



CN=Monitor Guide

1	Introduction	4
1.1	Quick Guide	4
1.2	What you use CN=Monitor for	4
1.3	Limitations.....	5
1.3.1	Available functionality.....	5
1.3.2	Monitor Performance Counters.....	5
2	Web page features.....	6
2.1	Menu Options.....	6
2.2	Access permissions.....	6
2.2.1	Authentication Dialog	8
2.2.2	Preferences Dialog	9
2.3	Start Page	10
2.3.1	Environments	10
2.3.2	Adding a temporary available server.....	11
2.3.3	Messages.....	11
2.4	Environment View	12
2.4.1	Server Availability tab	12
2.4.2	Statistics tab	13
2.4.3	About tab	14
2.5	Server View	15
2.5.1	Server Availability Tab	15
2.5.2	Statistics Tab.....	17
2.5.3	About Tab	17
2.6	Monitoring.....	18
2.6.1	Live Monitoring	18
2.6.2	History Monitoring.....	19
2.7	Replication.....	21
2.7.1	View replication status.....	21
2.7.2	Replication Details tab.....	22
2.7.3	Replication notes iPlanet based	22
2.7.4	Replication notes OpenLDAP.....	23
2.7.5	Replication notes OpenDS based	24
2.8	Load Balancer	24
2.8.1	Options for load balancer test.....	25
2.9	Query	26
2.9.1	Query Result.....	27
2.9.2	View Single Entry.....	27
2.10	Cache Sizes	28
2.11	Indexes	28
2.12	Certificate	29
2.13	Schema	30
2.14	Query Server(s)	30
3	Mobile features.....	31
3.1	Start Page	31
3.2	Environment View	31
4	Collect / Summary scripts.....	31
4.1	collectdb.php	32
4.2	collectservermessage.php.....	32
4.3	encryptpassword.php.....	33
4.4	collectsummary.php.....	34

5	LDAP Performance	34
6	Contact Information.....	35
6.1	Download Updates.....	35
6.2	Donate using PayPal.....	35
6.3	Contact Developer(s)	36

1 Introduction

This document is an introduction and guideline to the monitoring application CN=Monitor.

Read *CN=Monitor <version>.pdf* for instructions on how to install and configure CN=Monitor.

Available to download from: <http://cnmonitor.sourceforge.net/>

Send a mail to monitorldap@gmail.com if you have any questions, feature requests, positive or negative feedback or want to report a bug.

1.1 Quick Guide

Checklist to get started after you have installed CN=Monitor.

- 1) Make sure that CN=Monitor can read base dn:s:
cn=monitor and cn=config.
Either anonymously or with a high privileged user.
Verify connectivity by running the following LDAP queries:

```
$ ldapsearch -x -s base -H "ldap://<hostname>" -b cn=monitor  
$ ldapsearch -x -s base -H "ldap://<hostname>" -b cn=config
```

See chapter **Access Permissions** for more information.

- 2) Configure CN=Monitor
Environments, Servers and database connectivity.
- 3) Scheduling scripts (optional)
See chapter **Collect / monitoring scripts**.

1.2 What you use CN=Monitor for

- **Verify server availability**
Verify that all servers within your environment are answering on LDAP.
Get notified by mail if you have any server disturbances.
- **Monitor server and service load**
Live and historical monitoring of performance counters.
- **Monitor load and performance trends**
Compare server or service load between months and years.
- **Verify server configuration**
Certificates, indexes, schema and cache configurations.
- **Advanced LDAP Query**
Query several servers at the same time, compare entries between servers.
- **Verify Load balancer or cluster address**
Verify which servers that are responding behind your load balancer or cluster address and measure the response time.

1.3 Limitations

1.3.1 Available functionality

Server	Availability	Monitoring	Replication	Query	Configuration
389 / RH DS	X	X	X	X	X
OpenLDAP	X	X	X	X	X
Sun / ODSEE	X	X	X	X	X
IBM Tivoli	X	X		X	X*
Novell eDirectory	X	X		X	X*
OpenDS / OpenDJ / OUD	X	X	X	X	X
Other...	X			X	X*

X Only certificates and schemas can be verified.*

1.3.2 Monitor Performance Counters

Overview of what CN=Monitor can monitor depending on Directory Server.

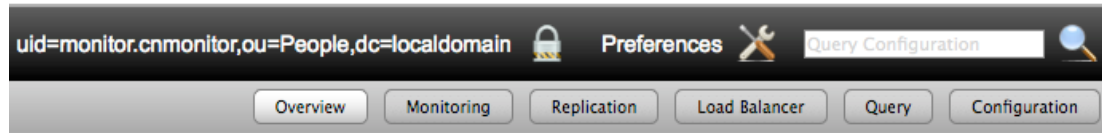
Information	RedHat/389	Open LDAP	Sun/ODSEE	Novell	IBM	OpenDS
Connection Peak			X		X	X
Threads	X (current)	X (max)	X		X	
Current Connections	X	X	X		X	X
Total Connections	X	X	X		X	X
Entries Sent	X	X	X		X	X
Bytes Sent	X	X	X	X		X
Start Time	X	X	X		X	X
Current Time	X	X	X		X	X
Anonymous Binds	X	(Included in Simple Binds)	X	(Included in UnAuthenticated Binds)	(Actual all completed binds)	(Included in Simple Binds)
UnAuthenticated Binds	X	(Included in Simple Binds)	X	X		(Included in Simple Binds)
Simple Binds	X	X	X	x		X
Strong Binds	X	(Included in Simple Binds)	X	X		(Included in Simple Binds)
Bind Security Errors	X		X	X		
Whole Search tree op.	X	X	X	X	(Included as Search Op.)	(Included as Search Op.)
Search op.	X	X	X	X	X	X
Compare op.	X	X	X	X	X	X
Add op.	X	X	X	X	X	X
Modify op.	X	X	X	X	X	X
ModifyRDN op.	X	X	X	X	X	X
Remove op.	X	X	X	X	X	X
In op.	X	X	X	X	X	X
Errors	X		X	X	(As slapderrorlog messages)	
Security Errors	X		X	X		

If the server can't return operational status using the LDAP protocol functionality gets limited. Still you can use CN=Monitor for LDAP verification, response time and unavailability notifications.

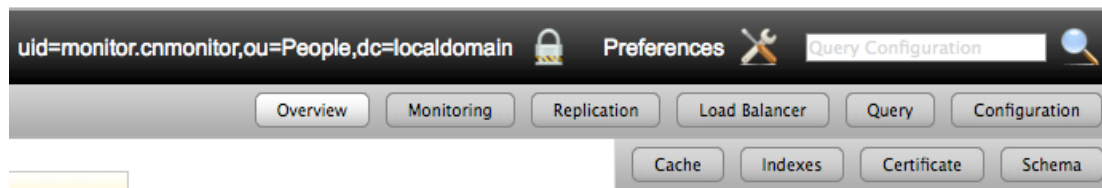
To retrieve some attributes you either need to authenticate using high privileges or enable read access for user or anonymous access to cn=monitor and cn=config databases. Read the **Access permissions chapter** in this document and consult your directory documentation.

2 Web page features

2.1 Menu Options



The following buttons / features are available by default.



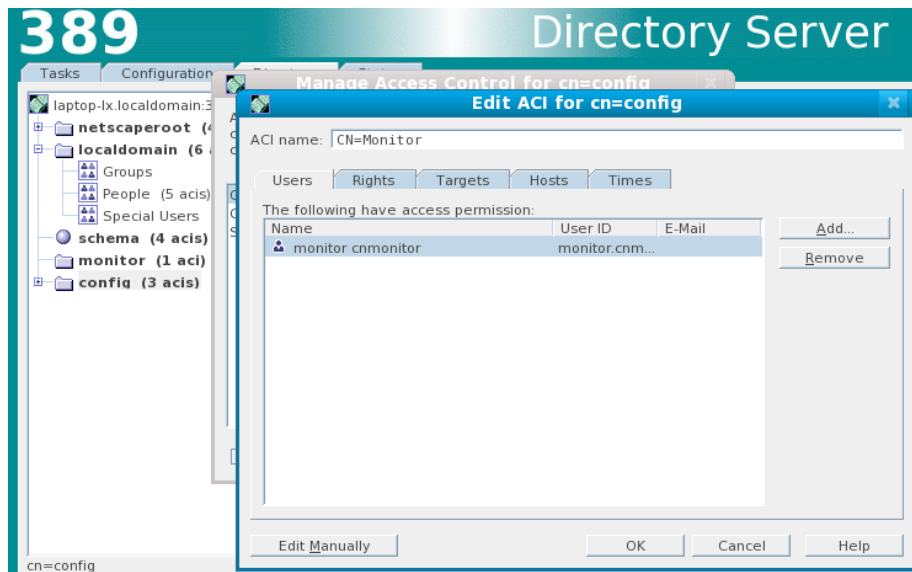
By clicking on the **Configuration** button new options appear to view your directory server configuration.

Note that the number of buttons may differ depending on directory server vendor and version.

2.2 Access permissions

To avoid using your administrator account, i.e. *cn=Directory Manager*, you need to configure access permissions to backend suffixes:

- **389 DS, RHDS, SunOne DS (iPlanet based)**
cn=monitor (by default opened for anonymous reading)
cn=config (by default **not opened for anonymous reading**)
As cn=config holds replication, index and cache information you should setup read access to this backend by using an ACI.
Example of setting up an ACI using the directory console:



ACI

```
(targetattr = "*")
(target = "ldap:///cn=config")
(version 3.0;
acl "CN=Monitor";
allow (read,compare,search)
(userdn = "ldap:///uid=monitor.cnmonitor,ou=People,dc=localdomain")
;)
```

In this example the user monitor.cnmonitor has access to the cn=config database. Limit the access rights to read, compare and search.

- **OpenLDAP**

You need to allow read access to the cn=monitor and cn=config suffix.

```
# enable monit database
database monitor

# allow only monitoring user to access monitor and config database
access to *
    by dn.exact="cn=CNMonitor User,ou=Monitor,dc=domain,dc=com" read
    by * none

# enable config database
database config

access to *
    by dn.exact="cn=CNMonitor User,ou=Monitor,dc=domain,dc=com" read
    by * none
```

- **Other vendors**

- For IBM Tivoli Directory Server you need to allow read access to the cn=monitor suffix.
- For Novell you need to allow read access to Root DN
- For OpenDS you need to allow read access to cn=config (index, cache configuration)

To verify vendor, which is a prerequisite to know where the monitor information can be collected from, you need to allow read access to Root DSE (by default open for read access).

Finally add DN and password for your created monitoring user in config.xml:

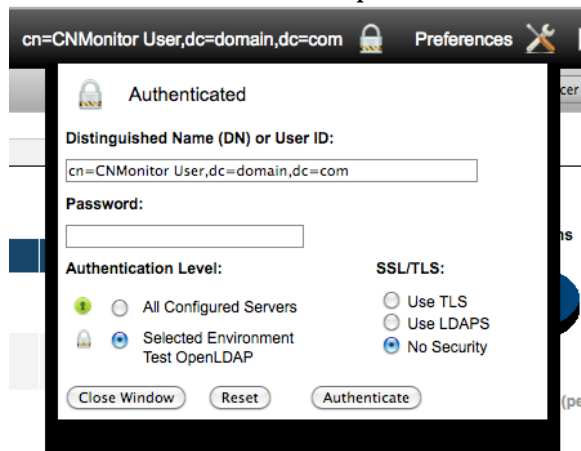
```
<server>
  <name>myserver.mydomain.com</name>
  <dn>uid=monitor.cnmonitor,ou=People,dc=localdomain</dn>
  <password>secret</password>
  <scheme>ldaps</scheme>
</server>
```

The password can also be encrypted using the encryptpassword.php script and using the <encpassword> configuration option in config.xml.

2.2.1 Authentication Dialog

To override your configured default access permissions you can use the Authentication Dialog.

Click on *Authenticate* to open the authenticate dialog.



Authenticate

1. Enter DN or User ID.
 User ID is by default required to match the filter. (|(uid=<userid>)(cn=<userid>)).
 You can set your own filter by adding the dnbyfilter configuration option. I.e. a filter such as (&(c=SE)(|(uid=?)(employeeNumber=?))) will allow users located in Sweden authenticating with either uid or employeeNumber.
2. Enter Password.
3. Choose Authenticate Level
 You can choose to use your entered credentials on different levels. All configured servers, servers within your environment or the selected server.
 Entered credentials are inherited. You can set new credentials on a lower level to override inherited credentials. That way you can have one set of credentials on environment level and a different set on server level.
 Static credentials added to the configuration file will be overridden.
4. Choose Encryption
 To avoid authentication being sent in clear text you can select to use either SSL or TLS.
 Usually SSL means LDAPS over port 636 and TLS over port 389.
5. Click **Authenticate**



On successful authentication the dialog will close and the page will be reloaded using entered credentials.

The authenticated DN will be displayed on the top of the page along with the *authenticated* symbol (a blue shield).

Reset Authentication

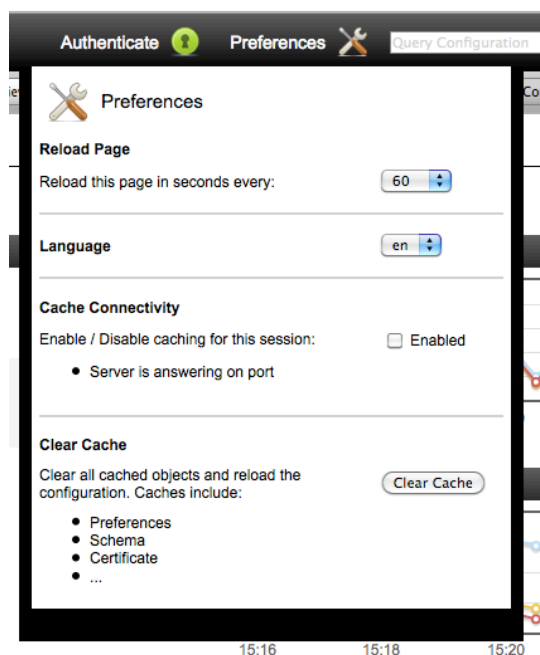
Remove a set of credentials on selected level.

1. Select the Authenticate Level to remove credentials
You must select the top level with actual entered credentials. Inherited credentials can not be removed.
Static credentials added to the configuration file cannot be removed.
2. Click Reset



On successful reset of credentials the dialog will close and the page will be reloaded using not configured or inherited or static credentials entered in the configuration file. The unlocked symbol will be displayed at the top of the screen.

2.2.2 Preferences Dialog

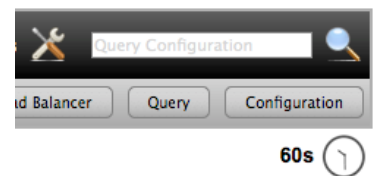


Here you can set options for your session or clear caches.

Reload Page

Reload the page every x second. This functionality will only be enabled for *start*, *environment* and *server* page. Note that the reload will stop when browsing to a different page.

You can access the reload page functionality either by clicking on the clock on any of these pages or by accessing the Preferences menu. Default setting for reload functionality is 60 seconds.



Language

Choose which language you want to use for this session. This will override the default and configured settings for option *language*.

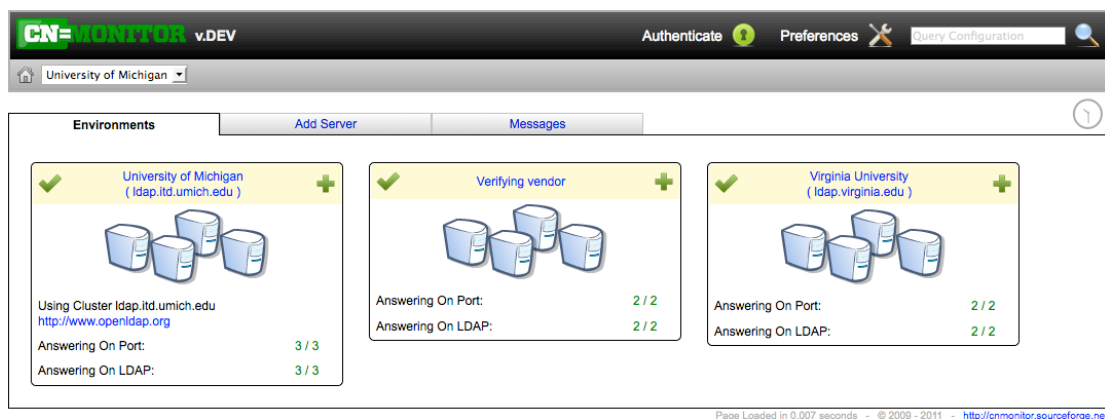
Cache Connectivity

Using this option is not recommended as it will cache LDAP connectivity but can increase performance when connecting to servers with slow response time. This will override the default and configured settings for option *cache_connection*.

Clear Cache

This will remove all cache files available for your session in the *temp* directory. You must clear the cache to reload the configuration.

2.3 Start Page



2.3.1 Environments

From here you can view configured environments and add new servers only available in your running session.

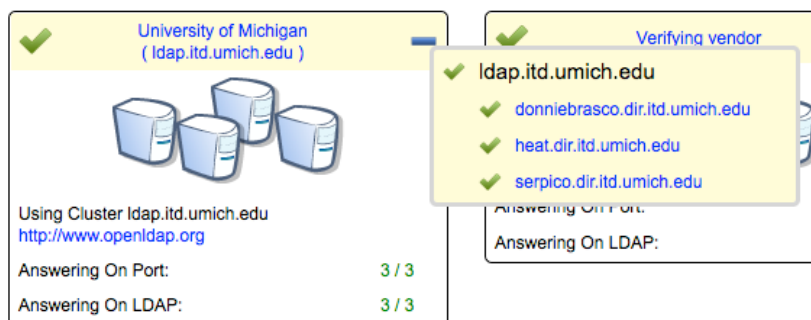
Server and Load balancer status for each configured environment will be shown.

✔ Indicates that all servers in your environment are responding to LDAP.

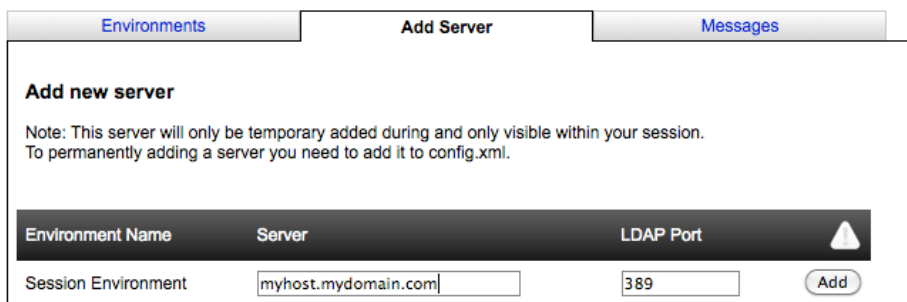
⚠ Indicates miscellaneous issues such as replication verification failure.

⚠ Indicates LDAP port or connectivity error.

You can get more information and links to specific servers by clicking the + button.



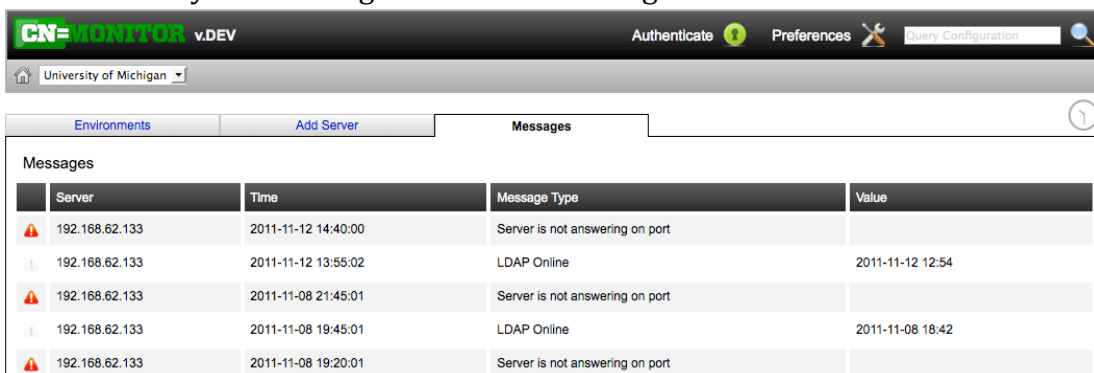
2.3.2 Adding a temporary available server



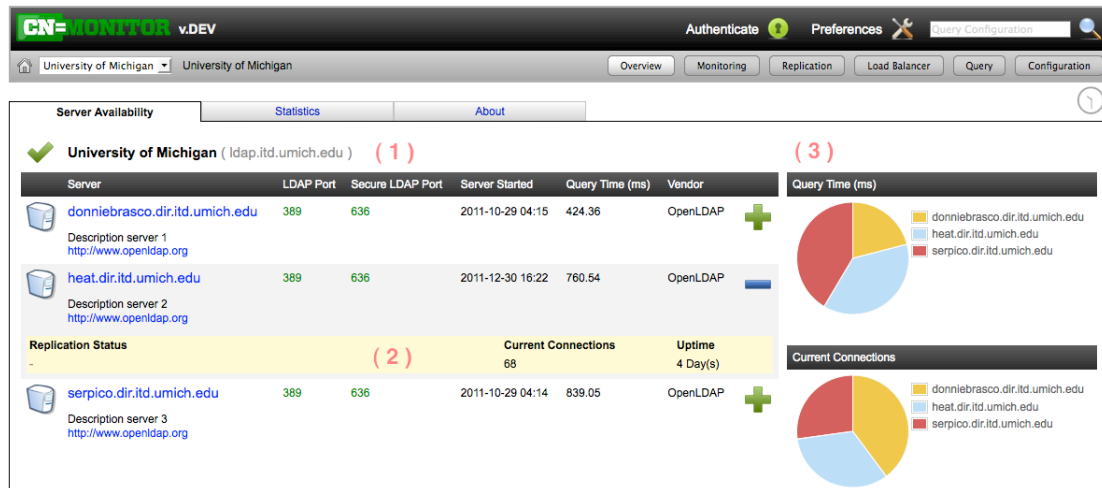
By using the *Add Server* tab you can add a temporary server to your session. This means that the server is only available within your web session and will be removed when closing down your web browser. Added servers will be added in a new created *Session Environment*.

2.3.3 Messages

Get a summary of latest registered error messages.



2.4 Environment View



In the environment view you will get an overview of the servers within your environment. Server status, and distributed load.

2.4.1 Server Availability tab

1) View Available Servers

Servers configured in selected environment will be listed.
If load balancer / cluster is configured this address will be verified. In this example the cluster address is responding successfully.

LDAP and LDAPS port availability, when the server started, query time from CN=Monitor to the replica in milliseconds and recognized vendor name will be shown.

If the vendor name isn't recognized it will be marked as *unknown*.

Additional information about the server, if configured with the options *description* and *URL*, will also be shown.



If server is *iPlanet* based and can be recognized as a hub or master the letter M (for master) or H (for hub) will be displayed.



A red server indicates connection issues.



A warning sign indicates replication issues.

If server is of type *iPlanet* and replication error exists an error message will be displayed:

2) Get detailed information

Detailed information like replication status, current connections and server uptime.

Replication Status	Current Connections	Uptime
-	68	4 Day(s)

On replication error the detailed information will be displayed and replication status will be marked red:

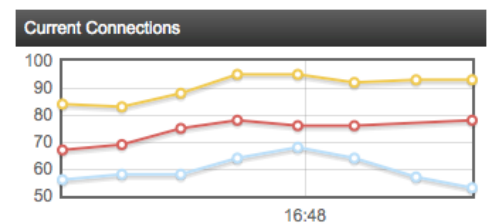
	10.0.1.12	1389	1636	2012-01-20 20:28	15.56	Sun Java System	
Master replica http://10.0.1.10:8080/dscc7							
Replication Status				Current Connections		Uptime	
Error: 0 / 2				1		0 Day(s)	

3) Operations

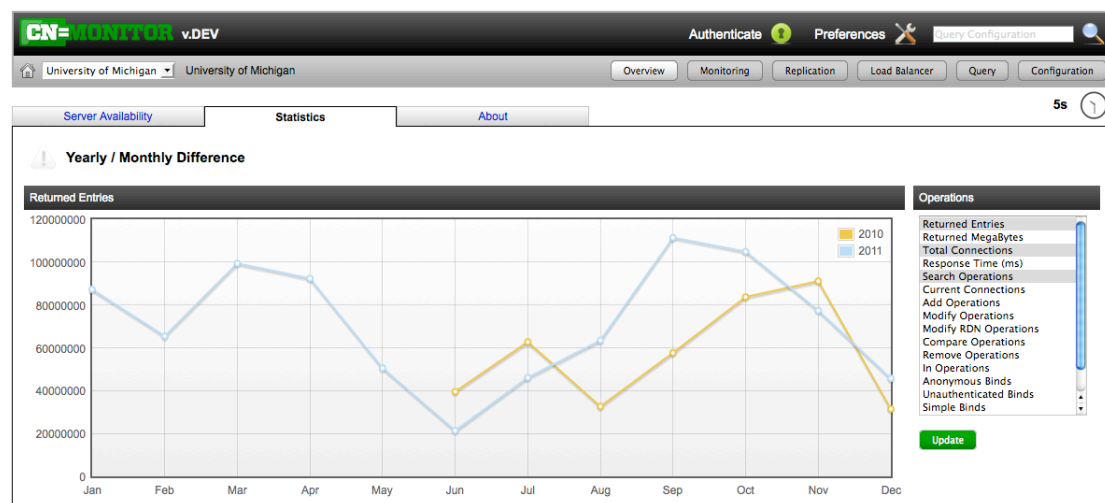
Pie charts showing the following operations:

- Query Time
Creates a basic LDAP query and returns query time in milliseconds.
- Current connections
Current number of connections against Directory Server.

By selecting to reload the page the pie charts will be changed to line graphs.



2.4.2 Statistics tab



Compare monthly or yearly differences of collected performance counters.

View Operations Graph

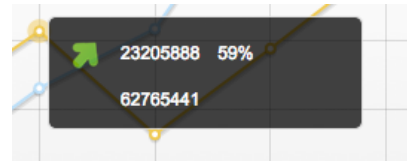
Operations for all configured servers divided per month and year.

Select which operations you want to view.

Detailed Information

View detailed information by moving the mouse pointer over a dot.

Includes difference in value and percentage compared to previous month and actual value for selected month.



To get this functionality up and running you need to enable database support and schedule both *collectdb.php* and *collectsummary.php*. For more information on how to configure these components see Installation document chapter *Setup Monitoring*.

The list of available operations to select from is depending on LDAP server type.

2.4.3 About tab

Server	Time	Message Type	Value
heat.dir.itd.umich.edu	2011-12-14 18:33:30	LDAP Online	2011-12-11 09:46
serpico.dir.itd.umich.edu	2011-11-14 19:45:01	LDAP Online	2011-10-29 04:14
heat.dir.itd.umich.edu	2011-11-14 19:45:01	LDAP Online	2011-10-29 06:04
donniebrasco.dir.itd.umich.edu	2011-11-14 19:45:01	LDAP Online	2011-10-29 04:15

Information about selected environment.

Information about the cluster

Cluster / Load balancer name and IP address that will be used.

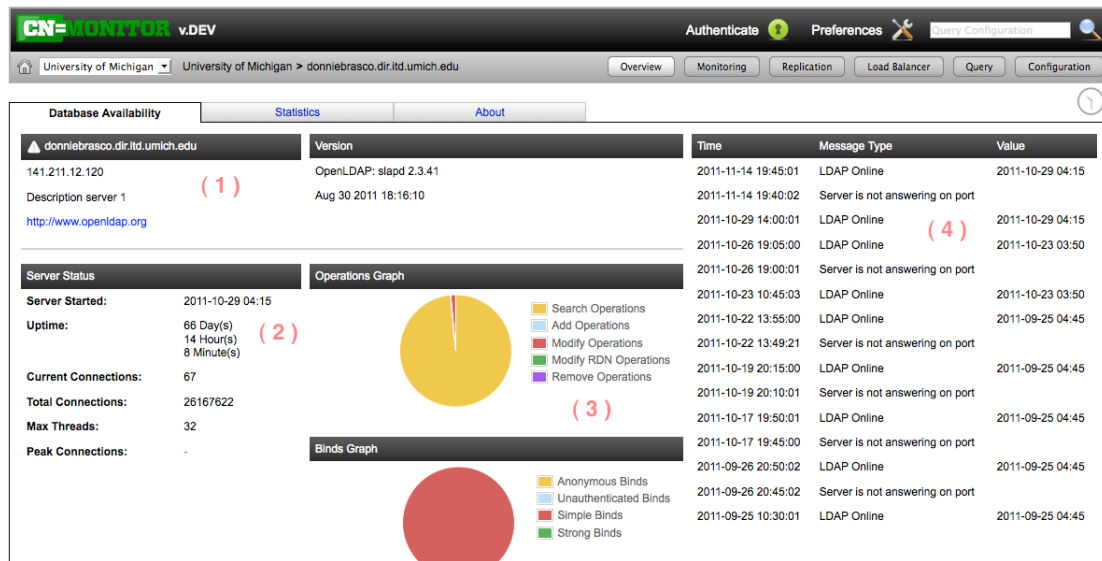
By default this will be the environment *name*. You can specify a load balancer address by adding the option *loadbalancer* to your environment configuration.

Available messages for the environment

Collected messages from servers configured for this environment.

To enable this functionality you need to have database support and schedule the *collectservermessage.php* component. For more information see Installation document chapter *Setup Monitoring*.

2.5 Server View



In the server view you will get current server statistics, historical statistics, certificate information and more.

2.5.1 Server Availability Tab

1) Server Information

Includes server name, IP address and vendor information.

2) Server Status

Displays, if available, when the server was started, its uptime, current and total connections, Max Threads (for Open LDAP this means the highest number of used threads, for RedHat DS/389 DS the configured number of open threads, Peak Connections (only available for Sun DS) displaying max nr of simultaneously used connections.

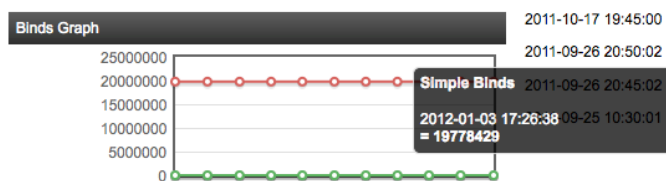
3) Graphs

Operations Graph

Displays a pie chart of LDAP operations.

Bind Graph

Displays a pie chart of LDAP bind operations.



By selecting to reload the page the pie charts will be changed to line graphs.

4) Server Messages

Messages collected from selected server.

To enable this functionality you need to have database support and schedule the *collectservermessage.php* component. For more information see Installation document chapter *Setup Monitoring*.

Compare Value function

Some values will show a question mark. You can click on these values and compare the value to other directory servers in your environment.

Select Servers

Value

Current Connections

Run

openldap1.localdomain
openldap2.localdomain
389ds1.localdomain
389ds2.localdomain
opendj1.localdomain
opendj2.localdomain

Result List

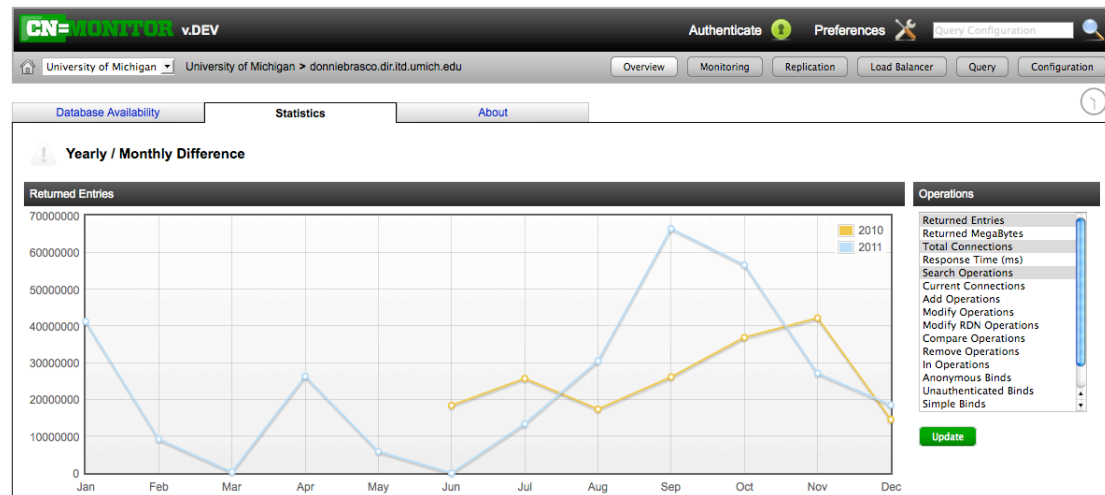
openldap1.localdomain	5
openldap2.localdomain	5
389ds1.localdomain	1
389ds2.localdomain	1
opendj1.localdomain	1
opendj2.localdomain	undefined

13

In this example comparing current connections CN=Monitor detects it as a value to summarize (*in this example: 13*). This is not applicable for all values.

We recommend that you use this feature to compare directory server versions, IP numbers and other comparable values not shown on environment page.

2.5.2 Statistics Tab



Compare monthly or yearly differences of collected performance counters. For more information about this view see *Statistics Tab* on environment level. The difference is that this view only shows the load of the selected server compared to the environment level that shows the summarized load on all servers.

The list of available operations to select from is depending on LDAP server type.

2.5.3 About Tab

Server Recognized As:	OpenLDAP
Description:	Description server 1
URL:	http://www.openldap.org
Naming Contexts:	dc=umich,dc=edu
Network	
DNS Name:	donniebrasco.dir.umd.umich.edu
IP Address:	141.211.12.120
LDAP Port:	389
Secure LDAP Port:	636
Vendor	
Vendor:	OpenLDAP: slapd 2.3.41
Version:	Aug 30 2011 18:16:10
Supported LDAP Version:	3
Supported SASL Mechanisms:	GSSAPI

Start TLS
Modify Password
Who am I?

LDAP Content Synchronization Control
Proxy Authorization Control
ManageDsaIT
Subentries
Paged Results Control
Values return filter
Matched Values Control
LDAP Post-read Control
LDAP Pre-read Control
Assertion Control

Modify-Increment
All Operational Attributes
OC AD Lists
True/False filters
Language Tag Options
Language Range Options

About selected server.

General information about the server

Shows what CN=Monitor recognizes this server as and available *Naming Contexts*.

Network

Network related information such as DNS A and C record, IP address and configured LDAP ports.

Vendor

Retrieved vendor and version information from LDAP server. Also supported LDAP Version and SASL mechanisms.

Supported Extensions

Supported extensions returned from the LDAP server. OID:s mapped to RFC:s if possible.

Supported Controls

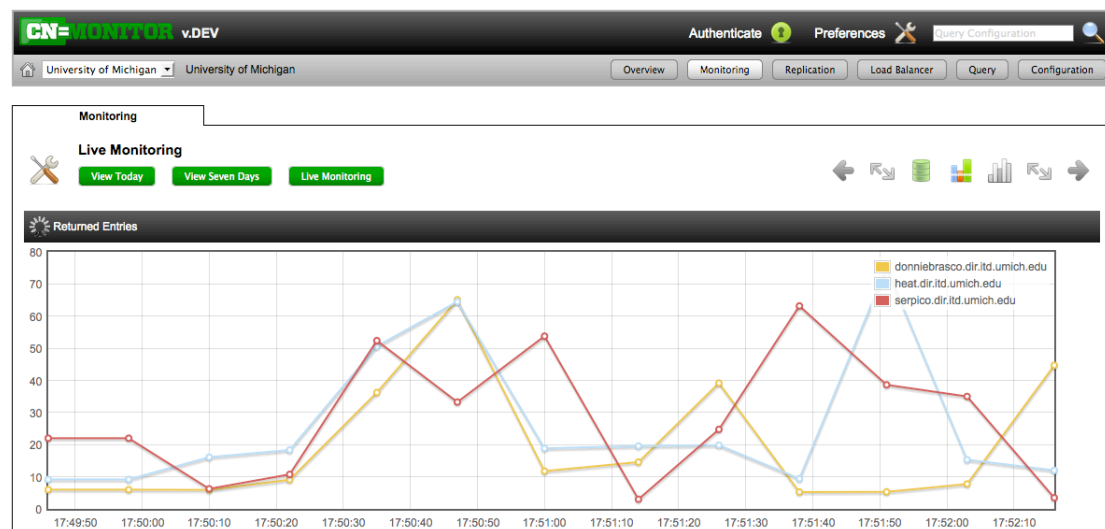
Supported Controls returned from the LDAP server. OID:s mapped to RFC:s if possible.

Supported Features

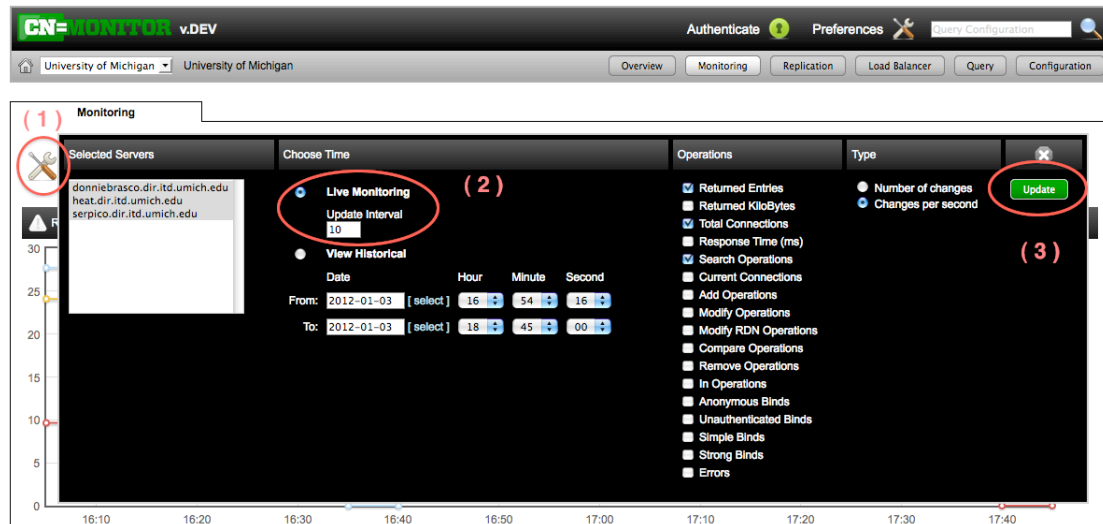
Supported Features returned from the LDAP server. OID:s mapped to RFC:s if possible.

2.6 Monitoring

2.6.1 Live Monitoring



With live monitoring you will get a view of current server load.



Either press the button **Live Monitoring** for default settings or:

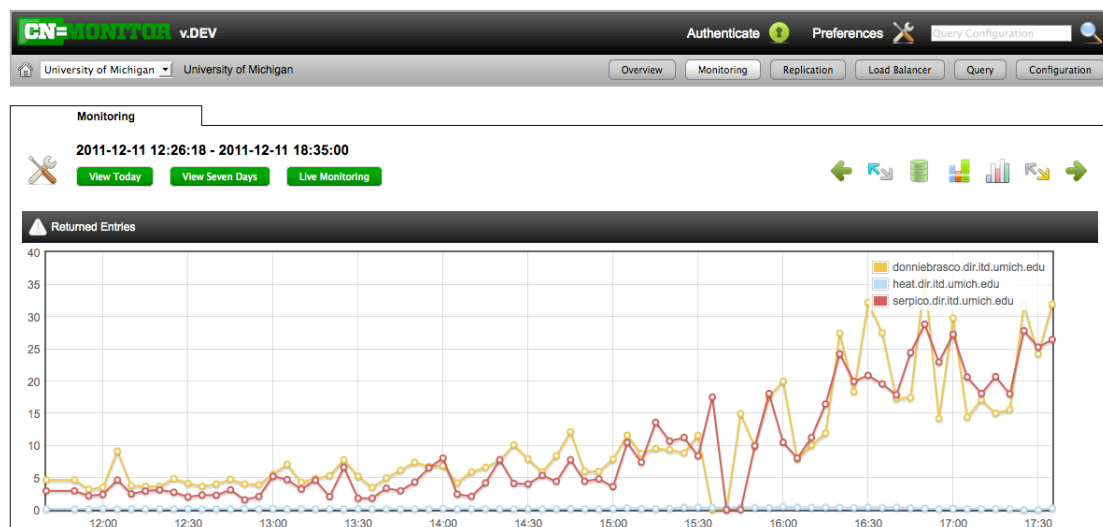
- 1) Click on the settings icon to open up the settings for monitoring.
- 2) Select Live Monitoring
- 3) Click Update

Available options for live monitoring

- 1) Combine Result.
Combines all servers in to one single line.
- 2) Average Result.
Displays a gray coloured line with the average value of all monitored servers.



2.6.2 History Monitoring



A view of gathered performance counters. Requires database support.



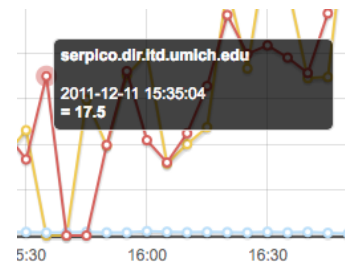
Default values for monitoring will be selected environment or server, current day and the following operations based on server type:

- IBM, OpenLDAP, iPlanet based and OpenDS based
Returned Entries, Total Connections, Search Operations
- Novell
Search Operations, Returned KiloBytes

Configuration Panel

Select from which date you want to see historical information and select which operations such as if you want to have the result displayed in a different time zone than UTC.

The list of available operations to select from is depending on LDAP server type.



Set the mouse pointer over a collected performance counter to show details about server name, collect date and value.

Options

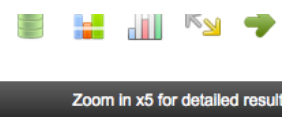


You have several options available when viewing collected performance counters.

- 1) Go back or forward in time by date.
- 2) Expand the date by 50% at any direction.
- 3) Combine all servers in to one single result.
- 4) Show average value.
- 5) Compare this graph with previous day (or time frame)

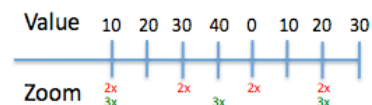
Handle large result sets

As large result sets will create a high load on both the web server and browser CN=Monitor won't deliver all measure



points (starting at 500 points per server). This should not affect any measured points except a less fine-grained result.

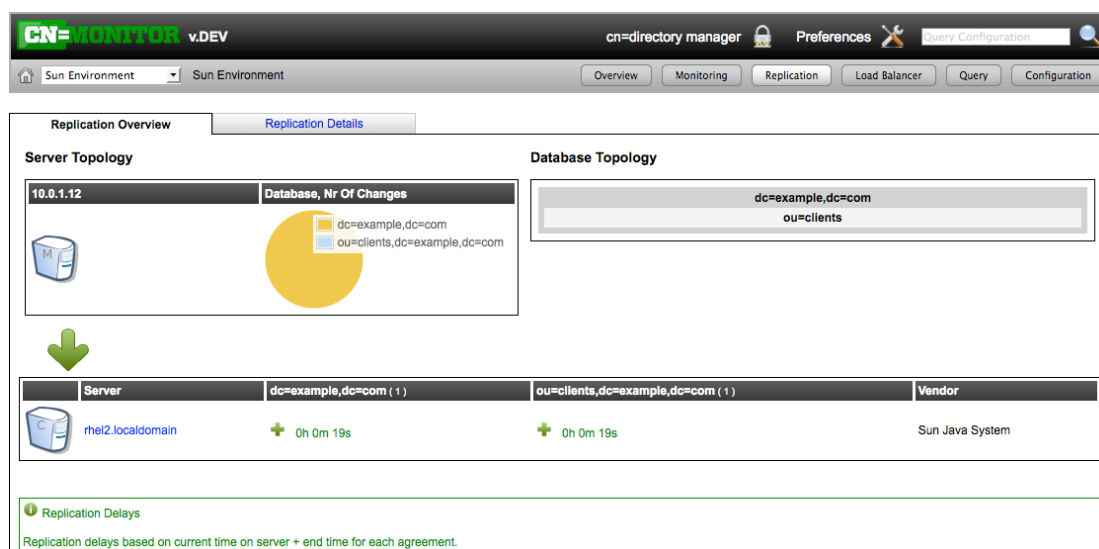
In the example to the right a 2x zoom (over 200 points) will deliver the values of 10, 30, 0 and 20. In the example with 3x zoom the values of 10, 40 and 0 (as 20 is lower than 40 indicating a server restart) will be delivered.



Zoom

A graph can be zoomed by holding down the mouse pointer and select an area to zoom in to.

2.7 Replication



2.7.1 View replication status.

View replication status if you are running OpenLDAP, an *iPlanet* (389 DS / Redhat / Sun / Oracle DSEE) based server or OpenDS based (OpenDS / OpenDJ / Oracle Unified Directory) server. Other server may be added in the future depending on server limitations and community support.

Server Topology




Compare replication load between your backend databases

Database Topology

Shows your replication agreements configuration

Displays available replication agreements

	Replication agreement ok
--	--------------------------

	Replication errors exist
	Replication warning exist (can be replication disabled or replication not completed within x hours)
	Replication ok. Showed in <i>Replication Details</i> tab




Acceptable Delay

Gray text indicating that no replication has been done within 24 hours.

Acceptable delay indication can be adjusted by changing the configuration file replication.php.

This will not be treated as an error. For servers with frequent updates this verification can indicate frozen replication agreements based on network issues.

Details about each agreement

Server	dc=example,dc=com (1)	ou=clients,dc=example,dc=com (1)	Vendor
 rhel2.localdomain	 0h 0m 19s	 0h 0m 19s	Sun Java System
Database	Start Replication Time	End Replication Time	Server Replication Time (CSN)
ou=clients,dc=example,dc=com	2012-01-20 20:49:41	2012-01-20 20:49:41	
Description	Replication Schedule	Nr Of Changes	Message
	*	0	0 incremental update session stopped : nothing to replicate
			In Progress
			FALSE

2.7.2 Replication Details tab

By using the tab Replication Details you can get a simple table view of returned replication status.

CN=MONITOR

v.DEV

cn=directory manager

Preferences

Query Configuration

Sun Environment

Sun Environment

Overview

Monitoring

Replication

Load Balancer

Query

Configuration

Replication Overview

Replication Details

Replication Details

Selected Server

Server	Database	Server Replication Time (CSN)
10.0.1.12	dc=example,dc=com	
10.0.1.12	ou=clients,dc=example,dc=com	

Agreements

Server	Database	Start Replication Time	End Replication Time	Server Replication Time (CSN)	LDAP Port	In Progress	Replication Status
rhel2.localdomain	dc=example,dc=com	2012-01-20 20:49:41	2012-01-20 20:49:41		1389	FALSE	0 Incremental update session stopped : nothing to replicate
rhel2.localdomain	ou=clients,dc=example,dc=com	2012-01-20 20:49:41	2012-01-20 20:49:41		1389	FALSE	0 Incremental update session stopped : nothing to replicate

This will also change found CSN values on the master server.

2.7.3 Replication notes iPlanet based

This includes 389 DS, Red Hat DS, Sun DS and Oracle DSEE servers.

To view the replication status you need to let CN=Monitor access the cn=config suffix.

There are two verification steps available for these servers.

Verification on replication agreement level

Reading last known status on each replication agreement on the master server.

If agreement failure exist CN=Monitor will show alerts and errors on start and environment page.

Verification based on CSN (Change Sequence Number)

Compare last sequence number between master and replica.

This extra verification can determine if the master server stops sending updates but still process changes. Users have seen this related to network issues or WAN replication.

CSN verification will not trigger replication alerts on start and environment page.

2.7.4 Replication notes OpenLDAP

Verification is based on CSN, Change Sequence Number, by comparing all servers in one single environment.

Unfortunately this means that you can't group masters in one environment and read-only replicas in another. They all have to be grouped in one single environment.

Replication error will be shown if CSN value differ more than 60 seconds between the server you are looking at and other replicas.

However, CSN verification doesn't guarantee that replication agreements exists and CN=Monitor will not show or alert agreements on the start or environment page unless you set the configuration option replicatype.

If you have configured `<replicatype>master</replicatype>` replication verification will be performed between this server and all other replicas in environment. This also includes sending alerts with `collectservermessage.php` on replication issues.

From version 3.1 you don't need to access the `cn=config` database to verify replication for OpenLDAP.

If you can access the `cn=config` database the `<rid>` will be shown as database ID. The `<rid>` is the replica ID uniquely identifying the replica locally in the `syncrepl` consumer server.

This is an example of a replication configuration.

slapd.conf

Configuration for syncrepl

```
# syncrepl Provider for primary db
overlay syncrepl
syncrepl-checkpoint 5 1

# syncrepl directive
syncrepl      rid=001
               provider=ldap://host2
               bindmethod=simple
               binddn="cn=Manager,dc=domain,dc=com"
               credentials=secret
               searchbase="dc=domain,dc=com"
               schemachecking=on
               type=refreshAndPersist
               retry="60 +"

mirrormode on
```

Configuration for your monitoring user.

You have to be able to access both `cn=monitor` and `cn=config`.

```
# enable monitoring
```

```
database monitor
# allow onlu rootdn to read the monitor
access to *
    by dn.exact="cn=CNMonitor User,dc=domain,dc=com" read
    by * none

# enable monitoring
database config
# allow onlu rootdn to read the monitor
access to *
    by dn.exact="cn=CNMonitor User,dc=domain,dc=com" read
    by * none
```

And the replication must update the contextCSN attribute. You can verify this by:

```
$ ldapsearch -x -h <host> -D "<monitoring dn>" -W -s base -b "<suffix>" contextCSN
```

Result, example:

```
dn: dc=domain,dc=com
contextCSN: 20100823161844.565867Z#000000#000#000000
contextCSN: 20100825160932.333710Z#000000#001#000000
```

2.7.5 Replication notes OpenDS based

This includes OpenDS, OpenDJ and Oracle Unified Directory Server.

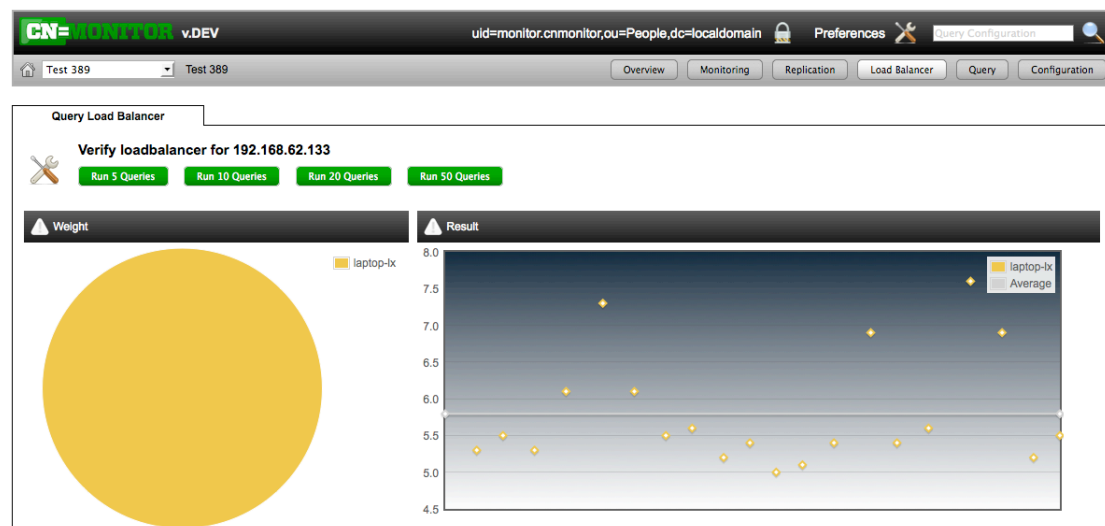
To view the replication status you need to let CN=Monitor access the cn=config suffix.

Verification is based on Change Sequence Number and configured replication agreements.

If the replication server can't contact a server and removes replication status in cn=monitor suffix the replication agreement is set to error.

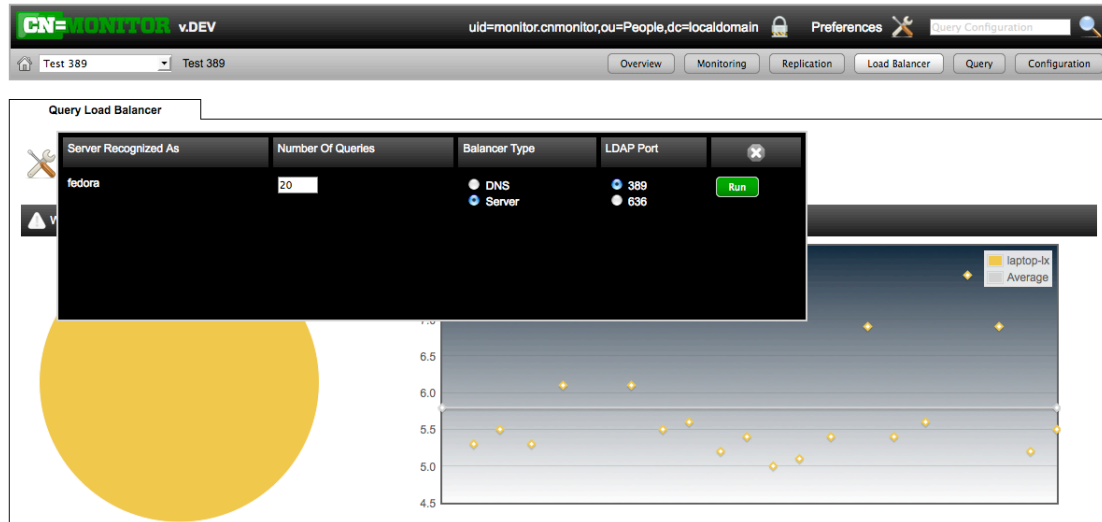
A server containing replication agreements will be treated as a *master* and errors will be displayed on start and environment page.

2.8 Load Balancer



In order to use this functionality you must set the <loadbalancer> option on environment level.

2.8.1 Options for load balancer test

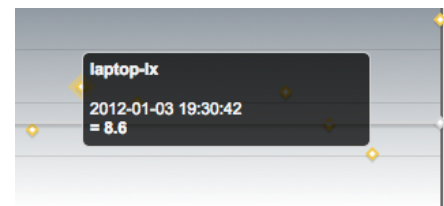


- 1) Select how many queries you want to send against the configured cluster / load balancer
- 1) Balancer Type
 DNS if you are using a DNS based balancer solution
 Server is only supported for iPlanet (Red Hat / Sun) based servers.
- 2) LDAP Ports
 Run queries against configured LDAP port 389 or LDAPS port 636.
- 3) Run test.

A pie chart represents the weight of responding servers.

The gray line represents the average of milliseconds in returned result.

Using mouse cursor over one of the dots will display detailed information about server name and number of milliseconds.



iPlanet instance name

To be able to match your hosts against the returned instance name the following is done:

For Red Hat / 389 DS (requires cn=config access):
 CN=Monitor returns the entry "cn=config,cn=ldbm database,cn=plugins,cn=config". Removes the common paths used for the directory server:

- *slapd-
- /db
- /opt/

For Sun / Oracle DSEE (requires cn=monitor access):
CN=Monitor returns the entry “cn=disk0,cn=disk,cn=monitor”. Removes the common paths used for the directory server:

- *slapd-
- /db
- /opt/

The instance name is matched against the hostname or configured alias. To use this feature your instance names must be unique within your environment. You can use the configuration option *alias* to map your instance name with your configured server.

2.9 Query

The screenshot shows the CN=Monitor v.DEV interface. The top navigation bar includes 'Authenticate', 'Configuration', and 'Query Configuration'. Below the navigation bar, there are tabs for 'Query', 'Result', and 'Single Entry'. The 'Query' tab is active, and the 'Result List' is displayed. The result list shows a table of LDAP entries for 'fedora1' and 'fedora2'. The table has columns for 'Server', 'uid', 'cn', 'sn', and 'givenName'. The 'Distinguished Name (DN)' is also shown for the first entry: 'uid=jwalker,ou=People,dc=example,dc=com'. The 'Created By' and 'Updated By' fields are also visible.

Server	uid	cn	sn	givenName
fedora1	1.1 jwalker	John Walker	Walker	John
Distinguished Name (DN) uid=jwalker,ou=People,dc=example,dc=com				
Created By cn=directory manager		Created TimeStamp 20101211012620Z	Updated By cn=directory manager	
Updated TimeStamp 20101211012620Z				
	1.2 jfalena	John Falena	Falena	John
fedora2	1.1 jwalker	John Walker	Walker	John
	1.2 jfalena	John Falena	Falena	John

Query one or several servers to verify data consistency or retrieve lists of users by searching a list of values.

Compared to other LDAP browsers this query mechanism has the ability to compare data between servers.

The screenshot shows the CN=Monitor v.DEV interface with the 'Query One or Several servers' form. The form has several sections: 'Select Servers' (listing 192.168.62.128, fedora1, and fedora2), 'Search' (with fields for Attribute (1), Value(s) (4), Base (3), and Query Filter (6)), 'Return Attributes' (with a list of attributes: uid, cn, sn, givenName), and a 'Run Query' button. The 'Protected Attributes' section lists 'userPassword'.

- 1) Select servers to query
You can select multiple servers
- 2) Attribute value to query
- 3) Base Suffix to query
- 4) Values
Can be a single value or a list of values
- 5) Attribute values to return from server
- 6) Filter to use for query

2.9.1 Query Result

The screenshot shows the CN=Monitor v.DEV interface. The 'Query' tab is selected, and the 'Result List' table is displayed. The table has columns for Server, uid, cn, sn, and givenName. The first row shows results for 'fedora1' with uid '1.1 jwalker', cn 'John Walker', sn 'Walker', and givenName 'John'. Below this, the Distinguished Name (DN) is shown as 'uid=jwalker,ou=People,dc=example,dc=com'. The table also includes 'Created By', 'Created TimeStamp', 'Updated By', and 'Updated TimeStamp' information. A 'Run Query' button is visible in the top right corner of the table area.

Server	uid	cn	sn	givenName
fedora1	1.1 jwalker	John Walker	Walker	John
Distinguished Name (DN) uid=jwalker,ou=People,dc=example,dc=com				
Created By cn=directory manager		Created TimeStamp 20101211012620Z	Updated By cn=directory manager	Updated TimeStamp 20101211012620Z
	1.2 jfalena	John Falena	Falena	John
fedora2	1.1 jwalker	John Walker	Walker	John
	1.2 jfalena	John Falena	Falena	John

Query Result can be exported to CSV format.
You can also view a single entry by clicking on the Text symbol or DN.

2.9.2 View Single Entry

The screenshot shows the CN=Monitor v.DEV interface with the 'Single Entry' tab selected. The entry is for 'uid=jwalker,ou=People,dc=example,dc=com'. The interface displays a list of attributes and their values for two different servers, 'fedora1' and 'fedora2'. The attributes are listed on the left, and the values are shown in a table. A 'Run Query' button is visible at the top right of the table area.

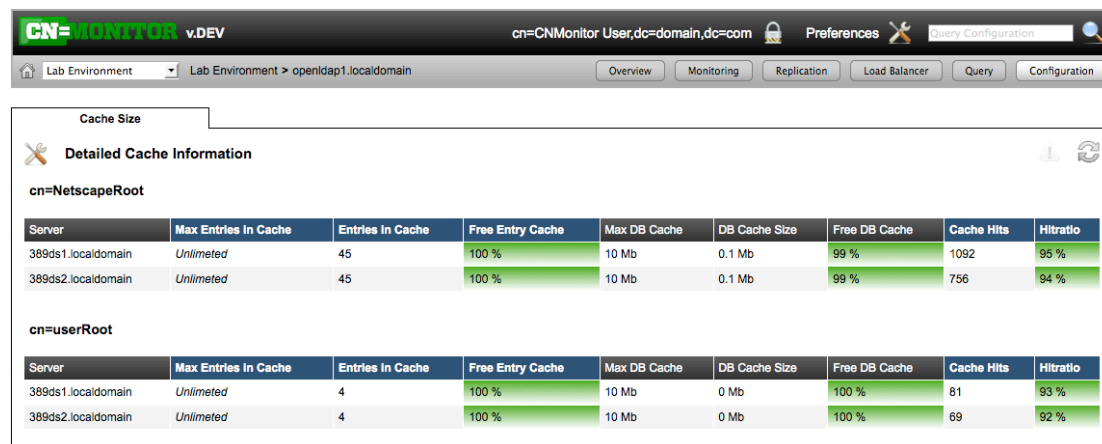
Attribute	Value (fedora1)	Value (fedora2)
cn	John Walker	John Walker
sn	Walker	Walker
givenName	John	John
objectClass	top person organizationalPerson inetOrgPerson	top person organizationalPerson inetOrgPerson
ou	Product Testing People	Product Testing People
l	Cupertino	Cupertino
uid	jwalker	jwalker
mail	jwalker@example.com	jwalker@example.com
telephoneNumber	+1 408 555 1476	+1 408 555 1476
facsimileTelephoneNumber	+1 408 555 1992	+1 408 555 1992
roomNumber	3915	3915

View single entry.

- 1) You can re-run your query using selected attributes.
Select the attributes to retrieve and click on the "Run Query" button.
- 2) You can compare selected entry with another directory server
Red colour "N / A" indicates that the attribute value doesn't exist.
Blue colour indicates that the attribute value is different.

Attributes only available on compare server will be displayed at the bottom and cannot be included to re-run queries.

2.10 Cache Sizes

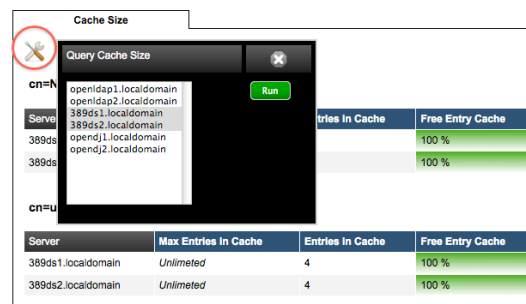


Compare cache sizes between several directory servers.

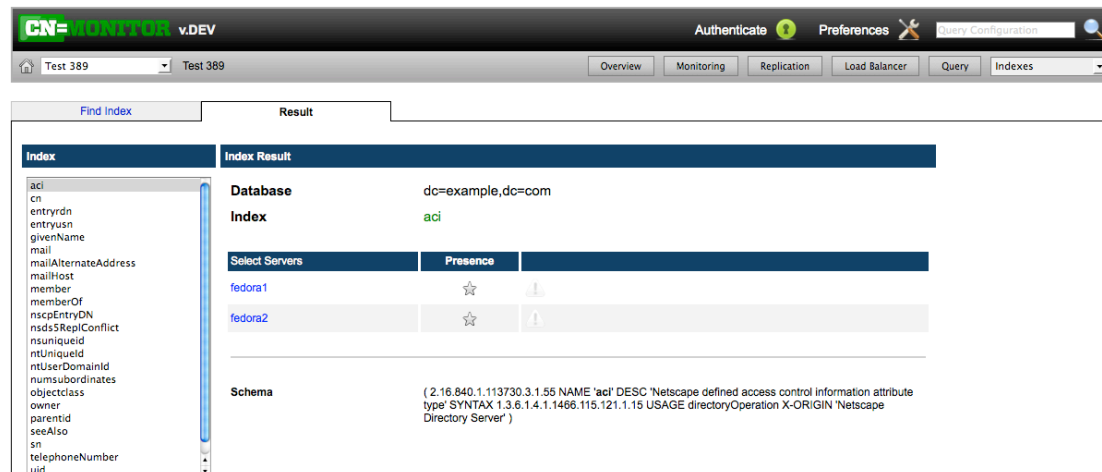
The view will be different based on what kind of cache values that can be fetched from directory server.

By opening the configuration panel you can select and compare cache values between servers.

Cache indicators will give you an indication if you need to adjust cache settings.



2.11 Indexes



Compare configured indexes between several directory servers.

- 1) Select which database and hosts to query for indexes.
 - 2) Select index
- Selected attribute schema syntax will be shows if the schema is accessible.

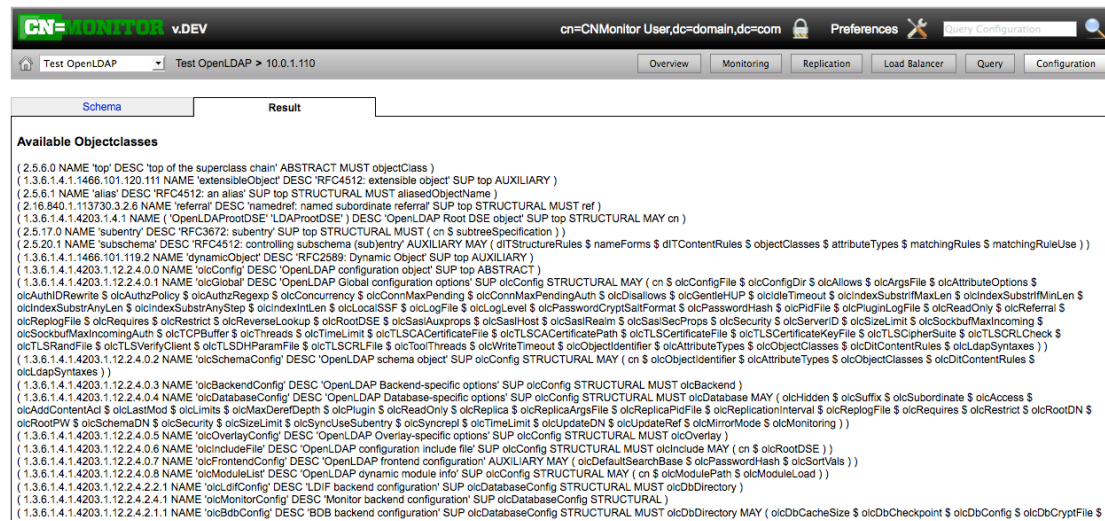
2.12 Certificate

C	ST	L
US	Michigan	Ann Arbor
US	Michigan	Ann Arbor
US	Michigan	Ann Arbor

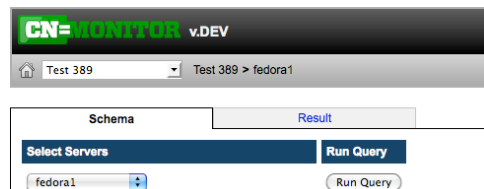
Compare certificate information between servers.

When selecting one or several servers and query for certificates you also make sure that you're not reading from the cache.

2.13 Schema



Retrieves LDAP schema from Directory Server



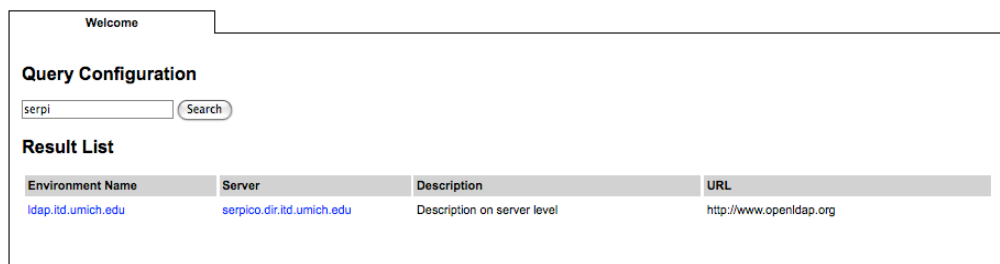
When selecting a server and query for the schema you also make sure that you're not reading from the cache.

2.14 Query Server(s)



Select a server or an environment by wildcard querying.

1. Start entering a couple of characters.
Suggestions of matching servers will be displayed in a select box.
Either select one of the servers by clicking using the mouse on one of the suggestions or pressing the down key, select a server or an environment and press enter.



2. If you can't find what you are looking for the search will continue to the query configuration page displaying a more detailed search result.

3 Mobile features

Available for iPhone and Android smartphones.

3.1 Start Page



On the start page you see essential environments information.
Server and load balancer / cluster availability.

3.2 Environment View



Environment view shows server availability and:

- Server started
- Query Time
- Current Connections
- Search Operations
- Replication Status

4 Collect / Summary scripts

To start using these scripts:

- Configure backend database
- Configure *wwwaddress*, *mailfrom*, *mailto* options

- Optional. If you want to trigger external scripts on events (i.e. server not responding or script failures) configure the option *runscript*.
- It is recommended to run each script from the command line as root before scheduling anything.

The result when running any of these scripts will be displayed on the screen and be stored in a log file located in the *temp* directory.

The *temp* directory is based on the environmental settings for your web server and will be displayed when running these scripts manually.

4.1 collectdb.php

This script collects and store current operational status (current connections, entries sent, number of binds etc.).

```
# php collectdb.php ["Environment Name"]
```

```
Start collecting Data (cn=monitor)
-----
Database - Is configured and responding

Environment: 0 ) Environment Name
-----
0 ) server1.mydomain.com
1 ) server2.mydomain.com
...
```

Collecting historical monitor information should be scheduled to run frequently. The following crontab example collects monitor information every 30 minutes:

```
*/30 * * * * cd /usr/share/cnmonitor/bin;php collectdb.php
```

Optional parameter

Optional parameter "Environment Name" can be specified to only run a specified environment. This is recommended if you want to collect monitor information using different time schedule on environment level.

Example:

```
*/5 * * * * php /usr/share/cnmonitor/bin/collectdb.php "Important
Environment"
*/30 * * * * php /usr/share/cnmonitor/bin/collectdb.php "Not so important
Environment"
```

A pid file is created to ensure that this script doesn't run if previous failures exist or if you have configured to run the script to frequent.

If you choose to use the "Environment" parameter this pid file will be unique for each collectdb scheduled.

4.2 collectservermessage.php

This script collects server status and may send alerts on mail or trigger external scripts.

The following server status can be detected: Port not available, LDAP not available, LDAP available, Replication Errors and LDAP server restarted.

```
# php collectservermessage.php
```



```
Start collecting Server Messages (cn=monitor)
-----
Database - Is configured and responding

Environment: 0 ) Environment Name
-----
0 ) server1.mydomain.com
0 ) start_time - server1.mydomain.com
1 ) server2.mydomain.com
1 ) start_time - server2.mydomain.com
...
```

Collecting server messages should be scheduled to run frequently.
The following crontab example collects monitor information every ten minutes:

```
*/10 * * * * php /usr/share/cnmonitor/bin/collectservermessage.php
```

A *pid* file is created to ensure that this script doesn't run if previous failures exist or if you have configured to run the script to frequent.
This *pid* file will be removed by the script every 35 minutes which results in new attempts to connect against configured servers.

There are two log files for this script.
General log: cli_collectservermessage.tmp
Server Connection log: cli_collectservermessage_server.tmp

On server log will be attached when sending out the mail notification in order to check for hanging connections.

4.3 encryptpassword.php

Encrypt password for configuration file. Requires at least PHP version 5.3.

```
$ php encryptpassword.php
```

```
Encrypting password
-----
Enter password to encrypt:
Enter password to encrypt.
```

```
Password Encrypted!
-----
+ Password encrypted to: KgnlYkS8CdZrXqYP6UDVoQ==

Insert into your configuration in environment or server section as:
<encpassword>KgnlYkS8CdZrXqYP6UDVoQ==</encpassword>
```

If support exist you should receive an encrypted password.

A list of possible encryption methods will be displayed.
You can change encryption method by adding the general environment configuration option:
<encryption>SEED-CBC</encryption>

4.4 collectsummary.php

Creates a summary of collected historical monitor information for long-term analysis. Note that this script doesn't do any LDAP queries. It is only contacting the SQL Database.

php collectsummary.php

```
Start creating summary (cn=monitor)
-----
Database - Is configured and responding

Environment: 0 ) <environment name>
-----
0 ) <hostname>
0 ) ent_sent - Summary Value: 11019370
0 ) ent_sent - Value Stored to db
0 ) byte_sent - Summary Value: 6269838403
0 ) byte_sent - Value Stored to db
0 ) tot_con - Summary Value: 5425092
0 ) tot_con - Value Stored to db
0 ) search - Summary Value: 11248920
0 ) search - Value Stored to db
0 ) add - Summary Value: 1842
0 ) add - Value Stored to db
0 ) modify - Summary Value: 31630
0 ) modify - Value Stored to db
0 ) modifyrdn - Summary Value: 27
0 ) modifyrdn - Value Stored to db
0 ) remove - Summary Value: 2472
0 ) remove - Value Stored to db
0 ) in - Summary Value: 20781537
0 ) in - Value Stored to db
0 ) anon_bind - Summary Value: 0
0 ) anon_bind - Value NOT Stored to db as it is empty
0 ) simple_bind - Summary Value: 3986880
0 ) simple_bind - Value Stored to db
0 ) strong_bind - Summary Value: 0
0 ) strong_bind - Value NOT Stored to db as it is empty
0 ) error - Summary Value: 0
0 ) error - Value NOT Stored to db as it is empty
...
```

Creates a summary of historical events every day at 4 am.

```
0 4 * * * php /usr/share/cnmonitor/bin/collectsummary.php
```

A *pid* file is created to ensure that this script doesn't run if previous failures exist or if you have configured to run the script to frequent.

5 LDAP Performance

You might ask. How does the monitoring work? How much LDAP queries are generated when using CN=Monitor?

CN=Monitor is accessing the following places to receive monitoring and configuration information:

Root DN	Vendor name information For eDirectory we also read monitoring information from here
cn=Monitor	Monitoring database Standard LDAP suffix to read LDAP performance / monitoring data
cn=Config	Configuration database Standard LDAP suffix to read LDAP configuration (cache and replication)

The following table describes how many LDAP connects and queries that are sent to different LDAP servers.

Vendor	Operation	Connects	Queries
OpenLDAP	collectdb.php	2	One query for each monitoring value. 15 queries in total.
iPlanet	collectdb.php	2	Two queries.
eDirectory	collectdb.php	2	Two queries.
IBM Tivoli	collectdb.php	2	Two queries.
<i>All</i>	Live Monitoring	One connect for each graph	One query for each graph.
<i>All</i>	Environments -> Environment -> Server -> Replication	Around 25 Connections	Around 30 queries

Note that caches are used to avoid sending unnecessary not frequently changed LDAP values such as Vendor information, certificate and schema.

As these caches holds server availability you need to clear the caches if the server becomes unresponsive or if any configuration affecting the caches are changed.

Enable directory server logs if you need to measure your own environment.

6 Contact Information

6.1 Download Updates

Updates are available at CN=Monitor project page:
<http://cnmonitor.sourceforge.net/>

6.2 Donate using PayPal

If you appreciate CN=Monitor. Feel free to donate any amount to support future development of this software and show your appreciation.

6.3 Contact Developer(s)

You can contact the developer of this software by sending an email to:

Andreas Andersson monitorldap@gmail.com

Or stay in touch using the Project news on the project site:

<http://cnmonitor.sourceforge.net/>