

برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

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:



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

New Virtual Machine		(?
1 Select creation type	How would you like to create a virtual machine?	
1a Select a creation type	Create a new virtual machine	This option guides you through creating a new virtual
2 Edit settings	Deploy from template	network connections, and storage. You will need to install a
2a Select a name and folder	Clone an existing virtual machine	guest operating system after creation.
2b Select a compute resource	Clone virtual machine to template	
2c Select storage	Clone template to template	
2d Select compatibility	Convert template to virtual machine	
2e Select a guest OS		
2f Customize hardware		
3 Ready to complete		
		Back Next Finish Cance

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

🔁 New Virtual Machine	
1 Select creation type	Enter a name for the virtual machine.
 1a Select a creation type 	Cisco ACS
2 Edit settings	Virtual machine names can contain up to 80 characters and they must be unique within each vCenter Server VM folder.
2a Select a name and folder	Select a location for the virtual machine.
2b Select a compute resource	Q Search
2c Select storage	VC-F.vcp.local
2d Select compatibility	
2 e Select a guest OS	Select a datacenter or VM folder to create the new virtual
2f Customize hardware	machine in.
3 Ready to complete	
	Back Next Finish Car

شرکت کاریار ارقام



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

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

🖻 New Virtual Machine		?
 Select creation type 1a Select a creation type Edit settings 2a Select a name and folder 2b Select a compute resource 2c Select storage 2d Select compatibility 2e Select a guest OS 2f Customize hardware 3 Ready to complete 	Q Search Image: Constraint of the search Image: Constraint of the search <	Select a cluster, host, vApp or resource pool to run this virtual machine.
	Compatibility: Compatibility checks succeeded.	Back Next Finish Cance

محل ذخیره ماشین مجازی در datastore مشخص شود:

1 Select creation type VMS 1a Select a creation type The 2 Edit settings asselect a name and folder 2b Select a compute resource Image: Compatibility 2c Select storage Image: Compatibility 2c Select a guest OS Image: Compatibility 3 Ready to complete Image: Compatibility	I Storage Policy: No le following datastore tual machine configur ame	ne s are accessible from the d ration files and all of the virtu Capacity		t you selected. Selec	ct the destination o	Storage DRS
2a Select a name and folder 2b Select a compute resource 2c Select storage 2d Select compatibility 2e Select a guest OS 2f Customize hardware 3 Ready to complete	ame]]	Capacity	Provisioned	Free	Туре	Storage DR
Con	mpatibility:	** succeeded.				

در مرحله ی بعد سازگاری ACS با نسخه ی ESXi 5.0 را مشخص می شود. طبق جدول بالا از VM) ESXi 5.0 (VM version 8) تا version 10) 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.



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

🔁 New Virtual Machine			? >>
 New Virtual Machine 1 Select creation type 1a Select a creation type 2 Edit settings 2a Select a name and folder 2b Select a compute resource 2c Select storage 2d Select compatibility 2e Select a guest OS 2f Customize hardware 3 Ready to complete 	The host or cluster supports more than one VMware virtual machine version. Select a compatibility for Compatible with: ESXI 5.5 and later • This virtual machine (VM version 10) provides the best performance and latest features in ESXI 5.5.	the virtual machine.	
	Back Next	Finish	Cancel

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

🔁 New Virtual Machine				? »
 1 Select creation type 1a Select a creation type 2 Edit settings 2a Select a name and folder 2b Select a compute resource 2c Select storage 2d Select compatibility 2e Select a guest OS 2f Customize hardware 3 Ready to complete 	Identifying the gues installation. Guest OS Family: Guest OS Version:	st operating system here allows the wizar Linux Other Linux (32-bit)	d to provide the appropriate defaults for the operating system	ion 10)
			Back Next Finish C	ancel

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 Internal ،HT Sharing را انتخاب کنید.



🔁 New Virtual Machine

شرکت کاریار ارقام

برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

	22.5		
1	2	L.	κ.
A	ЭA		r.,

Cores per Socket (*)	1	-	0	
Cores per Socket (*)	1		1210.001011	
OPULIANDIA		-	Sockets	s: 1
CPU Hot Plug	Enable CPU Hot	t Add		
Reservation	0	•	MHz	-
Limit	Unlimited	-	MHz	•
Shares	Normal	•	1000	
CPUID Mask	Expose the NX/XD	flag to g	guest	Advanced
Hardware virtualization	Expose hardwar	e assis	ted virtual	alization to the guest OS
Performance counters	Enable virtualize	d CPU j	performa	ance counters
HT Sharing (*)	Internal			
Scheduling Affinity	Hyperthreadin Available CPU Select physical proc	ig Statu: Is: cessor ;	s: Inac 2 (p affinity for	ctive physical CPUs) r this virtual machine.
New device:	Select		•	Add Compatibility: ESXI 5.5 and later (VM version
	Limit Shares CPUID Mask Hardware virtualization Performance counters HT Sharing (*) Scheduling Affinity New device:	Limit Unlimited Shares Normal CPUID Mask Expose the NXXXD Hardware virtualization Expose hardwar Performance counters Enable virtualize HT Sharing (*) Internal Scheduling Affinity Hyperthreadin Available CPU Select physical pro-	Limit Unlimited Shares Normal Shares Normal CPUID Mask Expose the NXXD flag to g Hardware virtualization Expose hardware assis Performance counters Enable virtualized CPU HT Sharing (*) Internal Scheduling Affinity Hyperthreading Status Available CPUs: Select physical processor New device: Select	Limit Unlimited • MHz Shares Normal • 1000 CPUID Mask Expose the NX/XD flag to guest Hardware virtualization Expose hardware assisted virtual Performance counters Enable virtualized CPU performa HT Sharing (*) Internal Scheduling Affinity Hyperthreading Status: Ina Available CPUs: 2 (j) Select physical processor affinity fo New device: Select •

در Memory، 4GB رم اختصاص دهید و میزان فضای Hard را GB 60 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.



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

🔁 New Virtual Machine			(? H
1 Select creation type	Virtual Hardware VM Options	SDRS Rules	
 1a Select a creation type 	▼ IIII *Memory		•
2 Edit settings	RAM (*)	4 v GB v	
 2a Select a name and folder 	Reservation		
 2b Select a compute resource 		Reserve all quest memory (All locked)	
 2c Select storage 	Limit		
 2d Select compatibility 	Linin		
 2e Select a guest OS 	Shares	Normal + 40960 +	
2f Customize hardware	Memory Hot Plug	Enable	
3 Ready to complete	👻 🚍 *New Hard disk	60 🗘 GB 🔽	
	Maximum Size	11.63 GB	
	VM storage policy	None 🔻 🕤	
	Location	datastore1	
	Disk Provisioning	Thick provision lazy zeroed Thick provision eager zeroed Thick provision	
	~		₹
	New device:	Add Compatibility: ESXI 5.5 and later	(VM version 10)
		Back Next Finish	Cancel

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

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

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

1 Select creation type	Virtual Hardware VM Options	SDRS Rules
1a Select a creation type	► 🔲 *CPU	
2 Eurosetta name and folder	▶ 🛲 *Memory	4 G B v
2b Select a compute resource	▶ 🚍 *New Hard disk	[60 → (GB ▼)
2c Select storage	▶ 🛃 New SCSI controller	LSI Logic Parallel
2d Select compatibility	✓ m *New Network	VM Network 🔹
2e Select a guest OS	Status	Connect At Power On
2f Customize hardware	Adapter Type	E1000
3 Ready to complete	MAC Address	Automatic 🗸
	▶	Client Device
	🕨 📻 New Floppy drive	Client Device
	🕨 🛄 Video card	Specify custom settings
	▶ ∰ VMCI device	
	 Other Devices 	
	New device:	Select Add Compatibility: ESXi 5.5 and later (VM version 1
		Deale Neutro Civiato Conce

شرکت کاریار ارقام برگزارکننده دوره های تخصصی فناوری اطلاعات،مشاوره ، طرح و اجرای مراکزداده ،امنیت شبکه



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 كاملا با Active Directory ويندوز وابسته است. قبل از كار با ACS، كاربران مورد نظر در Active Directory تعريف 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 و 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.



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

Connection Details		
Active Directory Domain Name:	MCS55.com	
Please specify the credentials used to	join this machine to the Active Directory Domain:	
Username:	training	
Password:		
You may use the Test Connection Butt Click on 'Save Changes' to connect to t can select the Directory Groups and Di	Test Connection he Active Directory Domain and save this configuration. Once you har rectory Attributes to be available for use in policy rules.	eacha
You may use the Test Connection Butt Click on 'Save Changes' to connect to t can select the Directory Groups and Di	Test Connection he Active Directory Domain and save this configuration. Once you har rectory Attributes to be available for use in policy rules.	eacha
You may use the Test Connection Butt Click on 'Save Changes' to connect to t can select the Directory Groups and Di End User Authentication Settings	on to ensure credentials are correct and Active Directory Domain is re Test Connection he Active Directory Domain and save this configuration. Once you ha rectory Attributes to be available for use in policy rules.	ve su
You may use the Test Connection Butt Click on 'Save Changes' to connect to t can select the Directory Groups and Di End User Authentication Settings Enable password change	on to ensure credentials are correct and Active Directory Domain is re Test Connection he Active Directory Domain and save this configuration. Once you have the available for use in policy rules.	ve su
You may use the Test Connection Butt Click on 'Save Changes' to connect to t can select the Directory Groups and Di End User Authentication Settings I Enable password change Enable machine authentication	on to ensure credentials are correct and Active Directory Domain is re Test Connection he Active Directory Domain and save this configuration. Once you ha rectory Attributes to be available for use in policy rules.	ve su

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



Users and Identity Stores > External Identity Stores > Active Direct	ctory
	_
General Directory Groups Directory Attributes	
Directory groups must be selected on this page to be ava policy rules. Click 'Select' to launch a dialog to select gro Selected Directory Groups:	ilable as options in group mapping conditions in oups from the directory.
Group Name	
Add A Edit V Replace A Deselect	Select
Group Name	
Example for group format : cisco.com/Users/Domain Users	
= Required fields	
Save Changes Discard Changes Clear Configur	ration
Sav کلیک کنید.	گروه های مورد نیاز را انتخاب کنید. و بر <i>r</i> e
External User Groups	
earch Base DN DC=MCS55,DC=com	
earch Filter	Go
Group Name	Group Type
MCS55.com/Users/Domain Guests	GLOBAL
MCS55.com/Users/Network Admins	GLOBAL
MCS55.com/Users/Network Maintenance Team	GLOBAL
MCS55.com/Users/Schema Admins	UNIVERSAL
OK Cancel	
Database: Active Directory Use * for wildcard search (i.e. admin*) Search filter applies to group name and not the fully qualified	d path.



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

General	Directory Groups	Directory Attributes]				
Directory policy rule	groups must be select es. Click 'Select' to la	ted on this page to be inch a dialog to select	available as opti groups from the	directory	napping condition:) in	
Selected	Directory Groups						
Selected	Directory Groups.				-		
Group N	ame						
MCS55.0	com/Users/Network A	dmins		- A			
WCS555.	com/users/network iv	antenance learn					
					-		
1	10						
Add /		epiace A Deselect	Select				
Group Na	ime						
Example	for group format :						
cisco con	n/Users/Domain User	3					
= Requi	ired fields						

access service > Service Selection Rules > Access Services > Service Selection Rules
 کود را پیدا کنید. در این مقاله از +TACACS استفاده می شود که از نوع Default Device Admin

Sin	igle re	sult select	tion 🤗 F	Rule based result	selection		
Servic	e Sel	ection Po	olicy				
Filter:	State	us 🔻	Match if:	Equals •	Enabled Clear F	iter Go 🗸	
		Status	Name	Protocol	Conditions	Results Service	Hit Count
1		0	Rule-1	match Tacacs		Default Device Admin	1
2	1775	0	Rule-2	match Radius	4	Default Network Access	0

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه



Identit	ty Store	Showing 1-9 of 9 50 • per page	Go
Fiter:	-	Match if Go 🔻	
	Name 🔺	Description	
0	AE1		
0	CN Usemanne	Predefined Certificate Authentication Profile	
0	DenyAccess		
0	Internal Hosts		
0	Internal Users		
Ø	LUAP	Domain Controller LUAP	
0	NAC Profiler	Default Entry for N/AC Profiler	
O	safeword	THIS IS NOT USED inic 2011.11.22	
0	saleword-ias		
QK	Cancel		[<u>P</u>]
Access	Policies > A	ccess Services > Default Device Admin > Identity	
ldenti	Single result ity Source:	selection C Rule based result selection AD1 Select Advanced Options	
Save	e Changes	Discard Changes	

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

ccess Pi	olicie: rd Po	icy <u>Exce</u>	eption Pr	Default Device Admin > Authorization			
Device	e Adn	ninistratio	on Autho	rization Policy			
Filter.	Stat	us	33	Match if Equals Enabled	Clear Filter	Ge 🗢	
		Status	Name	Conditions Compound Condition	F Shell Profile	Results Command Sets	Hit Count
		No data	to displa	v			
-		Default		If no rules defined or no enabled rule matches	Permit Access	DenyAlCommands	1
Create	1.	Duplic	ate •	Edit Delete A Move to V			Custernize Hit Count
Save C	hang	es D	iscard Ch	anges			

۸. در بخش AD1:ExternalGroups، Customize Conditions و از بخش Customize Results،
 Shell Profile و Shell Profile

ACS Host Name Authentication Method Authentication Status Compound Condition Device Filter Device Port Filter Eap Authentication Method Eap Tunnel Building Method End Station Filter Customize Results Available: Selected: Shell Profile Command Sets	Available:	Selected:	
Authentication Nieurod Authentication Status Compound Condition Device Filter Device IP Address Device Port Filter Eap Authentication Method Eap Tunnel Building Method End Station Filter Customize Results Available: Selected: Shell Profile Command Sets	ACS Host Name	AD1:ExternalGroups	A
Addrendication Status Compound Condition Device Filter Device Port Filter Eap Authentication Method Eap Tunnel Building Method End Station Filter Customize Results Available: Selected: Shell Profile Command Sets	Authentication Method		$\overline{\mathbf{x}}$
Compound Condition Device Filter Device Port Filter Eap Authentication Method Eap Tunnel Building Method End Station Filter Customize Results Available: Selected: Shell Profile Command Sets	Authentication Status	1	
Device IP Address Device Port Filter Eap Authentication Method Eap Tunnel Building Method End Station Filter Customize Results Available: Selected: Shell Profile Command Sets	Device Filter		
Device Port Filter Eap Authentication Method Eap Tunnel Building Method End Station Filter Customize Results Available: Selected: Shell Profile Command Sets	Device IP Address		
Eap Authentication Method Eap Tunnel Building Method End Station Filter	Device Port Filter	>>>	
Eap Tunnel Building Method End Station Filter	Eap Authentication Method		
End Station Filter Customize Results Available: Selected: Shell Profile Command Sets	Eap Tunnel Building Method	~	\leq
Customize Results Available: Selected: Shell Profile Command Sets	End Station Filter	-	-
		*	× ×

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

)evic	e Administration A	uthorization Policy			
Filter	Status	Match if Equals Enabled	Clear Filter	io 🗸	
	Status Na	me Conditions AD1.ExternalGroups	Re Sheli Profile	command Sets	Hit Count
	Default	If no rules defined or no enabled rule matches	Permit Access	DenyAllCommands	0
reate	e	I • Edit Delete A Move to Y			Customize Hit Count

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

General			
Name: Rule-1	Status: Lnabled	• 0	
The Customize b conditions and re Conditions Z AD1:LxtemalGroups: containe any	utton in the lower right ar sults are available here fo	ea of the policy rules : or use in policy rules.	screen controls which policy
Select, Deselect	Clear		
Select Deselect	Clear		
Select Deselect Results Shell Profile. Permit Acces	Clear :	Sel=ct	
Select Deselect Command Sets	Clear 5]el⊧ct	
Select Deselect Results Shell Profile. Permit Accel Command Seta:	Clear 3	Select]	~
Select Deselect C Rosults Shell Profile. Permit Acces Command Sets:	Clear	ີອໄສປ	~



.11

String Enum Definition	Showing 1-2 of 2 50 • per page Go
Filter: • Match if: • Go •	7
Enum Name	•
MCS55.com/Users/Network Admins	
MCS55.com/Users/Network Maintenance Team	
	Page 1 of 1 P PI
OK Cancel	
کست نید و Create را برای گروه ادمین انتخاب کنید.	Shell profile بر روی Select کلیک کن
The Customize button in the lower right area of the policy conditions and results are available here for use in policy	y rules screen controls which policy y rules.
Conditions	
Contains any	
MCS55 com/ leare/Nation& Admine	
Select Desclect Clear	
Results	
Shell Profile: Dermit Access Select	
Select Deselect	
이국 Cancel	- Liep
Shell Profiles	Showing 1-2 of 2 50 • per page Go
Filter: • Match if: • Go v	
Name Description	
Name Description	
Name Description O DenyAccess O Permit Access	
Name Description O DenyAccess O Permit Access	
Name Description O DenyAccess O Permit Access O Create Duplicate Edit Delete	1 of 1 Page 1



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

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 ۱۵ کا انتخاب کنید.

innege zerei					
Default Privilege:	Static	•	Value	15	•
Maximum Privilege:	Static	•	Value	15	•
Shell Attributes					
Access Control List:	Not in Use	• •			
Auto Command:	Not in Use	• •			
No Callback Verify:	Not in Use	• •			
No Escape:	Not in Use	• •			
No Hang Up:	Not in Use	• •			
Timeout:	Not in Use	• •			
Idle Time:	Not in Use	• •			
Callback Line:	Not in Use	• •			
Callback Rotary:	Not in Use	• •			

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

Filter:		 Match 	n if:	•	Go	~	
	Name	 Desc 	cription				
0	DenyAccess						
0	Full-Privilege	То р	ush default	privilege 15 for	IOS		
0	Permit Acces	s					
Crea	te Duplica	ite E	Edit Del	lete			

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

The Customize button in the lower right area of the policy rules screen e conditions and results are available here for use in policy rules.	ontrols which policy
Conditions	
AD1:External Groups:	
contains any	
MCS55.com/Users/Network Admins Select Decelect Clear Results Shell Profile: Ful-Provlege Commond Setz: Image: Select Image: Select Image: Select Select Image: Select Select Image: Select	
OK Cancel	le p

Filter: ▼ Match if: ▼ Go Command Set Name ▲ Description DenyAllCommands	6-15C
Command Set Name Description DenyAllCommands	
DenyAllCommands	

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



Name: Description	Full-Access		
Permit an Grant	y command that is not in the table below	Arguments	•
Add /\	Edit V Replace // Delete		-
Permit	•		
Select Com	nand/Arguments from Command Set	DenyAllCommands -	

Command Sets	
Filter:	✓ Match if: Go ♥
Command Set Nam	e Description
DenyAllCommands	
✓ <u>Full-Access</u>	
Create Duplicate	Edit Delete File Operations Export
OK Cancel	



برگزاركننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراكزداده ،امنيت شبكه

Comn	nand Sets
Filter:	✓ Match if: ✓ Go ▼
	Command Set Name Description
	DenyAllCommands
V	Full-Access
Crea	te Duplicate Edit Delete File Operations Export
-	
OK	Cancel

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

Device	e Adm	inistration	Author	ization Policy			
Filter.	Statu	IS .		Match II. Equals - Enabled - Clear F	Filter Go 🔻	·	
		Status	Name	Conditions AD1:ExternalGroups	R Shell Profile	csults Command Sets	Hit Count
1		0	Rule 1	contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full Access	0
**	8	Default		If no rules defined or no enabled rule matches.	Permit Access	DenyAllCommands	0
Create	- I *	Duplicati	e *	Edit Delete A Move to V			Customize Hit Coun

۸. 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	- 0	
Conditions AD1.ExternalGroups.	button in the lower right esuits are available here	area of the policy rules for use in policy rules.	screen controls which policy
contains any -			14
			*
Select	Clear		
Results Shell Profile. Permit Acc	4 85	Selec.	
Command Sets:			
	^		
NC Constant	+		-114
			Tiel



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

String	Enum Definition
Filter:	✓ Match if: ✓ Go ▼
	Enum Name
	MCS55.com/Users/Network Admins
	MCS55.com/Users/Network Maintenance Team
OK	Cancel
UK	Cancer

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

Conditions	
AD1:ExternalGroups:	
contains any	
MCS55.com/Users/Network Maintenance Team	A
Select Deselect Clear	
Results	
Shell Profile: Permit Access Select	
Command Sets:	

Shell	Profiles	
Filter:	-	Match if: Go 🔻
	Name 🔺	Description
0	DenyAccess	
0	Full-Privilege	To push default privilege 15 for IOS
0	Permit Access	
Crea	te Duplicate	Edit Delete
OK	Cancel	

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

Name:	Limited-Privilege	
Description:	To push default privilege 1 for IOS	

و Default Privilege ،Privilege Level کلیک کنید و در قسمت Maximum Tasks و به ترتیب Value و ۱۵ انتخاب کنید.

General Common	Tasks	Cust	om /	Attribute	s		
Privilege Level							
Default Privilege:	Static		•	Value	1	•	
Maximum Privilege:	Static		•	Value	15	•	
Shell Attributes							
Access Control List:	Not in	Use	•				
Auto Command:	Not in	Use	•				
No Callback Verify:	Not in	Use	•				
No Escape:	Not in	Use	•				
No Hang Up:	Not in	Use	•				
Timeout:	Not in	Use	•				
Idle Time:	Not in	Use	•				
Callback Line:	Not in	Use	•				
Callback Rotary:	Not in	Use	•				

Submit

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

Filter:	- N	Match if:
	Name 🔺	Description
0	DenyAccess	
0	Full-Privilege	To push default privilege 15 for IOS
0	Limited-Privilege	To push default privilege 1 for IOS
0	Permit Access	

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

The Customize button in the lower right area of the policy r conditions and results are available here for use in policy r Conditions	rules screen controls which policy ules.
AD1:ExternalGroups:	
contains any	
MCS55.com/Users/Network Maintenance Team	Û
Select Deselect Clear	
Results	
Shell Profile: Limited-Privilege Select	
Command Sets:	
Select Deselect	
K Cancel	6

Comr	nand Sets
Filter	- Match if: - Go -
	Command Set Name Description
	DenyAllCommands
	Full-Access
Crea	The Duplicate Edit Delete [File Operations Export
OK	Cancel

۲۴. درGeneral اسم انتخاب کنید و حتما در فیلد Description بنویسید. مطمئن باشید که تیک Permit any command that is not in the table below گزینه ی Permit any command that is not in the table below 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.



Name:	Show-Access	
Descriptio	n: / command that is not in the table below	
Grant	Command	Arguments
	Edit V Replace A Delete	
Add /	Command	Arguments
Grant	Command	
Grant Permit	✓ show	



rvame.	Show-Access	
Description:		
Permit any co	ommand that is not in the table below	
Grant	Command	Arguments
Permit	show	
Permit	exit	
Add A	Edit V Replace /\ Delete	
Add A	Edit V Replace A Delete	Arguments
Add ∧ 〕	Edit V Replace A Delete Command	Arguments
Add A	Edit V Replace / Delete Command	Arguments DenyAllCommands -



Command Sets	
Filter: • Matc	h if: 🔹 🖌 Go 💌
Command Set Name	Description
DenyAllCommands	
E Full-Access	
Show-Access	
Create Duplicate Edit	Delete [File Operations Export]
OK Cancel	



Access Policies

شرکت کاریار ارقام

برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

The Customize button in the lower right area of the policy rules screen con conditions and results are available here for use in policy rules.	
Conditions AD1:ExternalGroups: contains any MCS55.com/Users/Network Maintenance Team	
Select Deselect Clear Results Shell Profile: Limited-Privilege Command Sets: Select	
Show-Access	
Select Deselect	
sss Services > Default Device Admin > Aufhortzation	
sception Policy	

filter:	State	IS	•	Match if: Equals • Enabled • Clear Filter	ia 🔻		
		Status	Name	Conditions AD1:ExternalGroups	Re Shell Profile	command Sets	Hit Count
1	Bule-1		Rule-1	contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full-Access	0
2	1-1	0	Rule-2	contains any (MCS55.com/Users/Network Maintenance Team)	Limited-Privilege	Show-Access	0
		Default		If no rules defined or no enabled rule matches.	Permit Access	DenyAlCommands	0
reate		Duplica	te] •	Edit Delete A Move to V		C	ustomize Hit Count

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



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

Network Resources > Network Devices and AAA Clients									
	Network Devices								
	Filter:	IP Address	+ Match	if: Equals	•	192.168.26	.7	Clear Filter	Go 🔻
h		Name 🔺	IP Address	Description	N	DG:Location	NDG:Device	Туре	
		No data to dis	play						
L									
L									
F									
L	Creat	Duplica	ate Edit	Delete	File Ope	rations	xport		

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

Description:	H	
letwork Device Group	5	
Location	All Locations	Select
Device Type	All Device Types	Select
IP Address	es 🦉 IP Ranne(s) By Mask (Authentication Options
in angle i risare.	a O is range(s) of music (/ = range(a)
B IP: 192 168 26 7		Shared Secret: ••••••• Show
• IP: 192.168.26.7		Shared Secret: Show Show
IP: 192.168.26.7		Shared Secret: Show Show
IP: 192.168.26.7		Shared Secret: Show Single Connect Device Elegacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support
 IP: 192.168.26.7 		Shared Secret: Show Single Connect Device Elegacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support RADIUS
IP: 192.168.26.7		Shared Secret: Show

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 xxxx 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.

exec در authorization را انجام دهید و authentication را ایجاد کنید و login در Iogin در exec و 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

۰. برای تست به یکی از Cisco IOSها از طریق Telnet با کاربری ادمین وارد شوید و هر 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.



برگزارکننده دوره هاي تخصصی فناوری اطلاعات،مشاوره ، طرح و اجراي مراکزداده ،امنيت شبکه

username: users
password:
router1>emable
password:
routerla
router1#
router1#show version
Cisco IOS Software, C3550 Software (C3550-IPBASEK9-N), version 12.2(44)SE6, RELEASE S
OFTWORE (fcl)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon D9-Mar-D9 20:26 by gereddy
Image text hape: 0x00003000, data base: 0x00EA3DE8
RUM: Bootstrap program is C3550 boot loader
routerluptime is 16 hours, 46 minutes
System returned to ROM by power-on
System image file is "flash:c3550-ipbasek9-mz.122-14.SEC.bin"
53
This product contains crystographic 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 incort, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.C. and local country laws. By using this product you
some to comply with applicable laws and regulations. If you are upplied
to comply with U.S. and local laws return this product immediataly.
of other with other and repair on the product interactively.
I summary of [15] lays coverning figon crumographic products have be found at:
bit is flow a start and a first former of real start provided to the
and to V to an extension of a strain stree 31 cost to only 21 cost.
If you require further assistance please contact us by sending evail to
Ar you load a second deliberte britese bentaet us by fending chair to
CALOF OF GOLDE C. SOM
XANTERI CONT F
Lonmeno alloprization fattes.
I Outorite Window Station Fridad
commind activitization falles.

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.

						Launch Inte	eractive Viewer	
Showing Pa	ge 1 of 1				Gote	Page: Go		
AAA Protocol > T	ACACS+ Authoriz	ation						
Authorization Status Date :	: Pass or Fail June 08, 2012							
Generated on June	8, 2012 11:57:34 AM	IIST						
Reload								
-Pass *-Fail	-Click for deta	Is						
ACS View Timestamp	ACS Timestamp	Status	Details	Failure Reason	User Name	Command Set	Shell Profile	Network Device
Jun 8,12 6 21 19,410 AM	Jun 8,12 6:21:19 393 AM	-	4		saw2	[Casi4Vestit]		ab-mint
Jan 8.12 6:20 19:800 AM	3x1 8.12 6:20:59 799 AM	ж	2	13025 Command Billed to march a People rate	mer?	[CoddWmetizmenory]		
Ins 1,128:20 16 268 AM	Am 5,12 6:20:56 850 AM	*	2	11011 Command failed to match a Permit rale	a.e.2	[ContAV-configure terminal]		ab-coast
Jun 8,12 6:20 50.056 AM	Jun 8,12 6,20,50,036 AM	*	2	0	pier2	[Cnd.W-show version.]		SB-router
Non 8,12 6 20 78,505 AM	Am 8.12 0:20:38.490 AM	*	2	Commands run by	55M2	[Ond-Wreatols]		ab-oxaw
Net 8.12 0.20 34 426 AM	Jan 8,12 6:20:34.406 AM	*	44	user 2	sast2	[CmdAV=]	Linited-Privilege	lab-costar
Jun 8,12 5-20,02 515 AM	han 8,12 6:20:02.596 AM	~	9		EDA([End4Vertit]		ab-mar
3w 8.12 4:20 00.253 AM	Jan 8,12 6:20:00 246 AM	*	14	Commands run by	ansel.	[CndAl/wranics.2.]		Merestan
he 5,12 5 19 57 203 AM	3at 8.12 6:19:57 260 AM	4	94	user1	5001	[Cast.Wrecover rip]		at-rours
Jun 8,12 6:19 55,103 AM	Jan 8.12 6.19.55.076 AM		14		seet	[Cnd.W-configurateminal]		Mercelan
No. 8,12 6 19 52 763 AM	AN 8.12 0 19:52 740 AM	~	9		met .	[Cad-W=]	Pall-Privilege	ab-over