# Table of Contents

**Active Directory Help: Domains**
- Domain Health Issues..................................................35
- Domain Subnet Affinity Problems..................................35
- Domain Replication Issues..........................................36
- Directory Performance...............................................36

**Active Directory Help: Domain Controllers**
- Domain Status..........................................................38
- Site Status...............................................................38
- DC Status...............................................................39

**Active Directory Help: DNS**
- DNS Status..............................................................41
- DNS Server Status....................................................41
- DNS Zone Information................................................42
- DNS Performance.....................................................43

**Active Directory Help: Users**
- User Overview.........................................................45
- User Audit...............................................................45
- AD Administrator Audit.............................................46
- User Record Changes.................................................47
- Failed Logons..........................................................47
- AD Anomalous Logons...............................................48

**Active Directory Help: Computers**
- Computer Audit......................................................50
- Computer Changes..................................................50

**Active Directory Help: Groups**
- Group Audit............................................................52
- Group Changes.........................................................52

**Active Directory Help: Group Policy**
- Group Policy Audit...................................................54
- Group Policy Changes...............................................54
Table of Contents

Active Directory Help: Organizational Units ................................................... 56
Organizational Unit Audit ........................................................................ 56
Introduction

About this manual

This is the reference manual for the Splunk App for Windows Infrastructure.

In this manual you can find information and help pages on all of the default pages that come with the app. It also contains information about the Service Analyzer, Host Overview, and Performance Monitoring pages, and how to use them to learn more about your Microsoft Windows environment.

Get help on pages

There is a topic in this manual for each page in the Splunk App for Windows Infrastructure. You can access these pages in this manual, or through the Documentation function from within the app.

Each of these topics provides a description of the page along with a screenshot. It also provides basic usage instructions for the page.

Need more help?

If you need more help, Splunk has a growing, thriving community that can assist you. Post a question in the Splunk Answers site, or on the #splunk Internet Relay Chat channel. If you have a support contract, you can also submit a case.
Performance Monitor

Perfmon

This topic discusses the Perfmon page, which you access from the Host Inventory page by clicking a sparkline on that page.

Overview

The Perfmon page shows a graph that charts performance of one or more performance counters associated with a Windows host or service. The page lets you view performance metrics, compare metrics from a point in the past, and show an average of the metric from a specific point in the past.

The page provides a list of counters and allows you to add and remove existing counters from the display graph.

How to use this page

Change the time range

To change the time range, click the time picker and choose a value that suits your needs. Once you have, click Apply. The Splunk App for Windows Infrastructure updates the page based on the new time range.
**View data points**

The Perfmon page displays lines based on the data it has collected for the selected counter during the time period shown in the time picker. To see the individual data points, mouse over the line in the chart. A pop-up window shows the date, counter, object, instance, and host name, and the value at the cursor position.

**Compare data to previous points in time and average over time**

Use the "Compare to" and "Show Average from" controls to compare current data points to data points recorded at a point of time in the past or an average from a previous time.

1. To see the previous or average data points, click the checkbox next to "Compare to?" or "Show Average from?" The Splunk App for Windows Infrastructure updates the graph to show the data points.

2. To set the point in time to compare, click either "Compare to?" or "Show Average from?" A mini time picker window appears.

3a. Select an entry in the "End date and time" picker. Or,

3b. Enter a date and time in the past and click **Apply**. The Splunk App for Windows Infrastructure updates to include a dashed line (for comparing to a certain point in the past) or a dotted line (for comparing the average from a certain point in the past.)

4. Compare these data points to the current data point (the solid line.)

**Control visible data points and add and remove lines**

You can control the state of Performance Monitor data on this page by using the controls in the lower portion of the panel:

- Click the eye icon next to a performance counter to toggle its visibility in the chart.
- Click the **+ add** button to add performance counters to the graph. The Splunk App for Windows Infrastructure loads the "Select Performance Counters" dialog where you can add available counters for hosts. See "Select performance counters" later in this topic.
- To remove a counter, select it in the list and click the **remove** button.
Select performance counters

The "Select Performance Counters" dialog lets you add performance counters for items that have been collected with the Splunk Add-on for Windows.

1. Select the host that you want to see available counters for in the list.

2. In the Available Counters field, click a counter once to expand it and show the associated objects with it.

3. Click an object to display the available instances.

4. Click the desired instance.

5. Click the gray -> button to move the instance from the "Available Counters" field to the Selected Counters field.

6. Repeat this process for additional counters, if desired.

7. Click Save. The Splunk App for Windows Infrastructure updates the page with the new counter.

Share the page

To share the Perfmon page in its current state, click the Share link. The Splunk App for Windows Infrastructure displays a link that you can copy and paste into an email message or chat window.
Windows Help

Windows Overview

The Overview dashboard contains three panels: **Windows events**, **Windows performance counters**, and **All indexed data**.

The "Windows events" panel has counters for numbers of hosts, log names, and event IDs. The "Windows performance counters" panel has counters for numbers of hosts, performance objects, and performance counters.

**Windows events**: Provides information on the number of hosts from which event log data is being collected, the number of event logs and number of event IDs.

**Windows performance counters**: Provides information on the number of hosts from which performance data is being collected, number of objects and total number of counters.

**All indexed data**: Provides a chronologically-sorted list of the sources, source types, and hosts that the Splunk App for Windows Infrastructure has collected data on.

**How to use this page**

- You can control how much data this panel displays by clicking the time picker and choosing one of the available range presets or selecting a custom time range.
- You can click on the "Windows events" and "Windows performance counters" links. The Splunk App for Windows Infrastructure takes you to a
Event Monitoring

The Event monitoring page contains dashboard panels for many Windows Event Log statistics. They include trend lines which help you isolate areas of peak activity. You can mouse over the trend lines to get individual values, and click the trend lines to open a Search window that shows events collected in the time frame where you clicked.

The panels are:

- Event source names
- Task categories
- Hosts
- Event IDs
- The number of events by host over time
- The number of events by event code over time
- The number of events by log name over time
- The number of events by event type over time

How to use this page

Filter event log data

At the top of the Event Monitoring page, there is a row of drop-down boxes that lets you filter the indexed data via a number of parameters:

- Host
• Event Log Name
• Source Name
• Task Category
• Event Code
• Type

The parameters filter out data based on what you pick in each drop down. For example, if you select a host in the Host drop down, the other drop-downs update to show only data collected for that host. In this way, you can "drill down" to find the event log data for the host, log channel, source name, task category, event code, and type you seek.

Additionally, each drop down box is also a text field. You can click your mouse on any drop down box on the page to enter text into that box. The Splunk App for Windows immediately filters the collected data to show only entries that match what you type into any of the boxes.

Finally, the Additional Search Criteria text entry box allows you to search for a specific word or phrase across all of your indexed event log data.

Requirements

The dashboards on this page require you to enable one or more Windows event log inputs (Splunk recommends that you enable at least the Application, System, Security, and Setup log channels).

Use the wild-card capability on the 'Host' drop down control

This page has a Host drop-down control box. You can type in text, including wildcards, and the Splunk App for Windows Infrastructure filters the data to include only those events generated by hosts whose names match the text that you enter.

This works particularly well if you use a standard host naming convention in your environment. For example, if all domain controllers in the environment have host names which contain the strong "DC", or all IIS servers' host names contain the string "IIS", you can type in "DC" in any Host control to display data collected from all domain controllers, or "IIS" to display information from all computers in your environment that run Internet Information Server.
Performance Monitoring

Not to be confused with the Perfmon page.

This topic discusses the "Performance Monitoring" page.

Overview

The **Performance Monitoring** page contains dashboards for CPU, Memory, Physical Disk, Logical Disk, Network Interface, and System metrics.

How to use this page

You can customize the data that appears in the panels by selecting different counters and instances. You can also drill into specifics on memory, CPU, disk and network traffic by host, process, and user.

The dashboard also provides a list of useful reports at the bottom of the page. These reports can be used as a guide to customize new reports as you see fit.

Filter performance metrics

Each of the drop downs in the dashboards on the Performance Monitoring page is also a text box. You can click your mouse on any drop down box on the page to enter text into that box. The Splunk App for Windows immediately filters the collected performance metrics to show only entries that match what you type into any of the boxes.
Requirements

The dashboards on this page require the following inputs to display data:

- **CPU Metrics**: Requires Performance monitoring input "Processor".
- **Memory Metrics**: Requires Performance monitoring input "Memory".
- **Physical Disk Metrics**: Requires Performance monitoring input "PhysicalDisk".
- **Logical Disk Metrics**: Requires Performance monitoring input "LogicalDisk".
- **Network Metrics**: Requires Performance monitoring input "Network Interface".
- **System Metrics**: Requires Performance monitoring input "System".
Windows Help: Applications and Updates

Application Crashes

This page displays the status of application crashes on all of the machines in your environment. It has panels that show you information about:

- Which applications are crashing.
- Which hosts these crashes occur on.
- The number of crashes over time, by host.
- The number of crashes over time, by application.
- The details of each crash, by host.

It also provides a list of useful searches that can be used as a guide to customize the page as you see fit.

Requirements

This page requires you to enable one or more Windows event log inputs to function correctly. Enable at least the Application Event Log Log channel.

Application Installs
This page displays the status of application installs on all of the machines in your environment. It has panels that show you information about:

- The total number of installs, by host (A list with trend lines.)
- The total number of installs, by application (A list with trend lines.)
- The number of installs over time, by application (A line chart.)
- The details of an installation, by host.

It also provides a list of useful searches that can be used as a guide to customize the page as you see fit.

**Requirements**

This page requires you to enable the Windows event log inputs to function correctly. We recommend you enable at least the Application log channel.

---

### Windows Update

This page displays the status of Windows updates on all of the machines in your environment. It has panels that show you information on:

- The number of failed Windows updates, by host.
- The number of failed Windows updates, by Knowledge Base (KB) number.
- The number of failed Windows updates over time, by host.
- The number of failed Windows updates over time, by KB number.
- The number of successful Windows updates, by host.
- The number of successful Windows updates, by Knowledge Base (KB) number.
- The number of successful Windows updates over time, by host.
- The number of successful Windows updates over time, by KB number.

It also displays a list of useful searches at the bottom of the page that can be used as a guide to customize the page as you see fit.
Requirements

This page requires you to enable the `Windowsupdate.log` file monitoring input to function correctly.
Windows Help: Host Monitoring

Hosts Overview

This topic discusses the Hosts Overview page, which lets you see data that the Splunk App for Windows Infrastructure has collected about the hosts in your Windows environment.

Overview

The Hosts Overview page shows you a list of all hosts in your environment. The top of the page has controls that let you filter the host list based on host name, OS version, domain name, and architecture.

How to use this page

By default, the page shows all hosts that the app has data for.

Filter hosts by host name

To filter the host list based on host:

1. Click the Host field.

2. Choose a host from the pop-up list that appears. The Splunk App for Windows Infrastructure updates the list to show only the host(s) you select.

3. You can select as many hosts as you want to filter the list in this manner.

4. To remove filters, click the "x" to the left of the host name in the "Host" field.
Filter hosts by text string

To filter the host list based on a text string, enter that string in the Host (text search) field and press Enter. The Splunk App for Windows Infrastructure updates the list to show only those hosts that match the text string exactly. To specify a range of hosts, use a wildcard.

Filter hosts by OS version

To filter hosts by OS version, click the OS version list box and select a version of Windows. The Splunk App for Windows Infrastructure updates the list to include only the hosts that run the version of Windows that you chose.

Filter hosts by domain

To filter hosts by domain, click the Domain list box and select a domain. The Splunk App for Windows Infrastructure updates the list to include only the hosts that reside in the domain that you chose.

Filter hosts by architecture

To filter hosts by OS version, click the Architecture list box and select an architecture. The Splunk App for Windows Infrastructure updates the list to include only the hosts that have the architecture that you chose.

Host Inventory
This topic discusses the Windows Host Inventory page, which you access from the Component Health page.

**Overview**

The Host Inventory page lists detailed information about a host, including:

- The host name.
- The domain that the host resides in.
- Host hardware information.
- The version of Windows (including platform architecture) that the host runs.
- The service pack version and last installed update.
- A sparkline that shows recent processor usage.
- The amount of installed memory and a sparkline that shows recent changes in free memory.
- The amount of total and available free space.
- A sparkline that shows recent disk read I/O.
- A sparkline that shows recent disk write I/O.
- A list of key Windows Event Log events that have occurred recently.

**How to use this page**
See information on a specific host

To see host inventory on a specific host, select the host in the **Host Name** list.

Change the time range of data

To change the time range of data that the host inventory shows, use the time picker next to the "Host Name" field.

Sparklines

To see individual values that comprise each sparkline, mouse over the sparkline.

To get a detailed version of the data in the sparkline, click it. The Splunk App for Windows Infrastructure loads the Performance Monitoring page for the counter you clicked.

Key Events

Any key events that the host has logged show up in the left pane. To see more information about an event, click it. The details of the event show up in the right pane.

Host Monitoring Operations

The "Host Monitoring Operations" dashboard provides operations information about a specific host, and displays pie charts for:

- The peak CPU utilization above 50% over the last 24 hours.
- The peak memory utilization above 50% over the last 24 hours.
- The free disk space distribution.
How to use this page

You can filter this dashboard to show a single host by selecting it from the "Host" drop-down list in the upper right side of the dashboard.

If you click on any of the pie chart slices, the Splunk App for Windows Infrastructure loads the Host Monitoring Overview page filtered to the selected host.

Host Monitoring Disk Information

This topic discusses the "Host monitoring: Disk Information" page.

The "Disk Information" dashboard displays information on disk subsystems for each host. The dashboard has a single panel, which lists hostname, drive name, drive type, total disk space, free disk space, and percentage of free space.

How to use this page

You can filter the host list by selecting entries from the "Host", "File System", "Type", "Free Space %", or "Total Space (GB)" drop-down lists.

Host Monitoring Processes
This topic discusses the "Host Monitoring Processes" page.

The "Process Information" dashboard displays information on processes that run on each host. The dashboard has a single panel, which lists hostname, process name, start time, and any command-line arguments that might have been passed to the process.

**How to use this page**

You can filter the host list by selecting entries from the "Host" or "Name" drop-down lists. In this case, "Name" refers to the name of the process or processes you want to filter by.

---

**Host Monitoring Services**

This topic discusses the "Host Monitoring: Services" page.

The "Service Information" dashboard displays information on the services that run on each host. The dashboard has a single panel, which lists hostname, service name, start mode, and current service state.

**How to use this page**

You can filter the host list by selecting entries from the "Host", "StartMode", or "State" drop-down lists, or entering text into the "Name" text box. In this case, "Name" refers to the name of the service or services you want to filter by.
Windows Help: Network Monitoring

Network Activity

This topic discusses the Network Activity page, which shows you information about the network activity that has been collected from your Windows hosts.

How to use this page

Choose a list box to filter network activity based on that filter. You can either select an entry from the list box or select the search field and type in an entry. When you type in a string, the page only matches entries for events that have been collected previously.

You can choose or enter data from one of the following filters:

- **Local Host**: Where the network transaction originated.
- **Direction**: Whether the transaction was inbound or outbound from the local host.
- **Protocol**: The protocol of the network activity (TCP or UDP).
- **Packet Type**: The type of packet that was used in the transaction, one of "connect", "accept", or "transport".
- **Remote Host**: Where the network transaction was destined.
- **Remote Port**: The remote port that the network transaction used.
- **Local Port**: The local port that the network transaction used.
- **Process Name**: The program that initiated the network transaction.
- **User Name**: The user that initiated the network transaction.

The **Network Information** pane shows all network transactions that apply to the filters you set. You can use the time picker in the upper right to limit the range of data that the panel shows.

Top Hosts and Processes
This topic discusses the Top Network Hosts and Processes page, which shows you information about the top users of network resources on a host.

This page has four panels:

- **Top Hostnames - Inbound connections** - shows the top hosts that have inbound connections to the host you choose in the list box on the right.
- **Top Hostnames - Outbound connections** - shows the top hosts that the host you choose in the list box has outbound connections to.
- **Top processes - Inbound connections** - shows the processes on the host you choose in the list box that accept the most amount of network traffic.
- **Top processes - Outbound connections** - shows the processes on the host you choose that generate the most amount of network traffic.

**How to use this page**

- Choose a host from the **Local Host** list box on the top right to show the top network hosts and processes for that host.
- Choose the time picker to change the time range that this page should use to display top hosts and processes.
Windows Help: Print Monitoring

Printers Overview

This topic discusses the Print Overview page - which lets you view all of the active printers in your organization.

The page lists the following printer information:

- **Host**: The host that defined the printer.
- **Printer**: The name of the printer.
- **Status**: The current status of the printer.
- **Operation**: Whether or not a baseline was written for the printer status.
- **Driver**: The driver that the printer uses to print.
- **Print_processor**: The print processor for the printer.
- **Priority**: The print priority of the printer.
- **Port**: The port that the printer uses to send data to the print device.

How to use this page

Choose a list box to filter the number of printers the page shows. You can either select an entry from the list box or select the search field and type in an entry. When you type in a string, the page only matches entries for events that have been collected previously.

You can choose or enter data from one of the following filters:

- **Host**: Shows only printers that have been defined on the selected host.
- **Printers**: Shows only printers whose name matches the text you entered or name you selected.
- **Operation**: Whether or not a baseline was written for the printer status.

You can sort the printer list by clicking on a column header. Clicking the header multiple times toggles an ascending or descending sort.

Top Printers and Users

This topic discusses the "Top Printers and Users" page, which lets you see who prints the most on your network.
The page has two panels: "Top 10 users printing" and "Top 10 printers." Both panels are bar charts.

**How to use this page**

Use the time picker on the upper right of the page to change the time range of data that the panels show.

Mouse over the charts to get the values for number of printers and print jobs.

**Print Job Viewer**

This topic discusses the Print Job Viewer, which lets you view print jobs that have occurred over the time period that you select.

The page has one panel: "Print Monitoring Job Browser." This panel lists print jobs that have occurred based on the filter controls you use at the top of the page.

**How to use this page**

Choose a list box to filter print job activity. You can either select an entry from the list box or select the search field and type in an entry. When you type in a string, the page only matches entries for events that have been collected previously.

You can choose to enter data from one of the following filters:

- **Host:** The host that the printer resides on.
- **Printer:** The printer that printed the job.
- **Document:** A text field that lets you enter a partial or full string that represents the name of the job that was printed. To see all documents whose name matches a particular string, use an asterisk at the end of the string.
- **User:** The user that initiated the print job.

Use the time picker on the upper right of the page to change the time range of data that the panels show.
Active Directory Help

Active Directory Reports

The Active Directory module of the Splunk App for Windows Infrastructure contains several reports that let you view common security issues within Active Directory.

There are six groups of reports available for perusal:

**DNS Reports**

The **DNS Reports** collection lets you generate reports on your DNS operations by running real-time searches against the collected DNS data. These reports include:

- **DNS Failing Domains**: A list of the queries made by DNS servers that return failing responses (such as SERVFAIL, NXDOMAIN, etc.) This panel lets you sort by query, query type, response, count, and percentage of queries.

- **DNS Top Failing Domains**: A list of the top queries made by clients for domains that return failures. You can sort by query, query type, count, and percentage of queries.

- **DNS Top Hosts sending failing queries**: A list of the hosts that send the most failing DNS queries. You can sort by source IP address, count, and percentage of queries.
• **DNS Top Non-authoritative responses**: A list of the queries that DNS servers returned non-authoritative responses for. You can sort by query, query type, count, and percentage of queries.

• **DNS Top Querying Hosts**: A list of the hosts who made the highest number of DNS queries. You can sort by source IP address, count, and percentage of queries.

• **DNS Top Recursive Failure Domains**: A list of domains whose DNS servers failed to perform recursion - the ability to query DNS information on remote names handled by other DNS servers - correctly. You can sort by query, query type, count, and percentage of queries.

• **DNS Top Requested Queries**: A list of the top requested DNS queries. You can sort by query, query type, count, and percentage of queries.

**Note**: In order to view these statistics, your DNS servers must have debug logging enabled. If this feature is not turned on, then these reports will be blank.

### User Reports

The **User Reports** report collection lets you generate reports on your users from your AD servers.

These reports include:

• **All**: A list of all users in the selected domain. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official (SAM) account name, LDAP Common Name, user principle name, and User Account Control (UAC) attribute settings.
• **New:** A list of newly created users in the selected domain. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by user creation time, user added, and the user who performed the addition. You can also limit the list of accounts by selecting a time range with the time range picker at the top of the page.

• **Deleted:** A list of deleted accounts in the selected domain. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by user deletion time, user deleted, and the user who performed the deletion. You can also limit the list of accounts by selecting a time range with the time range picker at the top of the page.

• **Active:** A list of users who are active (meaning they have recently logged on) to the selected domain. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by username, full name, user principal name, and last logon time. You can also limit the list of accounts by selecting a time range with the time range picker at the top of the page.

• **Inactive:** A list of users who have not recently logged onto the selected domain. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principal name, and UAC attribute settings. You can also limit the list of accounts by selecting a time range with the time range picker at the top of the page.

• **Unused:** A list of users who have never logged onto the selected domain. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principal name, and UAC attribute settings.

• **Disabled:** A list of users whose ability to access the selected domain has been disabled. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principal name, and UAC attribute settings.

• **Non-expiring:** A list of accounts that do not expire. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principal name, and UAC attribute settings.
• **Password Not Required**: A list of accounts where a password is not required. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principle name, and UAC attribute settings.

• **No Password Expiry**: A list of accounts where the password does not expire. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principle name, and UAC attribute settings. You can also limit the list of accounts by selecting a time range with the time range picker at the top of the page.

• **Smartcard Not Required**: A list of accounts where a smartcard is not required to authenticate. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principle name, and UAC attribute settings.

• **Smartcard Required**: A list of accounts where a smartcard is required to authenticate. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principle name, and UAC attribute settings.

• **Password Too Old**: A list of accounts where the password is too old. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principle name, and UAC attribute settings.

• **No Manager**: A list of accounts that do not have a delegate assigned to them. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principle name, and UAC attribute settings.

• **Sensitive accounts**: A list of accounts whose security contexts have not been delegated to a service even though the service account has been set as trusted for Kerberos delegation. You can choose the domain whose users you want to view by selecting the domain drop-down list. You can sort by official account name, LDAP Common Name, user principle name, and UAC attribute settings.
Computer Reports

The **Computer Reports** report collection lets you generate reports on computer accounts from your AD servers.

These reports include:

- **All**: A list of all computers in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by LDAP Common Name, DNS host name, User Account Control attributes, installed operating system, and any OS service packs that have been installed.

- **Domain controllers only**: A list of all domain controllers in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by LDAP Common Name, DNS host name, User Account Control attributes, installed operating system, and any OS service packs that have been installed.

- **New**: A list of computers that have recently been added to the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by computers that were added, installed operating system, OS service pack, and the user who performed the addition.

- **Deleted**: A list of computers that have recently been removed from the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by computers that were deleted, installed operating system, OS service pack, and the user who performed the deletion. You can also limit the list of computers by selecting a time range with the time range picker at the top of the page.

- **Active**: A list of computers that have recently logged on to the selected domain in Active Directory. You can use the Domain drop-down list to
choose between domains known to the app. You can sort the list by computer name, DNS host name, installed operating system, OS service pack, and last logon time. You can also limit the list of computers by selecting a time range with the time range picker at the top of the page.

- **Inactive**: A list of computers that have not logged on to Active Directory recently. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by computer name, DNS host name, installed operating system, OS service pack, and last logon time. You can also limit the list of computers by selecting a time range with the time range picker at the top of the page.

- **Unused**: A list of computers that have never logged on to Active Directory. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by LDAP Common Name, DNS hostname, and

- **Disabled**: A list of computers whose ability to log into Active Directory has been disabled. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by computer name, DNS host name, installed operating system, and OS service pack. You can also limit the list of computers by selecting a time range with the time range picker at the top of the page.

- **Trusted**: A list of computers that either manage or are managed by a domain trust relationship. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by LDAP Common Name, DNS host name, UAC attributes, installed operating system, and OS service pack.

- **No Manager**: A list of computers that do not have a delegate assigned to them. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by LDAP Common Name, DNS host name, UAC attributes, installed operating system, and OS service pack.

**Security Group Reports**
The **Security Group Reports** report collection lets you generate reports on group accounts from your AD servers.

These reports include:

- **All**: A list of all security groups in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by LDAP Common Name, group type, LDAP member Distinguished Name, and member type.

- **New**: A list of recently-created groups in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by creation time, group name, group class, group type, and the user who performed the addition. You can also limit the list of groups by selecting a time range with the time range picker at the top of the page.

- **Deleted**: A list of recently-removed groups in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by creation time, group name, group class, group type, and the user who performed the addition. You can also limit the list of groups by selecting a time range with the time range picker at the top of the page.

- **Changed type**: A list of the changes that have been made to security groups in the selected domain, over the selected time period. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by the time that the group change occurred, the change action, the group name, the user who performed the change, the old group class or type, and the new group class or type. You can also limit the list of groups by selecting a time range with the time range picker at the top of the page.

- **Empty**: A list of groups in the selected domain that do not have any users.
in them. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by group name or type.

- **Large**: A list of groups in the selected domain that have a member count that is greater than a specified amount. You can use the Domain drop-down list to choose between domains known to the app. You can enter a positive number that represents the size of the group’s membership into the Minimum Size text field. The page then shows only groups whose membership equals or is greater than the number entered. You can then sort that list by group name, group type, the number of members, the LDAP Member Distinguished Name, and the member type.

- **Nested**: A list of groups in the selected domain that have been nested into other groups. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by LDAP Distinguished Name, LDAP Common Name, group type, and member type.

- **No Manager**: A list of groups in the selected domain that do not have a delegate assigned to them. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by group name, group type, LDAP Member Distinguished Name, and member type.

**Group Policy Object Reports**

The Group Policy Object Reports report collection allows you to generate reports on group policy objects from your AD servers.

These reports include:

- **All**: A list of all group policy objects in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by group policy ID, group policy name, group policy object version number, and the list of containers that the object has been
linked to.

- **New**: A list of recently-created group policy objects in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by add time, LDAP Common Name, group policy object display name, group policy object version number, and the list of containers that the object has been linked to. You can also limit the list of objects by selecting a time range with the time range picker at the top of the page.

- **Deleted**: A list of recently-removed group policy objects in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by delete time and LDAP Common Name. You can also limit the list of objects by selecting a time range with the time range picker at the top of the page.

- **Disabled**: A list of group policy objects that have been disabled. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by group policy object ID, group policy object name, group policy object version number, group policy object status, change time, and the list of containers that the object has been linked to.

**Organizational Unit Reports**

The **Organizational Unit Reports** report collection allows you to generate reports on group policy objects from your AD servers.

These reports include:

- **All**: A list of all organizational units in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by name, description, and the list of linked group policy objects.
**New**: A list of recently-created OUs in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by the time the OU was added, the OU name, description, and the list of linked group policy objects. You can also limit the list of objects by selecting a time range with the time range picker at the top of the page.

**Deleted**: A list of recently-deleted OUs in the selected domain. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by delete time, OU name, and description. You can also limit the list of objects by selecting a time range with the time range picker at the top of the page.

**No Manager**: A list of OUs in the selected domain that do not have a delegate assigned to them. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by OU name, description, and the list of linked group policy objects. You can also limit the list of objects by selecting a time range with the time range picker at the top of the page.

**GPO Linked**: A list of OUs with a direct GPO link. You can use the Domain drop-down list to choose between domains known to the app. You can sort the list by OU name, description, and the list of linked group policy objects.

**Active Directory Overview (Topology Report)**

This topic discusses the "Active Directory Overview (Topology Report)" page.

**Overview**

The Topology Report displays a view of all of the AD forests, domains, and domain controllers known to the Splunk App for Windows Infrastructure at the present time. You can return to this dashboard at any time by selecting Active
Directory > Active Directory Overview.

The Topology Report page splits into two halves, upper and lower. The upper half of the page is a selection panel which allows you to choose the forests, sites, domains, and domain controllers that the Splunk App for Windows Infrastructure knows about.

The lower half of the page displays additional information based on what you select on the upper half. It displays detailed information on the domain controllers in the selected forest and domain, and includes the following statistics:

- The host name of the domain controller (DC).
- The AD site that the DC belongs to.
- The operating system and version of Windows the server runs.
- The AD Flexible Single Master Operation (FSMO) role(s) the server holds.
- Information on the Directory Service Agent (DSA) options available for the DC.
- Information on the status of the AD services that the machine runs.
- Information on whether or not the server has registered itself in DNS.
- Information on whether or not the machine’s SYSVOL share is available on the network.

In this dashboard, icons in the "Masters Roles" column indicate the operations master roles for each server.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Schema Master</td>
<td>The Schema Master controls all updates to the Active Directory’s schema, then replicates it to all other domain controllers in the forest. There can be only one Schema Master in an entire forest.</td>
</tr>
<tr>
<td></td>
<td>Domain Naming Master</td>
<td>The Domain Naming Master controls the naming of all domains within the forest. It is the only domain controller that can add or remove domains from Active Directory. As such, only one Domain Naming Master can be present in a forest.</td>
</tr>
<tr>
<td></td>
<td>Relative ID Master</td>
<td>The Relative ID Master domain controller maintains the relative ID (RID) resource pool and is responsible for allocating RIDs to other domain controllers within a domain when they are requested during the creation of security principle objects like users and groups. There can only be one RID Master in a domain.</td>
</tr>
<tr>
<td>Icon</td>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>![Icon]</td>
<td>PDC Emulator Master</td>
<td>This domain controller emulates the Primary Domain Controller (PDC) role for a domain and handles time synchronization across the domain. It also handles various PDC duties (such as password changes, account lockouts and GPO manipulation) for domains which have both Windows Server 2000 and Server 2003 domain controllers present. Only one PDC emulator can be present in a domain.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Infrastructure Master</td>
<td>The Infrastructure Master handles updates to the security identifier (SID) and distinguished name (DN) of an object that is cross-referenced by another object in another domain. There can only be one Infrastructure Master in a domain.</td>
</tr>
</tbody>
</table>

The DSA options are listed as icons under the "DSA Options" column:

- A globe indicates that the server is a **Global Catalog** (GC).
- A padlock indicates that the server is a **Read-only Domain Controller** (RODC).

**How to use this page**

You can click on any domain controller in the list to get additional information about that domain controller. See **Domain Controller status** for more details.

You can limit the number of domain controller objects displayed by selecting the **Show n entries** list box on the left. You can also search for a specific string (such as the name of a domain controller) by typing in the string in the **Search:** field on the right.
Active Directory Help: Domains

Domain Health Issues

The **Health Issues** dashboard displays active problems occurring with the domain controllers within your AD. It also displays anomalous events that you should be aware of, such as reboots, problems with Knowledge Consistency Checkers (KCCs) on domain controllers, and other unexpected circumstances.

How to use this page

This selection panel lets you filter results based on Forest, Site, Domain, and Server.

You can also control how much information the app displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

Domain Subnet Affinity Problems

Occasionally, a server will appear from an IP address that is not associated with a site. The **Subnet Affinity Issues** dashboard provides a concise report for handling this case. When you see an IP address in this page, log on to your Forest Infrastructure Master and use the Active Directory Sites and Services tool to add the subnet and associate it with a Site. IP addresses that report more frequently are closer to the top of the list.
How to use this page

You can control how much information the page displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

Domain Replication Issues

This dashboard lets you review current AD replication agreements, and the status of those agreements.

How to use this page

This selection panel lets you filter results based on Forest, Site, Domain, and Server. You can also control how much information the app displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

You can change the context in which you view the replication agreements by selecting the Naming Context drop-down in the selection panel.

You can also adjust how much time is considered when constructing the reports by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

Directory Performance
This dashboard lets you view all AD-related performance metrics across all domain controllers in your AD forest in a chart.

**How to use this page**

To view a metric, select the desired domain controller from the **Server** drop-down list on the top of the dashboard. Then, select the performance **Object** and, finally, the desired **Counter** in the same fashion.

The Splunk App for Microsoft Exchange displays the chart on the lower portion of the dashboard.

You can also adjust how much data is displayed by selecting the time range you desire in the time range picker on the upper right side of the dashboard.
Active Directory Help: Domain Controllers

Domain Status

The **Domain Status** dashboard gives you information on the selected domain, including:

- Which domain controllers in the domain hold AD operations masters roles
- Which site(s) the domain is a part of
- Which domain controllers control the domain

You can choose which domain you want to view by choosing it in the **Domain** drop-down list in the upper right side of the dashboard.

You can click on one of the listed sites to get additional information about the site. See **Site status** for more information.

You can click on one of the listed domain controllers to get additional information about that controller. See **DC status**.

You can also adjust how much data you see by selecting the time range you desire in the time range picker.

Site Status
The **Site Status** dashboard gives you information about the sites in your Active Directory forest, including:

- A list of the domains included in the site.
- A list of the domain controllers included in the site.
- A list of the IP network subnets configured for the site.
- The number and replication status of any site links between this and other AD sites.
- The targeted and actual weighting of Active Directory-related activity across all of the domain controllers for a particular domain.

In the selection panel for this dashboard, you can select the site you want to view by choosing it in the **Site Name** drop-down list. This automatically updates the **Domain** drop down list next to it, which lets you select domains that are in the site you selected.

You can click on a domain in the **Domains in Site** list to get more information about that domain.

You can click on a domain controller in the **Domain Controllers in Site** list to get details about that domain controller.

You can also adjust how much data you see by selecting the time range you desire in the time range picker in the upper right side of the dashboard.

**DC Status**

![DC Status](image)

The **Domain Controller Status** dashboard gives you information on the domain controllers in your Active Directory environment, including:

- Information on Directory Services performance, with average values over time for important DS related performance counters.
- Information on replication performance.
- Any anomalous events that you should be aware of.
In the selection panel for this dashboard, you can select the domain you want to view by choosing it in the **Domain Controller** drop-down list.

You can click on individual counters in both the **Directory Services performance** and **Replication Performance** sections of the dashboard to review specifics about the values returned by those objects.

You can also adjust how much data is displayed by selecting the time range you desire in the time range picker on the upper right side of the dashboard.
The DNS Status dashboard displays an overview of current DNS operations and includes:

- A selectable list of known DNS servers in your AD environment. This includes server host name, the status of DNS on the server, the zones in which it participates, the OS version and service pack level, and a spark line depicting the average amount of DNS queries per second.
- A selectable list of known DNS zones in the environment. This consists of the zone name, the servers that control the zone, the number of records in the zone and a breakdown of specific record types.
- A list of anomalous DNS related events that have recently occurred.

You can select a server in the DNS Servers list to get more information about that server. See DNS Server status.

You can select a zone in the DNS Zones list to get additional details about that zone. See DNS Zone Information.

You can click on an anomalous event in the Anomalous events list to get specifics about that event.

You can also adjust how much data gets displayed by selecting the time range you desire in the time range picker at the upper right side of the dashboard.
The **DNS Server Status** dashboard is similar to the Domain Controller status dashboard described above. However, this dashboard contains information about DNS **Query Performance** and **Recursion Performance** instead of AD Directory Services and replication performance.

In the selection panel for this dashboard, you can select the DNS server that you want to view by choosing it in the **DNS Server** drop-down list.

You can click on a performance metric in either performance panel to get details about the selected metric. An **Anomalous Events** panel at the bottom of the dashboard lists events that warrant further investigation.

You can also adjust how much data is displayed by selecting the time range you desire in the time range picker at the upper right side of the dashboard.

**DNS Zone Information**
The **DNS Zone Information** dashboard contains details about a known Active Directory DNS zone, including:

- Important DNS zone configuration settings.
- A list of the DNS servers that control the zone.
- The status of replication of DNS servers that control the zone, and whether or not those servers are out of sync.

**Note:** You cannot change DNS settings in this dashboard. To change DNS settings, you must use the Windows **DNS** configuration tool on the DNS server(s) that control the zone that you wish to change.

You can get additional information about the DNS servers that control the zone by selecting the desired server in the **DNS Servers - Zone** list. See **DNS Server status** for additional information.

You can choose which DNS Zone you want to display by selecting it in the **DNS Zone:** drop-down list at the top of the dashboard.

You can also adjust how much data is displayed by selecting the time range you desire in the time range picker.

## DNS Performance

The **DNS Performance** dashboard lets you view specific DNS performance metrics in chart form, based on the server and performance metrics you choose in the drop-down lists in the dashboard selection panel.

In the selection panel for this dashboard, you can select the server whose performance metrics you want to view by choosing it in the **Server** drop-down list. This automatically updates the **Counter** drop down list next to it, which lets you select performance metrics for the server you selected.
Each metric is overlaid with CPU performance information so that you can correlate anomalous readings with CPU usage in real time.

You can adjust how much data gets displayed by selecting the time range you desire in the time range picker on the upper right side of the dashboard.
Active Directory Help: Users

User Overview

The **Users** series of dashboards give you vision into the defense mechanisms of your Active Directory operations. They provide information on logon failures, attempts to controvert user security settings, and user utilization, as well as display audits and reports on all AD objects in your environment.

**How to use this page**

Each of the User dashboards has two sections: upper and lower. The upper section of the dashboard is a selection panel that lets you filter the user list based on the forests, sites, domains, and domain controllers that you choose. You can filter with multiple objects at a time. The lower portion of the dashboard displays additional information based on what you select on the top half.

You can also control how much data gets displayed by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

User Audit

The **User Audit** dashboard displays information about Active Directory user objects, and includes specifics on:

- Active Directory record.
- Group Membership.
• Accounts that were locked out after failing to logon properly.
• Failed logons by the selected user.

In this dashboard's selection panel, you can choose the domain from which you want to display user audit data by selecting the Account Domain drop-down list. You must do so in order to get information on user account activity within the domain.

You can further narrow down your search by typing in the name of a valid user object in the User Account field. If you type in '*' (asterisk), the Splunk App for Microsoft Exchange searches against all users.

You can also control how much data gets displayed by selecting the time range you desire in the time range picker on the upper left side of the dashboard.

**AD Administrator Audit**

The Administrator Audit dashboard displays information about Active Directory user objects, and includes specifics on:

• Active Directory record.
• Group Membership.
• Accounts that were locked out after failing to logon properly.
• Failed logons by the selected user.

**How to use this page**

In this selection panel, you can choose the domain from which you want to display user audit data by selecting the Account Domain drop-down list. You must do so in order to get information on user account activity within the domain.

You can further narrow down your search by typing in the name of a valid user object in the User Account field. If you type in '*' (asterisk), the Splunk App for Windows inFrastructure searches against all users.
You can also control how much data gets displayed by selecting the time range you desire in the time range picker on the upper left side of the dashboard.

**User Record Changes**

The **User Record Changes** dashboard shows information about changes to user objects in the AD environment, from both a security and a directory services perspective.

**How to use this page**

This selection panel lets you filter results based on Forest, Site, Domain, and Server.

You can also control how much information the app displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

You can narrow your search by typing in the name of a user in the **Account User** field in the upper portion of the dashboard.

**Failed Logons**
The **Failed Logons** dashboard provides insight into recent failed attempts by users to log into your domain. Specific statistics include:

- Failed logons over time.
- Failed interactive logons by IP address.
- Failed logons by reason (for example, expired password, locked account, or disabled account.)
- Failed interactive logons by username.
- Failed logons by logon type.
- Users failing to logon from multiple IPs (for example, an active attempt to break into the network.)

**How to use this page**

This selection panel lets you filter results based on Forest, Site, Domain, and Server.

You can also control how much information the app displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

**AD Anomalous Logons**

The **Anomalous Logons** page contains information about questionable user activity on your network. It also shows the more sinister attempts to access restricted network resources. Specific statistics displayed here include:

- Users logging on from more than one AD site
- Users logging on from more than one workstation
- Attempts to log on to disabled or expired accounts
How to use this page

- Use the Forest, Site, Domain, and Server fields to limit results to the forest(s), site(s), domain(s), and user(s) that you want to see.
- To filter using these fields:
  - Select a field with your mouse.
  - Then, begin typing in the name of an element in the appropriate field. For example, type in the name of a forest in the Forest field. The Splunk App for Windows inFrastructure displays entries for forests it has collected data for. It also updates the page to contain only relevant information that matches the specified forest.
  - This method works identically for sites, domains, and users.
- Use the time range picker to limit results to the range of time that you want the app to display.
Active Directory Help: Computers

Computer Audit

The **Computer Audit** dashboard displays information about access to Active Directory from computer accounts, and includes statistics on:

- Active Directory record.
- Group Membership.
- Accounts that were locked out after attempting a logon from a specific workstation.
- Failed logons from specific computers.

**How to use this page**

In this selection panel, you can choose the domain from which you want to display computer audit data by selecting the **Account Domain** drop-down list. You must do so in order to get information on computer account activity within the domain.

You can further narrow down your search by typing in the name of a valid computer object in the **Computer Account** field. If you type in "*" (asterisk), the Splunk App for Windows inFrastructure searches against all computers.

You can also control how much data gets displayed by selecting the time range you desire in the time range picker on the upper left side of the dashboard.

**Computer Changes**
The **Computer Changes** dashboard displays information about changes to AD computer objects.

**How to use this page**

This selection panel lets you filter results based on Forest, Site, Domain, and Server. You can also control how much information the app displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

You can narrow your search by using one of the available drop downs to limit results based on **Administrator** (who made the changes) and **Computer Name**.
Active Directory Help: Groups

Group Audit

The **Group Audit** dashboard displays information about Active Directory group objects, and includes statistics on:

- Active Directory record.
- A full Group Membership list.
- Recent changes to the group membership.

**How to use this page**

In this selection panel, you can choose the domain from which you want to display group audit data by selecting the **Account Domain** drop-down list. You must do so in order to get information on group account activity within the domain.

You can further narrow down your search by typing in the name of a valid group object in the **Group Name** field. If you type in '*' (asterisk), the Splunk App for Windows Infrastructure searches against all groups.

You can also control how much data gets displayed by selecting the time range you desire in the time range picker on the upper left side of the dashboard.

**Group Changes**
The **Group Changes** dashboard shows information about changes to AD group objects, from the context of both changes to the group object itself and changes to the membership of the group.

**How to use this page**

This selection panel lets you filter results based on Forest, Site, Domain, and Server. You can also control how much information the app displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

You can also narrow your search by using one of the available drop-downs to limit results based on:

- **Administrator** (who made the changes)
- **Group, Group Class** (Security or Distribution)
- **Group Scope** (Global, Local or Universal).
Active Directory Help: Group Policy

Group Policy Audit

The **Group Policy Audit** dashboard displays information about Active Directory Group Policy objects (GPOs), and includes statistics on:

- Which group policy objects are linked to which containers.
- Recent changes to group policy.

How to use this page

In the upper portion of the dashboard, you can choose the domain from which you want to display user audit data by selecting the **Domain** drop-down list.

You can further narrow down your search by typing in a valid GPO in the **Group Policy Name** field.

Group Policy Changes

The **Group Policy Changes** dashboard shows information about changes to AD group policy objects, from the context of both changes to the GPO itself and changes to the membership of the group.
How to use this page

This selection panel allows you to filter results based on Domain, Administrator, and Group Policy name. You can also control how much information the app displays by selecting the time range you desire in the time range picker on the upper right side of the dashboard.

You can also narrow your search by using one of the available drop-downs to limit results based on:

- Administrator (who made the changes)
- Account Domain
- Group Policy Name
The **OU Audit** dashboard displays information about Active Directory Organizational Units and includes statistics on Active Directory record.

**How to use this page**

In this selection panel, you can choose the domain from which you want to display organization unit audit data by selecting the **Account Domain** drop-down list. You must do so in order to get information on OUs within the domain.

You can further narrow down your search by typing in the name of a valid OU in the **Group Policy Name** field. If you type in "*" (asterisk), the Splunk App for Windows inFrastructure searches against all OUs.

You can also control how much data gets displayed by selecting the time range you desire in the time range picker on the upper left side of the dashboard.