

Catalyst 3850系列交换机会话意识网络用在ISE配置示例的一个服务模板

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[本地定义的服务模板](#)

[在ISE定义的服务模板](#)

[ISE配置](#)

[Catalyst 3850系列交换机配置](#)

[验证](#)

[本地定义的服务模板](#)

[在ISE定义的服务模板](#)

[故障排除](#)

[本地定义的服务模板](#)

[在ISE定义的服务模板](#)

[相关信息](#)

简介

本文描述如何配置在一Cisco Catalyst 3850系列交换机的身份服务有会话意识网络框架的。这是允许更加了不起的灵活性和功能的一种新的方法配置身份服务(802.1x、MAC验证旁路(MAB) , Webauth)。它与可以存储本地或在思科身份服务引擎的服务模板一起使用思科常见分类策略语言(C3PL) (ISE)服务器。

先决条件

要求

Cisco 建议您了解以下主题：

- Catalyst 3850系列交换机， Cisco IOS CLI
- 思科ISE

- 身份服务(802.1x/MAB/WebAuth)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 3850系列交换机，Cisco IOS版本03.03.00SE或以上
- Cisco ISE版本1.2或以上

注意：参考[IBNS 2.0部署指南](#)为了查看支持矩阵。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

服务模板包含可以附加对用户会话通过在控制政策的一特定操作的一套策略属性。两示例在本文被提交：

- MAB和用于故障情景的一个本地定义的服务模板。
- MAB和用于故障情景的一个ISE定义的服务模板。

MAB在本文使用，示例。然而，使用802.1x和Webauth和用C3PL建立复杂策略是可能的。

配置

注意：使用[命令查找工具](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

网络图

被提交的两示例此处介入连接到交换机执行MAB的一个Windows PC。Windows MAC地址在ISE没有配置，是MAB为什么发生故障。然后，交换机运用在服务模板定义的策略。

本地定义的服务模板

在MAB失败以后，交换机运用本地定义的服务模板。

这是流：

1. Windows发送以太网帧。
2. 交换机执行MAB，并且发送往ISE的RADIUS请求与MAC地址作为用户名。
3. ISE没有配置的该终端，并且返回RADIUS拒绝。

4. 交换机激活本地定义的模板策略MAB_FAIL。

欲知更多完整信息，参考[基于身份的网络服务配置指南，Cisco IOS XE版本3SE \(Catalyst 3850交换机\)](#)。

这是基本示例：

```
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
```

在ISE定义的服务模板

这是流：

1. Windows发送以太网帧。
2. 交换机执行MAB，并且发送往ISE的RADIUS请求与MAC地址作为用户名。
3. ISE没有配置的该终端，并且返回RADIUS拒绝。

4. 交换机激活与ISE验证、授权和统计(AAA)的模板策略MAB_FAIL -列表。RADIUS请求用用户名传送作为模板名称(MAB_FAIL)和硬编码的密码：cisco123。并且，思科属性值(AV)对是附加的download-request=service-template。
5. 该AV对强制ISE对待该请求作为服务模板请求。所有检查认证和授权规则省略。ISE只检查与同样的授权配置文件是否命名(MAB_FAIL)存在。没有需要配置MAB_FAIL用户在本地用户存储。然后，ISE返回所有属性关联与该配置文件，在本例中是可下载的控制表(DACL)。
6. 如果DACL在交换机没有被缓存，发送那的另一个RADIUS请求DACL。
7. DACL内容返回。交换机运用策略。

ISE配置

在您添加网络接入设备后，授权配置文件要求：

检查**服务模板**复选框和使用名称和在交换机定义的那个一样是重要的。

Catalyst 3850系列交换机配置

此配置有从第一示例的四差异：

- 本地MAB_FAIL_LOCAL策略模板删除。
- 授权(CoA)支持的崔凡吉莱被添加。
-)使用MAB_FAIL策略模板的(在ISE配置的策略ISE列表。
- 服务模板检索的—Aaa authorization list被命名。

配置如下：

```

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
```

您必须配置RADIUS在交换机的CoA支持，在您更换模板(授权配置文件)后在ISE，因为发送CoA为了更新在交换机的模板。

[验证](#)

本地定义的服务模板

在Catalyst 3850系列交换机上，请输入此命令为了验证用户会话：

```
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
```

服务在ISE定义的模板

在Catalyst 3850系列交换机上，请输入此命令为了验证用户会话：

```
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
```

注意状态失败，但是特定模板和相关的DACL应用：

```
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
```

访问控制表(ACL)不是可视在接口下：

```
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#
```

验证是可能的，如果ASIC (硬件)正确地编程：

```
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 0x19600000 [CGACL]: xACSACLx-IP-MAB-FAIL-ACL-528741f3
  BO 0x1fffffa0 [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)
```

有的每用户会话不同的DAACL有在ASIC编程的一个分开的条目。在ISE，有三个独立的认证：

- 失败的MAB
- 成功的服务模板检索(MAB_FAIL)
- 成功的DAACL检索

这是仔细观察在步骤，当您收到要求服务模板时：

```
11001    已接收RADIUS Access-Request
11017    RADIUS创建个新会话
11022    添加了在授权配置文件指定的dACL
11002    返回的RADIUS Access-Accept
```

这清楚显示认证/授权规则没有处理。

[故障排除](#)

本地定义的服务模板

这是当前方案的调试。一些输出为了清晰省略：

```
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
dotlx:
Dotlx registry info debugging is on
Dotlx redundancy info debugging is on
Dotlx packet info debugging is on
```

Dotlx events debugging is on
Dotlx State machine transitions and actions debugging is on
Dotlx Errors debugging is on
Dotlx Supplicant EAP-FAST debugging is on
Dotlx Manager debugging is on
Dotlx 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]

```

在ISE定义的服务模板

这是当前方案的调试。一些输出为了清晰省略：

<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.

```

当没有在ISE时的正确授权配置文件，报告：

```

11001    已接收RADIUS Access-Request
11017    RADIUS创建个新会话
11003    返回的RADIUS访问拒绝

```

并且，提交事件5400验证失败消息，但是没有透露没有其他详细信息。在您创建与cisco123密码后的用户名，错误依然是同样，既使当有正确认证/授权规则。有的唯一的要求功能工作正确地是有一正确授权配置文件。

相关信息

- [基于身份的网络服务配置指南，Cisco IOS XE版本3SE](#)
- [统一的平台命令参考，Cisco IOS XE 3.2SE](#)
- [技术支持和文档 - Cisco Systems](#)