NetBrain® Integrated Edition 10.0

Domain Maintenance Guide

Contents

1. Maintenance Overview

To provide accurate and up-to-date network data for daily operations, it is essential to maintain your domain data and your system on a regular basis. The **Expected Result** column indicates a good status of your domain.

Category	Task	Expected Result
Data Maintenance (Weekly Tasks)	View Domain Health Report	All issues reflected in the report are resolved
	Clean Up Domain Access Issues	Resolve all managed devices under the following categories: ▪ Unknown IPs ▪ Missed Devices ▪ Discovered by SNMP ▪ Unknown SNMP SysObjectID ▪ Unclassified Network Devices ▪ Hostname-Changed Devices
	Resolve Duplicated IP and Subnet	IP Conflicted = 0
	Verify Benchmark/Discovery Task Result	▪ Benchmark/discovery tasks are enabled and successfully executed ▪ All devices are selected with all applicable live data ▪ All operations are selected on Update MPLS Cloud/Build Topology/System Operations/Update Maps areas
	Tune Live Access	Login = 0 Failed
	Clean Up Unassigned Site Members	Unassigned site members = 0
	Browse Map Update Result	All map updates are successful
System Maintenance (Monthly Tasks)	Maintain Data Storage	MongoDB disk space utilization < 70%
	Customize Auto-Update Schedule	Current resource = Latest version
	Monitor Server and Service Metrics	Status = Connected Services = Green (Running) CPU/Mem utilization < 70%

2. Logging into Domain Management Page

1. In your web browser, navigate to **http(s)://<IP address or hostname of NetBrain Web Server>/**. For example, **`https://10.10.3.141/`** or **`http://10.10.3.141/`**.

2. In the login page, enter your username or email address, and password.

3. Click **Log In**. Please update the initial password if it's your first-time login.

4. Click the domain name from the quick access toolbar and select **Domain Management**.
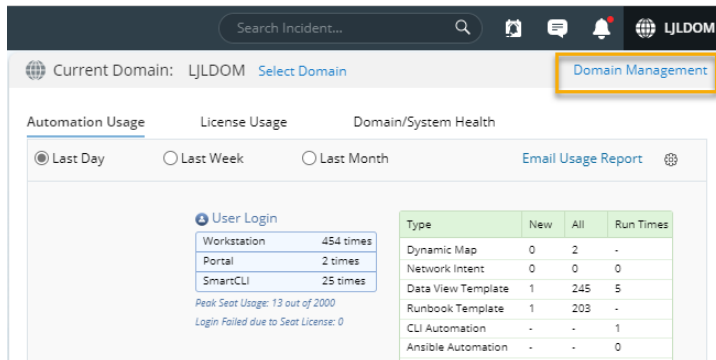
> **Note:** It is not recommended to use the same web browser to log in to the system with multiple user accounts. Only the last logged-in user can be recognized as the current user.

3. Viewing Domain Health Report

Domain Health Report records the key factors about domain health. You can get a quick overview of the current domain status with this report.

Desired Outcome: All issues reflected in the report are resolved.

1. In the Domain Management page, select **Operations > Domain Health Report** from the quick access toolbar.

2. In the **Domain Health Report** tab, click **Create Health Report** to generate a report.

3. View the highlighted area to get an overview.

4. Check the following areas to get more information. See [Viewing Domain Health Report](#) for more details.
   - Driver Associated Device
   - Basic Network Settings Completeness
   - Discovery Status
   - Site Definition Completeness
   - Benchmark Task Health
   - Cloud Health
   - Path Calculation Health
   - Disk Management Settings Completeness
   - Map Layout Settings Completeness

4. Cleaning Up Domain Issues

Creating and maintaining a domain with all devices properly discovered is the key to keep system data up-to-date to guarantee data accuracy and further utilize advanced features, such as path and map.

Fine Tune provides an overview of how devices are discovered, where you can get started to fix all the access issues. The devices listed in each category are updated as soon as a discovery task is completed, including both the on-demand discovery and the scheduled discovery. It's recommended to check and maintain in the Fine Tune at least once a week or whenever a discovery task is completed.

1. In the Domain Management page, click **Fine Tune** on the Start Page or select **Operations > Fine Tune** from the quick access toolbar.

2. Resolve the issues under the following categories:

   - **SNMP-Only Devices** — the devices accessed by SNMP but failed to be accessed via Telnet/SSH.
     - o **Desired Outcome**: Fix Telnet/SSH access issues on all devices in this list that use these protocols. This list should only contain devices that are SNMP-only.
   - **Missed Devices** — the devices existing in the current domain but failed to be verified during a discovery.
     - o **Desired Outcome**: Fix device access issues or remove decommissioned devices in this list to bring the number of devices down to 0.
   - **Unknown SNMP SysObjectID** — the devices whose SysObjectIDs are not defined in the Vendor Model table.
     - o **Desired Outcome**: Add all unknown OIDs in this list to the vendor model table to decrease the number down to 0.
   - **Unknown IP** — the IP addresses that cannot be accessed via Telnet/SSH and SNMP in the **Discover via Seed Routers** method during a discovery.
     - o **Desired Outcome**: Fix all known IPs with correct Telnet/SSH/SNMP in this list.
   - **SSH Fingerprint Check Failed** — the devices whose current fingerprint keys are different with the latest ones retrieved during live access.
     - o **Desired Outcome**: All devices with SSH fingerprint check failed are resolved.
   - **Hostname-Changed Device** — the device whose hostname is changed and exists with more than one hostname in a domain.
     - o **Desired Outcome:** All devices with hostname change are detected and the desired ones remain in the domain.

   > **Tip:** You can click Discovered Devices to view the devices discovered successfully.

Best Practice:

- [How to Remove Devices from Domain](#)

- [How to Identify a List of Devices That Have Lost Access for Certain Days in the System](#)

- [How to Manage Devices with Inconsistent Hostnames Retrieved via SNMP and CLI](#)

5. Resolving Duplicated IP and Subnet

The duplicate IPs refer to the interfaces configured with the same IPv4 addresses.

During the live network discovery, the system parses the VRF and IPv4 address for each interface and deals with the interfaces of duplicated IPs as follows:

- If two interfaces are configured with the same IP address, but with different VRFs, then two zones named after the VRFs will be created automatically after the IPv4 L3 topology is built, and these two interfaces will be moved to the corresponding zone according to its configured VRF. The system automatically performs this operation by default. To disable it, go to the **Domain Management** page, click **Operations**, point to **Domain Settings**, select **Advanced Settings**, and uncheck the **Automatically create zones and assign VRF interface based on VRF names** option.

- If two interfaces are configured with the same IP address, but without VRFs configured, these two interfaces will be moved to the Default Zone. To separate the two interfaces, you must create a zone manually, then move one of the interfaces and its neighbor interfaces into the created zone, and finally rebuild the IPv4 L3 topology.

> **Tip:** The Default Zone is auto-generated in each domain by the system to store interfaces in IPv4 L3 topology by default. It can neither be renamed nor deleted.

After the interfaces of duplicated IPs being moved into different zones, all duplicated IPs can be involved in IPv4 L3 topology link calculations. When you extend IPv4 L3 neighbors, all calculated links can be displayed on the same map page. Leaving duplicated IPs unresolved will lead to no L3 links on the interfaces with duplicated IP.

Desired Outcome: All interfaces of duplicated IPs are moved into different zones. No interfaces are listed with **Yes** in the **IP Conflicted** column.

Example: Devices "R1" and "Cisco-LAN-28" are configured with the same IP address, but without VRF configured. The device "Cisco-LAN-29" in a real network should be connected to the device "Cisco-LAN-28", but now it is wrongly connected to the device "R1" because of the duplicated IP issue.
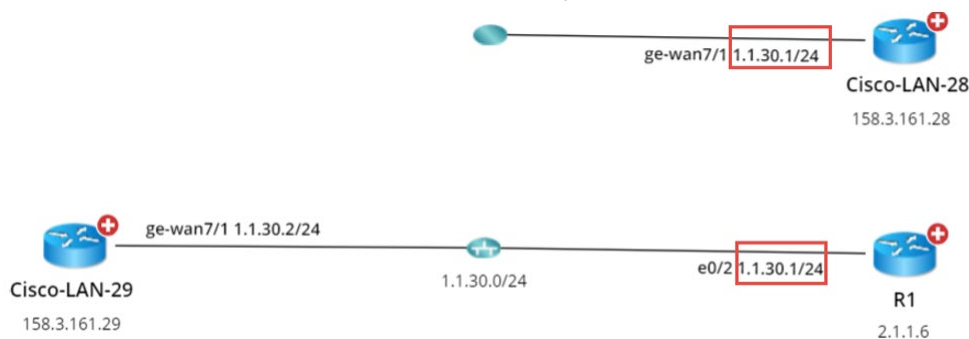
1. In the Domain Management page, click **Fine Tune** on the Start Page and then click **Duplicated IP and Subnet Manager** on the left pane. All subnets that contain duplicate IPs in the **Default Zone** are listed by default.

2. Create a zone.

1) Click **New zone**.

2) Enter the zone name, for example, **Zone1** and press **Enter**.

3. Move the interface of duplicated IP and its neighbor interface that can be connected correctly to the **Zone1** and rebuild the IPv4 L3 topology.

    1) Select the interface of duplicated IP and its neighbor interfaces that you want to establish the topology link, and then right-click to select **Move to**. In this example, select the **GE-WAN7/1** interface of the **Cisco-LAN-29** device and the **GE-WAN7/1** interface of the **Cisco-LAN-28** device, and then right-click to select **Move to**.

	Subnet ▲	Device Name	Interface Name	IP Address	IP Conflicted	VRF	Interface Description
▲	1.1.30.0/24 - (Default Zone) (3)						
		Cisco-LAN-29	GE-WAN7/1	1.1.30.1/24	Yes		
		R1	Move to	1.1.30.1/24	Yes		
		Cisco-LAN-28	GE-WAN7/1	1.1.30.2/24	No		

> **Tip:** If a lot of duplicated subnets are detected in the Default Zone, you can quickly search them within the **Search bar**. Use semicolons to separate the multiple items.

    2) Select **Zone1** that you created and click **OK**.

> **Note:** The **Move to** operation will delete all the manually added topology links of this interface.

    3) Click **Yes** in the pop-up dialog box to rebuild the IPv4 Layer 3 topology.

After the system finishes building the topology, the topology links are correctly connected.
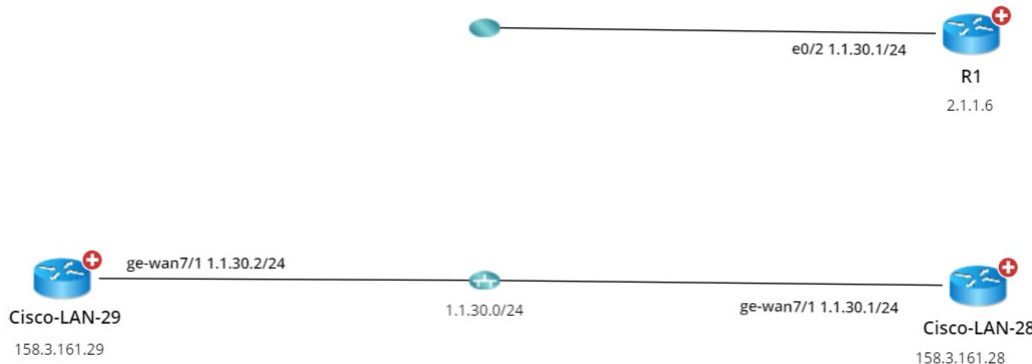
Best Practice:

- [How to Manually Build or Change L3/L2 Topology Links on Demand](#)

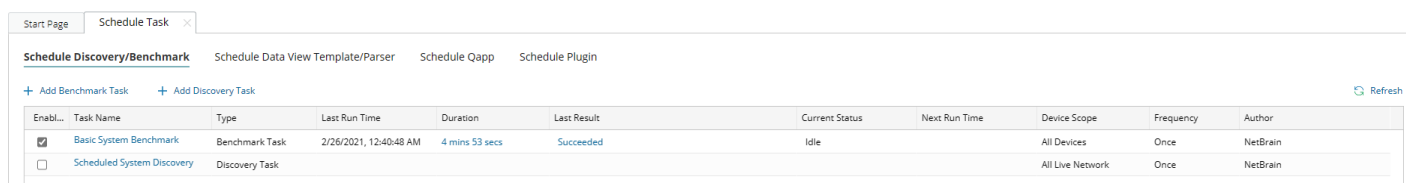# 6. Verifying Benchmark/Discovery Result

It is essential to have a successfully executed system benchmark to keep domain data up-to-date, as it does not only benchmark your network but also update network topologies, re-calculate sites, rebuild visual space, and update maps.

Desired Outcome:

- Benchmark/discovery tasks are enabled and successfully executed.
- All devices are selected with all applicable live data.
- All operations are selected on Update MPLS Cloud/Build Topology/System Operations/Update Maps areas.

Example: Verify benchmark results by browsing logs.

1. In the Domain Management page, click **Schedule Task** on the Start Page or select **Operations > Schedule Task** from the quick access toolbar.
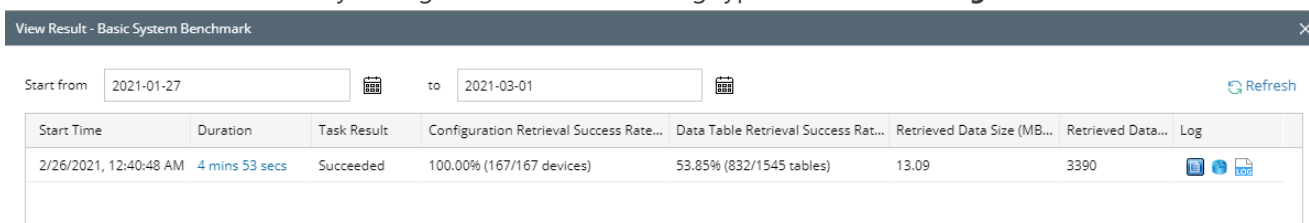
Enabl...	Task Name	Type	Last Run Time	Duration	Last Result	Current Status	Next Run Time	Device Scope	Frequency	Author
☑	Basic System Benchmark	Benchmark Task	2/26/2021, 12:40:48 AM	4 mins 53 secs	Succeeded	Idle		All Devices	Once	NetBrain
☐	Scheduled System Discovery	Discovery Task						All Live Network	Once	NetBrain

> **Tip:** You can view the latest execution result of all benchmark tasks from the **Last Result** column. To view the detailed latest execution log of a benchmark task, click the hyperlink (such as **Succeeded**) in its **Last Result** column.

2. Right-click the target task entry and then select **View Result** from the drop-down menu.

3. In the following dialog, the **Configuration Retrieval Success Rate** reflects how many devices are qualified and can be retrieved data successfully during the task. Select the log type to view in the **Log** column.

Start Time	Duration	Task Result	Configuration Retrieval Success Rate...	Data Table Retrieval Success Rat...	Retrieved Data Size (MB...	Retrieved Data...	Log
2/26/2021, 12:40:48 AM	4 mins 53 secs	Succeeded	100.00% (167/167 devices)	53.85% (832/1545 tables)	13.09	3390	

▼ **View Execution Log**

Click the 📄 icon in the target entry to view all execution logs. To only view the failed logs, select the **Only show failed logs** check box.

Execution Log - Basic System Benchmark: 2/26/2021, 12:40:48 AM		✕
☐ Only show failed logs		↻ Refresh

Date & Time	Messages	Total Time Spent
2/26/2021, 1:03:53 AM	Begin: retrieve devices data.	
2/26/2021, 1:06:39 AM	End: retrieve devices data.	0 hrs 2 mins 46 secs
2/26/2021, 1:06:39 AM	Begin run plugin:Built-in Plugins/Multisource/Benchmark_...	
2/26/2021, 1:06:45 AM	End: run plugin "Built-in Plugins/Multisource/Benchmark_...	
2/26/2021, 1:06:46 AM	Begin run plugin:Built-in Plugins/NB_System_Use/AWS_Pos...	
2/26/2021, 1:06:48 AM	End: run plugin "Built-in Plugins/NB_System_Use/AWS_Pos...	
2/26/2021, 1:06:49 AM	Begin: update Global Endpoint index.	
2/26/2021, 1:06:50 AM	End: update Global Endpoint index.	0 hrs 0 mins 1 secs

▼ **View Device Log**

1) Click the 🌐 icon in the target entry. By default, the devices with any data retrieval failures are listed.

Device Log - Basic System Benchmark: 2/26/2021, 12:40:48 AM							✕

15 Items   View: Devices with retrieval failures ▼   🔍 Search device name...   📤 Export ↻ Refresh

Device Name	Device Type	Retrieval Time (seconds...	Configuration	Route Table	ARP Table ...	MAC Table	NDP Table...
🔵 Multicast-R2	Cisco Router	8	Succeeded via CLI	Succeeded	Succeeded	Failed	Succeeded
📁 SW_Hub16	Cisco IOS Switch	10	Succeeded via CLI	Succeeded	Succeeded	Succeeded	Succeeded
📁 IPSEC-switch	Cisco IOS Switch	10	Succeeded via CLI	Succeeded	Succeeded	Succeeded	Succeeded
📁 sw2960-125	Cisco IOS Switch	11	Succeeded via SNMP	Failed	Succeeded	Failed	Succeeded
📁 NATT-MGMT	Cisco IOS Switch	11	Succeeded via CLI	Succeeded	Succeeded	Succeeded	Succeeded
📁 OSPFv3-R39	Cisco IOS Switch	11	Succeeded via CLI	Succeeded	Succeeded	Succeeded	Succeeded
📁 OSPFv3-R34	Cisco IOS Switch	11	Succeeded via CLI	Succeeded	Succeeded	Succeeded	Succeeded
🔵 Multicast-Receive2	Cisco Router	11	Succeeded via CLI	Succeeded	Succeeded	Failed	Succeeded
🔵 JMPLS-R2	Cisco Router	12	Succeeded via CLI	Succeeded	Succeeded	Succeeded	Succeeded
📁 SW_Hub18	Cisco IOS Switch	13	Succeeded via CLI	Succeeded	Succeeded	Succeeded	Succeeded

Live Access Log of Multicast-R2:

```
2021-02-26 13:40:51 Begin data retrieving task via Worker WIN-M6846GLCGUS(pid: 3956)
2021-02-26 13:40:51 Prepare retrieving command.
2021-02-26 13:40:51 Telnet to device 172.25.117.5 via FS(10.10.34.84)
2021-02-26 13:40:51 Telnet to device 172.25.117.5 successfully via FS(10.10.34.84)
2021-02-26 13:40:51 Return from Device:[Username:]
2021-02-26 13:40:51 Sending Username:nb
```
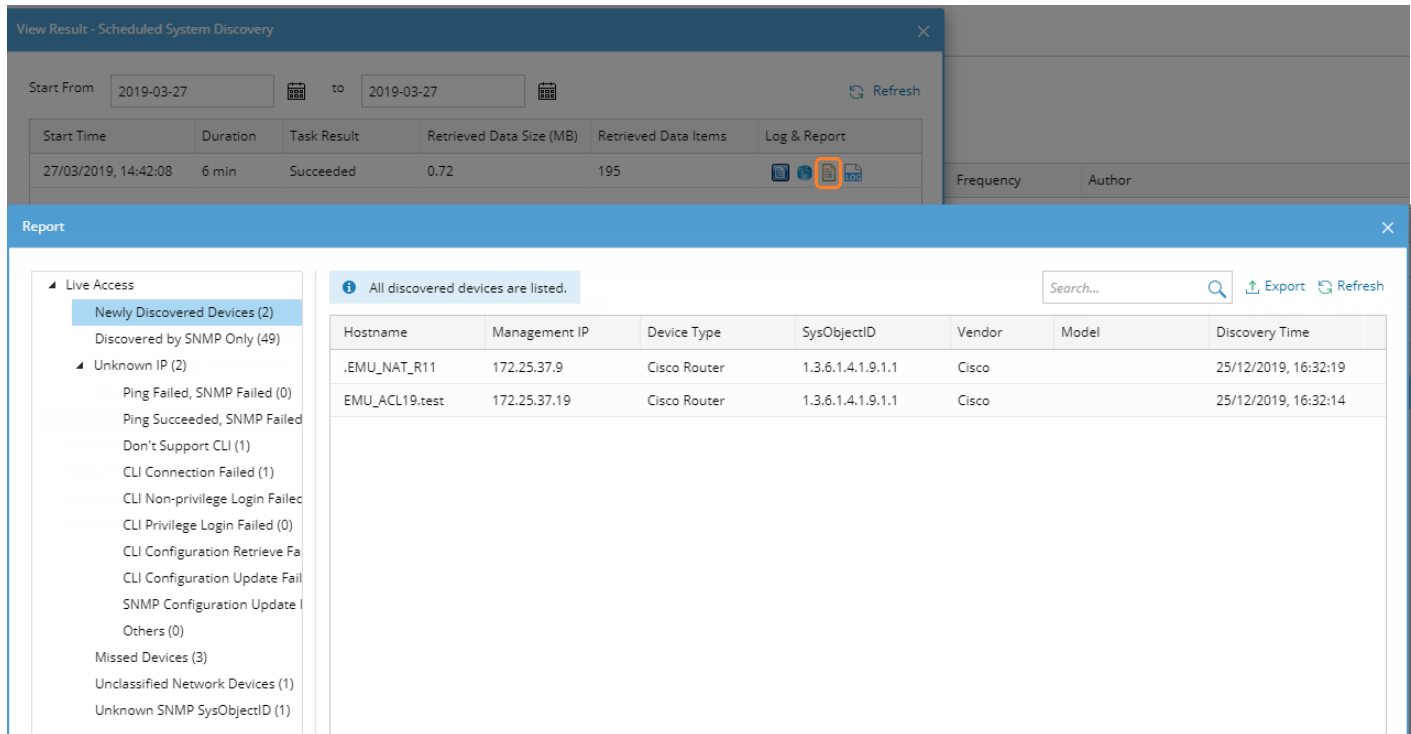
Progress: (Not Running)   Close

> **Tip**: To show other devices, select a category of **View** drop-down list.

2) Select a device entry to view its task log at the bottom of the dialog.

▼ View Discovery Report

For discovery tasks, you can click the 📄 icon to view discovery reports. To resolve the devices with access issues, see [Cleaning Up Domain Issues](#) for more details.

Start Time	Duration	Task Result	Retrieved Data Size (MB)	Retrieved Data Items	Log & Report
27/03/2019, 14:42:08	6 min	Succeeded	0.72	195	

View Result - Scheduled System Discovery

Start From 2019-03-27 to 2019-03-27   ↻ Refresh

Report

- ◢ Live Access
  - Newly Discovered Devices (2)
  - Discovered by SNMP Only (49)
  - ◢ Unknown IP (2)
    - Ping Failed, SNMP Failed (0)
    - Ping Succeeded, SNMP Failed
    - Don't Support CLI (1)
    - CLI Connection Failed (1)
    - CLI Non-privilege Login Failec
    - CLI Privilege Login Failed (0)
    - CLI Configuration Retrieve Fa
    - CLI Configuration Update Fail
    - SNMP Configuration Update I
    - Others (0)
  - Missed Devices (3)
  - Unclassified Network Devices (1)
  - Unknown SNMP SysObjectID (1)

ⓘ All discovered devices are listed.   Search... 🔍 ⬆ Export ↻ Refresh

Hostname	Management IP	Device Type	SysObjectID	Vendor	Model	Discovery Time
.EMU_NAT_R11	172.25.37.9	Cisco Router	1.3.6.1.4.1.9.1.1	Cisco		25/12/2019, 16:32:19
EMU_ACL19.test	172.25.37.19	Cisco Router	1.3.6.1.4.1.9.1.1	Cisco		25/12/2019, 16:32:14

Best Practice:

- ▪ [How to Validate Data Collected from Benchmark](#)

7. Tuning Live Access

Tuning live access enables you to check the reachability of live devices by polling the credentials configured in the Network Settings or verifying the credentials in the Device Settings. You can tune live access to synchronize login credentials, vendor and model changes, and check hostname changes if they occur in your network.

Desired Outcome: No network devices show as **Failed** in the **Login** column.

To tune live access, complete the following steps:

1. [Log in to the Domain Management page](). In the Domain Management page, select **Operations > Advanced Tools > Tune Live Access** from the quick access toolbar. The **Tune Live Access** tab opens with all devices in the domain listed.
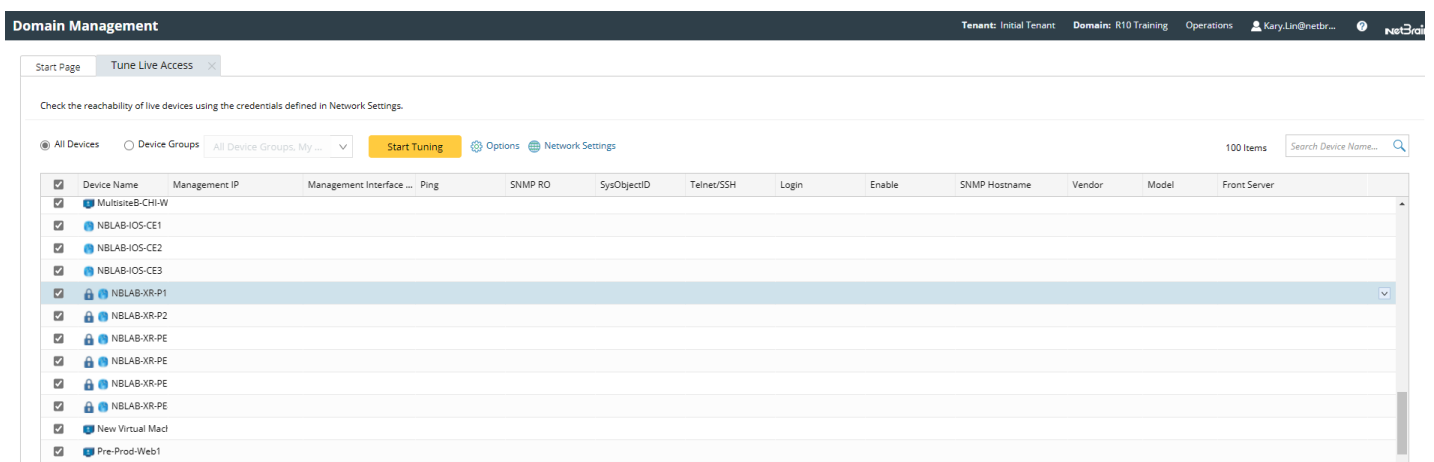
> **Tip**: The 🔒 icon indicates the Shared Device Settings of the device are locked so that the system will only verify the login credentials of the device in the Shared Device Settings during the tuning process.
>
> **Tip**: To view the latest live access results, right-click in the table list and select **Load Last Results**.

2. Select devices to tune live settings. By default, all devices in the domain are selected. You can select devices by device group.

3. To view or change the tuning mode and access method, click **Options**. See Tuning Options for more details.

> **Tip**: To specify Front Server, jumpbox, and credentials to use in the tuning process, click **Network Settings**.

4. Click **Start Tuning**.

5. When the tuning process is completed, a notification message is displayed. Click **OK**.

    After that, you can click a device entry in the table to view the detailed log of the tuning process.

> **Note**: If the system fails to access some devices with the **Auto Set Device Settings** option selected in the tuning options, you need to check the related credentials in the Network Settings.

> **Note**: If you repeat the tuning process, the system will retrieve data for only devices with failure records by default. To repeat the tuning process for other devices, clear the current live access result via the right-click menu.

Best Practice:

- [How to Manage Devices with Password Changed](#)

8. Cleaning Up Unassigned Site Members

Unassigned site members refer to the devices which are not assigned to any sites in your domain. If a device cannot meet any criteria of a site definition or isn't manually added to a site, it will be treated as an unassigned site member. The existence of unassigned site members would prevent the system from generating complete site maps.

<u>Desired Outcome</u>: No unassigned devices are listed in the Site Manager.

1. In the Domain Management page, click **Site** on the Start Page or select **Operations > Site Manager** from the quick access toolbar.

2. In the Site Manager, click **My Network** in the site tree and then locate **Site Definition** on the target leaf site.

3. Move the unassigned devices to the target leaf sites by using either of the following ways.

   - **Dynamic Search** — improve the existing Dynamic Search, such as criteria search and boolean expression. Click **Search**.

- **Manually Add** — click **Add Devices Manually**. Under the **Site** option, click **Unassigned** and then select target devices.
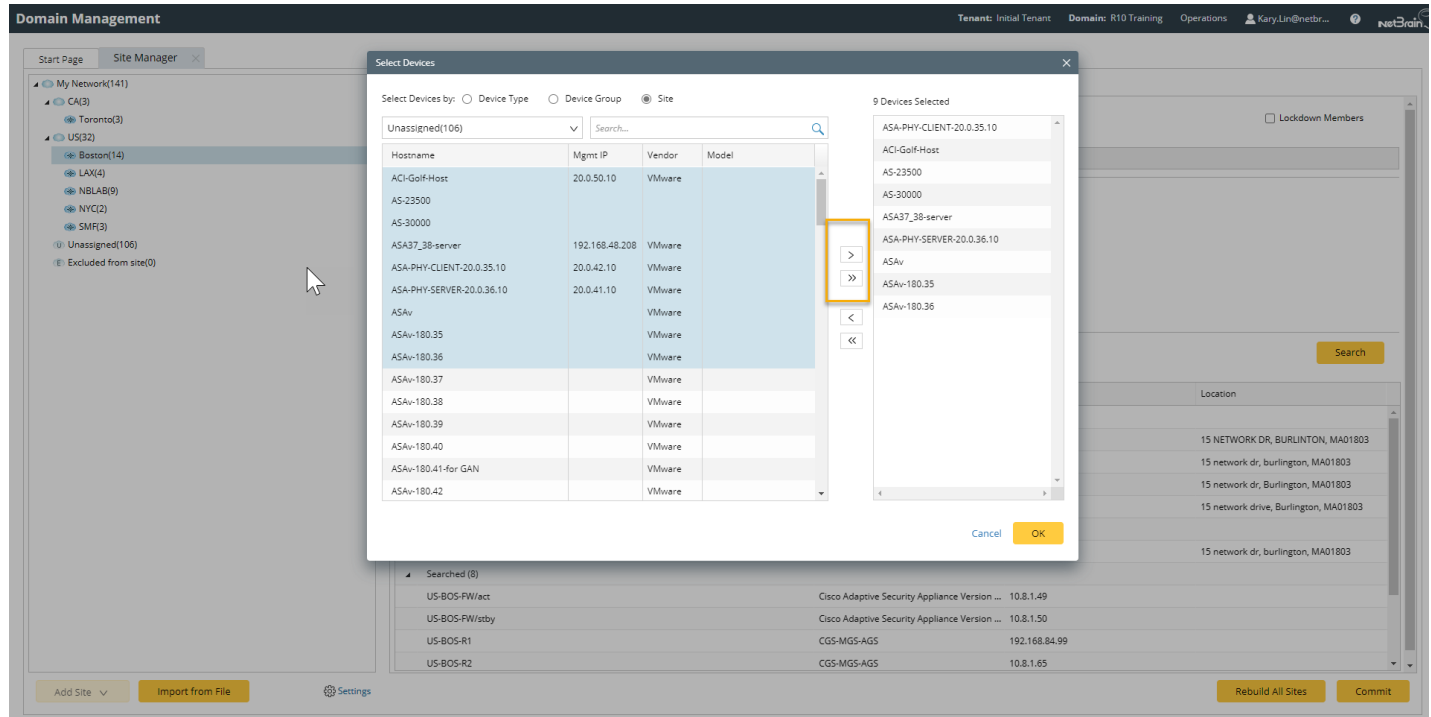
4. Repeat step 1 ~ 3 to add more site members until unassigned site members are all cleaned.

> **Tip:** If there are device types that are expected to be neither involved in any site build nor assigned to other sites, click **Settings** in the bottom of the **Site Manager** pane to select the target device types.

5. In the Site Manager, click **Rebuild All Sites** to rebuild the site topology. The **Site Member** pane opens automatically and lists the devices in the current site.

6. Click **Commit**.

Best Practice:

- How to Keep Site Maps Up-to-date

9. Browsing Map Update Result

Besides the maps created on-demand, each site or device group (excluding media) has its auto-generated map to reflect the topology among sites and devices. When network changes occur, map data is out-of-date, such as topology and data views. Through recurring benchmark tasks, you can schedule map updates with the latest benchmark data and regularly export maps to Visio files.

Desired Outcome: All map updates are successful.

The updates of the following map types can be scheduled in the system:

- Map files for sites, public/system device groups
- Public map file

To browse the result map updates, complete the following steps:

1. In the Domain Management page, select **Operations > Benchmark Tools > Update Map Manager** from the quick access toolbar.

2. On the **Update Map Manager** tab, all the maps updated through benchmark tasks are listed. You can click a link in the **Update Source** column to go to the benchmark task.

Map Name	Path	Update Source	Update Log	Map Restore History	Back Up Maps
#BGP 255	Device Group\System	Basic System Benchmark	Update Succeed Last Update Time: 15/10/2...		Yes
#EIGRP 1	Device Group\System	Basic System Benchmark			No
#OSPF 10	Device Group\System	Basic System Benchmark			No

> **Tip:** You can click **Restore All**, or point to the target entry and click **Restore** to restore maps by selecting the timestamp of backups.

10. Maintaining Data Storage

NetBrain system uses MongoDB to store all your data and files. By default, all your tenant data is saved in the MongoDB which is initially connected to NetBrain Application Server during installation.

Desired Outcome: MongoDB disk space utilization < 70%

To maintain data storage, complete either of the two following steps:

- Releasing Storage Capacity
- Enlarging Storage Capacity

Releasing Storage Capacity

The more automation tasks the system performs, the more data will be retrieved and generated. Generally, the data includes the following two types:

- Device data, such as configuration files, route tables, original CLI data, golden baseline data and parser data.
- Task data, such as Qapp/Gapp execution logs, benchmark/discovery execution logs, One-IP table entries and so on.

To customize the auto-clean rules for your domain data, do the following:

1. In the Domain Management page, select **Operations > Domain Settings > Global Data Clean Settings** from the quick access toolbar.

2. On the **Global Data Clean Settings** tab, make modifications based on your needs.

3. Click **Save**.

Enlarging Storage Capacity

When a MongoDB replica set is deployed in your system for redundancy and fault tolerance, you can store data in different MongoDB instances. For example:

- For a multi-tenant system, separate data storage by tenant.
- For a single-tenant system, separate tenant data and domain live data.

1. Log in to the System Management page.

2. In the System Management page, select the **Tenants** tab and click **Add**.

3. Configure the following settings for the tenant.

   1) Specify the following advanced options to customize data storage for better system performance.

> **Note:** These settings are only applicable if you have set up multiple MongoDB replica sets.

a) Expand **Advanced options**.

b) Select the corresponding check boxes and click **Server Settings** for configurations, such as IP address, replica set name, username, and password.

- **Store tenant data on a different server** — by default, all tenant data is stored in the default MongoDB replica set. If you specify another MongoDB replica set to store the data of this tenant, the data of all domains created under this tenant will also be stored on it.

- **Store all live data on a different server** — live data is an important part of tenant data, including device data and data view. By default, all live data is stored on the same MongoDB replica set with other tenant data.

c) Specify the License Allocation.

- Assign required nodes or ports for your network modules.

- Specify the Function Modules you can choose to apply to this tenant.

d) Specify the user privilege.

e) Click **OK** to save the settings.

2) Click **OK**.

11. Configuring System Update Settings

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

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

NetBrain Workstation Auto Update flow consists of the following steps:

1. Check and Download the Latest Version

2. Download Package from NetBrain Portal

3. Upload Package to NetBrain Workstation

4. Schedule Update

5. View Update Status

6. View Update History

Desired Outcome: The version of system resources is the latest.

Check and Download the Latest Version

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

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

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

2. Select the **Automatically check the latest version** check box.

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 Portal** 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.
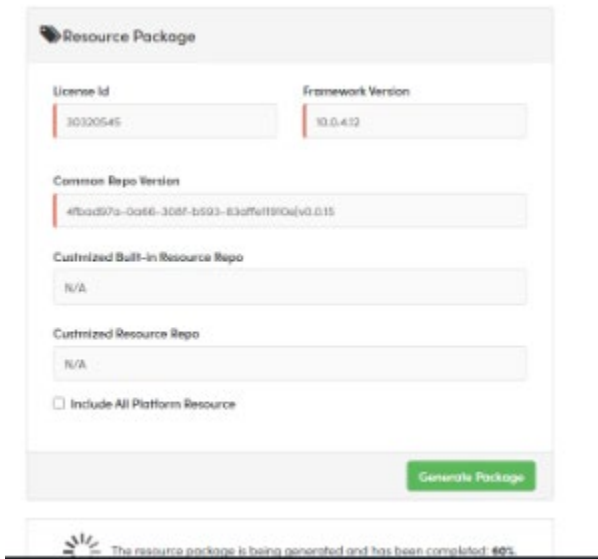4. Click the **Schedule** button to schedule the system update.

3. When this check is enabled, NetBrain Workstation will check whether a minor release, a patch, a customized built-in, a customized resource or common platform resource updates have been published since the last time check (either auto or manual check). The latest available version will be displayed with the release note.

Download Package from NetBrain Portal

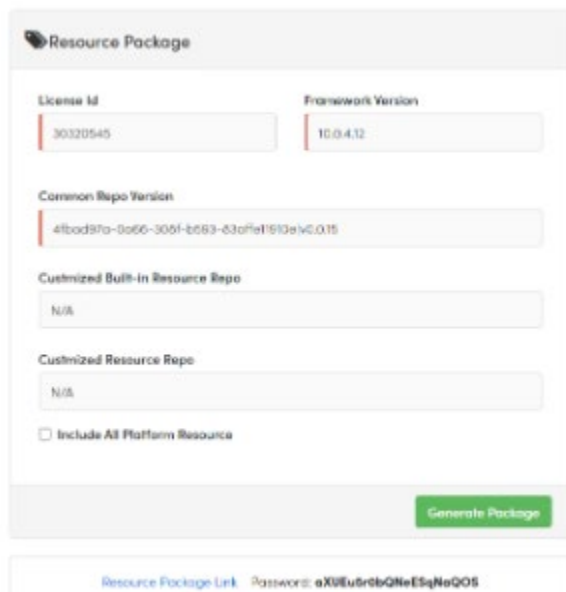Follow the steps below to download the system upgrade package from NetBrain Portal:

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

2. Confirm the required info and click Generate Package.

3. Package will be downloaded automatically to your local drive.

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

Upload Package to NetBrain Workstation

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

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

2. Click **Upload Latest Version**.

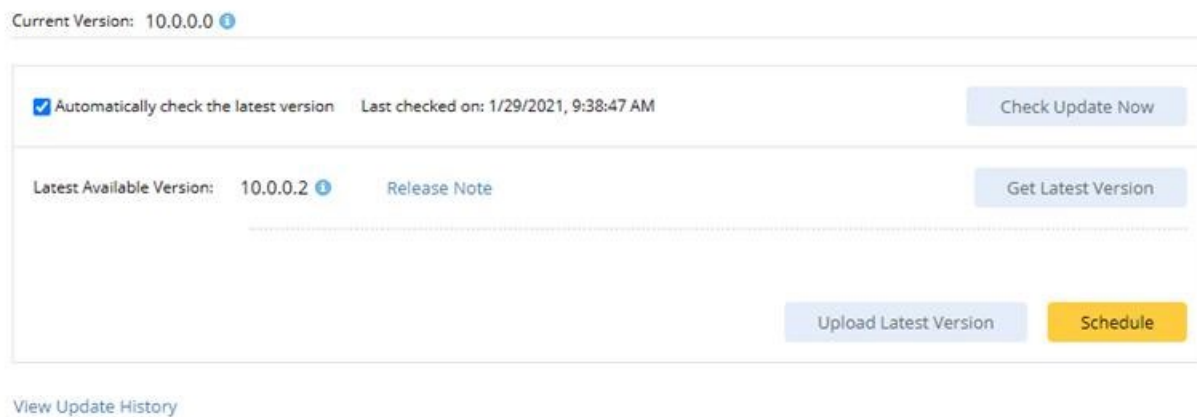3. Click **Browse** and select the system upgrade package (.zip file).

4. Enter the password and click **Upload**.
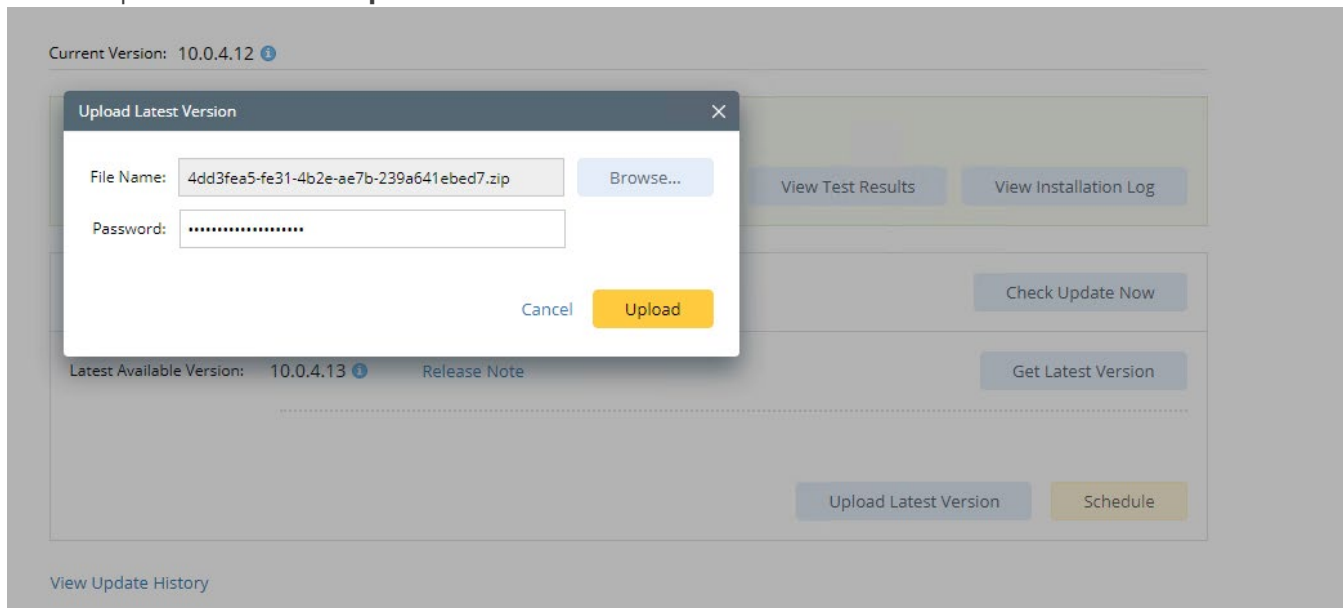
Schedule Update

Follow the steps below to schedule the system update:

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

2. Click **Schedule**.

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 Portal** 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.
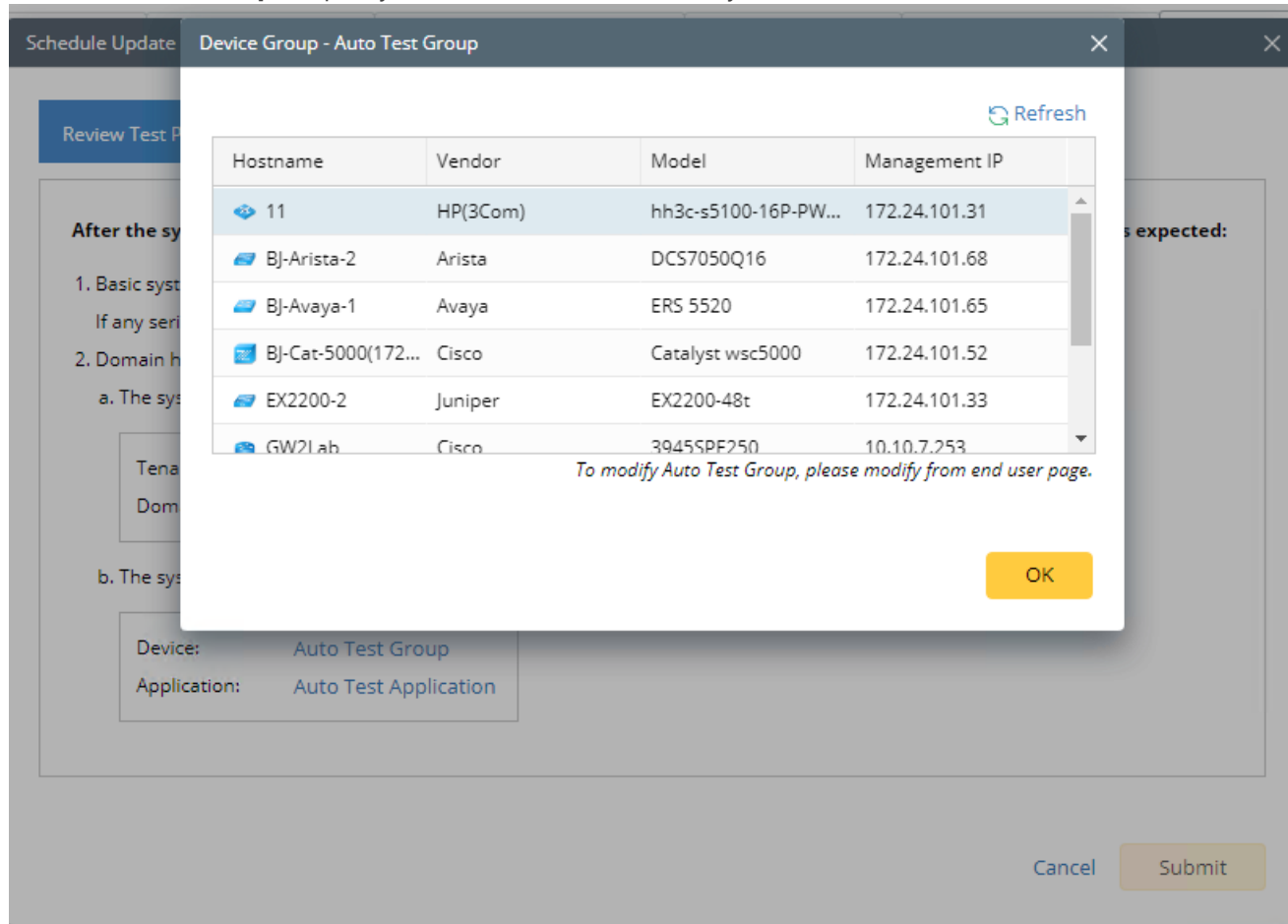
3. Review and update **Test Plan**

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

   Note: If there are more than one tenant or domain, step 1) must be completed before proceeding to step 2).

   Note: If there is only one tenant or 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.

Hostname	Vendor	Model	Management IP
11	HP(3Com)	hh3c-s5100-16P-PW...	172.24.101.31
BJ-Arista-2	Arista	DCS7050Q16	172.24.101.68
BJ-Avaya-1	Avaya	ERS 5520	172.24.101.65
BJ-Cat-5000(172...	Cisco	Catalyst wsc5000	172.24.101.52
EX2200-2	Juniper	EX2200-48t	172.24.101.33
GW2Lab	Cisco	3945SPF250	10.10.7.253

To modify Auto Test Group, please modify from end user page.

OK

Device: Auto Test Group
Application: Auto Test Application

Cancel   Submit

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

3) Click **Auto Test Application Folder** to specify the application for Data Accuracy Test.
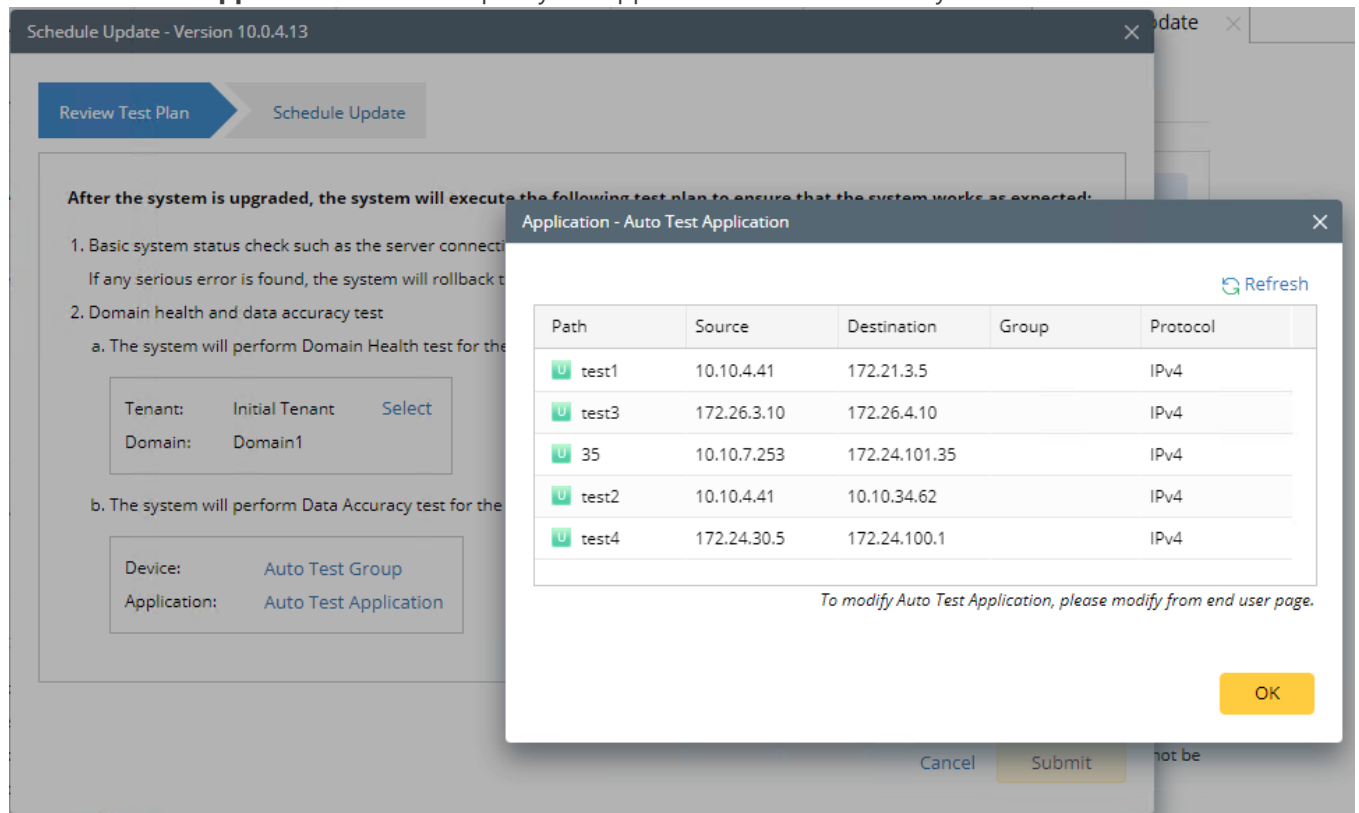
> **Note**: The last used Application Paths (up to 5 paths) will be automatically copied to the Auto Test Application Folder. You can also manually copy any existing Application Paths to the Auto Test Application Folder according to your needs.
>
> **Note**: A confirmation message will prompt if the selected tenant/domain does not have application path, you can click Yes to dismiss the message and continue with the update process.

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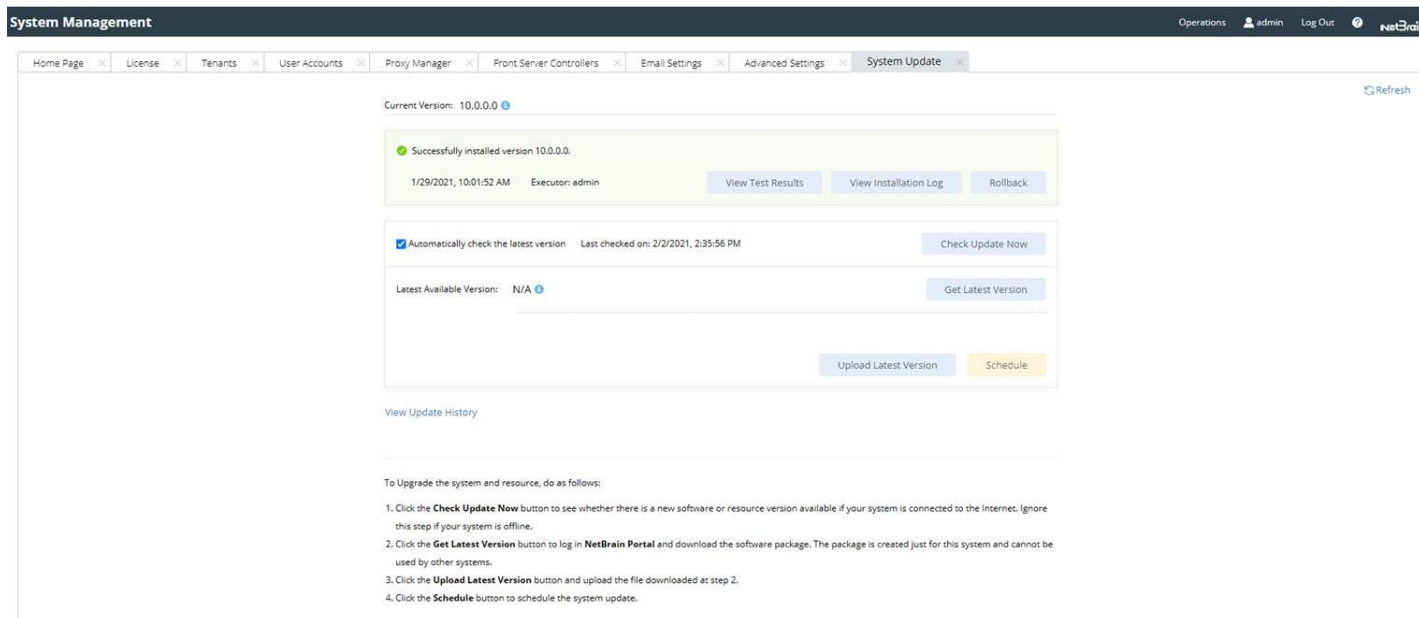

> **Tip:** You can edit or remove the system update time once it is scheduled.

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

View Update Status

There are three possible outputs of auto update:

- The system is successfully updated to the new version.

- The update fails, and the system is rolled back to the old version.

- The update fails, and the system rollback fails.

View Update History

Follow the steps below to view the update history:

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

2. Click **View Update History**.

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

- **Version:** the release number to which the system is updated.

- **Update time:** when the system finished the update.

- **Executor:** the person to schedule the update

- **Status:** one of three status in View Update Status.

- **Installation log:** the link of the installation log.

- **Test report:** the link of the test results.

Update History

Upgrade From ...	Upgrade To	Updated Time	Executor	Action	Status	Release Note	Installation Log	Test Report
10.0.2.59 ⓘ	10.0.2.102 ⓘ	Mar 3, 2021, 03:41:06 PM	admin	Upgrade	Executing	Release Note	Installation Log	Test Results

OK

12. 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.

Desired Outcome:

- Status = Connected
- Services = Green (Running)
- CPU/Mem utilization < 70%

With Service Monitor, system administrators can manage to troubleshoot a system-level issue and take remedial actions, or even optimize the system performance by performing the following operations:

- Check the status and connectivity of each server, and the performance metrics of relevant services in the system, to troubleshoot a login failure, a search failure, or an automation task execution failure.
- Analyze the trending data of system resource utilization metrics, such as CPU utilization, memory utilization, and disk/directory space usage.
- Restart NetBrain services.

Note: The Service Monitor Agent must be installed on the servers that you want to monitor.

To monitor server and service metrics:

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

2. In the Service Monitor home Page, you can monitor key server metrics, server connectivity, resource utilization, service status and so on.
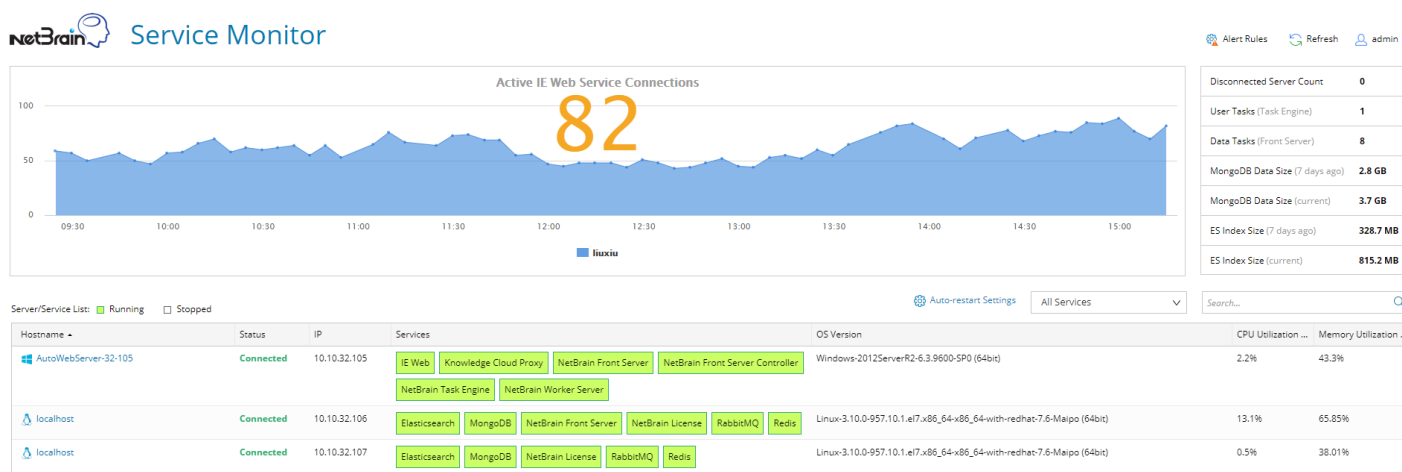
3. Customize the conditions for when to send out alert emails and take more actions for low disk space on MongoDB by clicking **Alert Rules**. See [Managing Alert Rules](#) for more details.