美洲台：与ACS 5.x及以后配置示例的LDAP集成

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[配置](#)
[流程图图表](#)
[Beacon Endpoint Profiler 系统的 MAB 配置](#)
[为 ACS 配置 MAB 以及使用 Beacon 作为外部用户数据库](#)
[创建授权配置文件](#)
[创建LDAP数据库连接](#)
[配置访问服务](#)
[交换机的 MAC 身份验证旁路配置](#)
[验证](#)
[相关信息](#)

简介

本文提供一配置示例为了配置信标和思科安全访问控制系统(ACS) 5.x和以后启用为MAC验证旁路有效和更高效地配置的Cisco设备(MAB)验证在已验证网络的non-802.1x有能力设备。

思科实现功能呼叫在他们的交换机的MAB的，以及在ACS的必须支持，为了适应在不能通过802.1X验证的802.1X启用的网络的终端。此功能保证没有配备有802.1X功能，例如，没有一功能802.1X请求方，可以在接纳前验证，以及有基本网络使用策略被强制执行在他们的连接中尝试的终端连接到802.1X启用的网络。

通过 MAB 可将网络配置为当标识的设备无法参与 802.1X 协议时允许此设备将其 MAC 地址用作主要凭证。为了能将有效部署和使用的MAB，环境必须有方法识别没有能力在802.1X验证上在环境的设备和随着时间的推移维护这些设备一个最新数据库和移动，添加，并且更改发生。此列表需要手工填充和被维护在认证服务器(ACS)，或者通过一些备用方法为了保证在MAC验证的设备这时完成和有效。

信标终端仿形铣床能自动化非正在验证终端，那些，不用802.1X恳求者和这些终端正确性的维护的识别的进程在变化的缩放网络的在终端描出和行为监控功能的。通过标准 LDAP 接口，Beacon 系统可以用作端点的外部数据库或目录，以通过 MAB 进行验证。当MAB请求从边缘基础设施时接收，ACS能查询信标系统为了确定是否应该承认一个给的终端根据关于信标已知的终端的最当前的信息的网络。这防止对手动配置的需要。

对于一相似的配置使用版本早于ACS 5.x，参考美洲台：与ACS配置示例的LDAP集成。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS软件版本12.2(25)SEE2的Cisco 3750交换机
- Cisco Secure ACS 5.x和以后

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

MAB是设备动态支持的一个重要功能例如打印机、IP电话、传真机和其他non-802.1x有能力设备在环境post-802.1X部署。如果没有 MAB 功能，对于连接至不支持 802.1X 的端点的网络接入端口，必须进行静态设置以免尝试 802.1X 身份验证，或者通过使用提供极其有限的策略选项的其他功能来进行设置。显然，这样注定了无法在大型企业环境中进行扩展。如果在所有接入端口上同时启用 MAB 和 802.1X，那么不支持 802.1x 的已知端点可以移至环境中的任意位置，并且仍能可靠（安全）地连接到网络。由于设备被承认网络验证，不同的策略可以应用到不同的设备。

此外，如有必要，还可以通过 MAB 向环境中不支持 802.1X 的未知端点（例如，访客或承包商的便携式计算机）提供对网络的有限访问权限。

顾名思义，MAC 身份验证旁路使用端点的 MAC 地址作为主要凭证。使用在接入端口启用的 MAB，如果终端连接并且不能应付802.1X身份验证质询，端口恢复对MAB模式。尝试对端点执行 MAB 的交换机使用站点的 MAC 向 ACS 发出标准 RADIUS 请求。它尝试连接到网络并且在终端的接纳前请求终端的验证从ACS的对网络。

配置

流程图图表

此流程图说明MAB如何与802.1X验证一道使用在思科边缘基础设施和新的终端尝试连接到网络。

本文使用此流程图工作流：

图 1：身份验证流程

ACS可以配置使用其自己的内部数据库或一个外部LDAP服务器为了验证MAC地址用户请求。默认情况下信标终端仿形铣床系统充分地支持LDAP的并且可以由ACS使用为了通过标准LDAP功能验证MAC地址用户请求。由于信标自动化发现以及描出在网络的所有终端， ACS能通过LDAP查询信标

为了确定MAC应该是否被承认网络，并且应该映射分组终端。这极大自动化并且提高MAB功能，特别在大型企业环境。

通过 Beacon 提供的行为监视功能，如果被监视设备的行为与已启用 MAB 的配置文件不一致，则会将这些设备转至已启用 LDAP 的配置文件之外，从而使下次常规重新验证尝试失败。

Beacon Endpoint Profiler 系统的 MAB 配置

为了支持 MAB 而配置 Beacon 系统来集成 ACS 的过程非常简单，因为在默认情况下已启用 LDAP 功能。主要配置任务是标识包含环境中要通过 MAB 身份验证的端点的配置文件，并对这些配置文件启用 LDAP。一般，信标配置文件，包含组织拥有的设备，在端口必须是提供的网络访问，当看到，知道无法通过802.1X验证。一般，这些是包含打印机、IP电话或者管理的UPS作为普通的示例的配置文件。

如果信标描出的打印机在名为*Printers的*配置文件安置了，并且在配置文件的IP电话命名了*Ipphones*，例如，则这些配置文件需要为LDAP启用这样在那些配置文件安置的终端导致成功认证作为已知IP电话和打印机在环境通过MAB。如果启用LDAP的一配置文件，如此示例所显示，这在终端配置文件配置里要求选择LDAP单选按钮，：

图 2：对配置文件启用 LDAP

当指引的ACS代理MAC验证通过LDAP，查询包括两子查询。这两必须返回一种有效，非无效的结果。对 Beacon 的首个查询是 Beacon 是否已知 MAC，例如是否已发现 MAC 并将其添加到 Beacon 数据库中。如果 Beacon 尚未发现此端点，此端点则视为未知。

如果 Beacon 尚未发现端点，且该端点不在 Beacon 数据库中，则不必执行第二个查询。如果该端点已被发现且位于 Beacon 数据库中，下一个查询将确定该端点的当前配置文件。如果终端还要被描出或当前在配置文件为LDAP启用的没有5，未知结果返回对ACS，并且终端的验证由信标的发生故障。它依赖于怎样这能一共导致有访问否认的设备对网络的ACS配置，或者给为未知或访客设备是适当的策略。

仅当 MAC 端点已被 Beacon 发现且位于已启用 LDAP 的配置文件中时，才会向 ACS 返回 Beacon 已知且已分析该端点，并以此作为响应。最重要，对于这些终端请指引提供当前配置文件名称。这使ACS映射已知终端对思科SecureAccess组。这可以精确确定策略，如有必要，可以为已启用 LDAP 的每个 Beacon 配置文件精确确定一个单独的策略。

为 ACS 配置 MAB 以及使用 Beacon 作为外部用户数据库

为 ACS 配置 MAB 以及使用 Beacon 作为外部用户数据库需要执行三个不同步骤。本文档说明的顺序遵循用于执行 MAB 完整配置的高效工作流，对于已配置其他身份验证模式的系统，可能有所不同。

当您尝试尝试连接到网络的一个特定的终端的时MAB， ACS查询在LDAP指引为了确定信标是否发现MAC，并且什么配置文件信标当前安置了MAC地址如描述前在本文。

在本文中，两独立的配置文件创建：

- BeaconKnownDevices —终端已发现的和描出由信标
- BeaconUnknownDevices —不由信标当前知道的设备的

信标未发现MAC，也当前未描出它对一支持LDAP的配置文件。BeaconKnownDevices配置文件在VLAN10将放置终端，并且BeaconUnkownDevices配置文件在VLAN 7.将放置终端。

以后在本文，对信标终端仿形铣床的一个LDAP连接从ACS创建，并且组从基于的信标终端仿形铣床选择在哪些终端将考虑作为BeaconKnown设备和分配在VLAN 10)将放置他们的BeaconKnownDevices配置文件(。所有未知设备信标未发现MAC，也当前未描出它到一支持LDAP的配置文件将分配在VLAN 7)将放置他们的BeaconUnkownDevices配置文件(。

创建授权配置文件

完成这些步骤为了创建授权配置文件：

1. 选择**策略元素>授权和权限>网络访问>授权配置文件**并且单击**创建**创建一新的授权配置文件。
2. 提供新的授权配置文件的**名称**。
3. 在**普通的任务**选项卡设置**VLAN为**与**值的静态**作为**10。**然后，单击 **Submit**。
4. 选择**策略元素>授权和权限>网络访问>授权配置文件**并且单击**创建**创建一新的授权配置文件。
5. 提供新的授权配置文件的**名称**。
6. 在**普通的任务**选项卡设置**VLAN**为与**值的静态**作为**7。**然后，单击 **Submit**。

创建LDAP数据库连接

完成步骤为了创建LDAP数据库连接：

1. 选择**用户，并且标识存储>外部标识存储> LDAP**并且单击**创建**创建一新的LDAP数据库连接。
2. 为新的**LDAP数据库连接**提供一**名称**并且**其次**单击。
3. 在**服务器连接**选项卡请输入**信标LDAP塞弗的主机名/IP地址，端口， Admin DN，密码**(在本例中的GBSbeacon)。然后单击 **Next**。
4. 在**目录组织**选项卡请输入必填信息。然后单击 **Finish**。
5. 点击新建立的**LDAP连接**(在本例中的信标)。
6. 选择**目录组**选项卡并且点击**精选**。连接。
7. 选择您要映射到**BeaconKnownDevices的**Next屏幕的所有组。
8. 在本例中这些组，即lab_laptop， 3com_gear和apple_users，选择。然后，单击 **Submit**。

配置访问服务

完成这些步骤为了配置访问服务：

1. 选择**访问策略>Access服务**并且单击**创建**创建一新的访问服务。
2. 在**常规选项卡请**提供新的服务的**名称**，然后在**基于旁边**单击**精选服务模板**。
3. 选择**网络访问- MAC验证旁路**和点击OK键。
4. 单击 **Next**。
5. 单击 **完成**。
6. 单击 **Yes**。
7. 点击**自定义**。
8. 移动从**联机的UseCase选择**并且点击OK键。
9. 单击**创建**创建一个新的**服务选择规则**。
10. 选择**协议**并且请使用**Radius**作为值。同样地，请选择**UseCase**并且请使用**主机查找**作为值。选择信标**验证**作为服务并且点击OK键。
11. 搬到新建立的规则顶部。
12. 点击**Save Changes**。
13. 选择**访问策略>Access Services>信标验证>标识**并且在**标识来源旁边**单击**精选**。

14. 选择**信标**并且点击OK键。
15. 点击**Save Changes**。
16. 选择**访问策略>Access Services>信标验证>授权**并且点击**自定义**。
17. 移动**信标：从联机的ExternalGroups选择**并且点击OK键。
18. 单击**创建**创建新规则。
19. 选择3com_users、apple_users和lab_laptop，条件和授权配置文件**BeaconKnownDevices**结果。然后，单击**OK**。
20. 点击**默认**。
21. 选择3com_users、apple_users和lab_laptop，条件和授权配置文件**BeaconUnKnownDevices**结果。然后，单击**OK**。
22. 点击**Save Changes**。这完成步骤。

交换机的 MAC 身份验证旁路配置

此交换机配置为802.1X验证提供一配置示例以启用的MAB和要求的动态VLAN再分配行为为了适用从ACS返回的RADIUS属性。

交换机

```
switch#show running-config ! version 12.2 no service pad
service timestamps debug uptime service timestamps log
datetime service password-encryption service sequence-
numbers ! ! aaa new-model aaa authentication login
default line aaa authentication enable default enable
aaa authentication dot1x default group radius aaa
authorization network default group radius aaa
accounting dot1x default start-stop group radius ! aaa
session-id common switch 1 provision ws-c3750g-24ts ip
subnet-zero ip routing no ip domain-lookup ! ! ! ! ! !
dot1x system-auth-control no file verify auto spanning-
tree mode pvst spanning-tree extend system-id ! vlan
internal allocation policy ascending ! ! interface Port-
channel1 switchport trunk encapsulation dot1q switchport
trunk allowed vlan 5,7,9,10 ! interface Port-channel2
description LAG/trunk to einstein switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk ! interface Port-channel3
description "LAG to Edison" switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk ! interface
GigabitEthernet1/0/1 switchport trunk encapsulation
dot1q switchport trunk allowed vlan 5,7,9,10 channel-
group 1 mode passive ! interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,7,9,10 channel-group 1 mode passive !
interface GigabitEthernet1/0/3 switchport trunk
encapsulation dot1q switchport trunk allowed vlan
5,7,9,10 channel-group 1 mode passive ! interface
GigabitEthernet1/0/4 switchport access vlan 7 switchport
mode access ! interface GigabitEthernet1/0/5 switchport
access vlan 5 switchport mode access spanning-tree
portfast ! interface GigabitEthernet1/0/6 switchport
trunk encapsulation dot1q switchport trunk allowed vlan
5,7,9 switchport mode trunk switchport nonegotiate !
interface GigabitEthernet1/0/7 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/8 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
```

```
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/9 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/10 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/11 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/12 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/13 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/14 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/15 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/16 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/17 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/18 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/19 switchport mode access dot1x mac-
auth-bypass dot1x pae authenticator dot1x port-control
auto dot1x timeout quiet-period 10 dot1x timeout reauth-
period 60 dot1x timeout tx-period 10 dot1x timeout supp-
timeout 10 dot1x max-req 1 dot1x reauthentication dot1x
auth-fail max-attempts 1 spanning-tree portfast !
interface GigabitEthernet1/0/20 switchport mode access
dot1x mac-auth-bypass dot1x pae authenticator dot1x
port-control auto dot1x timeout quiet-period 10 dot1x
timeout reauth-period 60 dot1x timeout tx-period 10
dot1x timeout supp-timeout 10 dot1x max-req 1 dot1x
reauthentication dot1x auth-fail max-attempts 1
spanning-tree portfast ! interface GigabitEthernet1/0/21
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/22
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/23
switchport access vlan 10 spanning-tree portfast !
interface GigabitEthernet1/0/24 switchport access vlan
10 spanning-tree portfast ! interface
GigabitEthernet1/0/25 ! interface GigabitEthernet1/0/26
! interface GigabitEthernet1/0/27 ! interface
GigabitEthernet1/0/28 ! interface Vlan1 no ip address
shutdown ! interface Vlan5 ip address 10.1.1.10
255.255.255.0 ! interface Vlan9 ip address 10.9.0.1
255.255.0.0 ! interface Vlan10 ip address 10.10.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! interface Vlan11 ip address 10.11.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! ip default-gateway 10.1.1.1 ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1 ip route 10.30.0.0
255.255.0.0 10.10.0.2 ip route 10.40.0.0 255.255.0.0
10.10.0.2 ip http server ip http secure-server ! ! snmp-
server community public RW snmp-server host 10.1.1.191
public radius-server host 10.10.0.100 auth-port 1645
acct-port 1646 key 7 05090A1A245F5E1B0C0612 radius-
server source-ports 1645-1646 ! control-plane ! ! line
con 0 password 7 02020D550C240E351F1B line vty 0 4
password 7 00001A0803790A125C74 line vty 5 15 password 7
```

```
00001A0803790A125C74 ! end
```

验证

当前没有可用于此配置的验证过程。

相关信息

- Cisco NAC Appliance (Clean Access)
- 思科安全访问控制系统
- 技术支持和文档 - Cisco Systems