

# **RLCatalyst Command Center User Manual**

Relevance Lab India Pvt Ltd  
July 2018

Ver 2.6

## **Introduction**

Welcome to the RLCatalyst Command Center user-guide. This user-guide is designed to provide documentation for users who will be installing, administering and using the Command Center product.

## **What is RLCatalyst Command Center**

RLCatalyst Command Center is a cloud-based software product that can be used to monitor services and their underlying infrastructure. The product provides early detection and warning of



problems in the targeted services or infrastructure. The product also provides capabilities to integrate problem tickets and capture incident details which can help to narrow down root cause.

## Getting Started

You will be provided the following pieces of information in your starter kit:

URL: <application URL>  
Company: \_\_\_\_\_  
User: \_\_\_\_\_  
Password: \_\_\_\_\_

Keep this information handy as you go through this guide and configure your system.

## Planning your deployment

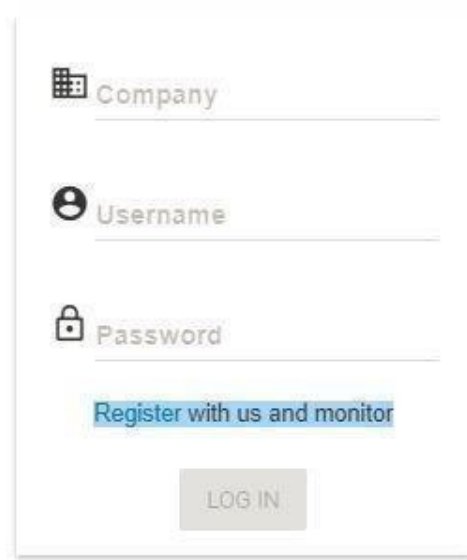
RLCatalyst Command Center is capable of multi-tenancy. Using the same instance of the software, you can create several **tenants**. Each tenant can configure his own machines for monitoring. Each tenant can also configure his own cloud accounts and get an independent view of his cloud assets.

The landlord can create new tenants in the system.

## Creating your first tenant

To plan the creation of a new tenant, use the planning sheet in **Appendix A** to collect all the information required upfront. Keep the sheet handy as you go through the following steps.

Open a browser (we recommend Chrome or Firefox). Enter the Application URL provided. The login page should open.

A login form with a light gray border and a white background. It contains three input fields: "Company" with a building icon, "Username" with a person icon, and "Password" with a lock icon. Below these fields is a blue link that says "Register with us and monitor". At the bottom is a gray button labeled "LOG IN".

Company

Username

Password

[Register with us and monitor](#)

LOG IN

*Image 1 - Login Page*

To register a tenant, click on the Register link which is available on the login page & application will display Register screen to the user.

A registration form with four input fields: "Company" (with a building icon), "Username" (with a person icon), "Email" (with an envelope icon), and "Password" (with a lock icon and a help icon). Below the fields is a "CREATE ACCOUNT" button.

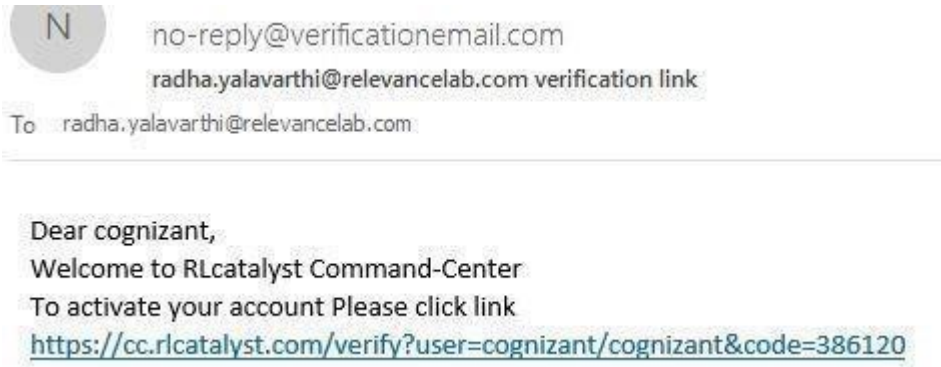
*Image 2 - Register Account Page*

Use details from **Appendix A** for Company Name, User Name, Email & set the Password as per Password policy. Click on Create Account button. You will see a *Thank You* screen confirming that a verification email has been sent to the email address registered.



*Image 3 - Verification email sent*

Check the verification email delivered to the registered email address & click on the verification link to activate the account. On successful validation, tenant will be allowed to login into the Command Center.



Image

4 - Verification email (sample)

## Logging in as a tenant

Open a browser (we recommend Chrome or Firefox). Enter the application URL provided. The login page should open. On the login page, fill the Company, User and Password fields as captured in **Appendix A**. Then click the Login button. You will see the landing page.

- Business Service Status View – by default this will not show any data. You will need to configure business services following the instructions in this guide.
- Service Health – providing a quick way of viewing at a glance, if any of the linked services (across BSM's) are in alarm state (Yellow & Red). By clicking on critical/warning service card, the system shall navigate to the Services page and should show the Service and Nodes tabs related to selected service.
- ServiceNow Ticket Snapshot – by default this will not show any data. You will need to configure a Service Now account following the instructions in this guide.
- BOT's Summary (Total)- We need to configure a Catalyst Account to view the count of Bot's summary.



Image 5 - Dashboard View of Business Services

## Historical BSM Health Indicator:

Historical BSM Health Indicator gives you the ability to see the trend of the BSM over last 30 days as a consolidated view. Using this view, the user can then navigate to specific outage view of interest.

The view can be available with a “Trend Icon” on Top-Left of BSM View and clicking that can show the Consolidated status of all BSM over last 30 days with appropriate status.

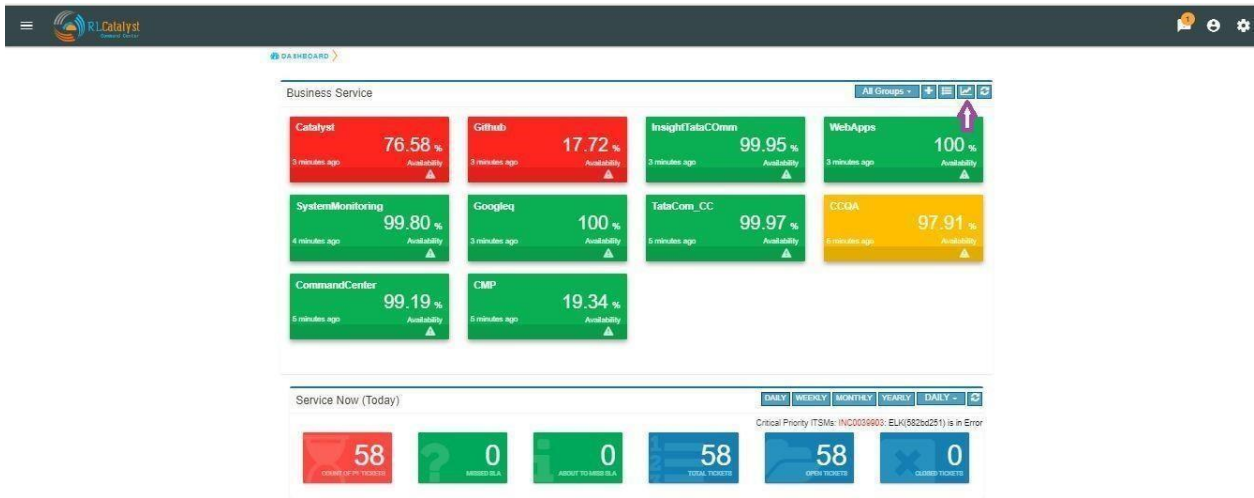


Image 6 - Trend Icon

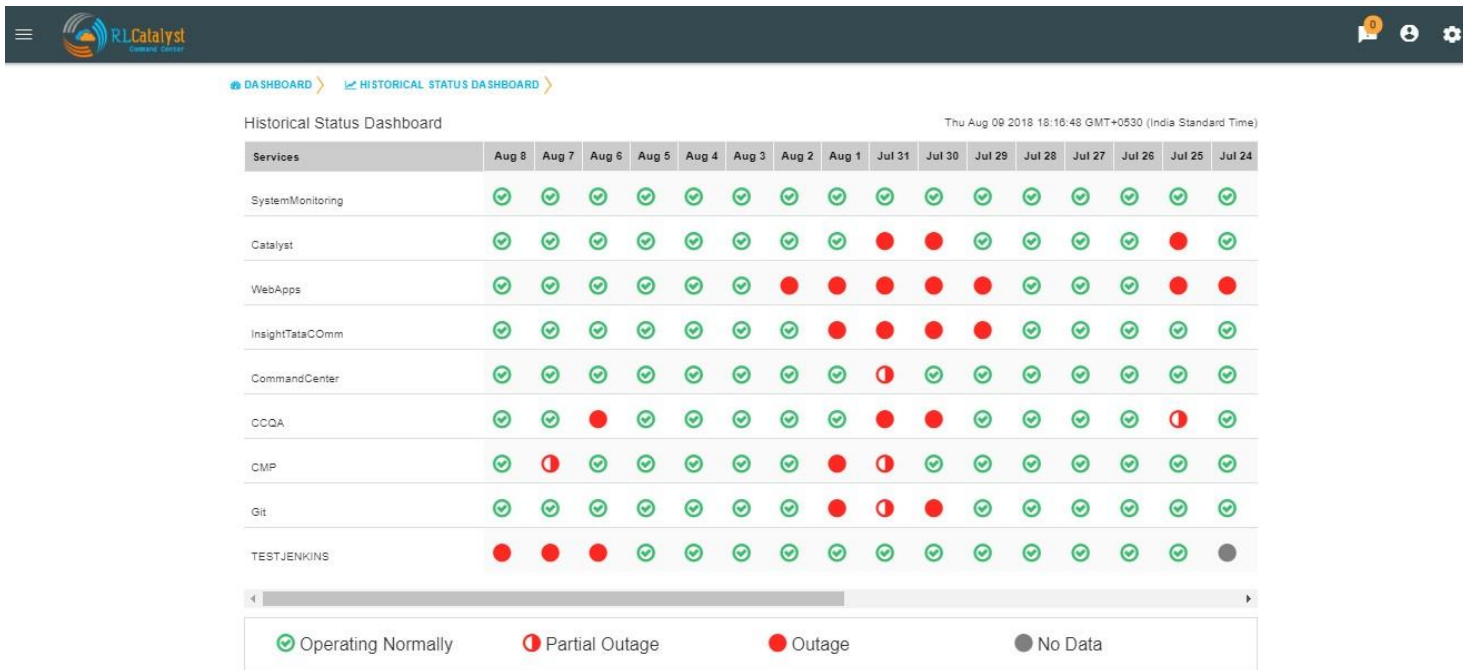


Image 7 - Historical Status Dashboard

Clicking the link of Outage (Red) or Partial Outage available in the Historical Status Dashboard will take you to the appropriate Outage Drill-down page

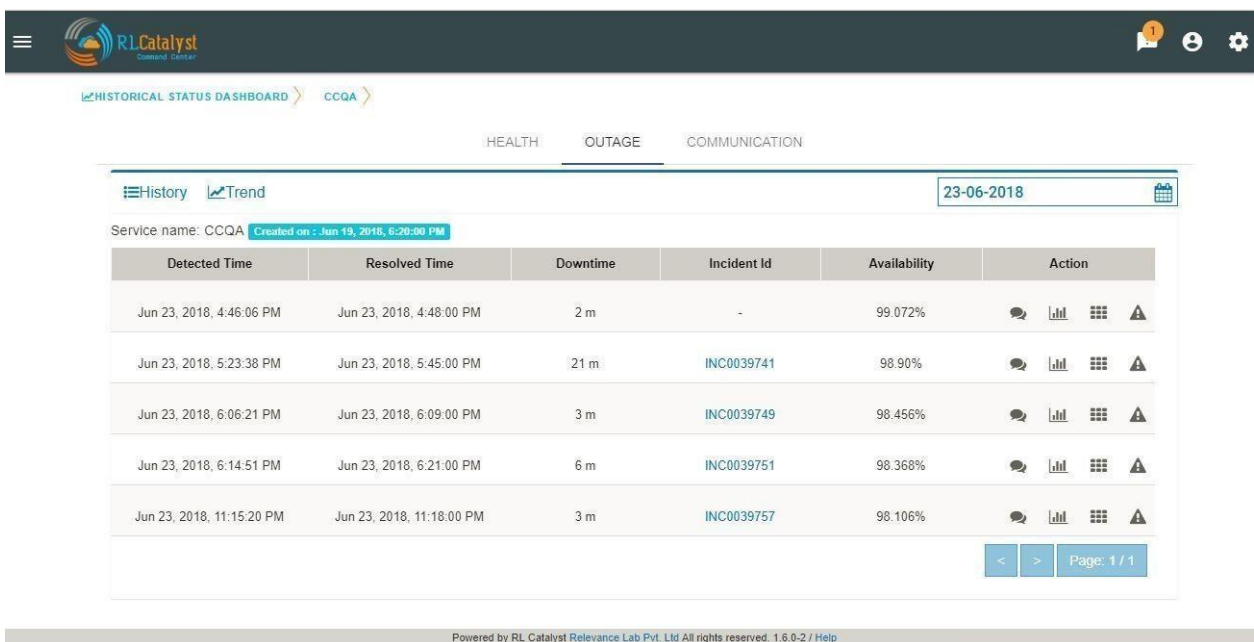


Image 8 - Outage Drill-down page

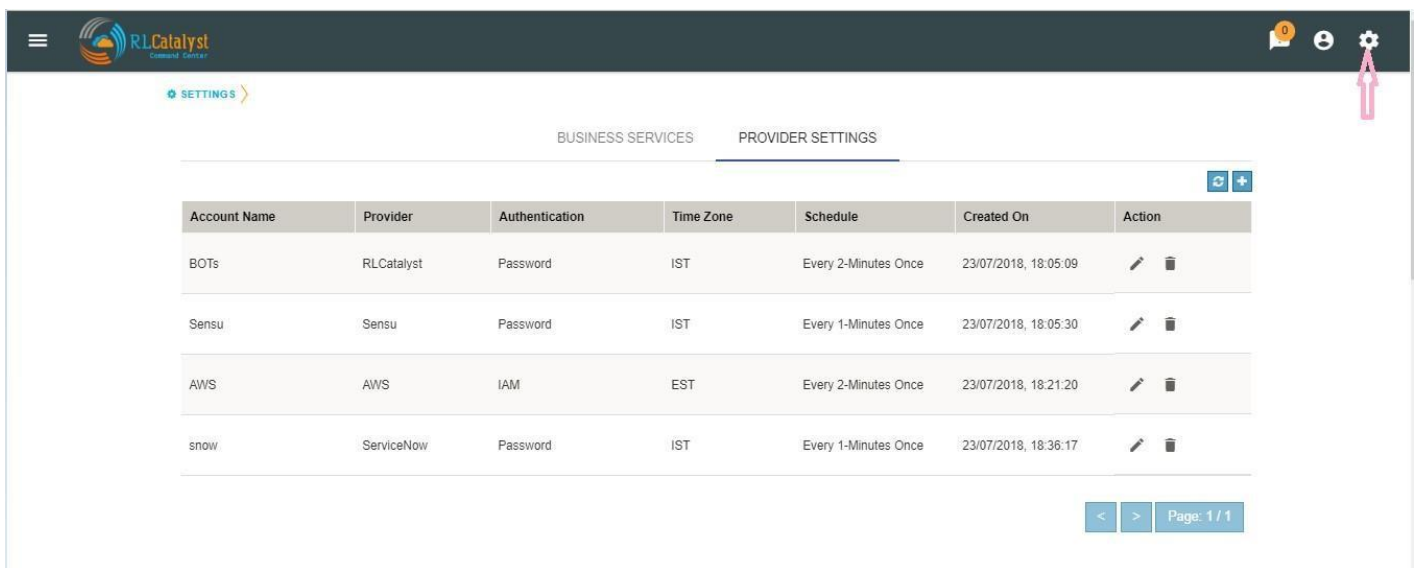


## Configuring Cloud Credentials









RLCatalyst Command Centre gives you the ability to view all your cloud assets (spanning across providers and accounts) in one place. These assets include:

- Virtual Machines
- ELBs
- Security Groups
- Networks

Configure your Cloud Account Details in the Command Centre Settings to view all your cloud assets in one place. Command Centre collects the information from the configured cloud account periodically. You can configure the interval in which this information refreshes.



The screenshot shows the RLCatalyst Command Centre interface. The top navigation bar includes a menu icon, the RLCatalyst logo, and user profile icons. The 'SETTINGS' section is active, and the 'PROVIDER SETTINGS' tab is selected. Below the tabs is a table of configured providers. A pink arrow points to the settings gear icon in the top right corner.

Account Name	Provider	Authentication	Time Zone	Schedule	Created On	Action
BOTs	RLCatalyst	Password	IST	Every 2-Minutes Once	23/07/2018, 18:05:09	 
Sensu	Sensu	Password	IST	Every 1-Minutes Once	23/07/2018, 18:05:30	 
AWS	AWS	IAM	EST	Every 2-Minutes Once	23/07/2018, 18:21:20	 
snow	ServiceNow	Password	IST	Every 1-Minutes Once	23/07/2018, 18:36:17	 

Page: 1 / 1

Image  
9 - Settings

In Provider Settings, we have categorized the providers based on their services. Depending on Category selection Provider List will load the available vendors.

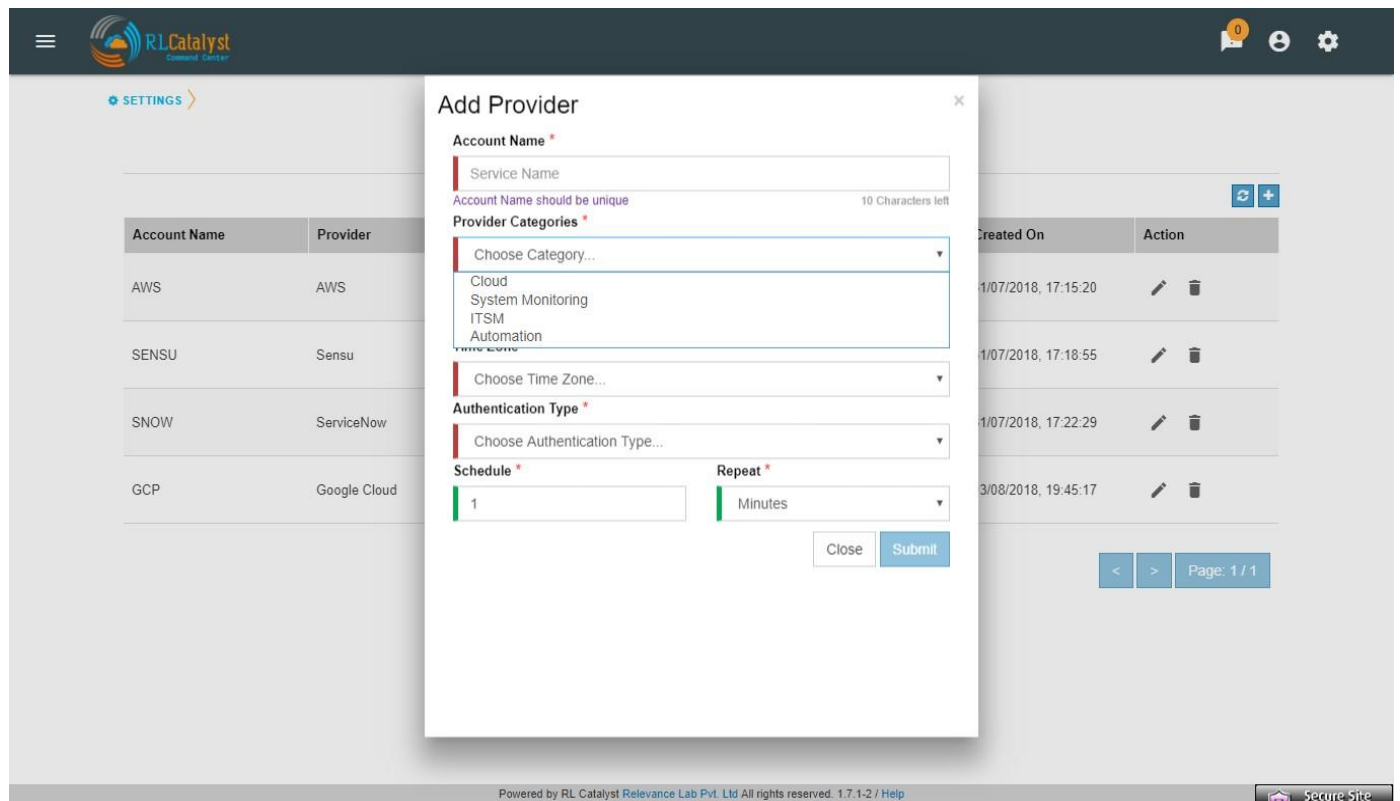


Image 10 - Provider Categories

Command Center will support for following Cloud Account providers.

- Microsoft Azure
- AWS
- Google Cloud

To configure a cloud account:

1. Click on the Settings icon in the top bar.
2. Click on the Provider Settings tab
3. Click + button and add your cloud account credentials in Settings with the details captured in **Appendix A**. Example provided below is for a Microsoft Azure account.

Field	Instructions
Account Name	Enter a Friendly name
Vendor	Choose Azure
Time Zone	Choose IST

Authentication Type	Choose OAuth
Client ID	Enter the Client ID of your Azure application E.g.: 9812d575-dja-4b48-8434-hdgh
Client Secret	Enter the Secret key of your Azure Application
Grant Type	Enter the text 'client credentials'
Resource	<a href="https://management.azure.com/">https://management.azure.com/</a>
Subscription ID	Enter the Azure subscription ID
Tenant ID	Enter the Azure Tenant ID
Schedule	Enter the Time Interval for collecting data from Cloud
Repeat	Choose the Interval Type – Minutes/Hourly

**Note:** To get the Client ID and Client Secret key, create an application in Azure and set the Role as Reader. To set the Role, Go to Subscription->Resource Group->Access Control (IAM)>Add>Permissions->Add Reader Permission

Add Provider ✕

**Account Name \***  
  
Account Name should be unique 5 Characters left

**Provider \***

**Time Zone \***

**Authentication Type \***

**Client ID \***

**Client Secret \*** 21 Characters left

**Grant Type \*** 21 Characters left

**Resource \*** 32 Characters left

**Subscription ID \*** 21 Characters left

**Tenant ID \*** 14 Characters left

**Schedule \***

**Repeat \*** 23 Characters left

Image 11 - Add cloud account details

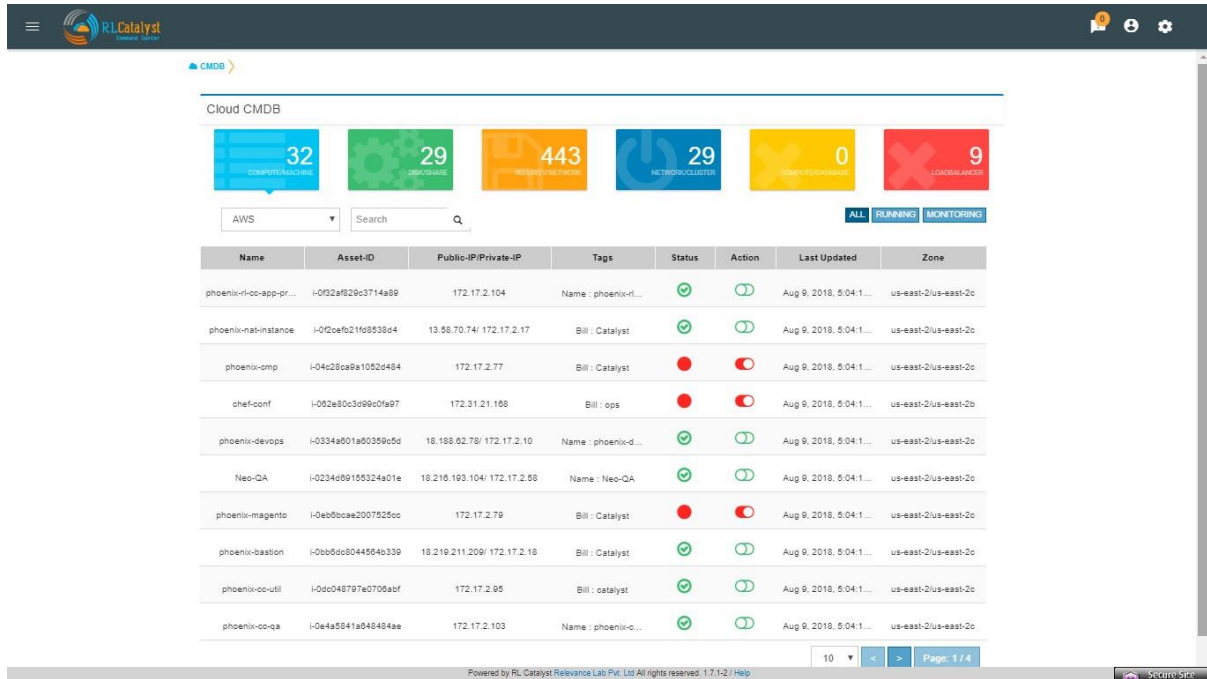
## Viewing Cloud Assets

From the menu at the top left of the top bar, choose CMDB. Cloud assets will be listed once the Cloud Credentials are added in Settings. From the dropdown choose the cloud account and get the summary view and list view as shown in screenshot. The CMDB lists the following: • Virtual machines

- Disks
- Security Groups
- Network Cluster
- Compute Databases
- Load Balancers

If the assets are tagged, the same information will be fetched into CMDB also.

You can filter the CMDB assets view by clicking on buttons “All, Running, Monitoring” which is available in the right corner just above the table. By default, ALL filter should be selected. ALL: displays all the nodes (Active & Inactive)



Cloud CMDB

Summary Cards: 32, 29, 443, 29, 0, 9

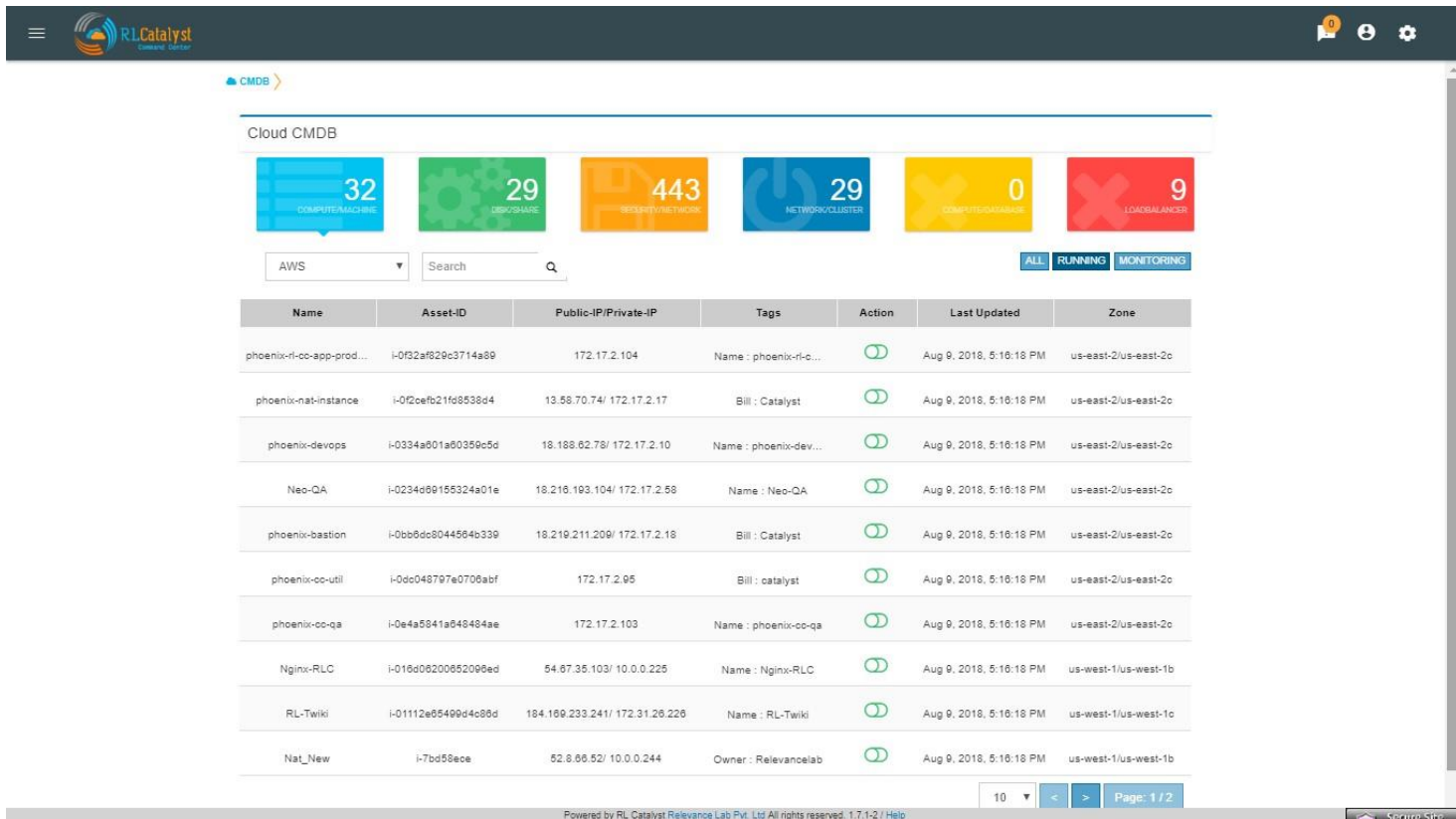
Filters: AWS, Search, ALL, RUNNING, MONITORING

Name	Asset-ID	Public-IP/Private-IP	Tags	Status	Action	Last Updated	Zone
phoenix-ri-cc-app-pr...	i-0f32af829c3714a89	172.17.2.104	Name : phoenix-ri...	✓	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
phoenix-nat-instance	i-0f2e6b21f65538d4	13.58.70.74/ 172.17.2.17	Bill : Catalyst	✓	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
phoenix-omp	i-04c20ca9a1052d484	172.17.2.77	Bill : Catalyst	✗	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
chef-conf	i-062e80c3d99c0fa97	172.31.21.168	Bill : ops	✗	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2b
phoenix-devops	i-0334a001a00359c5d	18.188.82.78/ 172.17.2.10	Name : phoenix-d...	✓	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
Neo-QA	i-0234d99155324a01e	18.216.193.104/ 172.17.2.58	Name : Neo-QA	✓	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
phoenix-magento	i-0eb0bcae2007522cc	172.17.2.79	Bill : Catalyst	✗	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
phoenix-bastion	i-0bb5dc8044504b339	18.219.211.209/ 172.17.2.18	Bill : Catalyst	✓	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
phoenix-co-usli	i-0dc048797e0709abf	172.17.2.95	Bill : catalyst	✓	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c
phoenix-co-qa	i-0e4a5841a045484ae	172.17.2.103	Name : phoenix-c...	✓	⏻	Aug 9, 2018, 5:04:1...	us-east-2/us-east-2c

Page: 1 / 4

Image 12 - CMDB view of cloud assets (ALL)

Running: displays all the running nodes



The screenshot displays the Cloud CMDB interface. At the top, there's a navigation bar with the RLCatalyst logo and user icons. Below it, a 'Cloud CMDB' section features six colored cards representing different services: ELK (32), DISKSPACE (29), RESOURCES/NETWORK (443), NETWORKCLUSTER (29), CONNECTIONMANAGER (0), and LOADBALANCER (9). A search bar and filters for 'AWS', 'ALL', 'RUNNING', and 'MONITORING' are present. The main area contains a table of cloud assets.

Name	Asset-ID	Public-IP/Private-IP	Tags	Action	Last Updated	Zone
phoenix-ri-co-app-prod...	i-0f32af829c3714a89	172.17.2.104	Name : phoenix-ri-c...		Aug 9, 2018, 5:16:18 PM	us-east-2/us-east-2c
phoenix-nat-instance	i-0f2cefb21f68538d4	13.58.70.74/ 172.17.2.17	Bill : Catalyst		Aug 9, 2018, 5:16:18 PM	us-east-2/us-east-2c
phoenix-devops	i-0334a601a50359c5d	18.188.62.78/ 172.17.2.10	Name : phoenix-dev...		Aug 9, 2018, 5:16:18 PM	us-east-2/us-east-2c
Neo-QA	i-0234d69155324a01e	18.216.193.104/ 172.17.2.58	Name : Neo-QA		Aug 9, 2018, 5:16:18 PM	us-east-2/us-east-2c
phoenix-bastion	i-0bb6dc8044564b339	18.219.211.209/ 172.17.2.18	Bill : Catalyst		Aug 9, 2018, 5:16:18 PM	us-east-2/us-east-2c
phoenix-cc-util	i-0dc048797e0708abf	172.17.2.95	Bill : catalyst		Aug 9, 2018, 5:16:18 PM	us-east-2/us-east-2c
phoenix-cc-qa	i-0e4a5841a048484ae	172.17.2.103	Name : phoenix-cc-qa		Aug 9, 2018, 5:16:18 PM	us-east-2/us-east-2c
Nginx-RLC	i-016d06200652096ed	54.87.35.103/ 10.0.0.225	Name : Nginx-RLC		Aug 9, 2018, 5:16:18 PM	us-west-1/us-west-1b
RL-Twiki	i-01112e05499d4c88d	184.169.233.241/ 172.31.26.226	Name : RL-Twiki		Aug 9, 2018, 5:16:18 PM	us-west-1/us-west-1c
Nat_New	i-7bd58ece	52.8.66.52/ 10.0.0.244	Owner : Relevancelab		Aug 9, 2018, 5:16:18 PM	us-west-1/us-west-1b

Page: 1 / 2

Image 13 - CMDB view of cloud assets (Running)

**Monitoring:** displays the monitoring nodes health services, Node, ELK Log Icons. Clicking on Services, Node & ELK Log Icons shall take the user to respective pages.

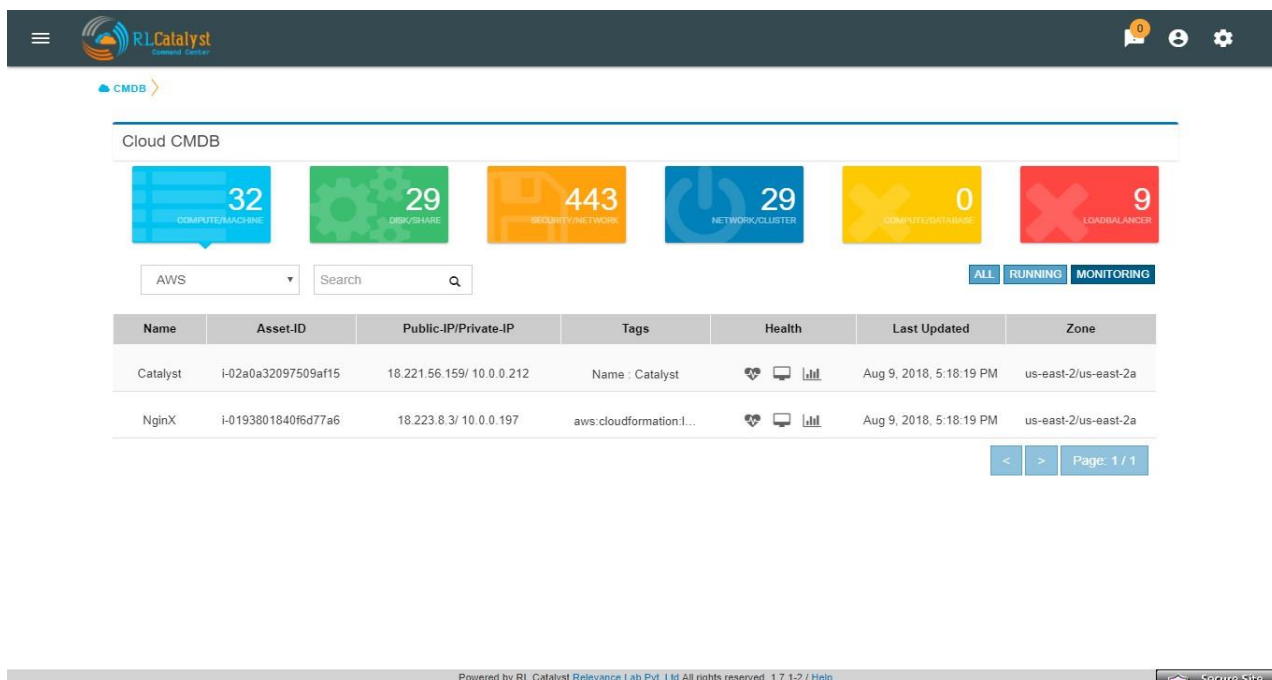


Image 14 - CMDB view of cloud assets (Monitoring)

## Configuring Business Services

Add **Business Services** to be monitored in the dashboard view. Each service added will be monitored in the predefined interval. The Business Services will appear as cards in the dashboard each showing the latest status of the service. Clicking on a card will show you a drill down view of the service with the alerts related to the service and the outage trends. Use the **Business Services** information captured in **Appendix A** as you follow the steps below.

To configure a business service

1. Click the + icon in the dashboard view to bring up the *Add Service* dialog.
2. Add the Business Service URL (should be accessible from the Command Centre)
3. Enter an alias or a name of the service. This will be the name displayed on the card in the dashboard.
4. Provide an email ID to which alerts will be send during Outages. You can provide more than one email ID separated by commas.
5. A verification e-mail will be sent to each email ID provided above. Clicking on the link in the email will confirm the email ID for receiving emails.
6. Check the box to get email notifications for linked services

×

## Add Service

Service URL

Service Name

50 Characters left

Email IDs

25 Characters left

☐ Enable email notification for dependant services

500 Characters left

Scheduler

Minutes

Close

Submit

Image 15 - Add Business Service

## Configuring the Catalyst Account

Configuring a Catalyst account allows you to access the summary of BOT runs on your dashboard page. It also enables the Remediation and Auto-Remediation features.

To configure a catalyst account:

1. Click on the Settings icon in the top bar.
2. Click on the Provider Settings tab
3. Click + button and add your catalyst account credentials in Settings with the details



Field	Instructions
Account Name	Enter a Friendly name
Vendor	Choose RLCatalyst
Time Zone	Choose IST
Authentication Type	Password
Host	URL to your RLCatalyst Instance E.g.: <a href="https://neo.rlcatalyst.com/">https://neo.rlcatalyst.com/</a>
User Name	Enter User Name
Password	Enter Password

Schedule	Enter the Time Interval for collecting data from Catalyst
Repeat	Choose the Interval Type – Minutes/Hourly

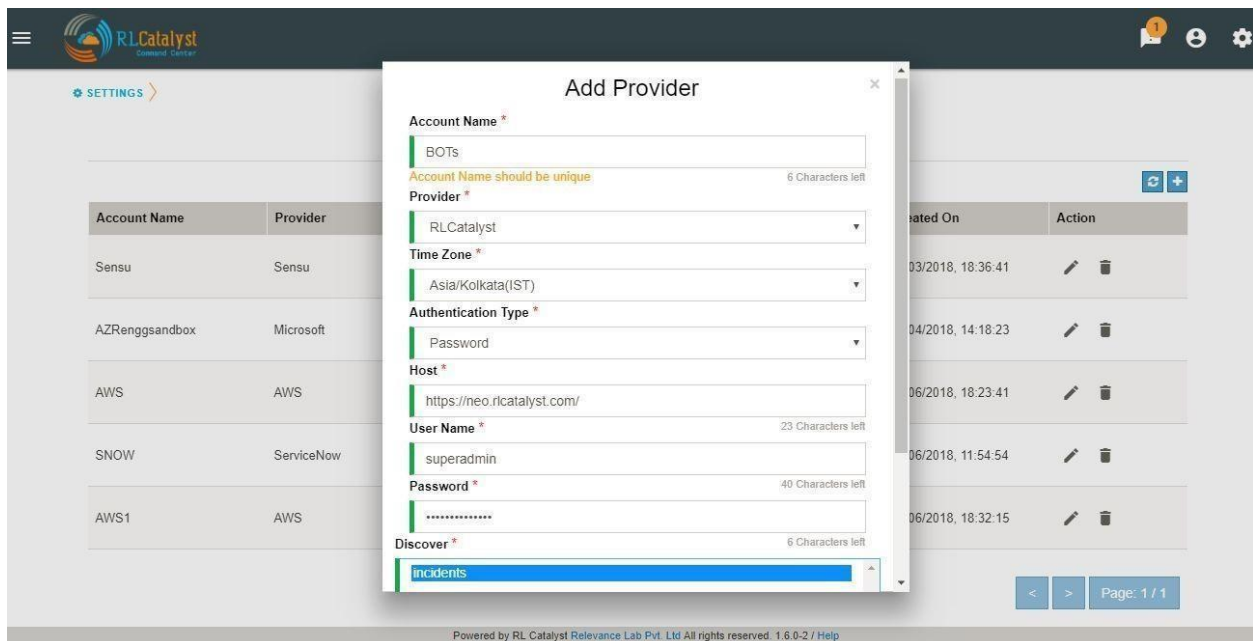


Image 16 - Add RL Catalyst Account

When you add a Catalyst account, **BOTs Summary** panel will appear on the dashboard.

## Installing the Monitoring agents

RLCatalyst Command Centre uses monitoring agents that run on the individual machines being monitored. Monitoring Agents can be installed manually or via an automated way through RLCatalyst.

## Install Agents through RLCatalyst

RLCatalyst installs monitoring agents in the target nodes on which the Business Services are running. This is done via a bootstrapping process which will install system monitoring, app monitoring and services monitoring agents into the instances. Once installed, the real-time monitoring alerts will be available under RLCatalyst Command Centre → Services and RLCatalyst Command Centre → Monitoring Tools

- Login to <customer name>neo.rlcatalyst.com with the given credentials ● Go to Work zone.
- Click on the tree on the left to choose the Organization, Business Group, Project and Environment. By default, there will be
  - Organization with the customer name
    - Business Group 'DevOps'
    - Project 'Demo Project'
    - Environments - <customer name>\_EVL, <customer name>\_DEV, <customer name>\_QA, <customer name>\_PROD, <customer name>\_DEVOPS
- Choose one of the environments
- Click on 'Import' button. Enter the IP address of the instance, credentials and Import. The agents will be installed automatically when imported.

**Note: The checks added for monitoring your services in Consul should be tagged/grouped properly with the business service name that has to be listed in the Dashboard View. RL Team will provide necessary help to get the service checks added**

## Installing monitoring agents on a Linux machine using a downloaded script

Note: Perform the following steps on each machine listed under each Business Service in

### Appendix A.

#### Prerequisites

1. To configure a machine or VM for monitoring with Command Center the following ports need to be opened in the firewall: 8301 ,8302 ,8500,8600, 3030

2. You need sudo privileges to install the clients
3. The machine should have a public IP address to communicate with the monitoring servers.

## Procedure

1. Download the agent\_installation.tar.gz file from the following URL:

<https://s3.us-east-2.amazonaws.com/cookbookslist/v2.6/linux-agent-installation.zip>

```
ubuntu@ip-172-31-26-19:~$ sudo wget https://s3.us-east-2.amazonaws.com/cookbookslist/v2.6/linux-agent-installation.zip
--2018-08-28 07:23:37-- https://s3.us-east-2.amazonaws.com/cookbookslist/v2.6/linux-agent-installation.zip
Resolving s3.us-east-2.amazonaws.com (s3.us-east-2.amazonaws.com)... 52.219.96.82
```

2. Extract the agent\_installation.zip file by the following command

```
unzip linux-agent-installation.zip
```

```
ubuntu@ip-172-31-26-19:~$ unzip linux-agent-installation.zip
Archive:  linux-agent-installation.zip
  inflating: linux-agent-installation.sh
```

*Image 14 - Extracting the Monitoring agent installers*

3. On successful extraction, execute the following command to give the privileges to run the script

```
chmod 755 linux-agent-installation.sh
```

```
ubuntu@ip-172-31-26-19:~$ chmod 755 linux-agent-installation.sh
```

*Image 15 - Preparing the Monitoring agent installers*

4. Execute the script with the following command will install monitoring clients

```
sudo ./linux-agent-installation.sh
```

```
ubuntu@ip-172-31-26-19:~$ chmod 755 linux-agent-installation.sh
ubuntu@ip-172-31-26-19:~$ sudo ./linux-agent-installation.sh
```

*Image 16 - Running the Monitoring agent installers*

5. To create the Consul checks, pass the parameters using following command

```
sudo ./linux-agent-installation.sh parameter1 parameter2 parameter3 parameter4 parameter5
```

### Example:

```
sudo ./linux-agent-installation.sh petclinic petclinic relevance  
http://18.219.197.233:8080/petclinic/ 20s
```

Parameter1	Service name <A friendly name for the service. This will be your Business Service>
Parameter2	tag application name <Name of this application e.g. MongoDB on which your Business Service depends>
Parameter3	tag tenant id <Company Name for this Tenant>
Parameter4	URL
Parameter5	checks interval e.g. 60s

```
ubuntu@ip-172-31-26-19:~$ sudo ./linux-agent-installation.sh petclinic petclinic relevance http://18.219.197.233:8080/petclinic/ 20s
```

You should now have the monitoring agents running on your machine.

## Install monitoring agents on a Windows machine through a downloaded script

Note: Perform the following steps on each machine listed under each Business Service in

### Appendix A.

#### Prerequisites

1. To configure a machine or VM for monitoring with Command Center the following ports need to be opened in the firewall: 8301 ,8302 ,8500,8600, 3030
2. You need to run PowerShell as Administrator (right-click and choose "Run As Administrator")
3. The machine should have a public IP address to communicate with the monitoring servers.

#### Procedure

1. Download the agent\_ installation.tar.gz file from the following URL:

<https://s3.us-east-2.amazonaws.com/cookbookslist/v2.6/windows-agent-installation.zip>

```
PS C:\RLAgent>
PS C:\RLAgent> Invoke-WebRequest -Uri https://s3.us-east-2.amazonaws.com/cookbookslist/v2.6/windows-agent-installation.zip -Outfile windows-agent-installation.zip
PS C:\RLAgent> dir

Directory: C:\RLAgent

Mode                LastWriteTime         Length Name
----                -
-a----             6/18/2018  10:20 AM           1092 windows-agent-installation.zip
```

1. Extract the script from the archive.

```
PS C:\RLAgent> Expand-Archive -Path ./windows-agent-installation.zip
PS C:\RLAgent> dir

Directory: C:\RLAgent

Mode                LastWriteTime         Length Name
----                -
d-----             6/18/2018  10:20 AM           windows-agent-installation
-a----             6/18/2018  10:20 AM           1092 windows-agent-installation.zip
```

2. Set the directory to the extracted folder and run the script using the following command

PowerShell -ExecutionPolicy bypass ./windows-agent-installation.ps1

```
PS C:\RLAgent> cd .\windows-agent-installation\
PS C:\RLAgent\windows-agent-installation> powershell -ExecutionPolicy bypass .\windows-agent-installation.ps1
Chef: 14.2.0
Chef already exists
windows-installation cookbook is already exists
Runing windows-installation cookbook to consul-clients and sensu-clients
[2018-06-18T10:23:57+05:30] WARN: No config file found or specified on command line, using command line options.
Starting Chef Client, version 14.2.0
[2018-06-18T10:24:04+05:30] WARN: Run List override has been provided.
[2018-06-18T10:24:04+05:30] WARN: Original Run List: []
[2018-06-18T10:24:04+05:30] WARN: Overriden Run List: [recipe::windows-installation]
```

3. The script should install the Monitoring agents. Verify that the agents are running by typing the following command

ps | findstr sensu

It should show the monitoring agent running

Similarly verify

ps | findstr consul

```
PS C:\> .\windows-installation-agent.ps1
chef-client already exists
Downloading the latest version of the installer
Installing agents
Done. Monitoring agents installed successfully
PS C:\chef\cookbooks> ps | findstr consul
267      16      32980      23976      19,23      5392      0 consul
PS C:\chef\cookbooks> ps | findstr sensu-client
235      13      17020      116      0,22      4380      0 sensu-client
PS C:\chef\cookbooks>
```

## Install monitoring agents on a Windows machine manually

### Prerequisites

1. To configure a machine or VM for monitoring with Command Center the following ports need to be opened in the firewall: 8301 ,8302 ,8500,8600, 3030
2. You need Administrator privileges to install the clients
3. The machine should have a public IP address to communicate with the monitoring servers.

### Procedures

1. Choose the Chef Windows package based on the Operating System (Ex: Windows 2012) & Architecture (Ex: X86\_64) from the below link in the required/available windows machine

<https://downloads.chef.io/chef#windows>

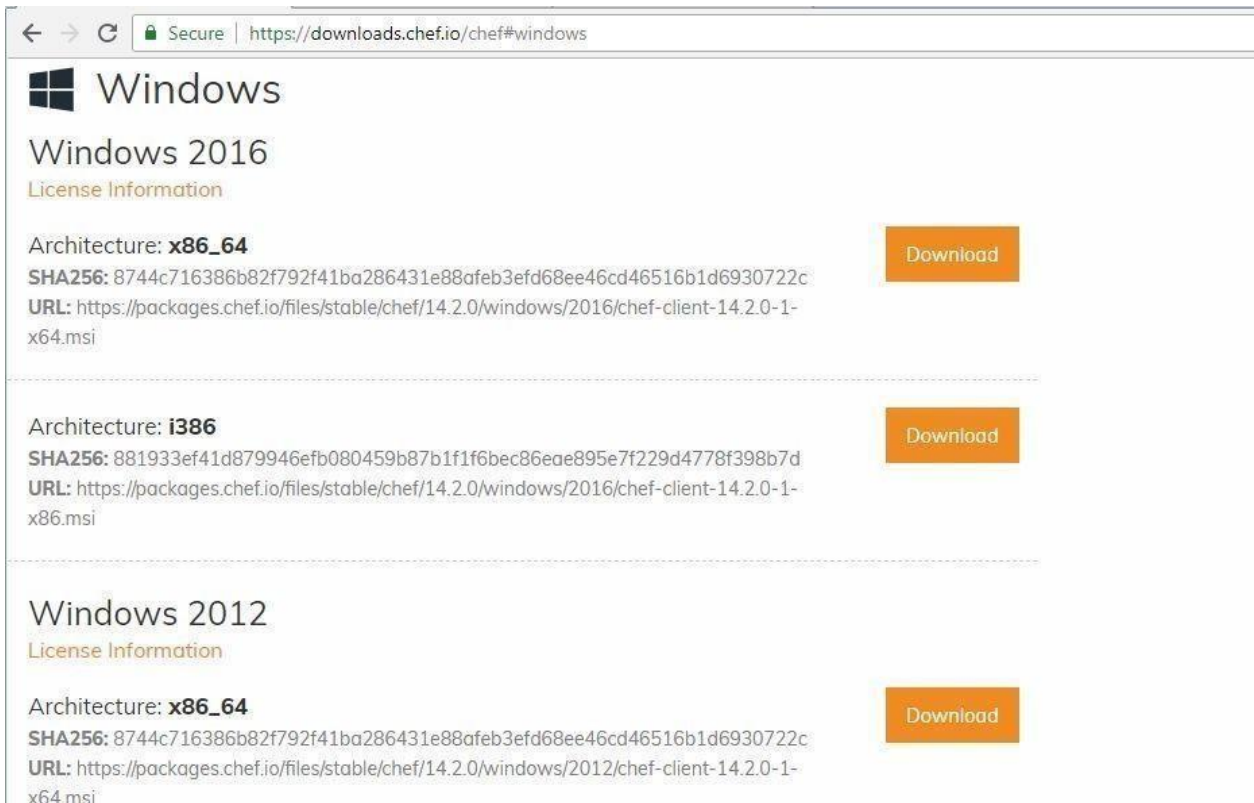


Image 17 - Downloading Chef

2. Install the downloaded windows package in the Windows machine on this location and it will create a chef directory. E.g.: C://



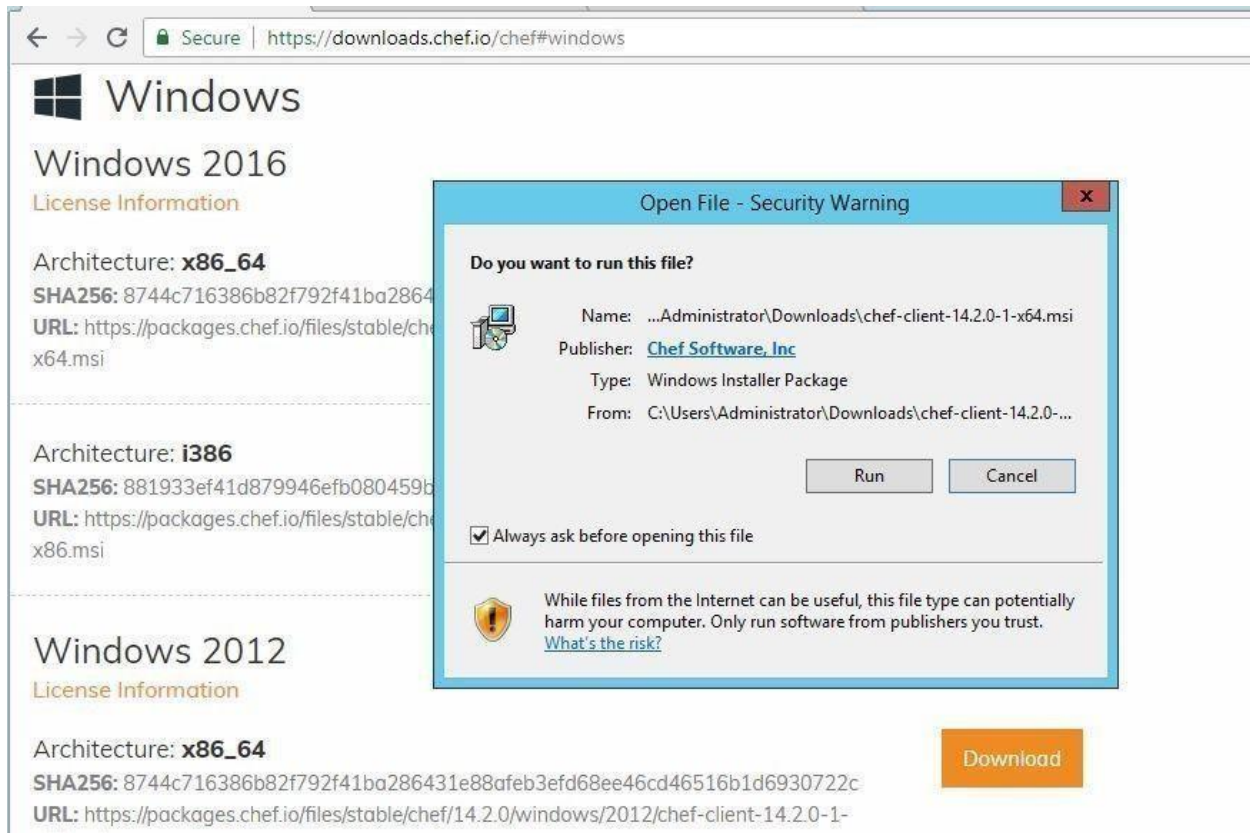


Image 18 - Installing Chef

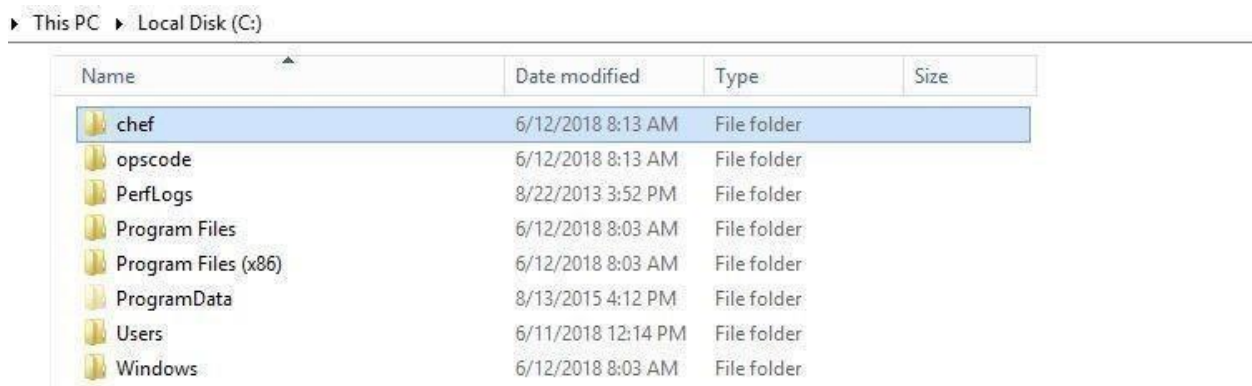


Image 19 - Verifying the Chef Installation

3. Create a directory with name "cookbooks" in "c:/chef" (optional).

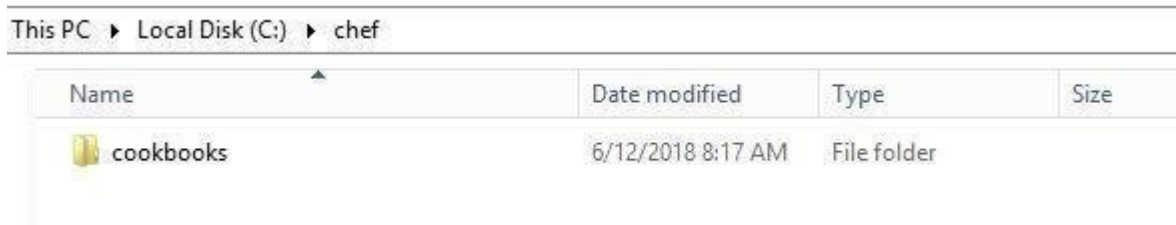


Image 20 - Chef cookbook location

- Download the following files for sensu and consul clients from the s3 bucket.

<https://s3.us-east-2.amazonaws.com/cookbookslist/v2.6/consul-client.zip> <https://s3.us-east-2.amazonaws.com/cookbookslist/v2.6/sensu-client.zip>

- Please unzip the following files of s3 files and examples files should be like E.g.:

C://chef/cookbooks/ consul-client

C://chef/cookbooks/ sensu-client

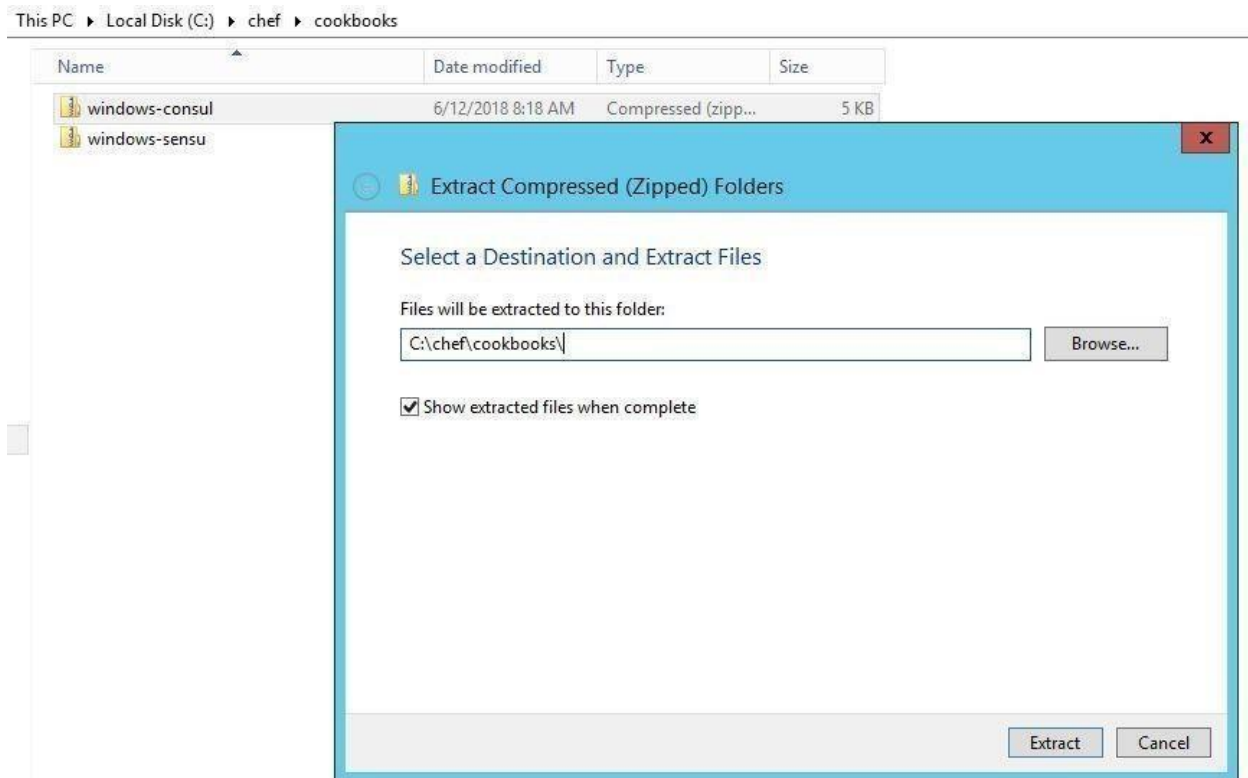


Image 21 - Extracting the Monitoring Agent Installers

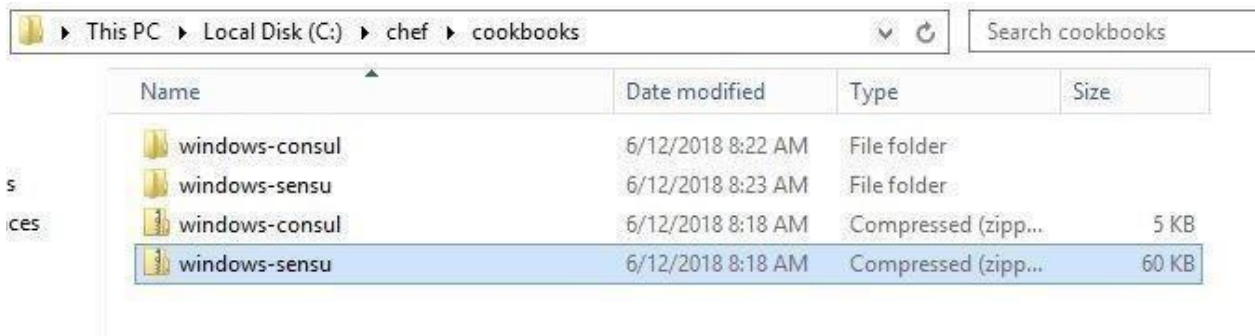


Image 22 - Verifying the extracted installers

6. Open the command prompt and navigate to the following location

```
C:\chef\cookbooks\
```

7. Run the following commands to install the consul and sensu clients

```
chef-client -z -o "recipe[sensu-client]" chef-client
-z -o "recipe[consul-client]"
```

This PC > Local Disk (C:) > chef > cookbooks

Name	Date modified	Type	Size
windows-consul	6/12/2018 8:22 AM	File folder	
windows-sensu	6/12/2018 8:23 AM	File folder	
windows-consul	6/12/2018 8:18 AM	Compressed (zipp...	5 KB
windows-sensu	6/12/2018 8:18 AM	Compressed (zipp...	60 KB

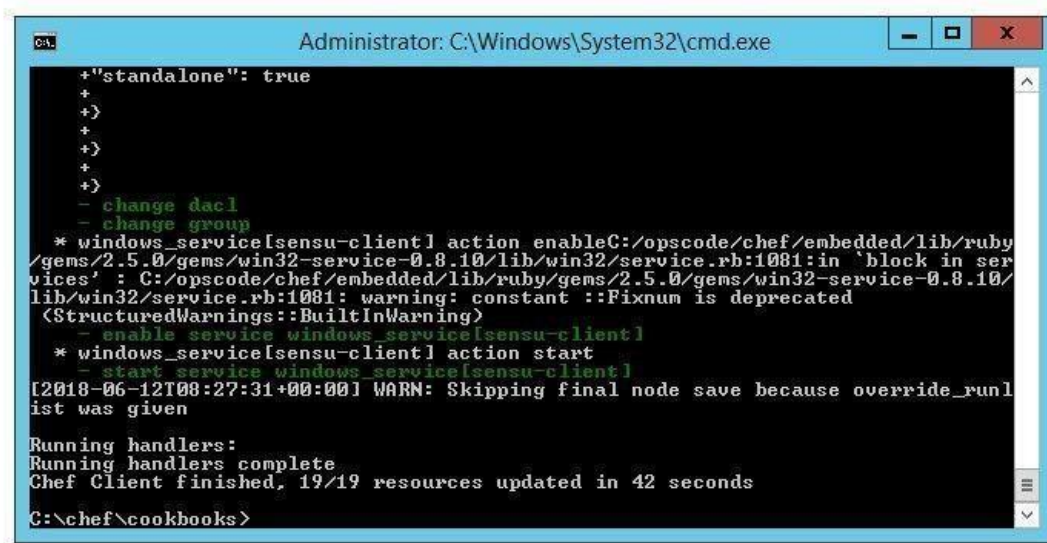
```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\chef\cookbooks>chef-client -z -o "recipe[windows-sensu]"
```

Image 23 - Running the monitoring agent installers

This PC > Local Disk (C:) > chef > cookbooks >

Name	Date modified	Type	Size
windows-consul	6/12/2018 8:22 AM	File folder	
windows-sensu	6/12/2018 8:23 AM	File folder	
windows-consul	6/12/2018 8:18 AM	Compressed (zipp...	5 KB
windows-sensu	6/12/2018 8:18 AM	Compressed (zipp...	60 KB



```

Administrator: C:\Windows\System32\cmd.exe

+ "standalone": true
+
+ }
+
+ }
+
+ }
- change dacl
- change group
* windows_service[sensu-client] action enableC:/opscod/chef/embedded/lib/ruby
/gems/2.5.0/gems/win32-service-0.8.10/lib/win32/service.rb:1081:in 'block in ser
vices': C:/opscod/chef/embedded/lib/ruby/gems/2.5.0/gems/win32-service-0.8.10/
lib/win32/service.rb:1081: warning: constant ::Fixnum is deprecated
(StructuredWarnings::BuiltInWarning)
- enable service windows_service[sensu-client]
* windows_service[sensu-client] action start
- start service windows_service[sensu-client]
[2018-06-12T08:27:31+00:00] WARN: Skipping final node save because override_runl
ist was given

Running handlers:
Running handlers complete
Chef Client finished, 19/19 resources updated in 42 seconds

C:\chef\cookbooks>
  
```

Image 24 - Monitoring agent installation in progress

- After the installation of clients, we can verify the services with names “consul and sensuclient” or the other way testing the above-mentioned ports by “netstat” command.

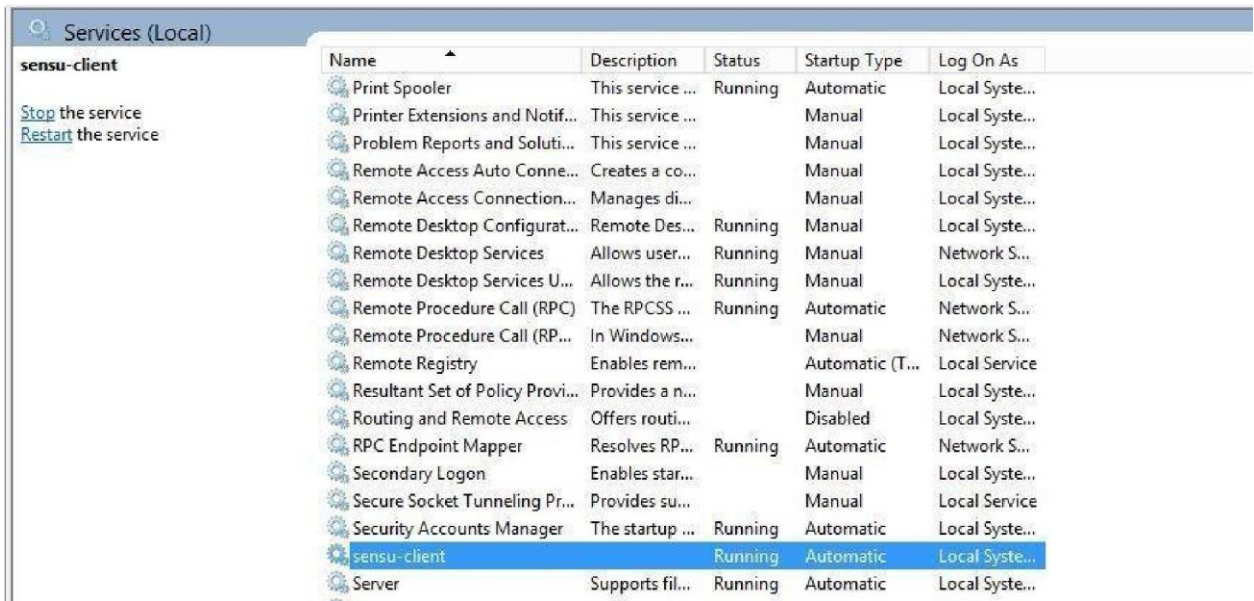


Image 25 - Verifying running agents

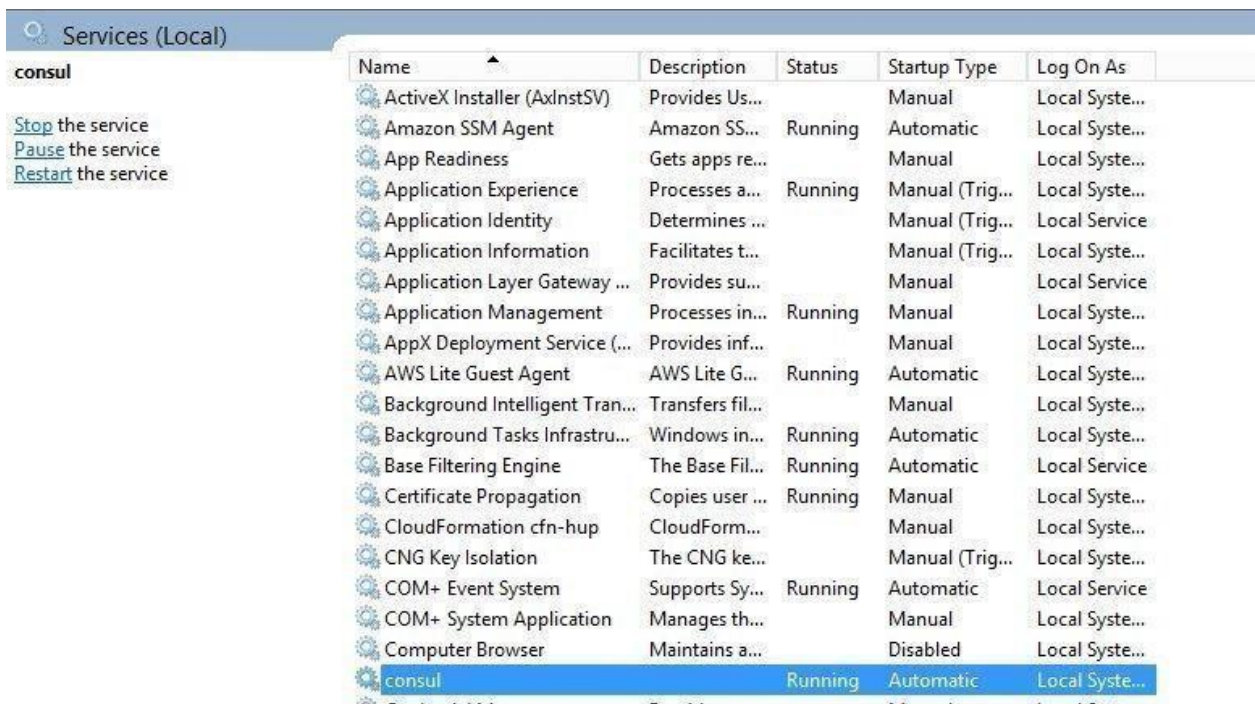


Image 26 - Verifying running agents



## Aggregated Alerts

Once the services are added and agents are installed, the alerts will be aggregated from multiple monitoring sources by the respective collectors. Alerts are currently aggregated from

- Ping BOTs – Checks Availability of Services
- Consul – Monitors Services
- Sensu – System Monitoring

When the service goes down or if an Outage happens, the corresponding card on the dashboard view will turn Red.

When any of the dependent services has a problem related to BSM will be Yellow. Clicking on the card will give details on linked services and the associated nodes.

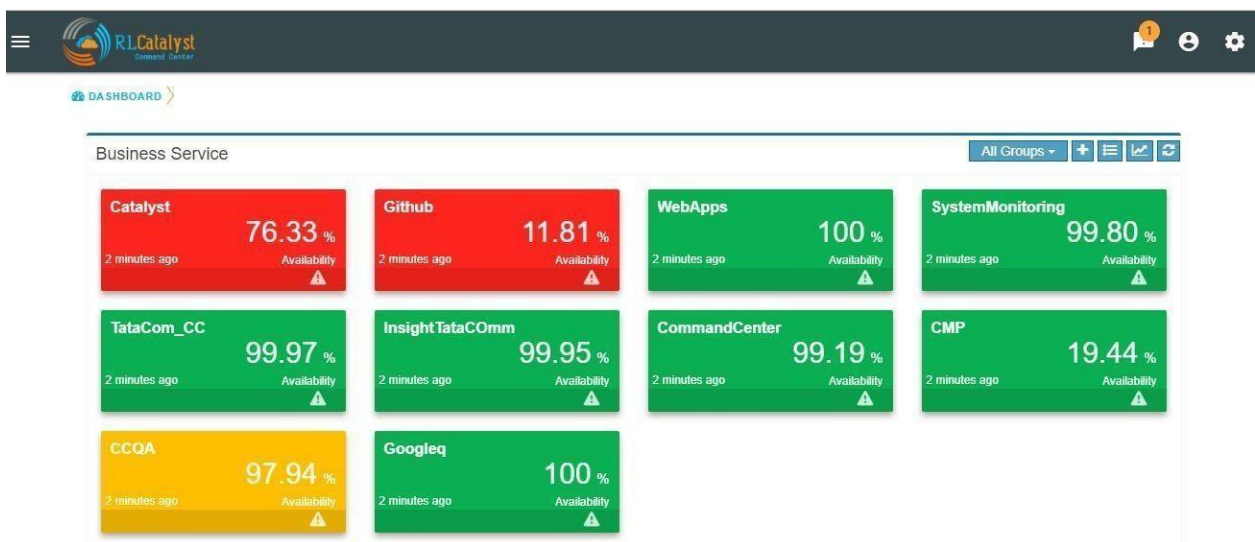



Image 27 - Outages as Red cards on Dashboard


**RL Catalyst**  
Reinforcement Learning

[DA SHBOARD](#) > [CFT800018](#) >

HEALTH

OUTAGE

COMMUNICATION

Service	Availability	Created on	Last Run	Status	Alerts
cft800018	10.95%	Aug 9, 2018, 11:47:00 AM	Aug 9, 2018, 5:26:00 PM		

### Linked Services

	Service Name	Node Address	Node Name
+	engine-health	10.0.0.197	ip-10-0-0-197
+	mongo-health	10.0.0.212	ip-10-0-0-212
+	nodejs-health	10.0.0.212	ip-10-0-0-212

### Nodes

	Node ID	Node Address	Last Updated	Action
—	10.0.0.212	10.0.0.212	Aug 9, 2018, 5:25:30 PM	

Name	Output	Last Updated	Status
disk_usage_check	CheckDisk OK: All disk usage under 80% and inode usage under 85%	Aug 9, 2018, 5:26:07 PM	
check_load	CheckLoad OK: Load average: 0.0, 0.01, 0.05	Aug 9, 2018, 5:26:10 PM	
cpu_usage_check	CheckCPU TOTAL OK: total=0.0 user=0.0 nice=0.0 system=0.0 idle=100.0 load...	Aug 9, 2018, 5:26:11 PM	
memory_usage_check	MEM OK - system memory usage: 20%	Aug 9, 2018, 5:26:03 PM	

+	10.0.0.197	10.0.0.197	Aug 9, 2018, 5:25:36 PM
---	------------	------------	-------------------------

Powered by RL Catalyst Reinforcement Lab Pvt. Ltd All rights reserved. 1.7.1.2 / Help




Image 28 - Drill down view from card

Click on the Alerts button to see the detailed Alerts from multiple sources (Pingbot, Consul & Sensu). Alerts aggregated by Node or Service in the Alerts Monitor screen.

Service alerts are shown on the Services tab of the Alert Monitor.



RLCatalyst Command Center					
<a href="#">DASHBOARD</a> > <a href="#">CCQA</a> > <a href="#">ALERT MONITOR</a> >					
SERVICE ALERT			NODE ALERT		
Timestamp	Service Name	Check Name	Source	Message	Severity
Aug 7, 2018, 6:42:03 AM	CCQA	Scheduler	Consul	Check Passed	✓
Aug 7, 2018, 6:42:03 AM	CCQA	CommandCenter	Consul	Check Passed	✓
Aug 7, 2018, 6:42:03 AM	CCQA	Consul	Consul	Check Passed	✓
Aug 6, 2018, 6:54:00 PM	CCQA	CCQA	Ping BOT	CCQA(8cb1b0eb) is Back To ...	✓
Aug 6, 2018, 6:52:03 PM	CCQA	Consul	Consul	Check Passed	✓
Aug 6, 2018, 6:52:03 PM	CCQA	CommandCenter	Consul	Check Passed	✓
Aug 6, 2018, 6:52:03 PM	CCQA	Scheduler	Consul	Check Passed	✓
Aug 6, 2018, 6:51:00 PM	CCQA	CCQA	Ping BOT	CCQA(8cb1b0eb) is in Error s...	✗

Powered by RL Catalyst [Relevance Lab Pvt. Ltd](#) All rights reserved. 1.7.1-2 / [Help](#)

Secure Site

Image 29 - Service Alerts

System alerts are shown in the Nodes tab of the Alert Monitor.

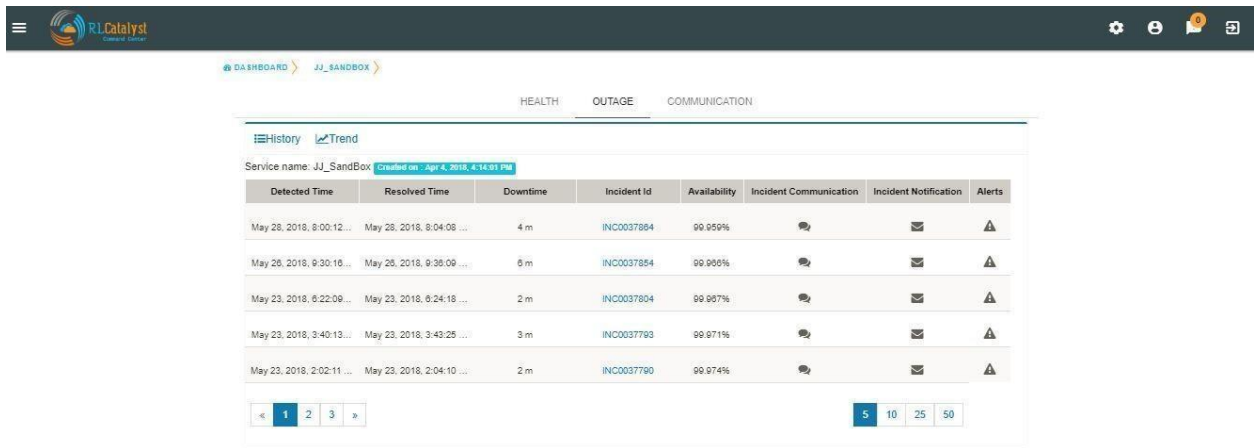
RLCatalyst Command Center						
<a href="#">DASHBOARD</a> > <a href="#">CCQA</a> > <a href="#">ALERT MONITOR</a> >						
SERVICE ALERT			NODE ALERT			
Timestamp	Node	Service Name	Check Name	Source	Message	Severity
Aug 7, 2018, 3:48:10 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	cpu_usages_check is back to normal	✓
Aug 7, 2018, 3:46:12 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	CheckCPU TOTAL CRITICAL: total=10...	✗
Aug 7, 2018, 3:40:09 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	cpu_usages_check is back to normal	✓
Aug 7, 2018, 3:36:08 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	CheckCPU TOTAL CRITICAL: total=10...	✗
Aug 7, 2018, 3:22:10 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	cpu_usages_check is back to normal	✓
Aug 7, 2018, 3:18:12 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	CheckCPU TOTAL CRITICAL: total=99....	✗
Aug 7, 2018, 3:14:09 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	cpu_usages_check is back to normal	✓
Aug 7, 2018, 3:12:12 PM	172.17.2.103	CCQA	cpu_usages_check	Sensu	CheckCPU TOTAL CRITICAL: total=10...	✗
Powered by RL Catalyst <a href="#">Relevance Lab Pvt. Ltd</a> All rights reserved. 1.7.1-2 / <a href="#">Help</a>						

Image 30 - Node Alerts

The dependent services of the Business Service and their health can be viewed under the Linked services section of the same page.

The dependent nodes of the Business Service and their health can be viewed under the Nodes section of the same page.

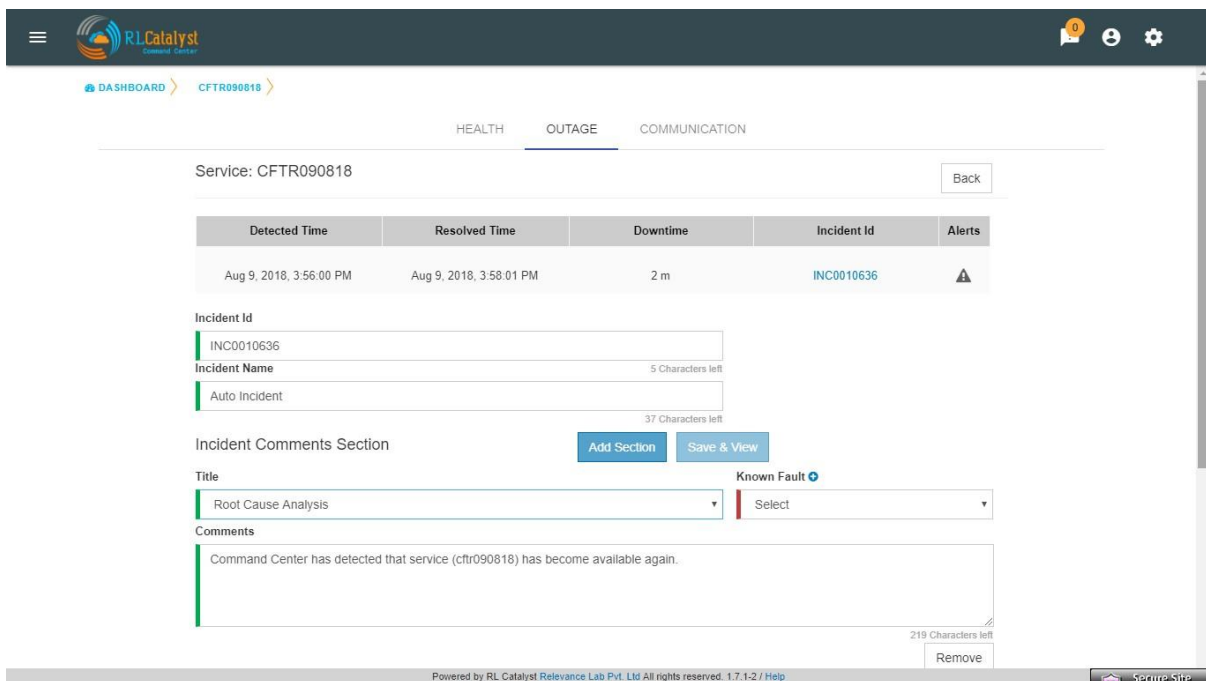
Click on the Outages tab to get a detailed list of all the outages detected by the system.



Detected Time	Resolved Time	Downtime	Incident Id	Availability	Incident Communication	Incident Notification	Alerts
May 28, 2018, 9:00:12...	May 28, 2018, 9:04:08 ...	4 m	INC0037884	99.959%			
May 26, 2018, 9:30:16...	May 26, 2018, 9:38:09 ...	6 m	INC0037884	99.995%			
May 23, 2018, 6:22:08...	May 23, 2018, 6:24:18 ...	2 m	INC0037884	99.997%			
May 23, 2018, 3:40:13...	May 23, 2018, 3:43:25 ...	3 m	INC0037793	99.971%			
May 23, 2018, 2:02:11...	May 23, 2018, 2:04:10 ...	2 m	INC0037790	99.974%			

Image 31 - Outage Details

Click on the Incident Id to open the associated ServiceNow ticket on the ServiceNow portal. Click on the Incident Communication icon to send out communication about the incident with Root Cause Analysis & Category.



Service: CFTR090818 Back

Detected Time	Resolved Time	Downtime	Incident Id	Alerts
Aug 9, 2018, 3:56:00 PM	Aug 9, 2018, 3:58:01 PM	2 m	INC0010636	

Incident Id  
INC0010636

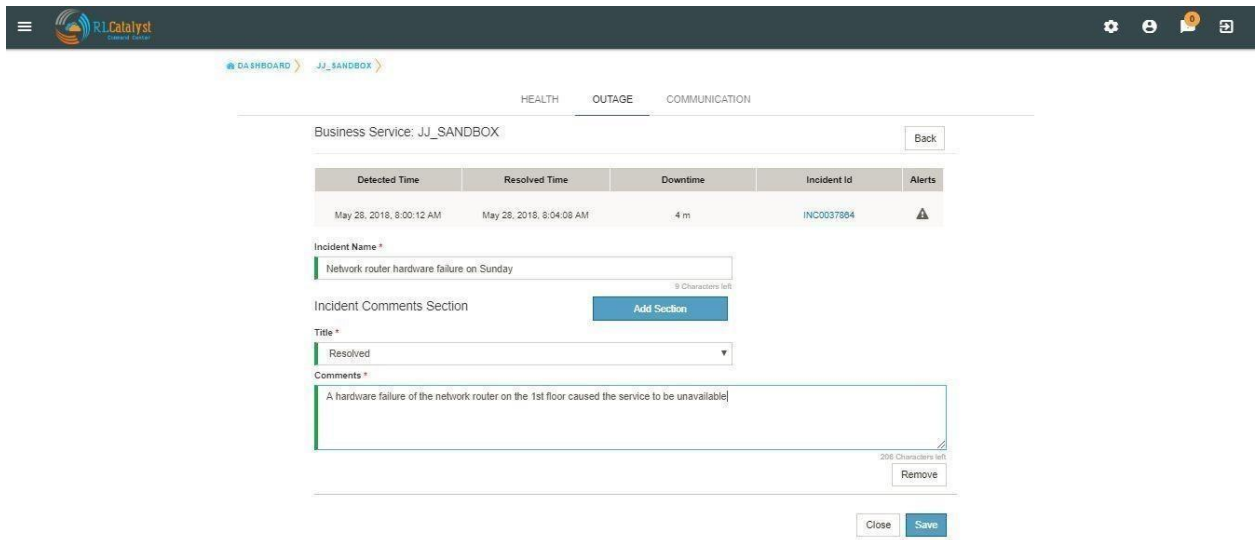
Incident Name  
Auto Incident

Incident Comments Section  
Add Section Save & View

Title  
Root Cause Analysis

Comments  
Command Center has detected that service (cftr090818) has become available again.

Image 32 - Incident Communication



Business Service: JJ\_SANDBOX Back

Detected Time	Resolved Time	Downtime	Incident Id	Alerts
May 28, 2018, 8:00:12 AM	May 28, 2018, 8:04:08 AM	4 m	INC0037884	

Incident Name \*

Network router hardware failure on Sunday 9 Characters left

Incident Comments Section Add Section

Title \*

Resolved ▼

Comments \*

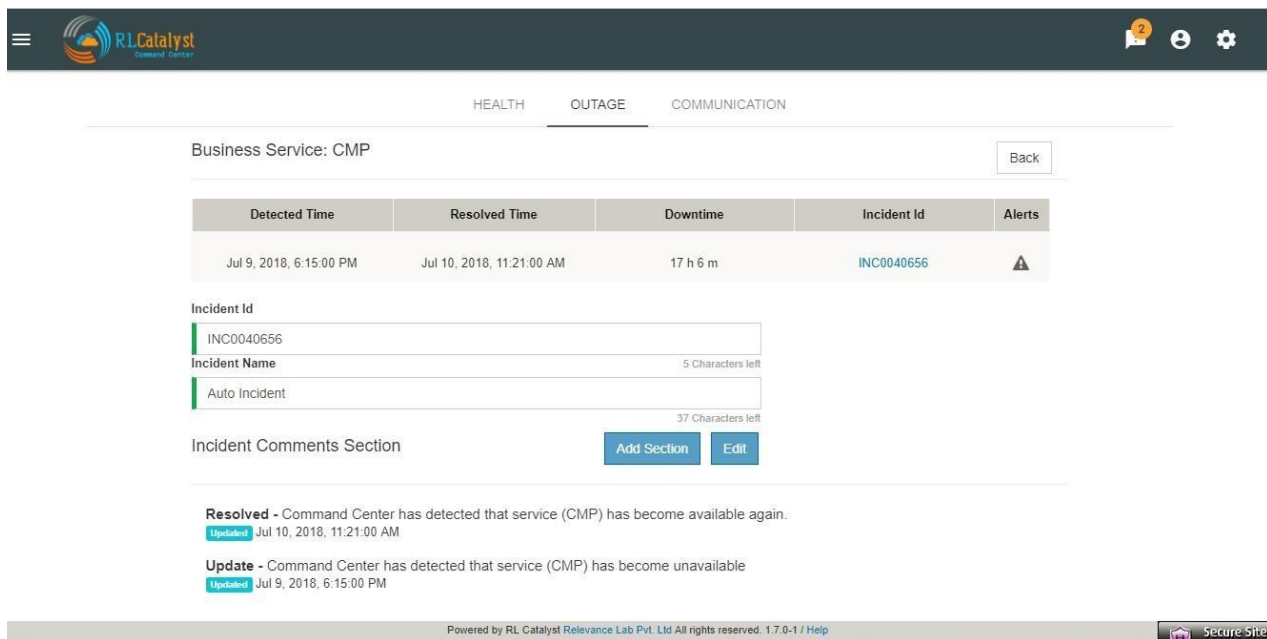
A hardware failure of the network router on the 1st floor caused the service to be unavailable 208 Characters left

Remove

Close Save

Image 33 - Incident Communication(Add Section)

Auto-create Incident Communications for Detection and Resolution: System automatically creates Incident Communication for application outage detection and resolution.



Business Service: CMP Back

Detected Time	Resolved Time	Downtime	Incident Id	Alerts
Jul 9, 2018, 6:15:00 PM	Jul 10, 2018, 11:21:00 AM	17 h 6 m	INC0040656	

Incident Id

INC0040656

Incident Name 5 Characters left

Auto Incident 37 Characters left

Incident Comments Section Add Section Edit

**Resolved** - Command Center has detected that service (CMP) has become available again.  
Updated Jul 10, 2018, 11:21:00 AM

**Update** - Command Center has detected that service (CMP) has become unavailable  
Updated Jul 9, 2018, 6:15:00 PM

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.7.0-1 / Help Secure Site

Image 34 - Auto Create Incident Communication

Click on the Communications tab to see a timeline of incidents.

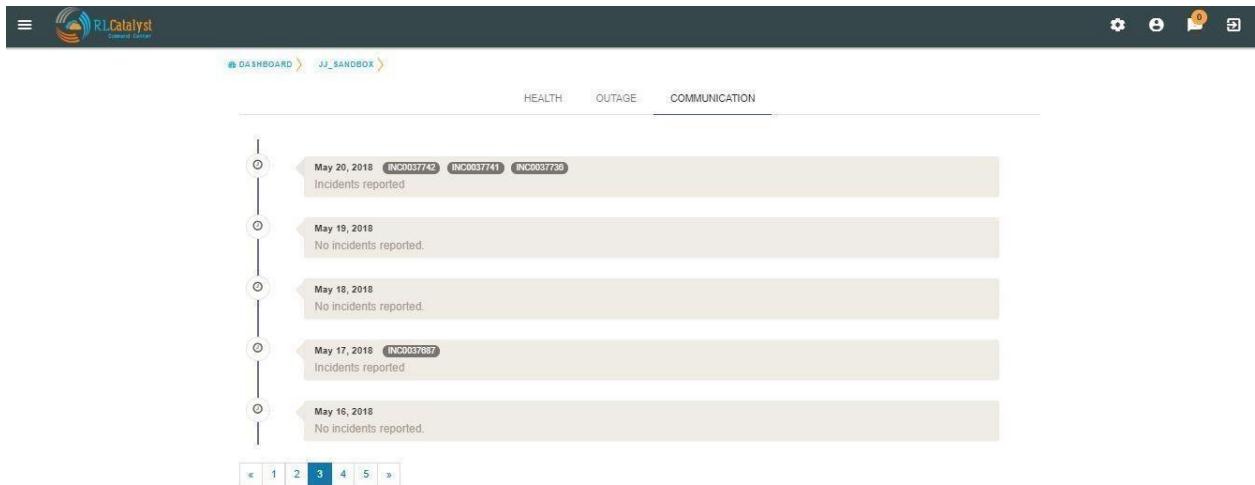


Image 35 - Communication timeline

Command Center provides a feature called “Fault Table” to capture known problems related to a service and then uses the information to help the user to categorize the root-cause of any outage that occurs.

User can add fault to “Fault Table” by clicking on + icon which is available in the “Known Faults” table (Menu->Known Faults link-> + icon)

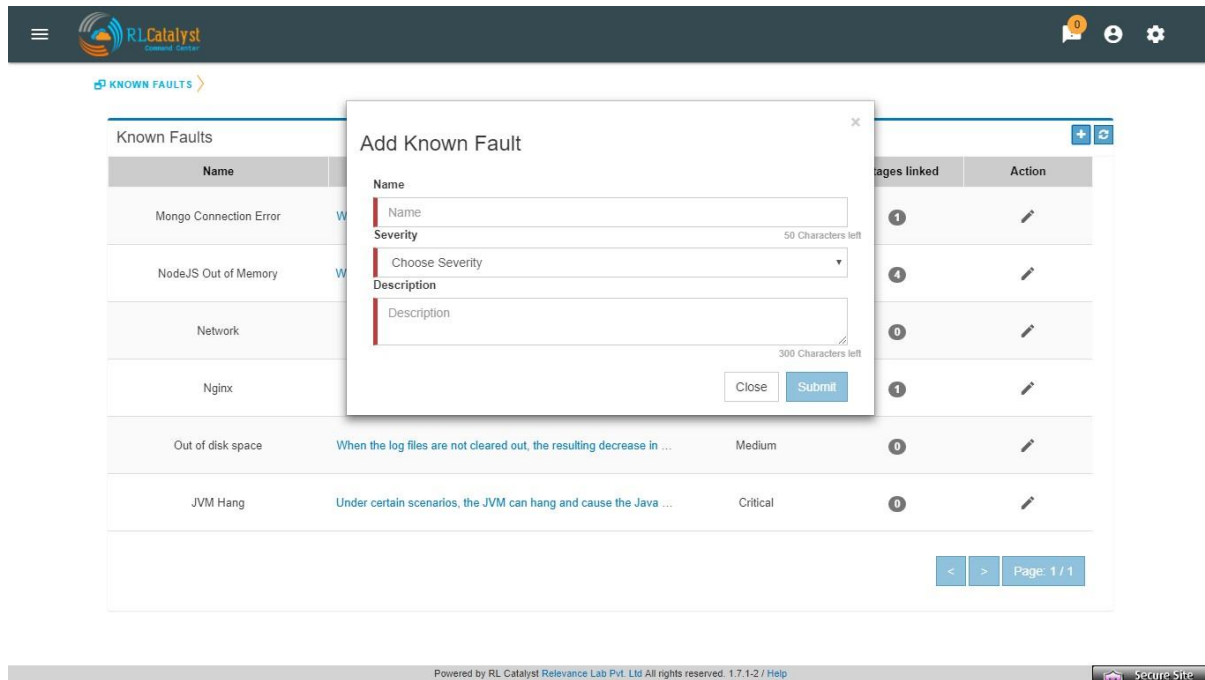







Image 36 - Add Known Fault

When a Root-cause identified incident communication is entered, the user can link the RCA Incident Communication to an item in the Fault Table associated to the BSM through Add Incident Communication screen.






[DASHBOARD](#) > [CMP](#) >

HEALTH
OUTAGE
COMMUNICATION

Service: CMP

Back

Detected Time	Resolved Time	Downtime	Incident Id	Alerts
Aug 7, 2018, 2:18:00 PM	Aug 7, 2018, 2:24:00 PM	6 m		

Incident Id

Incident ticket Id

Incident Name

15 Characters left

Auto Incident

37 Characters left

Incident Comments Section

Add Section

Save & View

Title

Root Cause Analysis

Known Fault

Select

Comments

Comments

360 Characters left

Remove

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.7.1-2 / Help


 Secure Site

Image 37 - Known Fault Selection

User shall be able to navigate to the Fault Table from any outage which is linked to a fault by clicking on “Fault” link in the Outages screen.

[History](#)
[Trend](#)

All (Select Fault)
19.06.2018 - 07.08.2018

Service name: CMP Created on : Jun 19, 2018, 6:21:30 PM

Detected Time	Resolved Time	Downtime	Incident Id	Availability	Fault	Action
Jul 6, 2018, 6:03:00 PM	Jul 9, 2018, 6:03:00 PM	3 d	<a href="#">INC0040581</a>	70.305%	NodeJS Out of Memory	<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jul 6, 2018, 5:39:00 PM	Jul 6, 2018, 5:57:00 PM	18 m	<a href="#">INC0040570</a>	70.442%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jul 6, 2018, 4:36:00 PM	Jul 6, 2018, 5:30:00 PM	54 m	<a href="#">INC0040541</a>	70.917%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jul 5, 2018, 11:48:00 AM	Jul 5, 2018, 2:42:00 PM	2 h 54 m	<a href="#">INC0040455</a>	65.845%	Nginx	<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jul 3, 2018, 6:12:00 PM	Jul 4, 2018, 11:45:00 AM	17 h 33 m	<a href="#">INC0040428</a>	71.302%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jul 3, 2018, 12:33:00 PM	Jul 3, 2018, 4:15:00 PM	3 h 42 m	<a href="#">INC0040404</a>	75.067%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jul 2, 2018, 10:30:00 PM	Jul 3, 2018, 12:27:00 PM	13 h 57 m	<a href="#">INC0040399</a>	99.881%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jun 27, 2018, 7:21:00 PM	Jun 28, 2018, 10:39:00 AM	15 h 18 m	<a href="#">INC0040119</a>	20.053%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jun 27, 2018, 5:03:00 PM	Jun 27, 2018, 5:09:00 PM	6 m	<a href="#">INC0040090</a>	19.903%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>
Jun 26, 2018, 7:51:00 PM	Jun 27, 2018, 10:42:00 AM	14 h 51 m	<a href="#">INC0039991</a>	19.717%		<a href="#">Chat</a> <a href="#">Trend</a> <a href="#">Grid</a> <a href="#">Alert</a>







10
<
>
Page: 2 / 4

Image

### 38 - Faults Link

User can view the count of outages linked to a fault by clicking on the “Outages Linked” link in the Fault table



Known Faults				
Name	Description	Severity	Outages linked	Action
Mongo Connection Error	When MongoDB is restarted while the application is up, the appl...	Critical	1	
NodeJS Out of Memory	When Sensu API returns too much data, the NodeJS application...	High	4	
Network	If the network queue builds up, the application may crash	Critical	0	
Nginx	Nginx 2	Critical	1	
Out of disk space	When the log files are not cleared out, the resulting decrease in ...	Medium	0	
JVM Hang	Under certain scenarios, the JVM can hang and cause the Java ...	Critical	0	

[<](#)
[>](#)
Page: 1 / 1

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.7.1-2 / Help

Image 39 - Outages Linked

Aggregated Alerts for all services are available from the left pane menu **'Services'**.

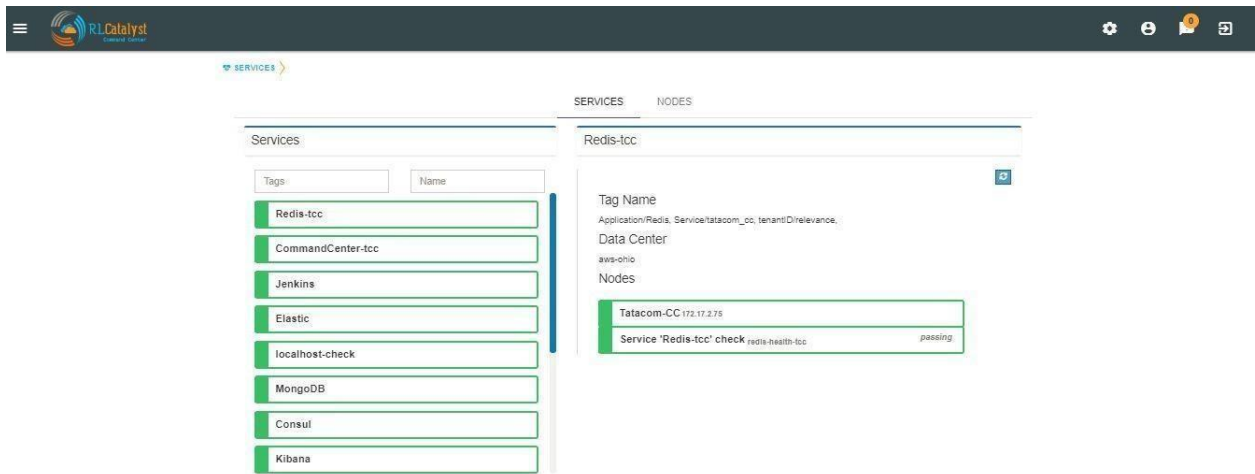


Image 40 - Aggregated Services Alerts View

Aggregated Alerts for all servers/instances are available from the left pane menu '**Monitoring Tools**'.

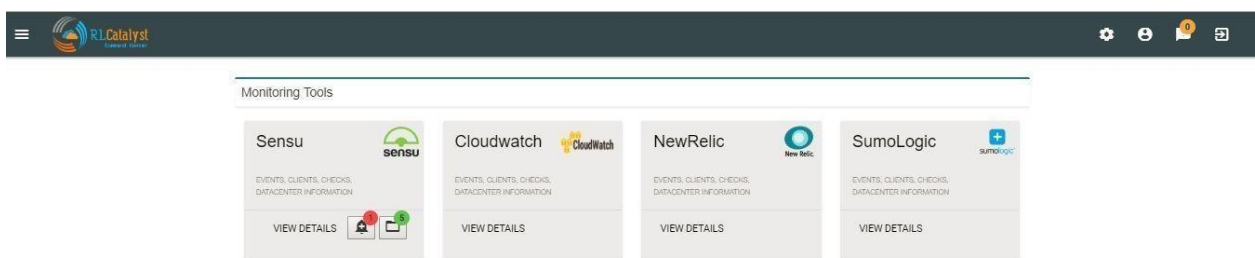
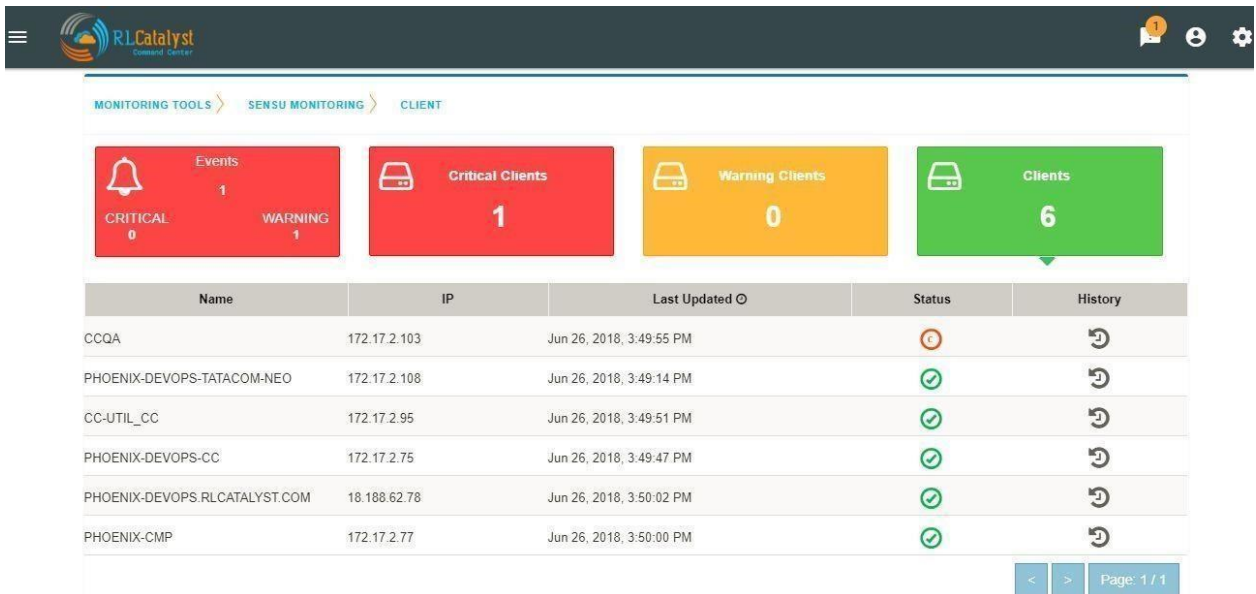


Image 41 - Aggregated System Alerts View

History for all servers/instances are available from the **Monitoring Tools->Clients->History**



42 - History of Servers/Instances

Click on History Icon, to view the detailed history information regarding each client.

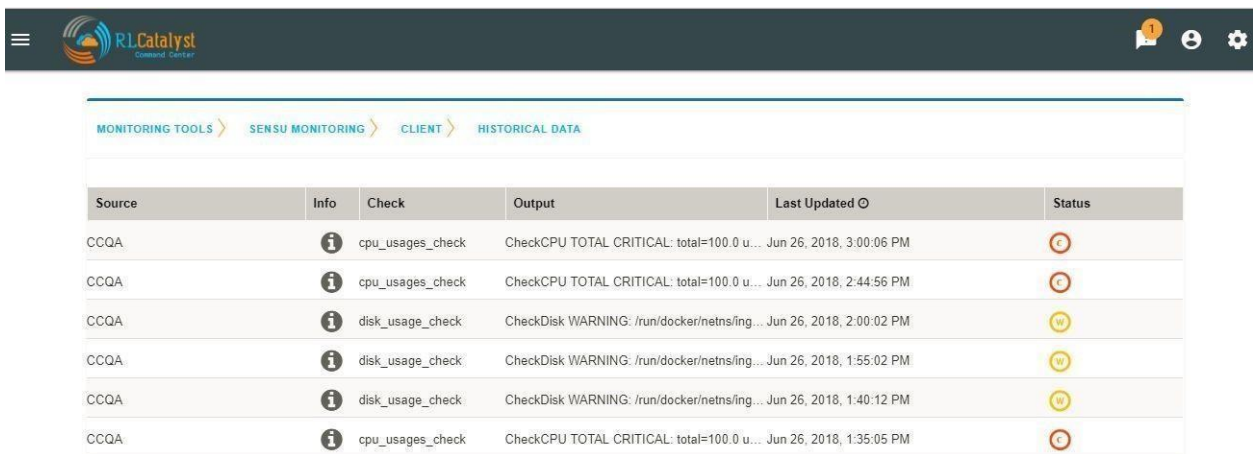


Image 43 - Historical Data related to Instances

## Logging in as a landlord

Open a browser (we recommend Chrome or Firefox). Enter the application URL provided. The login page should open. On the login page, fill the Company, User and Password fields as captured in **Appendix A**. Then

click the Login button. You will see the landing page of the tenant created first and by choosing the tenant be able to view the data of that tenant.

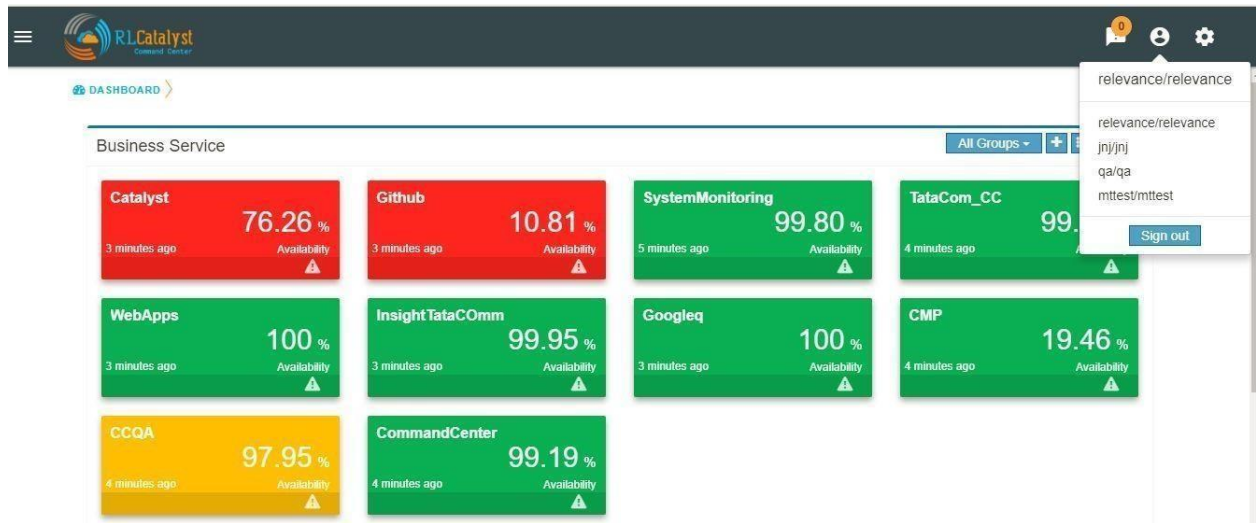


Image 44 - Landlord View

## Remediation feature

Command Center allows you to restart the service if a problem is encountered either at an underlying Node level or at a dependent service level. This feature is to give L0/L1 level support personnel a quick means of attempting to correct a problem.

When a dependent node/service has a critical alert, you have an option to remediate the problem by clicking on the icon to restart the service which is available in the BSM drilldown view screen. The BOT would then restart the node.

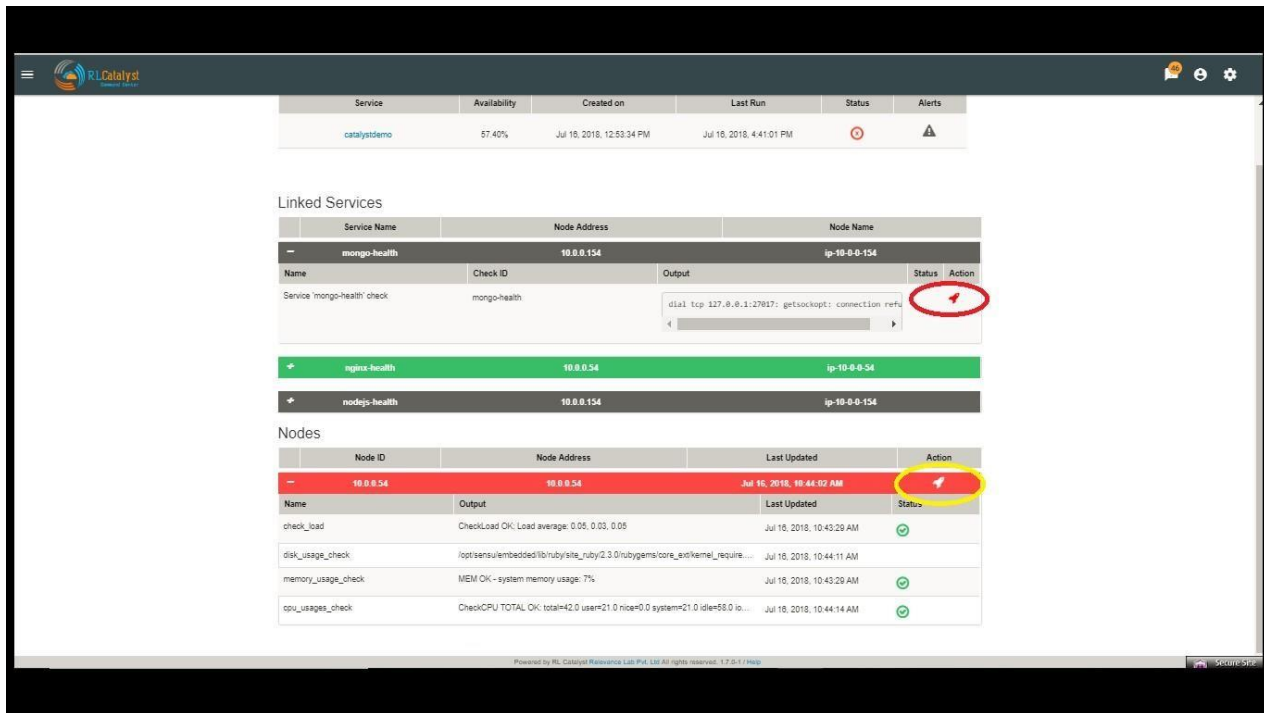


Image 45 - Remediation Icon

## Auto-Remediation feature

Command Center allows you to choose to configure certain Business Services (Managed Nodes) for auto healing. Whenever an outage is detected for a BSM configured with auto-healing, the system shall then kick-off the auto-remediation process. Auto-healing shall be initiated for nodes provided are in warning or critical status.

Manual remediation shall not be available for Nodes under a BSM that is enabled for Auto-healing.

You can opt for Auto-healing option by checking the Checkbox “Enable Auto-Remediation” which is available in the “Add Service” screen.

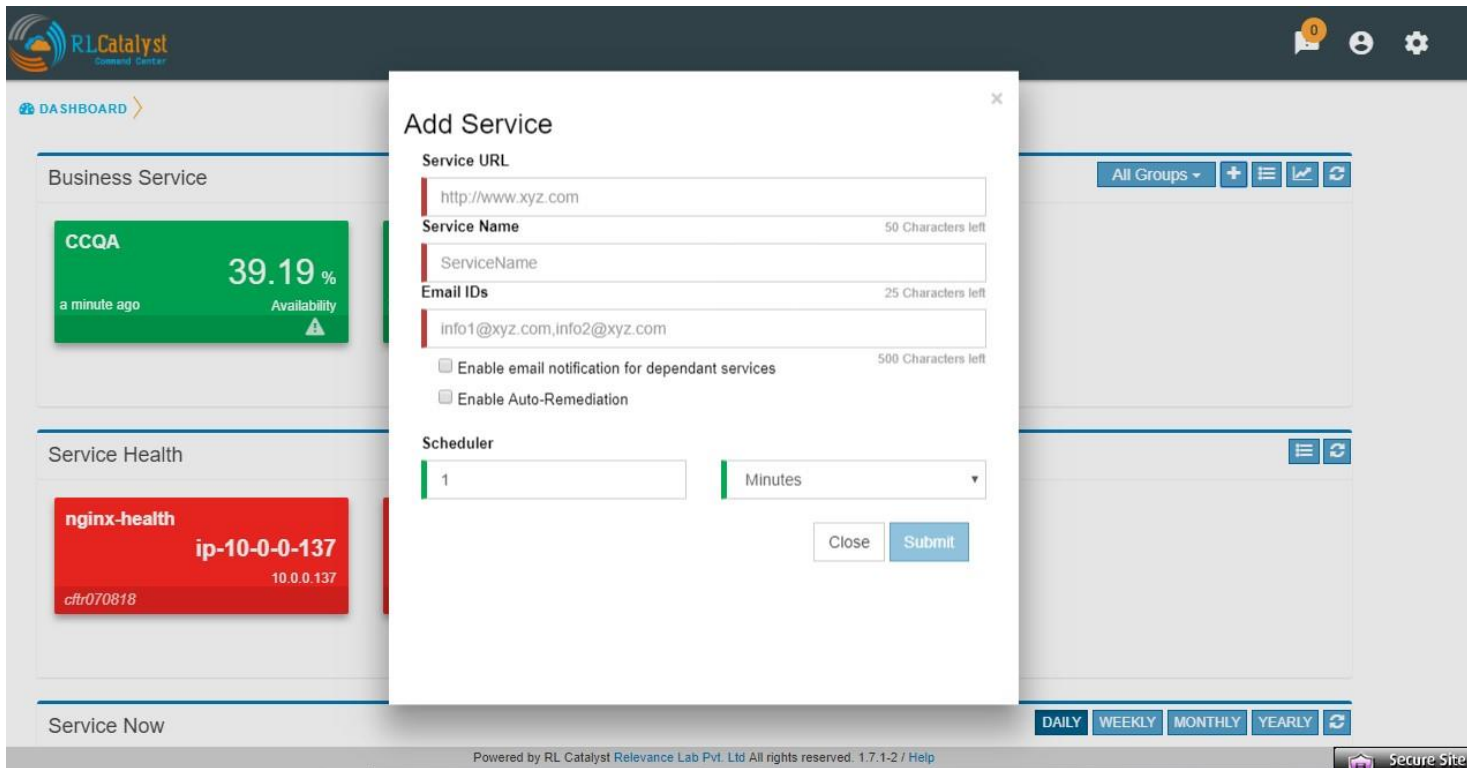


Image 46 - Auto Remediation

## Planned versus Unplanned outages

The idea of this feature is to provide a capability to plan a down-time so that the availability of the Business Service shall not be affected. CommandCenter has provided a screen to enter a planned outage. This screen shall take a date-time range, the nodes that are affected and the BSMs that are affected.

When an outage occurs, check if the outage falls within a planned outage window. If yes, do not consider that outage in the availability calculations.

By clicking on link "Plan Outage" which is available under the menu, application will open "Planned Outage Details" screen. By clicking on + icon you can add Plan outage for the required service.

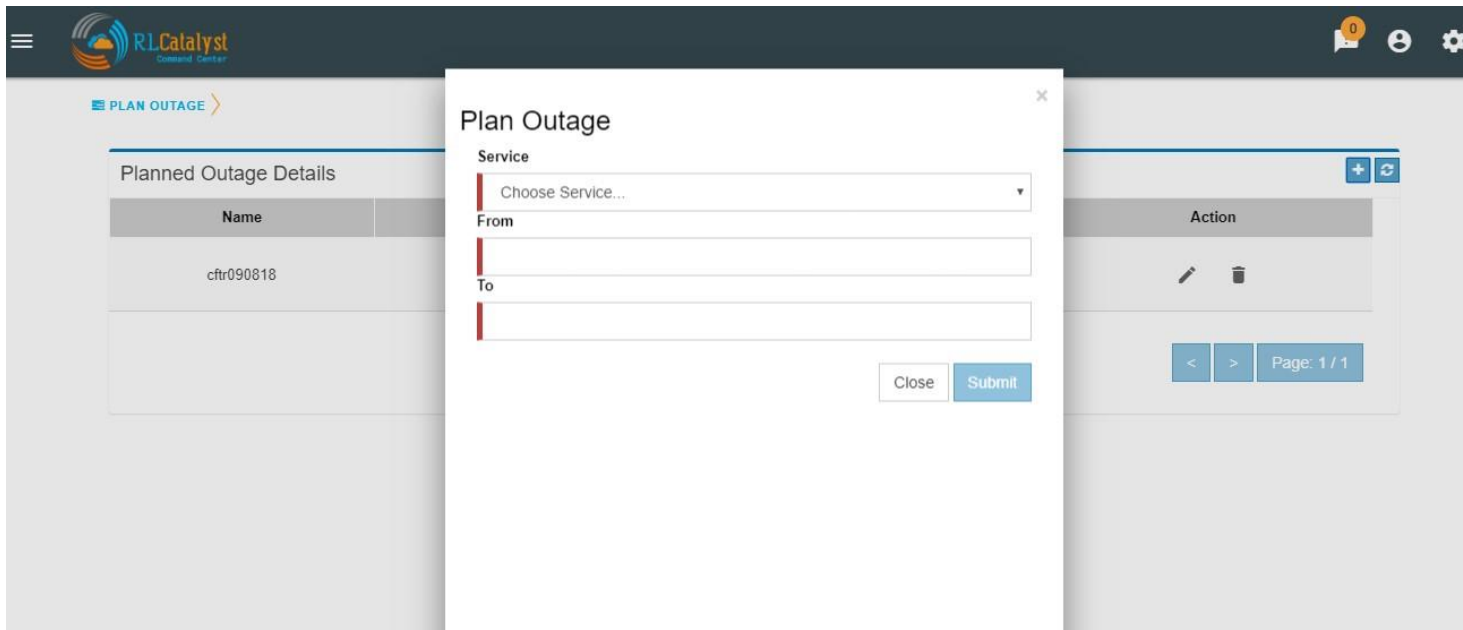


Image 47 - Planned Outage Details

## Appendix A

<b>Registration Information</b>	
---------------------------------	--

Name of the tenant	<This will be used to fill the Customer Name field in the registration form. This field will have to be unique for each tenant configured in the system>
User Name	<This will be the username with which the tenant will login>
Password	<This will be the initial password allocated to the tenant>

Email Address	<This will be the email ID which will be verified by the system during registration. Ensure you have access to this e-mail ID during registration>
<b>Provider Settings</b>	
Will an Amazon Web Services account be configured for this tenant?	
- AWS Access Key	



- AWS Secret Key	
- AWS Region for this account	<e.g. us-east-1>
- AWS Account Number	
Will a Microsoft Azure account be configured for this tenant?	
- Azure Client ID	< Client ID of your Azure application >
- Azure Client Secret	<Secret key of your Azure Application>
Subscription ID -	<Enter the Azure subscription ID>
- Tenant ID	<Enter the Azure Tenant ID>

Will a ServiceNow account be configured for this tenant?	
- Host	
- User-name	<username for your ServiceNow account>
- Password	<Password to your ServiceNow account>
-	
Will a Sensu account be configured for this tenant?	
- Host	
- User-name	<username for your ServiceNow account>

- Password	<Password to your ServiceNow account>

<b>Business Services</b>	
<Business Service 1>	

- Name	<Name of the service as it appears on the dashboard>
- URL	< URL for the business service >
- Linked Services (if any)	< Service1 – IP Address of node it runs on, Service2 – IP Address of node it runs on, Service3 – IP Address of node it runs on >

- Nodes (VMs or Machines)	<FQDN of Node1, FQDN of Node 2, FQDN of Node3>
<Business Service 2>	
- Name	<Name of the service as it appears on the dashboard>
- URL	< URL for the business service >
- Linked Services (if any)	< Service1 – IP Address of node it runs on, Service2 – IP Address of node it runs on, Service3 – IP Address of node it runs on >
- Nodes (VMs or Machines)	<FQDN of Node1, FQDN of Node 2, FQDN of Node3>

<Business Service 3>	
- Name	<Name of the service as it appears on the dashboard>
- URL	< URL for the business service >
- Linked Services (if any)	< Service1 – IP Address of node it runs on, Service2 – IP Address of node it runs on, Service3 – IP Address of node it runs on >
- Nodes (VMs or Machines)	<FQDN of Node1, FQDN of Node 2, FQDN of Node3>