Aangepaste scripts op CPAR 8.0 configureren

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Prime Access Registrar (CPAR) 8.0-gedrag kunt aanpassen met behulp van scripts en extensiepunten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CPAR 8.0 toediening

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CPAR 8.0 geïnstalleerd op CentOS 6.5 64-bits

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

CPAR kan aangepast worden door zowel interne als externe scripts. De scripts kunnen worden geschreven in C/C++/Java/TCL. De handleidingen kunnen worden gebruikt om de verwerking van de pakketten RADIUS, TACACS en DIAMETER aan te passen. De scripts kunnen in CPAR in extensiepunten worden genoemd. Extension points is een instelling/eigenschap die wordt weergegeven onder bepaalde configuratieelementen en die een script kan verwijzen. Volgens referentie gids is CPAR niet verantwoordelijk voor gegevensverlies, schade, etc. veroorzaakt door

aangepaste scripts.

Hier is een voorbeeld van twee verlengingspunten onder de configuratie van het netwerkapparaat

```
[ //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 incomming traffic
    OutgoingScript~ =                          // Extension point for outgoing traffic
    EnableDynamicAuthorization = FALSE
    NetMask =
    EnableNotifications = FALSE
    EnforceTrafficThrottling = TRUE
```

Volgens de CPAR toedieningsgids zijn er meerdere beschikbare verlengingspunten. Een inkomend script kan worden gebruikt op elk van deze extensiepunten.

- RADIUS-server
- Verkopers (van de onmiddellijke client)
- Cliënt (afzonderlijke NAS)
- NAS-verkoper achter-de-proxy
- Clientachter-de-proxy
- Remote Server (van type RADIUS)
- Service

Een authenticatie- of autorisatiemanager kan op elk van deze extensiepunten worden vermeld:

- Groepsverificatie
- Gebruikersverificatie
- groepsautorisatie
- Gebruikersautorisatie

Het uitgaande script kan op elk van deze extensiepunten worden vermeld:

- Service
- Clientachter-de-proxy
- NAS-verkoper achter-de-proxy
- Cliënt (afzonderlijke NAS)
- NAS-verkoper
- RADIUS-server

Het is van cruciaal belang de volgorde te begrijpen waarin scripts worden uitgevoerd door CPAR omdat er meerdere extensiepunten zijn. Raadpleeg tabel 7-1 van de beheerdershandleiding om de volgorde van 29 beschikbare scripting/extensiepunten te zien.

Een intern script is een script dat direct is ingesteld in CPAR CLI (aregcmd). Er zijn geen externe bestanden en veel programmeerkennis voor nodig. Een extern script is een script dat opgeslagen is in een bestand in een besturingssysteem (CENTOS of RHEL) en dat net is vermeld in CPAR CLI.

Configureren

Interne scripts voor uitgaande verkeer

In interne scripts kunt u deze modificatoren gebruiken:

1. +rsp: - voegt de reactie toe en wijst deze toe

2. -rsp: - verwijdert eigenschap van respons

3. #rsp: - eigenschap door nieuwe waarde vervangen

4. U kunt het bovenstaande gebruiken voor req (aanvragen/samenvoegen van pakketjes en env, dat een omgevingswoordenboek is). Voorbeelden +req: of -env:

Voeg een intern script toe onder /Radius/scripts. Configureer twee extra AVP die met het pakket Access-Accept moeten worden teruggegeven: Filter-ID en leverancierspecifieke (om zich aan te sluiten bij stemdomein).

```
--> 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
```

Test met het gebruik van een lokale radioclient:

```
--> simple




p011
--> p011 send
```

```
p014
--> p014
Packet: code = Access-Accept, id = 18, length = 64, attributes =
        Filter-Id = PhoneACL
        Cisco-AVPair = device-traffic-class=voice
```

Traces:

```
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
```

Interne scripts voor inkomend verkeer

Maak een nieuw script dat alle gebruikersnamen in formaat user@domain vervangt en gebruik dit als samengevoegd script voor de service die u gebruikt.

Configureren:

```
--> 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
```

Test met radclient (verzoek wordt waarschijnlijk afgewezen omdat de gebruikersnaam is veranderd in anoniem):

```
--> 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
```

Overtrekken:

Voordat de medewerkster-dienst wordt uitgevoerd, worden er drie scripts gevraagd. Eerst CPAR roept *CiscoInkomendScript op*, dan maakt het *gebruik van ParseServiceHints* die aan de lokale configuratie van de client/het apparaat van het netwerk zijn verbonden. Hiermee wordt de gebruikersnaam uit het pakket geëxtraheerd en in het omgevingswoordenboek geplaatst. Tweede script, *test* wordt gebruikt en gebruikersnaam in omgevingswoordenboek wordt veranderd van <gebruikersnaam> in anoniem

localhost-client:

```
[ //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
```

Uitvoer overtrekken:

```
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-IPAddress = 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
```

Externe scripts maken

Voeg een bestand *nadip.tcl toe* aan /opt/CSCOar/scripts/Straal/tcl/folder en voeg deze inhoud toe:

```
[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 ]
}
```

Inhoud van *nadip.tcl* wordt per regel uitgelegd:

Lijn 1 Procedure definitie en argumenten Aanvragen, beantwoorden, environ en drie beschikbare woordenboeken waar u sessie-/pakketgegevens kunt wijzigen.

Line #2 Debug line voor script dat als overtrek niveau 2 wordt afgedrukt.

Line #3 Content van de eigenschap NAS-IP-Address in request-woordenboek voordat u deze waarde instelt.

Lijn #4 Stel de eigenschap Nas-IP-Adres in het gevraagde woordenboek in op waarde 1.2.3.4.

Line #5 Print NAS-IP-Address opnieuw.

Wanneer het script wordt aangemaakt en opgeslagen in het besturingssysteem, moet u CPAR-verwijzing naar het script configureren. Stel taal in als TCL, filename moet exacte bestandsnaam zijn met extensie (in dit geval is het nadip.tcl). EntryPoint is de naam van de procedure in het bestand die u als script wilt uitvoeren. Referentie creëerde CPAR-script onder service (inkomendScript) en test met radclient.

Lijnen #2, #3, #5 kunnen bij de tracering worden waargenomen:

```
--> 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
```

Overtrekken:

```
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
```