AD/LDAP 配置教程

产品版本：ZStack 3.10.0

文档版本：V3.10.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴科技商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受云轴科技公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，云轴科技公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

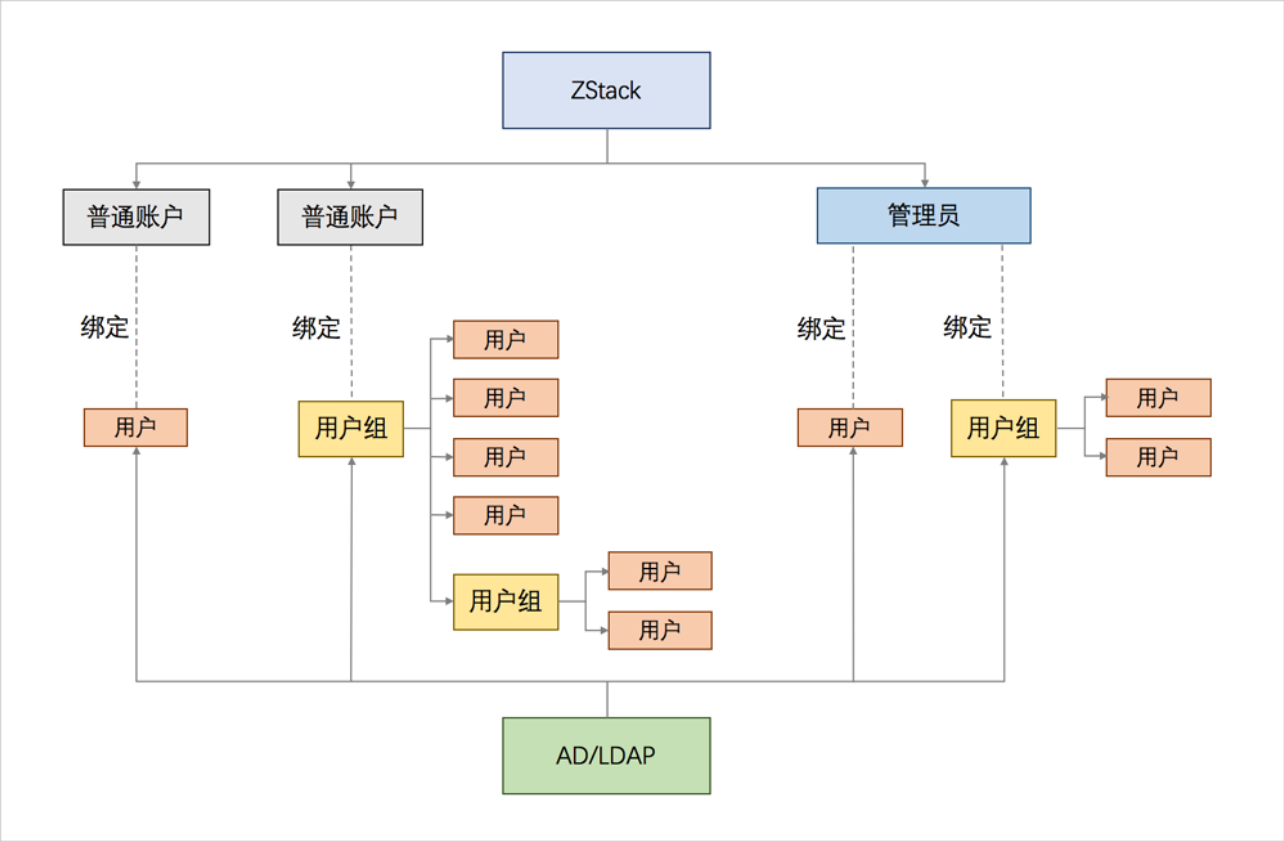
1 介绍

LDAP（Lightweight Directory Access Protocol）作为轻量级目录访问协议，可提供标准的目录服务。微软的WindowsAD软件（以下简称AD），以及众多流行的Linux发行版中提供的OpenLDAP软件（以下简称LDAP），均是基于LDAP协议的实现，它们为日益多样化的企业办公应用提供了一套独立、标准的登录认证系统。

ZStack支持无缝接入AD/LDAP统一认证服务，基于自定义规则添加AD/LDAP服务器，并获取成员列表；当AD/LDAP成员（用户/用户组）成功绑定ZStack账户（普通账户/管理员），就可使用成员登录属性直接登录ZStack云平台。

ZStack账户（普通账户/管理员）与AD/LDAP成员（用户/用户组）的绑定关系如图 *1: ZStack-AD/LDAP绑定关系*所示：

图 1: ZStack-AD/LDAP绑定关系



本教程将详细介绍ZStack接入AD/LDAP的配置方法。

注: 目前，仅支持接入一套AD/LDAP登录认证系统。

2 前提

在此教程中，假定已安装最新版本ZStack，具体方式请参考《用户手册》安装部署章节。

3 添加AD/LDAP

背景信息

ZStack支持基于自定义规则添加AD/LDAP服务器。

操作步骤

1. 进入**AD/LDAP**界面。

   在ZStack私有云主菜单，点击**平台管理** > **AD/LDAP**，进入**AD/LDAP**管理界面。

   如图 *2: AD/LDAP*界面所示：

   图 2: AD/LDAP界面

2. 添加AD/LDAP。

   点击**添加AD/LDAP**，弹出**添加AD/LDAP**界面。

   如图 *3:* 添加*AD/LDAP*所示：

   图 3: 添加AD/LDAP

注: 由于AD/LDAP统一认证服务是基于LDAP协议的不同实现，添加AD/LDAP的方法基本一致，以下将以添加AD服务器为例进行介绍。

在**AD/LDAP**设置界面，可参考以下示例输入相应内容：

- 选择添加的服务器类型：
  - **AD**：将添加WindowsAD类型的服务器
  - **LDAP**：将添加OpenLDAP类型的服务器

- **服务器**：填写AD/LDAP服务器的域名或IP地址

  以AD为例：*adtest.com*或*172.20.12.180*

- **端口**：填写访问AD/LDAP服务器所使用的端口，默认使用389端口
- **基准检索DN**：填写用于检索已绑定AD/LDAP成员的基准DN（Distinguished Name）

  注: 基准检索DN的设置会限制查询结果

  - 希望查询当前AD/LDAP域的所有成员，请设置基准检索DN为：域节点

    以AD为例：*DC=adtest,DC=com*

  - 希望查询当前AD/LDAP域中隶属某一组织的成员，请设置基准检索DN为：目标组织节点

    以AD为例：*OU=people,DC=adtest,DC=com*

- **登录属性**：设置AD/LDAP服务器的登录属性，登录属性决定了已绑定AD/LDAP成员的登录名

  以AD为例：

  - *distinguishedName*：表示已绑定AD成员可用*distinguishedName*相应的value（例如：*CN=xiaoming,OU=people,DC=adtest,DC=com*）作为ZStack登录名
  - *userPrincipalName*：表示已绑定AD成员可用*userPrincipalName*相应的value（例如：邮箱地址 *xiaoming@adtest.com*）作为ZStack登录名
  - *cn*：已绑定AD成员可用*cn*相应的value（例如：名称*xiaoming*）作为ZStack登录名

  注:

  - 支持自定义设置登录属性；默认情况下，设置AD服务器的登录属性为*cn*，LDAP服务器的登录属性为*uid*
  - 为确保成功登录，所指定的登录属性在AD/LDAP域中相应的value（作为登录名）必须全局唯一

- **用户DN**：填写用于AD/LDAP服务器认证的AD/LDAP成员的DN，需确保填写完整

  以AD为例：*CN=xiaoming,OU=people,DC=adtest,DC=com*

  注:

  所填写的用户DN，必须有权访问基准检索DN中的所有用户，因此是与基准检索DN相对应的或域级、或组织级、或用户组级的管理员DN

- **密码**：填写与用户DN相应的密码
- **清除规则**：可选项，自定义清除规则，系统将清理满足条件的绑定关系

  以AD为例：希望清除所有已离职员工的账号绑定关系，可设置清除规则*(description*=已离职*)*

如图 *4: 添加AD*所示：

图 4: 添加AD

点击**确定**按钮，系统会自动检测服务器、端口、基准检索DN、登录属性、用户DN、密码是否正确，等待时间不超过5秒。若填写有误，请根据右上角消息提示修改后重新提交；若确认无误将返回到**AD/LDAP**界面，AD/LDAP添加成功。

3. 管理AD/LDAP服务器。

在**AD/LDAP**管理界面，可对已添加的AD/LDAP进行管理，支持以下操作：

- 查看：

  点击已添加的AD/LDAP，展开详情页，可查看名称、端口号、基准检索DN、登录属性、用户DN、清除规则等基本属性。

- 测试：

  选中已添加的AD/LDAP服务器，点击**更多操作** > **测试**，会基于所填写配置信息尝试连接AD/LDAP。

- 同步：

  当AD/LDAP的配置信息发生变化，例如，设置新的清除规则，选中已更新配置信息的AD/LDAP，点击**更多操作** > **同步**，将清除ZStack中无效的绑定信息。

- 删除：

  目前仅支持添加一个AD/LDAP，如需添加其它AD/LDAP，或对已添加的AD/LDAP更新配置信息，需删除当前AD/LDAP，进行重新添加。

后续操作

至此，ZStack成功添加AD/LDAP，将获取AD/LDAP成员列表。接下来，ZStack需要绑定AD/LDAP成员。

4 绑定AD/LDAP成员

前提条件

ZStack账户（普通账户/管理员）与AD/LDAP成员（用户/用户组）的绑定关系如下：

- 普通账户：

  一套ZStack支持创建多个普通账户。

  - 一个普通账户可直接绑定一个或多个AD/LDAP成员（用户/用户组）
  - 普通账户绑定AD/LDAP用户组时，支持用户组中嵌套用户组
  - 一个AD/LDAP成员（用户/用户组）不可绑定多个普通账户
  - 一个AD/LDAP成员（用户/用户组）绑定一个普通账户后，不可再绑定管理员
  - 绑定普通账户的AD/LDAP成员登录ZStack后，所属资源、权限与当前所绑定的普通账户一致
- 管理员：

  一套ZStack仅支持创建一个管理员。

  - 管理员可直接绑定一个或多个AD/LDAP成员（用户/用户组）
  - 管理员绑定AD/LDAP用户组时，支持用户组中嵌套用户组
  - 一个AD/LDAP成员（用户/用户组）绑定管理员后，不可再绑定普通账户。
  - 绑定管理员的AD/LDAP成员登录ZStack后，所属资源、权限与当前所绑定的管理员一致

背景信息

普通账户绑定AD/LDAP成员，与管理员绑定AD/LDAP成员，操作方法完全一致，以下将以普通账户绑定AD/LDAP成员为例进行介绍。

操作步骤

1. 进入普通账户绑定AD/LDAP成员界面。

   在ZStack私有云主菜单，点击**平台管理** > **用户管理** > **账户**，进入**账户**界面，选择某一普通账户，进入其详情页。点击**AD/LDAP**，进入**AD/LDAP**界面。

   如图 *5: AD/LDAP界面*所示：

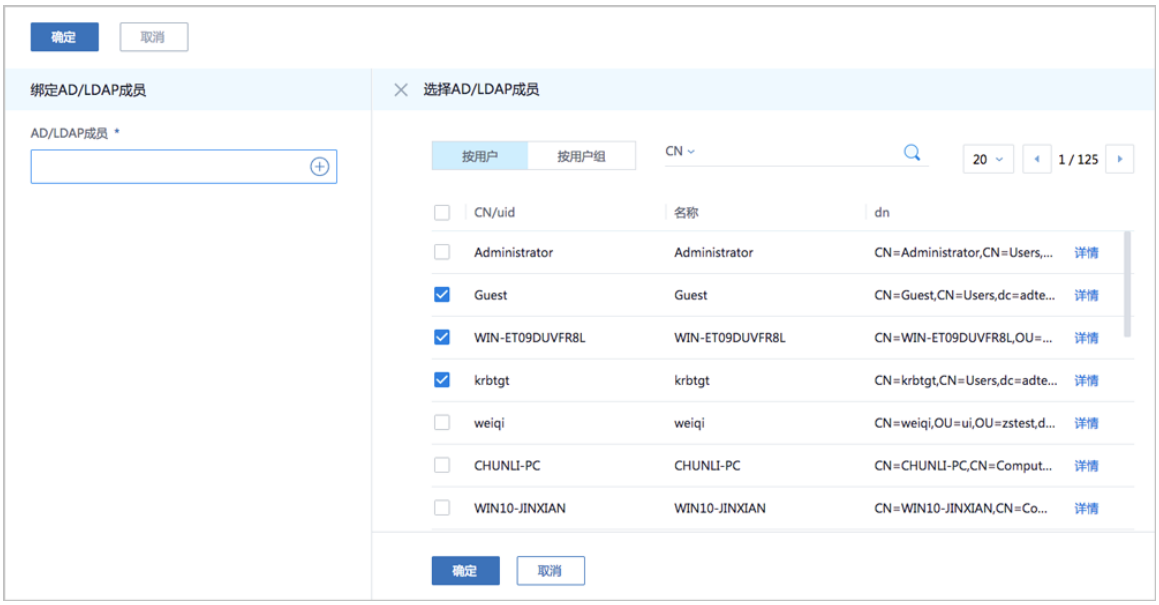
   图 5: AD/LDAP界面

2. 勾选绑定到普通账户的AD/LDAP成员。

   点击**操作 > 绑定AD/LDAP成员**，弹出**绑定AD/LDAP成员**界面，点击**+**，展开**选择AD/LDAP成员**列表页，分别提供**按用户**和**按用户组**两个分栏，可按需勾选绑定到该普通账户的AD/LDAP成员。

   如图 *6: 选择AD/LDAP成员*所示：

   图 6: 选择AD/LDAP成员

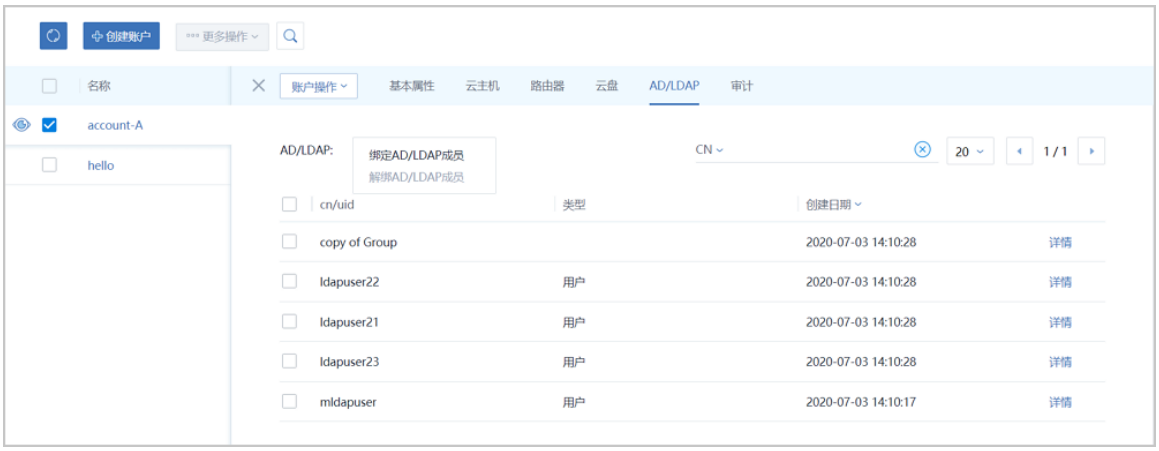


   - 目前支持按*CN*、*uid*、高级搜索等条件快速搜索
   - 可点击每个AD/LDAP成员的**详情**，查看更多属性

3. 依次点击**确定**按钮，所勾选AD/LDAP成员成功绑定到普通账户。

   如图 *7: 普通账户绑定AD/LDAP成员*所示：

   图 7: 普通账户绑定AD/LDAP成员



- 目前支持按*CN*、*uid*、高级搜索等条件快速搜索
- 可点击每个AD/LDAP成员的**详情**，查看更多属性
- 如需绑定更多AD/LDAP成员到普通账户，点击**操作** > **绑定AD/LDAP成员**即可。
- 如需将某一AD/LDAP成员从普通账户解绑，勾选该AD/LDAP成员，点击**操作** > **解绑AD/LDAP成员**即可，支持批量操作。

后续操作

至此，ZStack成功绑定AD/LDAP成员。接下来，可使用AD/LDAP成员登录属性直接登录ZStack云平台。

5 AD/LDAP登录

操作步骤

1. 打开AD/LDAP登录界面。

   如图 *8: AD/LDAP登录界面*所示：

   图 8: AD/LDAP登录界面

2. 使用已设置的AD/LDAP成员登录属性直接登录ZStack云平台。

   以AD为例：

   - 若已设置登录属性为*cn*，某一已绑定的AD成员可用*cn*相应的value（例如：名称*xiaoqiao.la*）作为ZStack登录名；
   - 该AD成员在AD域中使用的密码作为ZStack登录密码。

   如图 *9: 基于登录属性登录ZStack*所示：

   图 9: 基于登录属性登录ZStack

3. AD/LDAP成员成功登录ZStack，所属资源、权限与当前所绑定的ZStack账户一致。

   如图 *10: AD/LDAP登录成功*所示：

图 10: AD/LDAP登录成功

至此，ZStack接入AD/LDAP的配置方法介绍完毕。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

一个集群是类似物理主机（Host）组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统（虚拟机管理程序，Hypervisor），拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架（Rack）。

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

也称之为物理主机（或物理机），为云主机实例提供计算、网络、存储等资源的物理主机。

主存储（Primary Storage）

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、 Ceph、Shared Mount Point、Shared Block类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。支持ImageStore、Sftp（社区版）、Ceph类型。

镜像仓库（Image Store）

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机（VM Instance）

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

二层网络对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池（VXLAN Network Pool）

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络（即 VXLAN 网络），这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络（VXLAN）

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一时间点某一磁盘的数据状态文件。包括手动快照和自动快照两种类型。