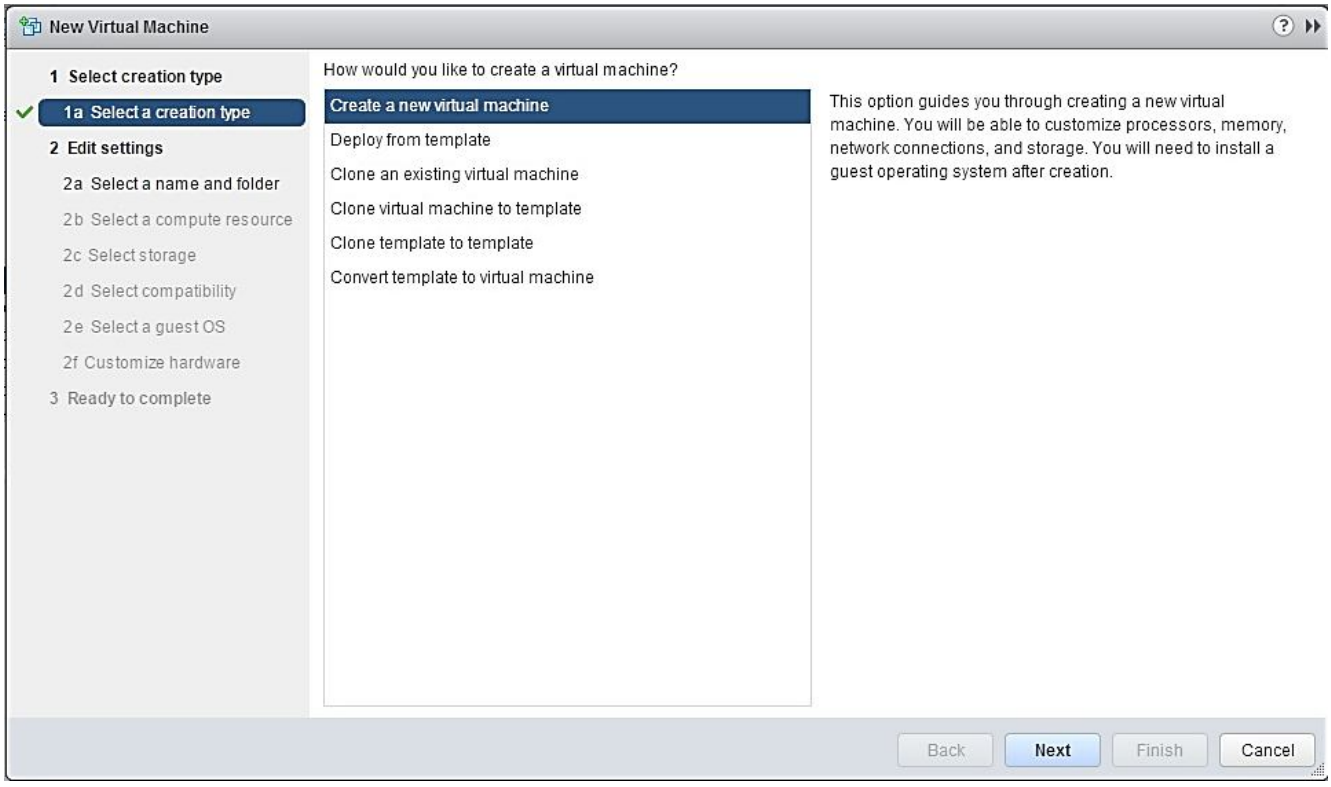
Cisco ACS

مراحل نصب و راه اندازی

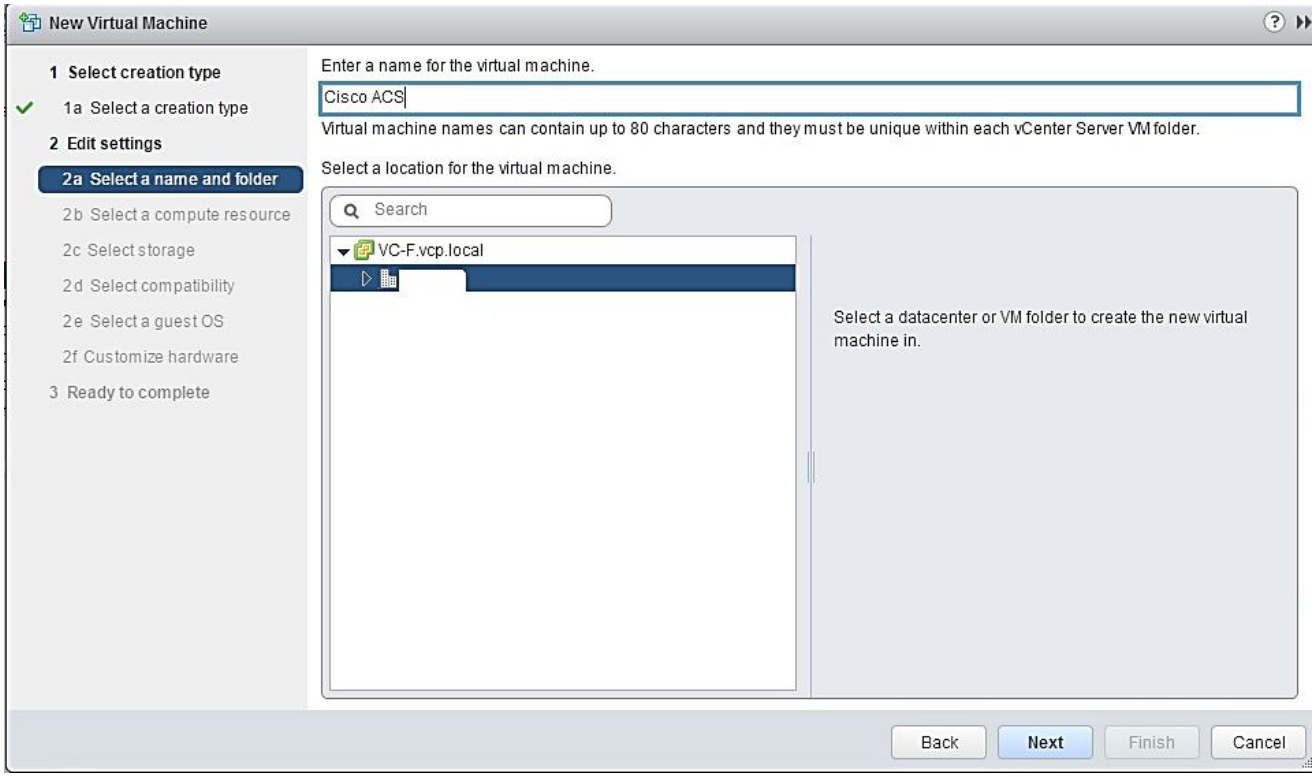
حداقل سیستم مورد نیاز

Requirement Type	Minimum Requirements
CPU	2 CPUs (dual CPU, Xeon, Core2 Duo or 2 single CPUs)
Memory	4 GB RAM
Hard Disk	A minimum of 60 GB is required. Maximum storage is up to 750 GB. **Note** ACS partitions the available disk space automatically during the installation process. **Note** It is recommended that you allocate the hard disk size to be greater than 500 GB for the secondary instance, which acts as a log collector.
NIC (Network Interface Card)	1 Gb dedicated NIC interface
Hypervisor	• VMware ESXi 5.0 • VMware ESXi 5.0 Update 2 • VMware ESXi 5.1 • VMware ESXi 5.5 • VMware ESXi 5.5 Update 1

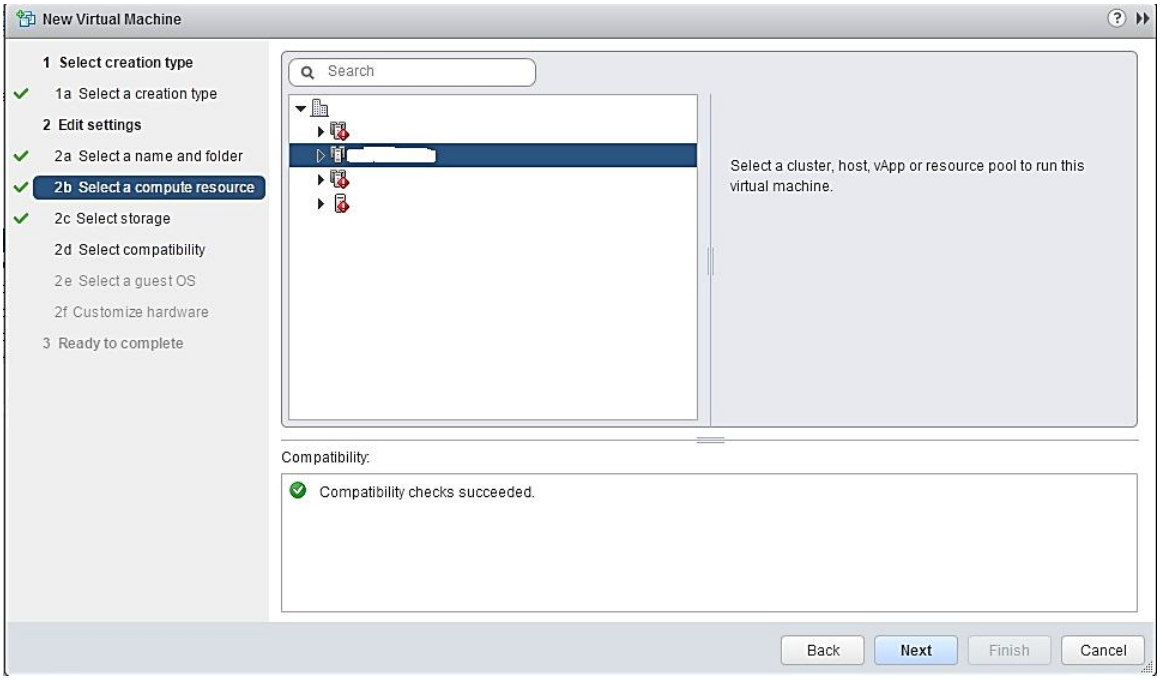
با vCenter، ماشین جدید درست می کنیم:



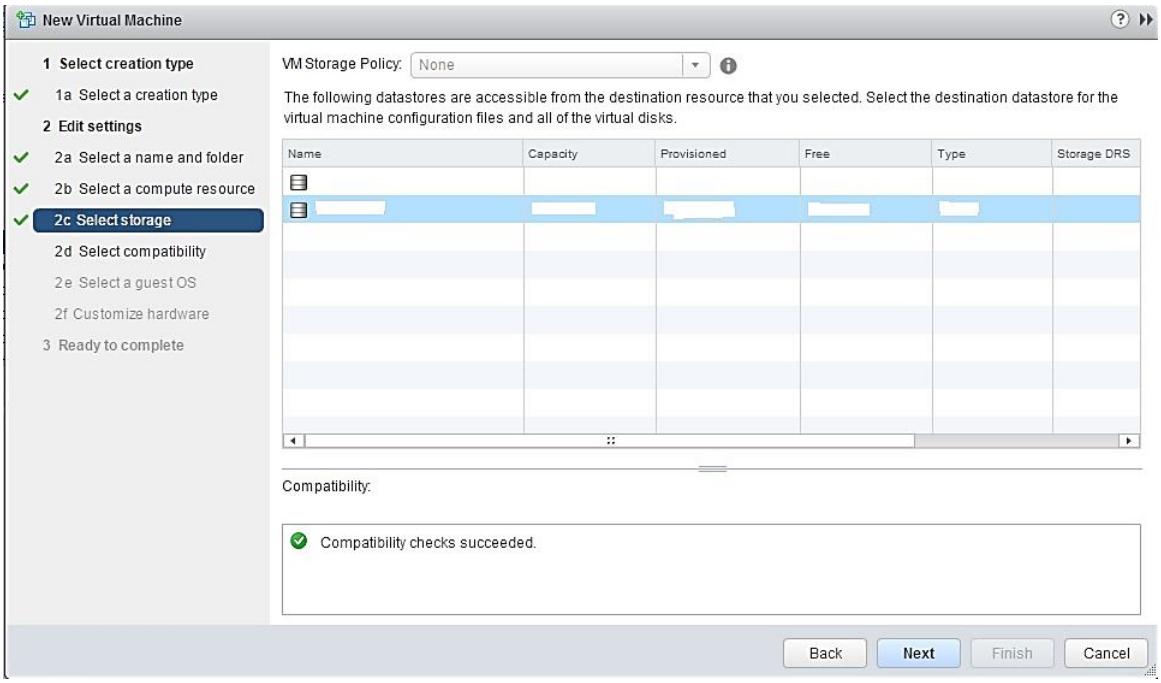
اسمی برای virtual machine انتخاب کنید و محل ذخیره در DataStore مشخص کنید:



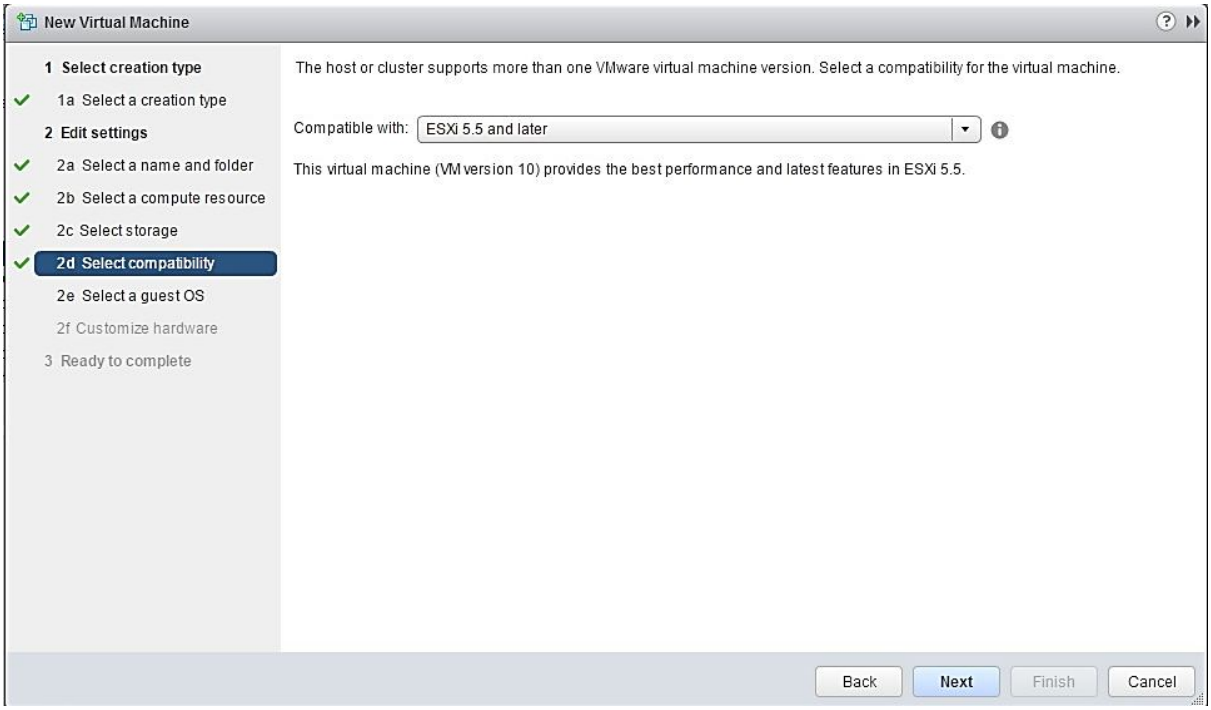
Host ای که باید ماشین در آن جا ذخیره شود مشخص کنید:



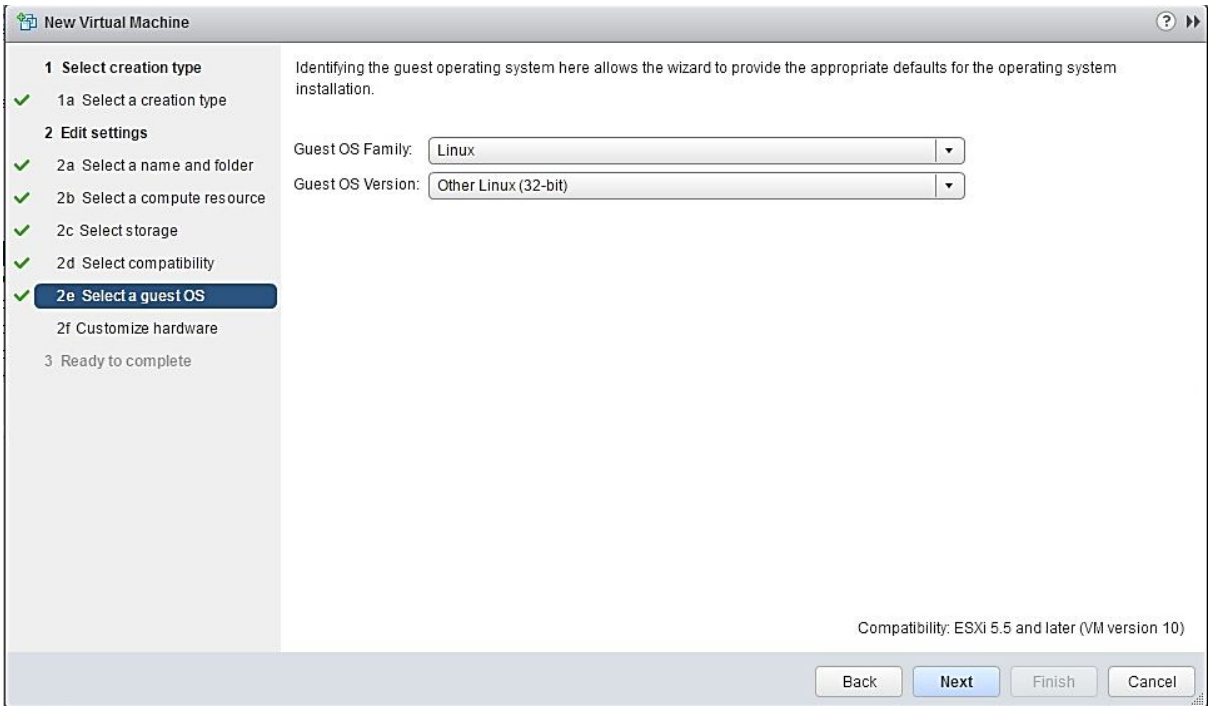
محل ذخیره ماشین مجازی در datastore مشخص شود:



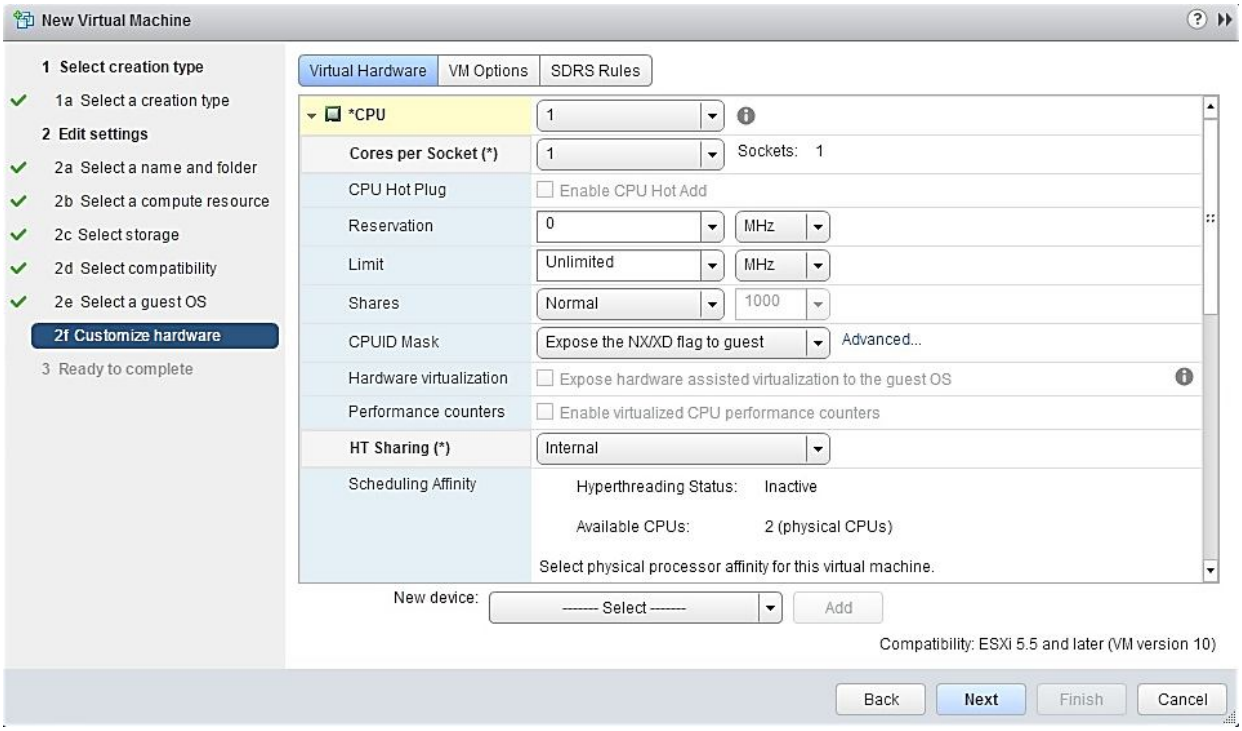
در مرحله ی بعد سازگاری ACS با نسخه ی ESXi را مشخص می شود. طبق جدول بالا از ESXi 5.0 (VM version 8) تا ESXi 5.5 Update 1 (VM version 10) را پشتیبانی می کند. برای سازگاری بیش تر و استفاده بهینه از آخرین نسخه طبق جدول بالا انتخاب کنید.



در این جا نوع سیستم عامل را Linux و نسخه آن را Other Linux (32bit) انتخاب کنید:

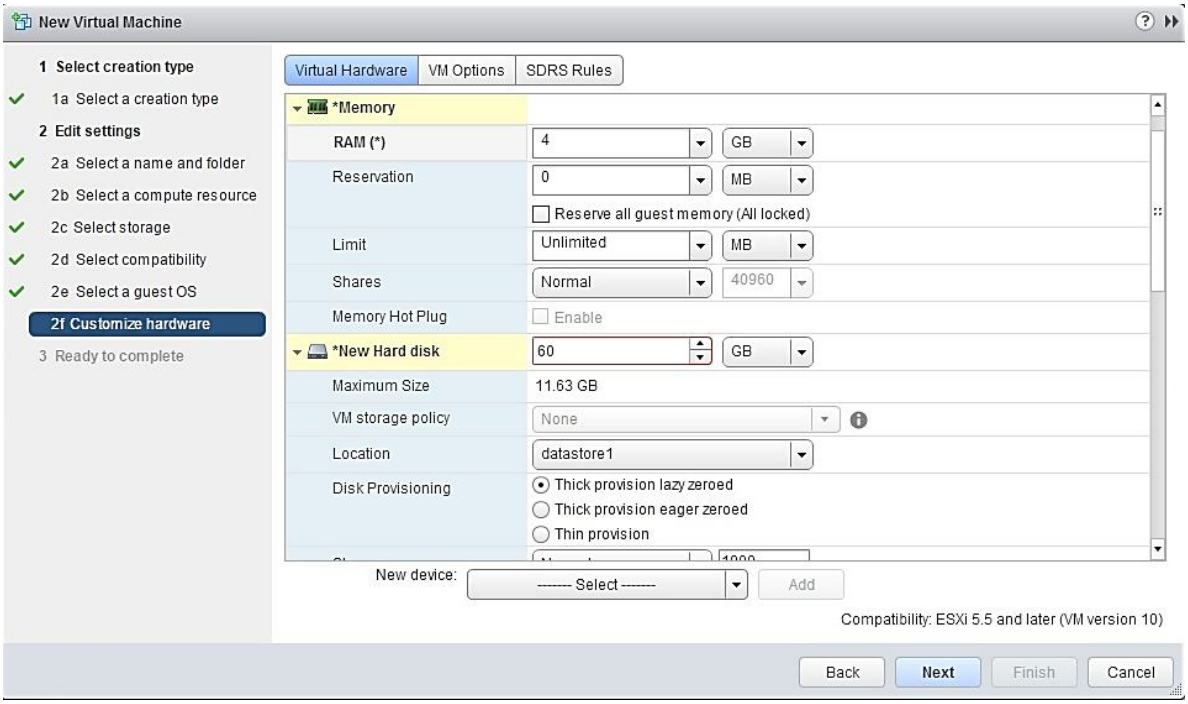


در صفحه ی بعد با تنظیمات تخصیص سخت افزار به ماشین مجازی است؛ در نوار CPU تعداد cpu و core های هر کدام ۱ بدهید و در قسمت HT Sharing، Internal را انتخاب کنید.



در Memory، 4GB رم اختصاص دهید و میزان فضای Hard را 60 GB دهید و نوع Disk Provisioning را Thick provision lazy zeroed انتخاب کنید.

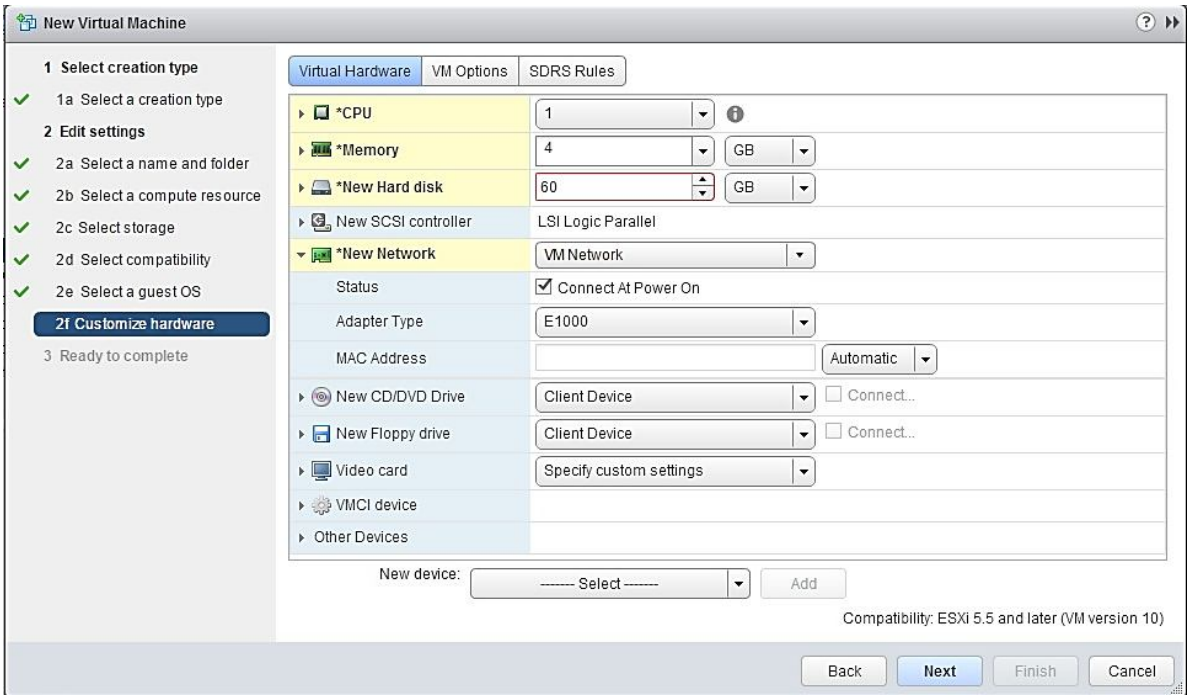
نکته: به هیچ عنوان نوع Disk Provisioning را Thin Provision انتخاب نکنید زیرا ACS پشتیبانی نمی کند. هر چند می توانید در حالت Thick Provision eager zeroed قرار دهید و Performance بسیار خوبی بگیرید.



در Network از تیک Connect at Power on مطمئن باشید و نوع Adapter را E1000 انتخاب کنید.

نکته: ACS هیچ یک از آداپتورهای VMXNET2 (Enhance) و VMXNET3 را پشتیبانی نمی کند.

نکته: ACS تا 4 NIC را پشتیبانی می کند. می توانید در پایین صفحه از قسمت New Device گزینه ی Network را انتخاب کنید.



و در پایان CD\DVD Drive را فایل ایمیج ACS انتخاب کنید. انتخاب این که فایل در datastore ذخیره کنید و یا از Host مربوط به سرور و یا پیدا کردن ایمیج از Client به انتخاب شما بستگی دارد.

کار با Cisco ACS

پیش نیاز

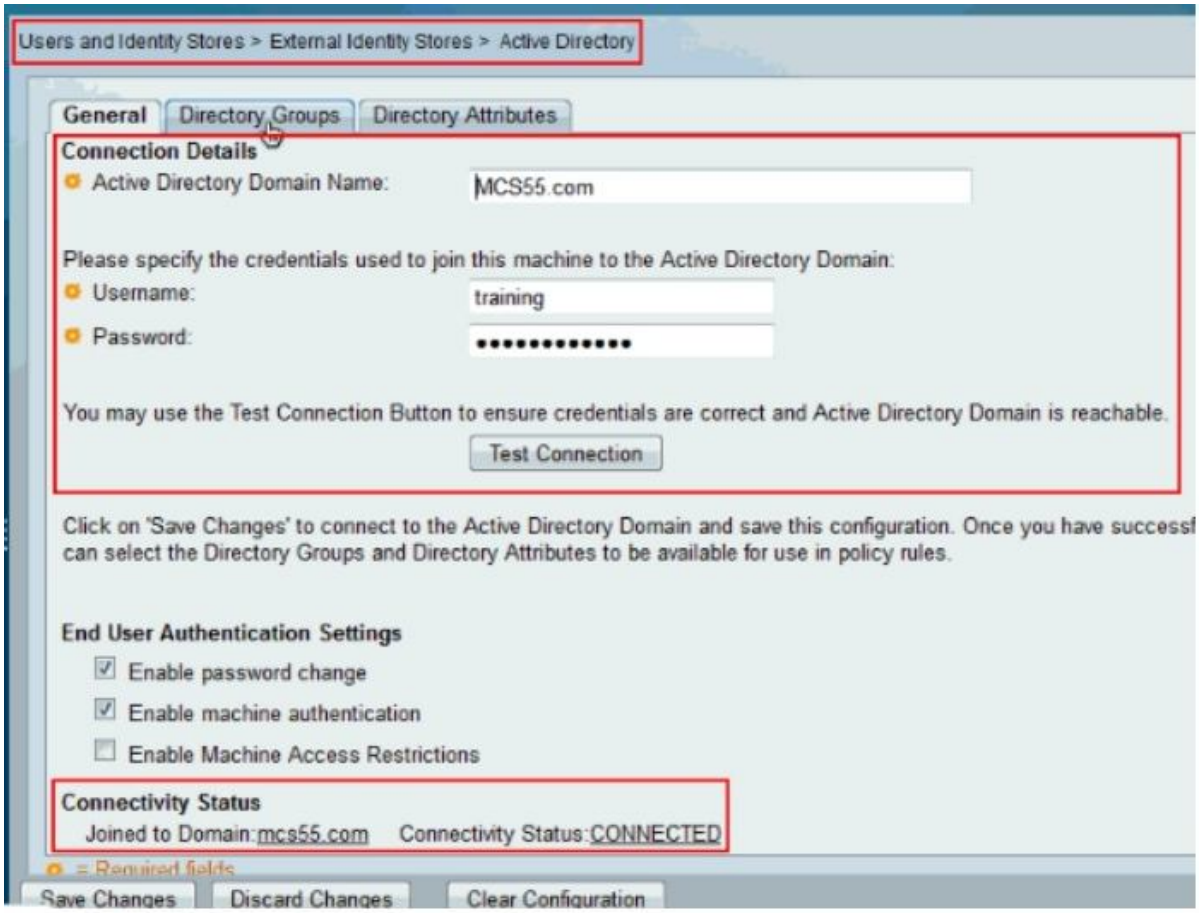
ACS 5.x کاملا با Active Directory ویندوز وابسته است. قبل از کار با ACS، کاربران مورد نظر در Active Directory تعریف شوند.

حداقل سیستم های قابل استفاده:

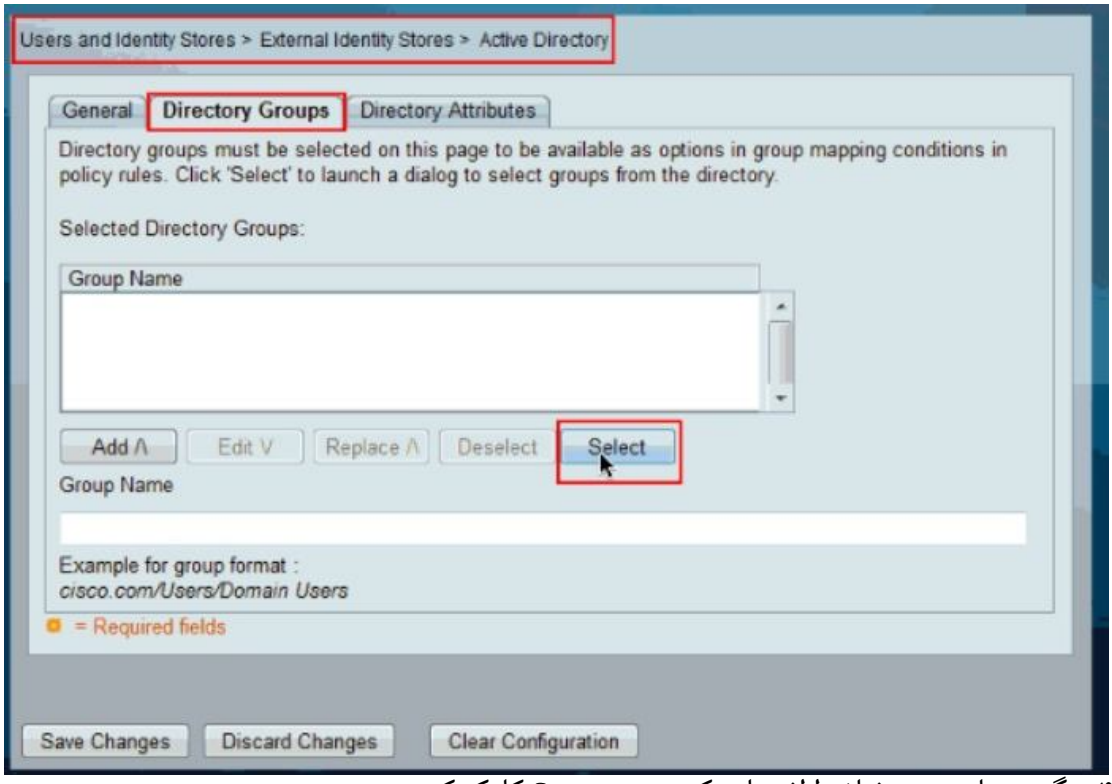
- Cisco Secure ACS 5.3
- Microsoft Windows Server 2003 Domain

در درجه اول User ها در Active Directory را به ACS معرفی می کنیم. ما دو User با سطح دسترسی متفاوت –یکی به عنوان Admin و دیگری برای پشتیبانی شبکه- ایجاد می کنیم:

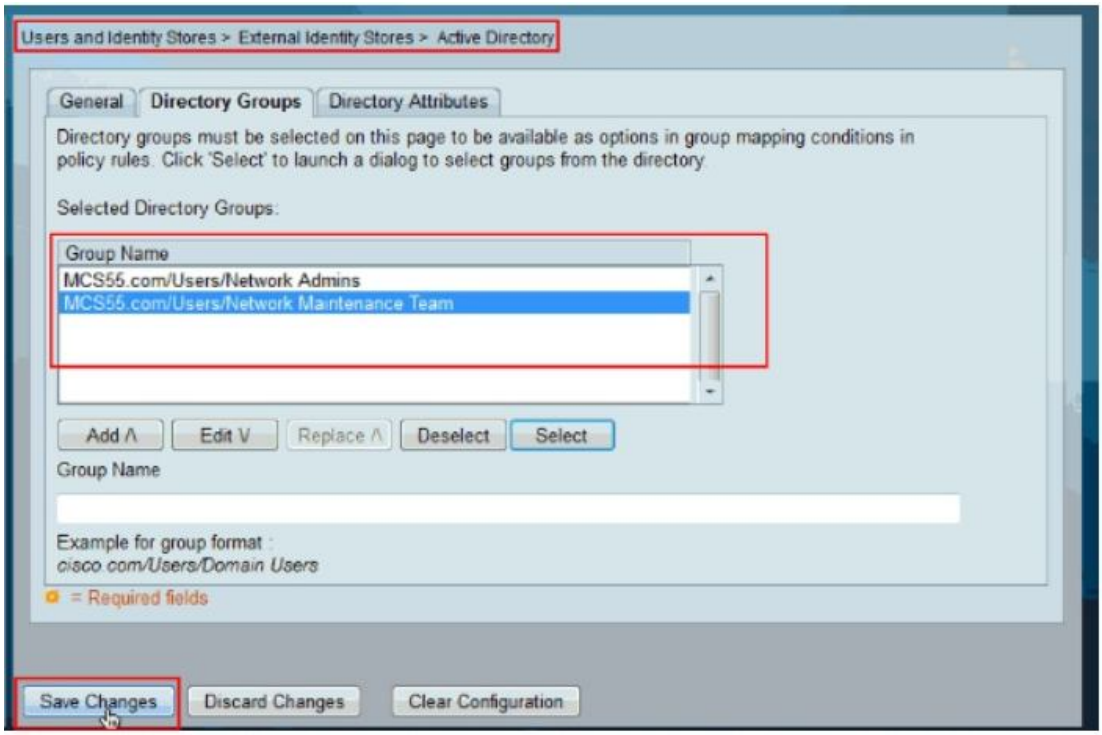
۱. با کاربری Admin به ACS GUI وارد شوید.
۲. **Users and Identity Stores > External Identity Stores > Active Directory** را انتخاب کنید و پس از وارد کردن Active Directory Domain Name و نام کاربری و رمز عبور، از صحت اتصال به Domain مورد نظر اطمینان حاصل کنید.



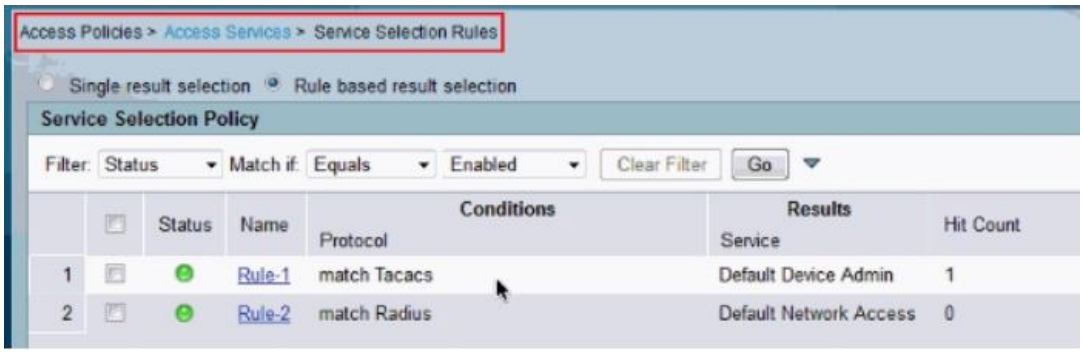
۳. بر تب **Directory Group** کلیک کنید و **Select** را انتخاب کنید.



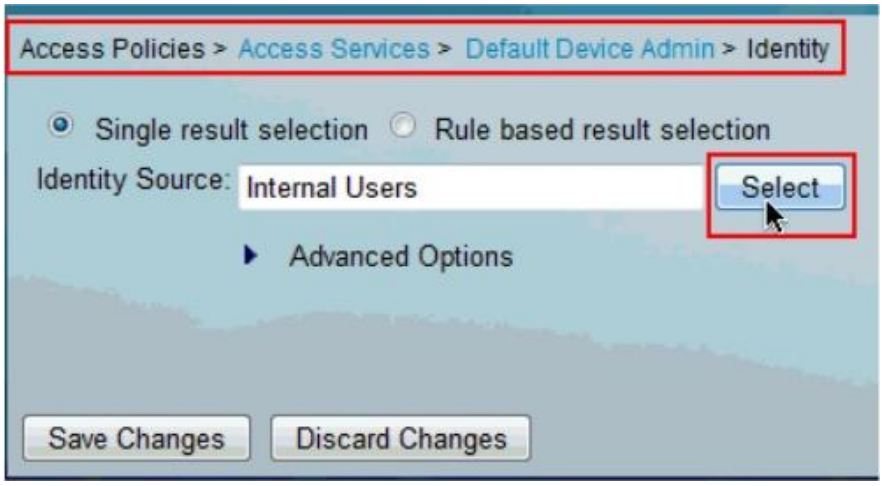
۴. گروه های مورد نیاز را انتخاب کنید. و بر **Save** کلیک کنید.

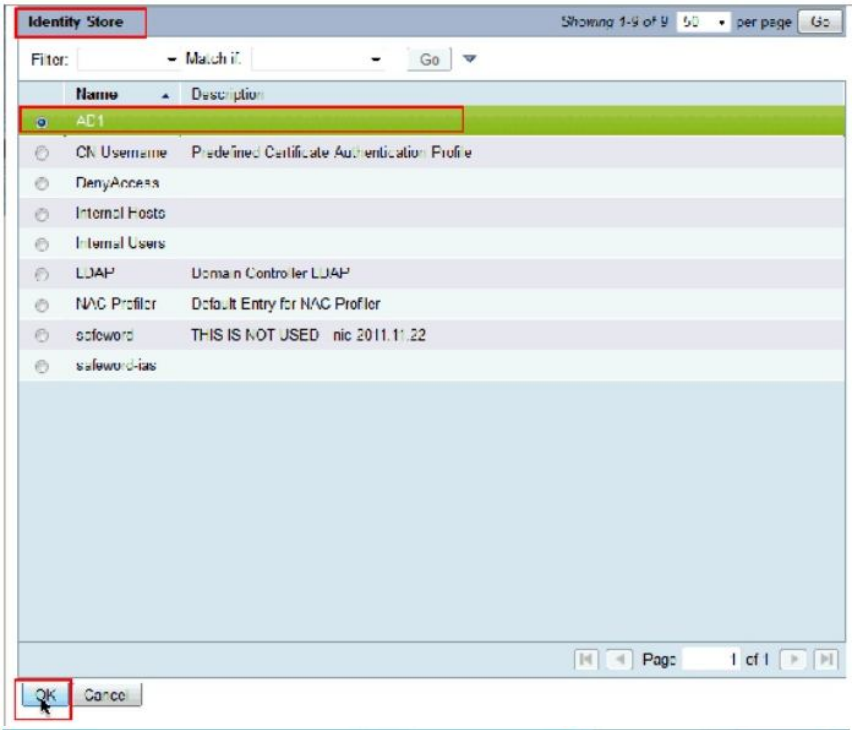


۵. **Access Policies > Access Services > Service Selection Rules** بروید و نوع access service خود را پیدا کنید. در این مقاله از +TACACS استفاده می شود که از نوع **Default Device Admin** است.

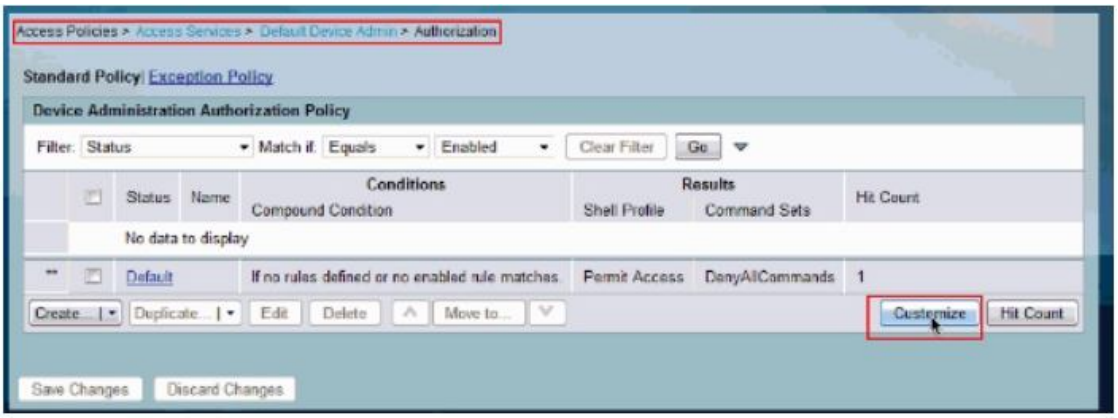


۶. **Access Policies > Access Services > Default Device Admin > Identity** را انتخاب کنید و در **Identify Source**، **AD1** را انتخاب کنید. و **Save** کنید.

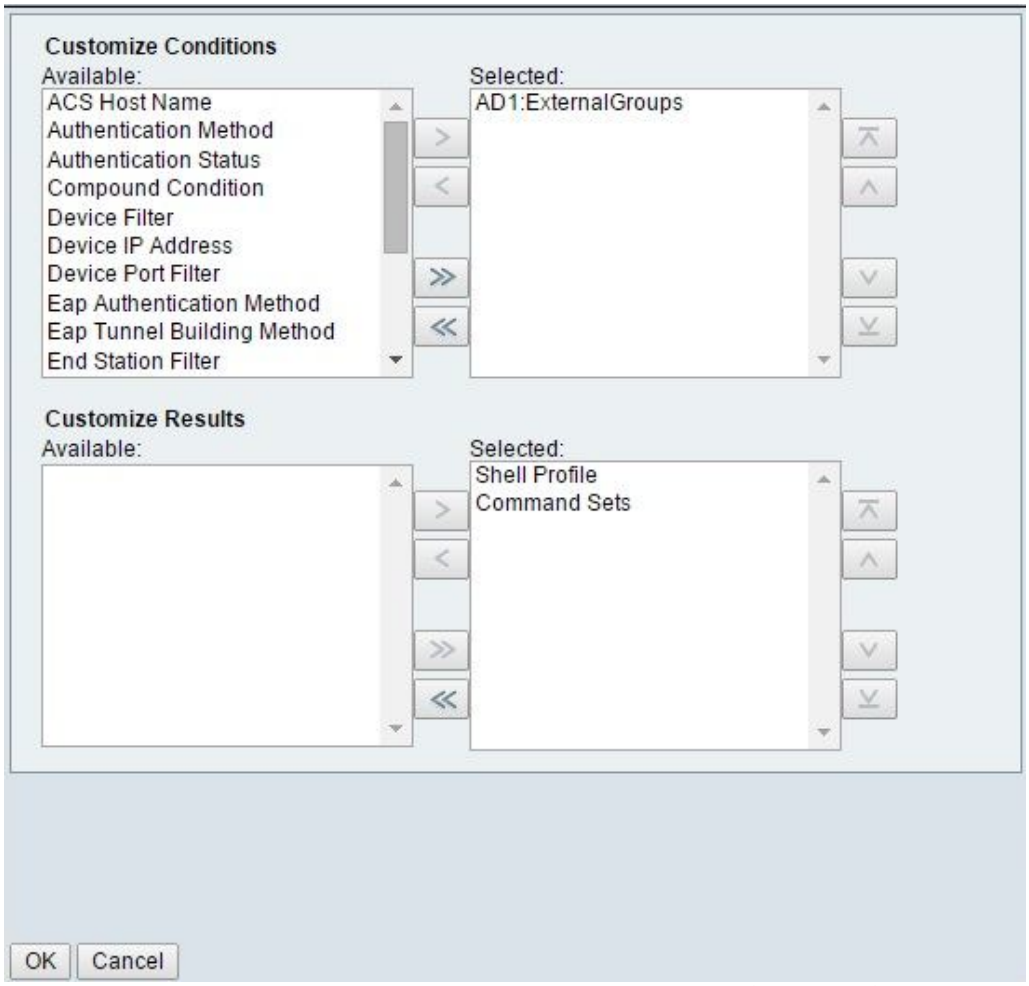




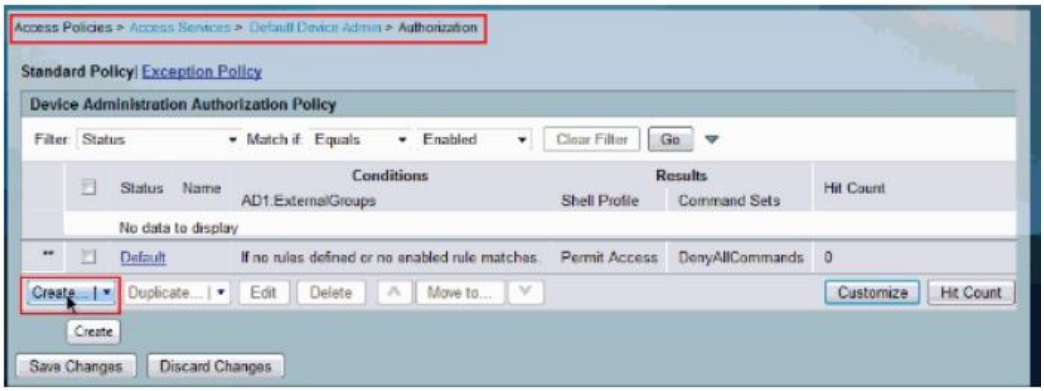
۷. **Access Policies > Access Services > Default Device Admin > Authorization** را انتخاب کنید و بر **Customize** کلیک کنید.



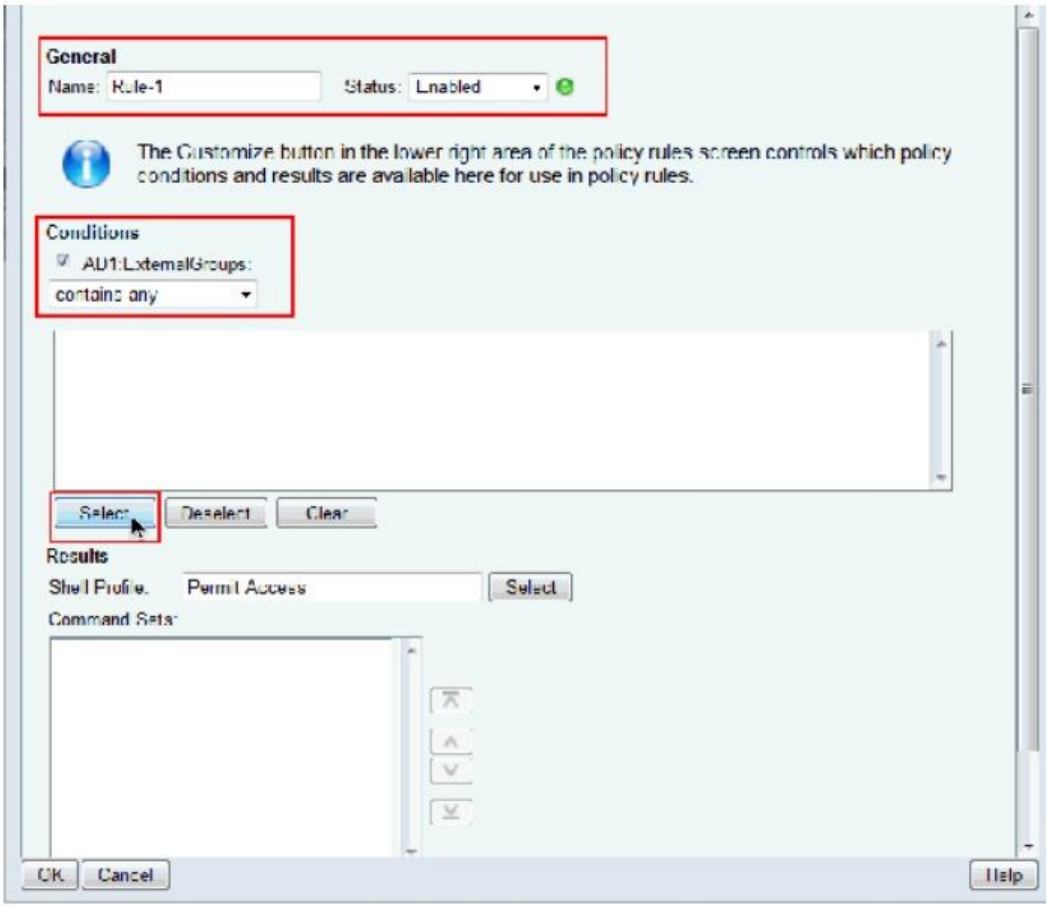
۸. در بخش **Customize Conditions**، **AD1:ExternalGroups** و از بخش **Customize Results**، **Shell Profile** و **Command Sets** انتخاب کنید.

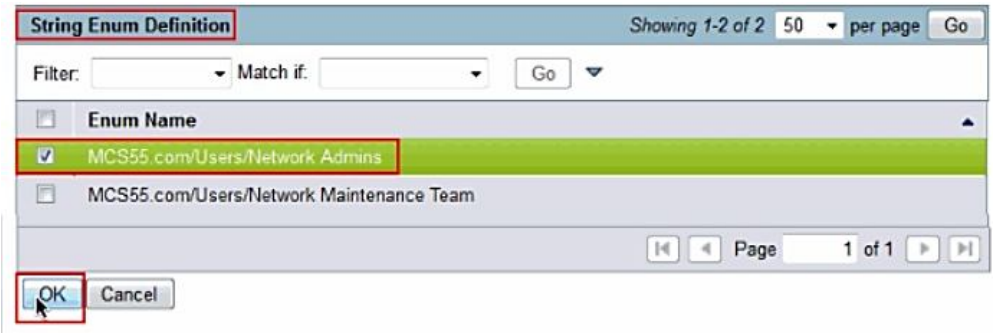


۹. بر روی **Create** کلیک کنید تا **Rule** جدید تعریف کنید.

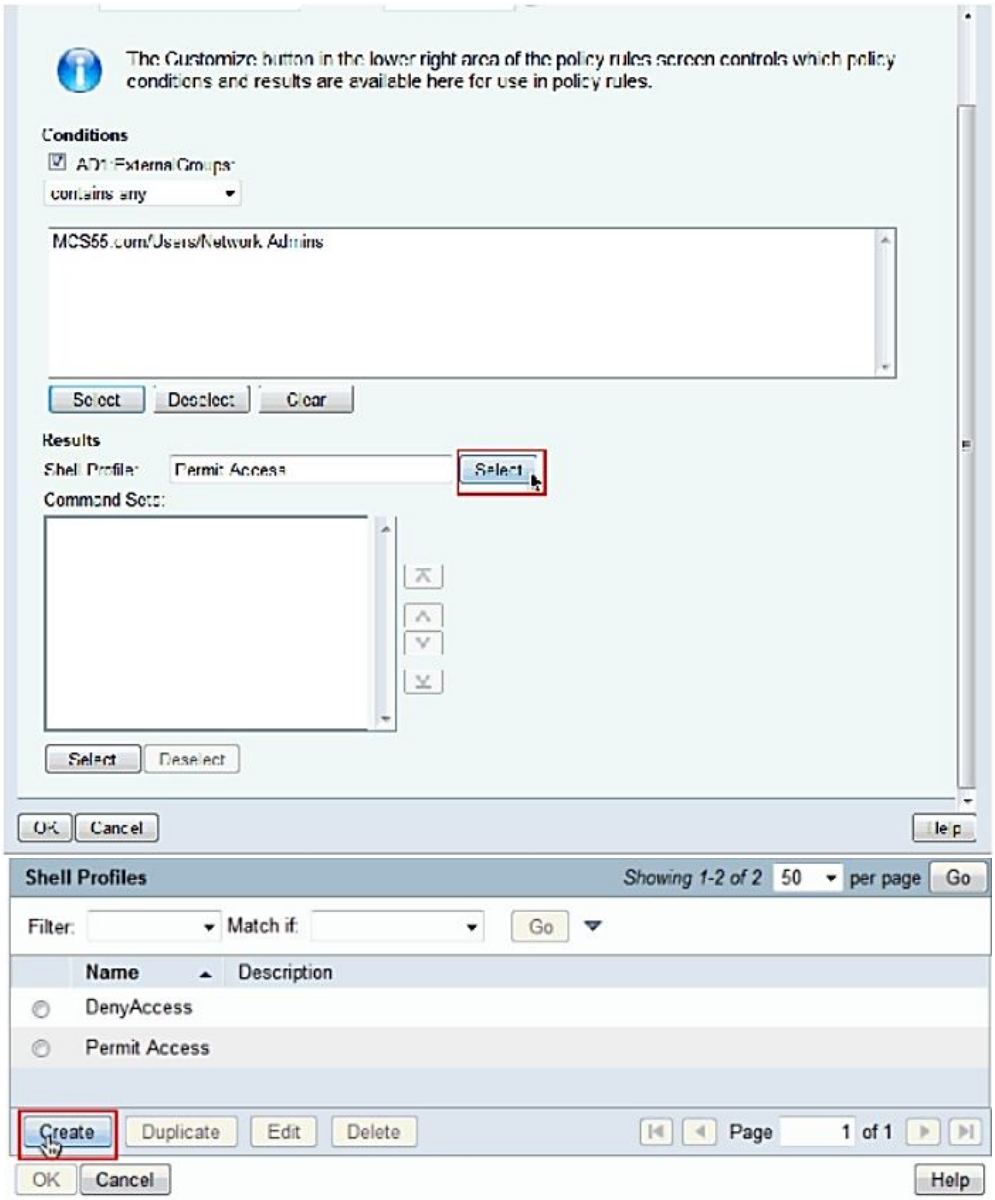


۱۰. در **AD1:ExternalGroups** بر **Select** کلیک کنید و گروهی که باید سطح دسترسی ادمین داشته باشند را انتخاب کنید.



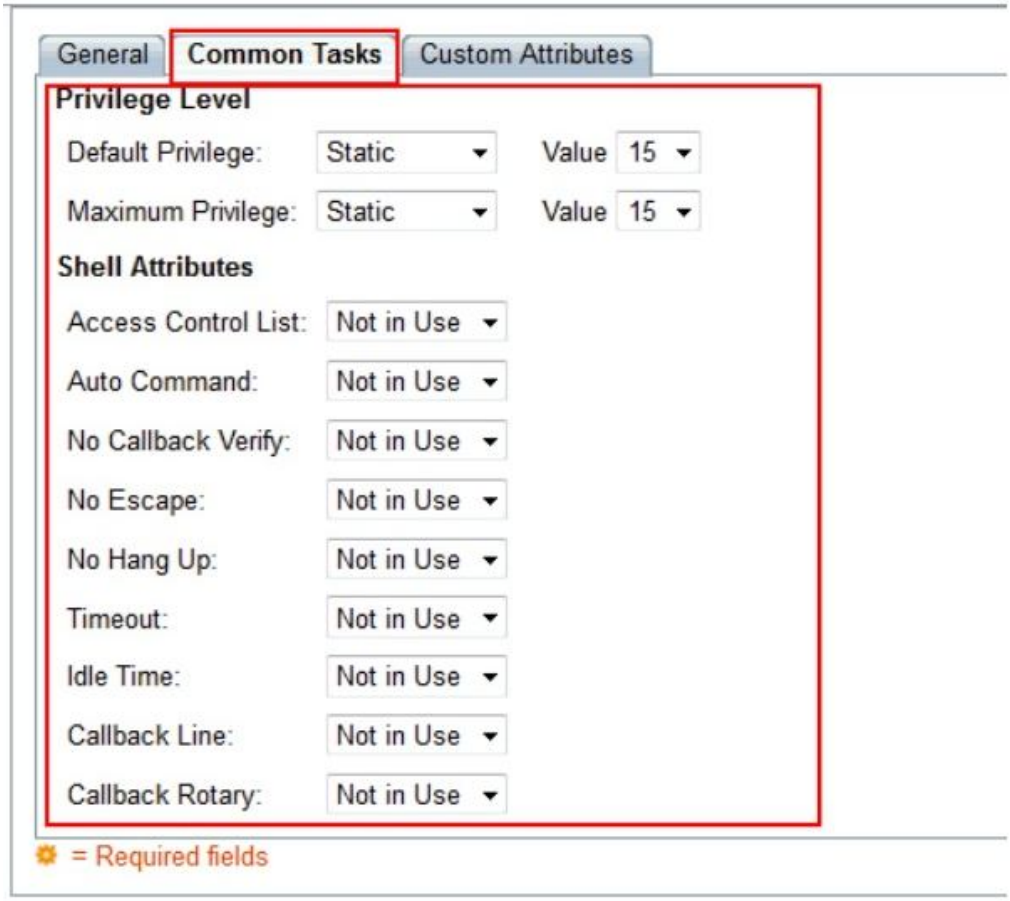


۱۱. در **Shell profile** بر روی **Select** کلیک کنید و **Create** را برای گروه ادمین انتخاب کنید.

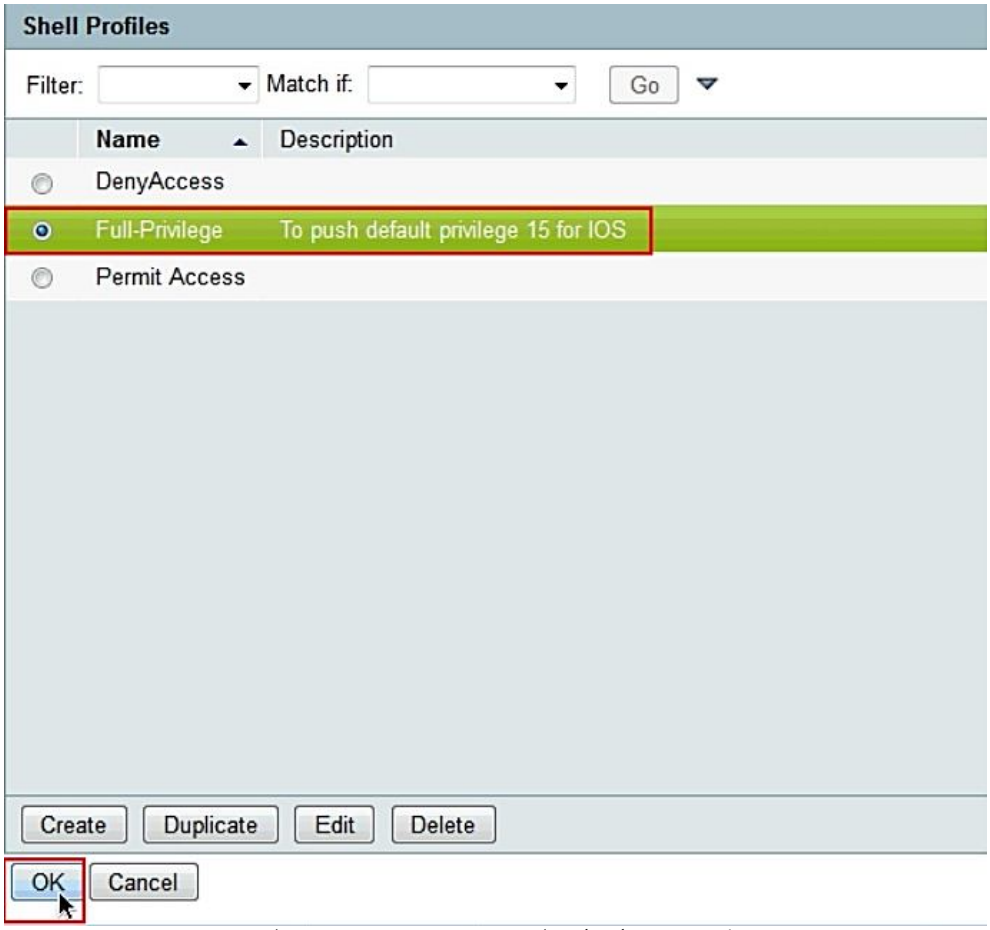


۱۲. در **General Tab** اسم انتخاب کنید و حتما در فیلد **Description** بنویسید. (**Description** می تواند در بسیاری از مواقع بالاخص در مشکلات شبکه و هم چنین برای تولید Document شبکه و ... کمک شایانی می کند.)

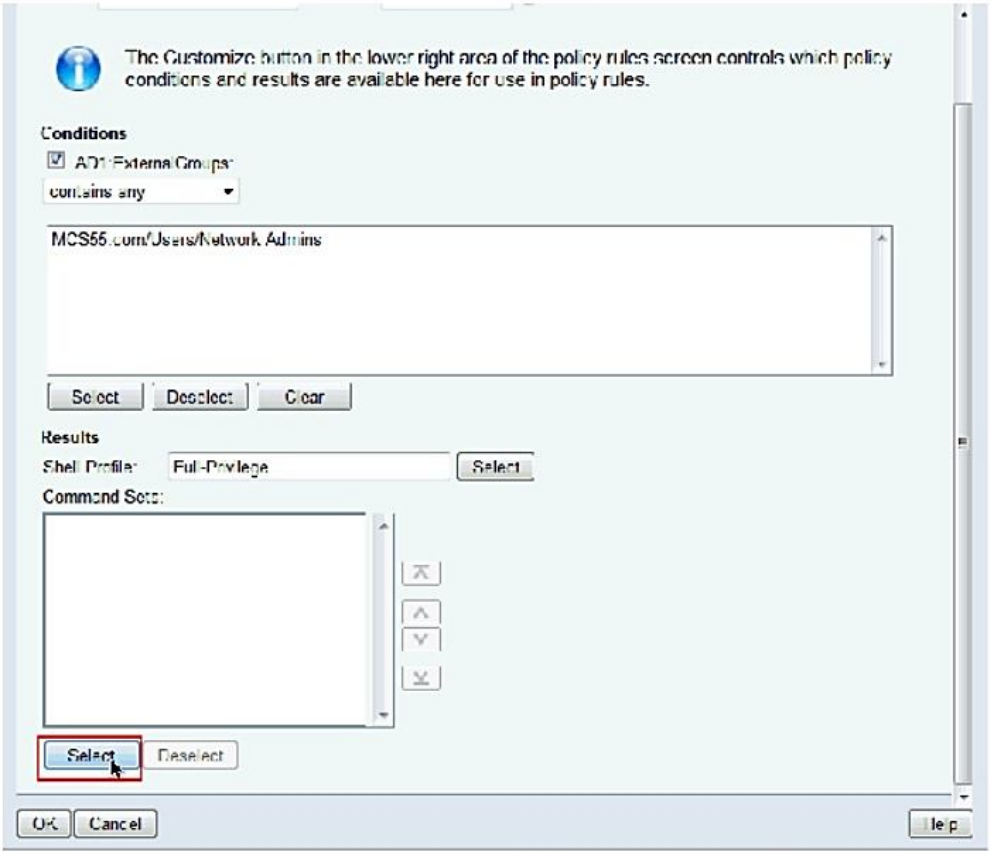
۱۳. بر تب **Common Tasks** کلیک کنید و در قسمت **Privilege Level** به علت سطح دسترسی بالا به گروه ادمین شبکه، **Default Privilege** و **Maximum Privilege** را با **Value** ۱۵ انتخاب کنید.

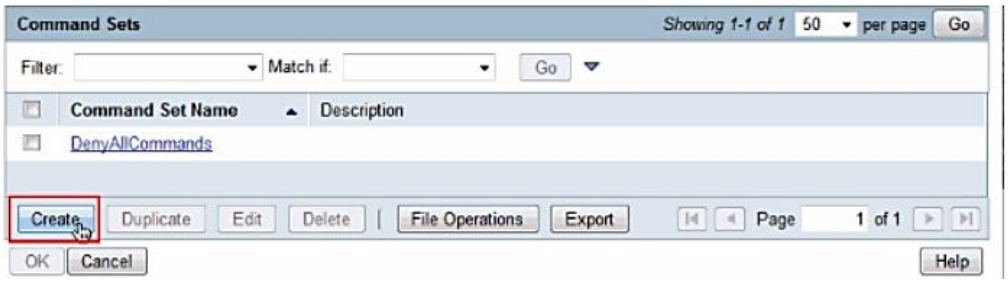


۱۴. سپس آن اسم را انتخاب کنید و بر **OK** کلیک کنید.

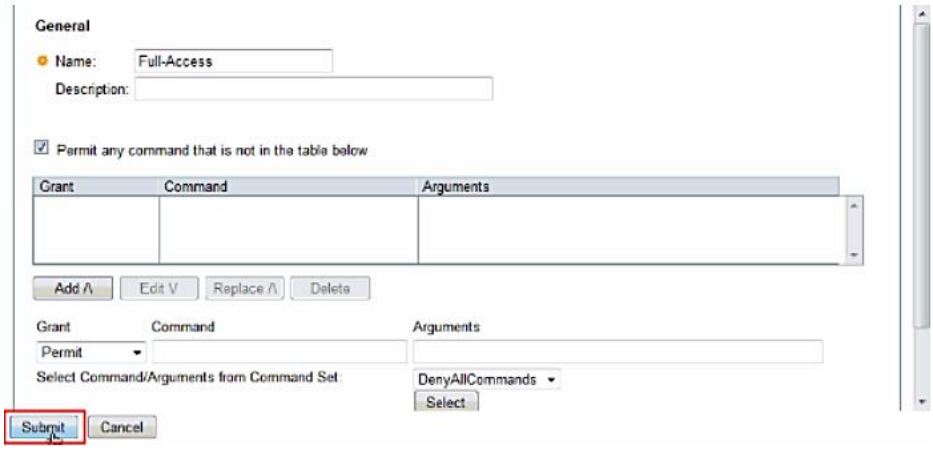


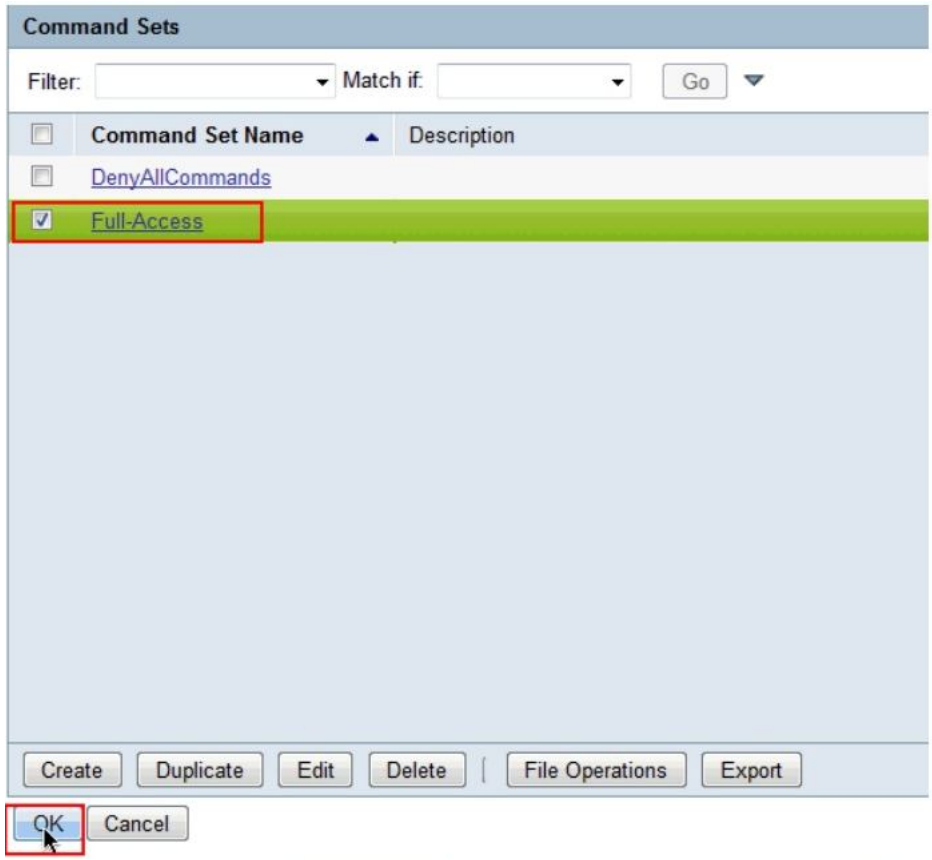
۱۵. در **Command Set**، **Select** کنید و برای ایجاد مجوز **Command** های **Cisco IOS** بر **Create** کلیک کنید.

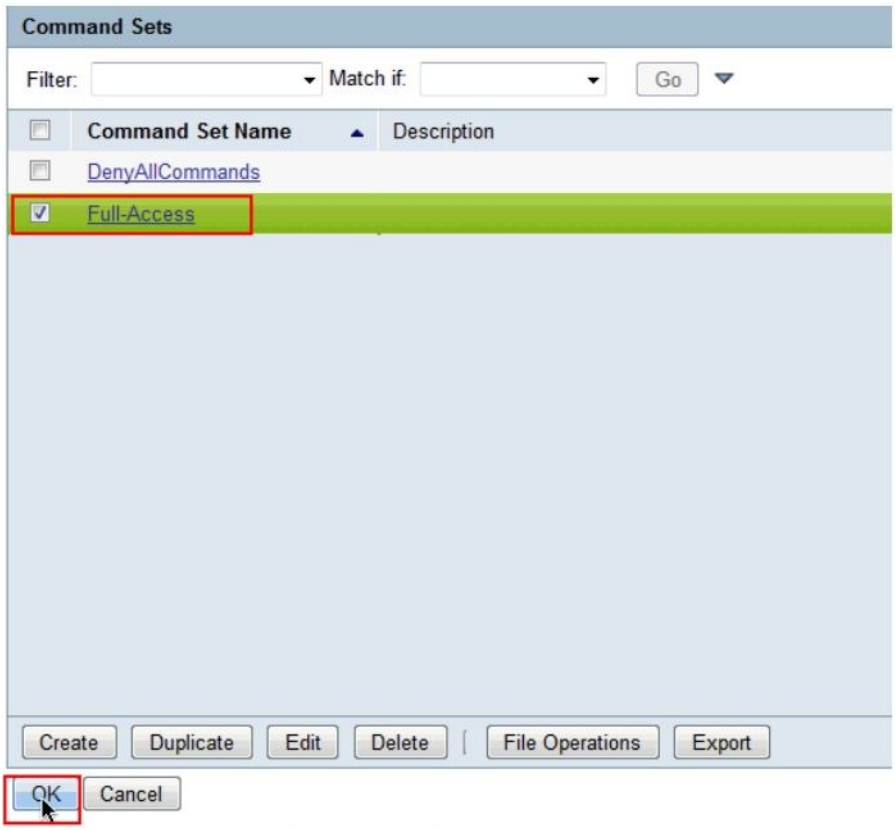




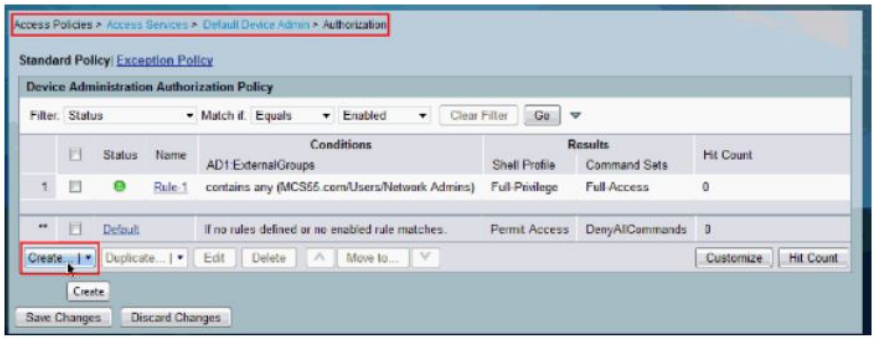
۱۶. در General اسم انتخاب کنید و حتما در فیلد Description بنویسید. مطمئن باشید که تیک Permit any command that is not in the table below باشد و بر Submit کلیک کنید.


General
Name:
Full-Access
Description:
Permit any command that is not in the table below
Grant
Command
Arguments
Add
Edit
Replace
Delete
Grant
Command
Arguments
Permit
Select Command/Arguments from Command Set:
DenyAllCommands
Select
Submit
Cancel

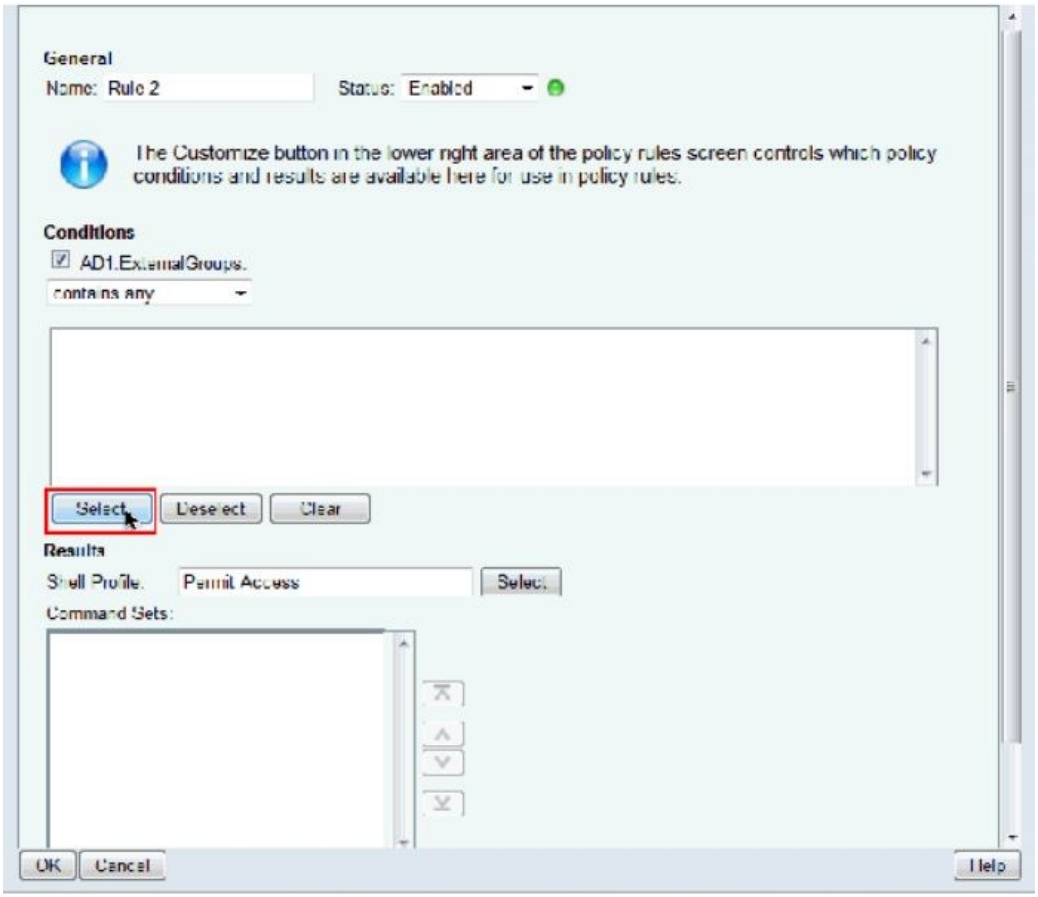

Command Sets
Filter:
Match if:
Go
Command Set Name
Description
DenyAllCommands
Full-Access
Create
Duplicate
Edit
Delete
File Operations
Export
OK
Cancel

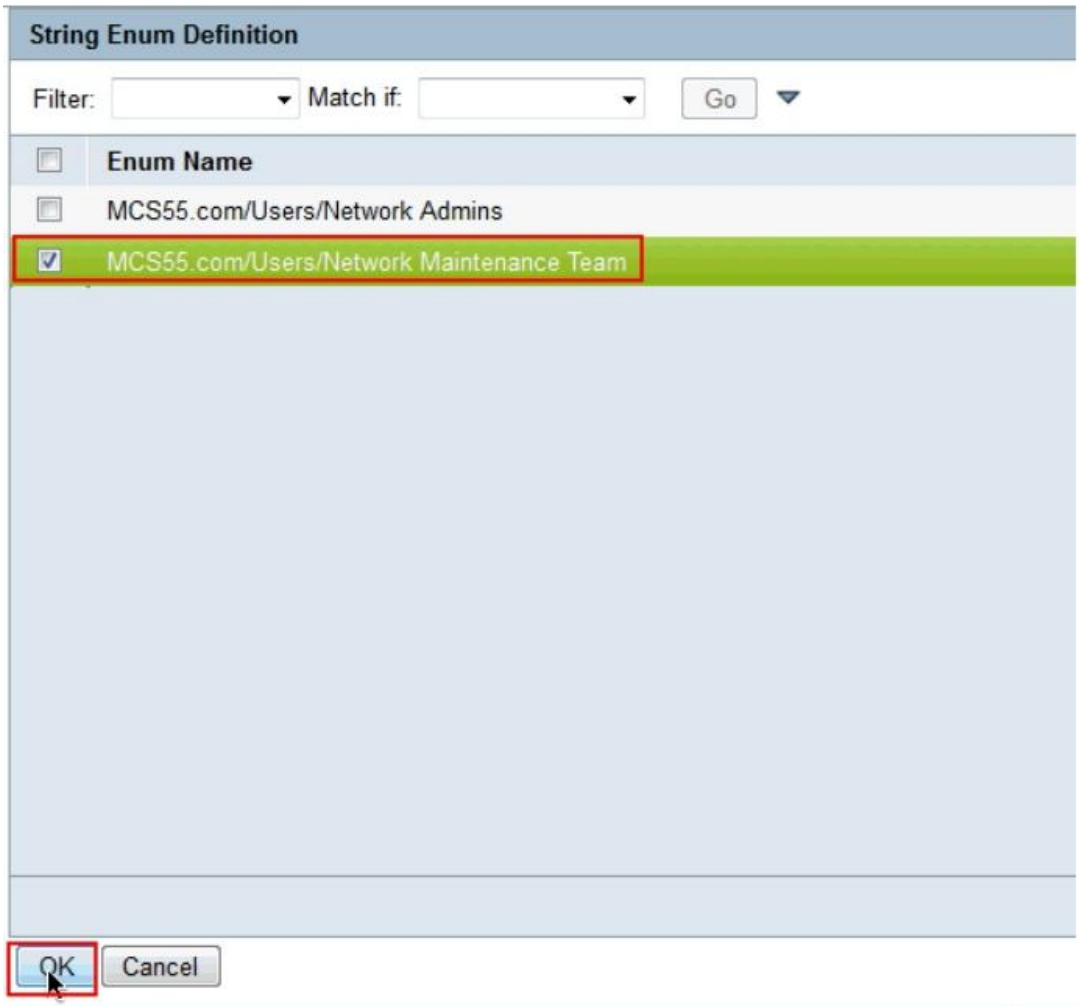


۱۷. حال در این قسمت برای گروه پشتیبانی **Rule** جدید تعریف کنید.

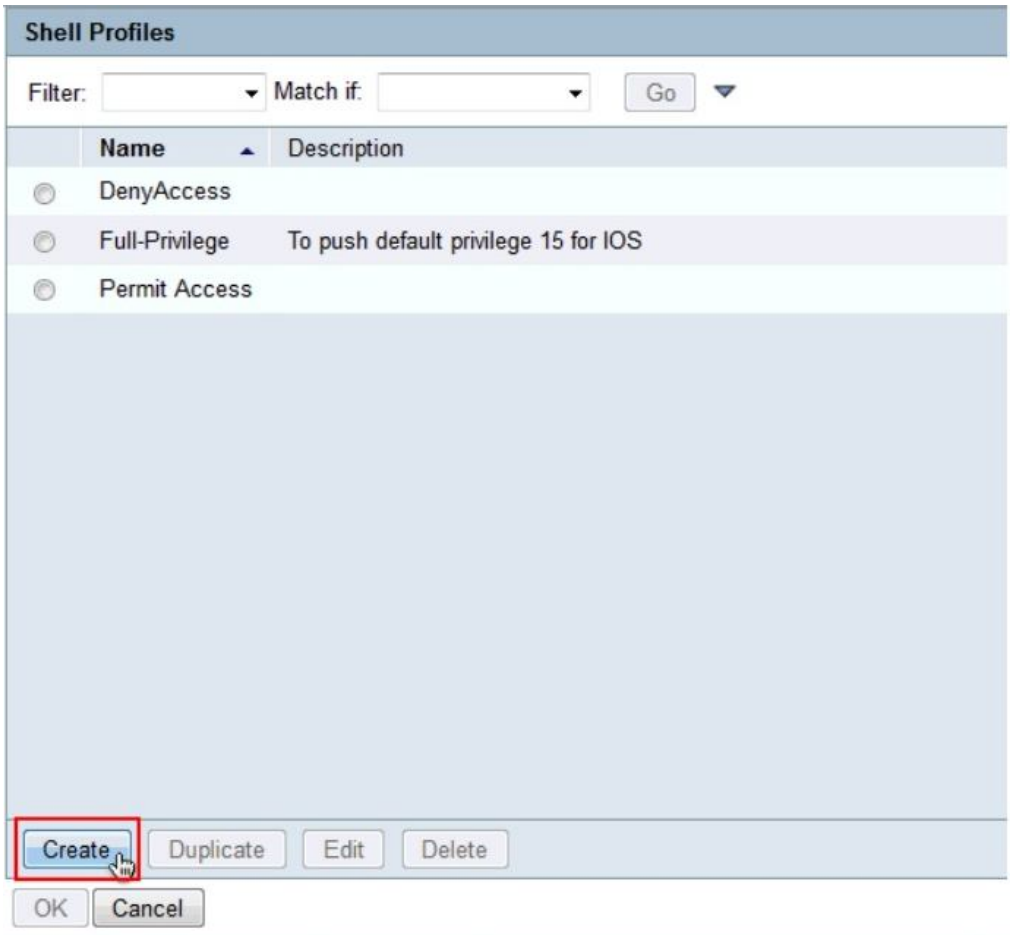


۱۸. در **AD1:ExternalGroups** بر **Select** کلیک کنید و گروهی که باید سطح دسترسی پشتیبانی داشته باشند را انتخاب کنید.


General
Name: Rule 2
Status: Enabled
The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.
Conditions
AD1.ExternalGroups
contains any
Select
Deselect
Clear
Results
Shell Profile
Permit Access
Select
Command Sets:
OK
Cancel
Help

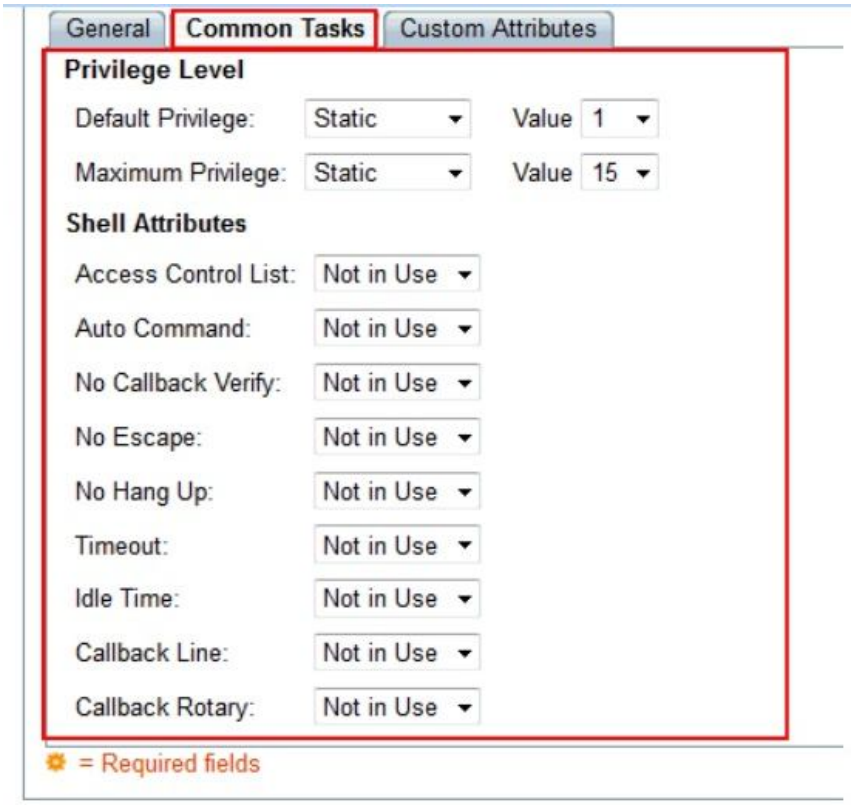


۱۹. در **Shell profile** بر روی **Select** کلیک کنید و **Create** را برای گروه پشتیبانی انتخاب کنید.

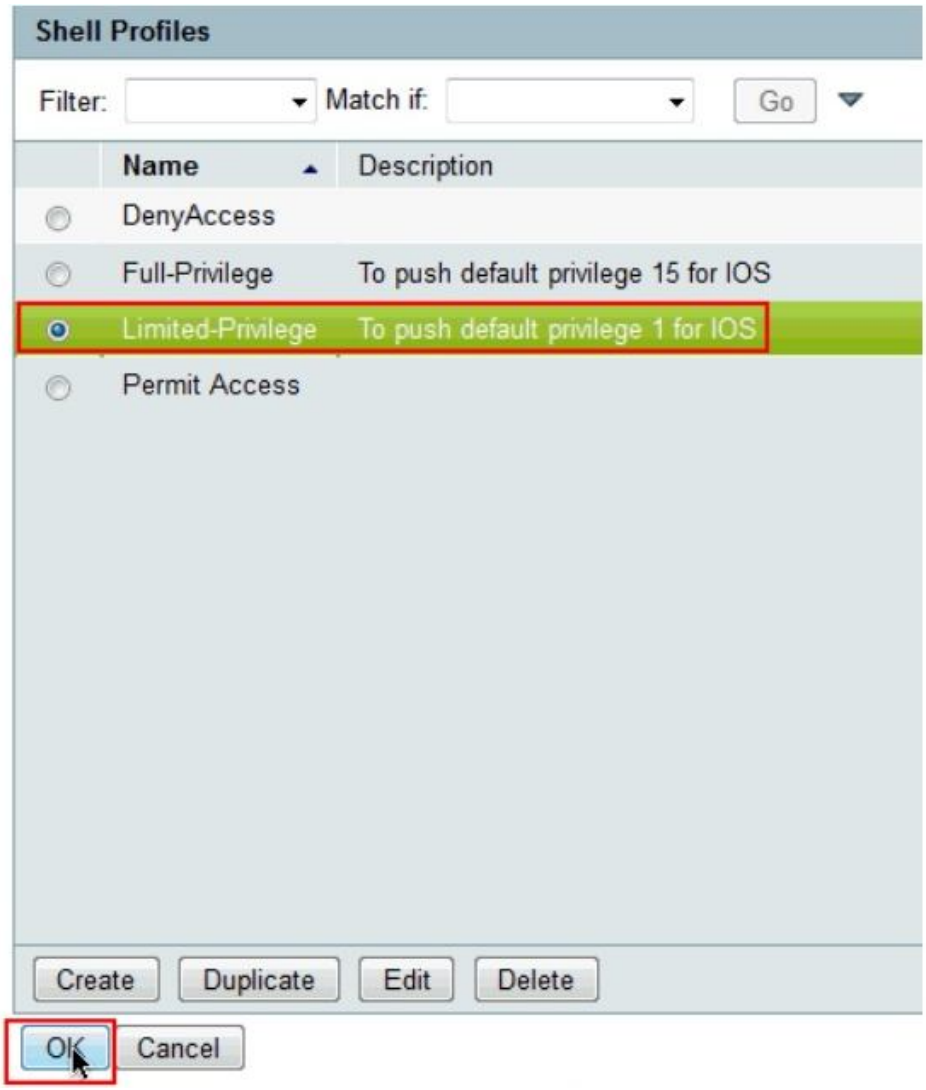


۲۰. در **General Tab** اسم انتخاب کنید و حتما در فیلد **Description** بنویسید.

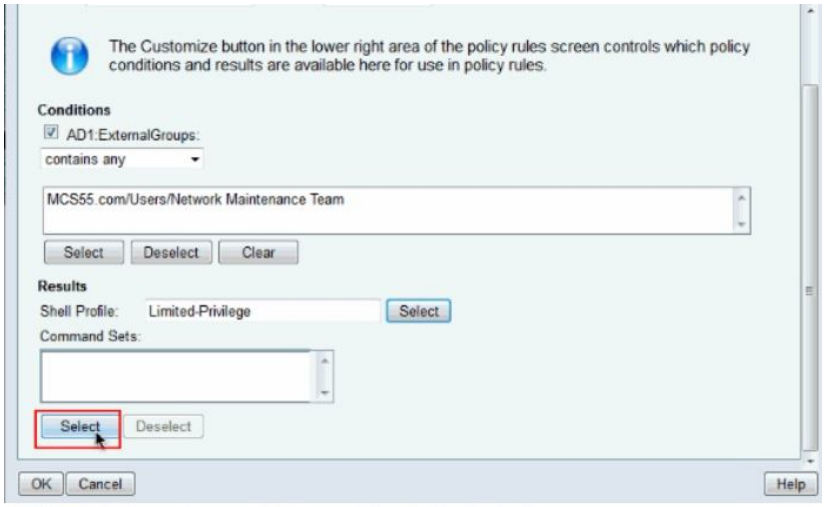
۲۱. بر تب **Common Tasks** کلیک کنید و در قسمت **Privilege Level**، **Default Privilege** و **Maximum Privilege** به ترتیب **Value** ۱ و ۱۵ انتخاب کنید.

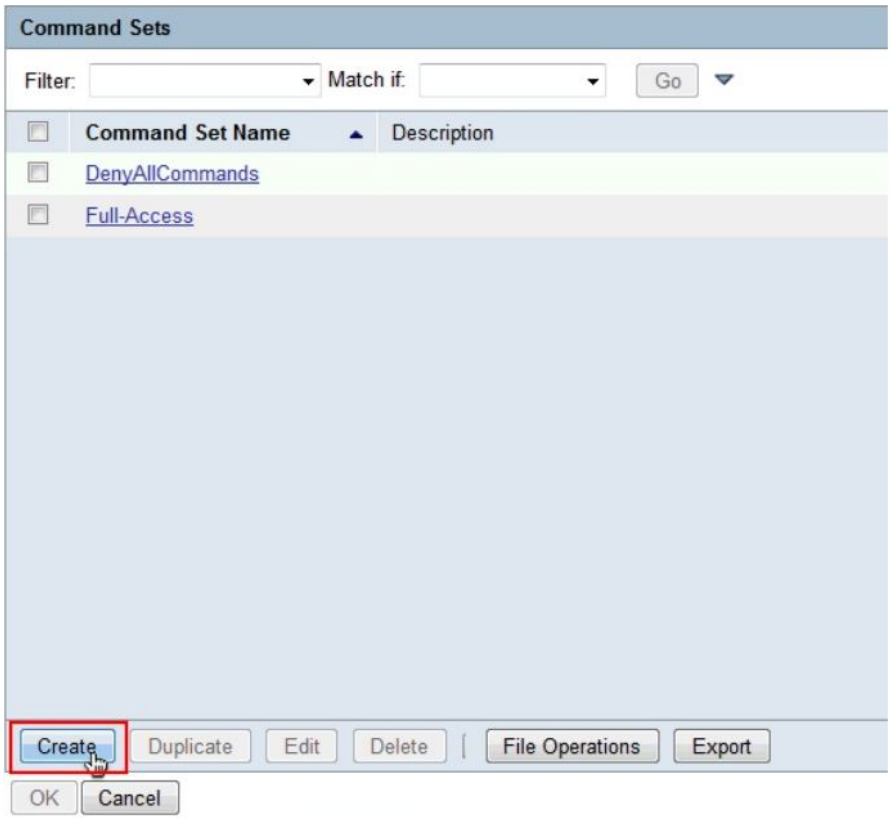


۲۲. سپس آن اسم را انتخاب کنید و بر **OK** کلیک کنید.

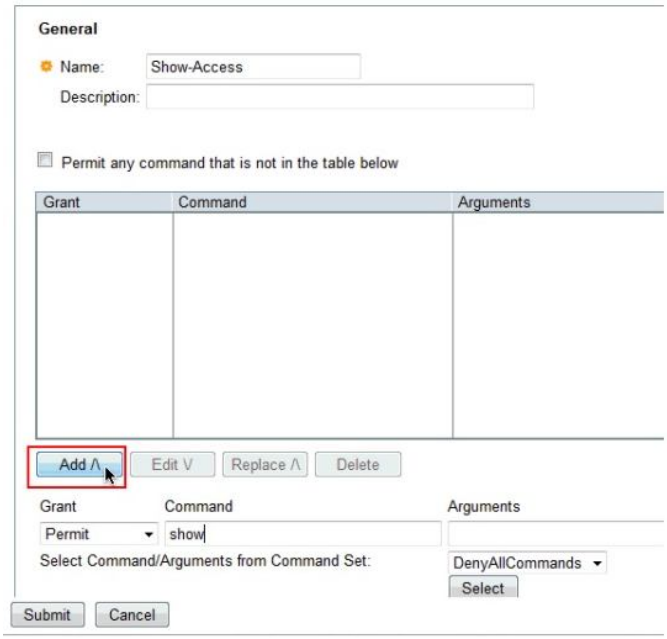


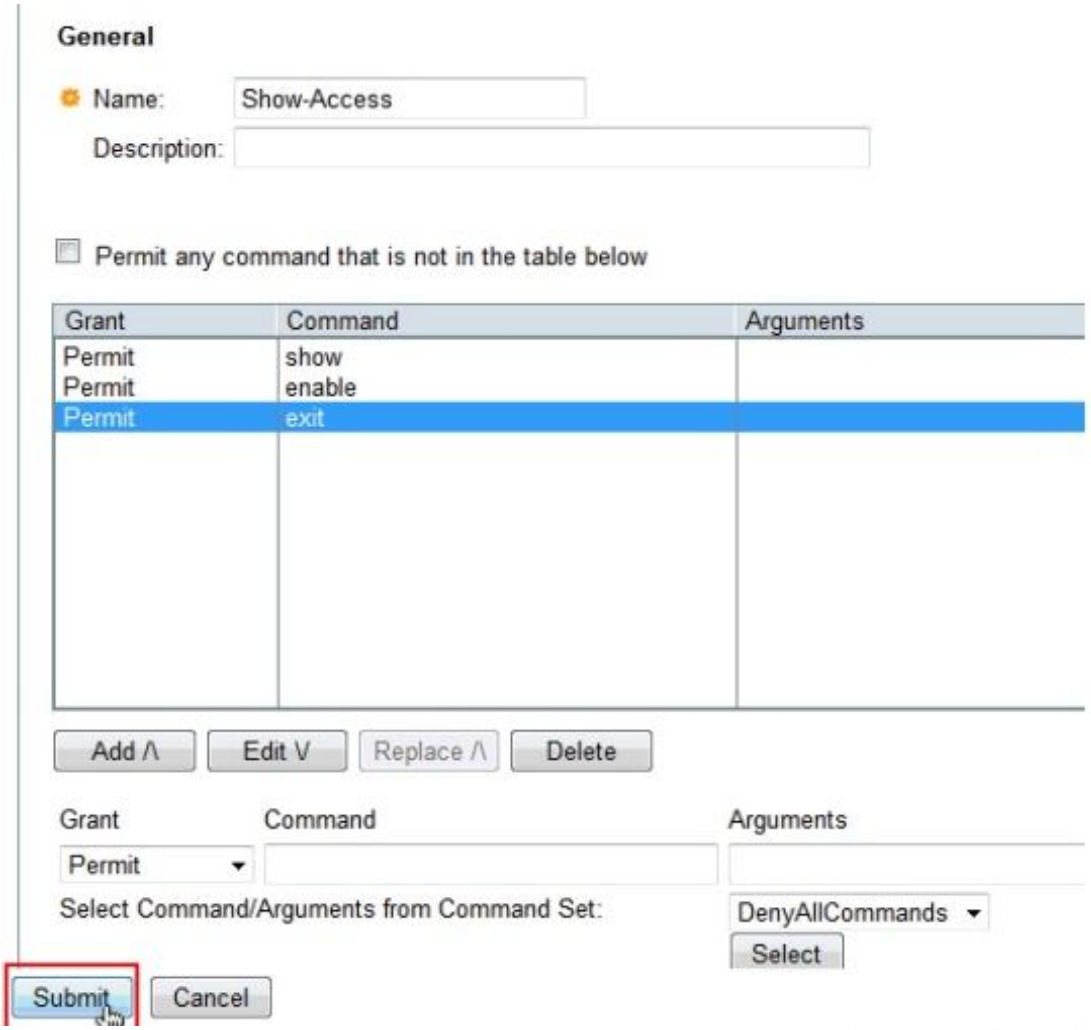
۲۳. در **Command Set**، **Select** کنید و برای ایجاد مجوز **Command** های **Cisco IOS** بر **Create** کلیک کنید.



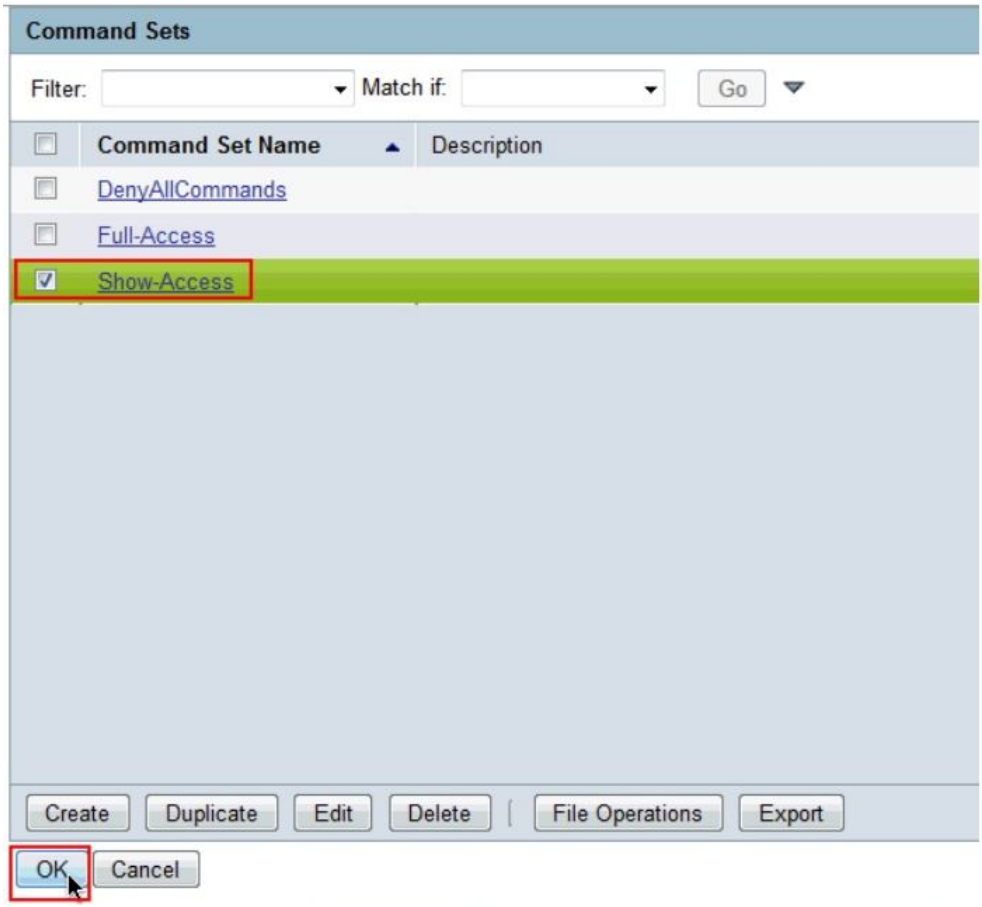


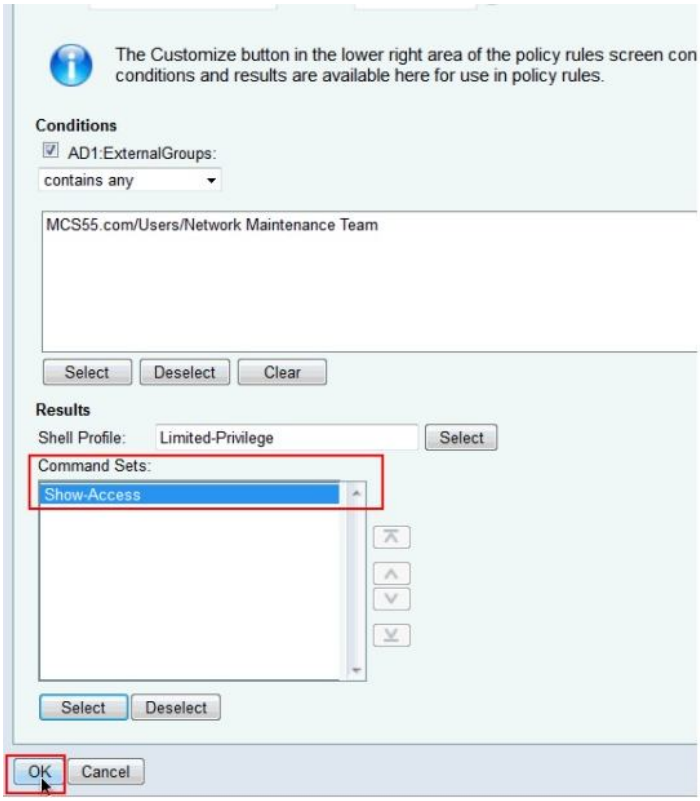
۲۴. در**General** اسم انتخاب کنید و حتما در فیلد **Description** بنویسید. مطمئن باشید که تیک **Permit any command that is not in the table below** نباشد و در **Grant** گزینه ی **Permit** را انتخاب کنید و فیلد **Command** مورد نظر و در صورت مورد نیاز فیلد **Arguments** وارد کنید و در جدول اضافه کنید. در آخر بر **Submit** کلیک کنید.

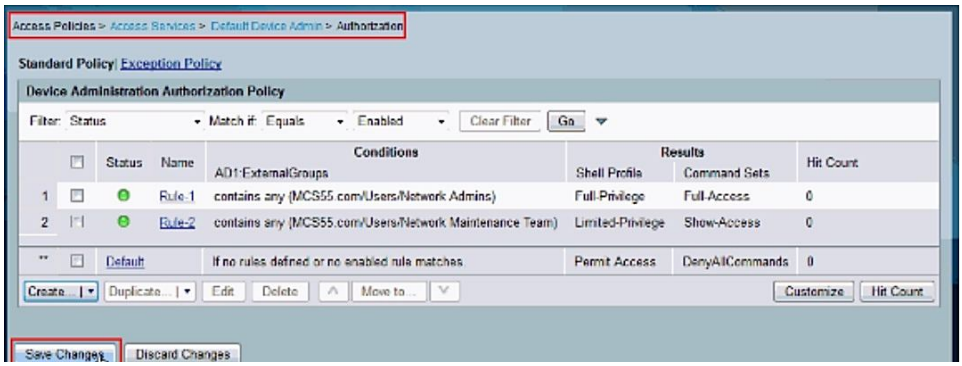

General
Name:
Show-Access
Description:
Permit any command that is not in the table below
Grant
Command
Arguments
Add /\
Edit V
Replace /\
Delete
Grant
Command
Arguments
Permit
show
Select Command/Arguments from Command Set:
DenyAllCommands
Select
Submit
Cancel



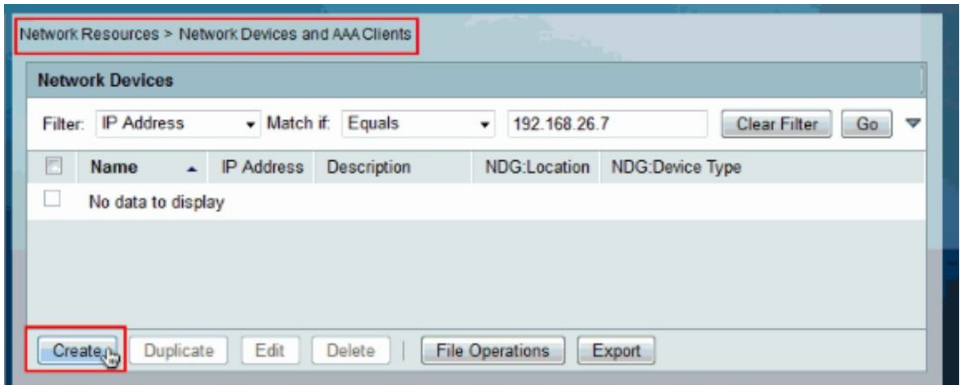
۲۵. تنظیمات انجام شده را ذخیره کنید.


Command Sets
Filter:
Match if:
Go
Command Set Name
Description
DenyAllCommands
Full-Access
Show-Access
Create
Duplicate
Edit
Delete
File Operations
Export
OK
Cancel

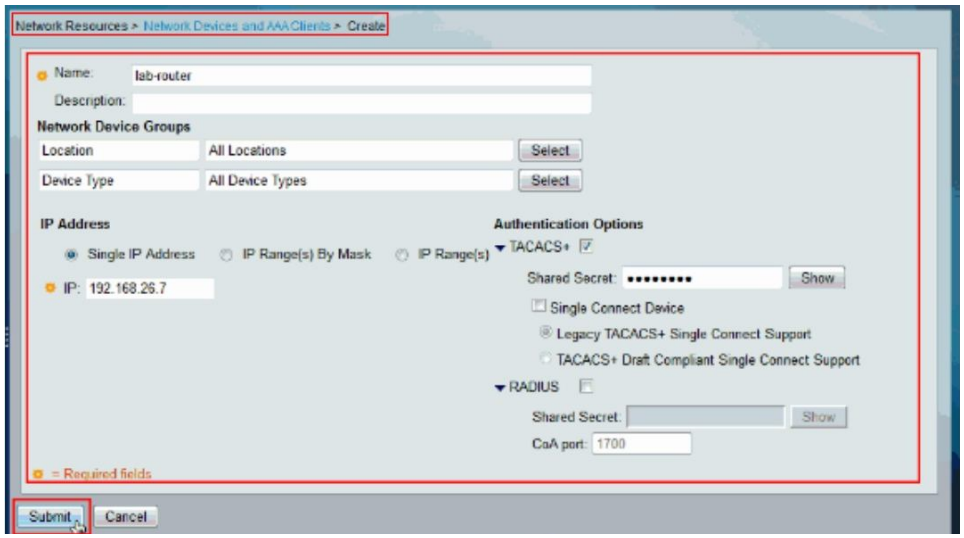




۲۶. به آدرس Network Resources > Network Devices and AAA Clients بروید و Cisco IOS جدید درست کنید.



۲۷. فیلد های **Name**، **IP Address**، **Shared Secret** و **TACACS+** وارد کنید و تایید کنید.



کانفیگ همه ی دیوایس های سیسکو برای Authentication و Authorization

۱- ابتدا کاربری داخلی با سطح دسترسی بالا برای هر دیوایس سیسکو ایجاد کنید.

username admin privilege 15 password 0 cisco123

۲- AAA را enable کنید و IP مربوط به ACS را بدهید (همان IP که با web-console نیز وصل می شوید.)

aaa new-model
tacacs-server host 192.168.26.51 key cisco123

۳- تست کنید که آیا دیوایس سیسکو می تواند سرور TACACS را ببیند؟

test aaa group tacacs+ user1 xxxxx legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.

نکته: توجه کنید که user1 و xxxxx به ترتیب نام کاربری و رمز عبور هستند.

۴- کانفیگ login را انجام دهید و authentication را ایجاد کنید و authorization در Exec و command را کانفیگ کنید:

```
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa authorization config-commands
```

تست و ارزیابی

۱. برای تست به یکی از Cisco IOSها از طریق Telnet با کاربری ادمین وارد شوید و هر command ای را تست کنید تا از دسترسی کامل اطمینان حاصل کنید.

```
username: user1
password:

router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#router rip
router1(config-router)#version 2
router1(config-router)#exit
router1(config)#exit
router1#
```

۲. حال با کاربری دسترسی پشتیبانی وارد شوید و command هایی که اجازه وارد کردن و یا آن هایی که اجازه ندارد را کنترل کنید. Command هایی که اجازه ندارد را با خطای Command Authorization Failed نمایش می دهد.

```
username: user2
password:

router1>enable
password:
router1#
router1#
router1#show version
Cisco IOS Software, C3550 Software (C3550-IPBASEK9-M), Version 12.2(44)SE6, RELEASE S
OFTWARE (fc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 20:26 by gereddy
Image text-base: 0x00003000, data-base: 0x00EA3DE8

ROM: Bootstrap program is C3550 boot loader

router1 uptime is 16 hours, 46 minutes
System returned to ROM by power-on
System image file is "flash:c3550-ipbasek9-mz.122-44.SE6.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

router1#conf t
Command authorization failed.

router1#wr mem
Command authorization failed.

router1#
```

۳. به محیط ACS GUI وارد شوید و به بخش **Monitoring and Reports viewer** وارد شوید. **AAA Protocol >TACACS+Authorization** را انتخاب کنید و عملیات کاربران گروه ادمین و پشتیبانی را بررسی کنید.