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

Ports to be Allowed Through the Firewall

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

Before we can start the ArcSight Logger Installer, we must prepare the system with some custom configurations changes. A non-root user account must exist in the system before installing the Logger. Follow the below steps and commands to prepare the system for the Logger installation. Perform all the below steps as ROOT user!

Create the Following New Folders

```
mkdir /home/ArcSightFiles

mkdir /opt/arcsight
```

Give the New Folder Read & Write Permissions

```
chmod 755 /home/ArcSightFiles

chmod 755 /opt/arcsight
```

Create a new Group Called ArcSight

```
groupadd -g 750 arcsight
```

Add new User Arcsight & Add User Arcsight to new group

```
useradd -m -g arcsight -u 1500 arcsight
```

Now we need to change the default User Process Limits to ensure that the logger is operational after installation. Follow the below steps AFTER the above has been completed successfully. All steps and commands must be executed as ROOT!

Path to User Process Limits Configuration File

```
vi /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

```
reboot
```

After Bootup & Logon, Verify the User Process Limits

```
ulimit -a
```

Verify the Following Output

```
Open files 65536

Max user processes 10240
```

Now we need to make the last adjustment before we can start the Logger Installer. Follow the below steps in order and make sure to perform all configurations as ROOT!

Navigate to the Following File

```
cd /etc/systemd/
```

Edit the Following File

```
vi logind.conf
```

Find the Following within the Configuration File

```
#RemoveIPC=no
```

Remove the # before the Line

```
RemoveIPC=no
```

Restart the Service

```
systemctl restart system-logind.service
```

Now that the system is prepared, we can start with the Logger Installation. Navigate to where you placed the Logger Installer File and follow the below as ROOT!

Make the Logger Installer Executable

```
chmod +x <LoggerInstaller>.bin
```

Note: Replace <LoggerInstaller> with your appropriate ArcSight Logger Installer name.

Execute the Logger Installer

```
./<LoggerInstaller>.bin -i console
```

Follow the Installer Process. But make sure to enter the following information during the Logger Installer!

Default Installation Path: /opt/arcsight

Full Path the the License File: “ends with .dat”

Logger System Service: Start Logger as a Service

Specify non-root user account: arcsight

Default Port: 443

Default Locale: 1 for English

Connecting the Logger via Web

URL Path

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

Default Credentials (First Logon)

```
Username: admin
Password: password
```

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