EVIDEN

Identity and Access Management

DirX Directory

LDAP Extended Operations

Version 9.1, Edition June 2025

Table of Contents

Preface

This manual is reference for the DirX Directory (DirX). It consists of the following sections:

- Chapter 1 contains reference pages for LDAP extended operations.

DirX Directory Documentation Set

DirX Directory provides a powerful set of documentation that helps you configure your directory server and its applications.

The DirX Directory document set consists of the following manuals:

- *DirX Directory Introduction*. Use this book to obtain a description of the concepts of DirX Directory.
- *DirX Directory Administration Guide*. Use this book to understand the basic DirX Directory administration tasks and how to perform them with the DirX Directory administration tools.
- *DirX Directory Administration Reference*. Use this book to obtain reference information about DirX Directory administration tools and their command syntax, configuration files, environment variables and file locations of the DirX Directory installation.
- *DirX Directory Syntaxes and Attributes*. Use this book to obtain reference information about DirX Directory syntaxes and attributes.
- *DirX Directory LDAP Extended Operations*. Use this book to obtain reference information about DirX Directory LDAP Extended Operations.
- *DirX Directory External Authentication*. Use this book to obtain reference information about external authentication.
- *DirX Directory Supervisor*. Use this book to obtain reference information about the DirX Directory supervisor.
- *DirX Directory Plugins for Nagios*. Use this book to obtain reference information about DirX Directory plugins for Nagios.
- *DirX Directory Disc Dimensioning Guide*. Use this book to understand how to calculate and organize necessary disc space for initial database configuration and enhancing existing configurations.
- *DirX Directory Guide for CSP Administrators*. Use this book to obtain information about installing, configuring and managing DirX Directory in the context of a Certificate Provisioning Service operating in accordance with regulations like the German “Signaturgesetz”.
- *DirX Directory Release Notes*. Use this book to install DirX Directory and to understand the features and limitations of the current release.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory**/DirX Identity* on UNIX systems and **C:\Program Files\DirX\Identity** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

1. DirX Directory LDAP Extended Operations

The LDAP "extended operation" concept is part of LDAPv3. Its purpose is to provide a mechanism for defining additional operations for services that are not available in the protocol. An LDAP extended operation allows a client to send an extended operation request to a server that supports the extended operation. The client includes the identifier of the extended operation to be performed and extended operation-specific data. The server performs the extended operation and then returns a response which can contain an identifier and/or data. For the complete description of the LDAP extended operation, see Section 4.12, “Extended Operation” in the *Lightweight Directory Access Protocol (v3)*, RFC 4511, June 2006.

The DirX Directory LDAP server provides support for LDAP extended operations. These operations are mainly for directory support and monitoring purposes, and provide management information base (MIB) table data and other diagnostic data of the DirX Directory server processes. The description of the **dirxextop** command in the *DirX Directory Administration Reference* provides more information about these operations.

1.1. Invoking DirX Directory LDAP Extended Operations

Use the **dirxextop** command or the **Monitoring** view in DirX Directory Manager to perform an LDAP extended operation.

1.2. Configuring DirX Directory LDAP Extended Operations

The extended operations **ldap_cfg_defaults**, **ldap_ext_info**, **ldap_show_config_dsas**, **ldap_ssl_ciphernames** and **startTLS** are performed without any restriction or authentication.The **LDAP Extended Operations Admins** (ldapExtOpAdmins) attribute and the **LDAP Extended Operations Admin Group** (ldapExtOpAdminGroups) attribute of the LDAP server configuration subentry controls the accessibility of all other extended operations; that is, the distinguished name specified in the **-D** option must be one of the values of the **LDAP Extended Operations Admins** attribute or the **LDAP Extended Operations Admin Groups** attribute to be allowed to perform an extended operation.For information about attributes for specifying more fine-grained access rights to LDAP extended operations, see the section **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attrributes*.

1.3. DirX Directory DSA LDAP Extended Operations Reference Descriptions

The following sections provide reference descriptions for LDAP extended operations performed by the DirX Directory DSA.

1.3.1. dsa_ac_log_on

1.3.1.1. Synopsis

dsa_ac_log_on [*parameter1*; *parameter2*; ...]

1.3.1.2. Purpose

Enables access control (AC) logging.

1.3.1.3. Parameters

parameter1; *parameter2*; ...
One or more parameters to restrict the logging output to the information that is relevant to a particular type of operation. Specify the parameter in the format:

parameter_name=parameter_value

Use a semicolon (;) to separate multiple parameters.

There are two types of parameter:

- Non-volatile parameters
- Volatile parameters

Non-volatile parameters are stored and are in effect while the DSA process is running. They are updated only when the operation is called with the same parameter. Volatile parameters are in effect only for the extended operation to which they are attached.

The following table provides the name, the type, a description and the default value for each parameter:

parameter_name	**Volatility**	**Description**	**Default Value**
max_file_no	non-volatile	Controls the maximum number of log files used by the round robin mechanism.	**10**
max_no_lines	non-volatile	Controls the maximum number of lines in each log file.	**10000**
flush	non-volatile	If set to **1**, fflush is called when a line is written. The information can be read from the log file immediately.	**0**
entry	volatile	Specifies the DN of an entry in LDAP format. Only sections of entries with a matching DN are written to the log file.	all

parameter_name	Volatility	Description	Default Value
requestor	volatile	Specifies the DN of the requestor in LDAP format. Only sections with a matching requestor DN are written to the log file. When filtering for anonymous sections, specify the keyword **anonymous** for the parameter value.	all
permission_category	volatile	Specifies the permission. Specify a comma-separated list of the following values: • **add** • **disclosureOnError** • **read** • **remove** • **browse** • **export** • **import** • **modify** • **rename** • **returnDN** • **compare** • **filterMatch**	all
auth_level	volatile	Specifies the authentication level. Specify a comma-separated list of the following values: • **none** • **simple** • **strong** • **other**	all

parameter_name	Volatility	Description	Default Value
protected_item	volatile	Specifies the protected item. Specify a comma-separated list of the following values: • **wholeEntry** • **userAttribute** • **userAttributeValue** • **operationalAttribute** • **operationalAttributeValue**	all
attribute	volatile	Specify a comma-separated list of LDAP attribute names.	all

1.3.1.4. Description

Use the **dsa_ac_log_on** LDAP extended operation to enable a special AC logging. This logging is useful for analysis of the effects of the configured access control items contributing to an access control decision.

On success, the DSA returns the string **AC logging is successfully enabled**.

The resulting log file is an ASCII textfile written to *install_path*/server/log*. The name of the log file is:

DSA_AC*pid.file_number*

Use the parameters to restrict the logging to the information that is relevant to a particular type of operation.

1.3.1.5. Example

In the following example, access control logging is enabled for the entry **cn=Digger,ou=Development,o=My-Company**. Access control logging is enabled for **filterMatch**, **browse**, and **read** operations:

```
dirxextop -D cn=admin,o=my-company -w dirx -t dsa_ac_log_on
-P entry=cn=Digger,ou=Development,o=My-Company;
permission_category=filterMatch,browse,read
```

On success, the LDAP extended operation returns the message:

```
AC logging is successfully enabled
```

Here is a snippet from a log file written after the command above has been performed successfully:

```
Con9_Op10         Wed Mar 24 14:22:01.588000     DAPThread
ACDF was called               R: cn=admin,o=My-Company           AL:
simple            PI: user attribute              DN:
cn=Digger,ou=Development,o=My-Company        ATTR: telephoneNumber
PC: read
Con9_Op10         List of all processed ACIs ordered by precedence:
Con9_Op10                         - Admin: enable most of operations
(permission: 2 - grant)
Con9_Op10                         - Admin: enable most of operations
(permission: 1 - grant)
Con9_Op10                         - Public Access: enable Read and
Search - disable Read password (permission: 3 - deny)
Con9_Op10                         - Users: can Modify their passwords
and telephoneNumbers (permission: 1 - grant)
Con9_Op10                         - Users: can Modify their passwords
and telephoneNumbers (permission: 2 - grant)
Con9_Op10                         - Public Access: enable Read and
Search - disable Read password (permission: 1 - grant)
Con9_Op10                         - Public Access: enable Read and
Search - disable Read password (permission: 2 - grant)
Con9_Op10         "Admin: enable most of operations (permission: 1 -
grant)" is discarded because the requested item is not included.
Con9_Op10         "Public Access: enable Read and Search - disable
Read password (permission: 3 - deny)" has lower precedence than the
lastly added relevant ACI. This and every further ACIs are discarded.
Con9_Op10         List of relevant ACIs:
Con9_Op10                         - Admin: enable most of operations
(permission: 2 - grant)
Con9_Op10         "Admin: enable most of operations (permission: 2 -
grant)" was selected as the most specific ACI.
Con9_Op10         Access granted.
```

1.3.1.6. See Also

dsa_ac_log_off, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in the *DirX Directory Syntaxes and Attributes*, **X.500 Security Features** in the *DirX Directory Introduction*.

1.3.2. dsa_ac_log_off

1.3.2.1. Synopsis

dsa_ac_log_off

1.3.2.2. Purpose

Disables access control (AC) logging.

1.3.2.3. Description

Use the **dsa_ac_log_off** LDAP extended operation to disable the AC logging.

On success, the DSA returns the string **AC logging is successfully disabled**.

Existing log files are preserved in the log folder. If logging is enabled again logging is continued in the next file of the round robin sequence.

1.3.2.4. Example

The following example access control logging is disabled:

```
dirxextop -D cn=admin,o=my-company -w dirx -t dsa_ac_log_off
```

On success, the LDAP extended operation returns the message:

AC logging is successfully disabled

1.3.2.5. See Also

dsa_ac_log_on, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in the *DirX Directory Syntaxes and Attributes*, **X.500 Security Features** in the *DirX Directory Introduction*.

1.3.3. dsa_dbam_aac

1.3.3.1. Synopsis

dsa_dbam_aac help |
  list [**bt=***begin_time* **et=***end_time*] |
  reset [**all**] |
  show [*index*] |
  start [**bt=***begin_time* **interval=***interval_spec* [*no_of_intervals*]] |
  status |
  stop

1.3.3.2. Purpose

Manages the DBAM AVIDX access counter (AAC) statistic histories. In the AAC statistic histories, the DSA records how often an attribute index is used in search operations.

The AAC statistic histories consist of a permanent statistic history with the index 0 and up to 54 statistic histories with the indexes 1 through 54. In the permanent statistic history, the DSA permanently records how often an attribute index is used in search operations. All other statistic histories are overwritten when the maximum number of statistics (54 statistics) is exceeded (first in first out) or a reset, start or stop command is performed.

The AAC statistic histories help an administrator to manage the attribute indexes and optimize the performance of search operations. For example, the administrator can identify attribute indexes that are never used and can then delete these attribute indexes.

1.3.3.3. Commands

1.3.3.4. help

Returns help information about the **dsa_dbam_aac** extended operation and its commands. The syntax is as follows:

dsa_dbam_aac help

1.3.3.4.1. Description

The **help** command returns brief information about each **dsa_dbam_aac** command.

1.3.3.4.2. Example

```
dsa_dbam_acc help
```

The sample command output is:

Usage :

```
help            |
list            [bt=begin-time] [et=end-time] |
reset           [all] |
show            [index] |
start           [begin-time interval-spec [no-of-intervals]] |
status          |
stop

begin-time,
```

```
end-time              : GeneralizedTime format as local time. Example
                      20151224105930
interval-spec         : <count><time-unit>. Example : 6H

                      <count> : positive integer starting from 1

                      <time-unit> : single character specifies time

                      unit, like H (hour), D (day),

                      W (week), M (month)
index                 : integer in the range 0 to 54
no-of-intervals       : positive integer
```

1.3.3.5. list

Lists available AAC statistics histories. The syntax is as follows:

dsa_dbam_aac list [*bt=*begin_time* *et=**end_time*]

1.3.3.5.1. Arguments

bt=*begin_time*
The statistic history start time in GeneralizedTime local time format.

*et=**begin_time*
The statistic history end time in GeneralizedTime local time format.

1.3.3.5.2. Description

The **dsa_dbam_aac list** command lists the available AAC statistics histories. When specified without any arguments, the command lists all available AAC histories. Use the arguments *bt=**begin-time* or *et=**end-time* or both to reduce the list. The list always starts with the most recent statistic history in descending order.

The output format of the command is as follows:

index [**M**|**S**] *begin_time*[*end_time*]

where

index is an integer value in the range **1** to **54**. The permanent AAC statistic has index 0 and is not listed. The permanent statistic is maintained continuously. The administrator does not have any control over this statistic.

The letter **M** indicates manual creation; that is, to start maintenance the AAC statistic histories a reset or start command was performed. The letter **S** indicates scheduled creation of the statistic history.

begin_time and *end_time* are timestamps in GeneralizedTime syntax and show the start

and end of the statistic history period. The *end_time* stamp is not displayed because the most recent statistic is not completed.

To display the details of an AAC statistic; that is, how often an attribute index is used in search operations during the statistic history period, use the **dsa_dbam_aac show** command.

1.3.3.5.3. Example

```
dsa_dbam_aac list
```

The output is as follows:

```
4 M 20150701000000
3 M 20150601000000 20150701000000
2 M 20150501000000 20150601000000
1 M 20150401000000 20150501000000
```

1.3.3.6. reset

Discontinues the maintenance of AAC statistics histories. The syntax is as follows:

dsa_dbam_aac reset [**all**]

1.3.3.6.1. Arguments

all
Removes all statistic histories and all AAC statistic history configuration.

1.3.3.6.2. Description

The **dsa_dbam_aac reset** command, when specified without any arguments, stops AAC statistic history maintenance and removes all statistic histories. Use the **all** argument to remove the AAC statistic history configuration data in addition to the statistic histories themselves.

1.3.3.6.3. Example

```
dsa_dbam_aac reset
```

1.3.3.7. show

Displays the counters of a specific ACC statistic history. The syntax is as follows:

dsa_dbam_aac show [*index*]

1.3.3.7.1. Arguments

index
An integer value in the range **0** to **54** that specifies the index of the AAC history. Index **0** is the default index and returns the current statistic of the permanent AAC. Index **1** to **54** returns the AAC statistic history associated with the specified *index*.

1.3.3.7.2. Description

The **dsa_dbam_aac show** command, when specified without any arguments, returns the current statistic of the permanent AAC (index 0). Use the *index* argument to return a specific AAC statistic history.

Use the **dsa_dbam_aac list** command to display all available AAC statistic histories if you do not know which statistics are available.

The output format contains a one-line header, followed by a two-line column description, followed by the multi-lined statistic counter. The counters provide information how often an attribute index was used in search operations. The statistic counters are always sorted in descending order. The hyphen character (-) indicates that the specific sub index is not configured.

For the permanent AAC statistic, the counters of all attribute indexes are displayed. The permanent AAC statistic header includes the time stamp in local time format of the last time the counters were saved to the DBAM block.

For all other statistic histories, the counters of a maximum of 400 attribute indexes are displayed. The AAC statistic history header includes the begin time and the end time in GeneralizedTime format.

1.3.3.7.3. Example

The following sample command returns the permanent AAC statistic:

```
dsa_dbam_aac show
```

The output provides details for all attribute indexes. The output is as follows:

```
Attribute access counter high score at Sat Jul 04 10:12:55 2015 :
Attribute name           : Index access counter
                         :      INITIAL        FINAL     CONTAINS
PRESENT
objectClass              :   1911746899            -           -
19207113
dxmADsSamAccountName     :   1790575257            -           -
0
cn                       :   1167586108         1920           -
```

```
0
dxrUserLink                :    758424228            -             -
56807545
employeeNumber             :    518684159           27             -
554491
dxrAssignFrom              :    407342374            -             -
2
dxrPrimaryKey              :    379713170            -             2
51063
l                          :    125345929            -             -
0
dxrIsPrimary               :     77805510            -             -
0
ou                         :     70507888            -             -
0
dxrProject                 :     55199743            -             -
0
dxrGroupMemberOK           :     48085760            -             -
1
modifyTimestamp            :     37452904            0             -
0
dxrState                   :     29984514            0             -
25212874
uniqueMember               :     12856898            -             -
0
departmentNumber           :     11149186            2             8
1059223
dxrRoleParamValue          :            0            0       8093945
19
dxrPrivilegeLink           :      5091699            -             -
4399664
dxrGroupMemberDelete       :      3957360            -             -
78910
```

In the output, you can see that the last AAC statistic history was saved at **Sat Jul 04 10:12:55 2015**. The objectClass attribute INITIAL index was the attribute index that was used most frequently in search operations, and the dxrGroupMemberDelete attribute indexes most infrequently.

The following sample command returns the AAC statistic history for index 3:

```
dsa_dbam_aac show 3
```

The output provides details for a maximum of 400 attribute indexes that were used in search operations most frequently. The output is as follows:

```
ttribute access counter high score from 20150601000000 to
20150630235959:
Attribute name           : Index access counter
                         :      INITIAL        FINAL     CONTAINS
PRESENT
uid                      :     14910248            -           -
105
dxmOprOriginator         :       333476            -           -
0
objectClass              :       237635            -           -
20
employeeNumber           :       153928            -           -
0
member                   :        53968            -           -
0
sn                       :        22345            -           7
33
modifyTimestamp          :         6581            -           -
0
cn                       :         4196            -           -
0
createTimestamp          :          579            -           -
0
description              :          236            -           -
0
memberOf                 :          213            -           -
0
ou                       :           21            -           -
175
uniqueMember             :          175            -           -
0
l                        :          165            -           -
0
```

In the output, you can see that this AAC statistic history was recorded between 1 June 2015

and 30 June 2015.

1.3.3.8. start

Directs DBAM to start a new AAC statistic history. The syntax is as follows:

dsa_dbam_aac start [*bt=*begin_time* *interval=*interval_spec* [*no_of_intervals*]]

1.3.3.8.1. Arguments

bt=*begin_time*
The start time of a new scheduled AAC statistic history in GeneralizedTime localtime format.

interval=*interval_spec*
The time period after which DBAM collects the number of attribute index accesses in search operations. Specify *interval_spec* in the format *count time-unit* where *count* is an integer value and *time-unit* is one of the following characters:

- **S** or **s** for seconds
- **H** or **h** for hours
- **D** or **d** for days
- **W** or **w** for weeks
- **M** or **m** for months

no_of_intervals
An integer value that specifies the number of intervals after which DBAM stops the AAC statistic history.

1.3.3.8.2. Description

The **dsa_dbam_aac start** command, when specified without any arguments, stops a previously started AAC statistic history and immediately starts a new AAC manual statistic history. DBAM stores the start and end times of the previous statistic history and the current AAC counters in a DBAM statistic history block and then initiates the creation of the new history. To finish the current period, invoke the stop command or invoke a start command.

If a begin time is specified, DBAM starts a new AAC scheduled statistic history at the specified time.

DSA down time can lead to a schedule that does not conform to the configured schedule. For example, if the next schedule is planned for 2:00 AM and the DSA is not running at this time, the DSA creates the statistic history when it starts up again and then returns to the configured schedule.

1.3.3.8.3. Example

In the following example, a manual AAC statistic history is created immediately:

```
dsa_dbam_aac start
```

In the following example, a scheduled AAC statistic history is created on 1 July 2016 at 0:00 AM. The DSA saves the statistic history counters every month (with an interval of one month):

```
dsa_dbam_aac start bt=20160701000000 interval=1M
```

In the following example, a scheduled AAC statistic history is created on 1 July 2016 at 0:00 AM. The DSA saves the statistic history counters every day. The DSA automatically stops recording of AAC statistic histories after 10 days:

```
dsa_dbam_aac start bt=20160701000000 interval=1D 10
```

1.3.3.9. status

Returns the current status of the AAC statistic history configuration. The syntax is as follows:

dsa_dbam_aac status

1.3.3.9.1. Description

The **dsa_dbam_aac status** command returns the current configuration data of the AAC statistic history. If no AAC statistic history is configured, then the result is empty. If a manual AAC statistic history is configured, then the result is “manual creation”. If a scheduled statistic history is configured, then the begin time, the interval specification and the time for the next schedule is returned.

1.3.3.9.2. Example

The following sample command returns the configuration data of a scheduled AAC statistic history:

```
dsa_dbam_aac status
```

The output is as follows:

```
bt=20150701000000 interval=1M et=20150801000000
```

In this example, collecting AAC statistic history started on 1 July 2015 0:00 AM. The data are collected once each month. Collecting data ends on 1 August 2015 0:00 AM.

The following sample command returns the configuration data of a manual created AAC

statistic history (the **dsa_dbam_aac start** command was performed without arguments):

```
dsa_dbam_aac status
```

The output is as follows:

```
manual creation
```

1.3.3.10. stop

Stops AAC statistic history collection. The syntax is as follows:

dsa_dbam_aac stop

1.3.3.10.1. Description

The **dsa_dbam_aac stop** command immediately stops AAC statistic history collection if active. DBAM stores the start and end times of the active statistic history and the current AAC counters in a DBAM statistic history block and doesn't initiate the creation of the new history. Use this command to stop the collection of AAC statistics history explicitly (instead of using automatic scheduled history; see the **dsa_dbam_aac start** command for details).

1.3.3.10.2. Example

```
dsa_dbam_aac stop
```

1.3.3.11. Description

The **dsa_dbam_aac** LDAP extended operation allows DirX Directory administrators to manage the recording of AAC statistic histories. In the AAC statistic histories, the DSA records how often an attribute index is used in search operations.

The AAC statistic histories help an administrator to administrate the attribute indexes and optimize the performance of search operations. For example, the administrator can identify attribute indexes that are never used and can delete these attribute indexes.

After the DBAM database is initialized, a permanent AAC statistic history is saved into a DBAM block every five minutes. If the DSA crashes, the counter for the last unsaved period is lost.

Use the **dsa_dbam_aac status** command to find out whether an AAC statistic history is configured.

Use the **dsa_dbam_aac start** command to initiate a new statistic history. For each new statistic history, DBAM creates a new DBAM statistic history block, resets the counters to zero and records the statistic history start time.

Use the **dsa_dbam_aac stop** command to stop a statistic history explicitly.

Use the **dsa_dbam_aac reset** command to stop the statistic history immediately and to remove all AAC statistic histories except for the permanent AAC statistic history.

Use the **dsa_dbam_aac list** command to get a list of all available AAC statistic histories. Then use the **dsa_dbam_aac show** command to display the counters of a specific AAC statistic history.

DBAM can keep a maximum of 54 statistic histories. After the 54th statistic history, DBAM history collection wraps around to the first DBAM statistic history block.

The maximum number of indexed attributes is 800. The permanent AAC statistic history records counters for all attribute indexes. All other AAC statistic histories records counters for maximal 400 attribute indexes.

1.3.3.12. Example

The following example shows how to apply the **dsa_dbam_aac** LDAP extended operation with the tool **dirxextop**. It shows the creation of a scheduled AAC statistic history. The start time is 1 July 2016 at 0:00 AM, the interval is one day and the time span is scheduled for 10 days:

```
dirxextop -D cn=admin,o=my-company -w dirx -t dsa_dbam_aac -P “start
bt=20160701000000 interval=1D 10”
```

Because **dirxextop** accepts only one parameter, you must enclose the arguments to the **dsa_dbam_aac** extended operation in double quotation marks ("").

1.3.3.13. See Also

dirxextop in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*.

1.3.4. dsa_dirxadm_cmd

1.3.4.1. Synopsis

dsa_dirxadm_cmd "**dirxadm_command***"***

1.3.4.2. Purpose

Performs **dirxadm** operations in a directory service that can only be accessed via LDAP protocol.This extended operation is available only on Linux systems.

1.3.4.3. Parameters

"*dirxadm_command*"
Specifies the **dirxadm** operation as a simple unencoded string enclosed in double quotes.

1.3.4.4. Description

Use the **dsa_dirxadm_cmd** LDAP extended operation to perform a **dirxadm** operation in a DSA that can only be accessed via LDAP protocol.

On success, the DSA returns the result of the **dirxadm** operation.

The **dsa_dirxadm_cmd** operation requires the **Execute** permission; that is, the user's distinguished name must be contained in the **LDAP Extended Operations Execute Users** or **LDAP Extended Operations Execute Groups** attribute of the LDAP server.

The **dsa_dirxadm_cmd** operation uses the bind operation specified in the environment variable **DIRX_DSA_EXTOP_ADM_BIND** to perform the bind operation to the DSA.

1.3.4.5. Example

In the following example a **lob show** operation is performed:

```
dirxextop -D cn=admin,o=my-company -w dirx -t dsa_dirxadm_cmd
-P "lob show -supplier /CN=1stDSA -agreementid 60"
```

On success, the LDAP extended operation returns the following output:

```
OBS=COOPERATIVE OBMV={VF=210304130754Z} AGR={SS={AREA={CP={/O=My-
Company},RA={BAS={/OU=Sales/CN=Abele}}},ATT={DEF=TRUE}},UM={SI={OC=TR
UE}}} US={D=FALSE,NU=19700101000000Z,US={SUS={AC=NO-
CHANGES,OU={SID=0,UT=20210304132919Z,OPMSN=10454720,AC=FALSE},AU={WS=
INVOKED}}}} RPOL={LDSUPP={BAS64=TRUE}}
```

In the following example the paging policy of the root entry is displayed:

```
dirxextop -D cn=admin,o=my-company -w dirx -t dsa_dirxadm_cmd
-P "show / -attribute PAGP"
```

On success, the LDAP extended operation returns the following output:

```
/ PAGP={PTO=20,MAXNUM=20,MAXMEM=4096}
```

1.3.4.6. See Also

dirxextop and **dirxadm** in the *DirX Directory Administration Reference*, **Environment Variables** in *DirX Directory Administration Reference*, **dirxadm** command in the *DirX Directory Administration Reference*, **dse bind** operation in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in the *DirX*

Directory Syntaxes and Attributes, **X.500 Security Features** in the *DirX Directory Introduction*.

1.3.5. dsa_relevant_aci

1.3.5.1. Synopsis

dsa_relevant_aci [*parameter*]

1.3.5.2. Purpose

Searches for access control subentries that include the specified entry in the user classes.The operation searches only for access control subentries that contain prescriptive access control items.Entry access control items and subentry access control items are not returned.

The result is the list of distinguished names.Every line contains exactly one distinguished name.If Distinguished names containing a new line or a non-printable character are written in base64 encoding.

1.3.5.3. Parameters

The distinguished name of the entry can be specified as a parameter using LDAP distinguished name syntax. If no parameter is specified, the result contains the relevant access control subentries for an anonymous bind.

1.3.5.4. Example

In the following example an access control search is executed for the **cn=admin,o=my-company** entry:

```
dirxextop -D cn=admin,o=my-company -w dirx -t dsa_relevant_aci
-P "cn=admin,o=my-company”
```

On success, the LDAP extended operation returns the following output:

```
cn=AccessControl-Subentry
cn=AccessControl-Subentry,o=My-Company
```

In the following example an access control search is executed for an anonymous bind:

```
dirxextop -D cn=admin,o=my-company -w dirx -t dsa_relevant_aci
```

On success, the LDAP extended operation returns the following output:

```
cn=AccessControl-Subentry,o=My-Company
```

1.3.5.5. See Also

dirxextop in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*, **Distinguished Names** in **DirX Directory String Representation for LDAP Binds** in *DirX Directory Syntaxes and Attributes*.

1.4. DirX Directory LDAP Server LDAP Extended Operations Reference Descriptions

The following sections provide reference descriptions for LDAP extended operations performed by the LDAP server.

1.4.1. ldap_cfg_upd

1.4.1.1. Synopsis

ldap_cfg_upd

1.4.1.2. Purpose

Activates changes made to the LDAP configuration subentry for an LDAP server without having to re-start the server.

1.4.1.3. Description

The **ldap_cfg_upd** LDAP extended operation allows DirX Directory administrators to change specific attributes of an LDAP server's configuration subentry and then activate the changes dynamically. Using dynamic update allows changes to the LDAP server configuration to be applied without the effects of an LDAP server re-start (permanent loss of client connections to the server and temporary loss of the service itself).

Use the **ldap_show_cfg_upd_attr** extended operation to return the list of attributes available for dynamic update.

To run the **ldap_cfg_upd** LDAP extended operation, use the **dirxextop** command or the DirX Directory Manager's Monitoring view (**Monitoring** → **LDAP** → **Configuration** → **Update CFG attributes**).

By default, the **ldap_cfg_upd** LDAP extended operation is listed in the LDAP Extended Execute Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Execute Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

When executed, **ldap_cfg_upd** LDAP extended operation returns a detailed update report that displays the progress and the result of the update operation. If the last line of the report shows that the operation was successful, the update is performed and the new settings in the LDAP configuration subentry become active. If the last line shows an error, the configuration changes are not applied and the old settings remain valid.

Use the **ldap_show_cfg_general**, **ldap_show_cfg_ssl** and **ldap_show_cfg_audit** extended operations to display the currently active settings for an LDAP server configuration in readable format. Note that the attributes of the LDAP server SSL configuration subentry and LDAP server audit configuration subentry can only be displayed; they cannot be dynamically updated.

Use the **ldap_show_cfg_upd_history** extended operation to view the update reports returned by the last 25 runs of the **ldap_cfg_upd** LDAP extended operation.

1.4.1.4. Example

The following example shows how to apply the **ldap_cfg_upd** LDAP extended operation on the local LDAP server with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_cfg_upd
```

The LDAP extended operation returns output like the following:

```
+++ LDAP-Cfg Update Started at:Fri Jan 8 09:57:03.426000
Cfg-Name:ldapConfiguration
UpdInfo: 0 previous updates suceeded. (LastSuccess: never)
UpdInfo: 0 previous updates failed.   (LastFail   : never)
-------------------------------------------------------------------
Read access to CFG aquired.
Updating:Maximum Connections     (cfg-updated)=2048
Updating:Conn Idle Time [sec]    (cfg-updated)=3600
Updating:Unbind Delay Time [sec] (cfg-updated)=0
Updating:Only Read-Ops allowed   (cfg-updated)=0
Updating:Backend Sharing         (cfg-updated)=1
Updating:Deny Anonymous Access   (default)=0
Updating:Only Anonym Allowed     (cfg-updated)=0
Updating:Max DAP-Conn Share Count(cfg-updated)=6
Updating:Max Req Search-Attr     (cfg-updated)=256
Updating:Max Search-Filter Items (cfg-updated)=128
LCFG Integer-Update finished.
-------------------------------------------------------------------
SSL configuration will NOT be updated.
AUDIT configuration will NOT be updated.
```

```
-------------------------------------------------------------------------
Updating:IP Allow List           (default)=all
Updating:IP-Deny                 (cfg)=12.23.34.45 (net:2d22170c)
Updating:IP-Deny                 (cfg)=11.22.33.44 (net:2c21160b)
-------------------------------------------------------------------------
Updating:Denied User             (cfg):cn=bab jensen,ou=sales,o=my-
company
Updating:Denied User             (cfg):cn=g farfel,ou=sales,o=my-
company
Updating:Allowed User            (cfg):all
Updating:Allowed User Groups     (default)=none
Updating:Denied User Groups      (default)=none
-------------------------------------------------------------------------
Updating:ExtOp-Read-OPs          (cfg):successfully set READ
privilege for ExtOp ldap_mib_static
Updating:ExtOp-Admin-Users       (cfg):X500DN:/o=my-
company/ou=sales/cn=mayer2
Updating:ExtOp-Admin-Users       (cfg):cn=admin,o=my-company
Updating:ExtOp-Read-Users        (default)=none
Updating:ExtOp-Exec-Users        (cfg):cn=admin,o=my-company
Updating:ExtOp-Monitoring-Users  (default)=none
Updating:ExtOp-Admin-Groups      (cfg):ou=salesgroup,o=my-comapny (5
members)
Updating:ExtOp-Admin-Groups      (cfg):cn=ptgroup2,o=my-company (4864
members)
Updating:ExtOp-Admin-Groups      (cfg):cn=hohner,ou=sales,o=my-
company (0 members)
Updating:ExtOp-Read-Groups       (cfg):ou=salesgroup,o=my-compay (5
members)
Updating:ExtOp-Exec-Groups       (default)=none
Updating:ExtOp-Monitoring-Groups (default)=none
-------------------------------------------------------------------------
Updating:Search
ServiceControls(cfg)=PreferChaining=T:ChainingProhibited=F:LocalScope
=F:DontUseCopy=F:DontDereferenceAlias=F:Subentries=F:CopyShallDo=T:Pr
iority=1:TimeLimit=245:SizeLimit=0:ScopeOfReferral=0:AttributeSizeLim
it=0
Updating:Compare
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=F:dontDereferenceAlias=F:subentries=F:copyShalldo=T:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
-------------------------------------------------------------------------
```

```
=0
Updating:Add
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Remove
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Modify
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:ModifyDN
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
-----------------------------------------------------------------------
Reading updated LCFG from DSA OK. Going to exchange data in local
configuration...
Exchanged: Maximum Connections     =2048 OK
Exchanged: Conn Idle Time [sec]    =3600 OK
Exchanged: Unbind Delay Time [sec] =0 OK
Exchanged: Only Read-Ops allowed   =0 OK
Exchanged: Backend Sharing         =1 OK
Exchanged: Deny Anonymous Access   =0 OK
Exchanged: Only Anonym Allowed     =0 OK
Exchanged: Max DAP-Conn Share Count=6 OK
Exchanged: Max Req Search-Attr     =256 OK
Exchanged: Max Search-Filter Items =128 OK
Exchanging Cfg-integers OK.
Exchanging IP Allow/Deny OK.
Cleanup IP Allow/Deny OK.
Exchanging User Allow/Deny OK.
Cleanup User Allow/Deny OK.
Exchanging Groups Allow/Deny OK.
Cleanup Groups Allow/Deny OK.
```

```
Exchanging Extop Privileges OK.
Cleanup Extop Privileges OK.
Exchanging Extop-Users Admin/Read/Exec/Mon OK.
Cleanup Extop-Users Admin/Read/Exec/Mon OK.
Exchanging Extop-Groups Admin/Read/Exec/Mon OK.
Cleanup Extop-Groups Admin/Read/Exec/Mon OK.
Exchanging ServiceControls OK.
LCFG-Exchange Finished OK.
Read access to LCFG released.
+++LDAP-Cfg Update Finished SUCCESSFUL at:Fri Jan 8 09:57:03.848000
=====================================================================
```

The last line of the example output shows that the operation was successful: the update is performed and the new settings in the LDAP configuration subentry are active.

1.4.1.5. See Also

ldap_show_cfg_audit, **ldap_show_cfg_general**, **ldap_show_cfg_ssl**, **ldap_show_cfg_upd_attr**, **ldap_show_cfg_upd_history** , **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations**, **Attributes for LDAP Server Configuration**, **Attributes for LDAP Server SSL Configuration**, **Attributes for LDAP Server Audit Configuration** in *DirX Directory Syntaxes and Attributes*.

1.4.2. ldap_disable_config_dsa

1.4.2.1. Synopsis

ldap_disable_config_dsa *DSA_name*

1.4.2.2. Purpose

Disables a contact DSA for an LDAP server.

1.4.2.3. Parameters

DSA_name
The name of the contact DSA to be disabled.

1.4.2.4. Description

The **ldap_disable_config_dsa** LDAP extended operation allows DirX Directory administrators to disable a contact DSA for an LDAP server; for example, before taking it off-line for maintenance. It is intended for use in a multiple contact DSA configuration, where an LDAP server has a list of contact DSAs from which it can choose. Using multiple contact DSAs in a master-shadow configuration enables DAP operations to be distributed among the consumer DSAs in a shadow configuration and provides simple failover capability in the event that one contact DSA fails or needs to be taken offline. For details

about this configuration, see the chapter "Using Multiple Contact DSAs" in the *DirX Directory Administration Guide*.

Use the mandatory *DSA_name* parameter to specify the name of the DSA to be disabled.

By default, the **ldap_disable_config_dsa** LDAP extended operation is listed in the LDAP Extended Execute Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Execute Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

The LDAP server excludes the disabled DSA from selection as a contact DSA until it is re-enbled with the **ldap_enable_config_dsa** LDAP extended operation or until the LDAP server is re-started.

Use the **ldap_show_config_dsas** to display the currently acitive contact DSA table.

At least one DSA must be in the enabled status. As a result, attempting to disable the last enabled DSA in a selection list fails.

1.4.2.5. Example

The following example shows how to apply the **ldap_disable_config_dsa** LDAP extended operation with the **dirxextop** command. In the example, the contact DSA **sslDSA2** is disabled:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_disable_config_dsa
-P /CN=sslDSA2
```

On success, the LDAP extended operation returns the message:

```
DisableConfigDSA() : OK!
```

If the specified *DSA_name* parameter is incorrect, the LDAP extended oepration returns the message:

```
DisableConfigDSA() : Given DSA name is not a configured contact-DSA
name!
```

1.4.2.6. See Also

ldap_disable_config_dsa, **ldap_show_config_dsas**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*.

1.4.3. ldap_enable_config_dsa

1.4.3.1. Synopsis

ldap_enable_config_dsa *DSA_name*

1.4.3.2. Purpose

Enables a contact DSA for an LDAP server.

1.4.3.3. Parameters

DSA_name
The name of the contact DSA to be enabled.

1.4.3.4. Description

The **ldap_enable_config_dsa** LDAP extended operation allows DirX Directory administrators to enable a contact DSA that was previously disabled with the **ldap_disable_config_dsa** LDAP extended operation. It is intended for use in a multiple contact DSA configuration, where an LDAP server has a list of contact DSAs from which it can choose. Using multiple contact DSAs in a master-shadow configuration enables DAP operations to be distributed among the consumer DSAs in a shadow configuration and provides simple failover capability in the event that one contact DSA fails or needs to be taken offline. For details about this configuration, see the chapter “Using Multiple Contact DSAs” in the *DirX Directory Administration Guide*.

Use the mandatory *DSA_name* parameter to specify the name of the DSA which is to be enabled.

By default, the **ldap_enable_config_dsa** LDAP extended operation is listed in the LDAP Extended Execute Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Execute Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

Use the **ldap_show_config_dsas** to display the currently active contact DSA table to determine which DSAs are disabled.

1.4.3.5. Example

The following example shows how to apply the **ldap_enable_config_dsa** LDAP extended operation with the **dirxextop** command. In the example, the contact DSA **sslDSA2** is enabled:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_disable_config_dsa
-P /CN=sslDSA2
```

On success, the LDAP extended operation returns the message:

```
EnableConfigDSA() : OK!
```

If the specified *DSA_name* parameter is incorrect or is omitted, the LDAP extended oepration returns an error message.For example:

```
EnableConfigDSA() : Given DSA name is not a configured contact-DSA
name!
```

1.4.3.6. See Also

ldap_enable_config_dsa, **ldap_show_config_dsas**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*.

1.4.4. ldap_show_cfg_audit

1.4.4.1. Synopsis

ldap_show_cfg_audit

1.4.4.2. Purpose

Displays the currently active settings of attributes in an LDAP server's LDAP audit configuration subentry.

1.4.4.3. Description

Use the **ldap_show_cfg_audit** LDAP extended operation to display the current values for the attributes of an LDAP server's audit configuration subentry in readable format.

Note that you cannot use the **ldap_cfg_upd** extended operation to update these attributes dynamically; you can only display their values. Use the **ldap_show_cfg_upd_attr** extended operation to return the list of attributes available for dynamic update.

To run the **ldap_show_cfg_audit** LDAP extended operation, use the **dirxextop** command or the DirX Directory Manager's Monitoring view (**Monitoring** → **LDAP** → **Configuration** → **Show active Audit settings**).

By default, the **ldap_show_cfg_audit** LDAP extended operation is listed in the LDAP Extended Read Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Read Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

Use the **ldap_show_cfg_general** extended operation to display the current values for attributes of an LDAP server's configuration subentry in readable format. Use the **ldap_show_cfg_ssl** extended operation to display the current values for an LDAP server's SSL configuration subentry in readable format.

Use the **ldap_show_cfg_upd_history** extended operation to view the update reports returned by the last 25 runs of the **ldap_cfg_upd** LDAP extended operation.

1.4.4.4. Example

The following example shows how to apply the **ldap_show_cfg_audit** LDAP extended operation to a remote LDAP server with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t -h xyz.net -p 6666
ldap_show_cfg_audit
```

The LDAP extended operation returns output like the following:

```
==================== LDAP Audit Info  ============================
Server            : DirX Directory V8.5 9.1.156 2016:06:04 20:10 64-
Bit
Copyright (c) 2016 Eviden
Hostname          : xyz.net
Current Local Time: Mon Jun 06 11:49:48 2016
Status            : ON
Audit Version     : 9.1
Destination File  : C:\Program
Files\DirX\Directory\ldap\audit\ldapConfiguration\audit.log
Audited Bytes     : 13004
Record Limit      : 5000 records
Max File Size     : 256 MB
Records in File   : 10 records
Overall Records   : 10 records
Overflow Policy   : moveFile
Wrap Count        : 0
Move Count        : 0
Detail Level      : max
Value Limit       : 128
Op Selection      : all  (errors included)
Buffer Size       : 0
Start Time        : none
Stop Time         : none
```

```
Cron Job          : no
unlink() errors   : 0
rename() errors   : 0
Encryption        : none
SessTracking      : on
SessTrackingLen   : 256
```

1.4.4.5. See Also

ldap_show_cfg_general, **ldap_show_cfg_ssl**, **ldap_show_cfg_upd_attr**, **ldap_show_cfg_upd_history**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations**, **Attributes for LDAP Server Configuration**, **Attributes for LDAP Server SSL Configuration**, **Attributes for LDAP Server Audit Configuration** in *DirX Directory Syntaxes and Attributes*.

1.4.5. ldap_show_cfg_general

1.4.5.1. Synopsis

ldap_show_cfg_general

1.4.5.2. Purpose

Displays the currently active settings of the attributes in an LDAP server's configuration subentry.

1.4.5.3. Description

Use the **ldap_show_cfg_general** LDAP extended operation to display the current values for the attributes of an LDAP server's configuration subentry in readable format. A plus sign (+) next to an attribute indicates that it is available for dynamic update. You can also use the **ldap_show_cfg_upd_attr** extended operation to return the list of attributes available for dynamic update.

To run the **ldap_show_cfg_general** LDAP extended operation, use the **dirxextop** command or the DirX Directory Manager's Monitoring view (**Monitoring** → **LDAP** → **Configuration** → **Show active General settings**).

By default, the **ldap_show_cfg_general** LDAP extended operation is listed in the LDAP Extended Read Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Read Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

Use the **ldap_show_cfg_audit** and the **ldap_show_cfg_ssl** extended operations to display the current values for attributes of an LDAP server's audit configuration subentry or its SSL configuration subentry in readable format.

Use the **ldap_show_cfg_upd_history** extended operation to view the update reports returned by the last 25 runs of the **ldap_cfg_upd** LDAP extended operation.

1.4.5.4. Example

The following example shows how to apply the **ldap_show_cfg_general** LDAP extended operation to the local LDAP server with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_show_cfg_general
```

The LDAP extended operation returns output like the following:

```
Fri Jan 8 09:57:03.848000)
UpdInfo: 0 previous online-updates failed since server start.
(LastFail   : never)
-------------------------------------------------------------------
-------
Note: Attributes with (+) can be updated w/o Server-Restart
-------------------------------------------------------------------
-------
SchemaName        :cn=schema
NamingContext     :o=my-company
SSL-SubentryName  :ldapSSLConfiguration4
Audit-SubentryName:ldapAudit
-------------------------------------------------------------------
-------
Port Number             =  8080
Secure Port Number      =   636
StartTLS enabled        =     1
Maximum Connections     =  2048 (+)
Conn Idle Time [sec]    =  3600 (+)
Unbind Delay Time [sec] =     0 (+)
Use {ASN1} Header (0=No)=     0
Only Read-Ops allowed   =     0 (+)
LDAP Result Cache       =     0
Max Cached Results      = 10000
Min Cache Time          =     0
Max Cache Time          = 86400
Min Cached Entries      =     0
Min Cached Entries      =  2000
Min Cached Attributes   =     0
```

```
Min Cached Attributes   =  2200
Min Cached Values       =     0
Min Cached Values       =  5000
Cache Table Size        =  4096
Max Size of LDAP Cache  =    50
Cache Update Strategy   =     3
Thread Pool size        =    32
Anonym DAP Pool Size    =     5
Backend Sharing         =     1 (+)
Deny Anonymous Access   =     0 (+)
CharSet in Request      =     1
CharSet in Result       =     1
Only Anonym Allowed     =     0 (+)
Sockets KeepAlive       =     1
Async Sockets           =     1
Max Send Timeout        =    30
Max Recv Timeout        =    30
Max Incomplete Ops/Conn =     0
Op Stack Limit          =   320
# of Overflow Threads   =     1
Max DAP-Conn Share Count=     6 (+)
Max Req Search-Attr     =   256 (+)
Max Search-Filter Items =   128 (+)
------------------------------------------------------------------------
-------
IP-Allow=all  (+)
IP-Deny=12.23.34.45  (+)
IP-Deny=11.22.33.44  (+)
IP-Listen=all
------------------------------------------------------------------------
-------
User-Allow=all  (+)
User-Deny=cn=bab jensen,ou=sales,o=my-company  (+)
User-Deny=cn=g farfel,ou=sales,o=my-company  (+)
Group-Allow=none  (+)
Group-Deny=none  (+)
------------------------------------------------------------------------
-------
ExtOpAdminUser=X500DN:/o=my-company/ou=sales/cn=mayer2  (+)
ExtOpAdminUser=cn=admin,o=my-company  (+)
ExtOpExecUser=cn=admin,o=my-company  (+)
```

```
ExtOpMonUser=none  (+)
ExtOpAdminGroup=ou=salesgroup,o=my-company (5 members)  (+)
ExtOpAdminGroup=cn=ptgroup2,o=my-company (4864 members)  (+)
ExtOpAdminGroup=cn=hohner,ou=sales,o=my-company (0 members)  (+)
ExtOpReadGroup=ou=salesgroup,o=my-company (5 members)  (+)
ExtOpExecGroup=none  (+)
ExtOpMonGroup=none  (+)
------------------------------------------------------------------------
-------
Search
ServiceControls=PreferChaining=T:ChainingProhibited=F:LocalScope=F:Do
ntUseCopy=F:DontDereferenceAlias=F:Subentries=F:CopyShallDo=T:Priorit
y=1:TimeLimit=245:SizeLimit=0:ScopeOfReferral=0:AttributeSizeLimit=0
(+)
Compare
ServiceControls=preferChaining=T:chainingProhibited=F:localScope=F:do
ntUseCopy=F:dontDereferenceAlias=F:subentries=F:copyShalldo=T:priorit
y=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit=0
(+)
Add
ServiceControls=preferChaining=T:chainingProhibited=F:localScope=F:do
ntUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:priorit
y=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit=0
(+)
Remove
ServiceControls=preferChaining=T:chainingProhibited=F:localScope=F:do
ntUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:priorit
y=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit=0
(+)
Modify
ServiceControls=preferChaining=T:chainingProhibited=F:localScope=F:do
ntUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:priorit
y=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit=0
(+)
ModifyDN
ServiceControls=preferChaining=T:chainingProhibited=F:localScope=F:do
ntUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:priorit
y=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit=0
(+)
```

1.4.5.5. See Also

ldap_show_cfg_audit, **ldap_show_cfg_ssl**, **ldap_show_cfg_upd_attr**, **ldap_show_cfg_upd_history**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations**, **Attributes for LDAP Server Configuration**, **Attributes for LDAP Server SSL Configuration**, **Attributes for LDAP Server Audit Configuration** in *DirX Directory Syntaxes and Attributes*.

1.4.6. ldap_show_cfg_ssl

1.4.6.1. Synopsis

ldap_show_cfg_ssl

1.4.6.2. Purpose

Displays the currently active settings of attributes in an LDAP server's LDAP SSL configuration subentry.

1.4.6.3. Description

Use the **ldap_show_cfg_ssl** LDAP extended operation to display the current values for the attributes of an LDAP server's SSL configuration subentry in readable format.

Note that you cannot use the **ldap_cfg_upd** extended operation to update these attributes dynamically; you can only display their values. Use the **ldap_show_cfg_upd_attr** extended operation to return the list of attributes available for dynamic update.

To run the **ldap_show_cfg_ssl** LDAP extended operation, use the **dirxextop** command or the DirX Directory Manager's Monitoring view (**Monitoring** → **LDAP** → **Configuration** → **Show active SSL settings**).

By default, the **ldap_show_cfg_ssl** LDAP extended operation is listed in the LDAP Extended Read Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Read Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

Use the **ldap_show_cfg_general** extended operation to display the current values for attributes of an LDAP server's configuration subentry in readable format. Use the **ldap_show_cfg_audit** extended operation to display the current values for an LDAP server's audit configuration subentry in readable format.

Use the **ldap_show_cfg_upd_history** extended operation to view the update reports returned by the last 25 runs of the **ldap_cfg_upd** LDAP extended operation.

1.4.6.4. Example

The following example shows how to apply the **ldap_show_cfg_ssl** LDAP extended operation to the local LDAP server with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_show_cfg_ssl
```

The LDAP extended operation returns output like the following:

```
+++ LDAP-SSL Configuration at:Wed Jun 8 09:26:26.507457
SslCfg-Name:ldapSSLConfiguration4
UpdInfo: 0 previous updates suceeded. (LastSuccess: never)
UpdInfo: 0 previous updates failed.   (LastFail   : never)
------------------------------------------------------------------------
SSL PortNumber: 636
Supported Protocols: SSLv3 TLSv10 TLSv11 TLSv12
Supported Ciphers: ALL
SASL Client-Auth Required: yes
SASL-Auth-Id Mapping: Certificate.subjectDN
Valid Root-CAs File: e:\OpenSSL\c-examples\testca.pem
#TrustedCACerts found in Subentry: 6
(1)CertIssuer: /O=My-Company/OU=DirX-Example/CN=test-CA
(1)Subject   : /O=My-Company/OU=DirX-Example/CN=test-CA
(2)CertIssuer: /C=DE/L=Berlin/O=My-Company/OU=Certificate Authority
PT
(internal)/CN=PT CA/emailAddress=klaus.reichel@my-company.net
(2)Subject   : /C=DE/L=Berlin/O=My-Company/OU=Certificate Authority
PT (internal)/CN=PT CA/emailAddress=klaus.reichel@my-company.net
(3)CertIssuer: /C=DE/L=Munich/O=Certis/OU=Certificate
Authority/CN=Certis CA/emailAddress=ca@certis.de
(3)Subject   : /C=DE/L=Munich/O=Certis/OU=Certificate
Authority/CN=Certis CA/emailAddress=ca@certis.de
(4)CertIssuer: /C=GB/O=pksco/CN=PKSCO PKI TEST Certificate Authority
(4)Subject   : /C=GB/O=pksco/CN=PKSCO PKI TEST Certificate Authority
(5)CertIssuer: /CN=My-Company TrustedRoot 2011/O=My-Company/C=DE
(5)Subject   : /CN=My-Company TrustedRoot Client-CA 2011/O=My-
Company/C=DE
(6)CertIssuer: /CN=My-Company TrustedRoot 2011/O=My-Company/C=DE
(6)Subject   : /CN=My-Company TrustedRoot 2011/O=My-Company/C=DE
Trace Level: 1
Trace File Path: e:\My-Company\DirX\ldap\log
CRL Checking: no
Allow Expired CRLs: yes
Allow NotYetValid CRLs: no
Tolerate Missing CRLs: yes
```

```
CRL-File: c:\OpenSSL\bin\PKI2\ca.crl
CRL-File: c:\OpenSSL\bin\PKI2\My-
Company_TrustedRoot_Expired_CRL_2011_pem.crla
OwnKeyMaterialFile: e:\My-Company\DirX\ldap\conf\cert_ldapserver.pem
OwnKeyMaterialPwdFile: e:\My-Company\DirX\ldap\conf\dirx_pkcs12.pwd
OwnKeyMaterial: 4680 Bytes
Bag Attributes
    localKeyID: 01 00 00 00
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFBjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIFlV/N30hCTACAggA
MBQGCCqGSIb3DQMHBAjnDXbb5NDL+QSCBMDkwplwQpyUIrjC0oRCnA40IPIBJN0g
9wgx4NNvQwtqrgMk+o+R/jhSkA92+SJ4O2QTmlmbn5s+Wrf0jSj576egxEyCNgD2
+F71vt9odZ/M9nxNdmM2Ncaqflo0blnErddog+IghgSgBRHU5hgCKKlr/OFx93CP
b0ch643XhCCbA0xLInfeyNI5+cBRspeKSztCX4KhxKdNovA3SJT5FcLi8On8SnwY
fZRR5rN2mMs1fNSOS3O4hw+H21+VeNOYeJyBnyCcFbToG+iYgzOJ8MbBrXSw8O4v
y3Wivgth0dYIZoN3Rpyx7vaS7gHMhYFAo+zUJ7qo7shlHMmo0Jp09oNxq+Bgj2Uo
q8eB6LzwyleHammDbbnIhwDCfRzf4aeGGlIsixDDWY9Lun+vKPnVfgnqGh993kDa
SKXiKE8hvMU0M2eqetn0s7BZATtY8QbWWUhiaZkG22VdlF2P0XqlLG5pHdB1STLE
DoDa7VH90OG6sSHLV16gCSiGKriUSitnm+0ubwXeqMBLkwwt23aN8AlpR9Byr6uY
7EEeq5wq4AIN5hO9Pu/L0mMHGUZ6rDAsF499mHzgrLCLdDw3FCX4FKtz6ORsHr5I
IC4p/ZWCbjU4dw7HtrBvIhETJzDCxdT0ybRA/GTQVteaCL/jFiuq8FxgjV+bfNO7
zB0q2zRDMpn36SbZ8AIsLIjKQd2Vv0j4kW4+S7Cy4z/GqZi6YAokoFD13y5exWhQ
KtK/uTpGdXU/TX+SexA198ohFf0h48vUVJjGIqmO7w1AXcHZnjBaS0/d25RBnUrx
X9kl0WkknPqDh8WpyUYQNOqy00Gp/zVWVcFhBRMgBrno4RvH9p6jUURwpAV6MMBm
iN/3b0vsVUeRrmjYyHa+rnE2dPe+/Z+WIOq8qMtQ5nIrZcgMrXIJLZbggvplj388
H6ilhTkFxgc9C6ubjDw+5qZ+q8bsFUBBpWZ5LW05mngLwMFeEkKUjAOuoWmwK1kb
MVyGRq8HGOE1Pp6PDrTlASn+42R0oWsMcVSaI02XYcxwUnNPD2ZWZ/+qpuqf/7gw
tppaytWq7dzXjdW1UiZ3YrTMlX6uI96P2YPaVVR11nkozsx0Fah3yLcnognlhNto
CIHt+7MzoDDp4s0G7fOYRbcejkspkJQCfASpI0e15Xyrn7Xd9On/Zux+oa2SqGX0
Hc1dT5h0jvyHmN2sBomtzKQN2E/p+931RUnyFCp0JlRNKquwSck7DMvCz3fal6Sr
2ELqbSnwaJz0bVmBBmAifOxMX8bpuJLQdqP0i9g5up0EbXVnAdi7ZrmGFbPefFR7
gtZeiMdwmK8IJOidjPqb/qmk2yxYArxRJgReDXZBgfhy4oTzPq5zz0RCo9eVEtgk
Ox+qdoX608Avf7BW1fvr1VgEAxDmLBhOB/F8i9HdqRQ3LbzqYsBdS64WbvntK/x6
nuIphwQsKABykD20l0bZT4u4Qpx6AiNvoNYAlGRfN5Ob2CCE5Kb/v+kr3OiFRb1J
oUKBhKsFvTn9bC9xae6Ufr/cj0JtqRs832ylvnENPD6dTHZPp43YfzIkd3i9chaP
qd61BQpxzzptf8saodatylsnOzh0LpVZuhsUI8FKA9UUAyVbmcQTzTg4
-----END ENCRYPTED PRIVATE KEY-----
Bag Attributes
    localKeyID: 01 00 00 00
subject=/O=My-Company/OU=DirX-Example/OU=DirX8.3/CN=dirxldapv3-2k
```

```
issuer=/O=My-Company/OU=DirX-Example/CN=test-CA
-----BEGIN CERTIFICATE-----
MIIDfjCCAmegAwIBAgICAwAwDQYJKoZIhvcNAQEFBQAwPjETMBEGA1UEChMKTXkt
Q29tcGFueTEVMBMGA1UECxMMRGlyWC1FeGFtcGxlMRAwDgYDVQQDEwd0ZXN0LUNB
MB4XDTEzMTAwMjA2Mzg0MFoXDTIzMDkzMDA2MzgzOVowVjETMBEGA1UEChMKTXkt
Q29tcGFueTEVMBMGA1UECxMMRGlyWC1FeGFtcGxlMRAwDgYDVQQLEwdEaXJYOC4z
MRYwFAYDVQQDEw1kaXJ4bGRhcHYzLTJrMIIBITANBgkqhkiG9w0BAQEFAAOCAQ4A
MIIBCQKCAQAA8P0pg2MmSQV6g66lc+v6vknpeeCHDAoJsrZBkCi2M3eO2D8Ex6Q4
LMSJEk6Wb8n+a0pui0Uic2oLTTxzysAPSlyXs2eWS+ICJiiR9eHdEOY5KRvE22qt
jC1hO1V47xi2IxhnFzcsZv/5PyhsbTjT48skPRPQFrOlgyPotQyCar7GVRmgOGeh
0kGG3kfmdYvoxqoOEb/XAF6KNXubgfOCNQhNQEkZg+Q0xOdHWSSVa3eBGD+JBBXD
PQ50bzr3LGg3zD9UcU7WlMG1oaLDpWiDvUXukDL4BCYqUV4DWhTfL6aSHpyGpAM5
BamqDHMiC/boVZaosVSMW5No3oogRfDNAgMBAAGjcDBuMB0GA1UdDgQWBBQS+Q82
LWhEYp2wEMJMIh2IY/TQ8DAfBgNVHSMEGDAWgBRfFYKlg1D6vaq4wBcw6YiNBdf4
HTAOBgNVHQ8BAf8EBAMCBaAwCQYDVR0TBAIwADARBglghkgBhvhCAQEEBAMCAEAw
DQYJKoZIhvcNAQEFBQADggEAAJZW78KjNndFFLlbiRWiF7WaNDZY5E7mOOZXg/Kf
1iQhhqFQxlBVYyEhbFcL9KHrkUHykM7IA18keBuKIqNUIEhoBznbQqgVmRjhRbSi
mkTxJbFmwFi/b/kq+elEwB79hyUUNkIHefP621o6rX3+aqOY9bHDd5dgxg/Lccxp
5mwz1sgsf0i83wCOvM452oRKn0tuLlRxOX4pi81qe7zeT9ByOvph/FcWsjfEf8MF
Mj5WI+Z0+nCQF4VRV0jwfPNQ7+C0EGvbeFZ2vBuRMJ8QZdPvM6Dbb8biuCCU+r3s
5QAH1nfjx6UZhRu+QduUb/qD0p/KjZfGR3nA+AqzyzDQeA==
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/O=My-Company/OU=DirX-Example/CN=test-CA
issuer=/O=My-Company/OU=DirX-Example/CN=test-CA
-----BEGIN CERTIFICATE-----
MIIDWTCCAkKgAwIBAgICAKAwDQYJKoZIhvcNAQEFBQAwPjETMBEGA1UEChMKTXkt
Q29tcGFueTEVMBMGA1UECxMMRGlyWC1FeGFtcGxlMRAwDgYDVQQDEwd0ZXN0LUNB
MB4XDTExMDcxMzEyMDgzNFoXDTIxMDcxMDEyMDgzM1owPjETMBEGA1UEChMKTXkt
Q29tcGFueTEVMBMGA1UECxMMRGlyWC1FeGFtcGxlMRAwDgYDVQQDEwd0ZXN0LUNB
MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQAAs6CidZEL1263HpHl0GTh
xjGqYgN5N4yQYlYwCsT/fNrXmIKHjPxpgg7EerLM/Lv3arUZvYZoEkYN7ySXVsUj
e4u37kmmnlQs42GgsYBBqbEN4e5rCrLj8F3yNur2+tclWUZYL3XydA7LElVZNzYi
f3m8ruT2BBKFUTrIxkenWNONIFqYU5x9LiiI+p0snWL624v7sV+e9Cv+Wt/C04zw
K7BgxJWIloteYnjGnHnwpG3zBd0o6ZPEFk5bdTD0GPWMEtfCwa8TQhhExoHLt76t
OFa3fcheORWfsFMoi5E0IMF+a1LRYB2l+vVB+vokXd9y6kXbAUbk/L0IfvpeYG3t
AgMBAAGjYzBhMB0GA1UdDgQWBBRfFYKlg1D6vaq4wBcw6YiNBdf4HTAfBgNVHSME
GDAWgBRfFYKlg1D6vaq4wBcw6YiNBdf4HTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0T
BAgwBgEB/wIBAjANBgkqhkiG9w0BAQUFAAOCAQAAn8XliHD/gu2vwaB0PpEvkcwC
jmepgP5pxbxiOGNkDy9Cdm2dtPVdD0Nwja9mqLze9eLAtmLmAc+Q4tT32V/lH1rH
EeHJR5PU/UI7BfzXGMHvL0Bf8ys77LQH+F/Z51nJc5LCtqtbqS42T4Kuzi7rUrjs
```

```
qXUZr93Zcw+n0DD4t6Bo4tORr6Z6soG2ZmB5Vyc+22sa5C9VqYLXeVWThVU9OXhW
j9vp5QduN65GkK/A/dtfd8FaOCl+5fI07WO6U4vSExXNkiJJksG5cHV6W5UiE1U1
KhPzIN8Ua1AkglvLcUTwqdYt5PiKT24dPSh/WOKaffpNC1vLdYZIukPKOZQZ
-----END CERTIFICATE-----
```

1.4.6.5. See Also

ldap_show_cfg_audit, **ldap_show_cfg_general**, **ldap_show_cfg_upd_attr**, **ldap_show_cfg_upd_history**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations**, **Attributes for LDAP Server Configuration**, **Attributes for LDAP Server SSL Configuration**, **Attributes for LDAP Server Audit Configuration** in *DirX Directory Syntaxes and Attributes*.

1.4.7. ldap_show_cfg_upd_attr

1.4.7.1. Synopsis

ldap_show_cfg_upd_attr

1.4.7.2. Purpose

Displays the list of LDAP configuration subentry attributes that can be dynamically updated with the **ldap_cfg_upd** LDAP extended operation.

1.4.7.3. Description

Use the **ldap_show_cfg_upd_attr** LDAP extended operation to return the list of attributes available for dynamic update with the **ldap_cfg_upd** LDAP extended operation.

To run the **ldap_show_cfg_upd_attr** LDAP extended operation, use the **dirxextop** command or the DirX Directory Manager's Monitoring view (**Monitoring** → **LDAP** → **Configuration** → **Show updateable CFG attributes**).

By default, the **ldap_show_cfg_upd_attr** LDAP extended operation is listed in the LDAP Extended Read Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Read Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

Use the **ldap_show_cfg_audit**, **ldap_show_cfg_general** and **ldap_show_cfg_ssl** and extended operations to display the currently active settings for an LDAP server configuration in readable format. Note that the attributes of the LDAP server SSL configuration subentry and LDAP server audit configuration subentry can only be displayed; they cannot be dynamically updated.

Use the **ldap_show_cfg_upd_history** extended operation to view the update reports returned by the last 25 runs of the **ldap_cfg_upd** LDAP extended operation.

1.4.7.4. Example

The following example shows how to apply the **ldap_show_cfg_upd_attr** LDAP extended operation on the local LDAP server with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_show_cfg__upd_attr
```

The LDAP extended operation returns output like the following:

```
List of 'Updateable' Attributes in LDAP Configuration +
------------------------------------------------------ +
1.3.12.2.1107.1.3.4.135    ldapSearchSvcCtl +
1.3.12.2.1107.1.3.4.136    ldapCompareSvcCtl +
1.3.12.2.1107.1.3.4.137    ldapAddSvcCtl +
1.3.12.2.1107.1.3.4.138    ldapRemoveSvcCtl +
1.3.12.2.1107.1.3.4.139    ldapModifySvcCtl +
1.3.12.2.1107.1.3.4.140    ldapModifyDNSvcCtl +
1.3.12.2.1107.1.3.4.143    ldapMaxConnections +
1.3.12.2.1107.1.3.4.144    ldapConnectionIdleTime +
1.3.12.2.1107.1.3.4.145    ldapUnbindDelayTime +
1.3.12.2.1107.1.3.4.156    ldapReadOnlyServer +
1.3.12.2.1107.1.3.4.180    ldapBackendSharing +
1.3.12.2.1107.1.3.4.181    ldapDenyIPList +
1.3.12.2.1107.1.3.4.182    ldapAllowIPList +
1.3.12.2.1107.1.3.4.183    ldapDenyAnonymousAccess +
1.3.12.2.1107.1.3.4.223    ldapOnlyAnonymAllowed +
1.3.12.2.1107.1.3.4.230    ldapDeniedUsers +
1.3.12.2.1107.1.3.4.231    ldapAllowedUsers +
1.3.12.2.1107.1.3.4.234    ldapExtOpAdmins +
1.3.12.2.1107.1.3.4.236    ldapMaxDapShareCount +
1.3.12.2.1107.1.3.4.256    ldapExtReadOperations +
1.3.12.2.1107.1.3.4.257    ldapExtExecuteOperations +
1.3.12.2.1107.1.3.4.258    ldapExtMonitoringOperations +
1.3.12.2.1107.1.3.4.259    ldapExtOpReadUsers +
1.3.12.2.1107.1.3.4.260    ldapExtOpExecuteUsers +
1.3.12.2.1107.1.3.4.261    ldapExtOpMonitoringUsers +
1.3.12.2.1107.1.3.4.269    ldapMaxReqAttrs +
1.3.12.2.1107.1.3.4.270    ldapMaxFilterItems +
1.3.12.2.1107.1.3.4.271    ldapExtOpAdminsGroups +
1.3.12.2.1107.1.3.4.272    ldapExtOpReadGroups +
1.3.12.2.1107.1.3.4.273    ldapExtOpExecuteGroups +
```

```
1.3.12.2.1107.1.3.4.274    ldapExtOpMonitoringGroups +
1.3.12.2.1107.1.3.4.275    ldapAllowedGroups +
1.3.12.2.1107.1.3.4.276    ldapDeniedGroups +
1.3.12.2.1107.1.3.4.284    ldapUserPolicies +
1.3.12.2.1107.1.3.4.289    ldapGroupPolicies +
-------------------------------------------------
```

1.4.7.5. See Also

ldap_cfg_upd, **ldap_show_cfg_audit**, **ldap_show_cfg_general**, **ldap_show_cfg_ssl**, **ldap_show_cfg_upd_history**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations**, **Attributes for LDAP Server Configuration**, **Attributes for LDAP Server SSL Configuration**, **Attributes for LDAP Server Audit Configuration** in *DirX Directory Syntaxes and Attributes*.

1.4.8. ldap_show_cfg_upd_history

1.4.8.1. Synopsis

ldap_show_cfg_upd_history

1.4.8.2. Purpose

Displays the update reports returned by the 25 most recent **ldap_cfg_upd** LDAP extended operations performed on an LDAP server.

1.4.8.3. Description

Use the **ldap_show_cfg_upd_history** LDAP extended operation to get information about the changes made over time to an LDAP server's configuration subentry. The most recent changes appear at the top of the list.

To run the extended operation, use the **dirxextop** command or the DirX Directory Manager's Monitoring view (**Monitoring** → **LDAP** → **Configuration** → **Show CFG-Update history**).

By default, the **ldap_show_cfg_upd_history** LDAP extended operation is listed in the LDAP Extended Read Operations attribute. Consequently, the DN of the user performing the extended operation must match a value in at least one of the following attributes: LDAP Extended Operations Admin/Admin Groups, LDAP Extended Operations Read Users/Groups. See the section **Attributes Controlling Extended Operations** in *DirX Directory Syntaxes and Attributes* for details.

Use the **ldap_show_cfg_upd_attr** LDAP extended operation to return the list of attributes available for dynamic update with the **ldap_cfg_upd** LDAP extended operation.

Use the **ldap_show_cfg_audit**, **ldap_show_cfg_general** and **ldap_show_cfg_ssl** and extended operations to display the currently active settings for an LDAP server configuration in readable format. Note that the attributes of the LDAP server SSL

configuration subentry and LDAP server audit configuration subentry can only be displayed; they cannot be dynamically updated.

1.4.8.4. Example

The following example shows how to apply the **ldap_show_cfg_upd_history** LDAP extended operation on the local LDAP server with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t
ldap_show_cfg__upd_history
```

This example shows a change to the Max LDAP Connection number from 555 (the value when the LDAP server was started) to 666 on the first update, to 777 on the second update. Each change is identified by the keyword >>CHANGED<<.

```
+++ LDAP-Update History at:Wed Jun 8 09:34:05.646305
Cfg-Name:ldapConfiguration
Total Updates Processed: 2
History-Protocols of last 25 Updates:
================================================================================
========
+++ LDAP-Cfg Update Started at:Wed Jun 8 09:33:39.994859
Cfg-Name:ldapConfiguration
UpdInfo: 1 previous updates suceeded. (LastSuccess: Wed Jun 8
09:30:17.520778)
UpdInfo: 0 previous updates failed.   (LastFail   : never)
--------------------------------------------------------------------------------
--------
Read access to CFG aquired.
Updating:Maximum Connections     (cfg-updated)=777  >>CHANGED<<
Updating:Conn Idle Time [sec]    (cfg-updated)=3000
Updating:Unbind Delay Time [sec] (cfg-updated)=0
Updating:Only Read-Ops allowed   (cfg-updated)=0
Updating:Backend Sharing         (cfg-updated)=1
Updating:Deny Anonymous Access   (default)=0
Updating:Only Anonym Allowed     (cfg-updated)=0
Updating:Max DAP-Conn Share Count(cfg-updated)=100
Updating:Max Req Search-Attr     (cfg-updated)=256
Updating:Max Search-Filter Items (cfg-updated)=128
LCFG Integer-Update finished.
--------------------------------------------------------------------------------
--------
```

```
SSL configuration will NOT be updated.
AUDIT configuration will NOT be updated.
--------------------------------------------------------------------
--------
Updating:IP Allow List           (default)=all
Updating:IP-Deny                 (cfg)=12.23.34.45 (net:2d22170c)
Updating:IP-Deny                 (cfg)=11.22.33.44 (net:2c21160b)
Updating:IP-Deny                 (cfg)=100.101.102.103 (net:67666564)
--------------------------------------------------------------------
--------
Updating:Denied User             (cfg):cn=bab jensen,ou=sales,o=my-
company
Updating:Denied User             (cfg):cn=g farfello,ou=sales,o=my-
company
Updating:Allowed Users           (default)=all
Updating:Allowed User Groups     (default)=none
Updating:Denied User Groups      (default)=none
--------------------------------------------------------------------
--------
Updating:ExtOp-Admin-Users       (cfg):cn=admin,o=my-company
Updating:ExtOp-Read-Users        (default)=none
Updating:ExtOp-Exec-Users        (cfg):cn=admin,o=my-company
Updating:ExtOp-Monitoring-Users  (default)=none
Updating:ExtOp-Admin-Groups      (cfg):ou=salesgroup,o=my-company (7
members)
Updating:ExtOp-Admin-Groups      (cfg):cn=ptgroup2,o=my-company
(29189 members)
Updating:ExtOp-Admin-Groups      (cfg):cn=hohner,ou=sales,o=my-
company (0 members)
Updating:ExtOp-Read-Groups       (cfg):ou=salesgroup,o=my-company (7
members)
Updating:ExtOp-Exec-Groups       (default)=none
Updating:ExtOp-Monitoring-Groups (default)=none
--------------------------------------------------------------------
--------
Updating:Search
ServiceControls(cfg)=PreferChaining=T:ChainingProhibited=F:LocalScope
=F:DontUseCopy=F:DontDereferenceAlias=F:Subentries=F:CopyShallDo=T:Pr
iority=1:TimeLimit=0:SizeLimit=0:ScopeOfReferral=0:AttributeSizeLimit
=0
Updating:Compare
```

```
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=F:dontDereferenceAlias=F:subentries=F:copyShalldo=T:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Add
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Remove
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Modify
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:ModifyDN
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
--------------------------------------------------------------------
--------
Reading updated LCFG from DSA OK. Going to exchange data in local
configuration...
Exchanged: Maximum Connections     =777 OK
Exchanged: Conn Idle Time [sec]    =3000 OK
Exchanged: Unbind Delay Time [sec] =0 OK
Exchanged: Only Read-Ops allowed   =0 OK
Exchanged: Backend Sharing         =1 OK
Exchanged: Deny Anonymous Access   =0 OK
Exchanged: Only Anonym Allowed     =0 OK
Exchanged: Max DAP-Conn Share Count=100 OK
Exchanged: Max Req Search-Attr     =256 OK
Exchanged: Max Search-Filter Items =128 OK
Exchanging Cfg-integers OK.
Exchanging IP Allow/Deny OK.
Cleanup IP Allow/Deny OK.
```

```
Exchanging User Allow/Deny OK.
Cleanup User Allow/Deny OK.
Exchanging Groups Allow/Deny OK.
Cleanup Groups Allow/Deny OK.
Exchanging Extop Privileges OK.
Cleanup Extop Privileges OK.
Exchanging Extop-Users Admin/Read/Exec/Mon OK.
Cleanup Extop-Users Admin/Read/Exec/Mon OK.
Exchanging Extop-Groups Admin/Read/Exec/Mon OK.
Cleanup Extop-Groups Admin/Read/Exec/Mon OK.
Exchanging ServiceControls OK.
LCFG-Exchange Finished OK.
Read access to LCFG released.
+++LDAP-Cfg Update Finished SUCCESSFUL at:Wed Jun 8 09:33:43.122789
================================================================================
========
--------------------------------------------------------------------------------
--------
================================================================================
========
+++ LDAP-Cfg Update Started at:Wed Jun 8 09:30:14.366041
Cfg-Name:ldapConfiguration
UpdInfo: 0 previous updates suceeded. (LastSuccess: never)
UpdInfo: 0 previous updates failed.   (LastFail   : never)
--------------------------------------------------------------------------------
--------
Read access to CFG aquired.
Updating:Maximum Connections     (cfg-updated)=666  >>CHANGED<<
Updating:Conn Idle Time [sec]    (cfg-updated)=3000
Updating:Unbind Delay Time [sec] (cfg-updated)=0
Updating:Only Read-Ops allowed   (cfg-updated)=0
Updating:Backend Sharing         (cfg-updated)=1
Updating:Deny Anonymous Access   (default)=0
Updating:Only Anonym Allowed     (cfg-updated)=0
Updating:Max DAP-Conn Share Count(cfg-updated)=100
Updating:Max Req Search-Attr     (cfg-updated)=256
Updating:Max Search-Filter Items (cfg-updated)=128
LCFG Integer-Update finished.
--------------------------------------------------------------------------------
--------
SSL configuration will NOT be updated.
```

```
AUDIT configuration will NOT be updated.
--------------------------------------------------------------------
--------
Updating:IP Allow List           (default)=all
Updating:IP-Deny                 (cfg)=12.23.34.45 (net:2d22170c)
Updating:IP-Deny                 (cfg)=11.22.33.44 (net:2c21160b)
Updating:IP-Deny                 (cfg)=100.101.102.103 (net:67666564)
--------------------------------------------------------------------
--------
Updating:Denied User             (cfg):cn=bab jensen,ou=sales,o=my-
company
Updating:Denied User             (cfg):cn=g farfello,ou=sales,o=my-
company
Updating:Allowed Users           (default)=all
Updating:Allowed User Groups     (default)=none
Updating:Denied User Groups      (default)=none
--------------------------------------------------------------------
--------
Updating:ExtOp-Admin-Users       (cfg):cn=admin,o=my-company
Updating:ExtOp-Read-Users        (default)=none
Updating:ExtOp-Exec-Users        (cfg):cn=admin,o=my-company
Updating:ExtOp-Monitoring-Users  (default)=none
Updating:ExtOp-Admin-Groups      (cfg):ou=salesgroup,o=my-company (7
members)
Updating:ExtOp-Admin-Groups      (cfg):cn=ptgroup2,o=my-company
(29189 members)
Updating:ExtOp-Admin-Groups      (cfg):cn=hohner,ou=sales,o=my-
company (0 members)
Updating:ExtOp-Read-Groups       (cfg):ou=salesgroup,o=my-company (7
members)
Updating:ExtOp-Exec-Groups       (default)=none
Updating:ExtOp-Monitoring-Groups (default)=none
--------------------------------------------------------------------
--------
Updating:Search
ServiceControls(cfg)=PreferChaining=T:ChainingProhibited=F:LocalScope
=F:DontUseCopy=F:DontDereferenceAlias=F:Subentries=F:CopyShallDo=T:Pr
iority=1:TimeLimit=0:SizeLimit=0:ScopeOfReferral=0:AttributeSizeLimit
=0
Updating:Compare
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
```

```
=F:dontUseCopy=F:dontDereferenceAlias=F:subentries=F:copyShalldo=T:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Add
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Remove
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:Modify
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
Updating:ModifyDN
ServiceControls(cfg)=preferChaining=T:chainingProhibited=F:localScope
=F:dontUseCopy=T:dontDereferenceAlias=F:subentries=F:copyShalldo=F:pr
iority=1:timelimit=0:sizelimit=0:scopeofreferral=0:attributesizelimit
=0
--------------------------------------------------------------------
--------
Reading updated LCFG from DSA OK. Going to exchange data in local
configuration...
Exchanged: Maximum Connections     =666 OK
Exchanged: Conn Idle Time [sec]    =3000 OK
Exchanged: Unbind Delay Time [sec] =0 OK
Exchanged: Only Read-Ops allowed   =0 OK
Exchanged: Backend Sharing         =1 OK
Exchanged: Deny Anonymous Access   =0 OK
Exchanged: Only Anonym Allowed     =0 OK
Exchanged: Max DAP-Conn Share Count=100 OK
Exchanged: Max Req Search-Attr     =256 OK
Exchanged: Max Search-Filter Items =128 OK
Exchanging Cfg-integers OK.
Exchanging IP Allow/Deny OK.
Cleanup IP Allow/Deny OK.
Exchanging User Allow/Deny OK.
```

```
Cleanup User Allow/Deny OK.
Exchanging Groups Allow/Deny OK.
Cleanup Groups Allow/Deny OK.
Exchanging Extop Privileges OK.
Cleanup Extop Privileges OK.
Exchanging Extop-Users Admin/Read/Exec/Mon OK.
Cleanup Extop-Users Admin/Read/Exec/Mon OK.
Exchanging Extop-Groups Admin/Read/Exec/Mon OK.
Cleanup Extop-Groups Admin/Read/Exec/Mon OK.
Exchanging ServiceControls OK.
LCFG-Exchange Finished OK.
Read access to LCFG released.
+++LDAP-Cfg Update Finished SUCCESSFUL at:Wed Jun 8 09:30:17.521376
================================================================
========
----------------------------------------------------------------
--------
```

1.4.8.5. See Also

ldap_cfg_upd, **ldap_show_cfg_audit**, **ldap_show_cfg_general**, **ldap_show_cfg_ssl**, **ldap_show_cfg_upd_attr**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations**, **Attributes for LDAP Server Configuration**, **Attributes for LDAP Server SSL Configuration**, **Attributes for LDAP Server Audit Configuration** in *DirX Directory Syntaxes and Attributes*.

1.4.9. ldap_show_config_dsas

1.4.9.1. Synopsis

ldap_show_config_dsas

1.4.9.2. Purpose

Displays the currently active contact DSA table.

1.4.9.3. Description

The **ldap_show_config_dsas** LDAP extended operation allows DirX Directory administrators to display status information about the DSAs in currently active contact DSA table. It is intended for use in a multiple contact DSA configuration, where an LDAP server has a list of contact DSAs from which it can choose. Using multiple contact DSAs in a master-shadow configuration enables DAP operations to be distributed among the consumer DSAs in a shadow configuration and provides simple failover capability in the event that one contact DSA fails or needs to be taken offline for maintenance. For details about this configuration, see the chapter “Using Multiple Contact DSAs” in the *DirX Directory Administration Guide*.

The **ldap_show_config_dsas** operation is performed without any restriction or authentication. Use the operation in conjunction with the LDAP extended operations **ldap_disable_config_dsa** and **ldap_enable_config_dsa** to monitor and manage the contact DSAs in a master-shadow configuration.

The contact DSA table displays the following information:

- The name of the server where the LDAP server is running.
- The date and time when the information is collected.
- For each contact DSA:
  - The name of the DSA. An asterisk (*****) in front of the DSA name indicates that this DSA will be selected for the next bind request.
  - The status of the DSA. Possible values are:
    - **enabled**—The DSA is enabled and ready to receive the next bind request.
    - **perm disabled**—The DSA is permamently disabled; that is, it is disabled for the lifetime of the LDAP server process or until it is re-enabled with the LDAP extended operation the **ldap_enable_config_dsa**.
    - **temp disabled**—The DSA is temporarily disabled. When a bind request to a selected contact DSA fails, the LDAP server disables the DSA for a configurable time period. The default is 60 seconds and can be changed with the **DIRX_AUTO_DISABLE_FAILING_DSA** environment variable. When this time period expires, this DSA is automatically re-enabled. The time period after which this DSA will be automatically re-enabled is also shown.
  - The PSAP address of the DSA.
  - The number of failed bind requests.
  - The number of permament deactivations of the DSA.
  - The number of temporary deactivations of the DSA and the date and time of the last recent temporary deactivation.
  - The number of re-activations of the DSA.
  - The number of selections for bind requests.

The LDAP server iterates through the active contact DSA table to select contact DSAs. DSAs that are not enabled are skipped in the selection.

Use the **ldap_disable_config_dsa** operation to disable a DSA permanently; that is, for the lifetime of the LDAP server process (the DSA is automatically re-enabled when the LDAP server is re-started). Use the **ldap_enable_config_dsa** operation to enable a DSA.

At least one DSA must be in the enabled status regardless of the event of failed bind requests or explicitly performed **ldap_disable_config_dsa** operations; that is, the last DSA is not temporarily disabled after a bind request fails and an **ldap_disable_config_dsa** extended operation to this DSA will fail.

1.4.9.4. Example

The following example shows how to apply the **ldap_show_config_dsas** LDAP extended operation with the **dirxextop** command:

```
dirxextop -t ldap_show_config_dsas
```

The sample output is as follows:

```
List of configured Contact-DSAs for LDAP server on
'hugo' at Tue May 17 14:21:26.335769

=================================================================
 DSA-Name:/CN=DSA1
    Status      :temp disabled (for next 50 sec)
 PSAP:TS=DSA1,NA='TCP/IP_IDM!internet=1.2.3.4+port=4711',DNS='(HOST=h
ugo,SSLPORT=21201,PLAINPORT=21200,MODE=ssl)'
    BindFails   :2
    PermDisables:0
    TempDisables:2  (Last: Tue May 17 14:21:15.753710)
    ReEnables   :1
    Selections  :5
-----------------------------------------------------------------
*DSA-Name:/CN=DSA3
    Status      :enabled
    PSAP
:TS=DSA1,NA='TCP/IP_IDM!internet=1.2.3.4+port=4711',DNS='(HOST=hugo,S
SLPORT=21201,PLAINPORT=21200,MODE=plain)'
    BindFails   :2
    PermDisables:0
    TempDisables:0
    ReEnables   :0
    Selections  :6
-----------------------------------------------------------------
 DSA-Name:/CN=DSA5
    Status      :perm disabled
    PSAP
:TS=DSA1,NA='TCP/IP_IDM!internet=1.2.3.4+port=4711',DNS='(HOST=hugo,S
SLPORT=21201,PLAINPORT=21200,MODE=plain)'
    BindFails   :2
    PermDisables:1
```

```
    TempDisables:2  (Last: Tue May 17 14:21:14.657613)
    ReEnables   :1
    Selections  :4
-------------------------------------------------------------------

(*) == DSA to be selected for next Backend-Bind
```

The example output shows that on the server **hugo**, DSAs **/CN=DSA1** and **/CN=DSA5** are excluded from selection while **/CN=DSA3** is available.The table shows that **/CN=DSA1** is temporarily disabled (a DAP bind failed) and will be re-tried in 50 seconds. **/CN=DSA5** is permanently disabled (via the LDAP external operation **ldap_disable_config_dsa**) and will be excluded for selection until it is re-enabled explicitly via the the LDAP external operation **ldap_enable_config_dsa** or until the LDAP server is re-started.

The asterisk (**) in front of */CN=DSA3** indicates that it is the next target for selection. **/CN=DSA1** is excluded for selection for the next 50 seconds. **/CN=DSA5** is permanently excluded from selection.

1.4.9.5. See Also

ldap_disable_config_dsa, **ldap_enable_config_dsa**, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*, **Environment Variables** in the *DirX Directory Administration Reference*.

1.4.10. ldap_show_policy_rules

1.4.10.1. Synopsis

ldap_show_policy_rules

1.4.10.2. Purpose

Displays the currently active user and group policies.

1.4.10.3. Description

Use the **ldap_show_policy_rules** LDAP extended operation to display the currently active user and group policies. The output consists of the following sections:

- A header section that provides general information, like the number of rules and the number of users; for example:

  ```
  LDAP-User-Policy Count: 1  (1st is newest) at: Tue Mar 21
  10:48:53.467559
  ================== LDAP USER POLICY RULES
  ================================
  ```

```
LDAP-User-Policy Rules:
Policy-ID: 1
Create-Time               : Tue Mar 21 10:48:29.983315
Total Allocated Handles   : 1
Total Registered Users    : 1
Total Rules               : 11
Total Rules-Parse-Err     : 0
Curr/Max Group-Rule Users : 14/1000000
Rules for anonymous       : yes
Rules for all             : yes
Memory in use by LUP      : 131072
```

where

LDAP-User-Policy Count—displays the number of policy versions the LDAP server maintains in memory. In this example, there is only one version. There is also a timestamp that indicates when the LDAP server performed **ldap_show_policy_rules**.

Policy-ID—indicates the number of times the policies were updated dynamically. This counter is incremented each time a dynamic update is performed. (See **ldap_cxfg_update** for details.) In this example, the policies became operative at start-up; there was no dynamic update.

Create-Time—specifies the time at which the policies were created. In this example, it is the startup-time of the LDAP server. If the value is greater than 1, it is the timestamp of the dynamic update.

Total Allocated Handles—specifies the total number of handles. The LDAP server allocates a handle for each user that establishes a connection to the server. The handle identifies the user and the connection. The LDAP server destroys the handle when the associated connection ends, for example, with an unbind operation. The LDAP server uses the handle in all operations following the bind opration to check the user's policies. In the example, there is 1 handle.

Total Registered Users—specifies the total number of registered users. The LDAP server registers a user to the LDAP user policies when the user establishes a connection to the LDAP server. The user remains registered as long as he is connected to the LDAP server. When registering the user, the LDAP server allocates a policy handle. (See **Total Allocated Handles** for details.) In the example there is 1 user.

Total Rules—indicates the total number of rules that are in effect. In the example, there are 11 rules.

Total Rules Parse Errors—indicates the number of errors that occur when the LDAP server parses the rules of the policies. If a parsing error occurs, the LDAP server ignores the rule and increments this counter. In the example, no parsing error occurred.

Curr/Max Group-Rule Users—indicates the number of users that are members of

groups and the maximum number of users that can be members in groups. In the example, there are 14 group members. The maximum number of group members for a rule is one million.

Rules for anonymous—indicates whether or not there are rules for users that perform anonymous binds to the LDAP server. In the example, there are rules for anonymous users.

Rules for all—indicates whether or not there are rules for all users. In the example, there are rules for all users.

Memory in use by LUP—specifies the number of bytes that the policies consume. If there are old handles, the LDAP server maintains both the current active policies and all old policies associated with the old handles. In the example, the user and group policies consume 131,072 bytes.

- The **USER** rules for each user, for example:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++
                  8 EXPLICIT USER RULES
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++
 Rule#1  User:'all' (Prio:1)
 Inherit             : yes
 SizeLimit           : 100
------------------------------------------------------------------------
----------
 Rule#2  User:'anonymous' (Prio:0)
 ConnLimit           : 2
 TimeLimit           : 11
*SizeLimit           : 100
 TLS required        : no
 Disclose Violation  : no
 Must-Contact-DSA    : /CN=DSA3
 Forbidden SrchBase  : ou=development2,o=pqr (0 Hits)
 Forbidden TargetObj : cn=richter,ou=sales,o=pqr (0 Hits)
------------------------------------------------------------------------
----------
 Rule#3  User:'cn=admin,o=pqr' (Prio:1)
 ConnLimit           : 7
*SizeLimit           : 100
 TLS required        : no
 Disclose Violation  : no
```

```
 Forbidden TargetObj : o=ocsi,o=central,dc=hlr,o=pqr (0 Hits)
 Forbidden TargetObj : ou=salesx,o=pqr (0 Hits)
 Forbidden TargetObj : cn=admin,o=pqr (0 Hits)
-----------------------------------------------------------------
-----------
…
```

The **USER** rules section begins with the total number of explicit user rules and then lists all user rules. If a user rule property is prefixed by an asterisk (**), for example SizeLimit**, the property is inherited from the rule for all users (**all**). The **Hits** counter indicates how often a user addressed the item in operations. For detailed information about policies, rules and properties, see **LDAP User Policies Attribute** in *DirX Directory Syntaxes and Attributes*.

- The **WCUSER** (wildcard user) rules, for example:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
                   4 WCUSER RULES
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
 Rule#1   WildcardPattern:'^cn=Hohner.*' (Prio:0)
 ConnLimit           : 5
 TimeLimit           : 20
*SizeLimit           : 100
…
```

The **WCUSER** rules section begins with the total number of wildcard user rules and then lists all wildcard user rules according to their priority in the same format as the **USER** rules section.

- The **SUBUSER** rules, for example:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++
                   1 SUBORDINATE USER RULES
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
 Rule#1   SubOrd:'ou=sales2,o=pqr' (Prio:1)
 ConnLimit           : 3
*SizeLimit           : 100
 TLS required        : 0
 Disclose Violation  : no
```

```
 Forbidden SrchBase  : ou=development,o=pqr (0 Hits)
 Forbidden TargetObj : ou=something,o=somewhere (0 Hits)
 Quota               : Max 100 Ops within 86400 sec
 Quota               : Max 100000 Bytes in Search-Results within 3
sec
```

The **SUBUSER** rules section begins with the total of rules for subordinate users and then lists all rules for subordinate users in the same format as the **USER** rules section.

- The **GROUPS** rules, for example:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
                    2 GROUPS WITH USER RULES
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
 GroupRule#2 : ou=mygroup,o=pqr  (Prio:0, 11 Group-Members, 11 Users
affected)
 TimeLimit           : 22
*SizeLimit           : 100
 Forbidden SrchBase  : ou=development,o=pqr
 Quota               : Max 50 Ops within 60 sec
 Quota               : Max 100 Bytes in Search-Results within 5 sec
----------------------------------------------------------------------
--------
 GroupRule#1 : ou=salesgroup,o=pqr  (Prio:1, 14 Group-Members, 3
Users affected)
 ConnLimit           : 4
*SizeLimit           : 100
----------------------------------------------------------------------
--------
----------------------------------------------------------------------
--------
                    14 USERS with GROUP RULES
----------------------------------------------------------------------
--------
  Group  | Tab | Member |
  Rule#  | Idx | Ships  | User
----------------------------------------------------------------------
--------
      1  |    0|      1 | cn=abale7,ou=salesx,o=pqr
```

```
      1  |    1|      1 | cn=adriana brummitt,ou=product
testing,o=pqr
      1  |    2|      1 | cn=ara krowlek,ou=product testing,o=pqr
      2* |    3|      2 | cn=digger,ou=development,o=pqr
…
```

The **GROUP** rules section begins with the total number of group rules and then lists all rules for groups in the same format as the **USER** rules section. A table follows the group rules that indicates which group rule applies to which user. An asterisk (*****) appended to the group rule indicates a priority overrule between groups. In the example, there are two group rules: **GroupRule#2** and **GroupRule#1**. The priority of **Group Rule#2** is **0** while the priority of **GroupRule#1** is **1**. The user **cn=digger,ou=development,o=pqr** is a member of both groups, so the **GroupRule#2** rule overrules the **GroupRule#1** rule for this user.

1.4.10.4. Example

The following example shows how to apply the **ldap_show_policy_rules** LDAP extended operation with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_show_policy_rules
```

In the example, the LDAP extended operation returns the following output:

```
LDAP-User-Policy Count: 1  (1st is newest) at: Tue Mar 21
10:48:53.467559
================== LDAP USER POLICY RULES
=================================
 LDAP-User-Policy Rules:
 Policy-ID: 1
 Create-Time               : Tue Mar 21 10:48:29.983315
 Total Allocated Handles   : 1
 Total Registered Users    : 1
 Total Rules               : 11
 Total Rules-Parse-Err     : 0
 Curr/Max Group-Rule Users : 14/1000000
 Rules for anonymous       : yes
 Rules for all             : yes
 Memory in use by LUP      : 131072
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
                  8 EXPLICIT USER RULES
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

```
++++++++
 Rule#1  User:'all' (Prio:1)
 Inherit             : yes
 SizeLimit           : 100
-------------------------------------------------------------------
--------
 Rule#2  User:'anonymous' (Prio:0)
 ConnLimit           : 2
 TimeLimit           : 11
*SizeLimit           : 100
 TLS required        : no
 Disclose Violation  : no
 Must-Contact-DSA    : /CN=DSA3
 Forbidden SrchBase  : ou=development2,o=pqr (0 Hits)
 Forbidden TargetObj : cn=richter,ou=sales,o=pqr (0 Hits)
-------------------------------------------------------------------
--------
 Rule#3  User:'cn=admin,o=pqr' (Prio:1)
 ConnLimit           : 7
*SizeLimit           : 100
 TLS required        : no
 Disclose Violation  : no
 Forbidden TargetObj : o=ocsi,o=central,dc=hlr,o=pqr (0 Hits)
 Forbidden TargetObj : ou=salesx,o=pqr (0 Hits)
 Forbidden TargetObj : cn=admin,o=pqr (0 Hits)
-------------------------------------------------------------------
--------
 Rule#4  User:'cn=digger,ou=development,o=pqr' (Prio:4)
 ConnLimit           : 4
*SizeLimit           : 100
 TLS required        : no
 Disclose Violation  : no
-------------------------------------------------------------------
--------
 Rule#5  User:'cn=hohner,ou=sales,o=pqr' (Prio:1)
 ConnLimit           : 3
 TimeLimit           : 11
*SizeLimit           : 100
 Forbidden SrchBase  : ou=sales2,o=pqr (0 Hits)
 Forbidden TargetObj : cn=richter,ou=sales,o=pqr (0 Hits)
-------------------------------------------------------------------
```

```
--------
 Rule#6  User:'cn=reichel,ou=sales,o=pqr' (Prio:1)
 ConnLimit           : 25
 TimeLimit           : 30
*SizeLimit           : 100
------------------------------------------------------------------------
--------
 Rule#7  User:'cn=richter2,ou=sales,o=pqr' (Prio:1)
 ConnLimit           : 17
 TimeLimit           : 20
 SizeLimit           : 5
 Min SrchBase RDNs   : 2
------------------------------------------------------------------------
--------
 Rule#8  User:'cn=smith john,ou=sales,o=pqr' (Prio:1)
 ConnLimit           : 37
 TimeLimit           : 40
*SizeLimit           : 100
------------------------------------------------------------------------
--------
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
                  4 WCUSER RULES
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
 Rule#1   WildcardPattern:'^cn=Hohner.*' (Prio:0)
 ConnLimit           : 5
 TimeLimit           : 20
*SizeLimit           : 100
------------------------------------------------------------------------
--------
 Rule#2   WildcardPattern:'^cn=Digger.*' (Prio:0)
 ConnLimit           : 4
 TimeLimit           : 30
*SizeLimit           : 100
------------------------------------------------------------------------
--------
 Rule#3   WildcardPattern:'^cn=.*igger' (Prio:1)
 ConnLimit           : 3
 TimeLimit           : 30
*SizeLimit           : 100
```

```
-------------------------------------------------------------------------
--------
 Rule#4   WildcardPattern:'^cn=D.*gger' (Prio:3)
 ConnLimit           : 2
 TimeLimit           : 30
*SizeLimit           : 100
-------------------------------------------------------------------------
--------
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
                    1 SUBORDINATE USER RULES
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
 Rule#1   SubOrd:'ou=sales2,o=pqr' (Prio:1)
 ConnLimit           : 3
*SizeLimit           : 100
 TLS required        : 0
 Disclose Violation  : no
 Forbidden SrchBase  : ou=development,o=pqr (0 Hits)
 Forbidden TargetObj : ou=something,o=somewhere (0 Hits)
 Quota               : Max 100 Ops within 86400 sec
 Quota               : Max 100000 Bytes in Search-Results within 3
sec
-------------------------------------------------------------------------
--------
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
                    2 GROUPS WITH USER RULES
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
 GroupRule#2 : ou=mygroup,o=pqr  (Prio:0, 11 Group-Members, 11 Users
affected)
 TimeLimit           : 22
*SizeLimit           : 100
 Forbidden SrchBase  : ou=development,o=pqr
 Quota               : Max 50 Ops within 60 sec
 Quota               : Max 100 Bytes in Search-Results within 5 sec
-------------------------------------------------------------------------
--------
 GroupRule#1 : ou=salesgroup,o=pqr  (Prio:1, 14 Group-Members, 3
Users affected)
```

```
 ConnLimit           : 4
*SizeLimit           : 100
------------------------------------------------------------------------
--------
------------------------------------------------------------------------
--------
                   14 USERS with GROUP RULES
------------------------------------------------------------------------
--------
  Group   | Tab | Member |
  Rule#   | Idx | Ships  | User
------------------------------------------------------------------------
--------
      1   |    0|      1 | cn=abale7,ou=salesx,o=pqr
      1   |    1|      1 | cn=adriana brummitt,ou=product
testing,o=pqr
      1   |    2|      1 | cn=ara krowlek,ou=product testing,o=pqr
      2*  |    3|      2 | cn=digger,ou=development,o=pqr
      2*  |    4|      2 | cn=hohner,ou=sales,o=pqr
      2*  |    5|      2 | cn=mayer,ou=sales,o=my-company
      2*  |    6|      2 | cn=morton,ou=development,o=pqr
      2*  |    7|      2 | cn=nörgler,ou=sales2,o=pqr
      2*  |    8|      2 | cn=reichel,ou=sales,o=pqr
      2*  |    9|      2 | cn=richter,ou=sales,o=pqr
      2*  |   10|      2 | cn=tinker,ou=development,o=pqr
      2*  |   11|      2 | uid=user.1010,ou=people,o=pqr
      2*  |   12|      2 | uid=user.1011,ou=people,o=pqr
      2*  |   13|      2 | uid=user.1012,ou=people,o=pqr
------------------------------------------------------------------------
----------
Note1: '*' behind GroupRule# indicates a priority overrule between
multiple groups
Note2: Rule-Classes are evaluated in the order USER -> GROUP ->
WCUSER -> SUBORDINATE -> ALL
       First found rule wins.
       Rules for 'anonymous' must be defined as USER rule.
       Rules for 'ALL' must be defined as USER rule.
Note3: '*' before a property-name indicates inherintance from the
ALL-rule.
==================== End of Policy
```

```
=====================================
```

1.4.10.5. See Also

ldap_show_policy_users, **ldap_show_single_user_policy_rules, LDAP User Policies Attribute** in *DirX Directory Syntaxes and Attributes*, **LDAP Group Policies Attribute** in *DirX Directory Syntaxes and Attributes*, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*.

1.4.11. ldap_show_policy_users

1.4.11.1. Synopsis

ldap_show_policy_users

1.4.11.2. Purpose

Displays the current status of each registered user.

1.4.11.3. Description

Use the **ldap_show_policy_users** LDAP extended operation to display the status of all registered users. The output consists of the following sections:

- A header section that provides general information, like the number of registered users and the number of rules; for example:

```
LDAP-User-Policy Registered Users at:Tue Mar 21 11:03:59.954718
 Policy-ID: 1
 Create-Time             : Tue Mar 21 10:48:29.983315
 Allocated Handles       : 2
 Total Registered Users  : 2
 Total USER Rules        : 8
 Total GROUP Rules       : 2
 Total WCUSER Rules      : 4
 Total SUBUSER Rules     : 1
 Rules for anonymous     : yes
 Rules for all           : yes
```

  where

  LDAP-User-Policy Registerd Users at—displays the time at which **ldap_show_policy_users** was performed.

  Policy-ID—specifies the number of times the policies were updated dynamically. (See

ldap_cxfg_update for details.) In this example, the policies became operative at start-up; there was no dynamic update.

Create-Time—indicates the time at which the policies were created. In this example, it is the startup-time of the LDAP server. If the value is greater than 1, it is the timestamp of the dynamic update.

Allocated Handles—specifies the number of handles. The LDAP server allocates a handle for each user that establishes a connection to the server. The handle identifies the user and the connection. The LDAP server destroys the handle when the associated connection ends, for example, with an unbind operation. The LDAP server uses the handle in all operations following to the bind operation to check the user's policies. In the example, there are two handles.

Total Registered Users—indicates the total number of registered users. The LDAP server registers a user to the LDAP user policies when he establishes a connection to the LDAP server. The user remains registered as long as he is connected to the LDAP server. When registering the user, the LDAP server allocates a policy handle. (See **Allocated Handles** for details.) In the example there are two users.

Total USER Rules—specifies the total number of user rules that are in effect.

Total GROUP Rules—specifies the total number of group rules that are in effect.

Total WCUSER Rules—specifies the total number of wildcard user rules that are in effect.

Total SUBUSER Rules—specifies the total number of subordinate user rules that are in effect.

Rules for anonymous—indicates whether or not there are rules for users that perform anonymous binds to the LDAP server.

Rules for all—indicates whether or not there are rules for all users.

- Sections that list all currently registered users to the following classes:
  - **USER** rules
  - **GROUP** rules
  - **WCUSER** (wildcard user) rules
  - **SUBUSER** (subordinate user) rules
  - without (w/o) any rules

  These sections list:
  - The number of users registerd to the class; for example:

    ```
    Users Registered to USER-Rules : 1
    ```

- The distinguished names of all users for whom the user rule applies, where **reg-count** provides the number of LDAP connections that the user has established; for example:

```
User#1: cn=admin,o=pqr (idx:2,reg-count:1)
```

- The user rule and detailed information about the status of the registered user; for example:

```
conn-limit:7, conn-limit-hits:0, conn-count:1
```

- A section that lists the total number of registrations to all classes; for example:

```
Total Registrations to USER rules   :5
Total Registrations to GROUP rules  :1
Total Registrations to WCUSER rules :0
Total Registrations to SUBUSER rules:0
Total Registrations to ALL rules    :0
Total Registrations w/o rules       :0
```

1.4.11.4. Example

The following example shows how to apply the **ldap_show_policy_users** LDAP extended operation with the **dirxextop** command:

```
dirxextop -D cn=admin,o=my-company -w dirx -t ldap_show_policy_users
```

In the example, the LDAP extended operation returns the following output:

```
=====================================================================
==
LDAP-User-Policy Registered Users at:Tue Mar 21 11:03:59.954718
 Policy-ID: 1
 Create-Time             : Tue Mar 21 10:48:29.983315
 Allocated Handles       : 2
 Total Registered Users  : 2
 Total USER Rules        : 8
 Total GROUP Rules       : 2
 Total WCUSER Rules      : 4
 Total SUBUSER Rules     : 1
```

```
 Rules for anonymous     : yes
 Rules for all           : yes
-------------------------------------------------------------------
--
Users Registered to USER-Rules    : 1
  User#1: cn=admin,o=pqr (idx:2,reg-count:1)
    conn-limit:7, conn-limit-hits:0, conn-count:1
-------------------------------------------------------------------
--
Users Registered to GROUP-Rules   : 1
  User#1: cn=richter,ou=sales,o=pqr (idx:9,reg-count:1)
    quota-ops-count:1, quota: Max 50 Ops within 60 sec. (Reset in 56
sec)
    quota-res-bytes-count:0, quota: Max 100 Search-Result-Bytes
within 5 sec. (Reset in 0 sec)
-------------------------------------------------------------------
--
Users Registered to WCUSER Rules : 0
-------------------------------------------------------------------
--
Users Registered to SUBUSER Rules : 0
-------------------------------------------------------------------
--
Users Registered to ALL-Rules     : 0
-------------------------------------------------------------------
--
Users Registered w/o Rules        : 0
-------------------------------------------------------------------
--
Total Registrations to USER rules   :5
Total Registrations to GROUP rules  :1
Total Registrations to WCUSER rules :0
Total Registrations to SUBUSER rules:0
Total Registrations to ALL rules    :0
Total Registrations w/o rules       :0
===================================================================
==
```

1.4.11.5. See Also

ldap_show_policy_rules, **ldap_show_single_user_policy_rules**, **LDAP User Policies**

Attribute in *DirX Directory Syntaxes and Attributes*, **LDAP Group Policies Attribute** in *DirX Directory Syntaxes and Attributes*, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*.

1.4.12. ldap_show_single_user_policy_rules

1.4.12.1. Synopsis

ldap_show_single_user_policy_rules *user*

1.4.12.2. Purpose

Displays all rules that apply to the specified user.

1.4.12.3. Parameters

user
the full qualified user's distinguished name in LDAP format; for example, **USER=cn=admin,o=my-company**. (For details about distinguished names in LDAP format, see **Distinguished Names** in the chapter **DirX Directory String Representation for LDAP Binds** in *DirX Directory Syntaxes and Attributes*.)

1.4.12.4. Description

Use the **ldap_show_single_user_policy_rules** to display all rules that apply to the specified *user*. Specify the user's distinguished name in LDAP format or one of the following keywords:

all—returns the rules that apply to all users.

anonymous—returns the rules that apply to anonymous users.

The output consists of the following sections:

- A header section that provides general information; for example:

  ```
  LDAP-User-Policy Rules at: Thu Nov 17 11:03:59.954718
  Policy-ID: 1
  ```

  where

  LDAP-User-Policy Rules at—displays the timestamp when **ldap_show_single_user_policy_rules** is performed.

  Policy-ID—indicates the number of times the policies were updated dynamically. (See **ldap_cxfg_update** for details.) In this example, the policies became operative at startup; there was no dynamic update.

- A section that provides the user's distinguished name and details on the rules that apply for this user, for example:

```
 User            : cn=richter,ou,sales,o=my-company
 Prio            : 0
 RuleClass       : GROUP
 RuleGroup       : ou=mygroup,o=my-company
*ConnLimit       : 3 (1)
 TimeLimit       : 22
…
```

  If a user rule property is prefixed with an asterisk (**), for example, ConnLimit**, the property is inherited from the rule for all users (**all**).

  For detailed information about policies, rules and properties, see **LDAP User Policies Attribute** in *DirX Directory Syntaxes and Attributes*.

Use the result to check the user's rules against the currently active user and group policies.

1.4.12.5. Example

The following example shows how to apply the **ldap_show_single_user_policy_rules** LDAP extended operation with the **dirxextop** command. In the example, the rules are requested for the user **cn=richter,ou=sales,o=my-company**:

```
dirxextop -D cn=admin,o=my-company -w dirx -t
ldap_show_single_user_policy_rules -P cn=richter,ou=sales,o=my-
company
```

In the example, the LDAP extended operation returns the following output:

```
===================== LDAP SINGLE-USER POLICY
==============================
 LDAP-User-Policy Rules at: Thu Nov 17 11:03:59.954718
 Policy-ID: 1
------------------------------------------------------------------------
-------
 User               : cn=richter,ou,sales,o=my-company
 Prio               : 0
 RuleClass          : GROUP
 RuleGroup          : ou=mygroup,o=my-company
*ConnLimit          : 3 (1)
```

```
 TimeLimit           : 22
*Min SrchBase RDNs   : 1
 Forbidden SrchBase  : ou=development,o=my-company
 Quota               : Max 50 Ops within 60 sec (3)
 Quota               : Max 10000 Search-Result-Bytes within 60 sec
(2604)
-------------------------------------------------------------------
-------
```

In this example, the LDAP server performed **ldap_show_single_user_policy_rules** on **Thu Nov 17 11:03:59.954718**. No dynamic update took place since LDAP server startup (**Policy-ID: 1**). There are policy rules for user **cn=richter,ou=sales,o=my-company**. The priority of the rules is the highest one (**Prio : 0**). The rules are derived from the user's membership in the group **ou=mygroup,o=my-company** (**RuleClass : Group**; **RuleGroup : ou=mygroup,o=my-company**). The rules **ConnLimit** and **Min SrchBase RDNs** are inherited from the rules for all users because they are prefixed with an asterisk (*****). The user has established 1 LDAP server connection; the maximum number of LDAP connections is **3** (***ConnLimit : 3 (1)**). His time limit for search requests is 22 seconds (**TimeLimit : 22**). The base object of a search request must have at least 1 RDN (***Min SrchBase RDNs : 1**); that is, the root object in search requests is not allowed. The user cannot perform search requests with a base object **ou=development,o=my-company** (**Forbidden SrchBase**). The maximum number of operations is **50 within 60 seconds** (**Quota**); the user has already performed **3** operations **(3)**. The maximum number of bytes in a search request is **10000 Search-Result Bytes within 60 sec**onds (**Quota**); the user has already received **2604** bytes **(2604)**.

1.4.12.6. See Also

ldap_show_policy_rules, ldap_show_policy_users, **LDAP User Policies Attribute** in *DirX Directory Syntaxes and Attributes*, **LDAP Group Policies Attribute** in *DirX Directory Syntaxes and Attributes*, **dirxextop** in the *DirX Directory Administration Reference*, **Attributes Controlling LDAP Extended Operations** in *DirX Directory Syntaxes and Attributes*.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.