【Windows Server 2019】活动目录 (Active Directory) ——理论

原创 NOWSHUT 已于 2022-10-14 23:45:18 修改 阅读量6.6k 收藏 43 点赞数 10

分类专栏： Windows Server 2019 配置与管理实战 文章标签： windows server 服务器 运维 活动目录（AD）

目录

1. Acitve Directory 的定义与作用

1.1 Acitve Directory 的定义

活动目录，Active Directory，简称为”AD“。活动目录是负责管理一定区域[1]内Windows网络中各类资源的Windows Server组件之一。

在由windows系统组成的网络中，存在着各种资源，如服务器、客户机、用户账户、打印机、各种文件等，这些资源都分布于各台计算机上。没有使用“活动目录”之前，需要在每台计算机上单独管理这些资源 。

1.2 Acitve Directory 的作用

使用“AD”的主要作用是：

- 为了**集中管理windows网络的各类资源**，“活动目录”就像是一个数据库，存储着windows网络中的所有资源。

- Active Directory域内的directory database（目录数据库）用来存储用户账户、计算机账户、打印机与共享文件夹等对象，而提供目录服务的组件是Active Directory Domain Services，**AD DS**（活动目录域服务），它负责目录数据库的存储、新建、删除、修改与查询等工作[1]。
- 普通用户通过“活动目录”可以很容易找到并使用网络中的各种资源。
- 管理员也可以通过活动目录，对网络上的所有资源进行集中管理，以控制不同用户在不同计算机上对不同资源的访问。

2. Acitve Directory 与 DNS

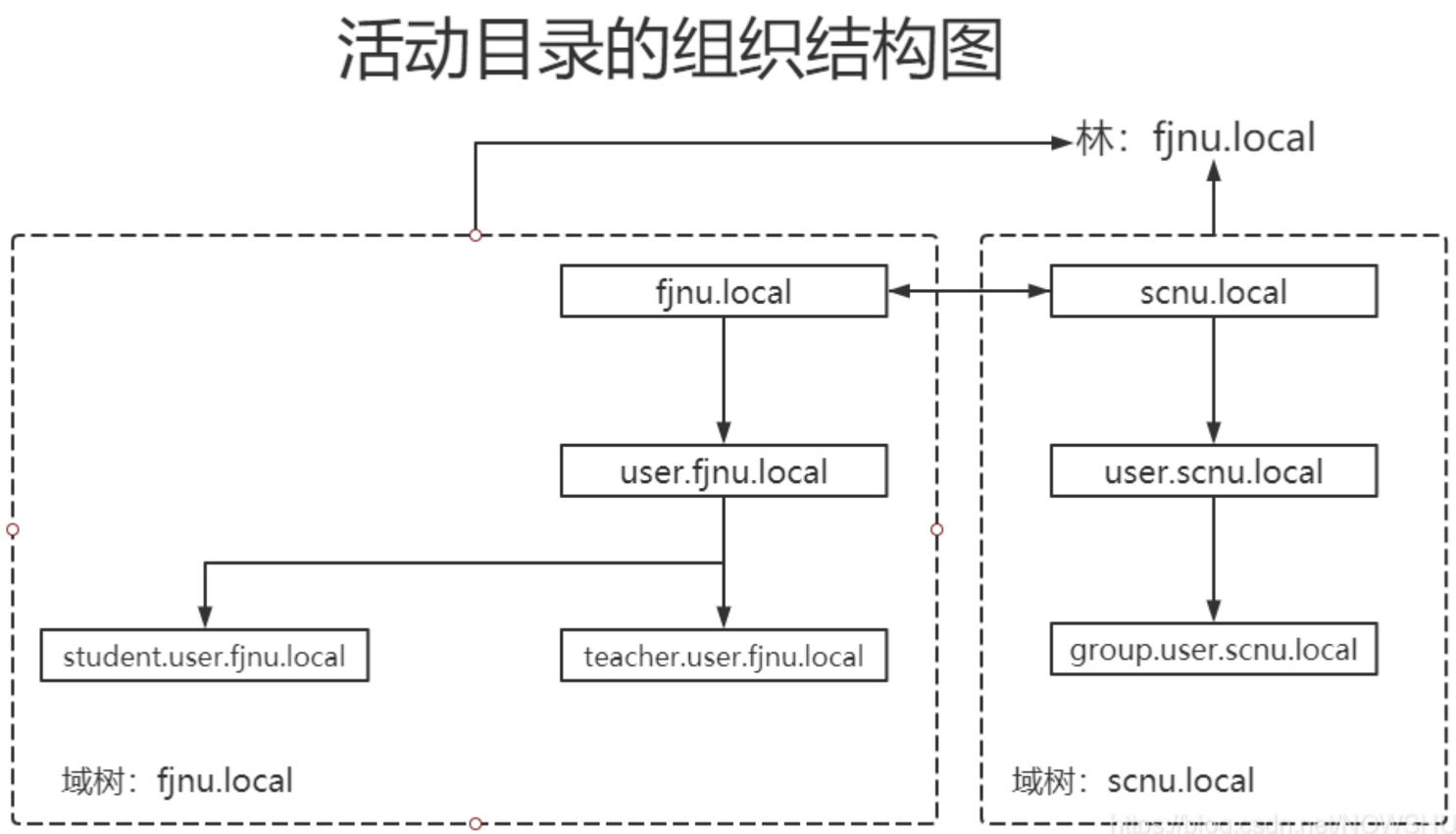
Active Directory是按**区域**[2]对资源进行管理的，各区域的命名规则与DNS的命名规则相同，因此**AD 必须要有DNS服务的支持**，借助DNS服务的域名解析，达到使用域名访问该域中计算机资源的目的。

活动目录使用域名主要用于在进行网络管理时，使用名称来访问计算机资源，这些用于网络管理的计算机名称，只能在活动目录中使用，而不能够被互联网上用户使用。因此，虽然活动目录和互联网都使用DNS域名服务，但其使用目的是不同的。 活动目录使用的域名仅在其管理的区域有效， 而全球互联网使用的域名在互联网上面有效。

在接下来的实验中，为了区别互联网中的域名，将AD的“区域名称”设置为：fjnu.lcoal。

3. Acitve Directory 的组织结构

AD的组织结构为树形图。根域（root domain）和其下所有子域构成一棵“域树”（domain tree）。域树的名称为根域的名称。同一网络中，可以有多棵不同的域树，所有域树构成“林”，林的名称为第一棵域树的名称（即第一棵域树根域的名称）。



3.1 名词解释

接下来的实验中会用到以下名词，先做了解。

（1）域控制器

在一个区域中，用于安装“活动目录”的服务器称为“域控制器”，负责该区域资源的管理与控制。

（2）子域

区域下面可以划分子域，子域的域控制器负责子域内资源的管理与控制。

（3）对象（Object）

AD DS内的资源是以对象的形式存在，例如用户和计算机这些都是对象。

（4）属性（Attribute）

对象是通过属性来描述其特征，即对象是具有相同属性的集合。

对象（Object）	属性（Attribute）
用户（user）	用户名（Name）
	密码（Age）
	联系方式（Tel.）

（5）容器（Container）

容器与对象相似，它拥有名字，也是一些属性的集合，不过容器中可以包含其他对象（例如用户、计算机等对象），也可以包含其他容器。

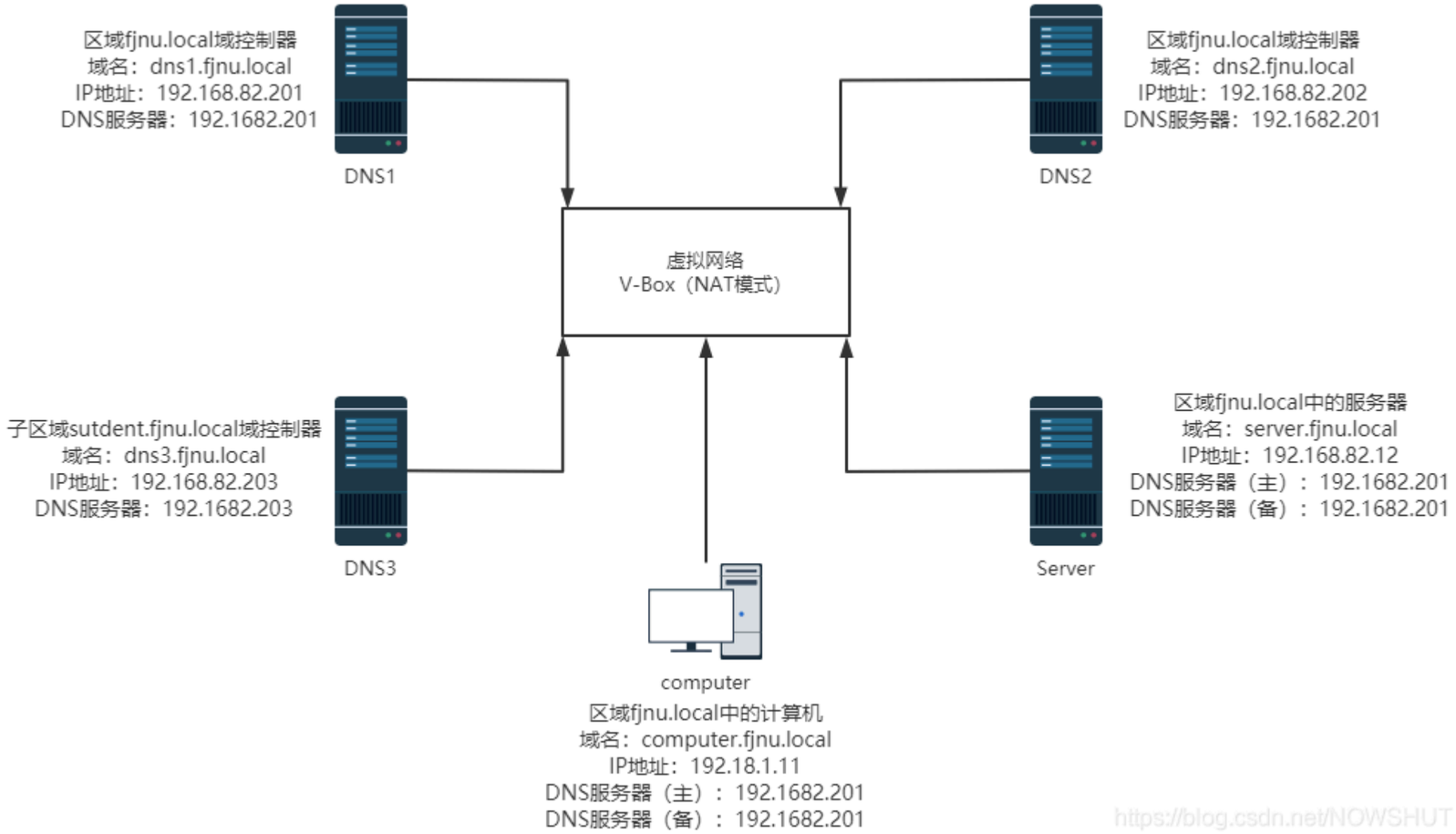
（6）组织单位（Organization Units，OU）

组织单位是一个比较特殊的容器，它除了可以包含其他对象与组织单位外，还能应用组策略（Group Policy）功能。

（7）关于域间信任（Trust）

两个域之间必须拥有信任关系（trust relationship），才可以访问对方域内的资源。而任何一个新的AD DS域被加入到域树后，这个域会自动信任其上层的父域，同时父域也会自动信任新子域，而且这些信任关系具备双向传递性（two-way transitive）。由于此信任工作是通过Kerberos security protocol来完成，因此也被为Kerberos trust[1]。
在同一个林下，不同的域树间也可以互相访问。只要两个域间互相信任。

4. 实验拓扑



- DNS1和DNS2共同管理区域fjnu.local内的资源，当一台出现故障时，另一台可以完全独立负责本区域的管理和控制。
- DNS3负责该子域内所有资源的集中管理，子域和父域之间默认是双向信任关系。
- computer是区域fjnu.local中的一台普通计算机，通过将该计算机加入域中，可以在域控制器上对该计算机上的资源进行集中管理。
- server是区域fjnu.local中的一台服务器，通过将该服务器加入域中，可以在域控制器上对该服务器上的资源进行集中管理。

参考资料

- 戴有炜，《2016 Windows Server 系统配置指南》，清华出版社，2018
- Microsoft Docs：AD DS Installation and Removal Wizard Page Descriptions
- Microsoft Docs：Forest and Domain Functional Levels

关联博文

关于***活动目录 (Active Directory)*** 请查阅接下来的博文：

- 【Windows Server 2019】活动目录 (Active Directory) ——理论

博文介绍了活动目录 (Active Directory) 的定义，作用以及与 DNS 的关系。同时也介绍了AD的组织结构，包括域控制器，子域，对象，属性，容器，组织单位，域间信任等术语的解释，实验拓扑图。

- 【Windows Server 2019】活动目录 (Active Directory) ——安装Active Directory域服务和提升为域控制器

  博文详细介绍了如何在DNS服务器上安装活动目录 (Active Directory)，如何将服务器提升为域控制器，以及如何验证域控制器。

- 【Windows Server 2019】活动目录 (Active Directory) ——在同一区域安装多台域控制器

  博文详细介绍了在同一个区域内部署多个域控制器，以及验证多台域控制器。

  为了提高域控制器的可靠性，防止一台域控制器可能产生的单点故障，通常情况下，在同一个域中存在多台域控制器，各个域控制器采用符合分担的方式工作，它们会定时同步数据，以确保所有域控制器保持相同的数据。当某台域控制器故障时，不会影响AD DS的服务。

- 【Windows Server 2019】活动目录 (Active Directory) ——子域的安装和验证

  博文详细介绍了在同一个区域内将一台服务器提升为子域控制器，同时验证DNS，子域控制器和子域和父域的信任关系。

- 【Windows Server 2019】活动目录 (Active Directory) ——将计算机加入域和脱离域

  博文介绍了如何将计算机加入AD域和脱离AD域，包括加入域，验证客户机加入到域后的信息，使用域账户用户在客户机上登录，使用本地账户用户在计算机上登录，脱离域。

- 【Windows Server 2019】活动目录 (Active Directory) ——创建、删除和管理对象、容器和组织单位（OU）

  博文详细介绍了如何创建、删除和管理AD域内的对象、容器和组织单位（OU）。创建，管理和删除都有两种方法进行。