Google Search Appliance Connectors

Deploying the Connector for Active Directory

Google Search Appliance Connector for Active Directory software version 4.0.3
Google Search Appliance software version 7.2

October 2014

Table of Contents

About this Guide

This guide is intended for anyone who needs to deploy the Google Search Appliance Connector 4.0.3 for Active Directory. The guide assumes that you are familiar with Windows or Linux operating systems and configuring the Google Search Appliance by using the Admin Console.

See the Google Search Appliance Connectors Administration Guide 4.0.3 for general information about the connectors, including:

- What's new in Connectors 4.0?
- General information about the connectors, including the configuration properties file, supported ACL features, and other topics
- Connector security
- Connector logs
- Connector Dashboard
- Connector troubleshooting

For information about using the Admin Console, see the Google Search Appliance Help Center.

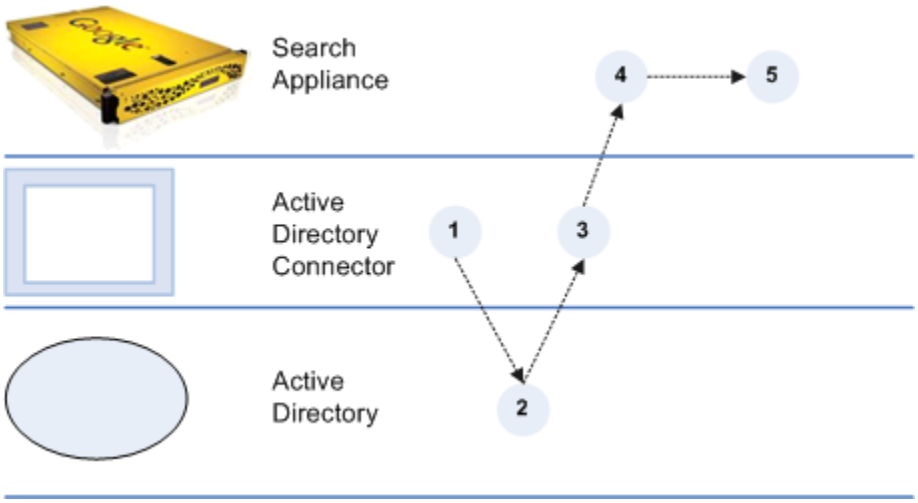
For information about previous versions of connectors, see the Connector documentation page in the Google Search Appliance Help Center.

Overview of the GSA Connector for Active Directory

The Connector for Active Directory feeds group information from an Active Directory network to the search appliance's onboard group database.

The Connector for Active Directory creates an XML groups feed for pushing the information to the search appliance. For detailed information about XML groups feeds and onboard group resolution, see Feeding Groups to the Search Appliance in the Feeds Protocol Developer's Guide. Take note that the cumulative number of group members on the search appliance cannot exceed the maximum for your search appliance model. For more information, see the Feeds Protocol Developer's Guide.

The following diagram provides an overview of how the search appliance gets group information from an Active Directory network through the Connector for Active Directory. For explanations of the numbers in the process, see the steps following the diagram.



1. The Connector for Active Directory starts communicating with Active Directory by presenting authentication credentials.
2. Active Directory gets group and member information from the Active Directory servers in the network and sends them to the connector.
3. The connector resolves group memberships and sends group definitions to the search appliance.
4. The search appliance gets the XML groups feed from the connector for Active Directory.
5. The search appliance adds them to the onboard groups database in the security manager.

Automatic updates every 15 minutes

After the initial process completes, the connector periodically sends updates to the search appliance, according to the value set in the connector configuration option `adaptor.incrementalPollPeriodSecs`. The default interval value is 15 minutes, but you can configure it to suit your needs. For more information, see "Common configuration options" in the Administration Guide.

ACL support

The Connector for Active Directory 4.0 supports:

- Active Directory groups
- Nested Active Directory groups

Domain support

The variable `ad.servers` contains a list of server identifiers. Each value in the `ad.servers` list is an alias for one particular domain.

For example, for a single domain, you might create the following configuration:

```
gsa.hostname=yourgsa.example.com
ad.defaultUser=Admin
ad.defaultPassword=PassW0RD
ad.servers=example
ad.servers.example.host=111.111.111.111
ad.servers.example.method=standard
ad.servers.example.port=389
```

A single instance of Active Directory connector can acquire groups from multiple Active Directory servers. Multiple domain support requires one connector per set of trusted domains.

If several domains have trust relationships among them all, then use one connector for all domains to successfully resolve Foreign Security Principals. Domains with no trust relationships can be traversed by different connectors.

For example, if domain1 and domain2 have trust relationships, use the following configuration:

```
ad.servers=domain1,domain2
ad.servers.domain1.host=<ip-address>
ad.servers.domain2.host=<ip-address>
```

For example, for multiple domains, you might create the following configuration:

```
gsa.hostname=yourgsa.example.com
ad.defaultUser=Admin
ad.defaultPassword=PassW0RD
# ad.servers is list of servers, one per domain
ad.servers=AMER,ASIA
ad.servers.AMER.host=111.111.111.111
ad.servers.AMER.method=standard
ad.servers.AMER.port=389
ad.servers.ASIA.host=222.222.222.222
ad.servers.ASIA.method=standard
ad.servers.ASIA.port=389
# Notice: ad.defaultUser can be overridden by providing particular
user for a particular server.
# Notice: ad.defaultPassword can be overridden by providing particular
password for a particular server.
ad.servers.ASIA.user=EXAMPLE\\Administrator
ad.servers.ASIA.password=yourpassword
```

Limitations

Usage limitations

Memory usage is dependent on the total number of Active Directory groups.

Groups database limitations

Take note of the following limitations of the groups database:

- Group feeds are not shown on “Feeds” page.
- On GSA release 7.2, the groups database scales to 1 million memberships on all GSA models.
- On GSA release 7.2 patch 1, the groups database scales to 4 million memberships on all GSA models.
- Limited visibility into groups database contents:
    - Use **Support Scripts > Export** onboard groups to list database contents
    - If multiple copies of a definition are present, only the last one matters.

- GSA refuses group feeds larger than the maximum cumulative number of group members that are allowed for your model of the search appliance.

For detailed information about this topic, see the Feeds Protocol Developer's Guide.

Supported operating systems for the connector

The Connector for Active Directory must be installed on one of the following supported operating systems:

- Windows Server 2012
- Windows Server 2008 (32 and 64 bit)
- Windows Server 2003 (32 and 64 bit)
- Ubuntu
- Red Hat Enterprise Linux 5.0
- SUSE Enterprise Linux 10 (64 bit)

Supported Active Directory repositories

The Connector for Active Directory 4.0 is compatible with the Active Directory repositories listed in the following table.

Active Directory Repository	**On Operating System**
Windows Server 2012 R2, Windows Server 2102	Windows Server 2012
Windows Server 2008 R2, Windows Server 2008	Windows Server 2008 or newer (32 and 64 bit)
Windows Server 2003	Windows Server 2003 or newer (32 and 64 bit)
Windows 2000 native	Windows 2000 or newer
any	Ubuntu
any	Red Hat Enterprise Linux 5.0
any	SUSE Enterprise Linux 10 (64 bit)

Before you deploy the Connector for Active Directory

Before you deploy the Connector for Active Directory, ensure that your environment has all of the following required components:

- GSA software version 7.2.0.G.90 or higher, to support up to 1 million group memberships
  If you need to support over 1 million group memberships, then use GSA software version 7.2.0.G.230 or higher.
  To download GSA software, visit the Google for Work Support Portal (password required).
- Java JRE 1.6u27 or higher installed on the Windows or Linux computer that runs the connector
- Connector for Active Directory 4.0.3 JAR executable
  For information about finding the JAR executable, see Step 2 Install the Connector for Active Directory.
- Credentials for the Active Directory servers to be read by the GSA

Deploy the Connector for Active Directory

Because the Connector for Active Directory is installed on a separate host, you must establish a relationship between the connector and the search appliance.

To deploy the Connector for Active Directory, perform the following tasks:

1. Configure the search appliance
2. Install the Connector for Active Directory
3. Optionally, configure adaptor-config.properties variables
4. Run the Connector for Active Directory

Step 1 Configure the search appliance

For the search appliance to work with the Connector for Active Directory, the search appliance needs to be able to accept feeds from the connector. To set up this capability, add the IP address of the computer that hosts the connector to the list of Trusted IP addresses so that the search appliance will accept feeds from this address.

To add the IP address of the computer that hosts the connector to the list of trusted IP addresses:

1. In the search appliance Admin Console, click **Content Sources > Feeds**.
2. Under **List of Trusted IP Addresses**, select **Only trust feeds from these IP addresses**.
3. Add the IP address for the connector to the list.
4. Click **Save**.

Step 2 Install the Connector for Active Directory

This section describes the installation process for the Google Search Appliance Connector for Active Directory on the connector host computer. This connector version does not support installing the connector on the Google Search Appliance.

You can install the Connector for Active Directory on a host running one of the supported operating systems.

As part of the installation procedure, you need to edit some configuration variables in the configuration file. Take note that you can encrypt the value for `ad.defaultPassword` before adding it to the file by using the Connector Dashboard, as described in "Encode sensitive values," in the Administration Guide.

To install the connector:

1. Log in to the computer that will host the connector by using an account with sufficient privileges to install the software.
2. Start a web browser.
3. Visit the connector 4.0.3 software downloads page at http://googlegsa.github.io/adaptor/index.html.
   Download the `exe` file by clicking on Microsoft Active Directory in the Windows Installer table.
   You are prompted to save the single binary file, `ad-install-4.0.3.exe`.
4. Start installing the file by double clicking `ad-install-4.0.3`.
5. On the **Introduction** page, click **Next**.
6. On the **GSA Hostname** page, enter the hostname or IP address of the GSA that will use the connector and click **Next**.
7. On the **Choose Install Folder** page, accept the default folder or navigate to the location where you want to install the connector files.
8. Click **Next**.
9. On the **Shortcut Folder**, accept the default folder or select the locations where you want to create product icons.
10. To create icons for all users of the Windows machine where you are installing the connector, check **Create Icons for All Users** and click **Next**.
11. On the **Pre-Installation Summary page**, review the information and click **Install**.
    The connector Installation process runs.
12. On the **Install Complete** page, click **Done**.
13. In the folder where you installed the connector, edit `adaptor-config.properties`.
    The following example shows the configuration variables you need to edit in the `adaptor-config.properties` file (bold items are example values that you need to replace):

    ```
    gsa.hostname=yourgsa.example.com
    ad.defaultUser=Admin
    ```

```
ad.defaultPassword=PassW0RD
ad.servers=firstServer,anotherAdServer
ad.servers.firstServer.host=111.111.111.111
ad.servers.firstServer.method=standard
ad.servers.firstServer.port=389
ad.servers.firstServer.user=EXAMPLE\\Administrator
ad.servers.firstServer.password=yourpassword
ad.servers.anotherAdServer.host=222.222.222.222
ad.servers.anotherAdServer.method=standard
ad.servers.anotherAdServer.port=389
```

`adaptor.namespace=host, port, method (ssl or standard)` is repeated for each Active Directory host.

Notes: You can override `ad.defaultUser` by providing a particular user for a particular server. You can override `ad.defaultPassword` by providing a particular password for a particular server.
See Step 3 for optional variables that you can also configure for the connector.

14. In the same folder, review, and if needed, edit `logging.properties`.
    For more information, See "Configure Connector Logs" in the Administration Guide.
15. In the same folder, run the `run.bat` file.

Step 3 Configure optional adaptor-config.properties variables

Optionally, you can edit or add additional configuration variables to the `adaptor-config.properties` file. The following table lists the most important variables that pertain to the Connector for Active Directory, as well as their default values. See also "Common configuration options" in the the Administration Guide.

Variable	Description	Default
`server.port`	Port for any crawlable documents this connector serves. Each instance of a Connector on same machine requires a unique port.	5678
`server.dashboardPort`	Port on which to view web page showing information and diagnostics.	5679

`server.hostname`	Optionally the hostname of the server running Connector, in case automatic detection fails.	Name of localhost
`adaptor.namespace=Default`	Namespace used for ACLs sent to GSA.	Default
`adaptor.fullListingSchedule`	Schedule for pushing all group definitions.	"0 3 * * *" which is 3AM
`adaptor.incrementalPollPeriodSecs`	Schedule for getting recent updates.	900 seconds which is 15 minutes
`adaptor.pushDocIdsOnStartup`	Whether to push all group definitions on startup, in addition to full listing schedule.	True
`ad.feedBuiltinGroups=false`	Whether to feed in builtin groups.	false
`feed.maxUrls`	Number of groups to define per communication with GSA.	5000

Step 4 Run the Connector for Active Directory

After you install the Connector for Active Directory, you can run it on the host machine:

On Windows, the installer creates the file `run.bat` containing this command.
On LInux, enter the following command on the host machine:

```
java -Djava.util.logging.config.file=logging.properties -jar adaptor-ad-4.0.3-withlib.jar
```

Verify that the connector has started and is running by navigating to the Connector Dashboard at `http://<CONNECTOR_HOST>:<nnnn>/dashboard` or `https://<CONNECTOR_HOST>:<nnnn>/dashboard`

where `<nnnn>` is the number you specified as the value for the `server.dashboardPort` in the configuration file.

To run the connector as a service, use the Windows service management tool or run the `prunsrv` command, as described in “Run a connector as a service on Windows” in the Administration Guide.

Uninstall the Google Search Appliance Connector for Active Directory

To uninstall the Connector for Active Directory:

1. Click the **Change GSA_AD_Adaptor Installation** icon on your desktop.
   The **Uninstall GSA_AD_Adaptor** page appears.
2. Click **Next**.
3. On the **Uninstall Options** page, select an option:
   - **Complete Uninstall.** Google recommends selecting **Complete Uninstall**.
   - **Uninstall Specific Features.** If you click **Uninstall Specific Features**, select **Application**.
4. Click **Uninstall**.
   Files are uninstalled.
5. On the **Uninstall Complete** page, select **No**, **I will restart my system myself**.
6. Click **Done**.

Troubleshoot the Connector for Active Directory

For information about troubleshooting the Connector for Active Directory, see “Troubleshoot Connectors,” in the Administration Guide.