Catalyst 3850 Series Switch Session Aware Networking with a Service Template on the ISE 컨피그레이션 예

목차

소개

이 문서에서는 세션 인식 네트워킹 프레임워크를 사용하여 Cisco Catalyst 3850 Series 스위치에서 ID 서비스를 구성하는 방법에 대해 설명합니다. 이것은 더 큰 유연성과 기능을 허용하는 ID 서비스(802.1x, MAB (MAC 인증 우회), WebAuth) 를 구성 하는 새로운 방법입니다. Cisco C3PL(Common Classification Policy Language)을 로컬 또는 Cisco ISE(Identity Services Engine) 서버에 저장할 수 있는 서비스 템플릿과 함께 사용합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst 3850 Series 스위치, Cisco IOS® CLI
- Cisco ISE
- ID 서비스(802.1x/MAB/WebAuth)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 3850 Series Switch, Cisco IOS 버전 03.03.00SE 이상
- Cisco ISE 버전 1.2 이상

참고: Support Matrix를 보려면 IBNS 2.0 구축 가이드를 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

서비스 템플릿에는 제어 정책의 특정 작업을 통해 사용자 세션에 연결할 수 있는 정책 특성 집합이 포함되어 있습니다. 이 문서에는 두 가지 예가 나와 있습니다.

- 실패 시나리오에 사용되는 MAB 및 로컬 정의 서비스 템플릿.
- 장애 시나리오에 사용되는 MAB 및 ISE 정의 서비스 템플릿.

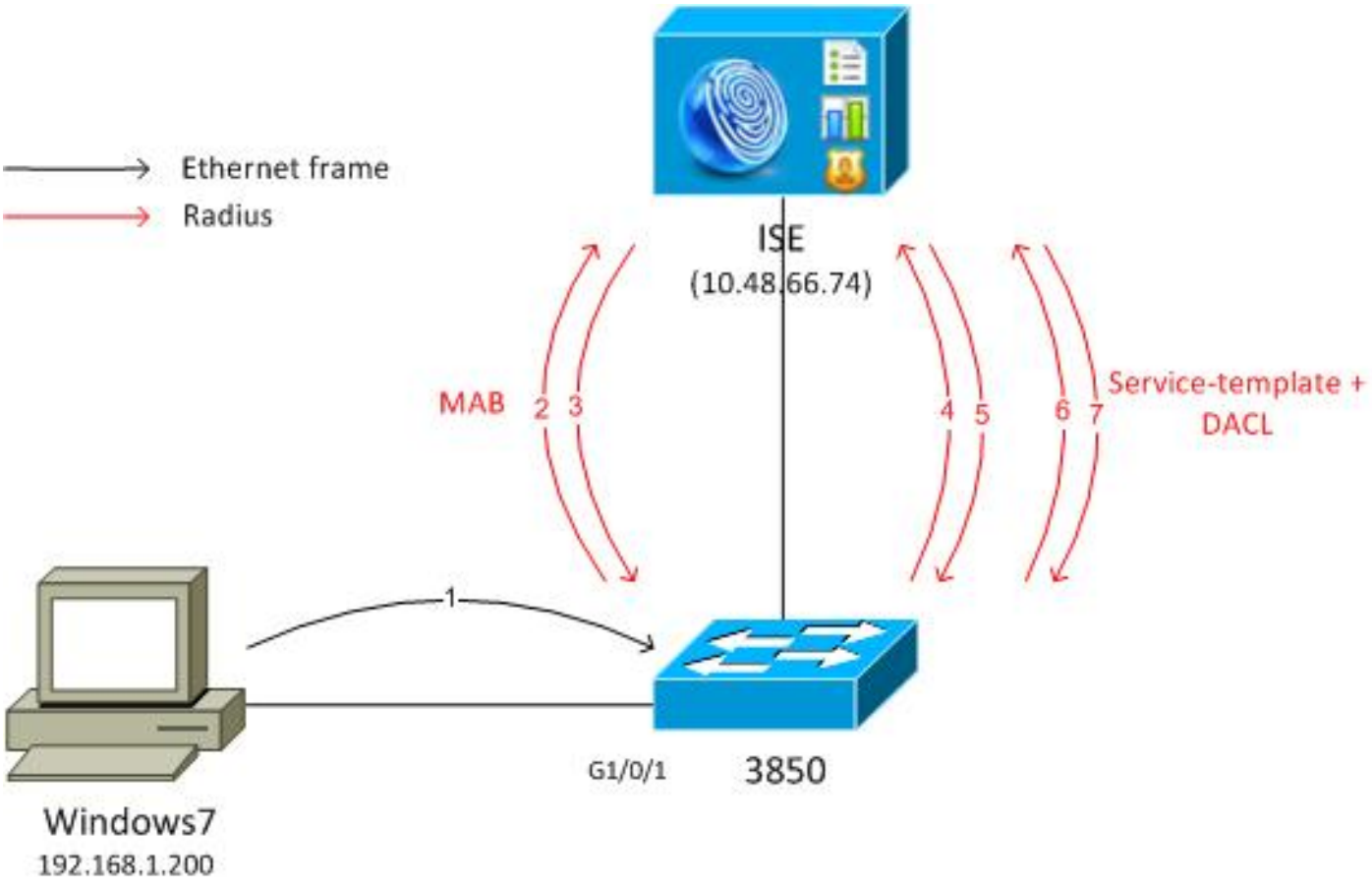
이 문서에서는 MAB가 예로 사용됩니다. 그러나 802.1x 및/또는 WebAuth를 사용하고 C3PL로 복잡한 정책을 구축할 수 있습니다.

구성

참고: 이 섹션에서 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용하십시오.

네트워크 다이어그램

여기에 제시된 두 가지 예는 모두 MAB를 수행하는 스위치에 연결되는 Windows PC와 관련이 있습니다. Windows MAC 주소가 ISE에 구성되어 있지 않으므로 MAB가 실패합니다. 그런 다음 스위치는 서비스 템플릿에 정의된 정책을 적용합니다.



로컬 정의 서비스 템플릿

MAB 실패 후 스위치는 로컬로 정의된 서비스 템플릿을 적용합니다.

흐름은 다음과 같습니다.

1. Windows에서 이더넷 프레임을 보냅니다.

2. 스위치는 MAB를 수행하고 MAC 주소를 사용자 이름으로 사용하여 ISE로 RADIUS 요청을 보냅니다.

3. ISE는 해당 엔드포인트를 구성하지 않고 RADIUS-Reject를 반환합니다.

4. 스위치는 로컬로 정의된 템플릿 정책 MAB_FAIL을 활성화합니다.

자세한 내용은 Cisco IOS XE Release 3SE(Catalyst 3850 스위치)의 Identity-Based Networking Services 컨피그레이션 가이드를 참조하십시오.

다음은 기본 예입니다.

```
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
```

ISE에 정의된 서비스 템플릿

흐름은 다음과 같습니다.

1. Windows에서 이더넷 프레임을 보냅니다.

2. 스위치는 MAB를 수행하고 MAC 주소를 사용자 이름으로 사용하여 ISE로 RADIUS 요청을 보냅니다.

3. ISE는 해당 엔드포인트를 구성하지 않고 RADIUS-Reject를 반환합니다.

4. 스위치는 ISE AAA(Authentication, Authorization, and Accounting) 목록을 사용하여 템플릿 정책 **MAB**_FAIL을 활성화합니다. RADIUS-Request는 템플릿 이름(**MAB_FAIL**)으로 사용자 이름과 하드코딩된 비밀번호로 전송됩니다. **cisco123**. 또한 Cisco AV(Attribute Value) 쌍도 **download-request=service-template에 연결됩니다**.

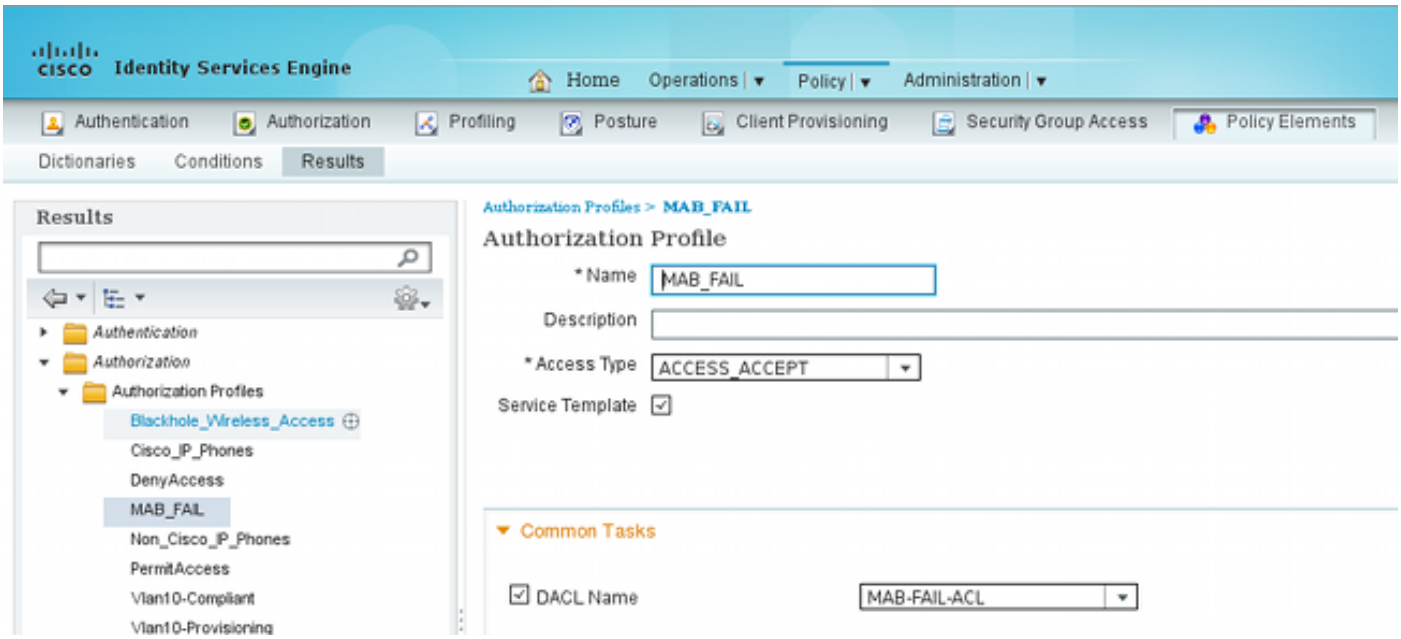
5. 해당 AV 쌍은 ISE에서 해당 요청을 서비스 템플릿 요청으로 처리하도록 강제합니다. 인증 및 권한 부여 규칙에 대한 모든 검사는 생략됩니다. ISE는 동일한 이름(**MAB**_FAIL)의 권한 부여 프로파일이 **존재하는지** 여부만 확인합니다. 로컬 사용자 저장소에서 **MAB_FAIL** 사용자를 구성할 필요가 없습니다. 그런 다음 ISE는 해당 프로파일과 연결된 모든 특성을 반환합니다. 이 예에서는 DACL(Downloadable Access Control List)입니다.

6. DACL이 스위치에 캐시되지 않은 경우 해당 DACL에 대해 다른 RADIUS-Request를 보냅니다.

7. DACL 콘텐츠가 반환됩니다. 스위치가 정책을 적용합니다.

ISE 구성

네트워크 액세스 장치를 추가 한 후, 인증 프로파일은 필요 합니다.



Service Template(**서비스 템플릿**) 확인란을 선택하고 스위치에 정의된 것과 동일한 이름을 사용해야 합니다.

Catalyst 3850 Series 스위치 컨피그레이션

이 구성은 첫 번째 예제와 네 가지 차이점이 있습니다.

- 로컬 **MAB_FAIL_LOCAL** 정책 템플릿이 제거됩니다.
- CoA(Change of Authorization) 지원이 추가되었습니다.
- **MAB**_FAIL 정책 템플릿(ISE에 구성된 정책)에 대한 ISE 목록이 사용됩니다.
- 서비스 템플릿 검색을 위한 AAA 권한 부여 목록의 이름이 지정됩니다.

구성은 다음과 같습니다.

```
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
```

ISE에서 템플릿(권한 부여 프로파일)을 변경한 후 스위치에서 RADIUS CoA 지원을 구성해야 합니다. 스위치에서 템플릿을 업데이트하기 위해 CoA를 전송해야 하기 때문입니다.

다음을 확인합니다.

로컬 정의 서비스 템플릿

Catalyst 3850 Series 스위치에서 다음 명령을 입력하여 사용자 세션을 확인합니다.

```
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
```

ISE에 정의된 서비스 템플릿

Catalyst 3850 Series 스위치에서 다음 명령을 입력하여 사용자 세션을 확인합니다.

```
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
```

상태는 Failed(**실패**)이지만, 특정 템플릿 및 관련 DACL이 적용됩니다.

```
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
```

ACL(Access Control List)은 인터페이스 아래에 표시되지 않습니다.

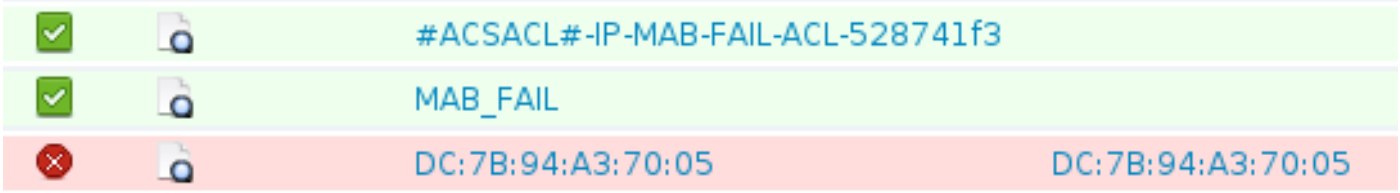
```
3850-1#show ip access-lists  interface g1/0/1 in
3850-1#show ip access-lists  interface g1/0/1
3850-1#show ip access-lists  interface g1/0/1 out
3850-1#
```

ASIC(하드웨어)가 올바르게 프로그래밍되었는지 확인할 수 있습니다.

```
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)
```

다른 DACL이 있는 각 사용자 세션에는 ASIC에 프로그래밍된 별도의 항목이 있습니다. ISE에는 세 가지 개별 인증이 있습니다.

- 실패한 MAB
- 성공적인 서비스 템플릿 검색(MAB_FAIL)
- 성공적인 DACL 검색



다음은 서비스 템플릿에 대한 요청을 수신할 때의 단계입니다.

11001 수신된 RADIUS 액세스 요청
11017 RADIUS가 새 세션을 생성했습니다.
11022 권한 부여 프로필에 지정된 dACL을 추가했습니다.
11002 반환된 RADIUS 액세스 수락

이는 인증/권한 부여 규칙이 처리되지 않음을 분명히 보여줍니다.

문제 해결

로컬 정의 서비스 템플릿

현재 시나리오의 디버그는 다음과 같습니다. 명확성을 위해 일부 출력은 생략됩니다.

```
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]
```

ISE에 정의된 서비스 템플릿

현재 시나리오의 디버그는 다음과 같습니다. 명확성을 위해 일부 출력은 생략됩니다.

```
<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.
```

ISE에 올바른 권한 부여 프로파일이 없는 경우 다음과 같이 보고됩니다.

11001 수신된 RADIUS 액세스 요청

11017 RADIUS가 새 세션을 생성했습니다.

11003 반환된 RADIUS 액세스 거부

또한 **Event 5400 Authentication failed(이벤트 5400 인증 실패)** 메시지가 표시되지만 더 이상 자세한 내용은 표시되지 않습니다. **cisco**123 비밀번호를 사용하여 사용자 이름을 생성한 후에는 올바른 인증/권한 부여 규칙이 있는 경우에도 오류가 동일하게 유지됩니다. 해당 기능이 올바르게 작동하려면 올바른 권한 부여 프로파일을 사용해야 합니다.

관련 정보

- Identity-Based Networking Services 컨피그레이션 가이드, Cisco IOS XE Release 3SE
- 통합 플랫폼 명령 참조, Cisco IOS XE 3.2SE
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.