ESXi 5.x- SSL Security Protocol Configuration – Command line utility

This document provides you with details about script utility package on how to automatically enable or disable SSLv3 protocol for ESXi 5.x [ESXi 5.0 P13 (ESXi500-201606001 release), ESXi 5.1 P09 (ESXi510-201605001 release) and ESXi 5.5U3b release onwards]. The utility package automates the steps mentioned in the KB- 2139396.

❖ Features

- Automatically modify the configuration files and run esxcli commands to disable\enable SSLv3 on all ESXi Services (Authd, Hostd/Rhttpproxy, SFCBD, Virtual SAN VP)
- Utility will take backup of configuration files before making any modifications. For example, /etc/sfcb/sfcb.cfg will be saved as /etc/sfcb/sfcb.cfg.bkup in the same directory.
- Utility has inbuilt scanner intelligence (TestSSLServer) for scanning ports 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 for a particular port.
- Utility can be used to apply security protocol configuration on selected, multiple ESXi Servers (run through vCenter Server) or single ESXi Server (run directly against ESXi Server), in one go.
- Utility generates report (csv file) with all ESXi server’s configuration result such as what security protocols were enabled earlier on each port, after configuration what protocols are enabled and etc.
- Utility provides a way to encrypt and record ESXi server(s) password, before providing it as an input.

❖ Different options available with the Utility

- Enable SSLv3 on all ESXi Server Ports
- Disable SSLv3 on all ESXi Server Ports

- Get All ESXi server's details from vCenter Server and record it in a csv file.
- Encrypt plain ESXi password to record ESXi server(s) password in csv file for providing it as an input to the utility later.

Note:

- Disabling SSLv3 protocol might break VC/ESXi product interoperability with other solutions. Please refer to compatibility guide before proceeding.
- VC/ESXi Services shall be restarted automatically, as needed, after SSLv3 protocol configuration is done on services.
- For SSLv3 configuration on ESXi services, script enables SSH on ESXi for logging into host via SSH connection and perform configuration changes for SSLv3 enablement/disablement. Once operation is complete, SSH service state is reverted to its original state.

❖ Prerequisites for running Utility

- Java runtime environment /JDK where Java version is 1.7.0_45 or higher.

❖ How to run the Utility?

- Copy/Download the `secprotomgmt.jar` from Runnable-jar folder (from the uploaded file) and unzip 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 secprotomgmt.jar --help

~~~~~~~~~~~~~~~~~~~ SSLv3 CONFIGURATION (ENABLE/DISABLE)
~~~~~~~~~~~~~~~~~~~
Usage: java -jar secprotomgmt.jar --vsphereip <vc/esxi server IP> --
username <uname> --password <pwd> [gethosts] [--hostsinfofile
<pathToHostsListfile>] [enablessl] [disablessl]

Example 1: To obtain hosts file information from vCenter Server
"java -jar secprotomgmt.jar --vsphereip 10.1.2.3 --username adminUser --
password dummy gethosts"

Example 2: To enable SSLv3 on multiple ESXi hosts
"java -jar secprotomgmt.jar --vsphereip 10.1.2.3 --username adminUser --
password dummy --hostsinfofile c:\ SecurityProtoMgmt\esxihosts.csv
```

```
enablessl"

Example 3: To disable SSLv3 on a SINGLE ESXi host
"java -jar secprotomgmt.jar --vsphereip 10.4.5.6 --username rootUser --
password dummyRoot disablessl"

~~~~~~~~~~~~~~~~~~~~ ESXi PASSWORD ENCRYPTION UTILITY ~~~~~~~~~~~~~~~~~~~~
For encrypting password (incase plain password of ESXi host can NOT be
recorded in hostsinfofile), use the following utility program
"java -jar passwordEncrypter.jar"
Follow the instructions and record the provided encrypted string into
hostsfile. SSL configuration utility has capability to decrypt this
password with provided SecretKey

C:\SecurityProtoMgmt>
```

PS:

When any of the argument to be specified, **for example** password as “dummy$123”, consists of special characters. Each client/shell environment (from where this utility is being triggered from) interprets some special symbols; as having different meanings. For instance, the password as-is may go fine on Windows, but NOT on MAC (password gets truncated to “dummy”). Since its at the client environment, simple way to pass such strings is within single or double quotes as,

```
--password 'dummy$123'  (OR) --password "dummy$123"
```

If due to the above mentioned behavior of OS/Shell-Client environment, utility execution fails complaining invalid user name, password and etc. Try the above solution.

1. Information on the usage of utility - gethosts

```
java -jar secprotomgmt.jar--vsphereip 10.1.2.3 --username adminUser --
password dummy gethosts
```

This command retrieves all connected ESXi hosts from provided VC inventory and puts them into CSV file (Comma separated values file). This file gets created under the folder where the jar files reside, in this case the file location would be: `C:\SecurityProtoMgmt\hostsinfo.csv`

This file need to be provided as input to the utility for applying SSL configuration changes on all/selected ESXi hosts, by **prepopulating** ESXi admin user and credentials information (This file can be easily edited through MS Excel like utilities)

2. Information on the usage of utility – SSLv3 enablement/disablement

```
java -jar secprotomgmt.jar --vsphereip 10.1.2.3 --username adminUser --
password dummy --hostsinfofile c:\ SecurityProtoMgmt\esxihosts.csv
enablessl
```

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.

3. Information on the usage of utility – SSLv3 configuration for SINGLE ESXi host

SSLv3 configuration can be done on a SINGLE ESXi host, without the need of VC or hosts information file being provided to the utility. The configuration utility can be triggered by just providing ESXi Server IP and SSLv3 enablement/disablement request as,

```
java -jar secprotomgmt.jar--vsphereip 10.4.5.6 --username rootUser --
password dummyRoot enablessl
```

```
java -jar secprotomgmt.jar--vsphereip 10.4.5.6 --username rootUser --
password dummyRoot disablessl
```

4. Information on the usage of utility – Password Encryption utility

One may feel that entering and storing ESXi administrator password in plain text, in hosts information CSV file is risky. For this purpose, Encryption utility is provided along with the SSL Configuration utility package. The encrypted utility is safe and secure to use, as it uses AES technique for encrypting password with dynamic key as entered by user. The resultant encrypted password can be safely entered in hosts information CSV file.
About dynamic Key: Due to AES restrictions key must be and can not exceed 16 characters in length. However, incase key entered by user is less than 16 characters in length, random characters are appended to the key to make it 16 characters. The same has to be noted and must be provided later for decryption.
Below is the command to start the utility [Copy/Download the `passwordEncrypter.jar` from Runnable-jar folder (from the uploaded file)], and follow the instructions as they appear on the command prompt

```
C:\SecurityProtoMgmt> java –jar passwordEncrypter.jar
```

5. Issues?

Reach out to Gururaja Hegdal (ghegdal@vmware.com)