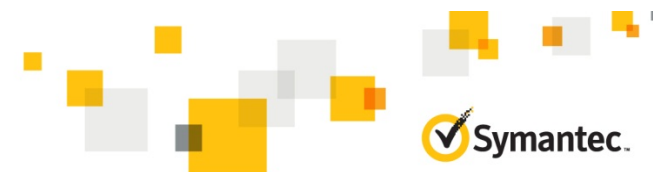# Analyzing modes and setting up communication with VMwareDisks agent

In a VMware virtual environment that employs non-shared VMware disks for storage, VCS provides the VMwareDisks agent to perform the disk import and deport operations during a failover. In the event of a failure, the VMwareDisks agent can communicate with the underlying ESX host or a vCenter Server to deport and import the disks.

By default, the Symantec High Availability Configuration Wizard configures the communication link with the ESX host. Based on your environment, you can choose to configure the communication link with a vCenter Server.

To configure a communication link with a vCenter Server, you must modify the "ESXDetails" attribute of the VMwareDisks agent.

How does the VMwareDisks agent work?

In the event of a failure, the VMwareDisks agent sends a disk detach request to the underlying ESX/ESXi host. After the disk detach operation is successful, the agent proceeds to attach the disks to the failover target system.
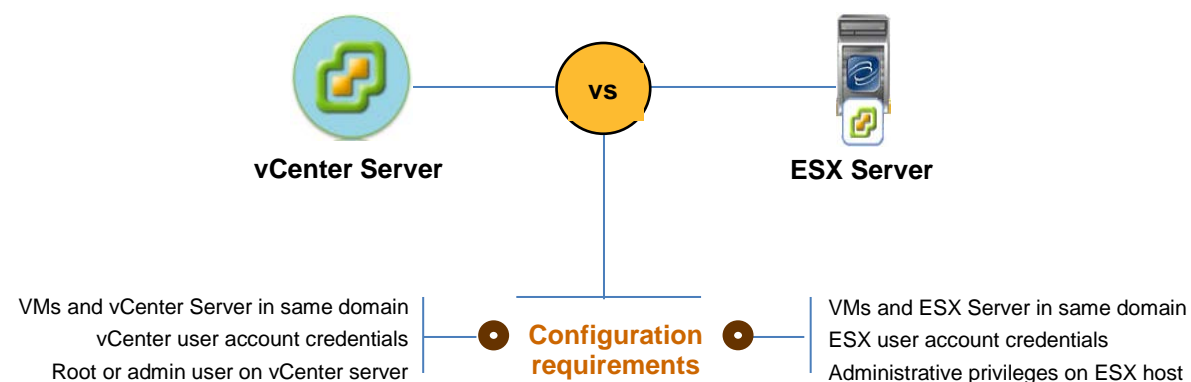
If you choose to set up the communication link between the VMwareDisks agent and a vCenter server, then the agent directs the disks detach and attach requests through the vCenter server.

In a scenario where the ESX/ESXi host itself faults, the VMwareDisks agent directs the disk detach and attach requests through the target ESX/ESXi host (vCenter server, if the communication link is set up with a vCenter server).

Note: If VMHA is not enabled and the host ESX faults, then the disks remain attached to the faulted virtual machine. This issue occurs because the target ESX host performs the disk detach operation. Since the underlying ESX host has itself faulted it fails to detach the disks.

The application availability is not impacted. However, the subsequent power ON of the faulted virtual machine fails because of the stale link that still exists, between the virtual machine and the disks attached.

As a workaround, you must manually detach the disks from the virtual machine and then power ON the machine.

vCenter Server   **VS**   **ESX Server**

VMs and vCenter Server in same domain
vCenter user account credentials
Root or admin user on vCenter server

Configuration requirements

VMs and ESX Server in same domain
ESX user account credentials
Administrative privileges on ESX host

Not a root or admin user?

You must have the administrative privileges or must be a root user to communicate the disk detach and attach operations through a vCenter server.

If you do not want to use the administrator user account or the root user, then you must create a role and add the following privileges to the created role:

- "Low level file operations" on datastore
- "Add existing disk" on virtual machine
- "Change resource" on virtual machine
- "Remove disk" on virtual machine

After you create a role and add the required privileges, you must add a local user to the created role. You can choose to add an existing user or create a new user.

Refer to the VMware product documentation for details on creating a role and adding a user to the created role.

Support for configuring communication with vCenter Server is available from SFW HA/VCS 6.1 onwards

Analyzing modes and setting up communication with VMwareDisks agent

Want to set up a link with vCenter server?

To set up a link between the VMwareDisks agent and a vCenter server, modify the "ESXDetails" attribute of the VMwareDisks agent using the Cluster Manager (Java Console) or the command line.

By default the "ESXDetails" attribute of the VMwareDisks agent uses the hostnames or IP addresses and the user account details of the ESX hosts on which the virtual machines are configured.
To enable the VMwareDisks agent to communicate with the vCenter Server, provide the hostname or IP address and the user account details of the vCenter Server to which the virtual machines belong.

A · To modify ESXDetails attribute using VCS Java Console

1. From the Java Console configuration tree, select the VMwareDisks resource and then select the **Properties** tab.

2. On the Properties tab, click the **Edit** icon next to the ESXDetails attribute.

3. On the Edit Attribute dialogue box, select all the entries specified under the Key-Value column and press "**-**" (minus sign) to delete them.

4. Encrypt the password of the vCenter Server user account.
   a. From the command prompt, run the following command:
      `Vcsencrypt –agent`
   b. Enter the vCenter Server user account password.
   c. Re-enter the specified password
      The encrypted value for the specified password is displayed.
      Note the encrypted password. You need to specify it in Step 7.

5. On the Edit Attribute dialogue box, click "+" to specify the values under the Key-Value column.

6. Under the Key column, specify the vCenter Server hostname or the IP address.

7. Under the Value column, specify the encrypted password of the vCenter Server user account (from step 4)

8. Click **OK** to confirm the changes.

9. Repeat the steps for all VMwareDisks resources from the Java Console configuration tree.

10. Save and close the configuration.

B · To modify ESXDetails attribute using command line

1. Change the VCS configuration to read/write mode:
   `haconf –makerw`

2. Delete the existing details of the ESX server.
   hares –modify *VMwareDIsks ResourceName* ESXDetails –delete –keys

3. Encrypt the password of the vCenter Server user account.
   a. From the command prompt, run the following command:
      `Vcsencrypt –agent`
   b. Enter the vCenter Server user account password.
   c. Re-enter the specified password.
      The encrypted value for the specified password is displayed.

4. Specify the vCenter Server details:
   ```
   hares –modify VMwareDIsks ResourceName ESXDetails
   –add vCenter IP address or hostname UserName=encrypted
   password
   ```

5. Repeat the steps for all VMwareDisks resources.

6. Save and close the configuration.

Support for configuring communication with vCenter Server is available from SFW HA/VCS 6.1 onwards