

IBM Security Directory Server  
Version 6.3.1.5

*Reporting Guide*





IBM Security Directory Server  
Version 6.3.1.5

## *Reporting Guide*



**Note**

Before using this information and the product it supports, read the general information under "Notices" on page 17.

**Edition notice**

**Note:** This edition applies to version 6.3.1.5 of *IBM Security Directory Server* (product number 5724-J39 ) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2014.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>About this publication</b> . . . . .	<b>v</b>
Access to publications and terminology . . . . .	v
Accessibility . . . . .	vii
Technical training . . . . .	vii
Support information . . . . .	vii
Statement of Good Security Practices. . . . .	vii

<b>IBM Security Directory Server audit reporting</b> . . . . .	<b>1</b>
Prerequisites for audit reporting . . . . .	2
Audit reporting configuration . . . . .	3
Creating and configuring the audit database. . . . .	3
Installing and configuring IBM Cognos reporting components. . . . .	3

Importing the reporting package. . . . .	4
Creating a data source . . . . .	5
Configuring the log management tool . . . . .	6
Globalization . . . . .	6
Setting language preferences . . . . .	7
Report model objects . . . . .	8
Query subjects for Audit namespace . . . . .	8
Query items for Audit namespace . . . . .	9
Creating custom reports . . . . .	13

<b>Index</b> . . . . .	<b>15</b>
------------------------	-----------

<b>Notices</b> . . . . .	<b>17</b>
--------------------------	-----------



---

## About this publication

IBM® Security Directory Server, previously known as IBM Tivoli® Directory Server, is an IBM implementation of Lightweight Directory Access Protocol for the following operating systems:

- Microsoft Windows
- AIX®
- Linux (System x®, System z®, System p®, and System i®)
- Solaris
- Hewlett-Packard UNIX (HP-UX) (Itanium)

*IBM Security Directory Server Reporting Guide* contains information about tools and software to generate directory server reports.

---

## Access to publications and terminology

This section provides:

- A list of publications in the “IBM Security Directory Server library.”
- Links to “Online publications” on page vi.
- A link to the “IBM Terminology website” on page vi.

### IBM Security Directory Server library

The following documents are available in the IBM Security Directory Server library:

- *IBM Security Directory Server, Version 6.3.1.5 Product Overview*, GC27-6212-01  
Provides information about the IBM Security Directory Server product, new features in the current release, and system requirements information.
- *IBM Security Directory Server, Version 6.3.1.5 Quick Start Guide*, GI11-9351-02  
Provides help for getting started with IBM Security Directory Server. Includes a short product description and architecture diagram, and a pointer to the product documentation website and installation instructions.
- *IBM Security Directory Server, Version 6.3.1.5 Installation and Configuration Guide*, SC27-2747-02  
Contains complete information for installing, configuring, and uninstalling IBM Security Directory Server. Includes information about upgrading from a previous version of IBM Security Directory Server.
- *IBM Security Directory Server, Version 6.3.1.5 Administration Guide*, SC27-2749-02  
Contains instructions for administrative tasks through the Web Administration tool and the command line.
- *IBM Security Directory Server, Version 6.3.1.5 Reporting Guide*, SC27-6531-00  
Describes the tools and software for creating reports for IBM Security Directory Server.
- *IBM Security Directory Server, Version 6.3.1.5 Command Reference*, SC27-2753-02  
Describes the syntax and usage of the command-line utilities included with IBM Security Directory Server.

- *IBM Security Directory Server, Version 6.3.1.5 Server Plug-ins Reference* , SC27-2750-02  
Contains information about writing server plug-ins.
- *IBM Security Directory Server, Version 6.3.1.5 Programming Reference*, SC27-2754-02  
Contains information about writing Lightweight Directory Access Protocol (LDAP) client applications in C and Java™.
- *IBM Security Directory Server, Version 6.3.1.5 Performance Tuning and Capacity Planning Guide*, SC27-2748-02  
Contains information about tuning the directory server for better performance. Describes disk requirements and other hardware requirements for directories of different sizes and with various read and write rates. Describes known working scenarios for each of these levels of directory and the disk and memory used; also suggests rules of thumb.
- *IBM Security Directory Server, Version 6.3.1.5 Troubleshooting Guide*, GC27-2752-02  
Contains information about possible problems and corrective actions that can be taken before you contact IBM Software Support.
- *IBM Security Directory Server, Version 6.3.1.5 Error Message Reference*, GC27-2751-02  
Contains a list of all warning and error messages associated with IBM Security Directory Server.

## Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

### IBM Security Directory Server documentation website

The <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm> site displays the documentation welcome page for this product.

### IBM Security Systems Documentation Central and Welcome page

IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product documentation. You can also find links to the product documentation for specific versions of each product.

Welcome to IBM Security Systems documentation provides and introduction to, links to, and general information about IBM Security Systems documentation.

### IBM Publications Center

The <http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss> site offers customized search functions to help you find all the IBM publications you need.

## IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.



---

## Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For more information, see the Accessibility Appendix in the *IBM Security Directory Server Product Overview*.

---

## Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

---

## Support information

IBM Support assists with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

*IBM Security Directory Server Troubleshooting Guide* provides details about:

- What information to collect before you contact IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

**Note:** The **Community and Support** tab on the product information center can provide additional support resources.

---

## Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



---

# IBM Security Directory Server audit reporting

IBM Security Directory Server provides tools and software to generate audit reports that are based on the audit log files.

## Ready-to-use reports

The following ready-to-use static reports are provided:

### Configuration Changes Audit Report

Enables administrators to generate reports about changes to directory server configuration.

The reports are based on the following input parameters:

- Start date and time
- End date and time

### LDAP Authentication Audit Report

Enables administrators to generate reports on bind events and failed bind events.

The reports are based on the following input parameters:

- Start date and time
- End date and time
- User bind DN
- Client IP
- Operation result

### LDAP Password Policy Violation Report

Enables administrators to generate reports on attempts to modify user passwords that failed because of password policy violation.

The reports are based on the following input parameters:

- Start date and time
- End date and time
- User bind DN

### Long-Running Searches Report

Enables administrators to generate reports on search operations that took more than the specified time to complete.

The reports are based on the following input parameters:

- Start date and time
- End date and time
- Operation response time in milliseconds

### User Activity Audit Report

Enables administrators to generate reports about user operations.

The reports are based on the following input parameters:

- Start date and time
- End date and time
- User bind DN

## Custom reports

You can also generate custom audit reports with Cognos® Workspace Advanced. For more information, see “Creating custom reports” on page 13

---

## Prerequisites for audit reporting

You must meet the prerequisites before you configure audit reporting for IBM Security Directory Server.

IBM Security Directory Server supports IBM Cognos Business Intelligence Server version 10.2.1.

You must install the following software:

### **IBM Cognos Business Intelligence Server, Version 10.2.1.**

To install this software, see the procedure in the *Install* section of the IBM Cognos Business Intelligence 10.2.1 documentation. Complete the steps in the topic, Installing and Configuring Product Components on One Computer.

### **Web server**

To see the supported web servers, follow these steps:

1. On the home page of the IBM Cognos Business Intelligence 10.2.1 documentation, click the **IBM Cognos 10.2.1 Business Intelligence software environments** link.
2. On the *IBM Cognos Business Intelligence 10.2 Supported Software Environments*, click the **10.2.1** tab.
3. In the *IBM Cognos Business Intelligence 10.2.1* section, under the **Requirements by type** column, click the **Software** link.
4. On the *Related software for Cognos Business Intelligence 10.2.1* page, search for the *Web Servers* section.
5. Ensure that one of these supported web servers is installed on your system.

### **Data sources**

To see the supported data sources, follow these steps:

1. On the home page of the IBM Cognos Business Intelligence 10.2.1 documentation, click the **IBM Cognos 10.2.1 Business Intelligence software environments** link.
2. On the *IBM Cognos Business Intelligence 10.2 Supported Software Environments*, click the **10.2.1** tab.
3. In the *IBM Cognos Business Intelligence 10.2.1* section, under the **Requirements by type** column, click the **Software** link.
4. On the *Related software for Cognos Business Intelligence 10.2.1* page that is displayed, search for the *Data Sources* section. Ensure that one of these supported data sources is installed and configured on your system.

### **IBM Security Directory Integrator**

For the log management tool to work, you must install IBM Security Directory Integrator Version 7.1.0.8 or later. For installation instructions, see the *Installation* section in the IBM Security Directory Integrator documentation.

---

## Audit reporting configuration

Before you can generate audit reports, you must install and configure several components.

- Audit database
- IBM Cognos reporting components
- Reporting package
- Data source
- Log management tool

The following topics describe the steps to install and configure these components.

### Creating and configuring the audit database

The audit database is a DB2 database, where all the audit events from the audit log file of directory server instance are dumped. You can create and configure the audit database by using the scripts that are provided when you install IBM Security Directory Server.

#### About this task

IBM Security Directory Server audit reporting supports only DB2 database.

#### Procedure

1. Install DB2 on the system where you want the audit database to be created.
2. Copy the **idscfgauditdb** utility and the `sdsAuditDB.sql` file from the following locations:

##### UNIX systems

```
sds_install_dir/report/idscfgauditdb
```

```
sds_install_dir/report/sdsAuditDB.sql
```

##### Windows systems

```
sds_install_dir\report\idscfgauditdb.cmd
```

```
sds_install_dir\report\sdsAuditDB.sql
```

3. Place both the files in the same directory on the system where you want the audit database to be created.
4. Run the **idscfgauditdb** utility with appropriate parameters. See **idscfgauditdb** utility in the IBM Security Directory Server documentation.

#### Results

The audit database instance, database, and the tables are created.

#### What to do next

Install and configure the reporting components.

### Installing and configuring IBM Cognos reporting components

After you configure the audit database, you must install and configure the IBM Cognos reporting components.

## About this task

During the database configuration process, complete the following steps:

- Set the JAVA\_HOME environment variable to point to the JVM that is used by the application server.
- Use the enterprise database as IBM Cognos content store.
- Delete the existing data source and create a new data source to enable an option of generating DDL during creation of the content store database. For information about data source creation, see *Creating a data source*.

All of the following procedures for installing IBM Cognos reporting components are available in the IBM Cognos Business Intelligence 10.2.1 documentation.

## Procedure

1. Ensure that Cognos Business Intelligence is installed according to the instructions in the prerequisites.
2. IBM Security Directory Server installs the audit reports. You can find the reports at *sds\_install\_dir/report/SDSAuditReportingPackage.zip*.
3. After you install the Cognos Business Intelligence server, create a content store in the database. Complete the steps in the following topics, according to your operating system:
  - a. Start IBM Cognos Configuration.
  - b. Create a content store database.
4. Configure the web gateway. Complete the steps in the topic, *Installing and configuring the gateway*.
5. Configure the web server. Complete the steps in the topic, *Configuring the web server*.

## What to do next

Import the reporting package.

## Importing the reporting package

Import the reporting package to work with the bundled report models and the static reports.

## Before you begin

Complete the following steps before you import the reporting package:

- Copy the reporting package file *SDSAuditReportingPackage.zip* to the directory where your deployment archives are saved. The default location is *c10\_location/deployment*. See *“Installing and configuring IBM Cognos reporting components”* on page 3.
- To access the Content Administration area in IBM Cognos Administration, you must have the required permissions for the administration tasks secured feature.

## Procedure

1. Access the IBM Cognos Gateway URI.

### Example:

```
https://hostname:portnumber/ibmcognos/cgi-bin/cognos.cgi
```

where

The *hostname* is the IP address or network host name where IBM Cognos gateway is configured.

The *portnumber* is the port on which the IBM Cognos gateway is configured.

2. Click **Launch**.
3. In the IBM Cognos Administration window, click the **Configuration** tab.
4. Click **Content Administration**.
5. Clear the history.
6. On the toolbar, click **New Import** icon. The New Import wizard opens.
7. From the **Deployment Archive** list, select `SDSAuditReportingPackage.zip`.
8. Click **Next**.
9. In the **Specify a name and description** field, add the description and screen tip.
10. Click **Next**.
11. In the **Select the public folders and directory** field, select the model that is displayed.
12. On the Specify the general options page, indicate whether to include access permissions and references to external namespaces and an owner for the entries after they are imported.
13. Click **Next**. The summary information opens.
14. Review the summary information and then click **Next**.
15. On the Select an action page, click **Save and run once**.
16. After the import file operation is submitted, click **Finish**.

## Results

You can now use the reporting package to create reports and to run the sample reports. The sample reports are available in the reporting model on the **Public Folders** tab in the IBM Cognos portal.

## What to do next

Create a data source

## Creating a data source

To work with the IBM Security Directory Server Cognos reporting, you must create a data source.

### About this task

- You must use the data source name, `SDSAudit`.
- Copy the file `db2cli.dll` from the DB2 client installation directory to the *IBM Cognos installation directory/bin* folder.
- The data source must point to the audit database. See “Creating and configuring the audit database” on page 3.

### Procedure

To create a data source, go to the IBM Cognos Business Intelligence 10.2.1 documentation and complete the steps in the topic, Create a Data Source

## What to do next

Configure the log management tool to dump audit events into the audit database.

## Configuring the log management tool

Configure the log management tool to dump audit events into the audit database.

### About this task

The original log management tool for IBM Directory Server is now enhanced. It can read and parse the audit events from the audit log and dump into the audit database. For more information about the audit database, see “Creating and configuring the audit database” on page 3.

To configure the log management tool to dump audit events into the audit database, you must update the audit database properties file at `sds_install_dir/idstools/idslogmgmt/idsauditdb.properties`.

### Procedure

1. Open the `idsauditdb.properties` file.
2. Set the value of the **IDS\_AUDITDB\_JDBCURL** property to the host name or IP address of the audit database.
3. Set the value of **IDS\_AUDITDB\_JDBCUSERNAME** property to the DB2 instance owner for the audit database.
4. Set the value of **IDS\_AUDITDB\_JDBCPASSWORD** to the instance owner password.
5. Log in to the system where the directory server instance is running by using the directory server instance owner's credentials.
6. Set the environment variable **IDS\_LOGMGMT\_ENABLE\_AUDIT\_COGNOS** to true.
7. Run the log management tool by using the following command:  

```
idslogmgmt -I instance name
```

**Note:** For security reasons, after step 7, it is suggested that you clear **IDS\_AUDITDB\_JDBCPASSWORD** value in `sds_install_dir/idstools/idslogmgmt/idsauditdb.properties`.

### Results

The log management tool reads, parses, and dumps the audit events from the directory server instance audit log file in to the audit database.

## What to do next

You can now create IBM Security Directory Server audit reporting from IBM Cognos.

---

## Globalization

You can use the globalization features of IBM Security Directory Server audit reporting package to produce the reports in your own language.



## Supported languages

IBM Security Directory Server Cognos reports support the following languages:

- cs=Czech
- de=German
- en=English
- es=Spanish
- fr=French
- hu=Hungarian
- it=Italian
- ja=Japanese
- ko=Korean
- pl=Polish
- pt\_BR=Brazilian Portuguese
- ru=Russian
- sk=Slovakian
- zh\_CN=Simplified Chinese
- zh\_TW=Traditional Chinese

**Note:** Custom reports are supported only in the English language.

## Messages

In the reports, some of the column values might display the message, "Language not supported." This message is displayed when you select a language that is not supported by the reporting model.


## Setting language preferences

You can personalize the way data appears in IBM Cognos workspace by changing your preferences. You can set the product language or content language to get the preferred output format of the reports.

### Before you begin

Install and configure the IBM Cognos Business Intelligence Server.

### Procedure

1. In the IBM Cognos Connection window, click **My Area Options**  .
2. Click **My Preferences**.
3. In the Set Preferences window, under the Regional options section, select **Product language**. Product language specifies the language that is used by the IBM Cognos user interface.
4. In the Set Preferences window, under the Regional options section, select **Content language**. Content language specifies the language that is used to view and produce content in IBM Cognos, such as data in the reports.
5. Click **OK**.

## Results

You can view the reports or user interface in the language that you specified.

---

## Report model objects

Use the information about the objects and the report model names, namespaces, and entities to work with the report models for creating custom audit reports.

### Query Items

The smallest piece of the model in a report. It represents a single characteristic of something, such as the date that a product was introduced.

Query subjects or dimensions contain query items. For example, a query subject that references an entire table contains query items that represent each column in the table.

Query items are the most important objects for creating reports. They use query item properties of query items to build their reports.

### Query Subjects

A set of query items that have an inherent relationship. In most cases, query subjects behave like tables. Query subjects produce the same set of rows regardless of which columns were queried.

### Packages

A subset of the dimensions, query subjects, and other objects that are defined in the project. A package is published to the IBM Cognos server. It creates reports, analyses, and ad hoc queries.

### Namespaces

Uniquely identifies query items, dimensions, query subjects, and other objects. You import different databases into separate namespaces to avoid duplicate names.

**Note:** The namespace for the Security Directory Server audit reporting model is named as Audit.

## Query subjects for Audit namespace

The namespace for the Security Directory Server audit reporting model is named as Audit. The query subjects in the Audit namespace are listed here.

### LDAP Audit

Represents the combination of all header and common attributes in an audit event for an IBM Security Directory Server instance. For example: audit version, timestamp, bind DN, client IP and port, operation result, LDAP client controls and criticality, operation response time, and so on.

### Audit Add

Represents the event attributes that are applicable only to an LDAP Add event. For example: Entry and Attributes.

### Audit Bind

Represents the event attributes that are applicable only to an LDAP Bind event. For example: Authentication Choice, Authentication Mechanism, and so on.

**Audit Compare**

Represents the event attributes that are applicable only to an LDAP Compare event. For example: Entry and Attribute.

**Audit Delete**

Represents the event attributes that are applicable only to an LDAP Delete event. For example: Entry.

**Audit ExtendedOp**

Represents the event attributes that are applicable only to an LDAP Extended Operation event. For example: OID.

**Audit ModifyDN**

Represents the event attributes that are applicable only to an LDAP ModifyDN event. For example: Entry, NewRDN, DeleteOldRDN, and NewSuperior.

**Audit RegEventNotify**

Represents the event attributes that are applicable only to an LDAP Event registration notification event. For example: event ID, base, and scope and operation type.

**Audit Search**

Represents the event attributes that are applicable only to an LDAP search event. For example: base, scope, filter, derefAliases, typesOnly, attributes, and entriesReturned.

**Audit UnregEventNotify**

Represents the event attributes that are applicable only to an LDAP event unregister notification event. For example: ID.

## Query items for Audit namespace

The query items in the Audit namespace are listed here.

**LDAP Audit**

The LDAP Audit query subject has the following query items:

**Audit Version**

Represents the audit version. If the audit version is 3, then **Audit Version** is AuditV3.

**Audit Timestamp**

Represents the time stamp when the event was audited. It corresponds to the time stamp that is present in the header part of the audit log.

**Event Type**

Represents the operation type such as, V3 Bind, V3 Modify, and so on. It corresponds to the operation type that is present in the audit header.

**Bind DN**

Represents the bind DN. For V3 unauthenticated or anonymous requests, this field is < \*CN=NULLDN\* >. It corresponds to the bind DN in the audit header.

**Client IP**

Represents the client IP from the audit header.

**Client Port**

Represents the client port from the audit header.

**Connection ID**

Represents the LDAP connection ID. It corresponds to the `connectionID` attribute from the audit header.

**Received Timestamp**

Represents the time stamp when the request was received. It corresponds to the `received` attribute from the audit header.

**Operation Result**

Shows the result or status of the LDAP operation. It corresponds to the result string from the audit header.

**Unique ID**

The unique request ID to be stored in the control. The Client IP is the client's original IP to be stored in the control. If `critical` is true the criticality of the control will be set to true; if false the criticality will be set to false.

**Audit Control Client IP**

Represents the client IP that is sent in the Audit control. It corresponds to the `ClientIP` attribute from the audit log.

**Request ID**

Represents the request ID that is sent in the additional information, if the control is the Audit control and server audit is configured to audit the additional information. It corresponds to the `RequestID` attribute from the audit log.

**Normalized**

Represents the `Normalized` attribute from the additional information that is sent on the group authorization control. The value is TRUE or FALSE.

**Control Value****Authorization Group**

Represents the group name that is sent on a Group authorization control, if the server audit is configured to audit the group. It corresponds to the `Group` attribute from the audit log.

**LDAP Control And Criticality**

Represents the string that represents the LDAP control and its criticality, which is sent in the request. It corresponds to a combination of control and criticality attributes from the audit log.

**Proxy DN**

Represents the proxy DN, if the control is a Proxy authorization control. It corresponds to the `ProxyDN` attribute from the audit log.

**Operation Response Time**

Represents time difference in milliseconds between the time when the request was received and the time when its response was sent. It corresponds to the `operationResponseTime` attribute from the audit log.

**Time on WorkQ**

Represents time in milliseconds, which was spent by the request in the worker queue before the execution was initiated on the operation. It corresponds to `timeOnWorkQ` attribute from the audit log.

**Rdbm Lock Wait Time**

Represents time in milliseconds, which was spent in acquiring locks over RDBM caches during operation execution. It corresponds to `rdbmLockWaitTime` attribute from the audit log.

**Client IO Time**

Represents time in milliseconds that was spent in receiving the complete operation request and returning the complete operation response. It corresponds to the `clientIOTime` attribute from the audit log.

**Audit Add**

The Audit Add query subject has the following query items:

**Add Entry**

Represents the DN of the entry that was added. It corresponds to the `entry` attribute from the LDAP Add event.

**Add Attributes**

Represents the attributes of the entry that was added. It corresponds to the `attributes` attribute from the LDAP Add event.

**Audit Bind**

The Audit Bind query subject has the following query items:

**User Name**

Represents the DN of the entry that did the bind. It corresponds to the `name` attribute from the Bind event.

**Authentication Choice**

Corresponds to the `authenticationChoice` attribute from the LDAP Bind event. The valid values are `unknown`, `simple`, `krbv42LDAP`, `krbv42DSA`, or `sasl`.

**Authentication Mechanism**

Corresponds to the `authenticationMechanism` attribute from the LDAP Bind event.

**Mapped Name**

Corresponds to the `mappedname` attribute from the LDAP Bind event.

**Authz ID**

Corresponds to the `authzId` attribute from the LDAP Bind event.

**Admin Account Status**

Corresponds to the `Admin Acct Status` attribute from the LDAP Bind event. The valid values are `Not Locked`, `Locked`, or `Lock Cleared`.

**Passthrough Bind DN**

Represents the bind DN used by IBM Security Directory Server to bind to a pass-through directory. It corresponds to `passthroughBindDN` attribute from the audit log.

**Passthrough Server**

Represents the host name IP address and port of the pass-through directory. It corresponds to `passthroughServer` attribute from the audit log.

**Passthrough Bind RC**

Represents the return code from the pass-through directory. It corresponds to `passthroughBindRC` attribute from the audit log.

### **Audit Compare**

The Audit Compare query subject has the following query items:

#### **Compare Entry**

Represents the DN of the entry on which the compare operation was done. It corresponds to the entry attribute from the LDAP Compare event.

#### **Compare Attribute**

Represents the name of the attribute on which the compare operation was done. It corresponds to the attribute attribute from the LDAP Compare event.

### **Audit Delete**

The Audit Delete query subject has the following query items:

#### **Delete Entry**

Represents the DN of the entry that was deleted. It corresponds to the entry attribute from the LDAP Delete event.

### **Audit ExtendedOp**

The Audit ExtendedOp query subject has the following query item:

**OID** Represents the OID of the extended operation that was done. It corresponds to the 0ID attribute from the LDAP extended event.

### **Audit ModifyDN**

The Audit ModifyDN query subject has the following query items:

#### **ModifyDN Entry**

Represents the DN of the entry on which the ModifyDN operation was done. It corresponds to the entry attribute from the LDAP ModifyDN event.

#### **New RDN**

Represents the new RDN attribute of the LDAP entry on which ModifyDN operation was done. It corresponds to the newrdn attribute from the LDAP ModifyDN event.

#### **Delete Old RDN**

Indicates whether the old RDN attribute was deleted from the LDAP entry. It corresponds to the deleteoldrdn attribute from the LDAP ModifyDN event.

#### **New Superior**

Represents the DN of the new parent of the LDAP entry on which the ModifyDN operation was done. It corresponds to the newSuperior attribute from the LDAP ModifyDN event.

### **Audit Modify**

The Audit Modify query subject has the following query items:

#### **Modify Object**

Represents the DN of the entry on which the Modify operation was done. It corresponds to the object attribute from the LDAP Modify event.

#### **Modify Action And Attribute**

Shows a list of the combination of modify actions and names of the attributes that were involved in the Modify operation.

### **Audit RegEventNotify**

The Audit RegEventNotify query subject has the following query items:

**Event ID**

Represents the ID the event that was registered. It corresponds to the eventID attribute from the audit log.

**RegEventNotify Base**

Represents the DN of the subtree for which the event is registered. It corresponds to the base attribute from the audit log.

**RegEventNotify Scope**

Represents the scope of the operation. It corresponds to the scope attribute from the audit log.

**Operation Type**

Represents the type of operations for which the event registration was done. It corresponds to the type attribute from the audit log.

**Audit Search**

The Audit Search query subject has the following query items:

**Search Base**

Represents the search base that is used in the LDAP Search operation. It corresponds to the base attribute from LDAP Search event.

**Search Scope**

Represents the search scope that is used in the LDAP Search operation. It corresponds to the scope attribute from the LDAP Search event.

**Deref Aliases**

Indicates whether the server must dereference the aliases. It corresponds to the derefAliases attribute from the LDAP Search event.

**Filter** Represents the search filter that is used in the Search operation. It corresponds to the filter attribute from the LDAP Search event.

**Types Only**

Indicates whether the Search operation is requesting attributes only. It corresponds to the typesOnly attribute from the LDAP Search event.

**Search Attributes**

Represents the list of attributes that were requested in the search request. It corresponds to the attributes attribute from the LDAP Search event.

**Entries Returned**

Represents the number of entries that were returned in the Search operation. It corresponds to the numberOfEntriesReturned attribute from the LDAP Search event.

**Audit UnregEventNotify**

The Audit UnregEventNotify query subject has the following query item:

**ID** Represents the ID of the event that was unregistered. It corresponds to the ID attribute from the audit log.

---

## Creating custom reports

You can use the IBM Cognos Workspace Advanced to create the custom audit reports.

## Procedure

1. In the IBM Cognos Workspace, insert the common query items from the LDAP Audit query subject.
2. Based on the event types, insert more query items from the event-specific query subjects. For example, to create a custom audit report for LDAP Compare operations, you can insert the following query items:
  - Audit Version
  - Audit Timestamp
  - Event Type
  - Bind DN
  - Client IP
  - Operation Response Time

Now, all the audit events that are available in the audit database would be displayed.

3. Add a custom filter. For example, you can add a custom filter on Event Type to include just the Compare events. Now, only the events that are related to LDAP Compare operations would be displayed.
4. Insert any more query items that you require from the event-specific query subject, for example, Audit Compare.
5. Save the report in the format that you require.



---

# Index

## A

- accessibility vii
- audit
  - logs 1
  - reports 1
    - configuring 3, 4, 6
    - creating custom 14
    - creating data source 5
    - data source creation 5
    - globalization 7
    - importing 4
    - installing 4
    - languages 7
    - log management tool 6
    - messages 7
    - model objects 8, 9
    - prerequisites 2
    - query items 9
    - query subjects 8
- audit database
  - configuring 3
  - creating 3

## C

- configuring
  - audit database 3
  - audit reporting components 4
  - reporting components 4
- creating
  - audit database 3
  - audit reporting data source 5
  - data source for audit reports 5
- custom reports
  - creating 14

## D

- data source
  - creating 5

## E

- education vii

## I

- IBM
  - Software Support vii
  - Support Assistant vii
- importing
  - audit reporting package 4
  - reporting package 4
- installing
  - audit reporting components 4
  - reporting components 4

## L

- log management tool
  - configuring for audit reports 6

## O

- online
  - publications v
  - terminology v

## P

- problem-determination vii
- publications
  - accessing online v
  - list of for this product v

## Q

- query items
  - audit reports 9
- query subjects
  - audit reports 8

## R

- reporting components
  - configuring 4
  - installing 4
- reporting package
  - importing 4
- reports
  - audit 7, 8, 9, 14
  - configuring 3
    - log management tool 6
  - creating custom 14
  - globalization 7
  - languages 7
  - messages 7
  - model objects 8, 9
  - query items 9
  - query subjects 8

## T

- terminology v
- training vii
- troubleshooting vii



---

## Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

## **Trademarks**

IBM, the IBM logo, and [ibm.com](http://ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.





Printed in USA

SC27-6531-00

