NetMRI DISA STIG Policy Updater

Policy Update Guide | 12/18/2017

Introduction

This guide will show how to use the NetMRI Advisor service to implement updated DISA STIG policies for NetMRI configuration management compliance. This process uses the NetMRI Sandbox as a PERL5 interpreter and script engine to install the policy updates. Review the NetMRI Administrator Guide for details about the Sandbox. The active update process, once started, takes approximately 10 minutes to complete. NetMRI services are not interrupted during this operation.

Prerequisites

The following prerequisites must be met for successful completion of the process.

- Operational NetMRI standalone or Operations Center deployment
- SCP file transfer program (*must* be SCP, SFTP will not work) (e.g. WinSCP)
- SSH command line utility (e.g. puTTy)
- Network connectivity to your NetMRI appliance from a workstation with the necessary utilities
- If NetMRI has been deployed virtually, a Remote Sandbox VM must be available. Refer to the NetMRI Administrator Guide for how to download and deploy a Remote Sandbox VM and register it with your virtual NetMRI appliance (see page 265). Physical appliances ship with a virtual on-box Sandbox instance. If using a custom PERL5 interpreter, refer to the **Install.txt** file for details on PERL module requirements.

Update Procedure

File Acquisition

DISA STIG Policy update files are currently distributed by email only. You will receive an email from your account team containing the files necessary to perform the policy updates. The files you will receive are:

- **Install.txt** – Contains instructions for deploying the policy updates. This guide includes these instructions for clarity, but this file should be reviewed in the event there have been changes to the process.
- **DISA_STIG_Update_<date>.tar.gz** – This is the zipped archive containing all the necessary files (policies, scripts, etc.) for updating the appliance.
- **DISA_STIG_Update_<date>.tar.gz.md5** – This is the verification hash for the above archive file.
- **README_DISA_STIG_Update_<date>.txt** – Contains detailed information about which policies have been updated for the current STIG cycle release and if new vendor support has been added.

Copying Files to the NetMRI Appliance and Sandbox

1) Refer to the NetMRI Administrator Guide, page 431 for additional information on file transfers to/from the NetMRI appliance for physical installations.
2) Using a SCP client, (this *must* be using the SCP protocol, SFTP will fail to copy) make a connection to the NetMRI appliance's (connect to the OC if you have an OC deployment) IP address or hostname, and log in with the administrator User ID and password (default **admin** account). If a Remote Sandbox VM is being utilized, connect directly to the Remote Sandbox using the **sbuser** account.

© 2018 Infoblox Inc. All rights reserved.

3) For physical appliances, transfer the installation archive to the **/Backup/Sandbox/** directory on the NetMRI appliance. The default session directory is already inside the **Backup** directory by default.

   For virtual appliances, transfer the installation archive to the **/sbuser** directory on the Sandbox VM. The default session directory is already inside the **sbuser** directory by default. If you are using a VM installation, you can skip to the next section of the guide.

   Example SCP copy command:

   ```
   scp ./U_SRG-STIG_2017_10_Update.tar.gz sbuser@10.100.0.121:~
   ```

4) Using a SSH client, log into the NetMRI's IP address using the same administrator ID and password and enter the command ***sandbox login*** to login to the Sandbox BASH session within the NetMRI appliance. Once in the Sandbox session, the sandbox session prompt will be displayed.

   ```
   NetMRI> sandbox login

   [root@sandbox ~]#
   ```

5) Verify the administrator's home directory (**/sbuser**) is the active directory using the print working directory command: **pwd**. If **/sbuser** is not the working directory displayed as the output, issue the change directory command, **cd**, to return to the default directory location.

   ```
   [root@sandbox ~]# pwd

   /sbuser
   ```

6) Copy the installation archive to the administrator's home directory in the Sandbox. The source file location "**/mnt/host/data/userdata/**" is the mounted location of the "**/Backup/Sandbox/**" directory on the NetMRI appliance. If you are using a Remote Sandbox, skip this step.

   ```
   [root@sandbox ~]# cp /mnt/host/data/userdata/<filename>.tar.gz .
   ```

Extract and Modify the Installation Files

1) Unpack the installation archive file.

   ```
   [root@sandbox ~]# tar zxvf DISA_STIG_Update_<date>.tar.gz
   ```

2) Change directory to the newly created DISA-STIG directory. Use the **pwd** command to verify the directory afterwards if desired.

   ```
   [root@sandbox ~]# cd DISA-STIG/
   ```

3) Edit the **STIG_updater.sh** script file using the sandbox's Vim text editor. This will configure the script for the local NetMRI appliance that is receiving the policy updates.

   ```
   [root@sandbox ~]# vi STIG_updater.sh
   ```

   a) Find the **SNMP_USERAUTH="admin:admin123";** string in the script and navigate to this line using the down arrow key.

   b) Press the 'i' key to enable insert mode. The status line at the bottom will change to

      ```
      - INSERT -
      ```

   c) Edit the **SNMP_USERAUTH** credentials to match the NetMRI administrator's credentials. Ensure the quotes and colon are left intact. If you are using special characters in your password, change the double quotes to single quotes as shown below.

      ```
      SNMP_USERAUTH='<user>:<password>';
      ```

© 2018 Infoblox Inc. All rights reserved.

d) Navigate two lines down using the down arrow key to the **SNMP_IP="192.168.2.1";** line. Edit this IP address entry to match the NetMRI appliance's IP address (SSH/WebGUI/management address).

```
SNMP_IP="<IPAddr>";
```

e) Save the changes to the script with the following key sequence

i) Escape Key (**ESC**)

ii) Colon (**:**)

iii) **wq**

f) Verify the changes using the **less** command. Press '**q**' to quit the viewer.

```
[root@sandbox ~]# less STIG_updater.sh
```

Run the Installation Script

1) Run the shell script on Sandbox.

```
[root@sandbox ~]# ./STIG_update.sh
```

2) The output of the running script should look similar to the lines below.

```
Tue Jan 31 17:58:51 UTC 2017 STIG_updater.sh: Beginning DISA STIG update.
Tue Jan 31 17:58:52 2017 - Pruning old DISA STIG Policy Rules.
...
Tue Jan 31 17:58:54 UTC 2017 prune_old_rules.pl run: OKAY
Tue Jan 31 17:58:54 2017 - Updating STIG Policies and Policy Rules
...
Tue Jan 31 17:59:13 2017 - STIG Policies and Policy Rules updated.
Tue Jan 31 17:59:13 UTC 2017 update_DISA_policy_rules.pl run: OKAY
```

Viewing the New STIG Policies and Rules

View and verify the new and/or updated STIG policies by going to the **Config Management > Policy Design Center > Policies/Rules** tabs in NetMRI. New policies and rules will be visible with the current STIG revision numbers.

If specific existing STIG revisions have been updated for content, syntax or device support, you can view them in the individual rule definitions.

© 2018 Infoblox Inc. All rights reserved.