V7防火墙使用默认证书配置SSL VPN LDAP认证典型案例（命令行配置）

SSL VPN　张新姿　2020-10-31 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：本案例适用于如M9006、M9010、M9014等M9K系列的防火墙。

注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P19版本上进行配置和验证的。

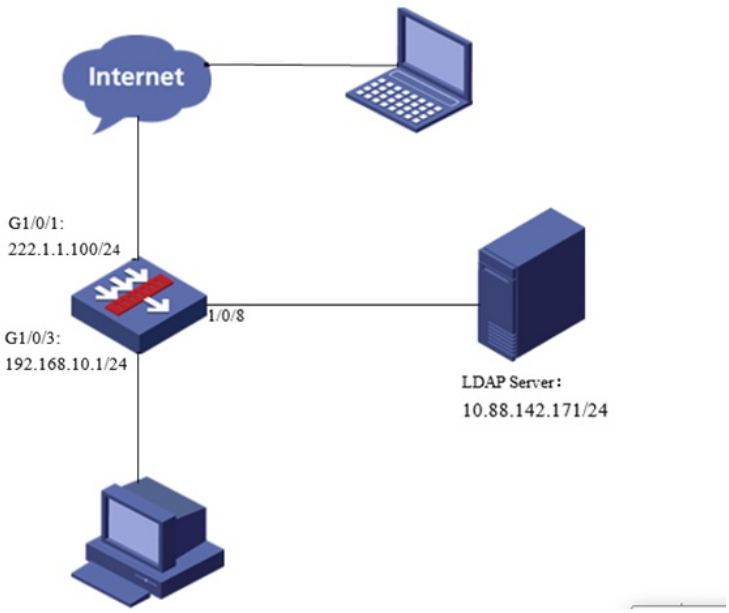
服务器系统：windows server 2012 R2

1.2 配置需求及实现的效果

V7防火墙部署在互联网出口，外网终端通过INode软件拨入SSL VPN，防火墙通过LDAP Server对用户进行远程认证和授权。认证成功后用户可以访问内网192.168.10.0网段的资源。IP地址及接口规划如下表所示：

外网接口	公网地址/掩码	内网接口	内网地址/掩码	与LDAP互联口	LDAP服务器地址
GE1/0/1	222.1.1.100/24	GE1/0/3	192.168.10.1/24	GE1/0/8	10.88.142.171

2 组网图



配置步骤

1 配置步骤

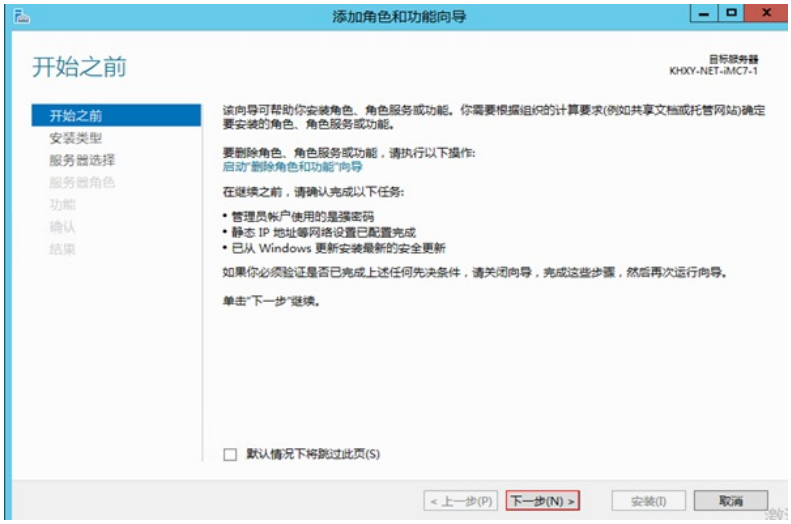
1.1 Windows server 2012镜像安装

请参考微软镜像安装手册或者百度自行解决，本文对Windows server 2012系统安装不做赘述。

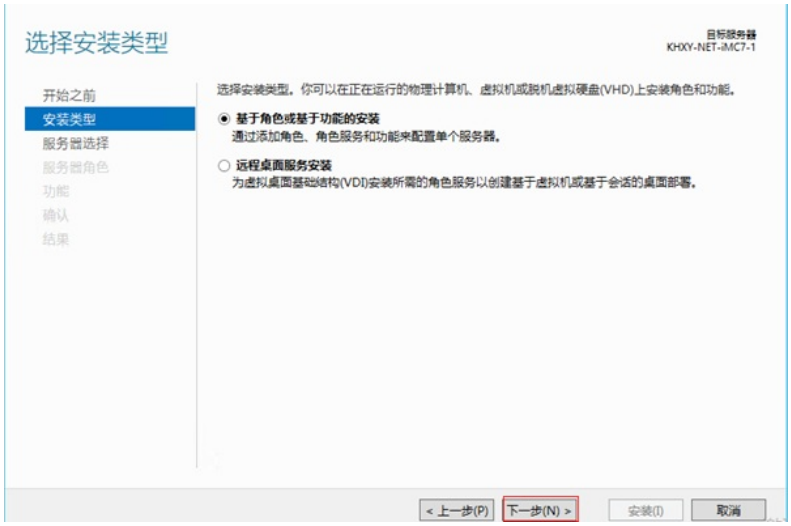
1.2 LDAP服务器设置

1、在服务器界面点击“开始”旁边的服务器管理器按钮，调出管理器界面后点击“添加角色和功能选项”。

2、在出现的角色和功能向导中点击下一步。

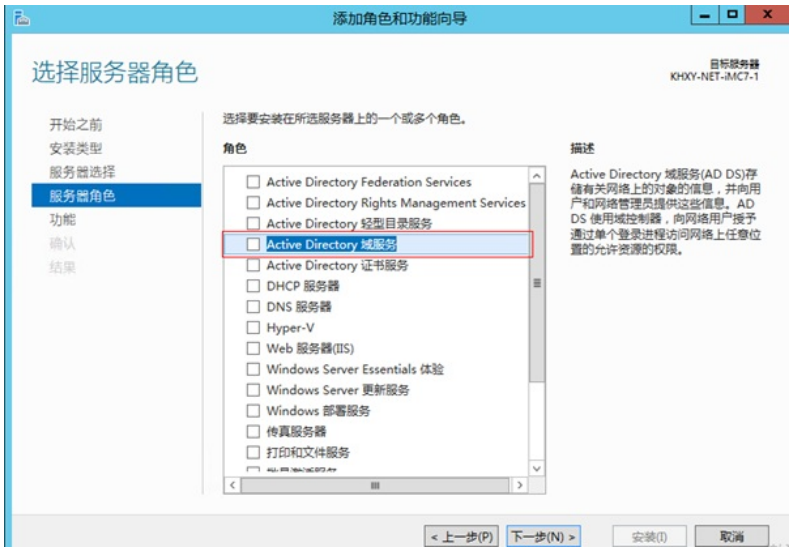


3、安装类型选择"基于角色或基本功能的安装"后点击下一步。

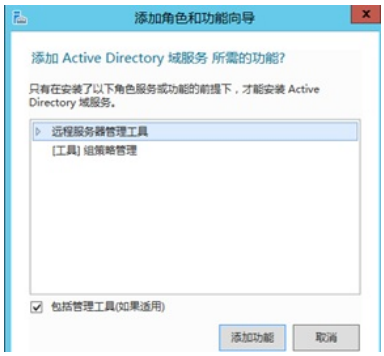


4、服务器选择显示为本机地址的服务器。

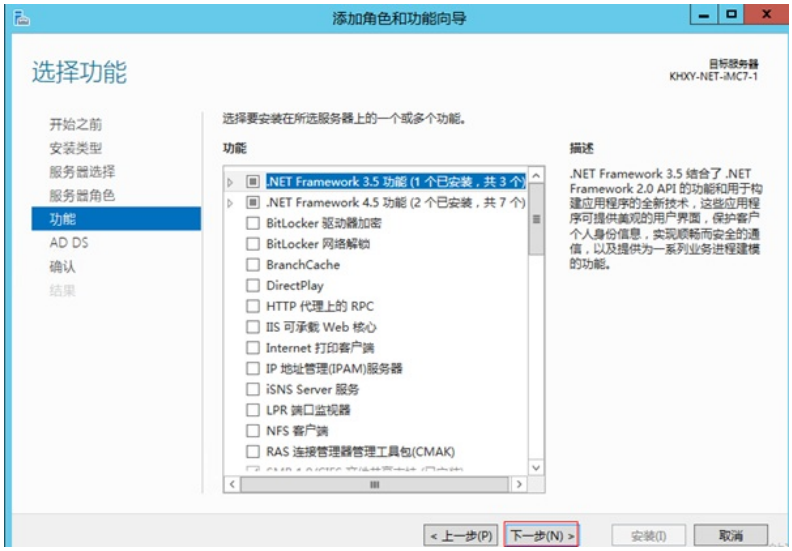
5、在服务器角色中点击Active Directory 域服务。



在点击过程中会弹出新的对话框，点击远程服务器管理工具后选择添加功能。



6、如果没有特殊需要不需要选择任何功能直接点击下一步即可。



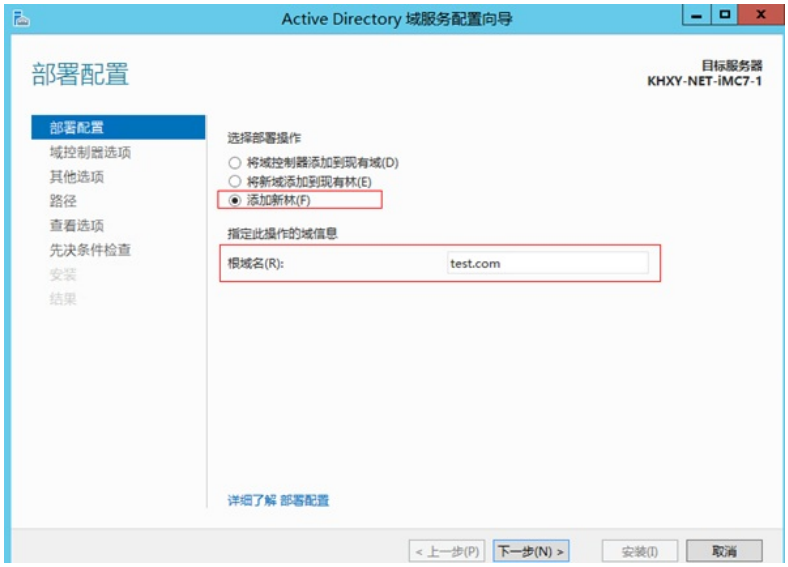
7、出现Active Directory 域服务点击下一步。

8、确认无误后点击安装Active Directory 域服务程序，安装成功后关闭向导。

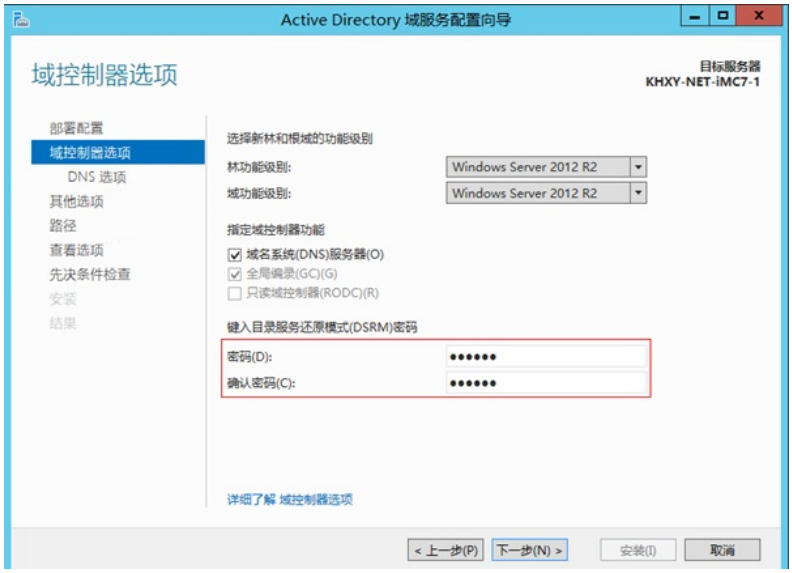
9、服务器部署成功后出现AD DS选项，点击“更多”打开域配置界面。

10、点击“将此服务器提升为域控制器”选项。

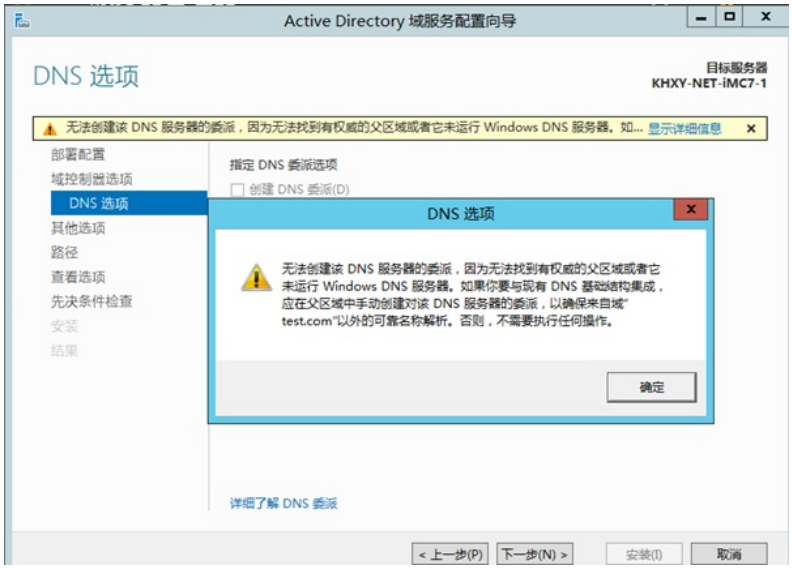
11、选择添加新林并且将根域名设置为test.com。



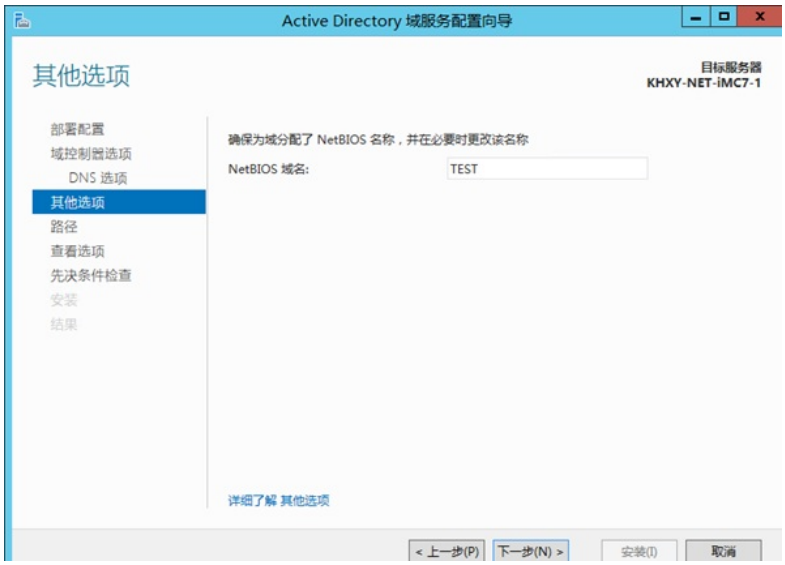
12、创建目录服务还原密码后点击下一步。



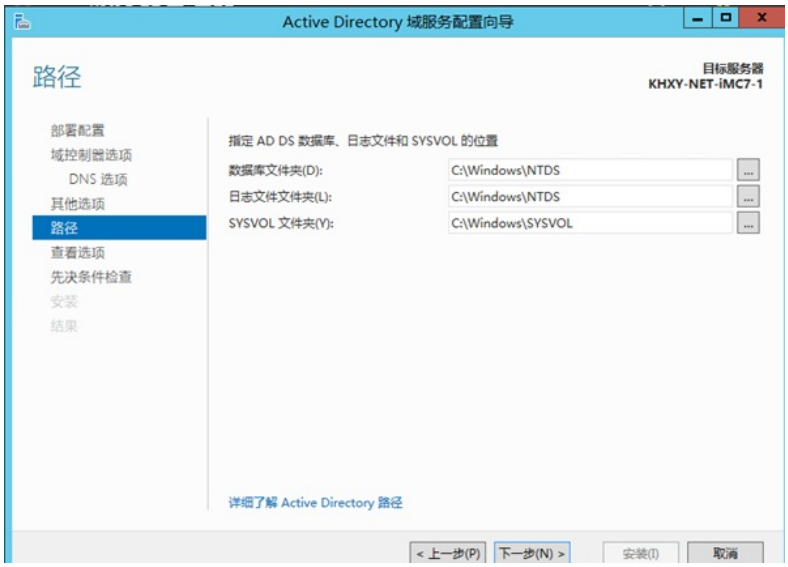
13、在DNS选项设置中会出现报错无法创建DNS服务器，可以忽略直接下一步即可。



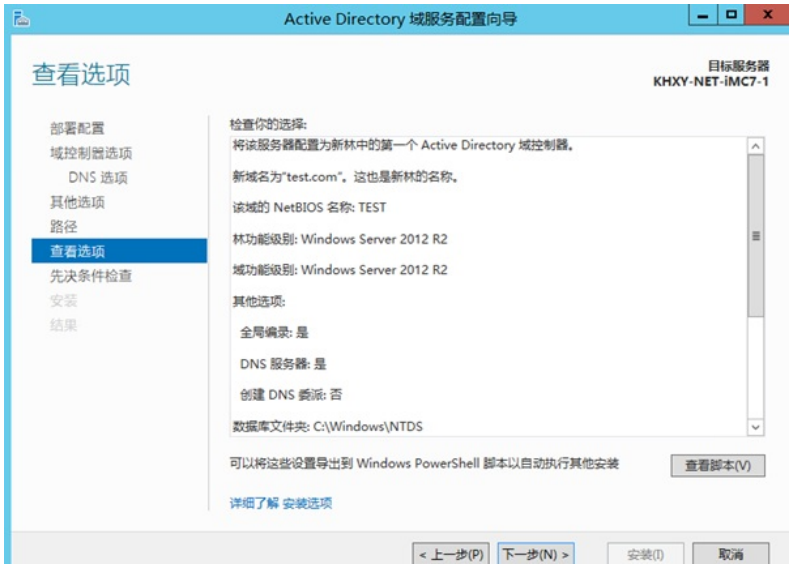
14、设置NetBIOS域名，系统已经根据根域默认为TEST不用修改点击下一步。



15、选择数据库、日志、SYSVOL文件夹的目录。

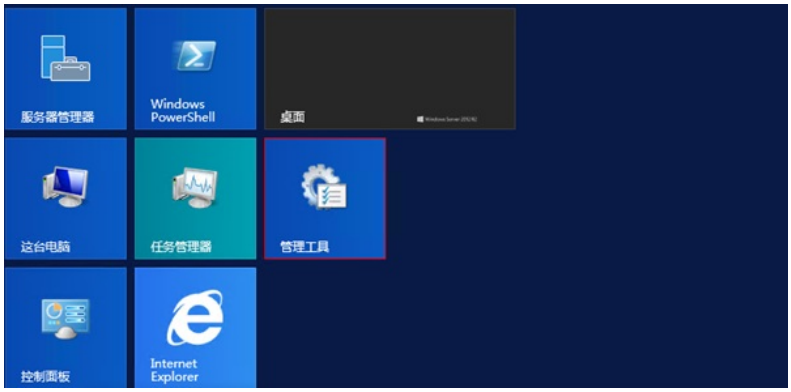


16、检查选项无误后选择下一步。



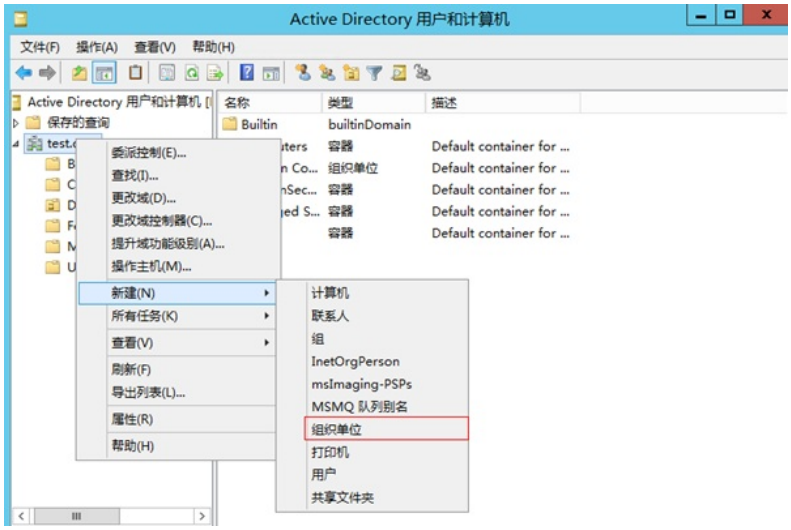
17、先决条件检查完成后选择安装，安装完成后点击关闭，关闭需要重启服务器后域名系统才能正常工作。

18、开启开启后选择管理工具。

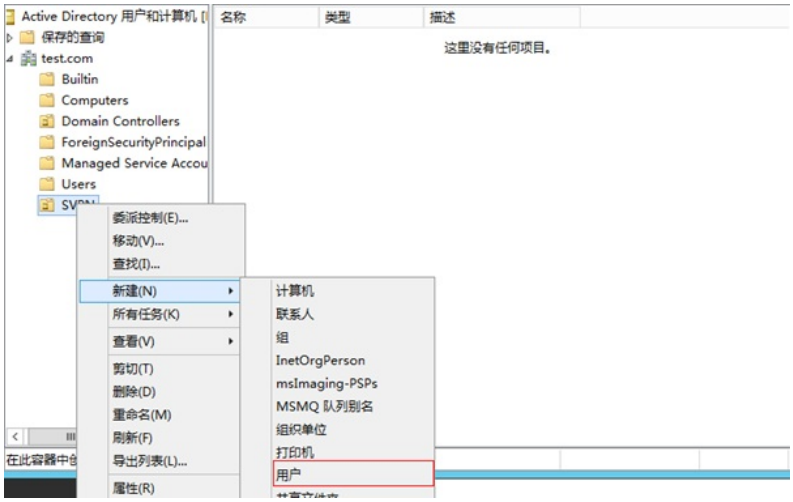


19、点击Active Directory 用户和计算机

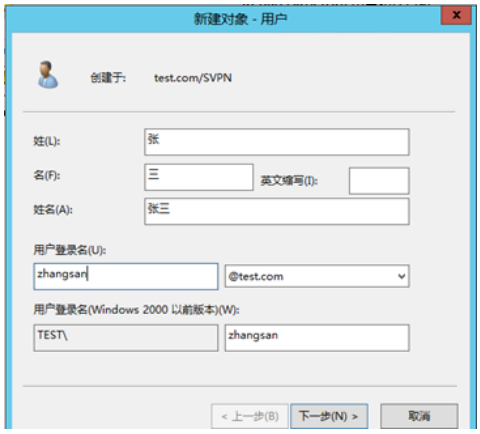
20、新建一个SVPN的组织单位用来存储SSL VPN用户。



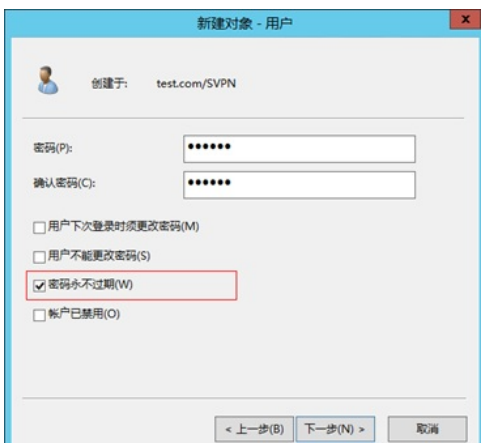
21、在SVPN组中添加用户



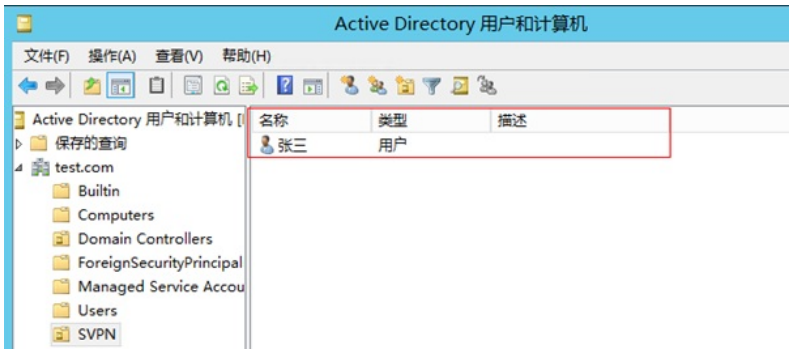
22、添加用户为张三设置登录账号为zhangsan。



23、设置密码并设置密码为永不过期。



24、设置完成后出现张三用户，至此LDAP服务器所有配置完成。



1.1 防火墙侧配置

1.1.1 配置SSL VPN网关

#SSLVPN网关IP地址填写防火墙1口地址222.1.1.1.00，端口号修改为4433，缺省端口为443，443端口和https端口冲突，然后使能网关配置。

<H3C>sys

[H3C]sslvpn gateway SSLVPNGW

[H3C-sslvpn-gateway-SSLVPNGW]ip address 222.1.1.100 port 4433

[H3C-sslvpn-gateway-SSLVPNGW]service enable

[H3C-sslvpn-gateway-SSLVPNGW]quit

#创建SSL VPN AC接口1,配置接口IP为10.10.10.1/24

[H3C]interface SSLVPN-AC 1

[H3C-SSLVPN-AC1]ip address 10.10.10.1 255.255.255.0

[H3C-SSLVPN-AC1]quit

#创建地址池名称为“SSLPOOL”，指定IP地址范围为10.10.10.2——10.10.10.254

[H3C]sslvpn ip address-pool SSLPOOL 10.10.10.2 10.10.10.254

#创建ACL 3999，允许SSL VPN用户访问的内网资源192.168.10.0/24网段

[H3C]acl advanced 3999

[H3C-acl-ipv4-adv-3999]rule permit ip destination 192.168.10.0 0.0.0.255

[H3C-acl-ipv4-adv-3999]quit

1.1.2 配置SSL VPN实例

配置SSL VPN访问实例“SSLVPNSL”引用SSL VPN网关“SSLVPNGW”

[H3C] sslvpn context SSLVPN

[H3C-sslvpn-context-SSLVPN]gateway SSLVPNGW

#引用SSL VPN接口1

[H3C-sslvpn-context-SSLVPN]ip-tunnel interface SSLVPN-AC1

#引用SSL VPN地址池，掩码和dns

[H3C-sslvpn-context-SSLVPN]ip-tunnel address-pool SSLPOOL mask 255.255.255.0

[H3C-sslvpn-context-SSLVPN]ip-tunnel dns-server primary 114.114.114.114

#创建路由列表“NEIWANG”，添加路由表项192.168.10./24

[H3C-sslvpn-context-SSLVPN]ip-route-list NEIWANG

[H3C-sslvpn-context-SSLVPN-route-list-NEIWANG] include 192.168.10.0 255.255.255.0

创建SSL VPN策略组“SSLVPNZIYUAN”，引用路由列表“NEIWANG”，配置ACL限制，只有通过ACL检查的报文才可以访问IP资源、配置SSL用户认证域为svpn域。

[H3C-sslvpn-context-SSLVPN]policy-group SSLVPNZIYUAN

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]filter ip-tunnel acl 3999

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]ip-tunnel access-route ip-route-list NEIWANG

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]quit

[H3C-sslvpn-context-SSLVPN]aaa domain svpn

[H3C-sslvpn-context-SSLVPN]service enable

[H3C-sslvpn-context-SSLVPN]quit

1.1.3 创建SSL VPN用户组

创建SSL VPN用户组名称为svpn并与SSL VPN资源“SSLVPNZIYUAN”绑定。

[H3C] user-group svpn

[H3C-ugroup-svpn]authorization-attribute sslvpn-policy-group SSLVPNZIYUAN

[H3C-ugroup-svpn]quit

1.1.4 创建LDAP服务器

login-dn是LDAP管理账号的路径（要求此管理账号有读权限或者管理员权限）、login-password对应管理员账号的密码、ip对应LDAP服务器的IP地址、search-base-dn表示要查找的用户所在的目录、user-parameters samaccountname参数表示查找用户属性samaccountname值，设备默认查询用户属性查询CN值。

[H3C]ldap server svpn

[H3C-ldap-server-svpn]login-dn cn=administrator,cn=users,dc=test,dc=com

[H3C-ldap-server-svpn]search-base-dn ou=svpn,dc=test,dc=com

[H3C-ldap-server-svpn]ip 10.88.142.171
[H3C-ldap-server-svpn]login-password simple xxxxxxx
[H3C-ldap-server-svpn]user-parameters user-name-attribute samaccountname
[H3C-ldap-server-svpn]quit

1.1.5 创建LDAP方案

创建LDAP方案将LDAP认证和授权全部指向LDAP服务器。

[H3C]ldap scheme svpn
[H3C-ldap-svpn]authentication-server svpn
[H3C-ldap-svpn]authorization-server svpn

1.1.6 创建SSL VPN认证域

创建SSL VPN认证域，将认证授权全部改向svpn方案，并且指定认证用户组为svpn组。

[H3C]domain svpn
[H3C-isp-svpn]authorization-attribute user-group svpn
[H3C-isp-svpn]authentication sslvpn ldap-scheme svpn
[H3C-isp-svpn]authorization sslvpn ldap-scheme svpn
[H3C-isp-svpn]accounting sslvpn none

1.1.7 配置与LDAP服务器互联端口

[H3C]interface GigabitEthernet 1/0/8
[H3C-GigabitEthernet1/0/8]ip address 10.88.142.1 255.255.255.0
[H3C-GigabitEthernet1/0/8]quit

1.1.8 将SSL VPN端口加入安全域，放通对应安全策略

#新建安全域，名称为“SSLVPN”，将SSL VPN端口1加入到安全域“SSLVPN”

[H3C]security-zone name SSLVPN
[H3C-security-zone-SSLVPN]import interface SSLVPN-AC1
[H3C-security-zone-SSLVPN]quit

#新建安全域LDAP将1/0/8接口加入该区域

[H3C]security-zone name LDAP
[H3C-security-zone-DMZ]import interface GigabitEthernet 1/0/8
[H3C-security-zone-DMZ]quit

#创建服务对象组，组名称为4433，匹配SSLVPN端

[H3C]object-group service 4433
[H3C-obj-grp-service-4433]service tcp destination eq 4433
[H3C-obj-grp-service-4433]quit

#配置配置安全策略将Untrust到Local域目的端口为TCP4433端口放通

[H3C]security-policy ip
[H3C-security-policy-ip]rule 5 name Untrst-Local
[H3C-security-policy-ip-5-Untrst-Local]action pass
[H3C-security-policy-ip-5-Untrst-Local]source-zone Untrust
[H3C-security-policy-ip-5-Untrst-Local]destination-zone Local
[H3C-security-policy-ip-5-Untrst-Local]service 4433
[H3C-security-policy-ip-5-Untrst-Local]quit

#配置配置安全策略,放通源安全域为SSLVPN，目前安全域为“Trust”的数据流量

[H3C-security-policy-ip]rule 10 name SSLVPN-Trust
[H3C-security-policy-ip-10-SSLVPN-Trust]action pass
[H3C-security-policy-ip-10-SSLVPN-Trust]source-zone SSLVPN
[H3C-security-policy-ip-10-SSLVPN-Trust]destination-zone Trust
[H3C-security-policy-ip-10-SSLVPN-Trust]quit

#配置配置安全策略,放通安全域为DMZ、Local域的数据流量

[H3C-security-policy-ip]rule 15 name DMZ-local
[H3C-security-policy-ip-15-DMZ-local]action pass
[H3C-security-policy-ip-15-DMZ-local]source-zone DMZ
[H3C-security-policy-ip-15-DMZ-local]source-zone Local
[H3C-security-policy-ip-15-DMZ-local]destination-zone DMZ
[H3C-security-policy-ip-15-DMZ-local]destination-zone Local
[H3C-security-policy-ip-15-DMZ-local]quit

1.2 保存配置

save force

1.3 配置验证，查看拨号成功的用户

<H3C>dis sslvpn session verbose
User : zhangsan
Context : SSLVPN
Policy group : SSLVPNZIYUAN

Idle timeout : 30 min
Created at : 19:52:36 UTC Sun 04/19/2020
Lastest : 19:52:36 UTC Sun 04/19/2020
User IPv4 address : 10.88.26.145
Alloced IP : 10.10.10.2
Session ID : 14
Web browser/OS : Windows

客户端使用INode登录截图：

配置关键点

1 注意事项

1 注意事项

1、安装Active Directory后服务器所在域会变更导致重启后无法使用原账号登录，登录时需要使用“域名\用户名”的方式去登录。

2、因为设备默认查询用户属性是查询CN值，当LDAP服务器用户名与登录账号不一致情况下需要设备查询samaccountname值来确定用户登录名，因此在设备LDAP Server下“user-parameters user-name-attribute samaccountname”命令是一定要添加的。