

Cisco مَادخْتَسَابِ ASR9K TACACS نِيوَكْتِ Identity Services Engine 2.4

تَايَوْتَحْمَلَا

[قَمْدَقْمَلَا](#)

[قَيْسَاسَا تَامَوْلَعْم](#)

[قَيْسَاسَا أَلَا تَابَلَطْتَمَلَا](#)

[تَابَلَطْتَمَلَا](#)

[قَمْدَخْتَسَمَلَا تَانوَكْمَلَا](#)

[نِيوَكْتَلَا](#)

[IOS® XR يَلَعِ اقْبَسَمِ قَمْدَحْمِ تَانوَكْمِ](#)

[اقْبَسَمِ قَمْدَحْمَلَا نِيْمَدْخْتَسَمَلَا تَاعْوَمْجَمِ](#)

[اقْبَسَمِ قَمْدَحْمِ مَاهَمِ تَاعْوَمْجَمِ](#)

[مَدْخْتَسَمَلَا لِبَقِ نَمِ قَمْرَعْمِ مَاهَمِ تَاعْوَمْجَمِ](#)

[هَجْوَمَلَا يَلَعِ AAA نِيوَكْتِ](#)

[ISE مَدْخِ نِيوَكْتِ](#)

[قَحْصَلَا نَمِ قَقْحْتَلَا](#)

[لِغَشْمِ](#)

[\(AAA\) قَبَسَاحْمَلَاوِ ضِيوَفْتَلَاوِ قَمْدَاصْمَلَا مَادْخْتَسَابِ لِغَشْمَلَا](#)

[نِيْدَاسِيسِ](#)

[يِرْذَجِ مَاطَنِ](#)

[اَهْجَالِصَاوِ عَاطْخَا أَلَا فَاشْكْتَسَا](#)

قَمْدَقْمَلَا

لِجْأِ نَمِ ASR 9000 قَلْسَلْسَلَا نَمِ (ASR) عِيْمَجْتَلَا تَامَدْخِ هَجْوَمِ نِيوَكْتِ دَنْتَسَمَلَا اِذْهَ فِصِي قَيْسَاسَا نَمِ Cisco 2.4 نَمِ قَيْوَهَلَا تَامَدْخِ كَرْحَمِ مَدْخِ مَادْخْتَسَابِ TACACS+ رِبَعِ ضِيوَفْتَلَاوِ قَمْدَاصْمَلَا

قَيْسَاسَا تَامَوْلَعْم

هَمَادْخْتَسَا مَتِي يَذَلَا مَاهَمَلَا يَلِي دَنْتَسَمَلَا ضِيوَفْتَلَاوِ يَرَادِإِلَا جَذْوَمِنَلَا ذِيْفَنْتِ يَلَعِ لَاطْمِ وَهَوِ قَيْسَيِيئَرَلَا مَاهَمَلَا نَمِضْتَتِ Cisco IOS® XR جَمَانِرِبِ مَاطَنِ يَفِ مَدْخْتَسَمَلَا لَوْصَوِ يَفِ مَكْحَتَلَلِ نِيْمَدْخْتَسَمَلَا تَاعْوَمْجَمِ نِيوَكْتِ قَيْفِيكِ مَاهَمَلَا يَلِي دَنْتَسَمَلَا ضِيوَفْتَلَاوِ ذِيْفَنْتَلَا قَبُولِطَمَلَا رَمَاوَا قَمْدَحْمَلَا لَخِ نَمِ مَاهَمَلَا تَاعْوَمْجَمِ نِيْمَدْخْتَسَمَلَا تَاعْوَمْجَمِ نِيوَكْتِ مَتِي. مَاهَمَلَا تَاعْوَمْجَمِو مَتِي (AAA) قَبَسَاحْمَلَاوِ ضِيوَفْتَلَاوِ قَمْدَاصْمَلَا تَامَدْخَلَا قَمْدَخْتَسَمَلَا Cisco IOS® XR جَمَانِرِبِ مَتِي. يَسَاسَا وَأَمَدْخْتَسَمِ قَيْوَهَ نَمِ قَقْحْتَلَلَا قَمْدَاصْمَلَا رَمَاوَا مَادْخْتَسَا لِيوَخْتَلَا رَمَاوَا مَادْخْتَسَا مَتِي. يَسَاسَا وَأَمَدْخْتَسَمِ قَيْوَهَ نَمِ قَقْحْتَلَلَا قَمْدَاصْمَلَا رَمَاوَا مَادْخْتَسَا لِيوَخْتَلَا رَمَاوَا مَادْخْتَسَا مَتِي. قَيْوَهَ مَهَمِ ذِيْفَنْتَلَا (يَسَاسَا وَأَمَدْخْتَسَمِ قَمْدَخْتَسَمَلَا نَذَا حَمِ نَمِ قَقْحْتَلَلَا تَاعَارْجِ لِيَجْسَتَبِ قِيْقِدْتِ لِحَسِ عَاشِنَاوِ لِمَعَلَا تَاسَلْجِ لِيَجْسَتَلَا قَبَسَاحْمَلَا رَمَاوَا مَادْخْتَسَا مَاطَنَلَا وَأَمَدْخْتَسَمَلَا قَمْدَاصْمَلَا عَاطْخَاوِ هَاوَأَشِنَا مَتِ قَيْوَهَ

قَيْسَاسَا أَلَا تَابَلَطْتَمَلَا

[تَابَلَطْتَمَلَا](#)


```

retrieval      Name of the usergroup
maintenance    Name of the usergroup
root-system    Name of the usergroup
provisioning   Name of the usergroup
read-only-tg   Name of the usergroup
serviceadmin   Name of the usergroup
cisco-support  Name of the usergroup
WORD           Name of the usergroup
<cr>

```

اقبس م ةدحم م اهم تاعومجم

يولوال نيوكتلل ةداع ،اهم ادختسال ني لوؤس ملل هذه اقبس م ةدحم الم اهم الم تاعومجم رفوت

- Cisco نم معدل يفظوم م اهم : Cisco معد
- Netadmin: م اهم لوؤس م م اهم
- (يحيضوتل ضرعل اضارأل) ةيمويلا لغشم الم م اهم : لغشم الم
- root-lr: م اهم لوؤس م م اهم
- م اظنل يوتسم يلعل لوؤس م الم م اهم : يردجل م اظنل
- م اظنل لوؤس م م اهم : م اظنل
- ServiceAdmin: م اهم ةراد م م اهم

اقبس م ةدحم الم اهم الم تاعومجم نم ققحتلل رمأوال هذه مدختسأ

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup ?
```

```

|           Output Modifiers
root-lr     Name of the taskgroup
netadmin   Name of the taskgroup
operator    Name of the taskgroup
sysadmin    Name of the taskgroup
root-system Name of the taskgroup
serviceadmin Name of the taskgroup
cisco-support Name of the taskgroup
WORD        Name of the taskgroup
<cr>

```

تم وعدمل م اهل نم ققحتلل رمأال اذه مدختسأ:

```
RP/0/RSP1/CPU0:ASR9k#show aaa task supported
```

تم وعدمل م اهل اب قمئاق يلي اميف

AAA	ACL	لوؤس الم	بكن	ATM	تامدخال ةيساسال	BCDL	BFD	BGP
ةمزع	ةمزع	لاصتال لزنم لاب	CDP	CEF	CGN	معد	Cisco config-mgmt	config-se
ري فشت	غايد	ريغ حومسم	جمارب ليغشتل	DWDM	ميآ	EIGRP	تامدخ ةكبش تنرثيإ	اه لوصو
جيسن	مقر-قلاف	ماظن تافل الم رادصإل	ةيامحل رادج	FR	HDLC	تامدخ فيضم الم	HSRP	ةهجاوال
درج	ل تامدخ IP	نم عبارل لوكوتورب تنرتنإل (IP)	IPv6	شعاد	L2VPN	يل	غثل	يجستل
عطاقم	زاهج	MPLS-LDP	مبأ-مبأ	MPLS-TE	ثبل	Netflow	ةكبش الم	رداصم

ضرع ل	دعت م ل	ك ب ش ل
لوكوت ورب ر ص ق أ م ن و أ ال و أ راس م (OSPF)	pkg-mgmt pos-dpt PPP	ع ل ض ي د م ا ي س ر أ ة د و ج ة م د خ ل ا
ق ش م ا ظ ن ل ا ر غ م س ي س	ة ط ي ر خ ق ي ر ط ل ا tty ل و ص و	ن ك ا س Vlan ل ا س ر ف ي ن و ي VRRP
ر ذ ج م ا ظ ن ل ا ر غ م س ي س	ر أ ي ب ي ب ي ر ذ ج م ا ظ ن ل ق ن ل ا	س ن ك ا س sonet-sdh VPDN

ع ب ر أ ل ا ن و ذ أ ل ا ة ف ا ك و أ ن و ذ أ ل ا ه ذ ه ن م ي أ ع م ة ر و ك ذ م ل ا م ا ه م ل ا ن م ة م ه م ل ك ح ن م ن ك م ي

ات ع ل و ط
ة ب ا ت ك
ذ ي ف ن ت
ح ي ح ص ت
ء ا ط خ ا ل ا

ة ع ا ر ق ة ي ل م ع ب ط ق ف ح م س ي ن ي ي ع ت د ي د ح ت
ة ع ا ر ق ة ي ل م ع ب ا ي ن م ض ح م س ي و ر ي ي ع ت ة ي ل م ع ب ح م س ي د ي د ح ت د ي د ح ت
ج م ا ن ر ب و ل ا ص ت ا ل ا ر ا ب ت خ ا ، ل ا ث م ل ا ل ي ب س ي ل ع ، ل و ص و ة ي ل م ع ب ح م س ي د ي د ح ت د ي د ح ت
Telnent.
ء ا ط خ ا ح ي ح ص ت ة ي ل م ع ب ح م س ت ة ي م س ت د ي د ح ت

م د خ ت س م ل ا ل ب ق ن م ة ف ر ع م م ا ه م ت ا ع و م ج م

ل ا ث م ي ل ي ا م ي ف . ة ص ا خ ت ا ج ا ي ت ح ا ة ي ب ل ت ل ة ص ص خ م م ا ه م ت ا ع و م ج م ن ي و ك ت ن ي ل و و س م ل ل ن ك م ي
ن ي و ك ت ل ا ي ل ع :

```
RP/0/RSP1/CPU0:ASR9k(config)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-tg)#task ?
  debug      Specify a debug-type task ID
  execute    Specify a execute-type task ID
  read       Specify a read-type task ID
  write      Specify a read-write-type task ID
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task debug aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#commit
```

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup TAC-Defined-TASK
Task group 'TAC-Defined-TASK'
```

```
Task IDs included directly by this group:
Task:          aaa   : READ   WRITE   EXECUTE   DEBUG
Task:          acl   : READ   WRITE   EXECUTE
```

```
Task group 'TAC-Defined-TASK' has the following combined set
of task IDs (including all inherited groups):
```

```
Task:          aaa   : READ   WRITE   EXECUTE   DEBUG
Task:          acl   : READ   WRITE   EXECUTE
```

ن ي ع م ر م أ ل ب و ل ط م ل ا ن ذ أ ل ا و م ا ه م ل ا ة ع و م ج م ي ل ع ر و ث ع ل ل ه م ا د خ ت س ا ن ك م ي ر م أ ل ا ف ص و

1. ل ا ث م

```
RP/0/RSP1/CPU0:ASR9k#describe show aaa usergroup
```

```
Package:
```

```
.....
```

```
User needs ALL of the following taskids:
```

```
aaa (READ)
```

```
RP/0/RSP1/CPU0:ASR9k#
```

رمال نيي عت بجي: ماهم الة وعومجم **show aaa userGroup**، لي غشت ب مدخت سملل حام سملل **read aaa** ني مدخت سملل الة وعومجم الة.

2. لاثم

```
RP/0/RSP1/CPU0:ASR9k(config)#describe aaa authentication login default group tacacs+
```

```
Package:
```

```
.....
```

```
User needs ALL of the following taskids:
```

```
aaa (READ WRITE)
```

```
RP/0/RSP1/CPU0:ASR9k(config)#
```

رمال الة قداصم الة لوخذ الة لي ج سملل الة لي غشت ب مدخت سملل حام سملل **read write aaa** ماهم الة وعومجم، ني وك ت الة عضو نم **tacacs+** ني مدخت سملل الة.

تاعومجم نم دي دال الة اثاروا ه نكمي يت الة ني مدخت سملل الة وعومجم دي دت ني لوؤس سملل نكمي ني وك ت الة لاثم ان ه ماهم الة.

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
```

```
Tue Feb 16 00:50:56.799 UTC
```

```
User group 'TAC-Defined'
```

```
  Inherits from task group 'operator'
```

```
User group 'TAC-Defined' has the following combined set  
of task IDs (including all inherited groups):
```

```
Task:      basic-services  : READ      WRITE      EXECUTE      DEBUG
```

```
Task:      cdp             : READ
```

```
Task:      diag            : READ
```

```
Task:      ext-access     : READ              EXECUTE
```

```
Task:      logging        : READ
```

```
RP/0/RSP1/CPU0:ASR9k#conf t
```

```
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
```

```
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup TAC-Defined-TASK
```

```
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit
```

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
```

```
Tue Feb 16 00:51:31.494 UTC
```

```
User group 'TAC-Defined'
```

```
  Inherits from task group 'operator'
```

```
  Inherits from task group 'TAC-Defined-TASK'
```

```
User group 'TAC-Defined' has the following combined set  
of task IDs (including all inherited groups):
```

```
Task:      aaa             : READ      WRITE      EXECUTE      DEBUG
```

```
Task:      acl             : READ      WRITE      EXECUTE
```

```
Task:          basic-services  : READ      WRITE      EXECUTE    DEBUG
Task:          cdp             : READ
Task:          diag            : READ
Task:          ext-access      : READ      EXECUTE
Task:          logging         : READ
```

هجوم الـ AAA نيوكت

متيس يذلا كرتشمل رسال او IP ناو نع مادختساب ASR هجوم ىلع TACACS مداخل نيوكت ب مق همادختسا.

```
RP/0/RSP1/CPU0:ASR9k(config)#tacacs-server host 10.106.73.233 port 49
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#key 0 cisco
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#commit
```

```
!
tacacs-server host 10.127.196.160 port 49
key 7 14141B180F0B
!
```

هنيوكت مت يذلا TACACS مداخل مادختسال ضيوفتلاو عقداصلم نيوكت ب مق

```
#aaa authentication login default group tacacs+ local
#aaa authorization exec default group tacacs+ local
```

(يراي تخا) هنيوكت مت يذلا TACACS مداخل مادختسال رماوأل ضيوفت نيوكت ب مق

نيوكت نم دكأتو، عقتوتم وه امك نالمعي ضيوفتلاو عقداصلم نا نم دكأت: **ةظحالم**
اهنيوكت متي مل اذا. رماوأل ضيوفت نيوكت لبق حيحص لكشب اضيأ رماوأل تاعومجم
زاهجلا ىلع رماوأل لاخدا نم نومدختسمل نكمتي ال دقف، حيحص لكشب

```
#aaa authorization commands default group tacacs+
```

(يراي تخا) هنيوكت مت يذلا TACACS مداخل مادختسال رماوأل ةبساحم ةي لمع نيوكت ب مق

```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ISE مداخل نيوكت

> **ةرادإلا** ىلا لقتنا، ISE مداخل ىلع AAA ءالمع ةمئاق ي ف هجوملل IP ناو نع ديدحتل 1. ةوطخل
وه كرتشمل رسال نوكي نا بجي. ةروصلال ي ف حضوم وه امك ةكبشلا زهجا > **ةكبشلا دراوم N**
ةروصلال ي ف حضوم وه امك ASR هجوم ىلع هنيوكت مت يذلا هسفن.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > New Network Device

Network Devices

* Name LAB_ASR

Description LAB_ASR device

IP Address * IP: 10.106.37.160 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location LAB Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type ASR Set To Default

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret ***** Show

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Submit Cancel

ةكبشلا زاغ نيوكت

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> LAB_ASR	10.106.37.16...	Cisco	LAB	ASR	LAB_ASR device

ةكبشلا زاغ نيوكت

حضورم وه امك ،لا ثمل ا يف ،ك تابل طتم بسح ني مدخت سمل ا تا عومجم في رعت ب مق 2 ة وطلخا
 ةرادا > ةرادا تحت تا عومجم ا في رعت ك نكمي . تا عومجم ع برأ مدخت ست ك ن ا ف ، ة وصال ا هذه يف
 يه لا ثمل ا اذه يف اه واصل ن ا مت ي تل ا تا عومجم ا . مدخت سمل ا ة يوه تا عومجم > تا عومجم > ة يوه ا

1. ASR لغ شم
2. ASR-operator-AAA
3. ASR-RootSystem
4. ASR-Sysadmin ة ي ع م ج

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

- Endpoint Identity Groups
- User Identity Groups
 - ALL_ACCOUNTS (default)
 - ASR-Operator
 - ASR-Operator-AAA
 - ASR-RootSystem
 - ASR-Sysadmin
 - Employee
 - GROUP_ACCOUNTS (default)
 - GuestType_Contractor (default)
 - GuestType_Daily (default)
 - GuestType_SocialLogin (default)
 - GuestType_Weekly (default)
 - OWN_ACCOUNTS (default)

User Identity Groups

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
ASR-Operator	
ASR-Operator-AAA	
ASR-RootSystem	
ASR-Sysadmin	
Employee	Default Employee User Group
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
GuestType_Contractor (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
GuestType_Weekly (default)	Identity group mirroring the guest type
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

مه طي طخت و ني مدخت اسم الا ءاش ن اب مق ، ة روص لا ي ف حضورم وه امك . 3 ة ووطخ لا ل ءه و ال ء اعوم جم ل ب ق نم اه ءاش ن ا مت ي ال ء ل ب ا ق م ال ني مدخت اسم ال ء اعوم جم ال

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/> Enabled	ASRaaa					ASR-Operator-AAA	
<input checked="" type="checkbox"/> Enabled	ASRRead					ASR-Operator	
<input checked="" type="checkbox"/> Enabled	ASRRoot					ASR-RootSystem	
<input checked="" type="checkbox"/> Enabled	ASRwrite					ASR-Sysadmin	

ني مدخت اسم ال / ء اي وه ال

ة ق دا ص م ل ل ني ي ل خ ا د ل ال ISE ي م د خ ت س م ا د خ ت س ا م ت ي ، ل ا ث م ال ا ذ ه ي ف : ء ط خ ال م ا ذ ه ق ا ط ن ج ر ا خ ء ي ج ر ا خ ال ء ي وه ال ر د ص م ب ض ي و ف ت ل ل و ء ق دا ص م ال ء اي ل م ع . ض ي و ف ت ل ل و ا ذ ن ت س م ال

م ا ي ق ل ل . ن ي ن ع م ال ني م د خ ت س م ل ل ه ع ف د ا ر م ال Shell ف ي ر ع ت ف ل م ف ي ر ع ت ب مق . 4 ء و ط خ ال ف ي ر ع ت ت ا ف ل م > ج ن ا ت ن ل ل > ء س ا ي س ل ل ر ص ا ن ع > ء ز ه ا ل ء ا ر ا د ا > ل م ع ل ل ز ك ا ر م ال ل ل ق ت ن ا ، ك ل ذ ب ك ل ذ ك و ر و ص ل ل ا ي ف ح ض و م وه امك د ي د ج ء ق ب ط ف ي ر ع ت ف ل م ني و ك ت ع ر م ل ل ن ك م ي . TACACS ي ه ل ا ث م ال ا ذ ه ي ف ء ر ع م ال shell ف ي ر ع ت ت ا ف ل م . ISE نم ء ق ب ا س ل ل ت ا ر ا د ا ص ل ل

1. ASR_Operator
2. ASR_RootSystem
- 3 - ASR_Sysadmin
4. Operator_with_AAA

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles

0 Selected

Refresh Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	ASR_Operator	Shell	
<input type="checkbox"/>	ASR_RootSystem	Shell	
<input type="checkbox"/>	ASR_Sysadmin	Shell	
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Operator_with_AAA	Shell	
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

Shell ل TACACS في فرع تافل م

روصل ال في حضورم وه امك ةم ي ق ل و مس ال او ل و ق ح ل ع و ن ل ا خ د ا ل ة ف ا ض ا ر ز ي ل ع ر ق ن ل ا ك ن ك م ي ة ص ص خ م ت ا م س م س ق ت ح ت .

ل غ ش م ل ا ر و د ل :

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles > ASR_Operator

TACACS Profile

Name: ASR_Operator

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege: (Select 0 to 15)
- Maximum Privilege: (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape: (Select true or false)
- Timeout: Minutes (0-9999)
- Idle Time: Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	task	nwx,#operator

Cancel Save

ي ر ذ ج ل ا م ا ط ن ل ا ر و د ل ا S R ل غ ش م ل ا ق ب ط في فرع تافل م :

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles > ASR_RootSystem

TACACS Profile

Name: ASR_RootSystem

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege (Select 0 to 15)
- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-9999))
- Idle Time (Minutes (0-9999))

Custom Attributes

+ Add Trash Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	nwc,#root-system

Cancel Save

sysadmin رودلرذجل ال ASR ماطن ةقبط فيرعت فلم

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles > ASR_Sysadmin

TACACS Profile

Name: ASR_Sysadmin

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege (Select 0 to 15)
- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-9999))
- Idle Time (Minutes (0-9999))

Custom Attributes

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	rwc_#sysadmin

Cancel Save

ضيوفتلاو ةقداصملا رودو لغشم لل ةبس نل لاسر Sysadmin ةقبط فيرعت فلم
 ةبساحملاو (AAA):

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Passiveld

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > Operator_with_AAA

TACACS Profile

Name: Operator_with_AAA

Description:

Task Attribute View | Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege (Select 0 to 15)
- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-9999))
- Idle Time (Minutes (0-9999))

Custom Attributes

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	nwc:aaa,#operator

Cancel Save

هذه الواجهة تتيح لك إعداد ملف تعريف AAA في بيئة Cisco ISE. يمكنك تخصيص إعدادات مثل Default Privilege، Maximum Privilege، Access Control List، Auto Command، No Escape، Timeout، و Idle Time. كما يمكنك إضافة سمات مخصصة (Custom Attributes) للتحكم في الوصول. في هذا المثال، تم إعداد السمة MANDATORY باسم task بقيمة nwc:aaa,#operator.

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassivelD Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences List > All_User_ID_Stores

Identity Source Sequence

Identity Source Sequence

* Name: All_User_ID_Stores

Description: A built-in Identity Sequence to include all User Identity Stores

Certificate Based Authentication

Select Certificate Authentication Profile: Preloaded_Certificate_1

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: Internal Endpoints

Selected: Internal Users, All_AD_Join_Points, Guest Users

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

Save Reset

ةراد جهن تاعومجم > ةزهألأ ةراد > لمعل زكارم يف ةقداصلال جهن نيوكتب مق. 6 ةوطخلال
 لىل يوتحي يذلا ةي وهلا نزم لسلسلت مادختسال [جهنلا ةعومجم رتخأ] > ةزهألأ
 تاعومجم مادختساب تابلطتمال لىل ءانب ضيوفتال نيوكتب مق. نييلخالل ني مدختسمل
 وه امك، ةلباقم Shell فيرعت تافل م نييعت و اق بس م اهؤاشن مت ي تال مدختسمل ةي وه
 ةروصلال يف حضورم.

Identity Services Engine Administration Work Centers License Warning

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassivelD

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Policy Sets > ASR TACACS policy

Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
ASR TACACS policy			AND DEVICE Device Type EQUALS All Device Types#ASR DEVICE Location EQUALS All Locations#LAB	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
Default			All_User_ID_Stores	0	Options

ةقداصلال جهن

دعاوقلا دن تست. بلطتمال لىل اذانتسا ةديدع قيرطب لي وختال تاسايس نيوكتب نكمي
 ةدحمال ةيلخالل مدختسمل ةي وه ةعومجم و عونلا و زاehl عقوم لىل ةروصلال يف انه ءحضورم
 راموالا تاعومجم عم لي وختال تقوي ةدحمال Shell فيرعت تافل م ع ف د متيس.

Authorization Policy - Local Exceptions			Authorization Policy - Global Exceptions			Authorization Policy (5)		
+	Status	Rule Name	Conditions	Results		Hits	Actions	
				Command Sets	Shell Profiles			
	ASR_Root_System_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-RootSystem DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	ASR_RootSystem	0		
	ASR_Sysadmin-Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Sysadmin DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	ASR_Sysadmin	0		
	ASR_Operator_AAA_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Operator-AAA DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	Operator_with_AAA	0		
	ASR_Operator_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Operator DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermitAllCommands	ASR_Operator	0		
	Default			DenyAllCommands	Deny All Shell Profile	0		

ليوختال ةسايس

ةحصلال نم ققحتال

ححص لكشب نيوكتال لمع ديكأتل مسقلا اذه مدختسا

لغشم

ف مدختسملال تالچس ةءارق دنع ةنيعملال ماهملال تاعومجمو ني مدختسملال ةعومجم نم ققحتال هوجومال.

username: ASRread

password:

```
RP/0/RSP1/CPU0:ASR9k#show user
```

```
ASRread
```

```
RP/0/RSP1/CPU0:ASR9k#show user group
```

```
operator
```

```
RP/0/RSP1/CPU0:ASR9k#show user tasks
```

```
Task:          basic-services  : READ    WRITE    EXECUTE  DEBUG
```

```
Task:                cdp      : READ
```

```
Task:                diag     : READ
```

```
Task:          ext-access  : READ          EXECUTE
```

```
Task:                logging  : READ
```

ةبساچملاو ضيوفتلاو ةقداصملا مادختساب لغشملا (AAA)

مدختسملال موقية ةءارسأدنع ةنيعملال ماهملال تاعومجمو ني مدختسملال ةعومجم نم ققحتال هوجومال ل لوخذال ليجستب

AAA ةمه ةءارق تانوذأ عم TACACS مءاخ نم اهءفدمت ل لغشملا ةمه ديدحت: ةطءالم اهذيفنت واهتباتك.

username: asraaa

password:

```
RP/0/RSP1/CPU0:ASR9k#sh user
asraaa
```

```
RP/0/RSP1/CPU0:ASR9k#sh user group
operator
```

```
RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:          aaa      : READ      WRITE      EXECUTE
Task:    basic-services : READ      WRITE      EXECUTE      DEBUG
Task:          cdp      : READ
Task:          diag     : READ
Task:    ext-access    : READ      EXECUTE
Task:    logging       : READ
```

نېداسېس

مدختس مالا موقې اتارېس اذنع ةنې عم لاهم لانا عومومو نېمدختس مالا عوموم نم ققحت لالهوم لالا لول خدلا لېجستب

```
username: asrwrite
password:
```

```
RP/0/RSP1/CPU0:ASR9k#sh user
asrwrite
```

```
RP/0/RSP1/CPU0:ASR9k#sh user group
sysadmin
```

```
RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:          aaa      : READ
Task:          acl      : READ      WRITE      EXECUTE      DEBUG
Task:          admin    : READ
Task:          ancp     : READ
Task:          atm      : READ
Task:    basic-services : READ      WRITE      EXECUTE      DEBUG
Task:          bcdl     : READ
Task:          bfd      : READ
Task:          bgp      : READ
Task:          boot     : READ      WRITE      EXECUTE      DEBUG
Task:          bundle   : READ
Task:    call-home     : READ
Task:          cdp      : READ      WRITE      EXECUTE      DEBUG
Task:          cef      : READ
Task:          cgn      : READ
Task:    config-mgmt   : READ      WRITE      EXECUTE      DEBUG
Task:    config-services : READ      WRITE      EXECUTE      DEBUG
Task:          crypto   : READ      WRITE      EXECUTE      DEBUG
Task:          diag     : READ      WRITE      EXECUTE      DEBUG
Task:          drivers  : READ
Task:          dwdm     : READ
Task:          eem      : READ      WRITE      EXECUTE      DEBUG
Task:          eigrp    : READ
Task:    ethernet-services : READ
--More--
(output omitted )
```

ېرذج ماظن

مدختسمال موقري رذجدنع ةني عمال ماهمال اناومجمو نيمدختسمال ةومجم نم ققحتال
بجمومال ال لوجدل ليجستب

```
username: asrroot
password:
```

```
RP/0/RSP1/CPU0:ASR9k#show user
asrroot
```

```
RP/0/RSP1/CPU0:ASR9k#show user group
root-system
```

```
RP/0/RSP1/CPU0:ios#show user tasks
Task:          aaa      : READ      WRITE      EXECUTE    DEBUG
Task:          acl      : READ      WRITE      EXECUTE    DEBUG
Task:          admin    : READ      WRITE      EXECUTE    DEBUG
Task:          ancp     : READ      WRITE      EXECUTE    DEBUG
Task:          atm      : READ      WRITE      EXECUTE    DEBUG
Task:          basic-services : READ      WRITE      EXECUTE    DEBUG
Task:          bcdl     : READ      WRITE      EXECUTE    DEBUG
Task:          bfd      : READ      WRITE      EXECUTE    DEBUG
Task:          bgp      : READ      WRITE      EXECUTE    DEBUG
Task:          boot     : READ      WRITE      EXECUTE    DEBUG
Task:          bundle   : READ      WRITE      EXECUTE    DEBUG
Task:          call-home : READ      WRITE      EXECUTE    DEBUG
Task:          cdp      : READ      WRITE      EXECUTE    DEBUG
Task:          cef      : READ      WRITE      EXECUTE    DEBUG
Task:          cgn      : READ      WRITE      EXECUTE    DEBUG
Task:          config-mgmt : READ      WRITE      EXECUTE    DEBUG
Task:          config-services : READ      WRITE      EXECUTE    DEBUG
Task:          crypto   : READ      WRITE      EXECUTE    DEBUG
Task:          diag     : READ      WRITE      EXECUTE    DEBUG
Task:          drivers  : READ      WRITE      EXECUTE    DEBUG
Task:          dwdm     : READ      WRITE      EXECUTE    DEBUG
Task:          eem      : READ      WRITE      EXECUTE    DEBUG
Task:          eigrp    : READ      WRITE      EXECUTE    DEBUG
```

```
--More--
(output omitted )
```

اهحالص او ااطخ ال فاشكتسا

اهحالص او نيوكتال ااطخ افاشكتسال اهم ادختسا كنكمي تامولعم مسقلا اذ رفوي

ةسدعلا زمرقوف رقنا .ةرشابملا تالجالسالا > TACACS > تايلمعمل نم ISE ريرقت نم ققحت
يليصفتال ريرقتال ضرعل ةربكمال

Refresh	Export To	Logged Time	Status	Details	Username	Type	Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
x					Username		Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
		May 14, 2018 03:35:25.792 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
		May 14, 2018 03:35:25.695 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
		May 14, 2018 03:35:25.597 PM	✓		ASRwrite	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
		May 14, 2018 03:35:12.959 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
		May 14, 2018 03:35:12.859 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
		May 14, 2018 03:35:12.771 PM	✓		ASRRoot	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
		May 14, 2018 03:34:53.788 PM	✓		ASRRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
		May 14, 2018 03:34:53.685 PM	✓		ASRRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
		May 14, 2018 03:34:53.581 PM	✓		ASRRRead	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
		May 14, 2018 03:29:46.359 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
		May 14, 2018 03:29:46.257 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
		May 14, 2018 03:29:46.150 PM	✓		ASRaaa	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22

اهحالص او ASR ااطخ افاشكتسال ةدعاسمال رماوالا ضعب هذه

- مدختسمل راهظا
- نيمدختسمل اةومجم راهظا
- مدختسمل ماهم راهظا
- لكلا مدختسمل راهظا

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب يصوت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل