



A S e r i e s F a i l u r e s

[HOME](#) [ABOUT](#) [VCAP-DCA INDEX](#) [THINAPP](#) [VCDX STUFF](#) [OTHER PAGES](#) [VCAP-DCD INDEX](#)

« VCAP-DCA Objective 9.1 : Install ESX Server with Custom Settings

VCAP-DCA Brownbag Session #1 »

Search

GO



Knowledge

Identify configuration files related to network security

Identify virtual switch security characteristics

Skills and Abilities

Add/Edit Remove users/groups on an ESX Host

You can manage this through the gui as shown [here](#) or using the vicfg-user command as shown below.

```
vicfg-user <conn_options> -e <user | group> -o <add | modify | delete | list> [options]
```

Customize SSH settings for increased security

Disabled by default for root. You can use SU to elevate to root privileges and should never allow root access via SSH.

If needed you can enable root access as shown [here](#).

Enable/Disable certificate checking

You can follow the guide from VMware [here](#) for enabling/disabling certificate checking.

Generate ESX Host certificates

Read the below section on Replacing the default certificate to get guidance on generating a host certificate.

Enable ESXi lockdown mode

Can be enabled during host addition to vCenter

or

Configuration—>Software—Security Profile

A good read on the topic of ESXi lockdown can be found [here](#).

Replace default certificate with CA-signed certificate

Check out [this article from vm-help.com](#) for an in depth instruction on replacing the default certificate with a CA signed one.

Configure SSL timeouts

[From the ESX Configuration Guide](#)

Timeout periods can be set for two types of idle connections:

- The Read Timeout setting applies to connections that have completed the SSL handshake process with port 443 of ESX.
- The Handshake Timeout setting applies to connections that have not completed the SSL handshake process with port 443 of ESX.
- Both connection timeouts are set in milliseconds. Idle connections are disconnected after the timeout period. By default, fully established SSL connections have a timeout of infinity.

1 Log in to the service console and acquire root privileges.

2 Change to the directory /etc/vmware/hostd/.

3 Use a text editor to open the config.xml file



> SRM (3)
> ThinApp (16)
> VCAP-DCA (38)
> VMware (57)



MY LATEST TWEETS



vFAIL.NET [vfail.net](#)

97 followers

RT @PlanetV12n: To Trunk Or Not To Trunk? (vDestination) [http://bit.ly/byqscT](#) >good read
about 1 week ago

New blog post: VCAP-DCA Update [http://bit.ly/b1DSLS](#)
about 1 week ago

Just found out lab will goto 4.1 next year. Items like those discussed in my VMTN posting not covered on the current [http://bit.ly/bYL2c6](#)
about 1 week ago

All VCAP-DCA Study notes now online at [http://bit.ly/9rnpHE](#) Final PDF version done and will be posted next week.
about 1 week ago

Virtualization

Quote of the Day

Web2PDF

converted by Web2PDFConvert.com

3 Use a text editor to open the config.xml file.

4 Enter the <readTimeoutMs> value in milliseconds.

For example, to set the Read Timeout to 20 seconds, enter the following command.

```
<readTimeoutMs>20000</readTimeoutMs>
```

5 Enter the <handshakeTimeoutMs> value in milliseconds.

For example, to set the Handshake Timeout to 20 seconds, enter the following command.

```
<handshakeTimeoutMs>20000</handshakeTimeoutMs>
```

6 Save your changes and close the file.

7 Enter the following command to restart the vmware-hostd process.

```
service mgmt-vmware restart
```

From ESXi config guide

Use the vifs command to get a copy of the config.xml file to edit.

- For Linux systems, use this command. `vifs -server <hostname> -username <username> -get /host/config.xml <directory>/config.xml`
- For Windows systems, use this command. `vifs -server <hostname> -username <username> -get /host/config.xml <directory>\config.xml`

2 Use a text editor to open the config.xml file.

3 Enter the <readTimeoutMs> value in milliseconds.

For example, to set the Read Timeout to 20 seconds, enter the following command.

```
<readTimeoutMs>20000</readTimeoutMs>
```

4 Enter the <handshakeTimeoutMs> value in milliseconds.

For example, to set the Handshake Timeout to 20 seconds, enter the following command.

```
<handshakeTimeoutMs>20000</handshakeTimeoutMs>
```

5 Save your changes and close the file.

6 Use the vifs command to put a copy of the config.xml file on the ESXi host.

- For Linux systems, use this command. `vifs -server <hostname> -username <username> -put <directory>/config.xml /host/config.xml`
- For Windows systems, use this command. `vifs -server <hostname> -username <username> -put <directory>\config.xml /host/config.xml`

7 Use the Restart Management Agents operation through the direct console to have the settings take effect.

Secure ESX Web Proxy

Check the sections for both the ESX(i) config guides for configuring the web proxy.

Enable strong passwords and configure password policies

For ESX you will issue the command like shown below.

```
esxcfg-auth -maxpassdays=90 -minpassdays=30 -passwarnage=75
```


This blog article is also another good read on the topic of password complexity

http://www.vm-help.com/esx40i/password_complexity.php

Identify methods for hardening virtual machines

The [vSphere security hardening guide](#) is a great resource for this section. It is very detailed and has a lot of options. Here are just a few from the document below.

- Prevent Virtual Disk Shrinking-Readily inducing this from within the guest could cause a DOS attack.
- Prevent other users from viewing remote console session(multiple at a time)

-  `RemoteDisplay.maxConnections=1`

- Disable VM to VM communication through VMCi

Analyze logs for security-related messages

Some log file description here. Will have to circle back around on this to study in more detail.

<http://www.vadapt.com/2010/03/vsphere-securitylog-files/>

Tools

ESX Configuration Guide

ESXi Configuration Guide

vSphere Command-Line Interface Installation and Scripting Guide



Configuration
Maximums for
VMware

vSphere is my favorite VMware document. It answers many of the "How many", "How much" type questions about VI capabilities. This is one of the documents that will most often be updated as new releases of VMware VI are released so it's a good one to keep tabs on.

<http://www.vmware.com/pdf/vsphere4/r41>

Powered by

[The Printed Owl](#)

CATEGORIES

- » [SRM](#) (3)
- » [ThinApp](#) (16)
- » [VCAP-DCA](#) (38)
- » [VMware](#) (57)

Product Documentation

vSphere Client

vSphere CLI

vicfg-user

vifs

vSphere 4.0 Security hardening guide

- [Objective 9.3 – Configure vCenter Server Linked Mode](#)
- [Objective 9.2 – Plan and Execute Scripted Installations](#)
- [Objective 8.2 – Administer vCenter Orchestrator](#)
- [VCAP-DCA Brownbag Session #1](#)
- [VCAP-DCA Objective 9.1 : Install ESX Server with Custom Settings](#)
- [VCAP-DCA Objective 3.5 – Utilize Advanced vSphere Performance Monitoring Tools](#)
- [VCAP-DCA Objective 3.4 – Perform Capacity Planning in a vSphere Environment](#)
- [VCAP-DCA Objective 3.3 – Implement and Maintain Complex DRS Solutions](#)
- [VCAP-DCA Objective 3.2 – Optimize Virtual Machine Resources](#)
- [VCAP-DCA Objective 3.1 – Tune and Optimize vSphere Performance](#)

 [VCAP-DCA](#), [VMware](#), [vsphere](#)

Share
this
post!

Print
article

This entry was posted by [Sean Crookston](#) on September 27, 2010 at 8:00 am, and is filed under [VCAP-DCA](#), [VMware](#). Follow any responses to this post through [RSS 2.0](#). You can [leave a response](#) or [trackback](#) from your own site.

COMMENTS (0)

RELATED POSTS

NO COMMENTS YET.

Submit Comment

Mystique theme by [digitalnature](#) | Powered by [WordPress](#)



RSS FEEDS

XHTML 1.1

TOP

PR 0

