NetIQ® Directory and Resource Administrator Log Archive Resource Kit

Technical Reference

July 6, 2011

Contents

The NetIQ Directory and Resource Administrator Log Archive Resource Kit (DRA LARK) is a set of tools that allows you to directly view, query, and repair data stored in a log archive. The kit also includes tools to selectively reindex a log archive or specific log archive partitions and fix incorrect log archive statistics.

Legal Notice

Overview

NetIQ Directory and Resource Administrator (DRA) stores auditing data in a folder called a **log archive**, collecting and storing information relating to any operation that the local Administration server performs. Each Administration server has its own log archive installed by default. For more information about log archives and DRA, see the *User Guide* and *Administrator Guide*.

The **DRA Log Archive Resource Kit** (LARK) is a set of tools created specifically to allow you to directly access data stored in a log archive partition. The LARK enables you to view log archive data in its raw form, which can be useful for diagnostic purposes. In addition, you can use these tools to retrieve log archive data for use with other applications or fix log archive issues.

The tools contained in the LARK allow you to perform the following tasks:

- View data in a log archive partition, using the **Log Archive Data Viewer**.
- Query data in a log archive partition, using the **Log Archive Query** tool.
- Reindex data in one or all log archive partitions in a specific log archive, using the **Log Archive Reindexer** tool.
- Fix incorrect log archive statistics, using the **Log Archive Statistics Updater** tool.
- Repair corrupted log archive `VolumeInfo.xml` files, using the **Log Archive Volume Repair** tool.
- Re-export data previously exported for the reporting cube to upload, using the **Log Archive Report Data Exporter** tool.

You can only use the Log Archive Query, Log Archive Reindexer, Log Archive Statistics Updater, Log Archive Volume Repair, and Log Archive Report Data Exporter tools from the command line. However, you can run the Log Archive Data Viewer from Windows Explorer.

For more information about these tools, see the subsequent sections of this document.

Requirements

The DRA LARK requires DRA 8.5 or later. For more information about installing NetIQ Directory and Resource Administrator, see the *Installation Guide for Directory and Resource Administrator and Exchange Administrator*.

To install the Log Archive Resource Kit, you must have system administrator privileges on the installation computer. To use the Log Archive Resource Kit tools, you must have system administrator privileges and read permission on the log archive.

Installing the Log Archive Resource Kit

You can install the Log Archive Resource Kit during the installation of NetIQ Directory and Resource Administrator or install the LARK afterwards by using the Resource Kit setup program included in the DRA installation kit.

You can only install the Log Archive Resource Kit on Administration server computers. If you attempt to install the Resource Kit on a computer that does not have all Administration server components already installed, the setup program stops the installation.

To install the Log Archive Resource Kit:

1. Log on to an Administration server computer, using an account that is a member of the local Administrators group.
2. Navigate to *`installation kit`*`\intel\DRA`, where *`installation kit`* is the location of the DRA installation kit on the Administration server.
3. Run `LogArchiveResourceKit.msi` and follow the instructions provided by the NetIQ Directory and Resource Administrator Log Archive Resource Kit Setup Wizard.

   Note
   When prompted that the publisher cannot be verified, click **Run**.

4. Click **Close** when the setup program finishes installation.

You can uninstall the Log Archive Resource Kit using the setup program or by using the Control Panel. When you uninstall the Log Archive Resource Kit, the setup program removes only executable and configuration files from the computer. All user-created data, such as query results, remains on the Administration server computer.

Viewing Log Archive Data

The Log Archive Resource Kit provides a Log Archive Data Viewer you can use to directly view auditing data contained in log archive partitions on the local computer. This tool is primarily intended for troubleshooting purposes and allows you to view log archive data exactly as it is on the Administration server.

The navigation pane of the Data Viewer displays a list of all log archive partitions on the Administration server. When you expand the top-level `Logvolume` log archive in the navigation pane, the Data Viewer lists all partitions and files contained within the log archive. The Data Viewer also displays the total number of records in each selected log archive file, as well as the time range the file covers.

The Data Viewer displays only the most commonly used fields in the results pane. To view all available fields for a specific event, right-click and view the event properties in a separate window.

To refresh the data displayed by the Data Viewer, click on a different log archive partition and then click again on the current partition. If you want to view data for a newly created log archive partition, close and then restart the Data Viewer.

If the log archive contains a large amount of data, the Data Viewer may not open immediately. The Data Viewer displays its progress in the status bar at the bottom of the window. If you want to manually stop the Data Viewer from loading all data in the log archive, click **Cancel** in the status bar. The Data Viewer displays only data loaded up to that point.

Note
The Data Viewer only displays data stored in ungroomed or restored log archive partitions.

To view log archive data using the Data Viewer:

1. Log on to an Administration server computer where you want to view log archive data, using an account that is a member of the local Administrators group and has read permission on the log archive.
2. In Windows Explorer, navigate to *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`, where *`installation folder`* is the location where you installed Directory and Resource Administrator.

3. Start `LogArchiveDataViewer.exe`.
4. In the navigation pane, expand `Logvolume`.
5. Expand the log archive partition for which you want to view data.
6. Click the appropriate `.nds` file.

   The Data Viewer displays the data in the `.nds` file in the results pane.
7. ***If you want to manually stop the Data Viewer from opening,*** click **Cancel** in the status bar at the bottom of the window.
8. ***If you want to sort the data, choose one of the following options:***
   - Click the heading of the column by which you want to sort.
   - To sort a group of columns, press the Shift key while clicking the column headings.
   - To deselect a column, press the Ctrl key while clicking the column heading.
9. ***If you want to filter the data, choose one of the following options:***
   - Click the arrow button in the column heading by which you want to filter the data.
   - To remove a column filter to show all results, select **All**.
   - To specify a custom filter, select **Custom**.
   - To show only rows with empty cells in the filtered column, select **Blank**.
   - To omit rows with empty cells in the filtered column, select **Non blanks**.
   - To show only rows with a specific value in all cells in the filtered column, select the value.
10. ***If you want to group the data,*** drag and drop a column heading by which you want to group the data over the **Drag a column header here to group by that column** text.
11. ***If you want to view the details of a particular event, complete the following steps:***

    a. Right-click the event and select **Properties**.

    b. View the specific event properties.

    c. After you have finished viewing the event properties, click **OK**.
12. After you have finished viewing the data, on the File menu, click **Exit**.

Querying Log Archive Data

The kit includes a Log Archive Query tool for querying the log archive using query specifications you provide in an XML file. The tool runs on any DRA Administration server computer and finds those records that match the specified filter criteria. The criteria typically includes a date-time range, as well as values or ranges for other fields. You specify a file name and path for the resulting records and for the XML query file. The tool displays the matching records in the order found in the log archive.

For your convenience, the kit includes several sample XML query files (`.xml`). You can edit a sample XML query file to specify the query and output you want. For more information about sample query files, see "Sample Log Archive XML Query File" on page 9 and "Modifying a Sample Log Archive XML Query" on page 10.

Understanding the Log Archive XML Query

Query files in XML format provide the information for querying the log archive to find records matching specified criteria and for displaying the matching records. The XML file includes the following elements.

Query Root Element

The query file includes the `query` root element:

`query`

Specifies the entire multi-line query and contains `selectors` and `filter` child elements. As the root element, only one `query` element exists in the XML document. The `query` element includes a `count` attribute to specify the maximum number of matching records to return.

Notes

- You must specify a maximum number of records in the `count` attribute.
- You cannot sort the exported records. The tool saves the matching records to the output file in the order found in the log archive, until reaching the limit.

The following example shows an XML query framework with `query`, `selectors`, and `filter` elements:

```
<?xml version="1.0" encoding="utf-8" ?>
<query xmlns="http://www.netiq.com/schemas/sm/2006/07/query" count="10000">
<selectors>
……
</selectors>
<filter>
……
</filter>
</query>
```

The `query` root element includes two child elements, `selectors` and `filter`.

Selectors Element

The `selectors` element specifies the list of fields, using one or more `column` child elements, to retrieve from the matching records.

The following example shows an XML query `selectors` element:

```
<selectors>
<column id="5006" prettyName="Assistant Admin Name" dataType="string"/>
<column id="931" prettyName="Operation Name" dataType="string"/>
<column id="5015" prettyName="Action" dataType="dateTime"/>
<column id="564" prettyName="Event Message" dataType="string"/>
<column id="5066" prettyName="Local Date and Time" dataType="dateTime"/>
</selectors>
```

Each child `column` element describes one requested field:

`column`

Specifies a field or column to retrieve. The `selectors` `column` element contains three attributes: `id`, `prettyName`, and `dataType`.

Each child `column` element includes the following attributes to specify a requested field:

id

Specifies a unique numeric value identifying a single field.

Note

The `FieldMap.xml` file includes a list of the field IDs and their corresponding names and types. You can find this file in the `Log Archive Resource Kit` folder on the Administration server.

---

prettyName

Specifies a descriptive name you specify for the field. The `prettyName` is used as a display name for the requested field in the query output.

dataType

Specifies the data type of the field. For more information about supported types, see "Supported Field Data Types" on page 7.

Note

The data type of the field *must* match the type for the field in the `FieldMap.xml` file, located in the `Log Archive Resource Kit` folder on the Administration server.

Supported Field Data Types

The query XML supports the following data types:

string	Case-sensitive string value
short	16-bit signed integer
ushort	16-bit unsigned integer
int	32-bit signed integer
uint	32-bit unsigned integer
long	64-bit signed integer
ulong	64-bit unsigned integer
dateTime	Date-time in UNIX timestamp format, in milliseconds For more information about converting date-time values to timestamp format, see the Unix Time Conversion Web site at www.onlineconversion.com/unix_time.htm. Add three zeros to a value in seconds to convert it to milliseconds.

Filter Element

The `filter` element specifies the criteria for finding matching records. The criteria expression includes logical operators and one or more sets of match specifications, including criteria type, field, and corresponding values to match.

The `column` child element specifies the field and the `literal` child element specifies values. Criteria types, such as `between` and `equal`, allow you to specify exact values, ranges, or lists of values to match. These nested child elements represent a logical expression. The query tool evaluates each target record for a match, according to the criteria specification.

The following example shows an XML query `filter` element:

```
<filter>
<and>
```

```
<between>
<column id="5066" dataType="dateTime"/>
<literal>1199145600000</literal>
<!-- 1/1/2008-->
<literal>1306886400000</literal>
<!-- 6/1/2011-->
</between>
<equal>
<column id="5060" dataType="int"/>
<literal>1</literal>
</equal>
<equal>
<column id="5006" dataType="string"/>
<literal>Administrator</literal>
</equal>
</and>
</filter>
```

A *logical operator* element provides a way to join several expressions in determining a true match. A logical operator can only be a child of the `filter` element or a child of another logical operator. The XML query supports the following logical operators:

and

Joins all child elements with the `and` operator, meaning that *all* child subexpressions must evaluate true to make this expression true.

or

Joins all child elements with the `or` operator, meaning *any* child subexpression evaluating true makes this expression true.

not

Negates the result of the child subexpressions.

Filter *criteria types* specify the type of match to perform, including an exact match, a valid range, a list of values, or a wildcard expression. A criteria type must be a child of a logical operator element. The filter criteria includes the following criteria types:

equal

Specifies an exact match criteria. Provide one value or literal to match. The query tool compares the target value to a single case-sensitive value.

greaterThan

Specifies an exclusive numeric value range criteria. Provide one value or literal. Use numeric values for the `dateTime` data type. The query tool designates a match if the target value is greater than the specified criteria.

lessThan

Specifies an exclusive numeric value range criteria. Provide one value or literal. Use numeric values for the `dateTime` data type. The query tool designates a match if the target value is less than the specified criteria.

between

Specifies an inclusive numeric value range criteria. Provide a pair of literals, where the first literal is the smallest value and the second literal is the greatest value of the range. Use numeric values for the `dateTime` data type. The query tool designates a match if the target value is within the inclusive range.

in

Specifies a multiple value match criteria. Provide a list of values or literals. The query tool designates a match if the target value matches any of the values in the list.

like

Specifies a wildcard expression criteria. Provide one wildcard expression, using wildcards such as ? and *. The query tool designates a match if the target value interprets as a match to the wildcard expression.

The filter criteria defines the fields or columns and corresponding values for finding matching records. Every criteria type includes two child elements, `column` and `literal`.

`column`

Specifies a field or column to use in determining matching records. The filter column element contains two attributes, `id` and `dataType`.

Note
The `FieldMap.xml` file includes a list of the field IDs and their corresponding names and types. You can find this file in the `Log Archive Resource Kit` folder on the Administration server.

A filter column element must have the following attributes to specify a field:

`id`

Specifies a unique numeric value identifying a single field.

Note
The `FieldMap.xml` file includes a list of the field IDs and their corresponding names and types. You can find this file in the `Log Archive Resource Kit` folder on the Administration server.

`dataType`

Specifies the data type of the field. For more information about supported types, see "Supported Field Data Types" on page 7.

Note
The data type of the field *must* match the type for the field in the `FieldMap.xml` file, located in the `Log Archive Resource Kit` folder on the log archive server.

`literal`

Specifies one or more values for the specified column to use in determining matching records. The query tool evaluates each target value for a match, in the context of the criteria type.

Sample Log Archive XML Query File

The sample log archive XML query file in this section specifies the following:

- A maximum of 10,000 matching records to return.
- Twenty-three columns to display for each matching record in the output file.
- A filter for a date range of January 1, 2011 through June 1, 2011.
- A filter for operation status of `Success`.
- A filter for Assistant Admin name equal to `Administrator`.

The following sample log archive XML query file illustrates how to specify the log archive query and output columns:

```
<?xml version="1.0" encoding="utf-8" ?>
<query xmlns="http://www.netiq.com/schemas/sm/2006/07/query" count="10000">
<selectors>
<column id="5060" prettyName="Operation Status" dataType="int"/>
<column id="5006" prettyName="Assistant Admin Name" dataType="string"/>
<column id="931" prettyName="Operation Name" dataType="string"/>
<column id="5015" prettyName="Action" dataType="dateTime"/>
<column id="5070" prettyName="Object Type" dataType="string"/>
<column id="5013" prettyName="DRA Server Name" dataType="string"/>
<column id="5025" prettyName="Object Friendly Name" dataType="string"/>
<column id="5008" prettyName="Assistant Admin OnePoint Path" dataType="string"/>
<column id="5010" prettyName="Object OnePoint Path" dataType="string"/>
<column id="5007" prettyName="Assistant Admin GUID" dataType="string"/>
<column id="5066" prettyName="Local Date and Time" dataType="dateTime"/>
<column id="5011" prettyName="Transaction ID" dataType="string"/>
<column id="5030" prettyName="Object GUID" dataType="string"/>
<column id="5083" prettyName="Source Object Friendly Name" dataType="string"/>
<column id="924" prettyName="Object Domain" dataType="string"/>
<column id="5012" prettyName="Domain Controller" dataType="string"/>
<column id="5086" prettyName="Source Object OnePoint Path" dataType="string"/>
<column id="5085" prettyName="Source Object GUID" dataType="string"/>
<column id="5091" prettyName="Member GUID" dataType="string"/>
<column id="5097" prettyName="Member Friendly Name" dataType="string"/>
<column id="5098" prettyName="Member OnePoint Path" dataType="string"/>
<column id="5099" prettyName="Member Type" dataType="string"/>
<column id="564" prettyName="Event Message" dataType="string"/>
</selectors>
<filter>
<and>
<between>
<column id="5066" dataType="dateTime"/>
<literal>1293840000000</literal><!-- 1/1/2011-->
<literal>1306886400000</literal><!-- 6/1/2011-->
</between>
<equal>
<column id="5060" dataType="int"/>
<literal>1</literal>
</equal>
<equal>
<column id="5006" dataType="string"/>
<literal>Administrator</literal>
</equal>
</and>
</filter>
</query>
```

Modifying a Sample Log Archive XML Query

For your convenience, two sample XML query (`.xml`) files are included in the same directory as `LogArchiveQuery.exe`. You can edit a sample XML query file to specify the query and output you want.

Use this example procedure to edit filter criteria for matching records, as well as the maximum output records and columns to display.

To modify a sample query for the Log Archive Query tool:

1. Log on to an Administration server computer where you want to query log archive data, using an account that is a member of the local Administrators group and has read permission on the log archive.
2. Navigate to *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`, where *`installation folder`* is the location where you installed Directory and Resource Administrator.
3. Open a sample `.xml` file, such as `SampleQuery1.xml`.
4. Save the sample `.xml` file using a new name, such as `DataQuery1.xml`.

5. ***If you want to change the fields displayed for matching records,*** complete the following steps:

   a. Locate the following line:

   ```
   <selectors>
   ```

   b. In the `<selectors>` section, change the existing `column` attributes to contain the `id`, `prettyName`, and `dataType` values for the fields you want to display in the matching records. For example, you can specify these fields to display:

   ```
   <column id="5060" prettyName="Operation Status" dataType="int"/>
   <column id="5006" prettyName="Assistant Admin Name" dataType="string"/>
   <column id="5066" prettyName="Local Date and Time" dataType="dateTime"/>
   <column id="5011" prettyName="Transaction ID" dataType="string"/>
   <column id="5037" prettyName="Object Container Friendly Name"
   dataType="string"/>
   <column id="5040" prettyName="Object Container OnePoint Path"
   dataType="string"/>
   <column id="5030" prettyName="Object GUID" dataType="string"/>
   <column id="5039" prettyName="Object Container GUID" dataType="string"/>
   ```

   Note
   The `FieldMap.xml` file includes a list of the field IDs and their corresponding names and types. You can find this file in the `Log Archive Resource Kit` folder on the Administration server.

6. ***If you want to change the date-time range,*** complete the following steps:

   a. Locate the `dateTime` lines in the `<filter>` section, such as:

   ```
   <between>
   <column id="5066" dataType="dateTime"/>
   <literal>1293840000000</literal>
   <!-- 1/1/2011-->
   <literal>1306886400000</literal>
   <!-- 6/1/2011-->
   </between>
   ```

   b. Change the `<literal>` values to the desired starting and ending date-time in UNIX timestamp format, in milliseconds.

   Note
   For more information about converting date-time values to UNIX timestamp format, see the Unix Time Conversion Web site at www.onlineconversion.com/unix_time.htm. After converting a date-time value to UNIX timestamp format, add three zeros to a value in seconds to convert it to milliseconds.

   For example, type `1294358400000` in the first value to indicate a 1/7/2011 starting date and type `1302134400000` in the second value to indicate a 4/7/2011 ending date, as shown:

   ```
   <between>
   <column id="503" dataType="dateTime" />
   <literal>1294358400000</literal>
   <!--  1/7/2011  -->
   <literal>1302134400000</literal>
   <!--  4/7/2011  -->
   </between>
   ```

7. ***If you want to specify a particular Assistant Admin,*** in the `<filter>` section, locate the `column id="5006"` line and change the `<literal>` value to the desired user name, for example:

   ```
   <equal>
     <column id="5006" dataType="string" />
     <literal>BobM</literal>
   </equal>
   ```

8. Save and close the file.

Using the Log Archive Query Tool

You can run the program `LogArchiveQuery.exe` from the command line on a DRA Administration server.

Note
The Log Archive Query tool does not require the `NetIQ DRA Log Archive` service to be running.

To query log archive data:

1. Log on to an Administration server computer where you want to query log archive data, using an account that is a member of the local Administrators group and has read permission on the log archive.
2. Open a command prompt and type the following command:

   `cd` *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`

   Where *`installation folder`* is the location where you installed Directory and Resource Administrator.
3. At the command prompt, type the following command:

   `LogArchiveQuery.exe` *`QueryXMLPath OutputPath`*

   Where:

   `QueryXMLPath` is the path and file name of a `.xml` file containing the query criteria.

   Records matching the query criteria are saved to the output file, in the order found in the log archive. For more information about query criteria, see "Understanding the Log Archive XML Query" on page 6.

   `OutputPath` is the path and file name where you want to save the matching records.

Reindexing Log Archive Data

The Log Archive Resource Kit provides a Log Archive Reindexer tool for selecting specific log archive partitions to reindex. The tool allows you to specify a whole log archive or a specific partition to reindex, as necessary.

You can use the reindexer to troubleshoot issues with previously indexed log archive data. The reindexer only reindexes partitions that need to be reindexed. You do not need to run the reindexer unless you are experiencing problems with indexed log archive partitions. You can also use the tool with the `CHECKONLY` option to evaluate existing log archive index data before reindexing.

The reindexer prepares the specified log archive partition for processing by the `NetIQ DRA Log Archive` service, queueing indexing processes for the `Log Archive` service. You must restart the `Log Archive` service after running the reindexer.

Note

- The reindexer does not perform the reindexing process itself. The `Log Archive` service reindexes all log archive data.
- The reindexer does not reindex all auditing data in a partition, but compares the partition data against the existing index and determines which data needs to be reindexed.
- The specified log archive partitions remain in their current state after you run the reindexer. When you restart the `Log Archive` service, the service starts reindexing the partitions prepared by the reindexer.
- After you restart the `Log Archive` service, the service both reindexes the specified partitions and imports and indexes new data at the same time. The service does not wait until the reindexing is complete to start importing new data.
- Do not re-run the reindexer until the `Log Archive` service finishes reindexing the partitions currently in progress. For information on verifying the service has finished reindexing, see Step 6 in "Reindexing Specific Log Archive Partitions" on page 14.
- NetIQ does not recommend reindexing the entire log archive at one time unless absolutely necessary. Reindexing all partitions in the log archive could take a significant amount of time.
- When you run the reindexer, you must specify the name of the log archive index private message queue, as configured on your Administration server.

By default, the reindexer does not reindex closed partitions. Use the `INCLUDECLOSED` parameter to override this behavior. You can only reindex ungroomed log archive partitions.

Evaluating Log Archive Partitions for Reindexing

If you want to evaluate a specific log archive partition before reindexing, you can run the `LogArchiveReindexer.exe` program with the `CHECKONLY` option to check the status of the existing index data without performing the reindexing process.

Run the program `LogArchiveReindexer.exe` from the command line on a DRA Administration server.

To evaluate a log archive partition:

1. Log on to an Administration server computer where you want to evaluate existing log archive index data, using an account that is a member of the local Administrators group and has read and write permission on the log archive.
2. Open a command prompt and type the following command:

   `cd` *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`

   Where *`installation folder`* is the location where you installed Directory and Resource Administrator.
3. At the command prompt, type the following command:

   `LogArchiveReindexer.exe Logvolume` *`LogArchivePartitionName`* `CHECKONLY`

Where *LogArchivePartitionName* is the name of the specific log archive partition you want to evaluate, if applicable. `Logvolume` is the name of the top-level DRA log archive and remains the same in every DRA installation.

Notes

- If you do not include the `CHECKONLY` option, the tool does not evaluate the specified log archive partitions but reindexes the specified log archive partitions.
- If you do not specify a particular log archive partition, the reindexer tool checks all ungroomed partitions within the log archive.
- The reindexer cannot evaluate the log archive partition for the current day. You can only use the tool to evaluate past log archive partitions.

4. Close the command prompt.

Reindexing Specific Log Archive Partitions

You can run the program `LogArchiveReindexer.exe` from the command line on a DRA Administration server.

To reindex a log archive partition:

1. Log on to an Administration server computer where you want to reindex log archive data, using an account that is a member of the local Administrators group and has read and write permission on the log archive.
2. Open a command prompt and type the following command:

   `cd` *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`

   Where *installation folder* is the location where you installed Directory and Resource Administrator.
3. At the command prompt, type the following command:

   `LogArchiveReindexer.exe Logvolume` *`LogArchivePartitionName`* `[INCLUDECLOSED]`

   Where *LogArchivePartitionName* is the name of the specific log archive partition you want to reindex, if applicable. `Logvolume` is the name of the top-level DRA log archive and remains the same in every DRA installation.

   Notes

   - If you do not specify a particular log archive partition, the reindexer tool reindexes all open, ungroomed partitions within the log archive.
   - If you include the `INCLUDECLOSED` option, the reindexer tool reindexes all ungroomed partitions within the log archive, including closed partitions.
   - You can run the reindexer tool multiple times before restarting the `Log Archive` service. Each time you run the reindexer on a specific log archive partition, the tool queues that partition to be reindexed the next time you restart the service.
   - When you reindex a closed log archive partition, the reindexer reopens the closed partition. The `Log Archive` service closes the partition after the service reindexes the reopened partition.
   - The reindexer cannot reindex the log archive partition for the current day. You can only use the tool to reindex past log archive partitions.

4. Repeat Step 3 for each log archive partition you want to reindex.

5. Restart the `NetIQ DRA Log Archive` service.

Note
When you restart the `NetIQ DRA Log Archive` service, your Administration server is temporarily unable to collect auditing data.

6. ***If you want to verify that the `Log Archive` service is processing the specified log archive partitions,*** complete the following steps:

   a. In Windows Explorer, navigate to *`installation folder`*`\NetIQ\DRA\NetIQLogArchiveData\index_data`, where *`installation folder`* is the location where you installed Directory and Resource Administrator.

   b. Click **View > Refresh** until Windows Explorer displays several files in the folder.

   c. Note the number of `AVAILABLE` files, then continue clicking **View > Refresh**. As the `Log Archive` service reindexes log archive partitions, the number of `AVAILABLE` files should decrease. When the number of files in the folder remains relatively steady, the service has finished reindexing.

7. Close the command prompt.

Updating Log Archive Statistics

In some Directory and Resource Administrator installations, Directory and Resource Administrator may incorrectly calculate the size of the log archive on an Administration server when manually reindexing. These incorrect calculations can cause the log archive to appear to be larger than it actually is. Using these erroneous statistics, Administration servers may generate incorrect warning messages that the log archive is full.

The Log Archive Resource Kit provides a Log Archive Statistics Updater tool for recalculating statistics for all ungroomed, closed log archive partitions on an Administration server. You cannot update statistics for groomed log archive partitions or the log archive partition for the current day.

You can run the program `UpdateStatistics.exe` from the command line on a DRA Administration server.

Note
- You must stop the `NetIQ DRA Log Archive` service before updating log archive statistics.
- The statistics updater does not recalculate statistics for index or temporary files located in the log archive folder on the Administration server.

To update log archive statistics:

1. Log on to an Administration server computer where you want to update log archive statistics, using an account that is a member of the local Administrators group and has read and write permission on the log archive.

2. ***If you want to check your current log archive statistics before running the tool,*** complete the following steps:

   a. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.

   b. Click **Log Archive Statistics**.

   c. Note the total size of the log archive in the **Data Size on Disk** column.

3. Stop the `NetIQ DRA Log Archive` service.
4. Open a command prompt and type the following command:

   `cd` *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`

   Where *`installation folder`* is the location where you installed Directory and Resource Administrator.
5. At the command prompt, type the following command:

   `UpdateStatistics.exe`
6. Start the `NetIQ DRA Log Archive` service.
7. ***If you want to verify that the Update Statistics tool updated your log archive statistics,*** complete the following steps:

   a. Start **Log Archive Configuration** in the NetIQ Security Manager > Configuration program group.

   b. Click **Log Archive Statistics**.

   c. Review the total size of the log archive in the Data Size on Disk column.

   Note
   - Due to the method Microsoft Windows uses to calculate folder size, the value Directory and Resource Administrator displays in the Data Size on Disk column differs slightly from the value Microsoft Windows displays in the folder properties.
   - If you do not see a significant change in the Data Size on Disk column, the statistics for the log archive may have been correct before you ran the tool.
8. Close the command prompt.

Re-Exporting Report Data

After you export data from a log archive partition for use in Reporting Center reports, Directory and Resource Administrator does not include a mechanism to re-export that same data a second time to the reporting server. If your Administration server becomes corrupted or experiences a failure of some kind, you may lose your exported log archive data.

The Log Archive Resource Kit provides a Log Archive Report Data Exporter tool that allows you to re-export previously exported log archive data for use in Reporting Center. The tool uses the configuration options specified in the Log Archive Configuration utility on your Administration server.

You can run the program `LogArchiveReportDataExporter.exe` from the command line on a DRA Administration server.

Notes
- You must stop the `NetIQ DRA Log Archive` service before running the Log Archive Report Data Exporter tool.
- The Log Archive Report Data Exporter tool begins re-exporting log archive data immediately after you enter the `LogArchiveReportDataExporter.exe` command.

To re-export previously exported log archive data:

1. Log on to an Administration server computer where you want to re-export log archive data, using an account that is a member of the local Administrators group and has read permission on the log archive.
2. Stop the `NetIQ DRA Log Archive` service.
3. Open a command prompt and enter the following command:

   `cd` *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`

   Where *`installation folder`* is the location where you installed Directory and Resource Administrator.
4. At the command prompt, type the following command:

   `LogArchiveReportDataExporter.exe Logvolume` *`LogArchivePartitionName`*

   Where *`LogArchivePartitionName`* is the name of the specific log archive partition you want to re-export. `Logvolume` is the name of the top-level DRA log archive and remains the same in every DRA installation.

   Notes
   - You can only use the tool to re-export one log archive partition at a time. You must specify the name of a particular log archive partition.
   - The re-export tool exports each `.nds` file within a specific log archive partition sequentially in numeric order.
5. Close the command prompt.
6. Start the `NetIQ DRA Log Archive` service.

Repairing Log Archive Volumes

In certain circumstances, the `VolumeInfo.xml` file that stores the configuration information for the DRA log archive may become corrupted or may be accidentally deleted. If the Administration server cannot access a valid `VolumeInfo.xml` file, Directory and Resource Administrator cannot generate reports on Assistant Admin actions.

The Log Archive Resource Kit provides a Log Archive Repair tool to recreate the `VolumeInfo.xml` file for the DRA log archive, based on information from the log archive partitions in the log archive.

Note
- You must stop the `NetIQ DRA Log Archive` service before running the Log Archive Repair tool.
- If a `VolumeInfo.xml` file exists, the repair tool does not delete the existing file. When you run the repair tool, the tool moves any existing `VolumeInfo.xml` file to a new folder in the log archive called `OldVolumeInfo` and renames the file `VolumeInfo.old.X.xml`, where `X` is incremented each time you run the repair tool on a particular log archive.
- If partitions have previously been groomed from the DRA log archive and you then run the repair tool, the tool attempts to recover data on groomed partitions from the corrupted `VolumeInfo.xml` file. If there is no `VolumeInfo.xml` file, or if the basic structure of the `VolumeInfo.xml` file is corrupted, the tool may not be able to recover groomed partition information.
- If any log archive partitions within the log archive are also corrupt, the repair tool cannot recreate the `VolumeInfo.xml` file.

Run the program `LogArchiveVolumeRepairTool.exe` from the command line on a DRA Administration server.

To repair the log archive `VolumeInfo.xml` file:

1. Log on to an Administration server computer where you want to evaluate existing log archive index data, using an account that is a member of the local Administrators group and has read and write permission on the log archive.
2. Stop the `NetIQ DRA Log Archive` service.
3. Open a command prompt and enter the following command:

   `cd` *`installation folder`*`\NetIQ\DRA\Log Archive Resource Kit`

   Where *`installation folder`* is the location where you installed Directory and Resource Administrator.
4. At the command prompt, type the following command:

   ```
   LogArchiveVolumeRepairTool.exe Logvolume
   ```

   Note
   `Logvolume` is the name of the top-level DRA log archive and remains the same in every DRA installation.
5. Close the command prompt.
6. Start the `NetIQ DRA Log Archive` service.