Troubleshooting

Checking VMware Compatibility

If you use third-party hardware to host the VM Expressway application, check the hardware compatibility. You can do this with the VMware compatibility guide tool from http://www.vmware.com/resources/compatibility/search.php.

VMware Checklist

Step 1   Check accessibility to the VM host server (by ping, physical console access, SSH remote access, KVM-over-IP console, and so on).

Step 2   Check network connectivity of the VMkernel (by executing the **vmkping** command using Tech Support Mode to verify network connectivity from the VMkernel NIC level).

Step 3   If you have problems connecting to the vSphere Client management console, execute the **command/sbin/services.sh** from an SSH session to restart the ESXi management agent.

Step 4   Check the VM host server utilization. CPU utilization, memory utilization, disk access speed, storage access speed, network access status, power utilization, and so on.

    If any specific application causes high utilization, stop or restart this application to isolate the overall VM host performance level. Or execute the command **esxtop** from Tech Support Mode to list all system processes running on the ESXi host application.

Step 5   Check the ESXi server file log (`hostd.logs`) under the folder `/var/log/vmware`. This log contains common error logs such as iSCI naming error, authentication error, and host convertibility error.

Step 6   Verify that adequate disk space is available on the physical volume that stores the database files. Free up disk space if necessary.

Step 7   Validate authentication to the vCenter Server database. The vCenter Server service may not be able to authenticate with the database if:

a) There are permission issues with the database when importing from one instance to another.

b) The password on the account you are using to authenticate to the database has changed but the password in the registry has not.

c) The vCenter Server database user is not granted correct permissions.

Isolating a Possible Root Cause

Potential issue area	What to look for
Storage	Look for the VM store application image stored either on the local drive, SAN, or NFS. VMs often freeze or hang up if the application failed to access the storage. Possible error messages are: • vCenter Server does not start • vCenter Server is slow to respond • vCenter Server fails after an indefinite amount of time
Network	Any network failure or locking causes a connection failure between the VM and the virtual network. Also, if using NFS or iSCSI, storage may cause application failures because the application cannot access the file system.
DNS	DNS server failures or communication failures between DNS and the VM server may cause the VMware application or the VM Expressway application to fail.
vCenter Server	If vCenter is not operating properly, although the VM Expressway application is still up and running, you may lose connection to the VM Expressway application from the network.
Host application	Check any critical alarms on the VM application for events on the host or application level (check the event information from vSphere Client).

Possible Issues

VM image fails to boot

If the VM image fails to boot, check the VT (Virtualization Technology) setting in BIOS. This needs to be enabled forhosting VMs. If it is not set, set it and reinstall ESXi then load the .ova file.

Expressway application fails to start

Look at the `/tmp/hwfail` file – its content indicates any violations in the installation.

For example, Expressway reserves 3 virtual NICs – these are required in the Expressway, do not try deleting one or more of them otherwise hwfail is created and the VM Expressway will not run.

Configured NTP does not work

For NTP to work on Expressway, the same NTP must also be configured on the VM host.

Guest console in vSphere 5 fails to run on some Microsoft platforms

When attempting to open a console screen from vSphere for the VM:

- Error message: "`The VMRC console has disconnected...attempting to reconnect.`"

- Screen remains black

The following operating systems are at risk:

- Windows 7 64 bit – reported on VMware forum (http://communities.vmware.com/thread/333026)

- Windows Server 2008 R2 (64-bit) – found by use

Web page/IP address unreachable after OVA deployment

This issue can be caused by a cache issue in the gateway switch.

To resolve, access vCenter, go to the console and ping the gateway: ping `<gateway_ip_address>`.

Clustering status incorrect after recreating a VM within a cluster

When recreating a VM within a cluster, the cluster must be broken and recreated for it to function correctly.

To resolve, take the following steps:

1. Back up the existing configuration from the original node you want to recreate.

2. Upgrade all nodes to X12.5.4.

3. Shut down guest on the original node.

4. Start up a new VM using the X12.5.4 .ova file and give it the same IP address as the original node.

5. Restore the backup configuration from the original node onto the new VM.

6. Rebuild the cluster and add the cluster configuration on the other nodes.

7. After approximately 10 minutes, clustering status on the **Status** > **Clustering** page should accurately indicate a normal status for the cluster.

Raid controller synchronization

If the VMware system is synchronizing its RAID disks, disk performance is seriously degraded. We strongly recommend that Expressway is not installed or run on VM platforms where RAID disks are in a degraded or synchronizing state.

Analyzing the Cause of VMware Issues

If issues exist with VMware on the Expressway host, we recommend that you collect logs from the host for analysis, using the following procedure:

Step 1   Using the vSphere client (or the vCenter Server managing this ESXi host) connect to the ESXi host on which the Expressway is running.

Step 2   Go to **File** > **Export** > **Export System logs**, choose the appropriate ESXi host and go with the default settings.

What to do next

After you have downloaded the logs analyze them, or have them analyzed to determine the issue.

More information on exporting logs can be found at: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=653.

Restoring the Default Configuration (Factory Reset)

Rarely, it may be necessary to run the "factory-reset" script on your system. This reinstalls the software image and resets the configuration to the default, functional minimum.

Before You Begin

If you've upgraded since the system was first set up, be aware that the reset reinstalls your latest software version.

The system uses the default configuration values that currently apply in the software version installed by the reset. These may differ from your previously configured values, especially if the system has been upgraded from an older version. In particular this may affect port settings, such as multiplexed media ports. After restoring the default configuration you may want to reset those port settings to match the expected behavior of your firewall. (As described below, optionally it's possible to retain a few configuration values like option keys, SSH keys, and FIPS140 mode, but we recommend that you reset all these values.)

Prerequisites

- As the virtual machine console is required to complete this process, **you need appropriate VMware access inorder to open the VM console.**

- The factory reset procedure described below rebuilds the system based on the most recent successfully installed software image. A file containing the software image in tar.gz format, named `tandberg-image.tar.gz`, stored in the `/mnt/harddisk/factory-reset/` system folder is used for the reinstallation. In some cases this file is not present on the system (most commonly with a fresh VM installation that has not been upgraded). If so, you must first put this file in place using SCP as root.

Process to Reset to the Default Configuration

You must do this procedure from the console. Because the network settings are rewritten, all calls and any SSH session used to initiate the reset will be dropped and you won't be able to see the procedure output.

The process takes approximately 20 minutes.

Step 1   Log in to the system as **root**.

Step 2   Type `factory-reset`

Step 3   Answer the questions as required. The recommended responses will reset the system completely to a factory default state:

Table 1:

Prompt	Recommended response
Keep option keys [YES/NO]?	NO
Keep FIPS140 configuration [YES/NO]?	NO
Keep IP configuration [YES/NO]?	NO
Keep ssh keys [YES/NO]?	NO
Keep server certificate, associated key and CA trust store [YES/NO]? This option does not preserve SNI / domain certificates, which are always deleted regardless of what you respond. Only the server certificate and associated key and CA trust store are saved (if you respond YES).	NO
Keep root and admin passwords [YES/NO]?	NO
Save log files [YES/NO]?	NO

Step 4   Confirm that you want to proceed.

Step 5   After the VM boots, you are taken to the Install Wizard. You must complete the wizard through the VM console. Some of the questions in the wizard may be skipped depending on your responses in step 3, but even if you preserved the IP configuration and password, you still need to complete the Install Wizard through the VM console.

Note   If you were using FIPS140 and you want to enable it again, see the relevant section in the Expressway Administrator Guide.

Resetting Your Administrator Password or Root Password

If you have forgotten the password for either an administrator account or the **root** account and you are using a VM (Virtual Machine) Expressway, you can reset it using the following procedure:

Step 1   Open the vSphere client.

Step 2   Click on the link **Launch Console**.

Step 3   Reboot the Expressway.

Step 4   In the vSphere console log in with the username `pwrec`. No password is required.

Step 5   When prompted, select the account (root or the username of the administrator account) whose password you want to change.

Step 6   You will be prompted for a new password.

What to do next

The **pwrec** account is only active for one minute following a reboot. After that time you will have to reboot the system again to reset the password.