

Configurazione di LDAPS in FXOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configura LDAP normale](#)

[Configura LDAPS](#)

[Risoluzione dei problemi](#)

[Risoluzione DNS](#)

[Handshake TCP e SSL](#)

[Debug](#)

[Ripristina da blocco](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Secure LDAP (LDAPS) su FXOS utilizzando Secure Firewall Chassis Manager (FCM) e CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Sistema operativo FXOS (Secure Firewall eXtensible Operating System)
- Secure Firewall Chassis Manager (FCM)
- Concetti relativi al protocollo LDAP (Lightweight Directory Access Protocol)

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Secure Firewall 9300 versione 2.12(0.8)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Si consiglia di verificare che il normale LDAP funzioni sul dispositivo Secure Firewall.

Configura LDAP normale

1. Accedere a FCM.
2. Selezionare Platform Settings > AAA > LDAP
3. Fare clic su Provider LDAP > Aggiungi
4. Configurare il provider LDAP e immettere le informazioni relative al DN di associazione, al DN di base, all'attributo e alla chiave per Microsoft Active Directory (MS AD).
5. Utilizzare il nome di dominio completo (FQDN) del server LDAP, in quanto necessario per la connessione SSL.

Edit WIN-JOR .local



Hostname/FQDN/IP Address:*	<input type="text" value="WIN-JOR.local"/>	
Order:*	<input type="text" value="1"/>	
Bind DN:	<input type="text" value="CN=sfua,CN=Users,DC=jor"/>	
Base DN:	<input type="text" value="DC=jor.DC=local"/>	
Port:*	<input type="text" value="389"/>	
Enable SSL:	<input type="checkbox"/>	
Filter:	<input type="text" value="cn=\$userid"/>	
Attribute:	<input type="text" value="CiscoAVpair"/>	
Key:	<input type="text"/>	Set: Yes
Confirm Key:	<input type="text"/>	
Timeout:*	<input type="text" value="30"/>	Secs
Vendor:	<input type="radio"/> Open LDAP <input checked="" type="radio"/> MS AD	

Configurazione LDAP

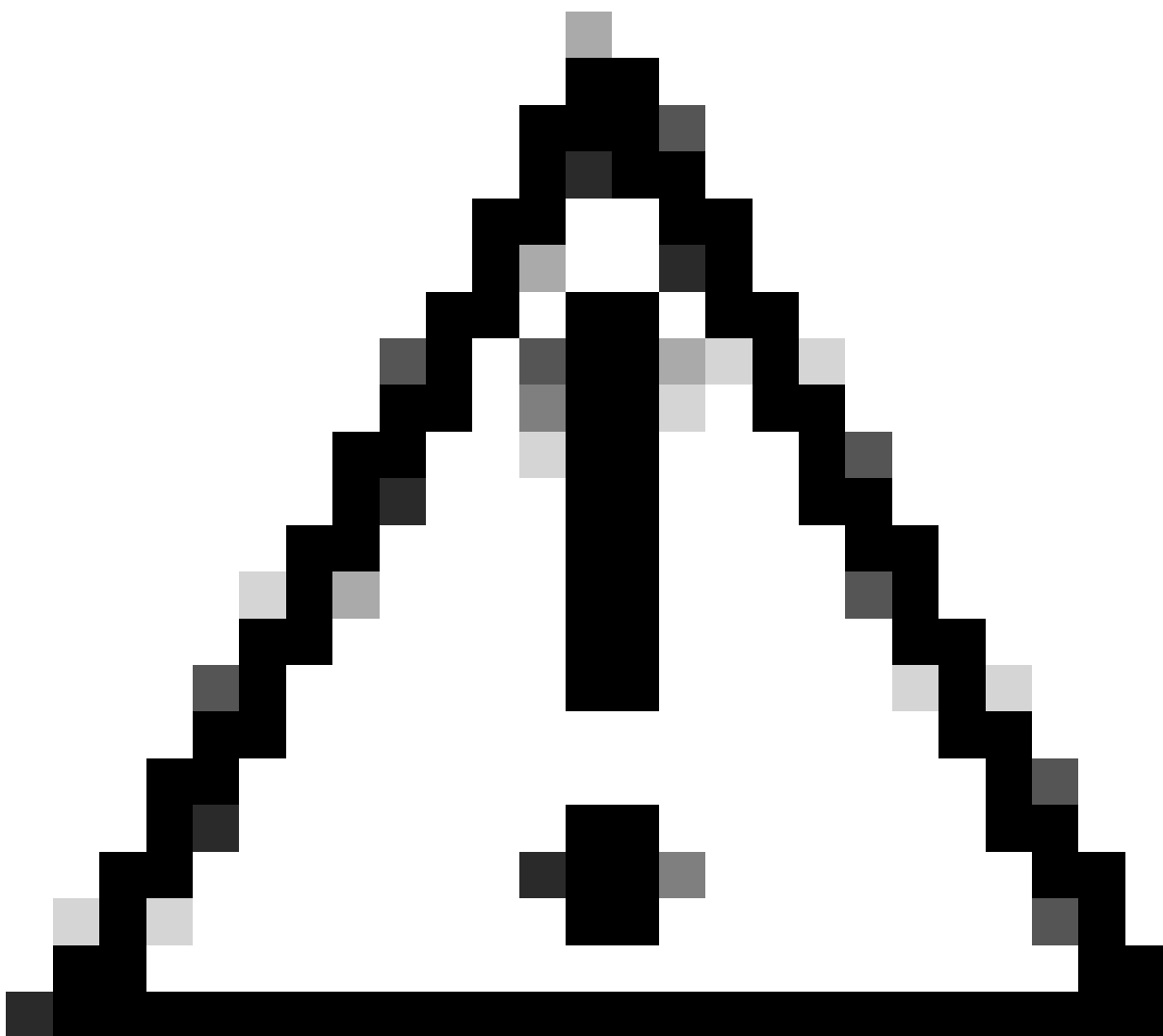
6. Passare a Sistema > Gestione utente > Impostazioni.

7. Impostare l'autenticazione predefinita o console su LDAP.

Local Users	Settings
Default Authentication	<input type="text" value="LDAP"/> <input type="button" value="v"/> *Local is fallback authentication method
Console Authentication	<input type="text" value="Local"/> <input type="button" value="v"/>

Selezione metodo di autenticazione

8. Provare ad accedere dal protocollo SSH allo chassis per verificare l'autenticazione con un utente LDAP.



Attenzione: prestare attenzione durante il test dell'autenticazione LDAP. Se si verifica un errore nella configurazione, la modifica può bloccare l'utente. Eseguire il test con una sessione duplicata o dall'accesso alla console con l'autenticazione locale in modo da eseguire il rollback o la risoluzione dei problemi.

Configura LDAPS

9. Dopo aver verificato la corretta connessione LDAP, tornare a Impostazioni piattaforma > AAA > LDAP.

10. Modificare il provider LDAP e abilitare SSL.

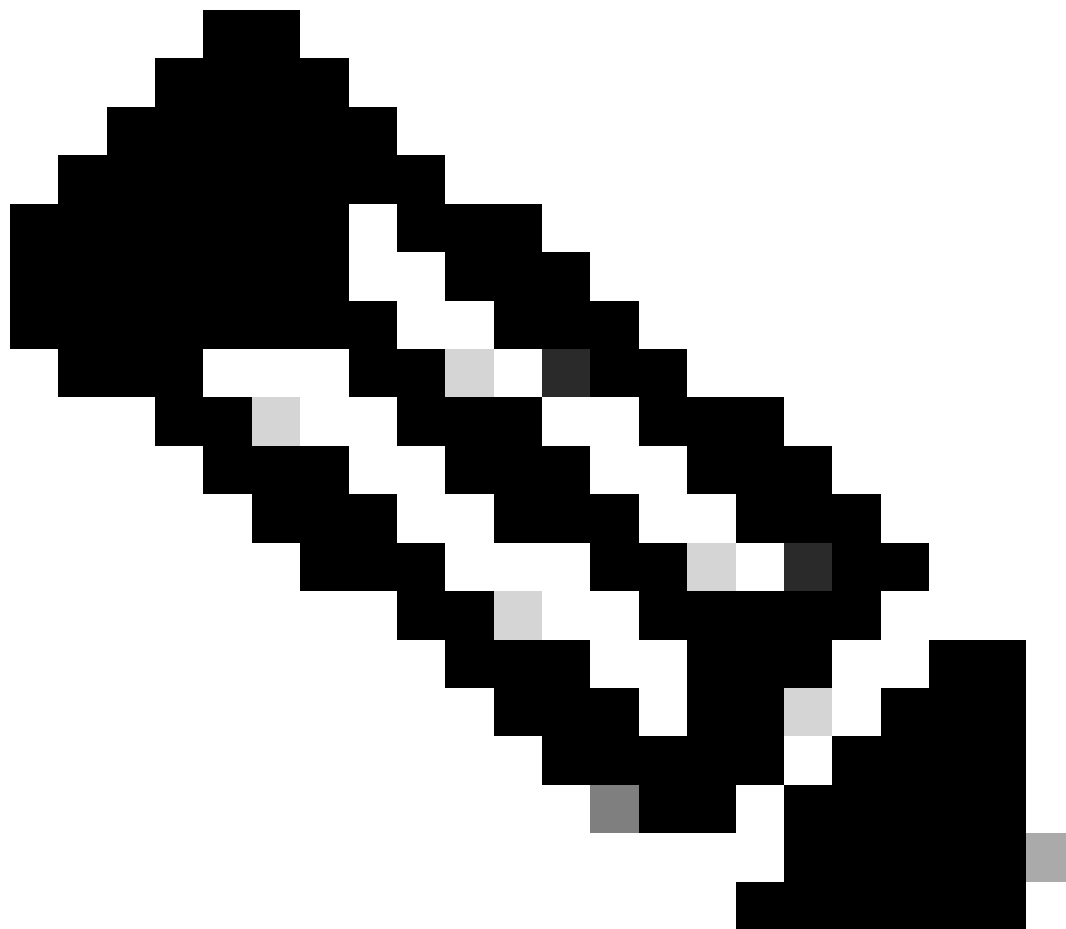
Port:*

389

Enable SSL:



Interfaccia grafica di selezione porte



Nota: la porta 389 deve essere utilizzata per la crittografia. La porta 636 non funziona. Miglioramento L'ID bug Cisco [CSCwc93347](#) è stato omesso per aggiungere porte personalizzate per LDAPS

11. Il certificato CA radice del server LDAP deve essere importato nello chassis. Se sono presenti certificati intermedi, importare la catena.

Per eseguire questa operazione, creare un trust point dalla CLI di FXOS.

<#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+rOqfXpjANBqkqhkiG9w0BAQsFAADBT

>MRUwEwYKcZImiZPyLQBGryFbG9jYwWxFzAVBgoJkiaJk/IsZAEZFgdqb3JnZWp1

>MSEwHwYDVQQDExhb3JnZWp1LVdJTl1KT1JHRUpVLUNBLTEwHhcNMjEzMDc0

>MDAwWhcNMjEzMDc0OTU5WjBTMRUwEwYKcZImiZPyLQBGryFbG9jYwWxFzAV

>BgoJkiaJk/IsZAEZFgdqb3JnZWp1MSEwHwYDVQQDExhb3JnZWp1LVdJTl1KT1JH

>RUPLUNBLTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDmBTWU6Leu

>bPxvc+EhC7fxjowEjjL0EXlMo3x7Pe3EW6Gng2iOMB1UpBNgSObbct83P6y6EmQi

>0RCCnEFfzy4stYPz/7499wALwMLSGNQWr10rjVB64ihfugbx95iDBcwuv6XK67h/

>T1caN4GZiLtYZjURGs5mLNB2f8hLp9QR2WoZqfAvrfvFB4I5RJjx0FYKIXW1dmPT

>AAPa/Qi+1Qv1exfzvXHXx1GMDCHle2yItFgl6o7OujT0AE3oplA/qQD+mTAJmdcR

>QLUDiUptqqYKgcbrH4Hu4PMje3INLd1vw1ThAwMFn+oXjRTM0KbEQ0/JEM6xRFMv

>LqzmDwxA8IoRagMBAAGjaTBnMBMGCSsGAQQBgjcUAgQGHgQAQwBBMA4GA1UdDwEB

>/wQEAWIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBQoweZEEke7BIOd94R5

>YxjvJHdzsjaQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAYGli

>n77K0OiqSljTeg+C1VLRX8VJwr7Pp5p4Mu0mRhZckmIKSUtYDla3ToVix5k4dXSU

>7MaVWDkW/1NvReaqCfis5mgfrpzoPukqKGiz7Zhd57gA4tBU/XbP/CXpTuAR3Isa

>NKz7yy+6tisf+8vfLtrN8c3IclS6ncyrdAdJ2iJY74jJm1eUPs3muaqApPPwoRF2

>GdALD/Y+Pq36cSjK+jGP1+2rD6cWl6thBp9plOOTL+qpq4DL+W6uctWeRMgGxcWn

>GsKhHysno9dZ+DnnOlx0tP+S1B9fmxF7ycCmmn328dZVEG7JXjHc8KoqwwWe+fwu

>GXLRM+rKaAICH52EEw==

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

>ENDOFBUF

FPR9300-01 /security/trustpoint* #

commit-buffer

12. Immettere la configurazione del server LDAP configurata sul provider LDAP. Prendere nota del nome del server LDAP.

13. Impostare la politica di revoca su rilassata.

<#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. Salvare le modifiche utilizzando il commit-buffer.

Risoluzione dei problemi

Risoluzione DNS

Verificare che l'FQDN sia stato risolto nell'IP corretto. La risoluzione dei nomi può causare problemi:

```
<#root>
```

```
FPR9300-01#
```

```
connect fxos
```

```
FPR9300-01(fxos)#
```

```
ethalyzer 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.local
```



```
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
```

Una risoluzione dei nomi DNS riuscita avrà il seguente aspetto:

```
<#root>
```

```
FPR9300-01(fxos)#
```

```
ethalyzer 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.local
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.
```

Handshake TCP e SSL

Per verificare la connessione LDAPS, impostare la cattura sulla porta 389.

Se vengono visualizzati avvisi quali CA sconosciuta, significa che il certificato CA radice del server LDAP non corrisponde. Verificare che il certificato sia effettivamente la CA radice del server.

```
<#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
```

Una connessione riuscita ha il seguente aspetto:

```
<#root>
```

```
FPR9300-01(fxos)#
```

```
ethalyzer 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
```

Debug

È possibile abilitare i debug per LDAP per ulteriori informazioni in caso di risoluzione dei problemi più approfondita.

Se la connessione SSL viene stabilita correttamente, non si verifica alcun errore grave:

```
<#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, issl: 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_cr1s_http_and_local_cb: - get CRL from CRLDP
2024 Feb 1 12:19:20.520626 ldap: ldap_cr1s_http_and_local_cb: - cr1s 0x121787dc
2024 Feb 1 12:19:20.520900 ldap: ldap_load_cr1_cr1dp: - get CRL from CRLDP
2024 Feb 1 12:19:20.521135 ldap: ldap_load_cr1_cr1dp: - cr1s 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_cr1_http: - entering...
```

Quando il certificato CA radice del server non corrisponde, è possibile osservare errori di certificato nel processo ldap_check_cert_chain_cb:

```
2024 Feb 1 12:07:08.624416 ldap: ldap_app_cb: - Check the configured hostname WIN-JOR.jor.local withpe
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, cr1strict 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
```

Ripristina da blocco

Se per qualsiasi motivo si è stati bloccati dalla GUI di Chassis Manager e LDAPS non funziona, è comunque possibile eseguire il ripristino se si dispone dell'accesso CLI.

A tale scopo, è necessario ripristinare il metodo di autenticazione locale per l'autenticazione predefinita o l'autenticazione della 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

Dopo queste modifiche, provare ad accedere nuovamente a FCM.

Informazioni correlate

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).