

FAC 远程 LDAP 账户同步和认证

版本	1.0
时间	2014 年 4 月
支持的版本	FortiOS v4.3.x, v5.0.x
审核	已通过
反馈	support_cn@fortinet.com

目录

环境介绍.....	3
步骤一：FAC 配置远程 LDAP 客户端	3
步骤二：在 LDAP 服务器上查询账号属性	3
步骤三：FAC 配置远程 LDAP 账号同步规则	5
步骤四：FAC 查看同步成功的账号	6
步骤五：FAC 配置 radius 服务器.....	6
步骤六：FG 配置 radius 客户端.....	7
步骤七：FG 配置认证策略	7
步骤八：查看认证状态.....	8

环境介绍

本文档主要讲解使用 FAC 同步远程 LDAP 服务器上的账户，以及使用 FG 和 FAC 上同步的 LDAP 账户认证。

测试设备 FG80C 版本 v5.0.6 build271，FAC VM 虚拟机 版本 v3.0 build007

步骤一：FAC 配置远程 LDAP 客户端

登录到 FAC web 管理页面，在菜单 Authentication—>Remote auth servers—>LDAP 中创建客户端，如下图，填写具体的 ldap 服务器信息

Edit Remote LDAP Server			
Name:	ldap1		
Server name/IP:	10.20.1.5	Port:	389
Base distinguished name:	dc=vmad,dc=com		
Bind type:	<input type="radio"/> Simple <input checked="" type="radio"/> Regular		
Username:	administrator@vmad.com	Password:	*****
User object class:	person		
Username attribute:	sAMAccountName		
Group membership attribute:	memberOf		

Server name/IP: 填写 LDAP 服务器的 IP 地址

Base distinguished name: 填写 LDAP 服务器域名

Username: 填写查询的账号

步骤二：在 LDAP 服务器上查询账号属性

本例使用 windows server 2003 作为 LDAP 服务器，查询账号的命令为（cmd 中）

dsquery user: 查询所有账户信息

查询 zhangsan 的具体账户信息:

```
dsquery * CN=zhangsan,OU=组 1,OU=技术部,DC=vmad,DC=com -attr *
```

结果如下:

```
cn: zhangsan
```

```
sn: zhang
```

description: 技术部组 1

givenName: san

distinguishedName: CN=zhangsan,OU=组 1,OU=技术部,DC=vmad,DC=com

instanceType: 4

whenCreated: 03/28/2014 06:14:48

whenChanged: 03/31/2014 07:12:57

displayName: zhangsan

uSNCreated: 192544

uSNChanged: 200729

name: zhangsan

objectGUID: {E5B43B2B-BA7D-4C0C-AA6F-4E18590C768C}

userAccountControl: 66048

badPwdCount: 0

codePage: 0

countryCode: 0

badPasswordTime: 0

lastLogoff: 0

lastLogon: 0

pwdLastSet: 130404608883750000

primaryGroupID: 513

objectSid: S-1-5-21-3047542098-1488597564-1768353452-1140

accountExpires: 9223372036854775807

logonCount: 0

sAMAccountName: zhangsan

sAMAccountType: 805306368

userPrincipalName: zhangsan@vmad.com

objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=vmad,DC=com

mail: zhangsan@163.com

ADsPath: LDAP://server1.vmad.com/CN=zhangsan,OU=组 1,OU=技术部,DC=vmad,DC=com

步骤三：FAC 配置远程 LDAP 账号同步规则

在菜单 Authentication—>User Management—>User Groups 中新建一个用户组，取名 group3

在菜单 Authentication—>User Management—>Remote User Sync Rules 中新建规则，如下图

The screenshot shows the configuration for a Remote User Synchronization Rule. The fields are as follows:

- Name: rusr
- Remote LDAP: ldap1 (10.20.1.5:389)
- Sync every: 1 minute(s)
- LDAP filter: (description=技术部组1)
- Token-based authentication sync priorities:
 - FortiToken 200 (assign an available token)
 - None (users are synced explicitly with no token-based authentication)
 - FortiToken 200 (assign if serial number is provided)
 - E-mail
 - SMS
 - FortiToken Mobile (assign an available token)
- Sync as: Remote User
- Group to associate users with: group3

其中 Remote LDAP 选择步骤 1 中创建的客户端

Sync every: 同步账号的频率，本例为 1 分钟

LDAP filter: 规则过滤器，不写则同步所有账号，本例过滤描述(description)属性为技术部组 1 的所有成员。常用的过滤规则写法如下：

(&(description=技术部*)!(description=技术部/研发)))，过滤描述(description)属性包含技术部字样但不包含技术部/研发的所有成员

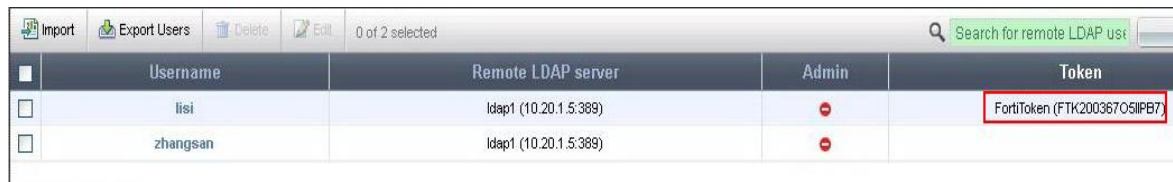
(|(description=技术部组 2)(description=财务部组 1))，过滤描述(description)属性是技术部组 2 或财务部组 1 的所有成员

Token-based authentication sync priorities: 基于 Token 认证的优先级，排在最上一行的最优先，以此类推。本例的规则是给同步到 FAC 上的用户分配 FortiToken 200，在 FortiToken 200 用尽后就不分配 Token 给用户了。

Group to associate with: 关联的用户组，本例使用 group3

步骤四：FAC 查看同步成功的账号

在 Authentication—>User Management—>Remote Users 菜单中查看成功同步的账户



	Username	Remote LDAP server	Admin	Token
<input type="checkbox"/>	lisi	ldap1 (10.20.1.5:389)	+	FortiToken (FTK20036705IIPB7)
<input type="checkbox"/>	zhangsan	ldap1 (10.20.1.5:389)	+	

注意，由于 FAC 上只有一个可用的 Token 200，因此账户 zhangsan 没有分配到 Token。

步骤五：FAC 配置 radius 服务器

在 Authentication—>RADIUS Service—>Clients 菜单中新建客户端，如下图



Edit RADIUS Client

Name: r1

Client name/IP: 10.20.1.162

Secret:

Description:

Authentication method:

- Enforce two-factor authentication
- Apply two-factor authentication if available (authenticate any user)
- Password-only authentication (exclude users without a password)
- FortiToken-only authentication (exclude users without a FortiToken)

Authenticate:

- All local users
- Local users from selected groups only (select groups below)
- Remote users from selected groups only (select groups below)
- All Windows AD users
- Windows AD users from selected groups only (select groups below)

Remote LDAP server: ldap1 (10.20.1.5:389)

Available remote user groups

Selected remote user groups

group3

Client name/IP: 填写防火墙的 IP 地址

Authenticate: 选择远程用户组

Selected remote user groups: 本例要填写 group3 步骤三中的用户组

步骤六：FG 配置 radius 客户端

在防火墙的用户&设备->认证->RADIUS 菜单中新建客户端，如下图

编辑RADIUS服务器

名称	<input type="text" value="r1"/>	
主服务器名称/IP	<input type="text" value="10.20.1.3"/>	
主服务器密钥	<input type="password" value="....."/>	<input type="button" value="测试"/>
从服务器名称/IP	<input type="text"/>	
从服务器密钥	<input type="password"/>	<input type="button" value="测试"/>
验证方案	<input checked="" type="radio"/> 用户默认验证方案 <input type="radio"/> 指定验证协议	
	<input type="text" value="PAP"/>	
NAS IP/呼叫站点ID	<input type="text"/>	
包含进所有用户组	<input checked="" type="checkbox"/> 启用	
<input type="button" value="确认"/>		<input type="button" value="取消"/>

Primary Server Name/IP: 填写 FAC 的 IP 地址

步骤七：FG 配置认证策略

在策略->策略->策略 菜单中新建认证策略，如下图

编辑输出策略

策略类型	<input checked="" type="radio"/> 防火墙 <input type="radio"/> VPN	
策略子类型	<input type="radio"/> 地址 <input checked="" type="radio"/> 用户认证 <input type="radio"/> 设备认证	
流入接口	<input type="text" value="wan2"/>	<input type="button" value="⊕"/>
源地址	<input type="text" value="all"/>	<input type="button" value="⊕"/>
流出接口	<input type="text" value="internal"/>	<input type="button" value="⊕"/>
<input checked="" type="checkbox"/> 启用NAT		
<input checked="" type="radio"/> 使用目标接口地址	<input type="checkbox"/> 保持端口号	
<input type="radio"/> 动态IP池	<input type="text" value="点击添加..."/>	

配置认证规则

<input type="button" value="Create New"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>					
用户/组	目标地址	服务	时间表	Security	流量控制配置	日志记录	Action
<input type="button" value="radius1"/>	all	ALL	always		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> ACCEPT
<input type="button" value="ANY"/>	all	ALL	always		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> DENY

步骤八：查看认证状态

使用用户 lisi 通过防火墙认证上网，在防火墙上查看认证状态如下：

User Name	User Group	Policy ID	Duration	IP Address	Traffic Volume	Method
lisi	radius1(r1)	3	0 day(s) 0 hour(s) 0 minute(s)	10.10.1.1	121.59 K	Firewall

在 FAC 上查看认证日志如下：

Log Record Detail	
ID	4153
Timestamp	Tue Apr 1 10:10:47 2014
Level	information
Action	Authentication
Status	Success
NAS Name/IP	10.20.1.162
Message	Remote LDAP user authentication with FortiToken s successful
User	lisi
Log Type	
Type Id	20002
Name	Authentication OK With FT K
Sub Category	Authentication
Category	Event
Description	Authentication successful with FortiToken