



# NetBrain® Integrated Edition 8.0 Domain Maintenance Guide

1.	Maintenance Overview .....	3
2.	Logging into Domain Management Page.....	4
3.	Viewing Domain Health Report .....	5
4.	Cleaning Up Domain Issues.....	6
5.	Resolving Duplicated IP and Subnet.....	7
6.	Verifying Benchmark/Discovery Result .....	9
7.	Tuning Live Access .....	12
8.	Cleaning Up Unassigned Site Members .....	14
9.	Browsing Map Update Result .....	17
10.	Maintaining Data Storage .....	18
11.	Customizing Auto-Update Schedule.....	20
12.	Monitoring Server and Service Metrics .....	22

# 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)	<a href="#">View Domain Health Report</a>	All issues reflected in the report are resolved
	<a href="#">Clean Up Domain Access Issues</a>	Resolve all managed devices under the following categories: <ul style="list-style-type: none"><li>▪ Unknown IPs</li><li>▪ Missed Devices</li><li>▪ Discovered by SNMP</li><li>▪ Unknown SNMP SysObjectID</li><li>▪ Unclassified Network Devices</li><li>▪ Hostname-Changed Devices</li></ul>
	<a href="#">Resolve Duplicated IP and Subnet</a>	IP Conflicted = 0
	<a href="#">Verify Benchmark/Discovery Task Result</a>	<ul style="list-style-type: none"><li>▪ Benchmark/discovery tasks are enabled and successfully executed</li><li>▪ All devices are selected with all applicable live data</li><li>▪ All operations are selected on Update MPLS Cloud/Build Topology/System Operations/Update Maps areas</li></ul>
	<a href="#">Tune Live Access</a>	Login = 0 Failed
	<a href="#">Clean Up Unassigned Site Members</a>	Unassigned site members = 0
	<a href="#">Browse Map Update Result</a>	All map updates are successful
System Maintenance (Monthly Tasks)	<a href="#">Maintain Data Storage</a>	MongoDB disk space utilization < 70%
	<a href="#">Customize Auto-Update Schedule</a>	Current resource = Latest version
	<a href="#">Monitor Server and Service Metrics</a>	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**.
4. Click the domain name from the quick access toolbar and select **Manage Domain**.

Current Domain: **BVT\_DB2DOM\_533b4** [Manage Domain](#)

Tenant: **Initial Tenant**  [Refresh](#)

Tenant Name	Domain Name	Maximum Nodes	Description	Creator
Initial Tenant	Toronto_Domain	1000 (161 used)		jz
Initial Tenant	BJ_Domain	1000 (159 used)		zhao
Initial Tenant	Domain1	1000 (2 used)		li
Initial Tenant	RACK	2000 (146 used)		fan

[New Domain](#) [Cancel](#) [Apply](#)

**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.

Domain Management Tenant: Initial Tenant Domain: domain1 Operations kang

Start Page Domain Health Report

Report Generated Time: 5/25/2020 11:25:10 AM Refresh Create Health Report

Basic Network Settings: 5 need attention Discovery Status: 5 need attention Path: 2 failed Others: 12 need attention Export

**Driver Associated Device:**  
21 Driver Applied, 234 Devices, 6794 Interfaces

Device Driver	Associated Device Count
Cisco IOS Switch	113
End System	62
Cisco Router	21
Cisco ASA Firewall	12
Cisco Nexus Switch	6
Arista Switch	2
Avaya Switch	2
Juniper EX Switch	2
Unclassified Device	2
3Com-HP Comware Switch	1

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:
  - **[Discovered by SNMP Only](#)** — the devices accessed by SNMP but failed to be accessed via SSH/Telnet.
    - **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.
  - **[Unknown IP](#)** — the IP addresses that cannot be accessed via Telnet/SSH and SNMP in the **Discover via Seed Routers** method during a discovery.
    - **Desired Outcome:** Fix all known IPs with correct Telnet/SSH/SNMP in this list.
  - **[Missed Devices](#)** — the devices existing in the current domain but failed to be verified during a discovery.
    - **Desired Outcome:** Fix device access issues or remove decommissioned devices in this list to bring the number of devices down to 0.
  - **[Unclassified Network Devices](#)** — the devices whose types are marked as **Unclassified Device** in the Vendor Model table, or not recognized due to unknown sysObjectIDs.
    - **Desired Outcome:** Re-discover all unclassified devices once OIDs are added to properly classify network devices in this list to decrease the number of devices down to 0.
  - **[Unknown SNMP SysObjectID](#)** — the devices whose SysObjectIDs are not defined in the Vendor Model table.
    - **Desired Outcome:** Add all unknown OIDs in this list to the vendor model table to decrease the number down to 0.
  - **[SH Fingerprint Check Failed](#)** — the devices whose current fingerprint keys are different with the latest ones retrieved during live access.
    - **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.
    - **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:

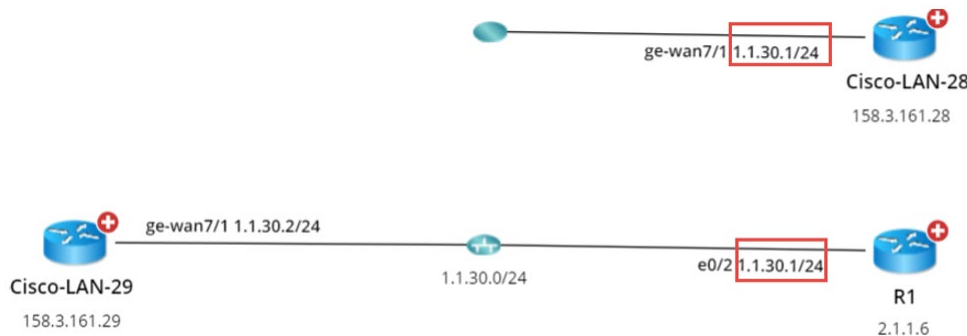
- If two interfaces are configured with the same IP address, but with different VRFs, then two zones named after the VRFs will be created automatically after the IPv4 L3 topology is built, and these two interfaces will be moved to the corresponding zone according to its configured VRF. The system automatically 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		1.1.30.1/24	Yes		
	Cisco-LAN-28	GE-WAN7/1	1.1.30.2/24	No		

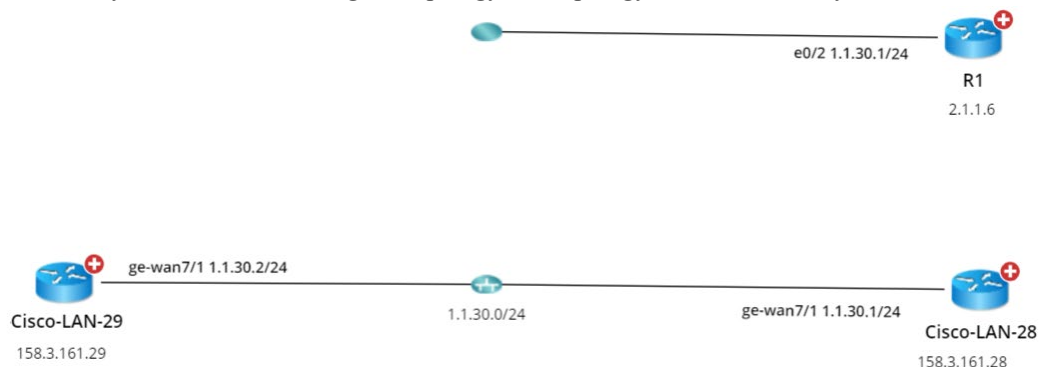
**Tip:** If a lot of duplicated subnets are detected in the Default Zone, you can quickly search them within the **Search bar**. Use semicolons to separate the multiple items.

- 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

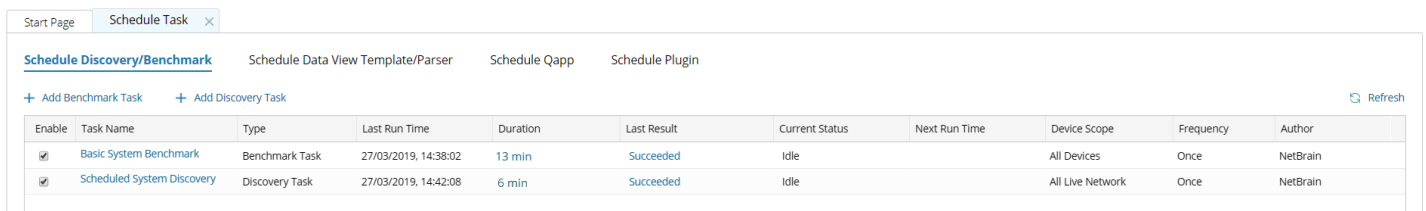
It is essential to have a successfully executed system benchmark to keep domain data up-to-date, as it does not only benchmark your network but also update network topologies, re-calculate sites, rebuild visual space, and update maps.

### 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.

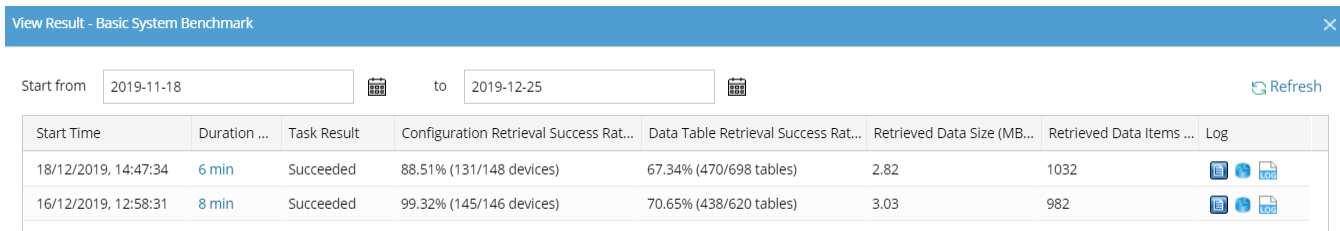


The screenshot shows the 'Schedule Task' window with a tab for 'Schedule Discovery/Benchmark'. Below the tabs are links to '+ Add Benchmark Task' and '+ Add Discovery Task', and a 'Refresh' button. A table lists the scheduled tasks:

Enable	Task Name	Type	Last Run Time	Duration	Last Result	Current Status	Next Run Time	Device Scope	Frequency	Author
<input checked="" type="checkbox"/>	Basic System Benchmark	Benchmark Task	27/03/2019, 14:38:02	13 min	Succeeded	Idle		All Devices	Once	NetBrain
<input checked="" type="checkbox"/>	Scheduled System Discovery	Discovery Task	27/03/2019, 14:42:08	6 min	Succeeded	Idle		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.



The screenshot shows the 'View Result - Basic System Benchmark' dialog. It has a date range selector from '2019-11-18' to '2019-12-25' and a 'Refresh' button. Below is a table of execution logs:

Start Time	Duration ...	Task Result	Configuration Retrieval Success Rat...	Data Table Retrieval Success Rat...	Retrieved Data Size (MB...	Retrieved Data Items ...	Log
18/12/2019, 14:47:34	6 min	Succeeded	88.51% (131/148 devices)	67.34% (470/698 tables)	2.82	1032	
16/12/2019, 12:58:31	8 min	Succeeded	99.32% (145/146 devices)	70.65% (438/620 tables)	3.03	982	

## ▼ 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: 2019/8/19 下午4:53:32

Date & Time	Messages	Total Time Spent
18/12/2019, 14:47:35	Begin: retrieve devices data.	
18/12/2019, 14:52:11	End: retrieve devices data.	0 hrs 4 mins 36 secs
18/12/2019, 14:52:11	There are no MPLS Cloud devices in your domain.	
18/12/2019, 14:52:11	Begin: update Global Endpoint index.	
18/12/2019, 14:52:13	End: update Global Endpoint index.	0 hrs 0 mins 1 secs
18/12/2019, 14:52:13	Begin:build topology	
18/12/2019, 14:52:13	Try to build topology IPv4 L3 Topology	
18/12/2019, 14:52:23	End: build IPv4 L3 Topology with 423 links.	0 hrs 0 mins 10 secs
18/12/2019, 14:52:23	Try to build topology IPv6 L3 Topology	

Refresh

☐ Only show failed logs

## ▼ 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: 27/03/2019, 14:38:02

3 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...
 NY_DIS_1	Cisco Router	11	Failed	Succeeded	Succeeded	Failed	Succeeded
 Sanjose_Core	Cisco Router	15	Failed	Succeeded	Succeeded	Succeeded	Succeeded
 BSTX_Core	Cisco Router	16	Failed	Succeeded	Succeeded	Succeeded	Succeeded

Live Access Log of NY\_DIS\_1:

09:39:15 Begin data retrieving task  
09:39:16 Prepare retrieving command.  
09:39:16 Telnet to device 172.24.31.66 via FS1(10.10.32.105)  
09:39:16 Telnet to device 172.24.31.66 successfully via FS1(10.10.32.105)  
09:39:16 Return from Device:[ Username:]  
09:39:16 Sending Username:netbrain


Progress: (Not Running)

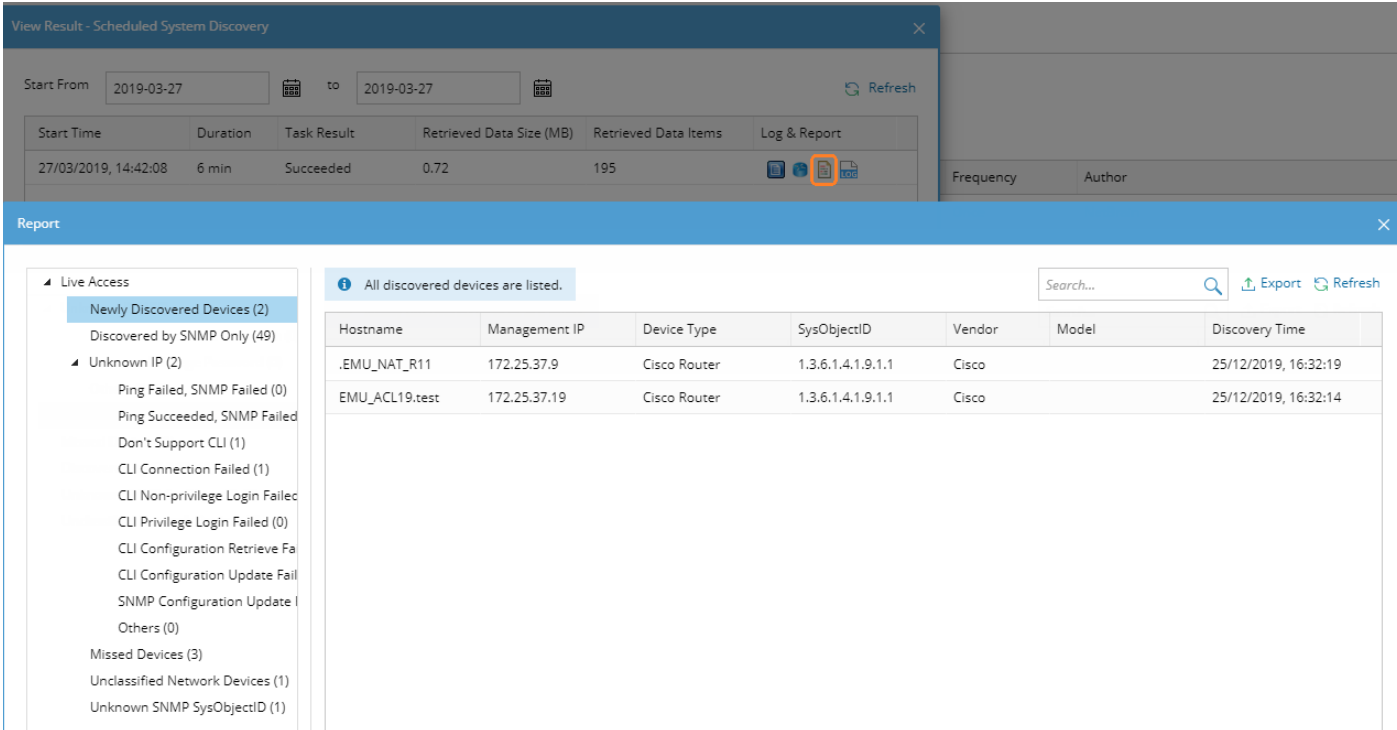
Close

**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.



The screenshot shows the 'View Result - Scheduled System Discovery' window. The top section displays the start time (2019-03-27) and duration (6 min). The task result is 'Succeeded'. The retrieved data size is 0.72 MB, and the retrieved data items are 195. The report is titled 'Report' and shows a list of discovered devices. The left sidebar lists categories like '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 Failed', '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)', and 'Unknown SNMP SysObjectID (1)'. The main table lists the discovered devices with columns: Hostname, Management IP, Device Type, SysObjectID, Vendor, Model, and Discovery Time.

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. 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.

Domain Management

Tenant: Initial Tenant Domain: BJRACK Operations kangshaotun

Start Page Tune Live Access

Check the reachability of live devices using the credentials defined in Network Settings.

All Devices Device Groups All Device Groups, My ... Start Tuning Options Network Settings 100 Items Search Device Name...

	Device Name	Management IP	Management Interface	Ping	SNMP RO	SysObjectID	Telnet/SSH	Login	Enable	SNMP Hostname	Vendor	Model	Front Server/Front Server Group
<input checked="" type="checkbox"/>	BJ-R3												
<input checked="" type="checkbox"/>	BJ_Acc_SW1												
<input checked="" type="checkbox"/>	BJ_Acc_SW2												
<input checked="" type="checkbox"/>	BJ_Acc_SW6												
<input checked="" type="checkbox"/>	BJ_Acc_SW4												
<input checked="" type="checkbox"/>	BJ_Dis_SW1												
<input checked="" type="checkbox"/>	BJ_Dis_SW2												
<input checked="" type="checkbox"/>	BJ_L2_Core_3												
<input checked="" type="checkbox"/>	BJ_L2_Core_4												
<input checked="" type="checkbox"/>	BJ_L2_Core_5												
<input checked="" type="checkbox"/>	BJ_L2_Core_6												
<input checked="" type="checkbox"/>	BJ_L2_test_1												

**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**.

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

4. Click **Start Tuning**.

- 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.

Start Page

Tune Live Access

Check the reachability of live devices using the credentials defined in Network Settings.

All Devices

Device Groups

All Device Groups, My ...

Start Tuning

Options

Network Settings

100 Items

Search Device Name...

	Device Name	Management IP	Management Interface	Ping	SNMP RO	SysObjectID	Telnet/SSH	Login	Enable	SNMP Hostname	Vendor	Model	Front Server/Front Server Group
<input checked="" type="checkbox"/>	BJ-R3	172.24.10.18	FastEthernet0/1.10	Succeeded	AuthNoPrivauthmd		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	2811	Iluxiu
<input checked="" type="checkbox"/>	BJ_Acc_SW1	172.24.101.21	Vlan10	Succeeded	nb		Succeeded	Failed		Unchanged	Cisco	catalyst295024	Iluxiu
<input checked="" type="checkbox"/>	BJ_Acc_SW2	172.24.101.22	Vlan10	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst295024	Iluxiu
<input checked="" type="checkbox"/>	BJ_Acc_SW6	172.24.101.26	Vlan10	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst295024	Iluxiu
<input checked="" type="checkbox"/>	BJ_Acc_SW4	172.24.101.24	Vlan10	Succeeded	netbrain		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst295024	Iluxiu
<input checked="" type="checkbox"/>	BJ_Dis_SW1	172.24.101.11	Vlan10	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst295024	Iluxiu
<input checked="" type="checkbox"/>	BJ_Dis_SW2	172.24.101.12	Vlan10	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst295024	Iluxiu
<input checked="" type="checkbox"/>	BJ_L2_Core_3	172.24.101.4	Vlan10	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst37xxStac	Iluxiu
<input checked="" type="checkbox"/>	BJ_L2_Core_4	172.26.4.30	FastEthernet2/0/3	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst37xxStac	Iluxiu
<input checked="" type="checkbox"/>	BJ_L2_Core_5	172.24.101.6	Vlan10	Succeeded	nb		Failed			Unchanged	Cisco	catalyst356048T	Iluxiu
<input checked="" type="checkbox"/>	BJ_L2_Core_6	172.24.101.7	Vlan10	Succeeded	nb		Failed			Unchanged	Cisco	catalyst356048T	Iluxiu
<input checked="" type="checkbox"/>	BJ_L2_test_1	172.24.33.10	Vlan10	Succeeded	netbrain		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst37xxStac	Iluxiu
<input checked="" type="checkbox"/>	BJ_core_3550	172.24.10.34	Vlan10	Succeeded	netbrain		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	catalyst355024	Iluxiu
<input checked="" type="checkbox"/>	BST	172.24.10.250		Succeeded	nb		Failed			Unchanged	Cisco	2503	Iluxiu
<input checked="" type="checkbox"/>	BST.POP1	172.24.32.5	Ethernet1	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	2514	Iluxiu
<input checked="" type="checkbox"/>	BSTX.Core	172.24.255.5	Loopback20000	Succeeded	nb		Succeeded	Succeeded	Succeeded	Unchanged	Cisco	2621	Iluxiu

13:29:26 Begin tune process  
13:29:26 Ping [172.24.101.24] via Front Server (Iluxiu); Succeeded  
13:29:26 Send RO = [netbrain][version:v2c] to [172.24.101.24] via Front Server (Iluxiu); Succeeded  
13:29:27 Retrieving [172.24.101.24]'s hostname, vendor and model via Front Server (Iluxiu); Succeeded  
13:29:27 Telnet to device 172.24.101.24 via Front Server (Iluxiu)  
13:29:27 Telnet to device 172.24.101.24 successfully via Front Server (Iluxiu)  
13:29:27 Return from Device:[ username:]  
13:29:27 Sending Username:netbrain  
13:29:27 Return from Device:[ Password:]  
13:29:27 Sending Password:\*\*\*\*\*  
13:29:30 Return from Device:[BJ\_Acc\_SW4]

**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.

**Desired Outcome:** No unassigned devices are listed in the Site Manager.

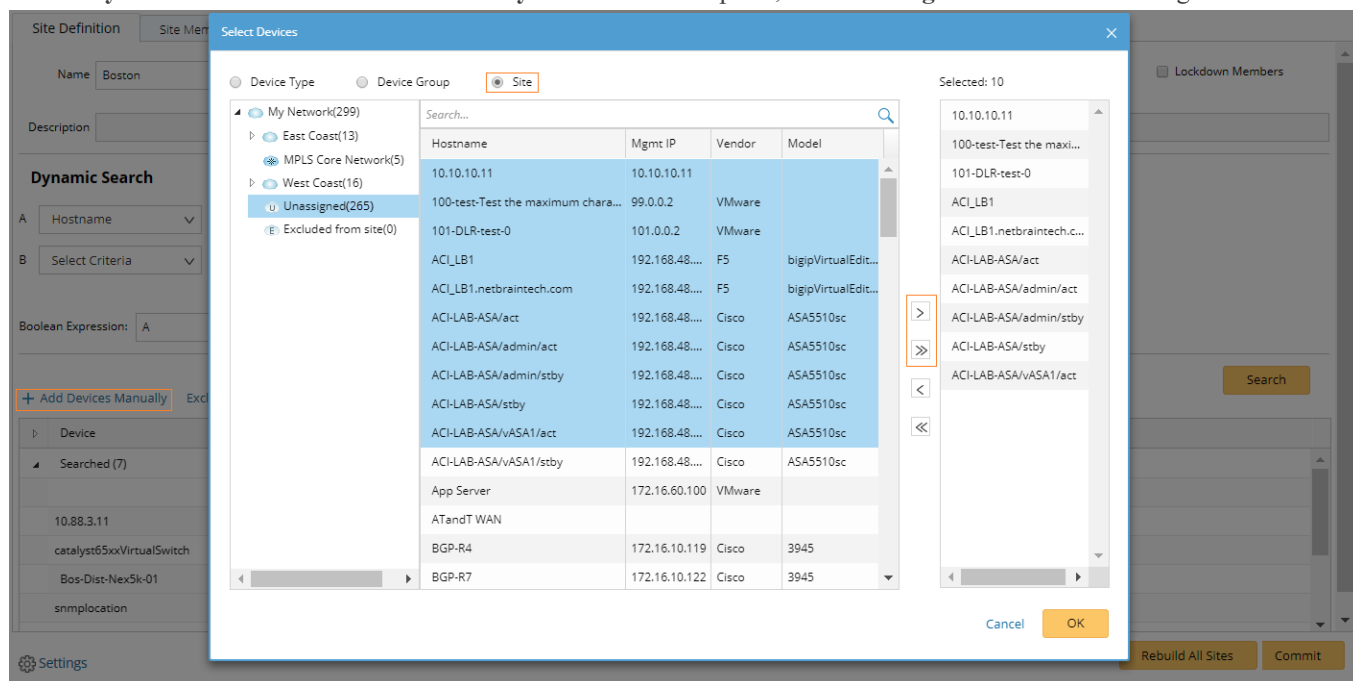
1. In the Domain Management page, click **Site** on the Start Page or select **Operations > Site Manager** from the quick access toolbar.
2. In the Site Manager, click **My Network** in the site tree and then locate **Site Definition** on the target leaf site.
3. Move the unassigned devices to the target 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**.

The screenshot displays the NetBrain Site Manager interface. On the left, a tree view shows the network hierarchy: My Network(299) > East Coast(13) > Boston(7). The 'Boston(7)' site is selected. The main panel shows the 'Site Definition' tab for the 'Boston' site. A 'Dynamic Search' section is active, showing a search criteria dropdown menu with options: Device Property, Interface Property, Module Property, Config File, and Front Server. The search results table below shows 7 devices found:

Device	Model	Management IP	Location
Searched (7)			
Bos-ask01-2960-01	catalyst296048TT	10.88.3.11	
Bos-Core-6500	catalyst65xxVirtualSwitch	10.88.1.129	
Bos-Dist-Nex5k-01	5548UP	10.88.3.12	snmplocation

At the bottom of the interface, there are buttons for 'Add Site', 'Import from File', 'Settings', 'Rebuild All Sites', and 'Commit'.

- **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**.

**Domain Management** Tenant: Initial Tenant Domain: ie71\_domain\_preview Operations kangshaotun NetBrain

Start Page Site Manager

My Network(299)  
East Coast(13)  
Boston(7)  
New York City(3)  
Ott(3)  
MPLS Core Network(5)  
West Coast(16)  
Unassigned(265)  
Excluded from site(0)

**Site Definition** Site Members

Name: Boston [Site Properties](#) ☐ Lockdown Members

Description:

**Dynamic Search**

A: Hostname Contains ^bos

B: Select Criteria

Boolean Expression: A

[+ Add Devices Manually](#) [Exclude Devices](#) [Search](#)

Device	Model	Management IP	Location
Searched (7)			
Bos-askt01-2960-01	catalyst296048TT	10.88.3.11	
Bos-Core-6500	catalyst65xxVirtualSwitch	10.88.1.129	
Bos-Dist-Nex5k-01	5548UP	10.88.3.12	snmplocation

[Add Site](#) [Import from File](#) [Settings](#) [Rebuild All Sites](#) [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.

Start Page

Schedule Task

Update Map Manager

Update Source: Basic System Benchma...

Map Type: ☒ Site Maps ☒ Device Group Maps ☒ Public Maps 

Restore All

Search...

Refresh

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

2) Click **OK**.

## 11. Customizing Auto-Update Schedule

Knowledge Cloud is a centralized resource base housing various types of regular/customized NetBrain resources. NetBrain IE system can download any NetBrain resources (that apply to your specific IE version) from Knowledge Cloud constantly. These [resources](#), once downloaded, will be deployed automatically in your IE system.

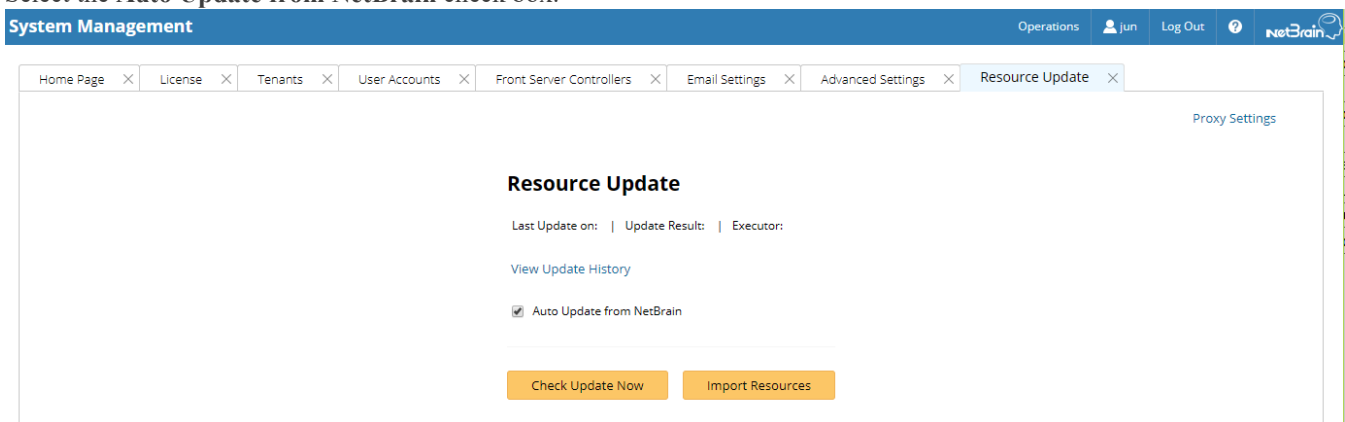
There are three ways to perform a resource update in your IE system.

- **Auto-update Resources (Recommended)** — the system will fetch the latest resources from Knowledge Cloud constantly (twice per day between 12AM and 3AM, 12 PM and 3 PM at local time zone) in a fully automatic manner. See [Auto-updating Resources](#) for more details.
- **Manually Trigger Resource Update** — manually initiate the auto-updating process and apply the latest resources (if any) immediately to the system. See [Manually Triggering Resource Update](#) for more details.
- **Manually Import Resources** — manually upload the latest resource package into the system when your servers are not allowed to access the Internet. See [Manually Importing Resources](#) for more details.

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

### Auto-Updating Resources

1. In the System Management page, select **Operations > Resource Update**.
2. Select the **Auto Update from NetBrain** check box.



**Tip:** If your Web Server has no Internet access, you can click **Proxy Settings** to set up a proxy server to access the internet.

### Manually Triggering Resource Update

1. In the System Management page, select **Operations > Resource Update**.
2. Click **Check Update Now** to see if there is any available new resource package and apply the updates to the system if any.

**Note:** Once the button is clicked, any available updates will be downloaded and installed automatically.

**Tip:** If your Web Server has no Internet access, you can click **Proxy Settings** to set up a proxy server to access the internet.

## Manually Importing Resources

---

1. In the System Management page, select **Operations > Resource Update**.
2. Check the last update time and result to see if your resources need an upgrade.

**Tip:** To check historical update records and results, click **View Update History**.

3. Click **Import Resources**, select the new resource package you obtained from [NetBrain Support Team](#).

## Resource List

---

The following resources can be auto-updated by Knowledge Cloud:

- Driver/Device Type/Vendor Model Table
- Qapp/Gapp/Parser Library
- Runbook Template/(Default) Data View Template
- Device Group/Device Icon/Image/Media Type/Topology Link Type (IPv4, IPv6, etc.)
- GDR Properties/Interface Type Translation
- Tech Spec/Schema/Visual Space/Network Tree Category and View
- Platform Plugin/Global Python Scripts (including Path Scripts)
- SPOG URL/API Adapter
- Variable Mapping/Global Variable
- Golden Baseline Dynamic Analysis Logic

## 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%

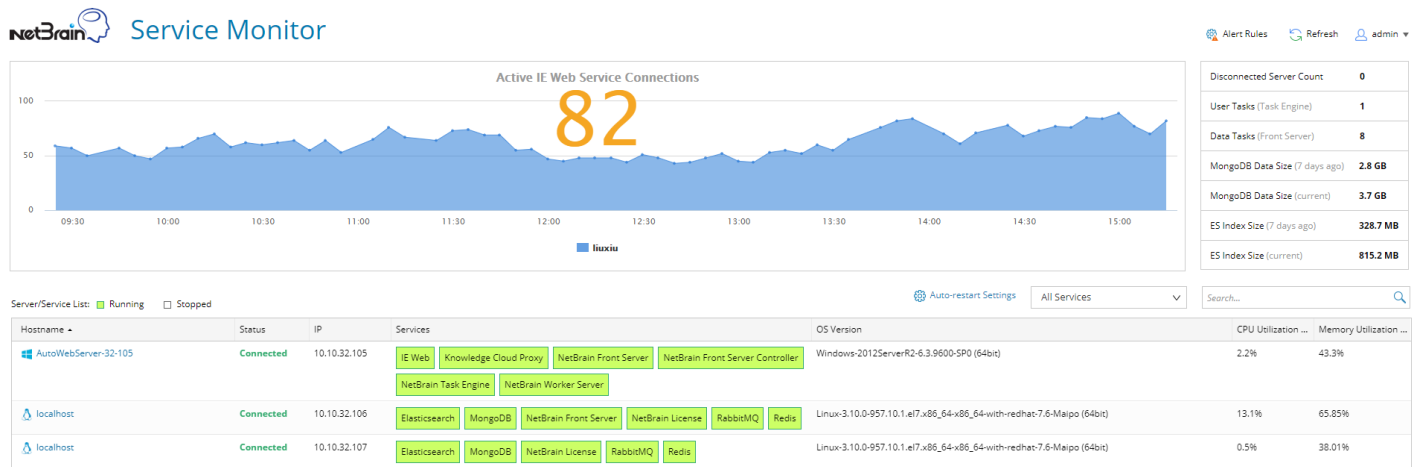
With Service Monitor, system administrators can manage to troubleshoot a system-level issue and take remedial actions, or even optimize the system performance by performing the following operations:

- 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 **MongoDB Disk Alert Rules**. See [Managing Alert Rules](#) for more details.