

راودال اةدعاق ىل لوصول اى ف مكحتل (RBAC) Nexus N5500 و 5600 و N6000 نم

تاىوتحمل

[ةمدقملا](#)

[ةىساسال اابلطتملا](#)

[اابلطتملا](#)

[ةمدختسملا اانوكملا](#)

[مدختسملا اابلطتم](#)

[مدختسملا راودا](#)

[مدختسملا رود دعاق](#)

[مدختسملا رود عيزوت](#)

[راهظال او نيوكتلا رماوا](#)

[مدختسملا رود عيزوت ةسلج حسم](#)

[نيوكتلا لاثم](#)

[صىخرتلا اابلطتم](#)

[ةحصلا نم ققحتلا](#)

[اهالصال واطخال افاشكتسا](#)

ةمدقملا

Nexus 5500 و Nexus 5600 تالوحم ىل مدختسملا لوصول ديقت ةيفي ك دنتسملا اذو حضوي (RBAC) رودلا ىل دنتسملا لوصول اى ف مكحتل مادختساب Nexus 6000 و

هيدل اذو مدختسملا لىوخت ديقتل نيوملا مدختسملا رود دعاق دىدحتب RBAC كل حسمى لوصول ةرادا تاىلمع ىل لوصول.

و Nexus 5500 تالوحم ىل لوصول نم دحت راودا نيومتو هتراداو مدختسم باسح عاشن اكنكمى Nexus 5600 و Nexus 6000.

ةىساسال اابلطتملا

اابلطتملا

ةىلاتل عىضاوملاب ةفرعم كيدل نوكت ناب Cisco ىصوت:

- Nexus 5500 و Nexus 5600 و Nexus 6000 Switches نم رماوال رطس ةهجاو نيوكت رماوا
- Cisco نم (CFS) ةينبال تامدخ.

ةمدختسملا اانوكملا

Nexus 5500 و Nexus 5600 و Nexus تالوحم ىل دنتسملا اذو في ةدراوال تامولعمل دنتست 6000 NXOS 5.2(1)N1(9) 7.3(1)N1(1) لىغشتلا ماظن لغشت ىتلا

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجال نم دنتسملا اذه ي ف ةدراولما تامولعملما عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجالما عي مج تادب رما يال لم تحت حملما ريثاتلل كمهف نم دكأتف ، ةرشابم كتك ب ش

مدختسملا تابلطتم

اهؤا فيتسا بجي يتلا مدختسملا تابلطتم ضع ب هذه

- راودأ عاشنإ ةكبشلا ةرادا رود مهيدل نيذلا ني مدختسملل طقف نكمي .
- **ضرعلا رود** جارخا ضرع ةكبشلا لوؤسم رود مهيدل نيذلا ني مدختسملل طقف نكمي .
- جارخا ضرع مهل حمسي ال ، ضرعلا رماو عي مج ذي فنن ني مدختسملل احو مسم ناك اذا يتح ني مدختسملا ءالؤه ةكبش لوؤسم رود ني يعيت متي مل ام ، **رودلا ضرع** .
- لقالا يلع دحاو مدختسم رود يلع مدختسملا باسح يوتحي نأ بجي .

مدختسملا راودأ

ةددعتم راودأ نم اعزج مدختسم لك نوكي نأ نكمي و ني مدختسم ةدعل رود لك ني يعيت نكمي

B رودلا ني مدختسم لحمسي و show رماو رادصاب A رودلا ني مدختسم لحمسي ، لاثلما لي بس يلع نيوكتلا تاريغت عارجاب

عارجا و show رما رادصاب مدختسملا اذهل نكمي ف ، B رودلا و A رودلا نم لكل مدختسم ني يعيت مت اذا نيوكتلا يلع تاريغت

لوصولا ضفر رما يلع ةيولوالا لوصولاب حامسلا رما بس تك ي

نيوكتلا رماو يلا لوصولا ضفري رود يلا يمتنت تنك اذا ، لاثلما لي بس يلع

يلا لوصولا كي دلف ، نيوكتلا رماو يلا لوصولا هي دل رود يلا يمتنت اضيأ تنك اذا ، كلذ عم و نيوكتلا رماو

ةيضا رتفا مدختسم راودأ ةسمخ كانه :

- network-admin - لوصولا يلا ةباتكلا و ءارقلا لوصولا
- لوصولا يلا ءارقلا لوصولا - ءكبشلا لوصولا
- VDC يلع رصتقي ءباتكلا و ءارقلا لوصولا - vdc-admin
- VDC يلع روصقم ءارقلا لوصولا - vdc ل غشم
- SAN يلوؤسم ل ءباتكلا و ءارقلا لوصولا - SAN-Admin

ةيضا رتفال مدختسملا راودأ فذح/لي دعت كنكمي ال : **عظالم**

لوصولا يلع حاتملا رودلا **show role** رمالا ضري : **عظالم**

مدختسملا رود دعاوق

ام رودل ياساسال رصنعلا يه ءدعاقل

اهذي فنن تب مدختسملل رودلا لحمسي يتلا تاي لمعلا ءدعاقل ددحت

تامل عمل هذه دعاوق قيبطت كنكمي:

- يداع ريبعت يف ةفرعمل رماوالا نم ةعومجم وأ رمأ-رماأ.
 - NX-OS جم انرب اهرفوي ةفيظو ىلع قبطنت رماوأ-ةزيملا.
 - مدختسملا لبق نم ةفرعمل وأ ةيضارتفالا تازيملا ةعومجم -تازيملا ةعومجم.
- رماأ يه ةيساسألا مكحتلا ةملمع .ةيمره ةقالع ءاشنإب تامل عمل هذه موقت

ةزيملاب ةنرتقملا رماوالا عيمج لثمت يتلاو ،ةزيملا يه ةيلاتلا مكحتلا ةملمع

ةلصللا تاذ تازيملا تازيملا ةعومجم عمجت .تازيملا ةعومجم يه ةريخألا مكحتلا ةملمع .ةلوهسب دعاوقلا ةرادب كل حمستو

هب دعاوقلا قيبطت متي يذلا بيترتلا مدختسملا لبق نم ددحمل ةدعاوقلا مقر ددحي

يلزانت بيترتب دعاوقلا قيبطت متي

ىلا امو ،3 ةدعاوقلا لبق قبطت يتلا ،2 ةدعاوقلا لبق 1 ةدعاوقلا قبطت ،لاثملا لىبس ىلعف لك.

مقر نم ةدعاوقلا لك نوكتت .نيعم رود ةطساوب اهذيفنت نكمي يتلا تايلمعلا ةدعاوقلا رمأ ددحي ،(ضفرلا وأ حامسلا) ةدعاوقلا عونو ةدعاوقلا

ىلع) يرايخا ةزيم مساو (debug و execو ضرعلاو نيوكتلا ،لاثملا لىبس ىلع) رمأ عون (ةهجاو و VTP و HSRP و FCOE ،لاثملا لىبس

مدختسملا رود عيزوت

Cisco Fabric Services تامدخل ةيساسألا ةينبلا راودألا ىلا ةدنتسملا تانيوكتلا مدختست يف نيوكتلا ةدحاو ةطقن ريفوتلو تانايبلا ةدعاوقلا ةلاعفل ةرادإلا نيكمتل (CFS) ةكبشلا

يوتحت CFS ةقطنم ىلا زاهجلا يمتني ،كزاهج ىلع ةزيملا CFS عيزوت نيكمتب موقت امدنع لىطعت متي .ةزيملا ل CFS عيزوتل اهنيكمتب اضيا تمق يتلاو ةكبشلا يف ىرخأ ةزهجأ ىلع يضرارتفالكشب مدختسملا رود ةزيملا CFS عيزوت

هبلع نيوكتلا تاريغت عيزوت ديرت زاهج لك ىلع مدختسملا راودألا CFS نيكمتب بحي

لخدت تنأ نأ رمأ رود لمعتسم لوأ ،حاتفملا ىلع لمعتسم راودألا عيزوت CFS تنأ نكمي نأ دعب ةيلمع اذه ذخأي نأ ةيجمرب NX-OS حاتفملا بلسي:

1. حاتفملا ىلع CFS ةسلج ئشنني
 2. CFS نيكمتم عم CFS ةقطنم يف تالوحملا عيمج ىلع مدختسملا رود نيوكت نيامت .مدختسملا رود ةزيملا
 3. لوحملا ىلع تقؤم تقؤم نزخم يف مدختسملا رود نيوكت تاريغت ظفح
- ميتل حيرص لكشب اهمازللاب موقت نأ ىلا لوحملا ىلع تقؤملا نزخملا يف تاريغتلا ىقبت CFS ةقطنم يف ةزهجالا ىلع اهعيزوت

تاءارجإلا هذه ذاختاب NX-OS جم انرب موقبي ،تاريغتلا ذيفنتب موقت امدنع

1. لوجملا ىلع هليغشت ىراجلا نيوكتلا ىلع تاريخيغتللا قىببطت.
2. CFS ةقطنم ىف ىرخألا تالوجملا ىلا ثدحملا مدختسملا رود نيوكت عيزوت.
3. CFS ةقطنم ىف ةدوجوملا ةزهجالا ىف مدختسملا رود نيوكت نيماأ اغلا.
4. CFS ةسلاج يهني.

تانويكوتلا هذه عيزوت متي:

- فاصوأل او راودأل امامسأ
- راودأل دعاوق ةمئاق

راهظال او نيوكتلا رماو

ضرغلا

ةدحول نيوكت
ةيفرطلا

لاثم ةوطخلا

1. switch# configure
terminal

switch(config)#

رودلا مسا / رودلا مسا

لاثم ةوطخلا

2. switch(config)# role
name userA

switch(config-role)#

vlan ةسايس صفر

لاثم ةوطخلا

3. switch(config-role)#vlan
switch(config-role-vlan)#

allowed vlan vlan-id

لاثم ةوطخلا

4. switch(config-role-
vlan)#allowed vlan 1

جرخم

لاثم ةوطخلا

5. switch(config-role-vlan)#
exit

switch(config-role)#

رودلا راهظا

لاثم ةوطخلا

6. switch(config-
role)#show role

العمل {رودلا راهظا

diff-قلم

لاثم ةوطخلا

7. switch(config-role)#
show

رودلا مازتلا

لاثم ةوطخلا

8. switch(config-role)# role
commit

بولسأ ليكشت لماش لخدي

رودلا نيوكت عضو لاخداو مدختسم رود ديحت

بولسأ ليكشت ةسايس vlan رود لخدي

اهيلا لوصول رودلا نكمي يتلا VLAN ةكبش ددحي
ةجالحا بسح VLAN تاكبش لكل رمألا اذه ررك

بولسأ ليكشت ةسايس vlan رود نم جورخلا

رودلا نيوكت ضرعي (ىرايخا)

عيزوتلل قلم عمل مدختسملا رود نيوكت ضرعي (ىرايخا)

ةدعاق ىف مدختسملا رود نيوكت تاريخيغتللا قىببطت (ىرايخا)
رود نيوكت عزوتو ىراجلا نيوكتلا ىلع ةتقوملا تانايبلا
نيوكت عيزوت نيكمتب تمق اذا ىرخألا تالوجملا ىلع مدختسملا
مدختسملا رود ةزيمل CFS

copy running-config

startup-config

9. ةوطخلال
لاثم:

switch#copy running-
config startup-config

ءدب نيوكت ىلإ هليغشت يراجلا نيوكتلا خسنا (يرايخا) ليغشتلا.

رودلا نيوكت عيزوت تاوطخلال هذه نكمت

ضرغلا

1. ةوطخلال switch# config t
switch(config)#

ببولسأ ليكشت لخددي

2. ةوطخلال switch(config)#
switch(config)#no role distribute

راودألا نيوكت عيزوت نيكمت (يضارتفالال) راودألا نيوكت عيزوت ليطعت

رودلا نيوكت تاريغيغت عارجاب تاوطخلال هذه موقت

ضرغلا

1. ةوطخلال Nexus# config T
Nexus(config)#

ببولسأ ليكشت لخددي

رودلا نيوكت تاريغيغت ب مازتلال Nexus(config)# رود مازتلا 2 ةوطخلال

رودلا نيوكت تاريغيغت تاوطخلال هذه لهاجتت

ضرغلا

1. ةوطخلال Nexus# config T
Nexus(config)#

ببولسأ ليكشت لخددي

2. ةوطخلال Nexus(config)#
رودلا

نيوكتلا تانايب ةدعاق حسمي و رودلا نيوكت تاريغيغت لهاجتتي ةقلعلا

ةيلاتلال ماهملا نم ةدحاو ذيفنتب مق ،مدختسمل باسحو RBAC نيوكت تامولعم ضرعلا

ضرغلا

رودلا راهظا

مدختسمل رود نيوكت ضرع

رودلا ةزيم راهظا

تازيمل ةمئاق ضرعي

تازيمل ةومجم نيوكت ضرع رودلا تازيم ةومجم راهظا

مدختسمل رود عيزوت ةسلج حسم

ةينبلا نيمأت عاغلإو ةيراجلا (تدجو نإ) Cisco Fabric تامدخ عيزوت لمع ةسلج حسم كنكمي مدختسمل رود ةزيملا

رمألا اذه رادصا دنع ةقلعلا تانايبلا ةدعاق ي ف تاريغيغت ي أ دق ف متيس :ريذحت

ضرغلا

1. ةوطخلال switch#
لاثم:

جيسنلا نيمأت عاغلإو لمعلا ةسلج حسم

رودلا لمع ةسلج حسم
رودلا لمع ةسلج ةلاح راهظا

2. ةوطخلال
لاثم:

مدختسمل رود CFS ةسلج ةلاح ضرعي (يرايخا)

رودلا لمع ةسلج ةلاح ضرع switch#

نڀوكتلا لاثم

اذه لوصولا نذا مادختساب مدختسم باسحل TAC عاشناب موقنس ،لاثلما اذه يف

- حضاو رما ىلى لوصولا
- نڀوكتلا رما ىلى لوصولا
- اياطال احيصت رما ىلى لوصولا
- ىلى لوصولا EXEC رما
- show رمالا ىلى لوصولا
- طقف 1-10 VLAN ةكبش ىلى لوصولا

```
C5548P-1# config t
Enter configuration commands, one per line. End with CNTL/Z
C5548P-1(config)# role name Cisco
C5548P-1(config-role)# rule 1 permit command clear
C5548P-1(config-role)# rule 2 permit command config
C5548P-1(config-role)# rule 3 permit command debug
C5548P-1(config-role)# rule 4 permit command exec
C5548P-1(config-role)# rule 5 permit command show
C5548P-1(config-role)# vlan policy deny
C5548P-1(config-role-vlan)# permit vlan 1-10
C5548P-1(config-role-vlan)# end
```

```
C5548P-1# show role name Cisco
```

```
Role: Cisco
Description: new role
vsan policy: permit (default)
Vlan policy: deny
Permitted vlans: 1-10
Interface policy: permit (default)
Vrf policy: permit (default)
```

Rule	Perm	Type	Scope	Entity
5	permit	command		show
4	permit	command		exec
3	permit	command		debug
2	permit	command		config
1	permit	command		clear

```
C5548P-1#
C5548P-1# config t
Enter configuration commands, one per line. End with CNTL/Z.
C5548P-1(config)# username TAC password Cisco123 role Cisco
```

```
C5548P-1(config)# show user-account TAC
user:TAC
    this user account has no expiry date
    roles: Cisco
```

صڀخرتلا تابلطتم

صڀخرتلا تابلطتم جتنملا
صڀخرت ي RBAC و نڀمدختسملا تاباسح بلطتت ال NX-OS

ةحصلا نم ققحتلا

نڤوكتلا اذه ةحص نم ققحتلل ءارجل ايلاح دجوي ال

اهحالصإو ءاطخأل فاشكتسا

نڤوكتلا اذهل اهلصإو ءاطخأل فاشكتسال ةددم تامولعم ايلاح رفوتت ال

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچي ف ني مدختسمل معد يوتحم مي دقتل ل ي رش بل او
امك ة قيق د نوك ت نل ةلأل ة مچرت ل ضفأ نأ ة ظحال م ي جزي . ة صاغل م هت غ لب
Cisco ي لخت . فرتحم مچرت م ا همدقي ي تلل ة ي فارتحال ة مچرتل عم ل ا حل او ه
ى ل ا مئاد عوچرلاب ي صؤت و ت ا مچرتل هذه ة ق د ن ع اهت ي ل وئى سم Cisco
Systems (رفو تم طبارل) ي ل صأل ا ي زيل چن إل ا دن تسمل ا