使用LDAP配置Firepower管理中心和FTD以进行外部身份验证

目录

简介

本文档介绍如何通过Cisco Firepower管理中心(FMC)和Firepower威胁防御(FTD)启用Microsoft轻量级目录访问协议(LDAP)外部身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科FTD
- 思科FMC
- Microsoft LDAP

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FTD 6.5.0-123
- FMC 6.5.0-115
- Microsoft Server 2012

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

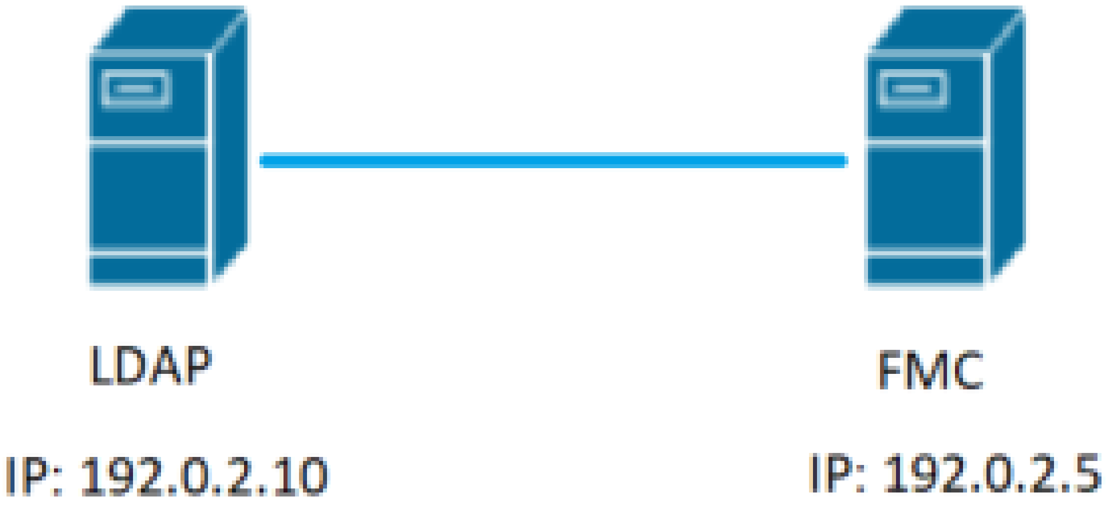
背景信息

FMC和受管设备包含用于管理访问的默认管理员帐户。您可以在FMC和受管设备上添加自定义用户帐户，可以将其作为内部用户，也可以作为LDAP或RADIUS服务器上的外部用户（如果您的型号支持）。FMC和FTD支持外部用户身份验证。

·内部用户 — FMC/FTD设备检查本地数据库以进行用户身份验证。

·外部用户 — 如果本地数据库中不存在该用户，则来自外部LDAP或RADIUS身份验证服务器的系统信息将填充其用户数据库。

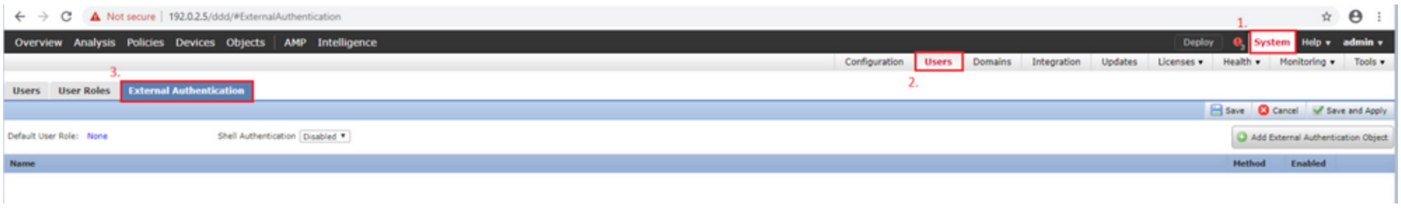
网络图



配置

FMC GUI中的基本LDAP配置

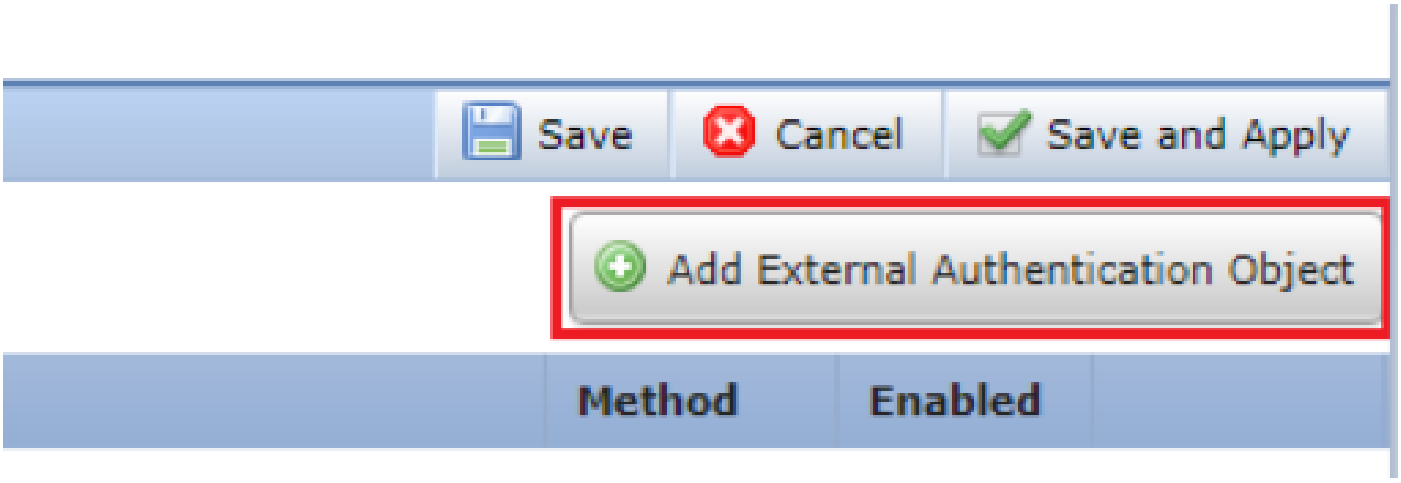
步骤1:导航至 System > Users > External Authentication:



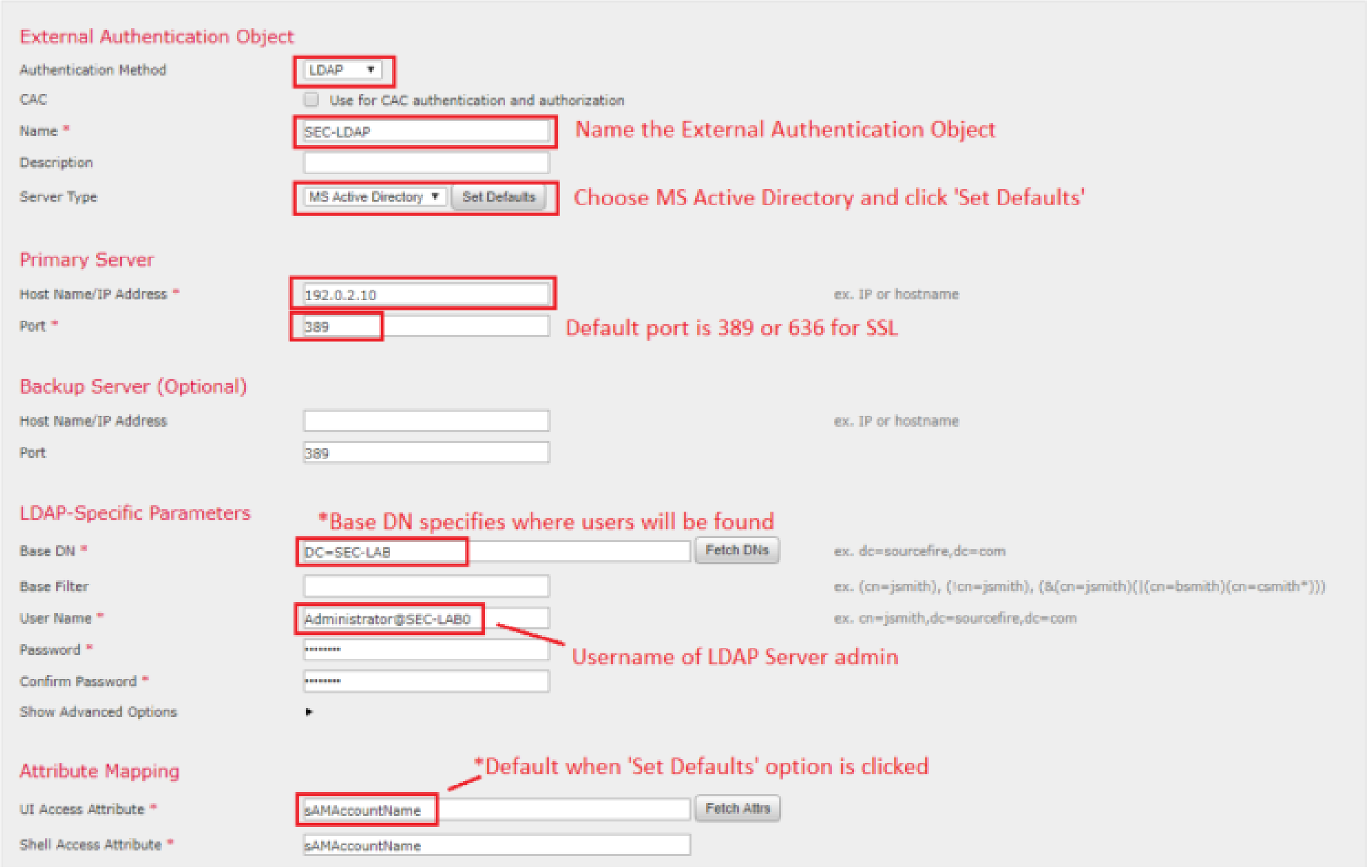
Default User Role: None

Shell Authentication Disabled

第二步：选择 Add External Authentication Object:



第三步：填写必填字段：



External Authentication Object

Authentication Method	LDAP ▾	
CAC	□ Use for CAC authentication and authorization	
Name *	SEC-LDAP	Name the External Authentication Object
Description		
Server Type	MS Active Directory ▾ Set Defaults	Choose MS Active Directory and click 'Set Defaults'

Primary Server

Host Name/IP Address *	192.0.2.10	ex. IP or hostname
Port *	389	Default port is 389 or 636 for SSL

Backup Server (Optional)

Host Name/IP Address		ex. IP or hostname
Port	389	

LDAP-Specific Parameters

*Base DN specifies where users will be found

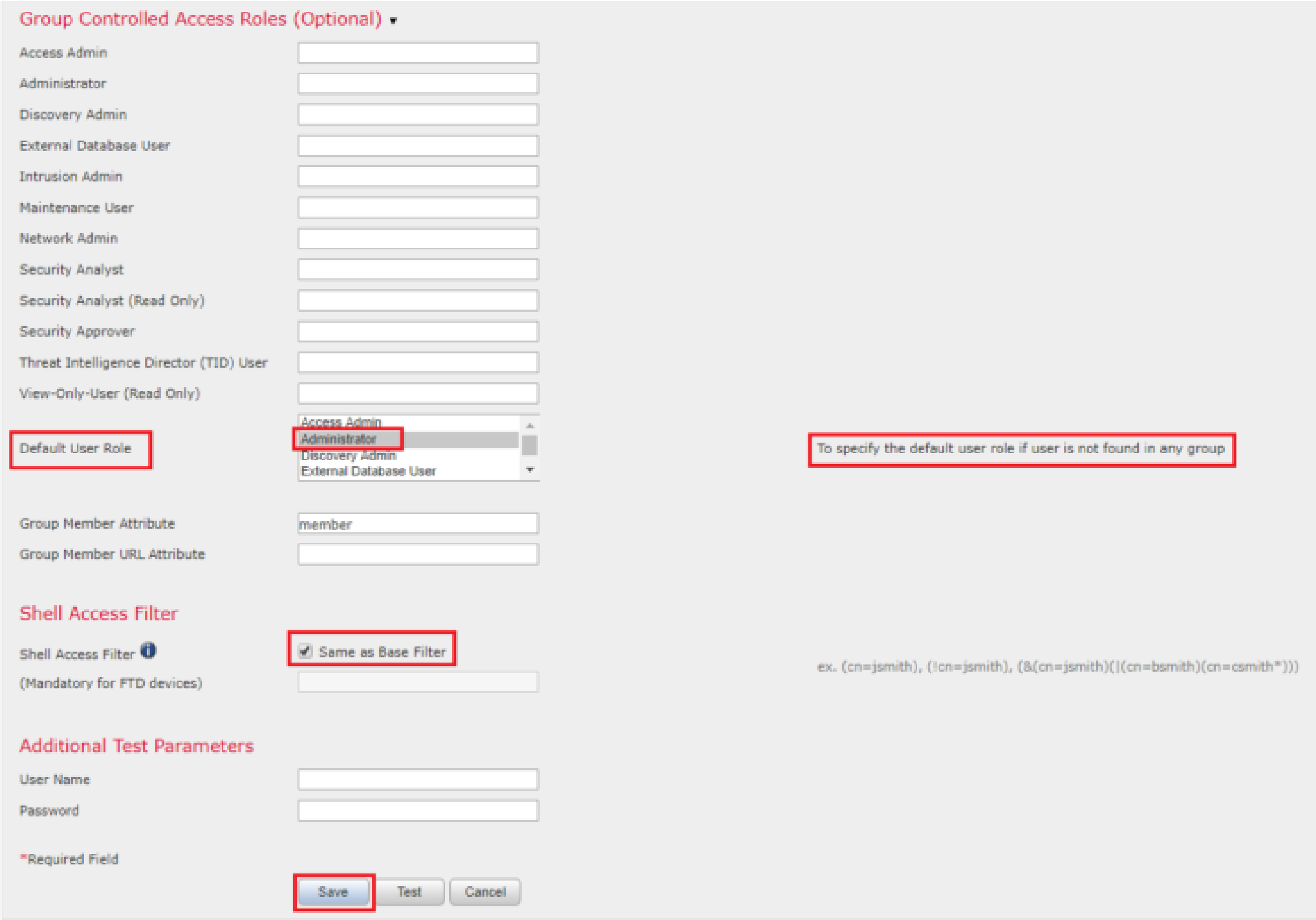
Base DN *	DC=SEC-LAB Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(|(cn=bsmith)(cn=csmith*)))
User Name *	Administrator@SEC-LAB0	ex. cn=jsmith,dc=sourcefire,dc=com
Password *	••••••••	
Confirm Password *	••••••••	
Show Advanced Options	▸	

Username of LDAP Server admin

Attribute Mapping

*Default when 'Set Defaults' option is clicked

UI Access Attribute *	sAMAccountName Fetch Attrs	
Shell Access Attribute *	sAMAccountName	



Group Controlled Access Roles (Optional) ▾

Access Admin	
Administrator	
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	
View-Only-User (Read Only)	
Default User Role	Access Admin Administrator Discovery Admin External Database User
Group Member Attribute	member
Group Member URL Attribute	

To specify the default user role if user is not found in any group

Shell Access Filter

Shell Access Filter ☑ Same as Base Filter

(Mandatory for FTD devices)

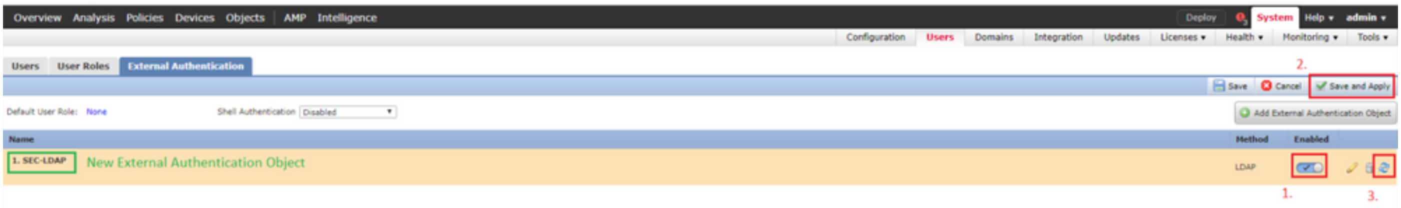
ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(|(cn=bsmith)(cn=csmith*)))

Additional Test Parameters

User Name	
Password	

*Required Field

第四步：启用 External Authentication 对象并保存：



Default User Role: None

Shell Authentication Disabled

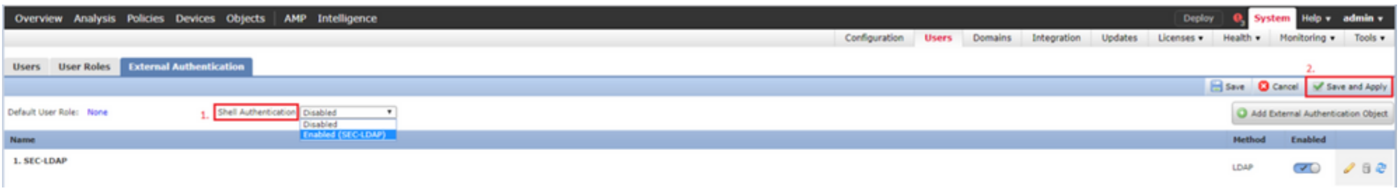
Name	Method	Enabled
1. SEC-LDAP New External Authentication Object	LDAP	✓

外部用户的外壳访问

FMC支持两个不同的内部管理员用户：一个用于Web界面，另一个具有CLI访问权限。这意味着谁可以访问GUI，谁也可以访问CLI之间有着明显的区别。在安装时，默认管理员用户的密码将同步，以便在GUI和CLI上相同，但是，它们由不同的内部机制跟踪，最终可能不同。

还必须授予LDAP外部用户外壳访问权限。

步骤1:导航至 System > Users > External Authentication 并点击 Shell Authentication 下拉框并保存：



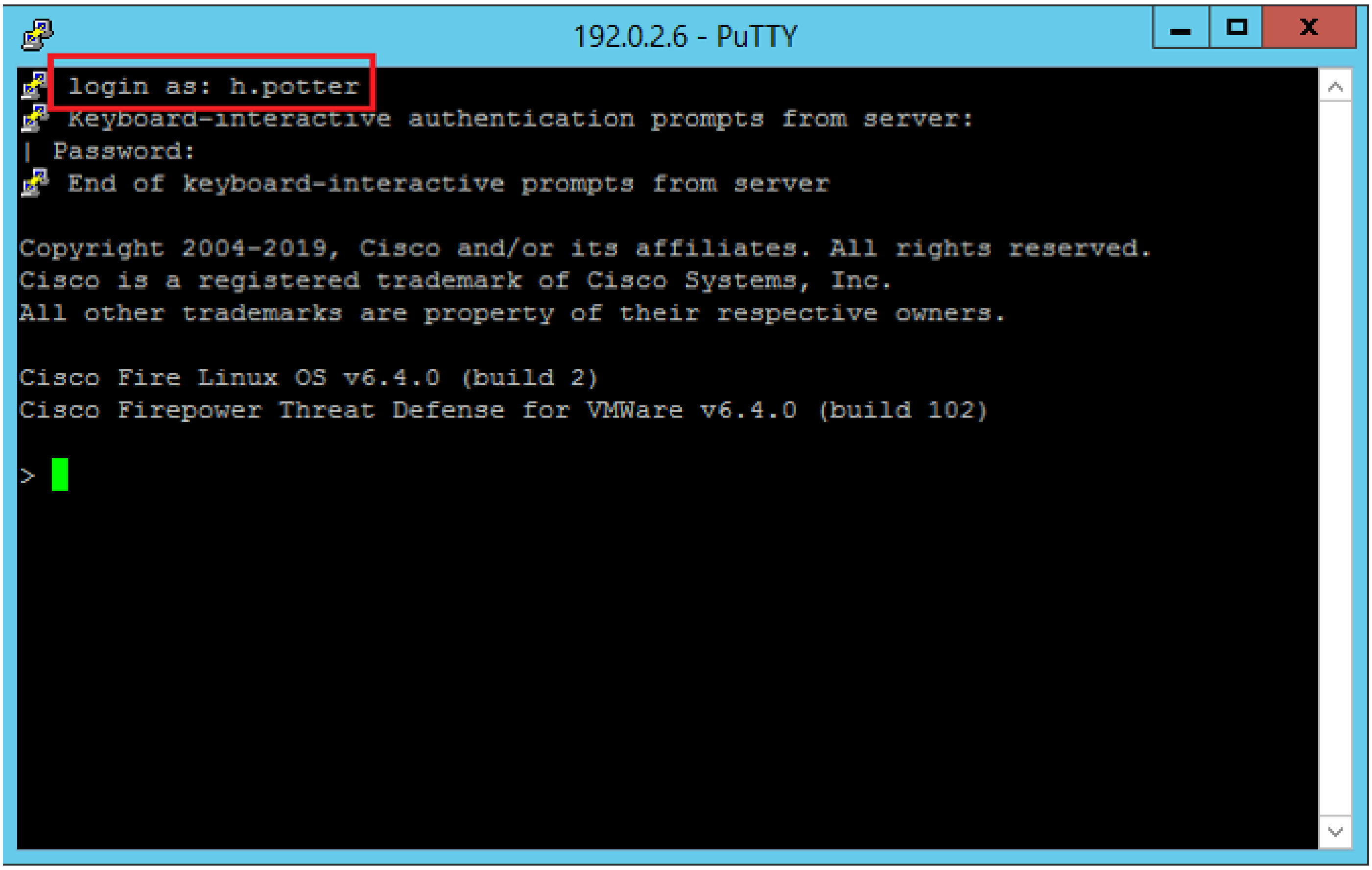
Default User Role: None

Shell Authentication Disabled
- Disabled
- Enabled (SEC-LDAP)

Name	Method	Enabled
1. SEC-LDAP	LDAP	✓

第二步：在FMC中部署更改。

配置外部用户的外壳访问后，通过SSH登录即启用，如图所示：

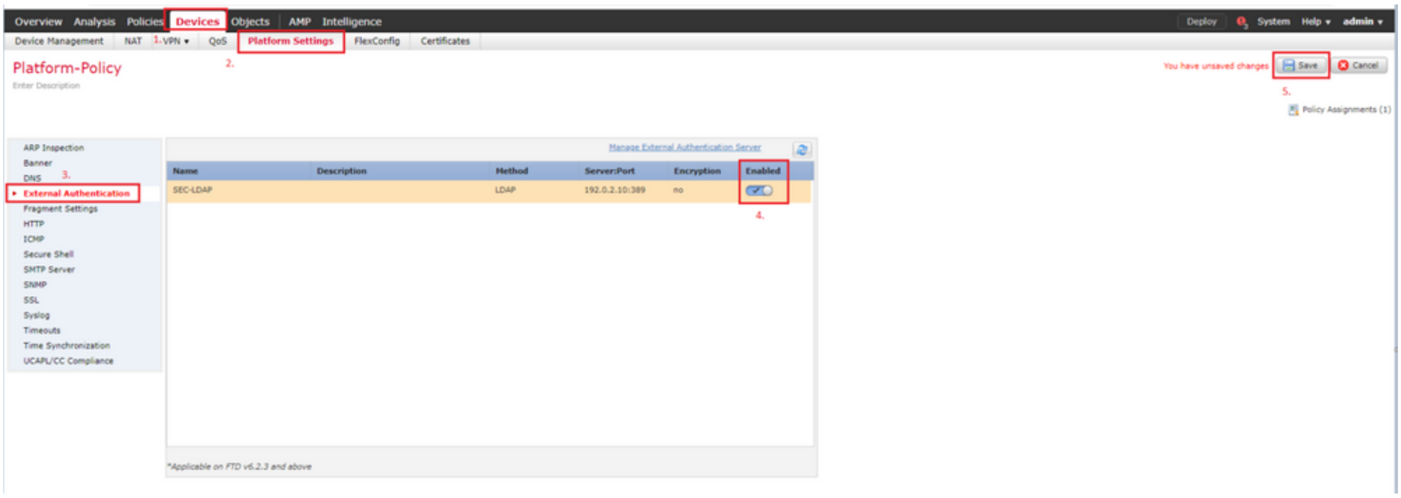


```
login as: h.potter
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.4.0 (build 2)
Cisco Firepower Threat Defense for VMWare v6.4.0 (build 102)

>
```

FTD的外部身份验证

可以在FTD上启用外部身份验证。

步骤1:导航至 Devices > Platform Settings > External Authentication.点击 Enabled 并保存：



Name	Description	Method	Server:Port	Encryption	Enabled
SEC-LDAP		LDAP	192.0.2.10:389	no	✓

*Applicable on FTD v6.2.3 and above

用户角色

用户权限基于分配的用户角色。您还可以创建自定义用户角色，这些角色具有根据组织需求定制的

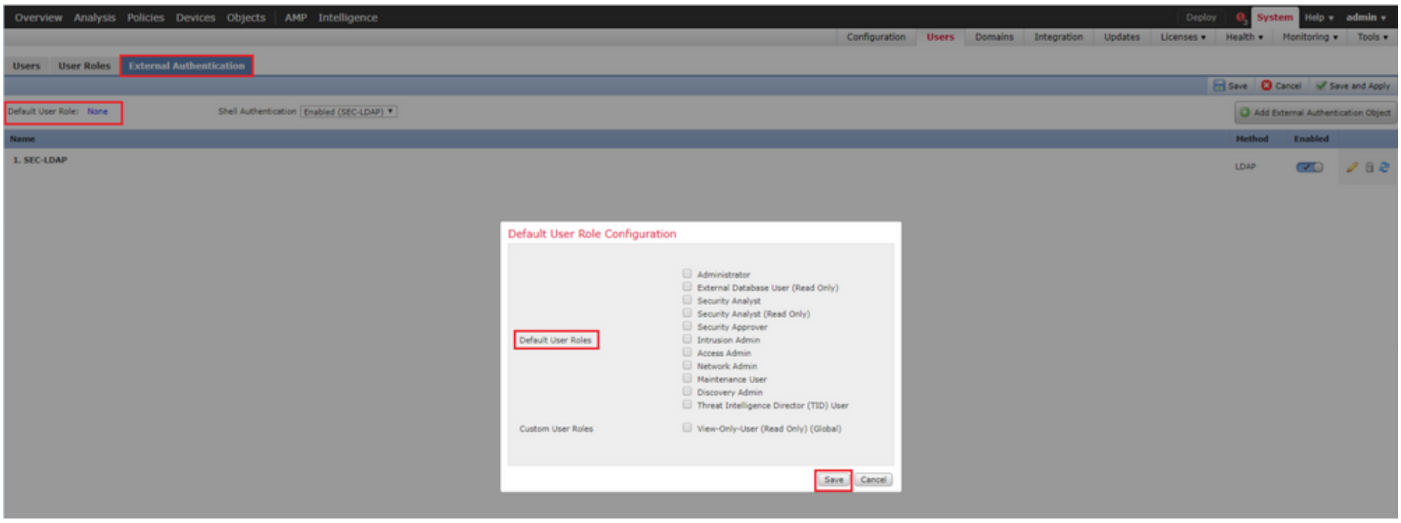
访问权限，或者您可以使用预定义角色，如安全分析师和发现管理员。

用户角色有两种类型：

1. Web界面用户角色
2. CLI用户角色

有关预定义角色的完整列表以及更多信息，请参阅用户角色。

要为所有外部身份验证对象配置默认用户角色，请导航至 System > Users > External Authentication > Default User Role. 选择要分配的默认用户角色，然后单击 Save.



Default User Role: None

Shell Authentication Enabled (SEC-LDAP) ▾

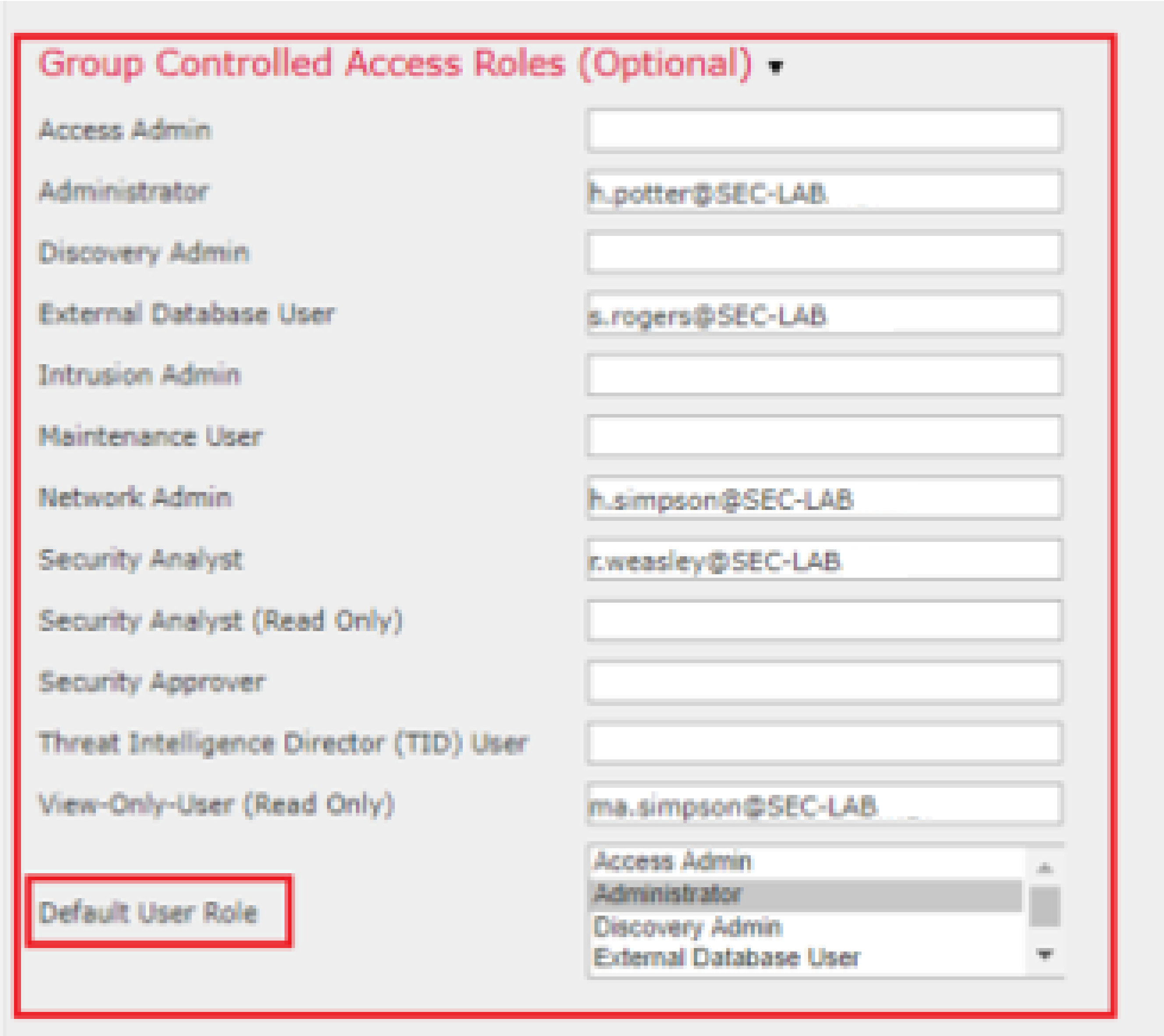
Name	Method	Enabled
1. SEC-LDAP	LDAP	✓

Default User Role Configuration

Default User Roles
- □ Administrator
- □ External Database User (Read Only)
- □ Security Analyst
- □ Security Analyst (Read Only)
- □ Security Approver
- □ Intrusion Admin
- □ Access Admin
- □ Network Admin
- □ Maintenance User
- □ Discovery Admin
- □ Threat Intelligence Director (TID) User

Custom User Roles
- □ View-Only-User (Read Only) (Global)

要选择默认用户角色或将特定角色分配给特定对象组中的特定用户，可以选择对象并导航至 Group Controlled Access Roles 如图所示：



Group Controlled Access Roles (Optional) ▾

Access Admin	
Administrator	h.potter@SEC-LAB
Discovery Admin	
External Database User	s.rogers@SEC-LAB
Intrusion Admin	
Maintenance User	
Network Admin	h.simpson@SEC-LAB
Security Analyst	r.weasley@SEC-LAB
Security Analyst (Read Only)	
Security Approver	
Threat Intelligence Director (TID) User	
View-Only-User (Read Only)	ma.simpson@SEC-LAB
Default User Role	Access Admin Administrator Discovery Admin External Database User

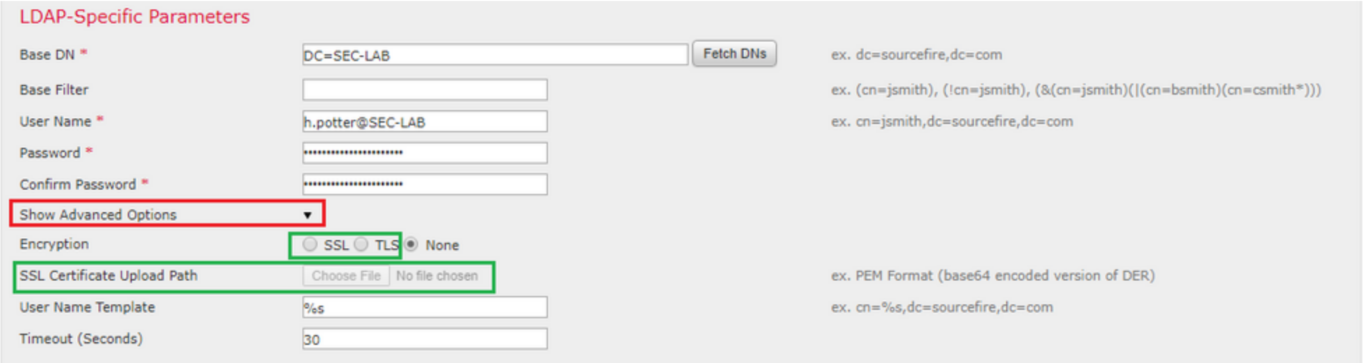
SSL或TLS

必须在FMC中配置DNS。这是因为证书的Subject值必须与 Authentication Object Primary Server Hostname.配置安全LDAP后，数据包捕获不再显示明文绑定请求。

SSL将默认端口更改为636,TLS将其保留为389。

注意：TLS加密需要所有平台上的证书。对于SSL，FTD还需要证书。对于其他平台，SSL不需要证书。但是，建议您始终为SSL上传证书，以防止中间人攻击。

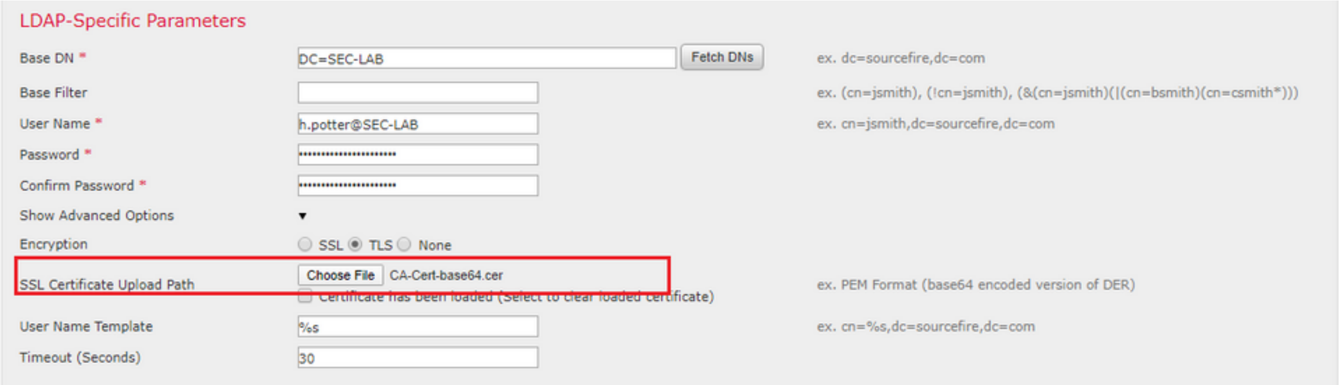
步骤1:导航至 Devices > Platform Settings > External Authentication > External Authentication Object 并输入高级选项SSL/TLS信息：



LDAP-Specific Parameters

Base DN *	DC=SEC-LAB Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(|(cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB	ex. cn=jsmith,dc=sourcefire,dc=com
Password *	••••••••••••••••••••••	
Confirm Password *	••••••••••••••••••••••	
Show Advanced Options	▼	
Encryption	○ SSL ○ TLS ● None	
SSL Certificate Upload Path	Choose File No file chosen	ex. PEM Format (base64 encoded version of DER)
User Name Template	%s	ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30	

第二步：上传签署服务器证书的CA的证书。证书必须是PEM格式。



LDAP-Specific Parameters

Base DN *	DC=SEC-LAB Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter		ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(|(cn=bsmith)(cn=csmith*)))
User Name *	h.potter@SEC-LAB	ex. cn=jsmith,dc=sourcefire,dc=com
Password *	••••••••••••••••••••••	
Confirm Password *	••••••••••••••••••••••	
Show Advanced Options	▼	
Encryption	○ SSL ● TLS ○ None	
SSL Certificate Upload Path	Choose File CA-Cert-base64.cer □ Certificate has been loaded (Select to clear loaded certificate)	ex. PEM Format (base64 encoded version of DER)
User Name Template	%s	ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30	

第三步：保存配置。

验证

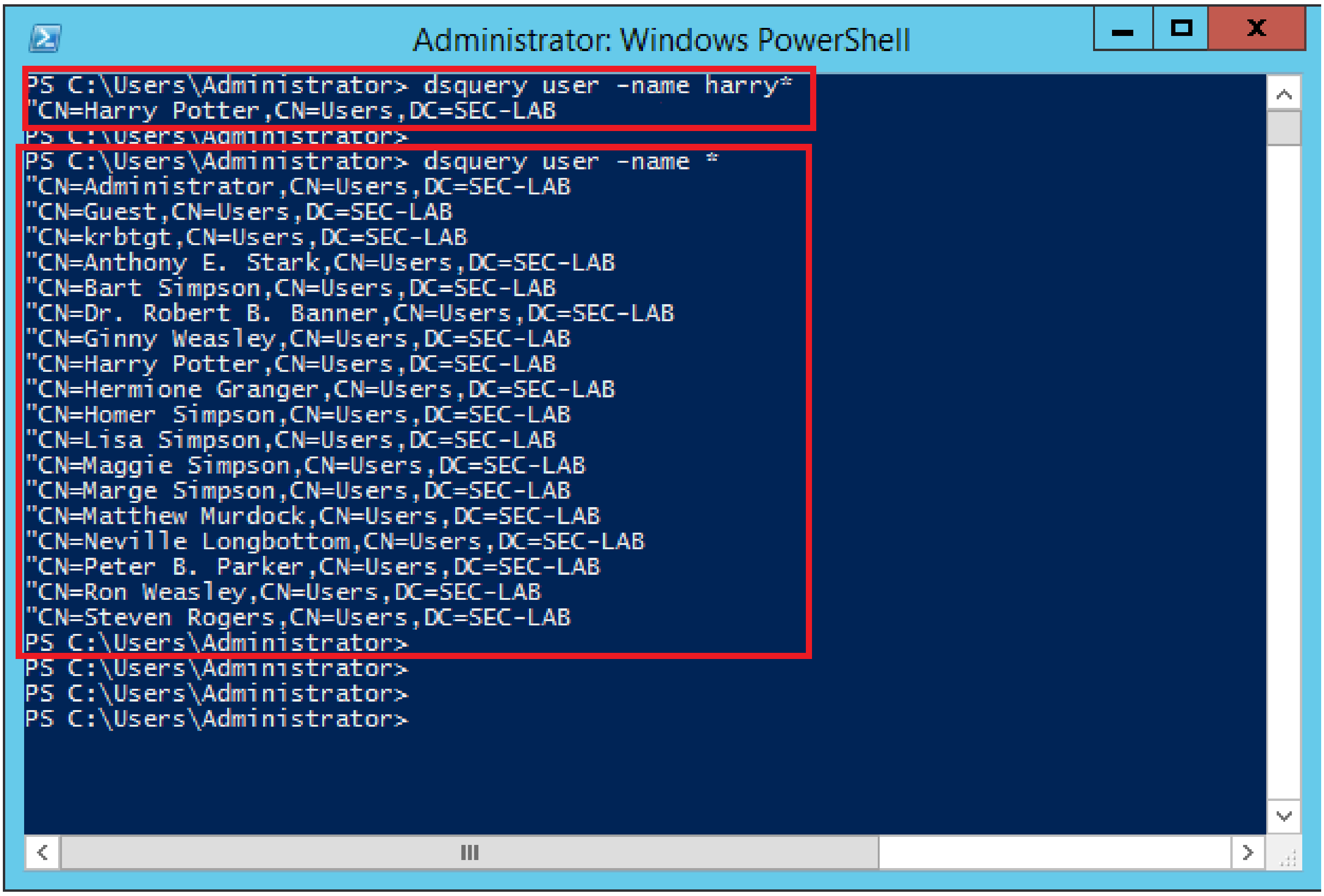
测试搜索库

打开配置了LDAP的Windows命令提示符或PowerShell，然后键入命令： dsquery user -name

.

例如：

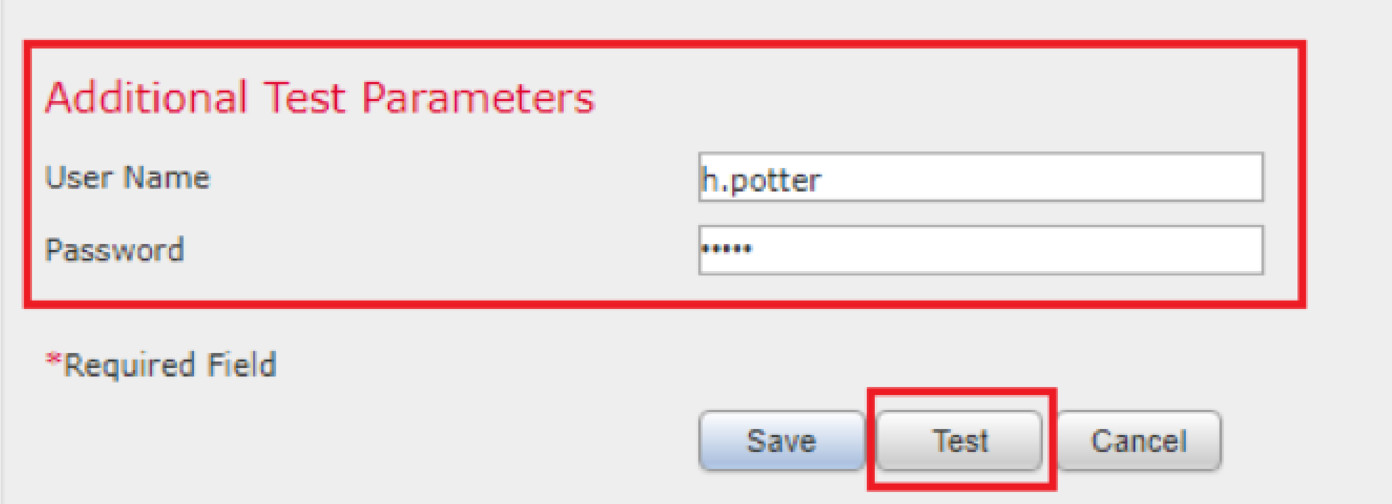
```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```



```
PS C:\Users\Administrator> dsquery user -name harry*
"CN=Harry Potter,CN=Users,DC=SEC-LAB
PS C:\Users\Administrator>
PS C:\Users\Administrator> dsquery user -name *
"CN=Administrator,CN=Users,DC=SEC-LAB
"CN=Guest,CN=Users,DC=SEC-LAB
"CN=krbtgt,CN=Users,DC=SEC-LAB
"CN=Anthony E. Stark,CN=Users,DC=SEC-LAB
"CN=Bart Simpson,CN=Users,DC=SEC-LAB
"CN=Dr. Robert B. Banner,CN=Users,DC=SEC-LAB
"CN=Ginny Weasley,CN=Users,DC=SEC-LAB
"CN=Harry Potter,CN=Users,DC=SEC-LAB
"CN=Hermione Granger,CN=Users,DC=SEC-LAB
"CN=Homer Simpson,CN=Users,DC=SEC-LAB
"CN=Lisa Simpson,CN=Users,DC=SEC-LAB
"CN=Maggie Simpson,CN=Users,DC=SEC-LAB
"CN=Marge Simpson,CN=Users,DC=SEC-LAB
"CN=Matthew Murdock,CN=Users,DC=SEC-LAB
"CN=Neville Longbottom,CN=Users,DC=SEC-LAB
"CN=Peter B. Parker,CN=Users,DC=SEC-LAB
"CN=Ron Weasley,CN=Users,DC=SEC-LAB
"CN=Steven Rogers,CN=Users,DC=SEC-LAB
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

测试LDAP集成

导航至 System > Users > External Authentication > External Authentication Object.页面底部有一个 Additional Test Parameters 部分如图所示：

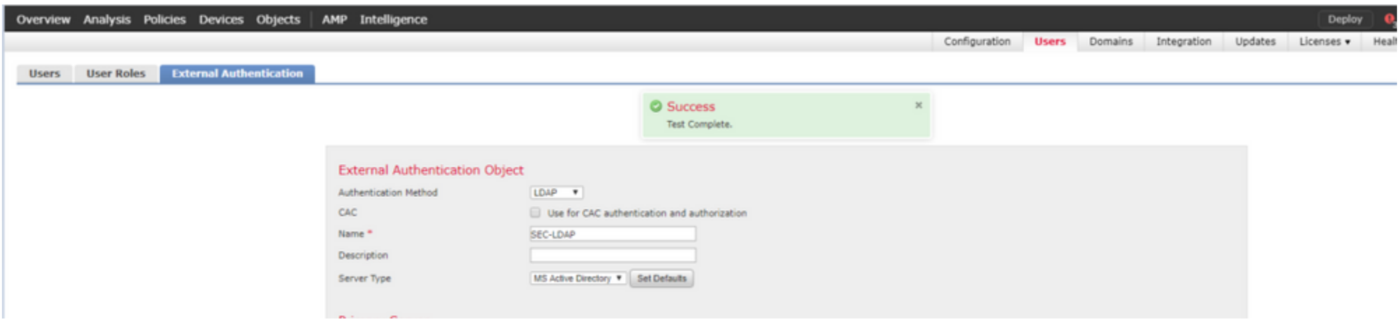

Additional Test Parameters

User Name: h.potter

Password: •••••

*Required Field

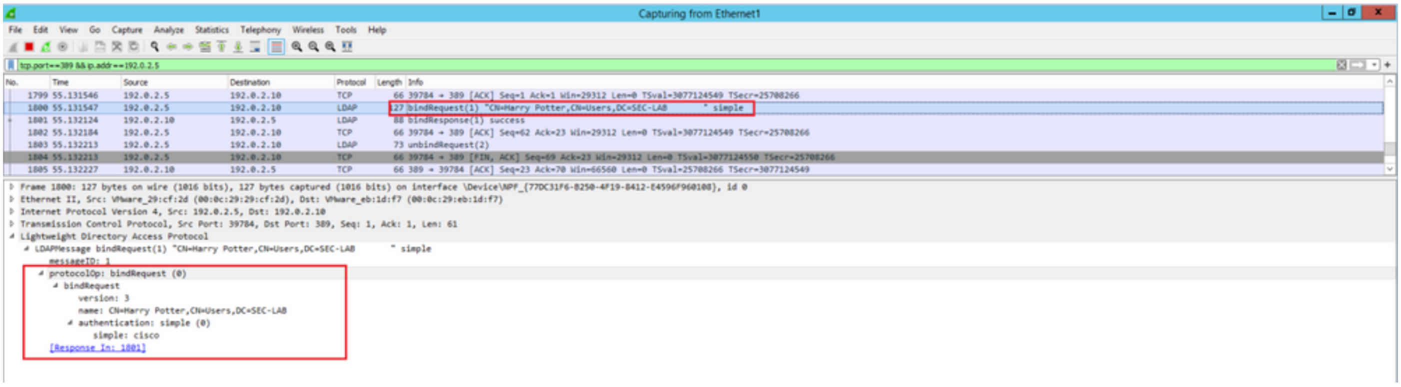
选择Test以查看结果。



Success
Test Complete.

External Authentication Object

Authentication Method: LDAP
CAC: □ Use for CAC authentication and authorization
Name *: SEC-LDAP
Description:
Server Type: MS Active Directory ▾ Set Defaults



```
tcp.port==389 && ip.addr==192.0.2.5

No.   Time        Source      Destination  Protocol Length Info
 1799 55.131546   192.0.2.5   192.0.2.10   TCP      66 39784 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3077124549 TSecr=25708266
 1800 55.131547   192.0.2.5   192.0.2.10   LDAP     127 bindRequest(1) "CN=Harry Potter,CN=Users,DC=SEC-LAB        " simple
 1801 55.132124   192.0.2.10  192.0.2.5    LDAP     88 bindResponse(1) success
 1802 55.132184   192.0.2.5   192.0.2.10   TCP      66 39784 → 389 [ACK] Seq=62 Ack=23 Win=29312 Len=0 TSval=3077124549 TSecr=25708266
 1803 55.132213   192.0.2.5   192.0.2.10   LDAP     73 unbindRequest(2)
 1804 55.132213   192.0.2.5   192.0.2.10   TCP      66 39784 → 389 [FIN, ACK] Seq=69 Ack=23 Win=29312 Len=0 TSval=3077124550 TSecr=25708266
 1805 55.132227   192.0.2.10  192.0.2.5    TCP      66 389 → 39784 [ACK] Seq=23 Ack=70 Win=66560 Len=0 TSval=25708266 TSecr=3077124549

▷ Frame 1800: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface \Device\NPF_{77DC31F6-8250-4F19-8412-E4596F960108}, id 0
▷ Ethernet II, Src: VMware_29:cf:2d (00:0c:29:29:cf:2d), Dst: VMware_eb:1d:f7 (00:0c:29:eb:1d:f7)
▷ Internet Protocol Version 4, Src: 192.0.2.5, Dst: 192.0.2.10
▷ Transmission Control Protocol, Src Port: 39784, Dst Port: 389, Seq: 1, Ack: 1, Len: 61
◢ Lightweight Directory Access Protocol
  ◢ LDAPMessage bindRequest(1) "CN=Harry Potter,CN=Users,DC=SEC-LAB        " simple
      messageID: 1
    ◢ protocolOp: bindRequest (0)
      ◢ bindRequest
          version: 3
          name: CN=Harry Potter,CN=Users,DC=SEC-LAB
        ◢ authentication: simple (0)
            simple: cisco
      [Response In: 1801]
```

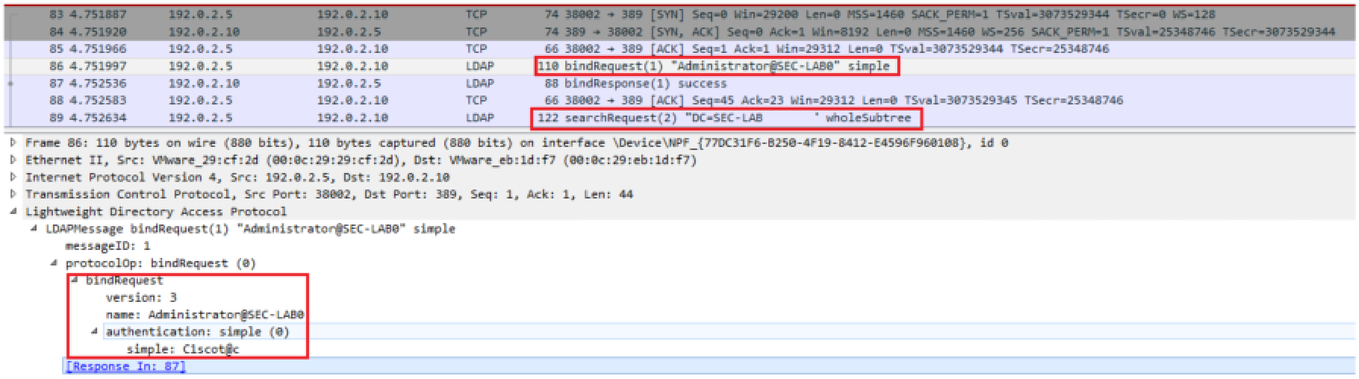
故障排除

FMC/FTD和LDAP如何进行交互以下载用户？

为了使FMC能够从Microsoft LDAP服务器提取用户，FMC必须首先使用LDAP管理员凭证在端口389或636(SSL)上发送绑定请求。一旦LDAP服务器能够对FMC进行身份验证，它将以成功消息做出响应。最后，FMC能够使用搜索请求消息发出请求，如图所示：

<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << --- FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

请注意，默认情况下，身份验证以明文形式发送密码：

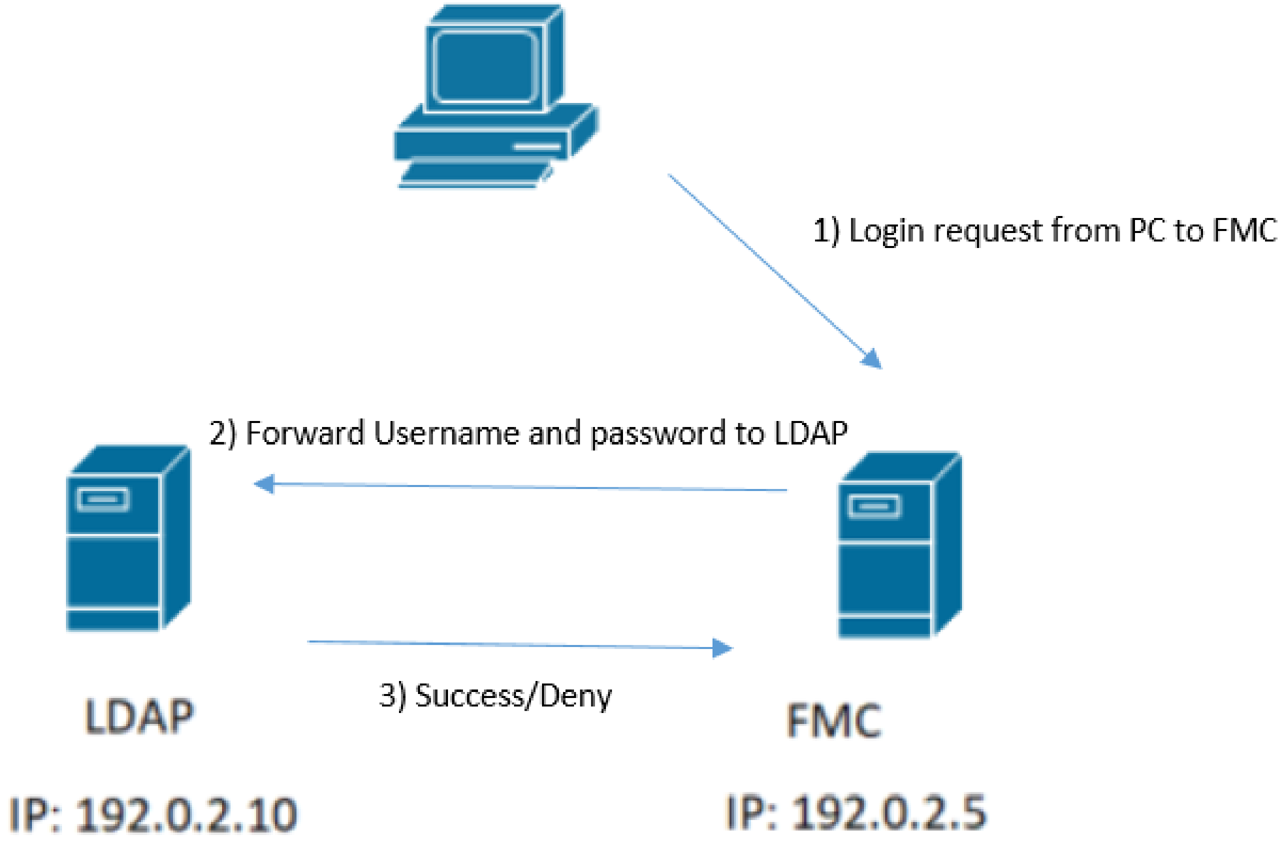


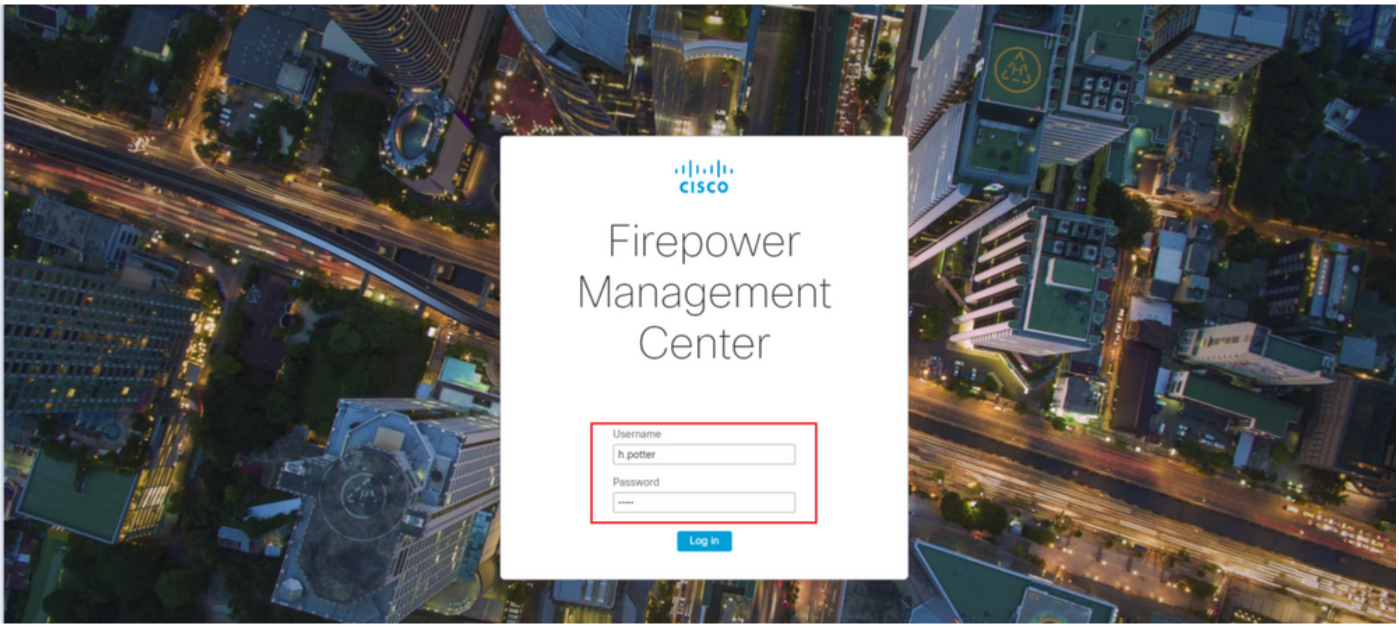
```
 83 4.751887   192.0.2.5    192.0.2.10   TCP    74 38002 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3073529344 TSecr=0 WS=128
 84 4.751920   192.0.2.10   192.0.2.5    TCP    74 389 → 38002 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=25348746 TSecr=3073529344
 85 4.751966   192.0.2.5    192.0.2.10   TCP    66 38002 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3073529344 TSecr=25348746
 86 4.751997   192.0.2.5    192.0.2.10   LDAP   110 bindRequest(1) "Administrator@SEC-LAB0" simple
 87 4.752536   192.0.2.10   192.0.2.5    LDAP   88 bindResponse(1) success
 88 4.752583   192.0.2.5    192.0.2.10   TCP    66 38002 → 389 [ACK] Seq=45 Ack=23 Win=29312 Len=0 TSval=3073529345 TSecr=25348746
 89 4.752634   192.0.2.5    192.0.2.10   LDAP   122 searchRequest(2) "DC=SEC-LAB        " wholeSubtree

▷ Frame 86: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{77DC31F6-8250-4F19-8412-E4596F960108}, id 0
▷ Ethernet II, Src: VMware_29:cf:2d (00:0c:29:29:cf:2d), Dst: VMware_eb:1d:f7 (00:0c:29:eb:1d:f7)
▷ Internet Protocol Version 4, Src: 192.0.2.5, Dst: 192.0.2.10
▷ Transmission Control Protocol, Src Port: 38002, Dst Port: 389, Seq: 1, Ack: 1, Len: 44
◢ Lightweight Directory Access Protocol
  ◢ LDAPMessage bindRequest(1) "Administrator@SEC-LAB0" simple
      messageID: 1
    ◢ protocolOp: bindRequest (0)
      ◢ bindRequest
          version: 3
          name: Administrator@SEC-LAB0
        ◢ authentication: simple (0)
            simple: C1scot@c
      [Response In: 87]
```

FMC/FTD和LDAP如何交互以验证用户登录请求？

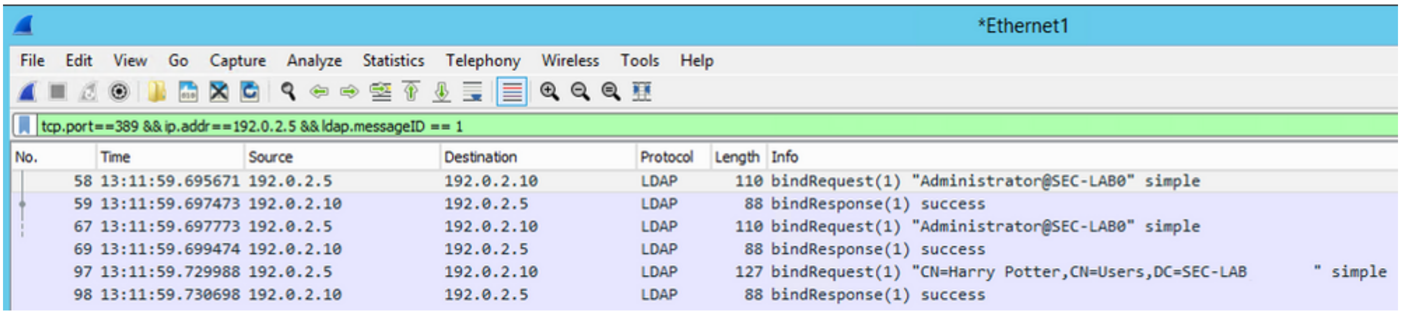
为了使用户能够在启用LDAP身份验证时登录到FMC或FTD，初始登录请求将发送到Firepower，但用户名和密码将转发到LDAP以成功/拒绝响应。这意味着FMC和FTD不会将密码信息保存在本地数

据库中，而是等待LDAP确认如何继续。


1) Login request from PC to FMC
2) Forward Username and password to LDAP
3) Success/Deny
LDAP
FMC
IP: 192.0.2.10
IP: 192.0.2.5

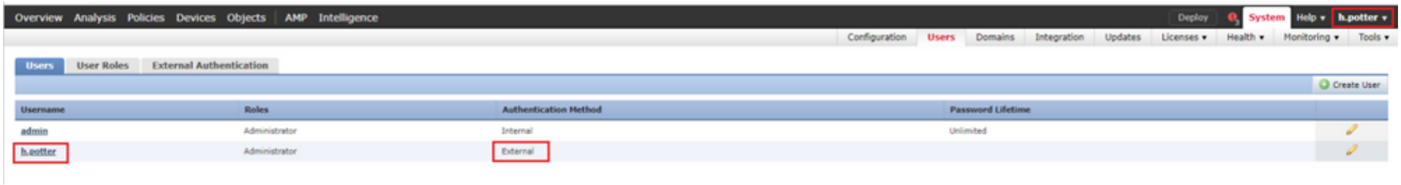


Username
h.potter
Password
·····


*Ethernet1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==389 && ip.addr==192.0.2.5 && ldap.messageID == 1

No.  Time             Source       Destination  Protocol Length Info
  58 13:11:59.695671 192.0.2.5    192.0.2.10   LDAP      110 bindRequest(1) "Administrator@SEC-LAB0" simple
  59 13:11:59.697473 192.0.2.10   192.0.2.5    LDAP       88 bindResponse(1) success
  67 13:11:59.697773 192.0.2.5    192.0.2.10   LDAP      110 bindRequest(1) "Administrator@SEC-LAB0" simple
  69 13:11:59.699474 192.0.2.10   192.0.2.5    LDAP       88 bindResponse(1) success
  97 13:11:59.729988 192.0.2.5    192.0.2.10   LDAP      127 bindRequest(1) "CN=Harry Potter,CN=Users,DC=SEC-LAB       " simple
  98 13:11:59.730698 192.0.2.10   192.0.2.5    LDAP       88 bindResponse(1) success
```

如果接受用户名和密码，则会在Web GUI中添加一个条目，如图所示：



Username	Roles	Authentication Method	Password Lifetime
admin	Administrator	Internal	Unlimited
h.potter	Administrator	External	

在FMC CLISH中运行命令show user以验证用户信息： > show user

命令显示指定用户的详细配置信息。将显示以下值：

Login — 登录名

UID — 数字用户ID
Auth（本地或远程）— 如何对用户进行身份验证
访问（基本或配置）— 用户的权限级别
已启用（启用或禁用）— 用户是否处于活动状态
重置（是或否）— 用户是否必须在下次登录时更改密码
Exp（Never或数字）— 必须更改用户密码之前的天数
Warn(N/A or a number) — 指定用户在其密码到期之前更改其密码的天数
Str（Yes或No）— 用户的密码是否必须满足条件才能检查强度
Lock（Yes或No）— 用户帐户是否由于登录失败太多而被锁定
Max(N/A or a number) — 锁定用户帐户之前的最大失败登录数

SSL或TLS未按预期工作

如果未在FTD上启用DNS，则可以在尾部日志中看到提示LDAP无法访问的错误：

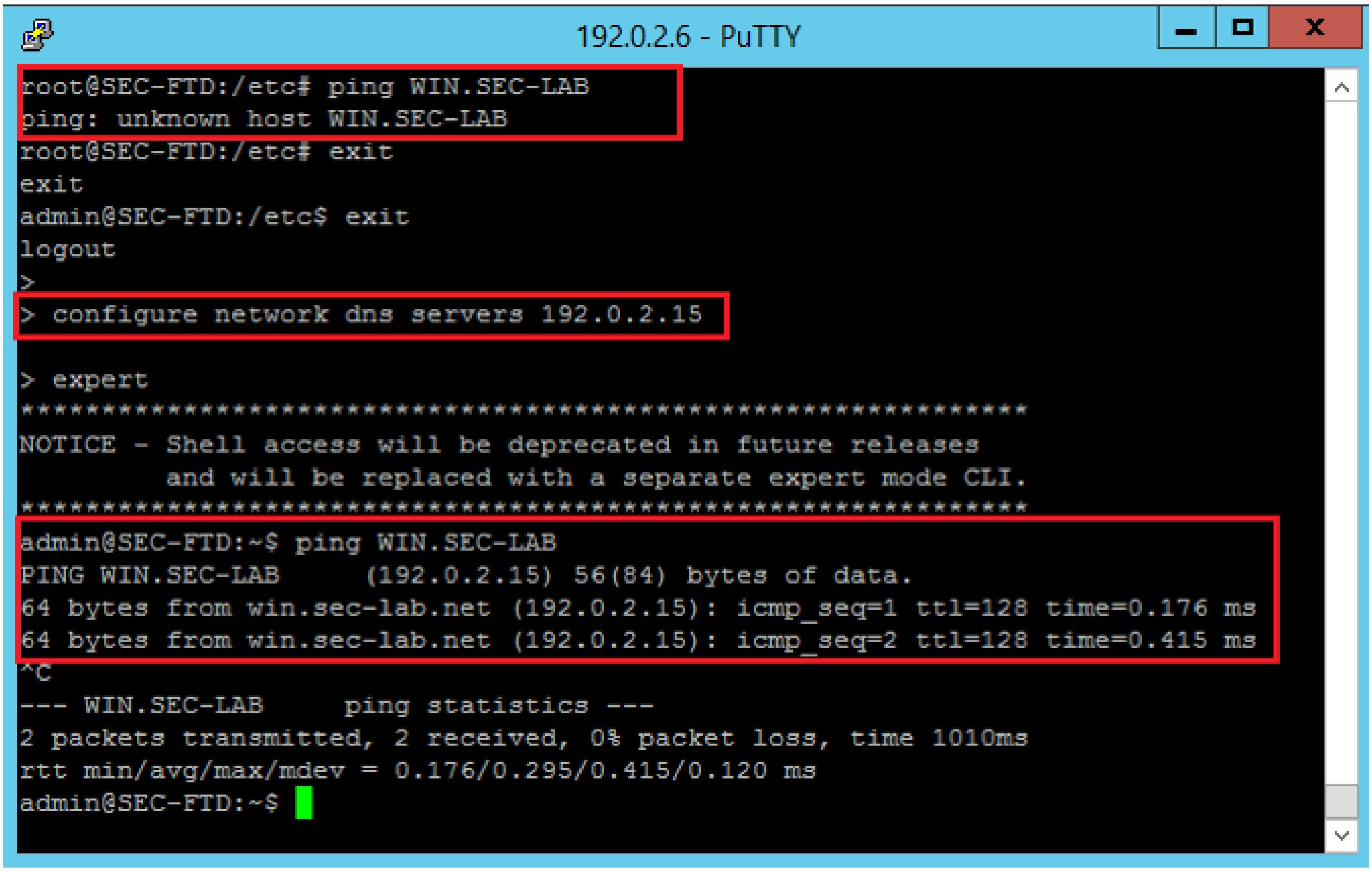
```
root@SEC-FMC:/$ sudo cd /var/common
root@SEC-FMC:/var/common$ sudo pigtail
```

```
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2.
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15 
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter 
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 61
```

确保Firepower能够解析LDAP服务器FQDN。否则，请添加映像中所示的正确DNS。

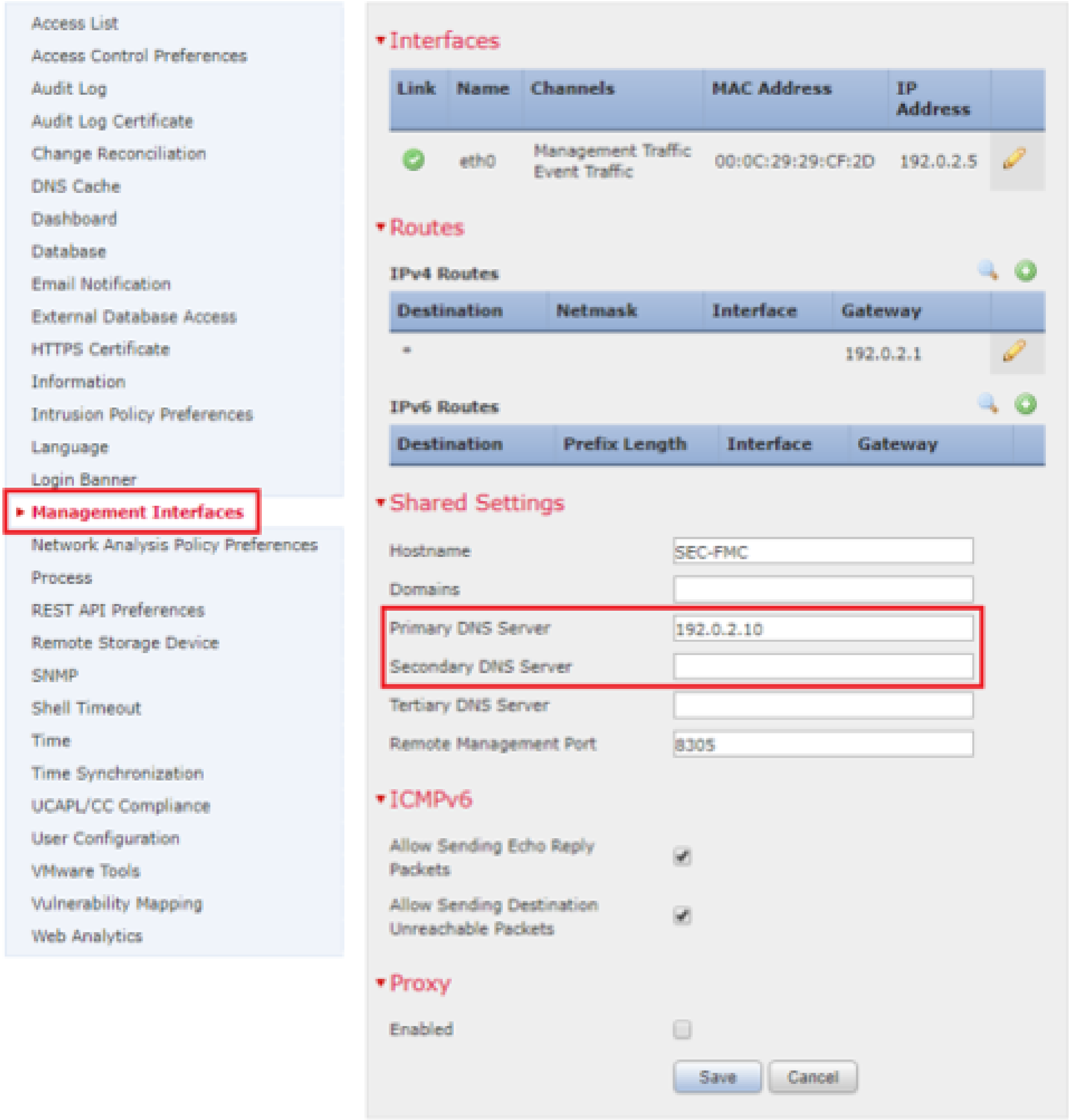
FTD：访问FTD CLISH并运行命令： > configure network dns servers

.



```
root@SEC-FTD:/etc# ping WIN.SEC-LAB
ping: unknown host WIN.SEC-LAB
root@SEC-FTD:/etc# exit
exit
admin@SEC-FTD:/etc$ exit
logout
>
> configure network dns servers 192.0.2.15

> expert
**************************************************************
NOTICE - Shell access will be deprecated in future releases
         and will be replaced with a separate expert mode CLI.
**************************************************************
admin@SEC-FTD:~$ ping WIN.SEC-LAB
PING WIN.SEC-LAB     (192.0.2.15) 56(84) bytes of data.
64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=1 ttl=128 time=0.176 ms
64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=2 ttl=128 time=0.415 ms
^C
--- WIN.SEC-LAB     ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.176/0.295/0.415/0.120 ms
admin@SEC-FTD:~$
```

FMC：选择 System > Configuration，然后选择Management Interfaces，如图所示：



▾Interfaces

Link	Name	Channels	MAC Address	IP Address
✓	eth0	Management Traffic Event Traffic	00:0C:29:29:CF:2D	192.0.2.5

▾Routes

IPv4 Routes

Destination	Netmask	Interface	Gateway
*			192.0.2.1

IPv6 Routes

Destination	Prefix Length	Interface	Gateway

▾Shared Settings

Hostname	SEC-FMC
Domains	
Primary DNS Server	192.0.2.10
Secondary DNS Server	
Tertiary DNS Server	
Remote Management Port	8305

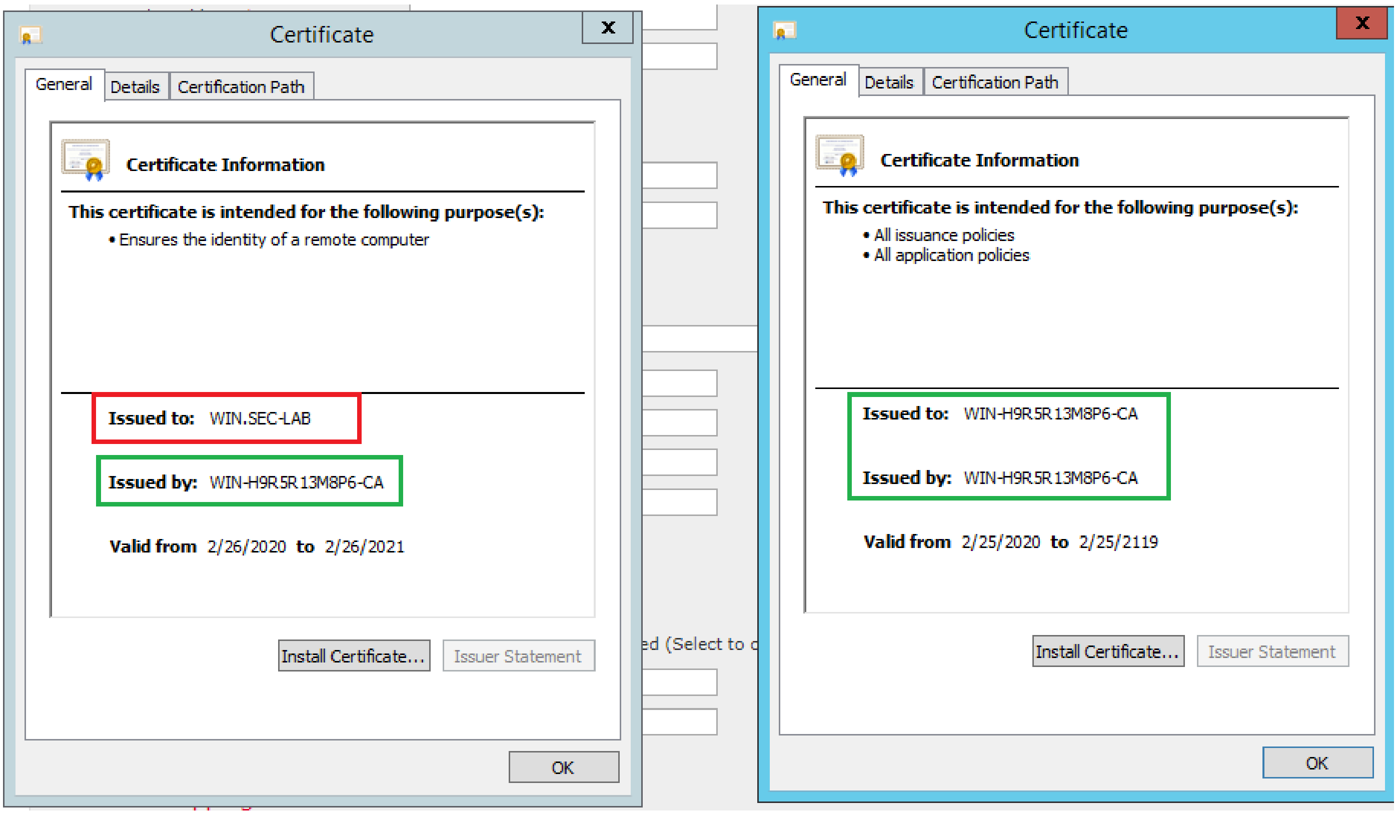
▾ICMPv6

Allow Sending Echo Reply Packets	☑
Allow Sending Destination Unreachable Packets	☑

▾Proxy

Enabled	☐

确保上传到FMC的证书是签署LDAP服务器证书的CA的证书，如图所示：



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: WIN.SEC-LAB

Issued by: WIN-H9R5R13M8P6-CA

Valid from 2/26/2020 **to** 2/26/2021

Install Certificate... | Issuer Statement | OK

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

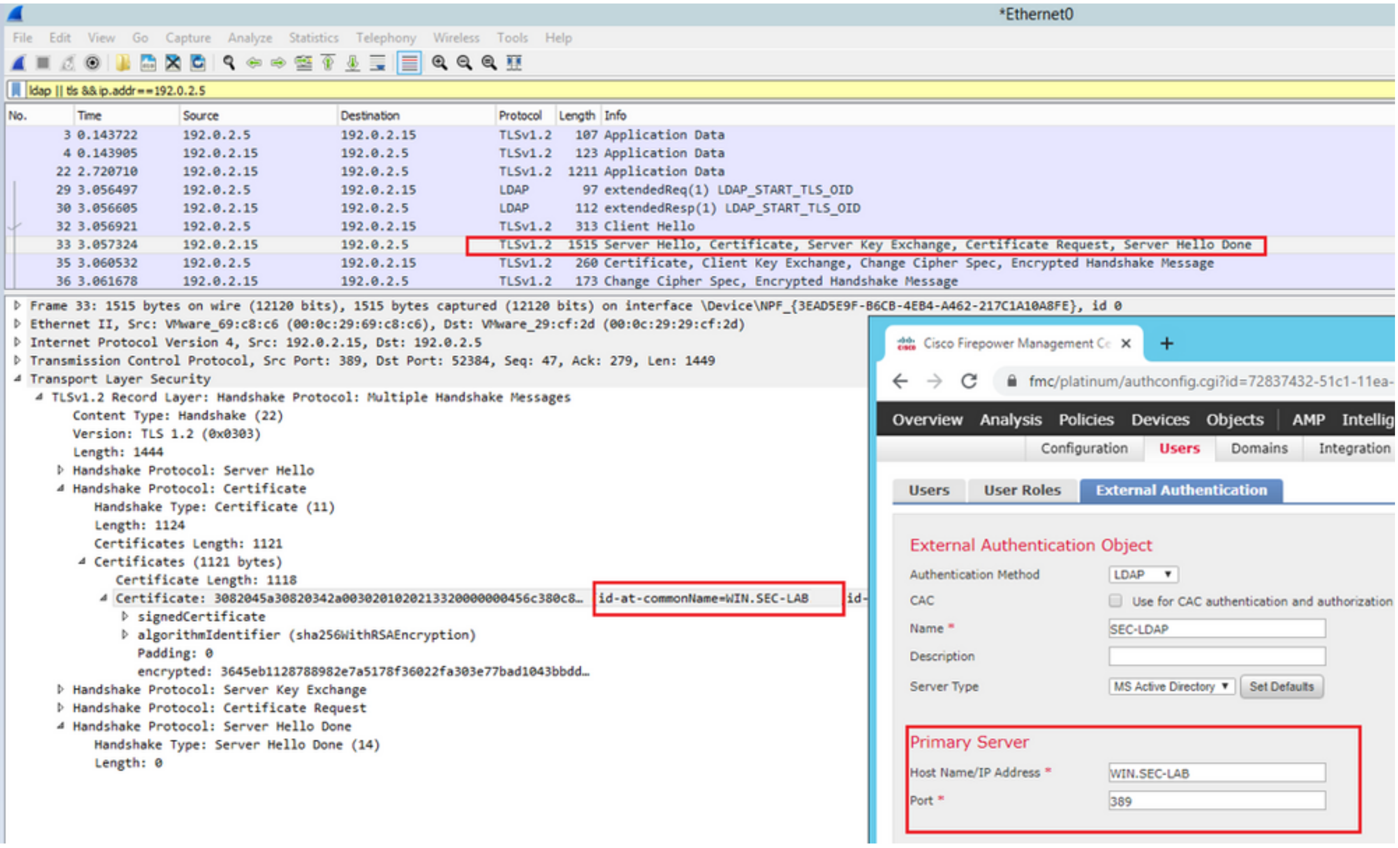
Issued to: WIN-H9R5R13M8P6-CA

Issued by: WIN-H9R5R13M8P6-CA

Valid from 2/25/2020 **to** 2/25/2119

Install Certificate... | Issuer Statement | OK

使用数据包捕获确认LDAP服务器发送正确的信息：



*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ldap || tls && ip.addr==192.0.2.5

No.   Time        Source        Destination   Protocol  Length Info
    3 0.143722    192.0.2.5     192.0.2.15    TLSv1.2    107 Application Data
    4 0.143905    192.0.2.15    192.0.2.5     TLSv1.2    123 Application Data
   22 2.720710    192.0.2.15    192.0.2.5     TLSv1.2   1211 Application Data
   29 3.056497    192.0.2.5     192.0.2.15    LDAP        97 extendedReq(1) LDAP_START_TLS_OID
   30 3.056605    192.0.2.15    192.0.2.5     LDAP       112 extendedResp(1) LDAP_START_TLS_OID
   32 3.056921    192.0.2.5     192.0.2.15    TLSv1.2    313 Client Hello
   33 3.057324    192.0.2.15    192.0.2.5     TLSv1.2   1515 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
   35 3.060532    192.0.2.5     192.0.2.15    TLSv1.2    260 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   36 3.061678    192.0.2.15    192.0.2.5     TLSv1.2    173 Change Cipher Spec, Encrypted Handshake Message

▷ Frame 33: 1515 bytes on wire (12120 bits), 1515 bytes captured (12120 bits) on interface \Device\NPF_{3EAD5E9F-B6CB-4EB4-A462-217C1A10A8FE}, id 0
▷ Ethernet II, Src: VMware_69:c8:c6 (00:0c:29:69:c8:c6), Dst: VMware_29:cf:2d (00:0c:29:29:cf:2d)
▷ Internet Protocol Version 4, Src: 192.0.2.15, Dst: 192.0.2.5
▷ Transmission Control Protocol, Src Port: 389, Dst Port: 52384, Seq: 47, Ack: 279, Len: 1449
◢ Transport Layer Security
  ◢ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1444
    ▷ Handshake Protocol: Server Hello
    ◢ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1124
        Certificates Length: 1121
      ◢ Certificates (1121 bytes)
          Certificate Length: 1118
        ◢ Certificate: 3082045a30820342a003020102021332000000456c380c8… id-at-commonName=WIN.SEC-LAB id-
          ▷ signedCertificate
          ▷ algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted: 3645eb1128788982e7a5178f36022fa303e77bad1043bbdd…
    ▷ Handshake Protocol: Server Key Exchange
    ▷ Handshake Protocol: Certificate Request
    ◢ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

Cisco Firepower Management Ce ✕ +
fmc/platinum/authconfig.cgi?id=72837432-51c1-11ea-
Overview Analysis Policies Devices Objects AMP Intellig
Configuration Users Domains Integration
Users User Roles External Authentication

External Authentication Object

Authentication Method: LDAP

CAC: □ Use for CAC authentication and authorization

Name *: SEC-LDAP

Description:

Server Type: MS Active Directory | Set Defaults

Primary Server

Host Name/IP Address *: WIN.SEC-LAB

Port *: 389

相关信息

- 用于管理访问的用户帐户

- Cisco Firepower管理中心轻量级目录访问协议身份验证绕行漏洞
- 在FireSIGHT系统上配置LDAP身份验证对象
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。