Splunk® Add-on for Microsoft Windows DNS Install and use the Splunk Add-on for Windows DNS 1.0.1

Generated: 3/08/2019 8:14 pm
Table of Contents

Overview.................................................................................................................................1
  About the Splunk Add-on for Windows DNS.................................................................1
  Source types for the Splunk Add-on for Windows DNS..............................................1
  Release notes.....................................................................................................................2

Installation.............................................................................................................................4
  Hardware and software requirements for the Splunk Add-on for Windows DNS...........4
  Install the Splunk Add-on for Windows DNS.................................................................4

Configuration.........................................................................................................................8
  Configure the Splunk Add-on for Windows DNS..............................................................8
  Troubleshoot the Splunk Add-on for Windows DNS......................................................8

Lookups................................................................................................................................10
  Lookups for the Splunk Add-on for Windows DNS.........................................................10
Overview

The Splunk Add-on for Windows DNS version 1.0.1 is not supported when installed alongside the Splunk Add-on for Windows version 6.0.0. The Splunk Add-on for Windows version 6.0.0 includes the Splunk Add-on for Windows DNS and the Splunk Add-on for Microsoft Active Directory.

The Splunk Add-on for Windows DNS reached its End of Life (EoL) on February 18, 2019.

About the Splunk Add-on for Windows DNS

<table>
<thead>
<tr>
<th>Version</th>
<th>1.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Products</td>
<td>Microsoft Windows DNS Server</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 Windows DNS lets you collect Domain Name Server debug logs from Windows hosts that run Windows DNS Server.

Windows DNS Server does not log certain events by default, and the Splunk Add-on for Windows DNS requires that you enable debug logging.

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 Windows DNS at http://answers.splunk.com/answers/app/3208.

Source types for the Splunk Add-on for Windows DNS

The Splunk Add-on for Windows DNS provides the following source types
Splunk Add-on for Windows DNS

<table>
<thead>
<tr>
<th>Source type</th>
<th>Description</th>
<th>CIM data models</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSAD:NT6:DNS-Zone-Information</td>
<td>Information about DNS zones</td>
<td></td>
</tr>
<tr>
<td>MSAD:NT6:DNS-Health</td>
<td>Information about the health of DNS servers</td>
<td></td>
</tr>
<tr>
<td>MSAD:NT6:DNS</td>
<td>DNS server activity statistics</td>
<td>Network Resolution (DNS)</td>
</tr>
</tbody>
</table>

The Splunk Add-on for Windows DNS version 1.0.1 is not supported when installed alongside the Splunk Add-on for Windows version 6.0.0. The Splunk Add-on for Windows version 6.0.0 includes the Splunk Add-on for Windows DNS and the Splunk Add-on for Microsoft Active Directory.

The Splunk Add-on for Windows DNS reached its End of Life (EoL) on February 18, 2019.

Release notes

The latest version of the Splunk Add-on for Windows DNS was released on October 25, 2016.

Known issues

The Splunk Add-on for Windows DNS has the following known issues:

None at this time.

Fixed Issues

<table>
<thead>
<tr>
<th>Publication Date</th>
<th>Defect Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-10-10</td>
<td>TAG-11961</td>
<td>Update to latest common build.</td>
</tr>
<tr>
<td>2016-10-04</td>
<td>TAG-11880</td>
<td>Splunk_TA_microsoft_dns - possible incorrect FIELDALIAS</td>
</tr>
</tbody>
</table>
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 input of the Splunk Add-on for Microsoft DNS:

<table>
<thead>
<tr>
<th>Windows AD input</th>
<th>Sourcetype</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinEventLog://DNS Server</td>
<td>WinEventLog</td>
</tr>
</tbody>
</table>

WinEventLogs are distinguished by their source.
Installation

Hardware and software requirements for the Splunk Add-on for Windows DNS

Splunk admin requirements

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

Windows DNS setup requirements

To use the Splunk Add-on for Windows DNS, you must enable DNS server debug logging. See Select and enable debug logging options on the DNS server on MS TechNet.

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 Windows DNS

1. Get the Splunk Add-on for Windows DNS by downloading it from https://splunkbase.splunk.com/app/3208 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.
This add-on has 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
- Download and configure the Splunk Add-on for Windows DNS

**Splunk App for Windows Infrastructure**
- Download and configure the Splunk Add-on for Microsoft Active Directory
- Download and configure the Splunk Add-on for Windows DNS

You can also use the add-on to collect Windows DNS data outside of these apps. For best results, however, you must configure your Windows DNS servers 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.

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

<table>
<thead>
<tr>
<th>Splunk instance type</th>
<th>Supported</th>
<th>Required</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk instance type</td>
<td>Supported</td>
<td>Required</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<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 DNS servers and where DNS knowledge management is required.</td>
</tr>
<tr>
<td>Indexers</td>
<td>Yes</td>
<td>Yes</td>
<td>Install this add-on to indexers only if they are also DNS servers and DNS knowledge is required.</td>
</tr>
<tr>
<td>Heavy Forwarders</td>
<td>Yes</td>
<td>See comments</td>
<td>All forwarder types are supported.</td>
</tr>
<tr>
<td>Universal Forwarders</td>
<td>Yes</td>
<td>See comments</td>
<td>All forwarder types are supported. If you use a universal forwarder for data collection, install the add-on to your indexers as well. The forwarder needs to be installed directly on the DNS server for DNS monitoring.</td>
</tr>
<tr>
<td>Light Forwarders</td>
<td>Yes</td>
<td>No</td>
<td>All forwarder types are supported. If you use a light forwarder for data collection, install the add-on to your indexers as well. The forwarder needs to be installed directly on the DNS server for DNS monitoring.</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.</td>
</tr>
</tbody>
</table>
Before you install this add-on to a cluster, remove the `eventgen.conf` file and all files in the `samples` folder.

<table>
<thead>
<tr>
<th>Distributed deployment feature</th>
<th>Supported</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<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 to facilitate easier installation.</td>
</tr>
</tbody>
</table>

**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 Windows DNS

The Splunk Add-on for Windows DNS does not require configuration as packaged by Splunk. To gain the knowledge that the add-on provides, install it into universal forwarders on your Windows DNS Server hosts. If a Windows host holds both Active Directory Domain Services and DNS Server roles, install this add-on and the Splunk Add-on for Microsoft Active Directory 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 Microsoft Active Directory into the indexers that receive Active Directory and DNS data, and any search heads that connect to and search those indexers.

Troubleshoot the Splunk Add-on for Windows DNS

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

The Splunk Add-on for Windows DNS expects 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 input of the Splunk Add-on for Microsoft DNS:

<table>
<thead>
<tr>
<th>Windows AD input</th>
<th>Sourcetype</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinEventLog://DNS Server</td>
<td>WinEventLog</td>
</tr>
</tbody>
</table>

WinEventLogs are distinguished by their source.
# Lookups

## Lookups for the Splunk Add-on for Windows DNS

### Splunk Add-on for Windows DNS

<table>
<thead>
<tr>
<th>Source type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns_action_lookup.csv</td>
<td>Maps DNS server response messages to action results</td>
</tr>
<tr>
<td>dns_recordclass_lookup.csv</td>
<td>Maps DNS record class numbers to DNS record classes</td>
</tr>
<tr>
<td>dns_vendor_lookup.csv</td>
<td>Maps source types to DNS vendor (Microsoft)</td>
</tr>
</tbody>
</table>