IE

NetBrain® Integrated Edition 8.0

System Upgrade Guide

Distributed Deployment

Version 8.03 | Last Updated 2020-12-08

Contents

1. Upgrading System 4

1.1. Terminating System Tasks and Sessions 5

1.2. Stopping Server Services 6

1.3. Backing Up MongoDB Data 7

1.4. Upgrading MongoDB 8

1.5. Upgrading Elasticsearch 10

1.6. Upgrading License Agent 12

1.7. Upgrading Redis 14

1.7.1. Installing Redis on Linux 14

1.8. Upgrading RabbitMQ 19

1.8.1. Installing RabbitMQ on Linux 20

1.9. Upgrading Web/Web API Server 25

1.10. Upgrading Worker Server 32

1.11. Installing Task Engine 37

1.12. Installing Front Server Controller 41

1.13. Upgrading Front Server 46

1.13.1. Installing Front Server 46

1.13.2. Uninstalling Proxy Server 50

1.14. Installing Service Monitor Agent 50

1.14.1. Installing Service Monitor Agent on Linux 51

1.14.2. Installing Service Monitor Agent on Windows 55

1.15. Unbinding Perpetual License 58

1.16. Activating Subscription License 59

1.17. Verifying Upgrade Results 60

1.18. Allocating Tenants to Front Server Controller 62

1.19. Adding a Front Server for a Tenant 64

1.20. Registering a Front Server 64

1.21. Upgrading External Authentication 68

1.22. Upgrading Email Settings 68

1.23. Customizing MongoDB Disk Alert Rules 69

1.24. Tuning Live Access 70

1.25. Scheduling Benchmark Task 70

2. Appendix: Editing a File with VI Editor 72

3. Appendix: Offline Installing Third-party Dependencies 73

4. Appendix: Restoring MongoDB Data 74

5. Appendix: Dumping MongoDB Data 76

6. Appendix: Restoring Dumped MongoDB Data 77

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 IEv7.0b/b1

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. Install Task Engine
12. Install Front Server Controller
13. Upgrade Front Server
14. Install Service Monitor Agent
15. Unbind Perpetual License
16. Activate Subscription License
17. Verify Upgrade Results
18. Allocate Tenants to Front Server Controller
19. Add a Front Server to a Tenant
20. Register a Front Server
21. Upgrade External Authentication
22. Upgrade Email Settings
23. Customize MongoDB Disk Alert Rules
24. Tune Live Access
25. 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	Knowledge Cloud Domain (https://knowledgecloud.netbraintech.com/)	HTTPS (443)
Web API Server Worker Server Task Engine Front Server Controller	MongoDB RabbitMQ	TCP 27017 TCP 5672
Web API Server Worker Server	Elasticsearch License Agent	TCP 9200 TCP 27654
Web API Server Worker Server Front Server Controller	Redis	TCP 6379 (non-ssl)/TCP 7000 (ssl)
Worker Server Task Engine Front Server	Front Server Controller	TCP 9095
Front Server	Live Network	ICMP/SNMP/Telnet/SSH/REST API

> **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 and Sessions

1. Log into System Management page.
2. Navigate to **Current Users** tab, click **End Session** to terminate any active sessions.
3. Select the **Task Manager** tab.
4. 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, you must stop the following relevant services:

1. Log in to the Windows servers and stop the following services in the Task Manager.
   - **W3SVC** (Web API Server service)
   - **WAS** (Web API Server service)

NetBrain Components	Service Name in v7.0b/v7.0b1
Redis	RedisMaster
RabbitMQ	RabbitMQ
Worker Server	ResourceManager
Front (Proxy) Server	proxyserverie
Task Engine	N/A
Front Server Controller	N/A

2. Disable the **Cron** task on the MongoDB. 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 mongodnetbrain status|grep -q -E
"(dead)|failed";
then /usr/sbin/service mongodnetbrain 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 mongodnetbrain status|grep -q -E
"(dead)|failed";
then /usr/sbin/service mongodnetbrain start; fi' >/dev/null 2>&1
```

1.3. Backing Up MongoDB Data

Before upgrading NetBrain Integrated Edition, 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 Appendix: 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, see Appendix: Dumping MongoDB data for another way to back up the data, and see Appendix: Restoring Dumped MongoDB data to restore the data.

The following section 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 `service mongodnetbrain stop` command to stop the MongoDB service.

      > **Note**: If you modified the MongoDB service name in the **install.conf** file during the MongoDB installation, you must replace the service name accordingly.
      >
      > **Tip:** You can always confirm the MongoDB service name by executing the `crontab -l` command.

   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 following command to create a directory under the **/etc** directory to save the backup data.

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

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

4. Run the `cd /home/mongodb` command to navigate to the **/home/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.
>
> - For a freshly installed system, the default directory is **/usr/lib/mongodb**.

5. Run the `du -hs data` command under the **/usr/lib/mongodb** directory to check the total size of MongoDB backup data.

6. Run the `cp -a data /etc/mongodb_databk` command under the **/usr/lib/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 `service mongodnetbrain start` command to start the MongoDB service.

1.4. Upgrading MongoDB

Pre-Upgrade Task

Ensure you have upgraded your OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8, 64-bit** or **CentOS 7.5/7.6/7.7/7.8, 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, don't 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, **netbraintemp03**.

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

3. Run the `cd /opt/netbraintemp03` command to navigate to the **/opt/netbraintemp03** directory.

4. Download the installation package.

   - **<u>Option 1:</u>** If the Linux server has no access to the Internet, obtain the **mongodb-linux-x86_64-rhel7-4.0.6-8.0.3.tar.gz** file from NetBrain and upload it to the **/opt/netbraintemp03** directory by using a file transfer tool.
   - **<u>Option 2:</u>** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/mongodb-linux-x86_64-rhel7-4.0.6-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to directly download the **mongodb-linux-x86_64-rhel7-4.0.6-8.0.3.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-rhel7-4.0.6-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to extract installation files.

```
[root@centos netbraintemp03]# tar -zxvf mongodb-linux-x86_64-rhel7-4.0.6-8.0.3.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 mongodnetbrain` command to restart the MongoDB service.

8. Run the `./upgrade.sh` command under the **upgrade_single_node** directory.

> **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.

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 Mon 2020-07-13 15:16:45 EDT; 1min 1s ago
   Process: 3025 ExecStop=/usr/bin/pkill mongod (code=exited, status=0/SUCCESS)
   Process: 3029 ExecStart=/bin/mongod -f /etc/mongodb/mongod.conf (code=exited,
status=0/SUCCESS)
   Main PID: 3031 (mongod)
   Memory: 181.4M (limit: 6.8G)
...
```

> **Tip:** It is highly recommended to run the `rm -rf /opt/netbraintemp03/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

Ensure you have upgraded your OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8, 64-bit** or **CentOS 7.5/7.6/7.7/7.8, 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, don't 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, **netbraintemp03**.

3. Run the `cd /opt/netbraintemp03` command to navigate to the **/opt/netbraintemp03** directory.

4. Download the installation package.

- **Option 1:** If the Linux server has no access to the Internet, obtain the **elasticsearch-linux-x86_64-rhel7-6.7.2-8.0.3.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp03** directory by using a file transfer tool.
- **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/elasticsearch-linux-x86_64-rhel7-6.7.2-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to directly download the **elasticsearch-linux-x86_64-rhel7-6.7.2-8.0.3.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-rhel7-6.7.2-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to extract installation files.

```
[root@centos netbraintemp03]# tar -zxvf elasticsearch-linux-x86_64-rhel7-6.7.2-8.0.3.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.

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 Mon 2020-07-13 15:28:12 EDT; 1min 15s ago
     Docs: http://www.elastic.co
 Main PID: 7751 (java)
    Memory: 4.2G
```

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" : "6.7.2",
    "build_flavor" : "oss",
    "build_type" : "rpm",
    "build_hash" : "56c6e48",
    "build_date" : "2019-04-29T09:05:50.290371Z",
    "build_snapshot" : false,
    "lucene_version" : "7.7.0",
    "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/netbraintemp03/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

Ensure you have upgraded your OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8, 64-bit** or **CentOS 7.5/7.6/7.7/7.8, 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, don't 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, **netbraintemp03**.
3. Run the `cd /opt/netbraintemp03` command to navigate to the **/opt/netbraintemp03** 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-rhel7-8.0.3.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp03** directory by using a file transfer tool.
   - **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/netbrain-licenseagent-linux-x86_64-rhel7-8.0.3.tar.gz` command under the **/opt/netbraintemp03** 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-rhel7-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to extract installation files.

```
[root@localhost netbraintemp03]# tar -zxvf netbrain-licenseagent-linux-x86_64-rhel7-8.0.3.tar.gz
License/
License/config/
License/config/install_licenseagent.conf
License/config/setup.conf
...
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.

   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: RPM package list:
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 Mon 2020-07-13 15:35:39 EDT; 4min 11s ago
  Main PID: 10668 (licensed)
   CGroup: /system.slice/netbrainlicense.service
           └─10668 /usr/bin/netbrainlicense/licensed -f /etc/netbrainlicense/licensed.conf

Jul 13 15:35:39 netbrain_data_server systemd[1]: Starting NetBrain license agent service...
Jul 13 15:35:39 netbrain_data_server systemd[1]: Started NetBrain license agent service.
```

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 your OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8, 64-bit** or **CentOS 7.5/7.6/7.7/7.8, 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, don't 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, **netbraintemp03**.

3. Run the `cd /opt/netbraintemp03` command to navigate to the **/opt/netbraintemp03** directory.

4. Download the installation package.

   - **Option 1:** If the Linux server has no access to the Internet, obtain the **redis-linux-x86_64-rhel7-6.0.4-8.0.3.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp03** directory by using a file transfer tool.
   - **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/redis-linux-x86_64-rhel7-6.0.4-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to directly download the **redis-linux-x86_64-rhel7-6.0.4-8.0.3.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-rhel7-6.0.4-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to extract installation files.

```
[root@localhost netbraintemp03]# tar -zxvf redis-linux-x86_64-rhel7-6.0.4-8.0.3.tar.gz
redis/
redis/config/
...
redis/config/setup.conf
...
redis/install.sh
...
```

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, see Appendix: Editing a File with VI Editor for more details.

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

#Note= Other than the username and password, other entries
#can only contain letters and numbers, and should start with a letter.

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

```
# 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.
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' or 'slave')
NodeRole=master
# This option will be used to install sentinel on master node. It can only be 'yes' or 'no'
MasterInstallSentinel=no
#Master Node (Master Node can support ip address, hostname or FQDN and is used if the Mode is
cluster and used in slave node)
MasterNode=
# Sentinel Port is used to start the redis sentinel service on specified port. We use default
port 6380.
SentinelPort=6380

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

# TLS. It can only be 'yes' or 'no'
UseSSL=no
Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem
# Stunnel Port is used to start the stunnel service on specified port. We use default port
7000.
StunnelPort=7000
# Stunnel Sentinel Port is used to start the redis sentinel service on specified port.
We use default port 7001 for SSL. this is needed only for slave node.
StunnelSentinelPort=7001
```

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: Creating log file
INFO: checking date
INFO: Preprocessing SUCCEEDED
INFO: Starting to check system
...
  Collecting system information SUCCEEDED.
INFO: System checking SUCCEEDED
```

```
INFO: Dependent packages checking
INFO: Dependent packages checking SUCCEEDED
INFO: checking password
INFO: checking useSSL
INFO: checking MasterInstallSentinel
INFO: checking ResourceLimit
INFO: checking Port
INFO: Mode is standalone
INFO: Role of node is master
INFO: Added Ports to firewall successfully.
INFO: Configuration parameters checking SUCCEEDED
INFO: installing openssl-devel.
INFO: openssl-devel has already been installed.
INFO: Installing /opt/netbraintemp03/redis/sources/redis-6.0.4-1.e17.x86_64.rpm
Preparing...                          ########################################
Updating / installing...
redis-6.0.4-1.el7                     ########################################
INFO: Official rpm package installing SUCCEEDED
INFO: Configuration parameters updating SUCCEEDED
INFO: Permission assigning SUCCEEDED
always madvise [never]
Created symlink from /etc/systemd/system/multi-user.target.wants/redis.service to
/usr/lib/systemd/system/redis.service.
 redis.service - Redis
   Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-01-14 00:38:49 EST; 37min ago
 Main PID: 13240 (redis-server)
   Memory: 1.8M
   CGroup: /system.slice/redis.service
           13240 /sbin/redis-server *:6379

Jul 13 15:47:04 netbrain_data_server systemd[1]: Started Redis.
INFO: Checking redis Status
INFO: Verification SUCCEEDED
INFO: Successfully installed Redis
INFO: Backup uninstall.sh SUCCEEDED
INFO: Backup fix_releaseinfo.json SUCCEEDED
```

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: 13240 (redis-server)
 Memory: 1.8M
...
```

> **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.

> **Tip:** It is highly recommended to run the `rm -rf /opt/netbraintemp03/redis/config/setup.conf` command to delete the **setup.conf** file from the server after Redis is successfully installed because the file may cause security vulnerability.

Parameters

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

Parameter	Default Value	Description
Password	`admin`	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. `{ } [ ] : " , ' | < > @ & ^ % \` and `spaces`
Mode	`standalone`	Set whether to enable cluster deployment. Keep the default value for a standalone deployment.
Port	`6379`	Specify the port number that the master Redis node listens to.
DataPath	`/var/lib/redis/`	Specify the storage path for all data files of Redis.
LogPath	`/var/log/redis/`	Specify the storage path for all log files of Redis.
NodeRole	`master`	Set the role for the current node. Available options are **master**, **slave**, and **sentinel**. Keep the default value for a standalone deployment.
MasterNode		This parameter is required only for cluster deployments.
SentinelPort	`6380`	The port number that the slave or sentinel Redis node listens to.
ResourceLimit	`no`	Set whether to limit the system resource usage for Redis.
CPULimit	`100%`	The maximum CPU utilization of the machine that can be consumed by Redis.
MemoryLimit	`100%`	The maximum memory capacity of the machine that can be consumed by Redis.
UseSSL	`no`	Set whether to enable the encrypted connections to Redis by using SSL. **Note:** Redis itself does not support SSL. It uses stunnel as SSL service agent. Stunnel will be automatically installed together with Redis.
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.

Parameter	Default Value	Description
StunnelPort	`7000`	Specify the port number for stunnel to establish an SSL encrypted tunnel on master and slave Redis node. **Note:** It is required only if **UseSSL** is enabled.
StunnelSentinelPort	`7001`	Specify the port number for stunnel to establish an SSL encrypted tunnel on the sentinel Redis node. **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 your OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8, 64-bit** or **CentOS 7.5/7.6/7.7/7.8, 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, don't 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.
>
> **Note:** 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.

Installing RabbitMQ on Linux

> **Note:** 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` command to check whether **socat** and **logrotate** have been installed on the server. If it has not been installed, you can choose either option below to install the dependencies.
>
> **- Online Install:** run the `yum -y install socat` and `yum -y install logrotate` command to install them online.
>
> **- Offline Install:** see Appendix: Offline Installing Third-party Dependencies for more details.

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, **netbraintemp03**.
3. Run the `cd /opt/netbraintemp03` command to navigate to the **/opt/netbraintemp03** directory.
4. Download the installation package.
   - **Option 1:** If the Linux server has no access to the Internet, obtain the **rabbitmq-linux-x86_64-rhel7-3.8.1-8.0.3.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp03** directory by using a file transfer tool.
   - **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/rabbitmq-linux-x86_64-rhel7-3.8.1-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to directly download the **rabbitmq-linux-x86_64-rhel7-3.8.1-8.0.3.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-rhel7-3.8.1-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to extract installation files.

```
[root@localhost netbraintemp03]# tar -zxvf rabbitmq-linux-x86_64-rhel7-3.8.1-8.0.3.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, see Appendix: Editing a File with VI Editor for more details.

```
[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=admin

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

# A unique cluster string 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. Two roles can be configured:
# master or slave. If the role of the current node is slave, you must specify
# the hostname of the master node in MasterNode.
NodeRole=master
MasterNode=localhost

# Resource limitation
ResourceLimit=no

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

# TLS
UseSSL=no
CertFile=/etc/ssl/cert.pem
KeyFile=/etc/ssl/key.pem
# Port
TcpPort=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: Creating installation log file
INFO: Preprocessing SUCCEED
INFO: Start checking system
INFO: 2020-07-13 16-04-17.475: Collecting system information SUCCEEDED.
INFO: Start checking date
INFO: Start checking rhel7x
selinux-policy version: 3.13.1
INFO: Starting to check if rpm exists
INFO: Start checking system
INFO: Start checking required CPU
INFO: Start checking minimum memory
INFO: System checking SUCCEEDED
INFO: Dependent packages checking
INFO: Dependent packages checking SUCCEEDED
INFO: checking UseSSL
INFO: checking ResourceLimit
INFO: Mode is standalone
INFO: Role of node is master
INFO: Added Ports to firewall successfully.
INFO: Configuration parameters checking SUCCEEDED
selinux-policy version: 3.13.1
installing openssl-devel.
INFO: openssl-devel has already been installed.
INFO: Installing /root/opt/netbraintemp03/rabbitmq/sources/erlang-22.1.7-1.el7.x86_64.rpm
warning: /root/opt/netbraintemp03/rabbitmq/sources/erlang-22.1.7-1.el7.x86_64.rpm: Header V4
RSA/SHA1 Signature, key ID 6026dfca: NOKEY
Preparing...                          ########################################
Updating / installing...
1:erlang-22.1.7-1.el7                 ########################################
INFO: Installing /opt/netbraintemp03/rabbitmq/sources/rabbitmq-server-3.8.1-1.el7.noarch.rpm
warning: /opt/netbraintemp03/rabbitmq/sources/rabbitmq-server-3.8.1-1.el7.noarch.rpm: Header V4
RSA/SHA256 Signature, key ID 6026dfca: NOKEY
Preparing...                          ########################################
Updating / installing...
1:rabbitmq-server-3.8.1-1.el7         ########################################
INFO: Official rpm package installing SUCCEEDED
INFO: Configuration parameters updating SUCCEEDED
INFO: Permission setting SUCCEED
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: 17679 (beam.smp)
   Status: "Initialized"
   Memory: 80.7M
   ...
INFO: Adding HA policy SUCCEEDED
   ...
   Active: active (running) since Mon 2020-07-13 16:05:23 EDT; 7ms ago
INFO: Verification SUCCEEDED
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: 19685 (beam.smp)
   Status: "Initialized"
   Memory: 74.5M
...
```

> **Tip:** It is highly recommended to run the `rm -rf /opt/netbraintemp03/rabbitmq/config/setup.conf` command to delete the **setup.conf** file from the server after RabbitMQ is successfully installed because the file may cause security vulnerability.

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	`admin`	Specify the admin password used to connect to RabbitMQ.
Mode	`standalone`	Set whether to enable cluster deployment. Modify it to **standalone** for a standalone deployment.
ClusterId	`rabbitmqcluster`	Specify the cluster id used by all nodes to join the cluster. **Note:** This parameter is required only for cluster deployments.
NodeRole	`master`	Set the role for the current node. Available options are **master** and **slave**. Keep the default value for a standalone deployment.

<table>
<tr><th>Parameter</th><th>Default Value</th><th>Description</th></tr>
<tr><td><b>MasterNode</b></td><td><code>localhost</code></td><td>This parameter is required only for cluster deployments. Keep the default value as it is for a standalone deployment.</td></tr>
<tr><td><b>ResourceLimit</b></td><td><code>no</code></td><td>Set whether to limit the system resource usage for RabbitMQ.</td></tr>
<tr><td><b>CPULimit</b></td><td><code>100%</code></td><td>Specify the maximum CPU utilization of the machine that can be consumed by RabbitMQ.</td></tr>
<tr><td><b>MemoryLimit</b></td><td><code>100%</code></td><td>Specify the maximum memory capacity of the machine that can be consumed by RabbitMQ.</td></tr>
<tr><td><b>UseSSL</b></td><td><code>no</code></td><td>Set whether to enable the encrypted connections to RabbitMQ by using SSL.

<b>Tip:</b> If <b>UseSSL</b> is set to <b>yes</b>, you can follow the steps below to modify RabbitMQ Plugin config file after service monitor is installed.

1) Run the <code>vi /etc/netbrain/nbagent/check/rabbitmq.yaml</code> command to open RabbitMQ Plugin config file.

2) Set the <b>ssl</b> value to <b>true</b> and save the changes. For how to modify the configuration file, see Appendix: Editing a File with VI Editor for more details.
<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','RMClientC
allback','ETL_Task']
          endWith: ['IndexDriver']
</pre></td></tr>
<tr><td><b>Certificate</b></td><td><code>/etc/ssl/cert.pem</code></td><td>Specify the storage path for all the certificates and key files used for SSL authentication.

<b>Note:</b> It is required only if <b>UseSSL</b> is enabled.</td></tr>
<tr><td><b>PrivateKey</b></td><td><code>/etc/ssl/key.pem</code></td><td>Specify the name of SSL private key file.

<b>Note:</b> It is required only if <b>UseSSL</b> is enabled.</td></tr>
<tr><td><b>TcpPort</b></td><td><code>5672</code></td><td>Specify the port number that RabbitMQ service listens to.</td></tr>
<tr><td><b>LogPath</b></td><td><code>/var/log/rabbitmq</code></td><td>Specify the directory to save logs of RabbitMQ.</td></tr>
</table>

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 Web/Web API Server

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

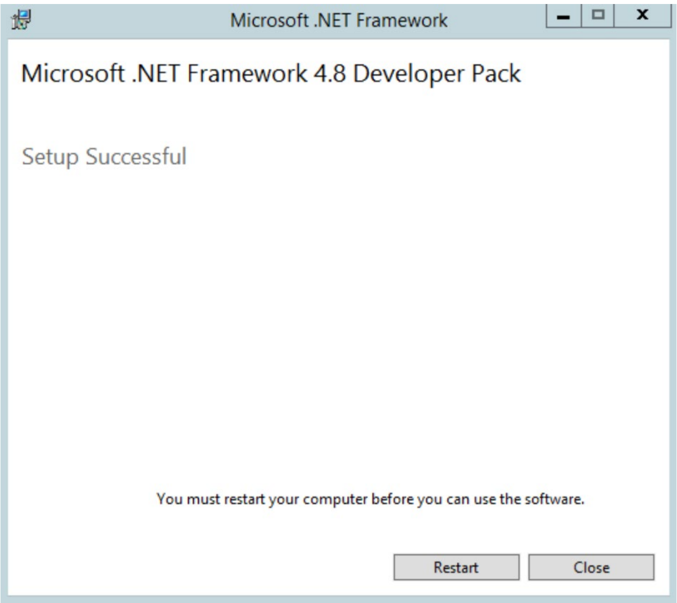
Complete the following steps to upgrade Web API Server and Web Server on the same machine with administrative privileges.

1. Download the **netbrain-ie-windows-x86_64-8.0.3.zip** file from http://download.netbraintech.com/netbrain-ie-windows-x86_64-8.0.3.zip and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-8.0.3.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-8.0.3.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.



Microsoft .NET Framework

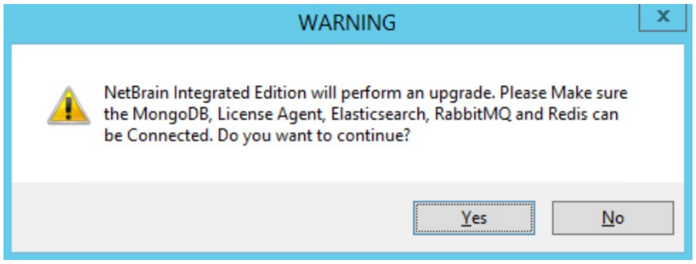
Microsoft .NET Framework 4.8 Developer Pack

Setup Successful

You must restart your computer before you can use the software.

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.

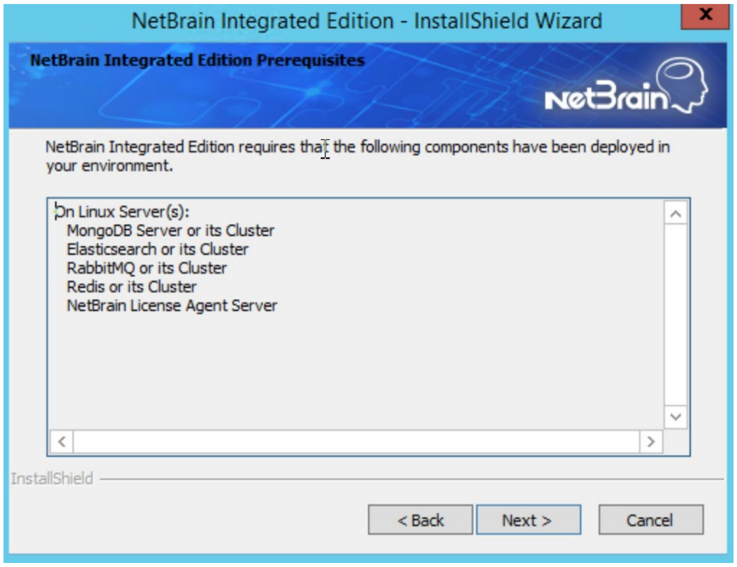


WARNING

NetBrain Integrated Edition will perform an upgrade. Please Make sure the MongoDB, License Agent, Elasticsearch, RabbitMQ and Redis can be Connected. Do you want to continue?

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**.



NetBrain Integrated Edition - InstallShield Wizard

NetBrain Integrated Edition Prerequisites

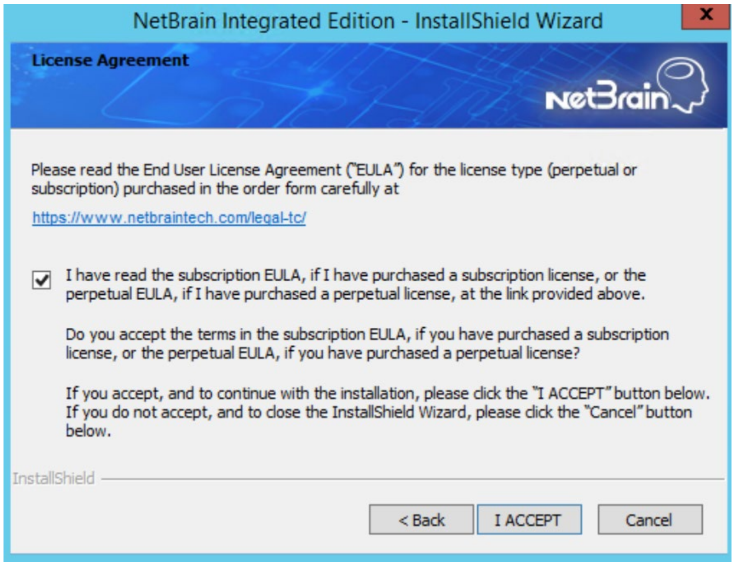
NetBrain Integrated Edition requires that the following components have been deployed in your environment.

On Linux Server(s):
MongoDB Server or its Cluster
Elasticsearch or its Cluster
RabbitMQ or its Cluster
Redis or its Cluster
NetBrain License Agent Server

InstallShield
< Back
Next >
Cancel

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**.



Please read the End User License Agreement ("EULA") for the license type (perpetual or subscription) purchased in the order form carefully at

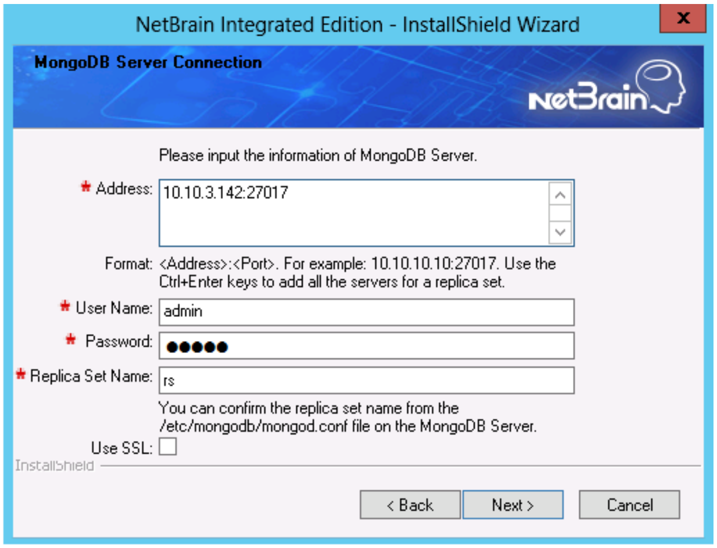
https://www.netbraintech.com/legal-tc/

☑ 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.

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 click the "I ACCEPT" button below. If you do not accept, and to close the InstallShield Wizard, please click the "Cancel" button below.

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



NetBrain Integrated Edition - InstallShield Wizard
MongoDB Server Connection
NetBrain

Please input the information of MongoDB Server.

* Address: 10.10.3.142:27017

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: admin

* Password: ●●●●●

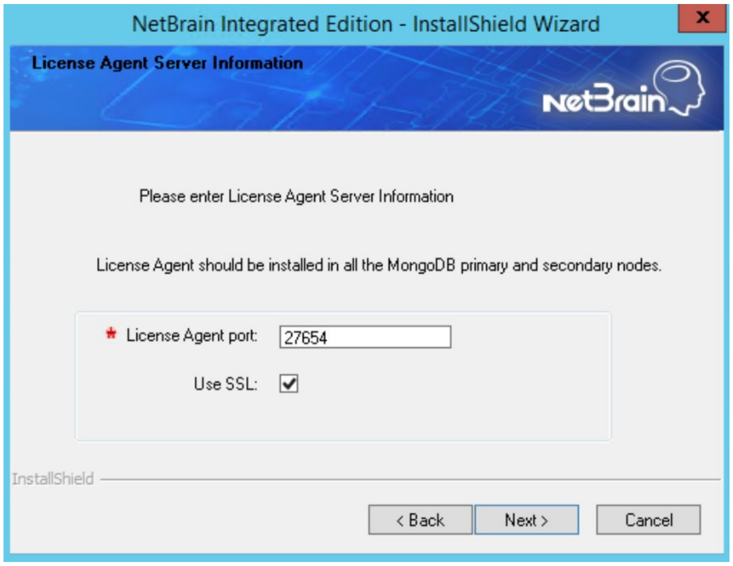
* Replica Set Name: rs

You can confirm the replica set name from the /etc/mongodb/mongod.conf file on the MongoDB Server.

Use SSL: □

InstallShield
< Back
Next >
Cancel

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



NetBrain Integrated Edition - InstallShield Wizard
License Agent Server Information
NetBrain

Please enter License Agent Server Information

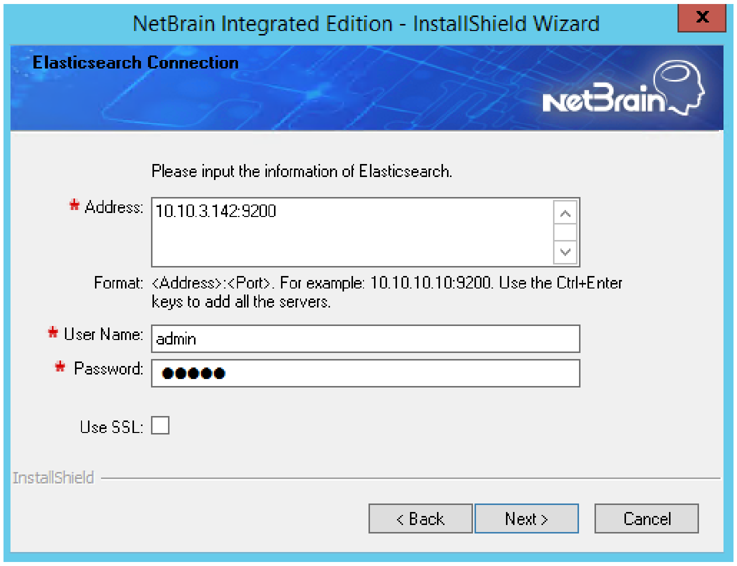
License Agent should be installed in all the MongoDB primary and secondary nodes.

* License Agent port: 27654

Use SSL: ☑

InstallShield
< Back
Next >
Cancel

10) On the Elasticsearch Connection page, enter the password that you created when installing Elasticsearch, and then click **Next**.



NetBrain Integrated Edition - InstallShield Wizard

Elasticsearch Connection

Please input the information of Elasticsearch.

* Address: 10.10.3.142:9200

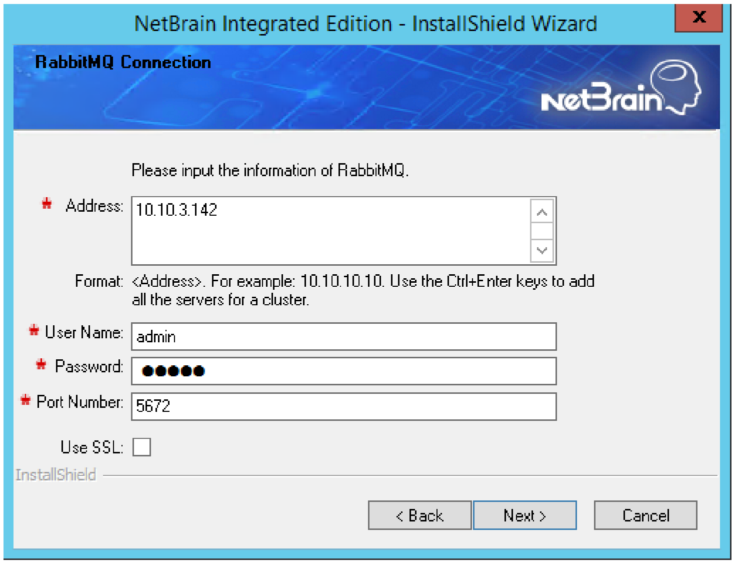
Format: <Address>:<Port>. For example: 10.10.10.10:9200. Use the Ctrl+Enter keys to add all the servers.

* User Name: admin

* Password: ●●●●●

Use SSL: □

11) On the RabbitMQ Connection page, enter the IP address of the Linux server and the admin password that you created when installing RabbitMQ, and then click **Next**.



NetBrain Integrated Edition - InstallShield Wizard

RabbitMQ Connection

Please input the information of RabbitMQ.

* 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.

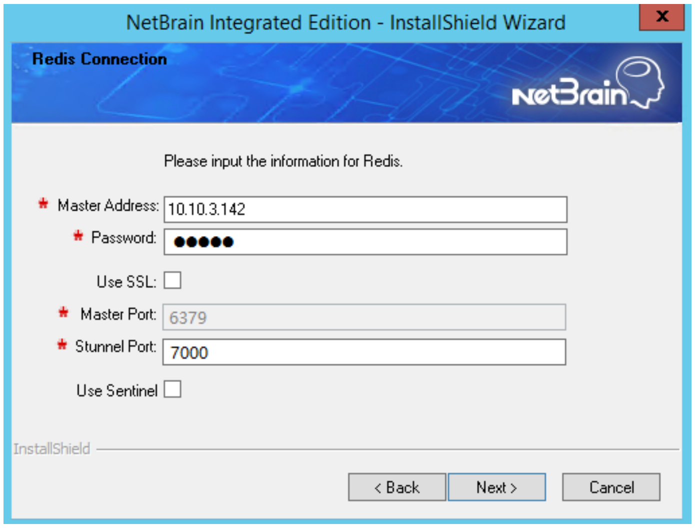
* User Name: admin

* Password: ●●●●●

* Port Number: 5672

Use SSL: □

12) On the Redis Connection page, enter the IP address of the Linux server and the admin password that you created when installing Redis, and then click **Next**.


NetBrain Integrated Edition - InstallShield Wizard

Redis Connection

Please input the information for Redis.

* Master Address: 10.10.3.142

* Password: ●●●●●

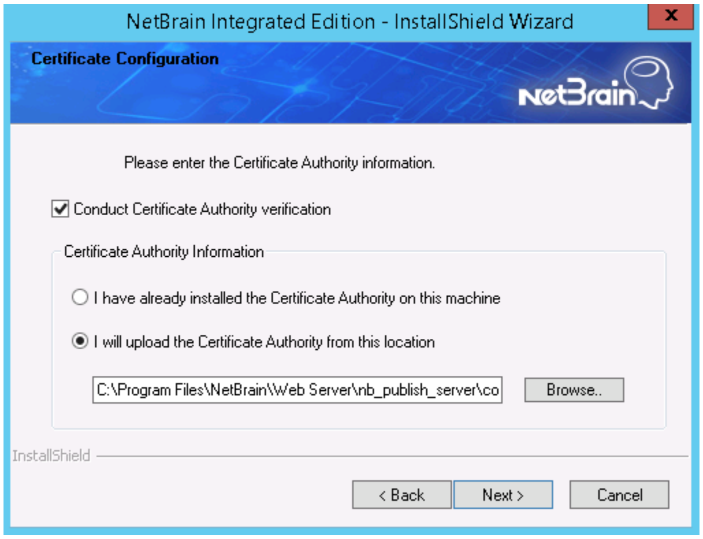
Use SSL: □

* Master Port: 6379

* Stunnel Port: 7000

Use Sentinel □

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 CA certificate file and then click **Next**.


NetBrain Integrated Edition - InstallShield Wizard

Certificate Configuration

Please enter the Certificate Authority information.

☑ Conduct Certificate Authority verification

Certificate Authority Information

○ I have already installed the Certificate Authority on this machine

● I will upload the Certificate Authority from this location

C:\Program Files\NetBrain\Web Server\nb_publish_server\co

To authenticate CA:

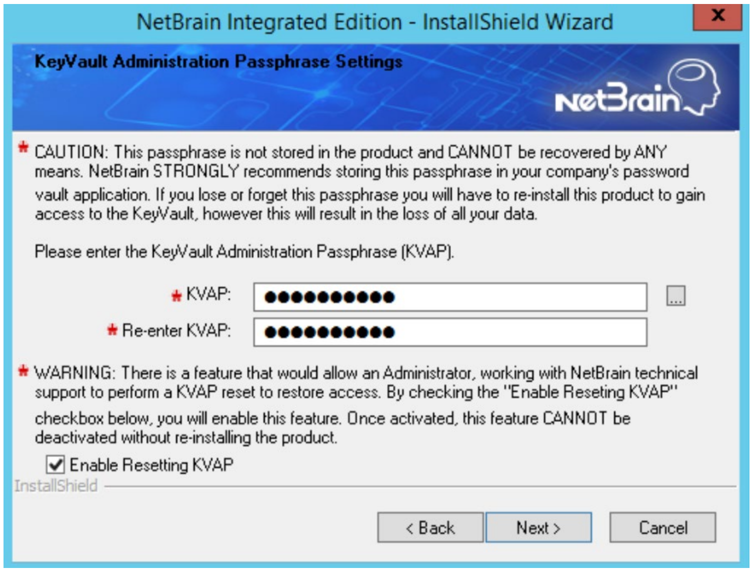
a) Select the **Conduct Certificate Authority verification** check box.

b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**; otherwise, select **I have already installed the Certificate Authority on this machine**.

> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met if you select **I have already installed the Certificate Authority on this machine:**
>
> - 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**.



NetBrain Integrated Edition - InstallShield Wizard

KeyVault Administration Passphrase Settings

* 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.

Please enter the KeyVault Administration Passphrase (KVAP).

* KVAP: ●●●●●●●●●●●

* Re-enter KVAP: ●●●●●●●●●●●

* 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 Reseting KVAP" checkbox below, you will enable this feature. Once activated, this feature CANNOT be deactivated without re-installing the product.

☑ Enable Resetting KVAP

> **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) 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.

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:\ NBIEInstall** drive of this machine directly to the **C:\ NBIEInstall** drive of the machines where Worker Server, Task Engine, and Front Server Controller will be installed.

1.10. Upgrading Worker Server

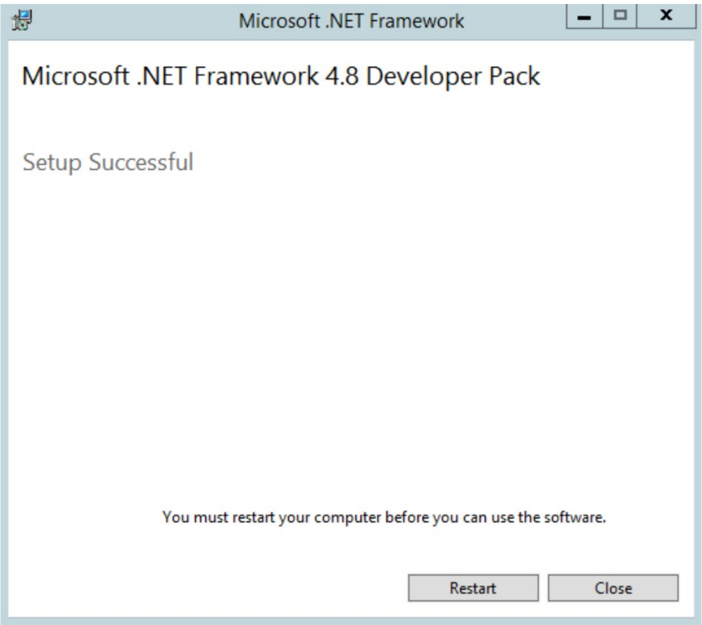
> **Note:** If you have deployed a Worker Server Cluster for load balancing, you can repeat the following steps to upgrade the Worker Servers on separate machines.
>
> **Note:** Make sure all cluster members have the same configurations for MongoDB, License Agent, Elasticsearch, RabbitMQ, and Redis. And your network configurations allow communications among them.
>
> **Note:** Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

Complete the following steps with administrative privileges.

1. Download the **netbrain-ie-windows-x86_64-8.0.3.zip** file from http://download.netbraintech.com/netbrain-ie-windows-x86_64-8.0.3.zip and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-8.0.3.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-8.0.3.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.



Microsoft .NET Framework

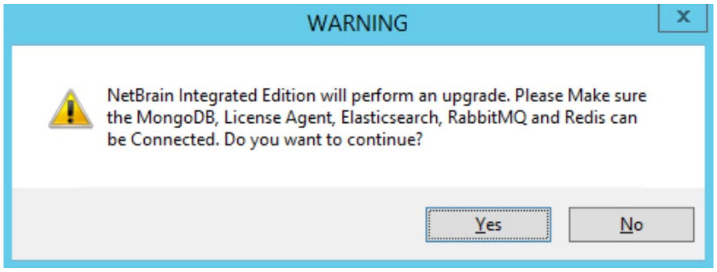
Microsoft .NET Framework 4.8 Developer Pack

Setup Successful

You must restart your computer before you can use the software.

2) Stop the service of worker server manually before continuing the upgrade.

3) Click **Yes** in the dialog box to initiate the upgrade.

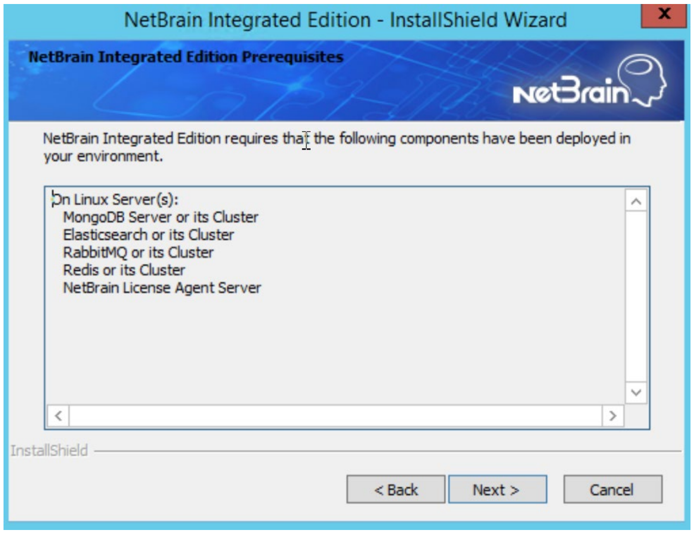


WARNING

NetBrain Integrated Edition will perform an upgrade. Please Make sure the MongoDB, License Agent, Elasticsearch, RabbitMQ and Redis can be Connected. Do you want to continue?

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**.



NetBrain Integrated Edition - InstallShield Wizard

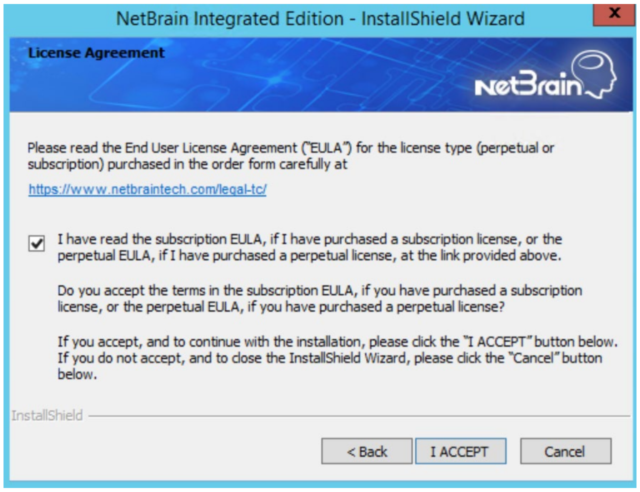
NetBrain Integrated Edition Prerequisites

NetBrain Integrated Edition requires that the following components have been deployed in your environment.

```
On Linux Server(s):
  MongoDB Server or its Cluster
  Elasticsearch or its Cluster
  RabbitMQ or its Cluster
  Redis or its Cluster
  NetBrain License Agent Server
```

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**.



Please read the End User License Agreement ("EULA") for the license type (perpetual or subscription) purchased in the order form carefully at

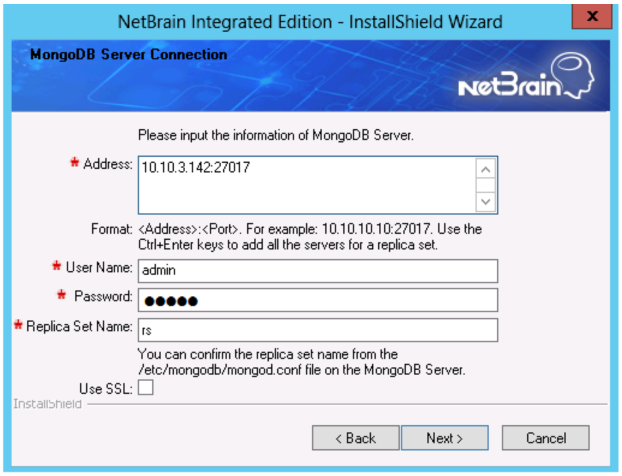
https://www.netbraintech.com/legal-tc/

☑ 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.

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 click the "I ACCEPT" button below. If you do not accept, and to close the InstallShield Wizard, please click the "Cancel" button below.

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


NetBrain Integrated Edition - InstallShield Wizard
MongoDB Server Connection
NetBrain

Please input the information of MongoDB Server.

* Address: 10.10.3.142:27017

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: admin

* Password: ●●●●●

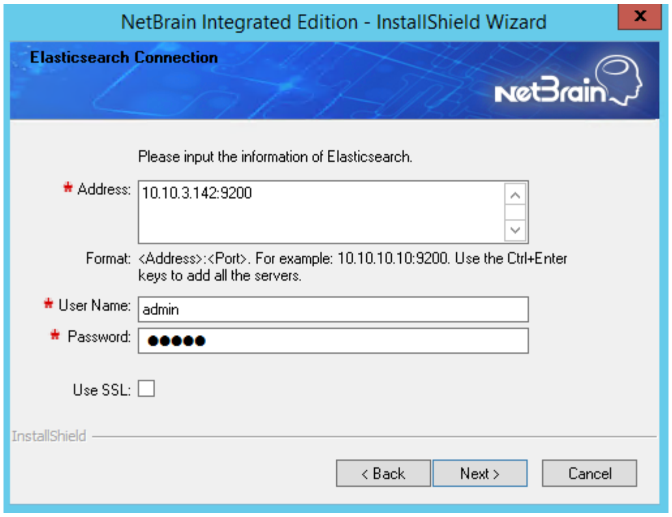
* Replica Set Name: rs

You can confirm the replica set name from the /etc/mongodb/mongod.conf file on the MongoDB Server.

Use SSL: □

InstallShield
< Back
Next >
Cancel

9) On the Elasticsearch Connection page, enter the password that you created when installing Elasticsearch, and then click **Next**.



Please input the information of Elasticsearch.

* Address: 10.10.3.142:9200

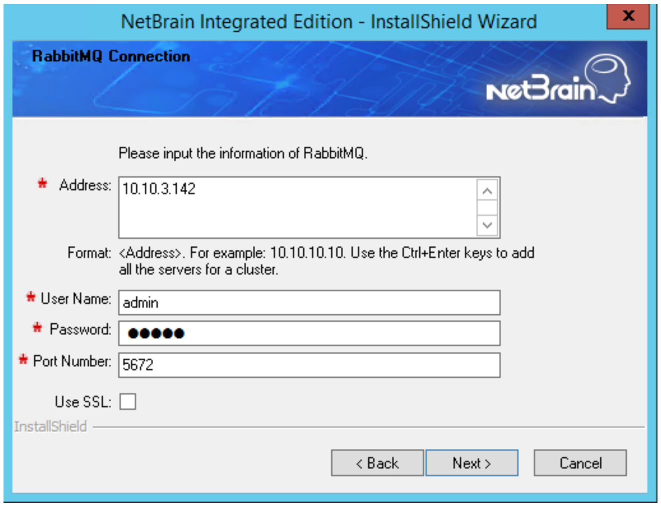
Format: <Address>:<Port>. For example: 10.10.10.10:9200. Use the Ctrl+Enter keys to add all the servers.

* User Name: admin

* Password: ●●●●●

Use SSL: □

10) On the RabbitMQ Connection page, enter the admin password that you created when installing RabbitMQ, and then click **Next**.



Please input the information of RabbitMQ.

* 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.

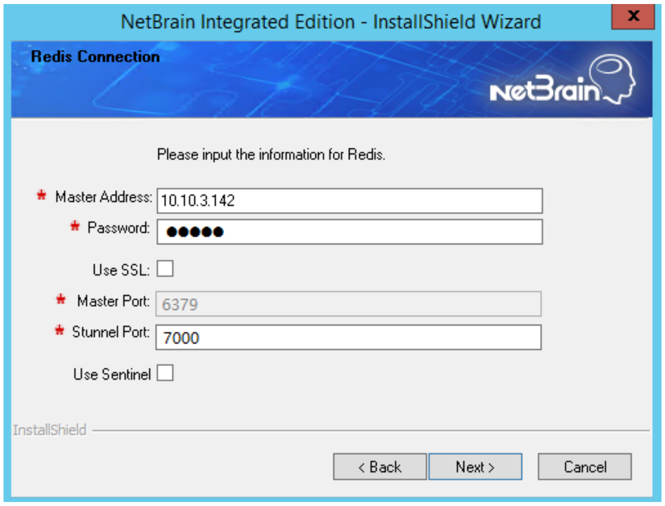
* User Name: admin

* Password: ●●●●●

* Port Number: 5672

Use SSL: □

11) On the Redis Connection page, enter the admin password that you created when installing Redis, and then click **Next**.



Please input the information for Redis.

* Master Address: 10.10.3.142

* Password: ●●●●●

Use SSL: □

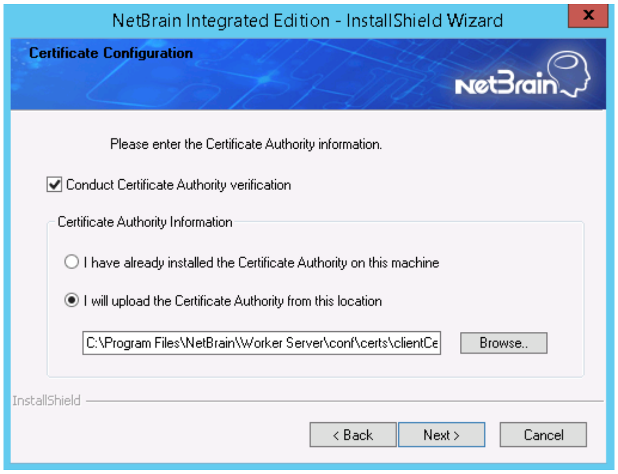
* Master Port: 6379

* Stunnel Port: 7000

Use Sentinel □

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 CA certificate file

and then click **Next**.



NetBrain Integrated Edition - InstallShield Wizard

Certificate Configuration

Please enter the Certificate Authority information.

☑ Conduct Certificate Authority verification

Certificate Authority Information

○ I have already installed the Certificate Authority on this machine

● I will upload the Certificate Authority from this location

C:\Program Files\NetBrain\Worker Server\conf\certs\clientCe

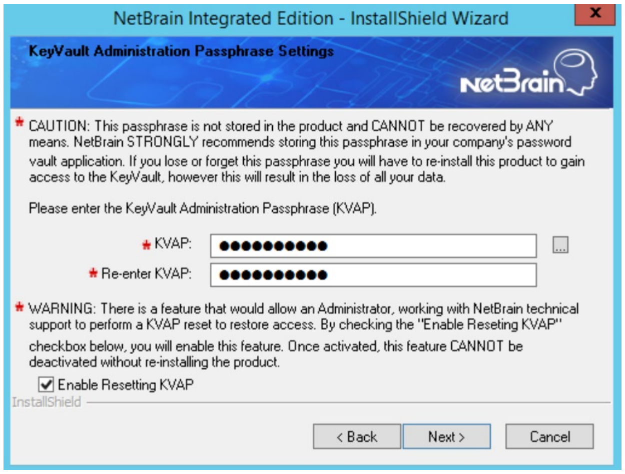
To authenticate CA:

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**; otherwise, select **I have already installed the Certificate Authority on this machine**.

> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met if you select **I have already installed the Certificate Authority on this machine:**
>
> - 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**.



NetBrain Integrated Edition - InstallShield Wizard

KeyVault Administration Passphrase Settings

* 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.

Please enter the KeyVault Administration Passphrase (KVAP).

* KVAP: ●●●●●●●●●●●

* Re-enter KVAP: ●●●●●●●●●●●

* 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 Reseting KVAP" checkbox below, you will enable this feature. Once activated, this feature CANNOT be deactivated without re-installing the product.

☑ Enable Resetting KVAP

> **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.

14) 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.

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

> **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.

1.11. Installing Task Engine

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

Depending on your network scale, you can deploy either a standalone Task Engine, or two for high availability.

Complete the following steps with administrative privileges.

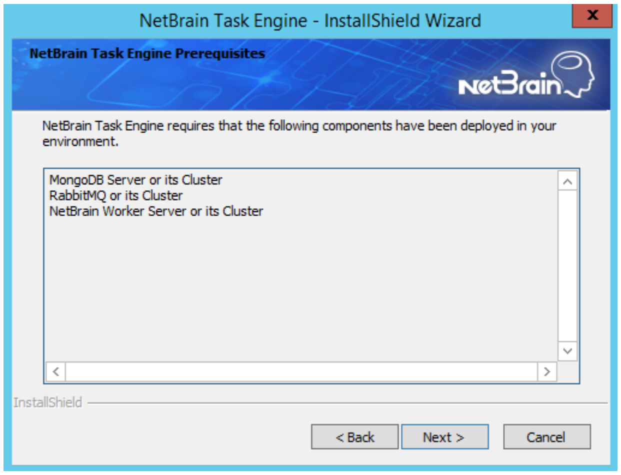
1. Download the **netbrain-taskengine-windows-x86_64-8.0.3.zip** file from http://download.netbraintech.com/netbrain-taskengine-windows-x86_64-8.0.3.zip and save it in your local folder.

2. Extract installation files from the **netbrain-taskengine-windows-x86_64-8.0.3.zip** file.

3. Right-click the **netbrain-taskengine-windows-x86_64-8.0.3.exe** file, and then select **Run as administrator** to start the Installation Wizard.

   1) On the Welcome page, click **Next**.

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



NetBrain Task Engine - InstallShield Wizard
NetBrain Task Engine Prerequisites
NetBrain

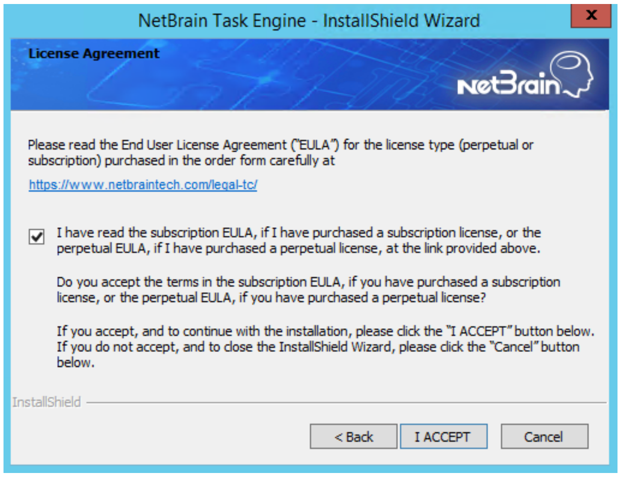
NetBrain Task Engine requires that the following components have been deployed in your environment.

MongoDB Server or its Cluster
RabbitMQ or its Cluster
NetBrain Worker Server or its Cluster

InstallShield
< Back
Next >
Cancel

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**.



Please read the End User License Agreement ("EULA") for the license type (perpetual or subscription) purchased in the order form carefully at https://www.netbraintech.com/legal-tc/

☑ 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.

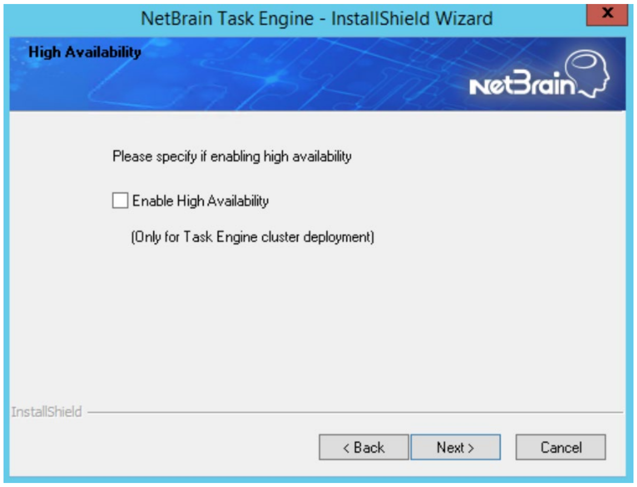
Do you accept the terms in the subscription EULA, if you have purchased a subscription license, or the perpetual EULA, if you have purchased a perpetual license?

If you accept, and to continue with the installation, please click the "I ACCEPT" button below. If you do not accept, and to close the InstallShield Wizard, please click the "Cancel" button below.

5) On the Customer Information page, enter your company name, and then click **Next**.

6) On the Destination Location page, click **Next** to install the Task Engine under the default directory **C:\Program Files\NetBrain\**. If you want to install it under another location, click **Change**.

7) On the High Availability page, leave the **Enable High Availability unchecked**, and then click **Next**.


NetBrain Task Engine - InstallShield Wizard

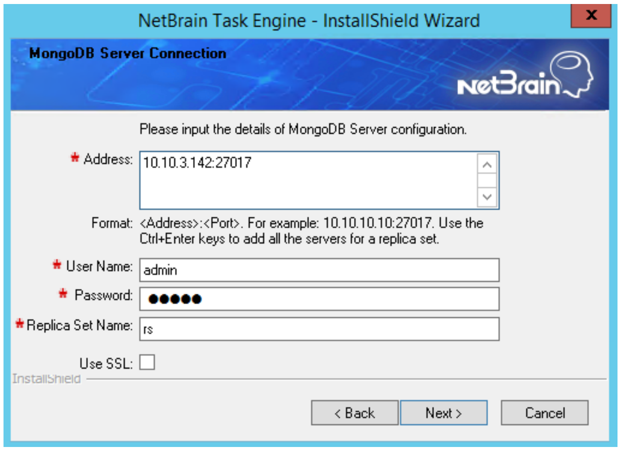
High Availability

Please specify if enabling high availability

☐ Enable High Availability

(Only for Task Engine cluster deployment)

8) On the MongoDB Server Connection page, enter the following information to connect to the MongoDB, and then click **Next**.


NetBrain Task Engine - InstallShield Wizard

MongoDB Server Connection

Please input the details of MongoDB Server configuration.

* Address: 10.10.3.142:27017

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: admin

* Password: ●●●●●

*Replica Set Name: rs

Use SSL: ☐

- **Address** — enter the IP address of MongoDB and the corresponding port number. By default, the port number is **27017**.

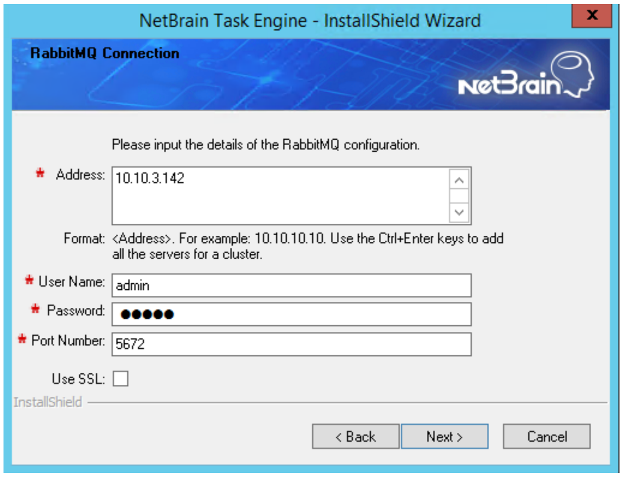
> **Tip:** You can enter the fully qualified domain name (FQDN) of MongoDB if all NetBrain servers are managed in the same domain. For example, `test.netbraintech.com:27017`.

- **User Name** — enter the username that you created when installing MongoDB.
- **Password** — enter the password that you created when installing MongoDB.
- **Replica Set Name** — enter the replica set name of MongoDB. By default, it is **rs**.

> **Note:** If you installed MongoDB by using MongoDB official installation package, you must also set up a replica set name. See the documentation https://docs.mongodb.com/manual/tutorial/deploy-replica-set/ on MongoDB official website for reference.

- **Use SSL** — used to encrypt the connections to MongoDB with SSL. If SSL is enabled on MongoDB, select this check box; otherwise, leave it unchecked.

9) On the RabbitMQ Connection page, enter the following information to connect to 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

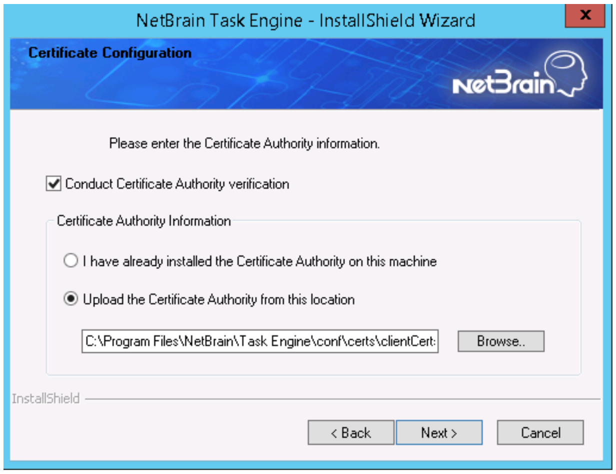
Use SSL: □

- **Address** — enter the IP address of RabbitMQ.

> **Tip:** You can enter the FQDN of RabbitMQ if all NetBrain servers are managed in the same domain.

- **User Name** — enter the admin username that you created when installing RabbitMQ.
- **Password** — enter the admin password corresponding to the username that you created when installing RabbitMQ.
- **Port Number** — enter the port number used by RabbitMQ to communicate with Web API Server, Worker Server, and Task Engine. By default, it is **5672**.
- **Use SSL** — used to encrypt the connections to RabbitMQ with SSL. If SSL is enabled on RabbitMQ, select it; otherwise, leave it unchecked.

10) (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 certificate file and then click **Next**.



NetBrain Task Engine - InstallShield Wizard

Certificate Configuration

Please enter the Certificate Authority information.

☑ Conduct Certificate Authority verification

Certificate Authority Information

○ I have already installed the Certificate Authority on this machine

● Upload the Certificate Authority from this location

C:\Program Files\NetBrain\Task Engine\conf\certs\clientCert:

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**; otherwise, select **I have already installed the Certificate Authority on this machine**.

> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met if you select **I have already installed the Certificate Authority on this machine:**
>
> - 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.

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

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

1.12. Installing Front Server Controller

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

Complete the following steps with administrative privileges.

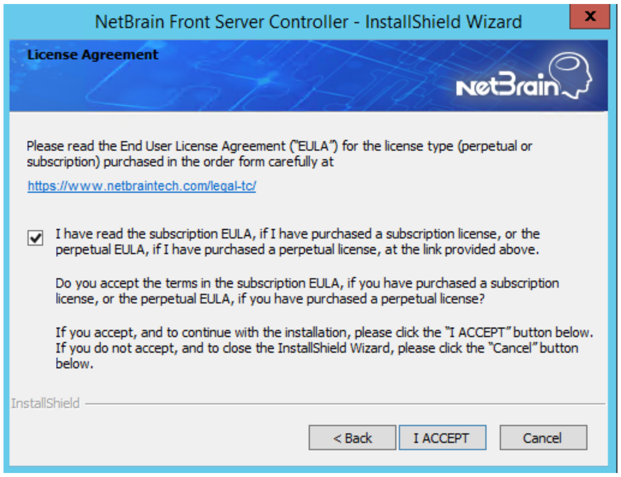
1. Download the **netbrain-frontservercontroller-windows-x86_64-8.0.3.zip** file from http://download.netbraintech.com/netbrain-frontservercontroller-windows-x86_64-8.0.3.zip and save it in your local folder.

2. Extract installation files from the **netbrain-frontservercontroller-windows-x86_64-8.0.3.zip** file.

3. Right-click the **netbrain-frontservercontroller-windows-x86_64-8.0.3.exe** file, and then select **Run as administrator** to start the Installation Wizard.

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

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



Please read the End User License Agreement ("EULA") for the license type (perpetual or subscription) purchased in the order form carefully at
https://www.netbraintech.com/legal-tc/

☑ 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.

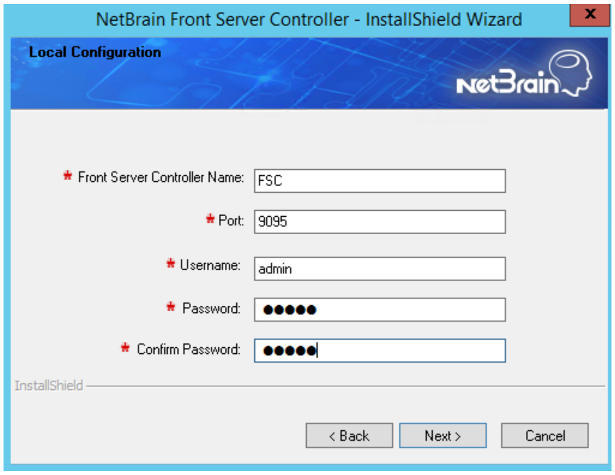
Do you accept the terms in the subscription EULA, if you have purchased a subscription license, or the perpetual EULA, if you have purchased a perpetual license?

If you accept, and to continue with the installation, please click the "I ACCEPT" button below. If you do not accept, and to close the InstallShield Wizard, please click the "Cancel" button below.

4) On the Customer Information page, enter your company name, and then click **Next**.

5) On the Destination Location page, click **Next** to install the Front Server Controller under the default directory **C:\Program Files\NetBrain\**. If you want to install it under another location, click **Change**.

6) On the Local Configuration page, configure the following information, and then click **Next**.



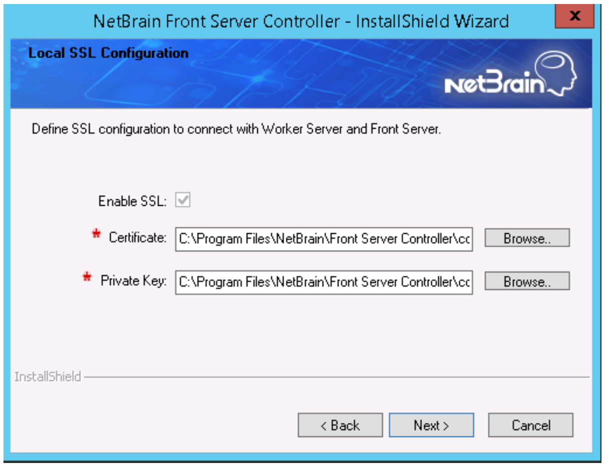
* Front Server Controller Name: FSC
* Port: 9095
* Username: admin
* Password: ●●●●●
* Confirm Password: ●●●●●

- **Front Server Controller Name —** create a name for the controller to authenticate the connections established from Worker Server.

> **Note:** This field cannot contain any of the special characters: `\ / : * ? " < > | . $`.
>
> **Note:** Keep notes of **Front Server Controller Name** as well as **Port**, **Username**, and **Password** because they are required when you allocate tenants to Front Server Controller and register a Front Server.

- **Port —** specify the port number used for the connections from Worker Server and Front Server. By default, it is **9095**.
- **Username —** create a username to authenticate the connections established from Worker Server.
- **Password —** create a password to authenticate the connections established from Worker Server.

7) (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**.



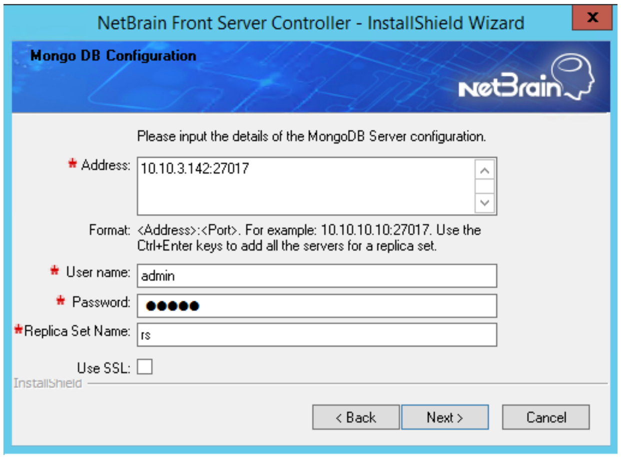
Define SSL configuration to connect with Worker Server and Front Server.

Enable SSL: ☑

* Certificate: C:\Program Files\NetBrain\Front Server Controller\cc

* Private Key: C:\Program Files\NetBrain\Front Server Controller\cc

8) On the MongoDB Connection page, enter the following information to connect to MongoDB and then click **Next**.



Please input the details of the MongoDB Server configuration.

* Address: 10.10.3.142:27017

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: admin

* Password: ●●●●●

*Replica Set Name: rs

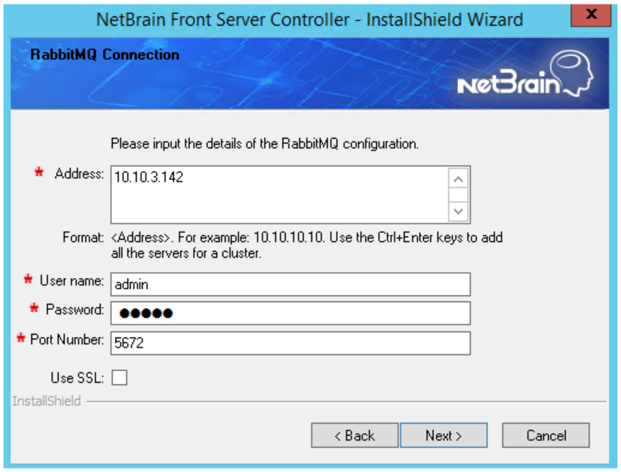
Use SSL: □

- **Address** — enter the IP address of MongoDB and the corresponding port number. By default, the port number is **27017**.

> **Tip:** You can enter the fully qualified domain name (FQDN) of MongoDB if all NetBrain servers are managed in the same domain. For example, `test.netbraintech.com:27017`.

- **User Name** — enter the username that you created when installing MongoDB.
- **Password** — enter the password that you created when installing MongoDB.
- **Replica Set Name** — enter the replica set name of MongoDB. By default, it is **rs**.
- **Use SSL** — used to encrypt the connections to MongoDB with SSL. If SSL is enabled on MongoDB, select this check box; otherwise, leave it unchecked.

9) On the RabbitMQ Connection page, enter the following information to connect RabbitMQ, and then click **Next**.



NetBrain Front Server Controller - 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

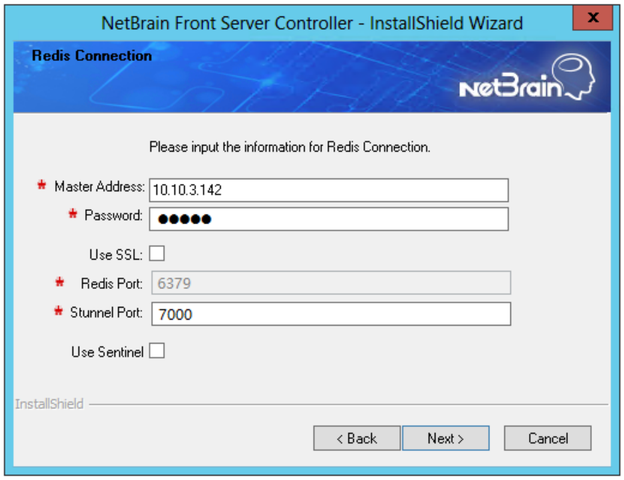
Use SSL: □

- **Address** — enter the IP address of RabbitMQ.

> **Tip:** You can enter the FQDN of RabbitMQ if all NetBrain servers are managed in the same domain.

- **User Name** — enter the admin username that you created when installing RabbitMQ.
- **Password** — enter the admin password corresponding to the username that you created when installing RabbitMQ.
- **Port Number** — enter the port number used by RabbitMQ to communicate with Web API Server, Worker Server, and Task Engine. By default, it is **5672**.
- **Use SSL** — used to encrypt the connections to RabbitMQ with SSL. If SSL is enabled on RabbitMQ, select it; otherwise, leave it unchecked.

10) On the Redis Connection page, enter the following information to connect to Redis, and then click **Next**.



NetBrain Front Server Controller - InstallShield Wizard

Redis Connection

Please input the information for Redis Connection.

* Master Address: 10.10.3.142

* Password: ●●●●●

Use SSL: □

* Redis Port: 6379

* Stunnel Port: 7000

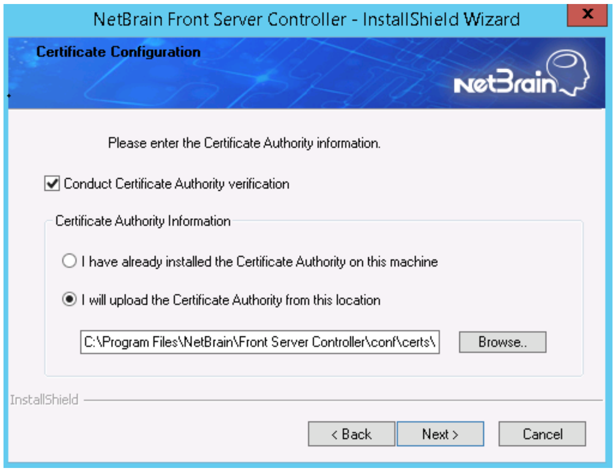
Use Sentinel □

- **Master Address** — enter the IP address of Redis.

> **Tip:** You can enter the FQDN of Redis if all NetBrain servers are managed in the same domain.

- **Password** — enter the admin password that you created when installing Redis.
- **Use SSL** — used to encrypt the connections to Redis with SSL. If SSL is enabled on Redis, select it; otherwise, leave it unchecked.
- **Redis Port** — enter the port number used by Redis to communicate with Web API Server, Worker Server, and Front Server Controller. By default, it is **6379**.
- **Stunnel Port** — required only if **Use SSL** is enabled. Enter the port number of the secure stunnel used to forward all traffics on Redis. By default, it is **7000**.
- **Use Sentinel** — required only if you set up a Redis Cluster. Leave it unchecked.

11) (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 certificate file and then click **Next**.



NetBrain Front Server Controller - InstallShield Wizard

Certificate Configuration

Please enter the Certificate Authority information.

☑ Conduct Certificate Authority verification

Certificate Authority Information

○ I have already installed the Certificate Authority on this machine

● I will upload the Certificate Authority from this location

C:\Program Files\NetBrain\Front Server Controller\conf\certs\

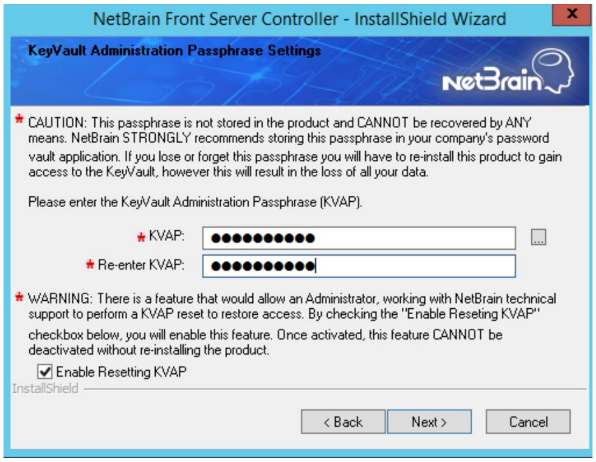
To authenticate CA:

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**; otherwise, select **I have already installed the Certificate Authority on this machine**.

> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met if you select **I have already installed the Certificate Authority on this machine:**
>
> - 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.

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



NetBrain Front Server Controller - InstallShield Wizard

KeyVault Administration Passphrase Settings

* 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.

Please enter the KeyVault Administration Passphrase (KVAP).

* KVAP: ●●●●●●●●●●●

* Re-enter KVAP: ●●●●●●●●●●●

* 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 Reseting KVAP" checkbox below, you will enable this feature. Once activated, this feature CANNOT be deactivated without re-installing the product.

☑ Enable Resetting KVAP

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

4. After successfully installing 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.

1.13. Upgrading Front Server

Complete the following steps to upgrade Front Server:

1. Installing Front Server
2. Uninstalling Proxy Server

1.13.1. Installing Front Server

Each Front Server is recommended to manage 5,000 network nodes at most. Depending on your network scale, you can deploy either a standalone Front Server, or multiple Front Servers for load balancing.

> **Note**: Ports 7778, 7086, and 29916 must be open for communications.

Select either of the following ways to install the Front Server, depending on your operating system:

- Installing Front Server on Linux
- Installing Front Server on Windows

1.13.1.1. Installing Front Server on Linux

Pre-Installation Task

Ensure you have upgraded your OS to **Red Hat Enterprise Linux Server7.5/7.6/7.7/7.8, 64-bit** or **CentOS 7.5/7.6/7.7/7.8, 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, don't 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 Front Server on Linux

> **Note:** 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.x86_64 glibc.i686 libstdc++.x86_64 libstdc++.i686 libuuid.x86_64 libuuid.i686 pam.x86_64 pam.i686` command to install these third-party packages online.
>
> - **Offline Install:** see Appendix: Offline Installing Third-party Dependencies for more details.

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, **netbraintemp03**.

3. Run the `cd /opt/netbraintemp03` command to navigate to the **/opt/netbraintemp03** 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-rhel7-8.0.3.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp03** directory by using a file transfer tool.

   - **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/netbrain-frontserver-linux-x86_64-rhel7-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to directly download the **netbrain-frontserver-linux-x86_64-rhel7-8.0.3.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-rhel7-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to extract installation files.

```
[root@localhost netbraintemp03]# tar -zxvf netbrain-frontserver-linux-x86_64-rhel7-8.0.3.tar.gz
FrontServer/
FrontServer/config/

FrontServer/install.sh
...
```

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

7. Run the `./install.sh` script under the **FrontServer** directory to install the Front Server.

   1) Read the License Agreement, and type **YES**.

   2) Type **I ACCEPT** to accept the License Agreement. The script starts to install the Front Server.

```
[root@localhost FrontServer]# ./install.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 installation log file SUCCEEDED
INFO: Preprocessing SUCCEEDED
INFO: Starting to check system info...
         ...
INFO: System checking SUCCEEDED.
INFO: Dependent packages checking SUCCEEDED.
INFO: 2020-07-14 13-28-16.389: Configuration parameters checking SUCCEEDED.
INFO: Current working directory:
/root/opt/netbraintemp03/FrontServer
INFO: Extracting files of Front Server SUCCEEDED.
usermod: no changes
INFO: Configuration parameters updating SUCCEEDED.
Created symlink from /etc/systemd/system/multi-user.target.wants/netbrainfrontserver.service to
/usr/lib/systemd/system/netbrainfrontserver.service.
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed Front Server.
```

> **Note:** The Front Server service will not be automatically started until it is successfully registered. You cannot register a Front Server immediately until adding the Front Server to a Tenant.

8. If you deployed multiple Front Servers for load balancing, repeat the above steps on other machines for an upgrade.

9. Run the `systemctl status netbrainfrontserver` command to check the service status of each node.

1.13.1.2. Installing Front Server on Windows

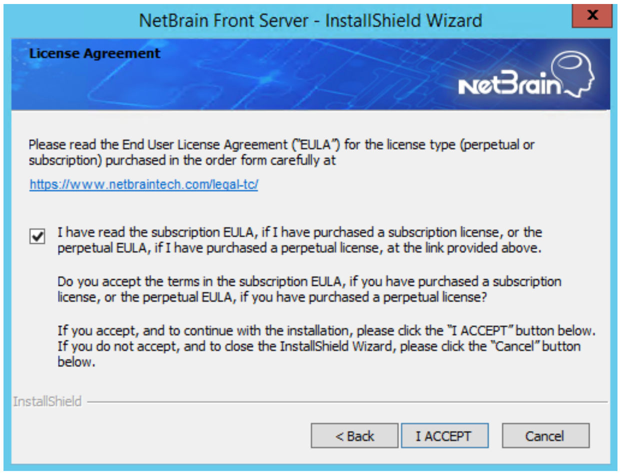
> **Note:** Before the upgrading, clean the **C:\Windows\Temp** folder to make sure the upgrade process goes smoothly.

Complete the following steps with administrative privileges.

1. Download the **netbrain-frontserver-windows-x86_64-8.0.3.zip** file from http://download.netbraintech.com/netbrain-frontserver-windows-x86_64-8.0.3.zip and save it in your local folder.

2. Extract installation files from the **netbrain-frontserver-windows-x86_64-8.0.3.zip** file.

3. Right-click the **netbrain-frontserver-windows-x86_64-8.0.3.exe** file, and then select **Run as administrator** to start the Installation Wizard.
   1) On the Welcome page, click **Next**.
   2) On the System Configuration page, review the system configuration summary and click **Next**.
   3) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA, …** check box and then click **I ACCEPT**.



Please read the End User License Agreement ("EULA") for the license type (perpetual or subscription) purchased in the order form carefully at
https://www.netbraintech.com/legal-tc/

☑ 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.

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 click the "I ACCEPT" button below. If you do not accept, and to close the InstallShield Wizard, please click the "Cancel" button below.

   4) On the Destination Location page, click **Next** to install the Front Server under the default directory **C:\Program Files\NetBrain\**. If you want to install it under another location, click **Change**.
   5) Review the summary of the current installation settings and click **Install**.

4. After the Front Server is successfully installed, click **Finish** to complete the installation process and exit the Installation Wizard. Close the pop-up registration program.

> **Note:** The Front Server service will not be automatically started until it is successfully registered. You cannot register a Front Server immediately until adding the Front Server to a Tenant.

5. If you deployed multiple Front Servers for load balancing, repeat the above steps on other machines for an upgrade.
6. After the installation is completed, you can open the Task Manager and navigate to the **Services** panel to check whether **NetBrainFrontServer** is running.

1.13.2. Uninstalling Proxy Server

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 NetBrain Proxy Server** app in the pane and select **Run as administrator** from the drop-down list to launch the Installation Wizard.
3. Click **Yes** when a confirmation dialog box prompts.
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.

1.14. Installing Service Monitor Agent

Select one of the following ways to install the Service Monitor Agent on each NetBrain server, depending on its operating system:

- Installing Service Monitor Agent on Linux
- Installing Service Monitor Agent on Windows

1.14.1. Installing Service Monitor Agent on Linux

Pre-Installation Task

Ensure you have upgraded your OS to **Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8, 64-bit** or **CentOS 7.5/7.6/7.7/7.8, 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, don't 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 Service Monitor on Linux

> **Note:** 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**. Run the `rpm -qa|grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel"` command to check whether **zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel** 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` command to install it online.
>
> - **Offline Install:** see Appendix: Offline Installing Third-party Dependencies for more details.

1. Log into the Linux server as the **root** user.

2. Run the `cd /opt/netbraintemp03` command to navigate to the **/opt/netbraintemp03** 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-rhel7-8.0.3.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp03** directory by using a file transfer tool.

   - **Option 2:** If the Linux server has access to the Internet, run the `wget http://download.netbraintech.com/netbrain-servicemonitoragent-linux-x86_64-rhel7-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to directly download the **netbrain-servicemonitoragent-linux-x86_64-rhel7-8.0.3.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-rhel7-8.0.3.tar.gz` command under the **/opt/netbraintemp03** directory to extract installation files.

```
[root@localhost netbraintemp03]# tar -zxvf netbrain-servicemonitoragent-linux-x86_64-rhel7-
8.0.3.tar.gz
ServiceMonitorAgent/
ServiceMonitorAgent/config/
ServiceMonitorAgent/config/setup.conf
...
ServiceMonitorAgent/install.sh
...
```

5. Run the `cd ServiceMonitorAgent/config` command to navigate to the **config** directory.

6. Modify the parameters in the **setup.conf** file located under the **config** directory according to your environment and save the changes. For how to modify the configuration file, see Appendix: Editing a File with VI Editor for more details.

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

# IE API Url, for example: http://ie.netbrain.com/ServicesAPI
# Attention please: /ServicesAPI is a fixed suffix
Server_Url=http://localhost/ServicesAPI

# Authentication Key to be used to communicate with Web API server.
# Note: please ensure this key must be the same as the API key created on Web API server.
Server_Key=netbrain

# LogPath is used to store log files for Servicemonitor.
# This directory must be at least a second level directory and used exclusively for this
purpose.
LogPath=/var/log/netbrain/nbagent

# Whether to enable verifying Certificate Authority (CA): By default, it is disabled.
yes indicates enabled; no indicates disabled.
# Note: To enable the verifying CA, it is needed to change configuration of the Web Server.
CA_Verify=no

# CertAuth specifies the CA file source path. Below CA file will be copied to folder
/etc/ssl/netbrain/nbagent
CertAuth=/etc/ssl/cacert.pem
```

> **Note:** If SSL is enabled with https binding created for the system website in IIS Manager, use **https** in **Server_Url**. Besides, if **CA_Verify** is enabled, hostname must be specified in **Server_Url**.

7. Run the `cd ..` command to navigate to the **ServiceMonitorAgent** directory.

8. Run the `./install.sh` script under the **ServiceMonitorAgent** directory to install 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]# ./install.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

Preprocessing SUCCEEDED
Starting install Service Monitor Agent ...
Starting system checking...
  Collecting system information...
...
  Collecting system information SUCCEEDED.
System checking SUCCEEDED.
Starting configuration parameters SUCCEEDED...
Configuration parameters checking SUCCEEDED.
Start dependencies checking...
Dependencies checking SUCCEEDED.
...
Obtaining file:///usr/share/nbagent
Installing collected packages: agent
  Running setup.py develop for agent
Successfully installed agent
WARNING: You are using pip version 19.2.3, however version 20.1.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Configuration parameters updating SUCCEEDED.
Starting permission setting...
Permission setting SUCCEEDED.
Starting deamon setting...
Created symlink from /etc/systemd/system/multi-user.target.wants/netbrainagent.service to
/usr/lib/systemd/system/netbrainagent.service.
Deamon setting SUCCEEDED.
Successfully installed Service Monitor Agent. Service is running.
INFO: Backup uninstall.sh SUCCEEDED
```

9. 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: 14522 (python3)
   Memory: 73.5M
...
```

10. (Only required if you have changed the default port number or configured DNS connection when installing MongoDB/License Agent/Elasticsearch/Redis/RabbitMQ). To make the Server Monitor can still detect and monitor its service, you must add the customized port number to the corresponding configuration file.

Server Name	File Name
MongoDB	mongodb.yaml
License Agent	license.yaml
Elasticsearch	elasticsearch.yaml
Front Server	fs.yaml
RabbitMQ	rabbitmq.yaml
Redis	redis.yaml

Example: If you configured the port number **27000** during MongoDB installation, do the following:

1) Run the `cd /etc/netbrain/nbagent/checks` command to navigate to the **checks** directory.

2) Add the customized port number to the **mongodb.yaml** file, and save the changes. For how to modify the file, see Appendix: Editing a File with VI Editor for more details.

> **Note**: If fully qualified domain name (FQDN) is used when installing MongoDB on this machine, add `dns:<MongoDB FQDN>` to the **mongodb.yaml** file.
>
> **Note**: Follow the text format in the example strictly, including alignment, punctuations, and spaces.

```
init_config:

instances:
    - name: default
      port: 27000
```

> **Tip:** It is highly recommended to run the `rm -rf /opt/netbraintemp03/ServiceMonitorAgent/config/setup.conf` command to delete the **setup.conf** file from the server after Service Monitor Agent is successfully installed because the file may cause security vulnerability.

Parameters

Parameter	Default Value	Description
Server_Url	`http://localhost/ServicesAPI`	The URL used to call the Web API service, http://<IP address of NetBrain Web API Server>/ServicesAPI. For example, **http://10.10.3.141/ServicesAPI**.

Parameter	Default Value	Description
		Note: If SSL will be enabled with https binding created for the system website in IIS Manager, type **https** in the URL. Besides, if **VerifyCA** is enabled, hostname must be specified in the URL.
Server_Key	`netbrain`	The key used to authenticate the connections to your NetBrain Web API Server. **Note:** The **Server_Key** must be kept consistent with the key configured when you installed Web API Server and Worker Server.
LogPath	`/var/log/netbrain/nbagent`	The storage path for the log files of the Service Monitor Agent. **Note:** Don't save the log files under any subfolders of the **InstallPath**.
CA_Verify	`no`	Set whether to authenticate the Certificate Authority (CA) of the certificates, which are used to enable SSL for the system website in IIS Manager. **Note:** It is required only if https is used in **Server_Url**.
CA_Path	`/etc/ssl/cacert.pem`	The storage path and file name of the root or class 2 CA file used for CA authentication. **Note:** It is required only if **CA_Verify** is enabled. Only the CA file in the **Base-64 encoded X.509 (.CER)** format is supported.

1.14.2. Installing Service Monitor Agent on Windows

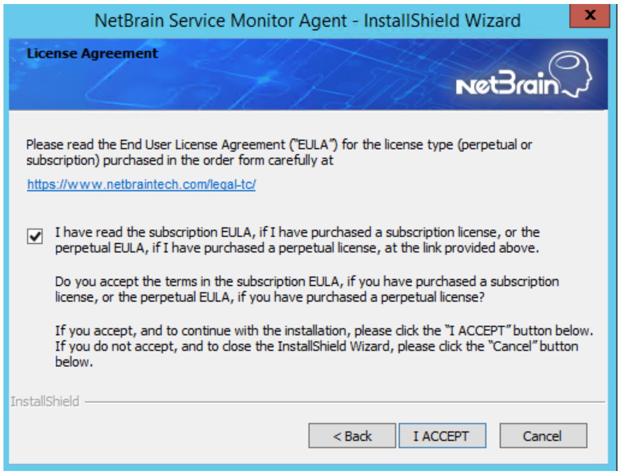
Complete the following steps with administrative privileges.

1. Download the **netbrain-servicemonitoragent-windows-x86_64-8.0.3.zip** file from http://download.netbraintech.com/netbrain-servicemonitoragent-windows-x86_64-8.0.3.zip and save it in your local folder.

2. Extract installation files from the **netbrain-servicemonitoragent-windows-x86_64-8.0.3.zip** file.

3. Right-click the **netbrain-servicemonitoragent-windows-x86_64-8.0.3.exe** file, and then select **Run as administrator** to start the Installation Wizard.
   1) On the Welcome page, click **Next**.
   2) On the System Configuration page, review the system configuration summary and click **Next**.

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



NetBrain Service Monitor Agent - InstallShield Wizard

License Agreement

Please read the End User License Agreement ("EULA") for the license type (perpetual or subscription) purchased in the order form carefully at

https://www.netbraintech.com/legal-tc/

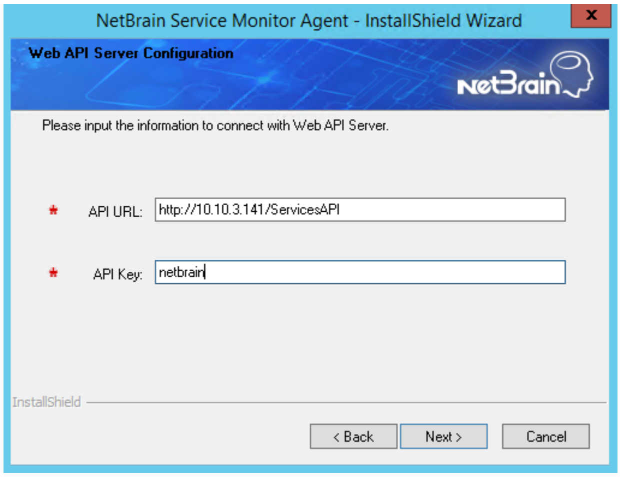
☑ I have read the subscription EULA, if I have purchased a subscription license, or the perpetual EULA, if I have purchased a perpetual license, at the link provided above.

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 click the "I ACCEPT" button below. If you do not accept, and to close the InstallShield Wizard, please click the "Cancel" button below.

4) On the Destination Location page, click **Next** to install the Service Monitor Agent under the default path **C:\Program Files\NetBrain\**. If you want to install it under another location, click **Change**.

5) On the Web API Server Configuration page, enter the following information to connect to your NetBrain Web API Server, and then click **Next**.



NetBrain Service Monitor Agent - InstallShield Wizard

Web API Server Configuration

Please input the information to connect with Web API Server.

* API URL: http://10.10.3.141/ServicesAPI

* API Key: netbrain

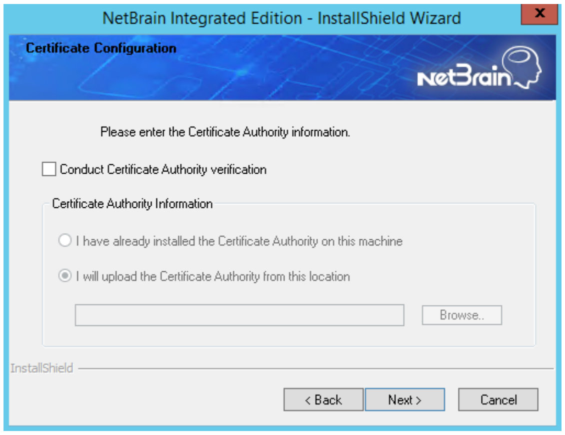
- **API URL** — the URL used to call the Web API service, **http://<IP address of NetBrain Web API Server>/ServicesAPI**. For example, **http://10.10.3.141/ServicesAPI.**

> **Note:** If SSL is enabled with https binding created for the system website in IIS Manager, use **https** in the URL. Besides, if you want to authenticate the Certificate Authority of the SSL certificate used by the system website (to be completed in the next step), the hostname must be specified in the URL.

- **API Key** — the key used to authenticate the connections to Web API Server. By default, it is **netbrain**.

> **Note:** The API Key must be kept consistent with the API Key configured when you installed Web API Server and Worker Server.

6) This step is required only if **https** is used in **API URL**. Configure whether to authenticate the Certificate Authority (CA) of the certificates used to enable SSL for NetBrain website in IIS Manager, and then click **Next**.



NetBrain Integrated Edition - InstallShield Wizard

Certificate Configuration

Please enter the Certificate Authority information.

☐ Conduct Certificate Authority verification

Certificate Authority Information

○ I have already installed the Certificate Authority on this machine

● I will upload the Certificate Authority from this location

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**; otherwise, select **I have already installed the Certificate Authority on this machine**.

> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met if you select **I have already installed the Certificate Authority on this machine:**
>
> - 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.

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

4. After NetBrain Service Monitor Agent is successfully installed, click **Finish** to complete the installation process and exit the Installation Wizard.

> **Tip:** After the installation is completed, you can open the Task Manager and navigate to the **Services** panel to check whether **NetBrainAgent** is running.

5. If you changed the default port number when installing a NetBrain server, you must add the customized port number to its corresponding configuration file so that the Server Monitor Agent can detect and monitor its service. See Configuration Files for Port Information for more details.

Configuration Files for Port Information

The Service Monitor Agent checks the following configuration files for the customized port or service name information about NetBrain servers installed on Windows.

Server Name	File Name
Front Server	**fs.yaml**
Front Server Controller	**fsc.yaml**
Web API Server	**iis.yaml**
Task Engine	**taskengine.yaml**
Worker Server	**workerserver.yaml**

Example: If you configured a port number **5662** during Task Engine installation, do the following:

1. Navigate to the **C:\ProgramData\Netbrain\nbagent\checks** directory.

> **Tip:** The **ProgramData** folder is hidden usually. You can copy and paste the directory to navigate to the **checks** folder directly.

2. Open the **taskengine.yaml** file with a text editor to modify it.

> **Note:** Follow the text format in the example strictly, including alignment, punctuations, and spaces.

```
init_config:

instances:
 - name: default
   port: 5662
```

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.
>
> 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 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.

> **Note:** If you want to create a tenant later, click **No**. See Creating a Tenant for more details.

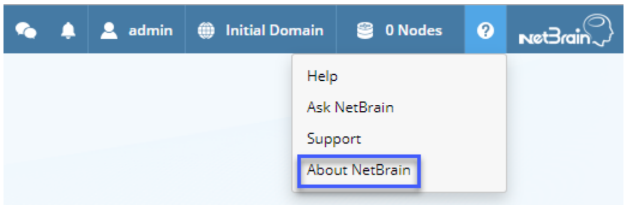
To browse the license information, navigate to **License > Current License Term**. See License Information for more details.

1.17. Verifying Upgrade Results

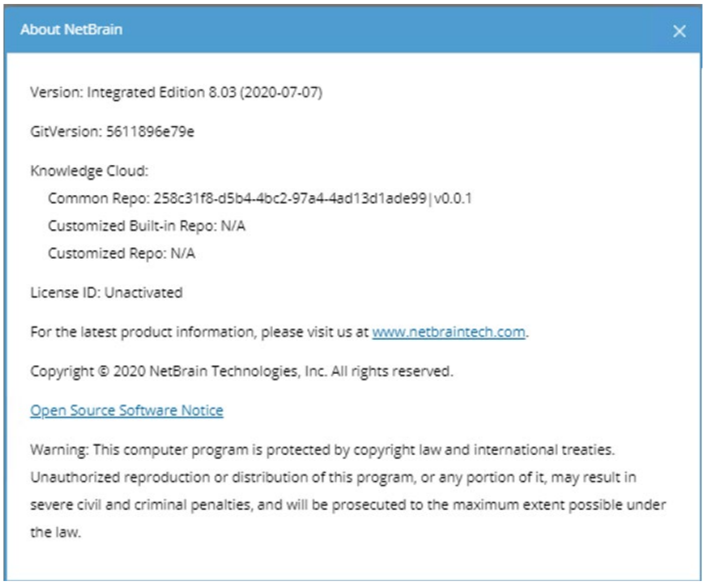
1. Do the following steps to check the IE version in web browser:

> **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.



Version: Integrated Edition 8.03 (2020-07-07)

GitVersion: 5611896e79e

Knowledge Cloud:

Common Repo: 258c31f8-d5b4-4bc2-97a4-4ad13d1ade99|v0.0.1

Customized Built-in Repo: N/A

Customized Repo: N/A

License ID: Unactivated

For the latest product information, please visit us at www.netbraintech.com.

Copyright © 2020 NetBrain Technologies, Inc. All rights reserved.

Open Source Software Notice

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

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.

Example:

```
[root@localhost ~]# mongo --host 10.10.3.142:27017 -u mongodb -p mongodb --
authenticationDatabase admin --authenticationMechanism SCRAM-SHA-256
MongoDB shell version v4.0.6
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.

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" : "8.0.03", "operateInfo" : { "opUser" : "NetBrain",
"opTime" :
  ISODate("2020-07-14T18:31:21.735") } }
```

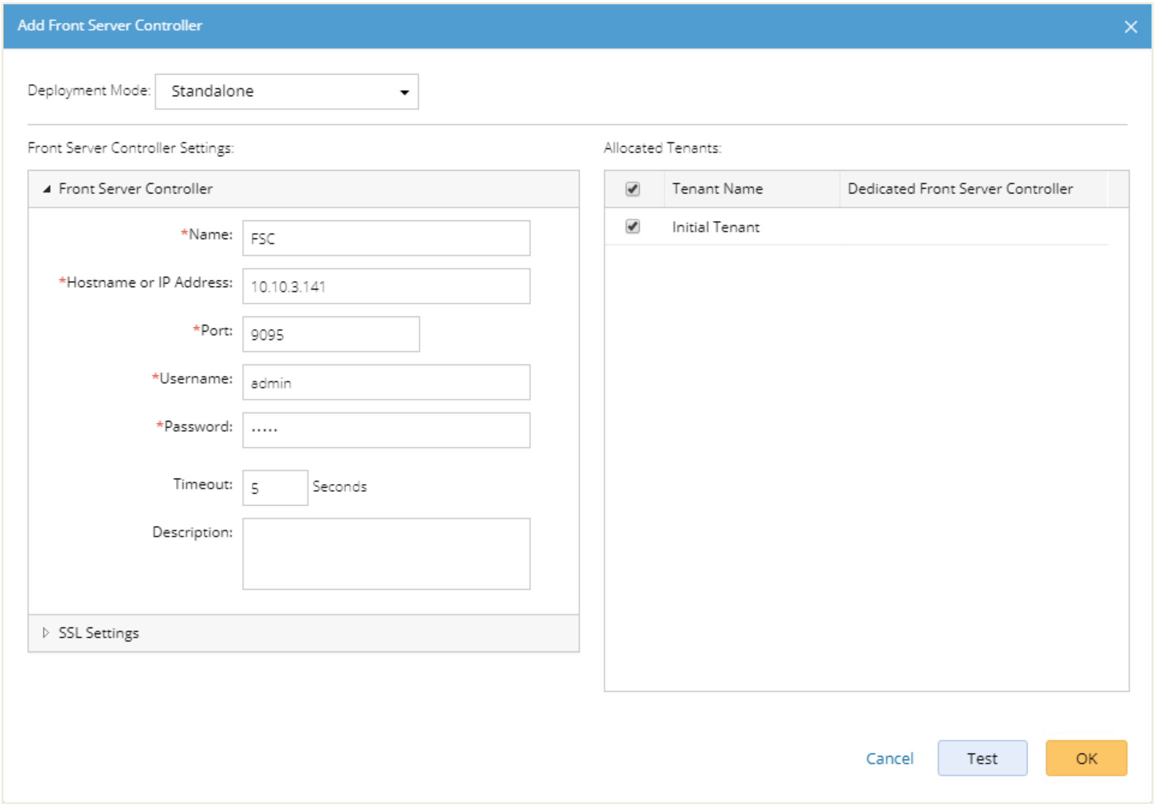
5) Run the `exit` command to exit the command prompt.

1.18. Allocating Tenants to Front Server Controller

1. In the System Management page, select the **Front Server Controllers** tab, and then click **Add Front Server Controller**.

2. In the **Add Front Server Controller** dialog, configure the settings for the Front Server Controller, and then allocate tenants to it.

   1) Select the deployment mode, and then specify the basic information about the Front Server Controller. See FSC Settings for more details.



Add Front Server Controller

Deployment Mode: Standalone

Front Server Controller Settings:

Front Server Controller

*Name: FSC

*Hostname or IP Address: 10.10.3.141

*Port: 9095

*Username: admin

*Password: •••••

Timeout: 5 Seconds

Description:

SSL Settings

Allocated Tenants:

☑	Tenant Name	Dedicated Front Server Controller
☑	Initial Tenant	

   - **Standalone** — applicable to a single Front Server Controller deployment.
   - **Group** — applicable to a failover deployment of Front Server Controller.

   2) Configure the SSL settings.

      a) If SSL is enabled on Front Server Controller, select the **Use SSL** check box to encrypt the connections established from the Worker Server and Front Server with SSL. Otherwise, leave it unchecked.

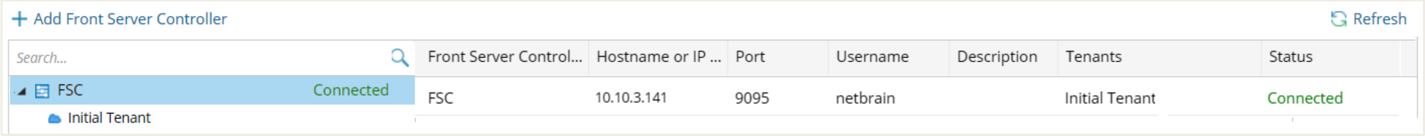
      b) To authenticate the Certificate Authority (CA) certificate on the Front Server Controller, select the **Conduct Certificate Authority verification** check box.

c) If CA has not been installed on the Worker Server and Task Engine, click **Browse** to upload the CA file, for example, **ca.pem**. Otherwise, click **I have already installed the Certificate Authority on Worker Server and Task Engine**.

> **Note:** Only certificates in the **Base-64 encoded X.509 PEM** format are supported.

3) Click **Test** to verify whether the Worker Server can establish a connection to Front Server Controller with the configurations.
4) In the **Allocated Tenants** area, select the target tenants to allocate them to the controller.
5) Click **OK** to save the settings.

The Front Server Controller is added.



Front Server Control...	Hostname or IP ...	Port	Username	Description	Tenants	Status
FSC	10.10.3.141	9095	netbrain		Initial Tenant	Connected

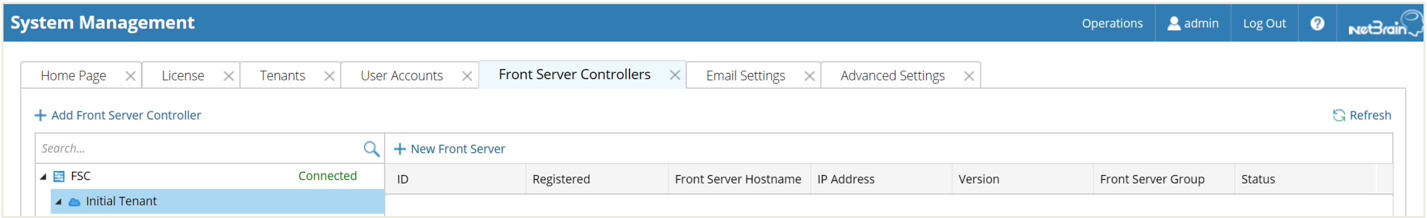
Front Server Controller Settings

The following items (except **Timeout** and **Description**) are required to be consistent with those configured during the installation of Front Server Controller.

Field	Description
Name	The name of the Front Server Controller created when you install the Front Server Controller.
Hostname or IP Address	Enter the IP address of Front Server Controller.
Port	The port number created when you install the Front Server Controller for listening to the connections from Worker Server. By default, it is **9095**.
Username	The user name created when you install the Front Server Controller to authenticate the connections from Worker Server.
Password	The password created on the NetBrain Front Server Controller page when installing the Front Server Controller.
Timeout	The maximum waiting time for establishing a connection from Worker Server to this Front Server Controller. By default, it is **5** seconds.
Description	The brief description to help you add more information about the Front Server Controller.

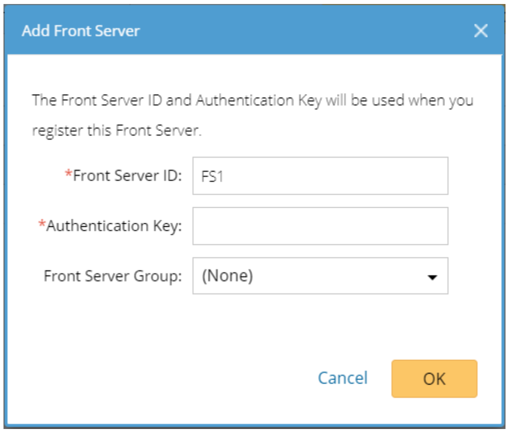
1.19. Adding a Front Server for a Tenant

1. In the Front Server Controller Manager, select the target tenant and click **Add Front Server**.



ID	Registered	Front Server Hostname	IP Address	Version	Front Server Group	Status

2. Enter the following properties of the Front Server.



The Front Server ID and Authentication Key will be used when you register this Front Server.

*Front Server ID: FS1

*Authentication Key:

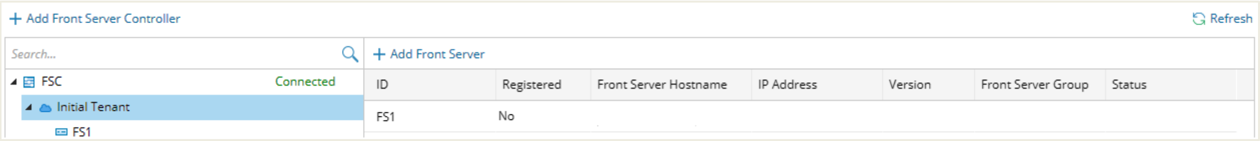
Front Server Group: (None)

- **Front Server ID** — create an ID for identifying the Front Server.
- **Authentication Key** — create an authentication key for the Front Server.

> **Tip**: Keep notes of the Authentication Key because it is required when you register this Front Server.

- **Front Server Group** — assign the Front Server to a group for load balancing. It is only applicable when multiple Front Servers are added to one tenant.

3. Click **OK**. The Front Server is added to the Front Server list.



ID	Registered	Front Server Hostname	IP Address	Version	Front Server Group	Status
FS1	No					

1.20. Registering a Front Server

Select either of the following ways to register the Front Server, depending on the operating system of your machine:

- Registering Front Server on Windows

- Registering Front Server on Linux

Registering a Front Server on Windows

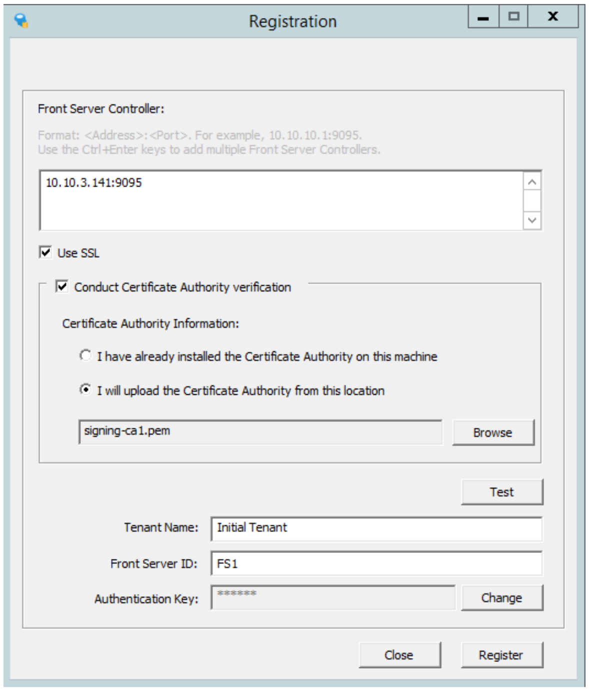
Example: Register a Front Server on Windows Server 2012 R2.

Complete the following steps with administrative privileges.

1. On the machine where the Front Server is installed, click the Windows start menu and then click the ⬇ icon to open the **Apps** pane.

2. Under the **NetBrain** category, right-click **Registration** and then select **Run as administrator** from the drop-down list.

3. In the **Registration** dialog, complete the registration form.



Registration

Front Server Controller:

Format: <Address>:<Port>. For example, 10.10.10.1:9095.
Use the Ctrl+Enter keys to add multiple Front Server Controllers.

10.10.3.141:9095

☑ Use SSL

☑ Conduct Certificate Authority verification

Certificate Authority Information:

○ I have already installed the Certificate Authority on this machine

● I will upload the Certificate Authority from this location

signing-ca1.pem

Tenant Name: Initial Tenant

Front Server ID: FS1

Authentication Key: ******

   1) Enter the following information about the Front Server Controller.

      - **Hostname or IP address** — the IP address or FQDN of Front Server Controller and the port number (defaults to 9095).

   2) Configure the SSL settings.

      a) Select the **Use SSL** check box to encrypt the connections to Front Server Controller with SSL. If SSL is disabled on Front Server Controller, leave it unchecked and skip step b) to c).

      > **Note:** Select the **Use SSL** check box only if you enabled SSL on Front Server Controller.

b) To authenticate the Certificate Authority (CA) of SSL certificates on Front Server, select the **Conduct Certificate Authority verification** check box.

c) If the CA has not been installed on this machine, click **Browse** to upload the CA file, for example, **ca.pem**; otherwise, select **I have installed the Certificate Authority on this machine**.

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

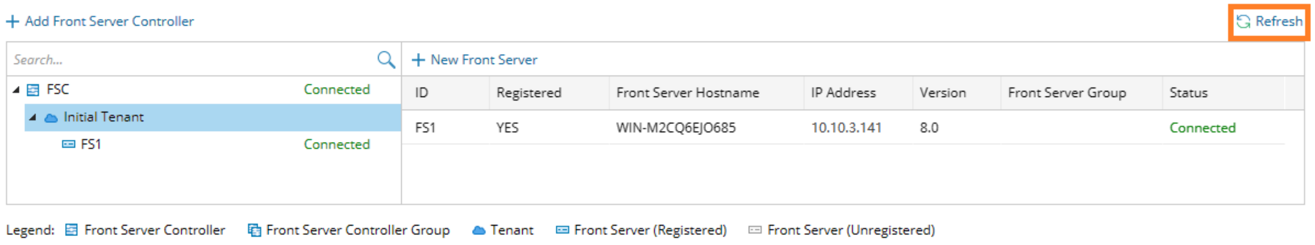
3) Click **Test** to verify whether this Front Server can establish a connection with Front Server Controller.

4) Keep all default values, and then enter the authentication key created when you add this Front Server to a tenant.

4. Click **Register**.

> **Tip:** After registering the Front Server successfully, you can open the Task Manager and navigate to the **Services** panel to check whether the **NetBrainFrontServer** service is running.

5. Click **Close** after the registration is finished. The Front Server information in the Front Server Controller Manager will be synchronized by clicking **Refresh**.



FSC Connected
Initial Tenant
FS1 Connected

ID	Registered	Front Server Hostname	IP Address	Version	Front Server Group	Status
FS1	YES	WIN-M2CQ6EJO685	10.10.3.141	8.0		Connected

Legend: Front Server Controller Front Server Controller Group Tenant Front Server (Registered) Front Server (Unregistered)

Registering a Front Server on Linux

1. On the machine where the Front Server is installed, run the `cd /usr/lib/netbrain/frontserver/conf` command to navigate to the **conf** directory.

2. Modify the following parameters in the **register_frontserver.conf** file located under the **conf** directory and save the changes. For how to modify the configuration file, see Appendix: Editing a File with VI Editor for more details.

```
[root@localhost conf]# vi register_frontserver.conf
# Enter <hostname or IP address>:<port> of the Front Server Controller. For example,
192.168.1.1:9095
# Use a semicolon to separate multiple Front Server Controllers.
Front Server Controller =10.10.3.141:9095

# Define the SSL settings
Enable SSL = No
Conduct SSL Certificate Authority = No
SSL Certificate Path =

# Define the Front Server register to
Tenant Name =Initial Tenant
Front Server ID =FS1
```

3. Run the `cd /usr/lib/netbrain/frontserver/bin` command to navigate to the **bin** directory.

4. Run the `./registration` command under the **bin** directory, and input the Authentication Key and press the **Enter** key.

```
[root@localhost bin]# ./registration
Loading configuration files...
Authentication Key:
Stopping Front Server Service...
Registering Front Server...
Successfully registered to the tenant "Initial Tenant".
10.10.3.141: active.

Succeeded to start up front server service.
```

5. Run the `service netbrainfrontserver status` command to verify whether the service of the Front Server starts successfully.

```
[root@localhost FrontServer]# service netbrainfrontserver status
Redirecting to /bin/systemctl status  NetBrainFrontServer.service
NetBrainFrontServer.service - NetBrain Front Server Daemon
Loaded: loaded (/usr/lib/systemd/system/NetBrainFrontServer.service)
Active: active (running)
```

Parameters

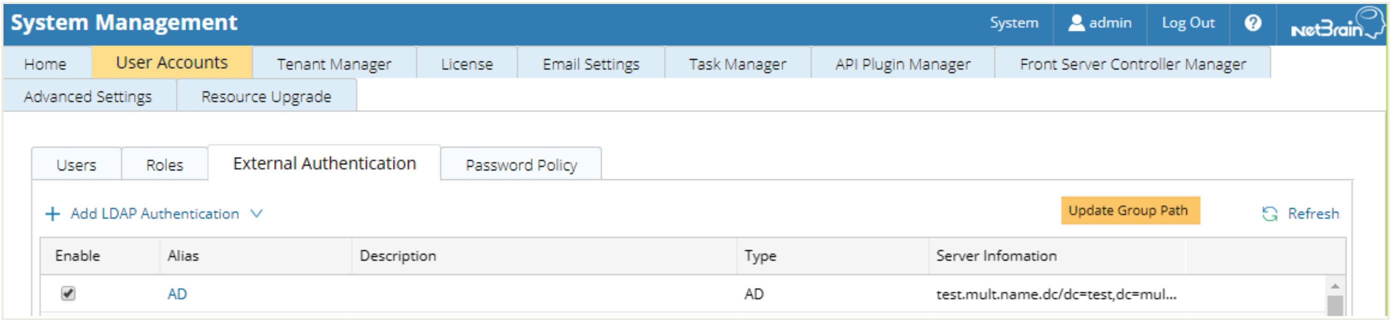
Parameter	Default Value	Description
Front Server Controller		The hostname, IP address, or FQDN of the Front Server Controller and the port number.
Enable SSL	`No`	Set whether to encrypt the connections to Front Server Controller with SSL. If SSL is enabled on the Front Server Controller, type **Yes**; otherwise, leave the default value as it is. **Note:** Type **Yes** only if you enabled SSL on MongoDB.
Conduct Certificate Authority Verification	`No`	Set whether to authenticate the Certificate Authority (CA) of SSL certificates on the Front Server. If you want to authenticate the Certificate Authority, type **Yes**.
SSL Certificate Path		The storage path and certificate name. **Note:** Only the certificate in the **Base-64 encoded X.509 PEM** format is supported.
Tenant Name	`Initial Tenant`	The name of the tenant that this Front Server will serve.
Front Server ID	`FS1`	The ID created when you add this Front Server to a tenant.

Parameter	Default Value	Description
Authentication Key		The authentication key created when you add this Front Server to a tenant.

1.21. Upgrading External Authentication

> **Note:** Following steps only apply to AD/LDAP environments where group function is pre-configured.

1. In the System Management page, click **User Accounts > External Authentication**.
2. Click **Update Group Path**.



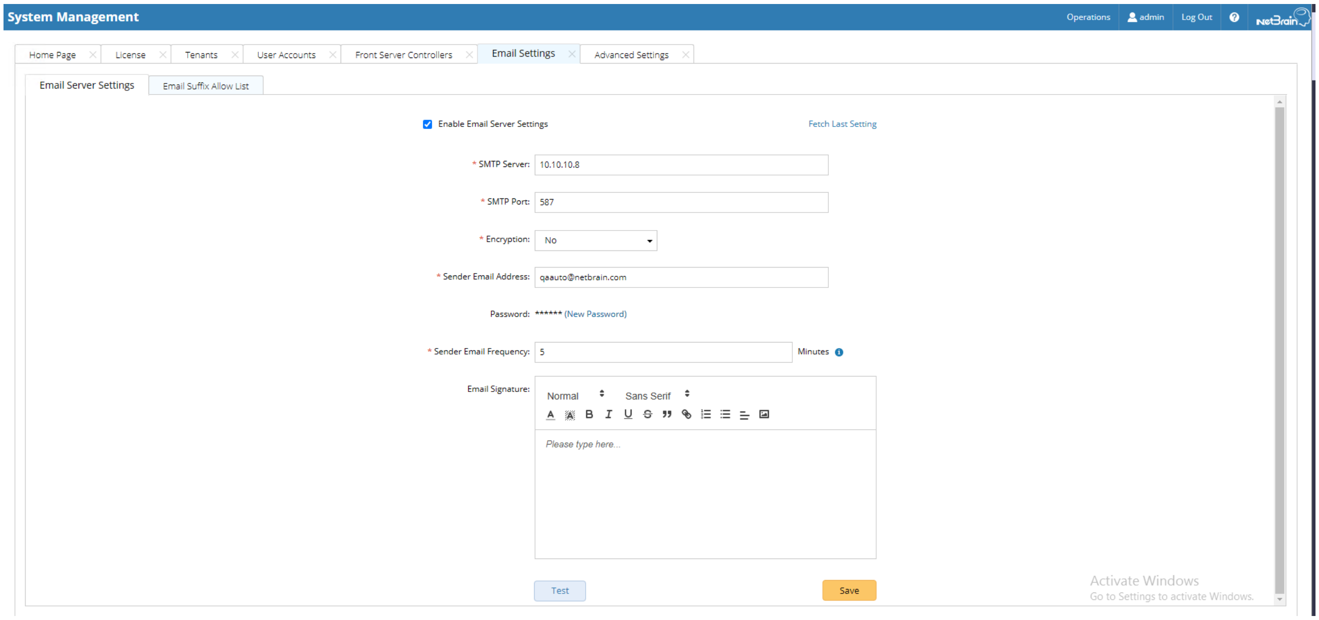
Enable	Alias	Description	Type	Server Infomation
☑	AD		AD	test.mult.name.dc/dc=test,dc=mul...

3. When the group paths are successfully updated, a notification message is displayed in a dialog box. Click **OK**.

1.22. Upgrading Email Settings

1. In the System Management page, click the **Email Settings** tab.

2. Click **Save** under the **Email Server Settings** tab page.



☑ Enable Email Server Settings

* SMTP Server: 10.10.10.8

* SMTP Port: 587

* Encryption: No

* Sender Email Address: qaauto@netbrain.com

Password: ****** (New Password)

* Sender Email Frequency: 5 Minutes

Email Signature:

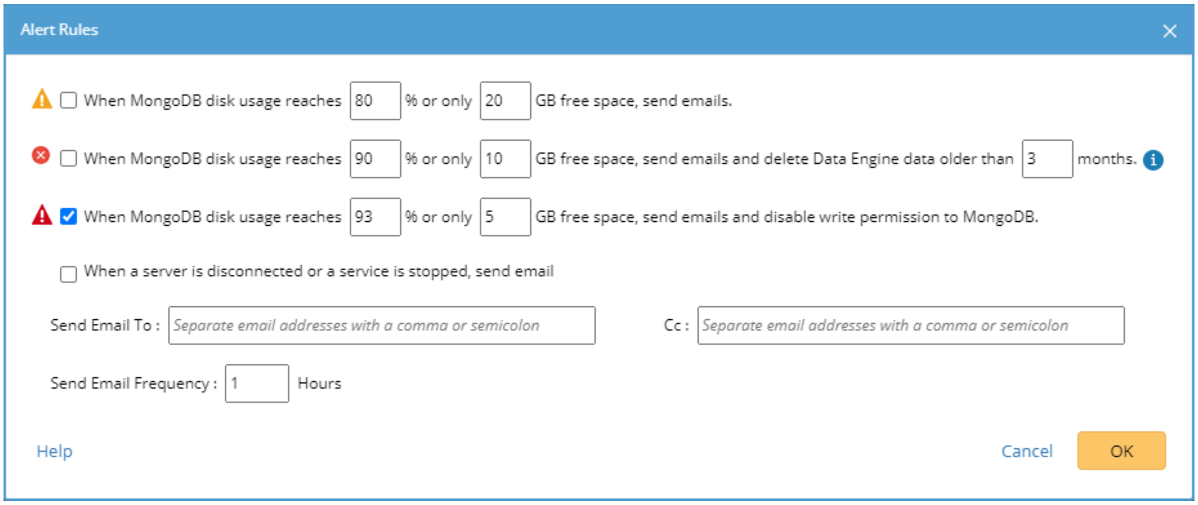
3. When the email settings are successfully upgraded, a notification message will be displayed in a dialog box. Click **OK**.

1.23. Customizing MongoDB Disk Alert Rules

To proactively prevent the system database from data loss or even corruption, you need to customize MongoDB disk alert rules. When the MongoDB usage reaches the predefined threshold, specified users can be notified by both email alerts and in-place warnings in the system.

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 and configure the settings based on your needs. See Managing Alert Rules for more details.



Alert Rules ×

□ When MongoDB disk usage reaches 80 % or only 20 GB free space, send emails.

□ When MongoDB disk usage reaches 90 % or only 10 GB free space, send emails and delete Data Engine data older than 3 months.

☑ When MongoDB disk usage reaches 93 % or only 5 GB free space, send emails and disable write permission to MongoDB.

□ When a server is disconnected or a service is stopped, send email

Send Email To : Separate email addresses with a comma or semicolon

Cc : Separate email addresses with a comma or semicolon

Send Email Frequency : 1 Hours

3. Click **OK**.

1.24. Tuning Live Access

1. In your web browser, navigate to **http(s)://<IP address of NetBrain Web Server>/** to log in to each 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**.

1.25. Scheduling Benchmark Task

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

4. To recover the v7.0b/b1 benchmark data:

    1) Download the **UpgradeDeviceData7.0To8.03.zip** file and save it to the **C:\Program Files\NetBrain\Worker Server** directory of your NetBrain Worker Server.

    > **Note:** If you changed the default installation directory for Worker Server, replace the above directory accordingly.

    2) Extract the zip file under the **\NetBrain\Worker Server** folder and double-click the **UpgradeDeviceData7.0To8.0.exe** file under the **\NetBrain\Worker Server\DE 7.0 to 8.03** folder to execute the benchmark data recovery. A sample output is as follows:

    ```
    begin to upgrade device data in domain <domain name>
    end of upgrading device data in domain <domain name>
    Press ENTER to continue.
    ```

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-centos7.5-8.0.tar.gz
   - **CentOS7.6:** http://download.netbraintech.com/dependencies-centos7.6-8.0.tar.gz
   - **CentOS7.7:** http://download.netbraintech.com/dependencies-centos7.7-8.0.tar.gz
   - **CentOS7.8:** http://download.netbraintech.com/dependencies-centos7.8-8.0.tar.gz
   - **CentOS7.9:** http://download.netbraintech.com/dependencies-centos7.9-8.0.tar.gz
   - **RHEL7.5:** http://download.netbraintech.com/dependencies-rhel7.5-8.0.tar.gz
   - **RHEL7.6:** http://download.netbraintech.com/dependencies-rhel7.6-8.0.tar.gz
   - **RHEL7.7:** http://download.netbraintech.com/dependencies-rhel7.7-8.0.tar.gz
   - **RHEL7.8:** http://download.netbraintech.com/dependencies-rhel7.8-8.0.tar.gz
   - **RHEL7.9:** http://download.netbraintech.com/dependencies-rhel7.9-8.0.tar.gz

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

3. Run the `tar -zxvf dependencies-<OS version>-8.0.tar.gz` command to decompress the package.

   > **Tip:** Possible values of **OS version** include: `centos7.5`; `centos7.6`; `centos7.7`; `centos7.8`; `rhel7.5`; `rhel7.6`; `rhel7.7`; `rhel7.8`

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

Complete the following steps to restore the MongoDB data with the backup data if you encounter data loss or corruption during the upgrade process.

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 mongodnetbrain` 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     root        42 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
```

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

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

   5) 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     root     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
-rwxr-xr-x. 1 netbrain netbrain  1147 Oct 19 14:51 mongod.conf2017|Oct|19|10:15:50
```

4. Run the `systemctl start mongodnetbrain` 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.

   Example:

```
[root@localhost upgrade_replica_set]# mongo --host 10.10.3.142:27017 -u mongodb -p mongodb --
authenticationDatabase admin --authenticationMechanism SCRAM-SHA-256
MongoDB shell version v4.0.6
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: 4.0.6
...
rsnetbrain:PRIMARY>
```

> **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` 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 to copy data files from the MongoDB Server directly.

> **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. If you have set up a MongoDB replica set for high availability, you only need to dump data from the primary node.

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

2. Open a command prompt and run the following command to create a directory under the **/etc** directory to save the backup data.
   `[root@localhost ~]# mkdir /etc/mongodb_databk`

3. Enter the following command in one line and run it to dump the MongoDB data to the **/etc/mongodb_databk** directory.

   ▪ For IEv7.x, run the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --gzip -out <filepath>` command.

   ▪ For IEv8.0, run the `mongodump --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --authenticationMechanism SCRAM-SHA-256 --gzip -out <filepath>` command.

   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 <dbname> --ssl --sslAllowInvalidCertificates --gzip -out <filepath>` commands.

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.

6. Appendix: 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.

Enter the `mongorestore --host <ip>:<port> -u <username> -p <password> --authenticationDatabase <database_name> --gzip --out <filepath>` command in one line and run it to restore the dumped data onto the MongoDB Server.

Example:

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

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