

EVIDEN

Identity and Access Management

DirX Directory

Nagios Plugins

Version 9.1, Edition June 2025



All product names quoted are trademarks or registered trademarks of the manufacturers concerned.

© 2025 Eviden

All Rights Reserved

Distribution and reproduction not permitted without the consent of Eviden.

Table of Contents

Copyright	ii
Preface	1
DirX Directory Documentation Set	2
Notation Conventions	3
1. DirX Directory Nagios Plugins	4
1.1. General Information	4
1.1.1. Prerequisites and Limitations	4
1.1.2. Installation Location	5
1.1.3. Plugin Operation	5
1.1.4. Plugin Configuration	6
1.1.4.1. Common Plugin Syntax	6
1.1.5. Common Return Code Format	8
1.2. DirX Directory Nagios Plugins Reference Descriptions	10
1.2.1. check_dirx_backup_status	10
1.2.1.1. Synopsis	10
1.2.1.2. Purpose	10
1.2.1.3. Arguments	10
1.2.1.4. Options	10
1.2.1.5. Description	10
1.2.1.6. Return Values	11
1.2.1.7. Example	11
1.2.1.8. See Also	12
1.2.2. check_dirx_ctx	12
1.2.2.1. Synopsis	12
1.2.2.2. Purpose	12
1.2.2.3. Arguments	12
1.2.2.4. Options	12
1.2.2.5. Description	12
1.2.2.6. Return Values	13
1.2.2.7. Example	14
1.2.2.8. See Also	15
1.2.3. check_dirx_dbam_preload_status	15
1.2.3.1. Synopsis	15
1.2.3.2. Purpose	15
1.2.3.3. Options	15
1.2.3.4. Description	15
1.2.3.5. Return Values	15
1.2.3.6. Example	16
1.2.3.7. See Also	16

1.2.4. check_dirx_dbam_usage	16
1.2.4.1. Synopsis	16
1.2.4.2. Purpose	16
1.2.4.3. Arguments	16
1.2.4.4. Options	16
1.2.4.5. Description	16
1.2.4.6. Return Values	17
1.2.4.7. Example	18
1.2.4.8. See Also	19
1.2.5. check_dirx_dsa_get_opmode	19
1.2.5.1. Synopsis	19
1.2.5.2. Purpose	19
1.2.5.3. Options	19
1.2.5.4. Description	19
1.2.5.5. Return Values	20
1.2.5.6. Example	20
1.2.5.7. See Also	20
1.2.6. check_dirx_heartbeat	20
1.2.6.1. Synopsis	20
1.2.6.2. Purpose	21
1.2.6.3. Arguments	21
1.2.6.4. Options	21
1.2.6.5. Description	22
1.2.6.6. Return Values	22
1.2.6.7. Example	23
1.2.6.8. See Also	23
1.2.7. check_dirx_ldap_current	23
1.2.7.1. Synopsis	23
1.2.7.2. Purpose	23
1.2.7.3. Arguments	23
1.2.7.4. Options	25
1.2.7.5. Description	25
1.2.7.6. Return Values	27
1.2.7.7. Examples	27
1.2.7.8. See Also	28
1.2.8. check_dirx_ldap_duration	28
1.2.8.1. Synopsis	28
1.2.8.2. Purpose	28
1.2.8.3. Arguments	28
1.2.8.4. Options	29
1.2.8.5. Description	29
1.2.8.6. Return Values	30

1.2.8.7. Example	30
1.2.8.8. See Also	31
1.2.9. check_dirx_ldap_resultsize	31
1.2.9.1. Synopsis	31
1.2.9.2. Purpose	31
1.2.9.3. Arguments	31
1.2.9.4. Options	31
1.2.9.5. Description	32
1.2.9.6. Return Values	32
1.2.9.7. Example	33
1.2.9.8. See Also	33
1.2.10. check_dirx_ldap_totals	33
1.2.10.1. Synopsis	33
1.2.10.2. Purpose	34
1.2.10.3. Arguments	34
1.2.10.4. Options	36
1.2.10.5. Description	36
1.2.10.6. Return Values	38
1.2.10.7. Example	38
1.2.10.8. See Also	39
1.2.11. check_dirx_no_of_fds	39
1.2.11.1. Synopsis	39
1.2.11.2. Purpose	39
1.2.11.3. Arguments	39
1.2.11.4. Options	39
1.2.11.5. Description	40
1.2.11.6. Return Values	41
1.2.11.7. Example	41
1.2.11.8. See Also	41
1.2.12. check_dirx_paging	42
1.2.12.1. Synopsis	42
1.2.12.2. Purpose	42
1.2.12.3. Arguments	42
1.2.12.4. Options	42
1.2.12.5. Description	42
1.2.12.6. Return Values	43
1.2.12.7. Example	43
1.2.12.8. See Also	44
1.2.13. check_dirx_server_files	44
1.2.13.1. Synopsis	44
1.2.13.2. Purpose	44
1.2.13.3. Arguments	44

1.2.13.4. Options	44
1.2.13.5. Description	45
1.2.13.6. Return Values	45
1.2.13.7. Example	46
1.2.13.8. See Also	47
1.3. DirX Directory Nagios Plugin Configuration File	47
1.3.1. check_dirx_config.pm	47
1.3.1.1. Purpose	47
1.3.1.2. Description	47
1.3.1.3. Example	48
Legal Remarks	51
Index	52

Preface

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

- Chapter 1 contains reference pages for DirX Directory plugins for Nagios.

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 Nagios Plugins

The DirX Directory Nagios plugins are a set of Perl-based executables that allow DirX Directory administrators to use the Nagios® Core™ Open Source monitoring application to monitor the status of important DirX Directory resources and operations and collect statistics about these resources and operations for long-term performance analysis.

DirX Directory provides the following plugins for monitoring the DirX Directory service with Nagios:

- The **check_dirx_backup_status** plugin, which evaluates the status of the most recent DirX Directory database backup operation.
- The **check_dirx_ctx** plugin, which monitors the CTX memory consumption of a DSA or an LDAP server.
- The **check_dirx_dbam_preload_status** plugin, which checks the status of the DirX Directory service database cache preloader.
- The **check_dirx_dbam_usage** plugin, which monitors the capacity of DBAM devices.
- The **check_dirx_dsa_get_opmode** plugin, which checks the current operation mode of the DirX Directory service.
- The **check_dirx_heartbeat** plugin, which checks the responsiveness of the DirX Directory service in a standalone or supplier-consumer replication configuration.
- The **check_dirx_ldap_current** and **check_dirx_ldap_totals** plugins, which check the current value of a specified MIB counter for an LDAP server.
- The **check_dirx_ldap_duration** plugin, which monitors the duration of LDAP client calls.
- The **check_dirx_ldap_resultsize** plugin, which monitors the result sizes of executed LDAP searches.
- The **check_dirx_no_of_fds** plugin, which monitors file descriptor usage for a DSA or LDAP server.
- The **check_dirx_server_files** plugin, which checks the number of files below the **server/ldif** and **server/supupdate** subdirectories to monitor LDIF and shadowing agreement administration.

The information provided in this chapter requires familiarity with the basic principles of Nagios monitoring and configuration. See the Nagios documentation for complete details.

1.1. General Information

This section provides information that applies to all of the DirX Directory Nagios plugins, followed by reference pages for each Nagios plugin and the plugin configuration file.

1.1.1. Prerequisites and Limitations

The DirX Directory Nagios plugins have the following pre-requisites and limitations:

- The Perl language/interpreter must be installed on each plugin host.

- On Windows, Perl distribution version 5.16.3 or newer.
- On Linux, Perl distribution version 5.8 or newer.
- The perl-ldap distribution must be installed on all plugin hosts that:
- Allow the plugins to make direct LDAP extended operation calls. See the section **Plugin Operation** for details.
- Run the **check_dirx_heartbeat** plugin.

See the **ReadMe.txt** file in the DirX Directory Nagios plugin installation folder (*install_path/monitoring/nagios*) for instructions on how to set up Perl and perl-ldap on the supported DirX Directory platforms.

- Because most of the plugins use new and specialized LDAP server extended operations available only in DirX Directory V8.3, they cannot be used with older DirX Directory versions.

1.1.2. Installation Location

DirX Directory provides the DirX Directory Nagios plugins in the location *install_path*/monitoring/nagios**. This folder contains the following files:

- The files that contain the plugin operation code (*.pl).
- The support module **check_dirx_common.pm**, which contains common routines used by many of the plugin *.pl files.
- The configuration module **check_dirx_config.pm.sample**, which contains local settings for plugin LDAP calls.

1.1.3. Plugin Operation

The DirX Directory Nagios plugins operate in a Nagios configuration as follows:

- The Nagios monitoring host runs on a host (typically a Linux machine). It periodically polls the status of the DirX Directory service by invoking the DirX Directory Nagios plugins via the Nagios Remote Plugin Executor (NRPE) to gather the required monitoring data for the objects they monitor.
- The DirX Directory Nagios plugins are installed on the remote monitored hosts, co-located with an NRPE daemon. Each DirX Directory Nagios plugin is tailored to the object it monitors. When called by the Nagios monitoring host, each plugin returns the following data to the Nagios monitoring host:
- The object's current status, for immediate display in the Nagios Web-based browser interface.
- Performance data about the object, to be stored in the Nagios system for later correlation and display in graph format via Nagios add-ons like **pnp4nagios**.
- The DirX Directory Nagios plugins interact with their monitored DirX Directory service objects via LDAP server extended operations. The plugins can be configured to use the

DirX Directory command **dirxextop** to perform these operations or to use direct LDAP calls to the extended operations. See the sections **Plugin Configuration** and **Common Plugin Syntax** for details.

1.1.4. Plugin Configuration

To use the DirX Directory Nagios plugins in an existing Nagios configuration, both the Nagios monitoring host and the remote DirX Directory Nagios plugin hosts must be configured to use NRPE and the plugins must be defined as Nagios services on the monitoring host and as NRPE commands on the remote plugin hosts. See the Nagios documentation, in particular, the NRPE documentation, for instructions.

The plugins have the following additional configuration requirements:

- Hosts that support the use of **dirxextop** for plugin LDAP extended operations must allow NRPE to execute this command. To enable **dirxextop** execution by NRPE:
- Add the account name of the user who installed Nagios user to the same group as the account name of the user who installed DirX Directory.
- Set an x-bit for **dirxextop** as necessary.
- The perl-ldap distribution must be installed on all hosts that shall support the use of direct LDAP extended operation calls by the plugins, as described in the section **Prerequisites and Limitations**. The perl-ldap distribution is also needed if the heartbeat plugin shall be used. See the **ReadMe.txt** file in the DirX Directory Nagios plugin installation folder (*install_path*/monitoring/nagios**) for instructions.
- The DirX Directory Nagios plugins include the **check_dirx_config.pm** configuration file, which contains the local settings for making LDAP calls. A template configuration file is supplied in *install_path*/monitoring/nagios/ check_dirx_config.pm.sample**. On each remote plugin host:
 - Copy this file and rename it to **check_dirx_config.pm**.
 - Edit the file with the local settings that apply. See the **check_dirx_config.pm** reference page for details.
- The user(s) specified in the configuration file for performing **dirxextop** operations or direct LDAP calls on the plugins' behalf must be configured in the LDAP Extended Operations Admins (ldapExtOpAdmin) attribute or in the LDAP Extended Operations Monitoring Users (ldapExtOpMonitoringUsers) attribute in the LDAP server configuration subentry. See the subsection **Attributes Controlling LDAP Extended Operations** in the section **Attributes for LDAP Server Configuration** in *DirX Directory Syntaxes and Attributes* for details.

1.1.4.1. Common Plugin Syntax

All plugins use the following calling convention:

[perl] check_dirx*_object.pl* -w warning_value -c critical_value [common_options]

Where:

perl

Specifies the perl command. This parameter is only required when invoking a plugin from a shell.

check_dirx_object

Specifies the plugin's executable name, starting with **check_dirx_** and followed by a string that describes the object to be monitored; for example, **backup_status**, **ctx**, **ldap_duration**, and so on.

-w *warning_value*

Specifies the value to be used as a warning threshold for determining the status of the monitored object. An object found to meet or exceed this threshold during a check operation is flagged with WARNING status (exit code **1**). The *warning_value* is interpreted as an absolute value or a relative percentage value, depending on the plugin. See the plugin reference descriptions for details.

-c *critical_value*

Specifies the value to be used as a critical threshold for determining the status of the monitored object. An object found to meet or exceed this threshold during a check operation is flagged with CRITICAL status (exit code **2**). The *critical_value* is interpreted as an absolute value or a percentage value, depending on the plugin. See the plugin reference descriptions for details.

common_options

Specifies one or more of the following options:

-h—Displays the usage description for the plugin.

-L—Executes direct LDAP calls for extended LDAP operation via perl (Net::LDAP). If this option is not specified, the **dirxextop** command is used. Using the **-L** option requires the perl-ldap distribution to be installed. Using **dirxextop** requires Nagios NRPE to be able to execute the command. See the section **Plugin Configuration** for details.

-v—Displays the DirX Directory Nagios plugin version, in the format:

plugin_name: plugin_version date

For example:

```
check_dirx_ctx.pl: V1.1 Build Feb-12, 2013
```

-x—Writes logging information to standard output. This option is for use in debug mode only for analyzing problems when running the plugin from a shell. Do not use this option when running the plugin from the Nagios monitoring host or the Nagios NRPE.

Most of the plugins require the **-w** and **-c** arguments and return an error if they are not specified.

Invoking a plugin without any arguments or options returns a usage description for the plugin.

1.1.5. Common Return Code Format

All DirX Directory Nagios plugins support the following return code format, as required by the Nagios product:

printable_string [| *performance_data*]

where:

printable_string

Is a simple message that is printable via standard output. The Nagios monitoring host displays the printable string returned by the plugin in current status displays. The DirX Directory Nagios plugins return *printable_string* in the format:

plugin_name *status* – *result_description*

where:

plugin_name

Is the name of the DirX Directory Nagios plugin returning the message.

status

Is the status code returned by the plugin and is one of the following Nagios-defined values:

OK—The status of the monitored object is within the boundaries defined by the specified warning and critical values). This status corresponds to the Nagios-defined exit code **0** (which the plugin must return on exit) and is displayed in green in Nagios current status displays.

WARNING—The *warning_value* specified to the plugin was exceeded. This status corresponds to the Nagios-defined exit code **1** (which the plugin must return on exit) and is displayed in yellow in Nagios current status displays.

CRITICAL—The *critical_value* specified to the plugin was exceeded. This status corresponds to the Nagios-defined exit code **2** (which the plugin must return on exit) and is displayed in red in Nagios current status displays.

UNKNOWN—The plugin encountered an execution error. This status corresponds to the Nagios-defined exit code **3** (which the plugin must return on exit) and is displayed in orange in Nagios current status displays. When this status is returned, it is recommended to run the plugin from the shell and use the **-x** (debug) option as necessary to determine the cause of the problem.

result_description

Is a short description of the result.

performance_data

Is current data relevant to the performance of the monitored object that is intended to be collected over time and used for long-term trend analysis. The Nagios system saves the returned performance data in a database reserved to the monitored object that can be displayed graphical format later on.

Performance data consists of one or more label/value pairs separated by spaces. Each label/value pair has the Nagios-defined format:

label=value[UOM];[warn];[crit];[min];[max]

where:

- *label* can contain any character. It must be enclosed in single quotes if it contains spaces, = or '. To specify a quotation character, use two single quotation marks ("). Label length is arbitrary, but ideally the first 19 characters are unique (due to a Nagios performance database limitation).
- *UOM* is the unit of measurement and is one of the following values:

unspecified - indicates a number (int or float) of items (for example, users, processes, load averages)

s - seconds | **us** - microseconds | **ms** - milliseconds

% - percentage

B - bytes | **KB** - kilobytes | **MB** - megabytes | **TB** - terabytes | **GB** - gigabytes

c - indicates a continuous counter (an increment-only counter)

- *warn* and *crit* are the current *warning_value* and *critical_value* respectively, are in the range format and must be the same unit of measurement.
- *value*, *min* and *max* are in the class [-0-9.] and must all be the same unit of measurement. *min* and *max* represent the minimum and maximum displayable value. *min* and *max* are not required if *UOM* is %.

warn/crit and *min/max* are optional; for example, if the threshold is not defined or *min* and *max* do not apply. Trailing semicolons present when these values are not specified can be omitted.

For example, the following label/value pair:

`NumProcesses=225;500;1000;0;100000`

directs Nagios to maintain a database for an integer value called **NumProcesses**. The database stores the current value of **225** and identifies it with the current time.

When Nagios later displays a graph for the **NumProcesses** item, a yellow warning line is displayed at a value of **500** and a red line is displayed at a level of **1000** to indicate the warning and critical levels in the graphical output. The values **0** and **100000** are hints for the Nagios database software that indicate in which range of numbers the values will appear to better organize the database.

The next section **DirX Directory Nagios Plugins Reference Descriptions** provides details about each DirX Directory Nagios plugin's calling syntax, operation and return codes. See the Nagios documentation for more information on required plugin exit/return code syntax.

1.2. DirX Directory Nagios Plugins Reference Descriptions

The following sections provide reference descriptions for each Nagios plugin.

1.2.1. check_dirx_backup_status

1.2.1.1. Synopsis

```
[perl] check_dirx_backup_status.pl -w warning_value -c critical_value [-L] [-h] [-v] [-x]
```

1.2.1.2. Purpose

Evaluates the status of the last **dirxbackup** save or delta save operation.

1.2.1.3. Arguments

-w *warning_value*

The number of seconds since the last **dirxbackup** save operation that defines the WARNING threshold for the time period between DirX Directory database backups. For example, **3600**.

-c *critical_value*

The number of seconds since the last **dirxbackup** save operation that defines the CRITICAL threshold for the time period between DirX Directory database backups. For example, **86400**.

1.2.1.4. Options

See the section **Common Plugin Syntax** for a description of the options used in this plugin.

1.2.1.5. Description

The **check_dirx_backup_status** plugin evaluates the time of the most recent **dirxbackup** operation and returns a status not equal to **OK** if either the warning threshold or the critical threshold is reached or an error occurs while the plugin is processing.

Use this DirX Directory Nagios plugin to monitor the frequency of DirX Directory database backup operations.

When called by Nagios (or from a shell), the **check_dirx_backup_status** plugin operates on output returned by a call to the **dsa_backup_status** extended operation. This operation returns the time, duration and completion status of the last **dirxbackup** save operation and the last delta save operation, if it is available. See **Example** for an example of the output.

The plugin calculates the difference between the current time and the timestamp of the most recent **dirxbackup** save operation returned in the output and then compares it to the warning and critical thresholds for backup frequency specified in the **-w** and **-c** arguments. It also checks the completion status returned in the output.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the date/time, duration and size of the most recent backup.

1.2.1.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The difference between the current time and the timestamp of the most recent dirxbackup save operation is less than <i>warning_value</i> and the dirxbackup save operation completed without error.
1	WARNING	The difference between the current time and the timestamp of the most recent dirxbackup save operation is greater than or equal to <i>warning_value</i> but less than <i>critical_value</i> and the dirxbackup save operation completed without error.
2	CRITICAL	The difference between the current time and the timestamp of the most recent dirxbackup save operation is greater than or equal to <i>critical_value</i> or the dirxbackup save operation completed with errors or has not been performed at all.
3	UNKNOWN	The plugin encountered an error (described in the return string if possible).

1.2.1.7. Example

Given the following plugin command:

```
check_dirx_backup_status.pl -w 3600 -c 86400
```

The plugin calls the **dsa_backup_status** extended operation. Suppose the operation returns the following data to the plugin:

```
Result of ExtOp :1.3.12.2.1107.1.3.2.13.38
Last full backup status : time 1387199374, duration 3 sec, size 33197
kb, no error
Last delta backup status : time 1387199435, duration 11 sec, size
36334 kb, no error
```

Given this output, the plugin determines that the delta backup operation is the most recent backup. It evaluates the status of this operation and the time at which it occurred. In this example, the plugin determines that the delta backup operation completed successfully, but the difference between the current time and the time at which the

backup operation occurred is more than the **3600** second limit specified in the **-w** argument. The plugin returns the following message:

DIRX-BACKUP-STATUS WARNING - Last delta backup at Mo 16 Dez 2013 14:10:35 W. Europe Standard Time, duration 11 sec, size 36334 kb

Note that the timestamp format shown in the output varies according to the operating system in use and other time-related local settings.

1.2.1.8. See Also

dirxbackup, **dirxextop** in the *DirX Directory Administration Reference*.

1.2.2. check_dirx_ctx

1.2.2.1. Synopsis

[perl] **check_dirx_ctx.pl** **-w** *warning_value* **-c** *critical_value* **-T** **DSA** | **LDAP** **[-L]** **[-h]** **[-v]** **[-x]**

1.2.2.2. Purpose

Checks the CTX memory consumption of a DSA or an LDAP server.

1.2.2.3. Arguments

-w *warning_value*

The percentage of the maximum CTX size that defines the WARNING threshold for CTX memory consumption. For example, a value of **50** indicates that when 50% of CTX memory is in use, a WARNING result should be returned.

-c *critical_value*

The percentage of the maximum CTX size that defines the CRITICAL threshold for CTX memory consumption. For example, a value of **90** indicates that when 90% of CTX memory is in use, a CRITICAL result should be returned.

-T **DSA** | **LDAP**

The target server to monitor. Specify **DSA** to monitor a DirX Directory DSA. Specify **LDAP** to monitor an LDAP server.

1.2.2.4. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-h**, **-v** and **-x** options. These options are common to all DirX Directory Nagios plugins.

1.2.2.5. Description

The **check_dirx_ctx** plugin evaluates the amount of CTX memory in use by a DSA or an LDAP server and returns a status not equal to **OK** if either the warning threshold or the critical threshold is reached or an error occurs while the plugin is processing. It also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to check the consumption of CTX memory by DSA and LDAP server processes in a DirX Directory service installation against the maximum available amount (in MB) defined in the DIRX_CTX_LIMIT environment variable.

When called by Nagios (or from the shell), the **check_dirx_ctx** plugin operates on data returned from a call to the **dsa_ctxinfo** extended operation (for **-T DSA**) or the **ldap_ctxinfo** extended operation (for **-T LDAP**). See **Example** for an example of the output.

The plugin extracts the following values from the returned data:

- The CTX maximum limit (EntireCtxLimitHard)
- The current CTX size (CurrTotal-CTX-Size)
- The high water mark of the CTX usage (HWM-Entire-CTX-Size).

Next, the plugin evaluates the percentage of memory consumption using the following calculation:

*Consumption in percent = 100 * CurrTotal-CTX-Size / EntireCTXLimitHard*

The plugin then checks whether the current consumption is above the percentages given in the **-w** and **-c** arguments. As long as the current consumption is below the percentage given in *warning_value*, the status is **OK**.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the current values of CTX and HWM.

The plugin also returns the following performance data for CTX and HWM:

- The current values
- The current warning and critical values
- The current minimum and maximum displayable values

Note that because this plugin monitors percentage values, administrators can increase or decrease the maximum available CTX memory allocation without affecting the plugin's configuration.

1.2.2.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The percentage of CTX memory in use is less than the percentage specified in <i>warning_value</i> .
1	WARNING	The percentage of CTX memory in use is greater than or equal to the percentage specified in <i>warning_value</i> but less than the percentage specified in <i>critical_value</i> .

Exit Code	Status	Reason
2	CRITICAL	The percentage of CTX memory in use is greater than or equal to the percentage specified in <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.2.7. Example

Given the following plugin command:

```
check_dirx_ctx.pl -w 50 -c 90 -T LDAP
```

The plugin calls the **ldap_ctxinfo** extended operation to evaluate the current CTX memory consumption of the LDAP server. Suppose that **ldap_ctxinfo** returns the following data to the plugin:

```
Result of ExtOp :1.3.12.2.1107.1.3.2.13.21
EntireCtxLimitHard : 1600 MB (exceeded 0 times),
EntireCtxLimitSoft : 1560 MB (exceeded 0 times)
CurrTotal-CTX-Size : 110 MB
HWM-Entire-CTX-Size: 120 MB
```

The plugin calculates the current memory consumption based on this data ($100 * 110 / 1600 = 6,875$) and compares it to the 50% and 90% values specified in the **-w** and **-c** arguments, respectively. Since current consumption (6.875 %) is below the 50% warning value, the plugin returns an exit code of 0 and the following message to Nagios:

DIRX-LDAP-CTX OK - Current CTX-size = 110 MB (HWM:120)

It also returns the following performance data string to Nagios for CTX and HWM:

LDAP-Ctx=110MB;800;1440;0;1600 LDAP-Ctx-HWM=120MB;800;1440;0;1600

where:

- **LDAP-Ctx=110MB** is the current CTX value
- **LDAP-Ctx-HTM=120MB** is the current HWM value
- **800** is the current warning value (50% of 1600) and **1440** is the current critical value (90% of 1600)
- **0** is the minimum displayable value for the item and **1600** is the maximum displayable value for the item

1.2.2.8. See Also

dirxextop, Environment Variables in the *DirX Directory Administration Reference*.

1.2.3. check_dirx_dbam_preload_status

1.2.3.1. Synopsis

```
[perl] check_dirx_dbam_preload_status.pl [-L] [-h] [-v] [-x]
```

1.2.3.2. Purpose

Checks the status of the DBAM buffer cache preloader.

1.2.3.3. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-h**, **-v** and **-x** options. These options are common to all DirX Directory Nagios plugins.

1.2.3.4. Description

The **check_dirx_dbam_preload_status** plugin evaluates the status of the preloader for the DBAM buffer cache and returns a status not equal to **OK** if the function is still running or disabled, or if an error occurs while the plugin is processing.

Use this DirX Directory Nagios plugin to monitor whether the DBAM buffer cache has been filled correctly. Performance issues can occur if the DBAM cache is not used as expected. If the status is CRITICAL, the plugin returns a message that explains why the preload function is disabled.

When called by Nagios (or from a shell), the **check_dirx_dbam_preload_status** plugin operates on output returned by a call to the **dsa_dbam_preload_status** extended operation. This operation returns status information about the DBAM buffer cache preload status. The plugin evaluates the status and returns an exit code and a message about the result in the format described in the section **Common Return Code Format**.

1.2.3.5. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The preloader has loaded the blocks partially or completely into the DBAM buffer cache and has completed without error.
1	WARNING	The preload operation is still in progress.
2	CRITICAL	The preload function is disabled.
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.3.6. Example

In this example, the plugin runs in a shell and returns successful status about the preloader to standard output:

```
check_dirx_dbam_preload_status.pl
```

The output is as follows:

```
DIRX-SERVER-DBAM-PRELOAD-STATUS OK - DBAM preloading enabled. Blocks loaded successfully in 5 seconds (complete database).
```

1.2.3.7. See Also

Environment Variables in the *DirX Directory Administration Reference*.

1.2.4. check_dirx_dbam_usage

1.2.4.1. Synopsis

```
[perl] check_dirx_dbam_usage.pl -w warning_value -c critical_value [-L] [-h] [-v] [-x]
```

1.2.4.2. Purpose

Checks the percentage of reserved space in use on DBAM devices in a DirX Directory service installation to monitor their capacity.

1.2.4.3. Arguments

-w *warning_value*

The percentage of reserved space in use that defines the WARNING threshold for problems with DBAM device capacity. For example, a value of **50** indicates that a warning should be returned if one of the DBAM devices has reached 50% of its maximum.

-c *critical_value*

The percentage of reserved space in use that defines the CRITICAL threshold for problems with DBAM device capacity. For example, a value of **90** indicates that a critical message should be returned if one of the DBAM devices has reached 90% of its maximum.

1.2.4.4. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-h**, **-v** and **-x** options. These options are common to all DirX Directory Nagios plugins.

1.2.4.5. Description

The **check_dirx_dbam_usage** plugin evaluates the current reserved space in use on all of the logical DBAM devices configured in a DirX Directory service installation and returns a

status not equal to **OK** if either the warning or critical threshold is reached or an error occurs while the plugin is processing. It also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor the capacity of the DBAM devices in a DirX Directory service installation and take steps to extend the DBAM database if warning or critical thresholds are reported. (See **Extending the Directory Database** in the *Disc Dimensioning Guide* for details.)

When called by Nagios (or from a shell), the plugin operates on output returned from a call to the **dsa_dbam_devinfo** extended operation. This output consists of the current percentage of reserved space (usage and fragmentation) in use on each logical device and each attribute index-specific device and the current percentage of reserved index entries and index clusters in use. It is identical to the output returned by the **dbamdevinfo** command. See **Example** for an example of the output (see also the **dbamdevinfo** command in the *DirX Directory Administration Reference*).

The plugin compares the percentages given for each logical device and for the index entries and index clusters to the values specified in the **-w** and **-c** arguments. The warning threshold or the critical threshold is reached if one of these percentages exceeds one of these values.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the current usage percentages for the evaluated logical devices, index entries and index clusters.

The plugin also returns the following performance data:

- The current percentage in use for each logical device and for index entries and index clusters
- The current warning and critical values in use
- The current minimum and maximum displayable values in use for subsequent graphical displays.

1.2.4.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The percentage of reserved space in use is less than <i>warning_value</i> .
1	WARNING	The percentage of reserved space in use is greater than or equal to <i>warning_value</i> but less than <i>critical_value</i> .
2	CRITICAL	The percentage of reserved space in use is greater than or equal to <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an execution error during its execution (described in the returned message if possible).

1.2.4.7. Example

Given the following plugin command:

```
check_dirx_dbam_usage.pl -w 50 -c 90
```

The plugin calls the **dsa_dbam_info** extended operation. Suppose it returns the following output to the plugin:

```
...
Logical device:  GENERAL | BITSTR | PSEUDO | TREE
    In use:          0.48 % (  4.879 MB of 1023.748 MB)
    Fragmentation:  0.01 %
Logical device:  REAL
    In use:          0.30 % (  3.039 MB of 1023.748 MB)
    Fragmentation:  0.00 %
Logical device:  AVIDX
    In use:          0.06 % (  4.063 MB of    7.000 GB)
    Fragmentation:  0.00 %
...
    Number of indices: 106      (maximum 300)
    Cluster usage:    2.57 % (23 of 895)
```

Because the command specifies a warning value of 50%, the plugin will return a warning status on the following percentages if at least one of the following conditions is met:

- 50% of 1023.748 MB for the logical devices GENERAL | BITSTR | PSEUDO | TREE
- 50% of 1023.748 MB for the logical device REAL
- 50% of 7.000 GB for logical device AVIDX
- 50% of 300 index entries
- 50% of 895 clusters

In this example, the output returned to the plugin indicates that all of the percentages are below the 50% warning value, so the plugin returns the following result description:

```
DBAM Fill/Fragmentation ok - CurrFill=0.48%, CurrFrag=0.01%,
CurrIDXinUSE=7%, CurrCLUSTERinUSE=2%
```

It also returns the following performance data:

```
AVIDX-Frag=0%;50;90;0;100; AVIDX-Fill=0%;50;90;0;100;
```

```
TREE-Frag=0%;50;90;0;100; TREE-Fill=0%;50;90;0;100;  
PSEUDO-Frag=0%;50;90;0;100; PSEUDO-Fill=0%;50;90;0;100;  
BITSTR-Frag=0%;50;90;0;100; BITSTR-Fill=0%;50;90;0;100;  
REAL-Frag=0%;50;90;0;100; REAL-Fill=0%;50;90;0;100;  
GENERAL-Frag=0%;50;90;0;100; GENERAL-Fill=0%;50;90;0;100;  
CurrIDXinUSE=7%;50;90;0;100; CurrCLUSTERinUSE=2%;50;90;0;100;
```

where:

- **0%** is the current fragmentation and reserved space in use for each logical device
- **7%** is the current percentage of index entries in use
- **2%** is the current percentage of index clusters in use
- **50** and **90** are the current values of the **-w** and **-c** arguments
- **0** and **100** are the current minimum and maximum displayable values

1.2.4.8. See Also

dbamdevinfo, **dirxextop** in the *DirX Directory Administration Reference*, *DirX Directory Disc Dimensioning Guide*.

1.2.5. check_dirx_dsa_get_opmode

1.2.5.1. Synopsis

```
[perl] check_dirx_dsa_get_opmode.pl [-L] [-h] [-v] [-x]
```

1.2.5.2. Purpose

Determines the current operating mode of a DirX Directory DSA.

1.2.5.3. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-h**, **-v** and **-x** options. These options are common to all DirX Directory Nagios plugins.

1.2.5.4. Description

The **check_dirx_dsa_get_opmode** plugin determines operating mode of a DirX DSA and returns a status not equal to **OK** if the DSA is not operating in READWRITE mode or an error occurs while the plugin is processing.

Use this DirX Directory Nagios plugin to monitor the operation mode of the DSA. (For details about the operation mode of the DSA, see the **dirxadm sys opmode** command in the *DirX Directory Administration Reference*.) If the operating mode is not READWRITE, the DSA rejects update operations. This situation prevents workflows from performing successfully.

When called by Nagios (or from a shell), the **check_dirx_dsa_get_opmode** plugin operates on output returned by a call to the **dsa_get_opmode** extended operation. This operation returns the current operating mode of the DSA.

The plugin evaluates the output and returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the current operating status of the DSA.

1.2.5.5. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The DSA is operating in READWRITE mode.
1	WARNING	The DSA is operating in POSTINDEXING, VERIFY or READONLY WAIT mode.
2	CRITICAL	The DSA is operating in READONLY mode.
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.5.6. Example

In this example, the plugin runs in a shell and returns successful status about the DSA operating mode to standard output:

```
check_dirx_dsa_get_opmode.pl
```

The output is as follows:

```
DIRX-SERVER-DSA-GET-OPMODE OK - READWRITE
```

1.2.5.7. See Also

dirxadm, **dirxextop**, **Environment Variables** in the *DirX Directory Administration Reference*.

1.2.6. check_dirx_heartbeat

1.2.6.1. Synopsis

```
[perl] check_dirx_heartbeat.pl -w warning_value -c critical_value [-s host] [-p port] [-D dn]  
-W pwd [-S host] [-P port] [-h] [-v] [-x]
```

1.2.6.2. Purpose

Verifies the responsiveness of the DirX Directory processes running in standalone and supplier (master) / consumer (shadow) DirX Directory service configurations.

1.2.6.3. Arguments

-w *warning_value*

The number of seconds that defines the WARNING threshold for the heartbeat operation's running time. For example, a value of **2** indicates that a WARNING result should be returned when the operation's execution time meets or exceeds 2 seconds without completion but is still under the *critical_value* timeframe.

-c *critical_value*

The number of seconds that defines the CRITICAL threshold for the heartbeat operation's running time. For example, a value of **4** indicates that a CRITICAL result should be returned when the operation's execution time meets or exceeds **4** seconds without completion.

1.2.6.4. Options

-s

The host name or IP address of the local DirX Directory service to be validated. If this option is not specified, the plugin uses the value specified in the plugin configuration file **check_dirx_config.pm***. The default is ***localhost**.

-p *port*

The port on which the local LDAP server listens for incoming requests. If this option is not specified, the plugin uses the value specified in the plugin configuration file **check_dirx_config.pm***. The default is ***389**.

-D *dn*

The distinguished name of the user that performs LDAP heartbeat checking operations on the plugin's behalf and that is also the target of these operations. If this option is not specified, the plugin uses the value specified in the plugin configuration file **check_dirx_config.pm***. The default is ***cn=admin,o=my-company**.

-W *pwd*

The password for the user account specified in the **-D** argument. If this option is not specified, the plugin uses the value specified in the plugin configuration file **check_dirx_config.pm***. The default is ***dirx**.

-S *host*

The host name or IP address of the remote DirX Directory service to be validated.

-P *port*

The port on which the remote LDAP server listens for incoming requests. The default is **389**.

See the section **Common Plugin Syntax** for a description of the **-L**, **-h**, **-v** and **-x** options. These options are common to all DirX Directory Nagios plugins.

1.2.6.5. Description

The **check_dirx_heartbeat** plugin determines the responsiveness of a local standalone or supplier DirX Directory service instance (DSA and LDAP server) and optionally of a remote consumer instance and returns a status not equal to **OK** if either the warning or critical threshold is reached or an error occurs while the plugin is processing.

Use this DirX Directory Nagios plugin to monitor the responsiveness of local update operations and also of data replication in supplier/consumer configurations.

When called by Nagios (or from a shell), the plugin performs an LDAP bind to the DirX Directory service specified in the **-s** option (or in the configuration file, if **-s** is not specified) as the user specified in the **-D** option (or in the configuration file, if this option is not used) and then writes a timestamp to this entry's **description** attribute. If the **-S** and **-P** options for a remote DirX Directory service instance are specified, the plugin subsequently performs an LDAP bind to the remote instance and then compares the timestamp of the (replicated) user entry's **description** attribute with the value on the master to verify that replication has occurred.

The plugin compares the elapsed time of the bind and update operation against the number of seconds specified as warning and critical values. The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**.

The specified user entry must have a **description** attribute. By means of the access control the user must have privileges for updating and reading its own description attribute. If replication is also to be checked, the specified user entry must reside in the replicated area on the supplier instance.

Specifying values for **-D**, **-W** and **-p** on the plugin command line overrides any values for these items specified in the configuration file **check_dirx_config.pm**.

Note that the **check_dirx_heartbeat** plugin requires the perl-ldap distribution to be installed on each DirX Directory service to be monitored. See the **ReadMe.txt** file in the Nagios plugin installation folder (*install_path*/monitoring/Nagios**) for instructions on how to set up Perl and perl-ldap on the supported DirX Directory platforms.

1.2.6.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The heartbeat operation has completed successfully within the timeframe specified by <i>warning_value</i> .
1	WARNING	The heartbeat operation's execution time is greater than or equal to <i>warning_value</i> but less than <i>critical_value</i> .
2	CRITICAL	The heartbeat operation's execution time is greater than or equal to <i>critical_value</i> .

Exit Code	Status	Reason
3	UNKNOWN	The plugin encountered an error during its execution (described in the returned message if possible).

1.2.6.7. Example

- In this example, the plugin runs in a shell and returns successful status about the local DirX Directory service responsiveness to **stdout**:

```
check_dirx_heartbeat.pl -w 2 -c 4
```

The output is as follows:

```
LDAP-Heartbeat: OK - completed in 0 sec (standalone)
```

- In this example, the plugin runs in a shell and returns successful status about the responsiveness of a supplier/consumer pair to **stdout**:

```
check_dirx_heartbeat.pl -w 2 -c 4 -S tmp1-w2k8-r3
```

The output is as follows:

```
LDAP-Heartbeat: OK - completed in 0 sec (with shadowing)
```

1.2.6.8. See Also

dirxadm in the *DirX Directory Administration Reference*

1.2.7. check_dirx_ldap_current

1.2.7.1. Synopsis

```
[perl] check_dirx_ldap_current.pl -w warning_value -c critical_value -k key_name [-d] [-L] [-h] [-v] [-x]
```

1.2.7.2. Purpose

Monitors the value of a selected absolute counter or delta counter in the LDAP MIB current table.

1.2.7.3. Arguments

-w *warning_value*

The value to be used as a warning threshold for determining the status of the monitored counter. A counter found to meet or exceed this threshold during a check operation is flagged with WARNING status (exit code **1**). The *warning_value* is interpreted as an absolute value or as a relative percentage value, depending on the counter specified in the **-k** argument.

-c critical_value

The value to be used as a critical threshold for determining the status of the monitored counter. A counter found to meet or exceed this threshold during a check operation is flagged with CRITICAL status (exit code **2**). The *critical_value* is interpreted as an absolute value or as a relative percentage value, depending on the counter specified in the **-k** argument.

-k key_name

The absolute or delta counter to be monitored, where *key_name* is one of the counters or delta counters selected from the following table:

Counter Key Name	Delta Counter Key Name	Description
CacheHitRatio	CachHitRatioDelta	Current percentage of search operations that were resolved by the LDAP result cache.
LdapConnections	LdapConnectionsDelta	Current number of LDAP connections.
LdapConnectionsHWM	LdapConnectionsHWMDelta	Current maximum number of LDAP connections.
DapConnections	DapConnectionsDelta	Current number of DAP connections.
DapConnectionsHWM	LdapConnectionsHWMD Delta	Current maximum number of DAP connections.
PoolThreadsRunning	PoolThreadsRunningDelta	Current number of pool threads handling an operation.
PoolThreadsIdle	PoolThreadsIdleDelta	Current number of idle pool threads.
OvflThreadsRunning	OvflThreadsRunningDelta	Current number of overflow threads rejecting operations if OpStackSize is exceeded.
OvflThreadsIdle	OvflThreadsIdleDelta	Current number of idle overflow threads.

Counter Key Name	Delta Counter Key Name	Description
OpStackSize	OpStackSizeDelta	Current number of operations waiting to be processed. New incoming operations are put onto the OpStack until the OpStackLimit is reached. If this limit is exceeded new operations are put onto the OvflStack from which they are processed by OvflThreads by rejecting the operations with a BUSY(51) return code.
OpStackSizeHWM	OpStackSizeHWMDelta	Current maximum number of operations waiting to be processed.
OvflStackSize	OvflStackSizeDelta	Current number of operations to be rejected.

Note that *key_name* is case sensitive.

Note: It is not recommended to monitor the delta counters without a deeper understanding as they would show the changes of changes.

1.2.7.4. Options

-d

The *key_name* specified in the **-k** argument is to be evaluated as a delta counter. When this option is not specified, the plugin evaluates *key_name* as an absolute counter. As the non-delta counters from this “current” table are floating counters (and not incrementing counters like in the “total” table) it is recommended to use **-d** for the non-delta counters (for example, OpStackSize or PoolThreadsRunning),

See the section **Common Plugin Syntax** for a description of the **-L**, **-v**, **-h** and **-x** options. These options are common to all Nagios plugins.

1.2.7.5. Description

The **check_dirx_ldap_current** plugin evaluates the value of a selected absolute or delta counter in the LDAP MIB current table and returns a status not equal to **OK** if either the warning or critical threshold is reached or an error occurs while the plugin is processing. It also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor one or more counters in the LDAP server’s MIB current table. You can only specify one counter on the plugin command line (with the **-k** argument). To monitor multiple LDAP server counters, set up separate invocations of the plugin for each counter to be monitored, and then specify each command line as a separate service to Nagios. See the Nagios documentation for details.

Use the **-k** *key_name* argument to select a counter. Select an absolute counter (see the **Counter Key Name** column in the table above for a list) to evaluate the absolute number of occurrences at the time of the call; for example, specify **LdapConnections** in *key_name* to evaluate the current number of open LDAP connections.

Select a delta counter (see the **Delta Counter Key Name** column in the table above for a list) to evaluate the difference in the number of occurrences since the last call to the plugin with the same *key_name* value; for example, specify **LdapConnectionsDelta** in *key_name* to evaluate the change of the number of open LDAP connections established since the last call to the plugin with **LdapConnectionsDelta** *key_name*. Note that many of the delta counters increment and decrement over time; as a result, it is possible that a delta counter can have a negative value.

For the LDAP MIB current table, absolute counters are usually more interesting to monitor than delta counters, because they can provide an indication of current server load; for example, the current number of LDAP binds or the current number of idle pool threads.

Use **-d** to both, for the non-delta as well as for the delta counters. This is necessary as even the non-deltas are non-linear-incrementing counters (their value can decrease or get negative). By supplying **-d** this counter-property is indicated for the Nagios database to be handled differently than continuous incrementing counters.

Use the **-w** and **-c** arguments to specify warning and critical thresholds. For most counters, criticality increases with increasing counter values; **LdapConnections** is an example. For these counters, call the plugin with a **-w** threshold that is less than the **-c** threshold. For some counters, criticality increases with decreasing counter values; **PoolThreadsIdle** is an example. For these counters, call the plugin with a **-w** threshold that is greater than the **-c** threshold.

Note that the plugin does not check whether the ranges specified in the **-w** and **-c** arguments make sense for the selected counter; that is, whether the values indicate absolute values or percentages. As a result, make sure you supply meaningful data to these arguments when building your plugin services.

When called by Nagios (or from a shell), the **check_dirx_ldap_current** plugin operates on output returned from a call to the **ldap_mib_current_tevd** extended operation. This operation returns all counters from the LDAP current MIB table, and the plugin evaluates the value of the specified key (**-k** argument). The plugin evaluates whether this value exceeds the warning or critical values specified in the **-w** and **-c** arguments and returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The message includes the current value of the selected counter.

The plugin also returns the following performance data to Nagios for storage:

- Selected counter's current value
- Current warning and critical values
- Current minimum and maximum displayable values

1.2.7.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	w < c: The counter value is greater than the value specified in <i>warning_value</i> . w > c: The counter value is smaller than the value specified in <i>warning_value</i> .
1	WARNING	w < c: The counter value is greater than or equal to the value specified in <i>warning_value</i> but less than the value specified in <i>critical_value</i> . w > c: The counter value is smaller than or equal to the value specified in <i>warning_value</i> but greater than the value specified in <i>critical_value</i> .
2	CRITICAL	w < c: The counter value is greater than or equal to the value specified in <i>critical_value</i> . w > c: The counter value is smaller than or equal to the value specified in <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.7.7. Examples

Given the following plugin command to evaluate the current number of open LDAP connections:

```
check_dirx_ldap_current.pl -w 100 -c 200 -k LdapConnections
```

If there are currently 120 open LDAP connections, the plugin returns the exit code 1 for WARNING and the following string containing a readable message followed by the performance data:

```
DIRX-LDAP-LdapConnections WARNING - Current LdapConnections=120  
|LDAP-LdapConnections=120;100;200;0;0
```

In this example, the performance data consists of the string:

LDAP-LdapConnections=120;100;200;0;0

Where the substrings have the following meanings:

- **LDAP-LdapConnections** is the unique name of the counter in the Nagios-RRD database

and used in the heading of the graphical charts that Nagios generates from the performance string.

- **120** is the number of currently open LDAP connections.
- **100** is the *warning_value* and **200** is the *critical_value* for the counter.
- **0;0** indicates null minimum and maximum displayable values and are ignored by Nagios.

1.2.7.8. See Also

check_dirx_ldap_total in *DirX Directory LDAP Extended Operations*, **dirxcp**, **dirxextop** in the *DirX Directory Administration Reference*.

1.2.8. check_dirx_ldap_duration

1.2.8.1. Synopsis

```
[perl] check_dirx_ldap_duration.pl -w warning_value -c critical_value -C range -T  
op_group _  
_[-L] [-h] [-v] [-x]
```

1.2.8.2. Purpose

Monitors the duration of LDAP client calls.

1.2.8.3. Arguments

-w *warning_value*

The percentage that defines the WARNING threshold for the number of long-duration operations. For example, a value of **5** indicates that if 5% the LDAP operations selected in the **-T** option run longer than the duration range selected in the **-C** option, a WARNING result should be returned.

-c *critical_value*

The percentage that defines the CRITICAL threshold for the number of long-duration operations. For example, a value of **10** indicates that if 10% of the LDAP operations selected in the **-T** option run longer than the duration range selected in the **-C** option, a CRITICAL result should be returned.

-C *range*

The duration range to be monitored. Supply one of the following values:

- 1 - LDAP operation durations in the range 0 to 10 ms
- 2 - LDAP operation durations in the range 10 to 100 ms
- 3 - LDAP operation durations in the range 100ms to 1 second.
- 4 - LDAP operation durations in the range 1 second to 10 seconds.
- 5 - LDAP operation durations in the range 10 seconds to 100 seconds.
- 6 - LDAP operation durations greater than 100 seconds.

-T *op_group*

The group of operations to be checked for duration. Supply one of the following keywords:

- **Dur_Bind** – Checks the durations of bind and unbind operations.
- **Dur_Retr** – Checks the durations of search and compare operations.
- **Dur_Upd** – Checks the durations of add, modify, modifyDN and delete operations.

1.2.8.4. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-v**, **-h** and **-x** options. These options are common to all Nagios plugins.

1.2.8.5. Description

The **check_dirx_ldap_duration** plugin evaluates the percentage of the selected LDAP operation group whose runtime falls into a selected timeframe and returns a status not equal to **OK** if either the warning or critical threshold is reached or an error occurs while the plugin is processing. The plugin also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor the frequency of long-duration LDAP operations for three groups of operations: bind and unbind operations, retrieval operations and update operations. In a well-configured and dimensioned DirX Directory service environment, these operations typically complete in a few milliseconds. However, it's also easy to initiate operations that can run for some time; for example, when initiating a search with a filter (**objectclass=**) **and all attributes requested**. **As long as long-duration operations occur infrequently and for well-known reasons (for example, during workflow scenarios), their occurrence is not a problem. However, if they occur more frequently, it can indicate that something is wrong or misconfigured; for example, that indexes are missing or the hardware is overloaded.** The ***check_dirx_ldap_duration** plugin allows you to use Nagios to monitor whether more long-duration operations occur than expected.

Use the **-T** argument to specify the group of operations to be monitored for duration: bind and unbind operations, search and compare operations, or add, update and delete operations. Note that you can only specify one group on the plugin command line per call. To monitor multiple LDAP operation groups, set up separate invocations of the plugin for each group to be monitored, and then specify each command line as a separate service to Nagios. See the Nagios documentation for details. Note that you cannot monitor the duration of a single LDAP operation with this plugin, only the specified groups of operations.

Use the **-C** argument to specify the duration range to be monitored for the operation group selected with the **-T** argument. To facilitate tracking and identification of long-duration operations, the LDAP server separates operation duration into 6 incremental ranges (or "classes") in milliseconds, from shortest runtime (0 to 10 milliseconds) to longest runtime (greater than 100 seconds). Each range increases the runtime interval by a factor of 10. The ranges are pre-defined and currently cannot be changed. The LDAP server maintains a counter for each range and increments the counter for the range that corresponds to the duration runtime of each LDAP operation. This data is kept in the LDAP server's LDAP MIB total table.

When called by Nagios (or from a shell), the plugin operates on the duration data retrieved from the LDAP MIB total table by a call to the **ldap_mib_total_tevd** extended operation. This operation returns the duration data for all operation groups and all ranges. The plugin reads the current "accumulated duration percentage" returned in the output for the group of LDAP operations selected with the **-T** option and for the duration range selected with the **-C** option. The accumulated percentage duration is the percentage of LDAP operations whose duration fell into this range or one of the ranges above it; that is it is the percentage of operations with a duration of at least the lower boundary of the range specified by **-C** option. The plugin checks whether the percentage returned in the output is at or above the percentages given in the **-w** and **-c** arguments.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the current value of the accumulated duration percentage.

It also returns the accumulated duration percentage as performance data to Nagios.

1.2.8.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The percentage of LDAP operations whose duration fell into the selected range and higher is less than the percentage specified in <i>warning_value</i> .
1	WARNING	The percentage of LDAP operations whose duration fell into the selected range and higher is greater than or equal to the value specified in <i>warning_value</i> but less than the value specified in <i>critical_value</i> .
2	CRITICAL	The percentage of LDAP operations whose duration fell into the selected range and higher is greater than or equal to the value specified in <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.8.7. Example

Given the following plugin command:

check_dirx_ldap_duration.pl -w 5 -c 10 -T Dur_Retr -C 4

This command instructs the plugin to monitor retrieval operations whether they exceed the duration range of 1 to 10 seconds and evaluates how many operations run longer than 1 second. The plugin calls the **ldap_mib_total_tevd** extended operation. Suppose the operation returns an accumulated duration percentage of 1% for range 4. This value indicates that 1% of the LDAP retrieval operations ran longer than 1 second. Since this runtime percentage is below the 5% warning value (less than 5% of retrieval operations ran longer than 1 second), the plugin returns an exit code of 0 for OK and the following string containing a readable message followed by the performance data:

DIRX-LDAP-Dur_Retr OK - Currently 1% of operations >1sec |Dur_Retr_Class4=1

1.2.8.8. See Also

check_dirx_ldap_resultsize in *DirX Directory LDAP Extended Operations*, **dirxcp**, **dirxextop** in the *DirX Directory Administration Reference*.

1.2.9. check_dirx_ldap_resultsize

1.2.9.1. Synopsis

```
[perl] check_dirx_ldap_resultsize.pl -w warning_value -c critical_value -C range -T  
data_type _  
_[-L] [-h] [-v] [-x]
```

1.2.9.2. Purpose

Monitors the size of search results returned by LDAP searches.

1.2.9.3. Arguments

-w *warning_value*

The *accumulated percentage* value that defines the WARNING threshold for the frequency of large search results for a given range.

-c *critical_value*

The *accumulated percentage* value that defines the CRITICAL threshold for the frequency of large search results.

-C *range*

The search size range to be monitored. Supply one of the following values:

- 1 – LDAP search sizes in the range 0 to 1 kB.
- 2 - LDAP search sizes in the range 1 kB to 10 kB.
- 3 - LDAP search sizes in the range 10 kB to 100 kB.
- 4 - LDAP search sizes in the range 100 kB to 1 MB.
- 5 - LDAP search sizes in the range 1 MB to 10 MB.
- 6 – LDAP search sizes greater than 10 MB.

-T *data_type*

The type of data to be monitored for size. Supply the keyword:

- **Size_Srch** – Checks the sizes of returned LDAP searches.

1.2.9.4. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-v**, **-h** and **-x** options. These options are common to all Nagios plugins.

1.2.9.5. Description

The **check_dirx_ldap_resultsize** plugin evaluates the percentage of LDAP search operations whose result sizes fall into a selected range and returns a status not equal to **OK** if either the warning or critical threshold is reached or an error occurs while the plugin is processing. The plugin also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor the frequency of large LDAP search results. Search result sizes that grow larger and larger over time can have implications for efficient DirX Directory service operation: large search results require a lot of memory, use CPU resources, produce a high level of disk and network I/O operations and occupy worker threads for long periods of time. Symptoms of these problems begin with reduced service responsiveness and end with service crashes when resources are exhausted. The **check_dirx_ldap_resultsize** plugin allows you to use Nagios to detect and respond to unexpected huge data transfers.

Use the **-T** argument to specify the type of data to be monitored for size. Note that the size of LDAP search results is currently the only type of data the plugin can monitor.

Use the **-C** argument to specify the size range to be monitored for the data type selected with the **-T** argument (currently LDAP search results). To facilitate tracking and identification of very large search results, the DirX Directory LDAP server separates the possible search sizes that can be returned by LDAP operations into six incremental ranges in bytes, from smallest (0 to 10 kilobytes) to largest (greater than 10 megabytes). Each range increases the size interval by a factor of 10. The ranges are pre-defined and currently cannot be changed. The LDAP server maintains a counter for each range and increments the counter for the range that corresponds to the size of the results returned by each LDAP operation. The search size data is kept in the LDAP server's LDAP MIB total table.

When called by Nagios (or from a shell), the **check_dirx_ldap_resultsize** plugin operates on LDAP server search size data returned from the LDAP MIB total table by a call to the **ldap_mib_total_tevd** extended operation. This operation returns the size data for all data types and all ranges. The plugin reads the current "accumulated search size percentage" returned in the output for the size range specified in the **-C** argument. The accumulated search size percentage is the sum of the percentages for this range and all of the ranges above it. It shows the percentage of search result sizes that fell into this range or higher. The plugin evaluates this value against the warning and critical percentages specified in the **-w** and **-c** arguments.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the current accumulated search size percentage for the selected range.

The plugin also returns the current accumulated percentage for the selected range as performance data to Nagios.

1.2.9.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The percentage of LDAP operations whose result sizes fell into the selected range and higher is less than the percentage specified in <i>warning_value</i> .
1	WARNING	The percentage of LDAP operations whose result sizes fell into the selected range and higher is greater than or equal to the value specified in <i>warning_value</i> but less than the value specified in <i>critical_value</i> .
2	CRITICAL	The percentage of LDAP operations whose result sizes fell into the selected range and higher is greater than or equal to the value specified in <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.9.7. Example

Given the following command line:

```
check_dirx_ldap_resultsize.pl -w 5 -c 10 -T Size_Srch -C 5
```

The plugin calls the **ldap_mib_total_tevd** extended operation. Suppose the operation returns an accumulated search size percentage of 2%. This value indicates that 2% of the LDAP searches returned sizes larger than 1MB. Since this percentage is below the 5% warning value (less than 5% of LDAP searches returned sizes larger than 1MB), the plugin returns an exit code of 0 for OK and the following string containing a readable message followed by the performance data:

```
DIRX-LDAP-Size_Srch OK - Currently 2% of operations >1MB
|Size_Srch_Class5=2
```

1.2.9.8. See Also

check_dirx_ldap_duration in *DirX Directory LDAP Extended Operations*, **dirxcp**, **dirxextop** in the *DirX Directory Administration Reference*.

1.2.10. check_dirx_ldap_totals

1.2.10.1. Synopsis

```
[perl] check_dirx_ldap_totals.pl -w warning_value -c critical_value -k key_name [-d] [-L] [-h] [-v] [-x]
```

1.2.10.2. Purpose

Monitors the value of a selected absolute counter or delta counter in the LDAP MIB total table.

1.2.10.3. Arguments

-w *warning_value*

The value to be used as a warning threshold for determining the status of the monitored counter. A counter found to meet or exceed this threshold during a check operation is flagged with WARNING status (exit code **1**). The *warning_value* is interpreted as an absolute value or a relative percentage value, depending on the counter specified in the **-k** argument.

-c *critical_value*

The value to be used as a critical threshold for determining the status of the monitored counter. A counter found to meet or exceed this threshold during a check operation is flagged with CRITICAL status (exit code **2**). The *critical_value* is interpreted as an absolute value or a relative percentage value, depending on the counter specified in the **-k** argument.

-k *key_name*

The absolute or delta counter to be monitored, where *key_name* is one of the counters or delta counter keys selected from the following table:

Counter Key Name	Delta Counter Key Name	Description
CurrentTime	CurrentTimeDelta	Current time.
TotalOps	TotalOpsDelta	Number of total operations performed.
CacheHitRatio	CacheHitRatioDelta	Percentage of successful searches in the LDAP result cache.
PduErrors	PduErrorsDelta	Number of LDAP decoding errors.
ClientShutdowns	ClientShutdownsDelta	Number of client shutdowns.
ReferralErrors	ReferralErrorsDelta	Number of unresolved referrals.
SslConnections	SslConnectionsDelta	Number of SSL connections.
SslErrors	SslErrorsDelta	Number of errors in SSL operations.
Binds	BindsDelta	Number of binds.
BindErrors	BindErrorsDelta	Number of errors in bind operations.
BindsV2	BindsV2Delta	Number of LDAPv2 binds.
BindsV3	BindsV3Delta	Number of LDAPv3 binds.
BindsAnonym	BindsAnonymDelta	Number of anonymous binds.
BindsSimple	BindsSimpleDelta	Number of simple authenticated binds.

Counter Key Name	Delta Counter Key Name	Description
BindsStrong	BindsStrongDelta	Number of strong authenticated (SASL EXTERNAL) binds.
Unbinds	UnbindsDelta	Number of unbinds.
Searches	SearchesDelta	Number of search operations.
SearchErrors	SearchErrorsDelta	Number of erroneous search operations.
SearchedEntries	SearchedEntriesDelta	Number of search result entries.
SearchedAttr	SearchedAttrDelta	Number of search result attributes.
SearchedReferrals	SearchedReferralsDelta	Number of referrals in search results.
SearchesOnelevel	SearchesOnelevelDelta	Number of one-level search operations.
SearchesBaselevel	SearchesBaselevelDelta	Number of base object search operations.
SearchesSubtree	SearchesSubtreeDelta	Number of subtree search operations.
Adds	AddsDelta	Number of add operations.
AddErrors	AddErrorsDelta	Number of erroneous add operations.
Modifys	ModifysDelta	Number of modify operations.
ModifyErrors	ModifyErrorsDelta	Number of erroneous modify operations.
ModifyDNs	ModifyDNsDelta	Number of modify DN operations.
ModifyDNErrors	ModifyDNErrorsDelta	Number of erroneous modify DN operations.
Deletes	DeletesDelta	Number of delete operations.
DeletesErrors	DeletesErrorsDelta	Number of erroneous delete operations.
Compares	ComparesDelta	Number of compare operations.
CompareErrors	CompareErrorsDelta	Number of erroneous compare operations.
Abandons	AbandonsDelta	Number of abandon operations.
ExtOps	ExtOpsDelta	Number of LDAP extended operations.
ExtOpErrors	ExtOpErrorsDelta	Number of erroneous LDAP extended operations.

Counter Key Name	Delta Counter Key Name	Description
RpcOps	RpcOpsDelta	Number of remote procedure calls (RPC).
DapDropouts	DapDropoutsDelta	Number of aborts from DSA server.
SchemaATadds	SchemaATaddsDelta	Number of attribute types added to the schema.
SchemaATdeletes	SchemaATdeletesDelta	Number of attribute types deleted from the schema.
SchemaOCadds	SchemaOCaddsDelta	Number of object classes added to the schema.
SchemaOCdeletes	SchemaOCdeletesDelta	Number of object classes deleted from the schema.
UntrustedBinds	UntrustedBindsDelta	Number of untrusted binds: binds rejected by the LDAP server due to a configuration setting; for example, LDAP deny IP list.
KBytesIn	KBytesInDelta	Amount of KB of total input data.
KBytesOut	KBytesOutDelta	Amount of KB of total output data.

Note that *key_name* is case-sensitive.

1.2.10.4. Options

-d

The *key_name* specified in the **-k** argument is to be evaluated as a delta counter. When this option is not specified, the plugin evaluates *key_name* as an absolute counter.

See the section **Common Plugin Syntax** for a description of the **-L**, **-v**, **-h** and **-x** options. These options are common to all Nagios plugins.

1.2.10.5. Description

The **check_dirx_ldap_totals** plugin evaluates the value of a selected absolute or delta counter in the LDAP MIB total table and returns a status not equal to **OK** if either the warning or critical threshold is reached or an error occurs while the plugin is processing. It also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor one or more counters in the LDAP server's MIB total table. You can only specify one counter on the plugin command line (with the **-k** argument). To monitor multiple LDAP server counters, set up separate invocations of the plugin for each counter to be monitored, and then specify each command line as a separate service to Nagios. See the Nagios documentation for details.

Use the **-k** *key_name* argument to select a counter. Select an absolute counter (see the **Counter Key Name** column in the table above for a list) to evaluate the number of

occurrences since LDAP server startup time; for example, specify **BindErrors** in *key_name* to evaluate the number of erroneous bind operations performed since LDAP server startup time.

Select a delta counter (see the **Delta Counter Key Name** column in the table above for a list) to evaluate the number of occurrences since the last call to the plugin with the same *key_name* value; for example, specify **BindErrorsDelta** in *key_name* to evaluate the number of erroneous bind operations performed since the last call to the plugin with **BindErrorsDelta** *key_name*.

For the LDAP MIB total table, delta counters are usually more interesting to monitor than absolute counters, because the absolute numbers for operations or errors always increase over an LDAP server process's lifetime. However, absolute values can provide an indication of server load.

Note that the **CacheHitRatio** counter increments and decrements over time, as a result, it is possible that its delta counter can have a negative value.

Use the **-d** option to indicate to Nagios (in the returned performance data string) that the counter specified in the **-k** option is a delta counter whose value should be interpreted as an incremental counter; for example, **SearchesDelta**.

When the **-d** option is not specified, for example with the **-k** option set to **Searches**, Nagios interprets the counter value as absolute and automatically calculates the deltas between collected counter values in subsequent graphical displays.

Use the **-w** and **-c** arguments to specify warning and critical thresholds. For most counters, criticality increases with increasing counter values; **BindErrors** is an example. For these counters, call the plugin with a **-w** threshold that is less than the **-c** threshold. For some counters, criticality increases with decreasing counter values; **CacheHitRatio** is an example. For these counters, call the plugin with a **-w** threshold that is greater than the **-c** threshold.

Note that the time period between delta values (change in value since the last plugin query) is equal to the frequency of Nagios calls to the plugin. When monitoring a delta counter, you need to know what this frequency is in order to establish meaningful warning and critical values for the counter. For example, suppose you want Nagios to monitor the number of searches and notify the administrator if too many occur within a certain time period. If Nagios calls the plugin every minute, you can determine warning and critical levels for the number of searches that occur within a minute; for example, 500 searches every minute for warning, and 1,000 searches every minute for critical, with the delta counter **SearchesDelta** as the counter to be monitored every minute.

Note that the plugin does not check whether the ranges specified in the **-w** and **-c** arguments make sense for the selected counter; that is, whether the values indicate absolute values or percentages. As a result, make sure you supply meaningful data to these arguments when building your plugin services.

When called by Nagios (or from a shell), the **check_dirx_ldap_totals** plugin operates on output returned from a call to the **ldap_mib_total_tevd** extended operation. This operation returns the value of the counter specified in the **-k** argument. The plugin evaluates whether this value exceeds the warning or critical values specified in the **-w** and **-c** arguments and

then returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the current value of the selected counter.

The plugin also returns the following performance data to Nagios for storage:

- Selected counter's current value
- Current warning and critical values
- Current minimum and maximum displayable values

1.2.10.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	w < c: The counter value is greater than the value specified in <i>warning_value</i> . w > c: The counter value is smaller than the value specified in <i>warning_value</i> .
1	WARNING	w < c: The counter value is greater than or equal to the value specified in <i>warning_value</i> but less than the value specified in <i>critical_value</i> . w > c: The counter value is smaller than or equal to the value specified in <i>warning_value</i> but greater than the value specified in <i>critical_value</i> .
2	CRITICAL	w < c: The counter value is greater than or equal to the value specified in <i>critical_value</i> . w > c: The counter value is smaller than or equal to the value specified in <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.10.7. Example

Given the following plugin command to examine the **SearchesDelta** counter:

```
check_dirx_ldap_totals.pl -w 100 -c 200 -d -k SearchesDelta
```

If there were 23 LDAP search operations since the last call, the plugin returns the exit code 0 for OK and the following string containing a readable message followed by the performance data:

```
DIRX-LDAP-SearchesDelta OK - Current SearchesDelta=23|LDAP  
SearchesDelta=23;100;200;0;0
```

In this example, the returned performance data consists of the string:

LDAP SearchesDelta=23;100;200;0;0

The meaning of the substrings is as follows:

- **LDAP SearchesDelta** is used in the heading of the graphical charts that Nagios generates from the performance string.
- **23** is the number of searches since the plugin was last called to evaluate this delta counter.
- **100** is the *warning_value* and **200** is the *critical_value* for the delta counter.
- **0;0** indicates null minimum and maximum displayable values and are ignored by Nagios.

1.2.10.8. See Also

check_dirx_ldap_current in *DirX Directory LDAP Extended Operations*, **dirxcp**, **dirxextop** in the *DirX Directory Administration Reference*.

1.2.11. check_dirx_no_of_fds

1.2.11.1. Synopsis

```
[perl] check_dirx_no_of_fds.pl -w warning_value -c critical_value -T DSA | LDAP [-L] [-h] [-v] [-x]
```

1.2.11.2. Purpose

Checks the file descriptor or handle consumption of a DSA or an LDAP server.

1.2.11.3. Arguments

-w *warning_value*

The number of file descriptors (Linux) or handles (Windows) in use that defines the WARNING threshold for file descriptor/handle consumption. For example, a value of **50** indicates that when 50 file descriptors/handles are in use, a WARNING result should be returned.

-c *critical_value*

The number of file descriptors (Linux) or handles (Windows) in use that defines the CRITICAL threshold for file descriptor/handle consumption. For example, a value of **90** indicates that when 90 file descriptors/handles are in use, a CRITICAL result should be returned.

-T **DSA | LDAP**

The target server to monitor. Specify **DSA** to monitor a DirX Directory DSA. Specify **LDAP** to monitor an LDAP server.

1.2.11.4. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-v**, **-h** and **-x** options. These options are common to all Nagios plugins.

1.2.11.5. Description

The **check_dirx_no_of_fds** plugin determines the number of file descriptors ("handles" on Windows) in use by the LDAP server or the DSA in a DirX Directory service installation and returns a status not equal to **OK** if either the warning threshold or the critical threshold is reached or an error occurs while the plugin is processing. It also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor file descriptor usage on a DirX Directory service host. File descriptors represent a critical resource for DirX Directory service installations. Typically, there are limits on the number of descriptors that a single process can establish. While Windows does not describe an explicit limit for handles (the limit on Windows is a specific amount of memory that the system provides for allocating descriptors), Linux systems like Linux only provide a limited number, displayable via the **ulimit -n** command. For a normal DirX Directory installation on Linux, the limit is **1024**.

Because sockets are descriptors, each LDAP connection can increase the number of file descriptors consumed by two in the LDAP server: one socket for the LDAP connection to the client and one more for the connection to the DSA. In the DSA, one request can also consume multiple sockets. Once the last descriptor is consumed, problems start to occur, from problems with external operations, such as LDAP clients no longer being able to connect to problems with internal operations, such as audit writing or shadowing journal writing. The **check_dirx_no_of_fds** plugin allows you to use Nagios to detect and respond to excessive file descriptor consumption before this resource is completely exhausted.

When called by Nagios (or from a shell), the **check_dirx_no_of_fds** plugin operates on output returned from a call to the extended operation **ldap_no_of_fds (-T LDAP)** or **dsa_no_of_fds (-T DSA)**.

On Windows, the plugin calls the Windows API function `GetProcessHandleCount()` to evaluate handle consumption.

On Linux, the plugin executes the command **/proc/*server_pid/fd***, where *server_pid* is the local DSA or LDAP server process identifier.

The plugin compares the current number of handles/file descriptors in use to the values specified in the **-w** and **-c** arguments.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**.

It also returns the current number of descriptors in use as performance data.

Note that the plugin will not be able to run on Linux if the LDAP server runs as a child of an s-Bit watchdog (**dirxdsas**). The reason for this limitation is that the information is retrieved from **/proc/*pid/fd***, which only receives root-read permissions. When the LDAP server is started by the

s-Bit dirxdsas watchdog, the **/proc/*pid** is created under ***root**. However, after the LDAP server Directory binds to the 389/636 ports, it switches its effective user ID to the user ID of the account of the DirX Directory installation. This user is subsequently prohibited from reading the **/proc** information when the extended operation for the number of file

descriptors is invoked later on by the Nagios plugin. The DSA does not have this problem because it is started as the user ID of the account of the DirX Directory installation and never changes its user ID.

1.2.11.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Result	Reason
0	OK	The number of handles/file descriptors in use is less than the number specified in <i>warning_value</i> .
1	WARNING	The number of handles/file descriptors in use is greater than or equal to the number specified in <i>warning_value</i> but less than the number specified in <i>critical_value</i> .
2	CRITICAL	The number of handles/file descriptors in use is greater than or equal to the number specified in <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an execution error (described in the return string if possible).

1.2.11.7. Example

In this example, given the plugin command-line:

check_dirx_no_of_fds -w 500 -c 2000 -T LDAP

The plugin returns the following return value string to Nagios:

DIRX-DSA-NO-FILE-DESCRIPTORS OK - 353 number of file descriptors in use

It returns the following performance data string to Nagios:

DIRX-DSA-NO-FILE-DESCRIPTORS=353;500;2000;0;10000

where:

- The current number of file descriptors in use is 353
- The current warning value is 500 file descriptors in use
- The current critical value is 2,000 file descriptors in use
- The minimum displayable number of file descriptors is 0
- The maximum displayable number of file descriptors is 10,000

1.2.11.8. See Also

dirxextop in the *DirX Directory Administration Reference*.

1.2.12. check_dirx_paging

1.2.12.1. Synopsis

[perl] **check_dirx_paging.pl** -w *warning_value* -c *critical_value* [-p] [-L] [-h] [-v] [-x]

1.2.12.2. Purpose

Checks the number of active paged search operations.

1.2.12.3. Arguments

-w *warning_value*

The number of active paged search operations that define the WARNING threshold. For example, **40**.

-c *critical_value*

The number of active search operations that defines the CRITICAL threshold. For example, **60**.

-p

Directs the plugin to treat the values specified for -w and -c as percentage values rather than absolute values.

1.2.12.4. Options

See the section **Common Plugin Syntax** for a description of the options used in this plugin.

1.2.12.5. Description

The **check_dirx_paging** plugin determines the number of currently active paged search operations in the DSA. A paged search operation consumes resources until:

- The search operation completes on the read and return of the last search result page.
- The LDAP connection is terminated with an explicit unbind operation.
- The socket connection is closed.

Releasing the resources that a paged search operation consumes also depends on the settings of the paging policy for maximum number of paged search operations, timeout and maximum amount of memory. (See **Paging Policy** in **DirX Directory DSA Operational Attributes** in the *DirX Directory Administration Reference* for details.)

This plugin counts the number of paged search operations at the time of the call and returns a status not equal to **OK** if either the warning threshold or the critical threshold is reached or an error occurs while the plugin is processing. It also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor the proper administration of the maximum number of paged search operations (component **MAXNUM**) of the paging policy.

When called by Nagios (or from a shell), the plugin operates on output returned from a call to the **dsa_paging_info** extended operation. This output returns information about paged search operations, especially the maximum number of paged search operations and the current number of paged search operations.

The plugin compares these values to the values specified in the **-w** and **-c** arguments. The warning threshold or the critical threshold is reached if the number of current search operations exceeds one of these values. If **-p** is specified, the plugin treats the thresholds as percentage values; for example, **-w 5** reports a warning if more than 5 incomplete paged search operations are detected and **-w 5 -p** issues a warning if more than 5% of the maximum number of paged search operations are detected.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**.

The plugin also returns the following performance data to Nagios for storage:

- The current count of paged search operations.
- The current warning and critical values in use.
- The current minimum and maximum displayable values in use for subsequent Nagios graphical displays.

1.2.12.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The number of active paged search operations is less than <i>warning_value</i> .
1	WARNING	The number of active paged search operations is greater than or equal to <i>warning_value</i> but less than <i>critical_value</i> .
2	CRITICAL	The number of active paged search operations is greater than or equal to <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an error (described in the return string if possible).

1.2.12.7. Example

Given the following plugin command:

```
perl check_dirx_paging.pl -w 40 -c 60
```

The plugin calls the **dsa_paging_info** extended operation. From the output of this extended operation, the plugin determines that 62 paged search operations are active, which is more than the specified critical value of 60. It returns the exit code 2 for CRITICAL and the following message:

DIRX-Paged-Searches CRITICAL - 62 of 64 in use

It returns the following performance data string to Nagios:

PagingCount=62;40;60;0;64

where:

- The current number of active paged search operations is 62
- The current warning value is 40 active paged search operations
- The current critical value is 60 active paged search operations
- The minimum displayable number of active paged search operations is 0
- The maximum displayable number of active paged search operations is 64

1.2.12.8. See Also

dirxextop in the *DirX Directory Administration Reference*.

1.2.13. check_dirx_server_files

1.2.13.1. Synopsis

`[perl] check_dirx_server_files.pl -w warning_value -c critical_value [-L] [-h] [-v] [-x]`

1.2.13.2. Purpose

Checks the number of files in the **server/ldif** and **server/supdate** subdirectories to monitor shadowing and LDIF agreement administration.

1.2.13.3. Arguments

-w *warning_value*

The number of files present in each subdirectory that defines the WARNING threshold for problems with LDIF and shadowing agreement administration. For example, **10000**.

-c *critical_value*

The number of files present in each subdirectory that defines the CRITICAL threshold for problems with LDIF and shadowing agreement administration. For example, **100000**.

1.2.13.4. Options

See the section **Common Plugin Syntax** for a description of the **-L**, **-v**, **-h** and **-x** options. These options are common to all Nagios plugins.

1.2.13.5. Description

The **check_dirx_server_files** plugin determines the number of files below the **server/ldif** and **server/supdate** subdirectories in a DirX Directory service installation and returns a status not equal to **OK** if either the warning threshold or the critical threshold is reached or an error occurs while the plugin is processing. It also generates performance data in addition to its status message.

Use this DirX Directory Nagios plugin to monitor the proper administration of shadowing agreements and LDIF agreements. If these agreements have not been administered correctly, a huge number of files can accumulate below the **server/ldif** and **server/supdate** subdirectories. Using this plugin allows for timely identification of shadowing and LDIF administration problems so that administrative steps can be taken to correct them before the file system runs out of free space.

When called by Nagios (or from a shell), the plugin operates on output returned from a call to the **dsa_server_files** extended operation. This output consists of a set of counters whose values indicate the current number of files contained in specific subdirectories below the **server** subdirectory. For each subdirectory in the list, the output provides the number of immediate subordinate files and subdirectories. See **Example** for an example of the output.

The plugin only evaluates the current number of files in the **server/ldif** and **server/supdate** subdirectories. For the **server/supdate** subdirectory, it evaluates the number of files recursively; that is, it counts the number of files in all of the subdirectories below **server/supdate**.

The plugin compares these values to the values specified in the **-w** and **-c** arguments. The warning threshold or the critical threshold is reached if the number of files in either **server/ldif** or **server/supdate** exceeds one of these values.

The plugin returns an exit code and a message about the result in the format described in the section **Common Return Code Format**. The result description includes the current values of the counters for the two evaluated subdirectories.

The plugin also returns the following performance data to Nagios for storage:

- The current values of the two subdirectory counters
- The current warning and critical values in use
- The current minimum and maximum displayable values in use for subsequent Nagios graphical displays.

1.2.13.6. Return Values

The following table shows the result values returned by the plugin and their meanings.

Exit Code	Status	Reason
0	OK	The number of files in the subdirectories is less than <i>warning_value</i> .

Exit Code	Status	Reason
1	WARNING	The number of files in the subdirectories is greater than or equal to <i>warning_value</i> but less than <i>critical_value</i> .
2	CRITICAL	The number of files in the subdirectories is greater than or equal to <i>critical_value</i> .
3	UNKNOWN	The plugin encountered an error during its execution (described in the return string if possible).

1.2.13.7. Example

Given the following plugin arguments:

check_dirx_server_files.pl -w 10000 -c 100000

The plugin calls the **dsa_server_files** extended operation. Suppose the **dsa_server_files** extended operation returns the following output to the plugin:

```
Result of ExtOp :1.3.12.2.1107.1.3.2.13.35
server/audit : 105
server/ldif : 16687
server/log : 521
server/supdate : 6
server/supdate/0910 : 5
server/supdate/1111 : 0
server/supdate/JOURNAL : 8
```

From this output, the plugin determines that the **server/ldif** directory contains 16,687 files, which is more than the specified warning value of 10,000. It returns the exit code 1 for WARNING and the following message:

```
DIRX-SERVER-FILES WARNING - server/ldif=16687, server/supdate=6
```

It also returns the following performance data:

```
server/ldif=16687;10000;100000;0;1000000
server/supdate=6;10000;100000;0;1000000
```

where:

- **16687** is the current number of files below the **server/ldif** directory.
- **6** is the current number of files below the **server/supdate** directory
- **10000** and **100000** are the current values of the **-w** and **-c** arguments

- **0** and **1000000** are the current minimum and maximum displayable values

1.2.13.8. See Also

dirxextop in the *DirX Directory Administration Reference*.

1.3. DirX Directory Nagios Plugin Configuration File

1.3.1. check_dirx_config.pm

1.3.1.1. Purpose

The DirX Directory Nagios plugin configuration file, used by all of the plugins ***.pl**, defines the operating parameters for the DirX Directory Nagios plugins. The settings in the file apply to all plugin instances running on a local host.

1.3.1.2. Description

The default location and file name for the DirX Directory Nagios plugin file **check_dirx_config.pm** is:

install_path/monitoring/nagios/check_dirx_config.pm.sample

Copy this file to each machine that hosts the DirX Directory Nagios plugins, rename it to **check_dirx_config.pm**, and update the variables to the settings on the local machine.

In the configuration file, comment lines begin with the hash tag character (**#**) in the first column and are ignored. The format of all other lines is:

\$variable="value"

The following variables must be specified:

\$DIRXINSTPATH

The path to the DirX Directory service installation on the local machine (*install_path*). See the chapter **File Locations** in the *DirX Directory Administration Reference* for details about the default directories, subdirectories and files for a DirX Directory service installation.

\$DIRXLIBPATH

The path to the DirX Directory libraries. The default is *install_path /lib*. See the chapter **File Locations** in the *DirX Directory Administration Reference* for details.

\$DIRXEXTOP

The path to the **dirxextop** executable. The default is *install_path*/bin**.

\$DIRXLDAPHOST

The name of the local DirX Directory LDAP server. The default is **localhost**.

\$DIRXLDAPPORT

The TCP port number on which the local DirX Directory LDAP server listens for incoming requests from LDAP clients. The default LDAP port number is **389**.

\$DIRXLDAPUSER

The user that performs **dirxextop** operations or direct LDAP calls on the plugins' behalf. This user must be configured in the attributes `ldapExtOpAdmin` or `ldapExtOpMonitoringUser` in the LDAP server configuration subentry, or the LDAP servers will reject the extended operations made by **dirxextop** or by direct LDAP calls from the plugin. See the subsection **Attributes Controlling LDAP Extended Operations** of section **Attributes for LDAP Server Configuration** in *DirX Directory Syntaxes and Attributes* for details.

If this user is also to be used as the target of **check_dirx_heartbeat** plugin, it must also be an ordinary LDAP entry, have a **description** attribute and exist in the replicated part of the DIT; otherwise, the update to this entry made by the plugin won't be replicated and the plugin will report a problem. Note that specifying **-D** and **-W** arguments to the **check_dirx_heartbeat** plugin override the user and password specified in **\$DIRXLDAPUSER** and **\$DIRXLDAPUSERPWD**. See the **check_dirx_heartbeat** reference page for details.

Specify **\$DIRXLDAPUSER** in LDAP distinguished name syntax; for example, **"cn=admin,o=my-company"**. For details about LDAP distinguished name syntax, see the section **Distinguished Names** in the chapter **DirX Directory String Representation for LDAP Binds** in *DirX Directory Syntaxes and Attributes*.

To enable anonymous binding, specify **""**. An empty value directs the plugins to call **dirxextop** or make direct LDAP calls as an anonymous user. You can use an anonymous bind if there is no limitation concerning access to the LDAP extended operations; that is, the LDAP Extended Operations Admins attribute has the value **all** and there are no values specified for the other LDAP Extended Operations * Users attributes. See the subsection **Attributes Controlling LDAP Extended Operations** in the section **Attributes for LDAP Server Configuration** in *DirX Directory Syntaxes and Attributes* for details.

\$DIRXLDAPUSERPWD

The password associated with the account specified in **\$DIRXLDAPUSER**. This is the password the plugins will use during **dirxextop** and direct LDAP bind operations. Specify **pw** in Directory-String syntax; for example, **"dirx"**. See the section **Attribute Syntax** in the chapter **DirX Directory String Representation for DAP Binds** in *DirX Directory Syntaxes and Attributes* for details.

1.3.1.3. Example

```
# Configuration setting for the DirX Nagios plugins
#
# Note, the settings below may need to be customized accordingly
#
# Apr 19, 2013:  the ldap functions return two values each
#               anonymous bind triggered by empty (userDN|userPWD)
# #####
#
# if perl scripts use functionality like "use strict"
```

```
# they have to reference the variables below in this script
# by e.g. $::DIRXLDAPHOST
#

# path to DirX installation
$DIRXINSTPATH="/data/dirx";
$DIRXLIBPATH="$DIRXINSTPATH/lib";
$DIRXEXTOP="$DIRXINSTPATH/bin/dirxextop";

# DirX LDAP Server address
$DIRXLDAPHOST="localhost";
$DIRXLDAPPORT=389;

# For administrative bind
$DIRXLDAPUSERPWD="dirx";
$DIRXLDAPUSER="cn=admin,o=my-company";

# For anonymous bind
#$DIRXLDAPUSER=" ";
#$DIRXLDAPUSERPWD=" ";
```

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



Eviden is a registered trademark © Copyright 2025, Eviden SAS – All rights reserved.

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.

Index

C

- `check_dirx_backup_status`, [10](#)
- `check_dirx_ctx`, [12](#)
- `check_dirx_dbam_preload_status`, [15](#)
- `check_dirx_dbam_usage`, [16](#)
- `check_dirx_dsa_get_opmode`, [19](#)
- `check_dirx_heartbeat`, [20](#)
- `check_dirx_ldap_current`, [23](#)
- `check_dirx_ldap_duration`, [28](#)
- `check_dirx_ldap_resultsize`, [31](#)
- `check_dirx_ldap_totals`, [33](#)
- `check_dirx_no_of_fds`, [39](#)
- `check_dirx_paging`, [42](#)
- `check_dirx_server_files`, [44](#)

D

- DirX Directory Nagios Plugin Configuration
 - File, [47](#)
- DirX Directory Nagios Plugins, [10](#)