



ANYSEC 行为管理 AD SSO 配置手册



版权所有:深圳市中科网威科技有限公司

 · 技术支持--0755-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-83658
 · 25-83658
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836



-、手册说明

1.1. 场景说明

该手册只针对"域控制器策略派发模式"有效。

1.2. 域控制器策略派发模式

"域控制器策略派发模式"通过域控制器的组策略来实现单点登录。可实现域用户登录 到域时自动完成到行为管理网关设备的 WEB 认证,在域用户从域注销出来时自动注销在行为 管理网关设备的登录。

二、域控制器设置

2.1.配置与用户登录脚本

1. 利用域管理员登录域后,找到 2008 AD server'管理工具'-'组策略管理',如图:

| | 194 | → 📝 ADSI 编辑器 |
|---------------------------|------------------|---|
| 01 | 63 | 🐺 DHCP |
| | <u>-</u> | A DNS |
| ──── 记事本 | • • • • • • | 🖏 Internet 信息服务(IIS)管理器 |
| ~ | | Q iSCSI 发起程序 |
| C Internet Explorer | Administrator | 🔀 Windows PowerShell Modules |
| | 文档 | Windows Server Backup |
| 组策略管理 | | - 🗳 Windows 部署服务 |
| Active Directory 田白和计算 | 计算机 | Windows 内存诊断 |
| 机 机 | | → 安全配置向导 |
| | 网络 | → 本地安全策略 |
| eSate用户上共 | | — — · · · · · · · · · · · · · · · · · · |
| @ Falancel | 控制面板 ▶ 過各和打印和 | ◎ 服务 |
| C Lthereal | | 1. 服务器管理器 |
| Active Directory 管理由心 | Melali Hi B X | — 🚰 高级安全 Windows 防火墙 |
| SE weeks precessi DE 1.0. | 管理工具 | ▶ 😴 共享和存储管理 |
| 😫 dns | | 💁 计算机管理 |
| | 帮助和支持 | ④ 任务计划程序 |
| 【 Internet 信息服务(IIS)管理器 | 运行 | ■ 事件查看器 |
| - | - | 🔄 数据源 (ODBC) |
| ▶ 所有程序 | | ☑ 系统配置 |
| | ○ 注谐 ▶ | ◎ 性能监视器 |
| | | 🗾 用干 Windows PowerShell 的 Active Direc |
| | | ■ |
| | | 🤌 组件服务 |

 · 技术支持--0755-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-836582
 · 25-83658
 · 25-83658
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836



2. 右键点击组策略选项, "Default Domain Policy",选择编辑



3. 组策略编辑页面,依次点击【用户配置】-【windows 设置】-【脚本(登录/注销)】



4. 双击"登录"选项,在弹出的登录脚本编辑窗口左下角点击"显示文件",将打开一个目录,然后将登入脚本文件(ad_login.exe)拷贝到该目录下,关闭该目录







5. 在弹出的登录脚本编辑窗口中单击"添加"按钮,在添加脚本窗口中,点击浏览,选择步骤4操作的登入脚本文件(ad_login.exe),并在脚本参数中输入范例 IP:5850, 其中 IP 为行为管理设备接口 IP,端口固定为 5850,参数之间以英文字符的冒号分隔,点击应用,再点击确定,一次关闭登入属性页面配置。



 · 技术支持--0755-83658229
 · 公24 小时技术值班热线-----135-1069-3536
 · 河河市龙华区观澜街道观光路1301-80号电子科技大学(深圳)高等研究院3号楼1401



6. 配置完脚本后,依次点击 PC 桌面左下角"开始-运行",在弹出的运行窗口中输入:"gpupdate /force"更新策略,并点击确定,配置策略生效

7. 登录脚本程序设定 OK, 当域用户登录时, 该脚本程序通过域下发到 PC 的启动目录, 并在该 PC 执行

2.2 配置注销脚本程序

1. 步骤如上述第5步

| 文件(F) 操作(A) 查看(V) 帮 | 助(H) | | |
|---|--------------------------------------|---------------------------------------|-------------------------------|
| 🗢 🔿 🖄 📅 🖾 🗟 🛛 🖬 | | | |
| ■ Default Domain Policy [WIN-6 ● ● 计算机配置 | 日本(登录/注销) | | |
| 土 <u>一</u> 束略 王 <u></u> 首选项 | 注销 | <u>名称</u> 回 | |
| 日 🕵 用户配置 | 显示属性 | 副注销 | |
| □ 東啲 | 描述: 数据包含 即本 Remarks | ····································· | <u>? ×</u> |
| □ □ □ □ ○ ○ | · 注销 | 即本(Default Domain Policy 的) | |
| Ⅱ □ 管理模板:从本地计: Ⅱ □ 首选项 | _ 名称 | | 移 (0) 移 (m) |
| | | <u>添力</u> 编辑 | Ω Φ) 〕(Ε) 除余 (Β) |
| | 」 要查看保存在此 〕 ↓ 扩展√; 显示文件 (S) | | |



- 用心服务

2. 在弹出的注销脚本编辑窗口中单击"添加"按钮,在添加脚本窗口中,点击浏览,选择步骤4操作的注销脚本文件(ad_logout.exe),并在脚本参数中输入范例 IP:5850,其中 IP 为行为管理设备接口 IP,端口固定为 5850,参数之间以英文字符的冒号分隔,点击应用,再点击确定,一次关闭注销属性页面配置。

| 文件(F) 操作(A) 查看(V) 帮 | 助(H) | | |
|---|-------------|-----------------------------------|--------|
| 🗇 🄿 🖄 📅 🖬 🖬 🛃 🗗 | 1 | | |
| 圓 Default Domain Policy [WIN-€ □ 🐏 计算机配置 | 副 脚本 | (登录/注销) | |
| 田 🧰 策略 田 🛅 首选项 | 注销 | | |
| 日 💰 用户配置 | 显示属性 | ■ 注销 | |
| □ □ 採曲 | 描述: 数据包含 | E销 国性 脚本 PowerShell 脚本 | ?× |
| 副本 (豆木/注明) 団 金 安全设置 団 (□) 文件夹重定向 団 (□) 基于策略的 QoS | | 注销 脚本 (Default Domain Policy 的) | |
| 王 🎢 Internet Explor 王 🦰 管理模板: 从本地计: | | 添加脚本 | × |
| | | 脚本名(N): [ad_logout. exe | 浏览 (8) |
| | | 脚本参数 (P): [172.16.100.25:5850] | |
| | | 确定 | |
| | | 要查看保存在此组策略对象中的脚本文件,请按下面 | 按钮。 |
| | ∖扩展√ः | 显示文件(\$) | |



3. 配置完脚本后,依次点击 PC 桌面左下角"开始-运行",在弹出的运行窗口中输入:"gpupdate /force"更新策略,并点击确定,配置策略生效

4. 登录脚本程序设定 OK, 当域用户登录时, 该脚本程序通过域下发到 PC 的启动目录, 并在该 PC 执行

三、 行为管理网关设置简述

1. AD 域用户导入

| □ 设备状态 | 修改LDAP/AD导入规则 | |
|-------------|---------------|--|
| ■ 实时监控 | 名称 | AD2008 |
| ■ 系统配置 | 服务器类型 | Active Directoty 🖌 |
| ■ 系统对象 | 服务器地址 | 172.16.122.226 |
| ■ 网络配置 | 服务器端口 | 389 |
| 圕 防火 墙 | 导入入口(BaseDN) | dc=hytf2013,dc=com |
| ■ VPN配置 | 用户查找 | ● 本地用户查询 ○ 匿名查询 |
| | 用户名 | cn=administrator,cn=users,dc=hytf2013,dc=com |
| □ 组织结构 | 密码 | |
| □ 批量导入 | 用户名属性字段 | sAMAccountName V 参数默认 |
| □ LDAP/AD导入 | 显示名属性字段 | displayName 🗸 |
| | 绑定属性字段 | 绑定格式同组织结构中的绑定格式,多条用",号分开 |
| | 描述属性字段 | |
| □ 抗重申请临时账号 | 导入目的组 | Root/AD2008 选 |
| □ 木甲抗账户列表 | 自动更新 | |
| □ DKey 管理 | 覆盖原有组织结构 | 査 ▼ |

2. 启用 AD SS0 开关



行为管理设定完毕, PC 登入登出测试