ARCSIGHT
SIEM ADMINISTRATOR AND ANALYST

#	Topic
1	Training Process
2	Introduction to SIEM and Arcsight Tool. 2.1 SIEM Requirement 2.2 History of ArcSight 2.3 Comparison of various SIEM tools with ArcSight, Pros and Cons
3	ArcSight Architecture 3.1 Brief about various components of Arcsight 3.2 ArcSight Event scheme and life cycle 3.3 Deployment of ArcSight architecture, linear, and dual destination 3.4 Understanding of failover destination setup for ESM and logger 3.5 Support matrix of ArcSight components Installation 3.6 Understanding of retention period of logger and ESM 3.7 Understanding of different ports and protocol being used across all Arcsight components 3.8 Understanding of recommended place of deployment of each components and traffic encryption mechanism.
4	Introduction to SIEM and ArcSight Tool 4.1 SIEM Requerment 4.2 History Of ArcSight 4.3 Deployment of ArcSight Architecture, liner and dual destination 4.4 Understanding of failover destination set up for ESM and logger 4.5 Support matrix of ArcSight components installation 4.6 Understanding of retention period of logger and ESM 4.7 Understanding of different ports and protocol being used across all ArcSight components 4.8 Understanding of recommended place of deployment of each componenets and traffic encryption mechanisism
5	Understanding of licensing model of ArcSight components with real time example
6	Installation Of ArcSight Smart connector 6.1 Understanding of various types of ArcSight Connectors 6.2 Difference between smart connector and flex connectors and its requirement 6.3 Details understanding of connector of connector destination setting 6.4 Installation of windows and syslog connectors on the lab 6.5 Details understanding of integration of various devices with ArcSight 6.6 Integration of windows and syslog devices on the web 6.7 Understanding of various types of syslog and integration mechanism 6.8 Configuring the destination settings, on the connectors 6.9 Configuring destination settings on the connectors 6.10 Up gradation of connectors 6.11 Increasing JVM and Connectors log analysis for troubleshooting perspective 6.12 Troubleshooting of connectors Issues, and Identify and troubleshoot in case device is not sending the logs to ArcSight
7	Installation of ArcSight smart connector Arcsight ESM 7.1 ArcSight ESM Overview 7.2 Searching events on the ESM Using the channels 7.3 Creating Field sets

8	Reports 8.1 Creating Query 8.2 Creating reports on trends, downloading reports
9	Correlation Rules 9.1 Understanding the various types of rules 9.2 Creating rules 9.3 Suppression of rules to avoid multiple firing 9.4 Investigation of incidents and identifying true positive and false positive 9.5 Finetuning of rules
10	Active List 10.1 Creating event based and field based active list 10.2 Understanding and creating threat feed
11	Dashboards 11.1 Understanding the use of dashboard 11.2 Understanding of various data moniter 11.3 Creating data monitors and dashboards 11.4 Analyzing the event from Dashboards
12	Other Resources Of ESM 12.1 Understanding and creating Query Viewers 12.2 User administration, and Privileges assignment 12.3 Creating notification and groups 12.4 Creating ArcSight Package, Importing and exporting packages 12.5 Crest of the resources which are available on navigator panel
13	Logger 13.1 Overview of logger 13.2 Creating receivers and forwarders 13.3 Creating field sets 13.4 Searching and downloading the logs 13.5 Storage setting and retention period setup 13.6 Brief overview of the resources of logger
14	14.1 ArcSight Command Center 14.2 Overview of ArcSigght Command center 14.3 ArcSight ESM Peering, Backup, and archival settings
15	Understanding of ArcSight UBA package resources
16	Tripwire VA Tool 16.1 Overview and brief understanding of the tools 16.2 Understanding the integration with Arcsight

Module – 1

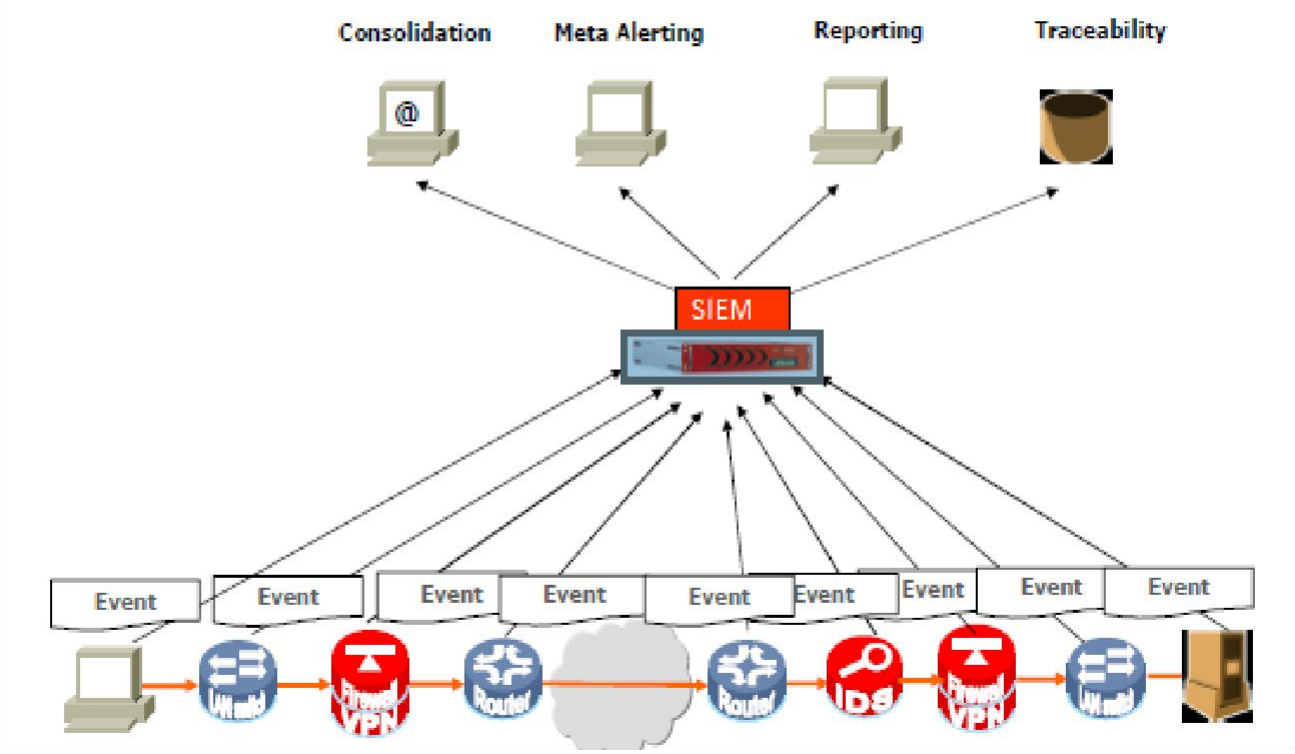
- Arcsight Architecture
- Connector Installation
- Devices integration

- What is SIEM and Why it is required
- Discuss what ArcSight ESM is and how it fits into a SOC
- Various components of Arcsight
- Discuss linear Architecture of Arcsight
- Discuss Dual destination Architecture of Arcsight
- Discuss pros and cons of both Architecture
- Arcsight Installation platforms
- License model, port protocols used
- Discuss about Arcsight Connector destination settings

What ArcSight ESM is and how it fits into a SOC :

- Security Operations Center
- SIEM Generations
    - Event, Alert, Incident
    - SIM+SEM = SIEM
    - SIEM definition
- SIEM Tools
    - ArcSight, Splunk, Logrhythm, Qradar etc..

Modern SOC :

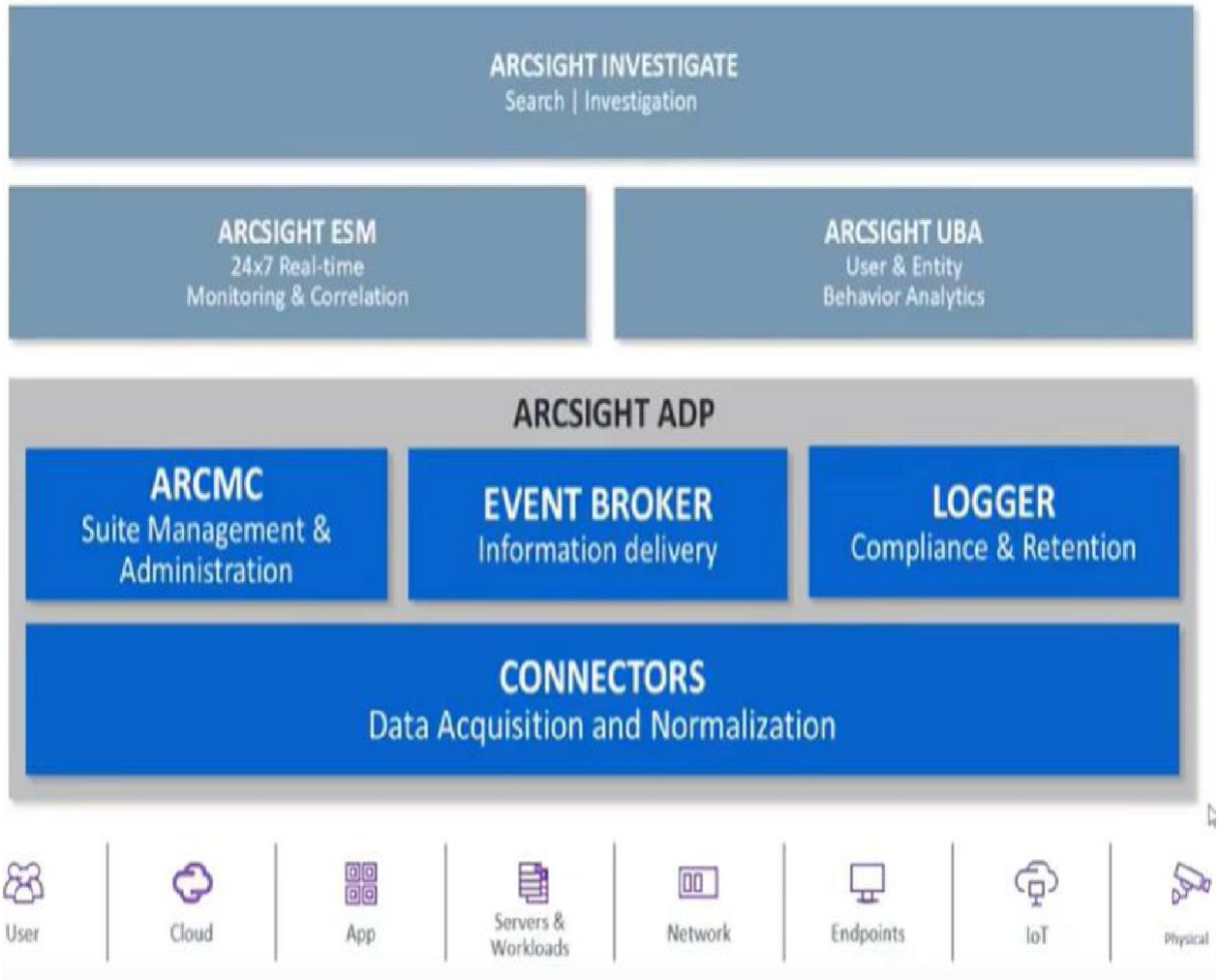


Security Monitoring :

ArcSight History :

- -> ArcSight - 2000
  - ->HP - 2010
    - -> Microfocus - 2017

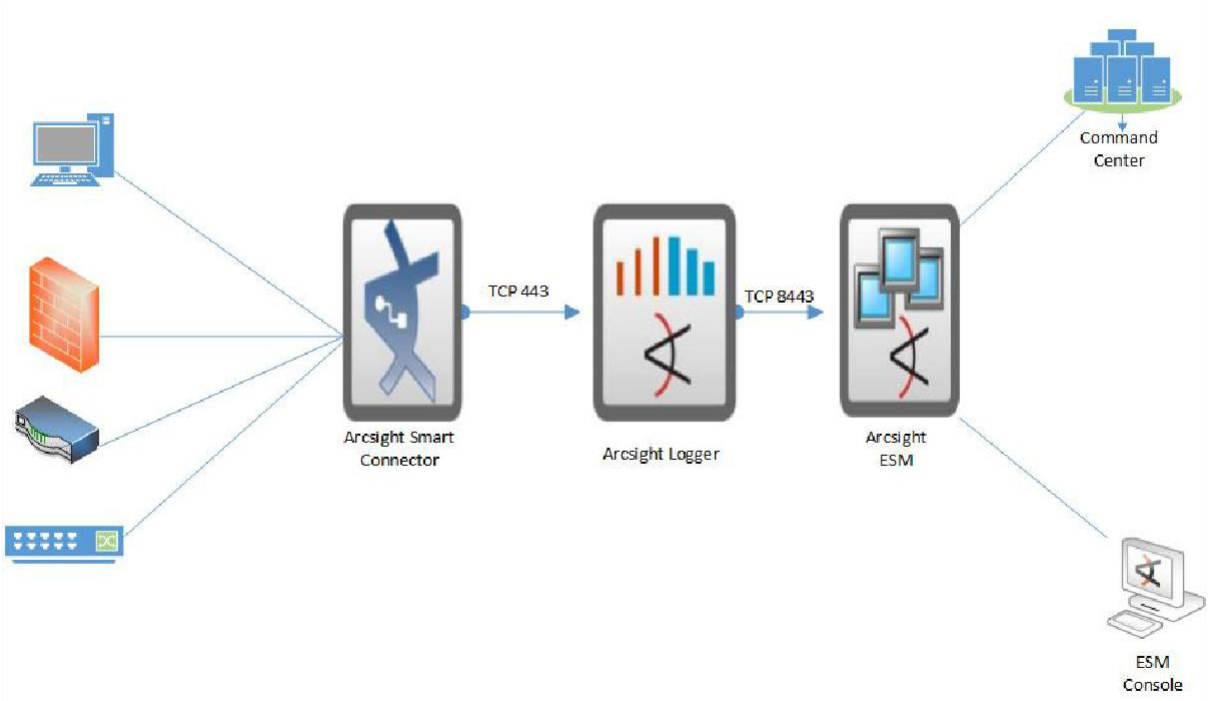
Arcsight Portfolio :



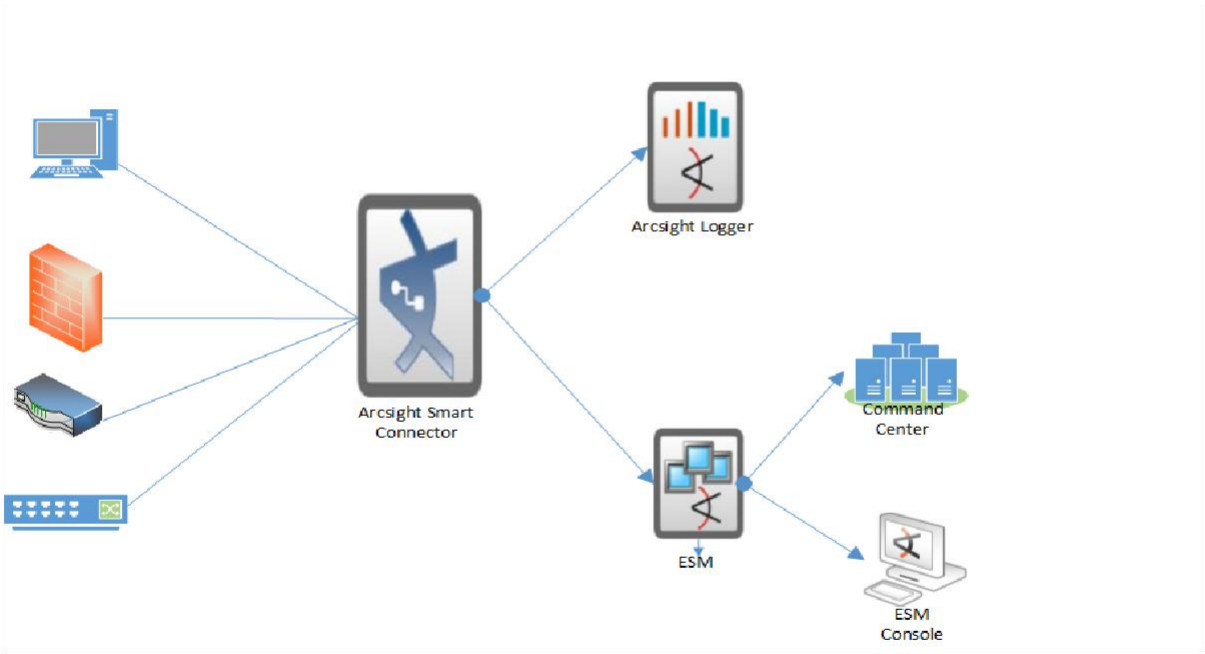
Arcsight Portfolio :

- **ArcSight Data Platform**
  - **Connector**
    - **Collect, Parse, Filter, Aggregate, Normalize and Categorize logs**
    - **CEF**
  - **Logger**
    - **Mainly used for long term storage.**
    - **Provides ultra-fast searching across the data.**
  - **Event Broker**
    - **This is an open architecture message bus platform of Arcsight built on apache kafka.**
    - **Ingests data from any source and sends it anywhere.**
  - **Arcsight Management Center**
    - **Administrate and monitor ArcSight managed nodes, such as Connector Appliances, Loggers, Connectors, other ArcMCs, and Event Broker.**

Arcsight Linear Architecture



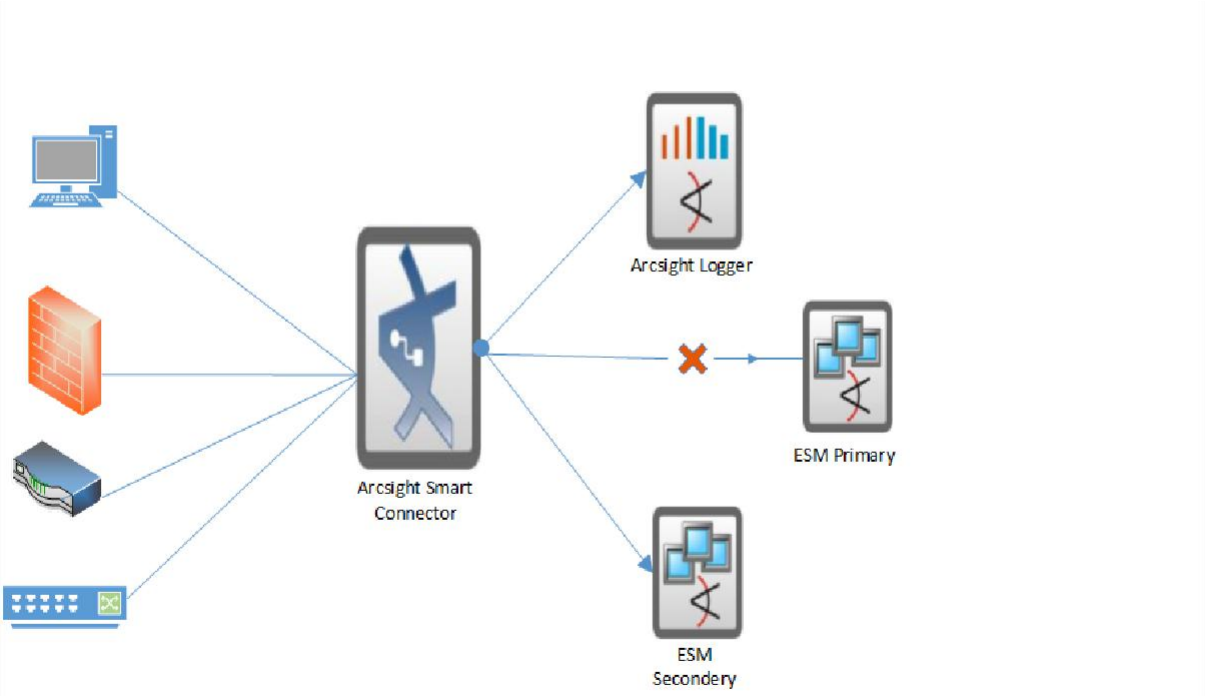
Arcsight Dual destination Architecture :



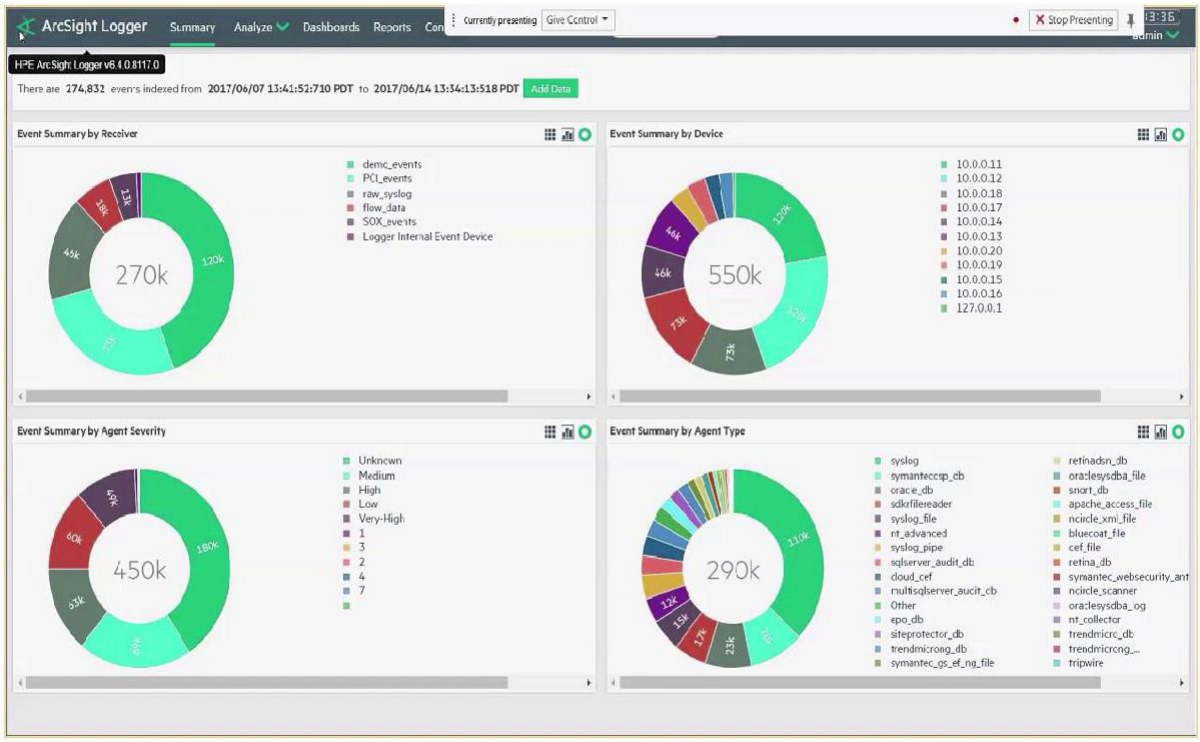
Connector Destinations – Multiple Destinations :

- SC can be configured to send copy of events to additional configured destinations
- Benefits
  - Allows development environment to work in parallel with production environment for testing
  - Provide a peer to peer high availability manager installation.
- One or more destination allowed.
- Configuration
  - Run ArcSight connector configuration wizard
  - Select "…add/remove/modify ArcSight Manager destinations"
  - Select "Add new destination" and provide other parameters for new destination.

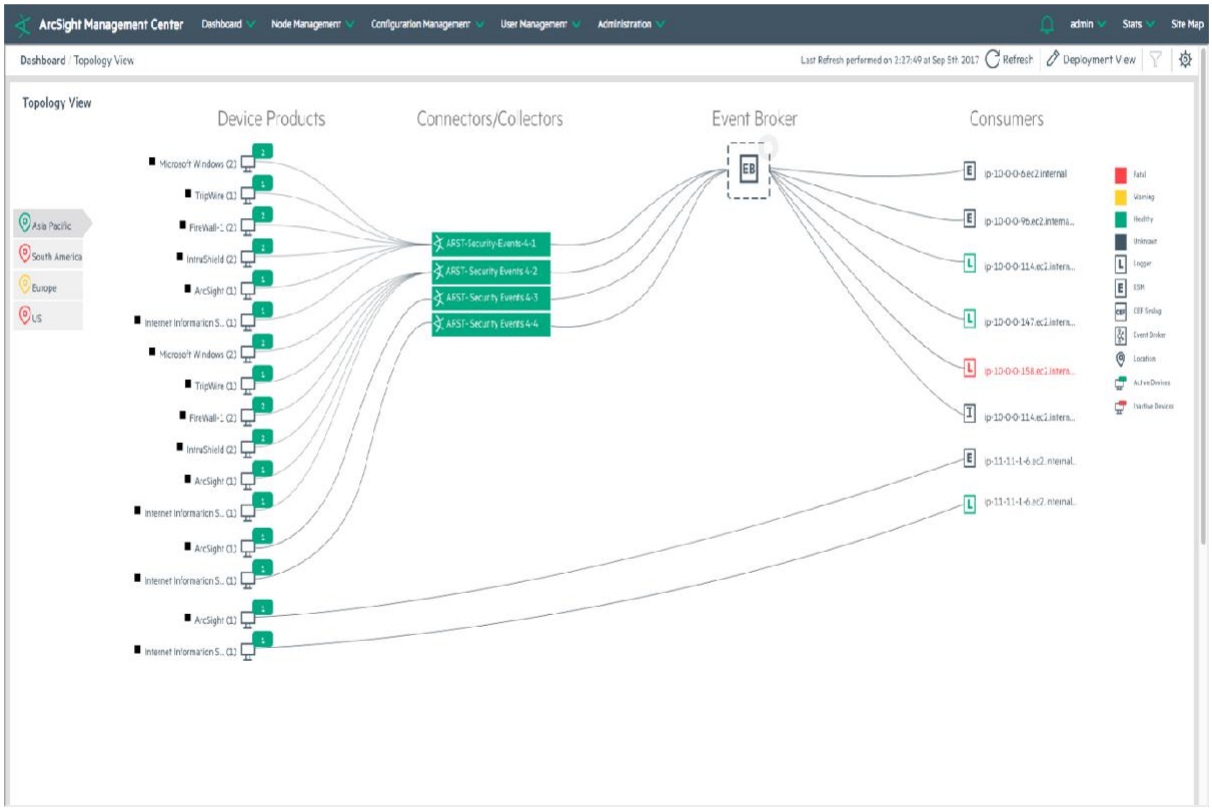
High Availability/Failover Architecture :



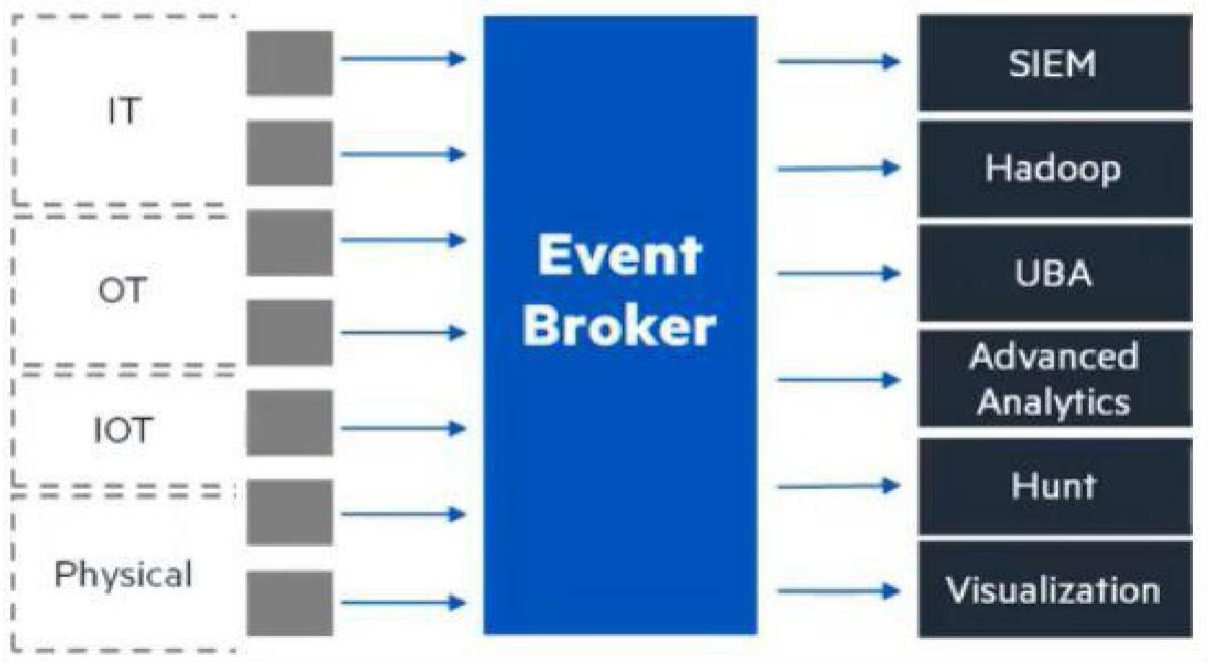
Arcsight Logger Web Interface :



ArcSight Management Center :



Event Broker :



List the problems ESM can solve :

- Log Retention
  - Storage groups
  - Flexible retention policies
- Correlation
  - Combine detection from multiple sources
  - Real-time correlation scenario
- Track Event Lifecycle
  - Phases of event life cycle

Real-time correlation scenario :

Log: %NICWIN-4-Security_538_Security: Security,rn=62822854 cid=0x00000002 eid=0x0000021a,Thu Oct 28 23:21:44 2010,538,Security,MyDomain/svc_altirisservice,Success Audit,host110,Logon/Logoff,,User Logoff: User Name: srini08 Domain: MyDomain Logon ID: (0x0,0xA4F93FB) Logon Type: 3

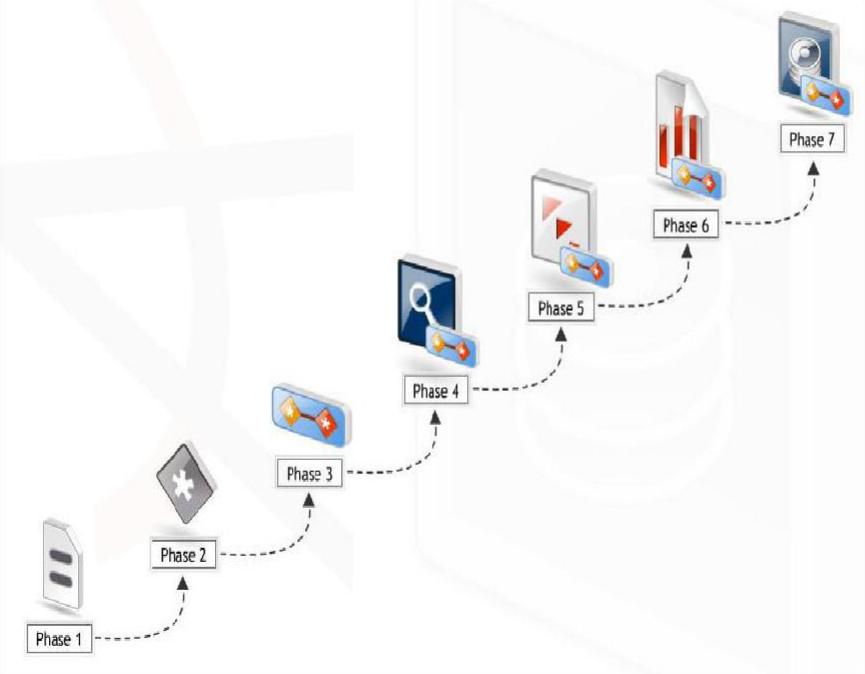
Alert: User tried to logon to the critical server during non-business hours

Agregation: 1count in 1 min

User Identification: **srini08**

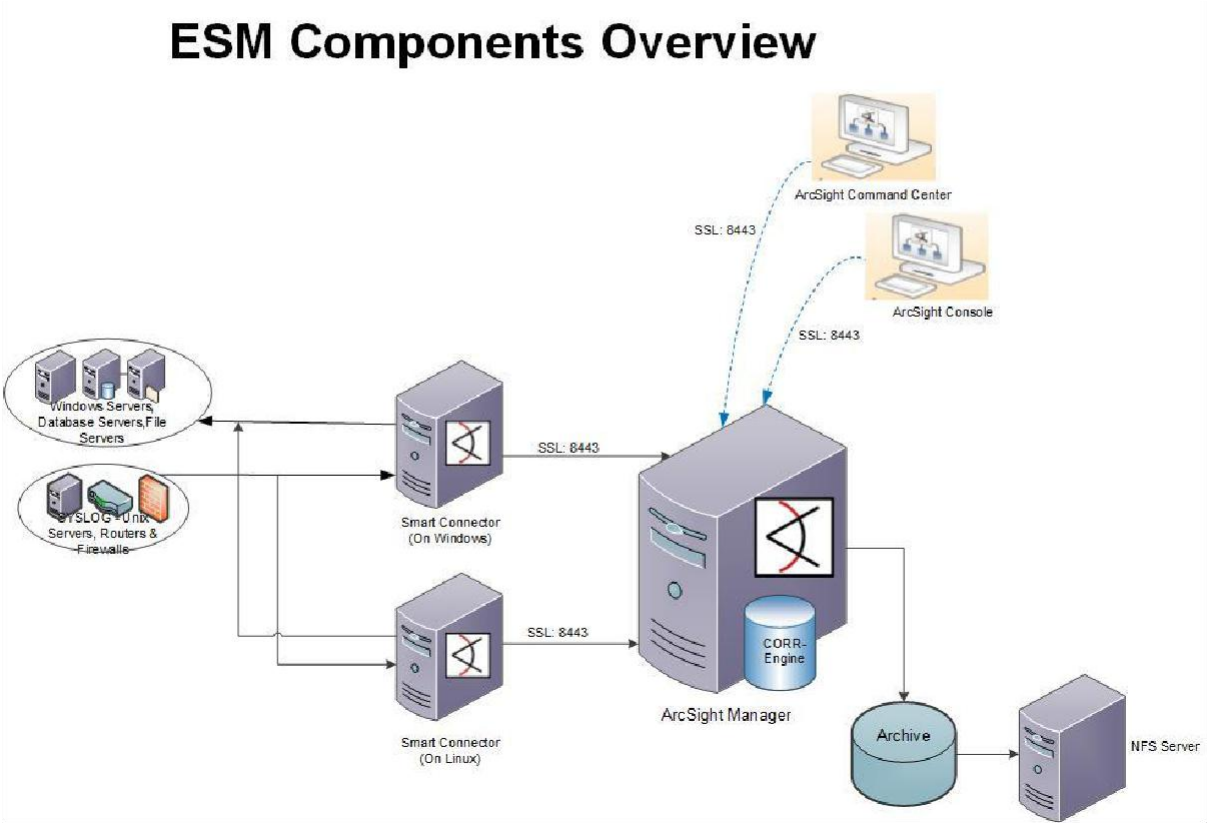
1. Type of Log: **logon information**
2. Date and Time: **Oct 28 23:21:44 IST**
3. Success and Failure: **Success**
4. Origination of event: **host110**
5. Name of affected System: **host110**

Phases of event life cycle :



- Phases of Event Lifecycle
    1. Data Collection and Event Processing
    2. Network Model Lookup and Priority Evaluation
    3. Correlation Evaluation
    4. Monitoring and Investigation
    5. Workflow
    6. Incident Analysis and Reporting
    7. Database Storage and Archive

Basic ArcSight Components :



- **ESM Architecture**
  - ESM Manager
  - CORR-Engine
  - Connectors
  - User Interfaces
- **ESM Manager**
  - Java based server
  - Writes normalized events into ESM database
  - Creates correlation events
  - Creates Audit and Monitor events

- CORR-Engine - Correlation Optimized Retention and Retrieval Engine
  - High performance storage engine (Postgres+mysql)
  - Optimized for
    - Faster log insertion rates
    - Faster query response times
    - Greater storage efficiency – 10x compression
    - Simpler administration and storage management

ArcSight Connectors :

- Basic Functions – Collect, Normalize and Forward/Cache.
- SmartConnectors – 300+ Arcsight created and supported
- FlexConnectors – Custom Connectors, user created and supported

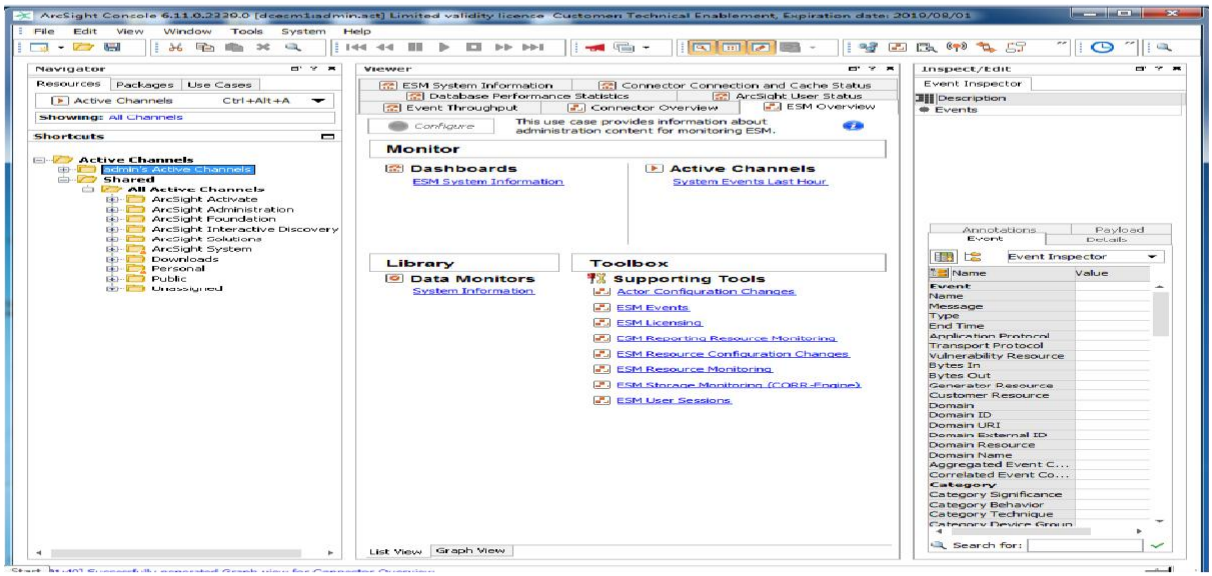
User Interfaces :

- ESM Console – Java based workstation thick console
  - Navigatior, Viewer, Inspect/Edit
  - Configure ESM content and resources

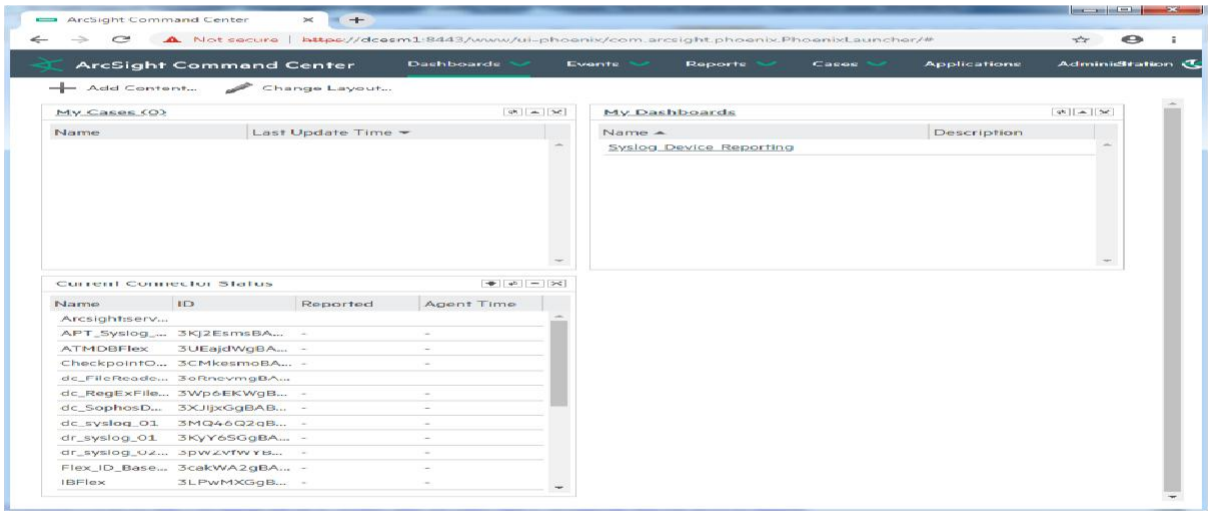
- Command Center – Secure Web based interface

  - Administrative functions for managing license, storage, archives, peer configuration, Content Sync etc.

Console :



Command Centre :



Lab Workshop

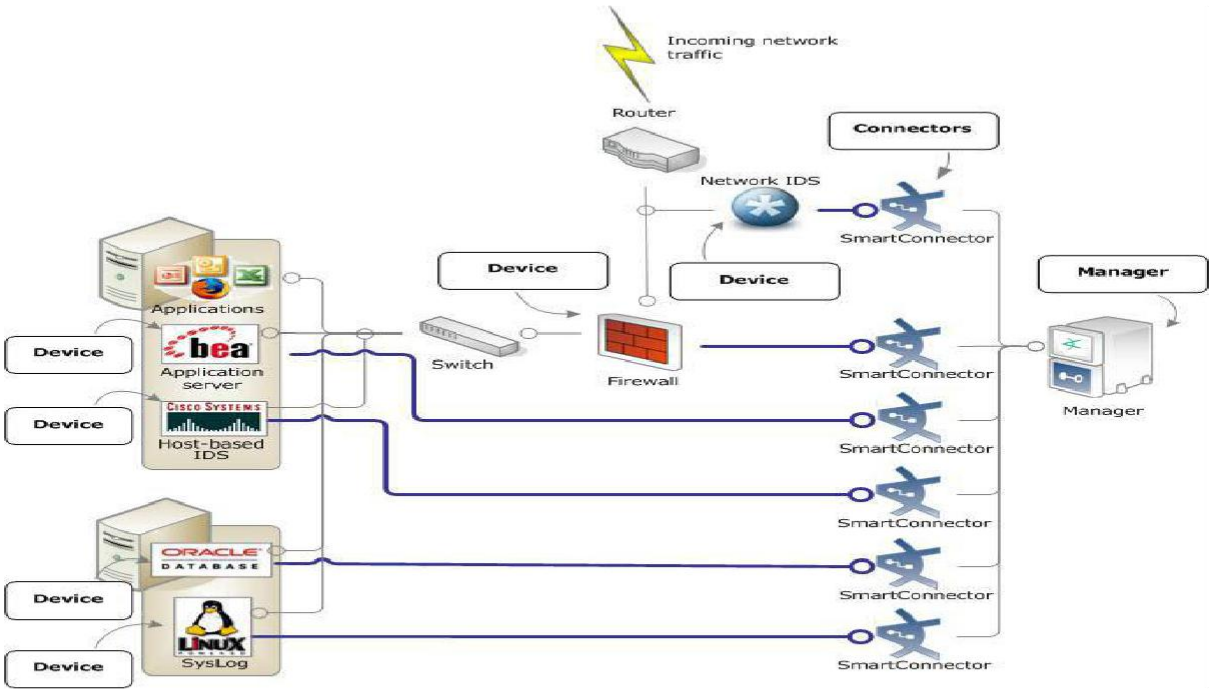
Module – 2

- Type of Connectors
- Connector Installation
- Devices integration

- Define the purpose of a connector
- Describe normalization
- Destination Settings like Caching, batching etc
- Type of Arcsight Connectors
- Discuss about Smart and Flex connectors
- Arcsight Connector installation
- Integration of devices
- Up-gradation of Connectors

What is Smart Connector :

- Smart Connectors is an standard connector released by Arcsight for supported devices, Its an application that collects raw events from security devices, processes them into ArcSight security events, and transports them to destination devices.



Normalization :

- Normalize means to conform to an accepted standard or norm
- Different logging format from each device has to be standardized
- Example Traffic Logs from different log sources
  - **Check Point:**
    - "14" "21Nov2016" "12:10:29" "eth-s1p4c0" "ip.of.firewall" "log" "accept“ "www-http" "192.0.2.0" "192.0.2.1" "tcp" "4" "1355" "" "" "" "" "" "" "" "" "“ "" "firewall" "len 68"
  - **Cisco Router:**
    - Nov 21 15:10:27: %SEC-6-IPACCESSLOGP: list 102 permitted tcp 192.0.2.0(1355) -> 192.0.2.1(80), 1 packet Cisco PIX: Nov 21 2016 12:10:28: %PIX-6-302001: Built inbound TCP connection 125891 for faddr 192.0.2.0/1355 gaddr192.0.2.1/80 laddr 10.0.111.22/80
    - SmartConnectors use a parser to normalize the event

Date	Time	Event_Name	Src_IP	Src_Port	Tgt_IP	Tgt_Port	Device_Type
21-Nov-16	12:10:29	Accept	192.0.2.0	1355	192.0.2.1	80	CheckPoint
21-Nov-16	12:10:27	List 102 permitted tcp	192.0.2.0	1355	192.0.2.1	80	Cisco Router

Smart Connectors Classification :

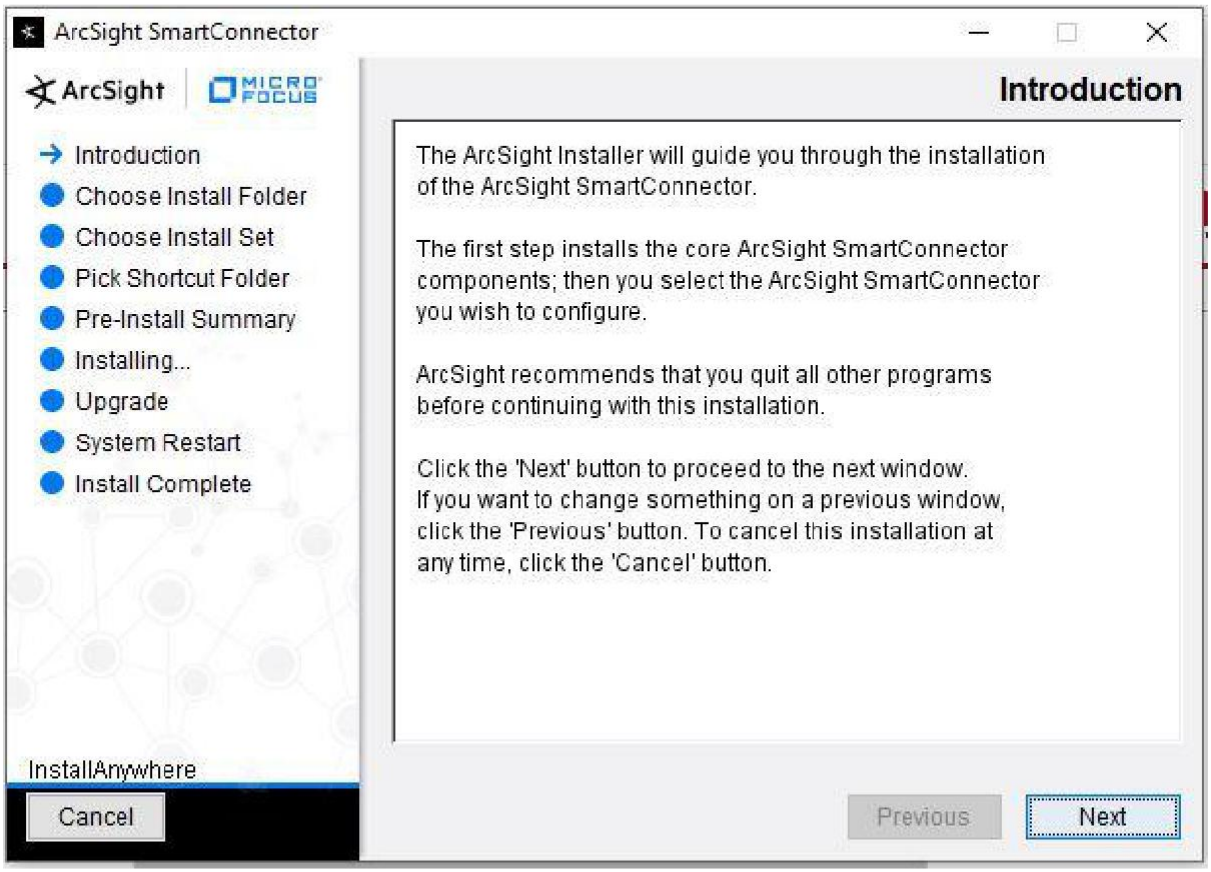
- By the Way of Log Retrieval
  - Push - Connector itself requests devices for their logs (ex: windows connector)
  - Pull - Devices themselves sends logs to connector server(ex: syslog connector)
- By Task
  - Event Log Connectors – Retrieve security log events from devices and applications
  - Scanner Connectors – Vulnerability data, asset import etc.
  - CounterACT connectors – Execute commands in the device to retrieve, modify or analyse its configuration.
- By Data Sources
  - Log Files or Folders of Log Files – Fixed delimited, REGEX
  - Database Reader(ODBC,JDBC) – Timebased, ID Based
  - Syslog – Listener port
  - SNMP – Listener “Trap” events
  - XML – Folder log file reader
  - API (Application Programming Interface) – Device or application specific API used to pull events

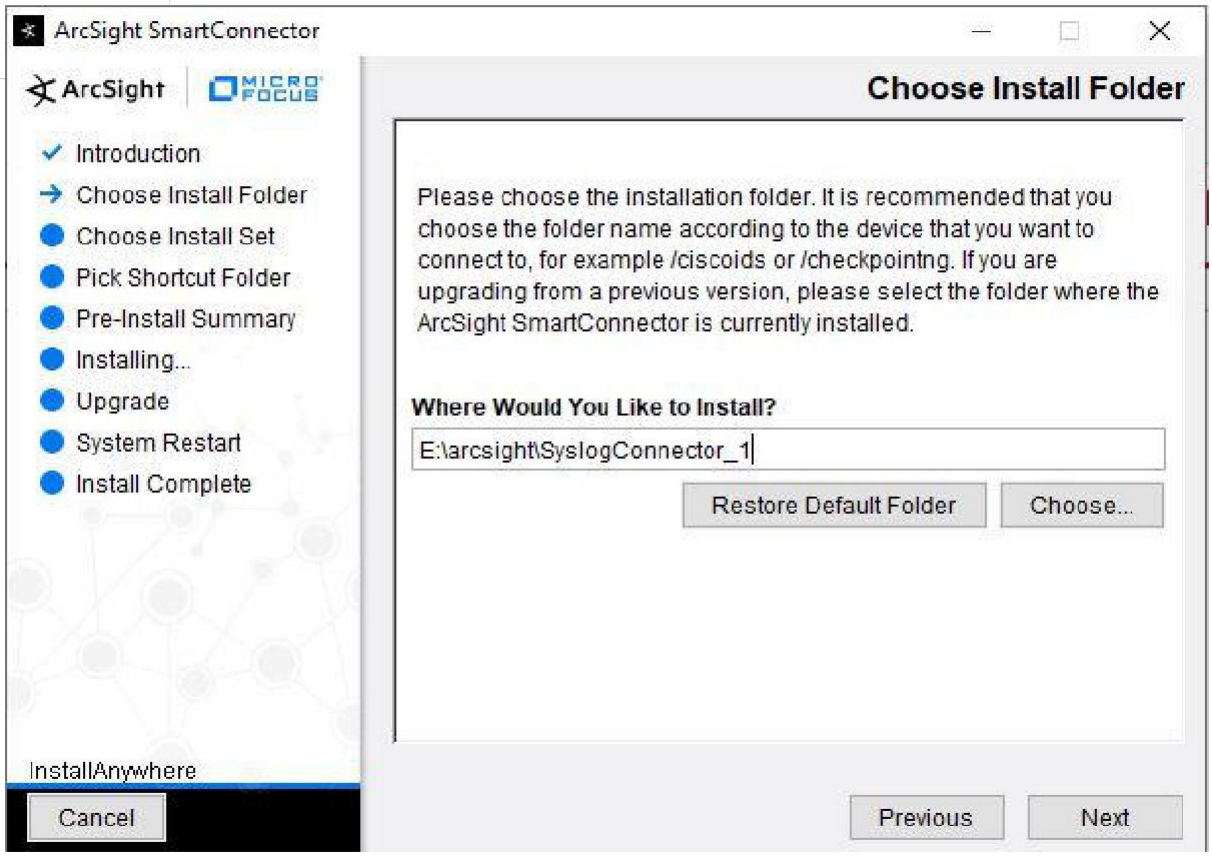
Installing Smart Connectors – Installation Check List:

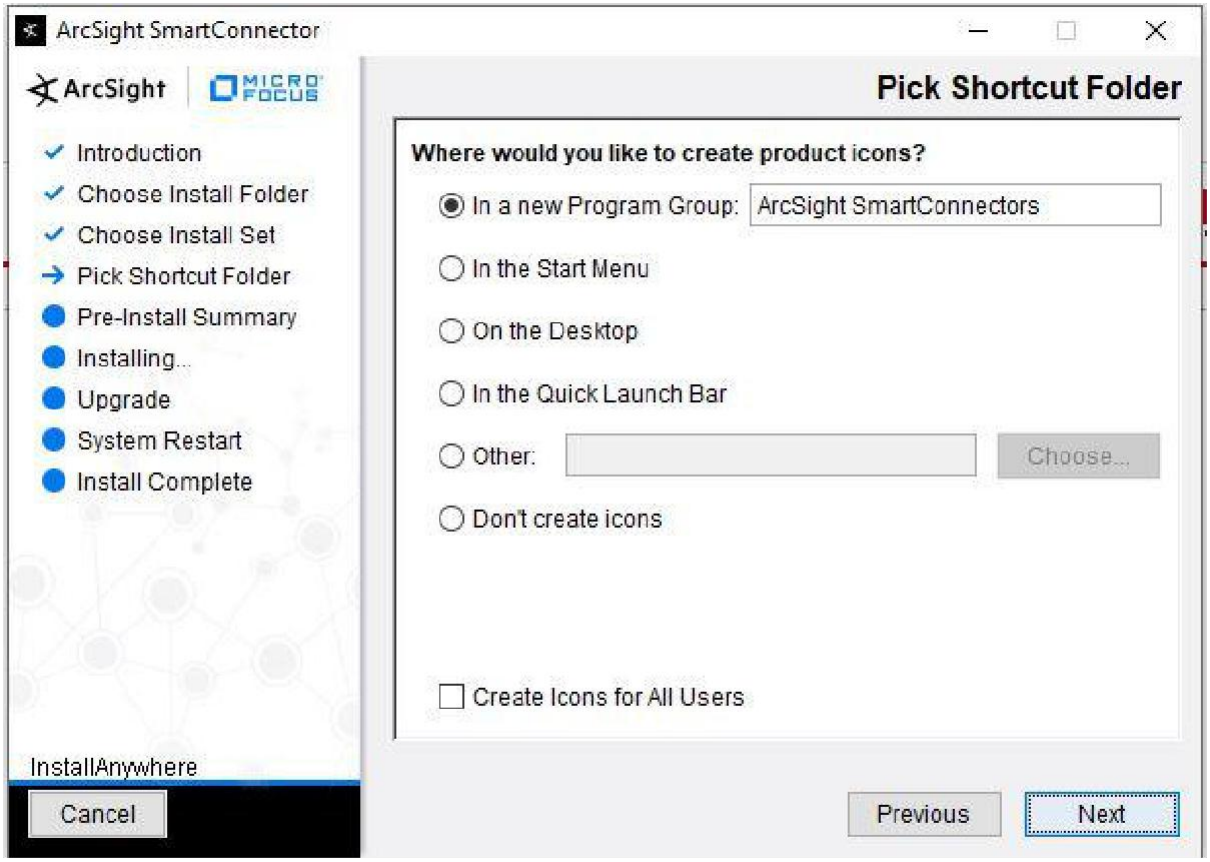
- Manager Hostname/IP address and port(default 8443) used
- ArcSight username/password having admin privilege.
- Connector type to install
- Required custom parameters – depends on connector type
- Connector Name – as it appears console
- Connector Location – Group folder in console
- Device Location and Comment – Not required but best practice
- Run connector as a service or not.

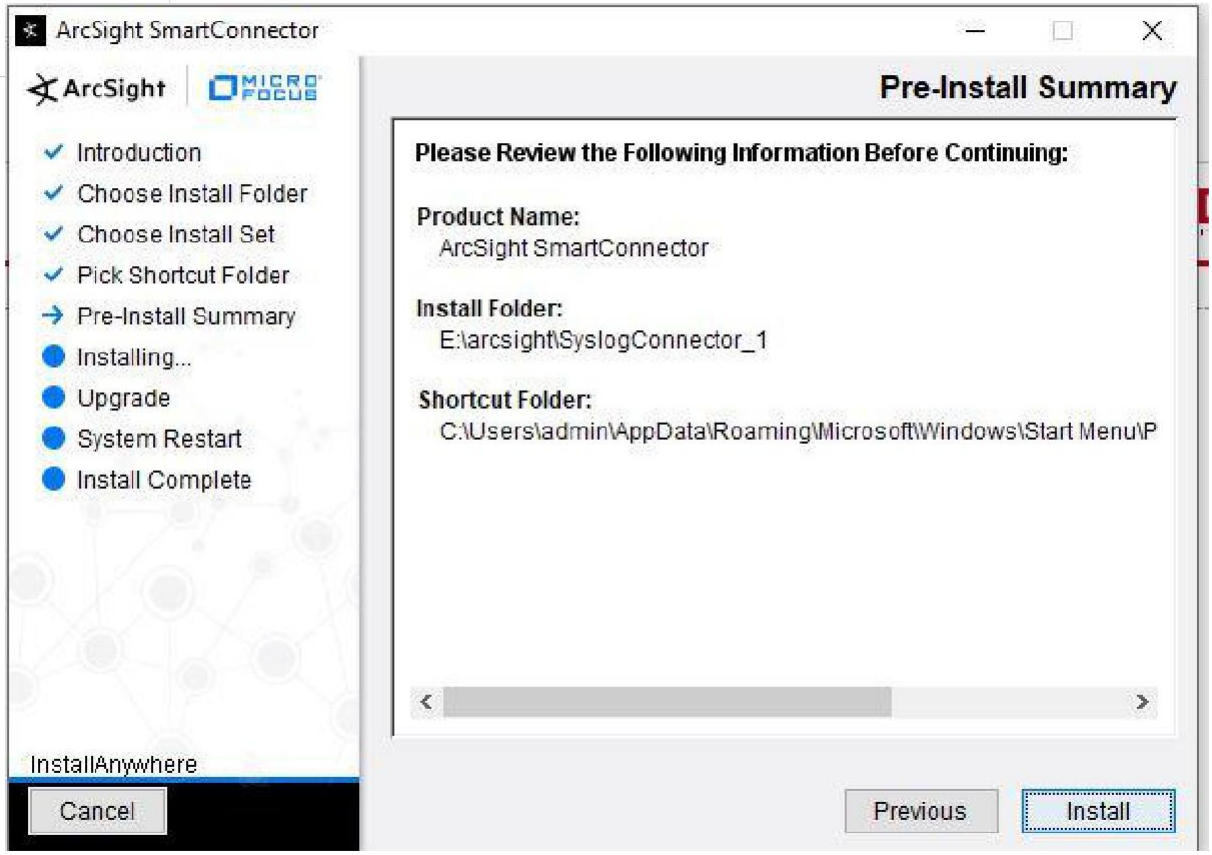
Smart Connector Installation:

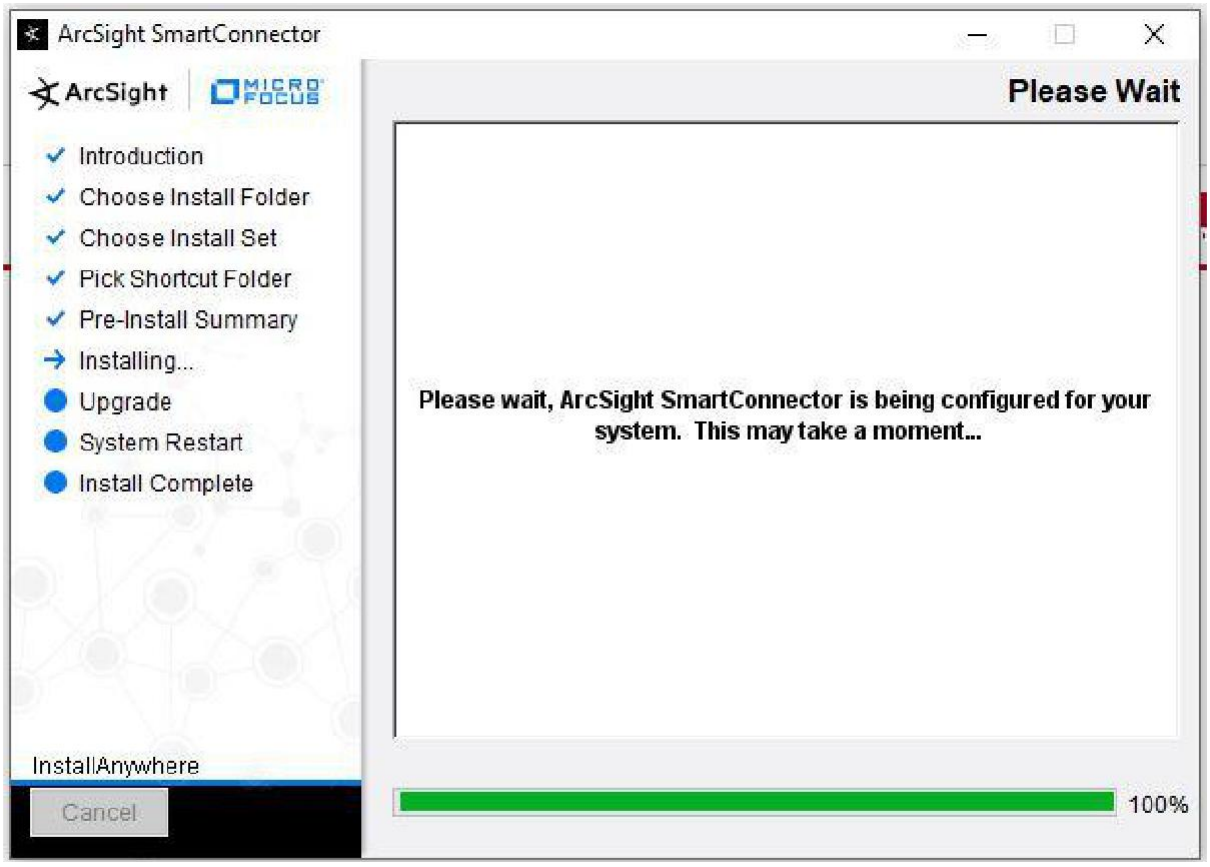
- Installation Process
  - GUI mode or CLI console mode.
  - Run self extracting binary.
    - Microsoft Windows.
    - Unix/Linux with X11.



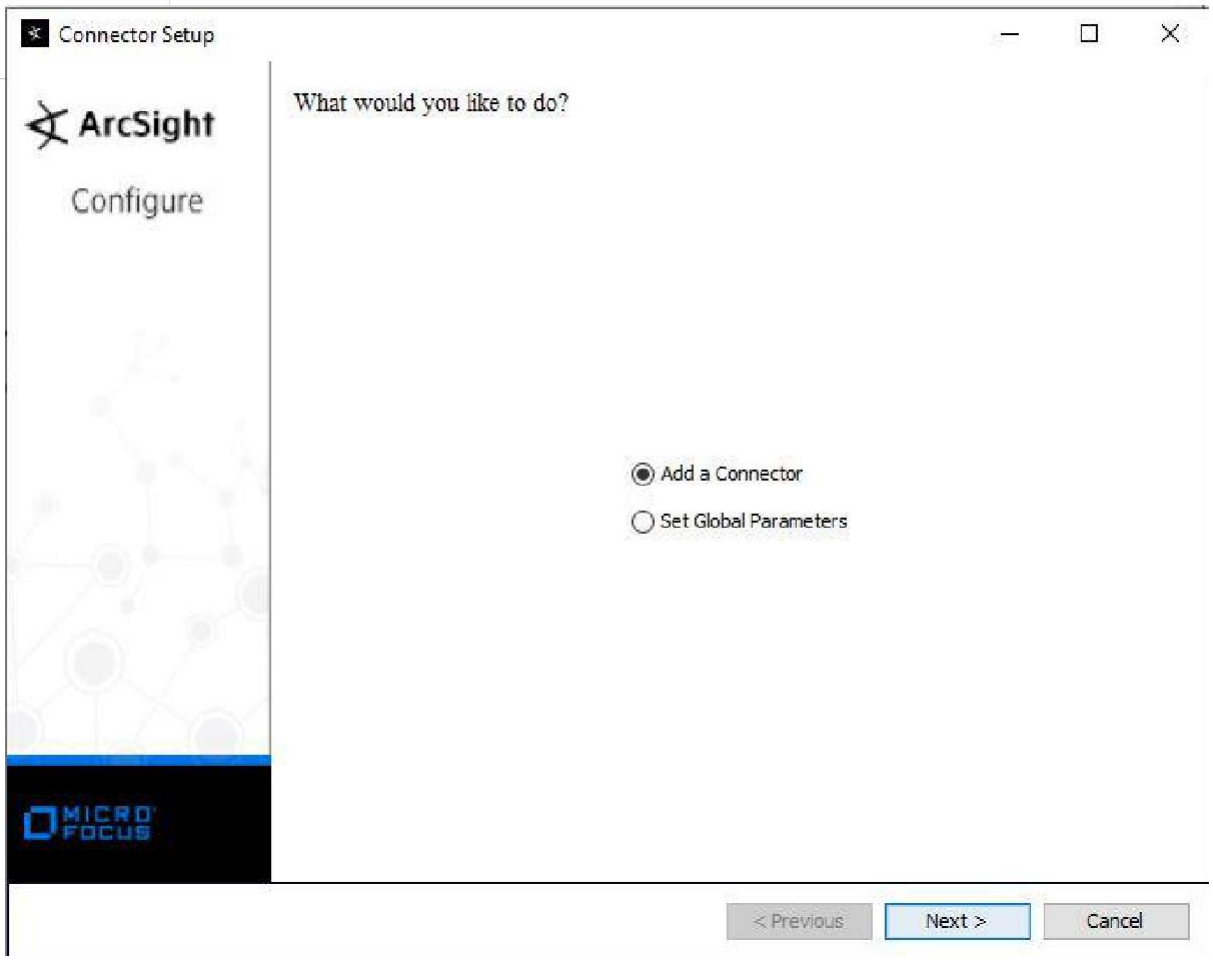

ArcSight SmartConnector
ArcSight
MICRO FOCUS
Introduction
Choose Install Folder
Choose Install Set
Pick Shortcut Folder
Pre-Install Summary
Installing...
Upgrade
System Restart
Install Complete
Choose Install Folder
Please choose the installation folder. It is recommended that you choose the folder name according to the device that you want to connect to, for example /ciscoids or /checkpointng. If you are upgrading from a previous version, please select the folder where the ArcSight SmartConnector is currently installed.
Where Would You Like to Install?
E:\arcsight\SyslogConnector_1
Restore Default Folder
Choose...
InstallAnywhere
Cancel
Previous
Next

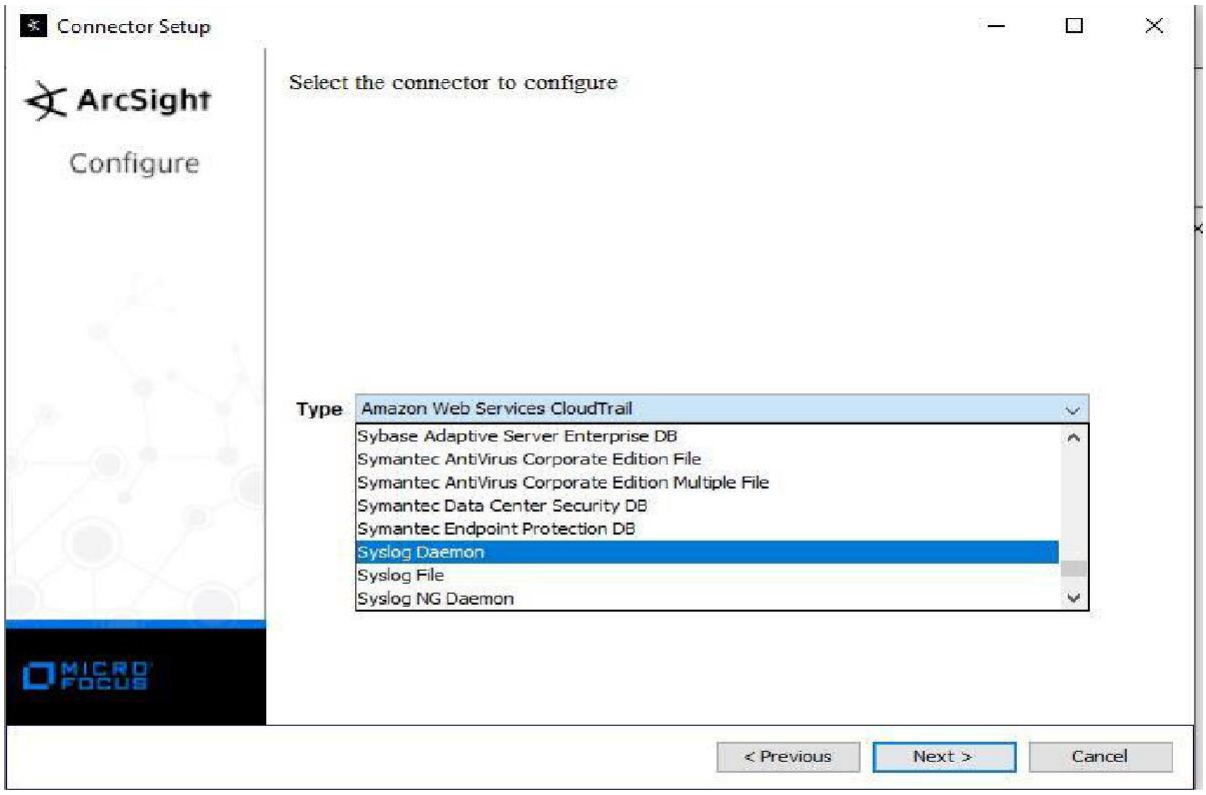

ArcSight SmartConnector
ArcSight
MICRO FOCUS
Introduction
Choose Install Folder
Choose Install Set
Pick Shortcut Folder
Pre-Install Summary
Installing...
Upgrade
System Restart
Install Complete
Pick Shortcut Folder
Where would you like to create product icons?
In a new Program Group:
ArcSight SmartConnectors
In the Start Menu
On the Desktop
In the Quick Launch Bar
Other:
Choose...
Don't create icons
Create Icons for All Users
InstallAnywhere
Cancel
Previous
Next

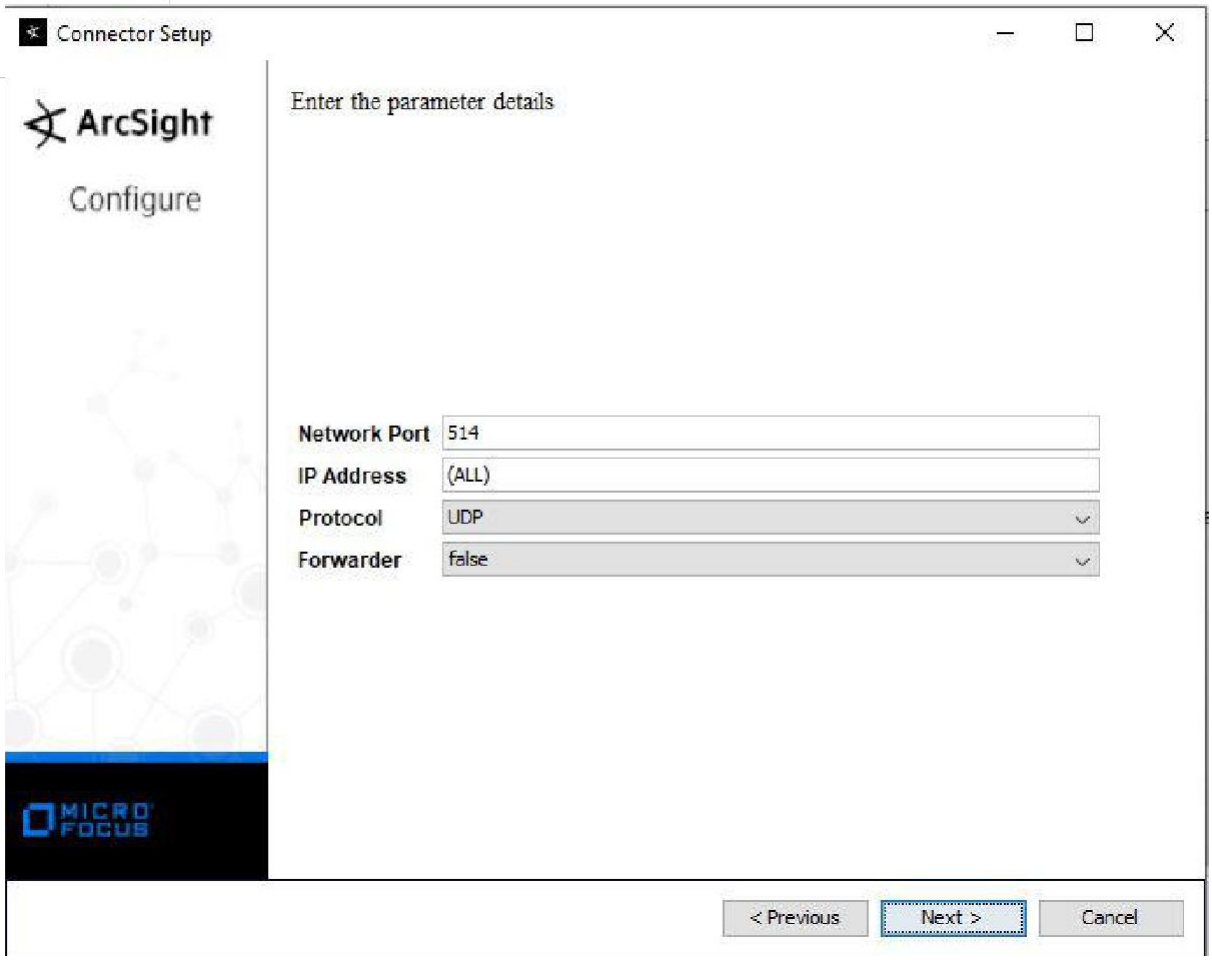


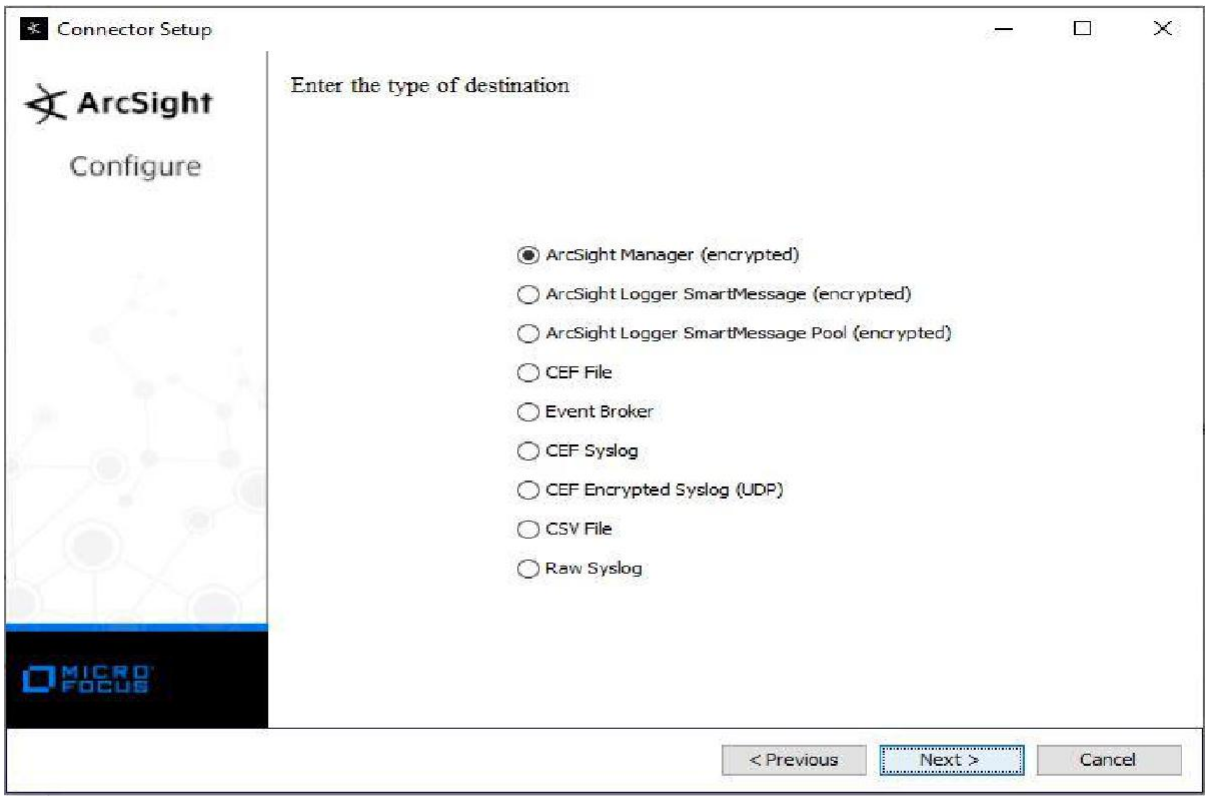


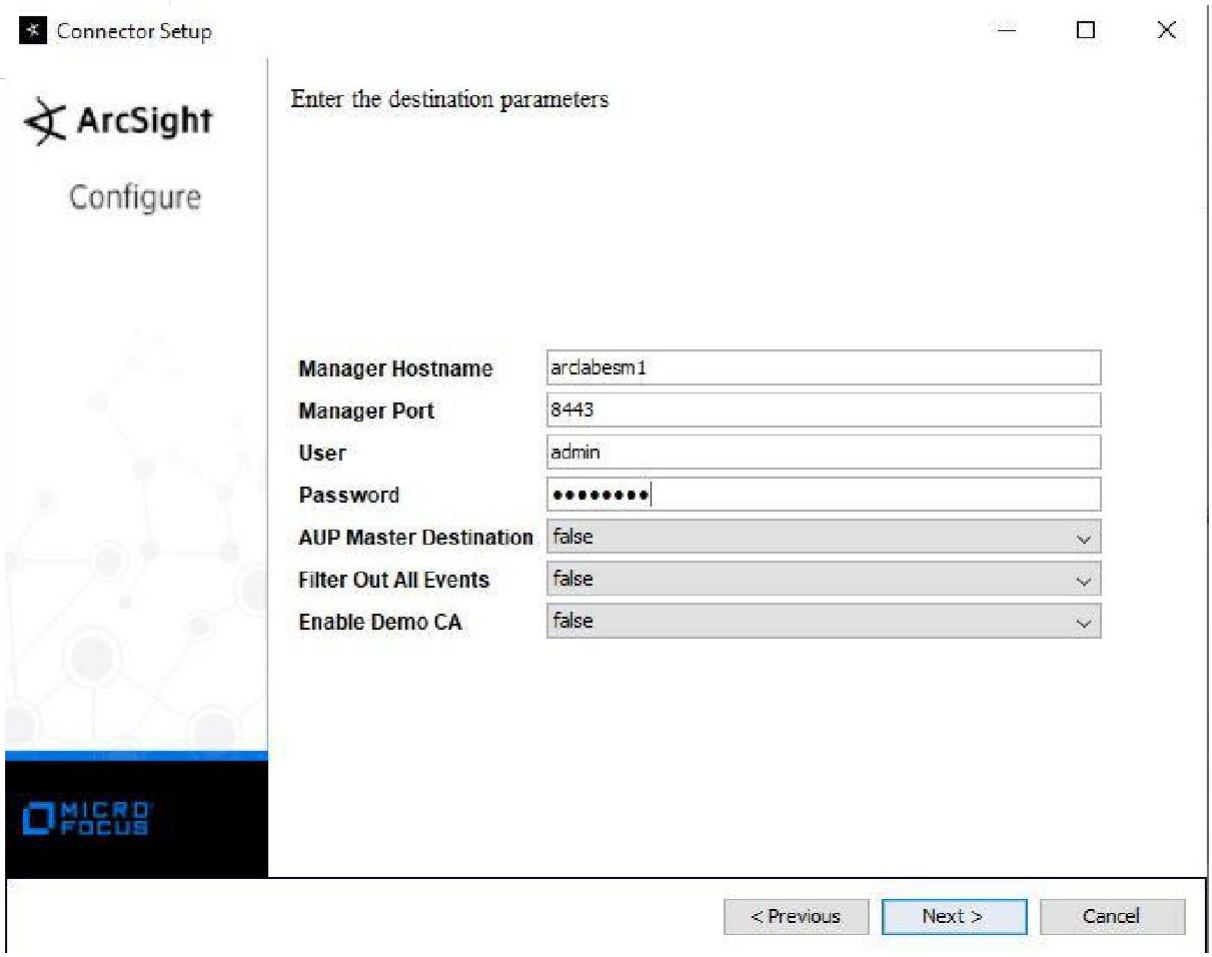
ARCSIGHT ADMIN & ANALYST WINDOWS USER

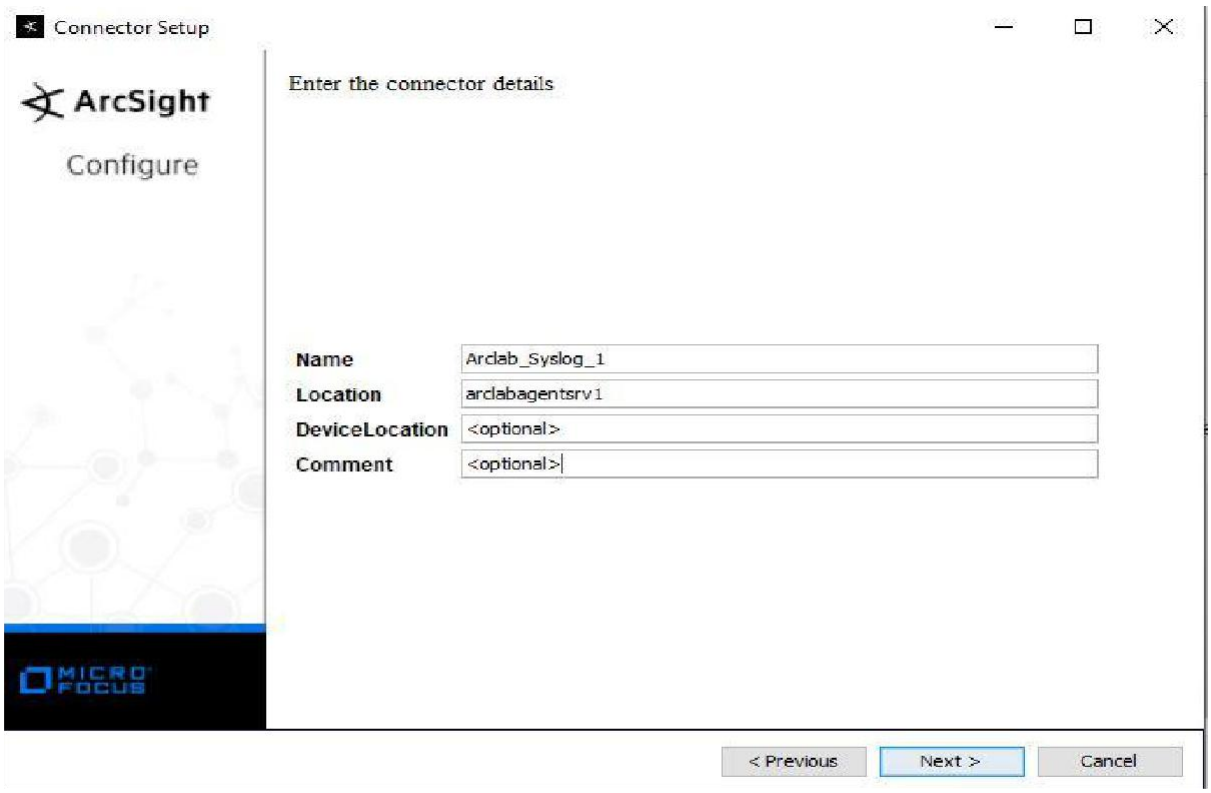

Connector Setup
ArcSight
Configure
What would you like to do?
Add a Connector
Set Global Parameters
MICRO FOCUS
< Previous
Next >
Cancel

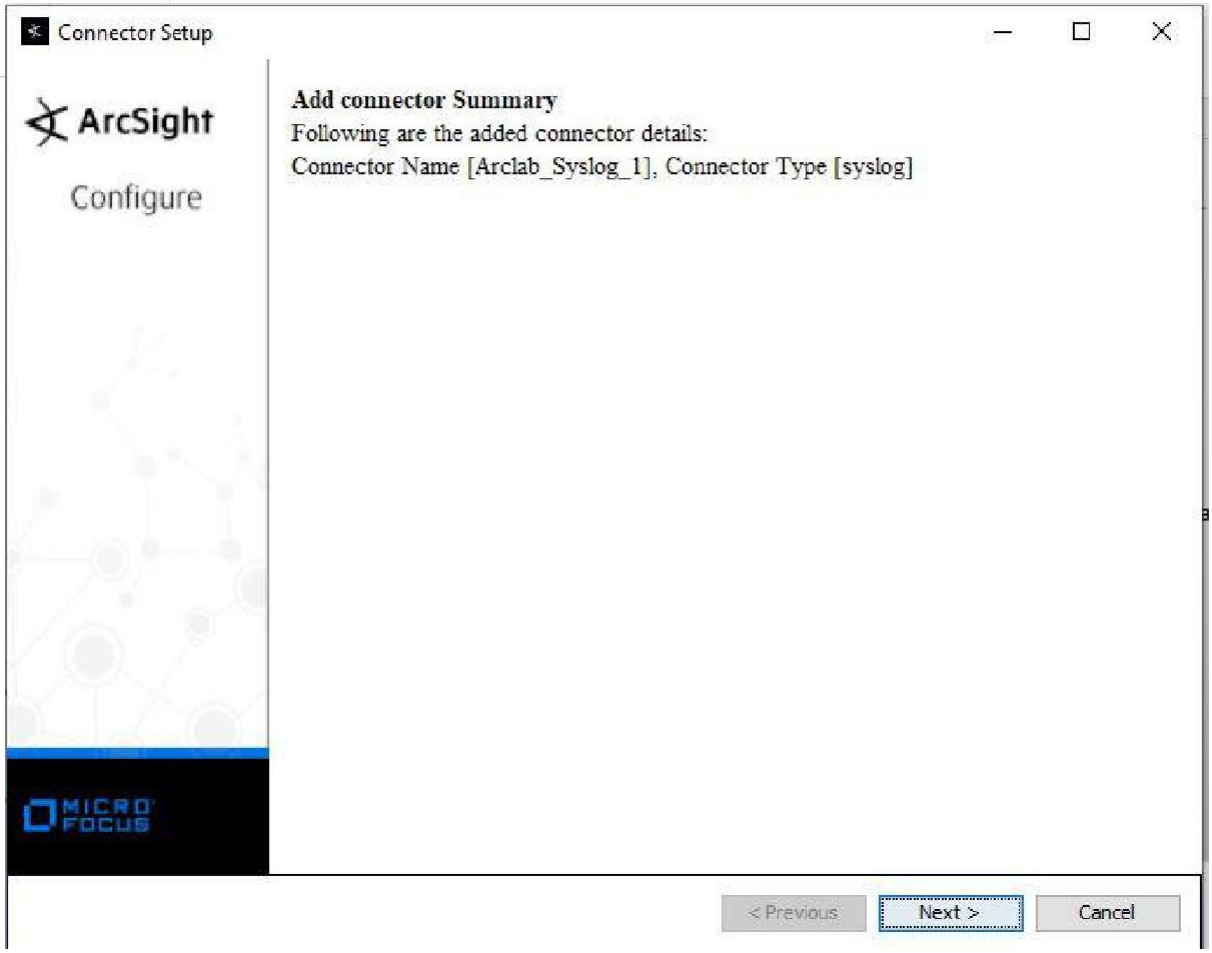

Connector Setup
ArcSight
Configure
Select the connector to configure
Type
Amazon Web Services CloudTrail
Sybase Adaptive Server Enterprise DB
Symantec AntiVirus Corporate Edition File
Symantec AntiVirus Corporate Edition Multiple File
Symantec Data Center Security DB
Symantec Endpoint Protection DB
Syslog Daemon
Syslog File
Syslog NG Daemon
MICRO FOCUS
< Previous
Next >
Cancel

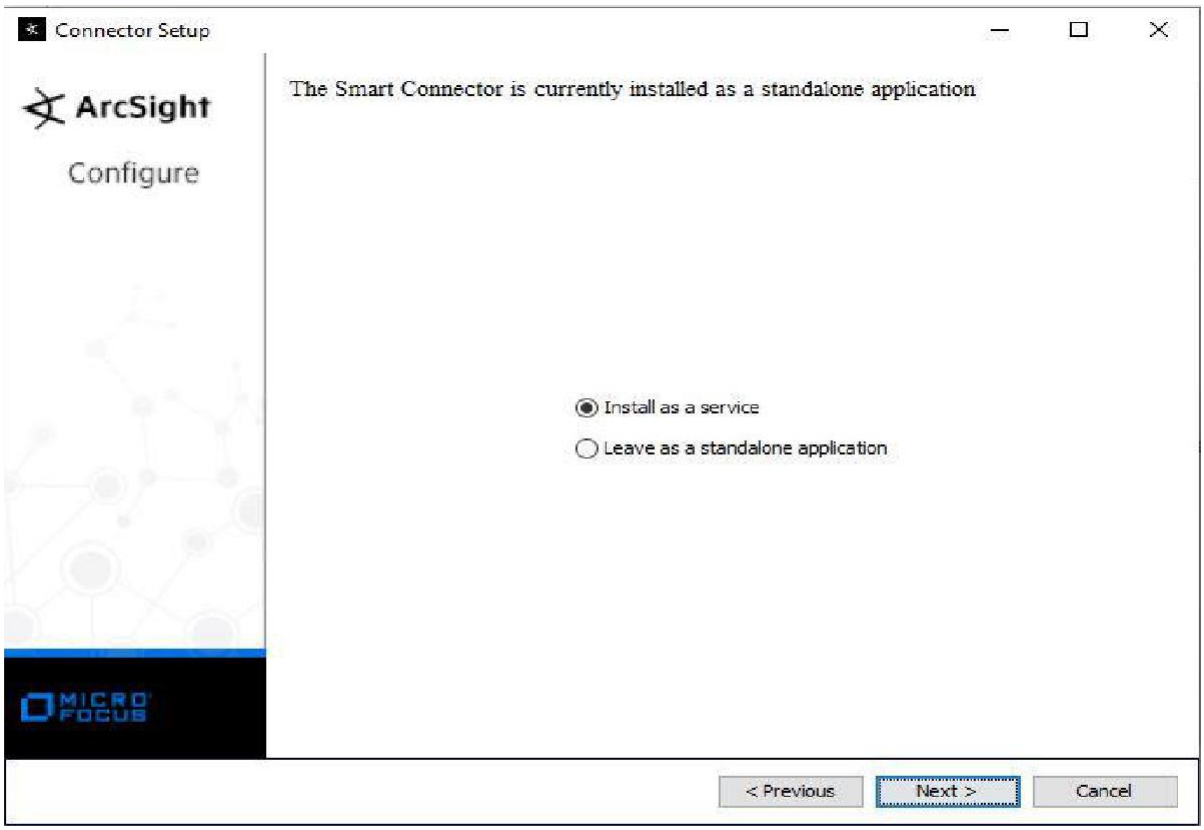

Connector Setup
ArcSight
Configure
Enter the parameter details
Network Port
514
IP Address
(ALL)
Protocol
UDP
Forwarder
false
MICRO FOCUS
< Previous
Next >
Cancel

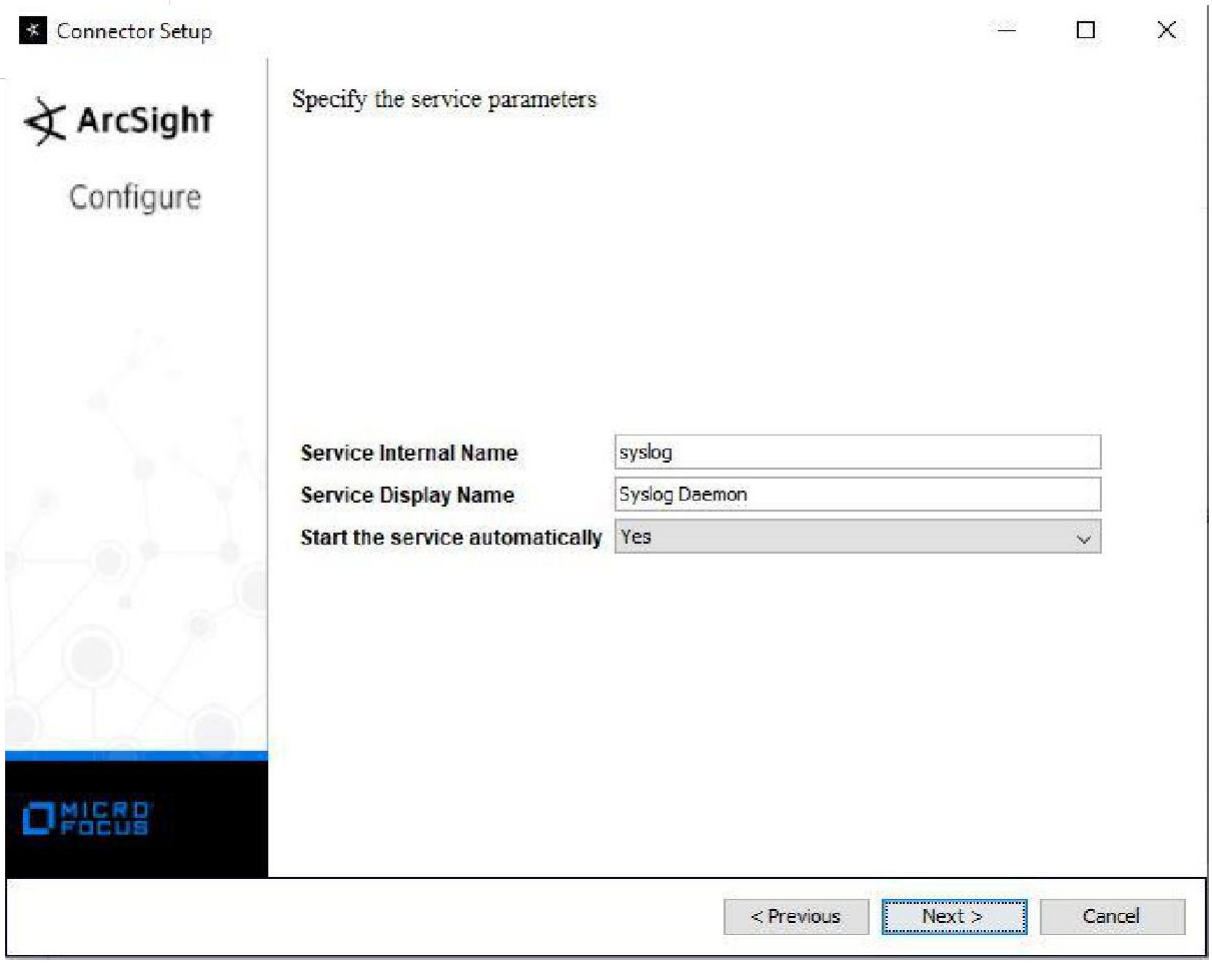

Connector Setup
ArcSight
Configure
Enter the type of destination
ArcSight Manager (encrypted)
ArcSight Logger SmartMessage (encrypted)
ArcSight Logger SmartMessage Pool (encrypted)
CEF File
Event Broker
CEF Syslog
CEF Encrypted Syslog (UDP)
CSV File
Raw Syslog
MICRO FOCUS
< Previous
Next >
Cancel

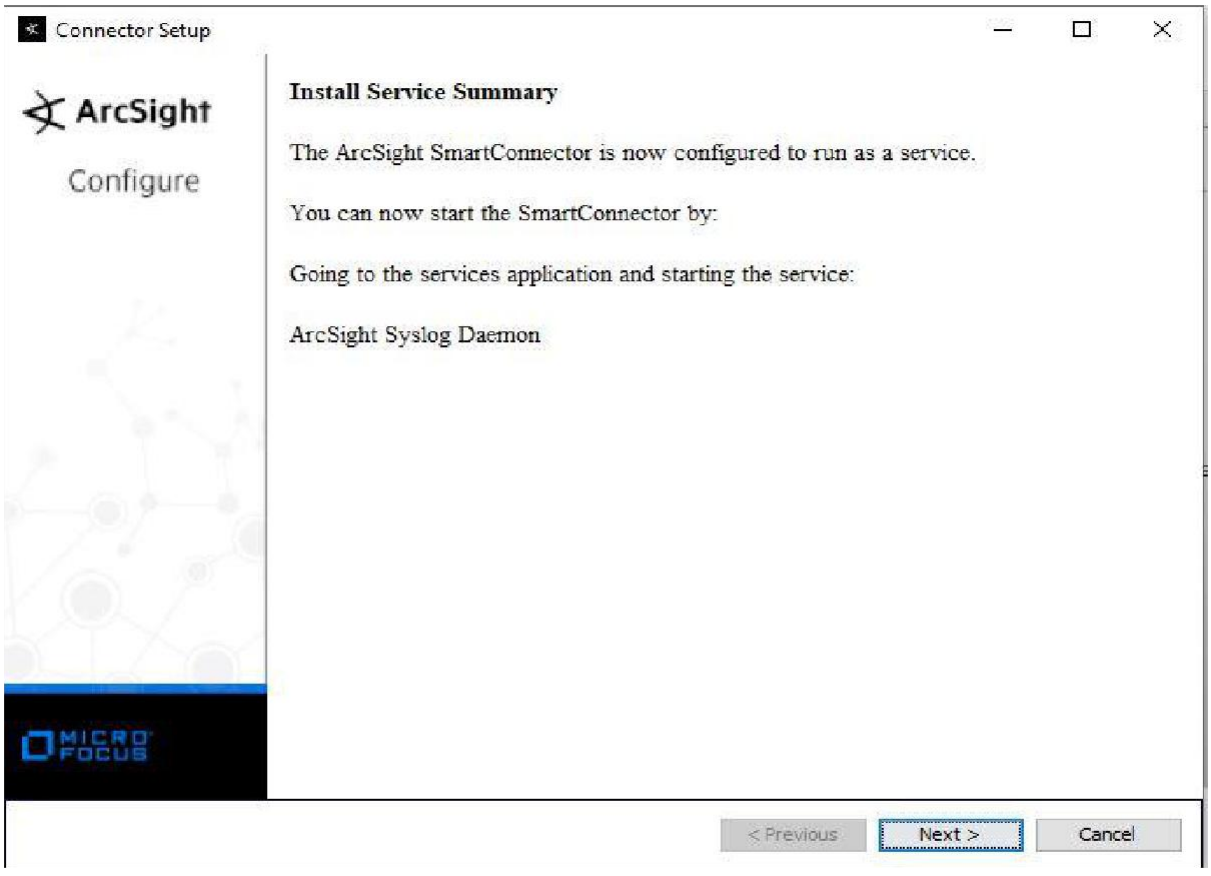

Connector Setup
ArcSight
Configure
Enter the destination parameters
Manager Hostname
arclabesm1
Manager Port
8443
User
admin
Password
AUP Master Destination
false
Filter Out All Events
false
Enable Demo CA
false
MICRO FOCUS
< Previous
Next >
Cancel

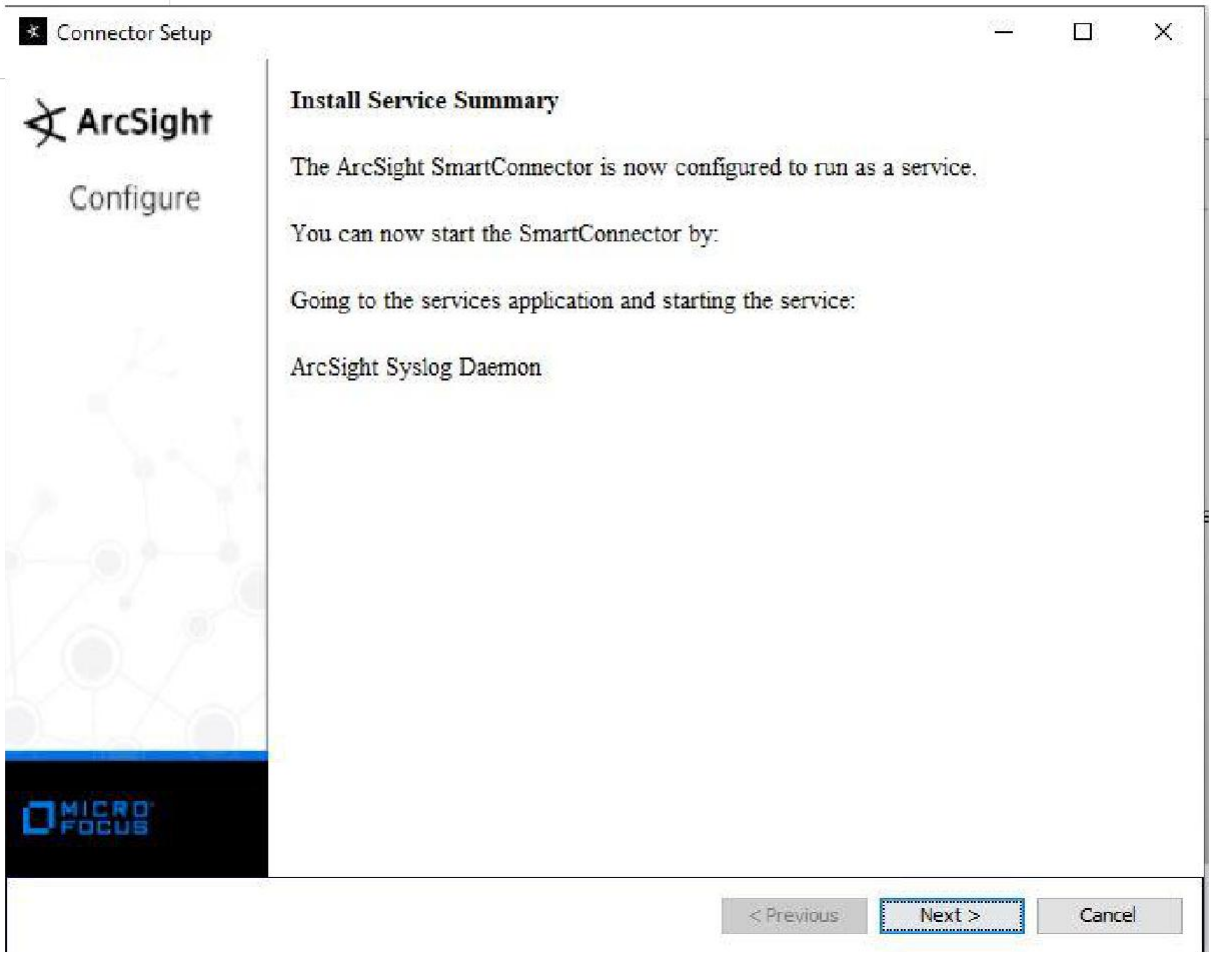

Connector Setup
ArcSight
Configure
Enter the connector details
Name
Arclab_Syslog_1
Location
arclabagentsrv1
DeviceLocation
<optional>
Comment
<optional>
MICRO FOCUS
< Previous
Next >
Cancel

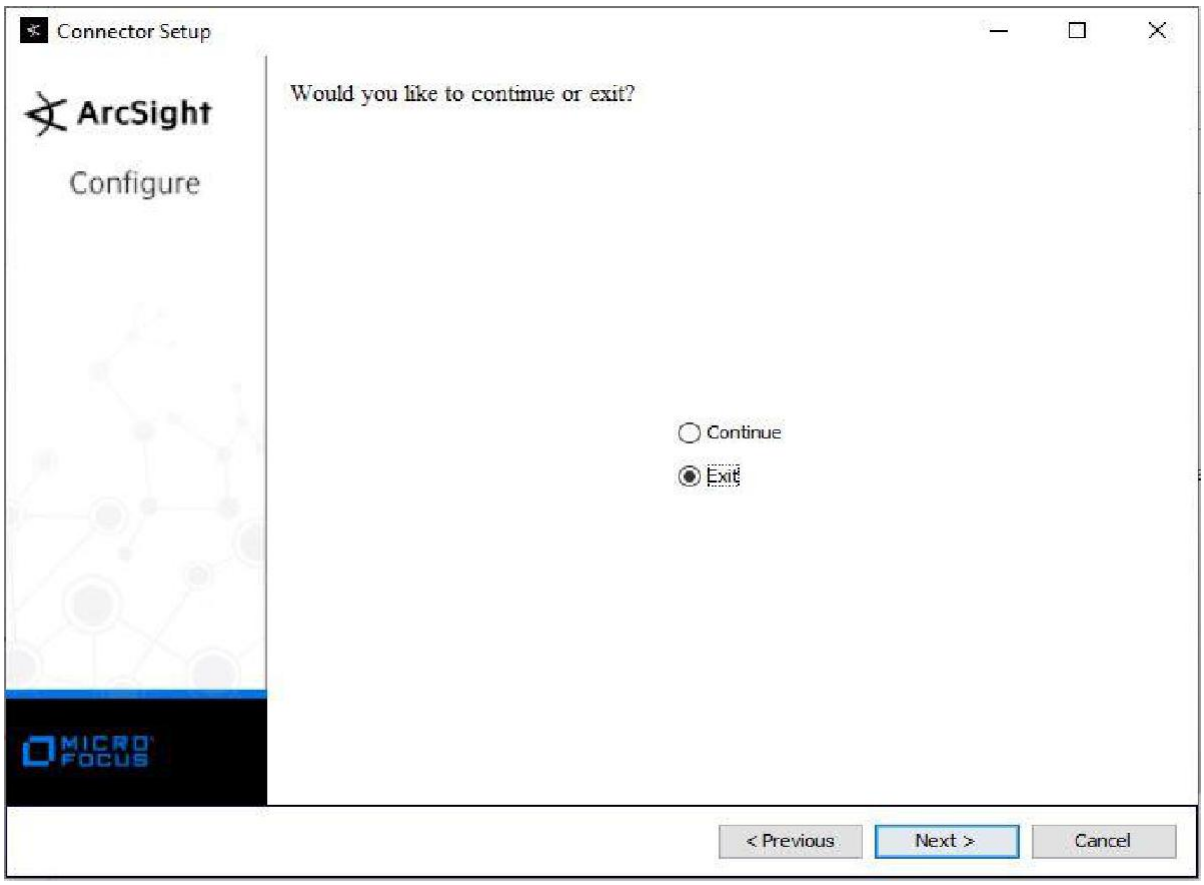

Connector Setup
ArcSight
Configure
Add connector Summary
Following are the added connector details:
Connector Name [Arclab_Syslog_1], Connector Type [syslog]
MICRO FOCUS
< Previous
Next >
Cancel

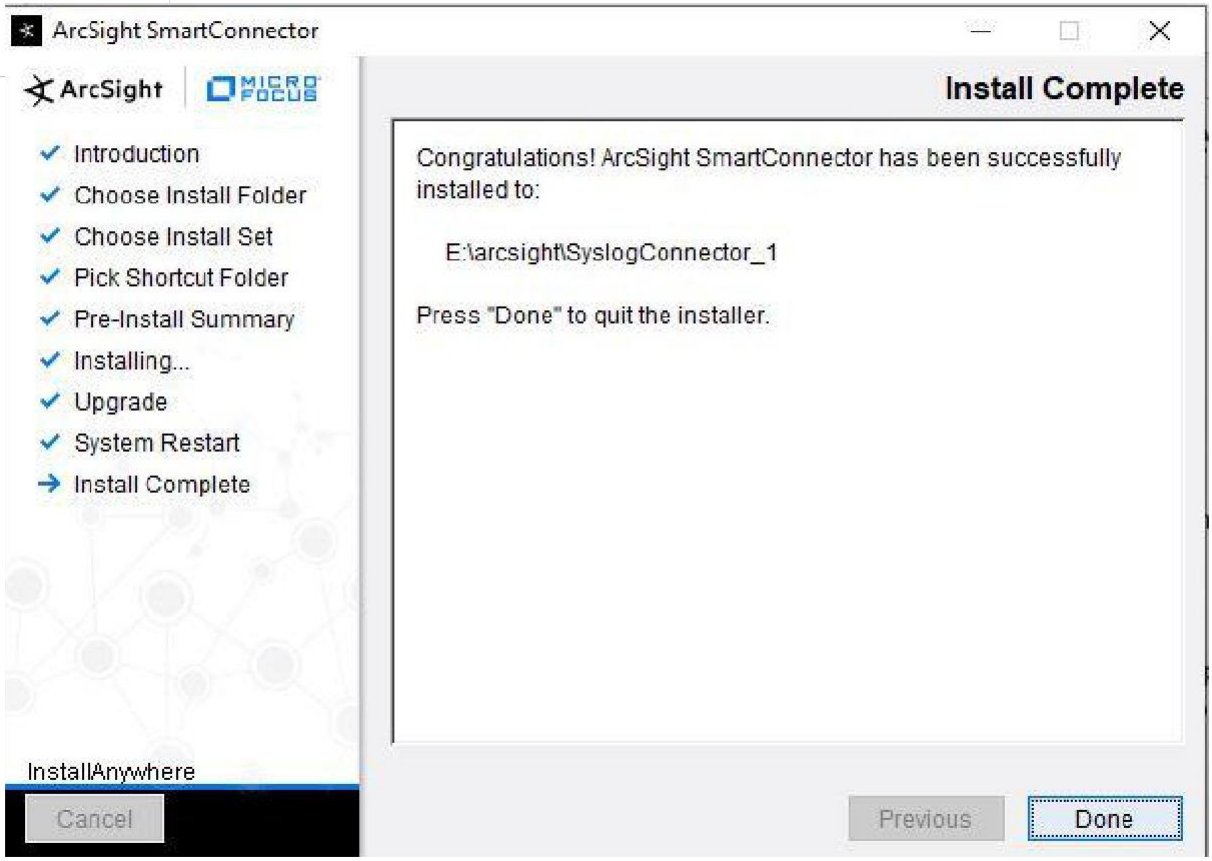

Connector Setup
ArcSight
Configure
The Smart Connector is currently installed as a standalone application
Install as a service
Leave as a standalone application
MICRO FOCUS
< Previous
Next >
Cancel

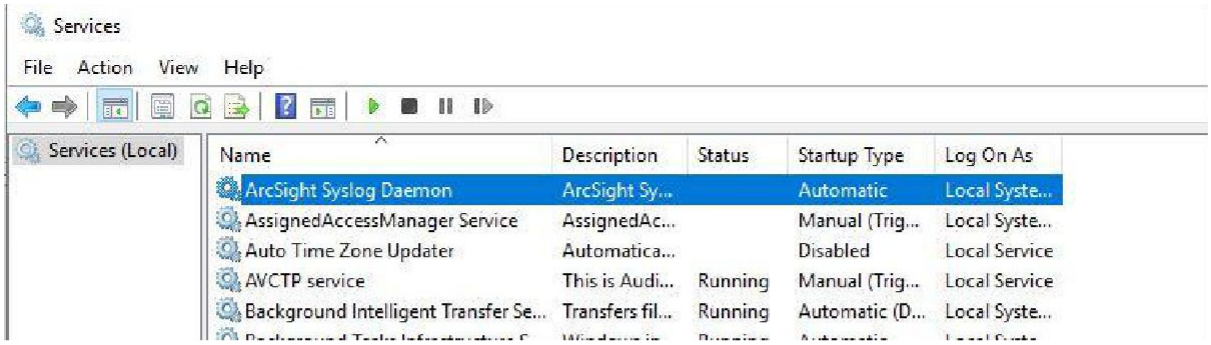

Connector Setup
ArcSight
Configure
Specify the service parameters
Service Internal Name
syslog
Service Display Name
Syslog Daemon
Start the service automatically
Yes
MICRO FOCUS
< Previous
Next >
Cancel


Connector Setup
ArcSight
Configure
Install Service Summary
The ArcSight SmartConnector is now configured to run as a service.
You can now start the SmartConnector by:
Going to the services application and starting the service:
ArcSight Syslog Daemon
MICRO FOCUS
< Previous
Next >
Cancel


Connector Setup
ArcSight
Configure
Install Service Summary
The ArcSight SmartConnector is now configured to run as a service.
You can now start the SmartConnector by:
Going to the services application and starting the service:
ArcSight Syslog Daemon
MICRO FOCUS
< Previous
Next >
Cancel


Connector Setup
ArcSight
Configure
Would you like to continue or exit?
Continue
Exit
MICRO FOCUS
< Previous
Next >
Cancel


ArcSight SmartConnector
ArcSight
MICRO FOCUS
Introduction
Choose Install Folder
Choose Install Set
Pick Shortcut Folder
Pre-Install Summary
Installing...
Upgrade
System Restart
Install Complete
Install Complete
Congratulations! ArcSight SmartConnector has been successfully installed to:
E:\arcsight\SyslogConnector_1
Press "Done" to quit the installer.
InstallAnywhere
Cancel
Previous
Done


Services
File Action View Help
Services (Local)
Name
Description
Status
Startup Type
Log On As
ArcSight Syslog Daemon
ArcSight Sy...
Automatic
Local Syste...
AssignedAccessManager Service
AssignedAc...
Manual (Trig...
Local Syste...
Auto Time Zone Updater
Automatica...
Disabled
Local Service
AVCTP service
This is Audi...
Running
Manual (Trig...
Local Service
Background Intelligent Transfer Se...
Transfers fil...
Running
Automatic (D...
Local Syste...

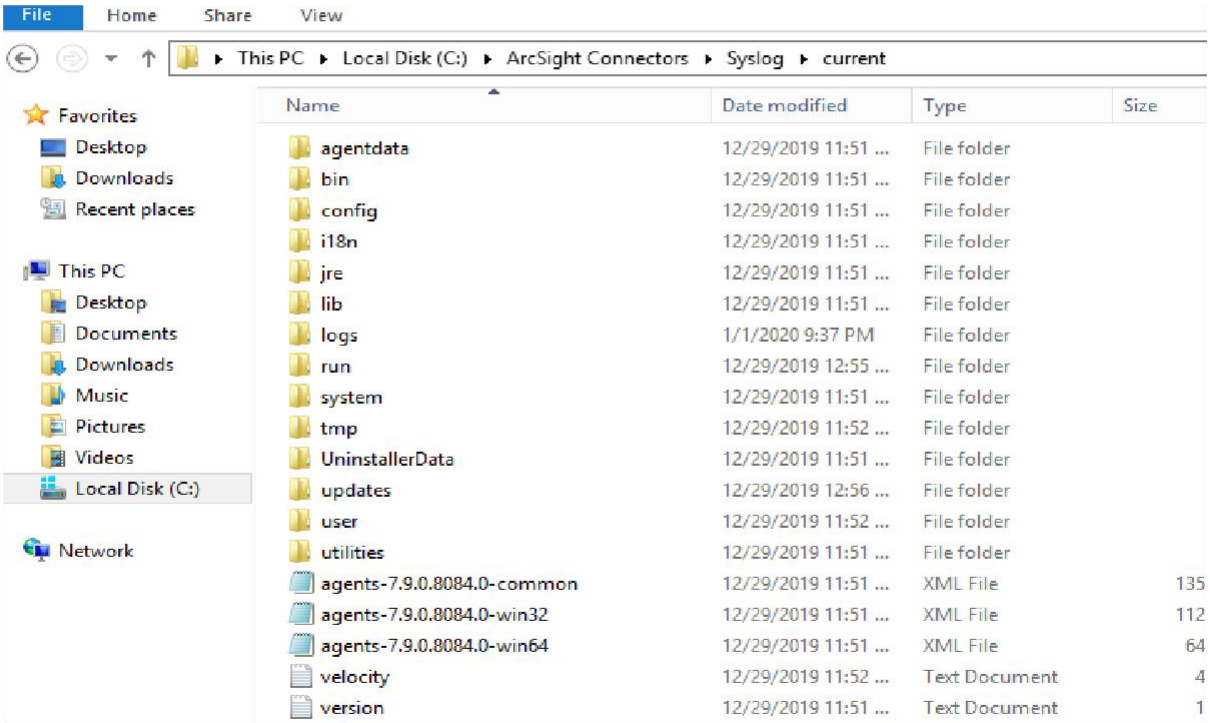
Up gradation of Smart Connector :

- To locally upgrade a connector:
- **Step 1:** Stop the running connector and run the new SmartConnector installer. The installer prompts you for the location to install the connector.
- **Step 2:** Select the location of the SmartConnector that you want to upgrade. The message "Previous Version Found". Do you want to upgrade?" appears.
- **Step 3:** Select the option to continue and upgrade the connector. The original installation is renamed by prefacing characters to the original folder name; the upgraded connector is installed in the location $ARCSIGHT_HOME\current.
- **Step 4:** Start the connector service & check the latest agent.log & agent.wrapper.log to confirm successful Connector up-gradation.

Uninstall a Connector and Connector Service :

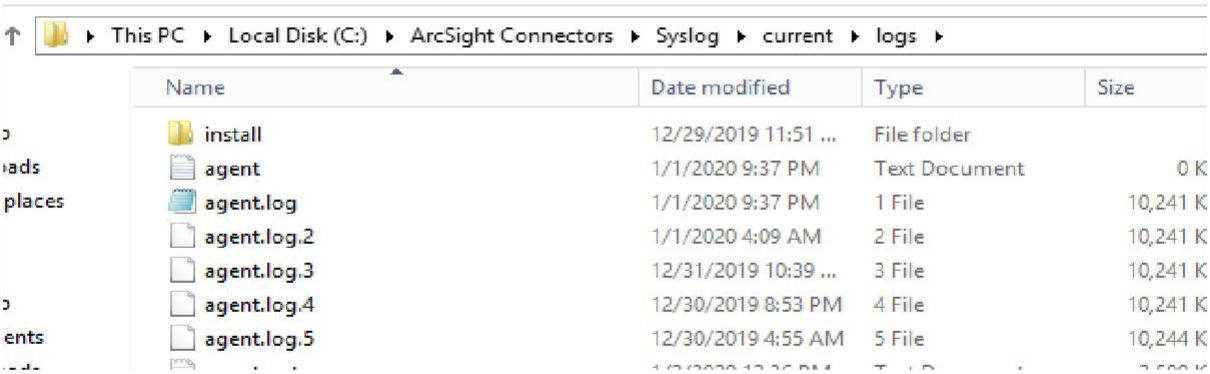
- Stop the connector service
- Remove the connector service by executing *runagentsetup*
- Uninstall the connector and its framework
- Delete the installation directory
- Delete the entry from ESM console

Logs File of the Connectors :



Agent.log file Analysis

- Check the latest agent.log file to see the connector log forwarding status, memory utilization and EPS etc.



Module – 3

- Installation of ESM
- Installation of ESM Console

Check ESM Installing Server Configuration.

Installation of ESM.

Installation of ESM Console.

Preparing for Install :

- Supported platform for ESM 6.11 – Refer ESM support matrix document
  - RHEL/CentOS 6.8
  - RHEL/CentOS 7.3
- Installation Methods
  - Command Line – typical
  - GUI – Require X11 Windows
  - System Hardware Requirements

	Minimum	Mid-Range	High Performance
Processors	8 cores (16 preferred)	32 cores	40 cores
Memory	48 GB RAM (64 preferred)	192 GB RAM	512 GB RAM
Hard Disk	Six 600 GB disks (1.5 TB) (RAID 10) 15,000 RPM	20 1 TB disks (10 TB) (RAID 10) 10,000 RPM	12 TB (RAID 10) Solid state

Preparing for Install – CPU and Memory checks :

```
[root@arclabesm2 ~]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                8
On-line CPU(s) list:   0-7
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):             8
NUMA node(s):          1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 44
Model name:            Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
Stepping:              2
CPU MHz:               2660.000
BogoMIPS:              5320.00
Hypervisor vendor:     VMware
Virtualization type:   full
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              12288K
NUMA node0 CPU(s):     0-7
Flags:                 fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge
tsc pni pclmulqdq ssse3 cx16 sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer
```

```
[root@arclabesm2 ~]# free -m
              total        used        free      shared  buff/cache   available
Mem:           9837         205        9304           8         328        9341
Swap:          5055           0        5055
[root@arclabesm2 ~]#
```

Linux Partitions :

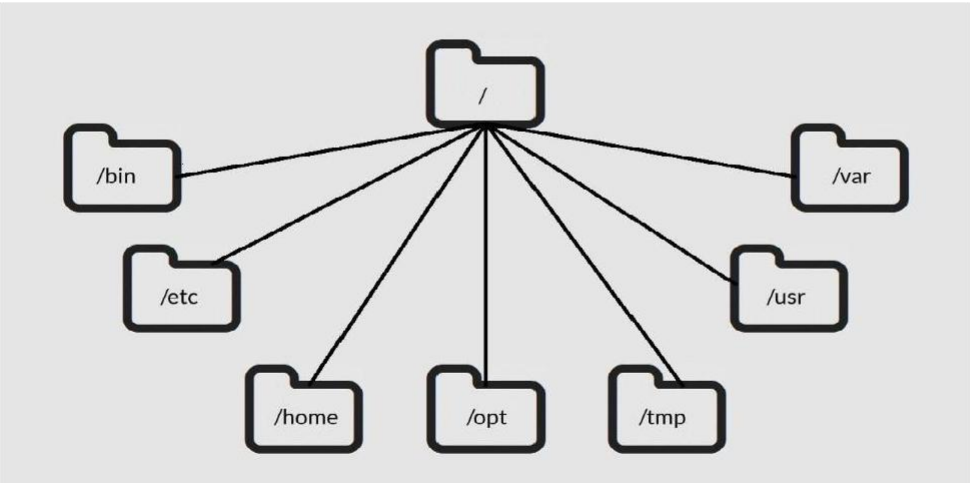
Isblk

```
[root@arclabesm2 ~]# lsblk
NAME            MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda               8:0    0  120G  0 disk
├─sda1            8:1    0    1G  0 part /boot
└─sda2            8:2    0  119G  0 part
  ├─centos-root 253:0    0   80G  0 lvm  /
  └─centos-swap 253:1    0    5G  0 lvm  [SWAP]
sr0              11:0    1  8.8G  0 rom
```

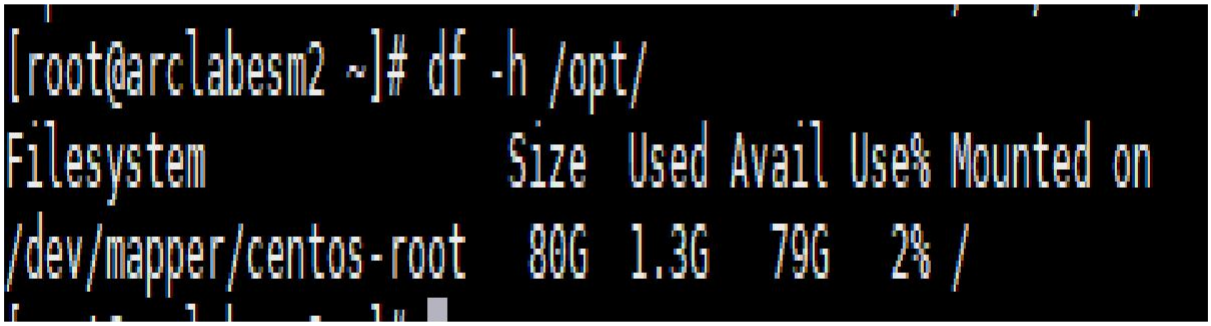
Df-h

```
[root@arclabesm2 ~]# df -h
Filesystem               Size  Used Avail Use% Mounted on
/dev/mapper/centos-root   80G  1.3G   79G   2% /
devtmpfs                 4.8G     0  4.8G   0% /dev
tmpfs                    4.9G     0  4.9G   0% /dev/shm
tmpfs                    4.9G  8.9M  4.8G   1% /run
tmpfs                    4.9G     0  4.9G   0% /sys/fs/cgroup
/dev/sda1               1014M  142M  873M  14% /boot
tmpfs                    984M     0  984M   0% /run/user/0
```

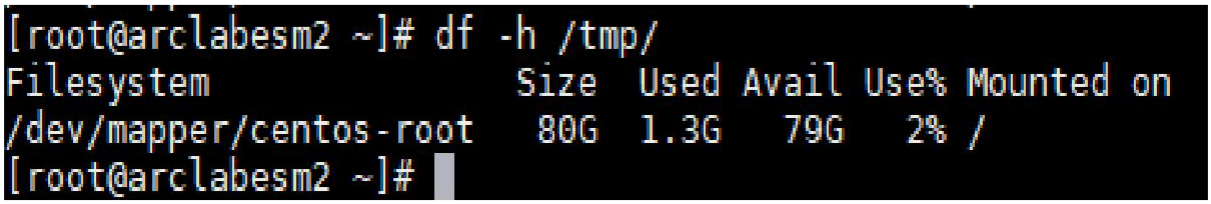
Linux File System Hierarchy



Verify Minimum Space Requirement df-h /opt

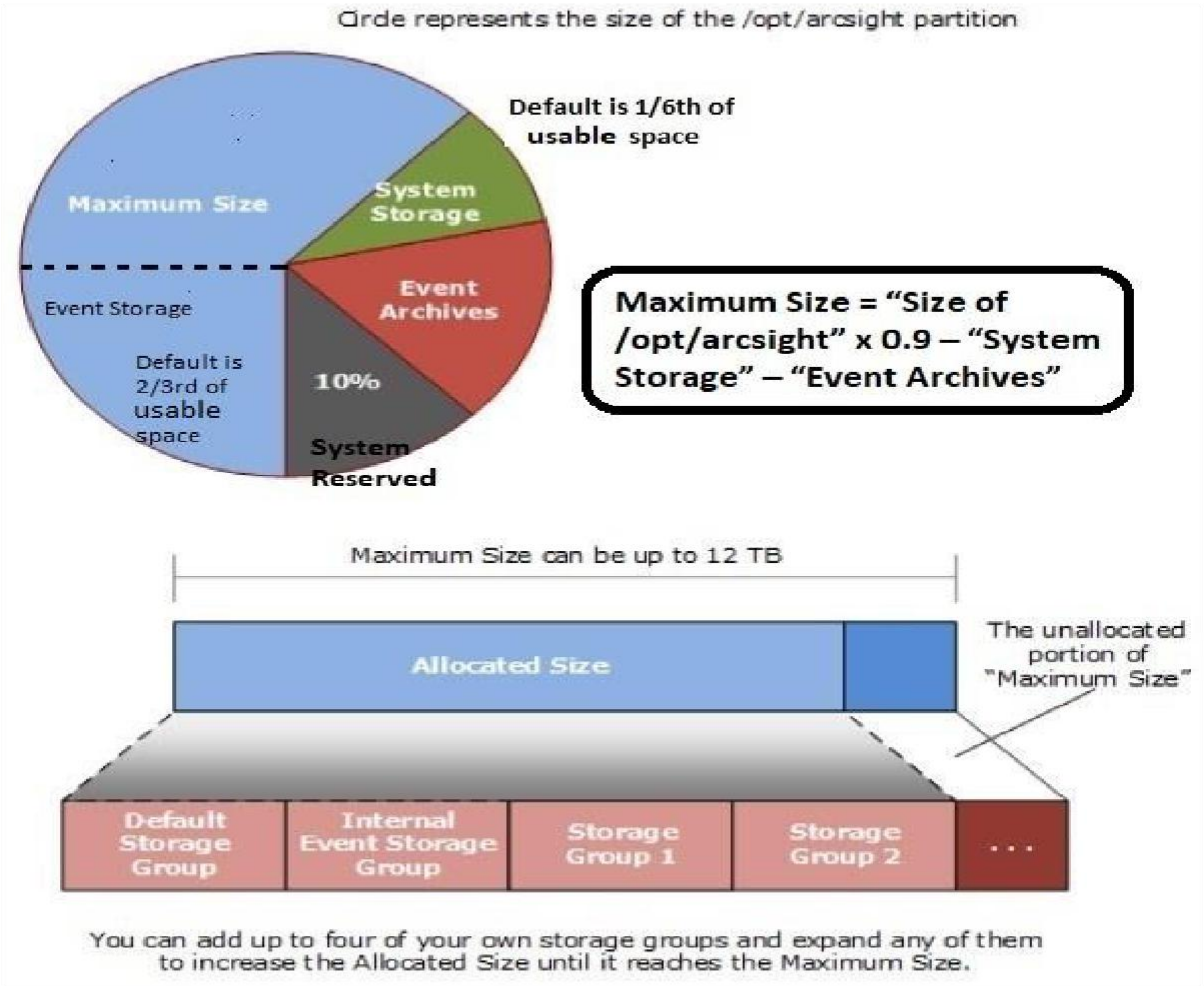


df-h /tmp



CORR Engine Sizing

- System Storage – non-event storage(resources, trends, lists etc.)
- Event Storage – storage for events.
- Online Event Archive – archive of online events.



Other Requirements:

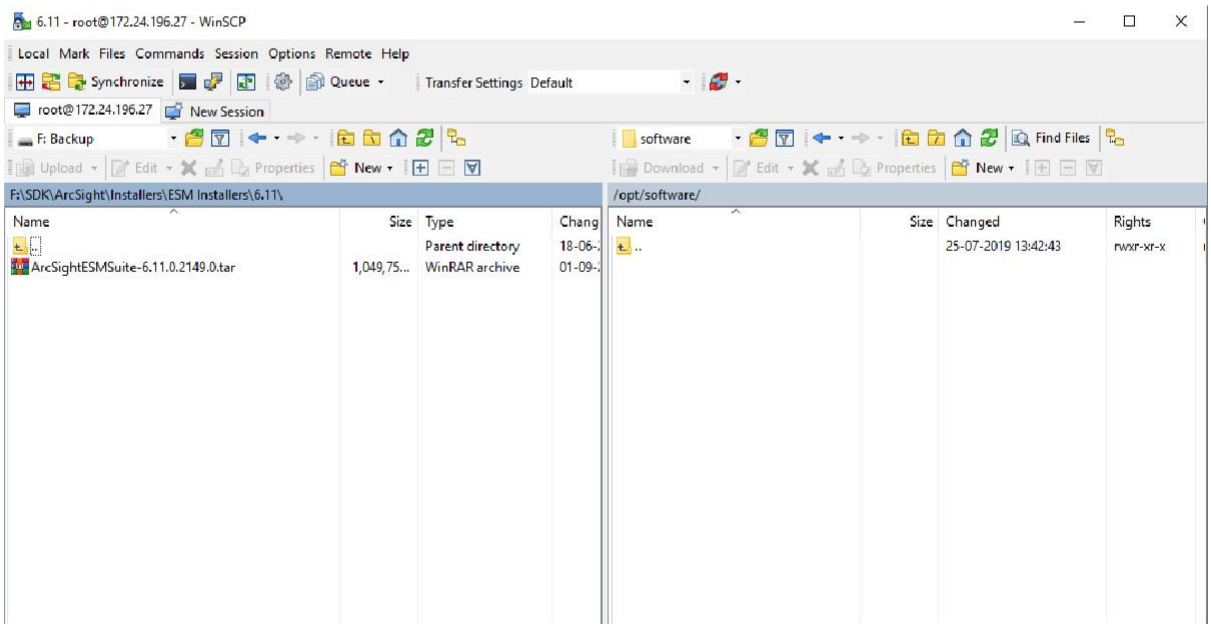
- ESM installation package (.tar file) – Extract later
    - ArcSightESMSuite-6.11.0.2149.0.tar (major.minor.build.patch)
- ESM License (.zip or .lic)
- Open TCP ports in IPTables – 8443,9000
- Temporary Directory /tmp – 4GB Min free space.
- Create arcsight group and user.
- Create directory /opt/Arcsight.
- Increase user process limit settings.

Port Connectivity Requirements:

Port	Flow	Description
22/TCP	Inbound	SSH log in (Unix only)
53/UDP	Inbound/Outbound	DNS requests and responses
8443/TCP	Inbound	SmartConnectors and Consoles
25/TCP	Outbound	SMTP to mail server
110/TCP	Outbound	POP3 to mail server, if applicable
143/TCP	Outbound	IMAP to mail server, if applicable
1645/UDP	Inbound/Outbound	RADIUS, if applicable
1812/UDP	Inbound/Outbound	RADIUS, if applicable
389/TCP	Outbound	LDAP to LDAP server, if applicable
636/TCP	Outbound	LDAP over SSL to LDAP server, if applicable

ESM Installation and Configuration Wizard:

- Copy installation .tar file to the system where you will be installing ESM.



ESM Installation and Configuration Wizard:

- Prepare the system:-

  - Login as root
  - Update /etc/hosts file with esm hostname
  - Make sure zip and unzip packages are installed. (yum install zip unzip)

- Untar the file: ArcSightESMSuite-6.11.0.2149.0.tar
- Run Tools/prepare_system.sh – It will create user arcsight, sets password, modify user process limit and open files limit
- Change ownership of all the files and folders that were extracted from the tar file to be owned by user *arcsight*
- Reboot the system.
- For /opt/arcsight folder fix ownership and permission as arcsight
    - chmod +x /opt/arcsight
- Verify the changes

$ ulimit -a

Check for the following two lines:

open files 65536

max user processes 10240

ESM Installation and Configuration Wizard:

- Change execution mode of ArcSight ESM setup and assign privileges to ArcSight User.

```
[root@dcesm1 software]# pwd
/opt/software
[root@dcesm1 software]# chown arcsight:arcsight ArcSightESMSuite.bin
[root@dcesm1 software]# chmod +x ArcSightESMSuite.bin
[root@dcesm1 software]# ll
total 1124876
-rwxrwxr-x. 1 arcsight arcsight 1074944000 Oct 13 23:17 ArcSightESMSuite-6.11.0.2149.0.tar
-r-x--x--x. 1 arcsight arcsight   76903829 Apr  5  2017 ArcSightESMSuite.bin
```

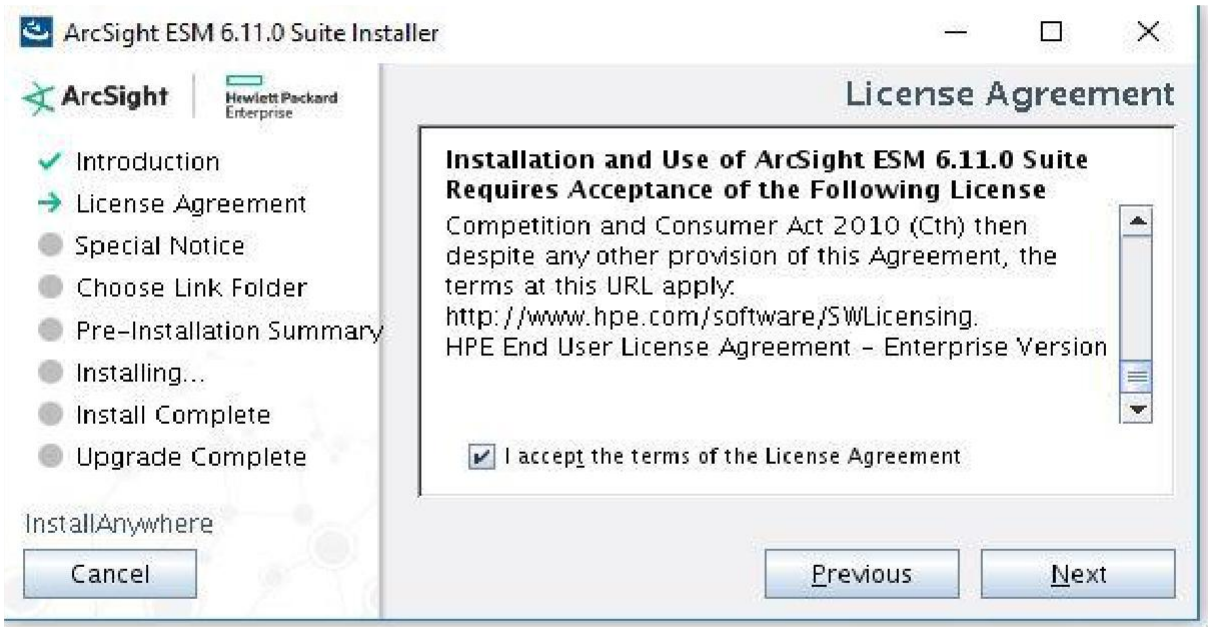
- Run the installation file as follows: (To run in GUI mode, X Window must be running. If it is not, the installer automatically runs in Console mode. GUI mode is entirely optional)

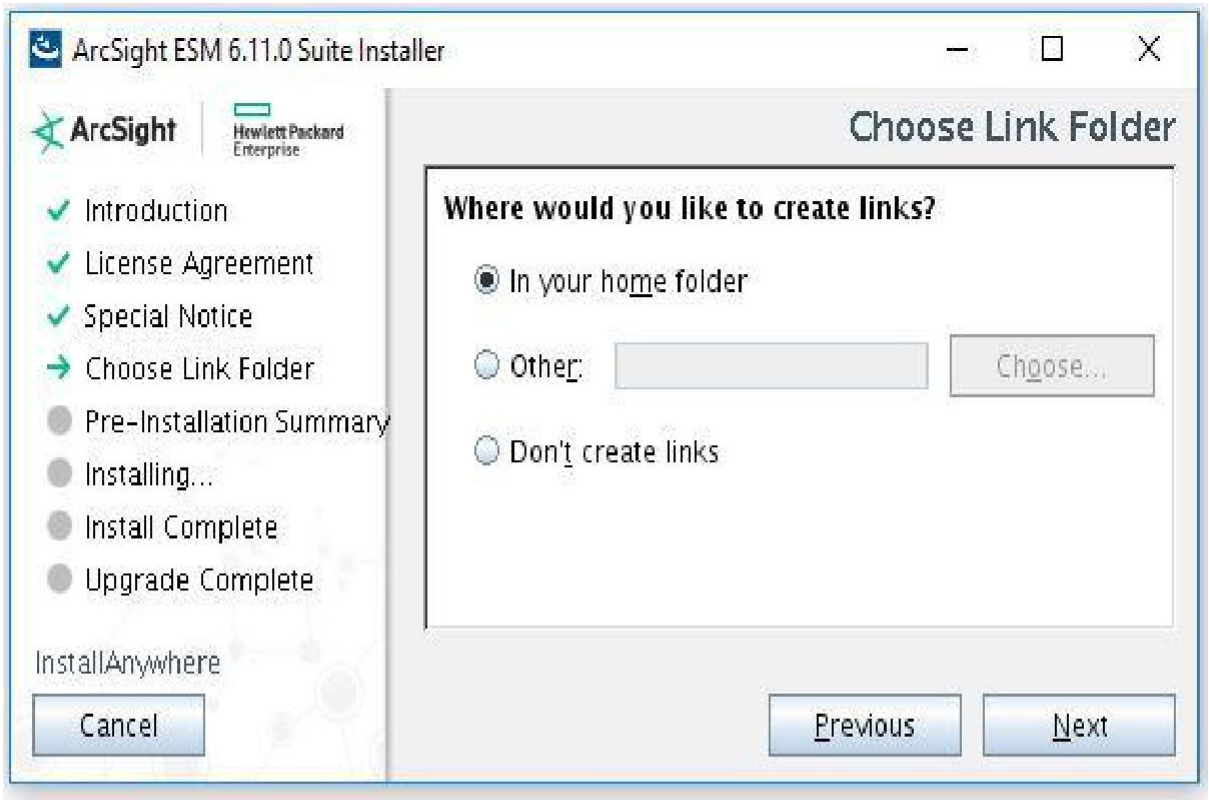
```
[root@dcesm1 software]# ./ArcSightESMSuite.bin
Preparing to install
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...
```

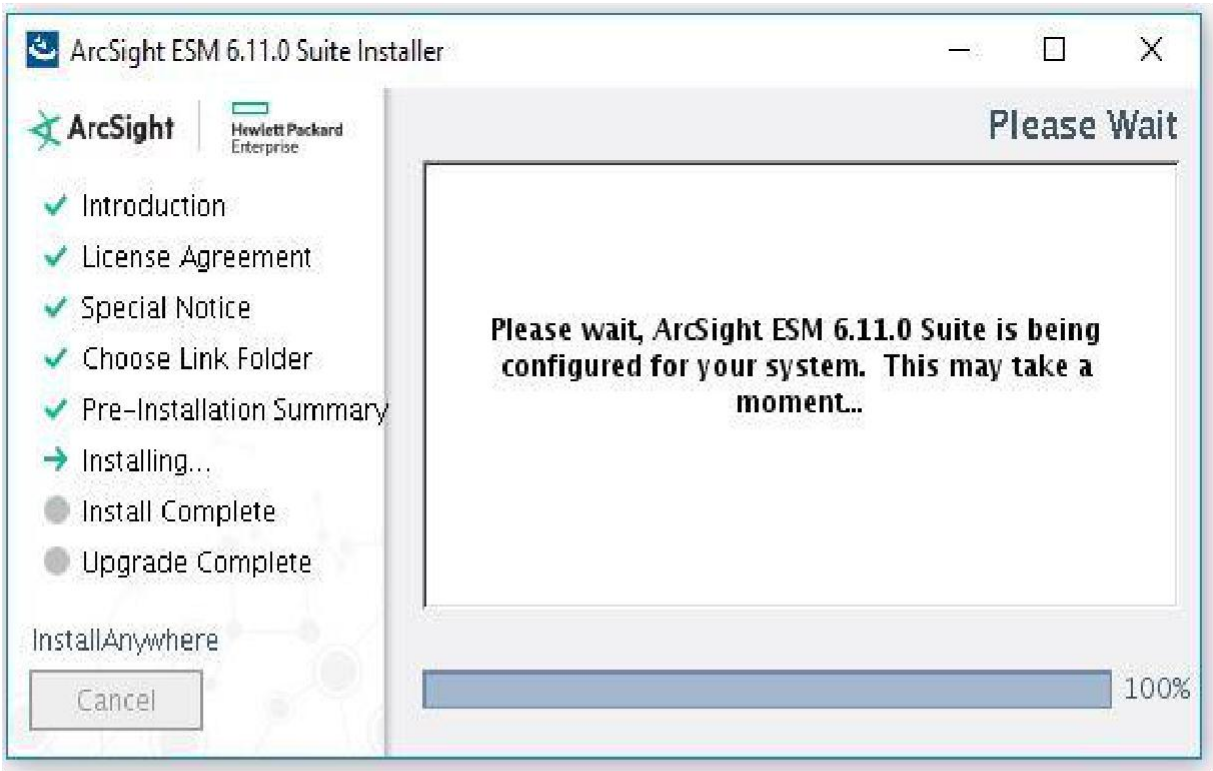
- Configuration wizard runs &following screen appears:

- Accept License Agreement



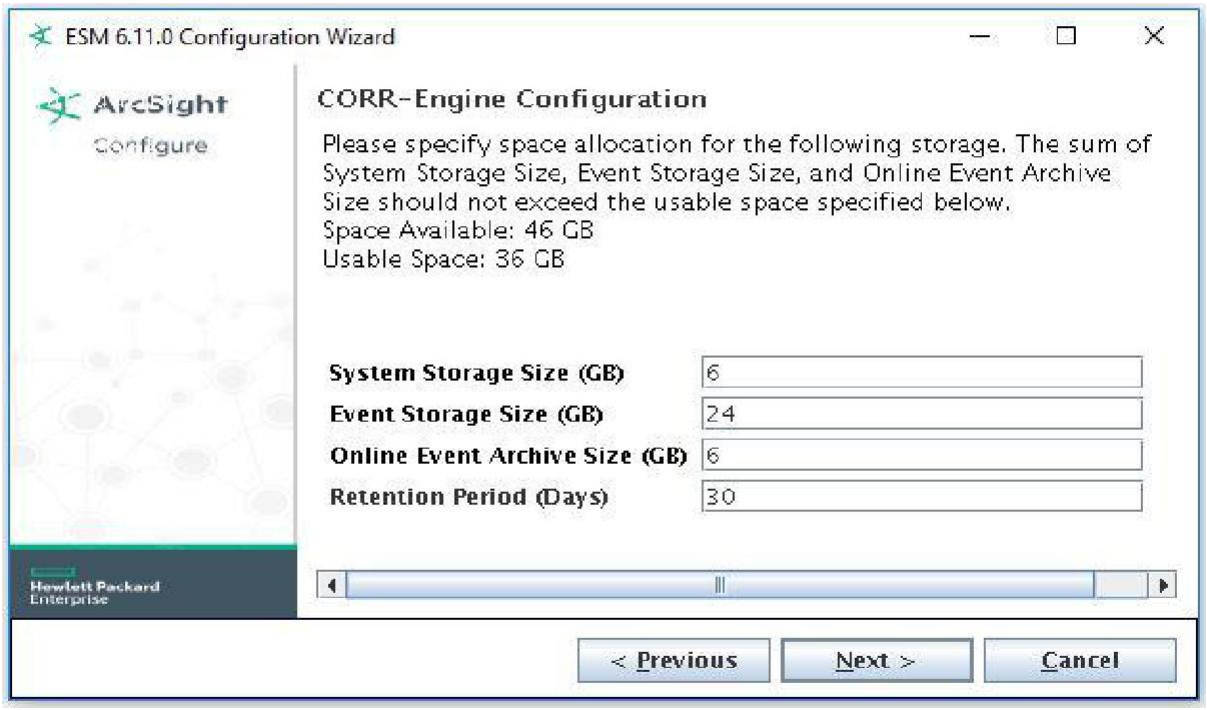



ArcSight ESM 6.11.0 Suite Installer
ArcSight
Hewlett Packard Enterprise
Introduction
License Agreement
Special Notice
Choose Link Folder
Pre-Installation Summary
Installing...
Install Complete
Upgrade Complete
InstallAnywhere
Cancel
Pre-Installation Summary
Please Review the Following Before Continuing:
Product Name:
ArcSight ESM 6.11.0 Suite
Install Folder:
/opt/arcsight
Link Folder:
/home/arcsight
Previous
Install

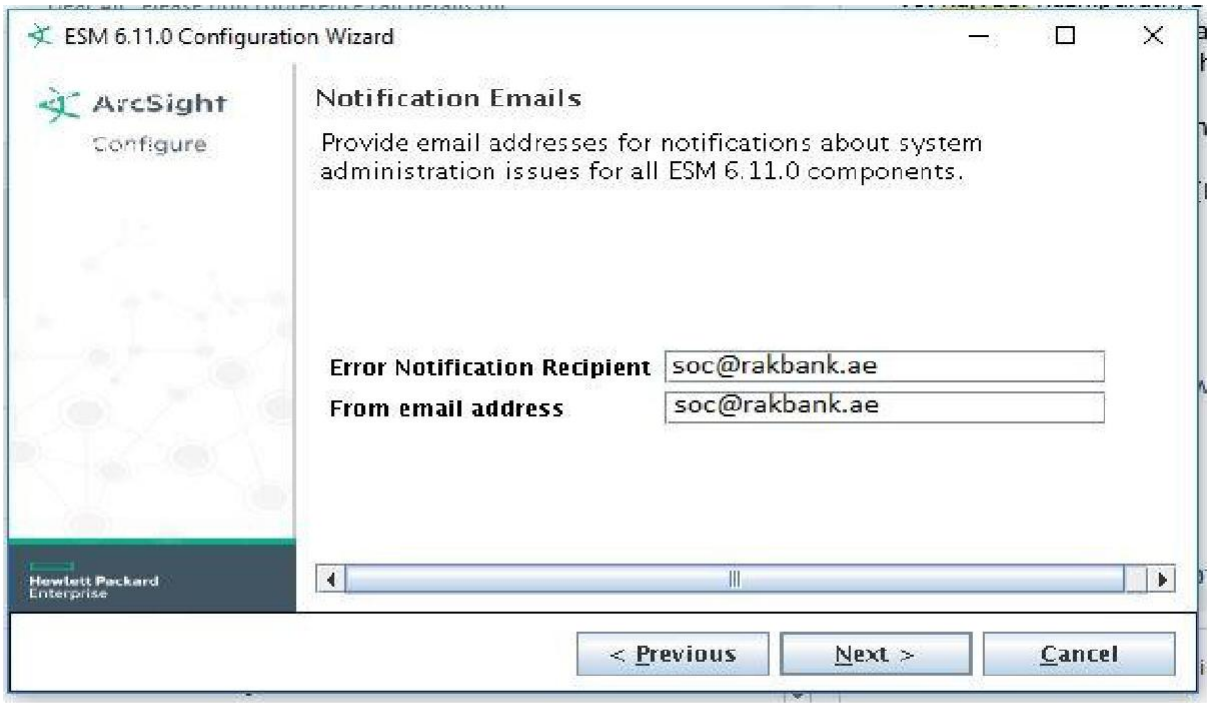

ArcSight ESM 6.11.0 Suite Installer
ArcSight
Hewlett Packard Enterprise
Introduction
License Agreement
Special Notice
Choose Link Folder
Pre-Installation Summary
Installing...
Install Complete
Upgrade Complete
InstallAnywhere
Cancel
Please Wait
Please wait, ArcSight ESM 6.11.0 Suite is being configured for your system. This may take a moment...
100%

Enter password for the CORRE Engine

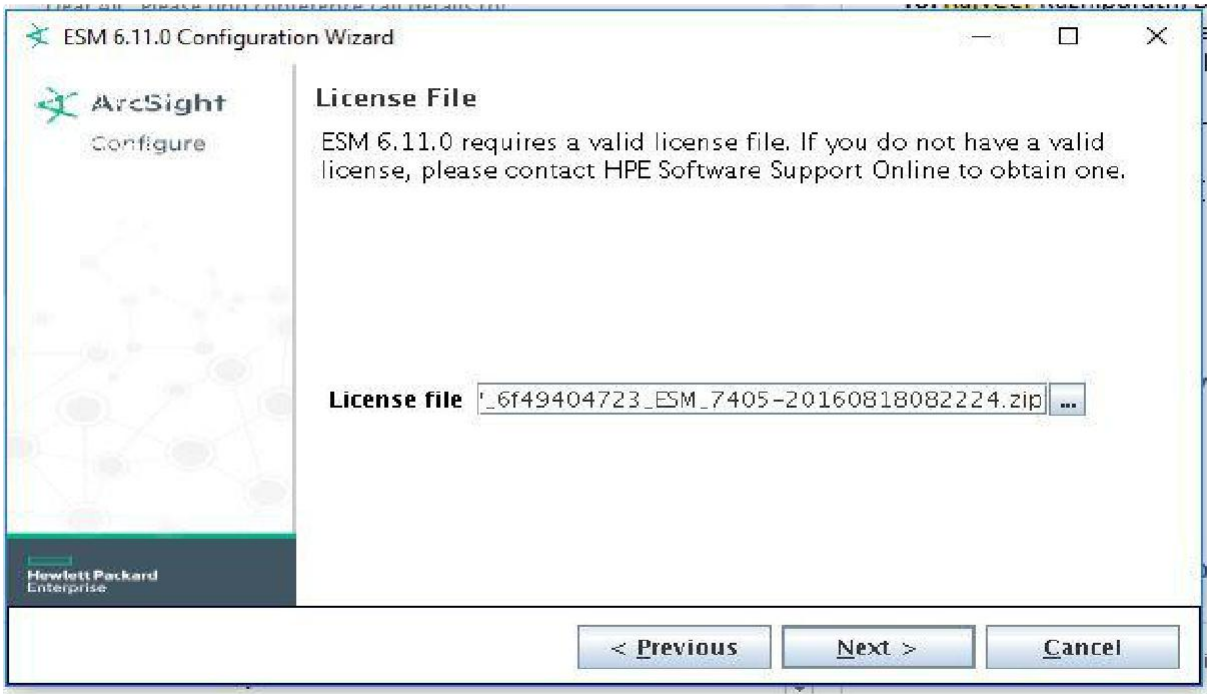
Default space allocation is specified. Click **Next.**



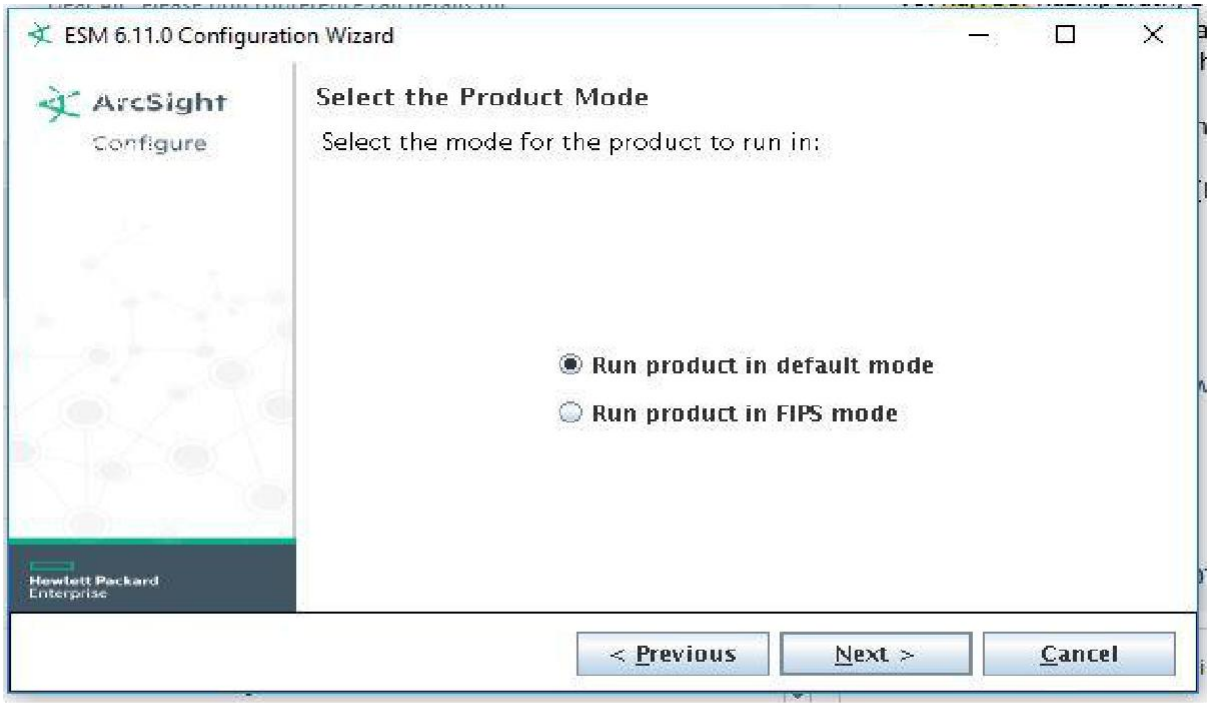
Click Error Notification recipients & from mail address:



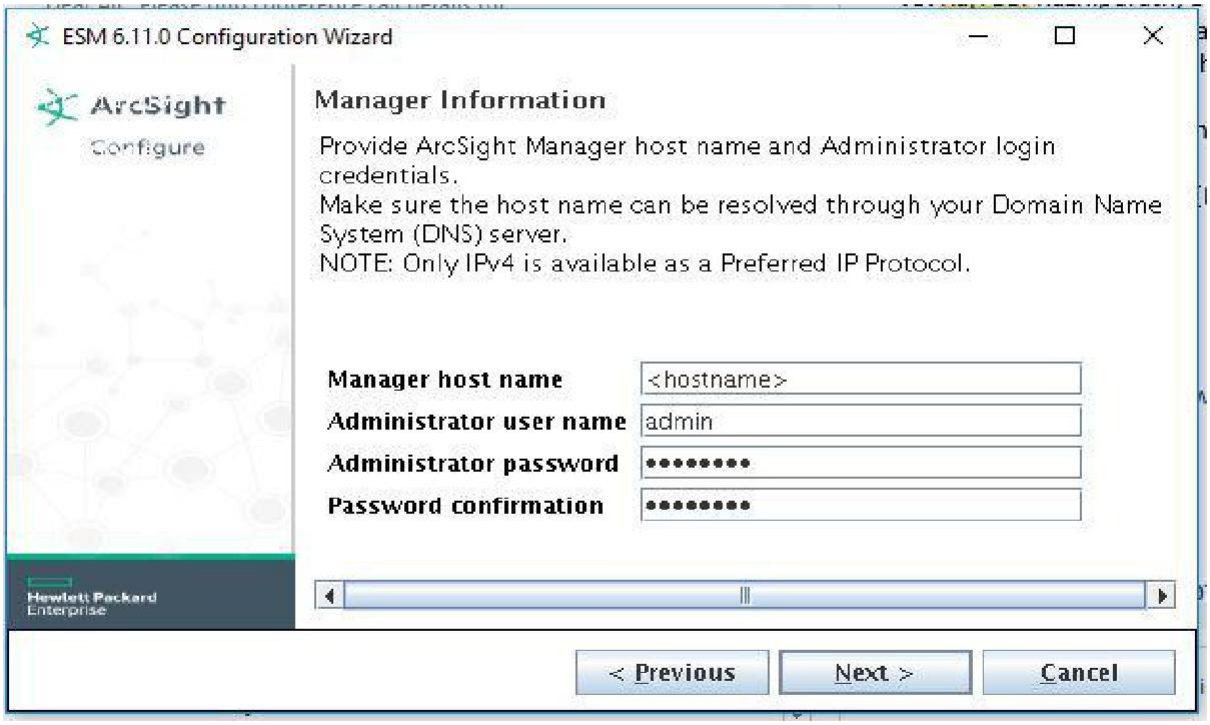
Select the ”License file” via connecting through Pen drive



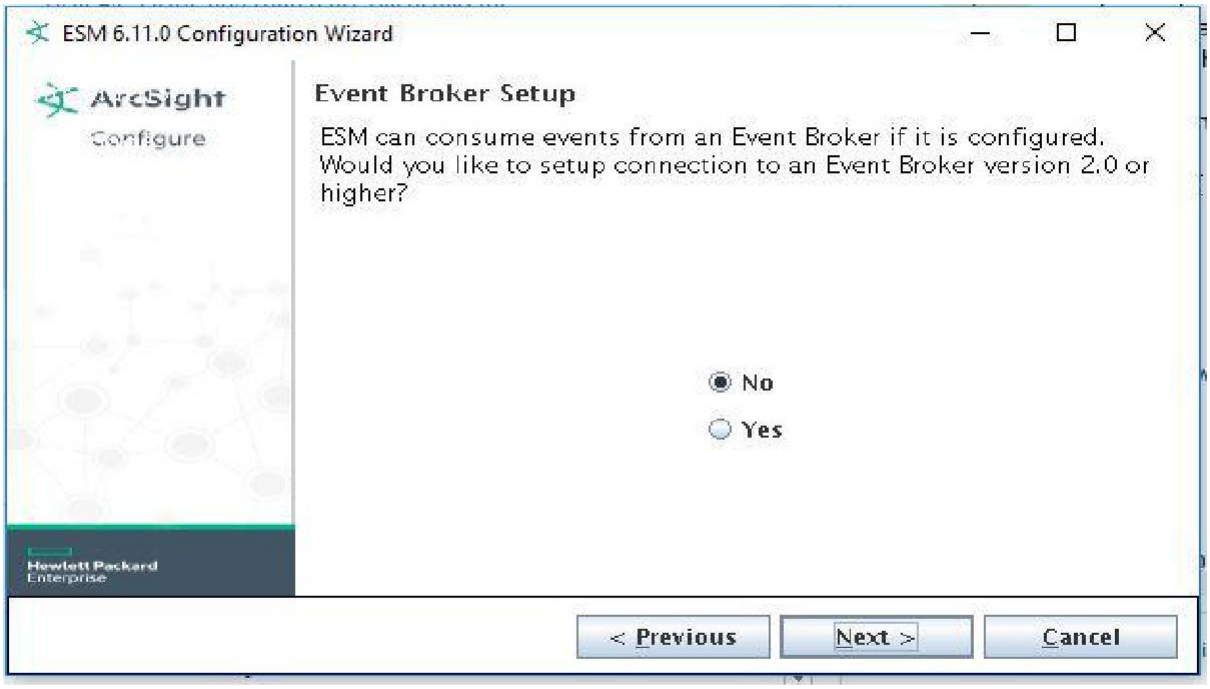
Select the default **“Run in default mode”**& click **“Next”**



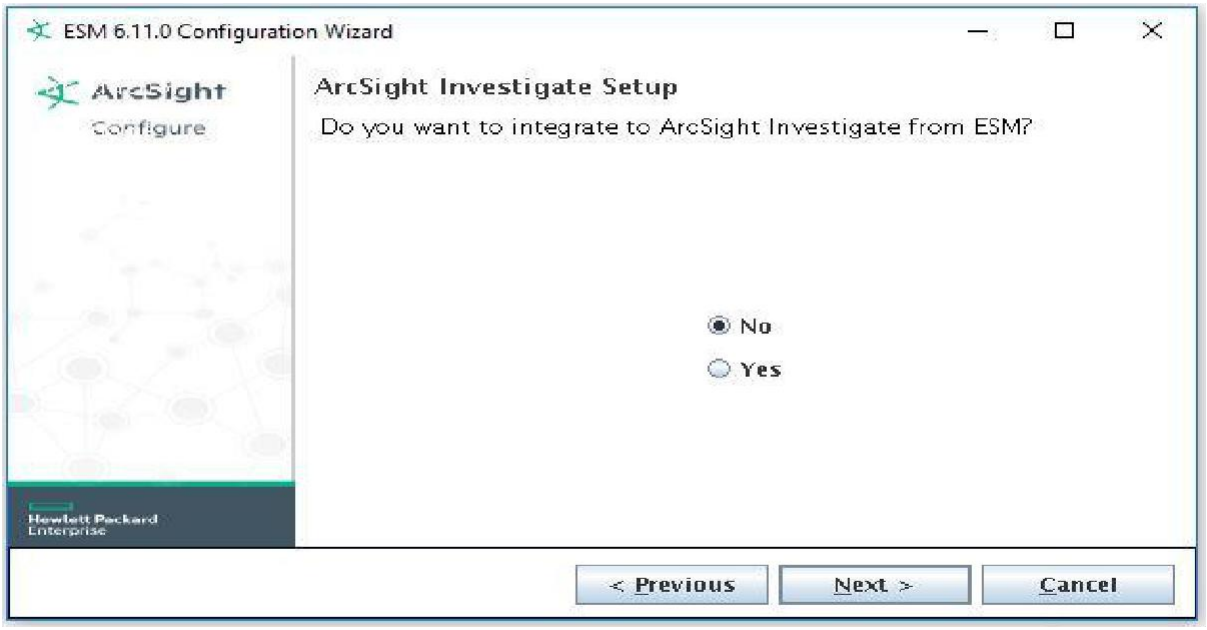
Mention the Manager Hostname & admin credentials



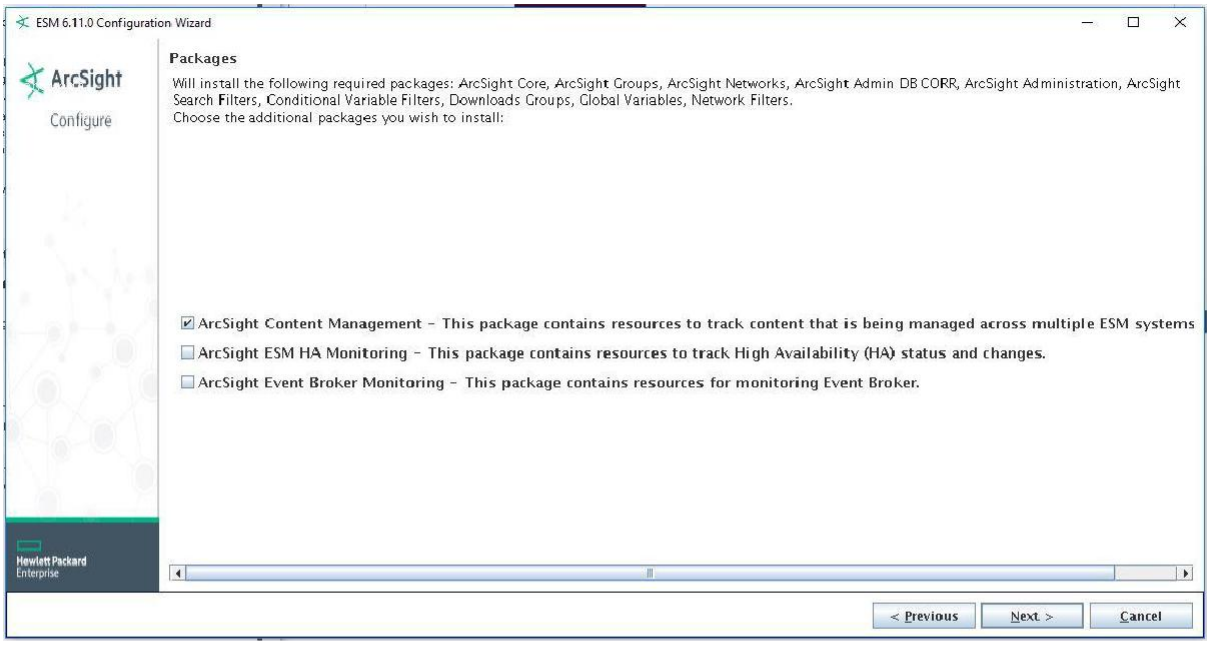
Select whether to set up connection to the Event Broker (if Event Broker is part of your implementation of ESM). Select "**No**"& click "**Next**



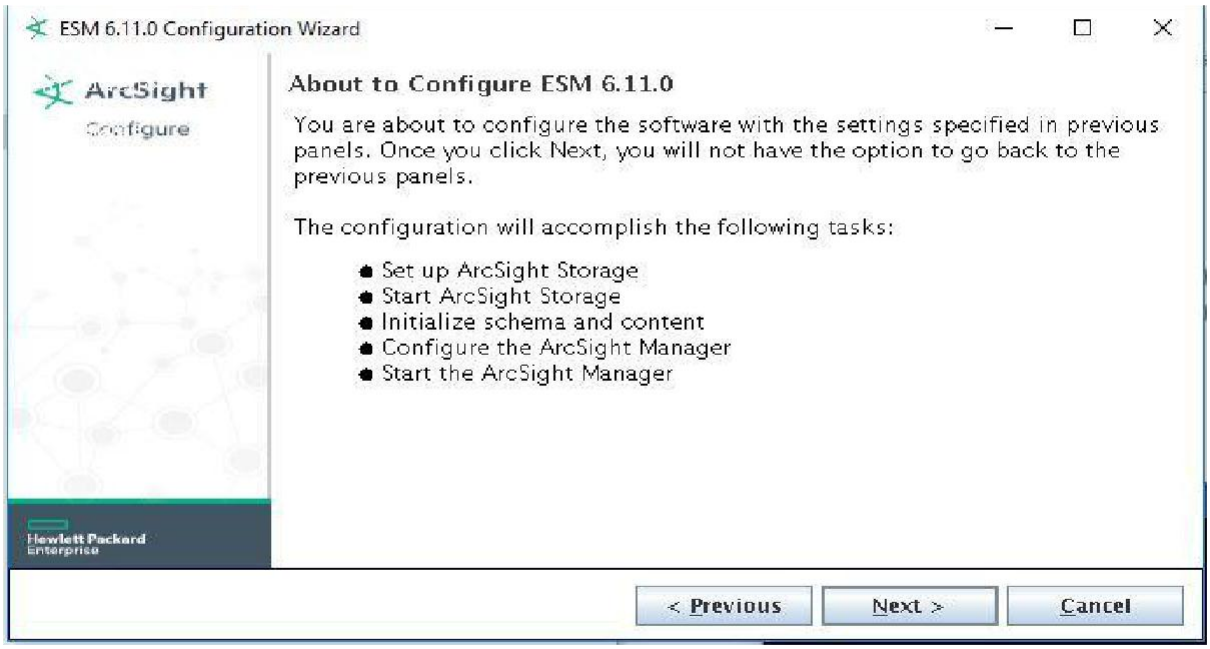
Select whether to set up ArcSight Investigate. Select Yes to enable the integration; select **“No”** to continue

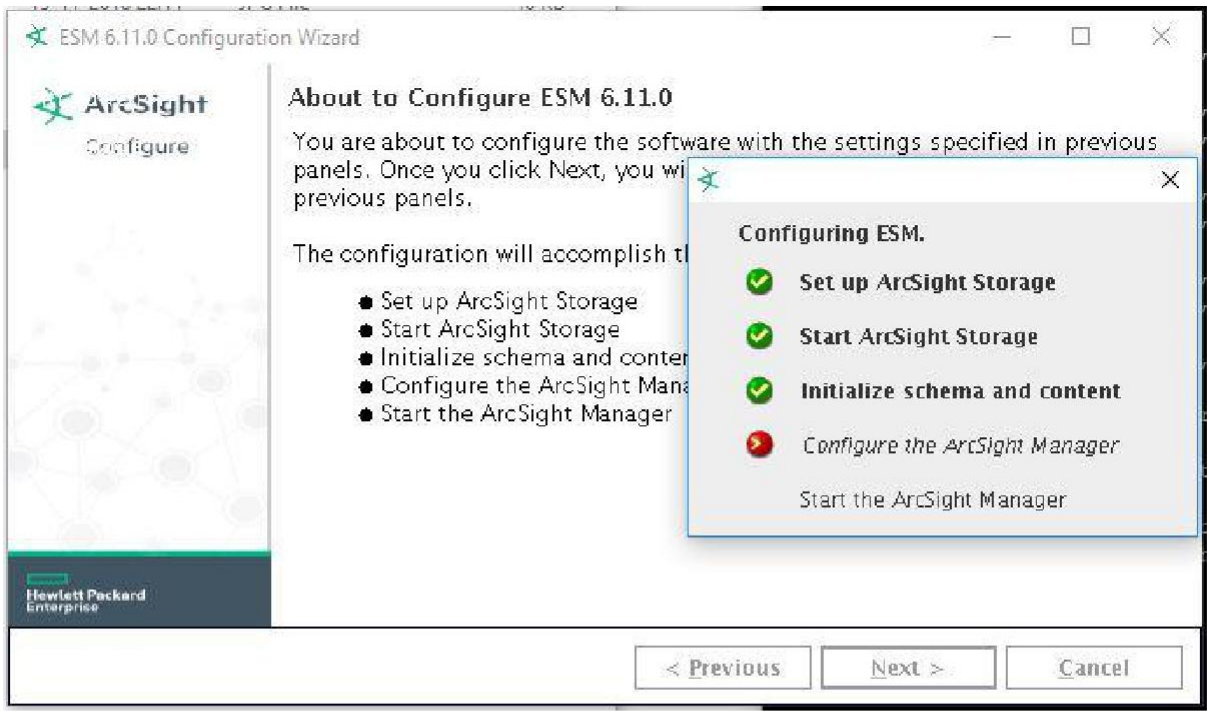


Select the optional packages that you are licensed to use

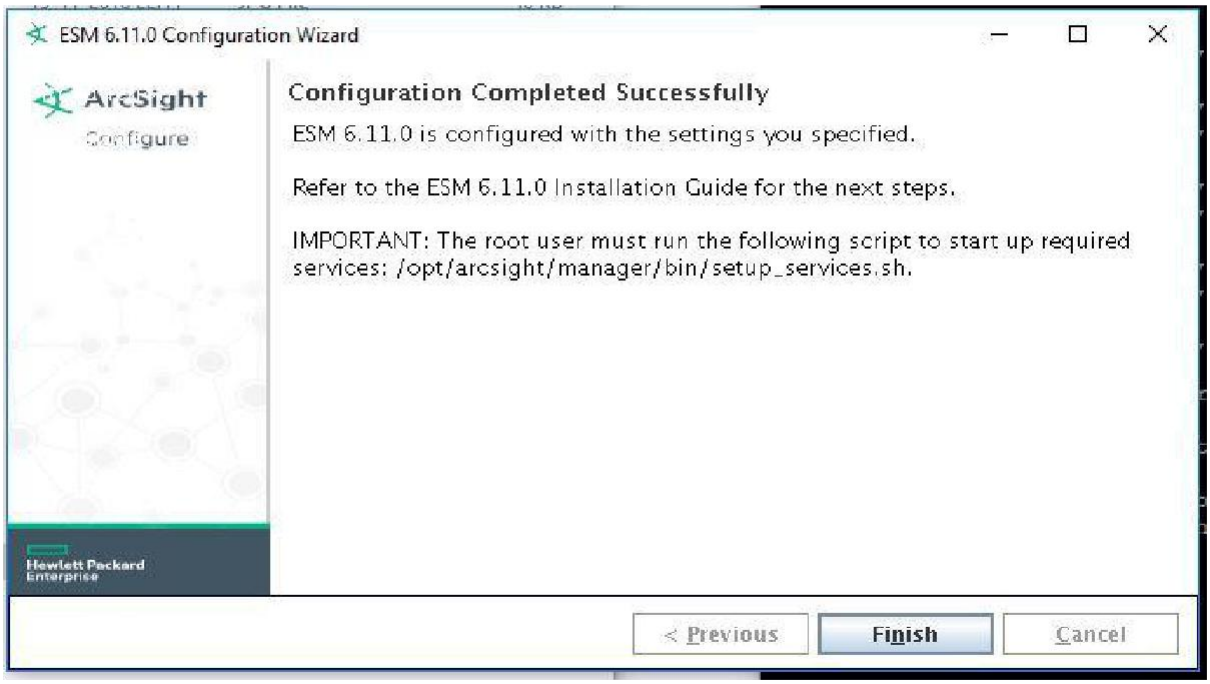


Under About to Configure ESM. Caution: Once you click **“Next”** the product is installed as specified





When the configuration says Configuration Completed Successfully, click Finish to exit



Important! This step is required in order to start the services. Log in as user root and run the following script to set up the required services:

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

Arcsight Service commands:

- /etc/init.d/arcsight_services status all
- /etc/init.d/arcsight_services start | stop | restart <servicename>

```
[arcsight@dcesmtest ~]$ /etc/init.d/arcsight_services status all
Build versions:
        esm:6.11.0.2339.0(BE2339)
        storage:6.11.0.1887.0(BL1887)
        process management:6.11.0-2149
        installer:6.11.0-2149

aps service is available
execprocsvc service is available
logger_httpd service is available
logger_servers service is available
logger_web service is available
manager service is available
mysqld service is available
postgresql service is available
```

Module – 4

- ESM Console Overview
- Active Channel
- Field sets
- Filter

Describe the ArcSight event schema Use of Logical Operators

ESM Console Overview

Describe an Active

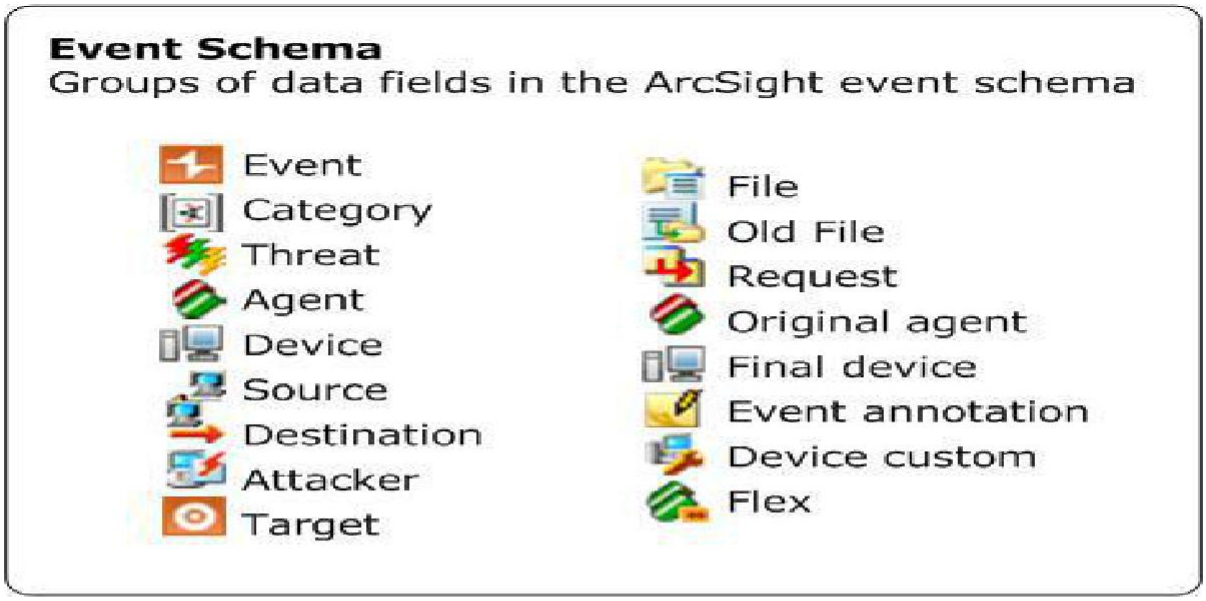
Channel Describe what a

field set is Define a filter

Describe the purpose of a filter

ArcSight Event Schema:

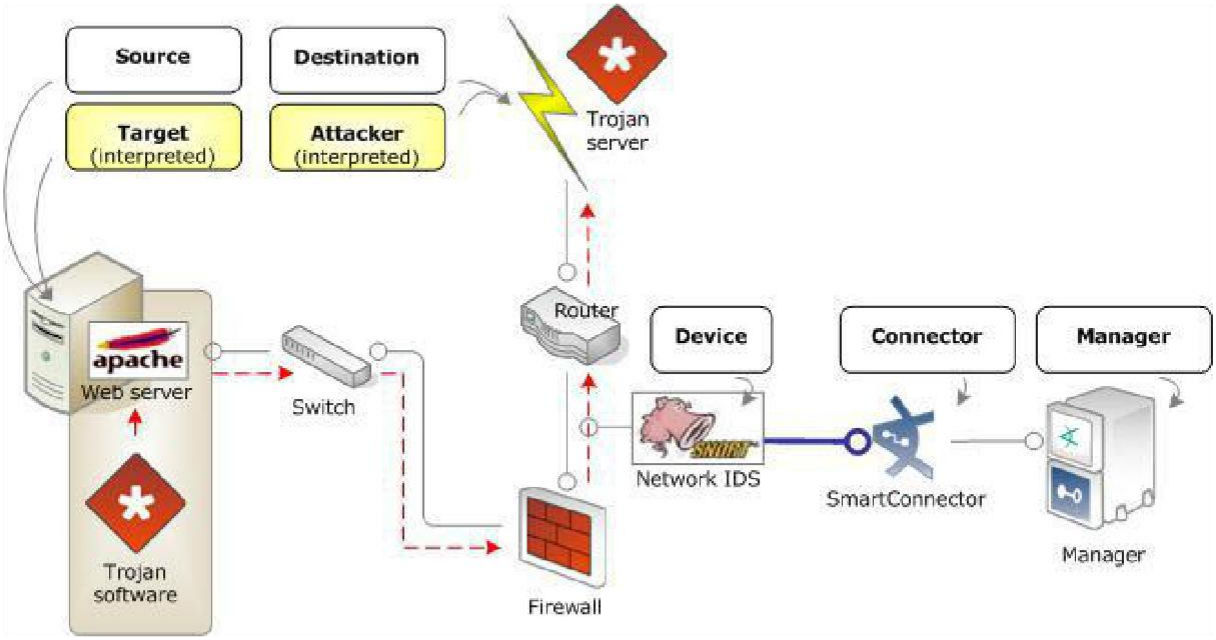
- The ESM event schema is the culmination of the normalization process, and the backbone of the data structure that drives ESM correlation
- The data collected from devices in a network is parsed into ESM's normalized schema.
- 400+ data fields in the schema are divided into 17 groups



- Event(root) - General information about the event managerReciptTime,endTime etc.
- Category - Assigned by smart connector
    - Object, Behavior, Outcome, Technique, Device Group, and Significance
- Threat - ESM's assessment of how important it is this event.
- Agent - SmartConnector that reported this event to the Manager
- Device - Describes characteristics of the sensor that reports the event to SmartConnector
- Source - Origin of the network traffic.
- Destination - Receiver of the network traffic.
- Attacker - An asset that initiated the action.
- Target - An asset that is the intended focal point of the action.
- File - Current state of an operating system file
- Old File - Previous state of an operating system file
- Request - Attributes of a request for some action
- Eg an HTTP GET or a database query
- Original agent - The SmartConnector that originally received the event.
- Final device - Last device to process an event before transmitted to SmartConnector

- Event annotation - User workflow assignments
- Device custom - Reserved for attributes specific to the device
- Flex - Used for extra data points

Source/Destination, Attacker/Target: A Trojan Attack:

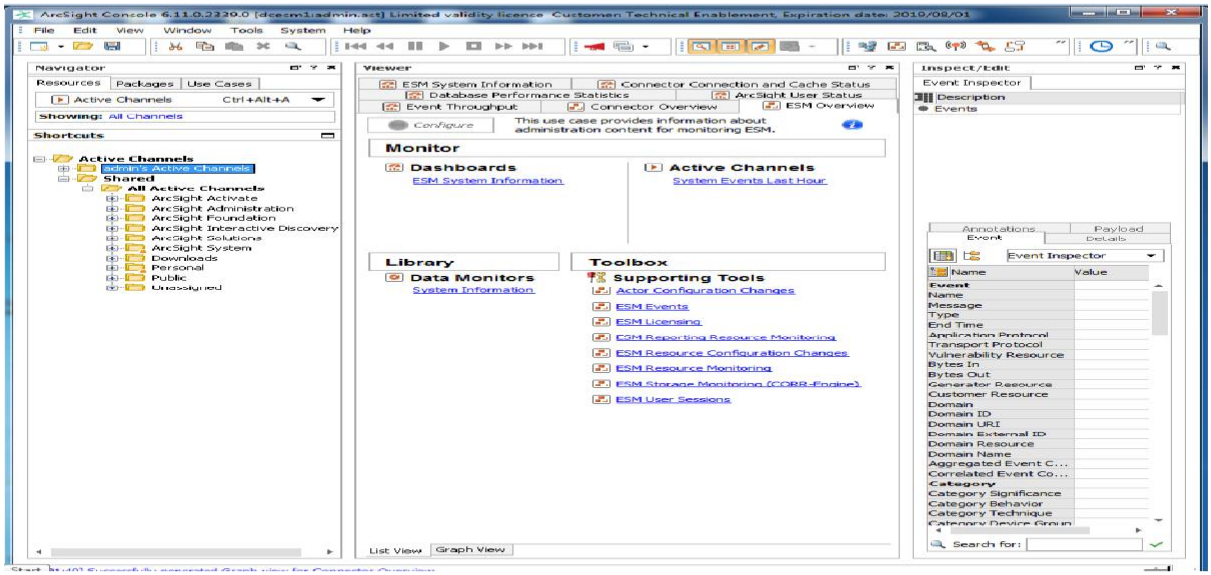


ESM Console:

There are 3 panels on the Console

- Navigator penal
- Viewer Panel
- Inspect/Edit Panel

Console:



Boolean Logic:

- IP & Port = Send events that match the IP Address AND the Port specified
- IP || Port = Send events that match the IP Address OR the Port specified
- IP != Port = Send events that DO NOT match either the IP Address or the Port specified

Type of Active Channels:

Using Active channel resource we can view the events on the viewer panel of the ESM console also download the events on the CSV format

There are two types of Active Channels based on time

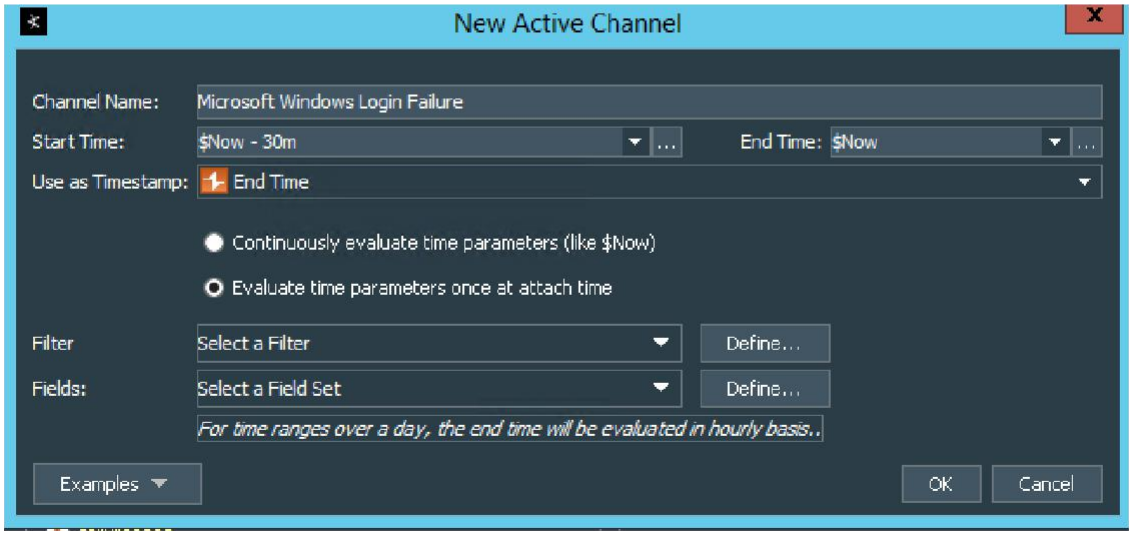
- Evaluate continuously
- Evaluate once at an attached time

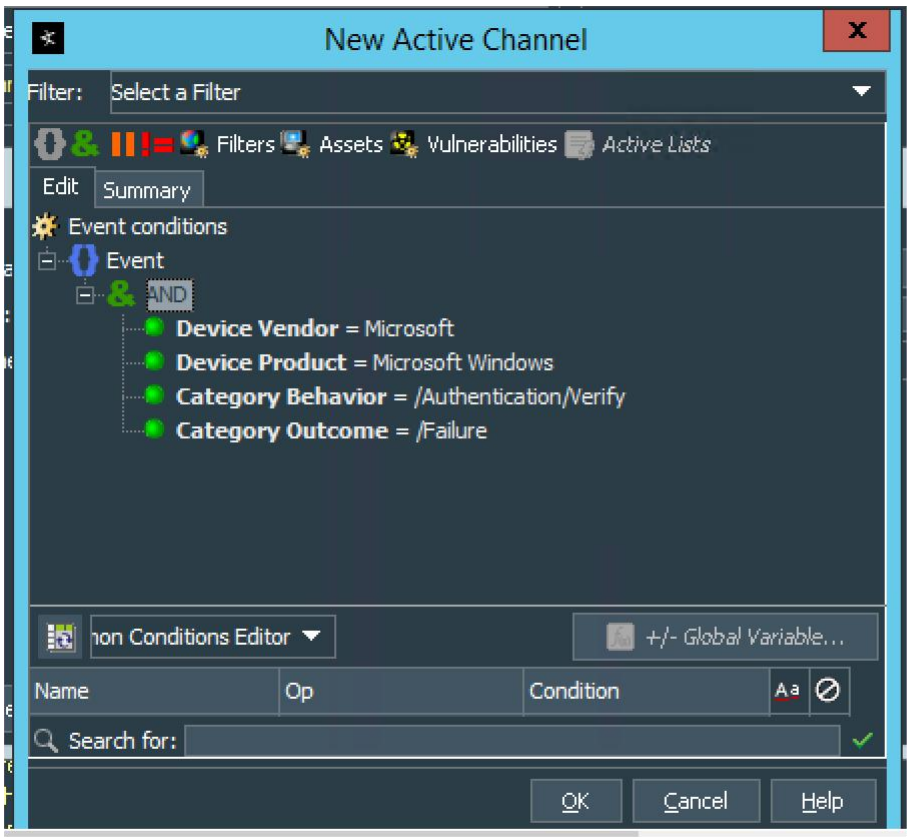
Active Channe:

- Allows you to view event data
- Allows you to perform monitoring and investigation activities
- 3 Types
    - Live Channels – Displays continuously refreshed live event data
    - Rules Channels – Displays replay events for testing rules
    - Resource Channels - Display the status of certain resources. Eg - assets in your network model
- The flash icon in the first column indicates a correlation event generated by a rule.

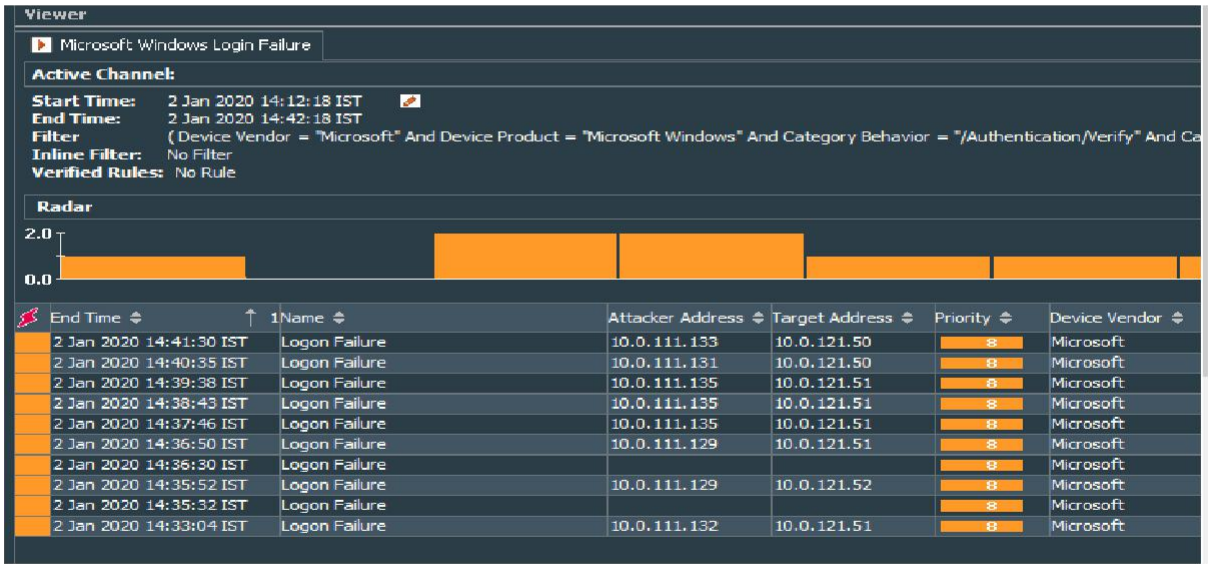
Active Chanel for Windows Logs:

- Create Active channel for Windows Login failure events



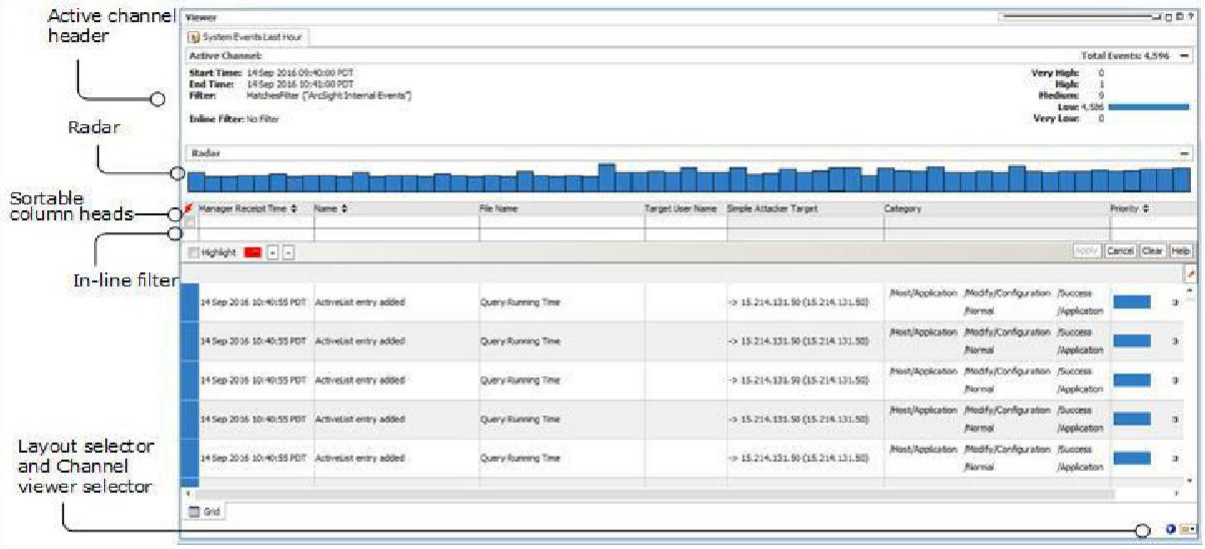


How events appears on the Active Channel:



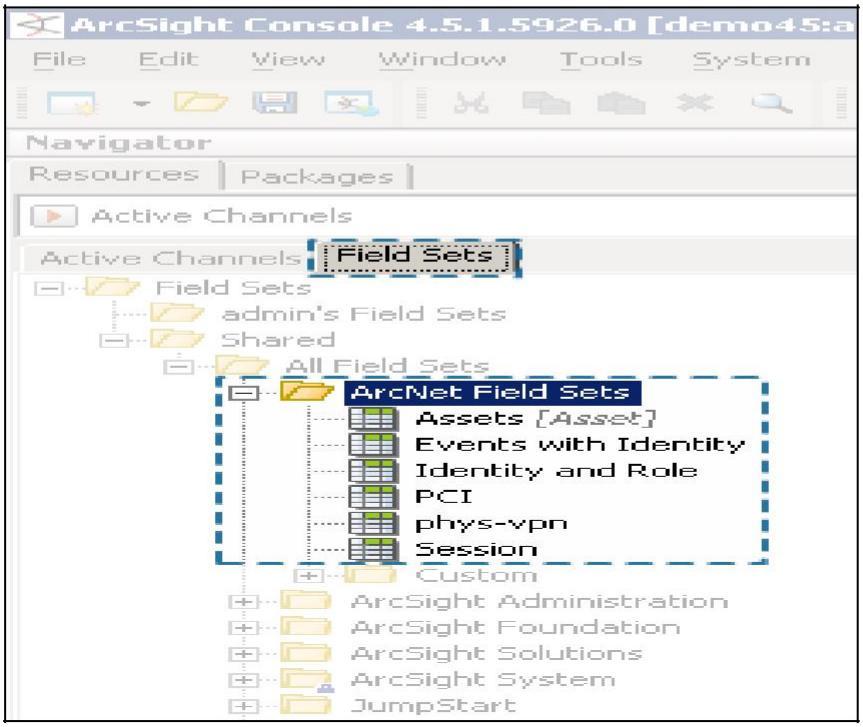
End Time	Name	Attacker Address	Target Address	Priority	Device Vendor
2 Jan 2020 14:41:30 IST	Logon Failure	10.0.111.133	10.0.121.50	8	Microsoft
2 Jan 2020 14:40:35 IST	Logon Failure	10.0.111.131	10.0.121.50	8	Microsoft
2 Jan 2020 14:39:38 IST	Logon Failure	10.0.111.135	10.0.121.51	8	Microsoft
2 Jan 2020 14:38:43 IST	Logon Failure	10.0.111.135	10.0.121.51	8	Microsoft
2 Jan 2020 14:37:46 IST	Logon Failure	10.0.111.135	10.0.121.51	8	Microsoft
2 Jan 2020 14:36:50 IST	Logon Failure	10.0.111.129	10.0.121.51	8	Microsoft
2 Jan 2020 14:36:30 IST	Logon Failure			8	Microsoft
2 Jan 2020 14:35:52 IST	Logon Failure	10.0.111.129	10.0.121.52	8	Microsoft
2 Jan 2020 14:35:32 IST	Logon Failure			8	Microsoft
2 Jan 2020 14:33:04 IST	Logon Failure	10.0.111.132	10.0.121.51	8	Microsoft

Active Channel – Display Elements:



Field Sets:

- Collection of fields displayed in an Active Channel
- Used to control columns displayed in Active Channel

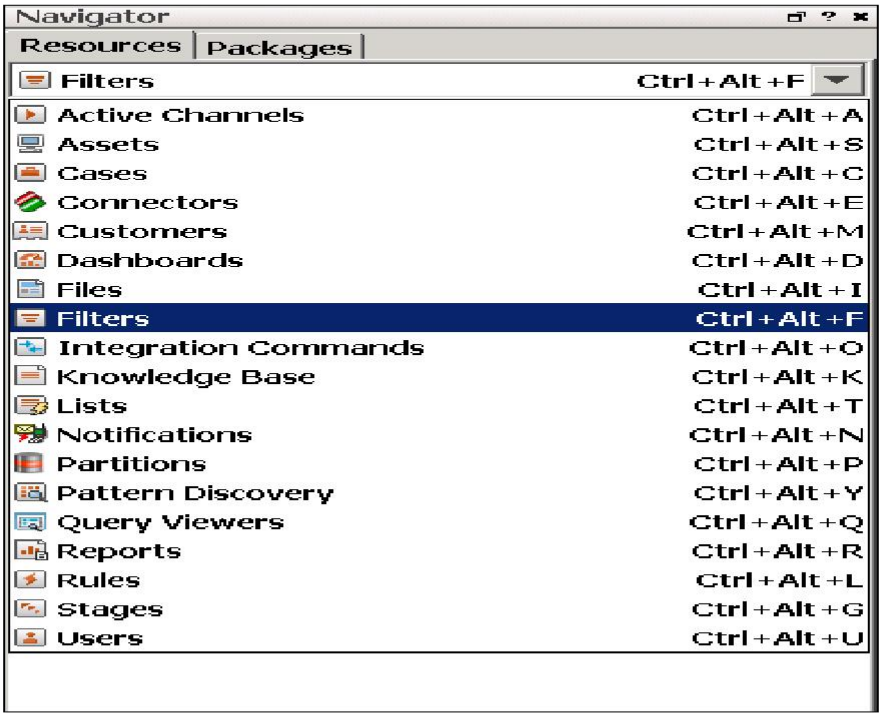


Time Stamps:

- Start Time - Time at which the event began
- End Time - Time at which the event ended
- Device Receipt Time - Timestamp applied by the data source on receipt of the event
- Agent Receipt Time - Timestamp applied by the ArcSight Smart Connectors
- Manager Receipt Time - Timestamp applied by the ESM Manager
-

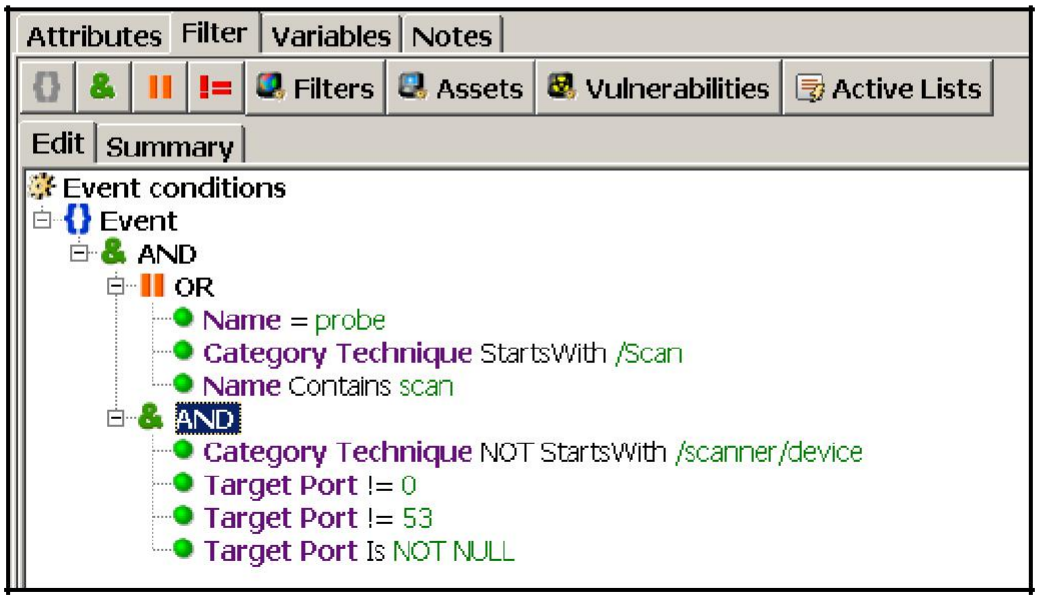
Filters:

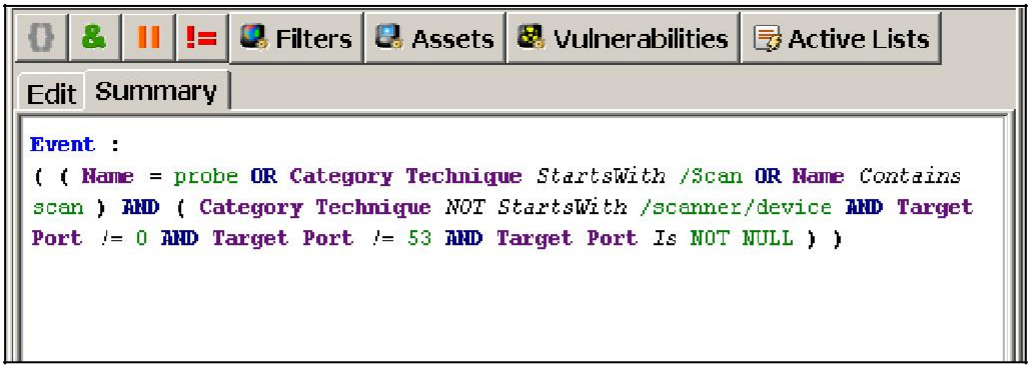
- A set of Boolean conditions that focus on particular event attributes
- Available under Navigator - Resources tree as independent resources
- Can be applied in two ways:
  - By ESM Manager
  - By Connectors

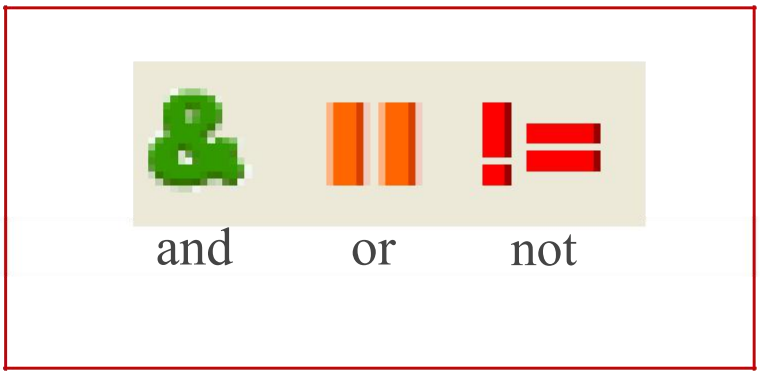


Filter Editor:

- Filter condition statements are constructed using ArcSight's Boolean Logic Editor.







Applying Filters:

- In ESM
- In Rules and Data Monitors during Correlation
- In Active Channels and Query Viewers during Monitoring and Investigation
- In Reports and Queries during Reporting and Analysis

- In Connector
  - Events that match conditions are forwarded to the destination
  - Non-matching events are discarded.

LAB:

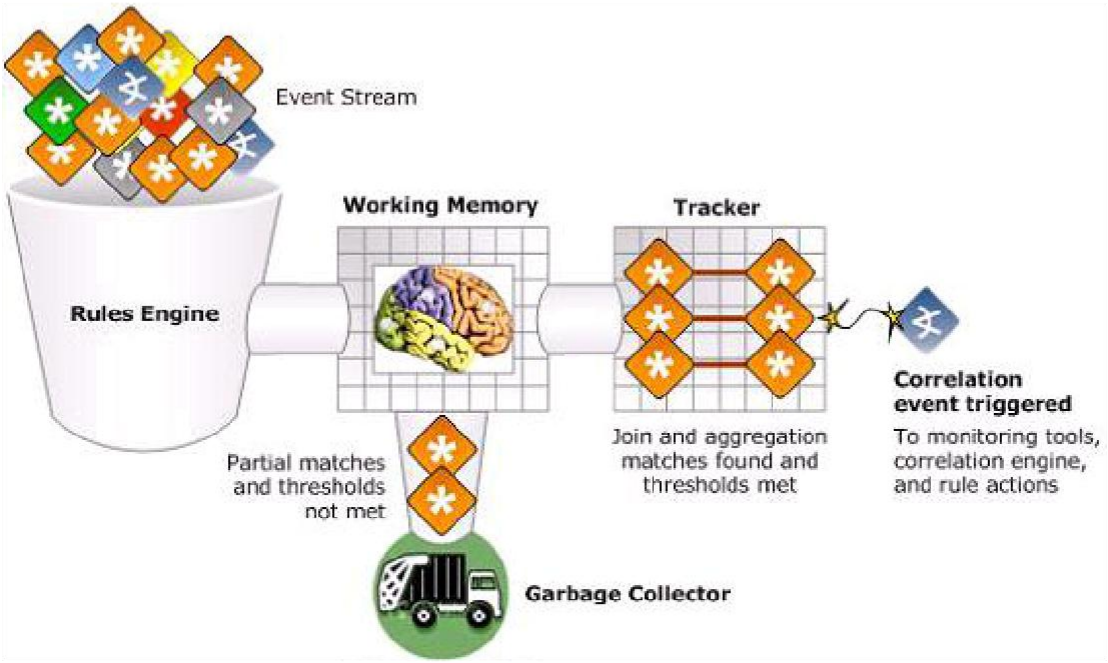
- Create Active channel
- Create Field Sets
- Create filters and apply it to active channel

Module 5

- Rules
- Active list
- Query and query viewers
- Report

Rules Overview:

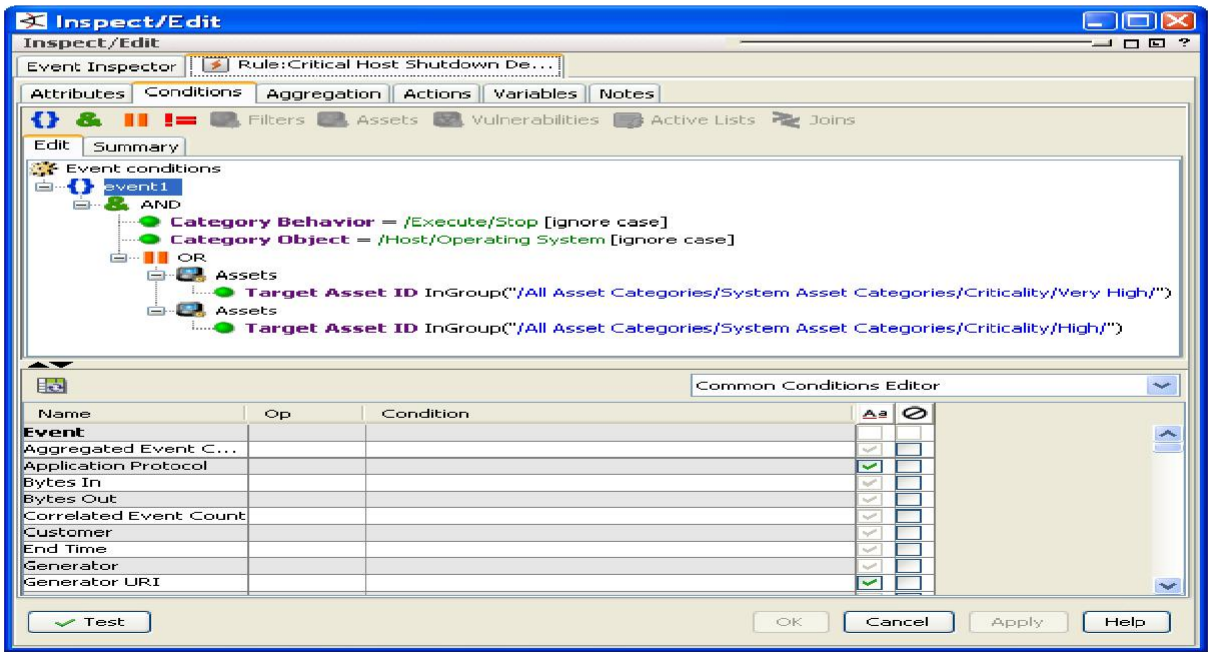
- Evaluate real-time and historical events against a set of conditions
- Rules engine holds matches in working memory
- If all conditions are met within the time thresholds, a correlation event is triggered



Rules: Attribute Relationships:

Rules – Edit:

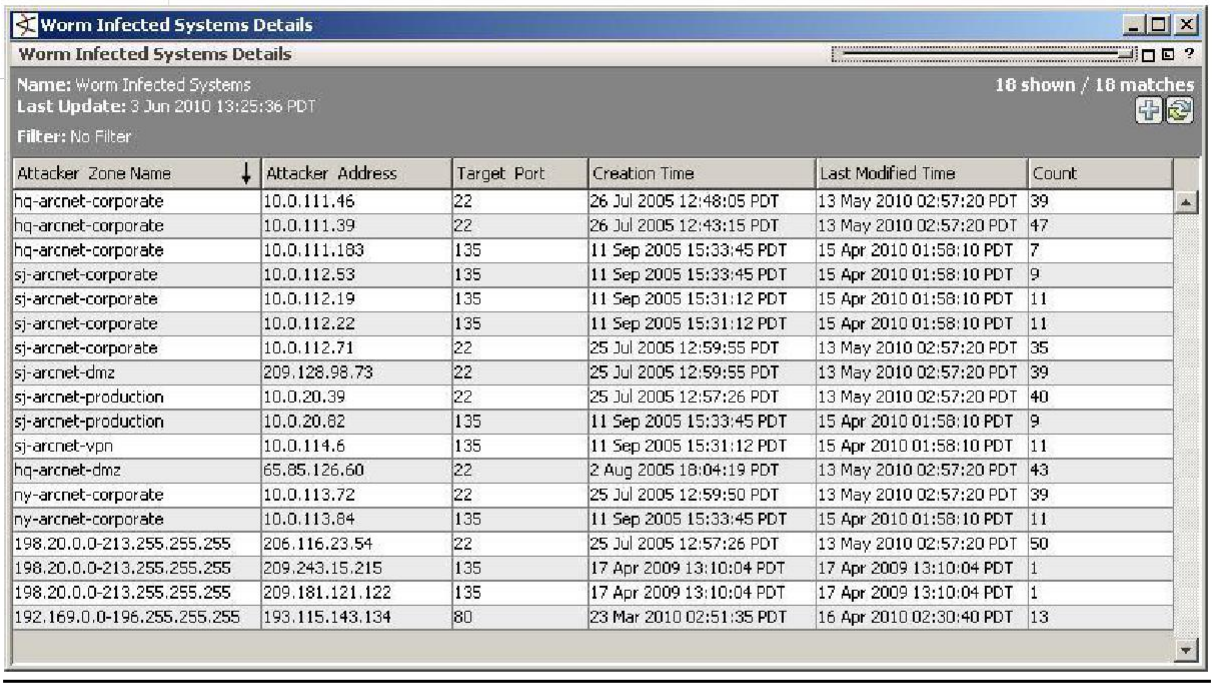
Rules Must be activated (save or linked into the real time rules folder)!!



Rules can be CPU-intensive when they make use of many filters or filters that are complex

Active Lists:

- A configurable data store that can hold information derived from events or other sources.
- A data source for other resources such as Query Viewers and Reports.
- Rules can create, read, and remove entries within Active Lists dynamically.


Worm Infected Systems Details

Worm Infected Systems Details

Name: Worm Infected Systems
Last Update: 3 Jun 2010 13:25:36 PDT
Filter: No Filter

18 shown / 18 matches

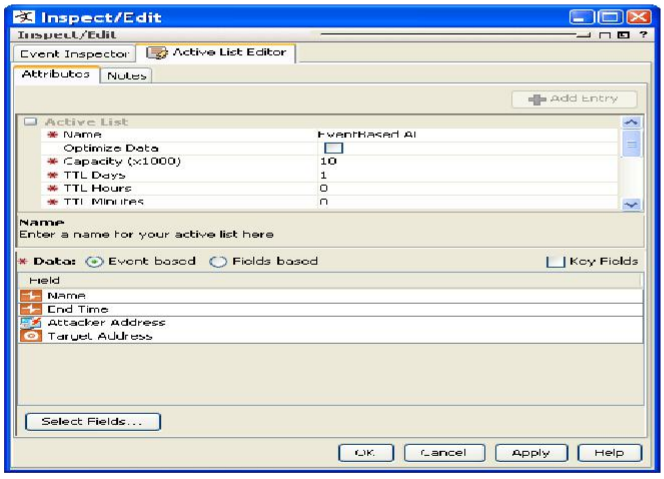
Attacker Zone Name	Attacker Address	Target Port	Creation Time	Last Modified Time	Count
hq-arcnet-corporate	10.0.111.46	22	26 Jul 2005 12:48:05 PDT	13 May 2010 02:57:20 PDT	39
hq-arcnet-corporate	10.0.111.39	22	26 Jul 2005 12:43:15 PDT	13 May 2010 02:57:20 PDT	47
hq-arcnet-corporate	10.0.111.183	135	11 Sep 2005 15:33:45 PDT	15 Apr 2010 01:58:10 PDT	7
sj-arcnet-corporate	10.0.112.53	135	11 Sep 2005 15:33:45 PDT	15 Apr 2010 01:58:10 PDT	9
sj-arcnet-corporate	10.0.112.19	135	11 Sep 2005 15:31:12 PDT	15 Apr 2010 01:58:10 PDT	11
sj-arcnet-corporate	10.0.112.22	135	11 Sep 2005 15:31:12 PDT	15 Apr 2010 01:58:10 PDT	11
sj-arcnet-corporate	10.0.112.71	22	25 Jul 2005 12:59:55 PDT	13 May 2010 02:57:20 PDT	35
sj-arcnet-dmz	209.128.98.73	22	25 Jul 2005 12:59:55 PDT	13 May 2010 02:57:20 PDT	39
sj-arcnet-production	10.0.20.39	22	25 Jul 2005 12:57:26 PDT	13 May 2010 02:57:20 PDT	40
sj-arcnet-production	10.0.20.82	135	11 Sep 2005 15:33:45 PDT	15 Apr 2010 01:58:10 PDT	9
sj-arcnet-vpn	10.0.114.6	135	11 Sep 2005 15:31:12 PDT	15 Apr 2010 01:58:10 PDT	11
hq-arcnet-dmz	65.85.126.60	22	2 Aug 2005 18:04:19 PDT	13 May 2010 02:57:20 PDT	43
ny-arcnet-corporate	10.0.113.72	22	25 Jul 2005 12:59:50 PDT	13 May 2010 02:57:20 PDT	39
ny-arcnet-corporate	10.0.113.84	135	11 Sep 2005 15:33:45 PDT	15 Apr 2010 01:58:10 PDT	11
198.20.0.0-213.255.255.255	206.116.23.54	22	25 Jul 2005 12:57:26 PDT	13 May 2010 02:57:20 PDT	50
198.20.0.0-213.255.255.255	209.243.15.215	135	17 Apr 2009 13:10:04 PDT	17 Apr 2009 13:10:04 PDT	1
198.20.0.0-213.255.255.255	209.181.121.122	135	17 Apr 2009 13:10:04 PDT	17 Apr 2009 13:10:04 PDT	1
192.169.0.0-196.255.255.255	193.115.143.134	80	23 Mar 2010 02:51:35 PDT	16 Apr 2010 02:30:40 PDT	13

Active List Types:

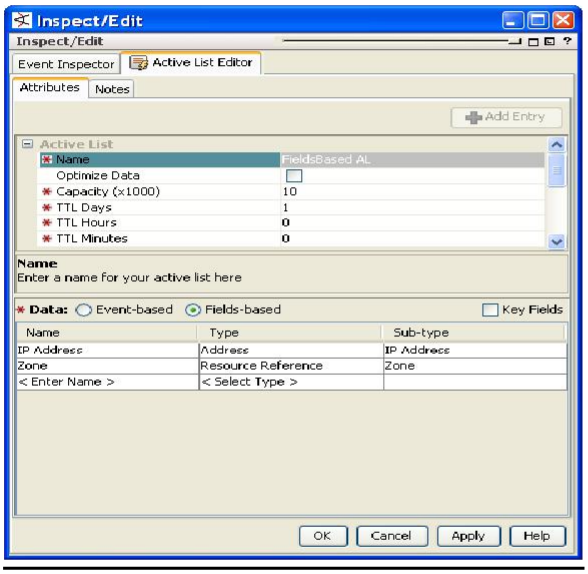
Capacity - maximum number of entries to be stored in the Active List

Time To Live (in Days, Hours, and Minutes) - time after which an entry will be removed, if the entry hasn't since been updated or reinserted

<u>Event-based</u>

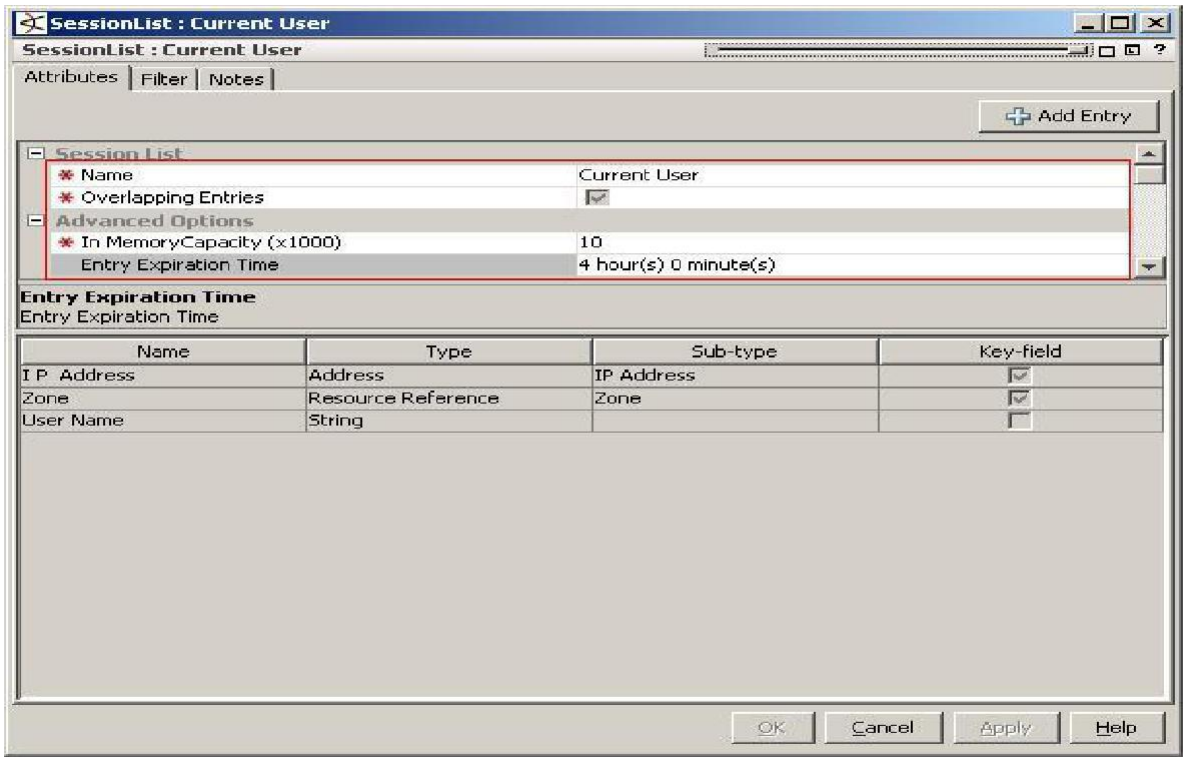


Fields-based



Session Lists

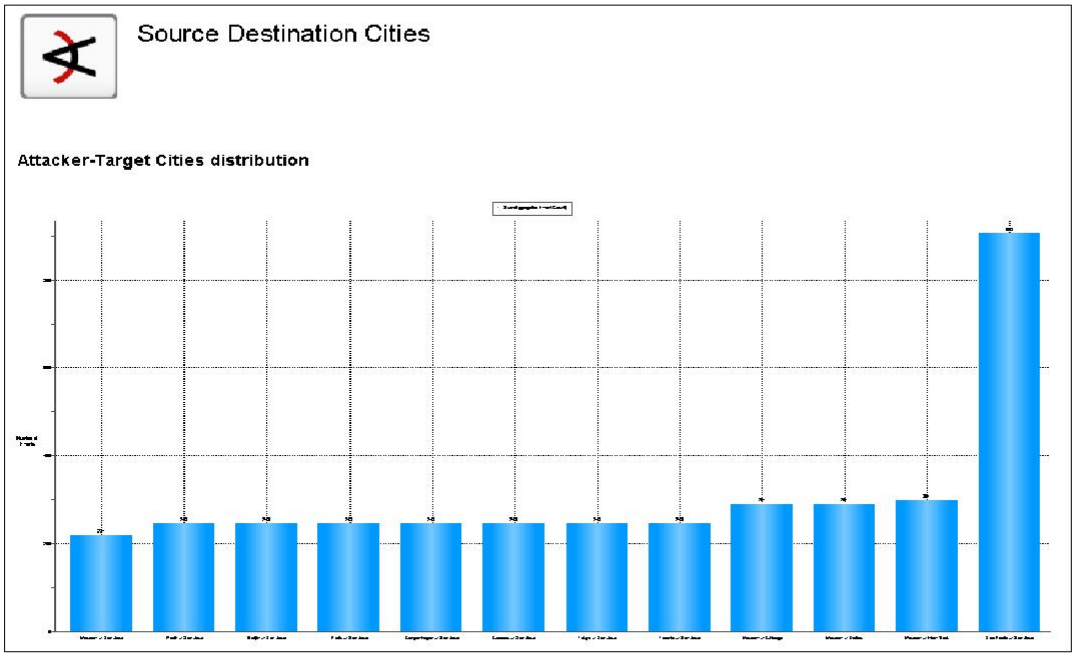
- Same as Active Lists but differ in below
  - Session Lists are always Fields-based.
  - Active Lists cannot have duplicate entries while Session Lists can.



Lab Workshop

Reports

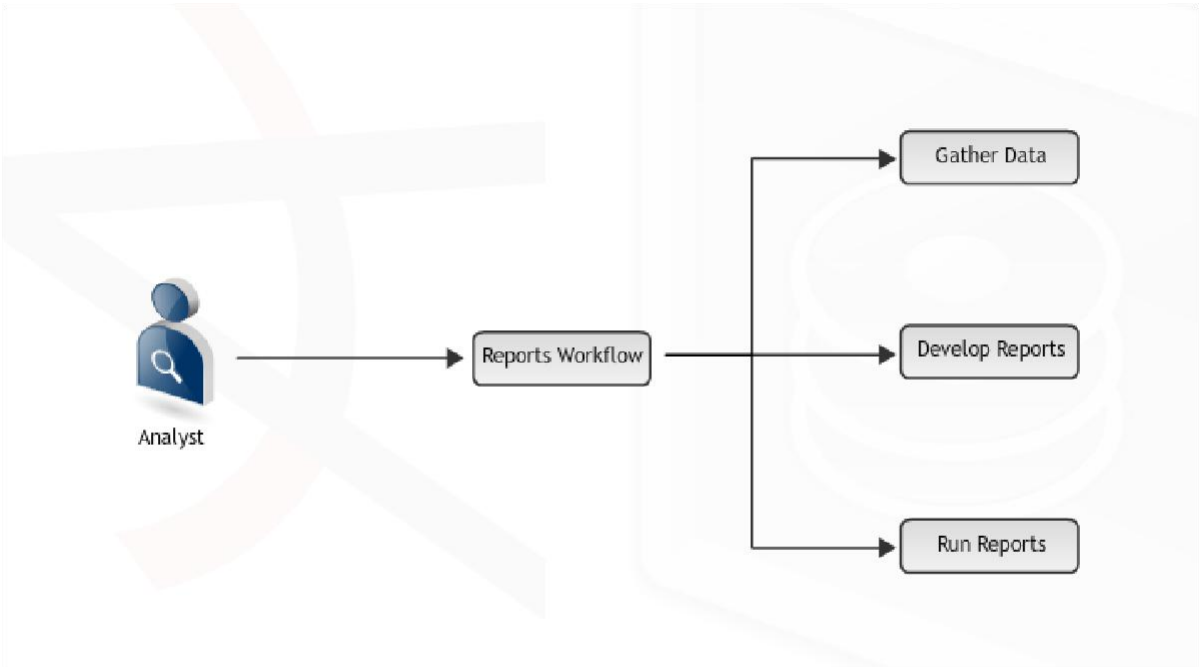
- Captured views or summaries of data
  - PDF, Excel, RTF, and CSV
- Running Reports
  - Can be scheduled to run at specific time intervals
  - Can be run on demand



Report Workflow:

Steps in the report workflow:

- Gather report data to be included (with a Query resource)
  - Active lists
  - Session lists
  - Notifications
  - Cases
  - Assets
  - Events
- Develop report
- Run report
  - Optionally schedule execution



Defining Data Sources - Query Resource:

Steps in the report workflow:

- Gather report data to be included (with a Query resource)
  - Active lists
  - Session lists
  - Notifications
  - Cases
  - Assets
  - Events
  - Trends
- Develop report
- Run report
  - Optionally schedule execution
  - Query results are used as inputs to Reports and Query Viewers

Query Creation:

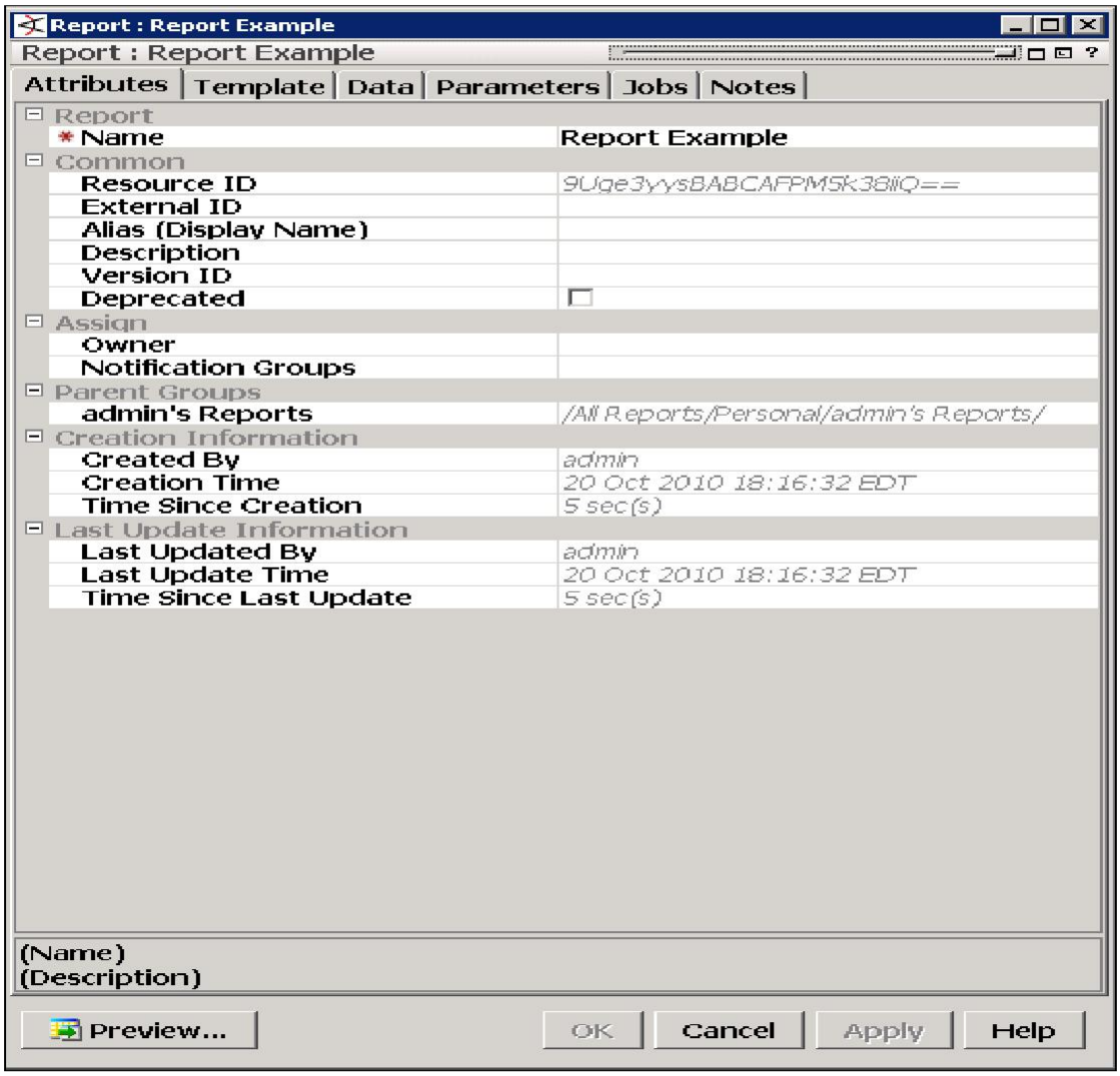
- Based on SQL logic:
  - Select
  - Group by
  - Order by
- Functions available for grouping and sorting
  - Count
  - Max
  - Min
  - Average
  - Sum

Creating a Report - Tabs Description:

During report creation, 6 tabs available:

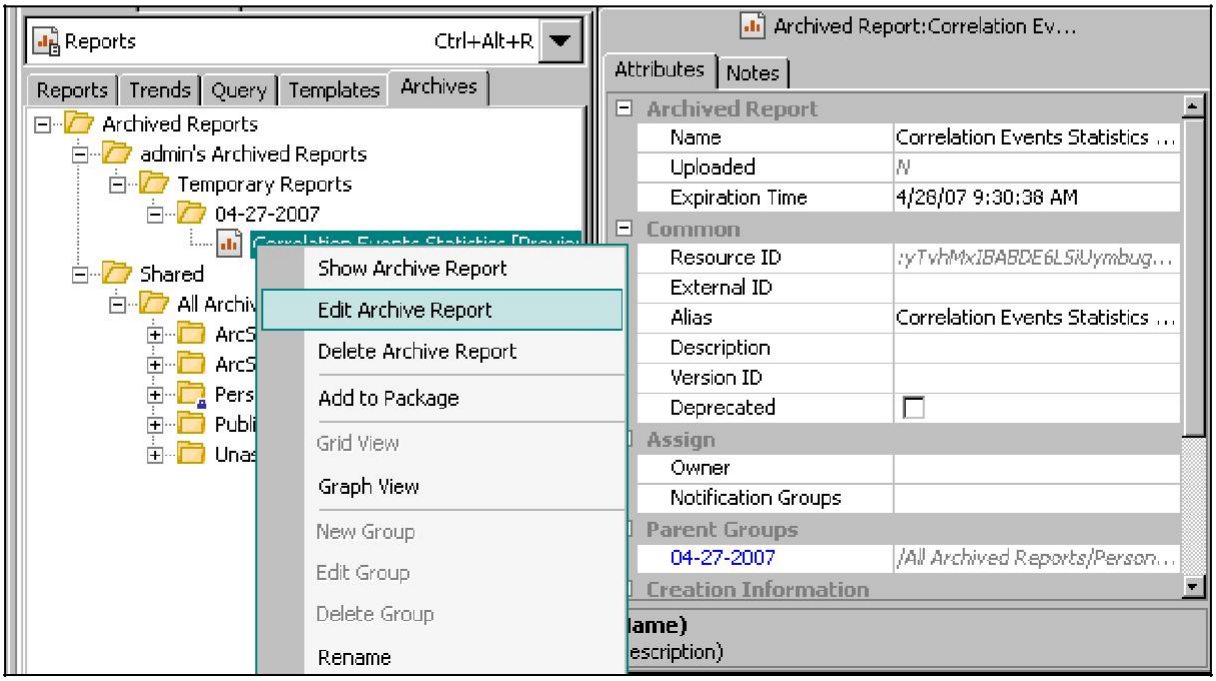
- **Attributes**: names and sets details about the report
- **Template**: provides formatting, color, labeling control and final presentation
- **Data**: selects data source: query, active list or session list; and column/field selection within the source
- **Parameters:** control query execution and report output
- **Jobs:** optionally schedules report run time(s)
- **Notes:** Use this section to add a brief report description

Creating a Report - Tabs Description:



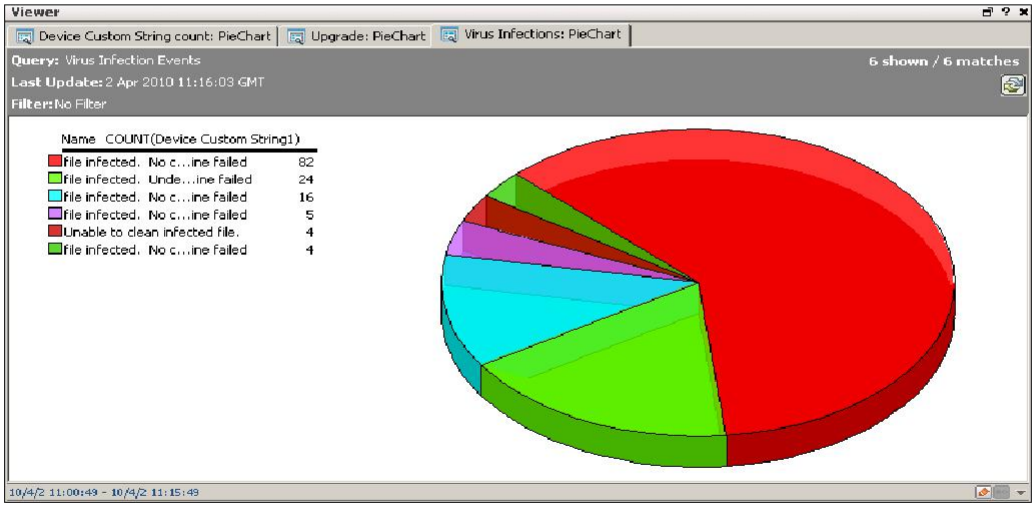
Report Archive:

- After running a report, you can save the report (archiving) to be viewed at another time



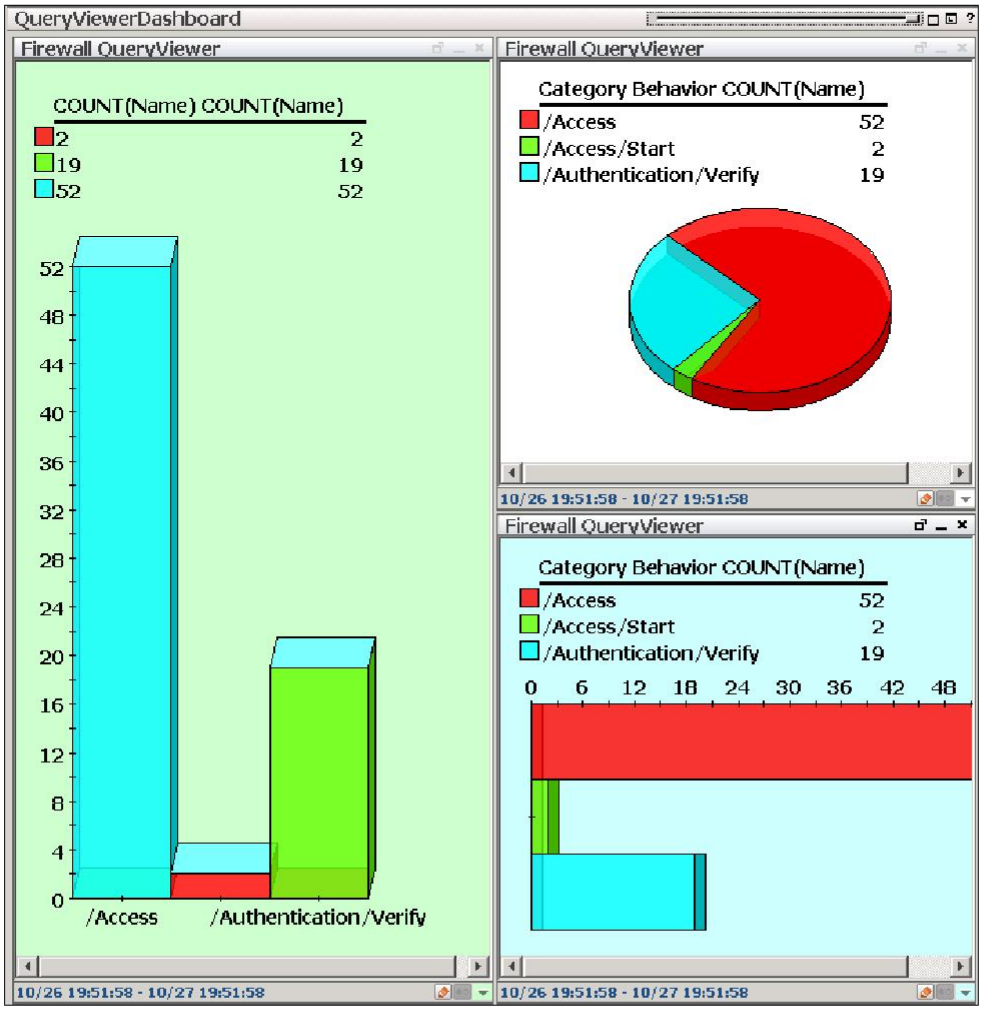
Query Viewers:

- Allows you to generate high-level summaries
- Query Viewer Reports helps to quickly share result data



Query Viewers:

- Display options available:
  - Table
  - Bar chart
  - Horizontal Bar Chart
  - Pie Chart
  - Multiple Query Viewer results can be attached to a Dashboard

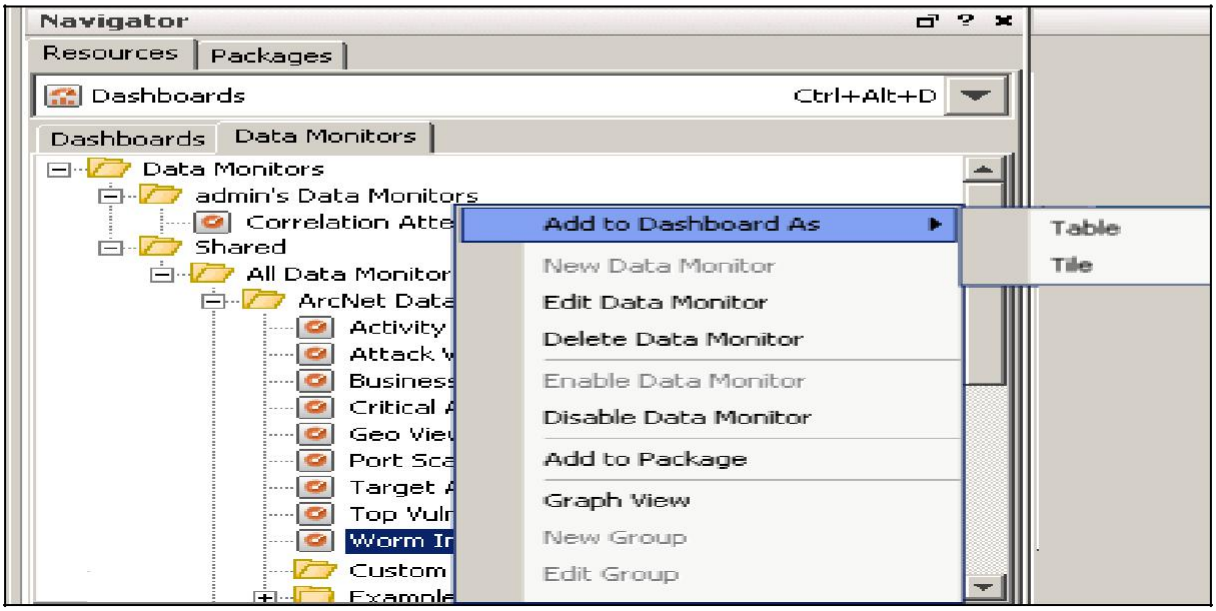


Module 6

- Creation of data monitor
- Creation of dashboard

Data Monitors:

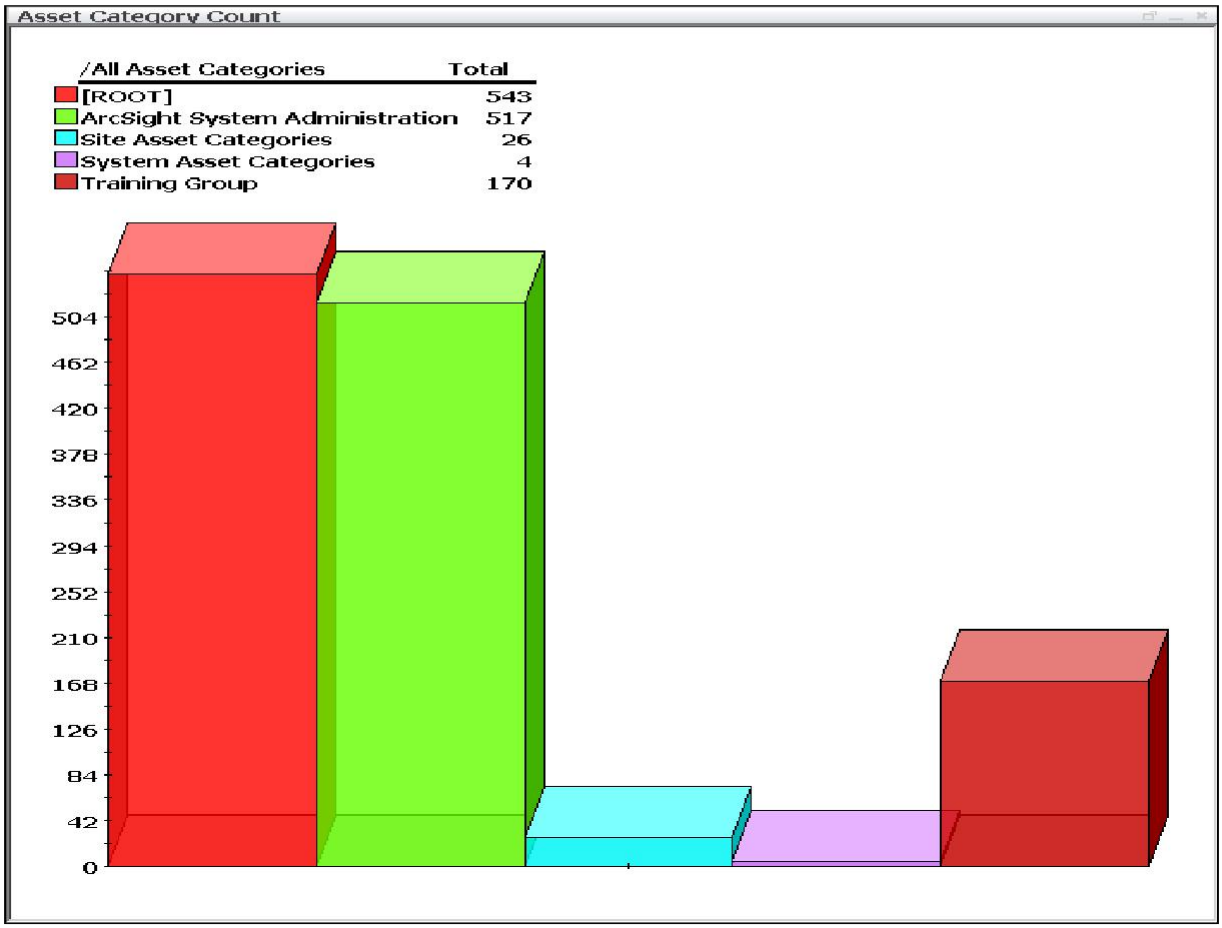
- Display summaries of events, Assets, and ESM status
- Display event data in numerous viewing layouts
- Can be added to Dashboards



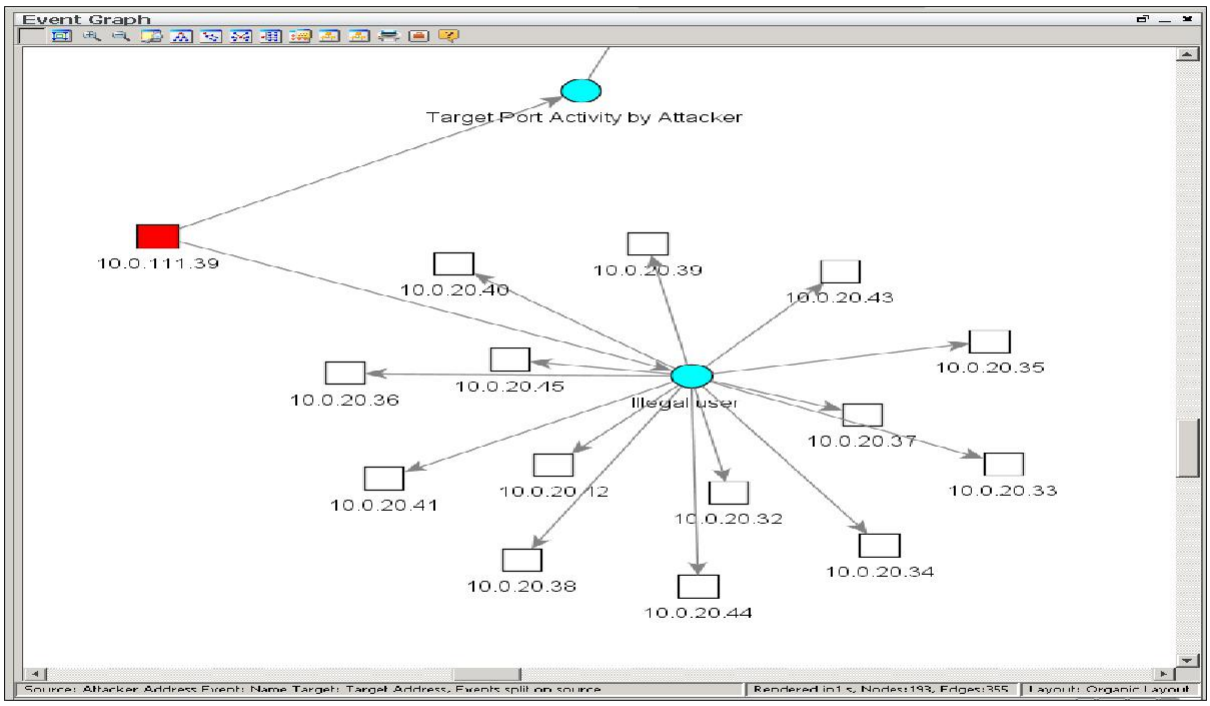
Types of Data Monitors:

- Asset Category Count
- Event Graph
- Geographic Event Graph
- Hierarchy Map
- Hourly Counts
- Last N Events
- Last State
- Top Value Counts (Bucketized)

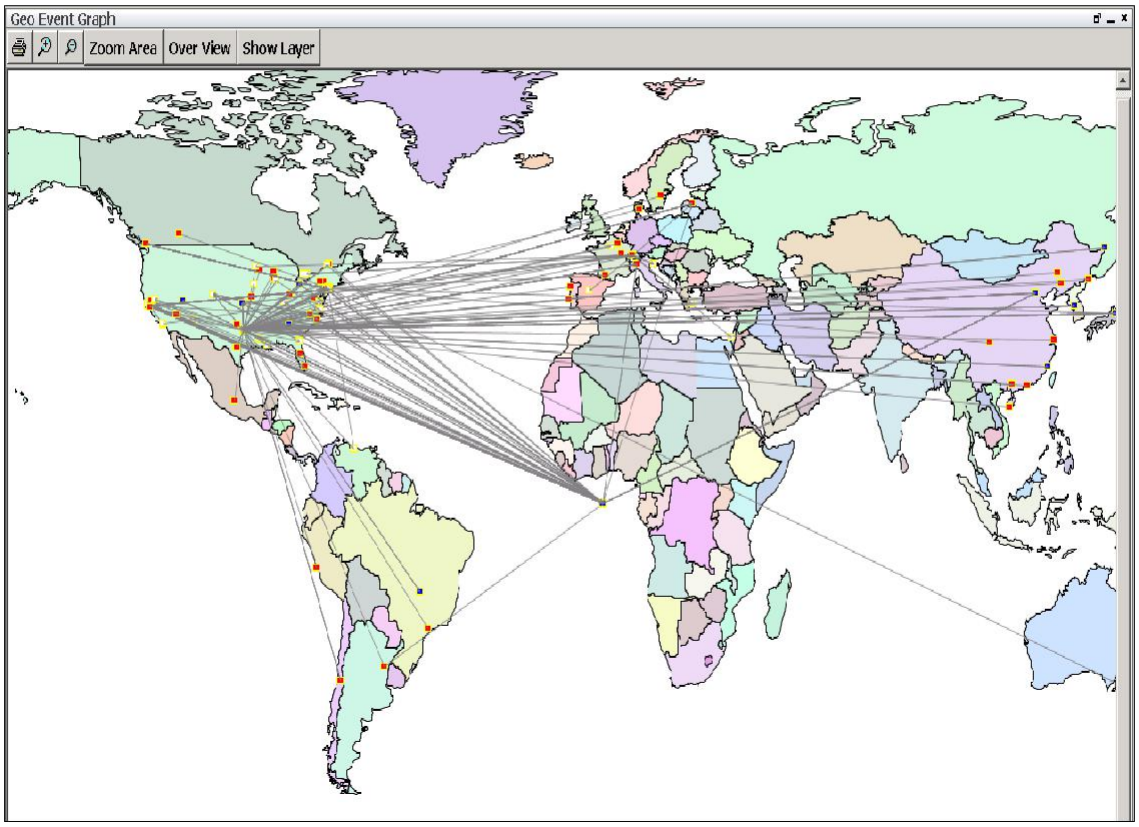
Asset Category Count



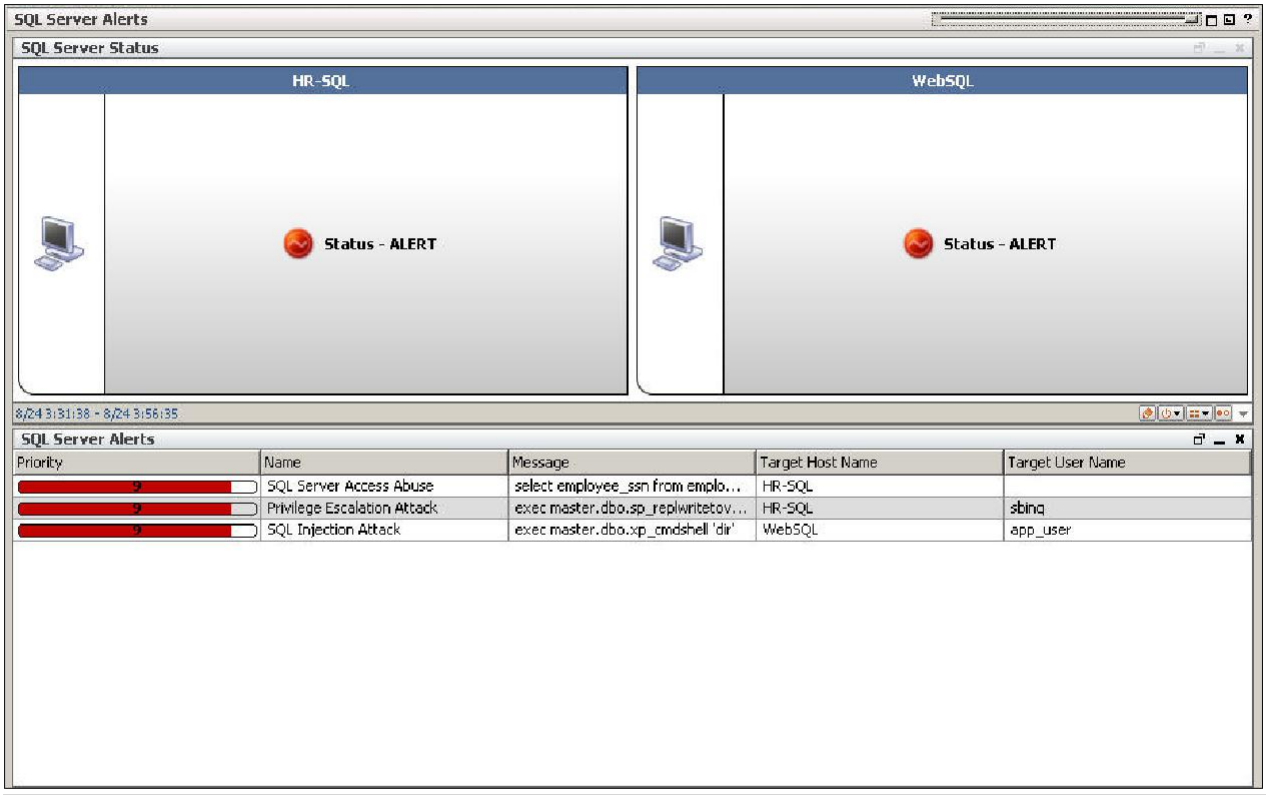
Event Graph



Geographic Event Graph

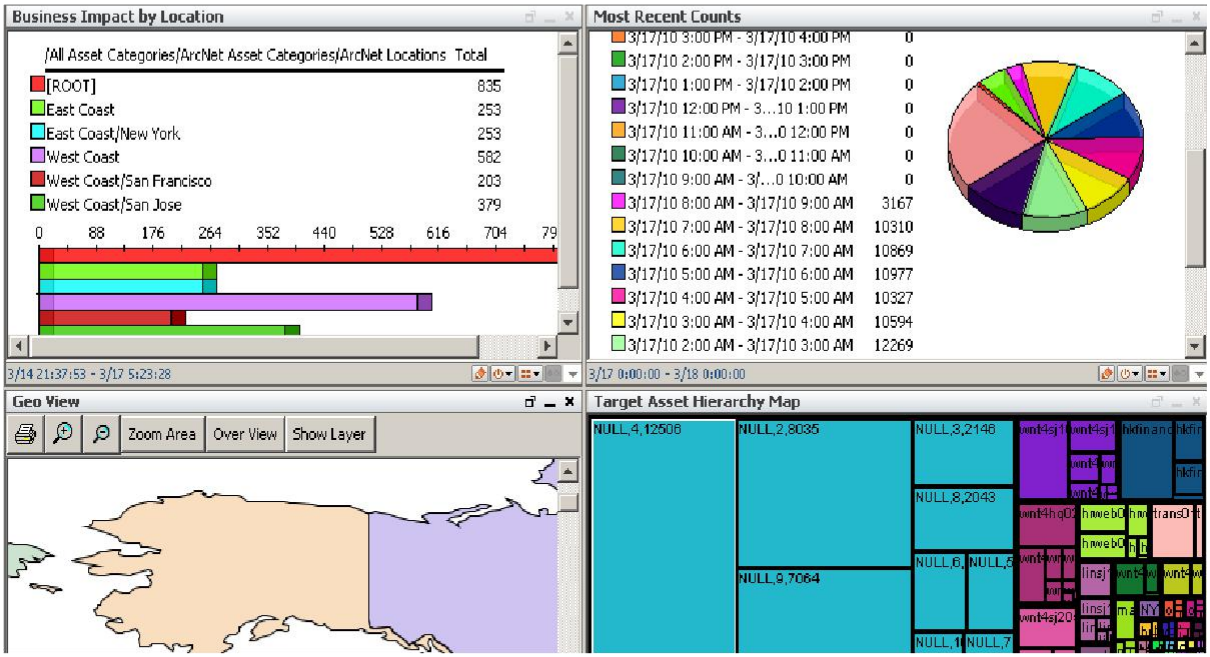


Last State



Dashboards

- Made up of Data Monitors and/or Query Viewers
- Ideal way to see event data in a variety of statistical views
- Can be loaded in two ways – using the Navigator panel or the Menu bar

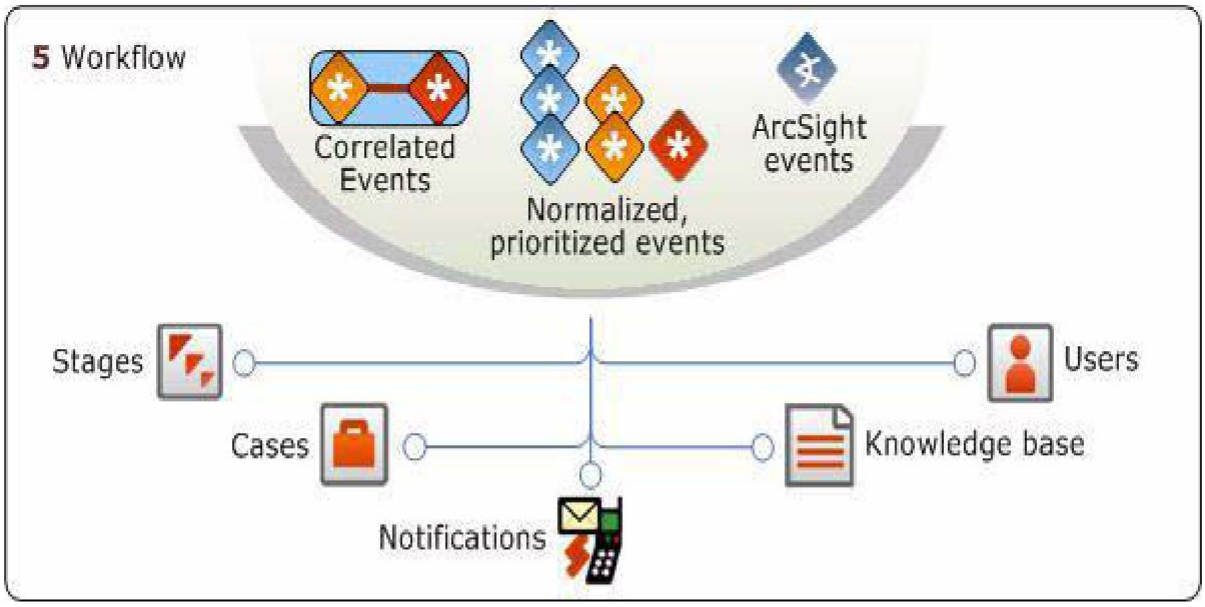


Lab Workshop

- Create the TOP Windows login failure dashboard

What is Workflow:

- Workflow - Process of informing people in the organization about incidents
- Tracks the responses of people
- Escalates incidents to other users
- ESM workflow resources
  - Stages
  - Annotations
  - Cases
  - Notifications



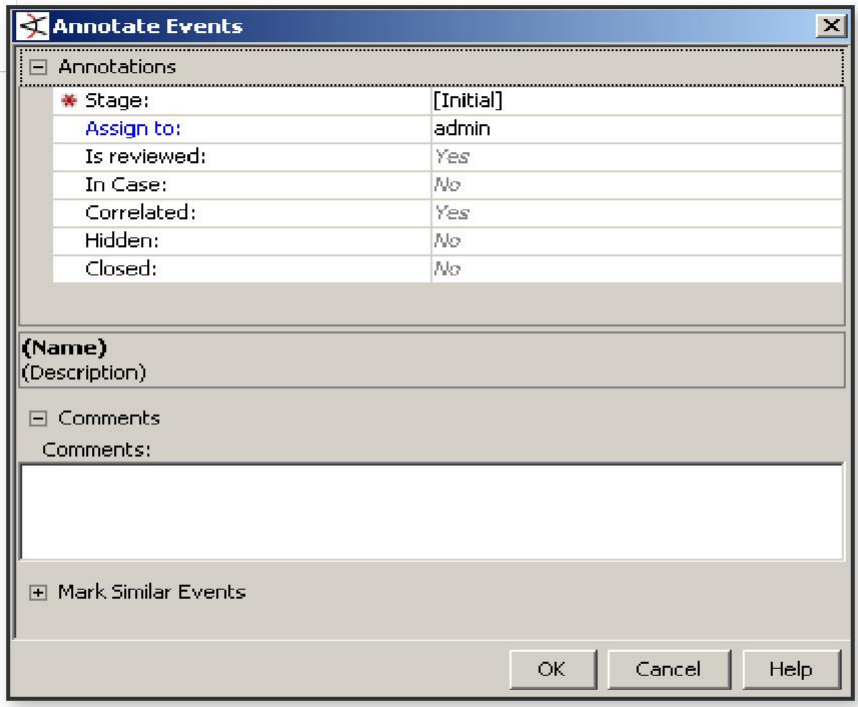
Stages:

- The various steps that an event passes through in an Annotation or a Case

- Default Stages in ESM
  - Queued - The event has not been inspected.
  - Initial - The event has been inspected.
  - Follow-Up - The event is under investigation.
  - Flagged as Similar - The event is similar to another event that is being investigated
  - Monitoring - The event is being monitored to check if it recurs as a pattern
  - Rule Created - The event is being used as a base to create a Rule to find recurrences and generate Notifications
  - Final - The investigation has concluded.
  - Closed - The investigation has been closed

Annotations:

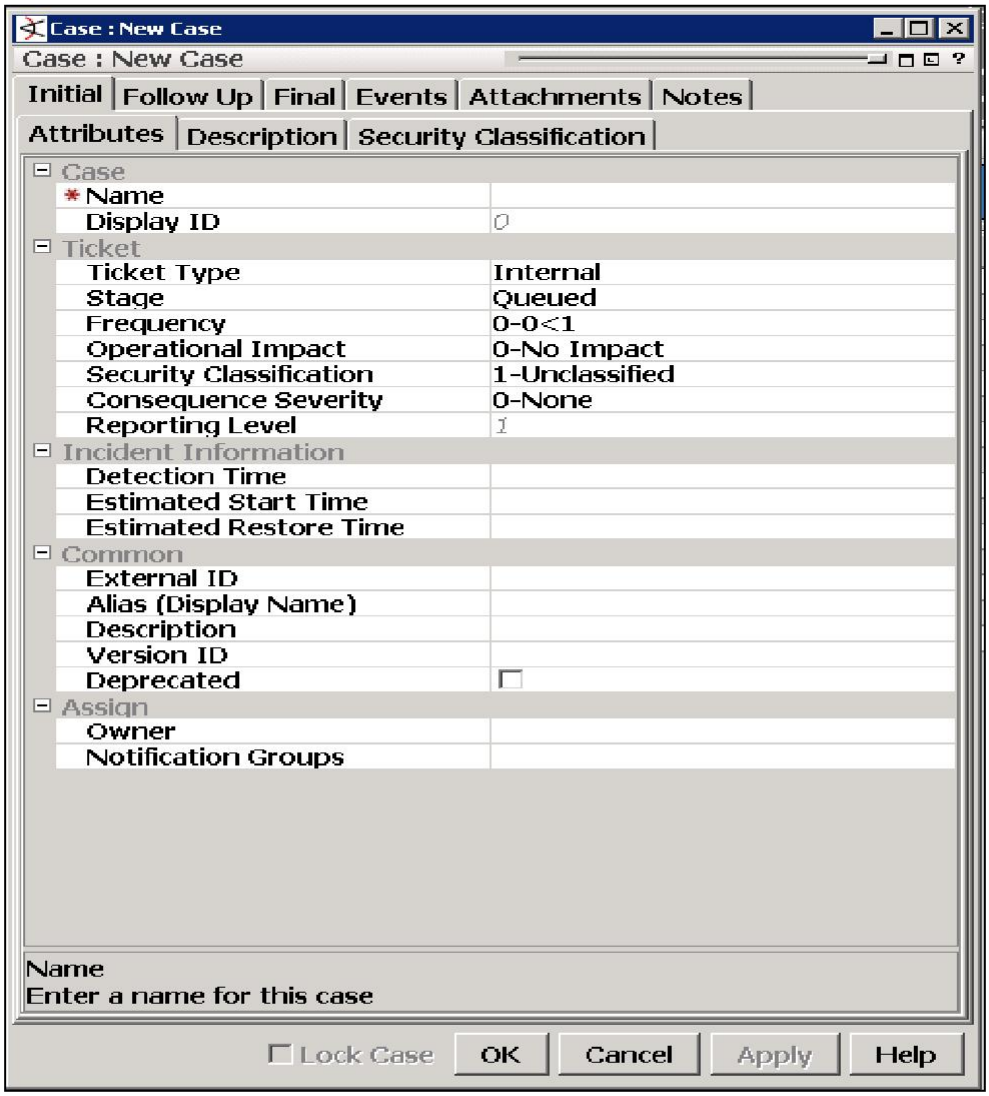
- Annotations are used to:
  - Assign events to users or user groups for escalation
  - To flag events for follow-up
  - Compare incoming events to annotated events and identify events with similar attributes



End Time	Name	Generator URI	Event Annotation Stage	Event Annotati	Event Annotation Comme	Event Annotati	Attacker Address	T
27 Jul 2019 22:38:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued					1
27 Jul 2019 22:35:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued			isReviewed		1
27 Jul 2019 22:32:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued			isReviewed		1
27 Jul 2019 22:30:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued			isReviewed		1
27 Jul 2019 22:23:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued					1
27 Jul 2019 22:20:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued					1
27 Jul 2019 22:19:15 GST	Test	/All Rules/Real-time Rules/KPC-Rules/Subin/Test	Queued				172.16.10.134	1
27 Jul 2019 22:18:48 GST	Test	/All Rules/Real-time Rules/KPC-Rules/Subin/Test	Queued				172.16.10.134	1
27 Jul 2019 22:18:28 GST	Test	/All Rules/Real-time Rules/KPC-Rules/Subin/Test	Queued				172.16.10.141	1
27 Jul 2019 22:18:25 GST	Test	/All Rules/Real-time Rules/KPC-Rules/Subin/Test	Follow-Up	anita	Plz followup	hidden		1
27 Jul 2019 22:18:18 GST	Test	/All Rules/Real-time Rules/KPC-Rules/Subin/Test	Follow-Up	anita	Plz followup	hidden		1
27 Jul 2019 22:18:01 GST	Test	/All Rules/Real-time Rules/KPC-Rules/Subin/Test	Queued				172.16.10.145	1
27 Jul 2019 22:17:43 GST	ArcSight User Login Timeout	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued					
27 Jul 2019 22:17:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued					1
27 Jul 2019 22:14:30 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Queued					
27 Jul 2019 22:14:15 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Queued					
27 Jul 2019 22:14:03 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Queued					
27 Jul 2019 22:14:00 GST	ASM Database Status Change - Normal	/All Rules/Real-time Rules/ArcSight Administration/ES...	Queued					1
27 Jul 2019 22:13:48 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Queued					
27 Jul 2019 22:13:36 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Queued			inCase		
27 Jul 2019 22:12:55 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Queued			isReviewed		
27 Jul 2019 22:12:43 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Flagged as Similar	adnan	assigned	hidden		
27 Jul 2019 22:12:28 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Monitoring	redline				
27 Jul 2019 22:12:16 GST	TestRuleTriggered	/All Rules/Real-time Rules/KPC-Rules/Subin/TestRuleT...	Queued					

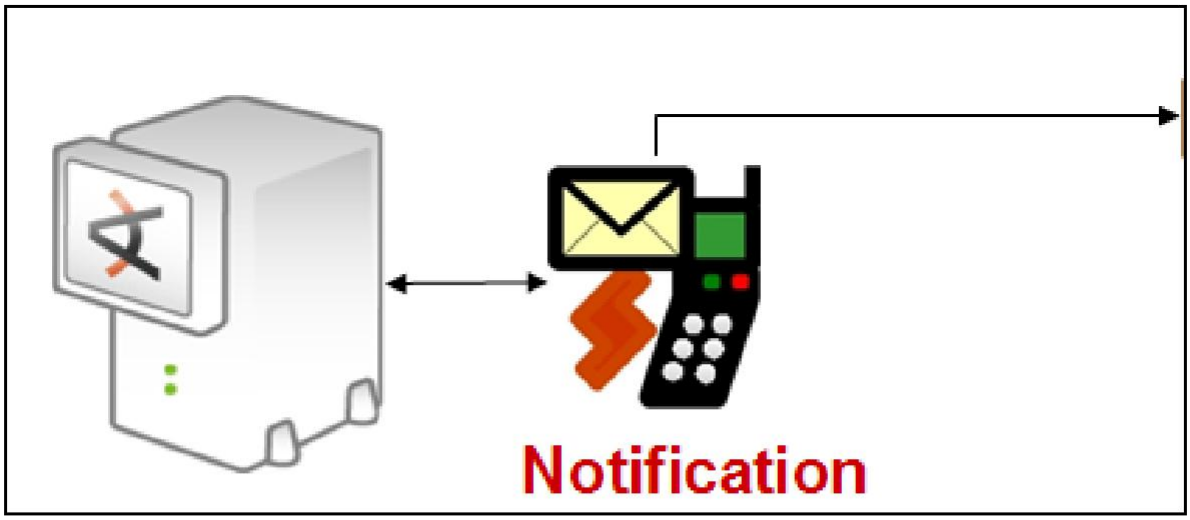
Cases:

- A Case contains information about a specific incident
  - Investigate, and resolve events of interest
  - Track individual or multiple related events
  - Attach additional troubleshooting information for more detailed investigation
  - Need to be locked before assigning to users. This will prevent modifying that case by others.



Notifications:

- Notify others about certain conditions from ESM
- Allows you to initiate messages by email, pager, text message, or ESM Console
- Notifications can be initiated:
  - As an automatic action in a rule
  - As a result of system alerts
  - When a case is opened or modified
  - Intentionally Left Blank



Module -5

- Logger
- Event Search
- ArcMC

- What is Logger?
- ArcSight Log Management Platform
- Logger Features
- Deployment Scenarios
- Describe how search results are displayed
- Use the unified search page to initiate any type of search
- Use search helper and search builder features
- Load, modify, and save search filters and saved searches

Introduction to Logger:

- Arcsight Logger is a Universal Log Management solution that can Collect Everything, Analyse Anything and can be Used Anywhere.
- Optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis.
- Logger unifies searching, reporting, alerting and analysis across ANY type of enterprise log data
- Available in two form factors:
    - Logger Appliance
    - Software Logger(Physical or Virtual machine)
    - Logger can receive structured events that are parsed and unstructured RAW events

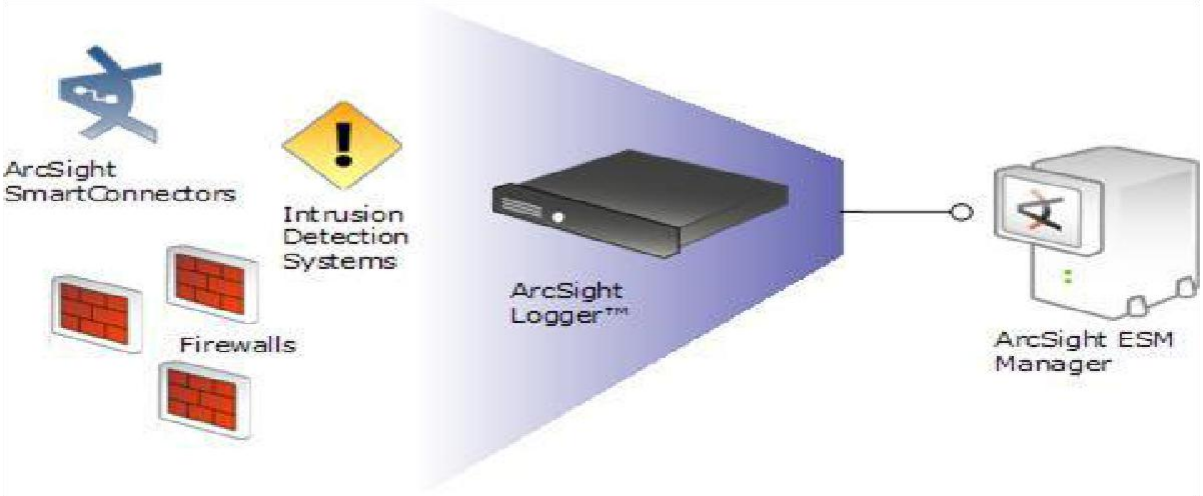
Standalone Logger and ADP Logger:

- *Same code, same features, just licensed differently*
- *All Loggers are licensed on GB of events ingested per day*
- **Standalone Logger**
    - Used without ADP
    - *Can consume events from raw devices or Connectors*
- **ADP Logger**

- Consumes events from raw devices, Event Broker or from Connectors
- Consumption license centrally managed by ArcMC

Deployment Scenarios:

Logger can act as a funnel, forwarding selected events to ArcSight Manager



Logger Components:

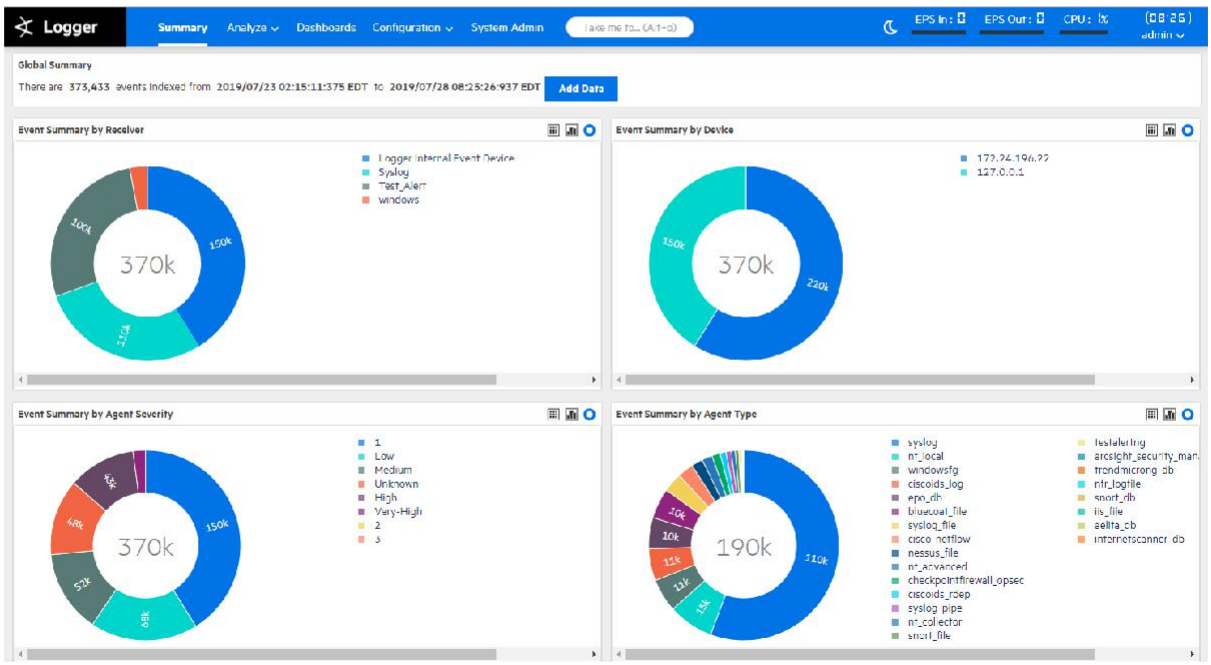
- **Receivers**
  - Receives events from SmartConnectors, FlexConnectors, Files, Network Connections
  - ADP Logger can also receive events from Event Broker
- **Forwarders**
  - Forwards events to ArcSight ESM, other Connectors, other Syslog or any TCP or UDP downstream device
- **Storage Groups**
  - Allow for the separation of events by retention period or by event type
- **Search**
  - Google-like search for events, over time, use pipeline operators for transformations and quick charts
- **Dashboards**
  - Visual summaries of activity over time, top entities
- **Reports**

- Repeatable, ad-hoc or scheduled, long term analysis and summary of events suitable for Management as well as Analysts

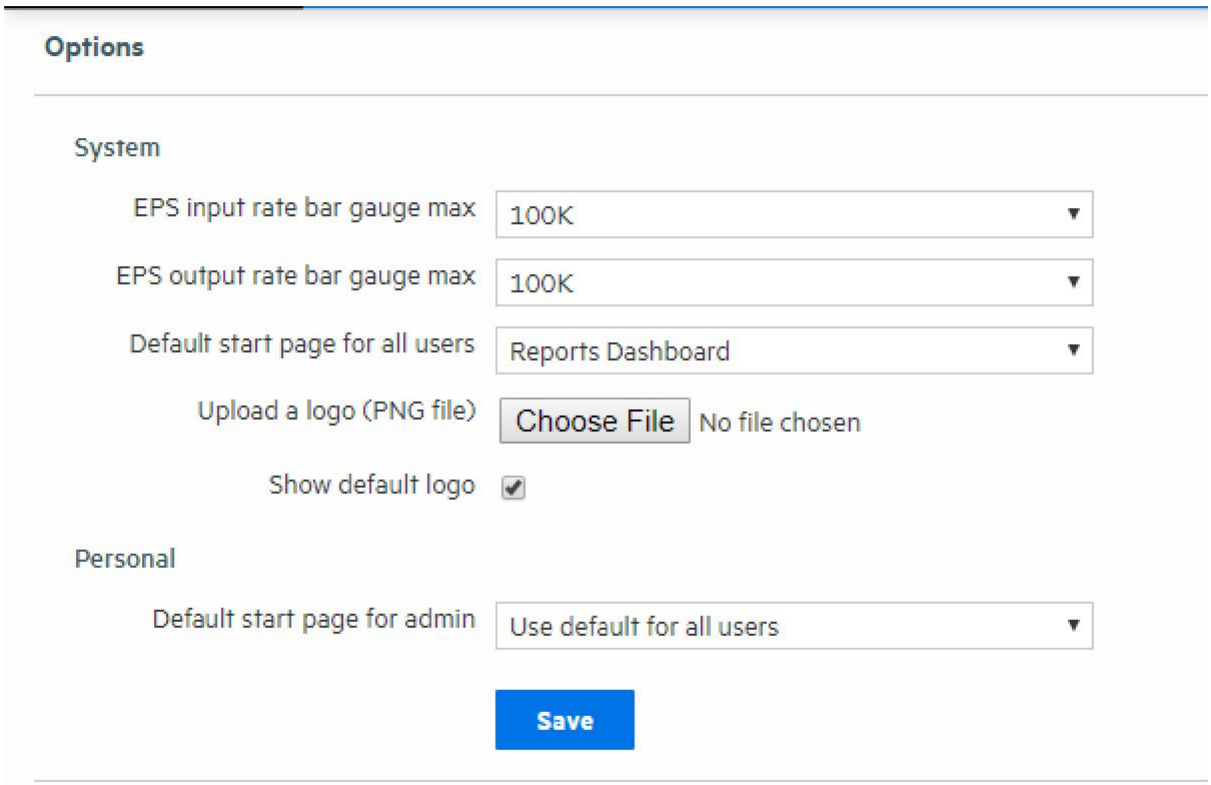
- **Lookups**
  - Dynamic comparisons with external sources of information, such as a list of malicious domains or blacklist IP Addresses
- **Alerts**
  - Both near real time and scheduled

Connecting to the Logger User Interface:

- **https**://<hostname or IP address>:<configured_port>



Change Default Theme and Views

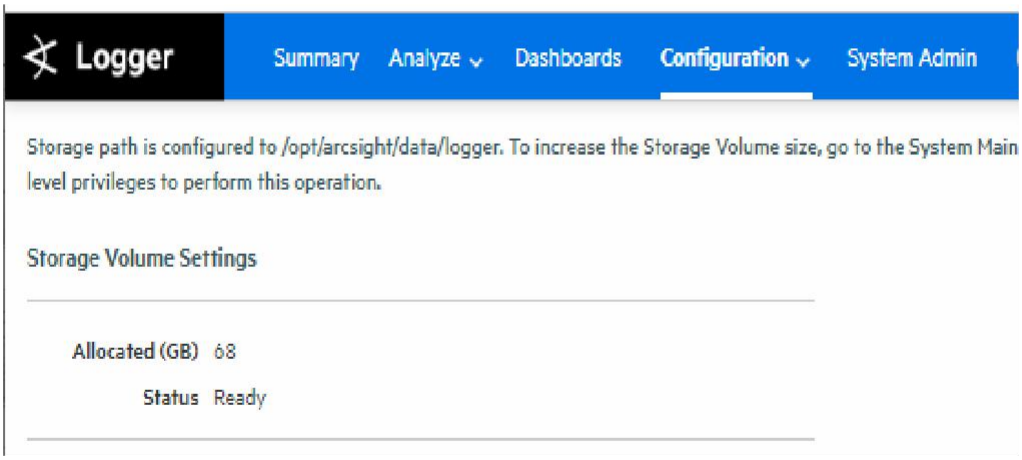


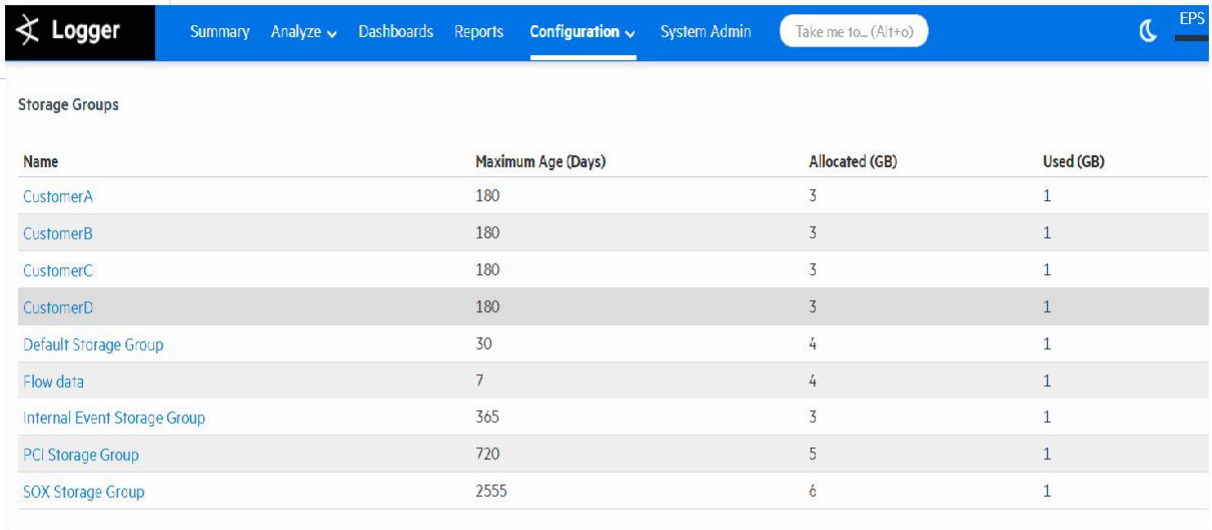
Logger Features:

- Storage Configuration
- Receiver Configuration
- Analysing Events
- Grouping Events
- Exporting Events
- Forwarder Configuration
- User Management

Logger Features - Storage Configuration

- The storage volume, either external or local, can be divided into multiple storage groups, each with a separate retention policy.
- Allows to create up to 100 storage groups
- Events are stored compressed. You cannot configure the compression level





Storage Groups

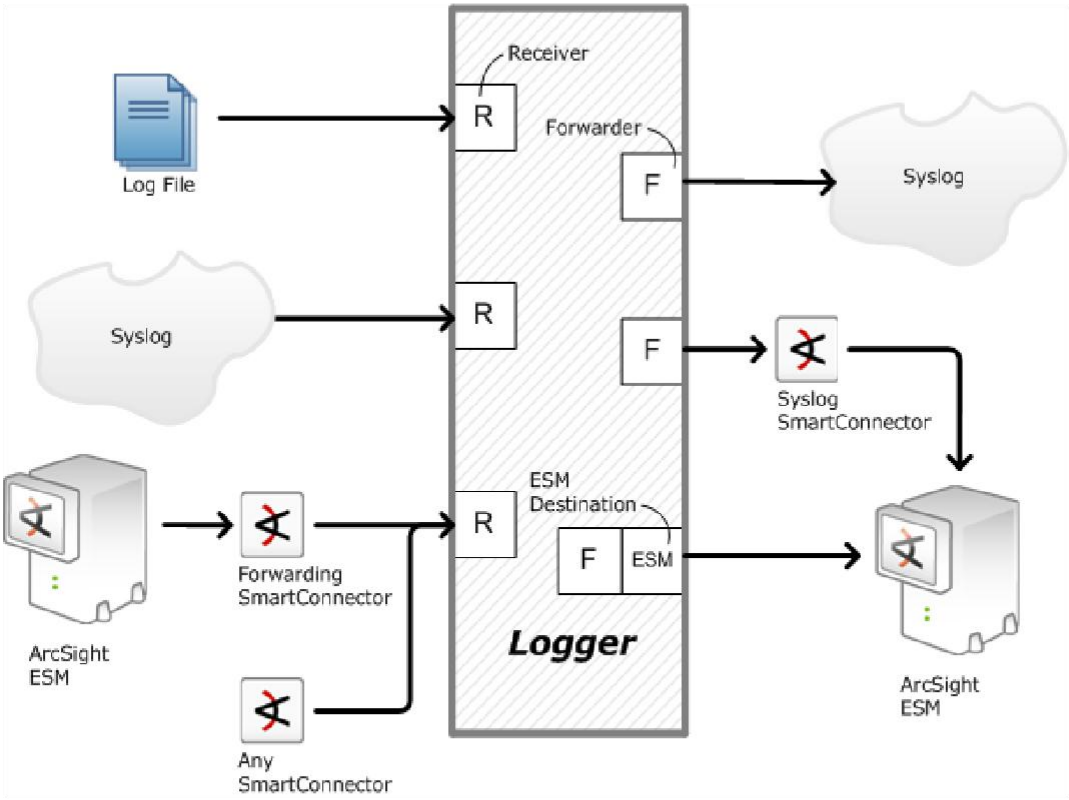
Name	Maximum Age (Days)	Allocated (GB)	Used (GB)
CustomerA	180	3	1
CustomerB	180	3	1
CustomerC	180	3	1
CustomerD	180	3	1
Default Storage Group	30	4	1
Flow data	7	4	1
Internal Event Storage Group	365	3	1
PCI Storage Group	720	5	1
SOX Storage Group	2555	6	1

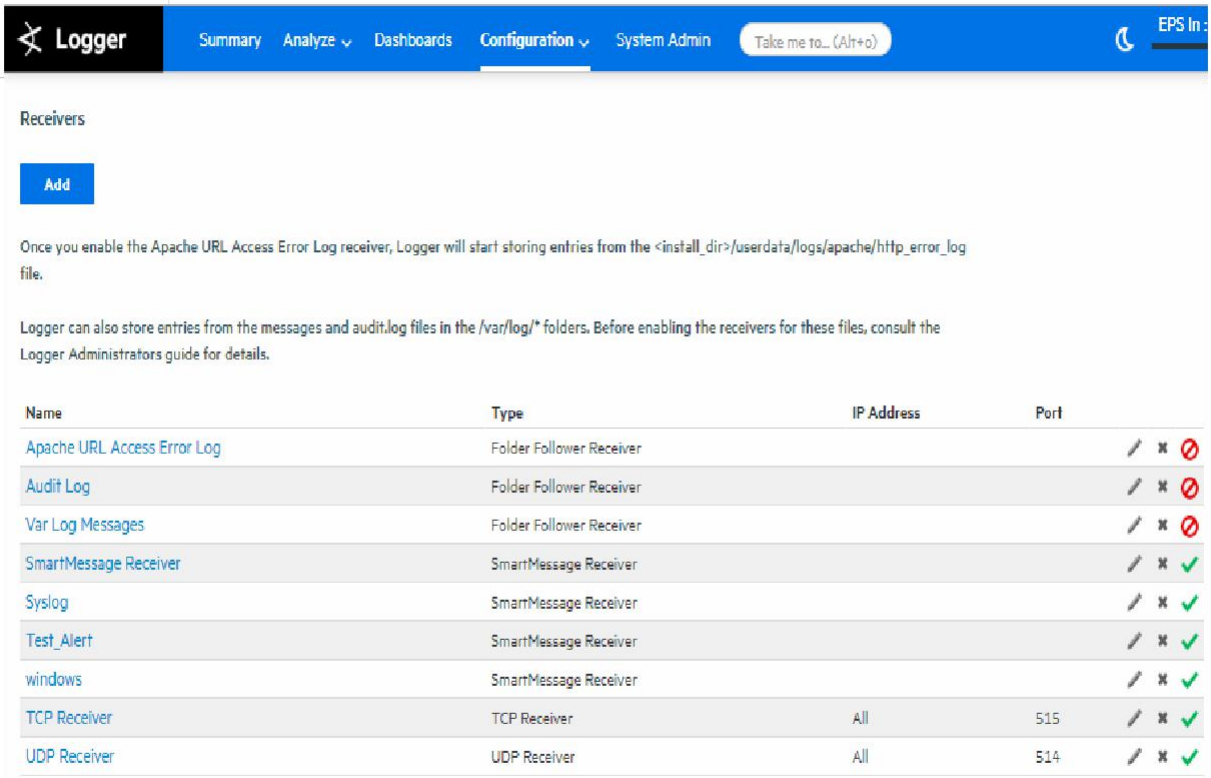
Sizing and Capacity:

- Software Logger
  - 5 GB / day minimum, steps of 5 GB/day up to 500 GB/day
- Appliance Logger
  - L7600 5 GB / day minimum, steps of 5 GB/day up to 250 GB/day
- 12 TB Addressable Storage per Logger instance
- Can mix and match peering to software and appliances
- Up to 100 peers – transparent searching across all peers
- High availability can be achieved by using
  - Logger destination pools (from Smart Connector)
  - HA appliances can be used to ingest a second copy of all events in case of primary failure

Logger Features - Receiver Configuration:

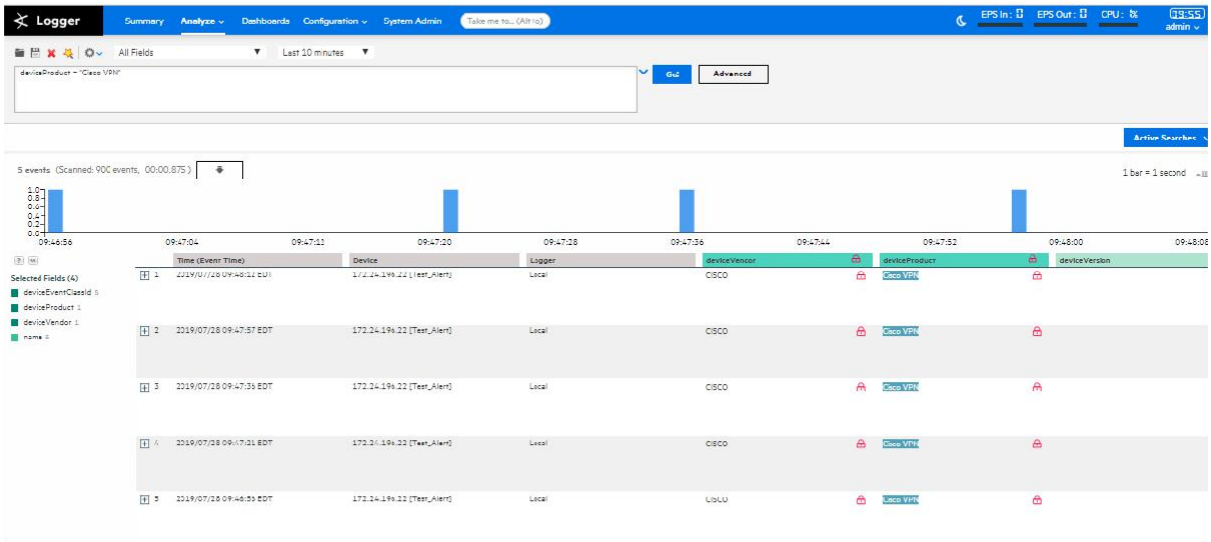
- Syslog Messages
- Encrypted Smart Messages
- CEF – Common Event Format
- Read Log Files – SCP, SFTP or FTP protocol




Logger
Summary
Analyze
Dashboards
Configuration
System Admin
Take me to... (Alt+o)
EPS In :
Receivers
Add
Once you enable the Apache URL Access Error Log receiver, Logger will start storing entries from the <install_dir>/userdata/logs/apache/http_error_log file.
Logger can also store entries from the messages and audit.log files in the /var/log/* folders. Before enabling the receivers for these files, consult the Logger Administrators guide for details.
Name
Type
IP Address
Port
Apache URL Access Error Log
Folder Follower Receiver
Audit Log
Folder Follower Receiver
Var Log Messages
Folder Follower Receiver
SmartMessage Receiver
SmartMessage Receiver
Syslog
SmartMessage Receiver
Test_Alert
SmartMessage Receiver
windows
SmartMessage Receiver
TCP Receiver
TCP Receiver
All
515
UDP Receiver
UDP Receiver
All
514

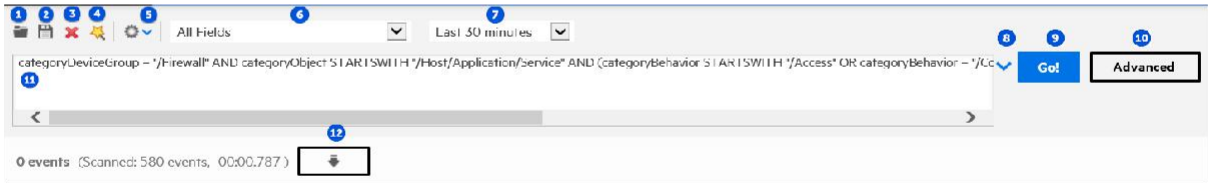
Logger Features - Analyzing Events:

- Events can be searched with particular matching query
- Queries can be based on plain English keywords (full-text search) or predefined fields
- Queries can be entered manually or automatically created by clicking on terms in the event table
- Queries can be saved as a filter or as a saved search.



Logger Features - Analysing Events:

Running a Search:



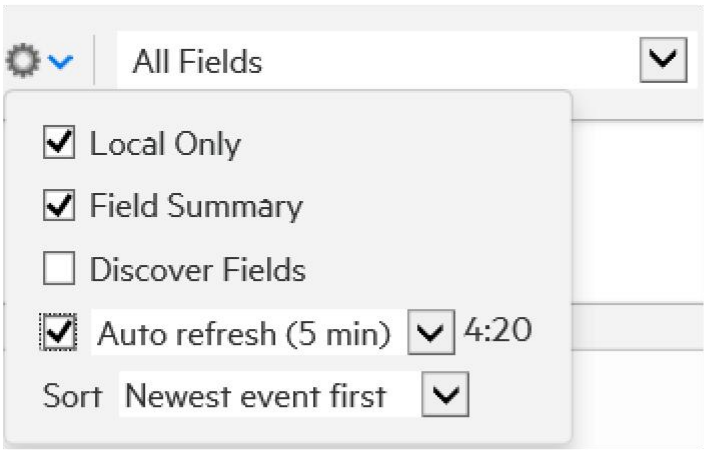
Search Bar Legend

Option	Description	Option	Description
1	Load saved search or filter	7	Set time range
2	Save query	8	Open search history
3	Clear query	9	Start or cancel search
4	Open Search Analyzer	10	Open Advanced Search Builder
5	Update search options	11	Enter query
6	Select fieldset	12	Export search results

Logger Features - Analysing Events:

Active Searches

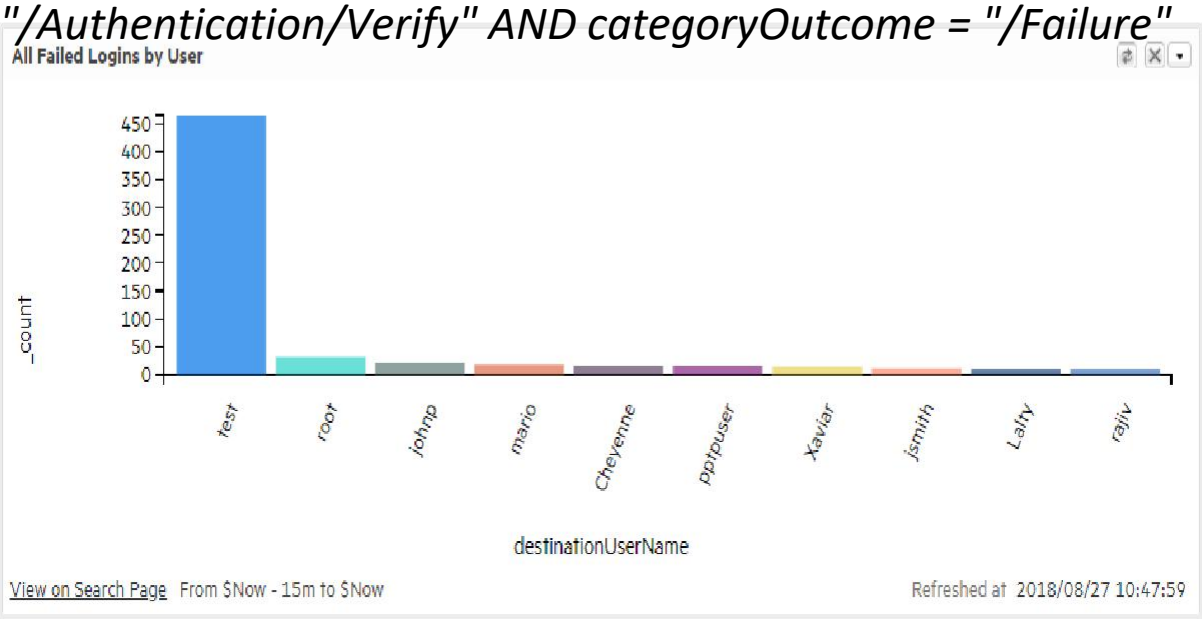
Auto Refresh Search Results



Logger Features - Analysing Events:

Chart Drill Down

All failed login attempts across **ANY** device in your organisation is as simple as - *categoryBehavior = "/Authentication/Verify" AND categoryOutcome = "/Failure"*



Logger Features - Grouping Events:

- Devices
  - As events are received, devices are automatically created for each IP/receiver pair.
  - Devices can also be created manually
- Device Groups
  - Devices can be categorized by membership in one or more device groups
  - While an incoming event belongs to one and only one device, it can be associated with more than one device group
- Storage Rules
  - Storage rules associate a device group with a storage group
    - Storage rules are ordered by priority, and the first matching rule determines to which storage group an incoming event will be sent
    - Up to 40 storage rules
  - Grouping is used to limit the searching within a group for faster retrieval

Logger Features - Exporting Events:

- Events that match the current query can be exported locally, to an NFS mount, a CIFS mount, as a file.
- Events can be exported in Comma-Separated Values (CSV) format for easy processing by external applications or as a PDF file for generating a quick report
- <install_dir>/data/logger directory - can be mounted to an NFS or CIFS

Logger Features - Forwarder :

Configuration:

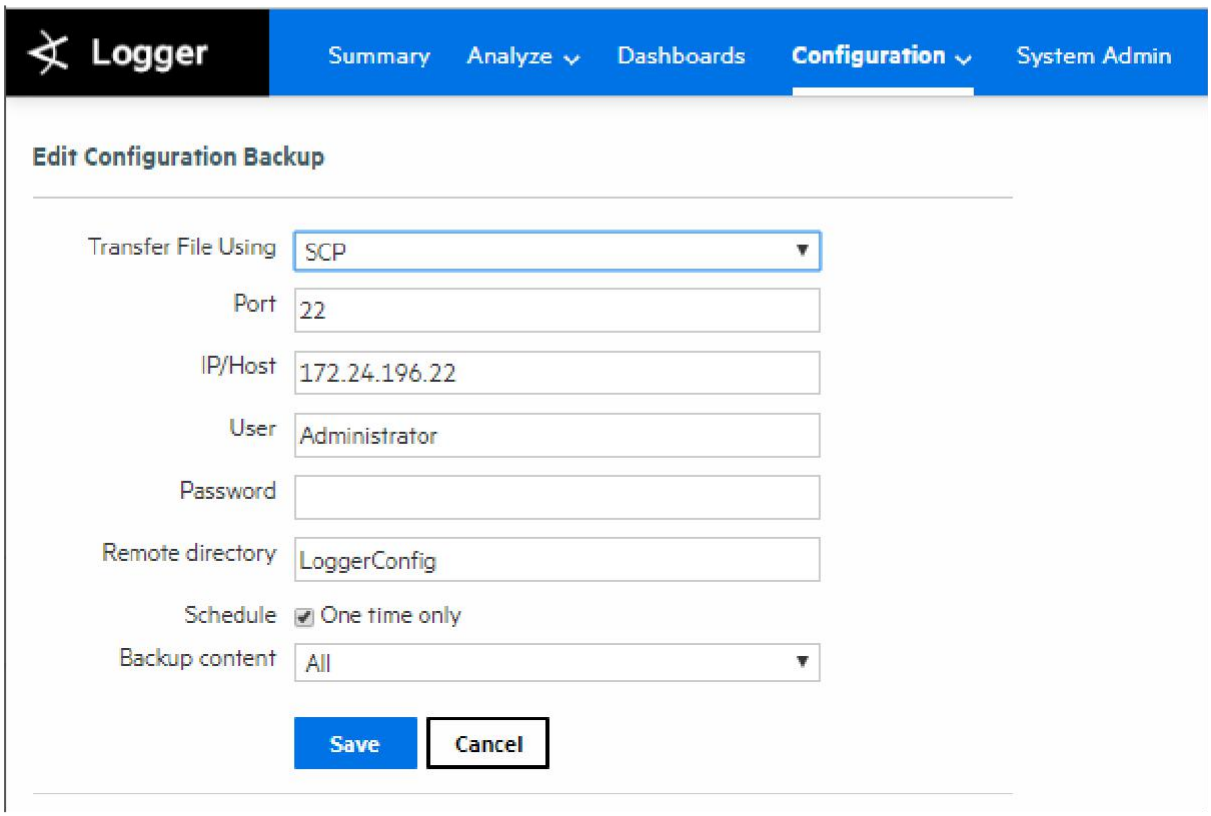
- Logger can send events (as they are received or past events) to other hosts or ArcSight Manager
- Logger can be configured to act as a funnel, receiving events at very high volumes and sending fewer, filtered events on to an ArcSight Manager

Logger Features - User Management:

- User accounts can be created by the Logger administrator to distinguish between different users of the system

- User Groups can have an enforced event filter applied to them

Logger Configuration Backup:




TRIPWIRE®
IP360 Tools

What is Vulnerability?

In cyber security, a vulnerability is a weakness which can be exploited by a cyber attack to gain unauthorized access to or perform unauthorized actions on a computer system

Vulnerabilities can allow attackers to run code, access a system's memory, install malware, and steal, destroy or modify sensitive data.

Vulnerability Scanning:

Vulnerability scanning is a security technique used to identify security weaknesses in a computer system. Vulnerability scanning can be used by individuals or network administrators for security purposes, or it can be used by hackers attempting to gain unauthorized access to computer systems.

Vulnerability Assessment Scanning Tools:

- Comodo HackerProof
- OpenVAS
- Nexpose Community
- Nikto
- Tripwire IP360
- Wireshark

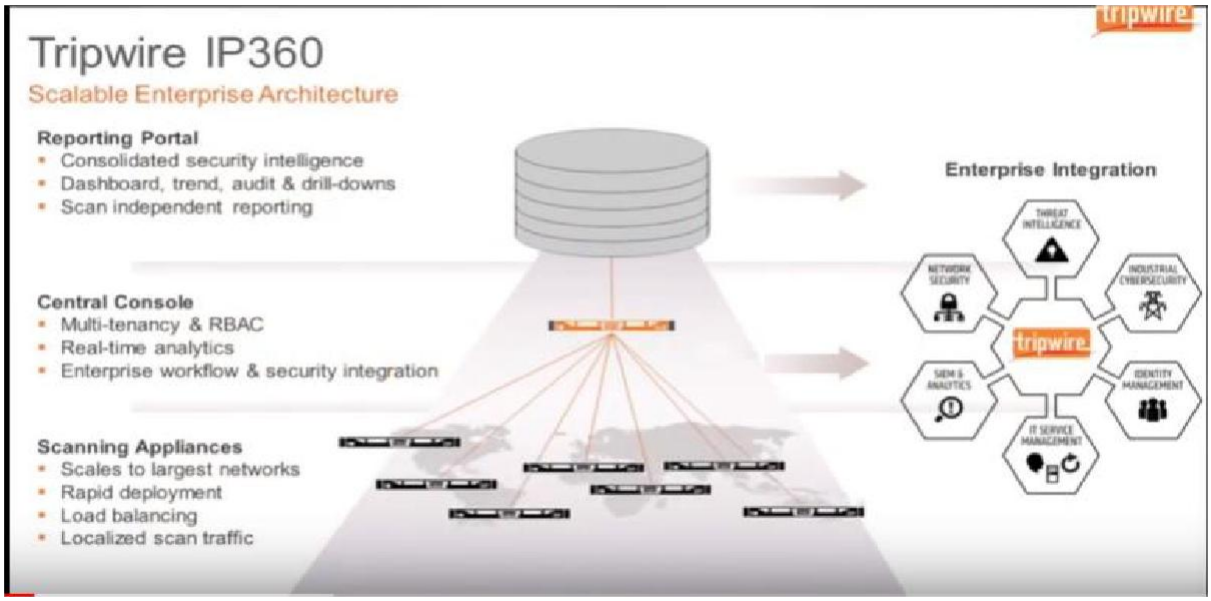
- Aircrack
- Nessus Professional
- Retina CS Community
- Microsoft Baseline Security Analyzer (MBSA)

Tripwire IP360 Vulnerability Management:

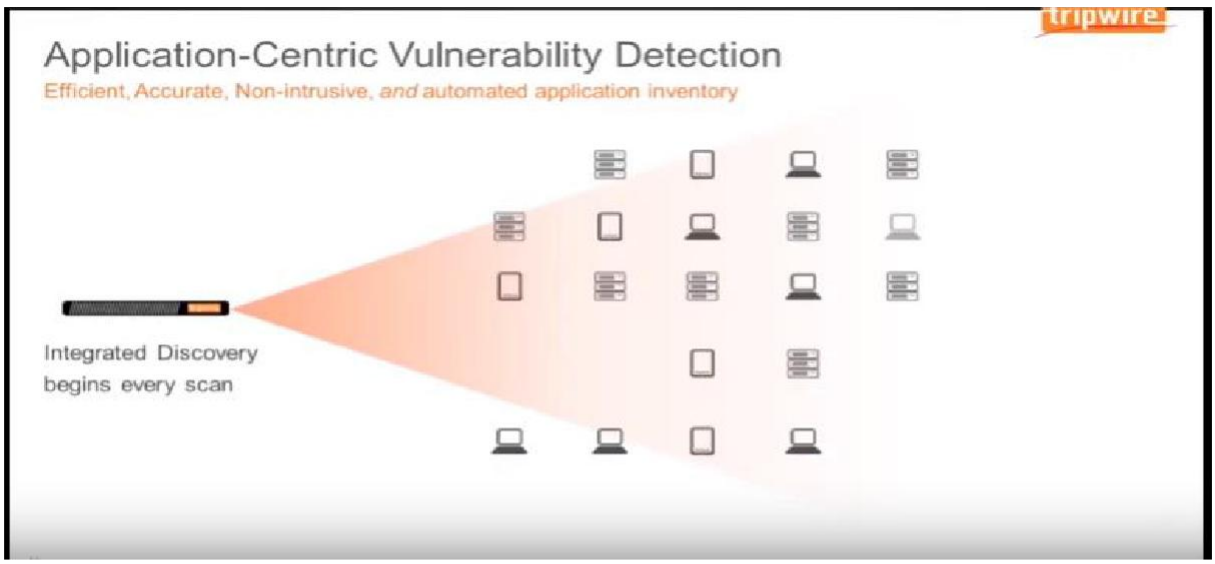
- Tripwire vulnerability management is the Appliance based technologies its can be installed as a physical appliance or Virtual appliance
- It has two components

1. Central Console
2. Scanning Appliance

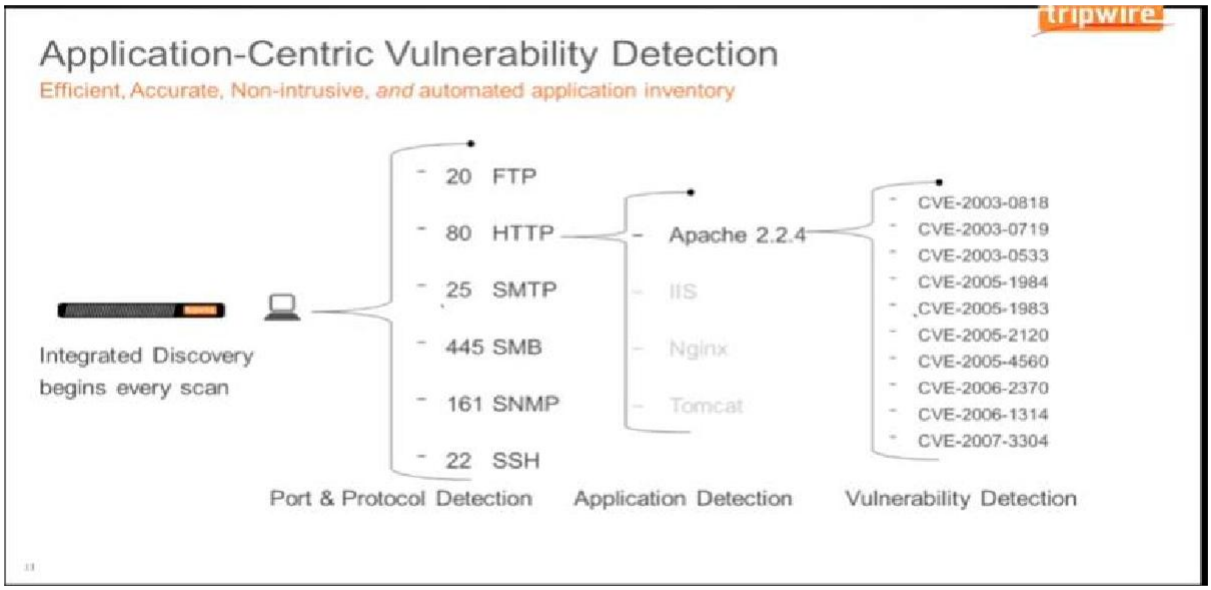
Tripwire IP360 Architecture:



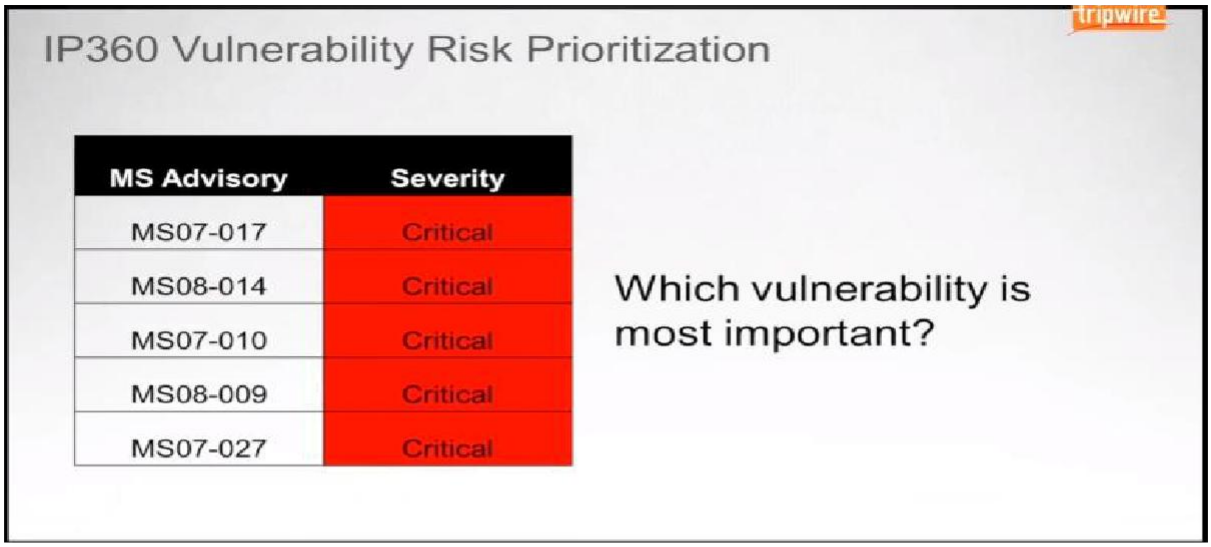
Profiling of Assets:



Way of scanning of an Asset:

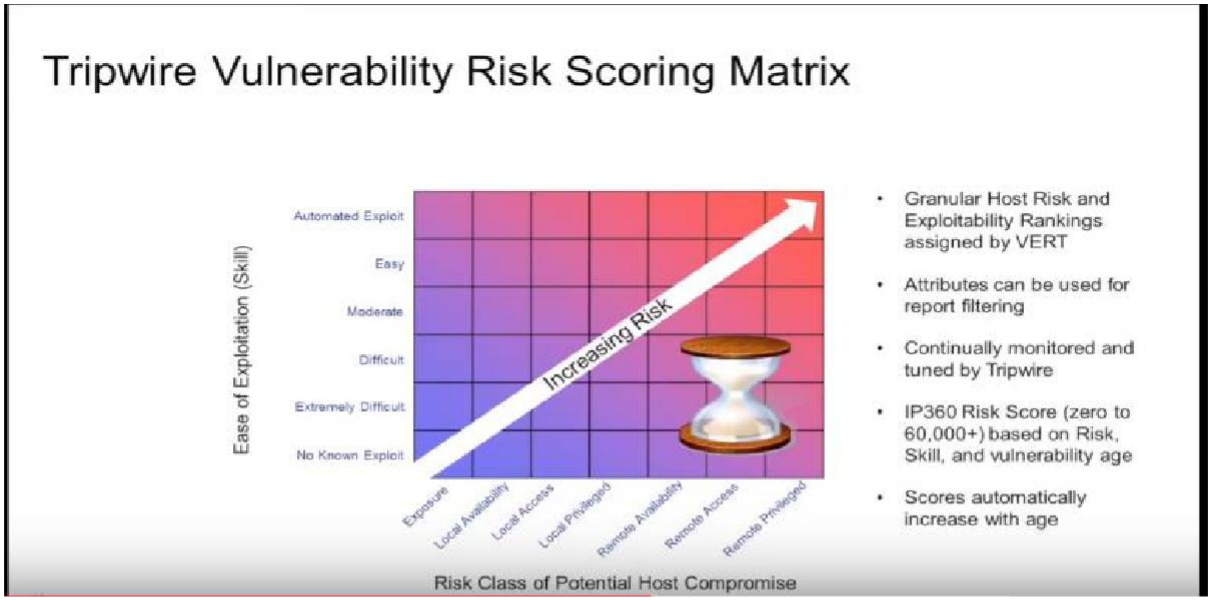


Vulnerabilities Risk Prioritization:



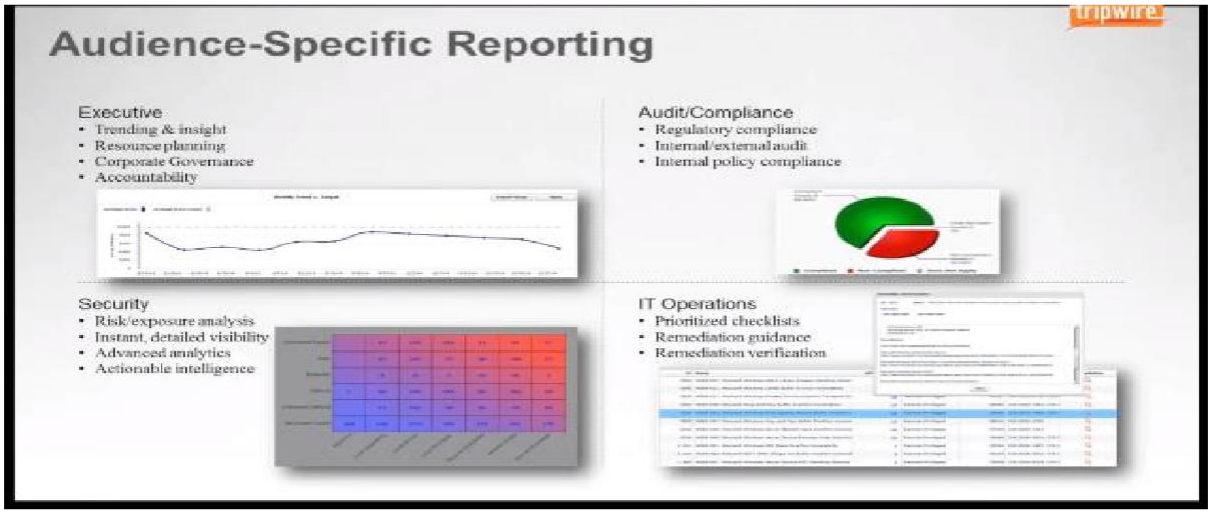
IP360 Vulnerabilities Risk Score:

Risk Scoring Matrix:

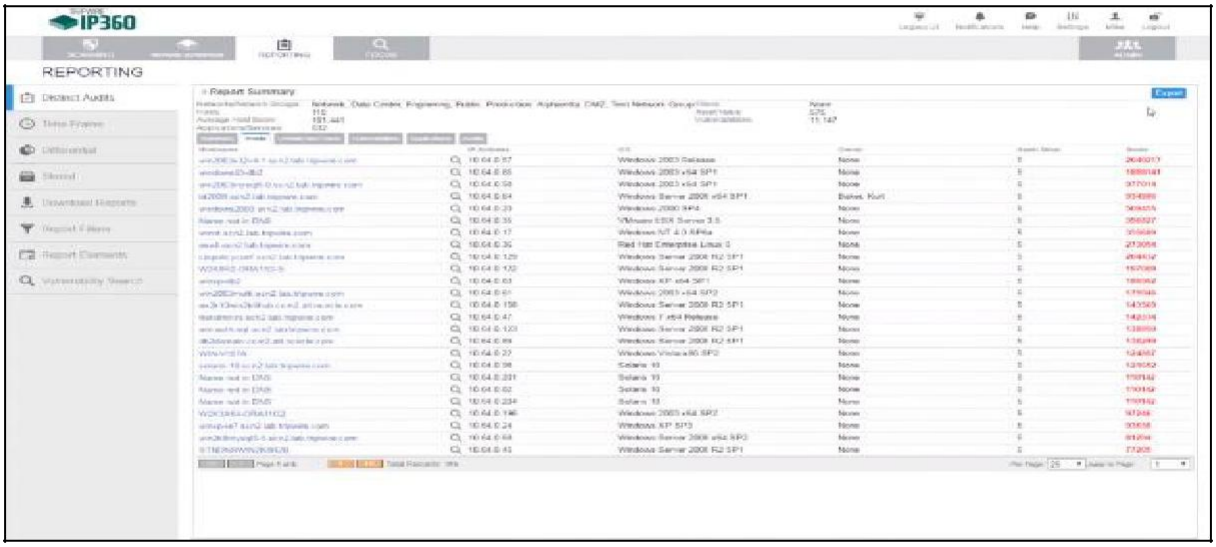


Accurate Metrics For Prioritization

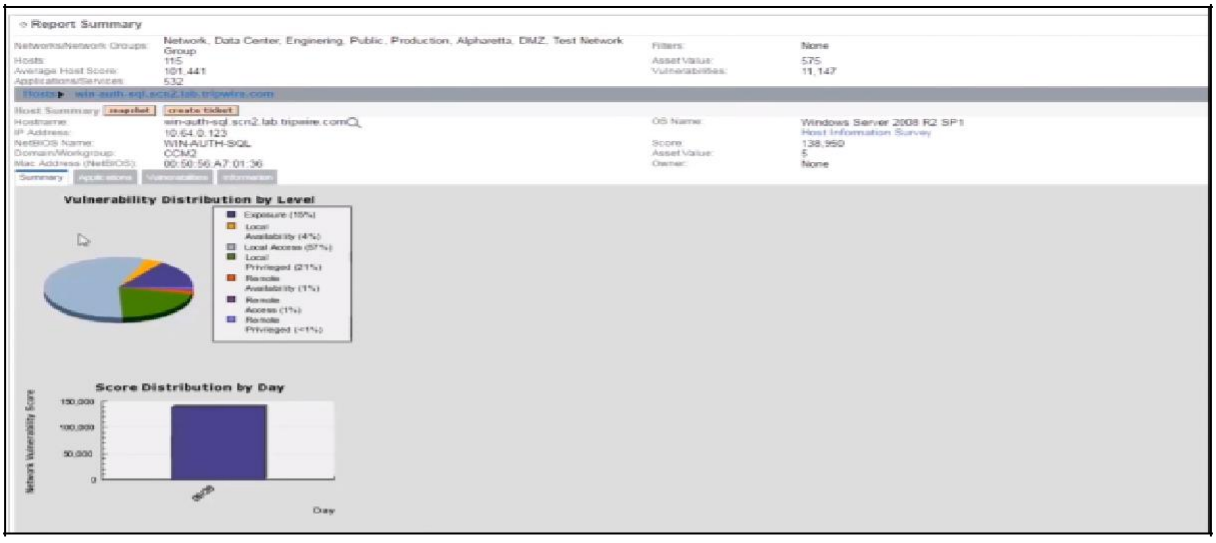
- Numerical Vulnerability Scores (zero to 60,000+) Based On:
  - Severity of potential host compromise
  - Sophistication and availability of exploits "in the wild"
  - Vulnerability age
- Host Scores (sum of vulnerability scores)
- Asset Values (assigned based on user-defined logic)
- Vulnerability Aging with SLAs for remediation
- Network Average Scores and Trends



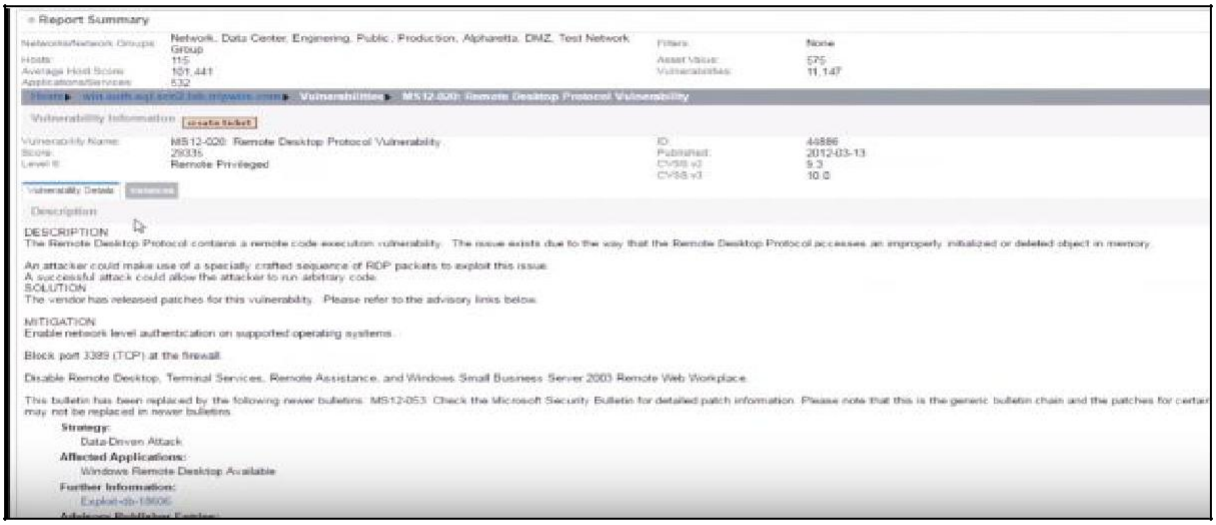
List of Vulnerabilities with Scoring:



Detail of a Vulnerability:



Recommended Patch for a Vulnerability:



What is User Behaviour Analytics (UBA):

User behaviour analytics (UBA) as defined by Gartner is a cyber security process about detection of insider threats, targeted attacks, and financial frauds

UBA solutions look at patterns of human behaviour, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns anomalies that indicate potential threats

Instead of tracking devices or security events, UBA tracks a system's users.

Big data platforms like Apache Hadoop are increasing UBA functionality by allowing them to analyse petabytes worth of data to detect insider threats and advanced persistent threats.

UBA Solutions Available in Market:

Aruba

Dtex

Exabeam

Forcepoint

Fortinet

Securonix

Fortscale

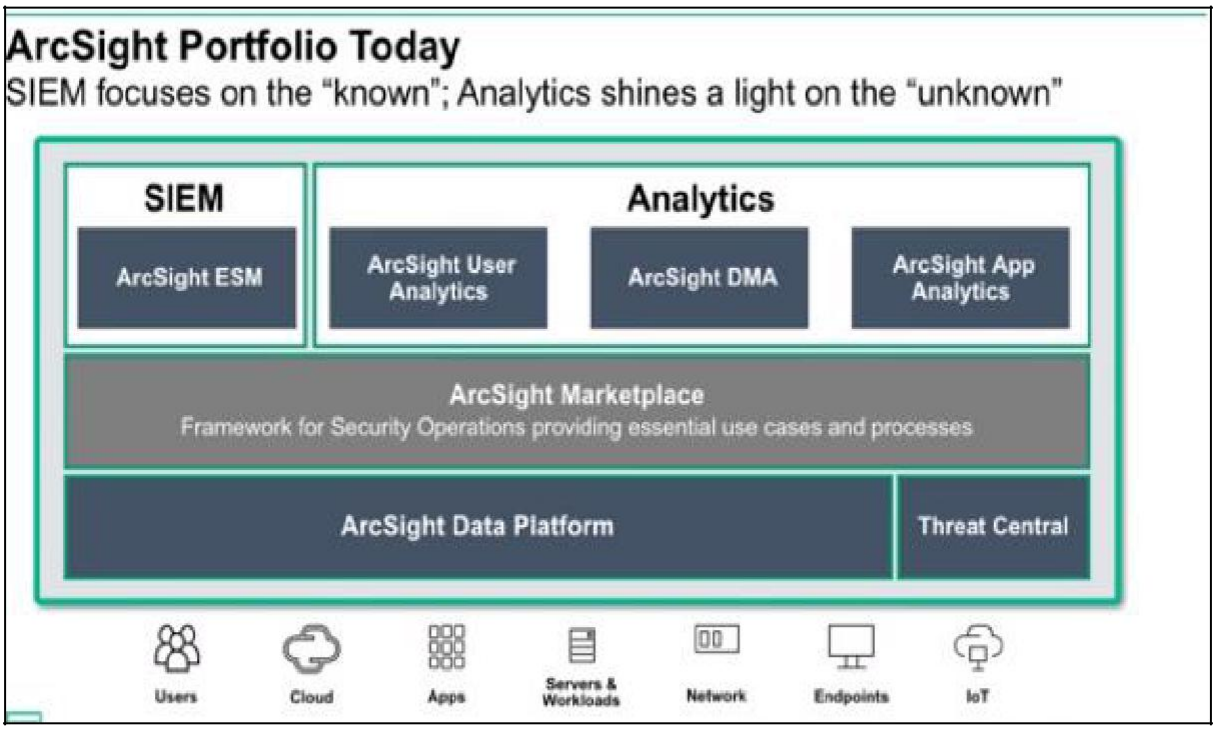
LogRhythm

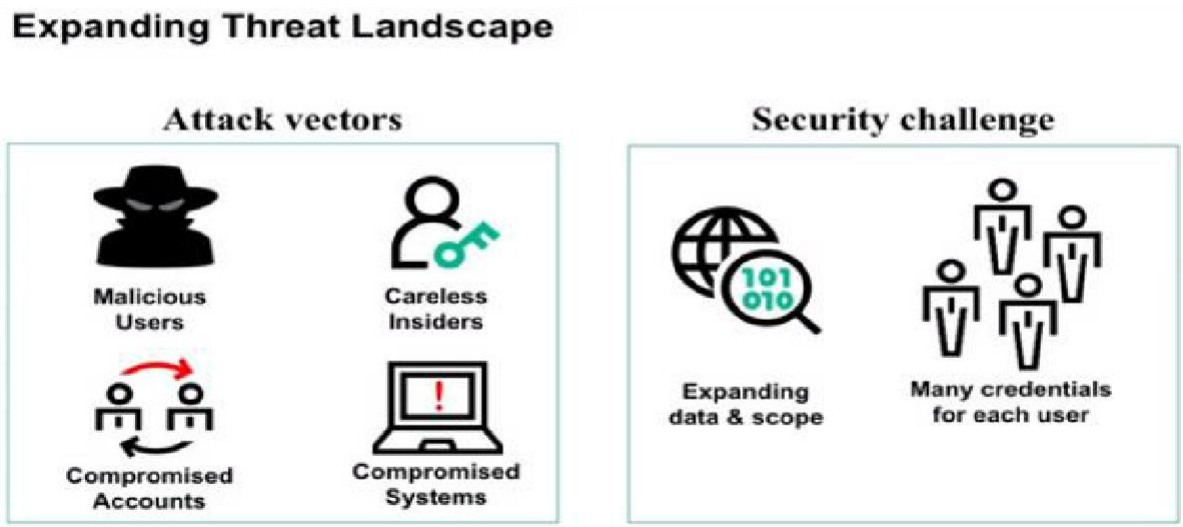
RSA

Securonix

Splunk

Arcsight Portfolio:



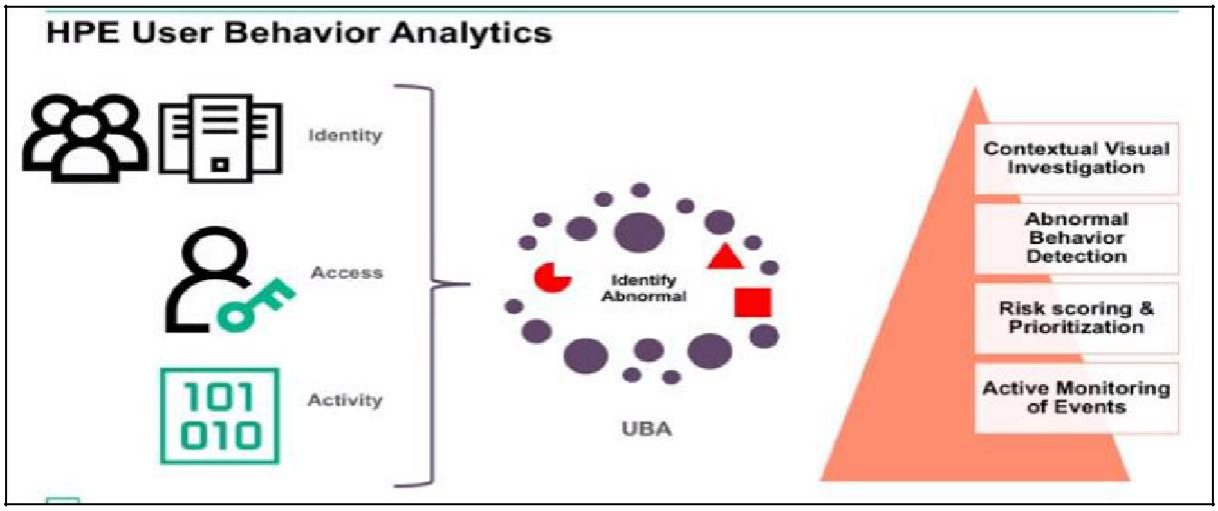


Expanding Threat Landscape – Insider Threats

83% of all data loss via **legitimate** credentials

82% of all breaches investigated - evidence of the attacker activity was **available** and **contained** in security log files

The Challenge: How Can Security Teams Detect and React Quickly?



UBA key solution areas & benefits

User Behaviour Analytics identifies stealing of trade secrets

UBA Success Stories

- Terminated User Activity
  - Not only were terminated users found to be logging on, analyst investigations showed users were also sending out emails post termination
  - Key: UBA links all accounts in events back to the core user identity – so any activity, from any of the accounts associated with a user, will be flagged as soon as it happens (and action can be taken to block that access)
- Geolocation-based Anomaly Detection
  - User activity was detected coming from Brazil and Mexico within 5 minutes
  - Key: With UBA, baselines are set showing "normal" activity, such as locations of logon, as well as details about the user, such as their office location. Activity outside that norm, such as "you'd have to be a super hero to be in both places at the same time" called out possible account compromise or sharing.
- Confidential Data Egress via Email
  - Through spike detection and tiered analytics, found a user sending an abnormally high number of emails to their personal email address – which happened to include source code as attachments
  - Key: DLP monitoring of files and emails will show policy violations, but they don't show the whole picture – such as how often a user normally violates policies, and if any other suspicious behavior has been seen by other systems. At this site, sending to personal email in moderation was acceptable – when UBA detected the spike and highlighted file transfers not normally done by that user or their group – policy violating behavior could be stopped and addressed quickly.

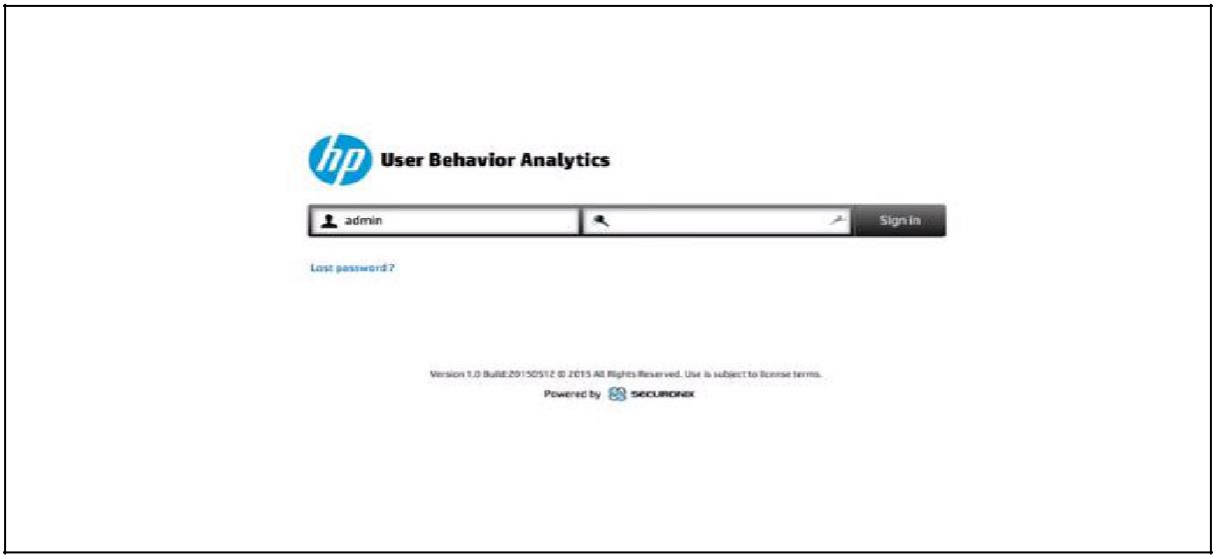
UBA Success Stories (cont.)

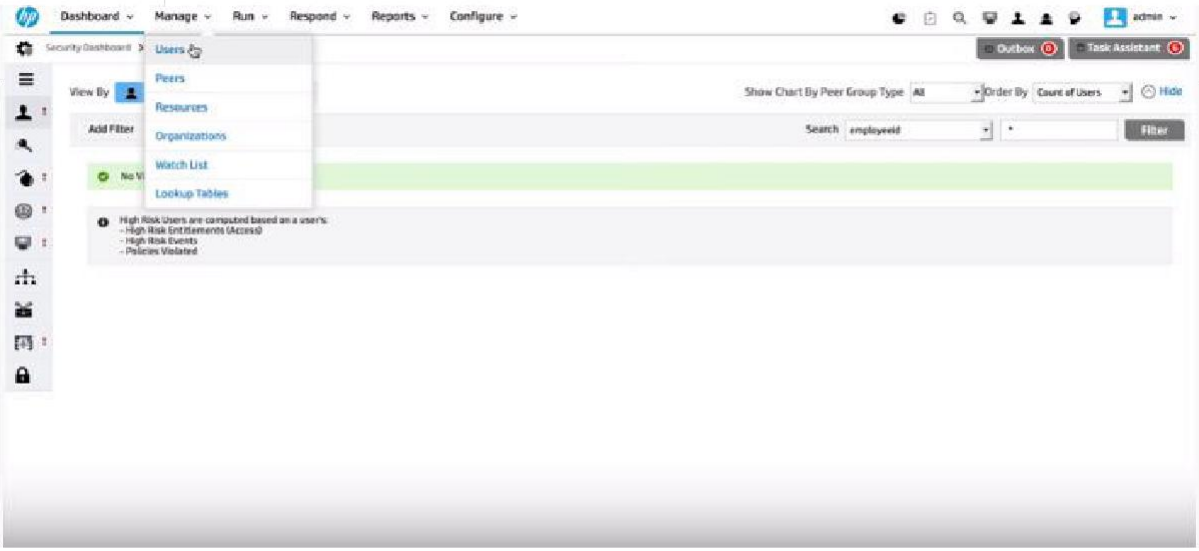
- Audit Log Tampering (and then some)
  - Account added to a watchlist when audit log clearing was seen the first time; subsequent tracking highlighted abnormal amounts of log clearing across multiple servers, as well as other policy violating admin activities.
  - Key: Just because a user "can" do something, it doesn't mean they should – and in many cases, doing so violates company policy. But if you don't track the "successes" – things users are allowed to do, especially administrator-level activities – users won't know how severe a problem is.
- Flight Risk Users Egressing Data
  - Many people check a job site now and again – no big deal; do it a lot, however, and they're probably actively hunting for a job; now add high volumes of data uploads to personal sites, and the combination of activity is a big concern
  - Key: For many threats and policy violations, the bad guy isn't necessarily trying to cover their tracks – they just figure nobody is paying attention / noticing what they're doing. And if you have to track / reconcile millions of events over thousands of users – they'd probably be right. With UBA, machine learning tracks all of the activity, across all accounts, over millions of events – and when a suspicious combination of events (even over a long timeframe) is found, this activity is highlighted immediately and HR can be notified to take immediate action.

UBA Success Stories (cont.)

- HPA:
  - Rare interactive logon for a service account – typically account always performed network logon, and then one time it was used for interactive logon over the monitoring period
- HPA:
  - Account re-enabled, used, then disabled in a short period of time
    - A user was going to travel to China, and rather than create a new temporary account, admins temporarily re-enabled an old account,
- HPA:
  - Network user adding and deleting a new interface to a network system, even though none of the other 150 users in that department had ever done changes like that before (over the monitoring period)
- HPA:
  - User from a training department badging into a server room floor – that they'd never badged into before.
    - While the reason was reportedly innocuous (selling/delivering Girl Scout cookies), the question came up – why does a trainer have access to a critical server room floor?

Login to Arcsight UBA:




Dashboard
Manage
Run
Respond
Reports
Configure
admin
Users
Peers
Resources
Organizations
Watch List
Lookup Tables
Outbox
Task Assistant
View By
Show Chart By Peer Group Type
All
Order By
Count of Users
Hide
Add Filter
Search
employeeid
Filter


THANK
YOU!