Cyber Defence Operation Centre

NEC Africa

Installing ArcSight Logger on CentOS 7

Document Information

Author:	Armand Kruger
Title:	Cyber Defence Analyst
Version:	1.0
Department:	Cyber Defence Operations Centre

Table of Content

Logger CentOS 7 Prerequisites

Note: Please make sure that the base OS (CentOS 7) is already preconfigured with the below setting before attempting the follow the below Logger Installation Guide!

Base OS Pre-Configured Settings:

- Valid Hostname (Not Localhost)
- Static IP
- Subnet Mask
- DNS Name Server
- Default Gateway
- Stable Internet Connection

Refer to – "*Installing & Maintaining an CentOS 7 Minimal Server Environment Fact Sheet*" for guidelines regarding the above pre-configured settings

CentOS 7 OS Packages to Install after CentOS 7 Installation:

- Java
- Net-Tools
- Tcpdump
- OpenSSH

Ports to be Allowed Through the Firewall

- TCP 22
- TCP 9000
- TCP 443
- TCP 515
- UDP 524

We Will Create a Bash Script that will automatically install all the above dependencies and apply port configurations. Make sure that you have a stable internet connection before attempting to execute the below script. Copy and Paste the "Script Content" into the script and execute it.

Creating a Bash Script

```
vi <script name>.sh
```

Making Bash Script Executable

```
chmod 755 <script name>.sh

OR

chmod +x <script name>.sh
```

Executing Script

```
./<script name>.sh
```

Script Content

```
!#/bin/bash
yum install java -y
yum install net-tools -y
yum install tcpdump -y
yum install openssh openssh-server openssh-clients openssl-libs -y
yum info java
yum info net-tools
yum info tcpdump
ssh V
systemctl stop firewalld
firewall-cmd --zone=public --add-port=22/tcp --permanent
firewall-cmd --zone=public --add-port=514/udp --permanent
firewall-cmd --zone=public --add-port=9000/tcp --permanent
firewall-cmd --zone=public --add-port=443/udp --permanent
firewall-cmd --zone=public --add-port=515/tcp --permanent
firewall-cmd --reload
systemctl start firewalld
firewall-cmd --list-all
```

After installing the necessary dependencies and opening the required ports, we need to adjust the "*user Process Limit*". Follow the Below commands is order to successfully adjust the required user process limit values.

Path to User Process Limits

```
/etc/security/limits.d/
```

If Limits.d Doesn't exist, Create the Directory

```
mkdir /etc/security/limits.d
```

Edit the Process Limit File

```
vi /etc/security/limits.d/20-nproc.conf.
```

If the File Contains Existing Values, delete them and add the Following

```
* soft nproc 10240
* hard nproc 10240
* soft nofile 65536
* hard nofile 65536
```

Reboot the Server & Verify User Process Limits

```
reboot
then
ulimit -a
```

Installing ArcSight Logger

(CLI Install)

Make Logger File Executable

```
chmod +x <logger file>.bin
```

Run Logger File

```
./<logger file>.bin -i console
```

Follow the Installation Steps and Specify the following

- Accept User Agreement
- Make Sure Default Install path is "/opt"
- Supply Full Path to the License File

Connecting the Logger via Web

URL Path

https://<Hostname> or <IP Address>:<Port>

Default Credentials (First Logon)

Username: admin
Password: password

Error Connecting to Logger (Via Web)

Error 403 Forbidden, you don't have permission to access / on this server

Solution to Above Error

During the Installation of the Logger .bin file, make sure that the user you are logged in with has access to the parent directory of the installation directory

Basic Logger Commands

Starting Logger

```
loggerd start
```

Stop All Sub-Processes

```
loggerd stop
```

Restart All Logger Sub-Processes

```
loggerd restart
```

Display Logger Processes Status

```
loggerd status
```

Stop the Logger

```
loggerd quit
```

Uninstalling the Logger

Browse to The Logger Installation Directory

```
/opt/
```

Run the Un-Installation File

```
./UninstallerData/Uninstall_ArcSight_Logger_6.2
```

Note: Change the version at the end of the code if you have a different ArcSight Logger Installation