HCIE-Security 备考指南

角色授权&认证授权（SVN）

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 角色授权/认证授权（SVN）需要掌握的知识点.....1
角色授权简介.....1
配置角色授权.....2
认证授权简介.....4
认证授权总体流程.....6
用户/组.....7
本地认证.....8
服务器认证.....9
证书认证.....10
辅助认证.....13
用户授权.....14
认证授权服务器.....17
认证授权配置流程.....20
手动创建用户/组.....24
配置认证选项.....30
配置访问控制策略组.....31
配置认证授权方式.....33
配置 RADIUS 服务器.....35
配置图形检验码认证.....36
认证授权规格.....37
HCIE-Security 模拟面试问题及面试建议.....37

HCIE-Security 角色授权/认证授权（SVN）需要掌握的知识点

- 掌握 SSL VPN 角色授权原理及配置
- 掌握 SSL VPN 认证授权原理及配置

角色授权简介

介绍角色的基本概念。

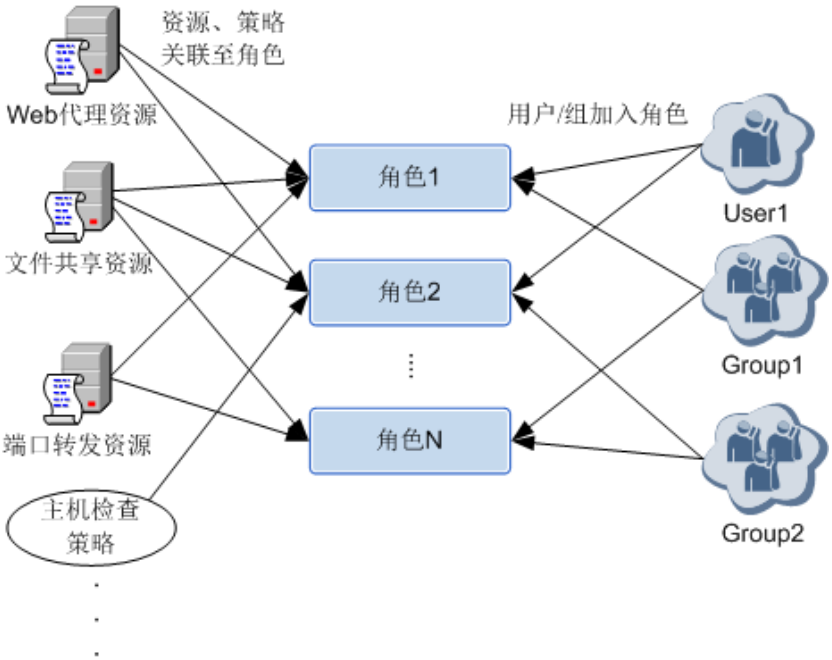
SVN 基于角色进行访问授权和接入控制，一个角色中的所有用户拥有相同的权限。角色是连接用户/组与业务资源、主机检查策略、登录时间段等权限控制项的桥梁，可以将权限相同的用户或组加入到某个角色，然后在角色中关联业务资源、主机检查策略等。

如图 1 所示，角色中可以包含多个用户/组，同时还可以关联多个业务资源或主机检测策略等权限控制项。

例如用户 User1 属于角色 2，角色 2 关联了 Web 代理资源（http://example.com）和主机检查策略，那么 User1 所使用的终端在通过主机检查策略的前提下，可以访问 http://example.com。

另外每个虚拟网关都存在一个缺省角色 **default**，只能编辑不能删除。缺省情况下 default 内用户可以访问所有资源。如果用户/组没有加入任何自定义角色缺省属于 default 角色，如果加入自定义角色则不再属于 default 角色。

图 1 角色授权示意图



角色具体可以关联的权限控制项如下：

- 业务启用：指定角色内用户可以使用的业务，包括 Web 代理、网络扩展、文件共享和端口转发。
- 资源授权：在启用某个业务的前提下，指定具体可以访问的资源。如果不指定具体资源，角色内用户无法访问任何资源。网络扩展业务比较特殊只要启用网络扩展业务，用户即可以访问所有 IP 资源，不涉及指定具体资源。
- 主机检查策略：指定角色关联的主机检查策略，只有通过主机检查策略检查的终端才能接入虚拟网关。
- 登录时间段：指定角色内用户允许登录虚拟网关的时间段。
- 跳转页面：指定角色内用户登录成功后跳转的页面。

一个用户/组可以加入多个角色，用户最终的权限与授权方式有关：

- 本地授权：用户/组在虚拟网关上存在。如果只将用户组加入自定义角色，则组内用户直接继承用户组权限；如果用户、组分别加入不同角色，用户权限取用户自身、用户直接父组关联角色权限的并集。
- 服务器授权：用户权限由服务器返回的授权组所关联的角色决定，即使本地存在此用户也不再查询用户自身关联的角色。如果授权组关联多个角色，则组内用户权限取这些角色的并集。

  采用服务器授权时需要确保虚拟网关上存在与服务器对应的授权组信息，也就是需要通过导入服务器组织结构或手动创建与服务器相同组织结构的方式在虚拟网关上创建用户组。然后将用户组加入角色进行授权。如果用户授权组在虚拟网关不存在，则使用/default 组所在角色的权限。

说明：

用户、用户父组只要有一方属于自定义角色，则用户不再受 default 角色权限控制。

- 本地授权：以下两种情况，用户都只受自定义角色权限控制。
  - 用户属于自定义角色、用户父组属于 default 角色。
  - 用户属于 default 角色、用户父组属于自定义角色。
- 服务器授权：如果一个用户同时属于多个父组，并且其中一个父组属于 default 角色，用户权限是除 defaut 组外其他几个组所属角色的并集。

配置角色授权

将具有相同权限的用户/组加入角色并基于角色对用户进行资源访问授权和接入控制。

背景信息

default 是虚拟网关的缺省角色，只能编辑不能删除。缺省情况下 default 内用户可以访问所有资源。

如果用户/组没有加入任何自定义角色缺省属于 default 角色，如果加入自定义角色则不再属于 default 角色。

一个用户/组可以加入多个角色，用户最终的权限与授权方式有关：

- 本地授权：用户/组在虚拟网关上存在。如果只将用户组加入自定义角色，则组内用户直接继承用户组权限；如果用户、组分别加入不同角色，用户权限取用户自身、用户直接父组关联角色权限的并集。
- 服务器授权：用户权限由服务器返回的授权组所关联的角色决定，即使本地存在此用户也不再查询用户自身关联的角色。如果授权组关联多个角色，则组内用户权限取这些角色的并集。

  采用服务器授权时需要确保虚拟网关上存在与服务器对应的授权组信息，也就是需要通过导入服务器组织结构或手动创建与服务器相同组织结构的方式在虚拟网关上创建用户组。然后将用户组加入角色进行授权。如果用户授权组在虚拟网关不存在，则使用/default 组所在角色的权限。

说明：

default 角色关联的用户/组无法编辑，自动关联没有加入自定义角色的用户/组。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 角色授权”。
3. 单击“新建”，配置角色参数。

参数	说明
角色	输入角色名称。不能输入缺省角色名称 default。
关联用户(组)	选择角色关联的用户或组。 可以从下拉列表中选择单个用户或组，也可以单击“多选”在用户组织结构上选择多个用户或组。 也可以在配置用户/组时关联角色。
允许登录时段	选择角色关联的时间计划，指定角色内用户允许登录虚拟网关的时间段。 缺省关联 default 时间段，表示所有时间段都可以登录虚拟网关。 如果修改已有角色关联的时间计划，对于在线用户不会立即生效，需要下次

参数	说明
	登录生效。
业务启用	选择角色内用户可以使用的业务。如果对应业务的全局开关未启用，即使这里启用业务终端用户也无法使用对应业务。
资源授权	单击“选择”，选择已经配置的业务资源。角色内用户只能访问经过授权的资源。
策略检查	
主机检查策略通过条件	• 以下所有规则都满足：角色内用户需要通过关联的所有主机检查策略的检查，才能接入虚拟网关。 • 满足以下任一规则：角色内用户只要通过关联的主机检查策略中的任一策略的检查，就能接入虚拟网关。
主机检查策略	选择角色关联的主机检查策略。
跳转页面设置	
PC 跳转页面	指定用户通过 PC 的浏览器登录虚拟网关页面后直接跳转到指定的页面。
移动终端跳转页面	指定用户通过移动终端的浏览器登录虚拟网关页面后直接跳转到指定的页面。

4. 单击“确定”。

认证授权简介

介绍认证授权的基本概念。

认证授权用于识别 SSL VPN 接入用户身份并赋予用户相应的访问权限，是进行资源访问控制的基本手段。

SVN 的认证授权是基于虚拟网关的，每个虚拟网关可以配置独立的认证授权方式。

说明：

下文如未特殊说明，以“用户”代表 SSL VPN 接入用户。

认证

认证用来验证用户的身份，SVN 对用户进行认证的方式包括：

- 本地认证

用户将标识其身份的用户名和密码发送给 SVN，SVN 上存储了密码，验证过程在 SVN 上进行，该方式称为本地认证。

- 服务器认证（RADIUS/LDAP/AD/SecurID）

  用户将标识其身份的用户名和密码发送给 SVN，SVN 上没有存储密码，SVN 将用户名和密码发送至第三方认证服务器，验证过程在认证服务器上进行，该方式称为服务器认证。

- 证书认证

  用户通过证书作为载体将标识其身份的信息发给 SVN，SVN 通过校验证书识别用户身份，该方式称为证书认证。用户可以将客户端证书导入浏览器也可以使用 USB Key，更安全更方便。

  证书认证支持两种：

  - 证书匿名：只校验客户端证书有效性。
  - 证书挑战：除了校验客户端证书有效性，还需要输入挑战密码，是一种双因子认证。

- 辅助认证

  配合上述认证方式使用，以提高安全性。包括图形校验码认证和终端标识码认证。

授权

授权用来控制用户的访问权限。SVN 对用户的业务授权通过角色实现，先将具有相同权限的用户/组加入某个角色，然后角色关联可访问的业务资源。

SVN 支持以下授权方式：

- 本地授权

  在本地创建用户/组，然后将用户/组加入角色进行授权。

- 服务器授权（RADIUS/LDAP/AD/SecurID）

  从服务器获取用户授权组，然后根据此授权组在 SVN 上所属的角色对用户授权。也就是服务器并不能直接对用户授权。

例如 LDAP 服务器授权，表示从 LDAP 服务器获取用户在服务器上所属组信息，然后基于此组在 SVN 上所属的角色进行授权。因此使用服务器授权时需要保证 SVN 上存在与服务器上对应的组信息，然后将组加入角色进行授权。

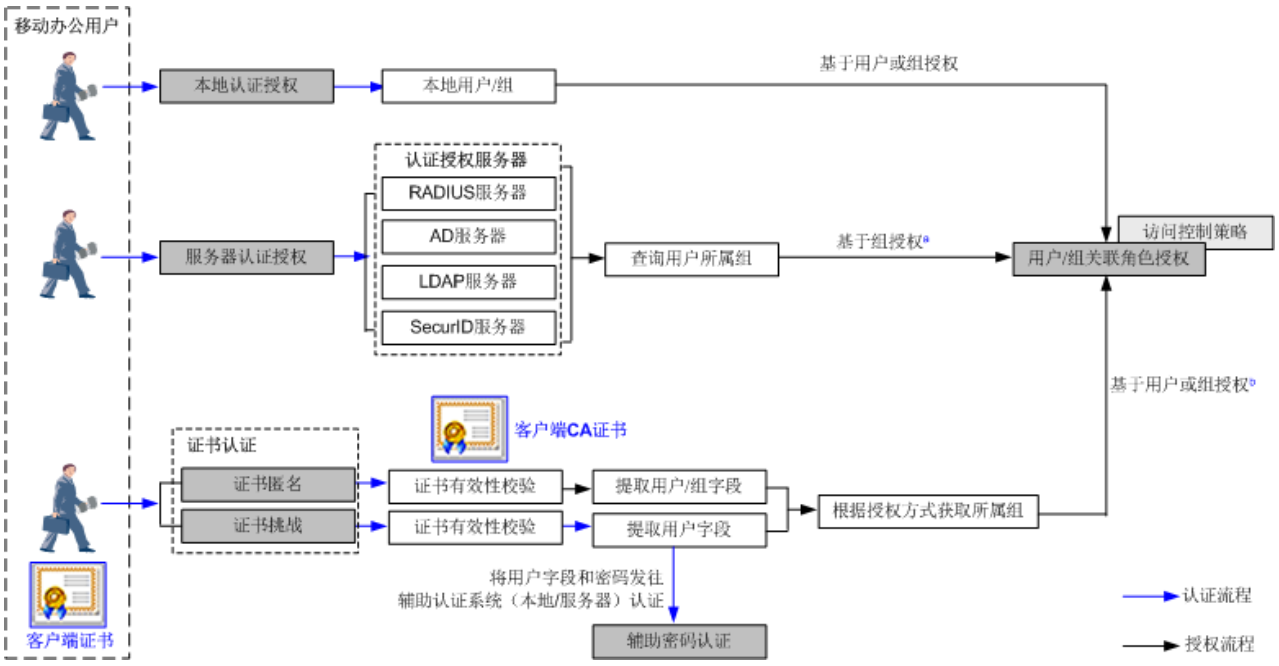
通常情况下认证授权配置为同一种方式即可，在需要认证授权分离的情况下可以选择不同的方式。例如授权组织结构与认证服务器上的组织结构不同，此时可以配置认证授权使用不同的服务器。

认证授权总体流程

了解整体的认证授权流程，有助于后续配置。

用户从接入认证到获取对应的访问权限需要经过多个环节，不同认证授权方式处理过程也不同，如图 1 所示。

图 1 认证授权流程示意图



a：使用服务器授权方式时，SVN 根据服务器返回的用户组信息进行授权，无法基于具体用户授权。因此需要在 SVN 上创建或导入与服务器上组信息对应的组，然后将组加入角色授权。
b：证书认证根据选择的授权方式不同，授权处理不同：本地授权时 SVN 上需要存在与证书中用户/组字段对应的用户/组，然后将用户/组加入角色授权；服务器授权时通过证书用户字段到服务器上查询用户所属组，然后基于组授权，也就是 SVN 上需要存在与服务器对应的组。

说明：

除了本地认证、服务器认证和证书认证外，SVN 还支持图形校验码认证、终端标识码认证 2 种辅助认证方式，可以与任何认证方式组合使用，图中不再给出。

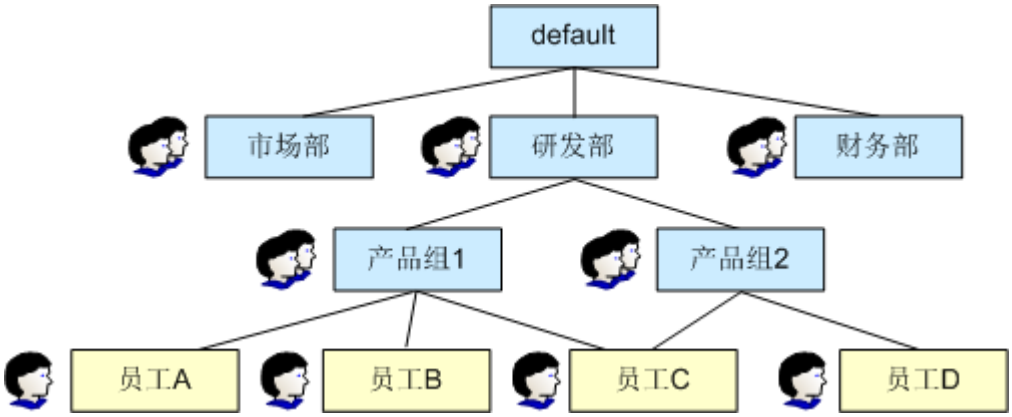
用户/组

用户是通过 SSL VPN 访问内网资源的主体，是 SVN 进行接入认证和访问权限控制的基本单元。

树形组织结构

用户按树形结构组织，用户隶属于组（部门）。管理员可以根据企业的组织结构来创建部门和用户。这种方式易于管理员查询、定位，是常用的用户组织方式。树形组织结构如图 1 所示。

图 1 用户/组的树形组织结构示意图



规划树形组织结构时必须遵循如下规定：

- default 组是设备默认自带的根组，不能被删除，且组名不能修改。其余所有组都是 default 组的子组，或者子组的子组。
- 设备最多支持 20 层用户结构，包括 default 组和用户，即 default 组和用户之间最多允许存在 18 层组。
- 每个组可以包括多个用户和组，但每个组只能属于一个父组。
- 一个用户最多可以属于三个父组。
- 组名允许重名，但所在组织结构的全路径必须确保唯一性。

用户/组的来源

说明：

使用本地认证授权时，需要在 SVN 上创建用户/组。

使用服务器认证授权时，认证阶段直接到服务器认证不需要本地存在用户；授权阶段 SVN 根据服务器返回的用

户组信息进行授权，无法基于具体用户授权。因此只需要在 SVN 上创建或导入与服务器对应的组信息，无需创建用户信息。

在 SVN 上创建用户和组时，可以使用以下方式：

- 手动创建

  管理员手动创建用户和组，并配置用户属性。例如，管理员可根据企业的组织架构创建组，然后在各组下创建用户信息。

- 从 CSV 文件导入

  将用户信息按照指定格式写入 CSV 文件中，再将 CSV 文件导入到 SVN 中，或者将之前从 SVN 上导出的 CSV 文件再次导入，批量创建用户和组。

- 从服务器导入

  如果实际环境中已经部署了身份验证机制，并且用户信息都存放在第三方认证服务器上，则可以通过执行服务器导入策略，将第三方认证服务器上用户和组的信息导入到 SVN 上。

  目前 SVN 只支持从 AD、LDAP 服务器导入用户和组。对于其他服务器，请使用手动创建、CSV 文件导入。

在线用户

用户访问资源前，首先需要经过 SVN 的认证，目的是识别这个用户当前在使用哪个 IP 地址。对于通过认证的用户，SVN 还会检查用户的属性（用户锁定状态、是否允许多人同时使用该账号登录等），只有认证和用户属性检查都通过的用户，该用户才能上线，称为在线用户。

SVN 上的在线用户监控表记录了用户和该用户当前所使用的地址的对应关系。

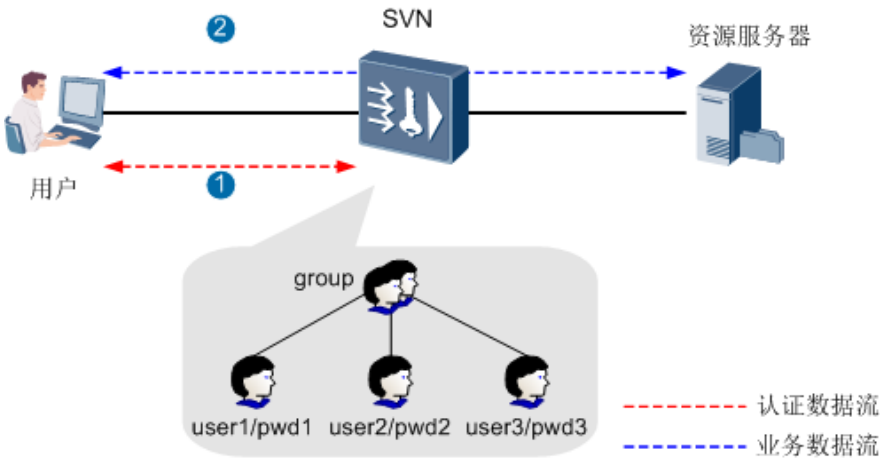
本地认证

介绍本地认证的原理。

管理员依据企业的组织结构，在 SVN 的虚拟网关上创建相应的用户/组，并设置用户的密码。认证时，由 SVN 来验证用户使用的用户和密码，对用户进行认证。

如图 1 所示，SVN 上存储了用户/组和密码等信息。用户在访问内网资源之前，必须先通过 SVN 的认证。认证成功后，SVN 记录用户和 IP 地址之间的对应关系。用户访问内网资源时，受本地用户/组的权限控制。

图 1 本地认证示意图



服务器认证

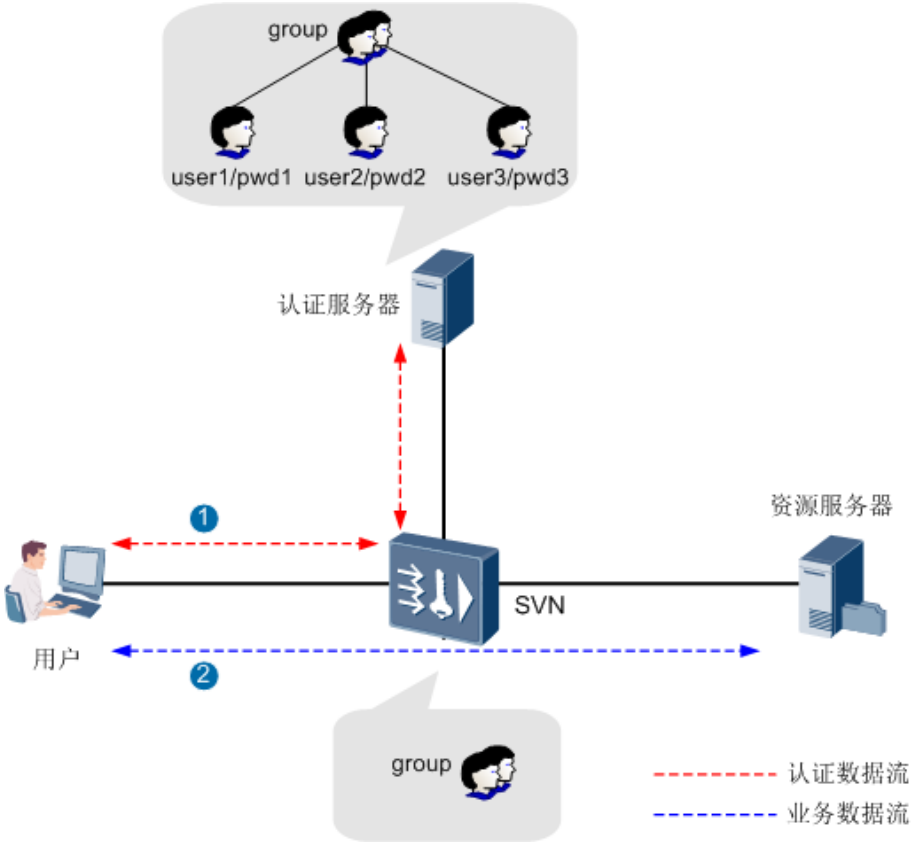
介绍服务器认证原理。

企业已经部署了 RADIUS（Remote Authentication Dial In User Service）、AD（Active Directory）、LDAP（Lightweight Directory Access Protocol）或 SecurID 认证服务器，并在认证服务器上存储了用户/组和密码等信息。认证时，SVN 作为认证服务器的代理客户端，将用户名和密码发送给认证服务器进行认证。

如图 1 所示，认证服务器上存储了用户/组和密码等信息。用户在访问内网资源之前，必须先通过认证服务器的认证。认证成功后，SVN 会记录用户和 IP 地址之间的对应关系。

认证阶段 SVN 的虚拟网关上不需要存在用户和用户组，但是后续授权阶段需要基于用户组授权，因此需要在 SVN 的虚拟网关上创建对应用户组。

图 1 服务器认证示意图



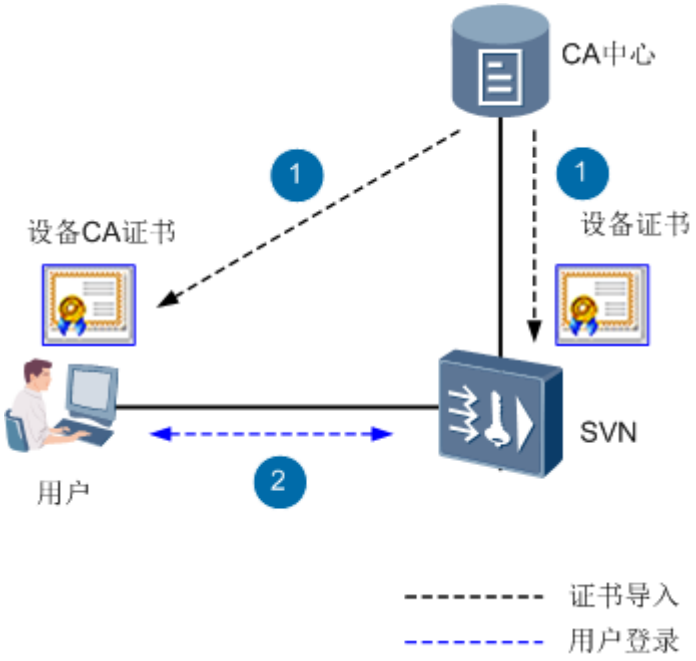
证书认证

介绍证书认证的原理。

用户登录虚拟网关时涉及证书认证的有两阶段：

- 阶段一：用户使用客户端中受信任颁发机构的 CA 证书验证虚拟网关身份，如图 1 所示。

  图 1 阶段 1：用户验证虚拟网关设备证书示意图



用户验证虚拟网关设备证书过程如下：

1. 用户侧和 SVN 的虚拟网关侧分别导入同一个证书颁发机构的 CA 证书和设备证书。
2. 用户登录时使用 CA 证书验证 SVN 发来的设备证书。

   如果设备证书满足以下 3 个条件则认证通过：

   - 设备证书在有效期内。
   - 设备证书是由 CA 证书对应的颁发机构颁发的。
   - 设备证书的 CN 字段取值与虚拟网关地址或域名一致。

   如果不满足条件系统将产生告警信息，用户也可以选择直接信任设备 CA 证书忽略告警。

- 阶段二：虚拟网关使用客户端 CA 证书验证用户身份，如图 2 所示。

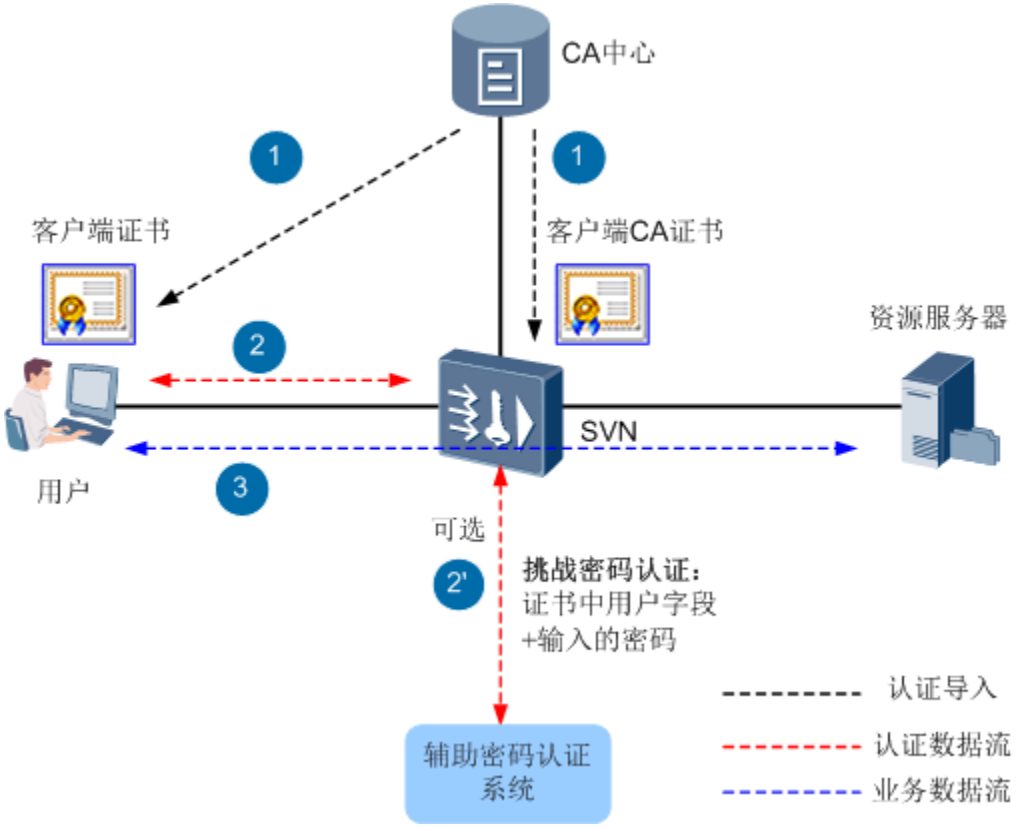
证书认证是与本地认证、服务器认证并列的一种认证方式，用户通过证书作为载体将标识其身份的信息发给 SVN，SVN 通过校验证书识别用户身份。用户可以将客户端证书导入浏览器也可以使用 USB Key，更安全更方便。

证书认证有两种方式：

- 证书匿名：虚拟网关只通过客户端 CA 证书验证客户端证书的有效性。

- 证书挑战：除了验证客户端证书有效性，还要验证密码。此种情况下用户不但要提供客户端证书，还要输入挑战密码，是一种双因子认证。

图 2 阶段 2：虚拟网关验证用户客户端证书示意图



虚拟网关验证用户客户端证书过程如下：

1. 用户侧和 SVN 的虚拟网关侧分别导入同一个证书颁发机构的客户端证书和客户端 CA 证书。
2. 虚拟网关对用户进行认证。
   - 证书匿名：虚拟网关使用客户端 CA 证书验证客户端证书有效性，验证项目包括是否与客户端 CA 证书属于同一个证书颁发机构、是否在有效期内、是否被吊销。如果通过验证则认证通过。
   - 证书挑战：虚拟网关除了验证客户端证书有效性，还根据用户过滤字段提取证书中的用户名作为用户帐号，将用户帐号和用户输入的挑战密码发送到辅助认证系统（本地或服务器认证）进行密码认证。两者都验证通过才认证通过。
3. 证书认证阶段结束，用户访问内网资源。

   用户可访问的资源由授权阶段决定，SVN 根据证书中的用户名到本地（本地授权）或服务器（服务器授权）获取授权组。SVN 基于授权组进行授权。

辅助认证

介绍辅助认证原理。

SVN 提供辅助认证与其他认证方式配合使用，增强了用户接入安全性。

终端标识码认证

将用户账号与指定终端绑定，用户只能从终端标识码匹配的终端登录虚拟网关。即使用户账号信息被盗取，由于无法获取指定的硬件终端，仍然无法访问，进一步保证了接入用户的合法性。

终端标识码认证过程如下：

1. 当用户通过某个终端登录虚拟网关时，如果对应的终端标识码在虚拟网关中没有记录，将提示用户提交终端标识码。用户执行提交操作。

   一个用户最多可以提交 5 个终端标识码，也就是限制用户可以通过 5 个终端登录虚拟网关。

   提交终端标识码的过程是客户端软件自动收集客户端的硬件信息，并将硬件信息转换成一个 MD5 值，然后将此 MD5 值发给虚拟网关。

2. 虚拟网关记录用户和终端标识码的对应关系到终端标识码列表。
3. 虚拟网关管理员审批终端标识码，审批通过后允许用户通过此终端登录虚拟网关，认证通过。

   虚拟网关提供自动审批功能，如果开启自动审批功能，用户提交终端标识码后即可登录虚拟网关。否则需要待管理员手动审批后才能登录。

4. 后续用户再次登录时，虚拟网关检查用户与终端标识码的对应关系，如果与虚拟网关中记录的对应关系匹配则通过认证。

图形校验码认证

图形检验码认证用于防止机器登录和暴力破解密码。用户登录虚拟网关时必须手工输入随机产生的图形检验码才能通过验证。

用户授权

用户授权是给用户分配权限的过程，权限包括可以访问的资源以及一些访问控制项。

SVN 的授权有两阶段：首先通过配置的授权方式获取用户所属组信息，然后通过组对应的角色对用户进行业务授权，也就是用户可访问的资源。

阶段一：根据配置的授权方式获取授权组信息

- 本地授权：用户认证通过后将用户在本地的所属组作为授权组。
- 服务器授权：用户认证通过后将服务器返回用户在服务器上的父组信息作为授权组。

对于证书认证用户，SVN 根据配置的用户过滤字段提取证书中的用户名，然后根据配置的授权方式（本地或服务器授权）获取授权组。

阶段二：基于授权组业务授权

对于本地授权基于用户和组都可以分配权限；对于服务器授权只能基于服务器返回的授权组分配权限，本地需要创建或导入与服务器对应的组。如果 SVN 上不存在服务器对应的授权组，用户使用 default 组的权限。

具体权限控制有两种方式：

- 角色授权

  将权限相同的用户或组加入到某个角色，然后在角色中启用允许使用的业务、关联可访问的业务资源、关联主机检查策略等。角色授权是用户授权的主要方式。

- 访问控制策略组

  访问控制策略组是角色授权的辅助手段，可以基于 IP、URL、端口更细化地控制用户权限。

角色授权

具体参见角色授权。

访问控制策略组

角色授权一般用于统一控制用户组或某些用户可以访问相同的资源，访问控制策略组可以在角色授权基础上进行更细化地访问控制。例如：角色授权中指定用户组可以使用网络扩展业务，也就是用户组内用户可以访问相同的内网 IP 资源，如果需要额外禁止某些用户访问某些 IP 资源，此时可以配置禁止用户访问这些目的 IP 地址的访问控制策略组。

访问控制策略组由多条不同类型的访问控制策略组成，每条策略中只包含需要控制的项目并不包含动作，策略组关联用户/组时指定策略组整体动作。

- 源 IP 型：通过用户的源 IP 地址来控制用户访问虚拟网关的权限。用户通过被限制的源 IP 登录时，即使用户名、密码正确也无法成功登录虚拟网关。
- 目的 IP 型：通过目的 IP、端口控制用户访问内网资源的权限。
- URL 型：通过 URL 控制用户访问内网资源的权限。

用户/组可以关联多个策略组，每个策略组可以指定优先级。用户上线时具体匹配过程如下：

步骤 1：获取需要匹配的策略

用户上线时虚拟网关先从策略组关联列表中按配置顺序取出用户关联的策略，每个在线用户最多生效的源 IP 型策略为 255 条、URL 型策略为 16 条、目的 IP 型策略为 1024 条，大于规格数的策略无效。

- 本地授权

  用户上线时优先从用户关联的访问控制策略组中取访问控制策略，如果用户关联的策略未超出规格则继续取父组关联的访问控制策略组中的策略。

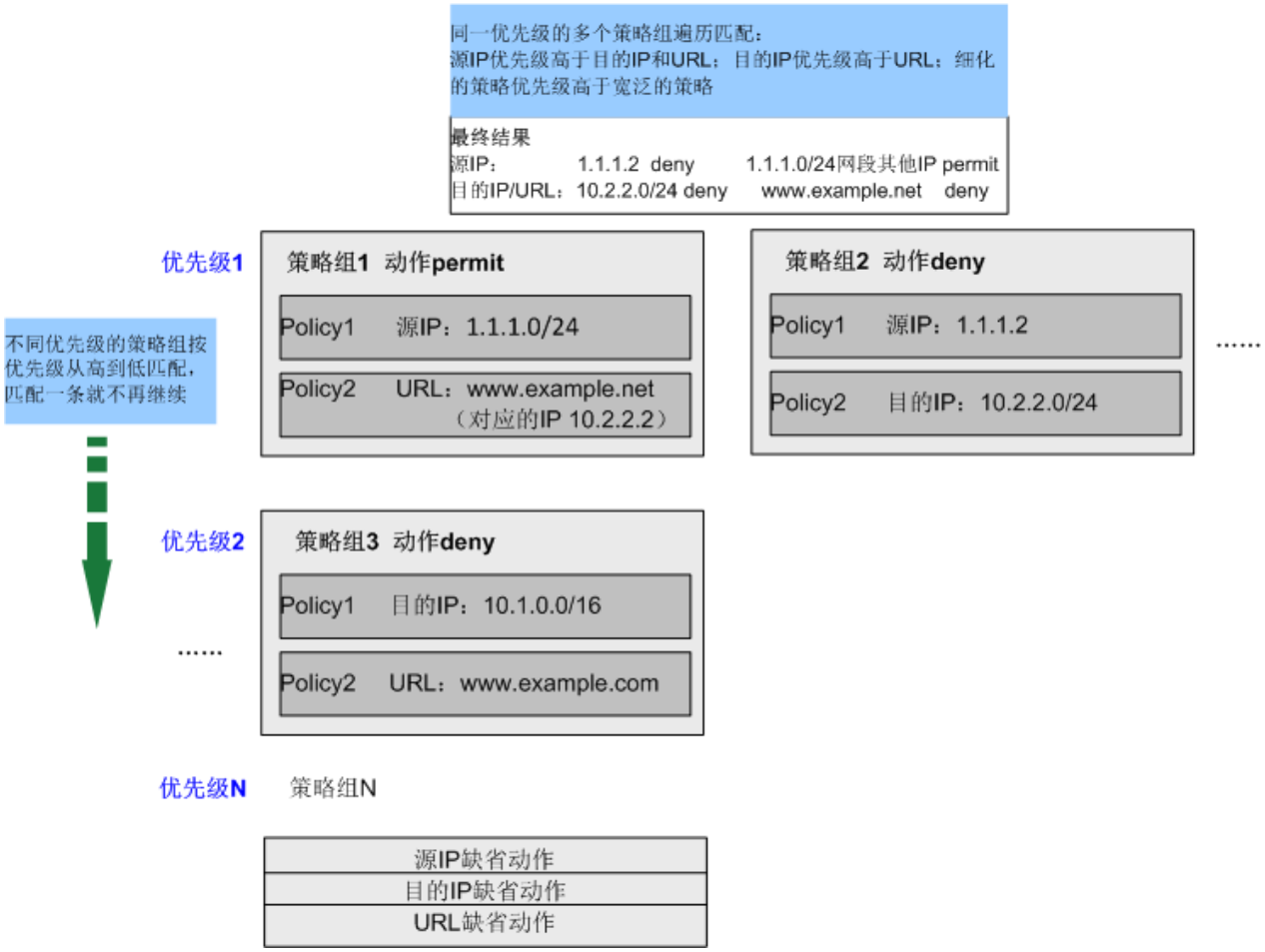
- 服务器授权

  用户上线时只从父组关联的访问控制策略组中取访问控制策略。

步骤 2：策略匹配

取出需要匹配的访问控制策略后，虚拟网关按图 1 所示的过程进行策略匹配。

图 1 访问控制策略组匹配示意图



- 优先级取值越小的策略组越优先匹配，匹配到一个策略组就不再继续匹配。如果没有匹配任何策略组则匹配默认策略动作。
- 如果存在多个优先级相同的策略组，需要遍历匹配各个策略组中的策略，匹配过程如下：
  - 源 IP 策略优先级高于目的 IP/URL 策略，如果禁止源 IP 访问虚拟网关，则不再匹配目的 IP 或 URL 策略。
  - 目的 IP 策略优先级高于 URL 策略。

    例如：策略组 1 的 Policy2 允许用户访问 www.example.net，但是策略组 2 的 Policy2 禁止用户访问该 URL 对应的 IP（10.2.2.2），最终结果是用户无法访问 www.example.net。
  - 同一类型的策略，条件细化的策略优先级高于条件宽泛的策略。

    例如：策略组 1 的 Policy1 允许 1.1.1.0/24 整个网段访问虚拟网关，但是策略组 2 的 Policy1 禁止 1.1.1.2 访问虚拟网关，最终结果是 1.1.1.0/24 网段中 1.1.1.2 无法访问虚拟网关，其余 IP 允许访问虚拟网关。

    IP 型策略具体匹配原则如下：

- 先匹配 IP 地址细化的策略，再匹配 IP 地址宽泛的策略。
- 如果 IP 相同则先匹配限制了具体端口的策略，并且端口范围越小的越排在前边。
- 如果端口相同则先匹配限制了具体协议类型的策略。
- 如果所有条件都相同，只有动作不同，则与默认策略动作相反的策略生效。

URL 型策略具体匹配原则如下：

- 先匹配 URL 细化的策略，再匹配 URL 宽泛的策略。

  先比较 URL 的级数（即.和/的个数），级数多的 URL 比级数少的优先级高；如果级数相同再比较是否包含*，不包含*的 URL 比包含*的优先级高；如果都包含*再比较*的位置，*在左边的 URL 比*在右边的优先级高。

  例如：“www.a.example.com、www.example.com、*.example.com、www.example.*、example.com”这 5 个 URL 优先级为从高到低。

- 如果 URL 相同则先匹配限制了具体端口的策略，并且端口范围越小的越排在前边。
- 如果端口相同则先匹配限制了具体协议类型的策略。
- 如果所有条件都相同，只有动作不同，则与默认策略动作相反的策略生效。

认证授权服务器

介绍 SVN 对 SSL VPN 用户进行认证授权时，支持对接的认证授权服务器。

认证授权服务器的主要作用如下：

- 使用服务器认证方式时验证用户身份。
- 使用服务器授权时 SVN 从服务器获取授权组信息，从而基于授权组进行授权。

了解各类服务器的基本概念和实现原理，将会有助于管理员在 SVN 上正确配置服务器对接参数，确保 SVN 和服务器正常通信。

本节对服务器以及 SVN 与服务器通信时所使用协议进行简要介绍，详细的内容请参见服务器自带的文档。

RADIUS 服务器

SVN 与 RADIUS 服务器之间使用 RADIUS 协议通信，RADIUS 协议使用 UDP 协议作为传输协议，具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。SVN 与 RADIUS 服务器之间使用共享密钥对传输的报文进行加密，具有较好的安全性。

RADIUS 协议的实现比较简单，适用于大用户量时服务器端的多线程结构。

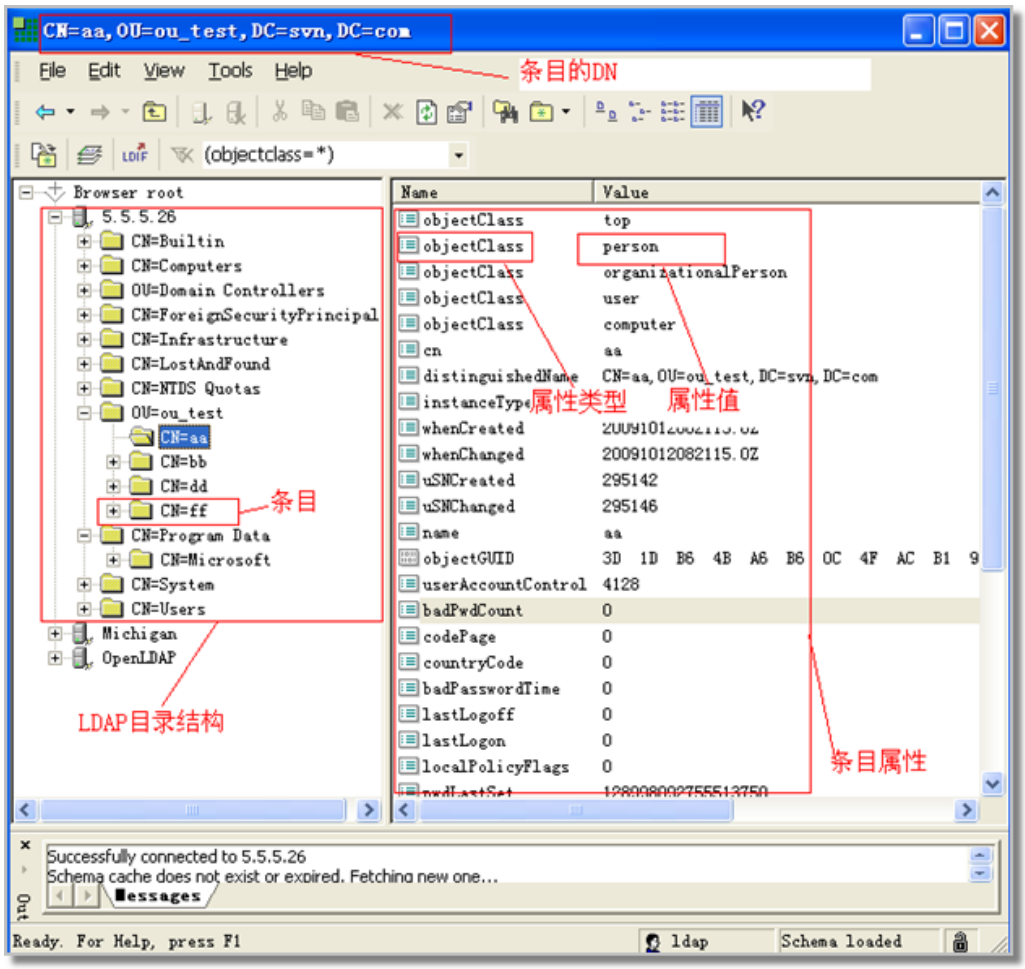
LDAP 服务器

LDAP 是轻量级目录访问协议的简称，是一种基于 TCP/IP 的访问在线目录服务的协议。LDAP 协议的典型应用是用来保存系统的用户信息，用于用户登录时的认证和授权。LDAP 的目录服务功能建立在 Client/Server 的基础之上，所有的目录信息存储在 LDAP 服务器上。

目录是一组具有类似属性、以一定逻辑和层次组合的信息。LDAP 协议中目录是按照树型结构组织，目录由条目（Entry）组成，条目是具有区别名 DN（Distinguished Name）的属性（Attribute）集合。属性由类型（Type）和多个值（Values）组成。LDAP 目录树的最顶部就是根，根的区别名称为“Base DN”。

如图 1 所示，通过 LDAP Client 来查看 LDAP 协议的目录结构。LDAP 服务器所管辖域 svn.com 中存在组织单元“ou_test”，其中包括 aa、bb、dd 和 ff 条目，则条目“aa”的 Base DN 为：“CN=aa,OU=ou_test,dc=svn,dc=com”。

图 1 LDAP 目录结构



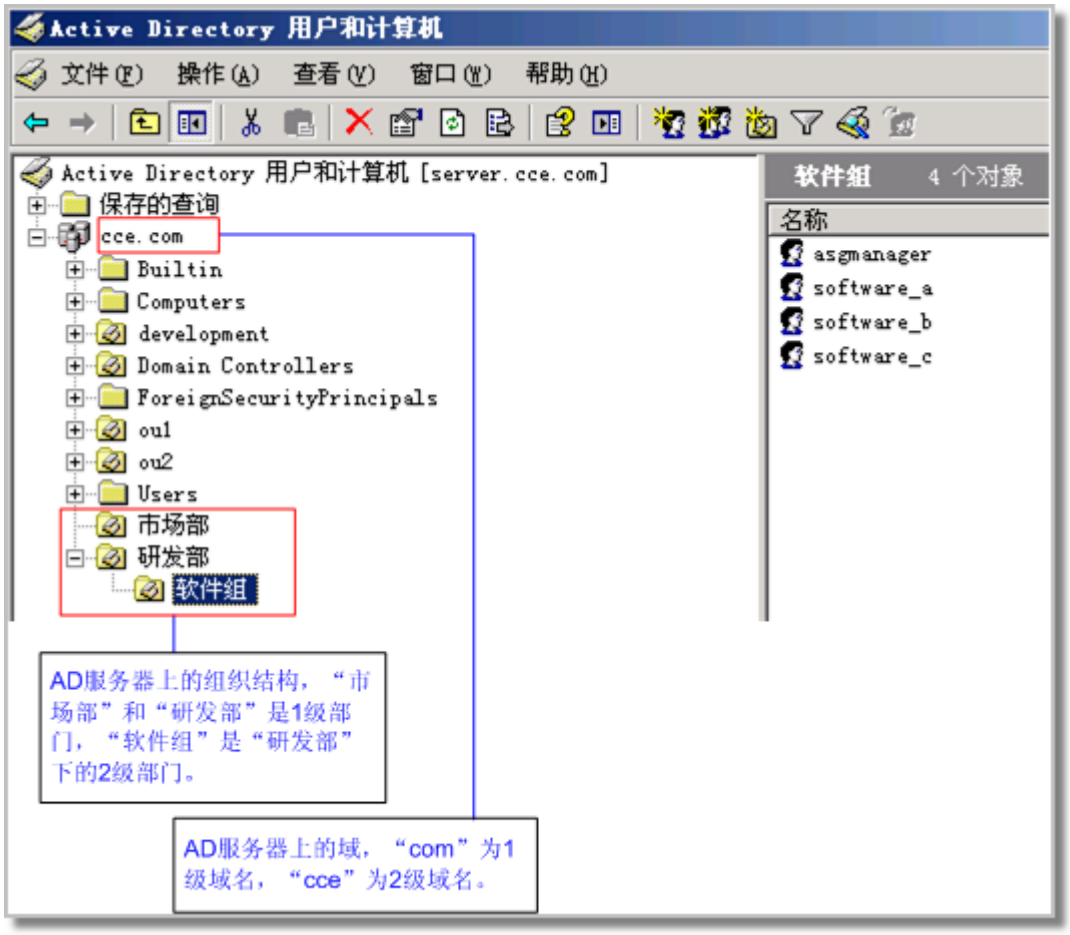
AD 服务器

AD 是 Windows Server 域环境中提供目录服务的组件，可以将活动目录理解为目录服务在微软平台的一种实现方式。

活动目录将登录身份验证以及目录对象的访问控制集成在一起，管理员可以管理分散在网络各处的目录数据和组织单位，经过授权的网络用户可以访问网络任意位置的资源。

如图 2 所示，AD 服务器所管辖域 cce.com 中包括“研发部”和“市场部”两个部门，则“研发部”的 Base DN 为：“OU=研发部,DC=cce,DC=com”。

图 2 AD 目录结构



SecurID 服务器

SecurID 服务器通过双因素认证能够有效的管理用户认证，用户登录时需要输入用户名及密码，密码由静态 PIN 码和动态 Token 序列号组成：

- 静态 PIN 码在 SecurID 服务器上进行设置，由管理员提供给用户。
- 动态 Token 序列号由令牌生成，这些动态 Token 序列号每隔一定的时间变化一次。

静态 PIN 码和动态 Token 序列号任一出现错误，用户无法登录成功。因为需要两个因素，所以 SecurID 认证方式能提供更加安全的身份认证机制。

SVN 与 SecurID 服务器之间使用共享密钥对传输的报文进行加密，具有较好的安全性。

认证授权配置流程

了解认证授权的配置流程，有助于您根据需要选择阅读后续的内容。

说明：

虚拟网关支持 3 级认证授权，认证或授权服务器无响应时进行下一级认证授权。

需要认证授权分离的场景下认证和授权方式可以不同，例如使用 AD 认证、LDAP 授权，AD 服务器只负责认证，LDAP 服务器负责提供授权组，把 LDAP 服务器的用户组导入虚拟网关即可。但是通常情况下认证授权使用同一方式即可，也就是身份验证和授权组信息都是同一个来源。

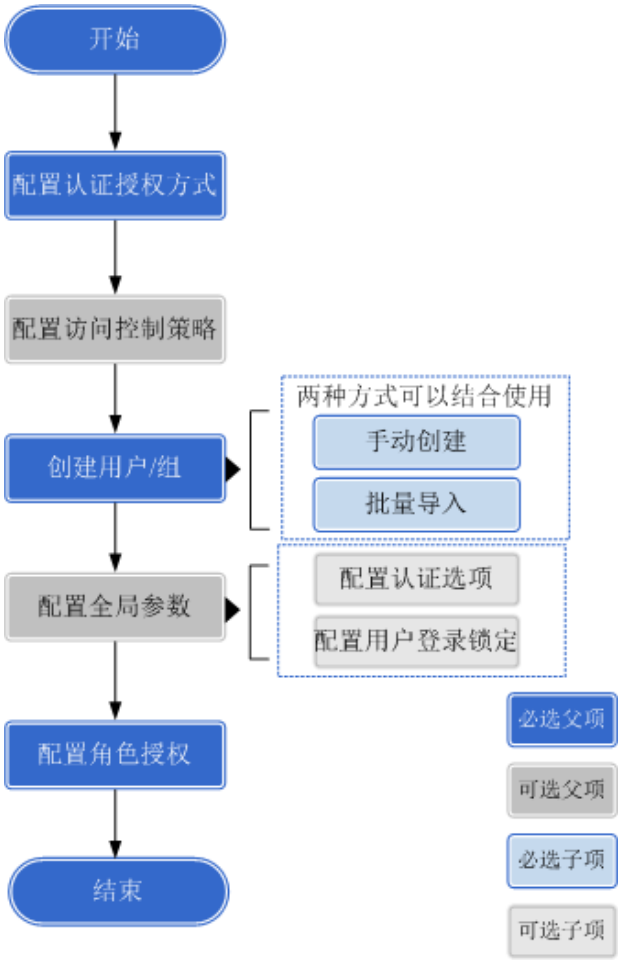
除了本地认证、服务器认证和证书认证外，SVN 还支持图形校验码认证、终端标识码认证 2 种辅助认证方式，可以与任何认证方式组合使用，图中不再给出。

本地认证授权

使用本地认证授权方式时，需要在虚拟网关上创建用户/组并设置密码，然后将用户/组加入角色进行业务授权。

本地认证授权的配置流程如图 1 所示。

图 1 本地认证授权配置流程



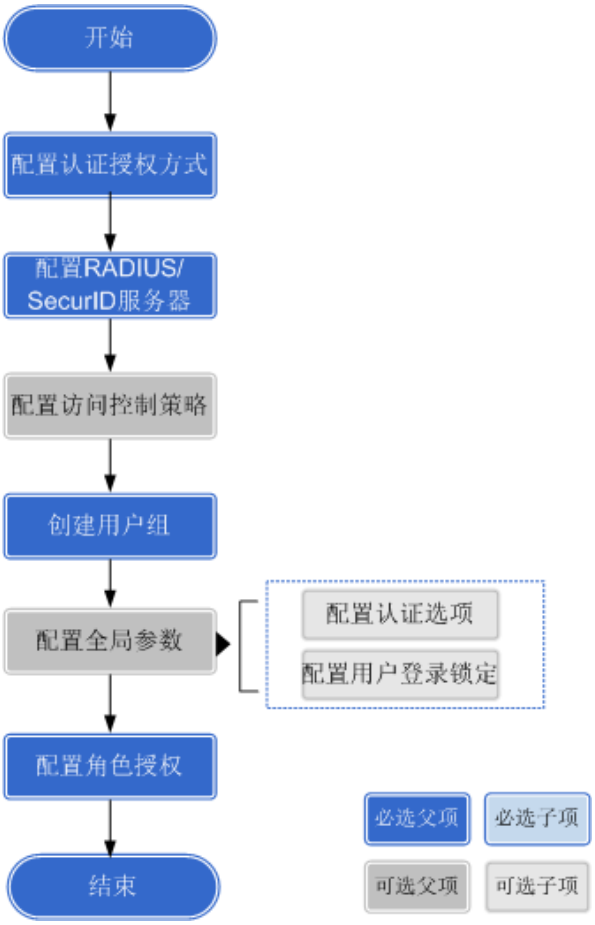
RADIUS/SecurID 服务器认证授权配置流程

使用 RADIUS/SecurID 服务器认证授权方式时，不支持将服务器上的用户组导入虚拟网关，因此需要在虚拟网关上手动创建用户组，与服务器上的组信息保持一致。然后将用户组加入角色进行授权。

使用服务器授权时由服务器返回用户的授权组信息，然后基于此组信息查询该组在虚拟网关上所属的角色，从而进行业务授权。因此在本地创建用户组即可，无需创建用户，有本地授权需求时才需要创建用户。

RADIUS/SecurID 服务器认证授权的配置流程如图 2 所示。

图 2 RADIUS/SecurID 服务器认证授权配置流程



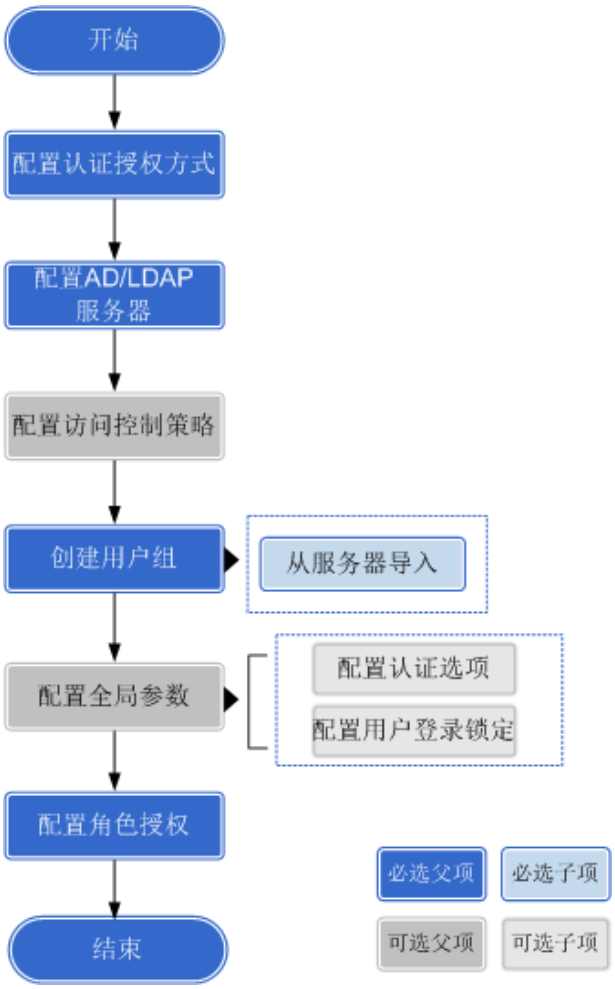
AD/LDAP 服务器认证授权配置流程

使用 AD/LDAP 服务器认证授权方式时，需要将服务器上的用户组导入到虚拟网关。然后将用户组加入角色进行授权。

使用服务器授权时由服务器返回用户的授权组信息，然后基于此组信息查询该组在虚拟网关上所属的角色，从而进行业务授权。因此只导入用户组即可，无需导入用户，有本地授权需求时才需要导入用户。

AD/LDAP 服务器认证授权的配置流程如图 3 所示。

图 3 AD/LDAP 服务器认证授权配置流程



证书认证、本地/服务器授权配置流程

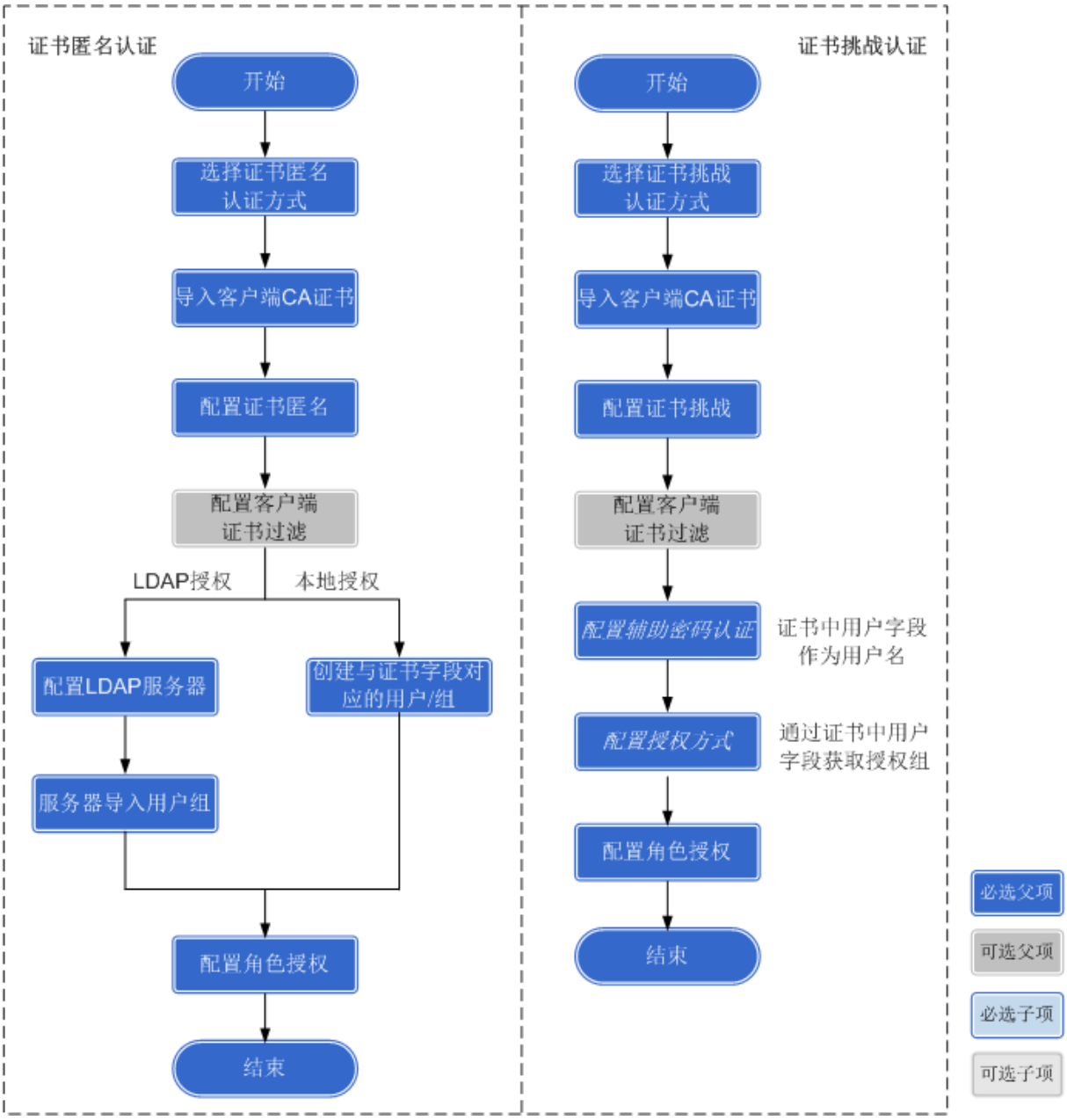
证书认证有两种方式：

- 证书匿名认证：只校验证书有效性，用户无需输入密码。在虚拟网关上配置证书中代表用户/组的过滤字段，然后虚拟网关提取证书中的字段用于用户授权。证书匿名认证仅支持本地和 LDAP 授权方式。
- 证书挑战认证：是结合证书有效性校验和密码认证的双因子认证方式。在虚拟网关上配置证书中代表用户的过滤字段，然后虚拟网关提取用户字段作为账号，将用户帐号和用户输入的挑战密码发送到辅助认证系统对用户进行认证。

  证书挑战认证支持所有授权方式。辅助密码认证、授权的配置请参见其他认证授权方式的配置。

证书认证的配置流程如图 4 所示。

图 4 证书认证配置流程



手动创建用户/组

在 SVN 上手动创建用户/组，并配置其属性。

背景信息

SVN 上的用户和组是企业组织结构的体现，在 SVN 上存储用户和组的主要目的是供授权所引用，实现基于用户的资源访问控制。

创建用户和组时必须遵循如下规定：

- default 组是 SVN 上默认存在的根组，所有组和用户都属于该组。default 组不能被删除，也不能修改其名称。
- 设备最多支持 20 层用户结构，包括 default 组和用户，即 default 组和用户之间最多允许存在 18 层组。
- 每个组可以包括多个用户和组，但每个组只能属于一个父组。
- 一个用户最多可以属于三个父组。

操作步骤

- 创建组。

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 用户 > 用户/组”。
3. 在“成员管理”中，单击“新建”，选择“新建组”。
4. 配置组的基本参数。

参数	说明
组名	输入组的名称。 组允许重名，但组所在组织结构的全路径必须确保唯一性。例如，/default/research/group1 和/default/marketing/group1 是两个不同的组。
描述	输入组的描述信息。 合理填写描述信息有助于管理员正确理解组的功能，便于查找和维护。
所属组	输入组所属的父组。 单击“选择”，在“组织结构”中选择所属的父组，然后单击“确定”。 每个组只能属于一个父组。
关联角色	选择用户组所属的角色。用户组内用户能访问的资源，是用户组所属的角色和用户自身所属角色能访问资源的并集。
用户组属性	
终端标识码认证	启用终端标识码认证。组内用户在登录虚拟网关时，必须进行终端标识码认证。如果认证不通过，用户将无法登录虚拟网关。 只有在终端标识码认证全局开关启用的情况下，才能配置此参数。
SSL 虚拟 IP 地址池	指定用户组使用的网络扩展地址池。只有在已经启用网络扩展业务并且配置客户端地址池的情况下才能配置。
NFS 组 ID	指定用户组对应的 NFS 文件系统的组 ID（GID）。 NFS 文件系统通过组 ID（GID）和用户 ID（UID）控制不同组/用户的文件读写权限，这里配置的组 ID 需要与服务器上的组 ID 相同。

5. 关联访问控制策略组。

访问控制策略组用于在角色授权的基础上，对用户/组进行细化的访问控制，包括基于源 IP、目的 IP/端口、URL 的访问控制。例如：角色授权中指定用户组可以使用网络扩展业务，也就是用户组内用户可以访问相同的内网 IP 资源，如果需要额外禁止某些用户访问某些 IP 资源，此时可以配置禁止用户访问这些目的 IP 地址的访问控制策略组。访问控制策略组的具体配置请参见访问控制策略组。

a. 选择“策略组配置”页签。

b. 单击“新建”，关联访问控制策略组。

参数	说明
ACL 组	选择关联的访问控制策略组。只能选择已经创建的访问控制策略组（“SSL VPN > 用户 > 访问控制组管理”）。
优先级	输入访问控制策略组的优先级。优先级取值越小的策略组越优先匹配。如果没有匹配任何策略组则匹配缺省动作（“系统 > 虚拟网关级策略 > 策略默认行为”）。 **说明：** 用户最终生效的访问权限，是用户所属直接父组和用户自身所关联的访问控制策略组的并集，因此 SVN 根据所有这些策略的配置及优先级最终决定用户的访问权限。具体匹配原则请参见用户授权。
行为	指定策略的行为动作，包括限制和允许访问策略中指定的 IP、URL 等资源。

c. 单击“确定”。

6. 单击“确定”。

配置完成后，在“组织结构”中可以查看到新创建的组，在新创建的组所属父组的“成员管理”中可以查看到其信息。

- 创建用户。

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 用户 > 用户/组”。
3. 在“成员管理”中，单击“新建”，选择“新建用户”。
4. 配置用户的参数。

参数	说明
登录名	输入用户的登录名，即用户进行认证时使用的名称。 登录名（账号）不允许重名。

参数	说明
显示名	输入用户的显示名。 显示名仅作为区分用户的标识，用户不能使用显示名发起认证请求。为方便记忆和管理，建议采用直观的名字（如员工的真实姓名）作为显示名，不同的用户允许使用相同的显示名。
描述	输入用户的描述信息。 合理填写描述信息有助于管理员识别用户，便于查找和维护。
所属组	输入用户所属的父组。 单击“选择”，在“组织结构”中选择新建用户所属的父组，单击“确定”。 一个用户最多可以属于三个父组。
关联角色	选择用户所属的角色。用户能访问的资源，是用户直接父组所属的角色和用户自身所属角色能访问资源的并集。
用户属性	
认证类型	选择用户的认证类型。 • “本地认证”表示由 SVN 来认证用户，这种情况下需要在 SVN 上配置用户的密码。 • “服务器认证”表示由认证服务器来认证用户，这种情况下不需要在 SVN 上配置用户的密码。
密码	输入用户的密码。 该参数只在“认证类型”为“本地认证”时需要配置。
确认密码	再次输入用户的密码。 该参数只在“认证类型”为“本地认证”时需要配置。
最大在线数	输入允许该用户账号在多个终端上同时登录虚拟网关的最大数量。只有在“SSL VPN > 认证授权 > 认证授权方式”中启用了“允许一个账号在多处同时登录”的情况下，才能配置此参数。 如果不输入该值，则使用“认证授权方式”中的“各账号的默认最大在线数”作为默认值。
终端标识码认证	启用终端标识码认证。用户在登录虚拟网关时，必须进行终端标识码认证。如果认证不通过，用户将无法登录虚拟网关。 只有在终端标识码认证全局开关启用的情况下，才能配置此参数。
虚拟 IP 地址	指定使用网络扩展业务时分配给用户的虚拟 IP 地址。只有在已经启用网络扩展业务的情况下才能配置虚拟 IP 地址。如果配置了与用户父组绑定的虚拟 IP 地址池，那么该虚拟 IP 地址必须在该虚拟 IP 地址池中；如果没有配置与用户父组绑定的虚拟 IP 地址池，那么该虚拟 IP 地址只要包含在本虚拟网关的网络扩展 IP 地址池中即可。 同一个虚拟虚拟网关内，分配给用户的虚拟 IP 地址是唯一的。
NFS 用户 ID	指定用户组对应的 NFS 文件系统的用户 ID（UID），用于用户使用 NFS 类型的文件共享时的权限控制。 NFS 文件系统通过组 ID（GID）和用户 ID（UID）控制不同组/用户的文件读写权限，这里配置的用户 ID 需要与服务器上的用户 ID 相同。

参数	说明
NFS 组 ID	指定用户组对应的 NFS 文件系统的组 ID（GID），用于用户使用 NFS 类型的文件共享时的权限控制。 NFS 文件系统通过组 ID（GID）和用户 ID（UID）控制不同组/用户的文件读写权限，这里配置的组 ID 需要与服务器上的组 ID 相同。

5. 关联访问控制策略组。

   访问控制策略组用于在角色授权的基础上，对用户/组进行细化的访问控制，包括基于源 IP、目的 IP/端口、URL 的访问控制。例如授权中指定用户组可以使用网络扩展业务，也就是用户组内用户可以访问所有的内网 IP 资源，此时可以通过配置基于目的 IP/端口的访问控制策略进一步限制用户访问的资源。访问控制策略组的具体配置请参见访问控制策略组。

   . 选择“策略组配置”页签。

   a. 单击“新建”，关联访问控制策略组。

参数	说明
ACL 组	选择关联的访问控制策略组。只能选择已经创建的访问控制策略组（“SSL VPN > 用户 > 访问控制组管理”）。
优先级	输入访问控制策略组的优先级。优先级取值越小的策略组越优先匹配。如果没有匹配任何策略组就匹配缺省动作（“系统 > 虚拟网关级策略 > 策略默认行为”）。 **说明：** 用户最终的访问权限，是用户所属直接父组和用户自身所关联的访问控制策略组的并集，因此 SVN 根据所有这些策略的配置及优先级最终决定用户的访问权限。具体匹配原则请参见用户授权。
行为	指定策略的行为动作，包括限制和允许访问策略中指定的 IP、URL 等资源。

   b. 单击“确定”。

6. 单击“确定”。

   配置完成后，在新创建用户所属父组的“成员管理”中可以查看到该用户的信息。

后续处理

组和用户创建完成后，可以使用如下操作进行调整：

- **添加已有用户**

将已经存在的用户添加到现有的组中。一个用户最多可以被加入到三个父组中，如果某用户加入的父组已达到上限，则该用户无法再加入新父组。

1. 在“组织结构”中单击待添加已有用户的组，然后在“成员管理”中，单击“新建”，选择“添加已有用户”。
2. 在“组织结构”中选中已经存在的用户，该用户将会出现在“已选用户”中。
3. 单击“确定”。

- **移动**

如果组或用户的父组发生变更，可以使用移动功能将用户或组移动到其他组中，以此来调整组织结构。

此外，通过调整“组成员”中的“组路径”，也可以实现移动组的目的。

1. 在“组织结构”中单击待移动组或用户所在的组，然后在“成员管理”中，选中所有待移动的组或用户，单击“移动”。
2. 在“组织结构”中，选中目的组，单击“确定”。

   移动时，目的组只能选择一个。

- **导出**

导出用户/组是指将用户信息以 CSV 文件的格式导出到 SVN 之外的存储介质上。管理员可以将用户/组导出到 CSV 文件中作为备份，后续也可以将导出的 CSV 文件再导入到设备中，实现批量创建用户/组的需求。如何导入 CSV 文件，请参见手动批量导入用户/组。

说明：

当 SVN 的 CF 卡剩余空间小于 4MB 时，不允许将用户信息导出到 CSV 文件中。

1. 在“组织结构”中单击待导出用户所属的父组或单击待导出的组，然后在“成员管理”中单击“导出”。

   当某个组下没有用户时，此组不支持单独导出。

2. 将以当前组的名称命名的 CSV 文件保存到 SVN 之外的存储介质（如管理员的 PC）上。

用户信息导出到 CSV 文件中后，密码以密文形式存放。

- **查看关联信息**

  查看关联信息方便管理员一站式查看用户/组关联的资源、访问控制策略以及角色，并支持导出。

  1. 在“组织结构”中单击待查看关联信息的组或用户，然后在“成员管理”中，单击组或用户对应的  。
  2. 在弹出的对话框中查看具体关联信息。

配置认证选项

介绍密码强度、用户登录失败锁定等认证选项的配置方法。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 用户 > 认证选项”。
3. 配置认证选项参数。

参数	说明
密码选项设置 以下配置只适用于本地认证的用户在 SSL VPN 虚拟网关页面修改密码的情况。	
密码强度设置	设置密码的高、中、低强度。
首次登录必须修改密码	选中复选框，表示用户在首次登录时必须修改密码。 不选中复选框，表示用户在首次登录时不需要修改密码。
密码过期设置	• 永不过期 表示密码永远都不过期。 • 过期时间设置 表示密码在指定的时间后过期。同时还可以设置在密码过期前提醒用户的时间，当用户在密码过期提醒时间之内登录后，将会跳转到密码过期提示页面，设备会提示用户需要修改密码。如果过期不修改将无法登录虚拟网关。
用户登录锁定配置 以下配置只有在“SSL VPN > 用户 > 用户登录锁定”中启用了用户登录锁定功能才生效。	
以何种特征锁定用户	选择以何种特征锁定用户。

参数	说明
	• 用户名：指锁定所有使用此用户名登录的用户。如果在“SSL VPN > 认证授权 > 认证授权方式”中启用了“允许一个账号在多处同时登录”，不能设置为用户名锁定方式。 • 源 IP：指锁定所有使用此源 IP 登录的用户。此种方式不适用于 NAT 接入的场景。
用户登录错误次数限制	输入用户认证失败次数的阈值，当用户连续认证失败次数达到阈值后，该用户将被锁定。
用户锁定时间	输入用户被锁定的时间。该锁定时间不受系统时间改变和夏令时调整的影响，在锁定时间内，设备不允许被锁定用户进行认证。

4. 单击“应用”。

配置访问控制策略组

访问控制策略组用于对用户/组进行细化的访问控制，在通过角色授权访问资源的基础上可以通过访问控制策略组对用户/组基于 IP、URL 等进行进一步的控制。访问控制策略组需要绑定到用户/组生效。

背景信息

在配置角色授权中可以基于角色为用户、组分配允许访问的资源，但是在某些情况下需要进行细化控制，例如：角色授权中指定用户组可以使用网络扩展业务，也就是用户组内用户可以访问相同的内网 IP 资源，如果需要额外禁止某些用户访问某些 IP 资源，此时可以配置禁止用户访问这些目的 IP 地址的访问控制策略组。

访问控制策略组由不同类型的访问控制策略组成：

- 源 IP 型：通过用户的源 IP 地址来控制用户访问虚拟网关的权限。用户通过被限制的源 IP 登录时，即使用户名、密码正确也无法成功登录虚拟网关。
- 目的 IP 型：通过目的 IP、端口控制用户访问内网资源的权限。
- URL 型：通过 URL 控制用户访问内网资源的权限。

访问控制策略组中仅配置需要控制的项目，具体控制动作（允许/限制）在将策略组应用到用户/组时指定，具体参见手动创建用户/组。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。

2. 选择“SSL VPN > 用户 > 访问控制组管理”。

3. 单击“新建”，输入访问控制策略组的名称和描述。

4. 配置策略组成员。

   a. 在策略列表中单击“新建”。

   b. 配置访问控制策略参数。

参数	说明
策略类型	选择策略类型，包括源 IP、目的 IP 和 URL 型。 源 IP 型策略只能配置 IP 地址，目的 IP 型策略可以配置 IP 地址、协议和端口，URL 型策略可以配置 URL、协议和端口。
IP 类型	选择是否控制“任意 IP”。如果选中“任意 IP”则不能再输入具体 IP 地址。
IP 地址/IP 段	输入控制的具体 IP 地址或 IP 地址段。
协议类型	选择控制的协议类型。
端口类型	选择是否控制“任意端口”。如果选中“任意端口”则不能再输入具体端口。
端口/端口段	输入控制的具体端口或端口段。
URL 类型	选择是否控制“任意 URL”。如果选中“任意 URL”则不能再输入具体 URL。
URL	输入控制的具体 URL，支持通配符。 **说明：** • 有的服务器会进行跳转，会导致 URL 策略控制失效。例如配置了禁止访问 URL1 的策略，用户访问 URL1 时，服务器自动将其跳转到 URL2。因为策略没有禁止访问 URL2，导致可以访问。解决方法，策略中将 URL2 也设置为禁止访问或者使用宽泛的 URL 匹配策略。 • 对于 Web 代理资源，子 URL 的策略优先生效。如果子 URL 设置了访问控制策略，则父 URL 设置的策略对子 URL 不生效；如果子 URL 未设置访问控制策略，则继承父 URL 的策略。 • 对于文件共享资源，URL 父目录设置的策略规则自动对子目录自动生效。 • 应用于文件共享的 URL 策略必须使用“file://前缀”的格式。

   c. 单击“确定”。

   d. **可选：**继续配置其他策略组成员。

      单击“新建”或选中已有的某条策略单击“复制”。

5. 单击“确定”。

后续处理

访问控制策略组配置完毕后，需要关联到用户或用户组并指定控制动作才能生效，具体参见手动创建用户/组。

配置认证授权方式

选择虚拟网关的认证授权方式，每个虚拟网关下的所有用户都采用相同的认证授权方式。

背景信息

认证授权方式含义如下：

- 认证方式：验证登录虚拟网关用户身份的方式，包括本地认证、服务器认证和证书认证。
- 授权方式：获取用户授权组信息的方式，包括本地授权和服务器授权。SVN 根据获取的组信息查找 SVN 上对该组的权限配置从而进行授权。

  因此采用服务器授权方式时，SVN 上需要存在与服务器上同名的组信息，管理员可以通过服务器导入功能将服务器上的组信息导入到 SVN。

通常情况下认证、授权采用相同方式即可，也就是身份验证和授权组信息都是同一个来源。某些特殊情况下需要认证、授权分离才会配置不同的认证、授权方式。例如：某公司通过 AD 服务器对员工进行域认证，但是授权需要按照 LDAP 服务器上的组织结构进行权限分配，此时需要选择 AD 认证、LDAP 授权。

虚拟网关支持多级认证授权，可以配置三种认证授权方式并指定其优先级。虚拟网关先对用户执行高优先级的认证授权，如果认证或授权中任意一个无响应将会进行下一优先级的认证授权，直到认证授权通过。如果直到第三级还未通过，则认证授权失败。

说明：

只有在认证或授权服务器无响应时才会进行下一级认证授权，用户不存在、密码错误、组信息不存在等认证授权失败的情况不会进行下一级认证授权。

采用服务器授权方式时，如果 SVN 上不存在授权服务器返回的授权组，则 SVN 对用户的处理方式受“禁止不属于任何授权组的用户登录”选项控制。具体阅读下文的“禁止不属于任何授权组的用户登录”参数介绍。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 认证授权 > 认证授权方式”。
3. 配置基本参数。

参数	说明
需要用户提供证书	当选择证书匿名和证书挑战认证方式时，必须选中此选项。认证时用户需要提供证书。 该选项对于 L2TP over IPSec 登录的用户不生效。
启用对实服务器证书校验	在桌面云业务中，如果负载均衡网关通过 HTTPS 方式访问实服务器则需要对实服务器证书进行校验，此时需要在 SVN 上导入实服务器 CA 证书。
禁止 Web 登录	选中此选项表示禁止终端用户通过浏览器访问虚拟网关，此时只能通过独立网络扩展客户端、L2TP over IPSec 方式访问内网资源。
从授权服务器获取授权组信息	当认证授权服务器分离时，必须选中此选项；否则服务器授权方式无效，SVN 从认证服务器获取授权组信息。
禁止不属于任何授权组的用户登录	此选项仅适用于服务器授权用户，如果 SVN 上不存在授权服务器返回的授权组，有如下两种处理方式： • 选中此选项：禁止该用户登录虚拟网关。 • 未选中此选项：该用户使用 default 组的权限。
允许一个账号在多处同时登录	如果允许用户使用一个账号在多处同时登录虚拟网关，可选择此项，并设置“各账号的默认最大在线数”。 • 如果已经启用用户登录锁定功能（“SSL VPN > 用户 > 用户登录锁定”），并且锁定特征为“用户名”，则无法启用此功能。 • 用户默认使用“各账号的默认最大在线数”作为虚拟网关各账号的最大在线数。如果需要单独设置某个账号的最大在线数，请在“SSL VPN > 用户 > 用户/组 > 成员管理”中进行设置。 • 此功能对 L2TP over IPSec 拨号登录的用户无效。 • 启用此功能时，请在“系统 > SSL 配置”中将“会话超时时间”设置为尽量小，以免未安全注销的用户账号占用并发用户数资源，建议保留默认值 5 分钟。 • 当 SVN 作为桌面云代理网关时，禁止启用此功能。

4. 配置认证授权方式。

参数	说明
认证方式	选择认证方式。包括本地认证、服务器认证（RADIUS/AD/LDAP/SecurID）、证书认证（证书匿名 Cert-anonymous、证书挑战 Cert-challenge） 不同优先级的认证方式不允许相同。 当采用证书认证时不支持多级认证授权。

参数	说明
辅助认证方式	当采用证书挑战 Cert-challenge 认证方式时，需要配置辅助认证方式进一步进行密码认证。
授权方式	选择授权方式。包括本地授权、服务器授权（RADIUS/AD/LDAP/SecurID）。 不同优先级的授权方式不允许相同。

5. 单击“应用”。

配置 RADIUS 服务器

当采用 RADIUS 服务器进行认证授权时，请配置 SVN 与 RADIUS 服务器的对接参数。

背景信息

一个虚拟网关只能配置一个 RADIUS 服务器。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 认证授权 > RADIUS 服务器”。
3. 配置 RADIUS 服务器的参数。

> **说明：**
>
> 在 SVN 上配置的参数必须与 RADIUS 服务器上的参数保持一致。

参数	说明
服务器信息	
主用服务器 IP 地址/端口	输入提供认证服务的主用 RADIUS 服务器的 IP 地址和端口号。 一般情况下，RADIUS 服务器提供认证服务时使用的端口号为 1812。
备用服务器 IP 地址/端口	输入提供认证服务的备用 RADIUS 服务器的 IP 地址和端口号。 SVN 会优先使用主用 RADIUS 服务器，当主用 RADIUS 服务器不可达时，才会使用备用 RADIUS 服务器。
基本信息	
服务器的应答超时时间	输入 SVN 等待 RADIUS 服务器应答的超时时间。 为判断某个 RADIUS 服务器是否失效，SVN 会向 RADIUS 服务器周期性地发送请求报文，如果在该时间内未得到 RADIUS 服务器发回的应答，需重传请求报文。

参数	说明
服务器的重传次数	输入 SVN 发送请求报文的重传次数。 SVN 向 RADIUS 服务器发出请求报文后，如果在“服务器的应答超时时间”内未得到 RADIUS 服务器发回的应答，SVN 需重传请求报文。重传次数超该值后，SVN 认为 RADIUS 服务器已不能正常工作。
组过滤字段	选择使用 RADIUS 服务器用户的 Class 还是 Filter-ID 字段作为组名进行授权，当采用 RADIUS 授权方式时需要配置此参数。 组过滤字段的配置要和 RADIUS 服务器上的配置相对应，否则可能授权不通过。SVN 最多可以获取四个 Class 或者 Filter-ID 属性用于授权，多余的将被丢弃，即一个 RADIUS 用户在登录虚拟网关时，如果属于四个以上的 RADIUS 组，多余的组属性将被丢弃。
共享密钥	输入 SVN 与 RADIUS 服务器通信时使用的共享密钥。 SVN 与 RADIUS 服务器使用该密钥对传输的报文进行加密。
确认共享密钥	再次输入共享密钥进行确认。

4. 单击“检测”。在弹出的窗口中输入测试账号及密码，单击“开始检测”，检测 RADIUS 服务器的连通性。

   说明：

   用于测试服务器连通性的用户名和密码可以为任意值，不需要与服务器端保持一致。

5. 单击“应用”。

配置图形检验码认证

图形检验码认证用于防止机器登录和暴力破解密码。启用图形校验码功能后，用户登录虚拟网关时必须手工输入随机产生的图形检验码。

操作步骤

1. 在界面右上角的“虚拟网关”中选择虚拟网关名称，进入对应的虚拟网关。
2. 选择“SSL VPN > 辅助认证 > 图形检验码认证”。
3. 选中“图形校验码”对应的“启用”，启用图形校验码认证。
4. 输入图形校验码失效时间，默认 3 分钟。

   图形验证码将在该失效时间后失效，用户需刷新后获取新的图形验证码输入。

认证授权规格

认证授权特性的规格如下：

项目	规格
认证方式	• 本地认证 • 服务器认证：RADIUS/LDAP/AD/SecurID（双因子认证） • 证书认证：证书匿名和证书挑战 • 辅助认证：终端标识码认证、图形校验码认证
授权方式	授权方式指从哪里获取授权组信息，实际业务授权通过角色完成。 • 本地授权 • 服务器授权：RADIUS/LDAP/AD/SecurID
多级认证授权	支持 3 级认证授权，认证或授权服务器无响应时进行下一级认证授权。
认证授权服务器	RADIUS/LDAP/AD/SecurID 服务器，其中 LDAP 服务器支持 AD 和 Open LDAP 两种类型。 每种类型的服务器在一个虚拟网关中只能配置一台。
服务器导入	支持 AD/LDAP 服务器用户导入。
最大用户数	每个虚拟网关支持创建的最大用户数由创建虚拟网关时指定的规格决定。
最大角色数	64

HCIE-Security 模拟面试问题及面试建议

1. SVN 有哪些认证授权方式？