NetBrain® Integrated Edition 10.0

System Setup Guide

Distributed Deployment

Version 10.0 | Last Updated 2021-08-11

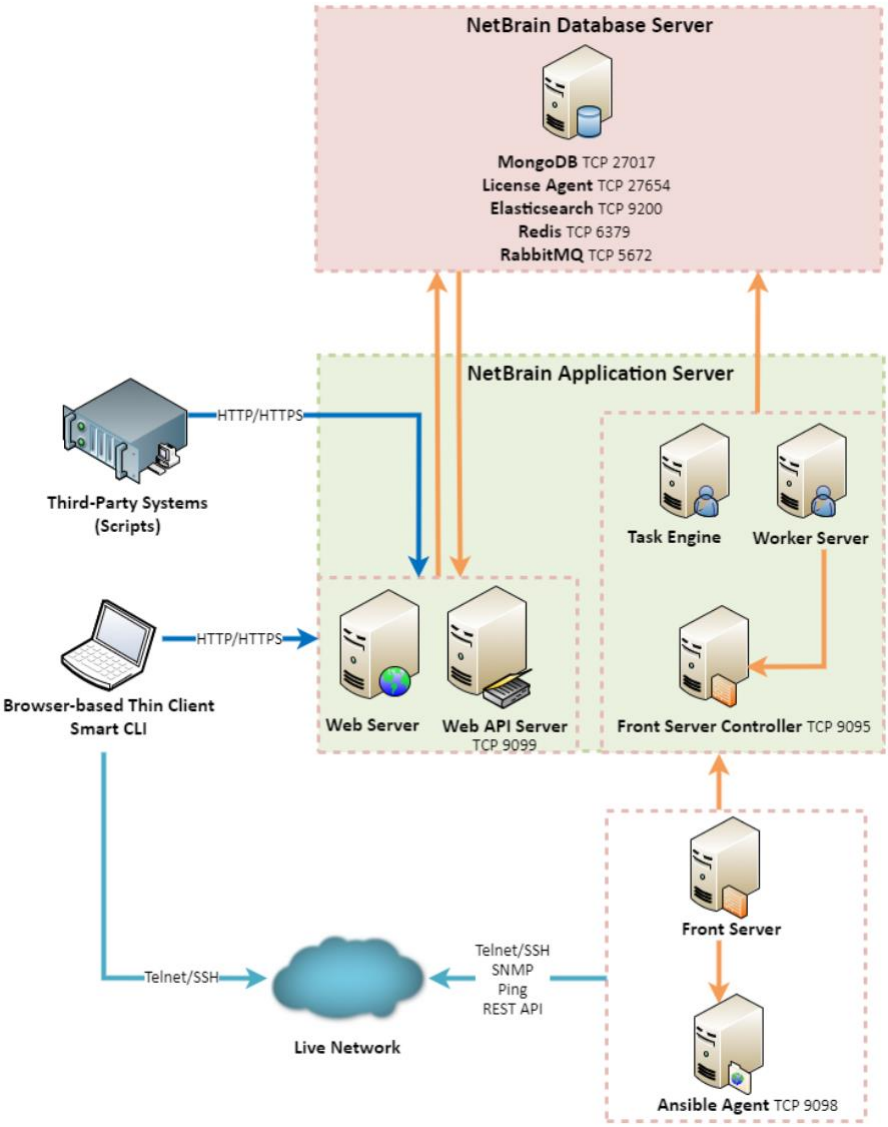
Contents

1. System Overview

NetBrain Integrated Edition is an adaptive automation platform, where you can integrate with your existing Network Management System (NMS) tools and IT workflows to automate documentation, troubleshooting, network change, and defense. It serves as an operating system of your whole network to relieve network professionals from manual CLI-digging and also empowers team collaboration to elevate productivity.

The browser-based interface of NetBrain Integrated Edition is backed by a full-stack architecture, adopting advanced distributed technologies to support large-scale networks with more expansion possibilities.

The distributed system architecture is as follows:



> **Note:** The port numbers listed in the above architecture diagram are defaults only. The actual port numbers used during installation might be different.

The system components include:

Component	Description
Browser-based Thin Client	provides a user interface for end users to access the system.
MongoDB	serves as a system data repository.
License Agent	provides services that validate and activate licenses.
Elasticsearch	serves as a full-text search and analytics engine in a distributed multi-user environment.
Redis	provides memory cache for the system.
RabbitMQ	prioritizes and forwards requested tasks.
Web Server	serves static content such as HTML, JavaScript, and CSS resources, which serves as the user interface of the Thin Client.
Web API Server	provides the front-end web applications to support the browser-based Thin Clients and serves RESTful API calls from third-party applications for integration.
Worker Server	serves as a resource manager to support computing tasks. It relies on both Redis and RabbitMQ to work.
Task Engine	coordinates computing tasks.
Front Server Controller	serves to coordinate and communicate with Front Servers and other components.
Front Server	serves as a polling server to collect and parse live network data. It is the only component required to access the live network.
Service Monitor Agent	monitors the health of your NetBrain Servers with operations management of related services.
Ansible Agent (add-on)	integrates with Ansible to define, execute playbooks and visualize results in Change Management Runbooks. See Ansible Integration for more details.
Smart CLI (add-on)	provides a Telnet/SSH client to connect to devices from Windows and can be integrated with NetBrain workflows. See Smart CLI for more details.

Considerations for System Scalability

The following table introduces the considerations for system scalability:

Server	Scalability
Web Server Web API Server	▪ Multiple Web Servers can be installed as per data center locations and load-balanced under your load balancing infrastructure to ensure the response time for accessing web pages of Thin Client. ▪ Multiple Web API Servers can be installed with Web Servers and load-balanced under your load balancing infrastructure when there is a large number of API calls for intensive API triggered diagnosis in large networks.
Worker Server	Deploying more Worker Servers is recommended for a large number of back-end network automation tasks, such as network monitoring, path discovery, runbook execution, triggered diagnosis.
Task Engine	Supports high availability with active/standby nodes.
RabbitMQ	Supports high availability with three nodes.
Redis	Supports high availability with master/replica/sentinel nodes.
MongoDB	Supports high availability with primary/secondary/arbiter nodes.
Elasticsearch	Supports high availability with normal/master-eligible-only nodes.
Front Server	Deploying more Front Servers is recommended for a large number of network nodes. Each Front Server is recommended to manage at most 5,000 nodes.
Front Server Controller	Supports high availability with active/standby nodes.

2. System Requirements

This section introduces the hardware requirements, network connectivity requirements, and more prerequisites for deploying a distributed system.

- Reference Specification
- Network Connectivity Requirements
- Deployment Prerequisites

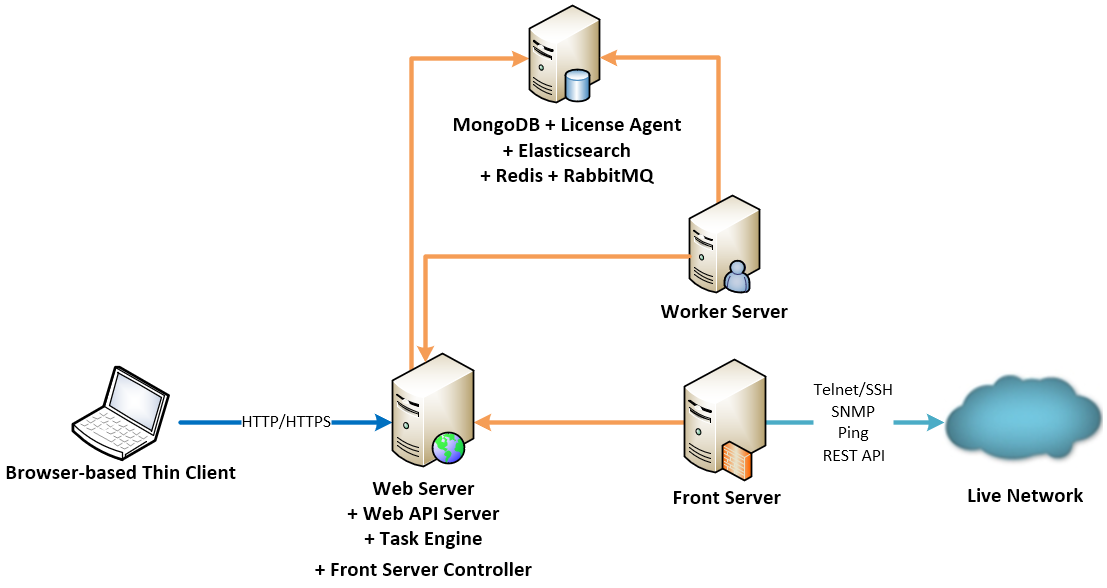
Reference Specification

As the number of network devices and concurrent users increase, the system requires a distributed environment, which requires more machines to provide resiliency and scale out flexibly based on your network scale. Both physical machines and virtual machines are supported.

Select an appropriate deployment way according to your node count:

- Distributed deployment for 2001-5000 nodes
- Distributed deployment for 5001-10000 nodes
- Distributed deployment for 10001-50000 nodes

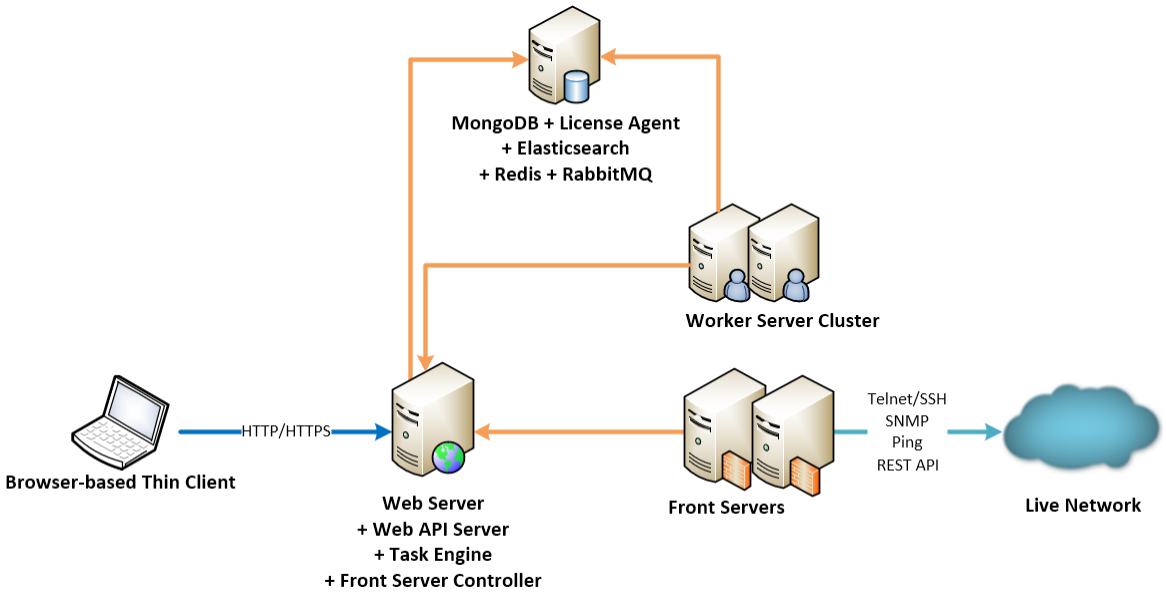
Distributed deployment for 2001~5000 nodes



Environment	NetBrain Component	Machine Count	CPU	Memory [2)]	Hard Disk	Operating System
2001~5000 nodes ≤20 users	Web Server Web API Server Task Engine Front Server Controller	1	4 Physical Cores [1)]	32GB	200GB	▪ Windows Server 2012/2012 R2 (Standard/Datacenter Edition), 64-bit ▪ Windows Server 2016/2019 (Standard/Datacenter Edition), 64-bit
	Worker Server	1	8 Physical Cores [1)]	32GB	200GB	
	Front Server	1 [4)]	4 Physical Cores [1)]	8GB	▪ 200GB (HDD) (Essential Mode; node # <=5000) [3)] ▪ 300GB (HDD) (IBA Mode; node # <=2000) [6)] ▪ 300GB (SSD) (IBA Mode; node # <=5000) [6)]	▪ Windows Server 2012/2012 R2 (Standard/Datacenter Edition), 64-bit ▪ Windows Server 2016/2019 (Standard/Datacenter Edition), 64-bit ▪ Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ Oracle Linux 7.7/7.8/7.9/8.2/8.3, 64-bit
	MongoDB License Agent Elasticsearch Redis RabbitMQ	1	4 Physical Cores [1)]	32GB	500GB [4)]	▪ Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit

Environment	NetBrain Component	Machine Count	CPU	Memory [2]	Hard Disk	Operating System
						▪ Oracle Linux 7.7/7.8/7.9/8.2/8.3, 64-bit

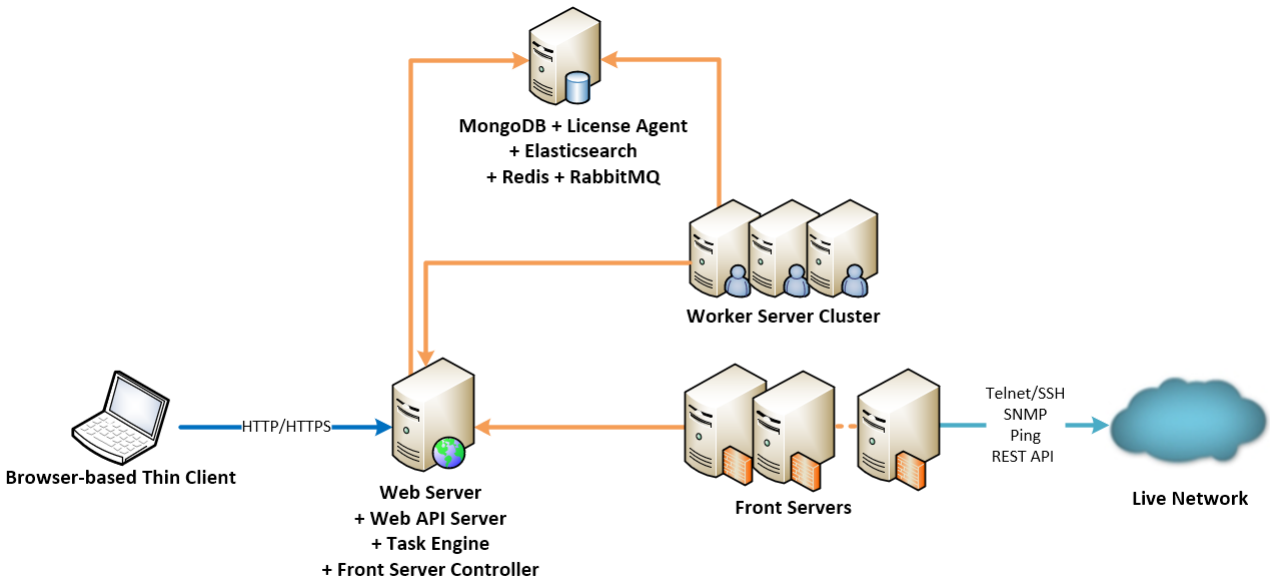
Distributed deployment for 5001~10000 nodes



Environment	NetBrain Component	Machine Count	CPU	Memory [2]	Hard Disk	Operating System
5001~10000 nodes ≤50 users	Web Server Web API Server Task Engine Front Server Controller	1	8 Physical Cores [1]	32GB	200GB	▪ Windows Server 2012/2012 R2 (Standard/Datacenter Edition), 64-bit ▪ Windows Server 2016/2019 (Standard/Datacenter Edition), 64-bit
	Worker Server	2	8 Physical Cores [1]	32GB	200GB	
	Front Server	2	4 Physical Cores [1]	8GB	▪ 200GB (HDD) (Essential Mode; node # <=5000) [3] ▪ 300GB (HDD)	▪ Windows Server 2012/2012 R2 (Standard/Datacenter Edition), 64-bit ▪ Windows Server 2016/2019 (Standard/Datacenter Edition), 64-bit ▪ Red Hat Enterprise Linux Server

Environment	NetBrain Component	Machine Count	CPU	Memory [2]	Hard Disk	Operating System
					(IBA Mode; node # <=2000) [6] ▪ 300GB (SSD) (IBA Mode; node # <=5000) [6]	7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ Oracle Linux 7.7/7.8/7.9/8.2/8.3, 64-bit
	MongoDB License Agent Elasticsearch Redis RabbitMQ	1	8 Physical Cores [1]	64GB	1TB [4]	▪ Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ Oracle Linux 7.7/7.8/7.9/8.2/8.3, 64-bit

Distributed deployment for 10001~50000 nodes



Environment	NetBrain Component	Machine Count	CPU	Memory [2)]	Hard Disk	Operating System
10001~50000 nodes ≤200 users	Web Server Web API Server Task Engine Front Server Controller	1	8 Physical Cores [1)]	32GB	200GB	▪ Windows Server 2012/2012 R2 (Standard/Datacenter Edition), 64-bit ▪ Windows Server 2016/2019 (Standard/Datacenter Edition), 64-bit
	Worker Server	3	8 Physical Cores [1)]	32GB	200GB	
	Front Server	3~10	4 Physical Cores [1)]	8GB	▪ 200GB (HDD) (Essential Mode; node # <=5000) [3)] ▪ 300GB (HDD) (IBA Mode; node # <=2000) [6)] ▪ 300GB (SSD) (IBA Mode; node # <=5000) [6)]	▪ Windows Server 2012/2012 R2 (Standard/Datacenter Edition), 64-bit ▪ Windows Server 2016/2019 (Standard/Datacenter Edition), 64-bit ▪ Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ Oracle Linux 7.7/7.8/7.9/8.2/8.3, 64-bit
	MongoDB License Agent Elasticsearch Redis RabbitMQ	1	8 Physical Cores [1)]	128GB	2TB [4)]	▪ Red Hat Enterprise Linux Server 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3, 64-bit ▪ Oracle Linux 7.7/7.8/7.9/8.2/8.3, 64-bit

Notes:

[1)] If hyper-threading is enabled, one physical core equals to two logical processors; in a virtual environment, the number of vCPUs required is twice the number of physical cores (as listed in the table).

[2)] Allocating at least half of the RAM amount for swap space on your Linux server is required to provide the necessary additional memory when the RAM space has been exhausted.

[3] For good performance of data processing and caching, it is recommended to install the Front Server on a machine equipped with Solid State Drive (SSD) when managing up to 5000 nodes.

[4] The required hard disk space must be exclusively reserved for NetBrain. And MongoDB must be installed on a machine equipped with Solid State Drive (SSD).

[5] Minimum bandwidth requirement between Front Server Controller and each Front Server: 10Mbps.

[6] If the Intent Based Automation (IBA) license is activated, It is recommended to install the Front Server on a machine equipped with:

- Solid State Drive (SSD) when managing up to 5000 nodes

- Hard Disk Drive (HDD) when managing up to 2000 nodes

[7] In order to achieve the best performance, it is recommended that the network delay between the Front Server Controller and the Front Server be within 30ms.

Network Connectivity Requirements

Source	Destination	Protocol *) and Port Number **)
Thin Client	Web Server Web API Server	HTTP/HTTPS (80/443)
Service Monitor Agent	Web API Server	HTTP/HTTPS (80/443)
Web API Server Worker Server Task Engine Front Server Controller	MongoDB	TCP 27017
Web API Server Worker Server	Elasticsearch	TCP (HTTP/HTTPS) 9200
Web API Server	License Agent	TCP 27654
Web API Server Worker Server Front Server Controller	Redis	TCP 6379
Web API Server Worker Server Task Engine Front Server Controller	RabbitMQ	TCP 5672

Source	Destination	Protocol *) and Port Number **)
Worker Server Task Engine Front Server	Front Server Controller	TCP 9095
Front Server	Live Network	ICMP/SNMP/Telnet/SSH/REST API
Front Server	Ansible Agent (add-on)	TCP 9098
MongoDB License Agent Elasticsearch Redis RabbitMQ Web Server Worker Server Task Engine Front Server Front Server Controller	Web API Server	TCP 9099
Web API Server	RabbitMQ	TCP 15672

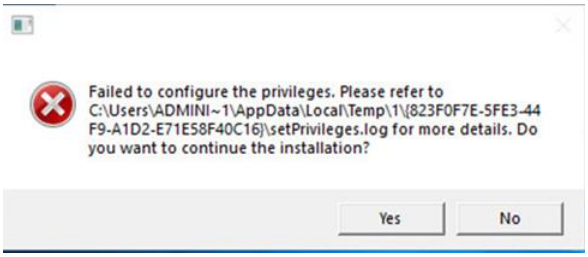
> **Note:** *) If SSL was enabled for any component including MongoDB/ElasticSearch/Redis/RabbitMQ/License Agent/Front Server Controller/Ansible Agent/Auto Update Server (within Web API Server), the SSL protocol should be added to firewall rules to enable SSL connection between servers.
>
> **Note:** **) The port numbers listed in this column are defaults only. The actual port numbers used during installation might be different.

Deployment Prerequisites

The following requirements must be satisfied before setting up your NetBrain system:

- The operating system must be installed with an English-language version (not language packs).
- When installing NetBrain servers, comply with your company security policy to set the passwords and archive them for further reference.
- NetBrain servers use hostnames to identify and communicate with each other. Make sure each server has a unique hostname.
- Add all the NetBrain installation folders and files (on both Windows and Linux) to the allow list of antivirus software for routine scans, and keep the TCP connections unblocked between NetBrain components.
- If the machine's firewall is turned on, make sure the firewall rules allow traffics to all the ports and protocols that will be used by the NetBrain system.

- **Special Requirements for Client Machine**
    - It is recommended to deploy the NetBrain Smart CLI on the same machine where the browser-based thin client is used, and the machine needs to meet the following minimum system specifications:
        - 4 Physical CPU Cores (If hyper-threading is enabled, one physical core equals to two logical processors; in a virtual environment, the number of vCPUs required is twice the number of physical cores)
        - 8GB RAM
    - Ensure to reserve at least 50% system capacity for the satisfactory performance of NetBrain Browser-based Thin Client and Smart CLI Application.
- **Special Requirements for Windows Server**
    - Users with administrative privileges of the machine are required to implement the installation.
    - NetBrain Integrated Edition should not be installed on the same server as an existing NetBrain Enterprise Edition (6.2 or earlier version), except that Front Server and Network Server (EEv6.2) can be installed on the same machine.
    - There must be more than **5GB** free space in the system drive (for example, C drive) to complete the installation no matter which drives the NetBrain system will be installed on.
    - Temporarily disable antivirus software during the installation process.
    - Ensure the NetBrain installation process using administrator account has the necessary permissions to modify "User Rights Assignment" in "Local Security Policy" or change the local user privileges. Otherwise, the following error message will prompt when installing each Windows component.



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

> **Note:** Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.
>
> **Note:** After clicking 'No', please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

- **Special Requirements for Linux Server**

- Users with root privileges of the machine are required to implement the installation.
- It is highly recommended to store the data files and log files of NetBrain servers into separated disk partitions. Make sure each partition has enough disk space.
  - More than **100GB** free space in the directory where the data files of MongoDB/Elasticsearch will be saved.
  - More than **50GB** free space in the directory where the log files of MongoDB/Elasticsearch will be saved.
  - More than **180GB** free space for the Front Server PostgreSQL data path.

3. Deploying and Installing System

Select an appropriate way to deploy the system based on your network scale and locations. Install the system components in the following order:

1. Install MongoDB on Linux.
2. Install Elasticsearch on Linux.
3. Install License Agent on Linux.
4. Install Redis on Linux.
5. Install RabbitMQ on Linux.
1. Install Service Monitor Agent.
2. Install Web/Web API Server on Windows.
3. Install Worker Server on Windows.
6. Install Task Engine on Windows.
7. Install Front Server Controller on Windows.
8. Install Front Server.

> **Note:** To avoid unexpected clock synchronization issues, it is highly recommended to configure Network Timing Protocol (NTP) client on the machines where NetBrain servers will be installed. See Configuring NTP Client on NetBrain Servers for more details.

3.1. Installing MongoDB on Linux

Pre-installation Tasks

- Service Monitor Agent will be installed with MongoDB and it has dependencies on the third-party package **zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa|grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel|gcc"` command to check whether it has been installed on this Linux server. If it has not been installed yet, you can choose either option below to install the dependencies:
  - **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install it online.
  - **Offline Install:** refer to Offline Installing Third-party Dependencies for more details.

> **Note**: You can also install the Service Monitor Agent separately.

Installing MongoDB

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

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

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

   > **Note**: Do not place the installation package under any personal directories, such as **/root**.

3. Run the `cd /opt/netbraintemp10.0` command to navigate to the /**opt/netbraintemp10.0** directory.

4. Download the installation package.

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

     > **Note:** The download link is case-sensitive.
     >
     > **Tip:** Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

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

```
[root@centos netbraintemp10.0]# tar -zxvf mongodb-linux-x86_64-rhel-4.0.19-10.0.tar.gz
MongoDB/
MongoDB/config/
MongoDB/config/setup.conf
...
MongoDB/others/
MongoDB/others/install.conf
MongoDB/others/setup.conf.template
```

```
MongoDB/others/uninstall.sh
...
MongoDB/install.sh
...
```

6. Run the `cd MongoDB/config` command to navigate to the **config** directory.

7. 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, refer to Editing a File with VI Editor.

```
[root@centos config]# vi setup.conf
#NetBrain Database configuration file
#Note: Entries other than the database username and password
#can only contain letters or numbers, and should start with a letter.
DataPath=/usr/lib
LogPath=/var/log
BindIp=10.10.3.142
FQDN=127.0.0.1
#The port must be between 1025 and 32767.
Port=27017
ReplicaSetName=rs
UseSSL=no
Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem
#The UserName or Password cannot be empty
#The UserName or Password should not contain: {}[]:",'|<>@&^%\ or a space.
#The length of UserName or Password should not be more than 64 characters.
UserName=admin
Password=Admin1.#
CPULimit=55%
MemoryLimit=55%
#List all replica set members. The members should be separated with spaces. The total number of
members should be an odd number.
#The first member will be used as the primary member, the last will be used as the arbiter. The
rest are the secondary members.
#It is recommended to use FQDN. The address of 0.0.0.0 or 127.0.0.1 is not allowed. For example:
#ReplicaSetMembers=192.168.1.1 192.168.1.2 192.168.1.3
ReplicaSetMembers=10.10.3.142
```

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

9. Run the `./install.sh` script under the **MongoDB** directory to install MongoDB as well as create the configured admin username and password for logging in to MongoDB. Configure the following parameters one by one with an interactive command line.

```
[root@centos MongoDB]# ./install.sh
INFO: Checking date.
INFO: Checking Linux OS version.
INFO: Starting to check if rpm exists.
INFO: MongoDB was not installed. Fresh installation is required.
INFO: Dependent Package:
INFO: Component Name: MongoDB
INFO: RPM name: mongodbconfig
INFO: RPM package list: mongodbconfig-4.0.19-el7.x86_64.rpm
```

```
INFO: Preprocessing SUCCEEDED
INFO: Collecting system information.
INFO: Collecting system information SUCCEEDED.
INFO: Checking systemd.
INFO: System checking SUCCEEDED
INFO: Username is admin
INFO: SSL enable status is no
INFO: Configuration parameters updating SUCCEEDED
INFO: Configuration parameters checking SUCCEEDED
Getting rpm dependency list of MongoDB and Service Monitor Agent...
INFO: Dependency list: zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel
tk-devel libffi-devel gcc
INFO: Component name: Service Monitor Agent
INFO: Service name: netbrainagent
INFO: Installation path: /usr/share/nbagent
INFO: Config path: /etc/netbrain/nbagent
INFO: Preprocessing SUCCEEDED.
INFO: Starting to install Service Monitor Agent ...
INFO: Starting to check system...
INFO: Collecting system information SUCCEEDED.
INFO: System checking SUCCEEDED.
INFO: Start dependencies checking...
INFO: Dependencies checking SUCCEEDED.
INFO: Starting to check configuration parameters...
Configuring Service Monitor Agent ...
The values in brackets are the default values of the parameters. To keep the default value for
the current parameter,
press the Enter key.
Please enter the URL (must end with /) to call NetBrain Web API service for the Service Monitor
[http(s):
//<IP address or hostname of NetBrain Application Server>/]: http://10.10.3.141/
Please enter the API Key to be used to communicate with application server which must be the
same as the one created on Web API server:
Please re-enter API key to confirm:
Please enter a log path for NetBrain Service Monitor [/var/log/netbrain/nbagent]:
NetBrain Web API service URL:   http://10.10.3.141/ServicesAPI
API key:                ******
NetBrain Service Monitor LogPath:       /var/log/netbrain/nbagent
Certificate Authority verification:             no
Do you want to continue using these parameters? [yes]
...
INFO: Successfully logged in MongoDB with username: "admin", password: "******"
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed MongoDB
INFO: Please restart the operating system to make kernel settings of MongoDB to take effect.
```

> **Note:** You'll need to use the interactive command line to install the Service Monitor Agent with MongoDB:
>
> - The log path for Service Monitor Agent must have at least 10G free space. You can keep the default path or input your required path after inputting the URL and API key.

> - If https:// is used in the Web API Service URL, you will be asked whether to enable the Certificate Authority verification and input the Certificate Authority file if enabled. The API Key is the key to be used later to install Web API Server and they must be same.

10. After MongoDB is successfully installed, run the `reboot` command to restart the machine.

11. After the machine starts, run the `ps -ef|grep mongo` or `systemctl status mongod` command to verify whether its service starts successfully.

```
[root@centos ~]# ps -ef|grep mongo
netbrain  46482     1  3 01:30 ?        00:00:03 /bin/mongod -f /etc/mongodb/mongod.conf
root      46639  37939  0 01:31 pts/2    00:00:00 grep --color=auto mongo

[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 Tue 2021-02-23 22:04:41 EST; 2min 41s ago
 Process: 6136 ExecStart=/bin/mongod -f /etc/mongodb/mongod.conf (code=exited, status=0/SUCCESS)
 Main PID: 6375 (mongod)
  Memory: 902.3M (limit: 8.5G)
...
```

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

Parameters

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

Parameter	Default Value	Description
DataPath	`/usr/lib`	Specify the storage path for all MongoDB data files. **Note:** Make sure the destination directory has more than **100GB** free space to save all the data files. **Tip:** You can run the `df -h` command to check which directory has been mounted to a large disk.
LogPath	`/var/log`	Specify the storage path for all MongoDB log files. **Note:** Make sure the destination directory has more than **50GB** free space to save all the log files.
BindIp	`127.0.0.1`	Specify the IP address of MongoDB. **Note:** Don't use **127.0.0.1**. **Note:** If you want to use the fully qualified domain name (FQDN) to connect to MongoDB, you need to set it as **0.0.0.0**.

Parameter	Default Value	Description
FQDN	`127.0.0.1`	Specify the fully qualified domain name (FQDN) of MongoDB. **Note:** If you select to specify the FQDN for MongoDB, you must specify the FQDN in the **ReplicaSetMembers** parameter and when installing other components that require to connect to MongoDB.
Port	`27017`	Specify the port number that the MongoDB service listens to. It is recommended to keep the default value.
ReplicaSetName	`rs`	Specify the replica set name used for replication. It is recommended to keep the default value. If you want to modify it, keep notes of your customized one because it is required to connect to MongoDB when you install other components, such as Web API Server, Worker Server, Task Engine, and Front Server Controller. **Note:** It can only contain letters and numbers, and must start with a letter.
UseSSL	`no`	Specify whether to encrypt the connections to MongoDB with SSL. To enable SSL, replace `no` with `yes`. For detailed requirements of SSL certificates and keys, refer to SSL Certificate Requirements.
Certificate	`/etc/ssl/cert.pem`	Specify the name and storage path of the certificate file that contains the public key. **Note:** It is required only if **UseSSL** is enabled.
PrivateKey	`/etc/ssl/key.pem`	Specify the name and storage path of the private key file. **Note:** It is required only if **UseSSL** is enabled.
UserName	`admin`	Specify the admin username used to connect with and log in to MongoDB. **Note:** The value of the **DBUser** and **DBPassword** parameters cannot contain any of the following special characters, and their length cannot exceed 64 characters. `{ } [ ] : " , ' | < > @ & ^ % \` and `spaces`
Password	`Admin1.#`	Specify the admin password used to connect with and log in to MongoDB.
CPULimit	`55%`	Specify the maximum CPU utilization that can be consumed by MongoDB. To make both MongoDB and Elasticsearch reasonably share the CPU resources of the same machine, the recommended value is **55%**.
MemoryLimit	`55%`	Specify the maximum memory capacity of the machine that can be consumed by the MongoDB. To make both MongoDB and Elasticsearch utilize the memory resources of the same machine, the recommended value is **55%**.
ReplicaSetMembers	`127.0.0.1`	Enter the actual IP address to be bound or FQDN.

3.2. Installing Elasticsearch on Linux

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

Installing Elasticsearch

NetBrain adopts Elasticsearch as a full-text search and analytics engine in a distributed multi-user environment.

> **Note**: Elasticsearch has a dependency on **AdoptOpenJDK v11.0.9**, which will be automatically installed while Elasticsearch is installed.

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

     > **Note:** The download link is case-sensitive.
     >
     > **Tip:** Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.
5. Run the `tar -zxvf elasticsearch-linux-x86_64-rhel-6.8.12-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

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

```
...
Elasticsearch/install.sh
...
```

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

7. Modify the parameters in the **setup.conf** file located under the **config** directory and save the changes. For how to modify the configuration file, refer to Editing a File with VI Editor.

```
[root@centos config]# vi setup.conf
# Account info
# The UserName or Password should not contain: {}[]:",'|<>@&^%\ or a space
# The first character of UserName and Password cannot be ! or #.
# The length of UserName or Password should not be more than 64 characters
UserName=admin
Password=Admin1.#

# DataPath is used to store data files for Elasticsearch. This directory must be at least a
second level directory and used exclusively for this purpose.
DataPath=/var/lib/elasticsearch
# LogPath is used to store log files for Elasticsearch. This directory must be at least a
second level directory and used exclusively for this purpose.
LogPath=/var/log/elasticsearch

# BindIp: The IP address to be bound to provide service. 127.0.0.1 is not allowed. If this IP
is set as default 0.0.0.0, you can use Fully Qualified
Domain Name (FQDN) in ClusterMembers.
BindIp=0.0.0.0

# Port is used to start elasticsearch service on specified port. The port must be between 1025
and 32767.
Port=9200

# CPULimit and MemoryLimit should be ended by % and the range is from 1% to 100%.
CPULimit=35%
MemoryLimit=25%

# Specify whether to enable Secure Sockets Layer(SSL)
# By default, it is disabled. "no" indicates disabled; "yes" indicates enabled.
UseSSL=no
# If SSL is enabled, you must enter the full path of the server certificate and key file.
Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem
CertAuth=/etc/ssl/cacert.pem

# SingleNode: Define the node type. Default 'yes' indicates standalone node. For cluster,
please set it as 'no'.
SingleNode=yes
# ClusterMembers: List all the cluster member's IP addresses here, using ',' to separate each
of them.
ClusterMembers=10.10.2.34,10.10.2.35,10.10.2.36

#It is not supported to firstly install the master-only node.
MasterOnlyNode=no
```

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

9. Run the `./install.sh` script under the **Elasticsearch** directory.

```
[root@centos Elasticsearch]# ./install.sh
INFO: Creating installation log file SUCCEEDED
INFO: Collecting system information SUCCEEDED.
INFO: Component Name: Elasticsearch
INFO: RPM name: elasticsearch-oss
INFO: Service name: elasticsearch
INFO: Installation path: /usr/share/elasticsearch
INFO: Config path: /etc/elasticsearch
INFO: Preprocessing SUCCEEDED.
INFO: Start installing Elasticsearch...
INFO: Starting to install Elasticsearch ...
INFO: Starting to system checking...
INFO: System checking SUCCEEDED.
INFO: Starting to configuration parameters checking...
...
Preparing...                          ################################# [100%]
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Updating / installing...
   1:elasticsearch-oss-0:6.8.12-1      ################################# [100%]
### NOT starting on installation, please execute the following statements to configure
elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch
INFO: Official rpm package installing SUCCEEDED.
INFO: Starting to configuration parameters updating...
...
INFO: Successfully connected to the elasticsearch. The setup is complete.
 elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset:
disabled)
   Active: active (running) since Wed 2021-02-24 00:11:21 EST; 31s ago
     Docs: http://www.elastic.co
 Main PID: 25040 (java)
   Memory: 4.1G
  CGroup: /system.slice/elasticsearch.service
          25040 /usr/local/jdk-11.0.1//bin/java -Xms3969m -Xmx3969m -XX:+UseConcMarkSweepGC -
...
INFO: Successfully installed Elasticsearch. Service is running.
   Active: active (running) since Wed 2021-02-24 00:11:55 EST; 10s ago
INFO: netbrainagent has been restarted.
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Succeeded in installing Elasticsearch
```

10. Run the following command to verify whether the Elasticsearch service is running.

```
curl -s -XGET --user <user:password> http://<IP address of Elasticsearch>:<Port>
```

Example:

```
[root@centos Elasticsearch]# curl -s -XGET --user admin:admin http://10.10.3.142:9200
{
  "name" : "localhost.localdomain",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : " zQxrYOooSzmUMRG5C-fwrA",
  "version" : {
    "number" : "6.8.12",
    "build_flavor" : "oss",
    "build_type" : "rpm",
    "build_hash" : "a9861f4",
    "build_date" : "2020-08-12T07:27:20.804867Z",
    "build_snapshot" : false,
    "lucene_version" : "7.7.3",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

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

Parameters

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

Parameter	Default Value	Description
UserName	**admin**	Specify the admin username used to log in to Elasticsearch. **Note:** The username and password cannot contain any of the following special characters, and its length cannot exceed 64 characters. `{ } [ ] : " , ' | < > @ & ^ % \` and `spaces`
Password	**Admin1.#**	Specify the admin password used to log in to Elasticsearch. **Note:** The password cannot be empty, and it cannot start with **!** or **#**.
DataPath	**/var/lib/elasticsearch**	Specify the storage path for all data files of Elasticsearch. It is recommended to keep the default path. **Note:** If you want to modify it, don't use an existing directory. **Note:** Make sure the directory has more than **100GB** free space to save all the data files. **Tip:** You can run the `df -h` command to check which directory has been mounted to a large disk.

Parameter	Default Value	Description
LogPath	`/var/log/elasticsearch`	Specify the storage path for all log files of Elasticsearch. **Note:** It is recommended to keep the default path as it is. If you want to modify it, don't use an existing directory. **Note:** Make sure the directory has more than **50GB** free space to save all the log files.
BindIp	`0.0.0.0`	Enter the IP address of the network card you want to use for the Elasticsearch. **Note**: Modify the value only if you have multiple network cards on this machine.
Port	`9200`	Specify the port number that Elasticsearch service listens to.
CPULimit	`35%`	Specify the maximum CPU utilization that can be consumed by Elasticsearch. To make both MongoDB and Elasticsearch utilize the CPU resources of the same machine, the recommended value is **35%**. And the sum of CPU utilization allocated to the MongoDB and Elasticsearch cannot exceed **90%** of the machine's CPU.
MemoryLimit	`25%`	Specify the maximum memory capacity of the machine that can be consumed by Elasticsearch. To make both MongoDB and Elasticsearch utilize the memory resources of the same machine, the recommended value is in the range of **12.5%~25%**. **Note:** The maximum memory that Elasticsearch can utilize is **35%**. Setting the value of the **MemoryLimit** parameter to higher than **35%** will not increase the performance of Elasticsearch. Instead, it may affect the performance of co-existing servers on this machine.
UseSSL	`no`	Set whether to enable the encrypted connections to Elasticsearch by using SSL. For detailed requirements of SSL certificates and keys, refer to SSL Certificate Requirements.
Certificate	`/etc/ssl/cert.pem`	Specify the name of the SSL certificate file containing the public key. **Note:** It is required only if **UseSSL** is enabled.
PrivateKey	`/etc/ssl/key.pem`	Specify the name of the SSL private key file. **Note:** It is required only if **UseSSL** is enabled.
CertAuth	`/etc/ssl/cacert.pem`	Specify the name of the SSL certificate chain or intermediate certificate (class 2 or class 3 certificate). **Note:** It is required only if **UseSSL** is enabled.

Parameter	Default Value	Description
SingleNode	`yes`	Set whether to enable cluster deployments. The default option `yes` means cluster deployment is disabled. For a standalone Elasticsearch, keep the default option as it is.
ClusterMembers	`10.10.2.34,10.10.2.35,10.10.2.36`	This parameter is only required for cluster deployments. For a standalone Elasticsearch, keep the default value as it is.
MasterOnlyNode	`no`	Set whether the node is master-eligible-only. For a standalone Elasticsearch, keep the default value as it is.

3.3. Installing License Agent on Linux

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

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

     > **Note:** The download link is case-sensitive.
     >
     > **Tip:** Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.
4. Run the `tar -zxvf netbrain-licenseagent-linux-x86_64-rhel-10.0.tar.gz` command under the **/opt/netbraintemp10.0** directory to extract installation files.

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

```
...
License/install.sh
...
```

5. Run the `cd License/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, refer to Editing a File with VI Editor.

```
[root@localhost config]# vi setup.conf
# The IP address of the License Agent Server.
BindIp=0.0.0.0
# The port number that the License Agent Server listens to. It should be more than 1025 and less
than 32767. By default, it is 27654.
Port=27654
# Specify whether to use SSL to encrypt the connections to the License Agent Server.
# By default, it is disabled. no indicates disabled; yes indicates enabled.
UseSSL=no
# If SSL is enabled, you must enter the full path of the server certificate and key file.
Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem
# LogPath is used to store log files for the service of netbrainlicense.
# This directory must be at least a second level directory and used exclusively for this
purpose.
LogPath=/var/log/netbrain/netbrainlicense
```

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

8. Run the `./install.sh` script under the **License** directory to install License Agent.

   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 each Linux component.

```
[root@localhost License]# ./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 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: Starting to check Linux OS info...
```

```
INFO: Creating installation log file SUCCEEDED
INFO: Dependent packages:
INFO: Component Name: License Agent
INFO: RPM name: netbrainlicense
INFO: Preprocessing SUCCEEDED.
...
INFO: Installing /opt/netbraintemp/License/sources/netbrainlicense-10.0-el7.x86_64.rpm
Preparing...                          ########################################
Find configuration file
/var/log/netbrain/installationlog/licenseagent/install_licenseagent.conf.
Bind IP: 0.0.0.0
License Agent port: 27654
The NetBrain License Agent will not use SSL to communicate.
Updating / installing...
   1:netbrainlicense-10.0-el7              ########################################
Bind IP: 0.0.0.0
License Agent port: 27654
The NetBrain License Agent will not use SSL to communicate.
User name: netbrain
User group: netbrain
NetBrain License Agent Server has been started.
Redirecting to /bin/systemctl status firewalld.service
Successfully installed NetBrain License Agent.
INFO: 2020-01-13 00-26-30.295: Rpm package installing SUCCEEDED.
INFO: 2020-01-13 00-26-30.304: Starting permission assigning...
INFO: Port 27654 is added to the firewall.
INFO: 2020-01-13 00-26-30.359: Permission assigning SUCCEEDED.
Created symlink from /etc/systemd/system/multi-user.target.wants/netbrainlicense.service to
/usr/lib/systemd/system/netbrainlicense.service.
?netbrainlicense.service - NetBrain license agent service
   Loaded: loaded (/usr/lib/systemd/system/netbrainlicense.service; enabled; vendor preset:
disabled)
   Active: active (running) since Mon 2020-01-13 00:26:30 EST; 18ms ago
  Process: 15534 ExecStop=/usr/bin/pkill licensed (code=exited, status=0/SUCCESS)
  Process: 15540 ExecStart=/usr/bin/netbrainlicense/licensed -f
/etc/netbrain/netbrainlicense/licensed.conf (code=exited, status=0/SUCCESS)
  Process: 15536 ExecStartPre=/bin/chmod o+r /sys/class/dmi/id/product_uuid (code=exited,
status=0/SUCCESS)
 Main PID: 15541 (licensed)
   Memory: 1.0M
   CGroup: /system.slice/netbrainlicense.service
           15541 /usr/bin/netbrainlicense/licensed -f
/etc/netbrain/netbrainlicense/licensed.conf
Jan 13 00:26:30 localhost.localdomain systemd[1]: Starting NetBrain license agent service...
Jan 13 00:26:30 localhost.localdomain systemd[1]: Started NetBrain license agent service.
INFO: 2021-02-24 01-30-48.747: Successfully installed License Agent. Service is running.
INFO: 2021-02-24 01-30-48.775: Backing up uninstall.sh SUCCEEDED
INFO: 2021-02-24 01-30-48.785: Successfully installed License Agent.
```

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

9. Run the `systemctl status netbrainlicense` command to check the service status of License.

```
[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 Wed 2021-02-24 01:30:48 EST; 8min ago
  Process: 6054 ExecStart=/usr/bin/netbrainlicense/licensed -f
/etc/netbrain/netbrainlicense/licensed.conf (code=exited, status=0/SUCCESS)
  Process: 5907 ExecStartPre=/bin/chmod o+r /sys/class/dmi/id/product_uuid (code=exited,
status=0/SUCCESS)
 Main PID: 6138 (licensed)
   Memory: 8.2M
   CGroup: /system.slice/netbrainlicense.service
           └─6138 /usr/bin/netbrainlicense/licensed -f
/etc/netbrain/netbrainlicense/licensed.conf

Jul 19 09:02:40 localhost.localdomain systemd[1]: Starting NetBrain license agent service...
Jul 19 09:02:40 localhost.localdomain systemd[1]: Started NetBrain license agent service.
```

Parameters

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

Parameter	Default Value	Description
BindIp	`0.0.0.0`	Specify the IP address of License Agent. **Note:** Modify the value only if you have multiple network cards on this machine.
Port	`27654`	The port number that the License Agent Server listens to.
UseSSL	`no`	Set whether to encrypt the connections to the License Agent with SSL. To enable SSL, modify it to **yes**. For detailed requirements of SSL certificates and keys, see SSL Certificate Requirements.
Certificate	`/etc/ssl/cert.pem`	Specify the storage path and name of the SSL certificate that contains the public key. **Note:** It is required only if **UseSSL** is enabled. **Note**: Do not set the values of the **Certificate**, **PrivateKey**, and **LogPath** arguments to any personal directories, such as **/root.** Besides, do not include any special characters or spaces except slashes (/) in the values.

Parameter	Default Value	Description
PrivateKey	`/etc/ssl/key.pem`	Specify the storage path and name of the SSL private key file. **Note:** It is required only if **UseSSL** is enabled.
LogPath	`/var/log/netbrain/netbrainlicense`	Specify the storage path for all License Agent log files.

3.4. Installing Redis on Linux

Pre-installation Tasks

- Redis has dependencies on the third-party package **logrotate**. Before you install the Redis, run the `rpm -qa|grep logrotate` command to check whether it has been installed on the server. If it has not been installed yet, you can choose either option below to install the dependencies.
  - **Online Install:** run the `yum -y install logrotate` command to install it online.
  - **Offline Install:** refer to Offline Installing Third-party Dependencies for more details.

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

Installing Redis on Linux

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

> **Note:** The download link is case-sensitive.
>
> **Tip:** Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

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

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

6. Run the `cd redis/config` command to navigate to the **config** directory.

7. Modify the parameters in the **setup.conf** file located under the **config** directory and save the changes. For how to modify the configuration file, refer to Editing a File with VI Editor.

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

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

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

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

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

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

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

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

NodeRole=master
#Master Node (Master Node can support ip address, hostname or FQDN and is used if the Mode is
```

```
cluster)
MasterNode=
# Sentinel Port is used to start the redis sentinel service on specified port. We use default
port 6380.
# For a multi-DC DR cluster there will be 2 instances of sentinel on same arbiter node so user
should change this value to default port 6381
or any other port which is not used by other service.
# Please enter the same sentinelPort for all nodes that belong to the same cluster
SentinelPort=6380

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

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

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

9. Run the `./install.sh` script under the **redis** directory to install Redis.

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

```
...
INFO: Checking redis Status
INFO: Verification SUCCEEDED
INFO: Backup uninstall.sh SUCCEEDED
INFO: Backup fix_releaseinfo.json SUCCEEDED
INFO: Successfully installed Redis
```

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

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

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

Parameters

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

Parameter	Default Value	Description
Password	**Admin1.#**	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**, **sentinel** and **dr-sentinel** . Keep the default value for a standalone deployment.
MasterNode		This parameter is only required for cluster deployments.
SentinelPort	**6380**	The port number that the sentinel or dr-sentinel node listens to. **Note:** Use alternative port such as 6381 when deploying the dr-sentinel node.

Parameter	Default Value	Description
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 an SSL service agent. Stunnel will be automatically installed together with Redis. For detailed requirements of SSL certificates and keys, refer to SSL Certificate Requirements.
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.
CertAuth	`/etc/ssl/cacert.pem`	Specify the name of the SSL certificate chain or intermediate certificate (class 2 or class 3 certificate). **Note:** It is required only if **UseSSL** is enabled.

3.5. Installing RabbitMQ on Linux

Pre-Installation Task

RabbitMQ has dependencies on the third-party package **socat** and **logrotate**. Before you install the RabbitMQ, run the `rpm -qa|grep socat` and `rpm -qa|grep logrotate` commands to check whether they have been installed on the server. If they have not been installed yet, you can choose either option below to install the dependencies.

- **Online Install:** run the `yum -y install socat` and `yum -y install logrotate` commands to install them online.
- **Offline Install:** refer to Offline Installing Third-party Dependencies for more details.

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

Installing RabbitMQ on Linux

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

     > **Note:** The download link is case-sensitive.
     >
     > **Tip:** Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

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

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

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

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

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

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

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

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

# Resource limitation
ResourceLimit=no

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

# TLS
UseSSL=no
Certificate=/etc/ssl/cert.pem
PrivateKey=/etc/ssl/key.pem

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

# Log path
LogPath=/var/log/rabbitmq
```

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

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

```
[root@localhost rabbitmq]# ./install.sh
INFO: Start checking date
INFO: Start checking os
INFO: Start checking required CPU
INFO: Start checking minimum memory
INFO: Selinux-policy version: 3.13.1
INFO: Component Name: RabbitMQ
INFO: RPM name: rabbitmq-server
INFO: Service name: rabbitmq-server
INFO: RPM package list: erlang-23.2.1-1.el7.x86_64.rpm rabbitmq-server-3.8.9-1.el7.noarch.rpm
INFO: Installation path: /usr/lib/rabbitmq/
INFO: Config path: /etc/rabbitmq/
INFO: Preprocessing SUCCEEDED
...
Preparing...                          ########################################
Updating / installing...
rabbitmq-server-3.8.1-1.el7           ########################################
INFO: Official rpm package installing SUCCEEDED
INFO: Configuration parameters updating SUCCEEDED
INFO: Permission setting 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: 53927 (beam.smp)
   Status: "Initialized"
   Memory: 70.8M (limit: 15.5G)
...
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed RabbitMQ
```

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

```
[root@localhost ~]# systemctl status rabbitmq-server
 rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset:
disabled)
   Active: active (running) since Mon 2020-07-13 16:05:23 EDT; 13min ago
   Process: 19522 ExecStop=/usr/sbin/rabbitmqctl shutdown (code=exited, status=0/SUCCESS)
 Main PID: 4509 (beam.smp)
   Status: "Initialized"
   Memory: 96.5M
...
```

Parameters

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

Parameter	Default Value	Description
Username	`admin`	Specify the admin username used to connect to RabbitMQ. **Note:** The username and password cannot contain any of the following special characters, and its length cannot exceed 64 characters. `{ } [ ] : " , ' | < > @ & ^ % \` and `spaces`
Password	`Admin1.#`	Specify the admin password used to connect to RabbitMQ.
Mode	`standalone`	Set the RabbitMQ deployment Mode. Available options are **standalone** or **mirror**. Keep the default value **standalone** for a standalone deployment.
ClusterId	`rabbitmqcluster`	Specify the cluster id used by all nodes to join the cluster. This parameter is required only for cluster deployments.
NodeRole	`master`	Set the role for the current node. Available options are **master** or **slave**. Keep the default value for a standalone deployment.
MasterNode	`localhost`	This parameter is required for both standalone and cluster deployments. For standalone Mode, this parameter should be set as a resolvable hostname of the local server.

Parameter	Default Value	Description
ResourceLimit	`no`	Set whether to limit the system resource usage for RabbitMQ.
CPULimit	`100%`	Specify the maximum CPU utilization of the machine that can be consumed by RabbitMQ.
MemoryLimit	`100%`	Specify the maximum memory capacity of the machine that can be consumed by RabbitMQ.

UseSSL	`no`	Set whether to enable the encrypted connections to RabbitMQ by using SSL.
		
		Tip: If **UseSSL** is set to **yes**, you can follow the steps below to modify the RabbitMQ Plugin config file after the service monitor is installed.
		
		1) Run the `vi /etc/netbrain/nbagent/check/rabbitmq.yaml` command to open the RabbitMQ Plugin config file.
		
		2) Set the **ssl** value to **true** and save the changes. For how to modify the configuration file, see Editing a File with VI Editor for more details.
		
		`[root@localhost check]# vi rabbitmq.yaml`
		`init_config:`
		
		`instances:`
		`- name: default`
		`managementPort: 15672,`
		`checkAvailableIntervalSeconds: 300`
		`ssl: true`
		`collectQueues:`
		`equal: []`
		`startWith:`
		`['FullTextSearch','TaskManager','event_callback','RMClientCallback','ETL_Task']`
		`endWith: ['IndexDriver']`

Certificate	`/etc/ssl/cert.pem`	Specify the storage path for all the certificates and key files used for SSL authentication. **Note:** It is required only if **UseSSL** is enabled.
PrivateKey	`/etc/ssl/key.pem`	Specify the name of SSL private key file. **Note:** It is required only if **UseSSL** is enabled.
Port	`5672`	Specify the port number that RabbitMQ service listens to.
LogPath	`/var/log/rabbitmq`	Specify the directory to save logs of RabbitMQ.

3.6. 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

3.6.1.Installing Service Monitor Agent on Linux

Pre-installation Tasks

- Service Monitor Agent will be installed with all Linux components and it has dependencies on the third-party package **zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc**. Run the `rpm -qa|grep -E "zlib-devel|readline-devel|bzip2-devel|ncurses-devel|gdbm-devel|xz-devel|tk-devel|libffi-devel|gcc"` command to check whether it has been installed on this Linux server. If it has not been installed yet, you can choose either option below to install the dependencies:
  - **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install it online.
  - **Offline Install:** refer to Offline Installing Third-party Dependencies for more details.

Installing Service Monitor Agent on Linux

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

     > **Note:** The download link is case-sensitive.

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

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

```
[root@localhost netbraintemp10.0]# tar -zxvf netbrain-servicemonitoragent-linux-x86_64-rhel-
10.0.tar.gz
ServiceMonitorAgent/
ServiceMonitorAgent/config/
ServiceMonitorAgent/config/setup.conf
...
ServiceMonitorAgent/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, refer to Editing a File with VI Editor.

```
[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://10.10.3.141/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=Admin1.#

# 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/nbagent

# CA_Verify determines whether to enable certificate Authority (CA) verification which is used
by the system website: By default, it is disabled.
yes indicates enabled; no indicates disabled.
# Note: To enable CA verification, 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
```

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 to install Service Monitor Agent ...
Starting to system checking...
  Collecting system information...
...
  Collecting system information SUCCEEDED.
System checking SUCCEEDED.
Starting to configuration parameters checking...
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
You are using pip version 18.1, however version 19.0.3 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Configuration parameters updating SUCCEEDED.
Starting to permission assigning...
Permission assigning SUCCEEDED.
Starting to deamon setting...
Deamon setting SUCCEEDED.
...
Successfully installed Service Monitor Agent. Service is running.
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed Service Monitor Agent.
```

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 Sat 2019-05-04 23:19:09 EDT; 5min ago
 Main PID: 4520 (python3)
   Memory: 73.5M
...
```

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

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

Example: If you use FQDN during MongoDB installation, do the following:

1) Run the `cd /etc/netbrain/nbagent/checks` command to navigate to the **checks** directory.
2) Add the following DNS info to the **mongodb.yaml** file, and save the changes. For how to modify the file, refer to Editing a File with VI Editor.

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

```
init_config:

instances:
    - name: default
      dns: mongo2.cloud.netbraintech.com
```

Example: If you installed multiple MongoDB instances on one server with different ports and service names (e.g,, instance 1 with service name mongod and port 27017; instance 2 with service name mongod2 and port 27018), 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, refer to Editing a File with VI Editor.

> **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.
>
> **Note**: Parameter `name` refers to the MongoDB service name.

```
init_config:

instances:
    - name: mongod
      port: 27017
    - name: mongod2
      port: 27018
```

Parameters

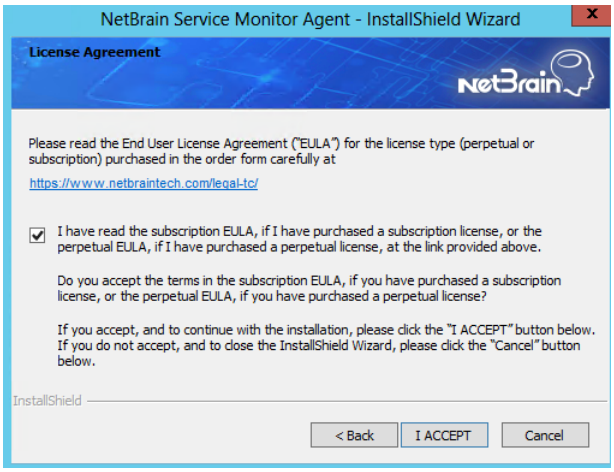
Parameter	Default Value	Description
Server_Url	`http://localhost/ServicesAPI`	The URL used to call the Web API service, http://<IP address of NetBrain Web API Server>/ServicesAPI. For example, **http://10.10.3.141/ServicesAPI**. **Note**: If SSL will be enabled with https binding created for the system website in IIS Manager, type **https** in the URL. Besides, if **CA_Verify** is enabled, hostname must be specified in the URL.
Server_Key	`Admin1.#`	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.
LogPath	`/var/log/netbrain/nbagent`	The storage path for the log files of the Service Monitor Agent. **Note:** At least 10GB free disk space is required.
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**.
CertAuth	`/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.

3.6.2.Installing Service Monitor Agent on Windows

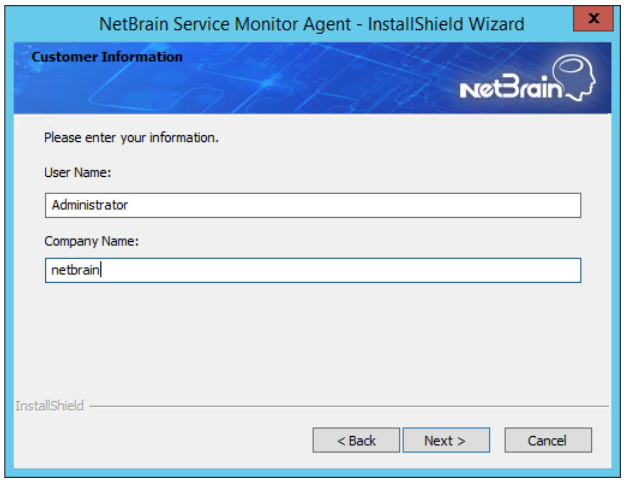
Complete the following steps with administrative privileges.

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

1) 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**.

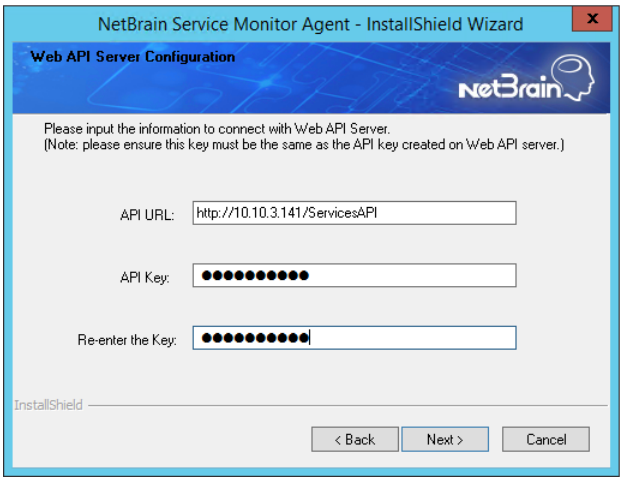


4) On the Customer Information page, enter your company name, and then click **Next**.



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

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



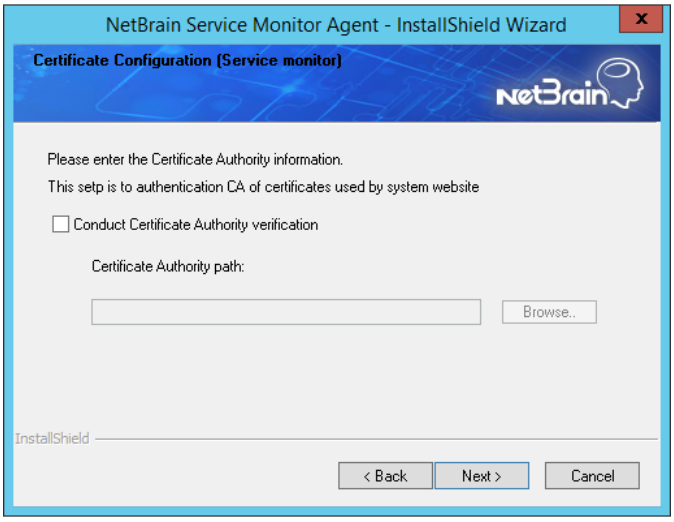
- **API URL** — the URL used to call the Web API service, **http://<IP address of NetBrain Web API Server>/ServicesAPI**. For example, **http://10.10.3.141/ServicesAPI.**

  > **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.

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

7) 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**.



To authenticate CA:

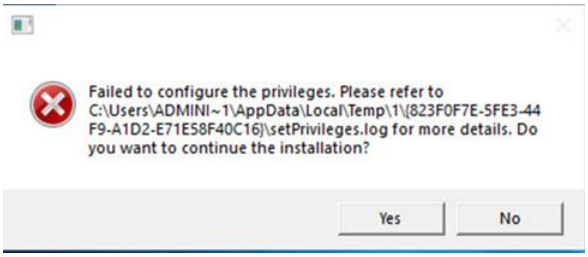
a) Select the **Conduct Certificate Authority verification** check box.

b) Click **Browse** to import the CA certificate file, for example, **ca.pem**.

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

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

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



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

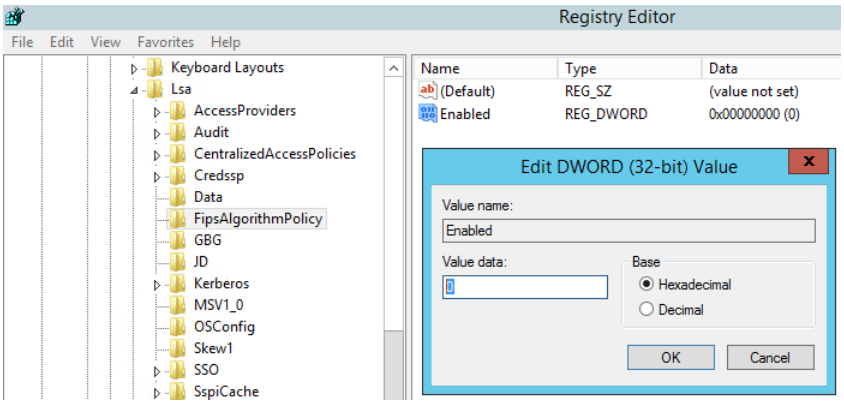
> **Note**: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.
>
> **Note**: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

4. After 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.

3.7. Installing Web/Web API Server on Windows

> **Note:** Service Monitor Agent needs to be installed prior to installing Web/Web API Server. Refer to Installing Service Monitor Agent on Windows for more detailed steps.

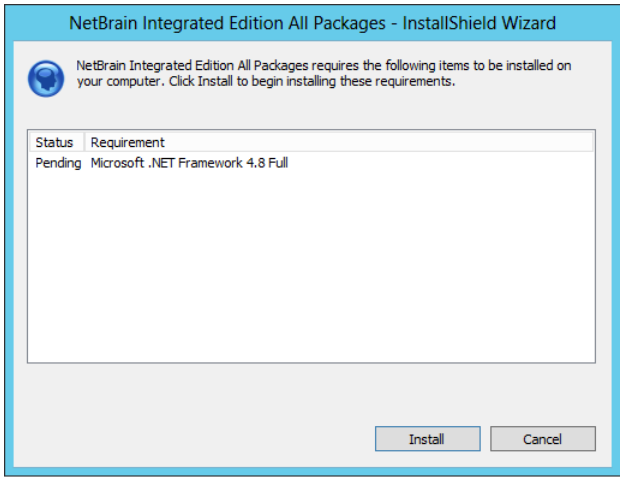
> **Note:** Web/Web API Servers are integrated into one installation package with Worker Server. It is highly recommended to install Worker Server on a standalone machine after the installation of Web/Web API Server. See Installing Worker Server on Windows for more details.
>
> **Note:** It is highly recommended that the extended memory of your machine is larger than 16GB.
>
> **Note:** Before the installation, the Existing Internet Information Services (IIS) must be removed, and the FIPS setting must be disabled by modifying the **Enabled** value to **0** under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy** directory of Windows registry.
>
> 
>

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

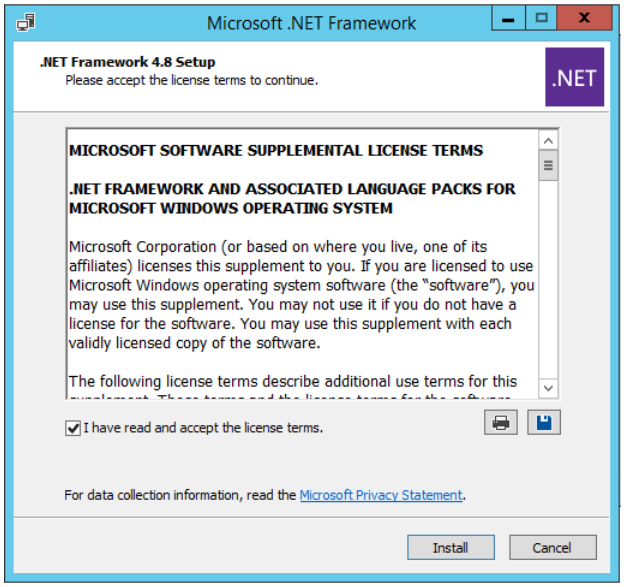
1. Download the **netbrain-ie-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to start the Installation Wizard.
4. Follow the Installation Wizard to complete the installation step by step:
   1) .NET Framework 4.8 must be pre-installed on this machine before you install the Application Server. The Installation Wizard will automatically check this dependency. If it has not been installed, the wizard will guide you through the installation as follows; it has been installed, the wizard will directly go to step 2).

      > **Note:** Make sure the Windows update is of the latest. For Windows Server 2012, you might be asked to install some software patches before the .NET Framework 4.8 installation can start.

a) Click **Install**.

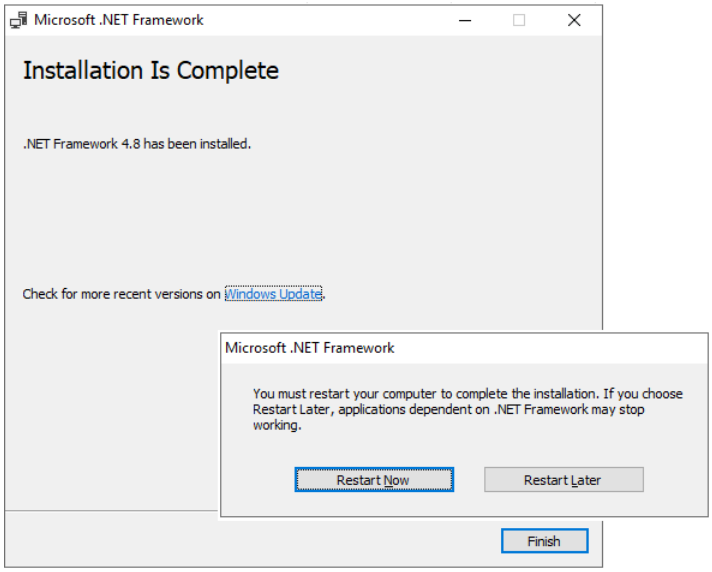


b) Read the license agreement of Microsoft .NET Framework 4.8, select the **I agree to the license terms and conditions** check box and click **Install**. It might take a few minutes for the installation to be completed.



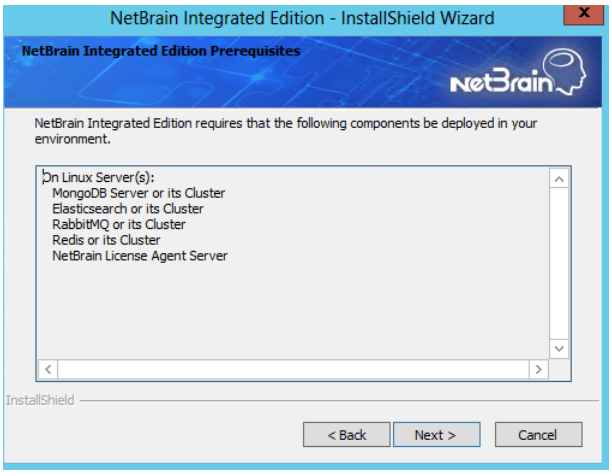
> **Note:** Some running applications must be closed during the installation of .NET Framework 4.8, such as Server Manager.

c) You must click **Restart Now** to restart the machine immediately. Otherwise, the upgrade will fail due to the failure of upgrading the new .Net Framework. After the machine reboots, continue with step 2).



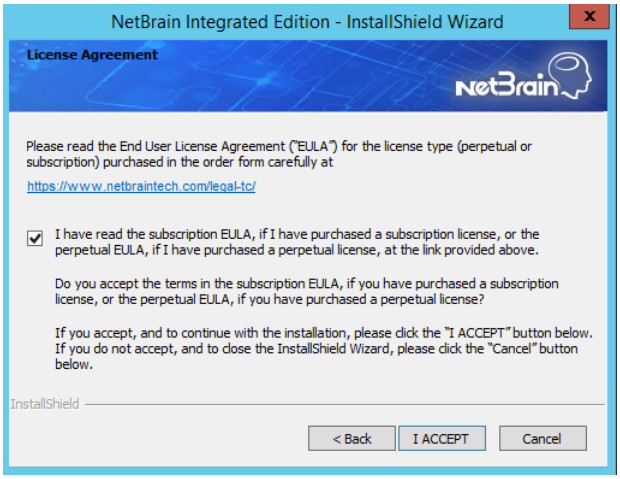
> **Note:** The interface above may not appear if the .NET Framework has never been installed on the server. In such case, it is still highly recommended to reboot the server after the installation of the .NET Framework completes.
>
> **Note:** Ensure the FIPS is disabled after restarting the machine. To disable the FIPS setting, modify the **Enabled** value to **0** under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy** directory of Windows registry

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



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

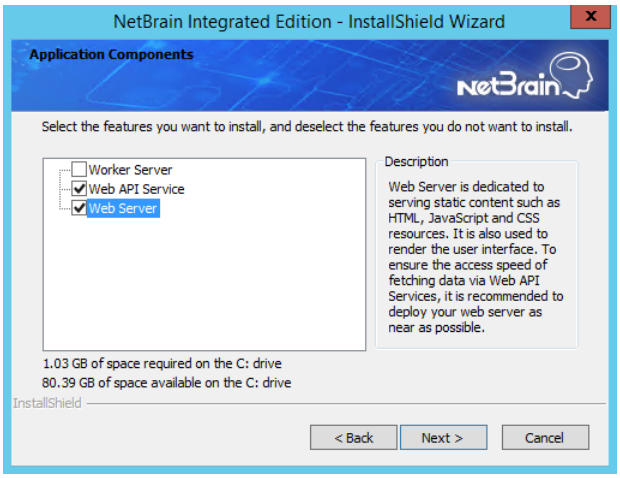
5) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA...** check box and then click **I ACCEPT**.



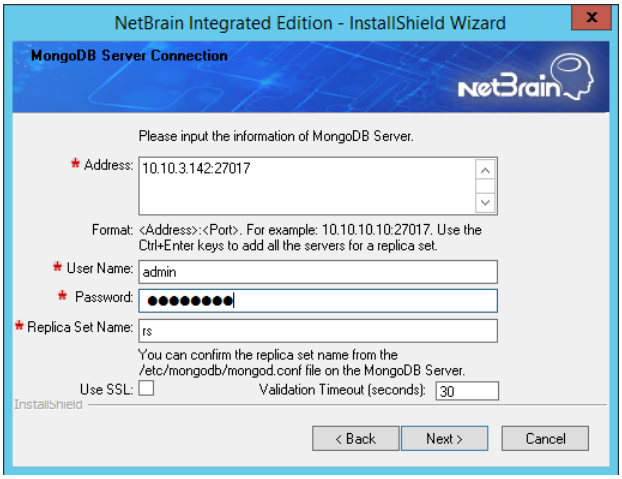
6) On the Customer Information page, enter your company name, and then click **Next**.

7) On the Destination Location page, click **Next** to install the Web Server and Web API Server under the default directory **C:\Program Files\NetBrain**. If you want to install them under another location, click **Change**.

8) Select both the **Web API Service** and **Web Server** check boxes, and then click **Next.**



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

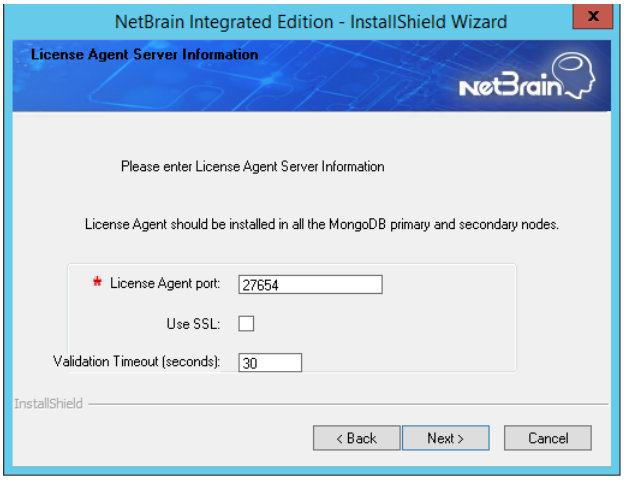


- **Address** — enter the IP address or resolvable FQDN of MongoDB and the corresponding port number. By default, the port number is **27017**.

  > **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`.

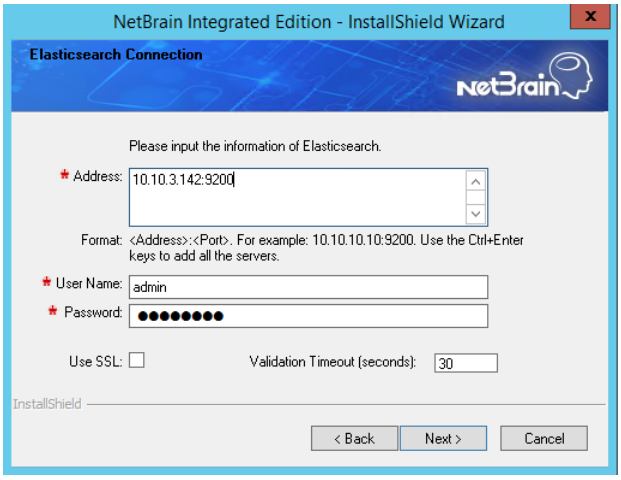
- **User Name** — enter the username that you created when installing MongoDB.
- **Password** — enter the password that you created when installing MongoDB.
- **Replica Set Name** — enter the replica set name of MongoDB. Keep the default value **rs** as it is unless you changed it.
- **Use SSL** — used to encrypt the connections to MongoDB with SSL. If SSL is enabled on MongoDB, select this check box; otherwise, leave it unchecked.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

10) On the License Agent Server Information page, enter the following information to connect to License Agent, and then click **Next**.



- **License Agent port** — the port number that the service of License Agent Server listens to. By default, it is **27654**.
- **Use SSL** — used to encrypt the connections to License Agent Server with SSL. If SSL is enabled on License Agent Server, select it; otherwise, leave it unchecked.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

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



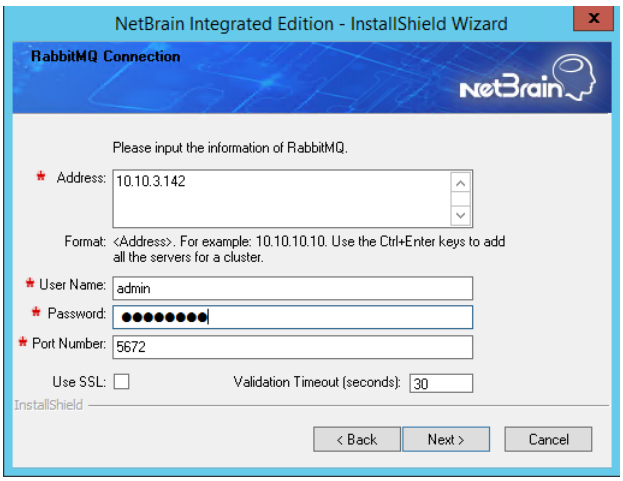
- **Address** — enter the IP address or resolvable FQDN of Elasticsearch and the corresponding port number. For example, `10.10.3.142:9200`.

> **Note:** If a proxy server is configured on this machine to access the Internet, you must add the IP address and port number of Elasticsearch into the proxy exception list of the web browser, to ensure this NetBrain server can communicate with Elasticsearch.

> **Tip:** You can enter the FQDN of Elasticsearch if all NetBrain servers are managed in the same domain. For example, **`test.netbraintech.com:9200`**.

- **User Name** — enter the username that you created when installing Elasticsearch.
- **Password** — enter the password that you created when installing Elasticsearch.
- **Use SSL** — used to encrypt the connections to Elasticsearch with SSL. If SSL is enabled on Elasticsearch, select it; otherwise, leave it unchecked.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

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

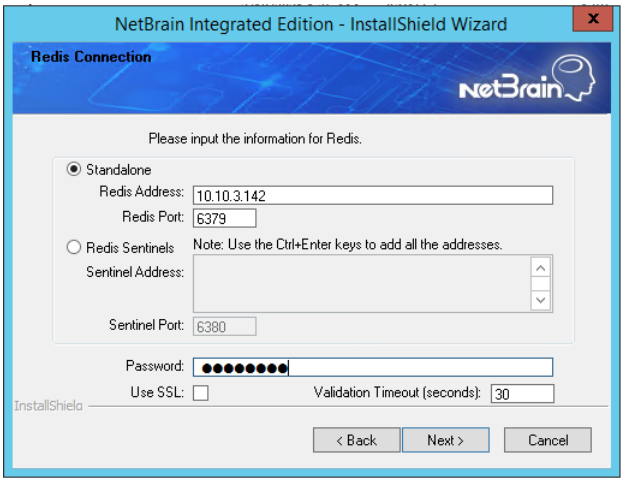


- **Address** — enter the IP address or resolvable FQDN of RabbitMQ.

> **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.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

13) On the Redis Connection page. enter the following information to connect to Redis by selecting the **Standalone** mode, and then click **Next**.

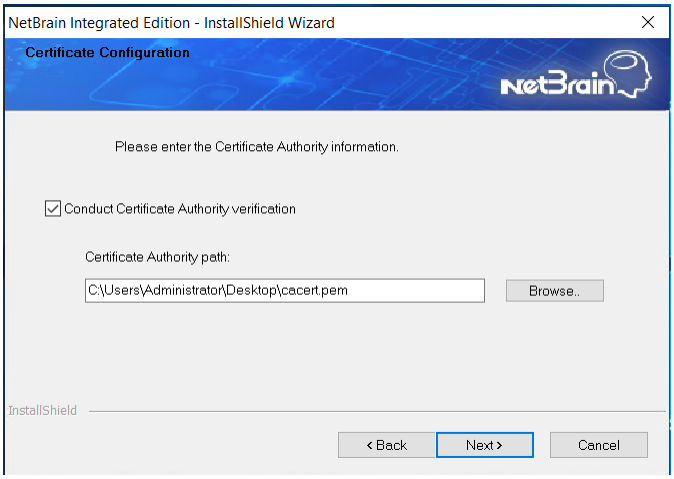


- **Redis Address** — enter the IP address of Redis.

  > **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**.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

14) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, License Agent, Elasticsearch, RabbitMQ, or Redis.) Configure whether to authenticate the Certificate Authority (CA) of the SSL certificates used on these servers, and then click **Next**.



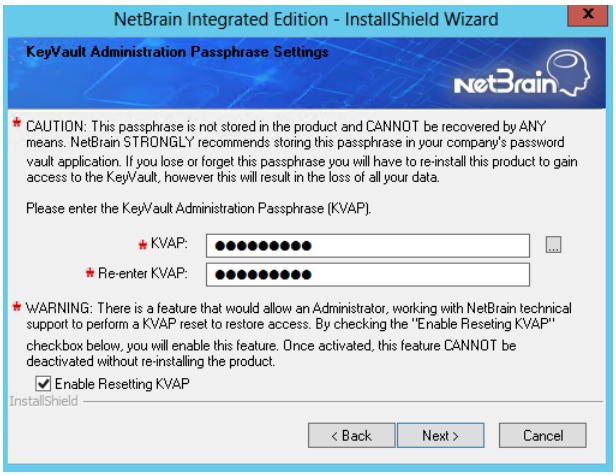
To authenticate CA:

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

b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem.**

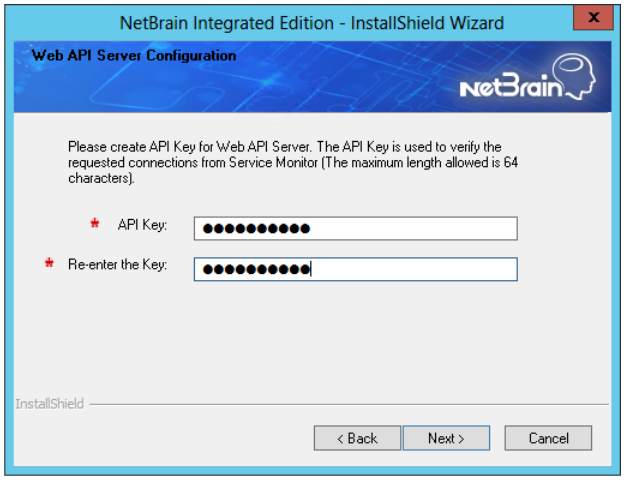
> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met for the CA certificate file:
> - The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
> - The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
> - Internet access must be ensured if the certificate is signed by third-party CA.

15) 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 select the **Enable Resetting KVAP** check box to enable the KVAP resetting. Click **Next**.



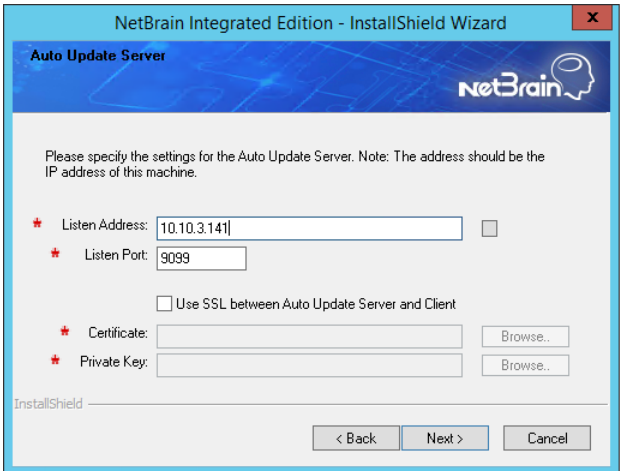
> **Tip:** The passphrase must contain at least one uppercase letter, one lowercase letter, one number, and one special character, and the minimum permissible length is 8 characters. All special characters except for the quotation mark (") are allowed.
>
> **Note:** Keep notes of the passphrase because it is required when you scale up or upgrade the Application Server. In case of losing the passphrase, keep the **Enable Resetting KVAP** check box selected so that NetBrain system admin can reset the passphrase at any time.

16) On the Web API Server Configuration page, create an API key for Web API Server to verify the connection request from Service Monitor Agent. Type it twice and click **Next.**



> **Note**: This API Key must be consistent with the one entered during installing Service Monitor Agent before.

17) On the Auto Update Server page, configure the listen address and listen port.

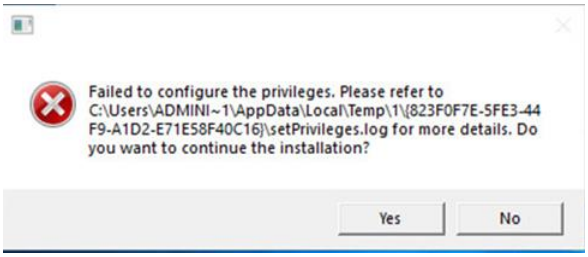


- **Use SSL between Auto Update Server and Client** — used to encrypt the connections between Auto Update Server and Client with SSL. Otherwise, leave it unchecked.
  - **Certicate** — required only if **Use SSL...** is selected. Click **Browse** to select the certificate file containing the public key. For example, **cert.pem**.
  - **Private Key** — required only if **Use SSL...** is selected. Click **Browse** to select the private key file. For example, **key.pem**.

> **Note**: The Listen Address must be the local server's IP address which can be reached from other NetBrain servers including Front Server.

18) Review the summary of the installation settings and click **Install**.

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



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

> **Note**: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.
>
> **Note**: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

5. After successfully installing the Web Server and Web API Server, click **Finish** to complete the installation process and exit the Installation Wizard.
6. Open the IIS Manager to check that the **Default Web Site** and **ServicesAPI** under the **Sites** 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** file from the **C:\NBIEInstall** of this machine directly to the **C:\NBIEInstall** drive of the machines where Worker Server, Task Engine, and Front Server Controller will be installed.

3.8. Installing Worker Server on Windows

Depending on your network scale, you can deploy either a standalone Worker Server or multiple for load balancing.

> **Note:** Service Monitor Agent needs to be installed prior to installing Worker Server. Refer to Installing Service Monitor Agent on Windows for more detailed steps.
>
> **Note:** Worker Server is integrated into one installation package with Web/Web API Servers. It is highly recommended to install Worker Server on a standalone machine after the installation of Web/Web API Server.

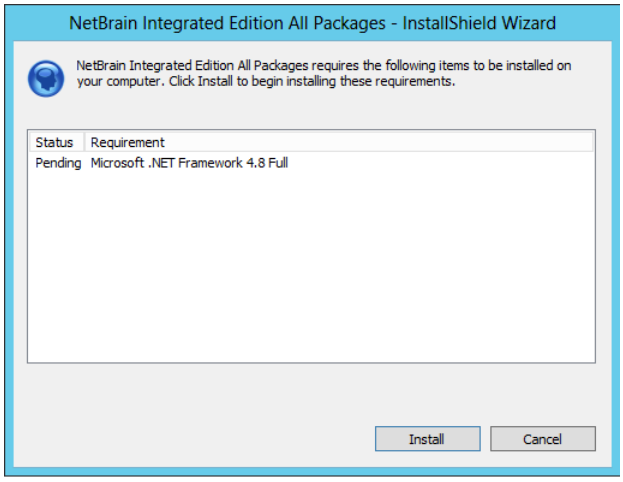
> **Note:** Don't install multiple Worker Servers at the same time and don't install Worker Server and Web API Server at the same time, either; install them one after another on separate machines. Otherwise, it will cause the database initialization failure.
>
> **Note:** It is highly recommended that the extended memory of your machine is larger than 16GB.

Complete the following steps with administrative privileges.

1. Download the **netbrain-ie-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-ie-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-ie-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to launch the Installation Wizard.
4. Follow the Installation Wizard to complete the installation step by step:
   1) .NET Framework 4.8 must be pre-installed on this machine before you install the Application Server. The Installation Wizard will automatically check this dependency. If it has not been installed, the wizard will guide you through the installation as follows; it has been installed, the wizard will directly go to step 2).

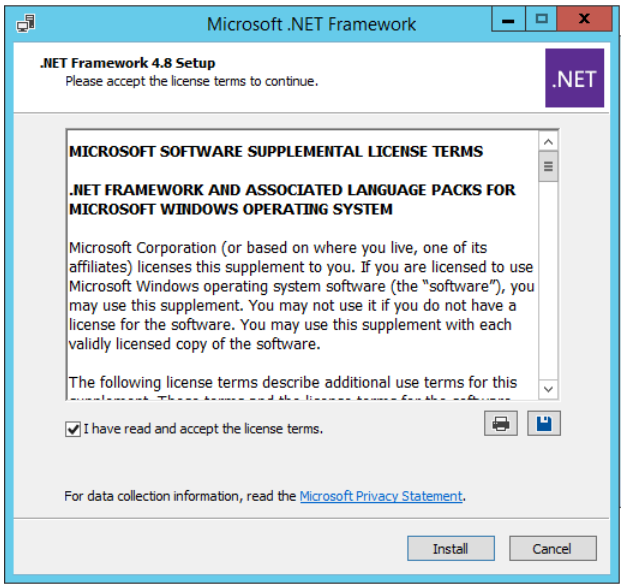
      > **Note:** Make sure the Windows update is of the latest. For Windows Server 2012, you might be asked to install some software patches before the .NET Framework 4.8 installation can start.

      a) Click **Install**.

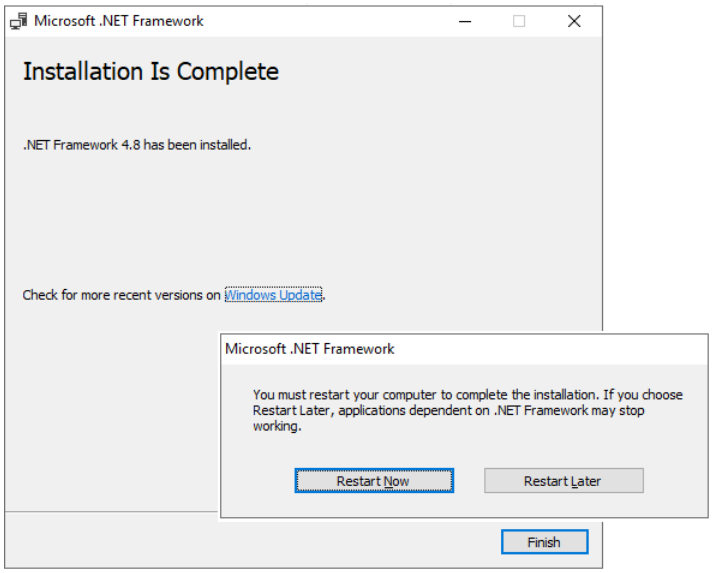
      b) Read the license agreement of Microsoft .NET Framework 4.8, select the **I agree to the license terms and conditions** check box and click **Install**. It might take a few minutes for the installation to be

completed.



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

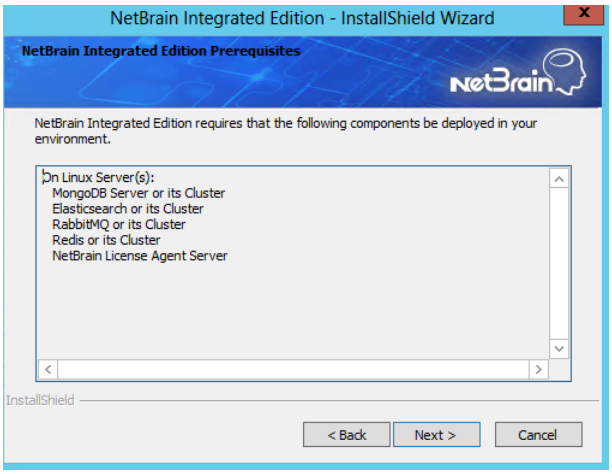
c) You must click **Restart Now** to restart the machine immediately. Otherwise, the upgrade will fail due to the failure of upgrading the new .Net Framework. After the machine reboots, continue with step 2).



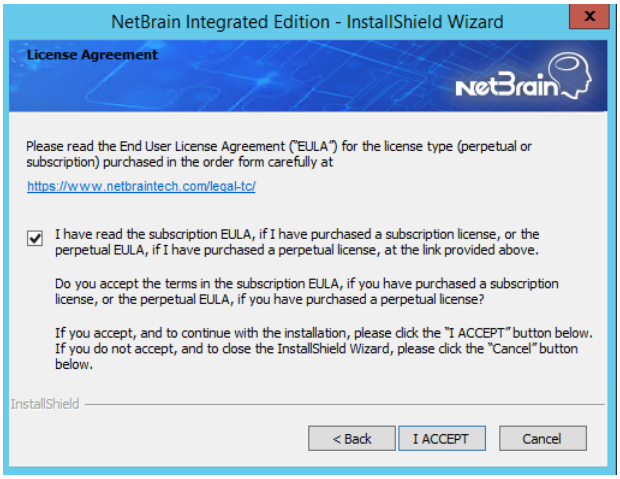
> **Note:** The interface above may not appear if the .NET Framework has never been installed on the server. In such case, it is still highly recommended to reboot the server after the installation of the .NET Framework completes.

> **Note:** Ensure the FIPS is disabled after restarting the machine. To disable the FIPS setting, modify the **Enabled** value to **0** under the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy** directory of Windows registry

2) On the Welcome page, click **Next**.
3) On the NetBrain Integrated Edition Prerequisites page, view the Linux components that must be deployed beforehand in your environment and click **Next**.

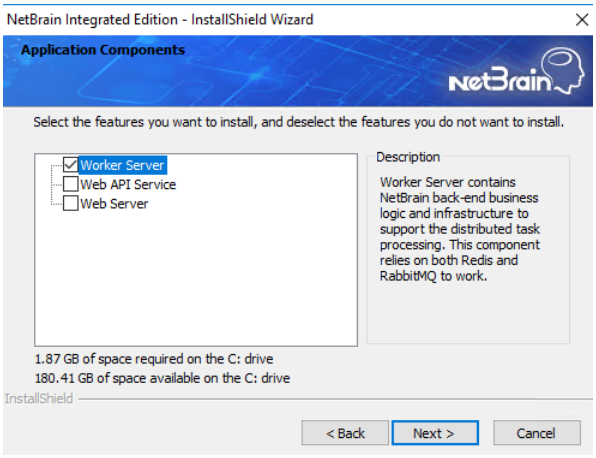


4) On the System Configuration page, review the system configuration summary and click **Next**.
5) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA...** check box and then click **I ACCEPT**.

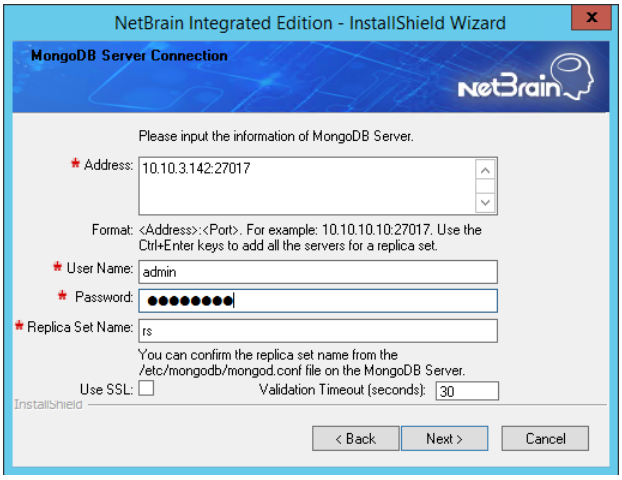


6) On the Customer Information page, enter your company name, and then click **Next**.
7) Click **Next** to install the Worker Server under the default directory **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.

8) Select the **Worker Server** check box, and then click **Next**.



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

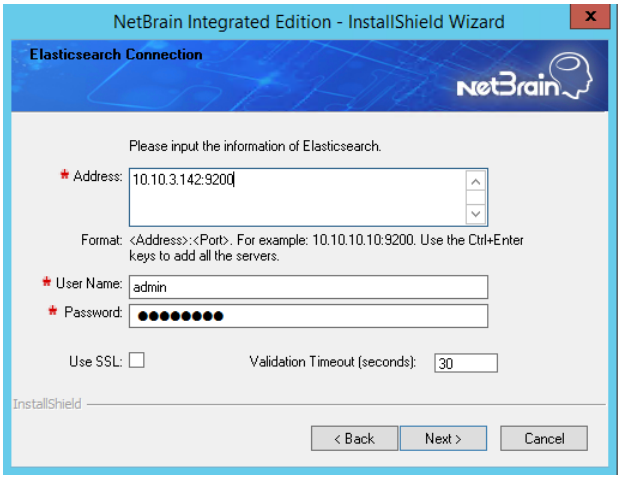


- **Address** — enter the IP address or resolvable FQDN of MongoDB and the corresponding port number. By default, the port number is **27017**.

  > **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. Keep the default value **rs** as it is unless you changed it.
- **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.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

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

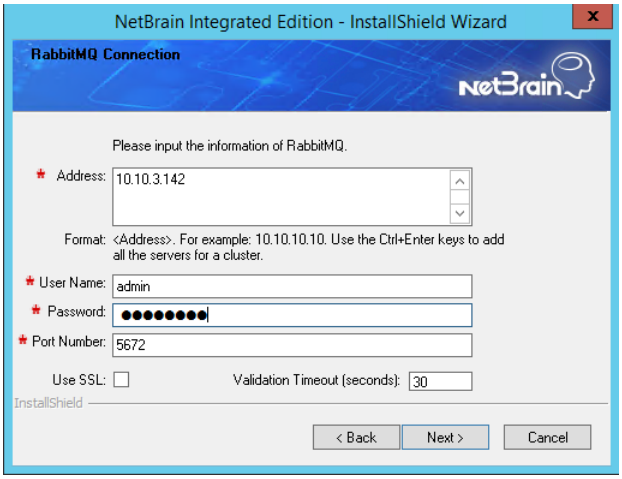


- **Address** — enter the IP address or resolvable FQDN of Elasticsearch and the corresponding port number. For example, `10.10.3.142:9200`.

  > **Note:** If a proxy server is configured on this machine to access the Internet, you must add the IP address and port number of Elasticsearch into the proxy exception list of the web browser, to ensure this NetBrain server can communicate with Elasticsearch.
  >
  > **Tip:** You can enter the FQDN of Elasticsearch if all NetBrain servers are managed in the same domain. For example, `test.netbraintech.com:9200`.

- **User Name** — enter the username that you created when installing Elasticsearch.
- **Password** — enter the password that you created when installing Elasticsearch.
- **Use SSL** — used to encrypt the connections to Elasticsearch with SSL. If SSL is enabled on Elasticsearch, select it; otherwise, leave it unchecked.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

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

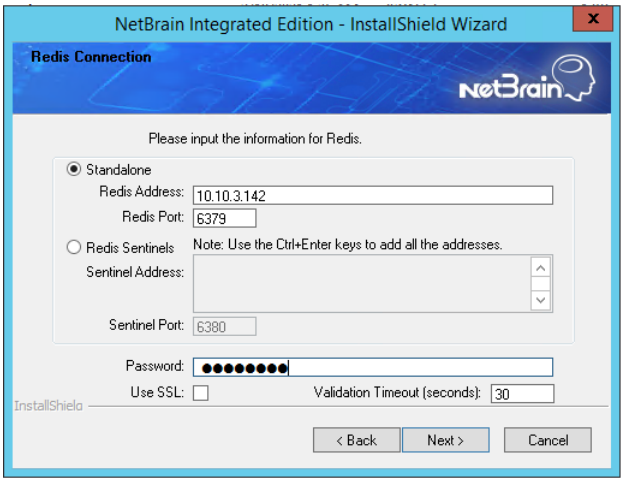


- **Address** — enter the IP address or resolvable FQDN of RabbitMQ.

  > **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.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

12) On the Redis Connection page, enter the following information to connect to Redis by selecting the **Standalone** mode, and then click **Next**.

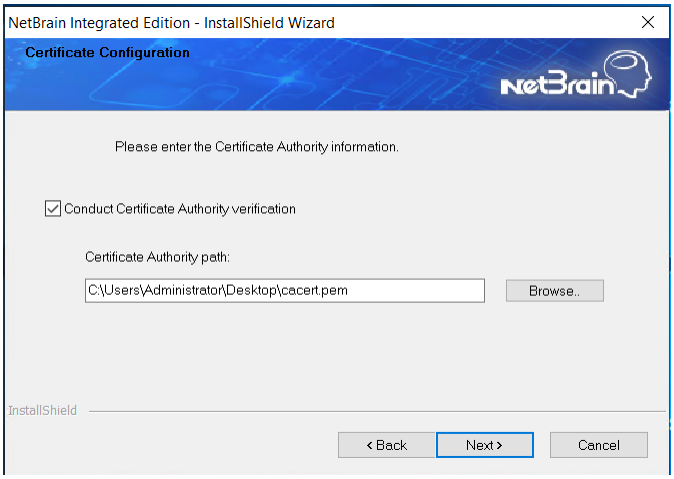


- **Redis Address** — enter the IP address of Redis.

  > **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**.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

13) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, License Agent, Elasticsearch, RabbitMQ, or Redis.) Configure whether to authenticate Certificate Authority (CA) of the SSL certificates used on these servers, and then click **Next**.



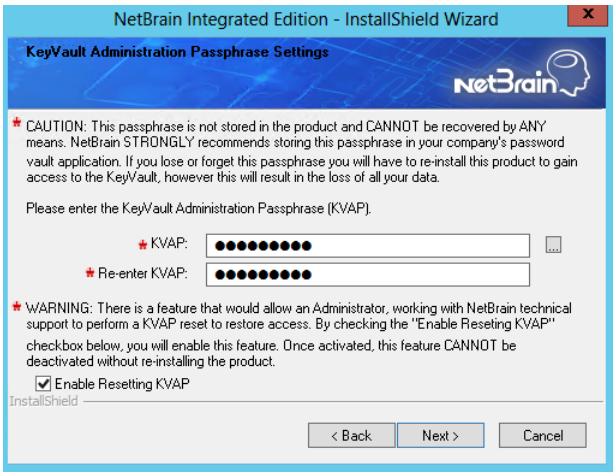
To authenticate CA:

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

b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem.**

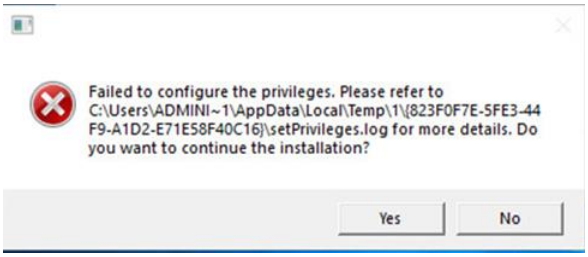
> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met for the CA certificate file:
> - The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
> - The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
> - Internet access must be ensured if the certificate is signed by third-party CA.

14) On the KeyVault Administration Passphrase Settings page, enter the passphrase that you created when installing Web API Server twice and select the **Enable Resetting KVAP** check box to enable the KVAP resetting. Click **Next**.



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

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



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

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

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

5. After successfully installing the Worker Server on your machine, click **Finish** to complete the installation process and exit the Installation Wizard.
6. Open the Task Manager and navigate to the Services panel to check that the **NetBrainWorkerServer** service is running.
7. If you have a large number of network tasks to be executed, you can deploy a Worker Server Cluster for load balancing by repeating the above installation steps 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.

3.9. Installing Task Engine on Windows

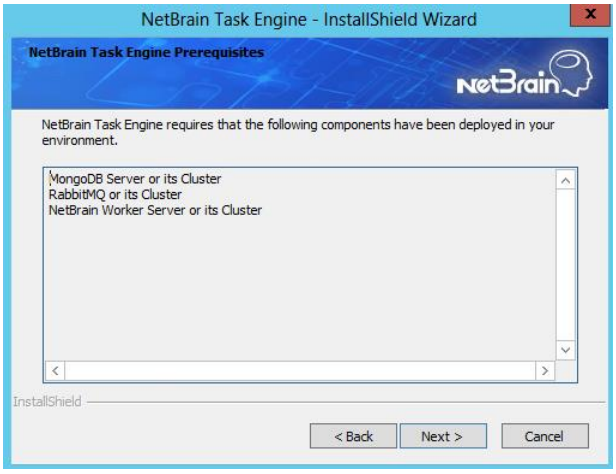
> **Note:** Service Monitor Agent needs to be installed prior to installing Task Engine. Refer to Installing Service Monitor Agent on Windows for more detailed steps.

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.

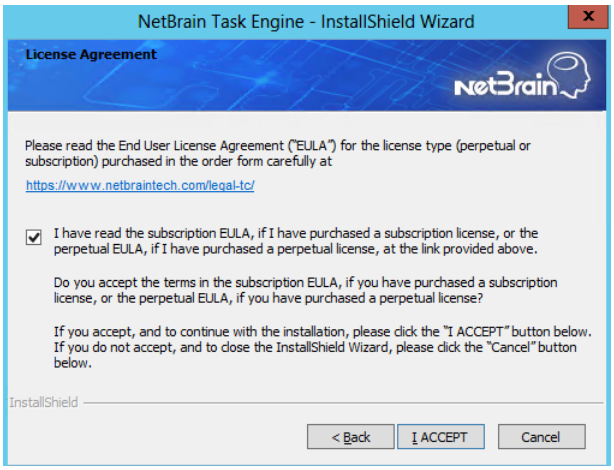
1. Download the **netbrain-taskengine-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-taskengine-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-taskengine-windows-x86_64-10.0.exe** file, and then select **Run as administrator**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



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

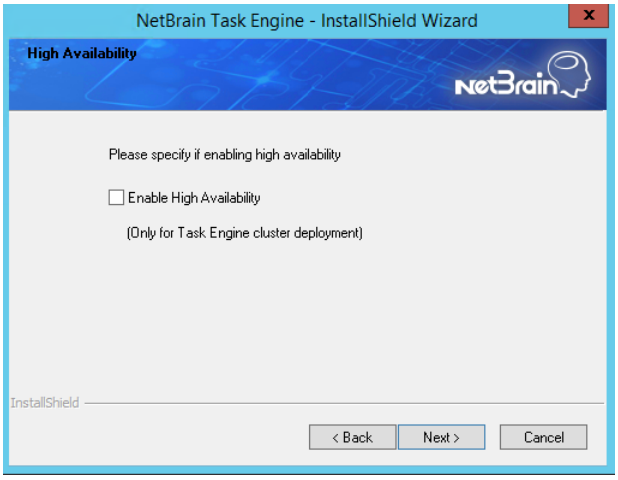
4) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA...** check box and then click **I ACCEPT**.



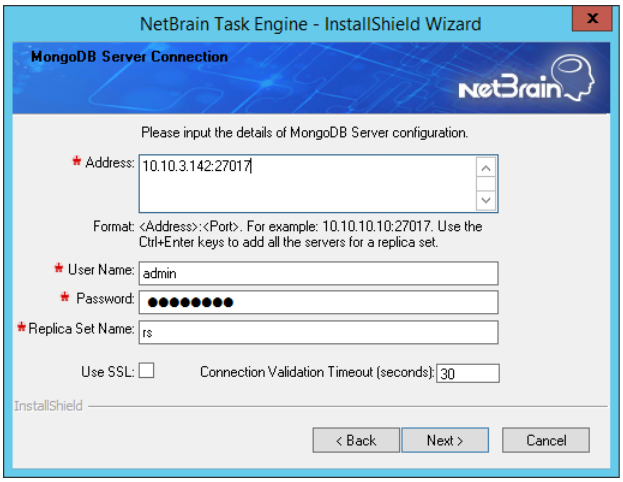
5) On the Customer Information page, enter your company name, and then click **Next**.

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 **Enable High Availability** unchecked.



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



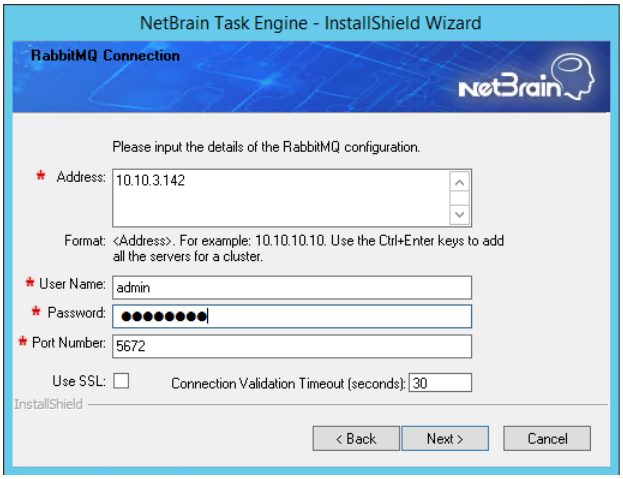
- **Address** — enter the IP address or resolvable FQDN of MongoDB and the corresponding port number. By default, the port number is **27017**.

  > **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. Keep the default value **rs** as it is unless you changed it.
- **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.

- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

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



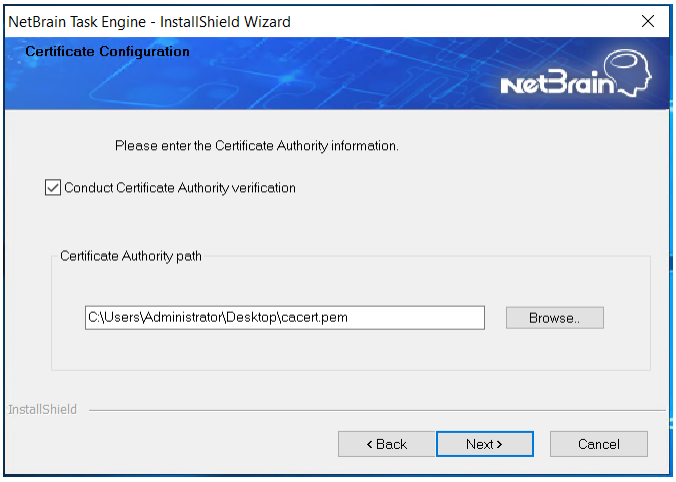
- **Address** — enter the IP address or resolvable FQDN of RabbitMQ.

  > **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.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

10) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB or RabbitMQ.) On the Certificate Configuration page, configure whether to authenticate the CA of SSL

certificates used on MongoDB or RabbitMQ, and then click **Next**.



To authenticate CA:

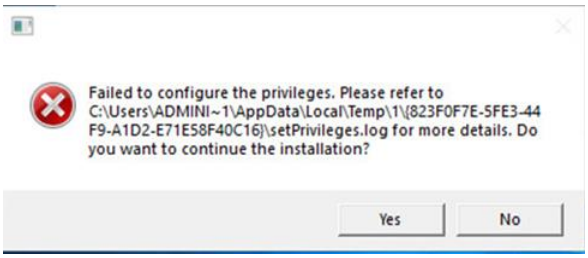
a) Select the **Conduct Certificate Authority verification** check box.

b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem.**

> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met for the CA certificate file:
> - The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
> - The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
> - Internet access must be ensured if the certificate is signed by third-party CA.

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

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



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

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

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

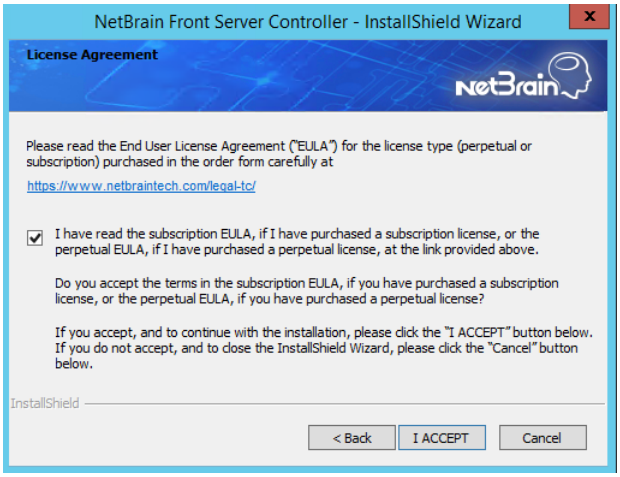
4. After successfully installing the Task Engine, click **Finish** to complete the installation process and exit the Installation Wizard.
5. Open the Task Manager and navigate to the **Services** panel to check that the **NetBrainTaskEngine** service is running.

3.10. Installing Front Server Controller on Windows

> **Note:** Service Monitor Agent needs to be installed prior to installing Front Server Controller. Refer to Installing Service Monitor Agent on Windows for more detailed steps.

Complete the following steps with administrative privileges.

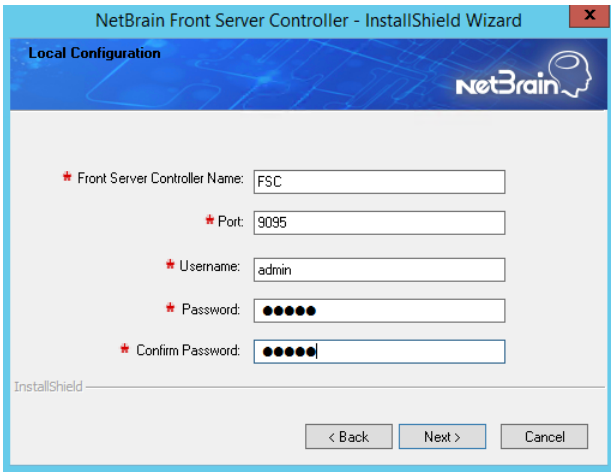
1. Download the **netbrain-frontservercontroller-windows-x86_64-10.0.zip** file and save it in your local folder.
2. Extract installation files from the **netbrain-frontservercontroller-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-frontservercontroller-windows-x86_64-10.0.exe** file,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



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

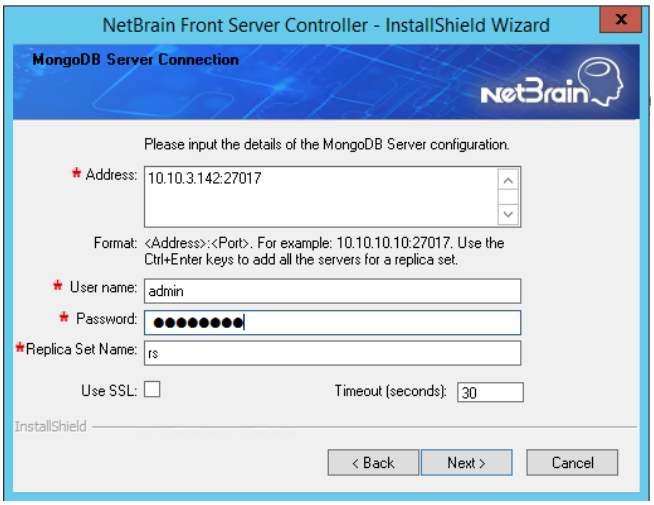
  > **Note:** This field cannot contain any of the special characters: `\ / : * ? " < > | . $`
  >
  > **Note:** Keep notes of **Front Server Controller Name** as well as **Port**, **Username**, and **Password** because they are required when you allocate tenants to Front Server Controller and register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

7) On the Local SSL Configuration page, configure whether to enable SSL on Front Server Controller, and then click **Next**.

- **Enable SSL** — used to encrypt the connections established from Worker Server and Front Server with SSL. For detailed requirements of SSL certificates and keys, refer to SSL Certificate Requirements.
  - **Certificate** — required only if **Enable SSL** is selected. Click **Browse** to select the certificate file containing the public key. For example, **cert.pem**.
  - **Private Key** — required only if **Enable SSL** is selected. Click **Browse** to select the private key file. For example, **key.pem**.

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

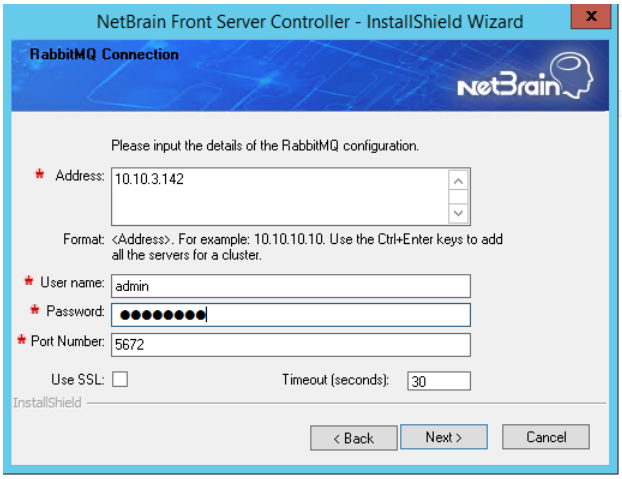


- **Address** — enter the IP address or resolvable FQDN of MongoDB and the corresponding port number. By default, the port number is **27017**.

  > **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. Keep the default value **rs** as it is unless you changed it.
- **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.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

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

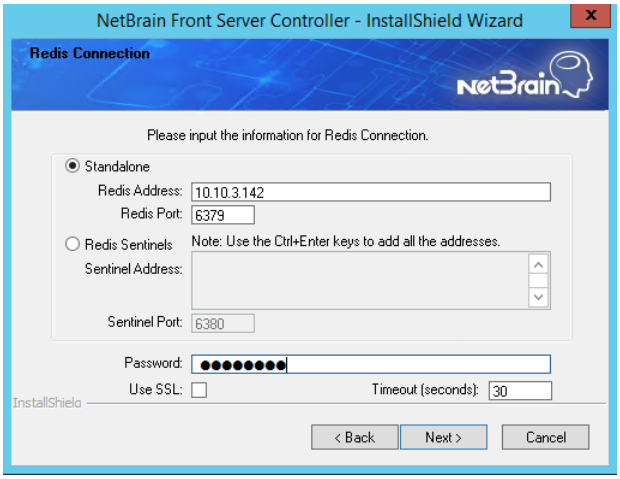


- **Address** — enter the IP address or resolvable FQDN of RabbitMQ.

  > **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.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

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

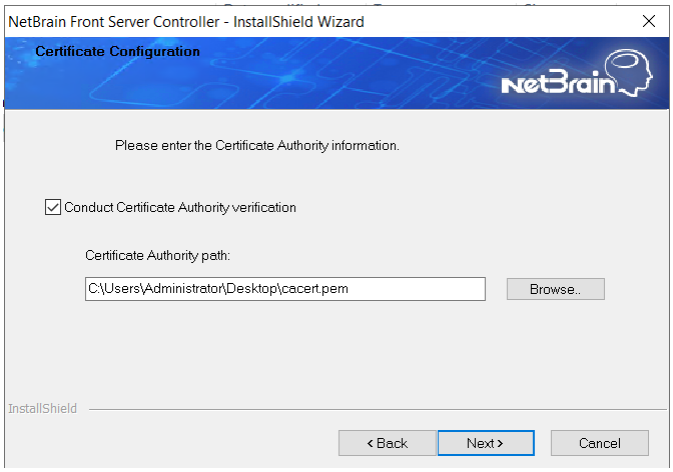


- **Redis Address** — enter the IP address of Redis.

  > **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**.
- **Validation Timeout (seconds)** — it is used to set the connection timeout threshold (in second) to validate the connection to the dependent server. This will not affect the application running timeout value.

11) (Required only if the **Use SSL** check box is selected when configuring the connections to MongoDB, RabbitMQ, or Redis). Configure whether to authenticate the CA of SSL certificates on these servers, and then click **Next**.



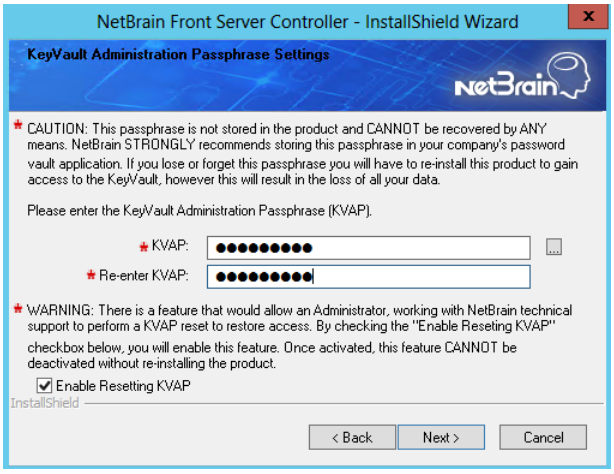
To authenticate CA:

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

b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem.**

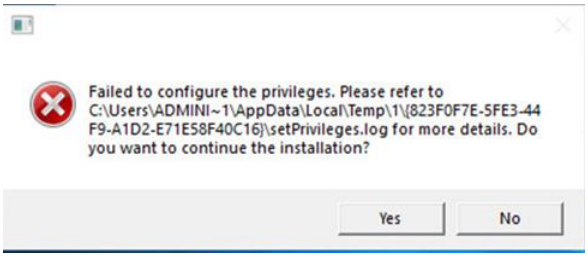
> **Note:** Only the certificate in **Base-64 encoded X.509 PEM** format is supported.
>
> **Note:** The following conditions must be met for the CA certificate file:
> - The CA certificate must contain CRL Distribution Points property with valid CRL HTTP distribution point URL. (CRL stands for Certificate Revocation List.)
> - The CRL Distribution Points URL must be accessible to Web Server/Worker Server.
> - Internet access must be ensured if the certificate is signed by third-party CA.

12) On the KeyVault Administration Passphrase Settings page, enter the passphrase that you created when installing Web API Server twice and select the **Enable Resetting KVAP** check box to enable the KVAP resetting. Click **Next**.



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

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



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

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

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

4. After successfully installing the Front Server Controller, click **Finish** to complete the installation process and exit the Installation Wizard.
5. Open the Task Manager and navigate to the **Services** panel to check that the **NetBrainFrontServerController** service is running.

3.11. 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 internal communications.

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

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

3.11.1. Installing Front Server on Linux

Pre-installation Tasks

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

- **Online Install:** run the `yum -y install zlib-devel readline-devel bzip2-devel ncurses-devel gdbm-devel xz-devel tk-devel libffi-devel gcc` command to install it online.
- **Offline Install:** refer to Offline Installing Third-party Dependencies for more details.

> **Note**: You can also install the Service Monitor Agent separately.

- 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 they have not been installed yet, you can choose either option below to install the dependencies:
  - **Online Install:** run the `yum install -y glibc libstdc++ libuuid pam` command to install these third-party packages online.
  - **Offline Install:** refer to Offline Installing Third-party Dependencies for more details.

Installing Front Server on Linux

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

     > **Note:** The download link is case-sensitive.
     >
     > **Tip:** Run the `yum -y install wget` command to install the **wget** command if it has not been installed on the server.

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

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

FrontServer/install.sh
...
```

6. Run the `cd FrontServer/config` command to navigate to the **config** directory.
7. Modify the value of DataPath (based on your enironment) in the **setup.conf** file located under the **config** directory and save the changes. For how to modify the configuration file, refer to Editing a File with VI Editor.

```
[root@localhost config]# vi setup.conf
#DataPath is used to store data and log files for Front server. This directory must be at least
a second
level directory and used exclusively for this purpose.
DataPath=/usr/lib/netbrain/frontserver
#The PostgreSQL port must be between 1025 and 32767.
Port=5432
#Password should not contain: {}[]:",'|<>@&^%\ or a space. This password is used by front server
to connect to PostgreSQL.
Password=Admin1.#
# To disable the Service Monitor Agent installation, set the 'DisableSM=1'
# The default value of 'DisableSM' is 0 which means Service Monitor Agent
# will be installed with FrontServer if it has not yet been installed.
DisableSM=0
```

8. Run the `cd ..` command to navigate to the **FrontServer** directory and 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: Starting to check Linux OS info...
INFO: Starting to check required CPU...
INFO: Starting to check minimum memory...
...
INFO: Creating application databases and update PostgreSQL user SUCCEEDED
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed Front Server.
```

> **Note:** The Front Server service will not be automatically started until the Front Server is added to a tenant and successfully registered. You cannot register a Front Server immediately until adding the Front Server to a Tenant.
>
> **Note:** Disk space check will be performed to ensure the requirement of minimum 180G free disk space is met.

> **Note:** If the Service Monitor Agent was not previously installed, you'll need to use the interactive command line to install it. See Installing MongoDB on Linux for more details.

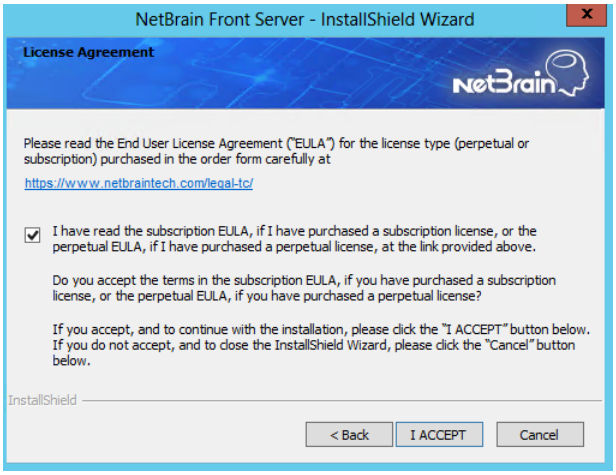
9. To install more Front Servers for load balancing, repeat the above installation steps on separate machines.

3.11.2. Installing Front Server on Windows

> **Note:** Service Monitor Agent needs to be installed prior to installing Front Server. Refer to Installing Service Monitor Agent on Windows for more detailed steps.

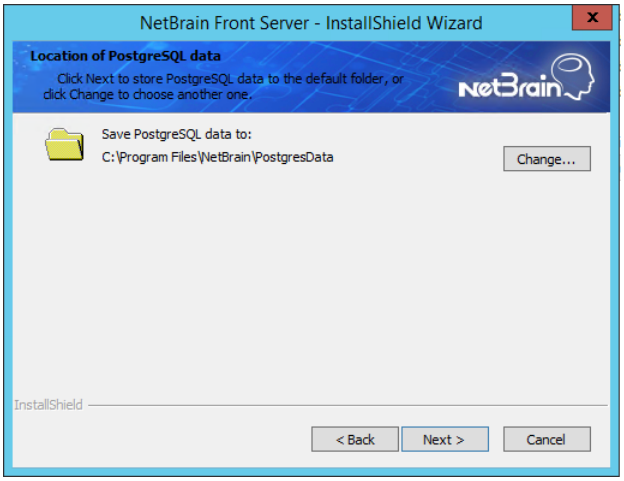
Complete the following steps with administrative privileges.

1. Download the **netbrain-frontserver-windows-x86_64-10.0.zip** file by using the download link provided in the email and save it in your local folder.
2. Extract installation files from the **netbrain-frontserver-windows-x86_64-10.0.zip** file.
3. Right-click the **netbrain-frontserver-windows-x86_64-10.0.exe** file, and then select **Run as administrator** to start the Installation Wizard.
   1) 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**.



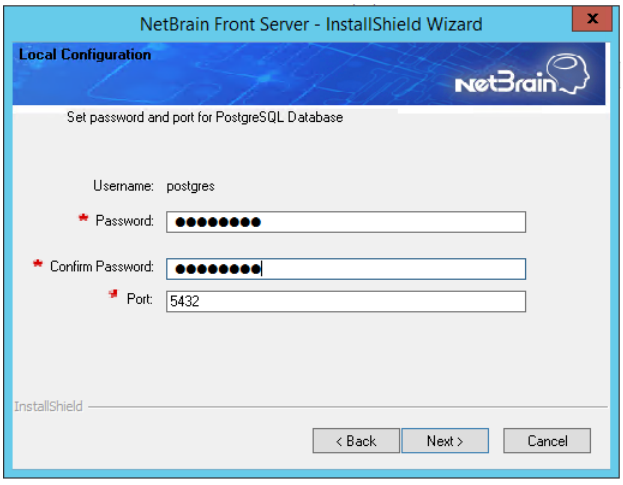
   4) On the Customer Information page, enter your company name, and then click **Next**.
   5) On the Destination Location page, click **Next** to install the Front Server under the default directory **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.

6) On the Location of PostgreSQL data page, click Next to store the PostgreSQL data to the default directory **C:\Program Files\NetBrain\PostgreData**. If you want to restore it under another location, click **Change**.



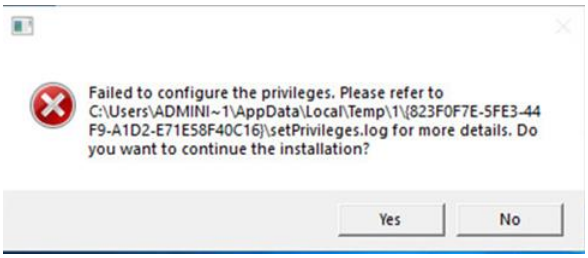
> **Note:** Make sure the designated data folder has more than 180GB free space.

7) On the Local Configuration page, set password and port for PostgreSQL database.



8) Review the summary of the current installation settings and click **Install**.

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



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

> **Note**: Local System accounts have additional privileges that are considered a high risk. Please verify that this is an acceptable risk in accordance with your SysAdmin policies.
>
> **Note**: After clicking **No**, please check with your system administration team to enable the relevant permissions, uninstall the affected component(s) and reinstall. Contact NetBrain support team if you need any assistance during the process.

4. After 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 the Front Server is added to a tenant and successfully registered. See Adding a Front Server to a Tenant and Registering the Front Server for more details.

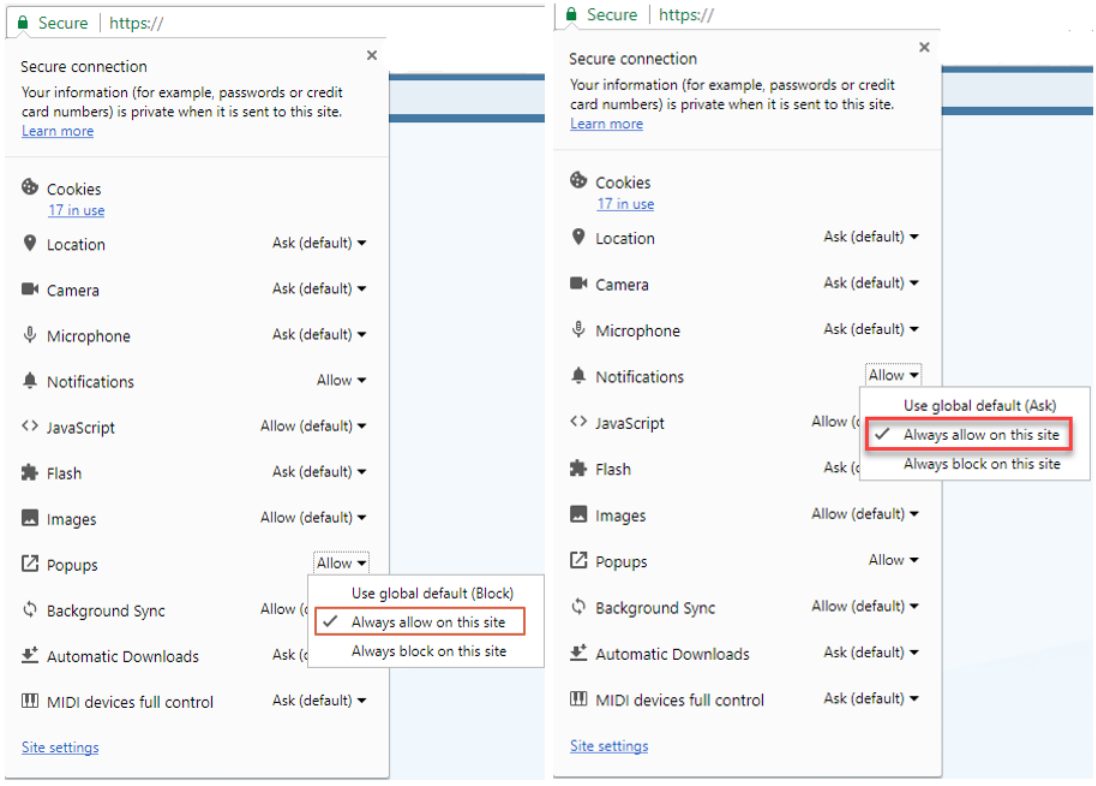
5. To install more Front Servers for load balancing, repeat the above installation steps on separate machines.

4. Setting Up Your System

Complete the following steps to set up your system:

1. Log in to System Management Page.
2. Activate Your License.
3. Create System Users Accounts.
4. Allocate the Tenant to a Front Server Controller.
5. Add a Front Server to the Tenant.
6. Register the Front Server.
7. Configuring Auto Upgrade Settings.
8. Monitor Server and Service Metrics.

> **Note:** The system is designed to work with a minimum screen resolution of 1440x900 pixels. Make sure the Notifications and Popups are allowed for the Web Server URL in your web browser and zoom it at 100% to get the best view.



4.1. Logging in to System Management Page

1. In your web browser, navigate to **http(s)://<Hostname or IP address of NetBrain Web Server>/admin.html**. For example, `https://10.10.3.141/admin.html` or `http://10.10.3.141/admin.html`.
2. In the login page, enter your username or email address, and password. The initial username/password is **admin/admin**.
3. Click **Log In**.
4. Modify your password first and then complete your user profile in the pop-up dialog, by entering the email address, first name, and last name, and then click **Save**.

4.2. Activating a Subscription License

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

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

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

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

        a) Follow the instructions to generate your license file. Attach the file to your email and send it to NetBrain Support Team. After receiving your email, the NetBrain team will fill in the license

information on NetBrain License Server and generate the corresponding activation file, and then send it back to you.

b) Click **Browse** to select the activation file that you received from the NetBrain team, and then click **Activate**.

4) A message box will prompt you the subscription license has been activated successfully. Click **OK**.

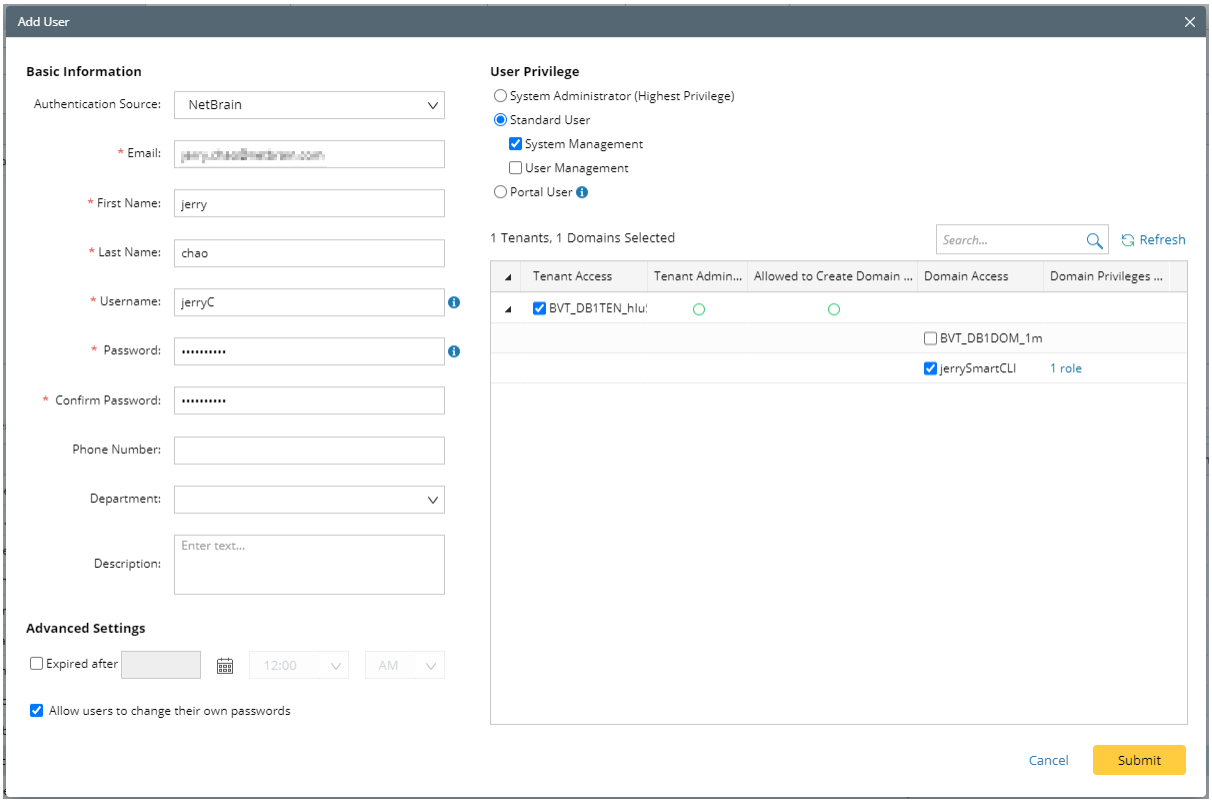
3. A confirmation dialog box prompts to ask you whether to generate an initial tenant. Click **Yes** and the initial tenant will be created automatically with all purchased nodes assigned.

4.3. Creating User Accounts

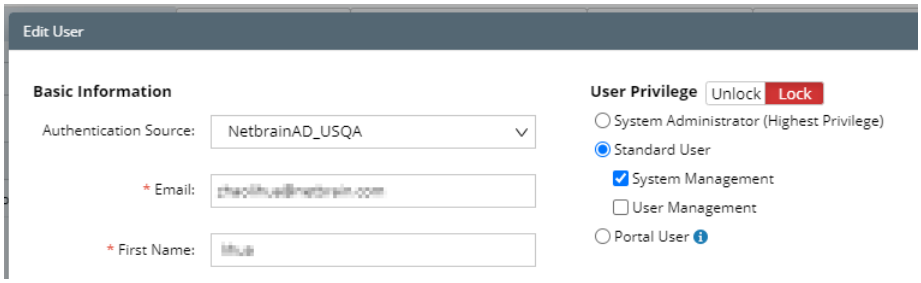
> **Tip:** To synchronize authenticated user accounts that are managed in third-party user management servers, refer to Third-Party User Authentication.

To manually create a user account, do the following:

1. In the System Management page, select the **User Accounts** tab.
2. Click **Add** at the upper-left corner, and complete the settings. This is an example:



1) Enter basic information. The fields marked with asterisks are mandatory.
2) Assign user rights, including access permissions and user roles. See online help for more details.

> **Note:** For authenticated users account from external servers (LDAP/AD/TACACS+), their roles and privileges can be locked as follows. After being locked, the roles and privileges will not be synced with any changed settings of external authentication.
>
> 
>

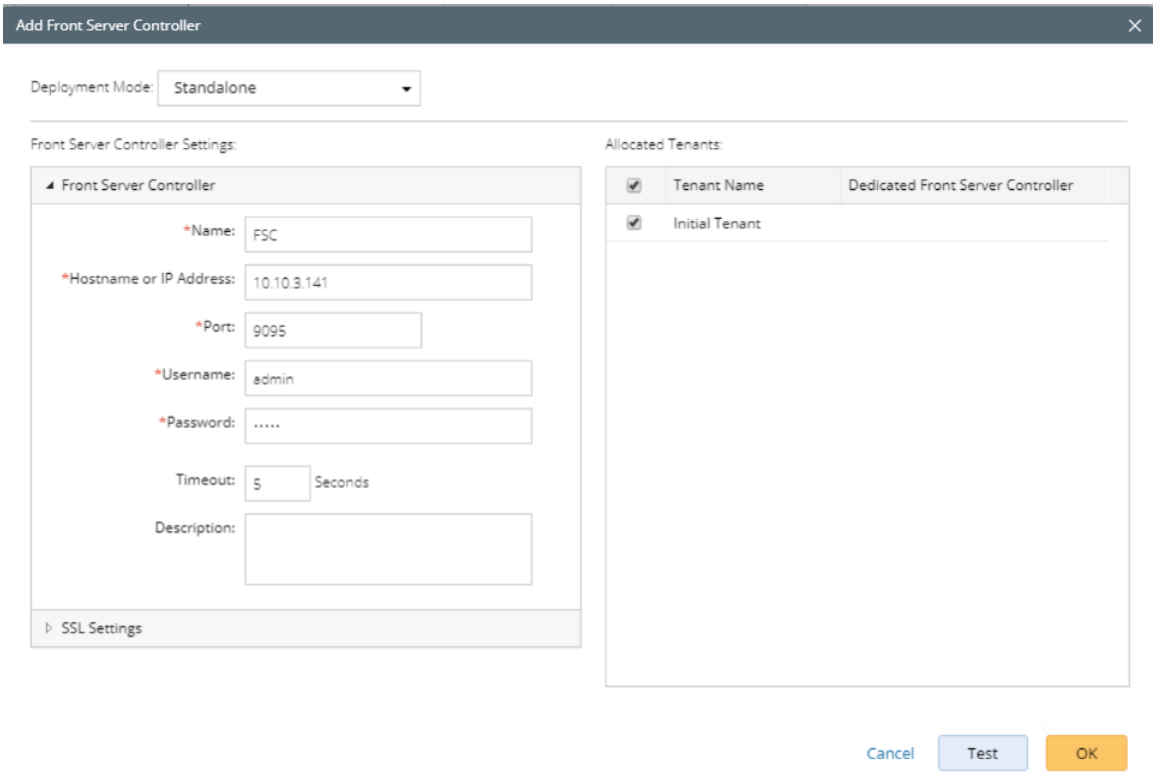
3) Configure the advanced settings if required, including account expiration and privilege to modify/reset password.

3. Click **Submit**. The user account will be added to the Existing User List.

4.4. 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.



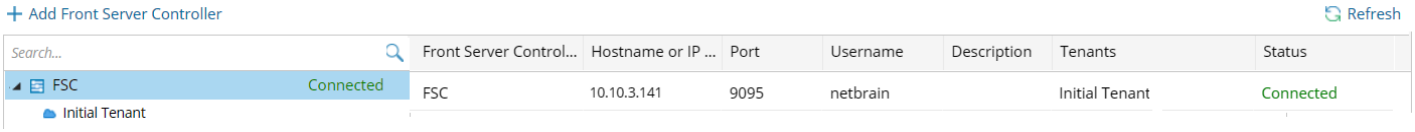
   - **Standalone** — applicable to a single Front Server Controller deployment.
   - **Group** — applicable to a failover deployment of Front Server Controller.

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**.

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

3) Click **Test** to verify whether the Web API 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.



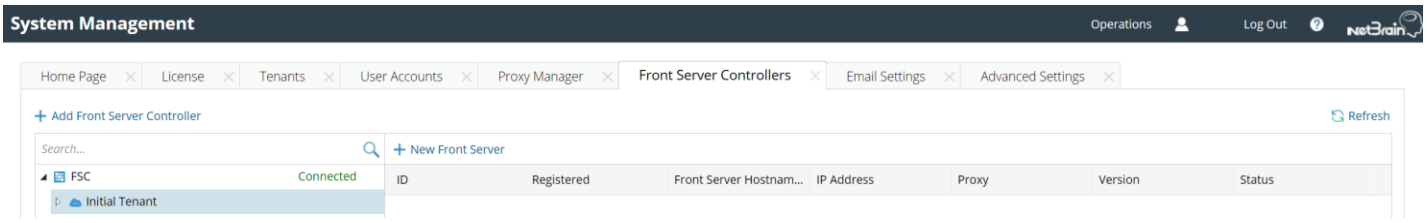
Front Server Controller Settings

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

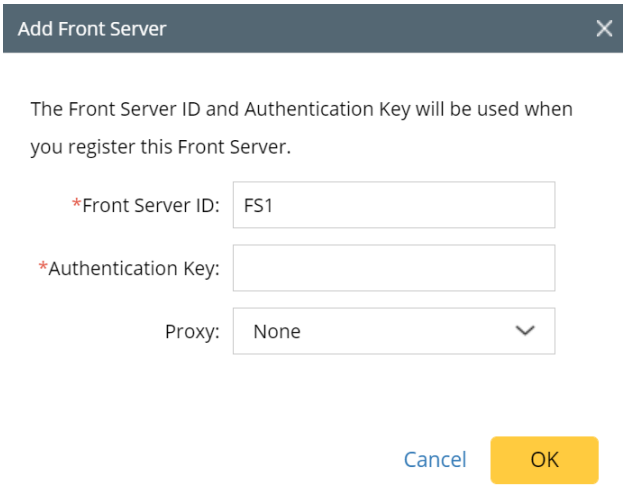
Field	Description
Name	The name of the Front Server Controller created when you install the Front Server Controller.
Hostname or IP Address	Enter the IP address of Front Server Controller.
Port	The port number created when you install the Front Server Controller for listening to the connections from 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.

4.5. Adding a Front Server for a Tenant

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



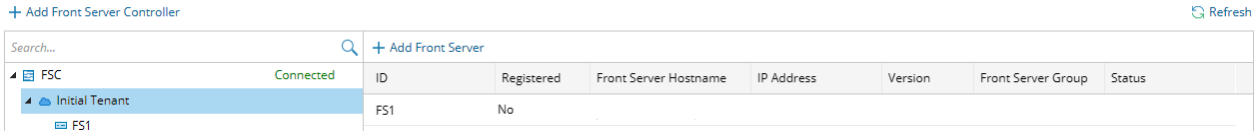
2. Enter the following properties of the Front Server.



- **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.

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



4.6. 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

> **Note**: If you deployed multiple Front Servers for load balancing, repeat the registration steps on separate machines.

Registering a Front Server on Windows

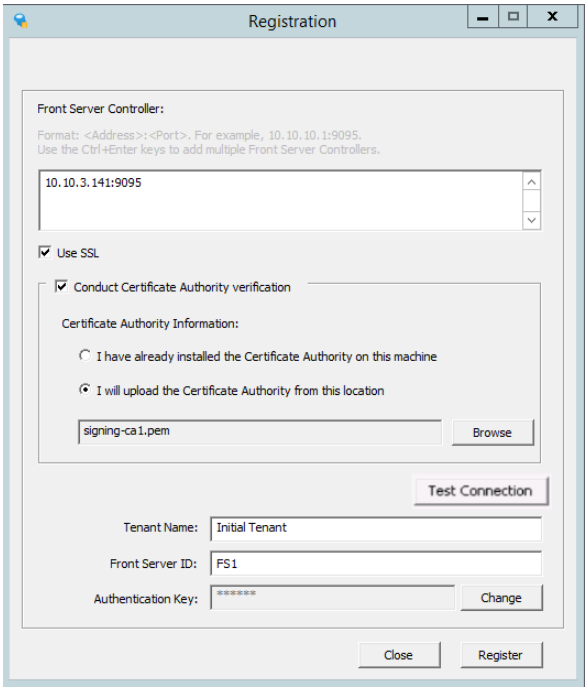
Example: Register a Front Server on Windows Server 2012 R2.

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.



   1) Enter the following information about the Front Server Controller.
      - **Hostname or IP address with port** — the IP address or FQDN 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 Controller, 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.

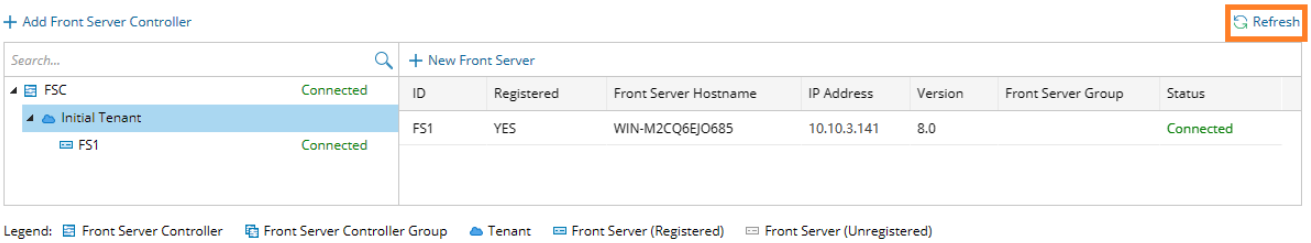
3) Click **Test Connection** to verify whether this Front Server can establish a connection with Front Server Controller.

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**.



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 default **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, refer to Editing a File with VI Editor.

```
[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. "no" indicates disable; "yes" indicates enable
Enable SSL = Yes

# If "Conduct SSL certificate authority" is enabled, please enter the full path of the
certificate file
Conduct SSL Certificate Authority = Yes
SSL Certificate Path = /root/test.pem

# Define the front server that got registered
Tenant Name =Initial Tenant
Front Server ID =FS1
```

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

4. Run the `./registration` command under the **bin** directory, 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 in starting 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 SSL Certificate Authority	`No`	Set whether to authenticate the Certificate Authority (CA) of SSL certificates on the Front Server Controller. If you want to authenticate the Certificate Authority, type **Yes**.
SSL Certificate Path		The full storage path and certificate name. **Note:** Only the certificate in the **Base-64 encoded X.509 PEM** format is supported. **Note:** Please ensure that the user **netbrain** can access the certificate file.
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.
Authentication Key		The authentication key created when you add this Front Server to a tenant.

4.7. Configuring Auto Upgrade Settings

Knowledge Cloud (KC) manages both the framework components and the platform resources and allows NetBrain Workstation to automatically upgrade a patch or minor release. Besides replacing the files, the auto-upgrade process may restart services, execute the database upgrading, check the system health and roll back the release if the update fails.

Due to security considerations, there will be no direct connection between KC and NetBrain Workstation. NetBrain System Administrator must download the software update package from NetBrain Customer Portal, manually upload the package into the system and then schedule system updates accordingly.

NetBrain Workstation Auto Upgrade flow consists of the following steps:

> **Note:** Only user with System Management permissions can perform the following actions.

1. Check the Latest Version
2. Download Package from NetBrain Customer Portal
3. Upload Package to NetBrain Workstation
4. Schedule Update
5. View Update Status
6. View Update History

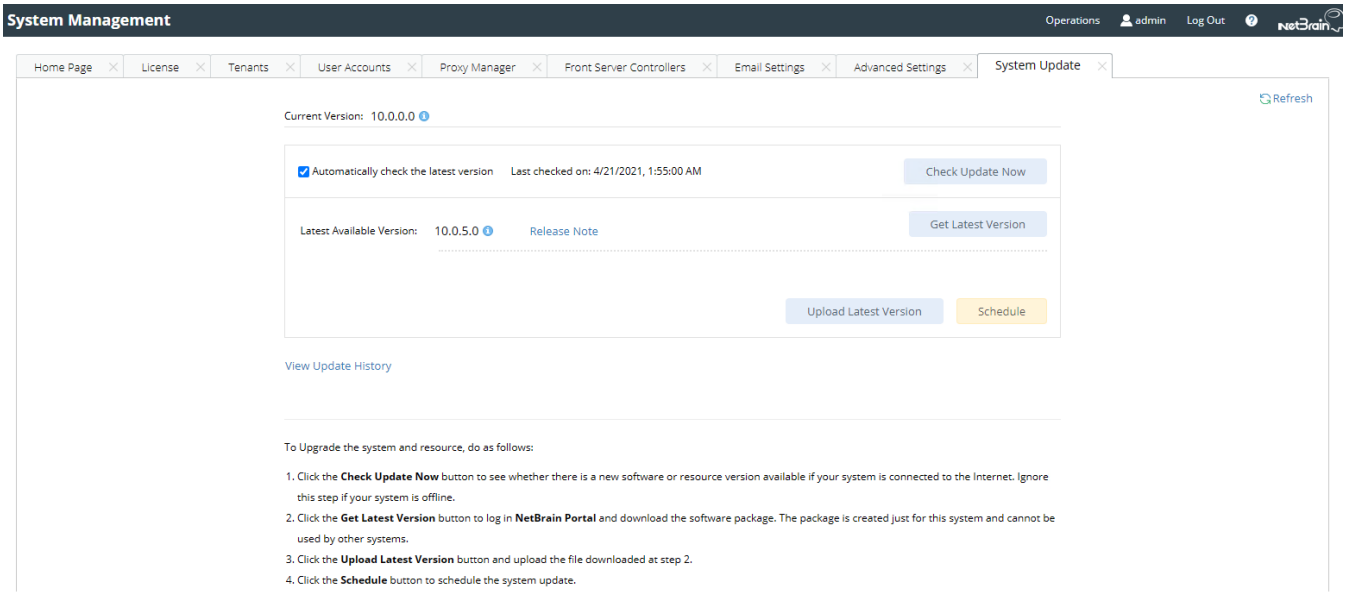
Check the Latest Version

Follow the steps below to check the available releases from NetBrain:

> **Note:** The following steps only apply to the online auto upgrade procedures.

1. In the System Management page, select **Operations > System Update**.
2. By default, the **Automatically check the latest version** check box is enabled. You can click **Check Update Now** to see if there is a new version available.

   > **Note:** The Web API Server is required to have internet access in order to perform the function of **Check Update Now**.



3. When this check is enabled, NetBrain Workstation will check whether a minor release, a patch, a customized built-in, a customized resource or common platform resource updates have been published since the last time check (either auto or manual check). The latest available version will be displayed with the release note.
4. If the respective release or patch is available, after reviewing the Release Note, click **Get Latest Version** to Download Package from NetBrain Customer Portal.

Download Package from NetBrain Customer Portal

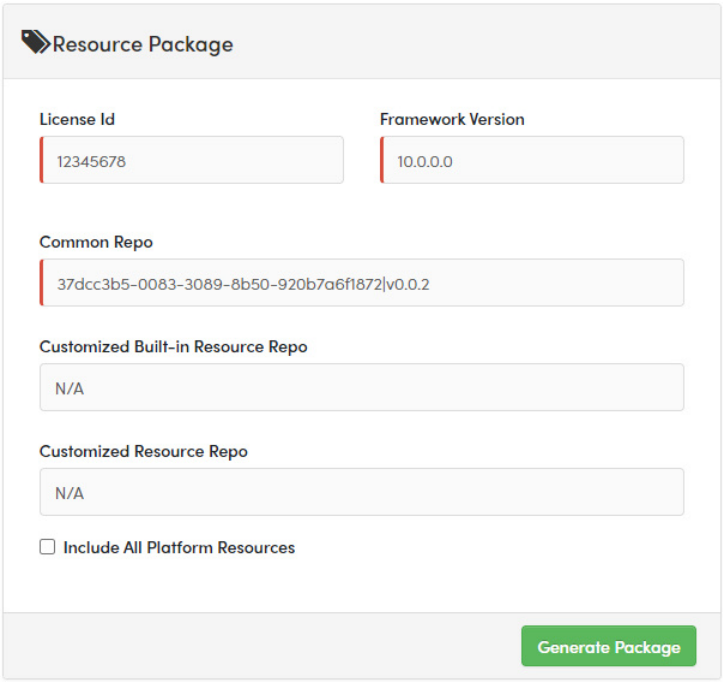
Follow the steps below to download the system upgrade package from NetBrain Customer Portal:

1. Log into the NetBrain Customer Portal with your username and password.

> **Note:** After clicking **Get Latest Version** in NetBrain Workstation, you will be redirected to the NetBrain Customer Portal. The portal account credentials are required by the web browser to grant access to the NetBrain Customer Portal.

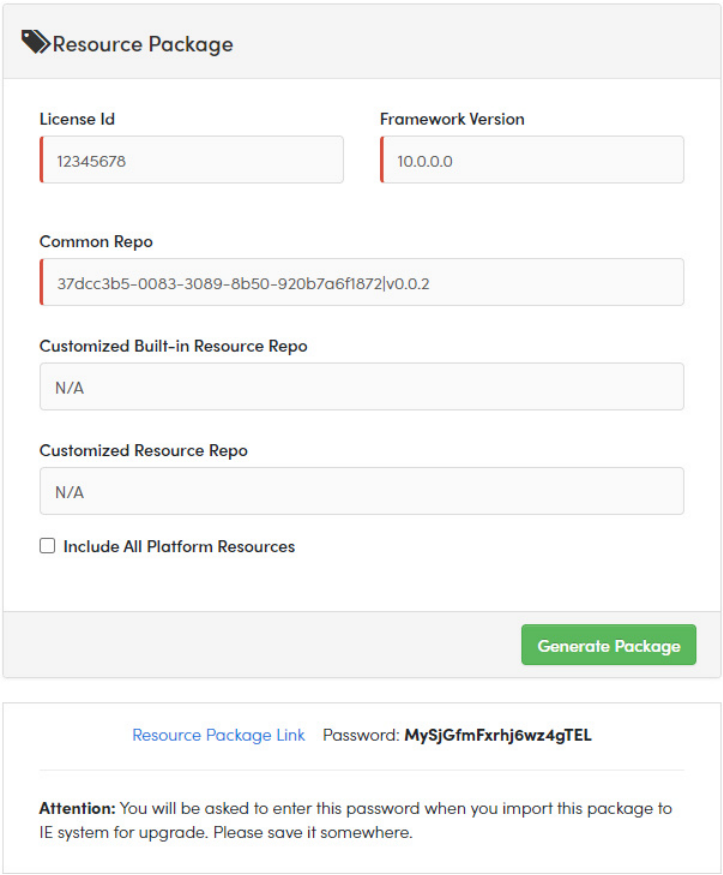
2. Confirm the required info and click **Generate Package**.

> **Tip:** Required info includes the License ID, Framework Version, Common Repo Version, Customized Built-in Resource Repo, Customized Resource Repo.



3. Click **Resource Package Link** to download the package to your local drive.

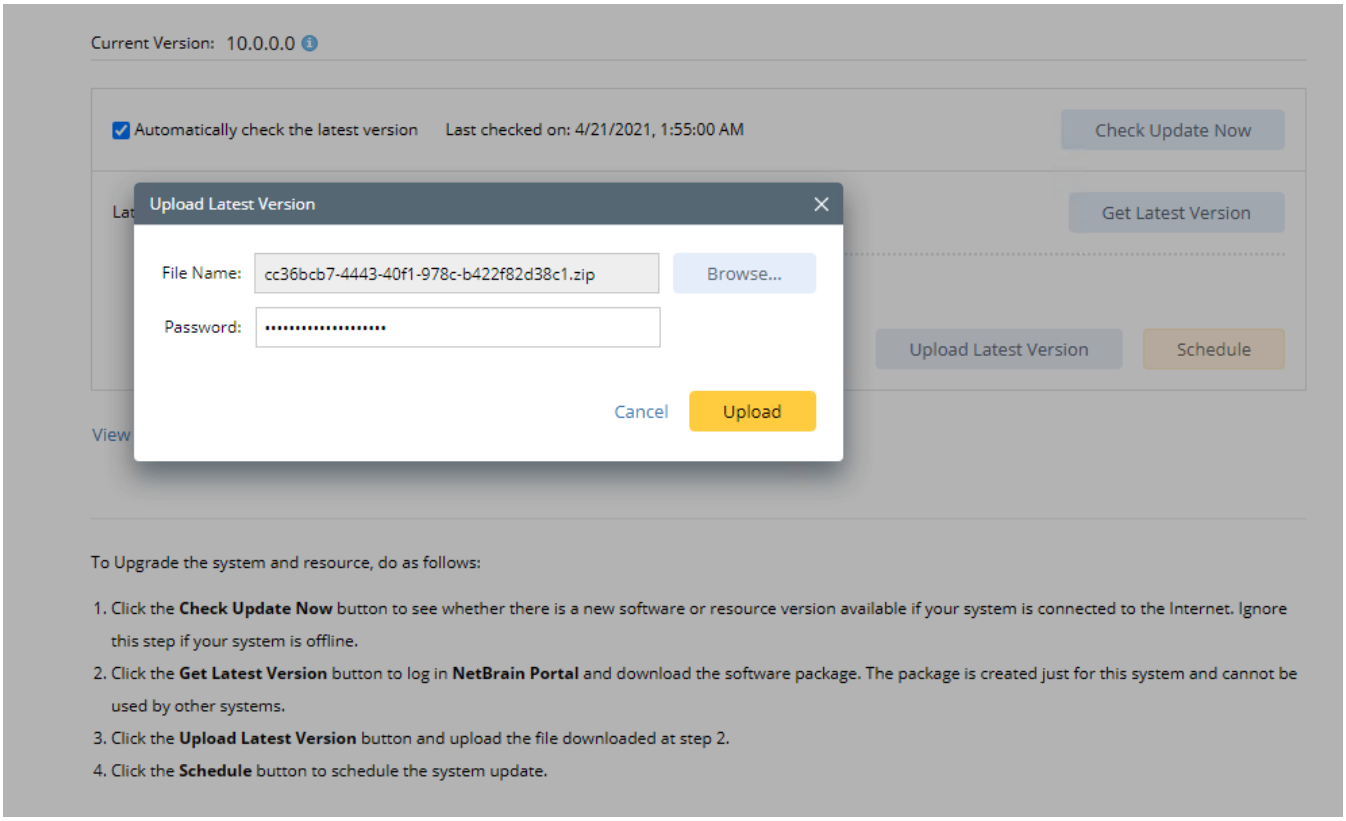
4. Keep note of the password for next step- Upload Package to NetBrain Workstation.



Upload Package to NetBrain Workstation

Follow the steps below to upload the system upgrade package to NetBrain Workstation:

1. In the System Management page, select **Operations > System Update**.
2. Click **Upload Latest Version**.
3. Click **Browse** and select the system upgrade package (.zip file).
4. Enter the password and click **Upload**.

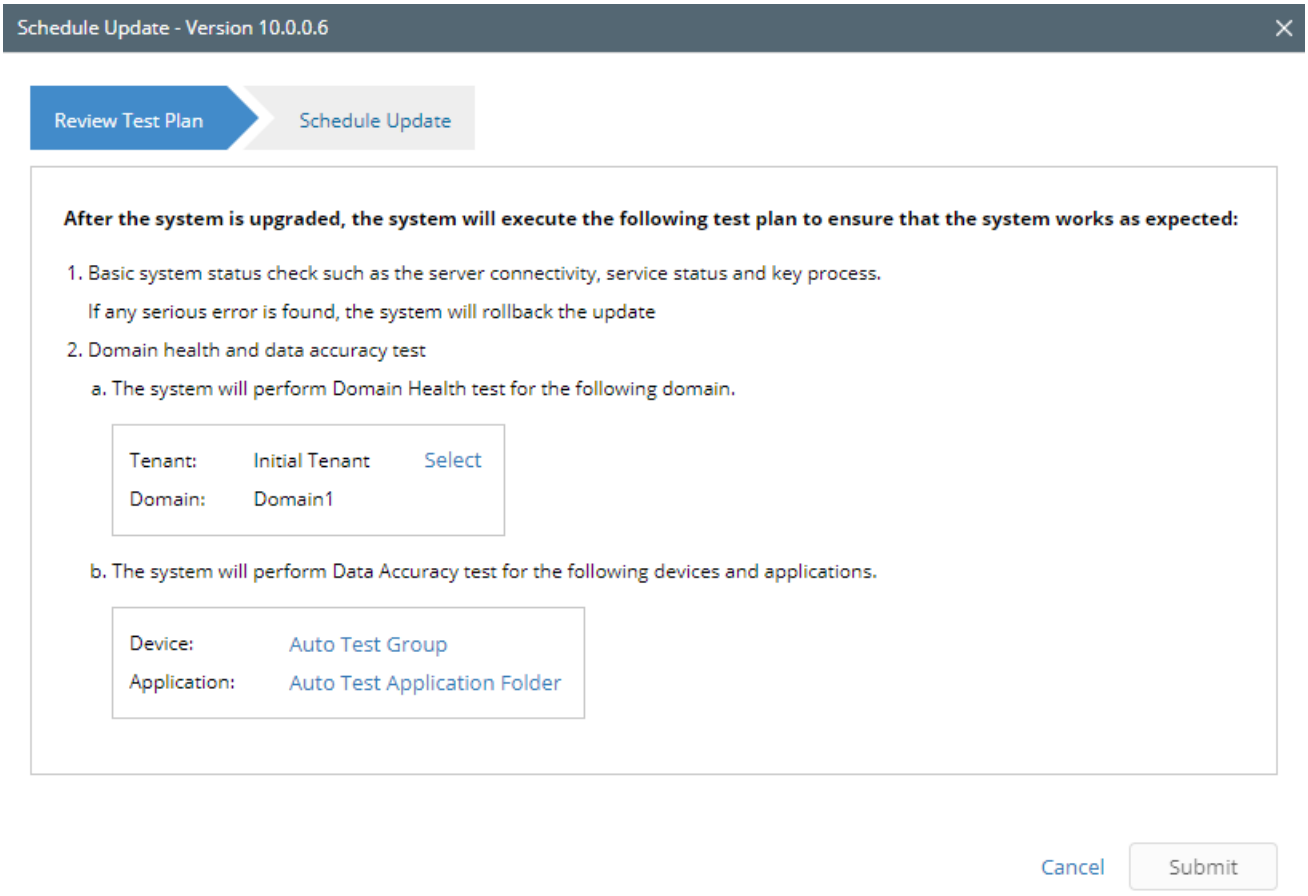


Schedule Update

Follow the steps below to schedule the system update:

1. In the System Management page, select **Operations > System Update**.
2. Click **Schedule**.

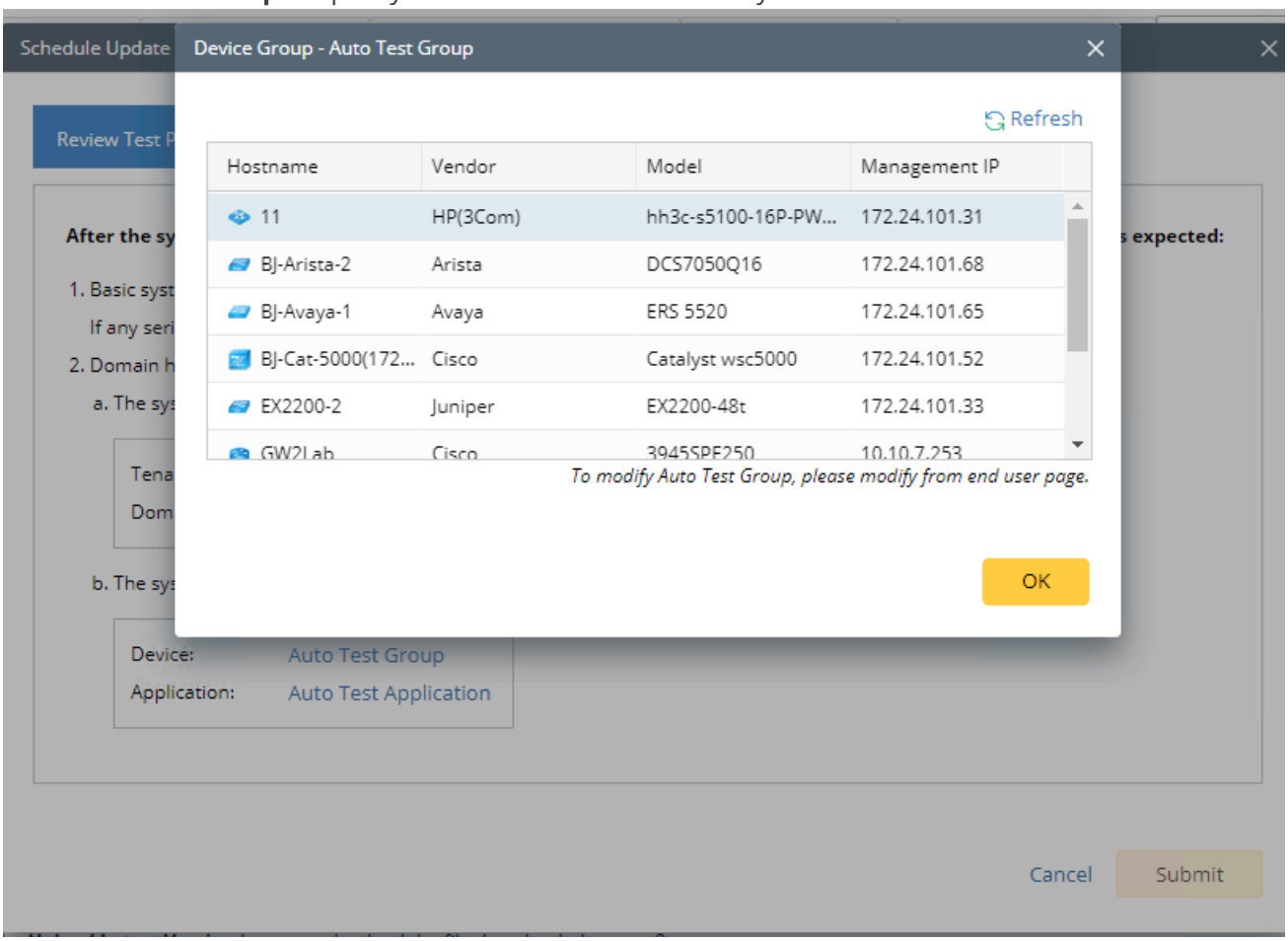
3. Review and update **Test Plan**



1) Click **Select** and specify the desired Tenant/Domain to perform Domain Health Check.

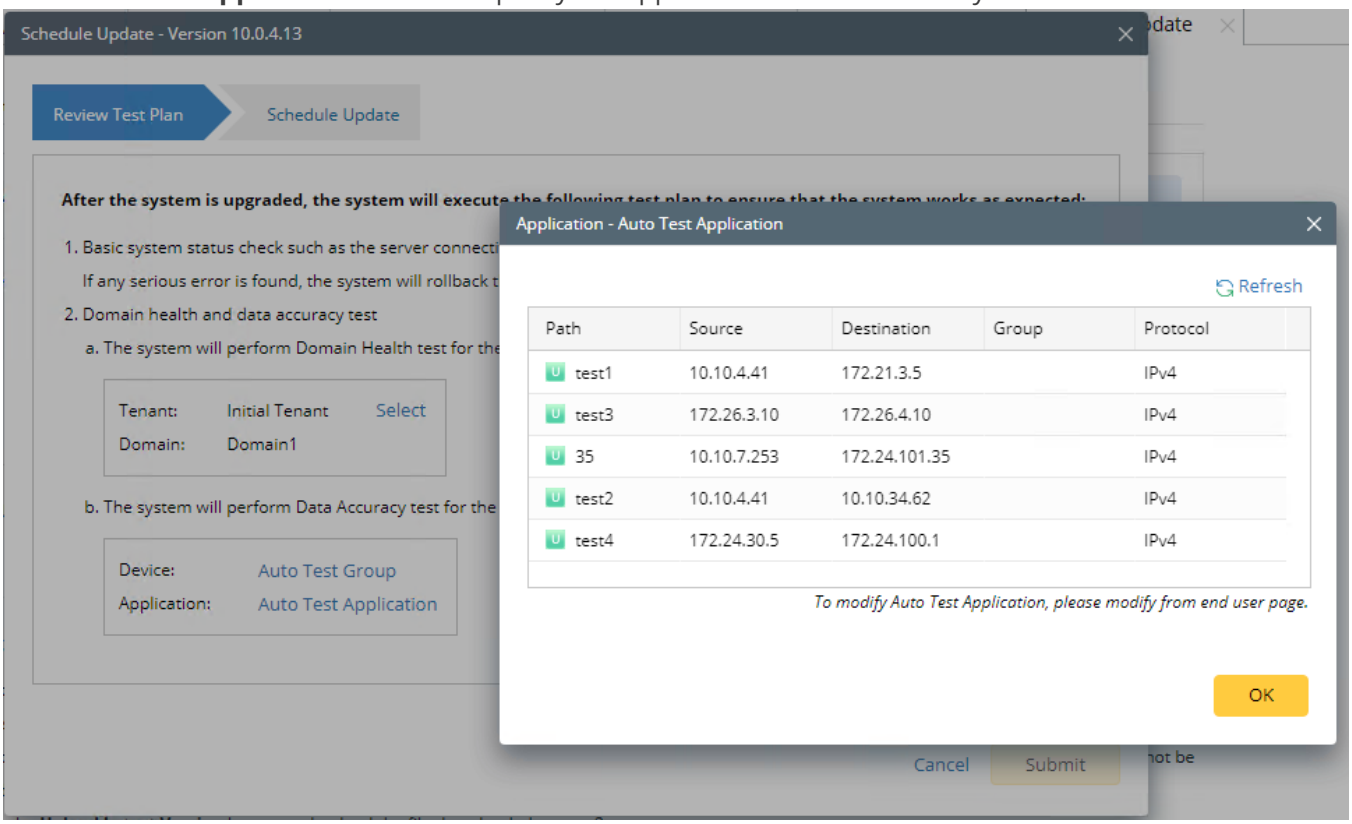
> **Note**: If there are more than one tenant or domain, step 1) must be completed before proceeding to step 2).
>
> **Note**: If there is only one tenant and domain, the Initial Tenant will be automatically selected and you can directly proceed to step 2).

2) Click **Auto Test Group** to specify the devices for Data Accuracy Test.



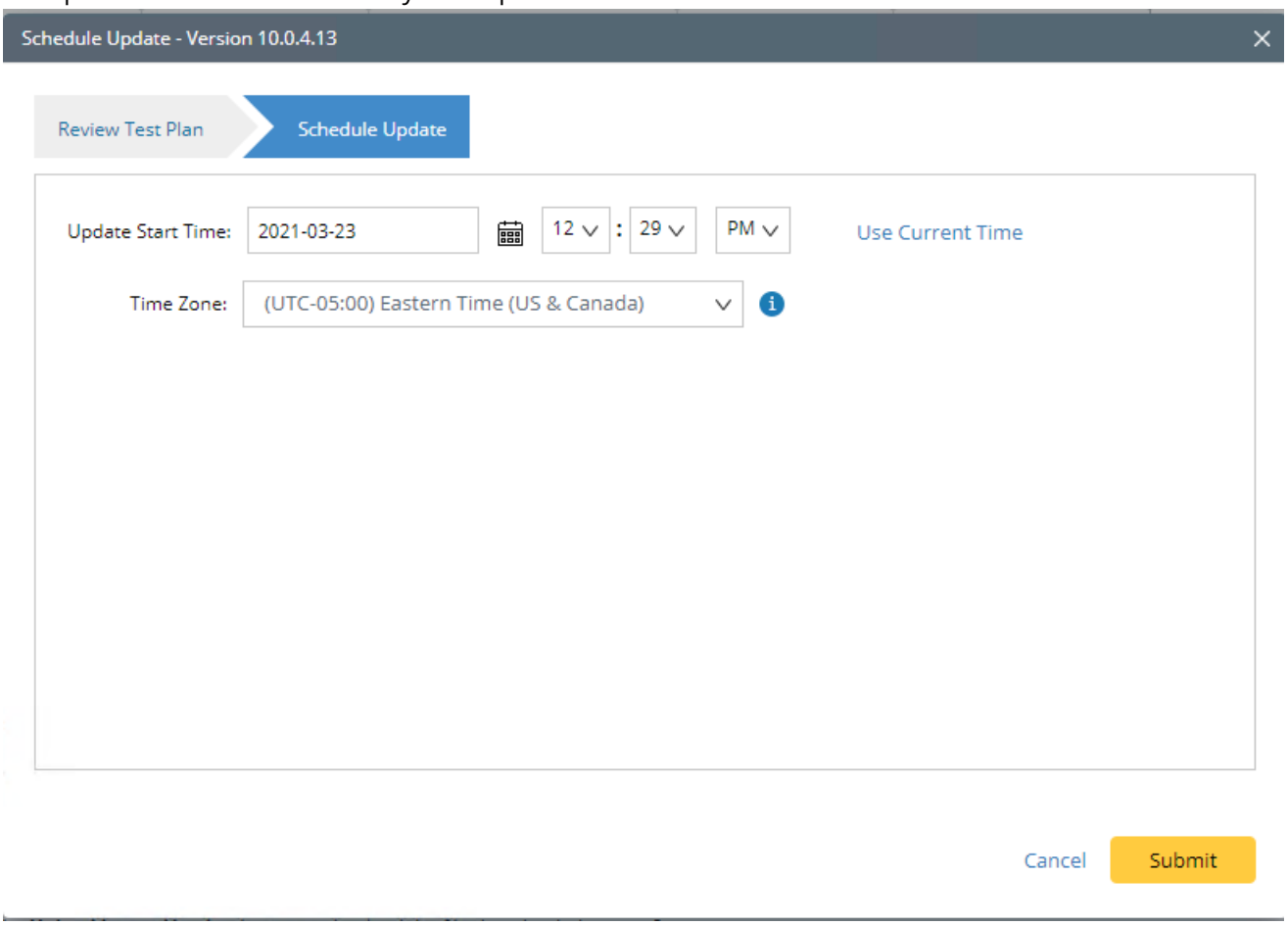
> **Tip**: The devices in the Auto Test Group are automatically selected according to the device type discovered by the system. You can also manually edit or delete any devices to suit your specific needs.

3) Click **Auto Test Application Folder** to specify the application for Data Accuracy Test.



> **Note**: The last used Application Paths (up to 5 paths) will be automatically copied to the Auto Test Application Folder. You can also manually change the auto selected path in Application Manager.

4. Set up the schedule to start the system update.



> **Tip:** You can edit or remove the system update time once it is scheduled.

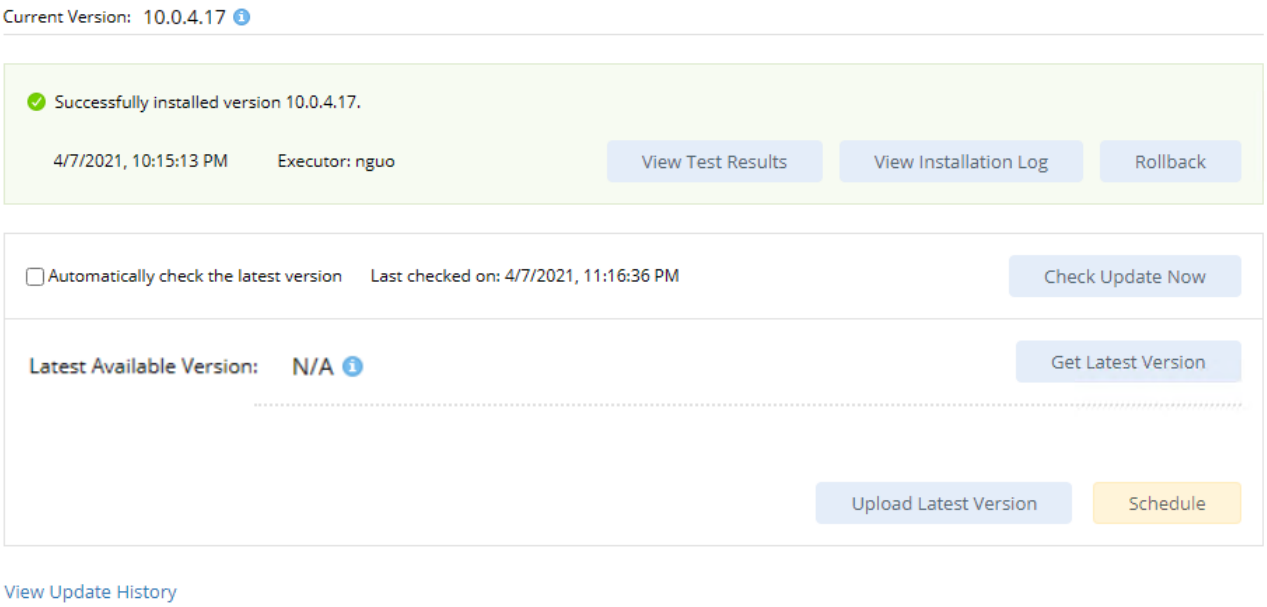
5. Click **Submit** to apply the above settings.

> **Note**: A confirmation message will prompt if the selected tenant/domain does not have application path, you can click Yes to dismiss the message and continue with the update process.

View Update Status

There are three possible outputs of auto update:

- The system is successfully updated to the new version.
- The update fails, and the system is rolled back to the old version.
- The update fails, and the system rollback fails.



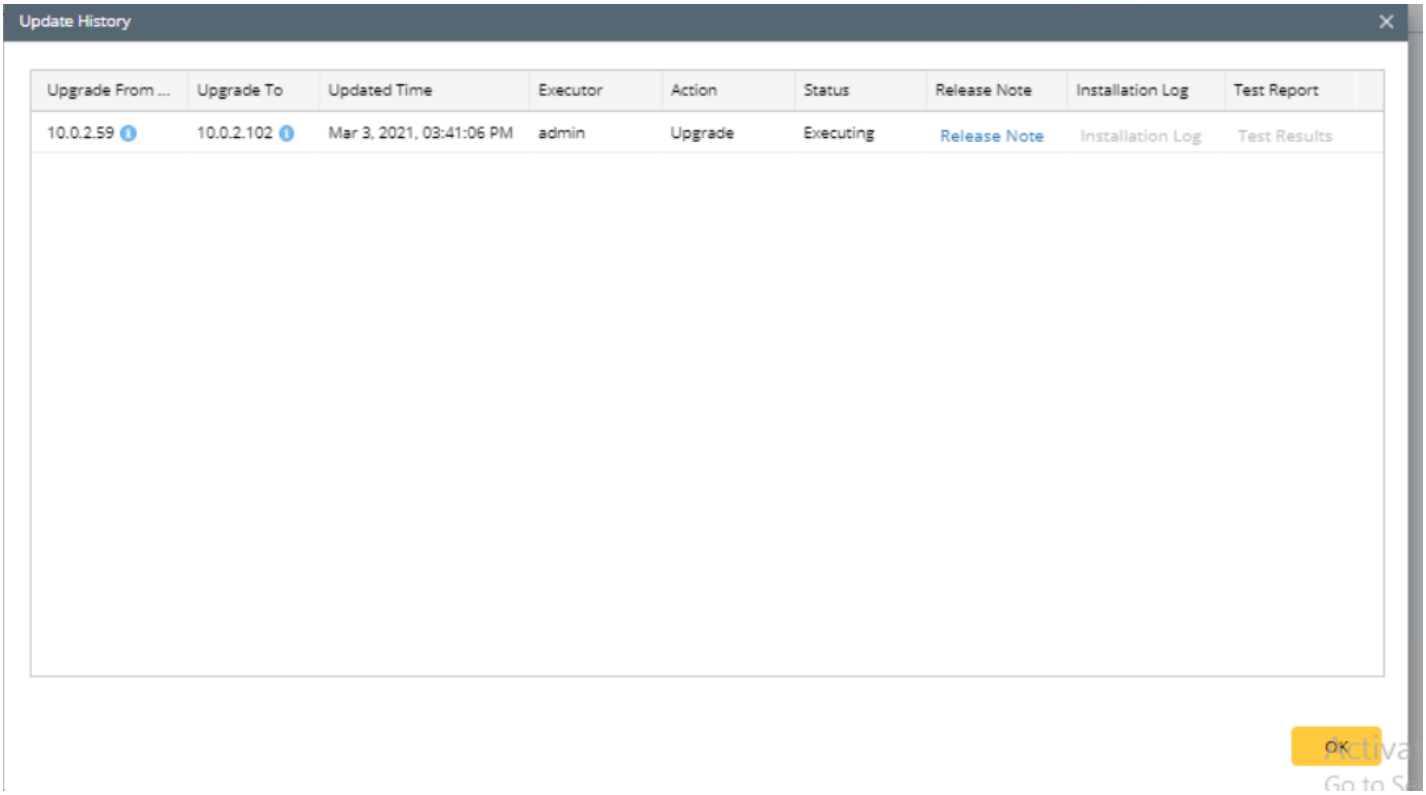
View Update History

Follow the steps below to view the update history:

1. In the System Management page, select **Operations > System Update**.
2. Click **View Update History**.

The update history only records the releases the system is scheduled to update with. The update history table provides the following information:

- **Version:** the release number to which the system is updated.
- **Update time:** when the system finished the update.
- **Executor:** the person to schedule the update
- **Status:** one of three status in View Update Status.
- **Installation log:** the link of the installation log.
- **Test report:** the link of the test results.



4.8. Monitoring Server and Service Metrics

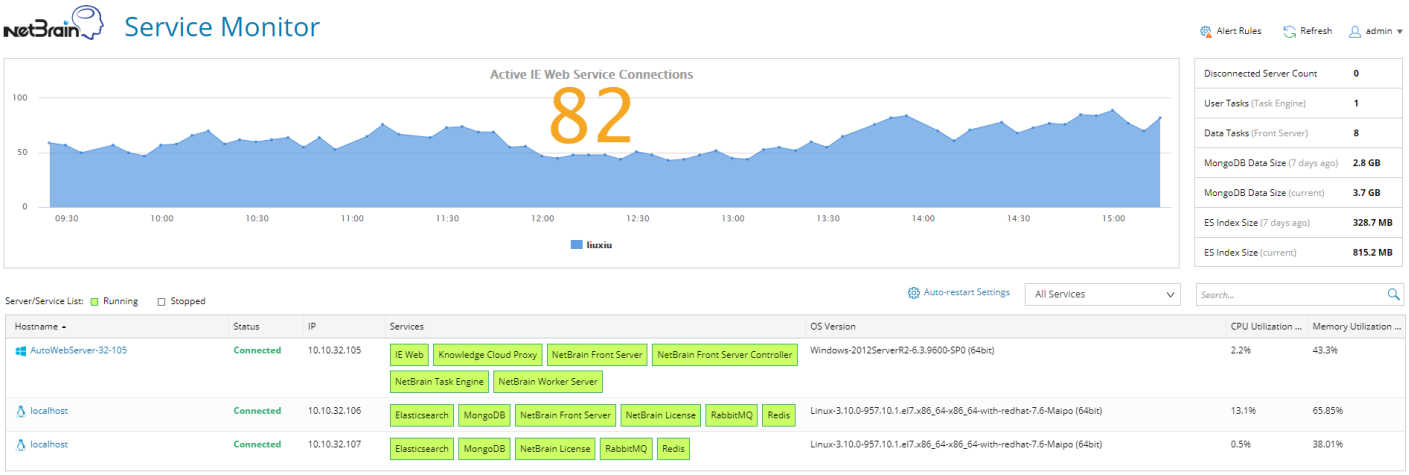
NetBrain Service Monitor provides a portal for administrators to observe the health of deployed Windows and Linux servers, with operations management of related services. It collects various types of metrics data from these deployed servers and visualizes them in tables or line charts.

> **Note:** The Service Monitor Agent must be installed on the servers that you want to monitor.
>
> **Note:** System upgrade feature heavily relies on all the NetBrain servers and service metrics, therefore it is required to ensure all the NetBrain servers and component metrics can be viewed in the Service Monitor page.

To monitor server and service metrics:

1. In the System Management page, click **Operations > Service Monitor** from the quick access toolbar.

2. In the Service Monitor home Page, you can monitor key server metrics, server connectivity, resource utilization, service status and so on.



3. Customize the conditions for when to send out alert emails and take more actions for low disk space on MongoDB by clicking **Alert Rules**. See Managing Alert Rules for more details.

5. Appendix

5.1. Offline Installing Third-party Dependencies

1. Download the dependency package from a server with the Internet access using one of the following download links according to the version of your Operating System:
   - **CentOS7.5:** http://download.netbraintech.com/dependencies-centos7.5.tar.gz
   - **CentOS7.6:** http://download.netbraintech.com/dependencies-centos7.6.tar.gz
   - **CentOS7.7:** http://download.netbraintech.com/dependencies-centos7.7.tar.gz
   - **CentOS7.8:** http://download.netbraintech.com/dependencies-centos7.8.tar.gz
   - **CentOS7.9:** http://download.netbraintech.com/dependencies-centos7.9.tar.gz
   - **CentOS8.2:** http://download.netbraintech.com/dependencies-centos8.2.tar.gz
   - **CentOS8.3:** http://download.netbraintech.com/dependencies-centos8.3.tar.gz
   - **RHEL7.5:** http://download.netbraintech.com/dependencies-rhel7.5.tar.gz
   - **RHEL7.6:** http://download.netbraintech.com/dependencies-rhel7.6.tar.gz
   - **RHEL7.7:** http://download.netbraintech.com/dependencies-rhel7.7.tar.gz
   - **RHEL7.8:** http://download.netbraintech.com/dependencies-rhel7.8.tar.gz
   - **RHEL7.9:** http://download.netbraintech.com/dependencies-rhel7.9.tar.gz
   - **RHEL8.2:** http://download.netbraintech.com/dependencies-rhel8.2.tar.gz
   - **RHEL8.3:** http://download.netbraintech.com/dependencies-rhel8.3.tar.gz
   - **OL7.7:** http://download.netbraintech.com/dependencies-ol7.7.tar.gz
   - **OL7.8:** http://download.netbraintech.com/dependencies-ol7.8.tar.gz
   - **OL7.9:** http://download.netbraintech.com/dependencies-ol7.9.tar.gz
   - **OL8.2:** http://download.netbraintech.com/dependencies-ol8.2.tar.gz
   - **OL8.3:** http://download.netbraintech.com/dependencies-ol8.3.tar.gz

2. Copy the downloaded dependency package to your Linux server.
3. Run the `tar -zxvf dependencies-<OS version>.tar.gz` command to decompress the package.

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

4. Run the `cd dependencies` command to navigate to the decompressed directory.
5. Run the `offline-install.sh` command to install the dependencies.

5.2. 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.

5.3. SSL Certificate Requirements

The requirements of SSL certificates may vary for different NetBrain servers, depending on their different roles in SSL encrypted connections, SSL-server or SSL-client.

- SSL Certificate Requirements for SSL-Server
- SSL Certificate Requirements for SSL-Client

Certificate Requirements for SSL-Server

The following table lists the requirements of SSL certificates for NetBrain servers that work as SSL-server in encrypted connections.

NetBrain Server	Required SSL Certificate and Key	Format
MongoDB License Agent Elasticsearch	▪ Certificate that contains a public key. For example, **cert.pem**. ▪ CA certificate (only required for Elasticsearch). For example, **ca.pem**.	**Base-64 encoded X.509 PEM**
Redis RabbitMQ Front Server Controller Ansible Agent	▪ Private key. For example, **key.pem**. **Note**: Private keys protected by a password are not supported.	**PKCS#8 key**

> **Tip**: The certificates in PEM format usually have extensions such as **.pem**, **.crt**, **.cer**, and **.key**.

Certificate Requirements for SSL-Client

> **Note:** By default, NetBrain servers that work as SSL-client don't require any SSL certificates. If you want to authenticate the Certificate Authority of the certificates for SSL-server, then the SSL certificates are required on SSL-client.

The following table lists the certificate requirements for SSL-client, including Web Server, Web API Server, Worker Server, Front Server, Task Engine, and Service Monitor Agent.

Authentication Method	Requirements	Format
Use the certificates installed on Windows	▪ All the certificates are valid and installed in the certificate store. ▪ The certificate store must be under the **Trusted Root Certification Authorities** directory instead of the **Personal** directory.	N/A
Upload certificates when installing NetBrain servers	▪ For Front Server and Worker Server: CA certificate containing root CA certificate and class 2 CA certificate is required. ▪ For other SSL-client: class 2 or class 3 CA certificate is required.	**Base-64 encoded X.509 PEM**

5.4. Third-Party User Authentication

In addition to creating user accounts manually, the system supports integrating with the following third-party user management systems for authentication.

- LDAP Authentication
- AD Authentication
- TACACS+ Authentication
- SSO Authentication

5.5. Configuring NTP Clients on NetBrain Servers

> **Note**: If all NetBrain servers are joined to a Windows domain, the NTP client service on these servers is automatically started by default. In this case, configuring NTP is not required.

Prerequisite: Before configuring NTP, prepare an internal NTP server or find the FQDN of a reliable external NTP server for usage. UDP port 123 must be open on the internal NTP server and on network firewalls to allow NTP traffic.

Follow the instructions to configure NetBrain servers as an NTP client:

- Configuring NTP on Windows
- Configuring NTP on Linux