失败的身份验证和授权

安全访问操作指南系列

作者：John Eppich

日期：2012 年 8 月

目录

对失败的身份验证和授权进行故障排除

概述

Cisco TrustSec 依赖于多个组件。当身份验证在 TrustSec 环境中失败时，可能难以找出问题的根本原因，因为您可能需要查看不同的组件。TrustSec 2.1 组件包括：

- 思科 ISE 节点
- 网络接入设备 (NAD)：Cisco Catalyst® 交换机、思科无线局域网控制器 (WLC)、Cisco ASA 自适应安全设备
- 请求方
- 外部身份库

借助最新的增强功能，思科致力于通过以下方式为故障排除提供单点视图：将交换机系统日志事件与内部 ISE 事件进行关联以及通过在 ISE 上提供接口按需对不同的身份验证相关信息进行轮询。ISE 上的其他增强功能包括配置验证程序（即 TCP Dump 实用程序），以及能够在客户端运行基于证书的 EAP 类型的 Cisco AnyConnect® 网络访问管理器时提供有关请求方问题的详细信息的功能。

简要故障排除步骤

图 3 显示故障排除流程的简图。

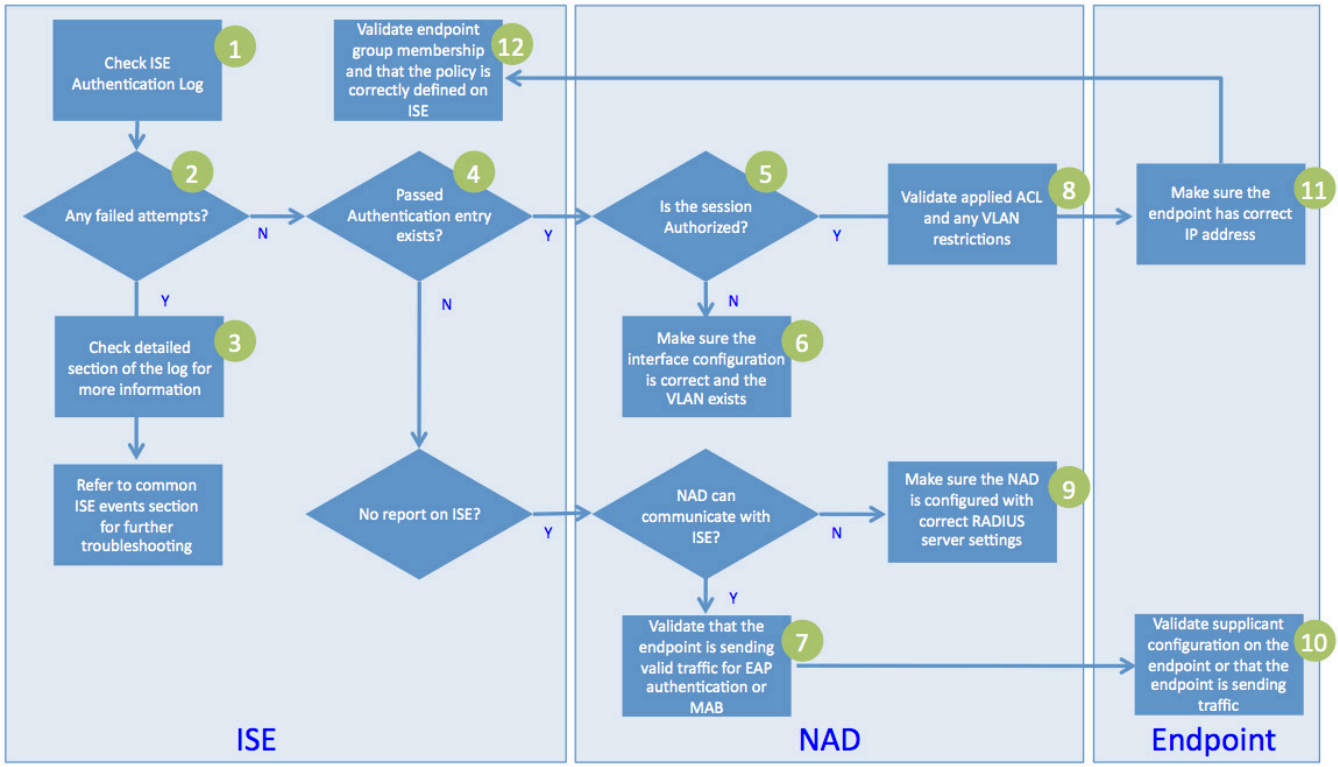

图 1. 简要故障排除步骤

检查 ISE 身份验证日志

步骤 1 登录到主 ISE 策略管理节点 (PAN)。
步骤 2 转至 Operations → Authentications。
步骤 3 （可选）如果事件在实时身份验证日志中不存在，请转至 Operations → Reports → Catalog → AAA Protocol → RADIUS Authentication。

检查日志中的所有失败的身份验证尝试

步骤 1 如果已知 MAC 地址或用户名，请使用过滤器仅查看来自特定终端的事件。

注：即使对于 802.1X 身份验证而言，改用 MAC 地址进行过滤也有益处，原因是：根据发生失败的具体过程，ISE 可能无法获知终端用户或计算机名称。

步骤 2 实时身份验证日志（图 4）显示最近 24 小时的事件，因此请确保查看最新事件。
步骤 3 成功事件的状态为带有绿色背景色的 。失败事件将通过带有红色背景色的 明确标识状态。
步骤 4 记录网络设备和设备端口，然后继续操作。图 4 实时身份验证日志：失败的身份验证事件。

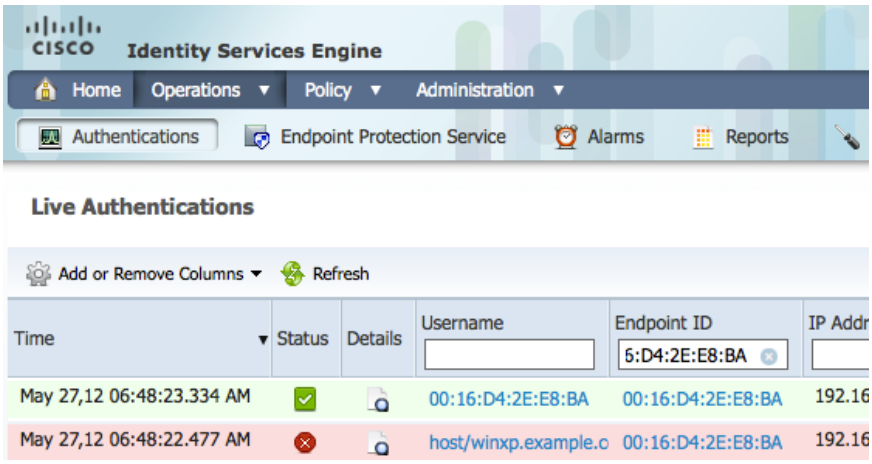

图 2. 实时身份验证

检查日志以了解详细信息

步骤 5 在实时身份验证日志中，检查 Failure Reason 列。
步骤 6 点击 按钮（Details 按钮）以了解详细信息。
步骤 7 点击身份验证失败消息以了解其他详细信息（图 5）。

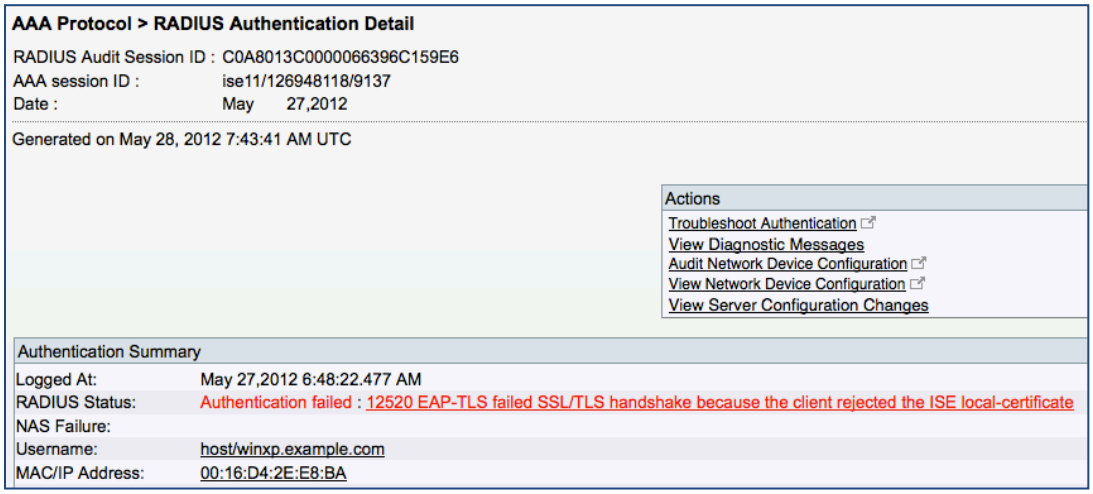

图 3. 失败的身份验证的详细信息

步骤 8 根据 Resolution Steps（图 6）执行补救操作。

本文档后续部分将对补救进行更详细的说明。

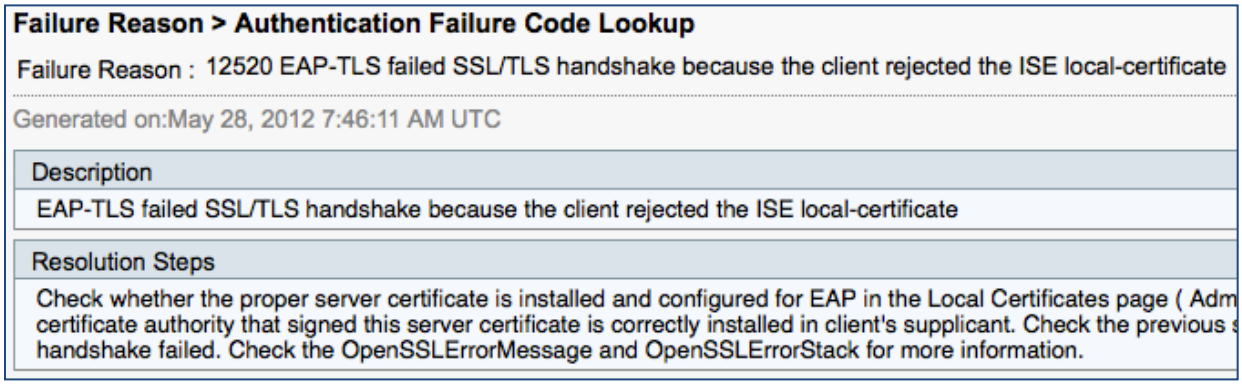

图 4. 身份验证失败代码查找

检查日志中的成功的身份验证条目或 MAC 地址

步骤 1 查看该终端的最新事件是否是成功的身份验证。

步骤 2 由于即使在身份验证成功后，终端也仍然有问题，因此 ISE 和网络接入设备 (NAD) 之间可能存在配置不匹配的情况。

步骤 3 如果没有该终端的事件，请按照图 3 中显示的流程图进一步对 NAD 和终端进行故障排除。

检查 NAD 接口状态或 ISE 详细报告

步骤 1 如果这是 Cisco Catalyst 交换机，请使用 Telnet 或安全外壳 (SSH) 登录并在支持的模式下运行以下命令：

```
show authentication sessions interface Gig x/y/z
```

步骤 2 （可选）如果交换机针对 ISE 配置为通过 SNMP 轮询信息，请选择 Operations → Authentications 来打开详细报告。然后，点击 按钮。图 7 显示结果：

图 1 身份验证详细信息：接口状态

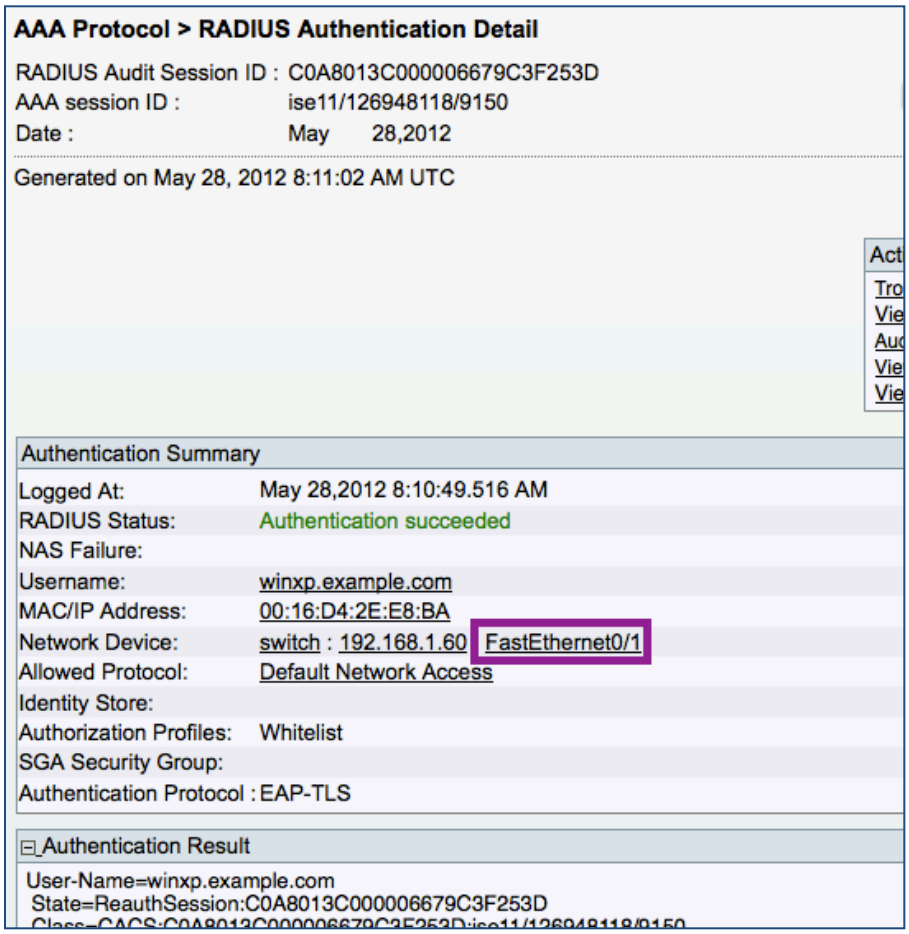

图 5.

步骤 3 （可选）在 Detailed Reports 中，点击接口名称（例如 Gigabit Ethernet x/y/z）。

步骤 4 随后将执行与步骤 1 中的 **`show authentication`** 命令等效的 SNMP 轮询，而无需您登录到个别交换机。

验证 WLC 或交换机配置

步骤 1 检查当前实施的 TrustSec 版本是否支持思科无线局域网控制器 (WLC) 配置或交换机操作系统平台和/或版本。

步骤 2 为使 NAD 能够授权，它需要在配置中具有以下条目：

```
aaa authorization network radius
```

步骤 3 对于动态 VLAN (dVLAN)，请在执行模式下运行以下命令，以检查 WLC 或交换机 VLAN 数据库是否包含 ISE 尝试分配的 VLAN：

```
show vlan
```

步骤 4 对于 dACL，请通过转至 Policy → Policy Elements → Results → Authorization → Downloadable ACLs 验证 ISE ACL 语法是否正确。

步骤 5 对于 Catalyst 交换机，可以使用 ISE Evaluate Configuration Validator 工具来验证配置。转至 Operations → Troubleshooting → Diagnostic Tools → General Tools（图 8）。

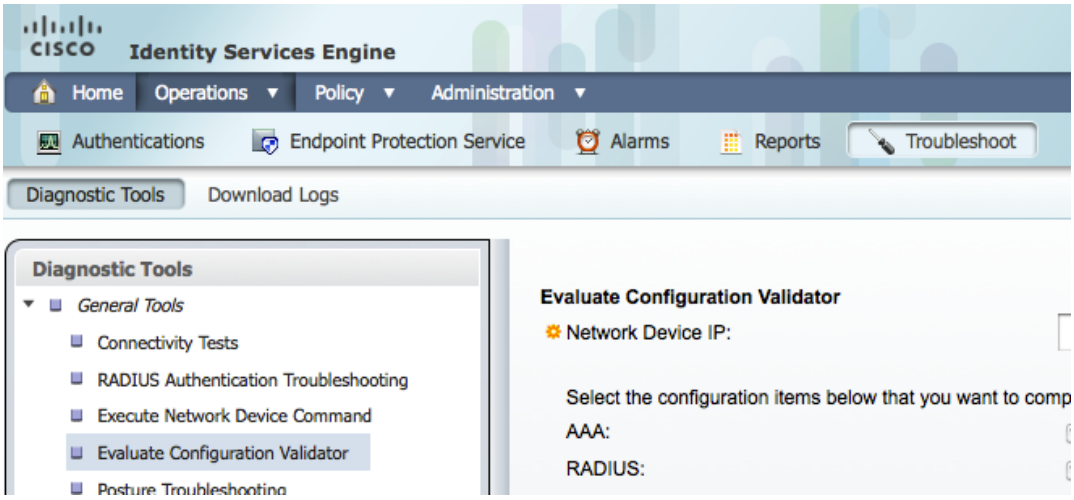

图 6. 评估验证器配置

验证终端到 NAD 通信

步骤 1 对于 Catalyst 交换机，请通过在执行模式下运行以下命令启用 802.1X 调试：

```
debug dot1x
```

步骤 2 通过检查调试日志，验证客户端是否在发送 EAP over LAN (EAPoL) 启动消息。

步骤 3 对于使用 MAC 身份验证绕行 (MAB) 的设备，请验证设备是否在发送流量。

如果使用推荐用于 Cisco TrustSec 2.1 的顺序和计时器设置来配置接口，则经过 30 秒后，交换机才会接受并使用来自终端的流量发送 MAB 请求。这对于频繁通信的设备（例如 Windows PC 设备）而言通常不是问题；但是，某些打印机可能需要一些时间来完成 MAB。如果您经历长时间延迟才成功对设备（例如打印机）执行 MAB，请考虑运行接口特定命令 **authentication control-direction in**，以允许在身份验证之前流量从网络传递到终端，从而加快 MAB 过程。

检查应用于 VLAN 和会话的 ACL

步骤 4 对于 dVLAN，请验证应用于 VLAN 的 ACL 是否未受到过多限制。为此，您可以查看 VLAN 接口 ACL 或将接口手动分配到未启用 802.1X 的接口并验证终端状况。

步骤 5 对于 dACL，请验证应用于会话的 ACL 是否未受到过多限制。以下列出一些有用的命令：

```
show authentication sessions interface <int_name>
show ip access-list interface <int_name>
show running-config interface <int_name>
show access-list <int_name>
```

在 NAD 上验证 RADIUS 配置

步骤 6 对于 Catalyst 交换机，请运行 Evaluate Configuration Validator（如程序 6 所述）以验证 RADIUS 配置。

步骤 7 从 NAD 尝试对 ISE 策略服务节点 (PSN) 执行 ping 操作。

步骤 8 如果在 NAD 和 ISE PSN 之间有任何过滤设备，请验证该设备是否允许 RADIUS 身份验证、授权和记帐（UDP 1645/1656 或 1812/1813）。

步骤 9 您可以使用 Cisco IOS® 软件测试功能运行测试身份验证。在执行模式下输入以下命令：

```
test aaa group radius {test_user} {test_password} new-code
```

验证终端是否具有正确的 IP 地址

步骤 1 接下来，我们需要验证请求方是否已正确配置并且是否正在运行。首先，我们将验证终端是否具有正确的 IP 地址。

步骤 2 对于 Windows 设备，请从命令提示符运行以下命令：

```
ipconfig /all
```

步骤 3 对于 Mac OS X 和 Linux 设备，请从命令提示符运行以下命令：

```
ifconfig
```

步骤 4 对于无客户端设备，请参阅设备用户指南以找出 IP 地址。

验证 ISE 终端组和授权策略

步骤 1 如果是对 MAB 身份验证进行故障排除，请通过转至 Administration → Identity Management → Endpoints 验证终端 MAC 地址是否在正确的终端组中。

步骤 2 详细终端屏幕将在身份组分配中显示当前终端组。如果分配不正确，请使用正确的组进行更新。

步骤 3 通过转至 Policy → Authorization 验证授权规则。

TrustSec 组件

请求方

如前所述，对身份验证失败进行故障排除时，首先应检查 ISE 策略管理节点 (PAN)。某些失败需要在 NAD 级别执行额外的诊断工作。大多数情况下，来自 ISE 和 NAD 的日志及调试应足以确定问题的根本原因。

可以对请求方执行的诊断工作很大程度上取决于特定请求方提供的故障排除工具。本地 Windows 请求方几乎没有任何调试工具。Cisco AnyConnect 网络访问管理器具有可以部署到客户端并用于生成详细报告文件的诊断和报告工具 (DART)。但是，报告文件主要供思科支持人员使用，通常不推荐最终用户使用。

嗅探器提供重要的故障排除信息，但是其在最终客户端上的使用也会受到限制。一般来说，使用思科交换端口分析器 (SPAN) 嗅探交换机的流量是收集 EAP 数据包跟踪的更可靠且有效的方式。

在客户端发送 EAPoL 启动请求，但是未能响应来自交换机的身份请求消息的情况下，会发生一些常见的请求方故障。通常，发生此情况是因为请求方无法找到有效的凭证。当客户端“静默”时，交换机或思科 ISE 将无法了解故障。

与 Windows 本地请求方或其他操作系统上可用的其他请求方不同，Cisco AnyConnect 网络访问管理器包含用于通知 ISE 故障原因的增强功能。例如，客户端配置错误且在 EAP 透明层安全 (EAP-TLS) 或受保护 EAP (PEAP) 身份验证中不信任 ISE 证书的情况（图 9）。

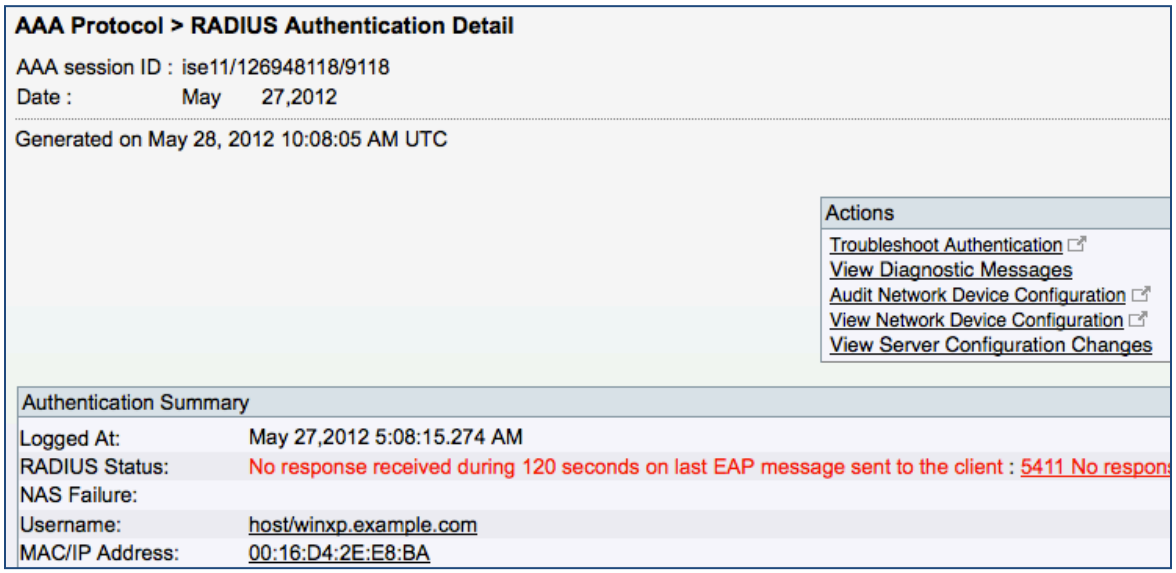

图 7. 失败的身份验证报告：本地请求方

在图 9 中，PC 上使用了 Windows 本地请求方。没有关于除以下原因代码以外的其他事件的详细信息：`5411 No response received during 120 seconds on last EAP message sent to the client`。此时，管理员将必须登录到受影响的终端对问题进行故障排除。

图 10 显示其中 PC 运行的是 Cisco AnyConnect 网络访问管理器的示例。失败原因明确指示问题在于请求方设置。

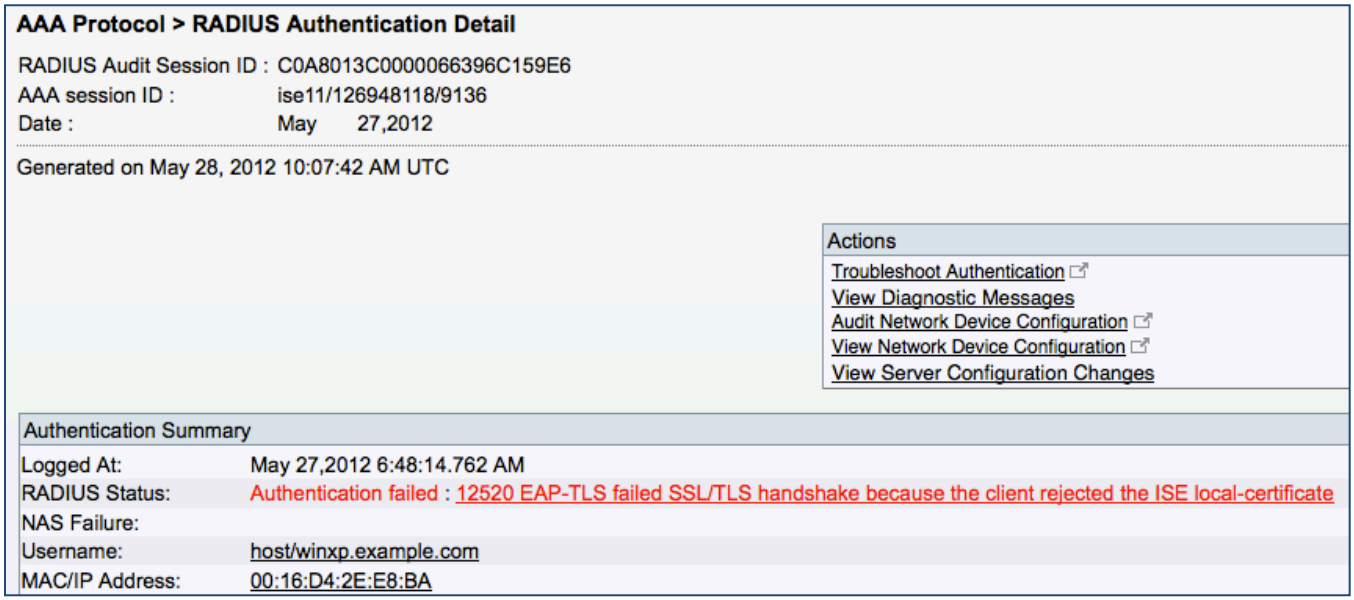

图 8. 失败的身份验证报告：Cisco AnyConnect NAM

网络接入设备 (NAD)

对 Cisco TrustSec 身份验证问题进行故障排除所需的大部分信息都可以从 ISE 本身收集。但是在某些情况下，ISE 无法提供足够的信息来对失败的身份验证进行故障排除。因此，有必要检查 NAD 的故障排除功能。

有用的 Cisco IOS show 命令

Cisco Catalyst 交换机上其中一个最有用的 show 命令是 **`show authentication sessions interface`**。命令输出显示指定端口的当前身份验证状态。其他有用的命令包括 `show dot1x interface` 和 `show running-config interface`。

```
Switch#show authentication sessions interface fastEthernet 0/1
            Interface:  FastEthernet0/1
          MAC Address:  0016.d42e.e8ba
           IP Address:  192.168.1.78
            User-Name:  winxp.example.com
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  100
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8013C000006679C3F253D
      Acct Session ID:  0x00000C51
               Handle:  0x68000667

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run

Switch#
Switch#
Switch#show dot1x interface fastEthernet 0/1
Dot1x Info for FastEthernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_DOMAIN
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 10

Switch#
Switch#
Switch#show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 599 bytes
!
interface FastEthernet0/1
 description 802.1x Enabled
 switchport access vlan 2
 switchport mode access
```

```
 switchport voice vlan 110
 authentication event fail action next-method
 authentication event no-response action authorize vlan 100
 authentication event server alive action reinitialize
 authentication host-mode multi-domain
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
end

Switch#
Switch#
```

SPAN

用于在身份验证器上调试 802.1X 失败情况的其中一种最有用的工具是交换端口分析器 (SPAN)。通过 SPAN，可以将在一个端口上发送和接收的所有 EAP 流量镜像到可由嗅探器进行分析的其他端口。通过嗅探身份验证器和客户端之间交换的实际 EAP 数据包，可以诊断从思科 ISE 不可见的一些失败。

要将 Cisco Catalyst 3000 系列交换机配置为将所有流量从一个端口（源端口）镜像到另一个端口（目标端口），请在配置模式下使用以下 Cisco IOS 命令：

```
(config)# monitor session 1 source interface Gigabit 0/1
(config)# monitor session 1 destination interface Gigabit 0/2 encapsulation replicate
```

要将 Cisco Catalyst 4500 系列交换机配置为将所有流量从一个端口（源端口）镜像到另一个端口（目标端口），请在配置模式下使用以下 Cisco IOS 命令：

```
(config)# monitor session 1 source interface Gigabit 1/1
(config)# monitor session 1 destination interface Gigabit 1/2
```

由于 Cisco Catalyst 4500 会监控具有以上显示的默认 SPAN 配置的所有第 2 层帧，因此在 Cisco Catalyst 4500 系列交换机上的第 2 层帧上使用 SPAN 无需特殊配置选项。

与 ISE PSN 的通信

当客户端尝试进行身份验证时，交换机没有或无法将 RADIUS 消息发送到 AAA 服务器有三种常见原因：

- 缺乏适当的网络连接
- 交换机上的 RADIUS 配置
- 缺乏来自客户端的响应

要验证网络连接，请从交换机对 AAA 服务器执行 ping 操作。以下是 ping 命令示例：

```
Switch#
Switch#ping 192.168.1.60

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.60, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

如果 ping 不成功，或者某些数据包被丢弃，请使用标准路由和交换调试技术在交换机和 AAA 服务器之间建立可靠的连接。

如果 ISE PSN 可以通过 ping 连通，则在此情况下使用 `test aaa` 诊断命令可有所帮助。以下示例说明此命令：

```
Switch#test aaa group radius testuser cisco123 new-code
User successfully authenticated

Switch#
```

`test aaa` 命令导致交换机向 AAA 服务器发送访问请求，从而（在本例中）使用密码 `cisco123` 对用户 `testuser` 进行 PAP（明文）身份验证。交换机将尝试向 radius-server host 命令中配置的服务器进行身份验证。或者，如果您使用的是 AAA 组而不是默认 RADIUS 组，则可以指定特定 RADIUS 组对配置为该组的一部分的特定服务器进行测试。

如果 **`test aaa`** 命令的结果为 `User successfully authenticated`（如先前代码片段中所示），则意味着有三种情况成立：交换机正确配置为与 AAA 服务器通信（正确的共享密钥）；交换机具有到 AAA 服务器的网络连接；test 命令中指定的用户名和密码有效。ISE 实时身份验证事件将显示以下身份验证：

```
Switch#test aaa group radius testuser cisco123 new-code
User rejected

Switch#
```

如果 `test aaa` 命令的结果为 `User authentication request was rejected by server`，则表明交换机配置有效并且网络连接进行了验证，但是 test 命令中提供的用户名和/或密码无效。此失败的身份验证将显示在 ISE 实时身份验证事件中。另一种可能性是交换机无法向 AAA 服务器进行身份验证。共享密钥不匹配，或者没有到 AAA 服务器的网络连接，这可能是 AAA 服务器没有收到 RADIUS 消息的原因。重新验证配置和/或验证网络连接将使交换机能够在 802.1X 身份验证期间与 AAA 服务器通信。

策略不匹配

如果 ISE 实时身份验证显示终端的身份验证成功，但是 `show authentication sessions interface Gigabit x/y/z` 的结果表明端口未经授权，则 ISE 策略和交换机之间可能策略不匹配。这意味着，虽然 ISE 能够对会话进行身份验证和授权，但是从 ISE 发送到 NAD 的属性值对无效。此情况的常见原因包括：

- VLAN 不存在。
- 存在 ACL 语法错误。
- 存在 AVP 语法错误。

如果 AAA 服务器已尝试分配交换机上未定义的 VLAN，则交换机将无法对端口授权。在以下示例中，AAA 服务器尝试分配名为 EMPLOYEE 的 VLAN。交换机返回以下系统日志消息：

```
Switch#
Switch#
May 28 07:06:11.156 UTC: %AUTHMGR-5-START: Starting 'dot1x' for client (0016.d42e.e8ba) on
Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %DOT1X-5-SUCCESS: Authentication successful for client (0016.d42e.e8ba)
on Interface Fa0/1 AuditSessionID
May 28 07:06:11.592 UTC: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for
client (0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or
shutdown VLAN EMPLOYEE to 802.1x port FastEthernet0/1 AuditSessionID C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %AUTHMGR-5-FAIL: Authorization failed for client (0016.d42e.e8ba) on
Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
May 28 07:06:11.592 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C0000066D9D16ABF7| AUTHTYPE DOT1X| EVENT APPLY
May 28 07:06:11.592 UTC: %EPM-6-IPEVENT: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C0000066D9D16ABF7| AUTHTYPE DOT1X| EVENT IP-WAIT
May 28 07:06:11.592 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C0000066D9D16ABF7| AUTHTYPE DOT1X| EVENT REMOVE
May 28 07:06:11.592 UTC: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client
(0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C0000066D9D16ABF7
Switch#
Switch#
```

从以下输出中您可以看到，交换机的员工 VLAN 命名为 EMP 而不是 EMPLOYEE：

```
Switch#sh vlan | i EMP
100  EMP      active    Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22,
```

由于交换机没有 VLAN 名称 EMPLOYEE 的精确匹配，因此其会向终端发送 EAP 失败消息。要修复此问题，请重命名交换机上的 VLAN，或者在 ISE 授权配置文件中定义正确的名称。

在以下示例中，dACL 使用错误的语法。ISE 发送了 `allow ip any any` 而不是 `permit ip any any`。

```
Switch#
May 28 07:11:59.395 UTC: %AUTHMGR-5-START: Starting 'dot1x' for client (0016.d42e.e8ba) on
Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
May 28 07:11:59.815 UTC: %DOT1X-5-SUCCESS: Authentication successful for client (0016.d42e.e8ba)
on Interface Fa0/1 AuditSessionID
May 28 07:11:59.815 UTC: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for
client (0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
May 28 07:11:59.823 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| EVENT APPLY
May 28 07:11:59.823 UTC: %EPM-6-AUTH_ACL: POLICY Auth-Default-ACL| EVENT Auth-Default-ACL Attached
Successfully
```

```
May 28 07:11:59.823 UTC: %EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fc368f7| EVENT
DOWNLOAD-REQUEST
May 28 07:11:59.840 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to
up
May 28 07:11:59.890 UTC: %EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4fc368f7| EVENT
DOWNLOAD-FAIL
May 28 07:11:59.890 UTC: %EPM-4-POLICY_APP_FAILURE: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| POLICY_TYPE dACL| POLICY_NAME xACSACLx-IP-
PERMIT_ALL_TRAFFIC-4fc368f7| RESULT FAILURE| REASON AAA download failure
May 28 07:11:59.890 UTC: %EPM-6-IPEVENT: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| EVENT IP-WAIT
May 28 07:11:59.890 UTC: %AUTHMGR-5-FAIL: Authorization failed for client (0016.d42e.e8ba) on
Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
May 28 07:11:59.890 UTC: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client
(0016.d42e.e8ba) on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
May 28 07:11:59.890 UTC: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0016.d42e.e8ba| AuditSessionID
C0A8013C000006719D1BFAB1| AUTHTYPE DOT1X| EVENT REMOVE
May 28 07:11:59.899 UTC: %EPM-6-AUTH_ACL: POLICY Auth-Default-ACL| EVENT DETACH-SUCCESS
May 28 07:11:59.899 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to
down
May 28 07:12:00.846 UTC: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (0016.d42e.e8ba)
on Interface Fa0/1 AuditSessionID C0A8013C000006719D1BFAB1
Switch#
Switch#
```

由于交换机无法处理 dACL，因此其会向终端发送 EAP 失败响应。要修复此问题，请在 ISE 上更正 dACL 中的语法错误，如下所示：

```
Switch#show authentication sessions interface FastEthernet 0/1
            Interface:  FastEthernet0/1
          MAC Address:  0016.d42e.e8ba
           IP Address:  192.168.2.100
            User-Name:  winxp.example.com
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8013C000006719D1BFAB1
      Acct Session ID:  0x00000C5D
               Handle:  0xB2000671

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run

Switch#
```

身份服务引擎 (ISE)

在查看特定失败的症状和原因之前，建议从 ISE 的角度查看身份验证成功所表现出来的状况。本节还将用来查看可用于对身份验证失败进行故障排除的工具。

实时身份验证日志

ISE 中的实时身份验证日志列出所有已到达 ISE 的身份验证。如果在此屏幕中没有用户的条目，则表明 ISE 尚未收到身份验证请求。

您可以通过登录到 ISE 主 PAN 并转至 Operations → Authentications 查看实时身份验证日志，这样将打开一个类似于图 11 中显示的屏幕。

注：实时身份验证日志屏幕由主 MnT 节点提供。相同的信息在备份 MnT 节点上也可用。此外，也可以通过登录到辅助 PAN 并且还直接登录到任一 MnT 节点来访问实时身份验证日志。

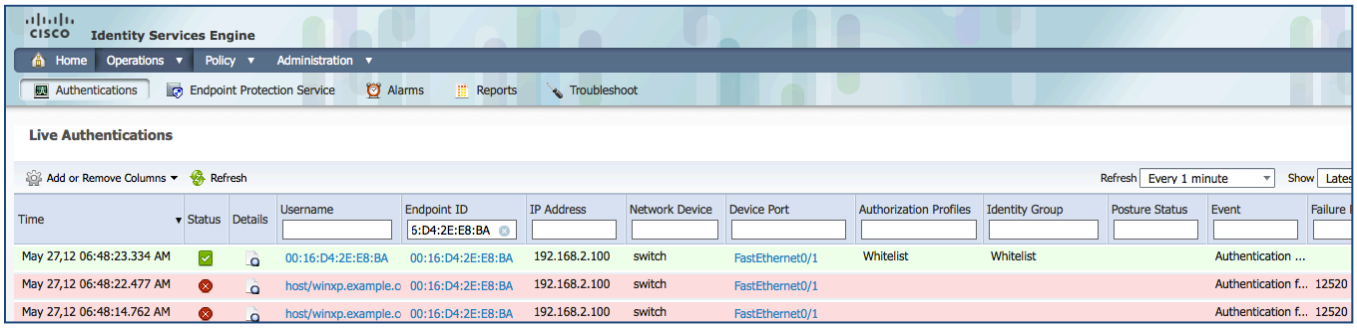

图 9. 实时身份验证日志

实时身份验证日志具有对于确定网络上的设备、其连接时间和位置及其身份验证方式至关重要的几条重要信息。

注：此处说明的所列的一些列仅通过使用 Add/Remove Columns 功能才可见。要使这些列可见，请右键点击标题行。

- **Time** - 显示收集代理接收到日志的时间。此列是必需的，不能禁用。
- **Status** - 显示身份验证成功还是失败。此列是必需的，不能禁用。
- **Details** - 在点击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列是必需的，不能禁用。
- **Username** - 显示与身份验证关联的用户名。
- **Endpoint ID** - 显示终端的唯一标识符，通常为 MAC 或 IP 地址。
- **IP Address** - 显示终端设备的 IP 地址。
- **Network Device** - 显示网络接入设备的 IP 地址。
- **Device Port** - 显示连接终端的端口号。
- **Authorization Profiles** - 显示用于身份验证的授权配置文件。
- **Identity Group** - 显示分配给为其生成了日志的用户或终端的身份组。
- **Posture Status** - 显示状态验证的状态和有关身份验证的详细信息。
- **Event** - 显示事件状态。
- **Failure Reason** - 显示失败的详细原因（如果身份验证失败）。

- 或者，可以选择显示以下类别：
- **Auth Method** - 显示 RADIUS 协议使用的身份验证方法，例如 Microsoft 质询握手身份验证协议版本 2 (MSCHAPv2)、IEE 802.1x 或 dot1x 等等。
- **Authentication Protocol** - 显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
- **Security Group** - 显示由身份验证日志确定的组。
- **Server** - 指示从中生成日志的策略服务。
- **Session ID** - 显示会话 ID。

详细报告

图 12 和 13 显示详细身份验证报告，其中显示使用 EAP-TLS 成功对计算机进行身份验证。在图 12 中，Authentication Summary 显示在实时身份验证日志页面中查看时可用的信息。在图 13 中，Related Events 来自与此会话相关的 NAD 的系统日志。当 NAD 将事件发送到 ISE MnT 节点时，这些事件自动关联并包含在详细报告中。

图 2

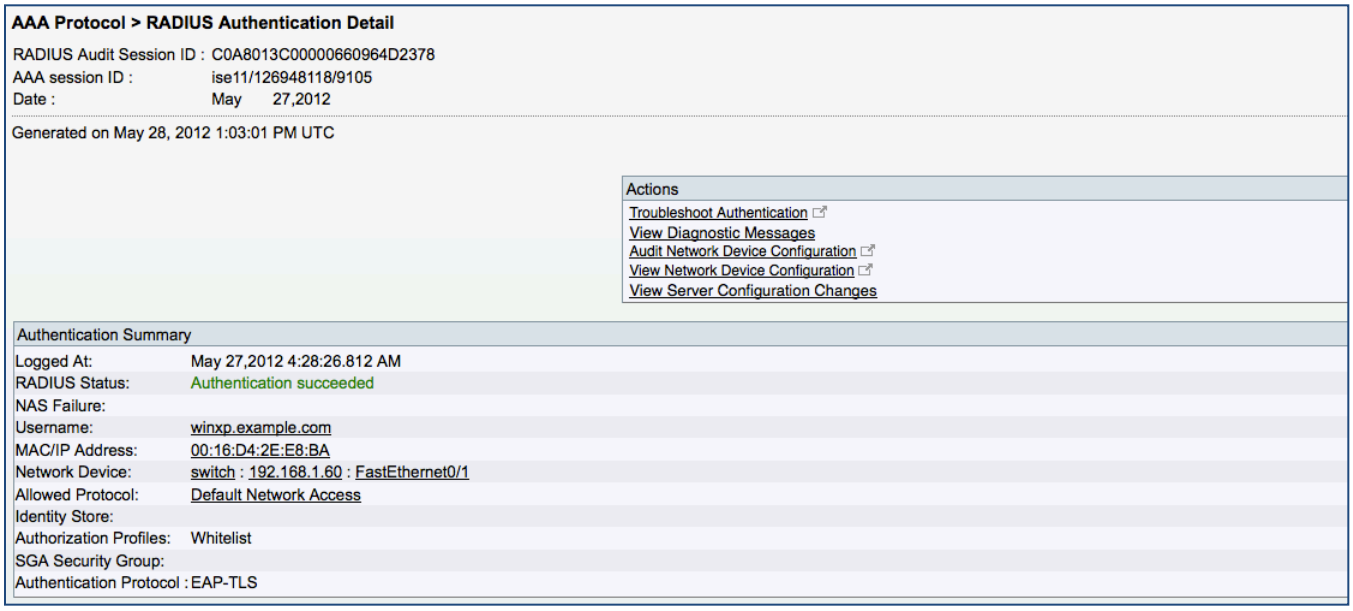

图 10. RADIUS 身份验证详细信息 1

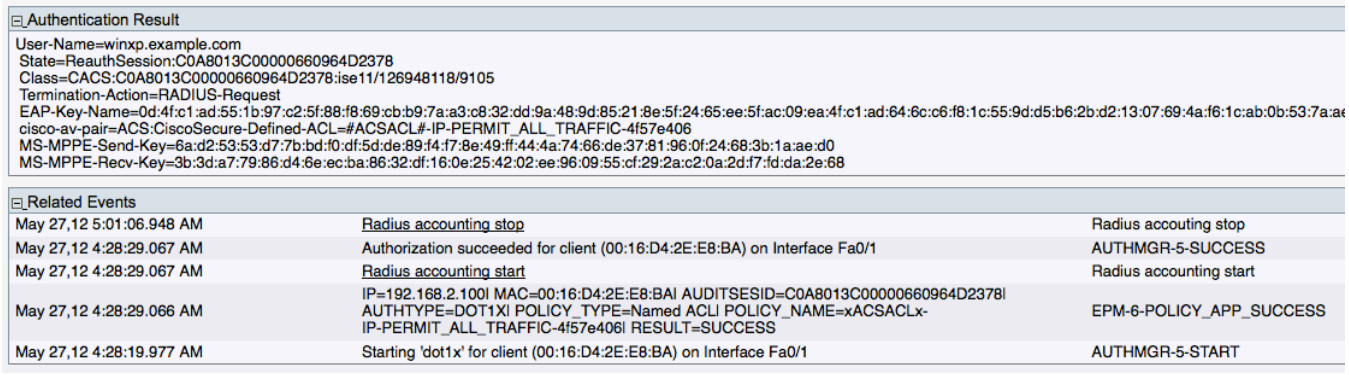

图 11. RADIUS 身份验证详细信息 2

要配置交换机以将系统日志发送到 ISE，请输入以下命令：

```
(config)# logging host {Primary_MnT} transport udp port 20514
(config)# logging host {Backup_MnT} transport udp port 20514
```

在图 14 中，Authentication Details 部分显示身份验证期间产生的其他信息。在图 15 中，Steps 部分显示会话在 ISE 中经历的详细过程。

Authentication Details	
Logged At:	May 27,2012 4:28:26.812 AM
Occurred At:	May 27,2012 4:28:26.804 AM
Server:	ise11
Authentication Method:	dot1x
EAP Authentication Method :	EAP-TLS
EAP Tunnel Method :	
Username:	winxp.example.com
RADIUS Username :	host/winxp.example.com
Calling Station ID:	00:16:D4:2E:E8:BA
Framed IP Address:	192.168.2.100
Use Case:	
Network Device:	switch
Network Device Groups:	Device Type#All Device Types,Location#All Locations
NAS IP Address:	192.168.1.60
NAS Identifier:	
NAS Port:	50001
NAS Port ID:	FastEthernet0/1
NAS Port Type:	Ethernet
Allowed Protocol:	Default Network Access

图 12. RADIUS 身份验证详细信息 3

Steps
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
Evaluating Service Selection Policy
15048 Queried PIP
15048 Queried PIP
15004 Matched rule
11507 Extracted EAP-Response/Identity
12500 Prepared EAP-Request proposing EAP-TLS with challenge
12625 Valid EAP-Key-Name attribute received
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12502 Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated
12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12809 Prepared TLS CertificateRequest message
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge

图 13. RADIUS 身份验证详细信息 4

报告

如果事件发生超过 24 小时，则其为历史事件，可以通过转至 Operations → Reports → Catalog → AAA Protocol → RADIUS Authentication 进行查看。

配置验证器

您可以使用此诊断工具评估网络设备的配置和确定所有配置问题。专业的故障排除人员设备上配置的是标准配置比较。图 16 显示 Evaluate Configuration Validator 选项。

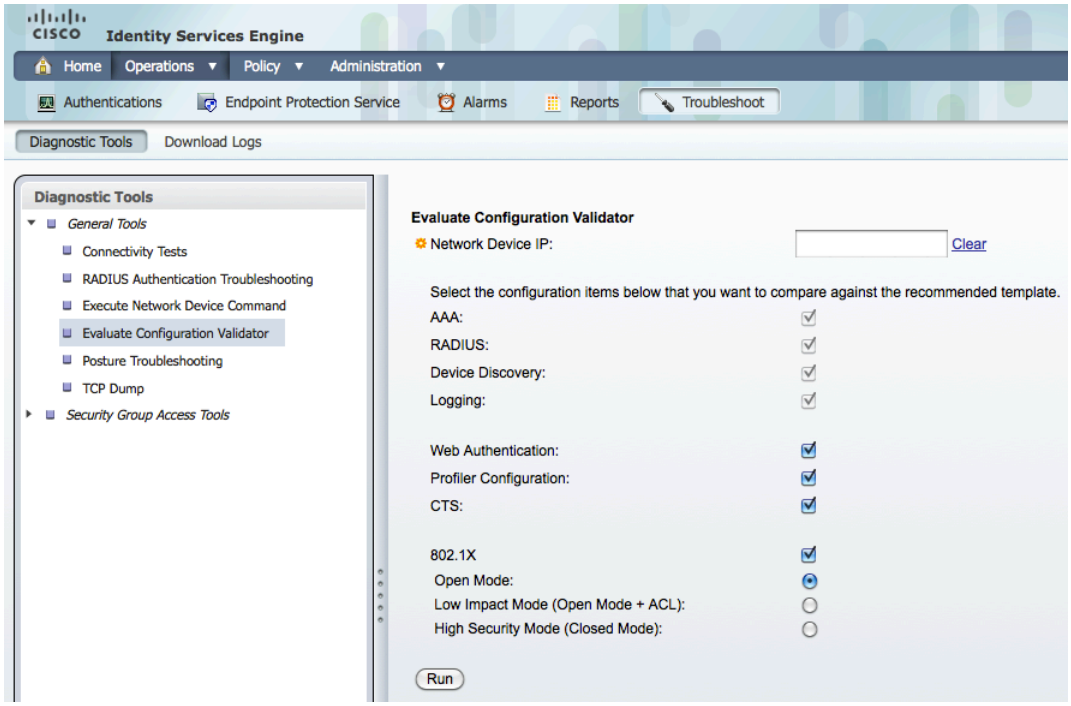

图 14. Evaluate Configuration Validator 选项

步骤 1 转至 Operations → Troubleshoot → Diagnostic Tools → Evaluate Configuration Validator。

步骤 2 输入要评估其配置的设备的 Network Device IP 地址，并且根据需要指定其他选项。

步骤 3 选择配置选项以针对建议模板进行比较。绿色复选标记表示此选项已选中。再次点击该选项将取消选中。从以下格式中选择：

步骤 4 Web Authentication - 选中此复选框可将设备的 Web Authentication 配置与标准配置相比较。

步骤 5 Profiler Configuration - 选中此复选框可将设备的 Profiler 配置与标准配置相比较。

步骤 6 CTS - 如果要将设备的 Security Group Access 配置与标准配置相比较，请选中此复选框。

步骤 7 802.1X - 如果要将设备的 802.1X 配置与标准配置相比较，请选中此复选框。然后，选择以下选项之一：

步骤 8 Open Authentication Mode

步骤 9 Low-Impact Mode (Open Mode + ACL)

步骤 10 High Security Mode (Closed Mode)

步骤 11 点击 Run。系统将显示 Progress Details 页面，提示您输入其他信息。

步骤 12 点击 User Input Required，并且根据需要修改字段。系统将显示一个新窗口，提示您为配置分析选择接口。

步骤 13 选中要分析的接口旁边的复选框，然后点击 Submit。系统将再次显示 Progress Details 页面。

步骤 14 点击 Show Results Summary。

TCP 转储

TCP 转储实用程序监控网络接口上与给定布尔表达式相匹配的数据包的内容。您可以使用此实用程序对网络上的问题进行故障排除。思科 ISE 故障排除诊断工具提供直观的用户界面（图 17）。

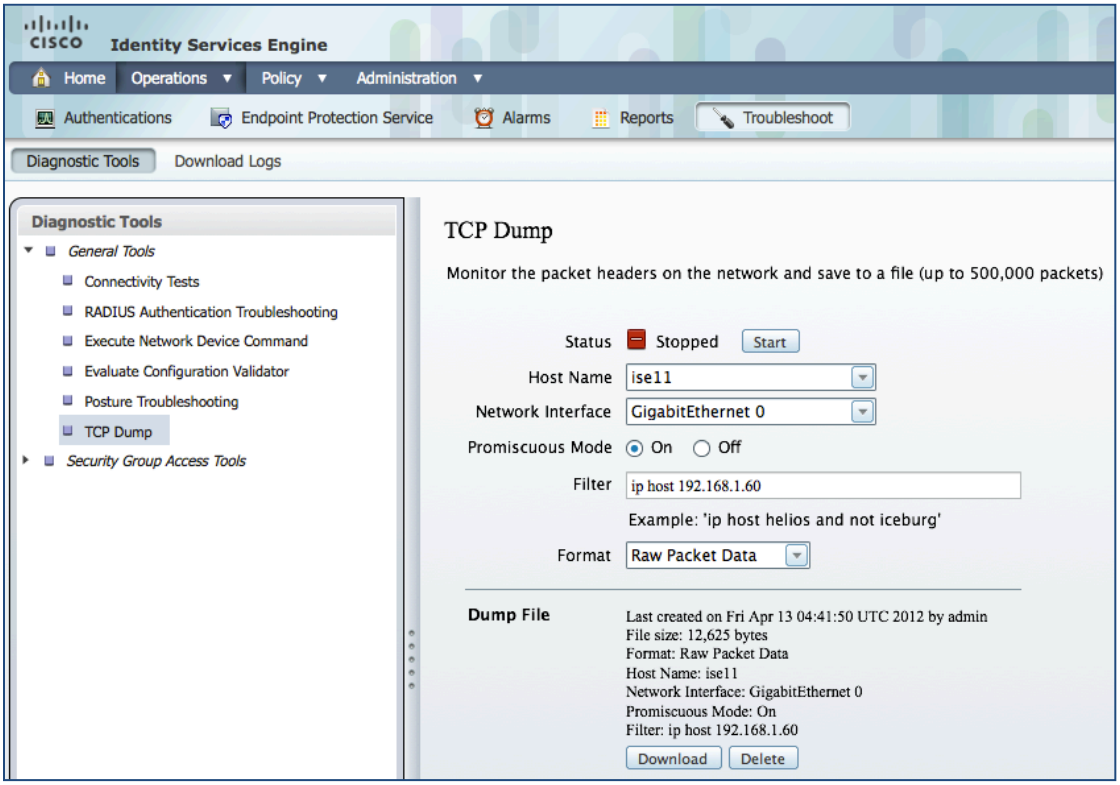

图 15. TCP Dump 选项

步骤 1 转至 Operations → Troubleshoot → Diagnostic Tools → TCP Dump。

步骤 2 从下拉菜单中选择要监控的网络接口。这是网络流量受监控或嗅探的接口。

步骤 3 通过点击单选按钮将 Promiscuous Mode 设置为 On 或 Off。默认设置为 On。

步骤 4 Promiscuous Mode 是默认数据包嗅探模式。我们建议您将被设置为 On。在此模式下，网络接口将所有流量传递到系统的 CPU。

步骤 5 在 Filter 字段中，输入要对其进行过滤的布尔表达式。支持标准 TCP Dump 过滤器表达式，例如以下表达式：`host 10.0.2.1` 和 `port 1812`。

步骤 6 点击 Start 开始监控网络。

步骤 7 当收集到足够数量的数据时点击 Stop，或者在累积最大数量的数据包 (500,000) 后等待过程自动完成。

失败的身份验证事件

TrustSec 身份验证可能由于许多原因而失败。其中包括未知用户、凭证错误、凭证到期、缺少证书、配置错误等等。通过仔细检查 ISE 日志，可以诊断其中许多失败。下面说明了常见失败及其症状。

5411 向客户端发出最后一条 EAP 消息之后的 120 秒内，未收到回应

适用对象	所有 EAP 类型
可能原因	NAD 或请求方：EAP 超时可能过于激进。 请求方：配置有基于证书的身份验证，而请求方没有有效的凭证或不信任 ISE 证书。 请求方和用户：配置有基于密码的身份验证，而用户未提供有效的凭证。
解决方法	验证请求方是否正确配置为与 ISE 开展完整的 EAP 对话。验证 NAS 是否正确配置为与请求方之间互相传输 EAP 消息。验证请求方或网络访问服务器 (NAS) 是否针对 EAP 对话不会短时间超时。检查用于将 NAS 连接到 ISE 的网络。如果外部 ID 库用于身份认证，则其可能不会足够快地响应当前超时。

12520 EAP-TLS 进行 SSL/TLS 握手失败，因为客户端拒绝 ISE 本地证书

适用对象	EAP-TLS（AnyConnect 网络访问管理器）
可能原因	请求方不信任 ISE PSN 证书。
解决方法	通过转至 Local Certificates 页面 (Administration > System > Certificates > Local Certificates) 检查是否为 EAP 安装并配置了适当的证书。另请确保签署此服务器证书的证书颁发机构正确安装在客户端的请求方中。检查此 EAP-TLS 对话的日志中的先前步骤，查找指示握手失败的消息。检查 `OpenSSLErrorMessage` 和 `OpenSSLErrorStack` 以获取详细信息。

22044 身份策略结果配置为用于基于证书的身份验证方法但接收到的是基于密码的身份验证请求

适用对象	EAP-TLS 和 PEAP-TLS
可能原因	ISE 身份验证策略配置为用于基于密码的身份验证，但是请求方发送的是证书凭证。
解决方法	在 Policy > Authentication 中检查相应的配置。当身份源配置为用于基于证书的身份验证但接收到的是基于密码的身份验证请求时，会发生此错误。

22045 身份策略结果配置为用于基于密码的身份验证方法但接收到的是基于证书的身份验证请求

适用对象	EAP-FAST 和 PEAP-MSCHAPv2
可能原因	ISE 身份验证策略配置为用于基于证书的身份验证，但是请求方发送的是基于密码的凭证。
解决方法	在 Policy > Authentication 中检查相应的配置。当身份源配置为用于基于密码的身份验证但接收到的是基于证书的身份验证请求时，会发生此错误。

22056 在适用的身份库中未找到主题

适用对象	EAP-FAST、PEAP-MSCHAPv2、MAB
可能原因	在配置的身份库中找不到用户或设备
解决方法	检查主题是否存在于任何一个选定的身份库中。请注意，如果某些身份库不支持当前身份验证协议，则表明这些身份库可能已被略过。 确保身份验证策略指向正确的身份库。 对于在具有多个域的 Microsoft Windows 网络中的身份验证，请确保请求方附加了域后缀（对于用户：administrator@example.com，对于计算机：winxp.example.com）。

24408 对 Active Directory 的用户身份验证失败，因为用户输入的密码错误

适用对象	EAP-FAST 和 PEAP-MSCHAPv2
可能原因	用户输入的密码错误。
解决方法	检查用户密码凭证。如果 RADIUS 请求使用 PAP 进行身份验证，另请检查为网络设备配置的共享密钥。

15039 根据授权配置文件被拒

适用对象	所有 EAP 类型
可能原因	默认授权规则是拒绝访问，而针对此会话没有任何特定授权规则。
解决方法	由于授权规则匹配，因此选择了具有 ACCESS_REJECT 属性的授权配置文件。选中相应的授权策略规则结果。

22040 密码错误或无效的共享密钥

适用对象	基于密码的 EAP 类型
可能原因	在内部身份库中检查用户的密码。 共享 RADIUS 密钥在 ISE 和 NAD 之间不匹配。
解决方法	在 Administration > Network Resources > Network Devices 中检查用户凭证和设备共享密钥。

11036 消息身份验证器代码 RADIUS 属性无效

适用对象	所有 EAP 类型和 MAB
可能原因	共享 RADIUS 密钥在 ISE 和 NAD 之间不匹配。
解决方法	检查 AAA 客户端和 ISE 服务器上的共享密钥是否匹配。确保 AAA 客户端和网络设备没有硬件问题或 RADIUS 兼容性问题。此外，请确保用于将设备连接到 ISE 的网络没有硬件问题。

11007 无法找到网络设备或 AAA 客户端

适用对象	所有 EAP 类型和 MAB
可能原因	NAD 可能不在 ISE 上的网络设备列表中。
解决方法	在 Administration > Network Resources > Network Devices 中验证是否配置了网络设备或 AAA 客户端。

5417 动态授权失败

适用对象	所有 EAP 类型和 MAB
可能原因	未从 ISE PSN 使用授权变更 (CoA) 配置 NAD。
解决方法	检查 ISE 和 NAD 之间的连接。确保 ISE 定义为 NAD 上的动态授权客户端，并且在设备上支持 CoA。

附录 A：参考

Cisco TrustSec 系统：

http://www.cisco.com/go/trustsec

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

思科身份服务引擎用户指南：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

对于 Cisco Catalyst 2900 系列交换机：
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000 系列交换机：
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000-X 系列交换机：
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 4500 系列交换机：
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 6500 系列交换机：
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

对于 Cisco ASR 1000 系列路由器：
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于思科无线局域网控制器：
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html