### Overview

The AZSIEM service allows Azure customers to integrate logs from assets deployed in Azure to their on-premises or Azure hosted ArcSight environment.

### The parsers in this document read additional Azure subscription information from events collected using the Microsoft AZSIEM service.

### Prerequisites

* Setup and configure the Microsoft Azure AZSIEM Server and Service -

[Microsoft Azure AZSIEM Setup](https://azsiempublicdrops.blob.core.windows.net/drops/Azure%20SIEM%20Integrator%20User%20Guide.pdf)

* Install and configure an ArcSight Windows Event Log – Native Connector (MicrosoftWindowsEventLog\_NativeConfig.pdf)
* Configure the ArcSight WiNC Connector to collect from the newly setup AZSIEM Azure Server as described in the ArcSight Windows Event Log – Native Connector guide. Configure the connector to collect from the server’s Forwarded Events container.
* Download the ArcSight WiNC Connector Parsers for Microsoft Azure AZSIEM Service



### Setup of ArcSight WiNC Connector with Azure ArcSight AZSIEM Parsers

* Extract the parser in the root of the ArcSight Windows Event Log – Native Connector folder
  + This will extract the parsers files into :

%CONNECTOR\_HOME%\user\agent\fcp\winc folder

* Restart the ArcSight WiNC Connector

### Data Mapping

The AZSIEM service writes the additional Azure subscription information into the UserData section of events fed into the Forwarded Events logs. These parsers extract that information and writes the additional data into the flexString1 and flexString2 ArcSight fields.

|  |  |
| --- | --- |
| ArcSight Field Name | Azure Field |
| flexString1 | **Azure Subscription Id** |
| flexString2 | **RoleName**.**RoleInstanceId**.**SourceStorageAccount**.**SourceFriendlyName**  Additional Azure subscription information is stored in the oldFileName field in ArcSight delimited by “.” |

### Parser Files

The table below lists out all of the parser files included in the zip. All the parser files are the same, they simply parser different Microsoft Event Types. The easiest way to make updates to these parser files is to open all of the files up at the same time in a notepad program like notepad++ do a search and replace on all open documents.

\---agent

\---fcp

\---winc

+---application

| exchange\_auditing.msexchangeis\_auditing.userdata.jsonparser.properties

| fsccontroller.userdata.jsonparser.properties

| fsceventing.userdata.jsonparser.properties

| fscmanualscanner.userdata.jsonparser.properties

| fscmonitor.userdata.jsonparser.properties

| fscrealtimescanner.userdata.jsonparser.properties

| fscscheduledscanner.userdata.jsonparser.properties

| fsctransportscanner.userdata.jsonparser.properties

| fscvsswriter.userdata.jsonparser.properties

| fseimc.userdata.jsonparser.properties

| fsemailpickup.userdata.jsonparser.properties

| fseondemandnav.userdata.jsonparser.properties

| fsevsapi.userdata.jsonparser.properties

| getenginefiles.userdata.jsonparser.properties

| microsoft\_forefront\_protection.userdata.jsonparser.properties

| msexchangeis\_auditing.userdata.jsonparser.properties

| mssqlserver.audit.userdata.jsonparser.properties

| mssqlserver.userdata.jsonparser.properties

| oracle\_orcl.userdata.jsonparser.properties

|

+---directory\_service

| ntds\_database.userdata.jsonparser.properties

| ntds\_general.userdata.jsonparser.properties

| ntds\_isam.userdata.jsonparser.properties

| ntds\_kcc.userdata.jsonparser.properties

| ntds\_ldap.userdata.jsonparser.properties

| ntds\_replication.userdata.jsonparser.properties

|

+---security

| microsoft\_windows\_eventlog.userdata.jsonparser.properties

| microsoft\_windows\_eventlog.userdata.userdata.jsonparser.properties

| microsoft\_windows\_security\_auditing.userdata.jsonparser.properties

| security.userdata.jsonparser.properties

| vssaudit.userdata.jsonparser.properties

|

\---system

microsoft\_antimalware.userdata.jsonparser.properties

microsoft\_windows\_eventlog.userdata.jsonparser.properties

microsoft\_windows\_security\_auditing.userdata.jsonparser.properties

nps.userdata.jsonparser.properties

remoteaccess.userdata.jsonparser.properties

schannel.userdata.jsonparser.properties

security.userdata.jsonparser.properties

service\_control\_manager.userdata.jsonparser.properties

wins.userdata.jsonparser.properties