Configuration de LDAPS dans FXOS

Table des matières

Introduction

Ce document décrit comment configurer Secure LDAP (LDAPS) sur FXOS à l'aide de Secure Firewall Chassis Manager (FCM) et CLI.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Système d'exploitation extensible Secure Firewall (FXOS)
- Gestionnaire de châssis de pare-feu sécurisé (FCM)
- Concepts LDAP (Lightweight Directory Access Protocol)

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Périphérique Secure Firewall 9300 version 2.12(0.8)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration

Il est recommandé de vérifier que le protocole LDAP simple fonctionne sur votre périphérique Secure Firewall.

Configurer le protocole LDAP simple

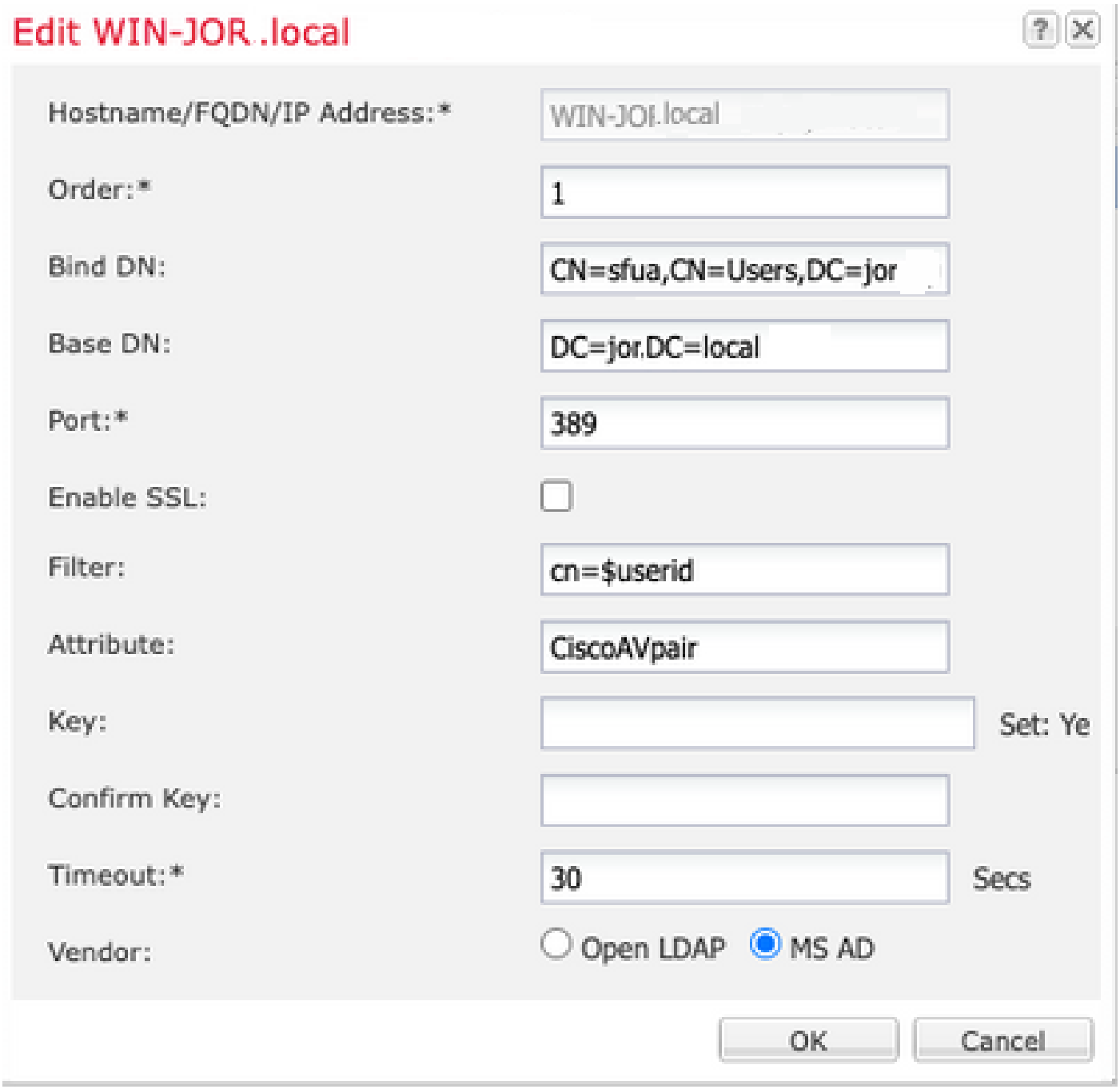
1. Connectez-vous à FCM.

2. Accédez à Platform Settings > AAA > LDAP

3. Cliquez sur Fournisseurs LDAP > Ajouter

4. Configurez le fournisseur LDAP et entrez le DN de liaison, le DN de base, les informations d'attribut et de clé pour Microsoft Active Directory (MS AD).

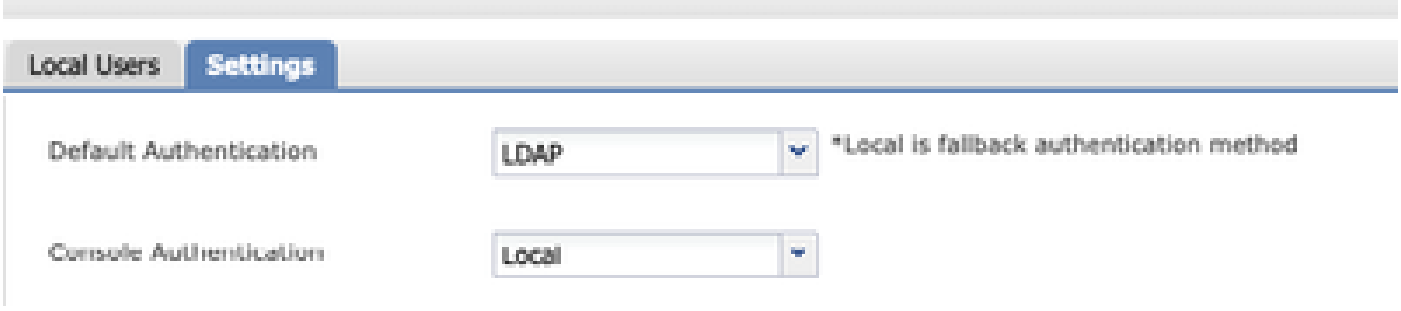
5. Utilisez le nom de domaine complet du serveur LDAP, car il est nécessaire pour la connexion SSL.



Configuration LDAP

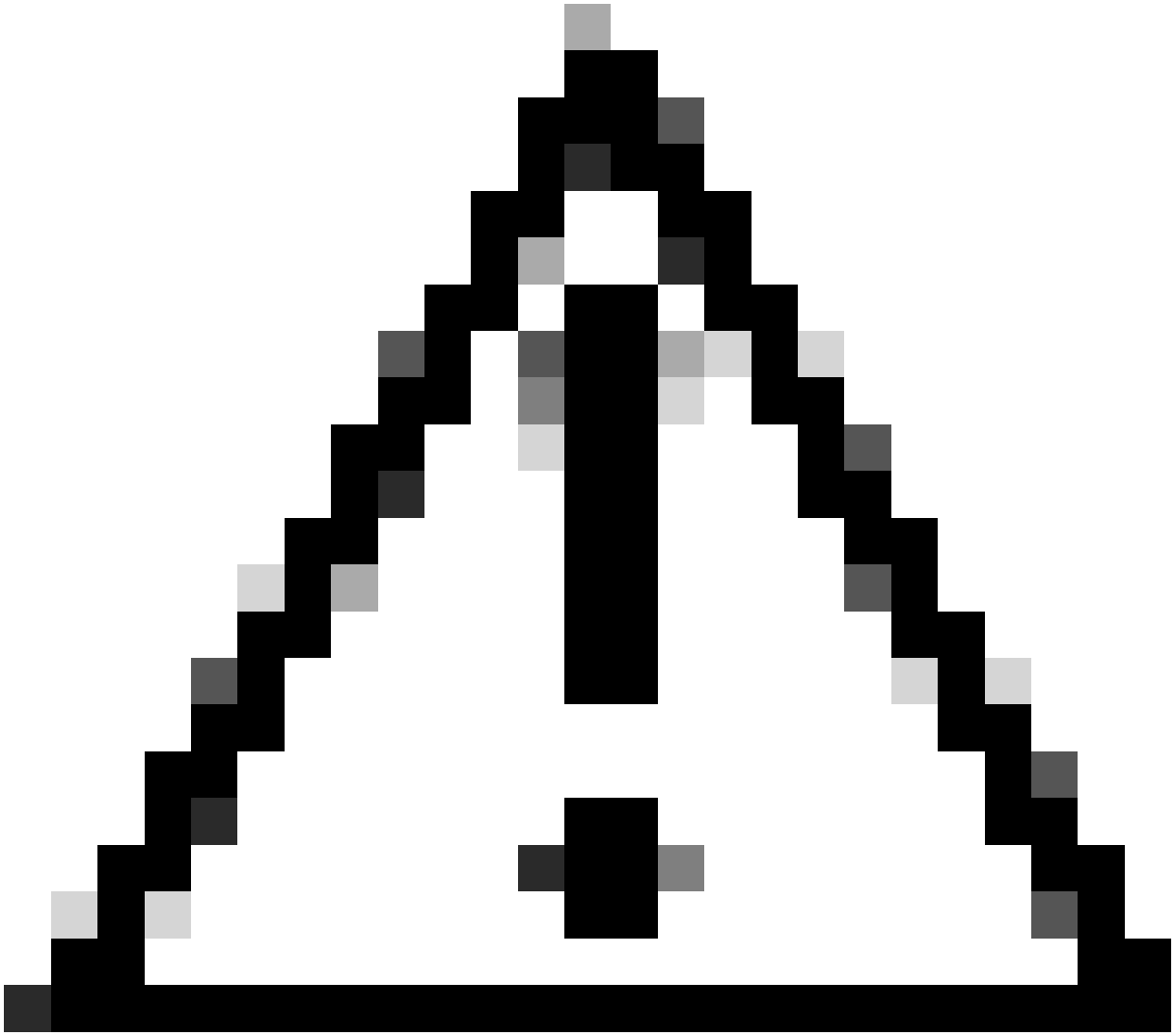
6. Accédez à Système > Gestion des utilisateurs > Paramètres.

7. Définissez l'authentification par défaut ou par console sur LDAP.



Sélection de la méthode d'authentification

8. Essayez de vous connecter de SSH au châssis pour tester l'authentification avec un utilisateur LDAP.



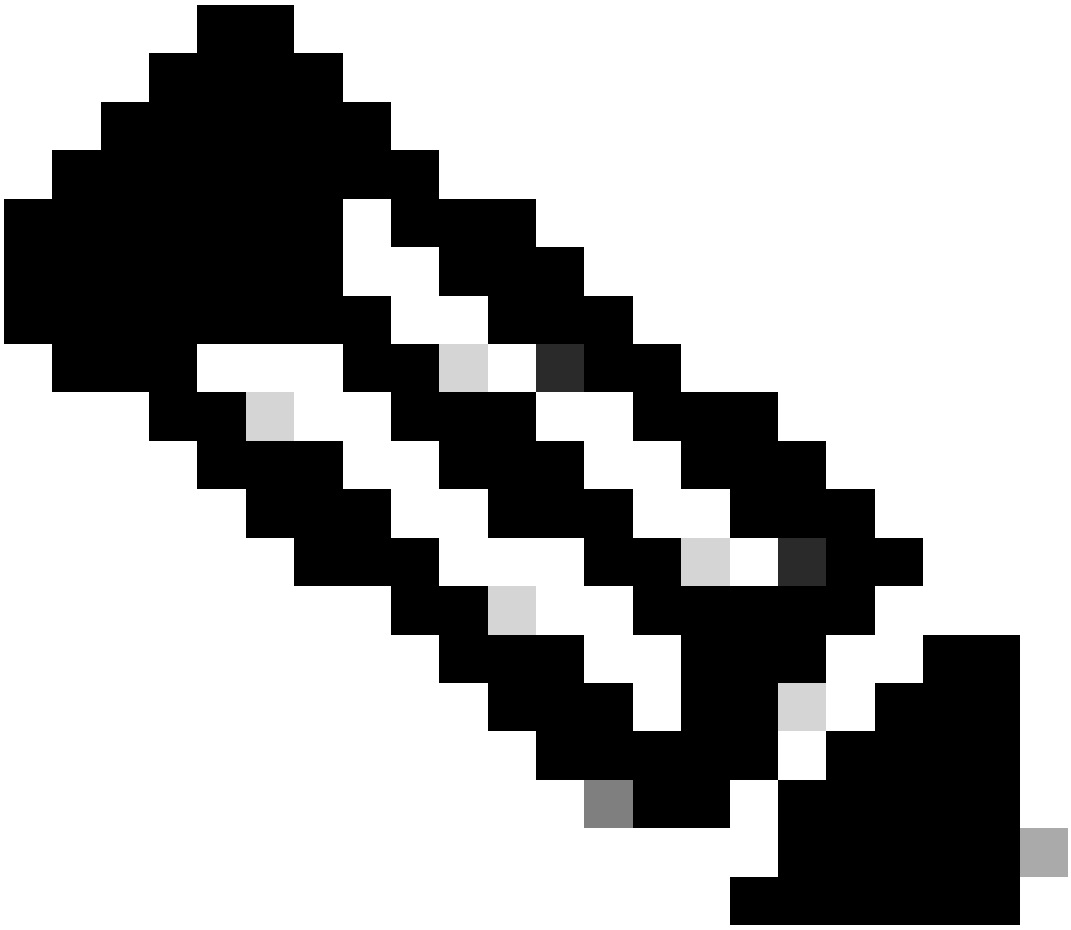
Attention : soyez prudent lors du test de l'authentification LDAP. Si une erreur se produit dans la configuration, cette modification peut vous bloquer. Testez une session dupliquée ou un accès à partir de la console avec l'authentification locale afin d'effectuer une restauration ou un dépannage.

Configuration des LDAPS

9. Une fois que vous avez testé une connexion LDAP réussie, naviguez à nouveau vers Platform Settings > AAA > LDAP.

10. Modifiez votre fournisseur LDAP et activez SSL.

Interface utilisateur graphique de sélection de port



> Remarque : le port 389 doit être utilisé pour le cryptage. Le port 636 ne fonctionne pas. Amélioration L'ID de bogue Cisco CSCwc93347 a été refusé pour ajouter des ports personnalisés pour LDAPS

---

11. Le certificat CA racine du serveur LDAP doit être importé dans le châssis. S'il existe des certificats intermédiaires, importez la chaîne ensemble.

Créez un point de confiance à partir de la CLI FXOS pour effectuer cette opération.

<#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. Entrez la configuration du serveur LDAP telle que configurée sur le fournisseur LDAP. Notez le nom de votre serveur LDAP.

13. Définissez la politique de révocation sur relaxed.

<#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. Enregistrez les modifications à l'aide de commit-buffer.

Dépannage

Résolution DNS

Vérifiez que le nom de domaine complet (FQDN) est résolu sur l'adresse IP correcte. Il peut y avoir des problèmes avec la résolution de noms :

<#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
```

Une résolution de nom DNS réussie ressemble à ceci :

<#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.
```

Connexion TCP et SSL

Afin de vérifier la connexion LDAPS, définissez les captures sur le port 389.

Si vous voyez des alertes telles que Unknown CA, cela signifie que le certificat d'autorité de certification racine du serveur LDAP ne correspond pas. Vérifiez que le certificat est bien l'autorité de certification racine du serveur.

<#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
```

Une connexion réussie ressemble à ceci :

<#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
```

Débogage

Vous pouvez activer les débogages pour LDAP pour plus d'informations en cas de dépannage plus approfondi.

Une connexion SSL réussie ressemble à ceci, aucune erreur majeure n'est observée :

```
<#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...
```

Lorsque le certificat d'autorité de certification racine du serveur ne correspond pas, vous pouvez observer des erreurs de certificat sur le processus ldap_check_cert_chain_cb :

```
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
```

Récupérer d'un verrouillage

Si vous avez été verrouillé pour une raison quelconque dans l'interface utilisateur graphique du gestionnaire de châssis et que le LDAPS ne fonctionne pas, vous pouvez toujours récupérer si vous disposez d'un accès CLI.

Pour ce faire, vous devez redéfinir la méthode d'authentification sur local pour l'authentification par défaut ou l'authentification de console.

<#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
```

Après ces modifications, essayez de vous reconnecter à FCM.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.