



NetBrain® Integrated Edition 10.0

System Upgrade Guide

Distributed Deployment

1. Upgrading System.....	4
1.1. Terminating System Tasks	6
1.2. Stopping Server Services	6
1.3. Backing Up MongoDB Data.....	7
1.4. Upgrading MongoDB.....	9
1.5. Upgrading Elasticsearch	11
1.6. Upgrading License Agent.....	14
1.7. Upgrading Redis	16
1.7.1. Installing Redis on Linux.....	16
1.8. Upgrading RabbitMQ	21
1.8.1. Installing RabbitMQ on Linux.....	21
1.9. Upgrading Service Monitor Agent	27
1.9.1. Upgrading Service Monitor Agent on Linux	27
1.9.2. Upgrading Service Monitor Agent on Windows	29
1.10. Upgrading Web/Web API Server	31
1.11. Upgrading Worker Server.....	37
1.12. Upgrading Task Engine	43
1.13. Upgrading Front Server Controller.....	46
1.14. Upgrading Front Server	51
1.14.1. Upgrading Front Server on Linux	51
1.14.2. Upgrading Front Server on Windows	54
1.15. Unbinding Perpetual License	56
1.16. Activating Subscription License.....	57

1.17.	Verifying Upgrade Results.....	58
1.18.	Customizing MongoDB Disk Alert Rules	60
1.19.	Tuning Live Access	61
1.20.	Scheduling Benchmark Task.....	61
2.	Appendix: Editing a File with VI Editor	62
3.	Appendix: Offline Installing Third-party Dependencies.....	63
4.	Appendix: Restoring MongoDB Data	64
5.	Appendix: Dumping MongoDB Data	66
6.	Appendix: Interactive Pre-Installation of Service Monitor Agent.....	68

1. Upgrading System

The upgrade process ensures data integrity, which means that the data in the current system will be still available after upgrading. If you encounter any issues during the upgrade process, contact [NetBrain Support Team](#) for help.

Note: Before upgrading your system, check its current version and the network connectivity requirements.

Upgrade from IEv7.1x

1. [Terminate System Tasks](#)
2. [Stop Server Services](#)
3. [Back Up MongoDB Data](#)
4. [Upgrade MongoDB](#)
5. [Upgrade Elasticsearch](#)
6. [Upgrade License Agent](#)
7. [Upgrade Redis](#)
8. [Upgrade RabbitMQ](#)
9. [Upgrade Web/Web API Server](#)
10. [Upgrade Worker Server](#)
11. [Upgrade Task Engine](#)
12. [Upgrade Front Server Controller](#)
13. [Upgrade Front Server](#)
14. [Upgrade Service Monitor Agent](#)
15. [Unbind Perpetual License](#)
16. [Activate Subscription License](#)
17. [Verify Upgrade Results](#)
18. [Customize MongoDB Disk Alert Rules](#)
19. [Tune Live Access](#)
20. [Schedule Benchmark Task](#)

Network Connectivity Requirements

Source	Destination	Protocol *) and Port Number **)
Thin Client	Web Server Web API Server	HTTP/HTTPS (80/443)
Service Monitor Agent	Web API Server	HTTP/HTTPS (80/443)
Web API Server Worker Server Task Engine Front Server Controller	MongoDB	TCP 27017
Web API Server Worker Server	Elasticsearch	TCP (HTTP/HTTPS) 9200
Web API Server	License Agent	TCP 27654
Web API Server Worker Server Front Server Controller	Redis	TCP 6379
Web API Server Worker Server Task Engine Front Server Controller	RabbitMQ	TCP 5672
Worker Server Task Engine Front Server	Front Server Controller	TCP 9095
Front Server	Live Network	ICMP/SNMP/Telnet/SSH/REST API
Front Server	Ansible Agent (add-on)	TCP 9098
MongoDB License Agent Elasticsearch Redis RabbitMQ Web Server Worker Server Task Engine Front Server Front Server Controller	Web API Server	TCP 9099

Source	Destination	Protocol *) and Port Number **)
Web API Server	RabbitMQ	TCP 15672

Note: *) If SSL was enabled for any component including MongoDB/ElasticSearch/Redis/RabbitMQ/License Agent/Front Server Controller/Ansible Agent/Auto Update Server (within Web API Server), the SSL protocol should be added to firewall rules to enable SSL connection between servers.

Note: **) The port numbers listed in this column are defaults only. The actual port numbers used during installation might be different.

1.1. Terminating System Tasks

1. Log in to the System Management page.
2. In the System Management page, select **Operations > Task Manager** from the quick access toolbar.
3. Select all running tasks and click **End Process**.

1.2. Stopping Server Services

To avoid any further dataset changes or data corruption while reinstalling MongoDB/Elasticsearch binary files or restoring MongoDB/Elasticsearch data, stop the relevant services.

1. Log in to the Windows servers where NetBrain applications are installed and stop the following services in the Task Manager.

Tip: If you have deployed a Worker Server cluster or Web API Server cluster, stop the services on each node.

Note: If the system was upgraded from the versions older than 7.1, ensure the service named **proxyservice** no longer exists in the **Services** tab of **Task Manager**; otherwise follow the steps [here](#) to uninstall the Proxy Server before proceeding with the upgrade procedures.

NetBrain Component	Service Name
Web API Server	W3SVC
Web API Server	WAS

Worker Server	NetBrainWorkerServer
Front Server	NetBrainFrontServer
Task Engine	NetBrainTaskEngine
Front Server Controller	NetBrainFrontServerController
Redis	RedisMaster
RabbitMQ	RabbitMQ

2. Disable the **Cron** task on the MongoDB Server. The **Cron** task is used to automatically pull up the MongoDB service timely when it is down.

- 1) Log in to the Linux server where the MongoDB is installed as **root** user.
- 2) Open a command prompt and run the `crontab -e` command to edit the auto script.

```
[root@localhost ~]# crontab -e
```

```
*/1 * * * * /bin/bash -c 'if /usr/sbin/service mongod status|grep -q -E "(dead)|failed";
then /usr/sbin/service mongod start; fi' >/dev/null 2>&1
```

- 3) Add a pound sign **#** (highlighted) at the beginning of the auto script and save the changes. For how to edit the autoscript, see [Appendix: Editing a File with VI Editor](#) for more details.

```
#*/1 * * * * /bin/bash -c 'if /usr/sbin/service mongod status|grep -q -E "(dead)|failed";
then /usr/sbin/service mongod start; fi' >/dev/null 2>&1
```

1.3. Backing Up MongoDB Data

Before upgrading the system, it is highly recommended to back up all MongoDB data in case of any data loss or corruption during the upgrade process. The backup data will be used to restore data after MongoDB is reinstalled. See [Restoring MongoDB Data](#) for more details.

In case that you don't want to stop the service of MongoDB or the volume of the MongoDB data is small, you can refer to [Dumping MongoDB Data](#) for another way to back up the data and refer to [Restoring Dumped MongoDB Data](#) to restore the dumped data.

The following steps introduces how to use the `cp` command to copy underlying MongoDB data files directly for backup.

Notes:

- Make sure you have stopped [all relevant services](#) before backing up data.

- The backup data can only be used to restore the database on the same server.

1. Log in to the Linux server where the MongoDB node is installed as the **root** user.
2. Stop the service of MongoDB.

- 1) Run the `systemctl stop mongod` command to stop the MongoDB service.

Note: If you modified the MongoDB service name in the `install_mongodb.conf` file during the MongoDB installation, you must replace the service name accordingly.

- 2) Run the `ps -ef|grep mongod` command to verify whether the **mongod** process is stopped.

```
[root@localhost ~]# ps -ef| grep mongod
root      15136 14237  0 10:42 pts/2      00:00:00 grep --color=auto mongod
```

Note: If the **mongod** process is stopped, the result should only contain one entry as shown above.

3. Run the `mkdir /etc/mongodb_databk` command to create a directory under the **/etc** directory to save the backup data.

```
[root@localhost ~]# mkdir /etc/mongodb_databk
```

Note: Ensure the backup directory (**/etc/mongodb_databk** in this example) has sufficient space to store the backup data.

4. Run the `cd /opt/mongodb` command to navigate to the **/opt/mongodb** directory.

Note: If you modified the following default directory to store all MongoDB data files during the MongoDB installation, you must use the new directory (available in **mongod.conf**) accordingly.

5. Run the `du -hs data` command under the **/opt/mongodb** directory to check the total size of MongoDB backup data.
6. Run the `cp -a data /etc/mongodb_databk` command under the **/opt/mongodb** directory to copy all MongoDB data files from the **data** directory to the **/etc/mongodb_databk** directory.

```
[root@localhost mongodb]# cp -a data /etc/mongodb_databk
```

7. Run the `cd /etc/mongodb_databk` command to navigate to the **/etc/mongodb_databk** directory.
8. Run the `ls -al` command under the **/etc/mongodb_databk** directory to browse the backup data.

```
[root@localhost mongodb_databk]# ls -al
total 136
drwxr-xr-x.  3 root root      18 Jun 6 22:49 .
```



```
drwxr-xr-x. 6 root root          79 Jun 6 22:48 ..
drwxr-xr-x. 4 netbrain netbrain 106496 Jun 6 22:49 data
```

9. Run the `systemctl start mongod` command to start the MongoDB service.

Note: If you modified the MongoDB service name in the `install_mongodb.conf` file during the MongoDB installation, you must replace the service name accordingly.

1.4. Upgrading MongoDB

Pre-Upgrade Task

- Service Monitor Agent will be installed or upgraded with MongoDB and it has dependencies on the third-party package **libffi-devel zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa|grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel|gcc"` command to check whether it has been installed on this Linux server. If it has not been installed yet, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install them online
 - **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Ensure you have upgraded the Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit, CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9/8.2/8.3, 64-bit** to avoid installation or upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, do not restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

Upgrading MongoDB

1. Log in to the Linux server as the **root** user.

Note: It is highly recommended to install **numactl** on the Linux Server to optimize MongoDB performance. Run the `rpm -qa|grep numactl` command to check whether **numactl** has already been installed. If it has not been installed yet and the Linux server has access to the Internet, run the `yum install numactl` command to install it online.

2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp10.0**.

Note: Don't place the installation package under any personal directories, such as **/root**.

3. Run the `cd /opt/netbraintemp10.0` command to navigate to the **/opt/netbraintemp10.0** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **mongodb-linux-x86_64-rhel-4.0.19-10.0.tar.gz** file from NetBrain and upload it to the **/opt/netbraintemp10.0** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.0** directory to directly download the **mongodb-linux-x86_64-rhel-4.0.19-10.0.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf mongodb-linux-x86_64-rhel-4.0.19-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

```
[root@centos netbraintemp10.0]# tar -zxvf mongodb-linux-x86_64-rhel-4.0.19-10.0.tar.gz
MongoDB/
MongoDB/config/
...
MongoDB/upgrade/upgrade_single_node/upgrade.sh
...
```

6. Run the `cd MongoDB/upgrade/upgrade_single_node` command to navigate to the **MongoDB/upgrade/upgrade_single_node** directory.
7. Run the `systemctl start mongod` command to restart the MongoDB service.
8. Run the `./upgrade.sh` command under the **upgrade_single_node** directory and enter the MongoDB user name/password with the interactive command line.

```
[root@localhost upgrade_single_node]# ./upgrade.sh
INFO: 2021-02-28 13:57-08.135: Starting to check if rpm exists.
Getting rpm dependency list of MongoDB and Service Monitor Agent...
INFO: 2021-02-28 13:57-17.185: Starting to upgrade Service Monitor Agent ...
...
The service of mongod is running.
Please enter the MongoDB username: mongodb
Please enter the MongoDB password:
Successfully connected to MongoDB.
```

```
...  
INFO: 2021-02-28 14-10-31.570: Upgrading MongoDB SUCCEEDED.
```

Note: Ensure MongoDB service is up and running before executing the `./upgrade.sh` command.

Note: If the default username and password were changed during the installation of MongoDB, you must enter these customized values during the upgrade.

Note: Before upgrading this component, Service Monitor Agent will be upgraded to the latest version. The entire process does not require any user inputs.

Note: If the Service Monitor Agent was not previously installed, you'll need to use the interactive command line to install it. See [Appendix: Interactive Pre-Installation of Service Monitor Agent](#) for more details.

9. After the MongoDB Server is successfully upgraded, run the `systemctl status mongod` command to check its service status.

```
[root@localhost ~]# systemctl status mongod  
mongod.service - MongoDB service  
Loaded: loaded (/usr/lib/systemd/system/mongod.service; enabled; vendor preset: disabled)  
Active: active (running) since Thu 2020-07-16 10:15:52 EDT; 56s ago  
Process: 18325 ExecStop=/usr/bin/pkill mongod (code=exited, status=0/SUCCESS)  
Process: 18373 ExecStart=/bin/mongod -f /etc/mongodb/mongod.conf (code=exited,  
status=0/SUCCESS)  
Main PID: 18382 (mongod)  
Memory: 213.6M (limit: 6.8G)  
...
```

Tip: It is highly recommended to run the `rm -rf /opt/netbraintemp10.0/MongoDB/config/setup.conf` command to delete the **setup.conf** file from the server after MongoDB is successfully upgraded because the file may cause security vulnerability.

1.5. Upgrading Elasticsearch

Pre-Upgrade Task

- Service Monitor Agent will be installed or upgraded with Elasticsearch and it has dependencies on the third-party package **libffi-devel zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa | grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel|gcc"` command to check whether it has been installed on this Linux server. If it has not been installed yet, you can choose either option below to install the dependencies:

- **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install them online
- **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Ensure you have upgraded the Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit**, **CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9/8.2/8.3, 64-bit** to avoid installation or upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, do not restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

Upgrading Elasticsearch

1. Log in to the Linux server as the **root** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp10.0**.
3. Run the `cd /opt/netbraintemp10.0` command to navigate to the **/opt/netbraintemp10.0** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **elasticsearch-linux-x86_64-rhel-6.8.12-10.0.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.0** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.0** directory to directly download the **elasticsearch-linux-x86_64-rhel-6.8.12-10.0.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf elasticsearch-linux-x86_64-rhel-6.8.12-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

```
[root@centos netbraintemp10.0]# tar -zxvf elasticsearch-linux-x86_64-rhel-6.8.12-10.0.tar.gz
Elasticsearch/
Elasticsearch/config/
...
Elasticsearch/upgrade.sh
```

6. Run the `cd Elasticsearch` command to navigate to the **Elasticsearch** directory.

7. Run the `./upgrade.sh` command under the **Elasticsearch** directory.

Note: If the default username and password were changed during the installation of Elasticsearch, you must enter these customized values during the upgrade.

Note: Before upgrading this component, Service Monitor Agent will be upgraded to the latest version. The entire process does not require any user inputs.

Note: If the Service Monitor Agent was not previously installed, you'll need to use the interactive command line to install it. See [Appendix: Interactive Pre-Installation of Service Monitor Agent](#) for more details.

8. After the Elasticsearch is successfully upgraded, run the `systemctl status elasticsearch` command to check its service status.

```
[root@localhost ~]# systemctl status elasticsearch
elasticsearch.service - Elasticsearch
Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
Active: active (running) since Thu 2020-07-16 10:23:46 EDT; 230ms ago
Docs: http://www.elastic.co
Main PID: 22168 (elasticsearch)
Memory: 4.6G
...
```

9. Run the `curl -s -XGET --user <username:password> http://<IP address>:<port>` command to check the current version of Elasticsearch.

Note: If you enabled SSL, replace `http` with `https`.

Example:

```
[root@localhost Elasticsearch]# curl -s -XGET --user admin:admin http://10.10.3.142:9200
{
  "name" : "node1",
  "cluster_name" : "elastic-search-cluster",
  "cluster_uuid" : "OctFIL44T--5mArFA93r-A",
  "version" : {
    "number" : "6.8.12",
    "build_flavor" : "oss",
    "build_type" : "rpm",
    "build_hash" : "8f0685b",
    "build_date" : "2020-07-16T18:41:22.859Z",
    "build_snapshot" : false,
    "lucene_version" : "7.7.3",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Tip: It is highly recommended to run the `rm -rf /opt/netbraintemp10.0/Elasticsearch/config/setup.conf` command to delete the **setup.conf** file from the server after Elasticsearch is successfully upgraded because the file may cause security vulnerability.

1.6. Upgrading License Agent

Pre-Upgrade Task

- Service Monitor Agent will be installed or upgraded with License Agent and it has dependencies on the third-party package **libffi-devel zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa|grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel|gcc"` command to check whether it has been installed on this Linux server. If it has not been installed yet, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install them online
 - **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Ensure you have upgraded the Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit, CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9/8.2/8.3, 64-bit** to avoid installation or upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, do not restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

Upgrading License Agent

1. Log in to the Linux server as the **root** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp10.0**.
3. Run the `cd /opt/netbraintemp10.0` command to navigate to the **/opt/netbraintemp10.0** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **netbrain-licenseagent-linux-x86_64-rhel-10.0.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.0** directory by using a file transfer tool.

- **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.0** directory to directly download the file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf netbrain-licenseagent-linux-x86_64-rhel-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

```
[root@localhost netbraintemp10.0]# tar -zxvf netbrain-licenseagent-linux-x86_64-rhel-10.0.tar.gz
License/
...
License/upgrade.sh
```

6. Run the `cd License` command to navigate to the **License** directory.
7. Run the `./upgrade.sh` command under the **License** directory.

Note: Before upgrading this component, Service Monitor Agent will be upgraded to the latest version. The entire process does not require any user inputs.

Note: If the Service Monitor Agent was not previously installed, you'll need to use the interactive command line to install it. See [Appendix: Interactive Pre-Installation of Service Monitor Agent](#) for more details.

- 1) Read the license agreement, and then type **YES** and press the **Enter** key.
- 2) Type **I ACCEPT** and press the **Enter** key to accept the license agreement. The script starts to check whether the system configuration of the Linux server meets the requirement, and all required dependent packages are installed for License Agent.

```
[root@localhost License]# ./upgrade.sh

Please read the End User License Agreement ("EULA") for the license type (perpetual or
subscription)
purchased in the order form at https://www.netbraintech.com/legal-tc/ carefully. I have read
the
subscription EULA, if I have purchased a subscription license, or the perpetual EULA, if I
have
purchased a perpetual license, at the link provided above. Please type "YES" if you have read
the
applicable EULA and understand its and understand its contents, or "NO" if you have not read
the
applicable EULA. [YES/NO]: YES

Do you accept the terms in the subscription EULA, if you have purchased a subscription
license, or
```

```
the perpetual EULA, if you have purchased a perpetual license? If you accept, and to continue with the installation, please type "I Accept" to continue. If you do not accept, and to quit the installation script, please type "CANCEL" to stop. [I ACCEPT/CANCEL]: I ACCEPT
INFO: Creating upgrading log...
INFO: Dependent Package:
INFO: Component Name: License Agent
INFO: RPM name: netbrainlicense
INFO: Starting to check system
...
INFO: Successfully installed License Agent. Service is running.
INFO: Backing up uninstall.sh SUCCEEDED.
INFO: Upgrading License Agent SUCCEEDED.
```

8. After the License Agent is successfully upgraded, run the `systemctl status netbrainlicense` command to check its service status.

```
[root@localhost ~]# systemctl status netbrainlicense
netbrainlicense.service - NetBrain license agent service
Loaded: loaded (/usr/lib/systemd/system/netbrainlicense.service; enabled; vendor preset: disabled)
Active: active (running) since Thu 2020-07-16 10:32:04 EDT; 218ms ago
Main PID: 27328 (licensed)
CGroup: /system.slice/netbrainlicense.service
        └─ 27328 /usr/bin/netbrainlicense/licensed -f
/etc/netbrain/netbrainlicense/licensed.conf
```

1.7. Upgrading Redis

Complete the following steps to upgrade Redis:

1. [Installing Redis on Linux](#)
2. [Uninstalling Redis on Windows](#)

1.7.1. Installing Redis on Linux

Pre-installation Task

- Ensure you have upgraded the Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit, CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9/8.2/8.3, 64-bit** to avoid installation or upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, do not restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

Installing Redis on Linux

1. Log in to the Linux server as the **root** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp10.0**.
3. Run the `cd /opt/netbraintemp10.0` command to navigate to the **/opt/netbraintemp10.0** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **redis-linux-x86_64-rhel-6.0.9-10.0.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.0** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.0** directory to directly download the **redis-linux-x86_64-rhel-6.0.9-10.0.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf redis-linux-x86_64-rhel-6.0.9-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

```
[root@localhost netbraintemp10.0]# tar -zxvf redis-linux-x86_64-rhel-6.0.9-10.0.tar.gz
redis/
redis/sources/
...
redis/include/source.sh
...
redis/config/setup.conf
...
```

6. Run the `cd redis/config` command to navigate to the **config** directory.
7. Modify the [parameters](#) in the **setup.conf** file located under the **config** directory and save the changes. For how to modify the configuration file, refer to [Editing a File with VI Editor](#).

```
[root@localhost config]# vi setup.conf
#Redis configuration file
```

```

#Note: Entries other than the password
can only contain letters or numbers, and should start with a letter.

#Account info.
#Password should not contain: {}[]:","|<>@&^%\\ or a space. The password should be the same
in all nodes if the mode is a cluster.
Password=Admin1.#

# Mode use 'standalone' if single installation, use 'cluster' if HA mode
Mode=standalone

# Port is used to start the redis service on specified port. We use default port 6379.
# Please enter the same Port for all nodes that belong to the same cluster
Port=6379

# Data Path is used to store redis files. Default path /var/lib/redis.
DataPath=/var/lib/redis

# Log Path is used to store redis log files. Default path /var/log/redis.
LogPath=/var/log/redis

# Role (NodeRole can only be 'master', 'slave' 'sentinel' or 'dr-sentinel')
# sentinel - start the redis in sentinel mode so that it can monitor a cluster
# dr-sentinel - start the redis in sentinel mode so that it can monitor a DR cluster for a
multi-DC on same node where you have redis already installed

NodeRole=master
#Master Node (Master Node can support ip address, hostname or FQDN and is used if the Mode is
cluster)
MasterNode=
# Sentinel Port is used to start the redis sentinel service on specified port. We use default
port 6380.
# For a multi-DC DR cluster there will be 2 instances of sentinel on same arbiter node so user
should change this value to default port 6381
or any other port which is not used by other service.
# Please enter the same sentinelPort for all nodes that belong to the same cluster
SentinelPort=6380

# Resource limitation. It can only be 'yes' or 'no'
ResourceLimit=no
# CPU Limit. It should end with %. Range is 1% to 100%
CPULimit=100%
#Memory Limit. It should end with %. Range is 1% to 100%
MememoryLimit=100%

# TLS. It can only be 'yes' or 'no'
UseSSL=no
Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem
CertAuth=/etc/ssl/cacert.pem

```

8. Run the `cd ..` command to navigate to the **redis** directory.
9. Run the `./install.sh` script under the **redis** directory to install Redis.

```
[root@localhost redis]# ./install.sh
INFO: Checking root
INFO: Checking date
INFO: Starting to check Linux OS info
INFO: Starting to check required CPU
INFO: Starting to check minimum memory
INFO: Creating installation log file SUCCEEDED
INFO: Starting to check crontab
INFO: Component Name: Redis
INFO: RPM name: redis
INFO: Service name: redis
INFO: RPM package list: redis-6.0.9-1.x86_64.rpm
INFO: Config path: /etc/redis
INFO: Preprocessing SUCCEEDED
INFO: Starting to check system
INFO: Collecting system information SUCCEEDED.
INFO: Starting to check if rpm exists
INFO: Starting to check systemd
INFO: System checking SUCCEEDED
...
redis.service - Redis
  Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2020-07-14 00:38:49 EST; 37min ago
  Main PID: 36704 (redis-server)
  Memory: 1.2M
  CGroup: /system.slice/redis.service
          56299 /sbin/redis-server *:6379
...
INFO: Checking redis Status
INFO: Verification SUCCEEDED
INFO: Backup uninstall.sh SUCCEEDED
INFO: Backup fix_releaseinfo.json SUCCEEDED
INFO: Successfully installed Redis
```

10. Run the `systemctl status redis` command to verify whether its service starts successfully.

```
[root@localhost ~]# systemctl status redis
redis.service - Redis
  Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2020-07-13 15:47:04 EDT; 10min ago
  Main PID: 52318 (redis-server)
  Memory: 7.7M
  ...
```

Note: When your disk space is insufficient for large amounts of logs, you can modify the log settings in the **redis.conf** file under the **/etc/logrotate** directory.


Parameters

The following table describes the parameters that can be configured when installing Redis.

Parameter	Default Value	Description
Password	<code>Admin1.#</code>	Specify the admin password used to connect to Redis. Note: The password cannot contain any of the following special characters, and its length cannot exceed 64 characters. <code>{ } [] : " , ' < > @ & ^ % \</code> and spaces
Mode	<code>standalone</code>	Set whether to enable cluster deployment. Keep the default value for a standalone deployment.
Port	<code>6379</code>	Specify the port number that the master Redis node listens to.
DataPath	<code>/var/lib/redis/</code>	Specify the storage path for all data files of Redis.
LogPath	<code>/var/log/redis/</code>	Specify the storage path for all log files of Redis.
NodeRole	<code>master</code>	Set the role for the current node. Available options are master , slave , sentinel and dr-sentinel . Keep the default value for a standalone deployment.
MasterNode		This parameter is only required for cluster deployments.
SentinelPort	<code>6380</code>	The port number that the sentinel or dr-sentinel node listens to. Note: Use alternative port such as 6381 when deploying the dr-sentinel node.
ResourceLimit	<code>no</code>	Set whether to limit the system resource usage for Redis.
CPULimit	<code>100%</code>	The maximum CPU utilization of the machine that can be consumed by Redis.
MemoryLimit	<code>100%</code>	The maximum memory capacity of the machine that can be consumed by Redis.
UseSSL	<code>no</code>	Set whether to enable the encrypted connections to Redis by using SSL. Note: Redis itself does not support SSL. It uses stunnel as an SSL service agent. Stunnel will be automatically installed together with Redis.
Certificate	<code>/etc/ssl/cert.pem</code>	Specify the storage path for all the certificates and key files used for SSL authentication. Note: It is required only if UseSSL is enabled.
PrivateKey	<code>/etc/ssl/key.pem</code>	Specify the name of SSL private key file. Note: It is required only if UseSSL is enabled.
CertAuth	<code>/etc/ssl/cacert.pem</code>	Specify the name of the SSL certificate chain or intermediate certificate (class 2 or class 3 certificate). Note: It is required only if UseSSL is enabled.

1.7.1.1. Uninstalling Redis on Windows

Complete the following steps with administrative privileges. Take Windows Server 2012 R2 for example.

1. Click the Windows start menu, and then click the  icon to open the **Apps** pane.
2. Right-click the **Uninstall Redis (Cache) Server** app in the pane, and then select **Run as administrator** from the list to launch the Installation Wizard.
3. Click **Yes** when a confirmation dialog box pops up.
4. Select the **Delete all existing user data** check box to delete all registry information and files under its installation path, and click **Next**.
5. Click **Finish** to exit the Installation Wizard.

1.8. Upgrading RabbitMQ

Complete the following steps to upgrade RabbitMQ:

1. [Installing RabbitMQ on Linux](#)
2. [Uninstalling RabbitMQ on Windows](#)

1.8.1.Installing RabbitMQ on Linux

Pre-Installation Task

- Ensure you have upgraded the Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit**, **CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9/8.2/8.3, 64-bit** to avoid installation or upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, do not restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

- Ensure the hostname of the Linux server must be resolvable by DNS or configured in **/etc/hosts** because RabbitMQ needs a resolvable hostname no matter whether it is a standalone server or a cluster.
- RabbitMQ has dependencies on the third-party package **socat** and **logrotate**. Before you install the RabbitMQ, run the `rpm -qa|grep socat` and `rpm -qa|grep logrotate` commands to check whether they have been installed on the server. If they have not been installed yet, you can choose either option below to install the dependencies.
 - **Online Install:** run the `yum -y install socat` and `yum -y install logrotate` commands to install them online.
 - **Offline Install:** refer to [Offline Installing Third-party Dependencies](#) for more details.
- RabbitMQ has dependencies on the third-party package openssl (1.0.2k and above) and selinux-policy-target (3.13.1 and above). Before you install the RabbitMQ, run the `rpm -qa|grep openssl` and `rpm -qa|grep selinux-policy-target` commands to check their version info. If the version number is less than the required one, you can run the `yum -y upgrade openssl` and `yum -y upgrade selinux-policy-target` commands to upgrade them online.

Note: If the Service Monitor Agent was not previously installed, it will be installed with RabbitMQ. You'll need to use the interactive command line to install it. See Installing MongoDB on Linux for more details. You can also install the Service Monitor Agent separately before installing RabbitMQ.

Installing RabbitMQ on Linux

1. Log in to the Linux server as the **root** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp10.0**.
3. Run the `cd /opt/netbraintemp10.0` command to navigate to the **/opt/netbraintemp10.0** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **rabbitmq-linux-x86_64-rhel-3.8.9-10.0.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.0** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.0** directory to directly download the **rabbitmq-linux-x86_64-rhel-3.8.9-10.0.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf rabbitmq-linux-x86_64-rhel-3.8.9-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

```
[root@localhost netbraintemp10.0]# tar -zxvf rabbitmq-linux-x86_64-rhel-3.8.9-10.0.tar.gz
rabbitmq/
rabbitmq/config/
rabbitmq/config/setup.conf
...
rabbitmq/install.sh
..
```

6. Run the `cd rabbitmq/config` command to navigate to the **config** directory.
7. Modify the **parameters** in the **setup.conf** file and save the changes. For how to modify the configuration file, refer to [Editing a File with VI Editor](#).

```
[root@centos config]# vi setup.conf
#RabbitMQ configuration file

#Account info
#The UserName or Password should not contain: {}[]:","|<>@&^%\ or a space
#The length of UserName or Password should not be more than 64 characters
UserName=admin
Password=Admin1.#

# Mode (Mode can only be 'mirror' or 'standalone')
Mode=standalone

# A unique cluster string is used to join all cluster nodes. Each cluster node must have the
same cluster ID.
ClusterId=rabbitmqcluster

# The role of the current node in the cluster. One or two roles can be configured:
# master or slave.
NodeRole=master
# Must specify a resolvable hostname of the master node in either standalone or mirror mode.
MasterNode=localhost

# Resource limitation
ResourceLimit=no

# CPULimit and MemoryLimit should be ended by % and the range is from 1% to 100%
CPULimit=100%
MemoryLimit=100%

# TLS
UseSSL=no
```

```

Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem

# Port --Please enter the same Port for all nodes that belong to the same cluster
Port=5672

# Log path
LogPath=/var/log/rabbitmq

```

8. Run the `cd ..` command to navigate to the **rabbitmq** directory.

9. Run the `./install.sh` script under the **rabbitmq** directory to install RabbitMQ.

```

[root@localhost rabbitmq]# ./install.sh
INFO: Start checking date
INFO: Start checking os
INFO: Start checking required CPU
INFO: Start checking minimum memory
INFO: Selinux-policy version: 3.13.1
INFO: Component Name: RabbitMQ
INFO: RPM name: rabbitmq-server
INFO: Service name: rabbitmq-server
INFO: RPM package list: erlang-23.2.1-1.el7.x86_64.rpm rabbitmq-server-3.8.9-1.el7.noarch.rpm
INFO: Installation path: /usr/lib/rabbitmq/
INFO: Config path: /etc/rabbitmq/
INFO: Preprocessing SUCCEEDED
...
Preparing... #####
Updating / installing...
rabbitmq-server-3.8.1-1.el7 #####
INFO: Official rpm package installing SUCCEEDED
INFO: Configuration parameters updating SUCCEEDED
INFO: Permission setting SUCCEEDED
Created symlink from /etc/systemd/system/multi-user.target.wants/rabbitmq-server.service to
/usr/lib/systemd/system/rabbitmq-server.service.
rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset:
disabled)
   Active: active (running) since Mon 2020-07-13 16:04:46 EDT; 8ms ago
 Main PID: 53927 (beam.smp)
   Status: "Initialized"
  Memory: 70.8M (limit: 15.5G)
...
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed RabbitMQ

```

10. Run the `systemctl status rabbitmq-server` command to verify whether its service starts successfully.

```

[root@localhost ~]# systemctl status rabbitmq-server
rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset:
disabled)
   Active: active (running) since Mon 2020-07-13 16:05:23 EDT; 13min ago
     Process: 19522 ExecStop=/usr/sbin/rabbitmqctl shutdown (code=exited, status=0/SUCCESS)
    Main PID: 4509 (beam.smp)

```



```
Status: "Initialized"
Memory: 96.5M
...
```

Parameters

The following table describes the parameters that can be configured when installing RabbitMQ.


Parameter	Default Value	Description
Username	admin	Specify the admin username used to connect to RabbitMQ. Note: The username and password cannot contain any of the following special characters, and its length cannot exceed 64 characters. { } [] : " , ' < > @ & ^ % \ and spaces
Password	Admin1.#	Specify the admin password used to connect to RabbitMQ.
Mode	standalone	Set the RabbitMQ deployment Mode. Available options are standalone or mirror . Keep the default value standalone for a standalone deployment.
ClusterId	rabbitmqcluster	Specify the cluster id used by all nodes to join the cluster. This parameter is required only for cluster deployments.
NodeRole	master	Set the role for the current node. Available options are master or slave . Keep the default value for a standalone deployment.
MasterNode	localhost	This parameter is required for both standalone and cluster deployments. For standalone Mode, this parameter should be set as a resolvable hostname of the local server.
ResourceLimit	no	Set whether to limit the system resource usage for RabbitMQ.
CPULimit	100%	Specify the maximum CPU utilization of the machine that can be consumed by RabbitMQ.
MemoryLimit	100%	Specify the maximum memory capacity of the machine that can be consumed by RabbitMQ.
UseSSL	no	Set whether to enable the encrypted connections to RabbitMQ by using SSL. Tip: If UseSSL is set to yes , you can follow the steps below to modify the RabbitMQ Plugin config file after the service monitor is installed. 1) Run the <code>vi /etc/netbrain/nbagent/check/rabbitmq.yaml</code> command to open the RabbitMQ Plugin config file. 2) Set the ssl value to true and save the changes. For how to modify the configuration file, see Editing a File with VI Editor for more details.

Parameter	Default Value	Description
		<pre>[root@localhost check]# vi rabbitmq.yaml init_config: instances: - name: default managementPort: 15672, checkAvailableIntervalSeconds: 300 ssl: true collectQueues: equal: [] startWith: ['FullTextSearch', 'TaskManager', 'event_callback', 'RMClientCallbac k', 'ETL_Task'] endWith: ['IndexDriver']</pre>
Certificate	/etc/ssl/cert.pem	Specify the storage path for all the certificates and key files used for SSL authentication. Note: It is required only if UseSSL is enabled.
PrivateKey	/etc/ssl/key.pem	Specify the name of SSL private key file. Note: It is required only if UseSSL is enabled.
Port	5672	Specify the port number that RabbitMQ service listens to.
LogPath	/var/log/rabbitmq	Specify the directory to save logs of RabbitMQ.

1.8.1.1. Uninstalling RabbitMQ on Windows

Complete the following steps with administrative privileges.

Take Windows Server 2012 R2 for example:

1. Click the Windows start menu and then click the  icon to open the **Apps** pane.
2. Right-click the **Uninstall RabbitMQ (Message) Server** app in the pane, and then select **Run as administrator** from the drop-down list to launch the Installation Wizard.
3. Click **Yes** when a confirmation dialog box pops up.
4. Select the **Delete all existing user data** check box to delete all registry information and files under its installation path and click **Next**.
5. Click **Finish** to exit the Installation Wizard.

1.9. Upgrading Service Monitor Agent

Select either of the following ways to upgrade your Service Monitor Agent, depending on the operating system:

- [Upgrading Service Monitor Agent on Linux](#)
- [Upgrading Service Monitor Agent on Windows](#)

1.9.1. Upgrading Service Monitor Agent on Linux

Pre-Upgrade Tasks

- Ensure you have upgraded the Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit**, **CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9/8.2/8.3, 64-bit** to avoid installation or upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, do not restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

- Service Monitor Agent has dependencies on the third-party package on **zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa | grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel gcc"` command to check whether **zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc** has been installed on this Linux server. If it has not been installed, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install it online.
 - **Offline Install:** see [Appendix](#) for more details.

Upgrading Service Monitor Agent on Linux

1. Log in to the Linux server as the **root** user.
2. Run the `cd /opt/netbraintemp10.0` command to navigate to the **/opt/netbraintemp10.0** directory.
3. Download the installation package.

- **Option 1:** If the Linux server has no access to the Internet, obtain the **netbrain-servicemonitoragent-linux-x86_64-rhel-10.0.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.0** directory by using a file transfer tool.
- **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.0** directory to directly download the **netbrain-servicemonitoragent-linux-x86_64-rhel-10.0.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

4. Run the `tar -zxvf netbrain-servicemonitoragent-linux-x86_64-rhel-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

```
[root@localhost netbraintemp10.0]# tar -zxvf netbrain-servicemonitoragent-linux-x86_64-rhel-10.0.tar.gz
ServiceMonitorAgent/
ServiceMonitorAgent/config/
ServiceMonitorAgent/config/setup.conf
...
ServiceMonitorAgent/upgrade.sh
ServiceMonitorAgent/fix_releaseinfo.json
```

5. Run the `cd ServiceMonitorAgent` command to navigate to the **ServiceMonitorAgent** directory.
6. Run the `./upgrade.sh` script under the **ServiceMonitorAgent** directory to upgrade the Service Monitor Agent.
 - 1) Read the License Agreement, and type **YES**.
 - 2) Type **I ACCEPT** to accept the License Agreement. The script starts to install Service Monitor Agent.

```
[root@localhost ServiceMonitorAgent]# ./upgrade.sh

Please read the End User License Agreement ("EULA") for the license type (perpetual or
subscription) purchased in the order form at
https://www.netbraintech.com/legal-tc/ carefully. I have read the subscription EULA, if I
have purchased a subscription license, or the
perpetual EULA, if I have purchased a perpetual license, at the link provided above. Please
type "YES" if you have read the applicable EULA
and understand its contents, or "NO" if you have not read the applicable EULA. [YES/NO]: YES

Do you accept the terms in the subscription EULA, if you have purchased a subscription
license, or the perpetual EULA, if you have purchased
a perpetual license? If you accept, and to continue with the installation, please type "I
Accept" to continue. If you do not accept, and to quit
the installation script, please type "CANCEL" to stop. [I ACCEPT/CANCEL]: I ACCEPT
INFO: Creating upgrading log file SUCCEEDED
INFO: Collecting system information SUCCEEDED.
INFO: Starting to get previous installation parameters.
...
INFO: Configuration parameters checking SUCCEEDED.
```

```
INFO: Start to install service monitor...
...
Successfully upgraded Service Monitor Agent. Service is running.
```

7. Run the `systemctl status netbrainagent` command to verify whether its service starts successfully.

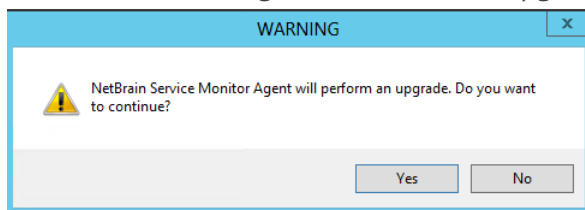
```
[root@localhost ~]# systemctl status netbrainagent
netbrainagent.service - NetBrain Service Monitor Agent Daemon
Loaded: loaded (/usr/lib/systemd/system/netbrainagent.service; enabled; vendor preset:
disabled)
Active: active (running) since Tue 2020-07-14 13:36:28 EDT; 71ms ago
Main PID: 4520 (python3)
Memory: 73.5M
...
```

8. Repeat the above steps to upgrade the Service Monitor Agent on more Linux servers.

1.9.2. Upgrading Service Monitor Agent on Windows

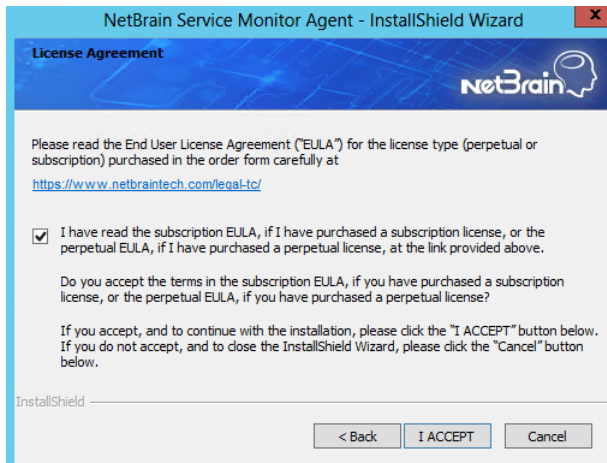
Complete the following steps with administrative privileges.

1. Download the **netbrain-servicemonitoragent-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-servicemonitoragent-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-servicemonitoragent-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) Click **Yes** in the dialog box to initiate the upgrade.

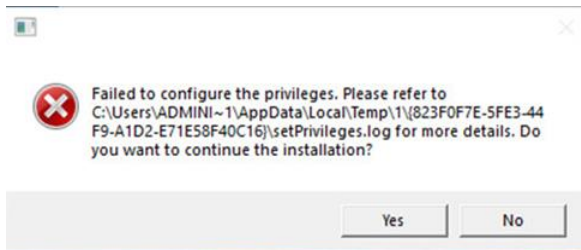


- 2) On the Welcome page, click **Next**.
- 3) On the System Configuration page, review the system configuration summary and click **Next**.

- 4) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



- 5) Review the summary of the installation information and click **Install**.
- 6) (Optional) Ensure the NetBrain installation process using administrator account has the necessary permissions to modify “User Rights Assignment” in “Local Security Policy” or change the local user privileges. Otherwise, the following error message will prompt when installing each Windows component.



Click **Yes** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System. If you have security concerns, please click **No** to abort the installation/upgrade.

Note: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.

Note: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

4. After successfully upgrading the Service Monitor Agent, click **Finish**.

Tip: You can open the Task Manager and navigate to the **Services** panel to check whether **NetBrainAgent** is running.

5. Repeat the above steps to upgrade the Service Monitor Agent on more Windows servers.

1.10. Upgrading Web/Web API Server

Note: Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

Note: It is not allowed to upgrade any Worker Server and Web API Server at the same time. Otherwise, it will cause DB data initializing failure.

Note: Service Monitor Agent needs to be installed prior to installing Web/Web API Server. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

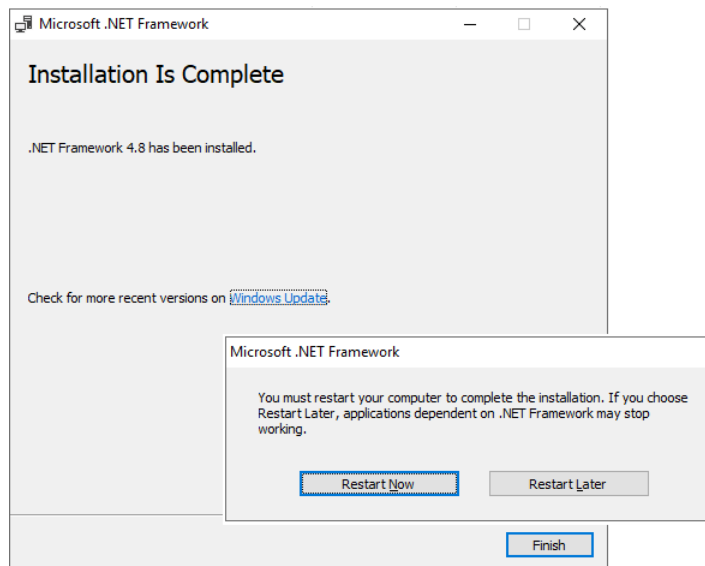
Complete the following steps to upgrade Web API Server and Web Server on the same machine with administrative privileges.

1. Download the **netbrain-ie-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to start the Installation Wizard.
4. Follow the Installation Wizard to complete the upgrade step by step:
 - 1) If **.NET Framework 4.8** has not been pre-installed on this machine, the Installation Wizard will guide you through the installation of **.NET Framework 4.8** first.

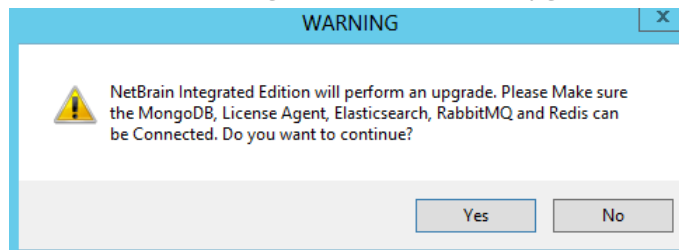
Note: Make sure the Windows update is of the latest. For Windows Server 2012, the update **KB2919442** and **KB2919355** must be installed before the .NET Framework 4.8 installation can start.

Note: Some running applications must be closed during the installation of .NET Framework 4.8, such as Server Manager.

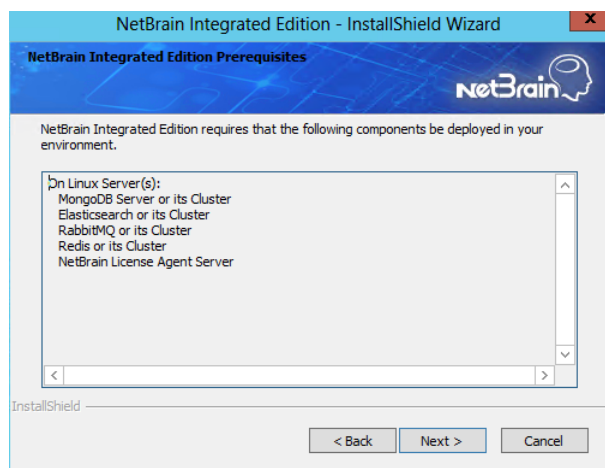
Note: After .NET Framework 4.8 is successfully installed, you must click **Restart** to restart the machine immediately. Otherwise, the upgrade will fail due to the failure of upgrading the new .Net Framework. After the machine reboots, ensure the FIPS is disabled after restarting the machine. To disable the FIPS setting, modify the **Enabled** value to **0** under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy** directory of Windows registry.



- 2) Stop the services of Web/Web API server manually before continuing the upgrade.
- 3) Click **Yes** in the dialog box to initiate the upgrade.

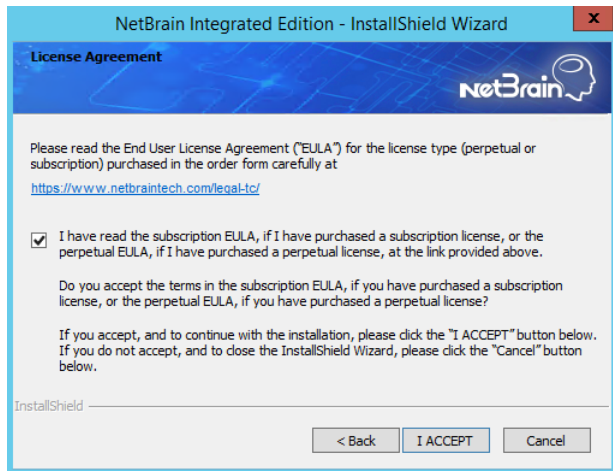


- 4) On the Welcome page, click **Next**.
- 5) On the NetBrain Integrated Edition Prerequisites page, read the components that must be set up in your environment beforehand and click **Next**.



- 6) On the System Configuration page, review the system configuration summary and click **Next**.

- 7) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



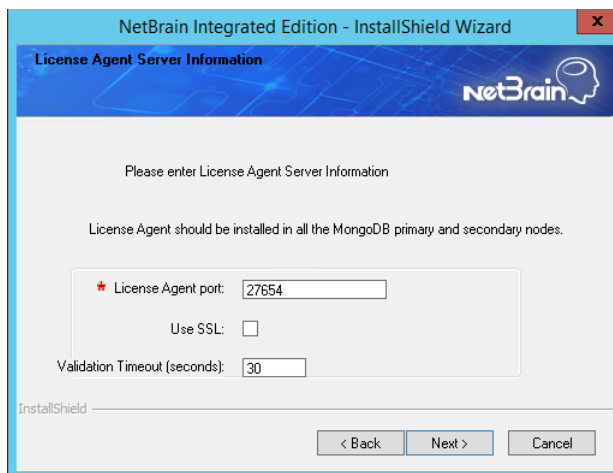
The screenshot shows the 'License Agreement' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main content area contains text about the End User License Agreement (EULA) and a link to the legal page. A checkbox labeled 'I have read the subscription EULA, if I have purchased a subscription license, or the perpetual EULA, if I have purchased a perpetual license, at the link provided above.' is checked. Below this, there is a paragraph asking for acceptance of the terms and a paragraph explaining the 'I ACCEPT' and 'Cancel' buttons. At the bottom, there are three buttons: '< Back', 'I ACCEPT', and 'Cancel'.

- 8) On the MongoDB Server Connection page, enter the password that you created when installing MongoDB and then click **Next**.



The screenshot shows the 'MongoDB Server Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main content area contains text asking for MongoDB server information. There are four input fields: 'Address' (10.10.3.142:27017), 'User Name' (admin), 'Password' (masked with dots), and 'Replica Set Name' (rs). Below these fields, there is a note about confirming the replica set name from the MongoDB server configuration file. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 9) On the License Agent Server Information page, verify the information to connect to the License Agent, and then click **Next**.



The screenshot shows the 'License Agent Server Information' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main content area contains text asking for License Agent server information. There is one input field for 'License Agent port' (27654). Below this field, there is a checkbox for 'Use SSL' and a text box for 'Validation Timeout (seconds)' (30). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

10) On the Elasticsearch Connection page, enter the password of the Elasticsearch, and then click **Next**.

The screenshot shows the 'Elasticsearch Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

- Address:** A text box containing '10.10.3.142:9200'.
- Format:** A label indicating the format: '<Address>:<Port>'. For example: '10.10.10.10:9200'. Use the Ctrl+Enter keys to add all the servers.
- User Name:** A text box containing 'admin'.
- Password:** A password field with masked characters (dots).
- Use SSL:** An unchecked checkbox.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

11) On the RabbitMQ Connection page, enter the IP address, port, and admin password of the RabbitMQ, and then click **Next**.

The screenshot shows the 'RabbitMQ Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

- Address:** A text box containing '10.10.3.142'.
- Format:** A label indicating the format: '<Address>'. For example: '10.10.10.10'. Use the Ctrl+Enter keys to add all the servers for a cluster.
- User Name:** A text box containing 'admin'.
- Password:** A password field with masked characters (dots).
- Port Number:** A text box containing '5672'.
- Use SSL:** An unchecked checkbox.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

12) On the Redis Connection page, enter the IP address, port, and admin password of the Redis, and then click **Next**.

The screenshot shows the 'Redis Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

- Standalone:** A radio button that is selected.
- Redis Address:** A text box containing '10.10.3.142'.
- Redis Port:** A text box containing '6379'.
- Redis Sentinels:** An unselected radio button.
- Note:** A label indicating the format: 'Note: Use the Ctrl+Enter keys to add all the addresses.'
- Sentinel Address:** A text box containing '10.10.3.142'.
- Sentinel Port:** A text box containing '6380'.
- Password:** A password field with masked characters (dots).
- Use SSL:** An unchecked checkbox.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

13) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, License Agent, Elasticsearch, RabbitMQ, or Redis.) On the Certificate Configuration page, confirm the Certificate

Authority (CA) of the SSL certificates used on these servers, and then click **Next**.

The screenshot shows the 'Certificate Configuration' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white and contains the following elements: a title bar with 'NetBrain Integrated Edition - InstallShield Wizard' and a close button; a subtitle 'Certificate Configuration'; a message 'Please enter the Certificate Authority information.'; a checked checkbox labeled 'Conduct Certificate Authority verification'; a text field for 'Certificate Authority path:' containing 'C:\Users\Administrator\Desktop\cacert.pem'; a 'Browse..' button; and a progress bar at the bottom labeled 'InstallShield'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

To authenticate CA:

- a) Select the **Conduct Certificate Authority verification** check box.
- b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

Note: Only the certificate in **Base-64 encoded X.509 PEM** format is supported.

Note: The following conditions must be met for the CA certificate file:

- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

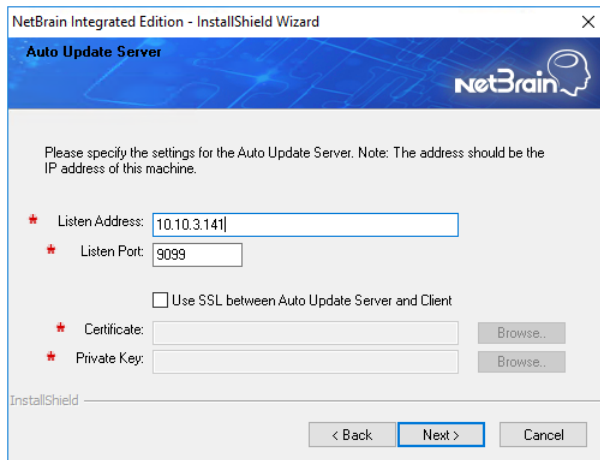
- 14) On the KeyVault Administration Passphrase Settings page, create a passphrase to initialize and manage the system KeyVault which contains all encryption keys to protect data security. Type it twice and click **Next**.

The screenshot shows the 'KeyVault Administration Passphrase Settings' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white and contains the following elements: a title bar with 'NetBrain Integrated Edition - InstallShield Wizard' and a close button; a subtitle 'KeyVault Administration Passphrase Settings'; a caution message: 'CAUTION: This passphrase is not stored in the product and CANNOT be recovered by ANY means. NetBrain STRONGLY recommends storing this passphrase in your company's password vault application. If you lose or forget this passphrase you will have to re-install this product to gain access to the KeyVault, however this will result in the loss of all your data.'; a message 'Please enter the KeyVault Administration Passphrase (KVAP).'; two password fields: 'KVAP:' and 'Re-enter KVAP:'; a warning message: 'WARNING: There is a feature that would allow an Administrator, working with NetBrain technical support to perform a KVAP reset to restore access. By checking the "Enable Resetting KVAP" checkbox below, you will enable this feature. Once activated, this feature CANNOT be deactivated without re-installing the product.'; a checked checkbox labeled 'Enable Resetting KVAP'; and a progress bar at the bottom labeled 'InstallShield'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

Tip: The passphrase must contain at least one uppercase letter, one lowercase letter, one number, and one special character, and the minimum permissible length is 8 characters. All special characters except for the quotation mark (") are allowed.

Note: Keep notes of the passphrase because it is required when you scale up or upgrade these servers. In case of losing the passphrase, keep the **Enable Resetting KVAP** check box selected so that NetBrain system admin can reset the passphrase at any time.

15) On the Auto Update Server page, verify the configuration summary and then click **Next**.



Note: The listen address is the address of Web API Server. It can only be the IP address of the machine.

Note: To enable the SSL between Auto Update Server and Client, select the Use SSL checkbox and upload the certificate file that contains the public key as well as the private key file in the respective fields below.

16) Review the summary of the installation settings and click **Install**. The installation will take some time and it depends on the scale of your database.

17)(Optional) Ensure the NetBrain installation process using administrator account has the necessary permissions to modify "User Rights Assignment" in "Local Security Policy" or change the local user privileges. Otherwise, the following error message will prompt when installing each Windows component.



Click **Yes** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System. If you have security concerns, please click **No** to abort the installation/upgrade.

Note: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.

Note: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

5. After successfully upgrading the Web Server and Web API Server, click **Finish**.
6. Open the IIS Manager to check that the **Default Web Site** and **ServicesAPI** service exist.
7. Open the Task Manager to check that the **NetBrainKCProxy** service is running.

Tip: To have the required configurations auto-populated during the installation of other system components, you can copy the **netbrain.ini** folder from the **C:\NBInstall** folder of this machine directly to the **C:\NBInstall** folder of the machines where Worker Server, Task Engine, and Front Server Controller will be installed.

Post-Upgrade Tasks

- Follow the steps below to recover the special settings if you have customized the **Web.config** file for your Web Server and/or Web API Server:
 - 1) Navigate to **NetBrain > Web Server** and locate the backup file **backup_Web.config** under **nb_publish_server** and **nb_publish_client**.
 - 2) Manually recover the settings one by one in **Web.config** according to the previous configurations in the backup file **backup_Web.config**.

Note: **DO NOT** directly replace the **Web.config** file with the backup file as it may cause log-in problems for NetBrain Workstation.

Note: Contact NetBrain Support if you have any questions regarding the specific items in the **Web.config** file that need to be recovered.

1.11. Upgrading Worker Server

Note: Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

Note: It is not allowed to upgrade any Worker Server and Web API Server at the same time. Otherwise, it will cause DB data initializing failure.

Note: Service Monitor Agent needs to be installed prior to installing Worker Server. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

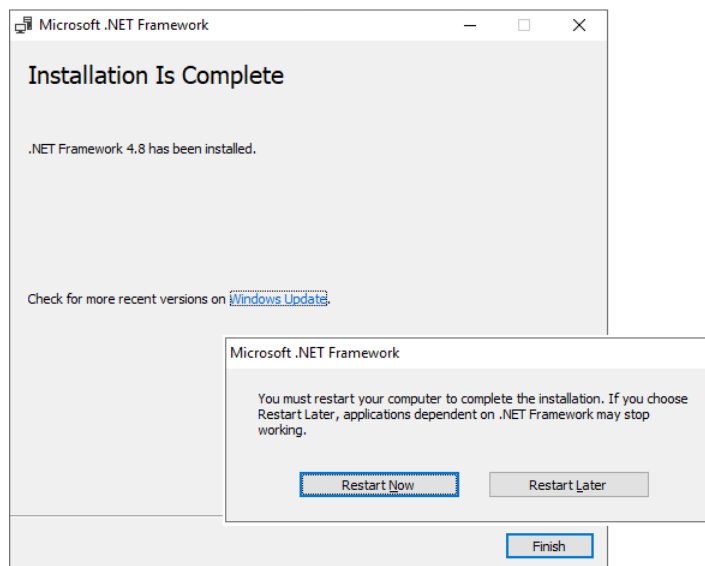
Complete the following steps with administrative privileges.

1. Download the **netbrain-ie-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to launch the Installation Wizard.
4. Follow the Installation Wizard to complete the upgrade step by step:
 - 1) If **.NET Framework 4.8** has not been pre-installed on this machine, the Installation Wizard will guide you through the installation of **.NET Framework 4.8** first.

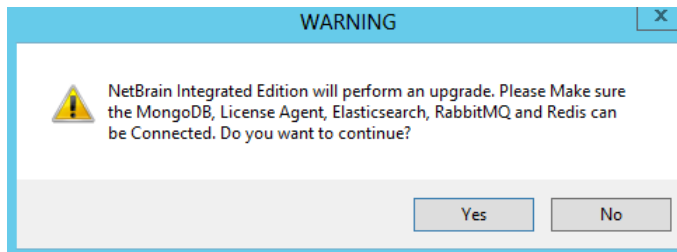
Note: Make sure the Windows update is of the latest. For Windows Server 2012, the update **KB2919442** and **KB2919355** must be installed before the .NET Framework 4.8 installation can start.

Note: Some running applications must be closed during the installation of .NET Framework 4.8, such as Server Manager.

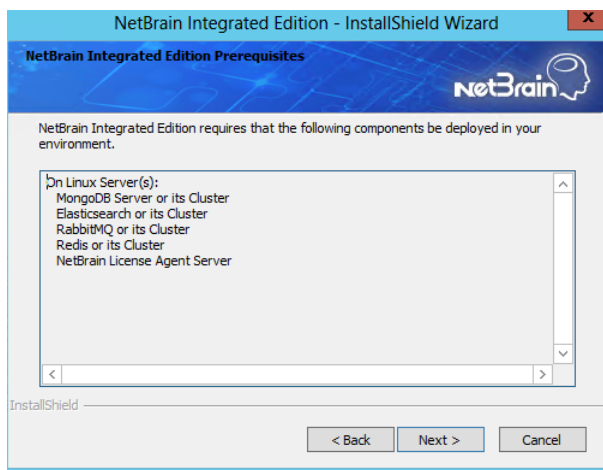
Note: After .NET Framework 4.8 is successfully installed, you must click **Restart** to restart the machine immediately. Otherwise, the upgrade will fail due to the failure of upgrading the new .Net Framework. After the machine reboots, ensure the FIPS is disabled after restarting the machine. To disable the FIPS setting, modify the **Enabled** value to **0** under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy** directory of Windows registry.



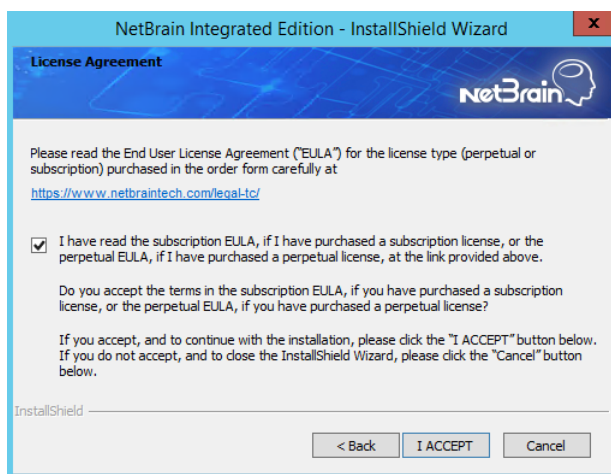
- 2) Stop the service of worker server manually before continuing the upgrade.
- 3) Click **Yes** in the dialog box to initiate the upgrade.



- 4) On the Welcome page, click **Next**.
- 5) On the NetBrain Integrated Edition Prerequisites page, read the components that must be set up in your environment beforehand and click **Next**.



- 6) On the System Configuration page, review the system configuration summary and click **Next**.
- 7) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



- 8) On the MongoDB Server Connection page, enter the password that you created when installing MongoDB and then click **Next**.

The screenshot shows the 'MongoDB Server Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

- Address:** A text box containing '10.10.3.142:27017'.
- Format:** A small text box containing '<Address>:<Port>'. Below it, a note says: 'Format: <Address>:<Port>. For example: 10.10.10.10:27017. Use the Ctrl+Enter keys to add all the servers for a replica set.'
- User Name:** A text box containing 'admin'.
- Password:** A text box with masked characters (dots).
- Replica Set Name:** A text box containing 'rs'.
- Use SSL:** An unchecked checkbox.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

- 9) On the Elasticsearch Connection page, enter the password of the Elasticsearch, and then click **Next**.

The screenshot shows the 'Elasticsearch Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

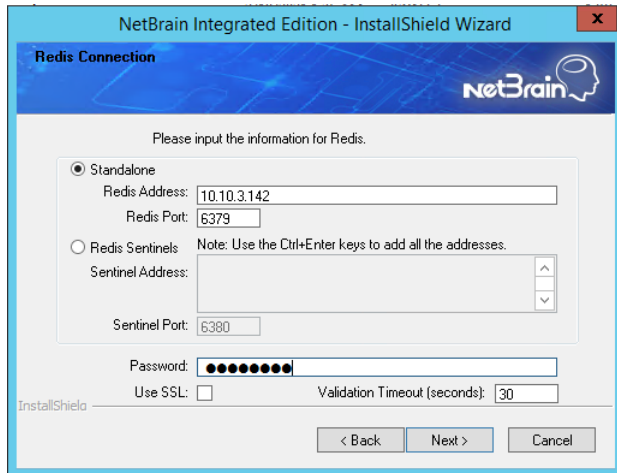
- Address:** A text box containing '10.10.3.142:9200'.
- Format:** A small text box containing '<Address>:<Port>'. Below it, a note says: 'Format: <Address>:<Port>. For example: 10.10.10.10:9200. Use the Ctrl+Enter keys to add all the servers.'
- User Name:** A text box containing 'admin'.
- Password:** A text box with masked characters (dots).
- Use SSL:** An unchecked checkbox.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

- 10) On the RabbitMQ Connection page, enter the IP address, port, and admin password of RabbitMQ, and then click **Next**.

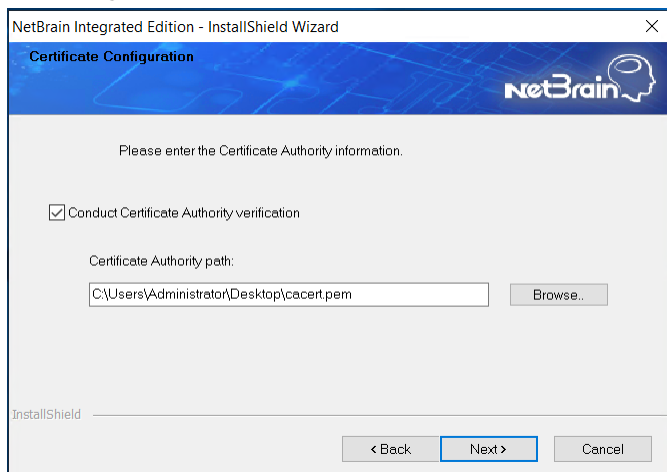
The screenshot shows the 'RabbitMQ Connection' window of the NetBrain Integrated Edition - InstallShield Wizard. The window has a blue header with the NetBrain logo. The main area is white with a blue border. It contains the following fields and controls:

- Address:** A text box containing '10.10.3.142'.
- Format:** A small text box containing '<Address>'. Below it, a note says: 'Format: <Address>. For example: 10.10.10.10. Use the Ctrl+Enter keys to add all the servers for a cluster.'
- User Name:** A text box containing 'admin'.
- Password:** A text box with masked characters (dots).
- Port Number:** A text box containing '5672'.
- Use SSL:** An unchecked checkbox.
- Validation Timeout (seconds):** A text box containing '30'.
- Buttons:** '< Back', 'Next >', and 'Cancel'.

- 11) On the Redis Connection page, enter the IP address, port, and admin password of the Redis, and then click **Next**.



- 12)(Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, License Agent, Elasticsearch, RabbitMQ, or Redis.) On the Certificate Configuration page, confirm the Certificate Authority (CA) of the SSL certificates used on these servers, and then click **Next**.



To authenticate CA:

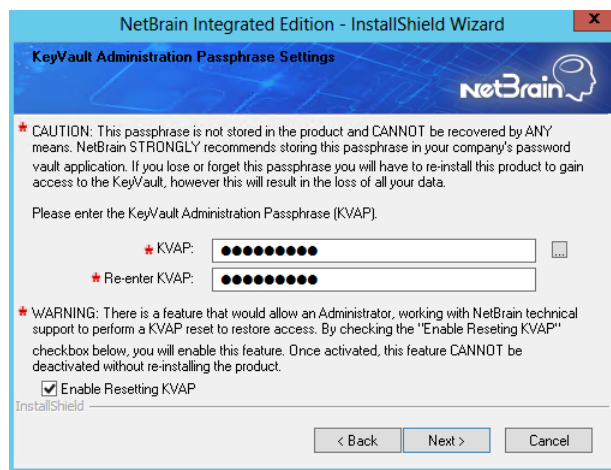
- Select the **Conduct Certificate Authority verification** check box.
- If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

Note: Only the certificate in **Base-64 encoded X.509 PEM** format is supported.

Note: The following conditions must be met for the CA certificate file:

- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

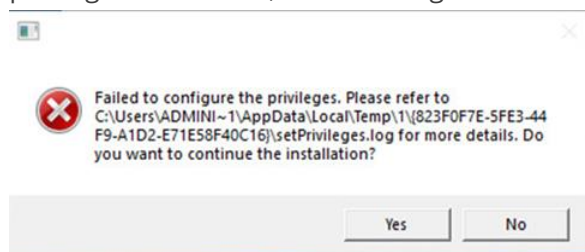
- 13) On the KeyVault Administration Passphrase Settings page, create a passphrase to initialize and manage the system KeyVault which contains all encryption keys to protect data security. Type it twice and click **Next**.



Tip: The passphrase must contain at least one uppercase letter, one lowercase letter, one number, and one special character, and the minimum permissible length is 8 characters. All special characters except for the quotation mark (") are allowed.

Note: Keep notes of the passphrase because it is required when you scale up or upgrade the Application Server. In case of losing the passphrase, keep the **Enable Resetting KVAP** check box selected so that NetBrain system admin can reset the passphrase at any time.

- 14) Review the summary of the installation information and click **Install**.
- 15)(Optional) Ensure the NetBrain installation process using administrator account has the necessary permissions to modify "User Rights Assignment" in "Local Security Policy" or change the local user privileges. Otherwise, the following error message will prompt when installing each Windows component.



Click **Yes** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System. If you have security concerns, please click **No** to abort the installation/upgrade.

Note: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.

Note: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

5. After successfully upgrading the Worker Server, click **Finish**.
6. Open the Task Manager and navigate to the **Services** panel to check that the **NetBrainWorkerServer** service is running.
7. If you have deployed a Worker Server Cluster for load balancing, you can repeat the above steps to upgrade the Worker Servers on separate machines.

Note: Make sure all cluster members have the same configurations for MongoDB, License Agent, Elasticsearch, RabbitMQ, and Redis. And your network configurations allow communications among them.

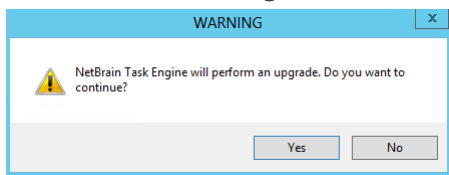
1.12. Upgrading Task Engine

Note: Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

Note: Service Monitor Agent needs to be installed prior to installing Task Engine. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

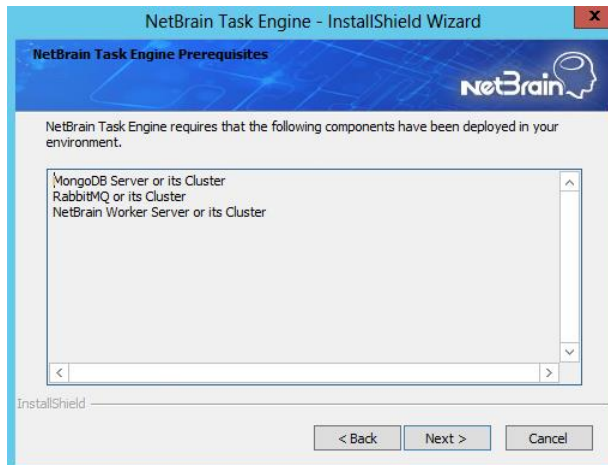
Complete the following steps with administrative privileges.

1. Download the **netbrain-taskengine-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-taskengine-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-taskengine-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) Click **Yes** in the dialog box to initiate the upgrade.

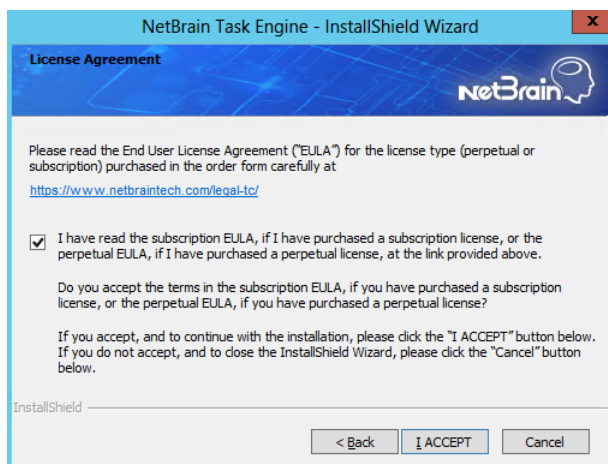


- 2) On the Welcome page, click **Next**.

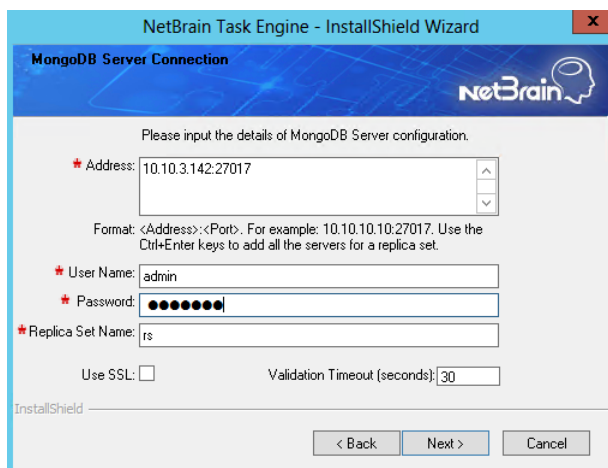
- 3) On the NetBrain Task Engine Prerequisites page, view the components that must be deployed beforehand in your environment and click **Next**.



- 4) On the System Configuration page, review the system configuration summary and click **Next**.
- 5) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



- 6) On the MongoDB Server Connection page, enter the password you created when installing MongoDB, and then click **Next**.



- 7) On the RabbitMQ Connection page, enter the IP address, port, and admin password of the RabbitMQ, and then click **Next**.

NetBrain Task Engine - InstallShield Wizard

RabbitMQ Connection

Please input the details of the RabbitMQ configuration.

* Address: 10.10.3.142

Format: <Address>. For example: 10.10.10.10. Use the Ctrl+Enter keys to add all the servers for a cluster.

* User Name: admin

* Password: ●●●●●●●●

* Port Number: 5672

Use SSL: ☐ Connection Validation Timeout (seconds): 30

InstallShield

< Back Next > Cancel

- 8) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB or RabbitMQ.) On the Certificate Configuration page, confirm the CA of SSL certificates, and then click **Next**.

NetBrain Task Engine - InstallShield Wizard

Certificate Configuration

Please enter the Certificate Authority information.

☒ Conduct Certificate Authority verification

Certificate Authority path

C:\Users\Administrator\Desktop\cacert.pem Browse..

InstallShield

< Back Next > Cancel

To authenticate CA:

- Select the **Conduct Certificate Authority verification** check box.
- If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

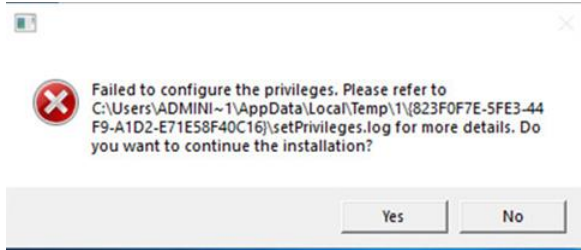
Note: Only the certificate in **Base-64 encoded X.509 PEM** format is supported.

Note: The following conditions must be met for the CA certificate file:

- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

- 9) Review the summary of the installation information and then click **Install**.

- 10)(Optional) Ensure the NetBrain installation process using administrator account has the necessary permissions to modify “User Rights Assignment” in “Local Security Policy” or change the local user privileges. Otherwise, the following error message will prompt when installing each Windows component.



Click **Yes** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System. If you have security concerns, please click **No** to abort the installation/upgrade.

Note: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.

Note: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

4. After successfully upgrading the Task Engine, click **Finish**.
5. Open the Task Manager and navigate to the **Services** panel to check that the **NetBrainTaskEngine** service is running.

Post-Upgrade Task

Uninstall the **Java(TM) SE Development Kit 9.0.1 (64-bit)** from the Windows Control Panel.

Note: Ensure **JDK 9.0.1** is not used by other applications before proceeding with the above step.

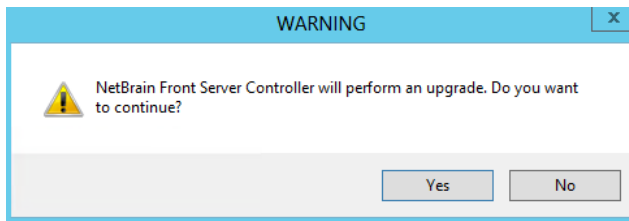
1.13. Upgrading Front Server Controller

Note: Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

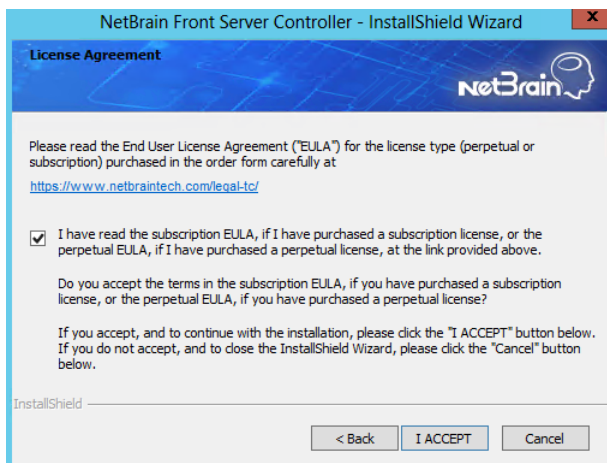
Note: Service Monitor Agent needs to be installed prior to installing Front Server Controller. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

Complete the following steps with administrative privileges.

1. Download the **netbrain-frontservercontroller-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-frontservercontroller-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-frontservercontroller-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) Click **Yes** in the dialog box to initiate the upgrade.



- 2) On the Welcome page, click **Next**.
- 3) On the System Configuration page, review the system configuration summary and click **Next**.
- 4) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



- 5) (Required only if SSL has already been enabled) On the Local SSL Configuration page, confirm the certificate and private key for the Front Server Controller to establish encrypted connections with Worker

Server and Front Server, and then click **Next**.

The screenshot shows the 'Local SSL Configuration' window of the NetBrain Front Server Controller - InstallShield Wizard. The window has a blue header with the NetBrain logo. Below the header, it says 'Define SSL configuration to connect with Worker Server and Front Server.' There are two sections: 'Enable SSL:' with a checked checkbox, and 'Certificate:' and 'Private Key:' fields, both with 'Browse...' buttons. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

- 6) On the MongoDB Connection page, enter the password you created when installing MongoDB and then click **Next**.

The screenshot shows the 'MongoDB Server Connection' window of the NetBrain Front Server Controller - InstallShield Wizard. The window has a blue header with the NetBrain logo. Below the header, it says 'Please input the details of the MongoDB Server configuration.' There are four fields: 'Address:' with a dropdown menu showing '10.10.3.142:27017', 'User name:' with a text box containing 'admin', 'Password:' with a masked password field, and 'Replica Set Name:' with a text box containing 'rs'. There are also 'Use SSL:' and 'Timeout (seconds):' fields. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

- 7) On the RabbitMQ Connection page, enter the IP address, port, and admin password of the RabbitMQ, and then click **Next**.

The screenshot shows the 'RabbitMQ Connection' window of the NetBrain Front Server Controller - InstallShield Wizard. The window has a blue header with the NetBrain logo. Below the header, it says 'Please input the details of the RabbitMQ configuration.' There are four fields: 'Address:' with a dropdown menu showing '10.10.3.142', 'User name:' with a text box containing 'admin', 'Password:' with a masked password field, and 'Port Number:' with a text box containing '5672'. There are also 'Use SSL:' and 'Timeout (seconds):' fields. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

- 8) On the Redis Connection page, enter the IP address, port, and admin password of the Redis, and then click **Next**.

The screenshot shows the 'Redis Connection' window of the NetBrain Front Server Controller - InstallShield Wizard. The window has a blue header with the NetBrain logo. Below the header, it says 'Please input the information for Redis Connection.' There are two radio buttons: 'Standalone' (selected) and 'Redis Sentinels'. The 'Standalone' section has fields for 'Redis Address' (10.10.3.142), 'Redis Port' (6379), 'Password' (masked with dots), 'Use SSL' (unchecked), and 'Timeout (seconds)' (30). The 'Redis Sentinels' section has a 'Sentinel Address' field with up/down arrows and a 'Sentinel Port' field (6380). At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

- 9) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, RabbitMQ, or Redis). On the Certificate Configuration page, confirm the CA of SSL certificates on these servers, and then click **Next**.

The screenshot shows the 'Certificate Configuration' window of the NetBrain Front Server Controller - InstallShield Wizard. The window has a blue header with the NetBrain logo. Below the header, it says 'Please enter the Certificate Authority information.' There is a checked checkbox 'Conduct Certificate Authority verification'. Below it, there is a 'Certificate Authority path:' label and a text field containing 'C:\Users\Administrator\Desktop\cacert.pem'. To the right of the text field is a 'Browse..' button. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

To authenticate CA:

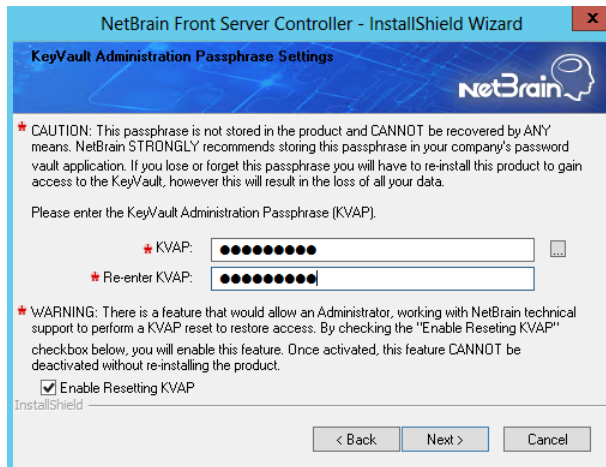
- Select the **Conduct Certificate Authority verification** check box.
- If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

Note: Only the certificate in **Base-64 encoded X.509 PEM** format is supported.

Note: The following conditions must be met for the CA certificate file:

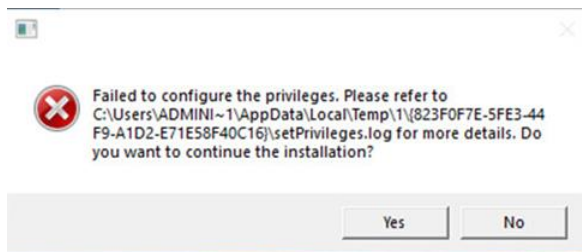
- The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
- The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
- Internet access must be ensured if the certificate is signed by third-party CA.

10) On the KeyVault Administration Passphrase Settings page, enter the passphrase that you created when installing the Web API Server twice and click **Next**.



11) Review the summary of the installation information and click **Install**.

12) (Optional) Ensure the NetBrain installation process using administrator account has the necessary permissions to modify "User Rights Assignment" in "Local Security Policy" or change the local user privileges. Otherwise, the following error message will prompt when installing each Windows component.



Click **Yes** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System. If you have security concerns, please click **No** to abort the installation/upgrade.

Note: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.

Note: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

4. After successfully upgrading the Front Server Controller, click **Finish**.
5. Open the Task Manager and navigate to the **Services** panel to check that the **NetBrainFrontServerController** service is running.

1.14. Upgrading Front Server

Select either of the following ways to upgrade your Front Servers, depending on their operating systems:

- [Upgrading Front Server on Linux](#)
- [Upgrading Front Server on Windows](#)

1.14.1. Upgrading Front Server on Linux

Pre-Upgrade Tasks

- Ensure you have upgraded the Linux OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit**, **CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit** or **Oracle Linux Server 7.7/7.8/7.9/8.2/8.3, 64-bit** to avoid installation or upgrade failure. Refer to [Linux System Upgrade Instructions Online](#) for more details. If your Linux server has no access to the Internet, refer to [Linux System Upgrade Instructions Offline](#).

Note: During and after the Linux OS upgrade, do not restart the Linux server, and keep all the NetBrain services on Linux server including MongoDB running normally and all the services on the Windows server stopped.

- Service Monitor Agent will be installed or upgraded with Front Server and it has dependencies on the third-party package **libffi-devel zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa|grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel|gcc"` command to check whether it has been installed on this Linux server. If it has not been installed yet, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install them online
 - **Offline Install:** refer to [Appendix: Offline Installing Third-party Dependencies](#) for further instructions.
- Front Server has dependencies on several third-party packages. Before you install the Front Server, run the `rpm -qa|grep -E "glibc|libstdc++|libuuid|pam"` command to check whether these dependencies have been installed. If not, you can choose either option below to install the dependencies:
 - **Online Install:** run the `yum install -y glibc libstdc++ libuuid pam` command to install these third-party packages online.
 - **Offline Install:** see [Appendix](#) for more details.

Upgrading Front Server on Linux

1. Log in to the Linux server as the **root** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the Front Server installation package. For example, **netbraintemp10.0**.
3. Run the `cd /opt/netbraintemp10.0` command to navigate to the **/opt/netbraintemp10.0** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **netbrain-frontserver-linux-x86_64-rhel-10.0.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp10.0** directory by using a file transfer tool.
 - **Option 2:** If the Linux server has access to the Internet, run the `wget <download link>` command under the **/opt/netbraintemp10.0** directory to directly download the **netbrain-frontserver-linux-x86_64-rhel-10.0.tar.gz** file from NetBrain official download site.

Note: The download link is case-sensitive.

Tip: Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

5. Run the `tar -zxvf netbrain-frontserver-linux-x86_64-rhel-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

```
[root@localhost netbraintemp10.0]# tar -zxvf netbrain-frontserver-linux-x86_64-rhel-10.0.tar.gz
FrontServer/
FrontServer/config/

FrontServer/upgrade.sh
FrontServer/fix_releaseinfo.json
```

6. Run the `cd FrontServer` command to navigate to the **FrontServer** directory.
7. Run the `./upgrade.sh` script under the **FrontServer** directory to upgrade the Front Server.
 - 1) Read the License Agreement, and type **YES**.
 - 2) Type **I ACCEPT** to accept the License Agreement.
 - 3) Enter and confirm the NetBrain Front Server PostgreSQL password.

Note: The length of the password must be greater than 8 characters.

- 4) Enter the port number listened by the NetBrain Front Server PostgreSQL.
- 5) Enter the data path for the NetBrain Front Server.

Note: Make sure the designated data directory has more than 180GB free space.

6) Confirm the above parameters by typing **YES**. The script will then start to install the Front Server.

```
[root@localhost FrontServer]# ./upgrade.sh
Please read the End User License Agreement ("EULA") for the license type (perpetual or
subscription) purchased in the order form at https://www.netbraintech.com/legal-tc/
carefully. I
have read the subscription EULA, if I have purchased a subscription license, or the
perpetual
EULA, if I have purchased a perpetual license, at the link provided above. Please type "YES"
if
you have read the applicable EULA and understand its contents, or "NO" if you have not read
the
applicable EULA. [YES/NO]: YES

Do you accept the terms in the subscription EULA, if you have purchased a subscription
license, or the
perpetual EULA, if you have purchased a perpetual license? If you accept, and to continue
with the
installation, please type "I ACCEPT" to continue. If you do not accept, and to quit the
installation
script, please type "CANCEL" to stop. [I ACCEPT/CANCEL]: I ACCEPT

...
Upgrade Linux Front Server.
The values in brackets are the default values of the parameters. To keep the default value
for the current parameter, press the Enter key.
Please enter the NetBrain Front Server PostgreSQL Password:

Please re-enter NetBrain Front Server PostgreSQL Password to confirm:
Please enter PostgreSQL port [5432]:

Please enter the data path for NetBrain Front Server [/usr/lib/netbrain/frontserver]:
Front Server password: *****
Front Server DB port: 5432
Front Server Data Path: /usr/lib/netbrain/frontserver
Do you want to continue using these parameters (yes/no)? [yes]
INFO: 2021-02-26 19-24-32.558: Dependent packages checking SUCCEEDED.
INFO: 2021-02-26 19-24-33.755: Checking password
INFO: 2021-02-26 19-24-33.759: Checking Port 5432
INFO: 2021-02-26 19-24-33.792: Configuration parameters checking SUCCEEDED.
INFO: 2021-02-26 19-24-35.035: Creating uninstallation log file SUCCEEDED
...
INFO: 2021-02-26 19-25-04.499: The Front Server has been upgraded successfully.
INFO: 2021-02-26 19-25-04.504: Upgrading Front Server SUCCEEDED.
```

Note: Disk space check will be performed to ensure the requirement of minimum 180G free disk space is met.

Note: Before upgrading this component, Service Monitor Agent will be upgraded to the latest version. The entire process does not require any user inputs.

Note: If the Service Monitor Agent was not previously installed, you'll need to use the interactive command line to install it. See [Appendix: Interactive Pre-Installation of Service Monitor Agent](#) for more details.

8. If you deployed multiple Front Servers, repeat the above steps on other machines.
9. Run the `systemctl status netbrainfrontserver` command to check the service status of each node.

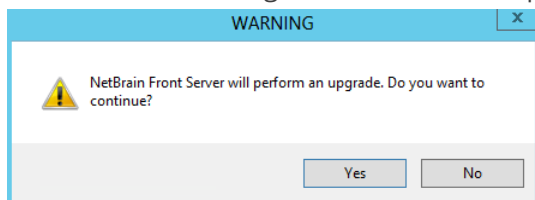
1.14.2. Upgrading Front Server on Windows

Note: Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

Note: Service Monitor Agent needs to be installed prior to installing Front Server. If you do not install the Service Monitor Agent, see [Installing Service Monitor Agent on Windows](#) for more detailed steps of installation. If you have installed before, refer to [Upgrading Service Monitor Agent on Windows](#) for more detailed steps of upgrading Service Monitor Agent.

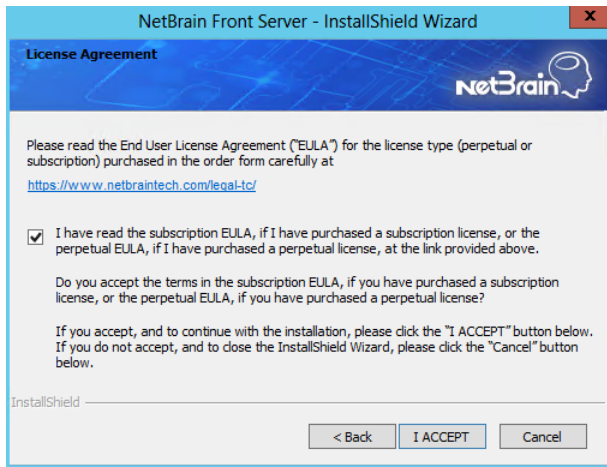
Complete the following steps with administrative privileges.

1. Download the **netbrain-frontserver-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-frontserver-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-frontserver-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to start the Installation Wizard.
 - 1) Click **Yes** in the dialog box to initiate the upgrade.



- 2) On the Welcome page, click **Next**.
- 3) On the System Configuration page, review the system configuration summary and click **Next**.

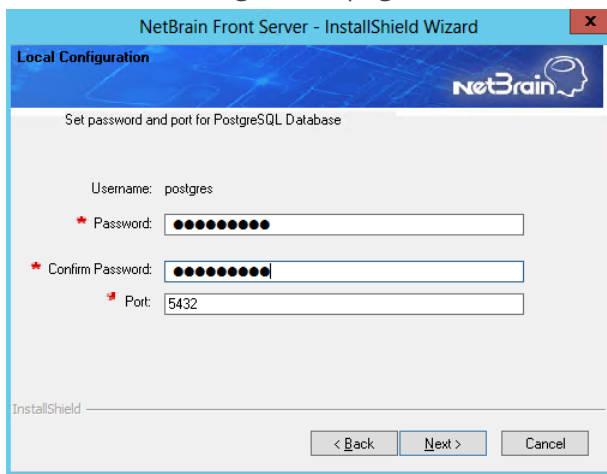
- 4) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA** check box and then click **I ACCEPT**.



- 5) On the Customer Information page, enter the Company Name and click **Next**.
- 6) On the PostgreSQL Data Location page, click **Next** to store PostgreSQL data to the default directory **C:\Program Files\NetBrain\PostgresData**. If you want to install it to another location, click **Change**.

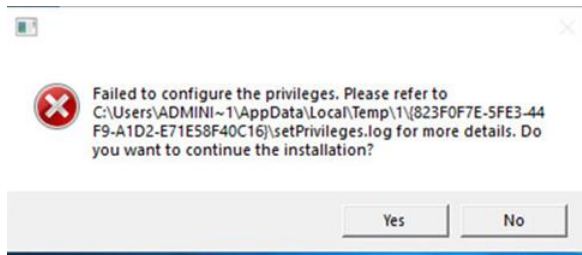
Note: Make sure the designated data folder has more than 180GB free space.

- 7) On the Local Configuration page, create and confirm the password for PostgreSQL Database.



Note: The length of the password must be greater than 8 characters.

- 8) Review the summary of the current installation settings and click **Install**.
- 9) (Optional) Ensure the NetBrain installation process using administrator account has the necessary permissions to modify "User Rights Assignment" in "Local Security Policy" or change the local user privileges. Otherwise, the following error message will prompt when installing each Windows component.



Click **Yes** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System. If you have security concerns, please click **No** to abort the installation/upgrade.

Note: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.

Note: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

4. After successfully upgrading the Front Server, click **Finish**.
5. If you have deployed multiple Front Servers, repeat the above steps on other machines.
6. After the installation is completed, you can open the Task Manager and navigate to the **Services** panel to check whether **NetBrainFrontServer** is running.

1.15. Unbinding Perpetual License

1. In your web browser, navigate to **http(s)://<IP address of NetBrain Web Server>/admin.html** to log in to the System Management page.

Note: In order to minimize the issue caused by insufficient privilege, it's strongly recommended to use the local "admin" account to log in to the System Management page.


2. Click **OK** on a pop-up notification dialog.
3. Click **Unbind**.
4. Validate your perpetual license information and unbind it from NetBrain License Server.
 - 1) Select **Online** and click **Next**.
 - 2) Enter your license password and click **Unbind**.
 - 3) Click **Yes** on a notification dialog box.

Note: If your NetBrain Web/Web API Server is not allowed to access the Internet, you can unbind the license from your local machine first, and then send the unbind file to [NetBrain Support Team](#) to unbind it from NetBrain License Server.

- 1) Select **Via Email** and click **Next**.
- 2) Enter your email address and click **Unbind**. The **netbrain.Unbind** file will be generated and downloaded to your local disk.
- 3) Send an email to [NetBrain Support Team](#) with the file attached. NetBrain support team will help remove your license information from NetBrain License Server.

1.16. Activating Subscription License

1. In the System Management page, click **Activate** under the **License** tab. The activation wizard prompts.
2. Activate your subscription license:
 - 1) Select **Activate Subscription License** and click **Next**.
 - 2) Enter the license ID and activation key that you received from NetBrain, with your first name, last name, and email address.
 - 3) Select the activation method based on your situation.
 - **Online** (recommended) — click **Activate** to connect to NetBrain License Server and validate your license information immediately.

Note: If your NetBrain Web/Web API Server is not allowed to access the Internet, you can configure a proxy server. Click the  icon at the upper-right corner, select the **Use a proxy server to access the internet** check box and enter the required information.

- **Via Email** — validate your license information by sending an email to NetBrain.

Note: Only use this activation method when your NetBrain Web/Web API Server is not allowed to access the Internet.


- a) Follow the instructions to generate your license file. Attach the file to your email and send it to [NetBrain Support Team](#). After receiving your email, the NetBrain team will fill in the license information on NetBrain License Server and generate the corresponding activation file, and then send it back to you.

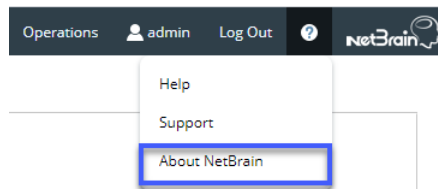
- b) Click **Browse** to select the activation file that you received from the NetBrain team, and then click **Activate**.
- 4) A message box will prompt you the subscription license has been activated successfully. Click **OK**.
3. A confirmation dialog box prompts to ask you whether to generate an initial tenant. Click **Yes** and the initial tenant will be created automatically with all purchased nodes assigned.

1.17. Verifying Upgrade Results

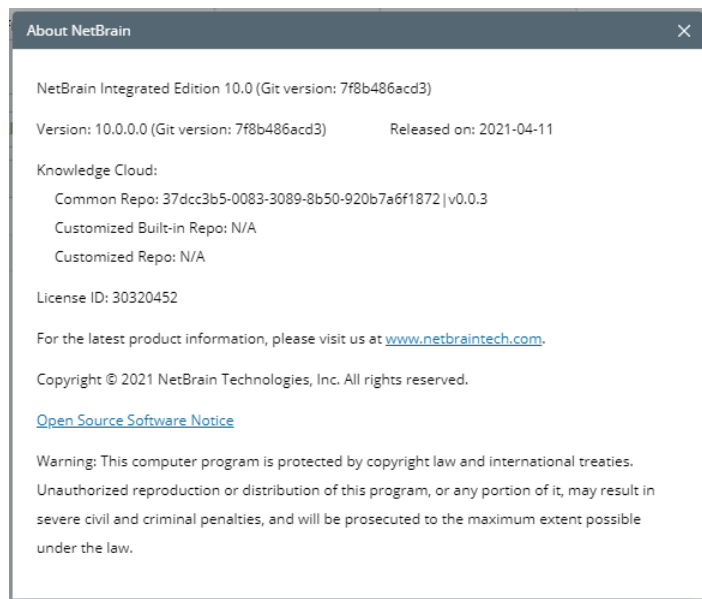
1. Do the following steps to check the IE version in web browser:

Note: It is highly recommended to clear your web browser's cache before reloading the IE web page.

- 1) In the system Management page, click the  icon and select **About NetBrain** from the quick access toolbar.



- 2) Check the version information.



2. Do the following steps to check the system version in MongoDB:

- 1) Log in to the Linux server where MongoDB is installed.

- 2) Open a command prompt and run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --authenticationMechanism SCRAM-SHA-256` command to connect to MongoDB.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

Example:

```
[root@localhost ~]# mongo --host 10.10.3.142:27017 -u mongodb -p mongodb --
authenticationDatabase admin --authenticationMechanism SCRAM-SHA-256
MongoDB shell version v4.0.19
connecting to: mongodb://10.10.3.142:27017/?authMechanism=SCRAM-SHA-
256&authSource=admin&gssapiServiceName=mongodb
...
```

Tip: If SSL is enabled, run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --ssl --sslAllowInvalidCertificates --authenticationMechanism SCRAM-SHA-256` command.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

- 3) Run the `use NGSystem` command to switch to the **NGSystem** database.

```
rsnetbrain:PRIMARY> use NGSystem
switched to db NGSystem
```

- 4) Run the `db.SystemInfo.find({_id: "SystemVersion"})` command to check the system version number.

```
rsnetbrain:PRIMARY> db.SystemInfo.find({_id: "SystemVersion"})
{ "_id" : "SystemVersion", "version" : "10.0", "operateInfo" : { "opUser" : "NetBrain",
"opTime" :
  ISODate("2020-07-14T18:31:21.735") } } }
```

- 5) Run the `exit` command to exit the command prompt.

Note: System Update feature heavily relies on all the NetBrain servers and service metrics, therefore it is required to ensure all the NetBrain servers and component metrics can be viewed in the Service Monitor page.

1.18. Customizing MongoDB Disk Alert Rules

To proactively prevent the system database from data loss or even corruption, you can customize MongoDB, Front Server, and Elasticsearch disk alert rules with progressive quotas assigned. When the usage reaches the predefined threshold, specified users can be notified by both email alerts and system alerts.

1. In the System Management page, click **Operations > Service Monitor** from the quick access toolbar.
2. In the Service Monitor home page, click **Alert Rules** at the upper-right corner. The default settings are as follows. When a Front Server disk or Elasticsearch disk usage is high, the system will also push alerts by email

Alert Rules

MongoDB:

- ☒ When MongoDB disk usage reaches % or only GB free space, send emails.
- ☐ When MongoDB disk usage reaches % or only GB free space, send emails and delete Data Engine data older than months. i
- ☒ When MongoDB disk usage reaches % or only GB free space, send emails and disable write permission to MongoDB.

Front Server:

- ☒ When Front Server disk usage reaches % or only GB free space, send emails.

Elasticsearch:

- ☒ When Elasticsearch disk usage reaches % or only GB free space, send emails.

Server/Service:

- ☒ When a server is disconnected or a service is stopped, send email

Send Email Settings:

Send Email To : Cc :

Send Email Frequency : Hours

[Help](#) [Cancel](#) [OK](#)

3. Change the settings based on your needs.
 - 1) Specify the disk usage threshold for different levels.

Note: To email alerts when a server is disconnected or a service is stopped, select the corresponding check box.

- 2) Enter the email address in the **Send Email To** or **CC** fields.

Note: Email alerts are enabled only when email addresses are added at least in one field. Use a colon or semicolon to separate multiple items.

- 3) Specify the frequency to send emails.
- 4) Click **OK** to save the configuration.

1.19. Tuning Live Access

To tune live access, complete the following steps:

1. In your web browser, navigate to **http(s)://<IP address of NetBrain Web Server>/** to log in to your domain.
2. Click the domain name from the quick access toolbar and select **Manage Domain**.
3. In the Domain Management page, select **Operations > Advanced Tools > Tune Live Access** from the quick access toolbar. The **Tune Live Access** tab opens with all devices in the domain listed.
4. Click **Start Tuning**.
5. When the tuning process is completed, a notification message is displayed. Click **OK**.

1.20. Scheduling Benchmark Task

1. In the Domain Management page, select **Operations > Schedule Task** from the quick access toolbar.
2. On the **Schedule Task > Schedule Discovery/Benchmark** tab, select the **Enable** check box for the **Basic System Benchmark** entry.

Note: A full benchmark must be performed by enabling the **L2 Topology** option under the **Build Topology** section of the **Additional Operation After Benchmark** tab.

3. Click the  icon to select the **Run Now** option from the drop-down list to run the benchmark task immediately.

Note: If you have multiple Front Servers, go to **Operations > Benchmark Tools > CheckPoint OPSEC Manager** to specify the target Front Server to access your CheckPoint firewalls and retrieve live data.

2. Appendix: Editing a File with VI Editor

The following steps illustrate how to edit a configuration file with the vi editor, which is the default text file editing tool of a Linux operating system.

1. Create a terminal and run the `cd` command at the command line to navigate to the directory where the configuration file is located.
2. Run the `vi <configuration file name>` command under the directory to show the configuration file.
3. Press the **Insert** or **I** key on your keyboard, and then move the cursor to the location where you want to edit.
4. Modify the file based on your needs, and then press the **Esc** key to exit the input mode.
5. Enter the `:wq!` command and press the **Enter** key to save the changes and exit the vi editor.

3. Appendix: Offline Installing Third-party Dependencies

1. Download the dependency package from a server with the Internet access using one of the following download links according to the version of your Operating System:

- **CentOS7.5:** <http://download.netbraintech.com/dependencies-centos7.5.tar.gz>
- **CentOS7.6:** <http://download.netbraintech.com/dependencies-centos7.6.tar.gz>
- **CentOS7.7:** <http://download.netbraintech.com/dependencies-centos7.7.tar.gz>
- **CentOS7.8:** <http://download.netbraintech.com/dependencies-centos7.8.tar.gz>
- **CentOS7.9:** <http://download.netbraintech.com/dependencies-centos7.9.tar.gz>
- **CentOS8.2:** <http://download.netbraintech.com/dependencies-centos8.2.tar.gz>
- **CentOS8.3:** <http://download.netbraintech.com/dependencies-centos8.3.tar.gz>
- **RHEL7.5:** <http://download.netbraintech.com/dependencies-rhel7.5.tar.gz>
- **RHEL7.6:** <http://download.netbraintech.com/dependencies-rhel7.6.tar.gz>
- **RHEL7.7:** <http://download.netbraintech.com/dependencies-rhel7.7.tar.gz>
- **RHEL7.8:** <http://download.netbraintech.com/dependencies-rhel7.8.tar.gz>
- **RHEL7.9:** <http://download.netbraintech.com/dependencies-rhel7.9.tar.gz>
- **RHEL8.2:** <http://download.netbraintech.com/dependencies-rhel8.2.tar.gz>
- **RHEL8.3:** <http://download.netbraintech.com/dependencies-rhel8.3.tar.gz>
- **OL7.7:** <http://download.netbraintech.com/dependencies-ol7.7.tar.gz>
- **OL7.8:** <http://download.netbraintech.com/dependencies-ol7.8.tar.gz>
- **OL7.9:** <http://download.netbraintech.com/dependencies-ol7.9.tar.gz>
- **OL8.2:** <http://download.netbraintech.com/dependencies-ol8.2.tar.gz>
- **OL8.3:** <http://download.netbraintech.com/dependencies-ol8.3.tar.gz>

2. Copy the downloaded dependency package to your Linux server.

3. Run the `tar -zxvf dependencies-<OS version>.tar.gz` command to decompress the package.

Tip: Possible values of **OS version** include: `centos7.5; centos7.6; centos7.7; centos7.8; centos7.9; centos8.2; centos8.3; rhel7.5; rhel7.6; rhel7.7; rhel7.8; rhel7.9; rhel8.2; rhel8.3; ol7.7; ol7.8; ol7.9; ol8.2; ol8.3.`

4. Run the `cd dependencies` command to navigate to the decompressed directory.

5. Run the `offline-install.sh` command to install the dependencies.

4. Appendix: Restoring MongoDB Data

If you encounter data loss or corruption during the upgrade process, complete the following steps to restore MongoDB data with the backup data.

1. Log in to the Linux server where the MongoDB is installed as the **root** user.

2. Stop the MongoDB Service.

1) Run the `systemctl stop mongod` command to stop the MongoDB service.

2) Run the `ps -ef|grep mongod` command to verify whether the **mongod** process is stopped.

```
[root@localhost ~]# ps -ef| grep mongod
root      15136 14237  0 10:42 pts/2      00:00:00 grep --color=auto mongod
```

Note: If the **mongod** process is stopped, the result should only contain one entry as shown above.

3. Restore the old data onto the MongoDB.

1) Run the `cd /usr/lib/mongodb` command to navigate to the **/usr/lib/mongodb** directory.

Note: If you modified the following default directory to store all MongoDB data files during the MongoDB installation, you must use the new directory (available in the **mongod.conf** file) accordingly. For an upgraded system, e.g., upgraded from IEv7.x, the default directory is **/opt/mongodb**.

2) Run the `ls -al` command to browse all directories and files under the **/usr/lib/mongodb** directory.

```
[root@localhost mongodb]# ls -al
total 142
drwxr-xr-x. 5 netbrain netbrain 146 Oct 19 15:02 .
drwxr-xr-x. 4 root      root      42 Sep 19 14:41 ..
drwxr-xr-x. 4 root      netbrain  42 Oct 19 15:03 data
drwxr-xr-x. 4 root      netbrain 100 Oct 19 15:03 log
-rwxr-xr-x. 2 netbrain netbrain 1004 Aug 25 17:26 mongodb-keyfile
-rwxr-xr-x. 1 netbrain netbrain 1076 Oct 19 15:02 mongod.conf
```

3) Run the `rm -rf ./data` command to delete the **data** directory.

4) Run the `mv /etc/mongodb_databk/data /usr/lib/mongodb/data` command under the **/usr/lib/mongodb** directory to move the data directory to the **/usr/lib/mongodb** directory.

5) Run the `chown -R netbrain:netbrain /usr/lib/mongodb/data/` command to change the ownership for the moved data folder.

6) Run the `ls -al` command to browse all directories and files under the **/usr/lib/mongodb** directory.

```
[root@localhost mongodb]# ls -al
total 142
```



```
drwxr-xr-x. 5 netbrain netbrain 146 Oct 19 15:02 .
drwxr-xr-x. 4 root root 42 Sep 19 14:41 ..
drwxr-xr-x. 4 netbrain netbrain 86016 Oct 19 15: 03 data
drwxr-xr-x. 4 root root 100 Oct 19 15: 03 log
-rwxr-xr-x. 2 netbrain netbrain 1004 Aug 25 17: 26 mongodb-keyfile
-rwxr-xr-x. 1 netbrain netbrain 1076 Oct 19 15:02 mongod.conf
```

4. Run the `systemctl start mongod` command to restart the MongoDB service.
5. Run the `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name>` command to connect to the node.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

Example:

```
[root@localhost upgrade_replica_set]# mongo --host 10.10.3.142:27017 -u mongodb -p mongodb --
authenticationDatabase admin
MongoDB shell version v3.6.4
connecting to: mongodb://10.10.3.142:27017/?authMechanism=SCRAM-SHA-
256&authSource=admin&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("0315bda2-73f3-4304-9166-c008b9b06ce3") }
MongoDB server version: v3.6.4
...
rsnetbrain:PRIMARY>
```

Tip: If SSL is enabled, run the command `mongo --host <IP or hostname of MongoDB Server:Port> -u <username> -p <password> --authenticationDatabase <database_name> --ssl --sslAllowInvalidCertificates` command.

5. Appendix: Dumping MongoDB Data

The built-in MongoDB command `mongodump` is a simple and efficient tool for backing up a small volume of MongoDB data. However, for a large volume of data, it is more time-consuming than using the `cp` command introduced in [Backing Up MongoDB Data](#).

Note: Make sure the service of MongoDB is running when you run the `mongodump` command.

Note: The dumped data can be used to restore data in any server.

1. Log in to the Linux server where the MongoDB is installed as **root** user.
2. Open a command prompt and run the `[root@localhost ~]# mkdir /etc/mongodb_databk` command to create a directory under the **/etc** directory to save the backup data.
3. Run the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --gzip --out <filepath>` command to dump the MongoDB data to the **/etc/mongodb_databk** directory.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

Example:

```
[root@localhost ~]# mongodump --host 127.0.0.1:27017 -u mongodb -p mongodb --
authenticationDatabase admin --gzip --out /etc/mongodb_databk
```

Tip: If SSL is enabled, run the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --ssl --sslAllowInvalidCertificates --gzip --out <filepath>` command.

4. Verify the backup result.
 - 1) Run the `cd /etc/mongodb_databk` command to navigate to the **/etc/mongodb_databk** directory.
 - 2) Run the `ls -al` command under the **mongodb_databk** directory to browse the backup data.

Restoring Dumped MongoDB Data

Restore the dumped data by using the `mongorestore` command provided by MongoDB.

Note: Make sure the service of MongoDB is running when you run the `mongorestore` command.

Note: Make sure other relevant services are stopped.

To restore the dumped MongoDB data onto the MongoDB server, run the `mongorestore --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --gzip <filepath>` command.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

Example:

```
[root@localhost ~]# mongorestore --host 127.0.0.1:27017 -u mongodb -p mongodb --  
authenticationDatabase admin --gzip /etc/mongodb_databk
```

Tip: If SSL is enabled, run the `mongorestore --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --ssl --sslAllowInvalidCertificates --gzip <filepath>` command.

Note: The `<database_name>` mentioned in the above command must be **admin** for NetBrain.

6. Appendix: Interactive Pre-Installation of Service Monitor Agent

Service Monitor Agent will be pre-installed with MongoDB, Elasticsearch, License Agent, Redis, RabbitMQ and Front Server if it was not previously installed.

In such scenario, you'll be prompted to configure the following parameters before the installation or upgrade of the above components takes place:

```
INFO: Starting to check configuration parameters...
Configuring Service Monitor Agent ...
The values in brackets are the default values of the parameters. To keep the default value for
the current parameter,
press the Enter key.
Please enter the URL (must end with /) to call NetBrain Web API service for the Service Monitor
[http(s)]:
//<IP address or hostname of NetBrain Application Server>/]: http://10.10.3.141/
Please enter the API Key to be used to communicate with application server which must be the same
as the one created on Web API server:
Please re-enter API key to confirm:
Please enter a log path for NetBrain Service Monitor Agent
[/var/log/netbrain/nbagent]: /log/nbagent
NetBrain Web API service URL: http://10.10.3.141/ServicesAPI
API key: *****
NetBrain Service Monitor Agent LogPath: /log/nbagent
Certificate Authority verification: no
Do you want to continue using these parameters? [yes]
...
```

Note: The log path for Service Monitor Agent must have at least 10G free space. You can keep the default path or input your required path after inputting the URL and API key.

Note: If https:// is used in the Web API Service URL, you will be asked whether to enable the Certificate Authority verification and input the Certificate Authority file if enabled.

Note: The API Key should be the same as the one to be/had been created when installing Web API Server.