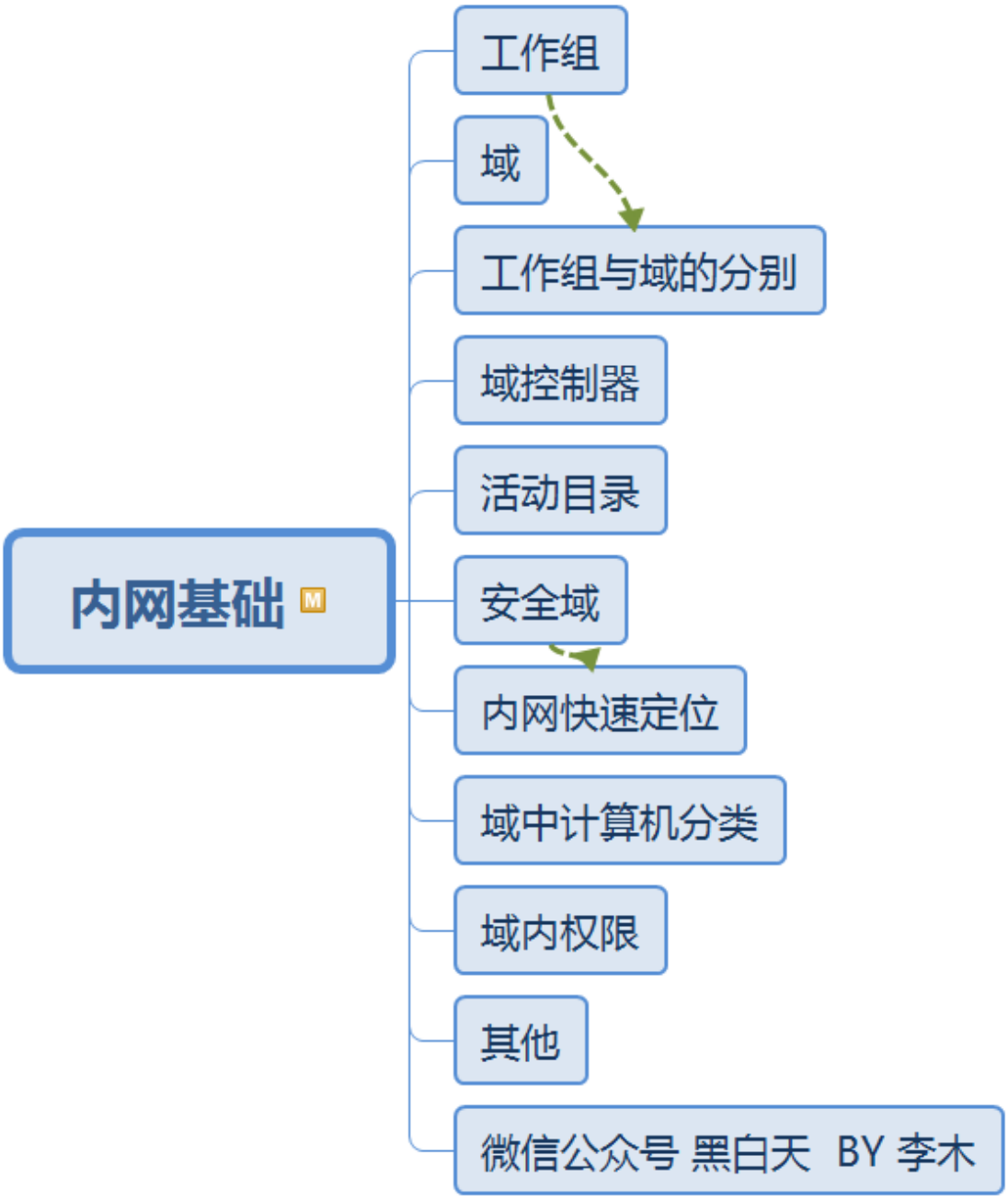
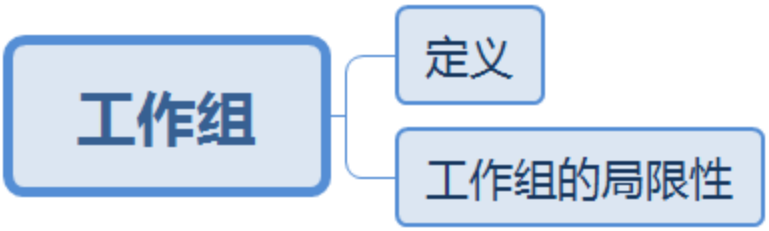
内网基础

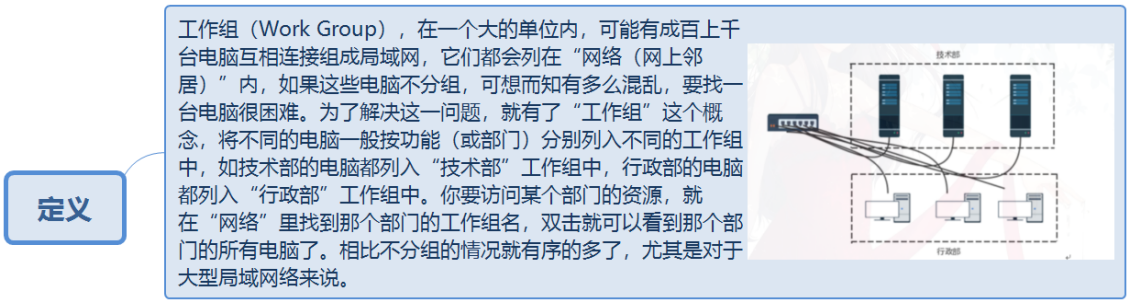

内网基础
工作组
域
工作组与域的分别
域控制器
活动目录
安全域
内网快速定位
域中计算机分类
域内权限
其他
微信公众号 黑白天 BY 李木

1. 工作组



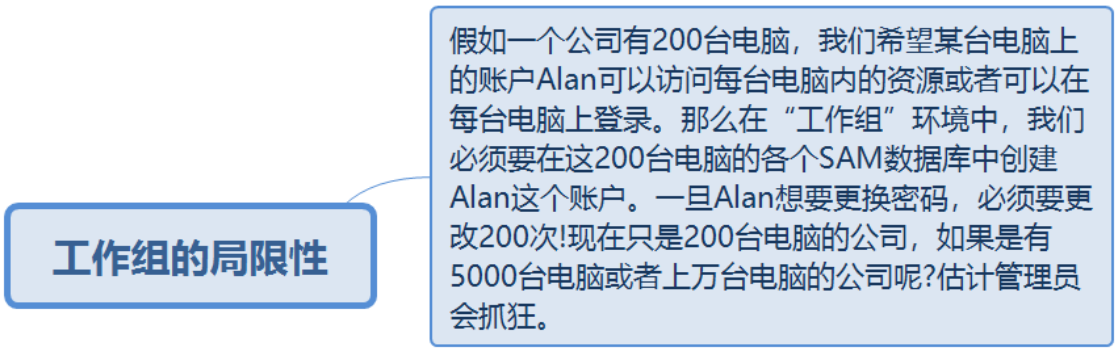
参见: [工作组与域的分别]

1.1. 定义



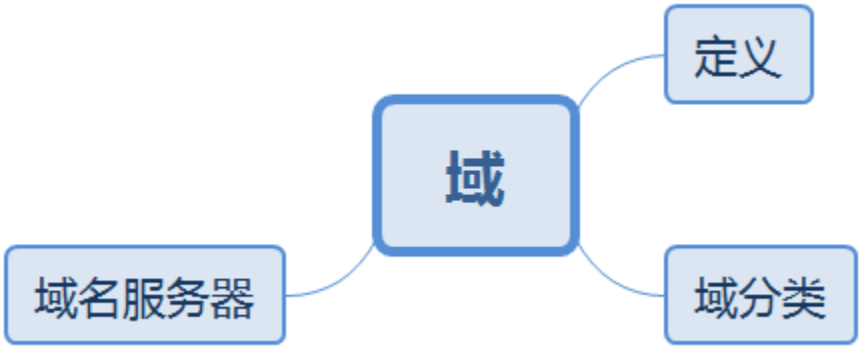
1.1.1. 工作组（Work Group），在一个大的单位内，可能有成百上千台电脑互相连接组成局域网，它们都会列在“网络（网上邻居）”内，如果这些电脑不分组，可想而知有多么混乱，要找一台电脑很困难。为了解决这一问题，就有了“工作组”这个概念，将不同的电脑一般按功能（或部门）分别列入不同的工作组中，如技术部的电脑都列入“技术部”工作组中，行政部的电脑都列入“行政部”工作组中。你要访问某个部门的资源，就在“网络”里找到那个部门的工作组名，双击就可以看到那个部门的所有电脑了。相比不分组的情况就有序的多了，尤其是对于大型局域网络来说。

1.2. 工作组的局限性

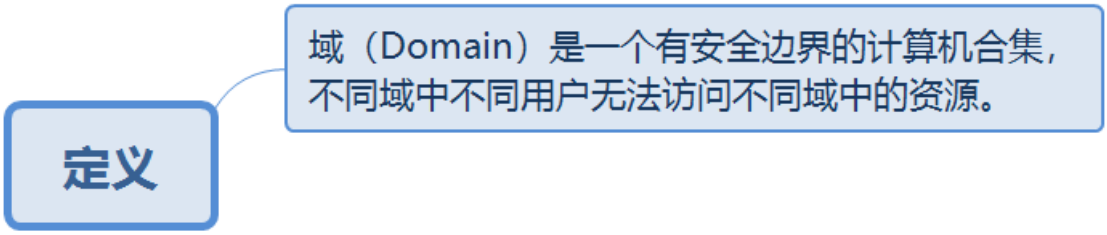


1.2.1. 假如一个公司有200台电脑，我们希望某台电脑上的账户Alan可以访问每台电脑内的资源或者可以在每台电脑上登录。那么在“工作组”环境中，我们必须要在这200台电脑的各个SAM数据库中创建Alan这个账户。一旦Alan想要更换密码，必须要更改200次!现在只是200台电脑的公司，如果是有5000台电脑或者上万台电脑的公司呢?估计管理员会抓狂。

2. 域



2.1. 定义



2.1.1. 域（Domain）是一个有安全边界的计算机合集，不同域中不同用户无法访问不同域中的资源。

参见: 工作组与域的分别

其实域和工作组在结构上很相似，只是表现形式有些不同：

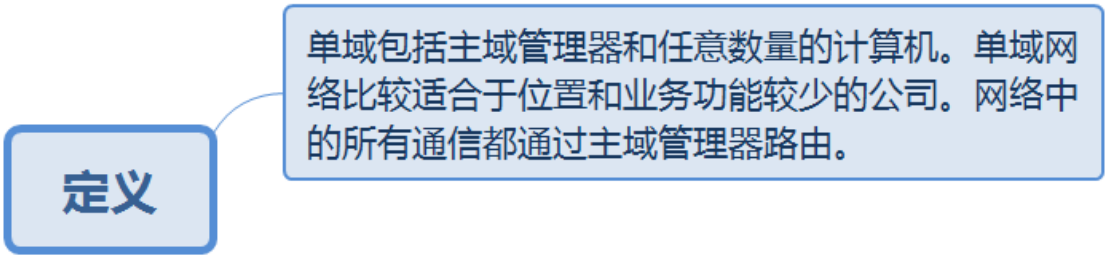
1、工作组：只能将数量不多的电脑连成一个可互相共享资源的网络，在这种工作方式下，信息的安全保护只能靠给共享信息设置密码或将使用权限设置给特殊用户来实现。

2、域：采用域控制器来进行信息管理，每个用户都有自己的账号和密码，并且可根据不同的情况赋予不同的使用权限，这种方式不但使网络信息安全得到了非常好的保障，同时也满足了大中型网络的要求

2.2. 域分类

2.2.1. 单域

2.2.1.1. 定义



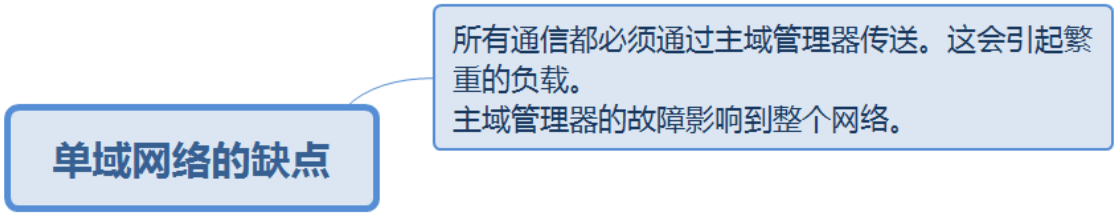
2.2.1.1.1. 单域包括主域管理器和任意数量的计算机。单域网络比较适合于位置和业务功能较少的公司。网络中的所有通信都通过主域管理器路由。

2.2.1.2. 单域网络的优点

2.2.1.2.1. 较为简单的体系结构。

中央控制和管理。

2.2.1.3. 单域网络的缺点

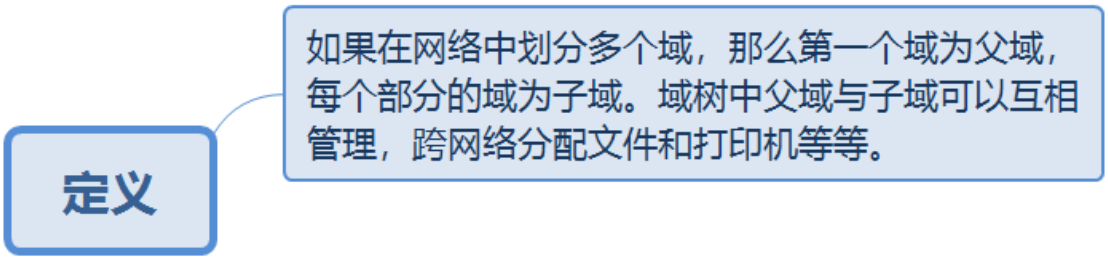


2.2.1.3.1. 所有通信都必须通过主域管理器传送。这会引起繁重的负载。

主域管理器的故障影响到整个网络。

2.2.2. 父子域

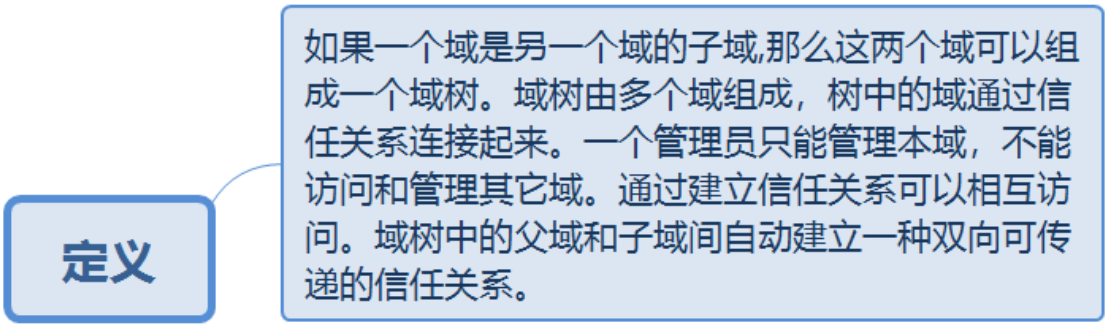
2.2.2.1. 定义



2.2.2.1.1. 如果在网络中划分多个域，那么第一个域为父域，每个部分的域为子域。域树中父域与子域可以互相管理，跨网络分配文件和打印机等等。

2.2.3. 域树

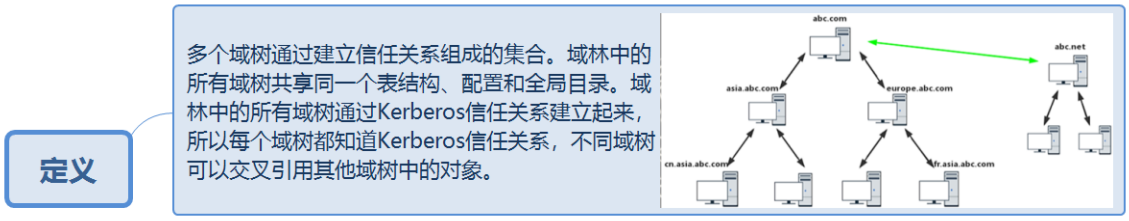
2.2.3.1. 定义



2.2.3.1.1. 如果一个域是另一个域的子域,那么这两个域可以组成一个域树。域树由多个域组成，树中的域通过信任关系连接起来。一个管理员只能管理本域，不能访问和管理其它域。通过建立信任关系可以相互访问。域树中的父域和子域间自动建立一种双向可传递的信任关系。

2.2.4. 域森林

2.2.4.1. 定义

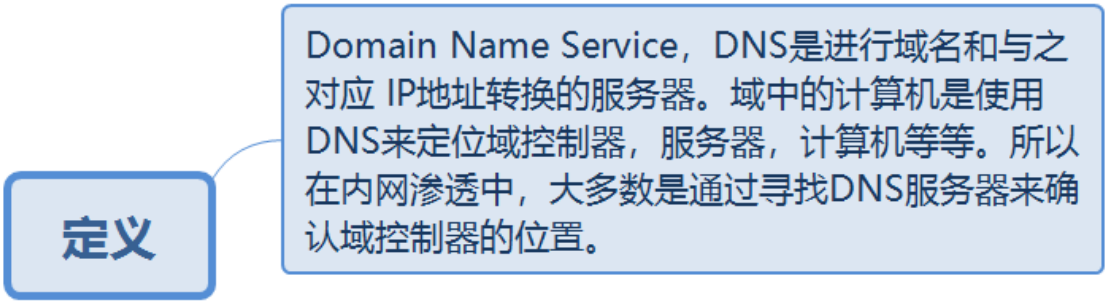


2.2.4.1.1. 多个域树通过建立信任关系组成的集合。域林中的所有域树共享同一个表结构、配置和全局目录。域林中的所有域树通过Kerberos信任关

系建立起来，所以每个域树都知道Kerberos信任关系，不同域树可以交叉引用其他域树中的对象。

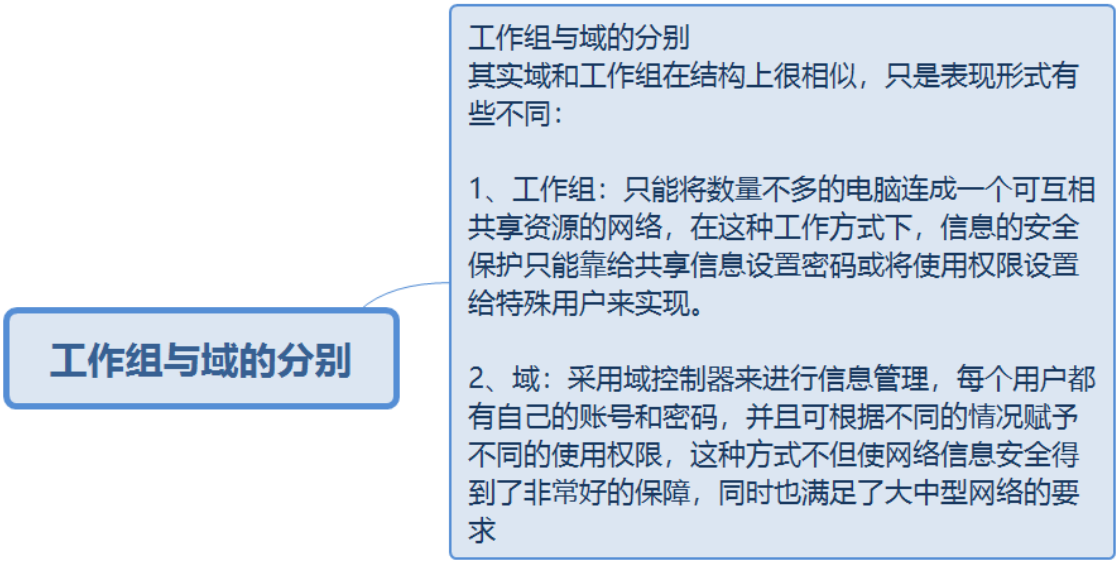
2.3. 域名服务器

2.3.1. 定义



2.3.1.1. Domain Name Service，DNS是进行域名和与之对应IP地址转换的服务器。域中的计算机是使用DNS来定位域控制器，服务器，计算机等等。所以在内网渗透中，大多数是通过寻找DNS服务器来确认域控制器的位置。

3. 工作组与域的分别



参见: 工作组

3.1. 工作组与域的分别

其实域和工作组在结构上很相似，只是表现形式有些不同：

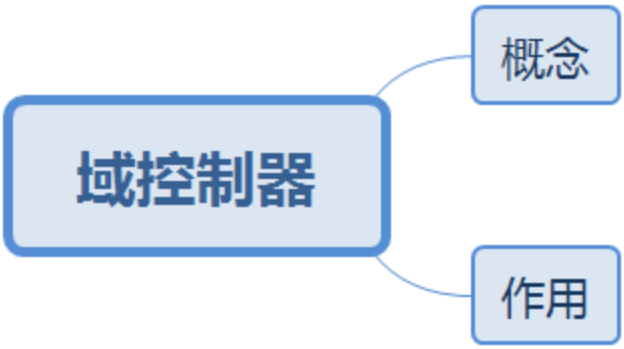
1、工作组：只能将数量不多的电脑连成一个可互相共享资源的网络，在这种工作方式下，信息的安全保护只能靠给共享信息设置密码或将使用权限设置给特殊用户来实现。

2、域：采用域控制器来进行信息管理，每个用户都有自己的账号和密码，并且可根据不同的情况赋予不同的使用权限，这种方式不但使网络信息安全得到了非常好的保障，同时也满足了大中型网络的要求

参见:

域(Domain)是一个有安全边界的计算机合集，不同域中不同用户无法访问不同域中的资源。

4. 域控制器

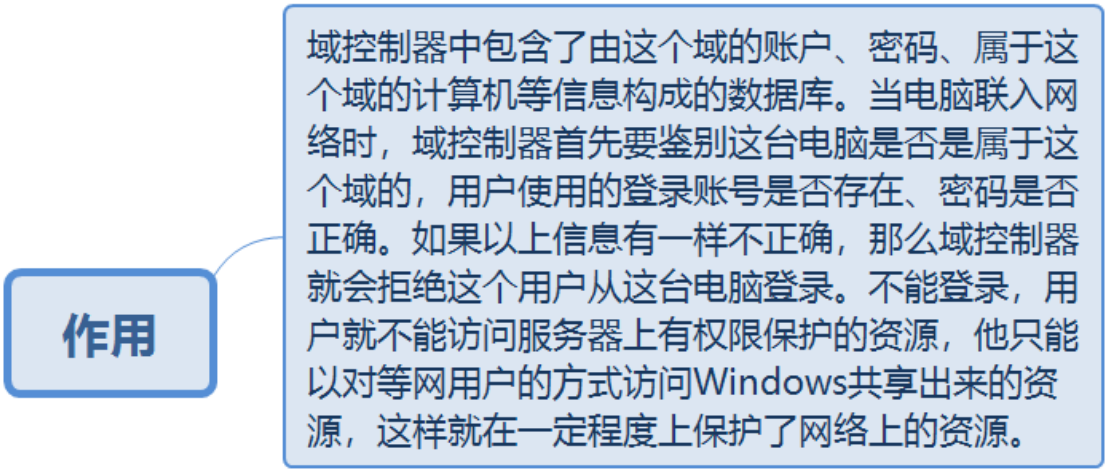


参见: 域控制器

4.1. 概念

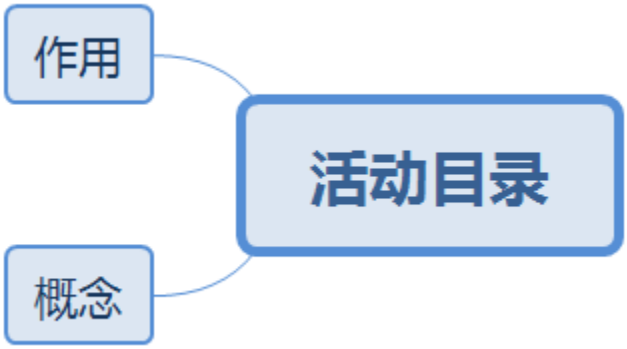
4.1.1. 域控制器是指在“域”模式下，至少有一台服务器负责每一台联入网络的电脑和用户的验证工作，相当于一个单位的门卫一样，称为“域控制器（Domain Controller，简写为DC）”。

4.2. 作用

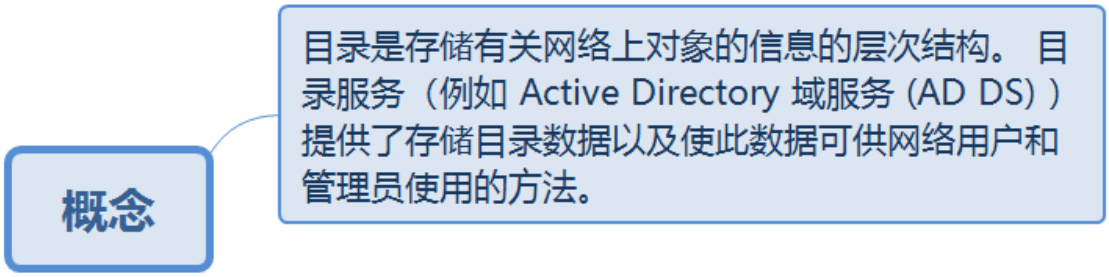


4.2.1. 域控制器中包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当电脑联入网络时，域控制器首先要鉴别这台电脑是否是属于这个域的，用户使用的登录账号是否存在、密码是否正确。如果以上信息有一样不正确，那么域控制器就会拒绝这个用户从这台电脑登录。不能登录，用户就不能访问服务器上有权限保护的资源，他只能以对等网用户的方式访问Windows共享出来的资源，这样就在一定程度上保护了网络上的资源。

5. 活动目录



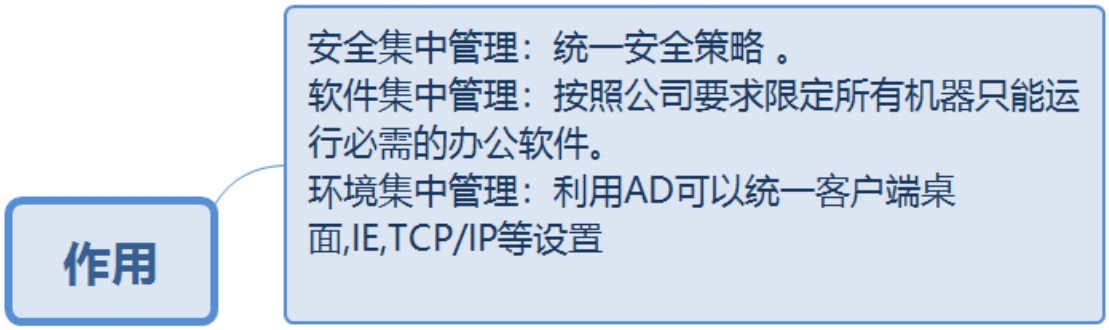
5.1. 概念



5.1.1. 目录是存储有关网络上对象的信息的层次结构。 目录服务（例如 **Active Directory** 域服务 **(AD DS)**

）提供了存储目录数据以及使此数据可供网络用户和管理员使用的方法。

5.2. 作用



5.2.1. 安全集中管理：统一安全策略 。

软件集中管理：按照公司要求限定所有机器只能运行必需的办公软件。

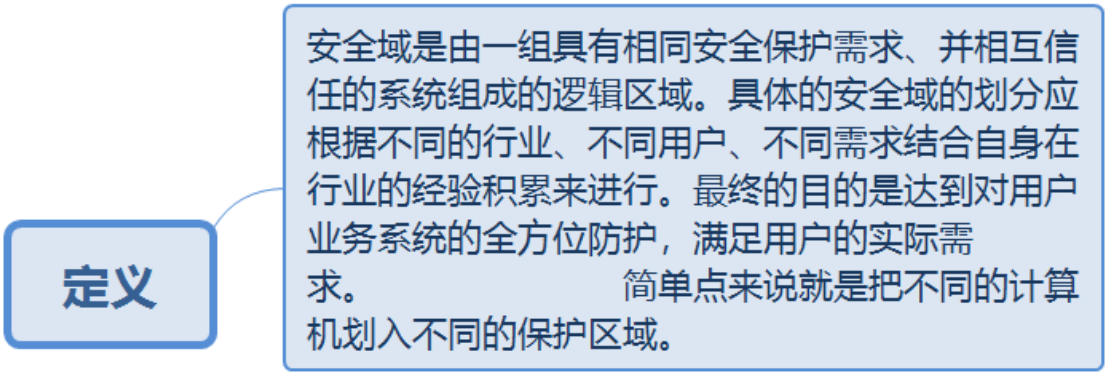
环境集中管理：利用**AD**可以统一客户端桌面**,IE,TCP/IP**等设置

6. 安全域

参见: 内网快速定位

6.1. 安全域基础知识

6.1.1. 定义

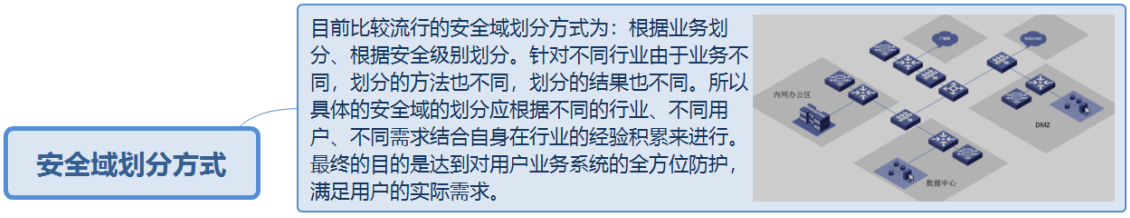


6.1.1.1. 安全域是由一组具有相同安全保护需求、并相互信任的系统组成的逻辑区域。具体的安全域的划分应根据不同的行业、不同用户、不同需求结合自身在行业的经验积累来进行。最终的目的是达到对用户业务系统的全方位

防护，满足用户的实际需求。

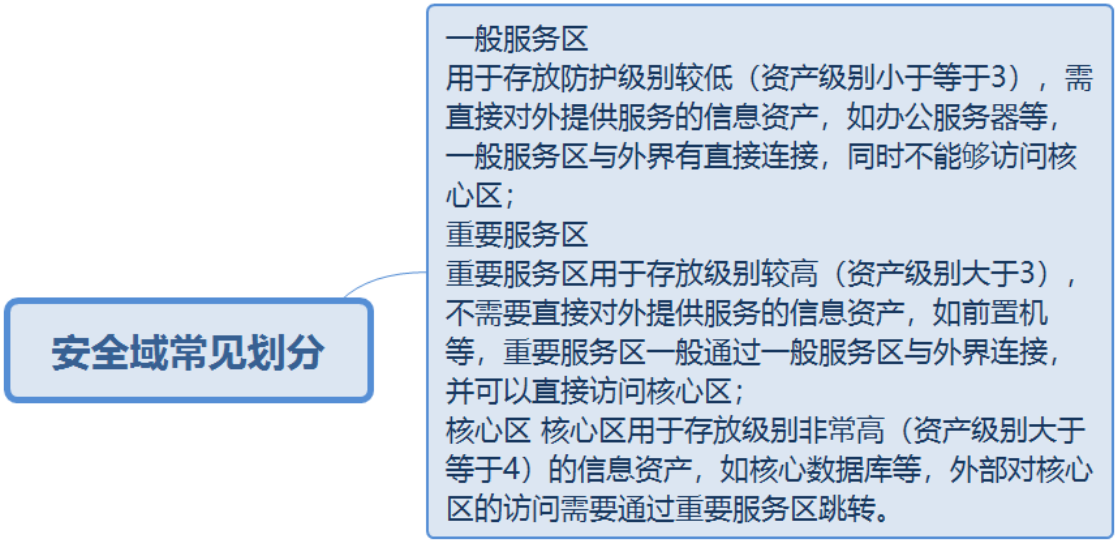
简单点来说就是把不同的计算机划入不同的保护区域。

6.1.2. 安全域划分方式



6.1.2.1. 目前比较流行的安全域划分方式为：根据业务划分、根据安全级别划分。针对不同行业由于业务不同，划分的方法也不同，划分的结果也不同。所以具体的安全域的划分应根据不同的行业、不同用户、不同需求结合自身在行业的经验积累来进行。最终的目的是达到对用户业务系统的全方位防护，满足用户的实际需求。

6.1.3. 安全域常见划分



6.1.3.1. 一般服务区

用于存放防护级别较低（资产级别小于等于**3**），需直接对外提供服务的信

息资产，如办公服务器等，一般服务区与外界有直接连接，同时不能够访问核心区；

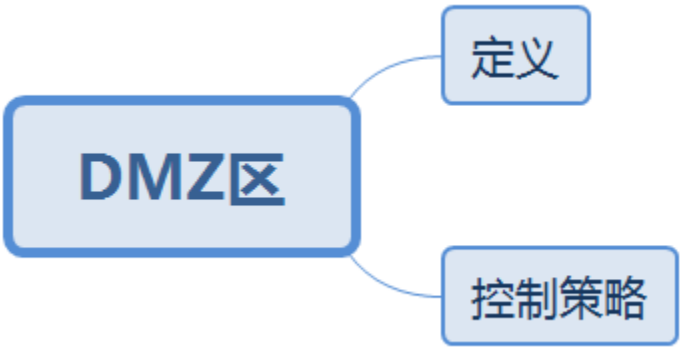
重要服务区

重要服务区用于存放级别较高（资产级别大于3），不需要直接对外提供服务的信息资产，如前置机等，重要服务区一般通过一般服务区与外界连接，并可以直接访问核心区；

核心区

核心区用于存放级别非常高（资产级别大于等于4）的信息资产，如核心数据库等，外部对核心区的访问需要通过重要服务区跳转。

6.2. DMZ区

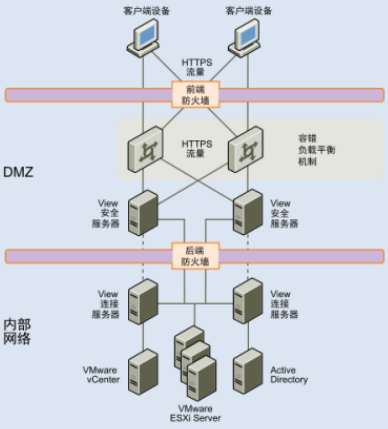


6.2.1. 定义

定义

两个防火墙之间的空间被称为DMZ。与Internet相比，DMZ可以提供更高的安全性，但是其安全性比内部网络低。

DMZ是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。该缓冲区位于企业内部网络和外部网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器设施，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络。因为这种网络部署，比起一般的防火墙方案，对来自外网的攻击者来说又多了一道关卡。
DNZ位于企业内网与外网之间，一般企业都会把web服务器，ftp服务器，代理服务器等等对外提供服务的服务器放在DNZ中。



DMZ可以理解为一个不同于外网或内网的特殊网络区域，DMZ内通常放置一些不含机密信息的公用服务器，比如Web、Mail、FTP等。这样来自外网的访问者可以访问DMZ中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使DMZ中服务器受到破坏，也不会对内网中的机密信息造成影响。
在DNZ中一般都有入侵检测，防火墙，WAF等等

我们可以将部分用于提供对外服务的服务器主机划分到一个特定的子网——DMZ内，在DMZ的主机能与同处DMZ内的主机和外部网络的主机通信，而同内部网络主机的通信会被受到限制。这使DMZ的主机能被内部网络和外部网络所访问，而内部网络又能避免外部网络所得知。
如果我们想要进入内网，我们就要通过DNZ的重重防御

6.2.1.1. 两个防火墙之间的空间被称为DMZ。与Internet相比，DMZ可以提供更高的安全性，但是其安全性比内部网络低。

DMZ是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。该缓冲区位于企业内部网络和外部网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服

务器设施，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络。因为这种网络部署，比起一般的防火墙方案，对来自外网的攻击者来说又多了一道关卡。
DNZ位于企业内网与外网之间，一般企业都会把web服务器，ftp服务器，代理服务器等等对外提供服务的服务器放在DNZ中。

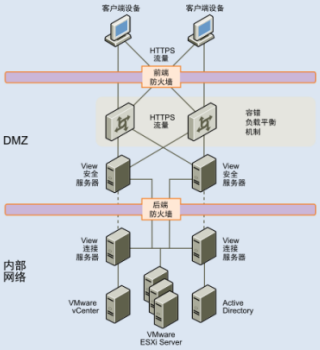
DMZ可以理解为一个不同于外网或内网的特殊网络区域，DMZ内通常放置一些不含机密信息的公用服务器，比如Web、Mail、FTP等。这样来自外网的访问者可以访问DMZ中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使DMZ中服务器受到破坏，也不会对内网中的机密信息造成影响。
在DNZ中一般都有入侵检测，防火墙，WAF等等

我们可以将部分用于提供对外服务的服务器主机划分到一个特定的子网——DMZ内，在DMZ的主机能与同处DMZ内的主机和外部网络的主机通信，而同内部网络主机的通信会被受到限制。这使DMZ的主机能被内部网络和外部网络所访问，而内部网络又能避免外部网络所得知。
如果我们想要进入内网，我们就要通过DNZ的重重防御

两个防火墙之间的空间被称为DMZ。与Internet相比，DMZ可以提供更高的安全性，但是其安全性比内部网络低。

DMZ是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。该缓冲区位于企业内部网络和外部网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器设施，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络。因为这种网络部署，比起一般的防火墙方案，对来自外网的攻击者来说又多了一道关卡。

DNZ位于企业内网与外网之间，一般企业都会把web服务器，ftp服务器，代理服务器等等对外提供服务的服务器放在DNZ中。



DMZ可以理解为一个不同于外网或内网的特殊网络区域，DMZ内通常放置一些不含机密信息的公用服务器，比如Web、Mail、FTP等。这样来自外网的访问者可以访问DMZ中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使DMZ中服务器受到破坏，也不会对内网中的机密信息造成影响。

在DNZ中一般都有入侵检测，防火墙，WAF等等

我们可以将部分用于提供对外服务的服务器主机划分到一个特定的子网——DMZ内，在DMZ的主机能与同处DMZ内的主机和外部网络的主机通信，而同内部网络主机的通信会被受到限制。这使DMZ的主机能被内部网络和外部网络所访问，而内部网络又能避免外部网络所得知。

如果我们想要进入内网，我们就要通过DNZ的重重防御

6.2.1.1.1.

6.2.2. 控制策略

6.2.2.1. 当规划一个拥有DMZ的网络时候,我们可以明确各个网络之间的访问关系,可以确定以下六条访问控制策略。

1.内网可以访问外网

内网的用户显然需要自由地访问外网。在这一策略中，防火墙需要进行源地址转换。

2.内网可以访问DMZ

此策略是为了方便内网用户使用和管理DMZ中的服务器。

3.外网不能访问内网

很显然，内网中存放的是公司内部数据，这些数据不允许外网的用户进行访问。

4.外网可以访问DMZ

DMZ中的服务器本身就是要给外界提供服务的，所以外网必须可以访问DMZ。同时，外网访问DMZ需要由防火墙完成对外地址到服务器实际地址的转换。

5.DMZ访问内网有限制

很明显，如果违背此策略，则当入侵者攻陷DMZ时，就可以进一步进攻到内网的重要数据。

6.DMZ不能访问外网

此条策略也有例外，比如DMZ中放置邮件服务器时，就需要访问外网，否则将不能正常工作。在网络中，非军事区(DMZ)是指为不信任系统提供服务的孤立网段，其目的是把敏感的内部网络和其他提供访问服务的网络分开，阻止内网和外网直接通信，以保证内网安全。

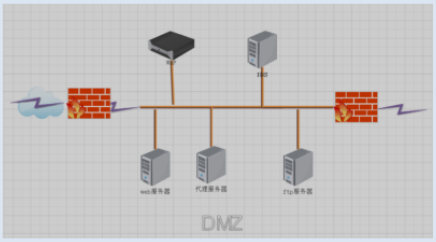
当规划一个拥有DMZ的网络时候,我们可以明确各个网络之间的访问关系,可以确定以下六条访问控制策略。

1.内网可以访问外网 内网的用户显然需要自由地访问外网。在这一策略中，防火墙需要进行源地址转换。

2.内网可以访问DMZ 此策略是为了方便内网用户使用和管理DMZ中的服务器。

3.外网不能访问内网 很显然，内网中存放的是公司内部数据，这些数据不允许外网的用户进行访问。

4.外网可以访问DMZ DMZ中的服务器本身就是要给外界提供服务的，所以外网必须可以访问DMZ。同时，外网访问DMZ需要由防火墙完成对外地址到服务器实际地址的转换。



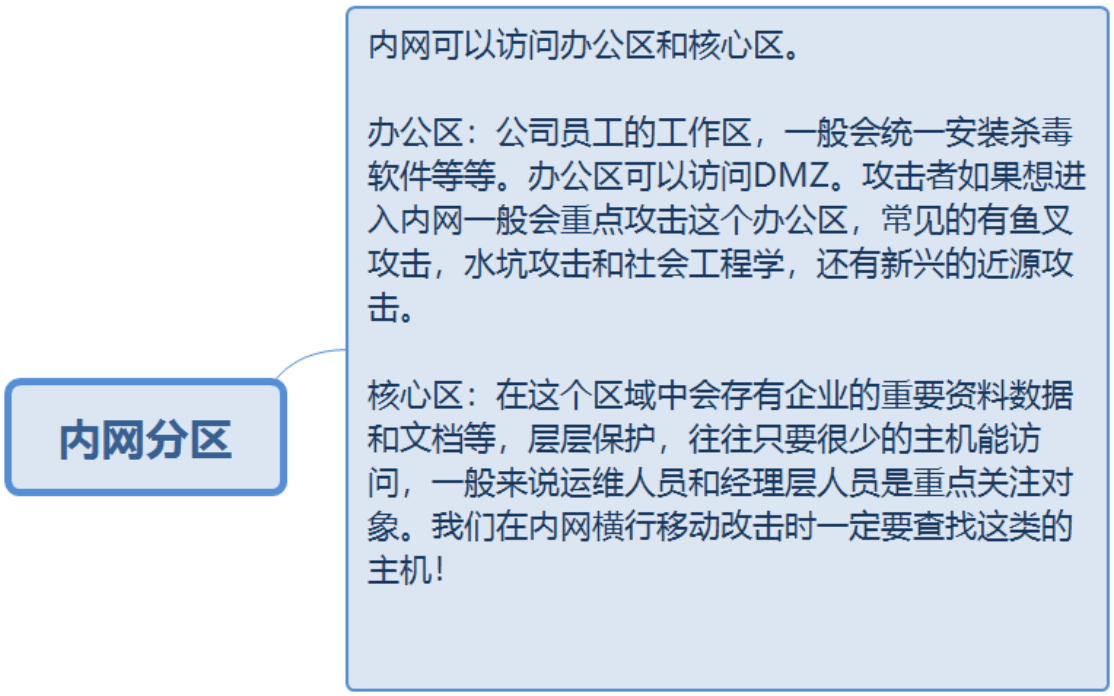
5.DMZ访问内网有限制 很明显，如果违背此策略，则当入侵者攻陷DMZ时，就可以进一步进攻到内网的重要数据。

6.DMZ不能访问外网

此条策略也有例外，比如DMZ中放置邮件服务器时，就需要访问外网，否则将不能正常工作。在网络中，非军事区(DMZ)是指为不信任系统提供服务的孤立网段，其目的是把敏感的内部网络和其他提供访问服务的网络分开，阻止内网和外网直接通信，以保证内网安全。

6.2.2.1.1.

6.3. 内网分区

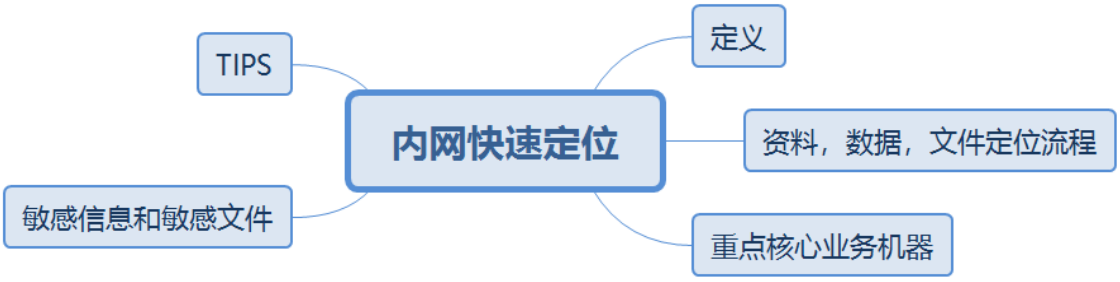


6.3.1. 内网可以访问办公区和核心区。

办公区：公司员工的工作区，一般会统一安装杀毒软件等等。办公区可以访问DMZ。攻击者如果想进入内网一般会重点攻击这个办公区，常见的有鱼叉攻击，水坑攻击和社会工程学，还有新兴的近源攻击。

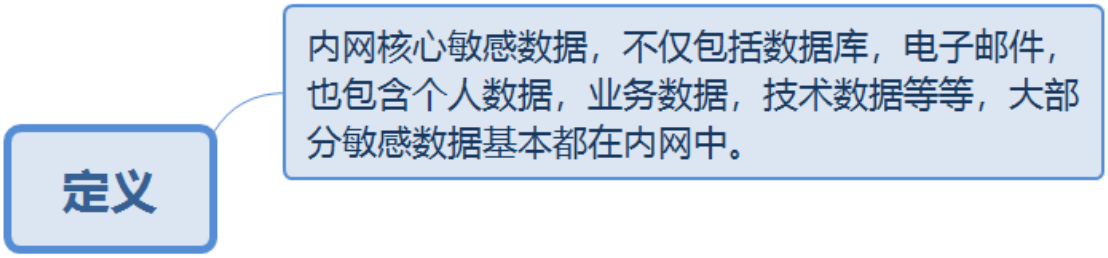
核心区：在这个区域中会存有企业的重要资料数据和文档等，层层保护，往往只要很少的主机能访问，一般来说运维人员和经理层人员是重点关注对象。我们在内网横行移动改击时一定要查找这类的主机！

7. 内网快速定位



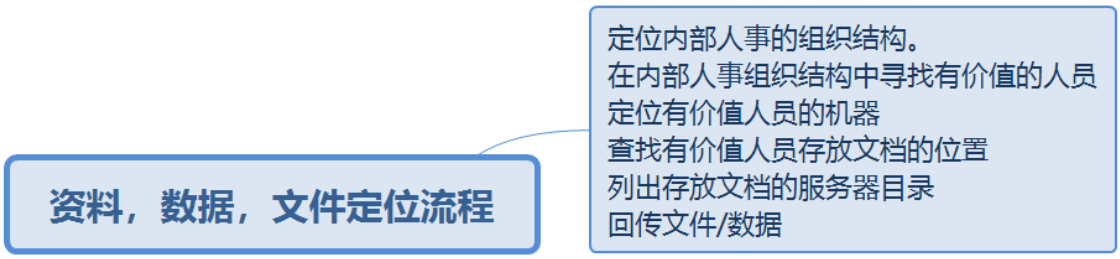
参见: 安全域

7.1. 定义



7.1.1. 内网核心敏感数据，不仅包括数据库，电子邮件，也包含个人数据，业务数据，技术数据等等，大部分敏感数据基本都在内网中。

7.2. 资料，数据，文件定位流程



7.2.1. 定位内部人事的组织结构。

在内部人事组织结构中寻找有价值的人员

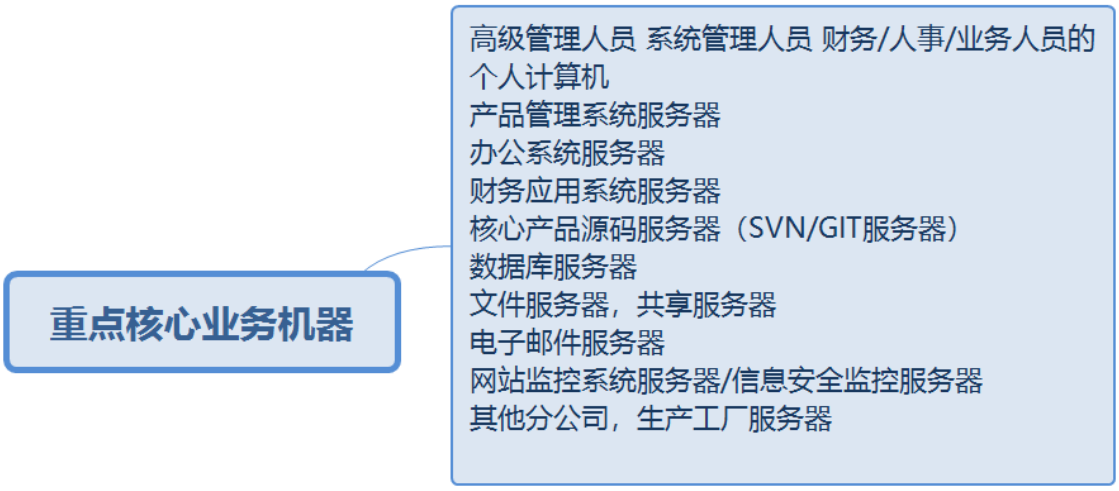
定位有价值人员的机器

查找有价值人员存放文档的位置

列出存放文档的服务器目录

回传文件/数据

7.3. 重点核心业务机器



7.3.1. 高级管理人员 系统管理人员 财务/人事/业务人员的个人计算机

产品管理系统服务器

办公系统服务器

财务应用系统服务器

核心产品源码服务器（SVN/GIT服务器）

数据库服务器

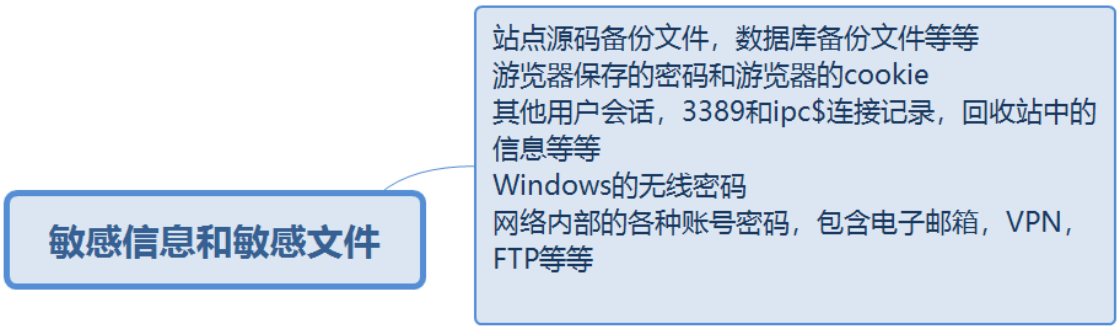
文件服务器，共享服务器

电子邮件服务器

网站监控系统服务器/信息安全监控服务器

其他分公司，生产工厂服务器

7.4. 敏感信息和敏感文件



7.4.1. 站点源码备份文件，数据库备份文件等等

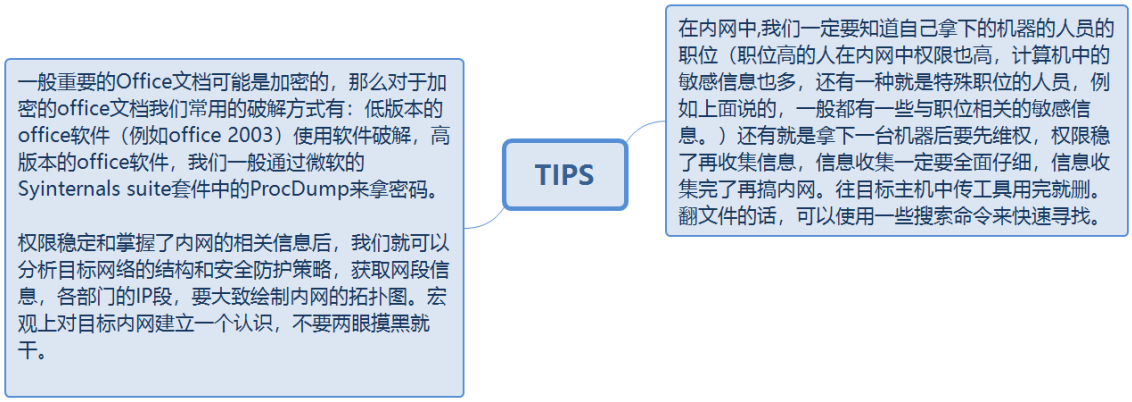
游览器保存的密码和游览器的cookie

其他用户会话，3389和ipc$连接记录，回收站中的信息等等

Windows的无线密码

网络内部的各种账号密码，包含电子邮箱，VPN，FTP等等

7.5. TIPS



7.5.1. 在内网中,我们一定要知道自己拿下的机器的人员的职位（职位高的人在内网中权限也高，计算机中的敏感信息也多，还有一种就是特殊职位的人员，例如上面说的，一般都有一些与职位相关的敏感信息。）还有就是拿下一台机器后要先维权，权限稳了再收集信息，信息收集一定要全面仔细，信息收集完了再搞内网。往目标主机中传工具用完就删。翻文件的话，可以使用一些搜索命令来快速寻找。

在内网中,我们一定要知道自己拿下的机器的人员的职位（职位高的人在内网中权限也高，计算机中的敏感信息也多，还有一种就是特殊职位的人员，例如上面说的，一般都有一些与职位相关的敏感信息。）还有就是拿下一台机器后要先维权，权限稳了再收集信息，信息收集一定要全面仔细，信息收集完了再搞内网。往目标主机中传工具用完就删。翻文件的话，可以使用一些搜索命令来快速寻找。

1.指定目录下搜集各类敏感文件
dir /a /s /b d:\"*.txt"
dir /a /s /b d:\"*.xml"
dir /a /s /b d:\"*.mdb"
dir /a /s /b d:\"*.sql"
dir /a /s /b d:\"*.mdf"
dir /a /s /b d:\"*.eml"
dir /a /s /b d:\"*.pst"
dir /a /s /b d:\"*conf*"
dir /a /s /b d:\"*bak*"
dir /a /s /b d:\"*pwd*"
dir /a /s /b d:\"*pass*"
dir /a /s /b d:\"*login*"
dir /a /s /b d:\"*user*"
2.指定目录下的文件中搜集各种账号密码
findstr /si pass *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si userpwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si pwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si login *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si user *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak

7.5.1.1. 1.指定目录下搜集各类敏感文件

dir /a /s /b d:\"*.txt"

dir /a /s /b d:\"*.xml"

dir /a /s /b d:\"*.mdb"

dir /a /s /b d:\"*.sql"

dir /a /s /b d:\"*.mdf"

dir /a /s /b d:\"*.eml"

dir /a /s /b d:\"*.pst"

dir /a /s /b d:\"*conf*"

dir /a /s /b d:\"*bak*"

dir /a /s /b d:\"*pwd*"

dir /a /s /b d:\"*pass*"

dir /a /s /b d:\"*login*"

dir /a /s /b d:\"*user*"

2.指定目录下的文件中搜集各种账号密码

findstr /si pass *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak

findstr /si userpwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak

findstr /si pwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak

findstr /si login *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak

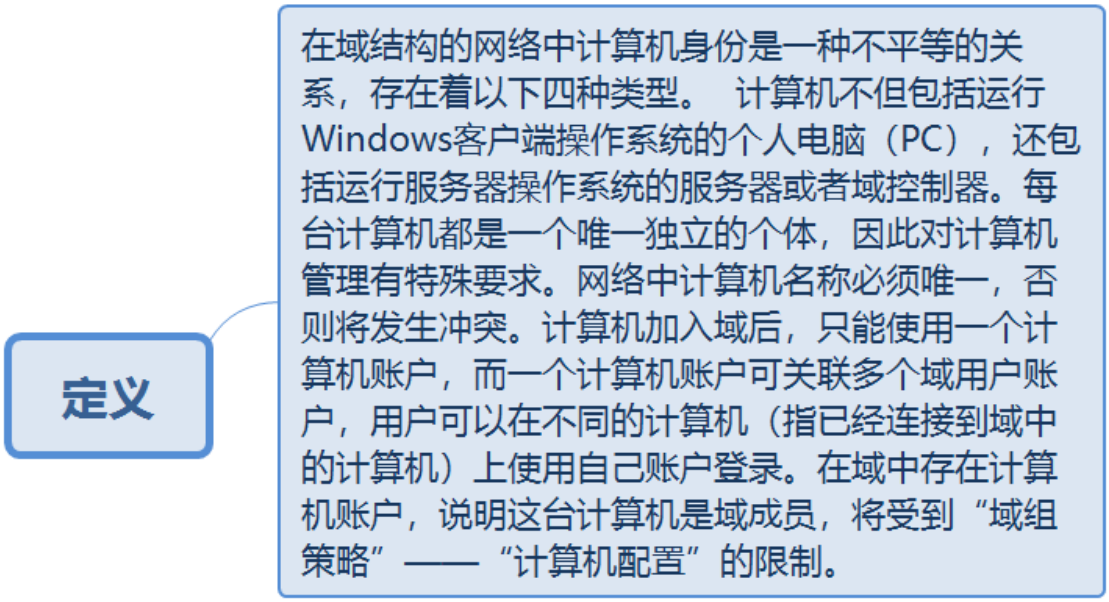
findstr /si user *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak

7.5.2. 一般重要的Office文档可能是加密的，那么对于加密的office文档我们常用的破解方式有：低版本的office软件（例如office 2003）使用软件破解，高版本的office软件，我们一般通过微软的Syinternals suite套件中的ProcDump来拿密码。

权限稳定和掌握了内网的相关信息后，我们就可以分析目标网络的结构和安全防护策略，获取网段信息，各部门的IP段，要大致绘制内网的拓扑图。宏观上对目标内网建立一个认识，不要两眼摸黑就干。

8. 域中计算机分类

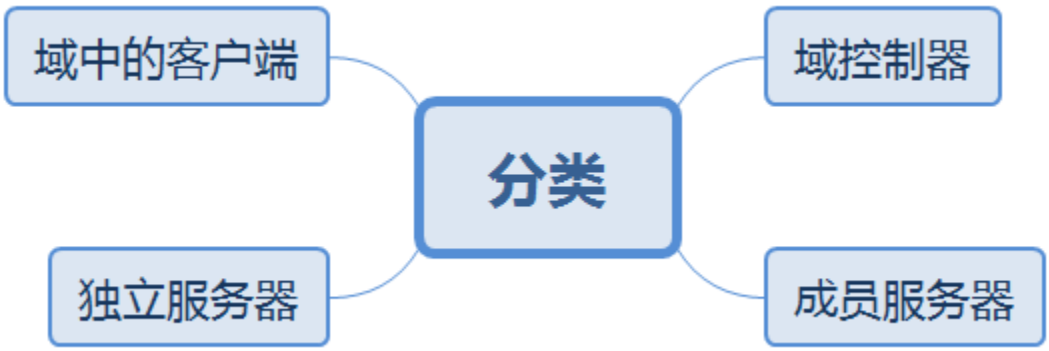
8.1. 定义



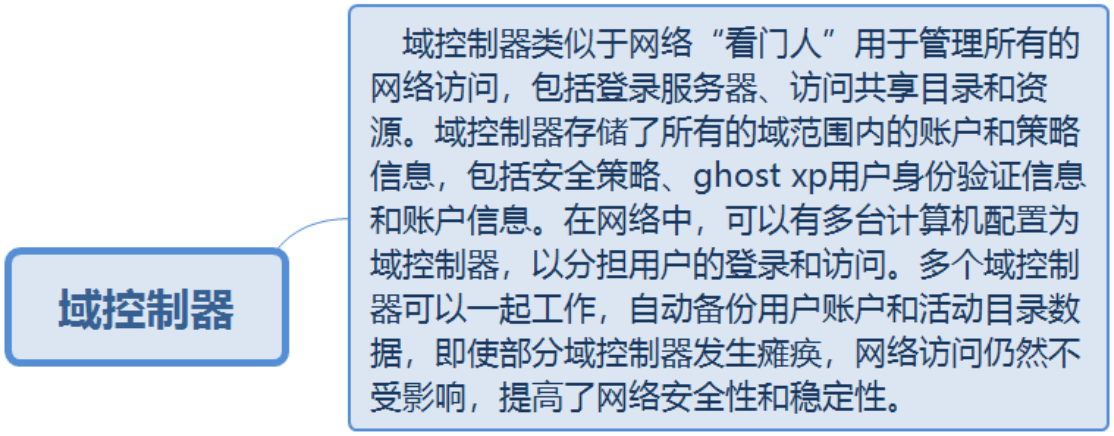
8.1.1. 在域结构的网络中计算机身份是一种不平等的关系，存在着以下四种类型。

计算机不但包括运行**Windows**客户端操作系统的个人电脑（**PC**），还包括运行服务器操作系统的服务器或者域控制器。每台计算机都是一个唯一独立的个体，因此对计算机管理有特殊要求。网络中计算机名称必须唯一，否则将发生冲突。计算机加入域后，只能使用一个计算机账户，而一个计算机账户可关联多个域用户账户，用户可以在不同的计算机（指已经连接到域中的计算机）上使用自己账户登录。在域中存在计算机账户，说明这台计算机是域成员，将受到“域组策略”——“计算机配置”的限制。

8.2. 分类



8.2.1. 域控制器

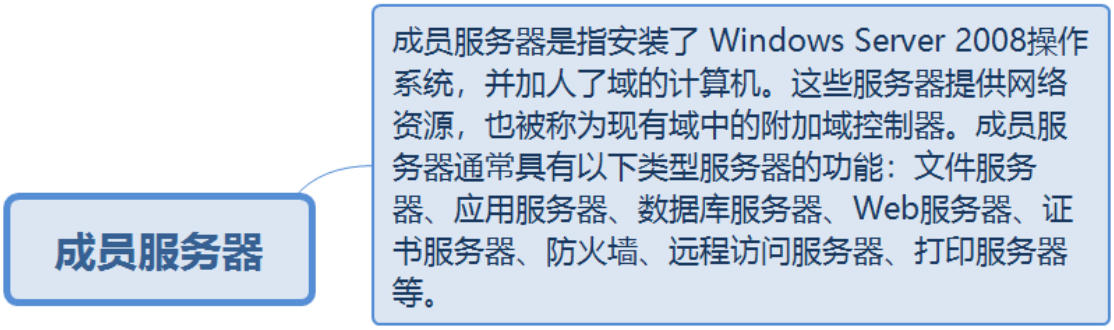


参见: 域控制器

8.2.1.1.

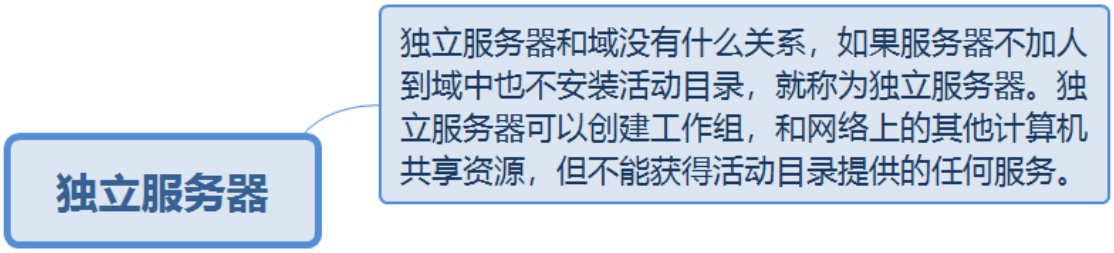
域控制器类似于网络“看门人”用于管理所有的网络访问，包括登录服务器、访问共享目录和资源。域控制器存储了所有的域范围内的账户和策略信息，包括安全策略、ghost xp用户身份验证信息和账户信息。在网络中，可以有多台计算机配置为域控制器，以分担用户的登录和访问。多个域控制器可以一起工作，自动备份用户账户和活动目录数据，即使部分域控制器发生瘫痪，网络访问仍然不受影响，提高了网络安全性和稳定性。

8.2.2. 成员服务器



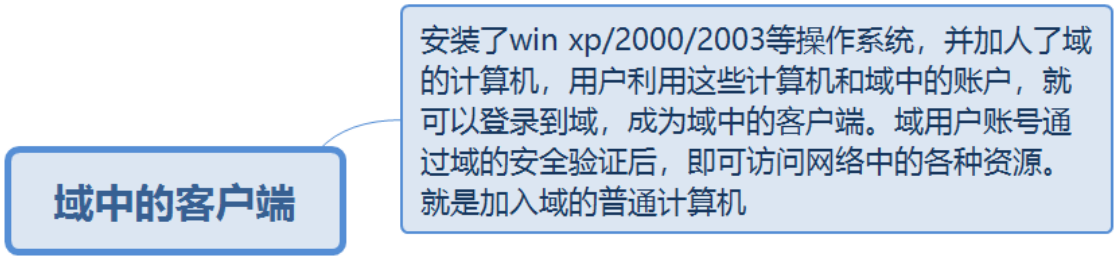
8.2.2.1. 成员服务器是指安装了 **Windows Server 2008**操作系统，并加人了域的计算机。这些服务器提供网络资源，也被称为现有域中的附加域控制器。成员服务器通常具有以下类型服务器的功能：文件服务器、应用服务器、数据库服务器、**Web**服务器、证书服务器、防火墙、远程访问服务器、打印服务器等。

8.2.3. 独立服务器



8.2.3.1. 独立服务器和域没有什么关系，如果服务器不加人到域中也不安装活动目录，就称为独立服务器。独立服务器可以创建工作组，和网络上的其他计算机共享资源，但不能获得活动目录提供的任何服务。

8.2.4. 域中的客户端

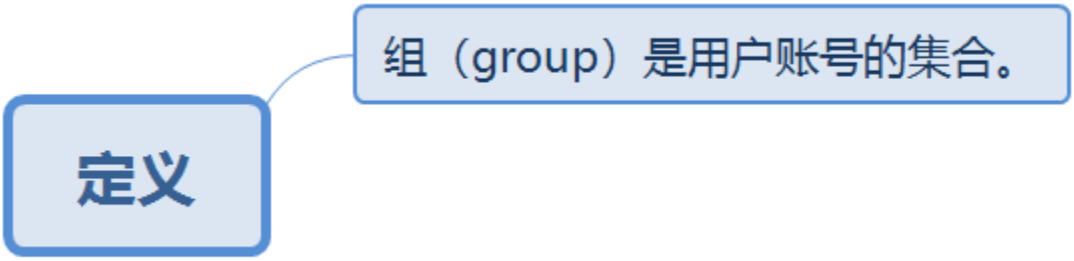


8.2.4.1. 安装了**win xp/2000/2003**等操作系统，并加人了域的计算机，用户利用这些计算机和域中的账户，就可以登录到域，成为域中的客户端。域用户账号通过域的安全验证后，即可访问网络中的各种资源。就是加入域的普通计算机

9. 域内权限

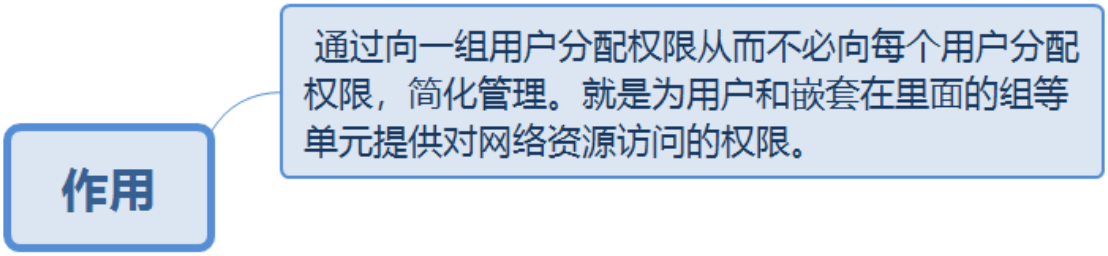
9.1. 域内置组权限

9.1.1. 定义



9.1.1.1. 组（group）是用户账号的集合。

9.1.2. 作用

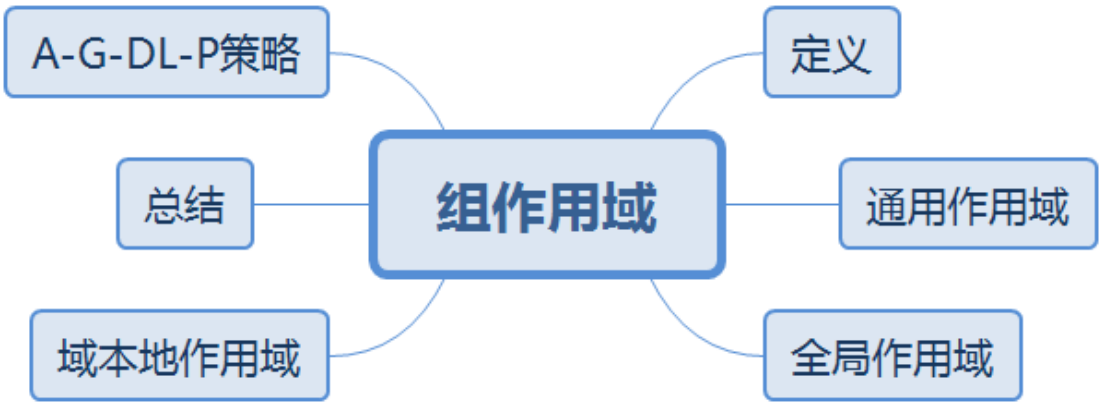


9.1.2.1.

通过向一组用户分配权限从而不必向每个用户分配权限，简化管理。就是为用户和嵌套在里面的组等单元提供对网络资源访问的权限。

9.1.3. 组作用域和组类型

9.1.3.1. 组作用域

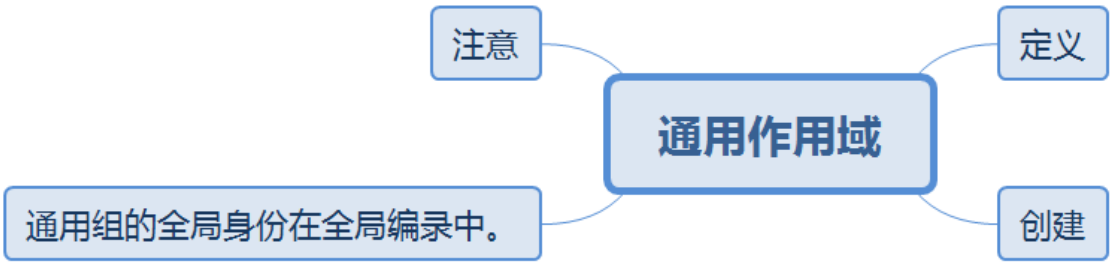


9.1.3.1.1. 定义

9.1.3.1.1.1. 组作用域

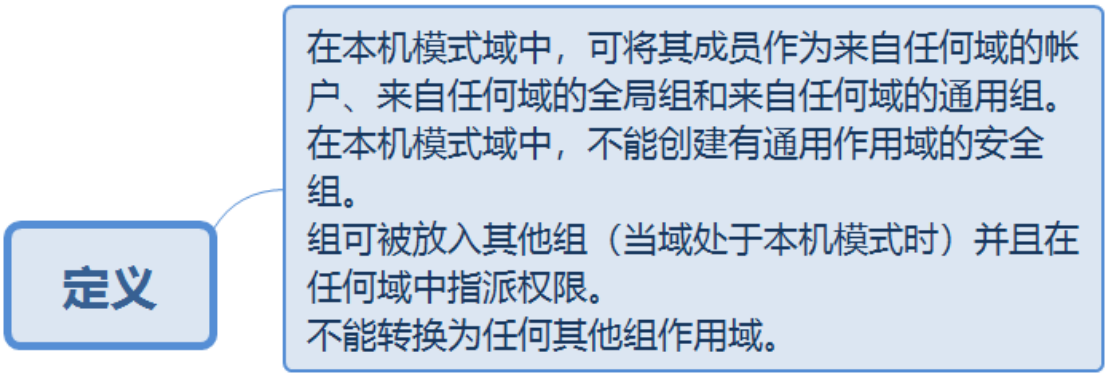
组作用域分为三类：Domain Local Group（本地域），Global Group（全局），Universal（通用）。这三类之间的区别，又要分为两种域模式Native Mode（本地模式）和Mixed Mode（混合模式）的不同来区别对待。

9.1.3.1.2. 通用作用域



参见: 通用组和全局组差别, 较重要的全局组、通用组的权限

9.1.3.1.2.1. 定义



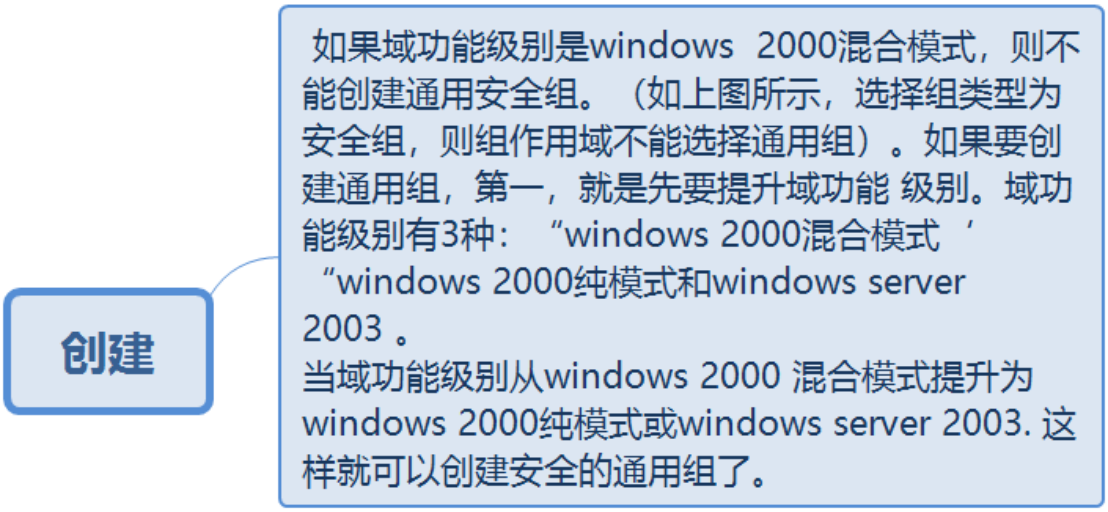
9.1.3.1.2.1.1. 在本机模式域中，可将其成员作为来自任何域的帐户、来自任何域的全局组和来自任何域的通用组。

在本机模式域中，不能创建有通用作用域的安全组。

组可被放入其他组（当域处于本机模式时）并且在任何域中指派权限。

不能转换为任何其他组作用域。

9.1.3.1.2.2. 创建



9.1.3.1.2.2.1. 如果域功能级别是windows 2000混合模式，则不能创建通用安全组。（如上图所示，选择组类型为安全组，则组作用域不能选择通用组）。如果要创建通用组，第一，就是先要提升域功能 级别。域功能级别有3种：“windows

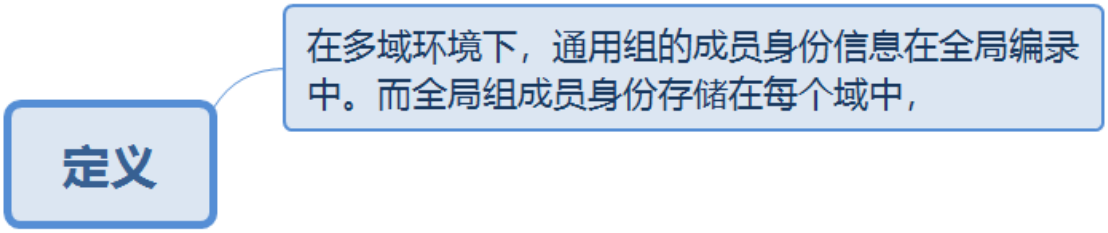
2000混合模式‘ “windows 2000纯模式和windows server 2003 。

当域功能级别从windows 2000 混合模式提升为windows

2000纯模式或windows server 2003. 这样就可以创建安全的通用组了。

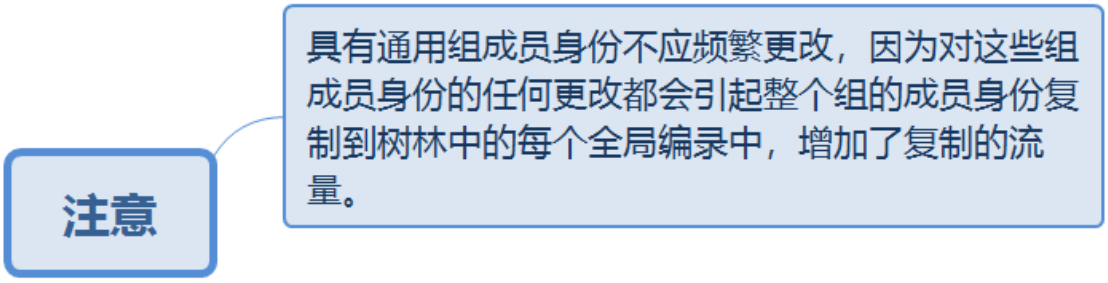
9.1.3.1.2.3. 通用组的全局身份在全局编录中。

9.1.3.1.2.3.1. 定义



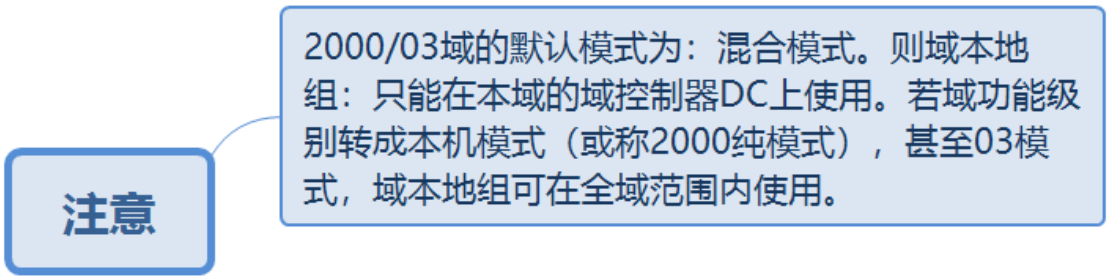
9.1.3.1.2.3.1.1. 在多域环境下，通用组的成员身份信息在全局编录中。而全局组成员身份存储在每个域中，

9.1.3.1.2.3.2. 注意



9.1.3.1.2.3.2.1. 具有通用组成员身份不应频繁更改，因为对这些组成员身份的任何更改都会引起整个组的成员身份复制到树林中的每个全局编录中，增加了复制的流量。

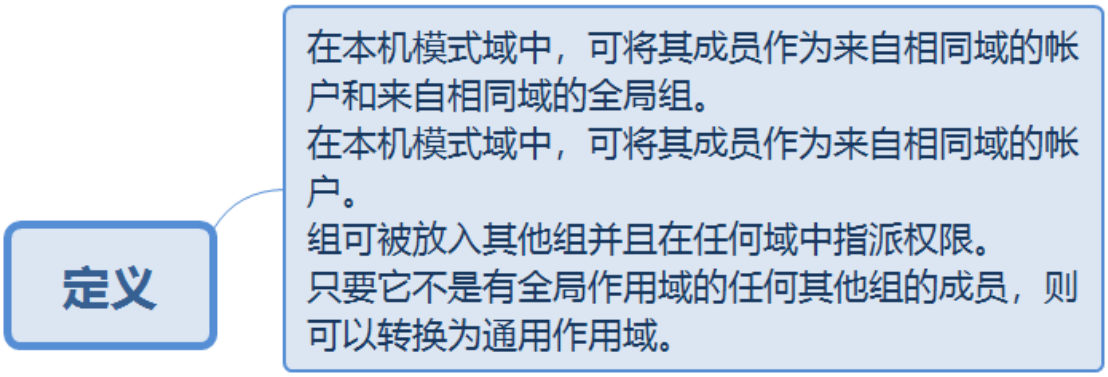
9.1.3.1.2.4. 注意



9.1.3.1.2.4.1. 2000/03域的默认模式为：混合模式。则域本地组：只能在本域的域控制器DC上使用。若域功能级别转成本机模式（或称2000纯模式），甚至03模式，域本地组可在全域范围内使用。

9.1.3.1.3. 全局作用域

9.1.3.1.3.1. 定义



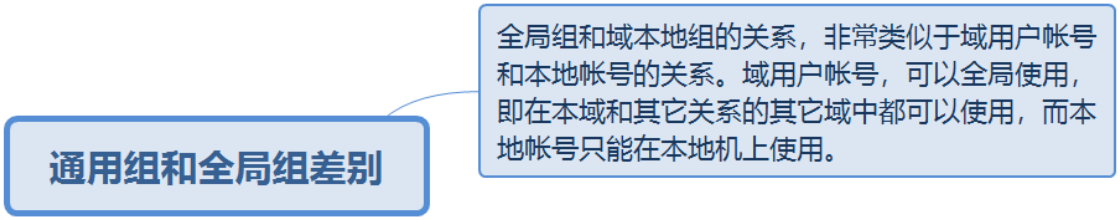
9.1.3.1.3.1.1. 在本机模式域中，可将其成员作为来自相同域的帐户和来自相同域的全局组。

在本机模式域中，可将其成员作为来自相同域的帐户。

组可被放入其他组并且在任何域中指派权限。

只要它不是有全局作用域的任何其他组的成员，则可以转换为通用作用域。

9.1.3.1.3.2. 通用组和全局组差别



参见: 通用作用域

9.1.3.1.3.2.1. 全局组和域本地组的关系，非常类似于域用户帐号和本地帐号的关系。域用户帐号，可以全局使用，即在本域和其它关系的其它域中都可以使用，而本地帐号只能在本地机上使用。

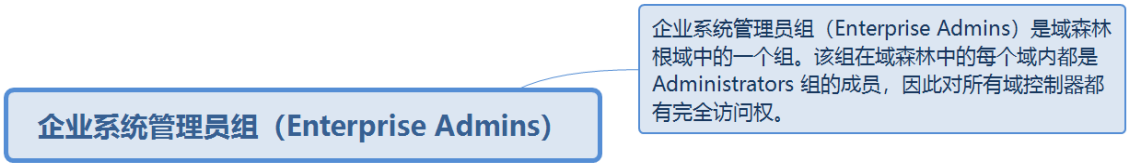
9.1.3.1.3.3. 较重要的全局组、通用组的权限

参见: 通用作用域

9.1.3.1.3.3.1. 域管理员组（Domain Admins）

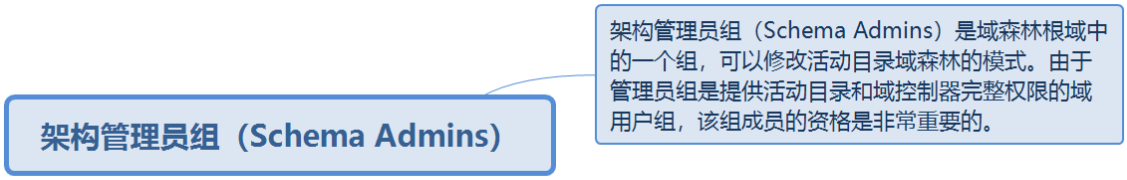
9.1.3.1.3.3.1.1. 域管理员组（Domain Admins）的成员在所有加入域的服务器和工作站、域控制器和活动目录上均默认拥有完整的管理员权限。因为该组会被添加到自己所在域的 Administrators 组 中，因此可以继承 Administrators 组的所有权限。同时，该组默认会被添加到每台域成员计算机的本地 Administrators 组中，这样，Domain Admins 就对域中的所有计算机拥有了所有权。如果希望某用户成为域系统管理器，建议将该用户加至 Domain Admins 组中，而不要直接将该用户添加到 Administrators 组中。

9.1.3.1.3.3.2. 企业系统管理员组（Enterprise Admins）



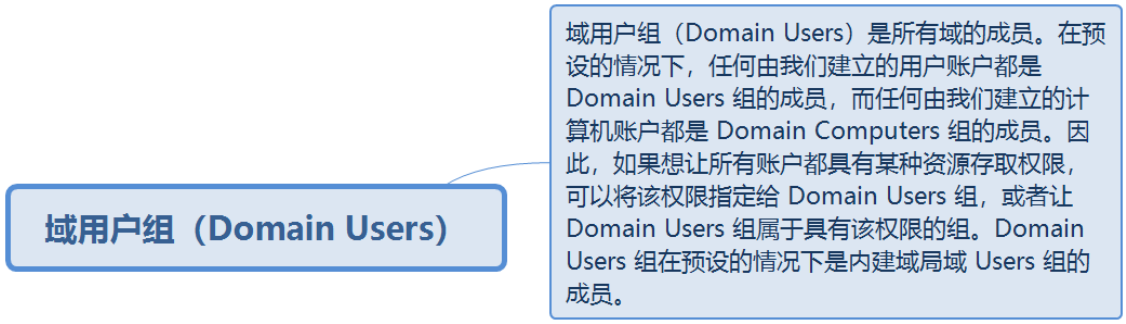
9.1.3.1.3.3.2.1. 企业系统管理员组（Enterprise Admins）是域森林根域中的一个组。该组在域森林中的每个域内都是 Administrators 组的成员，因此对所有域控制器都有完全访问权。

9.1.3.1.3.3.3. 架构管理员组（Schema Admins）



9.1.3.1.3.3.3.1. 架构管理员组（Schema Admins）是域森林根域中的一个组，可以修改活动目录域森林的模式。由于管理员组是提供活动目录和域控制器完整权限的域用户组，该组成员的资格是非常重要的。

9.1.3.1.3.3.4. 域用户组（Domain Users）



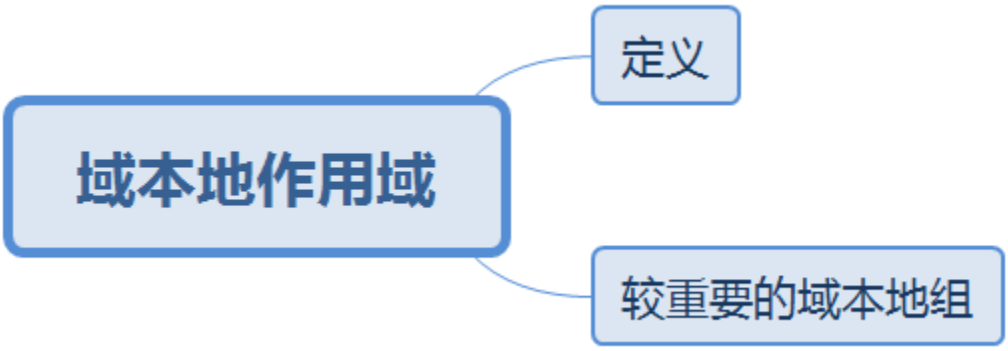
9.1.3.1.3.3.4.1. 域用户组（Domain Users）是所有域的成员。在预设的情况下，任何由我们建立的用户账户都是 Domain Users

组的成员，而任何由我们建立的计算机账户都是 Domain Computers 组的成员。因此，如果想让所有账户都具有某种资源存取权限，可以将该权限指定给 Domain Users 组，或者让 Domain Users

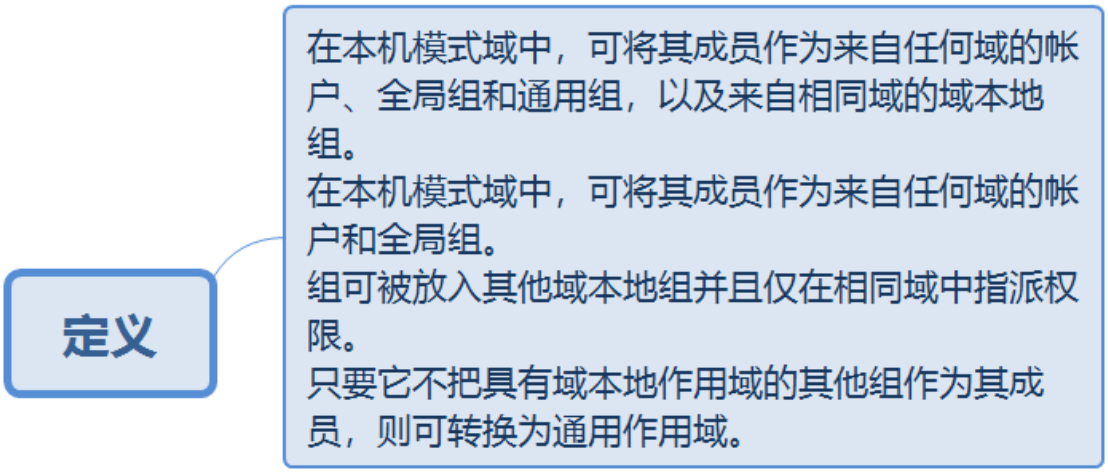
组属于具有该权限的组。Domain Users

组在预设的情况下是内建域局域 Users 组的成员。

9.1.3.1.4. 域本地作用域



9.1.3.1.4.1. 定义



9.1.3.1.4.1.1. 在本机模式域中，可将其成员作为来自任何域的帐户、全局组和通用组，以及来自相同域的域本地组。

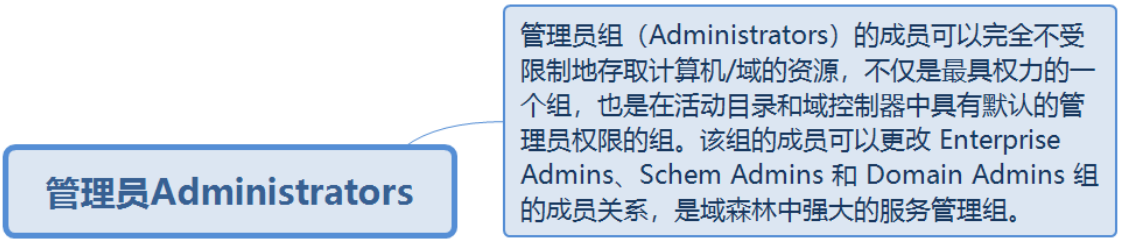
在本机模式域中，可将其成员作为来自任何域的帐户和全局组。

组可被放入其他域本地组并且仅在相同域中指派权限。

只要它不把具有域本地作用域的其他组作为其成员，则可转换为通用作用域。

9.1.3.1.4.2. 较重要的域本地组

9.1.3.1.4.2.1. 管理员Administrators

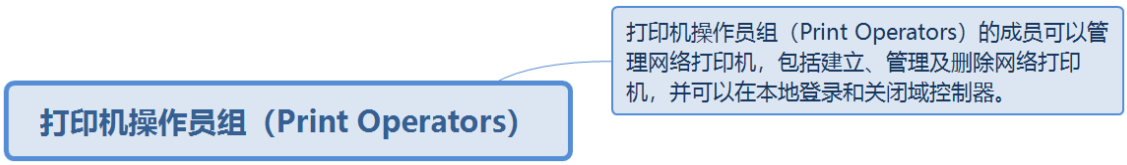


9.1.3.1.4.2.1.1. 管理员组（Administrators）的成员可以完全不受限制地存取计算机/域的资源，不仅是最具权力的一个组，也是在活动目录和域控制器中具有默认的管理员权限的组。该组的成员可以更改 Enterprise Admins、Schem Admins 和 Domain Admins 组的成员关系，是域森林中强大的服务管理组。

9.1.3.1.4.2.2. 远程登录组（Remote Desktop Users）

9.1.3.1.4.2.2.1. 远程登录组（Remote Desktop Users）的成员被授予远程登录的权限。

9.1.3.1.4.2.3. 打印机操作员组（Print Operators）



9.1.3.1.4.2.3.1. 打印机操作员组（Print Operators）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。

9.1.3.1.4.2.4. 账号操作员组（Account Operators）

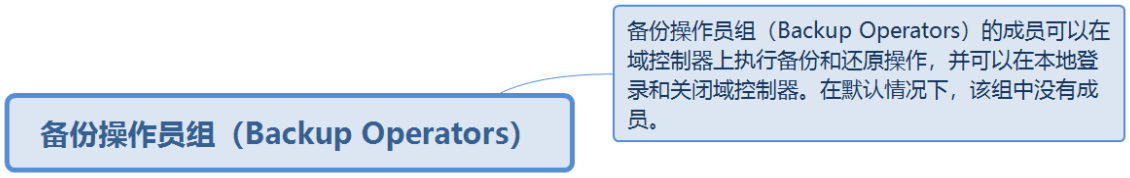
9.1.3.1.4.2.4.1. 账号操作员组（Account Operators）的成员可以创建和管理该域中的用户和组，并可以设置其权限，但是，不能更改隶属 Administrators 或 Domain Admins 组的账户，也不能修改这些组。Account Operators 可以在本地登录域控制器。在默认情况下，该组中没有成员。

9.1.3.1.4.2.5. 服务器操作员组（Server Operators）

9.1.3.1.4.2.5.1. 服务器操作员组（Server Operators）的成员可以管理域服务器，包括建立/管理/删除任何服务器的共享目录、管理网络打印机、备份任何服务器的文件、格式化服

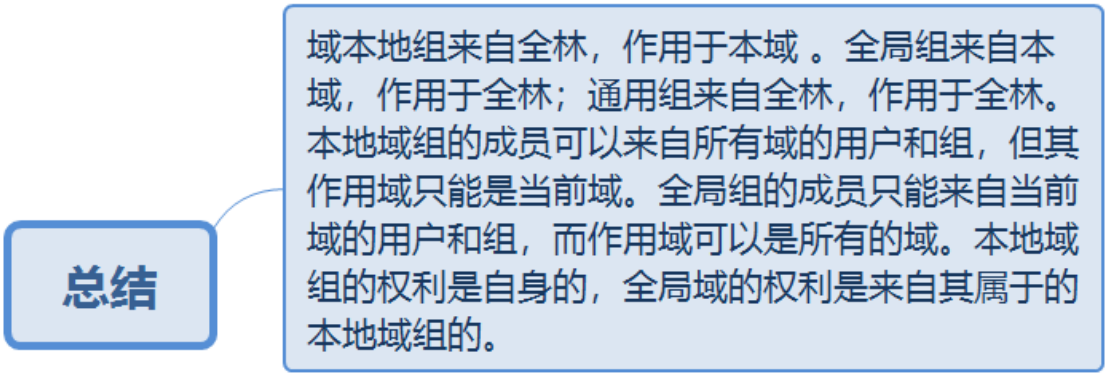
务器硬盘、锁定服务器，以及变更服务器的系统时间等权限，并能关闭域控制器。在默认情况下，该组中没有成员。

9.1.3.1.4.2.6. 备份操作员组（Backup Operators）



9.1.3.1.4.2.6.1. 备份操作员组（Backup Operators）的成员可以在域控制器上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。

9.1.3.1.5. 总结

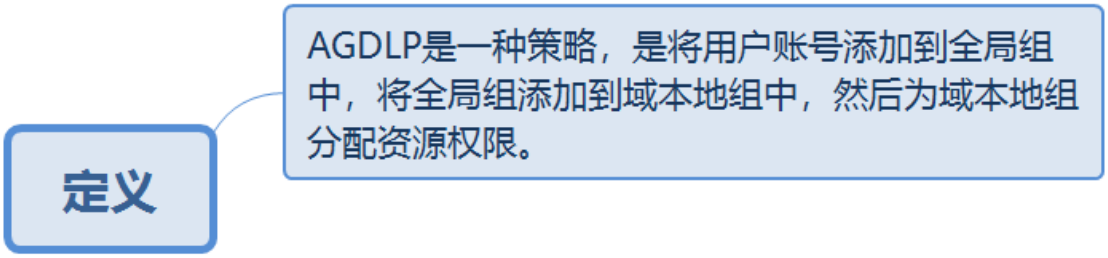


9.1.3.1.5.1. 域本地组来自全林，作用于本域

。全局组来自本域，作用于全林；通用组来自全林，作用于全林。本地域组的成员可以来自所有域的用户和组，但其作用域只能是当前域。全局组的成员只能来自当前域的用户和组，而作用域可以是所有的域。本地域组的权利是自身的，全局域的权利是来自其属于的本地域组的。

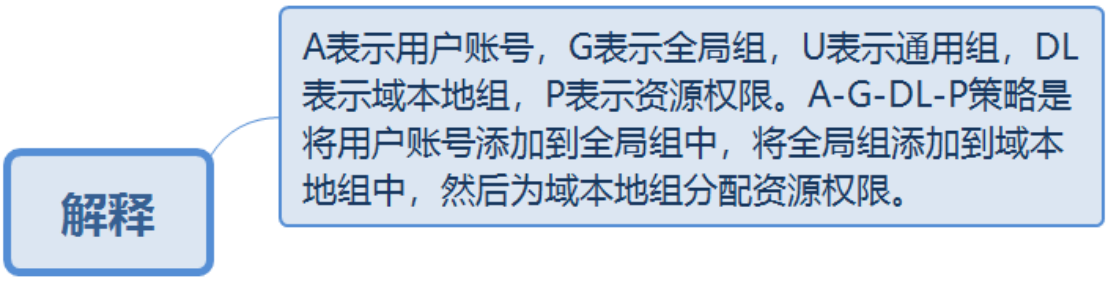
9.1.3.1.6. A-G-DL-P策略

9.1.3.1.6.1. 定义



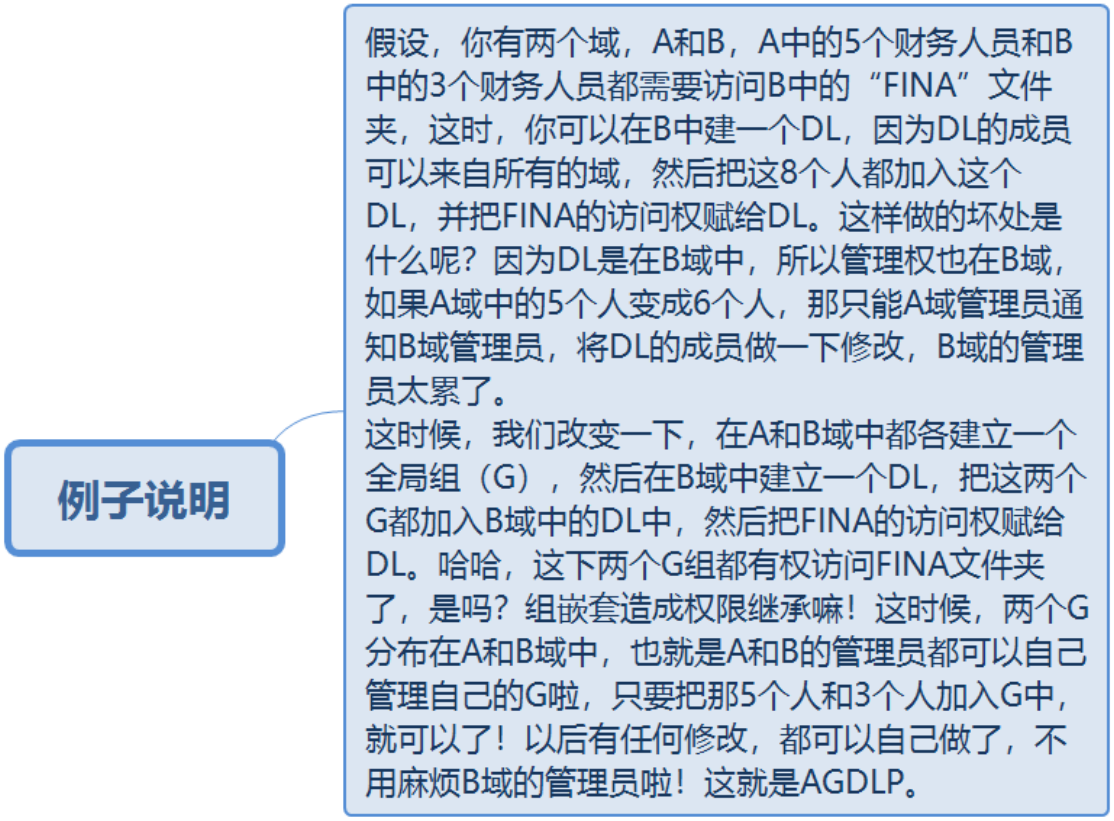
9.1.3.1.6.1.1. AGDLP是一种策略，是将用户账号添加到全局组中，将全局组添加到域本地组中，然后为域本地组分配资源权限。

9.1.3.1.6.2. 解释



9.1.3.1.6.2.1. A表示用户账号，G表示全局组，U表示通用组，DL表示域本地组，P表示资源权限。A-G-DL-
P策略是将用户账号添加到全局组中，将全局组添加到域本地组中，然后为域本地组分配资源权限。

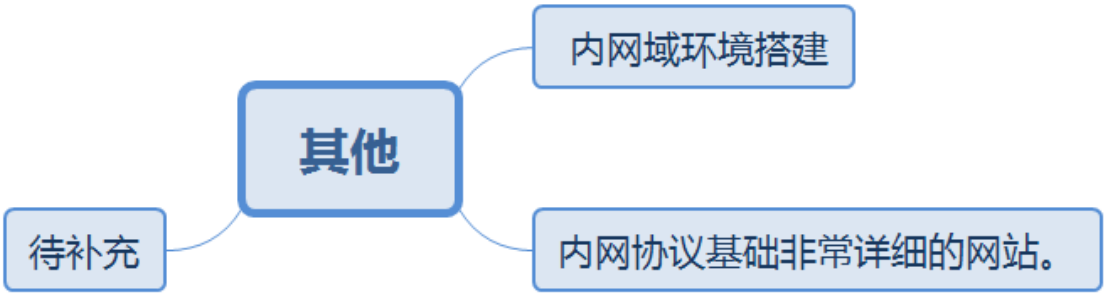
9.1.3.1.6.3. 例子说明



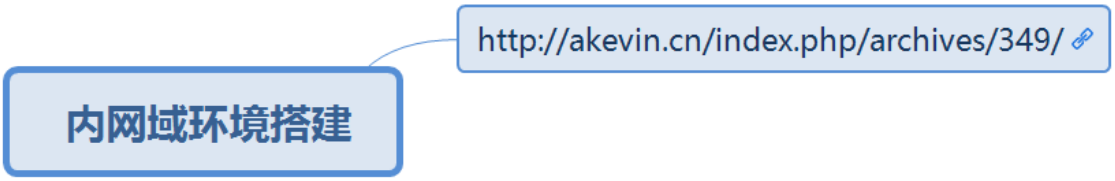
9.1.3.1.6.3.1. 假设，你有两个域，A和B，A中的5个财务人员和B中的3个财务人员都需要访问B中的“FINA”文件夹，这时，你可以在B中建一个DL，因为DL的成员可以来自所有的域，然后把这8个人都加入这个DL，并把FINA的访问权赋给DL。这样做的坏处是什么呢？因为DL是在B域中，所以管理权也在B域，如果A域中的5个人变成6个人，那只能A域管理员通知B域管理员，将DL的成员做一下修改，B域的管理员太累了。
这时候，我们改变一下，在A和B域中都各建立一个全局组（G），然后在B域中建立一个DL，把这两个G都加入B域中的DL中，然后把FINA的访问权赋给DL。哈哈，这下两个G组都有权访问FINA文件夹了，是吗？组嵌套造成权限继承嘛！这时候，两个G分布在A和B域中，也就是A和B的管理员都可以自己管理自己的G啦，只要把那5个人和3个人加入G中，

就可以了！以后有任何修改，都可以自己做了，不用麻烦B域的管理员啦！这就是AGDLP。

10. 其他

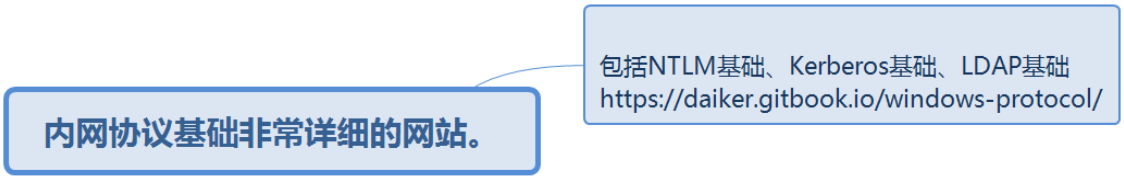


10.1. 内网域环境搭建



10.1.1. http://akevin.cn/index.php/archives/349/

10.2. 内网协议基础非常详细的网站。



10.2.1.

包括NTLM基础、Kerberos基础、LDAP基础

https://daiker.gitbook.io/windows-protocol/

10.3. 待补充

11. 微信公众号 黑白天 BY 李木

11.1.