Catalyst 3850 Series Switch Session Aware-netwerken met een servicesjabloon op het ISE-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u identiteitsservices kunt configureren op een Cisco Catalyst 3850 Series-switch met het Session Aware Networking-framework. Dit is een nieuwe manier om identiteitsservices te configureren (802.1x, MAC-verificatie-omzeiling (MAB), WebAuth) die meer flexibiliteit en functionaliteit biedt. Het gebruikt de Cisco Common Classification Policy Language (C3PL) samen met servicessjablonen die lokaal of op de Cisco Identity Services Engine (ISE)-server kunnen worden opgeslagen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst 3850 Series Switch, Cisco IOS® CLI
- Cisco ISE-software
- Identiteitsservices (802.1x/MAB/WebAuth)

Gebruikte componenten

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

- Catalyst 3850 Series Switch, Cisco IOS-versie 3.03.00SE of hoger
- Cisco ISE-softwareversie 1.2 of hoger

> **Opmerking**: raadpleeg de implementatiegids van IBNS 2.0 om de ondersteuningsmatrix te bekijken.

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 live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Servicessjablonen bevatten een reeks beleidskenmerken die via een specifieke actie in het controlebeleid aan een gebruikerssessie kunnen worden gekoppeld. In dit document worden twee voorbeelden gegeven:

- MAB en een lokaal gedefinieerde servicesjabloon die voor het storingsscenario wordt gebruikt.
- MAB en een ISE-gedefinieerde servicesjabloon die voor het storingsscenario wordt gebruikt.

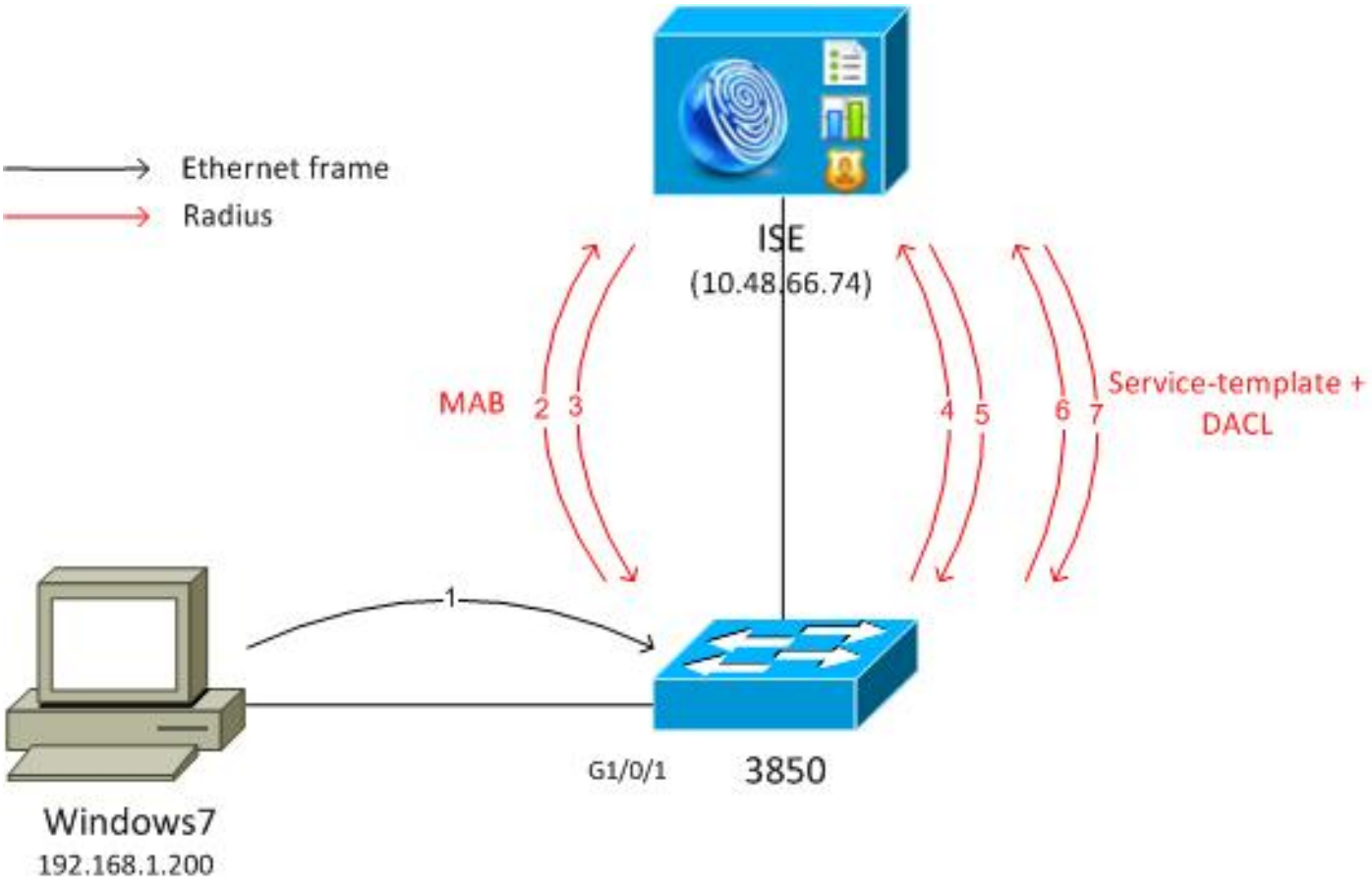
MAB wordt in dit document als voorbeeld gebruikt. Het is echter wel mogelijk om 802.1x en/of WebAuth te gebruiken en complexe beleidslijnen op te bouwen met C3PL.

Configureren

> **Opmerking**: Gebruik de Command Lookup Tool (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Beide voorbeelden die hier worden gepresenteerd, hebben betrekking op een Windows-pc die verbinding maakt met de switch die MAB uitvoert. Het MAC-adres van Windows is niet ingesteld op de ISE, wat de reden is dat MAB mislukt. Vervolgens past de switch het beleid toe dat in de servicesjabloon is gedefinieerd.



Lokaal gedefinieerde servicessjabloon

Na een MAB-fout past de switch de lokaal gedefinieerde servicesjabloon toe.

Hier is de flow:

1. Windows verstuurt het Ethernet-frame.

2. De switch voert MAB uit en verstuurt het RADIUS-Verzoek naar ISE met het MAC-adres als gebruikersnaam.

3. De ISE heeft dat eindpunt niet geconfigureerd en geeft RADIUS-Reject terug.

4. De switch activeert het lokaal gedefinieerde sjabloon beleid MAB_FAIL.

Raadpleeg voor meer volledige informatie de configuratiehandleiding voor op identiteit gebaseerde netwerkservices, Cisco IOS XE release 3SE (Catalyst 3850 Switches).

Hier is een eenvoudig voorbeeld:

```
aaa new-model
!
aaa group server radius ISE
 server name ISE
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting identity default start-stop group ISE
```

```
dot1x system-auth-control

service-template MAB_FAIL_LOCAL  <--- Local service template
 access-group MAB_FAIL_LOCAL_ACL

class-map type control subscriber match-all MAB-FAIL
 match result-type method mab authoritative <--- class MAB failure
!
policy-map type control subscriber POLICY_MAB
 event session-started match-all
 10 class always do-until-failure
  10 authenticate using mab aaa authc-list ISE priority 20 <--- try MAB
  20 authenticate using mab aaa authz-list ISE priority 20
 event authentication-failure match-first
 10 class MAB-FAIL do-until-failure
  20 activate service-template MAB_FAIL_LOCAL <--- apply local template service
for the MAB failure

interface GigabitEthernet1/0/1
 switchport mode access
 access-session port-control auto
 mab
 spanning-tree portfast
 service-policy type control subscriber POLICY_MAB

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 key cisco

ip access-list extended MAB_FAIL_LOCAL_ACL
 permit icmp any any
```

Servicesjabloon gedefinieerd op ISE

Hier is de flow:

1. Windows verstuurt het Ethernet-frame.

2. De switch voert MAB uit en stuurt het RADIUS-Verzoek naar de ISE met het MAC-adres als gebruikersnaam.

3. De ISE heeft dat eindpunt niet geconfigureerd en geeft een RADIUS-Reject terug.

4. De switch activeert het sjabloon beleid **MAB_FAIL** met de ISE-verificatie, autorisatie en accounting (AAA)-lijst. Het RADIUS-verzoek wordt met de gebruikersnaam als sjabloonnaam (**MAB_FAIL**) en het hardcodeerde wachtwoord verzonden: **cisco123**. Het Cisco Attribute Value (AV)-paar is ook in bijlage **download-request=service-sjabloon opgenomen**.

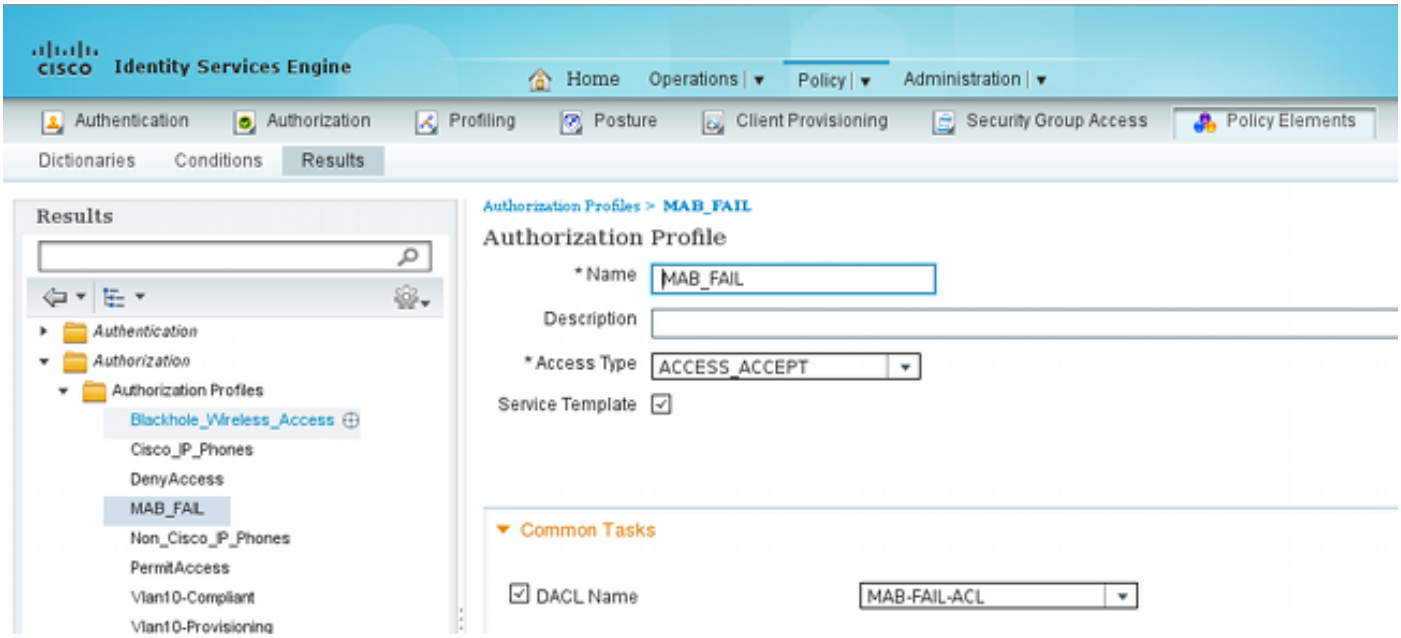
5. Dat AV-paar dwingt de ISE om dat verzoek te behandelen als een servicesjabloonverzoek. Alle controles op authenticatie en autorisatieregels zijn weggelaten. De ISE controleert alleen of het autorisatieprofiel met dezelfde naam (**MAB_FAIL**) bestaat. Het is niet nodig om de **MAB_FAIL** gebruiker te configureren in het lokale gebruikersarchief. Vervolgens retourneert de ISE alle eigenschappen die aan dat profiel zijn gekoppeld, zoals de Downloadbare Toegangscontrolelijst (DACL) in dit voorbeeld.

6. Als DACL niet op de switch wordt gecached, verzendt het een ander RADIUS-Verzoek om dat DACL.

7. De DACL-inhoud wordt geretourneerd. De switch past het beleid toe.

ISE-configuratie

Nadat u het netwerktoegangsapparaat hebt toegevoegd, is het autorisatieprofiel vereist:



Het is belangrijk om het aanvinkvakje **Service Template** aan te vinken en dezelfde naam te gebruiken als die op de switch is gedefinieerd.

Catalyst 3850 Series Switch-configuratie

Deze configuratie heeft vier verschillen van het eerste voorbeeld:

- De lokale **MAB_FAIL_LOCAL** beleidssjabloon wordt verwijderd.
- Ondersteuning voor wijziging van autorisatie (CoA) is toegevoegd.
- De ISE lijst voor de **MAB_FAIL** policy template (beleid geconfigureerd op de ISE) wordt gebruikt.
- Er wordt een AAA-autorisatielijst voor het ophalen van servicesjablonen genoemd.

Hier is de configuratie:

```
aaa new-model
!
aaa group server radius ISE
 server name ISE
!
aaa authentication dot1x default group ISE
```

```
aaa authorization network default group ISE
aaa authorization network ISE group ISE     <--- used to retrieve
service-template
from ISE
aaa accounting identity default start-stop group ISE

dot1x system-auth-control

aaa server radius dynamic-author
 client 10.48.66.74 server-key cisco

class-map type control subscriber match-all MAB-FAIL
 match result-type method mab authoritative <--- class MAB failure
!
policy-map type control subscriber POLICY_MAB
 event session-started match-all
 10 class always do-until-failure
  10 authenticate using mab aaa authc-list ISE priority 20 <--- try MAB
  20 authenticate using mab aaa authz-list ISE priority 20
 event authentication-failure match-first
 10 class MAB-FAIL do-until-failure
  20 activate service-template MAB_FAIL aaa-list ISE replace-all <--- apply
template
policy defined on ISE for the MAB failure

interface GigabitEthernet1/0/1
 switchport mode access
 access-session port-control auto
 mab
 spanning-tree portfast
 service-policy type control subscriber POLICY_MAB

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 key cisco
```

U moet RADIUS CoA-ondersteuning op de switch configureren nadat u de sjabloon (autorisatieprofiel) op de ISE hebt gewijzigd, omdat het de CoA verstuurt om de sjabloon op de switch bij te werken.

Verifiëren

Lokaal gedefinieerde servicessjabloon

Voer op de Catalyst 3850 Series switch deze opdracht in om de gebruikerssessie te verifiëren:

```
3850-1#show access-session int g1/0/1 details
           Interface:  GigabitEthernet1/0/1
              IIF-ID:  0x1091E80000000B0
         MAC Address:  dc7b.94a3.7005
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  dc7b94a37005
              Status:  Unauthorized
              Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
     Session timeout:  N/A
```

```
   Common Session ID:  0A30276F0000117D52D8816C
     Acct Session ID:  Unknown

             Handle:  0x50000368
      Current Policy:  POLICY_MAB

Local Policies:
       Template: MAB_FAIL_LOCAL (priority 150)
           Filter-ID:  MAB_FAIL_LOCAL_ACL

Method status list:
      Method           State
      mab              Authc Failed

3850-1#sh ip access-lists MAB_FAIL_LOCAL_ACL
Extended IP access list MAB_FAIL_LOCAL_ACL
   10 permit icmp any any
```

Servicesjabloon gedefinieerd op de ISE

Voer op de Catalyst 3850 Series switch deze opdracht in om de gebruikerssessie te verifiëren:

```
3850-1# show access-session interface g1/0/1 details
           Interface:  GigabitEthernet1/0/1
              IIF-ID:  0x1058A40000000AB
         MAC Address:  dc7b.94a3.7005
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  dc7b94a37005
              Status:  Unauthorized
              Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  0A30276F0000116851173EFE
     Acct Session ID:  Unknown
              Handle:  0xCC000363
      Current Policy:  POLICY_MAB

Local Policies:
       Template: MAB_FAIL (priority 150)
             ACS ACL:  xACSACLx-IP-MAB-FAIL-ACL-528741f3

Method status list:
      Method           State
      mab              Authc Failed
```

Merk op dat de staat **is mislukt**, maar dat de specifieke sjabloon en de bijbehorende DACL worden toegepast:

```
3850-1#show ip access-lists
Extended IP access list implicit_deny_acl
   10 deny ip any any
Extended IP access list xACSACLx-IP-MAB-FAIL-ACL-528741f3 (per-user)
    1 permit icmp any any     <--- DACL from ISE
```

De toegangscontrolelijst (ACL) is niet zichtbaar onder de interface:

```
3850-1#show ip access-lists  interface g1/0/1 in
```

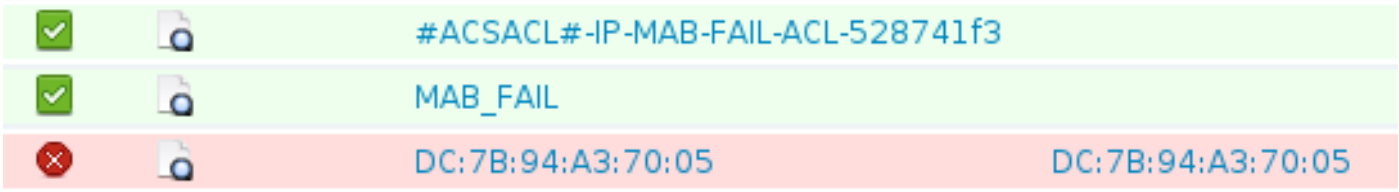
```
3850-1#show ip access-lists  interface g1/0/1
3850-1#show ip access-lists  interface g1/0/1 out
3850-1#
```

Het is mogelijk om te controleren of ASIC (hardware) correct geprogrammeerd is:

```
3850-1#  show platform acl
##############################################################
#########                                ###################
########      Printing LE Infos          ##################
#########                                ###################
##############################################################
##############################################################
##  LE INFO: (LETYPE: Group)
##############################################################
LE: 7   (Client MAC dc7b.94a3.7005)  (ASIC1)
------------
   leinfo: 0x5171eea0
   LE handle: 0x61120fb0
   LE Type: Group
   IIF ID: 0x1058a40000000ab
   Input IPv4 ACL: label 4 h/w 4 (read from h/w 4)
       BO 0x196000000 [CGACL]: xACSACLx-IP-MAB-FAIL-ACL-528741f3
       BO 0x1fffffa00 [CGACL]: implicit_deny_acl
   Output IPv4 ACL: label 0 h/w 0 (Group LE and label are not linked)
   Input IPv6 ACL: label 0 h/w 0 (Group LE and label are not linked)
   Output IPv6 ACL: label 0 h/w 0 (Group LE and label are not linked)
   Input MAC ACL: label 0 h/w 0 (Group LE and label are not linked)
   Output MAC ACL: label 0 h/w 0 (Group LE and label are not linked)
```

Elke gebruikerssessie die een andere DACL heeft, zal een aparte ingang hebben die geprogrammeerd is in ASIC. Op de ISE zijn er drie verschillende authenticaties:

- Mislukte MAB
- Succesvolle ophalen van servicesjabloon (**MAB_FAIL**)
- Succesvolle DACL-ophalen



Hier kunt u de stappen nader bekijken wanneer u het verzoek voor de servicesjabloon ontvangt:

11001	Ontvangen RADIUS-toegangsaanvraag
11017	RADIUS maakt een nieuwe sessie
11022	De dACL toegevoegd die in het autorisatieprofiel is gespecificeerd
11002	Teruggekeerde RADIUS-toegang - Accepteren

Hieruit blijkt duidelijk dat de regels voor verificatie/autorisatie niet worden verwerkt.

Problemen oplossen

Lokaal gedefinieerde servicessjabloon

Hier zijn de debugs voor het huidige scenario. Sommige outputs worden voor de duidelijkheid weggelaten:

```
3850-1#show debugging
epm:
 EPM session error debugging is on
 EPM session error detailed debugging is on
 EPM fsm error debugging is on
 EPM fsm error detailed debugging is on
 EPM packet error debugging is on
 EPM packet error detailed debugging is on
 EPM SPI errors debugging is on
 EPM session events debugging is on
 EPM fsm events debugging is on
 EPM fsm events detailed debugging is on
 EPM packet events debugging is on
 EPM packet events detailed debugging is on
 EPM SPI events debugging is on


Radius protocol debugging is on
Radius protocol verbose debugging is on
Radius packet protocol debugging is on
Auth Manager:
 Auth Manager errors debugging is on
 Auth Manager events debugging is on
 Auth Manager detailed debugs debugging is on
 Auth Manager sync debugging is on
dot1x:
 Dot1x registry info debugging is on
 Dot1x redundancy info debugging is on
 Dot1x packet info debugging is on
 Dot1x events debugging is on
 Dot1x State machine transitions and actions debugging is on
 Dot1x Errors debugging is on
 Dot1x Supplicant EAP-FAST debugging is on
 Dot1x Manager debugging is on
 Dot1x Supplicant State Machine debugging is on

*Nov 16 11:45:10.680: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] New client
dc7b.94a3.7005 - client handle 0x00000001 for SVM
*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] Create attr list,
session 0x50000368:
*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding MAC
dc7b.94a3.7005
*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding Swidb
0x38A8DABC
*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding
AAA_ID=117D
*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding
Audit_sid=0A30276F0000117D52D8816C
*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding IIF
ID=0x1091E80000000B0
*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Policy processing
started for 0x50000368(dc7b.94a3.7005)
*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Policy event will
be processed synchronously for 0x50000368
*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Processing default
action(s) for event SESSION_STARTED for session 0x50000368
```

```
*Nov 16 11:45:11.354: RADIUS/ENCODE: Best Local IP-Address 10.48.39.111 for
Radius-Server 10.48.66.74
*Nov 16 11:45:11.354: RADIUS(00000000): Send Access-Request to 10.48.66.74:1645
id 1645/2, len 260
*Nov 16 11:45:11.354: RADIUS:  authenticator 86 FC 11 6A 6E 8D A1 0B - A6 98
8B 80 A2 DD A9 69
*Nov 16 11:45:11.354: RADIUS:  User-Name           [1]   14  "dc7b94a37005"
*Nov 16 11:45:11.354: RADIUS:  User-Password       [2]   18  *
*Nov 16 11:45:11.354: RADIUS:  Service-Type        [6]   6   Call Check     [10]
*Nov 16 11:45:11.354: RADIUS:  Vendor, Cisco       [26]  31
*Nov 16 11:45:11.354: RADIUS:   Cisco AVpair       [1]   25  "service-type=Call Check"
*Nov 16 11:45:11.354: RADIUS:  Framed-MTU          [12]  6   1500
*Nov 16 11:45:11.354: RADIUS:  Called-Station-Id   [30]  19  "68-BC-0C-5A-61-01"
*Nov 16 11:45:11.354: RADIUS:  Calling-Station-Id  [31]  19  "DC-7B-94-A3-70-05"
*Nov 16 11:45:11.354: RADIUS:  Message-Authenticato[80]  18
*Nov 16 11:45:11.354: RADIUS:   2D 20 38 B1 DF B6 C1 0C 0D AA 1D 9D E4 3E C8 0B [ - 8>]
*Nov 16 11:45:11.354: RADIUS:  EAP-Key-Name        [102] 2   *
*Nov 16 11:45:11.354: RADIUS:  Vendor, Cisco       [26]  49
*Nov 16 11:45:11.354: RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=
0A30276F0000117D52D8816C"
*Nov 16 11:45:11.355: RADIUS:  Vendor, Cisco       [26]  18
*Nov 16 11:45:11.355: RADIUS:   Cisco AVpair       [1]   12  "method=mab"
*Nov 16 11:45:11.355: RADIUS:  NAS-IP-Address      [4]   6   10.48.39.111
*Nov 16 11:45:11.355: RADIUS:  NAS-Port            [5]   6   60000
*Nov 16 11:45:11.355: RADIUS:  NAS-Port-Id         [87]  22  "GigabitEthernet1/0/1"
*Nov 16 11:45:11.355: RADIUS:  NAS-Port-Type       [61]  6   Ethernet         [15]
*Nov 16 11:45:11.355: RADIUS(00000000): Sending a IPv4 Radius Packet
*Nov 16 11:45:11.355: RADIUS(00000000): Started 5 sec timeout
*Nov 16 11:45:12.008: RADIUS: Received from id 1645/2 10.48.66.74:1645, Access-Reject,
len 38
*Nov 16 11:45:12.009: RADIUS:  authenticator 9D 52 F8 CF 31 46 5A 17 - 4C 45 7E 89 9F
E2 2A 84
*Nov 16 11:45:12.009: RADIUS:  Message-Authenticato[80]  18
*Nov 16 11:45:12.009: RADIUS:   11 F4 99 84 9B CC 7C 61 C7 75 7E 70 87 EC 64 8D  [ |au~pd]
*Nov 16 11:45:12.009: RADIUS(00000000): Received from id 1645/2
*Nov 16 11:45:12.012: %MAB-5-FAIL: Authentication failed for client (dc7b.94a3.7005)
on Interface Gi1/0/1 AuditSessionID 0A30276F0000117D52D8816C
*Nov 16 11:45:12.013: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Client dc7b.94a3.7005,
Method mab changing state from 'Running' to 'Authc Failed'
*Nov 16 11:45:12.013: AUTH-EVENT: Raised event RX_METHOD_AUTHC_FAIL (6) on handle
0x50000368
*Nov 16 11:45:12.016: EPM_SESS_EVENT: Feature (EPM ACL PLUG-IN) has been
started (status 2)
*Nov 16 11:45:12.016: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC dc7b.94a3.7005| AuditSessionID
0A30276F0000117D52D8816C| EVENT APPLY
*Nov 16 11:45:12.016: %EPM-6-POLICY_APP_SUCCESS: Policy Application succeded for Client
[0.0.0.0] MAC [dc7b.94a3.7005] AuditSession ID [0A30276F0000117D52D8816C] for POLICY_TYPE
[Filter ID] POLICY_NAME [MAB_FAIL_LOCAL_ACL]
```

Servicesjabloon gedefinieerd op de ISE

Hier zijn de debugs voor het huidige scenario. Sommige outputs worden voor de duidelijkheid weggelaten:

```
<debug command omitted for clarity>

*Nov 16 03:34:28.670: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Processing default
action(s) for event SESSION_STARTED for session 0xCC000363.
*Nov 16 03:34:28.679: RADIUS(00000000): Send Access-Request to 10.48.66.74:1645
id 1645/249, len 260
*Nov 16 03:34:28.679: RADIUS:  authenticator CE 06 B0 C4 84 1D 70 82 - B8 66 2F
```

```
27 92 73 B7 E7
*Nov 16 03:34:28.679: RADIUS:  User-Name           [1]   14  "dc7b94a37005"
...
*Nov 16 03:34:29.333: RADIUS: Received from id 1645/249 10.48.66.74:1645, Access-Reject,
len 38
...
*Nov 16 03:34:29.335: %MAB-5-FAIL: Authentication failed for client (dc7b.94a3.7005)
on Interface Gi1/0/1 AuditSessionID 0A30276F0000116851173EFE
*Nov 16 03:34:29.336: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Authc failure from MAB (2),
status Cred Fail (1) / event fail (1)
*Nov 16 03:34:29.339: %EPM-6-AAA: POLICY MAB_FAIL| EVENT DOWNLOAD_REQUEST
*Nov 16 03:34:29.340: EPM_SESS_EVENT: Method list used for download is ISE
*Nov 16 03:34:29.340: RADIUS(00000000): Send Access-Request to 10.48.66.74:1645 id 1645/250,
len 113
*Nov 16 03:34:29.340: RADIUS:  authenticator B8 37 70 B0 33 F4 F2 FD - E4 C6 36
2A 4D BD 34 30
*Nov 16 03:34:29.341: RADIUS:  NAS-IP-Address      [4]   6   10.48.39.111
*Nov 16 03:34:29.341: RADIUS:  User-Name           [1]   10  "MAB_FAIL"
*Nov 16 03:34:29.341: RADIUS:  User-Password       [2]   18  *
*Nov 16 03:34:29.341: RADIUS:  Vendor, Cisco       [26]  41
*Nov 16 03:34:29.341: RADIUS:   Cisco AVpair       [1]   35  "download-request=
service-template"
*Nov 16 03:34:29.341: RADIUS:  Message-Authenticato[80]  18
*Nov 16 03:34:29.341: RADIUS:   EF D6 81 F7 5E 03 10 3B 91 EE 36 6E 9D 04
5B F4      [ ^;6n[]
*Nov 16 03:34:29.341: RADIUS(00000000): Sending a IPv4 Radius Packet
*Nov 16 03:34:29.341: RADIUS(00000000): Started 5 sec timeout
*Nov 16 03:34:29.342: EPM_SESS_EVENT: Received IPv4 Binding [ADD] Notification
[GigabitEthernet1/0/48 000c.29f3.ab14 10.48.39.131 1]
*Nov 16 03:34:29.342: EPM_SESS_EVENT: Received IPv4 Binding [ADD] Notification
[GigabitEthernet1/0/48 0050.5699.5350 10.48.39.211 1]
*Nov 16 03:34:29.867: RADIUS: Received from id 1645/250 10.48.66.74:1645,
Access-Accept, len 208
*Nov 16 03:34:29.867: RADIUS:  authenticator A3 11 DA 4C 17 7E D3 86 - 06 78
85 5F 84 05 36 0B
*Nov 16 03:34:29.867: RADIUS:  User-Name           [1]   10  "MAB_FAIL"
*Nov 16 03:34:29.867: RADIUS:  State               [24]  40
*Nov 16 03:34:29.867: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A
30 61  [ReauthSession:0a]
*Nov 16 03:34:29.867: RADIUS:   33 30 34 32 34 61 30 30 30 30 31 32 30 44
35 32  [30424a0000120D52]
*Nov 16 03:34:29.867: RADIUS:   38 37 34 38 32 45            [ 87482E]
*Nov 16 03:34:29.867: RADIUS:  Class               [25]  51
*Nov 16 03:34:29.867: RADIUS:   43 41 43 53 3A 30 61 33 30 34 32 34 61 30
30 30  [CACS:0a30424a000]
*Nov 16 03:34:29.868: RADIUS:   30 31 32 30 44 35 32 38 37 34 38 32 45 3A
69 73  [0120D5287482E:is]
*Nov 16 03:34:29.868: RADIUS:   65 32 2F 31 37 33 37 31 31 34 31 36 2F 35
30 30  [e2/173711416/500]
*Nov 16 03:34:29.868: RADIUS:   32                 [ 2]
*Nov 16 03:34:29.868: RADIUS:  Message-Authenticato[80]  18
*Nov 16 03:34:29.868: RADIUS:   1F 10 85 09 86 2C 5F 87 96 82 C8 3B 09 35 FD
96             [ ,_;5]
*Nov 16 03:34:29.868: RADIUS:  Vendor, Cisco       [26]  69
*Nov 16 03:34:29.868: RADIUS:   Cisco AVpair       [1]   63  "ACS:
CiscoSecure-Defined-ACL=#ACSACL#-IP-MAB-FAIL-ACL-528741f3"
*Nov 16 03:34:29.868: RADIUS(00000000): Received from id 1645/250
*Nov 16 03:34:29.869: %EPM-6-AAA: POLICY MAB_FAIL| EVENT DOWNLOAD-SUCCESS
*Nov 16 03:34:29.873: EPM_SESS_EVENT: Added method name ISE
*Nov 16 03:34:29.873: EPM_SESS_EVENT: Attribute CiscoSecure-Defined-ACL is
added to feat EPM ACL PLUG-IN  list
*Nov 16 03:34:29.875: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC dc7b.94a3.7005|
AuditSessionID 0A30276F0000116851173EFE| EVENT APPLY
*Nov 16 03:34:29.875: %EPM-6-AAA: POLICY xACSACLx-IP-MAB-FAIL-ACL-528741f3|
```

EVENT DOWNLOAD_REQUEST
*Nov 16 03:34:29.876: RADIUS(00000000): **Send Access-Request to 10.48.66.74:1645**
id 1645/251, len 141
*Nov 16 03:34:29.876: RADIUS: authenticator BA 4C 97 06 E9 9E D5 03 - 1C 48
63 E6 94 D7 F8 DB
*Nov 16 03:34:29.876: RADIUS: NAS-IP-Address   [4]   6   10.48.39.111
*Nov 16 03:34:29.876: RADIUS: **User-Name   [1]   35 "#ACSACL#-IP-
MAB-FAIL-ACL-528741f3"**
*Nov 16 03:34:29.876: RADIUS: Vendor, Cisco   [26] 32
*Nov 16 03:34:29.876: RADIUS: Cisco AVpair   [1]   26 "aaa:service=
ip_admission"
*Nov 16 03:34:29.876: RADIUS: Vendor, Cisco   [26] 30
*Nov 16 03:34:29.877: RADIUS: Cisco AVpair   [1]   24 **"aaa:event=
acl-download"**
*Nov 16 03:34:29.877: RADIUS: Message-Authenticato[80] 18
*Nov 16 03:34:29.877: RADIUS: B1 4C E4 15 24 06 B4 1D E4 48 60 A0 9F 75
27 29   [L$H`u')]
*Nov 16 03:34:29.877: RADIUS(00000000): Sending a IPv4 Radius Packet
*Nov 16 03:34:29.877: RADIUS(00000000): Started 5 sec timeout
*Nov 16 03:34:30.533: RADIUS: **Received from id 1645/251 10.48.66.74:1645,
Access-Accept**, len 202
*Nov 16 03:34:30.533: RADIUS: authenticator FA F9 55 1B 2A E2 32 0F - 33
C6 F9 FF BC C1 BB 7C
*Nov 16 03:34:30.533: RADIUS: User-Name   [1]   35 "#ACSACL#-IP-
MAB-FAIL-ACL-528741f3"
*Nov 16 03:34:30.533: RADIUS: State   [24] 40
*Nov 16 03:34:30.534: RADIUS: 52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A
30 61 [ReauthSession:0a]
*Nov 16 03:34:30.534: RADIUS: 33 30 34 32 34 61 30 30 30 30 31 32 30 45
35 32 [30424a0000120E52]
*Nov 16 03:34:30.534: RADIUS: 38 37 34 38 32 45   [87482E]
*Nov 16 03:34:30.534: RADIUS: Class   [25] 51
*Nov 16 03:34:30.534: RADIUS: 43 41 43 53 3A 30 61 33 30 34 32 34 61 30
30 30 [CACS:0a30424a000]
*Nov 16 03:34:30.534: RADIUS: 30 31 32 30 45 35 32 38 37 34 38 32 45 3A
69 73 [0120E5287482E:is]
*Nov 16 03:34:30.534: RADIUS: 65 32 2F 31 37 33 37 31 31 34 31 36 2F 35
30 30 [e2/173711416/500]
*Nov 16 03:34:30.534: RADIUS: 33   [3]
*Nov 16 03:34:30.534: RADIUS: Message-Authenticato[80] 18
*Nov 16 03:34:30.534: RADIUS: 96 9B AC 2C 28 47 25 B1 CF EA BD D0 7D F3
44 34   [,(G?}D4]
*Nov 16 03:34:30.534: RADIUS: Vendor, Cisco   [26] 38
*Nov 16 03:34:30.534: RADIUS: Cisco AVpair   [1]   32 "**ip:inacl#1=
permit icmp any any**"
*Nov 16 03:34:30.534: RADIUS(00000000): Received from id 1645/251
*Nov 16 03:34:30.535: %EPM-6-AAA: POLICY xACSACLx-IP-MAB-FAIL-ACL-528741f3|
EVENT DOWNLOAD-SUCCESS
*Nov 16 03:34:30.537: EPM_SESS_EVENT: **Executed [ip access-list extended
xACSACLx-IP-MAB-FAIL-ACL-528741f3]** command through parse_cmd. Result= 0
*Nov 16 03:34:30.538: EPM_SESS_EVENT: Executed [1 permit icmp any any]
command through parse_cmd. Result= 0
*Nov 16 03:34:30.539: EPM_SESS_EVENT: Executed [end] command through parse_cmd.
Result= 0
*Nov 16 03:34:30.541: EPM_SESS_EVENT: **ACL xACSACLx-IP-MAB-FAIL-ACL-528741f3
provisioning successful**
*Nov 16 03:34:31.136: EPM_SESS_EVENT: Successful feature attrs provided for
SM ACCOUNTING PLUG-IN
*Nov 16 03:34:31.136: EPM_SESS_EVENT: Successful feature attrs provided for
EPM ACL PLUG-IN
*Nov 16 03:34:31.136: AUTH-EVENT: Rcvd IPC call for pre 0x5F000002, inst
0xB2000072, hdl 0x95000073
*Nov 16 03:34:31.136: AUTH-EVENT: **Raising ext evt Template Activated (8)**
on session 0xCC000363, client (unknown) (0), hdl 0x00000000, attr_list

```
0xA5000E24
*Nov 16 03:34:31.142: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Handling external
PRE event Template Activated for context 0xCC000363.
```

Wanneer er geen correct autorisatieprofiel op de ISE is, meldt het:

11001	Ontvangen RADIUS-toegangsaanvraag
11017	RADIUS maakt een nieuwe sessie
11003	Teruggegeven RADIUS access-reject

Ook wordt het **mislukte** bericht van de **verificatie van Event 5400** gepresenteerd, maar er worden geen details meer onthuld. Nadat u de gebruikersnaam met het **Cisco123-**wachtwoord hebt gemaakt, blijft de fout gelijk, zelfs als er correcte verificatie-/autorisatieregels zijn. De enige voorwaarde voor een correcte werking van deze functie is een correct autorisatieprofiel.

Gerelateerde informatie

- Configuratiehandleiding voor op identiteit gebaseerde netwerkservices, Cisco IOS XE release 3SE
- Geconsolideerd platform met opdrachtreferentie, Cisco IOS XE 3.2SE
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.