Sangfor VDI POC Guidance

For VDC5.1/VMP5.1 Firmware Version

Version 1.0

2017-4-28

Amendment History						
No	Content	Date	Version before amendment	Version after amendment	Reviser	Approver
1	Add all content	2017/2/28		1	Xia Chunyan	
Notice: The period of validity for the document ends on new test report release. If the version number is less than 1.0, the document is a draft and only for your reference						

Index

1. Test preparation

1.1 Test target

Here are the test target should be reached：

- Verify terminal's compatibility
- Verify user experience
- Verify access control of external device
- Verify management of user and terminal
- Verify management of desktops
- Verify stability
- Verify security
- Verify failure recovery

1.2 Test environment

1.2.1 Version

The test book is based on firmware **VDC5.1**. Tiny difference could be noticed with other release.

1.2.2 Hardware

If you do not intend to install VMP with Sangfor all-in-one server，the following lowest recommendation for your existing server should be met. Meanwhile，please adopt the hardware configuration as recommended for better user experience

	Lowest	**Recommended**
CPU	64 bit CPU，supporting Intel VT-x	E5-2660 V3 (10C/20T 2.6GHZ) or better

Memory	16GB or more(8GB for VDI platform)	128GB ECC DDR4 or more
Hard disk	60GB or more	System :128GB or more Caching :240GB Intel SSD or more Data :4*2TB SATA(7.2K RPM) or more
NIC	GE/10GE*1	GE/10GE*3 or more
USB	2	4 or more

If you intend to test virtual storage function，at least 1 enterprise-level SSD caching disk over 240GB and several enterprise-level HDD （speed over 7200RPM） over 1TB for each server are required. If adopting RAID card，the card supporting JBOD/Non-Raid is recommended. If not，each hard disk in RAID should be configured as an independent RAID-0 or forbid RAID

1.2.3 Recommended deployment of VM

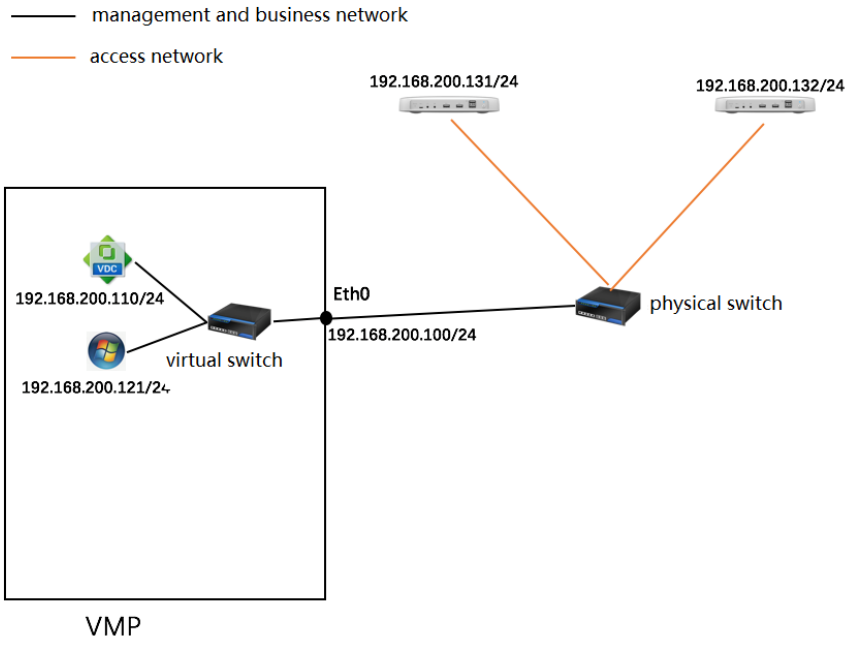
System	CPU	Memory	Disk	Remark
Win7	2 cores	2G or more	Self allocation	recommended（32 bit/64 bit）
Win10	4 cores	4G or more		
WinXP	1 cores	2G		Not recommended

1.2.4 Topology and IP allocation

〖Tips〗

The IP below is for your reference.

- **Test with one server（one VDS1350 as example）**

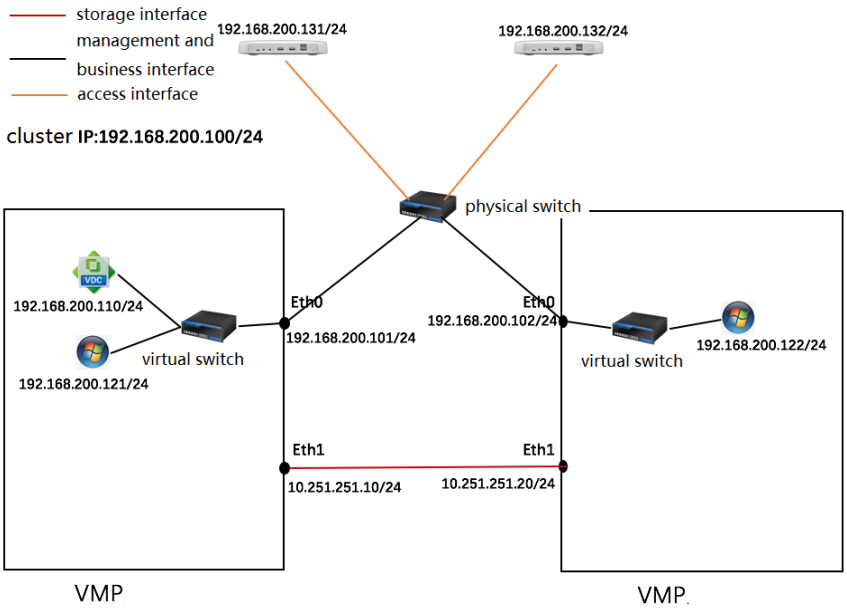


〖Tips〗

Eth0 is designed to be the management interface and data transmission for VDC in such design，which is suitable for one server

VMP	192.168.200.100/24
VDC	192.168.200.110/24
Virtual machine	192.168.200.121-125/24（5）
aDesk	192.168.200.131-135/24（2）

- **Test with cluster（ Applicable for several VDS1350 or third party servers with 2 WAN ports）**



〖Tips〗

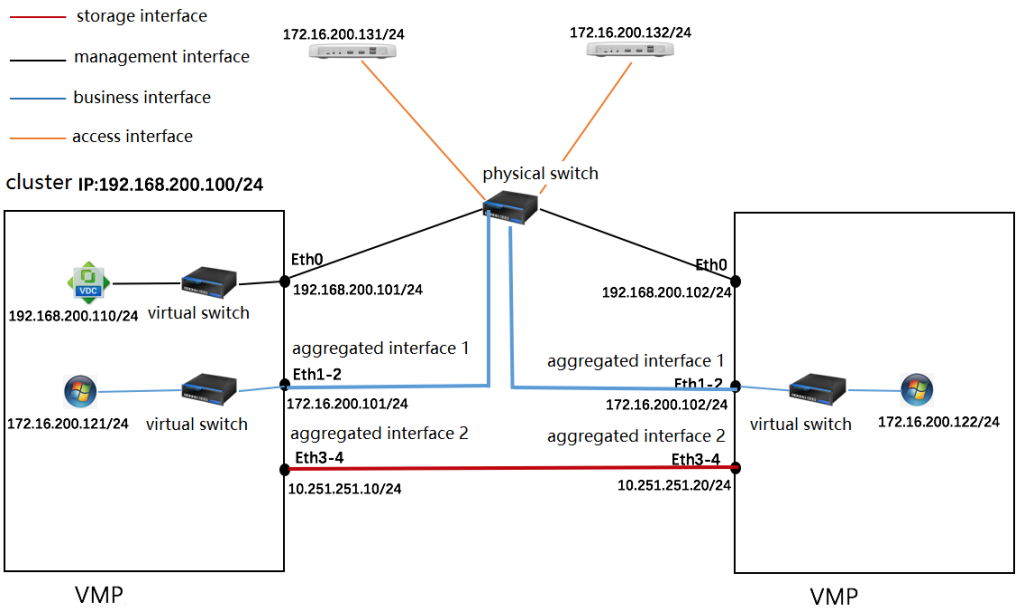
Eth0 is designed to be the management and data port for VDC in such design，Eth1 is storage communication port.

〖Tips〗

After the cluster has been built up，you may not take a server offline

VMP	Cluster IP	192.168.200.100/24	
	Server 1	Eth0：192.168.200.101/24	Eth1：10.251.251.10/24
	Server 2	Eth0：192.168.200.102/24	Eth1：10.251.251.20/24
VDC	192.168.200.110/24		
Virtual machine	192.168.200.121-125/24（5）		
aDesk	192.168.200.131-135/24（2）		

- **Test with cluster (recommended if the devices have enough WAN ports)**



Remark：Eth0 is designed to be the management port，aggregated interface 1（eth1 and eth2）is data tunnel for VDC，aggregated interface 2 （eth3 and eth4）is storage communication port

〖Tips〗

1. The management interface segment （192） should be connected to virtual machine segment （172），which means the communication between the segments is enabled

2. After the cluster has been built up，you may not take a server offline

VMP	Cluster IP	192.168.200.100/24		
	Server 1	Eth0：192.168.200.101/24	Aggregated interface1：172.16.200.101	Aggregated interface2：10.251.251.10/24
	Server 2	Eth0：192.168.200.102/24	Aggregated interface1：172.16.200.102	Aggregated interface2：10.251.251.20/24

VDC	192.168.200.110/24
Virtual machine	172.16.200.121-125/24（5）
aDesk	172.16.200.131-135/24（2）

1.2.5 Test materials

√ VMP&VDC up-to-date installation package

√ OS template（virtual machine VMA file） OS mirror（ISO file）

√ Application software

√ USB disk sizing of 4GB or more

√ Tools like Chrome、UltraISO、Xshell，etc

√ Authorization KEY and corresponding KEY ID （for new-installed VMP system 60 days probation period for 30 users are authorized）

2. Deployment and initiation

〖introduction〗

Please accomplish the deployment and initiation of VDI according to the following steps and expected time cost is 30-60 minutes

2.1 System initiation

〖process〗

The IP，username and password in the following example could be customized.

1. Connect the devices according to the topology above；
2. Login to VMP console with default IP（10.254.254.10）and default username

/password：admin,admin，modify the password to sangfor@123 and re-login；

3. Modify the IP of two servers to 192.168.200.101/24 and 192.168.200.102/24（non Sangfor server could be configured on installation）；
4. Synchronize system time. For new-installed VMP system 60 days free trial for 30 users are authorized and you don't need to insert KEY and input KEY ID（if probation period expires，you could activate with KEY and KEY ID，or you may reset to factory settings but all data will be lost）；
5. Login to server 1 and configure cluster IP to 192.168.200.100/24 and add server 2；
6. Initiate virtual storage： apply 2 copies mode and link aggregation with one switch（If you intend to test disk disaster recovery，you should keep a free disk）；
7. Configure detect IP（reachable gateway IP in physical network is recommended）；
8. After the cluster has been built up，please update to latest version and install all patches latest version. Third party server should install the latest version；
9. Create a VDC virtual machine in VMP and set the management address for VDC to 192.168.200.110/24；
10. Fill in VDC serial number（For new-installed VMP system 60 days probation period for 30 users are authorized and you need not to insert KEY and input KEY ID）;

〖Tips〗

If you cannot login to console on starting up，please access the server with a monitor to check whether it starts normally

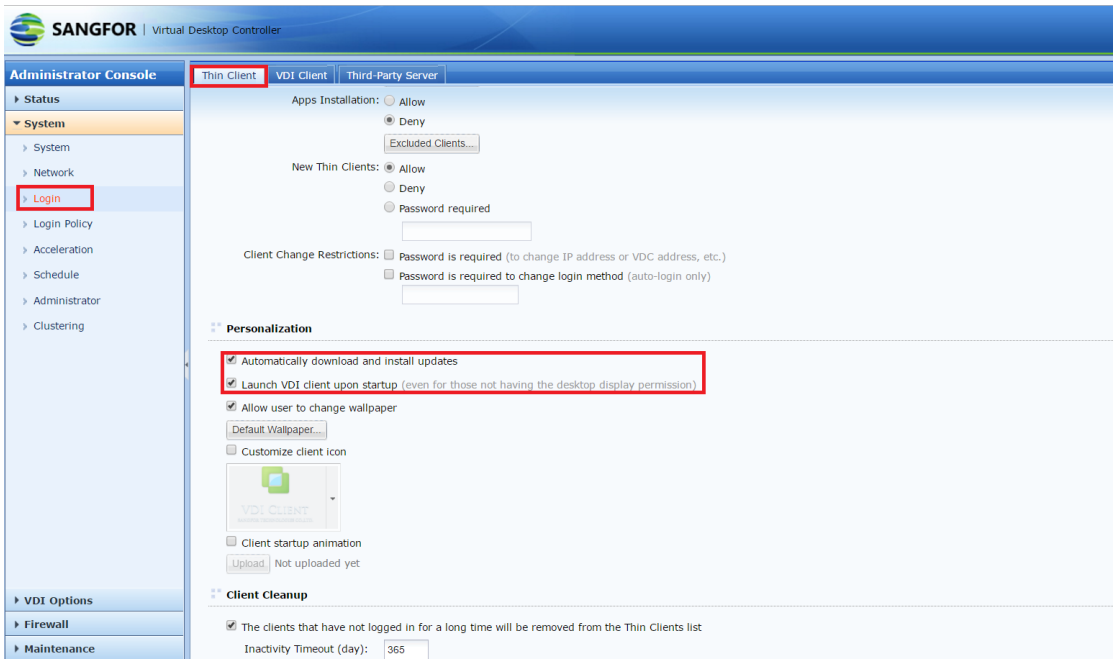
2.2 Create Virtual machine

1. Import virtual machine and name it "**Win7x64**" (use Win7 64 bit as example). Upload vma file and then create virtual machine (Importing process will remain in 98% for 5-20 minutes and please be patient)；
2. Template deployment. Install Agent and the software client requires，then render into template；
3. Create virtualization management platform（VMP）in VDC console and name it VMP. Fill in the VMP cluster IP (https://192.168.200.100:4433) in the demo above)，then enter username and password of VMP（admin/sangfor@123 in the demo above）and test the connection. If it succeeds，save the configuration；
4. Create virtual desktop. Name it "**Win7x64**" and select the virtual machine template. The 'Run on Node' is Clustered virtual machine. The 'datastore' and 'private disk' are on the virtual storage；
5. Associate user and role. Create user "**test1**" and "**test2**" sharing the password **123456**. Assign the authorization method to username/password. Create role named "**Win7x64**" and associate "**test1**" and "**test2**" with resource Win7x64；
6. Configure policy set. Create policy set named "**Win7x64**"，edit test1 and test2 to associate the policy set；

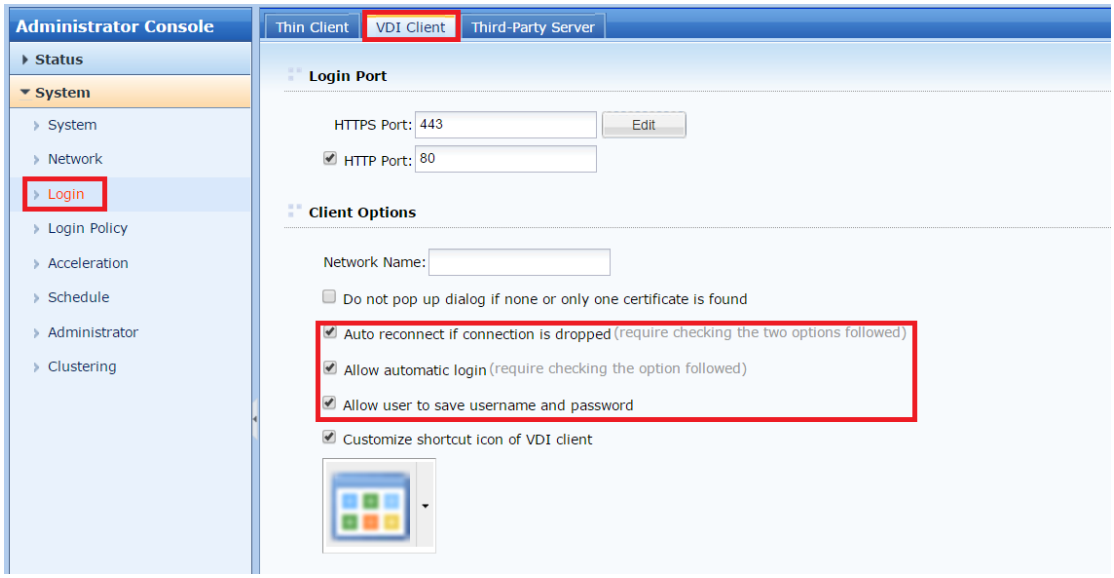
2.3 VDC console

Login VDC console；

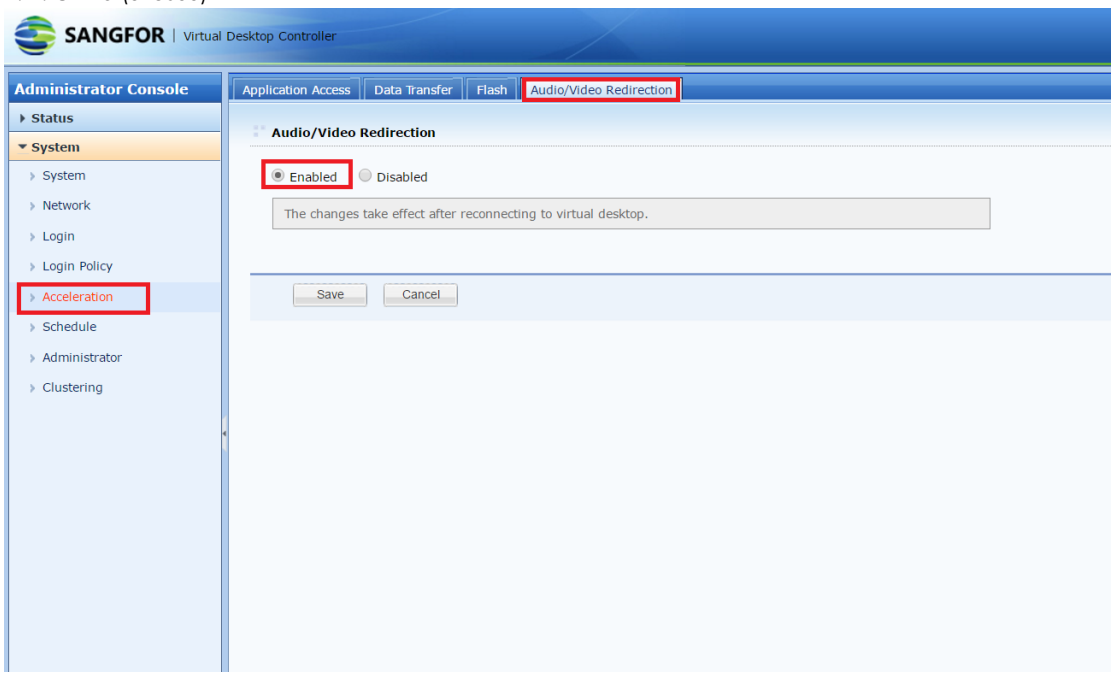
1. Enter【system】-【login】-【thin client】，select Automatically download and install updates，and Launch VDI client upon startup；



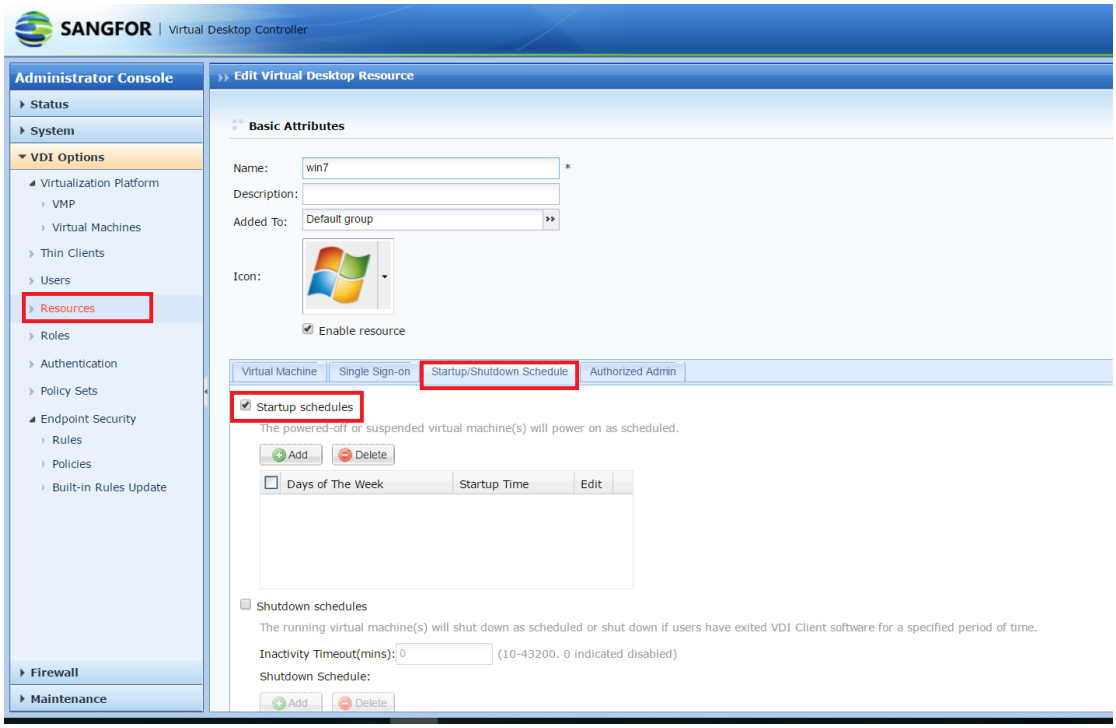
2. Enter【system】-【login】-【VDI Client】, select ‘Auto reconnect if connection is dropped’, ‘Allow automatic login’, ‘Allow user to save username and password’;

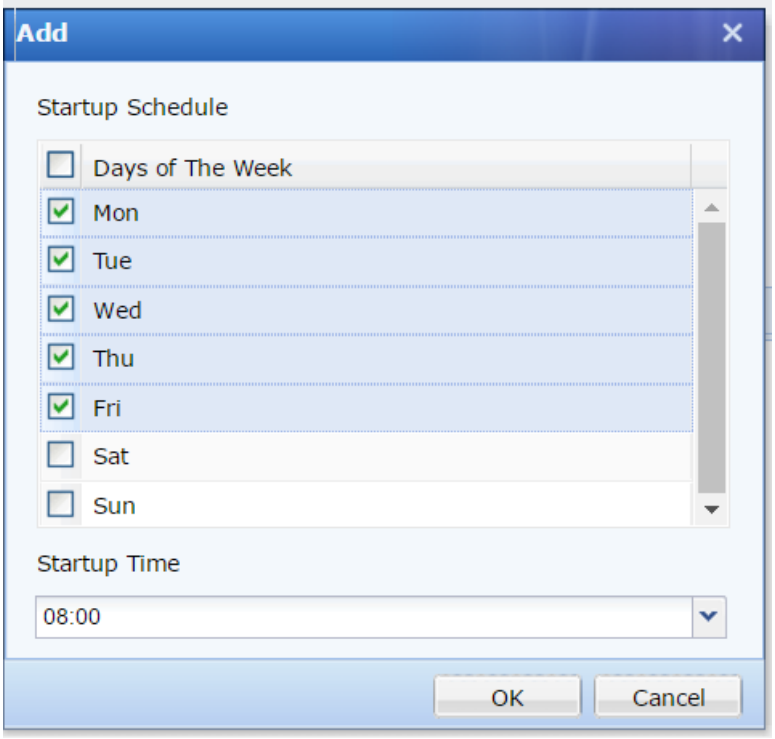


3. (**Optional**) Enter【system】-【acceleration】-【audio/video redirection】, select ‘enabled’ and save;

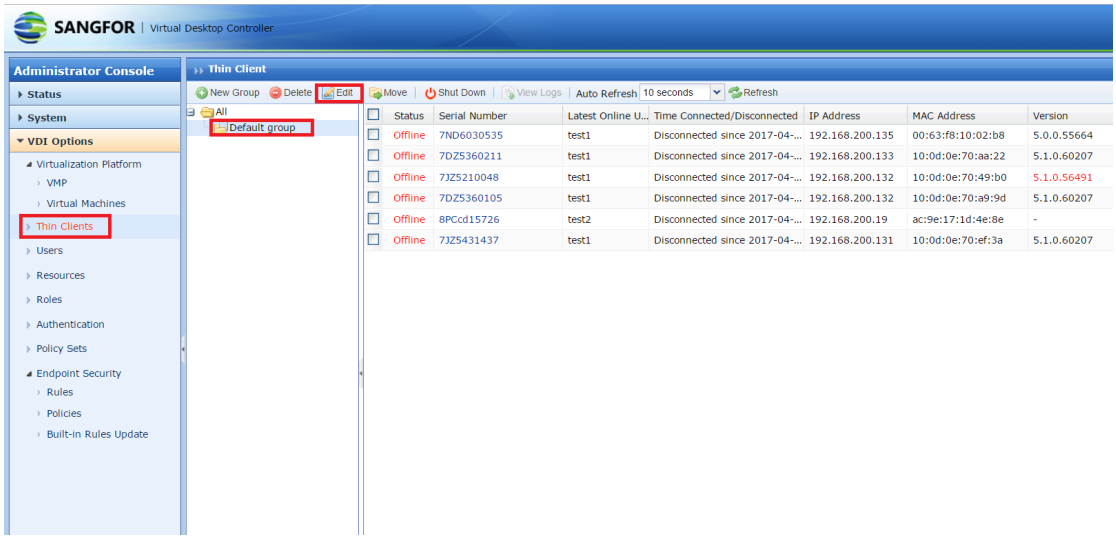


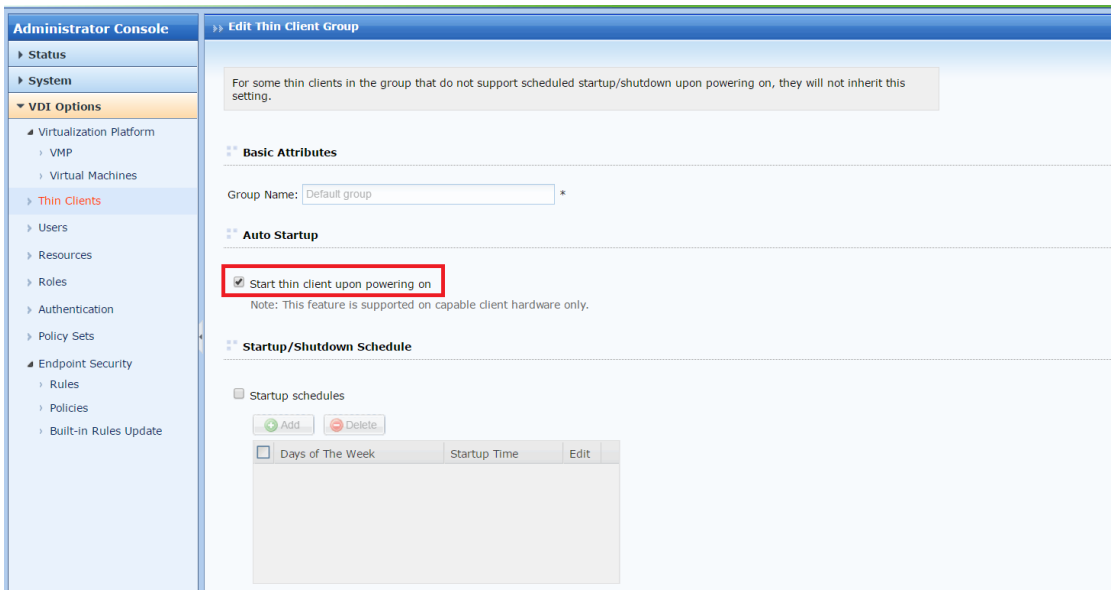
4. (**Optional**) startup and shutdown schedule. Enter【VDI options】-【resources】，choose the resource required to be scheduled，select【startup/shutdown schedule】. Here select startup schedule as example， then add the days in a week and startup time；



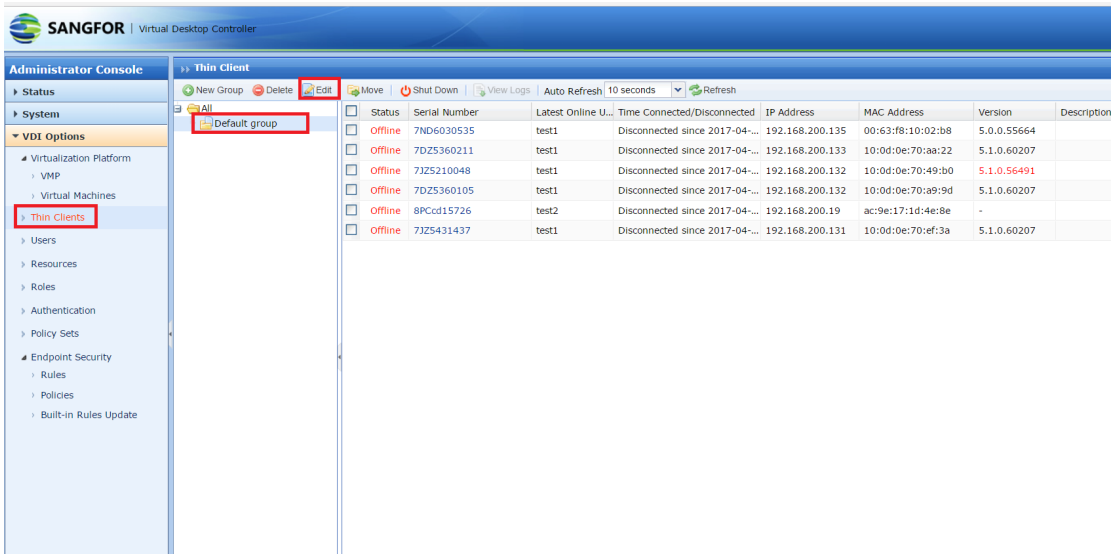


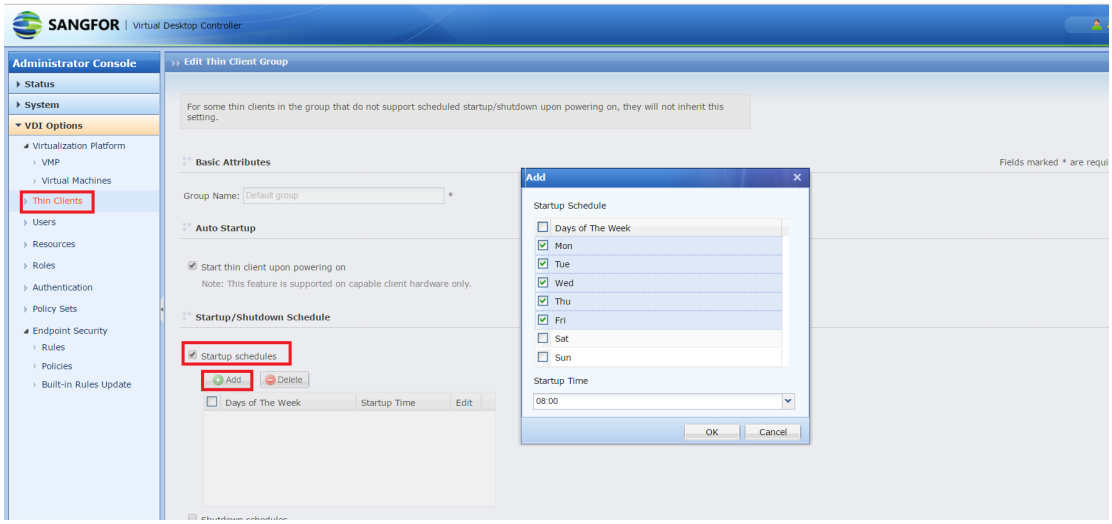
5. (**Optional**) Start thin client upon powering on. Enter【VDI options】-【thin clients】，select a user group （notice： selecting a user can not configure successfully) - "edit" ，select "Start thin client upon powering on" ；



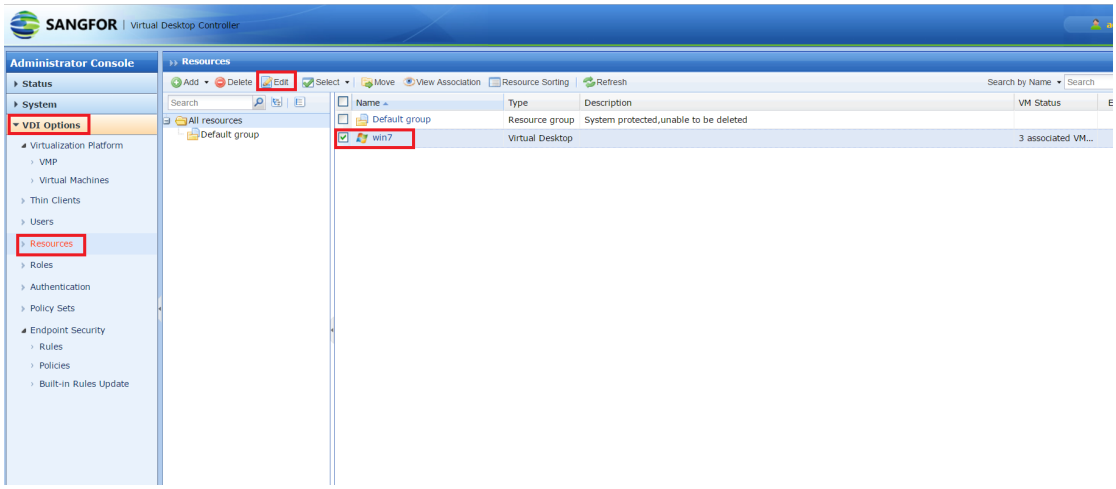


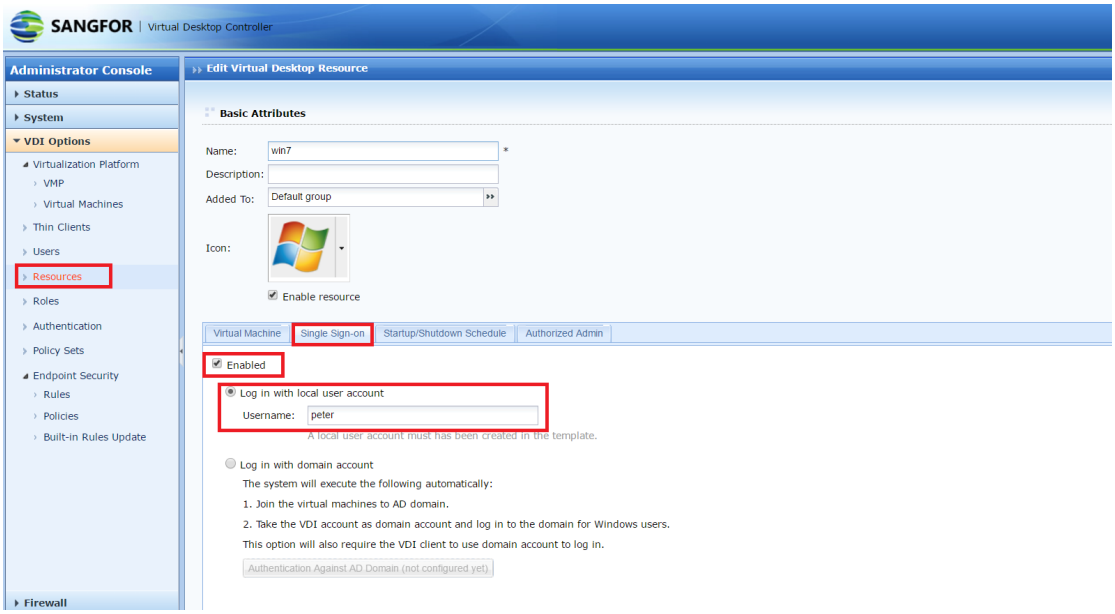
6. (**Optional**) Startup/shutdown schedules of thin client. Enter【VDI options】-【thin clients】，select a user group-“edit”. Here we select startup schedule as example，select“add”，then add the days in a week and startup time；





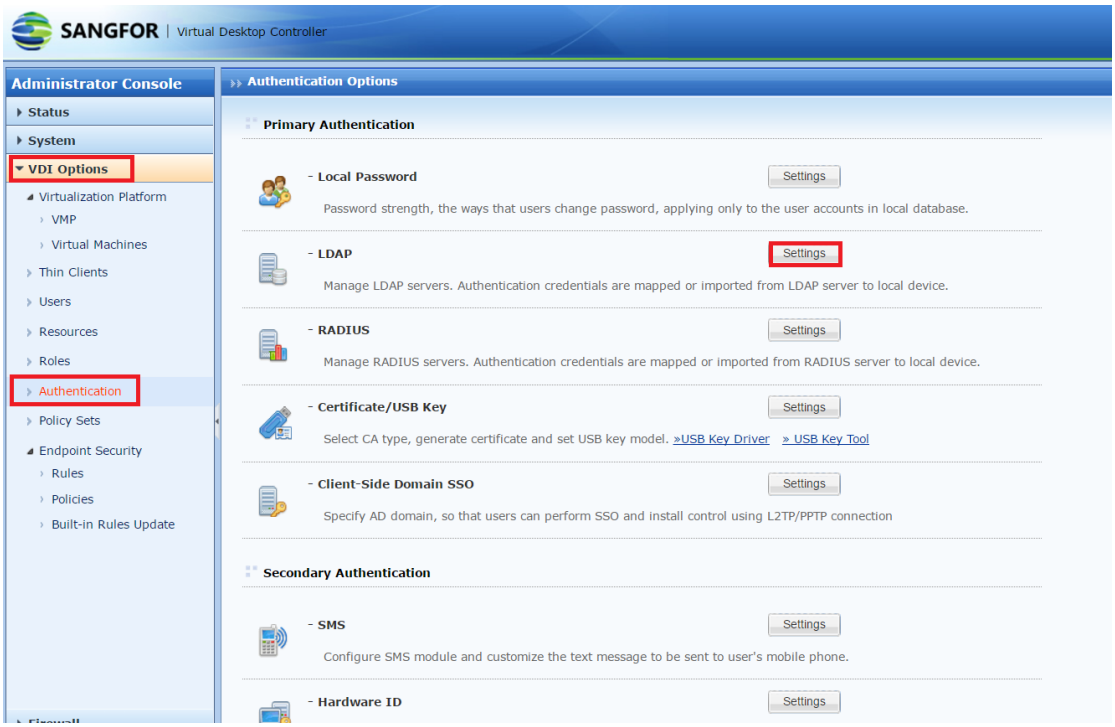
7. (**Optional**) Auto login to virtual desktop on startup. Enter【VDI options】-【resources】and select "Win7x64". Select "single sign-on" and "login with local user account" , fill in Windows user name ;





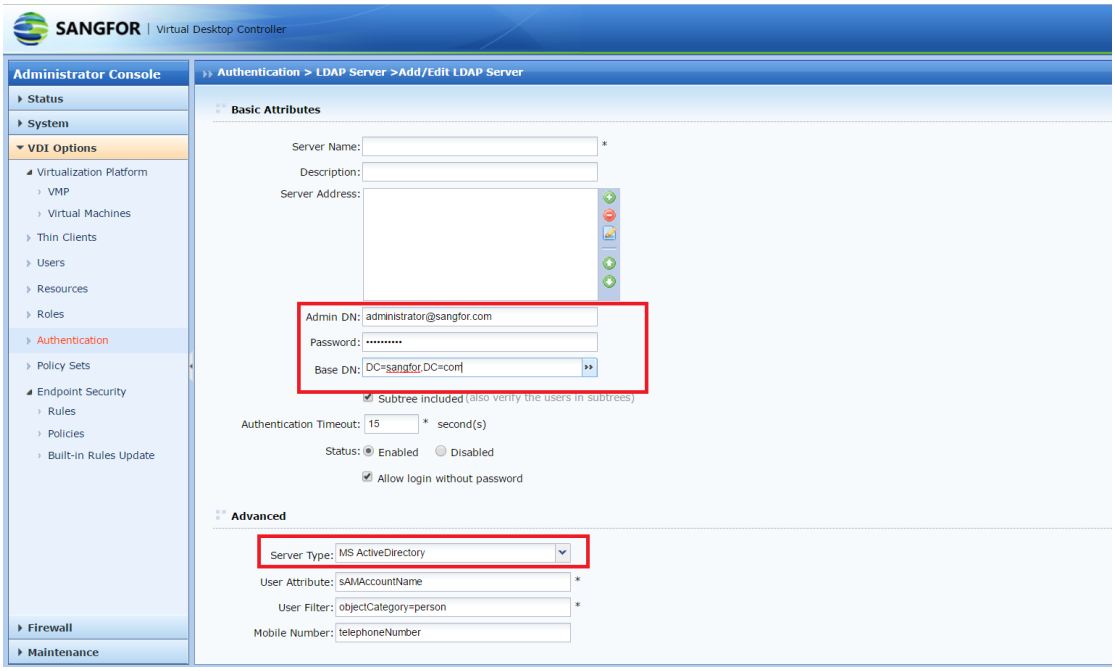
8. (**Optional**) Auto login to domain on startup.

✧ Enter【VDI options】-【authentication】-【LDAP】- "settings" ;

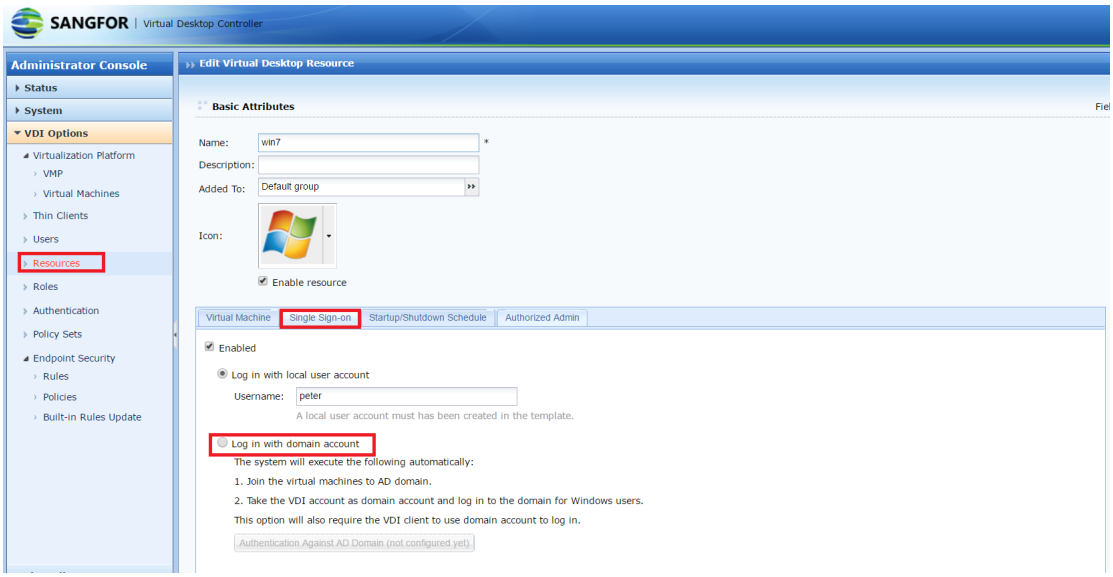


✧ Create LDAP server，provide the IP with AD domain control and the administrator account with access permission to user information，then the organization framework is available. Please notice the format of administrator

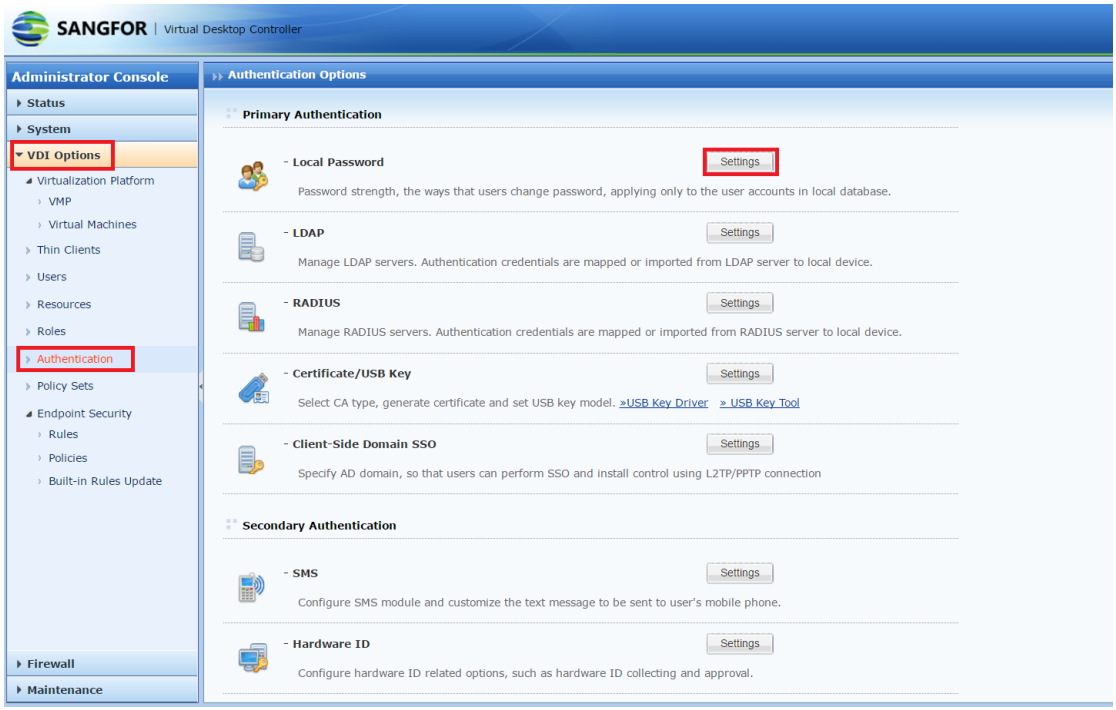
DN and after finishing the configuration，the LDAP user will belong to the default group in VDC；

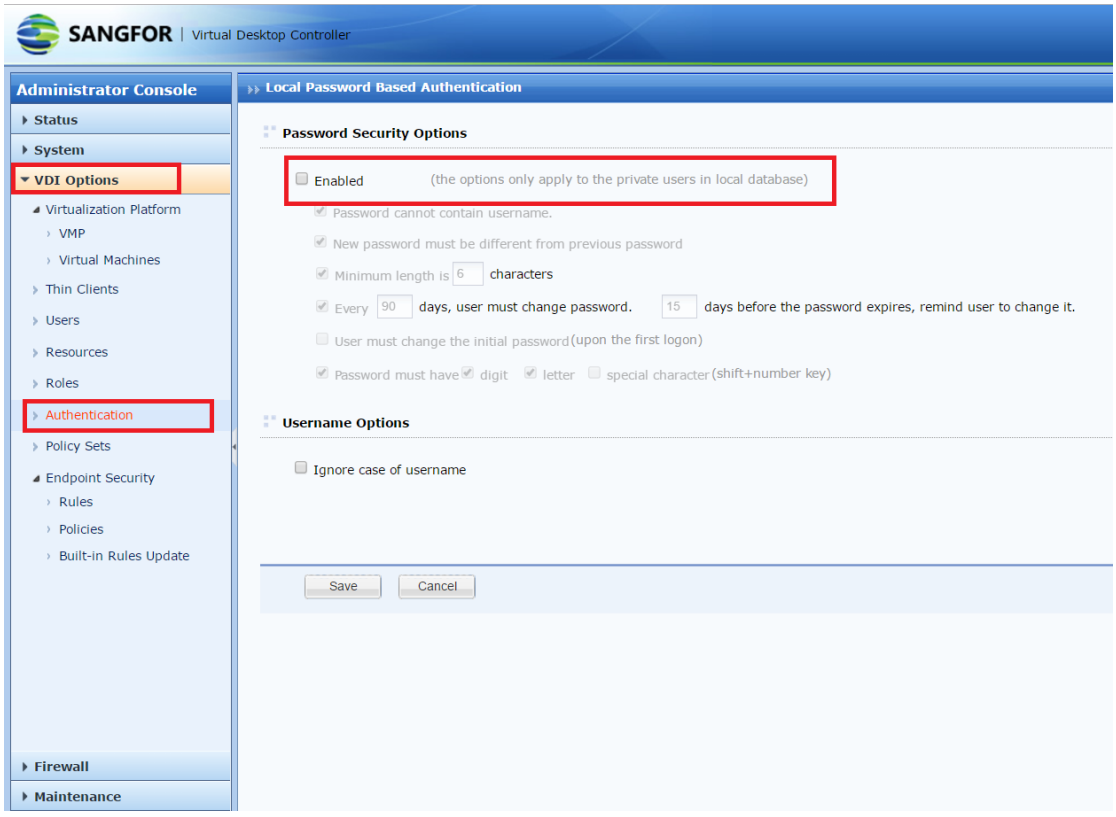


✧ Enter【VDI options】-【resources】, select "**Win7x64**", select 'single sign-on' and 'log in with domain account', configure server domain name，admin CN，admin password. Please notice the format of administrator name and only administrator name is necessary；

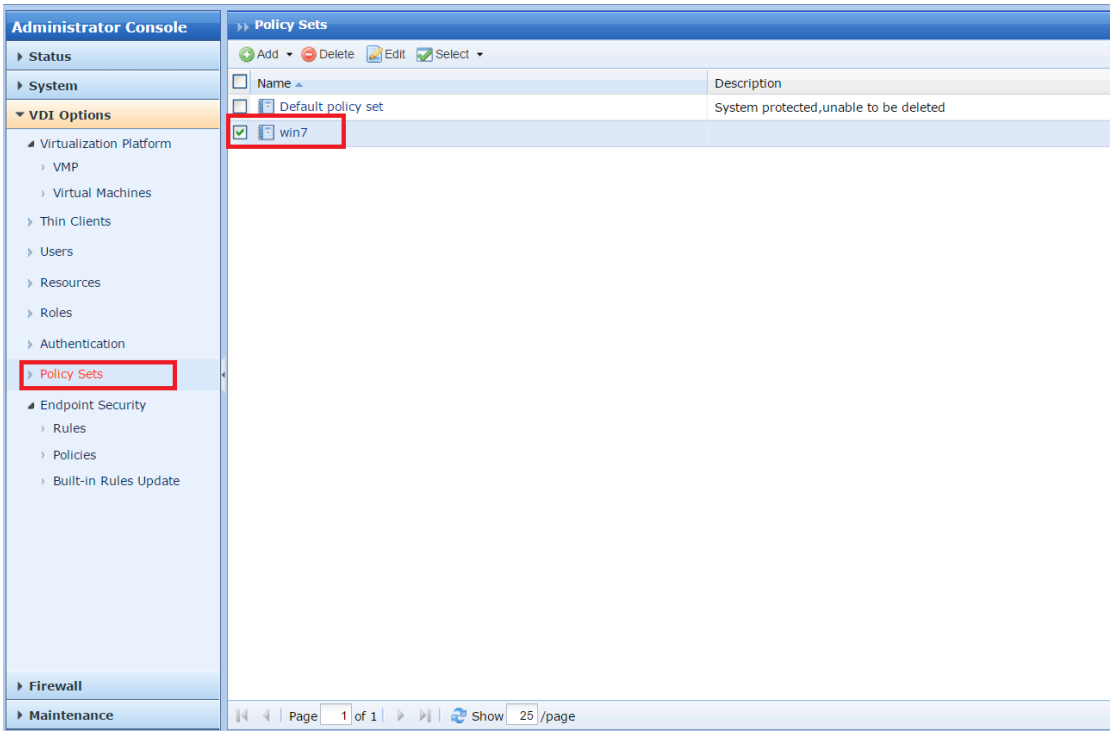


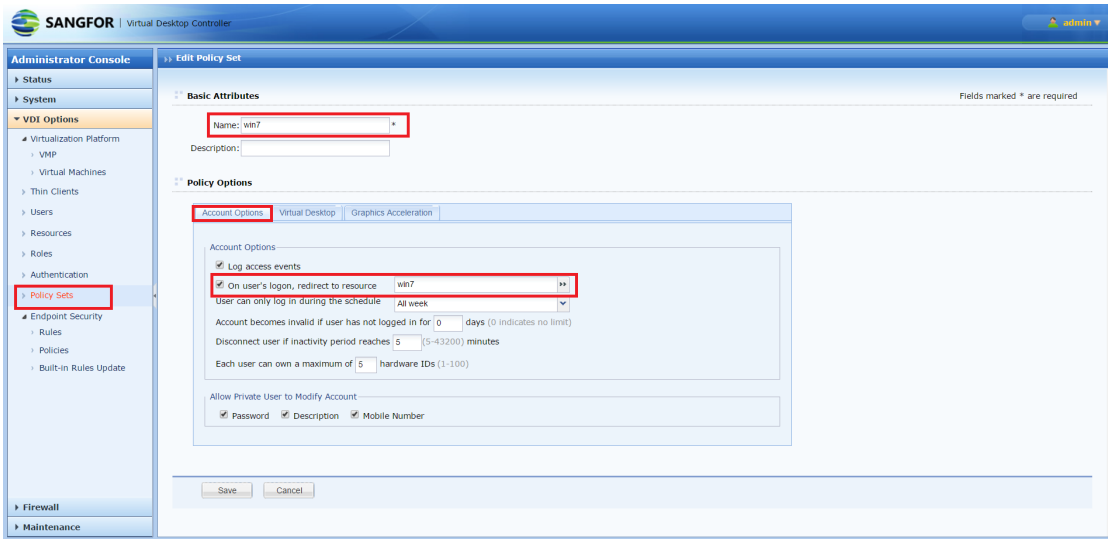
9. (**Optional**) 【VDI options】-【Authentication】- "local password" , select "settings" , **cancel** "enabled" ; (if it is enabled , you are required by force to modify password on first login) ;





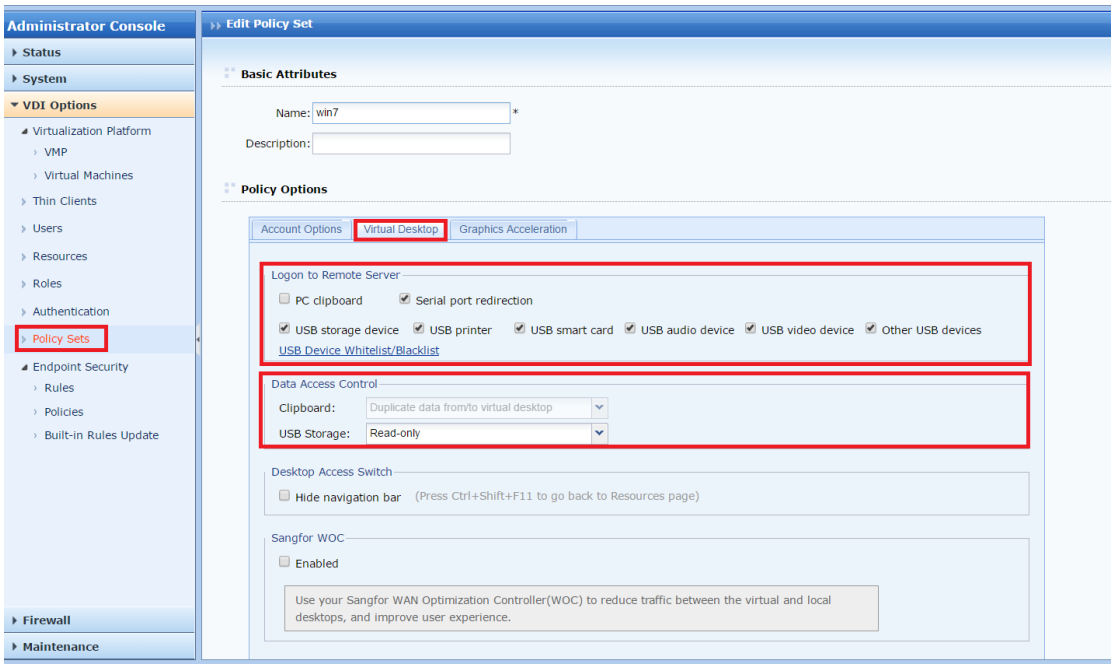
10. (**Optional**) Auto redirect to a virtual desktop resource. Enter【VDI options】-【policy sets】，select“**Win7**”and click“edit”，select“on user's logon，redirect to the resource”and choose“Win7”；





11. (**Optional**) Compatibility with USB device. Enter【VDI options】-【policy sets】，click【virtual desktop】，select all options in“logon to remote server”，

select "duplicate data from/to virtual desktop" for "clipboard" , select "read/write" in "USB storage" , select "hidden navigation bar" ;



3. Test items

〖introduction〗

Several times startups and shutdowns are involved in the test items. You may sort the test sequence to save time

3.1 Terminal compatibility

3.1.1 Thin client aDesk

〖scenario〗

Adopting Sangfor proper thin client aDesk as terminal to access desktop enables the same user experience as physical computer

〖process〗

Power on the aDesk and fill in username test1，password 123456 to enter virtual desktop

〖expected result〗

Enter the virtual desktop

3.2 Desktop management

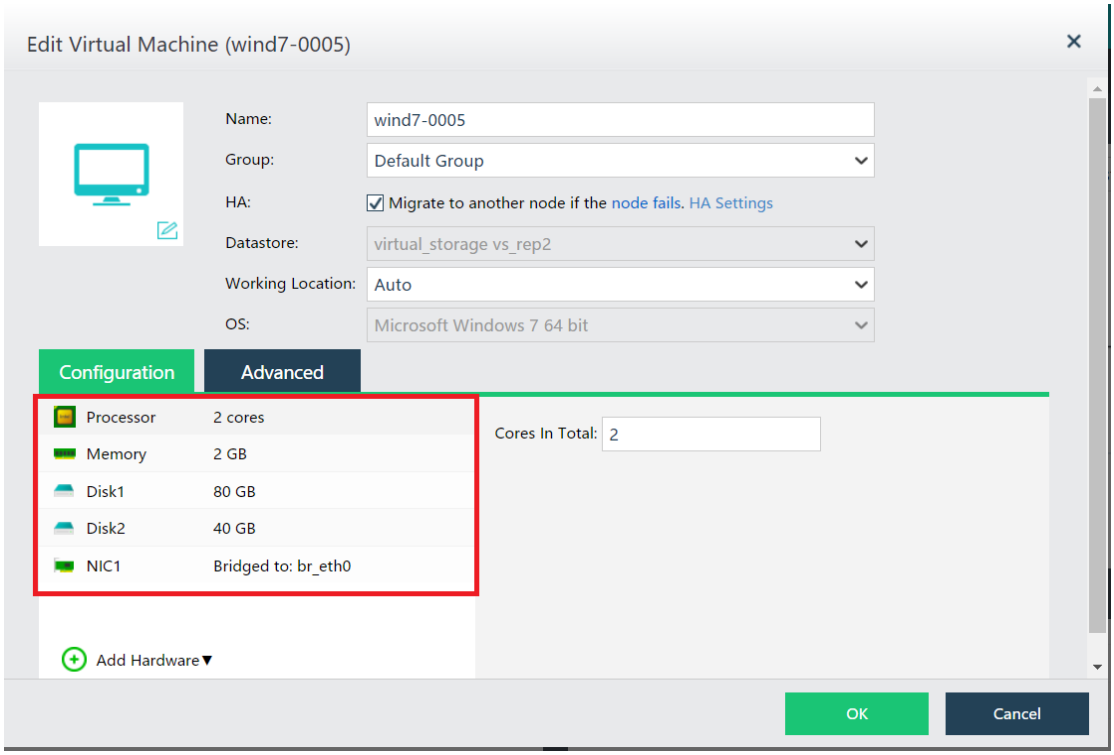
3.2.1 Resource allocation for virtual machine

〖scenario〗

VDI enables resource allocation for virtual machine like computing，storage，network resource and resource adjustment according to demand

〖process〗

Login VMP console and shut down a virtual machine. Enter edit page and modify memory，CPU，hard disk size and NIC. Then save and power on the virtual machine



〖expected result〗

The virtual machine resource been modified on powering on

3.2.2 Restore mode

〖scenario〗

Deployed virtual machine has two modes : private and restore. For virtual machine in restore mode，after each restart the system disk will restore to the status of related template

〖process〗

1. Create virtual desktop resource and choose the restore mode
2. Power on the new virtual machine in VDC console，ensure Agent installed and the connection between Agent and VDC succeeded（virtual machine status is green in VDC console）
3. Create folder and file in the virtual machine's system disk and restore

〖expected outcome〗

The new folder and file do not exist after restart

〖tips〗

When creating virtual machine in restore mode，it is default to follow "automatically restore desktop". In such case，the modification in desktop will be restored too after restart

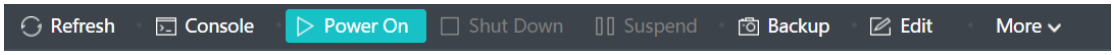
3.2.3 Basic operation of virtual machine

〖scenario〗

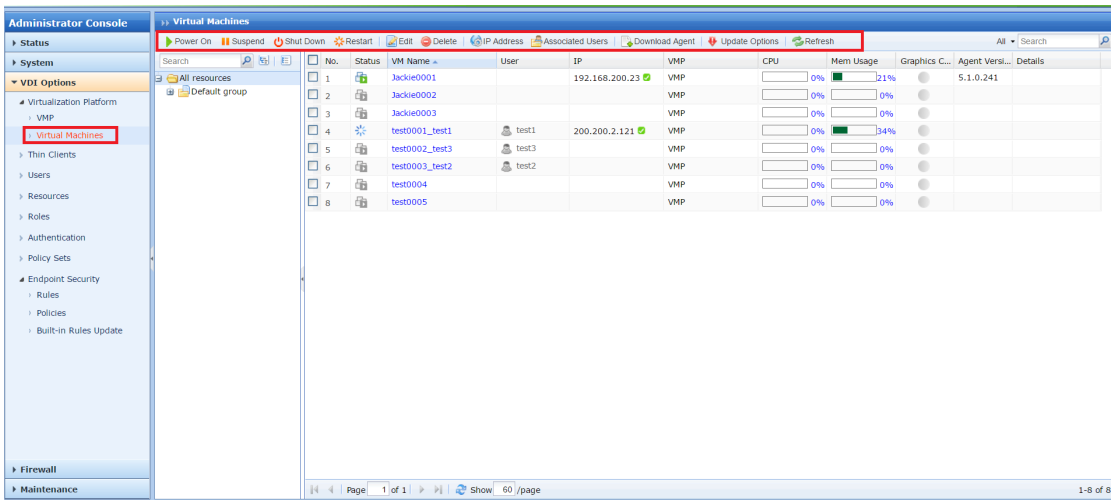
Administrator can start，suspend，restart，shut down virtual machine uniformly in VMP and VDC console

〖process〗

1. Login VMP console and then enter virtual machine console, click start or other button



2. Login VDC console，进入【VDI options】-【virtual machines】, select the virtual machine， and click "restart"



〖expected result〗

You can power on the virtual machine in both VMP and VDC

3.2.4 Desktop batch deployment

〖scenario〗

Support quick deployment with template for more than 100 desktops

〖process〗

Refer to virtual machine deployment

〖expected result〗

New virtual machines deployed can be seen in VMP console

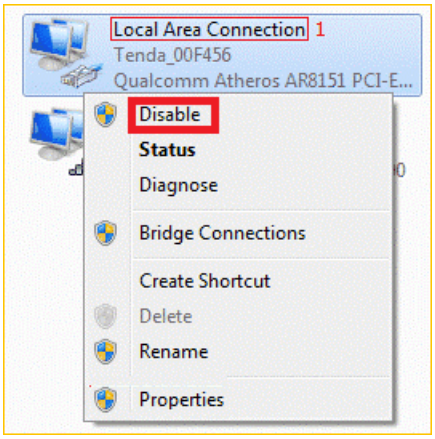
3.2.5 Independence of virtual machine NIC

〖scenario〗

The connection of virtual desktop does not depend on virtual NIC. User's operation on NIC in virtual machine will not influence the connection

〖process〗

Access to virtual desktop by aDesk and forbid NIC function



〖expected result〗

No impact on virtual desktop's connection to VDC

3.2.6 Remote desktop operation

〖scenario〗

Supporting remote access to desktop console without any plug-in

〖process〗

1. If you have logged in to the virtual desktop in an aDesk please logout the VDI account. The system is embedded with leak prevention

2. Login the VMP console and the mouse stay in the virtual machine icon for seconds. Click console and input username and password to enter virtual desktop.

〖expected result〗

Fluency of operation for virtual desktop.

3.2.7 Hidden navigation bar

〖scenario〗

After hiding the navigation bar，user cannot see the navigation bar in virtual desktop to restrict user's operation like exiting desktop，modifying VDI information.

〖process〗

Please refer to the "hidden navigation bar"

〖expected result〗

When getting access to virtual desktop with aDesk，there is no navigation bar and user can only exit desktop by combination key Ctrl+shift+F11

3.3 User experience

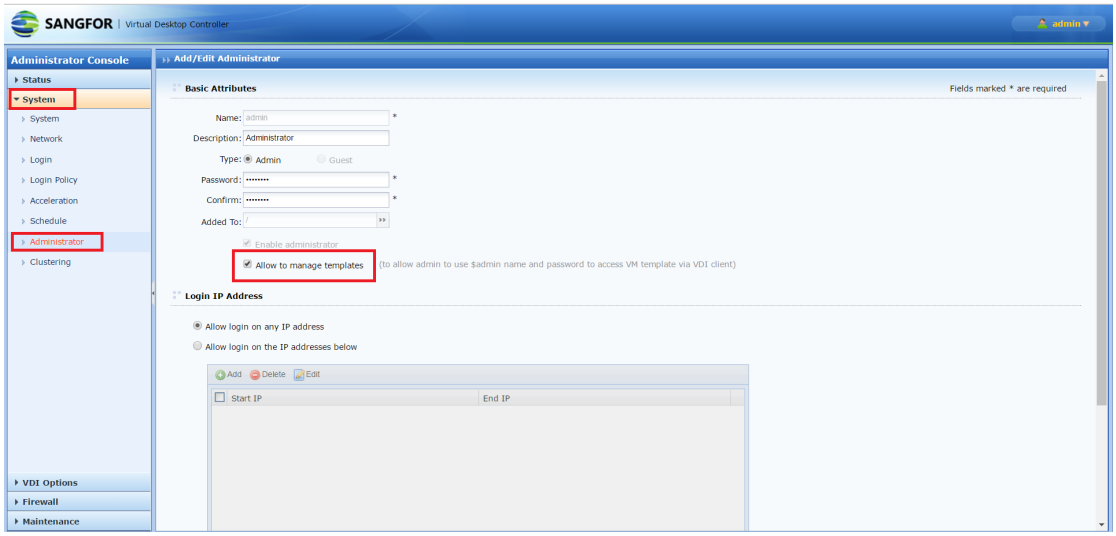
3.3.1 Software and drive installation in template

〖scenario〗

Access to template with an aDesk and install software and drive for external device. Then deploy virtual machine.

〖process〗

Login VDC console and enter【system】-【administrator】, select "allow to manage template"



Login to VDI in a aDesk，with the username： $+ "administrator's username and password"：administrator's password（in this example it is $admin and admin）.

Then you could install software and drive in the template desktop

〖expected result〗

Successful access to template and installation of software

3.3.2 Resolution ratio

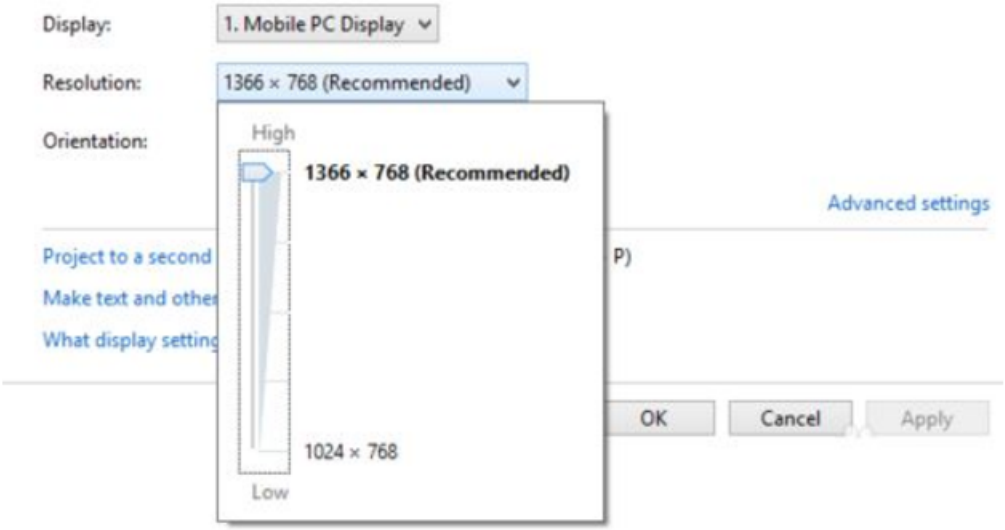
〖scenario〗

User can modify the resolution ratio in virtual machine and the resolution ratio in terminal will be adjusted correspondingly

〖process〗

1. Click the right mouse button in the desktop and click screen ratio

2. Select a screen resolution differing from present one



〖expected result〗

Configuration succeed

3.3.3 Auto startup on powering on for thin client

〖tips〗

Test the function with STD-200H

〖scenario〗

For the scenario where user adopt unified power system, you may activate auto Startup on powering on for thin client to simplify user's operation

〖process〗

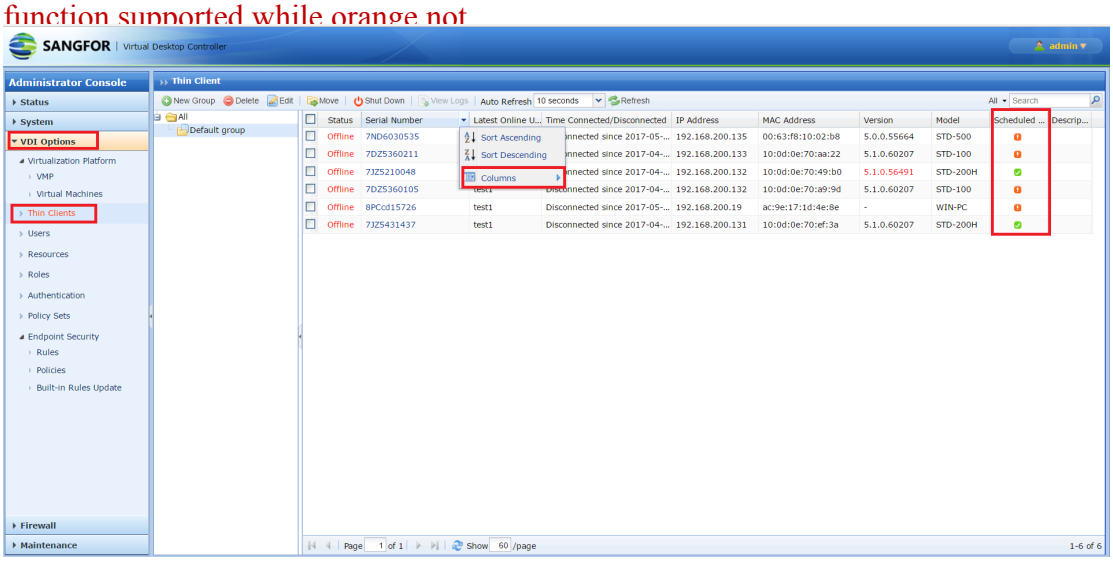
1. Ensure the function have been activated
2. Power on the aDesk

〖expected result〗

Auto startup and login to desktop

〖tips〗

Not all aDesk mode supports the operation. You may enter【VDI options】-【thin client】and observe the icon in scheduled startup/shutdown. If green means function supported while orange not



3.3.4 Auto login to virtual desktop on startup

〖scenario〗

User can login to desktop without any operation after startup to avoid inputting VDI account and desktop account

〖process〗

1. Ensure the function has been activated
2. Startup the aDesk and fill in VDI account. select remember password and auto login, then enter desktop
3. Restart aDesk

〖expected result〗

In restart you can login desktop directly

〖tips〗

Please do not test the function with mobile device （pad or cellphone）on your first try.

3.3.5 Auto login to domain

〖scenario〗

VDC supports LDAP authentication，administrator has no need to create account in VDC. Login to virtual desktop with username and password in domain，without logging in to VDI and Windows

〖process〗

1. Ensure the function has been activated
2. Power on the aDesk and fill in the account in domain server. Select remember password and auto login
3. Restart aDesk

〖expected result〗

1. Auto login to Windows desktop on restart
2. Domain information of virtual desktop can be checked in computer attribute

3.3.6 Associated shutdown of thin client and virtual desktop

Shutdown virtual machine then shutdown thin client automatically

〖scenario〗

When user shutdown virtual machine，the thin client needs to be shutdown too. After the function's activation，the thin client will be shutdown automatically

〖process〗

1. Ensure the navigation bar have been hidden
2. Shutdown the virtual machine

〖expected result〗

The power light of aDesk quenches after the virtual machine's shutdown

Shutdown thin client then shutdown virtual machine automatically

〖scenario〗

When user shutdown thin client，the virtual machine needs to be shutdown too. After the function's activation，the virtual machine will be shutdown automatically

〖process〗

Press the aDesk's power button and observe the virtual desktop's shutdown

〖expected result〗

Virtual machine 's shutdown can be observed in VMP after the aDesk's shutdown

〖tips〗

The function is only activated on the virtual desktop interface，not on login Interface or Android interface

3.3.7 Redirection of local video

〖scenario〗

Redirection of local video can reduce the server load on playing video and network traffic in aDesk end. Which makes playing local video more fluent

〖process〗

1. Ensure the function have been activated
2. Play local video on Windows Media Player or stormplayer

〖expected result〗

The video playing is fluent and CPU usage of virtual machine is less than 15%

〖tips〗

1. The function takes effect only with aDesk
2. The function takes effect only with specific video player：Windows Media

Player，stormplayer

3.3.8 Scheduled startup and shutdown for thin client

〖notice〗

Test the function with STD-200H

〖scenario〗

Scheduled startup and shutdown can be configured to avoid startup/shutdown storm and realize unified management. After the configuration the thin clients will startup or shutdown in schedule

〖process〗

1. Ensure the function has been activated
2. Modify the startup and shutdown time to 2，4 minute later and save

〖expected result〗

Auto startup 2 minutes later，auto shutdown 4 minutes later

3.3.9 Scheduled startup and shutdown for virtual machine

〖scenario〗

Scheduled startup and shutdown can be configured to avoid startup/shutdown storm and realize unified management. After the configuration the virtual machines will startup or shutdown as scheduled

〖process〗

1. Ensure the function has been activated

2. Modify the startup and shutdown time to 2，4 minute later and save

〖expected result〗

Login to VMP console，you can observe the virtual machines startup 2 minutes later and shutdown 4 minutes later

〖tips〗

If user is online ，the function will not work

3.4 Data access control

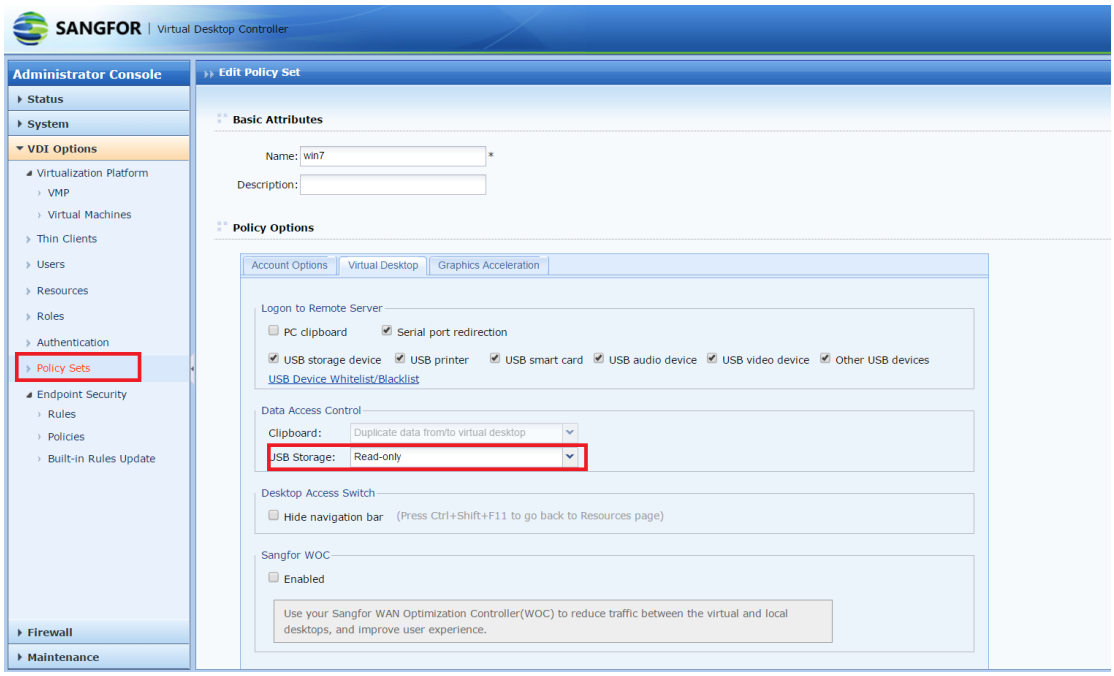
3.4.1 Data access control of USB flash drive

〖scenario〗

Read and write in USB flash drive can be controlled by set policy set. Read-only mode for USB flash enables data security in specific case

〖operation〗

1. Enter【VDI options】-【policy sets】，click "**Win7**" to edit and select read-only for USB storage



2. Re-login to VDI. Insert an USB flash and try to copy file into it

〖expected result〗

File can be read but the copy fails

3.4.2 USB camera/high speed camera

〖scenario〗

USB camera and high speed camera can be recognized and normally used with aDesk

〖process〗

1. Insert USB camera/high speed camera to aDesk
2. Drive installation
3. Open the device and test the function

〖expected result〗

All functions are realizable for camera

3.4.3 E-bank/Authentication KEY

〖scenario〗

E-bank /Authentication KEY is used in office situation. aDesk enables use of these devices

〖process〗

1. Insert E-bank /Authentication KEY to aDesk USB interface
2. Driver installation
3. Open the devices and test the function

〖expected result〗

All functions are working properly

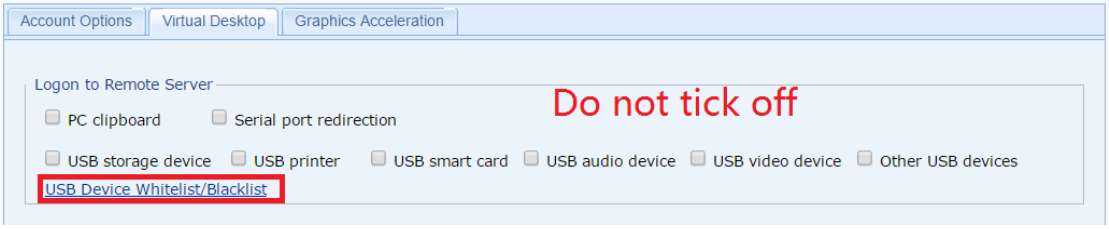
3.4.4 USB white list

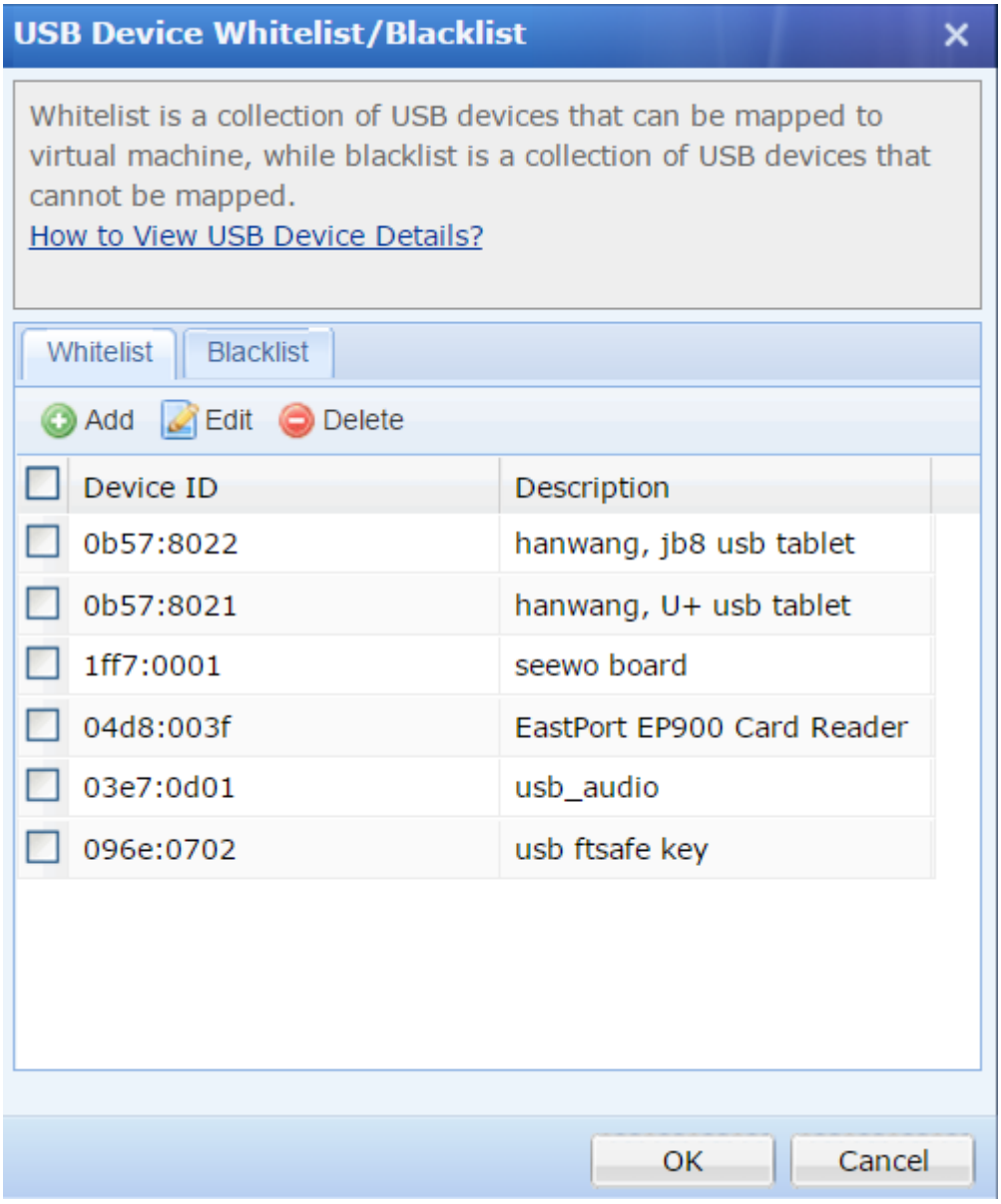
【scenario】

Some USB devices can be used after mapping to virtual desktop. For such devices you need adding them to white list for mapping by force

【process】

1. Insert an USB device and ensure the driver installed
2. Open device manager in virtual desktop and unfold "Other devices" or "USB controller" list to find the device
3. Double click the device and check the hardware information to get VID and PID
4. Select the corresponding【policy sets】in VDC console，cancel all access control and click USB device whitelist/blacklist，then add the device's VID and PID into the white list





〖expected result〗

1. Enter virtual desktop and the mapped device is visible in desktop
2. Normal use of the device

3.4.5 USB blacklist

〖tips〗

1. For serial port（COM）device，you may need a USB converter

〖scenario〗

For some USB devices，the desktop performance will be influenced if it is mapped to virtual desktop. In such case you may add the device into the blacklist

〖process〗

1. Check the device's VID/PID；
2. Add the VID/PID into blacklist

〖expected result〗

1. The device cannot be mapped or used in virtual desktop
2. The device can be used in aDesk/physical PC

3.5 Management of user and thin client

3.5.1 Auto update of thin client

〖scenario〗

After the system has been updated，all devices connecting to VDC should update automatically for reducing user's operations

〖process〗

1. Ensure the function has been activated
2. Update VMP and VDC

〖expected result〗

Startup the thin client after updating and a reminder for auto update is visible in the desktop

3.5.2 Message sending from administrator to user

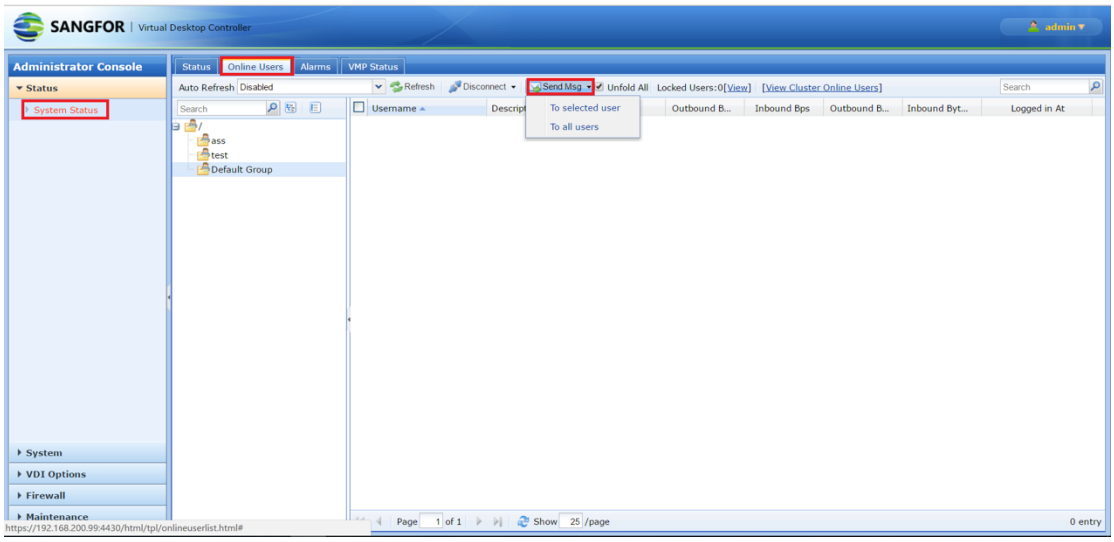
〖scenario〗

Administrator is able to send message to user for direct management

〖process〗

1. Login the 2 accounts test1 and test2 with a aDesk and PC to get access to virtual desktop

2. Login VDC console，enter 【status】-【system status】-【online users】，click“send Msg”-select“to all users”



〖expected result〗

Both of test1 and test2 get the message in a windows pops up

3.5.3 Batch assignation of virtual machine IP

〖scenario〗

Unified IP configuration and management of the derived virtual machines reduces deployment time and O&M cost. However，virtual machine in restore mode does not support the batch assignation

〖process〗

1. Login to VDC console
2. Confirm that Agent has been installed and connected to VDC
3. Click the virtual machine you want to configure. Click edit – set IP address and restart the virtual machine
4. Click multiple virtual machines and batch assign IP address，then restart

the virtual machines

〖expected result〗

After the restart，the virtual machine's IPs has been altered to the assigned IP

3.5.4 Binding user

- **Bind single user and virtual machine**

〖scenario〗

By activating the binding， the functions below are available：

1. Binding specific virtual machine with user
2. Lock the specific virtual machine
3. Set the bound virtual machine free for other users

〖operation〗

1. Select the virtual machine，click "associated users"
2. Check the virtual machine's status

〖expected result〗

The status has been changed

- **Batch bind users and virtual machines**

〖scenario〗

With batch binding of users and virtual machines，multiple virtual machines are bound with a set of users one by one. Thus you can target quickly the failed desktop if the seat number corresponds with virtual desktops

〖process〗

1. Select the virtual machines you want to configure， click "associated users"，and modify the association
2. Check the virtual machine's status

〖expected result〗

The status has been changed

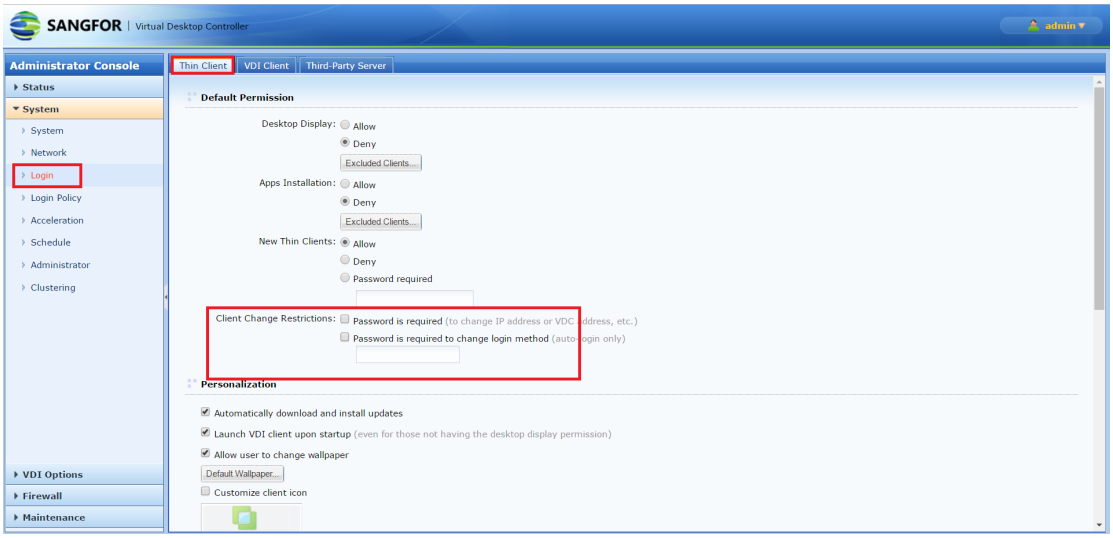
3.5.5 Modification limitation of client end's configuration

〖scenario〗

Requiring admin account can limit the client end's modification such as IP，VDC address to avoid uncontrolled modification

〖process〗

1. In VDC console，enter 【login】-【thin client】-【client change restriction】and set the new password sangfor123



2. Login to aDesk and try to modify the configuration such as IP，VDC address

〖expected result〗

1. A reminder for password appears and when you input a wrong password，the permission denied

2. When input sangfor123，the permission passed

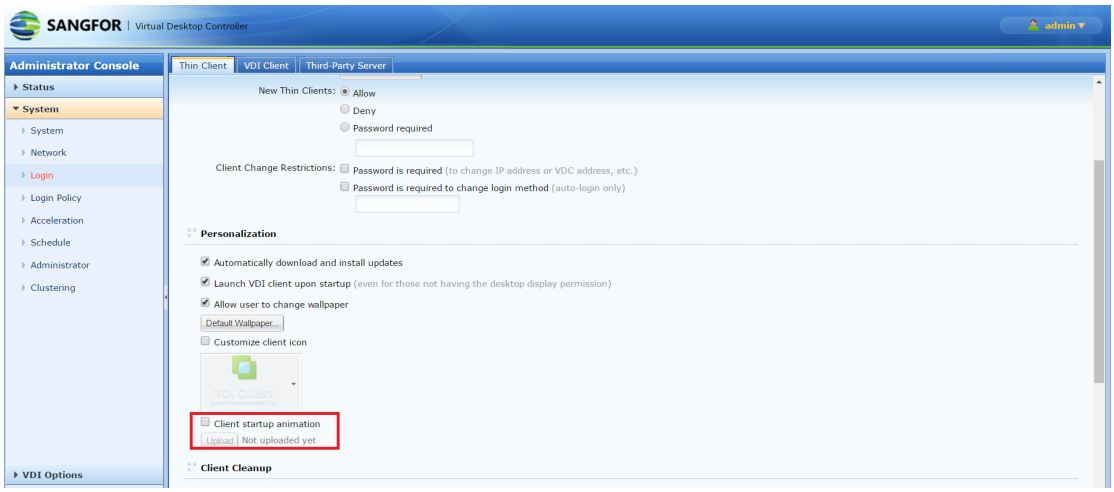
3.5.6 Customization of startup animation

〖scenario〗

Customization of startup animation. The enterprise's promotion video as example

〖process〗

1. In VDC console，enter【login】-【thin client】，tick off【client startup animation】，and upload animation



2. Restart aDesk and observe

〖expected result〗

The animation has been changed to the customized one

〖tips〗

The function are supported only for terminal based on ARM，not x86 or PC

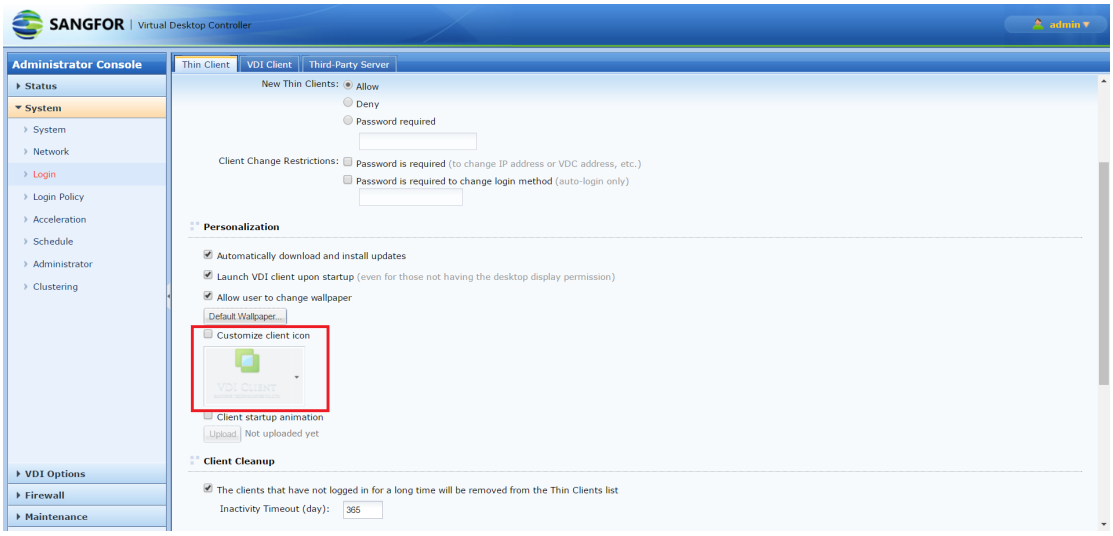
3.5.7 Customization of client icon

〖scenario〗

Customization of client icon，the enterprise's icon as example

〖process〗

In VDC console，enter【system】-【login】-【thin client】，select 【customize client icon】，and upload icon



〖expected result〗

Restart aDesk，the icon has been changed in login interface

〖tips〗

The function are supported only for terminal based on ARM，not x86 or PC

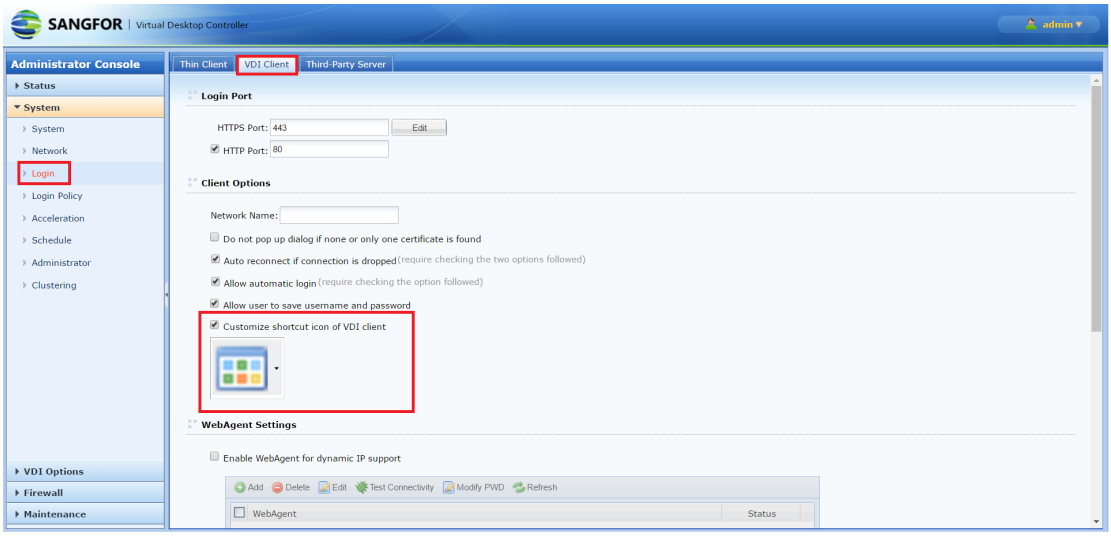
3.5.8 Customization of login shortcut icon

〖scenario〗

Customization of login shortcut icon of client end，the enterprise's icon as example

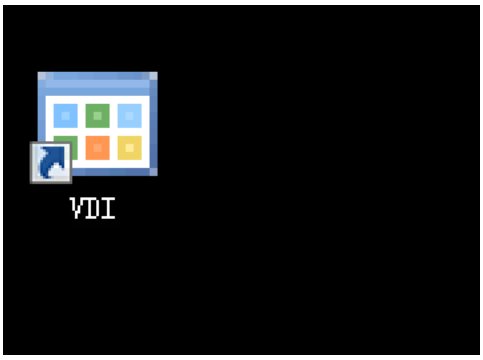
〖process〗

In VDC console，enter【system】-【login】-【VDI Client】，tick off 【customize shortcut icon of VDI client】，upload icon and save



〖expected result〗

The VDI icon has been changed when login with PC



〖tips〗

The function are supported only for PC

3.6 Security

3.6.1 USB-KEY authentication

〖scenario〗

If the access security is highly required，USB-KEY authentication can meet the demand

〖process〗

1. Please refer to USB-KEY authentication
2. Power on aDesk，enter login interface
3. Insert USB-KEY
4. Click "USB-Key login"
5. Enter PIN and login

〖expected result〗

Enter virtual desktop

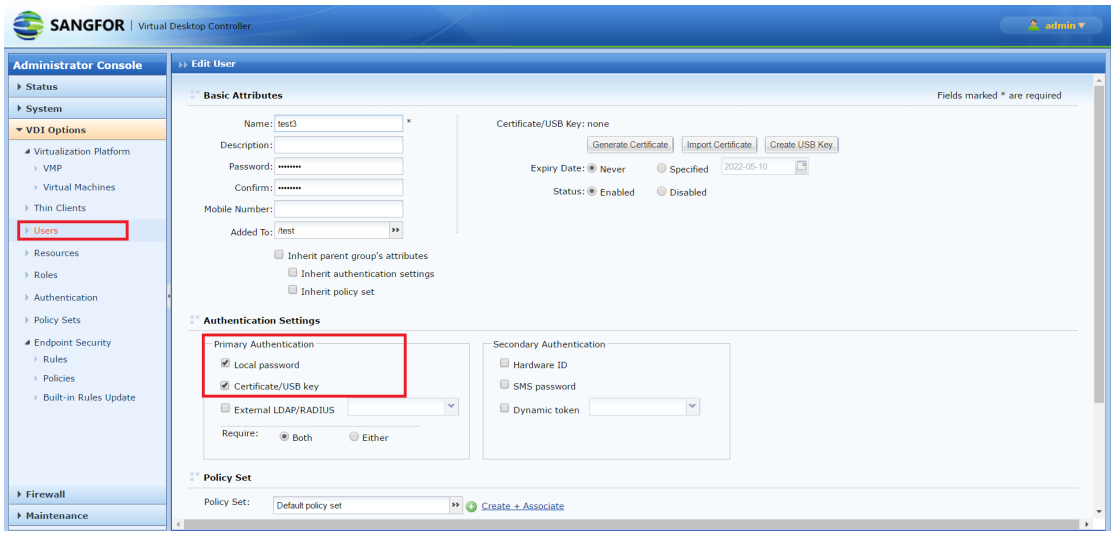
3.6.2 Password +USBKEY authentication

〖scenario〗

If the access security is highly required，password+USB-KEY authentication can meet the demand

〖process〗

1. In VDC console，enter【VDI options】-【users】，create **test3** with password **123456**，select "local password" and "certificate/USB key"



2. Please refer to USB-KEY authentication for configuration

〖expected result〗

1. Power on aDesk，in VDI login interface，enter test3 and pwd 123456，then insert KEY，and enter PIN. The login succeed

2. Only enter PIN，login fails；only enter account，login fails

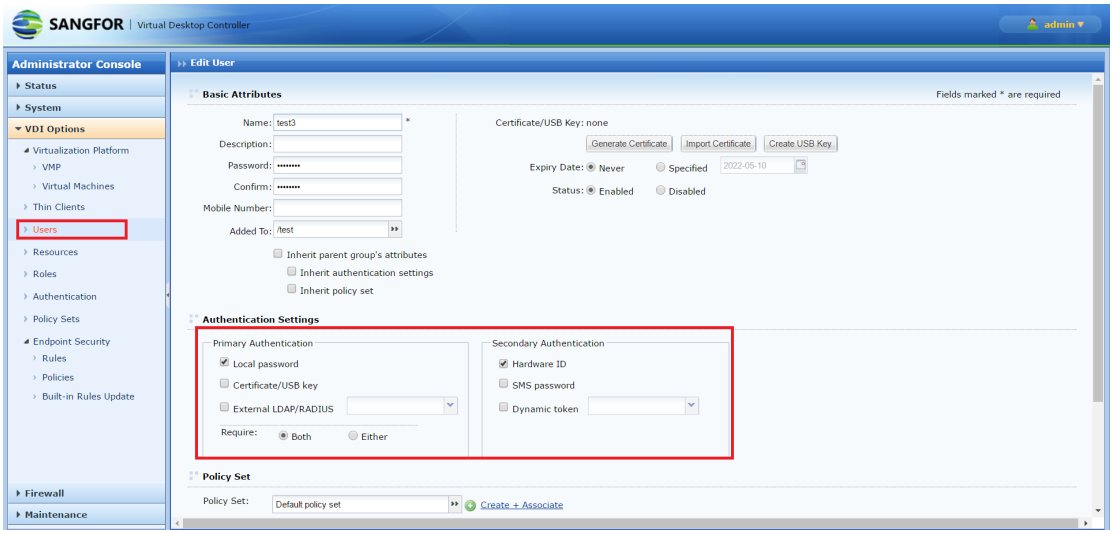
3.6.3 Password+hardware ID authentication

〖scenario〗

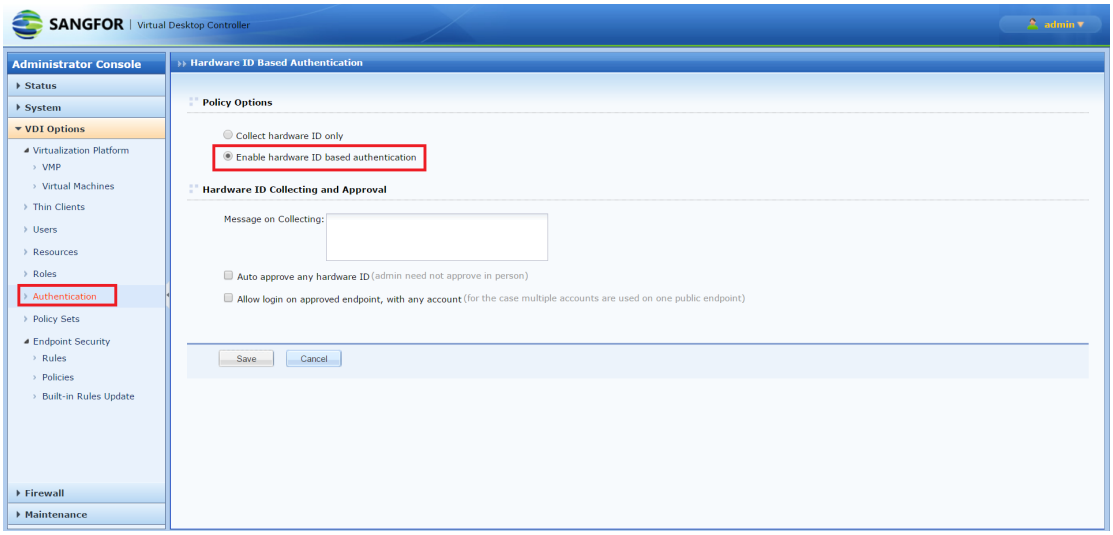
If the access security is highly required，password+hardware ID authentication can meet the demand. In such case，the VDI account is bound with device's hardware ID to enhance security

〖process〗

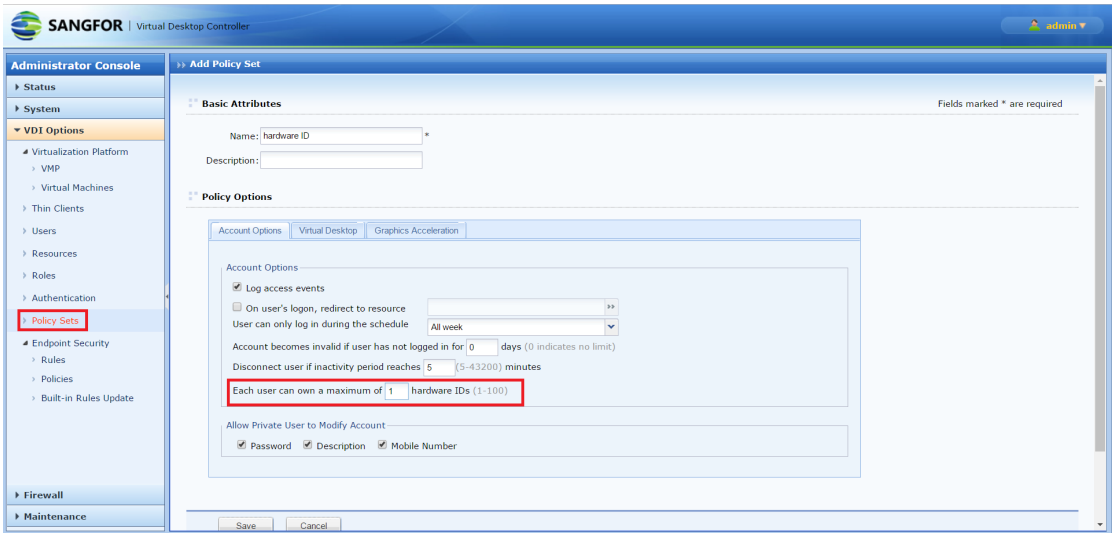
1. Enter【VDI options】-【users】，create user test3 with password 123456，select "local password" and "hardware ID"



2. Enter【VDI options】-【authentication】, click【hardware ID】, select "enable hardware ID based authentication"

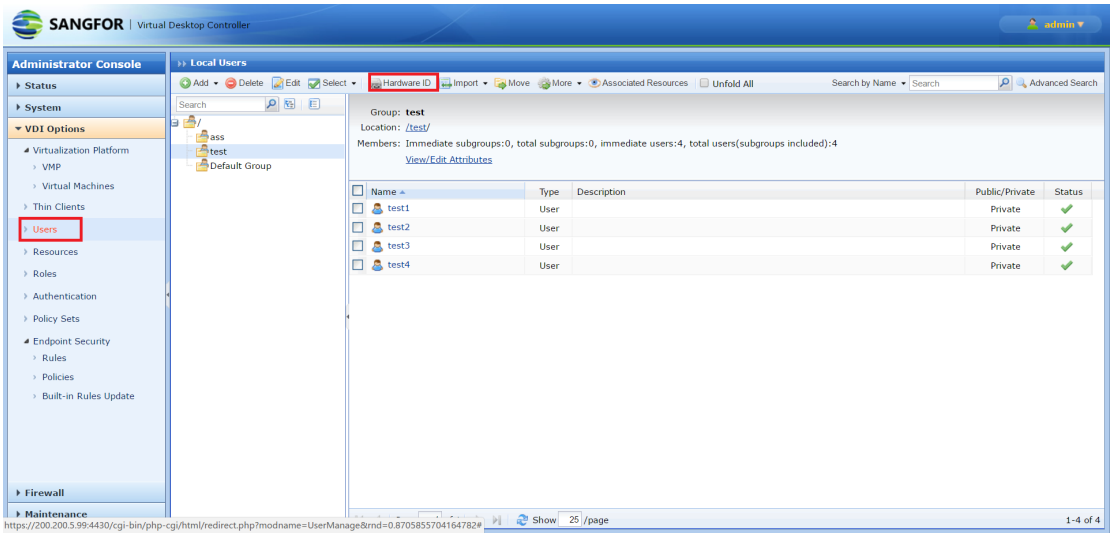


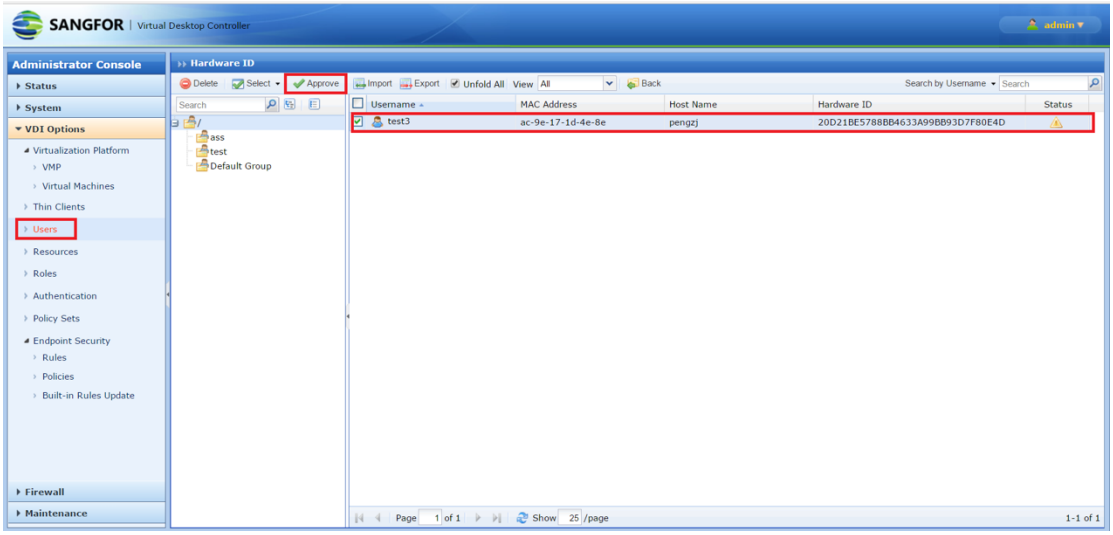
3. Enter【VDI options】-【policy sets】, create policy sets , name it "hardware ID" , configure "each user can own a maximum of 1 hardware ID"



4. Power on aDesk , enter username test3 , password 123456 , and login , the windows reminds "This account can only be registered on the authorized terminal. If you need to log in on this terminal, please submit your application to the administrator."

5. Enter【VDI options】-【user】,【hardware ID】, click test3 , and approve





6. Login again in the same terminal

〖expected result〗

1. Virtual desktop is accessible in terminal after the administrator's approval
2. Login with this account at another terminal fails

3.6.4 Combination with Sangfor IAM

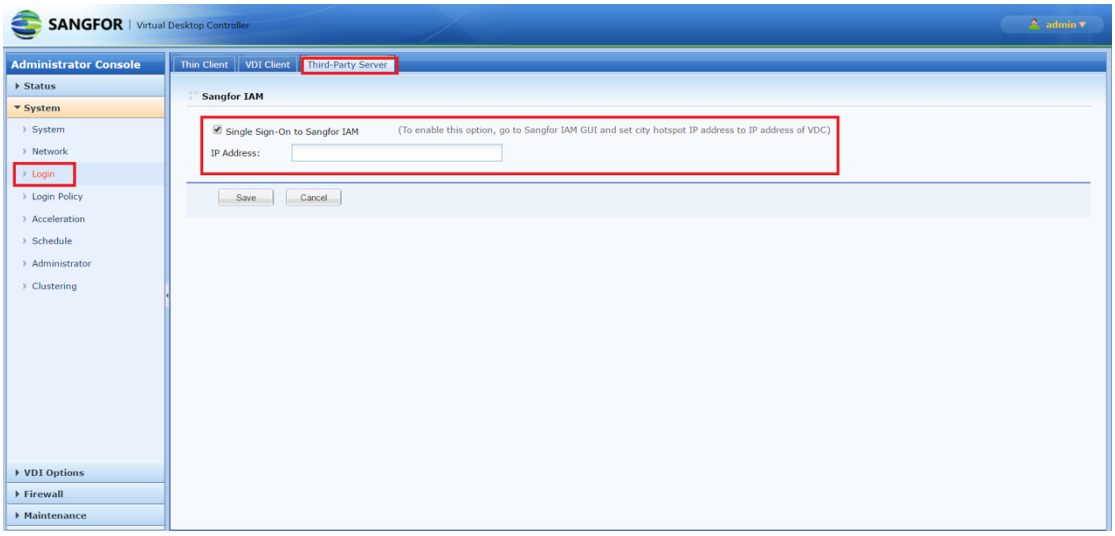
〖scenario〗

Combined with Sangfor IAM , user will login automatically to IAM device after the virtual machine's startup for auditing user's behavior. The virtual machine's IP

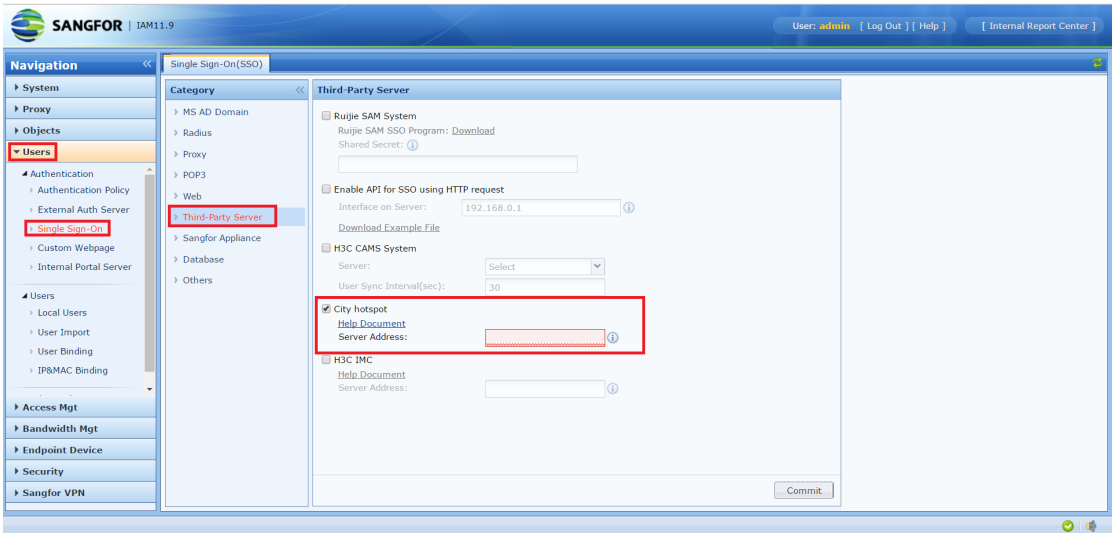
will be mapped to VDI username for your convenience

〖process〗

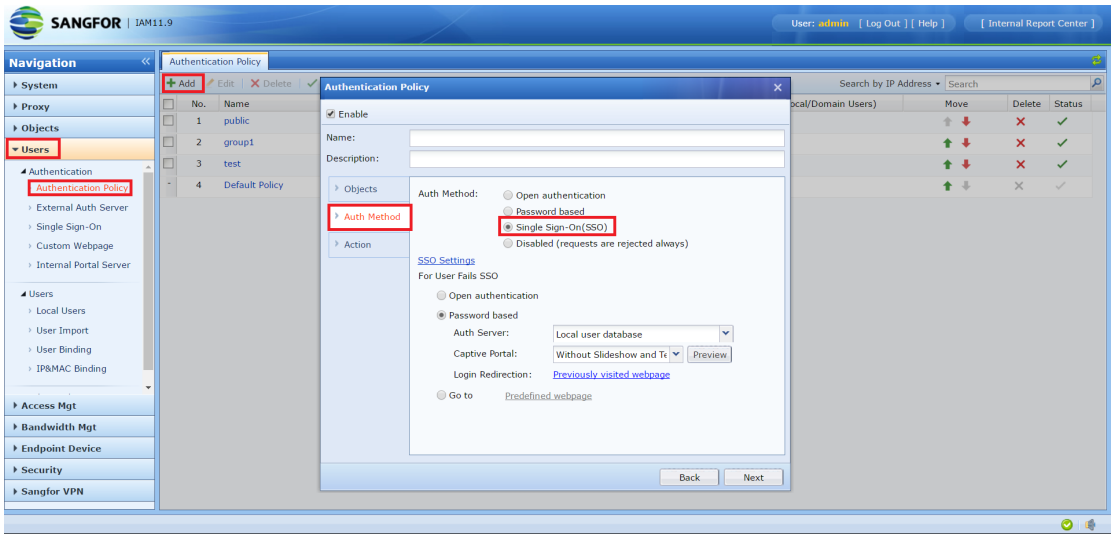
1. Enter【system】-【login】-【third-party server】，select“single sign-on to sangfor IAM”，and input IAM’s IP address



2. Login to IAM，enter【users】-【single sign-on】-【third-party server】，select“City Hotspot”and fill in the VDC’s IP (192.168.200.110 in this test) for server address



3. Authentication method must be single sign-on



〖expected result〗

Pass IAM authentication and VDI user is visible in IAM

3.7 Recovery

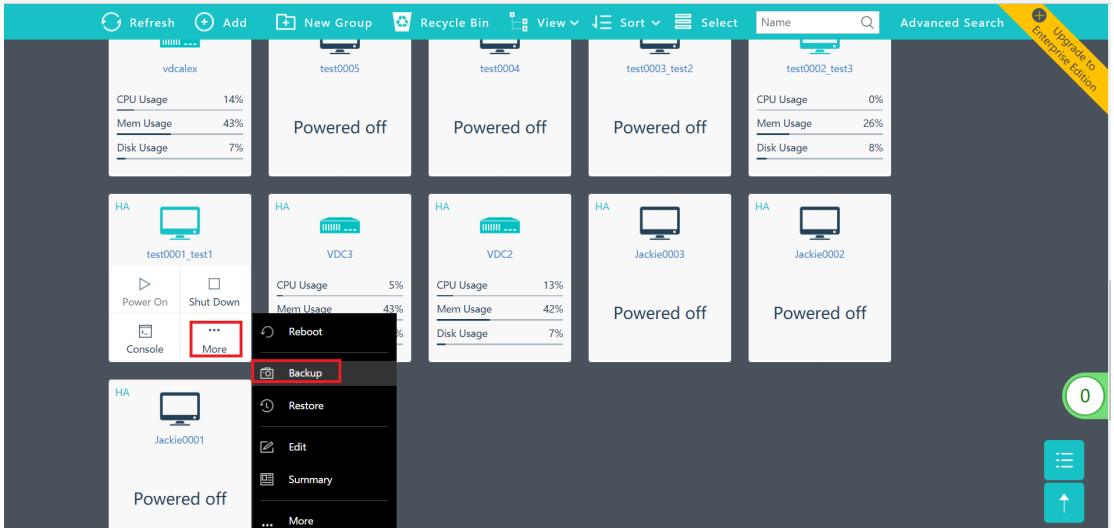
3.7.1 Create snapshot

〖scenario〗

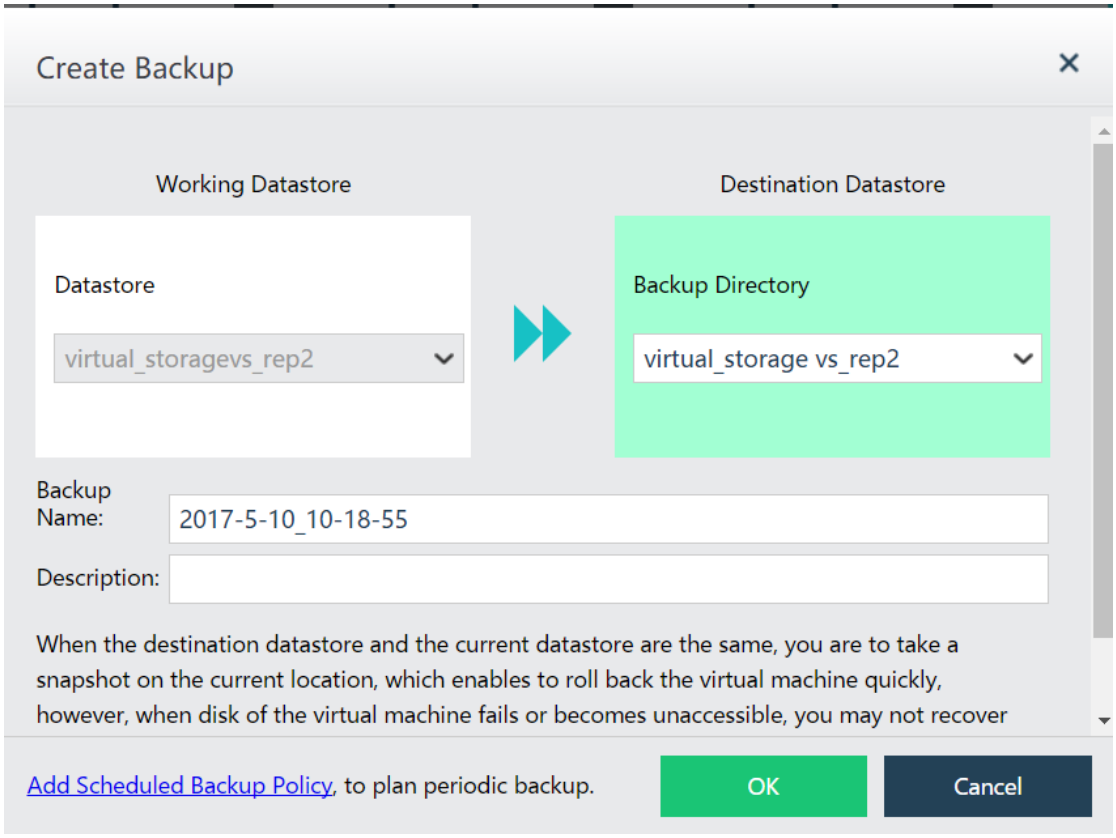
When you are going to execute important operation in virtual machine like putting a patch and installing software which could damage the virtual machine. You can create snapshot to enable quick recovery if problem occurs. After the operation，virtual machine's status will be stored.

〖process〗

1. Login VMP console
2. Click【computing】
3. Mouse stays in a virtual machine for seconds. Click【more】-【backup】



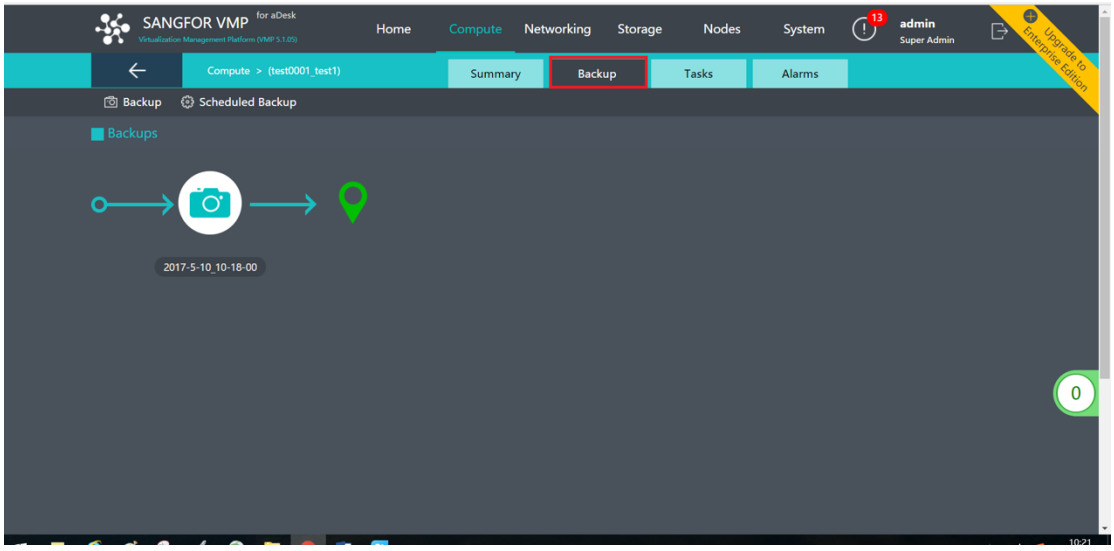
4. Select the same storage place as original copy



5. Click the virtual machine，【more】-【summary】-【backup】

〖expected result〗

The snapshot is visible



3.7.2 Recovery of snapshot

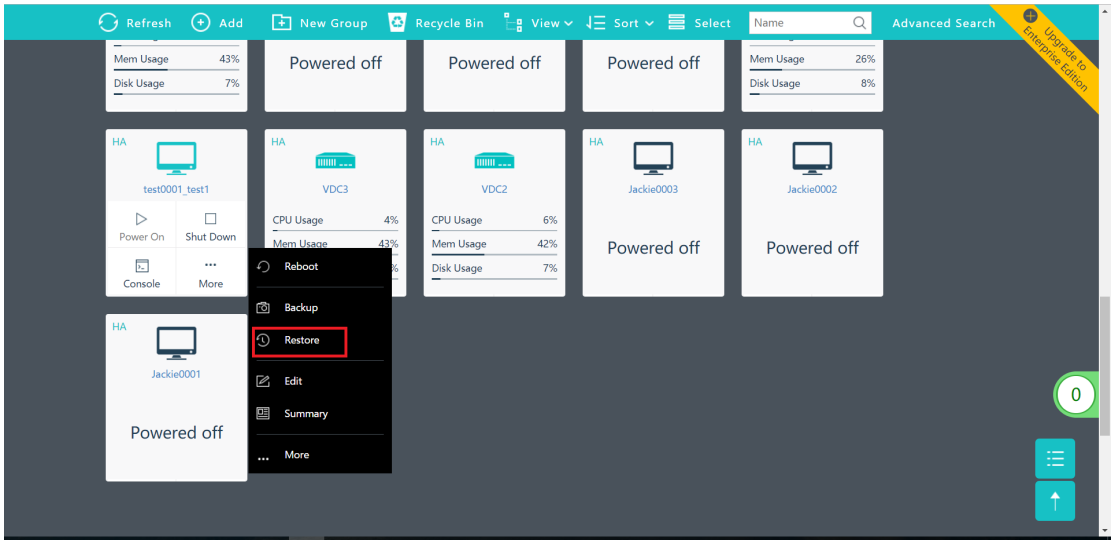
〖scenario〗

When you are going to execute important operation in virtual machine like putting a patch and installing software which could damage the virtual machine. You can create snapshot to enable quick recovery if problem occurs. After the operation，virtual machine's status will be stored.

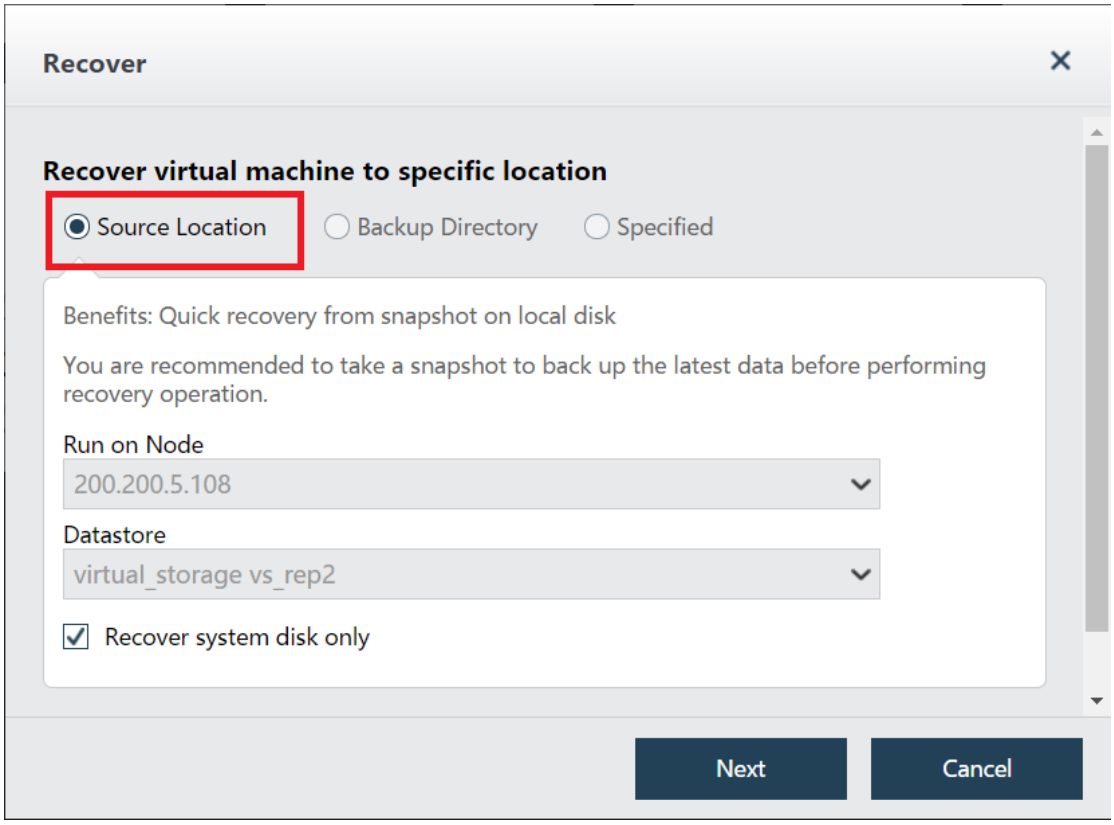
〖process〗

1. Select the virtual machine has been snapshot and make some change in the virtual machine like installing a software

2. Mouse stay in the virtual machine for seconds，click【more】-【restore】



3. We restore to source location as example



〖expected result〗

The virtual machine has been restored to previous status

3.7.3 Creation of backup

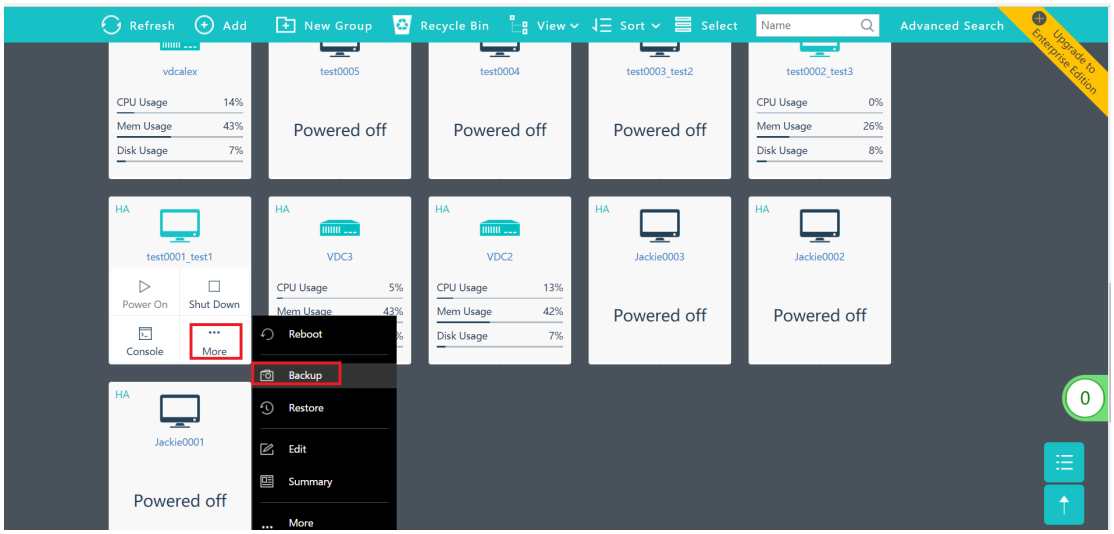
〖scenario〗

Sangfor Technologies Co., Ltd.
Block A1, Nanshan iPark No.1001 Xueyuan Road
Nanshan District, Shenzhen, Guangdong Province
P. R. China (518055)

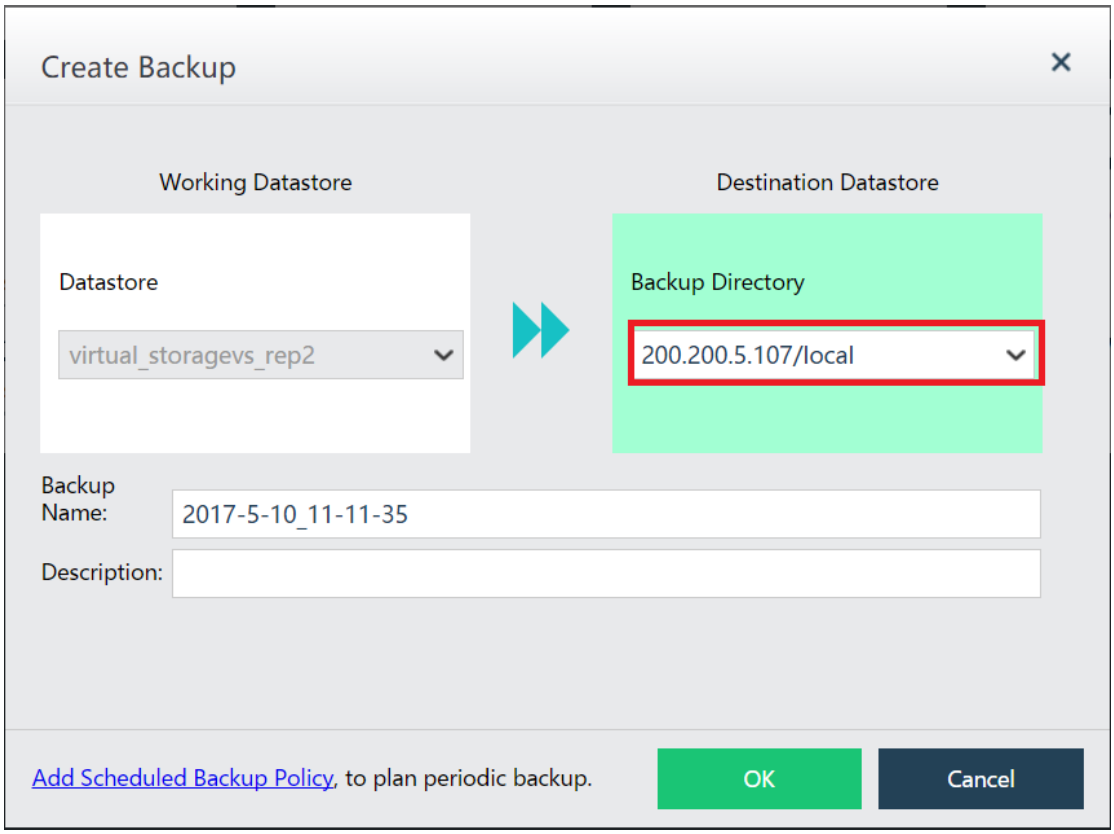
User can create backup for virtual machine in case of the storage damage，server breakdown or other physical failure. The backup will be stored in non-local storage and can be restored quickly by rebuilt VMP platform

〖process〗

1. Login VMP console
2. Click【computing】
3. Mouse stays in a virtual machine for seconds. Click【more】-【backup】



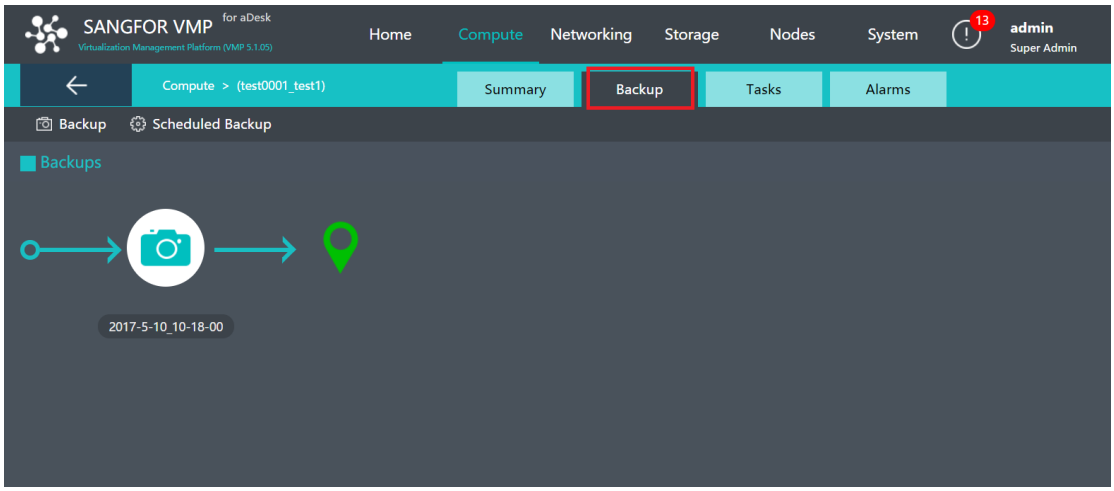
4. Select a different storage place with the original one



5. Click the virtual machine，【more】-【summary】-【backup】

〖expected result〗

The backup is visible



3.7.4 Recovery of backup

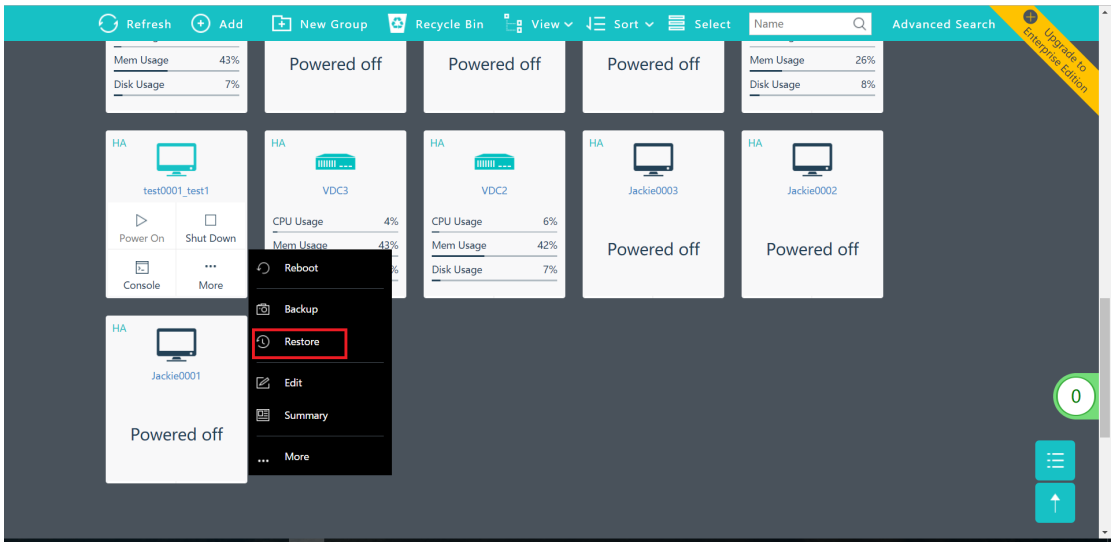
〖scenario〗

Sangfor Technologies Co., Ltd.
Block A1, Nanshan iPark No.1001 Xueyuan Road
Nanshan District, Shenzhen, Guangdong Province
P. R. China (518055)

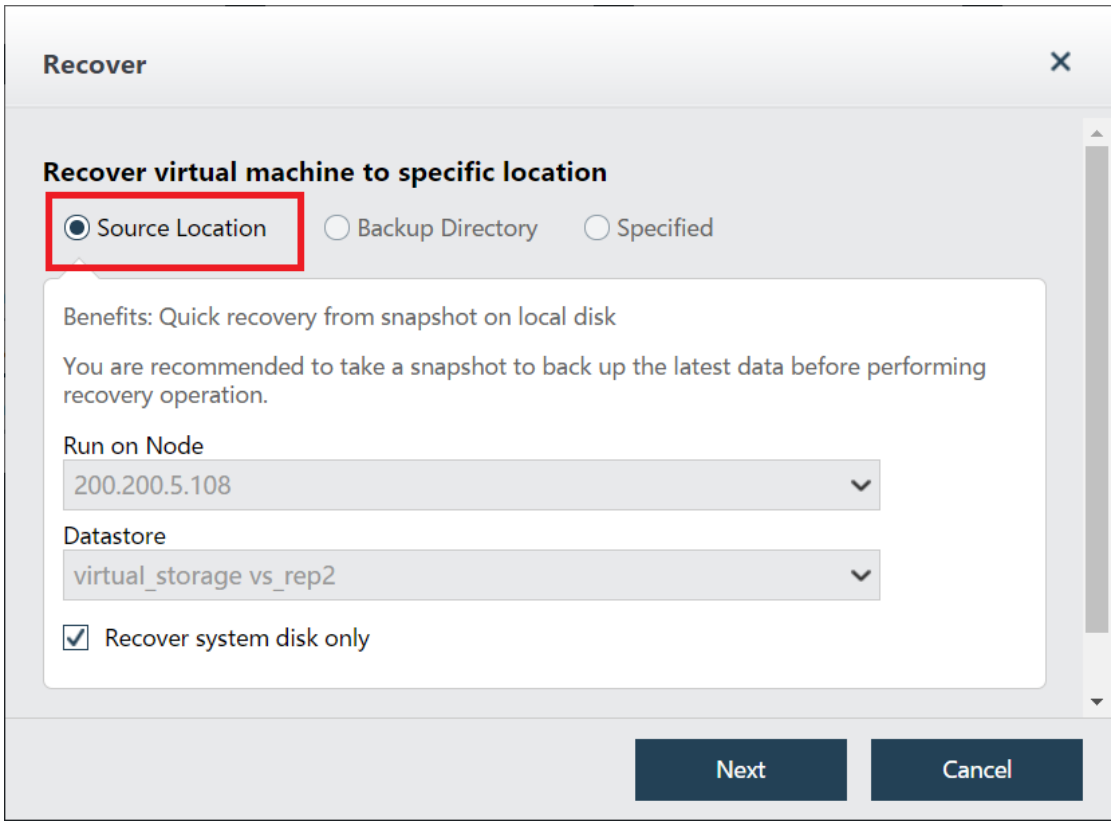
User can create backup for virtual machine in case of the storage damage，server breakdown or other physical failure. The backup will be stored in non-local storage and can be restored quickly by rebuilt VMP platform

〖process〗

1. Select the virtual machine has been snapshot and make some change in the virtual machine like installing a software
2. Mouse stay in the virtual machine for seconds，click【more】-【restore】



3. Restore to source location as example



〖expected result〗

The virtual machine has been restored to previous status

〖tips〗

The storage place for backup should differ from the original place. If external storage is not available，user can only execute snapshot

3.7.5 Auto backup

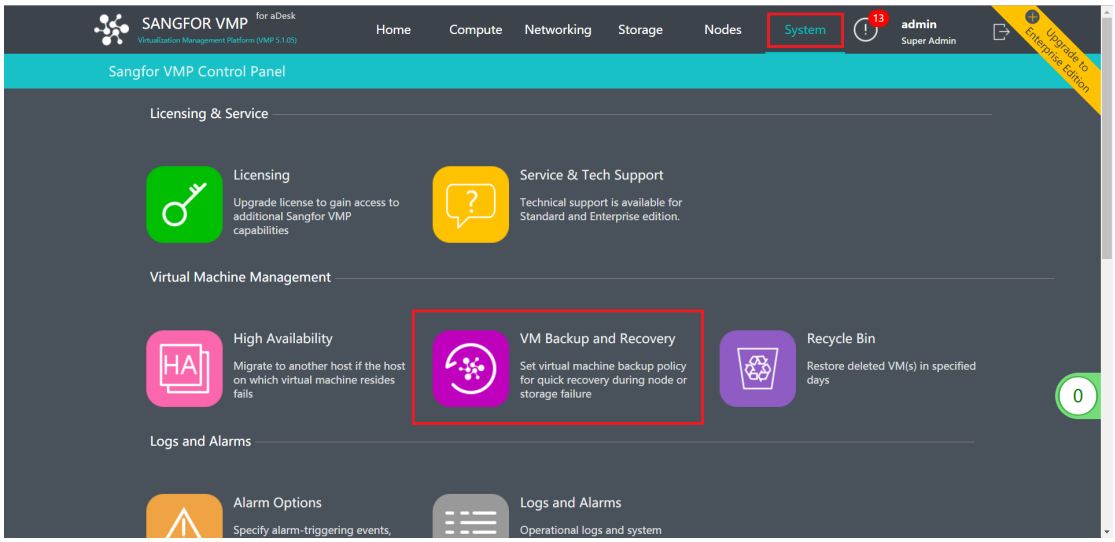
〖scenario〗

Customizing backup time and strategy for virtual machine

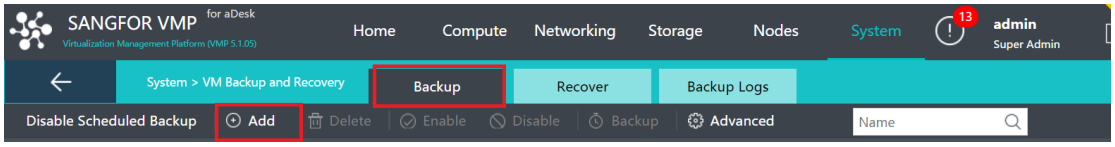
〖process〗

1. Login VMP console

2. click【system】-【VM backup and recovery】



3. Click【backup】-【add】



4. Edit the following content：

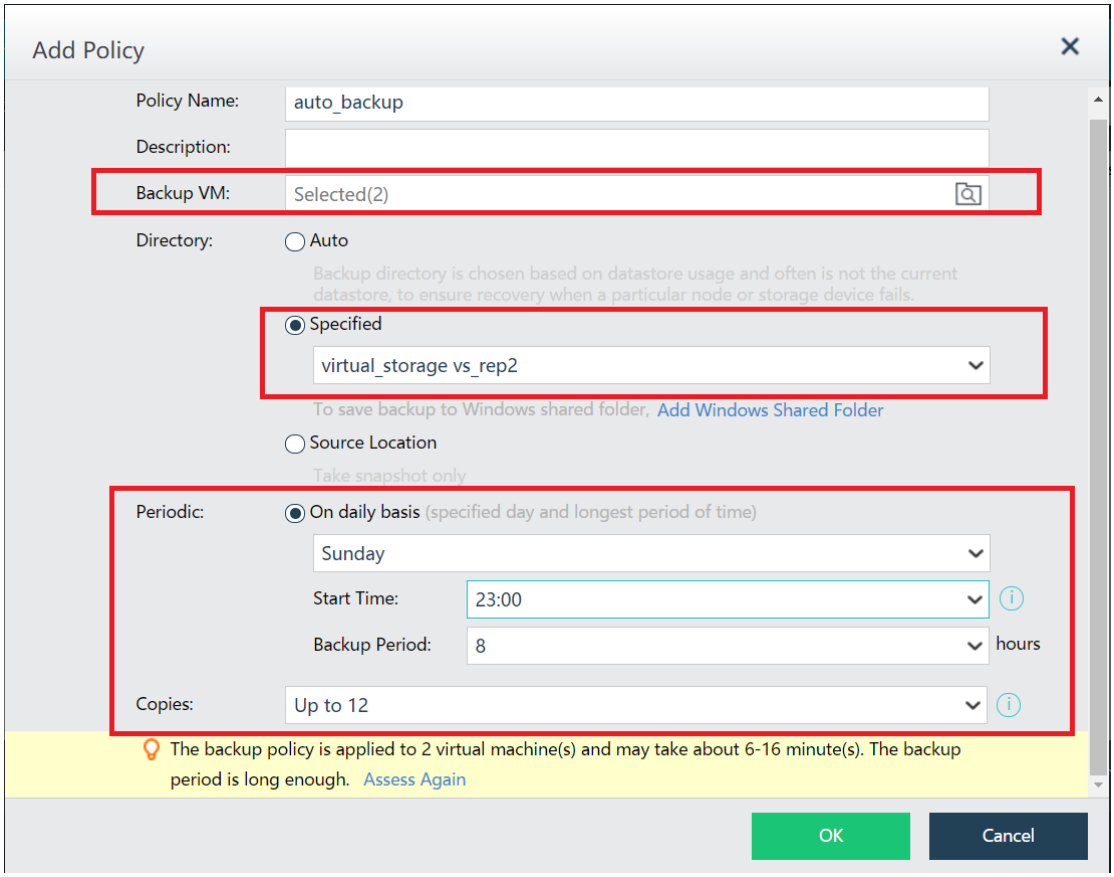
（1）policy name “auto_backup”

（2）backup VM：test1

（3）directory：virtual storage vs rep2

（4）periodic：5 minutes later than present date and time

（5）copies：12



〖expected result〗

5 minutes later the backup is visible in【more】-【summary】-【backup】

〖tips〗

The snapshot will be generated in the test，because there is no external storage.

3.8 HA

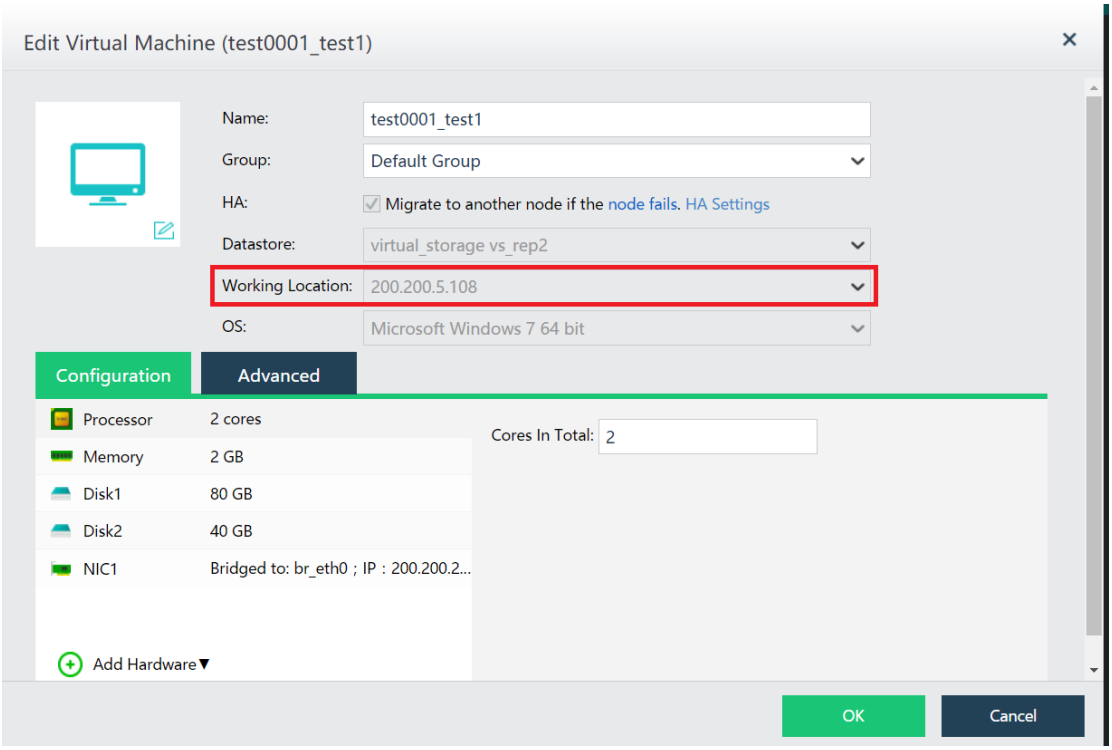
3.8.1 HA function

〖scenario〗

Auto migration of virtual machines on one or several failed nodes (breakdown, electrical failure etc.) to other node ensures business continuity.

〖process〗

1. Login VMP console，select a virtual machine，click “more” - “edit”，to check the running place



2. Pull out all network cables of the virtual machine or pull out all disks

〖expected result〗

aDesk’s connection with VDI break up and constant reconnection occurs. After the automatic migration done，the virtual machines influenced restart and the virtual desktop is accessible

〖tips〗

1. Shared storage （virtual storage or external storage）is required to test HA function

2. If there is no enough resource（CPU、memory、disk）in the node which you are migrating virtual machine to，the virtual machine can not startup after the migration

Sangfor Technologies Co., Ltd.
Block A1, Nanshan iPark No.1001 Xueyuan Road
Nanshan District, Shenzhen, Guangdong Province
P. R. China (518055)

SANGFOR
www.sangfor.com