# Table of Contents

**Introduction**
- About the Splunk App for Windows Infrastructure .......................................................... 1
- New to Splunk? .................................................................................................................. 2
- How this app fits into the Splunk picture ........................................................................... 4
- How to get support and find more information about Splunk Enterprise ...................... 4

**Plan your Splunk App for Windows Infrastructure deployment** ..................................... 5
- Platform and hardware requirements ............................................................................... 5
- Permissions checklist ........................................................................................................ 8
- What data the Splunk App for Windows Infrastructure collects ..................................... 9

**Set up basic infrastructure** ............................................................................................ 10
- What a Splunk App for Windows Infrastructure deployment looks like ......................... 10
- How to deploy the Splunk App for Windows Infrastructure ........................................... 11
- Install and configure a Splunk platform indexer ............................................................... 13
- Create the "send to indexer" app ..................................................................................... 15
- Set up a deployment server and create a server class ....................................................... 17
- Install a universal forwarder on each Windows host ....................................................... 19
- Add the universal forwarder to the server class .............................................................. 20

**Get Windows data** .......................................................................................................... 23
- Download and configure the Splunk Add-on for Windows ............................................. 23
- Deploy the Splunk Add-on for Windows ......................................................................... 29
- Confirm and troubleshoot Windows data collection ....................................................... 30
- Sample searches and dashboards .................................................................................... 31

**Get data from TA-Windows version 6.0.0 or later** .......................................................... 32
- Download and configure the Splunk Add-on for Windows version 6.0.0 or later .......... 32

**Get Active Directory data** ............................................................................................ 42
- Configure Active Directory audit policy ......................................................................... 42
- Download and configure the Splunk Add-on for Microsoft Active Directory .............. 44
- Deploy the Splunk Add-on for Microsoft Active Directory .......................................... 45
- Confirm and troubleshoot AD data collection ............................................................... 47
- Sample searches and dashboards .................................................................................... 48

**Get Domain Name Service (DNS) data** ....................................................................... 49
- Configure Windows Domain Name Server .................................................................... 49
- Download and configure the Splunk Add-on for Windows DNS .................................... 49
- Confirm and troubleshoot DNS data collection .............................................................. 50
- Sample DNS searches and dashboards .............................................................................. 51

**Deploy the Splunk App for Windows Infrastructure** ....................................................... 53
- Install the Splunk App for Windows Infrastructure on the Search Head ...................... 53
- Install the Splunk App for Windows Infrastructure on a search head cluster ............. 54
- Install the Splunk App for Windows Infrastructure using self service installation on Splunk Cloud ................................................................. 58
# Table of Contents

**Upgrade the Splunk App for Windows Infrastructure**
- How to upgrade the Splunk App for Windows Infrastructure ............................................. 64
- Upgrade from version 1.0.x ........................................................................................................ 64
- Upgrade from version 1.1.x ........................................................................................................ 69
- Upgrade from version 1.2.x ........................................................................................................ 69

**Use the Splunk App for Windows Infrastructure** ................................................................. 72
- Log in and get started ................................................................................................................ 72
- Configure the Splunk App for Windows Infrastructure ....................................................... 72
- Dashboard reference .................................................................................................................. 77
- Build custom dashboards ........................................................................................................ 78

**Build custom dashboards** .................................................................................................... 78
- Build custom dashboards ........................................................................................................ 78

**Troubleshoot the Splunk App for Windows Infrastructure** .................................................. 79
- Troubleshoot the Splunk App for Windows Infrastructure .................................................. 79

**Advanced topics** .................................................................................................................. 83
- Size and scale a Splunk App for Windows Infrastructure deployment .............................. 83

**Best practices guide** ............................................................................................................ 86
- Best practices guide ................................................................................................................ 86

**Release notes** ...................................................................................................................... 89
- Release notes for Splunk App for Windows Infrastructure ................................................ 89
- Third-party software attributions/credits ............................................................................ 89
Introduction

About the Splunk App for Windows Infrastructure

Overview

The Splunk App for Windows Infrastructure gives you deep visibility into the health and performance of your Microsoft Windows Server and Active Directory environments.

It includes components that let you monitor system, server, network, and printer availability. It includes modules which allow you to monitor other aspects of your Windows network, including:

- Microsoft Windows Server (through the separately available Splunk Add-on for Windows)
- Microsoft Windows Server Active Directory (through the included Splunk Supporting Add-on for Microsoft Windows Active Directory suite)

Use the Splunk App for Windows Infrastructure to:

- Identify infrastructure problems, such as non-running services and load issues
- Monitor the performance of all servers throughout your Windows environment
- Monitor security events, such as virus outbreaks and anomalous logons
- Track administrative changes to the environment
- Plan for capacity expansion

Important: Read and understand the Splunk App for Windows Infrastructure's platform and hardware requirements before downloading and attempting to install the app. Also, learn what data the app collects.

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.

How does it work?

Splunk universal forwarders gather logs and performance metrics from the following components of your Microsoft Windows deployment:

- Windows Server (via the Splunk Add-on for Windows)
- Active Directory

Splunk Universal forwarders then send them to a central Splunk instance that runs Splunk App for Windows Infrastructure. The app provides reports and dashboards that allow you to review the status of your Windows services.

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.

How do I get it?

Download the Splunk App for Windows Infrastructure from Splunkbase.
How do I install it?

The Splunk App for Windows Infrastructure has a revamped installation procedure. See "How to deploy the Splunk App for Windows Infrastructure" to read about it.

How do I upgrade from a previous version?

If you already run a previous version of the Splunk App for Windows Infrastructure, you can follow the upgrade instructions.

For information on what's new, as well as any known issues in this version, review the release notes.

New to Splunk?

If this is the first time you have used Splunk, then read on...this topic introduces the most important Splunk concepts you need to understand when installing and using Splunk apps.

Splunk and Splunk apps work together.

The key points to come away with are:

- All Splunk apps run on the Splunk platform.
- Understanding how Splunk works will greatly help you understand how Splunk apps work.
- Installing and configuring the app is only part of the experience - you might need to prepare Splunk before installing your app.
- Careful planning helps achieve a successful app deployment experience.

Splunk basics

Splunk is a software platform that accepts data from many different sources, such as files or network streams. Splunk stores a unique copy of this data in what's called an index. Once the data is there, you can connect to Splunk with your web browser and run searches across that data. You can even make reports or graphs on the data, right from within the browser.

You can extend Splunk's capability by installing apps. Splunk apps come with searches, reports, and graphs about specific products that are common to most IT departments. These searches, reports, and graphs reduce the amount of time it takes to glean real value from installing and running the Splunk platform.

Before you can really understand how Splunk apps work, you should understand how Splunk works. Fortunately, we've got you covered in that respect.

If you're new to Splunk, then the best place to learn more about it is in the Search Tutorial. It helps you learn what Splunk is and what it does, as well as what you need to run it and get step-by-step walk-throughs on how to set it up, get data into it, search with it, and create reports and dashboards on it.

Licensing

The next thing you want to learn about is Splunk's licensing model. Splunk charges you based on the amount of data you index. The licensing introduction from the Admin Manual is a great place to start learning about how licenses work. You
can also find out the types of licenses that are available, how to install, remove, and manage them, and what happens when you go over your license quota.

In the context of Splunk apps, the amount of licensing capacity you need depends on how each app defines the individual data inputs that it uses. Splunk apps use inputs to tell Splunk what data it needs to collect for the app's purpose. Some apps, such as the Splunk App for Enterprise Security, collect a lot of data, which your license must cover in order for you to be able to search that data without interruption. When planning for your app, make sure you include enough licensing capacity.

**Configuration**

Much of Splunk's extensibility is in how configurable it is. You must configure Splunk before it can collect data and extract knowledge. All Splunk apps use configuration files to determine how to collect, transform, display, and provide alerts for data. The Admin Manual shows you how to configure those files and includes a reference topic for each configuration file that Splunk uses. In some cases, you can also use Splunk Web or the CLI to make changes to a Splunk app's configuration.

Splunk also uses configuration files to configure itself. When Splunk initializes, it finds all of the configuration files located in the Splunk directory and merges them to build a final "master" configuration, which it then runs on. When you install a Splunk app on a Splunk instance, Splunk must determine which configuration files to use if it encounters a conflict. This is where configuration file precedence comes in.

It's important to understand how precedence works. In many cases, if there is a configuration file conflict, Splunk gives priority to an app's configuration file. In some situations, installing an app might inadvertently override a setting in a configuration file in the core platform, which might lead to undesired results in data collection. Be sure to read the previously mentioned topic thoroughly for details.

**Splunk Search**

Splunk provides the ability to look through all the data it indexes and create dashboards, reports, and even alerts. All Splunk apps rely on Splunk search, so it's a good idea to read the overview on search in the Search Manual to learn how powerful Splunk's search engine is (the Tutorial is also a good place to learn about Splunk search.)

You should also have an understanding of the Splunk search processing language. Splunk apps use the search language extensively to put together search results and knowledge objects which drive their dashboards, reports, charts, and tables.

Finally, it's a good idea to familiarize yourself with the search commands in the Search Reference. That manual describes the commands that both Splunk and your Splunk app can use.

**Sources and source types**

When Splunk indexes data, it does so from a source - an entity that provides data for Splunk to extract, for example, Windows event logs, or *nix syslogs. Splunk tags incoming data with a "source" field as it gets indexed. The source type is an indicator for the type of data, so that Splunk knows how to properly format and extract it as it comes in. It's also - conveniently enough - a way to categorize data, as you can use Splunk search to display all data of a certain source type.

Splunk apps use sources and source types to extract knowledge from the data they index. Many views in an application depend on searches with specific sources and source types defined in them. Splunk apps sometimes use the source types that come with Splunk, and sometimes they define their own.
Capacity planning and distributed Splunk

Another important factor to consider when using a Splunk app: Do you have enough hardware to realistically support a deployment for the Splunk app you’re using? Read our capacity planning documentation for a head-start on ensuring you have the machinery in place to run your Splunk app deployment at peak performance.

Learning about capacity planning is a perfect time to introduce another concept with which you should be familiar: distributed search. Nearly every Splunk app available can use distributed search, and many were developed with distributed search in mind. What this means is that you must working with multiple Splunk instances at once - with each instance playing a specific role - to use the app to its full potential. Initially, you add indexers to increase indexing performance, then you add search heads to increase search performance. The Distributed Deployment Manual provides details on how to add more Splunk instances to keep up with your app’s performance demands.

What's next?

From this point, you are ready to plan your app deployment. Continue reading for information about how this app fits into the Splunk picture, platform and hardware requirements, and other deployment considerations.

How this app fits into the Splunk picture

The Splunk App for Windows Infrastructure is one of a variety of apps and add-ons available within the Splunk ecosystem. All Splunk apps and add-ons run on top of a core Splunk Enterprise installation. You need to install Splunk Enterprise first, and then install the app and add-on components of the Splunk App for Windows Infrastructure.

- For specifics about what where to deploy the app components, see “What a Splunk App for Windows Infrastructure deployment looks like” in this manual.
- For details about apps and add-ons, refer to “What are apps and add-ons?” in the core Splunk Enterprise product documentation.
- To download Splunk Enterprise, visit the download page on splunk.com.
- To get more apps and add-ons, visit Splunk Apps.

How to get support and find more information about Splunk Enterprise

If you have questions about the Splunk App for Windows Infrastructure, log a case via the Splunk Support Portal.

If your Splunk Enterprise deployment is large or complex, you might want to engage a member of the Splunk Professional Services team to assist you in deploying the Splunk App for Windows Infrastructure.

Find more information about Splunk

You’ve got a variety of options for finding more information about Splunk:

- The core Splunk documentation
- Splunk Answers
- The #splunk IRC channel on EFNET
Plan your Splunk App for Windows Infrastructure deployment

Platform and hardware requirements

The Splunk App for Windows Infrastructure supports Splunk Enterprise 7.2.x to 8.0.x. All instances of Splunk Enterprise in a Splunk App for Windows Infrastructure deployment must run version 7.2.x to 8.0.x.

Distributed installation of this app

This table provides a quick reference for installing this app onto a distributed deployment of Splunk Enterprise.

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.

<table>
<thead>
<tr>
<th>Splunk instance type</th>
<th>Supported</th>
<th>Required</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Heads</td>
<td>Yes</td>
<td>Yes</td>
<td>Install this app onto all search heads where you require knowledge management.</td>
</tr>
<tr>
<td>Indexers</td>
<td>No</td>
<td>No</td>
<td>The Splunk App for Windows Infrastructure does not require installation on indexers, but some components that the app needs to work, such as the Splunk Add-on for Windows, must be installed there. Indexes to which Splunk Add-on for Windows is sending data must be defined on indexers.</td>
</tr>
<tr>
<td>Heavy Forwarders</td>
<td>No</td>
<td>No</td>
<td>The Splunk App for Windows Infrastructure does not do anything when you install it on a heavy forwarder, but you can install components that the app needs to function on HFs if you want.</td>
</tr>
<tr>
<td>Universal Forwarders</td>
<td>No</td>
<td>No</td>
<td>Use universal forwarders to get the data you need for the app. See the following chapters for instructions on how to configure forwarders to get data (each link goes to the first topic in the chapter):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Get Windows data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Get Active Directory data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Get Domain Name Service (DNS) data</td>
</tr>
<tr>
<td>Light Forwarders</td>
<td>No</td>
<td>No</td>
<td>You can use light forwarders to send data to indexers for the app, but remember that:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Light forwarders have been deprecated and could be removed in a future version of Splunk Enterprise.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Universal forwarders have better performance than light forwarders.</td>
</tr>
</tbody>
</table>

Distributed deployment 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 app on a search head cluster. Follow the procedures that this manual outlines to get the data for the app, then install the app on the cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• How to deploy the Splunk App for Windows Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Install the Splunk App for Windows Infrastructure on a search head cluster</td>
</tr>
<tr>
<td>Distributed deployment feature</td>
<td>Supported</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Indexer Clusters</td>
<td>Yes</td>
<td>Before you start the Splunk App for Windows Infrastructure installation, configure your indexer cluster.</td>
</tr>
<tr>
<td>Deployment Server</td>
<td>Yes</td>
<td>These instructions use a deployment server to set up some of the basic environment for the Splunk App for Windows Infrastructure, including the &quot;send to indexer&quot; package, which tells forwarders that connect to the deployment server to send data to indexers or indexer clusters that you have configured for use with the app.</td>
</tr>
</tbody>
</table>

**Hardware requirements**

The Splunk App for Windows Infrastructure installs onto a full Splunk Enterprise instance. The app does not install onto a universal forwarder or a light forwarder, because it requires Splunk Web to function fully.

The app has memory, CPU, and disk requirements that are above the standard hardware requirements for the core Splunk Enterprise platform. The added resource requirements depend on how you deploy the app. Be sure to deploy hardware that meets or exceeds the hardware requirements listed in the core Splunk Enterprise documentation.

- For additional details about supported versions of Windows for Splunk Enterprise, see "System requirements" in the core Splunk Enterprise documentation.
- For information about estimating hardware requirements for a Splunk deployment, read the following core Splunk Enterprise documentation topics:
  - Introduction to capacity planning for Splunk Enterprise in the Capacity Planning Manual.

**Operating system requirements**

You can install the Splunk App for Windows Infrastructure on Splunk Enterprise instances that run on many current versions of Windows, including:

- Windows 7, 8.1, and 10 (64-bit only).
- Windows Server 2008/2008 R2, Server 2012/2012 R2 (64-bit only) and Server 2016.

The app requires a 64-bit version of Windows because of App Key Value Store.

You can also install the app on a non-Windows Splunk Enterprise instance to display Windows data coming from external Windows sources:

- Linux

Neither Splunk nor the Splunk App for Windows Infrastructure runs on:

- Windows 95, 98, or Me
- Windows NT Workstation or Server 3.1, 3.5, or 4.0
- Windows 2000 Workstation or Server

**What browsers does the Splunk App for Windows Infrastructure support?**

The Splunk App for Windows Infrastructure supports all browsers that the current version of Splunk Enterprise supports.
**What are the other prerequisites?**

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.

**The Splunk Add-on for Windows version 6.0.0 or version 7.0.0**

**Version Compatibility Table**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.0</td>
<td>2.0.0</td>
<td>7.2.x to 7.3.x</td>
<td>2010, 2013, 2016, 2019</td>
<td>2008, 2008 R2, 2012, 2012 R2, 2016</td>
<td>N/A</td>
<td>N/A</td>
<td>3.0.0</td>
</tr>
<tr>
<td>7.0.0</td>
<td>2.0.0</td>
<td>7.2.x to 8.0.x</td>
<td>2010, 2013, 2016, 2019</td>
<td>2008, 2008 R2, 2012, 2012 R2, 2016</td>
<td>N/A</td>
<td>N/A</td>
<td>3.0.0</td>
</tr>
<tr>
<td>6.0.0</td>
<td>2.0.1</td>
<td>7.2.x to 7.3.x</td>
<td>2010, 2013, 2016, 2019</td>
<td>2008, 2008 R2, 2012, 2012 R2, 2016</td>
<td>N/A</td>
<td>N/A</td>
<td>3.0.1</td>
</tr>
<tr>
<td>7.0.0</td>
<td>2.0.1</td>
<td>7.2.x to 8.0.x</td>
<td>2010, 2013, 2016, 2019</td>
<td>2008, 2008 R2, 2012, 2012 R2, 2016</td>
<td>N/A</td>
<td>N/A</td>
<td>3.0.1</td>
</tr>
</tbody>
</table>

In order to collect data from the Windows and Exchange servers in your environment, you need the Splunk Technology Add-on for Windows version 6.0.0 or 7.0.0.

This add-on installs into the universal forwarder that you install on the Windows servers from which you want to collect Windows data. It also installs on search heads that run the Splunk App for Windows Infrastructure to provide knowledge objects to the app. Optionally, it also installs onto all indexers in the central Splunk App for Windows instance for data collection (on Windows hosts) and to add knowledge for extractions.

You can download the Splunk Add-on for Windows from Splunkbase.

**The Splunk Add-ons for Microsoft Active Directory 1.0.0 or later and Windows DNS v1.0.1 or later**

The suite of Splunk Add-ons for Active Directory must be installed on universal forwarders and search heads in the Windows deployment.

You can download the Splunk Add-ons for Microsoft Active Directory and Windows DNS from Splunkbase.

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.

**The Splunk Supporting Add-on for Active Directory (SA-LDAPsearch) v3.0.1**

The Splunk Supporting Add-on for Active Directory (SA-LDAPsearch) version 3.0.1 must be installed on the same instances of Splunk Enterprise that the Splunk App for Windows Infrastructure resides.
You can download the Splunk Supporting Add-on for Active Directory from Splunk Apps.

**A proficient understanding of distributed Splunk deployments**

If you plan for your Splunk App for Windows Infrastructure deployment to monitor a large number of Active Directory servers, or even a small number, you must understand how distributed Splunk works. You must understand how the instance of Splunk Enterprise that hosts the app interacts with the universal forwarders that send data to the app. You must also understand what you need to do to increase search and indexing performance to make the app run faster. Read the following core Splunk topics for additional information:

- Distributed overview - A high level description of distributed Splunk Enterprise.
- About forwarding and receiving data - A primer on how data forwarding works.
- About distributed search - A primer on how distributed search works.

**Time and patience**

The Splunk App for Windows Infrastructure is an advanced application that has several components that must be configured correctly in order for the app to run. Depending on the size of your Windows network, it can take a while to get a Splunk App for Windows Infrastructure deployment up and running correctly.

You will spend time procuring hardware, identifying servers you want to monitor, installing the app and its included add-ons, tweaking configurations, and troubleshooting any issues you come across.

The setup instructions in this manual span several chapters and uses the Splunk Enterprise *deployment server* for automation wherever possible. Still, expect to spend a minimum of 4 to 8 hours on the project, and longer if you have a large deployment.

If your deployment is large or complex, Splunk is here to help. You can contact Professional Services for assistance if you have an Enterprise support contract.

**Do not install and configure the Splunk App for Windows Infrastructure and the Splunk App for Microsoft Exchange on the same search head**

The Splunk App for Windows Infrastructure and the Splunk App for Microsoft Exchange should not be installed on the same search head, as both apps contain identical knowledge objects that may cause a conflict when installed on the same search head deployment. If you need dashboards and functionalities for both apps on the same search head, then install only the Splunk App for Microsoft Exchange as it covers all dashboards and functionalities of the Splunk App for Windows Infrastructure.

**Permissions checklist**

This topic details the list of permissions you must have in order to install the Splunk App for Windows Infrastructure.

**Administrative access to Active Directory**

In order to make changes to Active Directory services, such as enabling debug logging in DNS and increasing Active Directory audit policy, you must be a domain administrator in the Active Directory domain(s) you want to monitor.
Administrative access to Windows servers

You must have administrative access to all Windows hosts in the Splunk App for Windows Infrastructure deployment. The hosts in the deployment require this access to install Splunk Enterprise. Any hosts in the field also require this access to install universal forwarders. Splunk Enterprise must run as a user with administrative access to the host (usually, the Local System user).

What data the Splunk App for Windows Infrastructure collects

The Splunk App for Windows Infrastructure’s associated add-ons collect data from your Windows servers. They then send the data to an index, which the app uses in its dashboards, charts, and reports. This topic discusses the specifics of the data that the app collects and displays.

The Splunk App for Windows Infrastructure collects the following data using file inputs:

- Performance monitoring data.
- Active Directory logs (via the Splunk Add-on for Windows and the Splunk Add-on for Active Directory suite.)
- Windows network, host, and printer monitoring information (via the Splunk Add-on for Windows.)

Windows Event logs (via the Splunk Add-on for Windows):
  ♦ Security Logs
  ♦ Application logs

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.

Indexes that the Splunk App for Windows Infrastructure uses

The Splunk App for Windows Infrastructure puts the data it indexes into several indexes:

- Windows host, networking, and printer data get indexed into the windows index.
- The Windows event logs get indexed into the wineventlog index.
- The performance monitor logs get indexed into the perfmon index.
- The Active Directory data gets indexed into the msad index.
Set up basic infrastructure

What a Splunk App for Windows Infrastructure deployment looks like

This topic discusses the overall architecture of a Splunk App for Windows Infrastructure deployment.

Introduction

A Splunk App for Windows Infrastructure deployment consists of a Splunk Enterprise instance (that contains the index and runs Splunk Web, and that users access to view the app) and a number of universal forwarders--one for each Active Directory or Windows server you want to include in the deployment.

This setup procedure guides you through the install of nearly all components on one hosts. This means that:

- The host will act as the indexer to receive incoming data from forwarders.
- The host will act as a deployment server to manage forwarders and deploy apps and configurations.
- The host will act as a search head to host the app and view the incoming data.

Only the universal forwarders in this deployment will be on different hosts. This helps reduce confusion on what components need to be installed where. Once you have an understanding of how the app and its components work, you can read the topic on how to scale the deployment for increased performance on larger environments.

Deployment diagram

The diagram below depicts an example Splunk App for Windows Infrastructure deployment.
Get started

The next page details the installation of the first piece of your Splunk App for Windows Infrastructure deployment: setting up the indexer that will act as the hub for the entire operation.

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.

How to deploy the Splunk App for Windows Infrastructure

To install the Splunk App for Windows Infrastructure, complete the chapters below in sequence.

What if I know how to install Splunk Enterprise and Splunk apps?

If you already have indexers, search heads, forwarders, and a deployment server set up, then you can skip most of the basic infrastructure setup chapter.

If you have experience installing Splunk Enterprise, then perform the installation methods you are comfortable with. It is still a good idea to review the new procedure to get an understanding of how the components work together.

The process is as follows:

1. Set up indexer(s) to receive data.
2. Configure universal forwarders to forward data to the indexers.
3. Follow the “Get Data In” chapter to get the required data into the indexers.
4. Follow the “Complete Setup” topics to set up the app on search heads.
5. Run the guided setup experience to check for data presence and correct any problems.

Where to install components

The table below lists what components to install and where to install them. Installing the components on multiple locations is not required.

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.

Recommended Splunk App for Windows Infrastructure Component Installation Locations

<table>
<thead>
<tr>
<th>Search Head</th>
<th>Indexer</th>
<th>Univ. Fwder.</th>
<th>Deploy. Serv.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk App for Windows Infrastructure</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk Add-on for Windows 1</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>“Send to indexer” app 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk Add-on for MS Active Directory</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Splunk Add-on for Windows DNS</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Splunk Supporting Add-on for Active Dir.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You must configure this add-on before you install it. You only require this app when you use a deployment server and want to control all forwarding configurations from there.

W. Only if this host runs Windows and you want to monitor it with the app.

**Set up basic infrastructure**

This chapter sets up the basic building blocks for the environment.

1. **Install and configuring a Splunk indexer.**
2. **Create the “send to indexer” app.** This app configures forwarding on hosts that send data to the indexer.
3. **Set up a deployment server** to manage the “send to indexer” and other apps.
4. **Install a universal forwarder on each Windows host** and tell them to contact the deployment server for configuration and app downloads.
5. **As each universal forwarder connects, add them to a base “universal forwarder” server class** to turn them into deployment clients.

After you complete this chapter, you have the basic framework for a deployment.

**Get Data In**

The next chapters take you through configuring the apps and add-ons that the Splunk App for Windows Infrastructure needs and deploying them to the right deployment clients. At the end of each chapter, you can confirm that data is present on the indexer by running some sample search commands.

1. The "Get Windows data" chapter discusses getting Windows data into the indexer. Follow it from beginning to end to install the Splunk Add-on for Windows on every Windows host in the environment.
2. The "Get Active Directory data" chapter details configuring Active Directory and getting AD data into the indexer. Complete the instructions in this chapter to install the Splunk Add-ons for Active Directory onto Active Directory hosts in the environment.
3. The "Get Domain Name Services (DNS) data" chapter provides instructions on how to get Windows DNS data into the service. Perform the procedures in this chapter to deploy the Splunk Add-ons for Windows DNS on DNS hosts and get DNS data.

If you're using TA-Windows v6.0.0, you don't need TA_AD and TA_DNS. TA_AD and TA_DNS are merged with TA-Windows v6.0.0.

**Complete setup**

After getting data in and confirming that it is there, complete setup.

1. **Installing the app and some add-ons onto the indexer.**
Run the guided setup experience

After you add a license, activate the app.

1. Log into the indexer and select the app to start the guided setup experience.
2. Follow the prompts to confirm prerequisites, locate minimum data requirements, and configure aliases. You might need to go to other apps like the Splunk Supporting App for Active Directory to add or change configurations.
3. The app searches for your data, builds lookups and data models, and enables features and pages.
4. After it completes, it is ready for you to use! You can head over to the Reference manual to learn about the new pages that come with the app, and how to use all of the pages.

Install and configure a Splunk platform indexer

This topic discusses installing the basic building block of a Splunk App for Windows Infrastructure deployment: a Splunk platform indexer.

In this procedure, you will install the indexer and then configure it to receive data from other Splunk platform instances.

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.

Install the indexer

To install an indexer:

1. Prepare a host that meets or exceeds the Splunk platform system requirements. During preparations:
   - Write down the host name and IP address for the host.
   - Ensure that no firewall blocks any network traffic into the host.
2. Download the Splunk platform software onto the machine.
3. Install the correct version of the software for the operating system that the host runs.
4. After installation, confirm that the Splunk platform software functions. At a minimum:
   - The software should start without error. If it doesn't, try troubleshooting it.
   - You should be able to perform a basic search using the Search app. Learn how. If that doesn't work, figure out why.

If everything checks out, configure the indexer to have the correct indexes for the Splunk App for Windows Infrastructure.

Configure indexes

The indexer must have the indexes for the Splunk App for Windows Infrastructure defined before you can begin indexing the data. Every indexer in a Splunk App for Windows Infrastructure environment needs this configuration file.

To get this file:

1. In a web browser, proceed to the Splunk App for Windows Infrastructure download page.
2. Click the download link to begin the download process.
   - Make sure you download the latest version of the app.
   - You might need to sign in with your Splunk account before the download starts.
3. When prompted, choose an accessible location to save the download. Do not attempt to run the download.
4. Use an archive utility such as WinZip to unarchive the file to the `etc/apps/` directory in your Splunk platform deployment.

5. In the unarchived `etc/apps/splunk_app_windows_infrastructure` directory in your Splunk platform deployment, create a `/local/` directory.

6. Define your indexes.
   1. Create a `indexes.conf` file in `etc/apps/splunk_app_windows_infrastructure/local/`.
   2. In `indexes.conf`, define the `msad`, `perfmon`, `wineventlog`, and `windows` indexes.

   Examples:

   ```
   [msad]
   homePath = $SPLUNK_DB/msad/db
   coldPath = $SPLUNK_DB/msad/colddb
   thawedPath = $SPLUNK_DB/msad/thaweddb
   maxDataSize = 10000
   maxHotBuckets = 10

   [perfmon]
   homePath = $SPLUNK_DB/perfmon/db
   coldPath = $SPLUNK_DB/perfmon/colddb
   thawedPath = $SPLUNK_DB/perfmon/thaweddb
   maxDataSize = 10000
   maxHotBuckets = 10

   [wineventlog]
   homePath = $SPLUNK_DB/wineventlog/db
   coldPath = $SPLUNK_DB/wineventlog/colddb
   thawedPath = $SPLUNK_DB/wineventlog/thaweddb
   maxDataSize = 10000
   maxHotBuckets = 10

   [windows]
   homePath = $SPLUNK_DB/windows/db
   coldPath = $SPLUNK_DB/windows/colddb
   thawedPath = $SPLUNK_DB/windows/thaweddb
   maxDataSize = 10000
   maxHotBuckets = 10
   ```

   7. If `Splunk_TA_windows` is sending data to other then the above default indexes then a user must have defined those custom indexes on all indexers.

   8. Restart your Splunk platform instance. From the same PowerShell window:

   ```
   > cd \Program Files\Splunk\bin
   > .\splunk restart
   ```

   You can now configure the indexer to receive data from other Splunk instances.

**Configure receiving**

The Splunk App for Windows Infrastructure depends on an indexer that can receive data from other hosts. Without this capability, the app cannot function. You will now enable receiving on this indexer.

To configure the indexer to receive data from other Splunk platform instances:

1. Log into Splunk Enterprise on the indexer.
2. In the system bar, click **Settings > Forwarding and Receiving**. Your Splunk platform loads the "Forwarding and Receiving" page.
3. Under "Receive Data" click **Configure Receiving**.
4. Click **New**.

5. In the **Listen on this port** field, enter the port number that you want your Splunk platform to listen on for incoming data from other Splunk instances. The conventional port number is 9997.

6. Click **Save**. Splunk Enterprise saves the port number and enables receiving on the indexer.

Your indexer is now configured to receive data. Confirm the host name or IP address and port number of the indexer. You will need it for the next step of the setup process.

Before you proceed, read our documentation on apps. You will create a simple app in the next step.

### Create the "send to indexer" app

This topic discusses how to create the "Send to indexer" app. This app tells the universal forwarders in your Splunk App for Windows Infrastructure deployment to send data to the indexer.

**Why create an app?**

The short answer is, to make your deployment easier.

At first it might seem like this procedure is overly complicated. Performing this step makes it easier to control where universal forwarders send data. It also helps you understand another basic concept about Splunk: apps.

Splunk apps - like the Splunk App for Windows Infrastructure - help you extend the capabilities of Splunk Enterprise. In this case, creating and deploying the app helps you extend the capability of the indexer.

Once you complete the procedure, you can use the deployment server (described in the next topic) to deliver the app to all universal forwarders in your deployment. If you need to change the configuration, you can update the app and push it out to all of the forwarders again.

**App description**

The "Send to Indexer" app tells the universal forwarders in a Splunk App for Windows Infrastructure deployment to send data to one or more indexers in the deployment. The app prevents you from having to make potentially erroneous configuration changes on many hosts by limiting the change to one place. It also reduces the amount of configuration you have to do on those hosts.
The app consists of a single file, outputs.conf, that controls where and how the universal forwarders send data. This topic shows you how to create the outputs.conf file, and then how to package this file into the "Send to Indexer" app. Once that is done, you then install the app on your deployment server (described in the next step of the process.)

Create the outputs.conf file

Before packaging the "Send to Indexer" app, you must first create the outputs.conf file. In this procedure, you will create a file that supports sending data to a single indexer.

1. Open Notepad or a similar text editor.
2. In the editor, type in the following text, substituting indexer_hostname_or_ip_address and port with the host name or IP address and receiving port of the indexer you set up in the previous step:

   ```
   [tcpout]
   defaultGroup = default-autolb-group
   
   [tcpout:default-autolb-group]
   server = <indexer_hostname_or_ip_address>:<port>
   
   [tcpout-server://<indexer_hostname_or_ip_address>:<port>]
   ```
3. Save the file as outputs.conf (In Notepad, click File > Save As? and type in "outputs.conf" in the file dialog.

   **Note:** Learn more about outputs.conf at "Configure forwarders with outputs.conf" in the core Splunk Enterprise platform documentation.

Create the "send to Indexer" app

The next step of the process is to create the app and upload the outputs.conf file you just created as an asset for the app.

1. Log back into the indexer that you set up receiving on in "Install a Splunk Enterprise Indexer".
2. In the system bar, on the upper left, click Apps > Manage Apps. Splunk Enterprise loads the Apps settings page.
3. Click Add New. Splunk Enterprise loads the "Add New" page.
4. In the Name field, enter a name for the app, for example "Send to Indexer".
5. In the Folder field, enter "sendtoindexer".
6. In the Version field, enter "1.0.0".
7. In the Visible radio buttons, check "No."
8. In the Author field, type in your name.
9. In the Description field, type in a description for the app.
10. In the Templates list box, choose "barebones".
11. Click Save. Splunk Enterprise saves the app and returns you to the Apps page.

Place the outputs.conf file into the app

Finally, copy the outputs.conf file into the app:

1. Open a PowerShell window.
2. Type in the following:

   ```
   > Copy-Item -Path <location of outputs.conf> -Destination <Splunk directory>\etc\apps\sendtoindexer\local -Force
   ```
What's next?

You should now see your app in the list on the Apps page. In the next step, you will activate the deployment server and use it to deploy the app.

Set up a deployment server and create a server class

This topic discusses how to set up deployment server to distribute the "send to indexer" app you created previously to all of the universal forwarders that you will set up as part of the Splunk App for Windows Infrastructure deployment.

What is deployment server?

The Splunk Enterprise deployment server is a system that distributes apps, configurations, and other assets to other Splunk instances. Deployment server can send assets to other full Splunk Enterprise instances as well as light and universal forwarders.

Deployment server is available on every full Splunk Enterprise instance. To use it, you must activate it.

In this setup you will use the deployment server to distribute the "send to indexer" app to all universal forwarders in the Splunk App for Windows Infrastructure deployment. You accomplish this through the Forwarder Management scheme.

Learn more at "About deployment server and forwarder management."

Why use deployment server?

Deployment server is the fastest way to get apps and configurations deployed to your Splunk universal forwarders. It is the most native way to get your environment up and running. It's also free with Splunk Enterprise.

This procedure uses deployment server to get you familiarized with the concept of using it to distribute apps and configurations quickly and efficiently.

It is not a requirement to use deployment server, however. If you want, you can use an external tool, such as Windows System Center Configuration Manager or chef, puppet, or salt if your deployment runs on *nix servers.

Activate deployment server

To activate deployment server, you must place at least one app into %SPLUNK_HOME%/etc\deployment-apps on the host you want to act as deployment server. In this case, the app is the "send to indexer" app you created earlier, and the host is the indexer you set up initially.

1. On the indexer, use your operating system file management tools to move the "sendtoindexer" folder from the Splunk apps directory to the Splunk deployment apps directory.
   ♦ Open a PowerShell window and type the following:

   &gt; Move-Item -Path C:\Program Files\Splunk\etc\apps\sendtoindexer -Destination C:\Program Files\Splunk\etc\deployment-apps\sendtoindexer

2. From the same command-line prompt, restart Splunk Enterprise:

   &gt; cd C:\Program Files\Splunk\bin
   &gt; .\splunk restart
3. Log back into Splunk Enterprise. The indexer has now gained the deployment server capability.

**View apps in Forwarder Management**

Once you have logged back into Splunk, confirm that deployment server has activated and is aware of the new "send to indexer" app:

1. In the system bar, click **Settings > Forwarder Management**.
2. Click the **Apps** tab. You should see the “sendtoindexer” app in the list.

If you don't see the app, review the instructions in "Activate deployment server" and confirm that you have copied the entire "sendtoindexer" folder over to the Splunk deployment apps directory.

**Configure a server class for the app**

The next step is to define a server class for the "send to indexer" app.

Server classes are logical data structures that tell deployment servers where and what to send to one or more deployment clients. A server class treats a set of deployment clients as a group - any member of a server class receives apps and configurations defined within that class.

In this case, server classes tell deployment server when and where to deploy the "send to indexer" app. In this procedure you will create the server class, then assign the "send to indexer" app to this class. Later, you will add universal forwarder clients to the class.

1. From the **Apps** tab in Forwarder Management, in the "sendtoindexer" listing under “Actions”, click **Edit**. Splunk Enterprise loads the "Edit app: sendtoindexer" page.
2. Click the gray "+" sign under "Server Classes."
3. In the pop-up that appears, click **New Server Class**.
4. In the "New Server Class" dialog box that pops up, enter "Universal Forwarders". **Note:** When setting up server classes later on in the setup process, you can enter a unique name for the server class that describes the hosts that belong in the class, and that you will remember.
5. Click **Save**. Splunk Enterprise saves the class and loads the information page for the server class you just created. **Note:** When you first create a server class, the page says you have not added any apps or clients yet. This is okay.
6. Click **Add apps**. Splunk Enterprise loads the "Edit Apps" page.
7. Locate and click the "sendtoindexer" app in the "Unselected Apps" pane on the left. The app moves to the "Selected Apps" pane on the right.
8. Click **Save**. Splunk Enterprise saves the configuration and returns you to the server class information page.
What's next?

You have activated deployment server and configured a server class for the "send to indexer" app. Clients that are a member of this class will receive the app automatically when they connect to this deployment server.

The next phase of setup involves installing and configuring these clients.

Install a universal forwarder on each Windows host

This topic details installing and configuring a universal forwarder on the Windows host in your environment. This is the first step toward getting data into the indexer that you set up earlier.

What is a universal forwarder?

The universal forwarder is a version of Splunk Enterprise whose only purpose is to collect data from a host and send it somewhere. Unlike full Splunk Enterprise, the universal forwarder has extremely limited capability to transform or change the data it collects in any way. This allows for fast collection and dispatching of data with little impact on system and network resources.

In this application, you install universal forwarder on a Windows host to collect the data it contains. You then forward this data to the Splunk indexer, which indexes and stores the data and makes it available for the Splunk App for Windows Infrastructure.

Install universal forwarder

In order to begin the data collection and forwarding process, you must install a universal forwarder on every Windows host that you want data from.

1. Confirm that your Windows host meets the minimum system requirements for a Splunk universal forwarder installation.
2. Download the appropriate universal forwarder for your version of Windows.
3. Install the universal forwarder onto the Windows host. During the installation process, follow these prompts:
   - In the first dialog, check the box to accept the license agreement.
   - Click Customize Options to customize the installation options.
   - Click Next to advance through the "Destination Folder" dialog.
   - Click Next to advance through the "Certificate Information" dialog.
   - In the "User selection" dialog, make sure "Local System" is selected and click Next.
   - In the "Enable Windows inputs" dialog, make sure no inputs have been enabled and click Next.
   - In the "Specify a Deployment Server" dialog, enter the host name or IP address of the deployment server you just set up in the "Hostname or IP" field and enter "8089" in the second field. Then click Next.
   - Click Next to advance through the "Receiving Indexer" dialog.
   - Click Install to accept these configurations and install the universal forwarder.
4. After installation completes, confirm that the universal forwarder service runs.
   - You can check the splunkforwarder service in the Services control panel, or
   - You can check if the service runs from a PowerShell window (by going to the %SPLUNK_HOME%\bin directory and typing in .\splunk status.)
What's next?

You have installed and configured a universal forwarder on at least one Windows machine. Next, you will confirm that deployment server sees the forwarder and add the forwarder to the server class you defined earlier.

Add the universal forwarder to the server class

This topic discusses adding the universal forwarder you installed in the previous step to the server class you defined on the deployment server. This phase is the final step in configuring the basic infrastructure for the Splunk App for Windows Infrastructure deployment - from here, you can use this procedure to add universal forwarders and server classes as needed.

Universal forwarder becomes deployment client

When you specified the deployment server during the universal forwarder installation process, the forwarder became what is known as a deployment client. Deployment clients connect to deployment servers and get apps and configurations, then activate and execute those apps and configurations locally.

Earlier, you created the "send to indexer" app, which was an outputs.conf file that provided instructions on how to send data to the indexer. You configured this file to send data to the indexer you set up at the beginning of this process. Now, you will complete the loop and deploy the app to any deployment clients that connect to the deployment server.

Confirm that deployment server can see the deployment client

The first part of this final step is to confirm that the universal forwarder you just installed phones home to the deployment server.

1. Log into the Splunk indexer you set up previously.
2. In the system bar, click **Settings > Forwarder Management**
3. Click the **Clients** tab. You should see the universal forwarder you installed in the previous step. If you don’t, confirm that the forwarder service is active and that its configuration points to this deployment server.
4. Click the **Server Classes** tab.
5. In the server class you created earlier ("Universal Forwarders"), click **Edit**, and in the pop-up that appears, click **Edit Clients**. Splunk Enterprise loads the "Edit clients" page.

This page lists all clients that
have connected to the deployment server. Those clients appear on the page below the Include, Exclude, and Filter by Machine Type controls at the top. To add clients to the server class:

6. In the Include (whitelist) field at the top of the page, type in the host name of the deployment client.
7. Click Preview. Splunk Enterprise updates the list to show you which clients match the string you entered in the "Include (whitelist)" field.
8. If the results look good to you, click Save. Splunk Enterprise returns you to the Forwarder Management page and deploys the "send to indexer" app to the deployment client.

Review server class status

To confirm that the deployment server has deployed the "send to indexer" app to the deployment client, revisit the server class properties page:

1. From the Forwarder Management page, select the server class you created earlier by clicking its name in the list.
2. Review the page.

- In the upper section, you should see the "sendtoindexer" app in the list of apps within the server class. On the right side of the page, in the "Clients" column, you should see that the app has been deployed to a client.
- In the lower section, you should see the universal forwarder you installed previously. On the right side of the page, in the "Deployed Apps" column, you should see that at least 1 app has been deployed.

If you don't see these entries, try the following steps to troubleshoot:

- Make sure the app is in the Splunk deployment apps folder on the deployment server.
- Confirm that you have configured the deployment client with the deployment server host name or IP address and management port.
- Confirm that you can contact the deployment server on its management port from the deployment client (make sure that a firewall does not block that access.)
Summary

To summarize, you have:

- Set up an indexer and configured it as a receiver.
- Created the "send to indexer" app, which tells universal forwarders to send data to this indexer.
- Activated deployment server by copying the "send to indexer" app from the Splunk apps directory to the deployment apps directory.
- Installed a universal forwarder and pointed it at the deployment server.
- Created a server class and added the "send to indexer" app and deployment client to the class.

You can use this procedure to add more apps and deployment clients to this server class. As clients come online and you add them to the server class, they get the "send to indexer" app which tells them to send data to the indexer. Once you bring all deployment clients online, you then complete basic setup of your Splunk App for Windows Infrastructure deployment.

If you need to make a change to the forwarding configuration, edit the outputs.conf file in the "send to indexer" app. After you restart Splunk Enterprise, the deployment server picks up the new changes and deploys them to all deployment clients that contact it. As you add indexers to scale the deployment, you can edit the configuration to instruct the deployment clients to send data to all indexers.

What's next?

The next step of setup is to get the Windows, and Active Directory data that is present on those hosts into the indexer. Read the next chapters to learn how to get this data into the Splunk Enterprise indexer.
Get Windows data

Download and configure the Splunk Add-on for Windows

This topic discusses downloading and configuring the Splunk Add-on for Windows and deploying it to the deployment clients to gather Windows data and send it to the Splunk App for Windows Infrastructure indexers.

About the Splunk Add-on for Windows

The Splunk Add-on for Windows collects Windows data from Windows hosts. In the context of the Splunk App for Windows Infrastructure, the add-on collects Windows data and provides knowledge objects for the app. You should deploy the Splunk Add-on for Windows to:

- All hosts that run Active Directory Domain Services (including domain controllers and DNS servers).
- All Windows hosts from which you want Windows data.
- All indexers.
- All search heads.
- Basically, everywhere.

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.

Download the Splunk Add-on for Windows

1. Download the Splunk Add-on for Windows from Splunkbase and save it to an accessible place on the deployment server. You might need to sign in with your Splunk account before the download starts.
2. When prompted, choose an accessible location on your deployment server to save the download. Do not attempt to run the download.
3. Use an archive utility such as WinZip to unarchive the file to an accessible location.

Configure the Splunk Add-on for Windows

Before the add-on can collect Windows data, you must configure it.

Microsoft Windows event logs that are rendered in XML format will not populate in the Splunk App for Windows Infrastructure

- In the location where you unarchived the download file, locate the Splunk_TA_windows directory.
- Inside this directory, make a subdirectory local.
- Copy the inputs.conf file in the default subdirectory to the local directory.
- Open the inputs.conf in the local subdirectory with a text editor, such as Notepad.
- Edit the disabled and mode attributes. Optionally, as shown below, add an index attribute to use specific indexes.

- From version 5.0.1 onwards, Splunk Add-on for Windows collects data in multikv mode by default. This mode has a different event format over the existing single mode and the Splunk App for Windows Infrastructure app supports single mode only, so please change the value of mode parameter to single in the perfmon stanzas in /Splunk_TA_windows/default/inputs.conf on forwarder.
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; 
DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 
Transitions/sec; C3 Transitions/sec
disabled = 0
instances = *
mode = single
object = Processor
useEnglishOnly=true

## Logical Disk
[perfmon://LogicalDisk]
counters = % Free Space; Free Megabytes; Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % 
Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg. Disk 
sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; 
Disk Bytes/sec; Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; 
Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec
disabled = 0
instances = *
interval = 10
mode = single
object = LogicalDisk
useEnglishOnly=true

## Physical Disk
[perfmon://PhysicalDisk]
counters = Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read 
Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; 
Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Read Bytes/sec; Disk Write 
Bytes/sec; Avg. DiskBytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec 
disabled = 0
instances = *
interval = 10
mode = single
object = PhysicalDisk
useEnglishOnly=true

## Memory
[perfmon://Memory]
counters = Page Faults/sec; Available Bytes; Committed Bytes; Commit Limit; Write Copies/sec; Transition 
Faults/sec; Cache Faults/sec; Demand Zero Faults/sec; Pages/sec; Pages Input/sec; Page Reads/sec; Pages 
Output/sec; Pool Paged Bytes; Pool Nonpaged Bytes; Page Reads/sec; Pool Paged Allocs; Pool Nonpaged 
Allocs; Free System Page Table Entries; Cache Bytes; Cache Bytes Peak; Pool Paged Resident Bytes; System Code Total 
Bytes; System Code Resident Bytes; System Driver Total Bytes; System Driver Resident Bytes; System Cache 
Resident Bytes; % Committed Bytes In Use; Available KBytes; Available MBytes; Transition Pages 
RePurposed/sec; Free & Zero Page List Bytes; Modified Page List Bytes; Standby Cache Reserve Bytes; Standby 
Cache Normal Priority Bytes; Standby Cache Core Bytes; Long-Term Average Standby Cache Lifetime (s) 
disabled = 0
interval = 10
mode = single
object = Memory
useEnglishOnly=true

## Network
[perfmon://Network]
counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets Sent/sec; Current Bandwidth; Bytes 
Received/sec; Packets Received Unicast/sec; Packets Received Non-Unicast/sec; Packets Received Discarded; 
Packets Received Errors; Packets Received Unknown; Bytes Sent/sec; Packets Sent Unicast/sec; Packets Sent 
Non-Unicast/sec; Packets Outbound Discarded; Packets Outbound Errors; Output Queue Length; Offloaded
Connections; TCP Active RSC Connections; TCP RSC Coalesced Packets/sec; TCP RSC Exceptions/sec; TCP RSC Average Packet Size
disabled = 0
instances = *
interval = 10
mode = single
object = Network Interface
useEnglishOnly=true

## Process
[perfmon://Process]
counters = % Processor Time; % User Time; % Privileged Time; Virtual Bytes Peak; Virtual Bytes; Page Faults/sec; Working Set Peak; Working Set; Page File Bytes Peak; Page File Bytes; Private Bytes; Thread Count; Priority Base; Elapsed Time; ID Process; Creating Process ID; Pool Paged Bytes; Pool Nonpaged Bytes; Handle Count; IO Read Operations/sec; IO Write Operations/sec; IO Data Operations/sec; IO Other Operations/sec; IO Read Bytes/sec; IO Write Bytes/sec; IO Data Bytes/sec; IO Other Bytes/sec; Working Set - Private
disabled = 0
instances = *
interval = 10
mode = single
object = Process
useEnglishOnly=true

## ProcessInformation
[perfmon://ProcessorInformation]
counters = % Processor Time; Processor Frequency
disabled = 0
instances = *
interval = 10
mode = single
object = Processor Information
useEnglishOnly=true

## System
[perfmon://System]
counters = File Read Operations/sec; File Write Operations/sec; File Control Operations/sec; File Read Bytes/sec; File Write Bytes/sec; File Control Bytes/sec; Context Switches/sec; System Calls/sec; File Data Operations/sec; System Up Time; Processor Queue Length; Processes; Threads; Alignment Fixups/sec; Exception Dispatches/sec; Floating Emulations/sec; % Registry Quota In Use
disabled = 0
instances = *
interval = 10
mode = single
object = System
useEnglishOnly=true

Note: If you do not complete the above step, then windows perfmon data will not be considered in dashboards.

- From version 5.0.1 onwards, Splunk Add-on for Windows has removed indexes so you have two options either you can use default windows index as mentioned in below table or you can create your own custom index. For the former one, you have to add index parameter with the values mentioned in below table in /Splunk_TA_windows/default/inputs.conf on forwarder.

| Table A |
|-----------------|-----------------|-----------------|
| **Input Stanza** | **Indexes** | **Macro** |
### Input Stanza

<table>
<thead>
<tr>
<th>Input Stanza</th>
<th>Indexes</th>
<th>Macro</th>
</tr>
</thead>
<tbody>
<tr>
<td>[monitor://$WINDIR\System32\DHCP], [monitor://$WINDIR\WindowsUpdate.log],</td>
<td>windows</td>
<td>windows-index</td>
</tr>
<tr>
<td>[script://.\bin\win_listening_ports.bat], [script://.\bin\win_installed_apps.bat],</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[script://.\bin\win_timesync_status.bat], [script://.\bin\win_timesync_configuration.bat],</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[admon://default], [WinRegMon://default], [WinRegMon://hkcu_run], [WinRegMon://hklm_run]</td>
<td>windows</td>
<td>windows-index</td>
</tr>
<tr>
<td>[monitor://$WINDIR\debug\netlogon.log], [MonitorNoHandle://$WINDIR\System32\Dns\dns.log], [script://.\bin\runpowershell.cmd nt6-repl-stat.ps1], [powershell://Replication-Stats], [script://.\bin\runpowershell.cmd nt6-health.ps1], [powershell://AD-Health][script://.\bin\runpowershell.cmd nt6-siteinfo.ps1], [powershell://Siteinfo], [script://.\bin\runpowershell.cmd dns-zoneinfo.ps1], [script://.\bin\runpowershell.cmd dns-health.ps1], [admon://default]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Here are the few examples of inputs stanzas. Similarly, you can configure others.

```plaintext
[perfmon://CPU]
counters = Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec
disabled = 0
instances = *
interval = 10
mode = single
object = Processor
useEnglishOnly=true
index = perfmon

[WinEventLog://Application]
disabled = 0
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
index = wineventlog
```
How to change the configuration files to handle custom indexes

Update the following conf files for using custom index(es)

Update inputs.conf

1. Copy the inputs.conf file from the default subdirectory /Splunk_TA_windows/default/ to the local directory folder /Splunk_TA_windows/local/
2. Open the inputs.conf in the local subdirectory with a text editor, such as Notepad.
3. If you are using <<CUSTOM INDEX>> instead of TA_windows default indexes then add index = <<CUSTOM INDEX>> under stanzas as defined in the table (Table A) for TA_windows default index(es). Refer to the above table (Table A) for TA_windows default indexes.

Here are the few examples of inputs stanzas. Similarly, you can configure others.

```plaintext
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec
disabled = 1
instances = *
mode = single
object = Processor
useEnglishOnly=true
index = <<CUSTOM INDEX>>

[WinEventLog://Application]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
index = <<CUSTOM INDEX>>

[WinPrintMon://port]
type = port
interval = 600
baseline = 1
disabled = 1
index = <<CUSTOM INDEX>>
```
**Update macros.conf**

1. Copy the macros.conf file from the default subdirectory `/splunk_app_windows_infrastructure/default/` to the local directory folder `/splunk_app_windows_infrastructure/local/` folder on search head.
2. Open the macros.conf in the local subdirectory with a text editor, such as Notepad.
3. If you are using `<<CUSTOM INDEX>>` instead of TA_windows default indexes then update the following macro definitions as shown below.

<table>
<thead>
<tr>
<th>Default Index</th>
<th>Custom Index</th>
<th>Updated Macro</th>
</tr>
</thead>
<tbody>
<tr>
<td>perfmon</td>
<td><code>&lt;&lt;CUSTOM INDEX 1&gt;&gt;</code></td>
<td><code>[perfmon-index], definition = index=perfmon OR index=&lt;&lt;CUSTOM INDEX 1&gt;&gt;</code></td>
</tr>
<tr>
<td>wineventlog</td>
<td><code>&lt;&lt;CUSTOM INDEX 2&gt;&gt;</code></td>
<td><code>[wineventlog-index], definition = index=wineventlog OR index=&lt;&lt;CUSTOM INDEX 2&gt;&gt;</code></td>
</tr>
<tr>
<td>windows</td>
<td><code>&lt;&lt;CUSTOM INDEX 3&gt;&gt;</code></td>
<td><code>[windows-index], definition = index=windows OR index=&lt;&lt;CUSTOM INDEX 3&gt;&gt;</code></td>
</tr>
</tbody>
</table>

**Update authorize.conf**

1. Copy the authorize.conf file in the default subdirectory `/splunk_app_windows_infrastructure/default/` to the local directory folder `/splunk_app_windows_infrastructure/local/` on Searchhead.
2. Open the authorize.conf in the local subdirectory with a text editor, such as Notepad.
3. Add those main(default) index(es) in authorize.conf under role_winfra-admin stanza against srchIndexesDefault parameter like shown below.

```ini
[role_winfra-admin]
srchIndexesDefault = msad; msexchange; windows; perfmon; wineventlog; <<CUSTOM INDEX 1>>; <<CUSTOM INDEX 2>>; <<CUSTOM INDEX 3>>;
```

**Note:** If no custom index or default TA_windows indexes are defined then all data will be stored in main index.

**Update the following conf files for using main index**

**Update macros.conf**

1. Copy the macros.conf file from the default subdirectory `/splunk_app_windows_infrastructure/default/` to the local directory folder `/splunk_app_windows_infrastructure/local/` folder on search head.
2. Open the macros.conf in the local subdirectory with a text editor, such as Notepad.
3. If you are using `index=main` instead of TA_windows default indexes then update the following macro definitions as shown below.

<table>
<thead>
<tr>
<th>Default Index</th>
<th>Main Index</th>
<th>Updated Macro</th>
</tr>
</thead>
<tbody>
<tr>
<td>perfmon</td>
<td>main</td>
<td><code>[perfmon-index], definition = index=perfmon OR index=main</code></td>
</tr>
<tr>
<td>wineventlog</td>
<td>main</td>
<td><code>[wineventlog-index], definition = index=wineventlog OR index=main</code></td>
</tr>
<tr>
<td>windows</td>
<td>main</td>
<td><code>[windows-index], definition = index=windows OR index=main</code></td>
</tr>
</tbody>
</table>
Update authorize.conf

1. Copy the authorize.conf file in the default subdirectory `/splunk_app_windows_infrastructure/default/` to the local directory folder `/splunk_app_windows_infrastructure/local/` on Searchhead.
2. Open the authorize.conf in the local subdirectory with a text editor, such as Notepad.
3. Add those main(default) index(es) in authorize.conf under role_winfra-admin stanza against srchIndexesDefault parameter like shown below.

```
[role_winfra-admin]
srchIndexesDefault = msad;msexchange;windows;perfmon;wineventlog;default
```

Note: If you skip this step, your Splunk platform will not have the index configurations which can result into data loss.

What's next?

You have downloaded and configured the Splunk Add-on for Windows.

Next, you will deploy it to the deployment clients. Once they receive the add-on, they will use the configuration in the "send to indexer" app to send Windows data to the indexer.

Deploy the Splunk Add-on for Windows

This topic discusses deploying the Splunk Add-on for Windows to the deployment clients that you have configured to connect to the deployment server. Once you deploy the add-on, the deployment clients begin collecting Windows data and sending it to the indexer.

Place the add-on in the deployment apps directory on the deployment server

The deployment server must be made aware of the new app. You do this by placing it in the deployment apps directory:

1. Open a command prompt on the deployment server/indexer.
2. Copy the entire Splunk Add-on for Windows folder from its current location to the deployment apps directory:

   ```
   > Copy-Item -Path C:\Downloads\Splunk_TA_Windows -Destination "C:\Program Files\Splunk\etc\deployment-apps\Splunk_TA_Windows" -Recurse
   ```
3. Tell the deployment server to reload its deployment configuration.

```
> cd \Program Files\Splunk\bin
> .\splunk reload deploy-server
```
that you set up previously.
10. Click **Save**. Splunk Enterprise saves the configuration, returns you to the Forwarder Management menu, and deploys the Splunk_TA_Windows app to the deployment client.

![Edit App: Splunk_TA_windows](image)

**What's next?**

You have now deployed the Splunk Add-on for Windows onto your deployment client. In the future, you can use this procedure to deploy the add-on to additional clients.

Next, you will confirm that Windows data is coming into the indexer.

**Confirm and troubleshoot Windows data collection**

This topic discusses how to confirm and troubleshoot data collection from the Splunk Add-on for Windows.

**Check the indexer for data**

After you configure and deploy the Splunk Add-on for Windows into your deployment client, you should check the deployment server to see that data has arrived. The fastest way to do that is to load the Search and Reporting app and view the Data Summary:

1. In the system bar, click **Apps > Search & Reporting**. Splunk Enterprise loads the Search & Reporting app.
2. Click **Data Summary**. Splunk brings up the data summary page with the "Hosts" tab active.
3. Scan through the list of host names for the name of your deployment client.
   - If you do not see the deployment client host name, then there is a problem occurring between the client at the indexer. Confirm that:
     - You have properly configured receiving on the indexer.
     - You have properly configured the "send to indexer" app to forward data to the indexer.
     - No network issue exists between the deployment client and the indexer.
4. Click the host name in the list. Splunk Enterprise brings up a search window that displays all events associated with the deployment client host name.
5. Search through the data to see that all of the events you configured in the Splunk Add-on for Windows have been sent to the indexer. See "Sample searches and dashboards."

- If you do not see the events you expect, try these steps:
  - Confirm that you have configured the Splunk Add-on for Windows for all inputs that you want it to collect.
  - Confirm that you have placed the add-on in the deployment apps directory and reloaded the deployment server.
  - Confirm that the deployment client does not have errors attempting to collect the data.
  - More troubleshooting steps are available in the Splunk Troubleshooting manual.
What's next?

You have configured and deployed the Splunk Add-on for Windows to your deployment clients. This now means that Windows data is present on the indexer.

The next step is to get Active Directory data onto the indexer.

Sample searches and dashboards

This topic lists searches that you can perform to confirm that Windows data has arrived at the indexer.

Search Windows data

To confirm that Windows data is present on the indexer, use the Search app:

1. Log into Splunk Enterprise on the indexer, if you have not already.
2. Load the Search app. In the system bar, select Apps > Search & Reporting. Splunk loads the Search app.
3. Try the following searches to confirm that data is present:

   - This search confirms that the Splunk Add-on for Windows is sending data to the indexer:

     index=wineventlog

   - This search confirms that the Splunk Add-on for Windows has been installed properly on the deployment client named <host_name>:

     index=wineventlog host=<host_name>

   - If the user has used custom index in TA_windows then the user has to search with that index:

     index=windows

Can’t find the data?

Try the following:

- Use Forwarder Management to confirm that the Splunk Add-on for Windows has been deployed to your deployment clients.
- Confirm that you have enabled Windows inputs in the Splunk Add-on for Windows. If not, make changes and deploy the app again.
- Refer to the Troubleshooting manual for additional help.
Get data from TA-Windows version 6.0.0 or later

Download and configure the Splunk Add-on for Windows version 6.0.0 or later

This topic discusses downloading and configuring the Splunk Add-on for Windows v6.0.0 or later and deploying it to the deployment clients to gather Windows/AD/DNS data and send it to the Splunk App for Windows Infrastructure indexers.

To deploy the Splunk Add-on for Windows v6.0.0 or later, see Deploy the Splunk Add-on for Windows.

To confirm and troubleshoot the Splunk Add-on for Windows v6.0.0 or later, see Confirm and Troubleshoot Data Collection.

For Sample searches and dashboards the Splunk Add-on for Windows v6.0.0 or later, see Sample searches and dashboards.

About the Splunk Add-on for Windows v6.0.0 or later

The Splunk Add-on for Windows collects Windows data from Windows hosts. In the context of the Splunk App for Windows Infrastructure, the add-on collects Windows data and provides knowledge objects for the app. You should deploy the Splunk Add-on for Windows to:

- All hosts that run Active Directory Domain Services (including domain controllers and DNS servers).
- All Windows hosts from which you want Windows data.
- All indexers.
- All search heads.
- Basically, everywhere.

Download the Splunk Add-on for Windows v6.0.0 or later

1. Download the Splunk Add-on for Windows from Splunkbase and save it to an accessible place on the deployment server. You might need to sign in with your Splunk account before the download starts.
2. When prompted, choose an accessible location on your deployment server to save the download. Do not attempt to run the download.
3. Use an archive utility such as WinZip to unarchive the file to an accessible location.

Configure the Splunk Add-on for Windows v6.0.0 or later

Before the add-on can collect Windows data, you must configure it.

Microsoft Windows event logs that are rendered in XML format will not populate in the Splunk App for Windows Infrastructure

1. In the location where you unarchived the download file, locate the Splunk_TA_Windows directory.<
2. Inside this directory, make a subdirectory local.
3. Copy the inputs.conf file in the default subdirectory to the local directory.<
4. Open the inputs.conf in the local subdirectory with a text editor, such as Notepad.
5. Edit the disabled and mode attributes. Optionally, as shown below, add an index attribute to use specific indexes.
6. Save the `inputs.conf` file in the local subdirectory.

From version 5.0.1 onwards, Splunk Add-on for Windows collects data in multikv mode by default. This mode has a different event format over the existing single mode and the Splunk App for Windows Infrastructure app supports single mode only, so please change the value of `mode` parameter to `single` in the perfmon stanzas in `/Splunk_TA_Windows/default/inputs.conf` on forwarder.

```bash
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec
disabled = 0
instances = *
interval = 10
mode = single
object = Processor
useEnglishOnly=true

## Logical Disk
[perfmon://LogicalDisk]
counters = % Free Space; Free Megabytes; Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec
disabled = 0
instances = *
interval = 10
mode = single
object = LogicalDisk
useEnglishOnly=true

## Physical Disk
[perfmon://PhysicalDisk]
counters = Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec
disabled = 0
instances = *
interval = 10
mode = single
object = PhysicalDisk
useEnglishOnly=true

## Memory
[perfmon://Memory]
counters = Page Faults/sec; Available Bytes; Committed Bytes; Commit Limit; Write Copies/sec; Transition Faults/sec; Cache Faults/sec; Demand Zero Faults/sec; Pages/sec; Pages Input/sec; Page Reads/sec; Pages Output/sec; Pool Paged Bytes; Pool Nonpaged Bytes; Page Writes/sec; Pool Paged Allocs; Pool Nonpaged Allocs; Free System Page Table Entries; Cache Bytes; Cache Bytes Peak; Pool Paged Resident Bytes; System Code Total Bytes; System Code Resident Bytes; System Driver Total Bytes; System Driver Resident Bytes; System Cache Resident Bytes; % Committed Bytes In Use; Available MBytes; Available MBytes; Transition Pages RePurposed/sec; Free & Zero Page List Bytes; Modified Page List Bytes; Standby Cache Reserve Bytes; Standby Cache Normal Priority Bytes; Standby Cache Core Bytes; Long-Term Average StandBy Cache Lifetime (s)
disabled = 0
interval = 10
mode = single
object = Memory
```
## Network

```plaintext
[perfmon://Network]
counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets Sent/sec; Current Bandwidth; Bytes Received/sec; Packets Received Unicast/sec; Packets Received Non-Unicast/sec; Packets Received Discarded; Packets Received Errors; Packets Received Unknown; Bytes Sent/sec; Packets Sent Unicast/sec; Packets Sent Non-Unicast/sec; Packets Outbound Discarded; Packets Outbound Errors; Output Queue Length; Offloaded Connections; TCP Active RSC Connections; TCP RSC Coalesced Packets/sec; TCP RSC Exceptions/sec; TCP RSC Average Packet Size

disabled = 0
instances = *
interval = 10
mode = single
object = Network Interface
```

## Process

```plaintext
[perfmon://Process]
counters = % Processor Time; % User Time; % Privileged Time; Virtual Bytes Peak; Virtual Bytes; Page Faults/sec; Working Set; Page File Bytes Peak; Page File Bytes; Private Bytes; Thread Count; Priority Base; Elapsed Time; ID Process; Creating Process ID; Pool Paged Bytes; Pool Nonpaged Bytes; Handle Count; IO Read Operations/sec; IO Write Operations/sec; IO Data Operations/sec; IO Other Operations/sec; IO Read Bytes/sec; IO Write Bytes/sec; IO Data Bytes/sec; IO Other Bytes/sec; Working Set - Private

disabled = 0
instances = *
interval = 10
mode = single
object = Process
```

## ProcessInformation

```plaintext
[perfmon://ProcessorInformation]
counters = % Processor Time; Processor Frequency

disabled = 0
instances = *
interval = 10
mode = single
object = Processor Information
```

## System

```plaintext
[perfmon://System]
counters = File Read Operations/sec; File Write Operations/sec; File Control Operations/sec; File Read Bytes/sec; File Write Bytes/sec; File Control Bytes/sec; Context Switches/sec; System Calls/sec; File Data Operations/sec; System Up Time; Processor Queue Length; Processes; Threads; Alignment Fixups/sec; Exception Dispatches/sec; Floating Emulations/sec; % Registry Quota In Use

disabled = 0
instances = *
interval = 10
mode = single
object = System
```

## Processor

```plaintext
[perfmon://Processor]
object = Processor

counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec

instances = *
interval = 10
```
Outbound Bytes Compressed (Between Sites, After Compression)/sec; DS Client Binds/sec; DS Server Binds/sec; DS Client Name Translations/sec; DS Server Name Translations/sec; DS Security Descriptor Propagator Average Exclusion Time; DRA Outbound Objects Filtered/sec; DRA Outbound Values Total/sec; DRA Outbound Values (DNS only)/sec; AB ANR/sec; AB Property Reads/sec; AB Searches/sec; AB Matches/sec; AB Proxy Lookups/sec; ATQ Threads Total; ATQ Threads LDAP; ATQ Threads Other; DRA Inbound Bytes Total Since Boot; DRA Inbound Bytes Not Compressed (Within Site) Since Boot; DRA Inbound Bytes Compressed (Between Sites, Before Compression) Since Boot; DRA Inbound Bytes Compressed (Between Sites, After Compression) Since Boot; DRA Outbound Bytes Total Since Boot; DRA Outbound Bytes Not Compressed (Within Site) Since Boot; DRA Outbound Bytes Compressed (Between Sites, Before Compression) Since Boot; DRA Outbound Bytes Compressed (Between Sites, After Compression) Since Boot; LDAP New Connections/sec; LDAP Closed Connections/sec; LDAP New SSL Connections/sec; DRA Pending Replication Operations; DRA Threads Getting NC Changes; DRA Threads Getting NC Changes Holding Semaphore; DRA Inbound Link Value Updates Remaining in Packet; DRA Inbound Total Updates Remaining in Packet; DS % Writes from NTDSAPI; DS % Searches from NTDSAPI; DS % Reads from NTDSAPI; SAM Account Group Evaluation Latency; SAM Resource Group Evaluation Latency; ATQ Outstanding Queued Requests; ATQ Request Latency; ATQ Estimated Queue Delay; Tombstones Garbage Collected/sec; Phantoms Cleaned/sec; Link Values Cleaned/sec; Tombstones Visited/sec; Phantoms Visited/sec; NTLM Binds/sec; Negotiated Binds/sec; Digest Binds/sec; Simple Binds/sec; External Binds/sec; Fast Binds/sec; Base searches/sec; Subtree searches/sec; Onelevel searches/sec; Database adds/sec; Database modifies/sec; Database deletes/sec; Database recycles/sec; Approximate highest DNT; Transitive operations/sec; Transitive suboperations/sec; Transitive operations milliseconds run

interval = 10
disabled = 0
mode = single
useEnglishOnly=true
index = perfmon

[perfmon://DNS]
object = DNS
counters = Total Query Received; Total Query Received/sec; UDP Query Received; UDP Query Received/sec; TCP Query Received; TCP Query Received/sec; Total Response Sent; Total Response Sent/sec; UDP Response Sent/sec; TCP Response Sent; TCP Response Sent/sec; UDP Response Sent; UDP Recursive Queries; Recursive Queries/sec; Recursive Send TimeOuts; Recursive TimeOut/sec; Recursive Query Failure; Recursive Query Failure/sec; Notify Sent; Zone Transfer Request Received; Zone Transfer Request Received/sec; Zone Transfer Success; Zone Transfer Success/sec; AXFR Request Received; AXFR Request Received/sec; AXFR Request Sent; IXFR Request Received; IXFR Request Sent; IXFR Success Sent; IXFR Success Sent/sec; IXFR Request Sent; IXFR Request Received; IXFR Success Received; IXFR UDP Success Received; IXFR TCP Success Received; IXFR Reverse Lookup Received; IXFR Reverse Lookup Received/sec; IXFR Reverse Response Sent; IXFR Reverse Response Sent/sec; Dynamic Update Received; Dynamic Update Received/sec; Dynamic Update NoOperation; Dynamic Update NoOperation/sec; Dynamic Update Written to Database; Dynamic Update Written to Database/sec; Dynamic Update Rejected; Dynamic Update Rejected/sec; Dynamic Update TimeOuts; Dynamic Update TimeOuts/sec; Secure Update Received; Secure Update Received/sec; Secure Update Failure; Secure Update Failure/sec; Database Node Memory; Record Flow Memory; Caching Memory; UDP Message Memory; TCP Message Memory; Nbtstat Memory; Unmatched Responses Received

interval = 10
disabled = 0
mode = single
useEnglishOnly=true
index = perfmon

Note: If you do not complete the above step, then windows perfmon data will not be considered in dashboards.

- From version 5.0.1 onwards, Splunk Add-on for Windows has removed indexes so you have two options either you can use default windows index as mentioned in below table or you can create your own custom index. For the former one, you have to add index parameter with the values mentioned in below table in /Splunk_TA_Windows/default/inputs.conf on forwarder. As AD and DNS inputs are merged with TA-Windows those inputs are also mentioned in below table. User has to do the same for them also.

Table A

<table>
<thead>
<tr>
<th>Input Stanza</th>
<th>Indexes</th>
<th>Macro</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

36
Here are the few examples of input stanzas. Similarly, you can configure others.

```bash
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec
disabled = 0
instances = *
interval = 10
mode = single
object = Processor
useEnglishOnly=true
```
index = perfmon

[WinEventLog://Application]
disabled = 0
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
index = wineventlog

[WinPrintMon://port]
type = port
interval = 600
baseline = 1
disabled = 0
index = windows

[script://.\bin\runpowershell.cmd nt6-siteinfo.ps1]
source=Powershell
 sourcetype=MSAD:NT6:SiteInfo
interval=3600
disabled=0
index=msad

All the wineventlog inputs (Windows, AD, and DNS) will have renderXml=true (Xml Format) by default. Make it false for all WinEventLog Inputs as XML data is not supported.

[WinEventLog://Application]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false

[WinEventLog://Security]
disabled = 1
start_from = oldest
current_only = 0
evt_resolve_ad_obj = 1
checkpointInterval = 5
blacklist1 = EventCode="4662" Message="Object Type: (?\s*groupPolicyContainer)"
blacklist2 = EventCode="566" Message="Object Type: (?\s*groupPolicyContainer)"
renderXml=false

[WinEventLog://System]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false

[WinEventLog://ForwardedEvents]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
host=WinEventLogForwardHost

[WinEventLog://DFS Replication]
disabled = 1
renderXml=false
How to change the configuration files to handle custom indexes

**Update the following conf files for using custom index(es)**

**Update inputs.conf**

1. Copy the inputs.conf file from the default subdirectory `/Splunk_TA_Windows/default/` to the local directory folder `/Splunk_TA_Windows/local/` folder of forwarder.
2. Open the inputs.conf in the local subdirectory with a text editor, such as Notepad.
3. If you are using `<<CUSTOM INDEX>>` instead of TA_windows default indexes then add `index = <<CUSTOM INDEX>>` under stanzas as defined in the table (Table A) for TA_windows default index(es). Refer to the above table (Table A) for TA_windows default indexes.

Here are the few examples of inputs stanzas. Similarly, you can configure others.

```
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec
disabled = 1
instances = *
interval = 10
mode = single
object = Processor
useEnglishOnly=true
index = <<CUSTOM INDEX>>

[WinEventLog://Application]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
index = <<CUSTOM INDEX>>

[WinPrintMon://port]
type = port
interval = 600
baseline = 1
disabled = 1
index = <<CUSTOM INDEX>>
```
Update macros.conf

1. Copy the macros.conf file from the default subdirectory `~/splunk_app_windows_infrastructure/default/` to the `local` directory folder `~/splunk_app_windows_infrastructure/local/` folder on search head.
2. Open the macros.conf in the `local` subdirectory with a text editor, such as Notepad.
3. If you are using `<<CUSTOM_INDEX>>` instead of TA_windows default indexes then update the following macro definitions as shown below.

<table>
<thead>
<tr>
<th>Default Index</th>
<th>Custom Index</th>
<th>Updated Macro</th>
</tr>
</thead>
<tbody>
<tr>
<td>perfmon</td>
<td>&lt;&lt;CUSTOM_INDEX 1&gt;&gt;</td>
<td><code>[perfmon-index], definition = index=perfmon OR index=&lt;&lt;CUSTOM_INDEX 1&gt;&gt;</code></td>
</tr>
<tr>
<td>wineventlog</td>
<td>&lt;&lt;CUSTOM_INDEX 2&gt;&gt;</td>
<td><code>[wineventlog-index], definition = index=wineventlog OR index=&lt;&lt;CUSTOM_INDEX 2&gt;&gt;</code></td>
</tr>
<tr>
<td>windows</td>
<td>&lt;&lt;CUSTOM_INDEX 3&gt;&gt;</td>
<td><code>[windows-index], definition = index=windows OR index=&lt;&lt;CUSTOM_INDEX 3&gt;&gt;</code></td>
</tr>
<tr>
<td>msad</td>
<td>&lt;&lt;CUSTOM_INDEX 4&gt;&gt;</td>
<td><code>[msad-index], definition = index=msad OR index=&lt;&lt;CUSTOM_INDEX 4&gt;&gt;</code></td>
</tr>
</tbody>
</table>

Update authorize.conf

1. Copy the authorize.conf file in the default subdirectory `~/splunk_app_windows_infrastructure/default/` to the `local` directory folder `~/splunk_app_windows_infrastructure/local/` on Searchhead.
2. Open the authorize.conf in the `local` subdirectory with a text editor, such as Notepad.
3. Add those main(default) index(es) in authorize.conf under role_winfra-admin stanza against srchIndexesDefault parameter like shown below.

```
[role_exchange-admin] srchIndexesDefault = msad;msexchange;windows;perfmon;wineventlog;<<CUSTOM_INDEX 1>>;<<CUSTOM_INDEX 2>>;<<CUSTOM_INDEX 3>>;<<CUSTOM_INDEX 4>>;
```

Note: If no custom index or default TA_windows indexes are defined then all data will be stored in main index.

Update the following conf files for using main index

Update macros.conf

1. Copy the macros.conf file from the default subdirectory `~/splunk_app_windows_infrastructure/default/` to the `local` directory folder `~/splunk_app_windows_infrastructure/local/` folder on search head.
2. Open the macros.conf in the `local` subdirectory with a text editor, such as Notepad.
3. If you are using index=main instead of TA_windows default indexes then update the following macro definitions as shown below.

<table>
<thead>
<tr>
<th>Default Index</th>
<th>Main Index</th>
<th>Updated Macro</th>
</tr>
</thead>
<tbody>
<tr>
<td>msad</td>
<td></td>
<td><code>[msad-index], definition = index=msad OR index=&lt;&lt;CUSTOM_INDEX 4&gt;&gt;</code></td>
</tr>
<tr>
<td>Index</td>
<td>Main</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>perfmon</td>
<td>main</td>
<td>[perfmon-index], definition = index-perfmon OR index-main</td>
</tr>
<tr>
<td>wineventlog</td>
<td>main</td>
<td>[wineventlog-index], definition = index-wineventlog OR index-main</td>
</tr>
<tr>
<td>windows</td>
<td>main</td>
<td>[windows-index], definition = index-windows OR index-main</td>
</tr>
<tr>
<td>msad</td>
<td>main</td>
<td>[msad-index], definition = index-msad OR index-main</td>
</tr>
</tbody>
</table>

**Update authorize.conf**

1. Copy the authorize.conf file in the default subdirectory `/splunk_app_windows_infrastructure/default/` to the local directory folder `/splunk_app_windows_infrastructure/local/` on Searchhead.
2. Open the authorize.conf in the local subdirectory with a text editor, such as Notepad.
3. Add those main(default) index(es) in authorize.conf under role_winfra-admin stanza against srchIndexesDefault parameter like shown below.

```
[role_winfra-admin]
srchIndexesDefault = msad;msexchange;windows;perfmon;wineventlog;default
```

**Note:** If you skip this step, your Splunk platform will not have the index configurations which can result into data loss.

**What's next?**

You have downloaded and configured the Splunk Add-on for Windows.

Next, you will deploy it to the deployment clients. Once they receive the add-on, they will use the configuration in the “send to indexer” app to send Windows data to the indexer.
Get Active Directory data

Configure Active Directory audit policy

This topic discusses changing the Active Directory audit policy to allow the domain controllers in your Active Directory to generate the needed events and logs for the Splunk App for Windows Infrastructure.

Active Directory audit policy

By default, Active Directory does not automatically audit certain security events. You must enable auditing of these events so that your domain controllers log them into the Security event log channel.

You do this by creating a Group Policy object (GPO) and deploying that GPO to all domain controllers (DCs) in your AD environment. Once you activate the GPO, your DCs log these security events into the Security event log.

Then, you install universal forwarders (as deployment clients) to the domain controllers and deploy the appropriate Active Directory add-ons into those clients. They collect the logs and forward them to the central Splunk App for Windows Infrastructure indexers.

This topic shows you how to create individual Group Policy objects (GPOs) for both sets of settings. If you wish, you can combine both the PowerShell and audit settings into a single GPO. For ease of administration, you should create and deploy these GPOs separately from other GPOs.

Important information on security event auditing and indexing volume

When you enable auditing of the Security Event Log on your domain controllers, the DCs generate a lot of data. These events significantly increase indexing volume and might cause indexing license violations. You might also see decreased performance on your domain controllers based on how much additional data the servers generate.

If you are concerned about the impact that enabling security event auditing might have on your indexing volume, you can tweak policy settings to generate only the data that is important to you. Refer to the table below to learn about which policy settings generate which event types, and how the Splunk App for Windows Infrastructure uses those events to populate its dashboards, reports and lookups.

If you choose to disable certain policy settings in an effort to curb indexing volume, you directly affect how much data gets sent to the Splunk App for Windows Infrastructure. The table below lists what data you do not collect if you decide not to enable a particular policy setting. This is not an all-inclusive list - the app correlates some lookups across various policy settings, as multiple events often derive a single knowledge object. Failure to enable all of the policy settings might cause the Splunk App for Windows Infrastructure to display incomplete or incorrect knowledge objects in its dashboards and reports.

<table>
<thead>
<tr>
<th>Policy setting:</th>
<th>Required?</th>
<th>What the Splunk App for Windows Infrastructure uses it for:</th>
</tr>
</thead>
</table>
| Audit Account Logon Events | Yes | Administrator Audit dashboards  
Security->Logon dashboards  
Security->Reports->New (Computer or Domain) Accounts  
Session ID-to-User (tSessions) lookup  
Computer-to-IP Address (tHostinfo) lookup |
Policy setting: | Required? | What the Splunk App for Windows Infrastructure uses it for:
---|---|---
Audit Account Management | No | Administrator Audit dashboards
| | Change Management dashboards
Audit Logon Events | No | Administrator Audit dashboards
| | Logon and access information
Audit Object Access | No | Administrator Audit dashboards
| | Information on who changed a GPO and when
Audit Policy Change | No | Security->Reports->Group Policy Reports
| | GPO Change Management dashboard
Audit System Events | No | Directory Services replication events

**Advanced Audit Policy settings**

You might alternatively want to use the Advanced Audit Policy (AAP) configuration settings to control which events your domain controllers send to the Splunk App for Windows Infrastructure. While Splunk supports this method, it is outside the scope of this document to list all available AAP configuration options.

This is because of the number of available AAP configuration options and the fact that those options change with different Windows versions - for example, the options for the Windows Server 2008 family differ from those in the Windows Server 2012 families. Windows Vista and other workstation-class versions of Windows do not support AAP.

If you need more granularity in the types of audit events you want generated, you can review *eventtypes.conf* (located in the Splunk App for Windows Infrastructure installation at `%SPLUNK_HOME%/etc/apps/splunk_app_windows_infrastructure/default`) for the event codes that the app looks for. With that information, you can create a GPO that enables AAP and generates audit events for only those specific event codes.

**Note:** When you enable AAP, Windows disables configurations for standard Audit Policy.


**Create a new GPO**

1. From the Windows Start menu, click **Start > Administrative Tools > Group Policy Management.**
2. In the left pane, under “Group Policy Management,” expand the forest and domain for which you want to set group policy.
3. Right-click **Group Policy objects** and select **New.**
4. In the dialog window that opens, enter a unique name for your new GPO that you will remember in the **Name** field, and select **None** for the **Source Starter GPO** field.

**Edit the GPO to change audit policy**

1. Open the GPO for editing by right-clicking the newly created GPO In the Group Policy Objects window and selecting **Edit.**
2. In the GPO editor, select **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policy > Audit Policy.**
3. Enable both **Success** and **Failure** auditing of the following policy settings:
   - Audit account logon events
♦ Audit account management
♦ Audit directory service access
♦ Audit logon events
♦ Audit object access
♦ Audit policy change
♦ Audit privilege use
♦ Audit system events

4. Close the Group Policy Object Editor window to save your changes.
5. For windows server 2008, you can verify audit policy is applied or not from the steps mentioned in Security auditing settings are not applied to Windows Vista-based and Windows Server 2008-based computers when you deploy a domain-based policy.

Deploy the GPO

1. In Group Policy Management, in the left pane of the window, right-click on the Domain Controllers item and click Link an existing GPO..."
2. In the window that appears, select the GPO you created.
3. Click OK. The GPMC refreshes to show that your GPO is now linked to the Domain Controllers organizational unit.

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

The Splunk Add-on for Microsoft Active Directory is available on Splunkbase. When you download and deploy the add-ons to domain controllers, the add-ons collect Active Directory data and send it to Splunk App for Windows Infrastructure indexers.

To users who are using TA-windows version 6.0.0 or later: TA-AD has merged with TA-windows. See Download and configure the Splunk Add-on for Windows version 6.0.0 or later.

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.

More information about the Active Directory add-ons

The following table lists details about the Active Directory add-on.

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Description</th>
</tr>
</thead>
</table>

Download the Splunk Add-on for Microsoft Active Directory

The Splunk Add-ons for Microsoft Active Directory is available on Splunkbase.

Download the add-on package and save it to an accessible place on the deployment server:

1. In a web browser, proceed to the Splunk Add-on for Active Directory download page.
2. Click the download link to begin the download process. You might need to sign in with your Splunk account before the download starts.
3. When prompted, choose an accessible location on your deployment server to save the download. Do not attempt to run the download.
4. Use an archive utility such as WinZip to unarchive the file to an accessible location.

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

The Splunk Add-on for Microsoft Active Directory do not require any configuration edits by default. When you deploy them onto Active Directory domain controllers, they immediately begin collecting data as long as you have configured audit policy.

**Next steps**

You have downloaded the Splunk Add-on for Microsoft Active Directory. The next step involves deploying those add-ons into the universal forwarders that you install on your Active Directory domain controllers.

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

Deploy the Splunk Add-on for Microsoft Active Directory if you’re using TA_windows version 5.0.1. The deployment server (the Splunk Enterprise instance that manages and updates configurations and apps for universal forwarders in a Splunk Enterprise deployment) must be made aware of the Splunk Add-on for Microsoft Active Directory before you can deploy it to deployment clients.

This means that, during this part of the setup, you will define new deployment classes at the deployment server to account for these differences.

To users who are using TA-windows v6.0.0: TA-AD has merged with TA-windows. See Download and configure the Splunk Add-on for Windows version 6.0.0 or later.

If you’re using Splunk_TA_windows version 6.0.0 or later, you don’t need Splunk_TA_microsoft_ad or Splunk_TA_microsoft_dns. Splunk_TA_microsoft_ad and Splunk_TA_microsoft_dns are merged with Splunk_TA_windows in version 6.0.0.

**Best practice: Only deploy the Splunk Add-on for Microsoft Active Directory to a select group of domain controllers**

Consider the number of domain controllers that you deploy the Active Directory add-ons. Best practice recommends that only one domain controller in an Active Directory domain or forest receives the add-on, with one or two others receiving it as a backup.

**Place the Splunk Add-on for Microsoft Active Directory in the deployment apps directory on the deployment server.**

1. Open a command prompt on the deployment server/indexer.
2. Copy the add-on folder from their current location to the deployment apps directory:

   > Copy-Item -Path C:\Downloads\Splunk_TA_microsoft_ad -Destination "C:\Program Files\Splunk\etc\deployment-apps -Recurse -Force

3. Reload the deployment server configuration.

   > cd \Program Files\Splunk\bin
   > .\splunk reload deploy-server

4. From a web browser, log into Splunk Enterprise on the deployment server.
5. In the system bar, select **Settings > Forwarder Management**.
6. Click the **Apps** tab. The Splunk_TA_microsoft_ad* add-ons should appear in the list of apps.

**Define a new server class for domain controllers**

In this procedure, you will define a new server class for Windows Server 2008 domain controllers. In this server class, you will deploy the Splunk_TA_microsoft_ad add-on. Later, you will assign this server class to a universal forwarder that runs atop a host that runs Windows Server 2008.

1. In the "Splunk_TA_microsoft_ad" add-on entry in the list, click **Edit**. Splunk Enterprise loads the "Edit App: Splunk_TA_microsoft_ad" page.
2. Under "Server Classes", click +.
3. In the pop-up that appears, click **New Server Class**.
4. In the "New Server Class" dialog box that pops up, enter "Domain Controllers".

   **Note:** You can enter a unique name for the server class that describes the hosts that belong in the class, and that you will remember.

5. Click **Save**. Splunk Enterprise saves the class and loads the information page for the server class you just created.

   **Note:** The page indicates that you have not added any apps or clients yet. This is okay, as you have just created the class.

6. Click **Add apps**. Splunk Enterprise loads the **Edit Apps** page.
7. Locate and click the "Splunk_TA_microsoft_ad" add-on in the **Unselected Apps** pane on the left. The app moves to the "Selected Apps" pane on the right.
8. Click **Save**. Splunk Enterprise saves the configuration and returns you to the server class information page.

**Add domain controller clients to the server class**

If you have not installed a universal forwarder on a Windows domain controller, do so now. See "Install a universal forwarder on each Windows host".

1. In the server class information page, click **Add clients**. Splunk Enterprise loads the "Edit clients" page.
2. In the "Include (whitelist)" field, enter the host name of the domain controller.
3. Click **Preview**. Splunk Enterprise updates the host list at the bottom and places check marks on the hosts that match what you entered in the "Include (whitelist)" field.
4. Click **Save**. Splunk Enterprise adds the host to the server class and deploys the add-on to the deployment client on the Active Directory host.

**Add domain controller clients to the "universal forwarder" server class**

In the same way that you added the domain controller deployment client to the "domain controllers" server class to deploy the Active Directory add-on, add the client to the "universal forwarder" server class. This does two things:

- Deploys the Splunk Add-on for Windows to the domain controller, which lets the client collect Windows data from the domain controller.
- Deploys the "send to indexer" app to the domain controller, which lets the client forward Windows and Active Directory data to the Splunk App for Windows Infrastructure indexer.

To add the domain controller to the "universal forwarders" server class, see "Add the universal forwarder to the server class."
Next steps

You have now deployed the Active Directory add-on onto your domain controller deployment client. In the future, you can use this procedure to deploy the add-on(s) to additional client(s).

Next, you will confirm that Active Directory data arrives at the indexer.

Confirm and troubleshoot AD data collection

This topic discusses how to confirm and troubleshoot data collection from the Splunk Add-on for Microsoft Active Directory.

To users who are using TA-windows v6.0.0: TA-AD has merged with TA-windows. See Download and configure the Splunk Add-on for Windows version 6.0.0 or later.

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.

Check the indexer for data

After you configure and deploy the Splunk Add-on for Microsoft Active Directory into your domain controller deployment client, you should check the deployment server to see that data has arrived. The fastest way to do that is to load the Search and Reporting app and view the Data Summary:

1. In the system bar, click Apps > Search & Reporting. Splunk Enterprise loads the Search & Reporting app.
2. Click Data Summary. Splunk brings up the data summary page with the "Hosts" tab active.
3. Scan through the list of host names for the name of your domain controller deployment client.
   * If you do not see the deployment client host name, then there is a problem occurring between the client at the indexer. Confirm that:
     ◊ You have properly configured receiving on the indexer.
     ◊ You have properly configured the "send to indexer" app to forward data to the indexer.
     ◊ No network issue exists between the deployment client and the indexer.
4. Click the host name in the list. A search window appears and displays all events associated with the deployment client host name.
5. Search through the data to see that all of the events you configured in the Splunk Add-on for Microsoft Active Directory have been sent to the indexer. See Sample Active Directory searches and dashboards.

   • If you do not see the events you expect, try these steps:
     ◆ Confirm that you have placed the add-on in the deployment apps directory and reloaded the deployment server.
     ◆ Confirm that the deployment client does not have errors attempting to collect the data.
     ◆ More troubleshooting steps are available in the Splunk Troubleshooting manual.

What's next?

You have configured and deployed the Splunk Add-on for Microsoft Active Directory to your domain controller deployment clients. This now means that Active Directory data is present on your Splunk App for Windows Infrastructure indexer.

The next step is to get DNS data onto the indexer.
Sample searches and dashboards

This topic lists searches that you can perform to confirm that Windows data has arrived at the indexer.

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.

Search Active Directory data

To confirm that Active Directory data is present on the indexer, use the Search app:

1. Log into Splunk Enterprise on the indexer, if you have not already.
2. Load the Search app. In the system bar, select Apps > Search & Reporting. Splunk loads the Search app.
3. Try the following searches to confirm that data is present:

   This search confirms that the Splunk Add-on for Microsoft Active Directory is sending data to the indexer:

   ```
   index=msad earliest=1h
   ```

   This search confirms that the Splunk Add-on for Microsoft Active Directory has been installed properly on the deployment client named `<host_name>`:

   ```
   index=msad host=<host_name> earliest=1h
   ```

Can’t find the data?

Try the following:

- Use Forwarder Management to confirm that the Splunk Add-on for Microsoft Active Directory has been deployed to your deployment clients.
- Refer to the Troubleshooting manual for additional help.
Get Domain Name Service (DNS) data

Configure Windows Domain Name Server

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.

Enable DNS debug logging

If you want detailed DNS server statistics, enable debug logging on your DNS servers by following the instructions for your operating system:

- For Windows Server 2008 R2 or later, see Select and enable debug logging options on the DNS server on MS TechNet. This procedure works for Windows Server 2008 R2 or later even though the article shows that it is for Windows Server 2003 family operating systems, as the procedure is the same.

Impact of DNS debug logging on performance and license usage

When you enable debug logging on your DNS servers, you must consider the following caveats:

- If you enable DNS server debug logging, individual DNS server performance decreases significantly.

- Debug logging generates significant amounts of data that might exhaust disk space on your DNS servers, which can potentially cause downtime. You must watch and rotate your DNS server logs to prevent disk capacity issues from occurring.

- Debug logging also greatly increases the overall amount of data indexed by the Splunk App for Windows Infrastructure. Ensure that you have a Splunk license that can accommodate the additional indexing volume.

What's next?

You have configured the Windows DNS servers for debug logging. Next, you will install a universal forwarder on the DNS server and then deploy the Splunk Add-on for Windows DNS onto the client.

Download and configure the Splunk Add-on for Windows DNS

Note: To users who are using TA-windows version 6.0.0 or later: TA-AD has merged with TA-windows. See Download and configure the Splunk Add-on for Windows version 6.0.0 or later.

This topic discusses how to download and configure the Splunk Add-on for Windows DNS and deploy them to your deployment clients so that they forward DNS information to the Splunk App for Windows Infrastructure indexer.

The Splunk Add-on for Windows DNS collects DNS data and is available on Splunkbase. When you install the add-on into universal forwarders on your DNS servers, the add-on collects DNS data and sends it to the Splunk App for Windows Infrastructure.
More information about the DNS add-on

The following table lists details about the Splunk Add-on for Windows DNS.

<table>
<thead>
<tr>
<th>Add-on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk_TA_microsoft_dns</td>
<td>For DNS servers that run Windows Server 2008/2008 R2 and later</td>
</tr>
</tbody>
</table>

Download the Splunk Add-on for Windows DNS

Like the Splunk Add-on for Microsoft Active Directory, the Splunk Add-on for Windows DNS is available on Splunkbase. Make sure you download the latest version of the app. You might need to sign in with your Splunk account before the download starts.

1. In a web browser, proceed to the Splunk Add-on for Windows DNS download page.
2. Click the download link to begin the download process.
3. When prompted, choose an accessible location on your deployment server to save the download. Do not attempt to run the download.
4. Use an archive utility such as WinZip to unarchive the file to an accessible location, such as the `C:\Program Files\SplunkUniversalForwarder\etc\apps` directory.

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.

Configure the Splunk Add-ons for Windows DNS

The Splunk Add-on for Windows DNS does not require configuration by default. When you install it onto DNS servers, it immediately begins collecting data as long as you have configured DNS debug logging.

What's next?

You have downloaded the Splunk App for Windows Infrastructure and can now access the Splunk Add-ons for Windows DNS. The next step involves deploying those add-ons into the universal forwarders that you install on your Active Directory DNS servers.

Confirm and troubleshoot DNS data collection

Note: To users who are using TA-windows version 6.0.0 or later: TA-AD has merged with TA-windows. See Download and configure the Splunk Add-on for Windows version 6.0.0 or later.

Check the indexer for data

After you configure and deploy the Splunk Add-on for Windows DNS into your DNS server, check the deployment server to see that data has arrived by loading the Search and Reporting app and view the Data Summary.

For an example of searches to use to confirm ingestion of Splunk Sample DNS searches and dashboards.

1. In the system bar, click Apps > Search & Reporting. Splunk Enterprise loads the Search & Reporting app.
2. Click Data Summary. Splunk brings up the data summary page with the "Hosts" tab active.
3. Scan through the list of host names for the name of your DNS server.

If you do not see the deployment client host name, then there is a problem occurring between the client at the indexer. Confirm that:

- You have properly configured receiving on the indexer.
- You have properly configured the "send to indexer" app to forward data to the indexer.
- No network issue exists between the deployment client and the indexer.

4. Click the host name in the list. Splunk Enterprise brings up a search window that displays all events associated with the deployment client host name.

5. Search through the data to see that all of the events you configured in the Splunk Add-on for Windows DNS have been sent to the indexer.

If you do not see the events you expect, try these steps:

- Confirm that you have placed the add-on in the deployment apps directory and reloaded the deployment server.
- Confirm that the deployment client does not have errors attempting to collect the data.
- More troubleshooting steps are available in the Splunk Troubleshooting manual.

What's next?

You have configured and deployed the Splunk Add-on for Windows DNS to your domain controller deployment clients. This now means that Active Directory data is present on the indexer. This is the last piece of the data puzzle.

The next step is to complete setup by finishing a few more required tasks.

Sample DNS searches and dashboards

This topic lists searches that you can perform to confirm that Windows DNS data has arrived at the indexer.

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.

Search Windows DNS data

To confirm that Windows DNS data is present on the indexer, use the Search app:

1. Log into Splunk Enterprise on the indexer, if you have not already.
2. Load the Search app. In the system bar, select Apps > Search & Reporting. Splunk loads the Search app.
3. Try the following searches to confirm that data is present:

   ```
   eventtype=perfmon-dns
   ```

Can't find the data?

Try the following:

- Use Forwarder Management to confirm that the Splunk Add-on for Windows DNS have been deployed to your deployment clients.
• Refer to the Troubleshooting manual for additional help.
Deploy the Splunk App for Windows Infrastructure

Install the Splunk App for Windows Infrastructure on the Search Head

The Splunk App for Windows Infrastructure lets you view all of the data that you have collected during the setup process. This topic discusses installing the app as well as some required add-ons (described in detail) that complete the process and allow you to use the app.

Final setup phase

If you have followed the instructions in this manual, then by completing the procedures in this topic, you will complete the setup phase for the app.

The final tasks for setup are:

- Install the Splunk Add-on for Windows on the search head.
- Install the Splunk Supporting Add-on for Active Directory on the search head.
- Install the Splunk App for Windows Infrastructure on the search head.

In this procedure, you will install all of these components on the same server you installed in the basic infrastructure step.

Where is the search head?

In this manual, the search head is the indexer that you first set up. All Splunk Enterprise instances have an inherent capability of being a search head when they hold indexed data.

When you scale the Splunk App for Windows Infrastructure, the search head is on a separate host from the indexer. See Size a Splunk App for Windows Infrastructure deployment.

Install the Splunk Add-on for Windows

As part of getting Windows data into the instance, you have already installed the Splunk Add-on for Windows. To activate the Splunk Add-on for Windows for the Splunk App for Windows Infrastructure, copy the add-on from either the location where you saved the download or the deployment apps directory to the Splunk apps directory:

```
> Copy-Item -Path C:\Program Files\Splunk\etc\deployment-apps\Splunk_TA_windows -Destination C:\Program Files\Splunk\etc\apps -Recurse -Force
```

Install the Splunk Supporting Add-on for Active Directory (SA-ldapsearch)

Next, install and configure the Splunk Supporting Add-on for Active Directory in the Splunk apps directory:

1. In a web browser, proceed to the Splunk Supporting Add-on for Active Directory download page.
2. Click the download link to begin the download process.
   ♦ Make sure you download the latest version of the add-on.
   ♦ You might need to sign in with your Splunk account before the download starts.
3. When prompted, choose an accessible location on your deployment server to save the download. Do not attempt to run the download.
4. Use an archive utility such as WinZip or tar to unarchive the file to the Splunk apps directory.
5. The Splunk Supporting Add-on for Active Directory (SA-ldapsearch) must be configured properly and reside on all search heads in the deployment. See Configure the Splunk Supporting Add-on for Active Directory.

Install the Splunk App for Windows Infrastructure

The final piece of software to install is the Splunk App for Windows Infrastructure itself.

As part of getting Active Directory data into the instance, you have already downloaded the Splunk App for Windows Infrastructure. To activate the app:

1. Copy it from the location you saved the download previously to the Splunk apps directory:

   ```bash
   > Copy-Item -Path C:\Downloads\splunk_app_windows_infrastructure -Destination C:\Program Files\Splunk\etc\apps -Recurse -Force
   ```

2. Restart Splunk Enterprise on each machine in the instance.
3. Log back in to Splunk Enterprise.

Add the "winfra-admin" role to the user that will run the app on the search head

To use the Splunk App for Windows Infrastructure, the winfra-admin role must be present. The Splunk App for Windows Infrastructure provides this role, but you must assign it to the user that will run the app.

1. Log into Splunk Enterprise on the deployer.
2. In the system bar, click Settings > Access controls.
3. Click Users.
4. Click the user that will run the application. Splunk Enterprise displays the information page for the user.
5. In the Assign to roles section, in the Available roles column, click winfra-admin role. The role moves from the "Available roles" to the Selected roles column. Note: If you do not see the winfra-admin role in the list, make sure that you have installed the application, as described in "Install the Splunk App for Windows Infrastructure on the deployer".
6. Click Save. Splunk Enterprise assigns the role to the user you selected.

What's next?

You have completed setup of the Splunk App for Windows Infrastructure.

Now, you can log into Splunk Enterprise and complete the first-time setup experience.

Install the Splunk App for Windows Infrastructure on a search head cluster

The Splunk App for Windows Infrastructure can be installed in a search head cluster. The procedure to install the app on a search head cluster is different than performing it on a stand-alone search head.

This topic contains basic instructions on how to install and configure the Splunk App for Windows Infrastructure on a search head cluster. To learn more about how to install and configure search head clusters, see "Deploy a search head cluster" in the Distributed Search manual.

The final tasks for setup of the Splunk App for Windows Infrastructure are:

- Configure a search head cluster, including a separate instance for a search head cluster deployer.
• Install the Splunk Add-on for Windows version 5.0.1 or 6.0.0 on the search head cluster.
• Install the Splunk Supporting Add-on for Active Directory on the search head cluster.
• Install the Splunk App for Windows Infrastructure on the search head cluster.

  ♦ Check authorize.conf and macros.conf /splunk_app_microsoft_exchange/default/ on deployer and make sure all changes are done as per Download and configure the Splunk Add-on for Windows.
• Run the first time setup on the search head cluster.
• Add the winfra-admin role to the search head cluster members.
• Build lookups on a search head cluster member.

**Configure the search head cluster**

To install the Splunk App for Windows Infrastructure on a search head cluster, you must have a cluster configured.

When you designate hosts for a search head cluster, always install new instances of Splunk Enterprise. If you attempt to add an existing instance to a search head cluster, the process overwrites any configurations or apps that reside on the instance.

Also, designate a separate host as a search head cluster deployer.

To configure a search head cluster, see Deploy a search head cluster" in the Distributed Search manual.

**Install the Splunk Add-on for Windows on the deployer**

Install the Splunk Add-on for Windows version 5.0.1 or 6.0.0 onto the search head cluster deployer instance.

1. In a web browser, navigate to the Splunk Add-on for Windows download page.
2. Change the version to 5.0.1 or 6.0.0, and click the download link to start the download.
   ♦ Make sure you download the Splunk Add-on for Windows version 5.0.1 or 6.0.0. The Splunk Add-on for Windows version 5.0.0 is not compatible with the Splunk App for Windows Infrastructure.
   ♦ You might need to sign in with your Splunk account before the download starts.
3. When prompted, choose an accessible location on your deployer to save the download. Do not attempt to run the download.
4. Use an archive utility such as WinZip or tar to unarchive the file to the %SPLUNK_HOME%/etc/apps directory on the deployer.

**Install the Splunk Supporting Add-on for Active Directory (SA-ldapsearch) on the deployer**

Next, install the Splunk Supporting Add-on for Active Directory on the deployer:

1. In a web browser, proceed to the Splunk Supporting Add-on for Active Directory download page.
2. Click the download link to start the download.
   ♦ Make sure you download the latest version of the add-on.
   ♦ You might need to sign in with your Splunk account before the download starts.
3. When prompted, choose an accessible location on your deployer to save the download. Do not attempt to run the download.
4. Use an archive utility such as WinZip or tar to unarchive the file to the %SPLUNK_HOME%/etc/apps directory on the deployer.
Install the Splunk App for Windows Infrastructure on the deployer

Next, install is the Splunk App for Windows Infrastructure on the deployer.

1. Download the Splunk App for Windows Infrastructure if you have not already.
2. Use an archive utility such as WinZip or tar to unarchive the file to %SPLUNK_HOME%/etc/apps on the deployer.
3. Restart Splunk Enterprise on the deployer.

Add the "winfra-admin" role to the user that will run the app on the deployer

To run the first-time setup on the search head cluster deployer instance, the winfra-admin role must be present. The Splunk App for Windows Infrastructure provides this role, but you must assign it to the user that will run the app so that the first-time run experience works.

1. Log into Splunk Enterprise on the deployer.
2. In the system bar, click Settings > Access controls.
3. Click Users.
4. Click the user that will run the application. Splunk Enterprise displays the information page for the user.
5. In the Assign to roles section, in the Available roles column, click winfra-admin role. The role moves from the "Available roles" to the Selected roles column. Note: If you do not see the winfra-admin role in the list, make sure that you have installed the application, as described in "Install the Splunk App for Windows Infrastructure on the deployer".
6. Click Save. Splunk Enterprise assigns the role to the user you selected.

Add search peers with Windows data to the deployer

Before the first time setup experience can complete, you must add at least one search peer (indexer) with Windows data.

If you followed the instructions in this manual, then you already have an indexer with Windows data. Configure this host as a search peer to the deployer.

If you have not collected Windows data yet, then follow the setup chapters in this manual to get this data before continuing:

- Set up basic infrastructure
- Get Windows data
- (Optional) Get Active Directory data
- (Optional) Get Domain Name Service (DNS) data

To configure a search peer:

1. From the deployer, log into Splunk Enterprise.
2. Click Settings > Distributed search.
3. In the Actions column, next to Search peers, click Add new.
4. In the Peer field, enter the host name or IP address and management port number of the search peer (indexer) that contains the Windows data. For example, if the host name is idx1.mycompany.com, enter idx1.mycompany.com:8089. If the management port is not the default, use the port number that you configured.
5. In the Remote username field, enter the user that the deployer should use to authenticate into the search peer. This user must be an existing user on the search peer, and must have the 'admin' role.
6. In the Remote password field, enter the password for the user that the deployer should supply to the search peer when it connects.
7. In the Confirm password field, re-enter the password you used in the previous step.
8. Click Save. The deployer saves the configuration and authenticates into the search peer.
9. Restart Splunk Enterprise on the deployer.

Run the first-time setup experience on the deployer

Log into Splunk Enterprise and start the first-time setup experience.

1. On the deployer, log into Splunk Enterprise.
2. Open the Splunk App for Windows Infrastructure. From the system bar, click Apps > Splunk App for Windows Infrastructure.
3. Follow the prompts and confirm that you have all the data that the app needs.
4. (Optional) After the first-time setup completes, remove the search peers from the deployer.

Distribute the app, add-ons, and configurations to the other search head cluster members

Push the configuration bundle from the search head cluster deployer to one search head member.

1. From a command or shell prompt on the deployer, copy the app, add-ons, and configurations to the search head cluster apps directory:

```
Copy-Item -Path C:\Program Files\Splunk\etc\apps\Splunk_TA_windows -Destination C:\Program
Files\Splunk\etc\shcluster\apps -Recurse -Force
Copy-Item -Path C:\Program Files\Splunk\etc\apps\SA_LDAPsearch -Destination C:\Program
Files\Splunk\etc\shcluster\apps -Recurse -Force
Copy-Item -Path C:\Program Files\Splunk\etc\apps\splunk_app_windows_infrastructure -Destination
C:\Program Files\Splunk\etc\shcluster\apps -Recurse -Force
```
2. From a command or shell prompt on the deployer, push the app, add-ons, and configurations to one search head cluster member:

```
splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>
```

In this command:

* -target specifies the URI and management port of one of the search head cluster members. For example, if one of the members is splunk2.mycompany.com, you would specify https://splunk2.mycompany.com:8089.

3. The deployer displays the following message:

```
Warning: Depending on the configuration changes being pushed, this command might initiate a rolling-restart of the cluster members. Please refer to the documentation for the details. Do you wish to continue? [y/n]:
Proceed by responding to the message with y.
```
4. Wait for the deployer to send the configuration bundle to the search head cluster members.

On Splunk Enterprise 6.3 and earlier only, add roles to all search head cluster members

If you run an on-premises version of Splunk Enterprise of 6.3 or earlier, you must manually add the winfra-admin role to the user that runs the app on the other search head cluster members. This is because those versions do not handle replication of user roles across search head cluster members automatically.

You do not need to perform this procedure if you run Splunk Cloud.

1. Log into Splunk Enterprise on a search head cluster member.
2. In the system bar, click Settings > Access controls.
3. Click Users.
4. Click the user that will run the application. Splunk Enterprise displays the information page for the user.
5. In the Assign to roles section, in the Available roles column, click winfra-admin role. The role moves from the "Available roles" to the Selected roles column. Note: If you do not see the winfra-admin role in the list, make sure that you have distributed the apps and configurations as described in "Distribute the app, add-ons, and configurations to the other search head cluster members".
6. Click Save. Splunk Enterprise assigns the role to the user you selected.
7. Repeat this process on all the other search head cluster members.

Build lookups on one search head cluster member

To complete setup of the app, build lookups for the app on one search head cluster member.

1. Log into Splunk Enterprise on a search head cluster member.
2. Open the Splunk App for Windows Infrastructure. In the system bar, select Apps > Splunk App for Windows Infrastructure.
3. In the menu bar, select Tools and Settings > Build lookups.
4. Wait for the lookup build process to complete.
5. Once the build completes, click Finish and go back.

You can now use the Splunk App for Windows Infrastructure. Visit the Reference manual for information on how to use the app dashboards.

Install the Splunk App for Windows Infrastructure using self service installation on Splunk Cloud

1. Click on the Manage Apps button.
2. Under the **App Management** menu, click the **Install App** button. The **Browse More Apps** menu appears.
3. Search for the Splunk App for Windows Infrastructure, and click the **Install** button. **Note:** Not all apps are available to be installed using self service installation.
4. A Confirmation box appears. Review and click **Continue**.
5. Enter your Splunk.com login credentials, read and accept the login disclaimer, and click the **Login and Download** button.
6. (Optional) If the **App Installation Failed** window appears, review the apps or add-ons that are listed as app dependencies, review and accept the terms and conditions of the license(s), and click **Install** to install the app dependencies for the Splunk App for Windows Infrastructure. Once deployed, your Splunk Cloud instance will restart.

![](image1.png)

7. Log back into your Splunk Cloud deployment. A **Complete** window appears to show successful installation of the Splunk App for Windows Infrastructure.

![](image2.png)

8. Review the **Complete** window for release notes and source package review, and click the **View Apps** button.

9. On the **App Management** page, review the installed apps.
Upgrade the Splunk App for Windows Infrastructure

How to upgrade the Splunk App for Windows Infrastructure

The commands shown in this topic are PowerShell. If you use *nix, substitute the PowerShell directives with their *nix counterparts. If you use different directories for Splunk Enterprise and deployment server, substitute the directories shown with your specific directories.

The search head is the Splunk Enterprise instance that runs the Splunk App for Windows Infrastructure and shows all of the app data. These upgrade instructions should be performed on any host that has been designated as a search head in your deployment.

1. In case of standalone search head, remove the existing default.xml file from the local folder etc/apps/splunk_app_windows_infrastructure/local/data/ui/nav on the search head.
2. (Optional) Backup local changes (local folder) created on the search head and search head deployer.
3. Put the new Splunk App for Windows Infrastructure in the etc/shcluster/apps/ directory on your search head deployer. If you have a single search head, put the new Splunk App for Windows Infrastructure in etc/apps/.
4. Remove windows_apps.csv from the app:
   - Remove windows_apps.csv lookup if available from etc/shcluster/apps/splunk_app_windows_infrastructure/lookups on the search head deployer. In case of standalone search head, remove it from etc/apps/splunk_app_windows_infrastructure/lookups.
   - Remove following windows_apps lookup definition from etc/shcluster/apps/splunk_app_windows_infrastructure/local/transforms.conf if available on the search head deployer. In case of standalone searchhead, remove it from etc/apps/splunk_app_windows_infrastructure/local/transforms.conf if available on SH.

   [windows_app_lookup]
   filename = windows_apps.csv

   [windows_apps]
   filename=windows_apps.csv
   max_matches=1

5. Push the updated bundle from the search head deployer to all your search heads.
6. Once the app is pushed successfully, run the guided setup again on any one of the search heads.

Troubleshoot permissions issues after an upgrade

The Splunk App for Windows Infrastructure installs a new user role, winfra-admin. The Splunk user that uses the Splunk App for Windows Infrastructure must have this role, otherwise the app will not function correctly.

If, during the first time process, you see that the app does not find any data and you know that the data exists (such as in the case of an upgrade), be sure to add the winfra-admin role to the user that uses the app, as described in the troubleshooting page.

Upgrade from version 1.0.x

This topic discusses how to upgrade from version 1.0.x of the Splunk App for Windows Infrastructure to the latest version.
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.

How to upgrade If you have a deployment server

To upgrade the Splunk App for Windows Infrastructure, use your deployment server to update all of the deployment clients in the environment:

**Upgrade Splunk Enterprise if necessary**

Upgrade Splunk Enterprise and universal forwarders on all hosts in the deployment to version 7.2.x to 8.0.x

**Download and unpack apps and add-ons**

1. Download the following apps and add-ons from Splunk Apps and save them to an accessible location:
   ♦ The latest version of the Splunk App for Microsoft Exchange.
   ♦ The Splunk Add-on for Windows 6.0.0 or 7.0.0.
   ♦ The Splunk Supporting Add-on for Active Directory version 3.0.1.
2. Use WinZip or another archive utility to unarchive the Splunk App for Windows Infrastructure and Splunk Add-on for Windows packages.

**Configure and deploy add-ons to the deployment server**

1. Configure the Splunk Add-on for Windows, as described in "Download and configure the Splunk Add-on for Windows."
2. Copy the following updated add-ons from the Splunk App for Windows Infrastructure installation package to the deployment apps directory on the deployment server:
   ♦ The Splunk Add-on for Windows (Splunk_TA_windows)
   ♦ The Splunk Add-ons for Active Directory: TA-DomainController-NT5/TA-DomainController-NT6
   ♦ The Splunk Add-ons for Windows DNS: TA-DNSServer-NT5/TA-DNSServer_NT6

   ```powershell
   PS > $winfra_apps="C:\Downloads\splunk_app_windows_infrastructure\appserver\addons"
   PS > foreach ( $source in @("C:\Downloads\Splunk_TA_windows","$winfra_apps\TA-DomainController*","$winfra_apps\TA-DNSServer*") ) { Copy-Item -Path $source -Destination "C:\Program Files\Splunk\etc\deployment-apps" -Recurse }
   ```
3. Log into Splunk Enterprise the deployment server.
4. Go to Forwarder Management and deploy the add-ons to the appropriate Windows, and Active Directory deployment clients:

**Active Directory add-ons**

<table>
<thead>
<tr>
<th>If the server:</th>
<th>and it runs:</th>
<th>then install or deploy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>does not have a role in Active Directory</td>
<td>any supported version of Windows Server</td>
<td>Splunk_TA_Windows</td>
</tr>
<tr>
<td>is a domain controller</td>
<td>Windows Server 2003 or Server 2003 R2</td>
<td>Splunk_TA_Windows TA-DomainController-NT5</td>
</tr>
</tbody>
</table>
If the server: and it runs: then install or deploy:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2</td>
<td>Splunk_TA_Windows</td>
<td>TA-DomainController-2012r2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 or Server 2003 R2</td>
<td>Splunk_TA_Windows</td>
<td>TA-DNSServer-NT5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 or Server 2003 R2</td>
<td>Splunk_TA_Windows</td>
<td>TA-DomainController-NT5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA-DNSServer-NT5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA-DNSServer-NT6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Splunk_TA_Windows</td>
<td>TA-DomainController-2012r2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA-DNSServer-NT6</td>
</tr>
</tbody>
</table>

5. Install the updated Splunk Add-on for Windows onto all hosts in the central Splunk App for Windows Infrastructure instance.

6. Install the updated Splunk Supporting Add-on for Active Directory onto all search heads in the central Splunk App for Windows Infrastructure instance.

7. Install the updated Splunk App for Windows Infrastructure into all search heads in the central Splunk App for Windows Infrastructure instance.

8. Restart all hosts in the central Splunk App for Windows Infrastructure instance.

**Log in and run the first time experience**

1. Log into Splunk Enterprise on a search head in the central Splunk App for Windows Infrastructure instance. This activates the first-time setup experience.

2. Proceed through the first-time setup experience. Address any missing data issues by following the on-screen prompts.

3. Wait. As part of the upgrade, the Splunk App for Windows Infrastructure builds an accelerated data model which, depending on the size of your environment, can take some time. You can check the progress of the data model build by following the instructions in "Check data model build progress."

4. After the accelerated data model build is complete, use the app and confirm that all of the data is present and the pages show data as you expect.

**How to upgrade if you do not have a deployment server**

If you do not have a deployment server, you will set up one now as part of the upgrade process.

A deployment server reduces deployment complexity and room for errors due to typos in configuration files. Once you complete setup, you then only need to make app and configuration changes in one place.
Read more about deployment server

See the following topics to learn more about deployment server:

- "About deployment server and forwarder management" in the core Splunk Enterprise platform documentation.
- "Set up a deployment server and create a server class" in this manual.

Upgrade Splunk Enterprise if necessary

Upgrade Splunk Enterprise and universal forwarders on all hosts in the deployment to version 7.2.x to 8.0.x.

Download and unpack apps and add-ons

1. Download the following apps and add-ons from Splunk Apps and save them to an accessible location:
   - The latest version of the Splunk App for Microsoft Exchange.
   - The Splunk Add-on for Windows version 6.0.0 or 7.0.0.
   - The Splunk Supporting Add-on for Active Directory version 3.0.1.

2. Use WinZip or another archive utility to unarchive the Splunk App for Windows Infrastructure and Splunk Add-on for Windows packages.

Activate a deployment server and define server classes

1. Choose a host in your deployment that does not regularly experience high CPU or disk utilization and note the host name or IP address of the host.
   - If the host does not already have Splunk Enterprise installed on it, perform the installation.
2. On this host, log into Splunk Enterprise.
3. Create the "Send to indexer" app, as described in "Create the 'send to indexer' app."
4. Activate deployment server on the host by copying the following objects to the deployment apps directory:
   - The Splunk Add-on for Windows (Splunk_TA_windows).
   - The "Send to Indexer" app (sendtoindexer).
   - The Splunk Add-ons for Active Directory (TA-DomainController-*).
   - The Splunk Add-ons for Windows DNS (TA-DNSServer-*).

   PS > $winfra_apps="C:\Downloads\splunk_app_windows_infrastructure\appserver\addons"
   PS > foreach ( $source in @("C:\Downloads\Splunk_TA_windows","C:\Program Files\Splunk\etc\apps\sendtoindexer","$winfra_apps\TA-DomainController-*","$winfra_apps\TA-DNSServer-*","$winfra_apps\TA-SMTP-Reputation") ) { Copy-Item -Path $source -Destination "C:\Program Files\Splunk\etc\deployment-apps" -Recurse }

6. In Splunk Enterprise on the deployment server, define server classes:
   - A "universal forwarders" server class for all hosts in the deployment with a universal forwarder installed.
   - A server class for Active Directory.
   - A server class for Windows DNS.

7. Assign apps to the server classes according to the following table:

<table>
<thead>
<tr>
<th>Server Class Name</th>
<th>Add-ons to Add to the Server Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Forwarder</td>
<td>Splunk_TA_windows</td>
</tr>
<tr>
<td></td>
<td>sendtoindexer</td>
</tr>
</tbody>
</table>
### Server Class Name | Add-ons to Add to the Server Class
---|---
| TA-DomainController-NT6 (on Windows Server 2008 R2) TA-DomainController-2012r2 (on Windows Server 2012 R2) |

8. Restart Splunk Enterprise on the deployment server.

**Reconfigure universal forwarders as deployment clients**

1. On every universal forwarder in the deployment, issue the following command to turn the forwarder into a deployment client:

   ```bash
   PS > cd <Splunk Directory>\bin
   PS > .\splunk set deploy-server <host name or ip address of deployment server>:<port>
   
   * In the above example: <port> is the management port on the deployment server, and defaults to 8089.

2. On every universal forwarder in the deployment, remove the following add-ons from the Splunk apps directory (%SPLUNK_HOME%\etc\apps):
   - The Splunk Add-on for Windows.
   - The Splunk Add-ons for Active Directory (on Active Directory hosts).
   - The SMTP Reputation add-on (from the host with the outbound connection to the Internet)

3. Restart the universal forwarders.

**Confirm that the deployment server sees the universal forwarders**

1. Log back into the deployment server.
2. Use Forwarder Management to confirm that universal forwarders have phoned in to the deployment server.
3. Assign the clients to the server classes you defined earlier.
   - Assign all clients to the “Universal Forwarder” class.
   - Assign AD hosts to the AD server classes based on the version of Windows Server they run.
   - Assign DNS hosts to the DNS server classes based on the version of Windows Server they run.
4. In Forwarder Management, confirm that the apps deploy to the correct hosts.
5. Log into Splunk Enterprise on a search head in the deployment.
6. Load the Search and Reporting
7. Confirm that you see new data coming in from the deployment clients.

**Log in and run the first time experience**

1. Continuing on the search head, choose **Apps > Splunk App for Windows Infrastructure**. This activates the first-time setup experience.
2. **Proceed through the first-time setup experience.**
   - Address any missing data issues by following the prompts on-screen.
3. Wait. As part of the upgrade, the Splunk App for Windows Infrastructure builds an accelerated data model which, depending on the size of your environment, can take some time. You can check the progress of the data model build by following the instructions in "Check data model build progress."
4. After the accelerated data model build is complete, use the app and confirm that all of the data is present.
Upgrade from version 1.1.x

To upgrade from version 1.1.x to this version, update the search head(s) in the instance with the updated app:

1. Download the updated app installation package from Splunkbase and save it to an accessible location.
2. Unpack the archive.
3. Copy the `splunk_app_windows_infrastructure` folder to the `%SPLUNK_HOME%\etc\apps` folder on the search head(s) in the deployment. **Note:** If prompted, overwrite the existing folder.
4. Restart Splunk Enterprise on the search head(s).
5. Log back into Splunk Enterprise.
6. From the Home page, activate the Splunk App for Windows Infrastructure. Choose **Splunk App for Windows Infrastructure** from the list of apps on the left.

Upgrade from version 1.2.x

These upgrade instructions help you replace the Splunk App for Windows Infrastructure and the add-ons for Microsoft Active Directory and Windows DNS with the updated versions that are available on Splunkbase. You must download these updated add-ons for the updated Splunk App for Windows Infrastructure to continue to work properly.

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.

**Download the updated Splunk App for Windows Infrastructure**

1. Download the Splunk App for Windows Infrastructure from Splunkbase.

**Download the Splunk Add-on for Windows**

1. Download the Splunk Add-on for Windows from Splunkbase.

**Download the new add-ons for Active Directory and Windows DNS**

1. Download the Splunk Add-on for Microsoft Active Directory from Splunkbase.
2. Download the Splunk Add-on for Windows DNS from Splunkbase.
3. Unarchive the add-ons to a location that is accessible from all hosts in your Exchange deployment.

**Use a deployment server to make updates to apps and configurations**

This upgrade method is more streamlined than attempting to upgrade each host in the environment manually.

**Upgrade the search head**

The search head is the Splunk Enterprise instance that runs the Splunk App for Windows Infrastructure and shows all of the app data. These upgrade instructions should be performed on any host that has been designated as a search head in your Exchange deployment.

1. Update the Splunk Add-on for Windows.
2. Update the Splunk Supporting Add-on for Active Directory.
3. Install the Splunk Add-on for Microsoft Active Directory.
4. Install the Splunk Add-on for Windows DNS.
5. Update the Splunk App for Windows Infrastructure.
6. Restart Splunk Enterprise.

**Upgrade the indexer**

The indexer is the Splunk Enterprise instance that holds all of the data that the Splunk App for Windows Infrastructure has collected from Active Directory and Windows hosts. These instructions should be performed on any host that has been designated as an indexer in your Windows deployment. If a host acts as both an indexer and a search head, perform these instructions, then perform the "Upgrade the search head" instructions.

1. Upgrade the Splunk Add-on for Windows.
2. Restart Splunk Enterprise.

**Upgrade the forwarders**

Each Windows Server or Active Directory host must receive the appropriate Active Directory or DNS Add-ons to continue collecting the right data. Additionally, each of these add-ons must be configured to collect the right set of data.

**Prepare the new add-ons**

1. Copy the Splunk Add-on for Microsoft Active Directory (TA-Microsoft-AD) to the deployment apps directory on the deployment server.
2. Copy the Splunk Add-on for Windows DNS (TA-Microsoft-DNS) to the deployment apps directory on the deployment server.
3. Using a command prompt, PowerShell window, or Explorer window, go to the deployment apps directory on the deployment server.
4. If you have made any customizations to the old set of add-ons, copy and paste those configurations from the local directory of those add-ons into the local directory of the new add-ons.

**Create server classes, push the new add-ons, and delete the old add-ons**

1. On the deployment server, create a server class for the Splunk Add-on for Microsoft Active Directory and the Splunk Add-on for Windows DNS.
2. Assign the add-ons to the appropriate server class. For example, the TA-Microsoft-AD add-on should be assigned to a "Microsoft Active Directory" server class.
3. Assign the Windows Server and Active Directory hosts in your Windows deployment to the appropriate server classes. For example, Windows Server hosts that participate in Active Directory should be assigned to the server class that has the TA-Microsoft-AD add-on assigned to it.
4. Delete all of the old add-ons on the deployment server (for example, TA-DomainController-NT5, TA-DNSServer-*, and so on.)
5. Use the deployment server to push the new add-ons to all of the hosts in the deployment.
6. Restart the deployment server.
7. Restart all forwarders.

**Upgrade the Splunk App for Windows Infrastructure without a deployment server**

If you do not have a deployment server in your environment, you must perform these instructions manually.
Upgrade the Splunk Add-ons for Microsoft Active Directory and Windows DNS

A deployment server makes this part of the upgrade easier.

1. Download the Splunk Add-on for Microsoft Active Directory from Splunkbase.
2. Download the Splunk Add-on for Windows DNS from Splunkbase.
3. On every domain controller in your environment that has a Splunk universal forwarder and the old TA-DomainController* add-on installed, remove the add-on.
4. Install the new TA-Microsoft-AD controller onto the domain controllers.
5. On every DNS server in your environment that has a Splunk universal forwarder the old TA-DNSServer* add-on installed, remove the add-on.
6. Install the new TA-Microsoft-DNS controller onto the DNS servers.
7. Restart the universal forwarders on both the domain controllers and DNS servers.

Upgrade Splunk Add-on for Windows v6.0.0 or later

Refer to Upgrade the Splunk Add-on for Windows to upgrade from a previous version of TA_windows 6.0.0 or later.

Add the Splunk Add-ons for Microsoft Active Directory and Windows DNS to indexers and search heads

1. Install the TA-Microsoft-AD add-on into all Splunk Enterprise indexers and search heads in the deployment.
2. Install the TA-Microsoft-DNS add-on into all Splunk Enterprise indexers and search heads in the deployment.
3. Restart Splunk Enterprise on all indexers and search heads in the deployment.

Upgrade the Splunk App for Windows Infrastructure

1. Download the updated app installation package from Splunkbase and save it to an accessible location.
2. Unpack the archive.
3. Copy the splunk_app_windows_infrastructure folder to the $SPLUNK_HOME\etc\apps folder on the search head(s) in the deployment.
4. (Optional) If the operating system asks if you want to overwrite the existing folder, answer yes.
5. Restart Splunk Enterprise on the search heads.
7. From the Home page, activate the Splunk App for Windows Infrastructure. Choose Splunk App for Windows Infrastructure from the list of apps on the left.
Use the Splunk App for Windows Infrastructure

Log in and get started

This topic shows you how to log in to Splunk Web, access the Splunk App for Windows Infrastructure, and get started.

Log in to Splunk Web

To log into Splunk Web and access the Splunk App for Windows Infrastructure, navigate to:

http://<host>:8000

Use the host and port you chose during installation. The default port is 8000.

The first time you log in to Splunk, the default login details are:

Username - admin
Password - changeme

Splunk recommends that you change the admin password to a secure password.

Access the Splunk App for Windows Infrastructure

Once you've logged in to Splunk Web, you'll see Splunk Home, which lists all the apps that are currently installed. You should see the Search & Reporting app, as well as the Splunk App for Windows Infrastructure.

To access the Splunk App for Windows Infrastructure, click on it in the list. You'll see the Overview page.

Configure the Splunk App for Windows Infrastructure

After you install the Splunk App for Windows Infrastructure, you must configure it before it can be used.

When the Splunk App for Windows Infrastructure first runs, it checks your Splunk Enterprise environment to ensure that all data and supporting apps and add-ons that it needs are available. This process is known as the "First time run" process. The Splunk App for Windows Infrastructure does not let you use it until you have successfully installed the required supporting apps and all the data it needs is present on the instance you have installed it on.

You can run this process at any time after the initial run by selecting "Guided Setup" from the "Tools and Settings" menu within the app.

First-time run

This process runs the moment you load the Splunk App for Windows Infrastructure for the first time.
To start the process, click the green **Start** button. The Splunk App for Windows Infrastructure loads the **Prerequisites** page and begins detecting basic prerequisites for the app.

**Prerequisites**

The Splunk App for Windows Infrastructure detects the following prerequisites:

- **The Splunk Enterprise version.** Version numbers described in the platform and hardware requirements.
- **App key value store status.** As part of checking the Splunk Enterprise version, the app also checks to see if you have the app key value store enabled. If it is not enabled, it asks you to do so.
- **The Splunk Add-on for Windows version.** The app requires the Splunk Add-on for Windows (TA-Windows) to be installed on the same instance that it resides. See **What are the other prerequisites?** for supported version information.
- **The Supporting Add-on for Active Directory version.** The Splunk App for Windows Infrastructure needs the latest version of this required add-on installed on the same instance that it resides.
- **Splunk user credentials.** The app checks for the presence of the `winfra-admin` role for the user that has logged into the instance. If that role is not present, it asks you to add it.

If you have not satisfied one or more prerequisites, it appears in red with an ‘X’ next to it. The app provides assistance on how to correct the problem. This can range from downloading and installing add-ons, enabling app key value store, or configuring the logged in Splunk Enterprise user, for example.
To correct the problem:

1. Follow the guidance provided. You might need to download and install an app or visit a different page within the Splunk Enterprise instance.
2. Return to the Splunk App for Windows Infrastructure prerequisites setup page, if necessary.
3. Click the "Redetect" button next to the "Prerequisites" title.

If you have satisfied the prerequisite, it then turns green. Once you satisfy all prerequisites, the "Next" button at the top of the page activates and turns green. Click this button to proceed to the next step of the setup process.

Check Data

The second phase of the setup experience confirms that the data that the app needs to function is present. In this phase, the app checks for:

- **Data from the Splunk App for Windows Infrastructure.** The app confirms that data from your Windows servers exists on the indexer.
- **Data from the Splunk Add-on for Windows.** The app checks to see that Windows data has been gathered from the Windows servers in your deployment and is available.
- **Data from the Splunk Supporting Add-on for Active Directory.** This check confirms that the app sees Active Directory data coming in from the SA-LDAPsearch supporting add-on.

The app checks for a certain number of events that have occurred in the past 24 hours. If no events have occurred for a certain type, the app warns you of this and highlights the type in red. Other data types are not required for a successful deployment and appear as warnings in yellow.

When you encounter either an error or a warning, the likely case is that data is not coming in from the forwarders. To resolve this problem:

1. Review your forwarder configurations and, if necessary, follow the steps in the previous data collection chapters in this manual to confirm that you have enabled the appropriate data inputs and that the forwarders send out that data.
2. Once you have confirmed the forwarder setup, return to the Splunk App for Windows Infrastructure Check Data setup page.
3. Click the "Redetect" button.
If you have corrected the problem successfully, the data type turns green. Once you have all data types flowing in successfully, the "Next" button at the top of the page activates and turns green. Click the button to proceed to the next step in the setup process.

**Customize Features**

This page displays the list of dashboard panels that come with the Splunk App for Windows Infrastructure. Each panel displays information about specific features for Microsoft Windows and Active Directory.

Based on the information that the app gathered earlier in the setup process, it activates or deactivates panels in each of the three panel groups:

- **Windows**: This panel group contains options based on incoming Windows data that the Splunk App for Windows Infrastructure detected in the setup process. The Splunk App for Windows Infrastructure enables these panels if it detects that Windows data has been collected.

- **Active Directory**: This panel group contains options based on incoming Active Directory data that the Splunk App for Windows Infrastructure detected in the setup process. The Splunk App for Windows Infrastructure enables these panels if it detects that Active Directory data has been collected.

You can perform the following actions on this page:

- You can enable an entire panel group by clicking the checkbox next to **Windows** or **Active Directory** checkboxes at the top of the page.
- You can select the individual panels you would like the app to display.
- You can deselect individual panels that you would not like the app to display.
- You can tell the app to perform the data detection process by clicking the **Detect Features** button at the bottom of the page.
- If you are satisfied with the feature set that the app has detected, click the green **Next** button to complete app setup.

**Note**: If there is no data present for a panel that you have enabled, the Splunk App for Windows Infrastructure displays the panel within the app but does not show any data on the page.

**Detect Features**

The "Detect Features" process runs automatically as part of the setup process when you first install the app. As it detects features, it displays a dialog box that shows you its progress:
During the process, the app:

- Detects for presence of data for its dashboard panels.
- Builds lookup tables that allow it to function properly.

You can stop this detection process if needed by clicking the “Cancel” button. It is a good idea, however, to allow the process to run at least once, especially if it is the first time that the app has run the process.

Once the process has completed, the app enables dashboard panels for all the features that it has detected data. Click the Close button to return to the “Customize Features” page.

**Complete setup**

After you customize dashboard panels for the app, it presents the “Success! Splunk App for Windows Infrastructure has been configured” page.
Here you have several choices:

- Click the green **Windows Overview** button to proceed to the Windows Overview page.
- Click **Active Directory Overview** to head over to the Active Directory Overview page.
- Click **Home** to proceed to the home page.

**Dashboard reference**

The dashboard reference has been moved from this manual to the new Reference manual.

Proceed there to learn how to use the dashboards included with the Splunk App for Windows Infrastructure.

**Build custom dashboards**

All customer created dashboards built using the custom dashboard builder will no longer be available for use in versions 1.4.0 and above of the Splunk App for Windows Infrastructure.

All dashboards shipped as part of this app will still be available by navigating to **Core Views > Dashboards**.
Build custom dashboards

All customer created dashboards built using the custom dashboard builder will no longer be available for use in versions 1.4.0 and above of the Splunk App for Windows Infrastructure.

All dashboards shipped as part of this app will still be available by navigating to Core Views > Dashboards.
Troubleshoot the Splunk App for Windows Infrastructure

This topic discusses how you can troubleshoot your Splunk App for Windows Infrastructure deployment if you aren’t seeing the data that you expect.

Is the Splunk App for Windows Infrastructure deployment correctly configured?

The first thing to check when Splunk App for Windows Infrastructure data is incomplete or incorrect is to confirm that the central Splunk instance is properly configured and is receiving data.

1. Confirm that every indexer in the deployment has been configured to receive data. See Install and configure a Splunk Enterprise indexer in this manual or Enable a receiver in the core Splunk documentation for instructions.

2. If present, confirm that every search head in the central Splunk instance has been configured properly. Search heads must search all available indexers to get all indexed AD data.

See Distributed search deployment overview and Configure distributed search in the core Splunk Enterprise documentation for specific instructions on configuring search heads and search peers (indexers).

3. Confirm that you have installed and configured all the components properly.

   1. Indexes that the Splunk App for Windows Infrastructure requires must be present on all indexers.
      1. msad: for AD health metrics
      2. wineventlog: for Directory Service, Replication Service, DNS server event logs
      3. perfmon: for performance metrics
   2. The Splunk App for Windows Infrastructure must reside on all search heads in the deployment.
   3. The Splunk Supporting Add-on for Active Directory (SA-ldapsearch) must be configured properly and reside on all search heads in the deployment. See Troubleshoot issues with SA-LDAPsearch.
   4. eventtypes.conf (in %SPLUNK_HOME%/etc/apps/splunk_app_windows_infrastructure/local) must be configured with the proper indexes for the defined event types.

4. Confirm that the lookup tables for the app have been properly created.

   From the Tools and Settings menu, select Build lookups.

Troubleshoot issues with ldapsearch

When the Splunk App for Windows Infrastructure cannot complete a search using the SA-ldapsearch supporting add-on, it notifies you by displaying an error message in Manager’s status bar (at the top of your browser window), as follows:

```
External search command 'ldapsearch' returned error code 1. ERROR: com.unboundid.ldap.sdk.LDAPException: 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 525, vece
```

The Splunk App for Windows Infrastructure also writes a message to $SPLUNK_HOME/var/log/splunk/SA-ldapsearch.log, similar to the following:

```
```
If you see an error message similar to this when performing a search, use the following table to decode the data value and figure out how to resolve the error.

<table>
<thead>
<tr>
<th>Data value</th>
<th>What it means</th>
<th>What you should do</th>
</tr>
</thead>
<tbody>
<tr>
<td>255</td>
<td>Either the domain was not found or there was a syntax error in the search command.</td>
<td>Confirm that the domain that you want to monitor exists and is configured properly, or that your search string is properly formatted and syntactically correct.</td>
</tr>
<tr>
<td>525</td>
<td>The username provided in ldap.conf is not valid.</td>
<td>Edit ldap.conf and provide the correct user, then restart your central Splunk instance.</td>
</tr>
<tr>
<td>52E</td>
<td>The password provided in ldap.conf is not valid.</td>
<td>Edit ldap.conf and provide the correct password, then restart your central Splunk instance.</td>
</tr>
<tr>
<td>530</td>
<td>The user account provided is not allowed to log into Active Directory at this time.</td>
<td>Remove the user's log on time restrictions from within Active Directory, then try again.</td>
</tr>
<tr>
<td>531</td>
<td>The user account provided is not allowed to log into Active Directory from the current server.</td>
<td>Modify the local security policy of the server from which the specified user is trying to log in to Active Directory, then try again.</td>
</tr>
<tr>
<td>532</td>
<td>The user account provided has an expired password.</td>
<td>Change the user's password or set the &quot;Password never expires&quot; bit from within Active Directory, then try again.</td>
</tr>
<tr>
<td>533</td>
<td>The user account provided is disabled.</td>
<td>Re-enable the user account from within Active Directory, then try again.</td>
</tr>
<tr>
<td>701</td>
<td>The user account provided has expired.</td>
<td>Re-enable the user account from within Active Directory, then try again.</td>
</tr>
<tr>
<td>773</td>
<td>The user account provided has the &quot;User must reset password at next logon&quot; bit set.</td>
<td>Un-set the &quot;User must reset password at next logon&quot; bit for the user account from within Active Directory, then try again.</td>
</tr>
<tr>
<td>775</td>
<td>The user account provided is locked because an incorrect password has been entered too many times.</td>
<td>Re-enable the user account from within Active Directory and change the password to a known good one, then try again.</td>
</tr>
</tbody>
</table>

**Windows event log or performance events from universal forwarders go to the 'main' index**

When you install a universal forwarder on a Windows server, you must not select any options in the Enable Inputs screen of the installer. Doing so enables the scripted inputs that come with the forwarder by default. Those inputs send data to the "default" index as specified in their configuration files, which, on a standard Splunk installation, is main.

After you install the universal forwarder onto your Windows server, deploy the appropriate add-ons included in the Splunk App for Windows Infrastructure installation package. See "Deploy the Splunk Add-on for Windows" and "Deploy the Splunk Add-ons for Active Directory".

**Dashboards fail to load after upgrading the app or Splunk Enterprise**

If you experience an issue where some dashboard panels or menus fail to load after you upgrade either Splunk Enterprise or the Splunk App for Windows Infrastructure, clear your web browser’s cache, log out of Splunk Enterprise, then log back in. This should fix the problem.
No data types found after upgrade

If you experience a problem where the first-time run process detects no data after an upgrade, make sure you have added the new `winfra-admin` role to the user that runs the app.

1. In the upper right hand of the Splunk Web page, click **Settings**.
2. In the window that pops up, under “Users and Authentication”, click **Access Controls**. Splunk loads the “Access Controls” page.
3. Click **Users**. Splunk loads the “Users” page.
4. In the **Username** column, click the name of the user that runs the Splunk App for Windows Infrastructure. Splunk Enterprise loads the settings page for that user.
5. Scroll down to **Assign to roles**.
6. Add the `winfra-admin` role to the **Selected roles** pane by clicking on its entry in the **Available roles** pane.
7. Click **Save**. Splunk saves the changes and returns you to the Users page.

Error message: Configuration file settings may be duplicated in multiple apps

Your deployment receives the following error.

Configuration file settings may be duplicated in multiple apps: stanza="ActiveDirectory: Create Computer Lookup" file="savedsearches" apps="splunk_app_microsoft_exchange,splunk_app_windows_infrastructure"
This error happens when the Splunk App for Windows Infrastructure and the Splunk App for Microsoft Exchange are installed on the same search head. The Splunk App for Windows Infrastructure and the Splunk App for Microsoft Exchange contain identical knowledge objects that cause a conflict when installed on the same search head deployment.

Removing either the Splunk App for Windows Infrastructure or the Splunk App for Microsoft Exchange will resolve this issue.

**Lookup errors on all searches for WinEventLog:System:IAS and source:::Security** If running Windows App For Infrastructure 1.5.0 with Splunk_TA_windows 4.8.4.

If you experience the following search errors on UI while running Windows App For Infrastructure 1.5.0 with the Splunk_TA_windows 4.8.4, then remove windows_apps lookup and its transforms definition from Windows App For Infrastructure.

Error 'Could not find all of the specified lookup fields in the lookup table.' for conf 'source:::Security' and lookup table 'windows_app_lookup'.

Remove windows_apps.csv lookup from main app.

1. Remove windows_apps lookup from /etc/shcluster/apps/splunk_app_windows_infrastructure/lookups on the searchhead deployer (In case of standalone searchhead, remove it from /etc/apps/splunk_app_windows_infrastructure/lookups).

2. Remove following windows_apps lookup definition from /etc/shcluster/apps/splunk_app_windows_infrastructure/default/transforms.conf on the searchhead deployer (In case of standalone searchhead, remove it from /etc/apps/splunk_app_windows_infrastructure/default/transforms.conf).

   [windows_app_lookup]
   filename = windows_apps.csv

   [windows_apps]
   filename=windows_apps.csv
   max_matches=1

3. Push bundle from deployer to SHs (In case of standalone searchhead, restart Splunk on SH).

**Precheck error in Splunk App for Windows Infrastructure guided setup for Splunk version 7.0.x**

If you're using Splunk version 7.0.x and the Splunk App for Windows Infrastructure version 1.5.2, you may experience an error while running the guided setup precheck step. Bypass the the precheck step and continue. Bypassing the step does not impact app functionality.
Advanced topics

Size and scale a Splunk App for Windows Infrastructure deployment

This topic discusses possible options in sizing and scaling a Splunk App for Windows Infrastructure deployment.

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.

How to size an initial deployment

To initially size a Splunk App for Windows Infrastructure deployment and determine an initial hardware outlay, follow these guidelines:

1. Determine the number of machines that the environment should monitor.
   ♦ Count the number of Windows and Active Directory hosts in the network.

2. Determine the amount of daily indexing volume that will occur.
   ♦ Estimate your storage requirements. Build a test environment and log the following samples over a day:
     • Active Directory data (from a domain controller and DNS server).
     • Windows data (from a single Windows host)
   ♦ Multiply the figure for each data type listed above by the number of hosts in your environment that match the type.
   ♦ Add these figures together to come up with the estimated daily indexing volume.

3. Determine the number of people who will have access to the app.
   
   With these values you can determine how much of an initial hardware outlay you need:

4. See "Forwarder to indexer ratios" to determine how many indexers you need to handle incoming data streams from the forwarders.
5. See "Summary of performance recommendations" to determine how many search heads you should use in the environment based on indexing volume and number of people who will have access.

The following diagram depicts a typical distributed Splunk App for Windows Infrastructure Deployment:
Depending on the number of hosts in your deployment, add more indexers to deal with the indexing load.

**How to scale an existing environment**

When you install the Splunk App for Windows Infrastructure using the process described in this manual, you install most of the services on one host. This is to help you familiarize yourself with the Splunk Enterprise features as well as show that a single indexer based on Splunk Reference hardware can support such an installation.

However, in larger environments, running all components on one server is not feasible. Searching has a heavy impact on an indexer and multiple searches happening at once can overwhelm an indexer.

To address this problem, distribute the environment. You already have in a sense: universal forwarders on every host that provides data make the Splunk App for Windows Infrastructure environment distributed. The next step involves splitting out indexing and search operations into separate tiers to reduce performance pressure on both.

The general rules are:

- The more app users you have, the more indexers you should have. Splunk users create searches, and searches tax an indexer quickly. More indexers means more bandwidth for search heads to get data and return it to the requesting user. As numbers of users increase, you should add more search heads, which subsequently means adding more indexers.
- The more hosts with data you have, the more indexers you should have. While not nearly as harsh on indexers, a lot of data coming into one indexer can cause that indexer to bottleneck, reducing performance drastically. As indexing volume increases, you should add more indexers - at least one for every 1000 hosts.
- All environments differ. Because the Splunk App for Windows Infrastructure collects so much data, there is no one-size-fits-all calculation that you can make. A group that runs one version of Windows Server might collect far more data than another group that runs a different version. Fluctuations in network traffic and Active Directory...
usage patterns also determine how much indexing throughput you need.

See the Splunk Enterprise Capacity Planning manual for information on these concepts.
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:
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]
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.
Release notes

Release notes for Splunk App for Windows Infrastructure

This topic contains information on new features, known issues, and updates as we version the Splunk App for Windows Infrastructure.

Version 2.0.1 of the Splunk App for Windows Infrastructure was released on March 13, 2020.

What's new

Splunk App Windows Infrastructure version 2.0.1 now uses Python 3 interpreter by default for its inputs.

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

Known Issues

This version of the Splunk App for Windows Infrastructure has the following reported known issues and workarounds. If no issues appear below, no issues have yet been reported.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-02-14</td>
<td>TAG-12958</td>
<td>Winfra app - There's an invalid key error on Splunk 7.x because the App uses the Python 3 interpreter by default.</td>
</tr>
</tbody>
</table>

Fixed Issues

This version of the Splunk App for Windows Infrastructure has the following reported fixed issues. If no issues appear below, no issues have yet been reported.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-02-13</td>
<td>TAG-12949</td>
<td>Windows Infrastructure: Full Group Membership search only uses default domain for ldapgroup search.</td>
</tr>
</tbody>
</table>

Third-party software attributions/credits

Some of the components included in Splunk App for Windows Infrastructure are licensed under free or open source licenses.

View the license(s) associated with each component by selecting a component name on the left.

These attributions are in addition to the attributions we give for third-party vendors whose components the Splunk Enterprise software uses and redistributes. You can find those credits in the Release Notes. Additional credits for components used by the the Splunk Supporting Add-on for Active Directory can be found in the attributions page for that add-on.

We wish to thank the contributors to these projects:
jQuery DataTables v1.9.0

(https://datatables.net/license-bsd) - BSD 3-point (also GPLv2) license

https://datatables.net/

Copyright (c) 2008-2010, Allan Jardine

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Allan Jardine nor SpryMedia may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RequireJS v2.0.10

(https://github.com/jrburke/requirejs/blob/master/LICENSE) - BSD (also MIT) license

http://requirejs.org/

Copyright (c) 2010-2011, The Dojo Foundation

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

D3 v3.0

(http://d3js.org/) - D3 License (modified MIT)

http://d3js.org/ Copyright (c) 2012, Michael Bostock All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- The name Michael Bostock may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL MICHAEL BOSTOCK BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

jQuery UI 1.10.3

(http://jqueryui.com/) - MIT license

https://jqueryui.com/

Copyright 2013 jQuery Foundation and other contributors.

This software consists of voluntary contributions made by many individuals (AUTHORS.txt, http://jqueryui.com/about) For exact contribution history, see the revision history and logs, available at http://jquery-ui.googlecode.com/svn/

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

91
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.