\Orchestrating a brighter world

Cyber Defence Operation Centre

NEC Africa

Installing ArcSight ESM 6.11 on CentOS 7

Document Information

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

Table of Content

Chapter 1

Chapter 2

Chapter 3

ArcSight ESM 6.11 Prerequisites

Note: Please make sure that the base OS (CentOS 7) is already preconfigured with the below settings before attempting the follow the below ArcSight ESM 6.11 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 8443
- TCP 9000
- UDP 694
- TCP 7789
- UDP 22

Preparing the System for ArcSight ESM 6.11

Log in a Root User

```
Username: root
Password: *********
```

Create a New Folder in the Following Directory

```
mkdir /opt/arcsight
```

Give the Directory Read & Write Permissions

```
chmod 755 /opt/arcsight
```

Untar the ArcSight Installer File

```
tar xvf <ESMInstallerName>.tar
```

Note: Replace <ESMInstaller> with your ESM Installer File

After the file is untarred, it creates a script called **“prepare_system.sh”** in the **“Tools”** Sub-Directory. Run the **“prepare_system.sh”** & change ownership off all the files and folders that were extracted from the tar file to be owned by the arcsight user account

Navigate to the Sub-Directory “Tools”

```
cd /tools
```

Run the “prepare_system.sh script

```
./prepare_system.sh
```

Change Ownership of all Files & Directories to user arcsight

```
chown -R arcsight MainDirectory/
```

Reboot the System

```
reboot
```

After Bootup & Logon, Type the following Command

```
ulimit -a
```

Verify the Following Values

```
open files 65536

max user processes 10240
```

Install the Time Package

```
rpm -Uvh tzdata-2017g-1.e17.noarch.rpm
```

Set the Correct Time-Zone

```
timectl set-timezone Africa/Johannesburg
```

Restart the Logind Service

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

Reboot the System

```
reboot
```

Login as the arcsight user

```
Username: arcsight

Password: *********
```

Note: Make sure that you have the appropriate Read & Write Permissions to the /opt/arcsight folder & the folder that contains the license file before starting the ESMSuite Installer!

Starting the ArcSight ESM 6.11 Installer

Make the File Executable

```
chmod +x ArcSightESMSuite.bin
```

Run the Installation File (.bin)

```
./ArcSightESMSuite.bin -i console
```

Type the Following Command after the Suite Installer Stops (To continue with the ESM Installer)

```
/opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i console
```

Follow the Installation Steps and Make sure that you specify the following information during the Installation Procedure

- **Accept the License Agreement**
- **Installation Directory: /opt/arcsight**
- **Location of the License File (Full Path Included License File)**
- **CORR Password**
- **System Storage Space: (Depends on Available Storage)**
- **Event Storage Space: (Depends on Available Storage)**
- **Retention Period: 14 Days**
- **Email Notifications**
- **Product Mode: Default Mode**
- **Event Broker: No**
- **ArcSight Investigate: No**
- **Extra Packages: None (Continue)**
- **Review Summary & Continue**

Enter the Below Command immediately after the ESM Configuration Has Completed

```
/opt/arcsight/manager/bin/setup_services.sh
```

The ESM Installation should now be successfully completed, you should now be able to login from The Console (Windows-based or Linux-based).

Note: If the ESM Installation was unsuccessful, Uninstall the ESM Following the Below Steps and Commands and reinstall the ESM. Before Re-Installation, make sure that you have met all required prerequisites & system prepare requirements.

Uninstalling The ESM

Login as Root

```
Username: Root
Password: *******
```

Run the Following Command

```
/opt/arcsight/manager/bin/remove_services.sh
```

Reboot

```
reboot
```

Login as user arcsight

```
Username: arcsight
Password: *********
```

Verify if any ArcSight Processes are Running

```
ps -elf | grep /opt/arcsight
```

Shut Down Remaining ArcSight Processes (If there is Present)

```
kill -9 <process_id_number>
```

Navigate to the Following Directory

```
cd /opt/arcsight/suite/UninstallerData
```

Run the Following Script

```
./Uninstall_ArcSight_ESM_Suite_6.11.0
```

Note: After the script has completed, navigate to /tmp & /opt and make sure that there is no ArcSight related files present. If there is any ArcSight related files present, deleted all of them and reboot the system.