思科 ISE 2.x 与 Active Directory 的集成

Revised: 2020 年 6 月 17 日

思科 ISE 2.x 中的 Active Directory 配置

思科 ISE 2.x 中的 Active Directory 主要功能

以下是思科 ISE 2.x 中 Active Directory 的一些主要功能：

多加入支持

思科 ISE 支持对 Active Directory 域执行多加入。思科 ISE 最多支持 50 个 Active Directory 加入。思科 ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。Active Directory 多域加入包括一组不同的 Active Directory 域，每个加入均有其自己的组、属性和授权策略。

身份验证域

思科 ISE 在加入 Active Directory 域时会自动发现加入点的受信任域。然而，并非所有域都可与思科 ISE 相关联以执行身份验证和授权。思科 ISE 允许您从受信任域中选择部分域来执行身份验证和授权。此部分域称为身份验证域。建议您将计划执行身份验证的用户或机器所在的域定义为身份验证域。定义身份验证域可阻止一些域并限制在这些域中进行用户身份验证，从而提高安全性。它还有助于优化性能，因为您可以跳过与策略和身份验证无关的域，并帮助思科 ISE 更高效地执行身份搜索操作。

身份重写

此功能可让思科 ISE 修改从客户端或证书接收到的用户名，再将其发送给 Active Directory 进行身份验证。例如，用户名 jdoe@amer.acme.com 可以重写为 jdoe@acme.com。使用此功能，您可以修复用户名或主机名，否则身份验证会失败。

您还可以重写证书和进程请求中的身份，这些进程请求在未正确调配证书时出现。相同的身份重写规则适用于传入的用户名或机器名称，无论这些名称是来自非基于证书的身份验证还是来自证书内部。

模糊身份解析

如果思科 ISE 接收的用户或机器名称模糊，即不是唯一的，则在用户尝试进行身份验证时会导致问题。如果用户没有域标记，或者多个域中的多个身份有相同的用户名，就会发生身份冲突。例如，userA 存在于 domain1 上，另一个 userA 存在于 domain2 上。您可以使用身份解析设置来定义此类用户解析的范围。思科强烈建议您使用限定名，例如 UPN 或 NetBIOS。限定名可以降低模糊可能性，并通过减少延迟来提高性能。

基于安全标识符的组成员身份评估

ISE 使用安全标识符 (SID) 来优化组成员身份评估。SID 的作用体现在两个方面：第一，评估组时可提升效率（速度）；第二，在域关闭而用户为该域的组成员时，灵活应对延迟。当删除组并创建同名的新组作为原始组时，必须更新 SID 以将新 SID 分配给新创建的组。

基于用户名的身份验证测试（测试用户）

测试身份验证有助于对最终用户的身份验证和授权问题进行故障排除。您可以使用测试用户功能测试 Active Directory 身份验证。测试会在返回结果的同时返回组和属性详细信息（授权信息），可在管理门户上查看这些结果和信息。

诊断工具

诊断工具可用于自动测试和诊断 Active Directory 部署的一般连接性问题。此工具提供以下方面的相关信息：

- 运行测试的思科 ISE 节点
- 与 Active Directory 的连接
- 有关域的详细状态
- 有关思科 ISE-DNS 服务器连接的详细状态

工具为您运行的每项测试提供详细的报告。

证书身份验证配置文件增强功能

- 证书中的任何主题或备选名称属性（仅限 Active Directory）选项 - 您可以使用此选项，将 Active Directory UPN 作为用户名用于日志，并尝试使用证书中的所有主题名称和备选名称来查找用户。只有选择 Active Directory 作为身份源时，此选项才可用。
- 仅用于解决身份模糊选项 - 您可以使用此选项解决 EAP-TLS 身份验证中的身份问题。TLS 证书中可有多个身份。如果用户名模糊，例如合并后存在两个“jdoe”，并且客户端证书存在于 Active Directory 中，则思科 ISE 可使用二进制比较来排除模糊。

节点视图

您可以使用此页面查看在思科ISE 部署中每个节点上加入点的状态。节点视图为只读页面，仅提供状态。此页面不支持任何加入、退出或测试选项。但是，它提供每个加入点到主加入点页面的链接，可从该页面执行上述操作。此页面还显示最终诊断状态和诊断工具链接。

报告和警报

思科 ISE 在控制面板中提供新 AD 连接器操作报告和新警报，用于对 Active Directory 相关活动进行监控和故障排除。

高级调整

高级调整功能提供特定节点的更改和设置，以更深入地调整系统中的参数。此页面允许配置首选的 DC、GC、DC 故障切换参数和超时。此页面还提供类似禁用加密的故障排除选项。这些设置不适用于正常管理流程，只应在思科支持人员指导下使用。

将 Active Directory 与思科 集成的先决条件

本节介绍配置 Active Directory 以与思科 集成所需的手动步骤。但是，在大多数情况下，可以启用思科 来自动配置 Active Directory。以下是将 Active Directory 与思科 集成的先决条件。

- 确保您在 ISE 中具有超级管理员或系统管理员权限。
- 使用网络时间协议 (NTP) 服务器设置来同步思科 服务器和 Active Directory 之间的时间。您可以从思科 CLI 配置 NTP 设置。

- 思科 ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。如果要从特定加入点查询其他域，请确保加入点和其他具有需要访问的用户和计算机信息的域之间存在信任关系。如果信任关系不存在，您必须为不受信任的域创建另一个加入点。有关建立信任关系的详细信息，请参阅 Microsoft Active Directory 文档。
- 您必须在思科 加入到的域中具有至少一个可由思科 运行并访问的全局目录服务器。

执行各种操作所需的 Active Directory 帐户权限

加入操作	退出操作	思科 机器账户
对于用于执行加入操作的帐户，需要以下权限： • 搜索 Active Directory（以查看思科 机器账户是否已存在） • 将思科 机器账户创建到域（如果机器账户尚不存在） • 在新机器账户上设置属性（例如，思科 机器账户密码、SPN、dnsHostname）	对于用于执行退出操作的帐户，需要以下权限： • 搜索 Active Directory（以查看思科 机器账户是否已存在） • 从域中删除思科 机器账户 如果执行强制退出（在没有密码的情况下退出），则不会从域中删除计算机帐户。	对于新创建的用于传达到 Active Directory 连接的思科 机器账户，需要以下权限： • 能够更改自己的密码 • 读取与的用户/机器对应的用户/机器对象 • 查询 Active Directory 的某些部分以了解所需信息（例如，受信任域和替代 UPN 后缀等等。） • 能够读取 tokenGroups 属性 您可以在 Active Directory 中预先创建机器账户，如果 SAM 名称与思科 设备主机名匹配，则应在加入操作期间找到该名称并重复使用。 如果执行多个加入操作，则会在思科 中维护多个机器账户，每个加入操作对应一个账户。

注释 用于加入或退出操作的凭证不存储在思科 中。仅存储新创建的思科 机器账户凭证，这是为了使终端探测器也能够运行。

必须开放用于通信的网络端口

协议	端口（远程-本地）	目标	已通过身份验证	备注
DNS (TCP/UDP)	随机数大于或等于 49152	DNS 服务器/AD 域控制器	否	-
MSRPC	445	域控制器	是	-

协议	端口（远程-本地）	目标	已通过身份验证	备注
Kerberos (TCP/UDP)	88	域控制器	是 (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	域控制器	是	-
LDAP (GC)	3268	全局目录服务器	是	-
NTP	123	NTP 服务器/域控制器	否	-
IPC	80	部署中的其他 ISE 节点	是（使用 RBAC 凭证）	-

DNS 服务器

在配置您的 DNS 服务器时，请确保注意以下事项：

- 您在思科 ISE 中配置的 DNS 服务器必须能够解析要使用的域的所有正向和反向 DNS 查询。
- 建议使用权威 DNS 服务器来解析 Active Directory 记录，因为 DNS 递归可能会导致延迟并对性能造成重大不利影响。
- 所有 DNS 服务器都必须能够对 DC、GC 和 KDC（无论它们是否具有额外的站点信息）的 SRV 查询作出应答。
- 思科建议向 SRV 响应添加服务器 IP 地址以提高性能。
- 避免使用查询公共互联网的 DNS 服务器。当必须解析未知名称时，这些服务器可能会泄漏有关网络的信息。

添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点

开始之前

确保思科 ISE 节点可以与 NTP 服务器、DNS 服务器、域控制器和全局目录服务器所在的网络进行通信。您可以通过运行域诊断工具来检查这些参数。

必须创建加入点才能使用 Active Directory 以及使用被动 ID 工作中心的代理、系统日志、SPAN 和终端探测器。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击**添加**并从 Active Directory“加入点名称设置”输入域名和身份库名称。

步骤 3 点击**提交 (Submit)**。

此时将出现弹出窗口，询问您是否要将新创建的加入点加入到域中。如果要立即加入，请点击 **Yes**。

如果已点击**否**，则保存配置将会全局保存 Active Directory 域配置（在主策略服务节点和辅助策略服务节点中），但不会将任何 ISE 节点加入到该域。

步骤 4 选中所创建的新 Active Directory 加入点旁边的复选框并点击**编辑**，或者从左侧的导航窗格中点击新的 Active Directory 加入点。系统将显示部署加入/退出表，其中包含所有思科 ISE 节点、节点角色及其状态。

步骤 5 选中相关思科 ISE 节点旁边的复选框，然后点击**加入**将思科 ISE 节点加入到 Active Directory 域。

您必须明确地执行此操作，即使已保存配置。要通过单个操作将多个思科 ISE 节点加入到域，所要使用的账户的用户名和密码必须对于所有加入操作都相同。如果需要不同的用户名和密码以加入每个思科 ISE 节点，则应对每个思科 ISE 节点分别执行加入操作。

步骤 6 从打开的**加入域**对话框输入 Active Directory 用户名和密码。

强烈建议您选择**存储凭证**，在此情况下将会保存管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。

用于加入操作的用户本身应存在于域中。如果该用户存在于其他域中或子域中，应使用 UPN 符号注解用户名，如 jdoe@acme.com。

步骤 7 （可选） 选中**指定组织单位**复选框。

如果思科 ISE 节点机器账户要位于除 CN=Computers,DC=someDomain,DC=someTLD 以外的特定组织单位中，应选中此复选框。思科 ISE 会在指定的组织单位下创建机器账户，如果该机器账户已存在，则会将该账户移至此位置。如果未指定组织单位，思科 ISE 将使用默认位置。应以完整可分辨名称 (DN) 格式指定值。语法必须符合 Microsoft 规范。特殊保留字符，例如 /'+,;=<> 换行符、空格和回车符，必须用反斜线 (\) 转义。例如，OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ 和 Workstations,DC=someDomain,DC=someTLD。如果已创建机器账户，则无需选中此复选框。加入 Active Directory 域之后，您还可以更改计算机帐户的位置。

步骤 8 点击**确定 (OK)**。

您可以选择多个要加入 Active Directory 域的节点。

如果加入操作不成功，则系统会显示失败消息。点击每个节点的失败消息可查看该节点的详细日志。

注释 加入完成后，思科 ISE 将更新其 AD 组和对应的 SID。思科 ISE 自动启动 SID 更新过程。您必须确保允许此过程完成。

注释 如果缺少 DNS SRV 记录，您可能无法将思科 ISE 加入 Active Directory 域（域控制器不会对您尝试加入到的域公告其 SRV 记录）。请参阅以下 Microsoft Active Directory 文档，以获取故障排除信息：

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

下一步做什么

配置 Active Directory 用户组 ， 第 8 页

配置身份验证域。

退出 Active Directory 域

如果不再需要从此 Active Directory 域或从此加入点对用户或机器进行身份验证，则可以退出 Active Directory 域。

从命令行界面重置思科 ISE 应用配置或在备份或升级后恢复配置时，它将执行退出操作，从而将思科 ISE 节点与 Active Directory 域断开连接（如果已加入该节点）。但是，不会从 Active Directory 域中删除思科 ISE 节点账户。我们建议您使用 Active Directory 凭证从 Admin 门户执行退出操作，因为这也会从 Active Directory 域删除节点帐户。在更改思科 ISE 主机名时，也建议您如此操作。

开始之前

如果您退出 Active Directory 域，但是仍然使用 Active Directory 作为身份验证的身份源（直接使用或作为身份源序列的一部分），则身份验证会失败。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑**。系统将显示部署加入/退出表，其中包含所有思科 ISE 节点、节点角色及其状态。

步骤 3 选中思科 ISE 节点旁边的复选框，然后点击**退出**。

步骤 4 输入 Active Directory 用户名和密码，然后点击**确定**以退出该域并从思科 ISE 数据库中删除机器账户。

如果输入 Active Directory 凭证，则思科 ISE 节点将退出 Active Directory 域并从 Active Directory 数据库中删除思科 ISE 机器账户。

注释 要从 Active Directory 数据库中删除思科 ISE 机器账户，此处提供的 Active Directory 凭证必须具有从域中删除机器账户的权限。

步骤 5 如果您没有 Active Directory 凭证，请选中**无可用凭证**复选框，然后点击**确定**。

如果选中**退出没有凭证的域**复选框，则主思科 ISE 节点将退出 Active Directory 域。Active Directory 管理员必须手动删除加入期间在 Active Directory 中创建的设备帐户。

配置身份验证域

对于与其有信任关系的其他域，思科ISE加入的域具有可视性。默认情况下，思科ISE设置为允许依据所有可信任域进行身份验证。可以将与 Active Directory 部署的交互限制到身份验证域子集。通过配置身份验证域，可以为每个加入点选择特定域，以便仅对选择的域执行身份验证。身份验证域可以提高安全性，因为这些域指示思科ISE仅对来自所选域（而不是来自加入点信任的所有域）的用户进行身份验证。身份验证域还可改善性能以及身份验证请求处理延迟，因为身份验证域限制搜索区域（即，将搜索帐户与传入用户名或身份匹配的范围）。这在传入用户名或身份不包含域标记（前缀或后缀）时尤为重要。由于上述原因，配置身份验证域是最佳实践，我们强烈推荐此最佳实践。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击 **Authentication Domains** 选项卡。

系统会显示一个表，其中包含受信任域列表。默认情况下，思科 ISE 允许对所有受信任域执行身份验证。

步骤 3 要仅允许指定域，请取消选中 **Use all Active Directory domains for authentication** 复选框。

步骤 4 选中想要允许对其执行身份验证的域旁边的复选框，并点击 **Enable Selected**。在 **Authenticate** 列中，此域的状态会更改为 Yes。

还可以禁用选定的域。

步骤 5 点击 **Show Unusable Domains** 以查看无法使用的域的列表。无法使用的域是思科 ISE 由于单向信任、选择性身份验证等原因而无法用于身份验证的域。

下一步做什么

配置 Active Directory 用户组。

支持的组类型

思科 ISE 支持以下安全组类型：

- 通用
- 全局
- 内置

  内置组没有跨域的唯一安全标识符 (SID)。为解决此问题，思科 ISE 为其 SID 添加它们所属的域名作为前缀。

思科 ISE 使用 AD 属性 tokenGroups 评估用户的组成员身份。思科 ISE 机器帐户必须具有读取 tokenGroups 属性的权限。此属性可以包含用户可能是其成员的大约前 1015 个组（实际数量取决于 Active Directory 配置，并可通过重新配置 Active Directory 来增加数量）。如果用户所属的组多于此数量，则思科 ISE 在策略规则中使用的组不会超过前 1015 个。

配置 Active Directory 用户组

您必须配置 Active Directory 用户组，使其可以用于授权策略中。在内部，思科 ISE 使用安全标识符 (SID) 帮助解决组名称不明确问题和增强组映射。SID 提供准确的组分配匹配。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击 **Groups** 选项卡。

步骤 3 执行以下操作之一：

a) 依次选择 **Add** > **Select Groups From Directory** 以选择现有组。

b) 依次选择**添加** > **添加组**以手动添加组。您可以同时提供组名称和 SID，也可以仅提供组名称并按 **Fetch SID**。

对于用户界面登录，请勿在组名称中使用双引号 (”)。

步骤 4 如果您手动选择组，您可以使用过滤器进行搜索。例如，输入 **admin*** 作为搜索条件，然后点击 **Retrieve Groups**，即可查看以 admin 开头的用户组。您还可以输入星号 (*) 通配符过滤结果。一次只能检索 500 个组。

步骤 5 选中想要可用于授权策略的组旁边的复选框，然后点击 **OK**。

步骤 6 如果您选择手动添加组，请为新组输入名称和 SID。

步骤 7 点击**确定**。

步骤 8 点击**保存**。

注释 如果删除某个组，然后创建一个与此组相同名称的新组，则必须点击 **Update SID Values** 以向新创建的组分配新 SID。升级之后，SID 会在首次联接之后自动更新。

下一步做什么

配置 Active Directory 用户属性。

配置 Active Directory 用户和计算机属性

必须配置 Active Directory 用户和计算机属性，以便在授权策略的条件中使用这些属性。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击 **Attributes** 选项卡。

步骤 3 依次选择**添加** > **添加属性**以手动添加属性，或者依次选择**添加** > **从目录中选择属性**以从目录中选择属性列表。

步骤 4 如果选择从目录添加属性，请在**示例用户或机器账户**字段中输入用户的名称，然后点击**检索属性**以获取用户属性的列表。例如，输入 **administrator** 以获取管理员属性列表。您还可以输入星号 (*) 通配符过滤结果。

注释 当输入示例用户名时，确保从思科 ISE 连接到的 Active Directory 域选择用户。当您选择示例计算机获得计算机属性时，请务必在计算机名称前面加上“host/”或使用 SAM$ 格式。例如，可以使用 host/myhost。检索属性时显示的示例值仅用于说明，不能存储。

步骤 5 选中想要选择的 Active Directory 的属性旁边的复选框，并且点击 **OK**。

步骤 6 如果选择手动添加属性，请输入新属性的名称。

步骤 7 点击**保存**。

对用户进行 Active Directory 身份验证测试

“测试用户”工具可用于从 Active Directory 验证用户身份验证。您还可以获取组和属性并对其进行检查。您可以对单个加入点或对范围运行测试。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 选择以下选项之一：

- 要对所有加入点运行测试，请依次选择 **Advanced Tools** > **Test User for All Join Points**。
- 要对特定加入点运行测试，请选择该加入点并点击 **Edit**。选择思科 ISE 节点并点击**测试用户**。

步骤 3 在 Active Directory 中输入用户（或主机）的用户名和密码。

步骤 4 选择身份验证类型。如果选择查找 (Lookup) 选项，则无需步骤 3 中的密码输入。

步骤 5 如果您是对所有加入点运行此测试，请选择要对其运行此测试的思科 ISE 节点。

步骤 6 如果要从 Active Directory 检索组和属性，请选中“检索组”和“检索属性”复选框。

步骤 7 点击 **Test**。

系统将显示测试操作的结果和步骤。这些步骤可帮助确定故障原因并进行故障排除。

对 Active Directory 多加入配置的支持

思科 ISE 支持对 Active Directory 域执行多加入。思科 ISE 最多支持 50 个 Active Directory 加入。思科 ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。Active Directory 多域加入包括一组不同的 Active Directory 域，每个加入均有其自己的组、属性和授权策略。

您可以多次联接同一个域林，也即是说，如有必要，您可以在同一个域林中联接不止一个域。

思科ISE现在允许联接具有单向信任的域。此选项有助于绕过单向信任导致的权限问题。您可以联接以下任一受信任域，因此能够看见这两个域。

- 加入点 - 在思科 ISE 中，每个到 Active Directory 域的独立加入都叫作一个加入点。Active Directory 加入点是思科 ISE 身份库，可用于身份验证策略。它有用于属性和组的关联字典，这些属性和组可用于授权条件。
- 范围 - 一部分 Active Directory 加入点组合到一起就叫做范围。您可以在身份验证策略中使用范围代替单个加入点并用作身份验证结果。范围用于按照多个加入点对用户进行身份验证。如果您使用范围，就无需为每个加入点设置多个规则，可以创建只有单个策略的相同策略，节约了思科ISE用于处理请求的时间并且有助于提高性能。一个加入点可以用于多个范围中。范围可以包含在身份源序列中。因为范围不具有任何关联字典，所以您无法将范围用于授权策略条件中。

  当您执行思科ISE全新安装时，默认情况下并无范围。这称为无范围模式。当您添加范围时，思科ISE进入多范围模式。如果需要，您可以返回无范围模式。所有加入点将移至 Active Directory 文件夹。

  - Initial_Scope 是用于存储在无范围模式中添加的 Active Directory 加入点的隐式范围。当启用多范围模式时，所有 Active Directory 加入点将移至自动创建的 Initial_Scope。您可以重命名 Initial_Scope。
  - All_AD_Instances 是在 Active Directory 配置中不显示的一个内置伪范围。它只在策略和身份序列中作为身份验证结果显示。如果您要选择思科 ISE 中配置的所有 Active Directory 加入点，就可以选择此范围。

身份源序列和身份验证策略中的范围和加入点

通过思科 ISE，您可以定义多个 Active Directory 加入点，其中每个加入点表示与不同 Active Directory 域的连接。每个加入点可作为单独的身份库用于身份验证和授权策略以及身份序列中。加入点可分组以构成一个范围，您可以将该范围作为身份验证结果用于身份验证策略以及身份源序列中。

当您要将每个加入点视为完全独立的策略组时，可以选择各个加入点作为身份验证策略或身份源序列的结果。例如，在多租户方案中（其中思科 ISE 部署支持含有其自己的网络设备的独立组），网络设备组可用于选择 Active Directory 域。

但是，如果 Active Directory 域被视为同一企业的一部分，并且域之间没有任何信任，则可以使用范围来加入多个断开连接的 Active Directory 域，并创建通用身份验证策略。这样，就无需在身份验证策略中定义由不同身份库表示的每个加入点，也无需为每个域提供重复规则。所使用的实际加入点包含在身份验证身份库中，以供在授权策略中使用。

当多个域中有多个身份且用户名相同时，会出现身份模糊情况。例如，如果没有任何域标记的用户名不是唯一的，并且思科 ISE 配置为使用无密码协议（例如 EAP-TLS），则没有其他条件可用来找到正确的用户，因此，思科 ISE 会由于模糊身份错误而无法执行身份验证。如果您遇到此类模糊身份，可以使用身份验证策略规则中的特定范围或加入点，或者使用身份源序列。例如，您可以指导特定网络设备组的用户使用特定 Active Directory 范围甚至单个加入点，以限制搜索范围。同样，您也可以创建如下规则：如果身份以 @some.domain 结尾，则使用特定 Active Directory 加入点。这有助于将身份验证定向到正确的加入点。

创建新范围，添加 Active Directory 加入点

过程

步骤 1 依次选择 **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**。

步骤 2 点击 **Scope Mode**。
默认情况下，系统创建名为 Initial_Scope 的范围，当前所有加入点都放在此范围中。

步骤 3 要创建更多范围，请点击 **Add**。

步骤 4 输入新范围的名称和说明。

步骤 5 单击**提交**。

只读域控制器

在只读域控制器上支持以下操作：

- Kerberos 用户身份验证
- 用户查找
- 属性和组获取

支持 Active Directory 的身份验证协议和功能

Active Directory 支持使用某些协议对用户和设备进行身份验证、更改 Active Directory 用户密码等功能。下表列出了 Active Directory 支持的身份验证协议及相应功能。

表 *1: Active Directory* 支持的身份验证协议

身份验证协议	功能
EAP-FAST 和基于密码的受保护的可扩展身份验证协议 (PEAP)	用户和设备身份验证，能够使用 EAP-FAST 和 PEAP 结合 MS-CHAPv2 和 EAP-GTC 的内部方法更改密码
密码身份验证协议 (PAP)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)	用户和设备身份验证
可扩展身份验证协议 - 通用令牌卡 (EAP-GTC)	用户和设备身份验证
可扩展身份验证协议 - 传输层安全 (EAP-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
可扩展身份验证协议 - 通过安全隧道的灵活身份验证-传输层安全 (EAP-FAST-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
受保护的可扩展身份验证协议 - 传输层安全 (PEAP-TLS)	• 用户和设备身份验证 • 组和属性检索 • 二进制证书比较
轻型可扩展身份验证协议 (LEAP)	用户身份验证

Active Directory 用户身份验证流程

当对用户进行身份验证或查询时，思科 ISE 会检查以下内容：

- MS-CHAP 和 PAP 身份验证会检查用户是否被禁用、锁定、过期或者登录超时，如果上述条件为真，则身份验证失败。
- EAP-TLS 身份验证会检查用户是否被禁用或锁定，如果满足上述某些条件，则身份验证失败。

支持的用户名格式

以下是支持的用户名类型：

- SAM，例如：jdoe
- 以 NetBIOS 为前缀的 SAM，例如：ACME\jdoe
- UPN，例如：jdoe@acme.com
- 备选 UPN，例如：john.doe@acme.co.uk
- 子树，例如：johndoe@finance.acme.com
- SAM 机器，例如：laptop$
- 以 NetBIOS 为前缀的机器，例如：ACME\laptop$
- FQDN DNS 机器，例如：host/laptop.acme.com
- 仅主机名的机器，例如：host/laptop

Active Directory 基于密码的身份验证

密码身份验证协议 (PAP) 和 Microsoft 质询握手身份验证协议 (MS-CHAP) 是基于密码的协议。MS-CHAP 凭证只能通过 MS-RPC 进行身份验证。思科 ISE 为 PAP 身份验证提供两个选项 - MS-RPC 和 Kerberos。MS-RPC 和 Kerberos 是同等安全的选项。用于 PAP 身份验证的 MS-RPC 是默认和建议选项，原因如下：

- 它提供与 MS-CHAP 的一致性
- 它提供更清楚的错误报告
- 它允许与 Active Directory 进行更高效的通信。如果使用 MS-RPC，思科 ISE 会将身份验证请求发送到仅来自加入域的域控制器，并且该域控制器会处理请求。

如果使用 Kerberos，思科 ISE 需要遵循从加入域到用户账户域的 Kerberos 推荐（即，思科 ISE 需要与信任路径上从加入域到用户账户域的所有域进行通信）。

思科 ISE 会检查用户名格式并调用域管理器来找到适当的连接。找到账户域的域控制器之后，思科 ISE 尝试根据它来对用户进行身份验证。如果密码匹配，则授予用户对网络的访问权限。

基于密码的机器身份验证与基于用户的身份验证非常类似，不同之处在于机器名称采用主机/前缀格式。思科 ISE 无法按原样对此格式（即 DNS 名称空间）执行身份验证，在执行身份验证之前，该格式会转换为以 NetBIOS 为前缀的 SAM 格式。

基于证书的身份验证的 Active Directory 证书检索

思科 ISE 支持为使用 EAP-TLS 协议的用户和设备身份验证检索证书。Active Directory 上的用户或设备记录包括二进制数据类型的证书属性。此证书属性可以包含一个或多个证书。思科 ISE 将此属性标识为 userCertificate，并且不允许为此属性配置任何其他名称。思科 ISE 会检索此证书并将其用于执行二进制比较。

证书身份验证配置文件决定从哪个字段（例如 Subject Alternative Name (SAN) 或 Common Name 字段）获取用户名以在 Active Directory 中查找用于检索证书的用户。思科 ISE 检索到证书后，会将此证书与客户端证书进行二进制比较。当接收到多个证书时，思科 ISE 会对这些证书进行比较以确定相匹配的证书。找到匹配的证书后，则用户或设备身份验证通过。

添加证书身份验证配置文件

您必须创建证书验证配置文件，如果您想要使用可扩展身份验证协议 - 传输层安全 (EAP-TLS) 基于证书的身份验证方法，即必须创建证书身份验证配置文件。思科 ISE 不是通过传统的用户名与密码方法进行身份验证，而是将从客户端接收的证书与服务器中的证书进行比较，从而验证用户的身份。

开始之前

您必须是超级管理员或系统管理员。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **证书身份验证配置文件** > **添加**。

步骤 2 为证书身份验证配置文件输入名称和可选说明。

步骤 3 从下拉列表中选择身份库。

基本证书检查不需要使用身份源。如果希望对证书进行二进制比较，就必须选择身份源。如果您选择 Active Directory 作为身份源，使用者和通用名称以及使用者替代名称（所有值）都可用于查找用户。

步骤 4 从**证书属性**或**证书中的任何主体或备选名称属性**中选择身份的使用。此身份将用于日志以及查找。

如果选择**证书中的任何主体或备选名称属性**，则 Active Directory UPN 将用作日志的用户名，并将尝试使用证书中的所有主体名称和备选名称来查找用户。只有选择 Active Directory 作为身份源时，此选项才可用。

步骤 5 如果您想要将客户端证书与身份库中的证书进行匹配，请选择 **Match Client Certificate Against Certificate In Identity Store**。为此，您必须选择身份源（LDAP 或 Active Directory）。如果您选择 Active Directory，您可以选择仅为解决身份不明情况而匹配证书。

- Never - 此选项从不执行二进制比较。
- Only to resolve identity ambiguity - 此选项仅在遇到身份不明情况时，才将客户端证书与 Active Directory 中帐户的证书进行二进制比较。例如，系统发现若干个 Active Directory 帐户与证书中的身份名称匹配，就属于身份不明情况。
- Always perform binary comparison - 此选项始终将客户端证书与身份库（Active Directory 或 LDAP）中帐户的证书进行比较。

步骤 6 点击 **Submit** 以添加证书身份验证配置文件或保存更改。

修改密码更改、设备身份验证和设备访问限制设置

开始之前

您必须将思科 ISE 加入到 Active Directory 域。有关详细信息，请参阅添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点，第 5 页。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 选中相关思科 ISE 节点旁边的复选框，然后点击**编辑**。.

步骤 3 点击 **Advanced Settings** 选项卡。

步骤 4 根据需要，修改 Password Change、Machine Authentication 和 Machine Access Restrictions (MAR) 设置。

默认情况下，已启用这些选项。

步骤 5 如果您想要使用 Kerberos 进行纯文本身份验证，请选中 **Use Kerberos for Plain Text Authentications** 复选框。默认和推荐选项为 MS-RPC。ISE 1.2 中使用的是 Kerberos。

根据 Active Directory 实例进行授权

以下各节介绍思科 ISE 用于根据 Active Directory 对用户或机器进行授权的机制。

用于授权策略的 Active Directory 属性和组检索

思科 ISE 从 Active Directory 检索用户或设备属性和组以用于授权策略规则。这些属性可用于思科 ISE 策略并且决定了用户或设备的授权级别。思科 ISE 在身份验证成功后会检索用户和设备 Active Directory 属性，还可以为与身份验证无关的授权检索属性。

思科ISE可以使用外部身份库中的组来为用户或计算机分配权限；例如，将用户映射到发起人组。请注意 Active Directory 中的以下组成员身份限制：

- 策略规则条件可引用以下任意组：用户或计算机的主要组、用户或计算机作为直接成员的组，或者间接（嵌套）组。
- 不支持在用户或计算机的帐户域外的域本地组。

注释 您可以使用 Active Directory 属性 (msRadiusFramedIPAddress) 的值作为 IP 地址。可将此 IP 地址发送给授权配置文件中的网络接入服务器 (NAS)。msRADIUSFramedIPAddress 属性仅支持 IPv4 地址。在进行用户身份验证时，为用户获取的 msRadiusFramedIPAddress 属性值将转换为 IP 地址格式。

系统按加入点检索和管理属性和组。这些属性和组将用于授权策略（方法是首先选择加入点，然后选择属性）。您无法按范围为授权定义属性或组，但可以对身份验证策略使用范围。当您在身份验证策略中使用范围时，可以通过一个加入点对

用户进行身份验证，但要通过另一个具有用户帐户域信任路径的加入点检索属性和/或组。您可以使用身份验证域来确保一个范围中的任两个加入点在身份验证域中都没有任何重叠。

注释 请参阅 Microsoft 对可用 Active Directory 组的最大数量限制： http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

如果规则包含带有特殊字符（例如 /、!、@、\、#、$、%、^、&、*、(、)、_、+ 或 ~）的 Active Directory 组名称，则授权策略会失败。

支持 Boolean 属性

思科 ISE 支持从 Active Directory 和 LDAP 身份库中检索 Boolean 属性。

在配置 Active Directory 或 LDAP 的目录属性时，您可以配置 Boolean 属性。一旦使用 Active Directory 或 LDAP 进行身份验证，即可检索这些属性。

Boolean 属性可用于配置策略规则条件。

可从 Active Directory 或 LDAP 服务器抓取作为字符串类型的 Boolean 属性值。思科 ISE支持以下 Boolean 属性值：

Boolean 属性	支持的值
真	t、T、true、TRUE、True、1
错误	f、F、false、FALSE、False、0

注释 Boolean 属性不支持属性替代。

如果您将 Boolean 属性（例如 msTSAllowLogon）配置为字符串类型，则 Active Directory 或 LDAP 服务器中该属性的 Boolean 值是为思科 ISE 中字符串属性设置的。您可以将属性类型更改为 Boolean 或将该属性作为 Boolean 类型进行手动添加。

授权策略字典属性

授权策略由条件根据字典属性确定。每个 Active Directory 加入点都具有包含属性和组的关联字典。

字典	属性	说明
网络接入	AD-User-Join-Point	此属性指示哪个加入点用于用户身份验证。
网络接入	AD-Host-Join-Point	此属性指示哪个加入点用于机器身份验证。
网络接入	AD-User-DNS-Domain	此属性指示哪个域 DNS 限定名用于用户身份验证。

字典	属性	说明
网络接入	AD-Host-DNS-Domain	此属性指示哪个域 DNS 限定名用于机器身份验证。
网络接入	MachineAuthenticationIdentityStore	此属性指示哪个身份库用于机器身份验证。
网络接入	WasMachineAuthenticated	此属性指示是否已对用户的机器执行身份验证。
加入点	ExternalGroups	此属性指示用户所属的 Active Directory 组。
加入点	IdentityAccessRestricted	此属性指示用户账户已禁用或登录超时，因此禁止授予访问权限。
加入点	<ATTR name>	此属性指示用户的 Active Directory 属性。

身份重写

身份重写是一种定向思科 ISE 的高级功能，使其在传递至外部 Active Directory 系统之前处理其身份。您可以创建规则以将身份改为包含或排除域前缀和/或后缀或您所选择的其他附加标记的相应格式。

身份重写规则应用于传递至 Active Directory 之前从客户端接收的用于使用者搜索、身份验证和授权查询等操作的用户名或主机名。思科 ISE 将匹配条件标记，在发现第一个匹配项时，思科 ISE 停止处理策略并根据结果重写身份字符串。

在重写期间，以方括号" [] "括起来的所有内容（例如 [IDENTITY]）是变量，在评估端不会对其进行评估，但会添加与字符串中该位置匹配的字符串。没有方括号的所有内容在规则的评估端和重写端都会评估为固定字符串。

以下是身份重写的一些示例，假设用户输入的身份是 ACME\jdoe：

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **[IDENTITY]**。

  结果是 jdoe。此规则指示思科 ISE 删掉所有用户名的 ACME 前缀。

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@ACME.com**。

  结果是 jdoe@ACME.com。此规则指示思科 ISE 将格式从前缀更改为后缀表示法，或从 NetBIOS 格式更改为 UPN 格式。

- 如果身份与 **ACME\[IDENTITY]** 匹配，则重写为 **ACME2\[IDENTITY]**。

  结果是 ACME2\jdoe。此规则指示思科 ISE 将具有特定前缀的所有用户名更改为使用备用前缀。

- 如果身份与 **[ACME]\jdoe.USA** 匹配，则重写为 **[IDENTITY]@[ACME].com**。

  结果是 jdoe\ACME.com。此规则指示思科 ISE 删掉点后面的领域（在本例中是国家/地区），替换为正确的领域。

- 如果身份与 **E=[IDENTITY]** 匹配，则重写为 **[IDENTITY]**。

结果是 jdoe。如果身份来自证书，字段是邮件地址，而且 Active Directory 配置为按使用者搜索，则可以创建此示例规则。此规则指示思科 ISE 删除“E=”。

- 如果身份与 **E=[EMAIL],[DN]** 匹配，则重写为 **[DN]**。

  此规则会将证书使用者从 E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com 转变为纯 DN, CN=jdoe, DC=acme, DC=com。如果身份取自证书使用者，且 Active Directory 配置为按 DN 搜索用户，则可以创建此示例规则。此规则指示思科 ISE 删掉邮件前缀并生成 DN。

以下是编写身份重写规则的一些常见错误：

- 如果身份与 **[DOMAIN]\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@DOMAIN.com**。

  结果是 jdoe@DOMAIN.com。此规则在规则的重写端没有用方括号 [] 括起来的 [DOMAIN]。

- 如果身份与 **DOMAIN\[IDENTITY]** 匹配，则重写为 **[IDENTITY]@[DOMAIN].com**。

  同样，结果是 jdoe@DOMAIN.com。此规则在规则的评估端没有用方括号 [] 括起来的 [DOMAIN]。

身份重写规则始终应用在 Active Directory 加入点的情景中。即使由于身份验证策略而选择了范围，重写规则也适用于每个 Active Directory 加入点。如果使用的是 EAP-TLS，这些重写规则还适用于取自证书的身份。

启用身份重写

注释 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

开始之前

您必须将思科 ISE 加入到 Active Directory 域。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击 **Advanced Settings** 选项卡。

步骤 3 在 **Identity Rewrite** 部分下，选择是否要应用重写规则来修改用户名。

步骤 4 输入匹配条件和重写结果。您可以删除出现的默认规则并根据要求输入规则。思科 ISE 按顺序处理规则，并会应用与请求用户名相匹配的第一个条件。您可以使用匹配令牌（方括号中包含的文本）将原始用户名的元素传输到结果。如果无任何规则匹配，则身份名称保持不变。您可以点击 **Launch Test** 按钮预览重写处理。

身份解析设置

某些身份类型包括域标记，如前缀或后缀。例如，在如 ACME\jdoe 这样的 NetBIOS 身份中，“ACME”是域标记前缀，同样在如 jdoe@acme.com 这样的 UPN 身份中，“acme.com”是域标记后缀。域前缀应该与组织中 Active Directory 域的

NetBIOS (NTLM) 名称匹配，域后缀应该与组织中 Active Directory 域的 DNS 名称或备选 UPN 后缀匹配。例如，jdoe@gmail.com 会视为没有域标记，因为 gmail.com 不是 Active Directory 域的 DNS 名称。

身份解析设置允许您配置重要设置来调整安全和性能的平衡，以符合您的 Active Directory 部署。您可以使用这些设置来调整没有域标记的用户名和主机名的身份验证。在思科 ISE 不知道用户域的情况下，可以将其配置为在所有身份验证域中搜索用户。即使在一个域中找到了用户，思科 ISE 仍将等待所有响应以确保不存在模糊身份。这可能需要较长时间，具体取决于域的数量、网络中的延迟、负载等。

避免身份解析问题

强烈建议在身份验证期间，使用完全限定的用户和主机名称（即，带有域标记的名称）。例如，用户使用 UPN 和 NetBIOS 名称，主机使用 FQDN SPN 名称。这在您频繁遇到模糊错误的情况下尤其重要，例如，多个 Active Directory 帐户匹配传入用户名；例如，jdoe m 匹配 jdoe@emea.acme.com 和 jdoe@amer.acme.com。在某些情况下，使用完全限定名称是解决问题的唯一方法。在其他情况下，保证用户拥有唯一密码即可。因此，如果最初使用唯一身份，则更加高效，而且可以减少密码锁定问题。

配置身份解析设置

注释 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

开始之前

您必须将思科 ISE 加入到 Active Directory 域。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击 **Advanced Settings** 选项卡。

步骤 3 在 **Identity Resolution**（身份解析）部分下，对用户名或计算机名称的身份解析定义以下设置。此设置可提供用于用户搜索和身份验证的高级控制。

第一个设置适用于没有标记的身份。在这种情况下，可以选择以下任一选项：

- **Reject the request** - 此选项将导致没有任何域标记的用户（例如 SAM 名称）的身份验证失败。如果有多个加入域，而思科 ISE 必须在所有加入的全局目录中查找身份（这可能不太安全），则此选项非常有用。此选项强制用户使用具有域标记的名称。
- **Only search in the “Authentication Domains” from the joined forest** - 此选项只在加入点所在林的域（这些域在身份验证域部分中指定）中搜索身份。对于 SAM 帐户名称，这是默认选项，并且与思科 ISE 1.2 的行为相同。
- **Search in all the “Authentication Domains” sections** - 此选项在所有受信任林的所有身份验证域中搜索身份。这可能会增加延迟并影响性能。

根据身份验证域在思科 ISE 中的配置方式来选择选项。如果只选择特定身份验证域，将只搜索这些域（无论是选择“加入的林”还是“所有林”）。

如果思科 ISE 无法与它所需的所有全局目录 (GC) 通信，则使用第二个设置，以符合在“Authentication Domains”部分中指定的配置。在这种情况下，可以选择以下任一选项：

- **Proceed with available domains** - 如果在任一可用的域中找到匹配项，此选项将继续执行身份验证。
- **Drop the request**- 如果身份解析遇到某些无法访问或不可用的域，此选项将删除身份验证请求。

示例方案

本节介绍一些与思科 ISE 的 Active Directory 配置流程相关的基本方案。

企业收购

场景

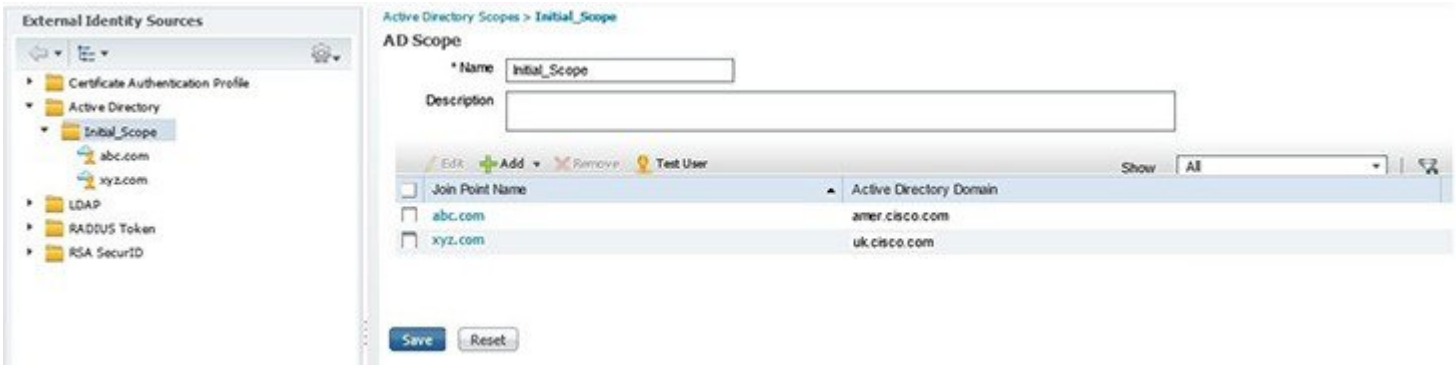
企业 abc.com 已收购或合并企业 xyz.com。作为 abc.com 的管理员，您希望统一网络身份验证基础设施，使 abc.com 和 xyz.com 的用户都能访问同一物理网络。

必需配置

已配置 abc.com 的单一 Active Directory 加入点。要添加其他不受信任 Active Directory 基础设施，请执行以下操作：

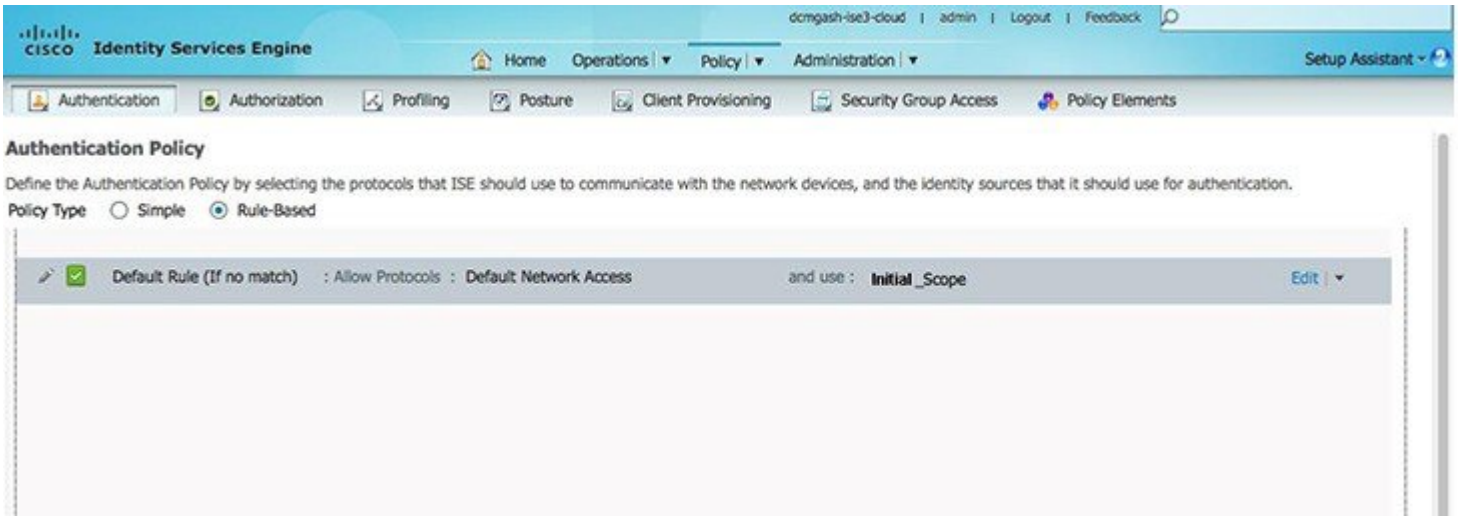
1. 进入范围模式以添加 Initial_Scope。
2. 为 xyz.com 添加新加入点。

图 *1:* 在 ***Initial_Scope*** 内创建的加入点



3. 配置身份验证策略并选择 Initial_Scope 作为所有身份验证的结果。

图 *2:* 选择作为身份验证策略中的结果的 ***Initial_Scope***



通过执行上述配置，您创建了一个范围，该范围将思科 ISE 配置为在任一公司的 Active Directory 中搜索用户。范围允许网络根据多个 Active Directory 基础设施执行身份验证，即使它们完全断开连接和/或相互不信任也如此。

多租户

场景

对于多租户方案，您必须定义多个客户的配置：CompanyA、CompanyB 和 CompanyC。对于每个客户，必须执行以下操作：

- 定义独立网络设备组。
- 定义身份流量可以高效扫描的范围。
- 配置并加入独立 Active Directory 加入点。
- 定义身份验证和授权策略，以便将来自这些设备组的 Active Directory 身份流量定向到这些 Active Directory 加入点。

必需配置

要提供以上所需的所有功能，请执行以下操作：

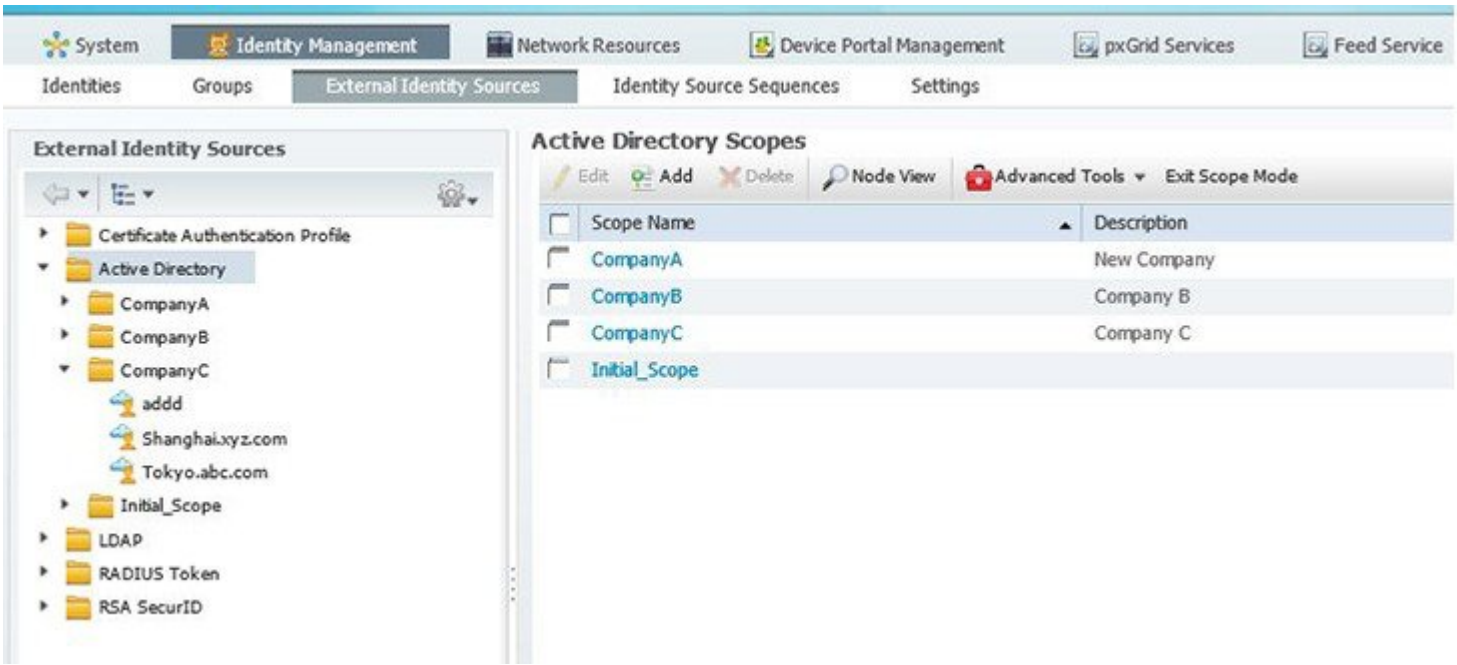
1. 将网络设备组 (NDG) 类型定义为 CompanyA、CompanyB 和 CompanyC，并为每个公司添加网络设备。

图 *3:* 定义每个公司的网络设备组

2. 定义每个公司的范围。在每个公司的范围内定义多个 Active Directory 加入点。

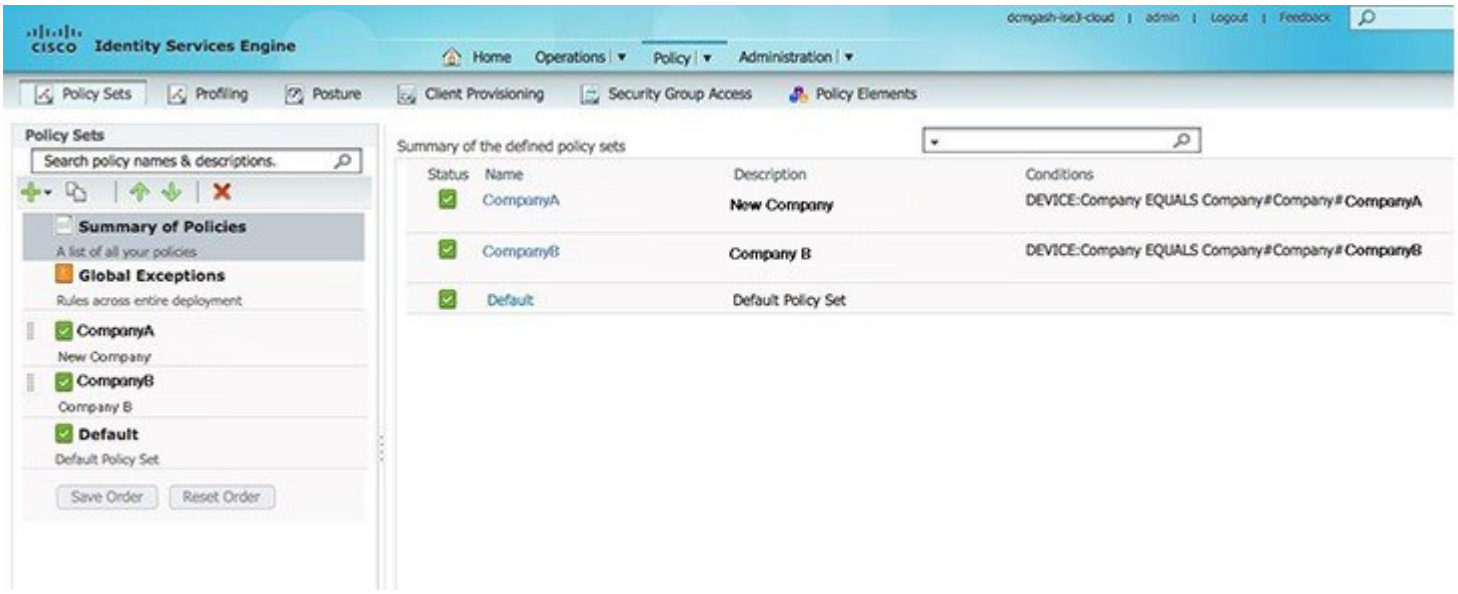
   如果所有公司的域都受信任，则只需要单个加入点。但在此示例中有多个不受信任的域，因此需要多个加入点。

图 *4:* 定义每个公司的范围和加入点



3. 配置策略集，以将公司的 NDG 与 Active Directory 范围绑定在一起，从而对公司执行身份验证。每个公司还应具有自己的策略，以便可在公司自己的策略组中定义授权策略。

图 *5:* 配置策略集



故障排除工具

思科 ISE 提供多种工具来对 Active Directory 错误进行诊断和故障排除。

诊断 Active Directory 问题

诊断工具是在每个思科 ISE 节点上运行的服务。当思科 ISE 使用 Active Directory 时，通过该工具可自动测试和诊断 Active Directory 部署并执行一组测试，以检测可能导致功能或性能故障的问题。

思科 ISE 无法加入 Active Directory 或对其进行身份验证有多个原因。此工具帮助确保正确配置用于将思科 ISE 连接到 Active Directory 的先决条件。该工具有助于检测网络、防火墙配置、时钟同步、用户身份验证等问题。此工具以逐步操作指南的形式工作，并帮助您根据需要解决中间每层的问题。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击**高级工具 (Advanced Tools)** 下拉列表，选择**诊断工具 (Diagnostic Tools)**。

步骤 3 选择要运行诊断的思科 ISE 节点。

如果未选择思科 ISE 节点，则在所有节点上运行测试。

步骤 4 选择特定的 Active Directory 加入点。

如果不选择 Active Directory 加入点，则在所有加入点上运行测试。

步骤 5 点击**在所有节点上运行测试 (Run All Tests on Node)** 开始测试。

步骤 6 点击 **View Test Details** 查看具有警告或失败状态的测试的详细信息。

下表允许您重新运行特定测试、停止正在运行的测试和查看特定测试的报告。

Active Directory 警报和报告

思科 ISE 提供多种警报和报告，用于对 Active Directory 相关活动进行监控和故障排除。

警报

Active Directory 错误和故障会触发以下警报：

- 配置的名称服务器不可用
- 所加入的域不可用
- 身份验证域不可用
- Active Directory 林不可用
- AD 连接器必须重新启动
- AD：ISE 帐户密码更新失败
- AD：计算机 TGT 刷新失败

报告

您可以通过以下两种报告监控 Active Directory 相关活动：

- RADIUS Authentications Report - 此报告显示 Active Directory 身份验证和授权的详细步骤。您可以在以下位置找到此报告：**Operations** > **Reports** > **Auth Services Status** > **RADIUS Authentications**。
- AD Connector Operations Report - AD 连接器操作报告提供 AD 连接器所执行后台操作的日志，例如思科 ISE 服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理。如果遇到 Active Directory 失败，您可以查看此报告的详细信息以确定可能的原因。您可以在以下位置找到此报告：**Operations** > **Reports** > **Auth Services Status** > **AD Connector Operations**。

查找模糊身份错误

一个林中可能存在具有相同名称的多个身份。在多加入情况下更可能发生此问题，特别是在 Active Directory 域中有多个对其用户名没有相互控制权的非相关公司时。使用 SAM 名称也会增加名称冲突的可能性。甚至，每个林的 NetBIOS 前缀也不是唯一的。UPN 能正常工作，但备用 UPN 可能发生冲突。所有此类情况都将产生模糊身份错误。

您可以使用 **Operations** 选项卡下的 **Authentications** 页查找以下属性。如果您遇到模糊身份错误，这些属性可帮助您了解和控制实际使用的身份。

- AD-Candidate-Identities - 只要一发现模糊身份，此属性便会显示找到的身份。它可用于确定身份模糊的原因。
- AD-Resolved-Identities - 找到身份并在身份验证、获取组和获取属性之类的操作中使用身份后，此属性将使用找到的身份进行更新。在身份冲突情况下，可能有多个此类身份。

- AD-Resolved-Providers - 此属性提供找到的身份所在的 Active Directory 加入点。

查看节点的 Active Directory 加入

您可以使用 **Active Directory** 页面上的**节点视图**按钮查看给定思科 ISE 节点的所有 Active Directory 加入点的状态或所有思科 ISE 节点上的所有加入点列表。

过程

步骤 1 依次选择**管理** > **身份管理** > **外部身份源** > **Active Directory**。

步骤 2 点击 **Node View**。

步骤 3 从 **ISE Node** 下拉列表中选择节点。
表格按节点列出 Active Directory 的状态。如果部署中有多个加入点和多个思科 ISE 节点，则更新此表可能需要几分钟时间。

步骤 4 点击加入点 **Name** 链接以转至该 Active Directory 加入点页面，然后执行其他特定操作。

步骤 5 点击**诊断摘要**列中的链接以转至**诊断工具**页面来对特定问题进行故障排除。诊断工具显示每个节点的每个加入点的最新诊断结果。

启用 Active Directory 调试日志

默认情况下，不会记录 Active Directory 调试日志。必须在您的部署中承担策略服务角色的思科 ISE 节点上启用此选项。启用 Active Directory 调试日志可能会影响 ISE 性能。

过程

步骤 1 依次选择**管理** > **系统** > **日志记录** > **调试日志配置**。

步骤 2 点击要从中获取 Active Directory 调试信息的思科 ISE 策略服务节点旁边的单选按钮，然后点击**编辑**。

步骤 3 点击 **Active Directory** 单选按钮，然后点击**编辑**。

步骤 4 从 Active Directory 旁的下拉列表中选择 **DEBUG**。这将包括错误、警告和 verbose 日志。要获得完整日志，请选择 **TRACE**。

步骤 5 点击**保存**。

获取 Active Directory 日志文件来进行故障排除

下载并查看 Active Directory 调试日志，对您可能遇到的问题进行故障排除。

开始之前

必须启用 Active Directory 调试日志记录。

过程

步骤 1 依次选择**操作** > **故障排除** > **下载日志**。

步骤 2 点击您要从其获得 Active Directory 调试日志文件的节点。

步骤 3 点击 **Debug Logs** 选项卡。

步骤 4 向下滚动此页面找到 ad_agent.log 文件。点击该文件并下载该文件。

Active Directory 高级调整

高级调整功能提供节点特定的设置，用于在思科支持人员指导下的支持操作，更深入地调整系统中的参数。这些设置不适用于正常管理流程，只应在指导下使用。

AD 连接器内部操作

以下各节介绍 AD 连接器中发生的内部操作。

域发现算法

思科 ISE 分三个阶段执行域发现：

1. 查询加入域 - 发现加入域林中的域和加入域外部信任的域。
2. 查询林中的根域 - 建立与林的信任。
3. 查询受信任林中的根域 - 发现受信任林中的域。

此外，思科 ISE 会发现 DNS 域名（UPN 后缀）、备选 UPN 后缀和 NTLM 域名。

默认域发现频率为每两小时一次。您可以从“高级调整”页面修改该值，但必须仅在咨询思科支持人员的情况下才能修改。

DC 发现

AD 连接器为给定的域选择域控制器 (DC)，如下所示：

1. 执行 DNS SRV 查询（不将范围限制为某个站点），以获取域中的域控制器的完整列表。
2. 对缺少 IP 地址的 DNS SRV 执行 DNS 解析。
3. 根据 SRV 记录中的优先级将 CLDAP ping 请求发送到域控制器，并仅处理第一个响应（如果有）。CLDAP 响应包含 DC 站点和客户端站点（例如，分配了思科 ISE 机器的站点）。
4. 如果 DC 站点和客户端站点相同，则会选择响应发起方（即 DC）。
5. 如果 DC 站点和客户端站点不同，则 AD 连接器会执行将范围限制为已发现的客户端站点的 DNS SRV 查询，获取服务于客户端站点的域控制器的列表，将 CLDAP ping 请求发送到这些域控制器，并仅处理第一个响应（如果有）。系

统会选择响应发起方（即 DC）。如果客户端站点中没有服务于站点的 DC，或者站点中没有当前可用的 DC，则选择在步骤 2 中检测到的 DC。

您可以通过创建和使用 Active Directory 站点来影响思科 ISE 使用的域控制器。有关如何创建和使用站点的信息，请参阅 Microsoft Active Directory 文档。

思科 ISE 还能够定义每个域的首选 DC 的列表。在 DNS SRV 查询之前会优先选择此 DC 列表。但是，此首选 DC 列表不是独占列表。如果首选 DC 不可用，则会选择其他 DC。您可在以下情况下创建首选 DC 列表：

- SRV 记录损坏、丢失或者未配置。
- 站点关联错误或丢失，或者站点无法使用。
- DNS 配置错误或无法编辑。

DC 故障切换

以下条件可触发域控制器 (DC) 故障切换：

- AD 连接器检测当前选定的 DC 在 LDAP、RPC 或 Kerberos 通信尝试期间是否变为不可用。DC 可能由于关闭或没有网络连接而不可用。在此类情况下，AD 连接器会启动 DC 选择并故障切换到新选择的 DC。
- DC 启动并对 CLDAP ping 作出响应，但由于某种原因（例如 RPC 端口阻塞、DC 处于中断复制状态或 DC 尚未正确停用），AD 连接器无法与其通信。在此类情况下，AD 连接器会使用黑名单启动 DC 选择（“错误”DC 将列入黑名单）并尝试与所选 DC 进行通信。使用黑名单选择的 DC 与黑名单都不会进行缓存。

ISE 机器密码更改

可以在 **Active Directory 高级调整**页面中配置加入到 Active Directory 的 ISE 机器中的密码更改间隔。默认值为 2592000 秒（30 天），有效值范围为 30 分钟到 60 天。

可以根据 AD GPC 设置的密码策略来配置的最小值为 1 天。

ISE 将在配置该值之前执行机器密码更改。例如，如果已配置的值为 86400 秒（1 天），则每 12 小时将需要更改一次密码。

注释 此设置适用于 2.2 补丁 8 及更高版本。

DNS 故障切换

您最多可以配置三个 DNS 服务器和一个域后缀。如果您在思科 ISE 中使用 Active Directory 身份库序列，则必须确保所有 DNS 服务器都可对要使用的任何可能的 Active Directory DNS 域的正向和反向 DNS 查询作出应答。仅当第一个 DNS 关闭时，才会发生 DNS 故障切换，并且故障切换 DNS 应具有与第一个 DNS 相同的记录器。如果 DNS 服务器无法解析查询，则 DNS 客户端不会尝试其他 DNS 服务器。默认情况下，DNS 服务器会重试查询两次，并且 3 秒后查询超时。

解析身份算法

对于身份，将根据身份类型、是否提供了密码以及身份中是否存在域标记来使用不同算法查找用户或机器对象。以下是思科 ISE 用于解析不同身份类型的不同算法。

注释 如果已根据所配置的身份重写规则来重写身份，则会对已重写的身份应用身份解析。

解析 SAM 名称

- 如果身份是 SAM 名称（没有任何域标记的用户名或机器名称），则思科 ISE 会搜索每个加入点的森林（执行一次）以查找身份。如果存在唯一匹配项，则思科 ISE 会确定其域或唯一名称，并继续执行 AAA 流程。
- 如果 SAM 名称不唯一，并且思科 ISE 配置为使用无密码协议（如 EAP-TLS），则没有其他条件可用于查找正确的用户，因此，思科 ISE 会由于“模糊身份”错误而无法执行身份验证。但是，如果用户证书存在于 Active Directory 中，则思科 ISE 会使用二进制比较来解析身份。
- 如果思科 ISE 配置为使用基于密码的协议（如 PAP 或 MSCHAP），则思科 ISE 会继续检查密码。如果存在唯一匹配项，则思科 ISE 会继续执行 AAA 流程。但是，如果有多个密码相同的账户，则思科 ISE 会由于“模糊身份”错误而无法执行身份验证。

应避免用户名冲突。这不仅会提高效率和安全性，还可防止账户锁定。例如，存在两个使用不同密码的“chris”，而思科 ISE 仅接收 SAM 名称“chris”。在此情况下，思科 ISE 会持续使用 SAM 名称“chris”尝试这两个账户，然后再决定正确的账户。在此类情况下，Active Directory 可能会由于不正确的密码尝试而锁定其中一个账户。因此，应尝试使用唯一用户名或具有域标记的用户名。或者，如果为每个 Active Directory 域使用特定网络设备，则可以使用身份重写来限定 SAM 名称。

解析 UPN

- 如果身份是 UPN，则思科 ISE 会搜索每个森林的全局目录以查找该 UPN 身份的匹配项。如果存在唯一匹配项，则思科 ISE 会继续执行 AAA 流程。如果有多个 UPN 相同的加入点，并且未提供密码或者凭密码无法确定正确的账户，则思科 ISE 会由于“模糊身份”错误而无法执行身份验证。
- 思科 ISE 还允许显示为 UPN 的身份同时匹配用户的邮件属性，即，它会搜索“身份=匹配的 UPN 或邮件”。某些用户使用其邮件名称（通常通过证书）而不是实际的基础 UPN 进行登录。如果身份类似于邮件地址，则会隐式完成此操作。

解析机器身份

- 如果是机器身份验证，其中身份具有主机/前缀，则思科 ISE 会搜索森林来查找匹配的 servicePrincipalName 属性。如果在身份中指定了完全限定域后缀（例如 host/machine.domain.com），则思科 ISE 会搜索该域所在的森林。如果身份的形式为主机/机器，则思科 ISE 会搜索服务主体名称的所有森林。如果存在多个匹配项，则思科 ISE 会由于“模糊身份”错误而无法执行身份验证。
- 如果机器采用另一个身份格式（例如 machine@domain.com、ACME\laptop$ 或 laptop$），则思科 ISE 使用普通 UPN、NetBIOS 或 SAM 解析算法。

解析 NetBIOS 身份

如果身份具有 NetBIOS 域前缀（例如 ACME\jdoe），则思科 ISE 会搜索 NetBIOS 域的森林。找到后，便会在找到的域中查找所提供的 SAM 名称（在本例中为“jdoe”）。NetBIOS 域未必唯一（即使在一个森林中也如此），因此，搜索可能会找到多个同名的 NetBIOS 域。如果发生此情况并已提供密码，则可使用该密码来找到正确的身份。如果仍然模糊或未提供密码，则思科 ISE 会由于“模糊身份”错误而无法执行身份验证。

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
CiscoSystems(USA)Pte.Ltd.
Singapore

欧洲总部
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于
Cisco 位于 www.cisco.com/go/offices 上的网站。