Veeam Firewall VIB for Cisco HyperFlex

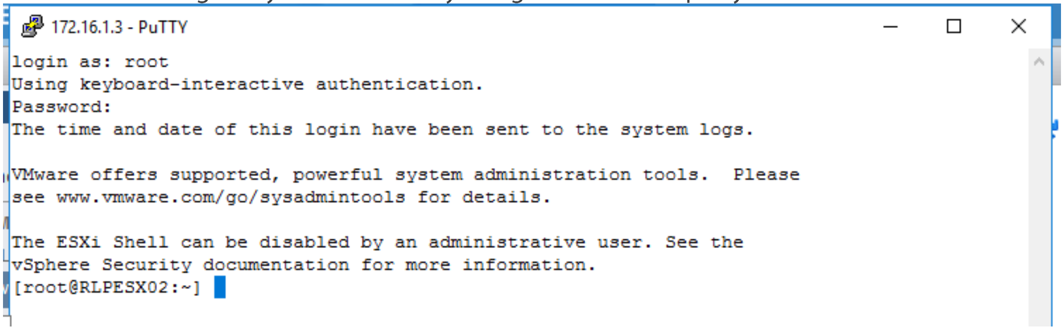
Author: Stefan Renner, 26.04.2017

The VeeamCiscoHXFirewall.vib opens the required firewall ports on vSphere to get Veeam access to the IOVisor of Cisco HyperFlex. We recommend to assign the Veeam Proxy Server IPs to the rule after installing the VIB.
The Firewall rule is persistent after a ESXi reboot. The Firewall rule is enabled by default after installation.
The VIB does not require a reboot for installation.

Install the Firewall VIB on ESXi:

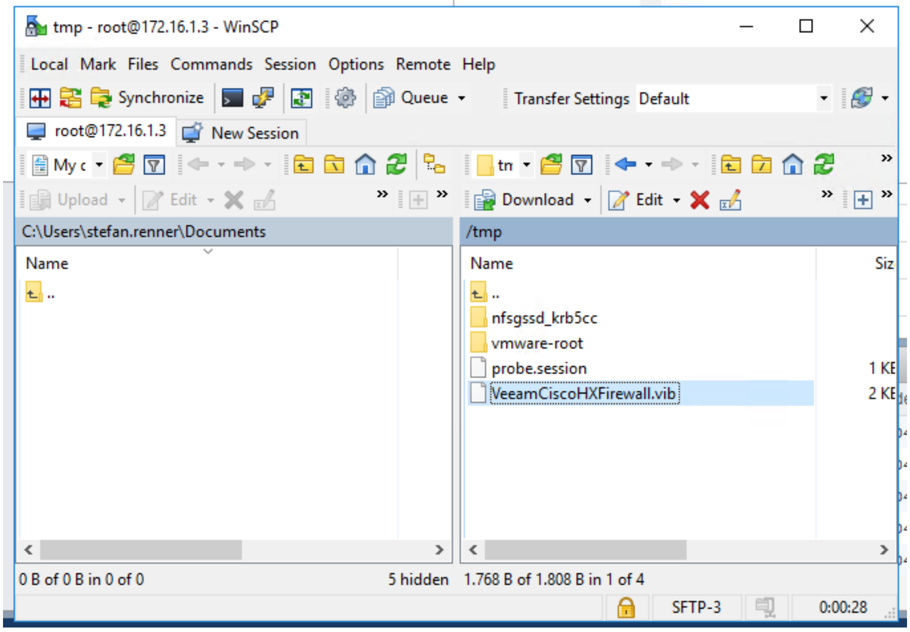
Repeat the following steps on all Cisco HyperFlex nodes in your cluster.

1. Enable ssh and login to your ESXi host by using a ssh tool like putty



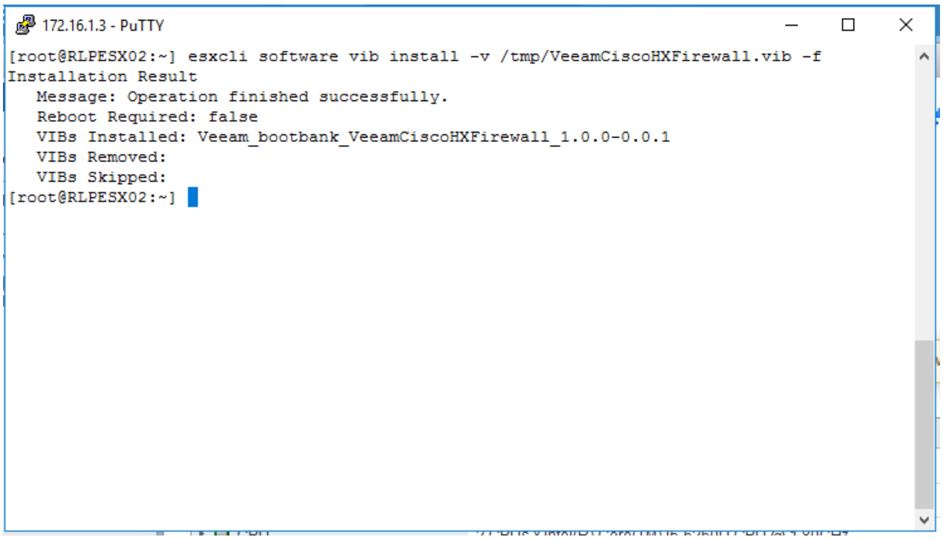
```
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@RLPESX02:~]
```

2. Copy the VIB file to the ESXi hosts tmp folder using HTTP or a SCP client



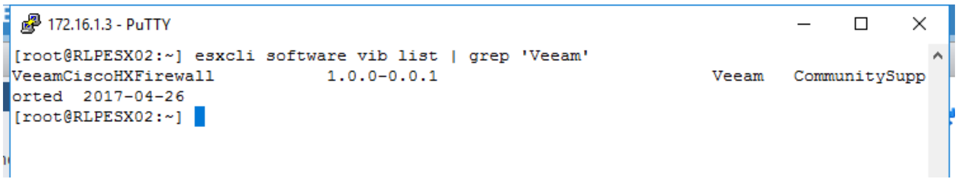
tmp - root@172.16.1.3 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
root@172.16.1.3
New Session
Upload
Edit
Download
Edit
C:\Users\stefan.renner\Documents
/tmp
Name
..
Name
Siz
..
nfsgssd_krb5cc
vmware-root
probe.session 1 KB
VeeamCiscoHXFirewall.vib 2 KB
0 B of 0 B in 0 of 0
5 hidden
1.768 B of 1.808 B in 1 of 4
SFTP-3
0:00:28

3. Install the VIB
   Command:
   `esxcli software vib install -v /tmp/VeeamCiscoHXFirewall.vib -f`



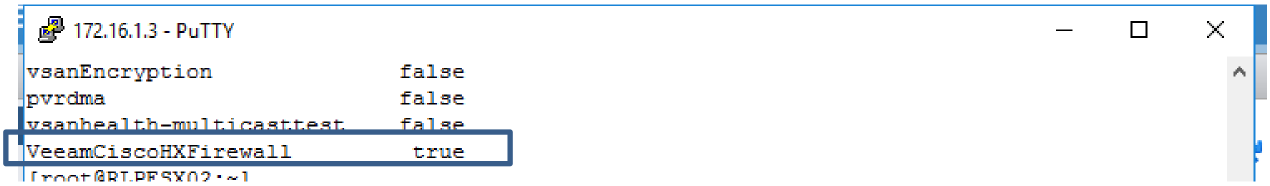
```
[root@RLPESX02:~] esxcli software vib install -v /tmp/VeeamCiscoHXFirewall.vib -f
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Veeam_bootbank_VeeamCiscoHXFirewall_1.0.0-0.0.1
   VIBs Removed:
   VIBs Skipped:
[root@RLPESX02:~]
```

4. Verify the VIB was installed
   Command:
   `esxcli software vib list | grep 'Veeam'`



```
[root@RLPESX02:~] esxcli software vib list | grep 'Veeam'
VeeamCiscoHXFirewall            1.0.0-0.0.1                        Veeam   CommunitySupp
orted  2017-04-26
[root@RLPESX02:~]
```

5. Verify the new firewall rule is active
   Command:
   `esxcli network firewall ruleset list`

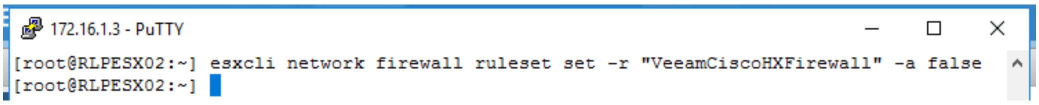


```
vsanEncryption                false
pvrdma                        false
vsanhealth-multicasttest      false
VeeamCiscoHXFirewall           true
[root@RLPESX02:~]
```

Note: If the VIB installation fails, you might need to set the acceptance level to CommunitySupport and retry the installation
Command: `esxcli software acceptance set --level=CommunitySupported`

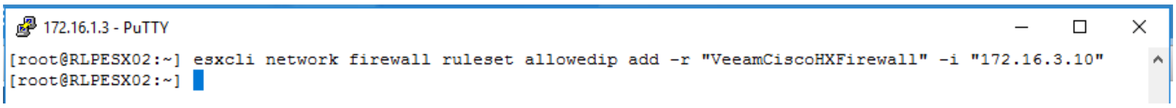
Recommended: Set the Veeam Proxy Servers

1. Enable allowed ip list for the new firewall rule
   Command:
   `esxcli network firewall ruleset set -r "VeeamCiscoHXFirewall" -a false`



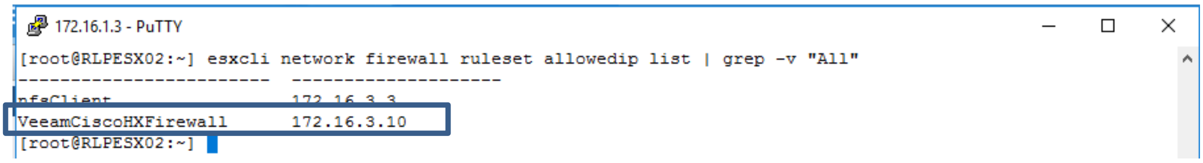
```
[root@RLPESX02:~] esxcli network firewall ruleset set -r "VeeamCiscoHXFirewall" -a false
[root@RLPESX02:~]
```

2. Set the Veeam proxy server data network IP (storage network)
   Repeat the following command for all Veeam proxy server or set a subnet.
   Command:
   `esxcli network firewall ruleset allowedip add -r "VeeamCiscoHXFirewall" -i "172.16.3.10"`



```
[root@RLPESX02:~] esxcli network firewall ruleset allowedip add -r "VeeamCiscoHXFirewall" -i "172.16.3.10"
[root@RLPESX02:~]
```

3. Verify the IPs are set
   Command:
   `esxcli network firewall ruleset allowedip list | grep -v "All"`

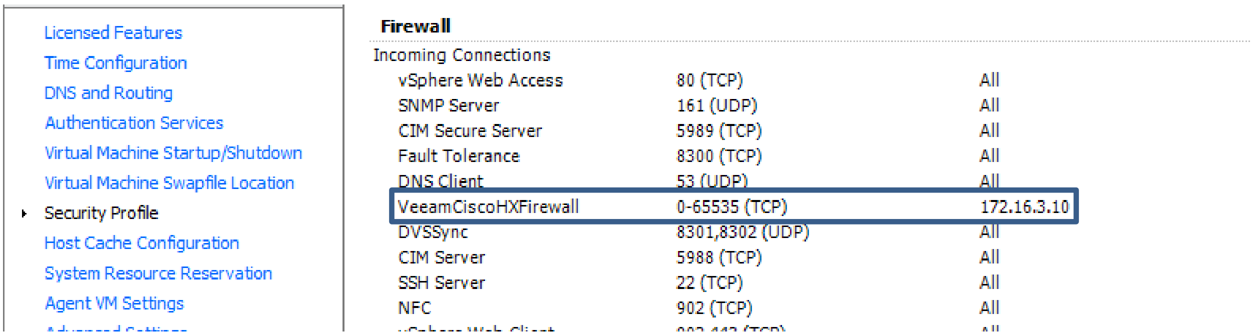


```
[root@RLPESX02:~] esxcli network firewall ruleset allowedip list | grep -v "All"
------------------------  ---------------------
nfsClient                 172.16.3.3
VeeamCiscoHXFirewall      172.16.3.10
[root@RLPESX02:~]
```

Note: Veeam recommends to set the all IPs of Veeam proxy servers in the firewall rule. Otherwise the firewall rule is enabled for all incoming connections. You can specify either the IP address or a subnet. Use one command per proxy.

Checks if everything is correctly configured

1. Check the Security Profile on the ESXi hosts

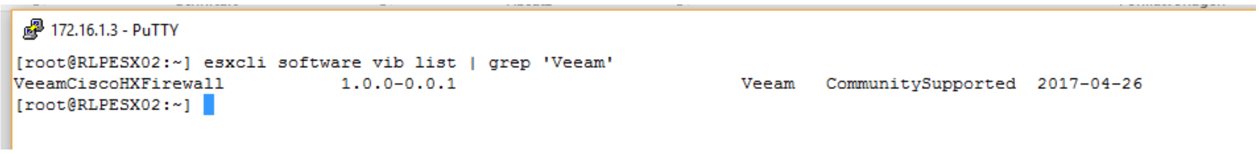


Firewall

Incoming Connections

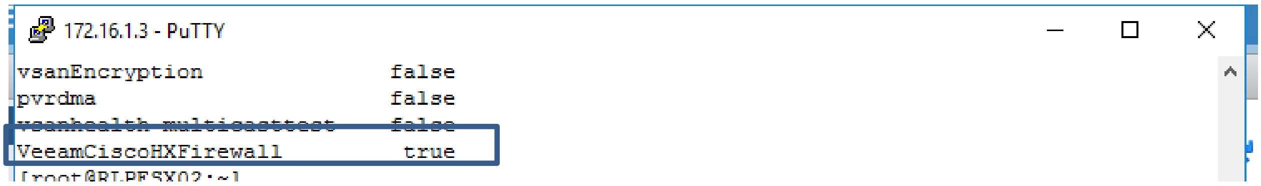
vSphere Web Access	80 (TCP)	All
SNMP Server	161 (UDP)	All
CIM Secure Server	5989 (TCP)	All
Fault Tolerance	8300 (TCP)	All
DNS Client	53 (UDP)	All
VeeamCiscoHXFirewall	0-65535 (TCP)	172.16.3.10
DVSSync	8301,8302 (UDP)	All
CIM Server	5988 (TCP)	All
SSH Server	22 (TCP)	All
NFC	902 (TCP)	All
vSphere Web Client	902,443 (TCP)	All

2. Check the VIB
   `esxcli software vib list | grep 'Veeam'`



```
[root@RLPESX02:~] esxcli software vib list | grep 'Veeam'
VeeamCiscoHXFirewall          1.0.0-0.0.1                         Veeam   CommunitySupported  2017-04-26
[root@RLPESX02:~]
```

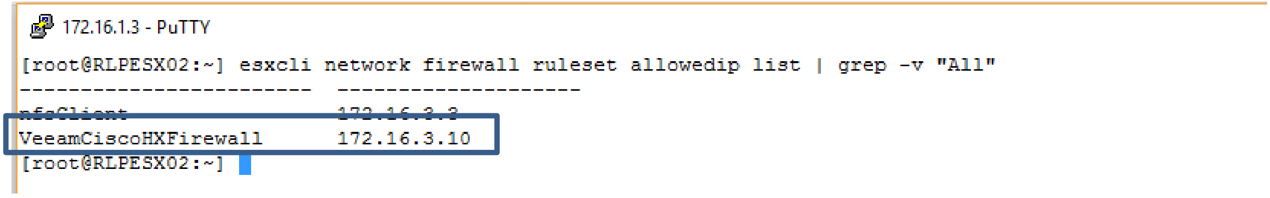
3. Check the ruleset
   `esxcli network firewall ruleset list`



```
vsanEncryption                false
pvrdma                        false
vsanhealth-multicasttest      false
VeeamCiscoHXFirewall           true
[root@RLPESX02:~]
```

4. Check which Veeam Proxy IPs are assigned

```
esxcli network firewall ruleset allowedip list | grep -v "All"
```



```
[root@RLPESX02:~] esxcli network firewall ruleset allowedip list | grep -v "All"
------------------------  --------------------
nfsClient                 172.16.3.3
VeeamCiscoHXFirewall      172.16.3.10
[root@RLPESX02:~]
```