nSSVMulti-managementnode +EnterprisenSDSConverged deployment implementation plan

Table of Contents

1. Basic information about the project

This project uses NexaVM cloud platform management software, cloud Enterprise Edition distributed storage software NSDS and 3 servers to deploy a private cloud environment.

2. Pre-implementation considerations

- The password of the operating system of the physical machine needs to be set to uppercase letters + lowercase letters + special characters + numbers, and the password for logging in to the UI of the cloud platform and storage platform needs to be set to a complex password.
- nSDS needs to be manually password-free during capacity expansion, and the password-free function on the UI cannot be used in capacity expansion scenarios
- When scaling out nSDS, you need to stop the iptables service of the new node

3. Hardware planning

This project has a total of 3 x86 servers, using NexaVM hyper-convergence solution to deploy the cloud platform, by two management nodes to control the entire cloud platform, providing management node high availability function, when any one of the management nodes loses contact, it will automatically trigger a second-level high availability switch, so as to ensure that the management node continues to provide services.

The three servers serve as compute nodes and storage nodes to provide KVM virtualization and distributed storage services, respectively, and two servers serve as management nodes to provide cloud platform management services.

RAID and hard disk planning

server	harddisk	planning
Hyperconverged Node * 3	Systemdisk:480GBormoreSSD* 2	RAID1，Write-through
	Cache disk: 480GB or more SSD *2	Non-RAID or JBOD
	Datadisk:4TBormoreHDD*4	Non-RAID or JBOD

In order to ensure the data security of the platform, the three-copy mechanism is used for storage replicas.

4. Network planning

4.1 Network topology planning

This project defines three types of network traffic models: management networks, business networks, and storage networks.

Management network: Dual-gigabit network is used, which is mainly used to manage hardware resources related to the cloud platform. In scenarios with sufficient network

resources, dual 10 Gigabit networks can also be used.

Business network: Dual-10 Gigabit service network is mainly used for the business network of cloud hosts on the cloud platform to provide application services.

Storage network: Dual 10 Gigabit is used, which is mainly used to carry distributed storage traffic. We recommend that you set the Access mode to check whether the switch supports Jumbo Frame, and if so, enable it and set the full-link MTU to 9000.

4.2 Network configuration planning

M-LAG should be configured on the management network, service network, and storage network to ensure high network availability, and Bonding mode 1 should be configured on the server NIC to ensure high network availability. If you want to configure the mode 4 LACP mode, you must configure LACP dynamic link aggregation on the corresponding interface of the switch.

Switch configuration in the standard scenario:

- Configure the Access mode for the port of the management network switch.
- Configure trunk mode for the service network switch port.
- Configure the Access mode for the storage network switch port.

Server NIC configuration in the standard scenario:

- Configure the Bond active/standby mode for the management network Gigabit NICs.
- The 10 Gigabit NIC of the service network is configured in Bond active/standby mode.
- The 10 Gigabit NIC on the storage network is configured in Bond active/standby

mode.

Server NIC and switch port planning

Server bond name	use	Bond mode	Server network card	Switch port configuration
bond0	Manage the network	Active/standby mode	enp175s0f0	Access mode
			enp176s0f0	
bond1	Business network	Active/standby mode		Trunkmode
bond2	Storage networking	Active/standby mode		Access mode

According to the above network architecture, network equipment and servers are connected. We recommend that you configure ACL rules for switches to strengthen network security protection and prevent network attacks on servers.

5. System installation and basic configuration

5.1 Prepare the installation package

Before installing and deploying, the following software installation packages need to be prepared:

Software	version	illustrate
NexaVM	1.10.18 H84r	Operating system and cloud platform management services
nSSV-Multinode-HA-Suite	1.10.18	ZSHA2 Dual Management Node High Availability Suite
nSDS	6.4	Enterprise Edition distributed storage package

TheNexaVMOSISOimagecanbeburnedtoaUSBflashdriveusingRufus (recommended)/UltraISO/orFedoraMediaWritertools.

5.2 Configure the server

- Confirmthatthedataontheharddiskintheserverhasbeenbackedup,andthe installation process will overwrite the write.
- GotoBIOSandenabletheCPUVTandHToptions.
- EnterBIOS,generallyinAdvancedopenCPUConfigurationclickCPUPOWEROpen ManagementConfigurationselectIntelCStateandPStatetoclose.
- EntertheRAIDconfigurationpagetoconfiguretheHDDaccordingtotheplanto provide certaindataredundancyfeatures.
- SettheUdiskasthefirstbootsequence,andsetthesystemdiskasthefirstboot sequenceafter theinstallationiscompleted.

5.3 System installation and basic configuration

All servers are used as KVM virtualization nodes, and you need to select the Cloud ComputeNode optionwheninstallingthesystem.

All physical machines do not need to configure IP addresses for the time being, and configure IP addresses inside the operating system after the operating system is installed.

The system partition must use the standard partition mode, and the detailed configuration is as follows:

- /boot to create a partition of 1GB;
- /, root partition, configure the remaining capacity (do not allocate SWAP

partitions);

- To install the system, you only need to check the system disk to be installed, and do not checkotherharddisks;
- The default time zone is Asia East 8, and it is recommended that administrators check the time of the physical machine in advance and configure it to the current time and time zone.
- The network is not configured during installation, and it is manually configured after enteringthesystem.
- IfUEFIbootisused,youneedtoconfigureanadditional1G/boot/efipartition; Ifthesystem diskcapacityexceeds2TBandthesystemdiskcapacityexceeds2T, youneedtoconfigure thedefaultBIOSBootpartitionof1024KIBtosupportGPT.
- SomeoldmodelsdonothavegoodsupportforUEFI,andthereisaproblemwith the installation system, you can consider modifying the boot item in BIOS to installthesystem inLegacymode.

5.4. Set up the basic network environment

The server network configuration needs to be configured according to the project plan to ensure that there is no network conflict with the existing service platform. If there are scenarios such as subsequent expansion and network interconnection, you need to reserve an IPaddressduringplanning inadvance.

Manage network configurations:

1. create a bond in master-standby mode, using bond0 for the default naming convention, zs-bond-ab for master-standby mode, and zs-bond-lacp for LACP mode:

   [root@node-1 ~]# zs-bond-ab -c bond0

2. To bind a physical NIC to the management network bond0:

   [root@node-1 ~]# zs-nic-to-bond -a bond0 enp175s0f0

   [root@node-1 ~]# zs-nic-to-bond -a bond0 enp175s0f1

3. Configure the management network bond0 IP address, and the -b parameter is to create a bridge based on the interface and configure the address:

   - Run the following command in Access mode:

     [root@node-1 ~]# zs-network-setting -b bond0 172.27.52.169 255.255.248.0 172.27.0.1

   - In trunk mode, the switch must configure VLANs to pass through the corresponding port (the VLAN ID in this example is 100), and then run the following commands:

     [root@node-1 ~]# zs-vlan -c bond0 100

     [root@node-1 ~]# zs-network-setting -b bond0.100 172.27.52.169 255.255.248.0 172.27.0.1

Service Network Configuration:

1. To create a bond in active/standby mode, the default naming rule is bond1:

   [root@node-1 ~]# zs-bond-ab -c bond1

2. Bind a physical NIC to a service network Bond1:

   [root@node-1 ~]# zs-nic-to-bond -a bond1 enp176s0f1

   [root@node-1 ~]# zs-nic-to-bond -a bond1 enp177s0f1

StorageNetworkConfiguration:

1. To create a bond in active/standby mode, the default naming rule is bond2:

   [root@node-1 ~]# zs-bond-ab -c bond2

2. To bind a physical NIC to a storage network bond2:

   [root@node-1 ~]# zs-nic-to-bond -a bond2 enp176s0f2

   [root@node-1 ~]# zs-nic-to-bond -a bond2 enp177s0f2

3. Configure the storage network bond2 IP address, bond2 as the storage network, no need to configure the gateway:

   [root@node-1 ~]# zs-network-setting -b bond2 192.168.79.11 255.255.255.0

Network Configuration Check:

1. Check whether the bond is created and whether the NIC is bound correctly

   [root@node-1 ~]# zs-show-network

2. Check that the IP address is configured correctly

```
[root@node-1 ~]# ip -4 addr
```

If you need to adjust the network configuration or make the wrong configuration, you can delete it according to the appendix.

Note: If you plan to use a VXLAN network, when you create a VTEP interface, you must directly configure the address on the bond NIC, physical NIC, or NIC VLAN sub-interface (for example, bond1, enp176s0f0, and bond1.208). If a NIC configured with a VTEP IP address is configured, you cannot use the same NIC (NIC for VTEP IP) and VLAN ID to create a Layer 2 network on the cloud platform.

6. Time synchronization configuration, server hostname, and SSH passwordless configuration

6.1. Time synchronization scheme

In the time synchronization scheme, a management node on the intranet serves as a time server to provide server synchronization services within the cluster, and the management node synchronizes with the customer's time source or public network time source. When the external network or network fails, the management node can still provide internal time synchronization services to ensure time synchronization within the cluster.

6.2. Server hostname configuration, time synchronization, and SSH passwordless configuration

Configure SSH password-free between servers, and set hostname and time synchronizationinbatches

1. Unzip the nSSV_tools.tar.gz toolkit, which can be used to enable SSH-less login between nodes, hostname configuration, and time synchronization server setup

   [root@node-1 ~]# tar -zxvf nSSV_tools.tar.gz

   [root@node-1 ~]# cd nSSV_tools/

2. Modify the ansible/hosts.example configuration file.:

   - Under [nodes] is the IP address of all nodes, ansible_user for the SSH username and ansible_pass for the SSH password. The same password should be used for each physical machine initially.
   - Under [chrony] is the cluster time synchronization server

   [root@node-1 nSSV_tools]# vim ansible/hosts.example

   Configuration example:

   ```
   [nodes]
   172.27.52.169  #Node IP, use the management network IP to configure
   172.27.52.134
   172.27.52.238


   [nodes:vars]
   ansible_user=root   # Node username and password
   ```

```
        ansible_ssh_pass=password


        [Chrony]
        172.27.52.169 #节点 IP, use the management network IP to configure
```

3. Editorial ansible/group_vars/nodes, Configuring Hostname Prefixes:

```
[root@node-1 nSSV_tools]# vim ansible/group_vars/nodes
  hostname_prefix: node-   # The server hostname prefix will be configured in node-1 format
```

4. Run the command to start the configuration. The tool will also automatically deploy the /etc/hosts file for each node, turn off the firewall, and more

```
[root@node-1 nSSV_tools]# ./prepare.sh -i ./ansible/hosts.example
```

5. Manually verify that the configuration is correct

7. Cloud platform management node service installation and configuration

7.1 Install the Admin Node service

The management node service plays a core role in the coordination and management of the cloud platform. Responsible for the management of virtual machines and the scheduling and allocation of resources, including computing, storage, and networking.

Install the management service on the two management nodes, and the detailed installation steps are as follows:

1. Use the bin file to install the Cloud Management Node service

```
[root@node-1 ~]# bash /opt/nSSV-install.bin -E
```

2. Set the default size of the management node to medium scale, and optimize the management node

```
[root@node-1 ~]# nSSV-ctl set_deployment -s medium
```

7.2 Install the Dual Admin Node High Availability Kit

The cloud platform provides multi-management node high-availability capabilities in the

form of a separate high-availability suite. When any of the management nodes loses connection, a high-availability switchover is triggered in seconds to ensure that the management nodescontinuetoprovideservices.

On one of the management nodes, run the following command to deploy the ManagementServicesHASuite:

1. Unpack the High Availability Suite tarball "nSSV-Multinode-HA-Suite.tar.gz"

   [root@node-1 ~]#mkdir zsha2_install

   [root@node-1~]#tar-xzvfnSSV-Multinode-HA-Suite.tar.gz-C./zsha2_install

2. Generate an installation configuration file and configure it

   [root@node-1 zsha2_install]#./zsha2 sample-config>zsha2-install.config

   [root@node-1 zsha2_install]# vim zsha2-install.config

   Configuration example:

   {

   "gateway": "172.28.16.1", # Arbitration Gateway, which is generally the gateway for the management node to manage the network

   "datalink": "", # Cloud does not need to fill in this configuration, just leave it as default "virtualIp":"172.27.19.20", # Dual-managementnodeserviceVIPaddress

   "myIp": "172.27.52.169", # 本 ThemanagementnodemanagestheIPaddressofthenetwork "peerIp": "172.27.52.134",#PeerManagementNodeIPaddress

   "peerSshUser":"root",#PeerManagementNodesshusername

   "peerSshPass":"password", #PeerManagementNodesshpassword

   "peerSshPort": 22, # Peer Management Node SSH port

   "dbRootPass":"zstack.mysql.password", #Databaserootpasswordforbothadminnodes(must be the same)

   "interface": "br_bond0", #NIC name, which is usually the bridge where the IP address of the management network is located

   "timeServer": "172.27.52.169# Time Synchronization Server IP,Enter the IP address of the first management nodeaccordingtothetimesynchronizationplanningschemeinthesolution

   }

3. Install the ZSHA2 high-availability package

```
[root@node-1 zsha2_install]# ./zsha2 install-ha -config zsha2-install.config
[root@node-1 zsha2_install]# zsha2 status
```

7.3. Change the database password to a complex password

To improve the security of the cloud platform, you need to change the default password of the database to a complex password. Complex passwords protect sensitive information in the database from unauthorized access and potential attacks by making it more difficult to crack passwords, while configuring database access policies to allow only internal methods withinthecluster.

1. Change the password of the root and nSSV users of the database, and the default password is a complex password

```
[root@node-1 ~]# cloud-ctl change_mysql_password --root-password zstack.mysql.password --user-name root --new-password Cloud@P0sswd24root
[root@node-1 ~]# cloud-ctl change_mysql_password --root-password Cloud@P0sswd24root --user-name cloud --new-password Cloud@P0sswd24cloud
```

Parameter explanation: --root-password is the current root user password; --user-name is the user name whose password needs to be changed; --new-password is the new password;

2. Configure database access restrictions so that only the management node can access the database

```
[root@node-1 ~]# cloud-ctl mysql_restrict_connection --root-password Cloud@P0sswd24root --restrict
```

7.4 Set up the Admin Node DNS server

SettheDNSserveraddressesofthetwomanagementnodessothatthecloudplatform can performdomainnameresolutionwhenconfiguringemailalarmsorDingTalkalarms。 Here'show tosetitup:

1. Edit and manage the NIC configuration file and add DNS configuration

```
[root@node-1 ~]# echo “DNS1=114.114.114.114” >> /etc/sysconfig/network-scripts/ifcfg-br_bond0
```

2. Edit the DNS configuration file

```
[root@node-1 ~]# echo “nameserver 114.114.114.114” >> /etc/resolv.conf
```

7.5 Configure the firewall rules of the cloud platform

Firewall rules are configured on each of the two management nodes to ensure that critical services can communicate properly.

1. Edit the management service configuration file and add firewall rules

```
[root@node-1 ~]# vim /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties
```

Add the following to the configuration file:

2. Restart the two Admin Node services separately for their firewall configurations to take effect

```
[root@node-1 ~]# zsha2 stop-node & zsha2 start-node
```

8. Distributed storage service installation and configuration

8.1 Installing a Distributed Storage Service

On the first management node server, decompress the distributed storage installation package and deploy the distributed storage nSDS service.

1. Unzip the distributed storage installation package

```
[root@node-1 ~]# mkdir sds
[root@node-1 ~]# tar -zxvf ZCE-installer.tar.gz -C sds/
```

2. Edit the storage installation configuration file and change the Prometheus monitoring port to 9089

```
[root@node-1 ~]# vim install.conf
  PROMETHEUS_PORT=9089
```

3. To install the storage management service, use install.sh to specify the network IP address used to deploy the distributed storage NSDS environment. By default, the network is planned as a management network for distributed storage, which is generally accessible by browsers

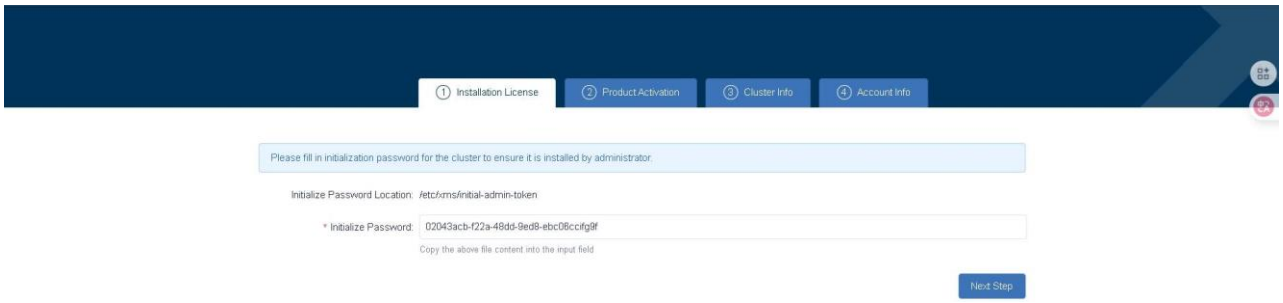
```
[root@node-1 ~]# ./install.sh 172.27.52.169
```

8.2 Distributed storage service configuration

8.2.1 Cluster initialization

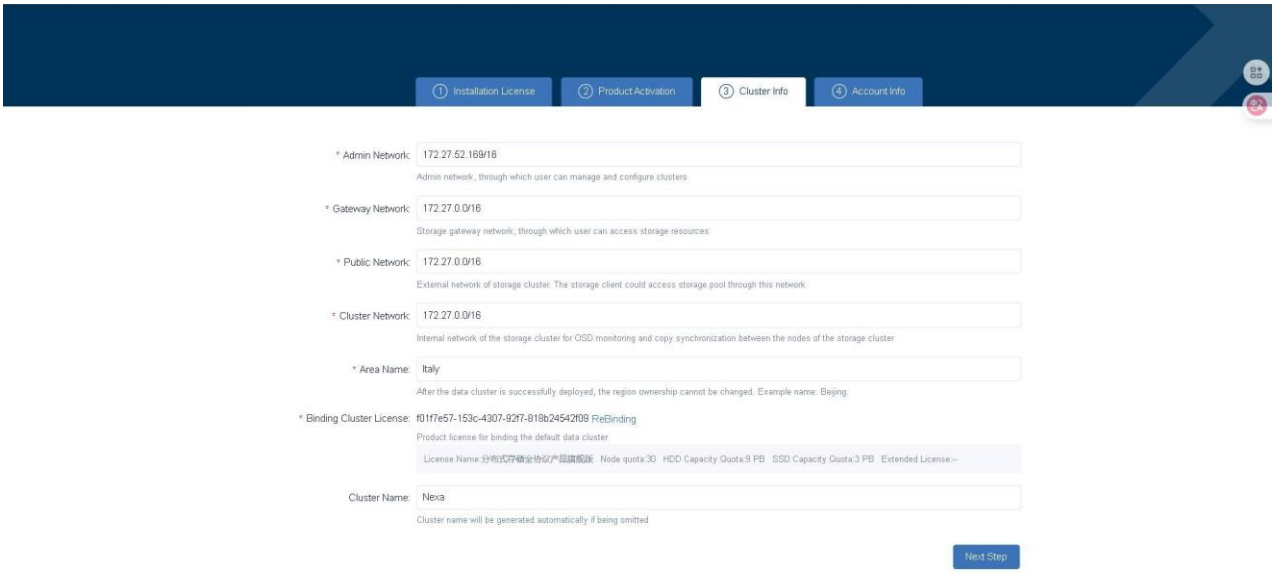
By default, the management IP address and port 8056 (for example, http://172.27.52.169:8056) are used on the DCS UI, and the cluster needs to be initialized whenyoulog intotheNSDSUIforthefirsttime.

When initializing, you need to enter the initialization key, which is stored in /etc/xms/initial-admin-token, and click Next (the installation and deployment version comes with a 1-month test authorization, please update the official authorization after the installation and deployment is completed).




```
# cat /etc/xms/initial-admin-token
63d75257-1cc6-48ec-a021-7378c8278a02
```

Configuredistributedstoragenetworkinformation;

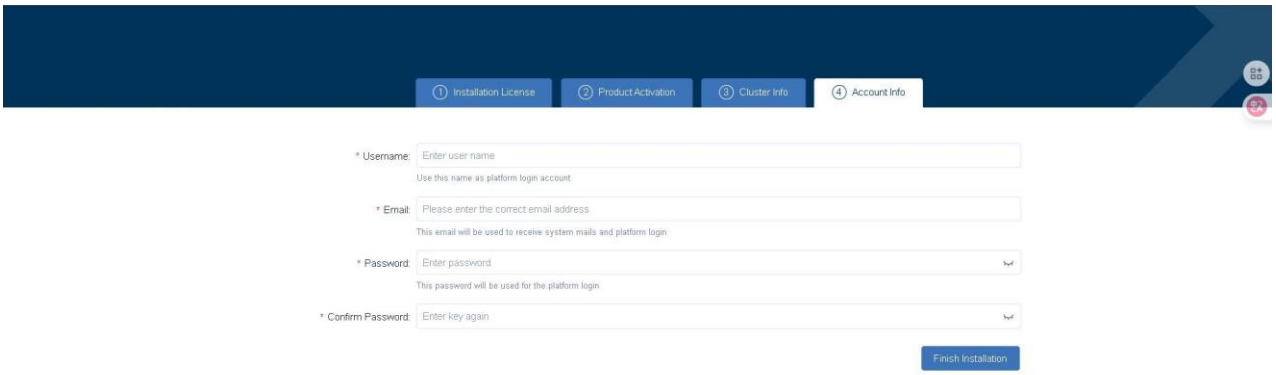


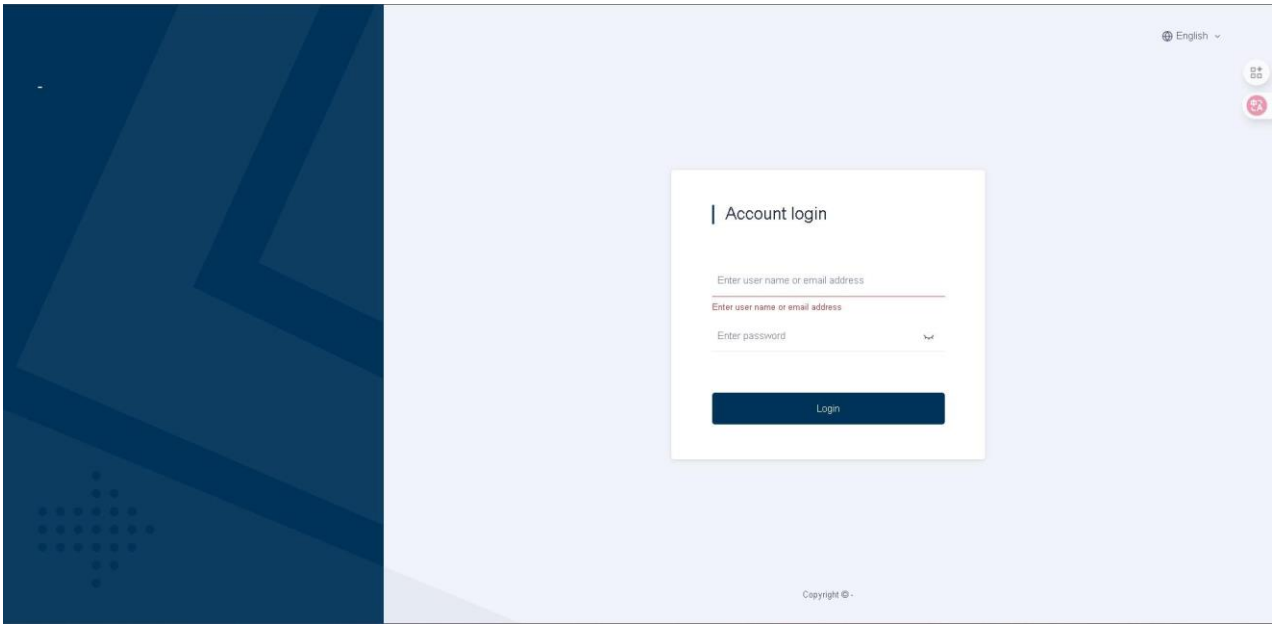
- **Cluster Name: Nexa** cluster information, 1–128 characters, lowercase letters (a-z), digits (0-9), and periods (.) and a hyphen (-), and the hyphen (-) cannot be placed at the beginning or end of the name. It is not advisable to start with a number.
- **Admin Network:** This network is used to manage and configure the storage cluster, provides management functions such as UI and API, and uses the IP specified when installing distributed storage by default, usually corresponding to the management network of the NexaVM cloud platform.
- **Gateway Network:** This network is used to access iSCSI raw devices and object storage. If you are not using iSCSI raw devices and object storage, the storage gateway network can be the same as the public or cluster network of the storage cluster. For scenarios that only use distributed block storage, we recommend that you usetheplannedstoragenetworkIP.
- **Public Network:** This network is used for RBD clients to access and provide Ceph Mon IPs. In the Cloud platform, the QEMU is usually connected to the RBD through this network, which corresponds to the storage network of the Cloud platform. For

scenarios that only use distributed block storage, we recommend that you use the planned storagenetworkIP.

- Cluster Network: This network is used for data monitoring and replica synchronization between hosts in a storage cluster. Small-scale clusters can be reused with the storage Public Network, and large-scale clusters with more than 10 nodes are recommended to be deployed separately from the Storage Public Network, which is usually shared with the "PublicIPCIDR".

Configure distributed storage account information;





8.2.2 Server added

The path to add a server is Resource Management - > Node - > Add, and the first server has been added as the management role (management service) and monitoring role (Ceph Monitor service) by default.

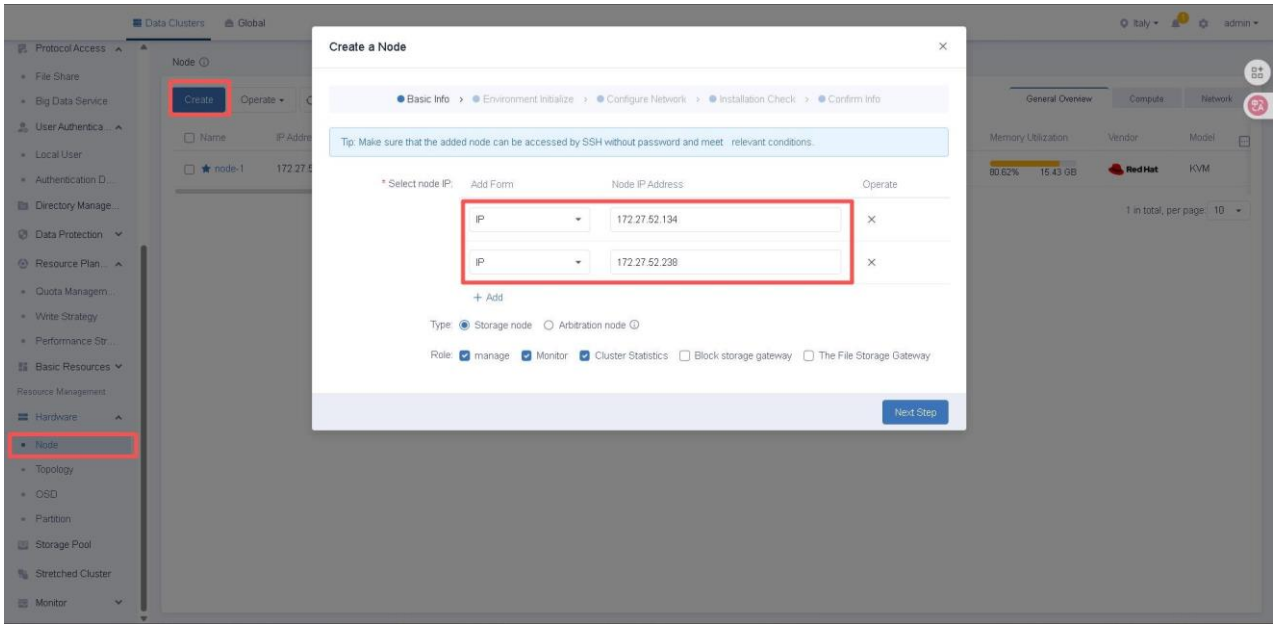
You need to add two other storage nodes as storage servers, and select the management role (management service) and monitoring role (Ceph Monitor service).

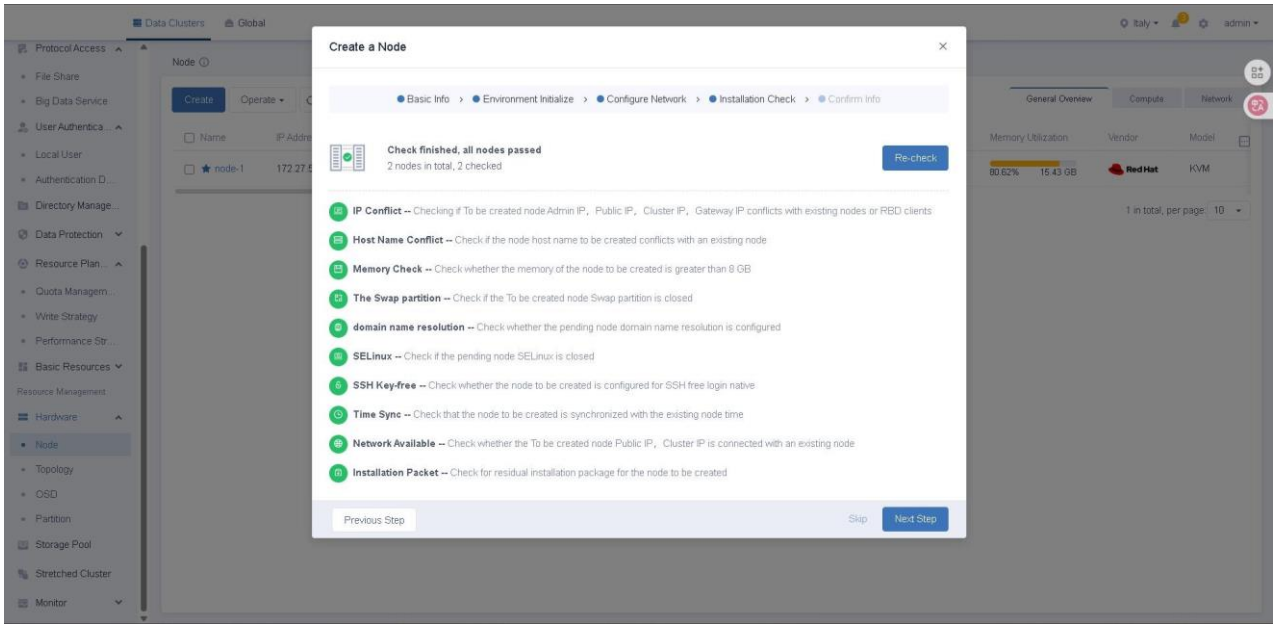
By default, all added servers are used as block storage gateways to provide storage functions. If there are more than three storage nodes, the storage nodes can be selected according to the actual situation

You need to add all compute nodes as gateway servers, and select the block storage gateway role by default to make them clients of the entire Ceph storage cluster. After the data isadded,runceph-son thecomputenodetoquerythecurrentcephstoragestatus.

Note: Before clicking Confirm, make sure that the machine to be added and the storage node in the cluster have been password-free from each other. And the time servers are

synchronized.

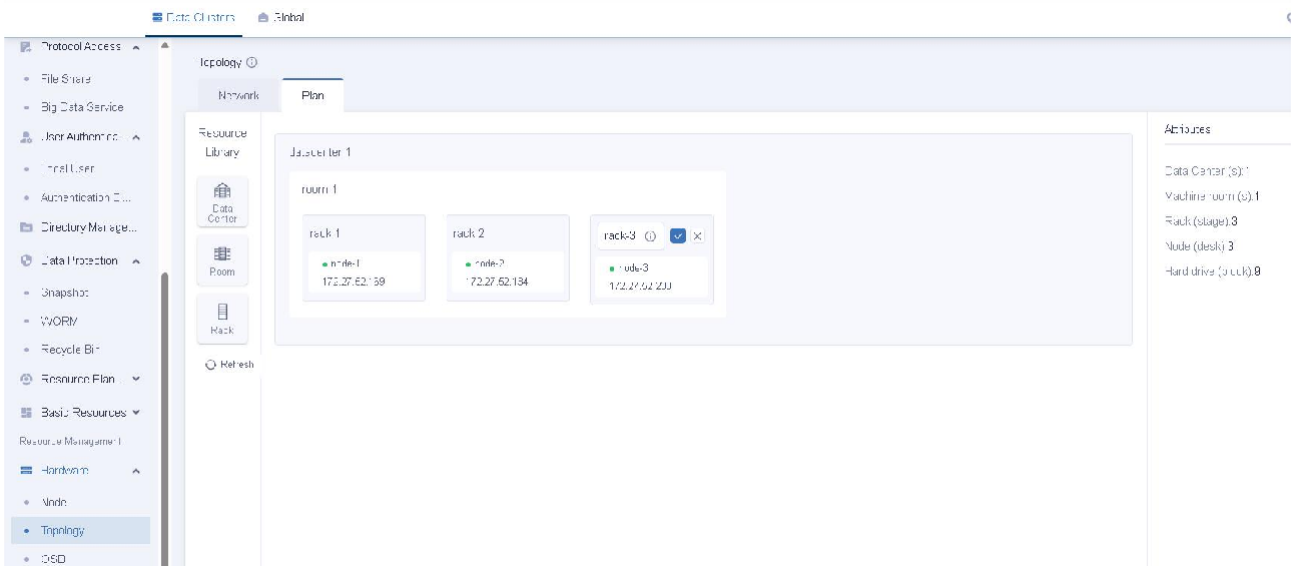




8.2.3 Topology creation

On the topology management page of Resource Management, create a data center and drag the data center on the left to complete the creation.

Create a rack, drag the left rack, and add all the servers to the cabinet.



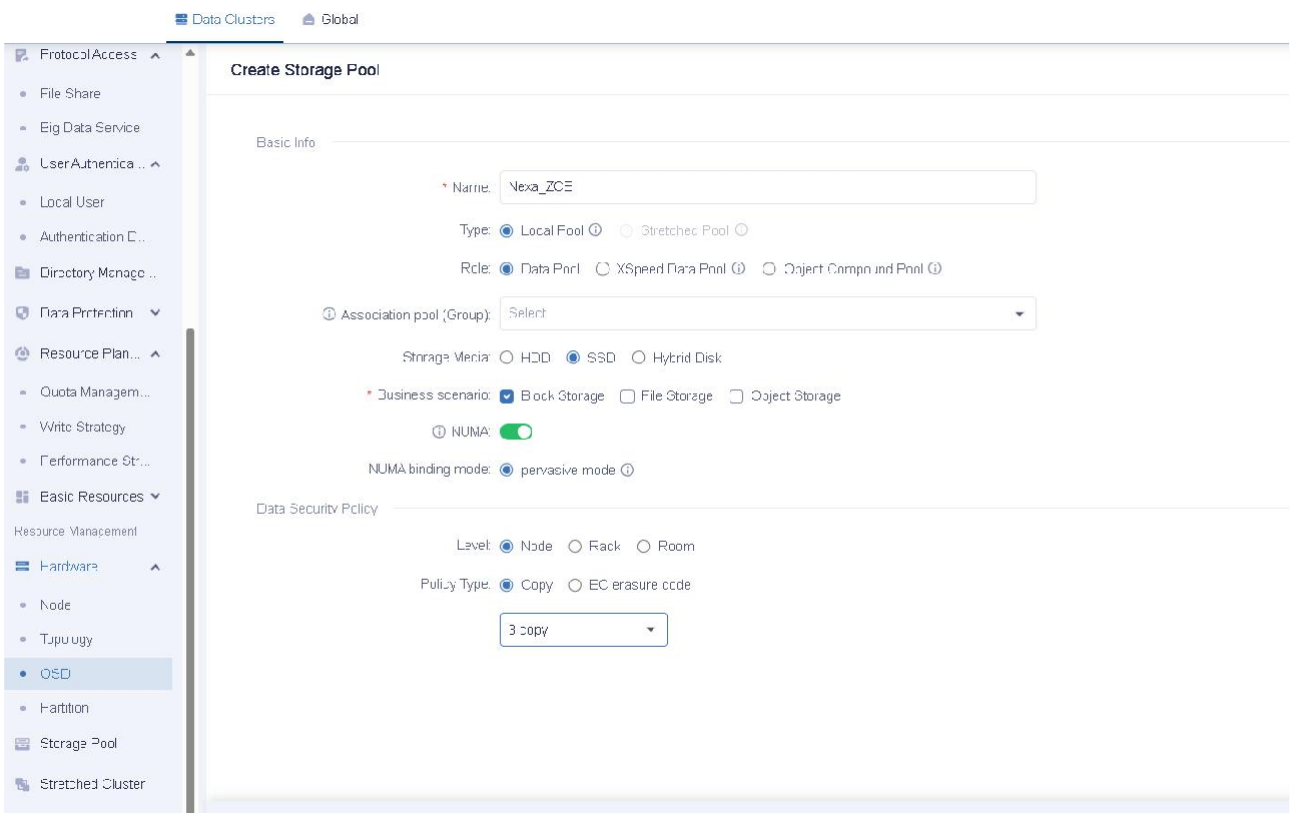
8.2.4 Add an SSD cache disk

On the Cache Management page of Resource Management, add a cache disk. If the environment is all SSDs, you can add disks without adding cache disks.

The ratio of SSDs to SATAs is usually recommended to be 1:5, and SSDs with PCIE interfacescanbeupto1:10.

8.2.5 Storage pool creation

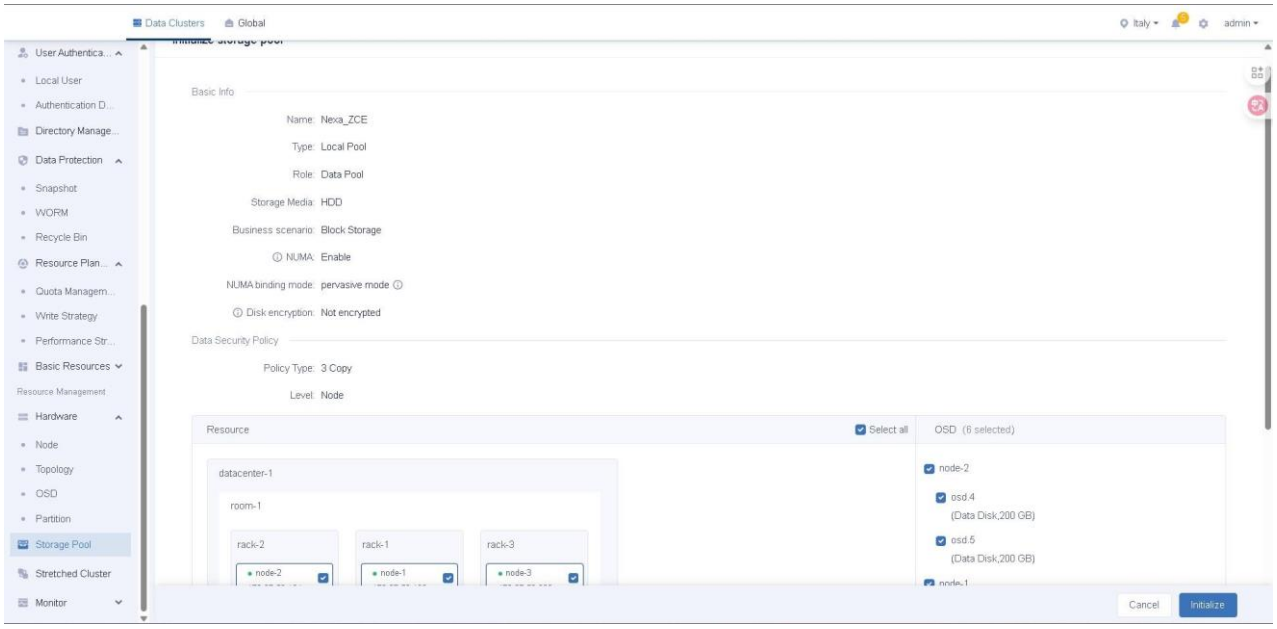
You need to create a storage pool before you create a hard disk. Create a storage pool, set the storage pool role according to the planning situation, set the data pool as an example, select a hybrid disk as a storage medium, configure a cache partition to select a hybrid disk, set the example is block storage, set the policy type to replica, and click "Create" after the configurationiscomplete.



After the storage pool is created, click "Create" to create a hard disk, check the HDD of each node and select the cache mode as Automatic.

When you need to set a cache partition for the disk, you can choose the manual mode; If the memory is sufficient, the memory read cache can be set to 512M, and click "Create" to continue.

After the disk is created, click Initialize to initialize the storage pool. Select each storage node, select Data Disks, and click Initialize.



9. Configure the image server of the cloud platform

There are two main types of mirror servers: ImageStore and Ceph

- ImageStore: applies to the Enterprise Edition, uses incremental storage, and supports online snapshots, online image creation, and online cloning.
- Ceph: Ceph distributed block storage is used to support online snapshots, online image creation, and online cloning.

In the distributed primary storage scenario, we recommend that you use a Ceph image server.

9.1 Ceph type mirror server configuration

You can add a Ceph image server during the initialization phase of the cloud platform or after initialization in the initialization path of Resource Center > Mirror Server > Add Mirror Server to the cloud platform.

Mirrored storage pools can be reused with primary storage pools unless otherwise

planned.

9.2 ImageStore Image Server Configuration

It is recommended to plan the number of two or more hard disks and configure RAID 1, RAID5,or RAID10forthisdatadisktoimprovedataredundancy.

Before adding an ImageStore image server, you need to format and mount the data disk in advance and configure automatic mounting at startup, and run the following command (for example, sdb is used as the data disk for configuration, and the on-site environment is used for deployment in the production environment):

1. Set the format of the data disk partition table to GPT

   [root@node-13 ~]# parted /dev/sdb mklabel gpt

   [root@node-13 ~]# parted /dev/sdb mkpart primary 0% 100%

2. Format the data disk

   [root@node-13 ~]# mkfs.xfs -f -i size=512 -l size=128m,lazy-count=1 -d agcount=16 /dev/sdb1

3. Create a data directory and attach a data disk

   [root@node-13 ~]# mkdir /cloud_bs

   [root@node-13 ~]# mount /dev/sdb1 /cloud _bs

4. Configure automatic mounting at start-up

```
[root@node-13 ~]# blkid /dev/sdb1
 /dev/sdb1: PARTLABEL="primary" PARTUUID="9e6c3e37-e02d-4649-b819-bc13580f00ef"
[root@node-13 ~]# chmod +x /etc/rc.d/rc.local
[root@node-13 ~]# echo 'sleep 5' >> /etc/rc.d/rc.local
[root@node-13 ~]# echo 'mount /dev/disk/by-uuid/9e6c3e37-e02d-4649-b819-bc13580f00ef
    /cloud_bs' >> /etc/rc.d/rc.local
```

5. Check whether the data disk is successfully attached

```
[root@node-13 ~]# df -h
```

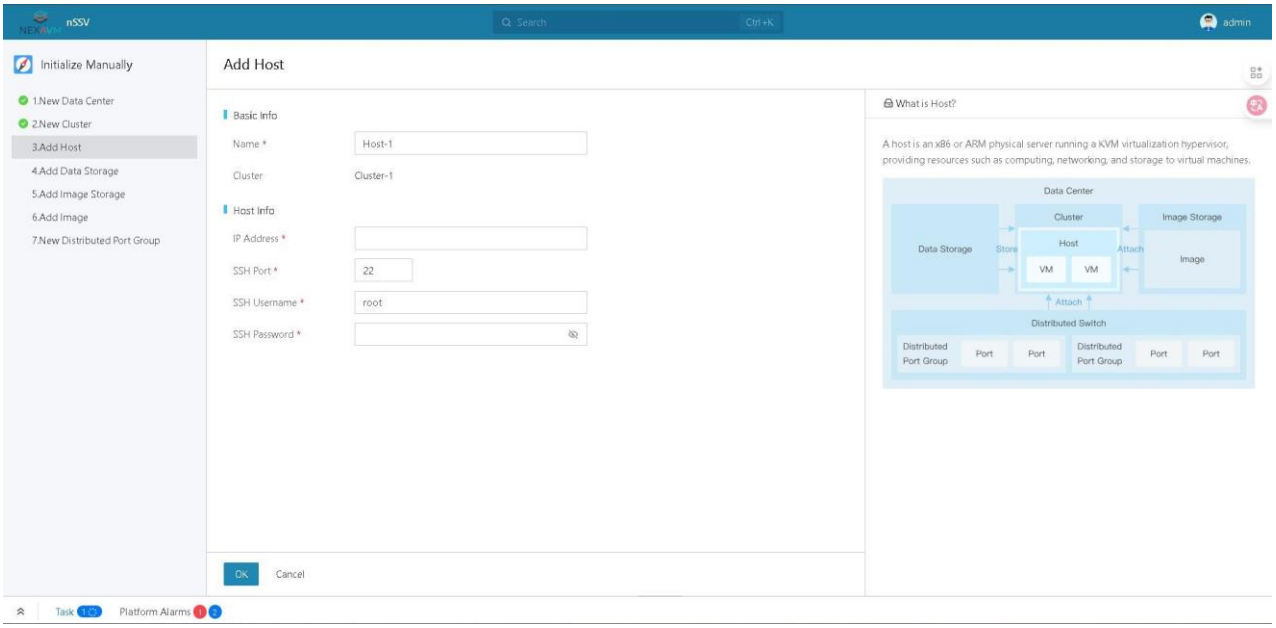
Note: If the hard disk capacity is huge, such as more than 32T, you can use mkfsThe agcount parameter of xfs is increased to 32 or 64

After the configuration is complete, you can add the cloud platform during the initialization phase or after initialization, and the path to add the cloud platform after initialization is Resource Center > Mirror Server > Add Mirror Server.

10. Initialize the configuration of the cloud platform

Log in to NexaVM for the first time and enter the corresponding URL in Chrome 49 or later http://172.27.19.20:5000 (The format is http://$VIP:5000)Enter the default account name admin and the default initial password, and the system interface will guide you to the basic initialization environment configuration of the NexaVM platform.

The initialization wizard is divided into nine steps, and you can also manually create key resources after exiting the wizard.



Create Region: The largest resource definition in the cloud platform, including resources such as clusters, Layer 2 networks, and primary storage. Generally, it corresponds to a computer room in the data center. If you need to add it manually, set the path to Resource Center > Hardware Facilities > area.

Create a cluster: A logical collection of physical machines (compute nodes). If you want to add it manually, set the path to Resource Center -> Hardware Facilities -> Cluster.

Add a physical machine: A physical host that provides computing, network, storage, and other resources for the virtual machine instance. If you need to add more physical machines, you can manually add them in the Resource Center > Hardware Facilities > the physical machine path.

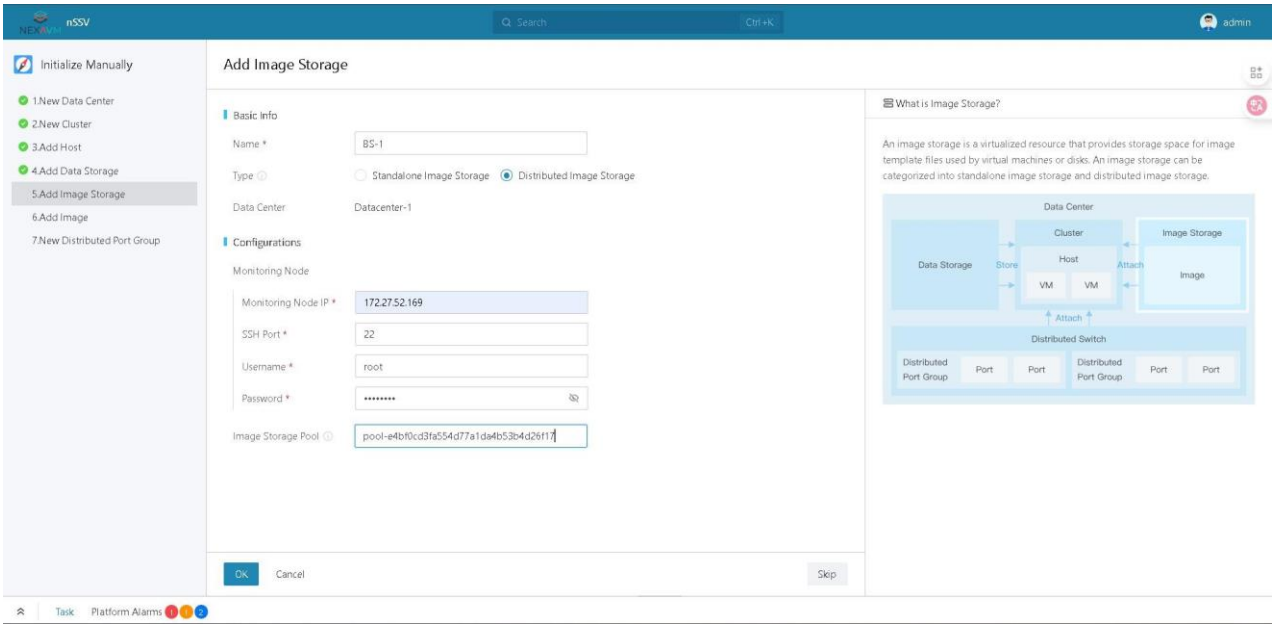
Add Mirror Server: A storage server used to store images of the virtual machine. The mirror server type is selected based on the plan in the scenario

- ImageStore type:

The mount path indicates the mount path of the data disk that is planned to be used for the storage image

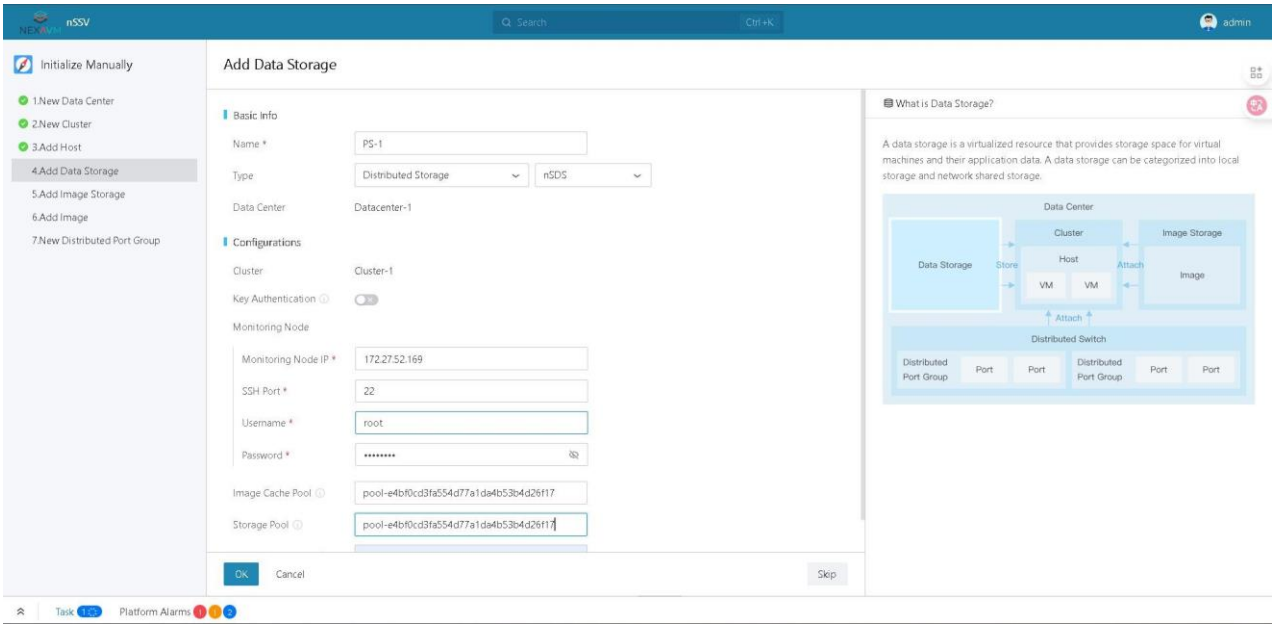
- Ceph Type:

You need to fill in the image storage pool to create a pool name in Ceph storage in advance, and the data network is the storage network, you need to note that only one Mon node IP is entered in the wizard process, usually the number of Ceph storage Mon nodes is 3 or more, you need to manually add the rest of the Mon nodes in the Ceph mirror server configuration path, and the added path is Resource Center > Hardware Facilities > Mirror Server - >Created MirrorServer->monitoringnode



Add Primary Storage: A storage server used to store virtual machine disk files (including: root cloud disk, data cloud disk, root cloud disk snapshot, data cloud disk snapshot, image cache, etc.).

You need to manually add the remaining Mon nodes in the configuration path of the primary storage > hardware facilities> primary storage, > "Created primary storage" > monitoring nodes



Create Computing Specifications: Define thespecificationsofthenumberofCPUs,memory, network settings, etc. involved in the virtual machine.

Add Image: The image template file used by the virtual machine or cloud disk includes two types:system imageandclouddiskimage.

Create a Layer 2 network: Corresponding to a Layer 2 broadcast domain, perform Layer 2 related isolation. The NIC name is the service network bond1 planned in the solution.

Create a three-layer network: The network configuration used by the virtual machine, including IP address ranges, gateways, DNS, etc.

11. Configure parameters for the production environment

After the cloud platform service part is completed, in order to ensure the performance, security, and stability of the system, you need to configure the recommended configuration in the production environment. The cloud platform has encapsulated some configuration items, and the template can be applied in the settings - > scenario encapsulation - > recommended configuration in the production environment. In a distributed storage hyper-converged

environment, an OSD needs to retain 5GB of memory, and the total reserved memory is 16GB+n*5GB (n is the number of OSDs on a single server). After the template values are modified, the template is applied for the configuration to take effect.

12. Authorization Updates

To speed up the deployment process, the cloud platform is deployed with a temporary license, which needs to be updated to a formal license after the deployment is completed.

Procedure to update the license of the cloud platform:

Click on the admin account in the upper right corner -> license management -> download the request code -> upload the official license after the application

After the distributed storage is successfully installed, the system provides a temporary license for 30 days by default, which needs to be updated in a timely manner. Enter the management interface, click the settings icon (gear) in the upper right corner, and select "Product Licensing" to enter the licensing page. Click Update Product, download the cluster key, apply for a formal license from the business and obtain the activation file, and then upload the file to complete the license update.

13. Database backup configuration

After the cloud platform is deployed, you need to configure periodic database backup tasks to protect the data security of the platform and prevent data loss. In extreme cases, if the system hard disk or hardware failure of the two management nodes is damaged or the cloud platform is unavailable at the same time, you can quickly install the cloud platform service on the other node and restore the database, and restore the cloud platform access within 5-10 minutes.

Management Node 1:

1. remote_backup_node1 backing up a database to a remote server, you need to perform password-free operations on the remote server on the management node in advance

```
[root@node-11  ~]# ssh-copy-id root@$remote_backup_node1_ip
```

2. On the management node, annotate the original default backup task and add a new scheduled backup task

```
[root@node-11 ~]# crontab -e
 #30 0,12 * * * cloud-ctl dump_mysql --keep-amount 14
 30 */2 * * * cloud-ctl dump_mysql --host root@172.28.16.13 --d --keep-amount 84
 0 8,21 * * * /opt/zstone-installer/backup-zstone-sql.sh
```

30 */2 * * * indicates that the database is backed up at 30 minutes every 2 hours and automatically backed up to the /var/lib/zstack/from-zstack-remote-backup/ directory of the remote server (172.28.16.13), and the latest 84 database backup files (one week) are continuously retained.

Management Node 2:

1. remote_backup_node2 backing up a database to a remote server, you need to perform password-free operations on the remote server on the management node in advance

```
[root@node-12  ~]# ssh-copy-id root@$remote_backup_node2_ip
```

2. On the management node, annotate the original default backup task and add a new scheduled backup task

```
[root@node-12 ~]# crontab -e
 #30 0,12 * * * cloud-ctl dump_mysql --keep-amount 14
 30 */2 * * * cloud-ctl dump_mysql --host root@172.20.0.100 --d --keep-amount 84
 0 8,21 * * * /opt/zstone-installer/backup-zstone-sql.sh
```

30 */2 * * * indicates that the database is backed up at 30 minutes every 2 hours, and is automatically backed up to the /var/lib/zstack/from-zstack-remote-backup/ directory of the remote server (172.20.0.100), and the latest 84 copies (one week) are retainedDatabase backup file.

Afterthescheduledtaskisconfigured,youmustruntheremotebackupcommandonthe managementnodetoverifywhetherittakeseffect.

```
[root@node-11  ~]# cloud-ctl dump_mysql --host root@172.28.16.13 --d --keep-amount 84
[root@node-12  ~]# cloud-ctl dump_mysql --host root@172.20.0.100 --d --keep-amount 84
```

Ensure that backup files exist in the /var/lib/zstack/from-zstack-remote-backup/ directory of the remotebackupserver.

If there are only 3 servers, the database of management node 1 can be backed up to the computing node of the non-multiplexed management service, and the database of management node 2 can be backed up to the management node 1.

14. nSSV platform security hardening

After the cloud platform is implemented, in order to improve the security of the cloud platform and prevent network attacks, you need to change the default password of the cloud platform account to a strong password and use the security hardening script to strengthen the security of the cloud platform port.

```
1. Run the security hardening script on the management node
[root@node-11 ~]# bash safe.sh
Enter the password of the management node: Enter the admin password of the cloud platform
.............. cloud Physical Machine Security Hardening Rectification Script ..............
1. Check the IP address of the physical machine
2. Security hardening configuration of physical machines
3. Restrict physical machine ports
4. Upgrade Physical Machines OpenSSH(OpenSSH VERSION 8.9)
5. Configure a new common user and disable SSH login as the root user
6. How to use
q. Abort (ctrl + c)
.................. Please read the usage method carefully ......................
Please select [1-6 or q]: Select 3
1. Configure the rule
2. Restore rules
3. Expand the node
```

```
4. Return

Please select [1-4]: Option 1

Please enter the port that needs to be restricted (default limit is 7069, 9090, 9092, 8000, 9100, 7070, 3306):

press enter

Please enter the IP address (eg. default IP address 169.254.0.0/16, 172.28.16.10, 172.28.16.11, 172.28.16.12,

172.28.16.13, 192.168.79.0/24): Enter directly

Exit the script after the configuration is complete
```

15. Implement key operational considerations

15.1 Planning Considerations

- The cloud platform needs to plan dual management nodes, and the VIP address in the management network segment needs to be used for unified login of the cloud platform in advance.
- In distributed storage scenarios, it is not recommended to use the old storage for recycling, and it is strictly forbidden to use distributed storage in an all-gigabit environment.
- WerecommendthatyouuseIntelseries10GigabitNICs.
- It is recommended that the management node of the cloud platform be configured with an SSD of no less than 960 GB for RAID 1, and the Write-through mode is configured to install the operating system.
- It is recommended that the system disk of the distributed storage mon role server be configured with no less than 480 GB SSD for RAID 1, and the Write-through mode is configured to install the operating system.
- Distributed storage system disks, cache disks are configured with Intel S4610 or above cache disks with equivalent performance, SSD slow disks have a DWPD greater than 3 to

ensure stability and performance, and SATA HDDs of 4T or more are recommended for data disks.

- We recommend that you configure JBOD or non-RAID pass-through mode for RAID cache disks and data disks to facilitate hot-swappable disk O&M in the later stage.
- It is recommended that you configure the gigabit or 10 gigabit bond AB active/standby mode for the management network, the gigabit or 10 gigabit bond AB active/standby mode for the service network, the 10 Gigabit bond AB active/standby mode for the storage network, and the M-LAG for the switches.
- For OS installation, please select a system disk configured with RAID 1 to install the operating system, use a standard partition for partitioning, and do not allocate a SWAP partition for distributed storage.
- To install the default password on the operating system, please use a strong password policy that combines uppercase and lowercase letters + numeric values + special characters to prevent weak passwords.
- Please plan the time source address that can be accessed in advance for unified time access of the cloud platform and SDS distributed storage.
- It is recommended to avoid the port conflict between the cloud platform and SDS distributed storage (9090) in advance, and change the port 9090 of the score store to 9089 before installing distributed storage to avoid port conflict.
- After the deployment is complete, add the distributed storage communication ports to the whitelist configuration file of the management node configuration file of the cloud platform to prevent the subsequent necessary ports from being blocked by the operating system firewall and affecting service health.

- It is recommended to use the 3-replica mechanism for storage pool initialization for use in the production environment.
- It is recommended to plan 3 mons for small and medium-sized mons and 5 mons for large scales.
- The ratio of SSD to SATA is usually recommended to be 1:5, the ratio of PCLE interface SSD can be up to 1:10, and the SSD is used as a cache partition, and the size of each partition is about 50~250G.
- If the network environment does not meet the requirements of HA (switch redundancy, NIC redundancy/networkportredundancy),asinglepointoffailuremayoccur.

15.2 Deployment Considerations

- It is recommended to use a strong password policy that combines uppercase and lowercase letters + numeric values + special characters for operating system passwords.
- When installing the distributed storage software, you need to change the prometheus monitoring port 9090 in the decompressed install.conf file to 9089 to avoid conflicts with theprometheusservice ofthecloudplatform.
- Plan the time server address in the environment in advance for time synchronization operation when deploying, if the time server is not confirmed before installing the double pipe, you need to configure the time source address separately, becauseBy default, the cloud platform uses the control node itself as the time source server, and you need to modify chrony.serverIp.0 = 10.10.10.1 in the /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties file #10.10.10.1 is an example, point to the correct time source address.

- Hyperconvergence needs to extract and edit the firewall rules for internal communication whitelisting in the Cloud Cloud Platform Management Node configuration file, and you need to add the whitelisting rules in the /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/ classes/zstack.properties file to add thewhitelistingrules.
- Please confirm the storage network planning, as subsequent adjustments require stopping business operations, which is troublesome. Network planning suggestions at the time of initialization: admin network can be selected to open the browser UI of the computer to access the network segment of the storage control platform (generally using the management network), the public network and the cluster network are generally used as block storage to access the network, and the storage network segment address and gateway network can be selected as the network provided for business access by object storage or file storage, and the network that can be accessed by the business can be configured.
- When adding primary storage and mirror servers to the management node of the Cloud platform, you need to fill in the UUID of the storage pool created in SDS, which is usually the storage pool that starts with pool-, which can be viewed on the storage pool details page, or use ceph osd pool ls to list the created pools. At the same time, you need to enter the storage network as the storageheartbeatnetwork.
- When adding a Ceph primary storage or mirror server, add the IP addresses of all three MONnodes toavoidsinglepointsoffailure.
- To set the global settings of the cloud platform, you need to set the platform reserved memory and the calculation rules: the number of OSDs of a single hyper-converged

server*5G+theoperatingsystemretains10G~20Gmemory.

- It is recommended to configure automatic cross-machine backup of the cloud platform database (write crontab to back up the database task on a scheduled basis, and it is recommended that the frequency of cross-machine backup be 2 hours and retain 84 copies).
- After the deployment is complete, it is recommended that you inspect the basic environment on the management node of the cloud platform and make rectifications based ontheinspectionsuggestions.
- It is recommended to turn off the RAID card cache for old servers; Prevent data consistency issues caused by battery aging;
- Please set the SSH login password for the physical machine and the login password for thecloud platformtoacomplexpassword

15.3 Other Notes

- It is forbidden to install additional software or services that are not controlled by the cloud platform or storage on management nodes, physical machines, or distributed storage nodes, and these software have not been effectively and comprehensively tested on the cloudplatformorstorage, andmaybeincompatible.
- Configuration adjustments on management nodes, physical machines, or distributed storage nodes are prohibited and may cause instability without being thoroughly tested effectively.
- If the storage capacity exceeds 80%, the capacity must be expanded immediately, if the service exceeds 90%, if it exceeds 95%, there is a risk of data loss, and if the storage

capacity usage of a single OSD of distributed storage exceeds 85%, the storage pool alarm will be performed, and if the threshold reaches 90%, the service I/O continuity will be affected.

- If distributed storage does not affect services, a maximum of three mon nodes can be powered offordamagedatthesametime.
- In addition, if you expand the storage pool, you need to keep the SSD model and HDD size in the current storage pool consistent with the previous configuration, and if the inconsistency is inconsistent,therewillbeabarreleffect.
- It is recommended that more than 30% of the platform resources be free to prevent the production business from being affected by the excessive amount of data for expansion and recovery
- It is not recommended to over-de-de-partition memory and storage to prevent major problems, such as automatic shutdown of virtual machines due to memory overflow and abnormalrestartofphysicalmachines
- The migration network is used for data transmission during online migration, and the management network is used by default
- If the system disk capacity is small (for example, less than 600 GB), we recommend that you set the monitoring data retention period to 1 month and the monitoring data samplingintervalto20 seconds

16. Documentation of the implementation process

- Hardware information

entry	Whether the hardware situation on site is consistent with the hardware information in the

	implementation plan
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ CPU power-saving mode

entry	Whether the physical machine BIOS has turned off the CPU power saving mode, CPU C state should be turned off.
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Configure a RAID configuration for a physical machine

entry	Before installing the system on a physical machine, configure RAID1 WT for the system disk, and configure JBOD or pass-through mode for the SSD cache disk and OSD data disk
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Physical machine system installation

entry	Check whether only system disks are selected for the system installed on the physical machine
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ SWAP partition configuration

entry	Check whether the Ceph storage node installation system does not allocate SWAP partitions

Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ The directory of the image repository

entry	If an image repository is used, whether the /etc/rc.d/rc.local directory is automatically mounted at startup and the registry directory is automatically mounted, and the executable permissions are granted
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Bond configuration

entry	Check whether the service network, management network, and storage network of each node are configured with bonds and bridges
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Switch configuration

entry	Check whether the service network, management network, and storage network of each node are configured with VLAN trunks or access as expected
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Management, storage network reachability

entry	Check whether the interconnection and accessibility of the management network and storage network IP addresses of each node are checked

Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Create an affinity group

entry	Whether affinity groups have been created, one on each physical machine of the virtual machine is created in batches, and the interoperability and accessibility of the IP of all business virtual machines are checked
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Network reachability after a physical machine restarts

entry	After the server is restarted, the network of each node checks whether the binding information of each bond still exists, and the IP network is still connected Optional: arp-scan --interface=br_bond0/br_bond1/br_bond2 --localnet Determine connectivity in batches (note that the NICs written must have IPv4 addresses), and can be installed without arp-scan (EPEL source installation is used in the case of external networks)
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Time synchronization

entry	Before installing the Cloud MN service, check whether the time synchronization server time is adjusted and confirmed to be the correct time for the standard
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel

	by email

➢ DNS server

entry	Are all physical machines in /etc/resolv.conf Configured DNS server address
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Password-free configuration

entry	In the CPU primary storage scenario, check whether the password-free, hostname, and time synchronization settings are performed for each node before installing the Cloud MN service
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Time source configuration

entry	After the Cloud MN service is installed, whether a fixed time synchronization source is configured in the cloud.properties of each management node
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Storage time source configuration

entry	After the Cloud MN service is installed, check whether the time points to a fixed time source and is fully synchronized before installing distributed storage
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Firewall port configuration

entry	After the Cloud MN service is installed, whether the firewall ports required for the distributed storage are configured before installing the distributed storage
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Storage monitoring port configuration

entry	In hyper-converged scenarios, before installing distributed storage, whether the monitoring port 9090 of the install.conf storage is changed to 9089 to avoid conflicts?
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Ceph initializes the network

entry	Ceph stores whether the corresponding network segment is filled in according to the expected plan when the network is filled in initially
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Primary Storage Fill POOL UUID

entry	When you add a primary storage or mirror server to the cloud platform, specify the POOL UUID
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Database offsite backup

entry	For each Management Node, whether an offsite backup of the Management Node database has been configured and checked
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Offsite backup policy

entry	Check whether the backup policy of the Management Node database is appropriate for each Management Node
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Resource reservations

entry	Whether the resource reservation (memory reservation or primary storage reservation) of the cloud platform is configured
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Database password

entry	Whether the default root/cloud database password of the management node has been changed (after the modification is complete, the MN service needs to be restarted to take effect)
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Security hardening

entry	Platform hardening options https, password policy, IP blacklist and whitelist, two-factor authentication, security group, anti-fraud, whether the customer has been recommended to configure it
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Complex password configurations

entry	Check whether the passwords of each physical machine and cloud platform have been modified to complex passwords
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Migration, mirroring, and disaster recovery network configuration

entry	Check whether the cloud platform cluster migration network, image server data network, and disaster recovery server backup network are configured
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ VPC system network

entry	The virtual machine uses a VPC network, and whether the VPC system network uses a physical management network or is shared with a public network
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Performance scenario configuration

entry	Whether the cloud platform requires performance scenarios, and if so, whether all performance scenario configurations have been configured (global setting scenario encapsulation)
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Recommended configurations for the production environment

entry	Whether the cloud platform is configured according to the recommended configuration of the production environment (global setting scenario encapsulation)
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Project inspection

entry	Check whether the automated baseline test (inspection script) logs are executed and the logs are obtained
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Analyze the inspection results

entry	Whether the inspection logs are analyzed on site and the risk factors are analyzed
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Implementation Problem Logging

entry	Whether a summary of the problems encountered in the implementation is documented

Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Implement daily reporting records

entry	Whether the daily implementation report is submitted to the project group, department group and project implementation information group
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Escalation and analysis of problems

entry	Whether the relevant problems in the implementation process are reported to the project implementation group for analysis and confirmation as soon as possible
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Add-on module configuration

entry	Check whether other add-on modules are configured: V2V, disaster recovery, vCenter, and bare metal
Actual situation	Screenshots or photo instructions are recommended
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

➢ Customer training

entry	Whether to conduct on-site guidance to users, share best practices, and make check-in records
Actual	Screenshots or photo instructions are recommended

situation	
Risk Remarks	For non-standard scenarios, please make special notes and notify the relevant personnel by email

Appendix:

1. If the network is misconfigured, use the following steps to clean up the misconfigured network reconfiguration

To delete a bridge configuration:

```
#Stop the creation of bridges
ip link set br_XXX down
#Delete the bridge
brctl delbr br_XXX
#Delete the bridge profile
rm -f /etc/sysconfig/network-scripts/ifcfg-br_XXX
```

To delete a VLAN configuration:

```
#Delete the vlan subinterface
zs-vlan -d bondX XX
```

To delete a bond:

```
#Delete the wrong bond
zs-bond-ab -d bondX
```

Then start again configuring the network and add the bond

If it is only an error such as address information, it can also be deleted by a script

```
zs-restore-network-setting -h
```

The script restores network setting, include ip, netmask, gateway and bridge.