

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Plantilla Local-definida del servicio](#)

[Mantenga la plantilla definida en el ISE](#)

[Configuración ISE](#)

[Configuración del Catalyst 3850 Series Switch](#)

[Verificación](#)

[Plantilla Local-definida del servicio](#)

[Mantenga la plantilla definida en el ISE](#)

[Troubleshooting](#)

[Plantilla Local-definida del servicio](#)

[Mantenga la plantilla definida en el ISE](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar los servicios de la identidad en un Cisco Catalyst 3850 Series Switch con el marco enterado del establecimiento de una red de la sesión. Ésta es una nueva manera de configurar los servicios de la identidad (802.1x, puente de la autenticación de MAC (MAB), WebAuth) que permite la mayores flexibilidad y funciones. Utiliza el lenguaje de la directiva de la clasificación típica de Cisco (C3PL) junto con las plantillas del servicio que se pueden salvar localmente o en el servidor del Cisco Identity Services Engine (ISE).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Catalyst 3850 Series Switch, [®] CLI del Cisco IOS
- Cisco ISE
- Servicios de la identidad (802.1x/MAB/WebAuth)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 3850 Series Switch, versión deL Cisco IOS 03.03.00SE o más adelante
- Versión 1.2 o posterior de Cisco ISE

Nota: Refiera al [Guía de despliegue IBNS 2.0](#) para ver la matriz de soporte.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Las plantillas del servicio contienen un conjunto de los atributos de la política que se pueden asociar a una sesión del usuario vía una acción específica en la directiva de control. Dos ejemplos se presentan en este documento:

- MAB y una plantilla local-definida del servicio usada para el escenario de falla.
- MAB y una plantilla ISE-definida del servicio usada para el escenario de falla.

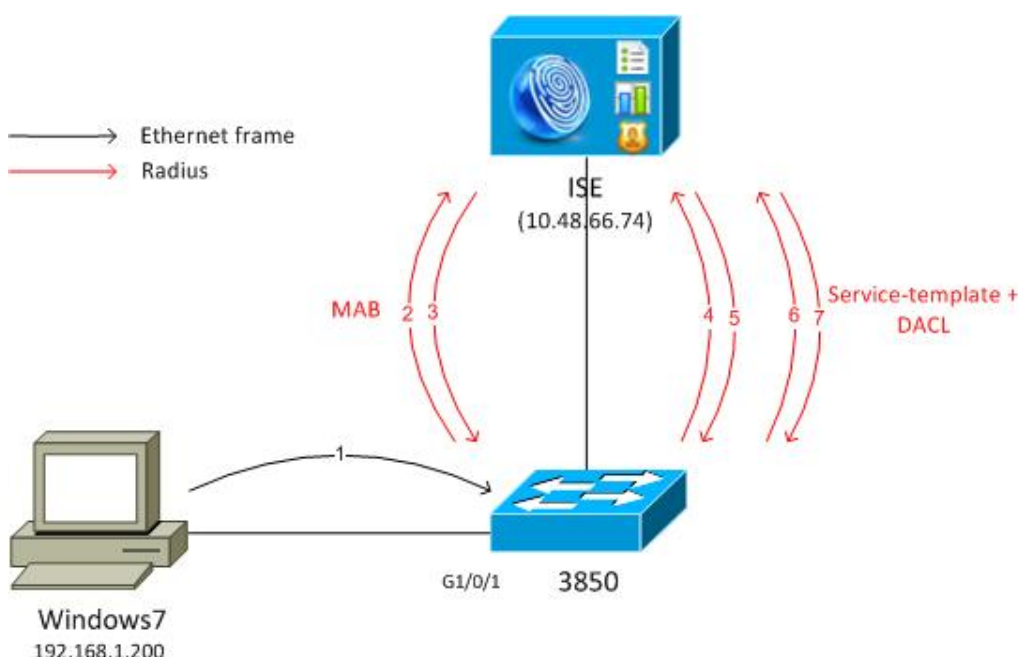
El MAB se utiliza como el ejemplo en este documento. Sin embargo, es posible utilizar el 802.1x y/o WebAuth y construir las directivas complejas con C3PL.

Configurar

Nota: Use la [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

Ambos ejemplos presentados aquí implican un PC de Windows que conecta con el Switch que realiza el MAB. La dirección MAC de Windows no se configura en el ISE, que es porqué el MAB falla. Entonces, el Switch aplica la directiva definida en la plantilla del servicio.



Plantilla Local-definida del servicio

Después del error MAB, el Switch aplica la plantilla local-definida del servicio.

Aquí está el flujo:

1. Windows envía la trama Ethernet.
2. El Switch realiza el MAB, y envía el pedido de RADIUS hacia el ISE con la dirección MAC como nombre de usuario.
3. El ISE no tiene que punto final configurado, y RADIUS-rechazo de las devoluciones.
4. El Switch activa la directiva local-definida MAB_FAIL de la plantilla.

Para más Información completa, refiera a los [servicios de red basados en la identidad guía de configuración, la versión 3SE \(Catalyst 3850 Switch\) del Cisco IOS XE](#).

Aquí está un ejemplo básico:

```
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
  20 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
```

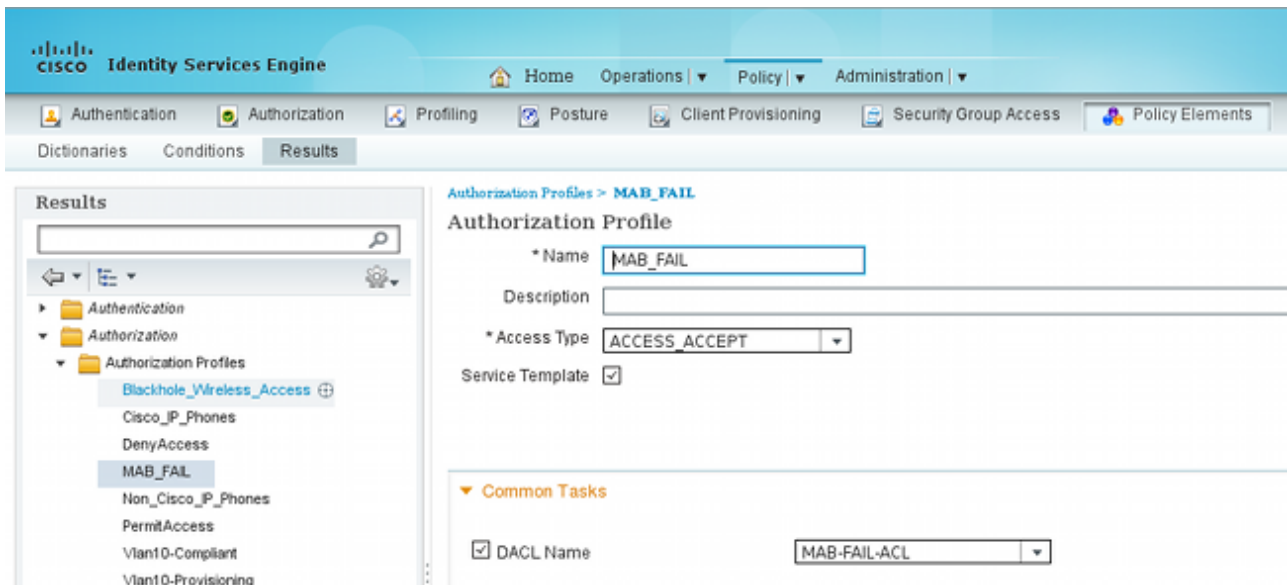
Mantenga la plantilla definida en el ISE

Aquí está el flujo:

1. Windows envía la trama Ethernet.
2. El Switch realiza el MAB, y envía el pedido de RADIUS hacia el ISE con la dirección MAC como nombre de usuario.
3. El ISE no tiene que punto final configurado, y vuelve un RADIUS-rechazo.
4. El Switch activa la directiva **MAB_FAIL** de la plantilla con el Authentication, Authorization, and Accounting (AAA) ISE - lista. El pedido de RADIUS se envía con el nombre de usuario como el nombre de la plantilla (**MAB_FAIL**) y la contraseña puesta en hard-code: **cisco123**. También, el par del valor de atributo de Cisco (AV) es **download-request=service-template** asociado.
5. Ese par AV fuerza el ISE para tratar esa petición como petición de la plantilla del servicio. Todas las comprobaciones para las reglas de la autenticación y autorización se omiten. El ISE marca solamente si existe el perfil de la autorización con el mismo nombre (**MAB_FAIL**). No hay necesidad de configurar al usuario **MAB_FAIL** en el almacén del usuario local. Entonces, el ISE vuelve todos los atributos asociados a ese perfil, que es la lista de control de acceso transferible (DACL) en este ejemplo.
6. Si el DACL no se oculta en el Switch, envía otro pedido de RADIUS para eso DACL.
7. Se vuelve el contenido DACL. El Switch aplica las directivas.

Configuración ISE

Después de que usted agregue el dispositivo de acceso a la red, se requiere el perfil de la autorización:



Es importante marcar la casilla de verificación de la **plantilla del servicio**, y utilizar el mismo nombre que el que está definido en el Switch.

Configuración del Catalyst 3850 Series Switch

Esta configuración tiene cuatro diferencias del primer ejemplo:

- Se quita la plantilla de política local **MAB_FAIL_LOCAL**.
- El cambio del soporte de la autorización (CoA) se agrega.
- La lista ISE para la plantilla de política **MAB_FAIL** (directiva configurada en el ISE) se utiliza.
- Una lista de la autorización AAA para la extracción de la plantilla del servicio se nombra.

Esta es la configuración:

```

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
```

Usted debe configurar el soporte CoA RADIUS en el Switch después de que usted cambie la plantilla (perfil de la autorización) en el ISE, porque envía el CoA para poner al día la plantilla en el Switch.

Verificación

Plantilla Local-definida del servicio

En el Catalyst 3850 Series Switch, ingrese este comando para verificar a la sesión del usuario:

```
3850-1#show access-session int g1/0/1 details
Interface: GigabitEthernet1/0/1
IIF-ID: 0x1091E8000000B0
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
```

Mantenga la plantilla definida en el ISE

En el Catalyst 3850 Series Switch, ingrese este comando para verificar a la sesión del usuario:

```
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
```

Observe que el estado **está fallado**, pero que la plantilla específica y los DACL asociados son aplicados:

```
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
```

La lista de control de acceso (ACL) no es visible bajo interfaz:

```
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#
```

Es posible verificar si ASIC (hardware) se programa correctamente:

```
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 0x1ffffffa00 [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)
```

Cada sesión del usuario que tiene un diverso DACL tendrá una entrada separada programada en ASIC. En el ISE, hay tres autenticaciones separadas:

- MAB fallado
- Extracción acertada de la plantilla del servicio (**MAB_FAIL**)
- Extracción acertada DACL

		#ACSACL#-IP-MAB-FAIL-ACL-528741f3	
		MAB_FAIL	
		DC:7B:94:A3:70:05	DC:7B:94:A3:70:05

Aquí está una mirada más atenta en los pasos cuando usted recibe el pedido la plantilla del servicio:

- 11001 Pedido de acceso recibido RADIUS
- 11017 El RADIUS creó una nueva sesión
- 11022 Agregó el dACL especificado en el perfil de la autorización
- 11002 Access-accept vuelto RADIUS

Esto muestra claramente que las reglas de la autenticación/de la autorización no están procesadas.

Troubleshooting

Plantilla Local-definida del servicio

Aquí están los debugs para el escenario actual. Algunas salidas se omiten para mayor clareza:

```
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 succeeded for Client
[0.0.0.0] MAC [dc7b.94a3.7005] AuditSession ID [0A30276F0000117D52D8816C] for POLICY_TYPE
[Filter ID] POLICY_NAME [MAB_FAIL_LOCAL_ACL]

```

Mantenga la plantilla definida en el ISE

Aquí están los debugs para el escenario actual. Algunas salidas se omiten para mayor claridad:

<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.

```

Cuando no hay perfil correcto de la autorización en el ISE, señala:

- 11001 Pedido de acceso recibido RADIUS
- 11017 El RADIUS creó una nueva sesión
- 11003 Access-Reject vuelto RADIUS

También, se presenta el **mensaje fallido de la autenticación del evento 5400**, pero se revelan no más de detalles. Después de que usted cree el nombre de usuario con la contraseña del **cisco123**, el error sigue siendo lo mismo, incluso cuando hay reglas correctas de la autenticación/de la autorización. El único requisito de tener que el trabajo de la característica es correctamente tener un perfil correcto de la autorización.

Información Relacionada

- [Servicios de red basados en la identidad guía de configuración, versión 3SE del Cisco IOS XE](#)
- [Referencia de comandos consolidada de la plataforma, Cisco IOS XE 3.2SE](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)