# vSphere HA/FDM – SSLv3 Security Protocol Configuration Command line utility

## ❖ Features

- Automatically add the advanced option *das.config.vmacore.ssl.sslOptions* on all HA enabled cluster and reconfigure HA on all Clustered ESXi hosts for changes to take effect.
- Utility has inbuilt scanner intelligence (TestSSLServer) for scanning port to determine what protocols are already enabled and whether configuration was successful.
- Utility reverts the configuration changes done, to restore the state as it was before, when there is a failure in doing configuration changes.
- Utility can be used to apply security protocol configuration either for entire Cluster or none.
- Utility generates report (csv file) with all Clustered ESXi server's configuration result such as what security protocols were enabled earlier, after configuration what protocols are enabled and etc.

## ❖ Prerequisites for running Utility:

- vCenter Server and ESXi Server services/ports are all configured with same version of security protocol(s). (If there are any exceptions, those are automatically considered)
- Take backup of all vSphere HA enabled Clusters configuration (settings, rules and etc)
- Java runtime environment /JDK where Java version is 1.7.0_45 or higher.

## ❖ Options available:

- Enable SSLv3 protocol on vSphere HA/FDM port 8182
- Disable SSLv3 protocol on vSphere HA/FDM port 8182

## ❖ How to run the Utility?

- Copy/Download the *fdmsecprotomgmt.jar* from Runnable-jar on to local drive folder say *c:\SecurityProtoMgmt*
- Open a command prompt and cd to the folder, lets say *cd SecurityProtoMgmt*
- Run a command like shown below to see various usage commands, *[READ ALL THE COMMANDS IN ENTIRETY TO KNOW WHAT COMMAND BEST SUITS FOR YOUR ENVIRONMENT]*

```
C:\SecurityProtoMgmt>java -jar fdmsecprotomgmt.jar --help
```

```
~~~~~~~~~~~~~~~~~~~~~~~~~ SSLv3 CONFIGURATION ~~~~~~~~~~~~~~~~~~~~~~~~~

Usage: java -jar fdmsecprotomgmt.jar --vsphereip <vCenter Server IP> --
username <uname> --password <pwd> --hostsinfofile <pathToHostsListfile>
[enablessl] [disablessl]

Example : To enable SSLv3 on One or More vSphere HA enabled Cluster & its
ESXi hosts

"java -jar fdmsecprotomgmt.jar --vsphereip 10.1.2.3 --username adminUser --
password dummy --hostsinfofile c:\SecurityProtoMgmt\clusteresxihosts.csv
enablessl"

You can obtain hosts file information, by using 'secprotomgmt.jar' utility

C:\SecurityProtoMgmt>
```

### 1. SSLv3 enablement/disablement

By having Hosts information file (hostsinfo.csv) ready with ESXi hosts to be configured, administrator credentials information, SSL configuration changes can be made as follows,
`--hostsinfofile` : Provide path to hostsinformation file that is created/populated with required information.

`enablessl`: This would enable SSLv3 protocol on all services of ESXi, along with default supported TLS protocols.

`disablessl`: This would disable SSLv3 protocol on all services of ESXi, leaving default supported TLS protocols as is.

### 1. Version Checker

Version check is done to ensure if supported version of vCenter Server and ESXi server are in vSphere HA enabled Cluster. The utility can be used on HotPatch builds ,if and only if, it is built on top of vSphere 5.5U3b builds.

### 2. Details

Utility retrieves all vSphere HA enabled Clusters and its ESXi hosts. For each vSphere HA enabled Cluster, all its ESXi hosts are matched with the ESXi hosts provided by user (through hosts information file). If there is an exact match i.e. Actual ESXi Hosts in vSphere HA enabled cluster (retrieved through vCenter Server) AND ESXi Hosts provided by user, then only utility would proceed. Further, if there is a match, Cluster is added with advanced option “`das.config.vmacore.ssl.sslOptions`” with value, set according to the requested protocols to enable/disable and all ESXi hosts within that cluster is reconfigured for HA, for changes to take effect. If there is an failure to apply change on any one of the ESXi host in the cluster, change is reverted for the entire Cluster (and hence all ESXi hosts in the cluster). If there is any error seen in rolling back the changes, please check and manually configure the settings as mentioned in the KB and Cluster settings can be reapplied from the backup configurations that you must have taken before running the utility.