域环境基础知识

域环境基础知识

1 内网工作环境

1.1 工作组

工作组（Work Group）是计算机网络的一个概念，也是最常见和最普通的资源管理模式，就是将不同的计算机按照功能或部门分别置于不同的组。试想，一个组织可能有成百上千台计算机，如果这些

计算机不进行分组，就会显得十分混乱。通过创建不同的工作组，不同的计算机可以按照功能或部门归属到不同的组内，整个组织的网络就会变得具有层次性。这样，只需在计算机的“网上邻居”中找到相应的工作组，就可以发现所包含的所有计算机，从而访问相应的资源。

要加入或创建工作组很简单。只需右击桌面上的“计算机”（或“此电脑”）图标，在弹出的快捷菜单中选择“属性”，在弹出的对话框中单击“更改设置”，然后在弹出的“系统属性”对话框中单击“更改”，在“计算机名”栏中输入自定义的主机名称，并在“工作组”栏中输入需要加入的工作组名称，单击“确定”按钮并重新启动计算机即可。注意，如果指定的工作组不存在，就会创建一个新的工作组。

在默认情况下，局域网内的计算机都是采用工作组方式进行资源管理的，即处在名 WORKGROUP的工作组中。

1.2 域

通过工作组对局域网的计算机进行分类，可以使资源的管理和访问更加层次化。但是工作组只适用于网络中计算机不多、资产规模较小、对安全管理控制要求不严格的情况。当组织中的网络规模越来越庞大时，需要统一的管理和集中的身份验证，并且能够为用户提供更加方便的网络资源搜索和使用方式时，就需要放弃工作组而使用域。

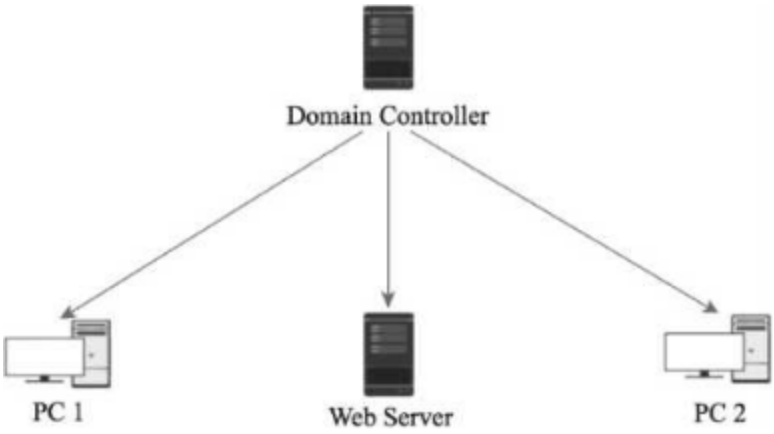
域（Domain）是一种比工作组更高级的计算机资源管理模式，既可以用于计算机数量较少的小规模网络环境，也可以用于计算机数量众多的大型网络环境。

在域环境中，所有用户账户、用户组、计算机、打印机和其他安全主体都在一个或多个域控制器的中央数据库中注册。当域用户需要想访问域中的资源时，必须通过域控制器集中进行身份验证。而通过身份验证的域用户对域中的资源拥有什么样的访问权限取决于域用户在域中的身份。

在域环境中，域管理员用户是域中最强大的用户，在整个域中具有最高访问权限和最高管理权限，可以通过域控制器集中管理组织中成千上万台计算机网络资源，所以在实际渗透过程中，能获得域管理员相关权限往往可以控制整个域控。

1.3 单域

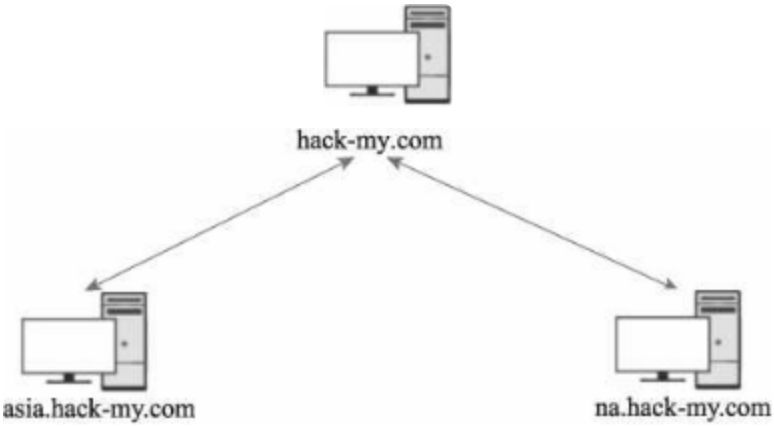
单域是指网络环境中只有一个域。在一个计算机数量较少、地理位置固定的小规模的组织中，建立一个单独的域，足以满足需求。



1.4 父域和子域

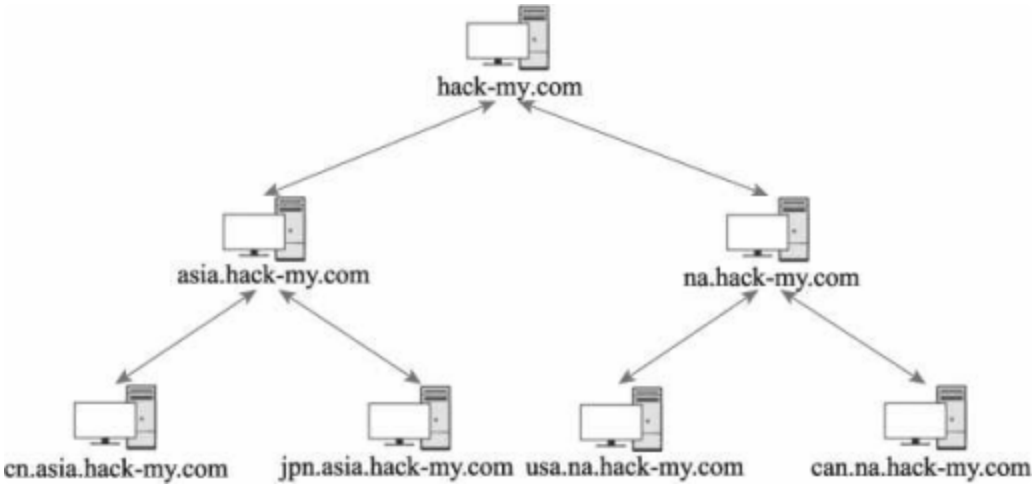
在有些情况下，为了满足某些管理需求，需要在一个域中划分出多个域。被划分的域称为父域，划分出来的各部分域称为子域。例如，一个大型组织的各部门位于不同的地理位置，这种情况下就可以把不同位置的部门分别放在不同的子域，然后部门通过自 己的域来管理相应的资源，并且每个子域都能拥有自己的安全策略。

从域名看，子域是整个域名中的一个段。各子域之间使用.来分割，一个就代表域名的一个层级。下图中 hack-my.com是父域，其余两个是其子域。



1.5 域树

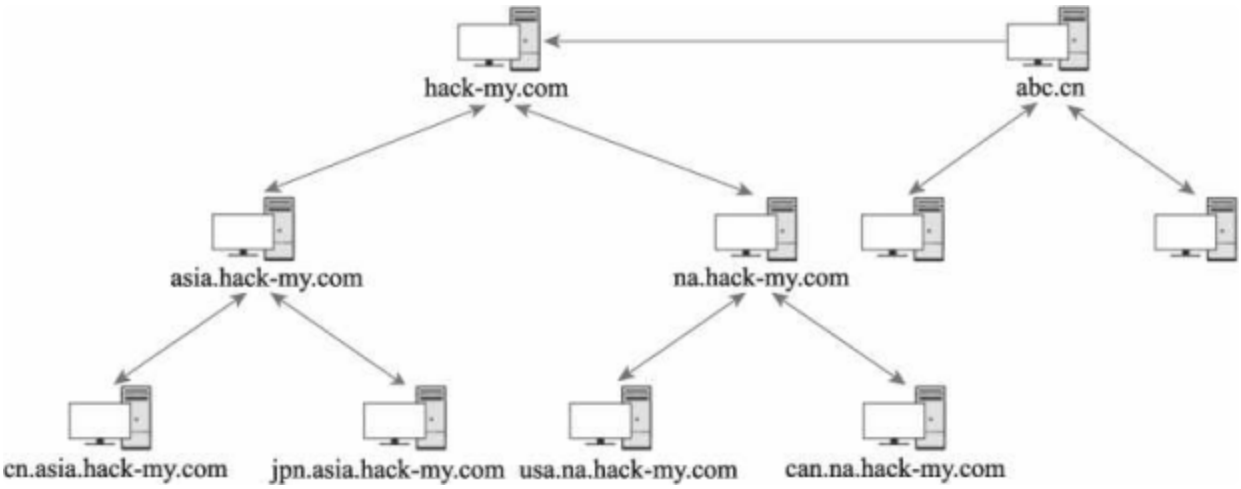
域树是多个域通过建立信任关系组成的一个域集合。在域树中，所有的域共享同一表结构和配置，所有的域名形成一个连续的名字空间，如下图所示，可以看出，域树中域的命名空间具有连续性，并且域名层次越深，级别越低



在域树中，域管理员只能管理本域，不能访问或者管理其他域。如果两个域之间需要互相访问，就需要建立信任关系(Trust Relation)。

1.6 域林

域林是指由一个或多个没有形成连续名字空间的域树组成域树集合，如图下图所示。域林与域树最明显的区别就是，域林中的域或域树之间没有形成连续的名字空间， 而域树是由一些具有连续名字空间的域组成。



1.7 域控制器

域控制器(Domain Controller, DC)是域环境核心的服务器计算机，用于在域中响应安全身份认证请求，负责允许或拒绝发出请求的主机访问域内资源，以及对用户进行身份验证、存储用户账户信息并执行域的安全策略等。可以说，域控制器是整个域环境的中控枢纽。域控制器包含一个活动目录数据库，其中存储着整个域的账户、密码、 计算机等信息。在技术领域，域控制器有时被简称为域控。

一个域环境可以拥有一台或多台域控制器，每台域控制器各自存储一份所在域的活动目录的可写副本，对活动目录的任何修改都可以从源域控制器同步复制到域、域树或 域林的其他控制器上。即使其中一台域控制器瘫痪，另一台域控制器可以继续工作，以保证域环境的正常运行。

1.8 活动目录

活动目录(Active Directory, AD)是指安装在域控制器上，为整个域环境提供集中式目录管理服务的组件。活动目录存储了有关域环境中各种对象的信息，如域、用户、 用户组、计算机、组织单位、共享资源、安全策略等。目录数据存储在域控制器的 Ntds.dit 文件中，文件路径为域控制器的 %SystemRoot%\ntds\ntds.dit ，文件中包括但不限于有关域用户、用户密码的哈希散列值、用户组、组成员身份和组策略的信息。活动目录主要提供了以下功能。

- 计算机集中管理：集中管理所有加入域的服务器及客户端计算机，统一下发组策略。
- 用户集中管理：集中管理域用户、组织通讯录、用户组，对用户进行统一的身份 认证、资源授权等。
- 资源集中管理：集中管理域中的打印机、文件共享服务等网络资源。
- 环境集中配置：集中的配置域中计算机的工作环境，如统一计算机桌面、统一网 络连接配置，统一计算机安全配置等。
- 应用集中管理：对域中的计算机统一推送软件、安全补丁、防病毒系统，安装网络打印机等。

1.9 域用户、机器用户、用户组介绍

1.9.1 域用户

域用户，顾名思义，就是域环境中的用户，在域控制器中被创建，并且其所有信息都保存在活动目录中。域用户账户位于域的全局组 Domain Users 中，而计算机本地用户账户位于本地 User s组中。当计算机加入域时，全局 Domain Users 会被添加到计算机本地的 Users 组中。因此，域用户可以在域中的任何一台计算机上登录。执行以下命令可以查看域中的所有域用户。

```
1   net user /domain
```

1.9.2 机器用户

机器用户其实是一种特殊的域用户。在域环境中，计算机上的本地用户 SYSTEM 对应域中的机器账户，在域中的用户名就是 机器名+$。执行以下命令可以查看域中所有的机器用户。当获取一台域中主

机的控制权后，发现没有域中用户凭据，此时可以利用一些系统 提权方法，将当前用户提升到 SYSTEM 以机器账户权限进行域内的操作。

```
net group "Domain Computers" /domain
```

1.9.3 域本地组

多域用户访问单域资源（访问同一个域）

可以从任何域添加用户账户、通用组和全局组，但只能在其所在域内指派权限。域本地组不能嵌套于其他组中。它主要是用于授予位于本域资源的访问权限。

1.9.5 全局组

单域用户访问多域资源（必须是一个域里面的用户）

只能在创建该全局组的域中添加用户和全局组。可以在域森林的任何域内指派权限。全局组可以嵌套在其他组中。

可以将某个全局组添加到同一个域的另一个全局组中，或者添加到其他域的通用组和域本地组中。

1.9.4 通用组

多域用户访问多域资源

通用组的成员可包括域树或域林中任何域的用户账号、全局组和其他通用组，可以在该域森林的任何域中指派权限，可以嵌套在其他组中，非常适合在域森林内的跨域访问中使用。

简单一句话概括：

- 域本地组：来自全林，作用于本域
- 全局组：来自本域，作用于全林
- 通用组：来自全林，作用于全林

wasj.com　　shanghai.wasj.com　　beijing.wasj.com

在

test 本地组 能从所有域中添加用户　但是只能在本域中指派权限

test2 全局组　　只能添加wasj.com当中的用户　　但是能在所有域中指派权限

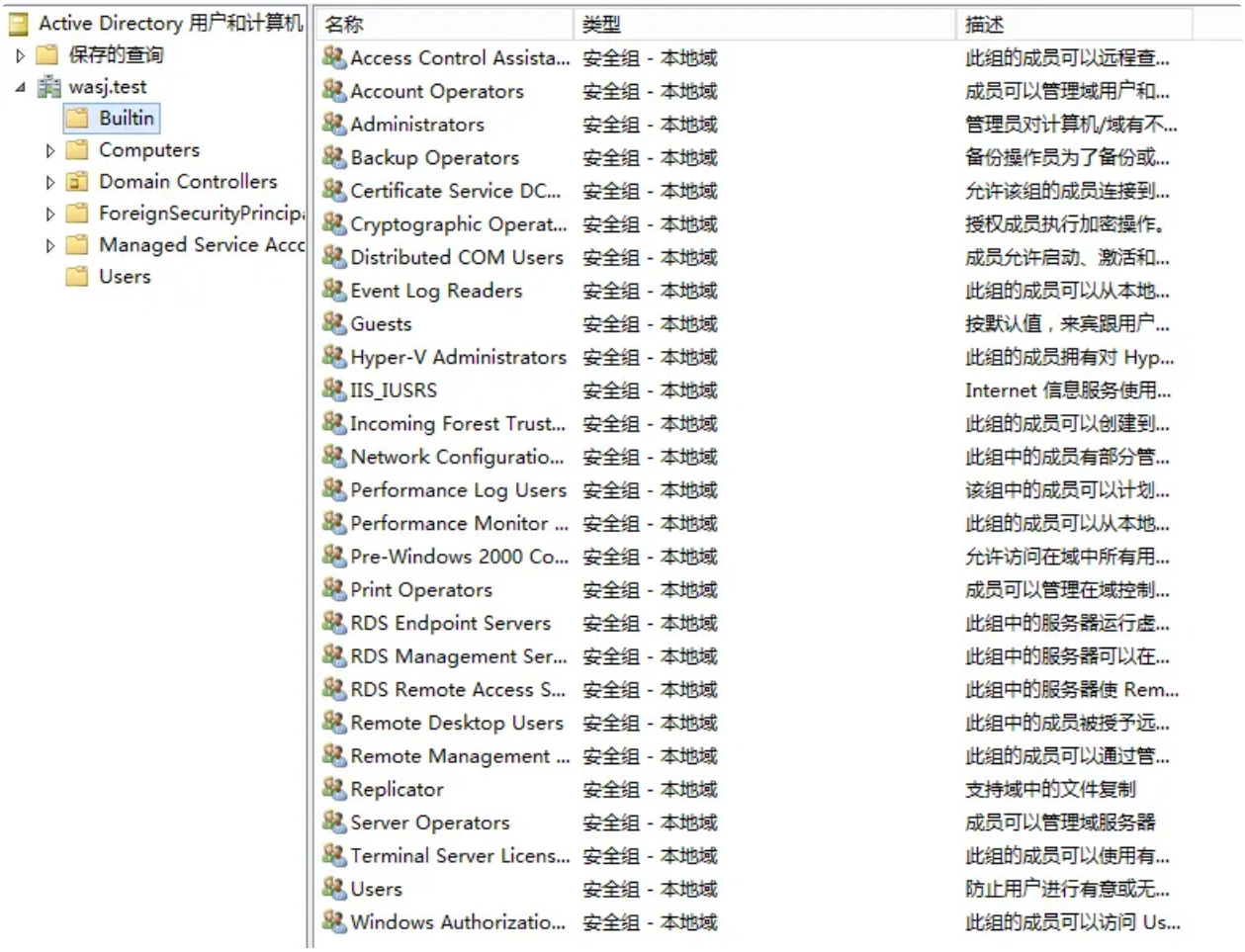
test 3 通用组　　能从所有域中添加用户 能在所有域中指派权限

内置组

在安装域控制器时，系统会自动生成一些组，称为内置组。内置组定义了一些常用的权限。通过将用户添加到内置组中可以使用户获得相应的权限。

活动目录控制台窗口的 Builtin 和 Users 组织单元中的组就是内置组。

- 内置的域本地组在 Builtin 组织单元中。
- 内置的全局组和通用组在 Users 组织单元中。



几个比较重要的域本地组

- **管理员组(Administrators)**：该组的成员可以不受限制地存取计算机/域内的资源。它不仅是最具权利的一个组，也是在活动目录和域控制器中默认具有管理员权限的组。该组的成员可以更改 Enterprise Admins、Schema Admins 和 Domain Admins 组的成员关系，是域森林中强大的服务管理组。
- **远程登录组(Remote Desktop Users)**：该组的成员具有远程登录权限。
- **打印机操作员组(Print Operators)**：该组的成员可以管理网络打印机，包括建立，管理及删除网络打印机，并可以在本地登录和关闭域控制器。
- **账号操作员组(Account Operators)**：该组的成员可以创建和管理该域中的用户和组并为其设置权限，也可以在本地登录域控制器。但是，不能更改属于Administrators或Domain Admins组的账号，也不能更改这些组。在默认情况下，该组中没有成员。
- **服务器操作员组(Server Operators)**：该组的成员可以管理域服务器，其权限包括建立、管理、删除任意服务器的共享目录、管理网络打印机、备份任何服务器的文件、格式化服务器硬盘、锁定服务器、变更服务器的系统时间、关闭域控制器等。在默认情况下，该组中没有成员。
- **备份操作员组(Backup Operators)**：该组的成员可以在域控制器中执行备份和还原操作，并可以在本地登录和关闭域控制器。在默认情况下，该组中没有成员。

几个比较重要的全局组、通用组的权限

- **域管理员组(Domain Admins)**：该组的成员在所有加入域的服务器、域控制器和活动目录中均默认拥有完整的管理员权限。因为该组会被添加到自己所在域的Administrators组中，因为可以继承Administrators组的所有权限。同时，该组默认会被添加到每台域成员计算机的本地Administrators组中。这样，Domain Admins组就获得了域中所有计算机的所有权。如果希望某用户成为域系统管

理员，建议将该用户添加到Domain Admins组中，而不要直接将该用户添加到Administrators组中。

- **企业系统管理员组(Enterprise Admins)**：该组是域森林根域中的一个组。该组在域森林中的每个域内都是Administrators组的成员，因此对所有域控制器都有完全访问权。
- **域用户组(Domain Users)**：该组是所有的域成员，在默认情况下，任何由我们建立的用户账号都属于Domain Users组，而任何由我们建立的计算机账号都属于Domain Computers组。因此，如果想让所有的账号都获得某种资源存取权限，可以将该权限指定给域用户组，或者让域用户组属于具有该权限的组。域用户组默认是内置域Users组的成员。
- **架构管理员组(Schema Admins)**：该组是域森林根域中的一个组，可以修改活动目录和域森林的模式。该组是为活动目录和域控制器提供完整权限的域用户组，因此，该组成员的资格是非常重要的。