



NetBrain[®] Next-Gen R12.1

System Setup Guide

Distributed Deployment

1. System Overview.....	4
2. System Requirements.....	7
3. Deploying and Installing System.....	18
3.1. Installing Service Monitor Agent on Linux	18
3.2. Installing MongoDB on Linux	22
3.3. Installing Elasticsearch on Linux	26
3.4. Installing License Agent on Linux	31
3.5. Installing Redis on Linux.....	35
3.6. Installing RabbitMQ on Linux	39
3.7. Installing Service Monitor Agent on Windows	44
3.8. Installing Web/Web API Server on Windows.....	48
3.9. Installing Worker Server on Windows	60
3.10. Installing Task Engine on Windows	70
3.11. Installing Front Servers Controller on Windows.....	75
3.12. Installing Front Servers	82
3.12.1. Installing Front Server on Linux.....	82
3.12.2. Installing Front Server on Windows.....	85
4. Setting Up Your System	89
4.1 Logging in to System Management Page.....	90
4.2 Activating a Subscription License	90
4.3 Creating User Accounts	91
4.4 Allocating Tenants to Front Server Controller	92
4.5 Adding a Front Server for a Tenant.....	94

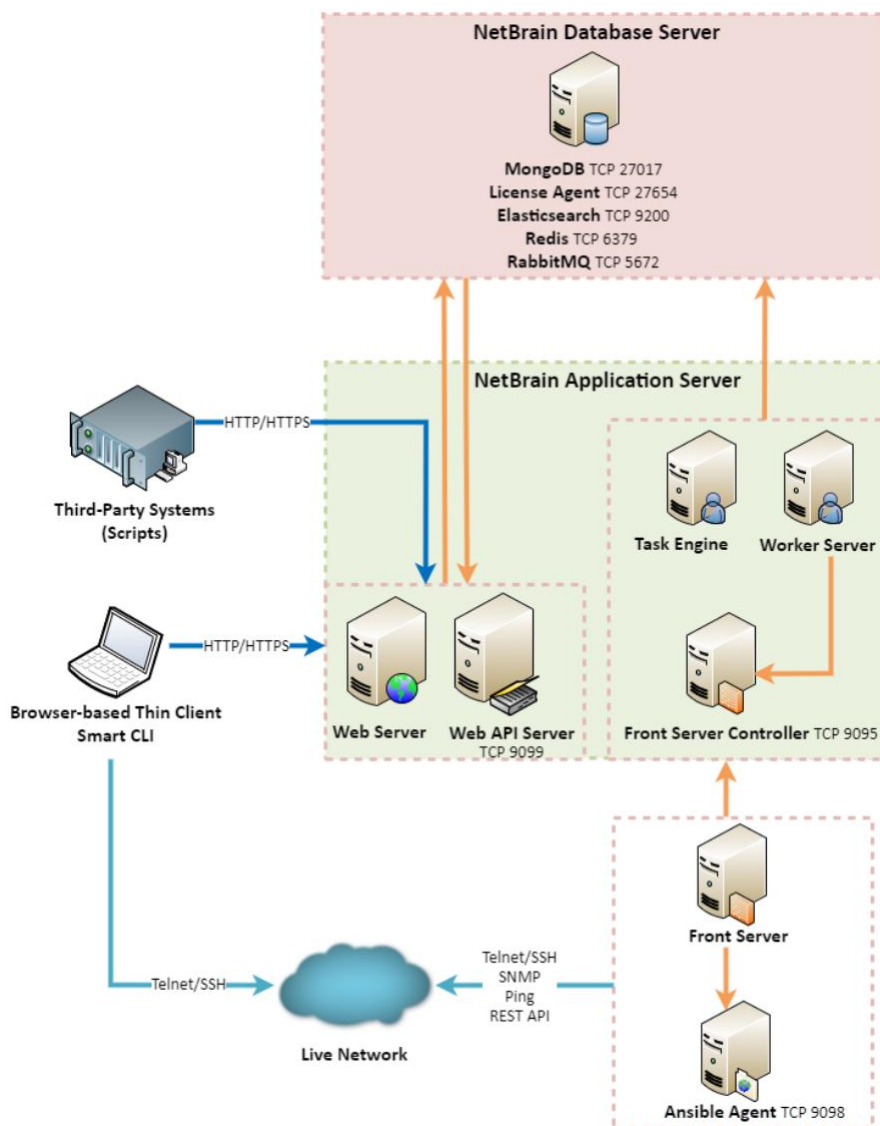
4.6	Registering a Front Server.....	95
4.7	Configuring Auto Upgrade Settings	99
4.8	Monitoring Server and Service Metrics	108
5.	Appendix.....	110
5.1	Offline Installing Third-party Dependencies	110
5.2	Editing a File with VI Editor.....	113
5.3	SSL Certificate Requirements	113
5.4	Third-Party User Authentication.....	114
5.5	Configuring NTP Clients on NetBrain Servers.....	115

1. System Overview

NetBrain 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 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	It provides a user interface for end users to access the system.
MongoDB	The database that stores user data (e.g., Map, site definition) and network data.
License Agent	It provides services that validate and activate licenses.
Elasticsearch	It serves as a full-text search and analytics engine in a distributed multi-user environment.
Redis	It provides memory cache for the system.
RabbitMQ	It translates messages from a component to another component.
Web Server	It serves static content such as HTML, JavaScript, and CSS resources, which serves as the user interface of the Thin Client.
Web API Server	It serves RESTful API calls from browsers and third-party applications for integration.
Worker Server	It serves as a resource manager to support computing tasks. It relies on both Redis and RabbitMQ to work.
Task Engine	It coordinates computing tasks.
Front Server Controller	It serves to coordinate and communicate with Front Servers and other components.
Front Server	It 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	It monitors the health of your NetBrain Servers with operations management of related services. Users can start/stop the service of components and view log of components.
Ansible Agent (add-on)	It integrates with Ansible to define, execute playbooks and visualize results in Change Management Runbooks. See Ansible Integration for more details.
Smart CLI (add-on)	It 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	<ul style="list-style-type: none"> ▪ 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

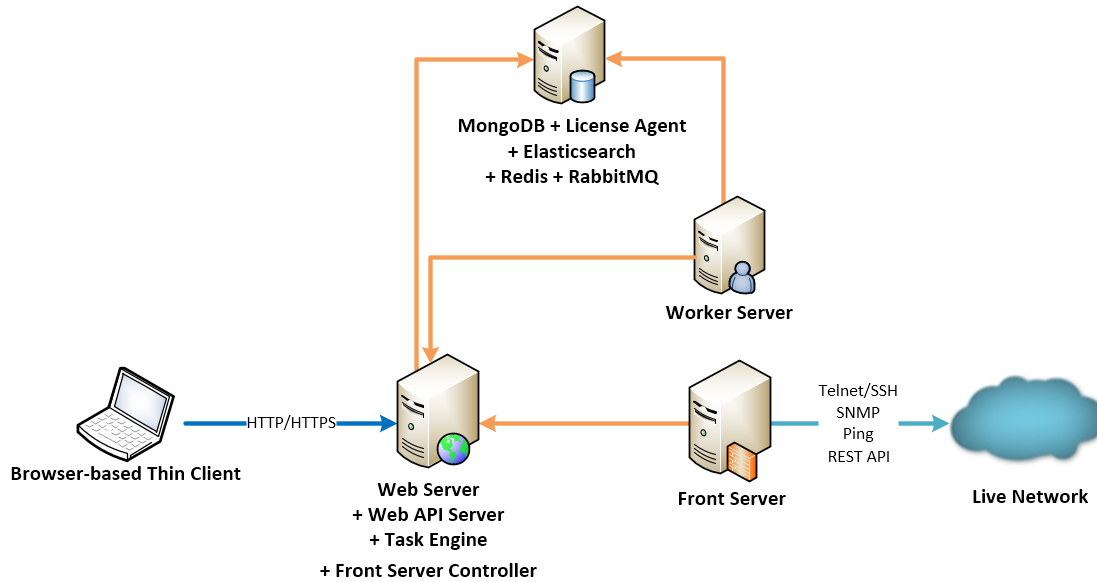
Note: The following specifications only apply to traditional network. Refer to [Public Cloud System Specification](#) if you have activated the public cloud (AWS/Azure) license.

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](#)

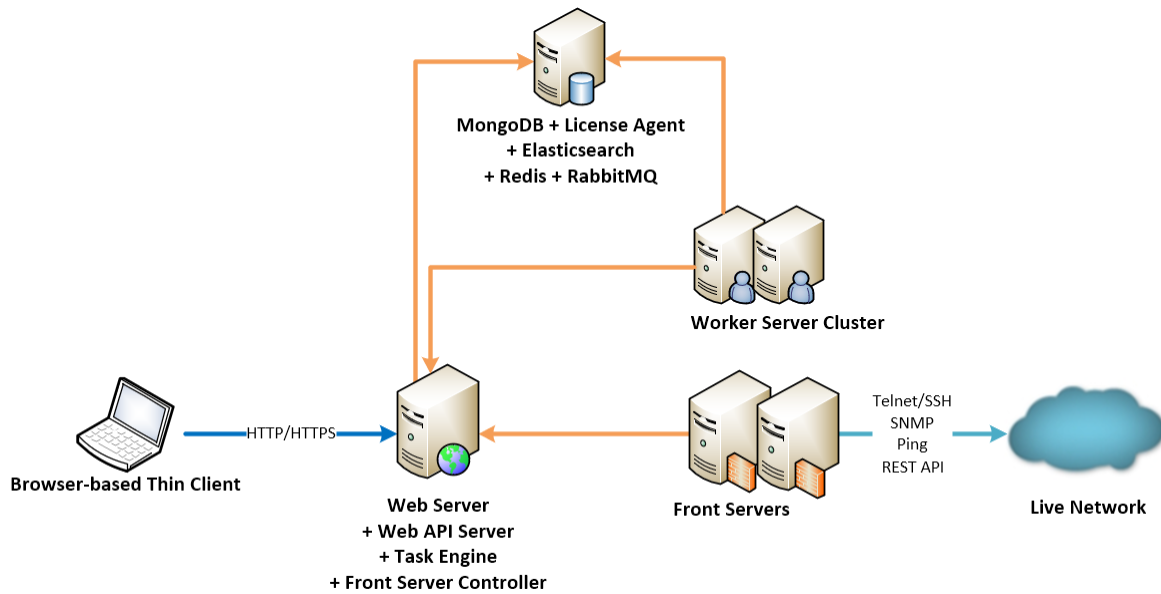
Distributed deployment for 2001~5000 nodes



Environment	System Component	Machine Count	CPU ^{10) 11)}	Memory ²⁾	Hard Disk ⁴⁾ (Free Space)	Operating System
2,001~5,000 nodes ≤ 20 users	Web Server Web API Server Task Engine Front Server Controller Service Monitor	1	4 Physical Cores ¹⁾	32GB	200GB	<ul style="list-style-type: none"> Windows Server 2016/2019/2022/2025 (Standard/Datacenter Edition), 64-bit
	Worker Server Service Monitor	1	8 Physical Cores ¹⁾	32GB	200GB	
	Front Server Service Monitor	1	4 Physical Cores ¹⁾	8GB	<ul style="list-style-type: none"> 300GB (HDD) (node # ≤2000) ⁶⁾ 300GB (SSD) (node # ≤5000) ⁶⁾ 	<ul style="list-style-type: none"> Windows Server 2016/2019/2022/2025 (Standard/Datacenter Edition), 64-bit Red Hat Enterprise Linux Server⁸⁾ 8.4/8.5/8.6/8.7/8.8/8.9/ 8.10/9.4/9.5, 64-bit Oracle Linux⁸⁾ 8.4/8.5/8.6/8.7/8.8/8.9/ 8.10/9.4/9.5, 64-bit Rocky Linux 8.4/8.5/8.6/8.7/8.8/8.9/ 8.10/9.4/9.5, 64-bit

Environment	System Component	Machine Count	CPU ¹⁰⁾ ¹¹⁾	Memory ²⁾	Hard Disk ⁴⁾ (Free Space)	Operating System
						<ul style="list-style-type: none"> Alma Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Amazon Linux 2023, 64-bit
	MongoDB License Agent Elasticsearch Redis RabbitMQ Service Monitor	1	4 Physical Cores ¹⁾	32GB	500GB (SSD)	<ul style="list-style-type: none"> Red Hat Enterprise Linux Server⁸⁾ 8.2/8.3/8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Oracle Linux⁸⁾ 8.2/8.3/8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Rocky Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Alma Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Amazon Linux 2023, 64-bit

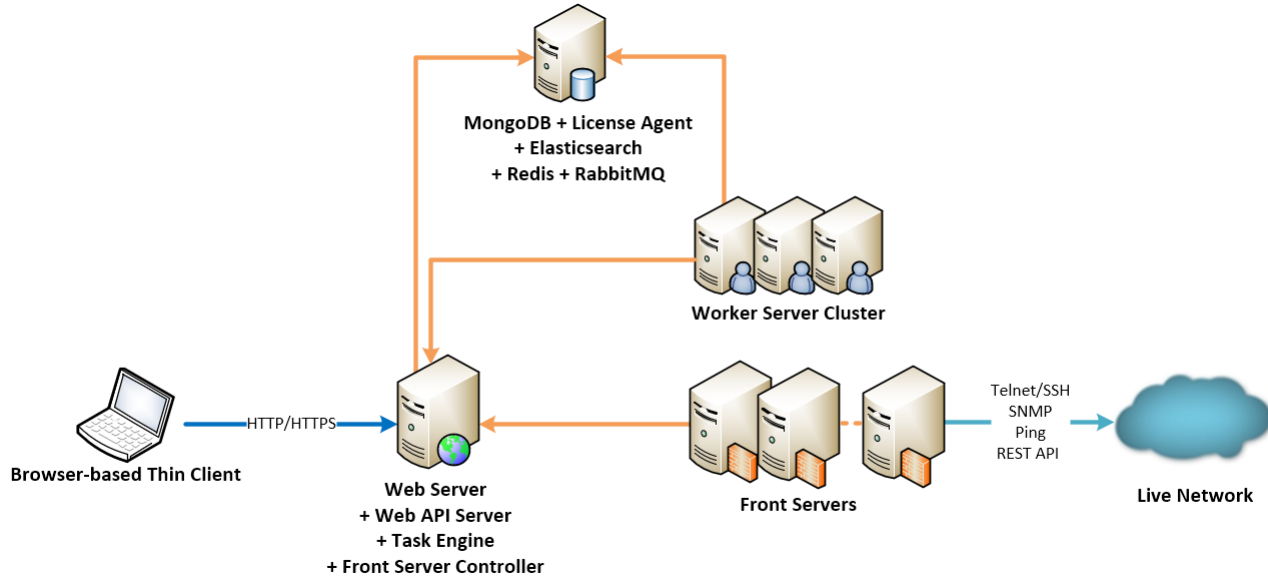
Distributed deployment for 5001~10000 nodes



Environment	System Component	Machine Count	CPU ^{10) 11)}	Memory ²⁾	Hard Disk ⁴⁾ (Free Space)	Operating System
5,001~10,000 nodes ≤ 50 users	Web Server Web API Server Task Engine Front Server Controller Service Monitor	1	8 Physical Cores ¹⁾	32GB	200GB	<ul style="list-style-type: none"> Windows Server 2016/2019/2022/2025 (Standard/Datacenter Edition), 64-bit
	Worker Server Service Monitor	2	8 Physical Cores ¹⁾	32GB	200GB	
	Front Server Service Monitor	2	4 Physical Cores ¹⁾	8GB	<ul style="list-style-type: none"> 300GB (HDD) (node # ≤2000)⁶⁾ 300GB (SSD) (node # ≤5000)⁶⁾ 	<ul style="list-style-type: none"> Windows Server 2016/2019/2022/2025 (Standard/Datacenter Edition), 64-bit Red Hat Enterprise Linux Server⁸⁾ 8.4/8.5/8.6/8.7/8.8/8.9/8.10 /9.4/9.5, 64-bit Oracle Linux⁸⁾ 8.4/8.5/8.6/8.7/8.8/8.9/8.10 /9.4/9.5, 64-bit

Environment	System Component	Machine Count	CPU ^{10) 11)}	Memory ²⁾	Hard Disk ⁴⁾ (Free Space)	Operating System
						<ul style="list-style-type: none"> Rocky Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10 /9.4/9.5, 64-bit Alma Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10 /9.4/9.5, 64-bit Amazon Linux 2023, 64-bit
	MongoDB License Agent Elasticsearch Redis RabbitMQ Service Monitor	1	8 Physical Cores ¹⁾	64GB	1TB (SSD)	<ul style="list-style-type: none"> Red Hat Enterprise Linux Server⁸⁾ 8.2/8.3/ 8.4/8.5/8.6/8.7/8.8/8.9/8.10 /9.4/9.5, 64-bit Oracle Linux⁸⁾ 8.2/8.3/8.4/8.5/8.6/8.7/8.8/ 8.9/8.10/9.4/9.5, 64-bit Rocky Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10 /9.4/9.5, 64-bit Alma Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10 /9.4/9.5, 64-bit Amazon Linux 2023, 64-bit

Distributed deployment for 10001~50000 nodes



Environment	System Component	Machine Count	CPU ^{10) 11)}	Memory ²⁾	Hard Disk ⁴⁾ (Free Space)	Operating System
10,001~50,000 nodes ≤ 200 users	Web Server Web API Server Task Engine Front Server Controller Service Monitor	1	8 Physical Cores ¹⁾	32GB	200GB	<ul style="list-style-type: none"> Windows Server 2016/2019/2022/2025 (Standard/Datacenter Edition), 64-bit
	Worker Server Service Monitor	3	8 Physical Cores ¹⁾	32GB	200GB	
	Front Server Service Monitor	3~10	4 Physical Cores ¹⁾	8GB	<ul style="list-style-type: none"> 300GB (HDD) (node # ≤2000) ⁶⁾ 300GB (SSD) (node # ≤5000) ⁶⁾ 	<ul style="list-style-type: none"> Windows Server 2016/2019/2022/2025 (Standard/Datacenter Edition), 64-bit Red Hat Enterprise Linux Server⁸⁾ 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Oracle Linux⁸⁾ 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Rocky Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit

Environment	System Component	Machine Count	CPU ^{10) 11)}	Memory ²⁾	Hard Disk ⁴⁾ (Free Space)	Operating System
						<ul style="list-style-type: none"> Alma Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Amazon Linux 2023, 64-bit
	MongoDB License Agent Elasticsearch Redis RabbitMQ Service Monitor	1	8 Physical Cores ¹⁾	128GB	2TB (SSD)	<ul style="list-style-type: none"> Red Hat Enterprise Linux Server⁸⁾ 8.2/8.3/8.4/8.5/8.6/8.7/8.8/8.9/ 8.10/9.4/9.5, 64-bit Oracle Linux⁸⁾ 8.2/8.3/8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Rocky Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Alma Linux 8.4/8.5/8.6/8.7/8.8/8.9/8.10/9.4/9.5, 64-bit Amazon Linux 2023, 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⁾ Each Front Server is recommended to manage 5,000 network nodes at most.

⁴⁾ The required hard disk space must be exclusively reserved for NetBrain.

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

⁶⁾ 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
- 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.

⁸⁾ With the end-of-life of Linux 7.* and some Linux 8.* versions, the following operating systems are only supported for upgrades to R12.1 and are not available for fresh installations: RHEL 7.5/7.6/7.7/7.8/7.9; CentOS 7.5/7.6/7.7/7.8/7.9/8.2/8.3/8.4/8.5; OL 7.7/7.8/7.9.⁹⁾ For Linux servers, make sure each path has enough free space to install the component files:

- **/var/**, **/etc/**, and **/usr/share/** more than 10GB

- **/usr/** more than 5GB

- **/bin/** more than 500MB

¹⁰⁾ CPU must support AVX2.

¹¹⁾ x86_64 processors are supported, while ARM-based processors are not supported.

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
Web API Server Worker Server	LLM Service****) (The default URL is https://api.openai.com .)	HTTPS 443

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.

Note: ***) The network latency should be less than 30 ms for Redis optimal performance.

Note: ****) The LLM service is optional.

Note: To optimize the performance, the network delays between MongoDB nodes should be less than 30 ms if a MongoDB replica set is installed.

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 traffic to all the ports and protocols that will be used by the NetBrain system.
- The Service Monitor Agent running on the Linux server(s) uses “netbrainadmin” user, and this user needs sudoers privilege to monitor other NetBrain components as well as to execute the system update tasks.

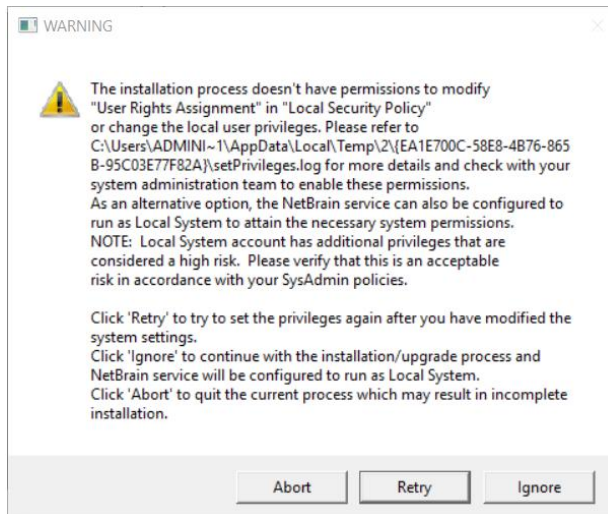
▪ **Special Requirements for Client Machine**

- 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 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.
- There must be more than **180GB** free space for the Front Server PostgreSQL data path.
- Temporarily disable antivirus software during the installation process.
- Ensure the port 9070 is open and available on the machine where the Web API Service is installed.
- Ensure the system update is paused prior to the installation.
- 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 **Ignore** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System.
- If you have security concerns, click **Abort** to quit the installation/upgrade process.
- Click **Retry** after you have modified the system settings.

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 **Abort**, 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 **200GB** 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 Service Monitor Agent on Linux](#).
2. [Install MongoDB on Linux](#).
3. [Install Elasticsearch on Linux](#).
4. [Install License Agent on Linux](#).
5. [Install Redis on Linux](#).
6. [Install RabbitMQ on Linux](#).
6. [Install Service Monitor Agent on Windows](#).
7. [Install Web/Web API Server on Windows](#).
8. [Install Worker Server on Windows](#).
9. [Install Task Engine on Windows](#).
10. [Install Front Server Controller on Windows](#).
11. [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 Service Monitor Agent on Linux

1. Log in to the Linux server as the **root** or **sudo** user.
2. Run the `cd /opt/netbraintemp12.1` command to navigate to the **/opt/netbraintemp12.1** 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-12.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp12.1** 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/netbraintemp12.1** directory to directly download the **netbrain-servicemonitoragent-linux-x86_64-rhel-12.1.tar.gz** file from NetBrain official download site.

Note: Contact [NetBrain Support Team](#) to get the download link. 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-12.1.tar.gz` command under the **/opt/netbraintemp12.1** directory to extract installation files.

```
[root@localhost netbraintemp12.1]# tar -zxvf netbrain-servicemonitoragent-linux-x86_64-rhel-12.1.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/netbrain/servicemonitoragent

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

# CertAuth specifies the CA file source path. Below CA file will be copied to folder
/etc/ssl/netbrain/nbagent
CertAuth=/opt/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 daemon setting...
Daemon 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
```

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.

Parameter	Default Value	Description
LogPath	<code>/var/log/netbrain/nbagent</code>	The storage path for the log files of the Service Monitor Agent. Note: At least 10GB free disk space is required.
CA_Verify	<code>no</code>	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	<code>/opt/cacert.pem</code>	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.

3.2. Installing MongoDB on Linux

1. Log in to the Linux server as the **root** or **sudo** 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, **netbraintemp12.1**.

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

3. Run the `cd /opt/netbraintemp12.1` command to navigate to the **/opt/netbraintemp12.1** 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-8.0.5-12.1.tar.gz** file from NetBrain and upload it to the **/opt/netbraintemp12.1** 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/netbraintemp12.1** directory to directly download the **mongodb-linux-x86_64-rhel-8.0.5-12.1.tar.gz** file from NetBrain official download site.

Note: Contact [NetBrain Support Team](#) to get the download link. 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-8.0.5-12.1.tar.gz` command under the **/opt/netbraintemp12.1** directory to extract installation files.

```
[root@Rocky netbraintemp12.1]# tar -zxvf mongodb-linux-x86_64-rhel-8.0.5-12.1.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@Rocky 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=/opt/cert.pem
PrivateKey=/opt/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@Rocky MongoDB]# ./install.sh
INFO: Creating installation log file SUCCEEDED

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: mongodbcfg
INFO: RPM package list: mongodbcfg-8.0.5-el8.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
...
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.
```

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@Rocky ~]# ps -ef|grep mongo
netbrain  46482      1   3 01:30 ?                00:00:03 /bin/mongo -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	<code>/usr/lib</code>	<p>Specify the storage path for all MongoDB data files.</p> <p>Note: Make sure the destination directory has more than 100GB free space to save all the data files.</p> <p>Tip: You can run the <code>df -h</code> command to check which directory has been mounted to a large disk.</p>
LogPath	<code>/var/log</code>	<p>Specify the storage path for all MongoDB log files.</p> <p>Note: Make sure the destination directory has more than 50GB free space to save all the log files.</p>
BindIp	<code>127.0.0.1</code>	<p>Specify the IP address of MongoDB.</p> <p>Note: Don't use 127.0.0.1.</p> <p>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.</p>
FQDN	<code>127.0.0.1</code>	<p>Specify the fully qualified domain name (FQDN) of MongoDB.</p> <p>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.</p>
Port	<code>27017</code>	<p>Specify the port number that the MongoDB service listens to. It is recommended to keep the default value.</p>
ReplicaSetName	<code>Rs</code>	<p>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.</p> <p>Note: It can only contain letters and numbers, and must start with a letter.</p>
UseSSL	<code>no</code>	<p>Specify whether to encrypt the connections to MongoDB with SSL.</p> <p>To enable SSL, replace no with yes. For detailed requirements of SSL certificates and keys, refer to SSL Certificate Requirements.</p>
Certificate	<code>/opt/cert.pem</code>	<p>Specify the name and storage path of the certificate file that contains the public key.</p> <p>Note: It is required only if UseSSL is enabled.</p>
PrivateKey	<code>/etc/ssl/key.pem</code>	<p>Specify the name and storage path of the private key file.</p> <p>Note: It is required only if UseSSL is enabled.</p>

Parameter	Default Value	Description
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. <code>{ } [] : " , ' < > @ & ^ % \</code> 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.

3.3. Installing Elasticsearch on Linux

Note: You must [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 v21.0.4** which will be automatically installed while Elasticsearch is installed.

1. Log in to the Linux server as the **root** or **sudo** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp12.1**.
3. Run the `cd /opt/netbraintemp12.1` command to navigate to the **/opt/netbraintemp12.1** 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-8.15.2-12.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp12.1** 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/netbraintemp12.1** directory to directly download the **elasticsearch-linux-x86_64-rhel-8.15.2-12.1.tar.gz** file from NetBrain official download site.

Note: Contact [NetBrain Support Team](#) to get the download link. 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-8.15.2-12.1.tar.gz` command under the **/opt/netbraintemp12.1** directory to extract installation files.

```
[root@Rocky netbraintemp12.1]# tar -zxvf elasticsearch-linux-x86_64-rhel-8.15.2-12.1.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@Rocky 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=/opt/cert.pem
PrivateKey=/opt/key.pem
CertAuth=/opt/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@Rocky Elasticsearch]# ./install.sh
INFO: Creating installation log file SUCCEEDED
INFO: Collecting system information SUCCEEDED.
INFO: Component Name: Elasticsearch
INFO: RPM name: elasticsearch
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...
...
INFO: Successfully installed searchguard.
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: The netbrainagent service 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@Rocky Elasticsearch]# curl -s -XGET --user admin:Admin1.# http://10.10.3.142:9200
{
  "name" : "localhost.localdomain",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "O5M5rlFaQAW_RaEAxcpl8Q",
  "version" : {
    "number" : "8.15.2",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "98adf7bf6bb69b66ab95b761c9e5aadb0bb059a3",
    "build_date" : "2024-09-19T10:06:03.564235954Z",
    "build_snapshot" : false,
    "lucene_version" : "9.11.1",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}

```

Note: If you enabled SSL, please use the `curl --tlsv1.2 -k -s -XGET --user <username:password> https://<IP address>:<port>` command instead.

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. <code>{ } [] : " , ' < > @ & ^ % \</code> and spaces
Password	Admin1.#	Specify the admin password used to log in to Elasticsearch.

Parameter	Default Value	Description
		Note: The password cannot be empty, and it cannot start with ! or #.
DataPath	<code>/var/lib/elasticsearch</code>	<p>Specify the storage path for all data files of Elasticsearch. It is recommended to keep the default path.</p> <p>Note: If you want to modify it, don't use an existing directory.</p> <p>Note: Make sure the directory has more than 100GB free space to save all the data files.</p> <p>Tip: You can run the <code>df -h</code> command to check which directory has been mounted to a large disk.</p>
LogPath	<code>/var/log/elasticsearch</code>	<p>Specify the storage path for all log files of Elasticsearch.</p> <p>Note: It is recommended to keep the default path as it is. If you want to modify it, don't use an existing directory.</p> <p>Note: Make sure the directory has more than 50GB free space to save all the log files.</p>
BindIp	<code>0.0.0.0</code>	<p>Enter the IP address of the network card you want to use for the Elasticsearch.</p> <p>Note: Modify the value only if you have multiple network cards on this machine.</p>
Port	<code>9200</code>	Specify the port number that Elasticsearch service listens to.
CPULimit	<code>35%</code>	<p>Specify the maximum CPU utilization that can be consumed by Elasticsearch.</p> <p>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.</p>
MemoryLimit	<code>25%</code>	<p>Specify the maximum memory capacity of the machine that can be consumed by Elasticsearch.</p> <p>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%.</p> <p>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.</p>
UseSSL	<code>no</code>	<p>Set whether to enable the encrypted connections to Elasticsearch by using SSL.</p> <p>For detailed requirements of SSL certificates and keys, refer to SSL Certificate Requirements.</p>
Certificate	<code>/opt/cert.pem</code>	<p>Specify the name of the SSL certificate file containing the public key.</p> <p>Note: It is required only if UseSSL is enabled.</p>

Parameter	Default Value	Description
PrivateKey	<code>/opt/key.pem</code>	Specify the name of the SSL private key file. Note: It is required only if UseSSL is enabled.
CertAuth	<code>/opt/cacert.pem</code>	Specify the name of the SSL certificate chain or intermediate certificate (class 2 or class 3 certificate). Note: It is required only if UseSSL is enabled.
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	<code>10.10.2.34,10.10.2.35,10.10.2.36</code>	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.

3.4. Installing License Agent on Linux

1. Log in to the Linux server as the **root** or **sudo** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp12.1**.
3. Run the `cd /opt/netbraintemp12.1` command to navigate to the **/opt/netbraintemp12.1** directory.
4. Download the installation package.
 - **Option 1:** If the Linux server has no access to the Internet, obtain the **netbrain-licenseagent-linux-x86_64-rhel-12.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp12.1** 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/netbraintemp12.1** directory to directly download the file from NetBrain official download site.

Note: Contact [NetBrain Support Team](#) to get the download link. 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-12.1.tar.gz` command under the **/opt/netbraintemp12.1** directory to extract installation files.

```
[root@localhost netbraintemp12.1]# tar -zxvf netbrain-licenseagent-linux-x86_64-rhel-12.1.tar.gz
License/
License/include/
License/include/check.sh
License/include/ini.sh
...
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=/opt/cert.pem
PrivateKey=/opt/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: Creating installation log file **SUCCEEDED**

INFO: Dependent packages:

INFO: Component Name: License Agent

INFO: RPM name: netbrainlicense

INFO: Preprocessing **SUCCEEDED**.

...

INFO: Installing /opt/netbraintemp11.1b/License/sources/netbrainlicense-12.1.-el.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-12.1.0-el #####

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.
```

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	/opt/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.
PrivateKey	/opt/key.pem	Specify the storage path and name of the SSL private key file. Note: It is required only if UseSSL is enabled.

Parameter	Default Value	Description
LogPath	/var/log/netbrain/netbrainlicense	Specify the storage path for all License Agent log files.

3.5. 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.

Installing Redis on Linux

- Log in to the Linux server as the **root** or **sudo** user.
 - Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp12.1**.
 - Run the `cd /opt/netbraintemp12.1` command to navigate to the **/opt/netbraintemp12.1** directory.
 - Download the installation package.
 - Option 1:** If the Linux server has no access to the Internet, obtain the **redis-linux-x86_64-rhel-7.2.7-12.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp12.1** 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/netbraintemp12.1** directory to directly download the **redis-linux-x86_64-rhel-7.2.7-12.1.tar.gz** file from NetBrain official download site.
- Note:** Contact [NetBrain Support Team](#) to get the download link. 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.
- Run the `tar -zxvf redis-linux-x86_64-rhel-7.2.7-12.1.tar.gz` command under the **/opt/netbraintemp12.1** directory to extract installation files.

```
[root@localhost netbraintemp12.1]# tar -zxvf redis-linux-x86_64-rhel-7.2.7-12.1.tar.gz
redis/
redis/config/
...
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

# Use Fully Qualified Domain Name (FQDN).
FQDN=127.0.0.1

# 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=
# 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
# Start the redis sentinel service on Sentinel port. Default port is 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 value 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=/opt/cert.pem
PrivateKey=/opt/key.pem
CertAuth=/opt/cacert.pem

# 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 Redis if it has not yet been installed.
DisableSM=0

```

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: Starting to check crontab
INFO: Component Name: Redis
INFO: RPM name: redis
INFO: Service name: redis
INFO: RPM package list: redis-7.2.7-1.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. <code>{ } [] : " , ' < > @ & ^ % \</code> 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.
BindIP	0.0.0.0	Specify the IP address of Redis.

Parameter	Default Value	Description
		Note: Don't use 127.0.0.1 . Note: Select either to specify the actual value of BindIp or the FQDN for Redis by setting BindIp as 0.0.0.0 .
FQDN	127.0.0.1	Specify the fully qualified domain name (FQDN) for Redis.
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.
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	/opt/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	/opt/key.pem	Specify the name of SSL private key file. Note: It is required only if UseSSL is enabled.
CertAuth	/opt/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.

3.6. 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.

Installing RabbitMQ on Linux

1. Log in to the Linux server as the **root** or **sudo** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the installation package. For example, **netbraintemp12.1**.
3. Run the `cd /opt/netbraintemp12.1` command to navigate to the **/opt/netbraintemp12.1** 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-3.13.7-12.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp12.1** 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/netbraintemp12.1** directory to directly download the **rabbitmq-linux-x86_64-rhel-3.13.7-12.1.tar.gz** file from NetBrain official download site.

Note: Contact [NetBrain Support Team](#) to get the download link. 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-3.13.7-12.1.tar.gz` command under the **/opt/netbraintemp12.1** directory to extract installation files.

```
[root@localhost netbraintemp12.1]# tar -zxvf rabbitmq-linux-x86_64-rhel-3.13.7-12.1.tar.gz
rabbitmq/
rabbitmq/others/
rabbitmq/others/uninstall.sh
...
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@Rocky 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
# 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
# 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=/opt/cert.pem
PrivateKey=/opt/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

# To disable the Service Monitor Agent Component check, set the 'DisableSM=1'
# The default value of 'DisableSM' is 0 which means Service Monitor Agent
# should be installed before installing RabbitMQ otherwise it will stop the installation.
DisableSM=0
```

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: 2025-04-15 14-13-35.976: Creating installation log file SUCCEEDED
INFO: Selinux-policy version: 3.14.3
INFO: Component Name: RabbitMQ
```

```

INFO: RPM name: rabbitmq-server
INFO: Service name: rabbitmq-server
INFO: RPM package list: erlang-26.2.5.4-1.el8.x86_64.rpm rabbitmq-server-26.2.5.4-1.el8.noarch.rpm
INFO: Installation path: /usr/lib/rabbitmq/
INFO: Config path: /etc/rabbitmq/
INFO: Preprocessing SUCCEEDED
...
Preparing... #####
Updating / installing...
rabbitmq-server-3.13.7-1.el8 #####
INFO: Official rpm package installing SUCCEEDED
INFO: Configuration parameters updating SUCCEEDED
INFO: Permission setting SUCCEEDED
Created symlink from /etc/systemd/system/multi-user.target.wants/rabbitmq-server.service to /usr/lib/systemd/system/rabbitmq-server.service.
rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-07-13 16:04:46 EDT; 8ms ago
     Main PID: 53927 (beam.smp)
       Status: "Initialized"
      Memory: 70.8M (limit: 15.5G)
   ...
INFO: Backing up uninstall.sh SUCCEEDED
INFO: Successfully installed RabbitMQ

```

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

```

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

```

Parameters

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

Parameter	Default Value	Description
Username	admin	Specify the admin username used to connect to RabbitMQ. Note: The username and password cannot contain any of the following special characters, and its length cannot exceed 64 characters. { } [] : " , ' < > @ & ^ % \ and spaces
Password	Admin1.#	Specify the admin password used to connect to RabbitMQ.

Parameter	Default Value	Description
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.
BindIP	0.0.0.0	Specify the IP address of RabbitMQ. Note: Don't use 127.0.0.1 . Note: Select either to specify the actual value of BindIp or set it as 0.0.0.0 .
ResourceLimit	no	Set whether to limit the system resource usage for RabbitMQ.
CPULimit	100%	Specify the maximum CPU utilization of the machine that can be consumed by RabbitMQ.
MemoryLimit	100%	Specify the maximum memory capacity of the machine that can be consumed by RabbitMQ.
UseSSL	no	Set whether to enable the encrypted connections to RabbitMQ by using SSL. Tip: If UseSSL is set to yes , you can follow the steps below to modify the RabbitMQ Plugin config file after the service monitor is installed. 1) Run the <code>vi /etc/netbrain/nbagent/check/rabbitmq.yaml</code> command to open the RabbitMQ Plugin config file. 2) Set the ssl value to true and save the changes. For how to modify the configuration file, see Editing a File with VI Editor for more details. <pre>[root@localhost check]# vi rabbitmq.yaml init_config: instances: - name: default managementPort: 15672, checkAvailableIntervalSeconds: 300 ssl: true collectQueues: equal: [] startWith: ['FullTextSearch', 'TaskManager', 'event_callback', 'RMClientCallbac</pre>

Parameter	Default Value	Description
		<pre>k', 'ETL_Task'] endWith: ['IndexDriver']</pre>
Certificate	<code>/opt/cert.pem</code>	Specify the storage path for all the certificates and key files used for SSL authentication. Note: It is required only if UseSSL is enabled.
PrivateKey	<code>/opt/key.pem</code>	Specify the name of SSL private key file. Note: It is required only if UseSSL is enabled.
Port	<code>5672</code>	Specify the port number that RabbitMQ service listens to.
LogPath	<code>/var/log/rabbitmq</code>	Specify the directory to save logs of RabbitMQ.

3.7. Installing Service Monitor Agent on Windows

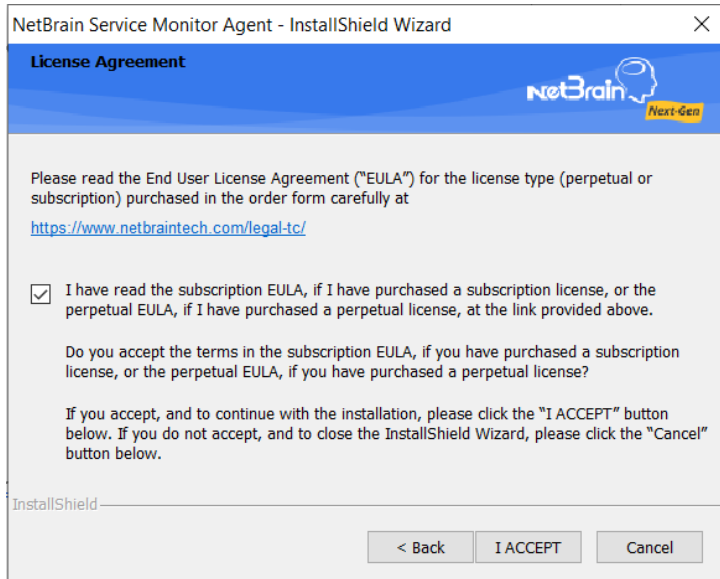
Complete the following steps with administrative privileges.

1. Download the **netbrain-servicemonitoragent-windows-x86_64-12.1.zip** file and save it in your local folder.

Tip: Contact [NetBrain Support Team](#) to get the download link.

2. Extract installation files from the **netbrain-servicemonitoragent-windows-x86_64-12.1.zip** file.
3. Right-click the **netbrain-servicemonitoragent-windows-x86_64-12.1.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**.



The screenshot shows the 'License Agreement' window of the NetBrain Service Monitor Agent - InstallShield Wizard. The window has a blue header with the NetBrain logo and 'Next-Gen' text. The main content area contains the following text:

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

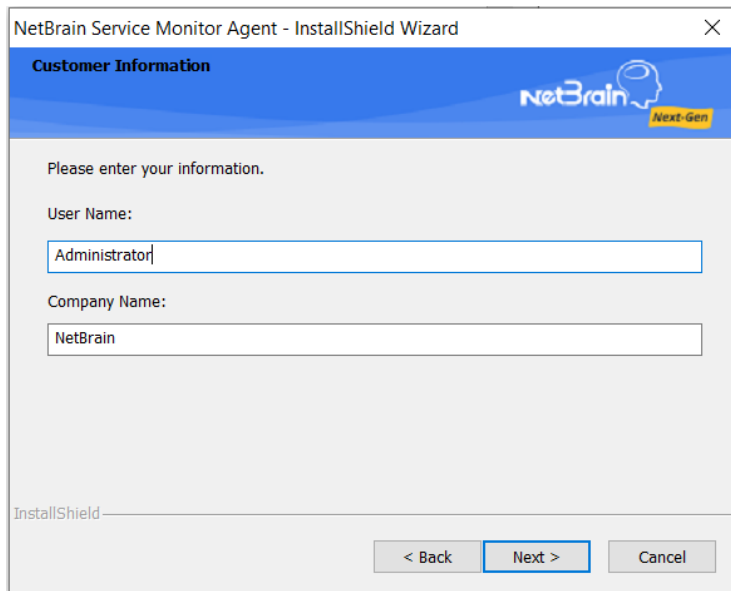
☒ I have read the subscription EULA, if I have purchased a subscription license, or the perpetual EULA, if I have purchased a perpetual license, at the link provided above.

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

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

At the bottom, there are three buttons: '< Back', 'I ACCEPT', and 'Cancel'. The 'I ACCEPT' button is highlighted.

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



The screenshot shows the 'Customer Information' window of the NetBrain Service Monitor Agent - InstallShield Wizard. The window has a blue header with the NetBrain logo and 'Next-Gen' text. The main content area contains the following text:

Please enter your information.

User Name:

Company Name:

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted.

- 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**.

The screenshot shows a window titled "NetBrain Service Monitor Agent - InstallShield Wizard" with a close button in the top right corner. The window has a blue header bar with the "NetBrain Next-Gen" logo. Below the header, the text reads: "Please input the information to connect with Web API Server. (Note: please ensure this key must be the same as the API key created on Web API server.)". There are three input fields, each preceded by a red asterisk: "API URL:" with the value "http://10.10.3.141/ServicesAPI", "API Key:" with masked characters, and "Re-enter the Key:" with masked characters. At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

- **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**.

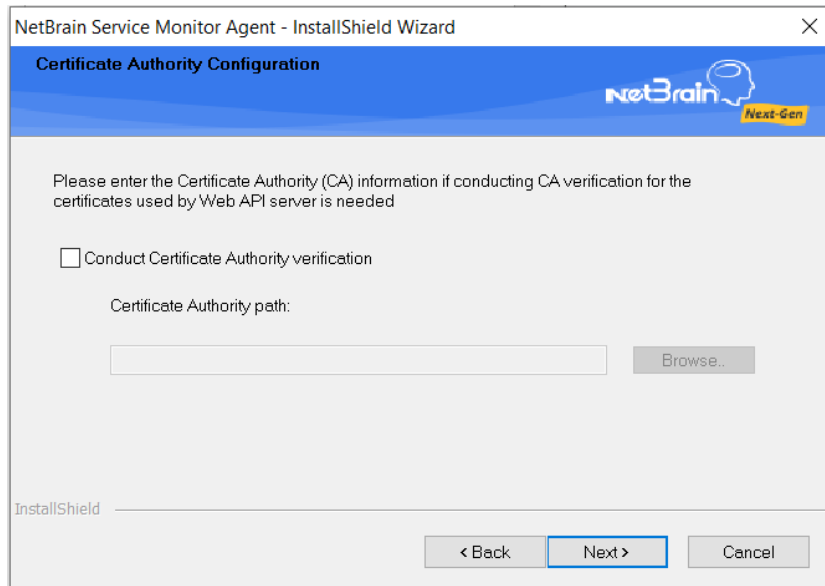
Note: If SSL will be enabled with https binding created for the system website in IIS Manager, use **https** in the URL. Besides, if you want to authenticate the Certificate Authority of the SSL certificate used by the system website (to be completed in the next step), the hostname must be specified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

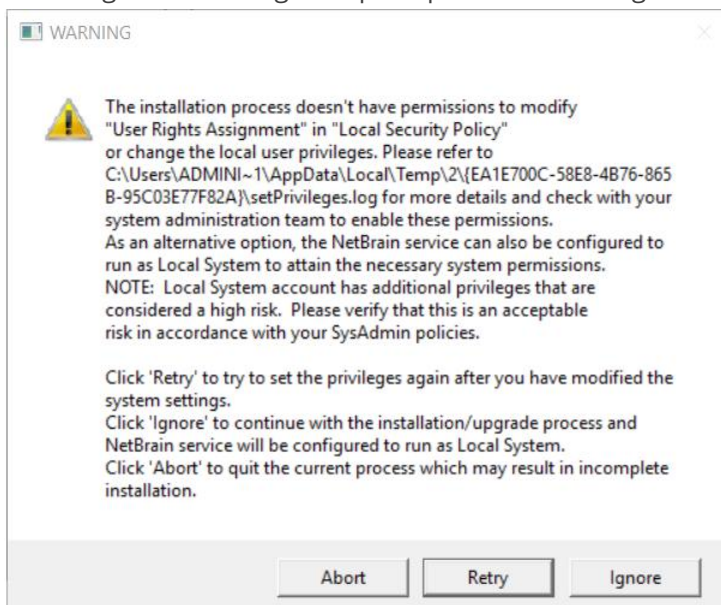
- 7) This step is required only if **https** is used in **API URL**. Configure whether to authenticate the Certificate Authority (CA) of the certificates used to enable SSL for NetBrain website in IIS Manager, and then click

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**.
 - 8) Review the summary of the installation information and click **Install**.
- (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 **Ignore** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System.

- If you have security concerns, click **Abort** to quit the installation/upgrade process.
- Click **Retry** after you have modified the system settings.

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 **Abort**, 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.

3.8. 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: Don't install multiple Web API Servers at the same time; install them one after another, ensuring each installation is successful before proceeding to the next. Otherwise, it will cause the database initialization failure.

Note: Ensure the port 9070 is open and available on the machine where the Web API Service is installed.

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

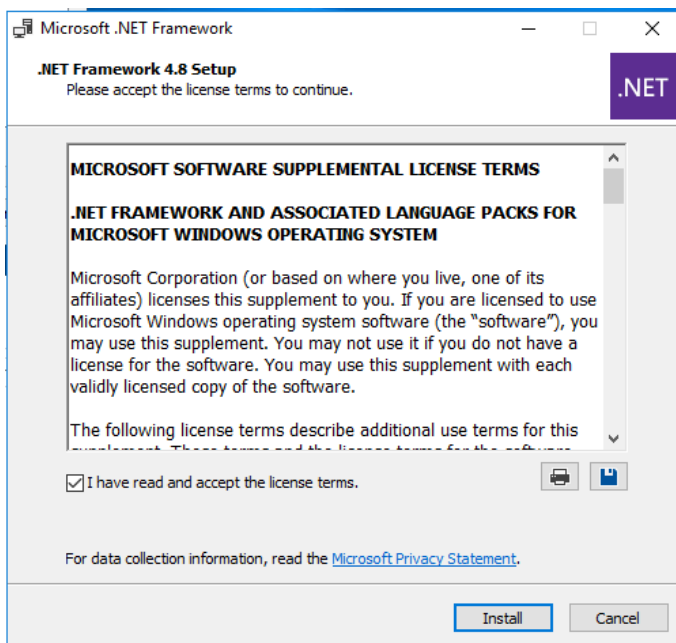
1. Download the **netbrain-core-windows-x86_64-12.1.zip** file and save it in your local folder.

Tip: Contact [NetBrain Support Team](#) to get the download link.

2. Extract installation files from the **netbrain-core-windows-x86_64-12.1.zip** file.
3. Right-click the **netbrain-core-windows-x86_64-12.1.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 and Microsoft Visual C++ 2022 Redistributable Package 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).

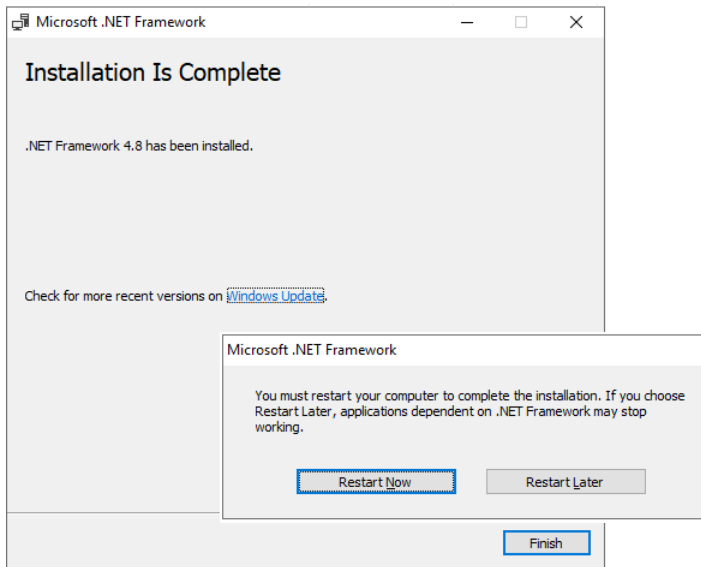
Note: Make sure the Windows update is of the latest.

- 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.



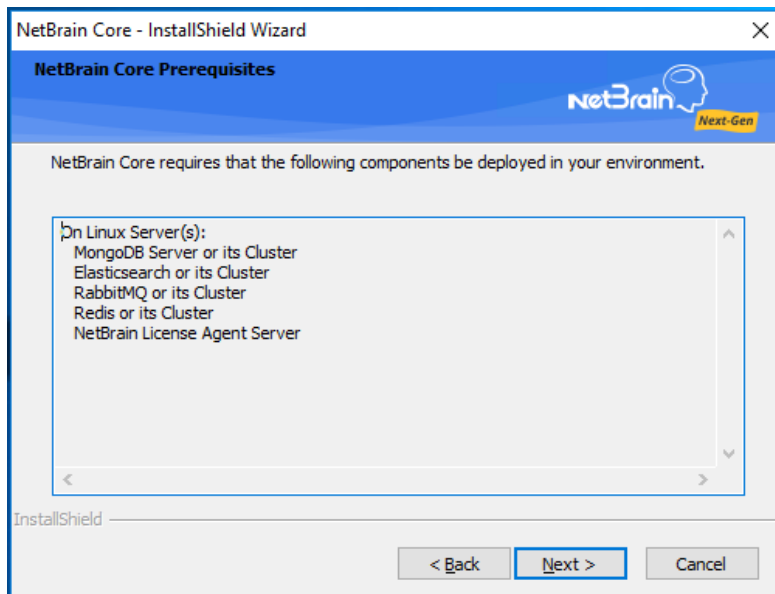
Note: Some running applications must be closed during the installation of .NET Framework 4.8, such as Server Manager.

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



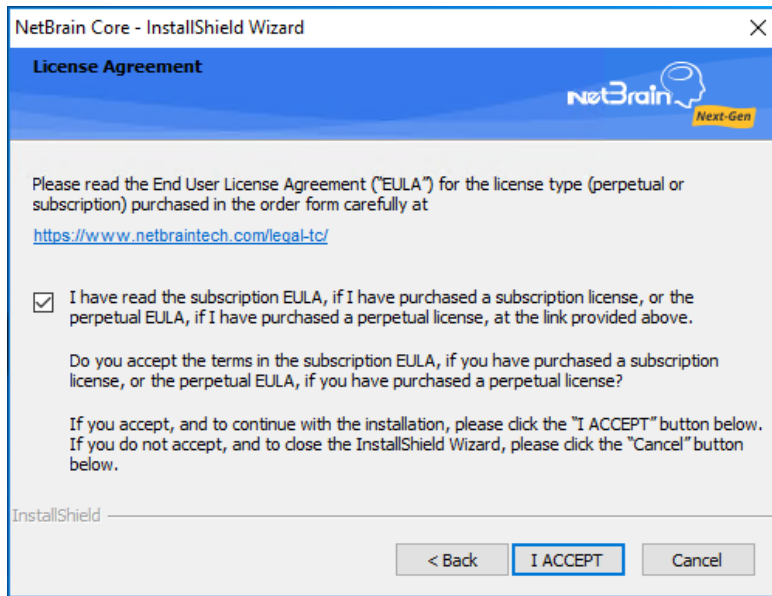
Note: The interface above may not appear if the .NET Framework has never been installed on the server. In such case, it is still highly recommended to reboot the server after the installation of the .NET Framework completes.

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

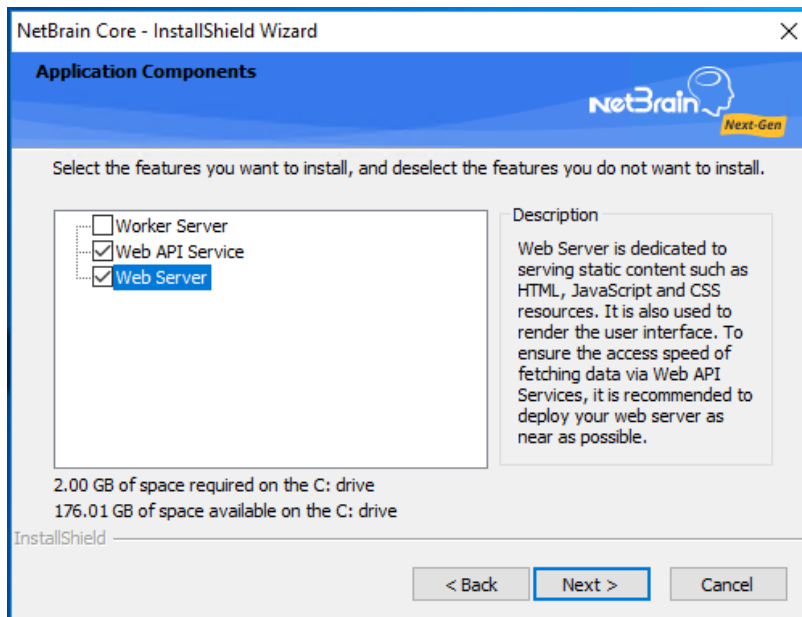


- 4) On the System Configuration page, review the system configuration summary and click **Next**.

- 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**.

NetBrain Core - InstallShield Wizard

MongoDB Server Connection

Please input the information of MongoDB Server.

★ Address: 10.10.3.142:27017

Format: <Address>:<Port>. For example: 10.10.10.10:27017. Use the Ctrl+Enter keys to add all the servers for a replica set. The first entry should be the primary server address; the last entry should be the arbiter address.

★ User Name: admin

★ Password: ●●●●●●●●

★ Replica Set Name: rs

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

Use SSL: ☐ Validation Timeout (seconds): 30

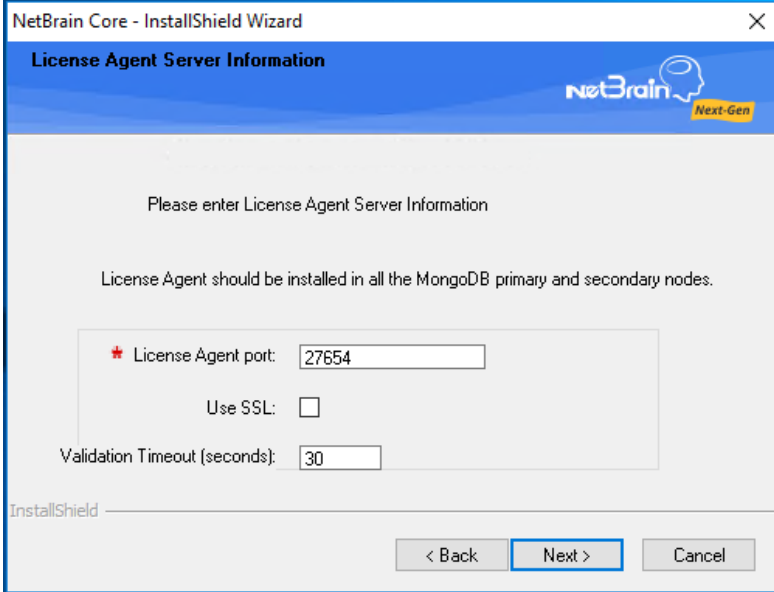
< Back Next > Cancel

- **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.

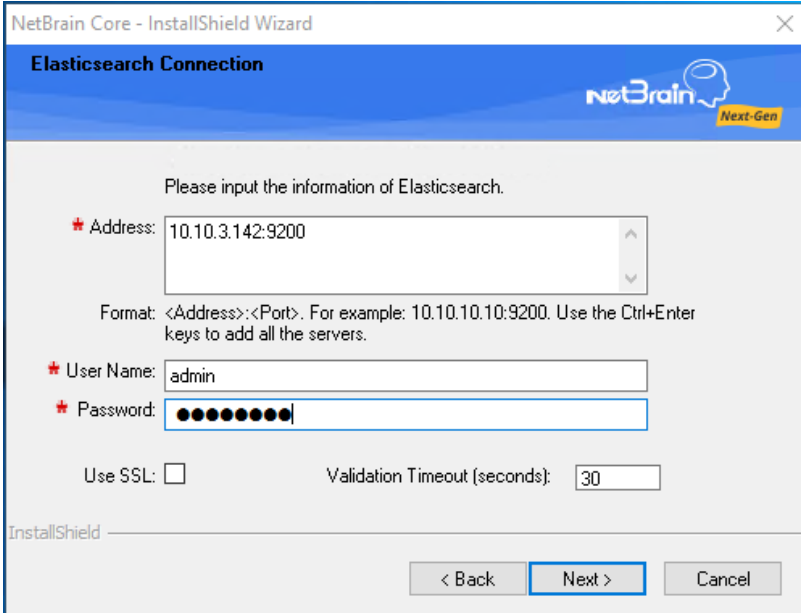
- 10) On the License Agent Server Information page, enter the following information to connect to License Agent, and then click **Next**.



The screenshot shows the 'License Agent Server Information' window of the NetBrain Core InstallShield Wizard. The window has a blue header with the NetBrain logo and 'Next-Gen' text. The main area is white with the title 'License Agent Server Information'. Below the title, it says 'Please enter License Agent Server Information' and 'License Agent should be installed in all the MongoDB primary and secondary nodes.' There are three input fields: 'License Agent port' with the value '27654', 'Use SSL' with an unchecked checkbox, and 'Validation Timeout (seconds)' with the value '30'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- **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**.



The screenshot shows the 'Elasticsearch Connection' window of the NetBrain Core InstallShield Wizard. The window has a blue header with the NetBrain logo and 'Next-Gen' text. The main area is white with the title 'Elasticsearch Connection'. Below the title, it says 'Please input the information of Elasticsearch.' There are four input fields: 'Address' with the value '10.10.3.142:9200', 'User Name' with the value 'admin', 'Password' with masked characters, and 'Validation Timeout (seconds)' with the value '30'. There is also an unchecked checkbox for 'Use SSL'. Below the 'Address' field, there is a note: 'Format: <Address>:<Port>. For example: 10.10.10.10:9200. Use the Ctrl+Enter keys to add all the servers.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- **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**.

The screenshot shows a window titled "NetBrain Core - InstallShield Wizard" with a sub-header "RabbitMQ Connection". The NetBrain logo is in the top right. The main text says "Please input the information of RabbitMQ." Below this are several input fields: "Address" with the value "10.10.3.142", "User Name" with "admin", "Password" with masked characters, and "Port Number" with "5672". There is a "Format: <Address>." note with an example. At the bottom, there is a "Use SSL:" checkbox (unchecked) and a "Validation Timeout (seconds):" field with "30". At the very bottom are three buttons: "< Back", "Next >", and "Cancel".

- **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**.

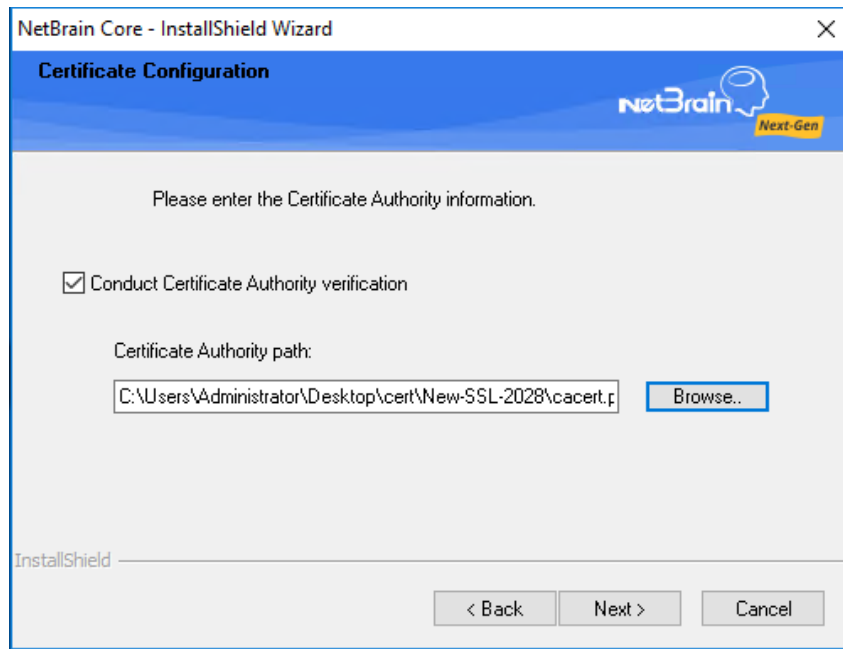
- **Redis Address** — enter the IP address of Redis.

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**.

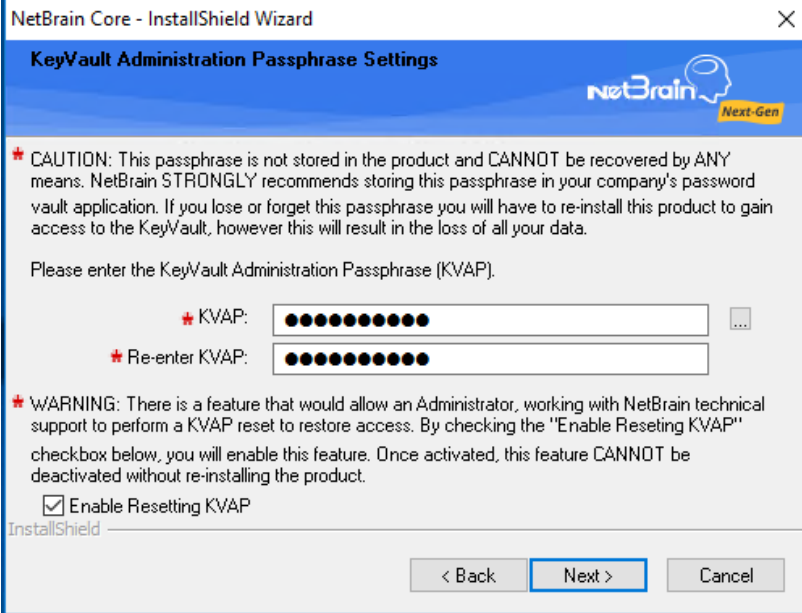
Note: Only the certificate in **Base-64 encoded X.509 PEM** format is supported.

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**.



The screenshot shows the 'KeyVault Administration Passphrase Settings' window. It includes a caution about the passphrase not being recoverable, a warning about the 'Enable Resetting KVAP' feature, and two password input fields. The 'Enable Resetting KVAP' checkbox is checked. The 'Next >' button is highlighted.

NetBrain Core - InstallShield Wizard

KeyVault Administration Passphrase Settings

CAUTION: This passphrase is not stored in the product and CANNOT be recovered by ANY means. NetBrain STRONGLY recommends storing this passphrase in your company's password vault application. If you lose or forget this passphrase you will have to re-install this product to gain access to the KeyVault, however this will result in the loss of all your data.

Please enter the KeyVault Administration Passphrase (KVAP).

* KVAP: [password field]

* Re-enter KVAP: [password field]

* WARNING: There is a feature that would allow an Administrator, working with NetBrain technical support to perform a KVAP reset to restore access. By checking the "Enable Resetting KVAP" checkbox below, you will enable this feature. Once activated, this feature CANNOT be deactivated without re-installing the product.

☒ Enable Resetting KVAP

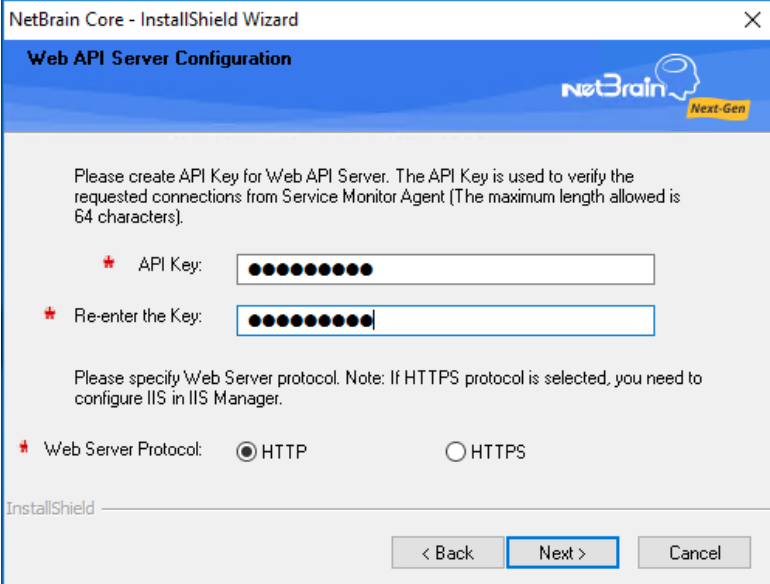
InstallShield

< Back **Next >** Cancel

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

Note: Keep notes of the passphrase because it is required when you scale up or upgrade 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**.



The screenshot shows the 'Web API Server Configuration' window. It prompts the user to create an API key (max 64 characters) and re-enter it. It also allows selecting the Web Server Protocol (HTTP or HTTPS). The 'Next >' button is highlighted.

NetBrain Core - InstallShield Wizard

Web API Server Configuration

Please create API Key for Web API Server. The API Key is used to verify the requested connections from Service Monitor Agent (The maximum length allowed is 64 characters).

* API Key: [password field]

* Re-enter the Key: [password field]

Please specify Web Server protocol. Note: If HTTPS protocol is selected, you need to configure IIS in IIS Manager.

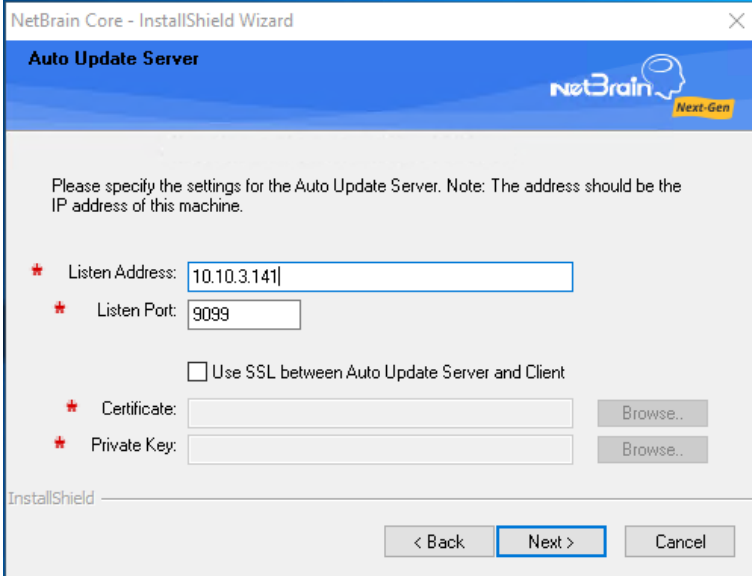
* Web Server Protocol: ☒ HTTP ☐ HTTPS

InstallShield

< Back **Next >** Cancel

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.

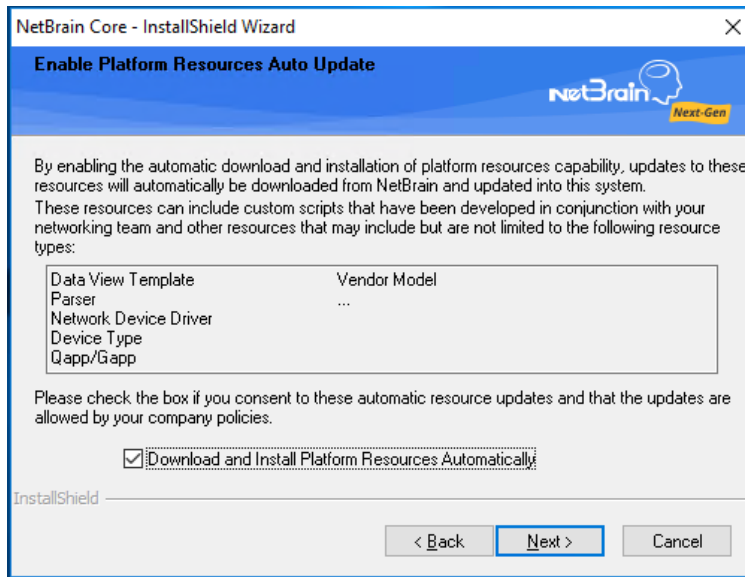


The screenshot shows the 'Auto Update Server' configuration window in the NetBrain Core - InstallShield Wizard. The window has a blue header with the NetBrain logo and 'Next-Gen' text. Below the header, a note states: 'Please specify the settings for the Auto Update Server. Note: The address should be the IP address of this machine.' The configuration fields include: 'Listen Address' with the value '10.10.3.141', 'Listen Port' with the value '9099', and an unchecked checkbox for 'Use SSL between Auto Update Server and Client'. Below these are fields for 'Certificate' and 'Private Key', each with a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

- **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.
 - **Certificate** — 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**.

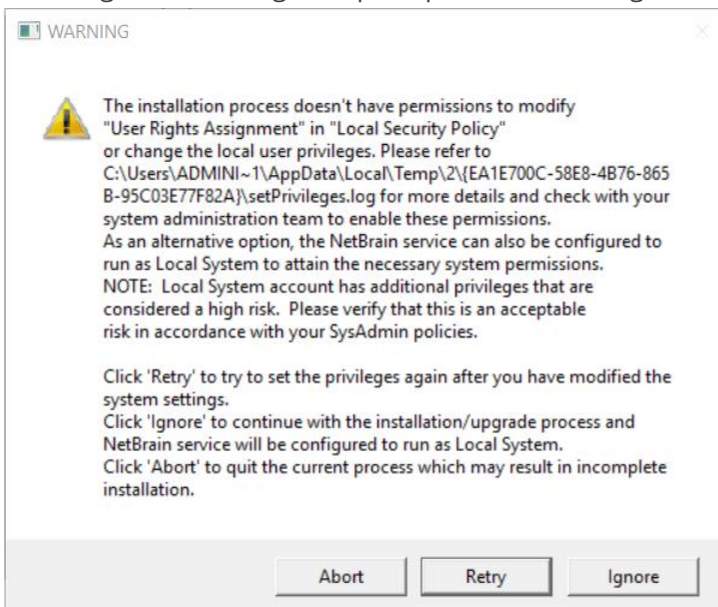
Note: The Listen Address must be the local server's IP address which can be reached from other NetBrain servers including Front Server.

18) On the Enable Platform Resources Auto Update page, if you want these resources to be downloaded automatically, check the Download and Install Platform Resources Automatically box. Click **Next**.



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

- (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 **Ignore** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System.
- If you have security concerns, click **Abort** to quit the installation/upgrade process.
- Click **Retry** after you have modified the system settings.

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 **Abort**, 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.

3.9. 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: 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-core-windows-x86_64-12.1.zip** file and save it in your local folder.

Tip: Contact [NetBrain Support Team](#) to get the download link.

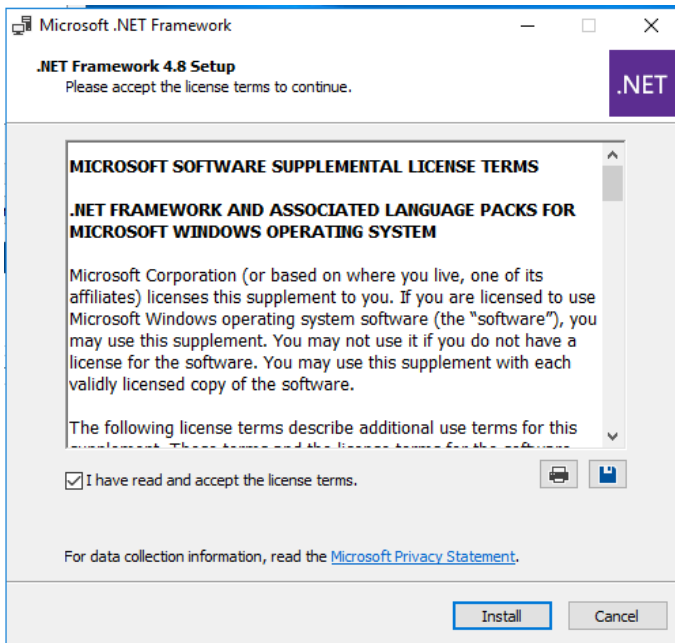
2. Extract installation files from the **netbrain-core-windows-x86_64-12.1.zip** file.
3. Right-click the **netbrain-core-windows-x86_64-12.1.exe** file, and then select **Run as administrator** to launch the Installation Wizard.

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; if it has been installed, the wizard will directly go to step 2).

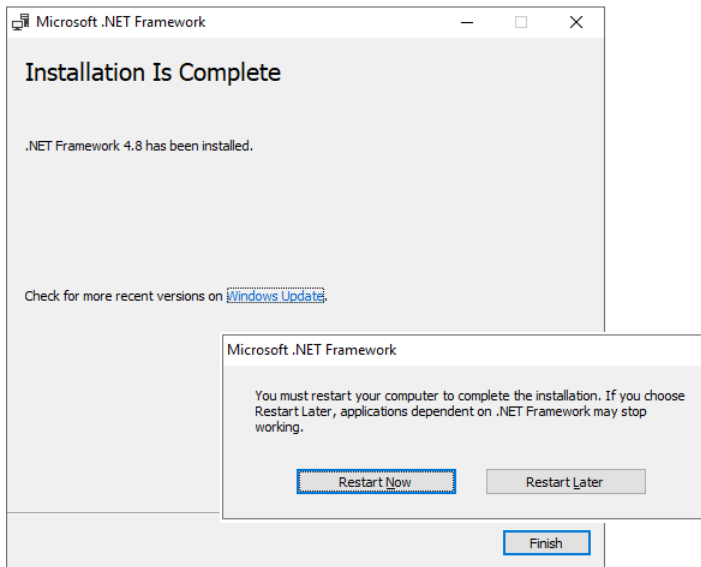
Note: Make sure the Windows update is of the latest.

- 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.

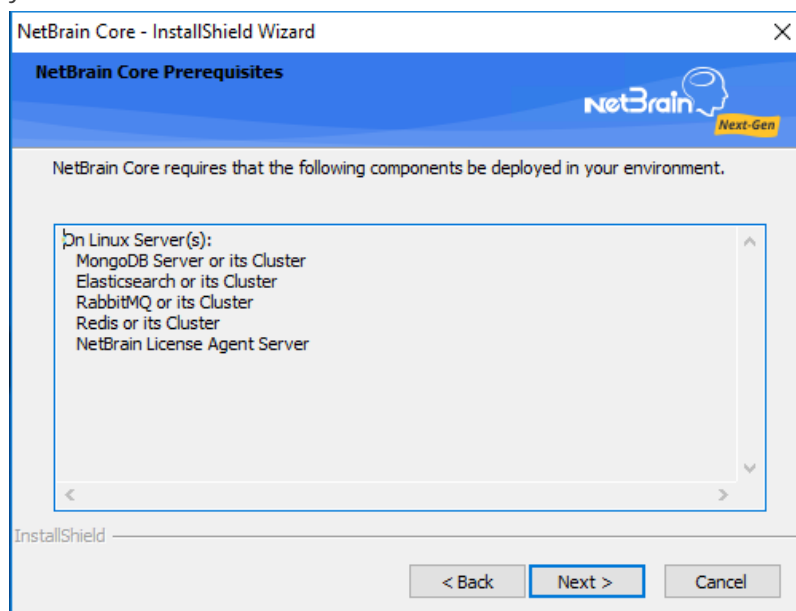
- c) You must click **Restart Now** to restart the machine immediately. Otherwise, the upgrade will fail due to the failure of upgrading the new .Net Framework. After the machine reboots, continue with step 2).



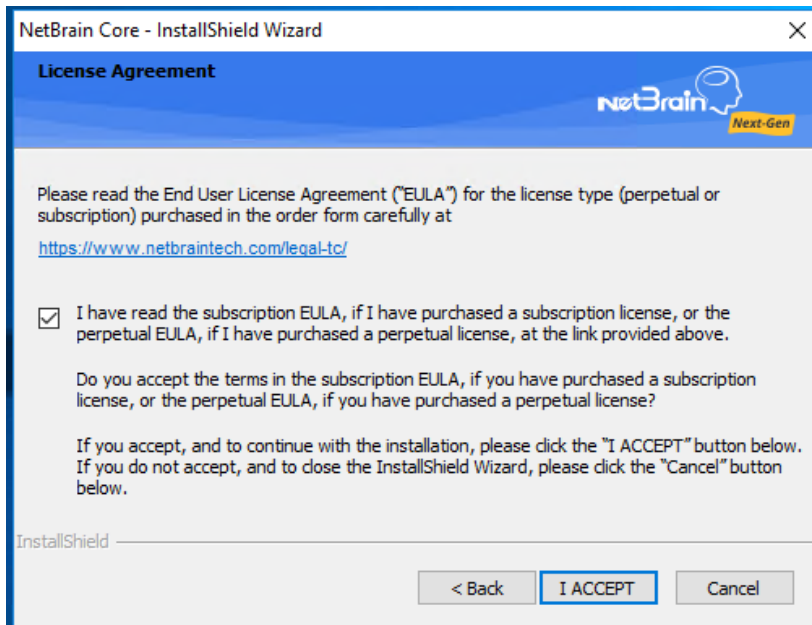
Note: The interface above may not appear if the .NET Framework has never been installed on the server. In such case, it is still highly recommended to reboot the server after the installation of the .NET Framework completes.

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.

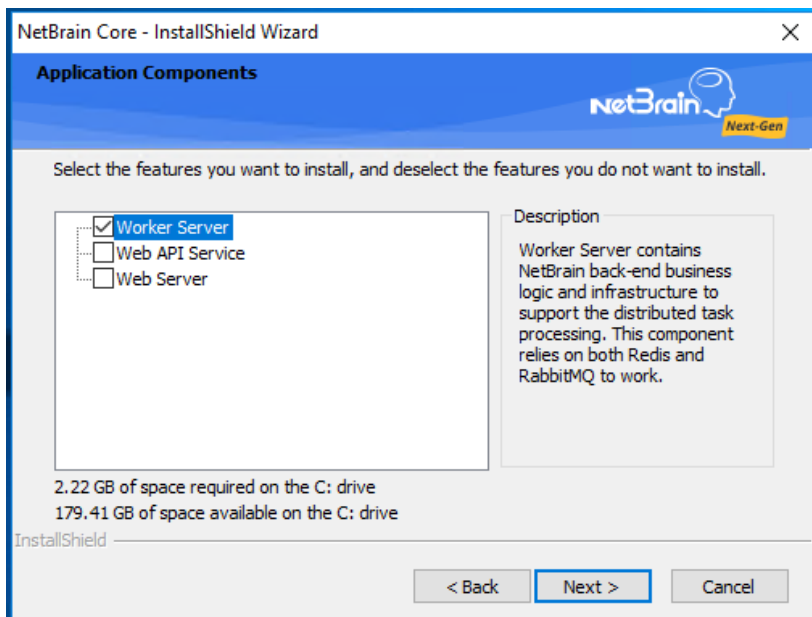
- 2) On the Welcome page, click **Next**.
- 3) On the NetBrain Core Prerequisites page, view the Linux components that must be deployed beforehand in your environment and click **Next**.



- 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**.

NetBrain Core - InstallShield Wizard

MongoDB Server Connection

Please input the information of MongoDB Server.

* Address: 10.10.3.142:27017

Format: <Address>:<Port>. For example: 10.10.10.10:27017. Use the Ctrl+Enter keys to add all the servers for a replica set. The first entry should be the primary server address; the last entry should be the arbiter address.

* User Name: admin

* Password: ●●●●●●●●

* Replica Set Name: rs

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

Use SSL: ☐ Validation Timeout (seconds): 30

< Back Next > Cancel

- **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**.

NetBrain Core - InstallShield Wizard

Elasticsearch Connection

Please input the information of Elasticsearch.

* Address: 10.10.3.142:9200

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

* User Name: admin

* Password: ●●●●●●●●

Use SSL: ☐ Validation Timeout (seconds): 30

InstallShield

< Back Next > Cancel

- **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**.

The screenshot shows a window titled "NetBrain Core - InstallShield Wizard" with a "RabbitMQ Connection" header. The NetBrain logo is in the top right. The main area contains the text "Please input the information of RabbitMQ." followed by several fields: "Address" with the value "10.10.3.142", "User Name" with "admin", "Password" with masked characters, and "Port Number" with "5672". There is a "Format: <Address>. For example: 10.10.10.10. Use the Ctrl+Enter keys to add all the servers for a cluster." note. At the bottom, there is a "Use SSL:" checkbox (unchecked) and a "Validation Timeout (seconds):" field with "30". Navigation buttons "< Back", "Next >", and "Cancel" are at the bottom right.

- **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**.

NetBrain Core - InstallShield Wizard

Redis Connection

Please input the information for Redis.

☒ Standalone

Redis Address: 10.10.3.142

* Redis Port: 6379

☐ Redis Sentinels Note: Use the Ctrl+Enter keys to add all the addresses.

* Sentinel Address:

* Sentinel Port: 6380

* Password: [Masked]

Use SSL: ☐ Validation Timeout (seconds): 30

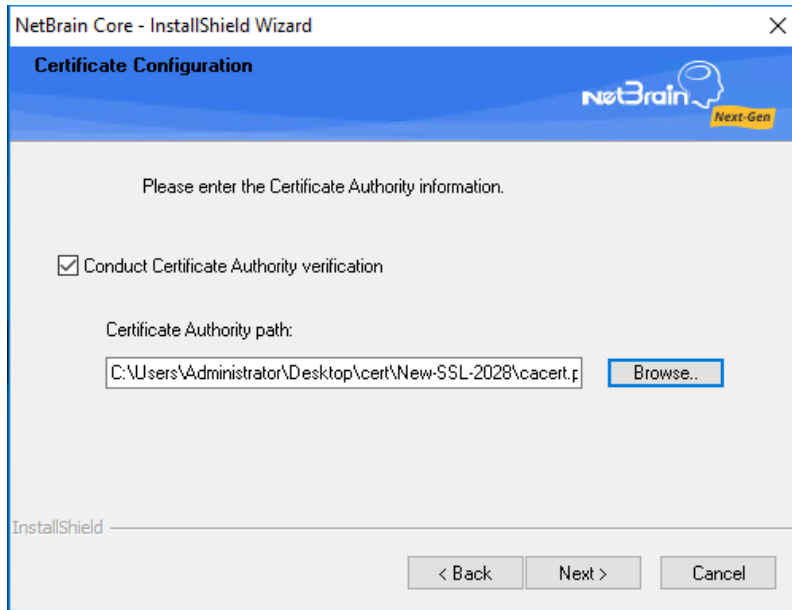
< Back Next > Cancel

- **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**.

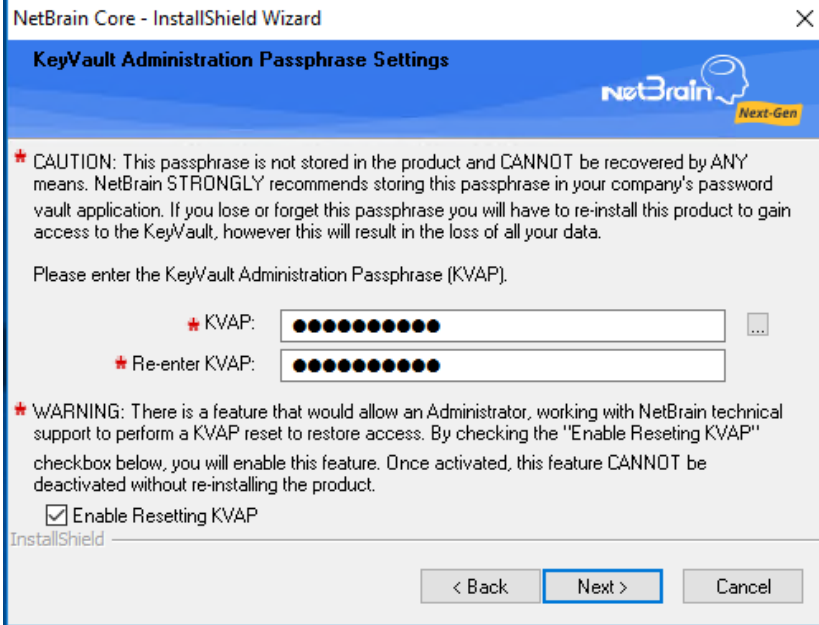
Note: Only the certificate in **Base-64 encoded X.509 PEM** format is supported.

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

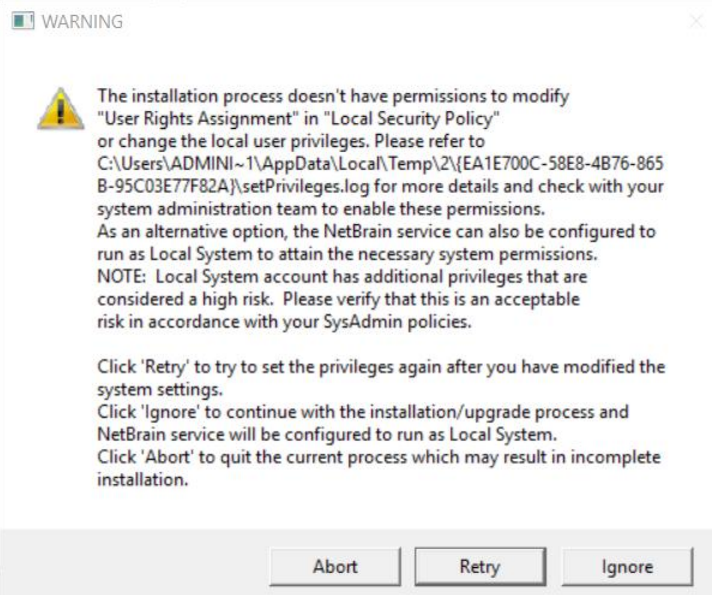
resetting. Click **Next**.



The screenshot shows a Windows-style dialog box titled "NetBrain Core - InstallShield Wizard". The main heading is "KeyVault Administration Passphrase Settings". It includes a caution message about the passphrase not being recoverable, followed by two input fields for "KVAP" and "Re-enter KVAP". Below these is a warning about the "Enable Resetting KVAP" checkbox, which is currently checked. At the bottom are buttons for "< Back", "Next >", and "Cancel".

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

- (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.



The screenshot shows a "WARNING" dialog box with a yellow warning icon. The text explains that the installation process lacks permissions to modify "User Rights Assignment" in "Local Security Policy" and provides a file path for more details. It offers two main options: "Retry" to attempt the installation after modifying permissions, or "Ignore" to continue with the installation where the NetBrain service will run as Local System. An "Abort" button is also present at the bottom.

- Click **Ignore** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System.
- If you have security concerns, click **Abort** to quit the installation/upgrade process.
- Click **Retry** after you have modified the system settings.

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 **Abort**, 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.

3.10. 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.

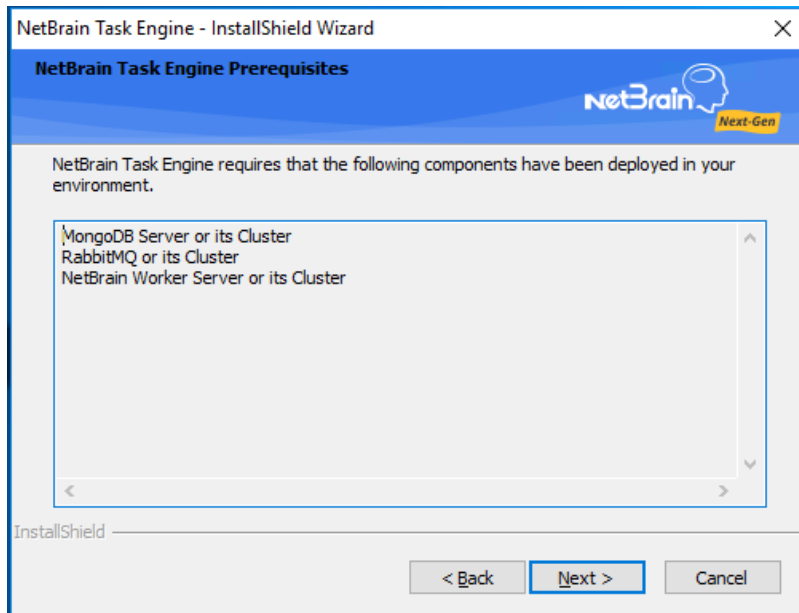
Complete the following steps with administrative privileges.

1. Download the **netbrain-taskengine-windows-x86_64-12.1.zip** file and save it in your local folder.

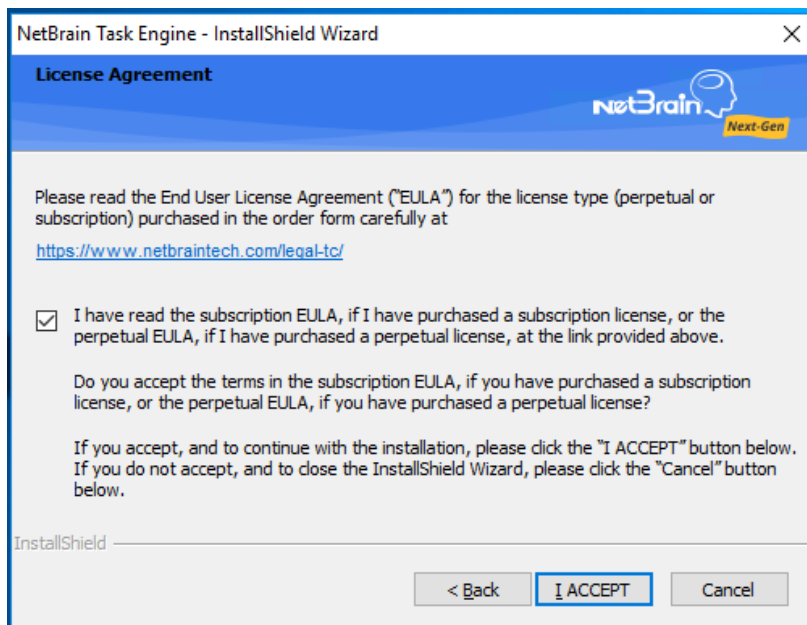
Tip: Contact [NetBrain Support Team](#) to get the download link.

2. Extract installation files from the **netbrain-taskengine-windows-x86_64-12.1.zip** file.
3. Right-click the **netbrain-taskengine-windows-x86_64-12.1.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**.

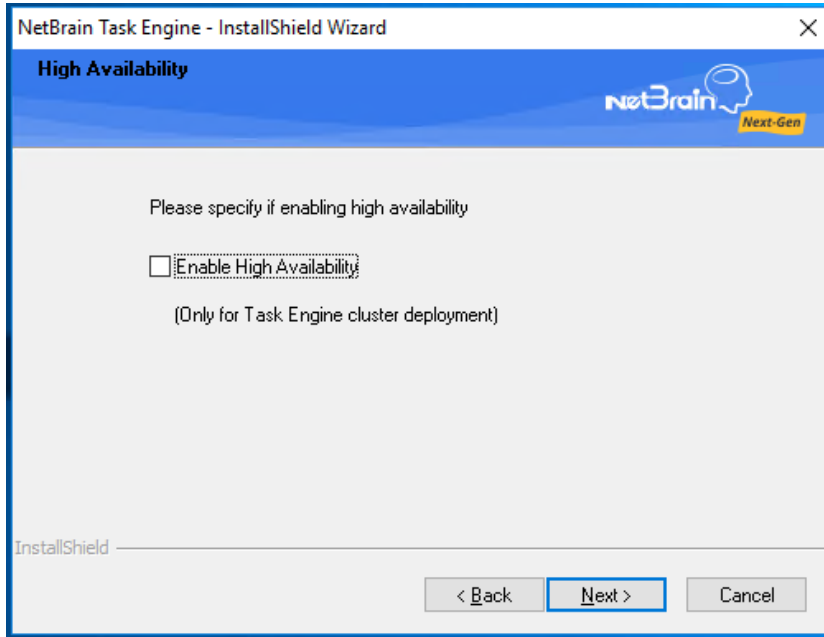


- 3) On the System Configuration page, review the system configuration summary and click **Next**.
- 4) On the License Agreement page, read the license agreements, select the **I have read the subscription EULA...** check box and then click **I ACCEPT**.

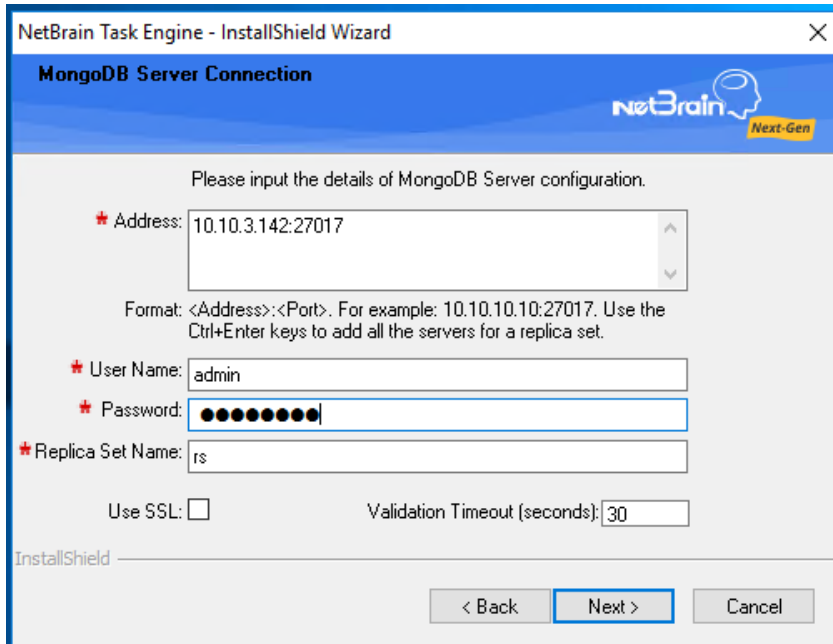


- 5) On the Customer Information page, enter your company name, and then click **Next**.
- 6) On the Destination Location page, click **Next** to install the Task Engine under the default directory **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.

- 7) On the High Availability page, leave **Enable High Availability** unchecked.

The screenshot shows the 'High Availability' page of the NetBrain Task Engine - InstallShield Wizard. The window has a blue header with the NetBrain logo and 'Next-Gen' tag. The main content area is light gray and contains the text 'Please specify if enabling high availability'. Below this is a checkbox labeled 'Enable High Availability' which is currently unchecked. Underneath the checkbox, it says '(Only for Task Engine cluster deployment)'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The title bar of the window reads 'NetBrain Task Engine - InstallShield Wizard'.

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

The screenshot shows the 'MongoDB Server Connection' page of the NetBrain Task Engine - InstallShield Wizard. The window has a blue header with the NetBrain logo and 'Next-Gen' tag. The main content area is light gray and contains the text 'Please input the details of MongoDB Server configuration.' Below this are several input fields: 'Address' with the value '10.10.3.142:27017', 'User Name' with the value 'admin', 'Password' with masked characters, and 'Replica Set Name' with the value 'rs'. There is also a 'Use SSL' checkbox which is unchecked, and a 'Validation Timeout (seconds)' field with the value '30'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The title bar of the window reads 'NetBrain Task Engine - InstallShield Wizard'.

- **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**.

NetBrain Task Engine - InstallShield Wizard

RabbitMQ Connection

Please input the details of the RabbitMQ configuration.

* Address: 10.10.3.142

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

* User Name: admin

* Password: ●●●●●●●●

* Port Number: 5672

Use SSL: ☐ Validation Timeout (seconds): 30

InstallShield

< Back Next > Cancel

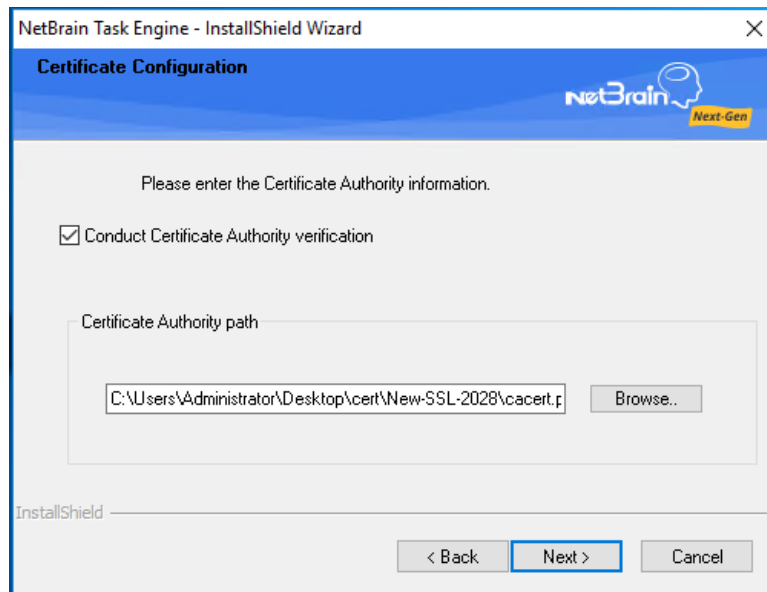
- **Address** — enter the IP address or resolvable FQDN of RabbitMQ.

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:

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

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

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

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

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

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

3.11. Installing Front Servers Controller on Windows

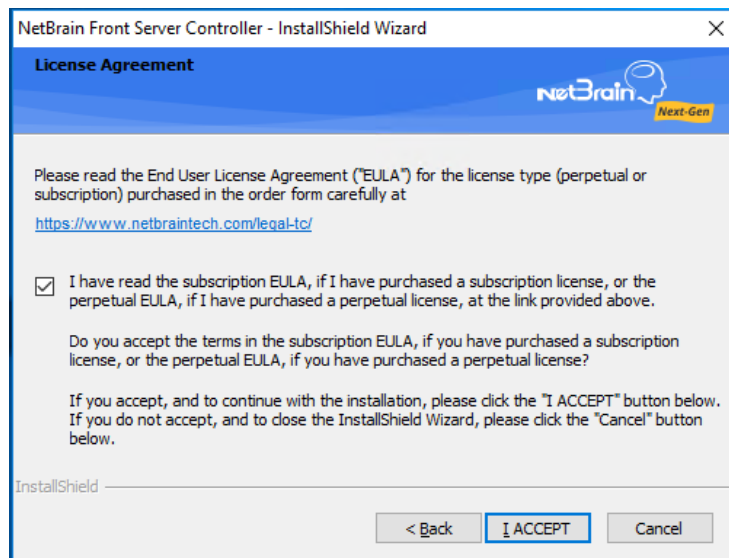
Note: Service Monitor Agent needs to be installed prior to installing Front Server Controller. Refer to [Installing Service Monitor Agent on Windows](#) for more detailed steps.

Complete the following steps with administrative privileges.

1. Download the **netbrain-frontservercontroller-windows-x86_64-12.1.zip** file and save it in your local folder.

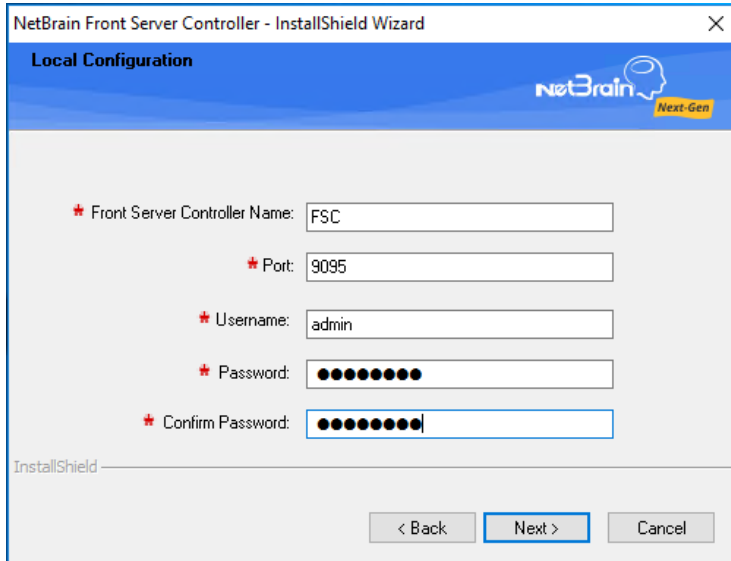
Tip: Contact [NetBrain Support Team](#) to get the download link.

2. Extract installation files from the **netbrain-frontservercontroller-windows-x86_64-12.1.zip** file.
3. Right-click the **netbrain-frontservercontroller-windows-x86_64-12.1.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**.

The screenshot shows a window titled "NetBrain Front Server Controller - InstallShield Wizard" with a sub-header "MongoDB Server Connection". The NetBrain logo is in the top right. The main text says "Please input the details of the MongoDB Server configuration." Below this are several fields: "Address" with the value "10.10.3.142:27017", "User Name" with "admin", "Password" with masked characters, and "Replica Set Name" with "rs". There is a "Format" note: "Format: <Address>:<Port>. For example: 10.10.10.10:27017. Use the Ctrl+Enter keys to add all the servers for a replica set." At the bottom, there is a "Use SSL" checkbox (unchecked) and a "Validation Timeout (seconds)" field with "30". Navigation buttons at the bottom are "< Back", "Next >", and "Cancel".

- **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**.

NetBrain Front Server Controller - InstallShield Wizard

RabbitMQ Connection

Please input the details of the RabbitMQ configuration.

* Address: 10.10.3.142

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

* User Name: admin

* Password: ●●●●●●●●

* Port Number: 5672

Use SSL: ☐ Validation Timeout (seconds): 30

< Back Next > Cancel

- **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**.

NetBrain Front Server Controller - InstallShield Wizard

Redis Connection

Please input the information for Redis.

☒ Standalone

* Redis Address: 10.10.3.142

* Redis Port: 6379

☐ Redis Sentinels Note: Use the Ctrl+Enter keys to add all the addresses.

* Sentinel Address:

* Sentinel Port: 6380

* Password: ●●●●●●●●

Use SSL: ☐ Validation Timeout (seconds): 30

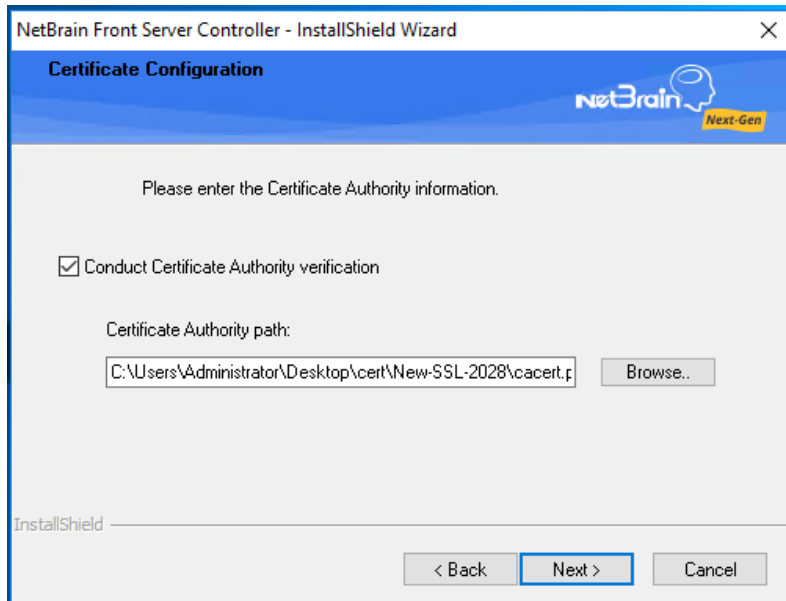
< Back Next > Cancel

- **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:

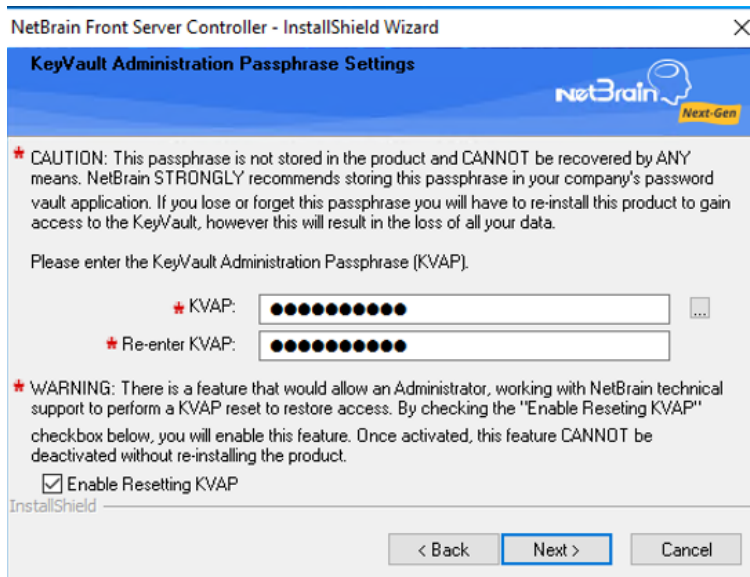
- a) Select the **Conduct Certificate Authority verification** check box.
- b) If the CA has not been installed on this machine, click **Browse** to import the CA certificate file, for example, **ca.pem**.

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.

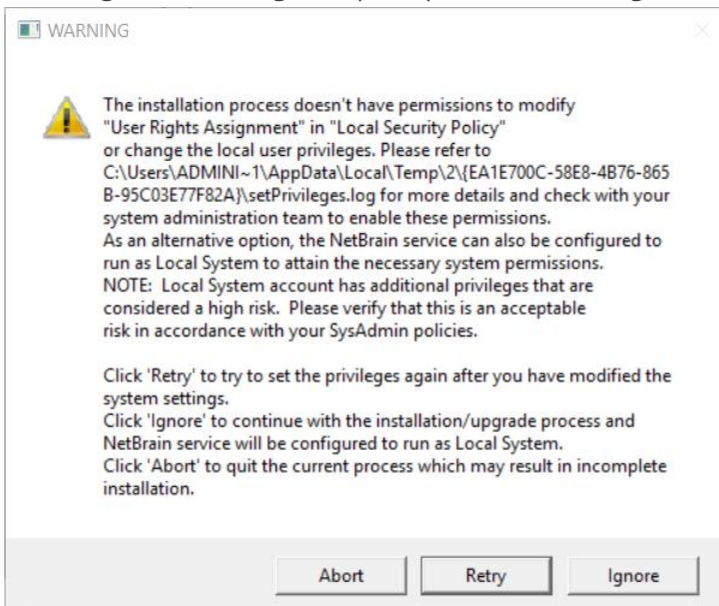
- 12) On the KeyVault Administration Passphrase Settings page, enter the passphrase that you created when installing Web API Server twice. Click **Next**.



The screenshot shows the 'KeyVault Administration Passphrase Settings' window. It includes a caution message about the passphrase not being recoverable, a warning about the 'Enable Resetting KVAP' feature, and two password input fields labeled 'KVAP' and 'Re-enter KVAP'. The 'Next >' button is highlighted.

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

- (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 **Ignore** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System.
- If you have security concerns, click **Abort** to quit the installation/upgrade process.
- Click **Retry** after you have modified the system settings.

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 **Abort**, 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.

3.12. Installing Front Servers

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 5432, 7778, 7087, 7088, 19814, 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](#)

3.12.1. Installing Front Server on Linux

Pre-installation Tasks

Front Server has dependencies on several third-party packages.

Before you install the Front Server, check whether these dependencies have been installed:

- For Amazon Linux 2023: Run the `rpm -q glibc libstdc++ libuuid pam libnsl` command.
- For other operating systems: Run the `rpm -q glibc libstdc++ libuuid pam glibc.i686 libstdc++.i686 libuuid.i686 pam.i686 libnsl libnsl.i686` command.

If the dependencies have not been installed yet, you can choose either option below to install the dependencies:

- **Online Install:** For Amazon Linux 2023:
 - Run the `yum install -y glibc libstdc++ libuuid pam libnsl` command to install the third-party packages online.
 - For all other operating systems: Run the `yum install -y glibc libstdc++ libuuid pam glibc.i686 libstdc++.i686 libuuid.i686 pam.i686 libnsl libnsl.i686` 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** or **sudo** user.
2. Run the `mkdir` command to create a directory under the **/opt** directory to place the Front Server installation package. For example, **netbraintemp12.1**.
3. Run the `cd /opt/netbraintemp12.1` command to navigate to the **/opt/netbraintemp12.1** 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-12.1.tar.gz** file from NetBrain and then upload it to the **/opt/netbraintemp12.1** 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/netbraintemp12.1** directory to directly download the **netbrain-frontserver-linux-x86_64-rhel-12.1.tar.gz** file from NetBrain official download site.

Note: Contact [NetBrain Support Team](#) to get the download link. 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-12.1.tar.gz` command under the **/opt/netbraintemp12.1** directory to extract installation files.

```
[root@localhost netbraintemp12.1]# tar -zxvf netbrain-frontserver-linux-x86_64-rhel-12.1.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 environment) 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.

3.12.2. 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.

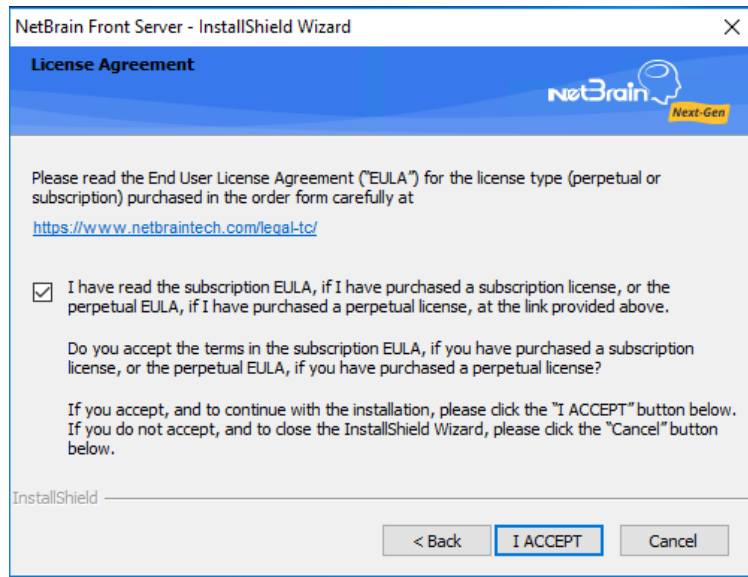
Complete the following steps with administrative privileges.

1. Download the **netbrain-frontserver-windows-x86_64-12.1.zip** file by using the download link provided in the email and save it in your local folder.

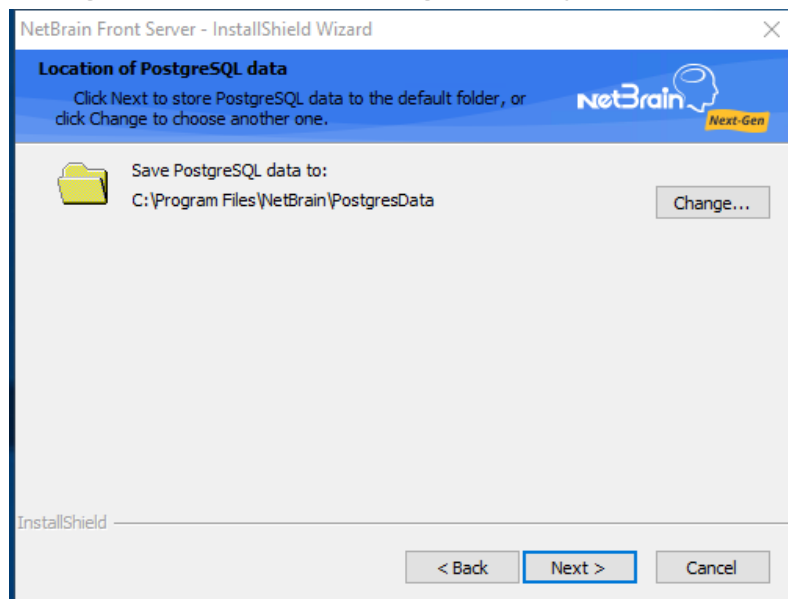
Tip: Contact [NetBrain Support Team](#) to get the download link.

2. Extract installation files from the **netbrain-frontserver-windows-x86_64-12.1.zip** file.
3. Right-click the **netbrain-frontserver-windows-x86_64-12.1.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**.

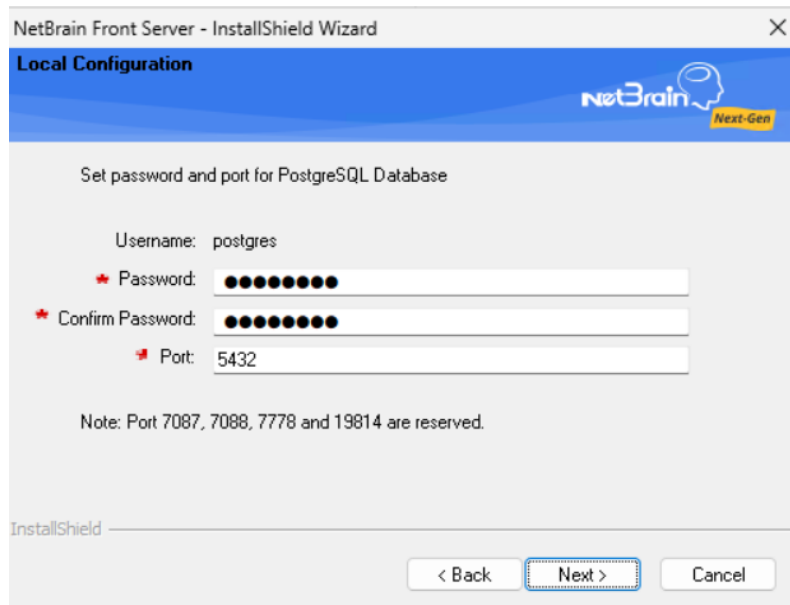


- 4) On the Customer Information page, enter your company name, and then click **Next**.
- 5) On the Destination Location page, click **Next** to install the Front Server under the default directory **C:\Program Files\NetBrain**. If you want to install it under another location, click **Change**.
- 6)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



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

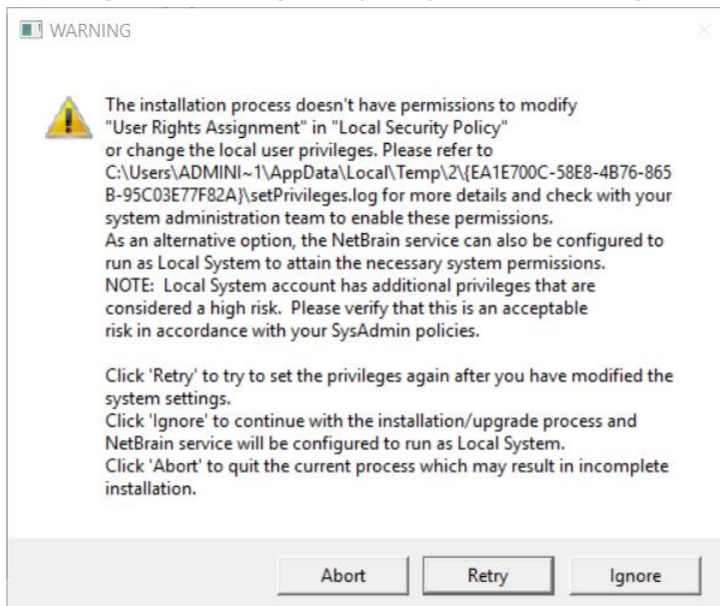
7) On the Local Configuration page, set password and port for PostgreSQL database.



The image shows the 'Local Configuration' window of the 'NetBrain Front Server - InstallShield Wizard'. The window has a blue header with the 'NetBrain Next-Gen' logo. The main content area is titled 'Set password and port for PostgreSQL Database'. It contains three input fields: 'Username' with the value 'postgres', 'Password' (masked with dots), and 'Confirm Password' (also masked with dots). Below these is a 'Port' field with the value '5432'. A note states: 'Note: Port 7087, 7088, 7778 and 19814 are reserved.' At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

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

- (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 **Ignore** to continue with installation/upgrade process and NetBrain service will be configured to run as Local System.
- If you have security concerns, click **Abort** to quit the installation/upgrade process.
- Click **Retry** after you have modified the system settings.

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 **Abort**, 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.

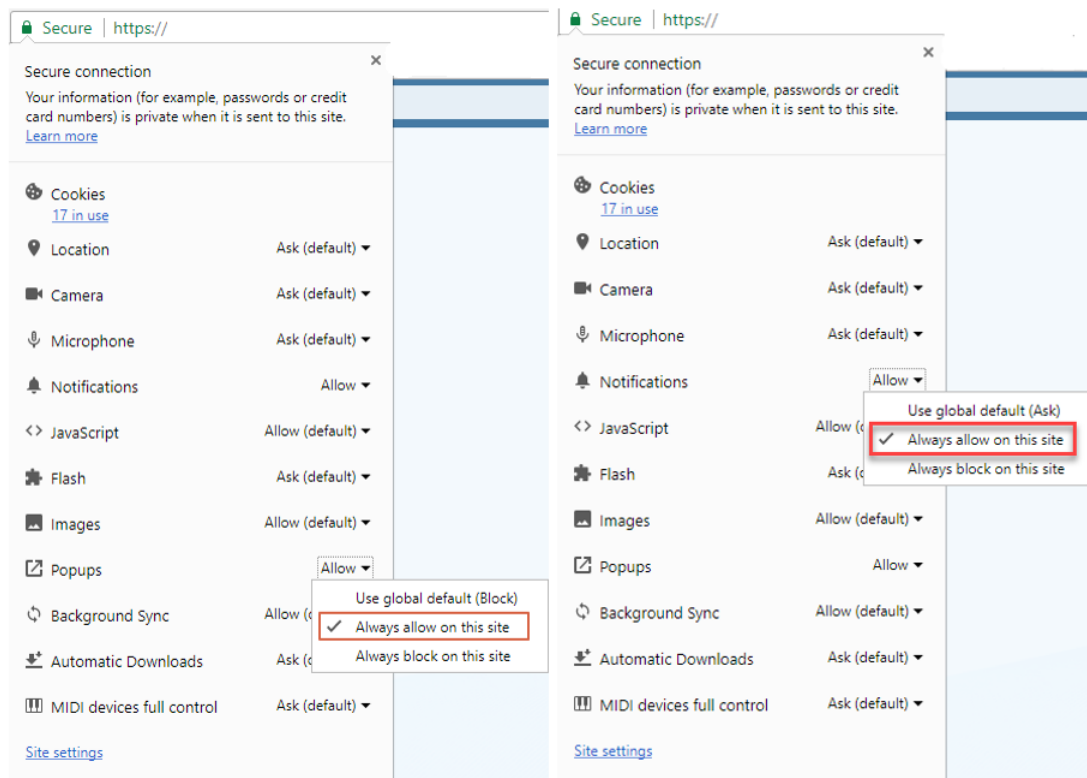
5. To install more Front Servers for load balancing, repeat the above installation steps on separate machines.

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. Check the tenant and domain nodes. If there is more than one domain, you need to allocate the domain.

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:

Add User

Basic Information

Authentication Source: NetBrain

* Email: jerry.chen@netbrain.com

* First Name: jerry

* Last Name: chao

* Username: jerryC

* Password:

* Confirm Password:

Phone Number:

Department:

Description: Enter text...

Advanced Settings

☐ Expired after 12:00 AM

☒ Allow users to change their own passwords

User Privilege

☐ System Administrator (Highest Privilege)

☒ Standard User

☒ System Management

☐ User Management

☐ Portal User

1 Tenants, 1 Domains Selected

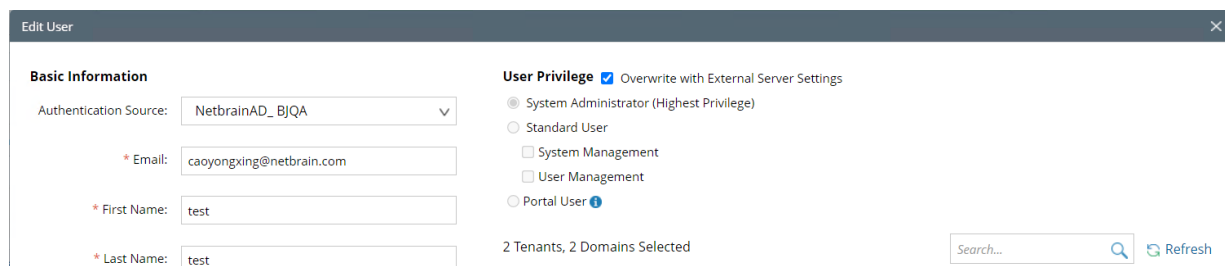
Tenant Access	Tenant Admin...	Allowed to Create Domain ...	Domain Access	Domain Privileges ...
<input checked="" type="checkbox"/> BVT_DB1TEN_hlu			<input type="checkbox"/> BVT_DB1DOM_1m	
			<input checked="" type="checkbox"/> jerrySmartCLI	1 role

Cancel Submit

- 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.

Add Front Server Controller [X]

Deployment Mode: Standalone

Front Server Controller Settings:

Front Server Controller

- *Name:
- *Hostname or IP Address:
- *Port:
- *Username:
- *Password:
- Timeout: Seconds
- Description:

SSL Settings

Allocated Tenants:

<input checked="" type="checkbox"/>	Tenant Name	Dedicated Front Server Controller
<input checked="" type="checkbox"/>	Initial Tenant	

Cancel Test OK

- **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.

[+ Add Front Server Controller](#)

[Refresh](#)

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

Front Server Controller Settings

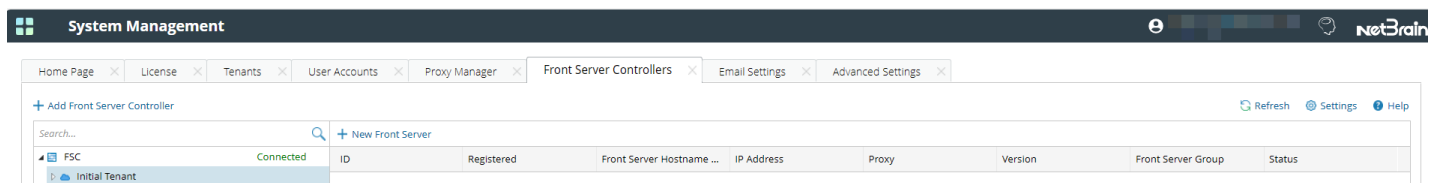
The following items (except **Timeout** and **Description**) are required to be consistent with those configured during the installation of Front Server Controller.

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.



3. Enter the following properties of the Front Server.

Add Front Server

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

*Front Server ID:

FS1

*Authentication Key:

Front Server Group:

(None)

Proxy:

None

Cancel

OK

- **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](#).

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

+ Add Front Server Controller

Refresh

Search...	+ Add Front Server						
<div><div>FSC</div><div>Connected</div><div><div>Initial Tenant</div><div>FS1</div></div></div>	ID	Registered	Front Server Hostname	IP Address	Version	Front Server Group	Status
	FS1	No					

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](#)

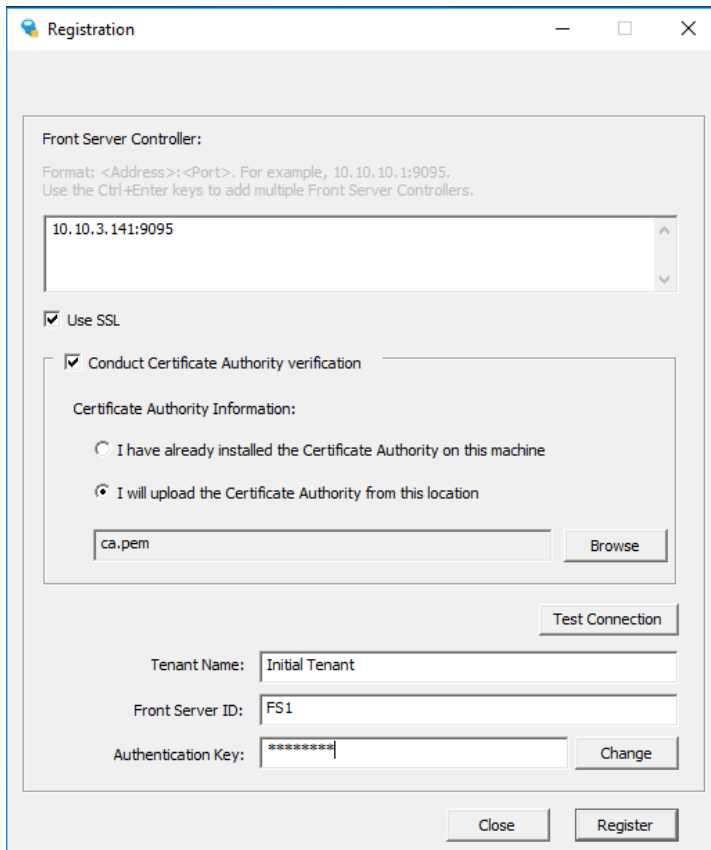
Note: If you deployed multiple Front Servers for load balancing, repeat the registration steps on separate machines.

Registering a Front Server on Windows

Example: Register a Front Server on Windows 10 Pro.

Complete the following steps with administrative privileges.

1. On the machine where the Front Server is installed, click the Windows start menu, scroll down the list and locate the **NetBrain** folder.
2. Under the **NetBrain** folder, right-click **Registration** and then select **More> 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** 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**.



The screenshot shows the 'Add Front Server Controller' window. On the left, a tree view shows 'PSC' (Connected) and 'Initial Tenant' (Connected) with 'FS1' listed below it. The main table displays the following information:

ID	Registered	Front Server Hostname	IP Address	Proxy	Version	Front Server Group	Status
FS1	YES	WIN-2ABAVLT44EB	10.10.3.141		10.1.11		Connected

Buttons for 'Refresh', 'Settings', and 'Help' are visible in the top right corner.

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 = no

# If "Conduct SSL certificate authority" is enabled, please enter the full path of the
certificate file
Conduct SSL Certificate Authority = no
SSL Certificate Path = /opt/cert.pem

# Define the front server that got registered
```

```
Tenant Name =Initial Tenant
Front Server ID =FS1
```

- Run the `cd ../bin` command to navigate to the bin directory.
- 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.
```

- 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. If you want to register a Front Server Controller group, use a semicolon to separate multiple Front Server Controllers.
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.

Parameter	Default Value	Description
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 System 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 System. 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 System 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 System](#)
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, click the  start menu > **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: After the check box **Automatically check the latest version** is enabled, users with 'sys admin' role will receive auto notification via email when a new version becomes available.

Note: To perform the **Automatically check the latest version** and **Check Update Now**:

- The Web API Server must have Internet access with the NetBrain public License Server.
- If the Web API Server has no Internet access, you can configure a proxy server to access the public License Server. Under System Management, navigate to the License tab > Internet Proxy Settings to configure the proxy server.

Note: In order to download and install platform resources automatically, you need to enable the **Automatically check the latest version** check box, as well as the **Download and Install Platform Resources Automatically** check box.

Current Version: 12.1.0.0  Email Notification: [23 Users](#)


✔ Successfully installed version 12.1.0.0


4/4/2025, 12:14:39 PM Executor: NetBrain

[View Test Results](#) [View Installation Log](#)

☒ Automatically check the latest version Last checked on: 4/4/2025, 12:20:31 PM

[Check Update Now](#)

☒ Download and Install Platform Resources Automatically 

Latest Available Version: **N/A** 

[Get Latest Version](#)

[Upload Latest Version](#) [Schedule](#)

[View Update History](#)

To Upgrade the system and resource, do as follows:

1. Click the **Check Update Now** button to see whether there is a new software or resource version available if your system is connected to the Internet. Ignore this step if your system is offline.
2. Click the **Get Latest Version** button to log in **NetBrain Customer Success Center** and download the software package. The package is created just for this system and cannot be used by other systems.
3. Click the **Upload Latest Version** button and upload the file downloaded at step 2.
4. Click the **Schedule** button to schedule the system update.

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.

3. 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.

Tip: If you don't want to download framework components, enable the **Exclude Framework Patch** check box.

Resource Package

License ID: 130322268

Current Framework Version: 12.1.0.0

Current Common Repo: 9a11ea10-06c9-3c53-bcf7-33de07c56b95|v0.0.2

Current Customized Built-in Resource Repo: N/A

Current Customized Resource Repo: N/A

Advanced Settings

☐ Exclude Framework Patch ⓘ

☐ Include All Platform Resources ⓘ


Generate Package

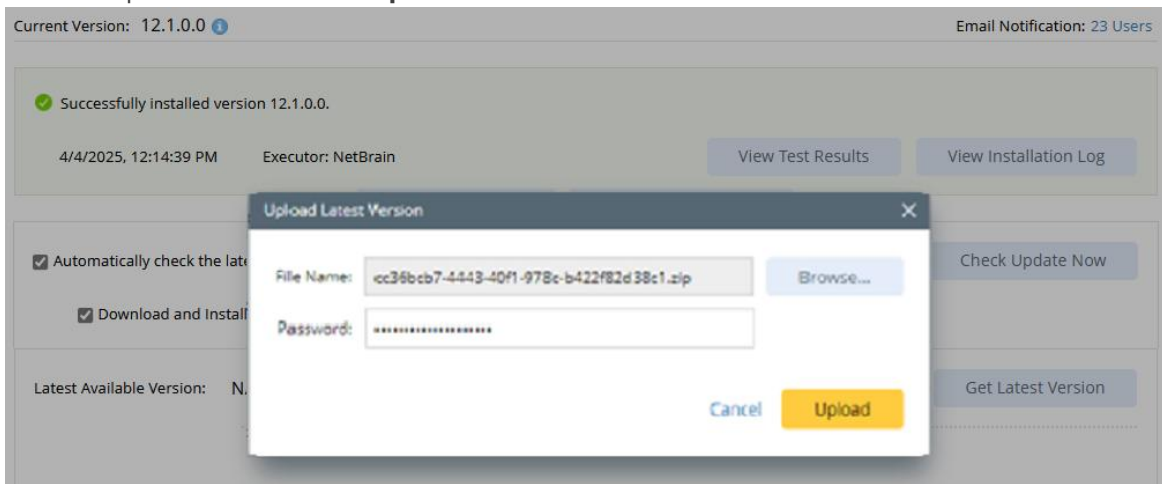
3. Click **Resource Package Link** to download the package to your local drive.
4. Keep note of the password for next step- [Upload Package to NetBrain System](#).

Upload Package to NetBrain System

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

Tip: To reduce the upload time, you can upload the auto-update package from the machine where the Web API Server is installed. If you've downloaded the package to another machine, you can transfer the package to the Web API Server and then upload the package from there.


1. In the System Management page, click the  start menu> **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**.



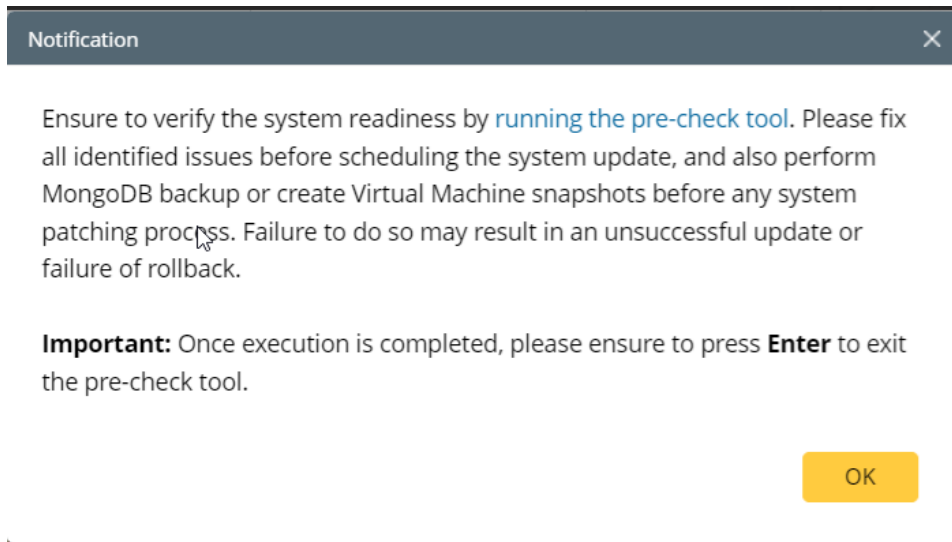
Tip: With the **Discard Uploaded Version** button, you can discard the previous uploaded update package before it is scheduled and delete the system update task before the scheduled task is executed.

Schedule Update

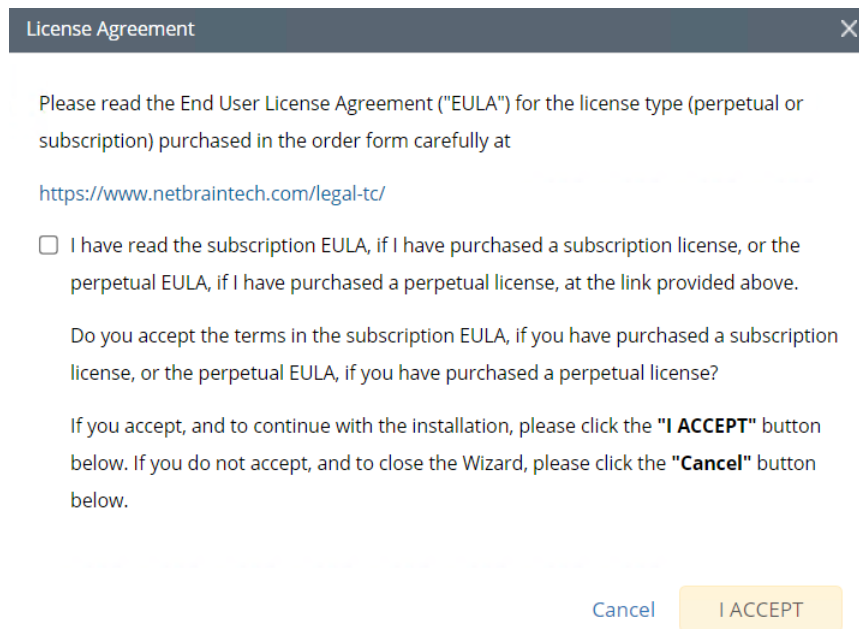
Follow the steps below to schedule the system update:

1. Run [the system update pre-check tool](#) to verify the environment readiness for the auto-update.
2. In the System Management page, click the  start menu> **System Update**.
3. Click **Schedule**.

4. In the Notification window, read the information and click **Next**.



5. Review the license agreement, select the **I have read the subscription EULA** check box and click **I ACCEPT**.



6. **(Optional)** Check the **Enable Test Plan** checkbox.

Tip: You can leave the **Enable Test Plan** checkbox unchecked to skip the test plan.

Note: Only user with domain and tenant access will be granted permission to run the test plan.

Review Test Plan Schedule Update

☒ Enable Test Plan

Before and after the system is upgraded, the system will execute the following test plan to ensure that the system works properly.

1. Basic system status check such as the server connectivity, service status and key process.
If any serious error is found, the system will rollback the update
2. Domain health and data accuracy test
 - a. The system will perform Domain Health test for the following domain.

Tenant: Initial Tenant Select

Domain: Domain1
 - b. The system will perform Data Accuracy test for the following devices and applications.

Device: Auto Test Group

Application: Auto Test Application

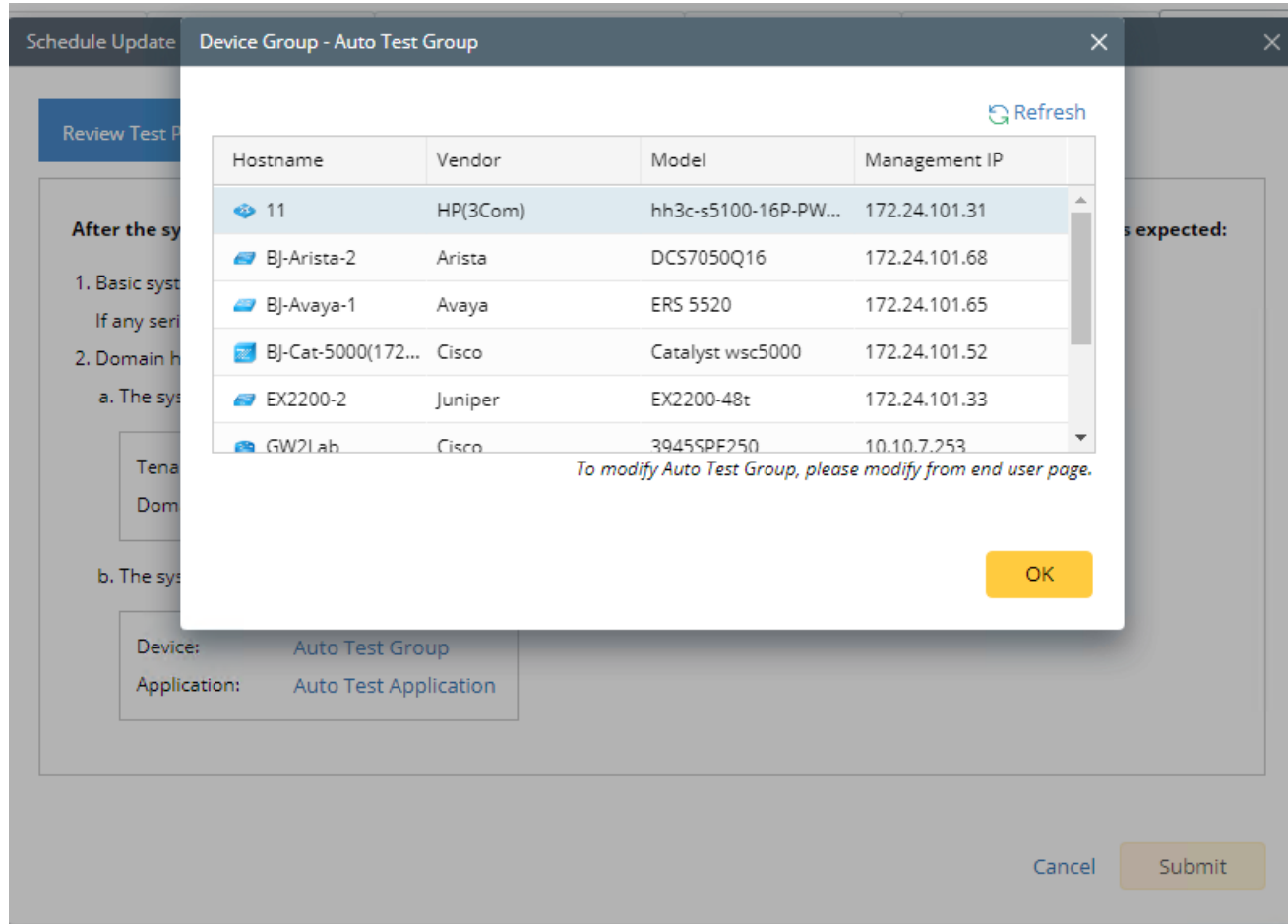
Cancel Submit

- 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.

The screenshot shows the 'Review Test Plan' interface. At the top, there are two tabs: 'Review Test Plan' (active) and 'Schedule Update'. Below the tabs, there is a section titled 'Enable Test Plan' with a checked checkbox. Below this, there is a section titled 'Before and after the system is upgraded, the system will perform the following tests:'.

1. Basic system status check such as the server connection. If any serious error is found, the system will rollback.

2. Domain health and data accuracy test.

a. The system will perform Domain Health test for the following domain:

Tenant: Initial Tenant [Select](#)

Domain: Domain1

b. The system will perform Data Accuracy test for the following application:

Device: Auto Test Group

Application: Auto Test Application

The 'Application - Auto Test Application' dialog box is open, showing a table of application paths. The table has columns: Path, Source, Destination, Group, and Protocol. The table contains 5 rows of data.

Path	Source	Destination	Group	Protocol
test1	10.10.4.41	172.21.3.5		IPv4
test3	172.26.3.10	172.26.4.10		IPv4
35	10.10.7.253	172.24.101.35		IPv4
test2	10.10.4.41	10.10.34.62		IPv4
test4	172.24.30.5	172.24.100.1		IPv4

Below the table, there is a note: 'To modify Auto Test Application, please modify from end user page.' and an 'OK' button.

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](#).

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

The screenshot shows the 'Schedule Update' interface. At the top, there are two tabs: 'Review Test Plan' and 'Schedule Update' (active). Below the tabs, there is a section titled 'Select the Start Time and Time Zone you want to Update. Your web server time zone is "(UTC-05:00) Eastern Time (US & Canada)"'.

Update Start Time: 2022-02-18 03 : 41 PM [Use Current Time](#)

Time Zone: (UTC-05:00) Eastern Time (US & Cana...

At the bottom right, there are 'Cancel' and 'Submit' buttons.

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

7. 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

The possible status of auto update are as follows:

Stage of the Auto Update	Possible Status
Before the execution of Auto Update	<ul style="list-style-type: none">• Ready for schedule.• Ready for running.
During the execution of Auto Update	<ul style="list-style-type: none">• Running.
After the execution of Auto Update	<ul style="list-style-type: none">• The system is successfully updated to the new version.• The system is successfully updated to the latest version, but the user performs a manual rollback and the rollback succeeds.• The system is successfully updated to the latest version, but the user performs a manual rollback and the rollback fails.• The update fails, and the system is rolled back to the old version.• The update fails at the beginning (due to insufficient disk space to perform auto-upgrade, unavailable component and etc.) and the roll back is not executed.

View Update History

Follow the steps below to view the update history:

1. In the System Management page, click the  start menu> **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:

- **Update From:** the release number from which the system is updated.
- **Update To:** the release number to which the system is updated.
- **Update Time:** when the system finished the update.
- **Executor:** the person to schedule the update
- **Action:** upgrade or user roll back.
- **Status:** one of the statuses in [View Update Status](#).
- **Release Note:** the link of the release note.
- **Installation Log:** the link of the installation log.
- **Test Report:** the link of the test results.

Upgrade From	Upgrade To	Updated Time	Executor	Action	Status	Release Note	Installation Log	Test Report
12.1.0.0	12.1.0.0	Apr 4, 2025, 12:20:19 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Apr 1, 2025, 12:19:34 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.0.0.0	12.1.0.0	Apr 1, 2025, 05:06:21 AM	admin	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Apr 1, 2025, 01:35:53 AM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Mar 31, 2025, 01:36:00 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Mar 29, 2025, 01:34:27 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Mar 29, 2025, 01:35:52 AM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Mar 28, 2025, 01:34:31 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Mar 27, 2025, 01:43:20 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.0.0.0	12.1.0.0	Mar 27, 2025, 05:32:36 AM	admin	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Mar 26, 2025, 03:06:05 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.0.0.0	12.1.0.0	Mar 26, 2025, 04:47:09 AM	admin	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.1.0.0	12.1.0.0	Mar 25, 2025, 12:20:12 PM	NetBrain	Upgrade	Succeeded	Release Note	Installation Log	Test Results
12.0.0.0	12.1.0.0	Mar 25, 2025, 06:06:38 AM	admin	Upgrade	Rollback failed	Release Note	Installation Log	Test Results

OK


4.8 Monitoring Server and Service Metrics

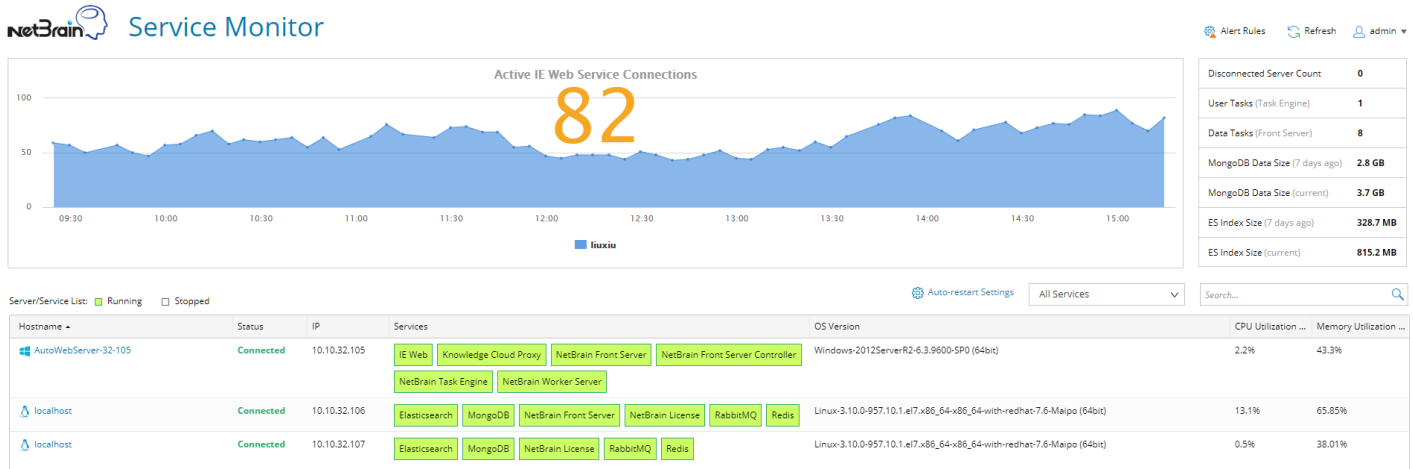
NetBrain Service Monitor provides a portal for administrators to observe the health of deployed Windows and Linux servers, with operations management of related services. It collects various types of metrics data from these deployed servers and visualizes them in tables or line charts.

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 the  start menu > **Service Monitor**.
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

- [Offline Installing Third-party Dependencies](#)
- [Editing a File with VI Editor](#)
- [SSL Certificate Requirements](#)
- [Third-Party User Authentication](#)
- [Configuring NTP Client on NetBrain Servers](#)

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:
 - **RHEL8.2:** <http://download.netbraintech.com/dependencies-rhel8.2.tar.gz>
 - **RHEL8.3:** <http://download.netbraintech.com/dependencies-rhel8.3.tar.gz>
 - **RHEL8.4:** <http://download.netbraintech.com/dependencies-rhel8.4.tar.gz>
 - **RHEL8.5:** <http://download.netbraintech.com/dependencies-rhel8.5.tar.gz>
 - **RHEL8.6:** <http://download.netbraintech.com/dependencies-rhel8.6.tar.gz>
 - **RHEL8.7:** <http://download.netbraintech.com/dependencies-rhel8.7.tar.gz>
 - **RHEL8.8:** <http://download.netbraintech.com/dependencies-rhel8.8.tar.gz>
 - **RHEL8.9:** <http://download.netbraintech.com/dependencies-rhel8.9.tar.gz>
 - **RHEL8.10:** <http://download.netbraintech.com/dependencies-rhel8.10.tar.gz>
 - **RHEL9.4:** <http://download.netbraintech.com/dependencies-rhel9.4.tar.gz>
 - **RHEL9.5:** <http://download.netbraintech.com/dependencies-rhel9.5.tar.gz>
 - **(Front Server) RHEL8.4:** <http://download.netbraintech.com/dependencies-fs-rhel8.4.tar.gz>
 - **(Front Server) RHEL8.5:** <http://download.netbraintech.com/dependencies-fs-rhel8.5.tar.gz>
 - **(Front Server) RHEL8.6:** <http://download.netbraintech.com/dependencies-fs-rhel8.6.tar.gz>
 - **(Front Server) RHEL8.7:** <http://download.netbraintech.com/dependencies-fs-rhel8.7.tar.gz>
 - **(Front Server) RHEL8.8:** <http://download.netbraintech.com/dependencies-fs-rhel8.8.tar.gz>
 - **(Front Server) RHEL8.9:** <http://download.netbraintech.com/dependencies-fs-rhel8.9.tar.gz>
 - **(Front Server) RHEL8.10:** <http://download.netbraintech.com/dependencies-fs-rhel8.10.tar.gz>
 - **(Front Server) RHEL9.4:** <http://download.netbraintech.com/dependencies-fs-rhel9.4.tar.gz>
 - **(Front Server) RHEL9.5:** <http://download.netbraintech.com/dependencies-fs-rhel9.5.tar.gz>

- **OL8.2:** <http://download.netbraintech.com/dependencies-ol8.2.tar.gz>
- **OL8.3:** <http://download.netbraintech.com/dependencies-ol8.3.tar.gz>
- **OL8.4:** <http://download.netbraintech.com/dependencies-ol8.4.tar.gz>
- **OL8.5:** <http://download.netbraintech.com/dependencies-ol8.5.tar.gz>
- **OL8.6:** <http://download.netbraintech.com/dependencies-ol8.6.tar.gz>
- **OL8.7:** <http://download.netbraintech.com/dependencies-ol8.7.tar.gz>
- **OL8.8:** <http://download.netbraintech.com/dependencies-ol8.8.tar.gz>
- **OL8.9:** <http://download.netbraintech.com/dependencies-ol8.9.tar.gz>
- **OL8.10:** <http://download.netbraintech.com/dependencies-ol8.10.tar.gz>
- **OL9.4:** <http://download.netbraintech.com/dependencies-ol9.4.tar.gz>
- **OL9.5:** <http://download.netbraintech.com/dependencies-ol9.5.tar.gz>
- **(Front Server) OL8.4:** <http://download.netbraintech.com/dependencies-fs-ol8.4.tar.gz>
- **(Front Server) OL8.5:** <http://download.netbraintech.com/dependencies-fs-ol8.5.tar.gz>
- **(Front Server) OL8.6:** <http://download.netbraintech.com/dependencies-fs-ol8.6.tar.gz>
- **(Front Server) OL8.7:** <http://download.netbraintech.com/dependencies-fs-ol8.7.tar.gz>
- **(Front Server) OL8.8:** <http://download.netbraintech.com/dependencies-fs-ol8.8.tar.gz>
- **(Front Server) OL8.9:** <http://download.netbraintech.com/dependencies-fs-ol8.9.tar.gz>
- **(Front Server) OL8.10:** <http://download.netbraintech.com/dependencies-fs-ol8.10.tar.gz>
- **(Front Server) OL9.4:** <http://download.netbraintech.com/dependencies-fs-ol9.4.tar.gz>
- **(Front Server) OL9.5:** <http://download.netbraintech.com/dependencies-fs-ol9.5.tar.gz>
- **Alma8.4:** <http://download.netbraintech.com/dependencies-almalinux8.4.tar.gz>
- **Alma8.5:** <http://download.netbraintech.com/dependencies-almalinux8.5.tar.gz>
- **Alma8.6:** <http://download.netbraintech.com/dependencies-almalinux8.6.tar.gz>
- **Alma8.7:** <http://download.netbraintech.com/dependencies-almalinux8.7.tar.gz>
- **Alma8.8:** <http://download.netbraintech.com/dependencies-almalinux8.8.tar.gz>
- **Alma8.9:** <http://download.netbraintech.com/dependencies-almalinux8.9.tar.gz>
- **Alma 8.10:** <http://download.netbraintech.com/dependencies-almalinux8.10.tar.gz>
- **Alma 9.4:** <http://download.netbraintech.com/dependencies-almalinux9.4.tar.gz>
- **Alma 9.5:** <http://download.netbraintech.com/dependencies-almalinux9.5.tar.gz>
- **(Front Server) Alma8.4:** <http://download.netbraintech.com/dependencies-fs-almalinux8.4.tar.gz>
- **(Front Server) Alma8.5:** <http://download.netbraintech.com/dependencies-fs-almalinux8.5.tar.gz>
- **(Front Server) Alma8.6:** <http://download.netbraintech.com/dependencies-fs-almalinux8.6.tar.gz>
- **(Front Server) Alma8.7:** <http://download.netbraintech.com/dependencies-fs-almalinux8.7.tar.gz>

- **(Front Server) Alma8.8:** <http://download.netbraintech.com/dependencies-fs-almalinux8.8.tar.gz>
- **(Front Server) Alma8.9:** <http://download.netbraintech.com/dependencies-fs-almalinux8.9.tar.gz>
- **(Front Server) Alma 8.10:** <http://download.netbraintech.com/dependencies-fs-almalinux8.10.tar.gz>
- **(Front Server) Alma 9.4:** <http://download.netbraintech.com/dependencies-fs-almalinux9.4.tar.gz>
- **(Front Server) Alma 9.5:** <http://download.netbraintech.com/dependencies-fs-almalinux9.5.tar.gz>
- **Rocky8.4:** <http://download.netbraintech.com/dependencies-rockylinux8.4.tar.gz>
- **Rocky8.5:** <http://download.netbraintech.com/dependencies-rockylinux8.5.tar.gz>
- **Rocky8.6:** <http://download.netbraintech.com/dependencies-rockylinux8.6.tar.gz>
- **Rocky8.7:** <http://download.netbraintech.com/dependencies-rockylinux8.7.tar.gz>
- **Rocky8.8:** <http://download.netbraintech.com/dependencies-rockylinux8.8.tar.gz>
- **Rocky8.9:** <http://download.netbraintech.com/dependencies-rockylinux8.9.tar.gz>
- **Rocky8.10:** <http://download.netbraintech.com/dependencies-rockylinux8.10.tar.gz>
- **Rocky9.4:** <http://download.netbraintech.com/dependencies-rockylinux9.4.tar.gz>
- **Rocky9.5:** <http://download.netbraintech.com/dependencies-rockylinux9.5.tar.gz>
- **(Front Server) Rocky8.4:** <http://download.netbraintech.com/dependencies-fs-rockylinux8.4.tar.gz>
- **(Front Server) Rocky8.5:** <http://download.netbraintech.com/dependencies-fs-rockylinux8.5.tar.gz>
- **(Front Server) Rocky8.6:** <http://download.netbraintech.com/dependencies-fs-rockylinux8.6.tar.gz>
- **(Front Server) Rocky8.7:** <http://download.netbraintech.com/dependencies-fs-rockylinux8.7.tar.gz>
- **(Front Server) Rocky8.8:** <http://download.netbraintech.com/dependencies-fs-rockylinux8.8.tar.gz>
- **(Front Server) Rocky8.9:** <http://download.netbraintech.com/dependencies-fs-rockylinux8.9.tar.gz>
- **(Front Server) Rocky8.10:** <http://download.netbraintech.com/dependencies-fs-rockylinux8.10.tar.gz>
- **(Front Server) Rocky9.4:** <http://download.netbraintech.com/dependencies-fs-rockylinux9.4.tar.gz>
- **(Front Server) Rocky9.5:** <http://download.netbraintech.com/dependencies-fs-rockylinux9.5.tar.gz>
- **Amazon Linux 2023:** <http://download.netbraintech.com/dependencies-amzn-amzn2023.tar.gz>
- **(Front Server) Amazon Linux 2023:** <http://download.netbraintech.com/dependencies-fs-amzn-amzn2023.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: `rhel8.2; rhel8.3; rhel8.4; rhel8.5; rhel8.5; rhel8.6; rhel8.7; rhel8.8; rhel8.9; rhel8.10; rhel9.4; rhel9.5; ol8.2; ol8.3; ol8.4; ol8.5; ol8.6; ol8.7; ol8.8; ol8.9; ol8.10; ol9.4; ol9.5; almalinux8.4; almalinux8.5; almalinux8.6; almalinux8.7; almalinux8.8; almalinux8.9; almalinux8.10; almalinux9.4; almalinux9.5; rockylinux8.4; rockylinux8.5; rockylinux8.6; rockylinux8.7; rockylinux8.8; rockylinux8.9; rockylinux8.10; rockylinu9.4; rockylinu9.5; amzn-amzn2023.`

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	<ul style="list-style-type: none">▪ 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

NetBrain Server	Required SSL Certificate and Key	Format
Elasticsearch Redis RabbitMQ Front Server Controller Ansible Agent	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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](#)