

ىلع ةصصخملا ةيصلنلا جماربلا نيوكت CPAR 8.0

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ةرداصللا رورملا ةكرحل يلخاد يصلن جمارب](#)

[ةدراوللا رورملا ةكرحل يلخاد يصلن جمارب](#)

[يجراخ يصلن جمارب عاشنا](#)

ةمدقملا

Cisco Prime Access Registrar (CPAR) 8.0 كولس صي صخت ةيفيكي دننتمسلا اذه فصوي قرحملا طاقنو ةيصلنلا جماربلا مادختساب.

ةيساسألا تابلطتملا

تابلطتملا

ةيلالتلا عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت:

- CPAR 8.0 ةرادا

ةمدختسملا تانوكملا

ةيلالتلا ةيداملا تانوكملاو جماربلا تارادصلا لىل دننتمسلا اذه يف ةدراوللا تامولعملا دننتمست:

- CPAR 8.0 لىل CentOS 6.5 تب 64 رادصلا

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالا نم دننتمسلا اذه يف ةدراوللا تامولعملا عاشنلا مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دننتمسلا اذه يف ةمدختسملا ةزهجالا عيمج تادب رما يال لمتمحمللا ريثاتلل كمهف نم دكأتف، ليغشنتلا دي قكتك تبش.

ةيساسأ تامولعم

ةباتك نكمي. ءاوس دح لىل عي جراخللاو ةيلخادلا ةيصلنلا جماربلا ةطساوب CPAR ليدعت نكمي مزح ةجلاعم ليدعتل ةيصلنلا جماربلا مادختسلا نكمي. C/C++/Java/TCL يف ةيصلنلا جماربلا طاقن يف CPAR يف ةيصلنلا جماربلا لىل ةراشال نكمي. رطقللاو TACACS و RADIUS لىل ةراشالاب حمستو نيوكتلا رصانع ضعيب تحت رهظت ةمس/دادعلا يه دادتمالا طاقن. دادتمالا نعل ةلوؤسم تسيلا (CPAR) مكحتلا يوتسم ةيامح نإف [يعجرملا لىل دلل](#) اقفو. يصلنلا جمارب

ةصصخلملةصنللماربللمبسبلكلذريغواتايفلتواتانايبللدقفيأ

لكشنتأداةكبشنتحتةطقندادتمانانثانملاثمنه

```
[ //localhost/Radius/Clients/piborowi ]
Name = piborowi
Description =
Protocol = tacacs-and-radius
IPAddress = 192.168.255.15
SharedSecret = <encrypted>
Type = NAS
Vendor =
IncomingScript~ = // Extension point for incoming traffic
OutgoingScript~ = // Extension point for outgoing traffic
EnableDynamicAuthorization = FALSE
NetMask =
EnableNotifications = FALSE
EnforceTrafficThrottling = TRUE
```

ةحاتملا دادتمالاطاقنمديدعلكانه، (CPAR) مكحتلليوتسمةيامحةرادلليلدلاقفو
ةليلاللقلمالاطاقنملكيف دراويصنجمانربىلإةراشإللكمفي

- مداخل RADIUS
- (رشابملا ليمعلا) دروملا
- (ةيدرفلا (NAS) ةكبشلاب ةلصتلملنيختلتادحو) ليمعلا
- NAS-Vendor-behind-proxy
- ليكولءارو ليمعلا
- (RADIUS عونللم) ديعبلمداخل
- ةمدخل

ققلمالاطاقنمةطقنلكيفليوختللاوأةقداصمللليصنجمانربىلإةراشإللكمفي
ةليلال:

- ةومجملةقداصم
- مدختسمللةقداصم
- ةومجملاضيوفت
- مدختسمللاضيوفت

ةليلاللقلمالاطاقنملكيفرداصلليصنللماربللىلإعوجرللكمفي

- ةمدخل
- ليكولءارو ليمعلا
- NAS-Vendor-behind-proxy
- (ةيدرفلا (NAS) ةكبشلاب ةلصتلملنيختلتادحو) ليمعلا
- دروم NAS
- مداخل RADIUS

ىوتسمةيامحةطساوبةيصنللماربللذيفنتهلخالنممتيذليذلبيترتلمهفمهملانم
[لئوسملا ليلد](#) نم 7-1 لودجلاىلإعجرا. ةددعتمدادتماطاقندوجولارظن (CPAR) مكحتللا
ةرفوتمدادتما/ةجمربةطقن29 بيترتىلععالطالل

(CLI) رماوالرطسةهجاويفرشابمهنىوكتمتيذلىوهيلخادلاليصنللماربللإن
ةفرعملنمريثكللاو ةيجراختافلمايابللطيالهنإن (CPAR) (aregcmd) دروملاةئيففرعمل
ليغشتللماظنفيفلمفيهنيزختمتيذلىوهيجراخلليصنللماربلل. ةجمربلليفي
CPAR تاجللمب ةصاخلا (CLI) رماوالرطسةهجاويفطقفهيلراشيو (RHEL أو CENTOS)

نيوكتلا

قرداصللا رورملا ةكرحل يلخاد يصن جم انرب

تال دعمل هذه مادختسا كنكمي ةيلخادلا ةيلعافتلا صوصنلا ي:

1. +RSP: - درلل ةمسو ةفاضلا
2. -rsp: - ةباجتسالال نم ةمسالال ليزي
3. #rsp: - ةديج ةميقب ةمسالال لدبتسي
4. ةلثمألا (ةئيبلال سوماق وهو، env و ةمزحلال لابقتسا/ابلط) req ل هالعأ مادختسا كنكمي +req: أو -env:

نم نيونثا نيوكتب مق. ةيذيفنتلا صوصنلا/RADIUS/ تحت يلخاد يذيفنت صن ةفاضلا مامضنالال) vendor-specific و filter-id: لوصولال لوبق ةمزح عم مهعاجرا متيل نييفاضلا AVP (توصولال لاجم ي).

```
--> ls -R
```

```
[ //localhost/Radius/Scripts/addattr ]
  Name = addattr
  Description =
  Language = internal
  Statements/
    1. +rsp:Filter-Id=PhoneACL
    2. +rsp:Cisco-AVPair=device-traffic-class=voice
```

```
--> ls -R
```

```
[ Services/local-users ]
  Name = local-users
  Description =
  Type = local
  IncomingScript~ =
  OutgoingScript~ = addattr
  OutagePolicy~ = RejectAll
  OutageScript~ =
  UserList = Default
  EnableDeviceAccess = True
  DefaultDeviceAccessAction~ = DenyAll
  DeviceAccessRules/
    1. switches
```

يلحملال client مدار مادختساب رابتخا:

```
--> simple
```

```
p011
--> p011 send
```

p014

--> **p014**

Packet: code = Access-Accept, id = 18, length = 64, attributes =
Filter-Id = PhoneACL
Cisco-AVPair = device-traffic-class=voice

تاریخات:

```
07/31/2019 10:31:26.254: P2363: Running Service local-users's OutgoingScript: addattr
07/31/2019 10:31:26.254: P2363: Internal Script for 1 +rsp:Filter-Id=PhoneACL : Filter-Id =
PhoneACL
07/31/2019 10:31:26.254: P2363: Setting value PhoneACL for attribute Filter-Id
07/31/2019 10:31:26.254: P2363: Trace of Response Dictionary
07/31/2019 10:31:26.254: P2363: Trace of Access-Request packet
07/31/2019 10:31:26.254: P2363:     identifier = 18
07/31/2019 10:31:26.254: P2363:     length = 30
07/31/2019 10:31:26.254: P2363:     respauth = fb:63:14:3f:c1:fb:ac:03:7d:16:29:61:ba:ef:13:4f
07/31/2019 10:31:26.254: P2363:     Filter-Id = PhoneACL
07/31/2019 10:31:26.254: P2363: Internal Script for 2 +rsp:Cisco-AVPair=device-traffic-
class=voice : Cisco-AVPair = device-traffic-class=voice
07/31/2019 10:31:26.254: P2363: Setting value device-traffic-class=voice for attribute Cisco-
AVPair
07/31/2019 10:31:26.254: P2363: Trace of Response Dictionary
07/31/2019 10:31:26.254: P2363: Trace of Access-Request packet
07/31/2019 10:31:26.254: P2363:     identifier = 18
07/31/2019 10:31:26.254: P2363:     length = 64
07/31/2019 10:31:26.254: P2363:     respauth = fb:63:14:3f:c1:fb:ac:03:7d:16:29:61:ba:ef:13:4f
07/31/2019 10:31:26.254: P2363:     Filter-Id = PhoneACL
07/31/2019 10:31:26.254: P2363:     Cisco-AVPair = device-traffic-class=voice
```

ةدراولا رورملا ةكرحل يلخاد يصن جم انرب

قيسنتللا في ني مدختسملا عامسأ لك لدبتسي دي دج يذيفنت صن عاشن اب مق
اهمدختست يتلا ةمدخلل نمضم يصن جم انربك هق يبطت ب مق ولوه جم لى | user@domain

ن ي وكتلا:

```
--> cd /Radius/Scripts

--> add test

--> set language internal

--> cd Statements

--> add 1

--> cd 1

--> set statements "#req:User-Name=~(.*)@[a-z]+.[a-z]+~\anonymous"

--> ls -R
```

```
[ //localhost/Radius/Scripts/test ]
Name = test
Description =
Language = internal
Statements/
```

```
1. #env:User-Name=~(.*)~anonymous
```

```
--> ls -R /Radius/Services/employee-service/
```

```
[ /Radius/Services/employee-service ]
Name = employee-service
Description =
Type = local
IncomingScript~ = test
OutgoingScript~ =
OutagePolicy~ = RejectAll
OutageScript~ =
UserList = default
EnableDeviceAccess = FALSE
DefaultDeviceAccessAction~ = DenyAll
```

إلى مدخستسمال مسا ريغت مت هنأل حجأالآىل ع بلطالض فرمت (RADCLIENT عم رابتخ|
لوهجم):

```
--> simple
```

```
p01e
```

```
--> p01e
```

```
Packet: code = Access-Request, id = 27, length = 72, attributes =
User-Name = <username>@cisco.com
User-Password = <password>
NAS-Identifier = localhost
NAS-Port = 7
```

```
--> p01e send
```

```
p020
```

```
--> p020
```

```
Packet: code = Access-Reject, id = 27, length = 35, attributes =
Reply-Message = Access Denied
```

عبتال:

ىوتسم ةيامح يعدتست. ةيصن جمارب ةثالث اعادتسإ متي، فظومال ةمدخ ذي فنن لبق
ق فرملال ParseServiceHints اعادتسإب موقت مت، CiscoIncomingScript لوالال (CPAR) مكحتال
يف هعضيو ةمزحل نم مدخستسمال مسا جرتسي. ةلحملال ةكبشلال زاخ/للم مع نيوكتب
مدخستسمال مسا ريغت مت و رابتخال اعادتسإ مت، يثالال يصنلال جمانربال. ةئيبال سوماق
لوهجم إلى <username> نم ةئيبال سوماق يف

يلحملال فيضالمالي عم:

```
[ //localhost/Radius/Clients/localhost ]
Name = localhost
Description =
Protocol = radius
IPAddress = 127.0.0.1
SharedSecret = <encrypted>
Type = NAS+Proxy
Vendor = Cisco
IncomingScript~ = ParseServiceHints
```

```
OutgoingScript~ =
EnableDynamicAuthorization = FALSE
NetMask =
EnableNotifications = FALSE
EnforceTrafficThrottling = TRUE
```

جارخا اإا عبتت:

```
07/31/2019 11:38:53.522: P2855: PolicyEngine: [SelectPolicy] Successful
07/31/2019 11:38:53.522: P2855: Using Client: localhost
07/31/2019 11:38:53.522: P2855: Using Vendor: Cisco
07/31/2019 11:38:53.522: P2855: Running Vendor Cisco's IncomingScript: CiscoIncomingScript
07/31/2019 11:38:53.522: P2855: Running Client localhost IncomingScript: ParseServiceHints
07/31/2019 11:38:53.522: P2855: Rex: environ->get( "Request-Type" ) -> "Access-Request"
07/31/2019 11:38:53.522: P2855: Rex: environ->get( "Request-Type" ) -> "Access-Request"
07/31/2019 11:38:53.522: P2855: Rex: environ->get( "User-Name" ) -> "<username>"

07/31/2019 11:38:53.522: P2855: Authenticating and Authorizing with Service employee-service
07/31/2019 11:38:53.522: P2855: Running Service employee-service's IncomingScript: test
07/31/2019 11:38:53.522: P2855: Numbered attribute got for the radius / tacacs packet. ignoring
# User-Name
07/31/2019 11:38:53.523: P2855: Numbered attribute got for the radius / tacacs packet. ignoring
# User-Name
07/31/2019 11:38:53.523: P2855: Numbered attribute got for the radius / tacacs packet. ignoring
# User-Name
07/31/2019 11:38:53.523: P2855: Internal Script for 1 #env:User-Name=~(.*)~anonymous : User-
Name = anonymous
07/31/2019 11:38:53.523: P2855: Setting value anonymous for attribute User-Name
07/31/2019 11:38:53.523: P2855: Trace of Environment Dictionary
07/31/2019 11:38:53.523: P2855: User-Name = anonymous
07/31/2019 11:38:53.523: P2855: NAS-Name-And-IP-Address = localhost (127.0.0.1)
07/31/2019 11:38:53.523: P2855: Authorization-Service = employee-service
07/31/2019 11:38:53.523: P2855: Source-Port = 51169
07/31/2019 11:38:53.523: P2855: Authentication-Service = employee-service
07/31/2019 11:38:53.523: P2855: Trace-Level = 1000
07/31/2019 11:38:53.523: P2855: Destination-Port = 1812
07/31/2019 11:38:53.523: P2855: Destination-IP-Address = 127.0.0.1
07/31/2019 11:38:53.523: P2855: Source-IP-Address = 127.0.0.1
07/31/2019 11:38:53.523: P2855: Enforce-Traffic-Throttling = TRUE
07/31/2019 11:38:53.523: P2855: Request-Type = Access-Request
07/31/2019 11:38:53.523: P2855: Script-Level = 6
07/31/2019 11:38:53.523: P2855: Provider-Identifier = Default
07/31/2019 11:38:53.523: P2855: Request-Authenticator =
5f:62:5a:72:0f:7b:a2:2a:9c:06:ba:2e:bd:f4:e4:4b
07/31/2019 11:38:53.523: P2855: Realm = cisco.com
07/31/2019 11:38:53.523: P2855: Getting User anonymous's UserRecord from UserList Default
07/31/2019 11:38:53.523: P2855: Failed to get User anonymous's UserRecord from UserList Default
07/31/2019 11:38:53.523: P2855: Running Vendor Cisco's OutgoingScript: CiscoOutgoingScript
07/31/2019 11:38:53.523: P2855: Trace of Access-Reject packet
07/31/2019 11:38:53.523: P2855: identifier = 27
07/31/2019 11:38:53.523: P2855: length = 35
07/31/2019 11:38:53.523: P2855: respauth = d3:7d:b3:f6:05:47:2c:66:d9:c0:01:7d:67:d7:93:99
07/31/2019 11:38:53.523: P2855: Reply-Message = Access Denied
07/31/2019 11:38:53.523: P2855: Sending response to 127.0.0.1
```

ي ج ر ا خ ي ص ن ج م ا ن ر ب ء ا ش ن ا

ي و ت ح م ل ا ا ذ ه ة ف ا ض ا و ل ي ل د /opt/ciscoAr/scripts/radius/tcl/ ن ا د ي ا ف ل م ة ف ا ض ا

```
[root@piborowi-cpar80-16 tcl]# cat /opt/CSCOar/scripts/radius/tcl/nadip.tcl
proc UpdateNASIP {request response environ} {
$request trace 2 "TCL CUSTOM_SCRIPT Updating NAS IP ADDRESS"
$request trace 2 "Before put: " [ $request get NAS-IP-Address ]
$request put NAS-IP-Address 1.2.3.4
$request trace 2 "After put: " [ $request get NAS-IP-Address ]
}
```

رطسب ارطس *nadip.tcl* ىوتحم حرش:

سيموق ةثالثو يحاوضلالو ةباجتسالو بلطلال. تاطيسوللو ءارجلال فيرعت لوألارطسلال ةمزحلل/لمعلال ةسلج تانايب ليذعت كنكمي شي ةرفوتل.

2. عبتت ىوتسمك هتعباط متيس يذلال يصنلال صنللل ءاطخالل حيحصت رطس 2 مقرر رطسلال.

ةميقلال هذه نييعت لبق بلطلال سوماق في NAS-IP ناوع ةمس ىوتحم 3 مقرر رطسلال.

1.2.3.4. ةميقلال ىلع بلطلال سوماق في NAS-IP ناوع ةمس نييعت ب مق 4 مقرر رطسلال.

ىرخأ ةرم NAS-IP ناوع ةمس ةعباط 5 مقرر رطسلال.

ىل CPAR عجرم نيوكتب مق، ليغشتلال ماظن في هظفحو يصنلال جمانربلال ءاشنل درجمب (هذه في) قحلم عم اقيقد فللمل مسانو كي نأ بجي، TCL كةغلل نييعت. يصنلال جمانربلال يصنل جمانربك هذيفنت ديرت يذلال فللمل في ءارجلال مساو وه *nadip.tcl*. *EntryPoint* مادختساب هرابتخاو (*IncomingScript*) ةمدخلال تحت CPAR ل يصنل جمانرب ءاشنل ب عجرملا ماق *Radclient*.

عبتتلال في 5 مقرر، 3 مقرر، 2 مقرر رطسألل ءظحاللم نكمي:

```
--> ls -R /Radius/scripts/nadipaddress/
```

```
[ /Radius/Scripts/nadipaddress ]
  Name = nadipaddress
  Description =
  Language = tcl <<<<<<<<
  Filename = nadip.tcl <<<<<<<<
  EntryPoint = UpdateNASIP <<<<<<<<
  InitEntryPoint =
  InitEntryPointArgs =
```

```
--> ls -R /Radius/services/employee-service/
```

```
[ /Radius/Services/employee-service ]
  Name = employee-service
  Description =
  Type = local
  IncomingScript~ = nadipaddress <<<<<<<<
  OutgoingScript~ =
  OutagePolicy~ = RejectAll
  OutageScript~ =
  UserList = default
  EnableDeviceAccess = FALSE
  DefaultDeviceAccessAction~ = DenyAll
```

عبتتلال:

```
07/31/2019 13:40:53.615: P3490: Running Service employee-service's IncomingScript: nadipaddress
07/31/2019 13:40:53.615: P3490: TCL CUSTOM_SCRIPT Updating NAS IP ADDRESS
07/31/2019 13:40:53.616: P3490:      Tcl: request trace 2 TCL CUSTOM_SCRIPT Updating NAS IP
ADDRESS -> OK
07/31/2019 13:40:53.616: P3490:      Tcl: request get NAS-IP-Address -> <empty>
07/31/2019 13:40:53.616: P3490: Before put:
07/31/2019 13:40:53.616: P3490:      Tcl: request trace 2 Before put:      -> OK
07/31/2019 13:40:53.616: P3490:      Tcl: request put NAS-IP-Address 1.2.3.4 -> OK
07/31/2019 13:40:53.616: P3490:      Tcl: request get NAS-IP-Address -> 1.2.3.4
07/31/2019 13:40:53.616: P3490: After put: 1.2.3.4
07/31/2019 13:40:53.616: P3490:      Tcl: request trace 2 After put:  1.2.3.4 -> OK
```


ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد ىوتحم مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتحم مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوءو تاملرتل هذه ةقء نء اهءل ءوئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل