RSD GLASS 3.4.4

Governance Services

Management Guide and Technical Reference for Shared Drive Connector

English

© Copyright RSD, 2015

RSD-000102-EN-880f220

Trademarks and Registered Names

All brand and product names quoted in this publication are trademarks or registered trademarks of their respective holders.

Notices

Governance Services is a software package property of RSD - Geneva, Switzerland that cannot be used without license.
RSD reserves the right to make any modifications to this product and to the corresponding documentation without prior notice or advice.

Manual: Governance Services - Management Guide and Technical Reference for Shared Drive Connector version 3.4.4
RSD-000102-EN-unknown

Copyright© RSD All rights reserved.

For all countries, copies or abstracts of this documentation cannot be made without written approval of RSD.

Contents

1. Introduction

The Shared Drive Connector is a level 4 driver that allows RSD GLASS® to govern documents stored in NetApp Data ONTAP and Windows NTFS shared drives: You can operate over documents stored on a NetApp or Windows shared drive repositories from RSD GLASS® and the changes on records with governed documents are reflected on the documents in the repository and vice versa.

For example, if you move or rename a governed document on the drive, the document components are updated; actions based on the content retention schedule are applied on the documents; etc. When you remove a cataloged document from the drive, it remains in GLASS as expected.

> **Important:**
>
> However, note that when a document component is on legal hold, the document can be removed from the drive.

> **Note:**
>
> The bulk export and import capabilities are not part of the connector and are handled by an external E-discovery toolset, Nuix. For further information, refer to the *Nuix Integration Guide*.

1.1. Architecture

The connector resources provide the following resources:

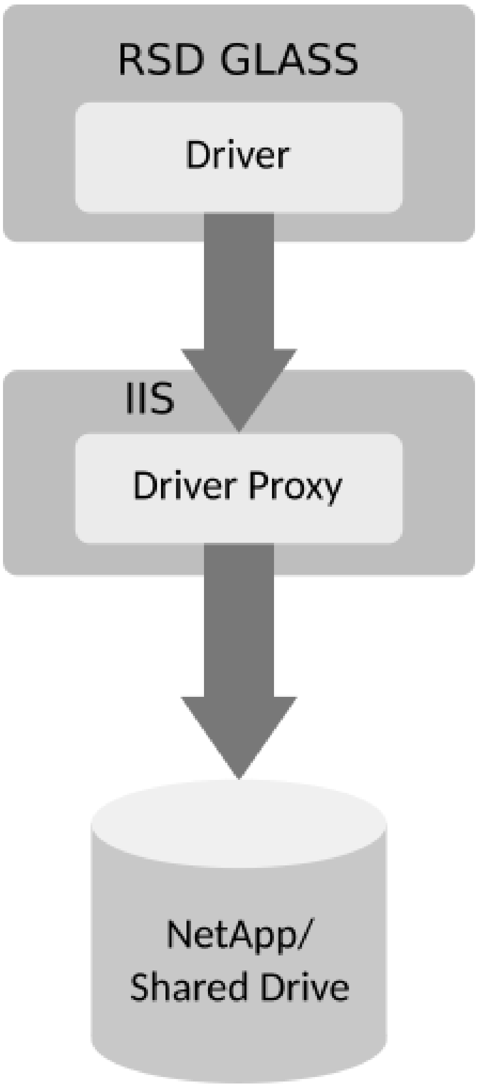
Driver for RSD GLASS®

Java resources to allow communication with the driver proxy

Driver proxy for IIS

Java resources to allow communication of the GLASS driver with the target repository

Figure 1: Architecture schema



1.2. Technical Requirements

Application server with GLASS:

- Tomcat 7
- WebSphere 8.0

Application server for the driver proxy:

- IIS

Repositories:

- NetApp Data ONTAP 8.1.4. on Microsoft Windows 2008 R2 or newer with NTFS file system

- Windows Shared Network Drive on Microsoft Windows 2008 R2 or newer with NTFS 3.x file system

1.3. Package Content

The `RSDGLASS_GS-SharedDrive-Driver.zip` connector package provides the following resources:

- Driver for RSD GLASS® in `RSDGLASS_GS-SharedDrive-Driver.zip`
    - Driver file `RSDGLASS_GS-SharedDrive-Driver.zip`
    - Driver libraries in the `lib` folder
- Driver proxy for IIS in `RSDGLASS_GS-SharedDrive-Proxy.zip`
    - Driver proxy in `RSDGLASS_GS-SharedDriveProxy.zip`
    - Proxy configuration files and the deploy binary

2. Installation

To install the solution, you need to do the following:

1. Deploy the driver to your GLASS.
2. Deploy the proxy driver to IIS.

2.1. Deployment to Application Servers with GLASS

The connector requires additional Java libraries to work correctly. Therefore you need to deploy the connector along with these libraries to the underlying application server. The libraries are located in the `lib` folder of the connector zip file.

2.1.1. Deploying to Apache Tomcat

To deploy the connector to Apache Tomcat, do the following:

1. Deploy RSDGLASS_GS-SharedDrive-Driver.jar to the `<CATALINA_BASE>\orm\connectors\` folder.
2. Copy the library jar files from the `lib` folder to the `<CATALINA_BASE>\orm\connectors\shareddrivelib\` folder.
3. Add the libraries to the classpath: in the `catalina.properties` file, add the following:

```
shared.loader=${catalina.base}/orm/connectors/shareddrivelib/*.jar
```

4. Optionally, adjust the logging properties in the `<CATALINA_BASE>\webapps\RSDGlass\WEB-INF\classes\log4j.properties` file.

Figure 2: log4j configuration with extensive logging

```
log4j.logger.com.rsd.glass=DEBUG
#comment out the log4j.logger.com.rsd.glass setting to ERROR
#log4j.logger.com.rsd.glass=ERROR

#define the log4j.logger.com.rsd.glass setting to DEBUG
log4j.logger.com.rsd.glass=DEBUG
log4j.logger.org.springframework.security.saml=DEBUG
log4j.logger.org.opensaml=DEBUG

log4j.logger.com.rsd.glass.framework.filters=TRACE
log4j.logger.com.rsd.glass.framework.saml=TRACE
log4j.logger.com.rsd.glass.core.security=TRACE
```

2.1.2. Deploying to JBoss

To deploy the connector to JBoss, do the following:

1. Set up a connector directory:
   - In standalone mode, do the following:
     1. Open the `$JBOSS_HOME\standalone\configuration\standalone.xml` file for editing.
     2. In the <system-properties> element, child element of the <server> element, define the glass.connector property with the path to the RSD GLASS connectors: `<property name="glass.connectors" value="<PATH_TO_THE_CONNECTORS_FOLDER>"/>`
   - In domain mode, do the following:
     1. Open the `$JBOSS_HOME\domain\configuration\domain.xml` file for editing.

    2. In the <system-properties> element, child element of the <server> element, define the glass.connectors property with the path to the RSD GLASS connectors: `<property name="glass.connectors" value="<PATH_TO_THE_CONNECTORS_FOLDER>"/>`

2. Deploy the RSDGLASS_GS-SharedDrive-Driver.jar file with the connector to the connector's repository, that is the path you defined in the glass.connectors property.
3. Install the additional libraries:

   a) Copy the library jar files to `$JBOSS_HOME\modules\org\jboss\as\web\main`

   b) In `$JBOSS_HOME\modules\org\jboss\as\web\mainmodule.xml`, add the libraries to the path.

2.2. Installing Driver Proxy

To install the driver proxy on an IIS server, do the following:

1. Create an application pool for the technical user.

   The technical user that will be used by the proxy to operate on the NetApp or Shared Drive resources. The user must meet following:

   - The user must be a domain user.
   - The user must be the server administrator.
   - The user must have full access to the target repository.
2. Create a site for the proxy.
3. Set requestValidationMode for the proxy to `2.0`.
4. Install to the site the driver app and configure it to point to the proxy site.
5. Deploy the driver proxy:

   a) Unzip the proxy driver `RSDGLASS_GS-SharedDrive-Proxy.zip` archive file.

   b) Open the `RSD.GLASS.SharedDriveProxy.SetParameters.xml` configuration file and insert the site path in the `IIS Web Application Name` property.

   c) Run the `RSD.GLASS.SharedDriveProxy.deploy.cmd` script.

   Figure 3: Running the deploy script

   ```
   D:\ProxyPackage> RSD.GLASS.SharedDrive.Proxy.deploy cmd /y
   ```

3. Integration

You can integrate RSD GLASS® with the Shared Drive connector with the Nuix e-discovery tool. With the integration, you can perform the governance-related operations from the Nuix GUI: identify documents to be deleted, non-records, record candidates, perform bulk-cataloging as well as manual cataloging. For further information refer to *Nuix Integration Guide*.

4. Governing a Repository

To govern a shared drive supported by the connector, you need to create its content repository and virtual content repository in RSD GLASS®. When the virtual content repository is created, the `connector` folder with the RSD GLASS® data is created in the root path of the drive. The folder is created by the connector's technical user and hence cannot be deleted or modified by the shared drive user.

Once the drive is governed by RSD GLASS®, the user can catalog and declare the documents in Governance Manager or using RSD GLASS® API.

4.1. Creating Content Repository

To create a content repository for your shared drive, do the following:

1. Log in to the Governance Manager.
2. Go to **Settings** > **Content Repositories**.
3. Click the **Content Repositories** tab label.
4. On the **Add/Update Entry** tab, define the content repository definition:
   a) In the **Driver** drop-down box, select the `Shared Drive` driver.
   b) Define the repository details:
   c) On the **Connection** tab on the right, define the drive connection details:

      1. **Shared drive Web API URL**: the URL of the proxy connector

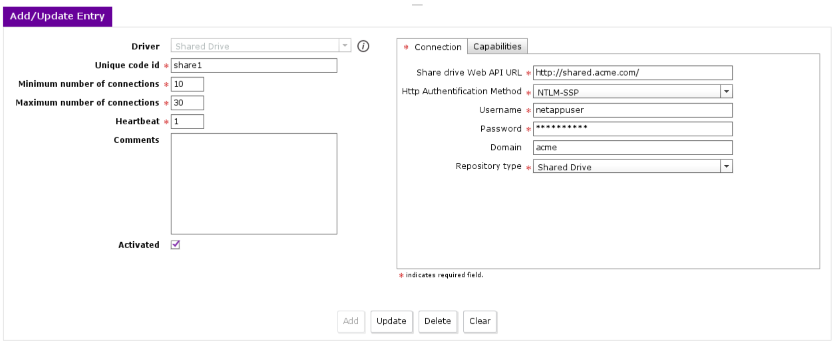
         > **Note:**
         >
         > Make sure to use the domain name and not its IP.

      2. **Http Authentication Method**: the method used to authenticate to your drive
      3. **Username**, **Password**, and **Domain**: credentials of the technical driver user

         > **Important:** The technical user must be a member of the local administrator group of the server and have full access to the repository resources.

      4. **Repository type**: select the type of the target repository; either **Netapp Shared Network Drives** or **Windows NTFS Shared Network Drives**

Figure 4: Details and connection parameters of a shared drive



Driver: Shared Drive
Unique code id *: share1
Minimum number of connections *: 10
Maximum number of connections *: 30
Heartbeat *: 1
Comments:
Activated: ☑

Share drive Web API URL *: http://shared.acme.com/
Http Authentification Method *: NTLM-SSP
Username *: netappuser
Password *: **********
Domain: acme
Repository type *: Shared Drive

* indicates required field.

   d) On the **Capabilities** tab, check the repository capabilities for RSD GLASS®.

      It is recommended to check all available capabilities.

   e) Click **Add**.

4.2. Creating Virtual Content Repository

To create a virtual content repository over the shared drive content repository, do the following

1. Log in to the Governance Manager.
2. Go to **Settings** > **Content Repositories**.
3. Click the **Content Repositories** tab label.
4. On the **Add/Update Entry** tab, define the content repository definition:
    a) On the left, define the repository details:
        - Unique code id: arbitrary string identified
        - Referenced repository id: identifier of the shared drive content repository
        - Storage level: repository level

          The storage level metadata is an enumeration that allows you to operate over a set of virtual content repositories during operations, for example, you can move documents only to virtual content repositories of a certain storage level.

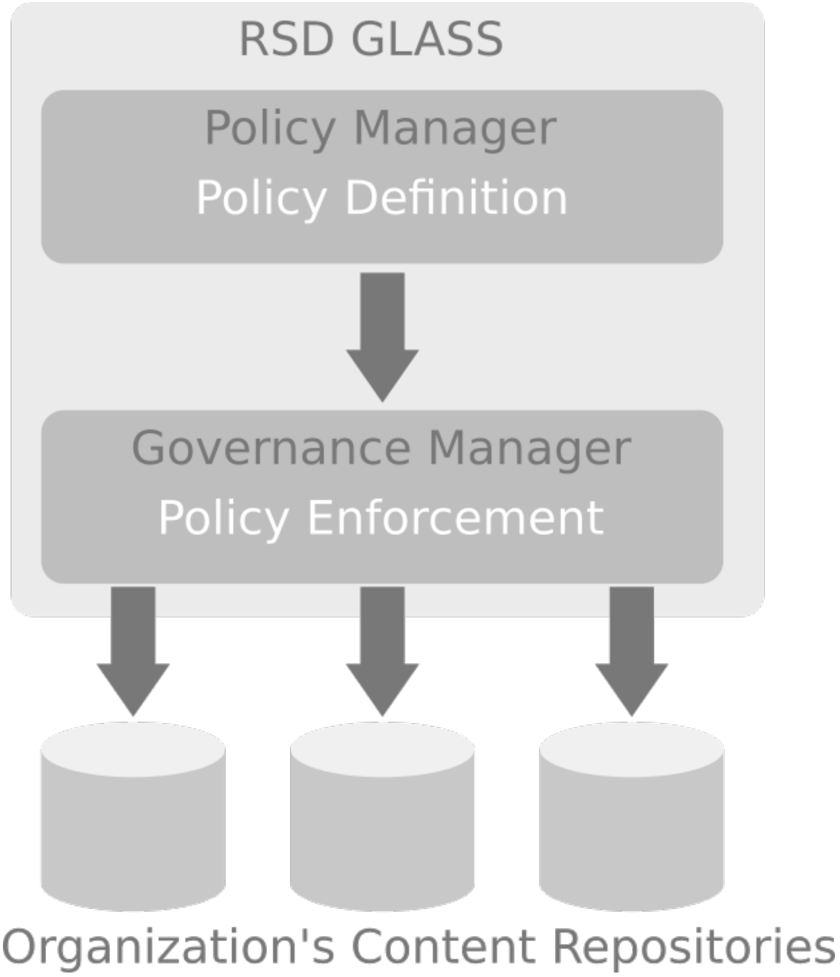
    b) On the **Context** path, define the location on the target drive, which should be governed.

    c) On the **Capabilities**, **Integrity**, and **Compliance Attributes** tabs on the right, define further virtual content repository properties.
5. Click **Add**.

On the target drive in the root path location, RSD GLASS® creates the new folder `connector`, which holds RSD GLASS® resources. Now you can govern the resources in the folder from RSD GLASS® and the changes will be reflected in the shared drive and vice versa.

5. Appendix: Introduction to Connectors

RSD GLASS® allows you to define information governance policies and have them applied across the organization. To apply policies and manage data, RSD GLASS® needs to communicate with different content repositories, such as, Google Drive, SharePoint, etc.

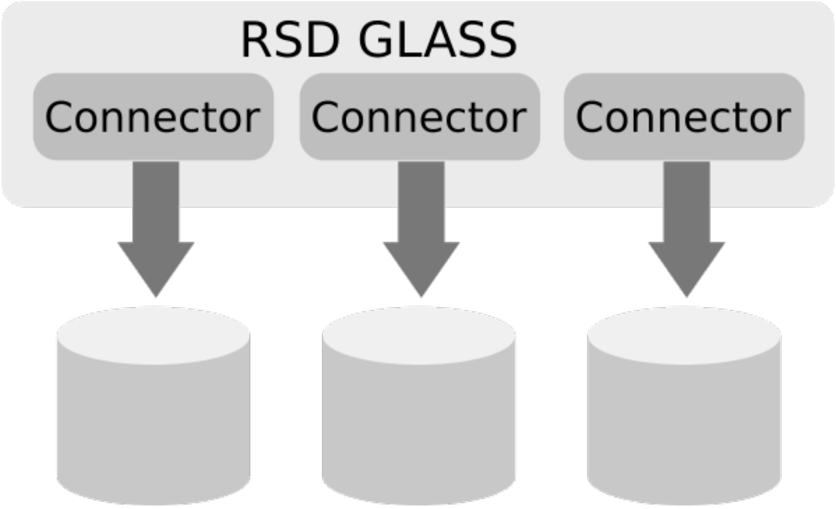


To accommodate such communication, RSD GLASS® comes with connectors for various repository types, including shared drives, general purpose systems, such as, Microsoft SharePoint and IBM FileNet, specialized business systems like SAP and Symantec Enterprise Vault, as well as cloud repositories such as Google Drive and Box.com.

RSD GLASS® uses connectors to connect to a repository, discover the stored information and applied policies, and manage the information life cycle for the repository. The abilities of individual connectors differ and each connector is classified depending on the extent of its capabilities (refer to *Connector Capabilities* on page 13).

> **Note:**
>
> All connectors connect to RSD GLASS® with the RSD GLASS® API for external connectors.

Figure 5: Connectors



5.1. Connector Capabilities

Each RSD GLASS® connector allows communication of RSD GLASS® with a repository. On the side of the repository is a GLASS driver that allows the repository to communicate with RSD GLASS®.

Level 1: Access-Only Connector

RSD GLASS® is able to capture information in the repository and access it through the connector. It does not allow you to store or delete information in the repository.

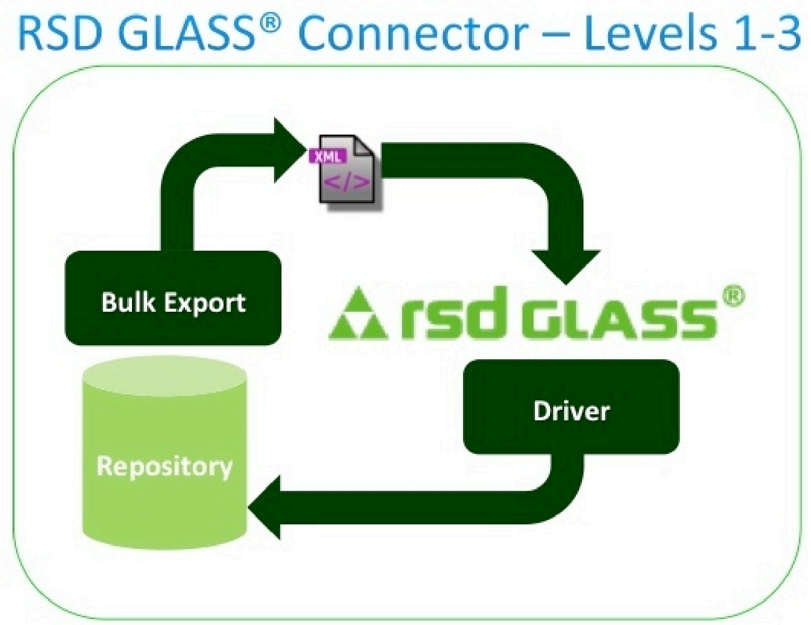
Level 2: Information Connector

RSD GLASS® is able to capture and access, as well as store and delete information. However, it cannot guarantee immutability of information, that is, information can be changed by other external processes or systems, even though locked by RSD GLASS®.

Level 3: Basic RM Connector

RSD GLASS® is able to capture and access, store and delete information and guarantee immutability of information: it can apply legal holds as well as records-management-level retention rules.

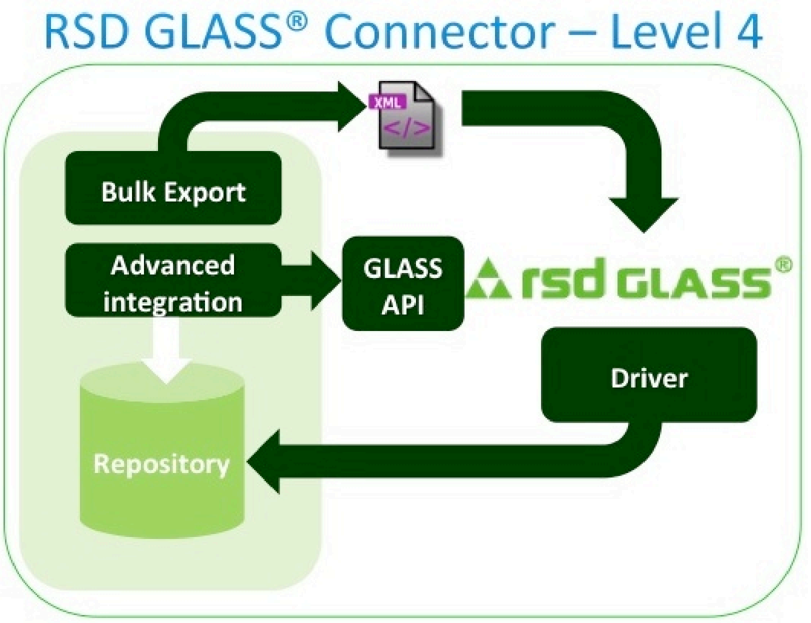
Figure 6: Schema of how a connector of level 1-3 works



Level 4: Optimized RM Connector

RSD GLASS® is able to capture and access, store and delete the information and guarantee immutability of information: it can apply legal holds as well as records-management-level retention rules. In addition it provides a rich interface integrated in the content application.

Figure 7: Schema of how a level-4 connector works



Table

Level	Batch export	Delete	Immutability	Integrated GUI
Level 1	X			
Level 2	X	X		
Level 3	X	X	X	
Level 4	X	X	X	X

For more information about RSD GLASS® connectors refer to the RSD GLASS® Connector Whitepaper.