Red Hat Directory Server 12

Monitoring server and database activity

Using logs and statistics to monitor server state, database activity, and replication

Last Updated: 2022-06-20

Red Hat Directory Server 12 Monitoring server and database activity

Using logs and statistics to monitor server state, database activity, and replication

Legal Notice

Abstract

Directory Server provides log files and several statistics about its databases that you can use to monitor Directory Server. You can query the statistics using LDAP statements or using the Simple Network Management Protocol (SNMP).

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:
  1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.
  2. Use your mouse cursor to highlight the part of text that you want to comment on.
  3. Click the **Add Feedback** pop-up that appears below the highlighted text.
  4. Follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
  1. Go to the Bugzilla website.
  2. As the Component, use **Documentation**.
  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
  4. Click **Submit Bug**.

CHAPTER 1. USING THE HEALTH CHECK TO IDENTIFY PROBLEMS

Perform a health check to analyze the Directory Server instance for potential issues and to get recommended solutions.

1.1. RUNNING THE DIRECTORY SERVER HEALTH CHECK

Use the **dsctl healthcheck** command to run a health check.

Procedure

- To run a health check, enter:

```
# dsctl instance_name healthcheck
Beginning lint report, this could take a while ...
Checking Backends ...
Checking Config ...
Checking Encryption ...
Checking FSChecks ...
Checking ReferentialIntegrityPlugin ...
Checking MonitorDiskSpace ...
Checking Replica ...
Checking Changelog5 ...
Checking NssSsl ...
Healthcheck complete.
1 Issue found!  Generating report ...
```

To display the output in JSON format, pass the **--json** parameter to the command:

```
# dsctl --json instance_name healthcheck
```

Example 1.1. Possible report of the health check

```
[1] DS Lint Error: DSELE0001
-------------------------------------------------------------------------------
Severity: MEDIUM
Affects:
 -- cn=encryption,cn=config

Details:
-----------
This Directory Server may not be using strong TLS protocol versions. TLS1.0 is known to
have a number of issues with the protocol. Please see:

https://tools.ietf.org/html/rfc7457

It is advised you set this value to the maximum possible.

Resolution:
-----------
There are two options for setting the TLS minimum version allowed.  You,
can set "sslVersionMin" in "cn=encryption,cn=config" to a version greater than "TLS1.0"
```

You can also use 'dsconf' to set this value. Here is an example:

```
# dsconf slapd-instance_name security set --tls-protocol-min=TLS1.2
```

You must restart the Directory Server for this change to take effect.

Or, you can set the system wide crypto policy to FUTURE which will use a higher TLS minimum version, but doing this affects the entire system:

```
# update-crypto-policies --set FUTURE
```

===== End Of Report (1 Issue found) =====

Example 1.2. Possible report of the health check in JSON format


```
[
    {
        "dsle": "DSELE0001",
        "severity": "MEDIUM",
        "items": [
            "cn=encryption,cn=config"
        ],
        "detail": "This Directory Server may not be using strong TLS protocol versions.
TLS1.0 is known to\nhave a number of issues with the protocol. Please
see:\n\nhttps://tools.ietf.org/html/rfc7457\n\nIt is advised you set this value to the
maximum possible.",
        "fix": "There are two options for setting the TLS minimum version allowed.  You,\ncan
set \"sslVersionMin\" in \"cn=encryption,cn=config\" to a version greater than
\"TLS1.0\"\nYou can also use 'dsconf' to set this value.  Here is an example:\n\n    #
dsconf slapd-instance_name security set --tls-protocol-min=TLS1.2\n\nYou must restart
the Directory Server for this change to take effect.\n\nOr, you can set the system wide
crypto policy to FUTURE which will use a higher TLS\nminimum version, but doing this
affects the entire system:\n\n    # update-crypto-policies --set FUTURE"
    }
]
```


Additional resources

- Overview of health checks

1.2. OVERVIEW OF HEALTH CHECKS

Overview of health checks performed by the **dsctl healthcheck** command.

Table 1.1. Health checks overview

Component	Severity	Result code	Description

Component	Severity	Result code	Description
Back end	Low	DSBLE0003	The database was not initialized. The database was created, but it is empty.
Back end	Medium	DSBLE0001	The mapping tree entry for a back end is missing in the configuration.
Config	Low	DSCLE0001	High-resolution time stamps are disabled.
Config	High	DSVIRTLE0001	A virtual attribute is incorrectly indexed. Indexed attributes used by roles or Class of Service (CoS) definitions can corrupt search results.
Operating System	Medium	DSPERMLE0001	The permissions set on the **/etc/resolve.conf** file are different to **0644**.
Operating System	High	DSDSLE0001	Low disk space.
Operating System	High	DSPERMLE0002	The permissions set on the **/etc/dirsrv/slapd-instance_name/pin.txt** and **/etc/dirsrv/slapd-instance_name/pwdfile.txt** files are different to**0400**.
Plug-ins	Low	DSRILE0001	An update delay is set for the Referential Integrity plug-in. This can cause replication issues.
Plug-ins	High	DSRILE0002	The Referential Integrity plug-in misses indexes. The plug-in queries certain attributes for every delete operation if they are not indexed. This can cause hard-to-detect unindexed searches and high CPU usage.
Replication	Low	DSREPLLE0002	Conflict entries exist in the database.
Replication	Low	DSSKEWLE0001	The replication time skew is larger than 6 hours and lower than 12 hours.
Replication	Medium	DSCLLE0001	Changelog trimming is disabled. In this case, the changelog grows without limits.
Replication	Medium	DSREPLLE0004	The health check failed to retrieve the replication status.
Replication	Medium	DSREPLLE0003	The topology is out of synchronization, but the replication is working.

Component	Severity	Result code	Description
Replication	Medium	DSREPLLE0005	A remote replica is not reachable.
Replication	Medium	DSSKEWLE0002	The replication time skew is larger than 12 hours and lower than 24 hours.
Replication	High	DSREPLLE0001	The topology is out of synchronization, and the replication is not working.
Replication	High	DSSKEWLE0003	The replication time skew is larger than 24 hours. Replication sessions could break.
Security	Medium	DSELE0001	The minimum TLS version is set to a value lower than TLS 1.2.
Security	High	DSCLE0002	A password storage scheme is weak.
Server	High	DSBLE0002	The health check failed to query the back end.
TLS certificates	Medium	DSCERTLE0001	The server certificate expires within the next 30 days.
TLS certificates	High	DSCERTLE0002	The server certificate has expired.

CHAPTER 2. MONITORING THE REPLICATION TOPOLOGY USING THE COMMAND LINE

To monitor the state of the directory data replication between suppliers, consumers, and hubs, you can use replication topology report that provides information on the replication progress, replica IDs, number of changes, and other parameters. To generate the report faster and make it more readable, you can configure your own credentials and aliases.

2.1. DISPLAYING A REPLICATION TOPOLOGY REPORT USING THE COMMAND LINE

To view overall information about the replication status for each agreement in your replication topology, you can display the replication topology report. To do so, use the **dsconf replication monitor** command.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.

Procedure

- To view a replication topology report, enter:

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication monitor
```

The **dsconf** utility will request authentication credentials for each instance in the topology:

```
Enter password for cn=Directory Manager on ldap://supplier.example.com: password
Enter a bind DN for consumer.example.com:389: cn=Directory Manager
Enter a password for cn=Directory Manager on consumer.example.com:389: password

Supplier: server.example.com:389
--------------------------------
Replica Root: dc=example,dc=com
Replica ID: 1
Replica Status: Online
Max CSN: 5e3acb77001d00010000

Status For Agreement: "example-agreement" (consumer.example.com:1389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20211209122116Z
Last Update End: 20211209122116Z
Number Of Changes Sent: 1:21/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20211209122111Z
Last Init End: 20211209122114Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: In Synchronization
```

```
Replication Lag Time: 00:00:00

Supplier: consumer.example.com:1389
--------------------------------
Replica Root: dc=example,dc=com
Replica ID: 65535
Replica Status: Online
Max CSN: 00000000000000000000
```

Additional resources

- Setting credentials for replication monitoring in the .dsrc file
- Using aliases in the replication topology monitoring output
- Displaying a replication topology report using the web console

2.2. SETTING CREDENTIALS FOR REPLICATION MONITORING IN THE .DSRC FILE

By default, the **dsconf replication monitor** command asks for bind DNs and passwords when authenticating to remote instances. To generate the report faster and easier in the future, you can set the bind DNs, and optionally passwords, for each server in the topology in the user's ~/**.dsrc** file.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.

Procedure

1. Optional: Create the ~/**.dsrc** file.
2. In the ~/**.dsrc** file, set the bind DNs, and passwords. For example:

```
[repl-monitor-connections]
connection1 = server1.example.com:389:cn=Directory Manager:*
connection2 = server2.example.com:389:cn=Directory Manager:[~/pwd.txt]
connection3 = hub1.example.com:389:cn=Directory Manager:S3cret
```

This example uses connection1 to connection3 as keys for each entry. However, you can use any unique key.

When you run the **dsconf replication monitor** command, the **dsconf** utility connects to all servers configured in replication agreements of the instance. If the utility finds the hostname in ~/**.dsrc**, it uses the defined credentials to authenticate to the remote server. In the example above, **dsconf** uses the following credentials when connecting to a server:

Hostname	Bind DN	Password setup method
server1.example.com	cn=Directory Manager	Requests the password

Hostname	Bind DN	Password setup method
server2.example.com	cn=Directory Manager	Reads the password from **~/pwd.txt**
hub1.example.com	cn=Directory Manager	S3cret

Verification

- Run the **dsconf replication monitor** command to see If **dsconf** utility uses credentials configured in the ~/**.dsrc** file. For more information, see

Displaying a replication topology report using the command line .

Additional resources

- Setting credentials for replication monitoring using the web console

2.3. USING ALIASES IN THE REPLICATION TOPOLOGY MONITORING OUTPUT

To make the report more readable, you can set your own aliases that will be displayed in the report output. By default, the replication monitoring report contains the hostnames of remote servers.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.

Procedure

If you want to see aliases in the report, use one of the following methods:

- Define the aliases in the ~/**.dsrc** file:

```
[repl-monitor-aliases]
M1 = server1.example.com:389
M2 = server2.example.com:389
```

- Define the aliases by passing the **-a alias=*host_name:port*** parameter to the **dsconf replication monitor** command:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication monitor -a
M1=server1.example.com:389 M2=server2.example.com:389
```

In both cases, the **dsconf replication monitor** command displays the alias in the output:

```
...
Supplier: M1 (server1.example.com:389)
```

```
--------------------------------
Replica Root: dc=example,dc=com

...
Supplier: M2 (server2.example.com:389)
--------------------------------
Replica Root: dc=example,dc=com
```

Additional resources

- Configuring replication naming aliases using the web console

CHAPTER 3. MONITORING THE REPLICATION TOPOLOGY USING THE WEB CONSOLE

To monitor the state of the directory data replication between suppliers, consumers, and hubs, you can use replication topology report that provides information on the replication progress, replica IDs, number of changes, and other parameters. To generate the report faster and make it more readable, you can configure your own credentials and aliases.

3.1. DISPLAYING A REPLICATION TOPOLOGY REPORT USING THE WEB CONSOLE

To view overall information about the replication status for each agreement in your replication topology, you can display the replication topology report.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.
- You are logged in to the web console.

Procedure

1. Navigate to **Monitoring → Replication**. The **Replication Monitoring** page opens.
2. Click **Generate Report**.
3. Enter the passwords for login to remote instances and click **Confirm Credentials Input**.
   Directory Server uses bind DNs values from existing replication agreements.
   The replication topology report will be generated on the **Report Result** tab.

NOTE

To generate another replication topology report, go to the **Prepare Report** tab.

Additional resources

- Setting credentials for replication monitoring in the .dsrc file
- Using aliases in the replication topology monitoring output
- Displaying a replication topology report using the web console

3.2. SETTING CREDENTIALS FOR REPLICATION MONITORING USING THE WEB CONSOLE

To generate the replication topology report faster and easier, you can set your own bind DNs, and optionally passwords, for each server in the topology for authentication. In this case, you do not need to confirm replication credentials each time you want to generate a replication topology report. By default, Directory Server takes these credentials from existing replication agreements.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumer.
- You are logged in to the web console.

Procedure

1. Navigate to **Monitoring → Replication**. The **Replication Monitoring** page opens.
2. Click **Add Credentials**.
3. Enter replication login credentials you want to use for authentication to remote instances:
   - **Hostname**. A remote instance hostname you want the server to authenticate to.
   - **Port**. A remote instance port.
   - **Bind DN**. Bind DN used for authentication to the remote instance.
   - **Password**. A password used for authentication.
   - **Interactive Input**. If checked, Directory Server will ask for a password every time you generate a replication topology report.
4. Click **Save**.

Verification

Generate the replication topology report to see If the report asks for the credentials. For more information, see

Displaying a replication topology report using the web console .

3.3. CONFIGURING REPLICATION NAMING ALIASES USING THE WEB CONSOLE

To make the report more readable, you can set your own aliases that will be displayed in the report output. By default, the replication monitoring report contains the hostnames of servers.

Prerequisites

- The host is a member of replication topology.
- You initialized the consumers.
- You are logged in to the web console.

Procedure

1. Navigate to **Monitoring → Replication**. The **Replication Monitoring** page opens.
2. Click **Add Alias**.

3. Enter alias details:
    - **Alias**. An alias that will be displayed in the replication topology report.
    - **Hostname**. An instance hostname.
    - **Port**. An instance port.
4. Click **Save**.

Verification

- Generate the replication topology report to see If the report uses new aliases. For more information, see

Displaying a replication topology report using the web console .

CHAPTER 4. TRACKING THE BIND DN FOR PLUG-IN-INITIATED UPDATES

In Directory Server, you can track which user performed an action that caused a plug-in to update an entry. If the tracking is enabled and a plug-in changes an entry as a consequence of an action performed by a user, you can see the user's name in the **modifiersname** attribute of updated entry.

4.1. TRACKING USER INFORMATION FOR ENTRY MODIFICATIONS PERFORMED BY A PLUG-IN

When the user performs an action that changes an entry, it can trigger other, automatic changes across the directory tree. By default, Directory Server is not tracking the name of the user who performed the action that has initiated the data modification. To track the user information, you can use the **nsslapd-plugin-binddn-tracking** parameter.

For example, when the administrator deletes a user, the Referential Integrity Postoperation plug-in automatically removes the user from all groups. You can see the initial action in the entry as being performed by the user account bound to the server. But all related updates are, by default, shown as being performed by the plug-in, with no information about which user initiated the update.

A second example might be using the MemberOf plug-in to update user entries with group membership. The update to the group account is shown as being performed by the bound user, while the edit to the user entry is shown as being performed by the MemberOf plug-in:

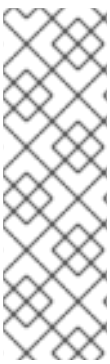
```
dn: cn=example_group,ou=groups,dc=example,dc=com
modifiersname: uid=example,ou=people,dc=example,dc=com

dn: uid=example,ou=people,dc=example,dc=com
modifiersname: cn=MemberOf Plugin,cn=plugins,cn=config
```

The **nsslapd-plugin-binddn-tracking** parameter enables the server to track which user originated an update operation, as well as the internal plug-in which actually performed the operation. The bound user is shown in the **modifiersname** and **creatorsname** operational attributes, while the plug-in which performed the update is shown in the **internalModifiersname** and **internalCreatorsname** operational attributes. For example:

```
dn: uid=example,ou=people,dc=example,dc=com
modifiersname: uid=admin,ou=people,dc=example,dc=com
internalModifiersname: cn=MemberOf Plugin,cn=plugins,cn=config
```

The **nsslapd-plugin-binddn-tracking** parameter tracks and maintains the relationship between the bound user and all updates performed for that connection.



NOTE

The **internalModifiersname** and **internalCreatorsname** attributes always show a plug-in as the identity. The value of the attribute is:

- **cn=ldbm database,cn=plugins,cn=config** when the core Directory Server performs the change
- **cn=*the DN of the plug-in*,cn=plugins,cn=config** when a plug-in changed the entry

4.2. ENABLING TRACKING THE BIND DN FOR PLUG-IN-INITIATED UPDATES USING THE COMMAND LINE

For data updates initiated by a plug-in, you often need to know which user has performed the action that led to the update. In the command line, set up the **nsslapd-plugin-binddn-tracking** parameter to track such user information.

Procedure

- Set the **nsslapd-plugin-binddn-tracking** parameter to **on**:

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace
nsslapd-plugin-binddn-tracking=on
```

Verification

- Display the **modifiersname** and **internalModifiersname** attributes of an entry that was changed by a plug-in. For example, if the **memberOf** attribute is enabled, display the attributes of a user after you added the user to a group:

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -x -b "uid=example-user,ou=People,dc=example,dc=com" -s base -x internalModifiersname -x modifiersname
dn: uid=example-user,ou=people,dc=example,dc=com
modifiersname: uid=admin,ou=people,dc=example,dc=com
internalModifiersname: cn=MemberOf Plugin,cn=plugins,cn=config
```

Additional resources

- Tracking user information for entry modifications performed by a plug-in

4.3. ENABLING TRACKING THE BIND DN FOR PLUG-IN-INITIATED UPDATES USING THE WEB CONSOLE

For data updates initiated by a plug-in, you often need to know which user has performed the action that led to the update. Using the web console, you can enable tracking of the user information.

Prerequisites

- You are logged in to the Directory Server instance in the web console.

Procedure

1. Open the **Server → Server Settings** menu.
2. On the **Advanced Settings** tab, select **Enable Plugin Bind DN Tracking**.
3. Click **Save**.

Verification

- Display the **modifiersname** and **internalModifiersname** attributes of an entry that was changed by a plug-in. For example, if the **memberOf** attribute is enabled, display the attributes of a user after you added the user to a group:

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -x -b "uid=example-user,ou=People,dc=example,dc=com" -s base -x internalModifiersname -x modifiersname
dn: uid=example-user,ou=people,dc=example,dc=com
modifiersname: uid=admin,ou=people,dc=example,dc=com
internalModifiersname: cn=MemberOf Plugin,cn=plugins,cn=config
```

Additional resources

- Tracking user information for entry modifications performed by a plug-in

CHAPTER 5. MONITORING THE DATABASE ACTIVITY

Administrators should monitor the database activity to ensure that tuning settings, such as caches, are properly configured.

5.1. MONITORING THE DATABASE ACTIVITY USING THE COMMAND LINE

To display the monitoring activity using the command line, display the dynamically-updated read-only attributes stored in the **cn=monitor,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config**.

Procedure

- To display the current activity of a database, enter:

  ```
  # dsconf -D "cn=Directory Manager" ldap://server.example.com monitor backend userRoot
  ```

  This command displays the activity of the **userRoot** database.

Additional resources

- Database monitoring attributes

5.2. MONITORING THE DATABASE ACTIVITY USING THE WEB CONSOLE

In the web console, Directory Server displays the values of the dynamically-updated read-only monitoring attributes from the **cn=monitor,cn=*database_name*,cn=ldbm database,cn=plugins,cn=config** in the `Monitoring´ tab.

Procedure

1. Navigate to **Monitoring → Database →** ***database name***.
2. Display the cache values on the **Entry Cache** and **DN Cache** tabs.

Additional resources

- Database monitoring attributes

5.3. DATABASE MONITORING ATTRIBUTES

Table 5.1. Inheritance settings

Attribute	Description
readonly	Indicates whether the database is in read-only mode (**1**) or in read-write mode (**0**).

Attribute	Description
entrycachehits	The total number of successful entry cache lookups. The value is the total number of times the server could retrieve an entry from the entry cache without reloading it from the database.
entrycachetries	The total number of entry cache lookups since you started the instance. The value is the total number, since the instance has been started, Directory Server tried to retrieve entry from the entry cache.
entrycachehitratio	The number of entry cache tries to successful entry cache lookups. This number is based on the total lookups and hits since you last started the instance. The closer the entry cache hit ratio is to 100%, the better. Whenever an operation attempts to find an entry that is not present in the entry cache, the server needs to access the database to obtain the entry. Thus, as this ratio drops towards zero, the number of disk accesses increases, and directory search performance decreases. To improve this ratio, increase the size of the entry cache of the database. To improve this ratio, increase the size of the entry cache by increasing the value of the **nsslapd-cachememsize** attribute in the **cn=*database_name*,cn=ldbm database,cn=plugins,cn=config** entry.
currententrycachesize	The total size, in bytes, of directory entries currently present in the entry cache. To increase the size of the entries which can be present in the cache, increase the value of the **nsslapd-cachememsize** attribute in the **cn=*database_name*,cn=ldbm database,cn=plugins,cn=config** entry.
maxentrycachesize	The maximum size, in bytes, of directory entries that Directory Server can maintain in the entry cache. To increase the size of the entries which can be present in the cache, increase the value of the **nsslapd-cachememsize** attribute in the **cn=*database_name*,cn=ldbm database,cn=plugins,cn=config** entry.
currententrycachecount	The current number of entries stored in the entry cache of a given backend.
maxentrycachecount	The maximum number of entries stored in the entry cache of a database. To tune this value, increase the value of the **nsslapd-cachesize** attribute in the **cn=*database_name*,cn=ldbm database,cn=plugins,cn=config** entry.

Attribute	Description
dncachehits	The number of times the server could process a request by obtaining a normalized distinguished name (DN) from the DN cache rather than normalizing it again.
dncachetries	The total number of DN cache accesses since you started the instance.
dncachehitratio	The ratio of cache tries to successful DN cache hits. The closer this value is to 100%, the better.
currentdncachesize	The total size, in bytes, of DN currently present in the DN cache. To increase the size of the entries which can be present in the DN cache, increase the value of the **nsslapd-dncachememsize** attribute in the **cn=*database_name*,cn=ldbm database,cn=plugins,cn=config** entry.
maxdncachesize	The maximum size, in bytes, of DNs that Directory Server can maintain in the DN cache. To increase the size of the entries which can be present in the cache, increase the value of the **nsslapd-dncachememsize** attribute in the **cn=*database_name*,cn=ldbm database,cn=plugins,cn=config** entry.
currentdncachecount	The number of DNs currently present in the DN cache.
maxdncachecount	The maximum number of DNs allowed in the DN cache.