Splunk® Add-on for Microsoft Active Directory Install and use the Splunk Add-on for Microsoft Active Directory 1.0.1

Generated: 7/31/2019 11:34 am
# Table of Contents

Overview......................................................................................................................................................1  
   About the Splunk Add-on for Microsoft Active Directory..............................................1  
   Source types for the Splunk Add-on for Microsoft Active Directory..............1  
   Release notes for Splunk Add-on for Microsoft Active Directory.............2

Installation.....................................................................................................................................................3  
   Hardware and software requirements for the Splunk Add-on for  
   Microsoft Active Directory.................................................................................................3  
   Install the Splunk Add-on for Microsoft Active Directory..........................3

Configuration.................................................................................................................................................7  
   Configure the Splunk Add-on for Microsoft Active Directory............................7  
   Troubleshoot the Splunk Add-ons for Microsoft Active Directory..............7

Lookups..........................................................................................................................................................9  
   Lookups for the Splunk Add-on for Microsoft Active Directory....................9
Overview

About the Splunk Add-on for Microsoft Active Directory

<table>
<thead>
<tr>
<th>Version</th>
<th>1.0.1 (TA-Microsoft-AD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Products</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td>Visible</td>
<td>No. This add-on does not contain any views.</td>
</tr>
</tbody>
</table>

The Splunk Add-on for Microsoft Active Directory (AD) lets you collect Active Directory and Domain Name Server debug logs from Windows hosts that act as domain controllers for a supported version of Windows Server.

The Splunk Add-on for Microsoft Active Directory requires that you configure Active Directory audit policy. This is because AD does not log certain events by default. After the Splunk platform indexes the events, you can analyze the data.

This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk apps, such as the Splunk Apps for Microsoft Exchange and Windows Infrastructure.


Discuss the Splunk Add-on for Microsoft Active Directory on Splunk Answers at http://answers.splunk.com/answers/app/3207.

Source types for the Splunk Add-on for Microsoft Active Directory

The Splunk Add-on for Microsoft Active Directory provides the following source types:

<table>
<thead>
<tr>
<th>Source type</th>
<th>Description</th>
<th>CIM data models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Add-on for Microsoft Active Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source type</td>
<td>Description</td>
<td>CIM data models</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>MSAD:NT6:Health</td>
<td>Active Directory health information</td>
<td></td>
</tr>
<tr>
<td>MSAD:NT6:SiteInfo</td>
<td>Active Directory site information</td>
<td></td>
</tr>
<tr>
<td>MSAD:NT6:Replication</td>
<td>Active Directory site replication information</td>
<td></td>
</tr>
<tr>
<td>MSAD:NT6:Netlogon</td>
<td>Active Directory login statistics</td>
<td></td>
</tr>
<tr>
<td>MSAD:SubnetAffinity</td>
<td>Active Directory Domain Subnet Affinity problem information</td>
<td></td>
</tr>
</tbody>
</table>

**Release notes for Splunk Add-on for Microsoft Active Directory**

The latest version of the Splunk Add-on for Microsoft Active Directory was released on **December 21, 2017**.

**What's new**

See the known issues and fixed issues of these release notes for product updates.

**Known issues**

This version of the Splunk Add-on for Microsoft Active Directory has the following reported known issues and workarounds. If no issues appear below, no issues have yet been reported.

**Fixed Issues**

<table>
<thead>
<tr>
<th>Publication Date</th>
<th>Defect Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-07-17</td>
<td>TAG-12447</td>
<td>Fixed issue causing NT6 powershell scripts not running as expected.</td>
</tr>
<tr>
<td>2017-02-17</td>
<td>TAG-11961</td>
<td>Update to latest common build.</td>
</tr>
</tbody>
</table>
Installation

Hardware and software requirements for the Splunk Add-on for Microsoft Active Directory

Splunk admin requirements

To install and configure the Splunk Add-on for Microsoft Active Directory, you must be a member of the admin or sc_admin roles.

Microsoft Active Directory setup requirements

To use the Splunk Add-on for Microsoft Active Directory, you must configure Active Directory audit policy. See Configure Active Directory audit policy for instructions.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run the add-ons.

- For Splunk Enterprise system requirements, see System Requirements in the Splunk Enterprise Installation Manual.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise Installation Manual, which includes information about forwarders.

Install the Splunk Add-on for Microsoft Active Directory

1. Get the Splunk Add-on for Microsoft Active Directory by downloading it from https://splunkbase.splunk.com/app/3207 or browsing to it using the app browser within Splunk Web.
2. Determine where and how to install this add-on in your deployment, using the tables on this page.
3. Perform any prerequisite steps before installing, if required and specified in the tables below.
4. Complete your installation.
These add-ons have been specifically created for use with the Splunk Apps for Microsoft Exchange and Windows Infrastructure. There are specific installation instructions for these add-ons for use with those apps:

**Splunk App for Microsoft Exchange**

- Download and configure the Splunk Add-on for Microsoft Active Directory

**Splunk App for Windows Infrastructure**

- Download and configure the Splunk Add-on for Microsoft Active Directory

You can also use the add-on to collect Active Directory data outside of these apps. For best results, however, you must configure your Windows Active Directory and DNS environments for increased logging.

**Distributed deployments**

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you use forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

**Where to install this add-on**

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in *Splunk Add-ons* for more information.

These tables provides a reference for installing this specific add-on to a distributed deployment of Splunk Enterprise.

**Splunk Add-on for Microsoft Active Directory**

<table>
<thead>
<tr>
<th>Splunk platform instance type</th>
<th>Supported</th>
<th>Required</th>
<th>Actions required / Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Heads</td>
<td>Yes</td>
<td>Yes</td>
<td>Install this add-on to one or more search heads that are also domain controllers and where Active Directory</td>
</tr>
<tr>
<td>Splunk platform instance type</td>
<td>Supported</td>
<td>Required</td>
<td>Actions required / Comments</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Indexers</td>
<td>Yes</td>
<td>No</td>
<td>Install this add-on to indexers only if they are also domain controllers and Active Directory knowledge is required. If you use a universal or light forwarder for data collection, install the add-on to your indexers.</td>
</tr>
<tr>
<td>Heavy Forwarders</td>
<td>Yes</td>
<td></td>
<td>All forwarder types are supported. The forwarder needs to be installed directly on the domain controller for Active Directory monitoring.</td>
</tr>
<tr>
<td>Universal Forwarders</td>
<td>Yes</td>
<td>See comments</td>
<td>All forwarder types are supported. The forwarder needs to be installed directly on the domain controller for Active Directory monitoring.</td>
</tr>
<tr>
<td>Light Forwarders</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Distributed deployment feature compatibility**

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

<table>
<thead>
<tr>
<th>Distributed deployment feature</th>
<th>Supported</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Head Clusters</td>
<td>Yes</td>
<td>You can install this add-on on a search head cluster for all search-time functionality, but configure inputs on forwarders to avoid duplicate data collection. Before you install this add-on to a cluster, remove the <code>eventgen.conf</code> file and all files in the <code>samples</code> folder.</td>
</tr>
<tr>
<td>Indexer Clusters</td>
<td>Yes</td>
<td>Before you install this add-on to a cluster, remove the <code>eventgen.conf</code> file and all files in the <code>samples</code> folder.</td>
</tr>
<tr>
<td>Deployment Server</td>
<td>Yes</td>
<td>Supported for deploying the configured add-on to multiple nodes. This is a Splunk best practice and the Splunk Apps for Microsoft Exchange and Windows Infrastructure use a deployment server</td>
</tr>
</tbody>
</table>
Distributed deployment feature | Supported | Comments
--- | --- | ---
 | | to facilitate easier installation.

**Installation walkthroughs**

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light
Configuration

Configure the Splunk Add-on for Microsoft Active Directory

The Splunk Add-on for Microsoft Active Directory does not require configuration as packaged by Splunk. To gain the knowledge that the add-on provides, install it into universal forwarders on your Active Directory domain controllers. If a Windows host performs both Active Directory Domain Services and DNS Server roles, install both it and the Splunk Add-on for Windows DNS into the same universal forwarder.

Additionally, to get the search time extractions that the add-on provides, install both this add-on and the Splunk Add-on for Windows DNS into the indexers that receive the Active Directory and DNS data, and any search heads that connect to and search those indexers.

Troubleshoot the Splunk Add-ons for Microsoft Active Directory

General troubleshooting

For helpful troubleshooting tips that you can apply to all add-ons, see "Troubleshoot add-ons". You can also access these support and resource links.

Data appears in the wrong index

Both the Splunk Add-ons for Microsoft Active Directory and Windows DNS expect the following indexes to be present on your indexers:

- msad
- perfmon
- winevents
- windows (for backward compatibility)
- wineventlog (for backward compatibility)

Ensure those indexes are present by installing the add-ons into all indexers in the deployment.
Sourcetype changes for WinEventLog data

The Splunk Add-on for Windows version 5.0.x introduces changes to WinEventLog data sourcetypes, and now assigns the WinEventLog sourcetype to the following WinEventLog inputs of the Splunk Add-on for Microsoft Active Directory:

<table>
<thead>
<tr>
<th>Windows AD input</th>
<th>Sourcetype</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinEventLog://DFS Replication</td>
<td>WinEventLog</td>
</tr>
<tr>
<td>WinEventLog://Directory Service</td>
<td>WinEventLog</td>
</tr>
<tr>
<td>WinEventLog://File Replication Service</td>
<td>WinEventLog</td>
</tr>
<tr>
<td>WinEventLog://Key Management Service</td>
<td>WinEventLog</td>
</tr>
</tbody>
</table>

WinEventLogs are distinguished by their source.
Lookups

Lookups for the Splunk Add-on for Microsoft Active Directory

Splunk Add-on for Microsoft Active Directory

The Splunk Add-on for Microsoft Active Directory does not have any lookups.