SANnav Globalview 2.1.1 fix for BSA-2021-1651 Content Notes

(Created on 12/21/2021)

Note: In this document, the term "SANnav" is used to refer to "SANnav Globalview" only.

This script is created for the SANnav Globalview 2.1.1 and includes the below mentioned changes.

Overview

This document describes the details of the content and installation instructions of the SANnav Globalview 2.1.1 fix for the vulnerability mentioned in the BSA-2021-1651.

This script includes the following fixes/updates:

- This script will remove the JNDI classes from the log4j jars for all SANnav docker images.

This script must be applied on top of SANnav Management Global 2.1.1.

Installation Instructions

****Notes:**

- SANnav will be restarted during the script execution. Please make sure that no user is logged into SANnav before executing the script.
- Make sure that these commands are run with either root or sudo.
- Make sure that the unzip and zip (yum install unzip, yum install zip) utilities are installed already on the SANnav server before applying this script.
- Make sure that a full SANnav backup is saved prior to executing this script.

Steps:

- Copy the Global_2.1.1_BSA2021_1651.tar.gz file into <SANnav_Install_Home>/bin folder
- Extract the content of the Global_2.1.1_BSA2021_1651.tar.gz
  - tar -zxvf Global_2.1.1_BSA2021_1651.tar.gz

- The extracted zip file contains the following three shell script files:
    - find-log4j.sh
    - patch-log4j.sh
    - fix-log4j-vulnerability.sh
- Make sure that the all the above three scripts have executable permission
- Execute the following commands to change the permissions of the files
    - chmod 755 find-log4j.sh
    - chmod 755 patch-log4j.sh
    - chmod 755 fix-log4j-vulnerability.sh
- Run the script **fix-log4j-vulnerability.sh**. The script will do the below:
    - Stop SANnav services
    - Stop Docker service
    - Executes the other two scripts in this package
    - Start Docker service
    - Start SANnav services.

IMPORTANT NOTE: Please wait for 15-20 minutes before launching SANnav Client. If you see any errors on the terminal, please contact Brocade support.

Important Considerations for Backup/Restore of SANnav Data

- Immediately after having successfully applied this script, it is recommended to take a backup which can be restored later.
- This script **<u>must be reapplied</u>** again after a successful restore.

Restoring a Backup that was taken <u>before</u> applying this script

- Install SANnav 2.1.1
- Restore the Backup that was taken before the script applied
- Apply the script

Restoring a Backup that was taken <u>after</u> applying this script

- Install SANnav 2.1.1
- Apply the script
- Restore the Backup that was taken after applying this script
- Apply the script again

Troubleshooting

If customer deployed / executed the script from a folder other than <SANnav_Install_Home>/bin folder.

```
./fix-log4j-vulnerability.sh
```

```
[root@sannav41225 /]# sh fix-log4j-vulnerability.sh
```

```
################################################
########### Fix Log4j Vulnerability ###########
################################################

tee: //logs/fix_log4j_vulnerability_2021_12_20_14_25_28_PM.log: No such file or directory
Stop the SANnav services.
fix-log4j-vulnerability.sh: line 56: //bin/stop-sannav.sh: No such file or directory
[root@sannav41225 /]#
```

To successfully deploy the script again,

- User must extract the tar.gz under <SANnav_Install_Home>/bin folder.
- After extracting the tar.gz file, the “fix-log4j-vulnerability.sh” script will be present under <SANnav_Install_Home>/bin folder.
- User will have to re-run fix-log4j-vulnerability.sh script.