Oracle DIVArchive Application Filtering

Feature Description

ORACLE TECHNICAL WHITE PAPER | UPDATED MAY 2015

Introduction

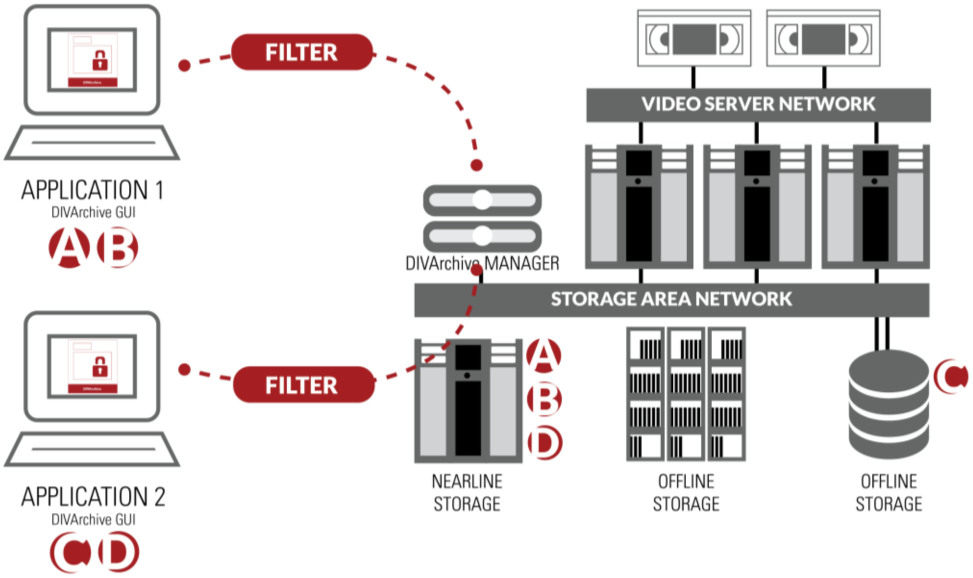
Oracle DIVArchive Application Filtering provides the capability to apply access filters based on the client application identification. Filters specify which archive resources—including object categories, media name (disk array or tape group), and source/destination servers—and which operations (archive, restore, or delete) are available to the applications connected to or controlling the overall Oracle DIVArchive solution.

Oracle DIVArchive Application Filtering enables several applications to share the archive resources while keeping their respective content private. Each application is only allowed to handle the content that it has access to.

Description

Oracle DIVArchive Application Filtering relies on the Access Gateway software component within the Oracle DIVArchive solution that acts as a manager proxy. Access Gateway software can run on the same server as the manager component or on a different server. It accepts connections from client applications, and then it applies certain access restrictions based on client identity. Restrictions specify which resources (categories, groups, or servers, for example) are available to the application.

All requests sent by client applications are delivered to the manager or rejected if they are not allowed due to access constraints configured for the application. Responses sent by the manager to the client are also filtered or edited according to access restrictions to remove information that should not be seen by a client application.



Application filtering process

Client applications are required to identify themselves by providing a username and a password when establishing connection with Access Gateway. Older clients that cannot provide explicit username and password credentials can be identified by the IP address of the system the request comes from.

Defining Filters

A **filter** is a restriction on a particular type of parameter. Every filter is specified with three attributes: type, value, and rights. Filters and client application identifications are specified in an access-conf.xml file.

Filter Type

The type attribute defines the type of checked parameter, such as the following:

- **objectCategory.** Object category filter.
- **objectName.** Object name filter.
- **mediaName.** Tape group or disk array filter; an application can be allowed to access only a limited set of media stored in the Oracle DIVArchive solution.
- **server.** Source, destination name, or path filter; an application can be limited to access content archived from one specific source.
- **message.** Constraint on message name; this is to restrict access to certain commands, such as insert tape, eject tape, and delete.

Filter Value

The value attribute is a comma-separated list of parameter values that apply to a filter. Values might also be shell regular expressions ('*' means 'any string'), such as the following:

- `value='ftp1,omneon*'`
  applies to parameter value ‘ftp1’ or any value starting with ‘omneon’
- `value='*'`
  applies to any parameter value

Filter Rights

The rights attribute specifies the type of access allowed by the filter, such as the following:

- **full.** Access without restrictions.
- **none.** No access at all.
- **read.** Read-only access; objects/groups/... can be listed or restored, but not archived, deleted, or copied.
- **ownObjects.** Access type specific for ‘message’ constraints. Means that the message (or command) can be applied to its own objects only, such as objects to which an application has full access.

Here are two examples of constraints:

```
<constraint type="category" value="public" access="full"/>
```

```
<constraint type="message" value="InsertTape,EjectTape,ExportTape" access="none"/>
```

The first constraint means this application has unrestricted access to objects whose category is “public.”

The second constraint means this application cannot execute insert, eject, or export commands.

Client Application Identification

Client identification is of the “login, password” type, and is sent by the application via the DIVA_Connect() request:

```
DIVA_STATUS DIVA_connect (
        DIVAString managerAddress,
        int        portNumber,
        DIVAString userName,
        DIVAString password,
        DIVAString applicationName
)
```

The components of the request above are defined as follows:

- **managerAddress.** IP address of Oracle DIVArchive Manager or Access Gateway.
- **portNumber.** Port on which Oracle DIVArchive Manager or Access Gateway is listening. The default port is pointed to by the constant value `DIVA_MGER_DEFAULT_PORT.`
- **username.** Username to log in to the Oracle DIVArchive system. If NULL or empty, the Oracle DIVArchive system will use the default username and privileges for this application.
- **Password.** Password for that user. Connection will be rejected if the password is incorrect.
- **applicationName.** Arbitrary string that is interpreted by the Oracle DIVArchive system as an application name. Used for information purposes only; may be `NULL` or empty string.

The call returns the same `DIVA_STATUS` values as the older no-user version of `DIVA_connect().` If the username or password is incorrect, the call will return `INVALID_PARAMETER` code, and the connection will not be established (closed).

Access Denied (DIVA_STATUS)

`ACCESS_DENIED` code can be returned by almost any API call if the message did not pass the access check. The application should be prepared to handle this value properly.

For compatibility reasons, API 5.8 and below will receive `INVALID_PARAMETER` status instead of `ACCESS_DENIED` if the message did not pass the check.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Hardware and Software, Engineered to Work Together

Application Filtering in DIVArchive: Feature Description
Updated May 2015