AD&LDAP 认证配置举例

目 录

1 简介

1. LDAP

LDAP 是轻量目录访问协议，英文全称是 Lightweight Directory Access Protocol，简称为 LDAP。目录服务是一种特殊的数据库系统，其专门针对读取，浏览和搜索操作进行了特定的优化。目录一般用来包含描述性的，基于属性的信息并支持精细复杂的过滤能力。目录一般不支持通用数据库针对大量更新操作操作需要的复杂的事务管理或回卷策略。而目录服务的更新则一般都非常简单。这种目录可以存储包括个人信息、web 链接、jpeg 图像等各种信息。为了访问存储在目录中的信息，就需要使用运行在 TCP/IP 之上的访问协议—LDAP。

2. AD

AD 是 Active Directory 的缩写，AD 应该是 LDAP 的一个应用实例。比如：windows 域控的用户、权限管理应该是微软公司使用 LDAP 存储了一些数据来解决域控这个具体问题，只是 AD 顺便还提供了用户接口，也可以利用 ActiveDirectory 当做 LDAP 服务器存放一些自己的东西而已。比如 LDAP 是关系型数据库，微软自己在库中建立了几个表，每个表都定义好了字段。显然这些表和字段都是根据微软自己的需求定制的，而不是 LDAP 协议的规定。然后微软将 LDAP 做了一些封装接口，用户可以利用这些接口写程序操作 LDAP，使得 ActiveDirectory 也成了一个 LDAP 服务器。

2 名词解释

1. 条目

条目，也叫记录项，是 LDAP 中最基本的颗粒，就像字典中的词条，或者是数据库中的记录。通常对 LDAP 的添加、删除、更改、检索都是以条目为基本对象的。

2. DN

每一个条目都有一个唯一的标识名，如 dn="cn=baby,ou=marketing,ou=people,dc=mydomain,dc=org"。通过 DN 的层次型语法结构，可以方便地表示出条目在 LDAP 树中的位置，通常用于检索。

3. Basedn

LDAP 目录树的最顶部就是根，也就是所谓的“Base DN"，如"dc=mydomain,dc=org"。

在运维审计系统的 BaseDN 是指，以当前的组织作为根，搜索当前组织的范围。

4. 属性

每个条目都可以有很多属性（Attribute），比如常见的人都有姓名、地址、电话等属性。每个属性都有名称及对应的值。

5. 用户 Filter

运维审计系统的用户 Filter 是指，通过属性来过滤用户。

例如：(&(objectclass=person)(sAMAccountName=testuser))，代表过滤出 objectclass 为 person 并且 sAMAccountName 为 testuser 的用户。

6. Simple 方法

Simple 需用绑定查询用户及口令，配置相对灵活复杂，几乎所有的目录服务器都支持该验证方法。

7. Digest-md5 方法

仅需要知道 ldap 服务器的 FQDN 和 IP 地址既可，不需要绑定用户名和密码，配置方法相对简单。

8. 查询用户

在域控中，具有查询权限的用户。

3 配置前提

1. Windows（AD）

- 准备 Windows 域控主机一台。
- 准备 Windows 域控主机的相关信息：IP 地址、端口、计算机全名、查询用户、查询用户密码、BaseDN、用户 Filter。
- 确保域控主机到运维审计系统的网络可达。

2. LDAP

- 准备 LDAP 服务器一台。
- 准备 LDAP 服务器的相关信息：IP 地址、端口、查询用户、查询用户密码、BaseDN、用户 Filter。
- 确保 LDAP 服务器到运维审计系统的网络可达。

3. AD/LDAP 典型配置

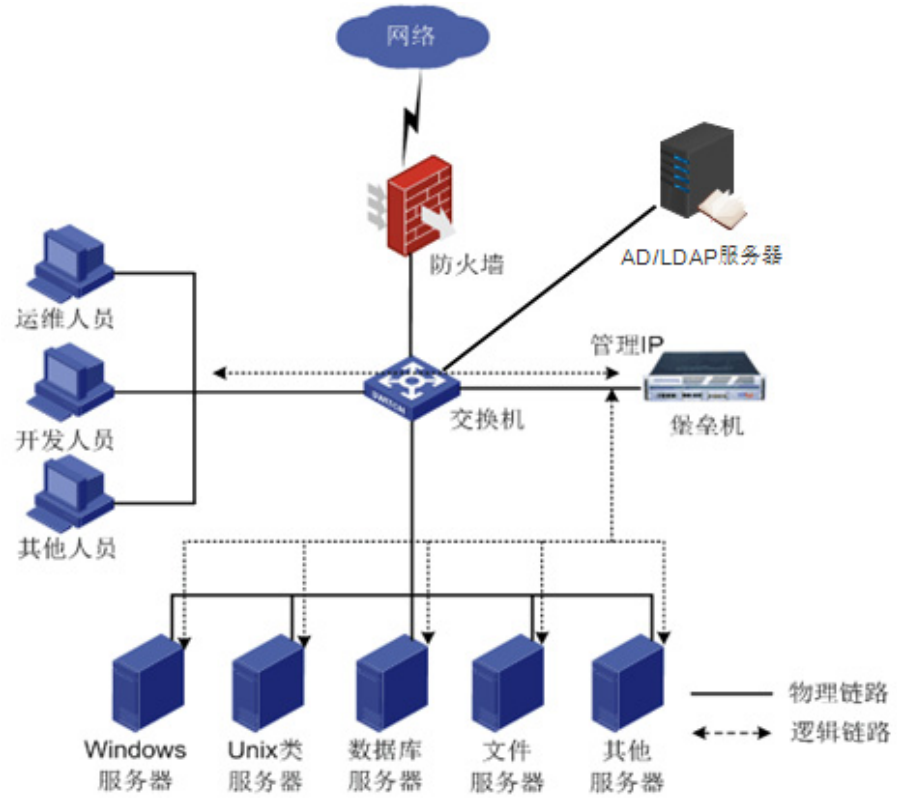
- DIGEST-MD5 设置：
  - 状态：启用服务器 1
  - 名称：Windows_AD
  - 方法：DIGEST-MD5
  - 服务器 1 全名：ad1.abc.com(AD（LDAP）服务器主机名全称)
  - 服务器 1 地址：192.168.6.200
  - 服务器 1 端口：389
  - 服务器 2 全名：ad2.abc.com
  - 服务器 2 地址：192.168.6.201
  - 服务器 2 端口：389
- SIMPLE 设置：
  - 状态：启用服务器 1
  - 名称：Windows_AD
  - 方法：SIMPLE
  - 服务器 1 地址：192.168.6.200
  - 服务器 1 端口：389

- 服务器 2 地址：192.168.6.201
- 服务器 2 端口：389
- 查询用户 DN：CN=Administrator,CN=Users,DC=dep,DC=com
- 查询用户密码：123456
- 用户 basedn：CN=Users,DC=dep,DC=com
- 用户 Filter：(&(objectclass=person)(sAMAccountName={username}))

4 配置举例

4.1 组网需求

图4-1 AD/LDAP 认证网络图



4.2 系统版本要求

适用产品版本：ESS 6101

4.3 Windows（AD） Digest-MD5认证

4.3.1 收集信息

- Windows 域控主机 IP 地址。
- Windows 域控主机的计算机全名。（控制面板\系统和安全\系统\计算机全名）
- Windows 域控主机 AD 服务的端口号。

4.3.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建 ldap 认证方式。

进入“策略配置 > 身份验证”，选择 ldap 协议，点击“创建”。

图4-2 创建 ldap 认证方式

3. 编辑 ldap 认证方式。

(1) 选择认证方法为“DIGEST-MD5”。

(2) 选择状态为：“启用服务器 1”。

(3) 填写“名称”、“服务器 1 全名”、“服务器 1 地址”、“服务器 1 端口”几个字段。

- 名称：填写此 AD 认证的名称。
- 服务器 1 地址：Windows 域控主机 IP 地址。
- 服务器 1 全名：Windows 域控主机的计算机全名。
- 服务器 1 端口：如果留空，默认为 389 端口。

(4) 点击“确定”，提交配置。

图4-3 配置 ldap 认证方式

4. 创建 ldap 用户。

进入“基本控制 > 用户账号”。点击“新建用户”。

图4-4 创建 ldap 用户

(1) 选择“身份验证方式”为刚才配置的名称。

(2) 填写“登录名”、“真实姓名”、“部门”、“ldap 用户名”这几个字段。

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- ldap 用户名：绑定该登录名对应的 ldap 账户，如果不填，则默认此项为登录名。

(3) 点击“保存”。

图4-5 配置 ldap 用户信息

5. 登录 ldap 用户。

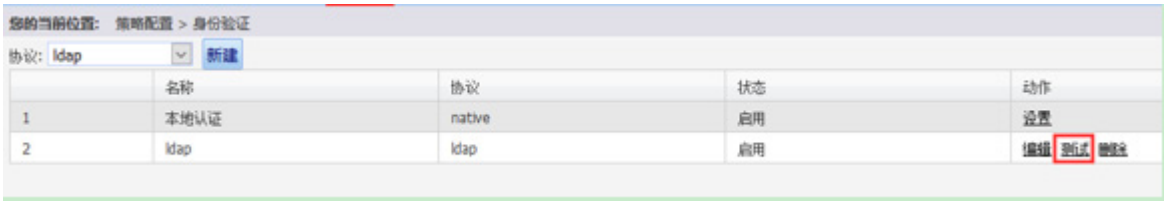
图4-6 ldap 用户登录

4.3.3 验证配置

进入超级管理员账户。

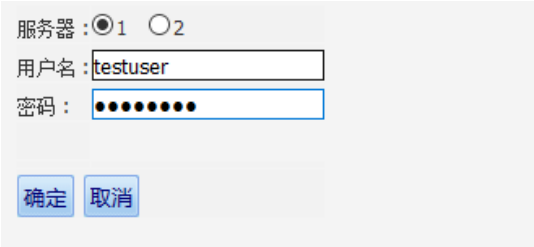
(1) 选择“策略配置 > 身份验证”，选择相应的 ldap 认证，点击“测试”。

图4-7 身份验证



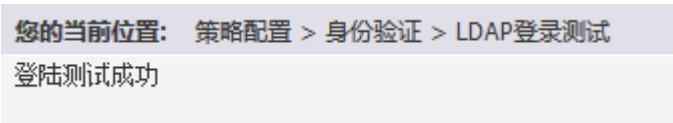
(2) 填写需要验证的账户密码，选择相应的服务器，点击“确定”。

图4-8 填写验证的账户密码



(3) 返回“登录测试成功”。

图4-9 登录成功



4.4 Windows（AD）simple认证

4.4.1 收集信息

- Windows 域控主机 IP 地址。
- Windows 域控主机 AD 服务的端口号。
- Windows 域控主机的查询用户的 DN（打开“cmd”，通过命令“dsquery user -name [username]”查询）。
- Windows 域控主机查询用户的密码。
- 用户 basedn（希望从哪一层组织下查找）。
- 用户 Filter（系统通过什么属性过滤用户）。

4.4.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建 ldap 认证方式。

进入“策略配置 > 身份验证”，选择 ldap 协议，点击“创建”。

图4-10 创建 ldap 认证方式

3. 编辑 ldap 认证方式。

(1) 选择认证方法为“SIMPLE”。

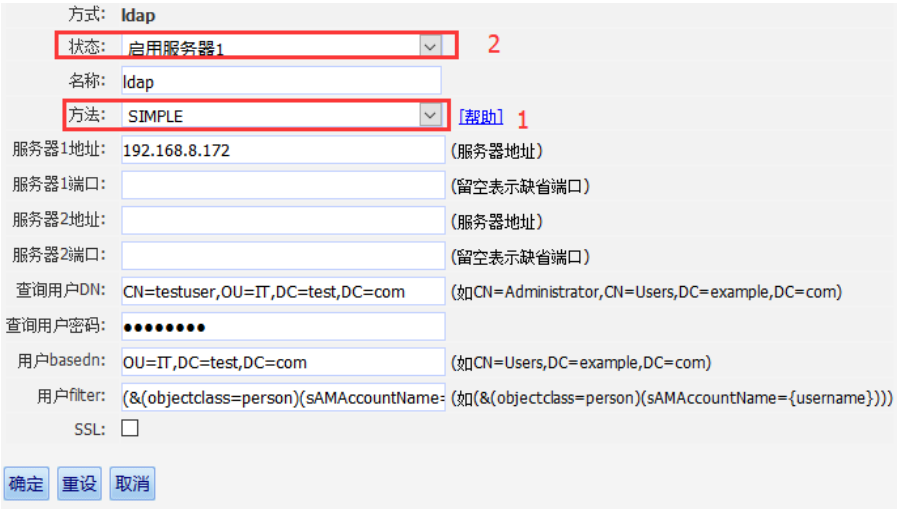
(2) 选择状态为：“启用服务器 1”。

(3) 填写“名称”、“服务器 1 地址”、“服务器 1 端口”、“查询用户 DN”、“查询用户密码”、“用户 BaseDN”、“用户 Filter”几个字段。

- 名称：填写此 ldap 认证的名称。
- 服务器 1 地址：Windows 域控主机 IP 地址。
- 服务器 1 端口：如果留空，默认为 389 端口。
- 查询用户 DN：具有查询权限的用户的 DN。
- 查询用户密码：查询用户密码。
- 用户 BaseDN：希望从那一层组织下查找。
- 用户 Filter：系统通过什么属性过滤用户。对于 windows 的域控可以通过“(&(objectclass=person)(sAMAccountName={username}))”过滤。其中{username}代表提交的变量，代表将来传入的用户名。

(4) 第 4 步：点击“确定”，提交配置。

图4-11 配置 ldap 认证方式



4. 创建 ldap 用户。

进入“基本控制 > 用户账号”。点击“新建用户”。

图4-12 创建 ldap 用户

(1) 选择“身份验证方式”为刚才配置的名称。

(2) 填写“登录名”、“真实姓名”、“部门”、“ldap 用户名”这几个字段。

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- ldap 用户名：绑定该登录名对应的 ldap 账户，如果不填，则默认此项为登录名。

(3) 点击“保存”。

图4-13 配置 ldap 用户

5. 登录 ldap 用户。

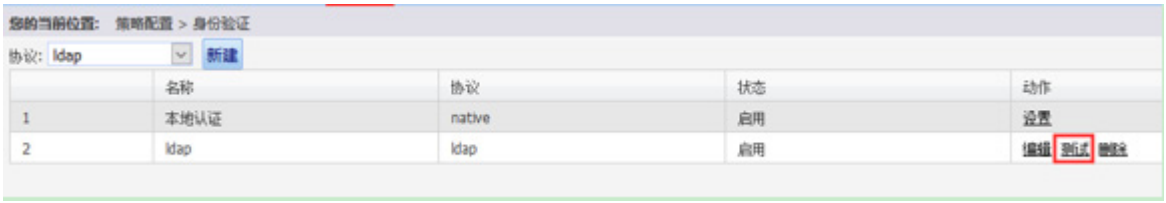
图4-14 ldap 用户登录

4.4.3 验证配置

进入超级管理员账户。

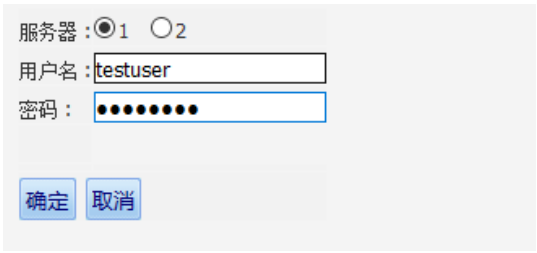
(1) 选择“策略配置 > 身份验证”，选择相应的 ldap 认证，点击“测试”。

图4-15 身份验证



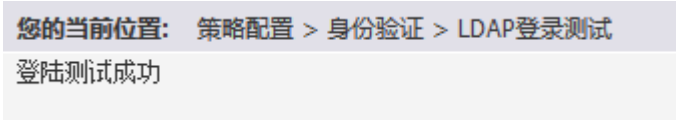
(2) 填写需要验证的账户密码，选择相应的服务器，点击“确定”。

图4-16 配置账户密码



(3) 返回“登录测试成功”。

图4-17 登录成功



4.5 Ldap simple认证

4.5.1 收集信息

- Ldap 服务器的 IP 地址。
- Ldap 服务器的 ldap 服务的端口号。
- Ldap 服务器的的查询用户的 DN。
- Ldap 服务器的查询用户的密码。
- 用户 basedn。（希望从那一层组织下查找）。
- 用户 filter。（系统通过什么属性过滤用户）。

4.5.2 配置步骤

1. 登录具有超级管理员角色的用户。

2. 创建 ldap 认证方式。

进入“策略配置 > 身份验证”，选择 ldap 协议，点击“创建”。

图4-18 创建 ldap 认证方式

3. 编辑 ldap 认证方式。

(1) 选择认证方法为“SIMPLE”。

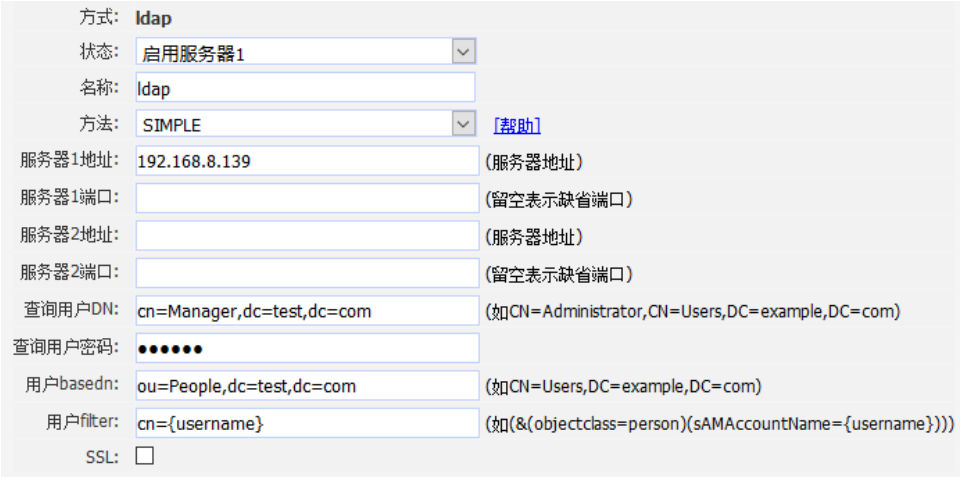
(2) 选择状态为：“启用服务器 1”。

(3) 填写“名称”、“服务器 1 地址”、“服务器 1 端口”、“查询用户 DN”、“查询用户密码”、“用户 BaseDN”、“用户 Filter”几个字段。

- 名称：填写此 ldap 认证的名称。
- 服务器 1 地址：Ldap 服务器的 IP 地址。
- 服务器 1 端口：如果留空，默认为 389 端口。
- 查询用户 DN：具有查询权限的用户的 DN。
- 查询用户密码：查询用户密码。
- 用户 BaseDN：希望从那一层组织下查找。
- 用户 Filter：系统通过什么属性过滤用户。这里通过 cn 属性可以过滤出用户，所以使用 cn={username}。

(4) 点击“确定”，提交配置。

图4-19 配置 ldap 认证方式



4. 创建 ldap 用户。

进入“基本控制 > 用户账号”。点击“新建用户”。

图4-20 创建 ldap 用户

(1) 选择“身份验证方式”为刚才配置的名称。

(2) 填写“登录名”、“真实姓名”、“部门”、“ldap 用户名”这几个字段。

- 登录名：登录运维审计系统的账户名。
- 真实姓名：该账户名的真实用户。
- 部门：选择相应的部门。
- ldap 用户名：绑定该登录名对应的 ldap 账户，如果不填，则默认此项为登录名。

(3) 点击“保存”。

图4-21 配置 ldap 用户信息

5. 登录 ldap 用户。

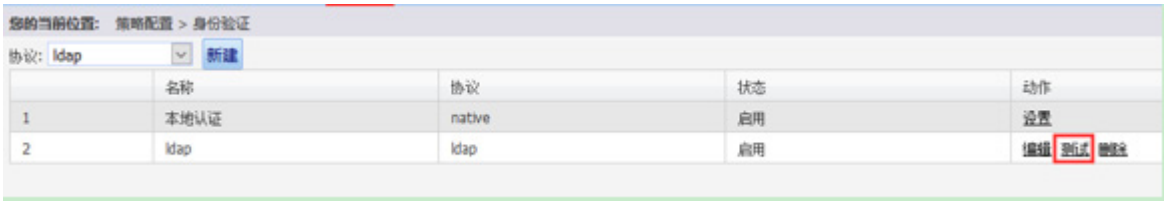
图4-22 Ldap 用户登录

4.5.3 验证配置

进入超级管理员账户。

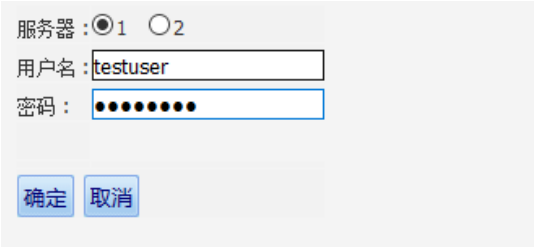
(1) 选择“策略配置 > 身份验证”，选择相应的 ldap 认证，点击“测试”。

图4-23 身份验证



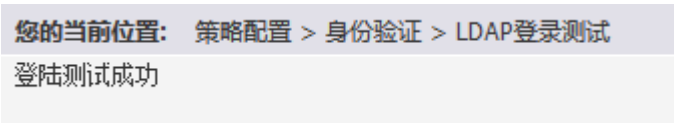
(2) 填写需要验证的账户密码，选择相应的服务器，点击“确定”。

图4-24 配置账户密码



(3) 返回“登录测试成功”。

图4-25 登录成功



4.6 Ldap用户批量导入

Ldap 用户的批量导入功能，仅限 simple 配置的方法。

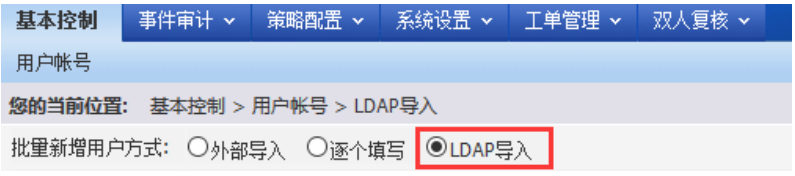
4.6.1 新建批量导入

(1) “基本控制 > 用户账号 > 批量导入”。

图4-26 批量导入

(2) “批量新增用户方式”选择“LDAP 导入”。

图4-27 配置批量新增用户方式



4.6.2 编辑批量导入规则

- Ldap 身份验证方式：选择之前配置的 ldap 的名称。

- 服务器地址：填写需要从哪一个 ldap 服务器进行导入。
- LDAP 服务端口：如果不填写，默认为 389 端口。
- 查询用户 DN：具有查询权限的用户的 DN。
- 查询用户密码
- 用户 basedn：希望从哪一层组织下导入。
- 用户 filter：系统通过什么属性过滤用户。这里通过 cn 属性可以过滤出用户，所以使用 cn=*。

图4-28 编辑批量导入规则

如果需要将 ldap 上的用户属性也导入运维审计系统，可以在这里设置。

图4-29 配置 ldap 上的用户属性

4.6.3 提交批量导入规则

运维审计系统会将查询到的用户以表格的方式列出。

如果确认无误，点击“确定”，创建用户。

图4-30 提交批量导入规则