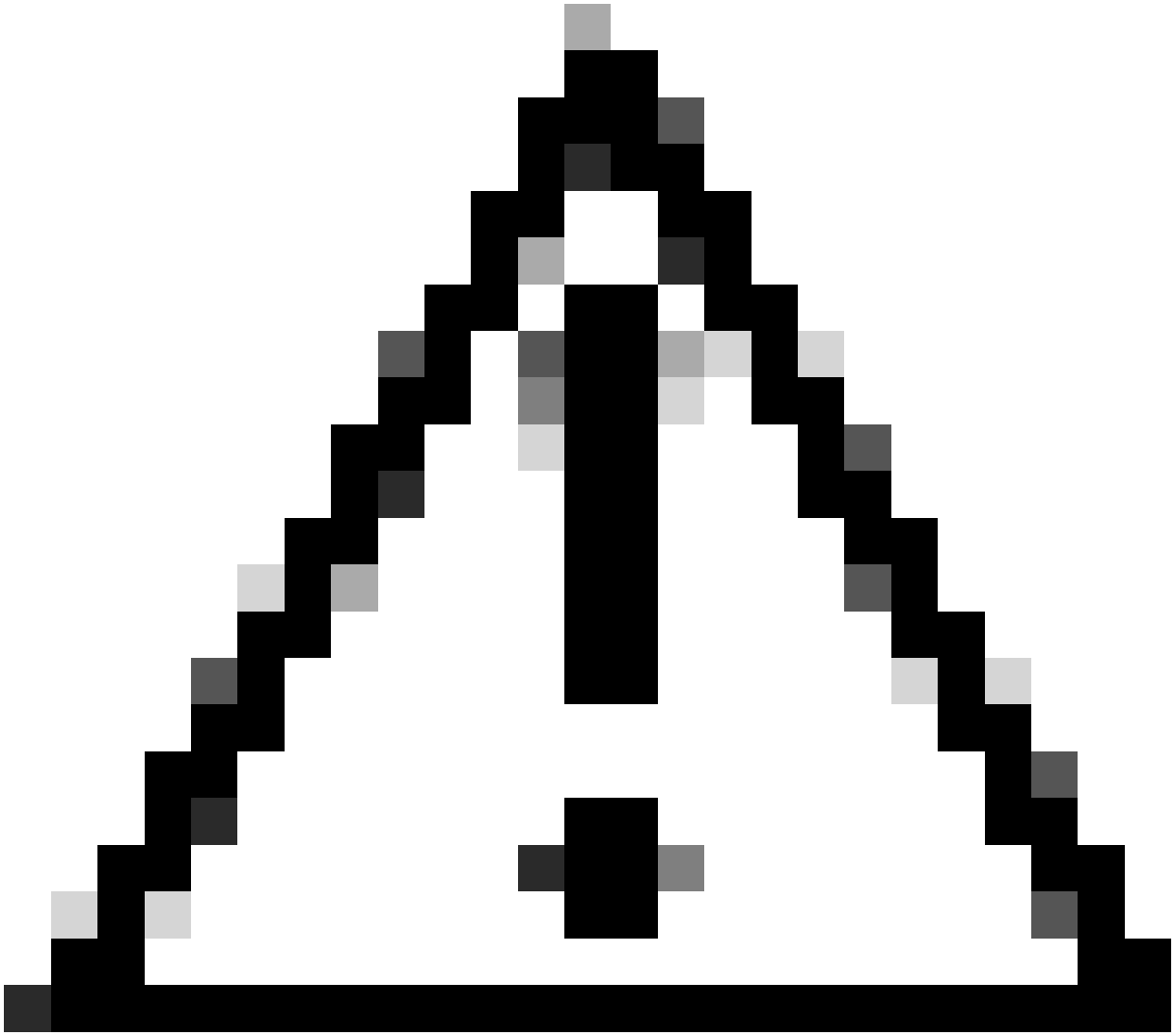
6. Ga naar Systeem > Gebruikersbeheer > Instellingen.

7. Stel standaard- of consoleverificatie in op LDAP.



Selecteren van verificatiemethode

8. Probeer in te loggen van SSH naar het chassis om de verificatie te testen bij een LDAP-gebruiker.



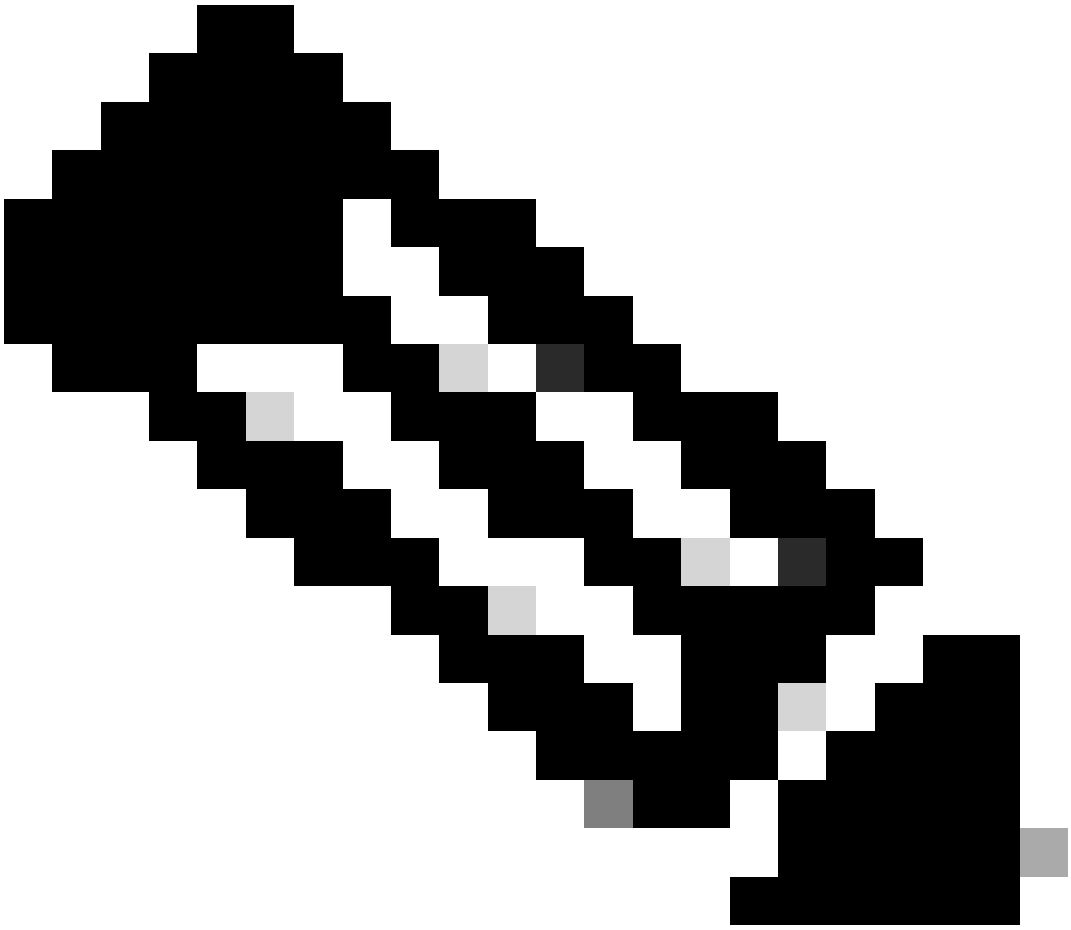
Waarschuwing: wees voorzichtig bij het testen van LDAP-verificatie. Als er een fout in de configuratie is, kan deze wijziging u buitensluiten. Test met een dubbele sessie of vanaf console toegang met lokale verificatie zodat terugdraaien of probleemoplossing kan worden uitgevoerd.

LDAPS configureren

9. Nadat u een succesvolle LDAP-verbinding hebt getest, navigeer u opnieuw naar Platform-instellingen > AAA > LDAP.

10. Bewerk uw LDAP-provider en schakel SSL in.

Poortselectie GUI



> Opmerking: poort 389 moet worden gebruikt voor codering. Port 636 werkt niet. Verbetering Cisco bug-id CSCwc93347 is ingediend om aangepaste poorten voor LDAPS toe te voegen

---

11. Het basiscertificaat van CA van de LDAP-server moet in het chassis worden geïmporteerd. Indien er tussentijdse certificaten zijn, moet u de keten samen invoeren.

Maak een trustpoint van FXOS CLI om dit uit te voeren.

<#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. Voer de LDAP-serverconfiguratie in zoals deze op de LDAP-provider is geconfigureerd. Noteer de naam van uw LDAP-server.

13. Stel het herroepingsbeleid in op ontspannen.

<#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. Veranderingen opslaan met behulp van commit-buffer.

Problemen oplossen

DNS-resolutie

Controleer of FQDN naar het juiste IP wordt opgelost. Er kunnen problemen zijn met de naamresolutie:

```
<#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
```

Een succesvolle DNS-naamresolutie ziet er als volgt uit:

<#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- en SSL-handdruk

Om de LDAPS-verbinding te verifiëren, stelt u de opnamen in op poort 389.

Als u waarschuwingen ziet zoals Onbekend CA, betekent dit dat het basiscertificaat van CA van de LDAP-server niet overeenkomt. Controleer dat het certificaat inderdaad de basis-CA van de server is.

<#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
```

Een succesvolle verbinding ziet er als volgt uit:

<#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
```

Debuggen

U kunt debugs voor LDAP inschakelen voor meer informatie in het geval van diepere probleemoplossing.

Een succesvolle SSL-verbinding ziet er zo uit, er wordt geen grote fout waargenomen:

```
<#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...
```

Wanneer het wortel CA certificaat van de server niet aanpast, kunt u certificaatfouten op het ldap_check_cert_chain_cb proces waarnemen:

```
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
```

Herstellen van uitgesloten zijn

Als u om welke reden dan ook was uitgesloten van de Chassis Manager GUI en LDAPS niet werkt, kunt u nog steeds herstellen als u CLI-toegang hebt.

Dit gebeurt door de verificatiemethode voor de standaardverificatie of voor de consoleverificatie terug te zetten naar lokaal.

<#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
```

Na deze veranderingen, probeer opnieuw aan te melden bij FCM.

Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.