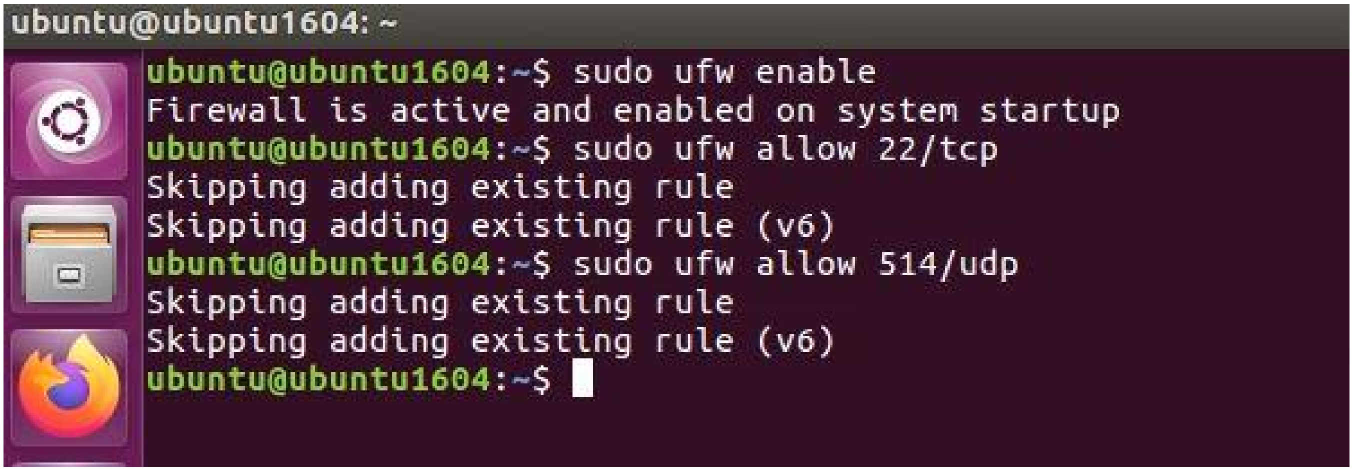
Arcsight Project

Detecting, Monitoring and Forwarding logs of Ubuntu OS to Arcsight Console

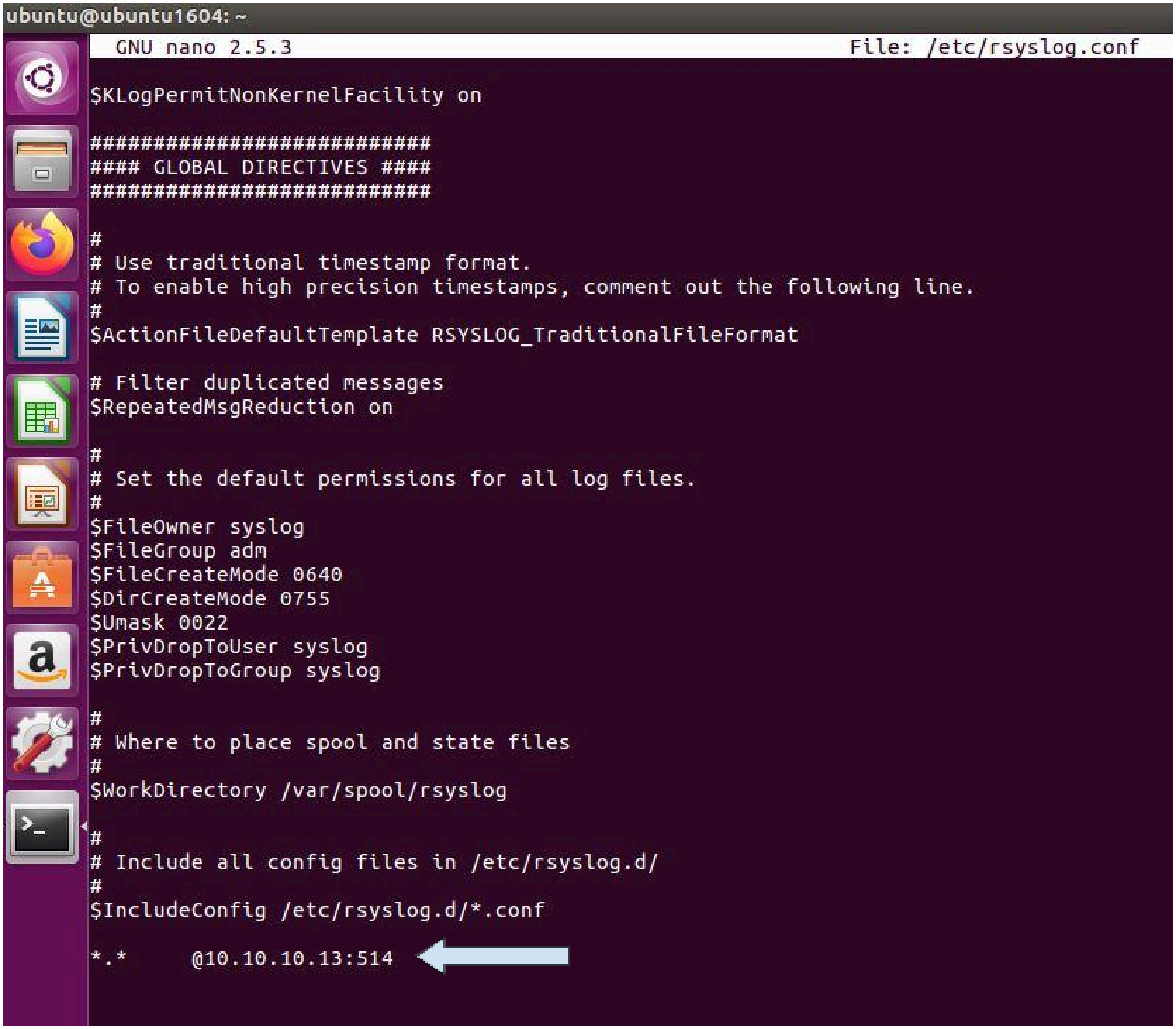
Detecting, Monitoring and Forwarding the Security log, Application logs, Syslog of the Ubuntu desktop system to the SIEM tool Arcsight Console using the Arcsight Smart Native connector version 8.2 installed in Windows OS as a service.

Step 1 - Enter these commands to allow 22/tcp and 514/udp port.



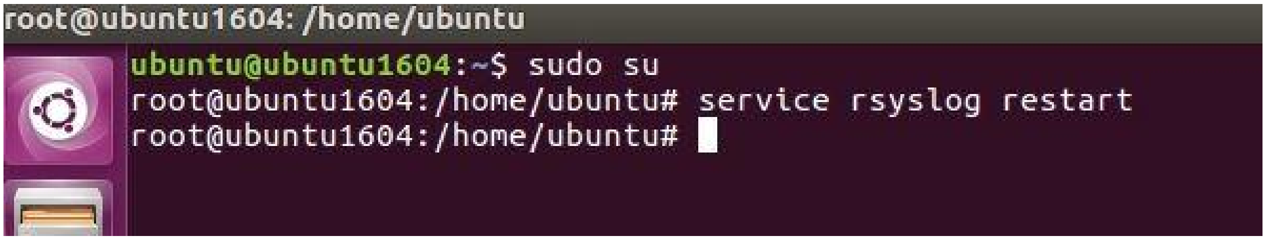
```
ubuntu@ubuntu1604: ~
ubuntu@ubuntu1604:~$ sudo ufw enable
Firewall is active and enabled on system startup
ubuntu@ubuntu1604:~$ sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
ubuntu@ubuntu1604:~$ sudo ufw allow 514/udp
Skipping adding existing rule
Skipping adding existing rule (v6)
ubuntu@ubuntu1604:~$
```

Enter command “sudo nano /etc/rsyslog.conf” to edit the configuration file.
In this file add the last line. Enter the IP Address of Windows OS in which we will be installing Arcsight Smart Connector.



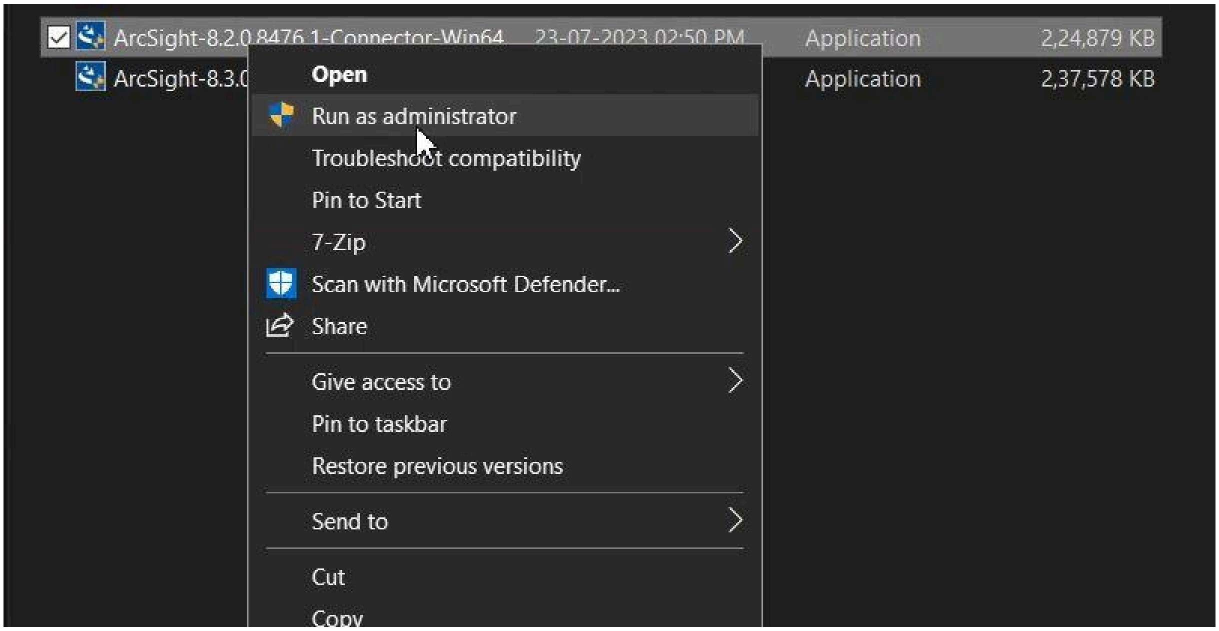
```
  GNU nano 2.5.3                                                File: /etc/rsyslog.conf

$KLogPermitNonKernelFacility on

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

*.*     @10.10.10.13:514
```

Enter this Commands to restart rsyslog.

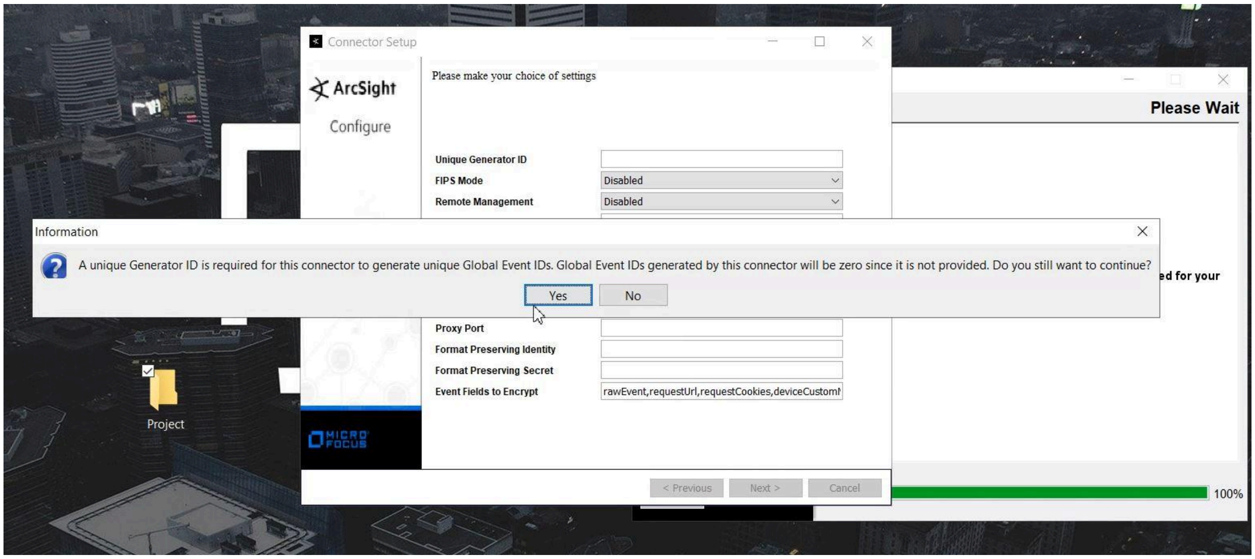


```
root@ubuntu1604: /home/ubuntu
ubuntu@ubuntu1604:~$ sudo su
root@ubuntu1604:/home/ubuntu# service rsyslog restart
root@ubuntu1604:/home/ubuntu#
```

Step 2 -Right Click the Arcsight Smart Connector and click on “Run as administrator”


ArcSight-8.2.0.8476.1-Connector-Win64 23-07-2023 02:50 PM Application 2,24,879 KB
ArcSight-8.3.0 Application 2,37,578 KB
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
7-Zip
Scan with Microsoft Defender...
Share
Give access to
Pin to taskbar
Restore previous versions
Send to
Cut
Copy

Click on Next → Yes



Please make your choice of settings

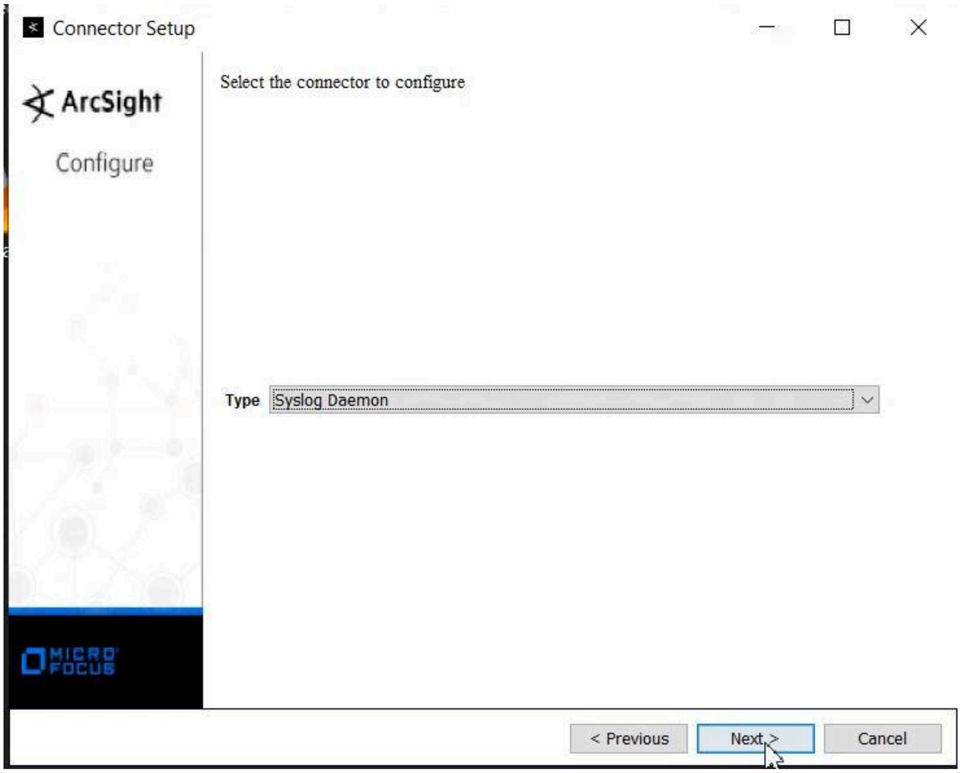
Unique Generator ID
FIPS Mode: Disabled
Remote Management: Disabled
Proxy Port
Format Preserving Identity
Format Preserving Secret
Event Fields to Encrypt: rawEvent,requestUrl,requestCookies,deviceCustomI

Information

A unique Generator ID is required for this connector to generate unique Global Event IDs. Global Event IDs generated by this connector will be zero since it is not provided. Do you still want to continue?

Yes No

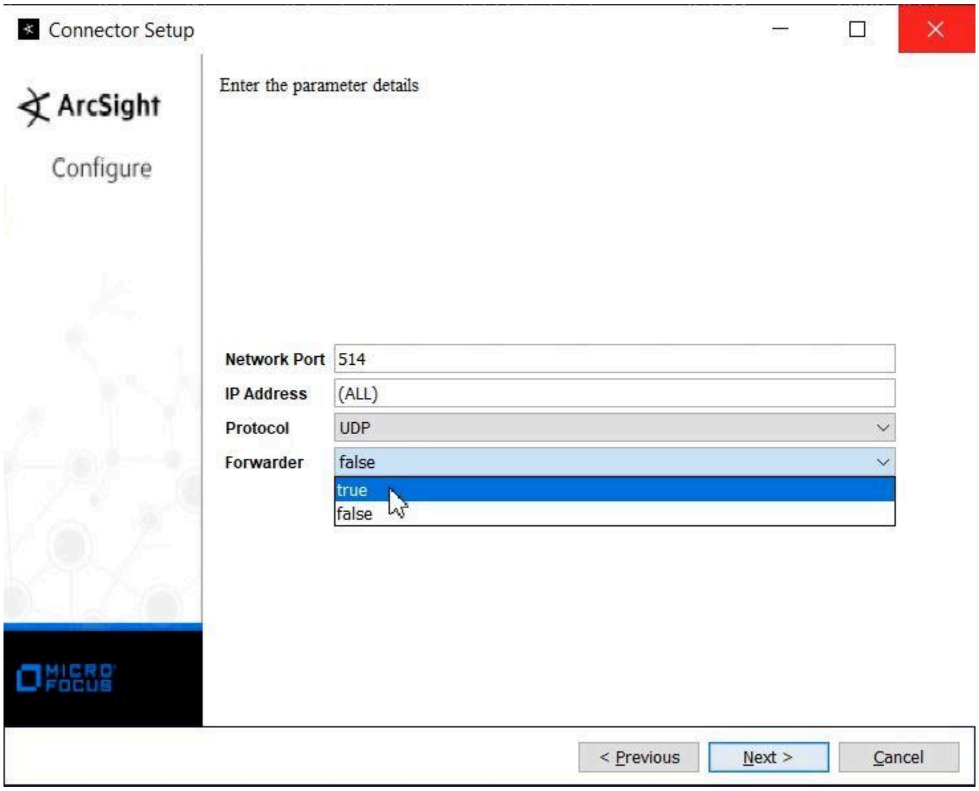
Select the type as “Syslog Daemon”



Select the connector to configure

Type: Syslog Daemon

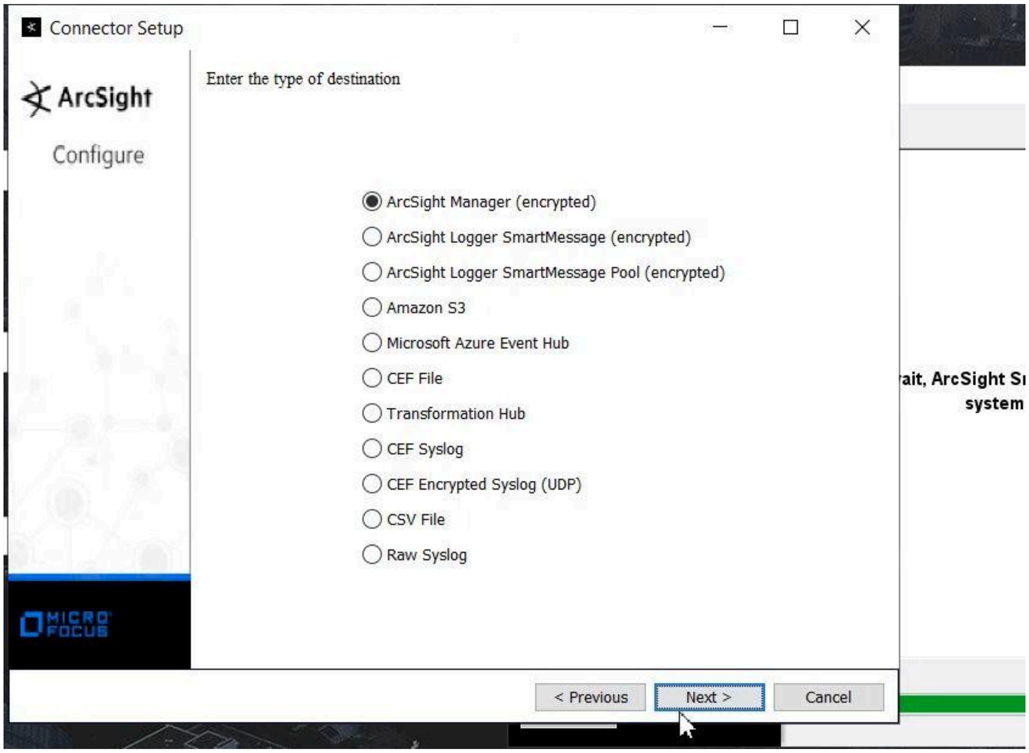
Choose the Options as given below.Select the Forward as (True).Then Next.



Enter the parameter details

Network Port	514
IP Address	(ALL)
Protocol	UDP
Forwarder	false

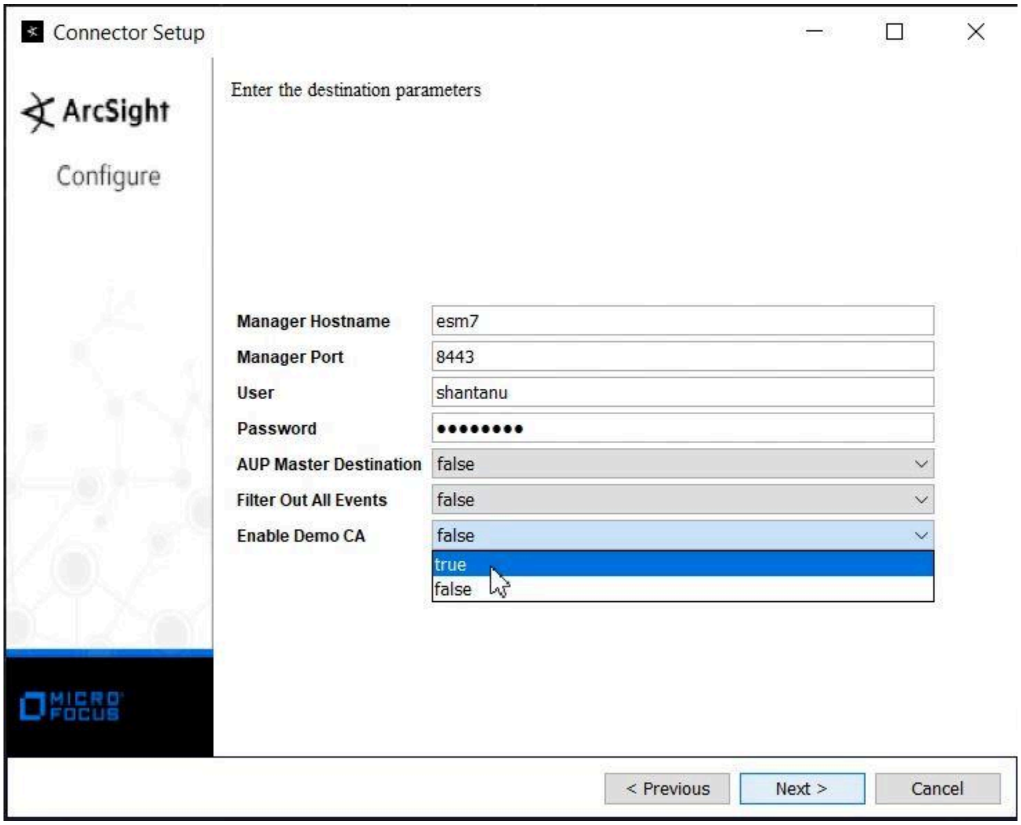
Select the type of destination as “Arcsight Manager (encrypted)”.Then Next



Enter the type of destination

- ● ArcSight Manager (encrypted)
- ○ ArcSight Logger SmartMessage (encrypted)
- ○ ArcSight Logger SmartMessage Pool (encrypted)
- ○ Amazon S3
- ○ Microsoft Azure Event Hub
- ○ CEF File
- ○ Transformation Hub
- ○ CEF Syslog
- ○ CEF Encrypted Syslog (UDP)
- ○ CSV File
- ○ Raw Syslog

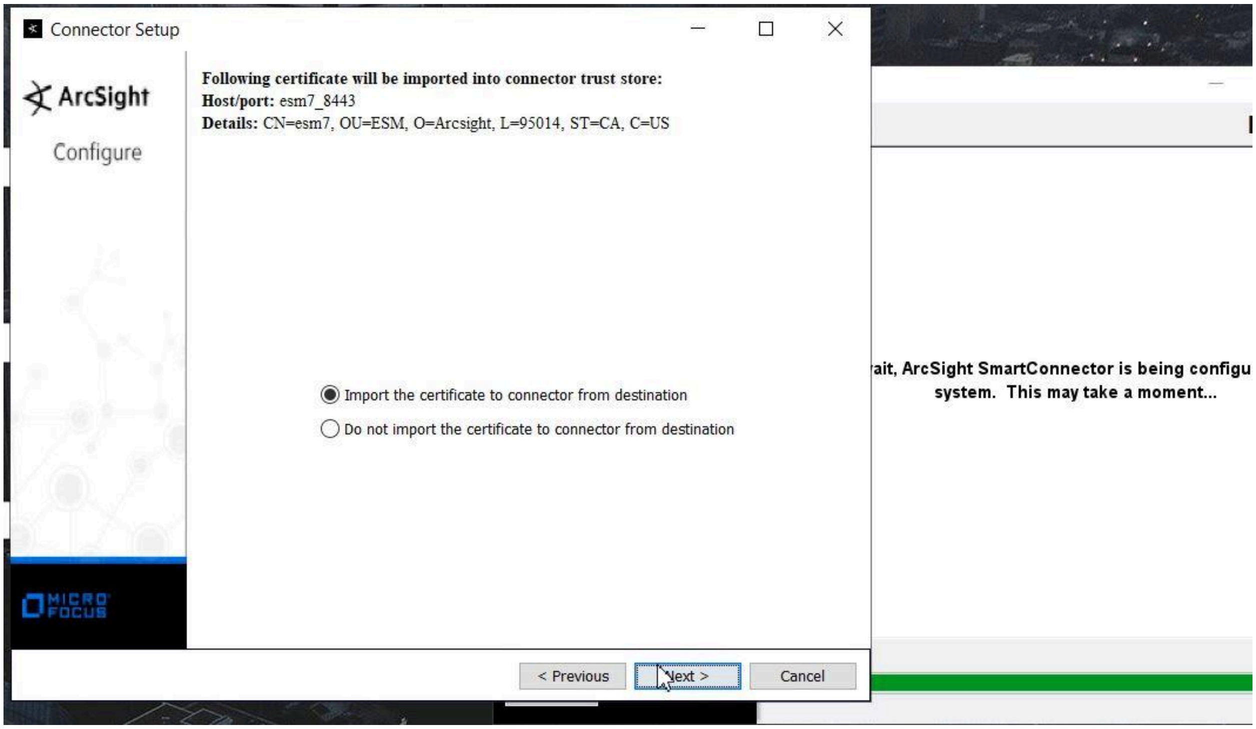
Enter the destination parameters according to your configuration as given below.
Select Demo CA as True.Then Next



Enter the destination parameters

Manager Hostname	esm7
Manager Port	8443
User	shantanu
Password	••••••••
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

Select the First option.Then Next.



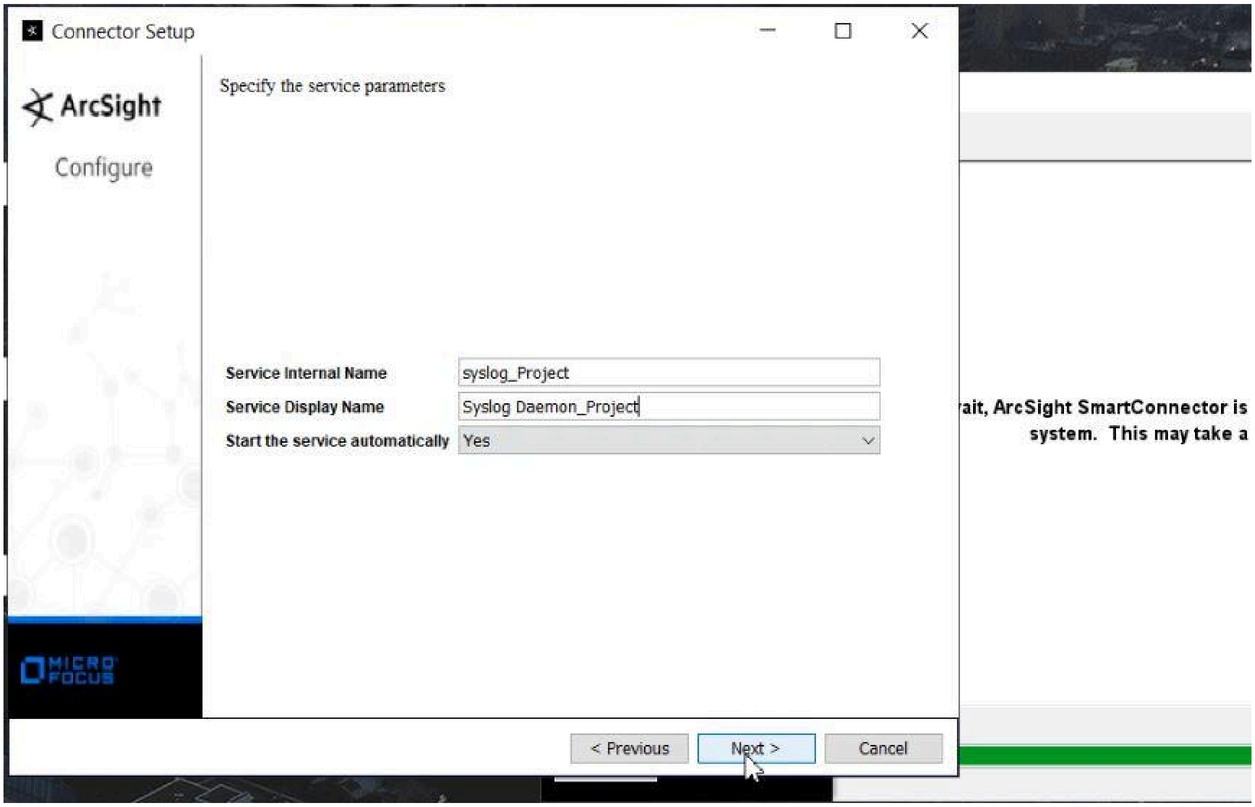
Connector Setup
ArcSight
Configure
MICRO FOCUS

Following certificate will be imported into connector trust store:
Host/port: esm7_8443
Details: CN=esm7, OU=ESM, O=Arcsight, L=95014, ST=CA, C=US

● Import the certificate to connector from destination
○ Do not import the certificate to connector from destination

< Previous
Next >
Cancel
ait, ArcSight SmartConnector is being configu
system. This may take a moment...

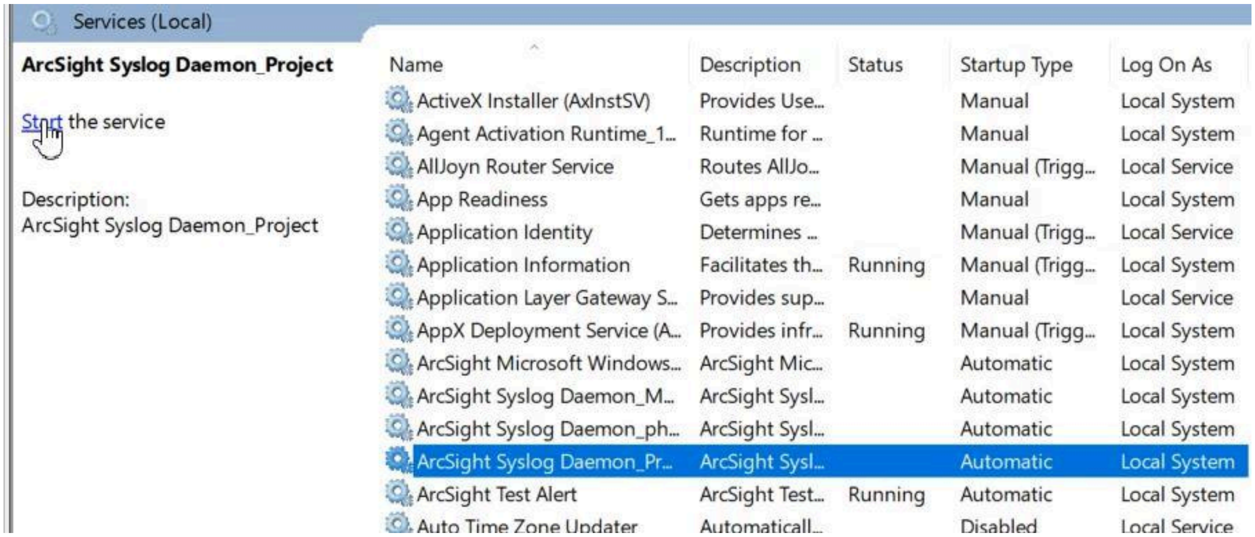
Enter the Service and Display name of service.Then next.



Specify the service parameters

Service Internal Name	syslog_Project
Service Display Name	Syslog Daemon_Project
Start the service automatically	Yes

Start the Service by going to services in Windows OS which we created using connector.



Services (Local)

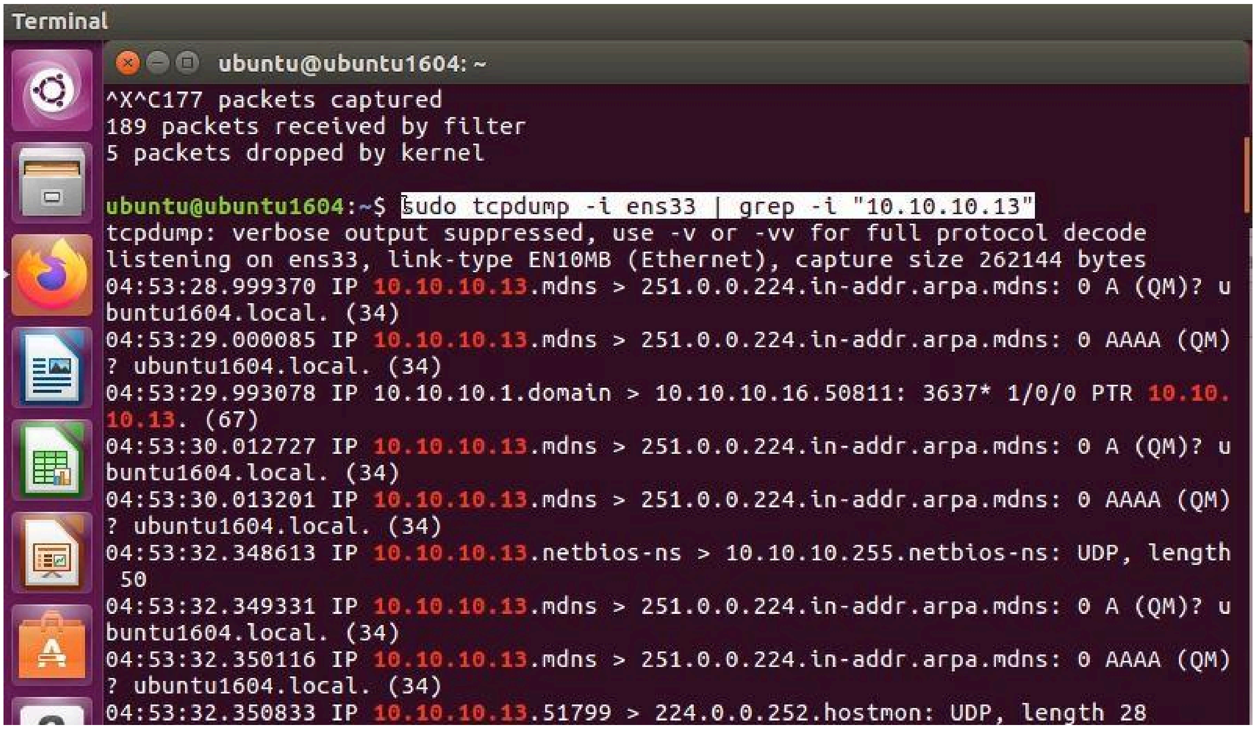
ArcSight Syslog Daemon_Project

Start the service

Description:
ArcSight Syslog Daemon_Project

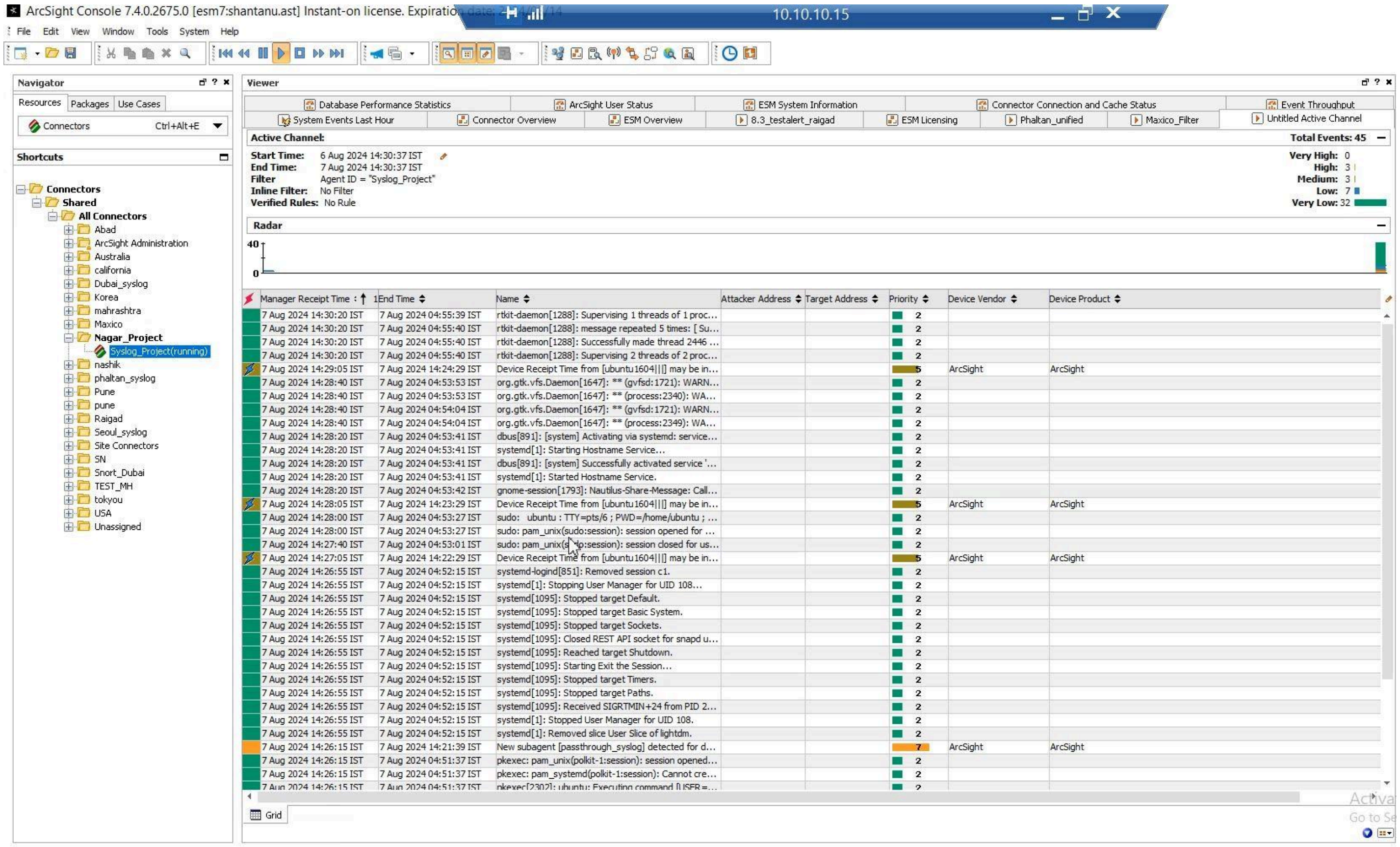
Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Local System
Agent Activation Runtime_1...	Runtime for ...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Local Service
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trigg...	Local Service
Application Information	Facilitates th...	Running	Manual (Trigg...	Local System
Application Layer Gateway S...	Provides sup...		Manual	Local Service
AppX Deployment Service (A...	Provides infr...	Running	Manual (Trigg...	Local System
ArcSight Microsoft Windows...	ArcSight Mic...		Automatic	Local System
ArcSight Syslog Daemon_M...	ArcSight Sysl...		Automatic	Local System
ArcSight Syslog Daemon_ph...	ArcSight Sysl...		Automatic	Local System
ArcSight Syslog Daemon_Pr...	ArcSight Sysl...		Automatic	Local System
ArcSight Test Alert	ArcSight Test...	Running	Automatic	Local System
Auto Time Zone Updater	Automaticall...		Disabled	Local Service

Step 3 - Enter this command in Ubuntu System to check weather the logs are Forwarding.



```
^X^C177 packets captured
189 packets received by filter
5 packets dropped by kernel

ubuntu@ubuntu1604:~$ sudo tcpdump -i ens33 | grep -i "10.10.10.13"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
04:53:28.999370 IP 10.10.10.13.mdns > 251.0.0.224.in-addr.arpa.mdns: 0 A (QM)? u
buntu1604.local. (34)
04:53:29.000085 IP 10.10.10.13.mdns > 251.0.0.224.in-addr.arpa.mdns: 0 AAAA (QM)
? ubuntu1604.local. (34)
04:53:29.993078 IP 10.10.10.1.domain > 10.10.10.16.50811: 3637* 1/0/0 PTR 10.10.
10.13. (67)
04:53:30.012727 IP 10.10.10.13.mdns > 251.0.0.224.in-addr.arpa.mdns: 0 A (QM)? u
buntu1604.local. (34)
04:53:30.013201 IP 10.10.10.13.mdns > 251.0.0.224.in-addr.arpa.mdns: 0 AAAA (QM)
? ubuntu1604.local. (34)
04:53:32.348613 IP 10.10.10.13.netbios-ns > 10.10.10.255.netbios-ns: UDP, length
 50
04:53:32.349331 IP 10.10.10.13.mdns > 251.0.0.224.in-addr.arpa.mdns: 0 A (QM)? u
buntu1604.local. (34)
04:53:32.350116 IP 10.10.10.13.mdns > 251.0.0.224.in-addr.arpa.mdns: 0 AAAA (QM)
? ubuntu1604.local. (34)
04:53:32.350833 IP 10.10.10.13.51799 > 224.0.0.252.hostmon: UDP, length 28
```

Go to Arcsight Console Home Page.In Navigator choose Connector.Find the Connector,right-click and choose start active channel to see logs.



ArcSight Console 7.4.0.2675.0 [esm7:shantanu.ast] Instant-on license. Expiration date: 10.10.10.15

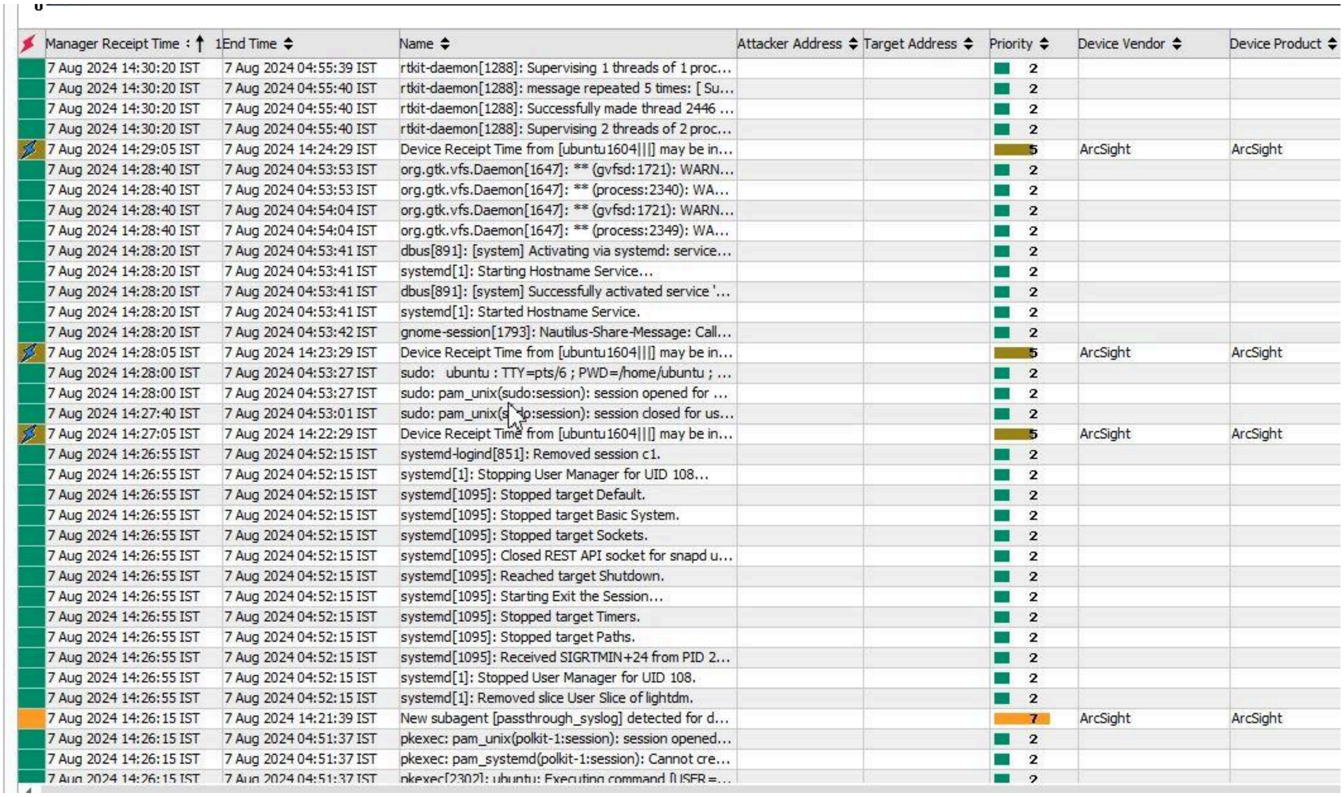
- Connectors
  - Shared
    - All Connectors
      - Abad
      - ArcSight Administration
      - Australia
      - california
      - Dubai_syslog
      - Korea
      - mahrashtra
      - Maxico
      - Nagar_Project
        - Syslog_Project(running)
      - nashik
      - phaltan_syslog
      - Pune
      - pune
      - Raigad
      - Seoul_syslog
      - Site Connectors
      - SN
      - Snort_Dubai
      - TEST_MH
      - tokyou
      - USA
      - Unassigned

Active Channel:

Start Time: 6 Aug 2024 14:30:37 IST
End Time: 7 Aug 2024 14:30:37 IST
Filter Agent ID = "Syslog_Project"
Inline Filter: No Filter
Verified Rules: No Rule

Total Events: 45
Very High: 0
High: 3
Medium: 3
Low: 7
Very Low: 32

Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:39 IST	rtkit-daemon[1288]: Supervising 1 threads of 1 proc…			2		
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:40 IST	rtkit-daemon[1288]: message repeated 5 times: [Su…			2		
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:40 IST	rtkit-daemon[1288]: Successfully made thread 2446 …			2		
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:40 IST	rtkit-daemon[1288]: Supervising 2 threads of 2 proc…			2		
7 Aug 2024 14:29:05 IST	7 Aug 2024 14:24:29 IST	Device Receipt Time from [ubuntu1604|||] may be in…			5	ArcSight	ArcSight
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:53:53 IST	org.gtk.vfs.Daemon[1647]: ** (gvfsd:1721): WARN…			2		
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:53:53 IST	org.gtk.vfs.Daemon[1647]: ** (process:2340): WA…			2		
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:54:04 IST	org.gtk.vfs.Daemon[1647]: ** (gvfsd:1721): WARN…			2		
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:54:04 IST	org.gtk.vfs.Daemon[1647]: ** (process:2349): WA…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	dbus[891]: [system] Activating via systemd: service…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	systemd[1]: Starting Hostname Service…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	dbus[891]: [system] Successfully activated service '…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	systemd[1]: Started Hostname Service.			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:42 IST	gnome-session[1793]: Nautilus-Share-Message: Call…			2		
7 Aug 2024 14:28:05 IST	7 Aug 2024 14:23:29 IST	Device Receipt Time from [ubuntu1604|||] may be in…			5	ArcSight	ArcSight
7 Aug 2024 14:28:00 IST	7 Aug 2024 04:53:27 IST	sudo: ubuntu : TTY=pts/6 ; PWD=/home/ubuntu ; …			2		
7 Aug 2024 14:28:00 IST	7 Aug 2024 04:53:27 IST	sudo: pam_unix(sudo:session): session opened for …			2		
7 Aug 2024 14:27:40 IST	7 Aug 2024 04:53:01 IST	sudo: pam_unix(s do:session): session closed for us…			2		
7 Aug 2024 14:27:05 IST	7 Aug 2024 14:22:29 IST	Device Receipt Time from [ubuntu1604|||] may be in…			5	ArcSight	ArcSight
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd-logind[851]: Removed session c1.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1]: Stopping User Manager for UID 108…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Default.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Basic System.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Sockets.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Closed REST API socket for snapd u…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Reached target Shutdown.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Starting Exit the Session…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Timers.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Paths.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Received SIGRTMIN+24 from PID 2…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1]: Stopped User Manager for UID 108.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1]: Removed slice User Slice of lightdm.			2		
7 Aug 2024 14:26:15 IST	7 Aug 2024 14:21:39 IST	New subagent [passthrough_syslog] detected for d…			7	ArcSight	ArcSight
7 Aug 2024 14:26:15 IST	7 Aug 2024 04:51:37 IST	pkexec: pam_unix(polkit-1:session): session opened…			2		
7 Aug 2024 14:26:15 IST	7 Aug 2024 04:51:37 IST	pkexec: pam_systemd(polkit-1:session): Cannot cre…			2		
7 Aug 2024 14:26:15 IST	7 Aug 2024 04:51:37 IST	pkexec[2302]: ubuntu: Executing command [USER=…			2		



Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:39 IST	rtkit-daemon[1288]: Supervising 1 threads of 1 proc…			2		
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:40 IST	rtkit-daemon[1288]: message repeated 5 times: [Su…			2		
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:40 IST	rtkit-daemon[1288]: Successfully made thread 2446 …			2		
7 Aug 2024 14:30:20 IST	7 Aug 2024 04:55:40 IST	rtkit-daemon[1288]: Supervising 2 threads of 2 proc…			2		
7 Aug 2024 14:29:05 IST	7 Aug 2024 14:24:29 IST	Device Receipt Time from [ubuntu1604|||] may be in…			5	ArcSight	ArcSight
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:53:53 IST	org.gtk.vfs.Daemon[1647]: ** (gvfsd:1721): WARN…			2		
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:53:53 IST	org.gtk.vfs.Daemon[1647]: ** (process:2340): WA…			2		
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:54:04 IST	org.gtk.vfs.Daemon[1647]: ** (gvfsd:1721): WARN…			2		
7 Aug 2024 14:28:40 IST	7 Aug 2024 04:54:04 IST	org.gtk.vfs.Daemon[1647]: ** (process:2349): WA…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	dbus[891]: [system] Activating via systemd: service…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	systemd[1]: Starting Hostname Service…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	dbus[891]: [system] Successfully activated service '…			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:41 IST	systemd[1]: Started Hostname Service.			2		
7 Aug 2024 14:28:20 IST	7 Aug 2024 04:53:42 IST	gnome-session[1793]: Nautilus-Share-Message: Call…			2		
7 Aug 2024 14:28:05 IST	7 Aug 2024 14:23:29 IST	Device Receipt Time from [ubuntu1604|||] may be in…			5	ArcSight	ArcSight
7 Aug 2024 14:28:00 IST	7 Aug 2024 04:53:27 IST	sudo: ubuntu : TTY=pts/6 ; PWD=/home/ubuntu ; …			2		
7 Aug 2024 14:28:00 IST	7 Aug 2024 04:53:27 IST	sudo: pam_unix(sudo:session): session opened for …			2		
7 Aug 2024 14:27:40 IST	7 Aug 2024 04:53:01 IST	sudo: pam_unix(s do:session): session closed for us…			2		
7 Aug 2024 14:27:05 IST	7 Aug 2024 14:22:29 IST	Device Receipt Time from [ubuntu1604|||] may be in…			5	ArcSight	ArcSight
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd-logind[851]: Removed session c1.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1]: Stopping User Manager for UID 108…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Default.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Basic System.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Sockets.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Closed REST API socket for snapd u…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Reached target Shutdown.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Starting Exit the Session…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Timers.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Stopped target Paths.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1095]: Received SIGRTMIN+24 from PID 2…			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1]: Stopped User Manager for UID 108.			2		
7 Aug 2024 14:26:55 IST	7 Aug 2024 04:52:15 IST	systemd[1]: Removed slice User Slice of lightdm.			2		
7 Aug 2024 14:26:15 IST	7 Aug 2024 14:21:39 IST	New subagent [passthrough_syslog] detected for d…			7	ArcSight	ArcSight
7 Aug 2024 14:26:15 IST	7 Aug 2024 04:51:37 IST	pkexec: pam_unix(polkit-1:session): session opened…			2		
7 Aug 2024 14:26:15 IST	7 Aug 2024 04:51:37 IST	pkexec: pam_systemd(polkit-1:session): Cannot cre…			2		
7 Aug 2024 14:26:15 IST	7 Aug 2024 04:51:37 IST	pkexec[2302]: ubuntu: Executing command [USER=…			2		

Conclusion

We now have a working Arcsight Console environment using Smart Connector, that will allow us to monitor and create logs within our virtual machines. Setting up these tools from scratch helps you get familiar with both of these tools.