域介绍

域的介绍

Windows域是计算机网络的一种形式，其中所有用户帐户 ，计算机，打印机和其他安全主体都在位于称为域控制器的一个或多个中央计算机集群上的中央数据库中注册。 身份验证在域控制器上进行。 在域中使用计算机的每个人都会收到一个唯一的用户帐户，然后可以为该帐户分配对该域内资源的访问权限。

域（Domain)是一个有安全边界的计算机集合(安全边界的意思是,在两个域中,一个域中 的用户无法访问另一个域中的资源)可以简单地把域理解成升级版的工作组。与工作组相比,域 的安全管理控制机制更加严格。用户要想访问域内的资源,必须以合法的身份登录域,而用户对域内的资源拥有什么样的权限,还取决于用户在域内的身份。

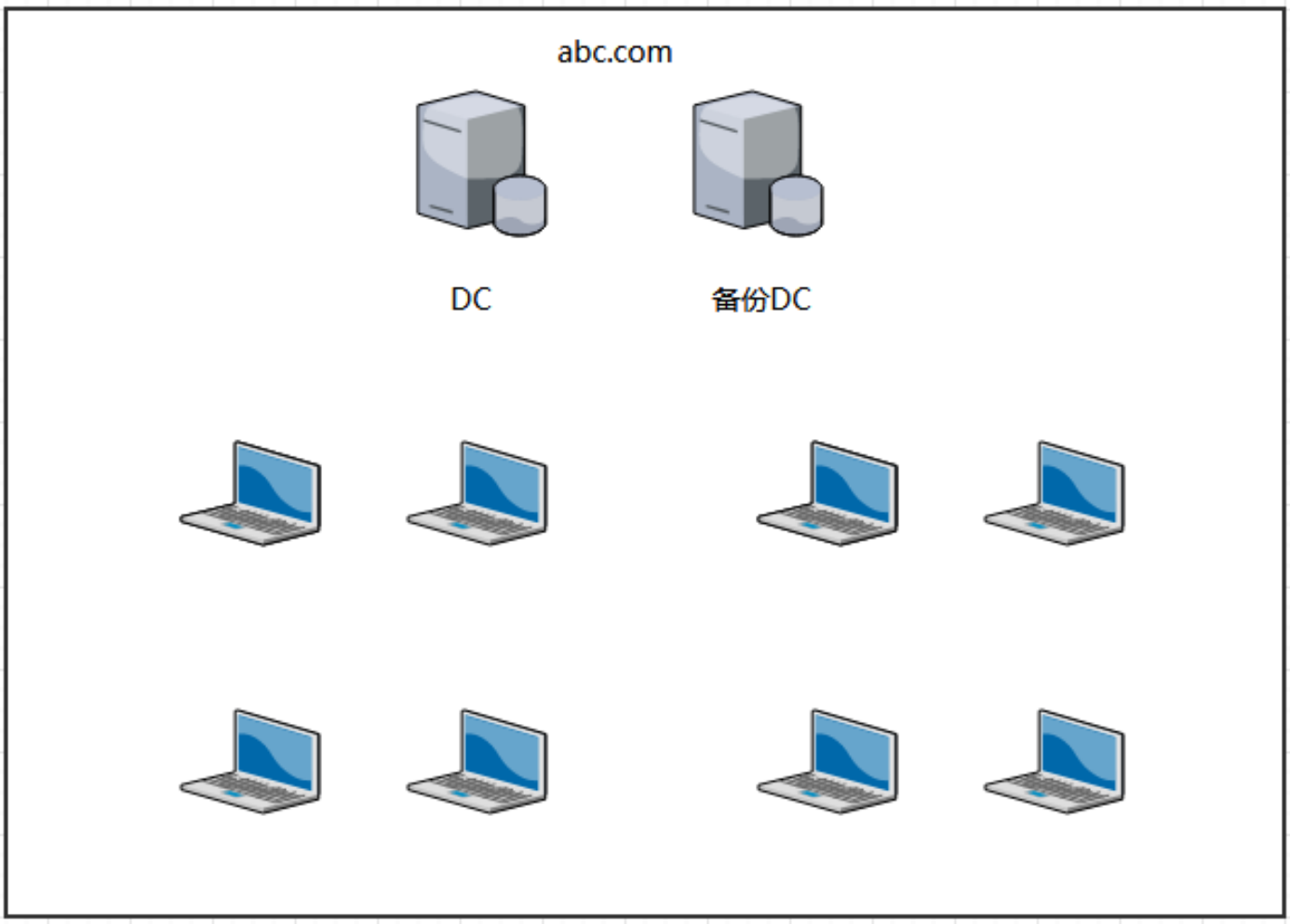
域控制器(Domain Controller,DC)是域中的一台类似管理服务器的计算机

域控制器中存在由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当计算 机连接到域时,域控制器首先要鉴别这台计算机是否属于这个域,以及用户使用的登录账号是否存在、密码是否正确。如果以上信息有一项不正确,域控制器就会拒绝这个用户通过这台计算机登录。如果用户不能登录,就不能访问服务器中的资源。

域控制器是整个域的通信枢纽,所有的权限身份验证都在域控制器上进行,也就是说,域内 所有用来验证身份的账号和密码散列值都保存在域控制器中

单域

通常,在一个地理位置固定的小公司里,建立一个域就可以满足需求。在一个域内,一般要 有至少两台域服务器,一台作为DC,另一台作为备份DC。



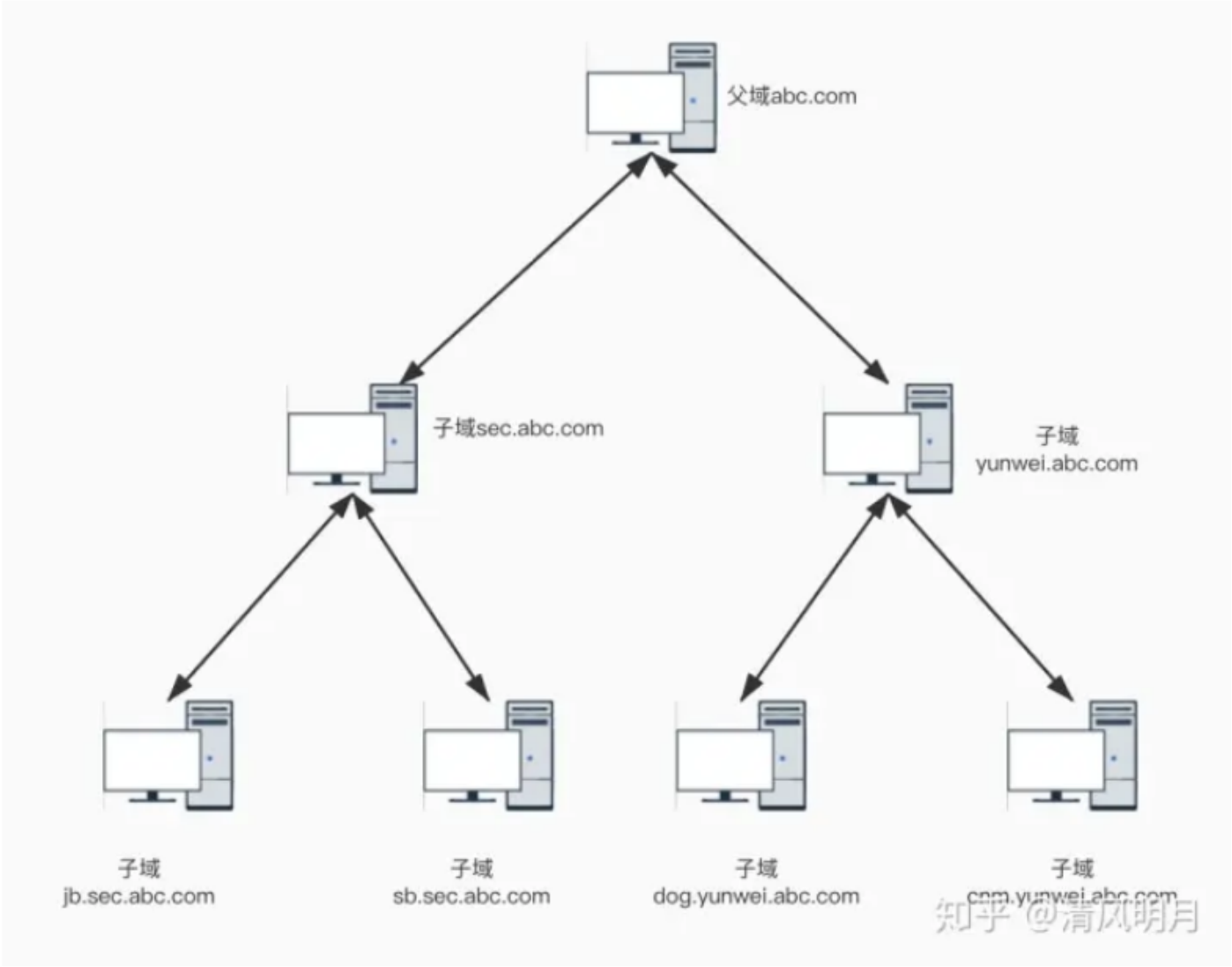
父域和子域

出于管理及其他需求,需要在网络中划分多个域。第一个域称为父域,各分部的域称为该域的子域。例如 大公司的各个分公司位于不同的地点,就需要使用父域及子域。如果把不同 地点的分公司放在同一个域内,那么它们之间在信息交互(包括同步、复制等)上花费的时间就 会比较长,占用的带宽也会比较大(在同一个域内,信息交互的条目是很多的,而且不会压缩; 在不同的域之间,信息交互的条日相对较少,而且可以压缩)。这样处理有一个好处,就是分公司 可以通过自己的域来管理自己的资源。还有一种情况是出于安全策略的考虑(每个域都有自己的 安全策略)例如,一个公司的财务部希望使用特定的安全策略(包括账号密码策略等)、那么可 以将财务部作为一个子域来单独管理

域树

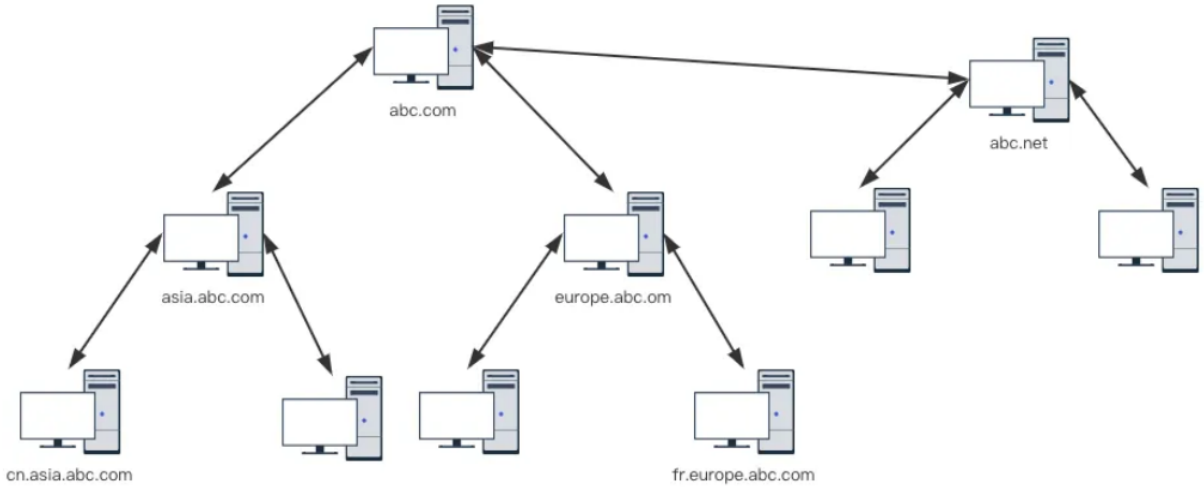
域树(Tree)是多个域通过建立信任关系组成的集合。一个域管理员只能管理本域,不能访问 或者管理其他域。如果两个域之间需要互相访问,则需要建立信任关系，信任关系是连接不同域的桥梁。域树内的父域与子域,不但可以按照需要互相管理、还可以跨网络分配文 件和打印机等设备及资源,从而在不同的域之间实现网络资源的共享与管理、通信及数据传输。

在一个域树中,父域可以包含多个子域。子域是相对父域来说的,指的是域名中的每一个段。 各子域之间用点号隔开,一个"."代表一个层次。放在域名最后的子域称为最高级子域或一级 域,它前面的子域称为二级域



域森林

域森林(Forest)是指多个域树通过建立信任关系组成的集合。例如,在一个公司兼并场景中 某公司使用域树 abc. com,被兼并的公司本来有自己的域树 abc. net,域树abc.net无法挂在域树abc.com下。所以,域树abc.com与域树 abc. net之间需要通过建立信任关系来构成域森林。通过域树之间的信任关系,可以管理和使用整个域森林中的资源,并保留被兼并公司自身原有的特性,如图1-4所示。



域名服务器

域名服务器(Domain Name Server,DNs)是指用于实现域名(Domain Name)和与之相对的IP地址(IP Address)转换的服务器。从对域树的介绍中可以看出,域树中的域名和DNS域名非常相似。而实际上,因为域中的计算机是使用DNS来定位域控制器、服务器及其他计算机、网络服务的,所以域的名字就是DNS域的名字。在内网渗透测试中,大都是通过寻找DNS服务器 来确定域控制器的位置的(DNS服务器和域控制器通常配置在同一机器上)