Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service

Centrify for Splunk Integration Guide

October 2021

Centrify Corporation

Legal Notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrify Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrify Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrify Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrify Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrify, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrify for Mobile, Centrify for SaaS, DirectManage, Centrify Express, DirectManage Express, Centrify Suite, Centrify User Suite, Centrify Identity Service, Centrify Privilege Service and Centrify Server Suite are registered trademarks of Centrify Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,442,962 and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Contents

Introduction

The Centrify for Splunk Integration Guide is written to assist Centrify Privileged Access Service customers with the task of easily integrating event data in Centrify PAS with Splunk. You can leverage the Centrify Add-on for Splunk to normalize Centrify events in Splunk.

This integration guide applies to the following Splunk versions and Centrify PAS releases:

Splunk Versions	Centrify Privileged Access Service Releases
6.5.x	2016
	2016.1
	2016.2
6.6.x.	2017
7.0.0	2017.1
	2017.2
	2017.3
8.0	2020.2
8.1	2020.6
8.x	2020.7

Splunk Components

The following diagram illustrates the Splunk components that interact with the Centrify Add-on for Splunk:

Centrify Add-on for Splunk

Add-ons are used in Splunk for data onboarding and parsing. The parsed events can be used for ad-hoc queries or to create visualizations. This Add-on can co-exist with other Splunk Add-ons without conflicts.

The Centrify Add-on for Splunk contains:

- Data inputs for Windows and Unix Centrify agents (disabled by default)
- A Parser to extract all of the Centrify event fields
- Event types to categorize Centrify event categories such as Centrify Configuration, Direct Authorize – Windows, and so on
- Tags so that Centrify authentication data complies with the Splunk Common Information Model (CIM)

Centrify App for Splunk

In general, the apps used in Splunk are mainly those for data visualization such as dashboards and report alerts.

The apps contain:

- Sample Centrify dashboards
- Sample weekly reports
- Sample alerts

Data Collection

Data collection can be accomplished in two ways:

- Using the Splunk Add-on for Windows or the Splunk Add-on for Unix and Linux
- Using the Centrify Add-on for Splunk

Using the Splunk Add-on for Windows or Splunk Add-on for Unix and Linux

If you are already using the Splunk Add-on for Windows and collecting Windows application logs on Indexers, you should already have the Splunk Forwarder and the Splunk Add-on for Windows installed on the Windows machine. Because Centrify logs are already part of the Windows application logs, you do not have to install anything else on the Splunk Forwarder. You should be able to see the Centrify data directly on the Indexers.

Similarly, you might already using the Splunk Add-on for Unix and Linux and sending specific UNIX and Linux logs to the Indexers. In this scenario, the Splunk Forwarder and the Splunk Add-on for Unix and Linux should be installed on the Unix machine. You can modify the `inputs.conf` file and add the Centrify-specific log directory and start forwarding that data to the Indexers.

Note that the data collection stanzas in the Centrify Add-on for Splunk remain disabled because they are not collecting data in this scenario. The expectation is that the Splunk Add-on for Windows and the Splunk Add-on for Unix and Linux are responsible for collecting data. In this case, the Centrify Add-on for Splunk is mainly used for field extractions and data normalization.

The requirements for component deployment are listed in the following table:

	Machines and Splunk Components			
	Windows Machines	Unix Machines	Indexers	Search Heads
Splunk Universal Forwarder	Yes	Yes	---	---
Splunk Add-on for Windows	Yes	---	---	---
Splunk Add-on for Unix and Linux	---	Yes	---	---
Centrify Add-on for Splunk	---	---	Yes (Needed for indexed time field extractions)	Yes (Needed for indexed time field extractions and data normalization)
Centrify App for Splunk	---	---	---	Yes

Using the Centrify Add-on for Splunk

If you do not have the Splunk Add-on for Windows or the Splunk Add-on for Unix and Linux and would like to use the Centrify Add-on for Splunk for data collection, you must install:

- Splunk Forwarder on the Windows and the Unix machines
- Centrify Add-on for Splunk on both types of machines

The `inputs.conf` file in the Centrify Add-on for Splunk contains entries for various file locations for monitoring the syslog depending on the OS platform.

You must enable the corresponding input stanza based on the OS platform. Data gets collected on the Forwarder and is then forwarded to the Indexers where the data gets indexed. Note that data collection stanzas in the `inputs.conf` file remains disabled on the Search Heads.

> **Note:** If the UNIX and Linux syslogs are stored in binary, you must use the rsyslog daemon service to put logs under any of the standard syslog locations before configuring the app on the Forwarder.

The requirements for component deployment are listed in the following table:

	Machines and Splunk Components			
	Windows Machines	Unix Machines	Indexers	Search Heads
Splunk Universal Forwarder	Yes	Yes	---	---
Centrify Add-on for Splunk	Yes	Yes	Yes (Needed for indexed time field extractions)	Yes (Needed for indexed time field extractions and data normalization)
Centrify App for Splunk	---	---	---	Yes

Overview of the Integration Steps

The general integration steps that you perform are as follows:

1. In a stand-alone environment, install and configure the Centrify Add-on for Splunk and the Centrify App for Splunk on the same machine (See Installation and configuration for a stand-alone environment).
2. For an on-premise deployment, install and configure the Centrify App for Splunk on the Forwarder, Indexer, and Search Head as identified in the previous tables (See Installation and Configuration for an On-Premise Deployment).
3. In a cloud deployment, install and configure the Centrify App for Splunk on the Forwarder, Indexer, and Search Head as identified in the previous tables (See Installation and Configuration for a Cloud Deployment).

Installation and configuration for a stand-alone environment

This section describes the steps to:

- Install the Centrify Add-on for Splunk and the Centrify App for Splunk
- Configure the Centrify Add-on for Splunk

Installing the Centrify Add-on for Splunk and the Centrify App for Splunk

To install the Add-on and the App from the command prompt, enter the following commands:

```
$SPLUNK_HOME/bin/splunk install app Centrify-add-on-for-splunk_xxx.tgz
```

```
$SPLUNK_HOME/bin/splunk install app Centrify-app-for-splunk_xxx.tgz
```

To install the Centrify Add-on for Splunk and the Splunk app from the UI:

1. Log in to the Splunk web site.
2. Go to: **Manage Apps** > **Install App from File**.
3. Choose `Centrify-add-on-for-splunk_xxx.tgz` and `Centrify-app-for-splunk_xxx.tgz`, one-by-one, and click install.
4. While selecting the build package, click the checkbox to upgrade the app.

Configuring the Centrify Add-on for Splunk

To start the data collection, you must configure the Centrify Add-on for Splunk.

• • • • • •

To configure the Centrify Add-on for Splunk:

1. Make sure that you have administrator rights on your computer.
2. Copy:
   `$SPLUNK_HOME/etc/apps/TA-centrify/default/inputs.conf.example`
   to:
   `$SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf.example`
3. Rename `inputs.conf.example` to `inputs.conf`.
4. Open the `inputs.conf` file in a text editor.
5. Find the input stanza for your OS platform among the input stanzas in `inputs.conf`.
6. To enable the stanza for monitoring the syslog for your OS platform, enable that stanza by changing the disabled property of the stanza from:
   `disabled = 1`
   to:
   `disabled = 0`.
7. Save the `inputs.conf` file.
8. Restart the Splunk app.

   Note: If Centrify PAS and Splunk are not installed on the same machine, you must forward Centrify events to the Splunk instance.

To forward Centrify events to the Splunk instance, use the following instructions for the Windows and Linux operating systems.

Windows

On a Windows machine, Centrify events are forwarded through the Splunk Universal Forwarder.

To configure events on Windows with the Centrify Add-on for Splunk:

1. Install the Splunk Universal Forwarder on a machine where the Centrify PAS are installed.
2. While performing the installation, enter the Splunk instance IP address and the port on which you are forwarding data. (Default port is 9997).

3. Install the Centrify Add-on for Splunk on Splunk Universal Forwarder using the following command:

   Note: Default username and password is **admin/changeme**

   ```
   $SPLUNK_HOME/bin/splunk install app <path of Centrify Add-on for Splunk build package>
   ```

4. Configure the Centrify Add-on for Splunk by following the steps above Configuring the Centrify Add-on for Splunk.
5. On the Splunk instance, configure receiving by navigating to **Settings** > **Forwarding and Receiving** > **Configure Receiving** > **New**. Enter the port on which events are forwarded (entered in step 2).

Linux

On a Linux machine, Centrify events are forwarded through syslog.

Follow these steps to configure syslog:

1. Enter the following information in `/etc/rsyslog.conf`:
   `*.*@@<IP-Address>:<port>`

   The `IP-address` should be the Splunk instance IP.
   The default port is 514.
2. Restart the rsyslog service using this command:
   `Service rsyslog restart`
3. On the Splunk instance, add data input to receive Centrify events:
   a. Go to: **Settings** > **Data Input** > **TCP** > **Add New** > Enter the port as in the `rsyslog.conf` file and select the source type as `syslog`.
   b. Click **Submit**.

Installation and Configuration for an On-Premise Deployment

This section describes the steps to:

- Install the Splunk Universal Forwarder
- Install the Centrify Add-on for Splunk
- Configure the Centrify Add-on for Splunk
- Install the Splunk Add-on for Windows
- Install the Splunk Add-on for Unix and Linux
- Forward data to the Indexer
- Install and configure Centrify Add-on for Splunk on the Indexer
- Install and configure Centrify Add-on and App for Splunk on the Search Head

Installing the Splunk Universal Forwarder

You must install the Splunk Universal Forwarder and one of the technology add-ons (TAs) such as Splunk Add-on for Windows/Unix and Linux or the Centrify Add-on for Splunk to collect Windows application logs. Follow the generic Splunk guidelines to install the Splunk Universal Forwarder on a Windows machine:

http://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Installtheuniversalforwardersoftware

Installing the Centrify Add-on for Splunk

Install the Splunk Universal Forwarder on a targeted system. If you are installing on the Splunk Universal Forwarder, the Splunk Web is not available.

You must extract the Add-on from the `$SPLUNK_HOME/etc/apps` directory.

Configuring the Centrify Add-on for Splunk for on-premise deployments

To configure the Centrify Add-on for Splunk for an on-premise deployment:

1. Make sure that you have admin rights to copy `$SPLUNK_HOME/etc/apps/TA-centrify/default/inputs.conf.example` to `$SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf`

   There are different input stanzas in `inputs.conf`. This particular `inputs.conf` file contains entries for various file locations for monitoring syslog, depending on the OS platform.

2. To enable any stanza based on your OS, change the disabled property of the stanza from `disabled=1` to `disabled=0`.

3. Note that source types are hard coded in the TA and you are advised not change this configuration.

   The reason for hard coding the source types is that Centrify dashboard apps are expecting very specific source types so if you change this practice, the dashboards stop working.

   NOTE: The index can be changed based on user needs.
   You can use the following configuration (example) when you want to index data with a specific index in `$SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf`

   ```
   # Red Hat, CentOS, Citrix XenServer, oracle Enterprise Linux, Scientific Linux, Fedora, SUSE, openSUSE
   [monitor:///var/log/messages] sourcetype = syslog
   disabled = 1
   index = centrify
   ```

4. Restart Splunk.

Installing the Splunk Add-on for Windows

Follow the generic Splunk guidelines to install the Splunk Add-on for Windows on a Windows machine:

https://docs.splunk.com/Documentation/WindowsAddOn/latest/User/InstalltheSplunkAdd-onforWindows

Installing the Splunk Add-on for Unix and Linux

Follow the generic Splunk guidelines to install the Splunk Add-on for Unix and Linux on a Unix machine:

http://docs.splunk.com/Documentation/UnixApp/latest/User/AbouttheSplunkAppforUnix

Forwarding Data to the Indexer

To forward data to the indexer:

1. Once you configure the Add-on, start forwarding data to the Indexer using the following command:

   `$SPLUNK_HOME/bin/splunk add forward-server <indexer>:<port>`

   Where `<indexer>` is the Indexer's address and `<port>` is the receiving port on the Indexer. Splunk recommends forwarding data on the Indexer port 9997.

2. See the list of configured Indexers using the `outputs.conf` file in: `$SPLUNK_HOME/etc/system/local/outputs.conf`.

Indexers

To install the Centrify Add-on for Splunk (to install Splunk Enterprise on the Indexer):

1. Enable the receiving on the available port by going to: **Splunk Web** > **Settings** > **Forwarding & Receiving** > Configure Receiving and enable the

port.

Splunk recommends enabling receiving on port 9997.

2. Install the Centrify Add-on for Splunk on the Indexer.

   This step helps to index data in `centrify_css_* sourcetype`.

3. Restart Splunk.

To configure the Centrify Add-on for Splunk, you do not need to have a specific configuration for the Add-on.

If you are using an index other than the main one, create an index on the Indexer.

Search Heads

To install and configure Centrify Add-on and App for Splunk on the Search Head:

1. Install the Splunk Centrify Add-on for Splunk and the Centrify App for Splunk on your Search Heads.
2. To configure the Centrify App for Splunk, create an index in your default index list in **Settings** > **Access Controls** > **Roles** > (Click on a particular role) > **Indexes Searched** by default

   You do not need a special configuration for the Centrify Add-on for Splunk.

   Note: The Forwarder, Indexer, and Search Head are on a single machine in a stand-alone deployment (but in a distributed environment, each component is on a separate machine).

Installation and Configuration for a Cloud Deployment

This section describes the steps to:

- Install the Splunk Universal Forwarder
- Install the Centrify Add-on for Splunk
- Configure the Centrify Add-on for Splunk
- Install the Splunk Add-on for Windows
- Install the Splunk Add-on for Unix and Linux
- Forward data to the Indexer
- Install and configure Centrify Add-on for Splunk on the Indexer
- Install and configure Centrify Add-on and App for Splunk on the Search Head

Installing the Splunk Universal Forwarder

You must install the Splunk Universal Forwarder and one of the technology add-ons (TAs) such as Splunk Add-on for Windows/Unix and Linux or the Centrify Add-on for Splunk to collect Windows application logs.

Follow the generic Splunk guidelines to install the Splunk Universal Forwarder on a Windows machine:

http://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Installtheuniversalforwardersoftware

Installing the Centrify Add-on for Splunk

To install the Splunk Universal Forwarder on a targeted system:

If you are installing on the Splunk Universal Forwarder, the Splunk Web is not available. Extract the Add-on from the `$SPLUNK_HOME/etc/apps` directory.

Configuring the Centrify Add-on for Splunk in cloud deployments

To configure the Centrify Add-on for Splunk in a cloud deployment:

1. Make sure that you have admin rights to copy `$SPLUNK_HOME/etc/apps/TA-centrify/default/inputs.conf.example` to `$SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf`

   There are different input stanzas in `inputs.conf`. This particular `inputs.conf` file contains entries for various file locations for monitoring syslog, depending on the OS platform.
2. To enable any stanza based on your OS, change the disabled property of the stanza from `disabled=1` to `disabled=0`.
3. Note that source types are hard coded in the TA and you are advised not change this configuration.

   The reason for hard coding the source types is that Centrify dashboard apps are expecting very specific source types so if you change this practice, the dashboards stop working.

   Note: The index can be changed based on user needs.

   You can use the following configuration (example) when you want to index data with a specific index in: `$SPLUNK_HOME/etc/apps/TA-centrify/local/inputs.conf`

   ```
   # Red Hat, CentOS, Citrix XenServer, oracle Enterprise Linux,
   Scientific Linux, Fedora, SUSE, openSUSE
   [monitor:///var/log/messages] sourcetype = syslog
   disabled = 1
   index = centrify
   ```
4. Restart Splunk.

Installing the Splunk Add-on for Windows

Follow the generic Splunk guidelines to install the Splunk Add-on for Windows on a Windows machine:

https://docs.splunk.com/Documentation/WindowsAddOn/latest/User/InstalltheSplunkAdd-onforWindows

Installing the Splunk Add-on for Unix and Linux

Follow the generic Splunk guidelines to install the Splunk Add-on for Unix and Linux on a Unix machine:

http://docs.splunk.com/Documentation/UnixApp/latest/User/AbouttheSplunkAppforUnix

Forwarding Data to the Indexer

Follow these steps:

1. Once you configure the Add-on, start forwarding data to the Indexer using the following command:

   `$SPLUNK_HOME/bin/splunk add forward-server <indexer>:<port>`

   Where `<indexer>` is the Indexer's address and `<port>` is the receiving port on the Indexer. Splunk recommends forwarding data on the Indexer port 9997.

2. See the list of configured Indexers using the `outputs.conf` file in: `$SPLUNK_HOME/etc/system/local/outputs.conf`.

Indexers

The procedure to install the Centrify Add-on for Splunk occurs in this manner:

You will have an open ticket with the Splunk Cloud team to install the Centrify Add-on on the Indexer. Installing the Centrify Add-on helps to index data in `centrify_css_* sourcetype`.

The Splunk cloud customers do not have direct access to their Indexers so they rely on the Splunk cloud team to do the configuration for them. The Splunk cloud team might create a separate index for them to ingest the data into a specific index. If this is the case, the `inputs.conf` file on the Universal Forwarder must be changed as described in Forwarding Data to the Indexer so that data is indexed properly.

To configure the Centrify Add-on for Splunk, you do not need to have a specific configuration for the Add-on.

Search Heads

You are expected to create a ticket with the Splunk cloud team to install the Splunk Centrify Add-on for Splunk and the Centrify App for Splunk on your Search Heads.

You do not need a special configuration for the Centrify Add-on for Splunk.

To configure the Centrify App for Splunk, an index created by the Splunk cloud team must be added in your default index list in:
Settings > **Access Controls** > **Roles** > (Click on a particular role) > **Indexes Searched** by default.

> **Note:** The Forwarder, Indexer, and Search Head are on a single machine in a stand-alone deployment (but in a distributed environment, each component is on a separate machine).

Splunk Index and Source Types

Splunk indexes and source types are determined based on what method is used for data collection. You can either choose the existing installation of the Splunk Add-on for Windows and Unix and Linux or the Centrify Add-on for Splunk.

Data Collection Using the Splunk Add-on for Windows and Unix and Linux

In this scenario, data is indexed to `wineventlog`, and the OS indexes and source type is either the `WinEventLog:Application`(Windows) or the `syslog` (Unix). You must add these indexes to the default searchable indexes by going to:

Settings > **Access Controls** > **Roles** > (Click on a particular role) > **Indexes Searched** by default

Data Collection Using Centrify Add-on for Splunk

In this case, data is indexed to the main index and the source type is either `WinEventLog:Application`(Windows) or `syslog` (Unix). Centrify uses the same source types as the Splunk Add-on for Windows and Unix and Linux so that field extractions can be performed regardless of the data collection method that you choose.

This method also prevents your data from being replicated to multiple indexes regardless of the data collection method used, and ensures that the Centrify data is extracted correctly in all scenarios.

CIM Compliance

The Centrify Authentication events are mapped to the Authentication model of the CIM.

To search the Centrify authentication raw events, you can execute this search query:

```
Search tag=authentication app=Centrify
```

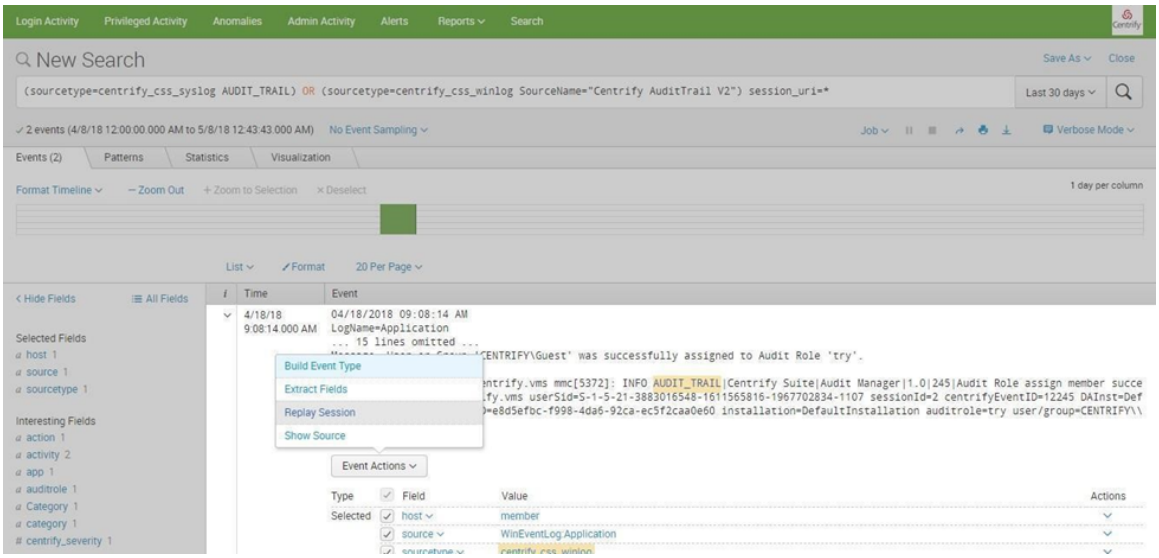
To search the Centrify failed or denied authentication data through a CIM authentication query, you can execute this search query:

```
| tstats values(Authentication.app) as app from
datamodel=Authentication WHERE Authentication.action=failure
Authentication.app=Centrify by
Authentication.dest,Authentication.user,Authentication.action
```

Session Playback

Centrify records all privileged user activity including screen actions, events, and metadata, and delivers a comprehensive picture of intentions and impacts. Its unique, searchable playback feature gives IT security managers and auditors the ability to see exactly what users did and the results of their actions. Session playback identifies privilege abuse or the source of a security incident.

Centrify's session playback is externalized to Splunk with Centrify's Session Recording and Monitoring. You can now playback the session video from the Centrify Audit event as shown in the following example:



Verification

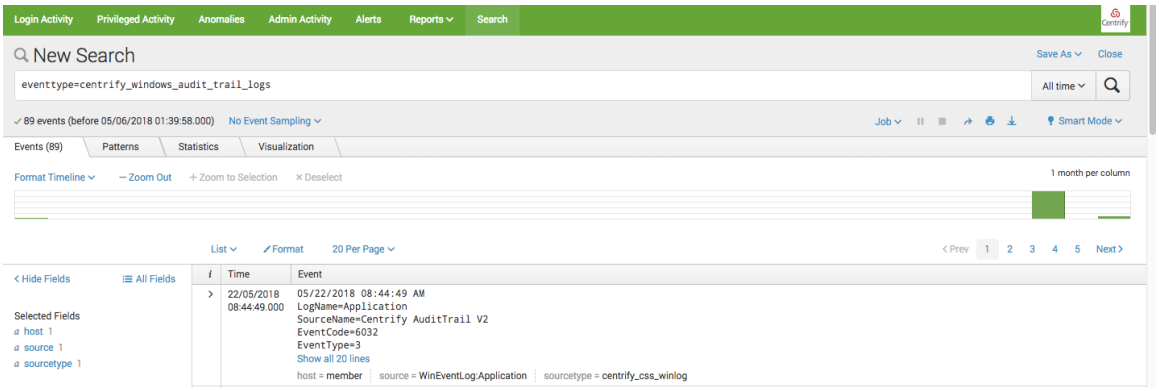
After the installation of the Centrify Add-on for Splunk is complete, all of the new Centrify audit trail events should be parsed and indexed by Splunk.

Sample Searches

Use the following sample searches to validate your installation:

- Search all Centrify logs generated on Windows Agents:
  `Search eventtype=centrify_windows_audit_trail_logs`
- Search All Audit Analyzer-related logs:
  `Search eventtype=Centrify_audit_analyzer`
- Search all successful/granted DirectAuthorize-Windows logs:
  `Search eventtype=centrify_directauthorize_windows eventstatus=GRANTED`
- Search all failed/denied DirectAuthorize-Windows logs:
  `Search eventtype=centrify_directauthorize_windows eventstatus=DENIED`

The search results for all Centrify logs generated on Windows Agents is shown in the following example:



Troubleshooting

If data is not populating in the dashboards, try the following solutions to resolve the issue:

- The Centrify Add-On for Splunk should not be modified on the Universal Forwarder. Specifically, the source type should not be modified. Data should flow from either the `WinEventLog:Application` or `syslog`.
- The Centrify Add-On for Splunk should be installed on Indexers as it performs index time extraction and indexing data in respective source types. Data from the WinEventLog:Application source type will be indexed in the `centrify_css_winlog` and the `syslog` source type data will be indexed in the `centrify_css_syslog` source type.
- If a new index has been created, it should be updated in the default index list in the user Roles shown in following location:

  Settings > **Access Controls** > **Roles** > (Click on particular role) > Indexes Searched by default.