Splunk® App for Windows Infrastructure
Deploy and Use the Splunk App for Windows Infrastructure 2.0.1

Best practices guide

Generated: 6/20/2020 11:37 pm
Best practices guide

Splunk has put together this Best Practices in the course of developing and using the Splunk App for Windows Infrastructure. You can expect continued updates to this guide as we update the app with feedback from our customers and partners.

If you're using TA-Windows version 6.0.0 or later, you don't need TA_AD and TA_DNS. TA_AD and TA_DNS are merged with TA-Windows version 6.0.0.

General

**Synchronize clocks on all hosts**

To ensure that the Splunk App for Windows Infrastructure sees all data coming in from the hosts in your Exchange environment, confirm that those hosts have their clocks synchronized.

- On Windows hosts, use the Windows Time service to synchronize with an available Network Time Protocol (NTP) host.
- On *nix hosts (if you use *nix hosts to host the Splunk App for Windows Infrastructure), use the `ntpd` client to synchronize with an available NTP host.

**Note:** The Windows Time service is not a full-fledged NTP client and Microsoft neither guarantees nor supports the accuracy of the service.

Active Directory

Below are some best practices for tuning Active Directory monitoring operations for the Splunk App for Windows Infrastructure.

- You must make these changes inside the universal forwarders that you have installed on the AD domain controllers in your environment.
- You must define the changes within the `Splunk_TA_microsoft_ad` add-on that you install into the universal forwarder.
- If you use a Splunk Enterprise deployment server, create server classes that deploy the add-ons with these updated configurations. Otherwise, make these changes after you have deployed the add-ons into the universal forwarders on the domain controllers.
- Once you update configurations, you must restart the universal forwarders on each domain controller for the new changes to take effect.

**Consider not including a baseline for Active Directory data collection**

You don't need to collect a baseline - or dump - of your Active Directory schema to use with the Splunk App for Windows Infrastructure. In fact, doing so can significantly increase the memory usage footprint on your domain controllers and your Splunk indexing volume. Unless you specifically need a baseline of your AD schema, consider turning it off.

1. Open `%SPLUNK_HOME%/etc/apps/Splunk_TA_microsoft_ad<version>/local/inputs.conf` for editing.
2. Modify the main `admon` stanza:

```plaintext
[admon://NearestDC]
disabled = 0
```
Consider disabling the Active Directory monitoring input on all but a select group of domain controllers

When you collect Active Directory data for the Splunk App for Windows Infrastructure, it is not necessary to enable the Active Directory monitoring input (admon) on every domain controller in your Exchange environment. If you have a number of domain controllers, consider selecting one (or two to three for redundancy) and enabling the admon inputs only on those hosts.

You should still install the Splunk_TA_microsoft_ad add-on into each domain controller. You should also install the Splunk Add-on for Windows (Splunk_TA_Windows) onto the host to get all other Windows data for the host into the Splunk App for Windows Infrastructure.

1. To configure active directory monitoring on a specific domain controller, open
   %SPLUNK_HOME%\etc\apps\Splunk_TA_microsoft_ad\local\inputs.conf for editing.
2. In the file, disable the main admon stanza.
   [admon://NearestDC]
   disabled = 1
3. Create a new Active Directory monitoring stanza and set the targetDc attribute to the NetBIOS name of the controller on which you want to run admon.
   For example, if the host on which you want to run admon is named SF-DC2, configure a new admon stanza like the following:
   [admon://ADMonitoring]
   targetDc = SF-DC2
   monitorSubtree = 1
   baseline = 0
   index = msad
   disabled = 0

Consider specifying a domain controller for Security Event Log Security ID (SID) translations

The Splunk Enterprise event log monitor translates security identifiers (SIDs) by default for the Security Event Log. Translation turns SIDs (the very long string that begins with S-1-5-21 and ends with a long jumble of numbers) into friendly account names.

The Splunk App for Windows Infrastructure does not need SID translation in the Security Event Log. This is because Active Directory events already contain this information. To reduce the amount of memory that domain controllers use to perform SID translation, configure the Splunk Add-on for Windows (Splunk_TA_Windows) to disable SID translation.

1. To disable SID translation, open %SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\local\inputs.conf for editing.
2. In this file, modify the Security Event Log stanza.
   [WinEventLog://Security]
   evt_resolve_ad_obj = 0

If you require SID translation, you can limit both its scope and where it occurs by setting the current_only and evt_dc_name attributes:

[WinEventLog://Security]
evt_dc_name = SF-DC2  # only use SF-DC2 to translate SIDs
current_only = 1  # only translate SIDs for events that come in for new events
Consider limiting AD object access events to reduce impact on license usage

When you enable auditing on your AD domain controllers, the DCs create Security Event Code 4662 events each time a user accesses any kind of AD object. (On Windows Server 2003 and Server 2003 R2, the event code is 566). This can greatly impact license volume and potentially cause violations.

To address the problem, limit the indexing of these event codes by blocking some of the events which contain them (the app uses the events for Group Policy monitoring but no other purpose.)

This procedure requires that you use Splunk universal forwarder version 6.1 or later. If you cannot use this version of the universal forwarder, then this strategy does not apply to you.