

# ISE状态部署最佳实践和考虑事项

## 目录

[简介](#)

[限制](#)

[状态客户端行为](#)

[请使用案件](#)

[用例1 -客户端重新验证强制NAD生成个新会话ID。](#)

[用例2 -交换机配置与顺序MAB DOT1X和优先级DOT1X MAB \(有线\)。](#)

[用例3 -无线客户端漫游，并且另外AP的认证去不同的控制器。](#)

[用例4 -部署用负载均衡器\(前2.6补丁程序6， 2.7补丁程序P2和3.0\)。](#)

[用例5 -阶段2发现探测比客户端验证与responded到由一个不同的服务器\(前2.6修补6， 2.7补丁程序2， 和3.0\)。](#)

[行为更改发表物2.6补丁程序6， 2.7修补2和3.0](#)

[考虑事项，当维护同样SessionID时](#)

## 简介

本文描述寻址有基于重定向的状态的几个使用案件的一些基准配置。在这些配置中客户端保持兼容，但是网络接入设备(NAD)限额访问，因为在重定向状态。

## 限制

在本文的配置不一定工作为Cisco NAD，但是为第三方NAD。

## 状态客户端行为

状态客户端将触发探测器在这些时刻：

- 首次登录
- 第3层(L3)更改/network接口卡(NIC)更改(新建的IP地址， NIC状态变换)

## 请使用案件

### 用例1 -客户端重新验证强制NAD生成个新会话ID。

在此用例，客户端是兼容的，但是由于重新验证，NAD在重定向状态(重定向URL和访问列表)。

默认情况下，身份服务引擎(ISE)配置每次执行连接对网络的一状态评估，特别地每个新会话的。

此设置配置在工作区>状态>设置>状态一般设置下。

## Posture General Settings ⓘ

Remediation Timer  Minutes ⓘ

Network Transition Delay  Seconds ⓘ

Default Posture Status  ⓘ

Automatically Close Login Success Screen After  Seconds ⓘ

Continuous Monitoring Interval  Minutes ⓘ

Acceptable Use Policy in Stealth Mode

### Posture Lease

Perform posture assessment every time a user connects to the network

Perform posture assessment every  Days ⓘ

Cache Last Known Posture Compliant Status

Last Known Posture Compliant State

Save

Reset

为了保持从生成个新会话ID的NAD在重新验证，请配置在授权配置文件的这些重新验证值。显示的重新验证计时器不是标准推荐，重新验证计时器应该每根据连接类型的部署考虑(无线/有线的)，设计(什么是在loadbalancer的持续时间规则)，等等。

策略>Policy元素>发生>授权>授权配置文件

Reauthentication

Timer  (Enter value in seconds)

Maintain Connectivity During Reauthentication

### ▼ Advanced Attributes Settings

Select an item  =  - +

### ▼ Attributes Details

Access Type = ACCESS ACCEPT  
 Session-Timeout = 3600  
 Termination-Action = RADIUS-Request

在交换机上，您需要配置每个接口或者模板，从ISE获得其重新验证计时器。

authentication timer reauthenticate server

**Note:** 如果有负载均衡器，您需要确保，持续时间配置用方式重新验证将返回对原始策略服务 (PSN)。

## 用例2 -交换机配置与顺序MAB DOT1X和优先级DOT1X MAB (有线)。

在这种情况下重新验证将终止，因为802.1x会话的一个核算终止将发送，当MAC验证旁路(MAB)在重新验证时尝试。

- 为MAB进程发送的核算终止，当发生故障验证时正确，因为客户端的用户名从802.1X用户名变成MAB用户名。
- Dot1x作为在核算终止的方法id也正确，虽然授权的方法dot1x。
- 当Dot1x方法成功时，发送核算从方法id开始作为dot1x。此处，此行为是正如所料。

为了解决此问题，请配置cisco-av-pair : 终端操作修正值= 1在使用的authZ配置文件，当终端是兼容的。此attribute-value (AV)对指定不管配置的顺序，NAD应该重新使用在原始验证的选择的方法。

## Advanced Attributes Settings

Cisco:cisco-av-pair = termination-action-modifier=1

## Attributes Details

Access Type = ACCESS\_ACCEPT  
Session-Timeout = 60  
Termination-Action = RADIUS-Request  
cisco-av-pair = termination-action-modifier=1

Save

Reset

### 用例3 -无线客户端漫游，并且另外AP的认证去不同的控制器。

对于此情况，无线网络将需要设计，以便接入点(AP)在伸手可及的距离内对漫游的使用其他AP同一个激活控制器。一示例是无线局域网控制器(WLC) Stateful Switchover (SSO)故障切换。关于WLC的高性能的(HA) SSO的更多信息，请参阅[高性能的\(SSO\)部署指南](#)。

### 用例4 -部署用负载均衡器(前2.6补丁程序6，2.7补丁程序P2和3.0)。

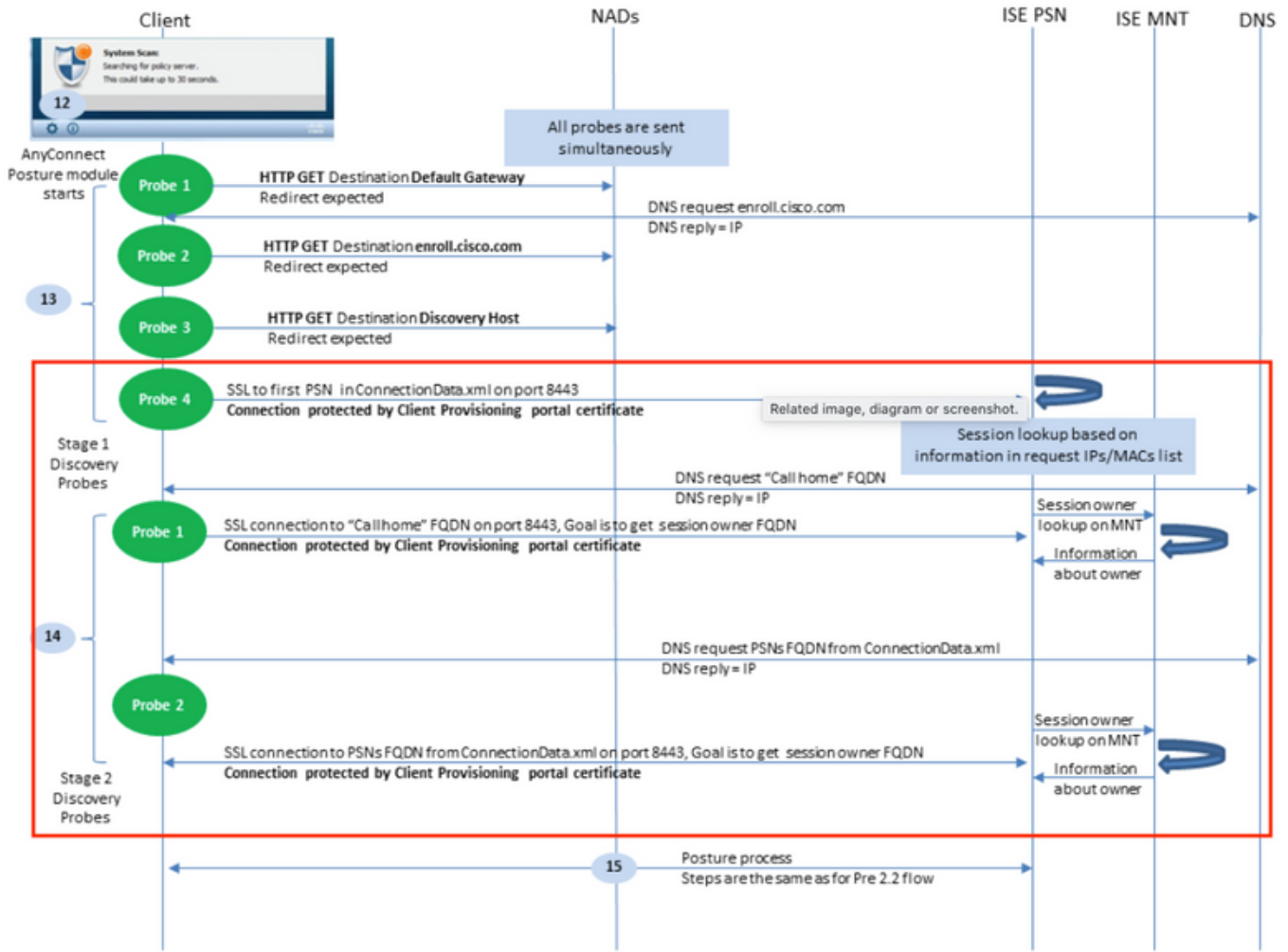
在部署用介入的负载均衡器，确保是重要的，在您做在上一个使用事例后的变动，会话继续去同样PSN。在为此步骤/补丁程序之前列出的版本，状态状态没有复制在节点之间通过轻的数据 Distribution (以前轻的会话目录)。因此，返回不同的状态状态结果不同的PSN是可能的。

如果持续时间没有正确地配置，重新鉴别的会话比最初使用的那个可能去不同的PSN。如果这发生，新的PSN可能指示会话符合状态作为未知和通过authZ结果与重定向访问控制表(ACL) /URL和限制终端访问。再次，在NAD的此更改不会由状态模块认可，并且探测器不会被触发。

关于如何配置负载均衡器的更多信息，请参阅[Cisco & F5部署指南：ISE负载均衡使用BIG-IP](#)。它为在负载被平衡的环境的ISE部署提供最佳实践设计的高水平概述和F5特定配置。

### 用例5 -阶段2发现探测比客户端验证与response到由不同的服务器(前2.6修补6，2.7补丁程序2，和3.0)。

看一看在红色方框内的探测器在此图表中。



PSN在original PSN将存储会话数据五天，“兼容”会话的会话数据仍然那么有时居住，即使客户端不再验证与该节点。如果在红色方框放入的探测器响应对由PSN除当前验证会话，并且PSN以前拥有了并且指示了兼容此的终端的那个之外，为了有状态模块的状态验证PSN的状况在终端和当前之间的一不匹配是可能的。

这是一些常见情况此不匹配能发生的地方：

- 当从网络时，断开核算终止没有为终端接收。
- NAD从一个PSN故障切换到另一个。
- 负载均衡器寄认证给同一个终端的不同的PSN。

为了从此行为保护，ISE可以配置只允许从一个特定的终端的发现探测到达当前验证的PSN。为了达到此，请配置每个PSN的一项不同的授权策略在您的部署。在这些策略，请参考包含可下载的访问控制表的一不同的authZ配置文件(DACL)仅允许探测器对在authZ情况指定的PSN。参见此示例：

每个PSN将有未知状态状态的一个规则：

Search	AND	Network Access-ISE Host Name EQUALS ise2-6-psn1	Session-PostureStatus NOT_EQUALS Compliant	Posture_Unknown_PSN1	Select from list	0	⚙️
PSN1_unknown1	AND	Network Access-ISE Host Name EQUALS ise2-6-psn2	Session-PostureStatus NOT_EQUALS Compliant	Posture_Unknown_PSN2	Select from list	0	⚙️
Dot1X_Internal_Compliance	AND	Session-PostureStatus EQUALS Compliant	InternalUser-IdentityGroup EQUALS User Identity Groups:ALL_ACCOUNTS (default)	PermitAccess	Select from list	1	⚙️

每个配置文件参考不同的DAACL。

**Note:**对于无线，请使用Airespace ACL。

Authorization Profiles > Posture\_Unknown\_PSN1

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

#### Common Tasks

DACL Name

每个DAACL只允许处理验证对PSN的探测器访问。

Downloadable ACL List > Posture\_Unknown\_DACL\_PSN1

### Downloadable ACL

\* Name

Description

IP version  IPv4  IPv6  Agnostic

\* DACL Content

1234567	permit udp any any eq 53
8910111	permit udp any any eq bootps
2131415	permit ip any host 10.10.10.1
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

在前一个示例中，10.10.10.1是PSN 1的IP地址。如果限制访问对仅PSN该把柄验证，被参考的DAACL可以为所有其它服务/IP被修改当必要时，但是。

## 行为更改发表物2.6补丁程序6，2.7修补2和3.0

状态状态被添加了到RADIUS会话目录通过轻的数据分配框架。每次状态状态更新在所有PSN接收

，将复制对在部署的所有PSN。一旦此更改有效，到达在不同的认证的不同的PSN认证和或探测器的暗示删除和所有PSN应该能应答到他们当前验证的所有终端不管。

在本文的五个使用事例中，请考虑这些行为：

用例1 -客户端重新验证强制NAD生成个新会话ID。客户端是兼容的，但是由于重新验证，NAD在重定向状态(重定向URL和访问列表)。

-此行为不会更改，并且在ISE和NAD应该仍然实现此配置。

用例2 -交换机配置与顺序MAB DOT1X和优先级DOT1X MAB (有线)。

-此行为不会更改，并且在ISE和NAD应该仍然实现此配置。

用例3 -无线客户端漫游，并且另外AP的认证去不同的控制器。

-此行为不会更改，并且在ISE和NAD应该仍然实现此配置。

用例4 -部署用负载均衡器。

-应该仍然跟随在负载均衡指南定义的最佳实践，但是，在认证转发对不同的PSN由负载均衡器情况下，正确状态状态应该返回对客户端。

用例5 -阶段2发现探测比客户端验证与responded到由一个不同的服务器

-这不应该是与新的behavior的一个问题，并且每PSN授权配置文件不应该是必要的。

## 考虑事项，当维护同样SessionID时

当您在本文时使用列出的方法，保持已连接对网络的用户可能潜在保持兼容在长时间时间。即使他们重新鉴别，sessionID不更改并且ISE将继续通过他们的匹配兼容状态的规则的AuthZ结果。

在此事件，定期重新估价需要配置，以便状态将要求确保终端保持兼容与公司策略在定义间隔。

这可以配置在工作区>状态>设置> Recessment配置下。

