SANGFOR

VDI

VM join AD Domain Configuration Guide

Version 5.4.0

Contents

Chapter 1 Function introduction

1.1 Application Scenario

This function is applicable to the Microsoft AD domain environment where the VM needs to join the customer intranet and controlled by the AD domain. At the same time, the configuration of the AD domain can be automatically completed in conjunction with the VDC, simplifying the deployment process of the desktop cloud and AD domain.

The following functions can be implemented:

1. VM joined to the domain. Including dedicated and restored desktop type.
2. VM join to the specified AD domain or OU. By default will join to computers OU, can configure the specified OU.
3. Domain users automatically login. Domain users can use VDI SSO to the VM.
4. Bind domain user login. Only the associated VDI account is allowed to login to the VM, other domain users are not allow to login.
5. Domain users automatically join the local administrator group or Power Users.
6. Domain users bind computer name login. Domain user configuration login to the specified computer name.
7. Domain username is not case sensitive.

1.2 Theory of implementation

1.2.1Restrict domain user login

1. VDC: Add plug in, enter the binding domain information and deliver the configuration.
2. Vdagent: Receive the configuration, read the relevant binding information and write the binding information to the registry.
3. Vdsso: Complete the input of the username and password, trigger the login operation and determine whether the current user is meets the login conditions or not. (Windows 7/10 and Windows XP are two completely different methods of operation)

1.2.2 Join the specified OU or join the local management group

1. VDC: Add the configuration interface and deliver the configuration.
2. Vdagent: Receive message from VDC and write to shared memory.
3. Vdnetdom: Read shared memory message and perform auto login operation.

1.2.3 Add domain and domain auto login

1. VDC: Add a configuration interface and send domain or auto login operation.
2. Vdagent: Receive message from VDC and write to shared memory.
3. Vdsso: Read shared memory messages for auto login.

1.2.4 Virtual machine configuration

1. Bind domain and domain user storage location, registry path:

   KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SfSysPrep\CP UID

   Related fields: binddomain(bind domain name), username(bound user),

isbindvmuser(whether bind users or not)

2. The xml configuration file send to the virtual machine, can be opened directly:

   C:\Users\ad_uu\AppData\Local\SangforVDI\ShellMsg_01_s1_5963248b.dat

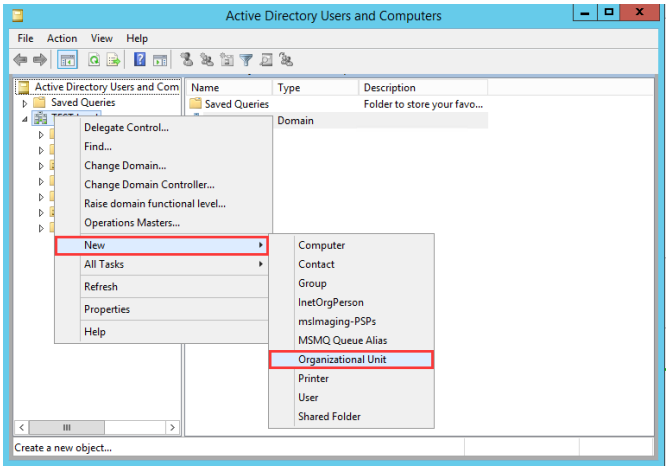
Chapter 2 Configuration process and precautions.

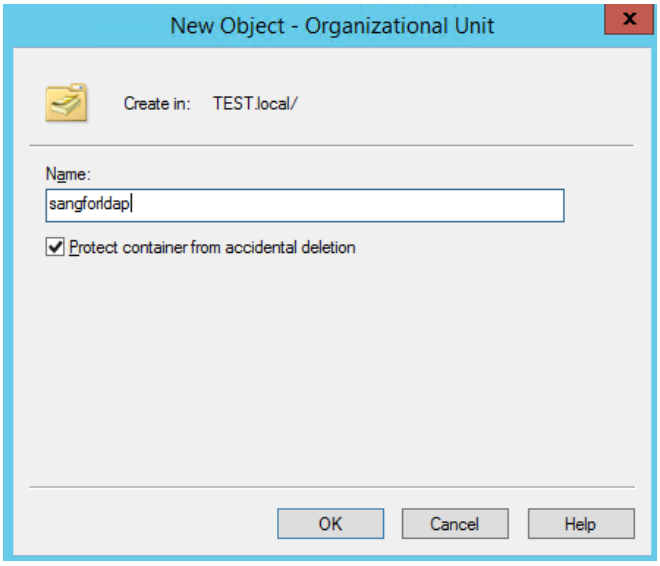
Precautions:

1. For VM joined the domain function, the template is not required to be added to the domain.
2. Don't modify the SID of created VM.

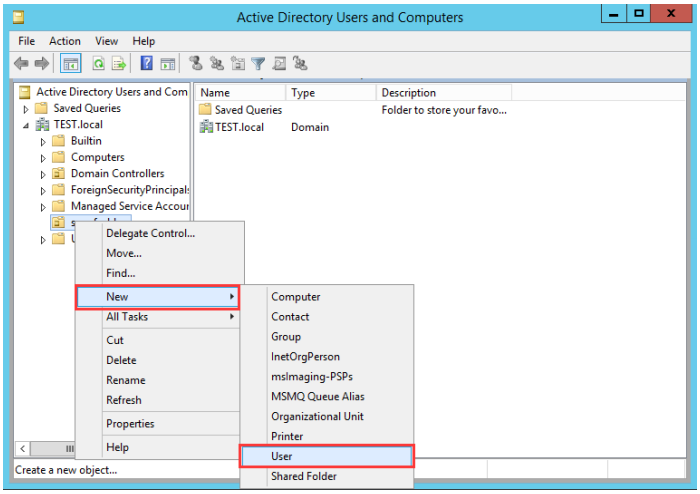
2.1 AD user creation

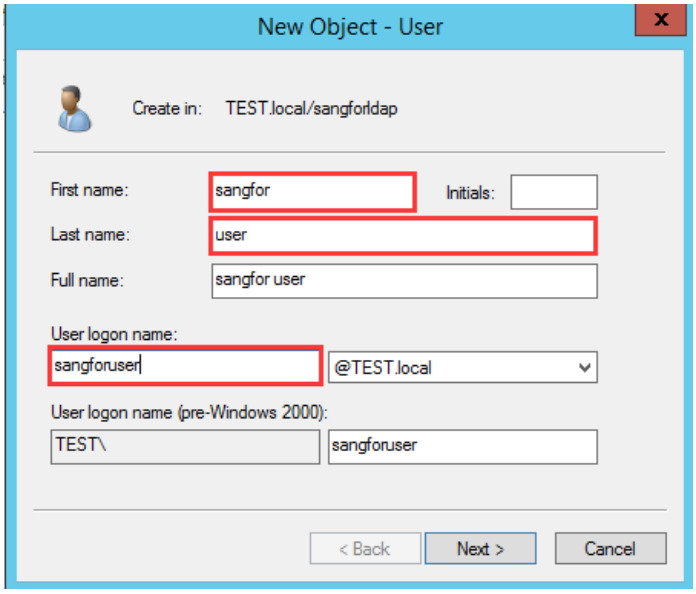
1. Go to **Active Directory Users and Computers**, create a new **Organization Unit** under the domain as figure below:

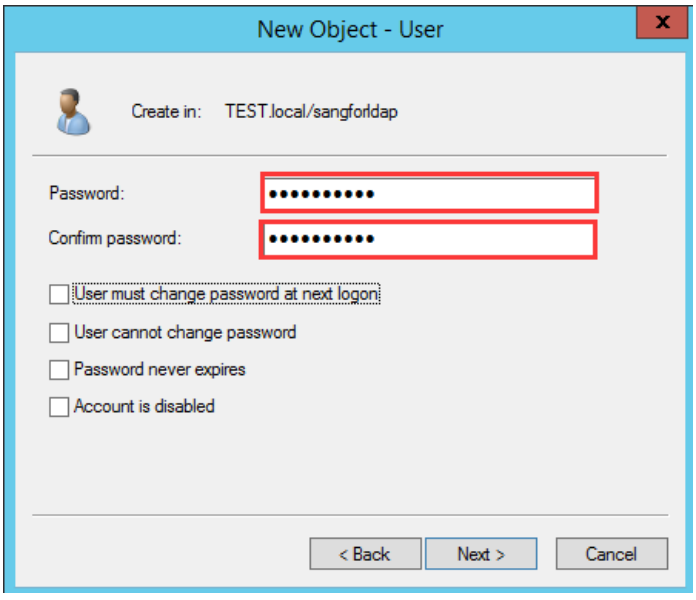




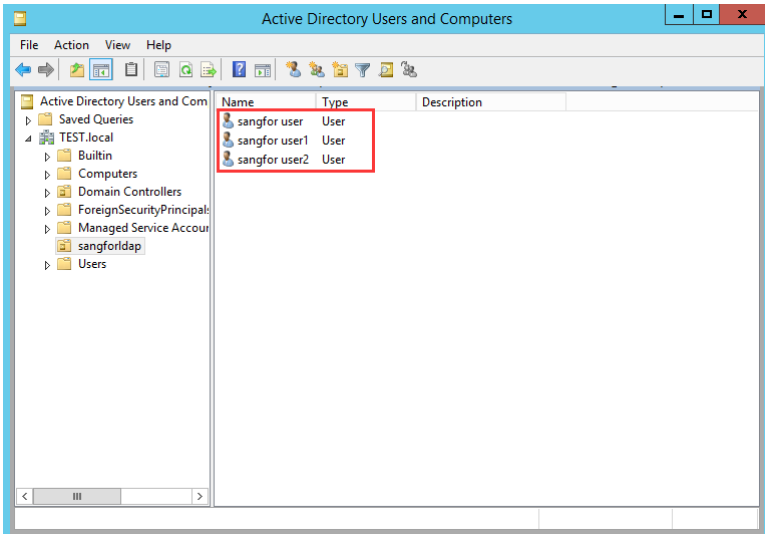
2. Create users under the organization unit created just now as figure below:


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
TEST.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Name Type Description
Saved Queries Folder to store your favo...
TEST.local Domain
Delegate Control...
Move...
Find...
New
All Tasks
Cut
Delete
Rename
Refresh
Properties
Help
Computer
Contact
Group
InetOrgPerson
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder
Create a new object...


New Object - User
Create in: TEST.local/sangforldap
First name: sangfor
Initials:
Last name: user
Full name: sangfor user
User logon name:
sangforuser
@TEST.local
User logon name (pre-Windows 2000):
TEST\
sangforuser
< Back
Next >
Cancel

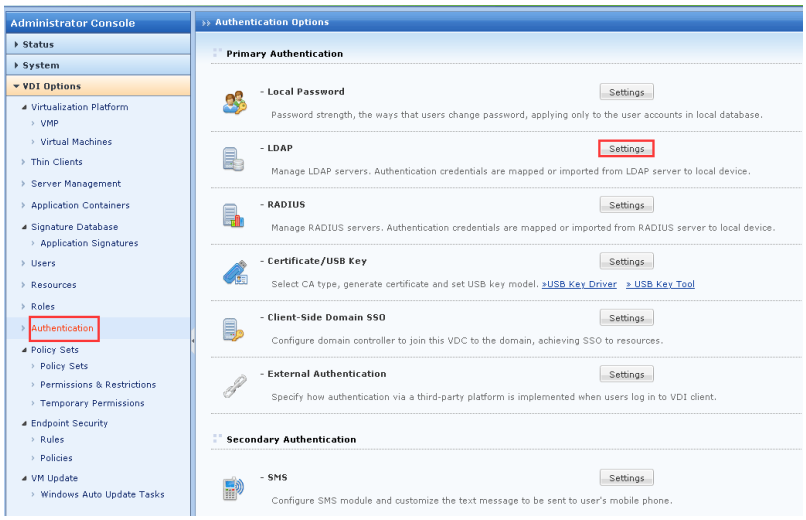

New Object - User
Create in: TEST.local/sangforldap
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel

3. Use the following method to create users.

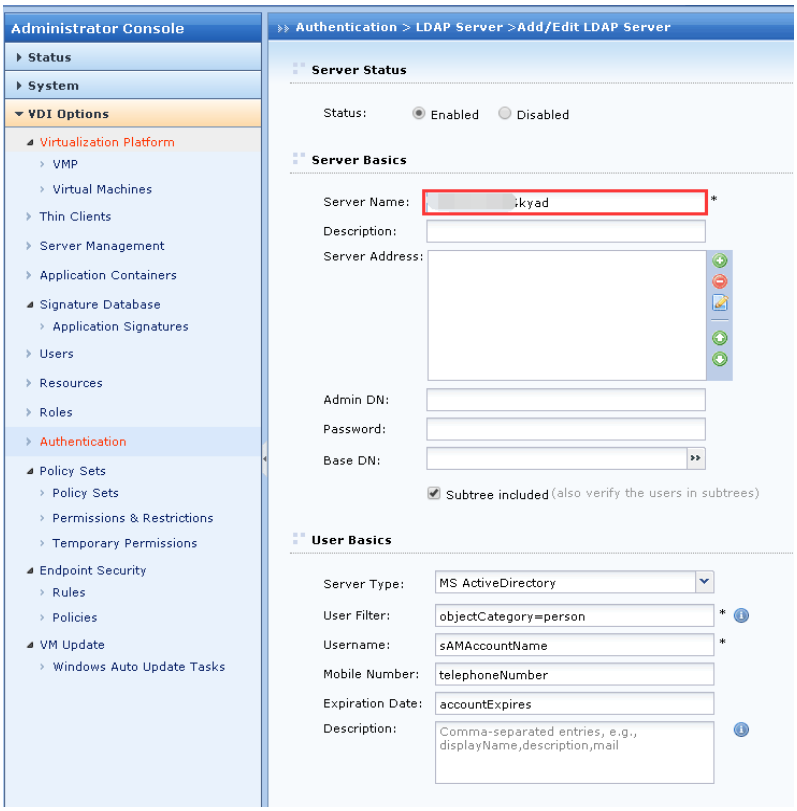


2.2 Configure LDAP authentication on VDC

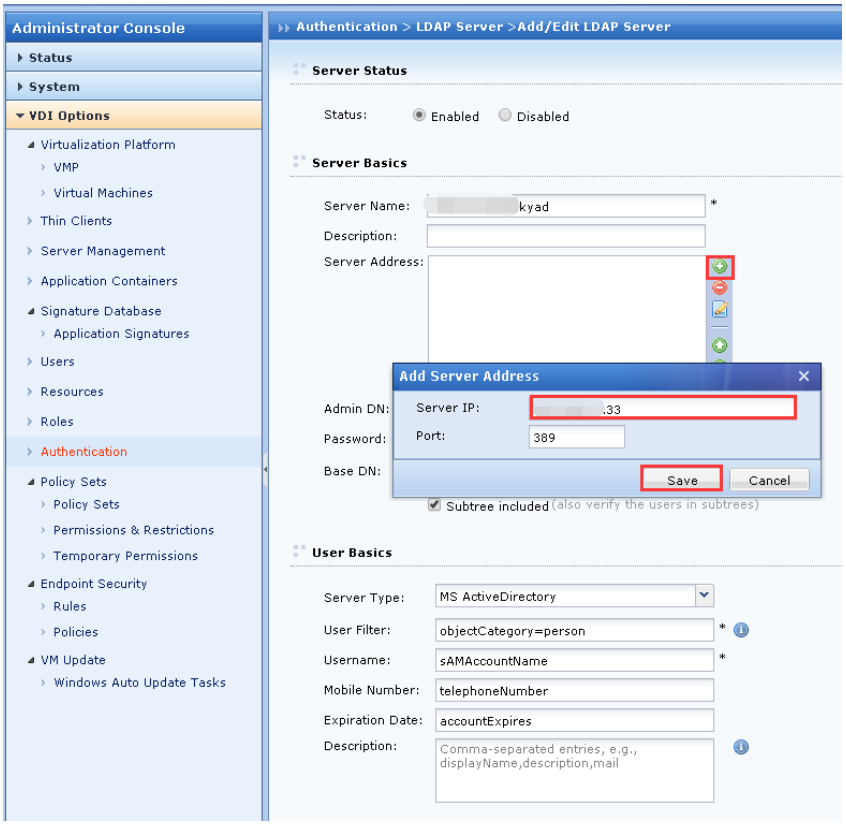
1. Go to **VDI Options** > **Authentication**, Click the **Settings** button beside the **LDAP** options as figure below:



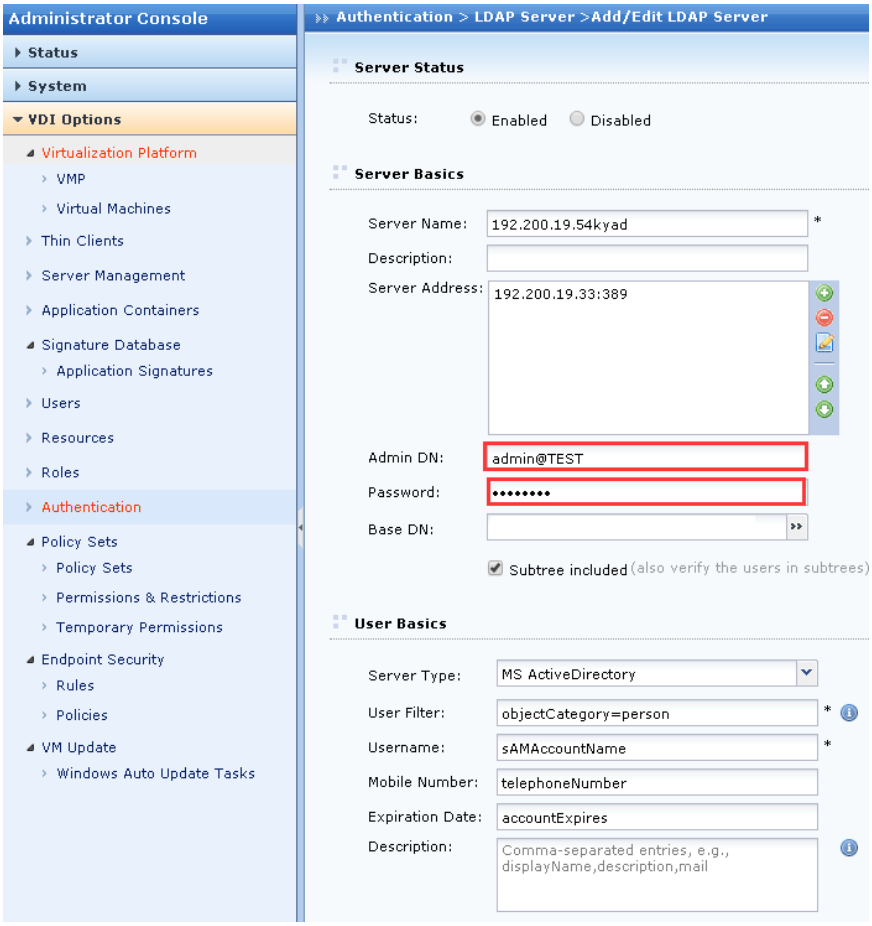
2. Click **New** button, then enter the server name:



3. Click the green button beside the box of **Server Address** to add the Server IP (default port is 389) as figure below:

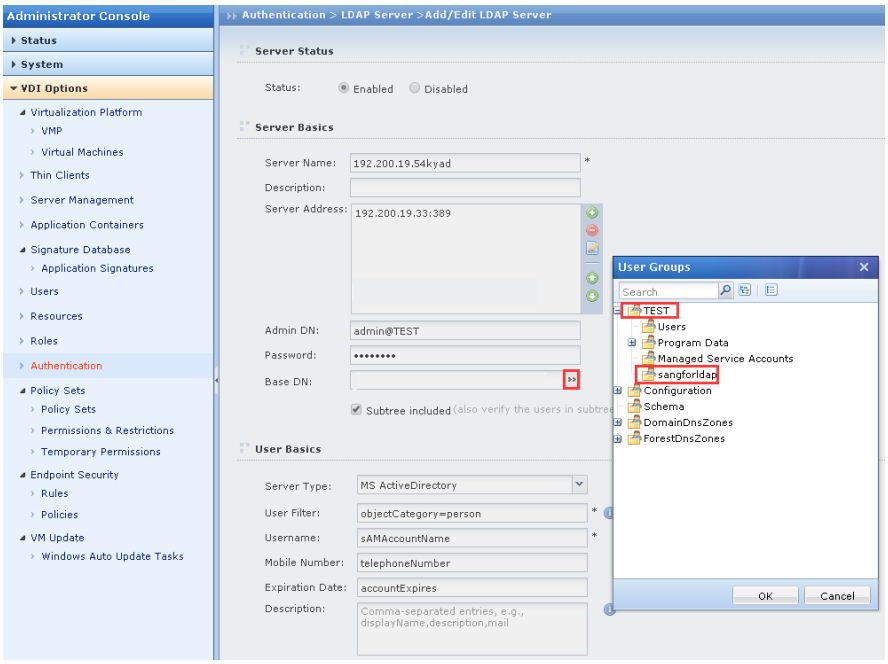


4. Enter the Admin DN and Password as figure below:

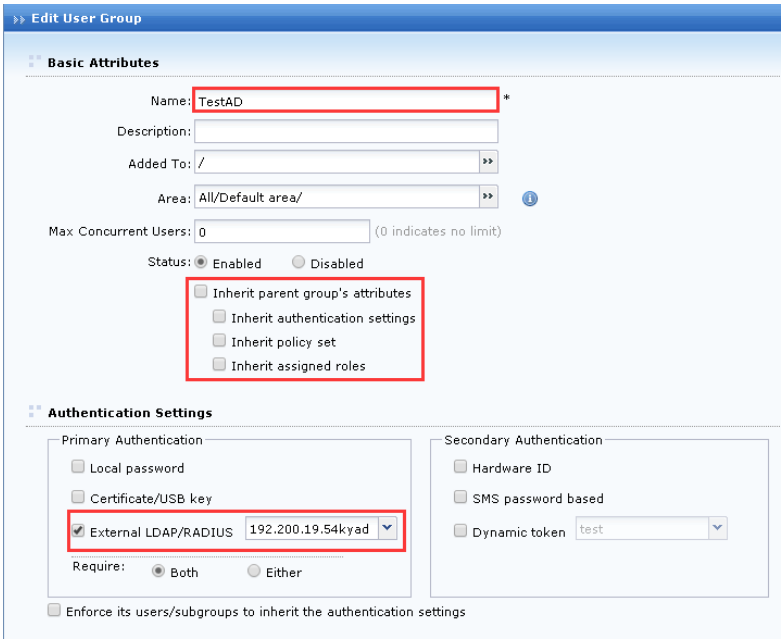


Note: For example the server administrator account is **admin** and the domain name is **TEST** then for the Admin DN path is **admin@TEST**.

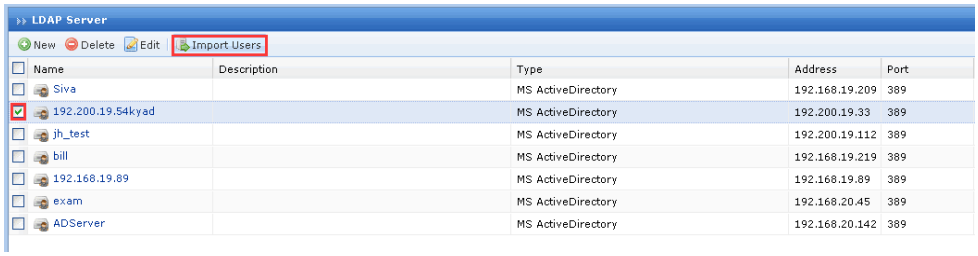
5. Click on the button beside the box of Base DN, then select the organization structure of the user on the domain and click **Save** button to complete the configuration as figure below:



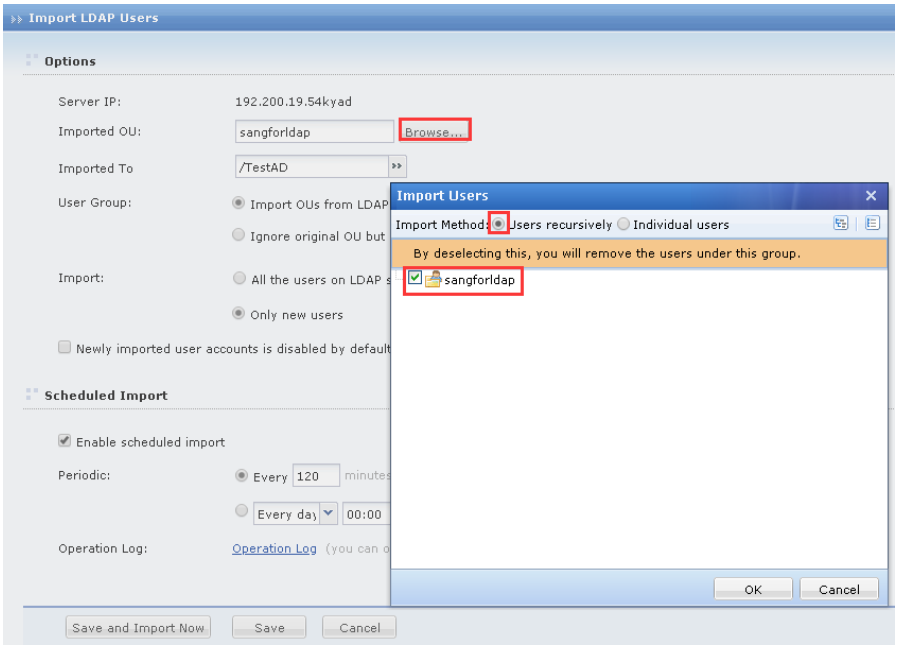
6. Go to **VDI options** > **Users** > **New** > **Group**, enter name of the group. Uncheck the **Inherit parent group's attributes.** On **Authentication Setting**, choose **External LDAP/RADIUS**, and choose the authentication method that created just now as figure below:



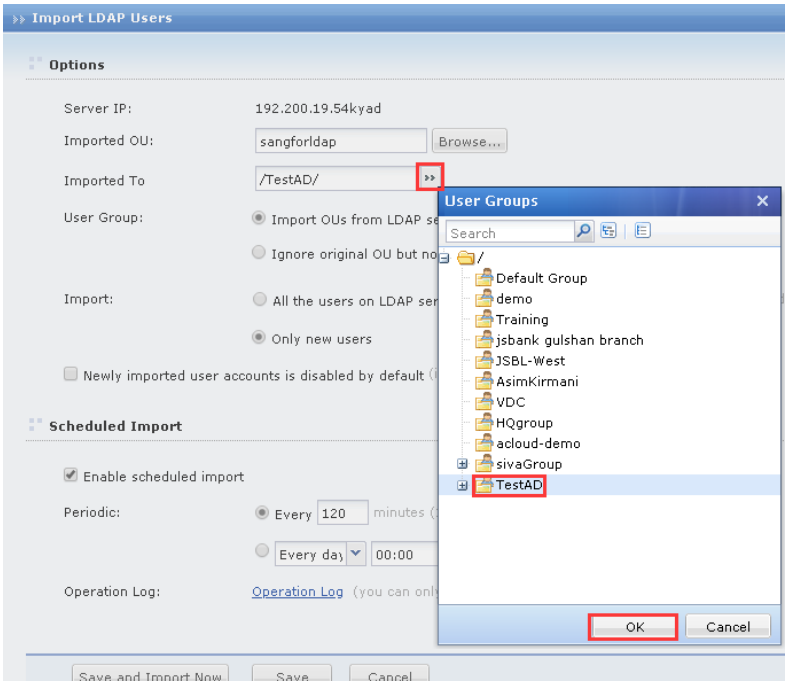
7. Go to **VDI Options** > **Authentication**, choose the authentication method created just now and click on the **Import Users** button as figure below:



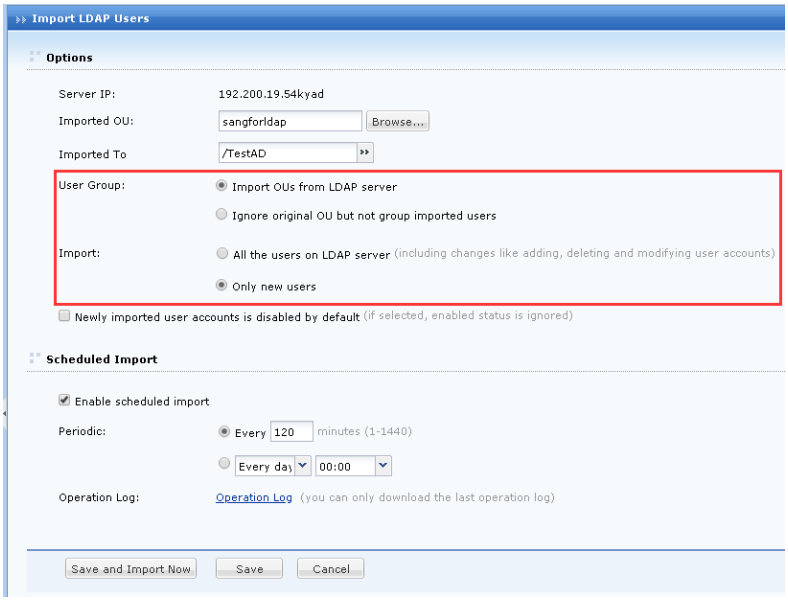
8. Click on the **Browse** button beside the box of **Imported OU**, then choose the **Users recursively** and the OU that created just now.



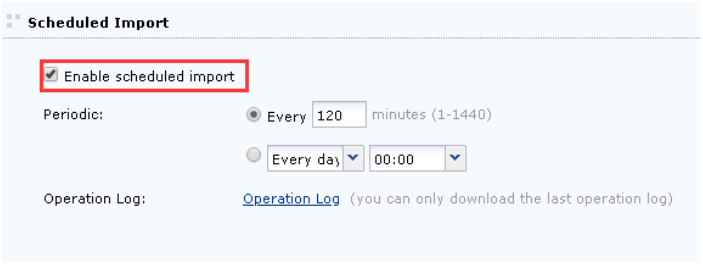
9. Click the button beside the box of **Imported To** to choose the user group that create just now.



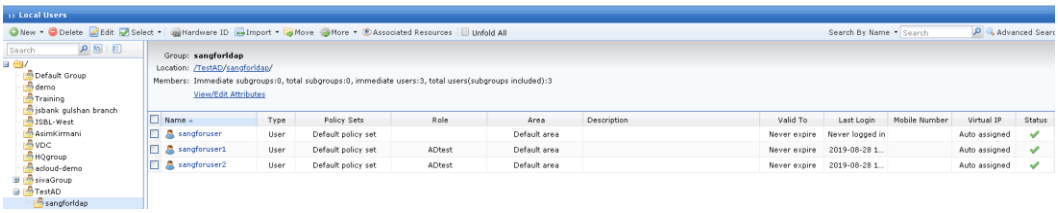
10. For the **User Group** and **Import** you can change depends on the requirement.



11. If schedule import is required, click on the **Enable schedule import** check box. The parameter can change according to the requirement.

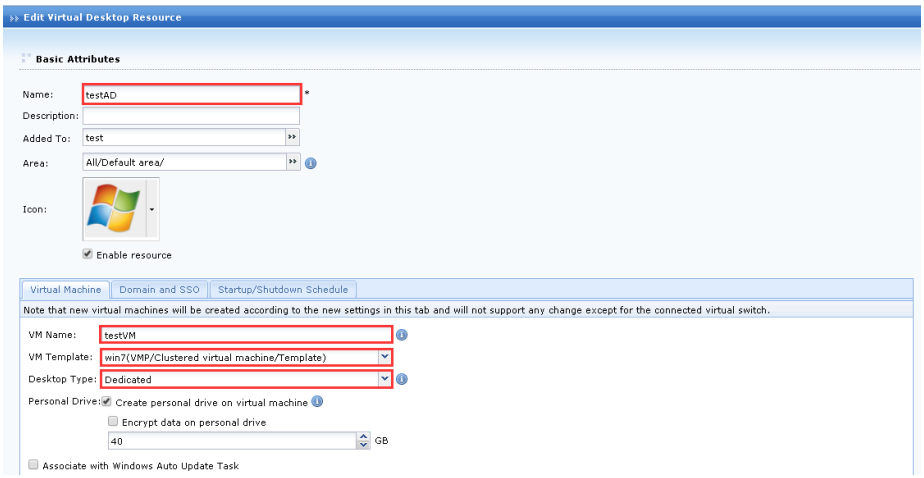


12. Click on the **Save and Import Now** button, users on domain will synchronize to user group. Go to **VDI Options** > **Users**, choose the user group and check whether domain users has been synchronized or not.



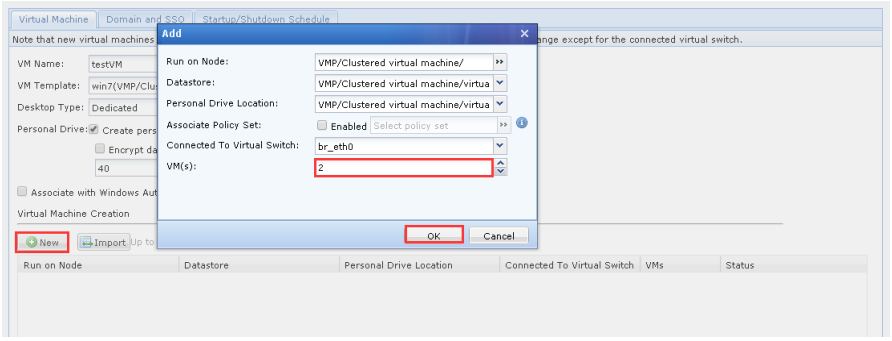
2.3 Create resource and join the VM to the domain

1. Go to **VDI Options** > **Resources** > **New** > **Virtual Desktop**, enter the name of the resource, VM name, VM template and Desktop Type as figure below:

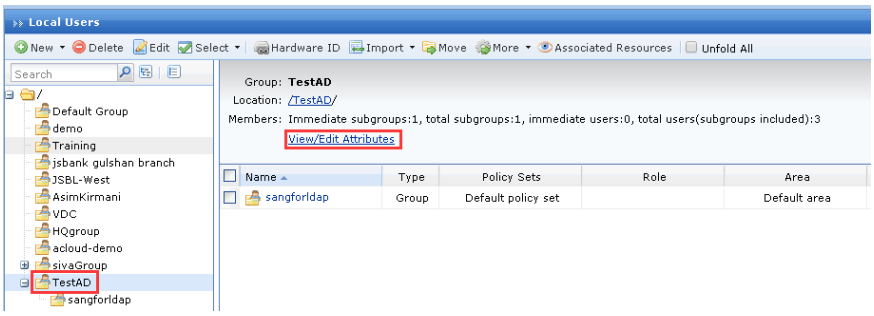


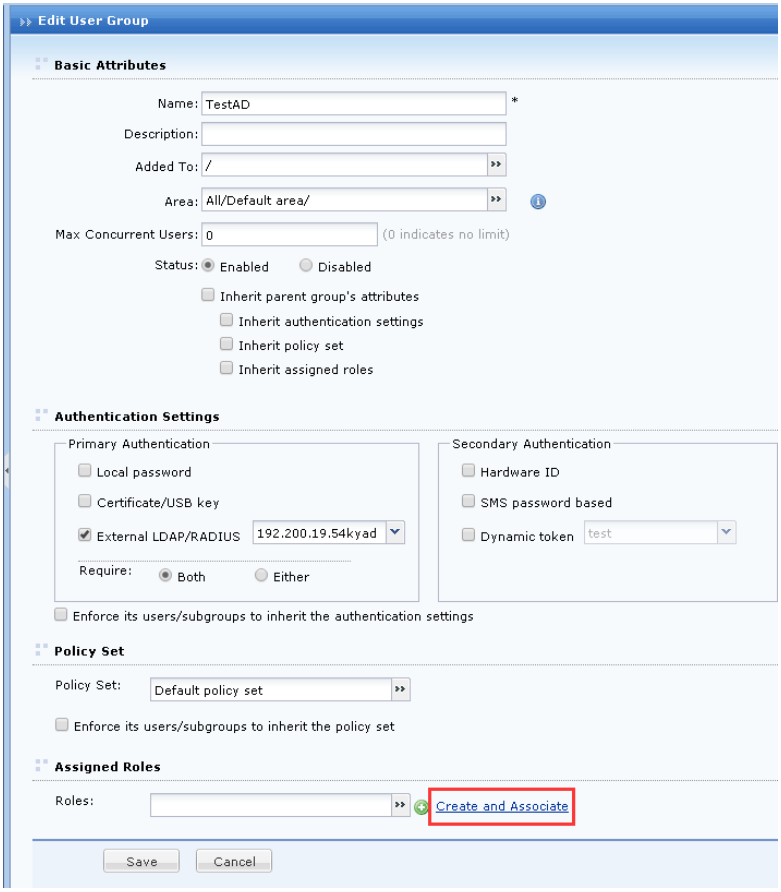
Note: Templates used by domain users only support Windows system template.

2. Under **Virtual Machine**, click the **Add** button and add corresponding VMs as figure below:

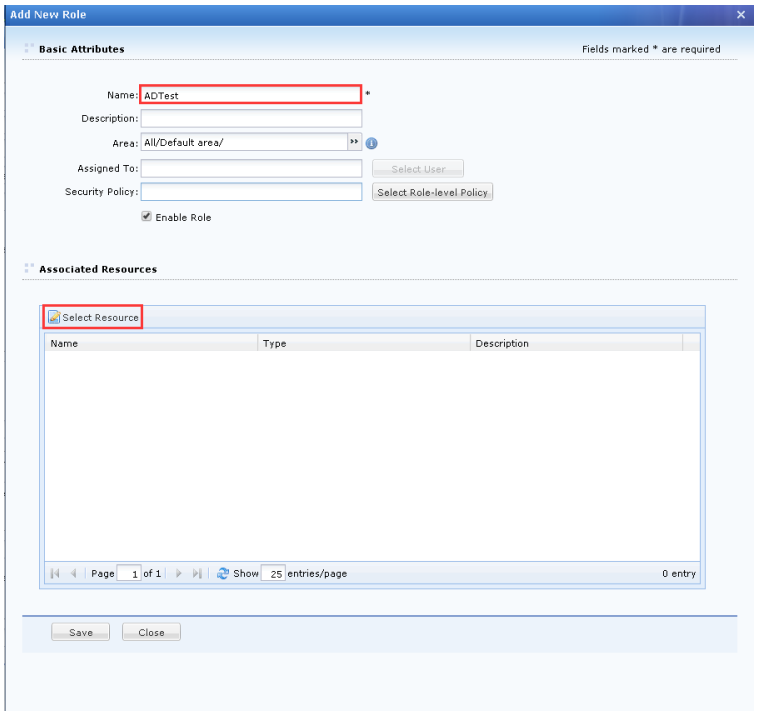


3. When VMs are created, go to **VDI Options** > **Users**, choose the group and click on **View/Edit Attributes**. After that on **Assigned Roles**, click on **Create and Associate** to create a new role.

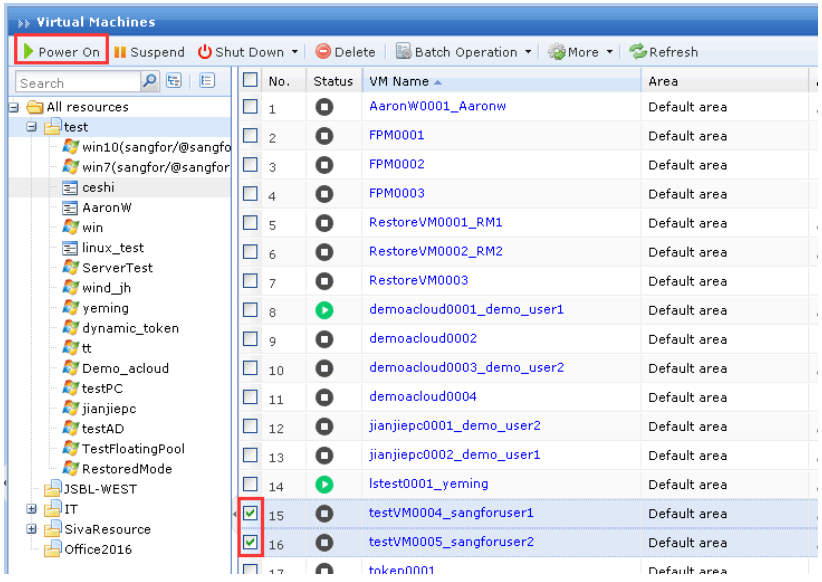




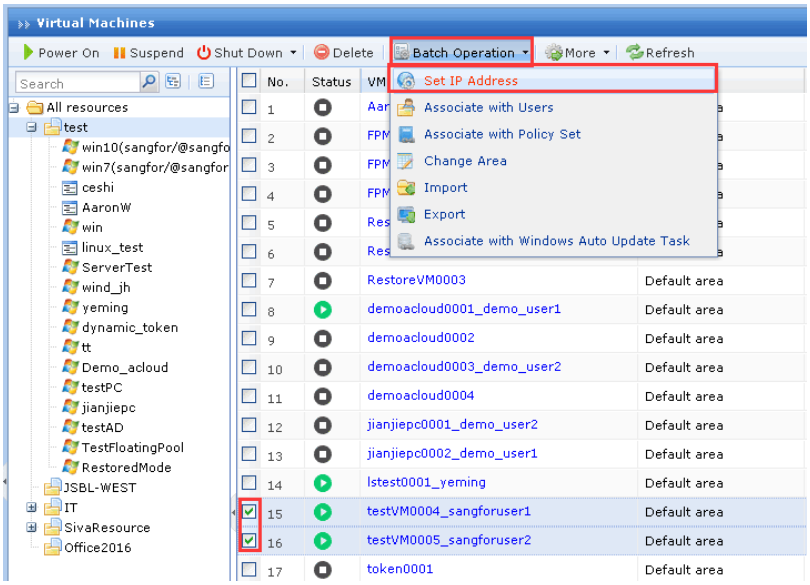
4. Enter the information, then click on the **Select Resource** button to choose the resource that created just now. Press **Save** button to save and create the role. After role has been created and selected, click the **Save** button to save the group attributes.



5. Go to **VDI Options** > **Virtualization Platform** > **Virtual Machines**, choose these VMs created just now then click on the **Power On** button to power on VM.



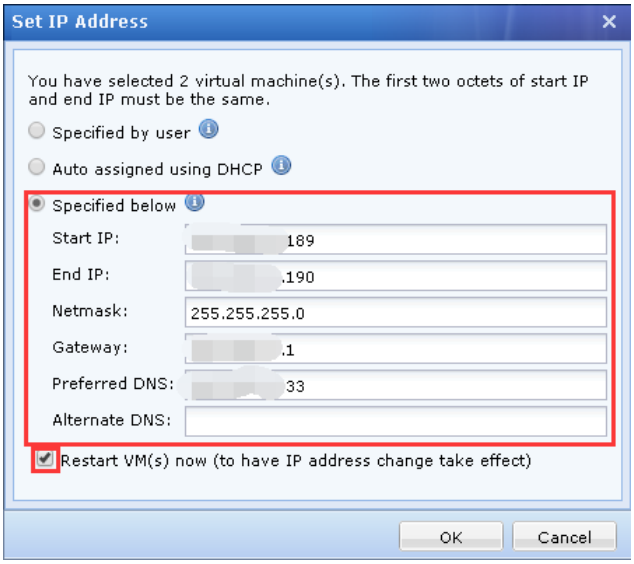
6. After these VMs power onand the status become green color, then select these VMs again and click on the **Batch Operation** > **Set IP Address**.



Note: The Status become green means the agent status is normal.

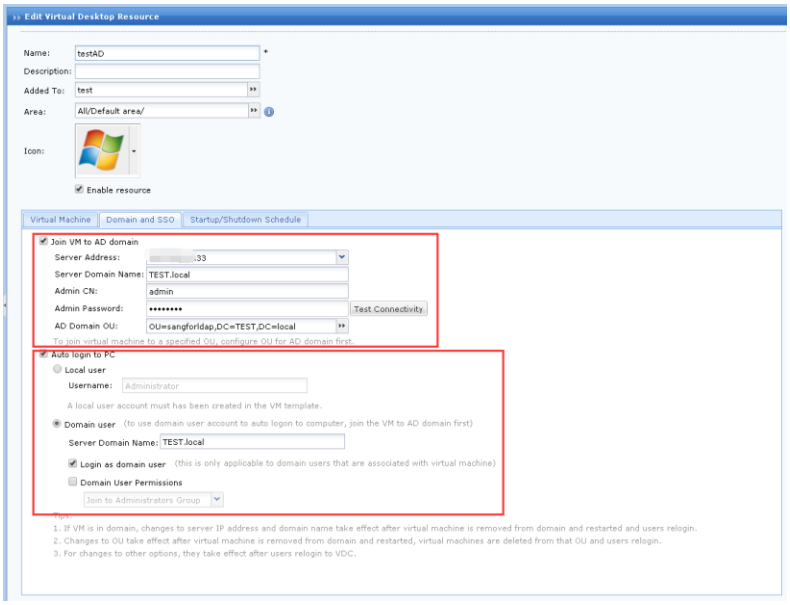
7. Assign IP for VM, you can specify IP/specified DHCP on the VDC or manually configure static IP for VM.

   In this scenario, batch operation method is used to assign IP for VMs. After IP address has is specified, the VM needs to be restarted so the **Restart VM(s) now** check box must be checked.



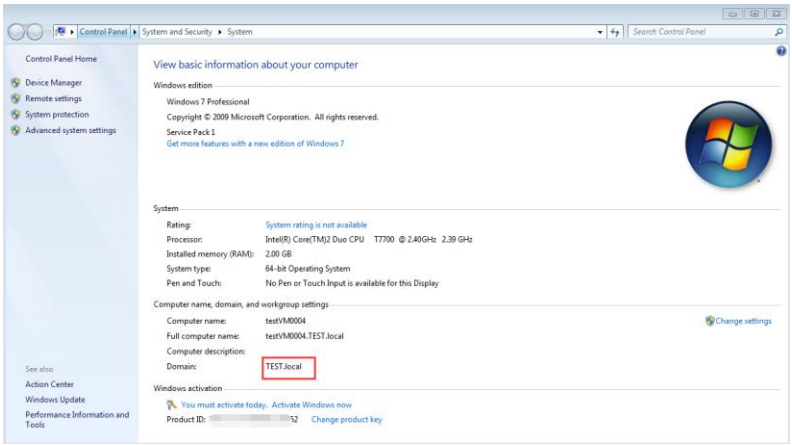
Note: In order to join VM to domain, required the VM IP able to ping domain server's domain name (VM must be able to resolve the domain name), domain server also can ping to the VM.

8. Modify the corresponding resources, go to **VDI Options** > **Resources** and click on the resources. On **Domain and SSO**, click on **Join VM to AD domain** and fill in the server details. Lastly click on the **Auto login to PC**, then choose **Domain User** and fill in server domain name and check on the **Login as domain user**. Lastly you can click on the **Test Connection** button to test the connectivity.

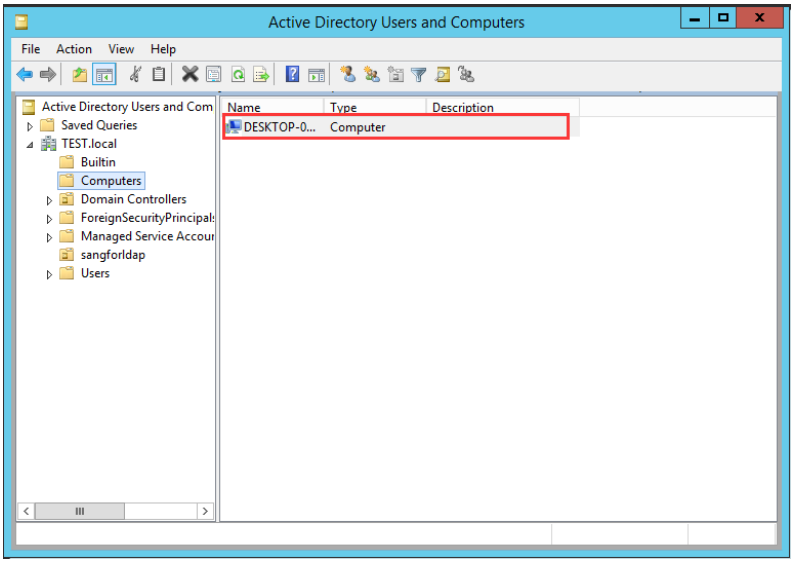


Note: The Admin CN is administrator account of the domain server, doesn't need to add a domain name. Example, if the server administrator account is admin and the domain name is TEST.local, then Admin CN is admin.

9. Open VDI Client, enter the domain username and password to login. After login, you will able to see the resource and click on the resource then will able to login to the VM.
10. After login to the VM, you can check whether the VM is joined to the VM or not.



11. Go to domain server, under **Computer** group check whether the VM has been added to the computer list or not. Aif yes, means that the VM has successfully joined the domain.



Note: For VDI version before 5.2, when first time access to resource it will first apply to join the domain and then automatically perform a restart then only will join to the domain. Version after 5.2, the domain will be added when the resource is accessed for the first time, doesn't required restart.

2.4 Introduction and configuration of AD domain optimization

Precautions:

1. Only support VM that running Windows operating system are automatically joined to the domain.
2. Template does not required to join a domain, but the created VM need able to ping to the domain server's domain name and domain server also need able to ping to the VM.

2.4.1 VM join the specified AD domain OU

Configure VM to join to specified OU and set the permission of different OU on the domain controller to facilitate rights managements. By default it will join the Computers OU.

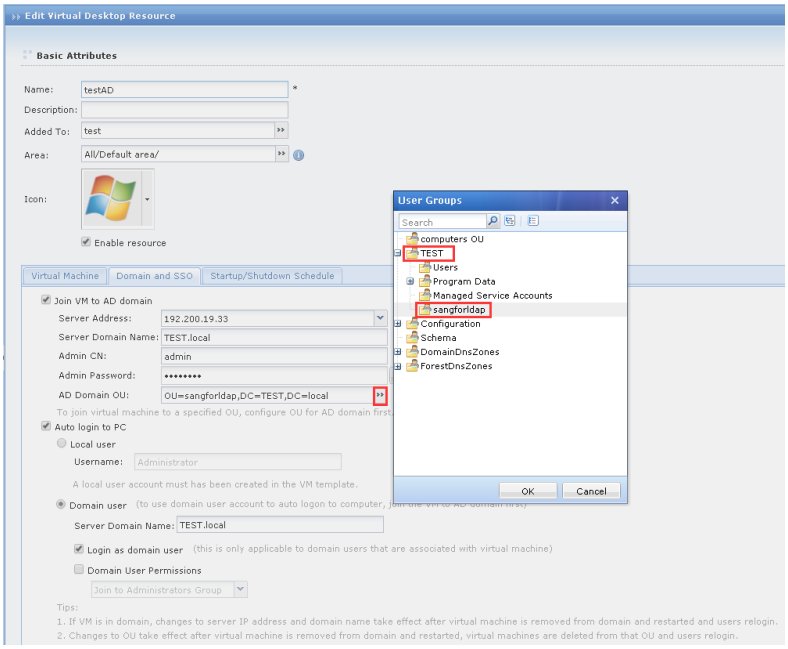
Version support: VDI 5.3.0 and above.

Configure Condition:

After the VM has been added to the domain, change the AD domain OU. After the AD domain OU changed, need to manually exit the domain then restart the VM and delete the original VM. Lastly logout and re-login again.

Configuration Method:

On VDC, go to VDI Options > Resources then select the resource and go to Domain and SSO. Click the button beside the box of AD Domain OU, it will have the corresponding domain information for administrator to select and click Save button to save.



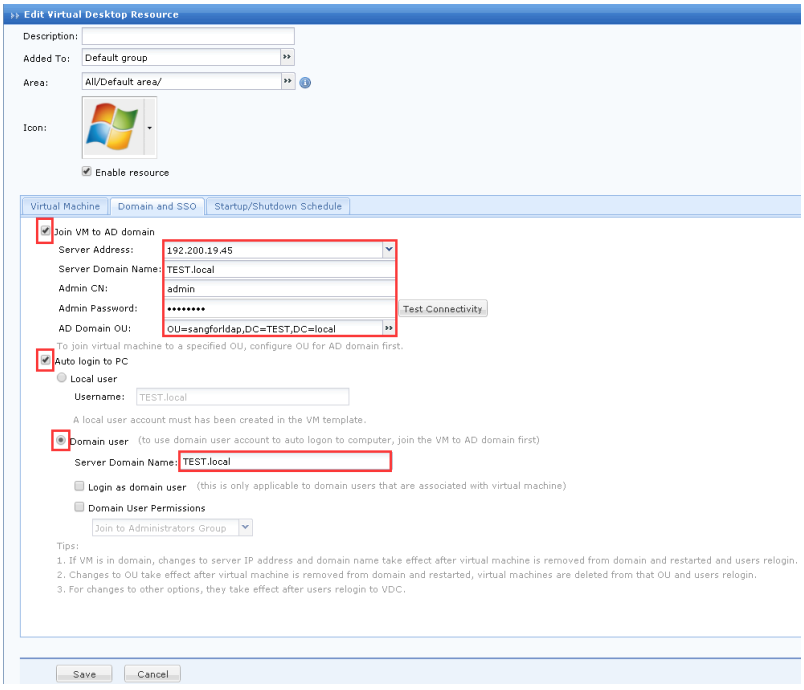
2.4.2 Domain user auto login

Version support: All version.

Configuration condition: Log out the VDI user and re-login.

Configration method:

In VDC, go to **VDI Options** > **Resources**, then choose the resource. After clicking on the resource, go to **Domain and SSO** then click on the **Join VM to AD domain** and fill in the server information. You can check the connectivity by blicking on the **Test Connectivity** button. After that click on the **Auto login to PC**, choose **Domain User** then fill in the server domain name click on the **Login ad domain user**. Lastly click on the save button.



2.4.3 Bind domain user login

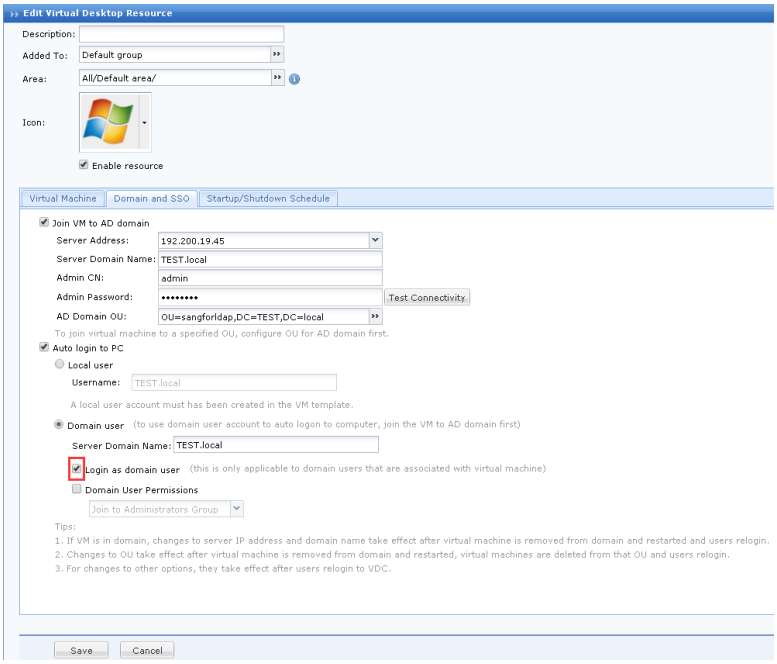
After configured bind domain user login, only the associated VDI account is allowed to login to the VM. Other domain users are phohibited from login to the VM.

Support version: VDI 5.3.0 and above.

Configuration conditions: Logout the VDI user, take effect after re-login.

Configuration method:

On VDI, go to **VDI Options** > **Resources**, select the resource and go to **Domain and SSO** click on the **Login as domain user**. Before select **Login as domain user**, the administrator must first join the VM to the domain and configure auto login to PC.



2.4.4 Domain user auto join local administrators group or Power Users.

By default domain users only have normal user right, when it is necessary to give users permission for user to install software then it can be done by configuring domain user to join local administrators group or Power Users group to give users more different permissions.

When this options is configured, domain users will automatically join to the VM local administrators group or the Power Users group, giving domain user a local administrators group or Power Users group privileges.

After un-check the options domain users are automatically removed from the corresponding group, restore normal user permission, no longer have local administrators or Power Users permission.

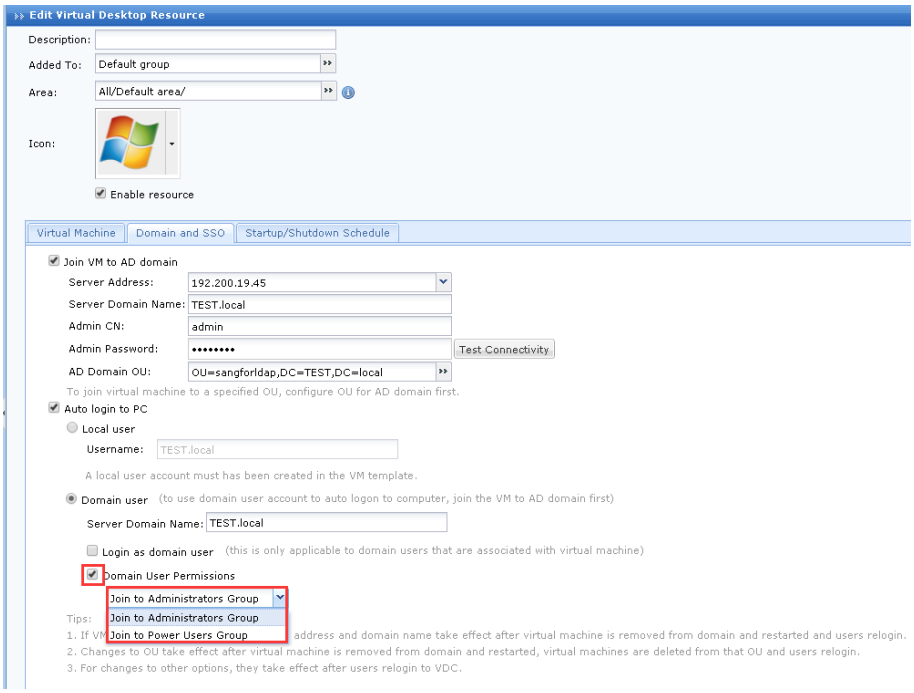
Support version: VDI 5.3.0 and above.

Configuration condiftion: Logout the VDI user, take effect afterre-login.

Configuration method:

In VDC, go to **VDI Options** > **Resources,** then choose the resources and go to **Domain**

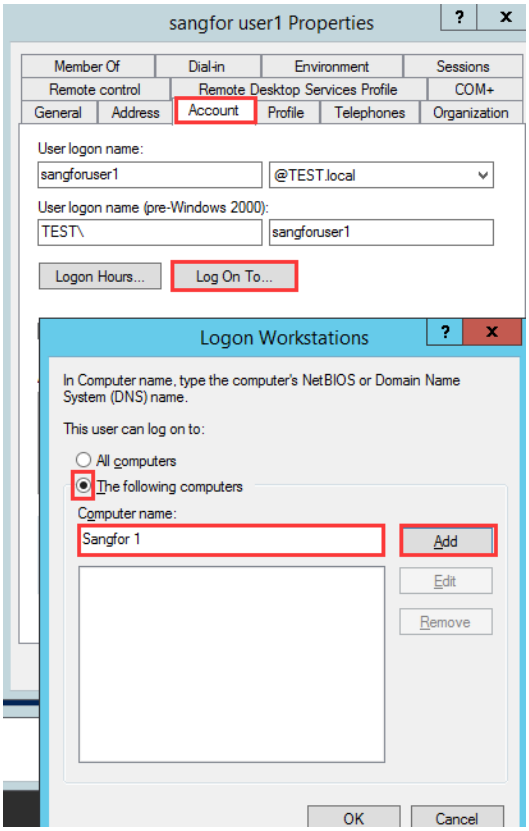
and SSO. Inside the **Auto login to PC**, it have a **Domain User Permissions** option. Click on the option, then choose **Join to Administrators Group** or **Join to Power Group**. The administrator must first join the VM to the domain and configure auto login to PC.



2.4.5 Other features

Support version: VDI 5.2 and above

1. Support domain user binding computer name login, which is domain user login to the specified computer name.



2. Support domain users are not case sensitive.

   When a domain user accesses a resources, iti s automatically converted to a lower-level associated virtual machine. This change takes effect only under the domain user and does not affect the local user. After the domain user is imported, the user name is changed to lowercase. The local domain user is still logged in, that is, the password is saved in the domain server.

Note: The VDC has been configured with LDAP domain authentication, if the VDC device has an uppercase domain user of the associated VM, then it will fails. (Version after 5.2 takes effect)

Chapter 3 Process log description

Process of joining domain:

1. Start resource, Windows update agent, restart once update complete.
2. Startup complete then join domain, after joined domain then restart.

   A. Join domain configuration and send log:

   C:\Windows\Temp\vdagent.log

   [INFO] [VDAgent::HandleLogon] recv windows logon info, addlocal flag:33554432 domain:adserver53.com,binddomain flag:16777216 domain:adserver53.com user:ad_1

   B. Join domain result log:

   C:\Program Files\Sangfor\SSL\VDI\Logs\VDNetdom.log

[VDNetdom] 0.JoinDomain of adserver53.com is succ. [INFO] [VDNetdom] Joins in domain(adserver53.com) successful , we need to reboot system.

C. **Bind user log:**

C:\Windows\Temp\vdagent.log

[INFO][SetBindDomain]Bind domain, loginmod:2 flag:1 domain:adserver53.com user:ad_1

Note: 1= Binding, 0= Not binding

D. **Join the management group log:**

C:\Windows\Temp\vdagent.log

[INFO] [AddLocalGroup] Add local group, loginmod:2 flag:2 domain:adserver53.com user:ad_1

[INFO] [AddLocalGroup] LastUser: CurrentUser: AddFlag:2

Note: 0 = Not joining, 2 = local management group, 4 = Power Users group

[INFO] [DelUserFromGrp] Delete User from Grp ret 2226

Note: Clear old user group relation first.

[INFO] [AddUserToGrp] Add User to Grp fail, ret 2226

Note: Join a new user group relationship.

3. Startup complete, automatic login.

Automatioc login log:

C:\Windows\System32\LogonUI.log (xp: c:\windows\system32\winlogon.log)

3.1 First check whether there is a trust relationship:

[PID:00760 TID:01116] [DBG] [VDSSO] IsMyComputerOnDomainTrust pszDomain:ADSERVE

3.2 Trust relationship exist:

[PID:00760 TID:01116] [INFO] [VDSSO] [TC_QUERY]netlog2_flags:48, rusted_dc_name:\\vdit.adserver53.com, status:0

[PID:00760 TID:01116] [INFO] [VDSSO] [TC_VERIFY]netlog2_flags:176, rusted_dc_name:\\vdit.adserver53.com, status:0

3.3 Enable startup login:

[PID:00760 TID:01116] [INFO] [VDSSO] Computer has join domain,will Autologin system

Chapter 4 Commom problem

4.1 VM joins domain / join OU failed

1. Check the Join VM to AD domain configuration on VDC

   Check VDC for Domain and SSO configuration, check Server Address, Domain Name Admin CN, password and etc.

2. Check whether VM can reach to domain or not, DNS must able to resolve the domain name

Need to make sure the derived VM is able to ping the domain name of the domain server, the domain server also can ping to the derived VM IP. The VM DNS must be able to resolve the domain name of the domain server.

3. Try to manually join the VM to domain
4. Log analysis
    1. If the VDC configuration is correct, check whether the configuration is delivered correctly.

       If the local user is logged in to the VM, check the delivery log: C:\Windows\Temp\vdagent.log. If the configuration does not match the following format, no domain or user then the configuration is faulty.

       [VDAgent::HandleLogon] recv windows logon info, addlocal flag:33554432 domain:adserver53.com, binddomain flag:16777216 domain:adserver53.com user:ad_1

    2. If the configuration is delivered correctly, check whether the domain addition process is abnormal.

       Log in the VM as local user, view the configuration log and open it in the VM.

       %VDI%\Logs\VDNetdom.log, %VDI%\Logs\VDAgent.log

        1. The VM is successfully added to the domain and needs to be restarted to take effect.

           [VDNetdom] Joins in domain(micota) successful, we need to reboot system.

        2. The virtual machine has joined the domain and don't need to rejoin the domain.

           [Agent] The computer is already in domain

        3. VM failed to resolve the domain name, it might caused by the DHCP allocation IP failed or the specified IP does not take effect or the assigned IP cannot reach to the domain.

           ```
           [INFO]  [VDNetdom] CurrentLocalIP:127.0.0.1
           [ERROR] [VDNetdom] gethostbyname is fail.Err:11004
           <DBG>   [VDNetdom] 0.TryConnect of son.adserver53.com return:0
           ```

    3. Computer join domain failed

       In VM, open **%VDI%\Logs\VDNetdom.log** log and search for related solutions on the Internet through the error message.

    4. Check whether the VM has been added to the domain, or has joined the domain before, there is a residual computer name in the OU on the domain.
    5. If above is no problem but still failed to join domain, kindly contact R&D.

4.2 Virtual desktop joined domain but auto login to domain failed

1. Confirm that the virtual desktop has joined the AD domain.
2. Try to manually enter the AD domain username and password to log in.
3. Test using RDP to login.

4. Follow the prompts message to search on search engines.

4.3 Joining the locam management group failure

1. Check the configuration.
2. Check the log.
3. View the process of joining the management group. If the log does not meet the above conditions, the cause of the failure is known based on the contents of the print log field.

4.4 Binding function is failure

1. Check configuration.
2. Check the log: C:\Windows\Temp\vdagent.log

   [INFO] [SetBindDomain] Bind domain, loginmod:2 flag:1 domain:adserver53.com user:ad_1
3. Check the registry, if there is binding information

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SfSysPrep\ CPUI D

   Binddomain = adserver53.com, binding domain.

   Isbindvmuser = 1, whether binding or not. 1 = bindin g, 0 = not binding

   Username = ad_1, binding user.

4.5 Auto login failure

Note: The trust relationship between the workstation domain AD domain servers failed, please check if the AD domain server is online or try to restart the computer.

1. Check the configuration, make sure the username and password is correct.
2. Check the log: C:\Windows\System32\LogonUI.log

[DBG] [VDSSO] IsMyComputerOnDomainTrust pszDomain:ADSERVER53

[INFO] [VDSSO] [TC_QUERY]netlog2_flags:0, trusted_dc_name:, status:1311

[INFO] [VDSSO] Computer do not join domain,but will not login system.

[INFO] [VDSSO] CurrentLocalIP:199.201.134.241

If prompt trust relationship fails, there are two situations:

1. As the log says, the virtual machine is not joined to the domain.
2. The virtual machine has been added to the domain, but the domain server communication test fails. After startup, the background will try to connect to the domain server 10 times (1 time 1 second). If it fails, the following log will be printed.

   [DBG] [VDSSO] CSSOProvider::GetCredentialCount VdeskMode:1, iTryCount:10, wszUserName:adserver53.com\ad_2, SSOLogMode:2

   [DBG] [VDSSO] IsMyComputerOnDomainTrust pszDomain:ADSERVER53

   [INFO] [VDSSO] [TC_QUERY]netlog2_flags:0, trusted_dc_name:, status:1787

Note: Will print 10 logs like above.

[INFO] [VDSSO] Computer do not join domain,but will not login system.

[INFO] [VDSSO] CurrentLocalIP:199.201.134.241

This is a network problem, you can log in successfully after using the domain user login manually.

If the login is still unsuccessful, kindly contact technical support for assist.

SANGFOR