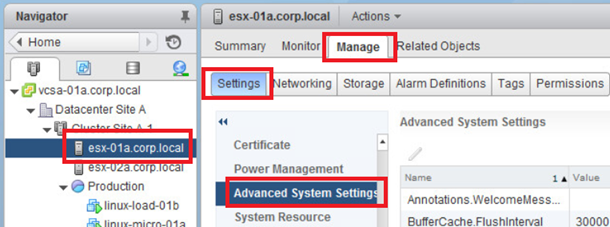
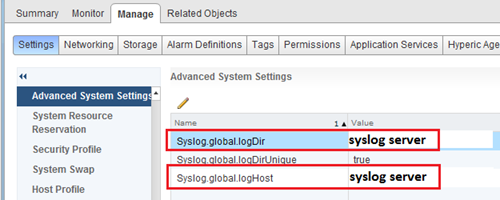
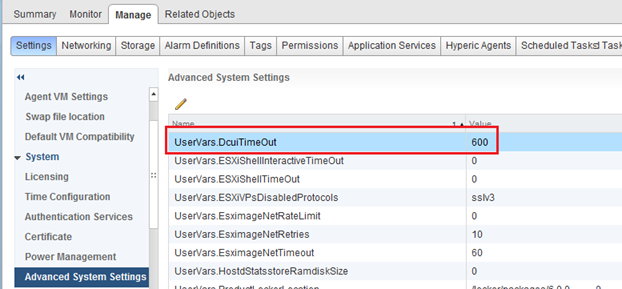
The following guide will quickly show you how to harden your vSphere 6 Host based on VMware’s Security Hardening guides which can be found [here](https://www.vmware.com/security/hardening-guides). The official hardening guides are in an excel format with detailed descriptions. This guide walks you through all the steps, screenshot by screenshot without reading through the excel spreadsheet. I will post Virtual Machine hardening in a future time. 

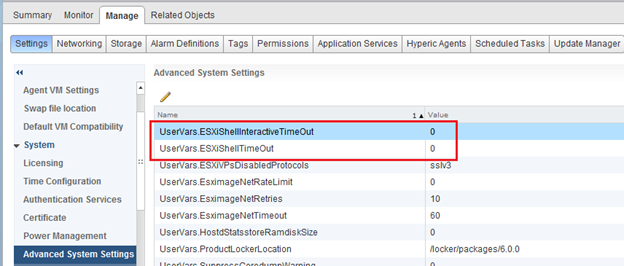
1. Login to **vCenter Web Client** with administrative credentials



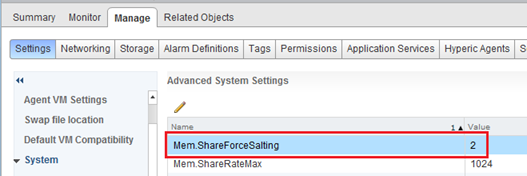
1. Click on a **Host** and select **Manager > Settings > Advanced System Settings**
2. Verify that the **Syslog.global.logDir** and **Syslog.global.logHost** values should not be the default of **/scratch/log**. Enter a log server if applicable



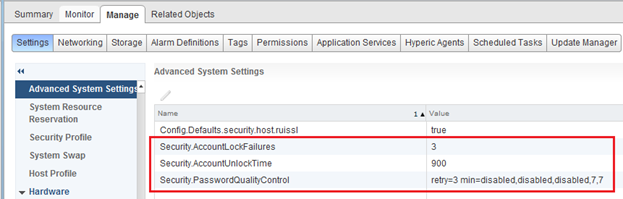
1. Make sure **UsersVars.DcuiTimeOut** is set to **600 (default 600)**
2. Make sure **UserVars.ESXiShellInteractiveTimeOut** and **UserVars.ESXiShellTimeOut** is set to a value greater than the default of **0**

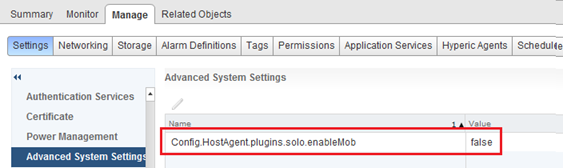
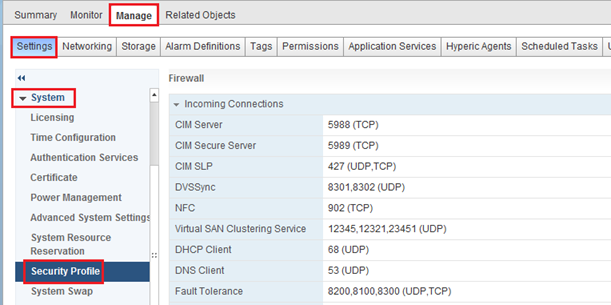


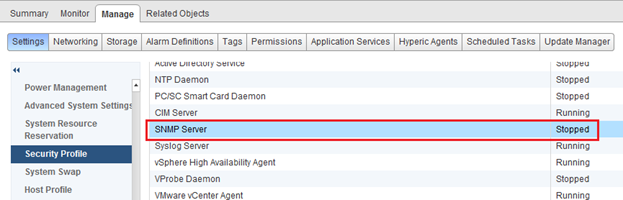
1. Make sure **Mem.ShareForceSalting** is set to a value of **2**



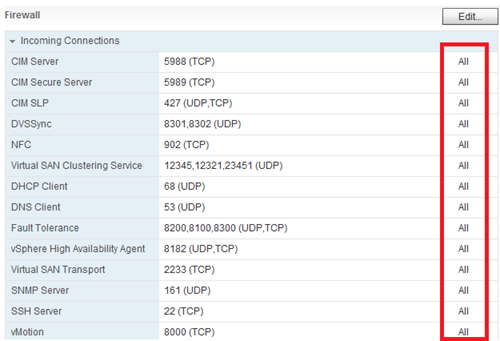
1. Change the following for Security
   1. **Security.AccountLockFailures** to 3
   2. **Security.AccountUnlockTime** to 900
   3. **Security.PasswordQualityControl** to **retry=3 min=disabled,disabled,disabled,7,7**



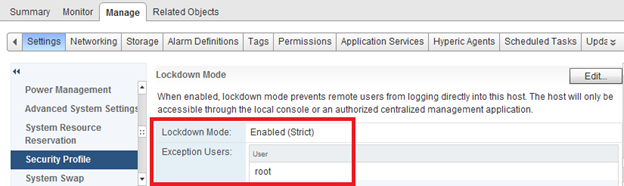
1. Make sure **Config.HostAgent.plugins.solo.enableMob** is set to a value of **false**
2. Now navigate to **Manage > Settings > Security Profile**
3. Make sure **SNMP Server** under Services section is set to **Stopped** if you are not suing SNMP in your environment.



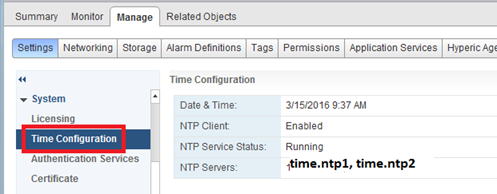
1. Scroll down to the bottom and change the**Host Image Profile Acceptance Level** to either **VMware Accepted** or **VMware Certified**
2. Under **Firewall**, all Incoming Connections and Outgoing connections should not be set to **All**. Set what IP Addresses are allowed to communicate with those services instead.



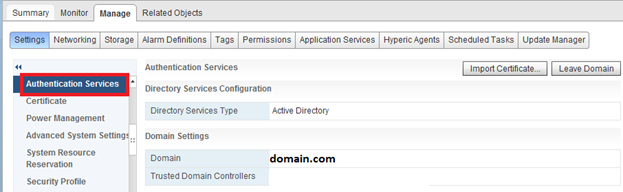
1. Under **Lockdown Mode** make sure **Lockdown Mode is Enabled (Strict)** and **Exception Users** are added accordingly.

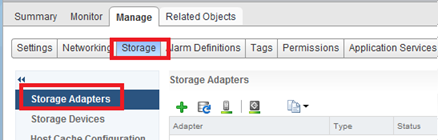


1. Navigate to **System > Time Configuration** on the left menu and make the following:
   1. NTP Client is Enabled
   2. NTP Service Status is Running
   3. NTP Servers are set with NTP Servers



1. Navigate to **Authentication Services** and verify that **Domain** and **Trusted Domain Controller settings** are configured as appropriate



1. Now navigate to **Manage > Storage > Storage Adapters** and for EACH **iSCSI Adapter**, scroll for **Authentication** section under **Adapter Details** section > **Properties** tab. The **Method** parameter should be set to **Use bidirectional CHAP**
2. Once you completed the host hardening make sure everything is working such as vMotion, DRS, etc. Once you verify everything is working, it is highly recommended to create a Host Profile from the host and remediate it out to the other host in your environment. Also export the Host Profile as well so all you work isn’t lost.