



# 将监控和报告工具集成到网络准入控制中

## 文档目的

本文档提供监控和报告工具的构建或扩展指南，旨在支持网络准入控制（NAC）的状态信息。本文档适用于 NAC 的最初版本，用作实施设备，为 Cisco® IOS® 路由器提供支持。随着思科不断演进 NAC，包括其它网络接入设备（NAD），如交换机和无线接入点，本文档也会随之更新。本文档包含重要系统组件的设计注意事项和输出格式详情。欲知 NAC 的更多信息，包括系统布局和设计实施方案建议，请访问：<http://www.cisco.com/go/nac>。

## 目标受众

本文档的受众包括监控和报告工具的供应商以及负责报告 NAC 集成的系统工程师。本文档假设您熟悉 NAC 体系结构、组件、配置和功能，还假设您熟悉支持 NAC 状态信息的监控和报告工具。

## 1. 概述

系统报告和监控是 NAC 不可或缺的组成部分，可提供状态相符性和系统采取的认证措施的审核轨迹。思科系统已经为第三方集成监控和事件报告产品定义了事件监控和报告界面。本文档对事件流和界面进行了描述。本文档分为以下几个部分：

- I 事件源
- I 设计注意事项
- I 输出详情

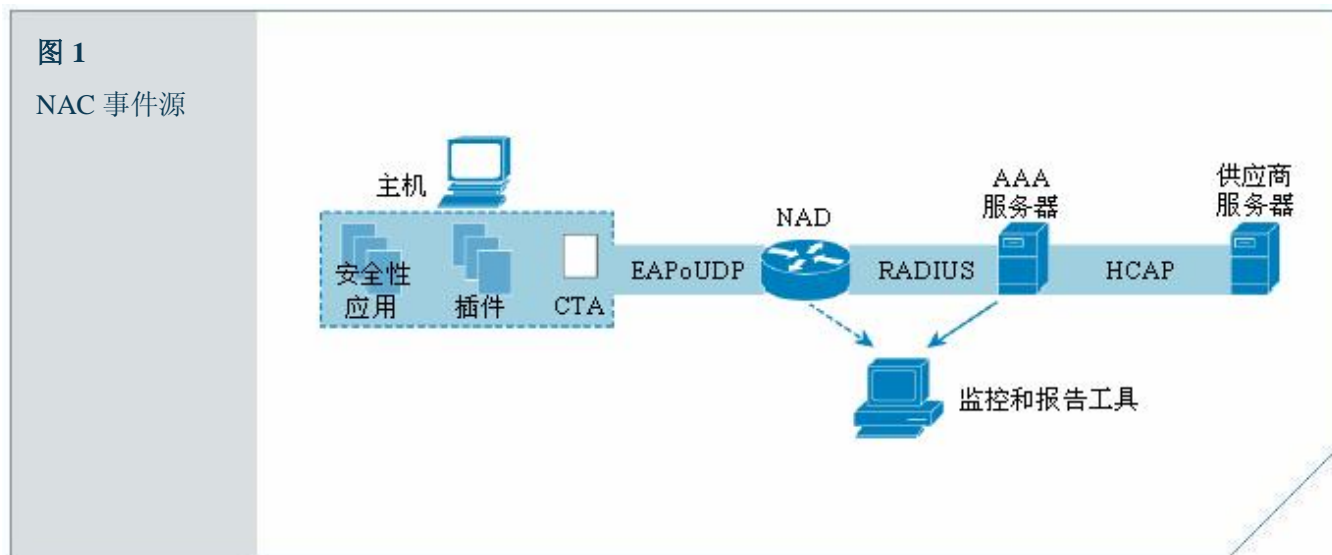
## 2. 监控和报告事件源

NAC 系统中包含 5 种组件：

- I 主机组件（通常是指端点设备），包括集成到 NAC 中的应用和端点共存的 Cisco Trust Agent，能够为网络提供 NAC 通信信道。
- I 网络接入设备（NAD），特别是 Cisco IOS®路由器，作为 NAC 第一阶段的组成部分，可以触发 NAC 进程，是策略执行设备。NAC 的第二阶段应当包括交换机和无线 802.11 (Wi-Fi)接入点。
- I 认证、授权和记帐（AAA）服务器，特别是思科安全接入控制服务器（ACS），是执行状态报告检查（从主机应用程序确认信息）并根据评估确定授权的决策点。虽然授权仍然由思科 ACS 定义，但 AAA 服务器可向第三方供应商服务器发送用于评估的状态报告检查信息。
- I 通过监控和报告工具，能够看到 NAC 系统状态和状态报告检查处理的实时和历史审计，如：提供与每个用户、每台主机或每个 NAD 相符和不相符的审计报告。
- I 状态验证服务器（PVS）可以是能够将状态报告集授权给一组或多组属性值对（AVP）的任何服务器。尽管 AAA 服务器是 PVS 的一个实例，但该术语通常用于描述能协助授权特定域的状态报告的代表服务器。例如，抗病毒服务器可以用作 PVS，做出特定抗病毒状态决策，因为抗病毒服务器熟悉最新的扫描引擎和签名文件版本。

## 将监控和报告工具集成到网络准入控制中

图 1 中列出了这些组件。



监控和报告工具的功能如下：

- I 收集并解释与 NAC 操作相关的所有 ACS 事件
- I 收集和报告与 NAC 相关的所有思科 IOS 系统日志事件
- I 收集和解释与 NAC 相关的所有供应商服务器事件，包括第三方供应商产品（例如 Symantec、Network Associates 和 Trend Micro）的服务器事件。

ACS 输出是需要集成的最重要组件。作为策略制定点，它是能够提供证书检查状态的详细信息、证书本身的详细情况和所制定的授权决策的唯一元件。来自路由器的集成输出是值得考虑的事情——如果不能到达访问 ACS，它确实能提供可视性。路由器不理解或记录状态证书——输出就限于系统日志（NAC 的微弱信号和噪音）。而在大型部署中，由于可能要大量部署多台路由器，企业会发现将系统日志转移到中心服务器并不现实。而将第三方服务器的输出链接到监控工具，可能会让某些企业产生一定的兴趣。

### 3. 设计注意事项

由于 NAC 中的路由器可以在整个企业进行部署，ACS 服务器及其监控和报告功能将被集中到一个或多个数据中心。在大多数的 NAC 部署中，

## 将监控和报告工具集成到网络准入控制中

第一阶段所涉及的数据量是可以预见的，如每秒 1-10 个事件，可以考虑每秒解决最多 25 个事件。ACS 生成的实际数据量相当小，因此对数据库存储的要求预计会较低。

### 3.1 重要的报告属性

事件报告应当包含以下多个属性：

- I 端点源信息，包括 IP 地址、主机名、采取的实施措施（访问控制列表[ACL]、VLAN 分配或状态令牌）、用户名（目录服务名称，如果有的话）、MAC 地址、事件的时间戳、使用的事件类型、客户端违规补救的平均时间。
- I 网络设备信息
  - 距离违规客户端最近的相邻设备的管理 IP 地址
  - 动态配置 ACL 的接口
  - 采取的措施类型
  - 措施的时间戳，包括措施的完整性（例如，成功或失败百分比）
- I ACS
  - 活动的（如有可能，要求 RADIUS 启动/停止记录，以确定状态）
  - 最后的 n 分钟
  - 最后的 n 小时
  - 最后的 n 天
  - 介于用户可配置的启动时间和停止时间之间

表 1 对生成 NAC 事件的众多事件类型进行了描述，并根据客户端访问请求和 NAD 控制活动，对一段时期发生的 NAC 活动进行了总结。

表 1. 事件类型

|                           |
|---------------------------|
| 收集和解释与NAC相关的所有ACS事件       |
| 收集和解释与NAC相关的所有思科IOS系统日志事件 |
| 收集和解释与NAC相关的所有抗病毒服务器事件    |
| 扩展支持200台路由器               |

## 将监控和报告工具集成到网络准入控制中

|  |
|--|
| 扩展支持1000台路由器   |
| 以每秒5个事件的速率处理网络准入事件   |
| 以每秒25个事件的速率处理网络准入事件（ACS验证目标）   |
| 提供实时监控仪表板，其中包含最近的相符事件结果的概述和详细视图，仪表板中的信息包括 IP 地址、主机名（NetBIOS 和/或完全合格的域名[FQDN]）、相符性检查结果（及原因）、采取的执行措施、用户名（如果有）、MAC 地址（如果有）、路由器识别和时间戳。 |
| 允许支持员工使用查找工具并根据IP地址、主机名或用户名（如果有）来主动或被动地支持相符性检查问题。<br>交叉参考监控和报告用户信息、活动目录帐户和用户资料信息（详细情况有待确定）<br>提供总体不相符报告（仅限于故障）的概述和可选详细信息           |
| 根据时间、路由器、主机身份信息、相符性检查结果、相符性执行措施和管理责任，过滤不相符的报告  |
| 提供相符性趋势报告<br>提供相符性记分卡报告的可选趋势（例如，完全符合的系统=0、部分符合的系统=1-5，不符合的系统=5）  |
| 将相符性记分卡评级与实时监控仪表板联系起来  |
| 根据IP地址、主机名和路由器，提供基于主机的相符性结果报告（成功、部分成功和失败）  |
| 提供无响应的系统报告（不提供证书的设备）   |
| 提供不符合的重试报告，其中包括单个设备重复执行的相符性检查的失败次数（类似于失败的用户认证尝试）   |
| 提供不符合的重试报告，告知单个设备重复执行的相符性检查的失败次数（类似于失败的用户认证尝试）<br>提供NAC系统可用性、请求延迟和扩展使用率（用于容量规划）的有关监控和报告信息  |

## 将监控和报告工具集成到网络准入控制中

|                        |
|------------------------|
| 提供追踪系统调优变化的管理变化日志报告    |
| 监控事件可能与电子邮件、寻呼机和脚本操作相关 |
| 无响应主机的总数               |

### 3.1.1 终端站点/用户报告示例

- l 报告每个终端站点/用户的所有准入活动
- l 报告每个终端站点/用户的多次事件活动
- l 按照最终用户应用群体对报告进行分组
- l 无响应的主机报告
- l 被拒绝的主机站点报告
- l 按照主机报告进行补救的时间
- l 思科 IOS 无响应主机报告
- l 按照应用类型（Symantec、Computer Associates、Trend 等）对网络状态进行的总结

### 3.1.2 NAD 报告示例

- l 所有适用网络设备的 NAC 活动报告
- l 网络设备类型（例如交换机或路由器）的活动总结
- l 思科 ACS 内部的活动总结

## 4. 输出详情

### 4.1 思科 ACS 日志客户化输出

集成到思科 ACS 中的基于浏览器的管理是能够用于执行 ACS 组件配置管理的唯一工具。

日志文件的属性是通过思科 ACS Web 界面进行配置的。日志文件提供接入 ACS 记录信息的唯一标准 API。ACS 配置指南提供必要字段的配置指南，用于进行关联和生成报告。日志输出根据思科 ACS 中的“系统配置”记录页面进行自定义。

### 4.2 如何接收输出

- I 在一个或多个 ACS 上监控并报告引擎的共同放置。配置如下：  
System Configuration > Logging > Remote Logging Setup。该配置不适用于 ACS 解决方案引擎部署。
- I 实时将思科 ACS 日志输出到与监控和报告引擎位于同一位置的 ACS 远端代理。配置如下：System Configuration > Logging > Remote Logging Setup。
- I 实时将日志直接输出到与兼容开放数据库连接（ODBC）的数据库中。配置如下：System Configuration > Logging。

### 4.3 已通过的认证

注意：状态验证不需要任何用户身份信息。对于部分或全部状态验证条目来说，用户名和组名字段可留空。

每次成功通过认证或状态验证后，就会在思科 ACS 已通过的认证日志中创建一条新条目。这只代表进行状态验证的时间，而不是该会话的持续时间。表 2 列出的属性是默认的属性。管理员可以选择其它的字段并关联到报告中。

## 将监控和报告工具集成到网络准入控制中

表 2. 认证信息

| 字段名称             | 描述                                     | 示例   |
|------------------|--|--|
| 日期               | 日期 (月/日/年)                             | 12/17/2003   |
| 时间               | 时间 (24小时)                              | 16:08:35   |
| 信息类型             | 信息类型                                   | 状态   |
| 用户名              | 用户名                                    | ghoward  |
| 组名               | 网络接入组 (最后映射的用户组)                       | 正常   |
| 主叫ID             | 主机源IP地址和/或MAC地址                        | 10.21.82.178   |
| NAS端口            | NAD端口                                  | 2个   |
| NAS IP地址         | NAD IP地址                               | 172.20.99.161  |
| PEAP-清除-名        | 用户名                                    | ghoward  |
| 思科: PA: 系统-状态-令牌 | 主机最后的系统状态令牌                            | <ul style="list-style-type: none"> <li>• 正常</li> <li>• 检查</li> <li>• 隔离</li> <li>• 已感染;</li> <li>• 未知</li> </ul> |
| 思科: PA: 应用-状态-令牌 | 逗号隔开的成对数值列表, 包括所有厂商及应用类型、它们各自的应用状态令牌等; | 思科: PA=正常, NAI: 抗病毒=隔离, 思科: 主机=检查  |
| “厂商、应用类型、属性”     | 主机可靠值                                  | 特殊属性   |
| 原因               | 决定原因 (策略名称和与之对应的法规编号)                  | 外部主机配置<br>=<name>; 策略名称<br>=<name>; 法规<br>ID=<rule-id><br>备注: 外部策略返回的状态令牌不显示<br>RuleID。                          |

ACS 通过认证日志默认条目示例:

| 日期         | 时间       | 信息类型      | 用户名     | 组名  | 主叫ID         | NAS端口 | NAS IP地址        | 过滤器信息  |
|------------|----------|-----------|---------|-----|--------------|-------|-----------------|--------|
| 12/17/2003 | 17:17:51 | Authen OK | ghoward | 默认组 | 10.21.82.178 | 2个    | 2 172.20.99.161 | 无过滤器激活 |

## 将监控和报告工具集成到网络准入控制中

### 4.4 失败尝试

每次认证失败，思科 ACS 失败尝试日志都会创建新条目。由于不是所有的状态验证都是身份鉴别，并且网络许可策略总是分配到处于某种形式的主机上，所以不是所有状态条目都能增加到该日志文件中。思科 ACS 错误配置是唯一可能在失败尝试日志中触发状态条目的操作。在该错误配置下，ACS 不能将某个状态级别与网络接入组进行映射。

默认 ACS 失败尝试日志条目示例：

| 日期         | 时间       | 信息类型 | 用户名         | 组名       | 主叫ID             | 认证失败代码     | 授权失败代码 | 授权数据 | NAS 端口 | NAS IP地址      | 过滤器信息 |
|------------|----------|------|-------------|----------|------------------|------------|--------|------|--------|---------------|-------|
| 12/17/2003 | 17:17:42 | 认证失败 | ghowar<br>d | 默认<br>的组 | 10.21.82.<br>178 | CS密码<br>无效 | ..     | ..   | 2      | 172.20.99.161 | ..    |

### 4.5 RADIUS 记帐

Cisco ACS RADIUS 记帐日志继续通过网络许可设备 NAD 转发启动/停止记帐记录，这时主机启动和停止网络会话。主机在网络上激活时，来自该日志的信息是决定准确性的唯一方法。

ACS RADIUS 记帐日志默认登录属性见表 3。管理员在相关报告中可以选择其它字段。

表 3 RADIUS 记帐日志记录的属性

| 字段名 | 描述         | 示例         |
|-----|------------|------------|
| 日期  | 日期 (月/日/年) | 12/17/2003 |
| 时间  | 时间 (24小时)  | 16:08:35   |
| 用户名 | 用户名        | ghoward    |

## 将监控和报告工具集成到网络准入控制中

|          |                              |  |
|----------|------------------------------|--|
| 组名       | 网络接入组                        | 正常   |
| 主叫站点ID   | 主机源IP地址和/或MAC地址              | 10.21.82.178   |
| 记帐状态类型   | 记帐成帧状态类型                     | 启动/停止  |
| 记帐会话ID   | 唯一的会话ID                      | 00000029   |
| 记帐会话时间   | 会话持续时间（秒）                    | 5  |
| 服务类型     | 服务类型介绍                       | 状态   |
| 记帐输入八位组  | 出主机的NAD接收的八位组个数              | 10034  |
| 记帐输出八位组  | 入主机的NAD发送的八位组个数              | 10035  |
| 记帐输入数据包  | 出主机的NAD接收的数据包个数              | 872  |
| 记帐输出数据包  | 入主机的NAD发送的数据包个数              | 456  |
| NAS端口    | NAD端口                        | 2个   |
| NAS IP地址 | NADIP地址                      | 172.20.99.161  |
| 原因       | 决策的原因（策略名称及与之对应的来自所有PPD的法规编号 | <ul style="list-style-type: none"> <li>• 下列原因之一将显示；</li> <li>• 外部主机配置=&lt;name&gt;：令牌无组映射；</li> <li>• 任何外部主机配置中，无对应的强制信任类型；</li> <li>• 任何策略不返回令牌。</li> </ul> |

思科 ACS RADIUS 记帐日志默认条目示例：

| 日期         | 时间       | 用户名     | 组名  | 呼叫站ID        | 记帐状态类型 | 记帐会话ID   | 记帐会话时间 | 服务类型  | 成帧协议 | 记帐输入八位组 | 记帐输出八位组 | 记帐输入数据包 | 记帐输出数据包 | 成帧IP地址 | NAS端口 | NAS IP地址      |
|------------|----------|---------|-----|--------------|--------|----------|--------|-------|------|---------|---------|---------|---------|--------|-------|---------------|
| 12/17/2003 | 17:18:05 | ghoward | 默认组 | 10.21.82.178 | 停止     | 00000032 | 11     | NAS提示 | ..   | ..      | ..      | ..      | ..      | ..     | 2     | 172.20.99.161 |
| 12/17/2003 | 17:17:53 | ghoward | 默认组 | 10.21.82.178 | 启动     | 00000032 | ..     | NAS提示 | ..   | ..      | ..      | ..      | ..      | ..     | 2     | 172.20.99.161 |

## 5. 思科 IOS 系统日志

### 5.1 EAPoUDP 的思科 IOS 系统日志字段

#### 5.1.1 会话的创建/取消

下列信息表示创建或删除条目：是关于在特定的接口的的主机的

```
00:21:59: %EOU-6-SESSION: IP=16.0.0.15| HOST=DETECTED|  
Interface=Ethernet1/3  
01:17:26: %EOU-6-SESSION: IP=16.0.0.15| HOST=REMOVED|  
Interface=Ethernet1/3
```

I 严重性——信息类

#### 5.1.2 状态验证状态

下列信息表示特殊主机的状态验证结果：

```
01:19:25: %EOU-6-POSTURE: IP=16.0.0.15| HOST=AUTHORIZED|  
Interface=Ethernet1/3  
01:19:25: %EOU-6-POSTURE: IP=16.0.0.15| HOST=REJECTED|  
Interface=Ethernet1/3
```

I 严重性——信息类

#### 5.1.3 Cisco Trust Agent 检测

下列信息表示思科 IOS 路由器是否能在特定主机上删除 Cisco Trust Agent。

```
01:21:23: %EOU-6-CTA: IP=16.0.0.15| CiscoTrustAgent=DETECTED  
01:21:23: %EOU-6-CTA: IP=16.0.0.15| CiscoTrustAgent=NOT DETECTED
```

I 严重性——信息类

## 将监控和报告工具集成到网络准入控制中

### 5.1.4 认证类型

下列信息表示特殊主机的认证类型。表 4 对认证类型进行了介绍：

01:21:23: %EOU-6-AUTHTYPE: IP=16.0.0.15| AuthType=EAP

00:23:09: %EOU-6-AUTHTYPE: IP=16.0.0.15| AuthType=CLIENTLESS

00:34:05: %EOU-6-AUTHTYPE: IP=16.0.0.15| AuthType=STATIC

表 4 认证类型

| 类型           | 介绍                     |
|--------------|------------------------|
| 扩展认证协议 (EAP) | 特定的主机由AAA服务器使用EAP进行认证。 |
| 无客户端         | 特定的主机无响应，但通过了认证。       |
| 静态           | 特定的主机通过静态认证。           |

I 严重性——信息类

### 5.1.5 主机策略

策略信息为主机特别规定接收的策略属性：

01:24:40: %EOU-6-POLICY: IP=16.0.0.15| TOKEN=Healthy

01:24:00: %EOU-6-POLICY: IP=16.0.0.15|

ACLNAME=#ACSACL#-IP-Healthy-3fcf2e35

01:24:00: %EOU-6-POLICY: IP=16.0.0.15| URL=<http://11.0.0.3>

I 严重性——信息类

### 5.1.6 与身份识别策略匹配

下列信息介绍了与特殊主机匹配的本地身份识别组合/策略。

01:30:51: %EOU-6-IDENTITY\_MATCH: IP=16.0.0.15|

PROFILE=EAPoUDP| POLICYNAME=P1

I 严重性——信息类

### 5.1.7 状态查询结果

下列信息提供了状态查询结果。表 5 介绍了该查询。

```
01:32:12: %EOU-6-SQ: IP=16.0.0.15| STATUSQUERY=VALIDATED
```

```
01:34:22: %EOU-6-SQ: IP=16.0.0.15| STATUSQUERY=FAILED
```

```
01:35:07: %EOU-6-SQ: IP=16.0.0.15| STATUSQUERY=NORESPONSE
```

表 5 状态查询

| 类型  | 介绍                    |
|-----|-----------------------|
| 已确认 | 主机再次成功通过确认。           |
| 失败  | 主机没有通过确认，必须进行全部NAC确认。 |
| 无响应 | 主机没有响应，删除主机会话。        |

### 5.1.8 EAPoUDP 版本不匹配

下列信息表明 EAP over User Datagram Protocol (EAPoUDP)版本不匹配。

```
01:41:43: %EOU-4-VERSION_MISMATCH: HOST=16.0.0.1| Version=5
```

I 严重性——警告

### 5.1.9 进程创建错误

下列信息表示 EAPoUDP 进程的故障。该故障可能是设备需要进行重新装载的地方缺少关键条件。

```
02:13:12: %EOU-2-PROCESS_ERR: HOST=16.0.0.1| Version=5
```

I 严重性——严重

只有配置“EOU 日志”后，EAPoUDP 信息才能显示。根据默认设置，EoU 日志没有启动。

```
p72-23.13#show eou
```

```
Global EAPoUDP Configuration
```

```
EAPoUDP Version = 1
```

## 将监控和报告工具集成到网络准入控制中

```
EAPoUDP Port= 0x5566
Clientless Hosts= Enabled
IP Station ID = Disabled
Revalidation= Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period = 3 Seconds
StatusQuery Period = 30 Seconds
Hold Period = 180 Seconds
AAA Timeout = 60 Seconds
Max Retries = 3
EAPoUDP Logging = Disabled <=====
Clientless Host Username = clientless
Clientless Host Password = clientless
```

### 5.1.9.1 特定接口 EAPoUDP 配置

```
Interface Ethernet 1/3
```

无特定接口的配置

```
p72-23.13#conf t
```

输入配置命令，1 行 1 个命令。以 CNTL/Z 结束。

```
p72-23.13(config)#eou logging
```

```
p72-23.13#sh eou
```

### 5.1.9.2 全局 EAPoUDP 配置

```
EAPoUDP Version = 1
```

```
EAPoUDP Port= 0x5566
```

```
Clientless Hosts= Enabled
```

```
IP Station ID = Disabled
```

```
Revalidation= Enabled
```

```
Revalidation Period = 36000 Seconds
```

```
ReTransmit Period = 3 Seconds
```

```
StatusQuery Period = 30 Seconds
```

```
Hold Period = 180 Seconds
```

## 将监控和报告工具集成到网络准入控制中

AAA Timeout = 60 Seconds

Max Retries = 3

EAPoUDP Logging = Enabled <=====

Clientless Host Username = clientless

Clientless Host Password = clientless

### 5.2 AuthProxy

#### 5.2.1 状态验证启动

下列信息表示特殊主机的状态验证启动。

01:54:12: %AP-6-POSTURE\_START\_VALIDATION: IP=16.0.0.15|

Interface=Ethernet1/3

I 严重性——信息类

#### 5.2.2 形式会话状态修改

下列信息表示状态验证状态所做的修改。

01:53:50: %AP-6-POSTURE\_STATE\_CHANGE: IP=16.0.0.15|

STATE=POSTURE INIT

01:54:51: %AP-6-POSTURE\_STATE\_CHANGE: IP=16.0.0.15|

STATE=POSTURE ESTAB

I 严重性——信息类

#### 5.2.3 AuthProxy 形式高速缓存极限超出

下列信息表示在 INIT 状态中已经超过最大极限的授权代理形式高速缓存条目数量。

01:53:50: %AP-4-POSTURE\_EXCEED\_MAX\_INIT: Exceeded maximum  
limit

(100) on entries in authentication proxy posture cache in initializing state

## 将监控和报告工具集成到网络准入控制中

### I 严重性——警告

打开 AuthProxy 系统日志，使用 `ip auth-proxy auth-proxy-audit` 命令启动全局 CLI 的记录功能。

```
p72-23.13#conf t
```

```
p72-23.13(config)#ip auth-proxy auth-proxy-audit
```

**备注：**在此操作中，将主动提供所有重大/警告/告警信息。



### 思科系统（中国）网络技术有限公司

#### 北京

北京市东城区东长安街1号  
东方广场一办公楼19-21层

邮政编码：100738

电话：(8610)85155000

传真：(8610)85181881

#### 上海

上海市淮海中路222号力宝  
广场32-33层

邮政编码：200021

电话：(8621)33104777

传真：(8621)53966750

#### 广州

广州市天河北路233号中信  
广场43楼

邮政编码：510620

电话：(8620)85193000

传真：(8620)38770077

#### 成都

成都市顺城大街308号冠城  
广场23层

邮政编码：610017

电话：(8628)86961000

传真：(8628)86528999

如需了解思科公司的更多信息，请浏览<http://www.cisco.com/cn>

思科系统（中国）网络技术有限公司版权所有。