Google Search Appliance Connectors

Deploying the Connector for Active Directory

Google Search Appliance Connector for Active Directory software version 4.0.2
Google Search Appliance software version 7.2

July 2014

Table of Contents

About this Guide

This guide is intended for anyone who needs to deploy the Google Search Appliance Connector 4.0.2 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 4.0.2 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.

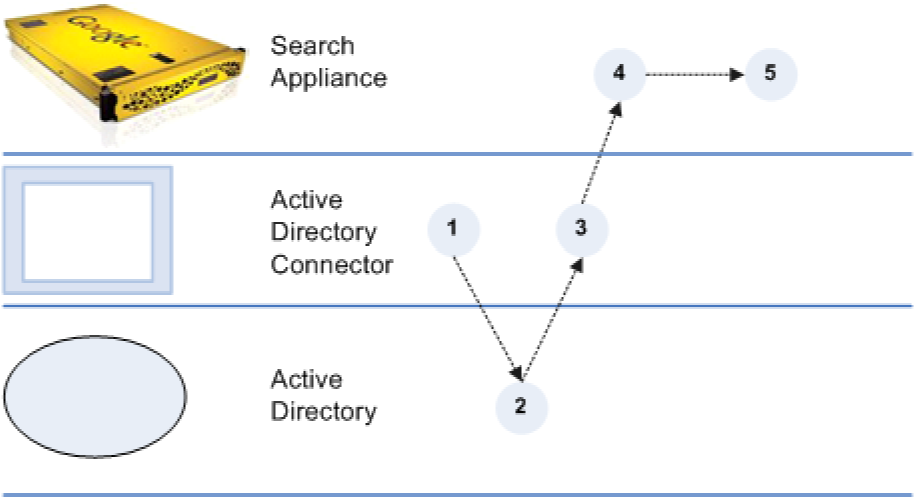
For information about previous versions of connectors, see the Connector documentation page in the Google Search Appliance Help Center.

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.

After the initial process completes, the connector periodically sends updates to the search appliance, according to the value set in the connector configuration. The default interval value is 15 minutes.

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 1 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=<ip-address>
ad.servers.domain2=<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 overriden by providing particular user
for a particular server.
# Notice: ad.defaultPassword can be overriden by providing particular
password for a particular server.
ad.servers.ASIA.user=EXAMPLE\\Administrator
ad.servers.ASIA.password=yourpassword
```

Groups database limitations

Take note of the following limitations of the groups database:

- Group feeds are not shown on “Feeds” page.
- Limited scalability.
- 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.
- For large feeds that use full feeding, verify GSA accepts repeated feeding.

Supported operating systems

The Connector for Active Directory 4.0 is compatible with the following operating systems:

- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Linux

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 download GSA software, visit the Google Enterprise 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 4.0.2 JAR executable
  For information about finding the JAR executable, see Download the connector software
- Credentials for the Active Directory servers to be read by the GSA

Download the connector software

The Connector for Active Directory must be installed on a host machine. This connector version does not support installing the connector on the Google Search Appliance.

To download the software for Connector for Active Directory:

1. Visit https://code.google.com/p/plexi/.
2. Click **Executable** for Microsoft Active Directory.
   The single binary file, `adaptor-ad-4.0.2-withlib.jar,` is downloaded.

Once you download the connector software, you can copy it to the host and configure it.

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 File Systems, 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

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 add some configuration variables and values to 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. Download the Connector for Active Directory JAR executable (`adaptor-ad-4.0.2-withlib.jar`) from https://code.google.com/p/plexi/.
2. Create a directory on the host where the connector will reside. For example, create a directory called ad_connector_40.
3. Copy the Connector for Active Directory 4.0 JAR executable to the directory.
4. Create an ASCII or UTF-8 file named `adaptor-config.properties` in the directory that contains the connector binary.

   The following example shows the configuration variables you need to add to the `adaptor-config.properties` file (bold items are example values that you need to replace):

```
gsa.hostname=yourgsa.example.com
ad.domain=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.

5. Create an ASCII or UTF-8 file named **`logging.properties`** in the same directory that contains the connector binary and add the following content:

```
.level=INFO
handlers=java.util.logging.FileHandler,java.util.logging.ConsoleHandler
java.util.logging.FileHandler.formatter=com.google.enterprise.adaptor.CustomFor
matter
java.util.logging.FileHandler.pattern=logs/adaptor.%g.log
java.util.logging.FileHandler.limit=10485760
java.util.logging.FileHandler.count=20
java.util.logging.ConsoleHandler.formatter=com.google.enterprise.adaptor.Custom
Formatter
```

6. Create a folder named `logs` in the same directory that contains `logging.properties`.

Step 3 Configure optional adaptor-config.properties variables

Optionally, you can add additional configuration variables to the `adaptor-config.properties` file that you created in the previous procedure. The following table lists the most important variables that pertain to the Connector for Active Directory, as well as their default values. Variable names are wrapped for readability.

Variable	Description	Default
server.dashboardPort	Port on which to view web page showing information and diagnostics.	5679
ad.feedBuiltinGroups=false	Whether to feed in builtin groups.	false
adaptor.namespace=Default	Namespace used for ACLs sent to GSA.	Default
server.port	Port for any crawlable documents this connector serves. Each instance of a Connector on same machine requires a unique port.	5678
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
feed.maxUrls	Number of groups to define per communication with GSA.	5000
server.hostname	Optionally the hostname of the server running Connector, in case automatic detection fails.	Name of localhost

Step 4 Run the Connector for Active Directory

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

```
java -Djava.util.logging.config.file=logging.properties -jar adaptor-ad-4.0.2-withlib.jar
```

To run the connector as a service, use the Windows service management tool or run:

```
prunsrv start adaptor-ad
```

Troubleshoot the Connector for Active Directory

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