1 Hot Standby

Hot standby is a solution for servers, in which the active server and the standby server are connected through TCP/IP, and data is replicated through the hot standby software. Under normal conditions, the active server is active, and the standby server monitors the active server. Once the standby server detects an anomaly on the active server, the standby server will immediately take over as the active server to ensure that the system can provide long-term and reliable services.

The hot standby works with a virtual IP address (VIP) to receive requests from the client and then send the requests to one of the servers to respond.

2 Configurations Preparation

2.1 Configurations Checklist

Check Item	Expected Results	Procedure	Exception Handling
Server Configurations Preparation			
1. Operating system	☐ **The operating systems of the two servers are of the same version.**	Press Windows + R to open **CMD**, and then enter **winver** to check the operating system version. The operating systems of the two servers must be of the same version (including the minor version number) Click to view the example..	If the operating system versions are inconsistent, reinstall one of the two operating systems or replace one of the two servers.
2. Host name	☐ **The host names of two servers are inconsistent.**	Press Windows + R to open **CMD**, and enter **hostname** to check the host name. The host name is one of the most important indicators to distinguish between the two servers in hot standby mode. The host names of the two servers cannot be the same. Click to view the example.	If the host names of the two servers are the same, press Windows + R to open **CMD** and → enter "sysdm.cpl" →change the host name.
3. Network adapter	☐ **At least two physical network adapters are enabled on each server, and the Npcap Loopback Adapter must be disabled.**	Go to **Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings**. Check the number of network adapters and make sure that NIC1 and NIC2 are enabled. Disable the Npcap Loopback Adapter. At least two physical network adapters are enabled on each server. The Npcap Loopback Adapter must be disabled on both servers because it will affect database decryption. Click to view the example.	If any of the specified network adapters haven't been enabled, right-click to select **Enable**. If there is a Npcap Loopback Adapter enabled, right-click to select **Disable**.
4. IP	☐ **Three unused IP addresses on the same network segment are available.**	Provide three unused IP addresses on the same network segment as the service IP of the active server, service IP of the standby server, and virtual IP (VIP)	If ping fails, check the network and firewall rules. In **Control Panel > System and Security > Windows**

		separately. Click to view the example.	**Firewall > Advanced Settings > Inbound Rules**, check if "File and Printer Sharing (Echo Request - ICMPv4-In)" is enabled. In addition, if the Internet uses IPv6, check if "File and Printer Sharing (Echo Request - ICMPv6-In)" is enabled. If the inbound rules of the two servers are disabled, select the **Inbound Rules** and right-click **Enable Rules**.
	☐ **The IP addresses are configured for the network adapters of the two servers.**	For the two servers, configure the first network adapter IP address as the service IP address and the other as the heartbeat IP address. Connect the first network port to a router or switch with a network cable, and connect the second with a network cable to make a heartbeat cable. **The heartbeat IP addresses of the two servers must be on the same network segment, and the service IP address and heartbeat IP address of a server cannot be on the same network segment.** Click to view the example.	
	☐ **Verify whether the configured IP addresses are accessible.**	Select a server to be the active server, ping the service IP address and heartbeat IP address of the standby server from the active server, and ping the service IP address and heartbeat IP address of the active server from the standby server. Both servers can be pinged no matter whether their firewalls are enabled or not. Click to view the example.	
5. Port	☐ **TCP 7320/7330 and UDP 3000/7340/7350 cannot be occupied.**	Press Windows + R to open **CMD**, and then enter "netstat -ano|findstr Required port number" to check the port has been occupied. TCP 7320/7330 and UDP 3000/7340/7350 are all the service communication ports of Rose software. Click to view the example.	If any port is being used by other programs, end the process that is occupying the port or deny access to the hot standby.
6. Time zone	☑ **Two servers are in the same time zone.**	To ensure that platform services are executed at the right time, the time zones of the active and standby servers must be consistent. Manually calibrate the time zone of the servers. Click to view the example.	Change the time zones of the active and standby servers to the same. Calibrate the time of the active server according to the time zone.
Software Configurations Preparation			
7. DSS service	☐ **Two servers install DSS Pro of the same version.**	The installation path of DSS on both servers should be consistent. If business plugins need to be installed, they should be installed on both servers. Otherwise, it	If the DSS installation paths of the two servers are inconsistent, or a wrong network adapter is selected,

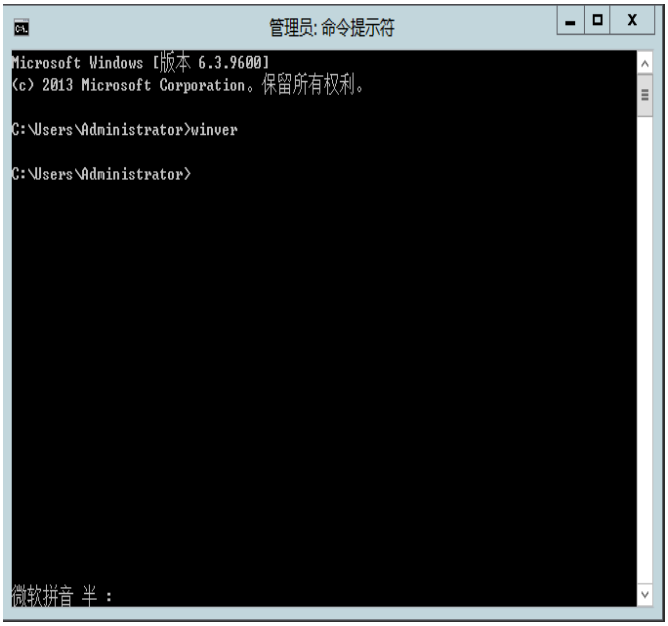
		will affect file and data synchronization. When selecting the network card, choose the one where the business IP is located. Start DSS after installation.	uninstall and reinstall the DSS.
8. Hot standby software	☐ **Two servers install ReplicatorPlus_ V2.0.exe of the same version.**	Follow the Installation instructions to complete the installation. The installation paths of the active and standby servers must be the same. The hot standby software cannot be overwritten. If a hot standby software has been installed, manually uninstall the earlier version before reinstalling the new one. Click to view the example.	After uninstalling the software, make sure all residual files in the software installation directory are removed. If there are residual files unable be cleared, reboot the server and manually delete the folder.
9. Hot standby service	☐ **HAService.exe, Replicator.exe, and SMonitor.exe processes are started smoothly.**	Open the **Task Manager** of the active and standby servers to check if the three processes (HAService.exe, Replicator.exe, and SMonitor.exe) are started smoothly. Click to view the example.	In **Task Manager > Services > Open Service** or in **CMD**, enter **services.msc** to open the service interface, and manually enable DSSMonitor service. If it fails, uninstall and reinstall the Rose software.
10. Allowlist in anti-virus software	☐ **Check the allows in the anti-virus software.**	If an anti-virus software is installed on the server, add the installation path of Rose to its software.	

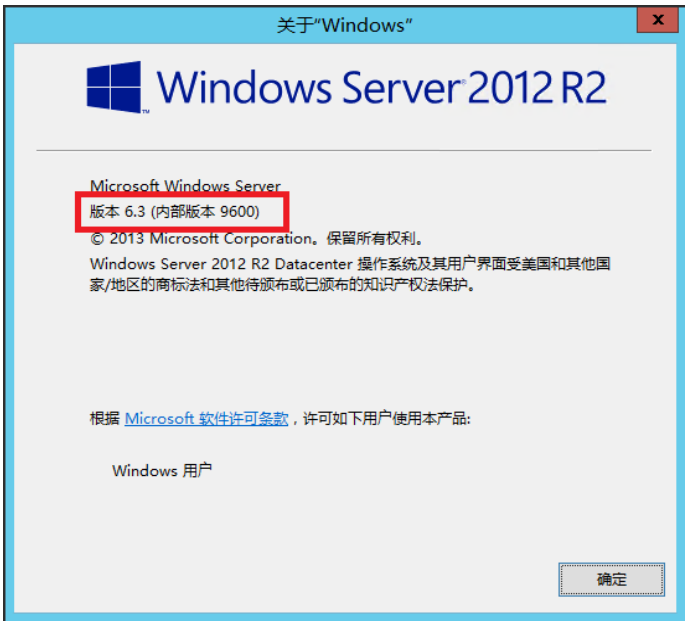
If all the above 9 check items are passed, skip the Examples of Configurations Preparation and directly go to the Deploying Hot Standby.

2.2 Examples of Configurations Preparation

2.2.1 Preparing Two Servers of the Same Operating System Version

Press Windows + R to open **CMD**, and then enter **Winver** to check the operating system version, as shown below. The operating systems of the two servers must be of the same version (including the minor version number).



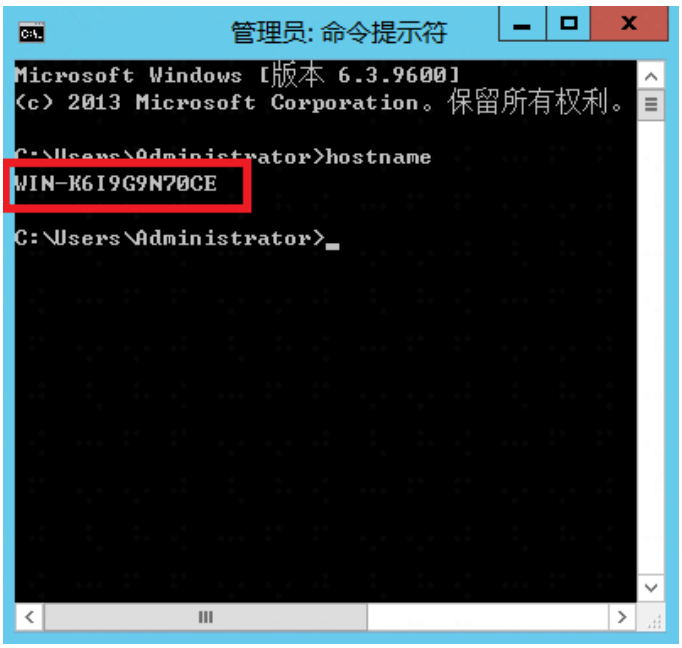


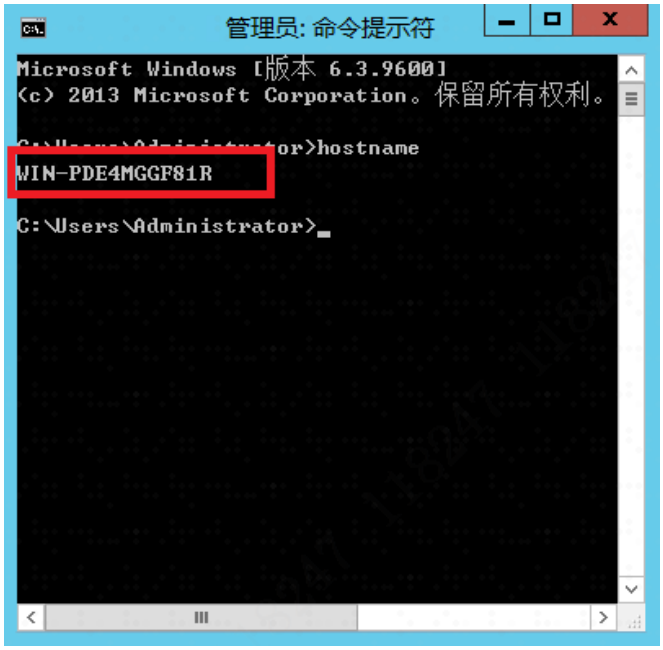
Notes: The hot standby software supports virtualized environments, but you cannot change devices at will because the license and environment information are bound. In addition, differences between public cloud platforms exist. Some public cloud platforms cannot switch IP addresses and need to configure load balancing or other things to enable platform access after switching the IP address.

Back to Checklist.

2.2.2 Ensuring That the Host Names of the Two Servers Are Inconsistent

Press Windows + R to open **CMD**, and then enter **hostname** to check the host name, as shown below. The host name is one of the most important indicators to distinguish between the two servers in hot standby. The host names of the two servers cannot be the same.

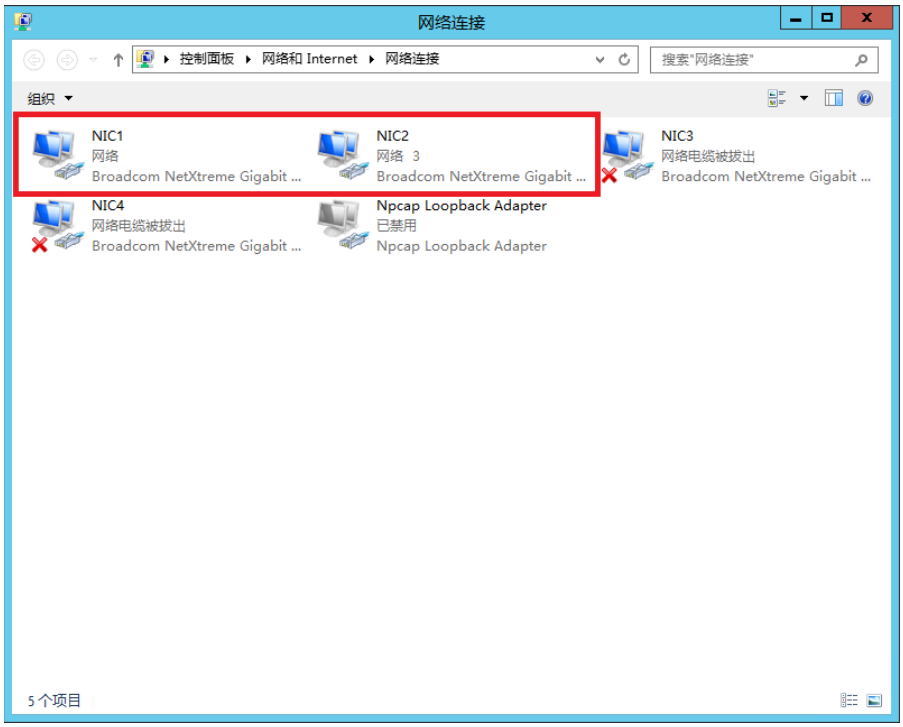




Back to Checklist.

2.2.3 Ensuring That at Least Two Physical Network Adapters Are Enabled on Each Server.

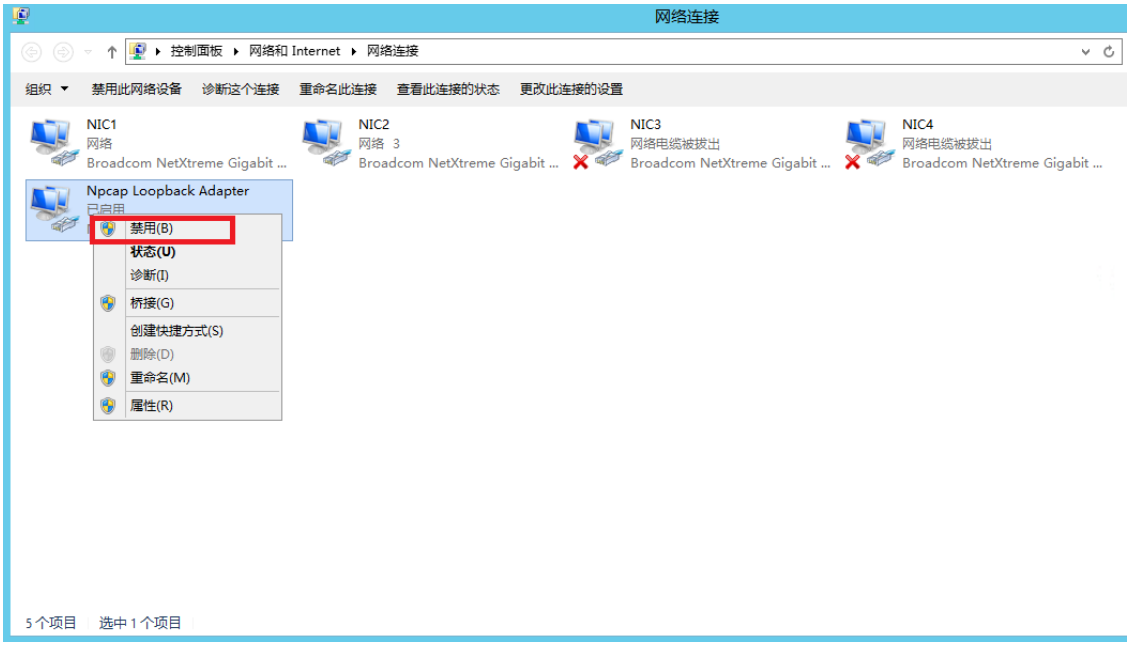
Go to **Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings**. Check the number of network adapters and make sure that NIC1 and NIC2 are enabled.



Back to Checklist.

2.2.4 Disabling Npcap Loopback Adapter

The Npcap Loopback Adapter must be disabled on both servers because it will affect database decryption. Go to **Control Panel > Network and Internet > Network Connections**, as shown below. If there is a Npcap Loopback Adapter enabled, right-click to select **Disable**.



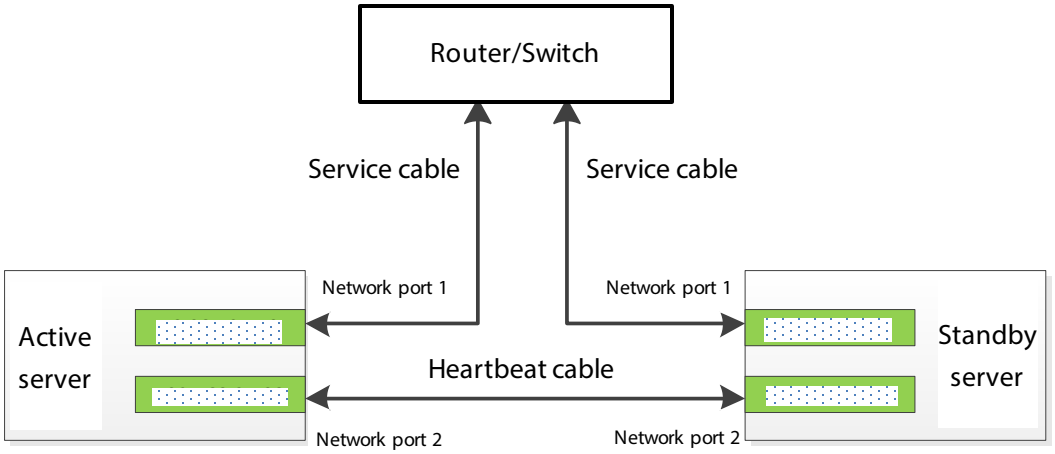
2.2.5 Providing Three Unused IP Addresses

Before configuring the hot standby, you need to provide three unused IP addresses on the same network segment as the service IP address of the active server, service IP address of the standby server, and virtual IP address (VIP), separately.

Back to Checklist.

2.2.6 Configuring IP Addresses of Two Servers

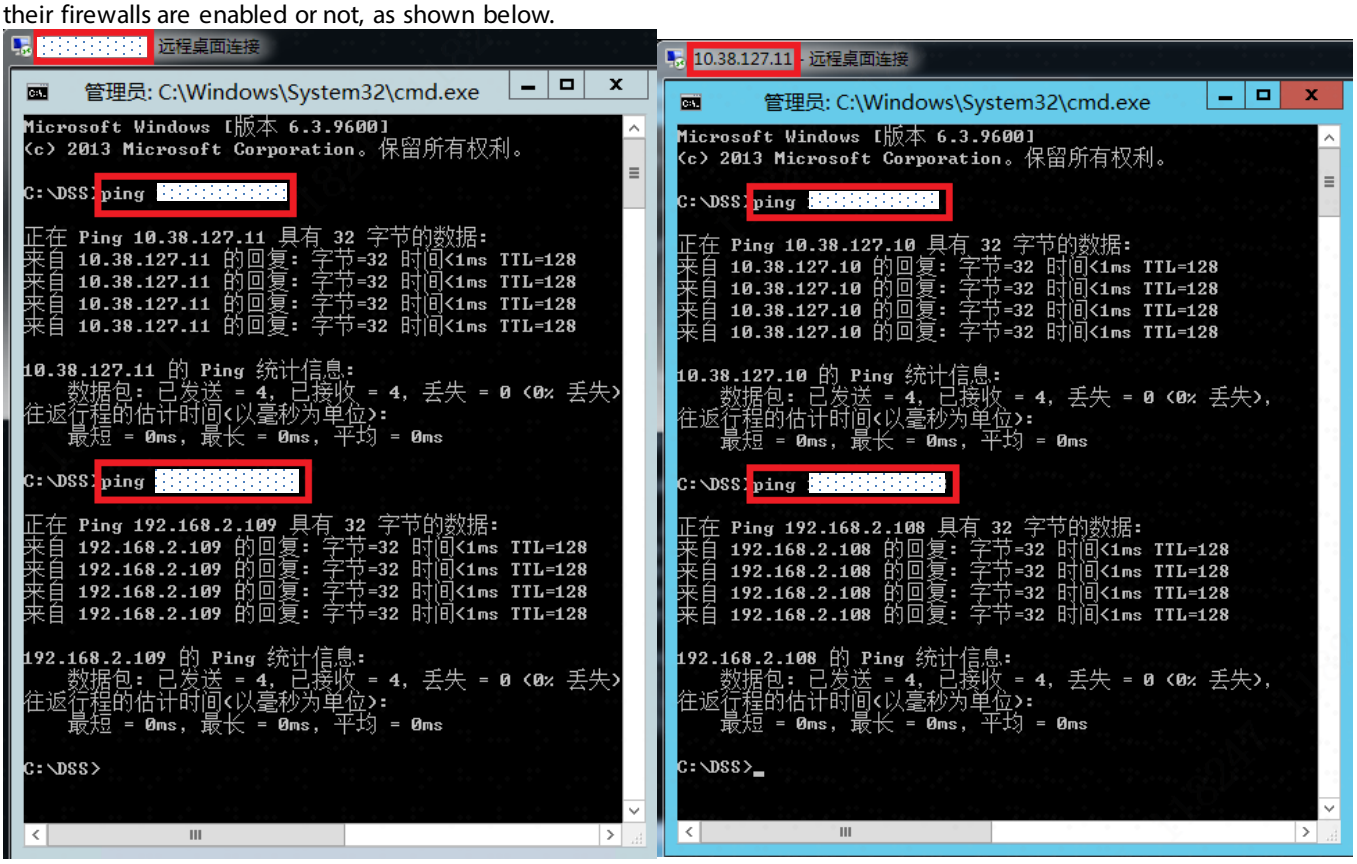
For the two servers, configure the first network adapter IP address as the service IP address and the other as the heartbeat IP address. **The service IP address and heartbeat IP address of a server cannot be on the same network segment. The service IP addresses of the active and standby servers must be on the same network segment, and the heartbeat IP addresses of the two servers also must be on the same network segment. Connect the first network port to a router or switch with a network cable, and connect the second port with a network cable to make a heartbeat cable.** Here gives an example of connections and IP addresses (for reference only).



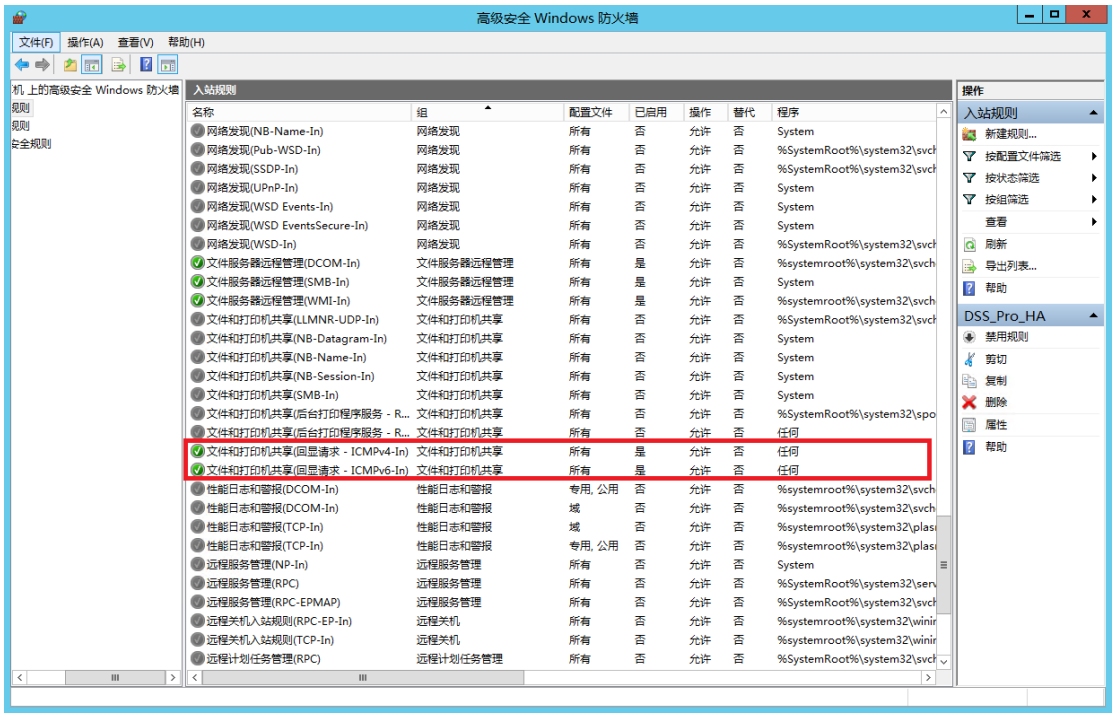
Back to Checklist.

Checking IP Communication Between Active and Standby Servers

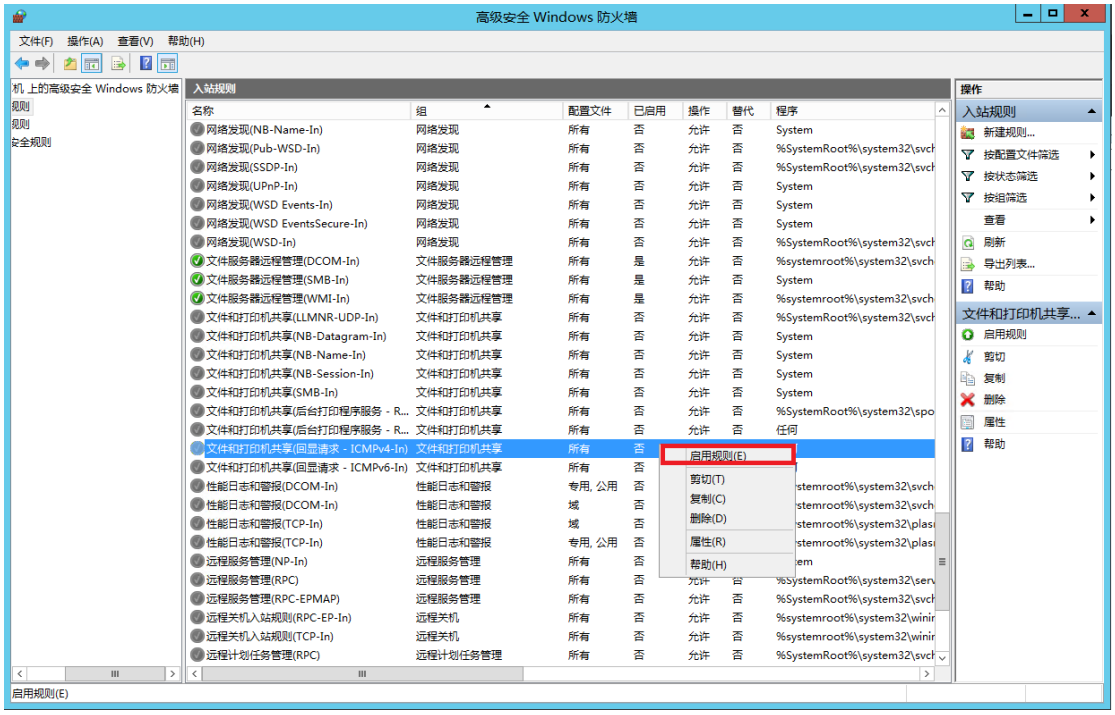
Ping the service IP address and heartbeat IP address of the standby server from the active server, and ping the service IP address and heartbeat IP address of the active server from the standby server. Both servers can be pinged no matter whether their firewalls are enabled or not, as shown below.



If ping fails, check the network and firewall rules. In **Control Panel > System and Security > Windows Firewall > Advanced Settings > Inbound Rules**, check if "File and Printer Sharing (Echo Request - ICMPv4-In)" is enabled. In addition, if the Internet uses IPv6, check if "File and Printer Sharing (Echo Request - ICMPv6-In)" is enabled. The following figure indicates that both rules are enabled.



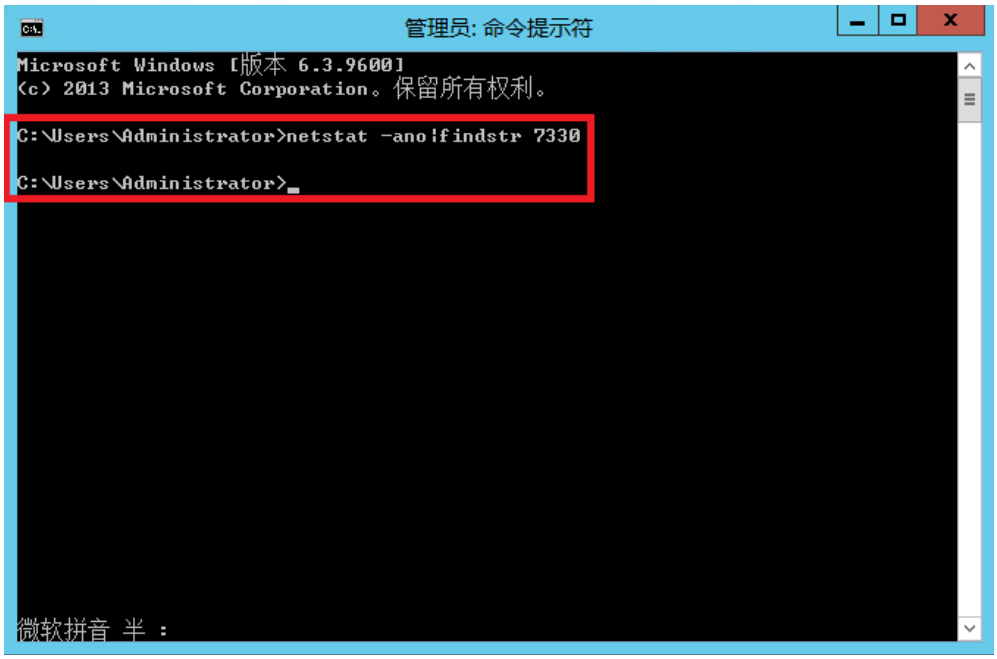
If the inbound rules of the two servers are disabled, select **Inbound Rules** and right-click **Enable Rules**, as shown below.



Back to Checklist.

2.2.7 Checking if Any Port of Hot Standby Software Is Occupied

TCP 7320/7330 and UDP 3000/7340/7350 are all the ports used by the hot standby software for communication. To test if the ports are occupied, open **CMD** and enter "netstat –anp|findstr Required port number". If any port is being used by other programs, end the process that is occupying the port or deny access to the hot standby.



Back to Checklist.

2.2.8 Ensuring Active and Standby Servers Are in the Same Time Zone

Check if the time zone and time of the active server are corresponding. For example, the current standard time in GMT-8 is 12:00, but the time displayed on the server is 10:00. If such an error exists, you need to manually calibrate the time of the active server. When the active server is brought in or switched to the standby server, the time will be synchronized, but the time zone will not be synchronized. **To ensure that platform services are executed at the right time, the time zones of the active and standby servers must be consistent.**

Back to Checklist.

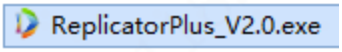
2.2.9 Ensuring That the DSS Product of the Same Version Is Installed and Deployed on the Two Servers

The DSS installation paths of two servers must be the same; otherwise, the data synchronization will be affected. Select the network adapter where the service IP address is located for the server. In other words, make sure that the server IP address is the service IP address instead of the heartbeat IP address, as shown below. Start DSS after installation. If the hot standby has not been configured, after the IP address is modified into VIP, the DSS service cannot be enabled, and it is normal.

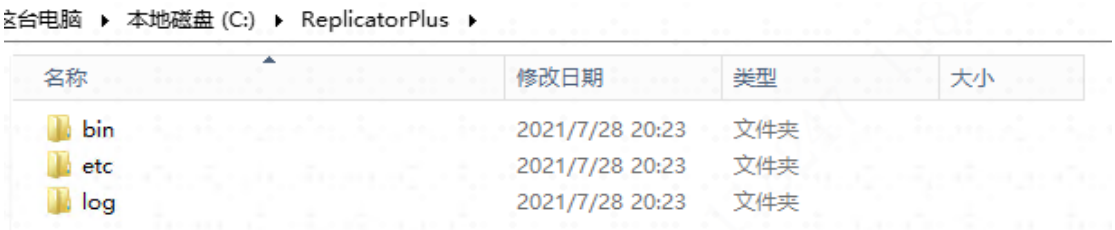
Back to Checklist.

2.2.10 Ensuring That Two Servers Install the Hot Standby Software of the Same Version

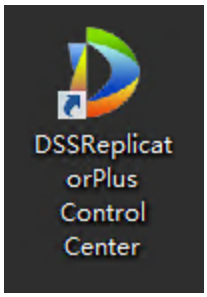
The name of the hot standby software of the new version is ReplicatorPlus_V2.0.exe, as shown below. Copy the hot standby software to the active and standby servers separately.



The hot standby software cannot be overwritten. If a hot standby software has been installed, manually uninstall the earlier version before reinstalling the new one. To update the installation package of the hot standby from Version 1.0 to Version 2.0, uninstall Version 1.0 before installing Version 2.0. The software cannot be overwritten. After uninstalling Version 1.0, there may be residues. You need to reboot the server and then delete the content of the ReplicatorPlus folder.



Double-click ReplicatorPlus_V2.0.exe, and follow the Installation instructions to install the hot standby software. The installation path of the hot standby software must be the same. After installation, a shortcut as below shall be shown on the desktop. The software must be executed on both servers.



Notes: After installing the software, change some firewall rules: Enable the following default ports and network communication permissions: TCP 7320/7330, UDP 7340, 7350 and heartbeat ports of private networks; ICMP: Enable the ICMP (ping) data packets of all network interfaces.

Back to Checklist.

2.2.11 Checking if Some Processes of the Hot Standby Software Are Started

Open the **Task Manager** of the active and standby servers to check if the three processes (HAService.exe, Replicator.exe, and SMonitor.exe) are started smoothly. If the processes are not started, manually enable DSSMonitor service in Service Management. If it fails, uninstall and reinstall the hot standby software.

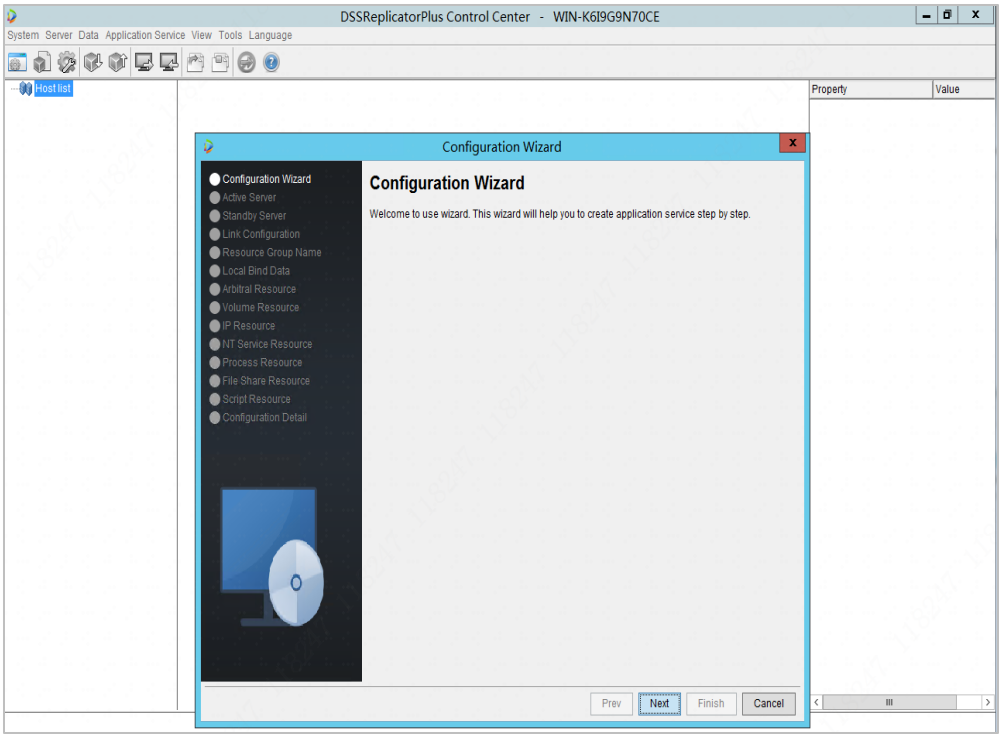
Back to Checklist.

3 Deploying Hot Standby

3.1 Configuring Hot Standby

Perform the operations on an active server that is configured with hot standby for the first time. The operations in this example are performed on an active server.

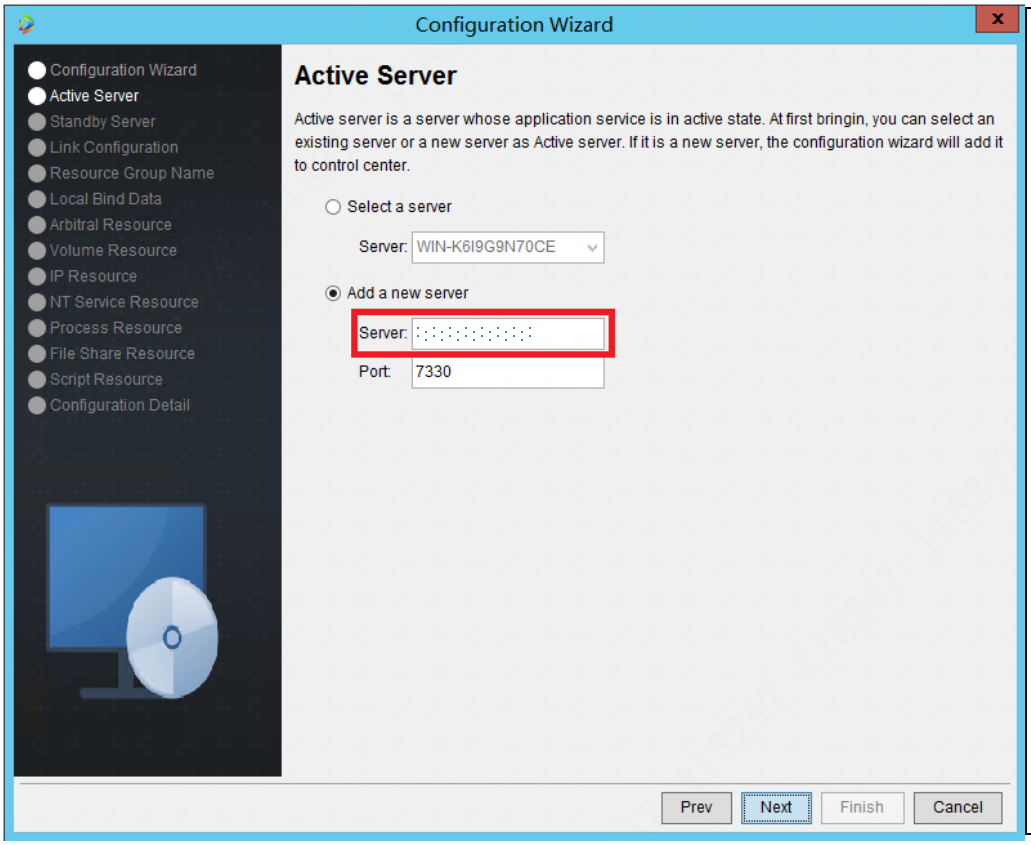
3.1.1 Configuration Wizard



When you open the software for the first time (double-click the shortcut icon DSSReplicatorPlus Control Center on the desktop), the "Configuration Wizard" will directly pop up. If the interface does not pop up, go to System > Wizard > Config Wizard. No configuration is required in this step.

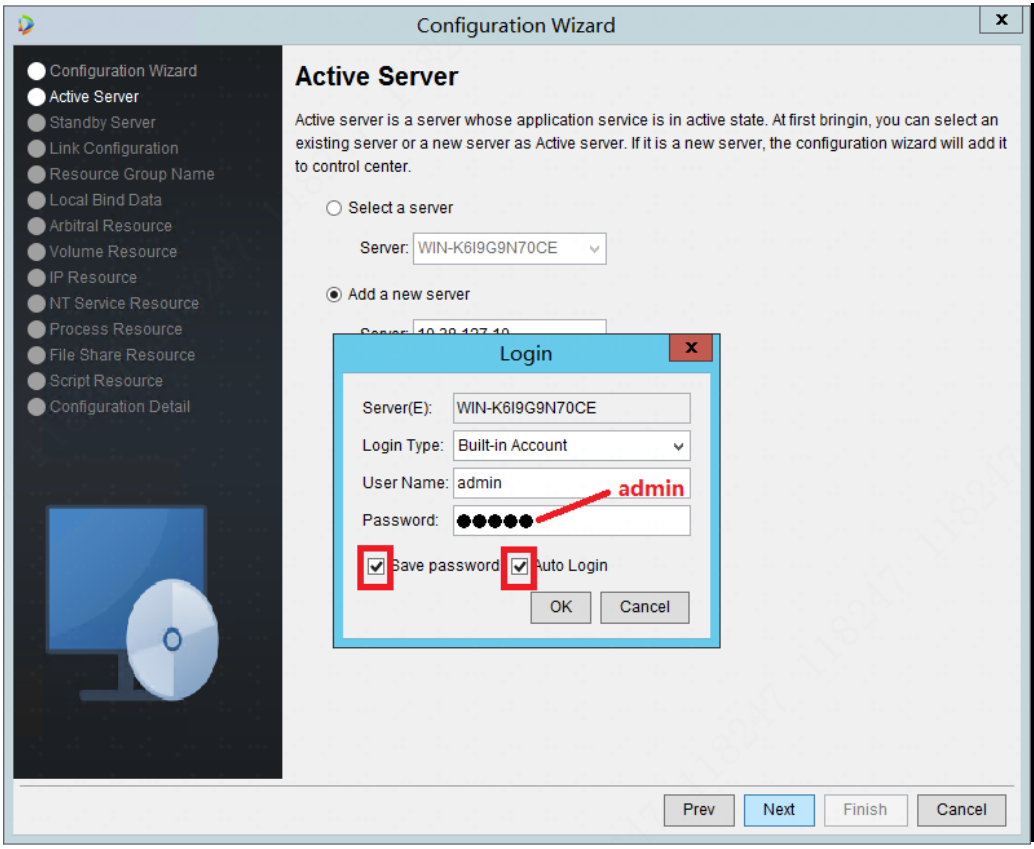
Click **Next** to go to **Active Server**.

3.1.2 Active Server



Select a server: If a server has been added, find the active server according to the host name, and then click **Next**.

Add a new server: For the initial configuration, "Add a new server" is selected by default. Configure "Server" as the IP address of the active server and "Port" as 7330. The settings are shown in the left figure.

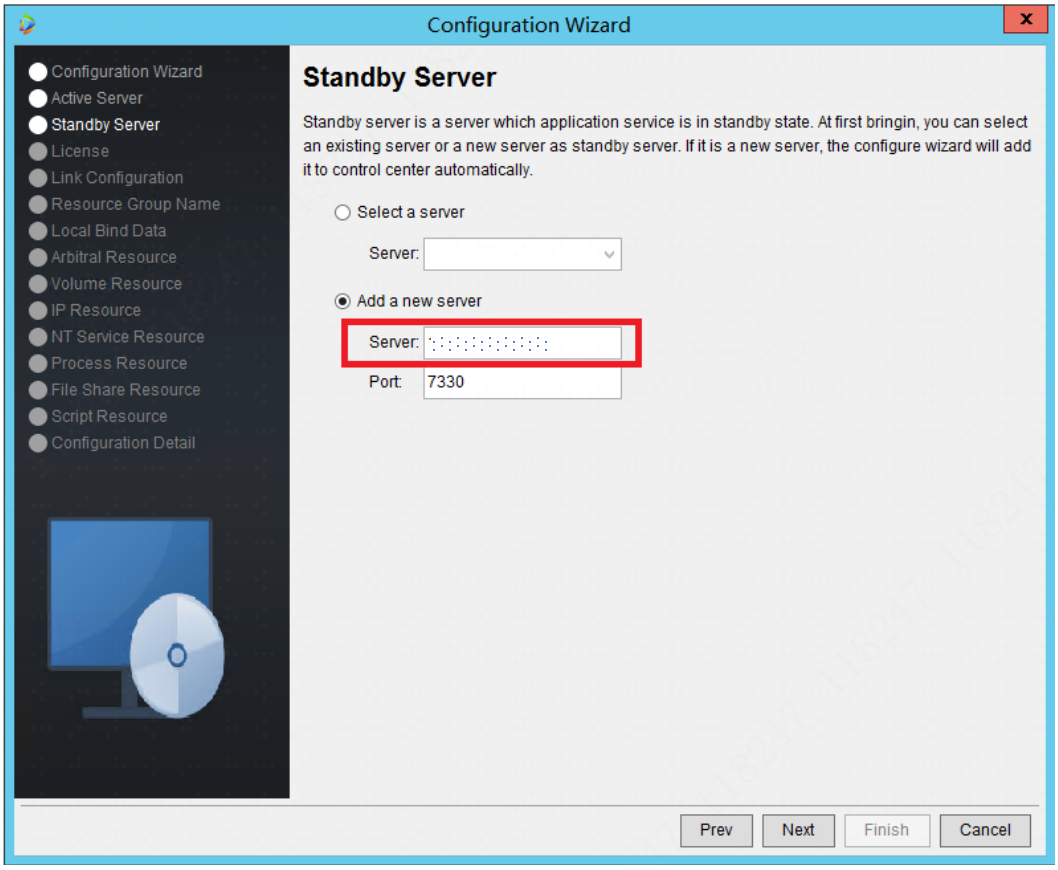


If the prompt "**Invalid server or no valid service on this server**" appears after you click **Next**, check if the TCP 7320/7330 and UDP 7340/7350 ports of the server in the IP address are occupied, and if DSSMonitor, DSSHAService, and DSSReplicator processes are launched.

If the settings are successful, click **Next** to go to **Login**. Use default settings. Configure "Password" as **admin**, select "Save password", and select "Auto Login". The settings are shown in the left figure.

Click **OK** to go to **Standby Server**.

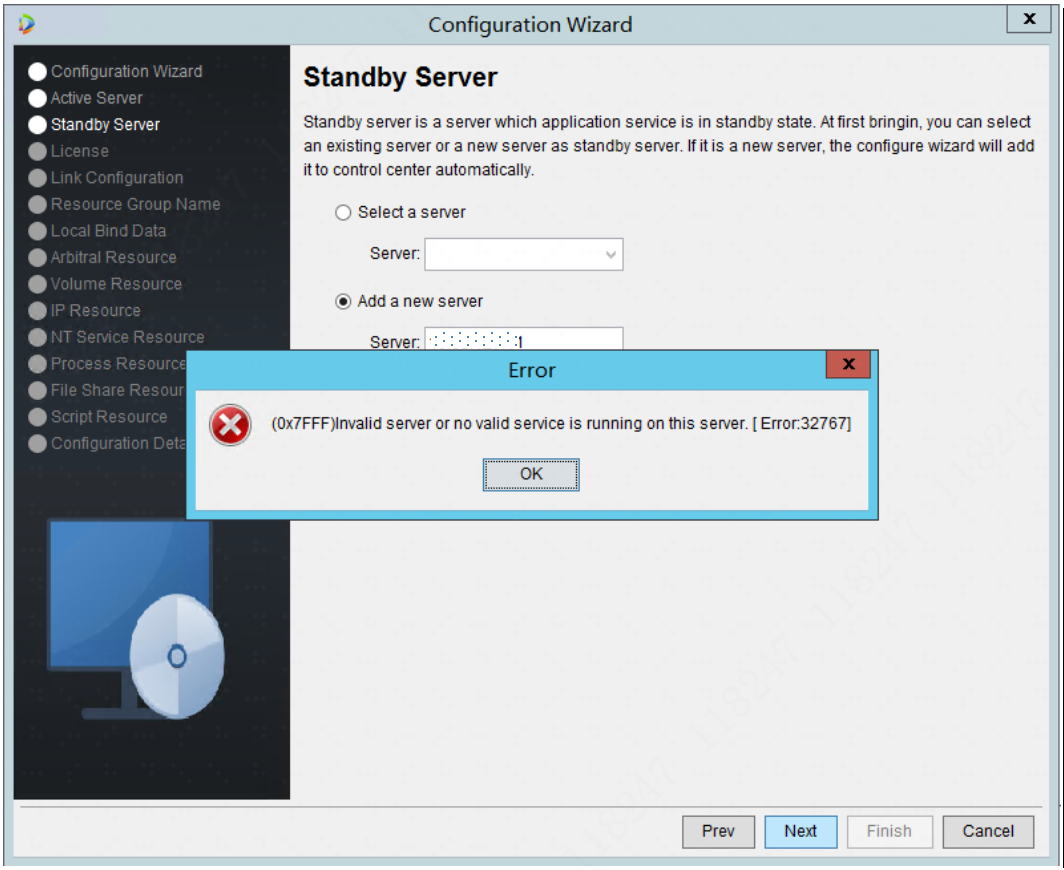
3.1.3 Standby Server



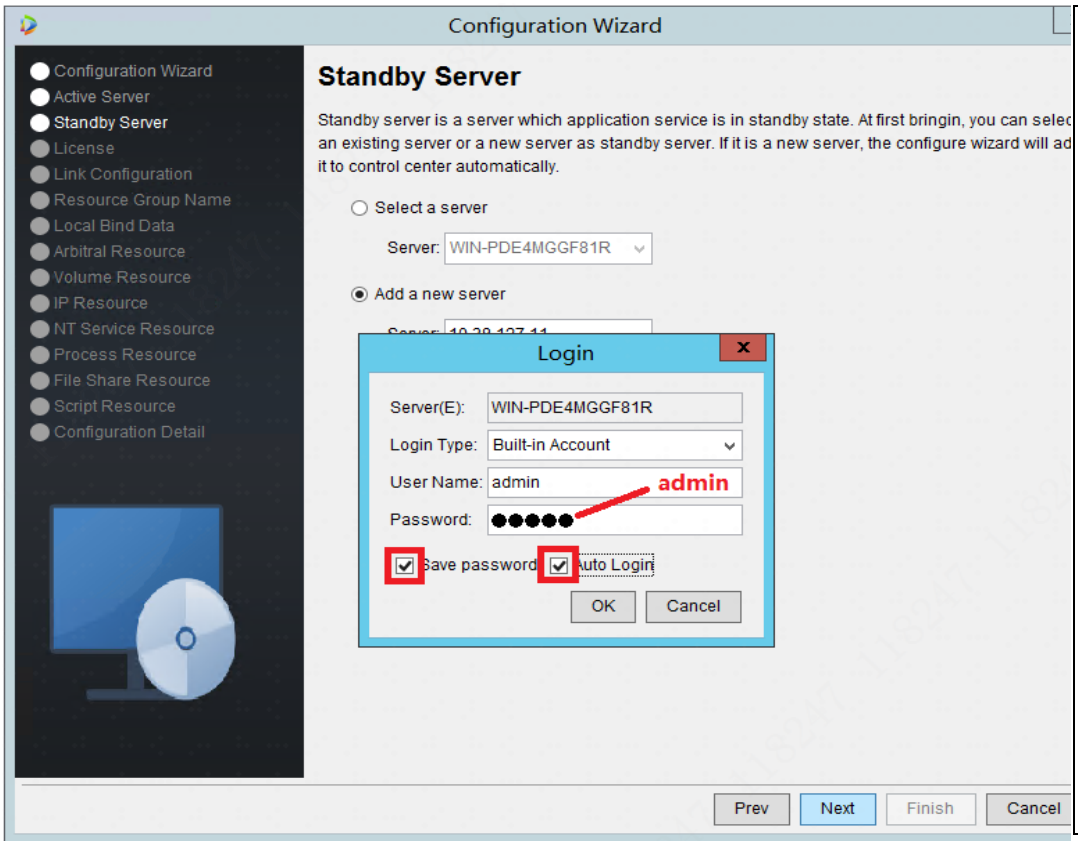
Select a server: If a service has been added, find the standby server according to the host name, and then click **Next**.

Add a new server: For the initial configuration, "Add a new server" is selected by default. Configure "Server" as the IP address of the active server and "Port" as 7330. The settings are shown below.

Click **Next** to go to **Login**, as shown below.



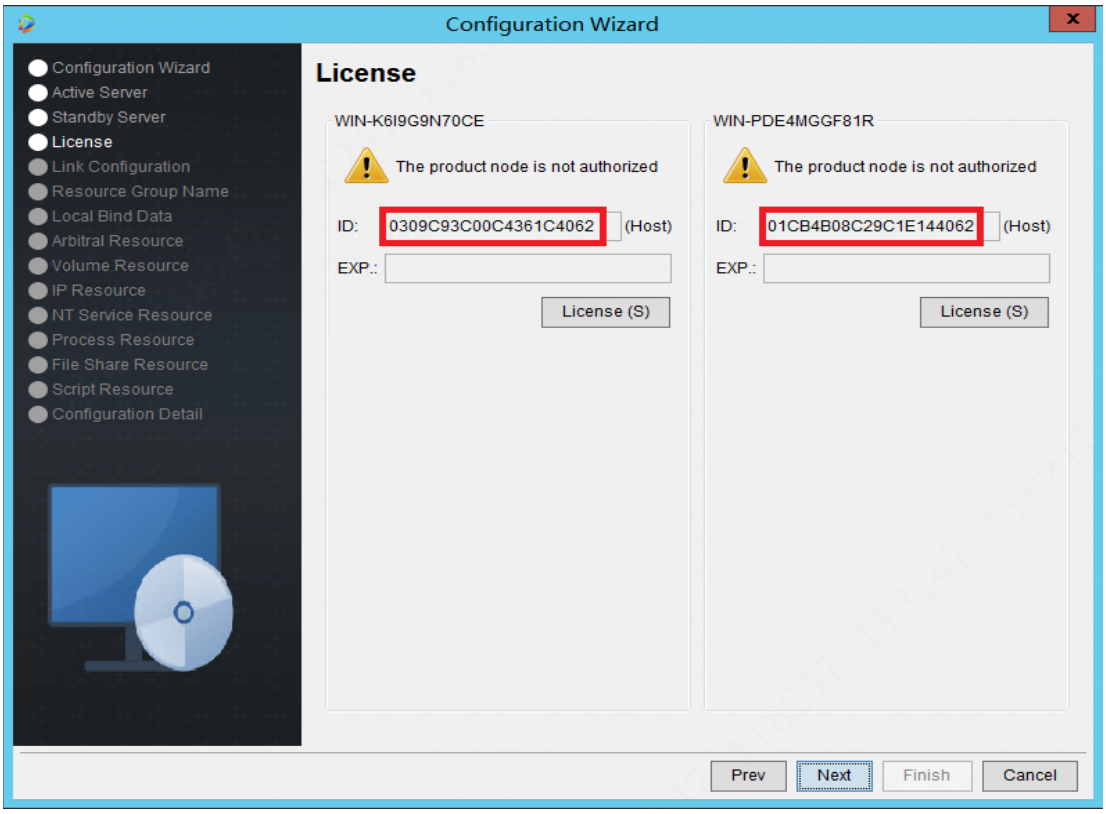
If TCP 7320/7330, UDP 7340/7350 and other ports are occupied by other application programs upon installation, or DSSMonitor, DSSHAService, DSSReplicator processes are not started, or the hot standby software has not been installed on the peer server, the prompt "Invalid server or no valid service on this server" will appear on the configuration panel of DSSReplicatorPlus Control Center, as shown in the right figure. At this point, end the process that is occupying the port, or deny access to the hot standby, or manually enable the DSSMonitor service in Service Management. If you fail to manually enable the service, uninstall and reinstall the hot standby software.



If the settings are successful, click **Next** to go to **Login**. Use default settings. Configure "Password" as "admin", select "Save password", and select "Auto Login". The settings are shown in the left figure.

Click **OK** to go to **Set license**.

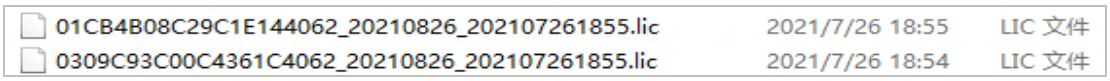
3.1.4 Set License

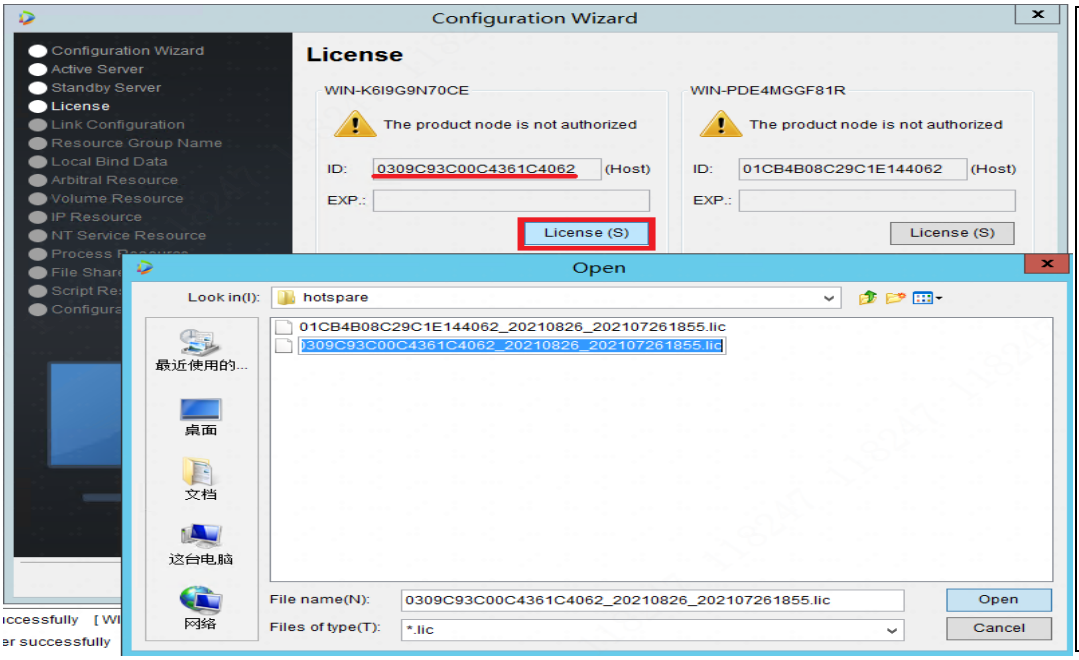


Copy the two Host IDs in the red boxes as shown in the right figure, paste them to a file saved in the .txt format, and enter the desired expiration date. If the expiration date is not entered, the default start time is the current day (Due to the time difference between home and abroad, there may be a 1-day time difference). The free trial period is 1 month by default, and if you want to use it for a longer time, you will be charged. Then send the file saved in the .txt format to local Dahua tech support team to apply for a license. It may take one to three working days to complete the application.

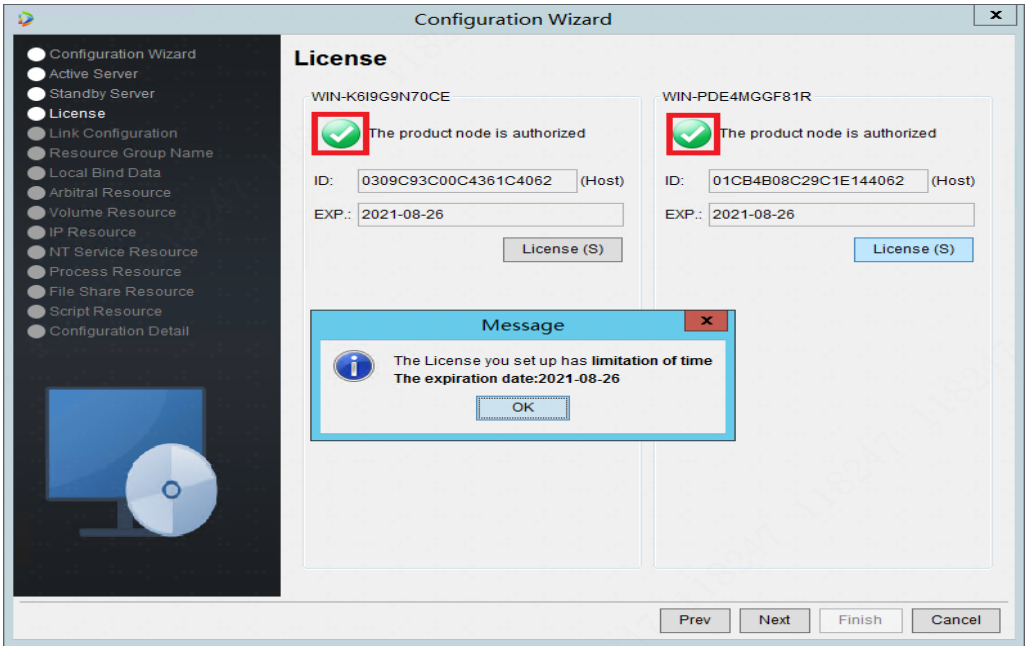
Note: After a software update (uninstallation and reinstallation), the old license cannot be used, and you will need to re-apply for a new license and import it.

The applied license file is in a format similar to the following two LIC files:





The format of a license file name: Host ID_Date_Time.lic. Copy the above license files to the active server, and click **License** at both sides, and import the license files according to the Host ID and file name.

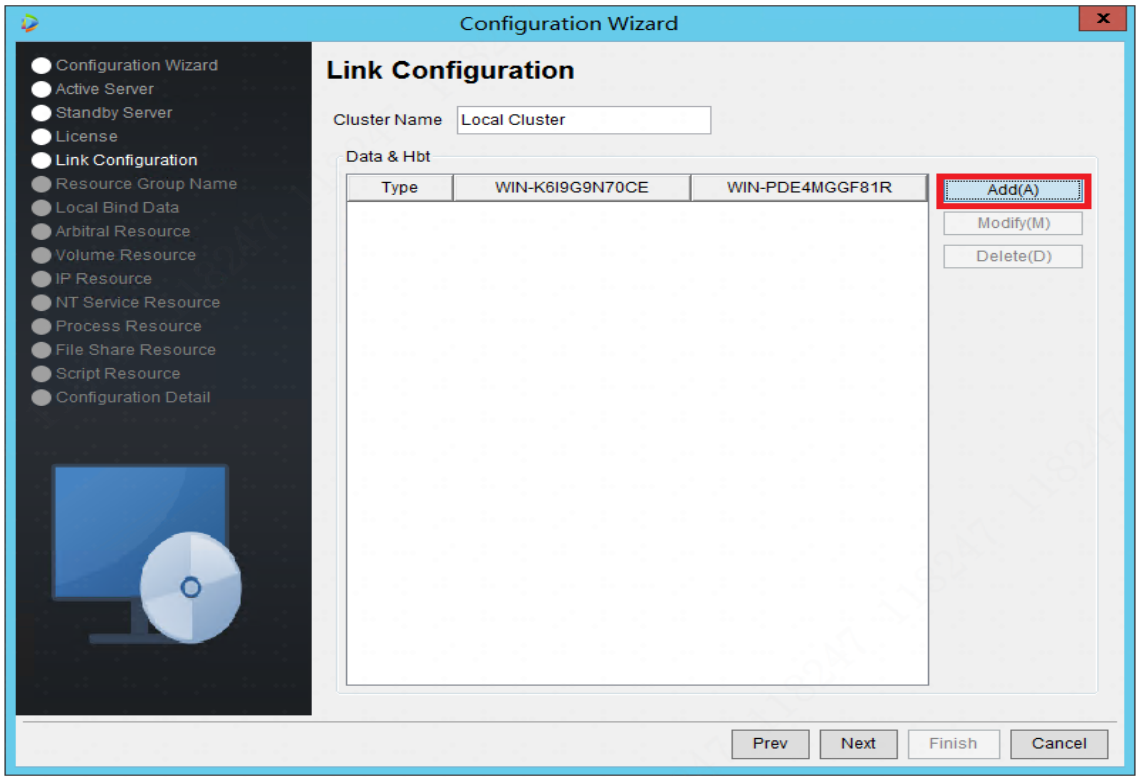


If the license has expired, the prompt "Setting License is failed [The license has expired:521]" will appear on the panel of DSSReplicatorPlus Control Center. At this point, re-import the valid license or deny access to the hot standby.

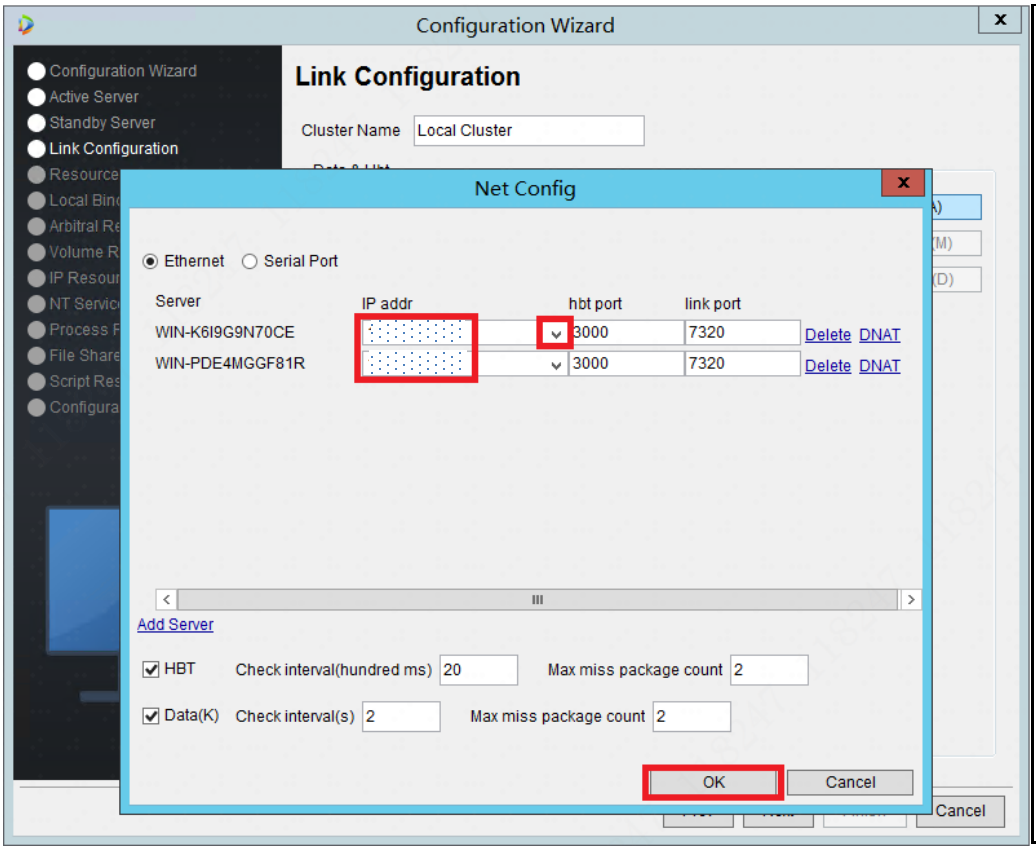
After the license files are loaded successfully, a pop-up window will be displayed to indicate the expiration date. Click **OK**, and the icon will turn from yellow to green. Then check whether the field "Exp" shows the expiration date. For the registration code with a perpetual license, "99999999" is shown in the field "Exp". For the registration code with a temporary license, the expiration date "Year-Month-Day" is shown in the field "Exp", as shown in the left figure.

Click **Next** to go to **Link Configuration**.

3.1.5 Link Configuration



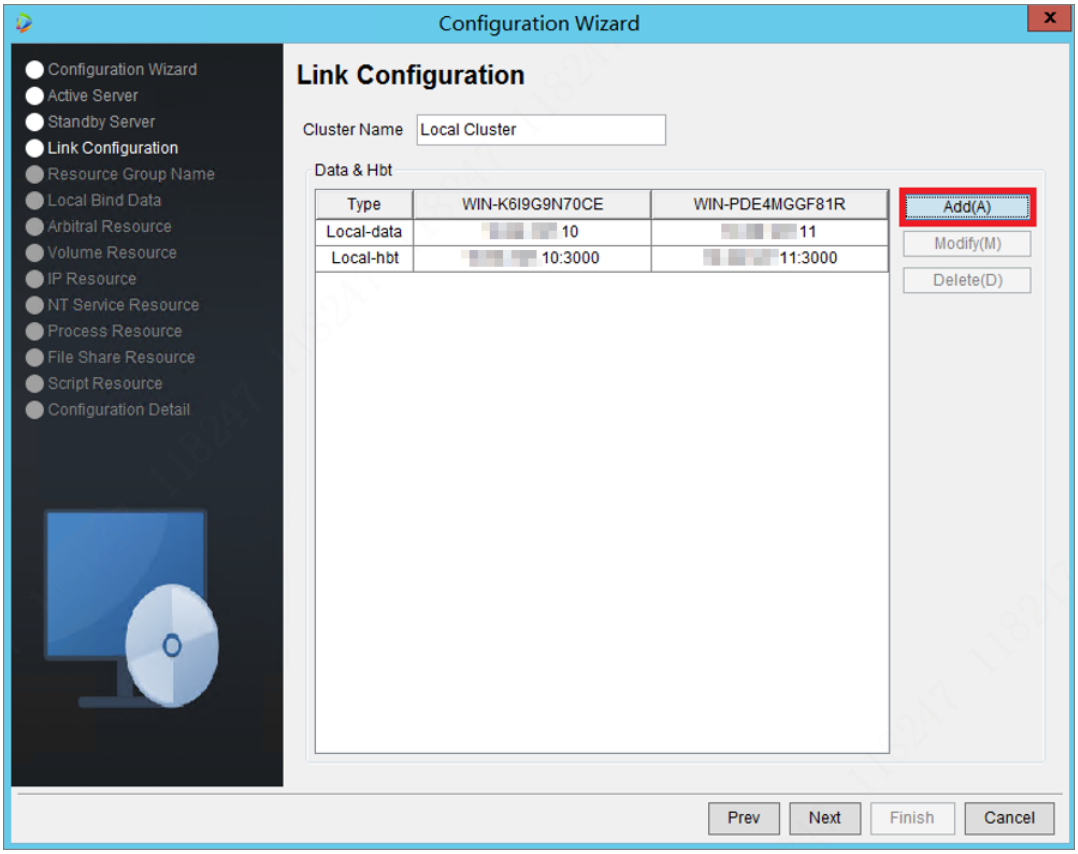
Click **Add**, and the "Net Config" window will pop up, as shown below.



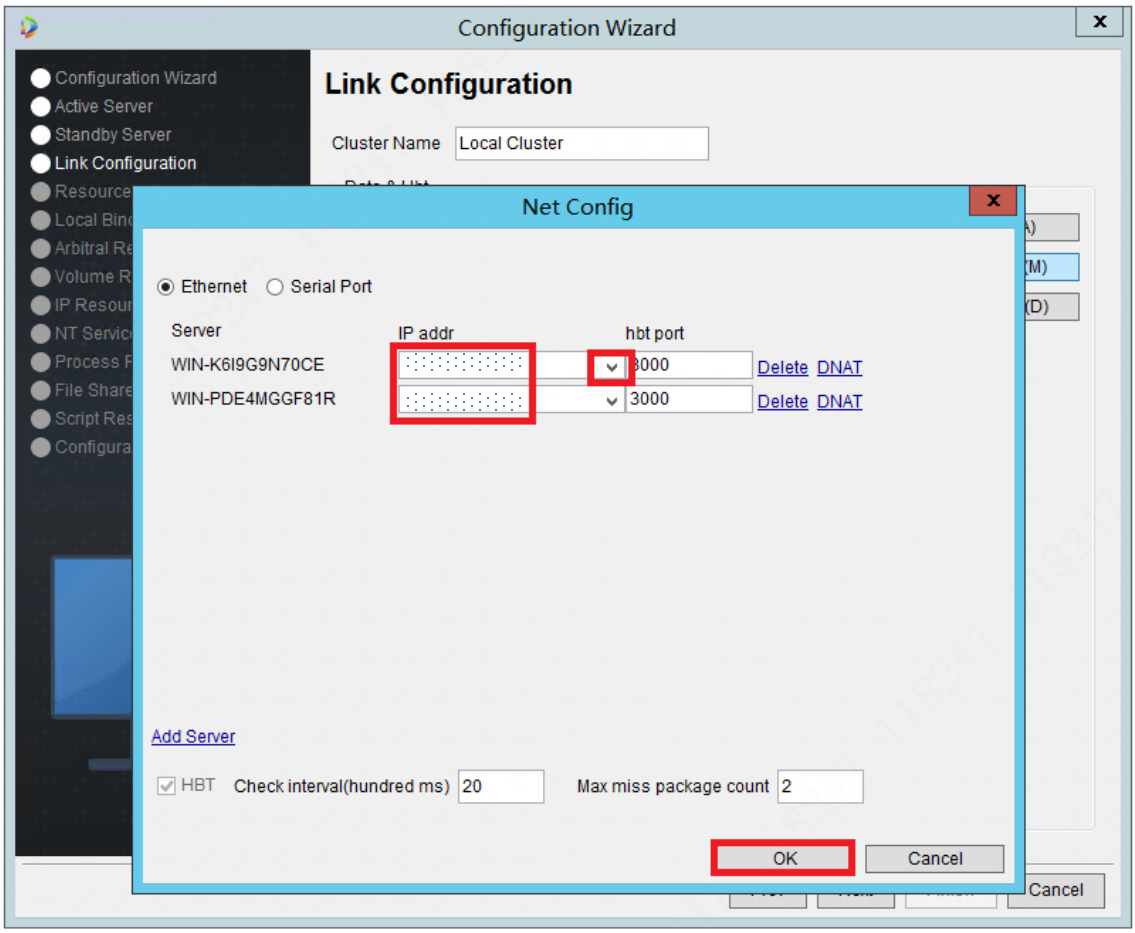
Configure the heartbeat type, IP address, heartbeat port, max packet-loss count, and check interval(s).

Select the service IP address. Make sure that all the IP addresses shown in the left figure are service IP addresses. You can leave other fields as default.

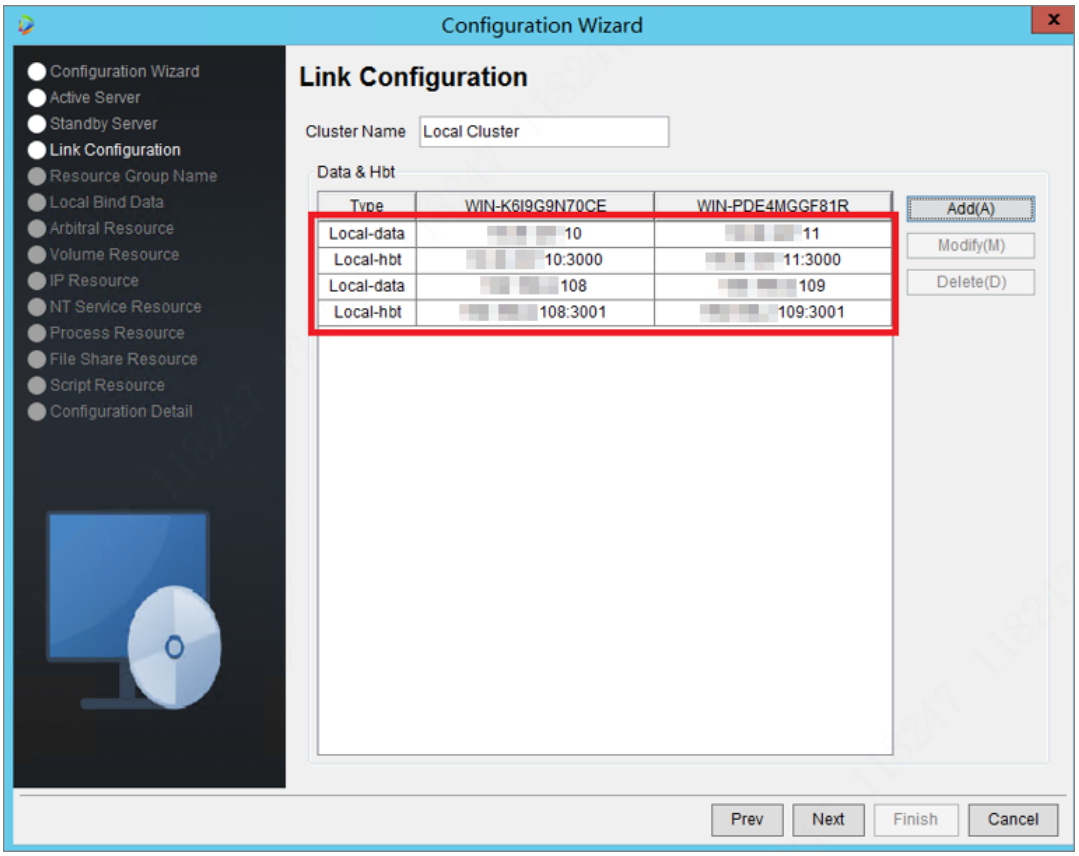
Click **OK**. The results are as follows:



Leave other fields as default. Click Add to add more heartbeat IP addresses.



Click **OK**. The results are as follows:

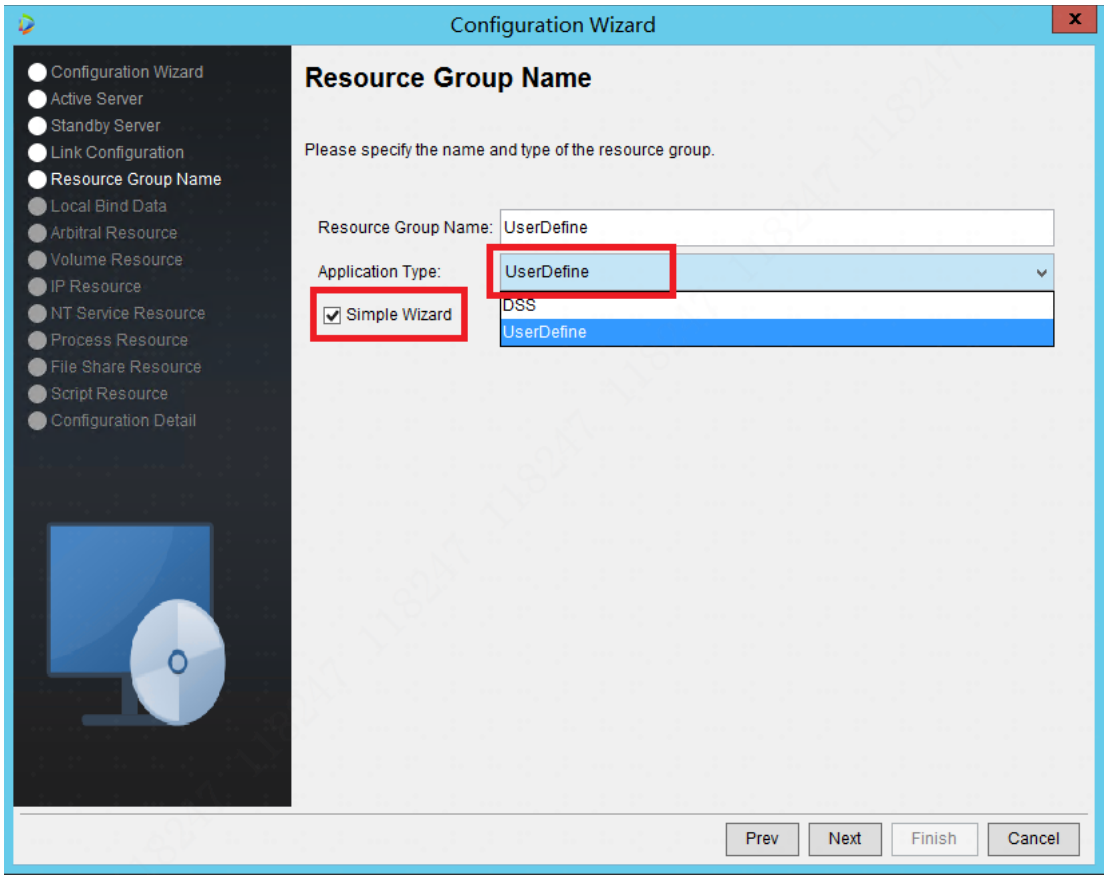


Notes: To enable the software firewall or the security software with network monitoring ports, enable the network communication permissions of all relevant ports (such as 3000 and UDP-type ports) first on both servers.

Click **Next** to go to **Resource Group Name**.

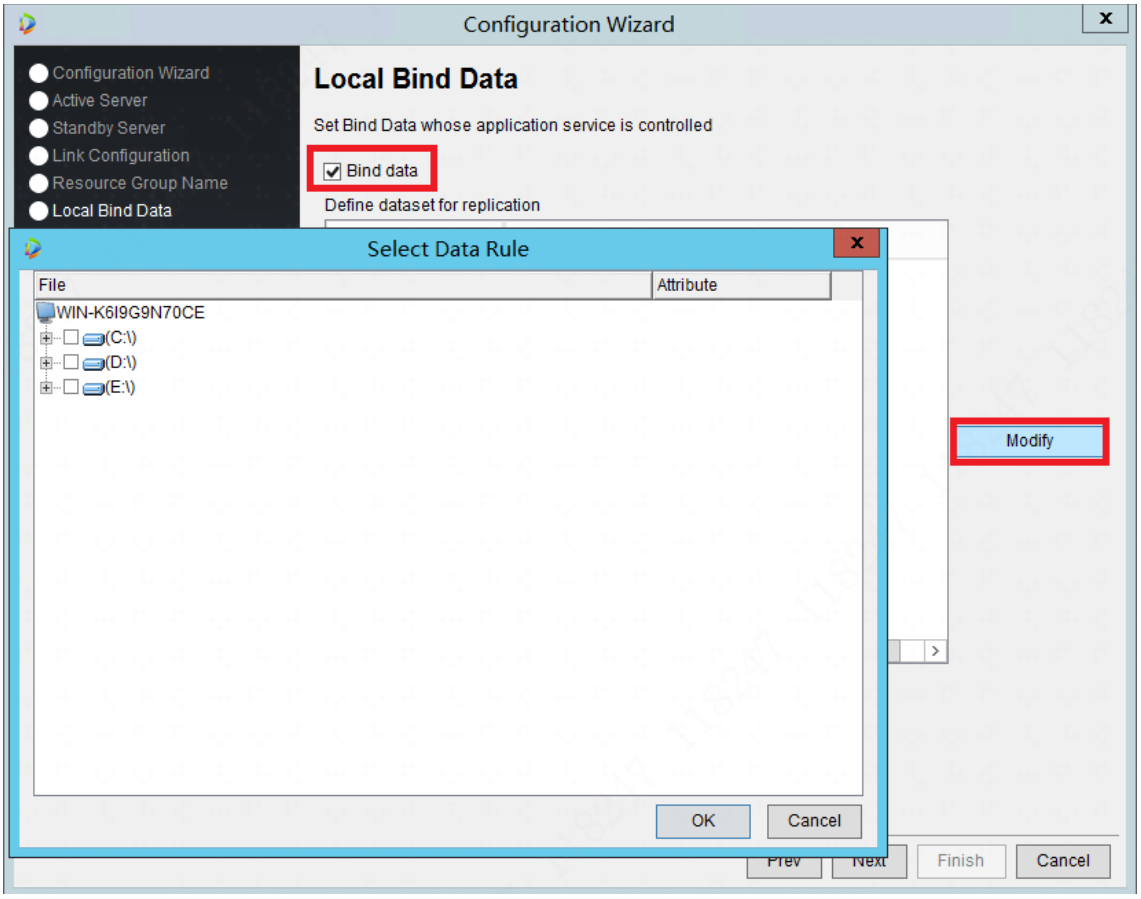
3.1.6 Resource Group Name

Select "UserDefine" under the "Application Type" tab, and select "Simple Wizard" to avoid unnecessary configurations.



Click **Next** to go to **Local Bind Data**.

3.1.7 Local Bind Data



Find the installation path of the DSS platform (ensure that the DSS installation directory on the primary and standby machines are identical, otherwise data synchronization will be abnormal), select the following directories or files:

Please configure the basic synchronization directory according to the DSS version.

V8.000.0000000.0 to V8.000.0000004.0

- **Images:**
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\webapps\upload
- **Offline maps:**
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\webapps\gisPack
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\bin\webapps-conf\emap\config_userDefined.properties
- **Databases:**
  DSS\DSS Server \mysql\data\dss
  DSS\DSS Server \mysql\data\ibdata1
  DSS\DSS Server \mysql\data\ib_logfile0
  DSS\DSS Server \mysql\data\ib_logfile1
- **Video storage:**
  DSS\DSS Server\SS\RecordPlan.xml
  DSS\DSS Server\SS\alarm_relation.db

V8.001.0000000.0 to V8.002.0000000.0

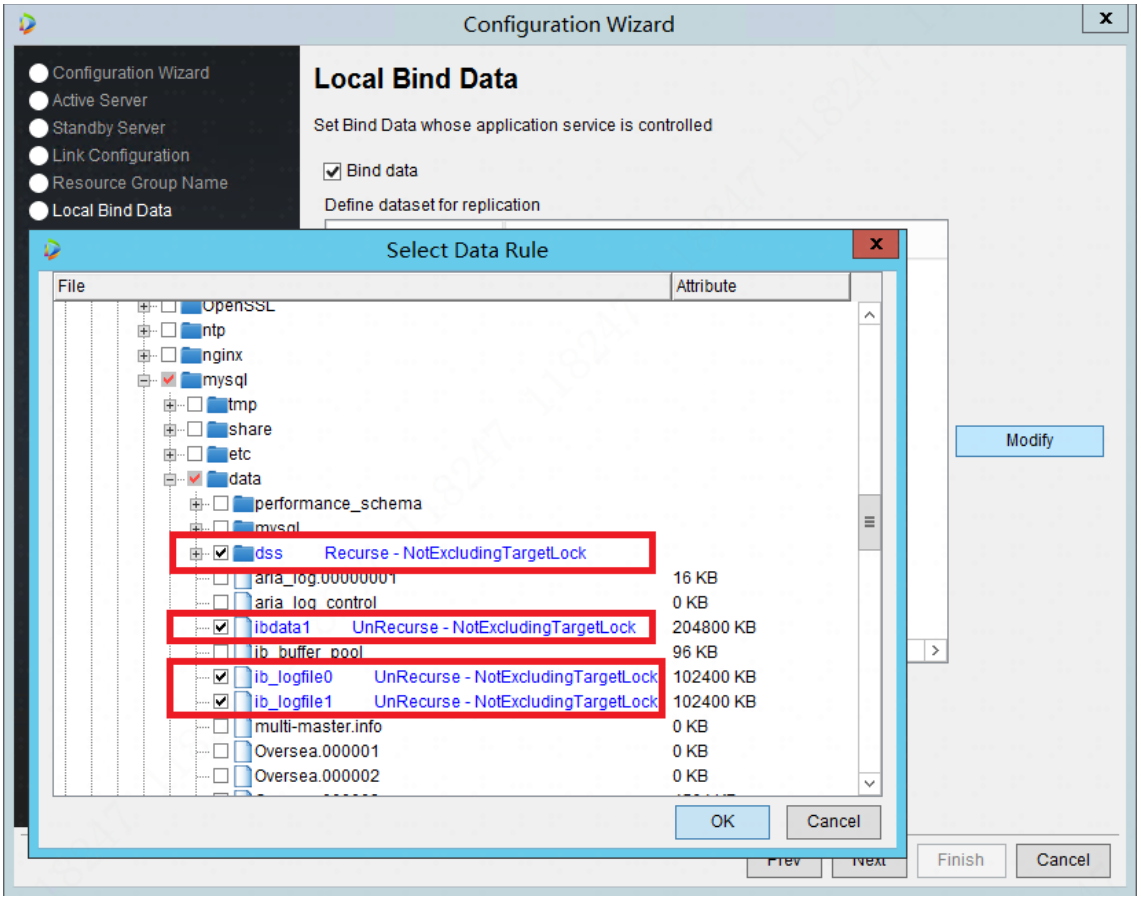
- **Images:**
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\webapps\upload
- **Offline maps:**
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\webapps\gisPack
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\bin\webapps-conf\emap\config_userDefined.properties
- **Databases:**
  DSS\DSS Server \mysql\data\dss
  DSS\DSS Server \mysql\data\ibdata1
  DSS\DSS Server \mysql\data\ib_logfile0
  Select DSS\DSS Server \mysql\data\mysql, and deselect the following 4 files : global_priv.frm, global_priv.MAD, global_priv.MAI and user.frm.
- **Plug-ins:**
  If you need to install DSS Retail, select DSS\DSS Server\mysql\data\retail.
- **Video storage:**
  DSS\DSS Server\SS\RecordPlan.xml
  DSS\DSS Server\SS\alarm_relation.db

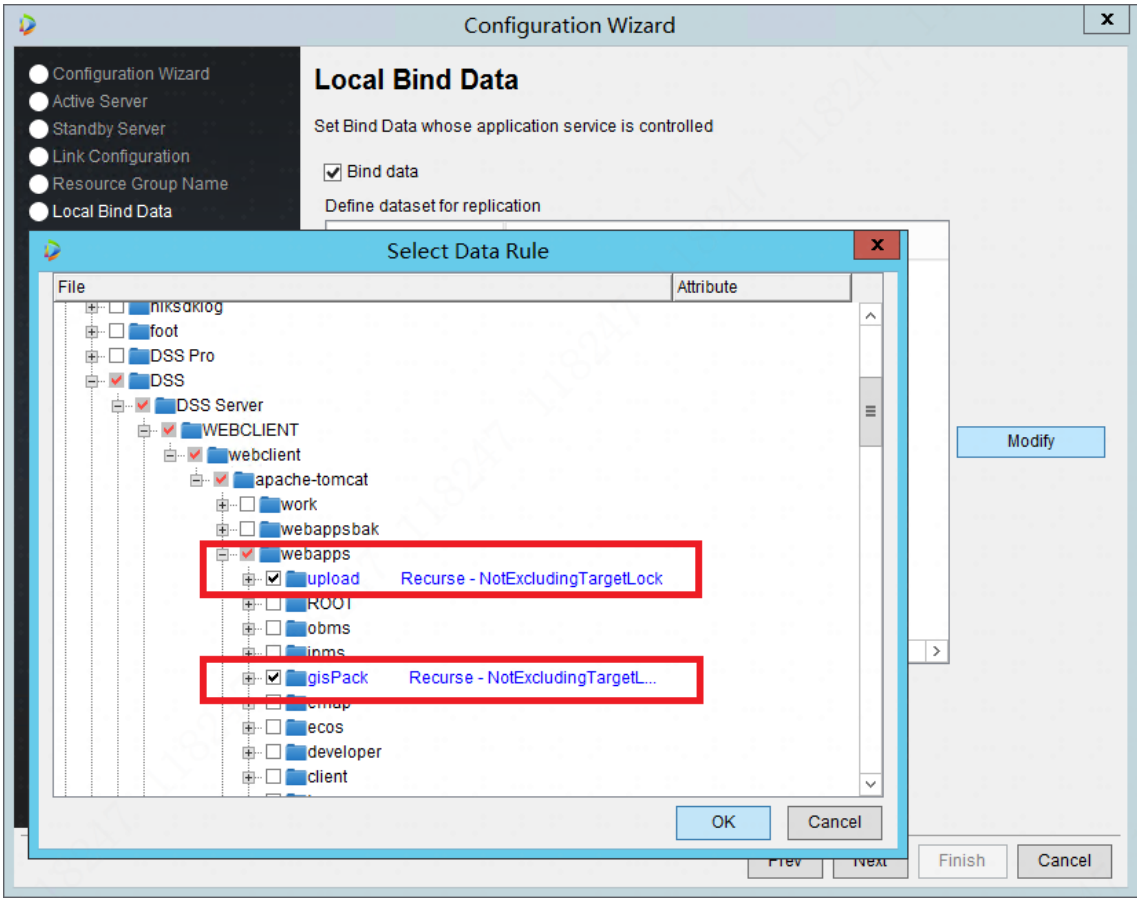
V8.003.0000000.0

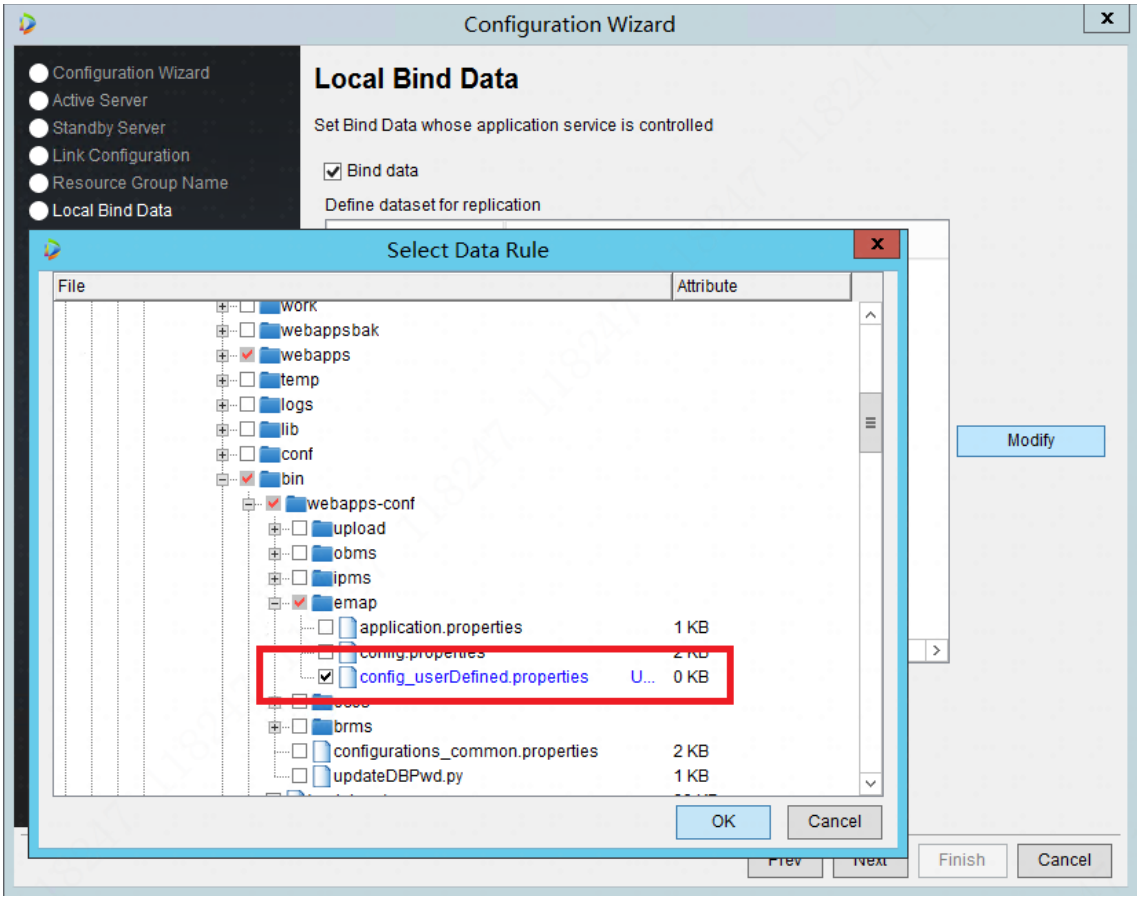
- **Images:**
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\webapps\upload
- **Offline maps:**
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\webapps\gisPack
  DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\bin\webapps-conf\emap\config_userDefined.properties
  Databases:
  DSS\DSS Server \mysql\data\dss
  DSS\DSS Server \mysql\data\ibdata1
  DSS\DSS Server \mysql\data\ib_logfile0
  Select DSS\DSS Server \mysql\data\mysql, and deselect the following 4 files : global_priv.frm, global_priv.MAD, global_priv.MAI and user.frm
- **Plug-ins:**
  If you need to install DSS Retail, select DSS\DSS Server\mysql\data\retail.
  If you need to install DSS Energy select DSS\DSS Server\mysql\data\enerage
- **Video storage:**
  DSS\DSS Server\SS\RecordPlan.xml
  DSS\DSS Server\SS\alarm_relation.db

The above are required configurations. For optional configurations, refer to the central storage, NTP time synchronization, WebClient certificate, CA certificate, and AcuPick component in the DSS business configuration.

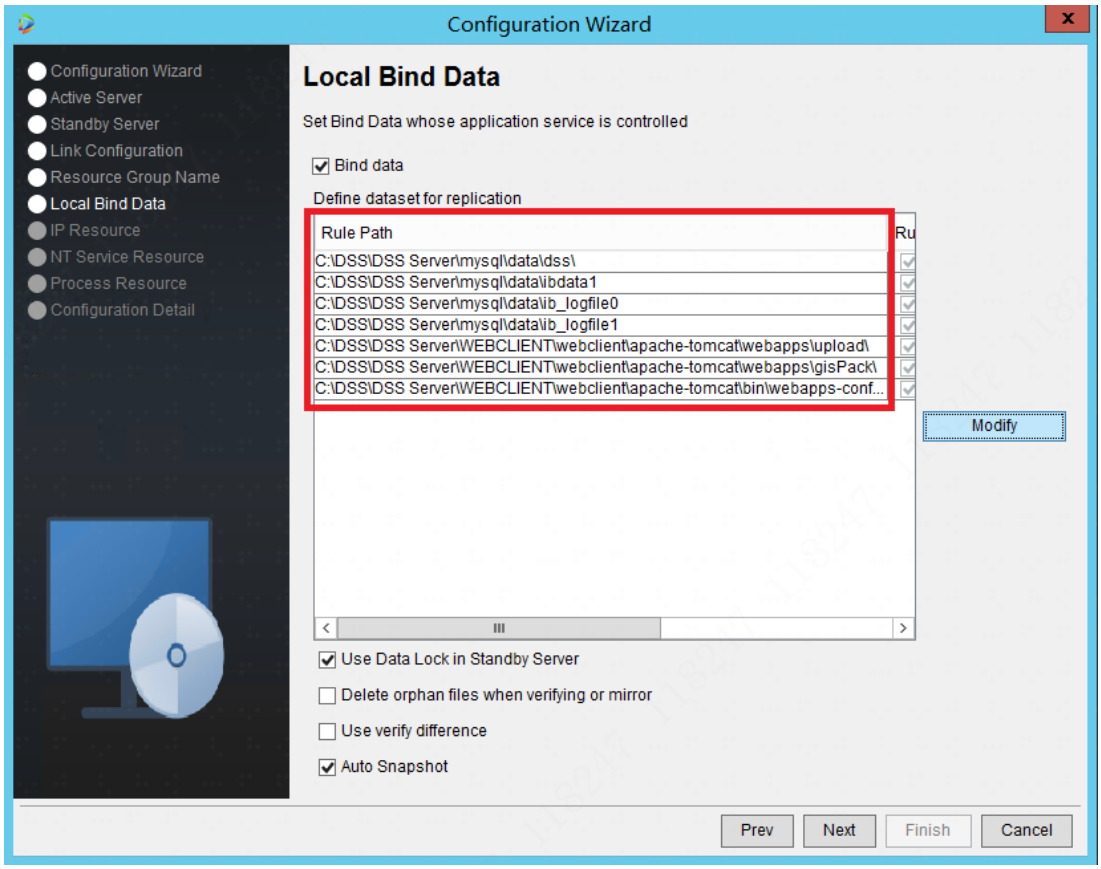
The images use the configuration of V8.0.0 to V8.0.4 as an example. See the table above for details.


Configuration Wizard
Configuration Wizard
Active Server
Standby Server
Link Configuration
Resource Group Name
Local Bind Data
Local Bind Data
Set Bind Data whose application service is controlled
Bind data
Define dataset for replication
Modify
Select Data Rule
File
Attribute
OpenSSL
ntp
nginx
mysql
tmp
share
etc
data
performance_schema
mysql
dss Recurse - NotExcludingTargetLock
aria_log.00000001 16 KB
aria_log_control 0 KB
ibdata1 UnRecurse - NotExcludingTargetLock 204800 KB
ib_buffer_pool 96 KB
ib_logfile0 UnRecurse - NotExcludingTargetLock 102400 KB
ib_logfile1 UnRecurse - NotExcludingTargetLock 102400 KB
multi-master.info 0 KB
Oversea.000001 0 KB
Oversea.000002 0 KB
OK
Cancel
Finish
Cancel


Configuration Wizard
Configuration Wizard
Active Server
Standby Server
Link Configuration
Resource Group Name
Local Bind Data
Local Bind Data
Set Bind Data whose application service is controlled
Bind data
Define dataset for replication
Modify
Select Data Rule
File
Attribute
foot
DSS Pro
DSS
DSS Server
WEBCLIENT
webclient
apache-tomcat
work
webappsbak
webapps
upload Recurse - NotExcludingTargetLock
ROOT
obms
gisPack Recurse - NotExcludingTargetL...
ecos
developer
client
OK
Cancel
Finish
Cancel



Click **OK** and the results are as follows. Seven items are added.

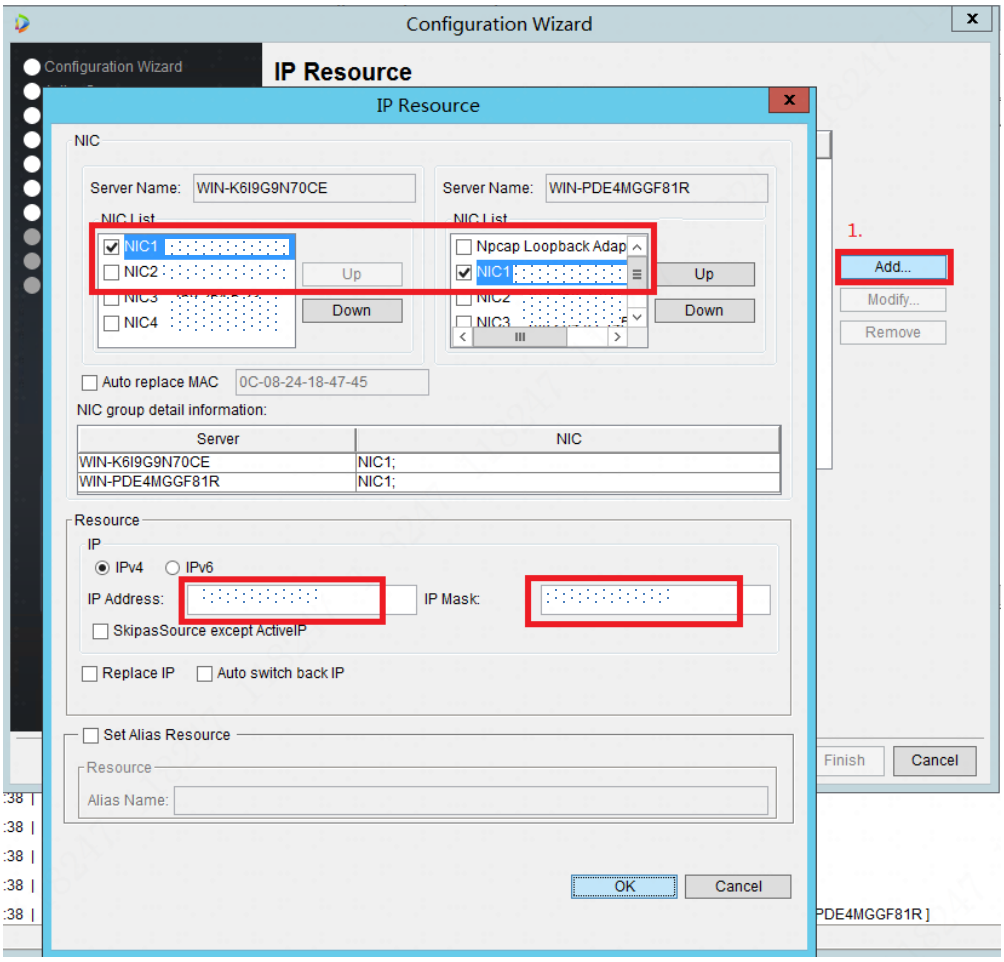


To synchronize alarms, human faces, captured vehicle data, evidence files, and other information, select the OSS_DAT or SUBOSS_DATA folder under each drive letter. This step is not configured in the initial configuration. For configuration details, see Binding Data Sources to a Disk

If you find that the amount of data is large during the deployment process, select "Use verify difference" to optimize the time of secondary verification.

Click **Next** to go to IP Resource.

3.1.8 IP Resource

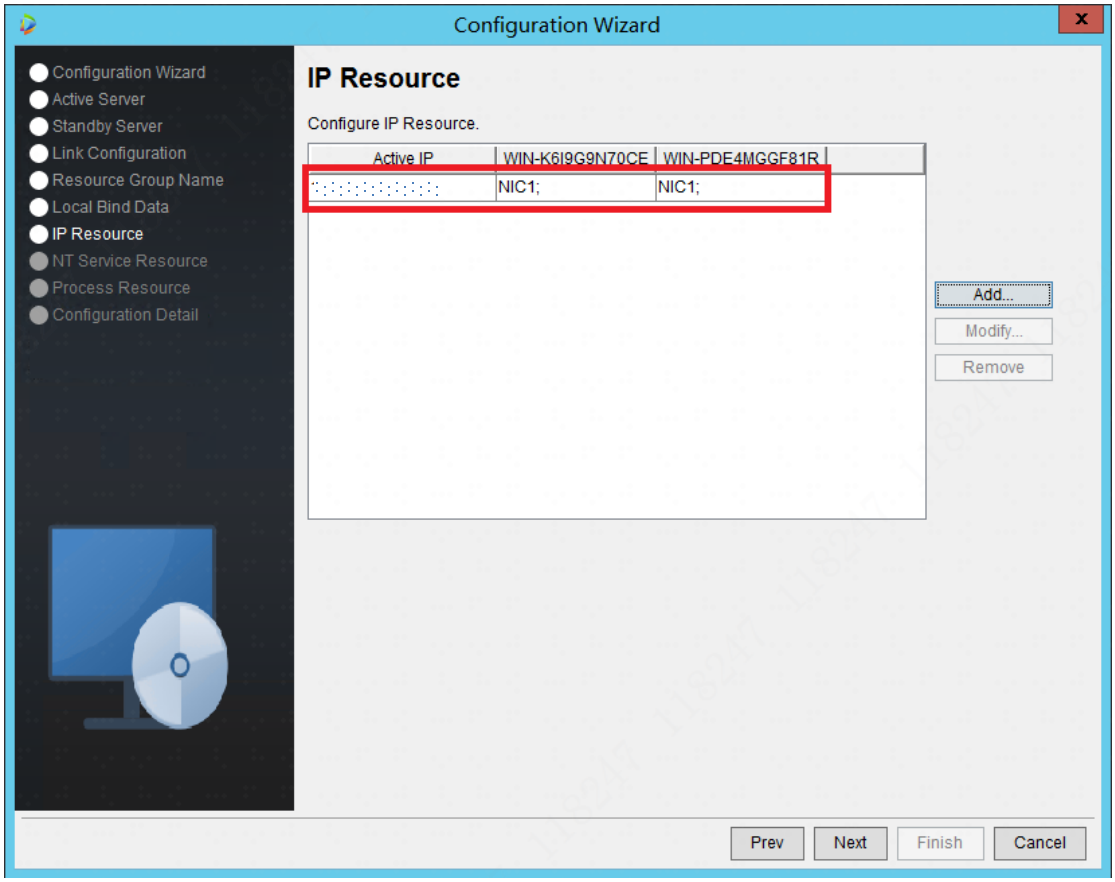


Click **Add** to go to the interface shown in the left figure.

In "NIC List", select the service IP addresses of the active server and the standby server. In "Resource", enter the VIP and the corresponding IP mask.

IP Mask: Same as the IP mask of the active server. An example of IP and IP Mask is shown in the figure, for reference only.

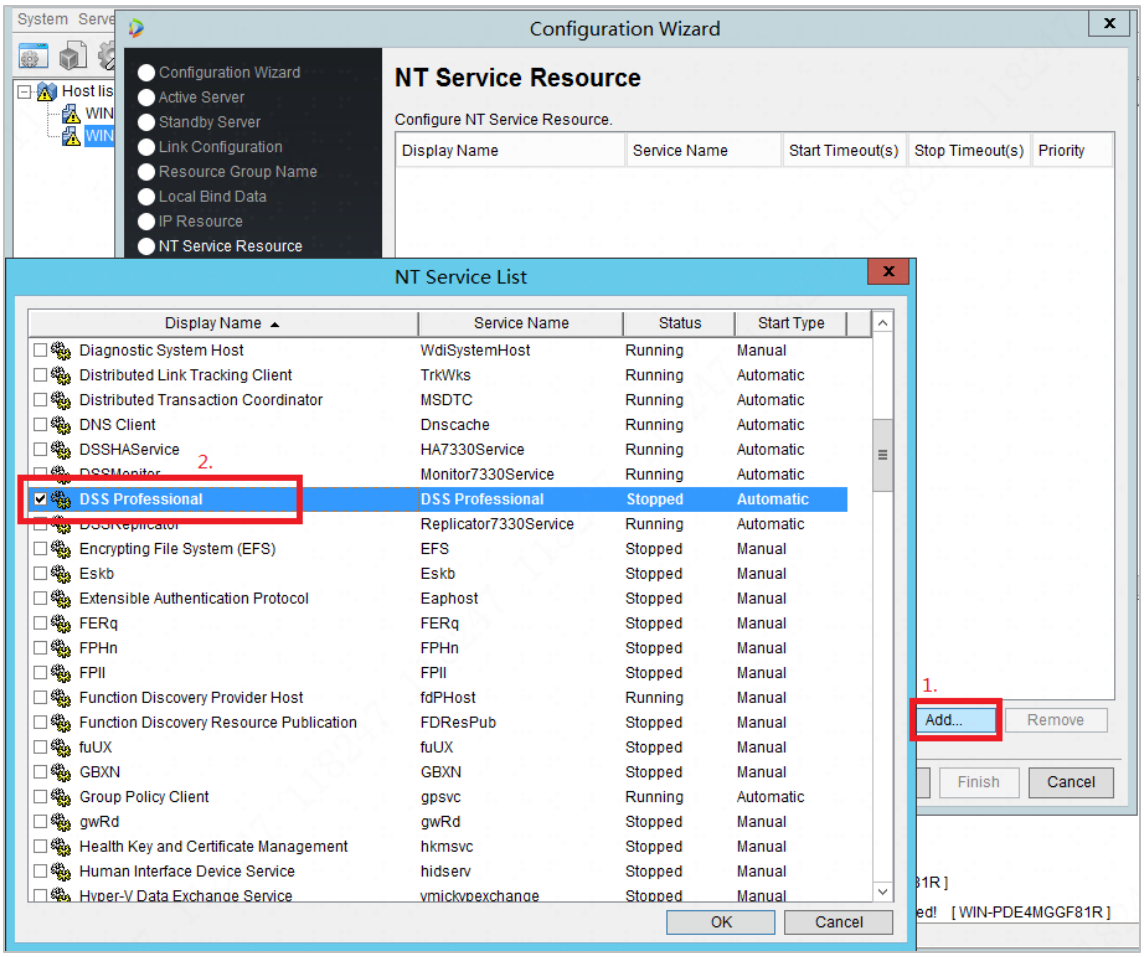
Click **OK** and check if the "Config IP Resource" is correctly configured. The NIC bound is service NIC.



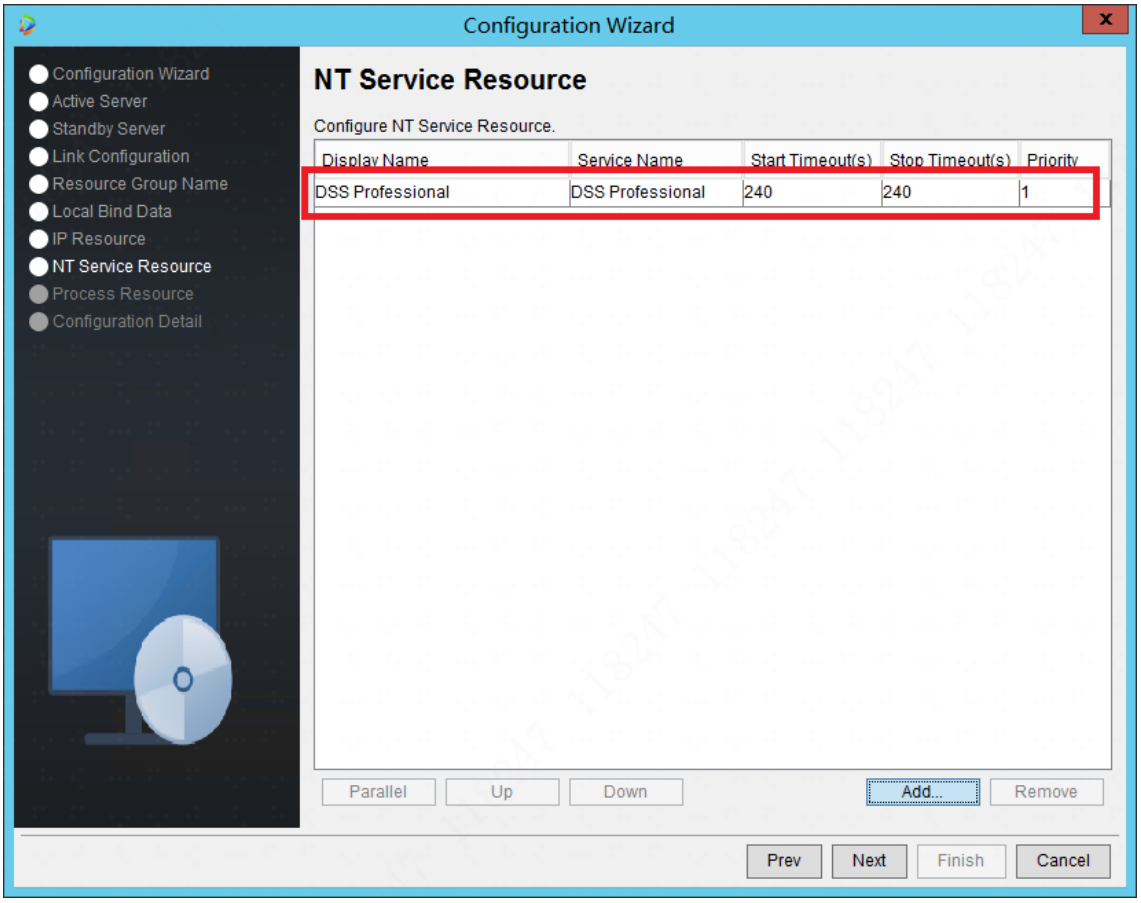
Click **Next** to go to **NT Service Resource**.

3.1.9 NT Service Resource

Click **Add** to go to the following window, and select **DSS Professional**.

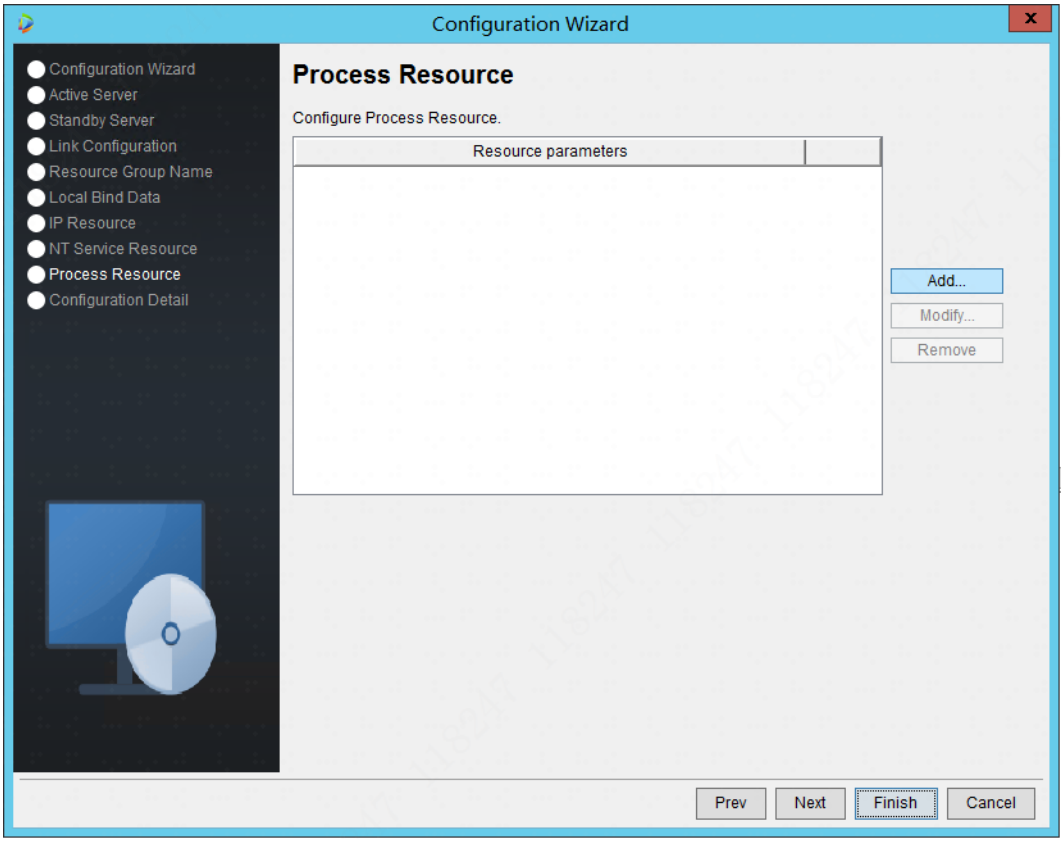


Click **OK**, and the following is shown:

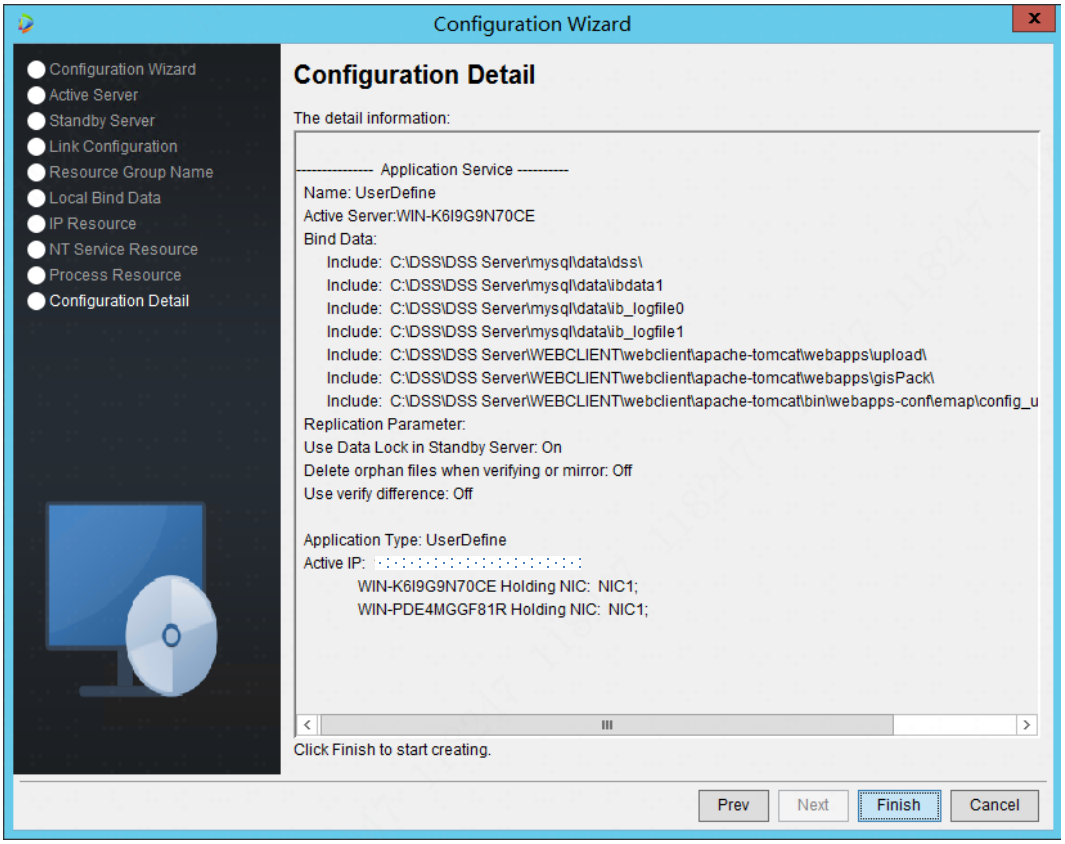


3.1.10 Process Resource

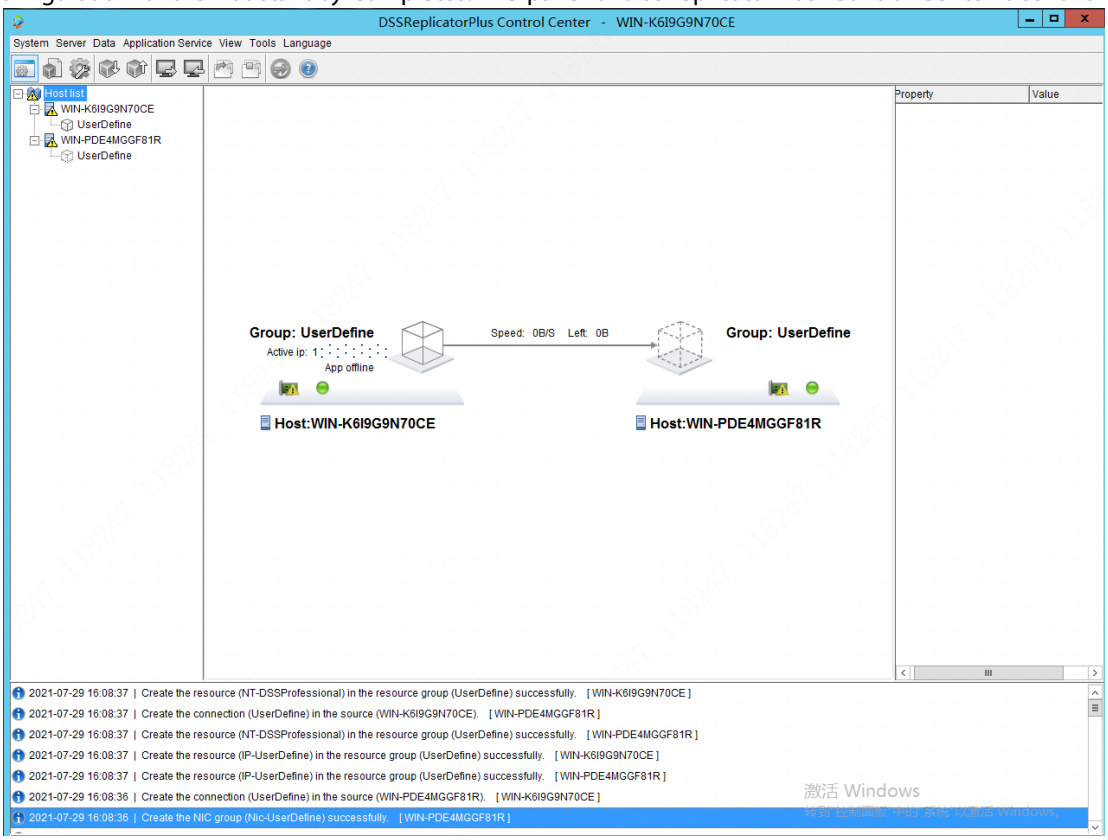
Click **Next**.



Click **Next**, as shown below.



Click **Finish**. The configuration of the hot standby completes. The panel of DSSReplicatorPlus Control Center is as follows.

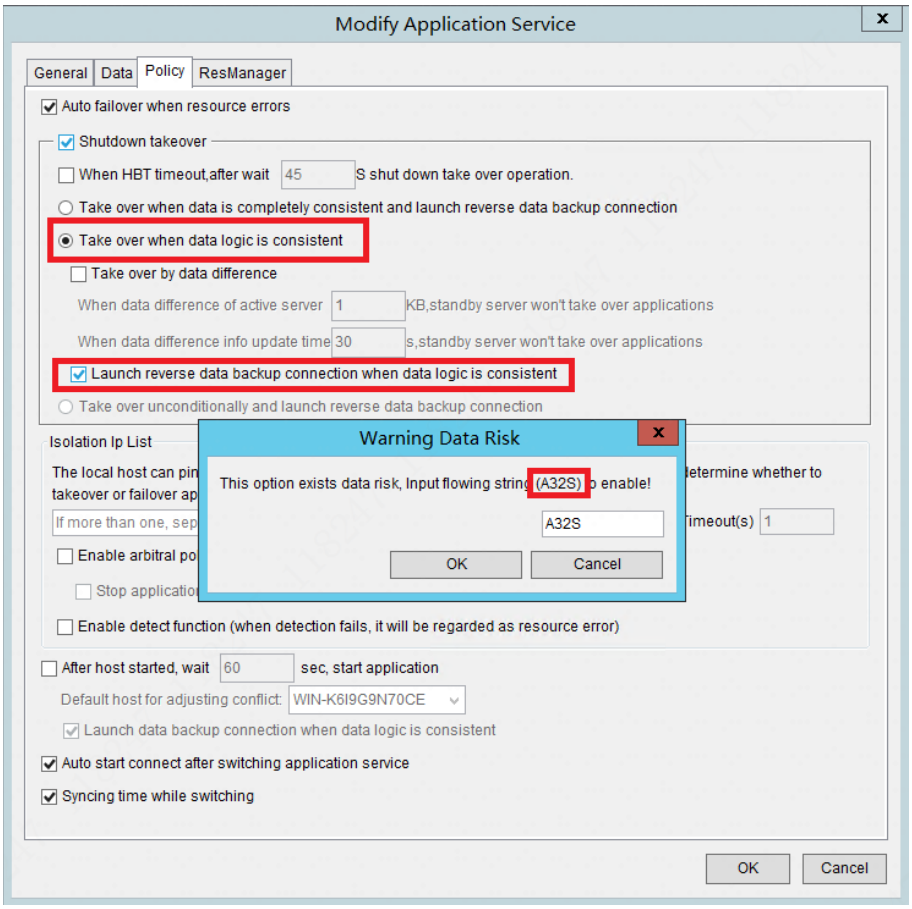


3.2 Configuring Data Consistency Policies

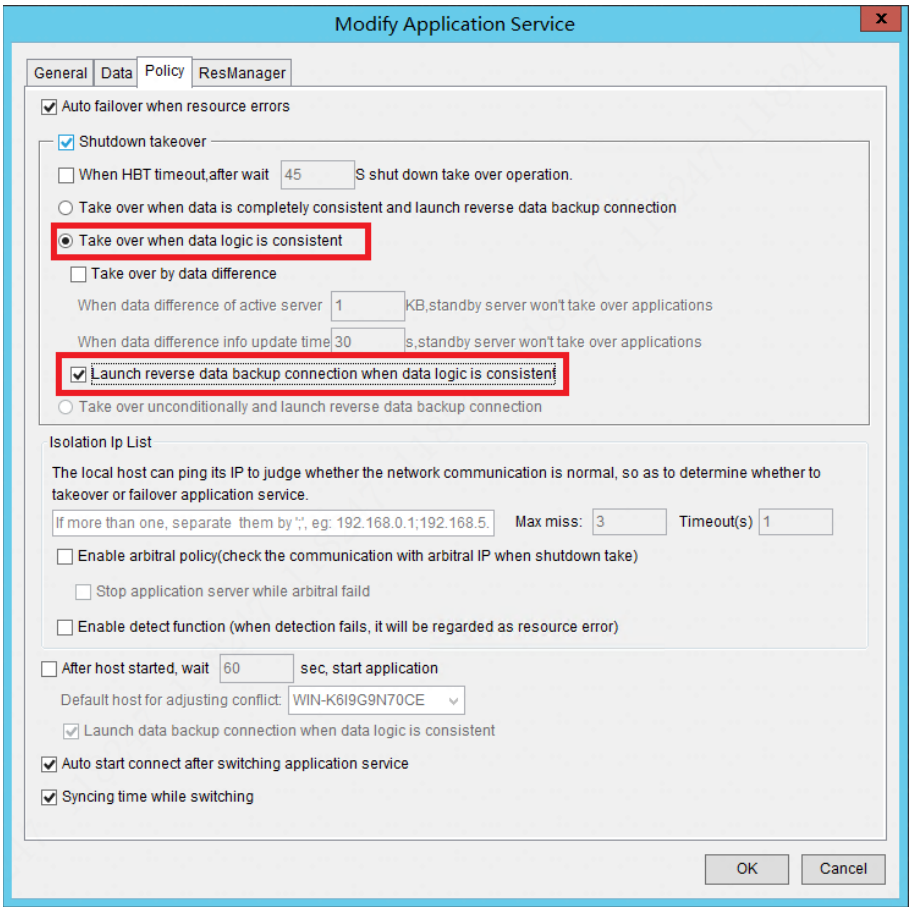
After the hot standby configuration is completed, data synchronization strategies need to be performed. It is recommended to configure the data logical consistency strategy. Because the default configuration strategy is data complete consistency strategy, in extreme cases such as power failure of the host or sudden network disconnection, the backup machine may not take over. If the user is very concerned about the continuity of the business, the data logical consistency strategy can be enabled, and the reverse data backup connection can be started as needed, and the synchronization time can be manually configured when switching.

Consistency strategy should be configured before introducing the service.

On the **Policy** page, select **Take over when data logic is consistent** and **Launch reverse data backup connection when data logic is consistent**. The Warning Data Disk prompt will automatically pop up.



Enter the default string in the box, and then click **OK**.



Click **OK** to close the prompt.

For specific differences between "Complete Consistency Strategy" and "Logic Consistency Strategy", refer to "4.1 Selecting the Data Consistency Policy".

After creating application service resources, the data consistency strategy selection is completed, and the application service can be started by performing the bring-in operation. Testing operations such as bring-out and switch can also be performed later to verify the correctness of the dual-machine hot standby configuration. The steps of bring-in, bring-out, switch, and other operations refer to the main functions of the dual-machine hot standby software.

3.3 DSS Service Configuration

Once the hot standby software is set up, you need to configure the DSS service. We recommend that you configure the DSS service in the following order (to reduce the number of switchover times of the active and standby servers).

Step 1: Modify the Server IP addresses of the DSS service on the active and standby servers.(You can also modify it after the DSS is installed).

Step 2: For the hot standby software, bring in the active server and run the hot standby. After initialization, log in to the client.

Step 3: Import the license into the active server. Log in to the client again (Note: Storage configuration is also available before the license is imported).

Step 4: Configure the Central Storage of the **active server** (Configure local network disk types, add a network disk and set disk types as planned). NTP Time Sync (Optional. This feature can be configured during standalone server operation. If this feature is not required, it can be skipped and reconfigured as required in the future).

Step 5: Manually switch over to the standby server for operations, and log in to the client after initialization.

Step 6: Import the license into the standby server.

Step 7: Configure the central storage of the **standby server** (Configure local network disk types, add a network disk and set disk types).

Step 8: Switch over to the active server for operations.

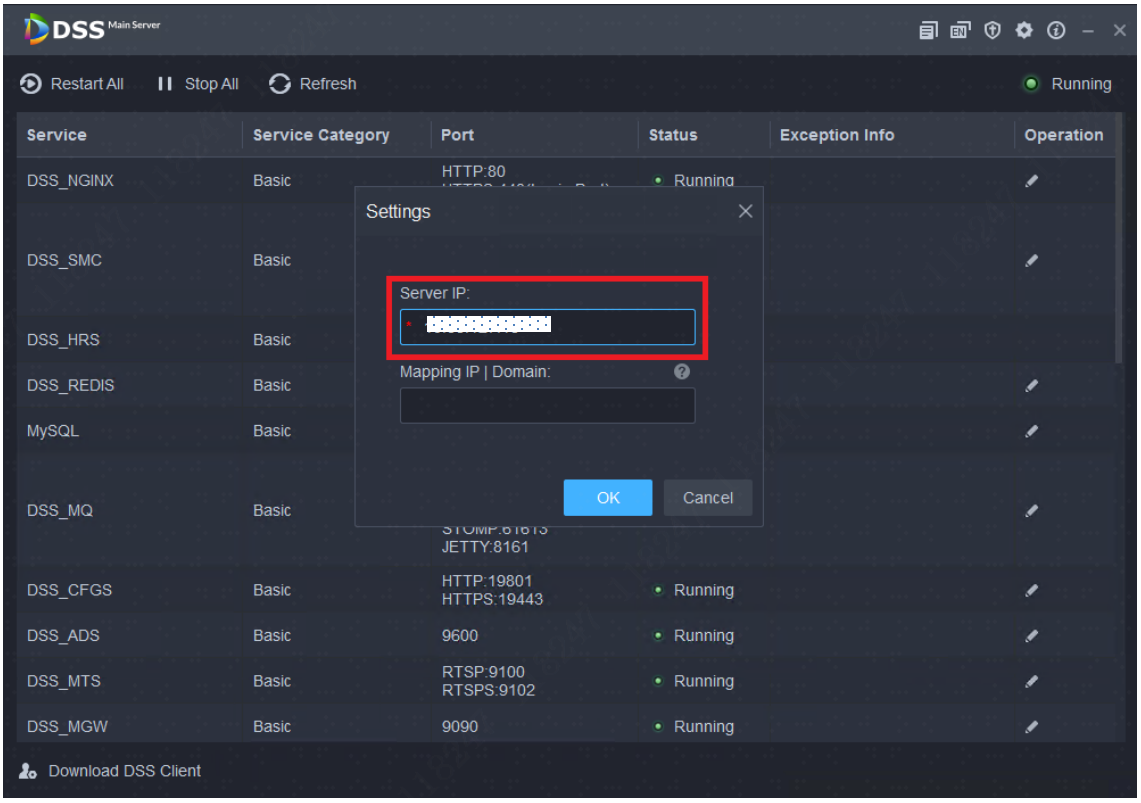
Step 9: Bring out the hot standby.

Step 11: Bind the resources of the hot standby and configure the script. Disk, Time Sync,WebClient Script Configuration.

Step 12: Select the sync direction of data sources and bring it in. The setup is complete.

3.3.1 Modifying Service IP Address of DSS

Switch to the DSS service configuration interface of the active server, and modify the service IP address. The service IP addresses of both the active and standby servers need to be changed to VIP. In this example, VIP is 10.38.127.15, as shown in the following figure.



The service IP address of the standby server also needs to be changed to VIP, in the same way as the active server.

Notes: When configuring VIP, make sure that HAService.exe, Replicator.exe, and SMonitor.exe processes are started smoothly. Open the Task Manager to check if the processes are started smoothly.

3.3.2 Importing License to Platform

Apply for two license certificates of DSS first. After the service has been successfully brought in, log in to the client, import one of the two DSS licenses to the active server, and confirm the activation. (At this point, you can log in to the platform to configure the NTP server and the image disk. This can save you the trouble of bringing in/out them repeatedly. If you do not want to perform the configuration, ignore this step subsequently).

After the standby server is successfully launched, log in to the client again, import another DSS license, and confirm that the import is successful. At this point, the licenses of the two servers are successfully imported. It means that the subsequent switchover will not affect the authorization of the licenses (At this point, you can also go to configure the NTP server or the image disk. If you do not want to perform the configuration, ignore this step subsequently).

Note: If the applied license is a trial license, due to the small number of authorization channels for a trial license, the switchover between active and standby servers may cause the license to expire when too many devices are added by abnormal means, and then you will not be able to use the license. For this case, you need to apply for a license that matches the number of devices added to the platform and re-import it according to the above steps.

3.3.3 Configuring Central Storage (Optional)

To use functional modules such as alarms and human faces, you need to configure image storage. DSS V8.0.4 and before are not supported.

V8.0.4 and later support the central storage of hot standby. Storage configuration is no longer limited by license. You can configure storage separately for two standalone servers, or set up the hot standby before configuring storage for the two servers separately.

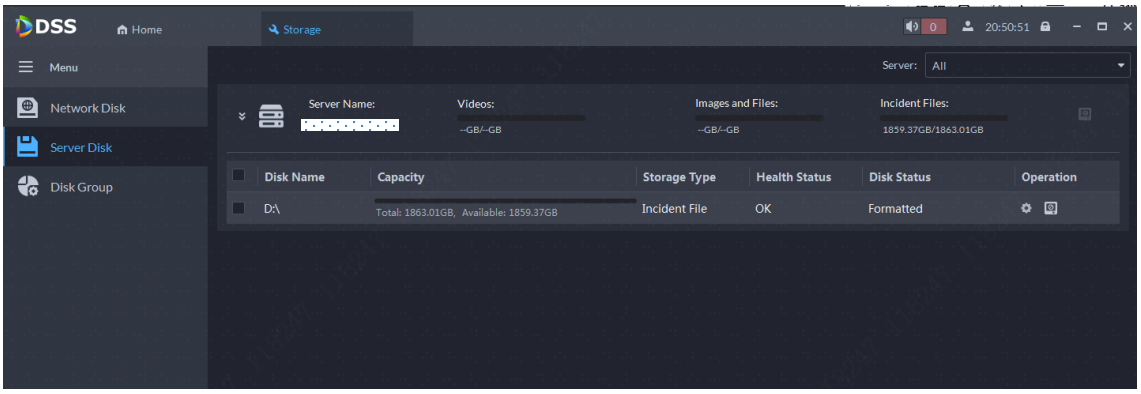
When using the central storage of hot standby, read the following notes carefully.

1. On a server of hot standby, one EVS can be added to the server multiple times as different users. But on a standalone or distributed server, one EVS can only be added once. If a network disk is used for storing images and files and when in user mode, the active and standby servers need to add **two unused users under one EVS**. If you want to add different users of the same EVS multiple times, the disk types of the added users must be the same.
2. **When configuring data source binding, make sure that the drive letter and the corresponding type of the disks for storing files or images must be identical, and the number and size of the disks must also be identical.**
3. In central storage, local disks cannot be used as video disks. Data on video disks cannot be synchronized. This will cause inconsistency in the data of the active and standby servers.
4. **If switching disk type or deleting is performed on the image storage disk configured with data synchronization, you need to update the binding relationship on the hot standby software in time. This prevents the loss of the mount point, which may result in abnormal data synchronization or abnormal switchover.**
5. **File synchronization of the hot standby is incremental. If you need to format the image storage disk that has been configured with data synchronization, the formatting on the client can only format the contents of the disk on the current active server, while the data of the same drive letter on the standby server will not be formatted. If you want to format the disk on the standby server, switch to the standby server.**

3.3.3.1 Configuring a Local Disk on the Client

Set the disk type on the DSS client (same operation for active and standby servers):

For V8.0.4 and later versions, evidence files can only be configured locally. If the storage of evidence files is required, it can only be configured on the local disk. An example of an evidence file disk (same configuration for images and files) is provided, as shown below. Format the local disk of the active server for evidence file storage:

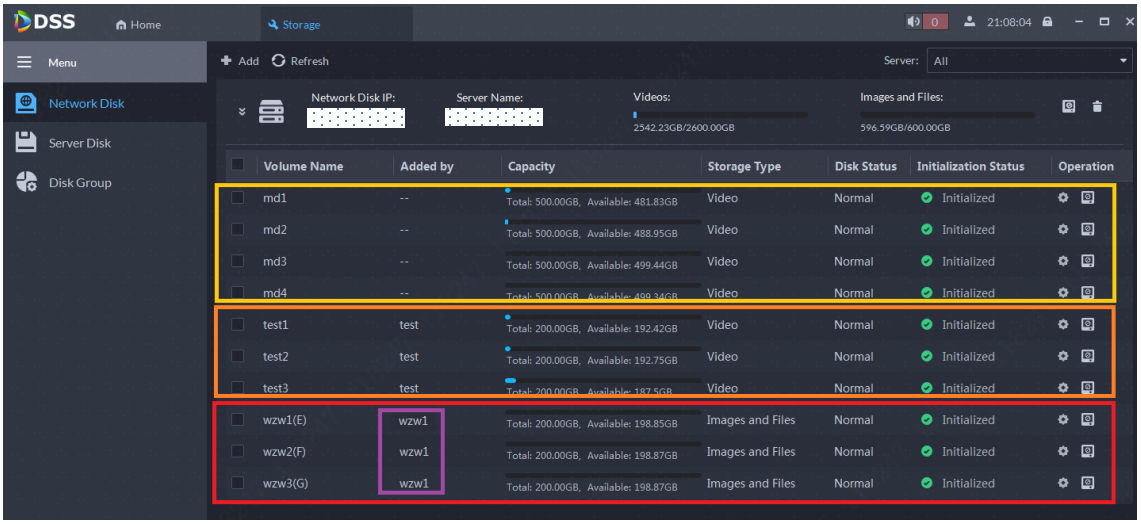


3.3.3.2 Adding a Network Disk on the Client

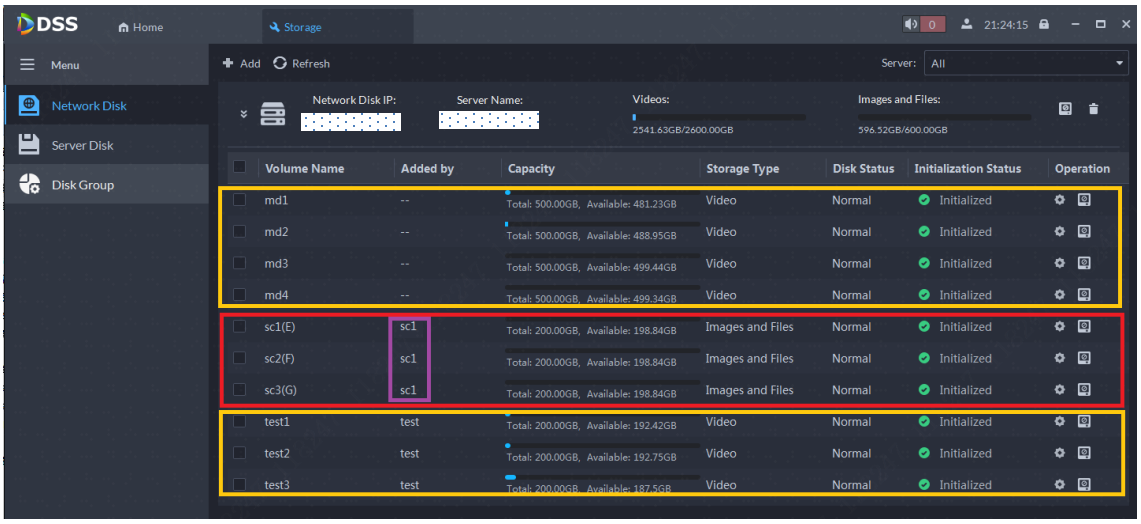
If one EVS is used for both image and video storage in a network disk, plan the relation between a user and a storage type, and at least three users are required (The normal mode can also be used as a special user, but EVS added in normal mode can only be used for video storage). Volumes can only be added in the same way that users are added.

An example of planning: one EVS and three users (wzw, sc, test). User "wzw" is used for image storage for the active server, user "sc" for image storage for the standby server, and user "test" for video storage. The normal mode is added for video storage.

Active server:



Standby server:

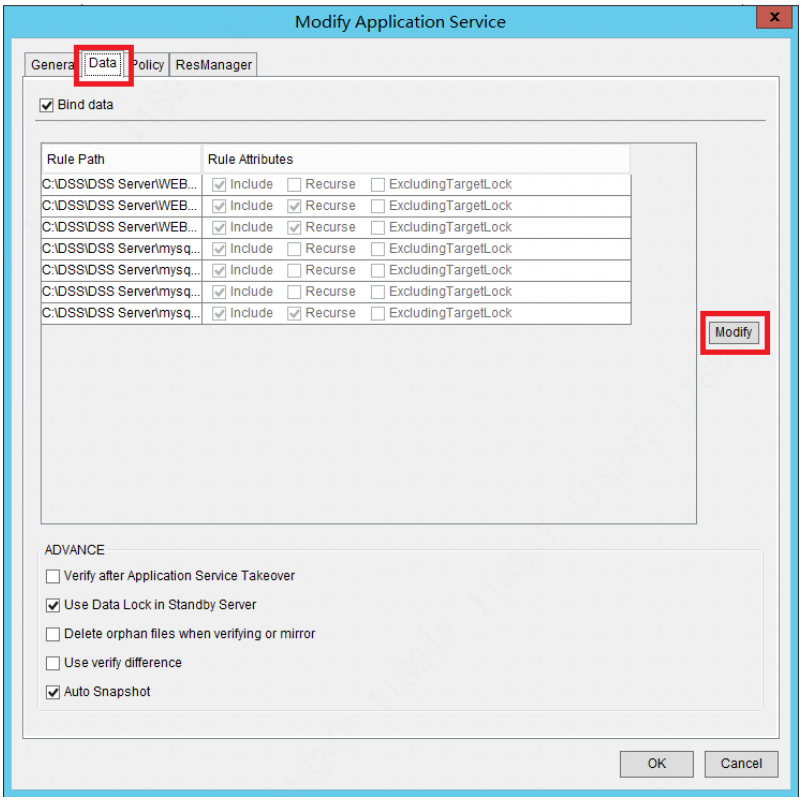


3.3.3.3 Using a Network Disk as a Video Disk

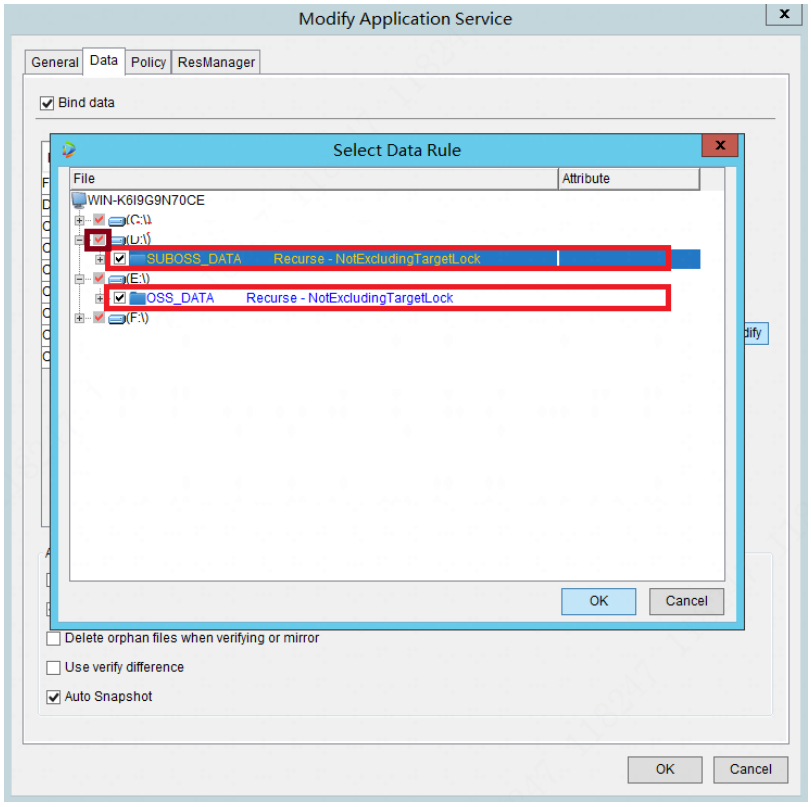
In the hot standby mode, local disks cannot be configured with video disks; otherwise, data cannot be synchronized. To use video storage, you need to add a network disk. Requirements for adding a network disk: **Both the active and standby servers add a disk under the same user of the same EVS as a video disk.** During a hot standby switchover, the corresponding server will automatically take over the video disk to ensure video data synchronization.

3.3.3.4 Configuring or Updating "Binding Data Sources to a Disk"

If the hot standby software is running, select the cube and right-click the service to bring it out. When the service is completely brought out, select **Application Service > Modify/Preview** in the menu bar at the upper right corner of the hot standby software. Then a box will pop up as follows. Click **Modify**.



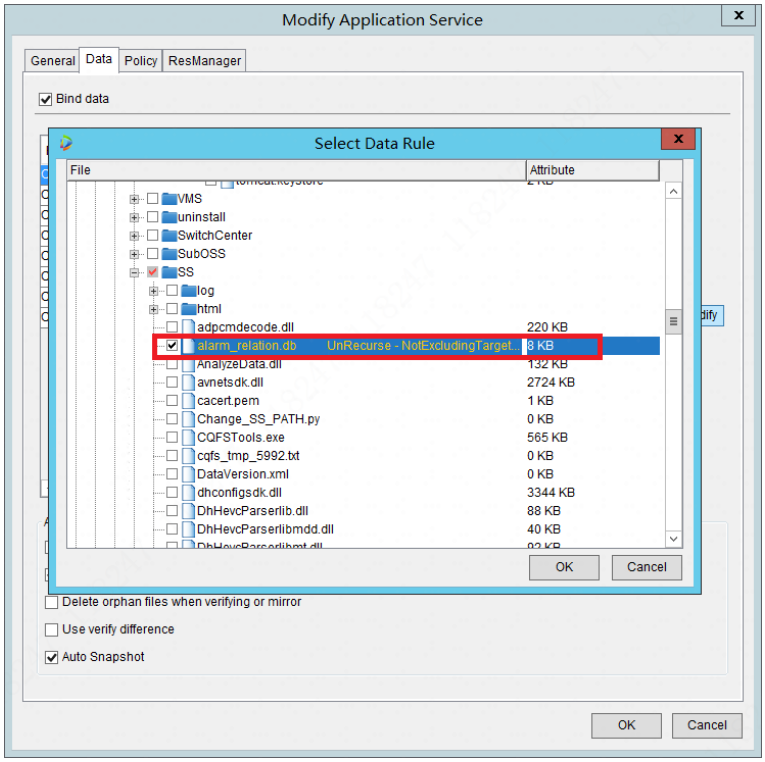
To configure "Binding Data Sources to an Image Disk", select SUBOSS_DATA and OSS_DATA directories (**Select the directory of each folder instead of the entire disk. The check mark for the entire disk is black**). An example of configuring SUBOSS_DATA and OSS_DATA is shown. Perform the same operation for multiple disks.

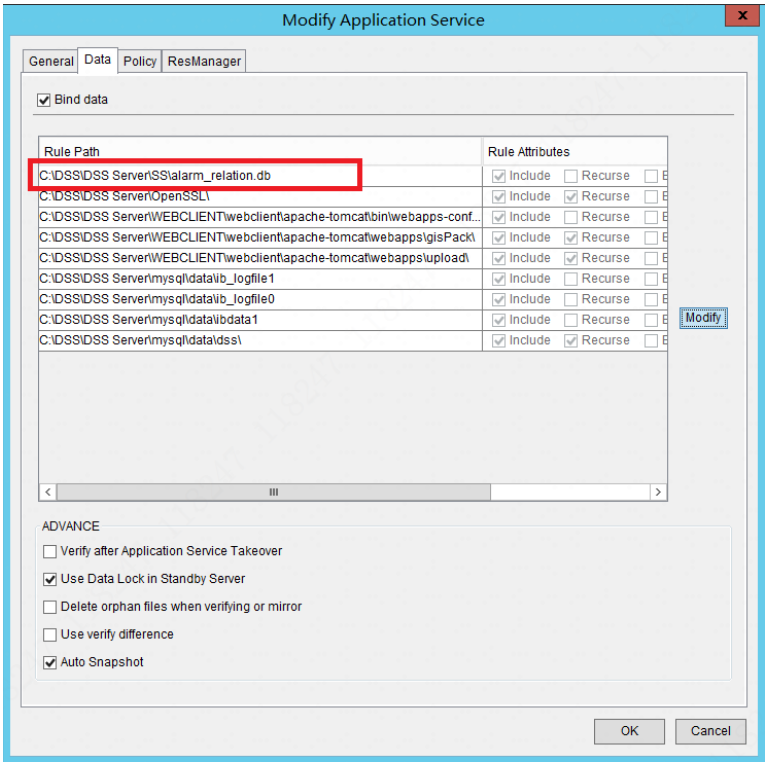


For other disks, configure them as above. When the configuration is complete, click **OK**.

To configure "Binding Data Sources to a Video Disk":

if the hot standby center is used for video storage, you need to configure **C:\DSS\DSS Server\SS\alarm_relation.db** for synchronization. If the **alarm_relation.db file is not found in the SS folder, double-click C:\DSS\DSS Server\SS\DSS_SS.exe. After opening the file, close the pop-up window.**





If you find that the amount of data is large during the deployment process, select "Use verify difference" to optimize the time of secondary verification.

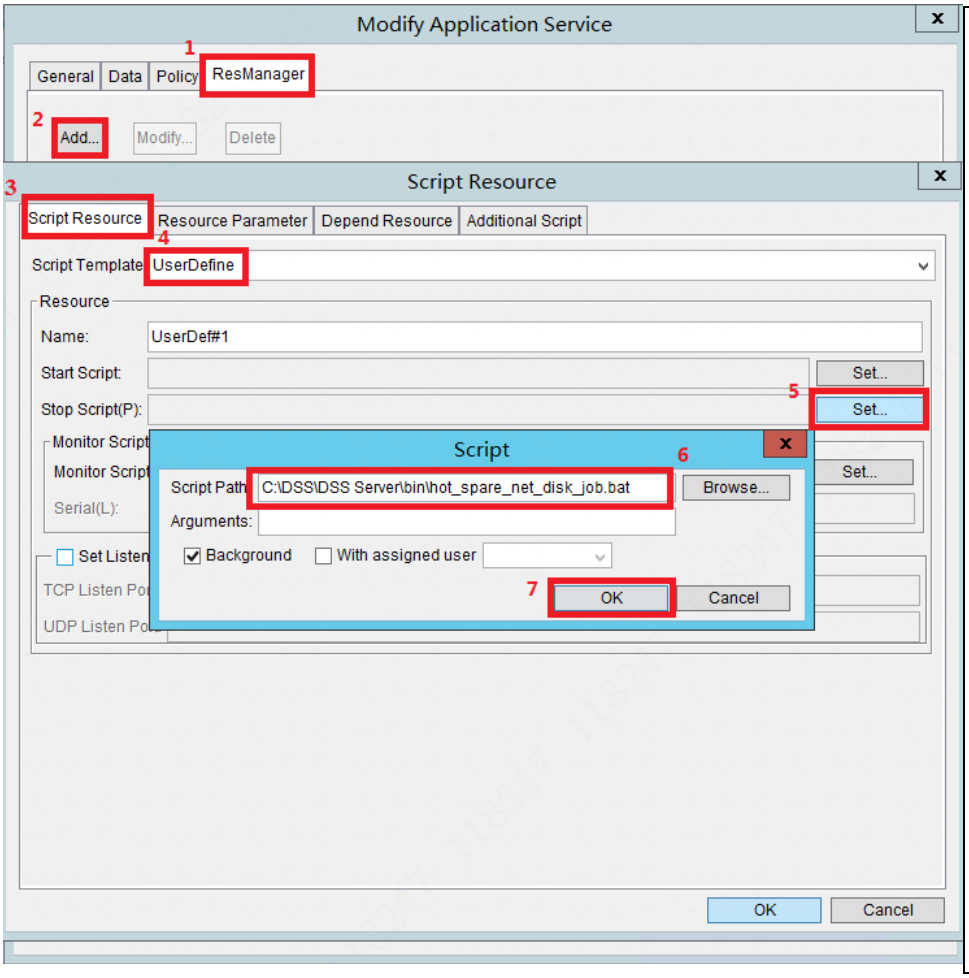
Click **OK** to save the configuration. After the folder configuration is synchronized, you need to configure the disk management script.

Note: When only 5 GB of space is left on the disk, an alert will appear on the Rose software. When only 3 GB is left, data synchronization will stop.

After configuring file synchronization, switch the disk type or delete the disk on the client. You need to update the file synchronization configuration in time. For example, when an F disk is formatted to be a video disk on the active server, if you want to update the binding of data sources, you need to remove the configuration of the F disk.

3.3.3.5 Configuring Scripts to a Network Disk

If a network disk is used for storage, you need to configure script resources for network disk management. This prevents the iSCSI from being disconnected after a server reboot. Detailed steps are listed below:



If the service is not brought out, bring out the service. When the service is completely brought out, select either of the two cubes and in the menu bar at the upper right corner of the hot standby software, select

Application Service

→ **Modify/Preview**

→ **ResManager**

→ **Add**

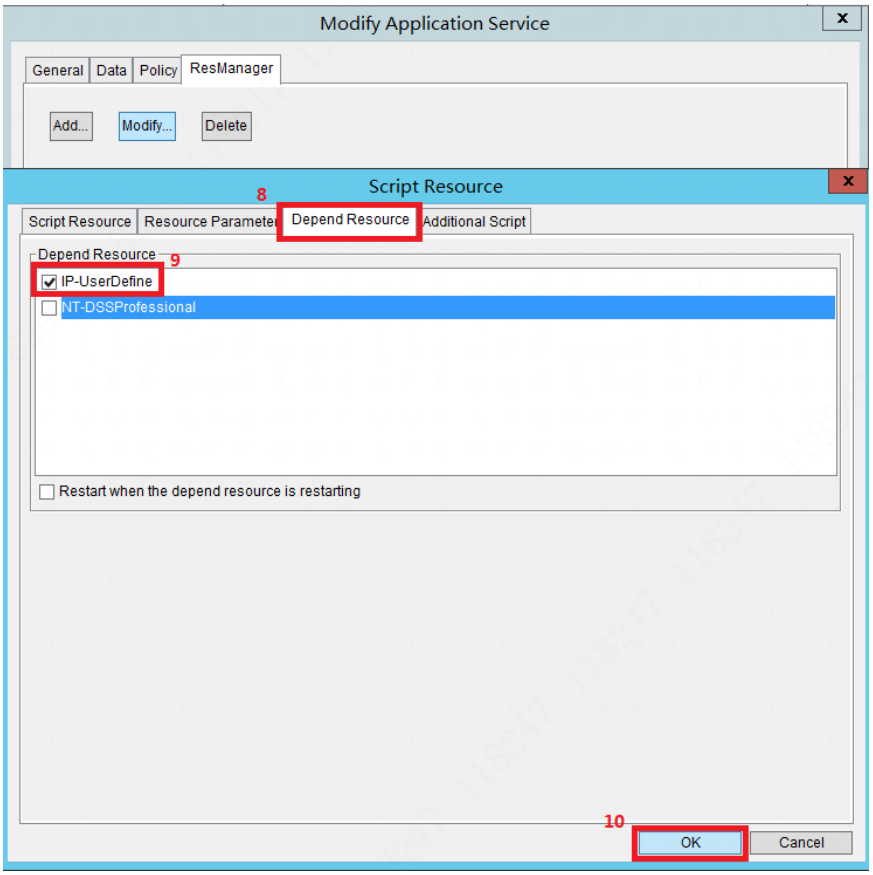
→ **Script Resource**

→Select **UserDefine** in **Script Template**.

→ Set **Stop Script**.

→ Select the script DSSDSS\DSS Server\bin\hot_spare_net_disk_job.bat.

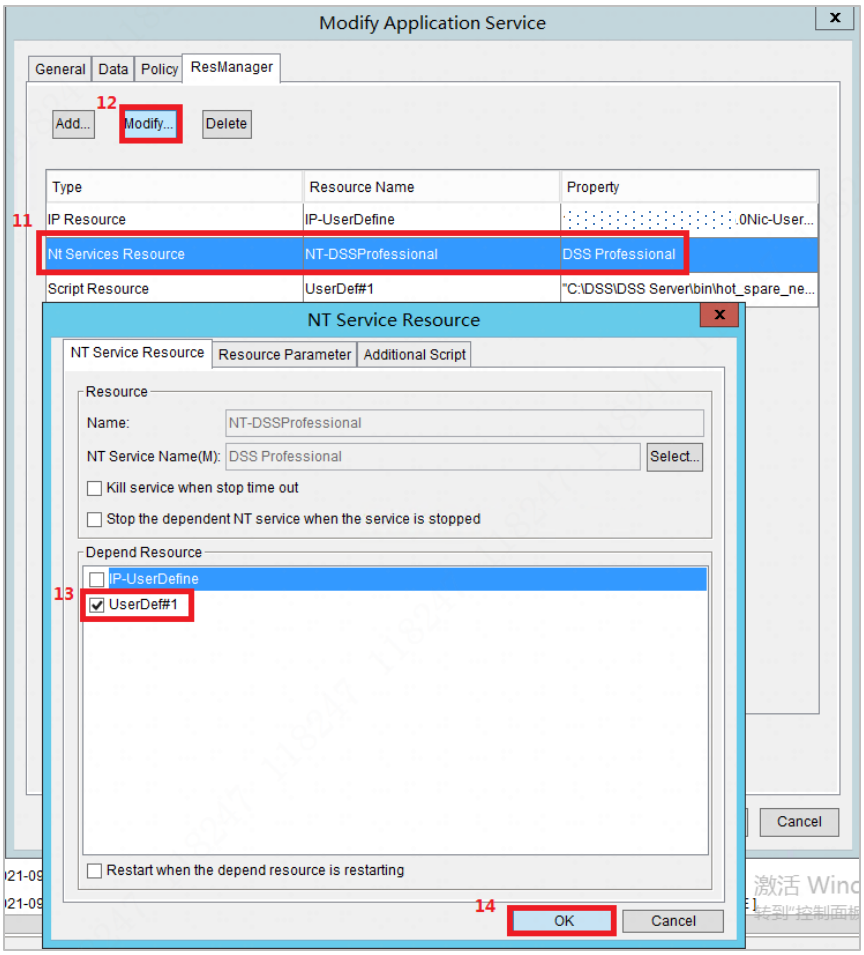
→ Click **OK**, and close the pop-up window of "Script".



Select **Depend Resource**.

→ Select **IP-UserDefine** and then **NT-DSSProfessional**.

→ Click **OK** and close the pop-up window of "Script Resource".



Select **NT Service Resource**.

→ Select **UserDef#1** and then **IP-UserDefine**.

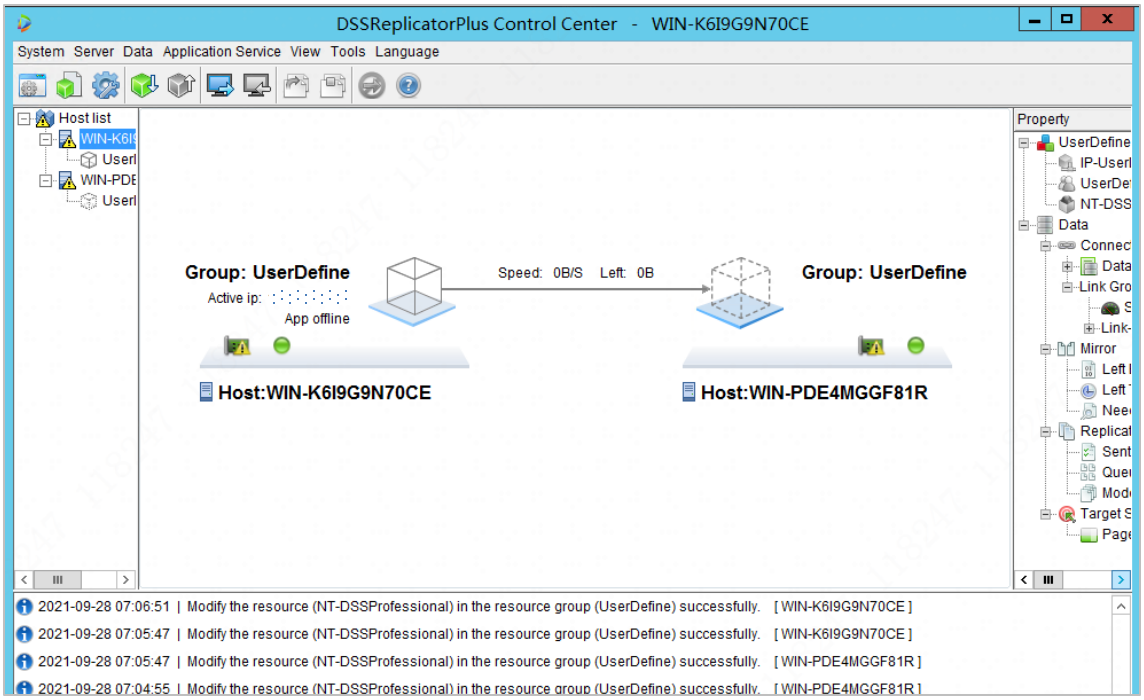
→ Click **OK**, and close **NT Service Resource**.

→ Click **OK**, and close the pop-up window of "Modify Application Service".

The configuration of disk management scripts is complete.

If the binding configuration is not required for other data sources, you can enable the service only by bringing it in on the active server again. At this point, if the data is not synchronized from the active server to the standby server, you can right-click on the cube to switch the data source.

Note: After the data sources have been bound to a disk, **be sure to confirm the data synchronization direction before bringing the service in**. In other words, reconfirm the active and standby servers. As shown below, the data of WIN-K619G9N70CE is synchronized to WIN-PDE4MGGF81R after the service is brought in. The ".disk.info" in WIN-PDE4MGGF81R will be overwritten by WIN-K619G9N70CE, and once the dual servers operate, the image data in WIN-PDE4MGGF81R before the configuration of data source binding cannot be queried.

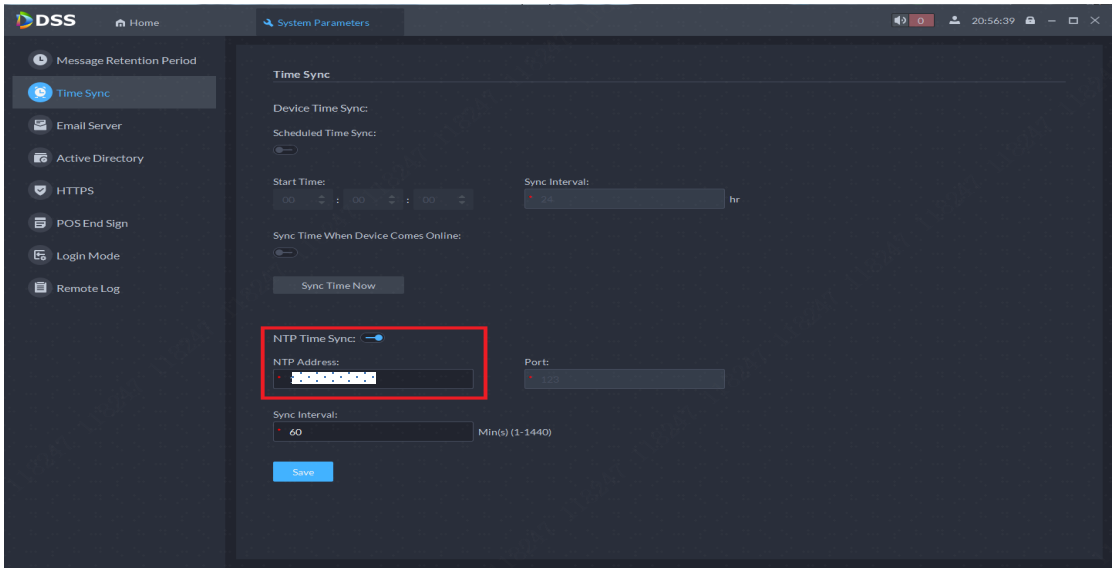


As shown above, if the data synchronization direction is not as expected, you can right-click on the cube and then perform **Switch** to change the data synchronization direction.

3.3.4 Configuring NTP Time Sync (Optional)

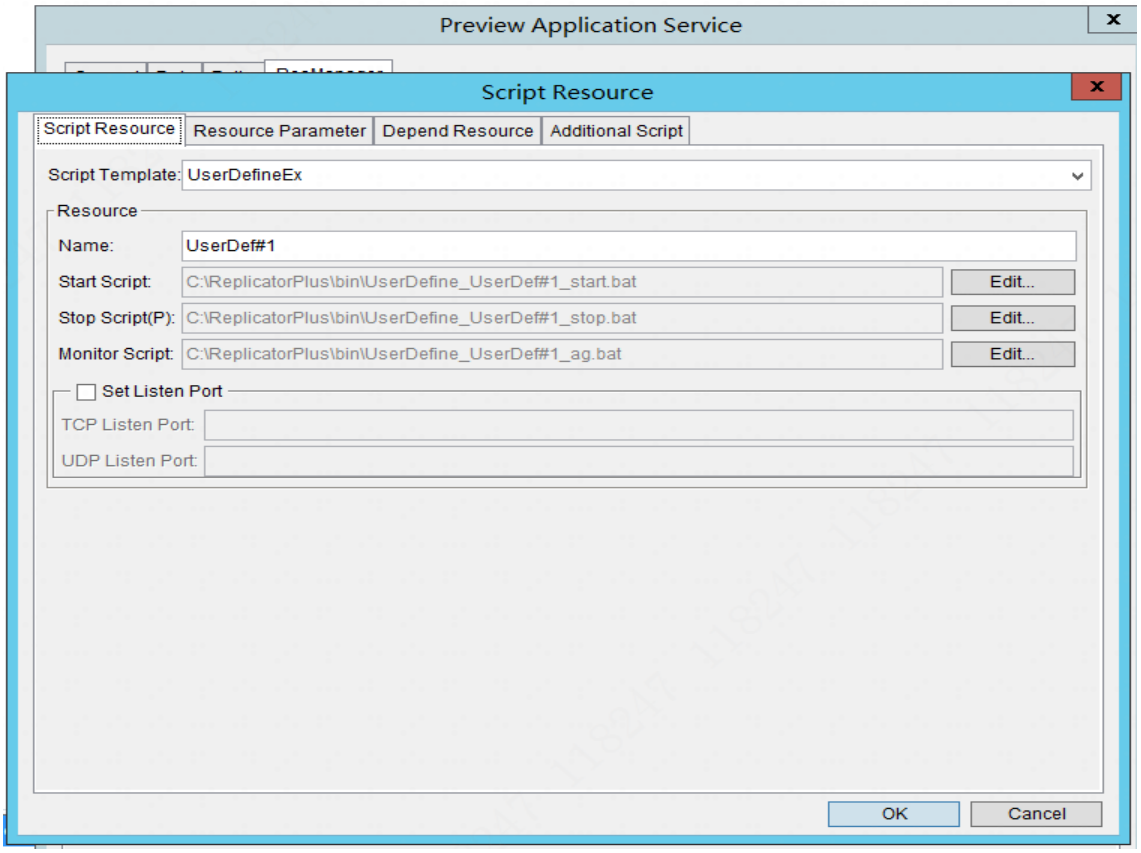
3.3.4.1 Configuring NTP Time Sync on the Active Server Client

NTP Time Sync can only be configured after the hot standby environment has been set up and the license has been imported. To use the NTP Time Sync in V8 and later, you need to enable the NTP Time Sync on the active and standby servers, log in to the active server client, and configure the **NTP Address** in **System Parameters**, as shown below.

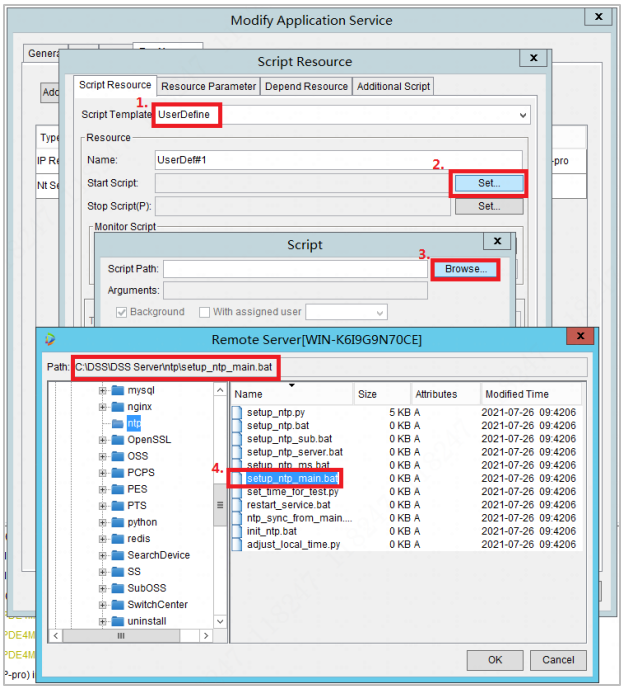


3.3.4.2 Configuring Scripts for NTP Time Sync

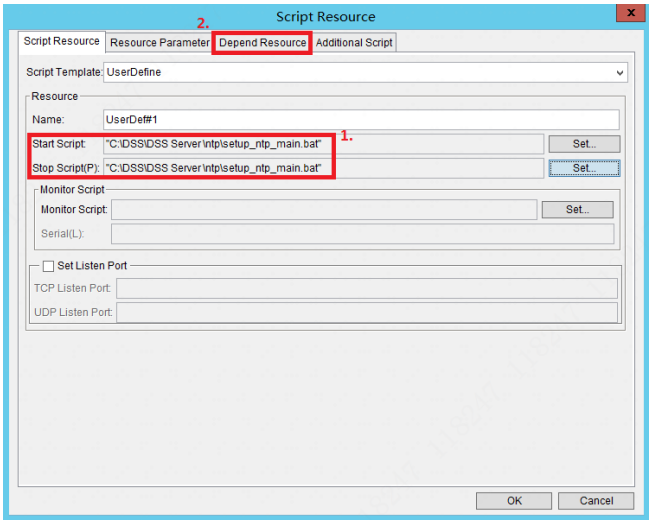
After the configuration is complete, bring out the service. When the service is completely brought out, select **Application Service > Modify/Preview > ResManager > Add > Script Resource** in the menu bar at the upper right corner of the hot standby software. Then a box will pop up as follows.

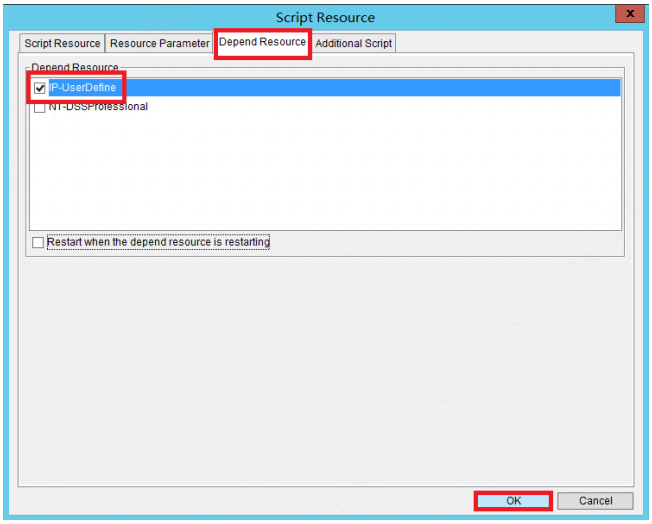


Select **UserDefine** in **Script Template**, and configure **Start Script** and **Stop Script** separately. The path of **Start Script** is C:\DSS\DSS Server\ntp\setup_ntp_main.bat, and the path of **Stop Script** is C:\DSS\DSS Server\ntp\setup_ntp_sub.bat.



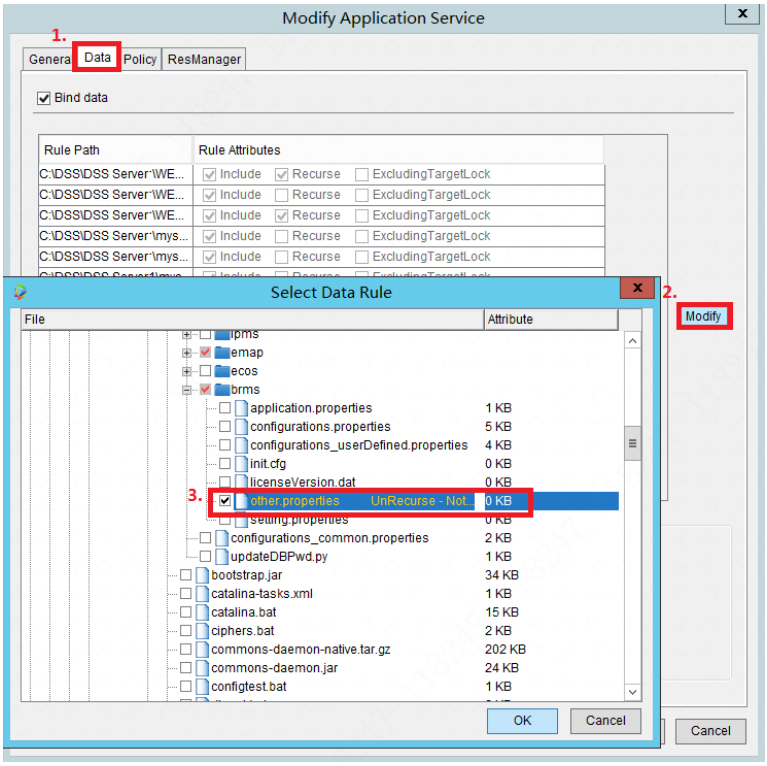
Then click **Depend Resource** to configure.



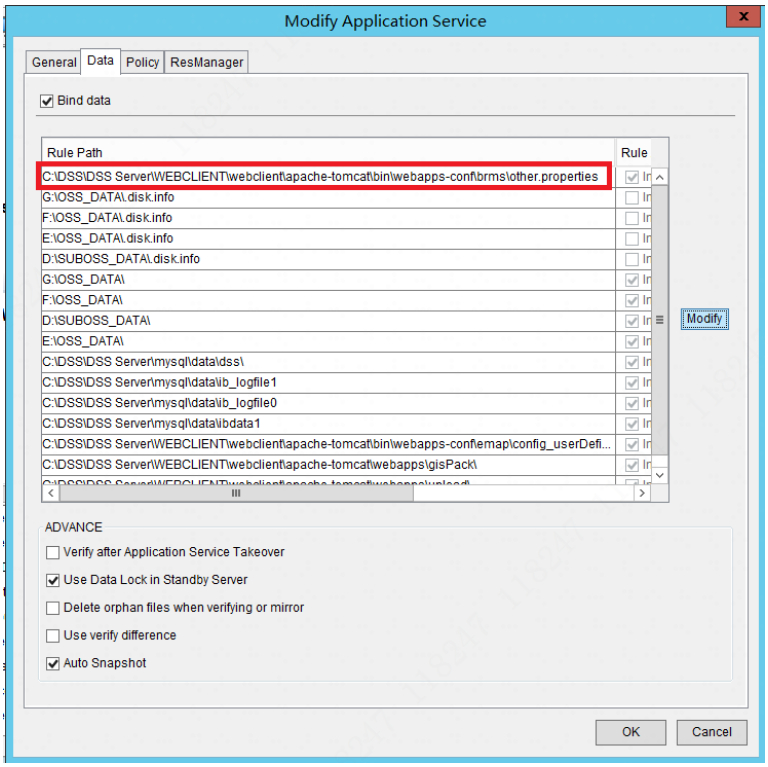


3.3.4.3 Binding the Data Sources of NTP Time Sync

After NTP scripts are configured, select **Data**, and click **Modify**. Select **C:\DSS\DSS Server\WEBCLIENT\webclient\apache-tomcat\bin\webapps-conf\brms\other.properties**, and click **OK**, as shown below.



You can see one more file in the folder. Click **OK**.



If the configuration is not required for other data sources, you can use the NTP Time Sync only by bringing in the service again.

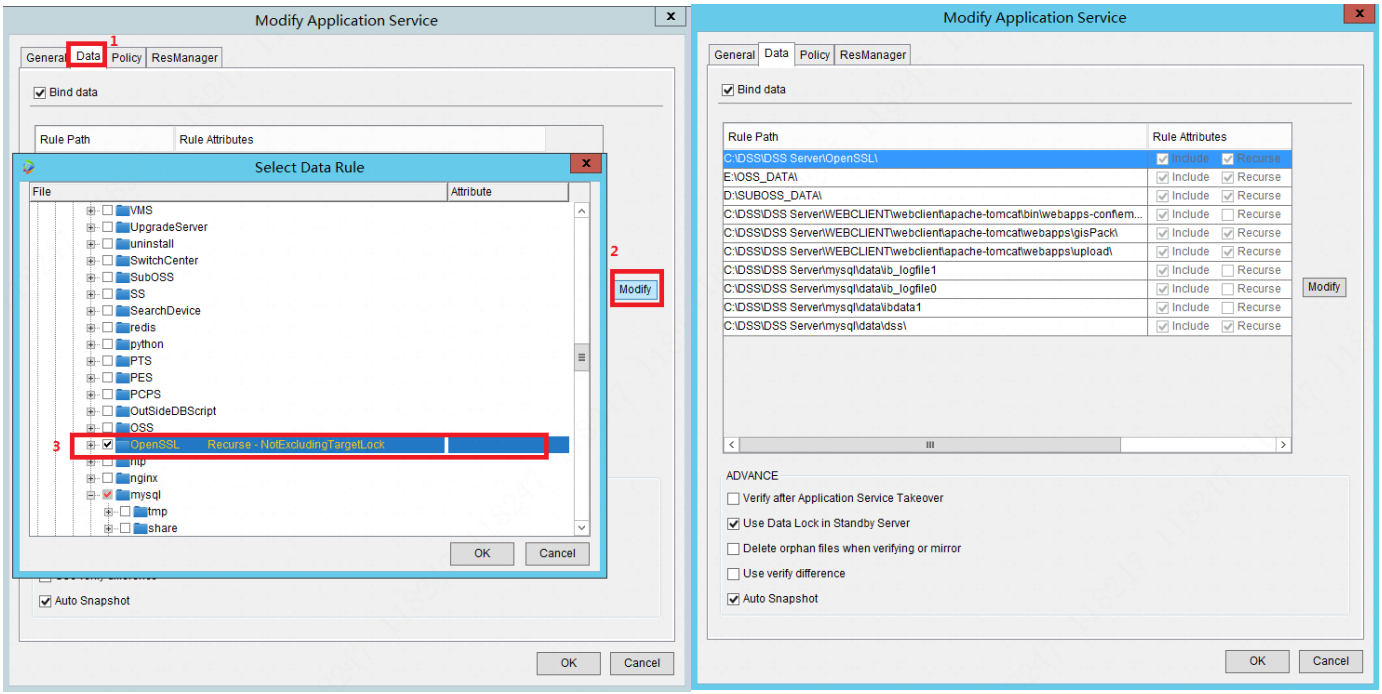
3.3.5 Configuring WebClient License (Optional)

For V8.000.0000004.0 and earlier versions that do not support WebClient, ignore the following configuration.

WebClient needs to be deployed on both the active and standby servers, and the DSS service needs to be stopped during deployment. The WebClient can be deployed before the hot standby is set up. If the WebClient is deployed after the hot standby is set up, you need to bring out the service. After the active and standby servers are deployed, you need to configure the scripts and synchronize the SSL licenses to make sure that the licenses of the active and standby servers are the same. This can avoid reinstalling the licenses when the standby server is running.

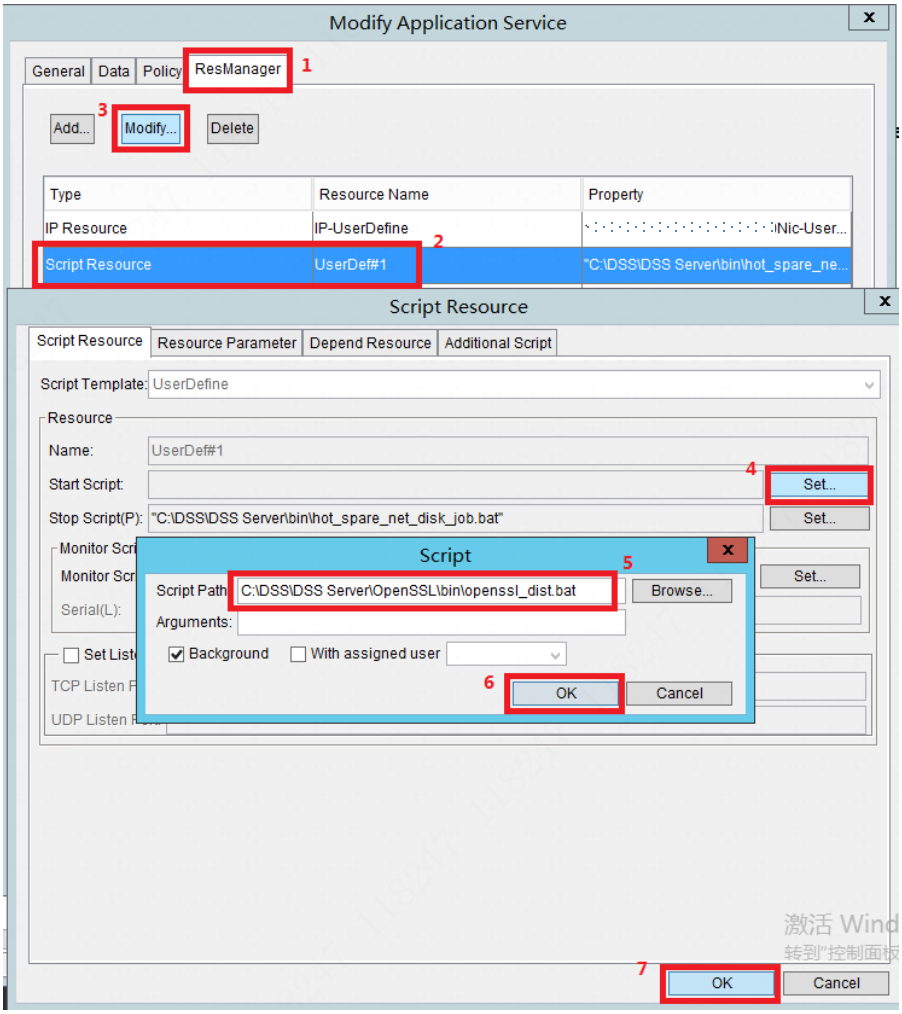
1. Configuring the Synchronization of OpenSSL Folder: DSS\DSS Server\OpenSSL

If the hot standby software is running, select the cube and right-click the service to bring it out. When the service is completely brought out, select **Application Service > Modify/Preview > Data > Modify** in the menu bar at the upper right corner of the hot standby software.



2. Configuring the Synchronization of License Script: C:\DSS\DSS Server\OpenSSL\bin\openssl_dist.bat

Application Service > Modify/Preview > ResManager



If you have previously configured a disk management script, there will be a script resource of "UserDef#1". Select the script and click **Edit**.

→ In **Start Script**, configure the script DSS\DSS Server\OpenSSL\bin\openssl_dist.bat.

→ Click **OK**, and close the pop-up window of "Script".

→ Click **OK** and close the pop-up window of "Script Resource".

The configuration of the WebClient script is complete. If the configuration is not required for other resources, bring in the service to enable it.

If the resource of "UserDef#1" does not exist, see Configuring Scripts to a Network Disk. After adding the resource, configure DSS\DSS Server\OpenSSL\bin\openssl_dist.bat in **Start Script**. Be sure to modify the dependency of the added resource. "NT-DSSProfessional" depends on "UserDef#1", and "UserDef#1" depends on "IP-UserDefine".

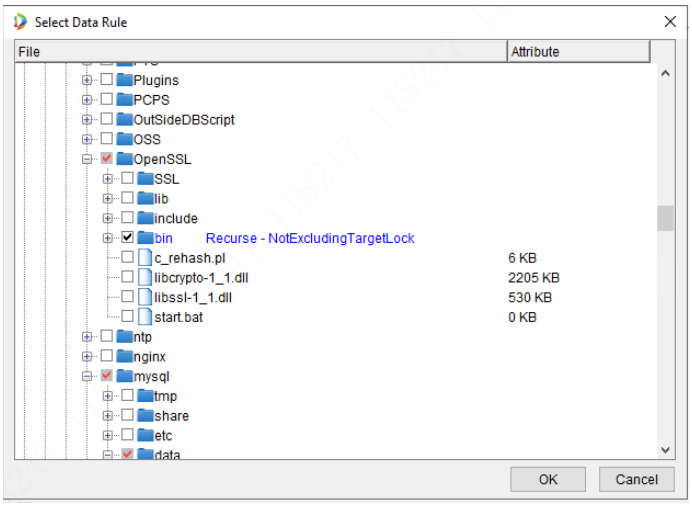
3.3.6 Configuring CA License (Optional)

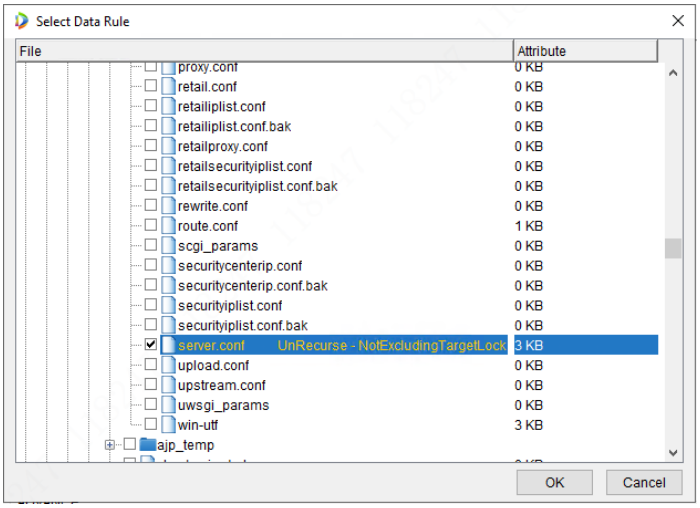
If you use CA License function, you need to configure the Synchronization of License.

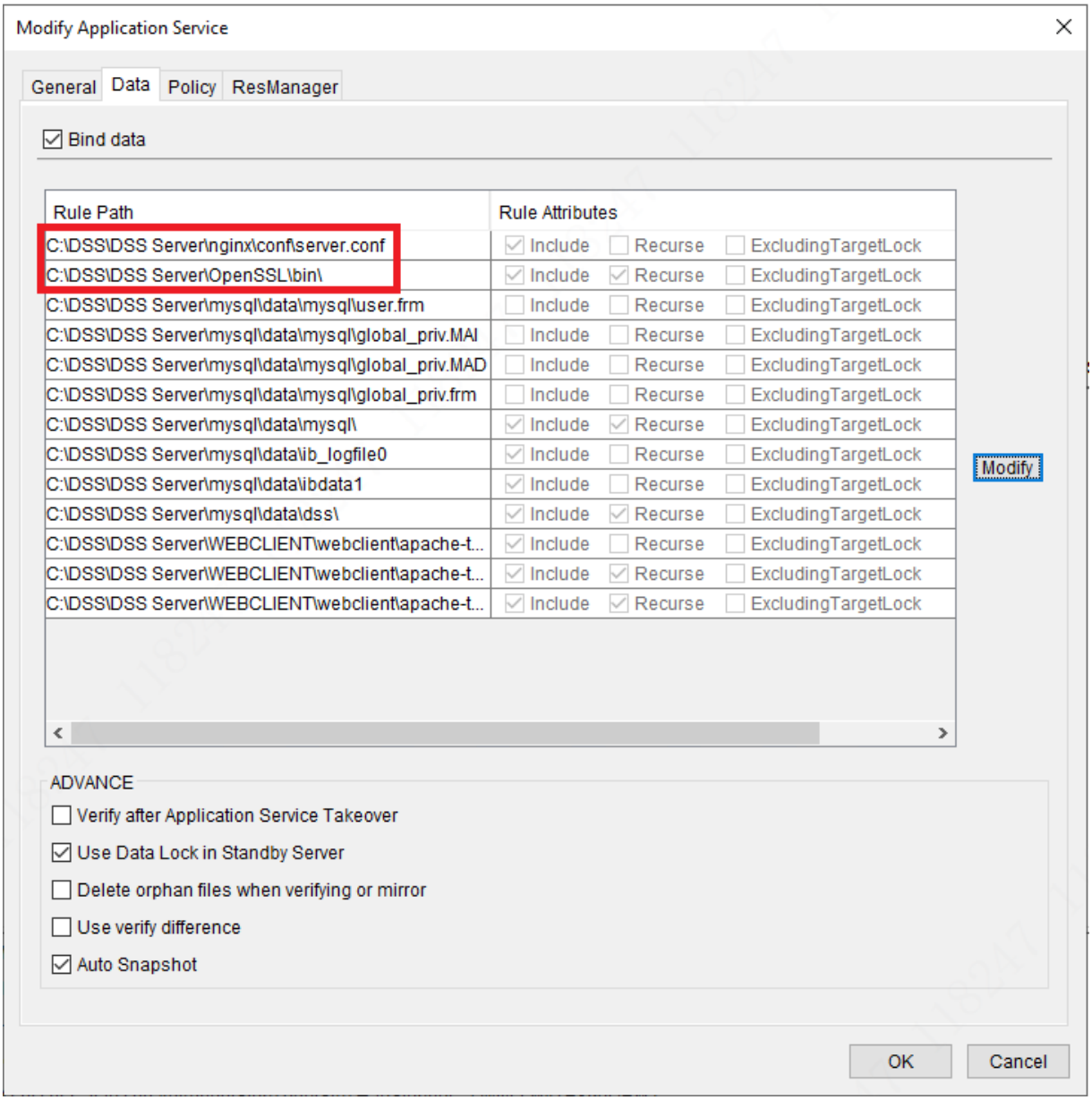
You need to synchronize the SSL licenses to make sure that the licenses of the active and standby servers are the same. This can avoid reinstalling the licenses when the standby server is running.

1. Configuring the Synchronization of OpenSSL Folder: DSS\DSS Server\OpenSSL\bin 、 DSS\DSS Server\nginx\conf\server.conf

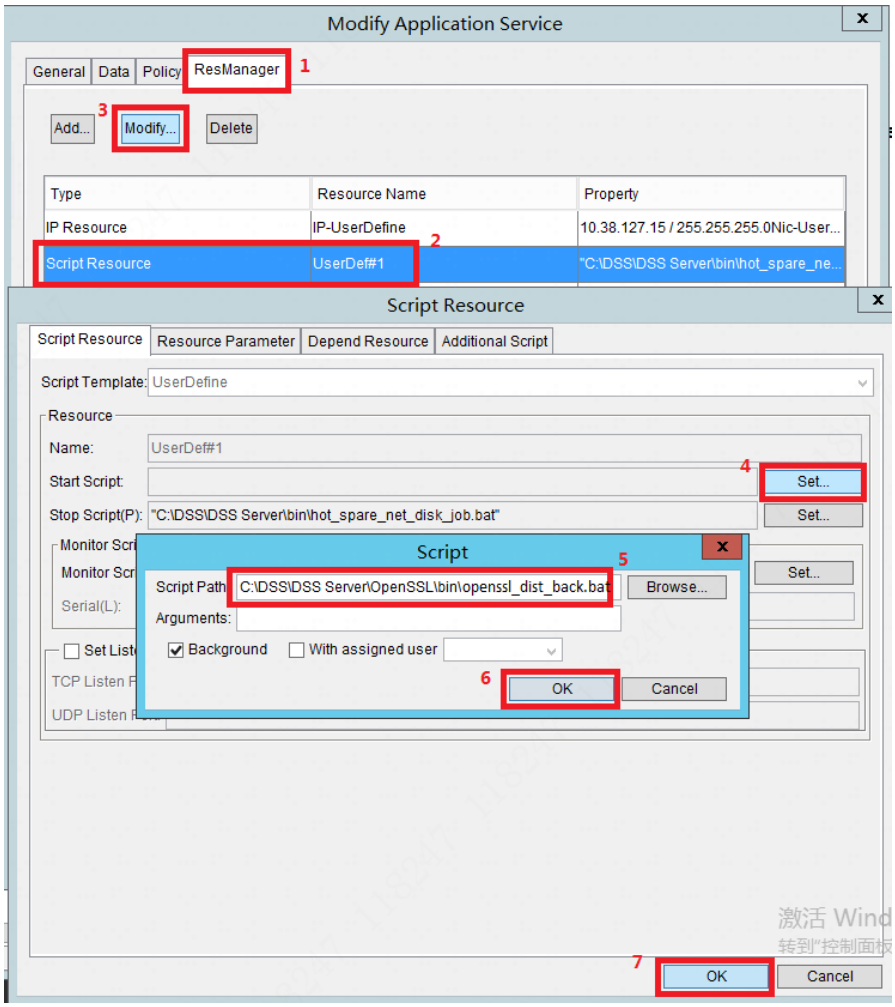
If the hot standby software is running, select the cube and right-click the service to bring it out. When the service is completely brought out, select **Application Service > Modify/Preview > Data > Modify** in the menu bar at the upper right corner of the hot standby software.







2. Configuring the Synchronization of License Script: C:\DSS\DSS Server\OpenSSL\bin\openssl_dist_back.bat Application Service > Modify/Preview > ResManager



If you have previously configured a disk management script, there will be a script resource of "UserDef#1". Select the script and click **Edit**.

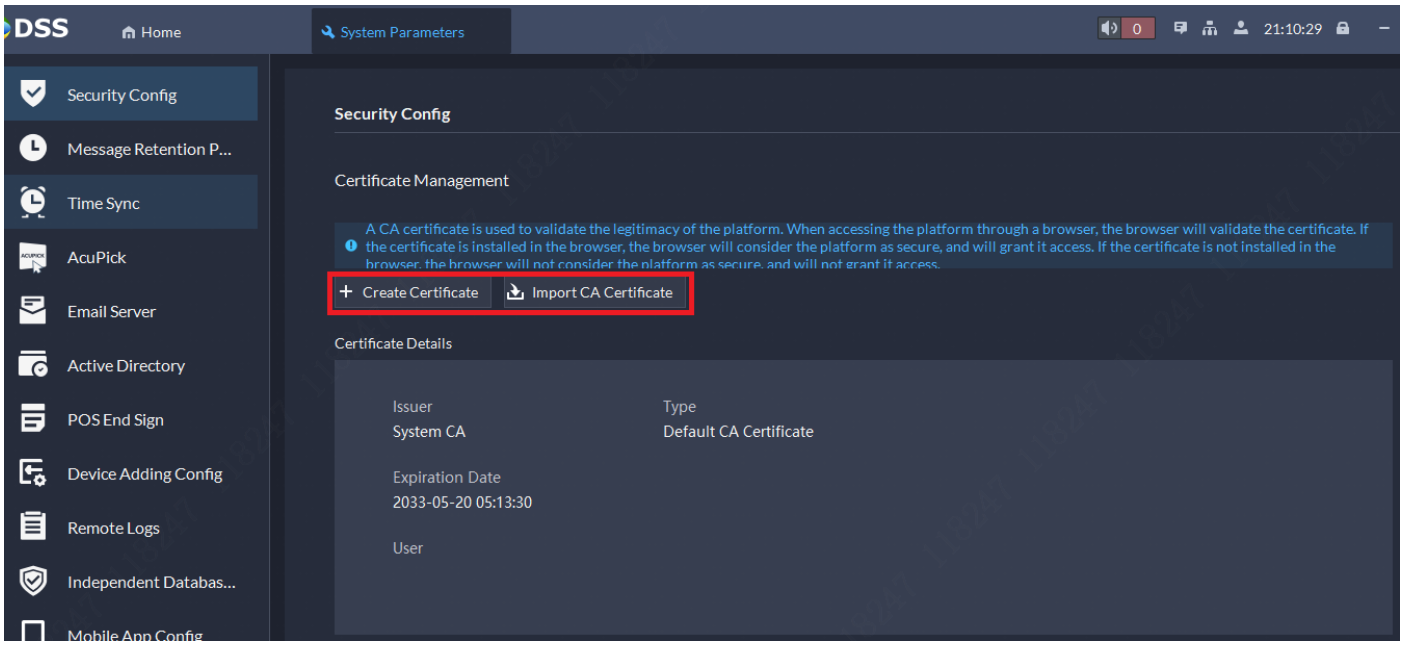
→ In **Start Script**, configure the script DSS\DSS Server\OpenSSL\bin\openssl_dist.bat.

→ Click **OK**, and close the pop-up window of "Script".

→ Click **OK** and close the pop-up window of "Script Resource".

The configuration of the WebClient script is complete. If the configuration is not required for other resources, bring in the service to enable it.

3. Generating or importing CA Certificate on the client

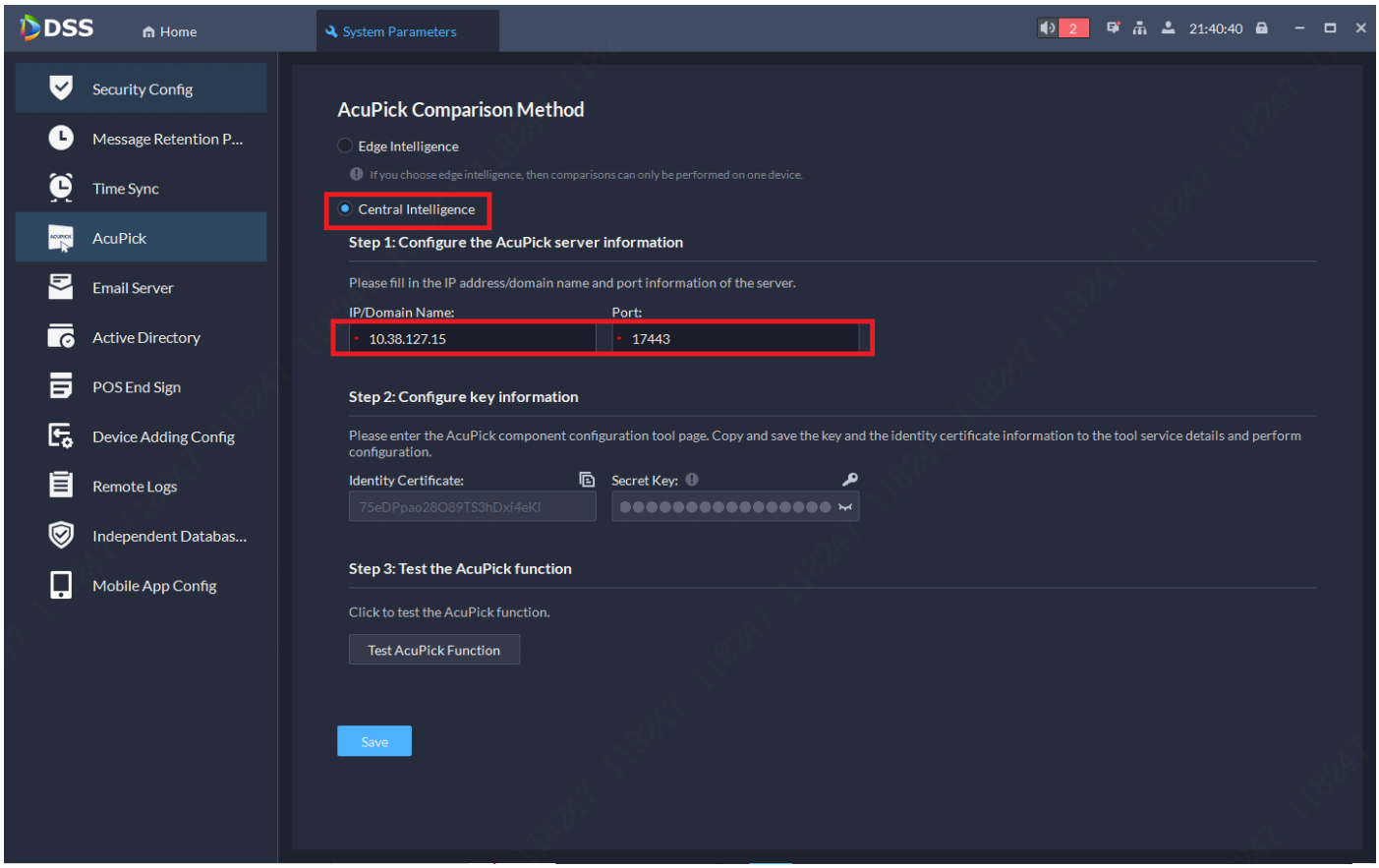


3.3.7 Configuring AcuPick Components (Optional)

Ignore AcuPick independent deployment. If AcuPick components are centrally deployed in Hot Standby software， then the active and standby servers need to be installed with AcuPick components, and their ports of AcuPick service should keep the same.

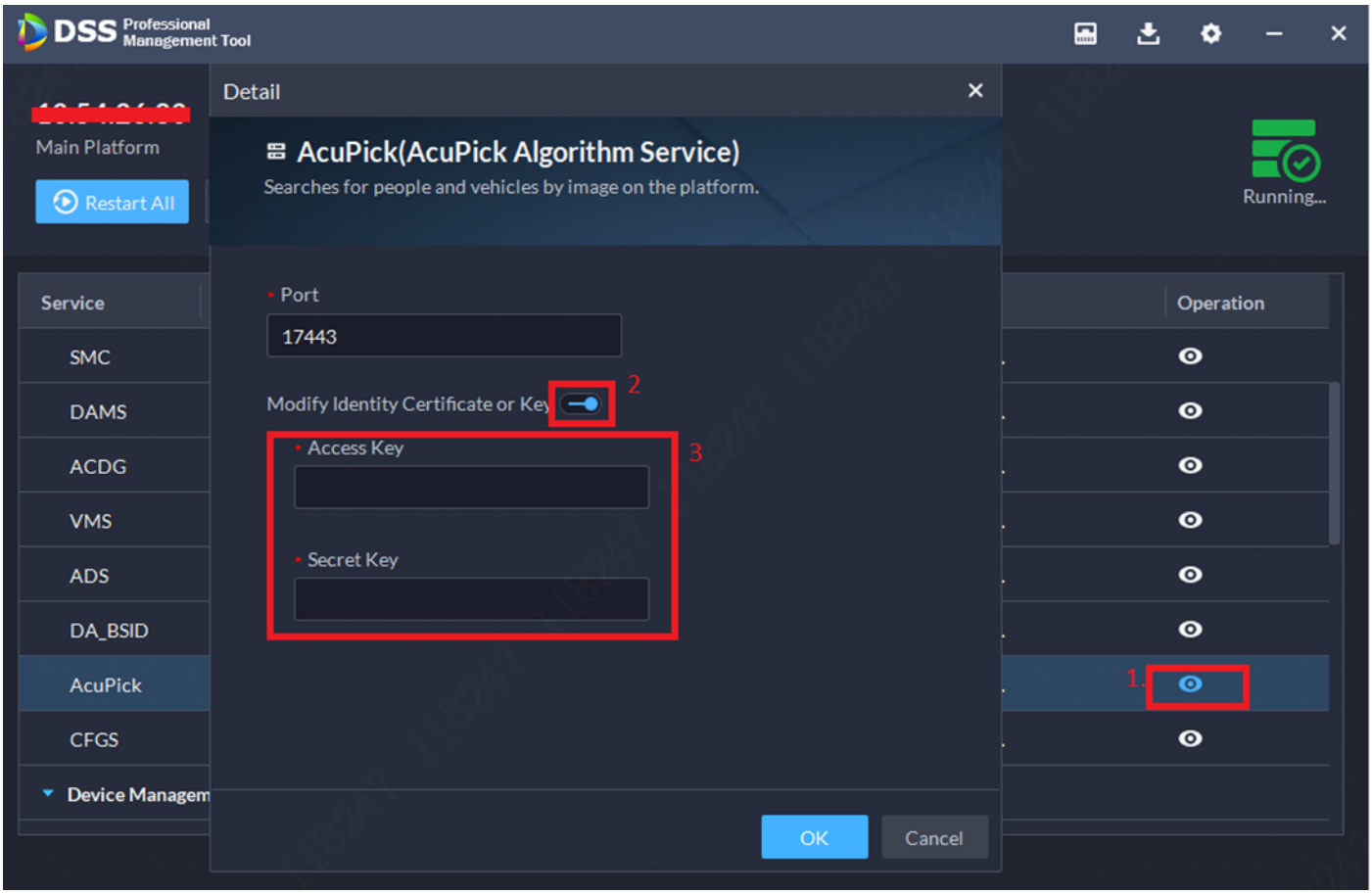
1. Configure AcuPick on Client

Select “Central Intelligence”, configure IP and port, and configure “IP/Domain Name” as VIP。



2. Configure the private key on AcuPick

Configure the key of Client on the configuration tools of the active and standup servers. As shown below.


DSS Professional Management Tool
Main Platform
Restart All
Running...
Service
Operation
SMC
DAMS
ACDG
VMS
ADS
DA_BSID
AcuPick
CFGS
Device Managem
Detail
AcuPick(AcuPick Algorithm Service)
Searches for people and vehicles by image on the platform.
Port
17443
Modify Identity Certificate or Key
Access Key
Secret Key
1.
2
3
OK
Cancel

4 Main Features of Hot Standby Software

4.1 Selecting the Data Consistency Policy

You need to configure the consistency policy before bringing in the service, otherwise, you may not be able to re-configure it.

There are two main types of data consistency policies for the hot standby as follows.

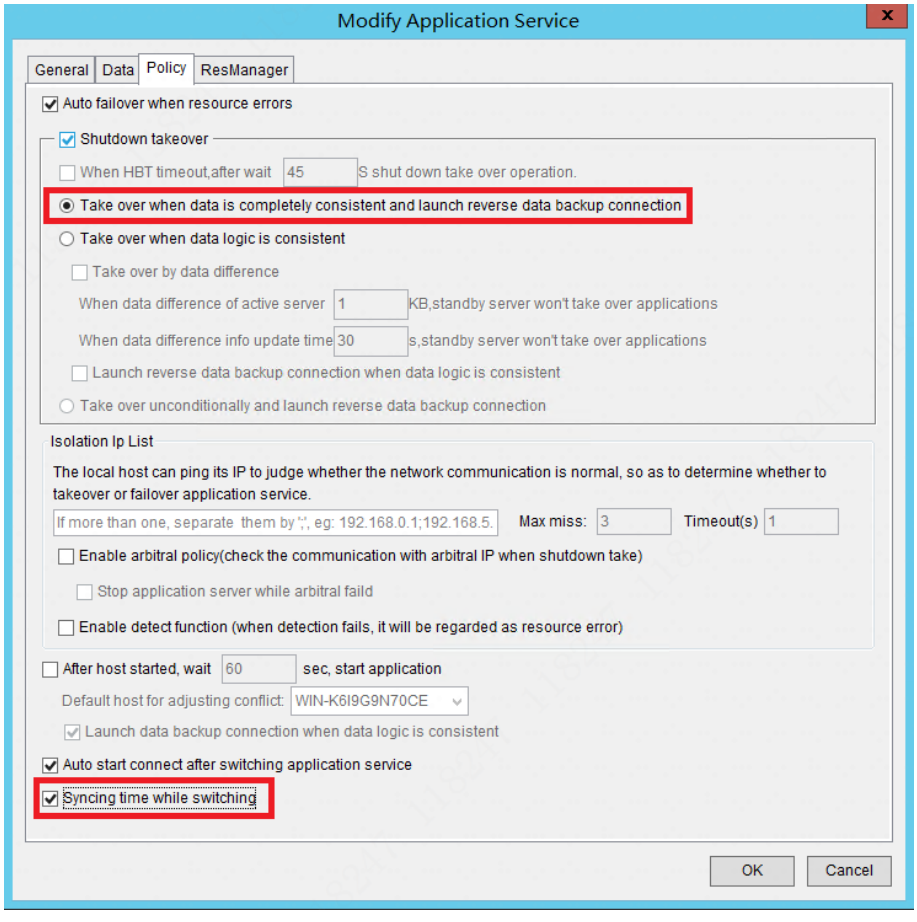
- Complete data consistency policy (Default)

Features: It can be ensured that the data of the active and standby servers are completely consistent, but in extreme cases, the standby server may not take over.

- Logic data consistency policy (Recommended)

Features: It cannot be ensured that the data of the active and standby servers are completely consistent. In extreme cases, data may be lost in milliseconds. But the continuity of services can be ensured.

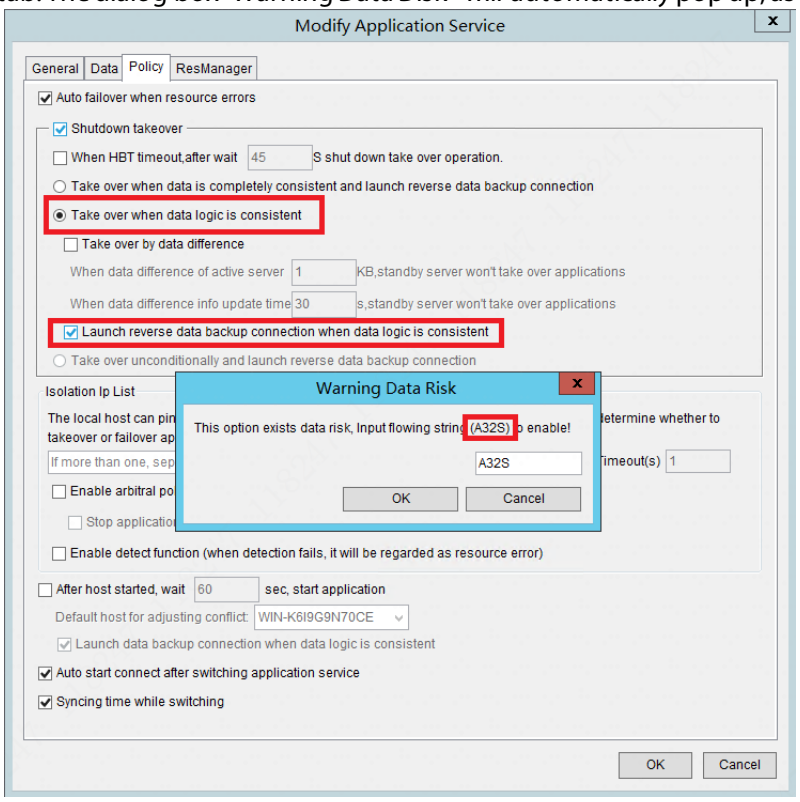
Because the complete data consistency policy configured by default takes data as a top priority, the standby server will not take over in case of data inconsistency. In extreme cases such as a power failure on the active server or sudden network disconnection, the data on the active server may not be transferred to the standby server in time, so the standby server may not take over. The default consistency policy is shown as follows.



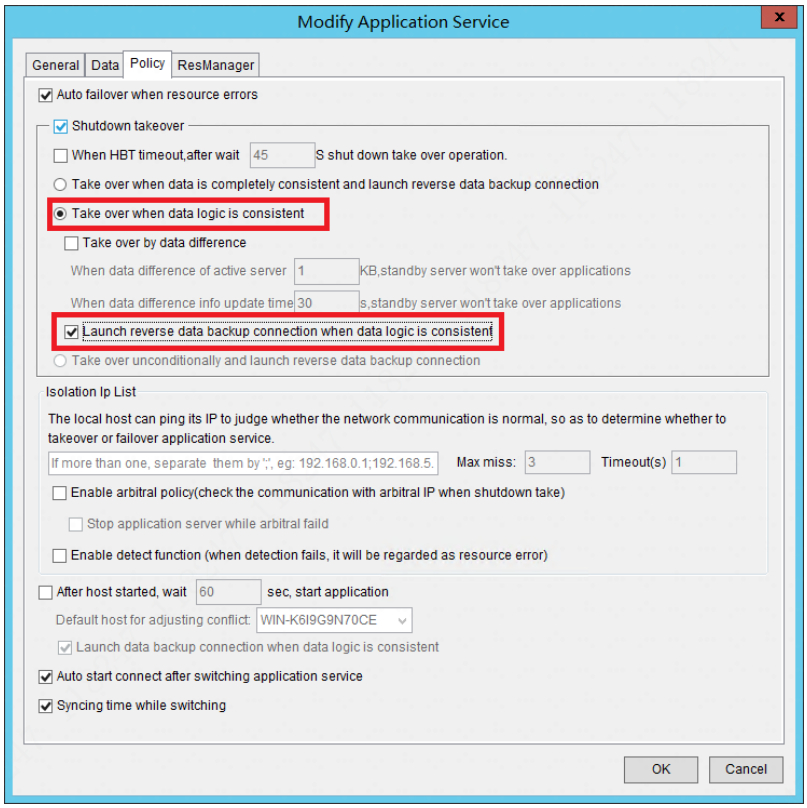
If you are very concerned about the service continuity, you can enable the logic data consistency policy, launch a reverse data backup connection as required, and manually configure the Syncing time while switching.

The configuration of logical consistency policy is shown as below:

Select "Take over when data logic is consistent" and "Launch reverse data backup connection when data logic is consistent" under the "Policy" tab. The dialog box "Warning Data Disk" will automatically pop up, as shown below.



Enter the default content in brackets in the dialog box prompt and click **OK**. After the configuration is complete, the interface as shown below will appear.



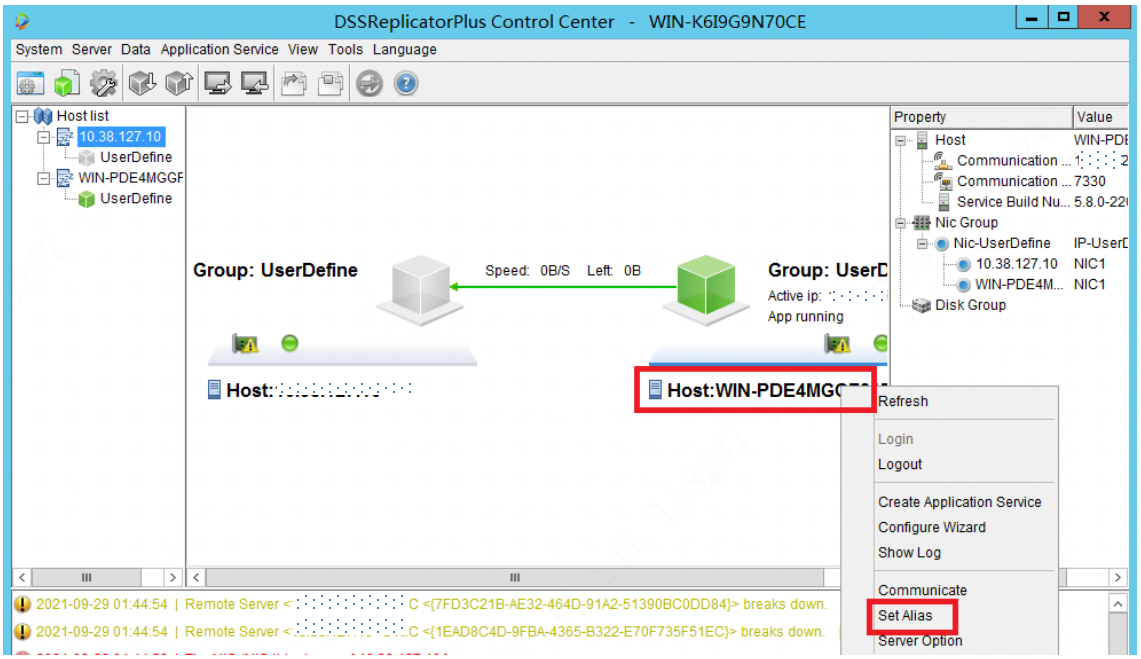
Click **OK** to close the dialog box.

Click to Back to Configuring Data Consistency Policies in **Setup of Hot Standby** to continue the setup of the hot standby.

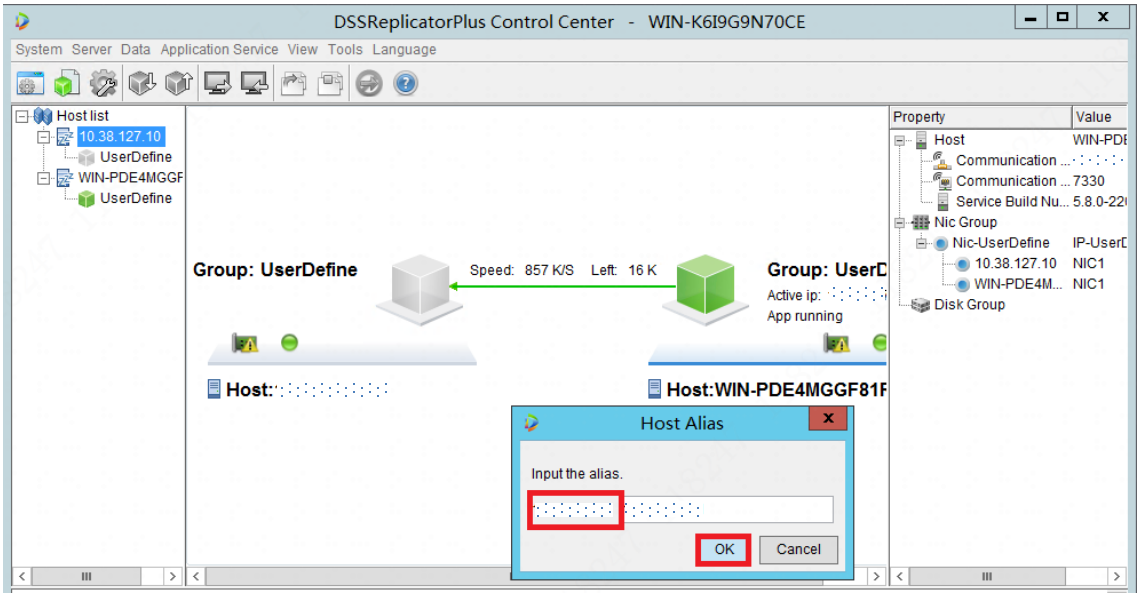
4.2 Setting Alias

To distinguish the two servers in a more intuitive way in the control center, you can modify the host name to an IP address and perform the operation without bringing out the application.

Right-click the **Host**, and select **Set Alias**.



Set the alias to an IP address. Confirm and save it.



4.3 Bringing in Application Service Resources

The "bring in" operation is to activate the hot standby. All the VIP services and data protection configured on the hot standby will be activated. This operation can mount a VIP on the active server, enable the services of the active server, and synchronize the data on the active server to the standby server for real-time protection. The active and standby servers don not remain unchanged. They can switch rules.

The "bring in" operation is to activate relevant services on the active server in the current cluster, no matter the operation is performed on the iron of the active server or the iron of the standby server. Therefore, before performing the "bring in" operation, you need to make sure that the server with the latest data is running as the active server. This can prevent data

from being overwritten. **If the latest data is located in the active server, perform the "bring out" operation, switch the rules of the active and standby servers, and then perform the "bring in" operation**. For the "switchover", "bring out", and other operations, see Section 2 and 3.

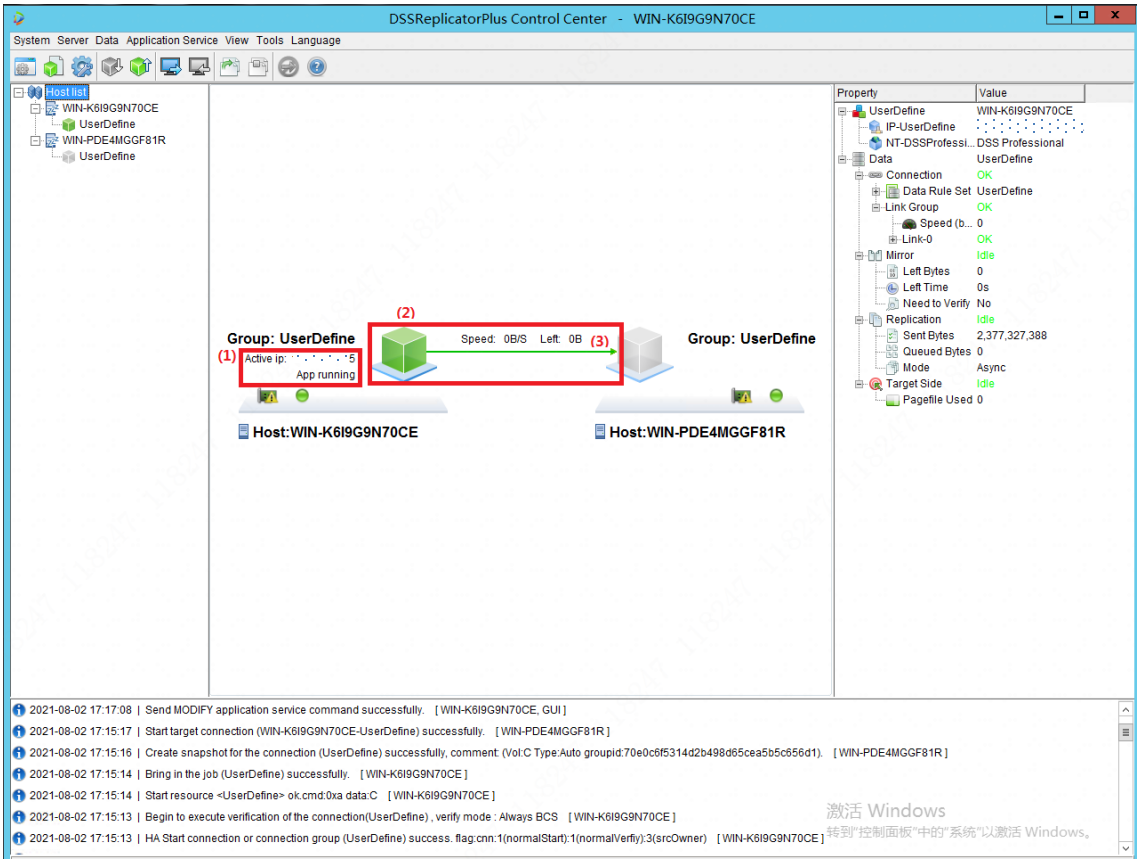
In the status panel of DSSReplicatorPlus Control Center, check if the current server is the active server using the following four methods, as shown in the following two figures.

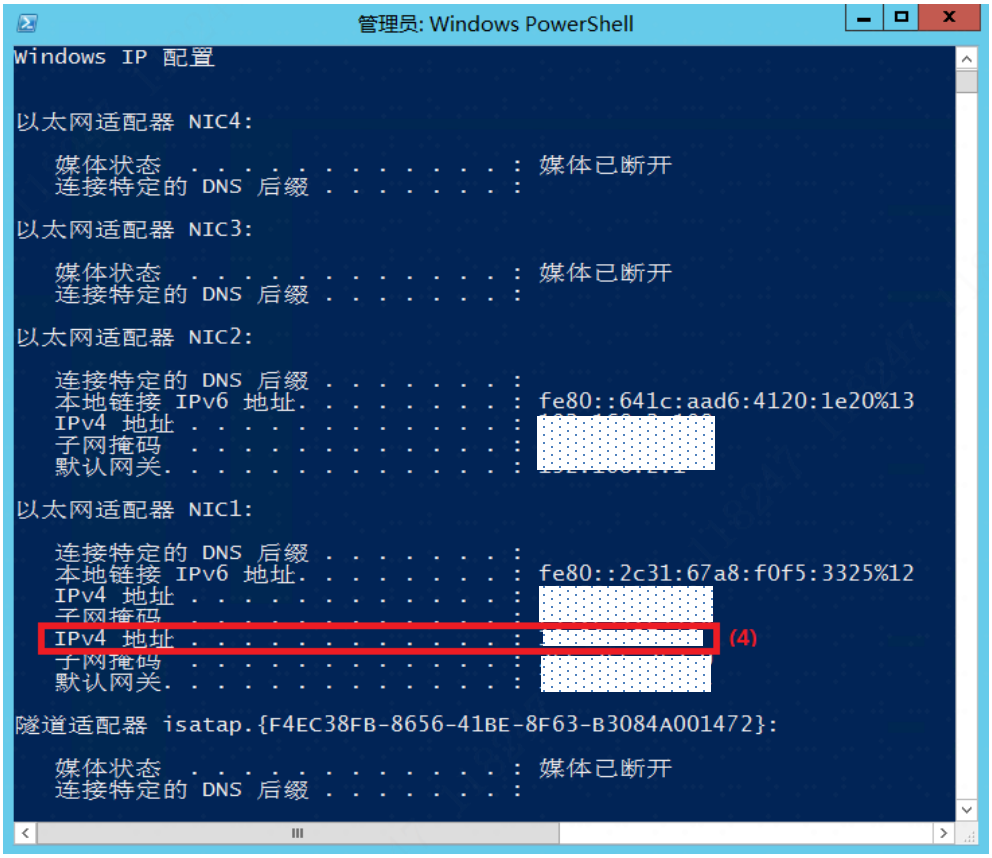
(1) The server where "Active ip" is located is the active server.

(2) The server with a cube icon of high brightness is the active server.

(3) The arrow in the icon is always pointed from the active server to the standby server.

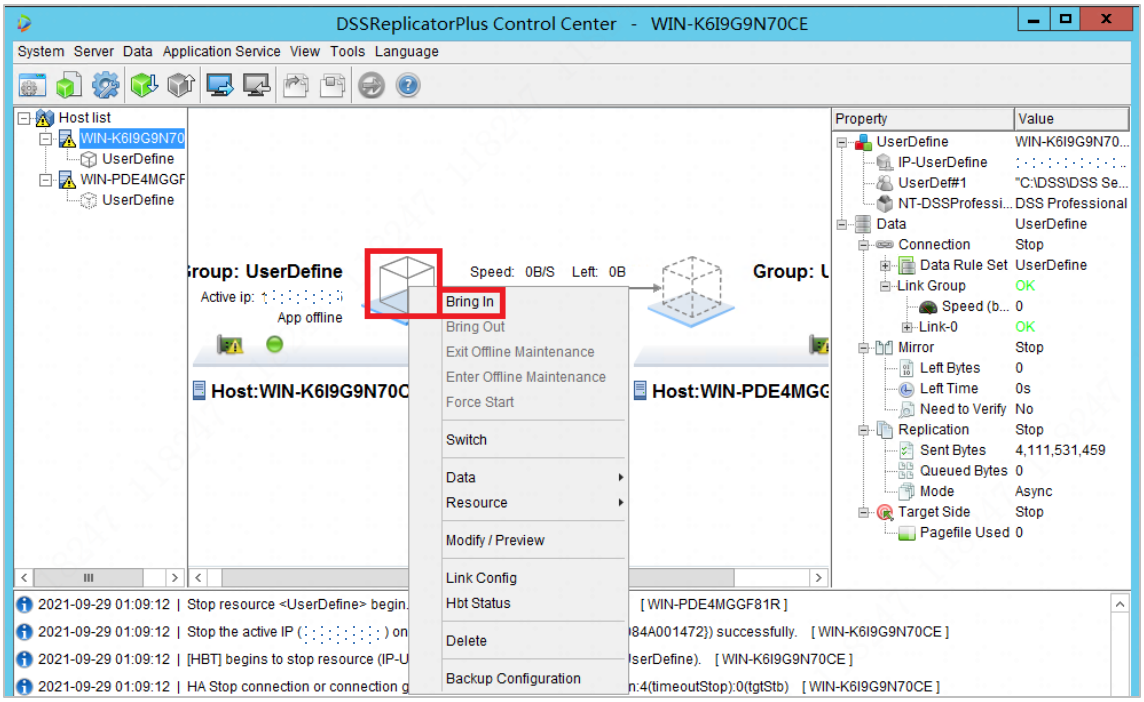
(4) Enter "ipconfig" in CMD, and the result with a VIP is the active server.



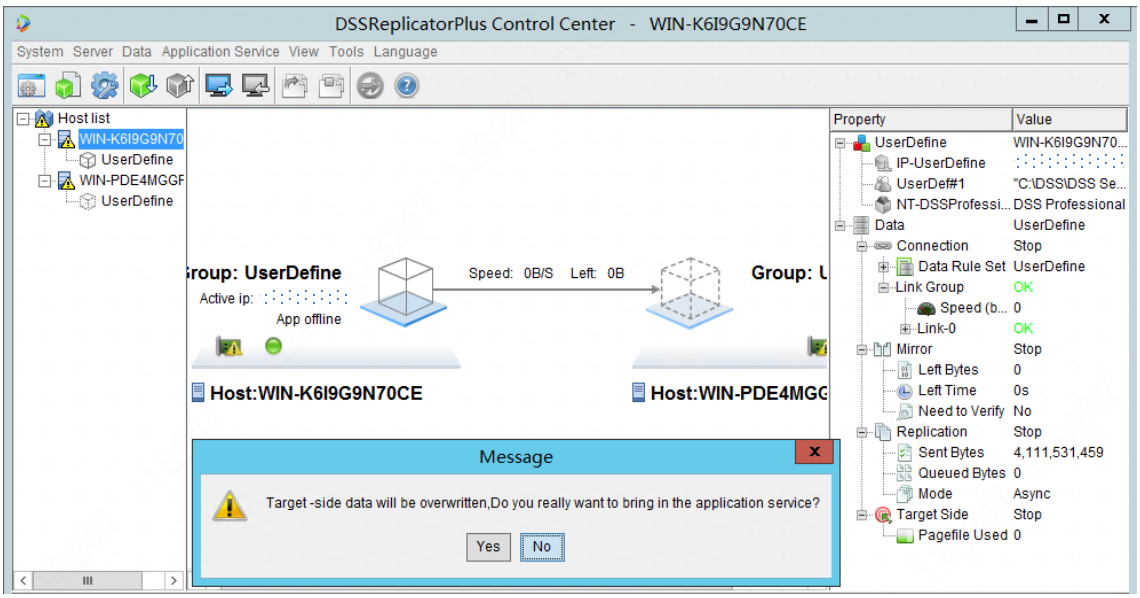


Select the application service on the active server or the standby server (around the cube icon). Take the selected active server as an example, as shown below.

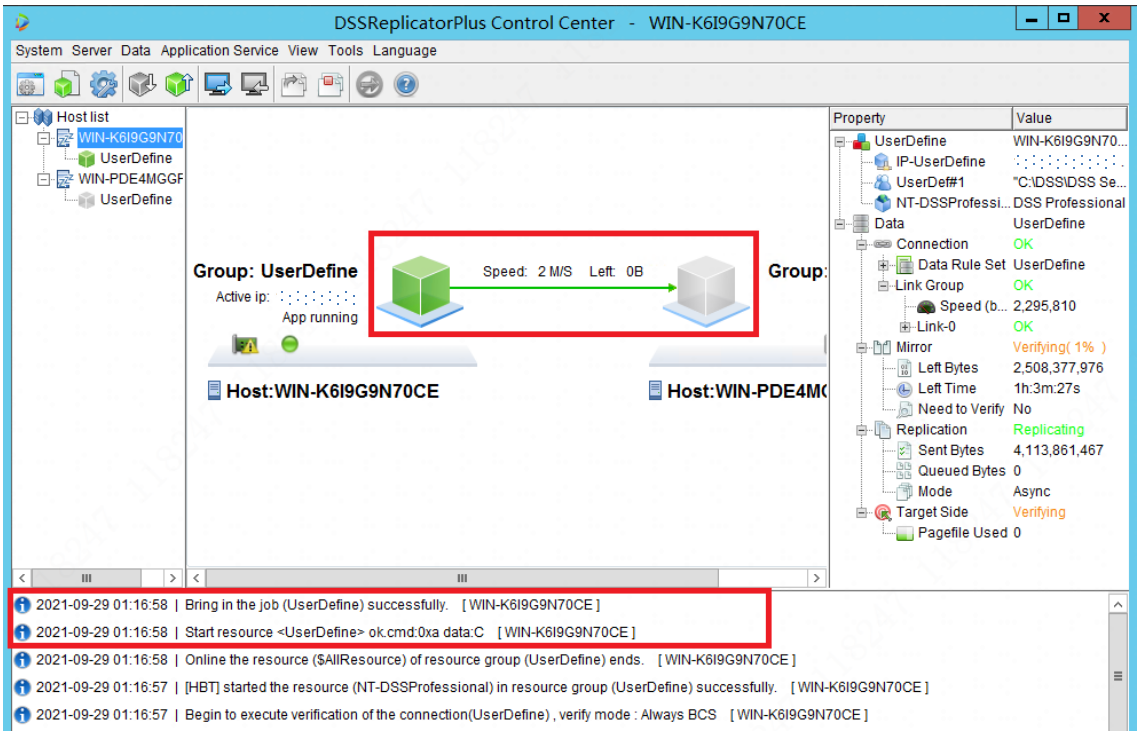
Right-click to select **Bring In** to bring in the service.



Click **Yes**.



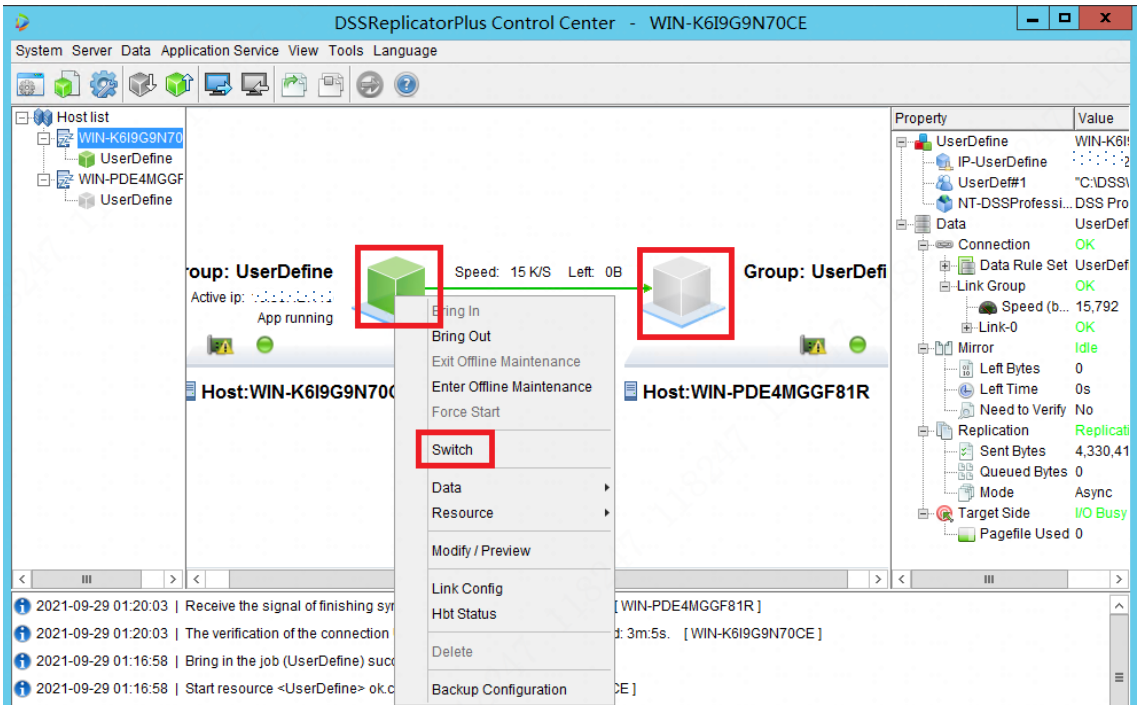
Wait until the application service is brought in and data is synchronized. The status panel of the DSSReplicatorPlus Control Center is shown below.



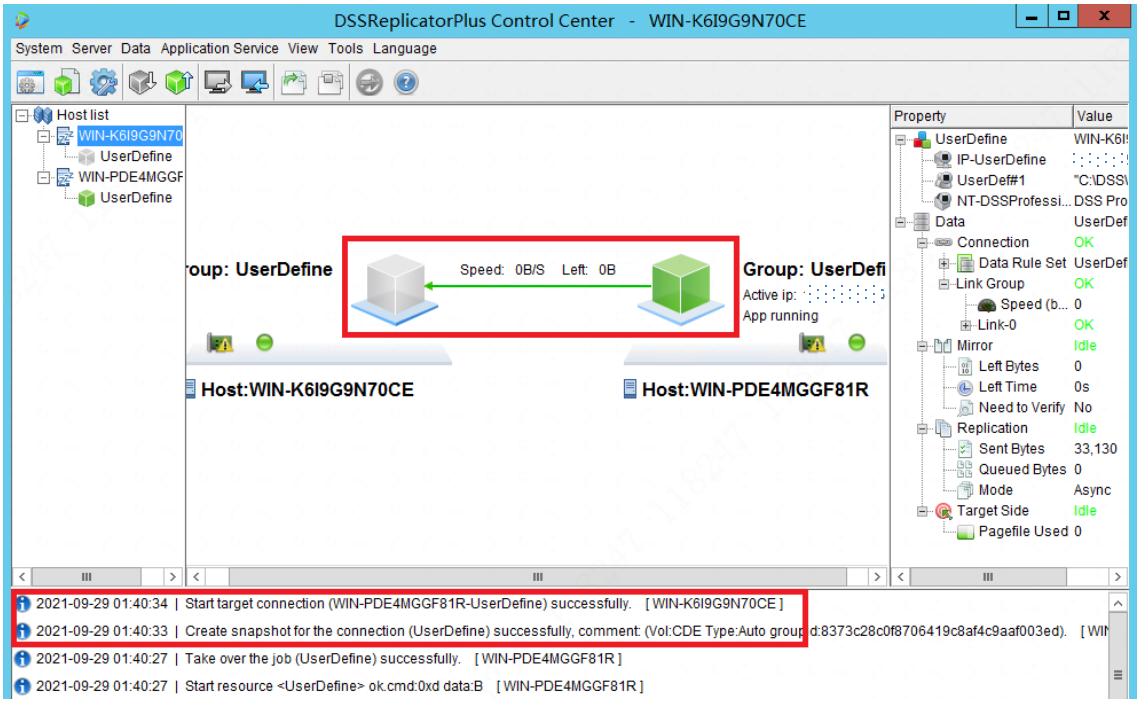
Check if the DSS server on the active server is in the "Running" state, and if the DSS server on the standby server is in the "Stopped" state. Check if the VIP exists on the active server by entering "ipconfig" in CMD. Check if the VIP can be pinged from other devices and if the VIP can be used to access DSS.

4.4 Switching Application Service Resources

Select the application service on the active server or the standby server. In other words, select either of the two cube icons. Right-click to select **Switch** to switch the application service to the standby server, as shown below.



Click **OK** in the pop-up box, and the hot standby starts switching. After the switching of the application program is complete, the status panel of DSSReplicatorPlus Control Center is shown as follows.

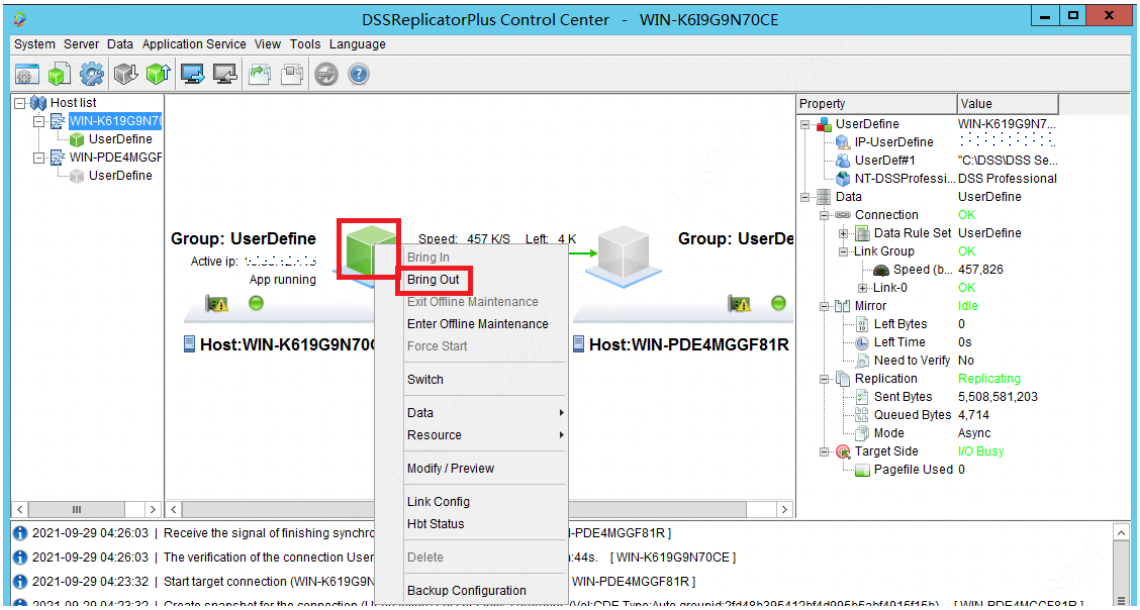


Check if the DSS Pro server on the active server is in the "Stopped" state, and if the DSS Pro server on the standby server is in "Running" state. Check if the VIP exists on the standby server, if the VIP can be pinged from other devices, and if the VIP can be used to access DSS Pro.

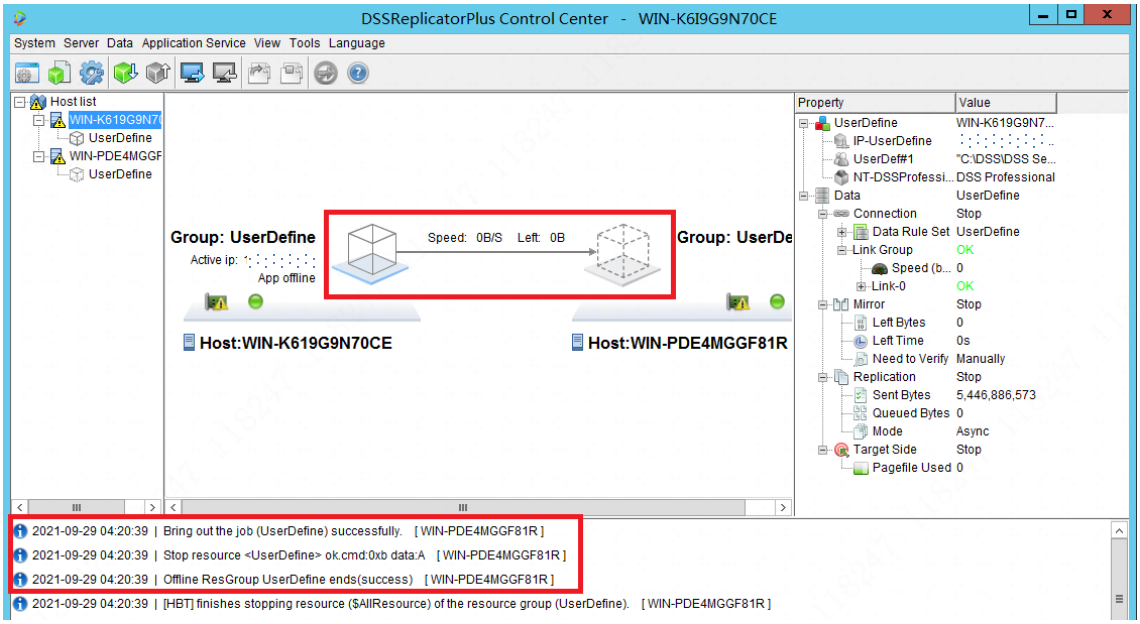
4.5 Bringing Out Application Service Resources

The "bring out" operation is deactivation. It means that the application and data protection will be disabled, and the VIP will be removed.

Select the application service on the active server or the standby server, and right-click to select **Bring Out** to bring the application service out, as shown below.



Click **OK** in the pop-up window. After the application service is brought out, the status panel of DSSReplicatorPlus Control Center is shown below.

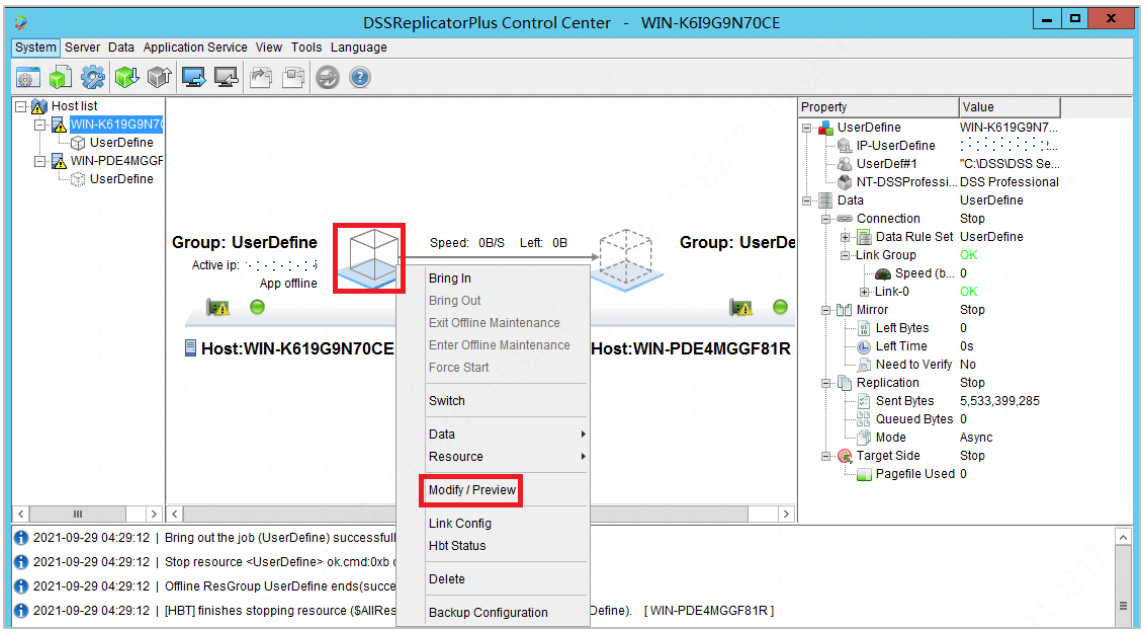


Check if the DSS Pro server on the active server is in the "Stopped" state, and if the DSS Pro server on the standby server is in "Stopped" state. Enter "ipconfig" in CMD, and no VIP is found. The VIP cannot be pinged from other devices, and the VIP cannot be used to access DSS Pro.

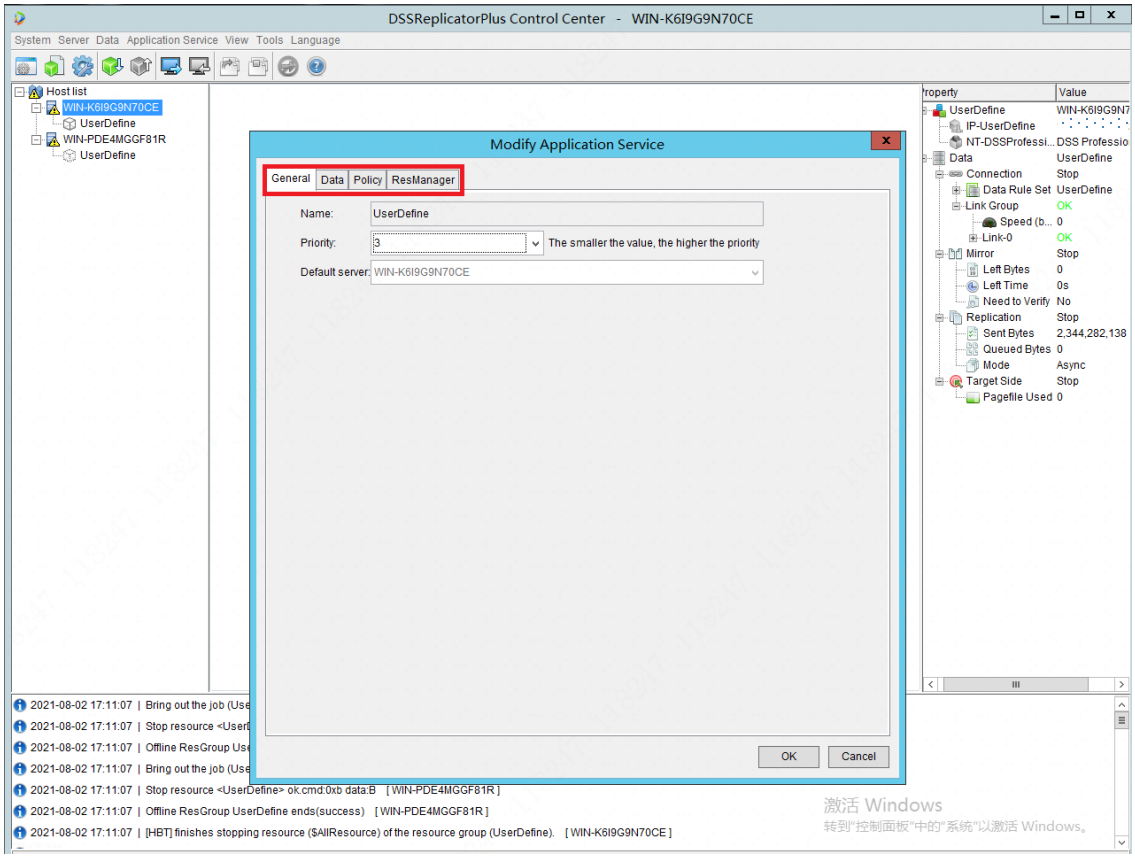
4.6 Modifying Application Service Configurations

Modifying Application Service Configurations focus on the configurations of the services protected by the applications in a cluster.

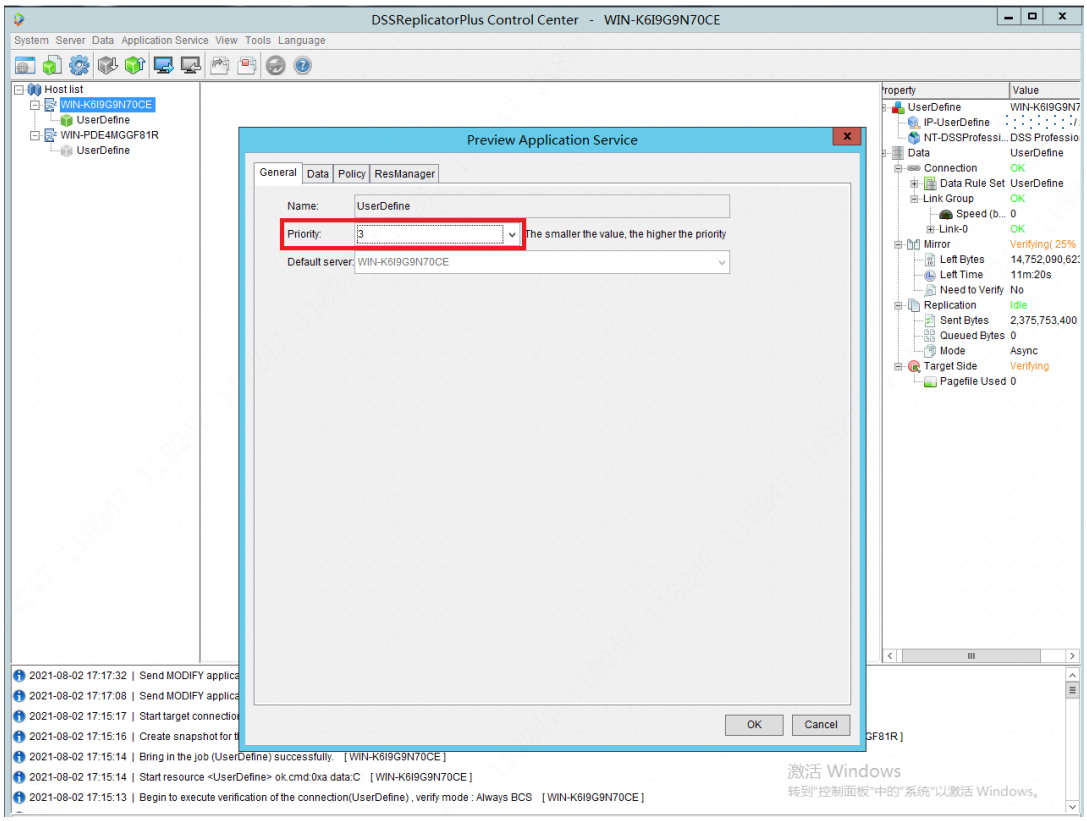
You need to **bring out the application service** before modifying its configurations, otherwise you can only view its relevant configurations. Right-click the cube to select **Modify/Preview**, as shown below.



Modify the configurations under "General", "Data", "Policy", "ResManager", and other tabs. Click **OK**, and bring them in again.



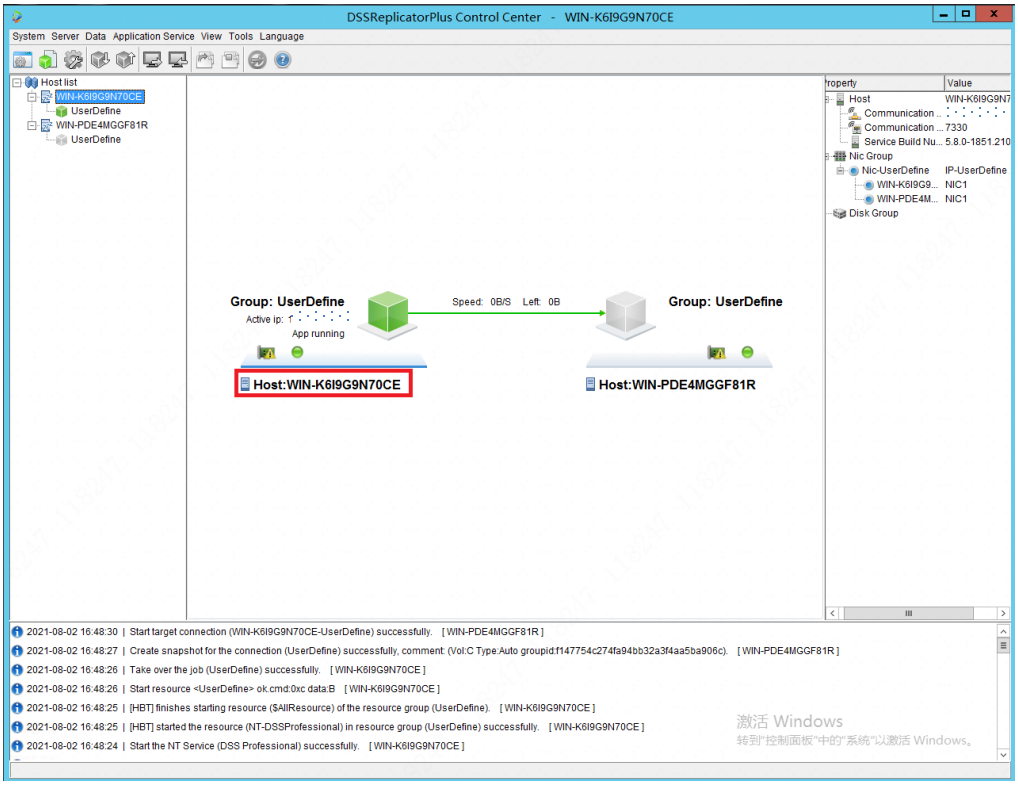
If you did not bring out the application program before modifying the application service configurations, you can only modify the "Priority" under "General" in "Modify Application Service", and cannot modify or can modify but cannot save the configurations under other tabs, as shown below.



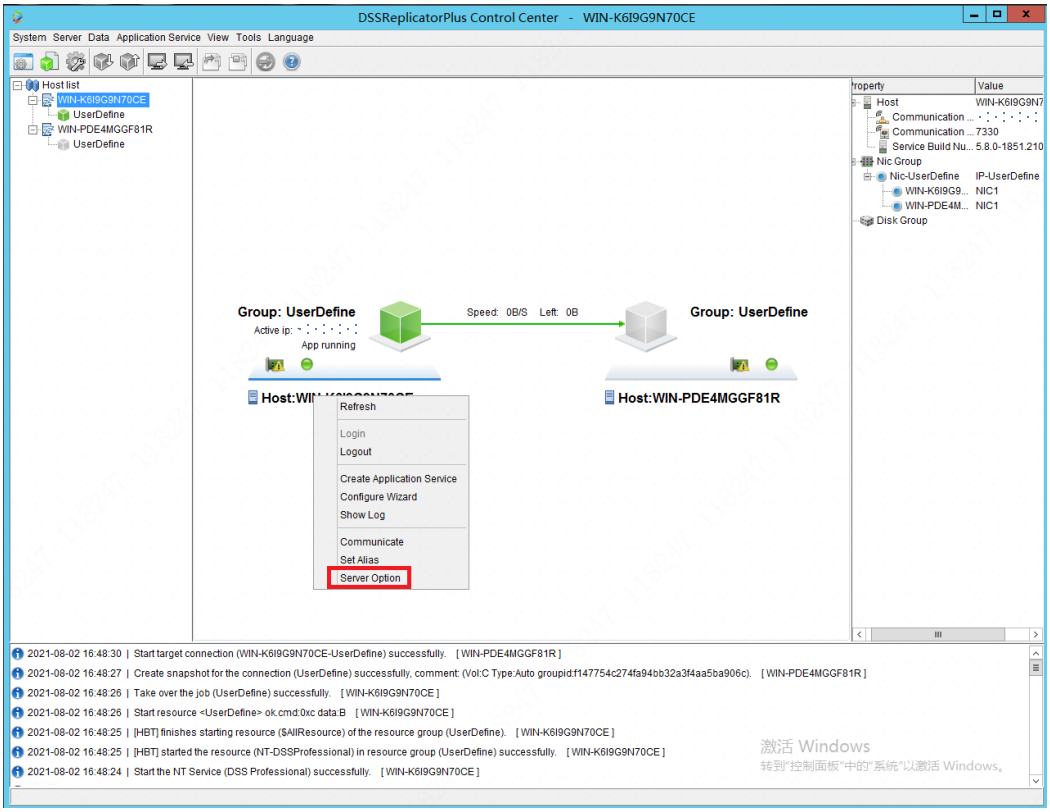
4.7 Prolonging the License Validity Period

You can prolong the license validity period by re-importing the license on the "Property" page of the server. The number of imports is unlimited.

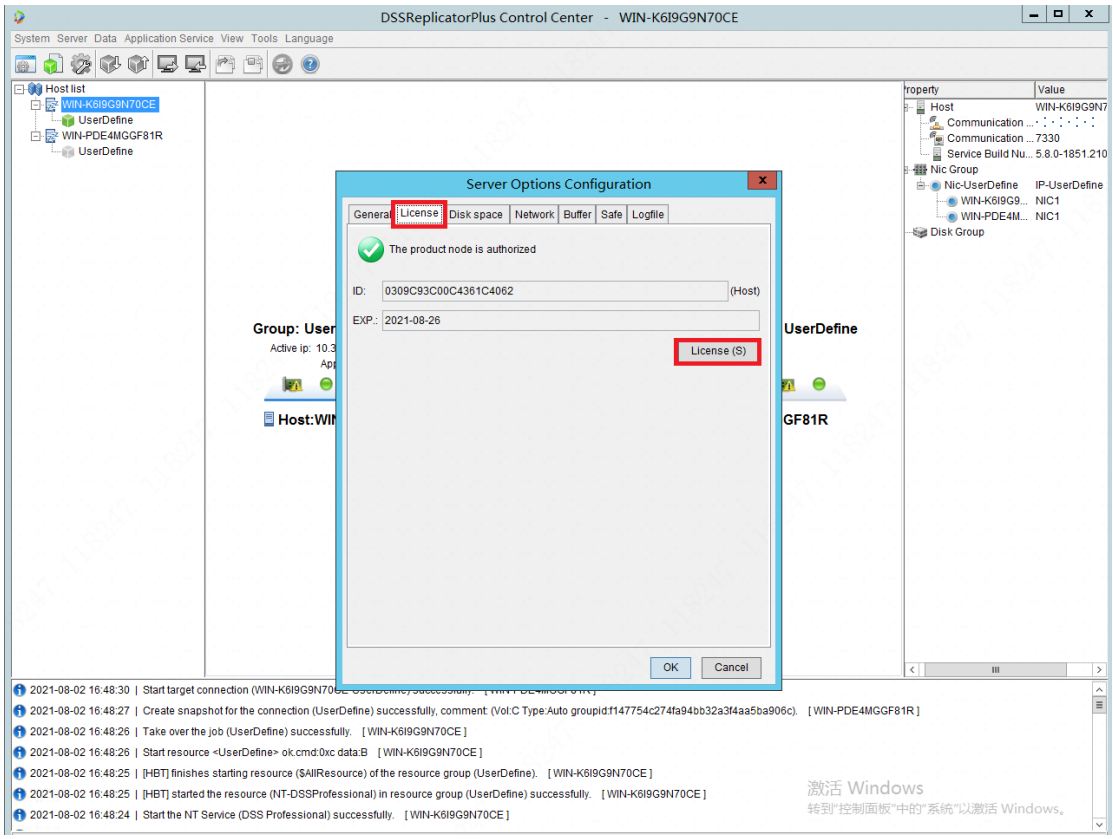
Select the application service on the active server or the standby server. Take the selected active server as an example, as shown below.



Right-click the box in the above figure, and select **Server Option**, as shown below.



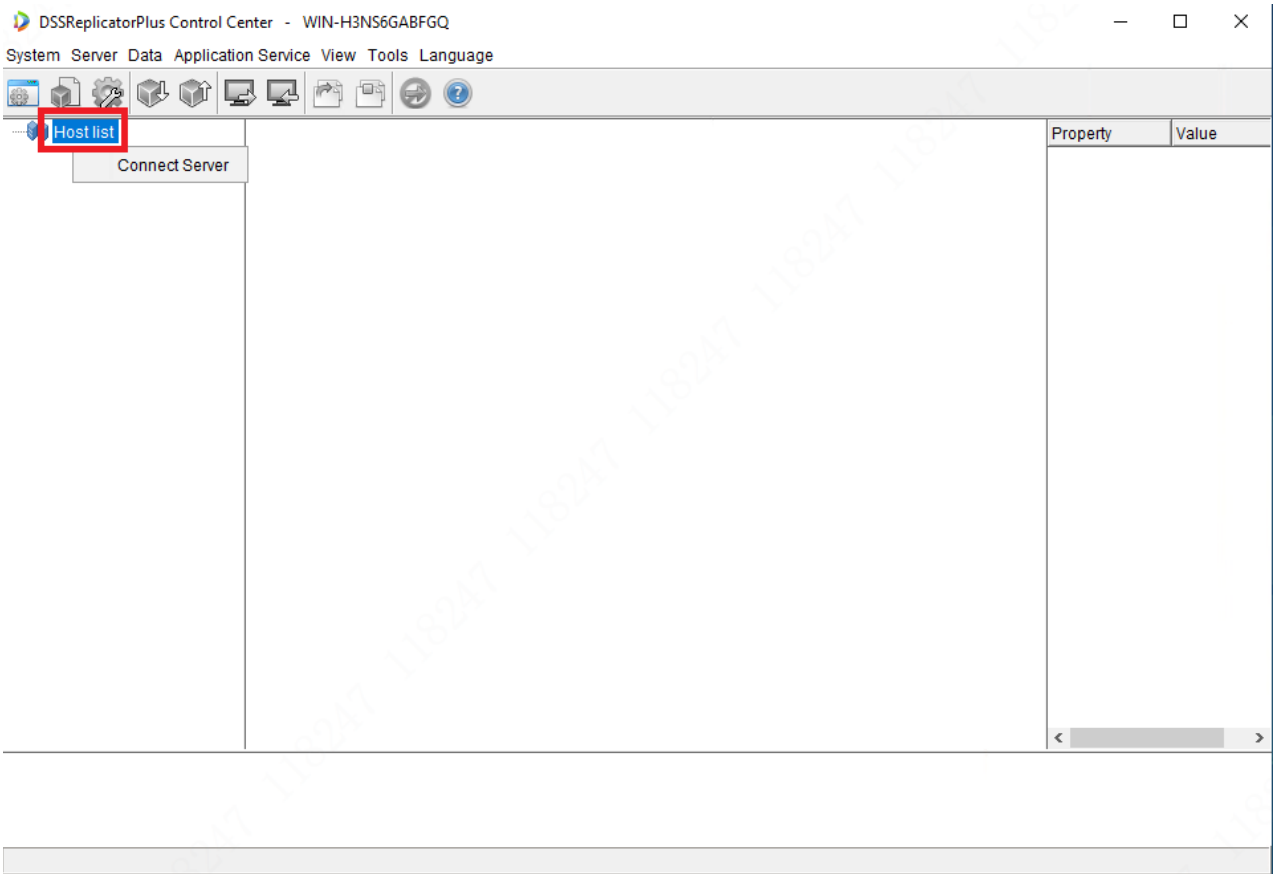
As shown below, select the **License** tab, and click **Set License**. Then upload the latest license, and click **OK**.



4.8 Displaying Hot Standby Operating Status

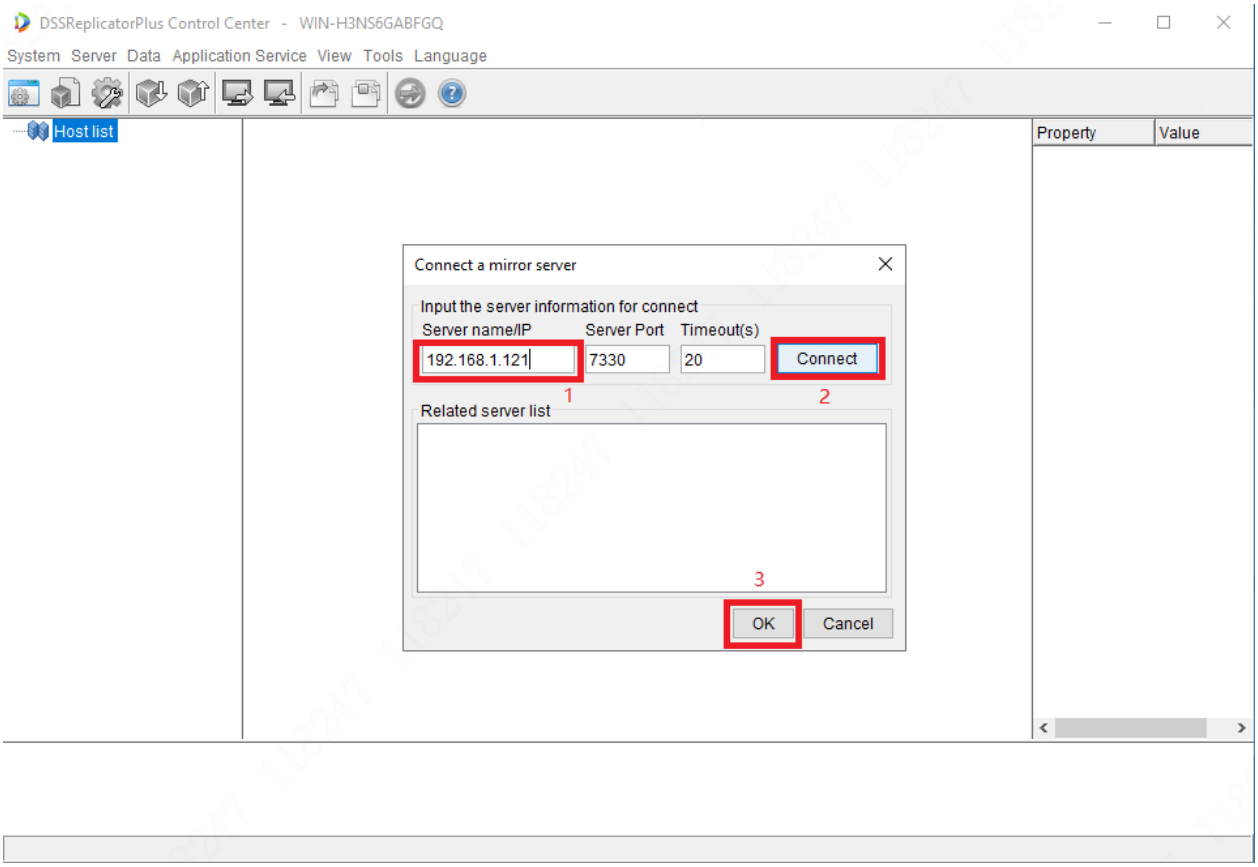
Hot standby is set up in the host, when finished, the host will display two servers information. Users need to connect the host manually to access the information. Steps are shown as below:x

Right-click on "Hostlist" and click "Connect Server", as shown below:

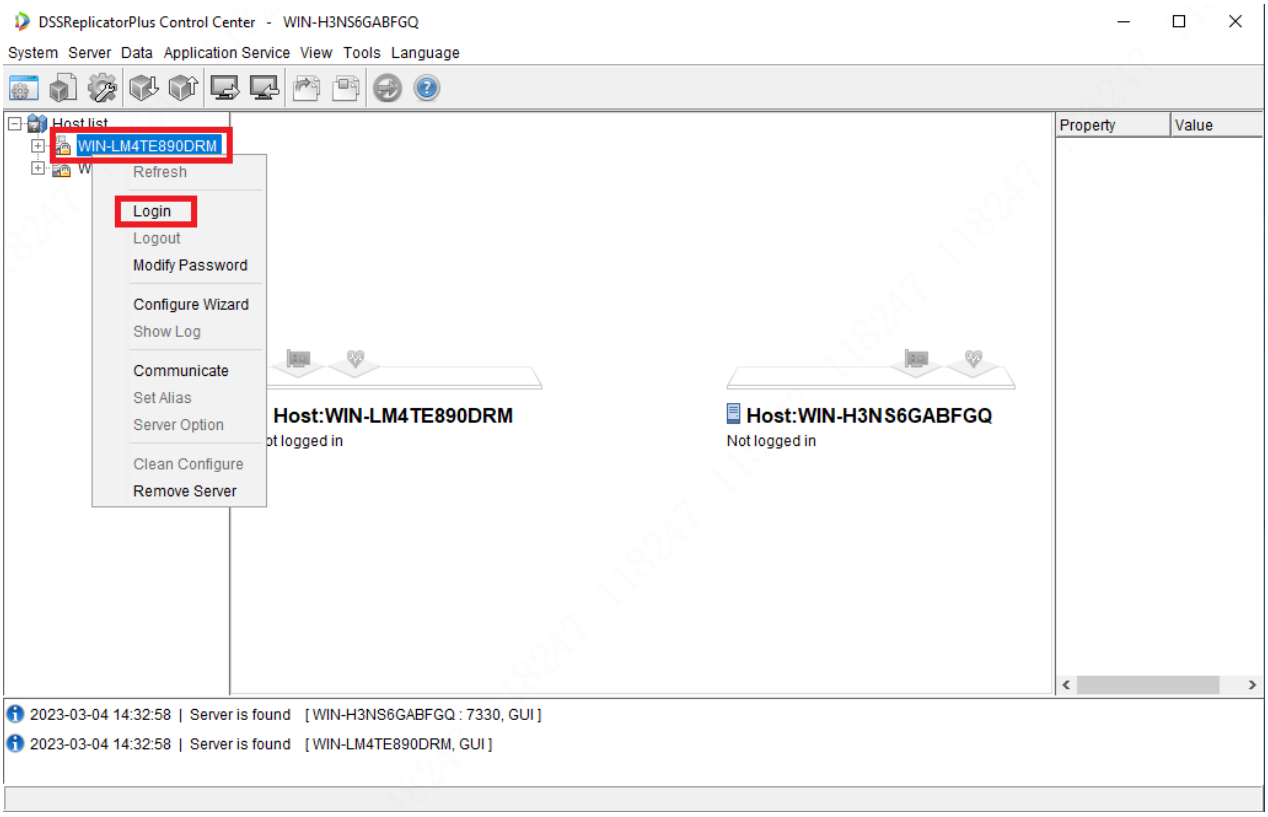


Enter the host IP in the pop-up box, and then click **Connect**.

Click **OK** after you obtained the service information.



Right-click **Login**, and log in to two servers respectively.



Enter the account password, select **Save Password** and **Auto Login**, and then click **OK**.

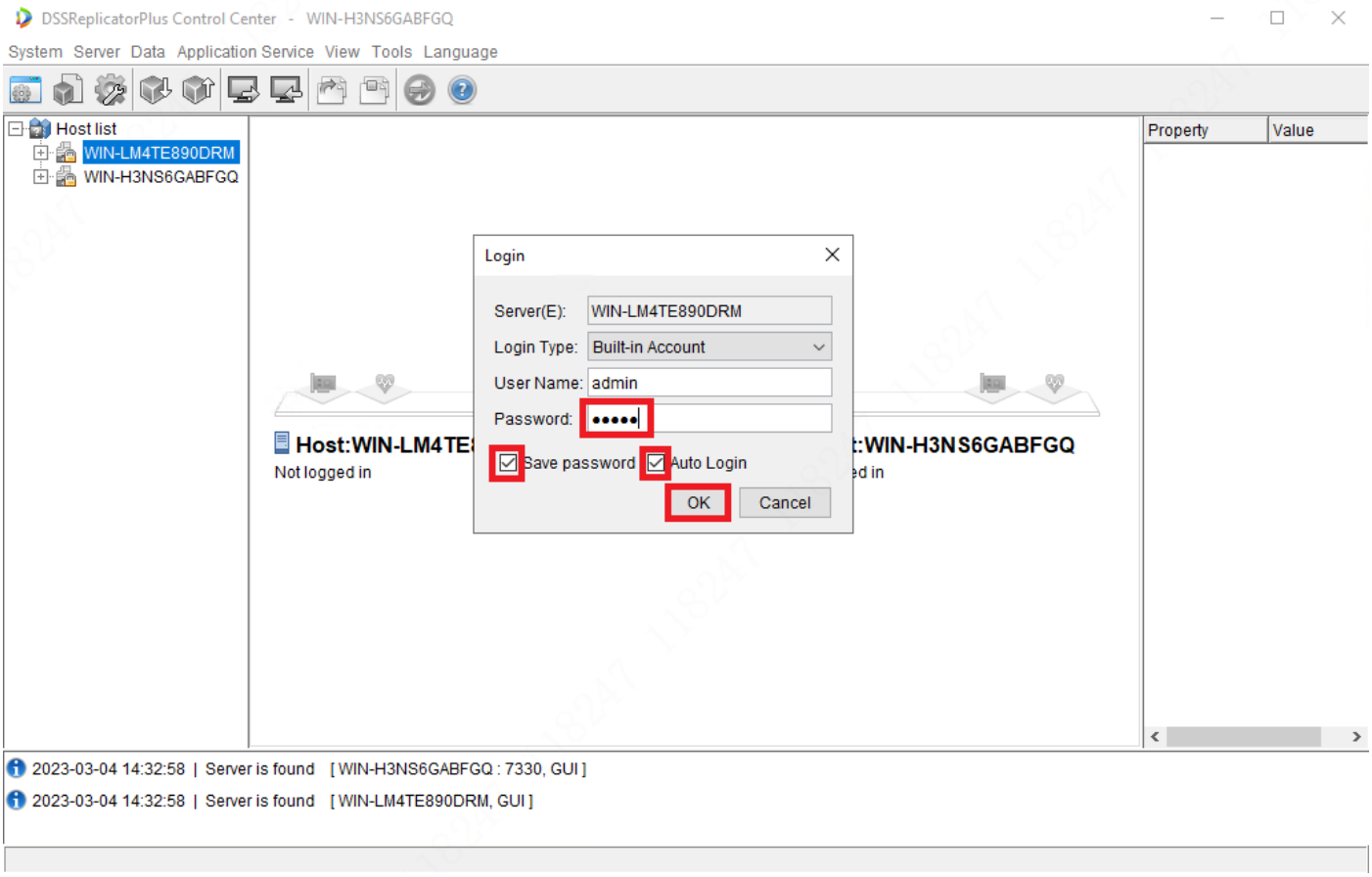
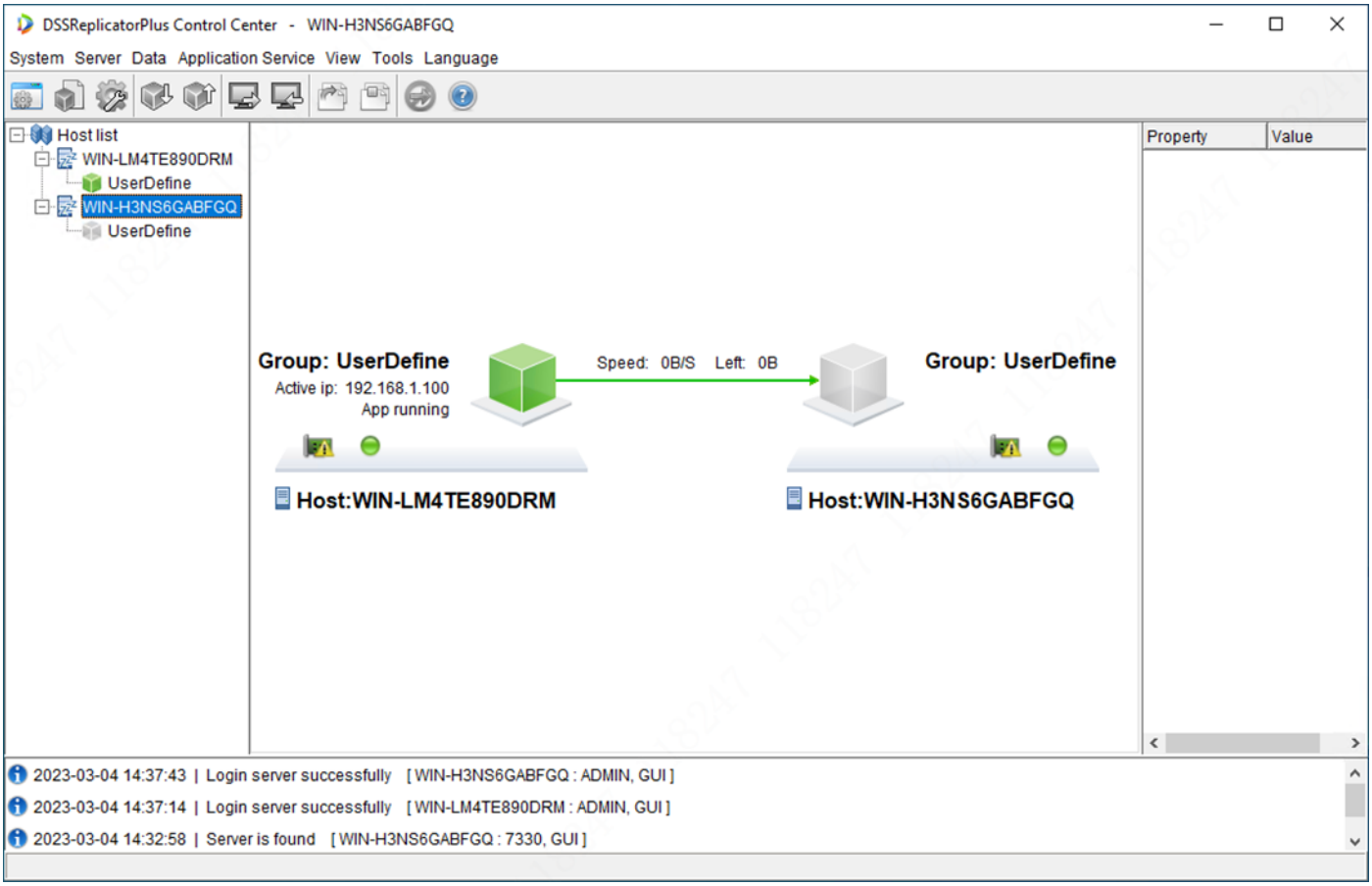


Figure 4-1 Both servers are logged in



5 Update

In the hot standby environment, make sure that the application program has been brought out before an update.

5.1 Updating the Hot Standby Software

Hot standby software does not support overwriting during installation and update, so the old version must be first uninstalled (no residual files under the installation directory). If some files still remain, the folder in which these files exist can be deleted after restarting the server. Check here for using the late version of software to set up hot standby.

5.2 DSS Platform Update

DSS Pro installation packages of the active and standby servers must be updated respectively. After a successful update (the software is not and cannot be started through servers), the application program can be brought in again through DSSReplicatorPlus Control Center.

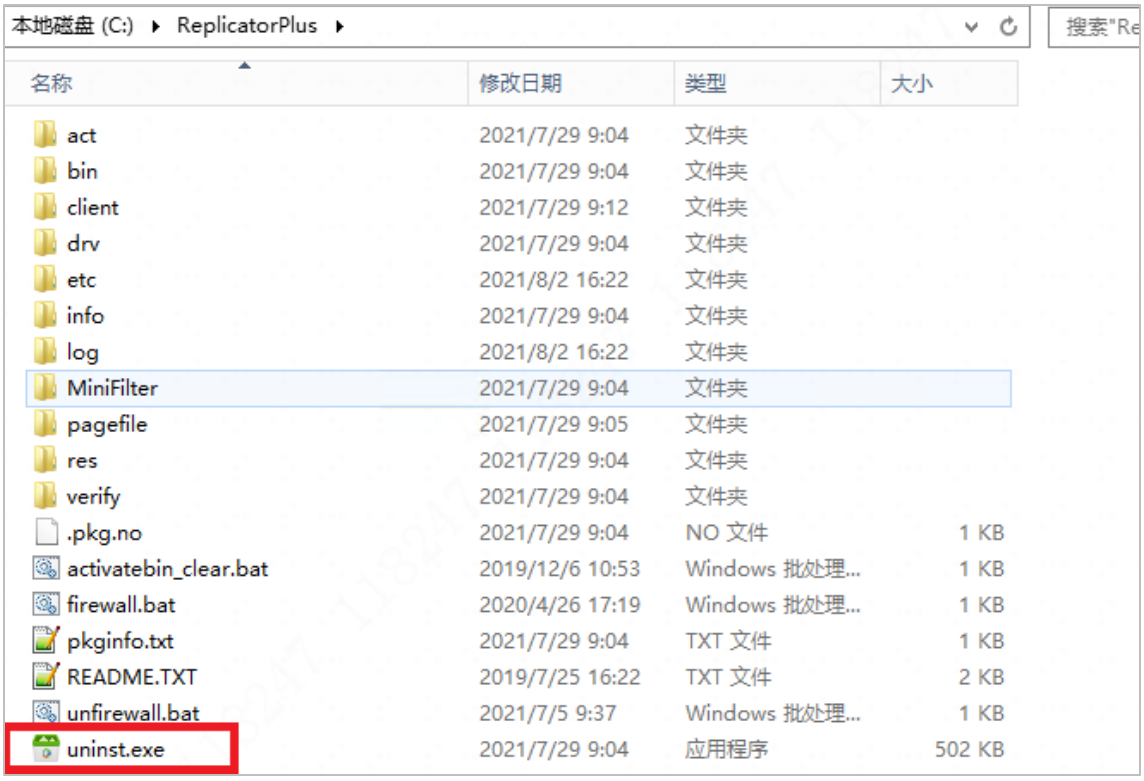
Notes: Platform update may add or modify the files (path) required to be synchronized. If modifications happen, then you need to modify service configuration of the application. For details, see Section 6 in Main Features of Hot Standby Software.

6 Uninstallation and Switching of Hot Standby

6.1 Complete Removal and Uninstallation of Hot Standby

(1) The application program must be brought out before the hot standby is uninstalled.

(2) Find the path where the installation files of DSSReplicatorPlus Control Center exist (Shortcut > Open File Location), and double click "uninst.exe" under the root directory of the application program, as shown in the following figure.



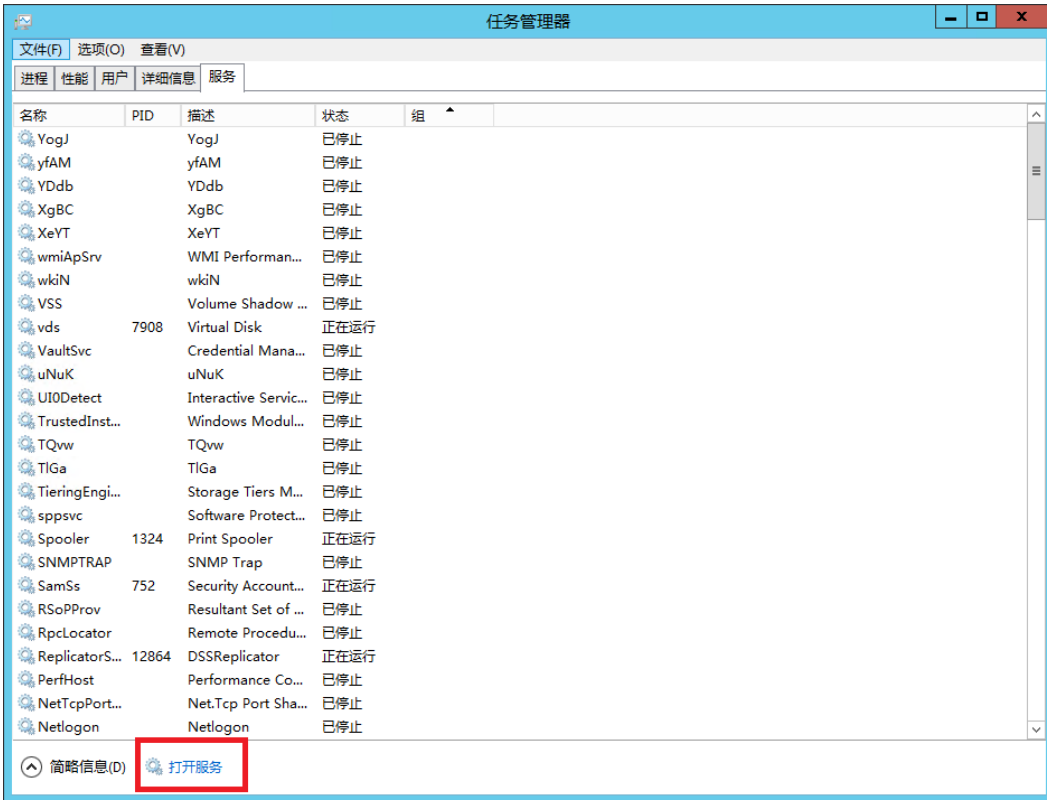
Click **Yes**.

(3) After the uninstallation, some folders may remain. You can restart the server, and then delete these folders. For details, see Section 2 in Frequent Problems and Solutions.

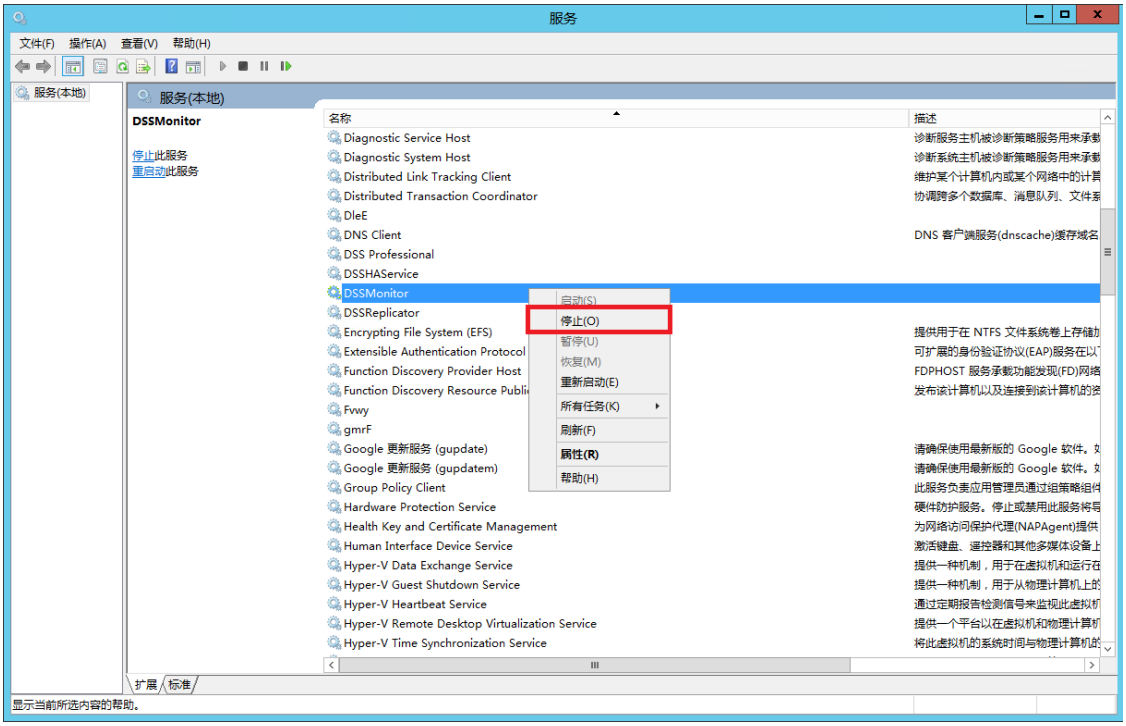
6.2 Switch to Standalone-Server Application under Hot Standby (Do not Uninstall Hot Standby Software)

(1) The application program must be brought out before restoring to standalone status.

(2) To open the service interface, select **Task Manager** > **Service** > **Start Service** or enter "services.msc" in CMD, as shown in the following figure.

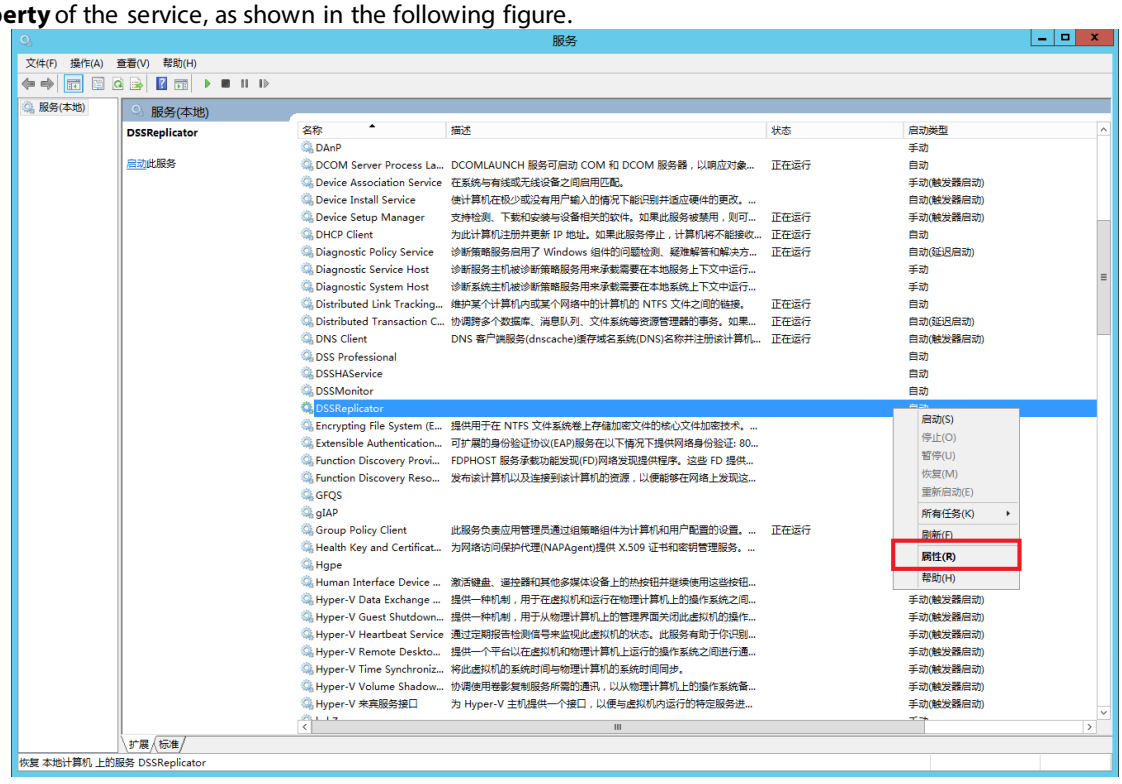


(3) Stop services DSSMonitor, DSSHAService, and DSSReplicator in the following sequence: DSSMonitor > DSSHAService > DSSReplicator

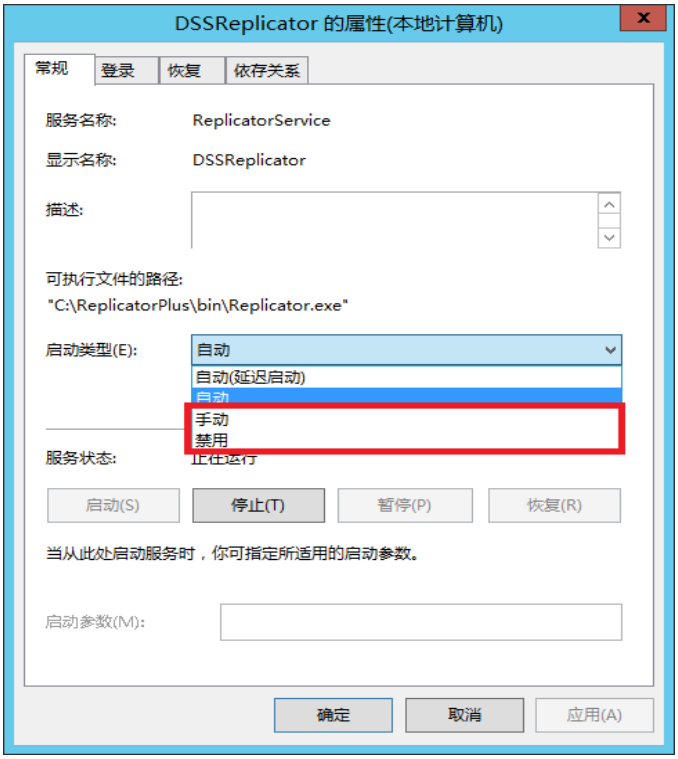


(4) Modify the status of the services DSSMonitor, DSSHAService, and DSSReplicator from **Auto** to **Disabled** or **Manual** (to prevent from reactivating the hot standby after restarting).

Right click **Property** of the service, as shown in the following figure.



Select **Manual** or **Disabled** for startup type, and click **Confirm**.



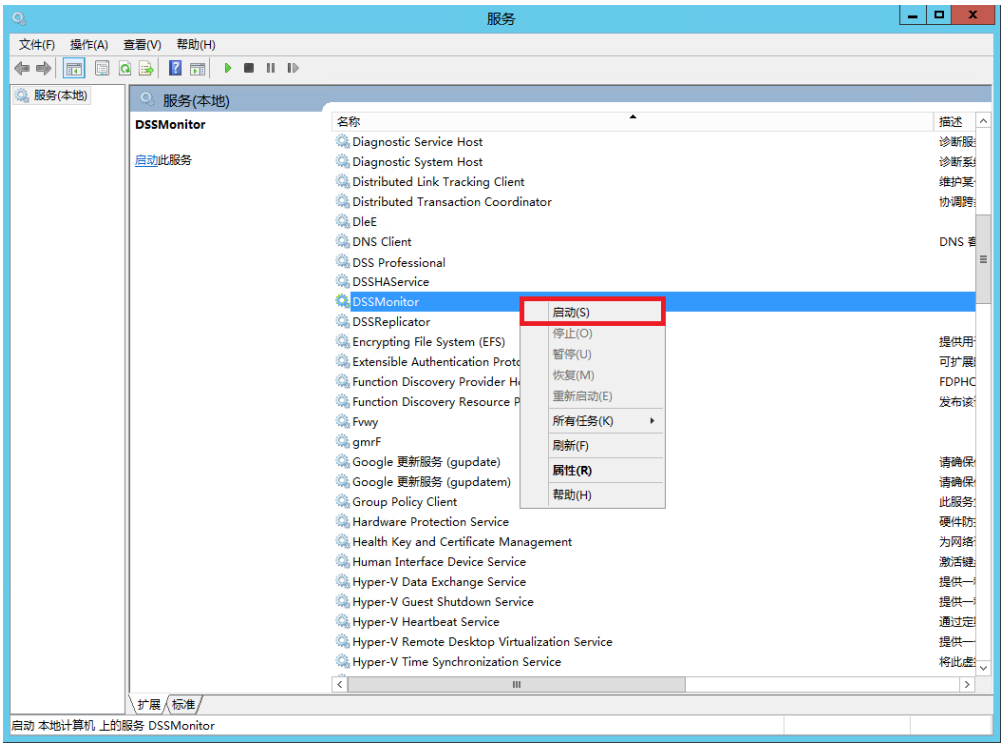
(5) Modify server IP address to business IP address through servers, and then start the servers with each server respectively.

6.3 Recover from Standalone-Server Status to Hot Standby

The standalone server here refers to the standalone server mentioned in **the previous section 2.** The main steps are as follow.

(1) Modify the status of DSSMonitor, DSSHAService, and DSSReplicator in the active and standby servers to **Auto**.

(2) Start DSSMonitor in the active and standby servers, as shown in the following figure.



(3) Bring in the application in DSSReplicatorPlus Control Center.

Note: First, confirm the active server before bringing in the application in DSSReplicatorPlus Control Center, because the data brought into the standby server will be overwritten by the active server. Ensure that the data in the active server must be actually demanded.

7 Notes

7.1 Time Difference During License Application

Because there is a jet lag between China and overseas countries, for example, it is January 1 abroad while it is January 2 in China. We will apply for the license on January 2 by default in China and the license may not be valid yet when use in abroad. Therefore, we recommend that you specify the expiration date one day earlier while applying for the license.

7.2 Unable to Access Platform While Recovering Environment of Hot Standby

Unable to access the platform through other browsers while recovering in Windows. Only after the job finished can the platform be accessed. Therefore, you need first to evaluate the recovery's impact under the environment of hot standby.

7.3 Under Hot Standby, Unable to Format Local HDDs of Active and Standby Servers to Video Disks

At present, you cannot synchronize the data of video storage format between the active and standby servers through the folder synchronization method. Therefore, for central video storage under hot standby, we recommend that you add EVS through IPSAN, which requires both active and standby servers to simultaneously add the same user of EVS. During hot standby switching, it will actively adjust the server mounted on EVS to guarantee normal reading and writing of video data.

7.4 Under Hot Standby, Making Drive Letters Consistent with Number of Disks while Storing Pictures and Files of Active and Standby Servers

Under hot standby, pictures and files are synchronously backed up through hot standby software. The backup requires consistency of drive letters and capacity between the two servers. If not consistent, it will lead to different data or abnormal data synchronization between the active and standby servers. For example: The capacity of the active server is

500 GB, while that of the standby server is 100 GB. Therefore, part of the data in the active server will not be synchronized to the standby server. The active server has Disk E while the standby server does not have Disk E, so the hot standby software will prompt the missing of the mount point and stop data synchronization.

7.5 Under Hot Standby, Being Storage Disk for Pictures and Files, Network Disk Requiring Active and Standby Servers to Add Different Users

Under hot standby, while being a storage disk for pictures and files, the network disk will be formatted as the NTFS disk of the current server, and equal to the local disk of the server. Under hot standby, storage of pictures and files is synchronized by folders through hot standby software. If using EVS to store pictures and files, it requires that EVS storage disks added to the active and standby servers are of the same capacity and quantity and in different disks. Generally, we recommend that you add single EVS through different users. You need to make sure that the capacity and quantity of disks are consistent among different users, so that user disks that are added into the active and standby servers through EVS will be normally synchronized. Using the same user to add EVS will cause abnormal data storage when two servers simultaneously read and write the same disk.

7.6 Under Hot Standby, Central Service Can Add Different Users of the Same EVS while Distributed Service Can Add Users Only Once

Under non-hot-standby environment or distributed standby server under hot-standby environment, whether an EVS is added through user mode or normal mode, any disk of the EVS can be set as storage disk for pictures, files, or videos, fulfilling the demands of storage. But under hot standby, an EVS added through the central server can only have one type of disk for one user, in order that the EVS can simultaneously store videos, pictures, and files. Therefore, under hot standby, the central server can add multiple users of the same EVS.

8 FAQ

1. After Uninstallation, Unable to Delete Folder DSSReplicatorPlus?

You can delete the server after restarting it.

2. Unable to Detect or Detect Wrong Heartbeat IP Address?

Before setting up, you must ensure that the IP addresses of the two connected heartbeat network ports are in the same network segment. If the IP address is still detected wrong after modification, you must restart the server, and then set up the hot standby again.

3. Unable to Access VIP Address because of VIP Address Conflicting with Other Devices After Setting up Hot Standby?

If the VIP address is occupied while using it, you must release the VIP address from other devices, and then transfer or take over to make a switch between the active and standby servers.

4. Unable to Access VIP Address on Other Active Servers Though This Address Has Already Existed on Active Server (Enter ipconfig in CMD to Check)?

This case generally occurs when the access crosses network segments, or when the network has strict access restrictions and requirements. Generally, the access does not pass through the gateway when in the same network segment, so normally you will not encounter such a case.

Because the MAC addresses of the NICs of the active and standby servers are different, after the active server loads the VIP address, the corresponding MAC address is mac1. After switching to the standby server, the MAC address corresponding to the VIP address is mac2. Some network have a strict restriction policy on the network environment. (For example, only the IP access of the MAC address registered for the first time is supported. If you want to change the MAC address for the registered

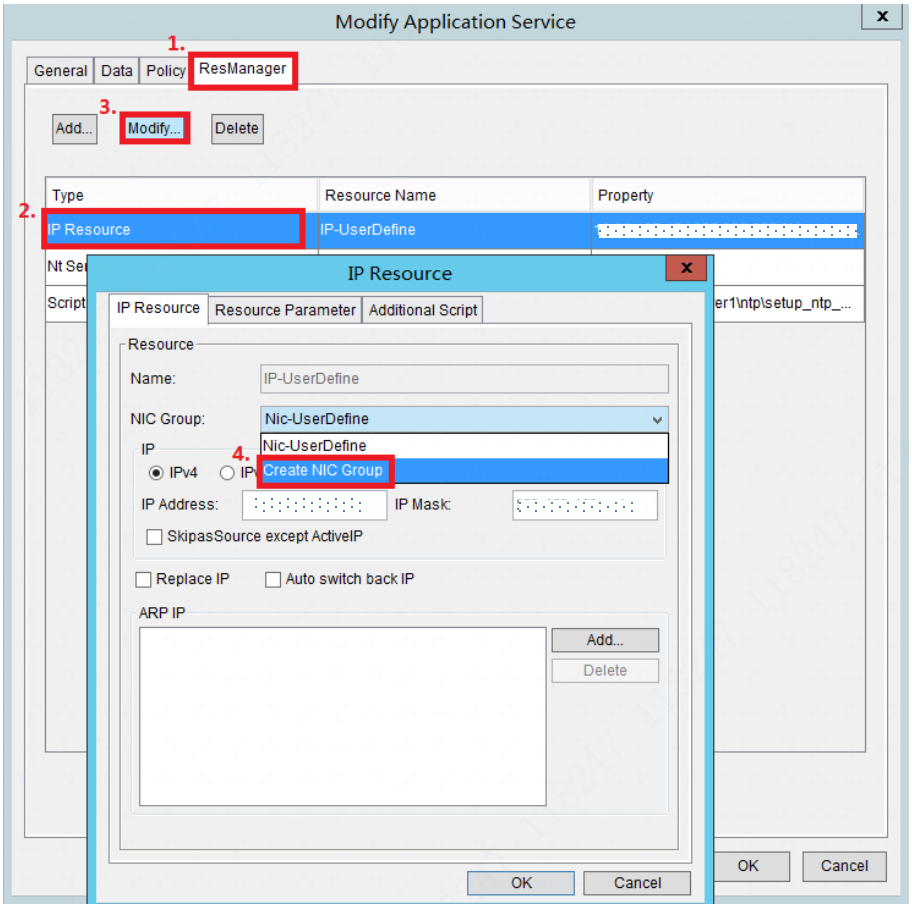
IP address, contact the administrator to unbind the original MAC address.) (or because the APR table of the switch is refreshed slowly, the new MAC address corresponding to the VIP address cannot be detected for a period of time after the switching, causing the communication failure).

Based on the reasons above, Rose provides a series of functions to avoid the case that it may not access the VIP address after the switching and then the switching fails.

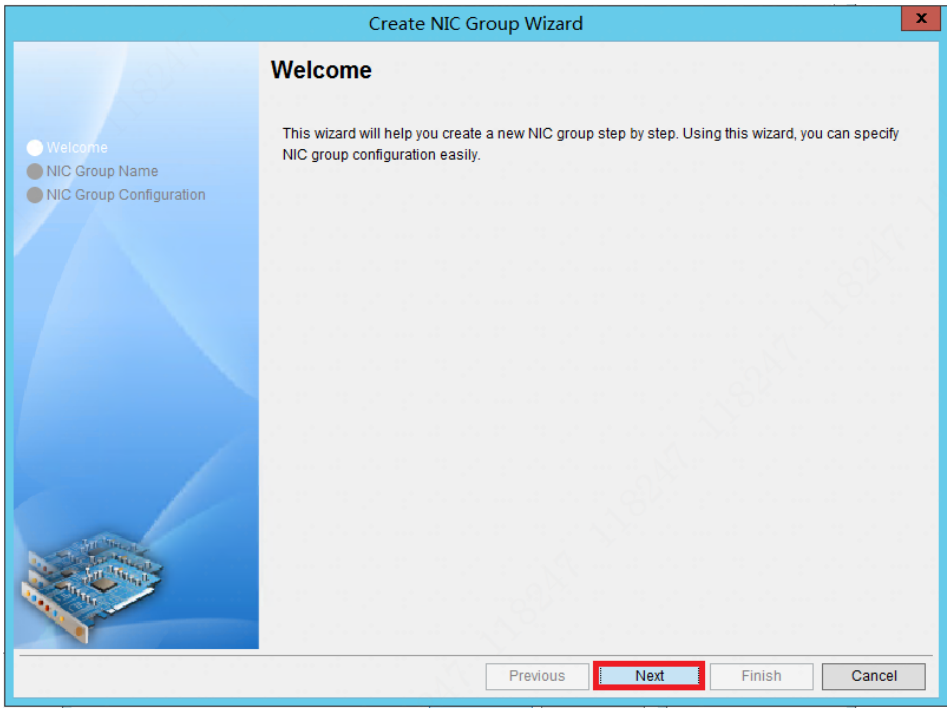
(1) Operating bring-in or switching will trigger an APR notification to actively notify cache refresh of the APR in the LAN.

(2) You can configure the function of virtual MAC address. After the function is configured, the server loaded by the VIP address will adjust the corresponding communication MAC address of the NIC to a fixed MAC address. For example, after switching, the MAC address of the original active server is restored to its original status, and the MAC address of the standby server is adjusted to MAC3, which corresponds to the VIP address mounted. This method can first ensure that the VIP address works every time with the MAC address being MAC3.

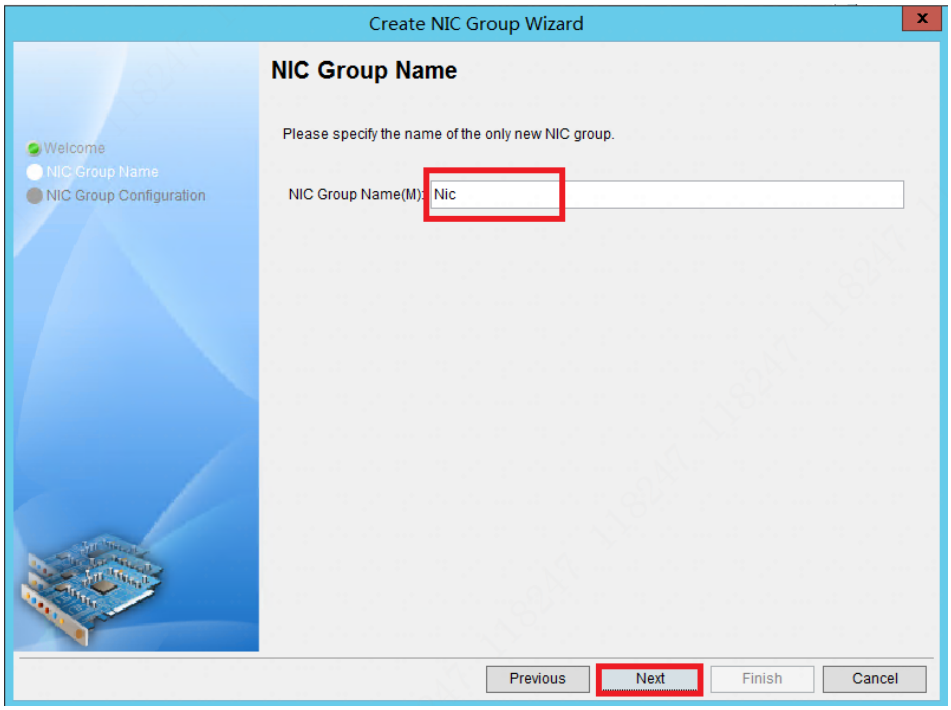
To bring out the service, and after the service is fully brought out, select from the menu bar at the upper-right corner of the hot standby software: **Application Service > Modify / Preview > ResManager > Select IP Resource > Modify > NIC Group**, select **Create NIC Group** in the drop-down list, and follow the configuration shown in the following figure:



After selecting **Create NIC Group**, you will see the following pop-up window.

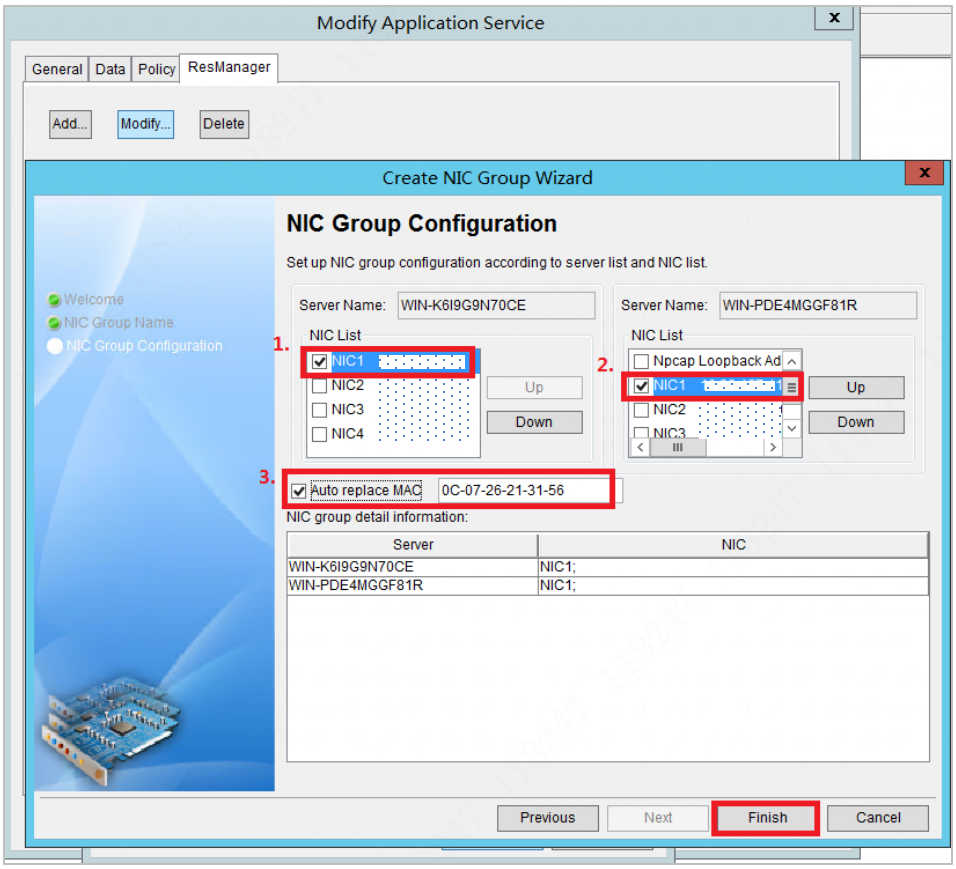


Click **Next**.

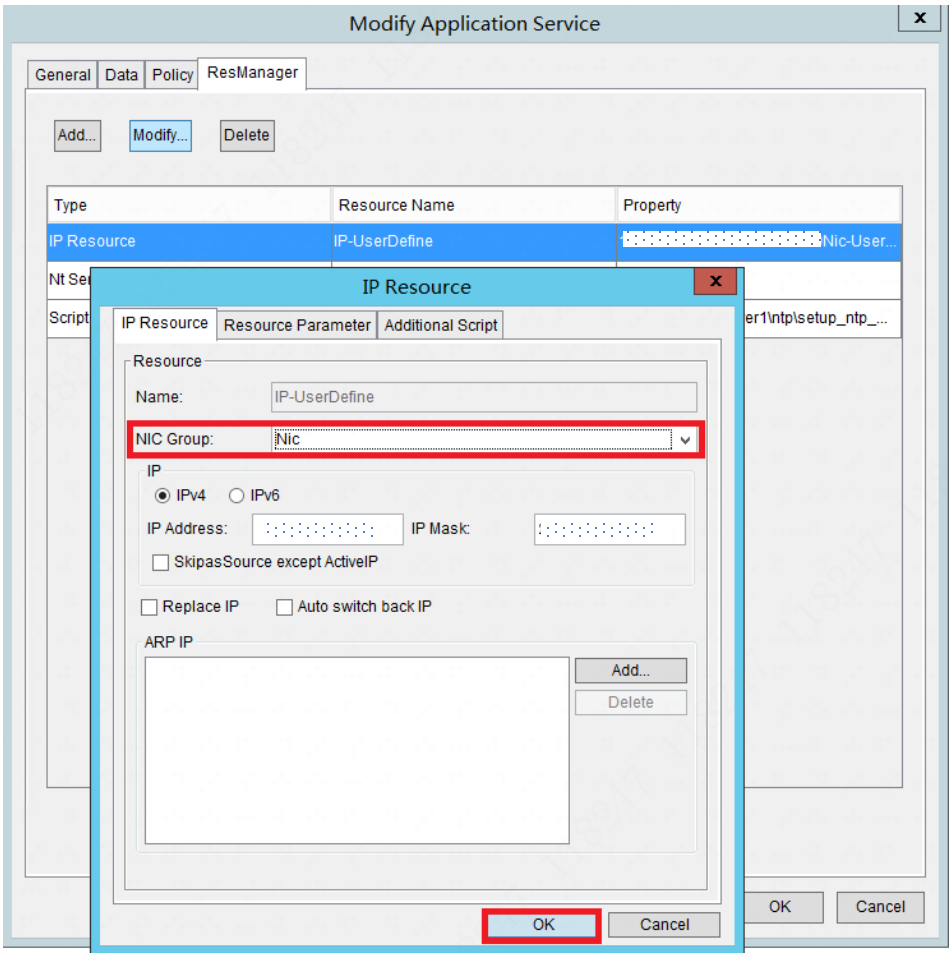


Configure **NIC Group Name** (custom), and click **Next**.

Select to configure the business IP NIC of the two servers. Configure **Auto replace Mac** as MAC3.



Click **Finish**, and the pop-up window of configuration will be closed. Then select the newly created NIC in NIC Group, and click OK, as shown in the following figure.



Note: Configuring the virtual MAC address may cause the local address of the current active server to be unable to provide external communication. This impacts daily management (one of the local addresses in the active and standby servers may fail to communicate). **We recommend that you perform such configuration after risk evaluation** to solve the problem that sometimes the VIP address cannot be accessed.

5. No Operation to Select IP Address through Third-Party Startup Platform After Installation of Service?

After installing the service, start the service through the server and configure the server IP address. And then bring in the application through a third-party platform.

6. Unable to Use Platform due to Failed Switching of Hot Standby while Active Server Being Stuck in the Shutdown Status?

Only the following two cases, which can trigger the automatic switching of the hot standby, are supported:

(1) The business network of the active server fails.

(2) The active server is offline, including the normal and abnormal shutdowns of the active server.

The normal and abnormal shutdown of the active server requires a complete shutdown of the system.

7. Hot Standby Not Switching to Standby Server while Windows System Itself Being Abnormal?

Conditions that trigger the automatic switching of the hot standby are explained in Question Six. Currently, only two cases mentioned in Question Six are supported.

8. Not Switching Hot Standby while JAVA Being Abnormal?

Conditions that trigger the automatic switching of the hot standby are explained in Question Six. Currently, only two cases mentioned in Question Six are supported.

Because hot standby software monitors the whole DSS service, monitoring one specific process under the service is temporarily not supported. Therefore, the switching will not be triggered while some process is abnormal.

9. Loss of Pictures and Video Files in Central Storage After Switching of Hot Standby?

While the hot standby is switching, which requires time, pictures, evidence files, and video files generated during the switching will lose some storage data.

If a large number of files are lost, confirm whether any of the following problems cause this incident.

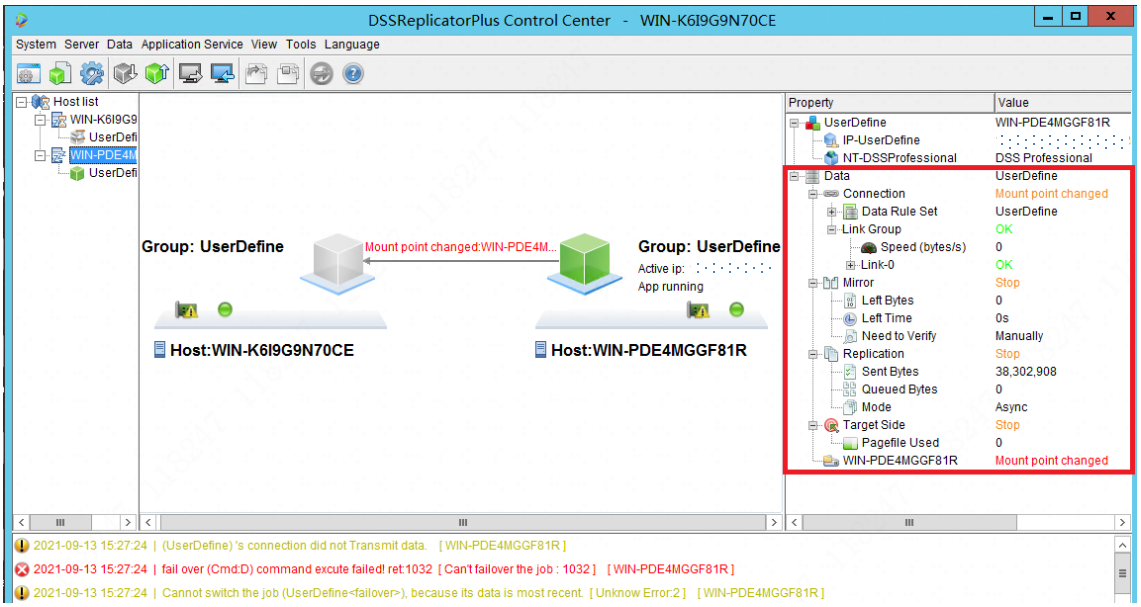
Video loss: Check whether all the video disks of the active and standby servers have added the same user of the same EVS.

Loss of pictures and files: Check whether the disk numbers where the pictures and files of the active and standby servers are stored are consistent with the number of the disks. Check whether the disk types corresponding to each drive letter are the same. Check whether the hot standby software is configured to bind the data sources of all pictures and files.

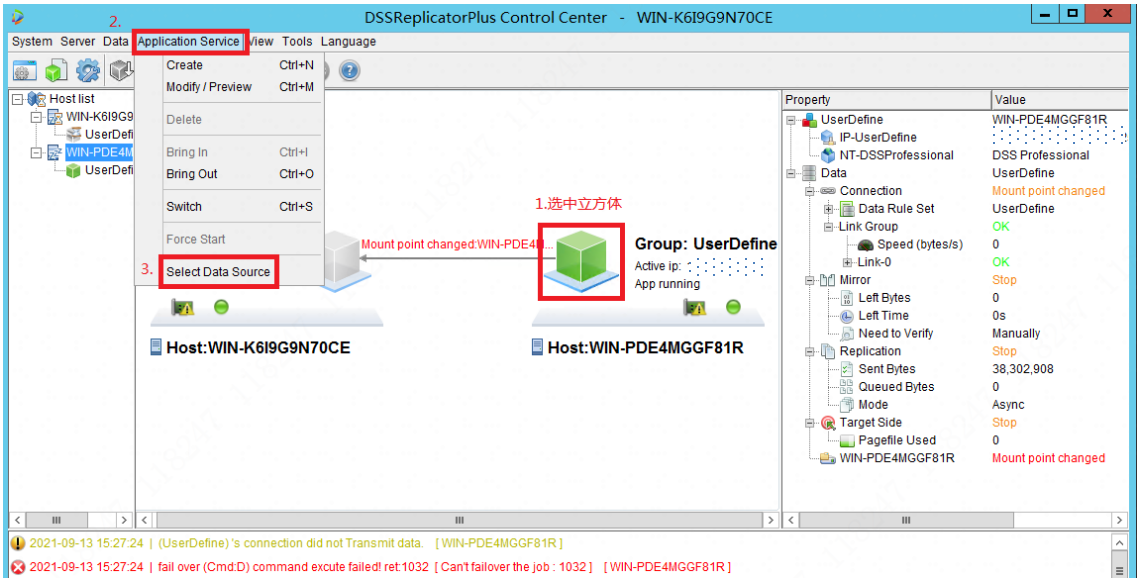
If all the above configurations are normal, contact technical support.

10. Hot Standby Software Prompting Change of Mount Point?

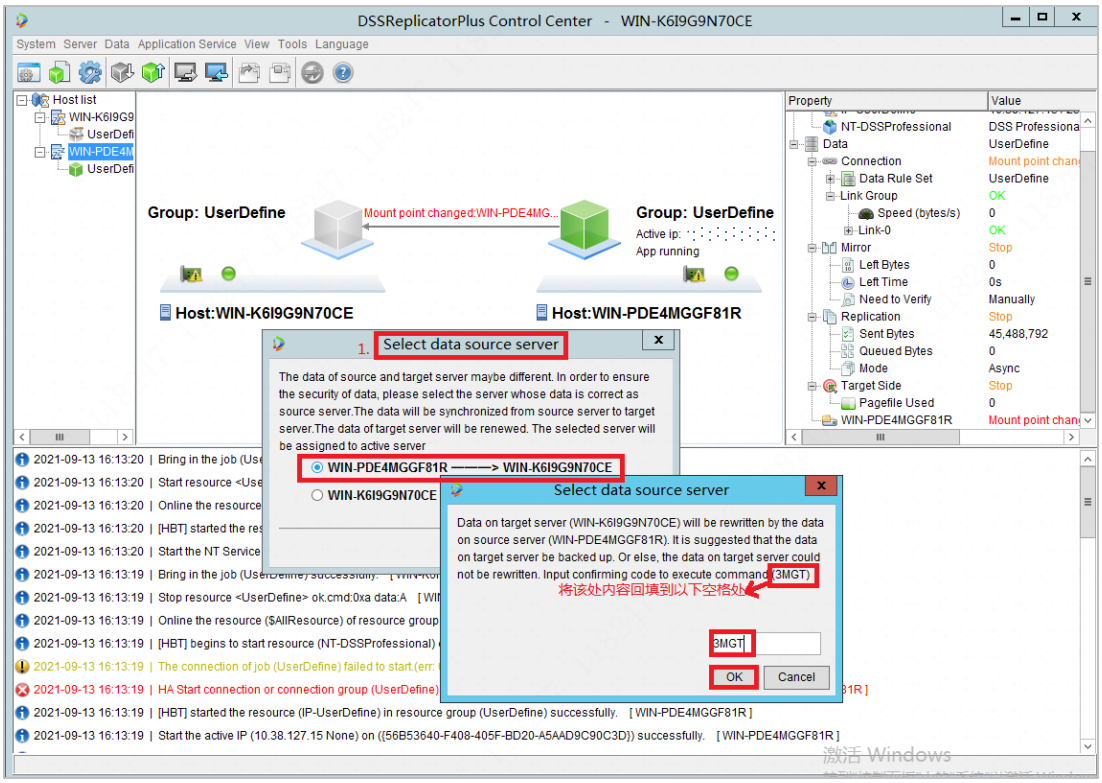
Change of mount point: While synchronizing the data of the active and standby servers, the data synchronized are operated, and then the hot standby software will stop the synchronization based on the data protection mechanism. The exception is shown in the following figure:



Now you need to manually recover in the hot standby software: Application Service > Select Data Source. After selecting the data source, the hot standby synchronization will be automatically recovered.

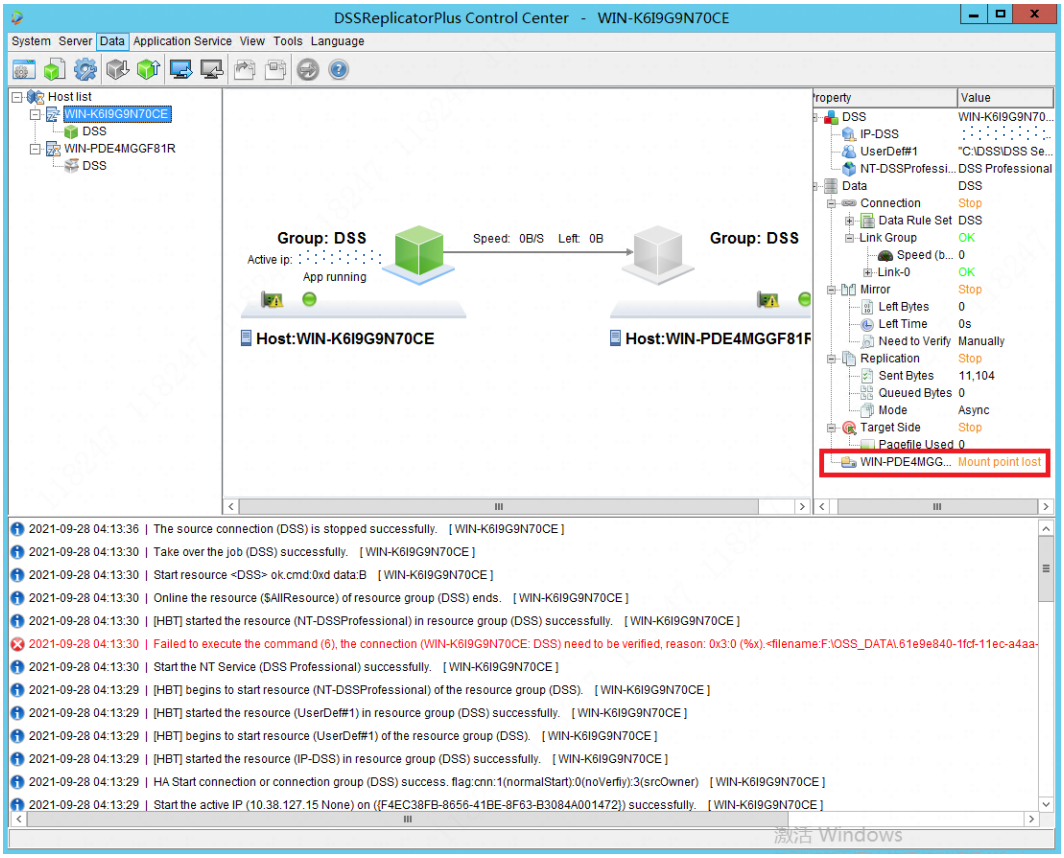


After clicking **Select Data Source**, the **Select Data Source Server** pop-up window will appear. Select the data synchronization direction, as shown in the following figure. When you choose to synchronize the data from WIN_PDE4MGGF81R to WIN_K6I9G9N70CE, the data in WIN_K6I9G9N70CE will be overwritten.



11. Hot Standby Software Prompting Loss of Mount Point?

Loss of mount point: Check whether the disks, configured with folder synchronization, are deleted or switched to other disk types. If such operations are performed, update the configuration of file synchronization in the hot standby software; if not, confirm whether the folder synchronization paths configured in the hot standby software are consistent in the active and standby servers. Configuration of file synchronization: **Application Service** > **Modify** / **Preview** > List of Data Presentation.


DSSReplicatorPlus Control Center - WIN-K6I9G9N70CE
System Server Data Application Service View Tools Language
Host list
WIN-K6I9G9N70CE
DSS
WIN-PDE4MGGF81R
DSS
Group: DSS
Active ip:
App running
Speed: 0B/S Left: 0B
Group: DSS
Host:WIN-K6I9G9N70CE
Host:WIN-PDE4MGGF81F
roperty
Value
DSS
WIN-K6I9G9N70...
IP-DSS
UserDef#1
"C:\DSS\DSS Se...
NT-DSSProfessi...
DSS Professional
Data
DSS
Connection
Stop
Data Rule Set
DSS
Link Group
OK
Speed (b...
0
Link-0
OK
Mirror
Stop
Left Bytes
0
Left Time
0s
Need to Verify
Manually
Replication
Stop
Sent Bytes
11,104
Queued Bytes
0
Mode
Async
Target Side
Stop
Pagefile Used
0
WIN-PDE4MGG...
Mount point lost
2021-09-28 04:13:36 | The source connection (DSS) is stopped successfully. [WIN-K6I9G9N70CE]
2021-09-28 04:13:30 | Take over the job (DSS) successfully. [WIN-K6I9G9N70CE]
2021-09-28 04:13:30 | Start resource <DSS> ok.cmd:0xd data:B [WIN-K6I9G9N70CE]
2021-09-28 04:13:30 | Online the resource ($AllResource) of resource group (DSS) ends. [WIN-K6I9G9N70CE]
2021-09-28 04:13:30 | [HBT] started the resource (NT-DSSProfessional) in resource group (DSS) successfully. [WIN-K6I9G9N70CE]
2021-09-28 04:13:30 | Failed to execute the command (6), the connection (WIN-K6I9G9N70CE: DSS) need to be verified, reason: 0x3:0 (%x).<filename:F:\OSS_DATA\61e9e840-1fcf-11ec-a4aa-
2021-09-28 04:13:30 | Start the NT Service (DSS Professional) successfully. [WIN-K6I9G9N70CE]
2021-09-28 04:13:29 | [HBT] begins to start resource (NT-DSSProfessional) of the resource group (DSS). [WIN-K6I9G9N70CE]
2021-09-28 04:13:29 | [HBT] started the resource (UserDef#1) in resource group (DSS) successfully. [WIN-K6I9G9N70CE]
2021-09-28 04:13:29 | [HBT] begins to start resource (UserDef#1) of the resource group (DSS). [WIN-K6I9G9N70CE]
2021-09-28 04:13:29 | [HBT] started the resource (IP-DSS) in resource group (DSS) successfully. [WIN-K6I9G9N70CE]
2021-09-28 04:13:29 | HA Start connection or connection group (DSS) success. flag:cnn:1(normalStart):0(noVerfiy):3(srcOwner) [WIN-K6I9G9N70CE]
2021-09-28 04:13:29 | Start the active IP (10.38.127.15 None) on ({F4EC38FB-8656-41BE-8F63-B3084A001472}) successfully. [WIN-K6I9G9N70CE]
激活 Windows