Azure SIEM Integrator

Microsoft

CONTENTS

PRIVACY POLICY

Azure SIEM integrator complies with Azure privacy policies. The Azure SIEM integrator collects some basic telemetry data and call stack information in the event that an exception occurs. Examples of data collected are

1. Perf counter information (%cpu usage on SIEM instance, events per second processed, queries per second etc.)
2. Exception information including call stacks
3. Feature usage information and statistics
4. IP Address and the DNS name of the SIEM instance running the product

The telemetry collection is turned on by default. You can turn it off by running the command below after installing the service.

```
Azsiem disabletelemetry
```

OVERVIEW

Both PaaS and IaaS services hosted in Azure generate a large amount of data in security logs. These logs have vital information that can provide intelligence and powerful insights into policy violations, internal and external threats, regulatory compliance, network, host, and user activity anomalies.

The Azure SIEM integrator enables you to integrate these logs from assets deployed in Azure to on-premises SIEM systems.

AZURE SECURITY AND AUDIT LOG SOURCES

Azure produces extensive logging for every service. These logs are categorized by two main types:

- Control Plane Logs
- Data plane logs (Diagnostic data)

Some of the key security and audit data sources available today are shown in the table below.

Log Source/Type	Description	SIEM Integration Status
Virtual Machines/Role Instances	Event log/Crash-dumps/IIS logs etc.	Supported Today
Azure Audit log	Management Operations (Create/Update/Delete API calls by Azure)	Supported Today
Storage	Storage Analytics Logs	
Network	• Network Security Group Logs (Events, Metrics etc.) • Azure Load Balancer Logs • Partner Security Appliances (e.g. WAF)	
Database	• SQL Audits	
Azure Key Vault	• Key Vault Logs	
Azure Active Directory	• Activities and Login Details	
Azure Security Center Alerts	• Alerts generated by ASC as well as from 3rd party partner solutions integrated with ASC	
Website/WebApp Logs	• Web App Diagnostic Logging	

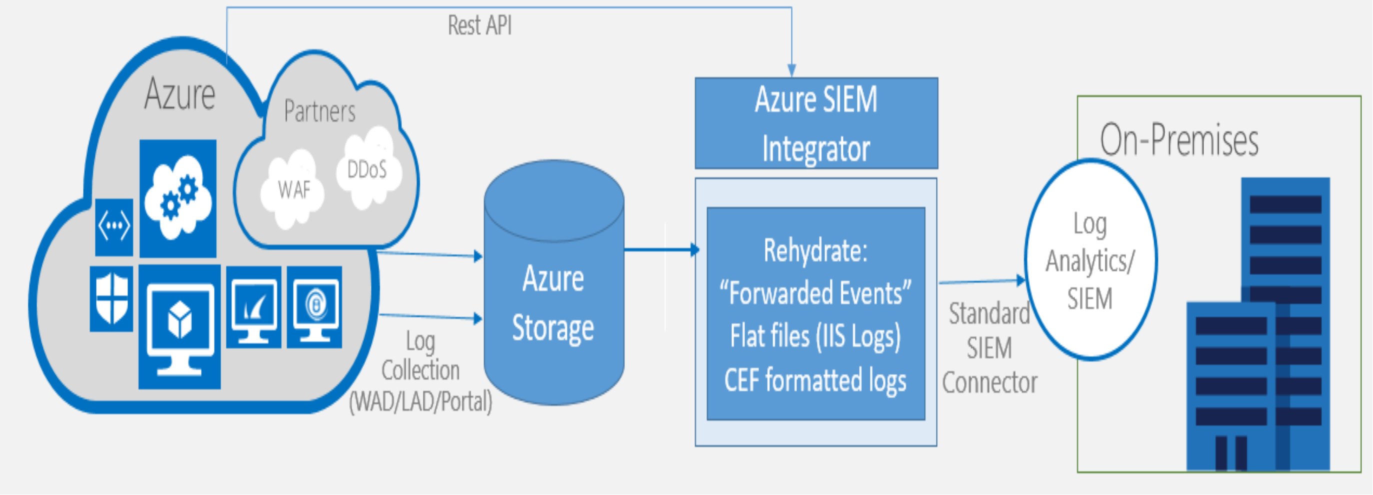
SIEM INTEGRATOR COMPONENTS

Azure SIEM integration has two parts

- Auditing and Collection: To turn on auditing, you can either do it in Azure Portal or with the Azure API and PowerShell cmdlets. Once auditing is enabled, most of the logs are stored in customer storage account. You can configure the retention period. Very few services (non-ARM based) store data centrally and expose the data through REST API.

- SIEM integration: The Azure SIEM integrator is a client side component that can be setup on machines in an on-premises environment or in a VM in Azure. The SIEM integrator collects data from Azure and rehydrates them as needed.

A high level architecture:



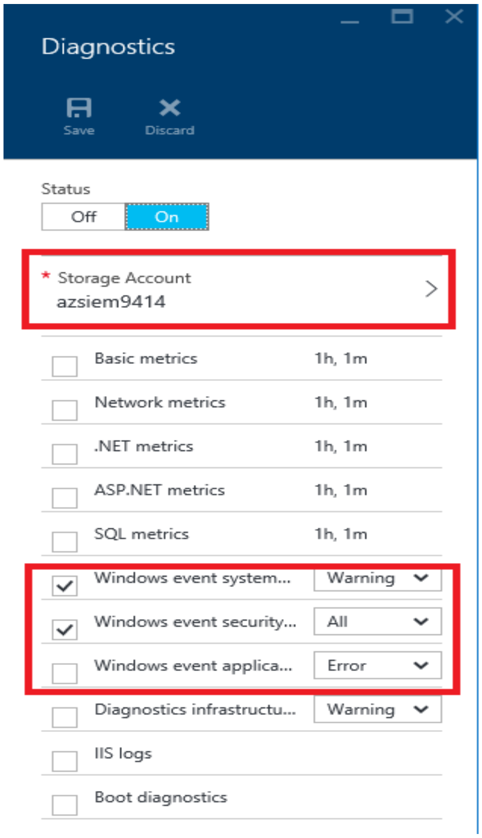
As shown above, the Azure resources and partner solutions produce audits and logs, which are either stored in customer storage accounts or accessible through rest api. Azure SIEM integrator which is a client side component that can be installed either on an on-premises machine or in VMs in azure that reads these logs and converts them to industry standard format (e.g. CEF or JSON) which is then hydrated to the SIEM without needing SIEM vendors to write any additional connectors.

HOW TO GET WINDOWS EVENT LOGS FROM VIRTUAL MACHINE TO THE SIEM?

STEP1: TURN ON LOG COLLECTION IN THE AZURE PORTAL

For an Azure Virtual Machine, you can turn on log collection using either the Azure portal or PowerShell cmdlets. To turn on log collection from the Azure portal:

1. Login to the Azure portal - https://portal.azure.com/
2. Click **Virtual Machines** from left service list
3. Click on the VM for which you want to turn on log collection
4. Click on **Diagnostics**
5. Configure the logs you would like to collect. Also select the storage account where the data will be landed.



Status
Off [✓ On]

* Storage Account
azsiem9414

□ Basic metrics 1h, 1m
□ Network metrics 1h, 1m
□ .NET metrics 1h, 1m
□ ASP.NET metrics 1h, 1m
□ SQL metrics 1h, 1m
☑ Windows event system... Warning
☑ Windows event security... All
□ Windows event applica... Error
□ Diagnostics infrastructu... Warning
□ IIS logs
□ Boot diagnostics

STEP2: SET UP THE AZURE SIEM INTEGRATOR

Prerequisites:

- You can install the SIEM integrator on a machine in on-premises or on virtual machine in Azure (Windows OS)
- This machine needs to have the standard SIEM agent installed (e.g. Splunk Universal Forwarder or ArcSight Windows Event Collector agent or Qradar wincollect) and pointing to the SIEM instance.
- This machine needs to have access to internet to connect to Azure storage (See FAQ for proxy scenario)

Setup:

1. Download the package from here and unzip it (Put it in a folder other than a directory inside any user profile)
2. Open an elevated cmd prompt
3. Run the command: `azsiem install accepteula`
4. Run the command:
   azsiem source add <**FriendlyNameForTheSource**> WAD **<Storage account Name> <StorageKey>**
   Example: `azsiem source add maheshsiemtest WAD azsiem9414 FullKey`
   Optionally, you can append the subscription ID to the friendly name if you would like the subscription id to show up in the event XML.
   `azsiem source add <FriendlyNameForTheSource.SubscriptionID> WAD <Storage account Name> <StorageKey>`

Note: The storage account name and key should match the storage account that you selected in log collection in step-1 above

5. Now you should start seeing the events in forwarded events folder on the same machine. Open **Event Viewer → Windows Event log → Forwarded Events**.
6. Make sure the standard SIEM connector (e.g. Splunk Universal Forwarder or ArcSight Windows Event Smart Collector or Qradar wincollect) installed on the machine is configured to pick events from forwarded events folder and pipe them to SIEM instance. Some screenshots are in the appendix (Windows Event in ArcSight, Windows Event in Splunk, Windows Events in QRadar)

HOW TO GET AZURE AUDIT LOGS TO THE SIEM?

1. Go to the same command window and type `azsiem createazureid`
   This command creates an Azure Active Directory Service Principal
2. Then run `azsiem authorize <Subscription Name>`
   (Note: You may see some warnings if you run the `authorize` command immediately after `createazureid`. This is because of few second latency between the AAD account creation and the account being available for use. If you wait about 10 seconds after running `createazureid` and then run `authorize`, then you should not see these warnings)

The command above assigns reader access on the subscription to the service principal. If you don't specify a subscription name, then the reader role will be assigned to all subscriptions you have admin access to.

3. Now you should start seeing Audit log JSON files in the directory below
   - \Users\azsiem\AzureResourceManagerJson
   - \Users\azsiem\AzureResourceManagerJsonLD

The tool generates both pretty printed and line delimited JSON.

4. Point the standard SIEM file forwarder connector to the appropriate folder to pipe the data to SIEM instance. You may need some field mappings based on SIEM product you are using.
   To learn more about Azure Audit log and the definition of properties, click the links below

   https://msdn.microsoft.com/library/azure/dn931934.aspx
   https://azure.microsoft.com/en-us/documentation/articles/resource-group-audit/

INTEGRATION WITH ARCSIGHT

For visual walk through please click here. High level steps are

i. Create a SmartMessage Receiver in ArcSight Logger
ii. On the Windows machine, install the “ArcSight Flex Connector JSON Folder Forwarder”
    1. Set the JSON Log Folder Location to “c:\Users\azsiem\AzureResourceManagerJson”
    2. Set the JSON Configuration File Name Prefix to “AzureRm”
iii. After the installation wizard is complete, copy AzureRM.jsonparser.properties (download from SIEM release drop site here) to “\Program Files\ArcSightSmartConnectors\current\user\agent\flexagent\AzureRM.jsonparser.properties”. The contents of “AzureRM.jsonparser.properties” can be modified as needed to change the mapping of Azure Resource Manager log entries to ArcSight events. See the Flex Connector documentation for the format of this file.
iv. The “ArcSight ArcSight FlexConnector JSON Folder Follower” service should be stopped initially after installation. If not, stop it from the services control panel application or from the command line using this command (The exact service name may be different if non-default options were chosen during setup)
    1. net stop "ArcSight ArcSight FlexConnector JSON Folder Follower"
v. Now, start the service from the control panel or from the command line using this command:
    1. net start "ArcSight ArcSight FlexConnector JSON Folder Follower"

Events should now be flowing to ArcSight Logger.

INTEGRATION WITH SPLUNK

Use Splunk Universal Forwarder to point to “c:\Users\azsiem\AzureResourceManagerJson”. Logs look like this

INTEGRATION WITH QRADAR

For detailed instructions, click here.

The high level steps are

- Install Log Source Extension (AzureRM_QRadarLogSourceExtension.xml. You can download from here)
- Create Custom Event properties to extract useful fields in Azure Resource Manager Operation Logs (e.g. Subscription ID, Resource Group, Operation Name)
- Add WinCollect File Forwarder Log Source to get events from “C:\Users\azsiem\AzureResourceManagerJsonLD” on the AZSIEM Machine (WinCollect agent must already be installed on that machine)

SCALE SUPPORT

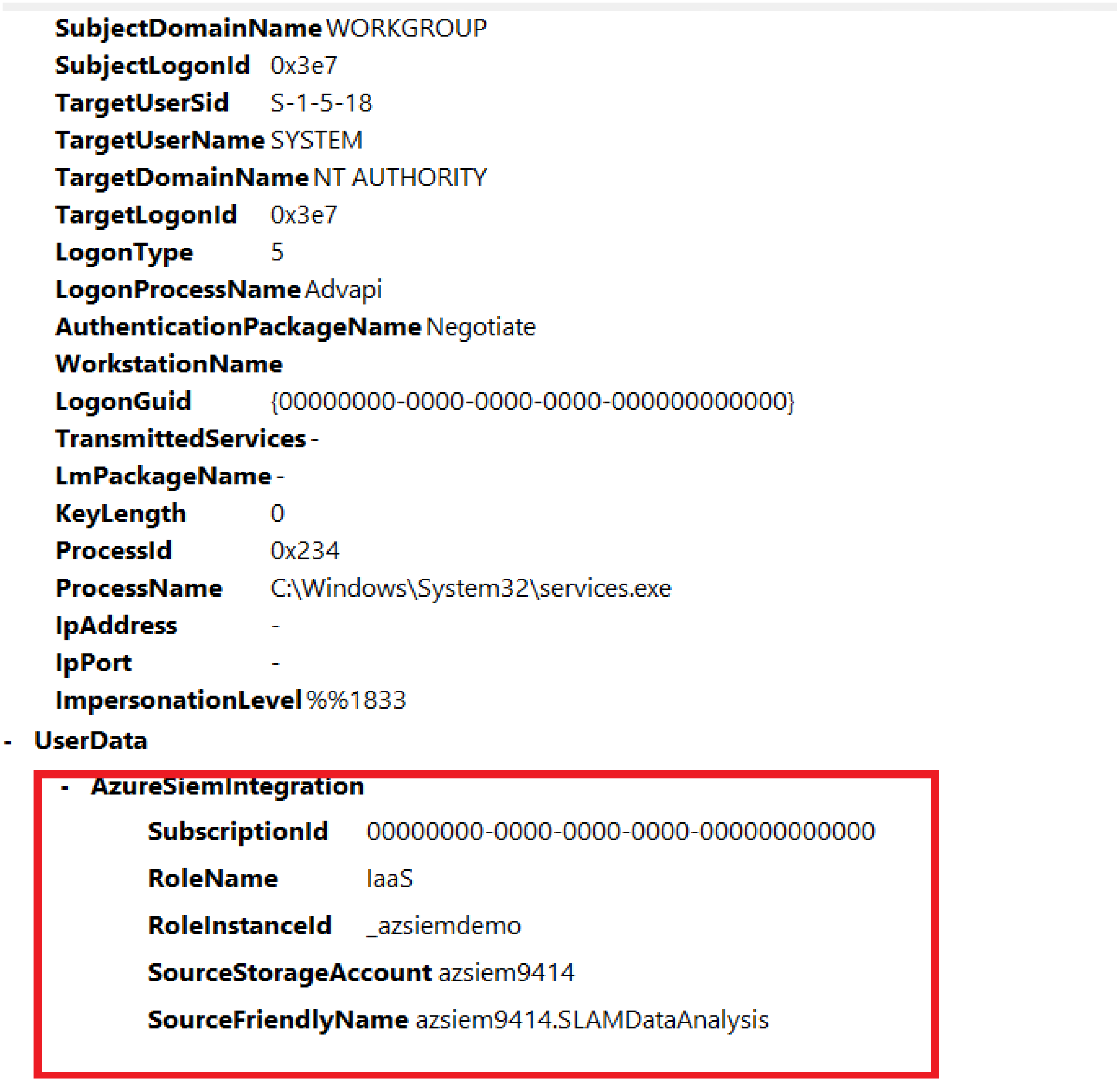
1. On a 8 proc machine – One single instance of SIEM integrator can process about 24 million events per day (1M / hour)
2. On a 4 proc machine – One single instance of SIEM integrator can process 1.5 million events per day (62.5K/hour).
3. You can run multiple instance of the SIEM integrators if event volume is high.

FAQ

1. **How to uninstall the application?**
   Open an elevated command prompt and go to the folder where azsiem binaries are located. Then run the command
   `Azsiem uninstall`
   If you have a created an azure id, then run the command `azsiem removeazureid` before running the uninstall command
2. **How can I see which are the storage account registered?**
   Run the command `azsiem source list`
3. **Our proxy setting does not allow azure storage access directly. How can I update the proxy configuration?**
   Open the **AZSIEM.EXE.CONFIG** file in the same directory **azsiem.exe** is located. Update the file to include the highlighted section with your proxy address. After update is done, stop and start the service (`net stop azsiem` and `net start azsiem`)

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <system.net>
    <connectionManagement>
      <add address="*" maxconnection="400" />
    </connectionManagement>
    <defaultProxy>
      <proxy
        usesystemdefault="true"
        proxyaddress="http://127.0.0.1:8888"
        bypassonlocal="true"
      />
    </defaultProxy>
  </system.net>
  <system.diagnostics>
    <performanceCounters filemappingsize="20971520" />
  </system.diagnostics>
```

4. **How can I see the subscription information in windows events?**
   If you provide a subscriptionid appended to friendly name while adding sources, then the event XML will have the metadata as shown below.



```
    SubjectDomainName WORKGROUP
    SubjectLogonId    0x3e7
    TargetUserSid     S-1-5-18
    TargetUserName SYSTEM
    TargetDomainName NT AUTHORITY
    TargetLogonId     0x3e7
    LogonType         5
    LogonProcessName Advapi
    AuthenticationPackageName Negotiate
    WorkstationName
    LogonGuid         {00000000-0000-0000-0000-000000000000}
    TransmittedServices -
    LmPackageName -
    KeyLength         0
    ProcessId         0x234
    ProcessName       C:\Windows\System32\services.exe
    IpAddress         -
    IpPort            -
    ImpersonationLevel %%1833
- UserData
  - AzureSiemIntegration
        SubscriptionId    00000000-0000-0000-0000-000000000000
        RoleName          IaaS
        RoleInstanceId    _azsiemdemo
        SourceStorageAccount azsiem9414
        SourceFriendlyName azsiem9414.SLAMDataAnalysis
```

5. **How can I disable telemetry collection?**

   You can run the command `azsiem disabletelemetry`

6. Where can I find the definition of the properties in audit log?

   https://msdn.microsoft.com/library/azure/dn931934.aspx
   https://azure.microsoft.com/en-us/documentation/articles/resource-group-audit/

7.

TROUBLESHOOTING

1. If you see no data is showing up in Forwarded Events folder, then check the following:
    a. Check the machine and confirm that it can access Azure. Try to open the Azure Portal (www.portal.azure.com) from the browser
    b. Make sure **azsiem** has write permission on the folder **users\azsiem**
    c. Make sure the source is not empty and storage name and key is correct. Run the command to find
    ```
    azsiem source list
    ```
    d. Make sure storage account configured for Diagnostics matches the storage account added to the source
    e. If all of the above is configured correctly, you may want to see the windows event log → Application channel to see if there are any errors reported from the SIEM integrator.
    f. Still issue is not resolved ??
        i. Download the storage explorer
        ii. Connect to the storage account configured for diagnostics collection.
        iii. Browse to the table – WadWindowsEventLogsTable to see if there is any data. If not, then diagnostics in the VM is not configured correctly

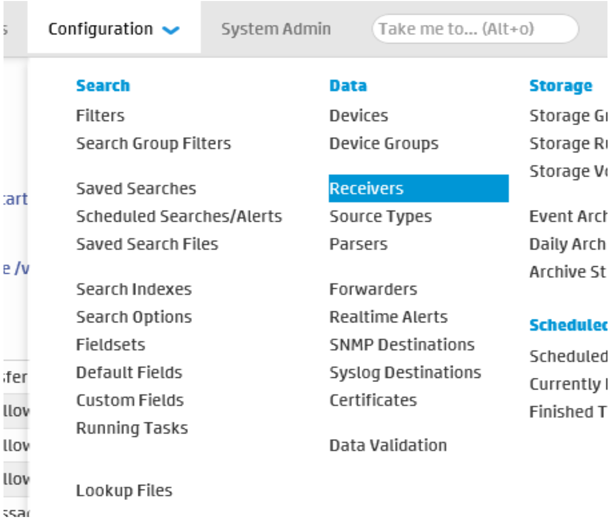
CONTACT US

Email: azuresiem@microsoft.com

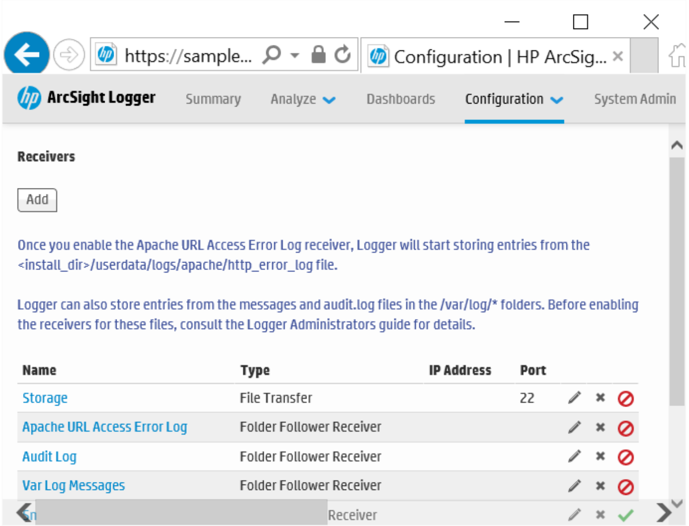
APPENDIX

AZURE AUDIT LOG INTEGRATION IN ARCSIGHT - VISUAL WALKTHROUGH

Step1: If you do not already have a “SmartMessage Receiver”, create one in ArcSight Logger by going to the “Receivers” page under the “Configuration” tab:



Choose “Add”

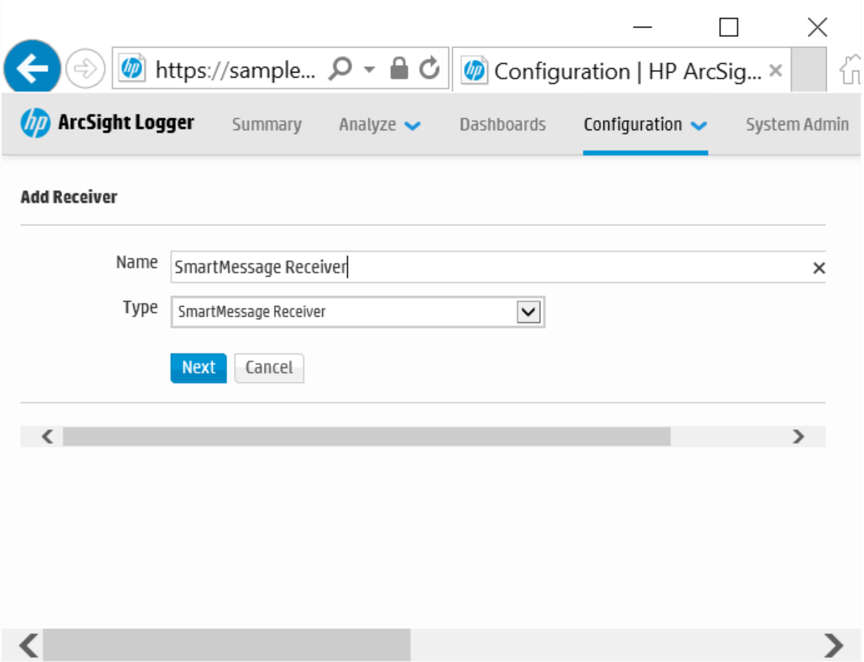


Once you enable the Apache URL Access Error Log receiver, Logger will start storing entries from the <install_dir>/userdata/logs/apache/http_error_log file.

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
Storage	File Transfer		22
Apache URL Access Error Log	Folder Follower Receiver		
Audit Log	Folder Follower Receiver		
Var Log Messages	Folder Follower Receiver		
	Receiver		

Choose “SmartMessage Receiver” and name it “SmartMessage Receiver”

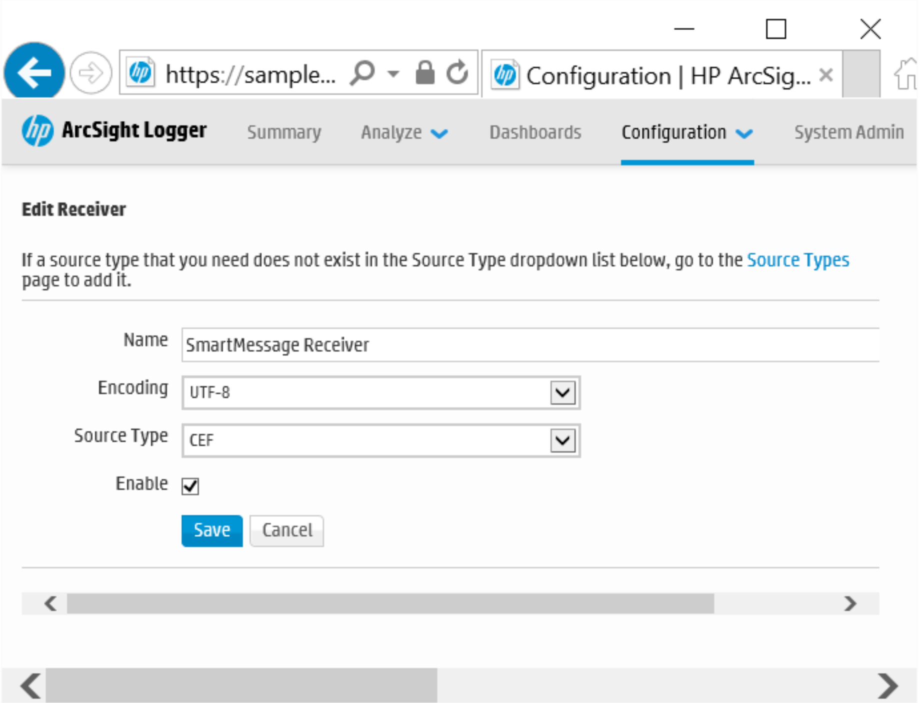


Add Receiver

Name: SmartMessage Receiver

Type: SmartMessage Receiver

Accept the choices on the next page



Edit Receiver

If a source type that you need does not exist in the Source Type dropdown list below, go to the Source Types page to add it.

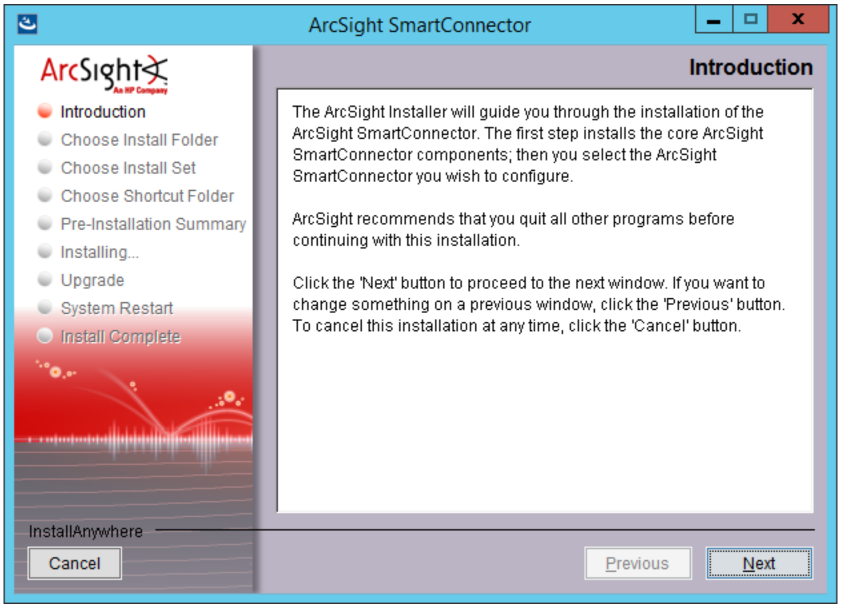
Name: SmartMessage Receiver

Encoding: UTF-8

Source Type: CEF

Enable: ☑

Now, on the Windows box with the Azure SIEM Integration Service, launch the ArcSight SmartConnector installation wizard and choose Next:



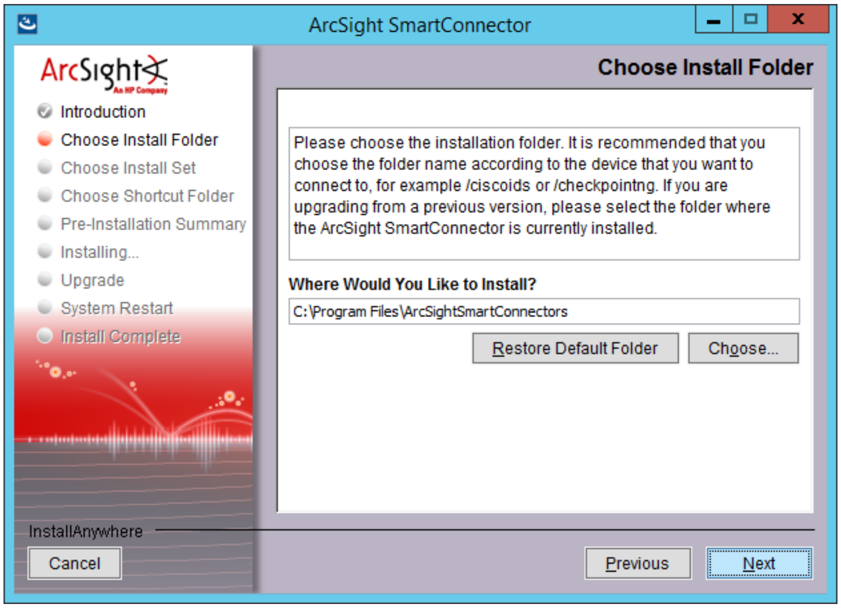
Introduction

The ArcSight Installer will guide you through the installation of the ArcSight SmartConnector. The first step installs the core ArcSight SmartConnector components; then you select the ArcSight SmartConnector you wish to configure.

ArcSight recommends that you quit all other programs before continuing with this installation.

Click the 'Next' button to proceed to the next window. If you want to change something on a previous window, click the 'Previous' button. To cancel this installation at any time, click the 'Cancel' button.

On Installation Folder page, choose Next



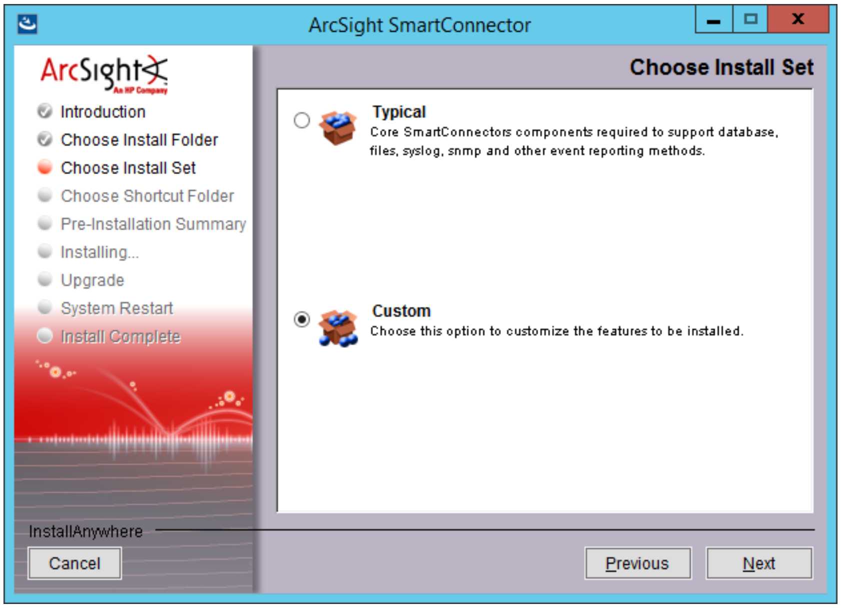
Choose Install Folder

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?

C:\Program Files\ArcSightSmartConnectors

On Install Set page, choose Custom



ArcSight SmartConnector

Choose Install Set

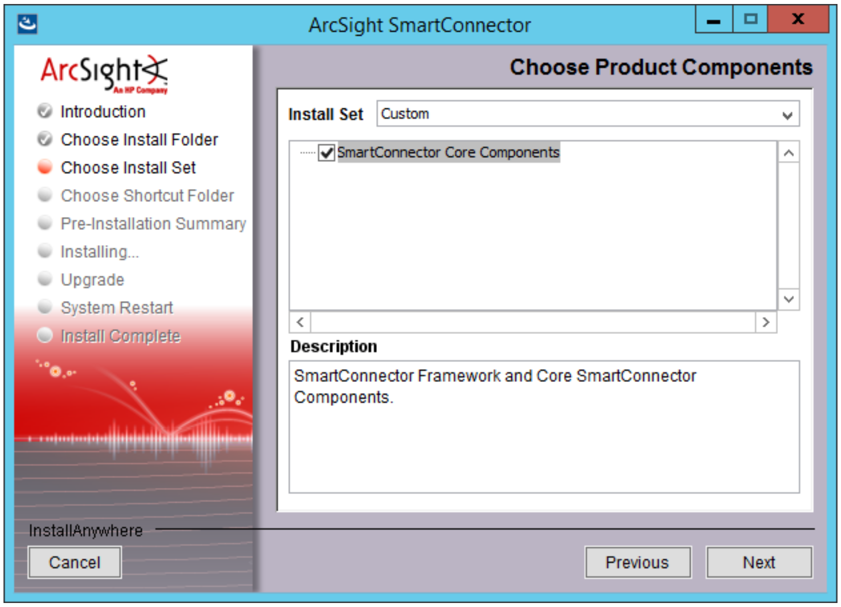
○ Typical

Core SmartConnectors components required to support database, files, syslog, snmp and other event reporting methods.

● Custom

Choose this option to customize the features to be installed.

On Product Components page, select Next



ArcSight SmartConnector

Choose Product Components

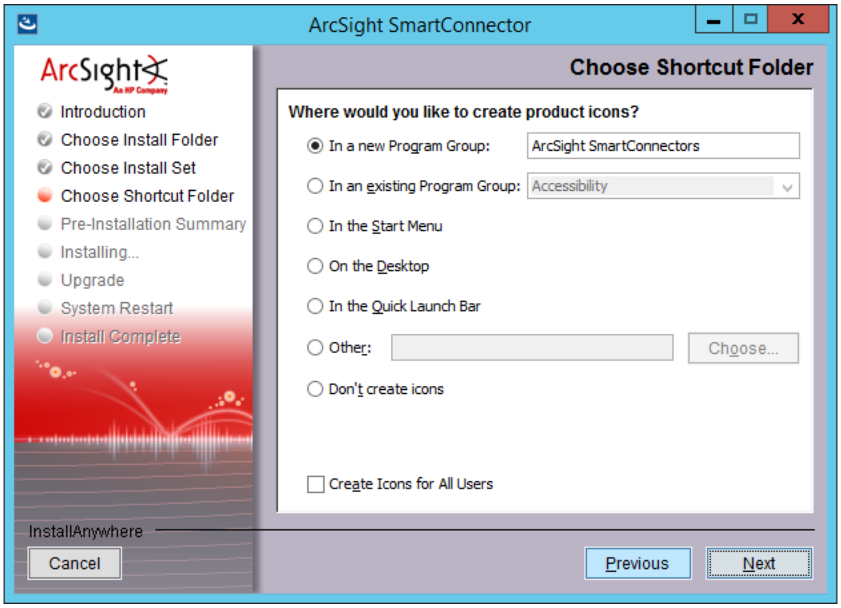
Install Set: Custom

☑ SmartConnector Core Components

Description

SmartConnector Framework and Core SmartConnector Components.

On Shortcut Folder page, select Next



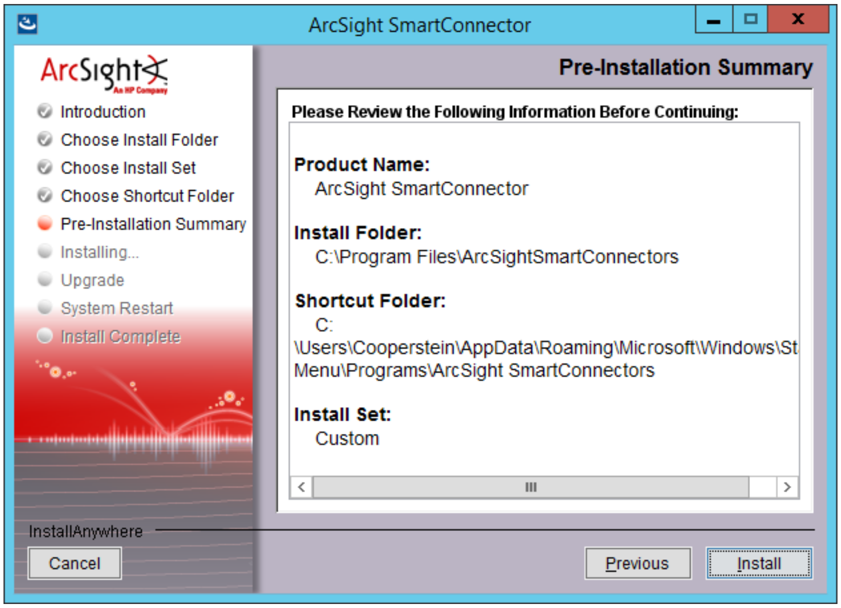
Choose Shortcut Folder

Where would you like to create product icons?

- ● In a new Program Group: ArcSight SmartConnectors
- ○ In an existing Program Group: Accessibility
- ○ In the Start Menu
- ○ On the Desktop
- ○ In the Quick Launch Bar
- ○ Other: Choose...
- ○ Don't create icons

□ Create Icons for All Users

On Summary page, select Next



Pre-Installation Summary

Please Review the Following Information Before Continuing:

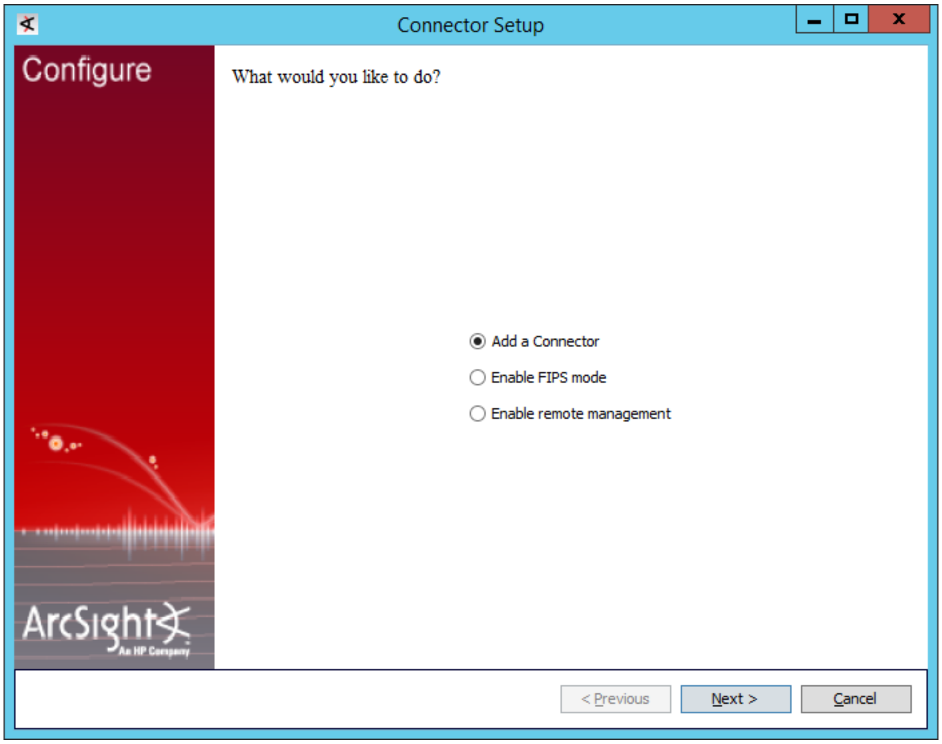
Product Name:
ArcSight SmartConnector

Install Folder:
C:\Program Files\ArcSightSmartConnectors

Shortcut Folder:
C:
\Users\Cooperstein\AppData\Roaming\Microsoft\Windows\St
Menu\Programs\ArcSight SmartConnectors

Install Set:
Custom

On next page, choose “Add a Connector” and select Next



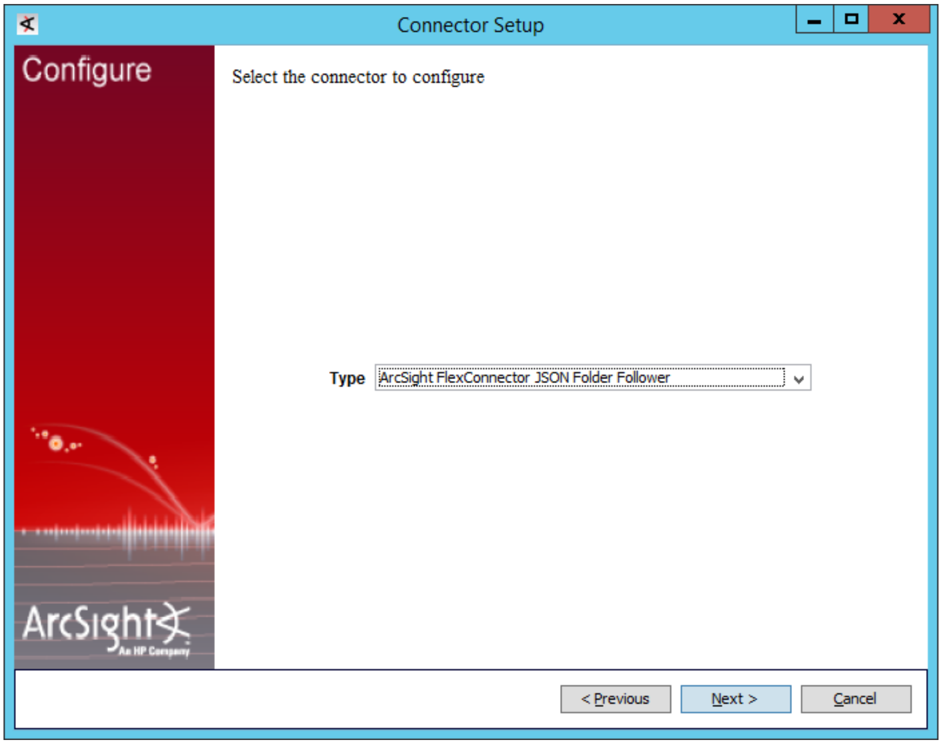
What would you like to do?

● Add a Connector

○ Enable FIPS mode

○ Enable remote management

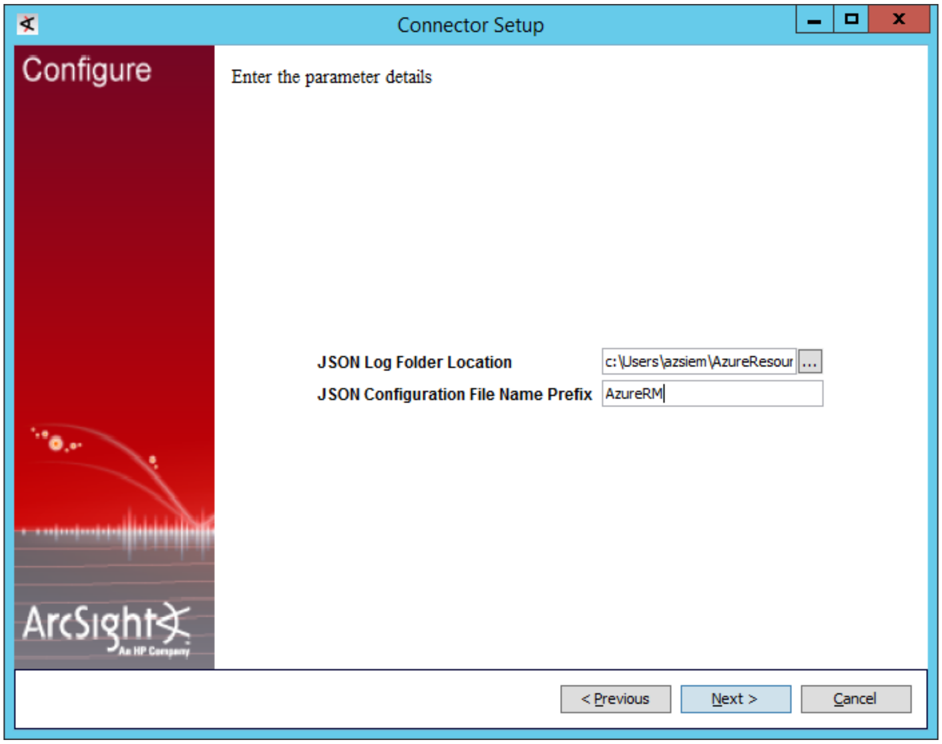
On next page, choose "ArcSight FlexConnector JSON Folder Follower"



Select the connector to configure

Type: ArcSight FlexConnector JSON Folder Follower

On next page, set the Folder Location to the path where JSON logs are being written (e.g. “c:\Users\azsiem\AzureResourceManagerJson”). Also, set the Configuration File Name Prefix to “AzureRM” and select Next

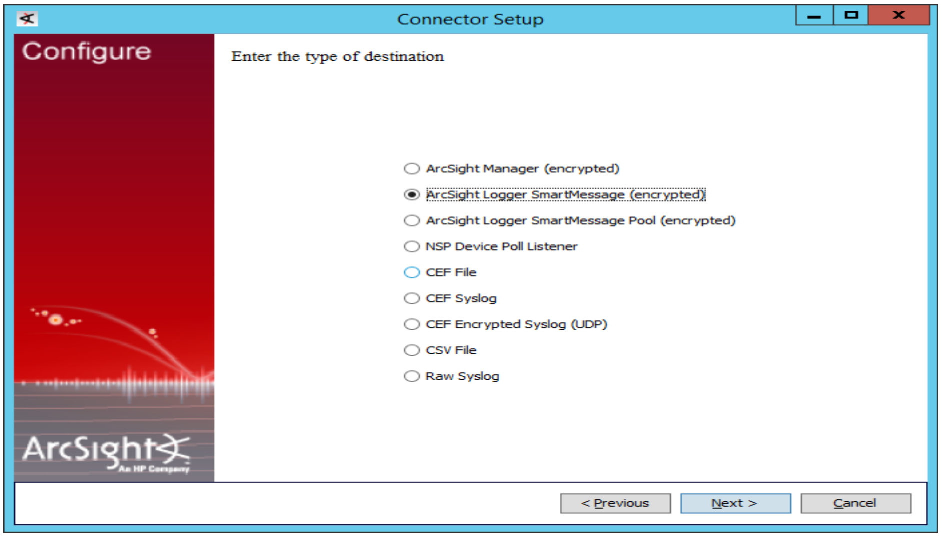


Enter the parameter details

JSON Log Folder Location: c:\Users\azsiem\AzureResour

JSON Configuration File Name Prefix: AzureRM

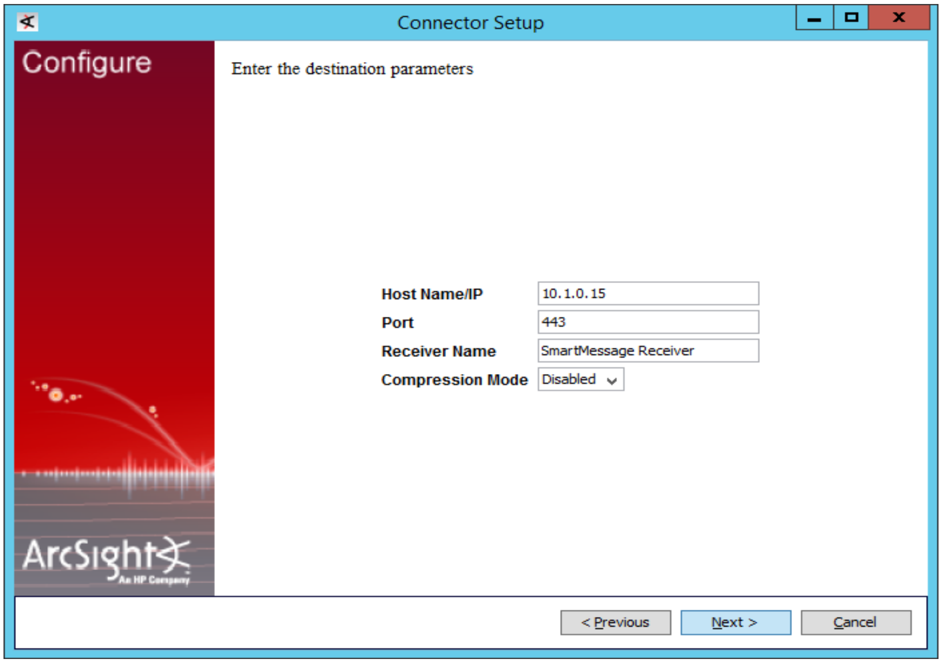
On next page, select “ArcSight Logger SmartMessage(encrypted)” and select Next



Enter the type of destination

○ ArcSight Manager (encrypted)
● ArcSight Logger SmartMessage (encrypted)
○ ArcSight Logger SmartMessage Pool (encrypted)
○ NSP Device Poll Listener
○ CEF File
○ CEF Syslog
○ CEF Encrypted Syslog (UDP)
○ CSV File
○ Raw Syslog

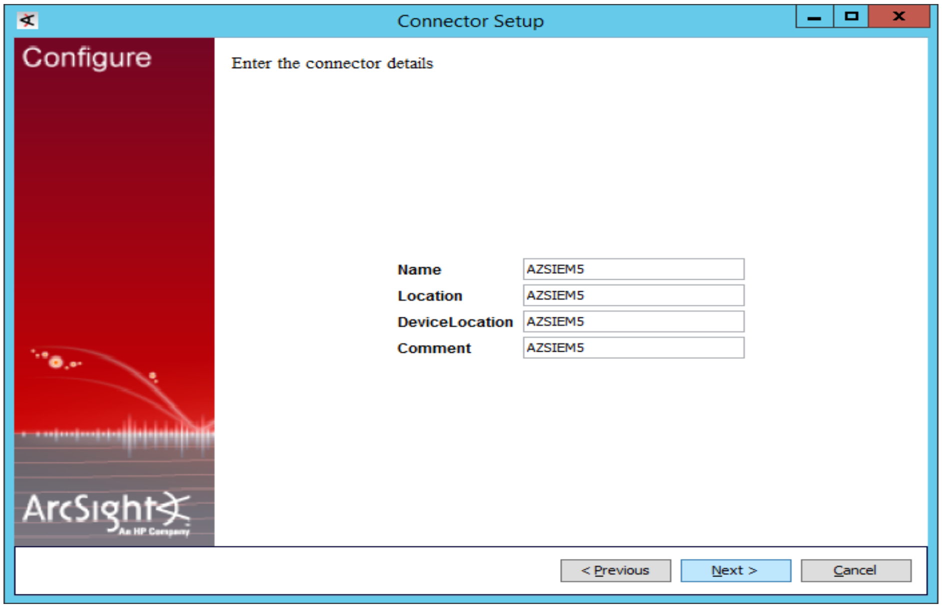
On next page, enter the ArcSight Logger machine's IP address and the Receiver Name of the SmartMessage receiver (e.g. "SmartMessage Receiver" if that's the name you used when creating a SmartMessage Receiver).



Enter the destination parameters

Host Name/IP	10.1.0.15
Port	443
Receiver Name	SmartMessage Receiver
Compression Mode	Disabled

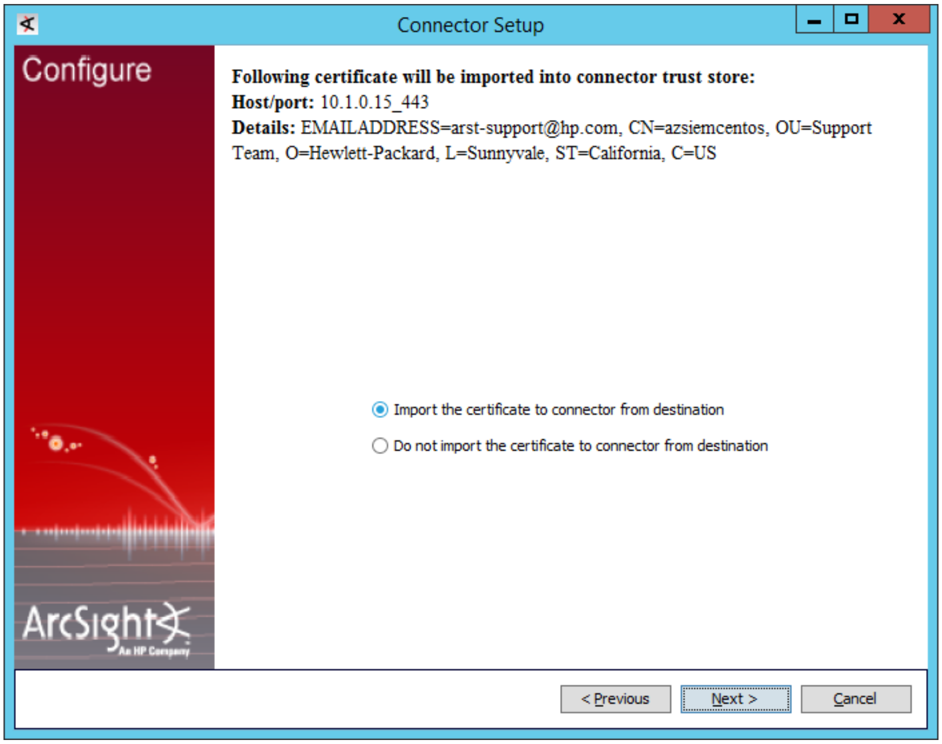
On next page, fill in information about the connector's machine (sample information shown)



Enter the connector details

Name	AZSIEM5
Location	AZSIEM5
DeviceLocation	AZSIEM5
Comment	AZSIEM5

The next page may be shown to ask you to import the certificate from the ArcSight Logger machine:

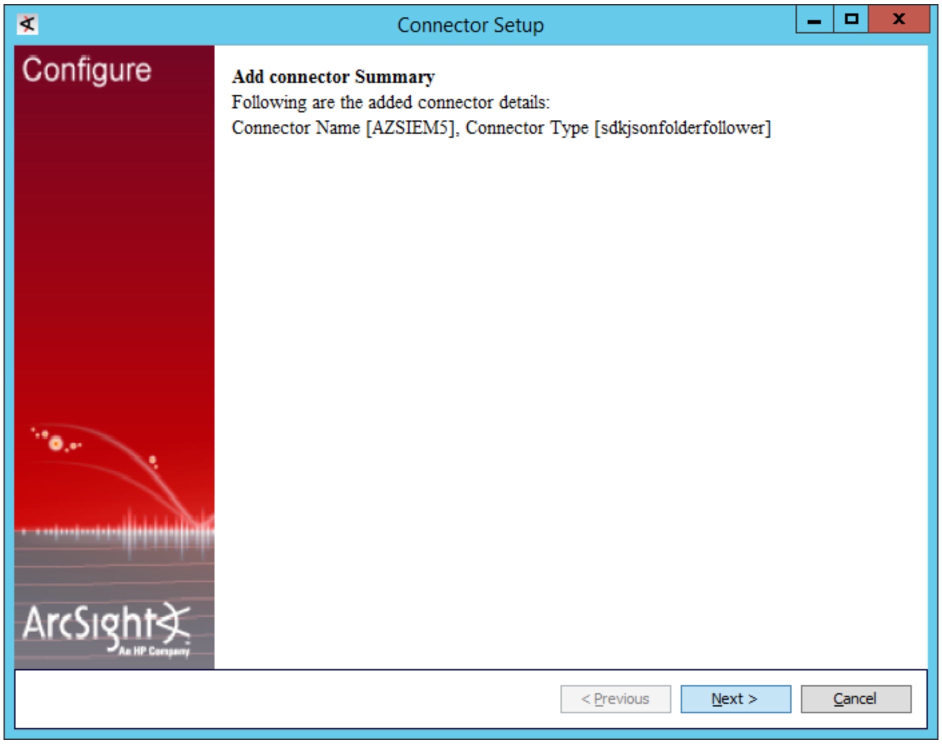


Following certificate will be imported into connector trust store:
Host/port: 10.1.0.15_443
Details: EMAILADDRESS=arst-support@hp.com, CN=azsiemcentos, OU=Support Team, O=Hewlett-Packard, L=Sunnyvale, ST=California, C=US

● Import the certificate to connector from destination

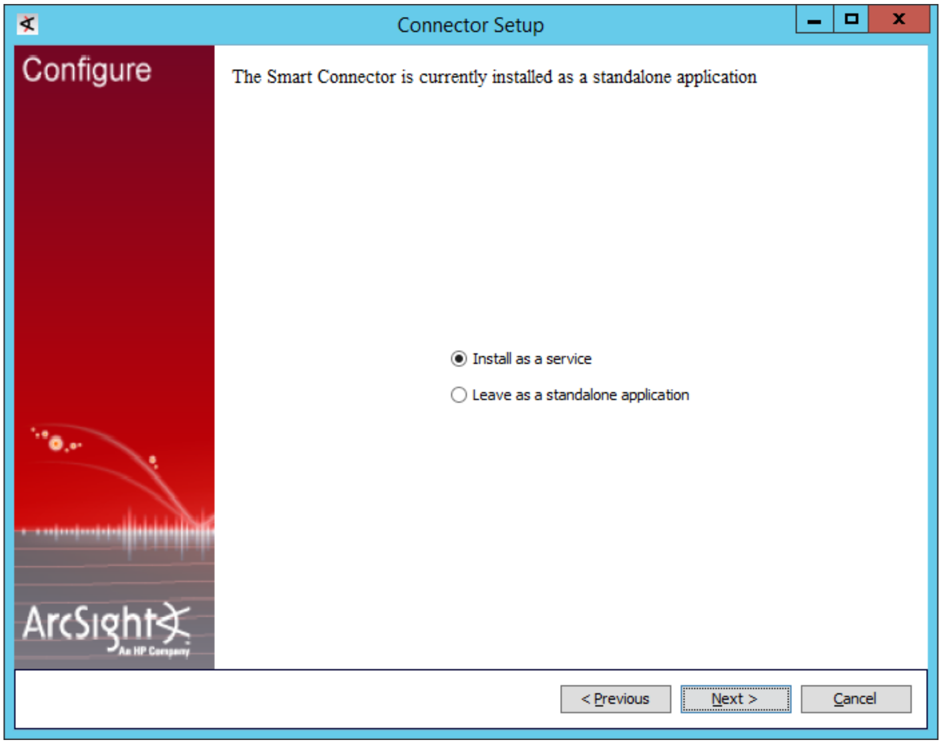
○ Do not import the certificate to connector from destination

On the summary page, select Next



Add connector Summary
Following are the added connector details:
Connector Name [AZSIEM5], Connector Type [sdkjsonfolderfollower]

On the next page, select “Install as a service”

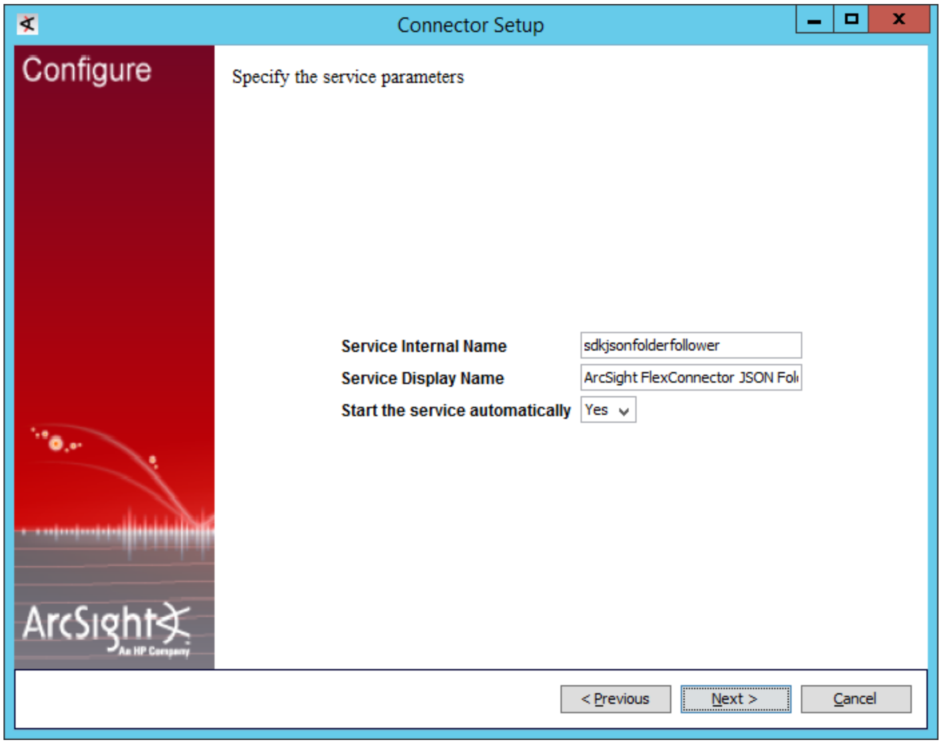


The Smart Connector is currently installed as a standalone application

● Install as a service

○ Leave as a standalone application

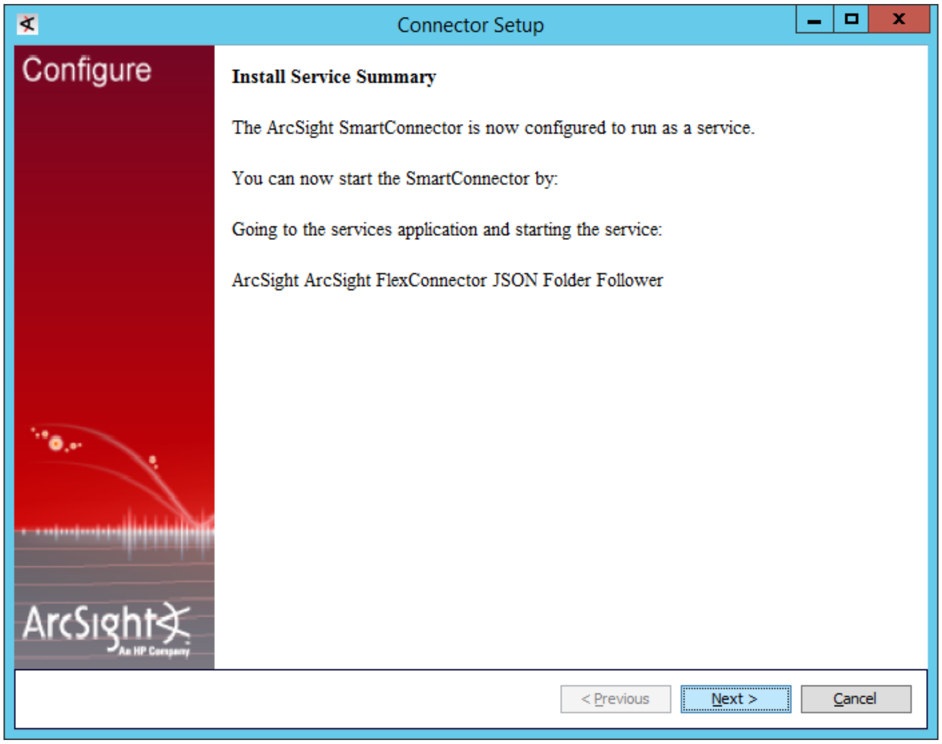
On the next page, leave the defaults alone:



Specify the service parameters

Service Internal Name	sdkjsonfolderfollower
Service Display Name	ArcSight FlexConnector JSON Fol
Start the service automatically	Yes

On the summary page, select Next



Install Service Summary

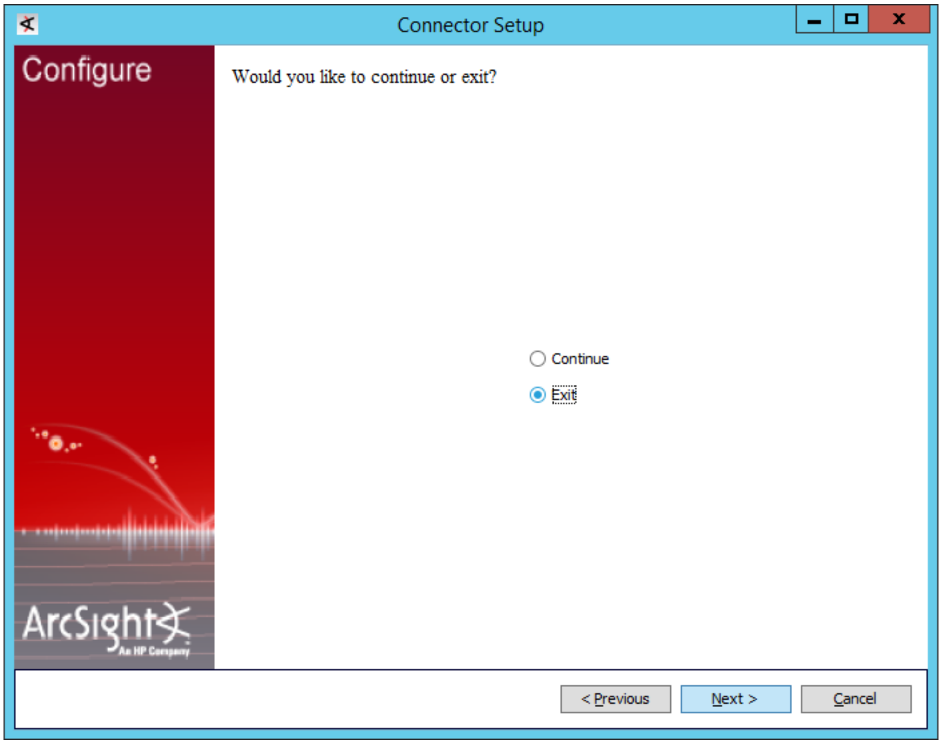
The ArcSight SmartConnector is now configured to run as a service.

You can now start the SmartConnector by:

Going to the services application and starting the service:

ArcSight ArcSight FlexConnector JSON Folder Follower

On the next page, select Exit

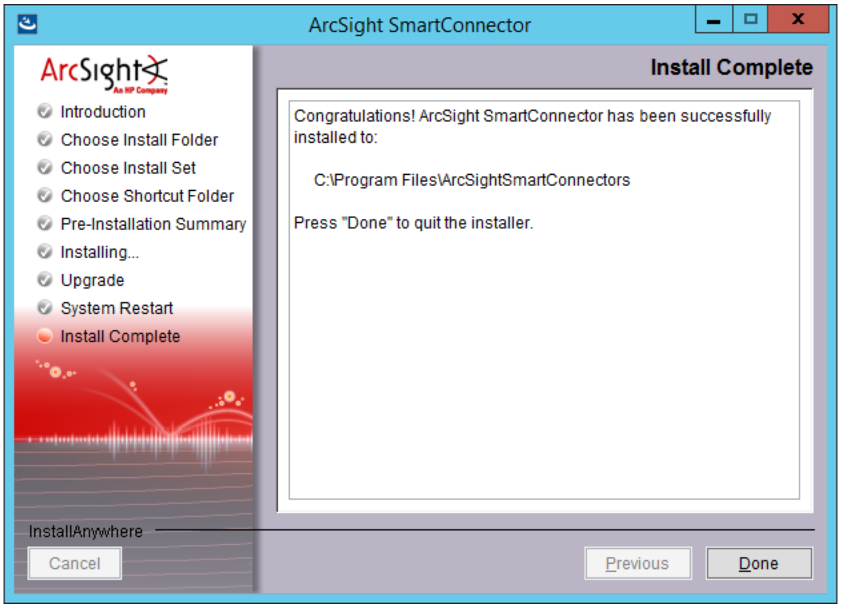


Would you like to continue or exit?

○ Continue

● Exit

You should now be at the final page of installation:



Install Complete

Congratulations! ArcSight SmartConnector has been successfully installed to:

C:\Program Files\ArcSightSmartConnectors

Press "Done" to quit the installer.

After the installation wizard is complete, download AzureRM.jsonparser.properties and copy to "\Program Files\ArcSightSmartConnectors\current\user\agent\flexagent\AzureRM.jsonparser.properties". The contents of "AzureRM.jsonparser.properties" can be modified as needed to change the mapping of Azure Resource Manager log entries to ArcSight events. See the Flex Connector documentation for the format of this file.

At this point, the "ArcSight ArcSight FlexConnector JSON Folder Follower" service should be stopped initially after installation. If not, stop it from the services control panel application or from the command line using this command (The exact service name may be different if non-default options were chosen during setup).

- net stop "ArcSight ArcSight FlexConnector JSON Folder Follower"

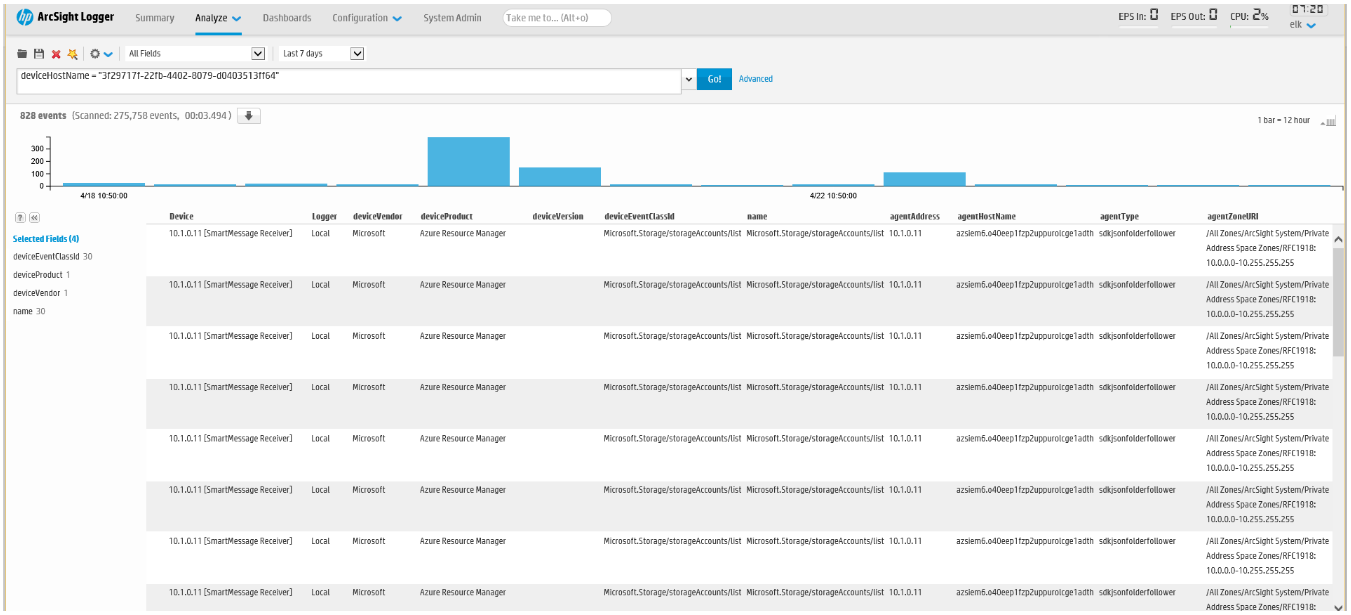
Stopping the service before starting it should insure that the "AzureRM.jsonparser.properties" file is picked up.

Now, start the service from the control panel or from the command line using this command:

- net start "ArcSight ArcSight FlexConnector JSON Folder Follower"

Events should now be flowing to ArcSight logger

Here is a screenshot of Azure Audit logs in ArcSight



All Fields | Last 7 days

deviceHostName = "3f29717f-22fb-4402-8079-d0403513ff64"

828 events (Scanned: 275,758 events, 00:03.494)

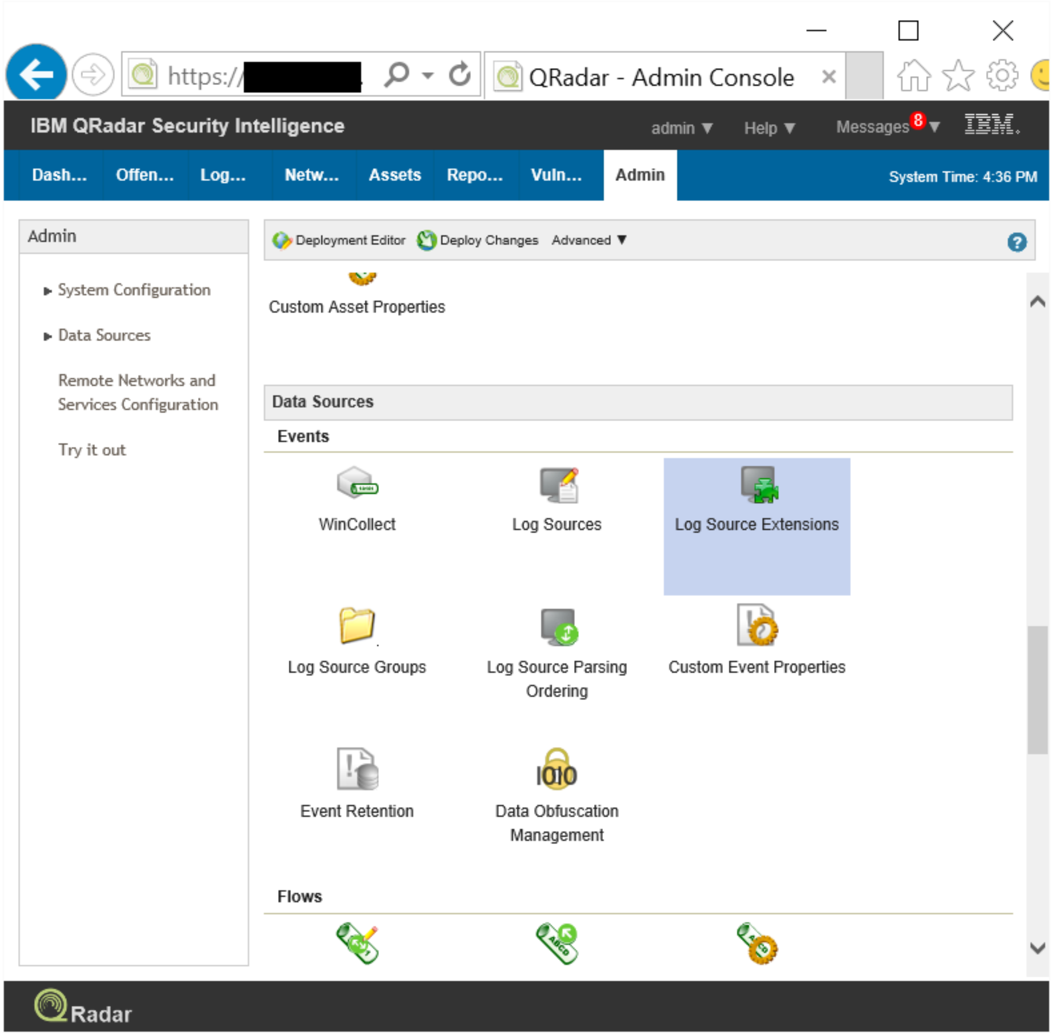
Selected Fields (4)
deviceEventClassId 30
deviceProduct 1
deviceVendor 1
name 30

Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassId	name	agentAddress	agentHostName	agentType	agentZoneURI
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255
10.1.0.11 [SmartMessage Receiver]	Local	Microsoft	Azure Resource Manager		Microsoft.Storage/storageAccounts/list	Microsoft.Storage/storageAccounts/list	10.1.0.11	azsiem6.o40eep1fzp2uppurolcge1adth	sdkjsonfolderfollower	/All Zones/ArcSight System/Private Address Space Zones/RFC1918:

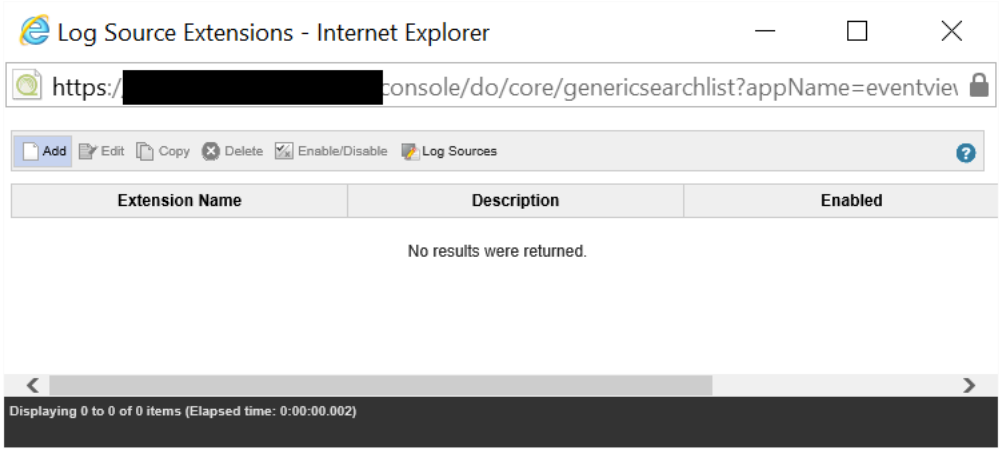
AZURE AUDIT LOG INTEGRATION IN QRADAR – DETAILED INSTRUCTIONS

These instructions assume you already have AZSIEM installed on a machine along with a WinCollect agent already configured as a Log Source in QRadar.

From the “Admin” tab, select “Log Source Extensions”


https://[redacted]
QRadar - Admin Console
IBM QRadar Security Intelligence
admin ▼
Help ▼
Messages 8 ▼
IBM.
Dash...
Offen...
Log...
Netw...
Assets
Repo...
Vuln...
Admin
System Time: 4:36 PM
Admin
▸ System Configuration
▸ Data Sources
Remote Networks and Services Configuration
Try it out
Deployment Editor
Deploy Changes
Advanced ▼
Custom Asset Properties
Data Sources
Events
WinCollect
Log Sources
Log Source Extensions
Log Source Groups
Log Source Parsing Ordering
Custom Event Properties
Event Retention
Data Obfuscation Management
Flows
QRadar

Select “Add”



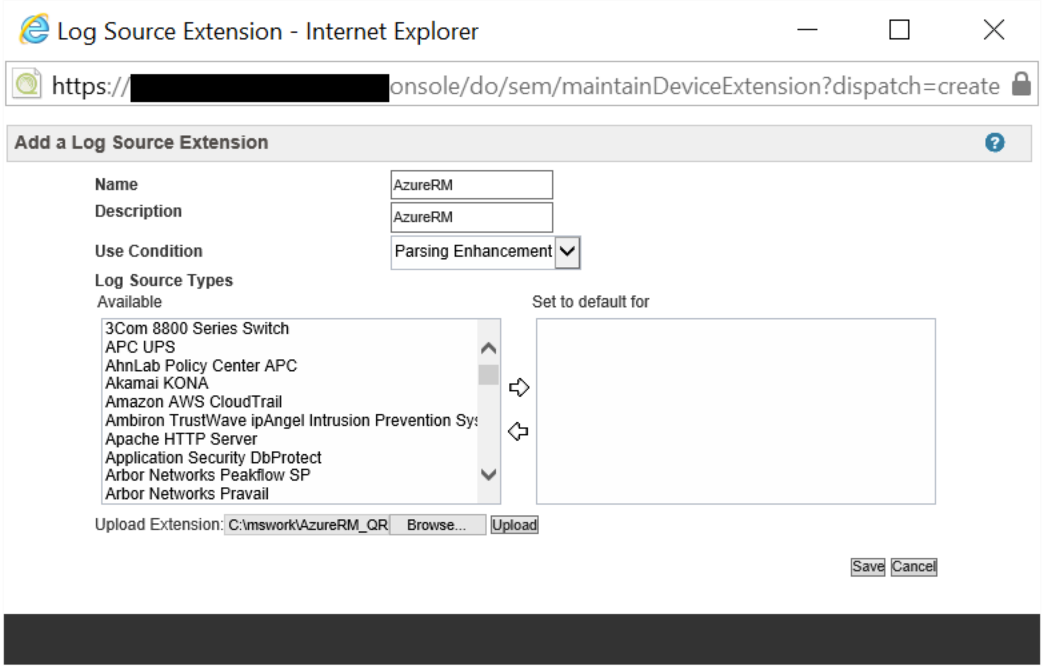
https:/[redacted]console/do/core/genericsearchlist?appName=eventviev

Extension Name	Description	Enabled

No results were returned.

Displaying 0 to 0 of 0 items (Elapsed time: 0:00:00.002)

Set the name and description to "AzureRM". Browse for the file "AzureRM_QRadarLogSourceExtension.xml". Then select "Upload" (Note – The Use Condition value is ignored in current versions of QRadar):



https://[redacted]onsole/do/sem/maintainDeviceExtension?dispatch=create

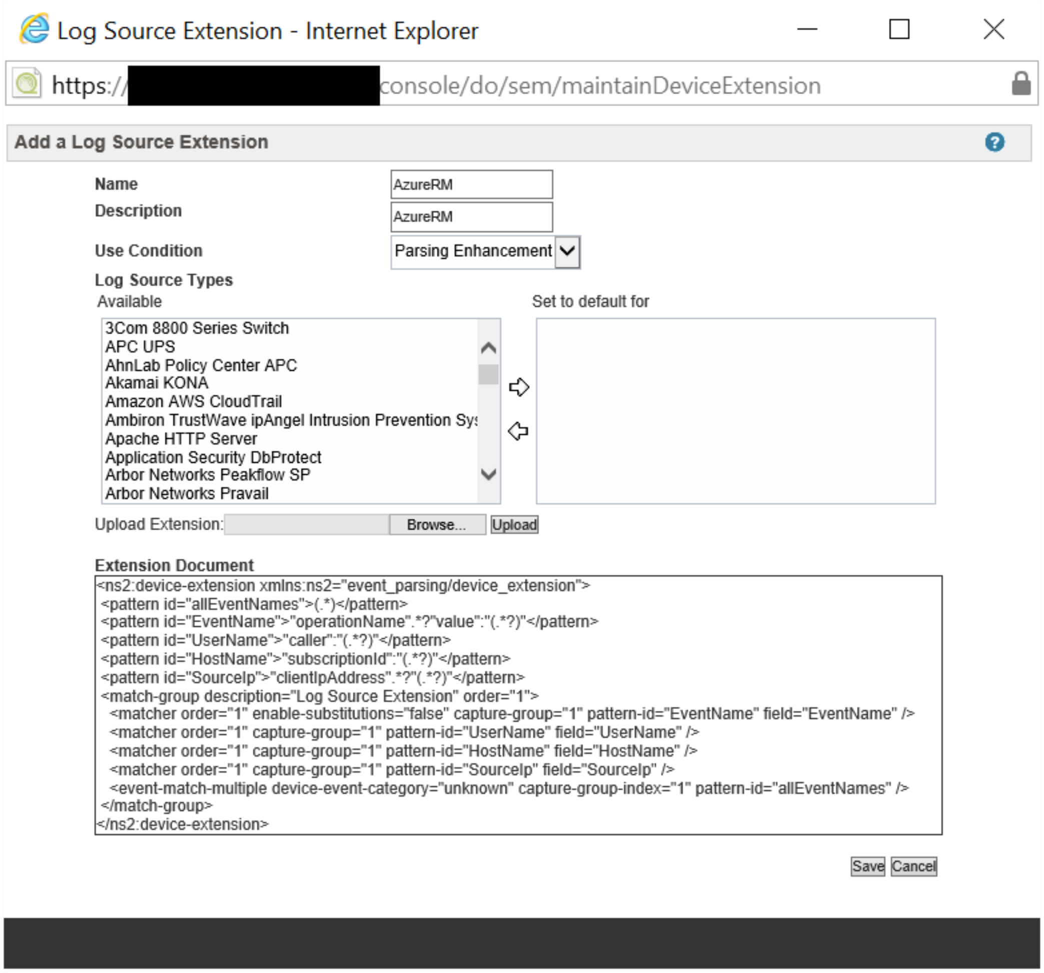
Add a Log Source Extension

Name: AzureRM
Description: AzureRM
Use Condition: Parsing Enhancement
Log Source Types
Available:
3Com 8800 Series Switch
APC UPS
AhnLab Policy Center APC
Akamai KONA
Amazon AWS CloudTrail
Ambiron TrustWave ipAngel Intrusion Prevention Sys
Apache HTTP Server
Application Security DbProtect
Arbor Networks Peakflow SP
Arbor Networks Pravail

Set to default for

Upload Extension: C:\mswork\AzureRM_QR

Select Save after the Log Source Extension has been uploaded:



https://[redacted]console/do/sem/maintainDeviceExtension

Add a Log Source Extension

Name: AzureRM

Description: AzureRM

Use Condition: Parsing Enhancement

Log Source Types

Available:

3Com 8800 Series Switch
APC UPS
AhnLab Policy Center APC
Akamai KONA
Amazon AWS CloudTrail
Ambiron TrustWave ipAngel Intrusion Prevention Sys
Apache HTTP Server
Application Security DbProtect
Arbor Networks Peakflow SP
Arbor Networks Pravail

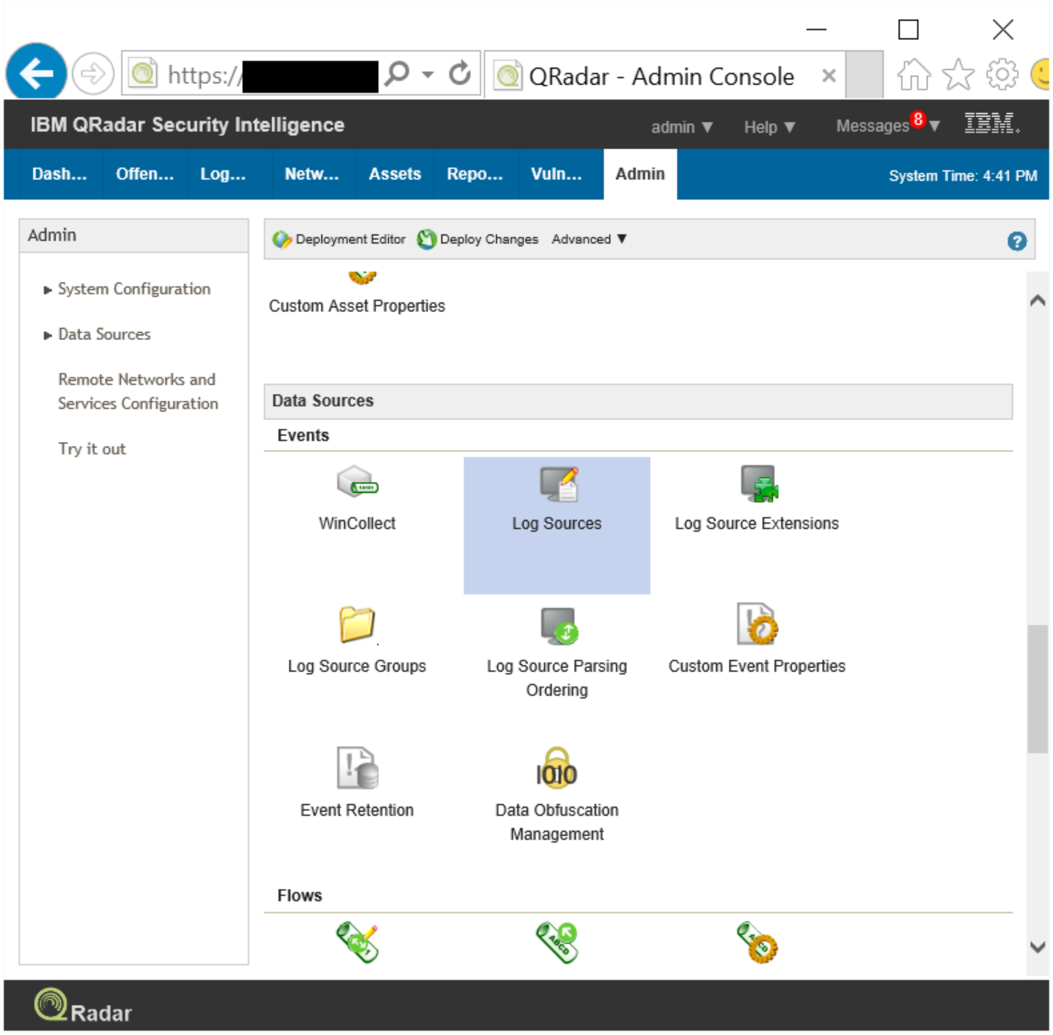
Set to default for

Upload Extension:

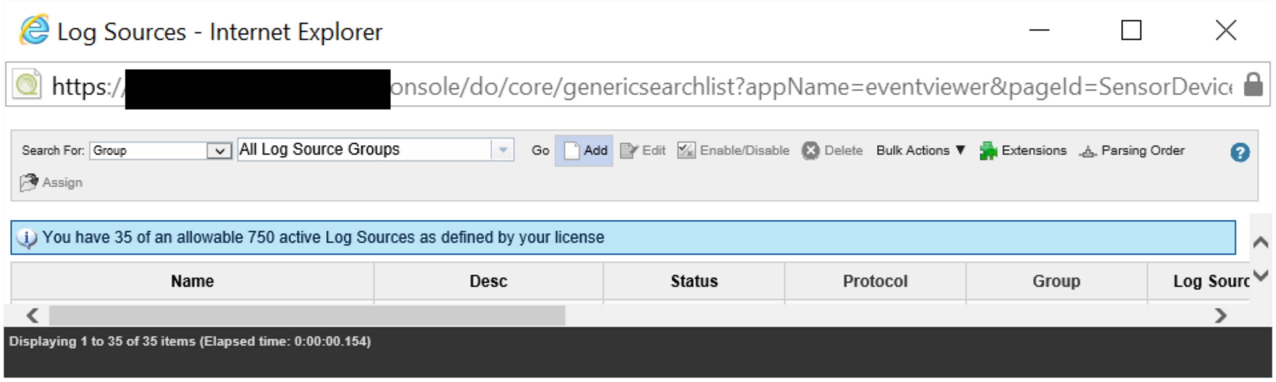
Extension Document

```
<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
 <pattern id="allEventNames">(.*)</pattern>
 <pattern id="EventName">"operationName".*?"value":"(.*?)"</pattern>
 <pattern id="UserName">"caller":"(.*?)"</pattern>
 <pattern id="HostName">"subscriptionId":"(.*?)"</pattern>
 <pattern id="SourceIp">"clientIpAddress".*?"(.*?)"</pattern>
 <match-group description="Log Source Extension" order="1">
  <matcher order="1" enable-substitutions="false" capture-group="1" pattern-id="EventName" field="EventName" />
  <matcher order="1" capture-group="1" pattern-id="UserName" field="UserName" />
  <matcher order="1" capture-group="1" pattern-id="HostName" field="HostName" />
  <matcher order="1" capture-group="1" pattern-id="SourceIp" field="SourceIp" />
  <event-match-multiple device-event-category="unknown" capture-group-index="1" pattern-id="allEventNames" />
 </match-group>
</ns2:device-extension>
```

After Saving, close the list of Log Source Extensions and return to the “Admin” tab and choose “Log Sources”



Choose “Add”


Log Sources - Internet Explorer
https://[redacted]onsole/do/core/genericsearchlist?appName=eventviewer&pageId=SensorDevic
Search For: Group
All Log Source Groups
Go
Add
Edit
Enable/Disable
Delete
Bulk Actions ▼
Extensions
Parsing Order
Assign

You have 35 of an allowable 750 active Log Sources as defined by your license

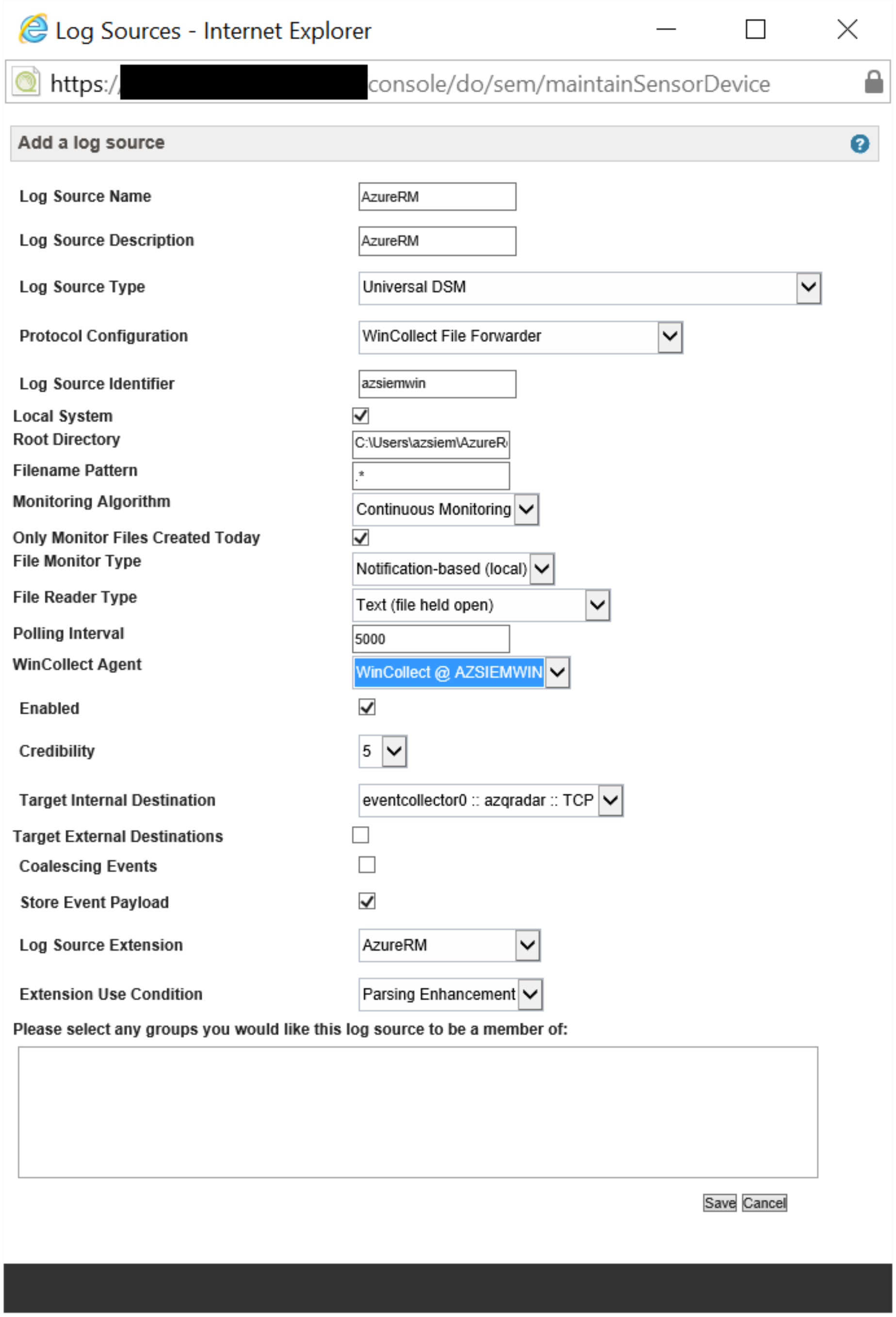
Name	Desc	Status	Protocol	Group	Log Sourc

Displaying 1 to 35 of 35 items (Elapsed time: 0:00:00.154)

Set the following options:

- Log Source Name = “AzureRM” (or choose your own)
- Log Source Description = “AzureRM” (or choose your own)
- Log Source Type = Universal DSM
- Protocol Configuration = WinCollect File Forwarder
- Log Source Identifier – (IP address or host name of machine running AZSIEM)
- Local System – ‘checked’
- Local System Root Directory = C:\Users\azsiem\AzureResourceManagerJsonLD (Note confirm this is the directory on the AZSIEM machine – Search for “AzureResourceManagerJsonLD” under “Users” if you do not find the directory in \users\azsiem)
- Filename Pattern = “.*”
- Monitoring Algorithm = Continuous Monitoring
- Only Monitor Files Created Today – ‘checked’ (or choose your own option)
- File Monitor Type – Notification-based (local)
- File Reader Type – Text (file held open)
- Polling Interval – 5000 (or choose your own value)
- WinCollect Agent – Choose the WinCollect agent on the machine running AZSIEM
- Enabled – ‘checked’
- Credibility – choose your own value
- Target Internal Destination – Choose TCP for your QRadar install (needed to support messages up to 4k)
- Target External Destinations – ‘unchecked’
- Coalescing Events – ‘unchecked’ (or choose your own value)
- Store Event Payload – ‘checked’
- Log Source Extension – AzureRM (or the name you specified for the Log Source Extension)
- Extension Use Condition – Ignored in current versions of QRadar

Select ‘Save’



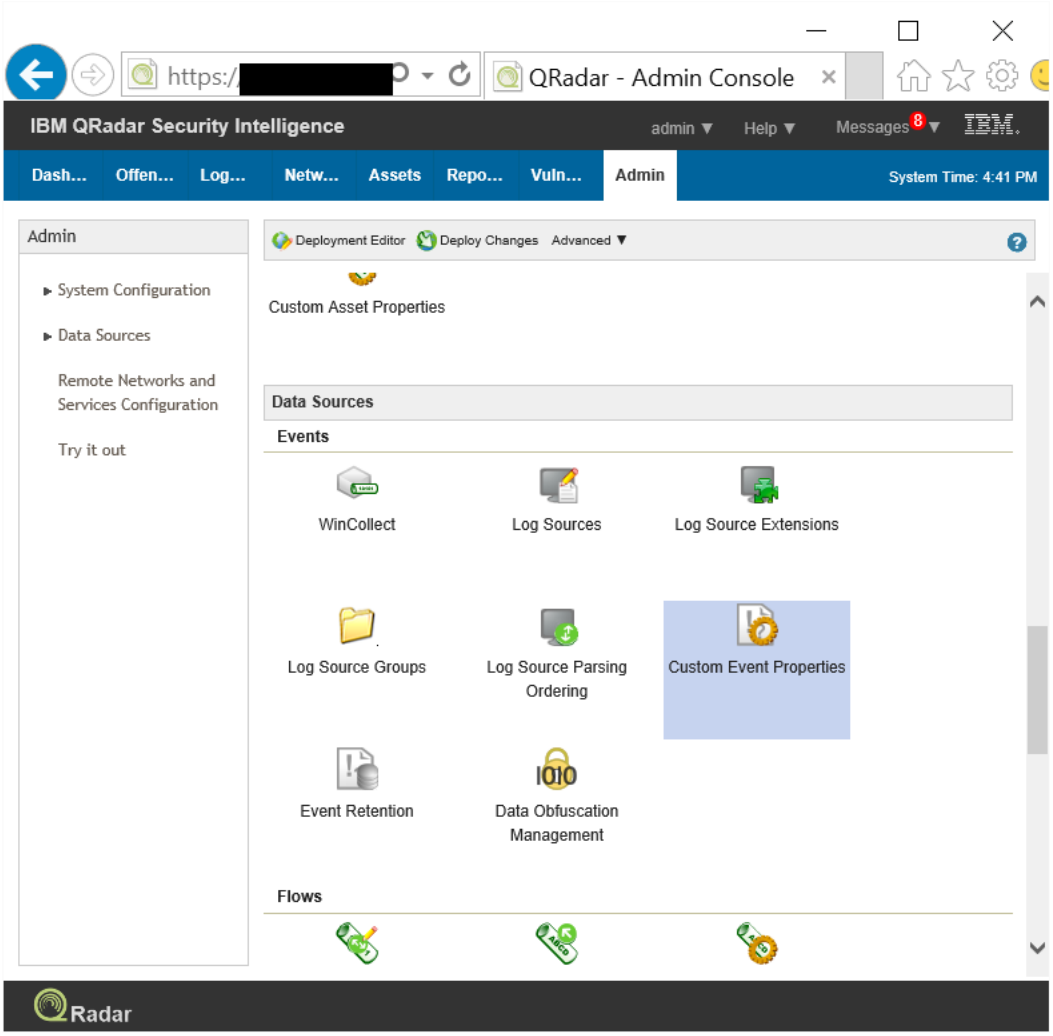
https:/[redacted]console/do/sem/maintainSensorDevice

Add a log source

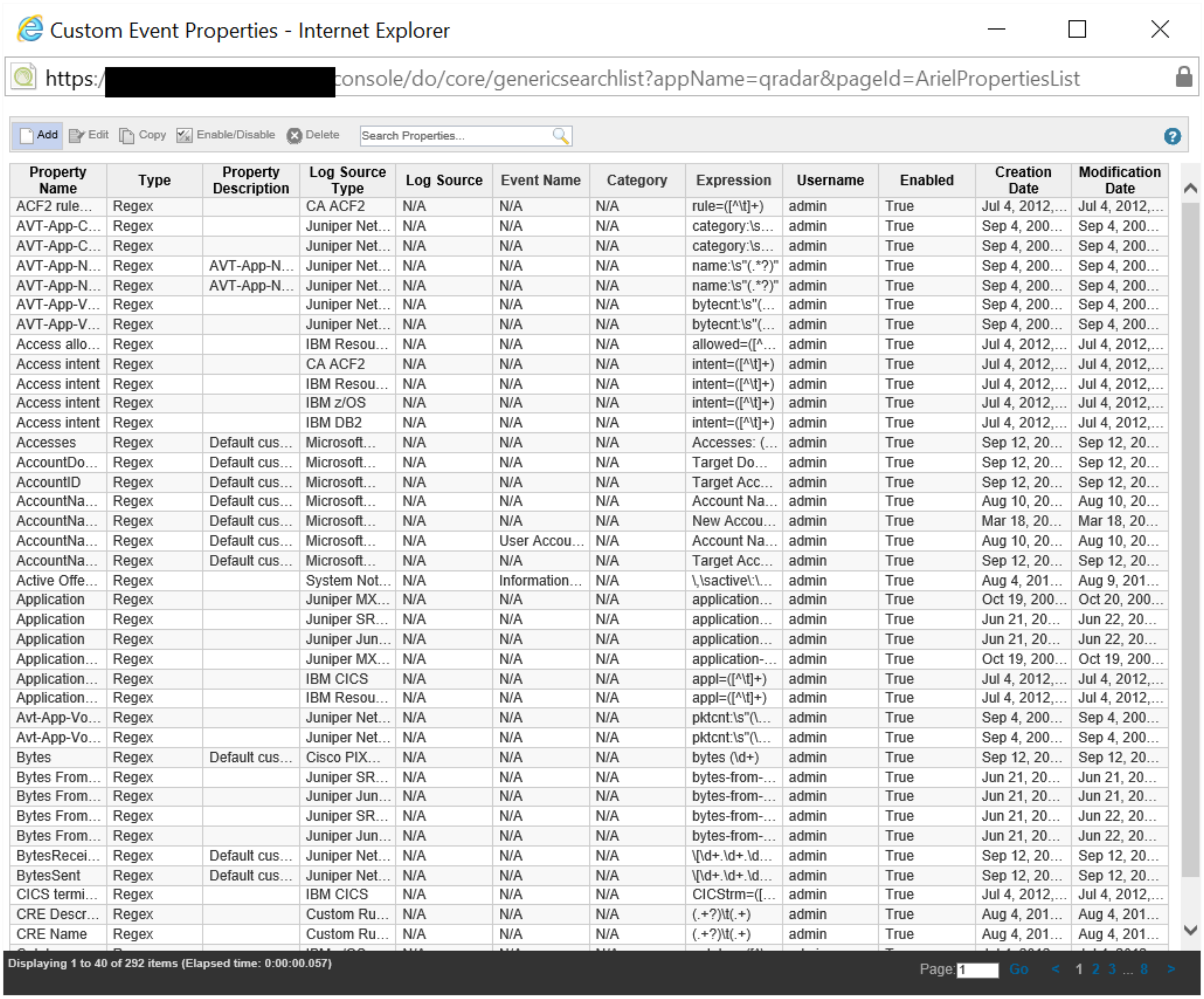
Log Source Name	AzureRM
Log Source Description	AzureRM
Log Source Type	Universal DSM
Protocol Configuration	WinCollect File Forwarder
Log Source Identifier	azsiemwin
Local System	☑
Root Directory	C:\Users\azsiem\AzureR
Filename Pattern	.*
Monitoring Algorithm	Continuous Monitoring
Only Monitor Files Created Today	☑
File Monitor Type	Notification-based (local)
File Reader Type	Text (file held open)
Polling Interval	5000
WinCollect Agent	WinCollect @ AZSIEMWIN
Enabled	☑
Credibility	5
Target Internal Destination	eventcollector0 :: azqradar :: TCP
Target External Destinations	☐
Coalescing Events	☐
Store Event Payload	☑
Log Source Extension	AzureRM
Extension Use Condition	Parsing Enhancement

Please select any groups you would like this log source to be a member of:

Close the list of Log Sources and return to the “Admin” tab. Click “Custom Event Properties”



Now, define a Custom Event Property for each additional property you with to extract from the Azure Resource Manager Operation Log JSON. For example, to define "ResourceGroup" as a Custom Event Property, do the following – Click "Add":



https:/[redacted]console/do/core/genericsearchlist?appName=qradar&pageId=ArielPropertiesList

Property Name	Type	Property Description	Log Source Type	Log Source	Event Name	Category	Expression	Username	Enabled	Creation Date	Modification Date
ACF2 rule...	Regex		CA ACF2	N/A	N/A	N/A	rule=([^\t]+)	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
AVT-App-C...	Regex		Juniper Net...	N/A	N/A	N/A	category:\s...	admin	True	Sep 4, 200...	Sep 4, 200...
AVT-App-C...	Regex		Juniper Net...	N/A	N/A	N/A	category:\s...	admin	True	Sep 4, 200...	Sep 4, 200...
AVT-App-N...	Regex	AVT-App-N...	Juniper Net...	N/A	N/A	N/A	name:\s"(.*?)"	admin	True	Sep 4, 200...	Sep 4, 200...
AVT-App-N...	Regex	AVT-App-N...	Juniper Net...	N/A	N/A	N/A	name:\s"(.*?)"	admin	True	Sep 4, 200...	Sep 4, 200...
AVT-App-V...	Regex		Juniper Net...	N/A	N/A	N/A	bytecnt:\s"(...	admin	True	Sep 4, 200...	Sep 4, 200...
AVT-App-V...	Regex		Juniper Net...	N/A	N/A	N/A	bytecnt:\s"(...	admin	True	Sep 4, 200...	Sep 4, 200...
Access allo...	Regex		IBM Resou...	N/A	N/A	N/A	allowed=([^...	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
Access intent	Regex		CA ACF2	N/A	N/A	N/A	intent=([^\t]+)	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
Access intent	Regex		IBM Resou...	N/A	N/A	N/A	intent=([^\t]+)	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
Access intent	Regex		IBM z/OS	N/A	N/A	N/A	intent=([^\t]+)	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
Access intent	Regex		IBM DB2	N/A	N/A	N/A	intent=([^\t]+)	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
Accesses	Regex	Default cus...	Microsoft...	N/A	N/A	N/A	Accesses: (...	admin	True	Sep 12, 20...	Sep 12, 20...
AccountDo...	Regex	Default cus...	Microsoft...	N/A	N/A	N/A	Target Do...	admin	True	Sep 12, 20...	Sep 12, 20...
AccountID	Regex	Default cus...	Microsoft...	N/A	N/A	N/A	Target Acc...	admin	True	Sep 12, 20...	Sep 12, 20...
AccountNa...	Regex	Default cus...	Microsoft...	N/A	N/A	N/A	Account Na...	admin	True	Aug 10, 20...	Aug 10, 20...
AccountNa...	Regex	Default cus...	Microsoft...	N/A	N/A	N/A	New Accou...	admin	True	Mar 18, 20...	Mar 18, 20...
AccountNa...	Regex	Default cus...	Microsoft...	N/A	User Accou...	N/A	Account Na...	admin	True	Aug 10, 20...	Aug 10, 20...
AccountNa...	Regex	Default cus...	Microsoft...	N/A	N/A	N/A	Target Acc...	admin	True	Sep 12, 20...	Sep 12, 20...
Active Offe...	Regex		System Not...	N/A	Information...	N/A	\,\sactive\:\...	admin	True	Aug 4, 201...	Aug 9, 201...
Application	Regex		Juniper MX...	N/A	N/A	N/A	application...	admin	True	Oct 19, 200...	Oct 20, 200...
Application	Regex		Juniper SR...	N/A	N/A	N/A	application...	admin	True	Jun 21, 20...	Jun 22, 20...
Application	Regex		Juniper Jun...	N/A	N/A	N/A	application...	admin	True	Jun 21, 20...	Jun 22, 20...
Application...	Regex		Juniper MX...	N/A	N/A	N/A	application-...	admin	True	Oct 19, 200...	Oct 19, 200...
Application...	Regex		IBM CICS	N/A	N/A	N/A	appl=([^\t]+)	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
Application...	Regex		IBM Resou...	N/A	N/A	N/A	appl=([^\t]+)	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
Avt-App-Vo...	Regex		Juniper Net...	N/A	N/A	N/A	pktcnt:\s"(\...	admin	True	Sep 4, 200...	Sep 4, 200...
Avt-App-Vo...	Regex		Juniper Net...	N/A	N/A	N/A	pktcnt:\s"(\...	admin	True	Sep 4, 200...	Sep 4, 200...
Bytes	Regex	Default cus...	Cisco PIX...	N/A	N/A	N/A	bytes (\d+)	admin	True	Sep 12, 20...	Sep 12, 20...
Bytes From...	Regex		Juniper SR...	N/A	N/A	N/A	bytes-from-...	admin	True	Jun 21, 20...	Jun 21, 20...
Bytes From...	Regex		Juniper Jun...	N/A	N/A	N/A	bytes-from-...	admin	True	Jun 21, 20...	Jun 21, 20...
Bytes From...	Regex		Juniper SR...	N/A	N/A	N/A	bytes-from-...	admin	True	Jun 21, 20...	Jun 22, 20...
Bytes From...	Regex		Juniper Jun...	N/A	N/A	N/A	bytes-from-...	admin	True	Jun 21, 20...	Jun 22, 20...
BytesRecei...	Regex	Default cus...	Juniper Net...	N/A	N/A	N/A	\[\d+.\d+.\d...	admin	True	Sep 12, 20...	Sep 12, 20...
BytesSent	Regex	Default cus...	Juniper Net...	N/A	N/A	N/A	\[\d+.\d+.\d...	admin	True	Sep 12, 20...	Sep 12, 20...
CICS termi...	Regex		IBM CICS	N/A	N/A	N/A	CICStrm=([...	admin	True	Jul 4, 2012,...	Jul 4, 2012,...
CRE Descr...	Regex		Custom Ru...	N/A	N/A	N/A	(.+?)\t(.+)	admin	True	Aug 4, 201...	Aug 4, 201...
CRE Name	Regex		Custom Ru...	N/A	N/A	N/A	(.+?)\t(.+)	admin	True	Aug 4, 201...	Aug 4, 201...

Displaying 1 to 40 of 292 items (Elapsed time: 0:00:00.057)

Copy the following example Azure Resource Manager JSON event to the “Test Field” (This will help confirm you have entered the regular expressions correctly)

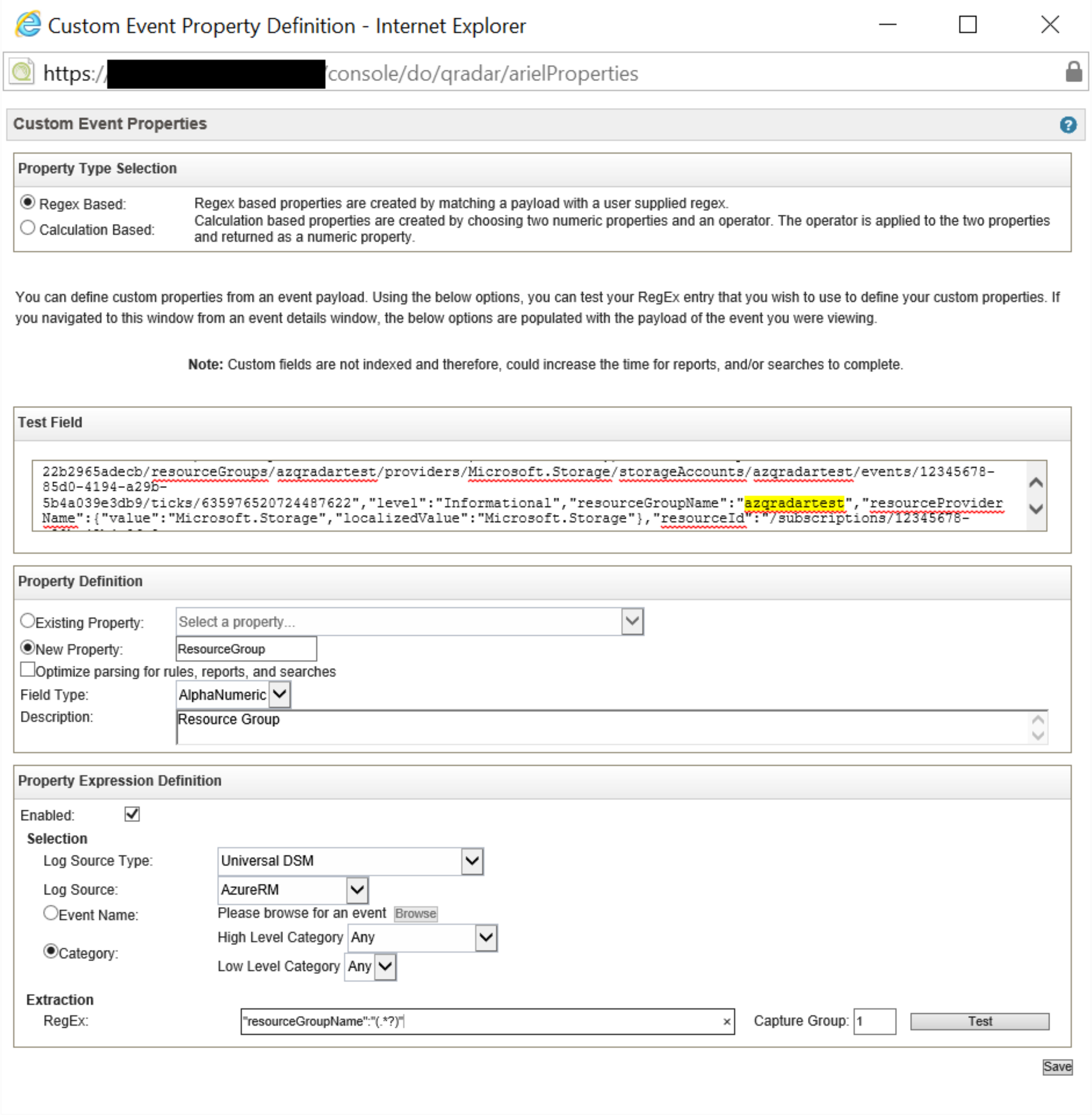
```
{"authorization":{"action":"Microsoft.Storage/storageAccounts/regenerateKey/action","scope":"/su
bscriptions/1234567-a20b-42b4-96c8-
22b2965adecb/resourceGroups/azqradartest/providers/Microsoft.Storage/storageAccounts/azqradartes
t"},"caller":"lauren@example.com","channels":"Operation","claims":{"aud":"https://management.cor
e.windows.net/","iss":"https://sts.windows.net/72f988bf-86f1-41af-91ab-
2d7cd011db47/","iat":"1462052874","nbf":"1462052874","exp":"1462056774","_claim_names":"{\"group
s\":\"src1\"}","_claim_sources":"{\"src1\":{\"endpoint\":\"https://graph.windows.net/72f988bf-
86f1-41af-91ab-2d7cd011db47/users/12345678-d3c4-43a1-b237-
b67f5a2f22a9/getMemberObjects\"}}","http://schemas.microsoft.com/claims/authnclassreference":"1"
,"http://schemas.microsoft.com/claims/authnmethodsreferences":"pwd,mfa","appid":"12345678-3bb0-
49c1-b47d-
974e53cbdf3c","appidacr":"2","http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname":"Ca
lia","http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname":"Lauren","in_corp":"true"
,"ipaddr":"131.101.114.230","name":"Lauren
Calia","http://schemas.microsoft.com/identity/claims/objectidentifier":"12345678-d3c4-43a1-b237-
b67f5a2f22a9","onprem_sid":"S-1-5-21-1234567890-1234567890-1234567890-
12345","puid":"1234567812345678","http://schemas.microsoft.com/identity/claims/scope":"user_impe
rsonation","http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier":"HJABCdefid7U8
-o-abcdefabcdefpm08vBvz8","http://schemas.microsoft.com/identity/claims/tenantid":"72f988bf-
86f1-41af-91ab-
2d7cd011db47","http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name":"lauren@example.com",
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn":"lauren@example.com","ver":"1.0"},"c
orrelationId":"12345678-523f-4da5-9fef-40fa0ff37c55","description":"","eventDataId":"12345678-
85d0-4194-a29b-5b4a039e3db9","eventName":{"value":"BeginRequest","localizedValue":"Begin
request"},"category":{"value":"Administrative","localizedValue":"Administrative"},"httpRequest":
{"clientRequestId":"12345678-1769-480b-87c8-
0c410a83804d","clientIpAddress":"167.219.3.17","method":"POST"},"id":"/subscriptions/12345678-
a20b-42b4-96c8-
22b2965adecb/resourceGroups/azqradartest/providers/Microsoft.Storage/storageAccounts/azqradartes
t/events/12345678-85d0-4194-a29b-
5b4a039e3db9/ticks/635976520724487622","level":"Informational","resourceGroupName":"azqradartest
","resourceProviderName":{"value":"Microsoft.Storage","localizedValue":"Microsoft.Storage"},"res
ourceId":"/subscriptions/12345678-a20b-42b4-96c8-
22b2965adecb/resourceGroups/azqradartest/providers/Microsoft.Storage/storageAccounts/azqradartes
t","resourceType":{"value":"Microsoft.Storage/storageAccounts","localizedValue":"Microsoft.Stora
ge/storageAccounts"},"operationId":"12345678-523f-4da5-9fef-
40fa0ff37c55","operationName":{"value":"Microsoft.Storage/storageAccounts/regenerateKey/action",
"localizedValue":"Microsoft.Storage/storageAccounts/regenerateKey/action"},"status":{"value":"St
arted","localizedValue":"Started"},"subStatus":{"value":"","localizedValue":""},"eventTimestamp"
:"2016-04-30T22:27:52.4487622Z","submissionTimestamp":"2016-04-
30T22:28:12.9973642Z","subscriptionId":"12345678-a20b-42b4-96c8-
22b2965adecb","tenantId":"72f988bf-86f1-41af-91ab-2d7cd011db47"}
```

Choose the following options:

- Property Type Selection - Regex Based
- New Property – “ResourceGroup”
- Optimize parsing rules, reports, and searches – ‘unchecked’ (or choose your own value)
- Field Type – AlphaNumeric
- Field Description – “Resource Group”
- Enabled – ‘checked’
- Log Source Type – Universal DSM

- Log Source – “AzureRM”
- Choose “Category” and HighLevelCategory – Any, Low Level Category - Any
- Extraction RegEx (note – Include the quotes when copying the field and make sure they are not the sloped “smart quotes”) – "resourceGroupName":"(.*?)"
- Capture Group 1

Confirm that the Resource Group name is highlighted in Yellow and hit Save. Hit ‘Test’ if necessary to confirm that the RegEx found a hit.



Custom Event Property Definition - Internet Explorer

https:/[redacted]console/do/qradar/arielProperties

Custom Event Properties

Property Type Selection

● Regex Based: Regex based properties are created by matching a payload with a user supplied regex.

○ Calculation Based: Calculation based properties are created by choosing two numeric properties and an operator. The operator is applied to the two properties and returned as a numeric property.

You can define custom properties from an event payload. Using the below options, you can test your RegEx entry that you wish to use to define your custom properties. If you navigated to this window from an event details window, the below options are populated with the payload of the event you were viewing.

Note: Custom fields are not indexed and therefore, could increase the time for reports, and/or searches to complete.

Test Field

```
22b2965adecb/resourceGroups/azqradartest/providers/Microsoft.Storage/storageAccounts/azqradartest/events/12345678-
85d0-4194-a29b-
5b4a039e3db9/ticks/635976520724487622","level":"Informational","resourceGroupName":"azqradartest","resourceProvider
Name":{"value":"Microsoft.Storage","localizedValue":"Microsoft.Storage"},"resourceId":"/subscriptions/12345678-
```

Property Definition

○ Existing Property: Select a property...

● New Property: ResourceGroup

□ Optimize parsing for rules, reports, and searches

Field Type: AlphaNumeric

Description: Resource Group

Property Expression Definition

Enabled: ☑

Selection

Log Source Type: Universal DSM

Log Source: AzureRM

○ Event Name: Please browse for an event Browse

● Category: High Level Category Any

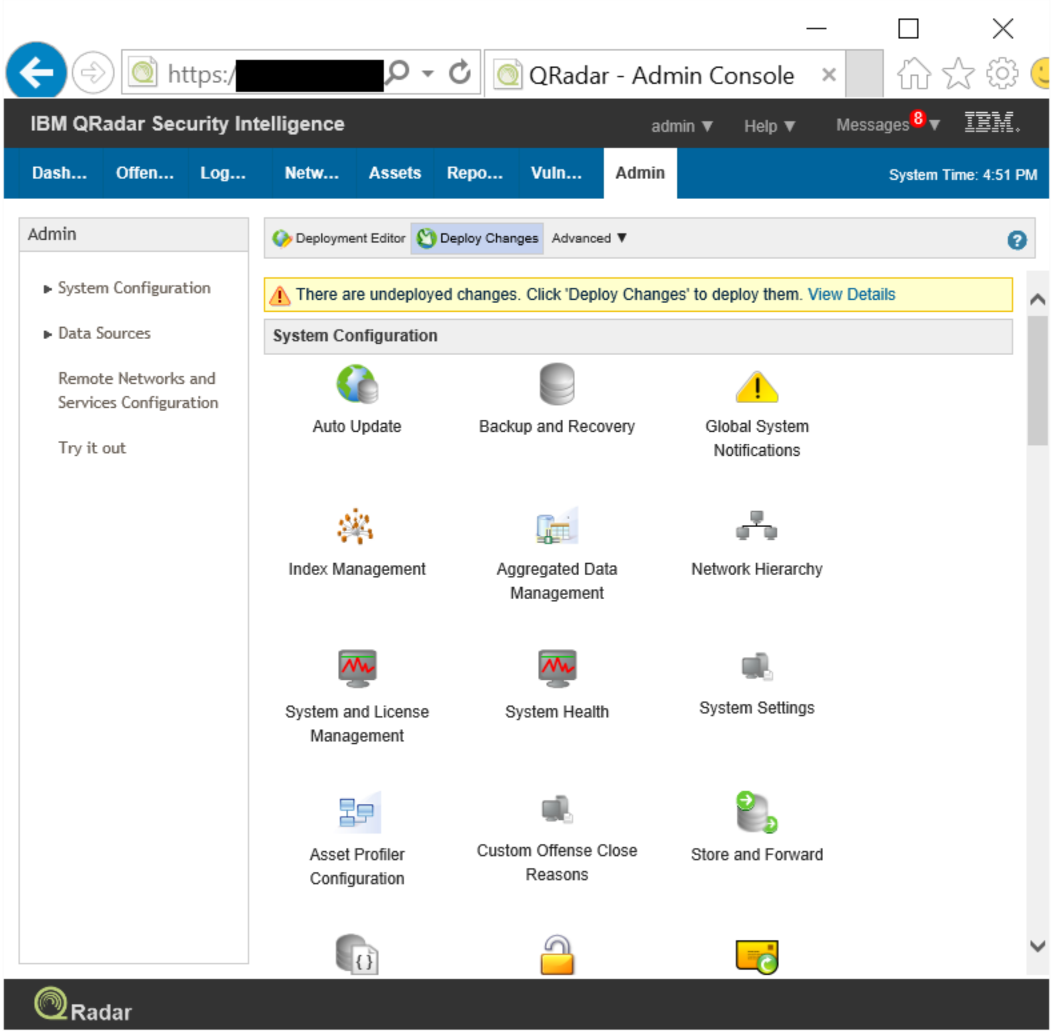
Low Level Category Any

Extraction

RegEx: "resourceGroupName":"(.*?)"

Capture Group: 1

Close the list of Custom Event Properties and return to the “Admin” tab. Click “Deploy Changes”



There are undeployed changes. Click 'Deploy Changes' to deploy them. View Details

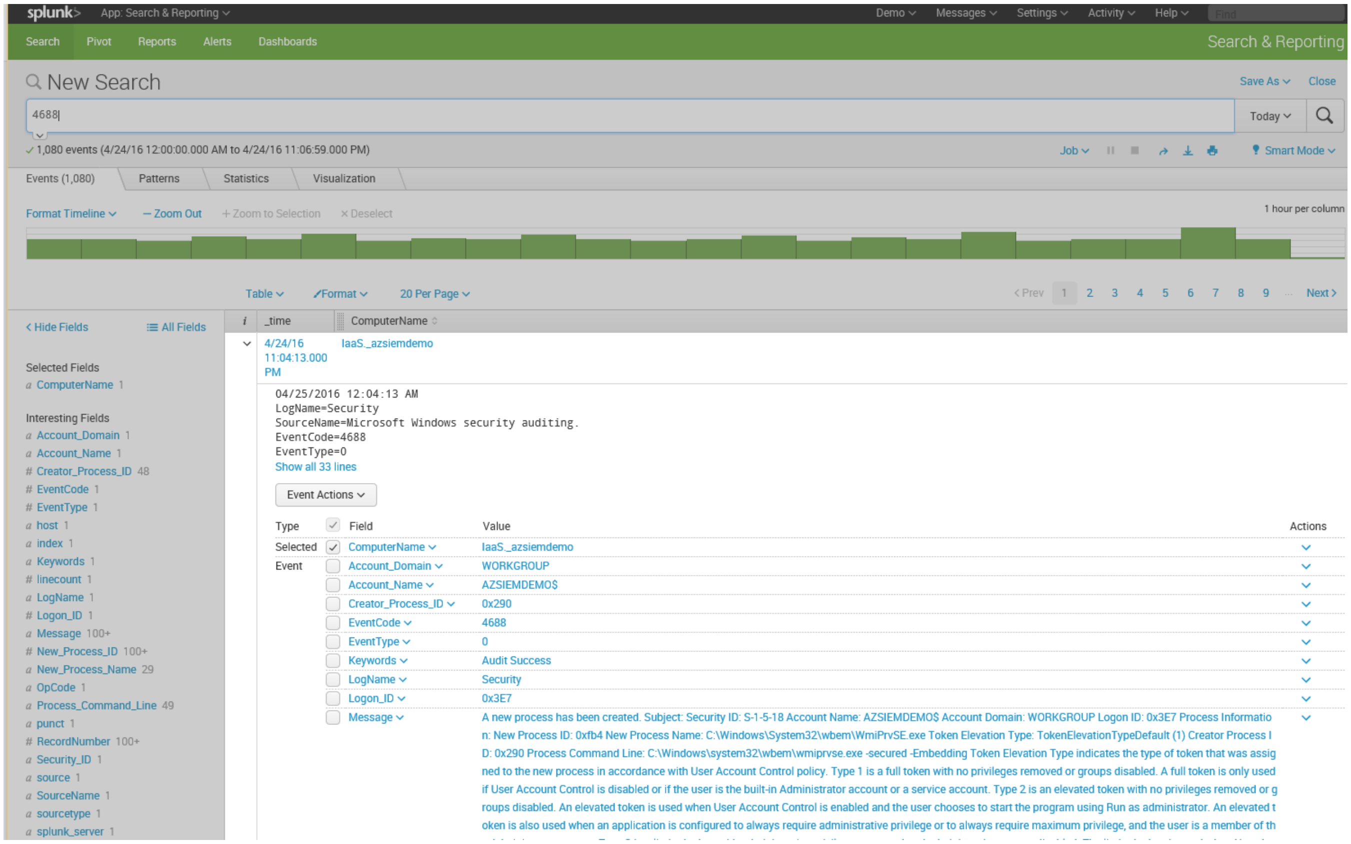
Events should now be searchable in “Log Activity” tab. Event names may show up as “Unknown” because QRadar doesn’t have a mapping for the Azure Resource Manager “Operation Name” values. Additional Custom Event Properties can be added to retrieve useful information about the Azure Resource Manager Operation events. For example, here are RegEx expressions for two important values that can be added as Custom Event Properties following the steps above:

```
Subscription Id - "subscriptionId":"(.*?)"

Operation Name - "operationName".*?"value":"(.*?)"
```

The RegEx should be copied along with the quotes, taking care to make sure they are not sloped “smart quotes”.

WINDOWS EVENTS IN SPLUNK



```
4688|
```

✓ 1,080 events (4/24/16 12:00:00.000 AM to 4/24/16 11:06:59.000 PM)

Selected Fields
a ComputerName 1

Interesting Fields
a Account_Domain 1
a Account_Name 1
Creator_Process_ID 48
EventCode 1
EventType 1
a host 1
a index 1
a Keywords 1
# linecount 1
a LogName 1
Logon_ID 1
a Message 100+
New_Process_ID 100+
a New_Process_Name 29
a OpCode 1
a Process_Command_Line 49
a punct 1
RecordNumber 100+
a Security_ID 1
a source 1
a SourceName 1
a sourcetype 1
a splunk_server 1

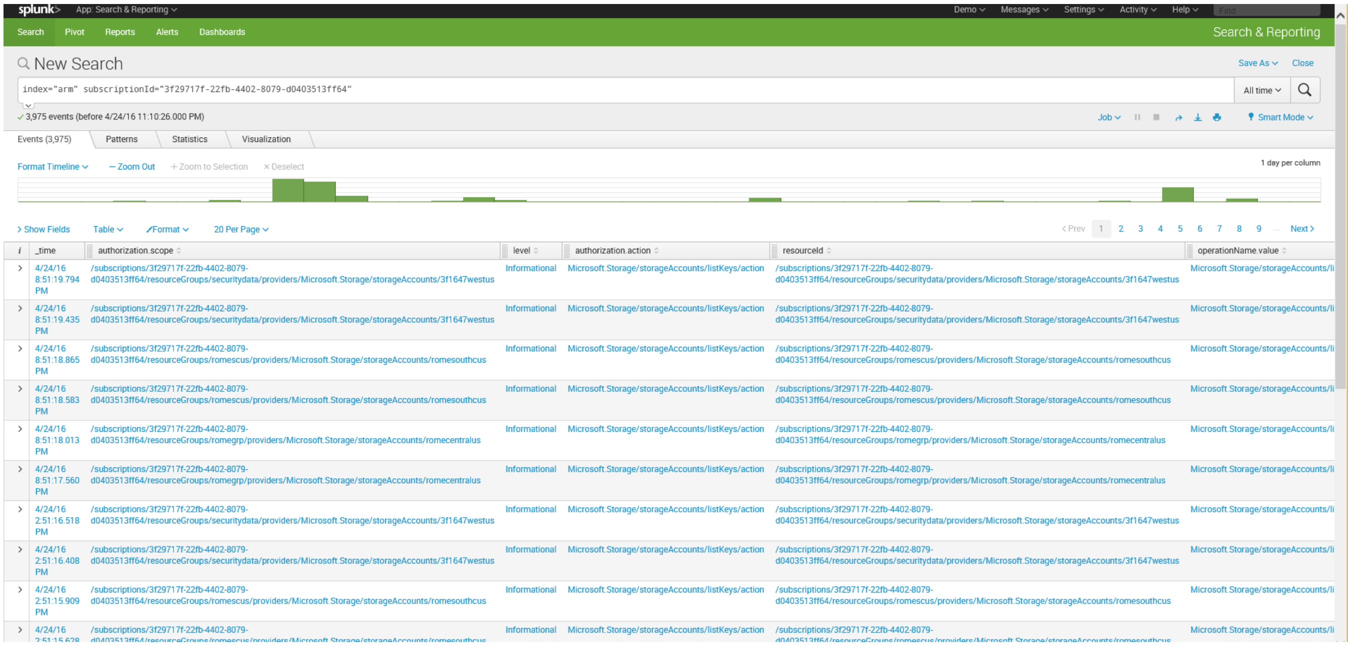
_time	ComputerName
4/24/16 11:04:13.000 PM	IaaS._azsiemdemo

```
04/25/2016 12:04:13 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4688
EventType=0
```

Show all 33 lines

Type	☑	Field	Value	Actions
Selected	☑	ComputerName	IaaS._azsiemdemo	
Event	□	Account_Domain	WORKGROUP	
	□	Account_Name	AZSIEMDEMO$	
	□	Creator_Process_ID	0x290	
	□	EventCode	4688	
	□	EventType	0	
	□	Keywords	Audit Success	
	□	LogName	Security	
	□	Logon_ID	0x3E7	
	□	Message	A new process has been created. Subject: Security ID: S-1-5-18 Account Name: AZSIEMDEMO$ Account Domain: WORKGROUP Logon ID: 0x3E7 Process Information: New Process ID: 0xfb4 New Process Name: C:\Windows\System32\wbem\WmiPrvSE.exe Token Elevation Type: TokenElevationTypeDefault (1) Creator Process ID: 0x290 Process Command Line: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of th	

AZURE AUDIT LOG IN SPLUNK

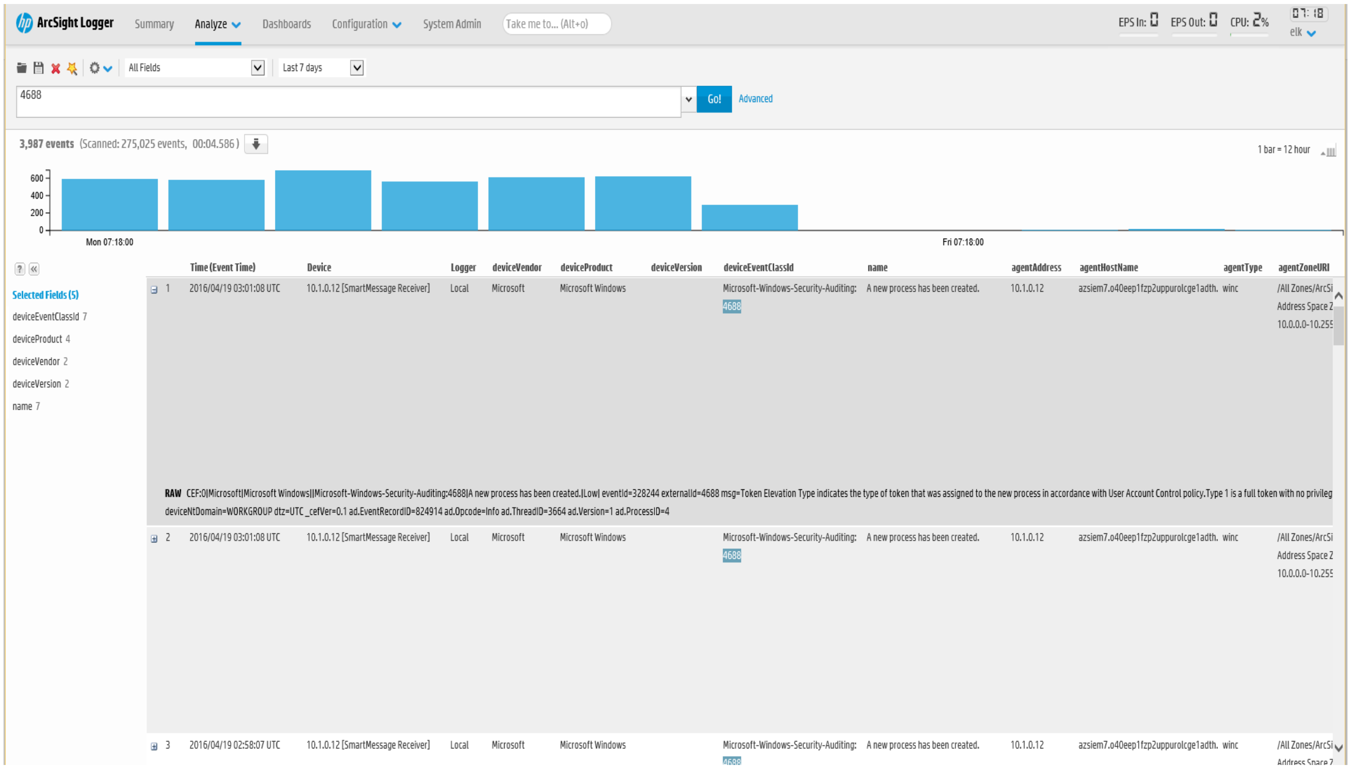


```
index="arm" subscriptionId="3f29717f-22fb-4402-8079-d0403513ff64"
```

✓ 3,975 events (before 4/24/16 11:10:26.000 PM)

i	_time	authorization.scope	level	authorization.action	resourceId	operationName.value
>	4/24/16 8:51:19.794 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Microsoft.Storage/storageAccounts/li
>	4/24/16 8:51:19.435 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Microsoft.Storage/storageAccounts/li
>	4/24/16 8:51:18.865 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Microsoft.Storage/storageAccounts/li
>	4/24/16 8:51:18.583 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Microsoft.Storage/storageAccounts/li
>	4/24/16 8:51:18.013 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romegrp/providers/Microsoft.Storage/storageAccounts/romecentralus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romegrp/providers/Microsoft.Storage/storageAccounts/romecentralus	Microsoft.Storage/storageAccounts/li
>	4/24/16 8:51:17.560 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romegrp/providers/Microsoft.Storage/storageAccounts/romecentralus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romegrp/providers/Microsoft.Storage/storageAccounts/romecentralus	Microsoft.Storage/storageAccounts/li
>	4/24/16 2:51:16.518 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Microsoft.Storage/storageAccounts/li
>	4/24/16 2:51:16.408 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/securitydata/providers/Microsoft.Storage/storageAccounts/3f1647westus	Microsoft.Storage/storageAccounts/li
>	4/24/16 2:51:15.909 PM	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Microsoft.Storage/storageAccounts/li
>	4/24/16 2:51:15.628	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Informational	Microsoft.Storage/storageAccounts/listKeys/action	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourceGroups/romescus/providers/Microsoft.Storage/storageAccounts/romesouthcus	Microsoft.Storage/storageAccounts/li

WINDOWS EVENTS IN ARCSIGHT



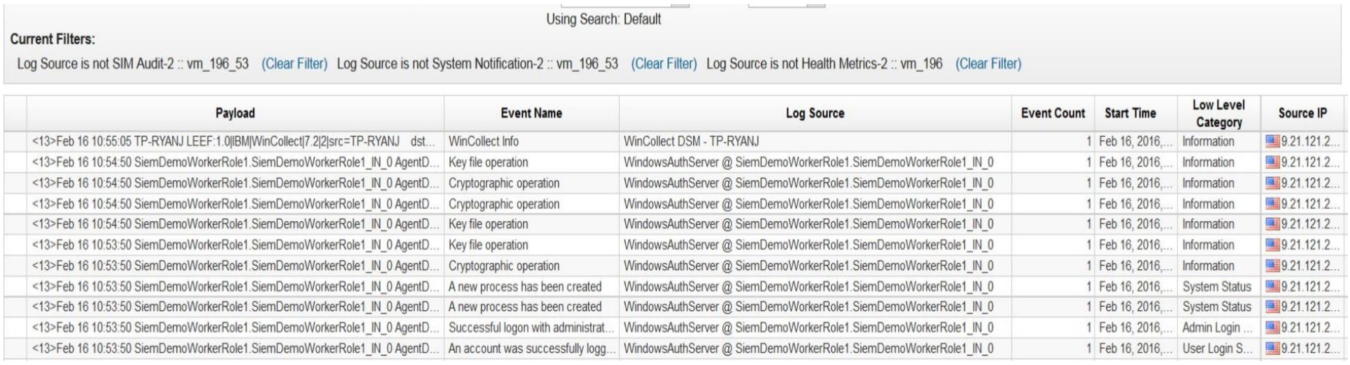
Search: 4688

3,987 events (Scanned: 275,025 events, 00:04.586)

	Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassId	name	agentAddress	agentHostName	agentType	agentZoneURI
1	2016/04/19 03:01:08 UTC	10.1.0.12 [SmartMessage Receiver]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security-Auditing: 4688	A new process has been created.	10.1.0.12	azsiem7.o40eep1fzp2uppurolcge1adth.	winc	/All Zones/ArcSi Address Space Z 10.0.0.0-10.255
2	2016/04/19 03:01:08 UTC	10.1.0.12 [SmartMessage Receiver]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security-Auditing: 4688	A new process has been created.	10.1.0.12	azsiem7.o40eep1fzp2uppurolcge1adth.	winc	/All Zones/ArcSi Address Space Z 10.0.0.0-10.255
3	2016/04/19 02:58:07 UTC	10.1.0.12 [SmartMessage Receiver]	Local	Microsoft	Microsoft Windows		Microsoft-Windows-Security-Auditing: 4688	A new process has been created.	10.1.0.12	azsiem7.o40eep1fzp2uppurolcge1adth.	winc	/All Zones/ArcSi Address Space Z

```
RAW  CEF:0|Microsoft|Microsoft Windows||Microsoft-Windows-Security-Auditing:4688|A new process has been created.|Low| eventId=328244 externalId=4688 msg=Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.Type 1 is a full token with no privileg
deviceNtDomain=WORKGROUP dtz=UTC _cefVer=0.1 ad.EventRecordID=824914 ad.Opcode=Info ad.ThreadID=3664 ad.Version=1 ad.ProcessID=4
```

WINDOWS EVENTS IN QRADAR

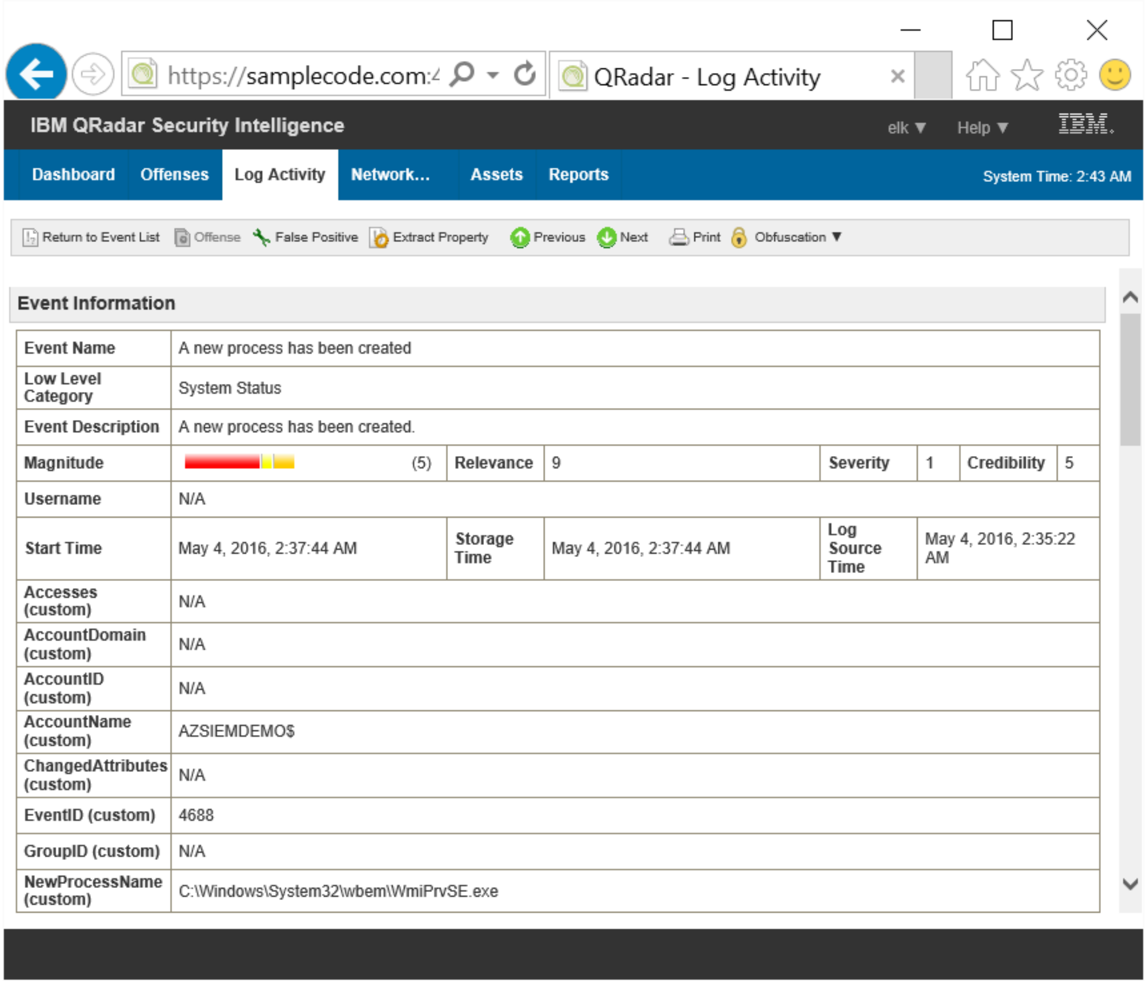


Using Search: Default

Current Filters:

Log Source is not SIM Audit-2 :: vm_196_53 (Clear Filter) Log Source is not System Notification-2 :: vm_196_53 (Clear Filter) Log Source is not Health Metrics-2 :: vm_196 (Clear Filter)

	Payload	Event Name	Log Source	Event Count	Start Time	Low Level Category	Source IP
	<13>Feb 16 10:55:05 TP-RYANJ LEEF:1.0|IBM|WinCollect|7.2|2|src=TP-RYANJ dst...	WinCollect Info	WinCollect DSM - TP-RYANJ	1	Feb 16, 2016,...	Information	9.21.121.2...
	<13>Feb 16 10:54:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	Key file operation	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	Information	9.21.121.2...
	<13>Feb 16 10:54:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	Cryptographic operation	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	Information	9.21.121.2...
	<13>Feb 16 10:54:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	Cryptographic operation	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	Information	9.21.121.2...
	<13>Feb 16 10:54:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	Key file operation	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	Information	9.21.121.2...
	<13>Feb 16 10:53:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	Key file operation	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	Information	9.21.121.2...
	<13>Feb 16 10:53:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	Cryptographic operation	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	Information	9.21.121.2...
	<13>Feb 16 10:53:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	A new process has been created	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	System Status	9.21.121.2...
	<13>Feb 16 10:53:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	A new process has been created	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	System Status	9.21.121.2...
	<13>Feb 16 10:53:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	Successful logon with administrat...	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	Admin Login ...	9.21.121.2...
	<13>Feb 16 10:53:50 SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0 AgentD...	An account was successfully logg...	WindowsAuthServer @ SiemDemoWorkerRole1.SiemDemoWorkerRole1_IN_0	1	Feb 16, 2016,...	User Login S...	9.21.121.2...



Event Information

Event Name	A new process has been created						
Low Level Category	System Status						
Event Description	A new process has been created.						
Magnitude	(5)	Relevance	9	Severity	1	Credibility	5
Username	N/A						
Start Time	May 4, 2016, 2:37:44 AM	Storage Time	May 4, 2016, 2:37:44 AM	Log Source Time	May 4, 2016, 2:35:22 AM		
Accesses (custom)	N/A						
AccountDomain (custom)	N/A						
AccountID (custom)	N/A						
AccountName (custom)	AZSIEMDEMO$						
ChangedAttributes (custom)	N/A						
EventID (custom)	4688						
GroupID (custom)	N/A						
NewProcessName (custom)	C:\Windows\System32\wbem\WmiPrvSE.exe						