

esxcfg-vswif – to retrieve the portgroup for the service console and to get the same IP address as in the file `/etc/sysconfig/network-scripts/ifcfg-vswitch<SC NIC number>`.

esxcfg-vswtch – to see the vswitch associated with the service console portgroup

esxcfg-nics – to retrieve uplink information.

Routing

To pass the routing configuration check the default gateway must be set up and reachable for the ESX host, since EsxDiag will consider a ping reply as a successful test outcome. To fix your routing you should edit the `/etc/sysconfig/network` and execute `/etc/init.d/network` with 'restart' parameter.

Commands used:

ip with **route** parameter – to show current routing configuration.

ping and **arping** – to ping

Name resolution

This will check whether the ESX Server name resolution subsystem and appropriate network environment (DNS servers) are properly configured and operational. For the host lookups `/etc/nsswitch.conf` and `/etc/host.conf` should be configured to use DNS. Also DNS servers list as well as the primary domain prefix ('search' or 'domain' parameters in `/etc/resolv.conf`) should be set. The 'A' record should be specified for the server's hostname.

As you might know the host names are retrieved from the following files and they should be identical:

```
/etc/vmware/esx.conf  
/etc/sysconfig/network  
/etc/hosts
```

The localhost entry should be in the `/etc/hosts`.

If you get FAILED status make sure the DNS servers are configured properly and reachable to reply to the DNS requests, check your DNS server zones configuration.

Commands used:

dig – to get reply to DNS requests

Services

This set of tests is checking if all important services (such as `crond`, `vmware-vmkauthd`, `xinetd`, `pegasus`, `syslog`, `ntpd`, `vmware-webAccess`, `sshd`, `mgmt-vmware`) are enabled at startup for the current init level (3 by default) and all processes this service depends on are

running. Some of the services are considered to be non-critical (e.g. ntpd, vmware-webAccess, pegasus) so if you get FAILED status on them - it is just FYI.

For sshd additional check is performed since sometimes the init script started with 'status' parameter says "sshd is running" even if the main process `/usr/sbin/sshd` is not running.

If you get overall FAILED status check the services which failed to start. You can start them with the commands mentioned below.

Commands used:

chkconfig - to check whether any service startup is enabled at the init level
service - to start/stop/restart the service,
alternatively you can run `/etc/init.d/<service name> start (stop/restart)`.

Time synchronization

Many critical applications rely on accurate time synchronization, including Microsoft Active Directory and VMware DRS. With EsxDiag you can check, modify and apply the correct NTP configuration for all ESX Servers within your VIB environment.

The outgoing UDP 123 port should be open. Even if the port is closed the checks will be executed, since 'esxcfg-firewall' can generate invalid 'iptables' config. NTP servers should be specified in the `/etc/ntp.conf` and in the `/etc/ntp/step-tickers`.

Specified NTP servers should be available through the NTP protocol. The time on the server should be synchronized with the NTP servers configured or with VMware recommended (vmware.pool.ntp.org, vmware.pool.ntp.org, vmware.pool.ntp.org).

Current time of fset should be reasonable. Absolute value for the time offset should be less than 15 seconds.

The ntpd service should be enabled on the current runlevel and currently started.

Time synchronization daemon (ntpd) should be operational.

If you get overall FAILED status please refer to the recommendations of VMware knowledge base at:

http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=1339

Commands used:

esxcfg-firewall -q ntpClient - to check if the outgoing UDP 123 port is open.

chkconfig - to check ntpd service.

`service ntpd status` - to check ntpd.

ntpdate -q or **ntpdate** - to synchronize time - if the first command fails, since they are using different outgoing port number - udp datagram may be blocked by external firewall.

Network storage

In the current version of EsxDiag only NAS and iSCSI are tested.

To pass the test for remote network storage availability you should have all the remote NAS (NFS) mounts accessible from the ESX host and eventually allow getting the list of files.

The targets should be specified in the `/etc/vmkiscsi.conf` ('DiscoveryAddress' parameter) and generated having used Virtual Infrastructure Client.

The sockets for all discovered targets have to be created by `'/usr/sbin/vmkiscsid'` process.

To check availability EsxDiag creates a file with random name on iSCSI LUN mounted to vmfs path.

All remote iSCSI paths (adapter: target: LUN) should be properly configured to have access.

If you get overall FAILED status check if all remote storage hosts/devices are alive and reachable via the network. In case of iSCSI storage adapters: try to edit in the Virtual Infrastructure Client:

Configuration tab-> Hardware pane -> Storage adapters or click Rescan.

Also try to use commands below to rescan iSCSI devices.

Commands used:

esxcfg-nas -l – to get the list of NAS mounts.

esxcfg-vmhbadevs -m – to get the list of iSCSI devices.

vmkfstools – to get additional information on vmfs device.

vmkiscsi-tool – to get additional information on iSCSI device.

lsof – to get the list of opened sockets.

esxcfg-swiscsi -s – to rescan iSCSI LUNs.

As you can see this script definitely can add value if you want to fast-check your fresh ESX 3.x installation. I'd recommend you to give it a try.

In fact, EsxDiag is a part of the Veeam Configurator product that helps you manage and control the configuration of your entire Virtual Infrastructure from a single Windows interface.

You can read more at http://www.veeam.com/veeam_configurator.asp

The free EsxDiag utility is available at <http://www.veeam.com/free-script/>