

ASA 8.x : 带有 MAC 支持的 AnyConnect SSL VPN CAC 智能卡配置

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[Cisco ASA 配置](#)

[部署注意事项](#)

[认证, 授权, 计费\(AAA\)配置](#)

[配置 LDAP 服务器](#)

[管理证书](#)

[生成密钥](#)

[安装根 CA 证书](#)

[注册 ASA 并安装身份证书](#)

[AnyConnect VPN 配置](#)

[创建 IP 地址池](#)

[创建隧道组和组策略](#)

[隧道组界面和镜像设置](#)

[证书匹配规则 \(如果将使用 OCSP \)](#)

[配置 OCSP](#)

[配置 OCSP Responder 证书](#)

[配置 CA 以使用 OCSP](#)

[配置 OCSP 规则](#)

[Cisco AnyConnect Client 配置](#)

[下载 Cisco Anyconnect VPN 客户端 – Mac OS X](#)

[启动 Cisco AnyConnect VPN 客户端 – Mac OS X](#)

[新建连接](#)

[启动远程访问](#)

[附录 A - LDAP 映射和 DAP](#)

[情形 1 : 使用远程访问权限拨入的 Active Directory 实施 - 允许/拒绝访问](#)

[活动目录设置](#)

[ASA 配置](#)

[方案 2 : 使用组成员的 Active Directory 实施 - 允许/拒绝访问](#)

[活动目录设置](#)

[ASA 配置](#)

[情形 3 : 多个 memberOf 属性的动态访问策略](#)

[ASA 配置](#)

[附录 B - ASA CLI 配置](#)

[附录 C - 故障排除](#)

[AAA 和 LDAP 故障排除](#)

[示例 1：属性映射正确的允许的连接](#)

[示例 2：Cisco 属性映射配置错误的允许的连接](#)

[DAP 故障排除](#)

[示例 1：使用 DAP 允许的连接](#)

[示例 2：使用 DAP 拒绝的连接](#)

[故障排除认证中心/OCSP](#)

[附录 D - 在 MS 中验证 LDAP 对象](#)

[LDAP 查看器](#)

[活动目录服务接口编辑器](#)

[附录 E](#)

[相关信息](#)

[简介](#)

本文在思科可适应安全工具(ASA)提供一配置示例为AnyConnect VPN远程访问为MAC支持普通的访问卡(CAC)为验证。

范围本文是用可适应安全设备管理器(ASDM)，Cisco AnyConnect VPN客户和Microsoft Active Directory (AD) /Lightweight目录访问协议(LDAP)报道思科ASA的配置。

本指南中的配置使用 Microsoft AD/LDAP 服务器。本文也包括高级特性例如OCSP，LDAP属性地图，并且动态访问修正(DAP)。

[先决条件](#)

[要求](#)

思科ASA、思科AnyConnect客户端，Microsoft AD/LDAP和公共密钥基础设施(PKI)基本的了解是有利的在完整设置的领悟。熟悉 AD 组成员、用户属性以及 LDAP 对象有助于了解证书属性和 AD/LDAP 对象的授权过程之间的相互关系。

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- 以后Cisco 5500系列可适应的安全工具(ASA)该运行软件版本8.0(x)和
- ASA的8.x Cisco Adaptive Security Device Manager (ASDM) 6.x版
- 支持 MAC 的 Cisco AnyConnect VPN 客户端 2.2

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](#)。

Cisco ASA 配置

本部分包括通过 ASDM 配置 Cisco ASA 的内容。其中介绍了用于部署使用 SSL AnyConnect 连接的 VPN 远程访问隧道所需的步骤。CAC证书使用验证，并且在证书的用户主体名称(UPN)属性在授权的活动目录填充。

部署注意事项

- 本指南不讨论基本配置内容，例如接口、DNS、NTP、路由、设备访问、ASDM 访问等。假定网络操作员已熟悉这些配置。有关详细信息，请参阅[多功能安全设备](#)。
- 红色突出显示的部分为基本 VPN 访问所必需的配置。例如，VPN通道可以设置CAC卡，无需进行OCSP检查、LDAP映射和动态访问策略(DAP)检查。DoD 需要执行 OCSP 检查，但是隧道无需配置 OCSP 也可工作。
- 蓝色突出显示的部分是可选的高级功能，此功能可以增强设计的安全性。
- ASDM 和 AnyConnect/SSL VPN 不能使用相同接口上的相同端口。建议更改任意一个接口上的端口以便可以进行访问。例如，将端口 445 用于 ASDM，而将 443 用于 AC/SSL VPN。在 8.x 版本中，ASDM URL 访问已发生变化。请使用 `https:// <ip_address>:<port>/admin.html`
- 所需的 ASA 映像的版本至少为 8.0.2.19，并且需要 ASDM 6.0.2。
- AnyConnect/CAC 受 Vista 支持。
- 有关更多策略实施的 LDAP 和动态访问策略映射示例，请参阅[附录 A](#)。
- 有关如何在 MS 中检查 LDAP 对象，请参阅[附录 D](#)。
- 有关用于防火墙配置的应用程序端口列表，请参阅相关信息。

认证，授权，计费(AAA)配置

您验证与使用在他们普通的访问卡(CAC)的证书通过DISACertificate权限(CA)服务器或他们自己的组织CA服务器。证书必须对远程网络访问有效。除验证之外，您必须也授权使用Microsoft Active Directory或轻量级目录访问协议(LDAP)对象。国防部(DoD)要求使用授权的主体名称(UPN)属性，是证书的附属的替代方案名称(SAN)部分的一部分。UPN 或 EDI/PI 必须遵循 1234567890@mil 格式。这些配置显示了如何在 ASA 中通过 LDAP 服务器 (用于授权) 来配置 AAA 服务器。有关通过 LDAP 对象映射进行的其他配置，请参阅[附录 A](#)。

配置 LDAP 服务器

完成这些步骤：

1. 选择 **Remote Access VPN > AAA Setup > AAA Server Group**。
2. 在 AAA 服务器组表中，单击 **Add** 3。
3. 输入服务器组名称，并选择 **LDAP** 协议单选按钮。请参阅图 1。
4. 在所选组表的服务器中，单击 **Add**。确保所创建的服务器在前一张表中处于突出显示状态。
5. 在编辑 AAA 服务器窗口中，执行以下步骤。请参阅图 2。**注意：**如果已针对此类连接配置了 LDAP/AD，请选择 **Enable LDAP over SSL** 选项。选择 LDAP 所处的接口。本指南显示接口内部。输入服务器的 IP 地址。输入 **Server Port**。默认的 LDAP 端口是 389。选择 **Server Type**。输入 **Base DN**。请向 AD/LDAP 管理员咨询这些值。**图-1**在 Scope 选项下，选择适当的答案。这取决于 Base DN。请向 AD/LDAP 管理员寻求帮助。在 Naming Attribute 中，输入 **userPrincipalName**。这是 AD/LDAP 服务器中用于用户授权的属性。在 Login DN 中，输入管理员 DN。**注意：**您具有管理权限，或查看/搜索 LDAP 结构 (包括用户对象和组成员) 的权

限。在 Login Password 中，输入管理员的口令。保留 LDAP 属性的默认设置 **none**。**图-2注意**：在配置过程中，您稍后要使用此选项添加要授权的其他 AD/LDAP 对象。选择 **OK**。

6. 选择 **OK**。

管理证书

要在 ASA 上安装证书，需要执行两个步骤。首先，安装所需的 CA 证书（根证书机构和辅助证书机构）。其次，请向特定的 CA 登记 ASA，并获取身份证书。DoD PKI 使用以下证书：Root CA2、Class 3 Root、ASA 登记所使用的 CA## Intermediate、ASA ID 证书和 OCSP 证书。但是，如果选择不使用 OCSP，则不需要安装 OCSP 证书。

注意：请与您的安全 POC 联系，以获得根证书以及如何为设备登记身份证书的说明。SSL 证书应该能够满足 ASA 进行远程访问。无需双重 SAN 证书。

注意：本地计算机也必须安装 DoD CA 链。可以使用 Internet Explorer 在 Microsoft Certificate Store 中查看证书。DoD 设计了一个批处理文件，它可以自动将所有 CA 添加到计算机中。有关详细信息，请咨询 PKI POC。

注意：用户身份验证只需要以下 CA：DoD CA2、Class 3 Root，以及颁发 ASA 证书的 ASA ID 和中间 CA。当前所有中间 CA 都位于 CA2 和 Class 3 Root 链之下，只要添加了 CA2 和 Class 3 Root，这些中间 CA 都将成为可信 CA。

生成密钥

完成这些步骤：

1. 选择 **Remote Access VPN > Certificate Management > Identity Certificate > Add**。
2. 选择 **Add a new id certificate**，然后选择密钥对选项旁边的 **New**。
3. 在 **Add Key Pair** 窗口中，输入密钥名称 **DOD1024**。单击单选按钮以添加新密钥。请参阅图 3。**图 3**
4. 选择密钥的大小。
5. 保留 Usage 的默认设置 **General Purpose**。
6. 单击 **Generate Now**。**注意**：DoD Root CA 2 使用 2048 位密钥。使用一 2048 个位密钥对的第二密钥应该生成能使用此 CA。完成上一个在步骤上为了添加第二密钥。

安装根 CA 证书

完成这些步骤：

1. 选择 **Remote Access VPN > Certificate Management > CA Certificate > Add**。
2. 选择 **Install from File**，并浏览到相应证书。
3. 选择 **Install Certificate**。**图 4：安装根证书**
4. 应出现以下窗口。请参阅图 5。**图 5注意**：针对要安装的每个证书重复步骤 1 到 3。DoD PKI 要求为下列每一项提供证书：Root CA 2、Class 3 Root、CA## Intermediate、ASA ID 和 OCSP Server。如果不使用 OCSP，则不需要 OCSP 证书。**图 6：安装根证书**

注册 ASA 并安装身份证书

1. 选择 **Remote Access VPN > Certificate Management > Identity Certificate > Add**。
2. 选择 **Add a new id certificate**。
3. 选择 **DoD-1024** 密钥对。请参阅图 7。图 7：身份证书参数
4. 转到 **Certificate subject DN** 框，并单击 **Select**。
5. 在 **Certificate Subject DN** 窗口中，输入设备的信息。有关示例，请参阅图 8。图 8：编辑 DN
6. 选择 **OK**。**注意**：确保在添加主题 DN 时使用的设备主机名已在系统中配置。PKI POC 会告知您哪些字段必须填写。
7. 选择 **Add certificate**。
8. 单击 **Browse**，以选择要保存请求的目录位置。请参阅图 9。图 9 证书请求
9. 使用 Wordpad 打开文件，将请求复制到相应的文档中，并发送给 PKI POC。请参阅图 10。
图 10：注册请求
10. 从 CA 管理员处收到证书之后，请选择 **Remote Access VPN > Certificate Management > ID Certificate > Install**。请参阅图 11。图 11：导入身份证书
11. 在 **Install certificate** 窗口中，浏览到该 ID 证书，并选择 **Install Certificate**。有关示例，请参阅图 12。图 12：安装身份证书**注意**：建议导出 ID 证书信任点，以保存已颁发的证书和密钥对。这样，当出现 RMA 或硬件故障时，ASA 管理员可将证书和密钥对导入到新的 ASA 中。有关详细信息，请参阅[导出和导入信任点](#)。**注意**：单击 **SAVE**，以将配置保存在闪存中。

[AnyConnect VPN 配置](#)

在 ASDM 中，有两种方式可用于配置 VPN 参数。第一种方式是使用 SSL VPN 向导。该工具易于使用，适用于不熟悉 VPN 配置的用户。第二种方式是手动配置每个选项。本配置指南采用手动方式。

注意：用户可以使用两种方法下载 AC 客户端：

1. 从 Cisco 网站上下载客户端，并将其安装到计算机上。
2. 通过 Web 浏览器访问 ASA，然后下载客户端。

注意：例如，<https://asa.test.com>。本指南使用第二种方法。将 AC 客户端永久安装到客户端计算机后，您只需从应用程序中启动 AC 客户端即可。

[创建 IP 地址池](#)

如果您使用其他方法（如 DHCP），则此操作是可选的。

1. 选择 **Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**。
2. 单击 **Add**。
3. 在 **Add IP Pool** 窗口中，输入 IP 池的名称、起始 IP 地址和结束 IP 地址，并选择一个子网掩码。请参阅图 13。图 13：添加 IP 池
4. 选择 **Ok**。
5. 选择 **Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy**。
6. 选择适当的 IP 地址分配方法。本指南使用内部地址池。请参阅图 14。图 14：IP 地址分配方法
7. 单击 **Apply**。

[创建隧道组和组策略](#)

组策略

注意： 如果不想创建新策略，您可使用默认的内置组策略。

1. 选择 **Remote Access VPN -> Network (Client) Access -> Group Policies**。
2. 单击 **Add**，然后选择 **Internal Group Policy**。
3. 在添加内部组制度窗口，请输入名称对于组制度在命名文本框。请参阅图 15。**图 15：添加内部组策略**在 **General** 选项卡上，选择 **SSL VPN Client in the Tunneling Protocols** 选项，除非您使用其他协议（如 **Clientless SSL**）。在 **Servers** 部分中，取消选中 **inherit** 复选框，并输入 **DNS** 和 **WINS** 服务器的 IP 地址。如果适用，输入 **DHCP** 范围。在 **Servers** 部分中，取消选中 **Default Domain** 中的 **inherit** 复选框，并输入适当的域名。在 **General** 选项卡上，取消选中 **Address Pool** 部分中的 **Inherit** 复选框，并添加在上一步创建的地址池。如果您使用另一种 IP 地址分配方法，请保留 **Inherit** 的默认状态，并作相应的更改。所有其他配置选项卡均保留默认设置。**注意：** 最终用户可以使用两种方法下载 **AC** 客户端：一种方法是从 **Cisco.com** 上下载 **AC** 客户端。第二种方法是在用户尝试进行连接时，由 **ASA** 为用户下载客户端。本示例使用后一种方法。
4. 然后，选择 **Advanced > SSL VPN Client > Login Settings**。请参阅图 16。**图 16：添加内部组策略**取消选中 **Inherit** 复选框。选择与您的环境相应的 **Post Login Setting**。选择与您的环境相应的 **Default Post Login Selection**。选择 **OK**。

隧道组界面和镜像设置

注意： 如果不想创建新组，可以使用默认的内置组。

1. 选择 **Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile**。
2. 选择 **Enable Cisco AnyConnect Client.....**。
3. 即会出现一个对话框，询问您 **Would you like to designate an SVC image?**
4. 选择 **Yes**。
5. 如果已存在映像，请通过 **Browse Flash** 选择该映像。如果不存在映像，请选择 **Upload**，并浏览到本地计算机上的文件。请参阅图 17。您可以从 **Cisco.com** 下载这些文件；其中包含一个 **Windows**、**MAC** 和 **Linux** 文件。**图 17：添加 SSL VPN 客户端映像**
6. 然后启用 **Allow Access**、**Require Client Cert**，并根据需要启用 **Enable DTLS**。请参阅图 18。**图 18：启用访问**
7. 单击 **Apply**。
8. 然后，创建一个连接配置文件/隧道组。选择 **Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile**。
9. 在 **Connection Profiles** 部分中，单击 **Add**。**图 19：添加连接配置文件**为该组命名。在身份验证方法中选择 **Certificate**。选择之前创建的组策略。确保启用 **SSL VPN Client**。其他选项保留默认状态。
10. 然后，选择 **Advanced > Authorization**。请参阅图 20。**图 20：授权**选择之前创建的 **AD-LDAP** 组。选中 **Users must exist....to connect**。在映射字段中，分别为主字段和辅字段选择 **UPN** 和 **None**。
11. 选择菜单项 **SSL VPN**。
12. 在 **Connection Aliases** 部分中，执行以下步骤：**图 21：连接别名**选择 **Add**。输入您要使用的组别名。确保选中 **Enabled**。请参阅图 21。
13. 单击 **Ok**。

注意： 单击 **Save**，以将配置保存在闪存中。

[证书匹配规则 \(如果将使用 OCSP \)](#)

1. 选择 **Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps**。请参阅图 22。在 **Certificate to Connection Profile Maps** 部分中，选择 **Add**。在 **Map** 部分中，您可保留已有映射的 **DefaultCertificateMap** 配置，或新建一个映射（如果已将证书映射用于 IPsec）。规则优先级保持默认。在映射组下，保留默认设置--**Not Mapped**--。请参阅图 22。
图 22：添加证书匹配规则单击 Ok。
2. 在底部表上单击 **Add**。
3. 在 **Add certificate Matching Rule Criterion** 窗口中，执行以下步骤：**图 23：证书匹配规则标准** 保留 **Field** 列的默认值 **Subject**。保留 **Component** 列的默认值 **Whole Field**。将 **Operator** 列改为 **Does Not Equal**。在 **Value** 列中，输入两个双引号""。单击 **OK** 和 **Apply**。有关示例，请参阅图 23。

[配置 OCSP](#)

OCSP 的配置可能会有所不同，这取决于 OCSP Responder 供应商。有关详细信息，请参阅供应商手册。

[配置 OCSP Responder 证书](#)

1. 从 OCSP Responder 获取自生成的证书。
2. 执行前述步骤，并为 OSCP 服务器安装证书。**注意：**针对 OCSP 证书信任点，确保选中 **Do not check certificates for revocation**。

[配置 CA 以使用 OCSP](#)

1. 选择 **Remote Access VPN> Certificate Management > CA Certificates**。
2. 突出显示 OCSP，以选择要配置使用 OCSP 的 CA。
3. 单击 **Edit**。
4. 确保选中 **Check certificate for revocation**。
5. 在 **Revocation Methods** 部分中，添加 **OCSP**。请参阅图 24。**OCSP撤销检查**
6. 如果要遵循严格的 OCSP 检查，请确保取消选中 **Consider Certificate valid...cannot be retrieved**。

注意：配置/编辑使用 OCSP 撤销的所有 CA 服务器。

[配置 OCSP 规则](#)

注意：在执行以下步骤之前，请确认已创建证书组匹配策略，且已配置好 OCSP Responder。

注意：在某些 OCSP 实施中，ASA 可能需要 DNS A 和 PTR 记录。此项检查目的在于确认 ASA 来自 .mil 站点。

1. 选择 **Remote Access VPN> Certificate Management > CA Certificates 2**。
2. 突出显示 OCSP，以选择要配置使用 OCSP 的 CA。
3. 选择 **Edit**。
4. 单击 **OCSP Rule** 选项卡。
5. 单击 **Add**。

6. 在 Add OCSP Rule 窗口中，执行以下步骤。请参阅图 25。**图 25：添加 OCSP 规则**在 Certificate Map 选项中，选择 **DefaultCertificateMap** 或之前创建的映射。在 Certificate 选项卡中，选择 **OCSP responder**。在索引选择，请输入 **10**。在 URL 选项中，输入 IP 地址或 OCSP Responder 的主机名。如果使用主机名，请确保已在 ASA 中配置了 DNS 服务器。单击 **Ok**。单击 **Apply**。

[Cisco AnyConnect Client 配置](#)

本部分包括 Cisco AnyConnect VPN 客户端的配置。

假设 — 已在主机 PC 上安装 Cisco AnyConnect VPN 客户端和中间件应用程序。已测试 ActivCard Gold 和 ActivClient。

注意： 本指南使用 group-url 方法，仅用于首次 AC 客户端安装。安装好 AC 客户端后，您可像启动 IPsec 客户端一样启动 AC 应用程序。

注意： 本地计算机上需要安装 DoD 证书链。检查 PKI POC，以获取证书/批处理文件。

注意： 已经安装了用于 MAC OSX 的读卡器驱动程序，并且与您当前使用的操作系统版本兼容。

[下载 Cisco Anyconnect VPN 客户端 – Mac OS X](#)

1. 通过 Safari 启动与 ASA 的 Web 会话。地址格式应为：`https://外部接口`。例如，`https://172.18.120.225`。
2. 即会出现一个弹出窗口，要求您验证 ASA 证书。单击 **Continue**。
3. 即会出现另一个弹出窗口，以解锁 CAC 密钥链。输入您的 pin 码。请参阅图 31。**图 31：输入 PIN**
4. 出现 SSL Vpn 服务网页后，单击 **Continue**。
5. 在解锁密钥链后，浏览器将会提示您是否信任 ASA 的证书。单击 **trust**。
6. 输入根口令以解锁密钥链，并建立安全连接，然后单击 **Ok**。
7. 选择要用于客户端验证的证书，然后单击 **Ok**。
8. 然后浏览器将会请求根/用户口令以允许下载 AnyConnect 客户端。
9. 如果通过验证，则会开始下载 AnyConnect 客户端。请参阅图 32。**图 32：AnyConnect 下载**
10. 下载应用程序后，浏览器将会提示您接受 ASA 证书。单击 **Accept**。
11. 即会建立连接。**图 33: AnyConnect 连接的图**

[启动 Cisco AnyConnect VPN 客户端 – Mac OS X](#)

从 Finder 中 — Applications > Cisco AnyConnect VPN 客户端

注意： 有关可选的 AnyConnect Client 配置文件配置的信息，请参阅附录 E。

[新建连接](#)

出现 AC 窗口。请参阅图 37。

图 37：新建 VPN 连接

1. 如果 AC 未自动进行连接，请选择相应主机。

2. 当出现提示时，输入口令。请参阅图 38。图 38：输入 PIN

启动远程访问

1. 选择要连接的组和主机。
2. 由于使用了证书，请选择 **Connect** 以建立 VPN。请参阅图 39。注意：由于连接使用了证书，因此无需输入用户名和口令。图 39：连接注意：有关可选的 AnyConnect Client 配置文件配置的信息，请参阅附录 E。

附录 A - LDAP 映射和 DAP

在 ASA/PIX 版本 7.1(x) 和更高版本中，引入了一种被称作 LDAP 映射的功能。这项强大的功能提供 Cisco 属性与 LDAP 对象/属性之间的映射，因此无需更改 LDAP 架构。对于 CAC 身份验证实施，该功能可支持对远程访问连接实施其他策略。以下为 LDAP 映射的示例。请注意，如果要在 AD/LDAP 服务器中进行更改，您需要具备管理员权限。在 ASA 8.x 软件方面，动态访问策略 (DAP) 功能介绍。DAP 可结合 CAC，以用于查看多个 AD 组以及推送策略、ACL 等等。

情形 1：使用远程访问权限拨入的 Active Directory 实施 - 允许/拒绝访问

本示例将 AD 属性 msNPAllowDailin 映射到 Cisco 属性 cVPN3000-Tunneling- Protocol。

- AD 属性值：TRUE = 允许；FALSE = 拒绝
- Cisco 属性值：1 = FALSE, 4 (IPSec) 或 20 (4 IPSEC + 16 WebVPN) = TRUE,

对于 ALLOW 情况，进行以下映射：

- TRUE = 20

对于 DENY 拨入情况，进行以下映射：

- FALSE = 1

注意：请确保 TRUE 和 FALSE 均为大写形式。有关详细信息，请参阅[配置外部服务器以便进行安全设备用户授权](#)。

活动目录设置

1. 在 Active Directory 服务器中，单击 **Start > Run**。
2. 在 Open 文本框中，键入 **dsa.msc**，然后单击 Ok。这用来启动活动目录管理控制台。
3. 在 Active Directory 管理控制台中，请单击加号，展开 Active Directory Users and Computers。
4. 单击加号展开域名。
5. 如果已为用户创建 OU，请展开 OU 以查看所有用户；如果已将所有用户分配在 Users 文件夹中，请展开该文件夹以查看所有用户。请参阅图 A1。图 A1：Active Directory 管理控制台
6. 双击要编辑的用户。单击用户属性页中的 Dial-in 选项卡，并单击 **Allow** 或 **Deny**。请参阅图 A2。图 A2：用户属性
7. 然后单击 Ok。

ASA 配置

1. 在 ASDM 中，选择 **Remote Access VPN > AAA Setup > LDAP Attribute Map**。
2. 单击 **Add**。
3. 在 Add LDAP Attribute Map 窗口中，执行以下步骤。请参阅图 A3。**图 A3：添加 LDAP 属性映射**在 Name 文本框中输入名称。在 Map Name 选项卡中，在 Customer Name 文本框中键入 **msNPAllowDialin**。在 Map Name 选项卡中，从 Cisco Name 下拉选项中选择 **Tunneling-Protocols**。单击 **Add**。选择 **Map Value** 选项卡。单击 **Add**。在 Add Attribute LDAP Map Value 窗口中，在 Customer Name 文本框中键入 **TRUE**，并在 Cisco Value 文本框中键入 20。单击 **Add**。在 Customer Name 文本框中键入 **FALSE**，并在 Cisco Value 文本框中键入 1。请参阅图 A4。单击 **Ok**。单击 **Ok**。单击 **Apply**。配置结果如图 A5。**图 A5：LDAP 属性映射配置**
4. 选择 **Remote Access VPN > AAA Setup > AAA Server Groups**。请参阅图 A6。**图 A6：AAA 服务器组**
5. 单击要编辑的服务器组。在 Selected Group 部分的 Servers 中，选择服务器 IP 地址或主机名，然后单击 **Edit**。
6. 在 Edit AAA Server 窗口中的 LDAP Attribute Map 文本框中，从下拉菜单中选择已创建的 LDAP 属性映射。请参阅图 A7。**图 A7：添加 LDAP 属性映射**
7. 单击 **Ok**。

注意：在测试期间请开启 LDAP 调试，以便确认 LDAP 绑定和属性映射是否可以正常工作。有关故障排除命令，请参阅[附录 C](#)。

[方案 2：使用组成员的 Active Directory 实施 - 允许/拒绝访问](#)

本示例使用 LDAP 属性 `memberOf` 映射到 Tunneling Protocol 属性，以便建立作为条件的组成员。为使此策略生效，必须具备以下条件：

- 针对 ALLOW 情况，使用现有组，或是创建一个新组并将 ASA VPN 用户添加到新组中。
- 针对 DENY 情况，使用现有组，或是创建一个新组并将非 ASA 用户添加到新组中。
- 确保在 LDAP 查看器中检查该组是否具备正确的 DN。请参阅[附录 D](#)。如果 DN 错误，映射将无法正常运行。

注意：请注意，在本版本中，ASA 仅可读取 `memberOf` 属性的第一个字符串。确保新创建的组位于列表顶端。或者，在名称前插入一个特殊字符，因为 AD 会首先查看特殊字符。要处理此警告，请在 8.x 软件中使用 DAP 来查看多个组。

注意：确保用户属于某个 DENY 组，或属于至少一个其他组，这样才会始终将 `memberOf` 发送回 ASA。虽然不是必需操作，但建议您指定 FALSE 拒绝条件。如果现有组名称包含空格，请按照以下方式输入属性：

```
CN=Backup Operators,CN=Builtin,DC=gsgseclab,DC=org
```

注意：DAP 允许 ASA 查看 `memberOf` 属性中的多个组。请参阅 DAP 部分。

映射

- AD 属性值：`memberOf CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org`
`memberOf CN=TelnetClients, Cn=users, DC=labrat, Dc=com`
- Cisco 属性值：1 = FALSE, 20 = TRUE,

对于 **ALLOW** 情况，进行以下映射：

- `memberOf CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org= 20`

对于 **DENY** 情况，进行以下映射：

- memberOf CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org = 1

注意：在以后的版本中，将会有有一个用于允许和拒绝连接 Cisco 属性。有关 Cisco 属性的详细信息，请参阅[配置外部服务器以便进行安全设备用户授权](#)。

活动目录设置

1. 在 Active Directory 服务器中，单击 **Start > Run**。
2. 在 Open 文本框中，键入 **dsa.msc**，然后单击 **Ok**。这用来启动活动目录管理控制台。
3. 在 Active Directory 管理控制台中，请单击加号，展开 Active Directory Users and Computers。请参阅图 A8。**图 A8：活动目录组**
4. 单击加号展开域名。
5. 右键单击 **Users** 文件夹，并选择 **New > Group**。
6. 输入组名称。例如：ASAUsers。
7. 单击 **Ok**。
8. 单击 **Users** 文件夹，然后双击刚创建的组。
9. 选择 **Members** 选项卡，然后单击 **Add**。
10. 键入要添加的用户的 Name，然后单击 **Ok**。

ASA 配置

1. 在 ASDM 中，选择 **Remote Access VPN > AAA Setup > LDAP Attribute Map**。
2. 单击 **Add**。
3. 在 Add LDAP Attribute Map 窗口中，执行以下步骤。请参阅图 A3。在 Name 文本框中输入名称。在 Map Name 选项卡中，在 Customer Name 文本框 c 中键入 **memberOf**。在 Map Name 选项卡中，从 Cisco Name 下拉选项中选择 **Tunneling-Protocols**。选择 **Add**。单击 **Map Value** 选项卡。选择 **Add**。在 Add Attribute LDAP Map Value 窗口中，在 Customer Name 文本框中键入 **CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org**，并在 Cisco Value 文本框中键入 20。单击 **Add**。在 Customer Name 文本框中键入 **CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org**，并在 Cisco Value 文本框中键入 1。请参阅图 A4。单击 **Ok**。单击 **Ok**。单击 **Apply**。配置结果如图 A9。**图 A9 LDAP 属性映射**
4. 选择 **Remote Access VPN > AAA Setup > AAA Server Groups**。
5. 单击要编辑的服务器组。在 Selected Group 部分的 Servers 中，选择服务器 IP 地址或主机名，然后单击 **Edit**。
6. 在 Edit AAA Server 窗口中的 LDAP Attribute Map 文本框中，从下拉菜单中选择已创建的 LDAP 属性映射。
7. 单击 **Ok**。

注意：测试期间请开启 LDAP 调试，以便确认 LDAP 绑定和属性映射是否可以正常工作。有关故障排除命令，请参阅[附录 C](#)。

情形 3：多个 memberOf 属性的动态访问策略

本示例使用 DAP 查看多个 memberOf 属性。在 8.x 版本之前，ASA 仅读取第一个 memberOf 属性。在 8.x 版本和更高版本中，ASA 可查看所有 memberOf 属性。

- 针对 ALLOW 情况，使用现有组，或是新建一个组（或多个组）并将 ASA VPN 用户添加到新组中。
- 针对 DENY 情况，使用现有组，或是创建一个新组并将非 ASA 用户添加到新组中。
- 确保在 LDAP 查看器中检查该组是否具备正确的 DN。请参阅[附录 D](#)。如果 DN 错误，映射将

无法正常运行。

ASA 配置

1. 在 ASDM 中，选择 **Remote Access VPN > Network (Client) Access > Dynamic Access Policies**。
2. 单击 **Add**。
3. 在 Add Dynamic Access Policy 中，执行以下步骤：在 Name 文本框 b 中输入名称。在 Priority 部分，输入 1 或者大于 0 的其他数字。在 Selection Criteria 中，单击 **Add**。在 Add AAA Attribute 中，选择 **LDAP**。在 attribute ID 部分中，输入 **memberOf**。在 value 部分中，选择 **=** 并输入 AD 组名。针对要引用的每个组重复此步骤。请参阅图 A10。图 A10 AAA 属性映射单击 **Ok**。在 Access Policy Attributes 部分中，选择 **Continue**。请参阅图 A11。图 A11 添加动态策略
4. 在 ASDM 中，选择 **Remote Access VPN > Network (Client) Access > Dynamic Access Policies**。
5. 选择 **Default Access Policy**，并选择 **Edit**。
6. 默认操作应设为 **Terminate**。请参阅图 A12。图 A12 编辑动态策略
7. 单击 **Ok**。

注意： 如果未选择 **Terminate**，您将无法进入任何组，因为默认值为 **Continue**。

附录 B - ASA CLI 配置

ASA 5510

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname asa80 domain-name army.mil enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
GigabitEthernet0/0 nameif outside security-level 0 ip
address x.x.x.x 255.255.255.128 ! interface
GigabitEthernet0/1 nameif inside security-level 100 no
ip address ! boot system disk0:/asa802-k8.bin ftp mode
passive dns server-group DefaultDNS domain-name army.mil
! -----ACL's-----
----- access-list out extended permit ip any
any -----
----- pager lines 24 logging console
debugging mtu outside 1500 ! -----VPN Pool----
----- ip local pool
CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0 -
-----
----- ! no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-602.bin no asdm
history enable arp timeout 14400 access-group out in
interface outside route outside 0.0.0.0 0.0.0.0
172.18.120.129 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute ! -----
---LDAP Maps & DAP----- ldap
attribute-map memberOf map-name memberOf Tunneling-
Protocols March 11, 2008 ASA - CAC Authentication for
AnyConnect VPN Access Company Confidential. A printed
copy of this document is considered uncontrolled. 49
map-value memberOf
```

```
CN=_ASAUsers,CN=Users,DC=gsgseclab,DC=org 20 ldap
attribute-map msNPAllowDialin map-name msNPAllowDialin
Tunneling-Protocols map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20 dynamic-access-policy-
record CAC-USERS description "Multi-Group Membership
Check" priority 1 dynamic-access-policy-record
DfltAccessPolicy action terminate -----
----- ! -----
-----LDAP Server-----
----- aaa-server AD-LDAP protocol ldap aaa-server AD-
LDAP (outside) host 172.18.120.160 ldap-base-dn
CN=Users,DC=gsgseclab,DC=org ldap-scope onelevel ldap-
naming-attribute userPrincipalName ldap-login-password *
ldap-login-dn
CN=Administrator,CN=Users,DC=gsgseclab,DC=org -----
-----
--- ! aaa authentication http console LOCAL http server
enable 445 http 0.0.0.0 0.0.0.0 outside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart ! -----
-----CA Trustpoints-----
---- crypto ca trustpoint ASDM_TrustPoint0 revocation-
check oosp enrollment terminal keypair DoD-1024 match
certificate DefaultCertificateMap override oosp
trustpoint ASDM_TrustPoint5 10 url http://oosp.disa.mil
crl configure crypto ca trustpoint ASDM_TrustPoint1
revocation-check oosp enrollment terminal fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S.
Government,C=US keypair DoD-1024 match certificate
DefaultCertificateMap override oosp trustpoint
ASDM_TrustPoint5 10 url http://oosp.disa.mil no client-
types crl configure crypto ca trustpoint
ASDM_TrustPoint2 revocation-check oosp enrollment
terminal keypair DoD-2048 match certificate
DefaultCertificateMap override oosp trustpoint
ASDM_TrustPoint5 10 url http://oosp.disa.mil no client-
types crl configure crypto ca trustpoint
ASDM_TrustPoint3 revocation-check oosp none enrollment
terminal crl configure ! -----Certificate
Map----- crypto ca certificate
map DefaultCertificateMap 10 subject-name ne "" -----
-----CA Certificates (Partial Cert is Shown)-----
----- crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37 3082044c 30820334 a0030201 02020137
300d0609 2a864886 f70d0101 05050030 60310b30 09060355
04061302 55533118 30160603 55040a13 0f552e53 2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603 55040b13 03504b49 311b3019 06035504 03131244
6f44204a 49544320 526f6f74 crypto ca certificate chain
ASDM_TrustPoint1 certificate 319e 30820411 3082037a
a0030201 02020231 9e300d06 092a8648 86f70d01 01050500
305c310b 30090603 55040613 02555331 18301606 0355040a
130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355
040b1303 446f4431 0c300a06 0355040b crypto ca
certificate chain ASDM_TrustPoint2 certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
f70d0101 05050030 60310b30 09060355 04061302 55533118
30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74
310c300a 06035504 0b130344 6f44310c 300a0603 55040b13
f766e045 f15ddb43 9549dle9 a0ea6814 b64bcece 089e1b6e
1be959a5 6fc20a76 crypto ca certificate chain
ASDM_TrustPoint3 certificate ca 05 30820370 30820258
a0030201 02020105 300d0609 2a864886 f70d0101 05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13
```

```

0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504
0b130344 6f44310c 300a0603 55040b13 03504b49 31163014
06035504 03130d44 6f442052 6f6f7420 43412032 301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530
3031305a 305b310b 30090603 55040613 02555331 18301606
0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30
0a060355 040b1303 446f4431 0c300a06 0355040b 1303504b
49311630 14060355 0403130d 446f4420 526f6f74 20434120
32308201 crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04 30820267 308201d0 a0030201 02020104
300d0609 2a864886 f70d0101 05050030 61310b30 09060355
04061302 55533118 30160603 55040a13 0f552e53 2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603 55040b13 03504b49 311c301a 06035504 03131344
6f442043 4c415353 20332052 6f6f7420 ! ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtip inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
! -----SSL/WEBVPN-----
----- ssl certificate-authentication
interface outside port 443 webvpn enable outside svc
image disk0:/anyconnect-win-2.0.0343-k9.pkg 1 svc enable
tunnel-group-list enable -----
-----VPN Group/Tunnel Policy----- group-
policy CAC-USERS internal ggroup-policy AC-USERS
internal group-policy AC-USERS attributes vpn-tunnel-
protocol svc address-pools value CAC-USERS webvpn svc
ask none default svc tunnel-group AC-USERS type remote-
access tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP default-group-policy
AC-USERS authorization-required authorization-dn-
attributes UPN tunnel-group AC-USERS webvpn-attributes
authentication certificate group-alias AC-USERS enable
tunnel-group-map enable rules no tunnel-group-map enable
ou no tunnel-group-map enable ike-id no tunnel-group-map
enable peer-ip -----
----- prompt hostname context

```

附录 C - 故障排除

AAA 和 LDAP 故障排除

- debug ldap 255 — 显示 LDAP 交换
- debug aaa common 10 — 显示 AAA 交换

示例 1：属性映射正确的允许的连接

本示例显示在与附录 A 中场景 2 的成功连接期间 debug ldap 和 debug aaa common 的输出。

图 C1：debug LDAP 和 debug aaa common 输出 – 正确的映射

```
AAA API: In aaa_open
```

```
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap://
172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator
to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160,
status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=gsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50...../.....60...*.H.....0@1.0....&....,d
....com1.0.....
&....,d...
[78] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0....&....,d
....com1.0.....
&....,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
```

```
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = .....q.....mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
```



```
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#
```

示例 2 : Cisco 属性映射配置错误的允许的连接

本示例显示在与附录 A 中场景 2 的允许连接期间 `debug ldap` 和 `debug aaa common` 的输出。

图 C2 : debug LDAP 和 debug aaa common 输出 – 不正确的映射

```
AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with
uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator
to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389,
status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
```

```

Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50...../.....60...*.H.....0@1.0.....&....,d
....com1.0.....
&....,d...
[82] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&....,d
....com1.0.....
&....,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = .....q.....mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=or
g
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT

```

```
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

DAP 故障排除

- **debug dap errors** — 显示 DAP 错误
- **debug dap trace** — 显示 DAP 功能跟踪

示例 1：使用 DAP 允许的连接

本示例显示在与附录 A 中所示场景 3 的成功连接期间 **debug dap errors** 和 **debug dap trace** 的输出。请注意多个 **memberOf** 属性。您可同时属于 **_ASAUsers** 和 **Vpnuser** 组，或属于任何一个组，这取决于 ASA 配置。

图 C3：debug DAP

```
#debug dap errors debug dap errors enabled at level 1
#debug dap trace debug dap trace enabled at level 1 #
The DAP policy contains the following attributes for
user: 1241879298@mil -----
----- --- 1: action =
continue DAP_TRACE: DAP_open: C8EEFA10 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.4 = user DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=gsgseclab,DC=org DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated = 20070626163734.0Z DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.uSNCreated = 33691 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2
= _ASAUsers DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.uSNChanged = 53274 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
1241879298 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectGUID = .....F..5.... DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPwdCount = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.codePage = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPasswordTime = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.lastLogoff = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
= 128273494546718750 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.primaryGroupID = 513 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.userParameters = m:
d. DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectSid = .. DAP_TRACE: Username:
1241879298@mil, aaa.ldap.accountExpires =
```

```
9223372036854775807 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.logonCount = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.sAMAccountName = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType = 805306368 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE DAP_TRACE: Username:
1241879298@mil, aaa.cisco.username = 1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user"; DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"]
= "1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"]
= "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["givenName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750"; DAP_TRACE:
```

```

dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains
binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] =
"CACUSERS"; DAP_TRACE:
dap_add_to_lua_tree:endpoint["application"]["clienttype"]
= "IPSec"; DAP_TRACE: Username: 1241879298@mil,
Selected DAPs: CAC-USERS DAP_TRACE: dap_request: memory
usage = 33% DAP_TRACE: dap_process_selected_daps:
selected 1 records DAP_TRACE: Username: 1241879298@mil,
dap_aggregate_attr: rec_count = 1 DAP_TRACE: Username:
1241879298@mil, DAP_close: C8EEFA10 d.

```

示例 2：使用 DAP 拒绝的连接

本示例显示在与附录 A 中所示场景 3 的未成功连接期间 **debug dap errors** 和 **debug dap trace** 的输出。

图 C4：debug DAP

```

#debug dap errors debug dap errors enabled at level 1
#debug dap trace debug dap trace enabled at level 1 #
The DAP policy contains the following attributes for
user: 1241879298@mil -----
----- --- 1: action =
terminate DAP_TRACE: DAP_open: C91154E8 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.4 = user DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=gsgseclab,DC=org DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated = 20070626163734.0Z DAP_TRACE:

```

```
Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.uSNCreated = 33691 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged
= 53274 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.department = NETADMIN DAP_TRACE: Username:
1241879298@mil, aaa.ldap.name = 1241879298 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F..5.... DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userAccountControl = 328192 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
0 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.countryCode = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.badPasswordTime = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
= 0 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.pwdLastSet = 128273494546718750 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userParameters = m: d. DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectSid = .. DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.logonCount = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.sAMAccountName = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType = 805306368 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=or
g DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE DAP_TRACE: Username:
1241879298@mil, aaa.cisco.username = 1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user"; DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"]
= "1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeN
ame"] = "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["givenName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298"; DAP_TRACE:
```

```

dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] =
"DnsAdmins"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains
binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil"; DAP_TRACE: Username: 1241879298@mil,
Selected DAPs: DAP_TRACE: dap_request: memory usage =
33% DAP_TRACE: dap_process_selected_daps: selected 0
records DAP_TRACE: Username: 1241879298@mil,
dap_aggregate_attr: rec_count = 1

```

故障排除认证中心/OCSP

- debug crypto ca 3

- 在配置模式下 — 记录 class ca 控制台 (或缓冲区) 调试

以下示例显示了一次使用 OCSP Responder 成功进行的证书验证，以及一个错误的证书组匹配策略

。

图 C3 显示了具有经过验证的证书和有效的证书组匹配策略的调试输出。

图 C4 显示了一个配置错误的证书组匹配策略的调试输出。

图 C5 显示了具有已撤销证书的用户调试输出。

图 C5 : OCSP 调试 - 成功的证书验证

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint:
ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert
with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap,
index 10 for
WebVPN group map processing. No tunnel group is
configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
```

```
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for
WebVPN group map
```

图 C5 : 失败的证书组匹配策略的输出

图 C5 : 已撤销证书的输出

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,validid cor
=noct
oamuthori,zed.
map rule: subject-name ne ".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence
# 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint
trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org, issuer_name:
cn=gsgseclab,dc=gsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=gsgseclab,dc=org, map rule:
subject-name
ne ".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is
revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

在 Microsoft server 2003 CD 中提供了其他一些可供安装的工具，您可以使用这些工具来查看 LDAP 结构和 LDAP 对象/属性。要安装这些工具，请选择 CD 中的 **Support** 目录，然后选择 Tools。安装 **SUPTOOLS.MSI**。

[LDAP 查看器](#)

- 完成安装后，请选择 **Start > Run**。
- 键入 **ldp**，然后单击 **Ok**。这将启动 LDAP 查看器。
- 选择 **Connection > Connect**。
- 输入服务器名，然后单击 **Ok**。
- 选择 **Connection > Bind**。
- 输入用户名和密码。**注意**：需要拥有管理员权限。
- 单击 **Ok**。
- 查看 LDAP 对象。请参阅图 D1。**图 D1：LDAP 查看器**

[活动目录服务接口编辑器](#)

- 在 Active Directory 服务器中，单击 **Start > Run**。
- 键入 **adsiedit.msc**。这将启动编辑器。
- 右键单击对象，并单击 **Properties**。

此工具将显示特定对象的所有属性。请参阅图 D2。

图 D2：ADSI 编辑

[附录 E](#)

您可以创建一个 AnyConnect 配置文件，并将其添加到工作站。此配置文件可引用各种值（如 ASA 主机）或证书匹配参数（如识别名或颁发者）。此配置文件将存储为 .xml 文件，且可通过 Notepad 进行编辑。您可手动将该文件添加到每个客户端，或者通过组策略将其从 ASA 中推入客户端。文件存储在：

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco  
AnyConnect VPN Client\Profile
```

完成这些步骤：

1. 选择 AnyConnectProfile.tmpl，并使用 Notepad 打开该文件。
2. 对该文件进行相应修改，如修改颁发者或主机 IP。有关示例，请参阅图 F1。
3. 完成后，以 .xml 格式保存文件。

这是 Cisco AnyConnect VPN 客户端配置文件 XML 文件的一个示例。

有关配置文件管理，请参阅 Cisco AnyConnect 文档。简而言之：

- 配置文件名称必须是与您的公司相应的唯一名称。例如：CiscoProfile.xml
- 此配置文件名称必须相同，尽管公司内部的各个组之间可以使用不同的配置文件名称。

此文件由 Secure Gateway 管理员维护，并通过客户端软件分发。基于此 XML 的配置文件可随时分发到各客户端。支持的分发机制有：随软件捆绑分发，或作为自动下载机制的一部分。自动下载机制仅适用于某些 Cisco Secure 网关产品。

注意：强烈建议管理员通过在线验证工具或 ASDM 中的配置文件导入功能，对所创建的 XML 配置文件进行验证。可借助本目录中的 AnyConnectProfile.xsd 完成验证。AnyConnectProfile 是代表

AnyConnect 客户端配置文件的根元素。

```
xml version="1.0" encoding="UTF-8" - -
<AnyConnectProfile
xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd"> !-- The ClientInitialization
section represents global settings !-- for the client.
In some cases, for example, BackupServerList, host
specific !-- overrides are possible. !-- --> -
<ClientInitialization> !-- The Start Before Logon
feature can be used to activate !-- the VPN as part of
the logon sequence. !-- UserControllable: Does the
administrator of this profile allow the user !-- to
control this attribute for their own use. Any user
setting !-- associated with this attribute is stored
elsewhere. --> <UseStartBeforeLogon
UserControllable="false">>false</UseStartBeforeLogon> !--
- This control enables an administrator to have a one
time !-- message displayed prior to a users first
connection attempt. As an !-- example, the message can
be used to remind a user to insert their smart !-- card
into its reader. !-- The message to be used with this
control is localizable and can be !-- found in the
AnyConnect message catalog. !-- (default: "This is a
pre-connect reminder message.")
<ShowPreConnectMessage>>false</ShowPreConnectMessage> !--
This section enables the definition of various
attributes !-- that can be used to refine client
certificate selection. --> - <CertificateMatch> !--
Certificate Distinguished Name matching allows for exact
!-- match criteria in the choosing of acceptable client
!-- certificates. - <DistinguishedName> -
<DistinguishedNameDefinition Operator="Equal"
Wildcard="Disabled"> <Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition> </DistinguishedName>
</CertificateMatch> </ClientInitialization> - !-- This
section contains the list of hosts from which !-- the
user is able to select. - <ServerList> !-- This is the
data needed to attempt a connection to a specific !--
host. --> - <HostEntry> <HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress> </HostEntry>
- <HostEntry> <HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress> </HostEntry>
</ServerList> </AnyConnectProfile>
```

[相关信息](#)

- [X.509 和 RFC 3280 指定的证书和 CRL](#)
- [RFC 2560 指定的 OCSP](#)
- [Public Key Infrastructure 简介](#)
- [“草案标准”描出的轻量级OCSP](#)
- [RFC 2246指定的SSL/TLS](#)
- [技术支持和文档 - Cisco Systems](#)