排除ISE会话管理和状态故障

目录

预览

简介

背景信息

问题

- 最终用户体验
- ISE管理员体验
- 常见问题场景
- 陈旧/幻像会话问题
  - ISE会话管理逻辑
  - MNT和会话管理
  - PSN和会话管理
  - PSN上过时的会话
  - PSN上的虚拟会话
  - 陈旧会话和虚拟会话如何中断状态流程
- 新的身份验证尝试时发现进程不会启动
  - 在不同的PSN上重新进行身份验证
  - NAD在重新身份验证时生成新的会话ID
- 确定问题何时由陈旧/幻像会话引起的快速方法
- 陈旧/幻像会话高级故障排除
  - DART捆绑包
  - DART捆绑包分析
  - ISE日志调查
  - 调查ISE报告
- 如何确定问题何时由未重新启动发现导致
- 高级故障排除：没有发现重新启动

解决方案

- 传统方法 — 问题避免
  - 可以最大限度地减少ISE部署中陈旧或幻像会话数量的最佳实践
  - Posture Over VPN使用案例
  - 可以实施最佳实践，以最大程度降低不重新启动ISE终端安全评估模块的影响
  - 重新身份验证实施
  - 具有负载均衡器的环境
- 现代方法 — 状态共享
  - 轻量级数据分布架构
  - 通过RSD共享终端安全评估状态
  - 通过RSD共享终端安全评估状态 — 陈旧/幻像会话
  - RSD上的状态共享 — PSN之间的故障转移

简介

本文档介绍常见的身份服务引擎(ISE)终端安全评估服务问题，例如“AnyConnect ISE终端安全评估模块显示兼容……”

背景信息

本文档介绍常见身份服务引擎(ISE)终端安全评估服务问题：“AnyConnect ISE终端安全评估模块在ISE上的会话状态为挂起时显示合规性。”

虽然症状始终相同，但此问题的根源有多种。通常，对此类问题进行故障排除会非常耗时，会导致严重的影响。

本文档解释以下内容：

- 常见的问题场景。
- 快速问题识别算法。
- 常见问题情景的经典解决方案。
- 通过Radius会话目录共享终端安全评估状态。
- 从最终用户和ISE管理员角度来看问题表现。
- ISE、AnyConnect和网络操作背后的理论引发问题。

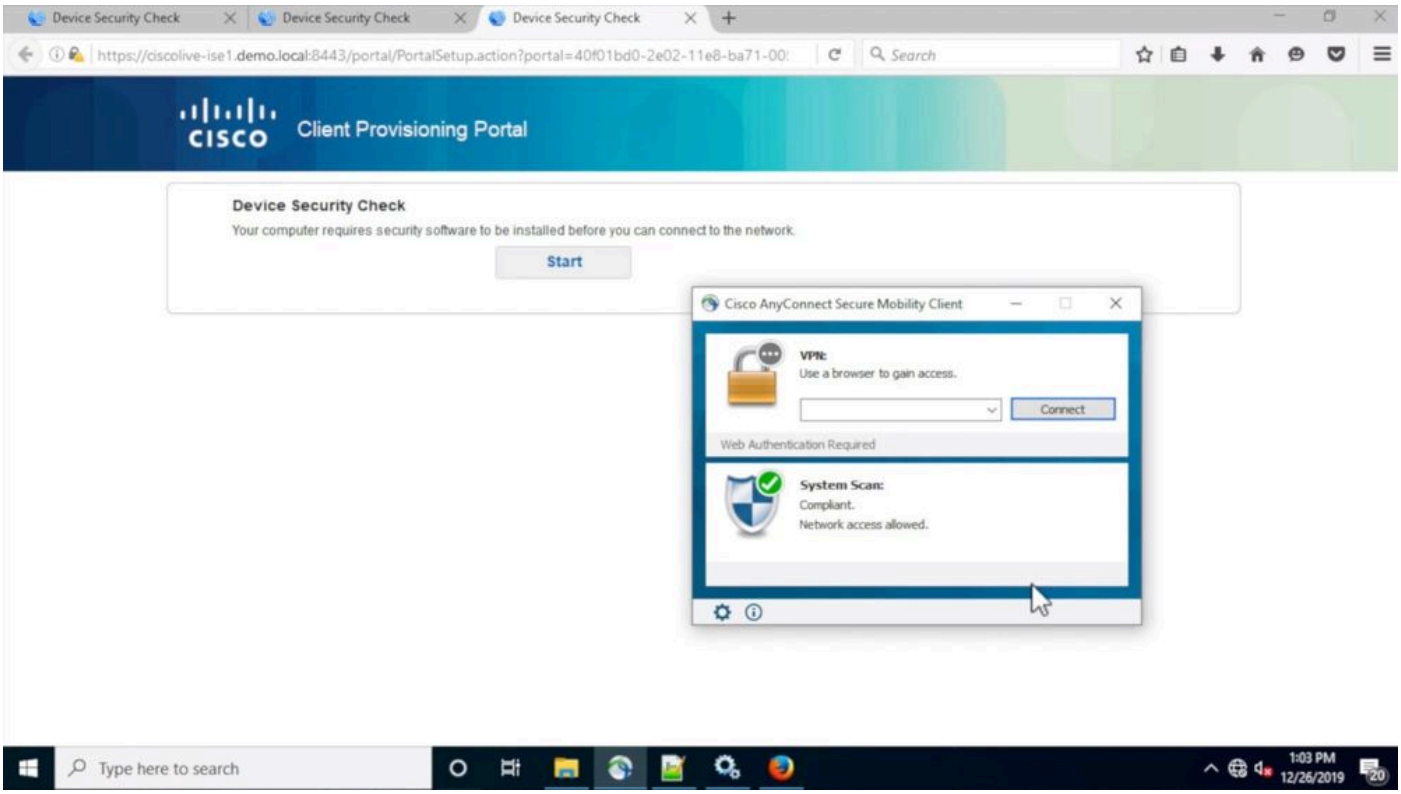
有关后面介绍的概念的更好解释，请参阅ISE终端安全评估样式比较（针对高级版和高级版2.2）

问题

最终用户体验

此问题通常表现为浏览器中缺少网络访问或持续重定向到ISE客户端调配门户，同时AnyConnect ISE终端安全评估模块将终端安全评估状态显示为Compliant。

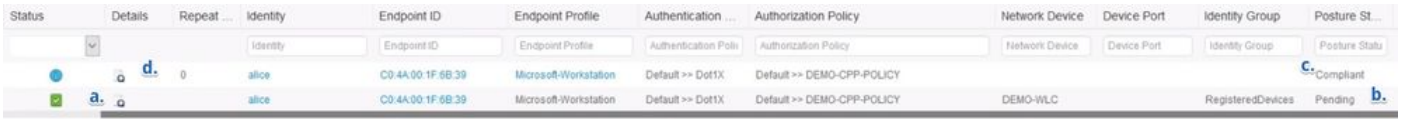
典型的最终用户体验：



ISE管理员体验

最初对此问题进行分类时，ISE管理员开始调查Radius Live日志以确保身份验证命中ISE。在此阶段发现的第一个症状表示实时日志中终端和ISE之间的状态不匹配。或者，Radius身份验证报告终端上次成功身份验证显示Pending状态状态。

典型的ISE管理员体验：



- 上次身份身份验证成功：爱丽丝。
- 会话的状态是Pending。
- 身份的最后会话事件：爱丽丝。
- 会话事件将状态显示为Compliant。

注意：在本例中，当所述问题出现时，C和D并不总是出现在实时日志中。状态状态为Compliant的会话事件更常见于由陈旧或幻像会话引起的场景（本文档后面部分将进行介绍

)。

常见问题场景

此问题通常表现在两个有问题的场景中，并且每个场景都有多个根本原因。场景：

- AnyConnect ISE终端安全评估模块在终端安全评估过程中被策略服务节点(PSN)错误通知，导致显示错误的终端安全评估状态。在这种情况下，TAC通常与PSN会话缓存中的陈旧或幻像会话配合工作。
- AnyConnect ISE显示上一个发现周期的安全评估状态，因为当前身份验证未触发发现进程。

AnyConnect中的ISE终端安全评估模块具有触发发现进程的有限数量的事件。在身份验证或重新身份验证期间，可能未检测到这些事件。

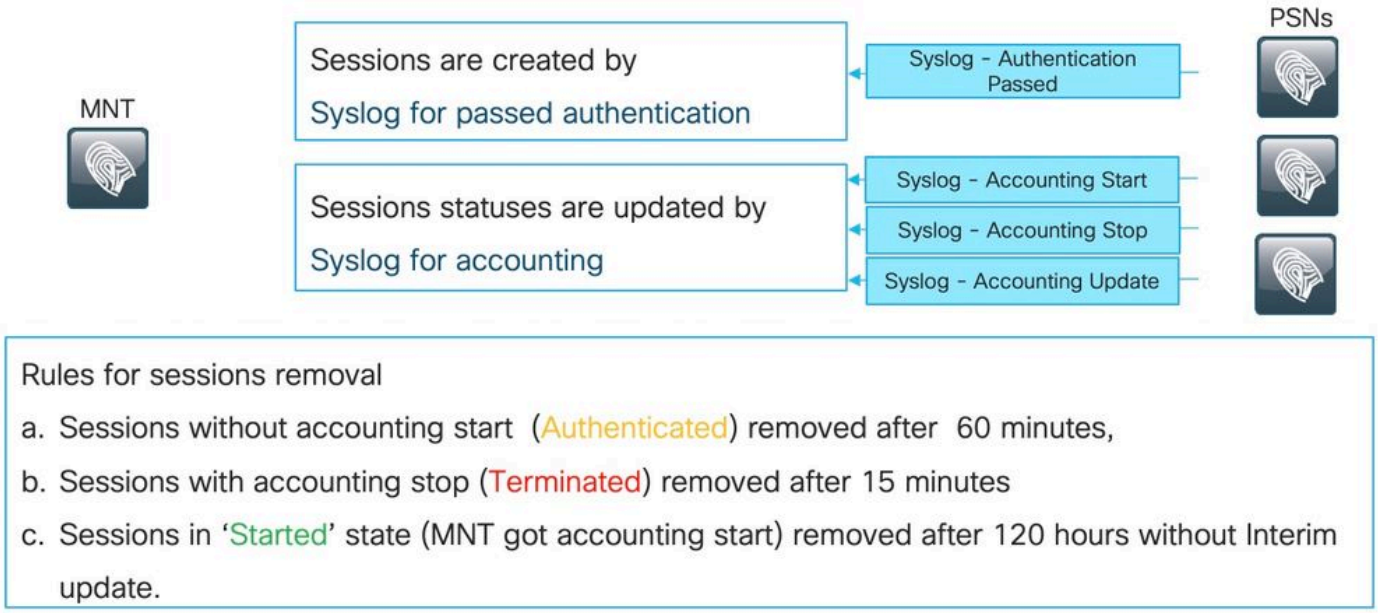
陈旧/幻像会话问题

为了更好地了解问题，请调查所需的ISE会话管理逻辑和AnyConnect发现流程。

ISE会话管理逻辑

在ISE部署中，有两个人员负责会话管理流程：PSN和监控节点(MNT)。 要正确排除故障并确定问题，必须了解两个角色上的会话管理理论。

MNT和会话管理



如本图所述，MNT节点根据来自PSN的已通过的身份验证系统日志消息创建季节。会话状态稍后可由系统日志更新，以便记帐。

MNT上的会话删除在以下三种情况下发生：

1.没有记账开始的会话在创建后约60分钟删除。每5分钟执行一个cron作业以检查会话状态和清除状态。

2.在同一cron作业处理记账停止后约15分钟内终止的会话被删除。

3.每次执行时相同的cron会删除超过5天（120小时）处于“已启动”状态的会话。“已启动”状态表示MNT节点已处理身份验证和记帐以启动Syslog会话。

注意：这些是正常的MnT清除计时器，不保证墙时钟删除时间。如果出现以下情况，则删除可能会延迟：

- SessionPurgeJob未成功运行。
- MnT面临资源或数据库压力。
- 记账停止不能与现有会话相关联。

来自PSN的系统日志消息示例：

当在DEBUG中启用runtime-aaa组件时，消息将记录到prrt-server.log中。可以使用粗体部分构建搜索正则表达式。

通过身份验证：

<#root>

AcsLogs

,

2020-04-07 10:07:29,202

,DEBUG,0x7fa0ada91700,cntx=0000629480,sesn=skuchere-ise26-1/375283310/10872,CPMSessionID=0A3E946C000000

5200 NOTICE Passed-Authentication: Authentication succeeded

, ConfigVersionId=87, Device IP Address=10.62.148.108, DestinationIPAddress=192.168.43.26, DestinationP

bob@example.com

, NAS-IP-Address=10.62.148.108, NAS-Port=50105, Service-Type=Framed, Framed-IP-Address=192.168.255.205,

0A3E946C00000073559C0123

\;42SessionID=skuchere-ise26-1/375283310/10872\;, Calling-Station-ID=

00-50-56-B6-0B-C6

, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/5, EAP-Key-Name=, cisco-av-pair=service-type=F

记帐开始：

<#root>

AcsLogs

,

2020-04-07 10:07:30,202

,DEBUG,0x7fa0ad68d700,cntx=0000561096,sesn=skuchere-ise26-1/375283310/10211,CPMSessionID=0A3E946C000000

3000 NOTICE Radius-Accounting: RADIUS Accounting start request

, ConfigVersionId=87, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=7, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.10

0A3E946C00000073559C0123

:skuchere-ise26-1/375283310/10210, Called-Station-ID=00-E1-6D-D1-4F-05, Calling-Station-ID=

00-50-56-B6-0B-C6

, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000041, Acct-Authentic=Remote, Event-Tim

---

中期会计更新：

<#root>

AcsLogs,2020-04-07 22:57:48,642,

DEBUG,0x7fa0adb92700,cntx=0000629843,sesn=skuchere-ise26-1/375283310/10877,CPMSessionID=0A3E946C0000007

3002 NOTICE Radius-Accounting: RADIUS Accounting watchdog update

, ConfigVersionId=87, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=8, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.10

00-50-56-B6-0B-C6

, Acct-Status-Type=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=2293926, Acct-Output-Octets=0, A

0A3E946C00000073559C0123

, cisco-av-pair=method=dot1x, AcsSessionID=skuchere-ise26-1/375283310/10877, SelectedAccessService=Defa

---

记帐停止：

<#root>

AcsLogs,2020-04-08 11:43:22,356

,DEBUG,0x7fa0ad68d700,cntx=0000696242,sesn=skuchere-ise26-1/375283310/11515,CPMSessionID=0A3E946C000000

3001 NOTICE Radius-Accounting: RADIUS Accounting stop request

, ConfigVersionId=88, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=12, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.1

00-50-56-B6-0B-C6

, Acct-Status-Type=Stop, Acct-Delay-Time=0, Acct-Input-Octets=4147916, Acct-Output-Octets=0, Acct-Sessi

0A3E946C00000073559C0123

, cisco-av-pair=method=dot1x, AcsSessionID=skuchere-ise26-1/375283310/11515, SelectedAccessService=Defa

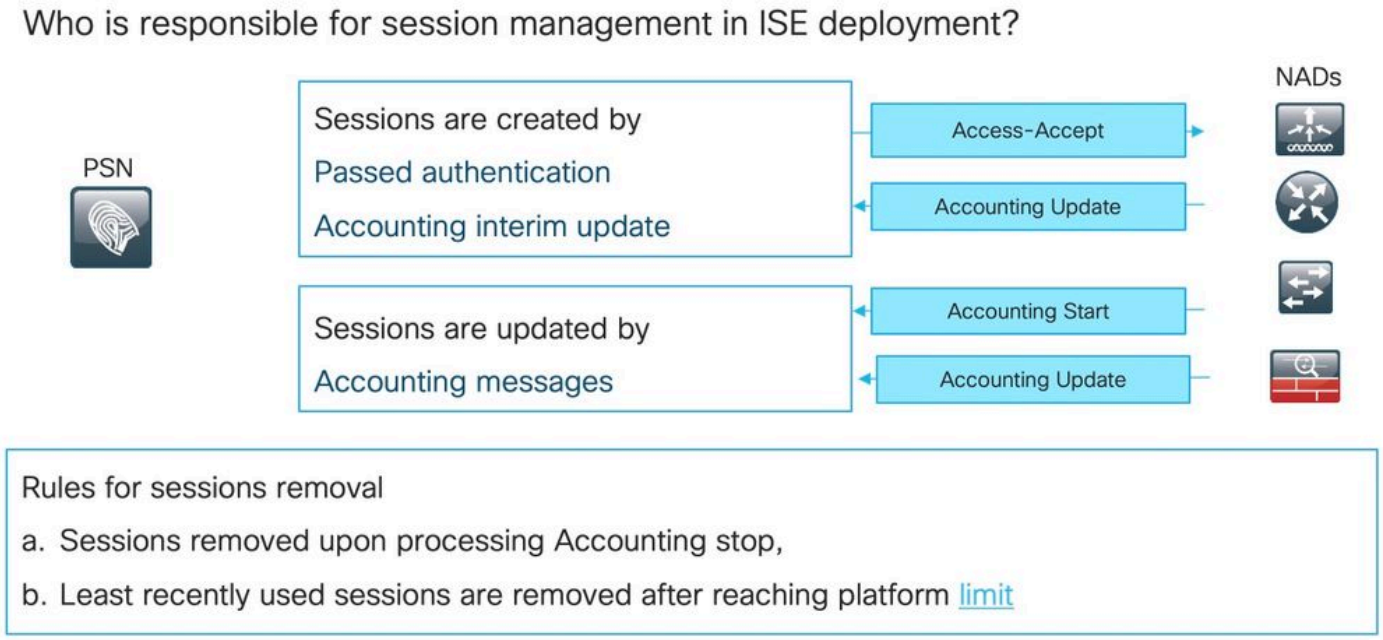
---

PSN和会话管理

PSN会话缓存是一个内存数据库，用于存储特定PSN的所有活动会话。会话缓存始终位于节点本地。在ISE中没有可以执行从一个节点到另一个节点的完整会话状态复制的机制。

对于每个活动会话ID，PSN存储身份验证/授权阶段收集的所有属性(例如，内部/外部用户组、网络接入设备(NAD)属性、证书属性等)。 PSN使用这些属性来选择不同的策略类型，例如身份验证、授权、客户端调配和状态。

重新启动节点（或节点上的服务）后，会话缓存将被完全删除。



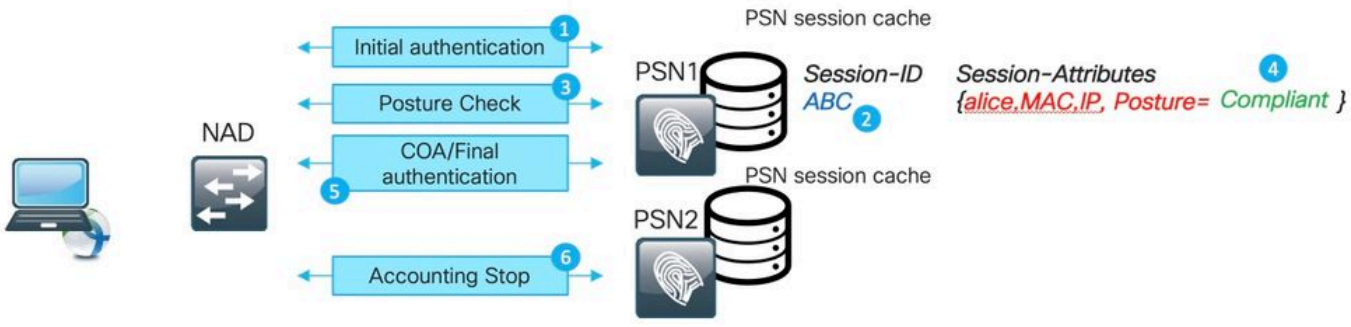
当前会话处理逻辑在两个场景中在会话缓存中创建一个新条目。现有会话的后续详细信息可以通过来自NAD的记帐消息进行更新。

- 会话已在PSN上成功通过身份验证。
- PSN具有会话缓存中不存在会话的记帐临时更新。通过会话删除，PSN将实现以下逻辑：
  - 处理记帐停止消息后，会立即删除会话缓存条目。
  - 当节点达到活动会话的限制时，PSN开始删除最近最少使用的会话。

PSN上过时的会话

在ISE部署中，未执行实际身份验证的PSN已处理现有会话的记帐停止：

过时的会话示例：



---

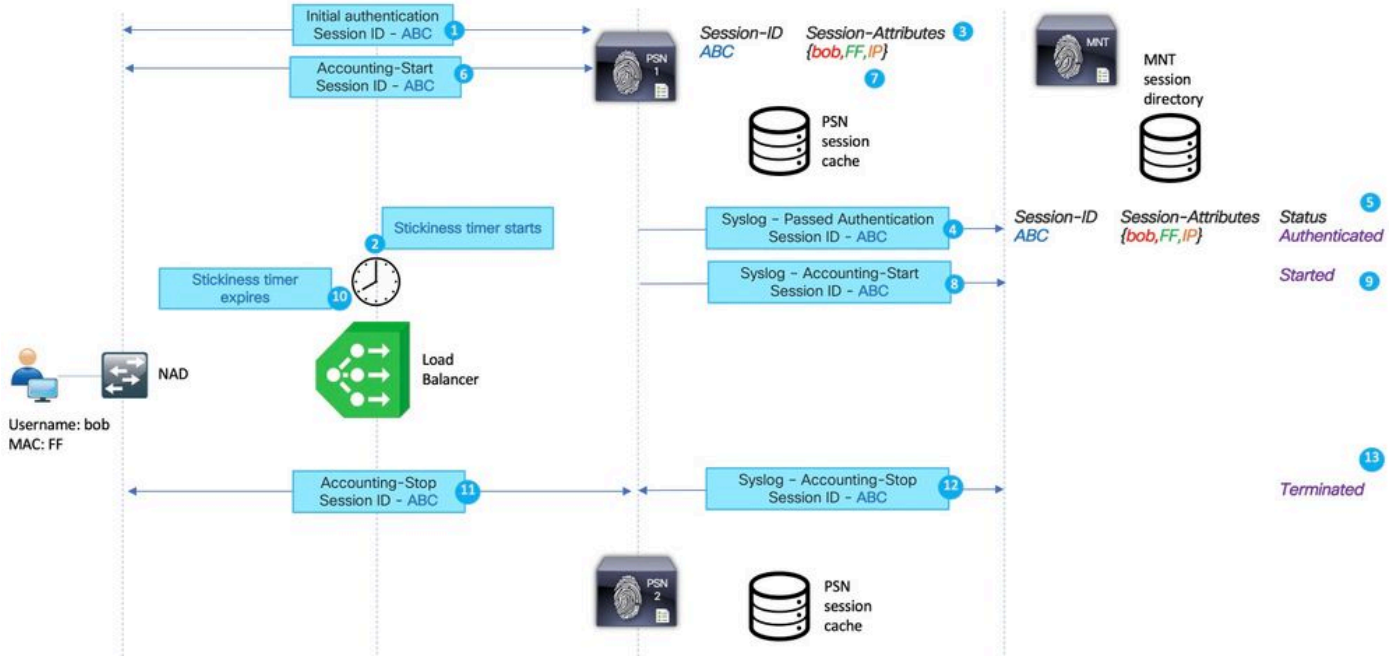
1. 在PSN上为会话ABC成功进行身份验证。
2. PSN在会话缓存中创建条目。
3. 进行状态评估。
4. 会话标记为Compliant。
5. 授权更改(COA)由状态更改触发，导致终端重新身份验证以应用下一个访问级别。
6. 会话ABC到PSN2的记帐停止。

之后，ABC在PSN1上陷入陈旧状态，因为此PSN上未处理记帐停止消息以将其删除。如果部署未遇到大量身份验证尝试，则会删除会话。

在以下情况下，过时的会话显示在PSN会话缓存中：

- 由于负载均衡器上的粘性计时器过期，记帐停止被发送到错误的PSN。
- NAD上的错误配置与为身份验证和记帐配置的PSN不同。
- 网络路径上的临时连接问题导致了NAD故障切换到下一个PSN。

负载均衡器(LB)环境中过时的会话示例：



---

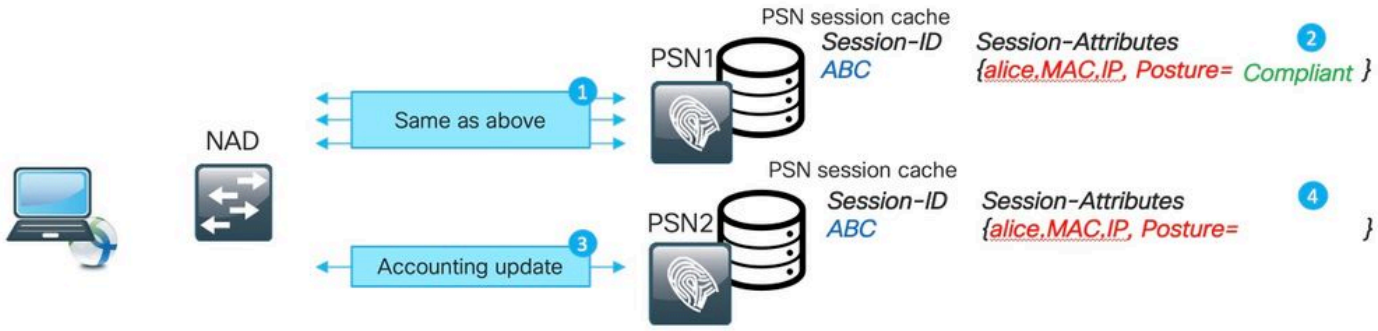
1. 会话ABC的初始身份验证由PSN1执行。此身份验证在负载均衡器上启动粘性计时器。
2. PSN1在本地缓存中为会话ABC创建一个条目。
3. 已传递身份验证的系统日志消息将传输到MNT节点。
4. 会话ABC的条目会创建到MNT会话目录中，并且处于Authenticated状态。

5. 会话ABC的记帐开始消息到达PSN1。
6. 会话ABC的会话缓存条目会使用Accounting-Start中的信息更新。
7. Accounting-Start的系统日志消息被传输到MNT节点。
8. 会话状态更新为Started。
9. 负载均衡器上的粘性计时器过期。
10. 负载平衡器将会话ABC的记帐停止转发到PSN2。
11. Accounting-Stop的Syslog消息由PSN2转发到MNT。
12. 会话ABC在MNT上标记为terminated。

PSN上的虚拟会话

幻像会话是会计临时更新到达PSN且未对该会话执行身份验证的场景。在这种情况下，将在PSN会话缓存中创建一个新条目。如果PSN没有收到此会话的记帐停止消息，则不会删除该条目，除非PSN达到活动会话的限制。

幻像会话示例：



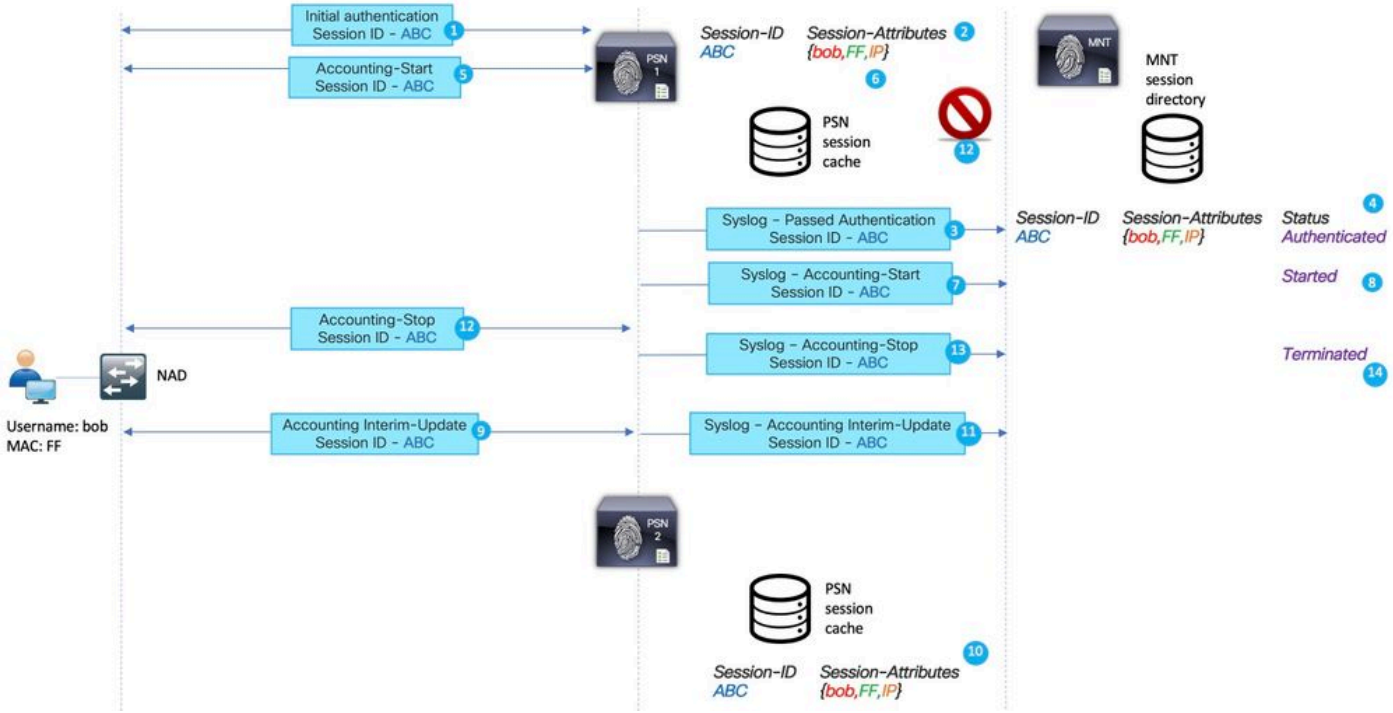
---

1. 在PSN1上为ABC会话执行与旧会话示例中所述的步骤相同的步骤。
2. 会话ABC在PSN1会话缓存中的状态为Compliant。
3. 会话ABC的记帐临时更新到达PSN2。
4. ABC的会话条目在PSN2上创建。由于会话条目是根据记帐消息创建的，因此其属性数量有限。例如，状态状态对于会话ABC不可用，并且用户组或其他授权特定属性也不存在。

在以下情况下，虚拟会话显示在PSN会话缓存中：

- 网络传输中的短期中断。
- 网络接入设备的不当行为。
- 负载均衡器上的错误行为或配置错误。

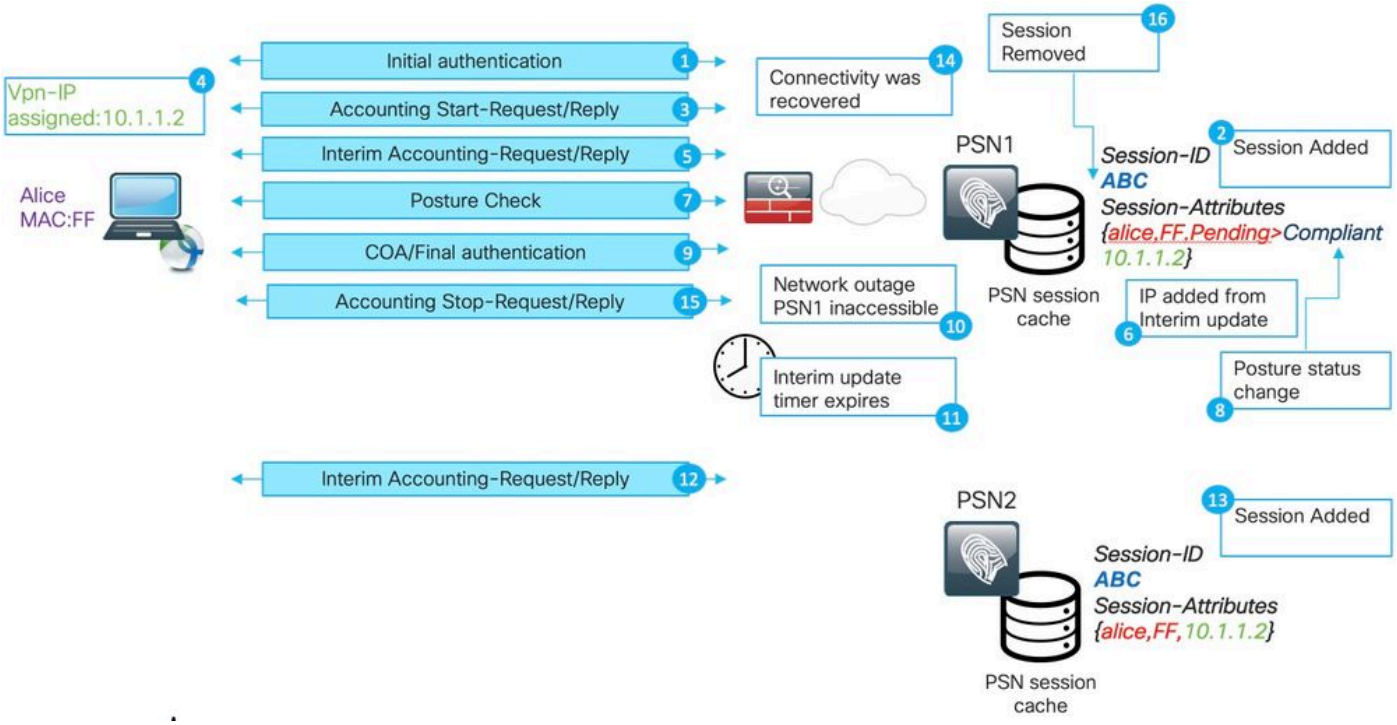
下一个屏幕截图是幻像会话示例，其中指向PSN1的网络路径上出现临时问题：



---

1. 会话ABC的初始身份验证由PSN执行。
2. PSN1在本地缓存中为会话ABC创建一个条目。
3. 已通过身份验证的系统日志消息将传输到MNT节点。
4. 在TimesTen DB中创建会话ABC的条目，其状态为Authenticated。
5. 会话ABC的记帐开始消息位于PSN 1上。
6. 使用来自Accounting-Start的信息更新会话ABC的会话缓存条目。
7. Accounting-Start的系统日志消息被传输到MNT节点。
8. 会话状态更新为Started。
9. 会话ABC的临时记帐更新被转发到PSN2。
10. PSN2在本地缓存中为会话ABC创建一个条目。
11. 会话ABC的Accounting-Stop被转发到PSN1。
12. 会话ABC的条目将从PSN1上的会话缓存中删除。
13. Accounting-Stop的Syslog消息由PSN1转发到MNT。
14. 会话ABC在MNT上标记为已终止。

这描述了为长寿VPN连接创建的虚拟会话场景：



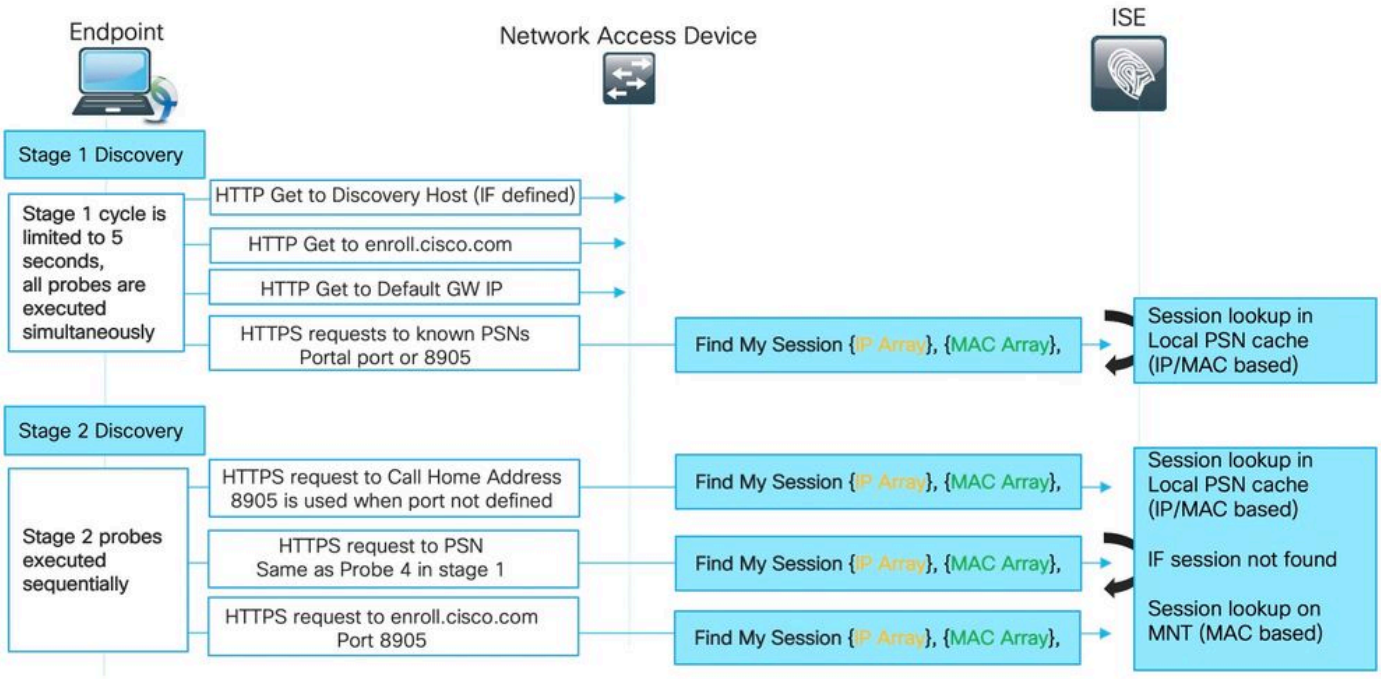
---

1. PSN1上的初始身份验证。
2. 会话ABC在会话缓存中创建。
3. 记帐会启动PSN处理的消息。
4. 新的IP地址分配给虚拟专用网络(VPN)适配器。
5. 具有IP地址信息的临时记帐更新位于PSN上。
6. IP地址信息会添加到会话缓存中。
7. PSN1进行状态评估。
8. 状态会在会话中更新。
9. ISE执行COA推送；这会触发要分配的新访问级别。
10. 网络路径发生中断，导致PSN1无法访问。
11. 在临时更新间隔到期后，ASA/FTD检测到PSN1不可访问。
12. 临时记帐更新到达PSN2。
13. 虚拟会话在PSN2会话缓存中创建。

如果PSN1稍后变为可访问(14)，则转发所有后续的记帐消息(15,16)，这会在PSN2会话缓存中保留会话ABC一段未定义的时间。

陈旧会话和虚拟会话如何中断状态流程

要了解陈旧和虚拟会话如何中断安全评估，您可以查看AnyConnect ISE安全评估模块发现流程：



第1阶段发现：

在此阶段，ISE终端安全评估模块执行四个同时探测以定位对终端进行身份验证的PSN。

首先，图中的三个探测是基于重定向的(默认GW IP、发现主机IP（如果已定义）和enroll.cisco.com IP);当重定向的URL取自NAD本身时，这些探测功能始终将代理指向正确的PSN。

探测4将发送到ConnectionData.xml文件中显示的所有主服务器。此文件在第一次成功的安全评估尝试后创建。如果客户端在PSN之间迁移，则可以稍后更新文件内容。

在Windows系统上，文件位置为C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\。

由于所有阶段1探测同时执行，因此仅当所有其他三个探测都失败或ISE终端安全评估模块在5秒内无法与重定向URL中返回的PSN建立正确通信时，才使用探测4的结果。

当probe four位于PSN上时，它包含在终端上发现的活动IP和MAC地址列表。PSN使用此数据在本地缓存中查找此终端的会话。如果PSN的终端存在陈旧或幻像会话，则可能导致客户端稍后显示错误的终端安全评估状态。

当代理收到探测四的多个应答时（ConnectionData.xml可以包含多个主PSN），始终使用最快的应答。

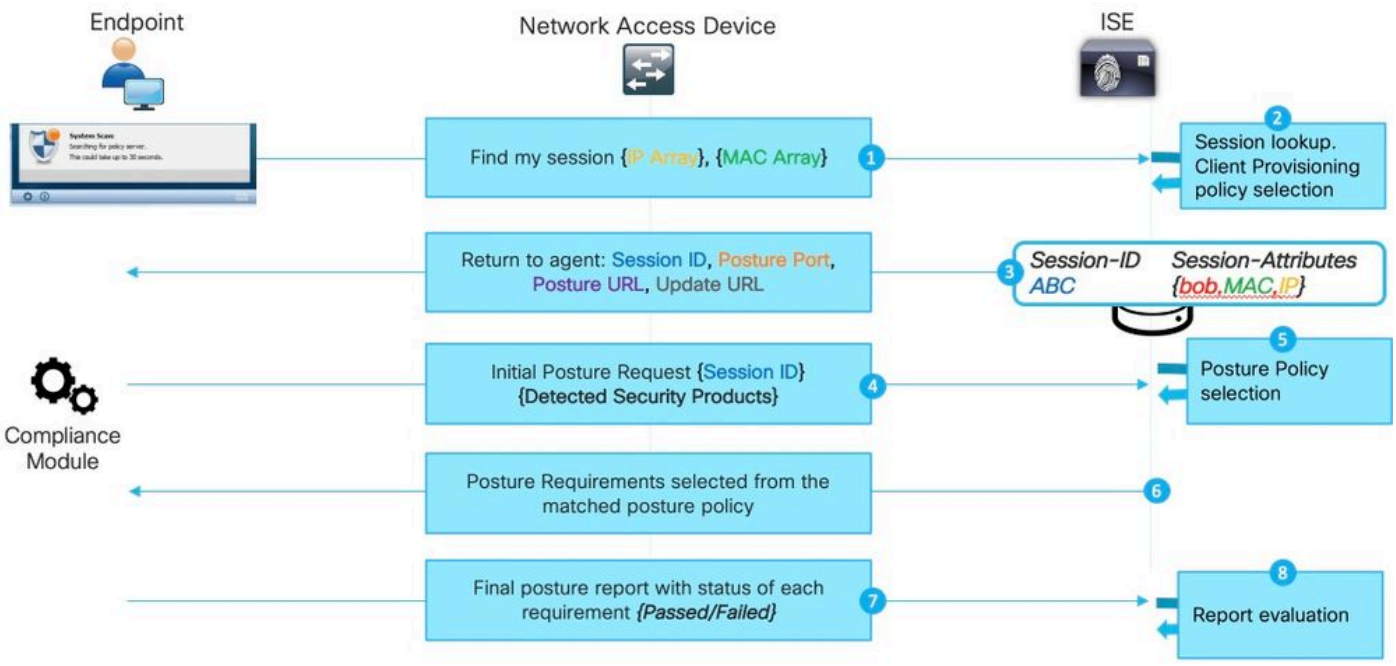
第2阶段发现：

所有第2阶段发现探测都是无重定向的，这意味着每个探测都会触发目标PSN上的会话查找。如果PSN无法在本地会话缓存中找到会话，则必须执行MNT查找（仅基于MAC地址）以查找会话所有者并将所有者名称返回给代理。

由于所有探测都会触发会话查找，第2阶段发现可能会受到因陈旧或幻像会话导致的问题严重影响。

如果PSN移至第2阶段，会话缓存中存在的发现探测将为同一终端创建一个陈旧或幻像条目。这会导致向最终用户返回错误的终端安全评估状态。

此示例显示当PSN保持陈旧会话或幻像会话时状态如何显示：



注意：仅当所有基于重定向的发现探测失败或实施非重定向状态时，才会出现此问题。

---

1. ISE终端安全评估模块发出的任何Find my session probe。
2. PSN在会话缓存中执行会话查找。如果要找到会话，则会出现过时的会话或幻像会话问题。
3. PSN运行客户端调配策略选择。如果虚拟会话缺少身份验证/授权属性，并且您配置的所有策略都是特定的（例如，为特定Active Directory组创建策略），则PSN无法分配正确的客户端调配策略。这可在错误消息中显示：“绕过AnyConnect扫描您的网络未配置为使用思科NAC代理”。

- 如果客户端调配策略是通用的（幻像会话中可用的属性足以将策略与AnyConnect配置相匹配），PSN将回复继续评估过程所需的详细信息。
- 在此步骤中，当处理过时的会话时，PSN立即回复安全评估状态Compliant，并且未完成所有后续步骤。PSN不会发送COA，因为它认为会话已经合规。在Radius Live日志中，没有显示状态为Compliant的会话事件。

4.对于虚拟会话场景，ISE终端安全评估模块继续初始终端安全评估请求。此请求包含有关在终端上检测到的所有安全和补丁管理产品的信息。

---

5. PSN使用来自请求和会话属性的信息来匹配正确的终端安全评估策略。此时，幻像会话缺少属性，并且没有要匹配的策略。在这种情况下，PSN会应答其合规的终端。如果安全评估策略不匹配，这是默认ISE行为。

注意：当存在可从虚拟会话属性中选择的通用策略时，您可以继续执行步骤6。

---

6. PSN将所选安全评估策略返回给代理。

注意：当无法选择任何策略时，PSN返回Compliant状态。

7.代理会将每个策略/需求的状态返回为“通过”或“失败”。

8.报告评估在ISE上进行，会话状态更改为Compliant。

注意：如果终端安全评估问题是由虚拟会话引起的，ISE管理员可以注意到一些故障终端安全评估COA。如果是，则从错误的PSN和错误的会话ID执行COA请求。

新的身份验证尝试时发现进程不会启动

ISE终端安全评估模块用于监控终端上有限数量的事件以触发发现进程。

触发发现的事件：

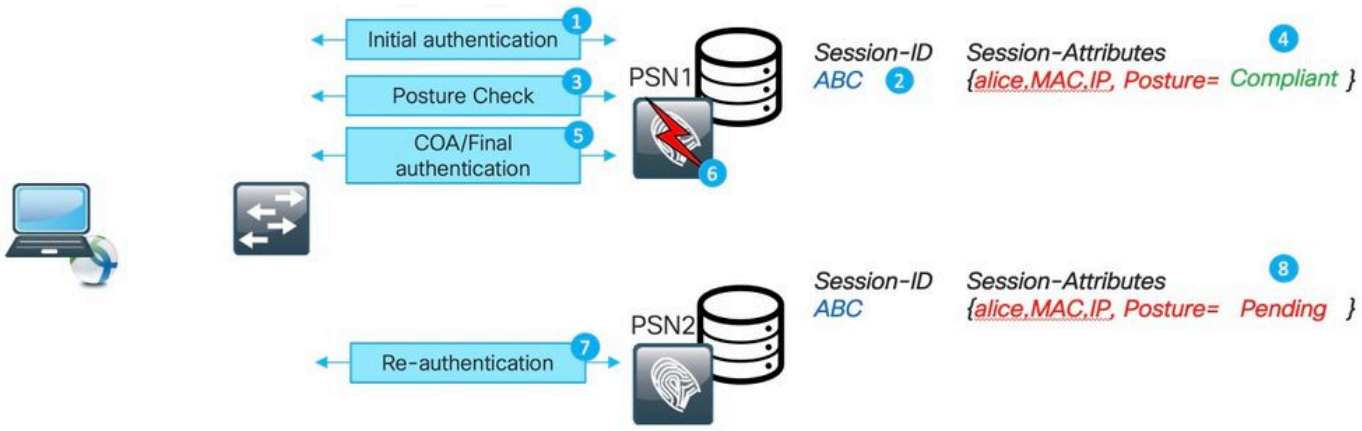
- 初始ISE终端安全评估模块安装。
- 用户登录。
- 电源事件。
- 接口状态更改。
- 操作系统在睡眠后恢复。
- 默认网关(DG)更改。
- 状况重新评估(PRA)故障，请参阅Cisco bug ID CSCvo69557。ISE状况模块未检测到新的dot1x身份验证、PC解锁和IP地址更改。

在以下情况下，ISE终端安全评估模块无法检测新的身份验证或重新身份验证尝试：

- 重新身份验证命中不同的PSN（可能是由于LB决策或原始PSN的问题）。
- NAD在重新身份验证时生成新的会话ID。

在不同的PSN上重新进行身份验证

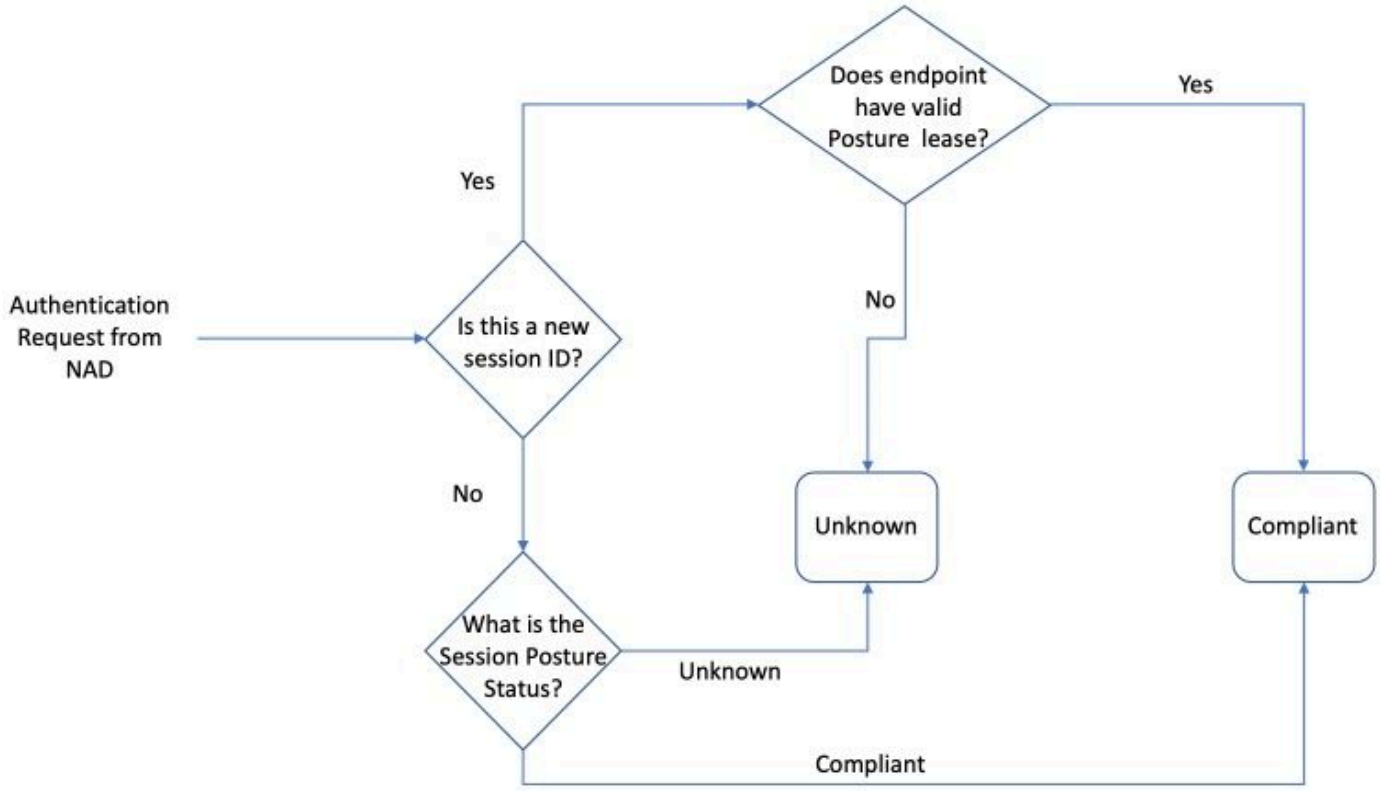
下图描绘了由原始PSN中断导致的不同PSN上的重新身份验证示例。具有负载均衡器的场景看起来类似。在负载均衡器的情况下，由于粘性计时器过期，重新身份验证被定向到不同的PSN。



---

1. PSN1上的初始身份验证。
2. 会话ABC在PSN1会话缓存中创建。
3. 使用PSN1执行状态评估。
4. 会话ABC安全评估状态变为Compliant。
5. COA由状况状态更改触发，导致终端重新身份验证以应用下一个访问级别。
6. PSN1变为不可用。
7. 会话ABC的重新身份验证命中PSN2。
8. 由于这是PSN2的新会话，会话的状态更改为Pending。

初始状态由PSN分配给会话：



注意：State-machine仅描述状态状态的初始选择。根据从ISE终端安全评估模块收到的报告评估，每个会话最初被标记为“未知”(Unknown)，之后会变为“合规”(Compliant)或“不合规”(Non-Compliant)。

NAD在重新身份验证时生成新的会话ID

这可以在两种最常见的情形下发生：

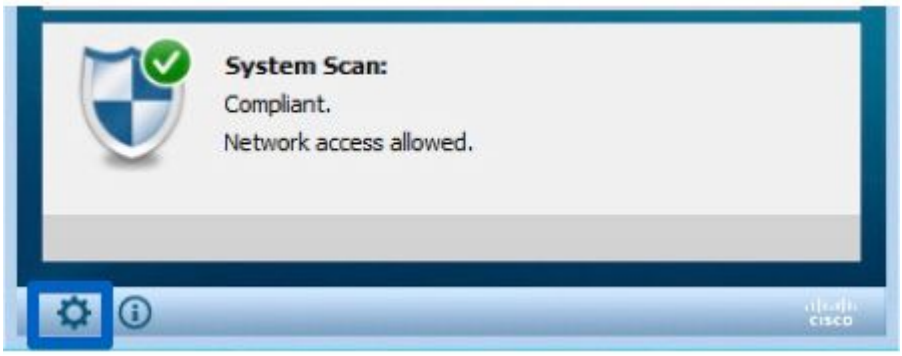
- 在ISE端重新身份验证配置不正确（此问题的解决方案将在本文档后面介绍。）
- NAD方面的不当行为；通常，在重新身份验证尝试期间，NAD会保留相同的会话ID。这是一个可能出现的有漏洞的行为，必须在NAD上进行调查。
  - 新的会话ID可以在某些其他场景中生成。例如，在某些情况下，无线漫游可能是一个原因。
  - ISE PSN始终将新会话置于posture Pending状态，除非配置了终端安全评估租用。安全评估租赁将在本文档后面部分进行说明。

确定问题何时由陈旧/幻像会话引起的快速方法

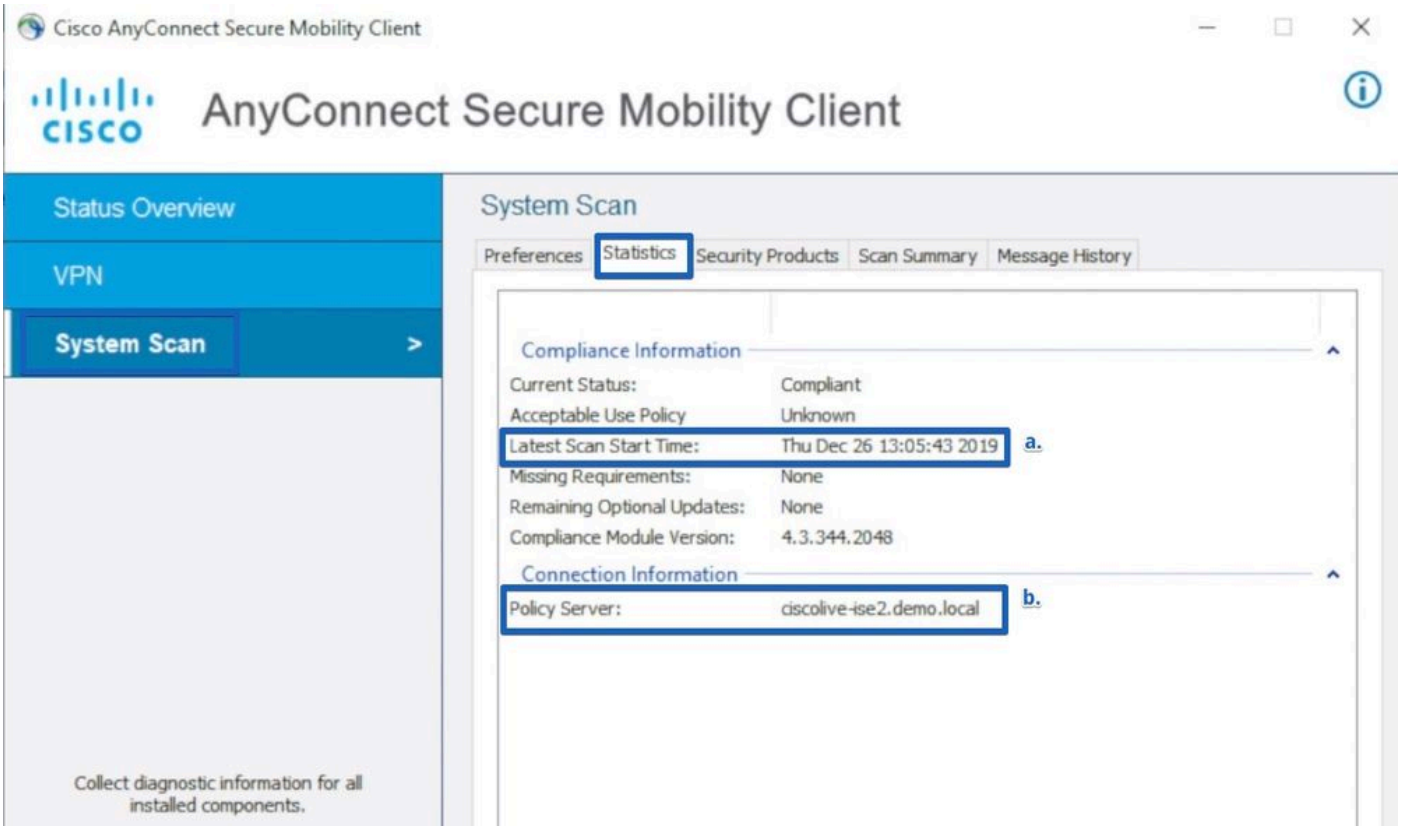
确定AnyConnect在重定向状态时是否显示合规性是由过期/幻像会话引起的。当终端处于有问题的状态时，您必须获取对终端的访问权限。

调查系统扫描详细信息

1.单击AnyConnect UI中的齿轮图标。



2.在新窗口中，定位至“系统扫描”>“统计信息”。

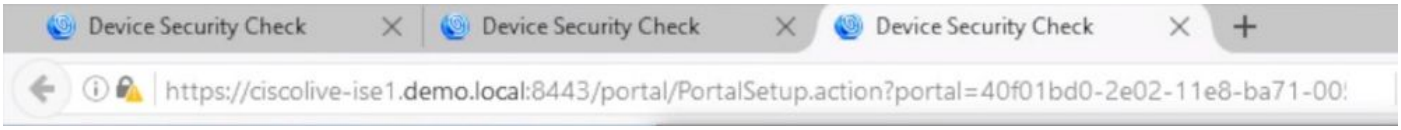


接下来，请注意两个重要因素：

- 最新扫描开始时间：此处的时间戳必须接近发现问题的时间。
- 策略服务器:此字段指示对终端执行状态评估的策略服务器的名称。必须将FQDN与来自重定向URL的FQDN（用于重定向基本状态）或来自上次身份验证尝试的PSN名称（用于无重定向状态）进行比较。

---

1. 将系统扫描统计信息中的策略服务器FQDN与对终端进行身份验证的节点名称进行比较：



此演示显示了问题识别所需步骤的记录：

陈旧/幻像会话高级故障排除

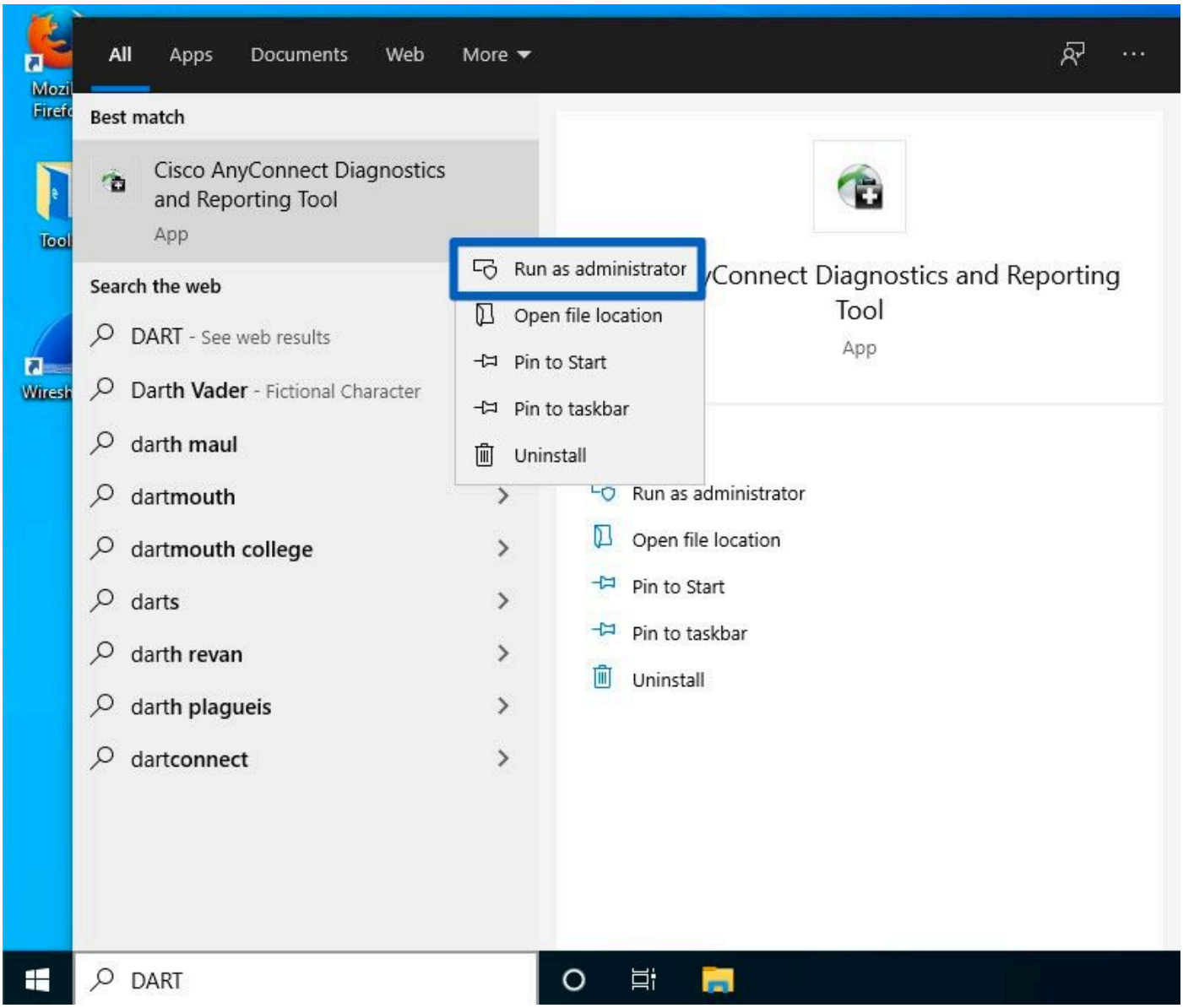
上一个示例将陈旧或幻像会话问题与未启动的发现进程问题区分开来。同时，您必须确定触发问题的实际会话，了解它如何变成陈旧或幻像会话问题。虽然在某些情况下无法避免陈旧和幻像会话，但必须确保实施最佳实践，以防止在环境中创建陈旧/幻像会话。

DART捆绑包

分析从重现问题的终端获取的DART捆绑包。

---

1. 仅在DART中保留重要日志，建议在重现问题之前清除日志。
2. 为此，DART捆绑工具必须以管理员身份启动并执行日志清除。
3. 在Windows上，导航到“开始”并开始键入DART >右键单击，然后选择 — 以管理员身份运行。



4.在第一个向导屏幕上，单击下一步。



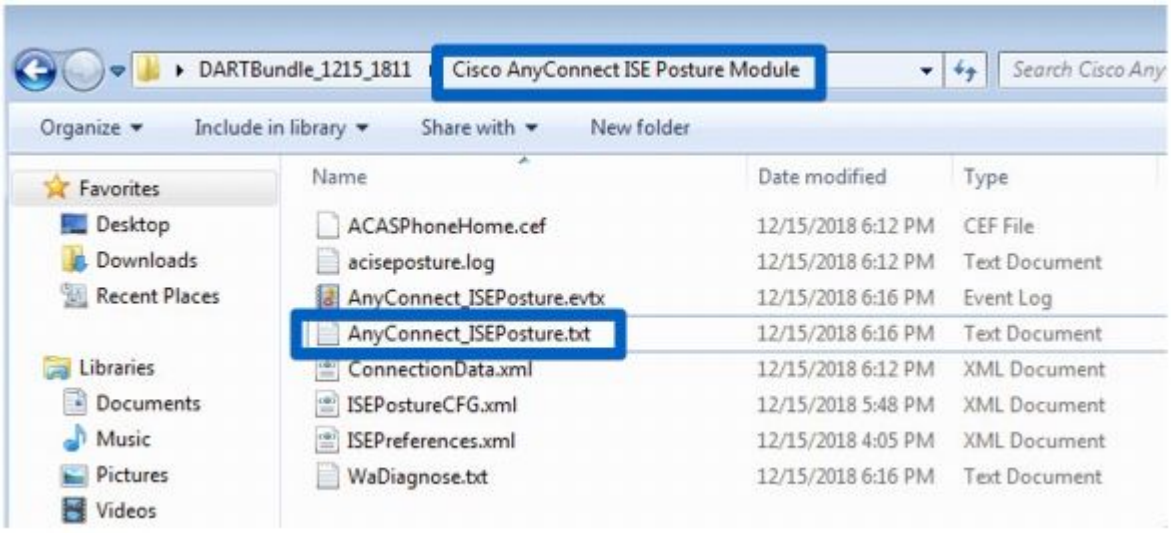
5.在下一个向导屏幕上，单击Clear All Logs。



6.重现问题后，可以从此处收集DART；单击下一步。

DART捆绑包分析

收集DART捆绑包后，将其取消存档，并重点关注Cisco AnyConnect ISE终端安全评估模块文件夹中的AnyConnect_ISEPosture.txt文件。此文件包含所有发现相关事件。



1.开始故障排除并确定发现重启的所有时刻。要搜索的关键字是Restarting Discovery或HTTP Discovery。导航到在问题时刻发生发现重启的行：

```
Line 3575: 2018/12/15 17:48:08                    1251 Level: info  Restarting Discovery.
Line 3840: 2018/12/15 17:48:59                    1251 Level: info  Restarting Discovery.
Line 3991: 2018/12/15 17:50:24                    1251 Level: info  Restarting Discovery.
Line 4214: 2018/12/15 18:00:54   <output          1251 Level: info  Restarting Discovery.
Line 4308: 2018/12/15 18:01:14   omitted>         1251 Level: info  Restarting Discovery.
Line 4530: 2018/12/15 18:11:45                    1251 Level: info  Restarting Discovery.
Line 4642: 2018/12/15 18:12:01                    1251 Level: info  Restarting Discovery.
```

2.在发现重新启动后的几行中，有一行包含Probing no MNT stage targets（这是第1阶段发现启动的指示符）：

```
SwiftHttpRunner::collectNoMntTargets Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libswift\Swi
ftHttpRunner.cpp Line: 1157 Level: debug  Probing no MNT stage targets (#5):
Redirection target 192.168.255.1, Redirection target enroll.cisco.com,
Auth-Status target ciscolive-ise2.demo.local with path /auth/status,
Auth-Status target ciscolive-ise1.demo.local with path /auth/status,
```

3.建议以不同颜色突出显示从ConnectionData.xml（身份验证状态目标）获取的所有具有相同颜色且先前已连接PSN的基于重定向的探测器。通常，PSN FQDN是相似的，并且可能难以发现差异。

4.阅读日志文件以查看每个探测的结果（这是失败探测的显示示例）：

```
2018/12/15 18:12:01 [Information] aciseagent Function: Target::Probe Thread Id: 0x1130
File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libnaccommon\Target.
cpp Line: 200 Level: debug Status of Redirection target enroll.cisco.com is 6 <Not
Reachable.>.
```

5.在发现重新启动第1阶段或第2阶段后，您会在文件中的某个位置看到一个来自一个或多个PSN的成功回复：

```
Target::fetchPostureStatus Thread Id: 0xBF0 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libnaccommon
\Target.cpp Line: 401 Level: debug  POST request to URL (
https://ciscolive-ise2.demo.local:8443/auth/ng-discovery), returned status 0
<Operation Success.>.
```

5.后面几行中，有一行带有关键字MSG_NS_SWISS_NEW_SESSION。此行包含实际会话ID，PSN在会话查找后选择了它。使用此会话ID进一步调查ISE，以确定会话如何变成陈旧/幻像：

```
SwiftHttpRunner::invokePosture Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libswift\Swi
ftHttpRunner.cpp Line: 1407 Level: debug  MSG_NS_SWISS_NEW_SESSION,
{{ise_fqdn="ciscolive-ise2.demo.local"}, {posture_port="8443"},
{posture_path="/auth/perfigo_validate.jsp"},
{posture_domain="posture_domain"}, {posture_status="Compliant"},
{session_id="0a3e949c000002585cf00588"},
{config_uri="/auth/anyconnect?uuid=f62337c2-7f2e-4b7f-a89a-3508d761173c"},
{acpack_uri="/auth/provisioning/download/066ac0d6-2df9-4a2c-a129-fabf1ace36aa"},
 {acpack_port="8443"}, {acpack_ver="4.6.3049.0"}, {pra_enabled=0}}.
```

ISE日志调查

1.在client-webapp组件启用到DEBUG的guest.log中，PSN使用过期/幻像会话进行回复，可以看到该会话。

---

2. PSN收到来自ISE终端安全评估代理的请求。这是来自AnyConnect的请求，因为User-Agent值：

<#root>

cisco.cpm.client.posture.PostureStatusServlet -::-

Got http request from 192.168.255.228 user agent is: Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.48; Any

cisco.cpm.client.posture.PostureStatusServlet -::-

mac_list

from http request ==> C0:4A:00:1F:6B:39

cisco.cpm.client.posture.PostureStatusServlet -::-

iplist

from http request ==> 192.168.255.228

cisco.cpm.client.posture.PostureStatusServlet -::-

Session id from http request -

req.getParameter

(

sessionId

) ==> null

3.请求包含IP地址和MAC地址数组。在本例中，每个数组仅包含一个值。日志显示来自请求的会话ID为null，这表示来自非基于重定向的探测功能的请求。稍后，您可以看到如何使用来自数组的值来定位会话ID:

<#root>

cpm.client.provisioning.utils.ProvisioningUtil -::- the input ipAddress from the list currently process

```
cpm.client.provisioning.utils.ProvisioningUtil -::- the ipAddress that matched the http request remote
cpm.client.provisioning.utils.ProvisioningUtil -::- the clientMac from the macarray list for the for lo
cisco.cpm.client.posture.PostureStatusServlet -::- Found Client IP matching the remote IP 192.168.255.2
cpm.client.provisioning.utils.ProvisioningUtil -::-
```

Session = 0a3e949c000000495c216240

4.在包含关键字Sent http response的行之后，可以查看来自回复的内容：

<#root>

```
cisco.cpm.client.posture.PostureStatusServlet -::- Sent an http response to  192.168.255.228 with X-ISE
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-PDP value is clemea19-ise1.demo.local
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-POSTURE value is /auth/perfigo_validat
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-POSTURE_PORT value is 8443
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_PORT value is 8443
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-GUESTFLOW value is false
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_CONFIG_URL value is https://clemea1
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_CONFIG_URI value is /auth/anyconnec
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_URL value is https://clemea19-i
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_URI value is /auth/provisioning
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_VER value is 4.6.3049.0
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-STATUS_PATH value is /auth/status
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-BACKUP_SERVERS value is clemea19-ise2.
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-SessionId value is 0a3e949c000000495c2
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-PostureDomain value is posture_domain
cpm.client.provisioning.utils.ProvisioningUtil -::-
```

header X-ISE-POSTURE_STATUS value is Unknown

调查ISE报告

知道过期/幻像会话的ID后，您可以调查Radius Accounting报告，以便更好地了解导致会话过期/幻像的原因：

---

1. 导航到操作>报告>终端和用户> Radius记账报告，并运行此报告7天；使用终端ID作为过滤器密钥。

2.以下是显示如何在ciscolive-ise2上保留过时会话的报告的示例：

2019-05-30 16:42:13.36	3 Stop	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise1
2019-05-30 16:32:20.819	2 Interim-Update	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise2
2019-05-30 16:32:16.263	1 Start	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise2

- PSN ciscolive-ise2是会话的记账开始。
- 会话的临时更新已在同一PSN上处理。
- 有问题的会话ID的记账停止消息发送到其他PSN(ciscolive-ise1。)

如何确定问题何时由未重新启动发现导致

同样的逻辑也适用于上一个问题，但是，唯一的区别是，您必须将焦点放在“Latest Scan Start Time（最新扫描开始时间）”上。对于此类问题，上次扫描的时间戳为过去。

通常，当最终用户发现问题时，会进行扫描。在ISE Radius Live日志中，发现有问题的终端最近的身份验证尝试。

此演示显示了问题识别所需步骤的记录：

高级故障排除：没有发现重新启动

此方法类似于高级故障排除陈旧/虚拟会话部分。主要的故障排除要素是DART捆绑调查。

在DART捆绑包中，您可以搜索发现重新启动（如前一个问题中所示），并确认报告问题时没有发现重新启动。

在ISE端，重点查看Radius Live Logs/ Radius身份验证报告，以确认PSN之间存在故障转移或NAD生成了新会话ID。

解决方案

传统方法 — 问题避免

过去，ISE没有解决本文档中所述问题的功能，因此，唯一的方法是依靠在网络和ISE端实施的一组最佳实践来最大程度降低风险。

可以最大限度地减少ISE部署中陈旧或幻像会话数量的最佳实践

尽可能始终实施基于重定向的终端安全评估

此建议的一个常见反击因素是，操作系统或浏览器中出现不良的用户体验。这表示在后台的AnyConnect ISE终端安全评估模块执行评估流程时进行重定向。

作为解决方案，可以仅重定向ISE终端安全评估模块发现探针并选择性地允许所有其他流量。此示例显示重定向的ACL旨在仅将HTTP请求重定向到发现主机（本示例中为10.1.1.1）和enroll.cisco.com(172.16.1.80):

```
ip access-list extended REDIRECT-DH-ENROLL
 permit tcp any host 10.1.1.1 eq www
 permit tcp any host 172.16.1.80
 deny   ip any any
```

为了保持可接受的安全级别，重定向ACL可与从ISE分配的DACL结合使用。

挂起状态仅允许连接到终端经过身份验证的PSN

此方法适用于不支持URL重定向的环境（通过第三方NAD实施）。

作为解决方案，实施多个状态挂起授权策略（每个PSN一个）。 每个策略必须包含进行身份验证的PSN名称作为条件之一。在授权配置文件中，必须阻止所有PSN（已进行身份验证的节点除外）。

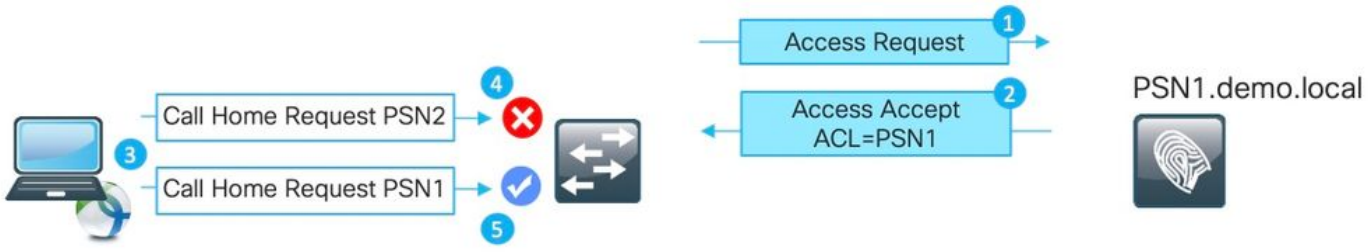
为两个节点创建授权策略：



---

1. PSN1的Posture Pending策略。
2. PSN1名称用作策略中的条件。
3. 带有ACL的授权配置文件阻止对除PSN1外的所有PSN的访问。
4. PSN2的Posture Pending策略。
5. PSN2名称用作策略中的条件。
6. 带有ACL的授权配置文件阻止对除PSN2外的所有PSN的访问。
7. 状态“兼容”授权策略。

下图说明了该方法的工作原理：



---

1. 身份验证命中PSN1。
2. 作为配置授权策略的结果，PSN1分配授权配置文件，阻止对PSN1以外的所有其他节点的访问。
3. AnyConnect ISE终端安全评估模块重新启动发现过程。
4. NAD与之前分配的ACL一样阻止对PSN2的探测。

5. NAD上分配的ACL允许探测到PSN1。

负载均衡器最佳实践

- 在负载均衡器上启用粘性，以使用Calling-Station-ID作为粘性密钥进行身份验证和记帐。请参阅Cisco & F5部署指南中的ISE最佳实践：使用BIG-IP的ISE负载均衡。
- 使用比平均工作日更长的粘性计时器来覆盖PC进入睡眠模式的时刻（例如10小时而不是8小时）。
- 如果实施重新身份验证，请使用略低于粘性计时器的重新身份验证计时器（如果粘性配置为10小时，则使用8小时）。 这可以确保通过重新身份验证延长粘滞间隔。

Posture Over VPN使用案例

确保accounting-interim更新间隔大于或等于vpn-session-timeout。这样可以最大程度地减少长VPN会话期间PSN之间的记帐抖动。 此示例显示为20小时配置的临时记帐更新间隔。这不会阻止传输分配给终端的IP地址的初始临时更新。

```
aaa-server ISE protocol radius

 interim-accounting-update periodic 20

group-policy SSL-VPN attributes

 vpn-idle-timeout 1200

 vpn-session-timeout 1200
```

可以实施最佳实践，以最大程度降低不重新启动ISE终端安全评估模块的影响

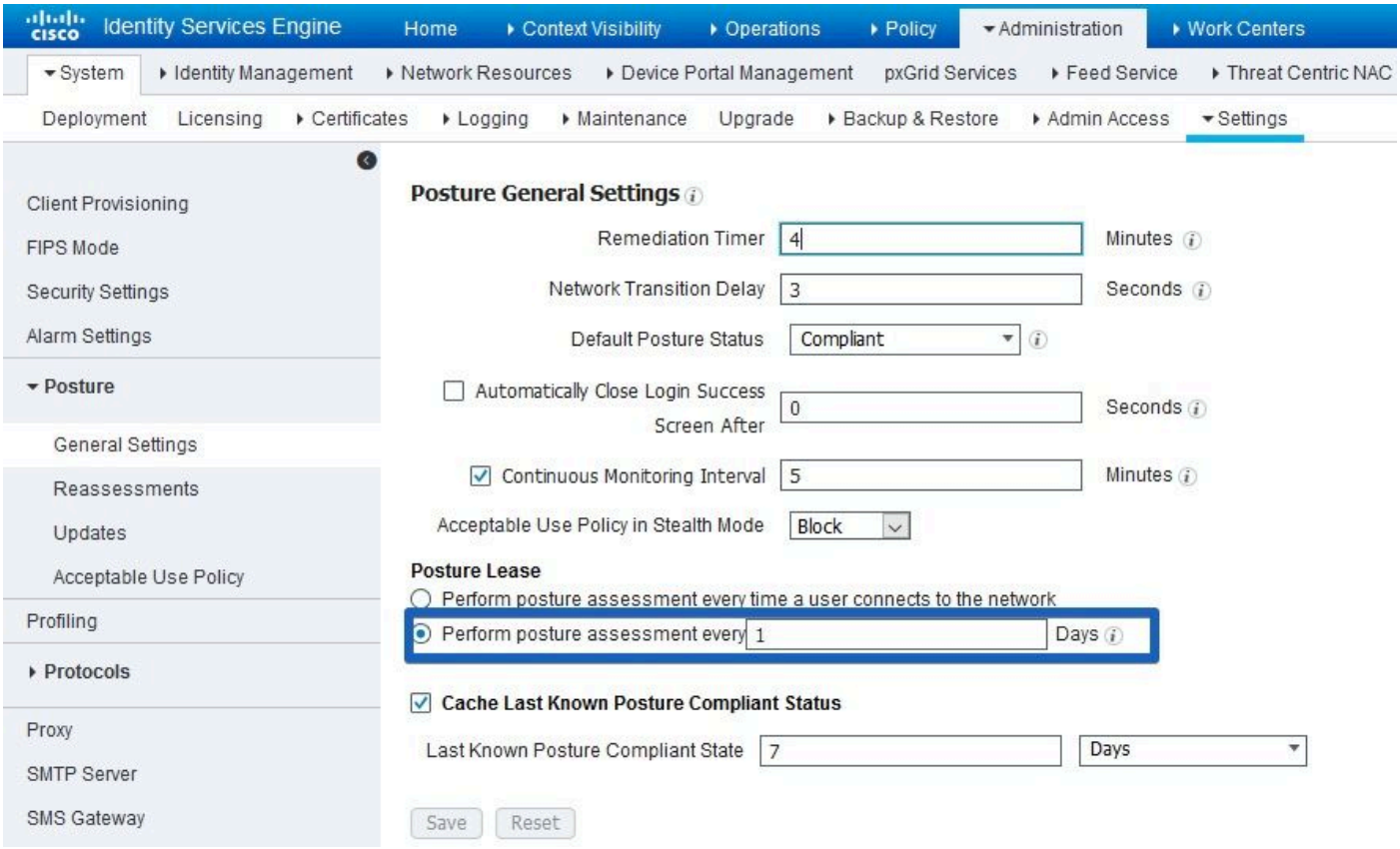
启用状态租用

这是ISE上的一个功能，将终端标记为compliant一段时间（1-365天）。 终端安全评估租用值是终端属性，这意味着它存储在ISE数据库上。包括终端安全评估租赁的所有终端属性在ISE部署中的所有节点上复制。

当PSN收到终端的新会话时，可以使用状态租用立即将会话标记为兼容。为了做出此决策，PSN使用3个值，这些值为：

---

1. 在ISE设置中为终端安全评估租用定义的天数：导航到Administration > System > Posture > General Settings:



2. PostureExpiry属性的值是包含Epoch时间戳的终端属性。PostureExpiry值最初在ISE管理员启用终端安全评估租约后对终端首次成功进行终端安全评估尝试时填充。稍后，此值会在租期到期后进行的下一次成功安全评估尝试时更新。当打开其中一个状态终端时，您可以在情景可视性>终端中看到PostureExpiry:

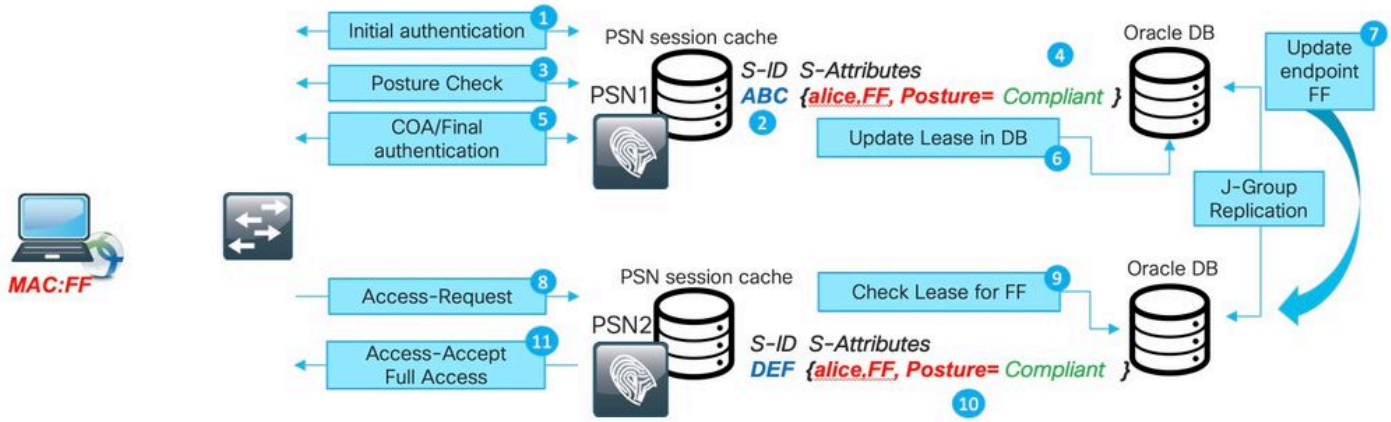


3.此值可以转换为人类可读的时间戳，例如，此处 — https://www.epochconverter.com/



3.当终端安全评估租用的身份验证到达PSN时，它使用PostureExpiry和系统日期来检索上次成功的状态检查所经过的天数。如果结果值在设置中定义的安全评估租用间隔内，会话将收到Compliant状态。如果结果值大于租用值，则会话会收到Unknown状态。这会触发再次执行安全评估并且可保存新的PostureExpiry值。

下图描述了发生故障切换时的过程：

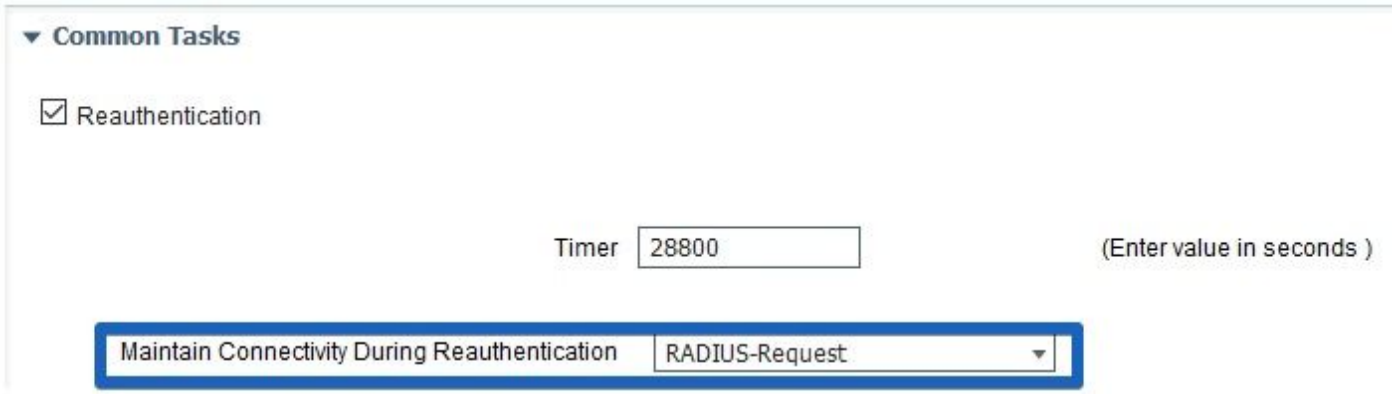


---

1. PSN1进行初始身份验证。
2. 会话ABC在会话缓存中创建。
3. 进行状态评估。
4. 会话状态更改为Compliant。
5. COA由状况状态更改触发，导致终端重新身份验证以应用于下一个访问级别。
6. PostureExpiry值保存在终端中。
7. 终端数据在部署中复制。
8. 下一个身份验证命中PSN2。
9. PSN2检查终端是否处于有效的终端安全评估租约中。
10. 会话会作为Compliant添加到会话缓存。
11. 由于有效租约，会话创建时安全评估状态为Compliant。

重新身份验证实施

始终使用RADIUS-Request从ISE推送重新身份验证计时器，在Maintain Connectivity During Reauthentication中选择。此设置确保NAD在重新身份验证时保持相同的会话ID。



具有负载均衡器的环境

可以实施相同的一组最佳实践（在过时/幻像会话部分中说明）。

不同的子网可用于待处理和合规状态

当网络设计提供使用不同子网（例如Pending和Compliant状态）的机会时，此方法可保证终端安全评估状态每次更改都会导致默认网关更改。

与重新身份验证计时器相同的时间间隔内使用的状态评估

状态评估可以启用且间隔等于重新身份验证计时器。当原始PSN不可用时，PRA故障将重新启动发现过程。

现代方法 — 状态共享

作为ISE 2.6的已实施增强功能（在Cisco Bug ID CSCvi35647中）补丁6的一部分，ISE部署中的所有节点之间共享会话状态的新功能可实现。

此增强功能已集成到ISE 2.7补丁2和ISE 3.0的未来版本中。

此新功能基于ISE 2.6中引入的轻量级会话目录(LSD)机制。在较新版本中，此功能被重命名为轻量级数据分发(LDD)Radius会话目录。默认情况下启用轻型数据分发，并允许在ISE节点之间共享有限的会话上下文。PSN之间没有完整的会话上下文复制，每个会话仅共享有限数量的属性。

当部署中的一个节点必须确定当前会话所有者时，轻会话目录就无需执行对MNT的资源昂贵API调用。启动COA流时，必须查找所有者。使用LDD，每个PSN可以从本地Radius会话目录缓存找到会话的所有者。

轻量级数据分布架构

此功能包含以下元素：

- Radius会话目录(RSD)缓存：此缓存存在于每个ISE节点上，并存储ISE部署中显示的所有活动会话。每个会话在缓存中的属性数量有限。以下是每个会话的Radius会话目录中存储的属性示例：
  - 会话 ID
  - 终端MAC
  - 呼叫站ID
  - 终端IP
  - PSN IP — 进行身份验证的PSN
  - PSN FQDN
  - NAS-IP-Address
  - NAS-IPv6-Address
  - 状态 — 已验证、已启动、已停止

- RabbitMQ Exchange:在ISE部署中的每个节点上存在发布者、相关队列和消费者时形成交换。这可确保所有ISE节点之间形成全网状拓扑。

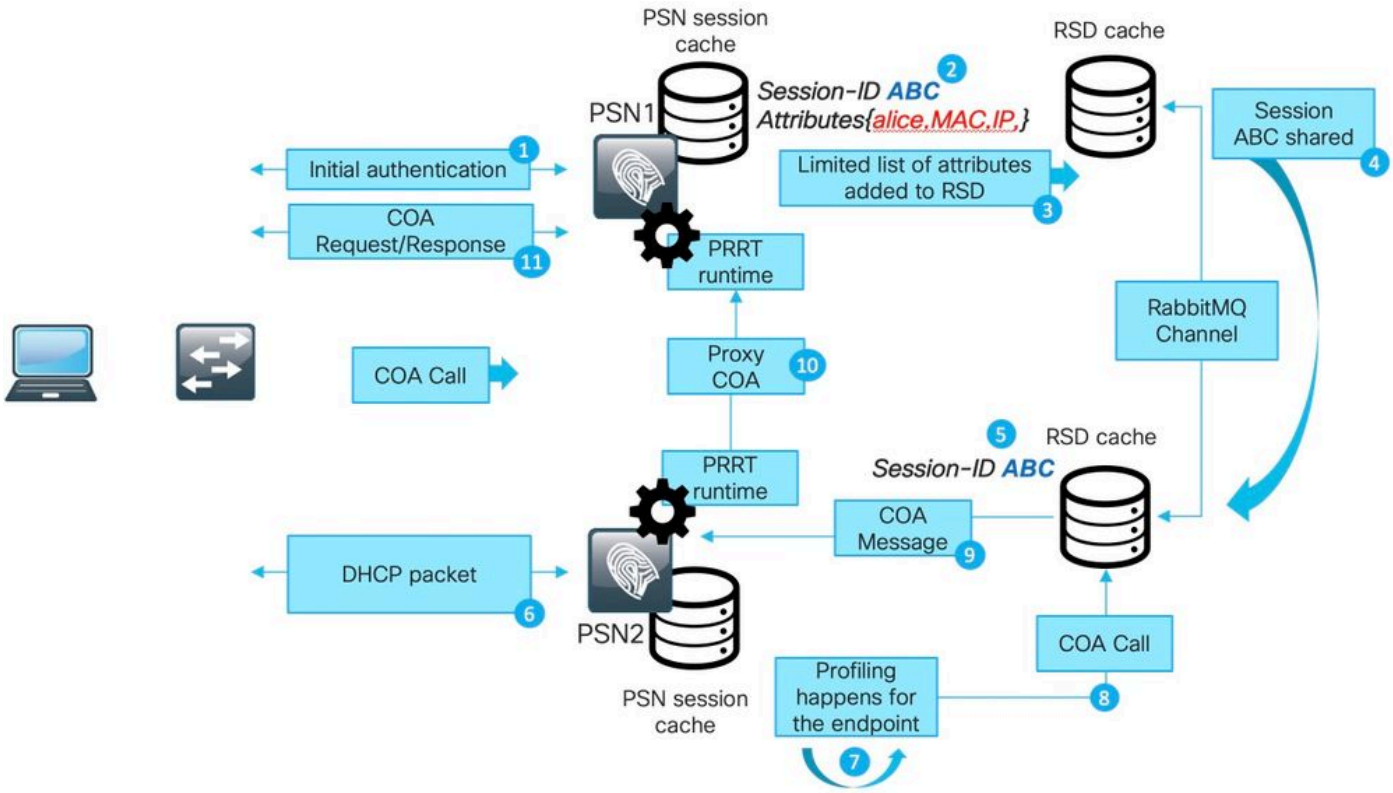
- 发布者:Radius会话目录代表发布者。当PSN处理新的成功身份验证时，会在PSN会话缓存中创建一个新会话。对于此会话，会将一组有限的属性放入Radius会话目录中。

- 消费者：在所有其他节点上，Radius会话目录代表消费者。



注意：通用RabbitMQ术语和体系结构不在本文档范围之内。

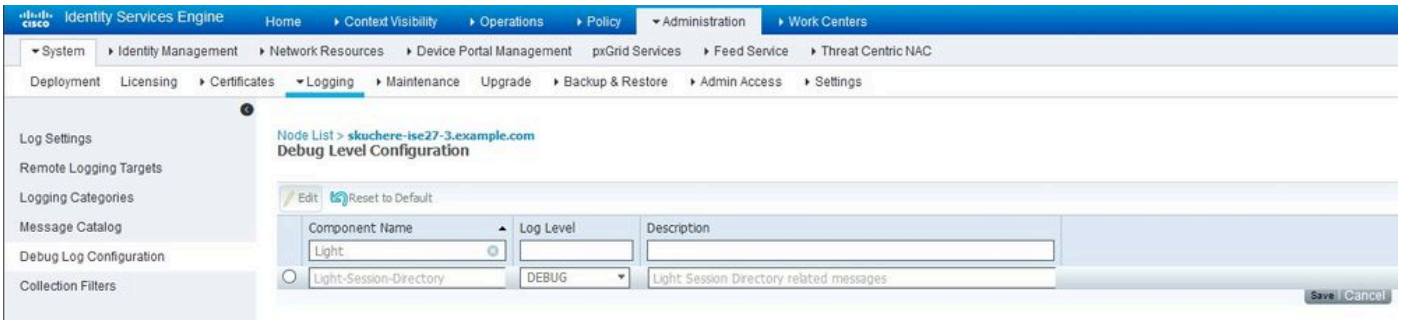
下一个示例解释了COA流如何与RSD缓存配合使用：



---

1. PSN1进行初始身份验证。
2. 会话ABC在会话缓存中创建。
3. 所需的属性保存在RSD中。
4. 会话通过RabbitMQ与所有其他ISE节点共享。
5. 会话在所有ISE节点的RSD缓存中创建。
6. 新的配置文件数据到达PSN2。
7. 重新分析终端，并且（在需要COA执行PSN2的更改的情况下）继续执行下一步。
8. 将内部API调用提交到RSD缓存以执行COA。
9. 来自RSD缓存的数据用于准备代理COA消息。它从一个ISE节点移至另一个ISE节点，并包含目标节点可用于向NAD发回CAO请求的所有详细信息。COA消息首先在内部传输到PRRT运行时（ISE内的实际AAA服务器）。
10. PSN2向PSN1发送COA消息。
11. PSN1向NAD发送COA消息。

要在ISE上排除通过LDD的通信故障，请将Light-Session-Directory组件启用到DEBUG:



以下是lsd.log文件中的调试消息示例，用于在原始PSN上创建和发布会话：

```
DEBUG  [pool-45-thread-6][] cisco.cpm.lsd.service.LSDRedisClient -::::- Mapping Session ID 0a3e94980000
DEBUG  [PrRTEvents-Executor-2][] cisco.cpm.lsd.service.LSDNetAccessEventListener -::::- Publishing sess
DEBUG  [PrRTEvents-Executor-2][] cisco.cpm.lsd.service.SessionPublisher -::::- Forwarding session 07a26
```

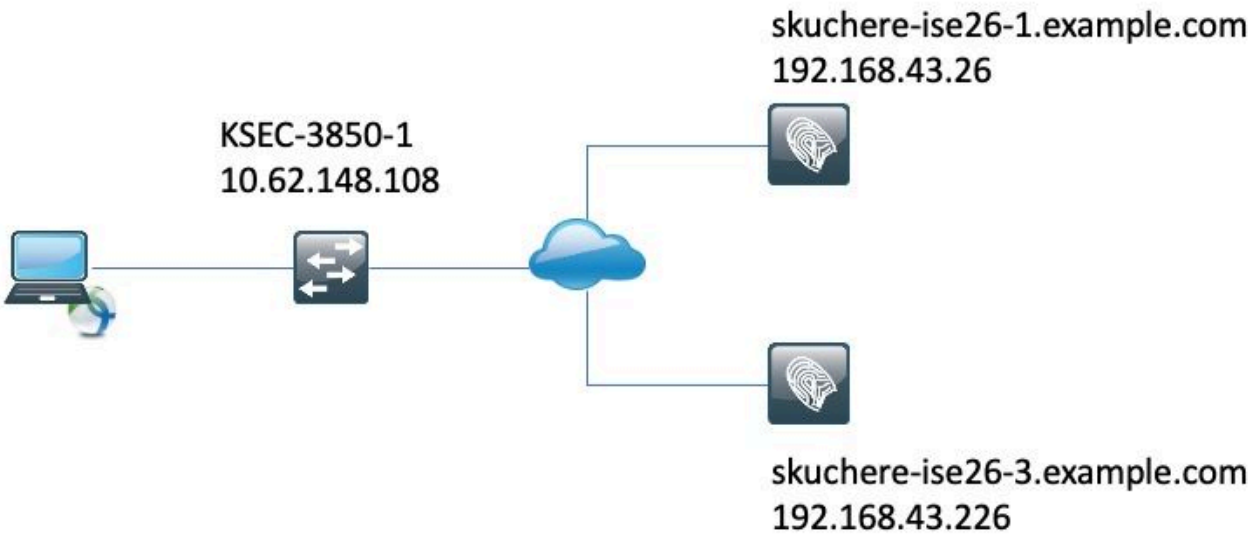
在所有其他ISE节点上，您可以看到会话是如何消耗的：

```
[pool-35-thread-38][] cisco.cpm.lsd.service.SessionConsumer -::::- Consumer is processing : sessionID:[
```

通过RSD共享终端安全评估状态

状态状态共享解决了以下问题：根本原因是过时/幻像会话或在未触发发现重启的其他PSN上重新进行身份验证。当会话变为合规时，此信息会进入会话RSD，以后可由部署中的每个PSN使用。

所述特征还不能解决其它一些角的情况。例如，当NAD在同一PSN上使用不同的会话ID运行重新身份验证时。可以采用本文档中描述的最佳实践处理这些场景。此图显示了用于测试状态共享状态的拓扑：



通过RSD共享终端安全评估状态 — 陈旧/幻像会话

要创建陈旧会话，最初必须在skuchere-ise26-1上执行身份验证。然后，必须重新配置NAD以将记帐发送到skuchere-ise26-3。在将一个记帐消息转发到错误的PSN后，必须重新配置NAD（再次）以将记帐发送回skuchere-ise26-1。

此图显示一个记帐报告，证明在skuchere-ise26-3上存在幻像会话:

Stop	3.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296
Interim-Update	2.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-3	0A3E946C0000007D5B679296
Start	1.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296

---

1. Accounting-Start消息由skuchere-ise26-1处理。
2. 临时记帐 — 由skuchere-ise26-3处理的同一会话的更新。
3. 会话稍后在skuchere-ise26-1上完成。

终端连接到网络，但重定向不再有效。在skuchere-ise26-3的PSN的guest.log中，您可以在启用了client-webapp组件的DEBUG中看到以下日志消息：

```
2020-04-08 13:30:48,217 DEBUG [https-jsse-nio-192.168.43.226-8443-exec-4][] cisco.cpm.client.posture.Ut
```

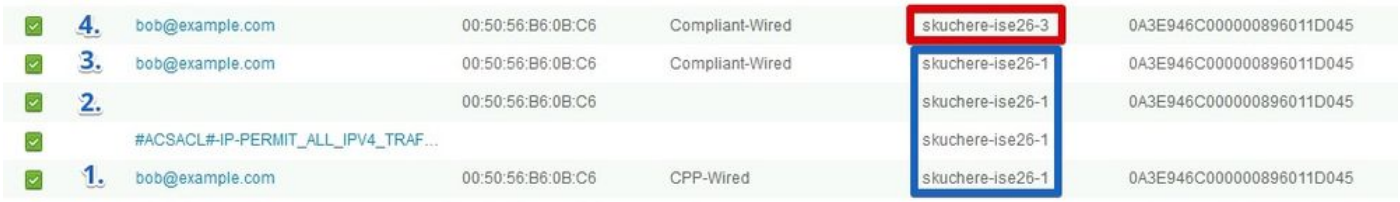
当PSN检测到它保留终端过期/幻像会话时，它不会回复ISE终端安全评估模块，这允许您从发生最新身份验证的PSN获取信息。

作为会话查找时过时/幻像会话问题的解决方案，PSN会检查RSD中是否存在终端的任何新会话。如果RSD包含的会话ID与本地会话缓存中的PSN不同，则它假定会话（显示在会话缓存中）已过时。

RSD上的状态共享 — PSN之间的故障转移

要重现此场景，可在分配给合规状态终端的授权配置文件中启用一个短重新身份验证计时器。之后，重新配置NAD以将身份验证和记帐发送到另一个PSN(skuchere-ise26-3)。重新身份验证计时器到期后，同一会话将在不同PSN上取消身份验证。

下图显示身份验证报告，其中显示从skuchere-ise26-1到skuchere-ise26-3的同一会话的故障切换：



4.	bob@example.com	00:50:56:B6:0B:C6	Compliant-Wired	skuchere-ise26-3	0A3E946C000000896011D045
3.	bob@example.com	00:50:56:B6:0B:C6	Compliant-Wired	skuchere-ise26-1	0A3E946C000000896011D045
2.		00:50:56:B6:0B:C6		skuchere-ise26-1	0A3E946C000000896011D045
	#ACSACL#-IP-PERMIT_ALL_IPV4_TRAF...			skuchere-ise26-1	
1.	bob@example.com	00:50:56:B6:0B:C6	CPP-Wired	skuchere-ise26-1	0A3E946C000000896011D045

---

1. 在skuchere-ise26-1上发生身份验证，分配具有重定向的授权配置文件。
2. COA在成功的状况评估之后。
3. 授权配置文件到合规状态的下一个身份验证已分配。
4. 身份验证命中不同的PSN，但它仍会收到合规状态的授权配置文件。

在ise-psc.log中故障切换后，会话在新PSN上处于合规状态，并且在DEBUG中启用了epm-pip和nsf-session组件：

<#root>

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.SessionCache -::::-

Looking up session 0A3E946C000000896011D045 for attribute Session Session.PostureStatus


2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- Execution con
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.PIPManager -::::- Returning a PIP co
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- Execution con
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.SessionCache -::::- Looking up sessi
2020-04-09 11:06:42,176 DEBUG [SessionLifecycleNotifier][] cpm.nsf.session.internal.LRUAgingAlogrithm -
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.SessionCache -::::- Returning for se
```

IndexValues: {}

2020-04-09 11:06:42,177 DEBUG [Thread-7979][] cisco.cpm.posture.pip.PostureStatusPIP -::::-

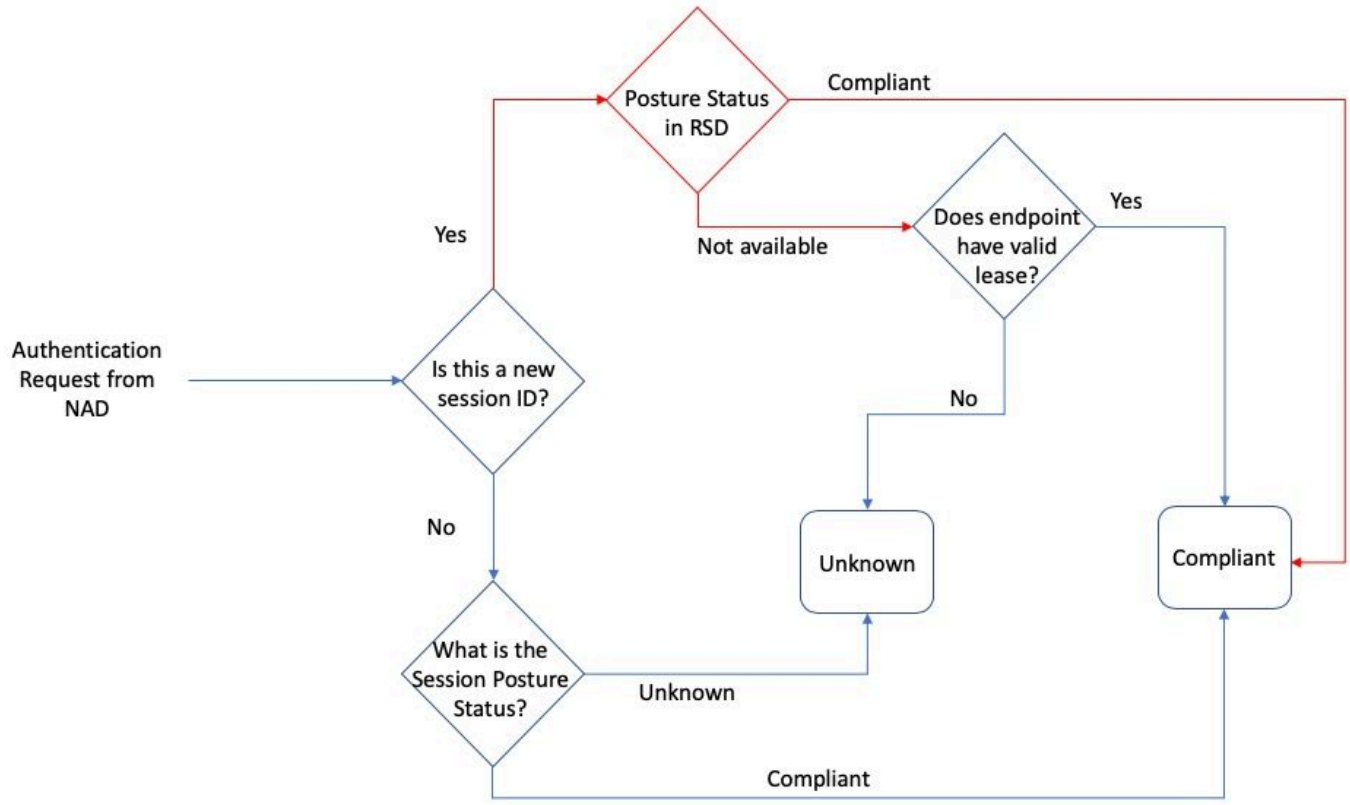
set postureStatus based on posture LSD dictionary: Compliant

2020-04-09 11:06:42,177 DEBUG [Thread-7979][] cisco.cpm.posture.pip.PostureStatusPIP -::::-

PostureStatusPIP for mac 00-50-56-B6-0B-C6 - Attribute Session.PostureStatus value is Compliant

---

通过在状态选择过程中添加额外逻辑即可解决原始问题。此图显示了所更改的内容（更改以红色突出显示）：



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。