Command Center Documentation

Release 1.0.1

cc

Jun 29, 2020

Contents:

CHAPTER 1

Indices and tables

- genindex
- modindex
- search

1.1 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.

1.2 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.

1.3 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.

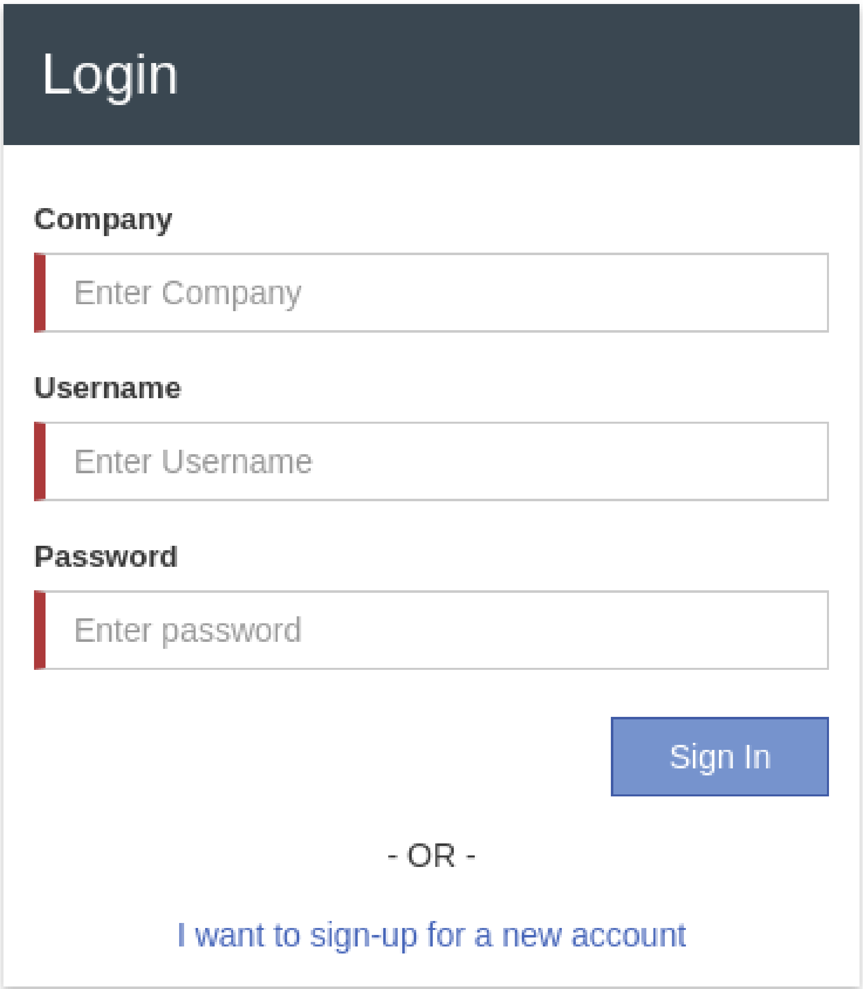
1.3.1 Planning your deployment

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.

1.3.2 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.



Login

Company

Enter Company

Username

Enter Username

Password

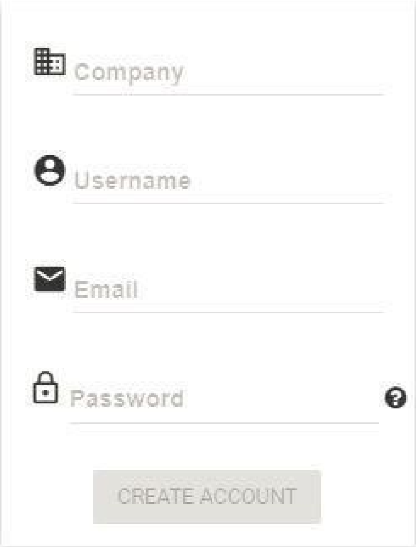
Enter password

Sign In

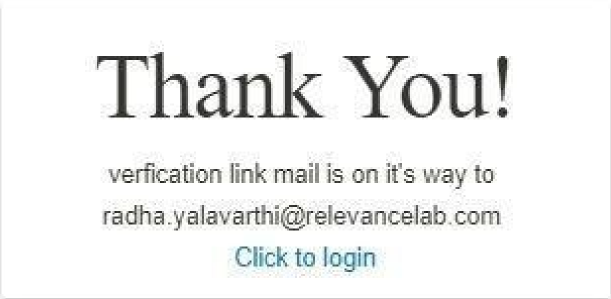
- OR -

I want to sign-up for a new account

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



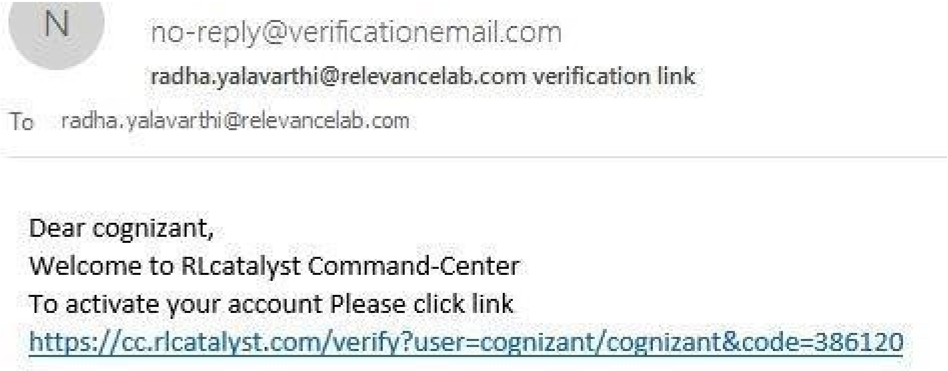
Use details from *Appendix A* for Company Name, User Name, Email & set the Password as per Password policy. Click on Create Account button. You will see a Thank You screen confirming that a verification email has been sent to the email address registered.



Thank You!

verfication link mail is on it's way to
radha.yalavarthi@relevancelab.com
Click to login

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.



N

no-reply@verificationemail.com
radha.yalavarthi@relevancelab.com verification link
To radha.yalavarthi@relevancelab.com

Dear cognizant,
Welcome to RLcatalyst Command-Center
To activate your account Please click link
https://cc.rlcatalyst.com/verify?user=cognizant/cognizant&code=386120

Logging in as a tenant

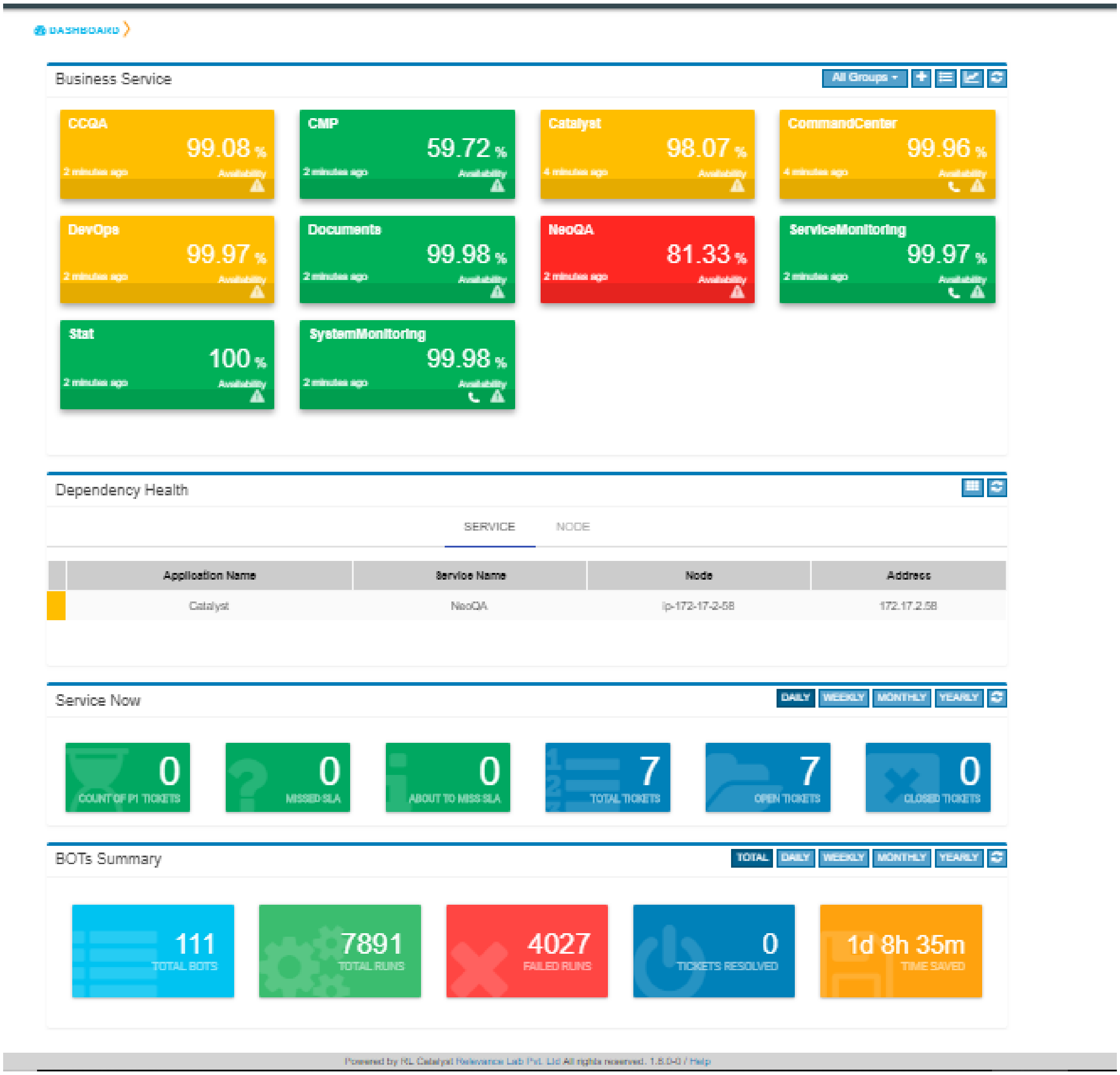
Open a browser (we recommend Chrome or Firefox). Enter the application URL provided. The login page should open. On the

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.



Business Service

CCQA 99.08 % 2 minutes ago Availability

CMP 59.72 % 2 minutes ago Availability

Catalyst 98.07 % 4 minutes ago Availability

CommandCenter 99.96 % 4 minutes ago Availability

DevOps 99.97 % 2 minutes ago Availability

Documents 99.98 % 2 minutes ago Availability

NeoQA 81.33 % 2 minutes ago Availability

ServiceMonitoring 99.97 % 2 minutes ago Availability

Stat 100 % 2 minutes ago Availability

SystemMonitoring 99.98 % 2 minutes ago Availability

Dependency Health

	Application Name	Service Name	Node	Address
🟨	Catalyst	NeoQA	ip-172-17-2-58	172.17.2.58

Service Now

0 COUNT OF P1 TICKETS

0 MISSED SLA

0 ABOUT TO MISS SLA

7 TOTAL TICKETS

7 OPEN TICKETS

0 CLOSED TICKETS

BOTs Summary

111 TOTAL BOTS

7891 TOTAL RUNS

4027 FAILED RUNS

0 TICKETS RESOLVED

1d 8h 35m TIME SAVED

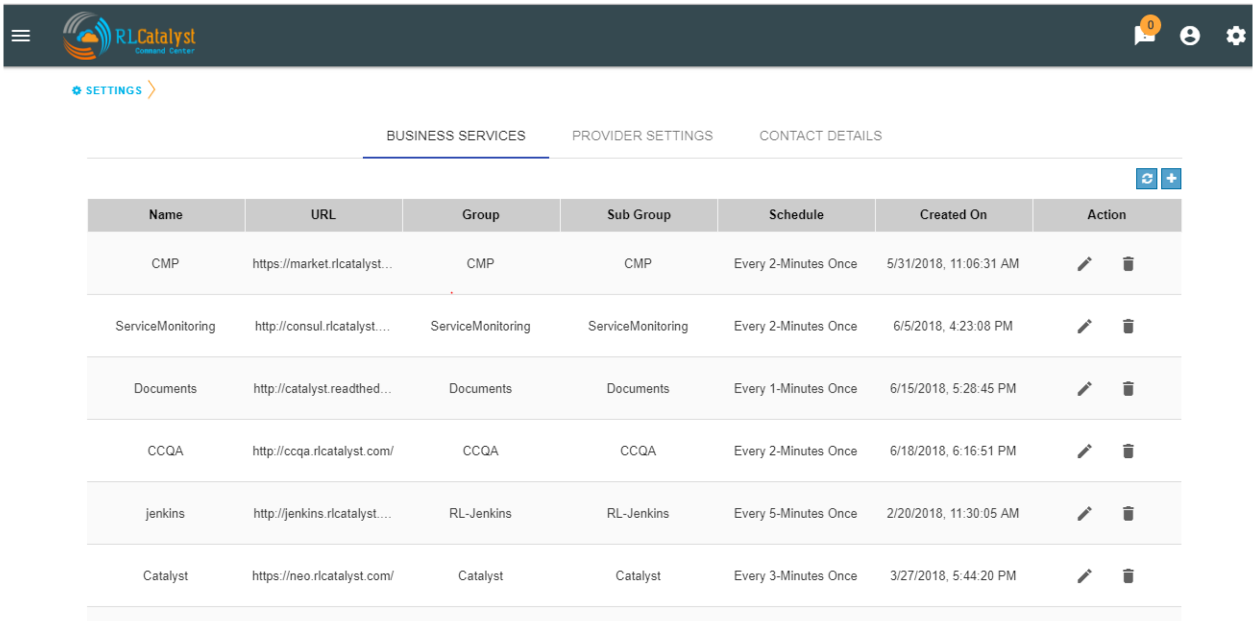
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.8.0-0 / Help

1.3.3 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

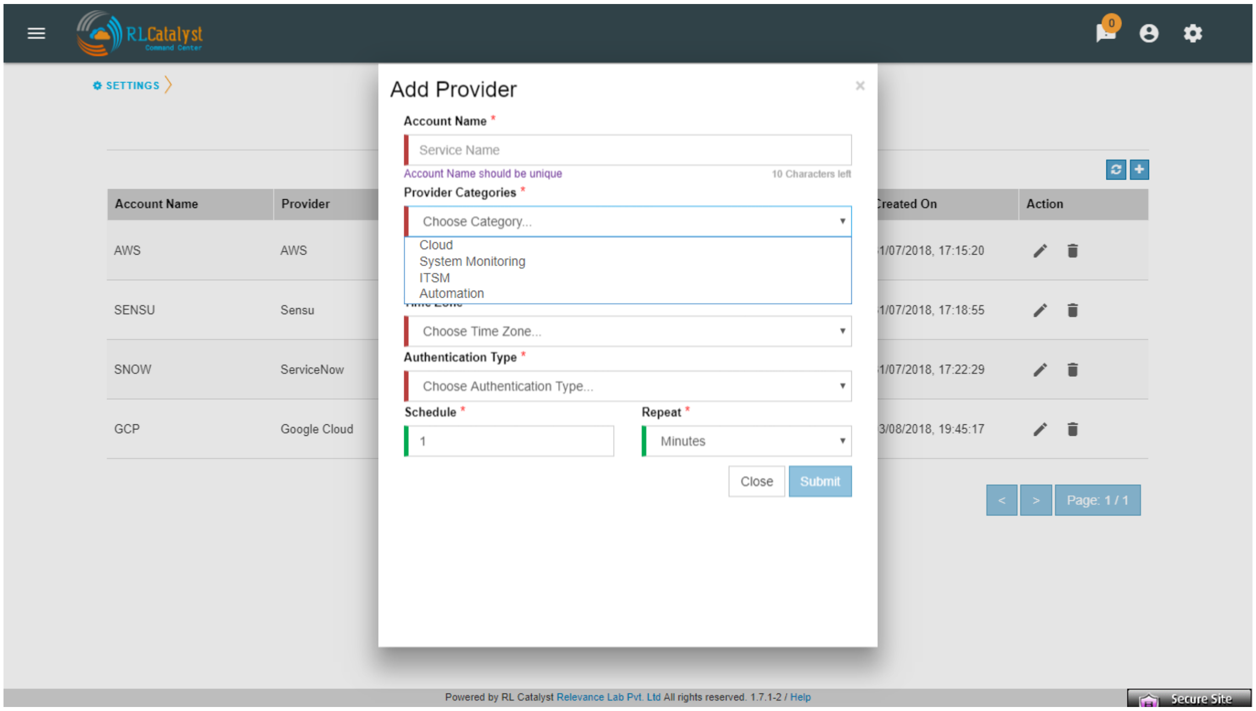
- Virtual Machines
- ELBs
- Security Groups
- Networks

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.



Name	URL	Group	Sub Group	Schedule	Created On	Action
CMP	https://market.rlcatalyst...	CMP	CMP	Every 2-Minutes Once	5/31/2018, 11:06:31 AM	✎ 🗑
ServiceMonitoring	http://consul.rlcatalyst....	ServiceMonitoring	ServiceMonitoring	Every 2-Minutes Once	6/5/2018, 4:23:08 PM	✎ 🗑
Documents	http://catalyst.readthed...	Documents	Documents	Every 1-Minutes Once	6/15/2018, 5:28:45 PM	✎ 🗑
CCQA	http://ccqa.rlcatalyst.com/	CCQA	CCQA	Every 2-Minutes Once	6/18/2018, 6:16:51 PM	✎ 🗑
jenkins	http://jenkins.rlcatalyst....	RL-Jenkins	RL-Jenkins	Every 5-Minutes Once	2/20/2018, 11:30:05 AM	✎ 🗑
Catalyst	https://neo.rlcatalyst.com/	Catalyst	Catalyst	Every 3-Minutes Once	3/27/2018, 5:44:20 PM	✎ 🗑

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



Add Provider

Account Name *
Service Name
Account Name should be unique
10 Characters left

Provider Categories *
Choose Category...
Cloud
System Monitoring
ITSM
Automation

Choose Time Zone...

Authentication Type *
Choose Authentication Type...

Schedule * 1
Repeat * Minutes

Account Name	Provider	Created On	Action
AWS	AWS	1/07/2018, 17:15:20	
SENSU	Sensu	1/07/2018, 17:18:55	
SNOW	ServiceNow	1/07/2018, 17:22:29	
GCP	Google Cloud	3/08/2018, 19:45:17	

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

Command Center will support for following Cloud Account providers.

- Microsoft Azure
- AWS
- Google Cloud
- DigitalOcean

To configure a Azure cloud account

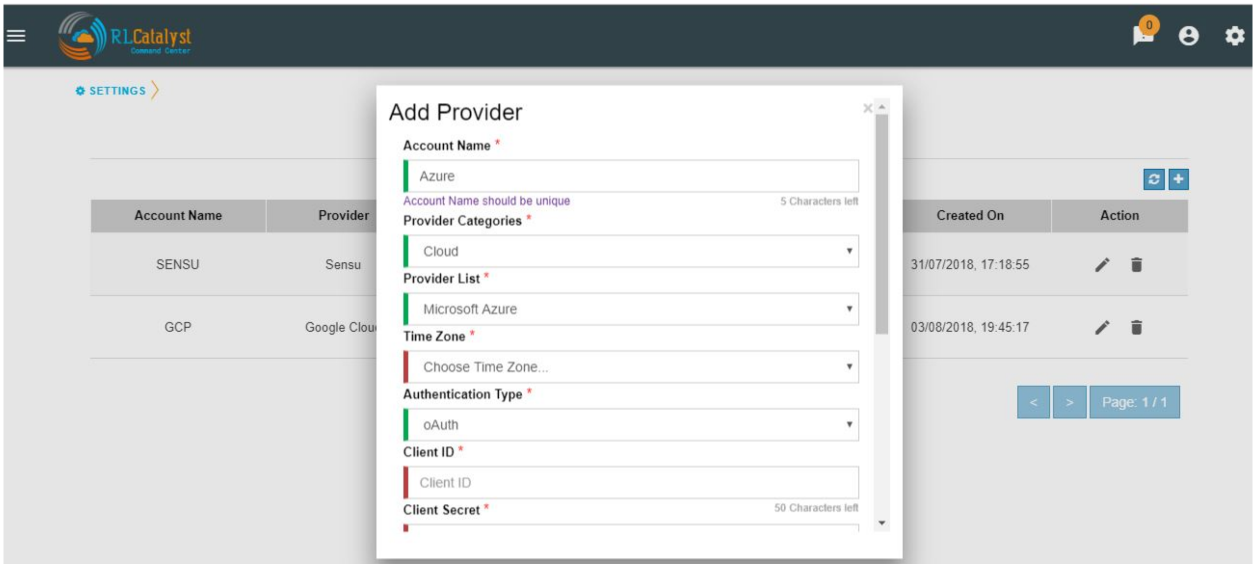
1. Click on the Settings icon in the top bar
2. Click on the Provider Settings tab
3. Click + button and add your cloud account credentials in Settings with the details captured in Appendix A. Example provided below is for a Microsoft Azure account.

Field	Instructions
Account Name	Enter a Friendly name
Provider Categories	Choose Cloud
Provider Categories	Choose Microsoft 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	https://management.azure.com/

Resource | https://management.azure.com/ |

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 *: Azure (Account Name should be unique; 5 Characters left)

Provider Categories *: Cloud

Provider List *: Microsoft Azure

Time Zone *: Choose Time Zone...

Authentication Type *: oAuth

Client ID *: Client ID

Client Secret *: 50 Characters left

Account Name	Provider	Created On	Action
SENSU	Sensu	31/07/2018, 17:18:55	
GCP	Google Clou	03/08/2018, 19:45:17	

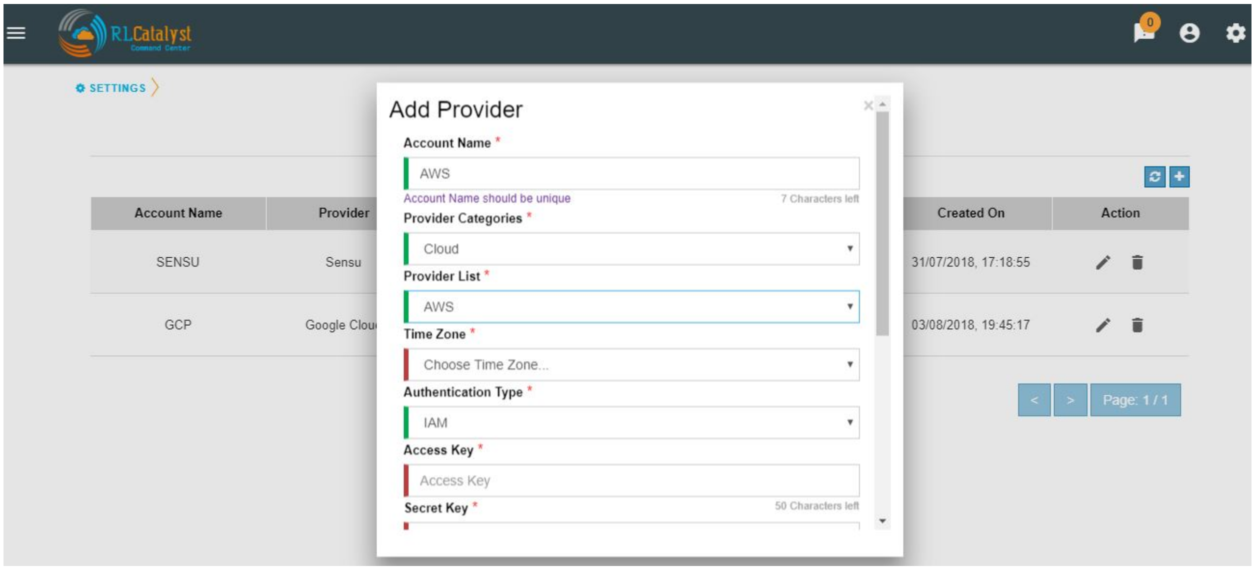
To configure a AWS cloud account

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 AWS account.

Field	Instructions
Account Name	Enter a Friendly name
Provider Categories	Choose Cloud
Provider List	Choose AWS
Time Zone	Choose IST
Authentication Type	Choose IAM
Access Key	Enter the Access Key of your AWS Application
Secret Key	Enter the Secret key of your AWS Application
Region	Enter the Region of your AWS Application
Account Number	Enter the Account Number of AWS Application

Account Number | Enter the Account Number of AWS Application |

Choose the required options | +——————————+————————————————————————————————+ | Schedule | Enter the Time Interval for collecting data from Cloud | +——————————+————————————————————————————————+ | Repeat | Choose the Interval Type – Minutes/Hourly | +——————————+————————————————————————————————+



Account Name	Provider	Created On	Action
SENSU	Sensu	31/07/2018, 17:18:55	
GCP	Google Clou	03/08/2018, 19:45:17	

< > Page: 1 / 1

Add Provider

Account Name *
AWS
Account Name should be unique — 7 Characters left

Provider Categories *
Cloud

Provider List *
AWS

Time Zone *
Choose Time Zone...

Authentication Type *
IAM

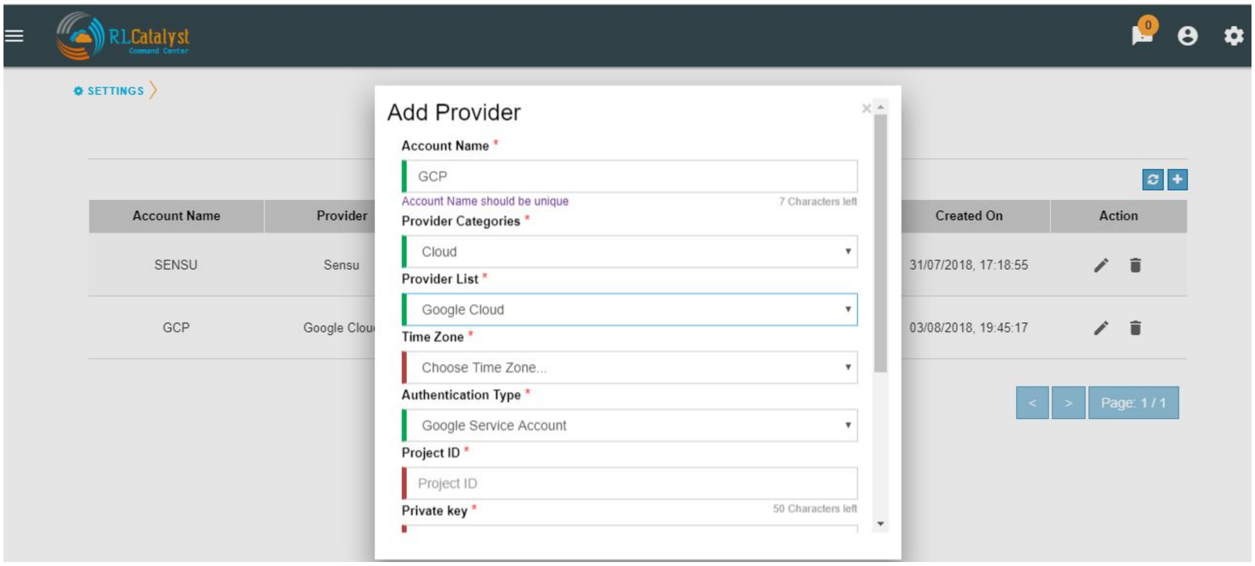
Access Key *
Access Key

Secret Key * — 50 Characters left

To configure a Google 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 Google Cloud account.

Field	Instructions
Account Name	Enter a Friendly name
Provider Categories	Choose Cloud
Provider List	Google Cloud
Time Zone	Choose IST
Authentication Type	Choose Google Service Account
Project ID	Enter the Project ID of your Google application
Private Key	Enter the Private key of your Google Application
Client Email	Enter the email of client generated email
Client Certificate URL	Enter the client generated URL
Schedule	Enter the Time Interval for collecting data from Cloud
Repeat	Choose the Interval Type – Minutes/Hourly



Add Provider

Account Name *
GCP
Account Name should be unique — 7 Characters left

Provider Categories *
Cloud

Provider List *
Google Cloud

Time Zone *
Choose Time Zone...

Authentication Type *
Google Service Account

Project ID *
Project ID
50 Characters left

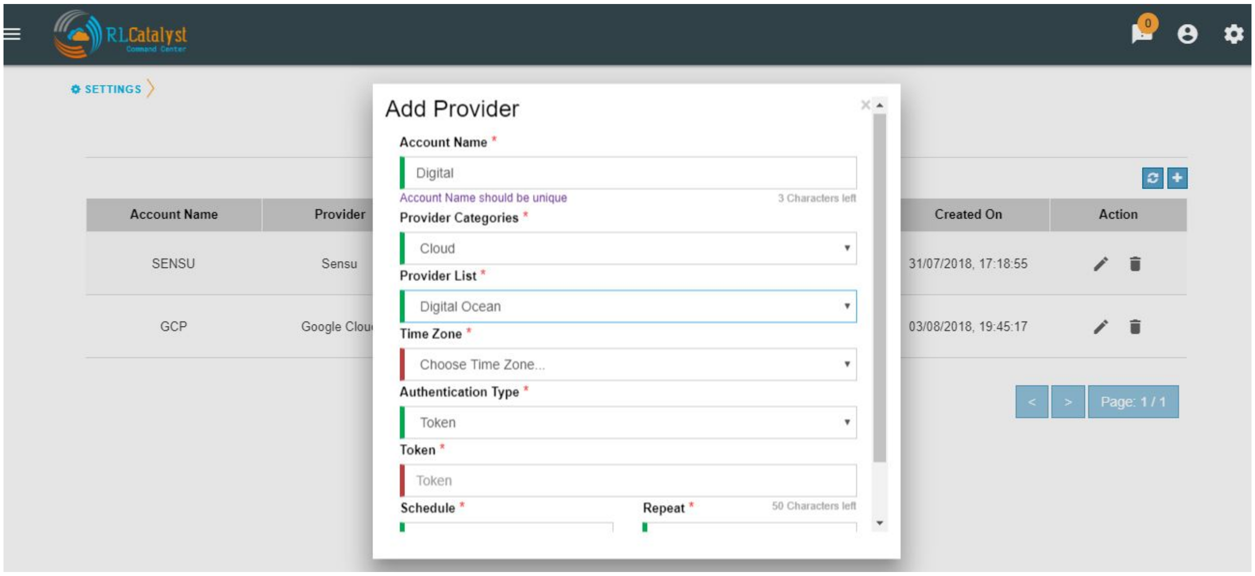
Private key *

Account Name	Provider	Created On	Action
SENSU	Sensu	31/07/2018, 17:18:55	
GCP	Google Clou	03/08/2018, 19:45:17	

To configure a DigitalOcean 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 DigitalOcean account.

Field	Instructions
Account Name	Enter a Friendly name
Provider Categories	Choose Cloud
Provider List	Choose Digital Ocean
Time Zone	Choose IST
Authentication Type	Choose Token
Token	Enter the token of your Digital Ocean application
Schedule	Enter the Time Interval for collecting data from Cloud
Repeat	Choose the Interval Type – Minutes/Hourly



Add Provider

Account Name *
Digital
Account Name should be unique — 3 Characters left

Provider Categories *
Cloud

Provider List *
Digital Ocean

Time Zone *
Choose Time Zone...

Authentication Type *
Token

Token *
Token
50 Characters left

Schedule * Repeat *

Account Name	Provider	Created On	Action
SENSU	Sensu	31/07/2018, 17:18:55	
GCP	Google Clou	03/08/2018, 19:45:17	

1.3.4 Configuring ITSM Credentials

Add ITSM service in provider settings, It will raise incident when service is down or not available. After adding ITSM, Dashboard and ITSM menu will update with cards. Clicking on the card will display the data regarding the particular card. ITSM will provide the direct link to the ITSM provider as whenever we select any incident it will redirect to the particular ITSM service.

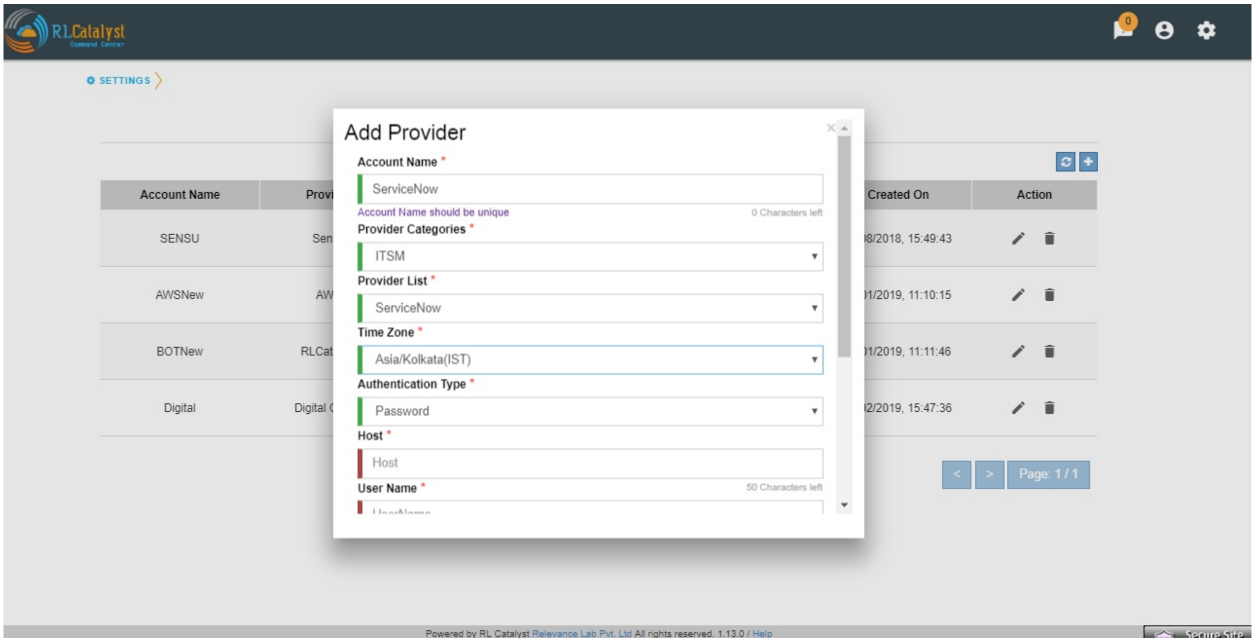
Command Center will support for following ITSM providers.

- ServiceNow
- FreshService

To configure a ServiceNow account

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

Field	Instructions
Account Name	Enter a Friendly name
Provider Categories	Choose ITSM
Provider List	Choose ServiceNow
Time Zone	Choose IST
Authentication Type	Password
Host	URL to your ServiceNow Instance E.g.:ven01746.service-now.com
UserName	Enter UserName
Password	Enter Password
Schedule	Enter the Time Interval for collecting data from Catalyst
Repeat	Choose the Interval Type-Minutes/Hourly



Account Name	Provi	Created On	Action
SENSU	Sen	)8/2018, 15:49:43	
AWSNew	AW	)1/2019, 11:10:15	
BOTNew	RLCat	)1/2019, 11:11:46	
Digital	Digital (	)2/2019, 15:47:36	

Add Provider

Account Name *: ServiceNow
Account Name should be unique — 0 Characters left

Provider Categories *: ITSM

Provider List *: ServiceNow

Time Zone *: Asia/Kolkata(IST)

Authentication Type *: Password

Host *: Host

User Name * — 50 Characters left: UserName

< > Page: 1 / 1
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.13.0 / Help
Secure Site

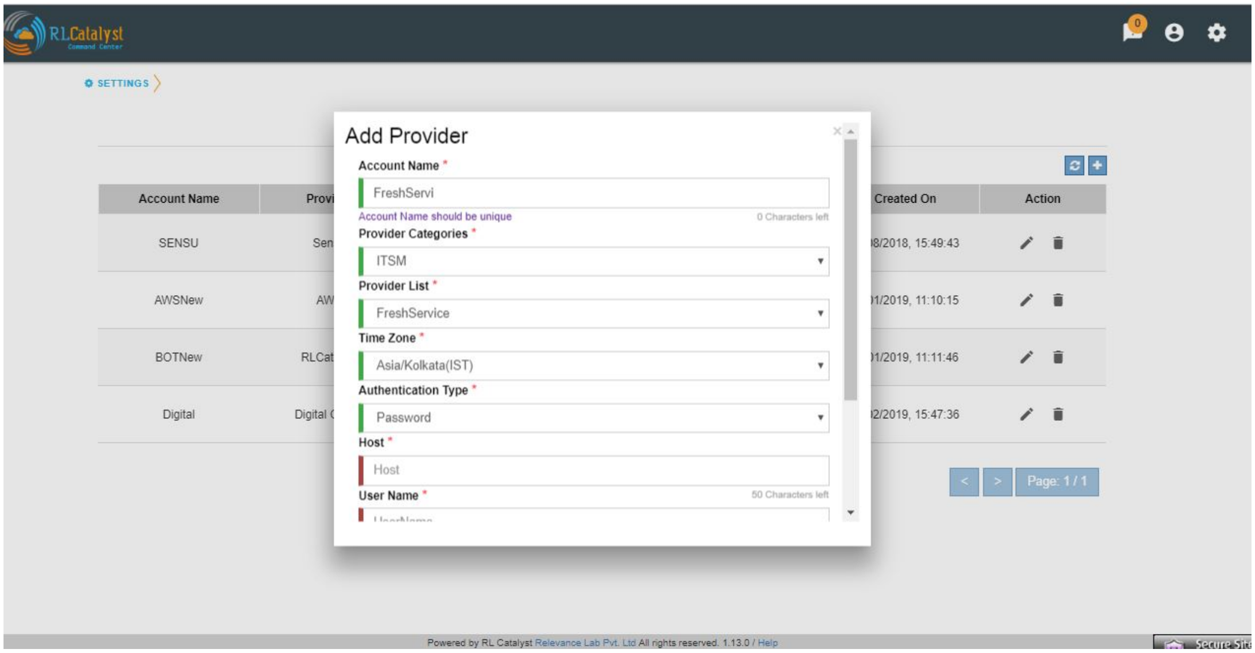
To configure a FreshService account

1. Click on the Settings icon in the top bar

2. Click on the Provider Settings tab

3. Click + button and add your ITSM account credentials in Settings with the details captured in Appendix A. Example provided below is for a FreshService account.

Field	Instructions
Account Name	Enter a Friendly name
Provider Categories	Choose ITSM
Provider List	Choose FreshService
Time Zone	Choose IST
Authentication Type	Password
Host	URL to your FreshService Instance E.g.https://rlab.freshservice.com
UserName	Enter UserName
Password	Enter Password
Schedule	Enter the Time Interval for collecting data from Catalyst
Repeat	Choose the Interval Type-Minutes/Hourly



Account Name	Provi	Created On	Action
SENSU	Sen	8/2018, 15:49:43	
AWSNew	AW	1/2019, 11:10:15	
BOTNew	RLCat	1/2019, 11:11:46	
Digital	Digital (	2/2019, 15:47:36	

Add Provider

Account Name *
FreshServi
Account Name should be unique
0 Characters left

Provider Categories *
ITSM

Provider List *
FreshService

Time Zone *
Asia/Kolkata(IST)

Authentication Type *
Password

Host *
Host

User Name *
50 Characters left

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.13.0 / Help

1.3.5 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.

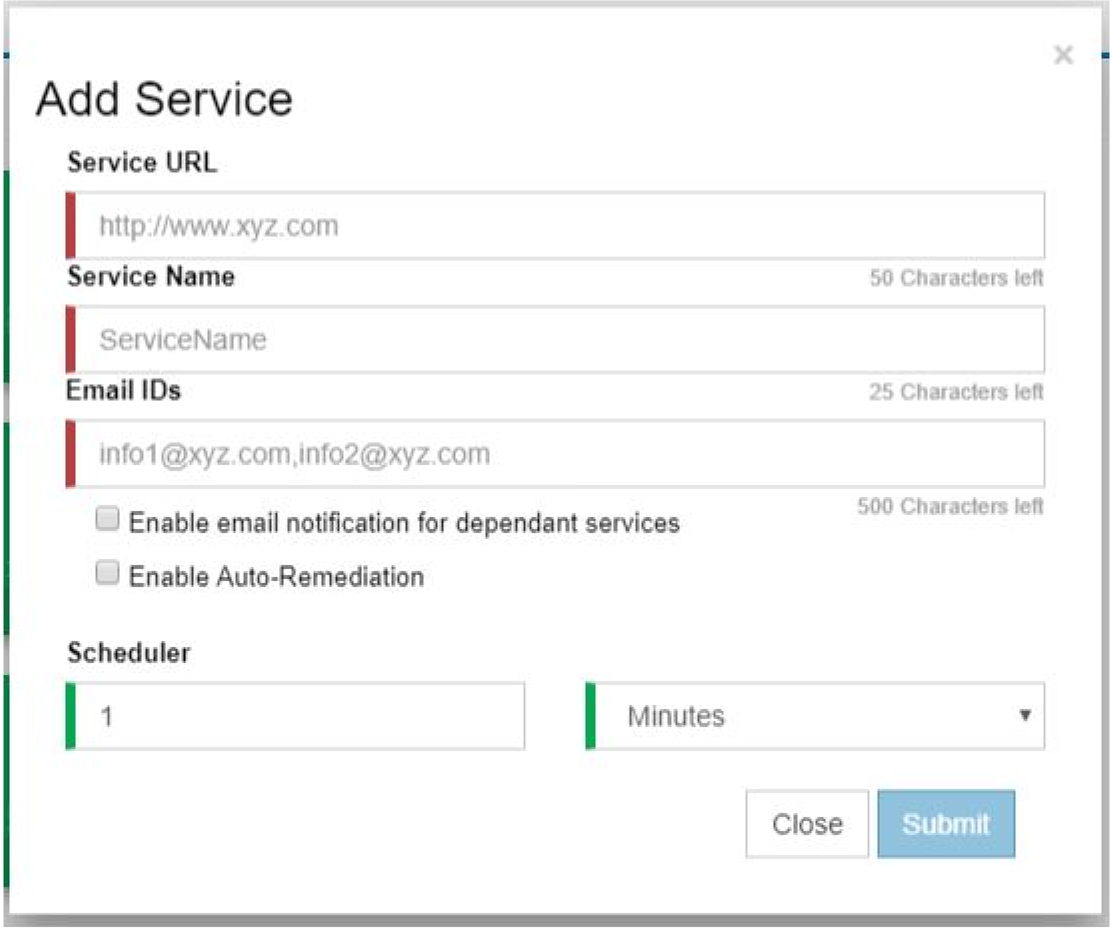
2. Add the Business Service URL (should be accessible from the Command Centre)

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

http://www.xyz.com

Service Name — 50 Characters left

ServiceName

Email IDs — 25 Characters left

info1@xyz.com,info2@xyz.com

500 Characters left

□ Enable email notification for dependant services

□ Enable Auto-Remediation

Scheduler

1 — Minutes ▾

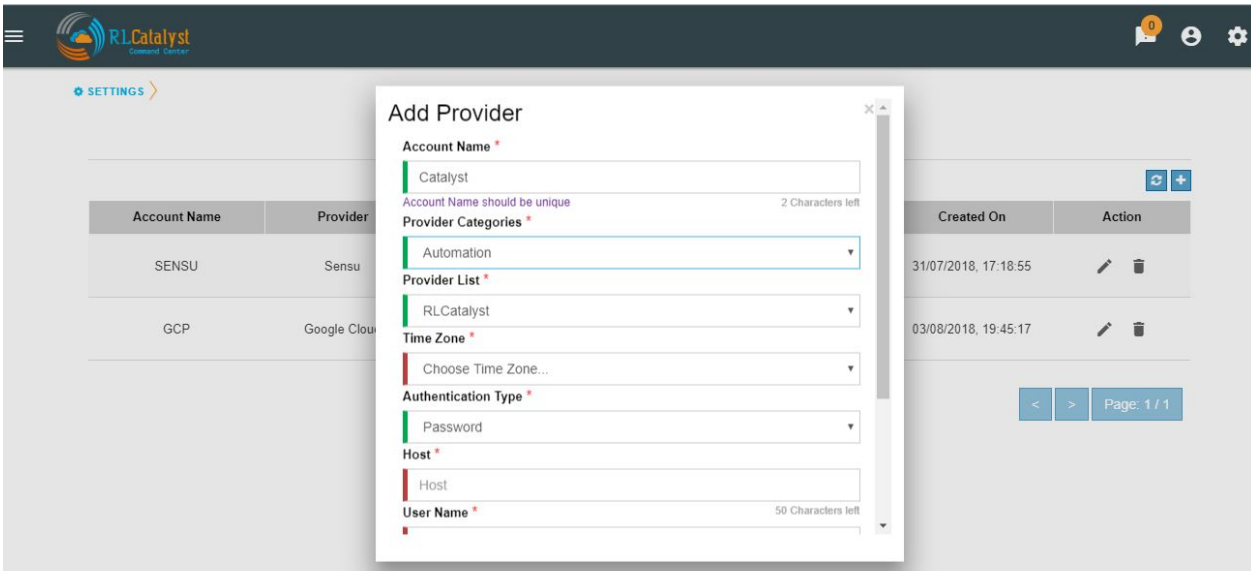
1.3.6 Configuring the Catalyst Account

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
Provider Categories	Choose Automation
Provider List	Choose RLCatalyst
Time Zone	Choose IST
Authentication Type	Password
Host	URL to your RLCatalyst Instance E.g.:https://neo.rlcatalyst.com/
UserName	Enter UserName
Password	Enter Password
Schedule	Enter the Time Interval for collecting data from Catalyst
Repeat	Choose the Interval Type-Minutes/Hourly



Account Name	Provider	Created On	Action
SENSU	Sensu	31/07/2018, 17:18:55	
GCP	Google Clou	03/08/2018, 19:45:17	

Add Provider

Account Name *
Catalyst
Account Name should be unique — 2 Characters left

Provider Categories *
Automation

Provider List *
RLCatalyst

Time Zone *
Choose Time Zone...

Authentication Type *
Password

Host *
Host

User Name * — 50 Characters left

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

1.3.7 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.

1. Login to <customer name>neo.rlcatalyst.com with the given credentials -> Go to Work zone.

2. Click on the tree on the left to choose the Organization, Business Group, Project and

   Environment. By default, there will be o Organization with the customer name

   o Business Group 'DevOps' o Project 'Demo Project'

   o Environments - <customer name>_EVL, <customer name>_DEV, <customer name>_QA,

<customer name>_PROD, <customer name>_DEVOPS

3. Choose one of the environments
4. 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

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 Tenat>
Parameter4	URL
Parameter5	Checks interval e.g. 60s

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

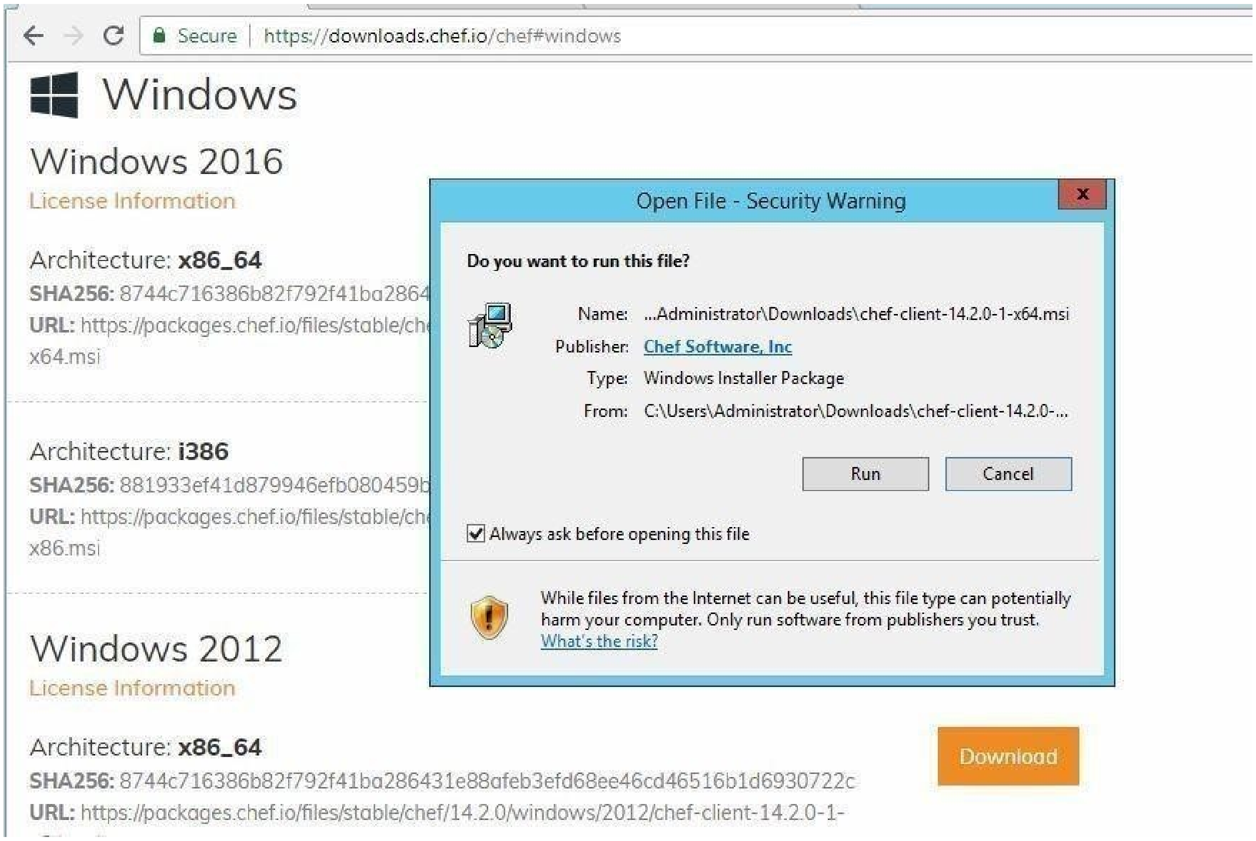
Install monitoring agents on a Windows machine manually

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.

Procedure

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



Windows 2016

License Information

Architecture: **x86_64**

SHA256: 8744c716386b82f792f41ba2864

URL: https://packages.chef.io/files/stable/che
x64.msi

Architecture: **i386**

SHA256: 881933ef41d879946efb080459b

URL: https://packages.chef.io/files/stable/che
x86.msi

Windows 2012

License Information

Architecture: **x86_64**

SHA256: 8744c716386b82f792f41ba286431e88afeb3efd68ee46cd46516b1d6930722c

URL: https://packages.chef.io/files/stable/chef/14.2.0/windows/2012/chef-client-14.2.0-1-

Open File - Security Warning

Do you want to run this file?

Name: ...Administrator\Downloads\chef-client-14.2.0-1-x64.msi

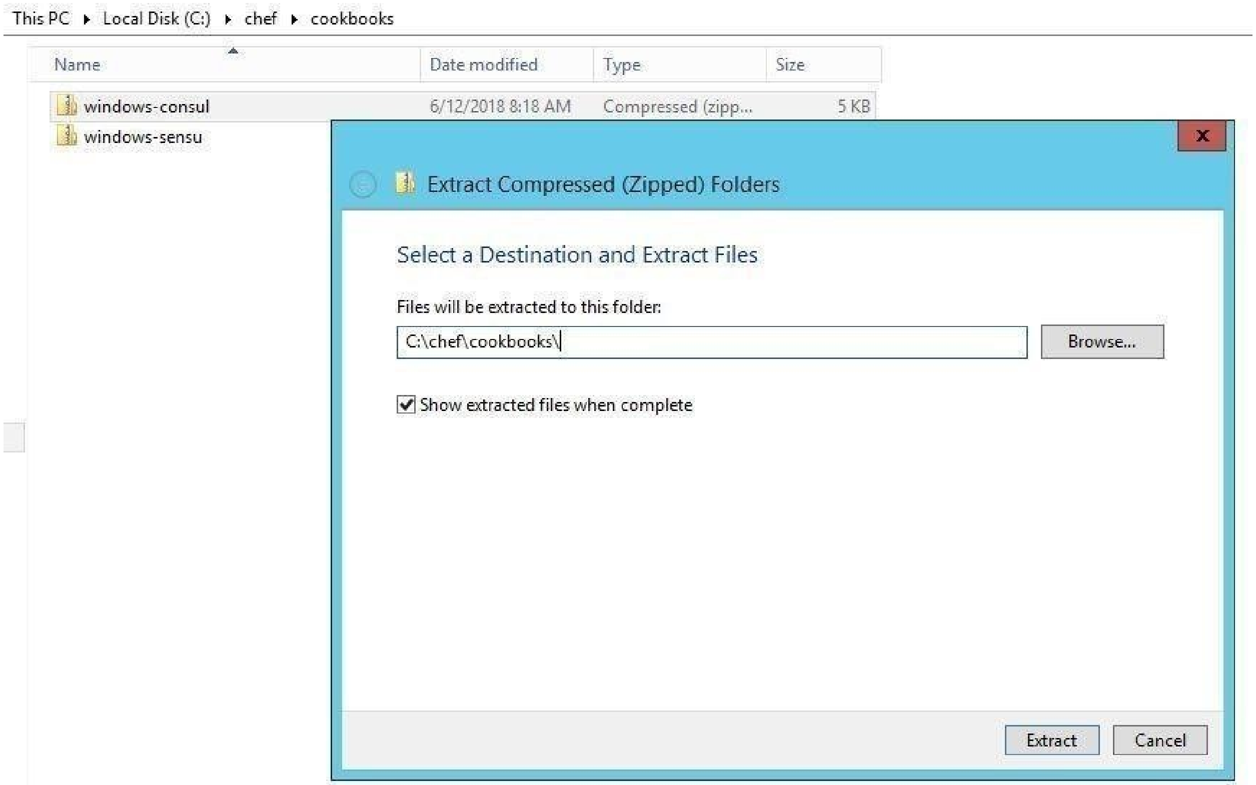
Publisher: Chef Software, Inc

Type: Windows Installer Package

From: C:\Users\Administrator\Downloads\chef-client-14.2.0-...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?



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

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

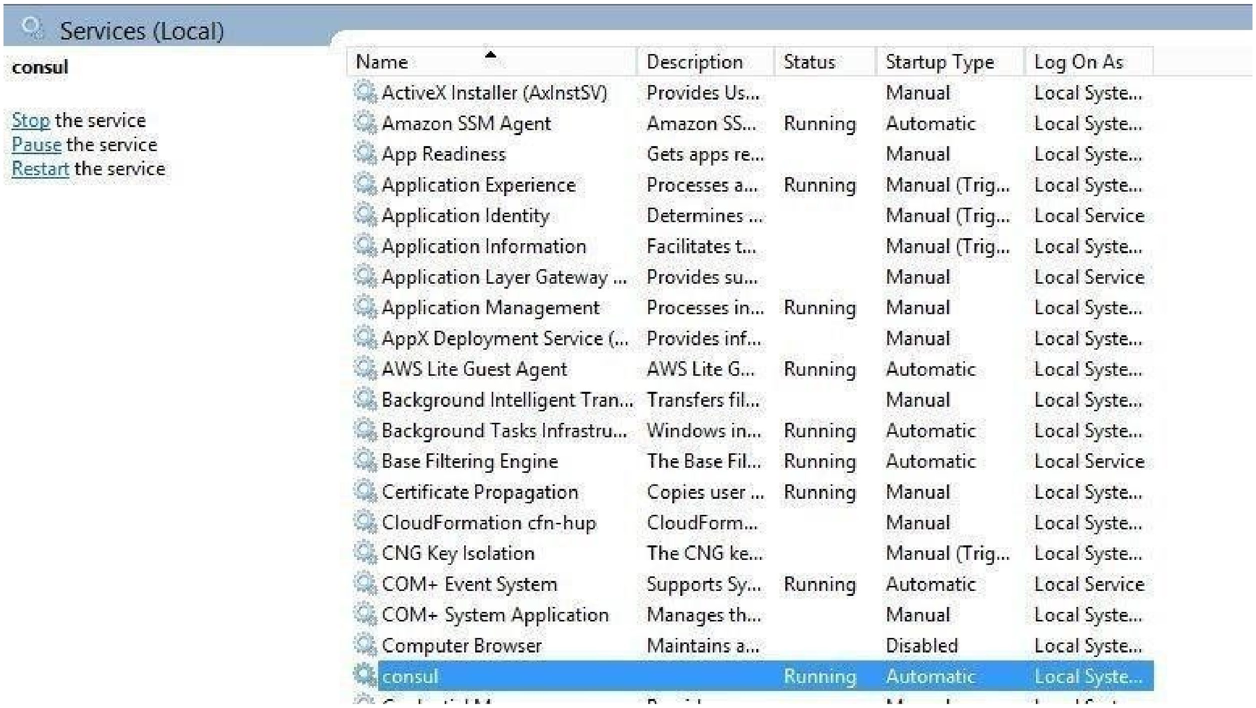
Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

C:\chef\cookbooks\

☑ Show extracted files when complete

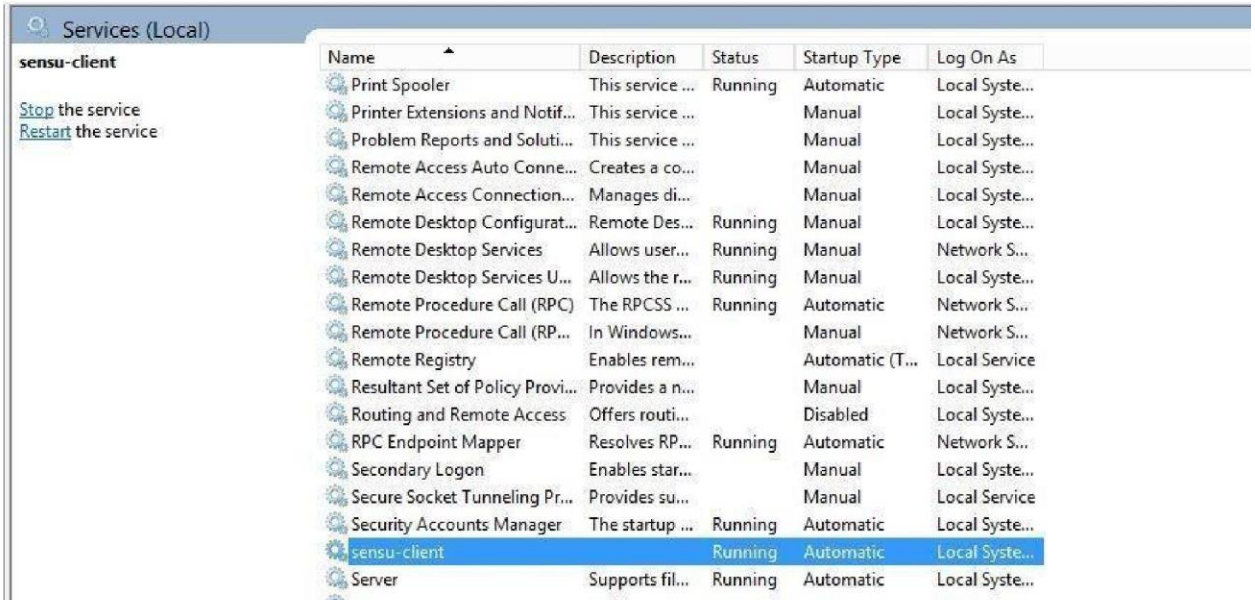


Services (Local)

consul

Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Amazon SSM Agent	Amazon SS...	Running	Automatic	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Experience	Processes a...	Running	Manual (Trig...	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...		Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...	Running	Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
AWS Lite Guest Agent	AWS Lite G...	Running	Automatic	Local Syste...
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
CloudFormation cfn-hup	CloudForm...		Manual	Local Syste...
CNG Key Isolation	The CNG ke...		Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local Syste...
Computer Browser	Maintains a...		Disabled	Local Syste...
consul		Running	Automatic	Local Syste...



Services (Local)

sensu-client

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Print Spooler	This service ...	Running	Automatic	Local Syste...
Printer Extensions and Notif...	This service ...		Manual	Local Syste...
Problem Reports and Soluti...	This service ...		Manual	Local Syste...
Remote Access Auto Conne...	Creates a co...		Manual	Local Syste...
Remote Access Connection...	Manages di...		Manual	Local Syste...
Remote Desktop Configurat...	Remote Des...	Running	Manual	Local Syste...
Remote Desktop Services	Allows user...	Running	Manual	Network S...
Remote Desktop Services U...	Allows the r...	Running	Manual	Local Syste...
Remote Procedure Call (RPC)	The RPCSS ...	Running	Automatic	Network S...
Remote Procedure Call (RP...	In Windows...		Manual	Network S...
Remote Registry	Enables rem...		Automatic (T...	Local Service
Resultant Set of Policy Provi...	Provides a n...		Manual	Local Syste...
Routing and Remote Access	Offers routi...		Disabled	Local Syste...
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Secondary Logon	Enables star...		Manual	Local Syste...
Secure Socket Tunneling Pr...	Provides su...		Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
sensu-client		Running	Automatic	Local Syste...
Server	Supports fil...	Running	Automatic	Local Syste...

Install monitoring agent(Zabbix) on a Ubuntu machine manually

Procedure

1. Zabbix apt repositories are available on Zabbix official website. Add the repository to install required packages for Zabbix agent using the following command wget http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.4-1%2Bbionic_all.deb

2. **Un-zip the downloaded file using following command** dpkg -i zabbix-release_3.4-1+trusty_all.deb

3. **As you have successfully added Zabbix apt repositories in your system let's use the following command to install Zabbix a**
   sudo apt-get update sudo apt-get install zabbix-agent

4. **After installation of Zabbix agent. Edit Zabbix agent configuration file /etc/zabbix/zabbix_agentd.conf and update Zabbix**
   #Server=[zabbix server ip] #Hostname=[Hostname of client system]

   Server=192.168.1.10 Hostname=Server2

   Here 192.168.1.10 is the IP of Zabbix server to allow for connection with this Zabbix client.

5. **After adding Zabbix server IP in the configuration file, now restart agent service using below command.**
   sudo systemctl start zabbix-agent

1.4 Features

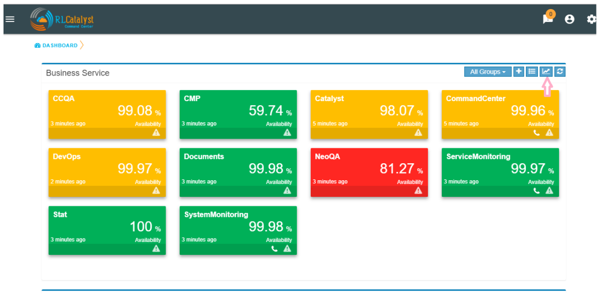
1.4.1 Historical BSM Health Indicator

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.

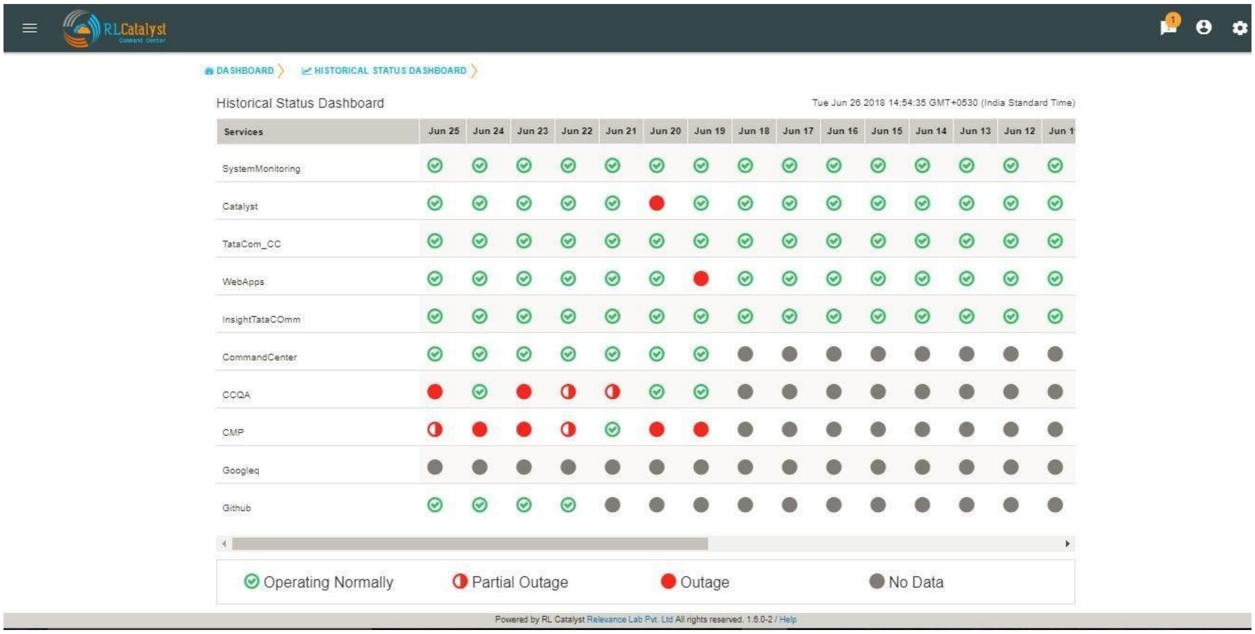
There is tab like "Business Services" in the main page.When we click on that tab,it's navigated to Business services page.In that page we see the bot's summary information,snow tickets information etc. . . .

images/Navigation_BSM.PNG



Business Service

CCQA 99.08 % 3 minutes ago Availability	CMP 59.74 % 3 minutes ago Availability	Catalyst 98.07 % 5 minutes ago Availability	CommandCenter 99.96 % 5 minutes ago Availability
DevOps 99.97 % 2 minutes ago Availability	Documents 99.98 % 3 minutes ago Availability	NeoQA 81.27 % 3 minutes ago Availability	ServiceMonitoring 99.97 % 3 minutes ago Availability
Stat 100 % 3 minutes ago Availability	SystemMonitoring 99.98 % 3 minutes ago Availability		



Historical Status Dashboard

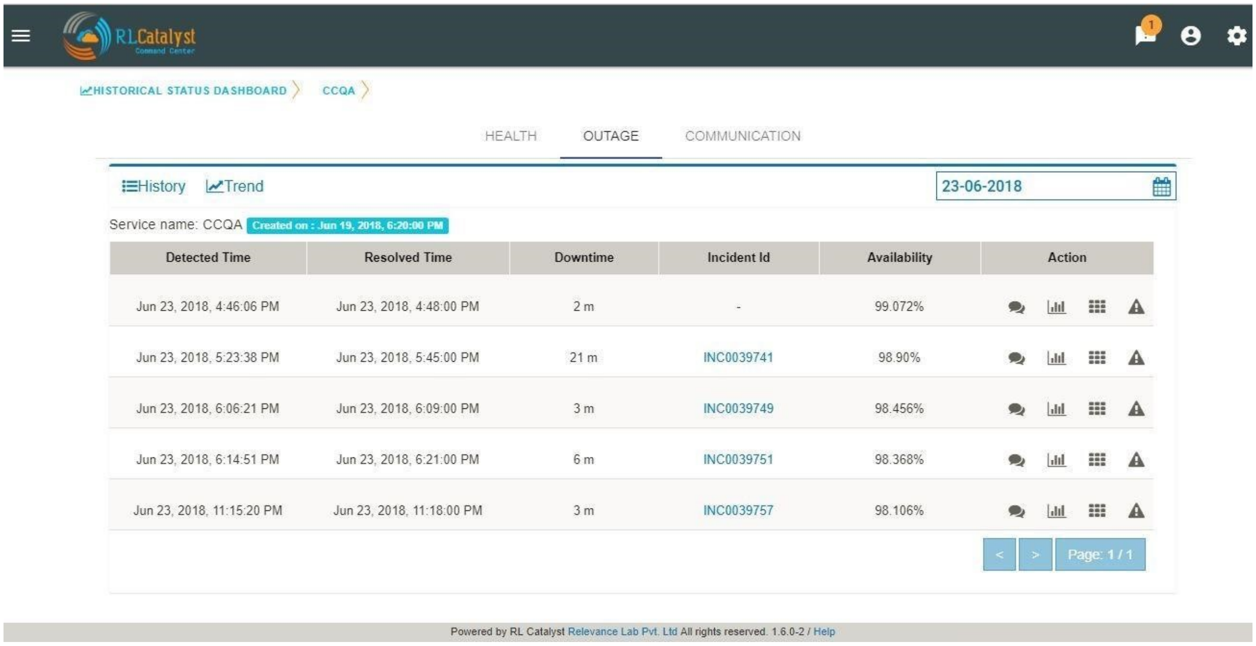
Tue Jun 26 2018 14:54:35 GMT+0530 (India Standard Time)

Services	Jun 25	Jun 24	Jun 23	Jun 22	Jun 21	Jun 20	Jun 19	Jun 18	Jun 17	Jun 16	Jun 15	Jun 14	Jun 13	Jun 12	Jun 1
SystemMonitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst	✓	✓	✓	✓	✓	🔴	✓	✓	✓	✓	✓	✓	✓	✓	✓
TataCom_CC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WebApps	✓	✓	✓	✓	✓	✓	🔴	✓	✓	✓	✓	✓	✓	✓	✓
InsightTataCOmm	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CommandCenter	✓	✓	✓	✓	✓	✓	✓	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫
CCQA	🔴	✓	🔴	◐	◐	✓	✓	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫
CMP	◐	🔴	🔴	◐	✓	🔴	🔴	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫
Googleq	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫
Github	✓	✓	✓	✓	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫

✓ Operating Normally ◐ Partial Outage 🔴 Outage ⚫ No Data

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.6.0-2 / Help

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



Service name: CCQA Created on : Jun 19, 2018, 6:20:00 PM

Detected Time	Resolved Time	Downtime	Incident Id	Availability	Action
Jun 23, 2018, 4:46:06 PM	Jun 23, 2018, 4:48:00 PM	2 m	-	99.072%	
Jun 23, 2018, 5:23:38 PM	Jun 23, 2018, 5:45:00 PM	21 m	INC0039741	98.90%	
Jun 23, 2018, 6:06:21 PM	Jun 23, 2018, 6:09:00 PM	3 m	INC0039749	98.456%	
Jun 23, 2018, 6:14:51 PM	Jun 23, 2018, 6:21:00 PM	6 m	INC0039751	98.368%	
Jun 23, 2018, 11:15:20 PM	Jun 23, 2018, 11:18:00 PM	3 m	INC0039757	98.106%	

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.6.0-2 / Help

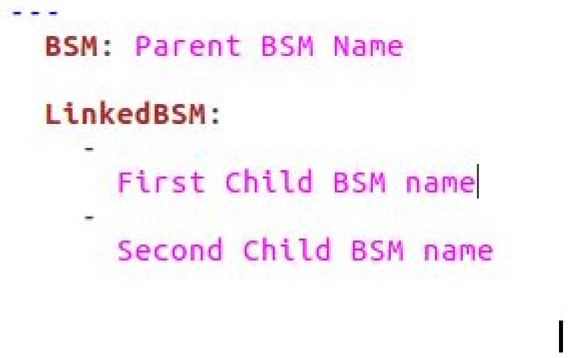
1.4.2 Multi-level Business Service

Multi-level Business Service feature will show the Dependent Business services(Linked Business Services) of the Business Service. User can provide any Business service as Dependent Business service of another Business Service. Whenever dependent Business Service went down the parent Business Service also shown as Yellow.

Configuration

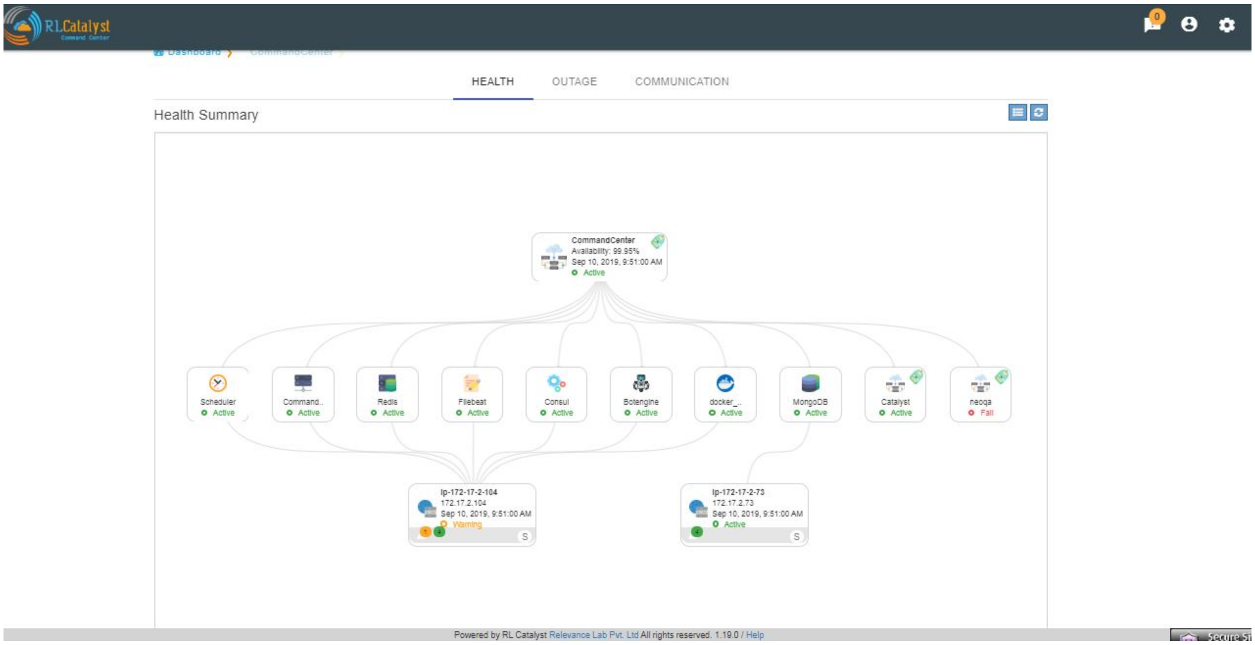
User will provide the Dependency between Business Service using Yaml file. The Yaml file should follow the following rules.

- File Name should be in the following order <tenantID>.<BSM Name>.yml.
- The YAML file should contain Parent BSM and their linked BSM's
- Once the YAML is complete it should be added to the topologies folder.
- Then the scheduler server should be restart to refresh all the topologies picked from the file.



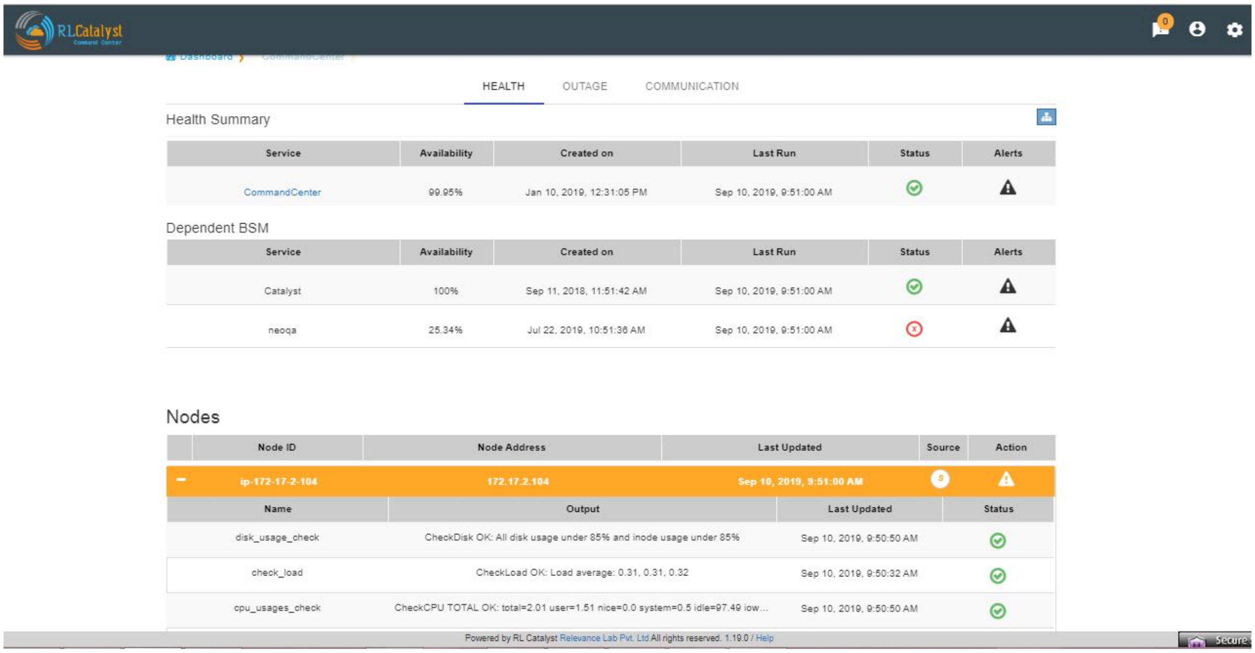
```
---
  BSM: Parent BSM Name

  LinkedBSM:
    -
      First Child BSM name
    -
      Second Child BSM name
```

The dendent Business service will show in the topology(Graphical view and List View) and quick view topology.



Health Summary

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help



Health Summary

Service	Availability	Created on	Last Run	Status	Alerts
CommandCenter	99.95%	Jan 10, 2019, 12:31:05 PM	Sep 10, 2019, 9:51:00 AM	✓	⚠

Dependent BSM

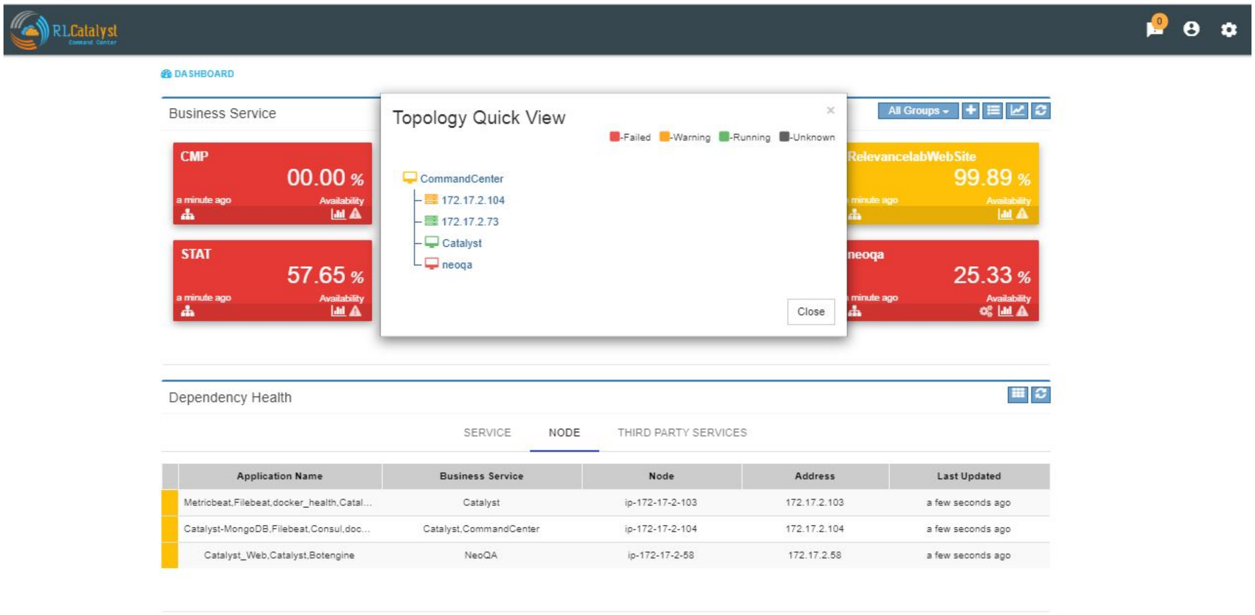
Service	Availability	Created on	Last Run	Status	Alerts
Catalyst	100%	Sep 11, 2018, 11:51:42 AM	Sep 10, 2019, 9:51:00 AM	✓	⚠
neoqa	25.34%	Jul 22, 2019, 10:51:36 AM	Sep 10, 2019, 9:51:00 AM	ⓧ	⚠

Nodes

	Node ID	Node Address	Last Updated	Source	Action
−	ip-172-17-2-104	172.17.2.104	Sep 10, 2019, 9:51:00 AM	S	⚠

Name	Output	Last Updated	Status
disk_usage_check	CheckDisk OK: All disk usage under 85% and inode usage under 85%	Sep 10, 2019, 9:50:50 AM	✓
check_load	CheckLoad OK: Load average: 0.31, 0.31, 0.32	Sep 10, 2019, 9:50:32 AM	✓
cpu_usages_check	CheckCPU TOTAL OK: total=2.01 user=1.51 nice=0.0 system=0.5 idle=97.49 iow...	Sep 10, 2019, 9:50:50 AM	✓

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help



	Application Name	Business Service	Node	Address	Last Updated
	Metricbeat,Filebeat,docker_health,Catal...	Catalyst	ip-172-17-2-103	172.17.2.103	a few seconds ago
	Catalyst-MongoDB,Filebeat,Consul,doc...	Catalyst,CommandCenter	ip-172-17-2-104	172.17.2.104	a few seconds ago
	Catalyst_Web,Catalyst,Botengine	NeoQA	ip-172-17-2-58	172.17.2.58	a few seconds ago

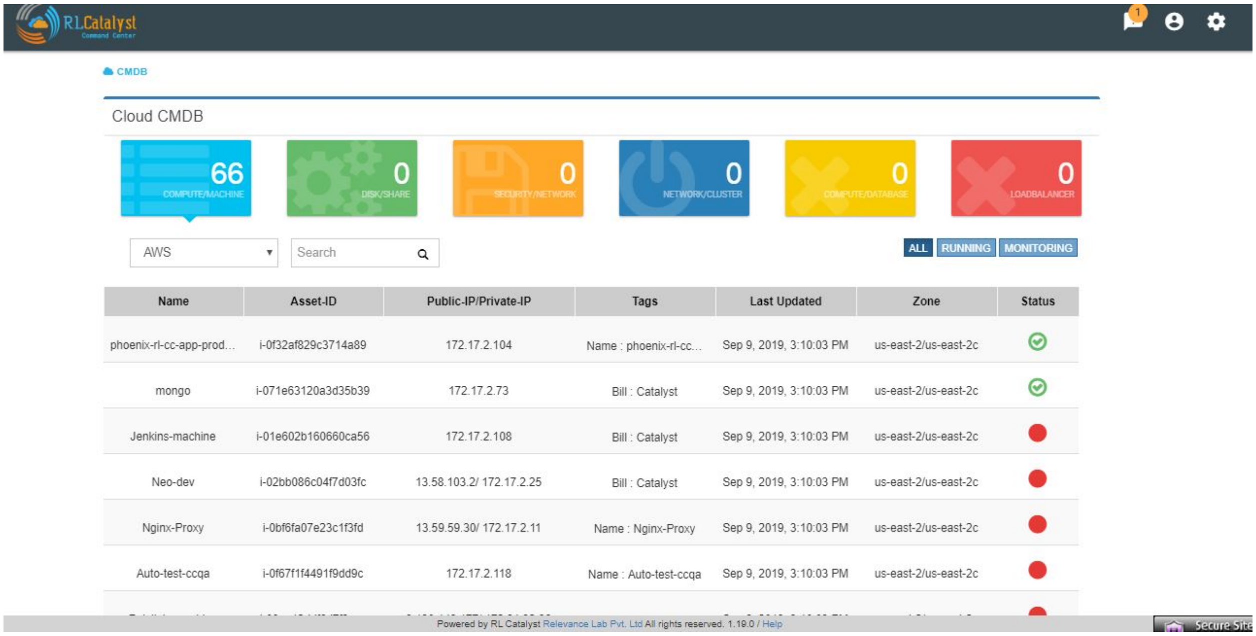
1.4.3 Viewing Cloud Assets

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

1. Virtual machines
2. Disks
3. Security Groups
4. Network Cluster
5. Compute Databases
6. 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)

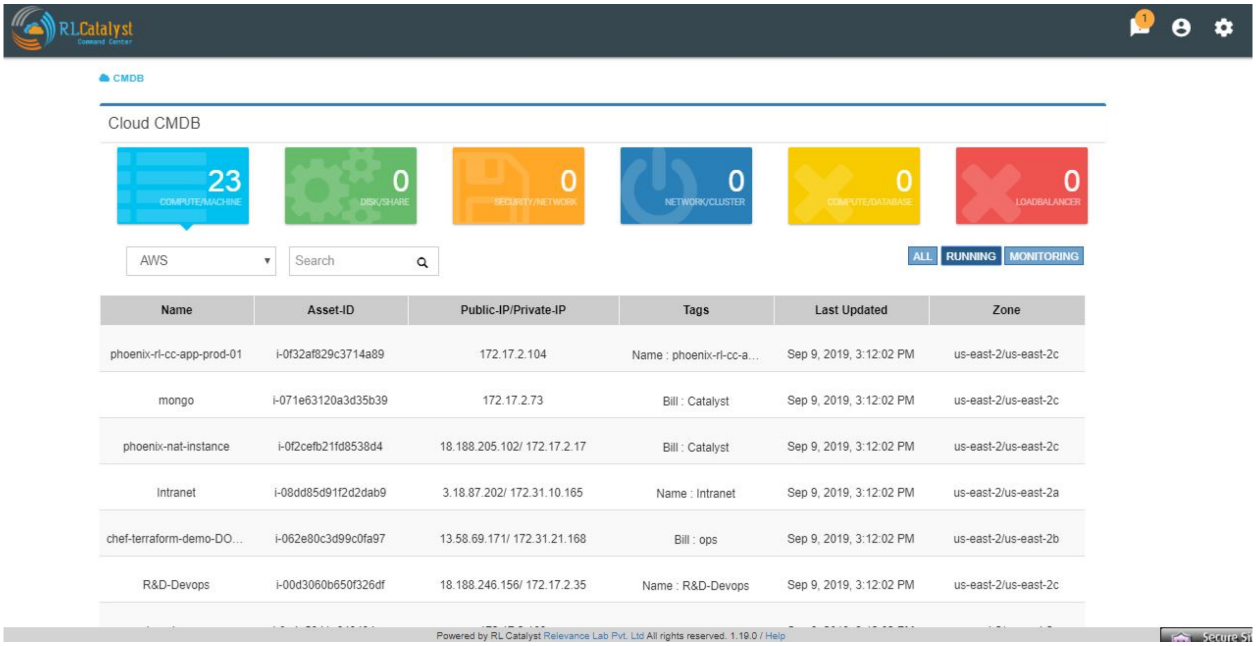


Cloud CMDB

Name	Asset-ID	Public-IP/Private-IP	Tags	Last Updated	Zone	Status
phoenix-rl-cc-app-prod…	i-0f32af829c3714a89	172.17.2.104	Name : phoenix-rl-cc…	Sep 9, 2019, 3:10:03 PM	us-east-2/us-east-2c	✓
mongo	i-071e63120a3d35b39	172.17.2.73	Bill : Catalyst	Sep 9, 2019, 3:10:03 PM	us-east-2/us-east-2c	✓
Jenkins-machine	i-01e602b160660ca56	172.17.2.108	Bill : Catalyst	Sep 9, 2019, 3:10:03 PM	us-east-2/us-east-2c	●
Neo-dev	i-02bb086c04f7d03fc	13.58.103.2/ 172.17.2.25	Bill : Catalyst	Sep 9, 2019, 3:10:03 PM	us-east-2/us-east-2c	●
Nginx-Proxy	i-0bf6fa07e23c1f3fd	13.59.59.30/ 172.17.2.11	Name : Nginx-Proxy	Sep 9, 2019, 3:10:03 PM	us-east-2/us-east-2c	●
Auto-test-ccqa	i-0f67f1f4491f9dd9c	172.17.2.118	Name : Auto-test-ccqa	Sep 9, 2019, 3:10:03 PM	us-east-2/us-east-2c	●

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

Running: displays all the running nodes

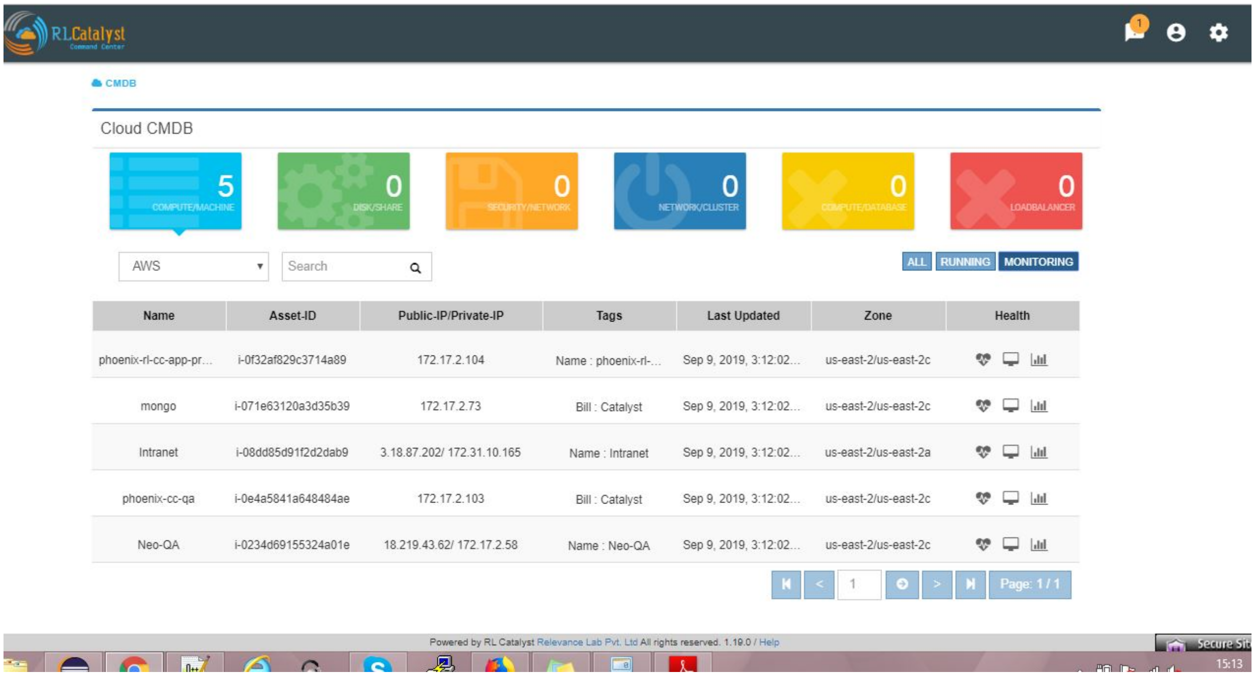


Cloud CMDB

Name	Asset-ID	Public-IP/Private-IP	Tags	Last Updated	Zone
phoenix-rl-cc-app-prod-01	i-0f32af829c3714a89	172.17.2.104	Name : phoenix-rl-cc-a…	Sep 9, 2019, 3:12:02 PM	us-east-2/us-east-2c
mongo	i-071e63120a3d35b39	172.17.2.73	Bill : Catalyst	Sep 9, 2019, 3:12:02 PM	us-east-2/us-east-2c
phoenix-nat-instance	i-0f2cefb21fd8538d4	18.188.205.102/ 172.17.2.17	Bill : Catalyst	Sep 9, 2019, 3:12:02 PM	us-east-2/us-east-2c
Intranet	i-08dd85d91f2d2dab9	3.18.87.202/ 172.31.10.165	Name : Intranet	Sep 9, 2019, 3:12:02 PM	us-east-2/us-east-2a
chef-terraform-demo-DO…	i-062e80c3d99c0fa97	13.58.69.171/ 172.31.21.168	Bill : ops	Sep 9, 2019, 3:12:02 PM	us-east-2/us-east-2b
R&D-Devops	i-00d3060b650f326df	18.188.246.156/ 172.17.2.35	Name : R&D-Devops	Sep 9, 2019, 3:12:02 PM	us-east-2/us-east-2c

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

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.

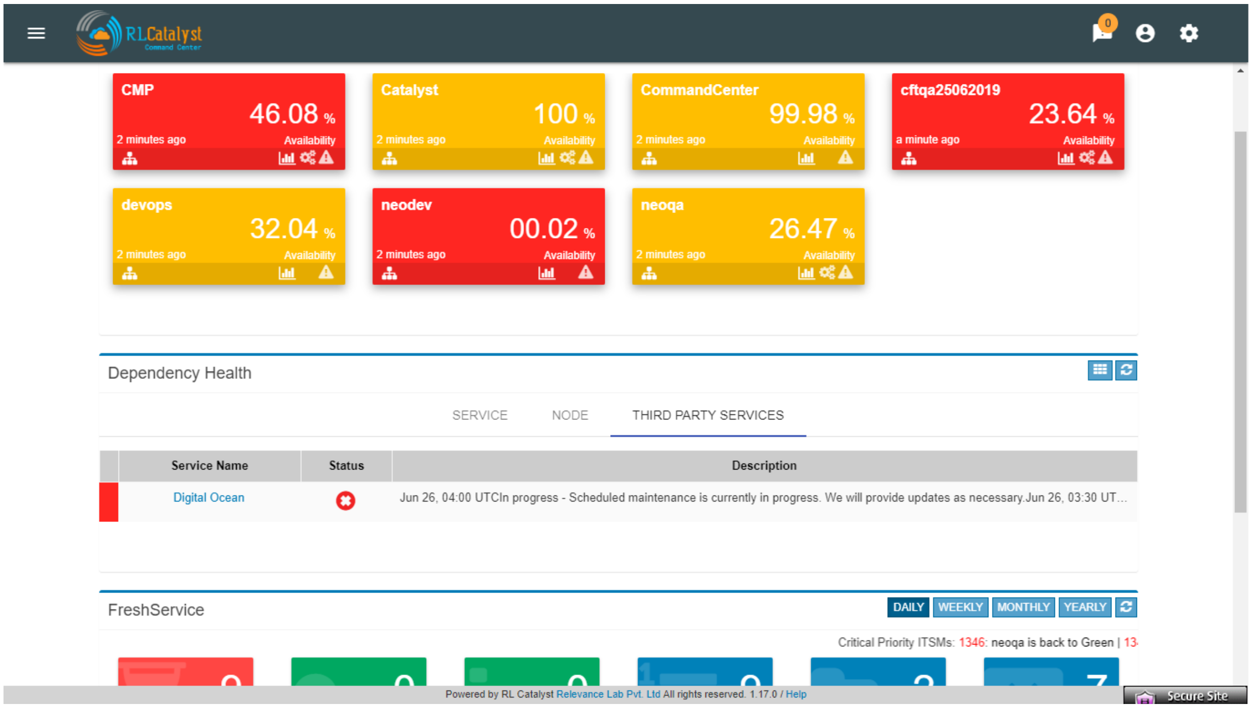


Name	Asset-ID	Public-IP/Private-IP	Tags	Last Updated	Zone	Health
phoenix-rl-cc-app-pr…	i-0f32af829c3714a89	172.17.2.104	Name : phoenix-rl-…	Sep 9, 2019, 3:12:02…	us-east-2/us-east-2c	
mongo	i-071e63120a3d35b39	172.17.2.73	Bill : Catalyst	Sep 9, 2019, 3:12:02…	us-east-2/us-east-2c	
Intranet	i-08dd85d91f2d2dab9	3.18.87.202/ 172.31.10.165	Name : Intranet	Sep 9, 2019, 3:12:02…	us-east-2/us-east-2a	
phoenix-cc-qa	i-0e4a5841a648484ae	172.17.2.103	Bill : Catalyst	Sep 9, 2019, 3:12:02…	us-east-2/us-east-2c	
Neo-QA	i-0234d69155324a01e	18.219.43.62/ 172.17.2.58	Name : Neo-QA	Sep 9, 2019, 3:12:02…	us-east-2/us-east-2c	

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

1.4.4 RSS-Feed for cloud providers

A new tab Third party tab will be displayed in Dependency Health panel, which will monitor the cloud provider status which tenant has added in the provider settings.



Service Name	Status	Description
Digital Ocean	✖	Jun 26, 04:00 UTCIn progress - Scheduled maintenance is currently in progress. We will provide updates as necessary.Jun 26, 03:30 UT…

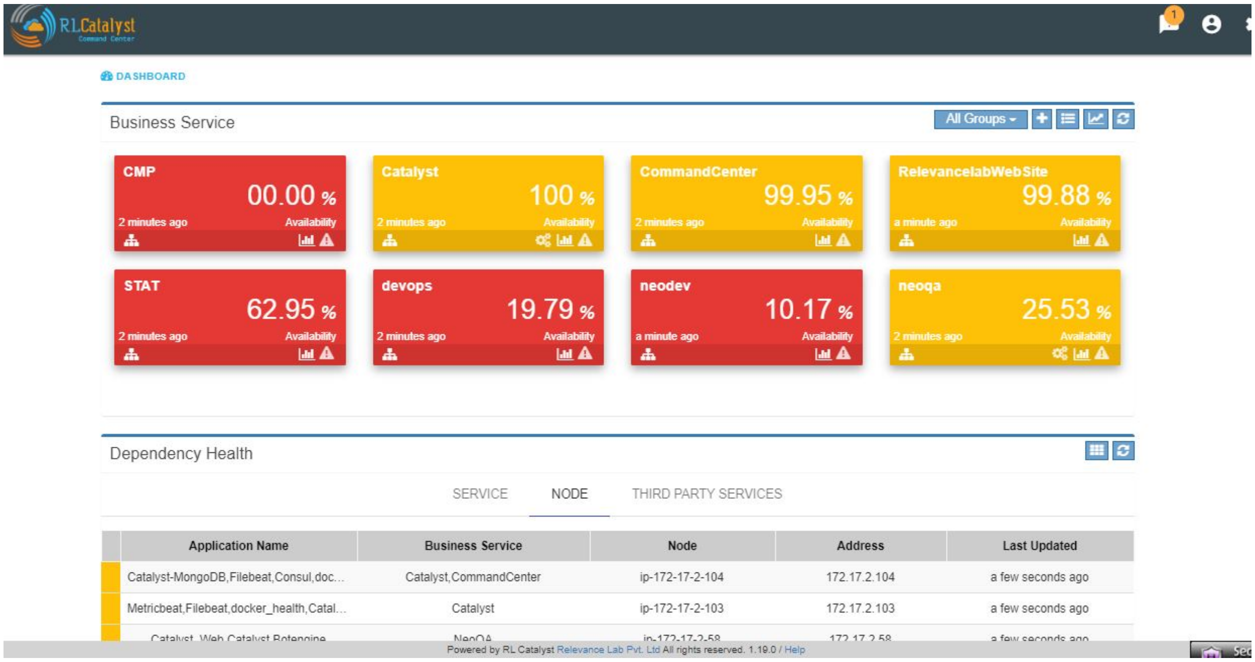
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.17.0 / Help

1.4.5 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



Business Service

CMP 00.00 % 2 minutes ago Availability	Catalyst 100 % 2 minutes ago Availability	CommandCenter 99.95 % 2 minutes ago Availability	RelevancelabWebSite 99.88 % a minute ago Availability
STAT 62.95 % 2 minutes ago Availability	devops 19.79 % 2 minutes ago Availability	neodev 10.17 % a minute ago Availability	neoqa 25.53 % 2 minutes ago Availability

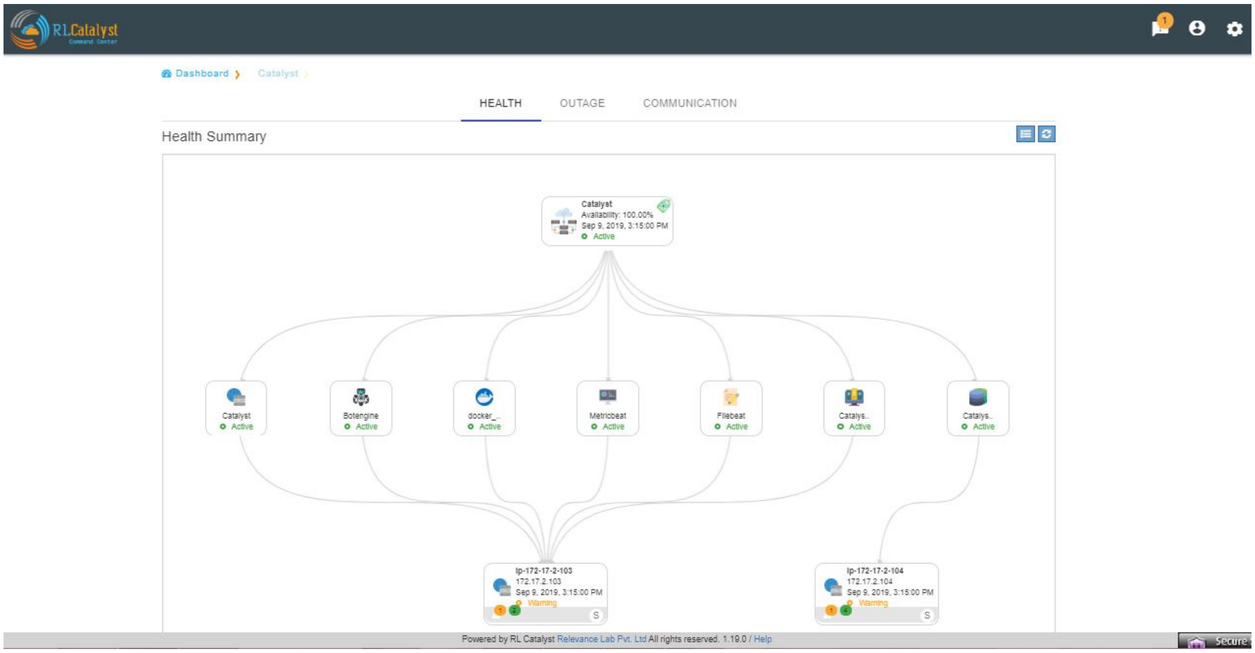
Dependency Health

SERVICE NODE THIRD PARTY SERVICES

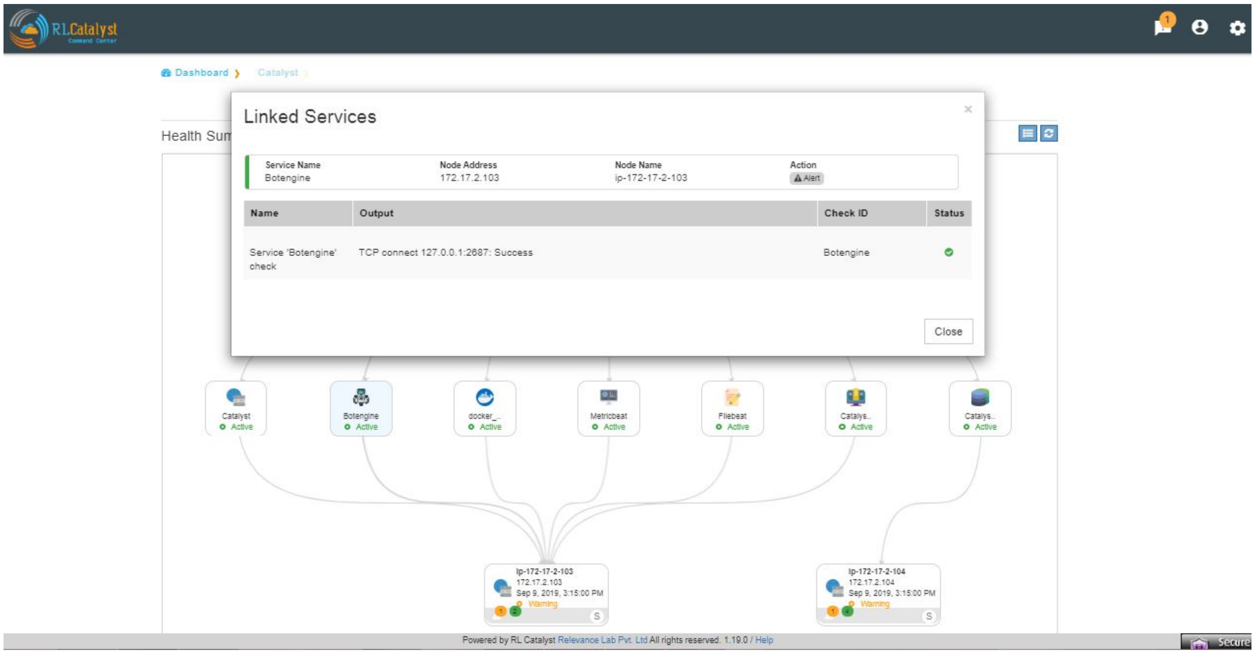
Application Name	Business Service	Node	Address	Last Updated
Catalyst-MongoDB,Filebeat,Consul,doc...	Catalyst,CommandCenter	ip-172-17-2-104	172.17.2.104	a few seconds ago
Metricbeat,Filebeat,docker_health,Catal...	Catalyst	ip-172-17-2-103	172.17.2.103	a few seconds ago
Catalyst_Web,Catalyst,Botengine	NeoQA	ip-172-17-2-58	172.17.2.58	a few seconds ago

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

Here the details of linked services and the associated nodes of a particular BSM is shown in a graphical representation.



clicking on each box in the graphical view will pop-up and shows the details of that particular thing in a detailed manner.

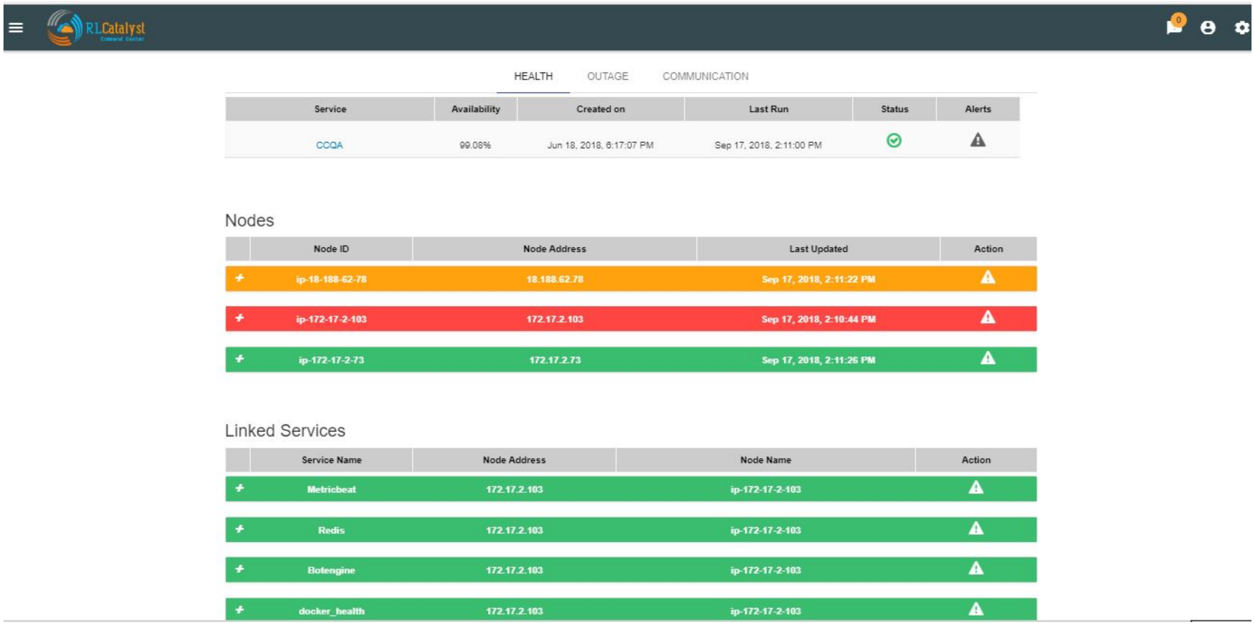


Linked Services

Service Name	Node Address	Node Name	Action
Botengine	172.17.2.103	ip-172-17-2-103	Alert

Name	Output	Check ID	Status
Service 'Botengine' check	TCP connect 127.0.0.1:2687: Success	Botengine	✓

At the top right corner, you can see a button which gives us an another option of viewing the details of linked services and asociated nodes for a particular BSm in a listed view.



Service	Availability	Created on	Last Run	Status	Alerts
CCQA	99.08%	Jun 18, 2018, 6:17:07 PM	Sep 17, 2018, 2:11:00 PM	✓	⚠

Nodes

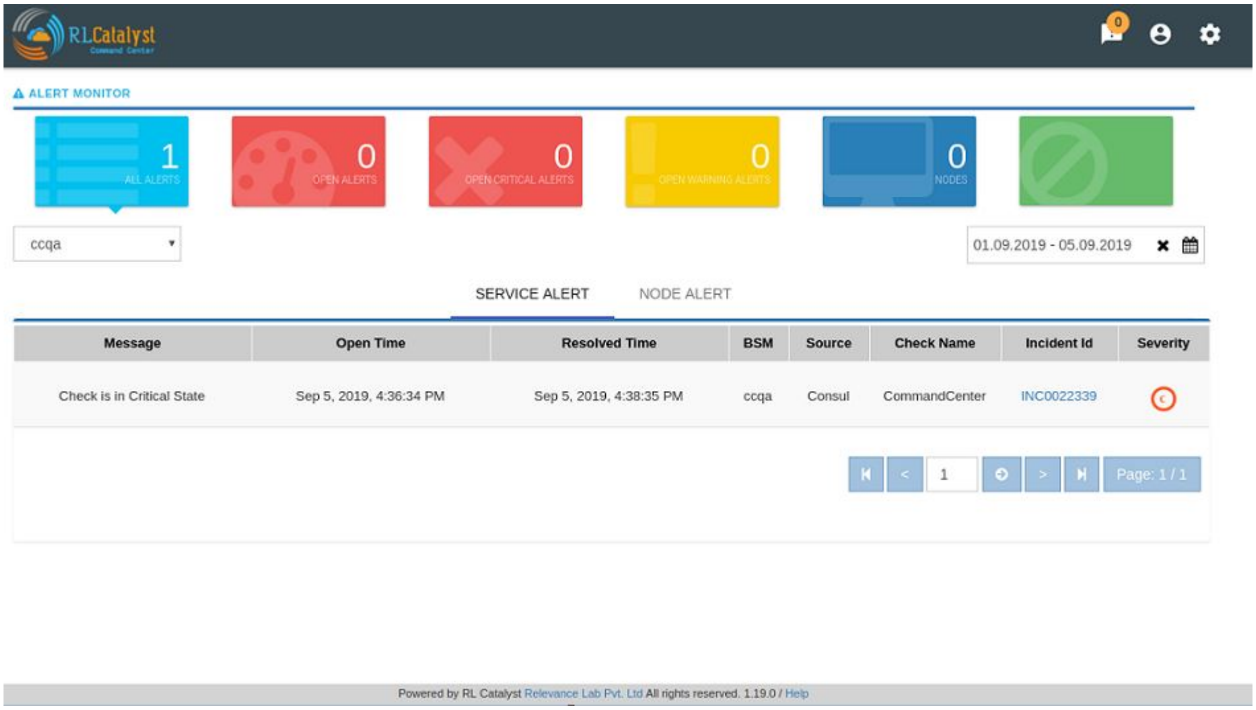
	Node ID	Node Address	Last Updated	Action
+	ip-18-188-62-78	18.188.62.78	Sep 17, 2018, 2:11:22 PM	⚠
+	ip-172-17-2-103	172.17.2.103	Sep 17, 2018, 2:10:44 PM	⚠
+	ip-172-17-2-73	172.17.2.73	Sep 17, 2018, 2:11:26 PM	⚠

Linked Services

	Service Name	Node Address	Node Name	Action
+	Metricbeat	172.17.2.103	ip-172-17-2-103	⚠
+	Redis	172.17.2.103	ip-172-17-2-103	⚠
+	Botengine	172.17.2.103	ip-172-17-2-103	⚠
+	docker_health	172.17.2.103	ip-172-17-2-103	⚠

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.

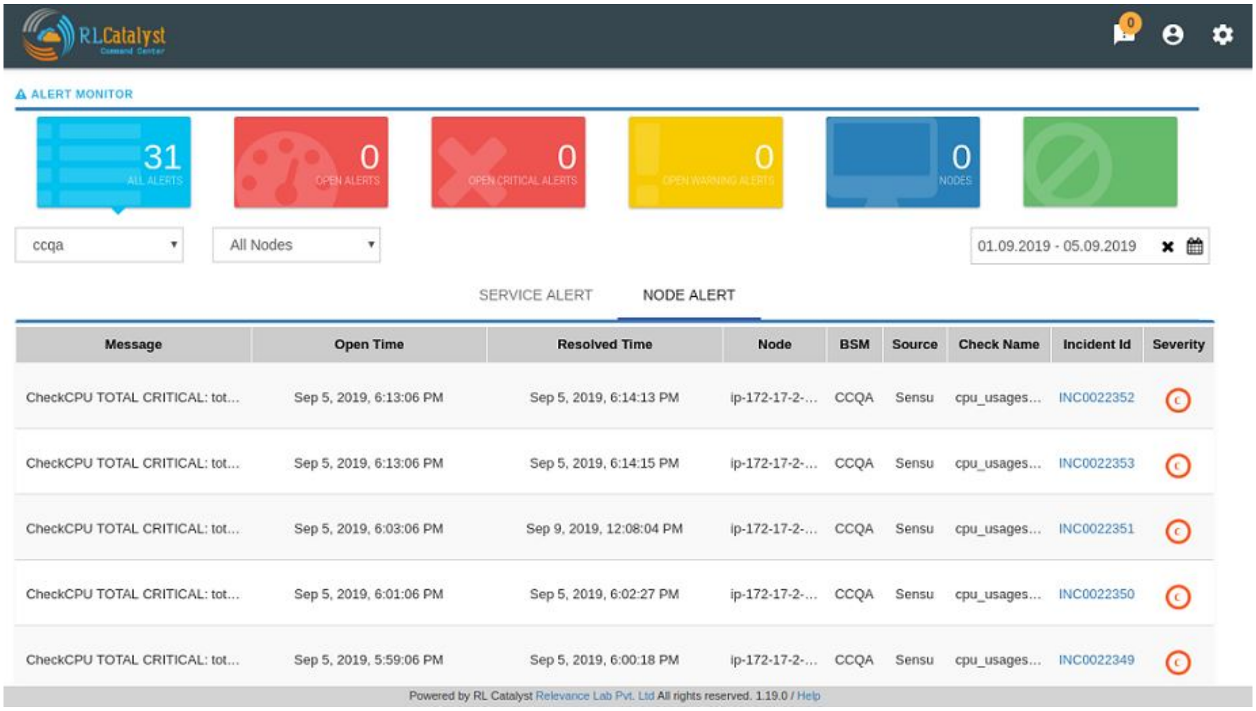
Service alerts are shown on the Services tab of the Alert Monitor.



Message	Open Time	Resolved Time	BSM	Source	Check Name	Incident Id	Severity
Check is in Critical State	Sep 5, 2019, 4:36:34 PM	Sep 5, 2019, 4:38:35 PM	ccqa	Consul	CommandCenter	INC0022339	c

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

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



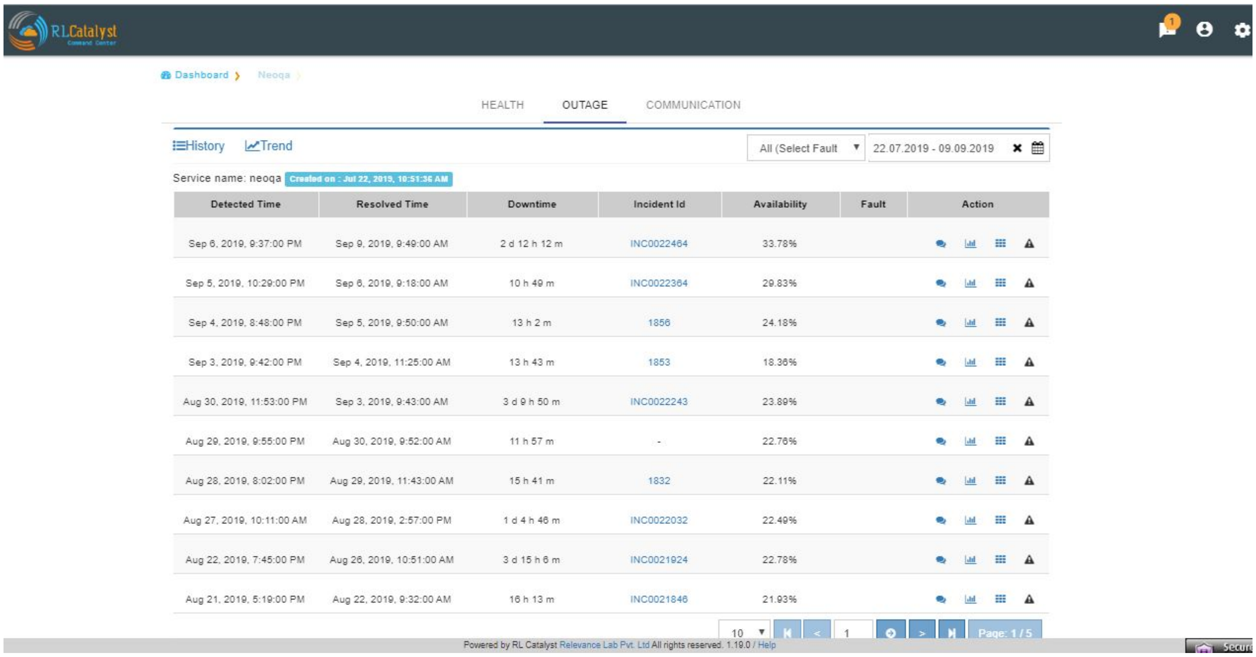
Message	Open Time	Resolved Time	Node	BSM	Source	Check Name	Incident Id	Severity
CheckCPU TOTAL CRITICAL: tot...	Sep 5, 2019, 6:13:06 PM	Sep 5, 2019, 6:14:13 PM	ip-172-17-2-...	CCQA	Sensu	cpu_usages...	INC0022352	ⓒ
CheckCPU TOTAL CRITICAL: tot...	Sep 5, 2019, 6:13:06 PM	Sep 5, 2019, 6:14:15 PM	ip-172-17-2-...	CCQA	Sensu	cpu_usages...	INC0022353	ⓒ
CheckCPU TOTAL CRITICAL: tot...	Sep 5, 2019, 6:03:06 PM	Sep 9, 2019, 12:08:04 PM	ip-172-17-2-...	CCQA	Sensu	cpu_usages...	INC0022351	ⓒ
CheckCPU TOTAL CRITICAL: tot...	Sep 5, 2019, 6:01:06 PM	Sep 5, 2019, 6:02:27 PM	ip-172-17-2-...	CCQA	Sensu	cpu_usages...	INC0022350	ⓒ
CheckCPU TOTAL CRITICAL: tot...	Sep 5, 2019, 5:59:06 PM	Sep 5, 2019, 6:00:18 PM	ip-172-17-2-...	CCQA	Sensu	cpu_usages...	INC0022349	ⓒ

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

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.



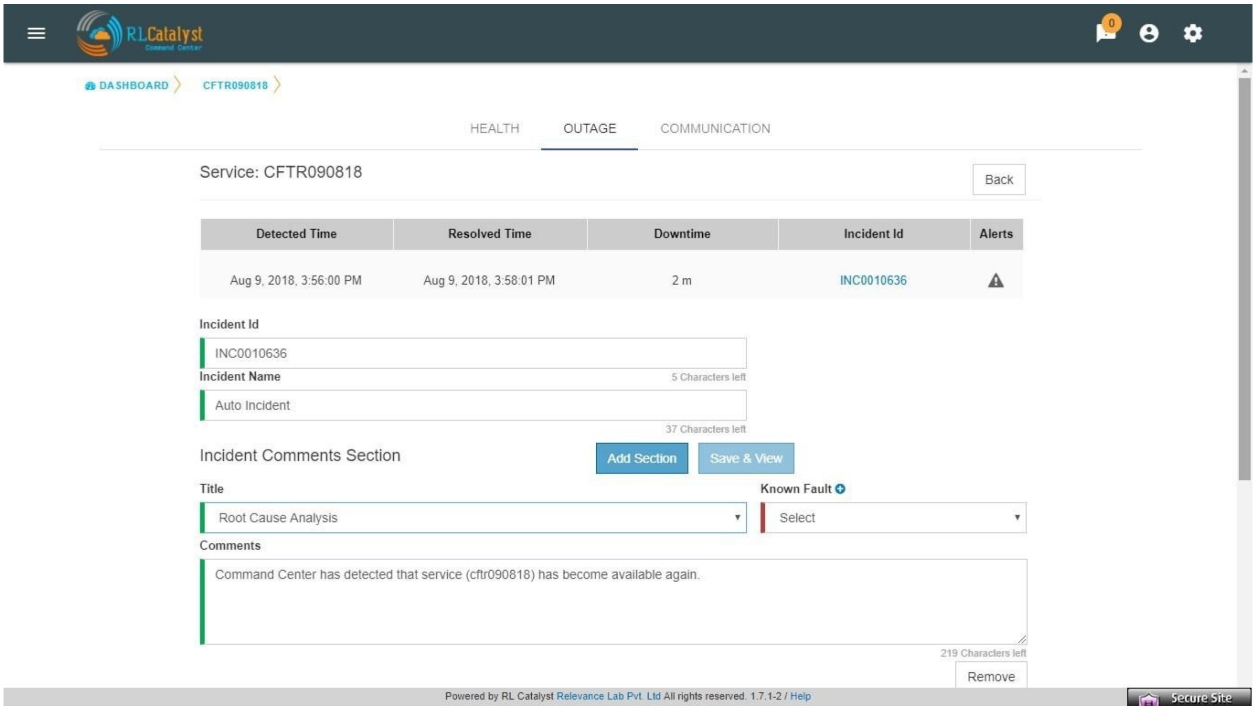
Service name: neoqa Created on : Jul 22, 2019, 10:51:36 AM

Detected Time	Resolved Time	Downtime	Incident Id	Availability	Fault	Action
Sep 6, 2019, 9:37:00 PM	Sep 9, 2019, 9:49:00 AM	2 d 12 h 12 m	INC0022464	33.78%		💬 📊 ▦ ▲
Sep 5, 2019, 10:29:00 PM	Sep 6, 2019, 9:18:00 AM	10 h 49 m	INC0022364	29.83%		💬 📊 ▦ ▲
Sep 4, 2019, 8:48:00 PM	Sep 5, 2019, 9:50:00 AM	13 h 2 m	1856	24.18%		💬 📊 ▦ ▲
Sep 3, 2019, 9:42:00 PM	Sep 4, 2019, 11:25:00 AM	13 h 43 m	1853	18.36%		💬 📊 ▦ ▲
Aug 30, 2019, 11:53:00 PM	Sep 3, 2019, 9:43:00 AM	3 d 9 h 50 m	INC0022243	23.89%		💬 📊 ▦ ▲
Aug 29, 2019, 9:55:00 PM	Aug 30, 2019, 9:52:00 AM	11 h 57 m	-	22.76%		💬 📊 ▦ ▲
Aug 28, 2019, 8:02:00 PM	Aug 29, 2019, 11:43:00 AM	15 h 41 m	1832	22.11%		💬 📊 ▦ ▲
Aug 27, 2019, 10:11:00 AM	Aug 28, 2019, 2:57:00 PM	1 d 4 h 46 m	INC0022032	22.49%		💬 📊 ▦ ▲
Aug 22, 2019, 7:45:00 PM	Aug 26, 2019, 10:51:00 AM	3 d 15 h 6 m	INC0021924	22.78%		💬 📊 ▦ ▲
Aug 21, 2019, 5:19:00 PM	Aug 22, 2019, 9:32:00 AM	16 h 13 m	INC0021846	21.93%		💬 📊 ▦ ▲

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

1.4.6 Incident Communication

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

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 (5 Characters left)

37 Characters left

Incident Comments Section

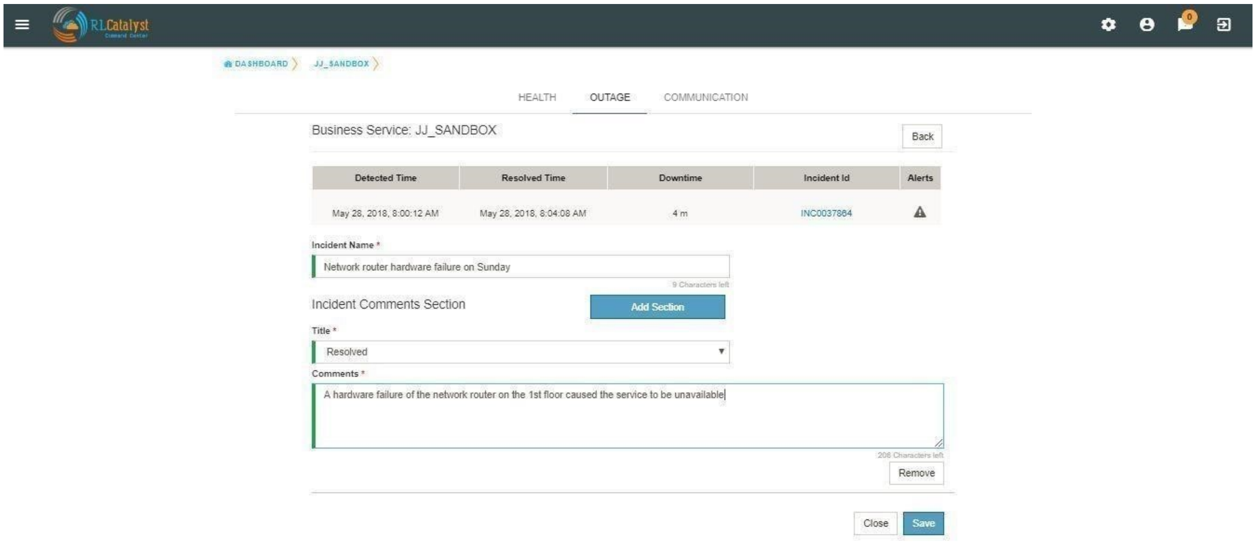
Title: Root Cause Analysis

Known Fault: Select

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

219 Characters left

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



Business Service: JJ_SANDBOX

Detected Time	Resolved Time	Downtime	Incident Id	Alerts
May 28, 2018, 8:00:12 AM	May 28, 2018, 8:04:08 AM	4 m	INC0037864	⚠

Incident Name *: Network router hardware failure on Sunday

9 Characters left

Incident Comments Section

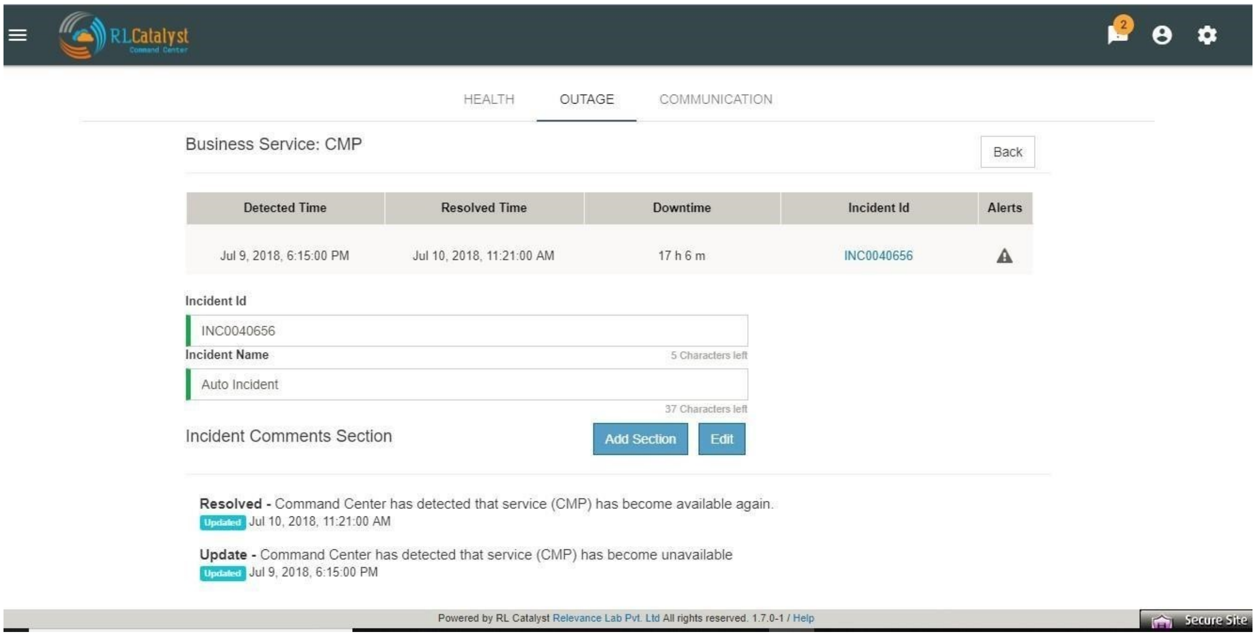
Title *: Resolved

Comments *: A hardware failure of the network router on the 1st floor caused the service to be unavailable

208 Characters left

Auto-create Incident Communications for Detection and Resolution :

System automatically creates Incident Communication for application outage detection and resolution.



Business Service: CMP

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

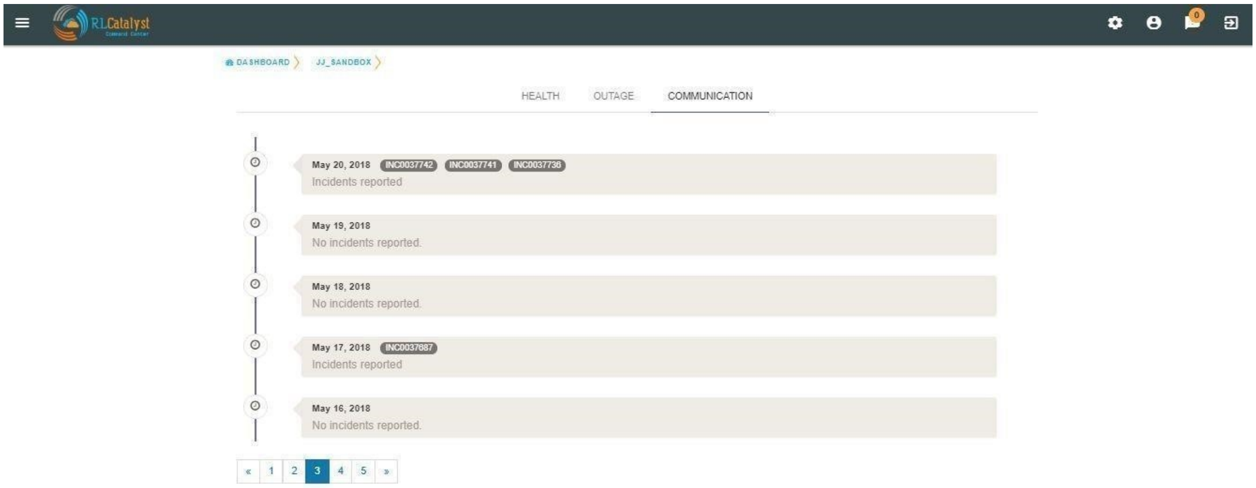
Incident Comments Section

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

Click on the Communications tab to see a timeline of incidents



May 20, 2018 INC0037742 INC0037741 INC0037736
Incidents reported

May 19, 2018
No incidents reported.

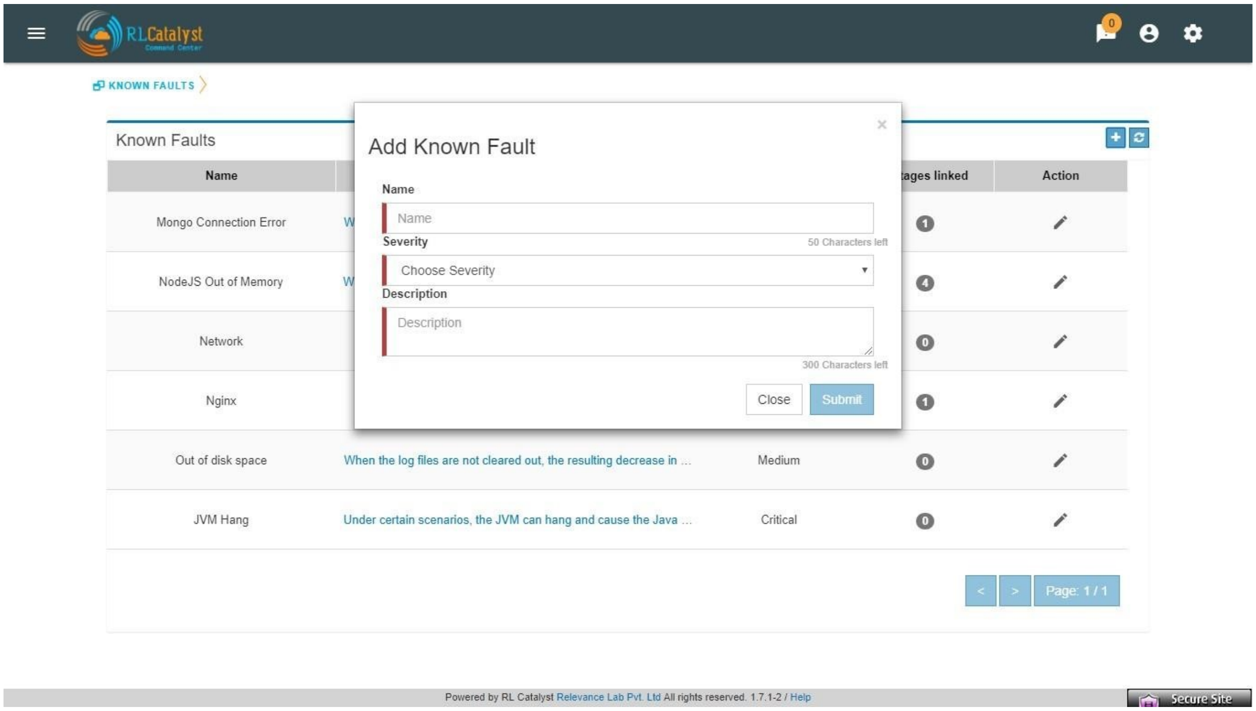
May 18, 2018
No incidents reported.

May 17, 2018 INC0037687
Incidents reported

May 16, 2018
No incidents reported.

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)



Known Faults

Name			ages linked	Action
Mongo Connection Error	W		1	
NodeJS Out of Memory	W		4	
Network			0	
Nginx			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	

Add Known Fault

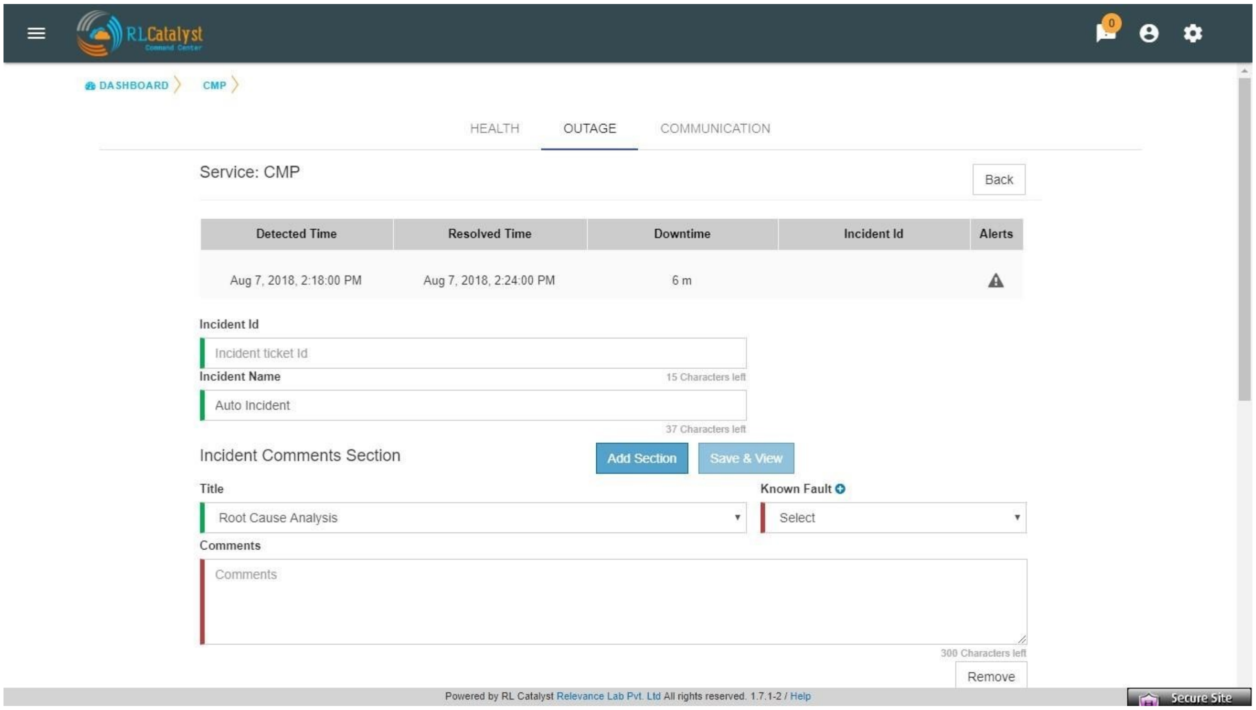
Name
Name
50 Characters left

Severity
Choose Severity

Description
Description
300 Characters left

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

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.



Service: CMP

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
15 Characters left

Incident Name
Auto Incident
37 Characters left

Incident Comments Section

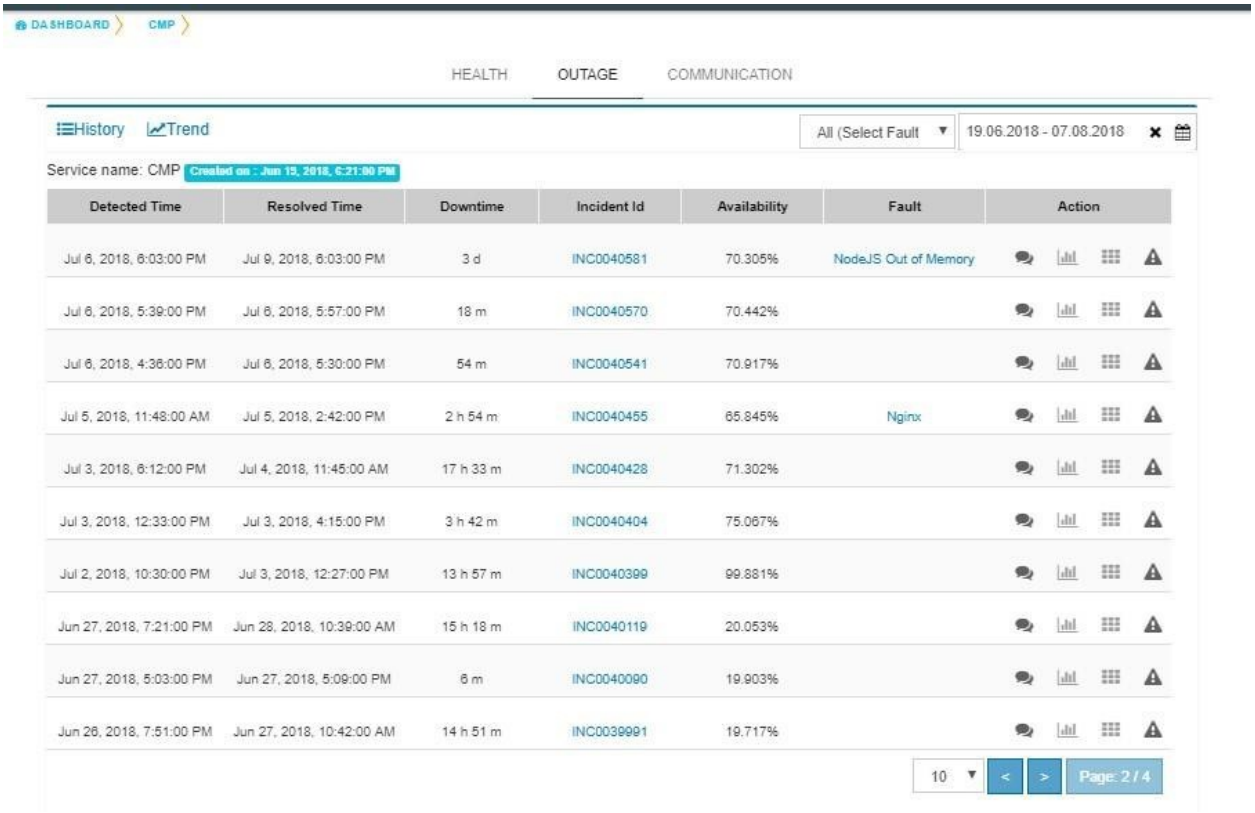
Title
Root Cause Analysis

Known Fault
Select

Comments
Comments
300 Characters left

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

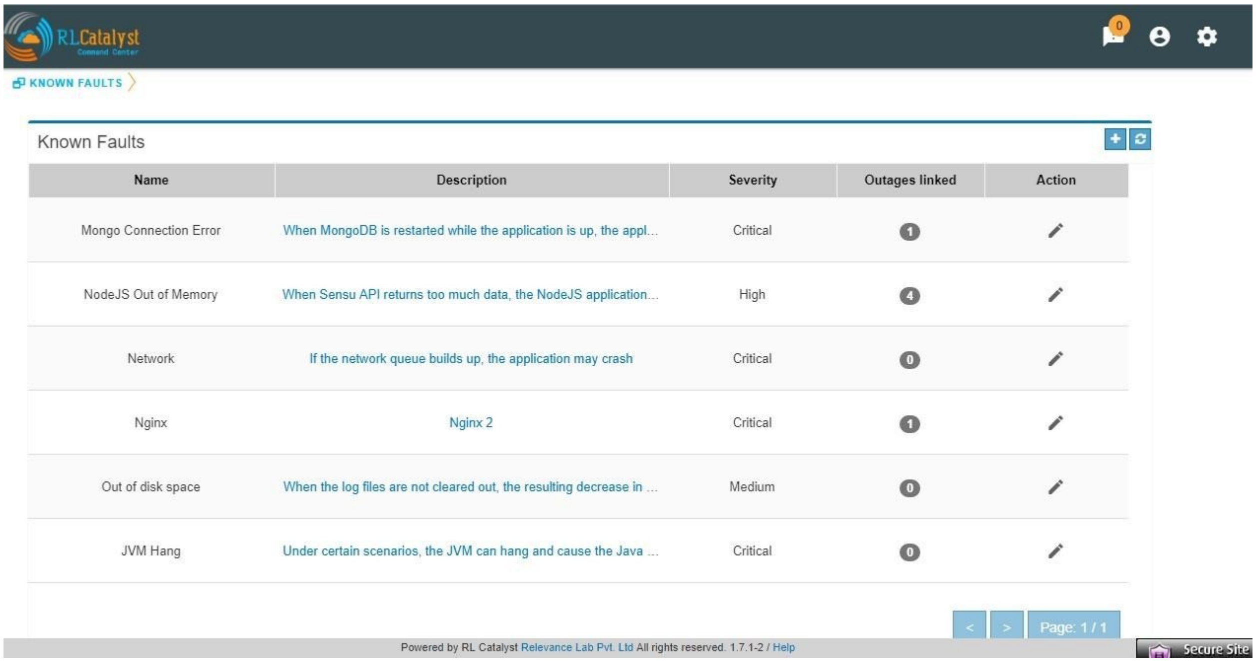
User shall be able to navigate to the Fault Table from any outage which is linked to a fault by clicking on "Fault" link in the Outages screen.



Service name: CMP Created on : Jun 15, 2018, 6:21:00 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	INC0040581	70.305%	NodeJS Out of Memory	
Jul 6, 2018, 5:39:00 PM	Jul 6, 2018, 5:57:00 PM	18 m	INC0040570	70.442%		
Jul 6, 2018, 4:36:00 PM	Jul 6, 2018, 5:30:00 PM	54 m	INC0040541	70.917%		
Jul 5, 2018, 11:48:00 AM	Jul 5, 2018, 2:42:00 PM	2 h 54 m	INC0040455	65.845%	Nginx	
Jul 3, 2018, 6:12:00 PM	Jul 4, 2018, 11:45:00 AM	17 h 33 m	INC0040428	71.302%		
Jul 3, 2018, 12:33:00 PM	Jul 3, 2018, 4:15:00 PM	3 h 42 m	INC0040404	75.067%		
Jul 2, 2018, 10:30:00 PM	Jul 3, 2018, 12:27:00 PM	13 h 57 m	INC0040399	99.881%		
Jun 27, 2018, 7:21:00 PM	Jun 28, 2018, 10:39:00 AM	15 h 18 m	INC0040119	20.053%		
Jun 27, 2018, 5:03:00 PM	Jun 27, 2018, 5:09:00 PM	6 m	INC0040090	19.903%		
Jun 26, 2018, 7:51:00 PM	Jun 27, 2018, 10:42:00 AM	14 h 51 m	INC0039991	19.717%		

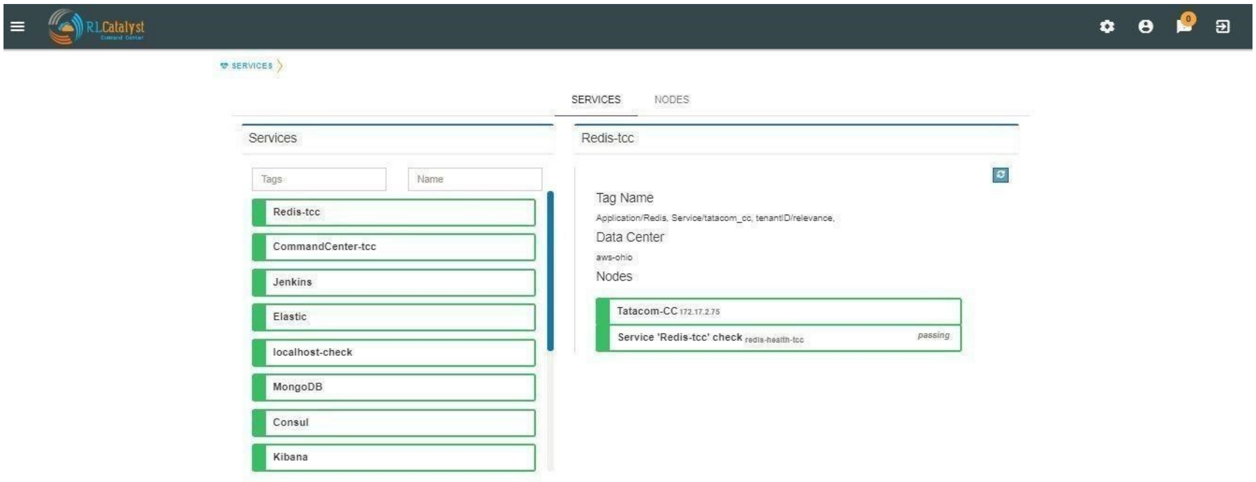
User can view the count of outages linked to a fault by clicking on the "Outages Linked" link in the Fault table



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	

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

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



Redis-tcc

Tag Name

Application/Redis, Service/tatacom_cc, tenantID/relevance,

Data Center

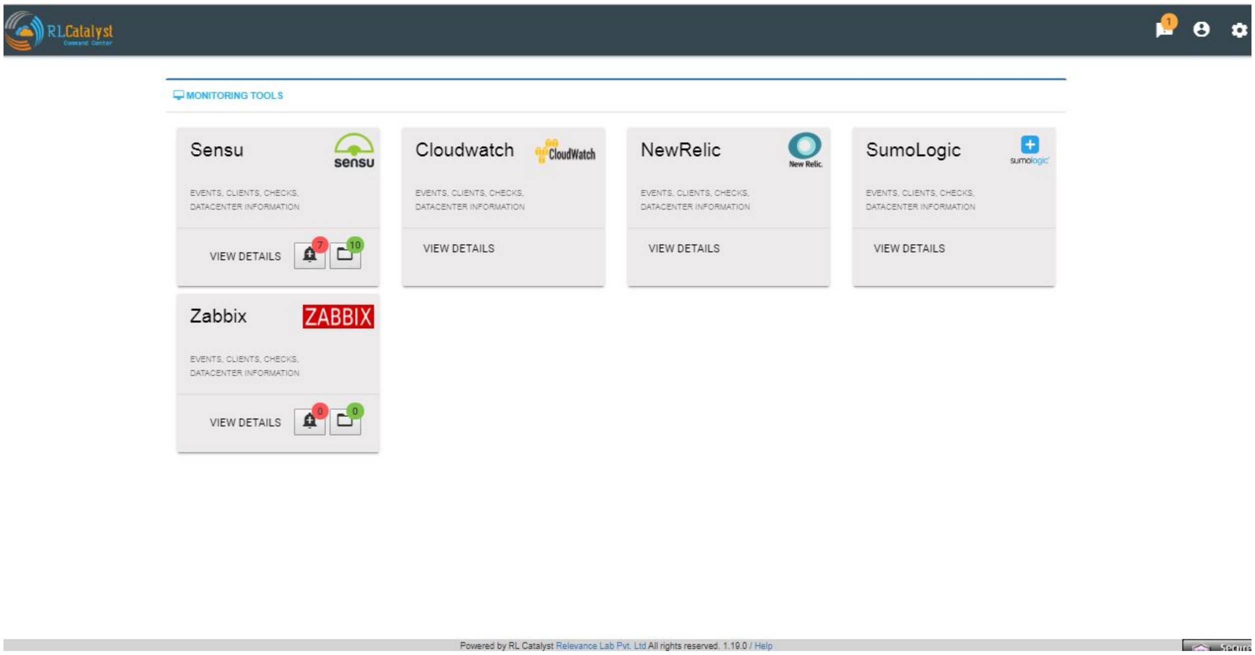
aws-ohio

Nodes

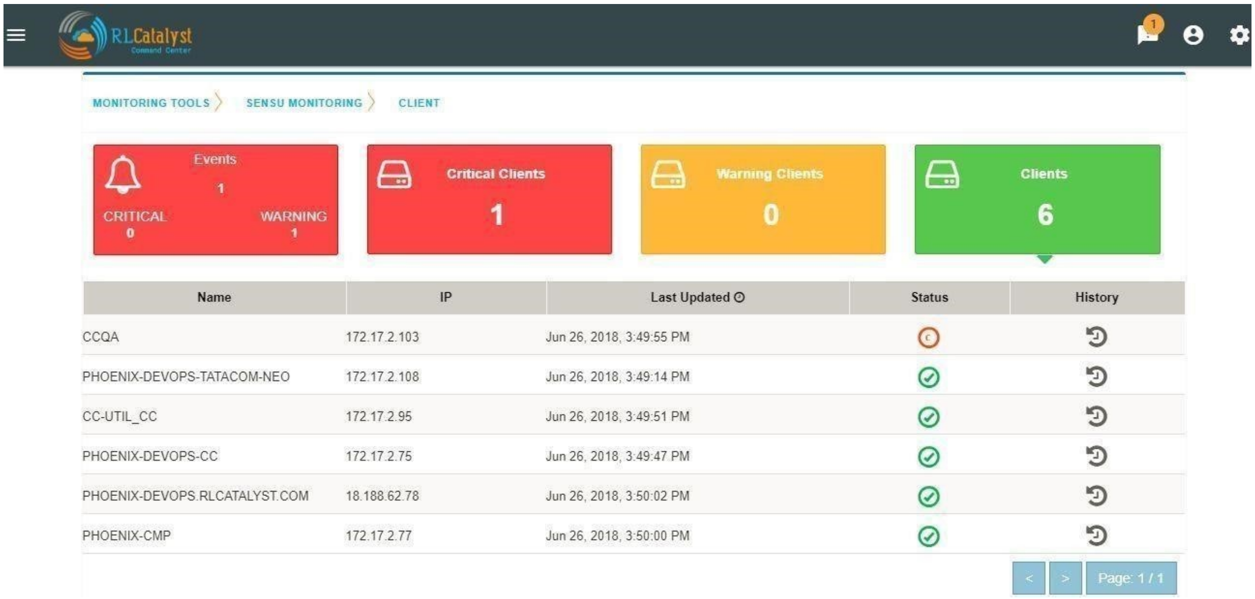
Tatacom-CC 172.17.2.75

Service 'Redis-tcc' check redis-health-tcc passing

Aggregated Alerts for all servers/instances are available from the left pane menu ‘Monitoring Tools’

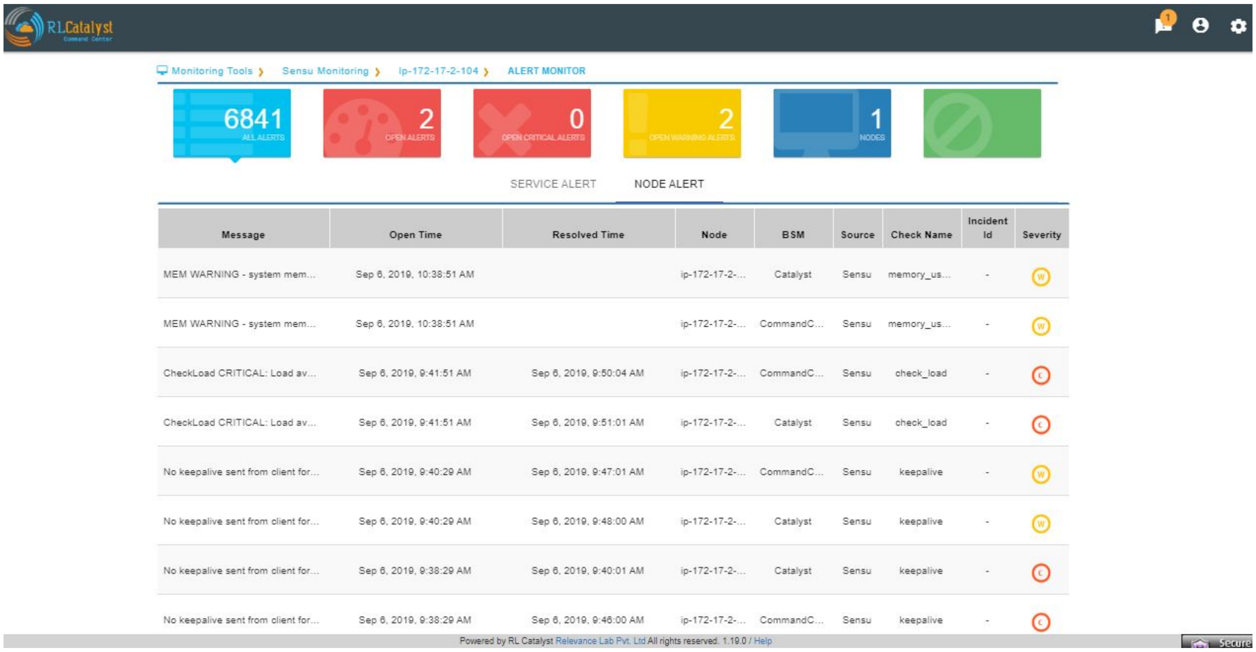

RLCatalyst
Command Center
1
MONITORING TOOLS
Sensu
sensu
EVENTS, CLIENTS, CHECKS, DATACENTER INFORMATION
VIEW DETAILS
7
10
Cloudwatch
CloudWatch
EVENTS, CLIENTS, CHECKS, DATACENTER INFORMATION
VIEW DETAILS
NewRelic
New Relic.
EVENTS, CLIENTS, CHECKS, DATACENTER INFORMATION
VIEW DETAILS
SumoLogic
sumologic
EVENTS, CLIENTS, CHECKS, DATACENTER INFORMATION
VIEW DETAILS
Zabbix
ZABBIX
EVENTS, CLIENTS, CHECKS, DATACENTER INFORMATION
VIEW DETAILS
0
0
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

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



Name	IP	Last Updated	Status	History
CCQA	172.17.2.103	Jun 26, 2018, 3:49:55 PM	C	
PHOENIX-DEVOPS-TATACOM-NEO	172.17.2.108	Jun 26, 2018, 3:49:14 PM	✓	
CC-UTIL_CC	172.17.2.95	Jun 26, 2018, 3:49:51 PM	✓	
PHOENIX-DEVOPS-CC	172.17.2.75	Jun 26, 2018, 3:49:47 PM	✓	
PHOENIX-DEVOPS.RLCATALYST.COM	18.188.62.78	Jun 26, 2018, 3:50:02 PM	✓	
PHOENIX-CMP	172.17.2.77	Jun 26, 2018, 3:50:00 PM	✓	

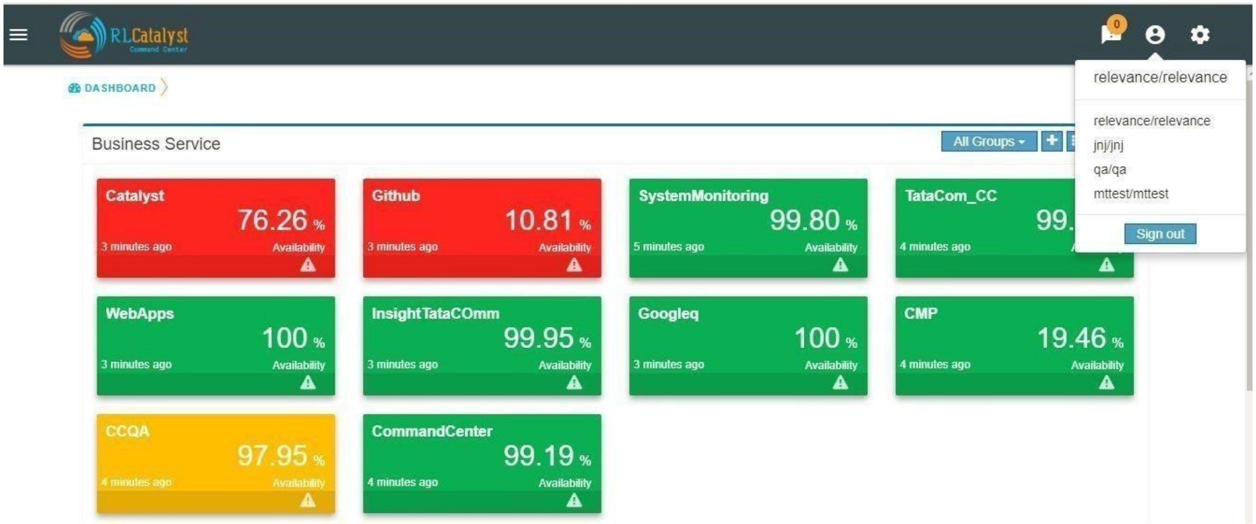
Click on History Icon, to view the detailed history information regarding each client



Message	Open Time	Resolved Time	Node	BSM	Source	Check Name	Incident Id	Severity
MEM WARNING - system mem...	Sep 6, 2019, 10:38:51 AM		ip-172-17-2-...	Catalyst	Sensu	memory_us...	-	W
MEM WARNING - system mem...	Sep 6, 2019, 10:38:51 AM		ip-172-17-2-...	CommandC...	Sensu	memory_us...	-	W
CheckLoad CRITICAL: Load av...	Sep 6, 2019, 9:41:51 AM	Sep 6, 2019, 9:50:04 AM	ip-172-17-2-...	CommandC...	Sensu	check_load	-	C
CheckLoad CRITICAL: Load av...	Sep 6, 2019, 9:41:51 AM	Sep 6, 2019, 9:51:01 AM	ip-172-17-2-...	Catalyst	Sensu	check_load	-	C
No keepalive sent from client for...	Sep 6, 2019, 9:40:29 AM	Sep 6, 2019, 9:47:01 AM	ip-172-17-2-...	CommandC...	Sensu	keepalive	-	W
No keepalive sent from client for...	Sep 6, 2019, 9:40:29 AM	Sep 6, 2019, 9:48:00 AM	ip-172-17-2-...	Catalyst	Sensu	keepalive	-	W
No keepalive sent from client for...	Sep 6, 2019, 9:38:29 AM	Sep 6, 2019, 9:40:01 AM	ip-172-17-2-...	Catalyst	Sensu	keepalive	-	C
No keepalive sent from client for...	Sep 6, 2019, 9:38:29 AM	Sep 6, 2019, 9:46:00 AM	ip-172-17-2-...	CommandC...	Sensu	keepalive	-	C

1.4.7 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.



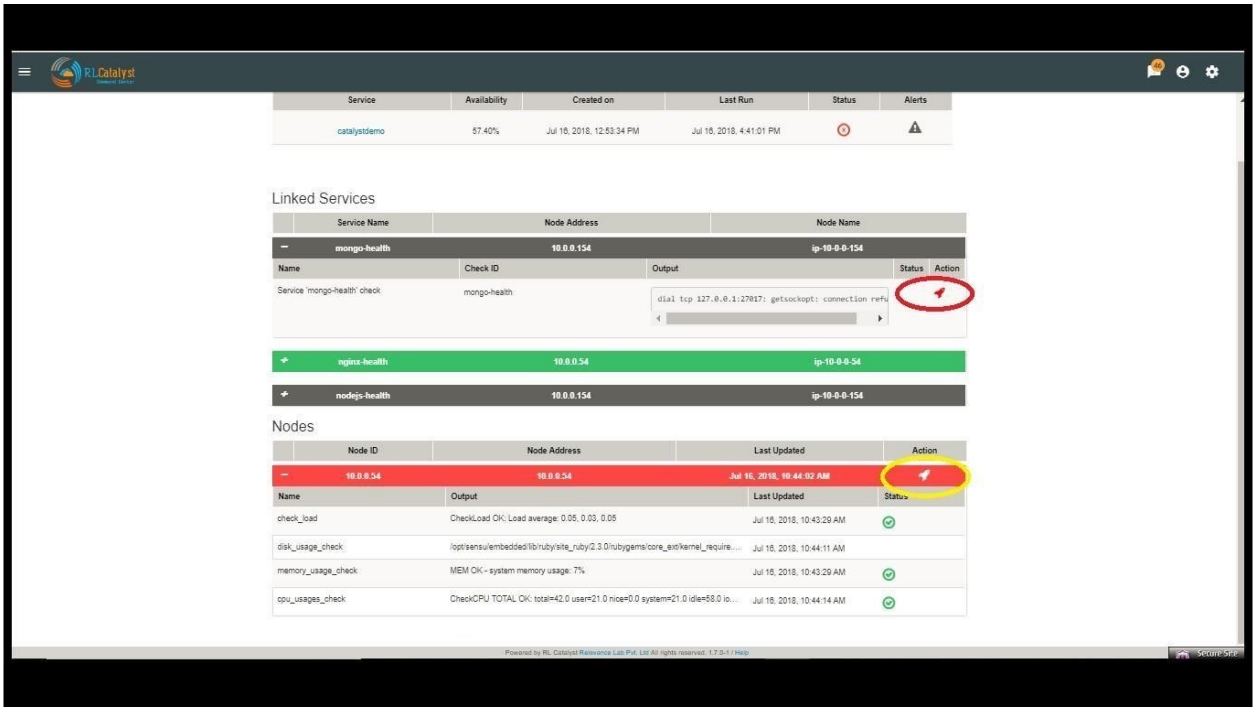
Business Service

Service	Availability	Updated
Catalyst	76.26 %	3 minutes ago
Github	10.81 %	3 minutes ago
SystemMonitoring	99.80 %	5 minutes ago
TataCom_CC	99.	4 minutes ago
WebApps	100 %	3 minutes ago
InsightTataCOmm	99.95 %	3 minutes ago
Googleq	100 %	3 minutes ago
CMP	19.46 %	4 minutes ago
CCQA	97.95 %	4 minutes ago
CommandCenter	99.19 %	4 minutes ago

1.4.8 Remediation

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.



Service	Availability	Created on	Last Run	Status	Alerts
catalystdemo	57.40%	Jul 16, 2018, 12:53:34 PM	Jul 16, 2018, 4:41:01 PM	⊗	⚠

Linked Services

	Service Name	Node Address	Node Name
−	mongo-health	10.0.0.154	ip-10-0-0-154
+	nginx-health	10.0.0.54	ip-10-0-0-54
+	nodejs-health	10.0.0.154	ip-10-0-0-154

Name	Check ID	Output	Status	Action
Service 'mongo-health' check	mongo-health	dial tcp 127.0.0.1:27017: getsockopt: connection refu		

Nodes

	Node ID	Node Address	Last Updated	Action
−	10.0.0.54	10.0.0.54	Jul 16, 2018, 10:44:02 AM	

Name	Output	Last Updated	Status
check_load	CheckLoad OK: Load average: 0.05, 0.03, 0.05	Jul 16, 2018, 10:43:29 AM	✓
disk_usage_check	/opt/sensu/embedded/lib/ruby/site_ruby/2.3.0/rubygems/core_ext/kernel_require....	Jul 16, 2018, 10:44:11 AM	
memory_usage_check	MEM OK - system memory usage: 7%	Jul 16, 2018, 10:43:29 AM	✓
cpu_usages_check	CheckCPU TOTAL OK: total=42.0 user=21.0 nice=0.0 system=21.0 idle=58.0 io...	Jul 16, 2018, 10:44:14 AM	✓

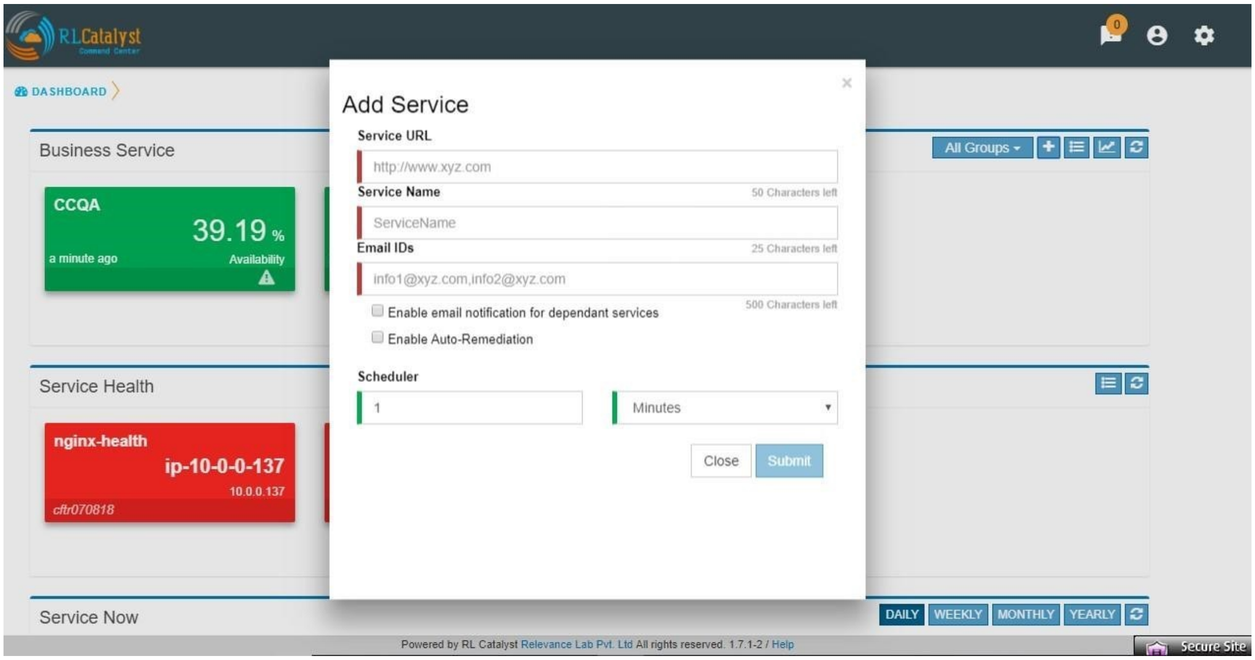
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.7.0-1 / Help

1.4.9 Auto Remediation

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.



Add Service

Service URL: http://www.xyz.com

Service Name: ServiceName (50 Characters left)

Email IDs: info1@xyz.com,info2@xyz.com (25 Characters left)

500 Characters left

□ Enable email notification for dependant services

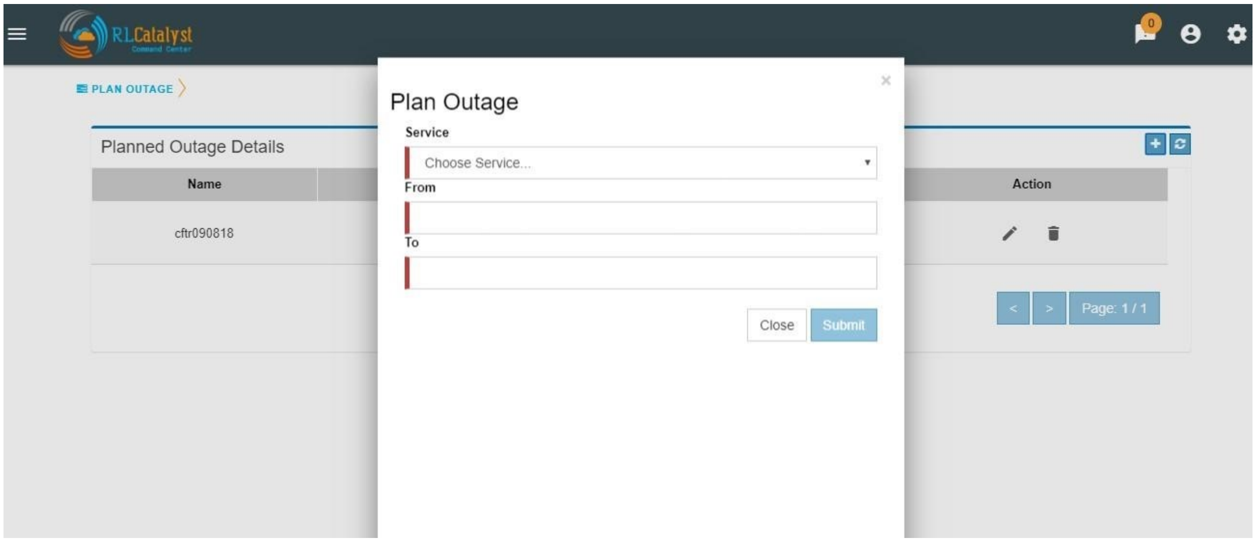
□ Enable Auto-Remediation

Scheduler: 1 Minutes

1.4.10 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.



Plan Outage

Service: Choose Service...

From:

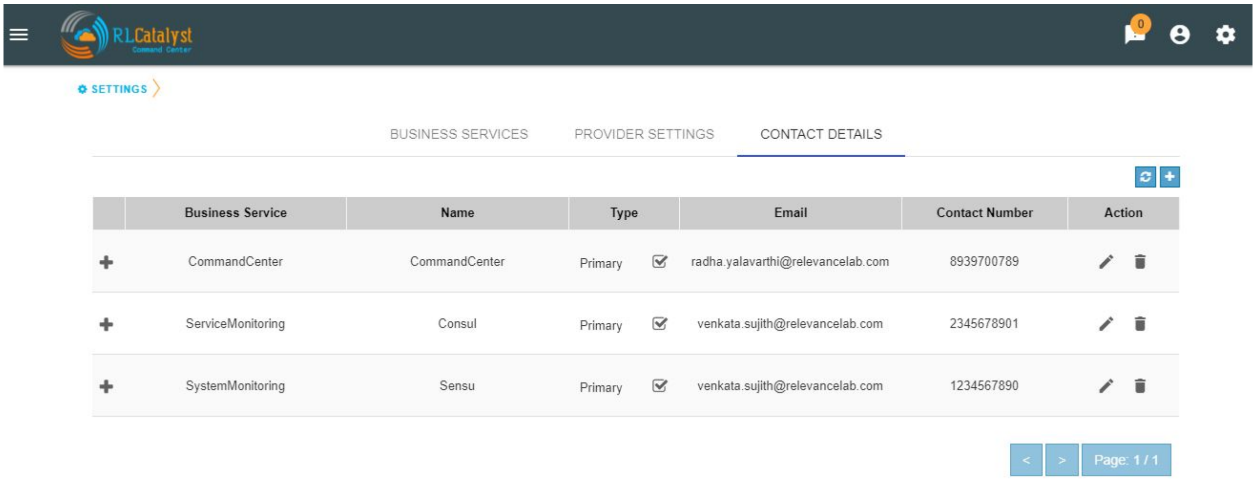
To:

Name	Action
cftr090818	

1.4.11 Contact Person

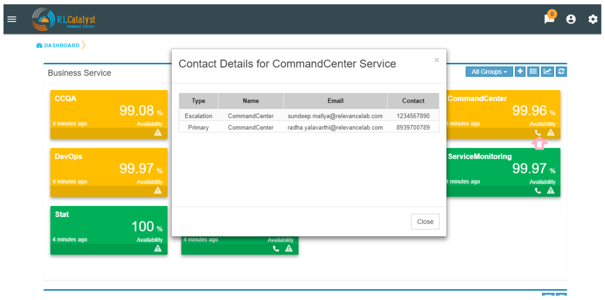
In an operations center which is using a tool like Command Center, one of the first pieces of information required when a problem is detected is the contact person designated for that Business Service. The idea of this feature is to ensure that Command Center provides an easy way to enter and display this information.

In the Settings screen, provided one more tab called Contact Details.In this screen, we can add Contact Details for each BSM.



	Business Service	Name	Type	Email	Contact Number	Action
+	CommandCenter	CommandCenter	Primary ☑	radha.yalavarthi@relevancelab.com	8939700789	✎ 🗑
+	ServiceMonitoring	Consul	Primary ☑	venkata.sujith@relevancelab.com	2345678901	✎ 🗑
+	SystemMonitoring	Sensu	Primary ☑	venkata.sujith@relevancelab.com	1234567890	✎ 🗑

On the Dashboard screen, each BSM card should show a ContactDetails icon. Clicking this icon should present the Contact details for that BSM in a pop-up screen.



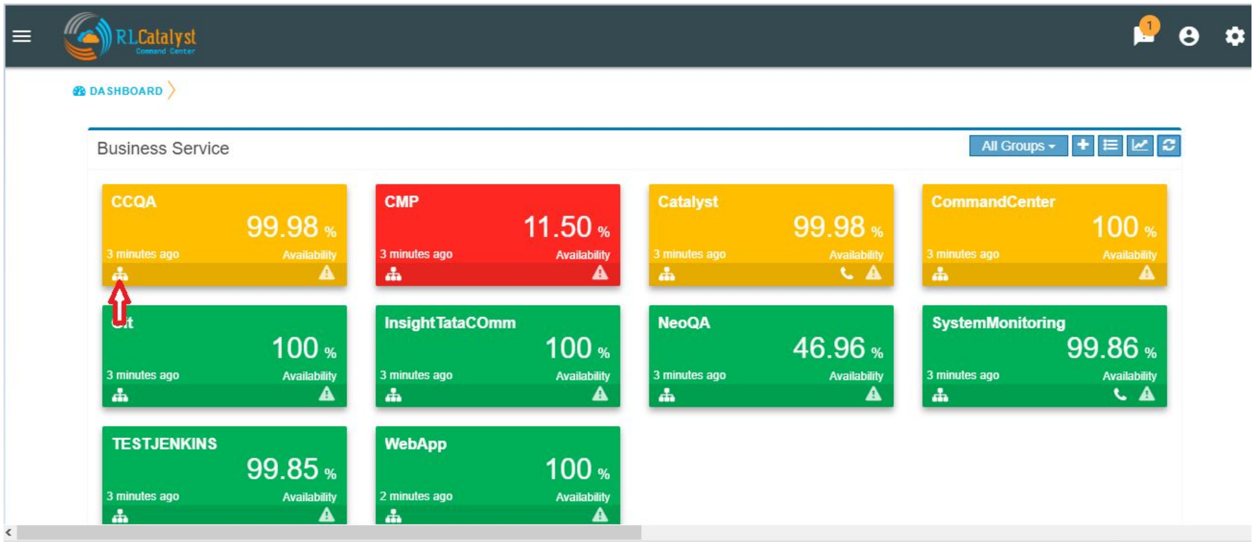
Contact Details for CommandCenter Service

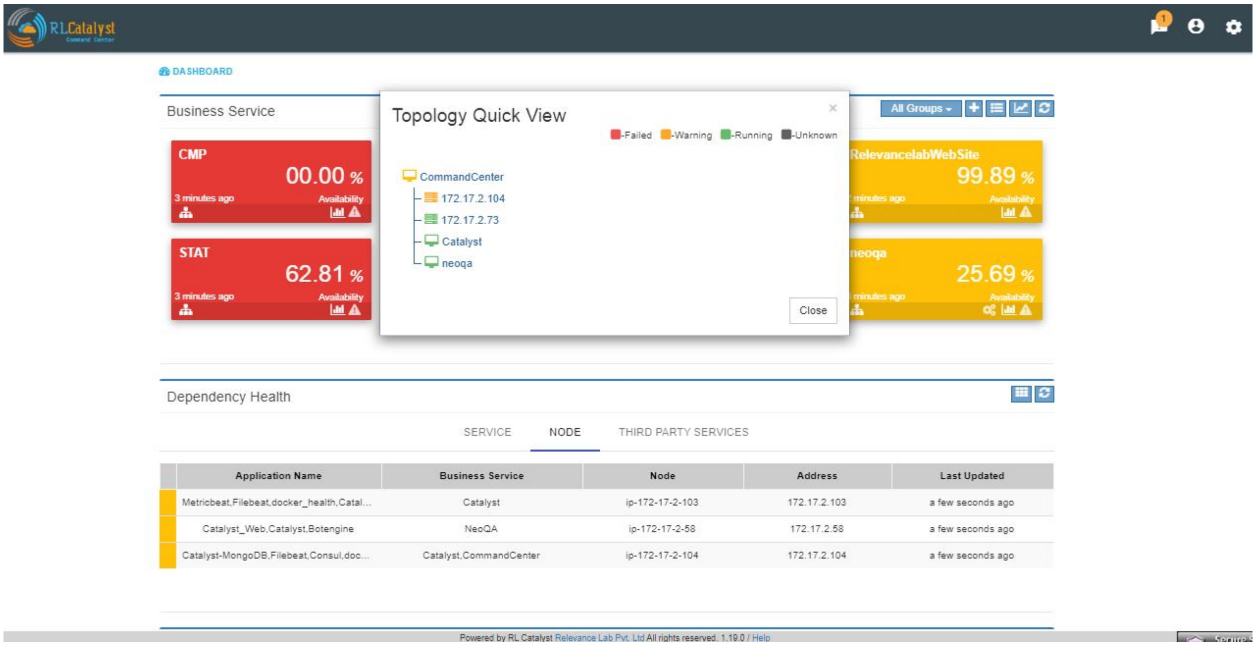
Type	Name	Email	Contact
Escalation	CommandCenter	sundeep.mallya@relevancelab.com	1234567890
Primary	CommandCenter	radha.yalavarthi@relevancelab.com	8939700789

1.4.12 Impact Tree

Impact tree provides a quick way to view the quick glance where in the topology the problem is.

On the main Dashboard view, if a BSM card appears yellow, the user should be able to click on an icon that shows at a quick glance pop-up.This pop-up should show a tree-view with the BSM at the top, with the Nodes under it and the services under the nodes.Based on the alerts each level will be marked with a Yellow or Red highlight.





Dependency Health

SERVICE | NODE | THIRD PARTY SERVICES

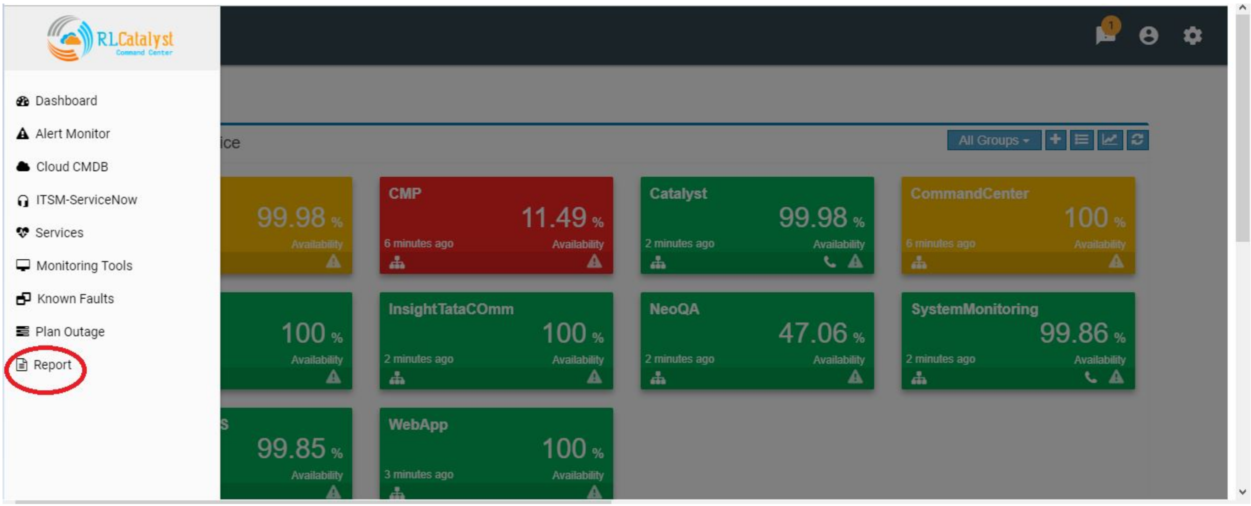
	Application Name	Business Service	Node	Address	Last Updated
🟧	Metricbeat,Filebeat,docker_health,Catal...	Catalyst	ip-172-17-2-103	172.17.2.103	a few seconds ago
🟧	Catalyst_Web,Catalyst,Botengine	NeoQA	ip-172-17-2-58	172.17.2.58	a few seconds ago
🟧	Catalyst-MongoDB,Filebeat,Consul,doc...	Catalyst,CommandCenter	ip-172-17-2-104	172.17.2.104	a few seconds ago

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

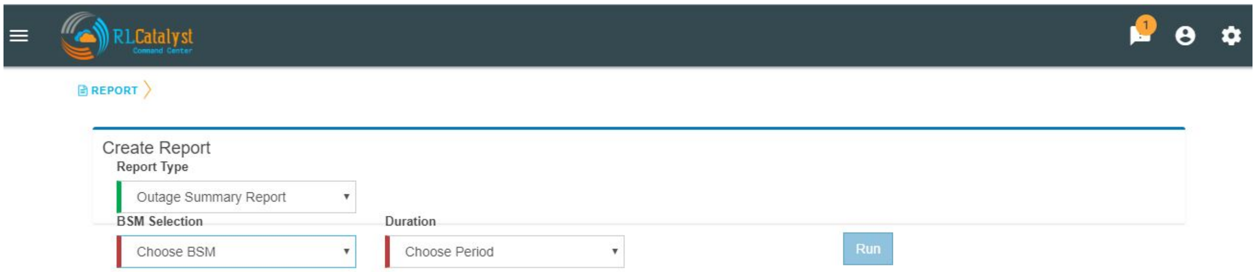
1.4.13 Outage Summary Report

Outage Summary Report will facilitate an operation manager what outages were faced,planned deployments and what early warning was provided by the tool.A report that can be run for different time-periods and which lists the outages and alerts shall be provided.

A new item called "Reports" be added to the application-menu (top-left).



Clicking on the “Reports” menu item shall lead the user to a screen where he can choose the report to run.



Create Report

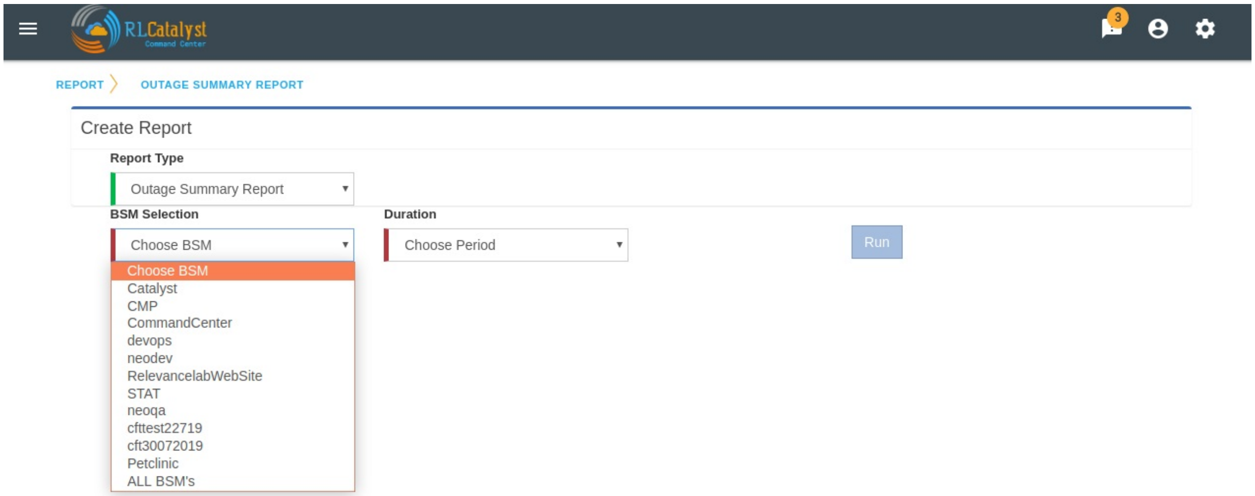
Report Type: Outage Summary Report

BSM Selection: Choose BSM

Duration: Choose Period

On choosing the report to run from a drop-down menu, the user shall be displayed the input fields which are specific to that rep

BSM: This will be a drop-down that allows a specific BSM item or All BSMs that will run the report under the logged in tenant.



Create Report

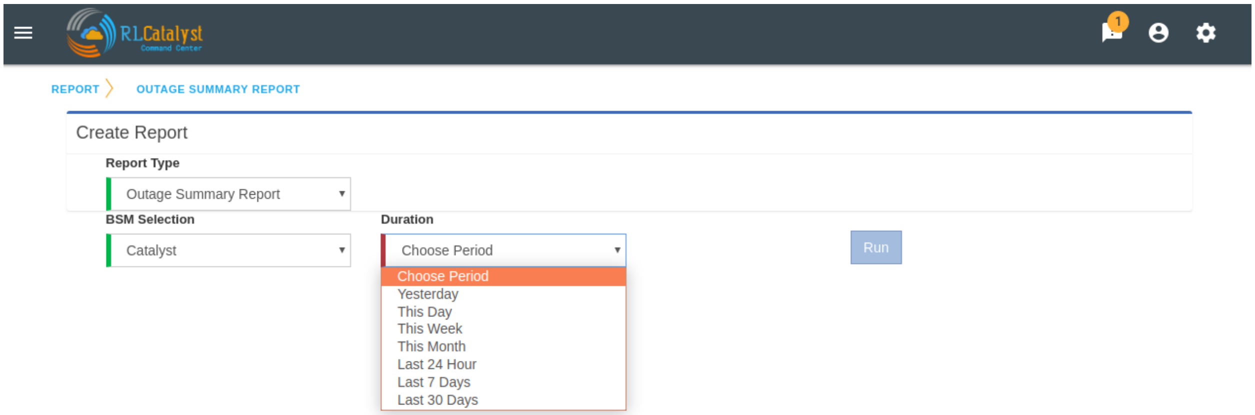
Report Type: Outage Summary Report

BSM Selection: Choose BSM

Duration: Choose Period

Time-period: This will be a drop-down box that allows the user to choose the time-period. Available choices shall be

> Yesterday: Will mean the time-period from yesterday 12:00am to 11:59pm. This day: Will mean the time-period from 12:00am of the current date to now. This week: Will mean the time-priod from 12:00am of Monday of the current week to now This month: Will mean the time-period from 12:00am of 1st of the current month to now Last 24 hours: will mean 24 hour period from current time. Last 7 days: will mean 24*7 hour period from current time. Last 30 days: will mean 30*24 hour period from current time.



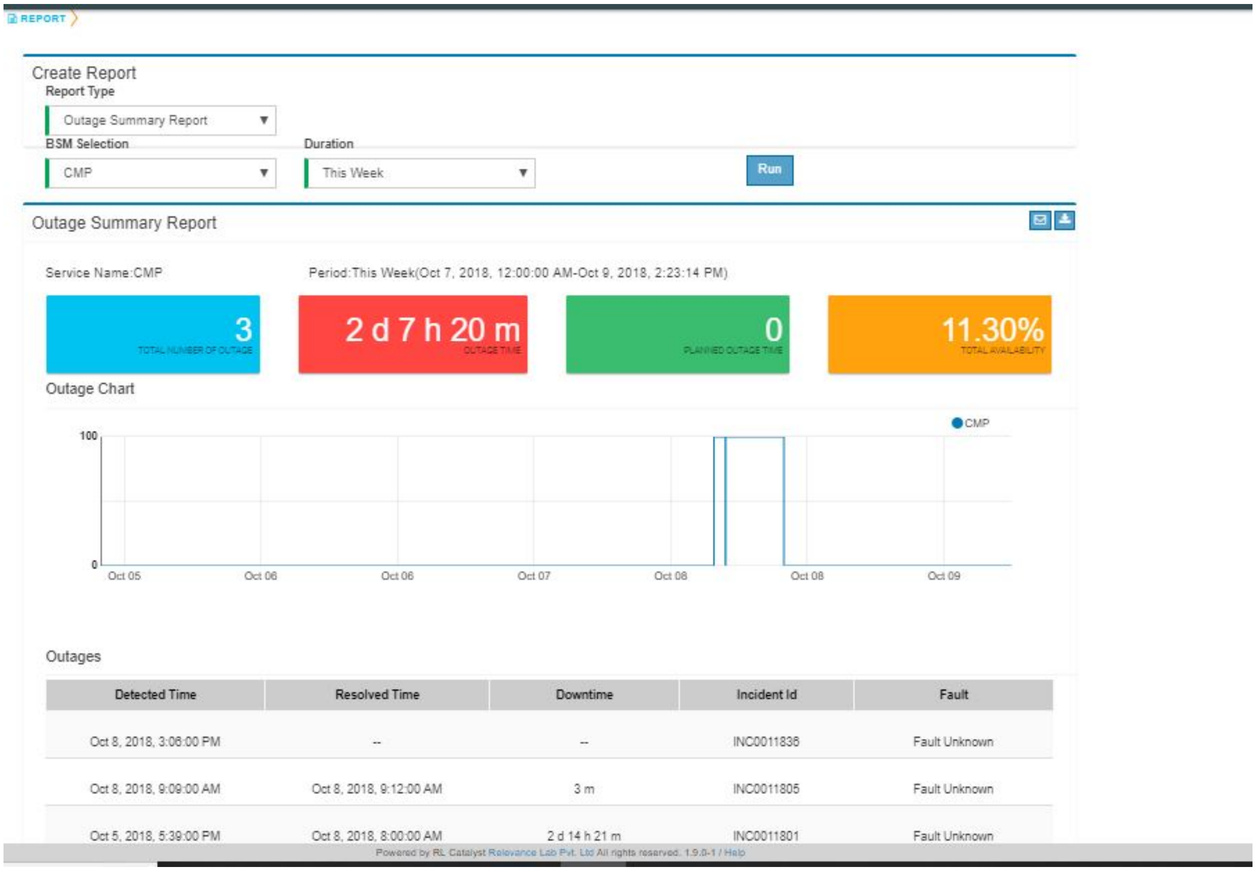
Create Report

Report Type: Outage Summary Report

BSM Selection: Catalyst

Duration: Choose Period

Based on BSM Selection & Duration filter selection,outage summary report shall be generate with the two buttons “Download report as PDF” and “E-mail report”.



Create Report

Report Type: Outage Summary Report

BSM Selection: CMP

Duration: This Week

Outage Summary Report

Service Name:CMP

Period:This Week(Oct 7, 2018, 12:00:00 AM-Oct 9, 2018, 2:23:14 PM)

3 TOTAL NUMBER OF OUTAGE	2 d 7 h 20 m OUTAGE TIME	0 PLANNED OUTAGE TIME	11.30% TOTAL AVAILABILITY

Outage Chart

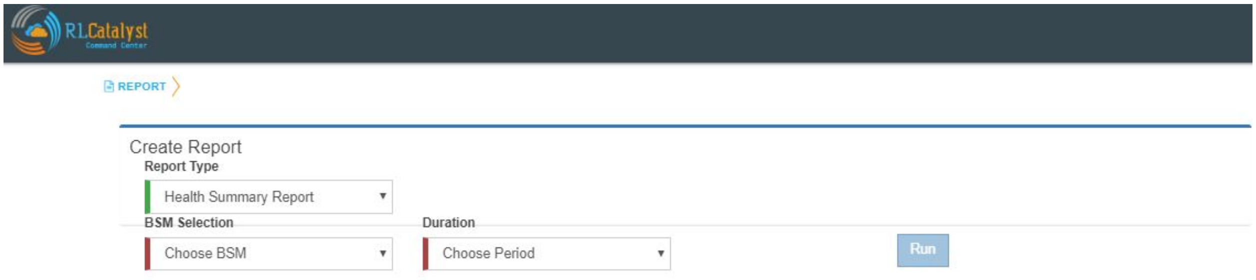
Outages

Detected Time	Resolved Time	Downtime	Incident Id	Fault
Oct 8, 2018, 3:06:00 PM	--	--	INC0011836	Fault Unknown
Oct 8, 2018, 9:09:00 AM	Oct 8, 2018, 9:12:00 AM	3 m	INC0011805	Fault Unknown
Oct 5, 2018, 5:39:00 PM	Oct 8, 2018, 8:00:00 AM	2 d 14 h 21 m	INC0011801	Fault Unknown

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.9.0-1 / Help

1.4.14 Health Summary Report

Clicking on the "Reports" menu item shall lead the user to a screen where he can choose the report to run.



Create Report

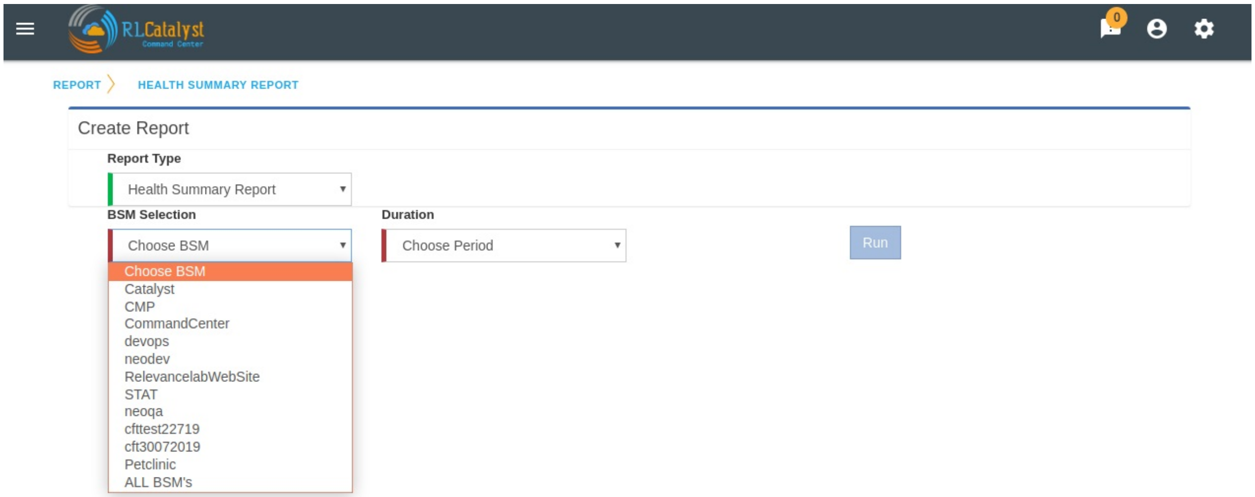
Report Type: Health Summary Report

BSM Selection: Choose BSM

Duration: Choose Period

On choosing the report to run from a drop-down menu, the user shall be displayed the input fields which are specific to that rep

BSM: This will be a drop-down that allows a specific BSM item or All BSMs that will run the report under the logged in tenant.



Create Report

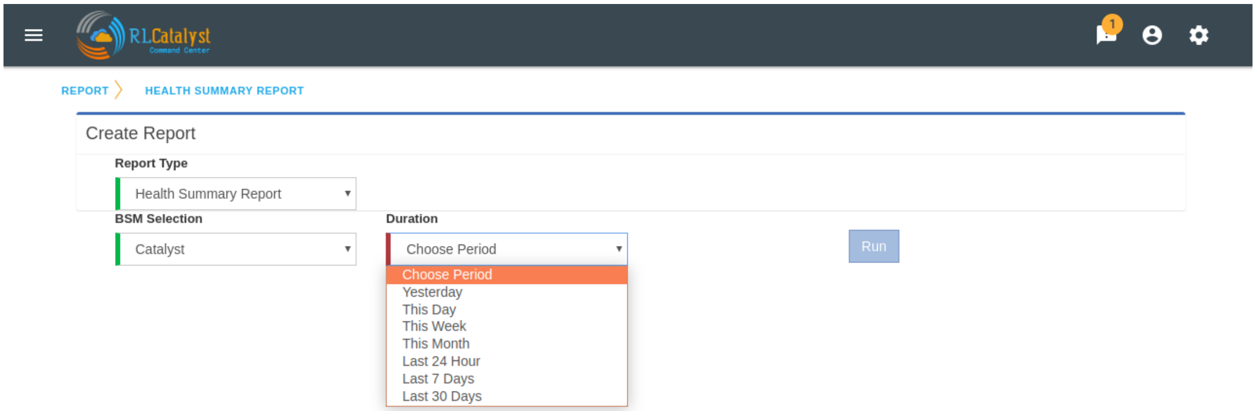
Report Type: Health Summary Report

BSM Selection: Choose BSM

Duration: Choose Period

Time-period: This will be a drop-down box that allows the user to choose the time-period. Available choices shall be

> Yesterday: Will mean the time-period from yesterday 12:00am to 11:59pm. This day: Will mean the time-period from 12:00am of the current date to now. This week: Will mean the time-priod from 12:00am of Monday of the current week to now This month: Will mean the time-period from 12:00am of 1st of the current month to now Last 24 hours: will mean 24 hour period from current time. Last 7 days: will mean 24*7 hour period from current time. Last 30 days: will mean 30*24 hour period from current time.



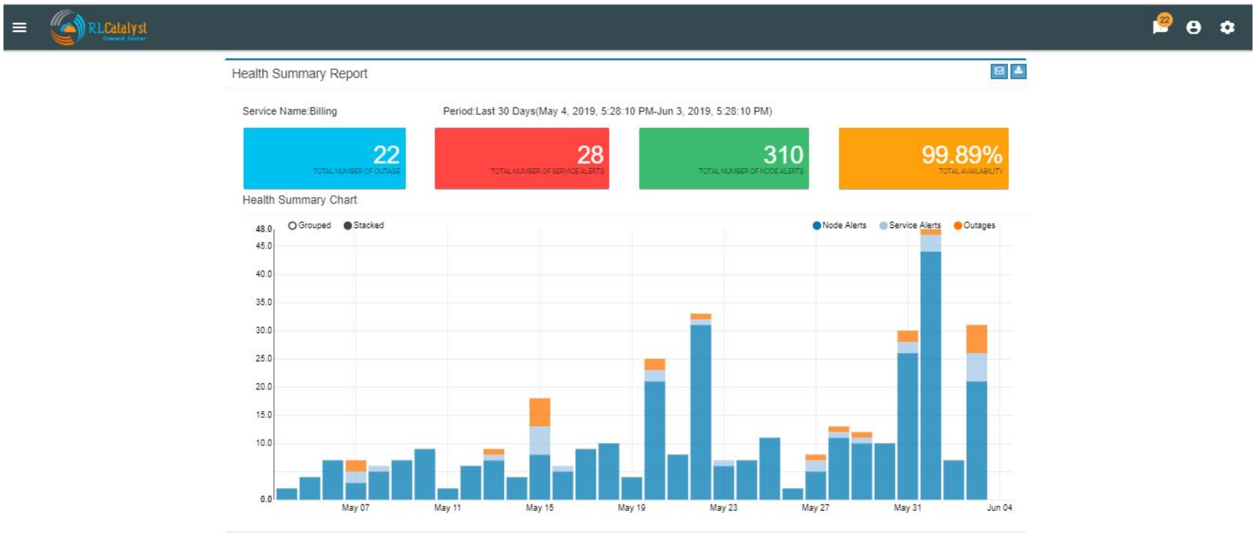
Create Report

Report Type: Health Summary Report

BSM Selection: Catalyst

Duration: Choose Period

Based on BSM Selection & Duration filter selection,outage summary report shall be generate with the two buttons “Download report as PDF” and “E-mail report”.



Health Summary Report

Service Name:Billing

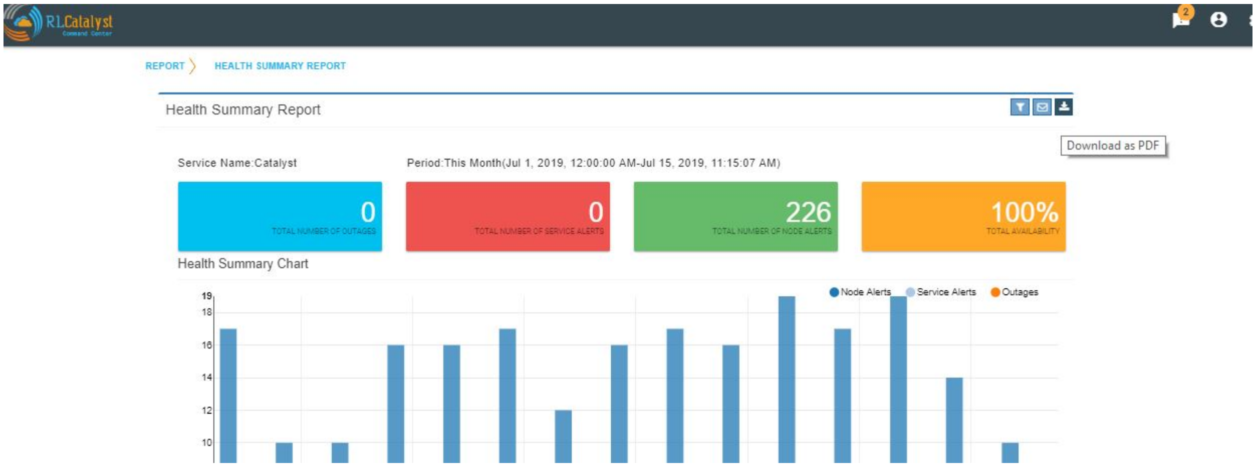
Period:Last 30 Days(May 4, 2019, 5:28:10 PM-Jun 3, 2019, 5:28:10 PM)

22	28	310	99.89%
TOTAL NUMBER OF OUTAGE	TOTAL NUMBER OF SERVICE ALERTS	TOTAL NUMBER OF NODE ALERTS	TOTAL AVAILABILITY

Health Summary Chart

1.4.15 Command Center reports available in PDF format

Command center is providing reports in PDF format with graph and data for both Health summary report and Outage summary report. user can download or send as email the pdf report format. report will be available in all the filters.



REPORT 〉 HEALTH SUMMARY REPORT

Health Summary Report

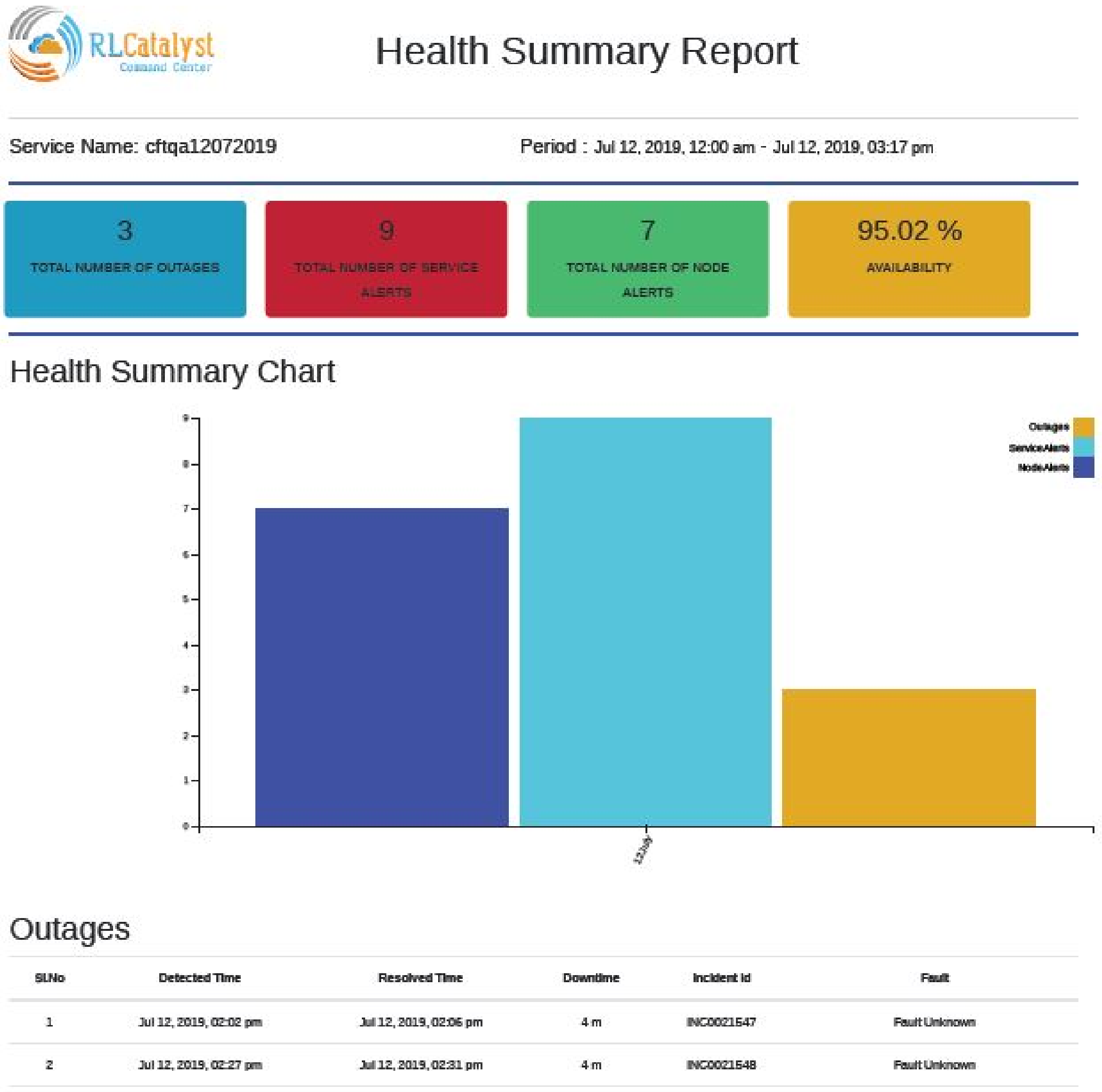
Service Name:Catalyst

Period:This Month(Jul 1, 2019, 12:00:00 AM-Jul 15, 2019, 11:15:07 AM)

0	0	226	100%
TOTAL NUMBER OF OUTAGES	TOTAL NUMBER OF SERVICE ALERTS	TOTAL NUMBER OF NODE ALERTS	TOTAL AVAILABILITY

Health Summary Chart

Downloaded report will be same as bellow for Health summary report.



Health Summary Report

Service Name: cftqa12072019

Period : Jul 12, 2019, 12:00 am - Jul 12, 2019, 03:17 pm

3 TOTAL NUMBER OF OUTAGES	9 TOTAL NUMBER OF SERVICE ALERTS	7 TOTAL NUMBER OF NODE ALERTS	95.02 % AVAILABILITY

Health Summary Chart

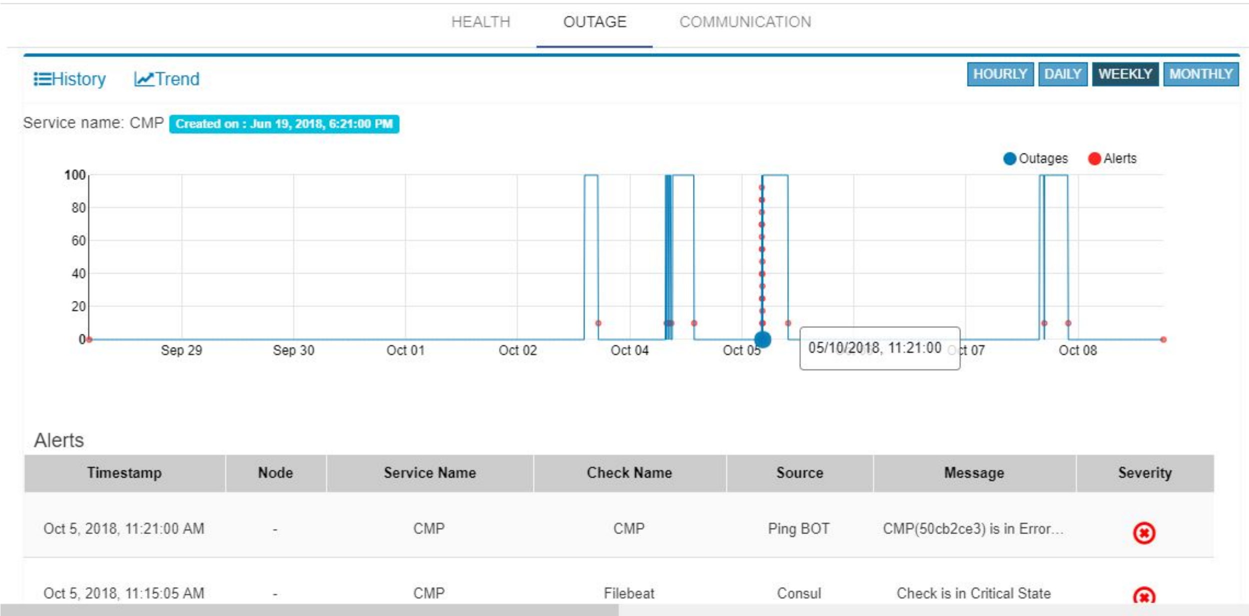
Outages

SlNo	Detected Time	Resolved Time	Downtime	Incident Id	Fault
1	Jul 12, 2019, 02:02 pm	Jul 12, 2019, 02:06 pm	4 m	INC0021547	Fault Unknown
2	Jul 12, 2019, 02:27 pm	Jul 12, 2019, 02:31 pm	4 m	INC0021548	Fault Unknown

1.4.16 Pre-outage Window Analysis

In case of an outage, an operations manager would like to quickly check what alerts have been raised in the time immediately preceding the outage. Pre-outage window analysis feature is to make this information readily available.

In the Outage page under trend-view, shall display the alerts raised against that service or its linked nodes & services on the trend chart as red (error) dots. When the user clicks on a specific outage, screen shall show the alerts in the bottom panel.

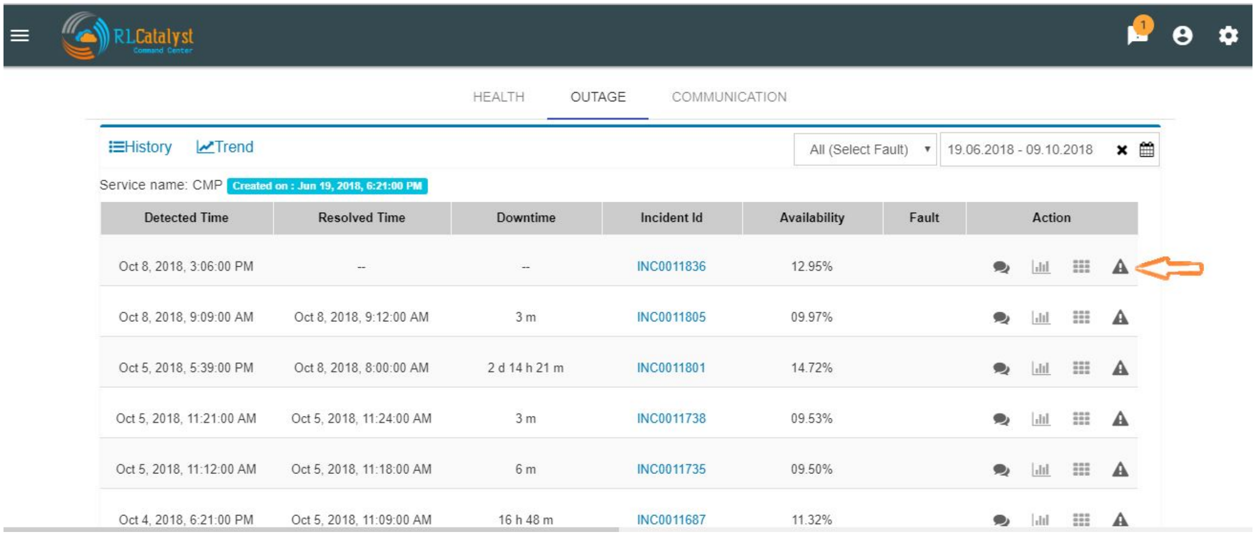


Service name: CMP Created on : Jun 19, 2018, 6:21:00 PM

Alerts

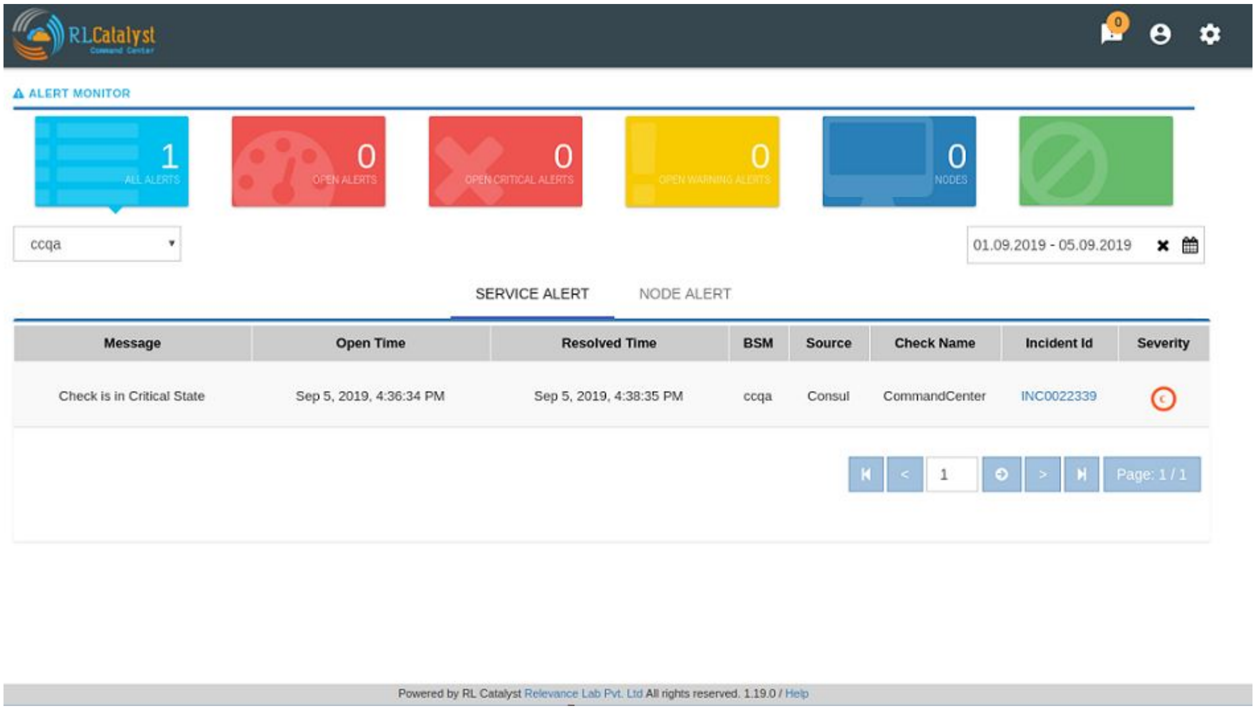
Timestamp	Node	Service Name	Check Name	Source	Message	Severity
Oct 5, 2018, 11:21:00 AM	-	CMP	CMP	Ping BOT	CMP(50cb2ce3) is in Error…	⊗
Oct 5, 2018, 11:15:05 AM	-	CMP	Filebeat	Consul	Check is in Critical State	⊗

In the Outage page under History-view, an Alerts icon shall be displayed to the user under the "Action" column. Clicking on the icon should lead the user to the Alerts Monitor page with the alerts for only that BSM listed with the latest alert being the last alert seen preceding the Outage detection time.



Service name: CMP Created on : Jun 19, 2018, 6:21:00 PM

Detected Time	Resolved Time	Downtime	Incident Id	Availability	Fault	Action
Oct 8, 2018, 3:06:00 PM	--	--	INC0011836	12.95%		💬 📊 ▦ ⚠
Oct 8, 2018, 9:09:00 AM	Oct 8, 2018, 9:12:00 AM	3 m	INC0011805	09.97%		💬 📊 ▦ ⚠
Oct 5, 2018, 5:39:00 PM	Oct 8, 2018, 8:00:00 AM	2 d 14 h 21 m	INC0011801	14.72%		💬 📊 ▦ ⚠
Oct 5, 2018, 11:21:00 AM	Oct 5, 2018, 11:24:00 AM	3 m	INC0011738	09.53%		💬 📊 ▦ ⚠
Oct 5, 2018, 11:12:00 AM	Oct 5, 2018, 11:18:00 AM	6 m	INC0011735	09.50%		💬 📊 ▦ ⚠
Oct 4, 2018, 6:21:00 PM	Oct 5, 2018, 11:09:00 AM	16 h 48 m	INC0011687	11.32%		💬 📊 ▦ ⚠



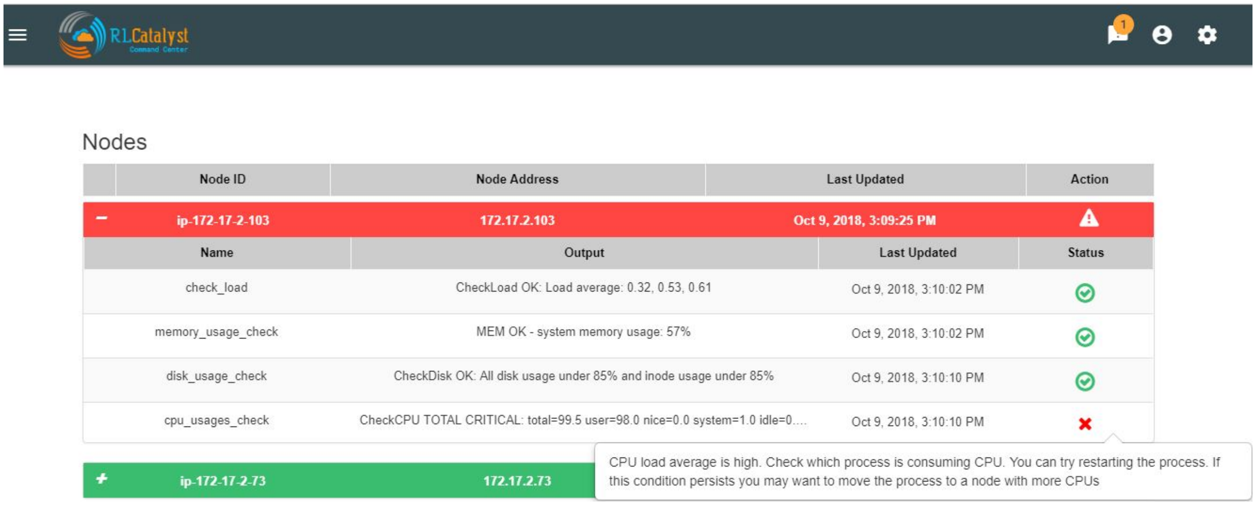
Message	Open Time	Resolved Time	BSM	Source	Check Name	Incident Id	Severity
Check is in Critical State	Sep 5, 2019, 4:36:34 PM	Sep 5, 2019, 4:38:35 PM	ccqa	Consul	CommandCenter	INC0022339	C

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.19.0 / Help

1.4.17 Information pop-up when checks fail

Command Center will show the user warnings or errors for system parameters when certain thresholds are crossed for certain metrics (CPU, disk usage, memory usage). The idea of this feature is to provide the user with helpful information against these warnings.

The user shall be shown an “info” icon against each warning or error for the system checks (CPU, disk usage, memory usage)in the BSM drilldown screen. This icon will be shown under the “Action” column.Clicking on the icon will show the appropriate message to the user.



Nodes

	Node ID	Node Address	Last Updated	Action
−	ip-172-17-2-103	172.17.2.103	Oct 9, 2018, 3:09:25 PM	⚠

Name	Output	Last Updated	Status
check_load	CheckLoad OK: Load average: 0.32, 0.53, 0.61	Oct 9, 2018, 3:10:02 PM	✓
memory_usage_check	MEM OK - system memory usage: 57%	Oct 9, 2018, 3:10:02 PM	✓
disk_usage_check	CheckDisk OK: All disk usage under 85% and inode usage under 85%	Oct 9, 2018, 3:10:10 PM	✓
cpu_usages_check	CheckCPU TOTAL CRITICAL: total=99.5 user=98.0 nice=0.0 system=1.0 idle=0....	Oct 9, 2018, 3:10:10 PM	✖

CPU load average is high. Check which process is consuming CPU. You can try restarting the process. If this condition persists you may want to move the process to a node with more CPUs

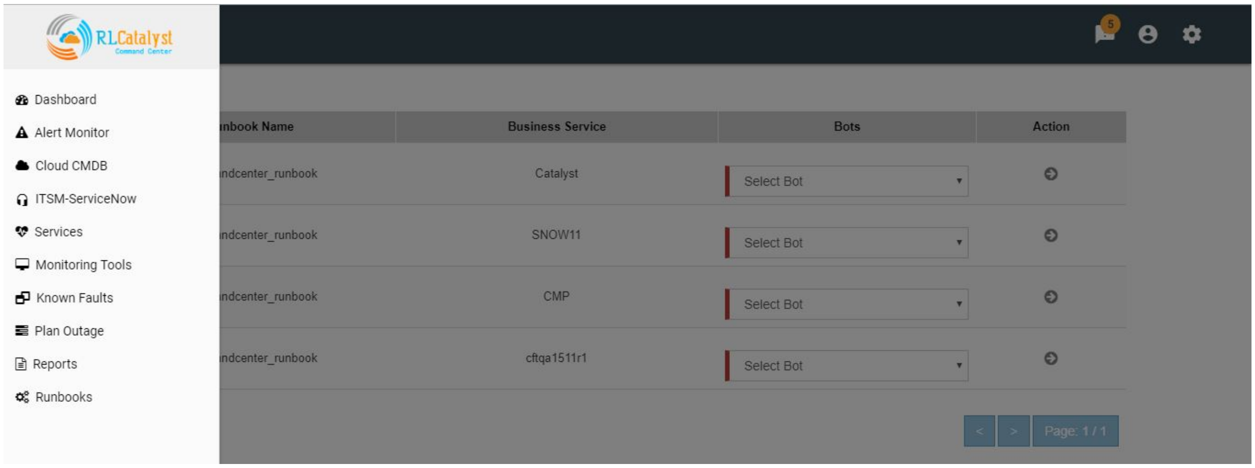
+	ip-172-17-2-73	172.17.2.73

1.4.18 Runbook Automation

Operations teams define runbooks so that all team-members have access to precise information regarding routines and procedures that are carried out. These runbooks contain information about the specific systems that are being monitored like server IPs, dependent services and the topology. Runbooks also document the Standard Operating Procedures that are to be followed for specific situations. Runbooks are important repositories of knowledge when team-members are trying to resolve outages or trouble-shooting problems. They also provide a reliable documentation that can be followed to achieve specific outcomes.

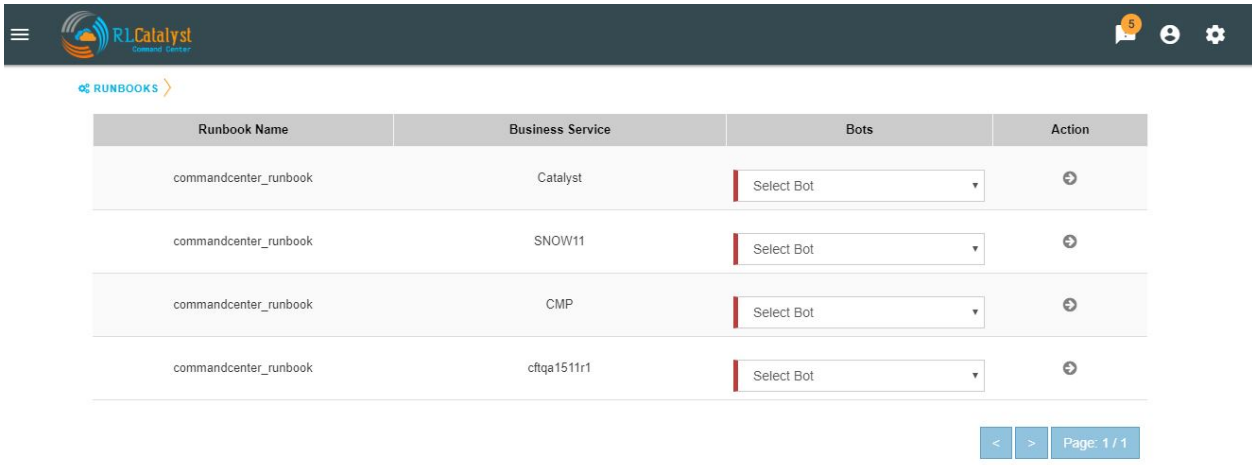
RLCatalyst now allows users to automate these runbooks as collections of BOTs and execute specific runbooks against Business Services and the underlying infrastructure or components.

A new item called "Runbooks" link is added to the application-menu (top-left).



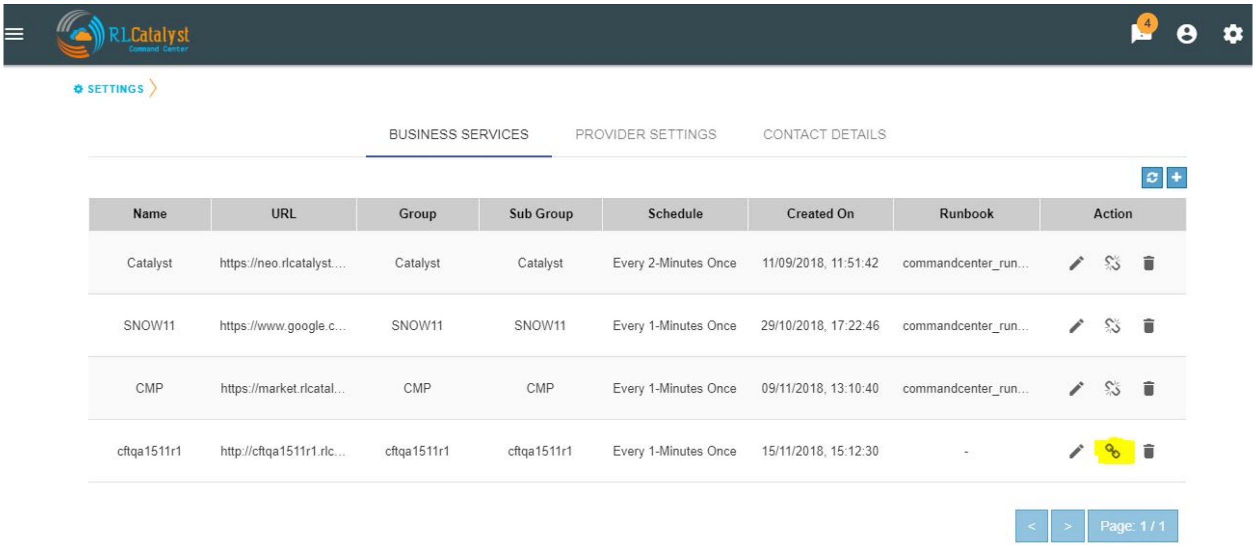
ınbook Name	Business Service	Bots	Action
ndcenter_runbook	Catalyst	Select Bot ▾	➲
ndcenter_runbook	SNOW11	Select Bot ▾	➲
ndcenter_runbook	CMP	Select Bot ▾	➲
ndcenter_runbook	cftqa1511r1	Select Bot ▾	➲

Clicking on "Runbooks" link will navigate to the Runbooks screen.



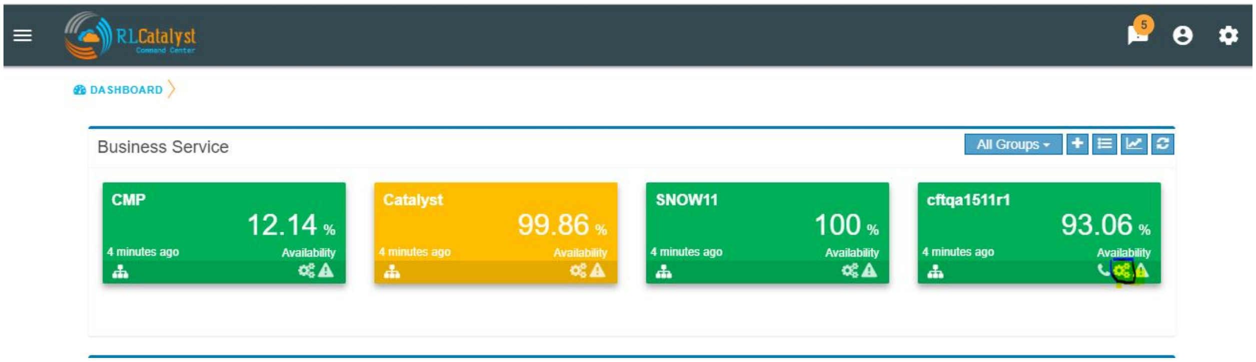
Runbook Name	Business Service	Bots	Action
commandcenter_runbook	Catalyst	Select Bot ▾	➲
commandcenter_runbook	SNOW11	Select Bot ▾	➲
commandcenter_runbook	CMP	Select Bot ▾	➲
commandcenter_runbook	cftqa1511r1	Select Bot ▾	➲

You can opt for Runbook Automation option by associating the runbook to the BSM by clicking on the "Link Runbook" button which is available under Business Services tab in the Settings screen.



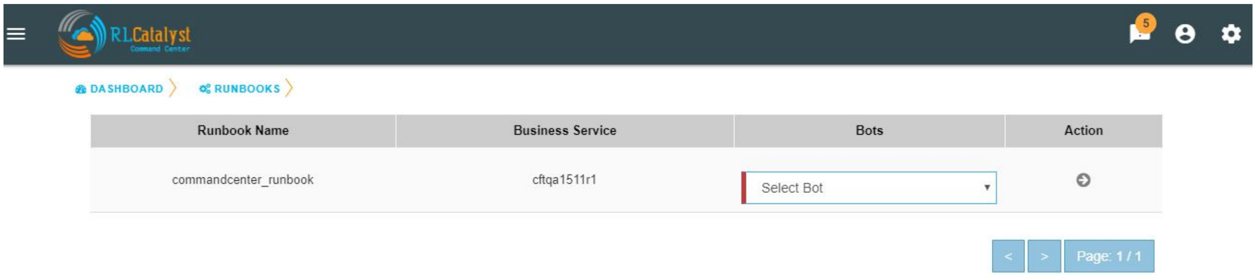
Name	URL	Group	Sub Group	Schedule	Created On	Runbook	Action
Catalyst	https://neo.rlcatalyst....	Catalyst	Catalyst	Every 2-Minutes Once	11/09/2018, 11:51:42	commandcenter_run...	
SNOW11	https://www.google.c...	SNOW11	SNOW11	Every 1-Minutes Once	29/10/2018, 17:22:46	commandcenter_run...	
CMP	https://market.rlcatal...	CMP	CMP	Every 1-Minutes Once	09/11/2018, 13:10:40	commandcenter_run...	
cftqa1511r1	http://cftqa1511r1.rlc...	cftqa1511r1	cftqa1511r1	Every 1-Minutes Once	15/11/2018, 15:12:30	-	

On the Dashboard screen, BSM card should show a Runbook icon when a Runbook has been linked with the Business Service.



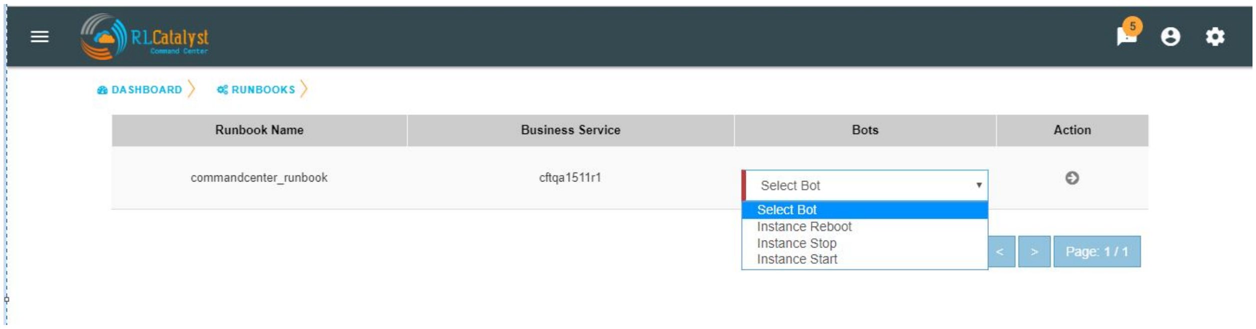
CMP	Catalyst	SNOW11	cftqa1511r1
12.14 %	99.86 %	100 %	93.06 %
4 minutes ago	4 minutes ago	4 minutes ago	4 minutes ago
Availability	Availability	Availability	Availability

Clicking on Runbook icon in the DashBoard screen, should navigate to the Runbooks screen of that Business Service



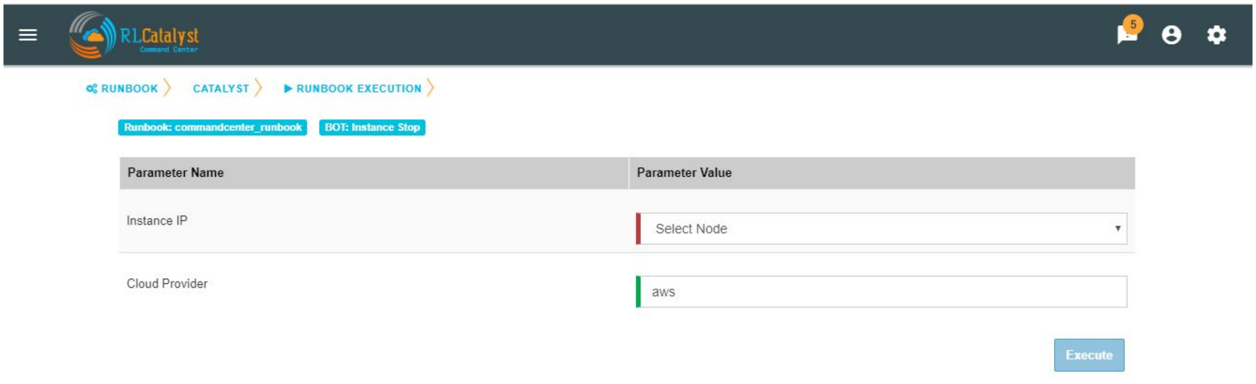
Runbook Name	Business Service	Bots	Action
commandcenter_runbook	cftqa1511r1	Select Bot ▾	

You can choose the required BOT from the BOT's selection menu in the Runbooks screen and click on Next Step button.



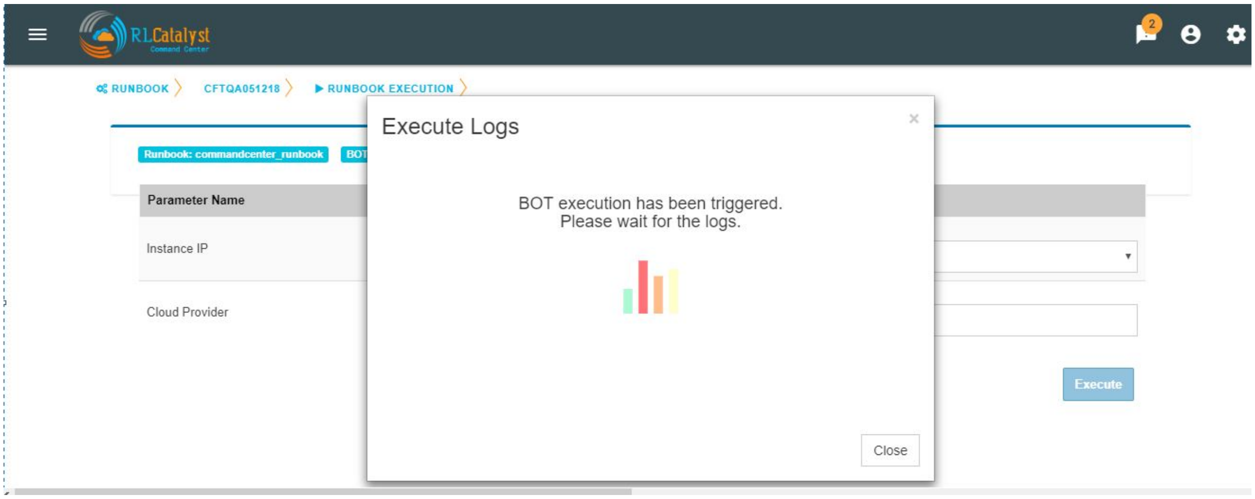
Runbook Name	Business Service	Bots	Action
commandcenter_runbook	cftqa1511r1	Select Bot	

You can execute BOT by passing required parameters to the IP, Cloud Provider and click on Execute Button.



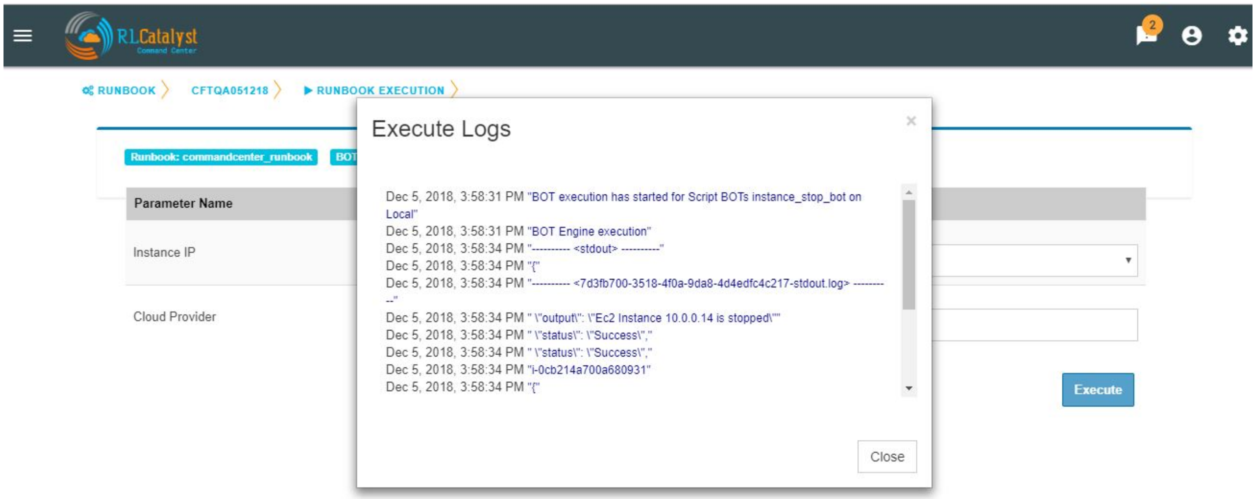
Parameter Name	Parameter Value
Instance IP	Select Node
Cloud Provider	aws

On BOT execution ,user can see a popup message about the BOT execution after that logs of that particular BOT execution as a popup.



Execute Logs

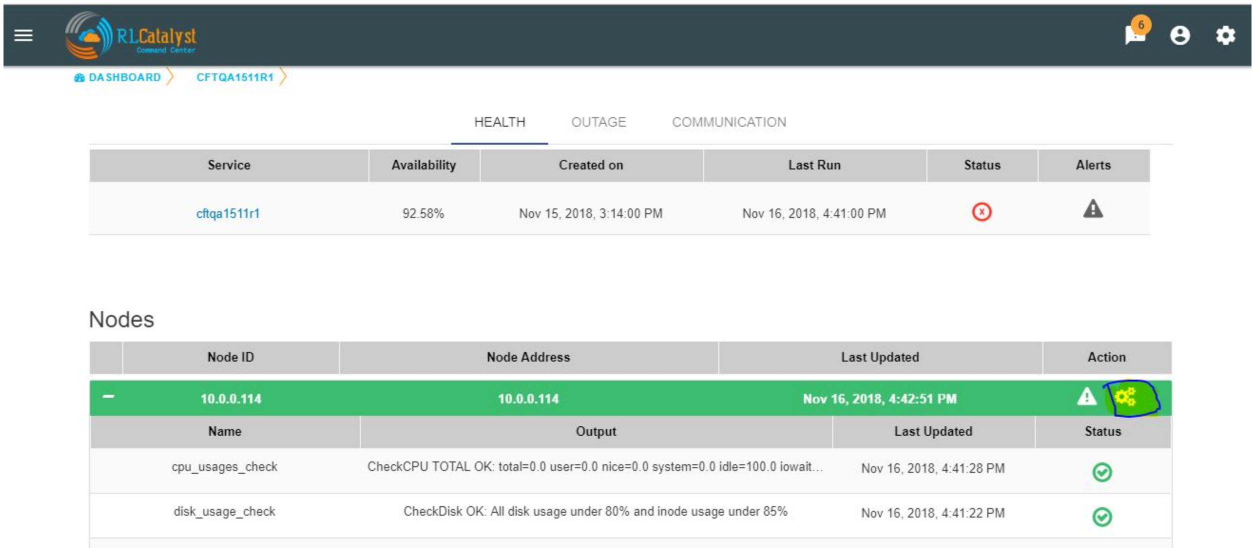
BOT execution has been triggered.
Please wait for the logs.



Execute Logs

```
Dec 5, 2018, 3:58:31 PM "BOT execution has started for Script BOTs instance_stop_bot on
Local"
Dec 5, 2018, 3:58:31 PM "BOT Engine execution"
Dec 5, 2018, 3:58:34 PM "---------- <stdout> ----------"
Dec 5, 2018, 3:58:34 PM "{"
Dec 5, 2018, 3:58:34 PM "---------- <7d3fb700-3518-4f0a-9da8-4d4edfc4c217-stdout.log> --------
--"
Dec 5, 2018, 3:58:34 PM " \"output\": \"Ec2 Instance 10.0.0.14 is stopped\""
Dec 5, 2018, 3:58:34 PM " \"status\": \"Success\","
Dec 5, 2018, 3:58:34 PM " \"status\": \"Success\","
Dec 5, 2018, 3:58:34 PM "i-0cb214a700a680931"
Dec 5, 2018, 3:58:34 PM "{"
```

You can execute BOT from the BSM Drilldown screen by clicking on the “Run BOTS” icon available against nodes.



Service	Availability	Created on	Last Run	Status	Alerts
cftqa1511r1	92.58%	Nov 15, 2018, 3:14:00 PM	Nov 16, 2018, 4:41:00 PM	⊗	⚠

Nodes

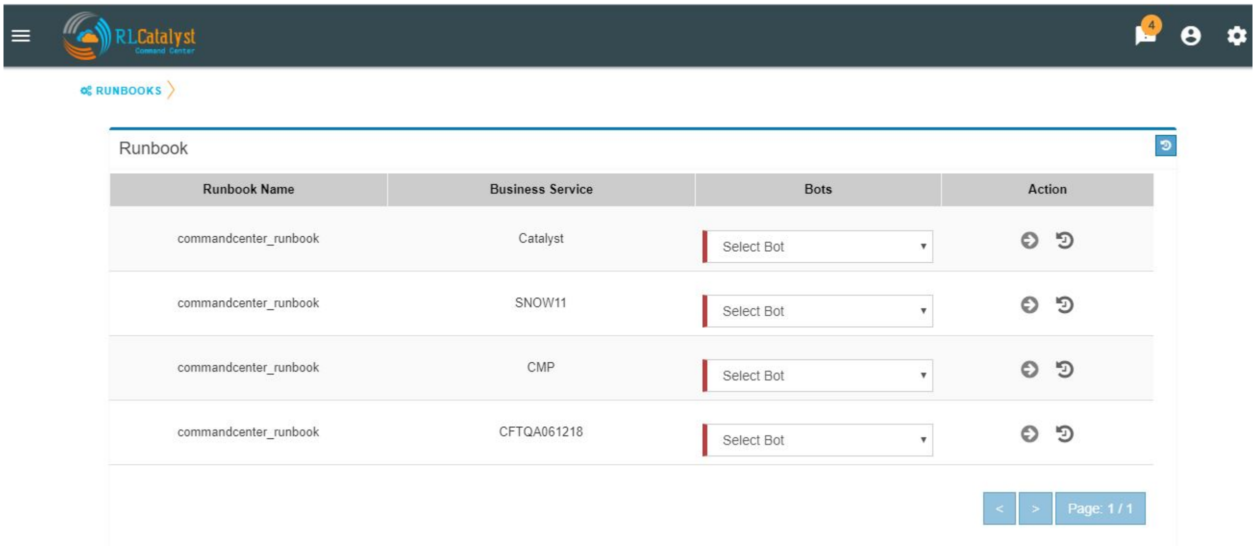
	Node ID	Node Address	Last Updated	Action
−	10.0.0.114	10.0.0.114	Nov 16, 2018, 4:42:51 PM	⚠ ⚙

Name	Output	Last Updated	Status
cpu_usages_check	CheckCPU TOTAL OK: total=0.0 user=0.0 nice=0.0 system=0.0 idle=100.0 iowait...	Nov 16, 2018, 4:41:28 PM	✓
disk_usage_check	CheckDisk OK: All disk usage under 80% and inode usage under 85%	Nov 16, 2018, 4:41:22 PM	✓

1.4.19 Runbook History

Runbook History will record Success and Failure streams intended to log problems that occur in a runbook. They are written to the Runbook history when a runbook is executed.

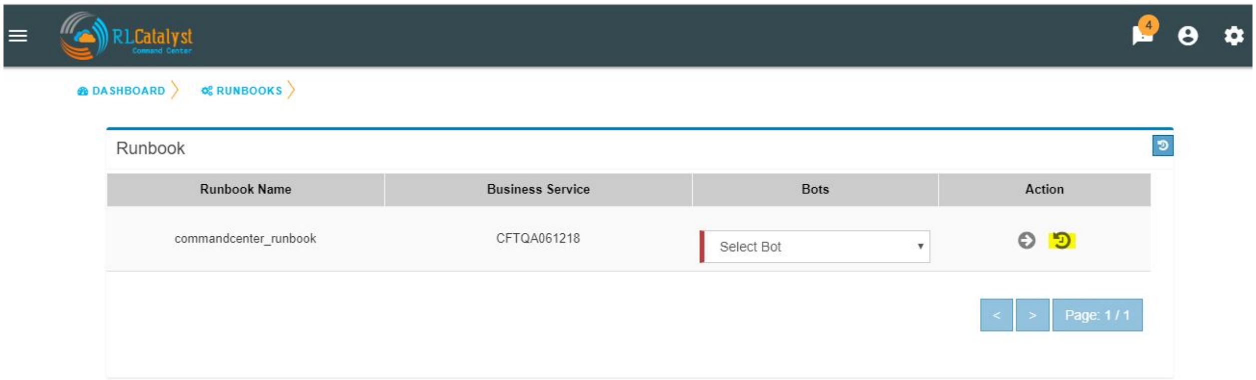
A new item called “Runbooks History” will show as an icon in the Runbook screen and it will display the available runbooks history



Runbook

Runbook Name	Business Service	Bots	Action
commandcenter_runbook	Catalyst	Select Bot	
commandcenter_runbook	SNOW11	Select Bot	
commandcenter_runbook	CMP	Select Bot	
commandcenter_runbook	CFTQA061218	Select Bot	

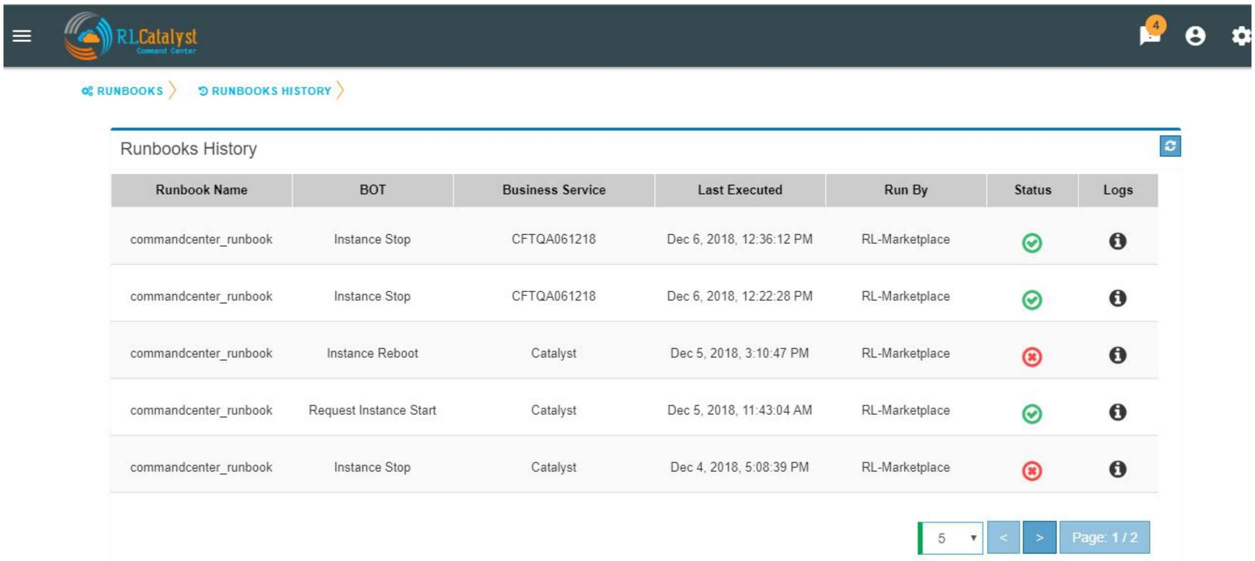
Clicking on “Runbooks History” icon in the Runbook screen will navigate to “Runbooks History” screen.



Runbook

Runbook Name	Business Service	Bots	Action
commandcenter_runbook	CFTQA061218	Select Bot	

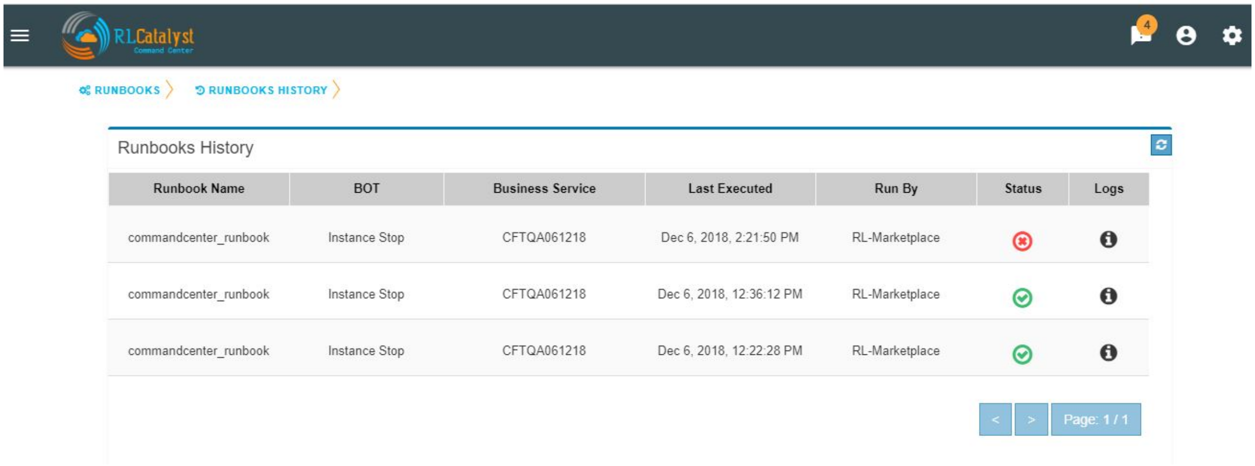
You can view the particular Runbook history by clicking on the “History” icon which is available in the specific Business Service related Runbook screen.



Runbooks History

Runbook Name	BOT	Business Service	Last Executed	Run By	Status	Logs
commandcenter_runbook	Instance Stop	CFTQA061218	Dec 6, 2018, 12:36:12 PM	RL-Marketplace	✓	ⓘ
commandcenter_runbook	Instance Stop	CFTQA061218	Dec 6, 2018, 12:22:28 PM	RL-Marketplace	✓	ⓘ
commandcenter_runbook	Instance Reboot	Catalyst	Dec 5, 2018, 3:10:47 PM	RL-Marketplace	✗	ⓘ
commandcenter_runbook	Request Instance Start	Catalyst	Dec 5, 2018, 11:43:04 AM	RL-Marketplace	✓	ⓘ
commandcenter_runbook	Instance Stop	Catalyst	Dec 4, 2018, 5:08:39 PM	RL-Marketplace	✗	ⓘ

By clicking on “History” screen you can view the specific Business Service related runbook history.



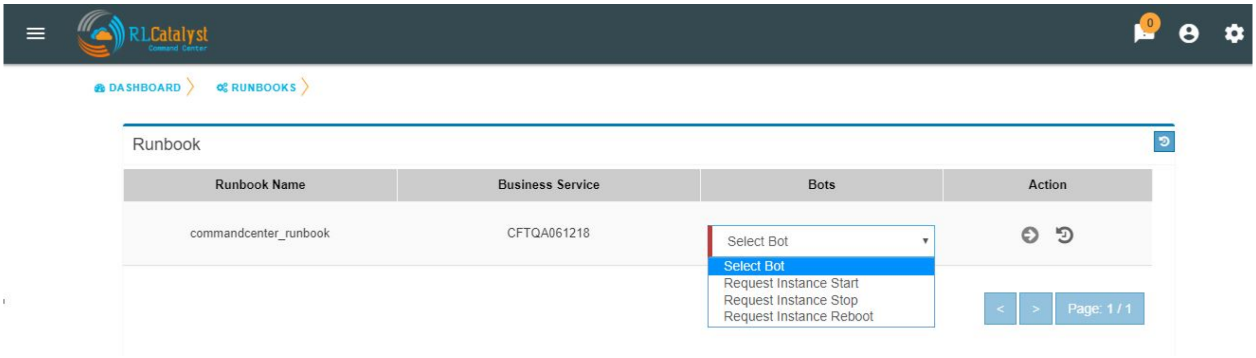
Runbooks History

Runbook Name	BOT	Business Service	Last Executed	Run By	Status	Logs
commandcenter_runbook	Instance Stop	CFTQA061218	Dec 6, 2018, 2:21:50 PM	RL-Marketplace	✗	ℹ
commandcenter_runbook	Instance Stop	CFTQA061218	Dec 6, 2018, 12:36:12 PM	RL-Marketplace	✓	ℹ
commandcenter_runbook	Instance Stop	CFTQA061218	Dec 6, 2018, 12:22:28 PM	RL-Marketplace	✓	ℹ

1.4.20 Role based access to BOT's

CommandCenter facilitates the role-based access permissions to the BOT's. Based on the level defined for the logged-in user, the system will display the BOTs to the user which he is entitled to run. Level 0, Level 1 are the two levels defined in the CommandCenter. You can extend the levels based on need.

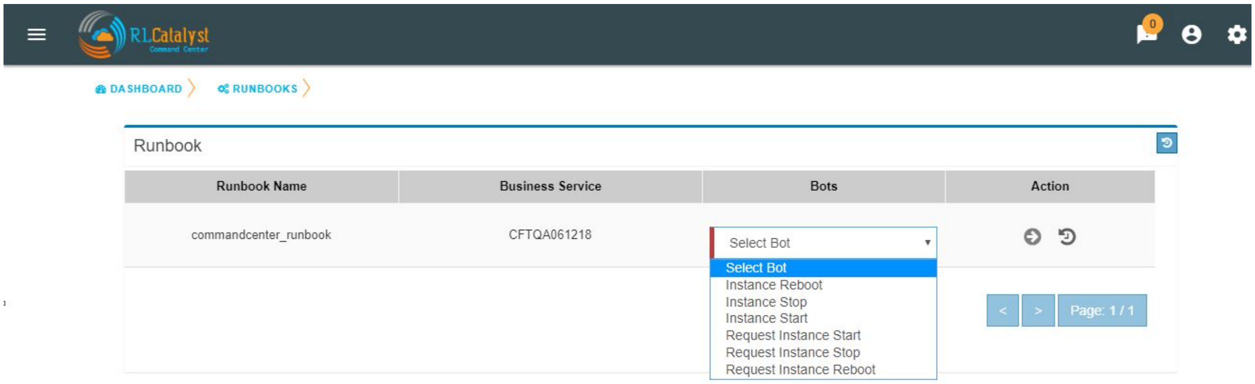
BOTs availability for L0 user :



Runbook

Runbook Name	Business Service	Bots	Action
commandcenter_runbook	CFTQA061218	Select Bot	

BOTs availability for L1 user :



Runbook

Runbook Name	Business Service	Bots	Action
commandcenter_runbook	CFTQA061218	Select Bot	

1.4.21 Event triggered runbook execution

Event triggered runbook execution feature will run the BOT when event is triggered. User can add their own event by editing BOTs factory file. Once the alerts got triggered from sensu/consul/pingbot the respected BOT will run. User can add notifications bot like(SMS_BOT/Email/slack). Once the BOT is triggered user can verify this from CC(Runbook -> Bots history.)

BOT Context

This list consist of the BOT parameters that CC can accept currently to execute Event triggered BOTs. When a BOT is written, it can have parameters only from below list. If some other parameter is passed, BOT will be executed with default parameter given with BOT's definition.

BOT Parameter Name	Description
Account Name	Enter a Friendly name
awsInstanceIp	IP of AWS instance on which operation is to be performed by BOT
sourceCloud	Credential name by which credential is saved Catalyst.
sender_name	Name of sender by which SMS to be sent.
message	Body of Message.
apiKey	API key required to send SMS to user.
number	Receivers phone number.

Event triggered BOT

Event triggered runbook execution feature will run the BOT when event is triggered.

User can configure which BOT can execute on which event by editing runbook. Once the event got triggered from server the configured BOT will run.

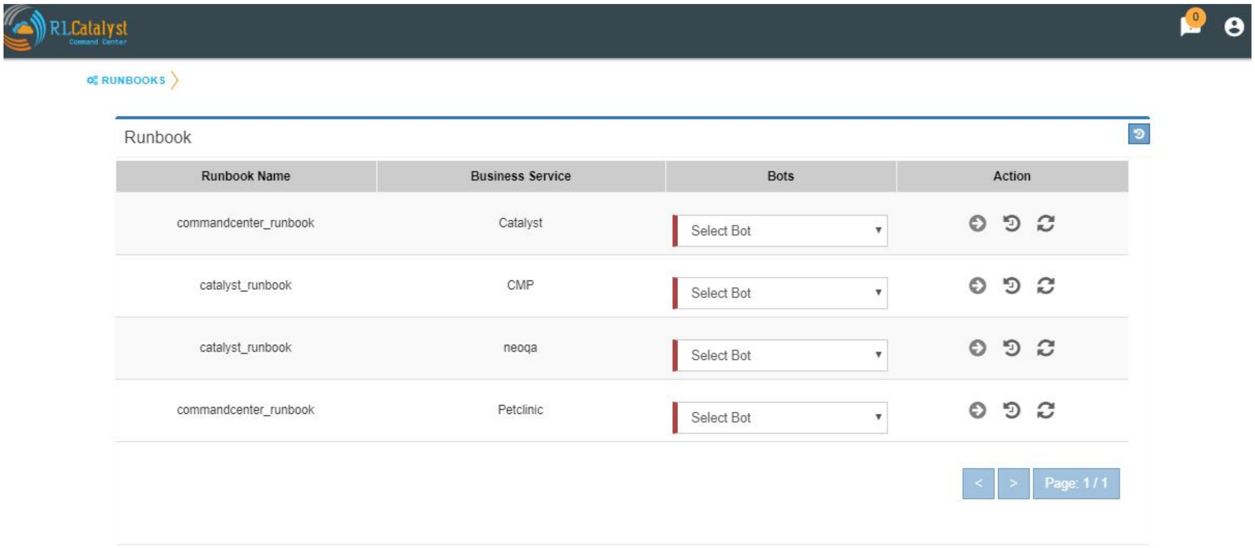
Event trigger Parameter Name	Description
checkID	Check ID in server
severity	severity of check in server
source	Server name
state	Check state
botID	BOT ID from catalyst.

Once the BOT and Event are created need to sync the Botfactory in Catalyst and then CC.

Refresh Runbook in CC

User can update the cache in CC using “Refresh Runbook” icon.

Refresh Icon in CC:

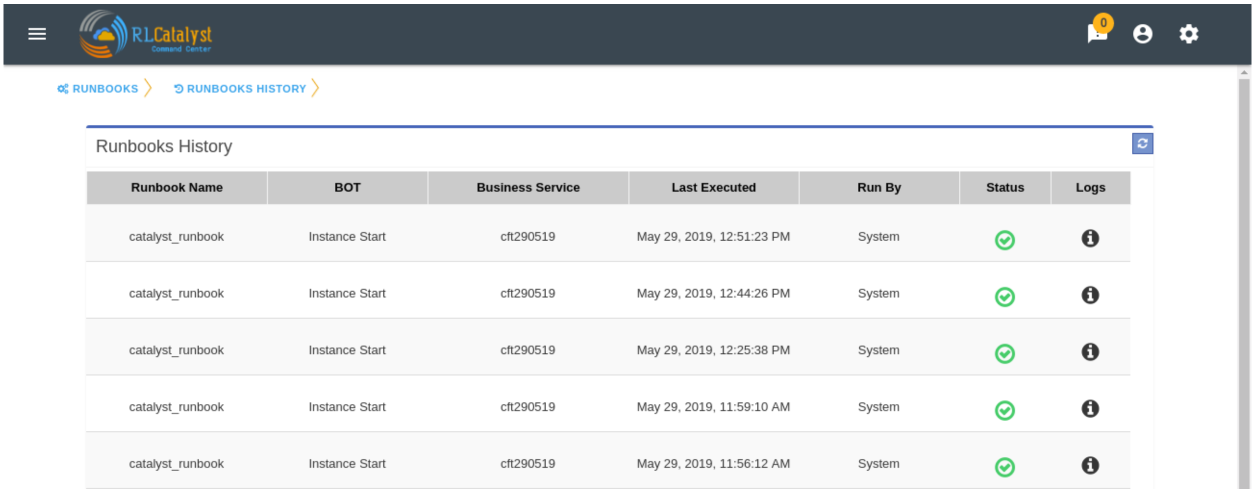


Runbook

Runbook Name	Business Service	Bots	Action
commandcenter_runbook	Catalyst	Select Bot ▾	➜ ⟲ ⟳
catalyst_runbook	CMP	Select Bot ▾	➜ ⟲ ⟳
catalyst_runbook	neoqa	Select Bot ▾	➜ ⟲ ⟳
commandcenter_runbook	Petclinic	Select Bot ▾	➜ ⟲ ⟳

< > Page: 1 / 1

History of runbook contains the RunBy column as user can verify the BOTs triggerd information based on tenant or automation BOT.



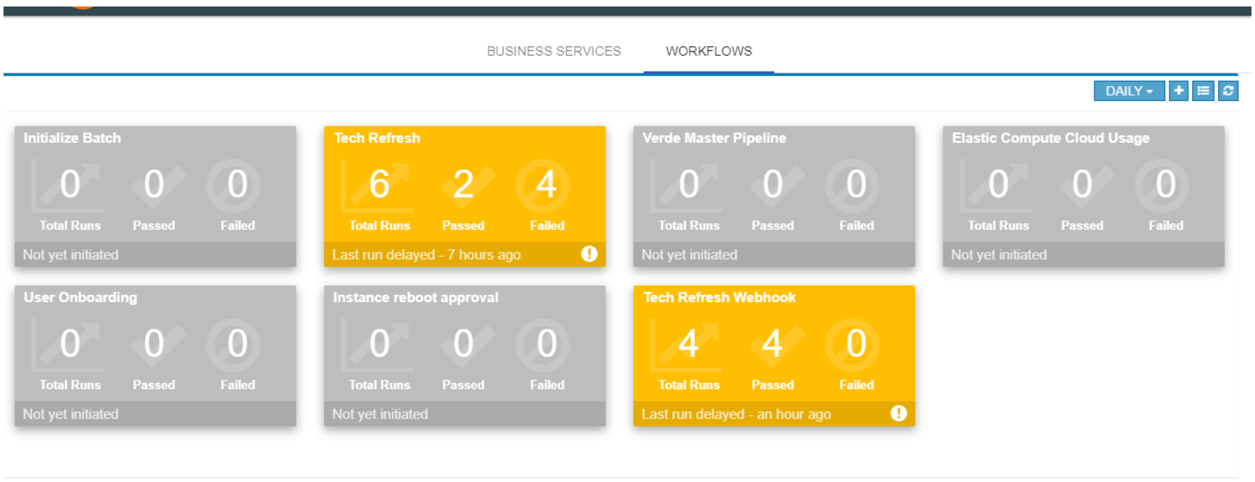
Runbooks History

Runbook Name	BOT	Business Service	Last Executed	Run By	Status	Logs
catalyst_runbook	Instance Start	cft290519	May 29, 2019, 12:51:23 PM	System	✓	ℹ
catalyst_runbook	Instance Start	cft290519	May 29, 2019, 12:44:26 PM	System	✓	ℹ
catalyst_runbook	Instance Start	cft290519	May 29, 2019, 12:25:38 PM	System	✓	ℹ
catalyst_runbook	Instance Start	cft290519	May 29, 2019, 11:59:10 AM	System	✓	ℹ
catalyst_runbook	Instance Start	cft290519	May 29, 2019, 11:56:12 AM	System	✓	ℹ

1.4.22 Workflow Monitoring

Workflow monitoring feature is used to monitor the workflows, which are run under the RLCatalyst Workflow Engine. The individual nodes in the workflow are modelled as BOTs.

There is tab like “workflows” in main page.when you clicked on that link, it will navigated to workflow monitoring page.On the workflow dashboard page, each workflow is represented by a card which shows the total number of runs completed and passed and failed outcomes.



Initialize Batch
0 Total Runs 0 Passed 0 Failed
Not yet initiated

Tech Refresh
6 Total Runs 2 Passed 4 Failed
Last run delayed - 7 hours ago

Verde Master Pipeline
0 Total Runs 0 Passed 0 Failed
Not yet initiated

Elastic Compute Cloud Usage
0 Total Runs 0 Passed 0 Failed
Not yet initiated

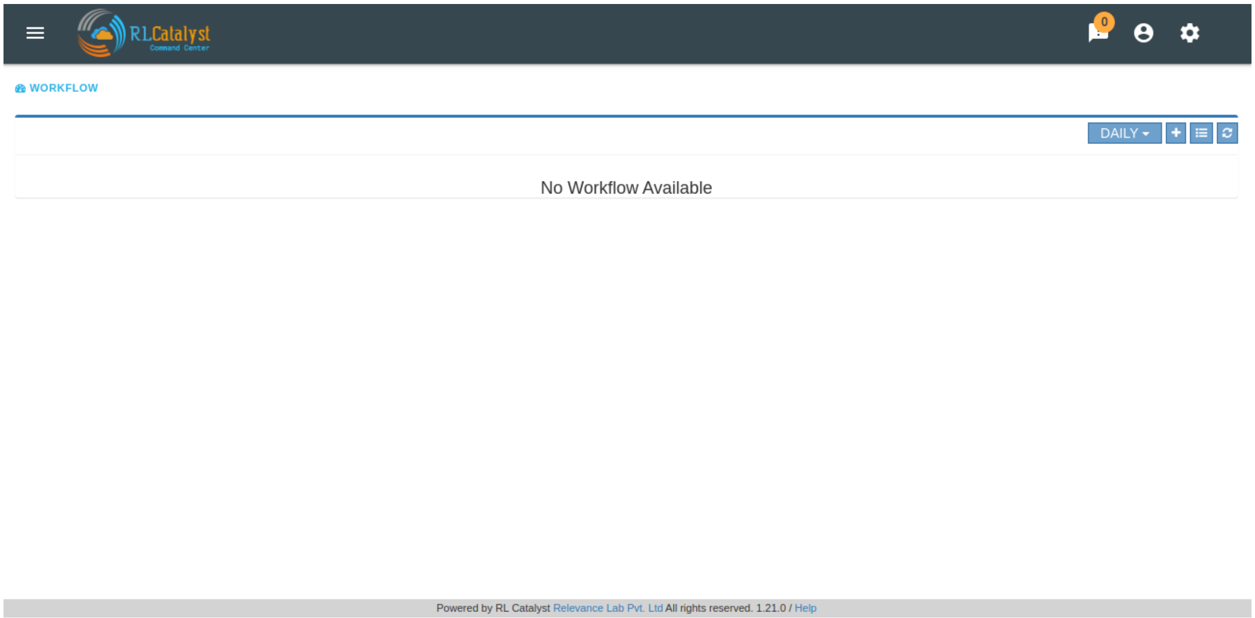
User Onboarding
0 Total Runs 0 Passed 0 Failed
Not yet initiated

Instance reboot approval
0 Total Runs 0 Passed 0 Failed
Not yet initiated

Tech Refresh Webhook
4 Total Runs 4 Passed 0 Failed
Last run delayed - an hour ago

images/Workflow_Dashboard.png

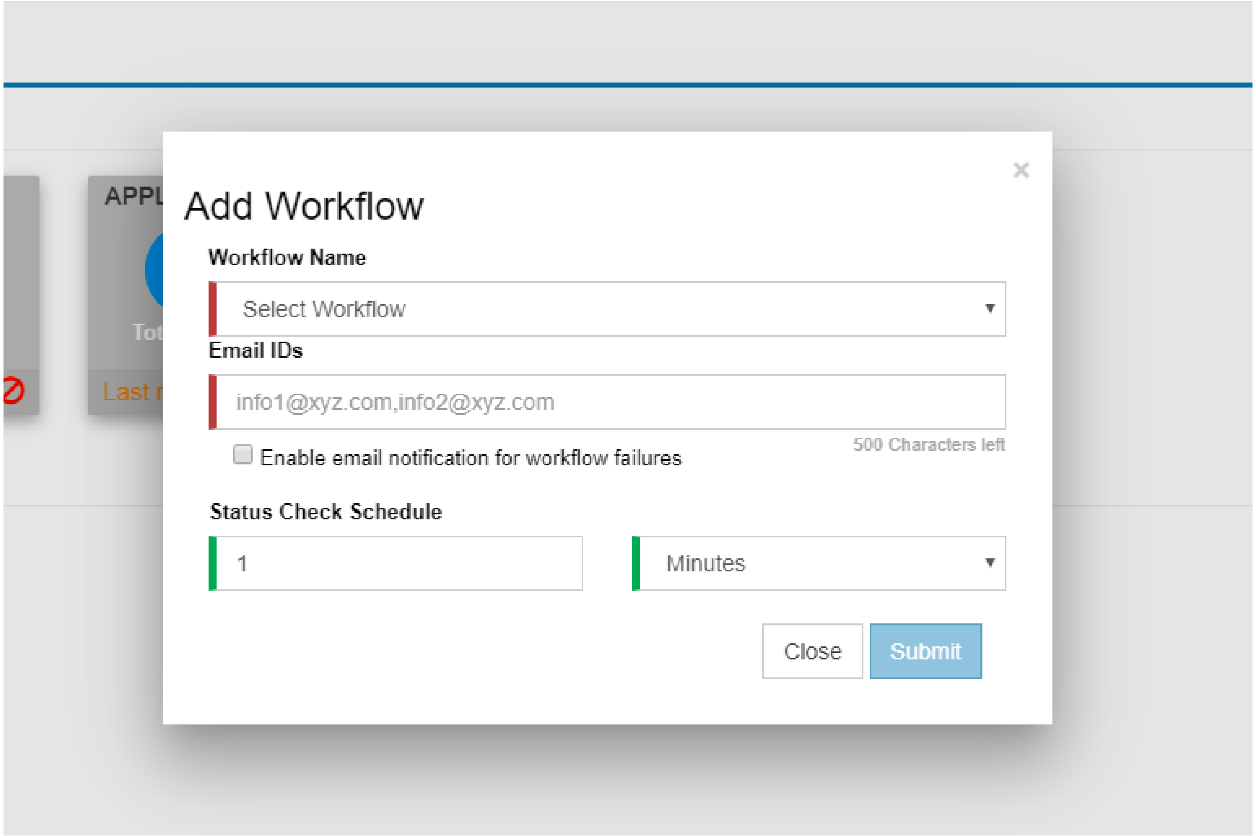
Initially there are no workflows it shows "No workflows available" message.



No Workflow Available

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.21.0 / Help

You can add a workflow by clicking on the '+' button.



Add Workflow

Workflow Name

Select Workflow

Email IDs

info1@xyz.com,info2@xyz.com

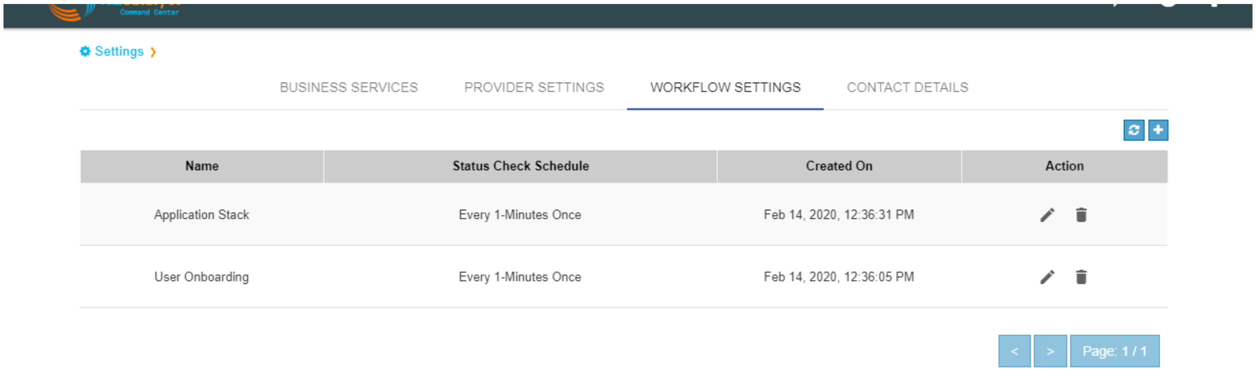
500 Characters left

□ Enable email notification for workflow failures

Status Check Schedule

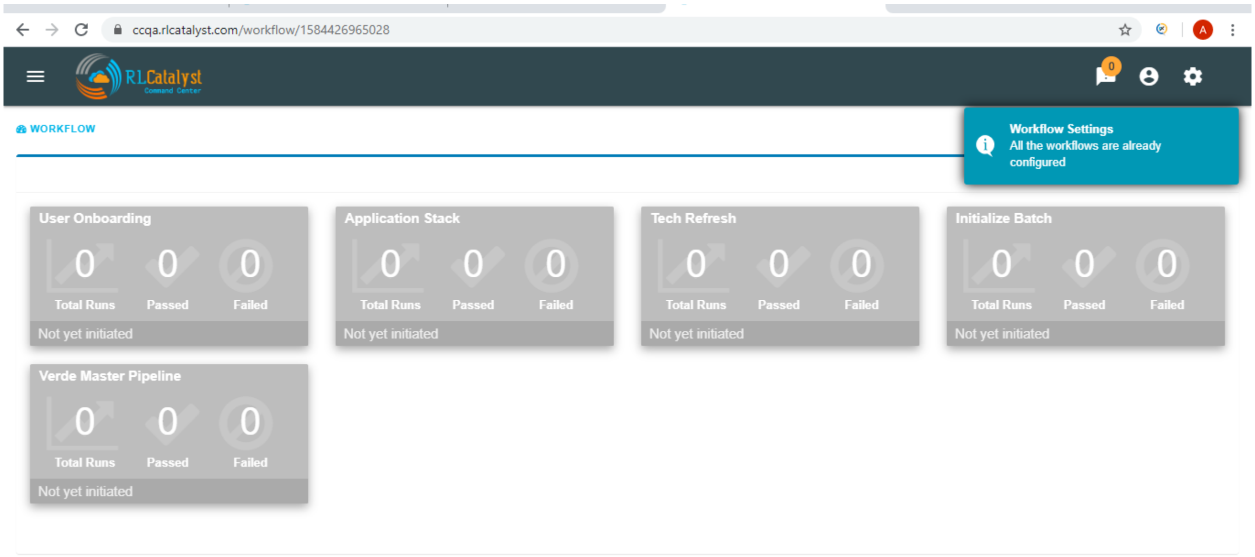
1 | Minutes

We can add the workflow from Workflow Settings tab on the Settings page. You can also edit or delete the workflow from the Workflow settings tab.



Name	Status Check Schedule	Created On	Action
Application Stack	Every 1-Minutes Once	Feb 14, 2020, 12:36:31 PM	✎ 🗑
User Onboarding	Every 1-Minutes Once	Feb 14, 2020, 12:36:05 PM	✎ 🗑

The RLCatalyst Command Center pulls the workflow details from the RLCatalyst Workflow Engine. Only those workflows which are added to the RLCatalyst Workflow Engine, will be available for addition through the “Add Workflow” screen. Once all workflows are added for monitoring, clicking the + button shows “All the workflows are already configured” message.



Workflow Settings
All the workflows are already configured

User Onboarding
0 Total Runs 0 Passed 0 Failed
Not yet initiated

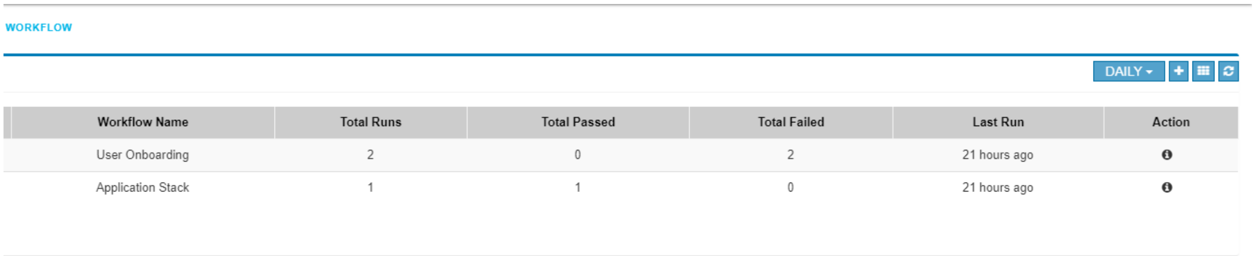
Application Stack
0 Total Runs 0 Passed 0 Failed
Not yet initiated

Tech Refresh
0 Total Runs 0 Passed 0 Failed
Not yet initiated

Initialize Batch
0 Total Runs 0 Passed 0 Failed
Not yet initiated

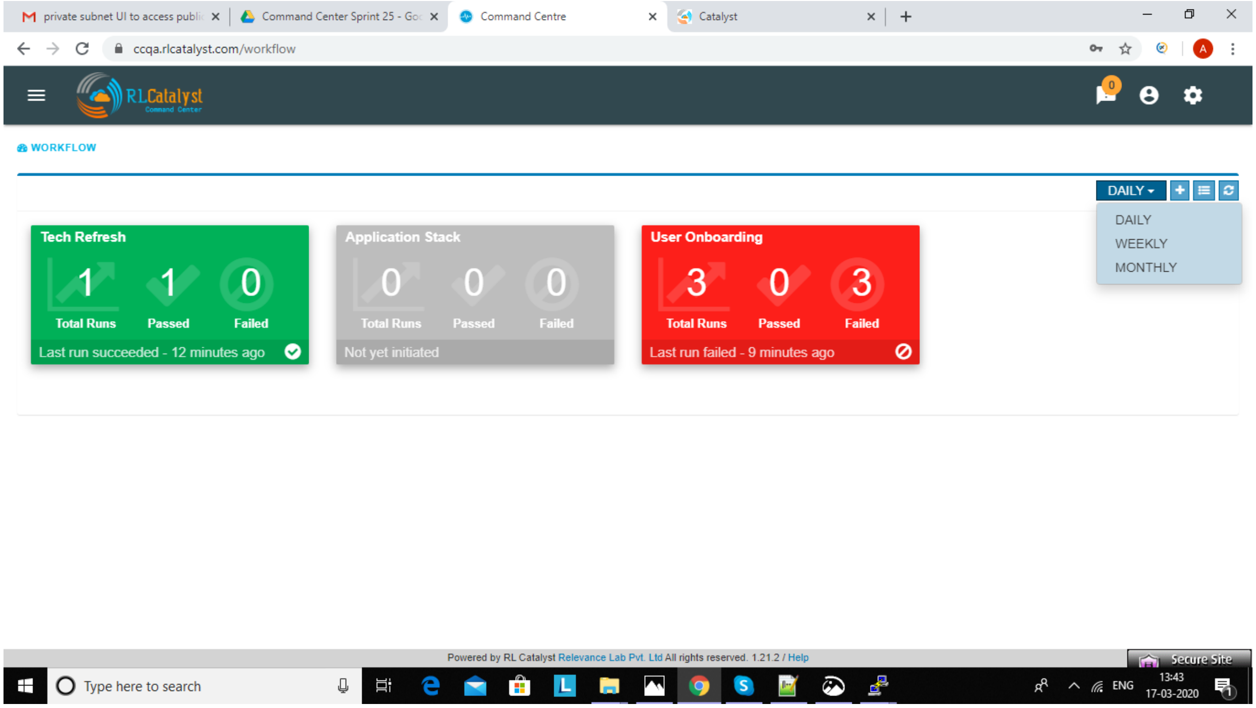
Verde Master Pipeline
0 Total Runs 0 Passed 0 Failed
Not yet initiated

In the workflow Monitoring page navigate to the top right menu there is option called ‘list view’,which shows added workflows are diaplyed in list view.



Workflow Name	Total Runs	Total Passed	Total Failed	Last Run	Action
User Onboarding	2	0	2	21 hours ago	ℹ
Application Stack	1	1	0	21 hours ago	ℹ

Filters for daily, weekly and monthly views are available on the workflow dashboard screen. Choosing “Daily” filter will show current date data. Similarly we can choose “Weekly” or “Monthly” filters to see the workflow metrics for corresponding periods.



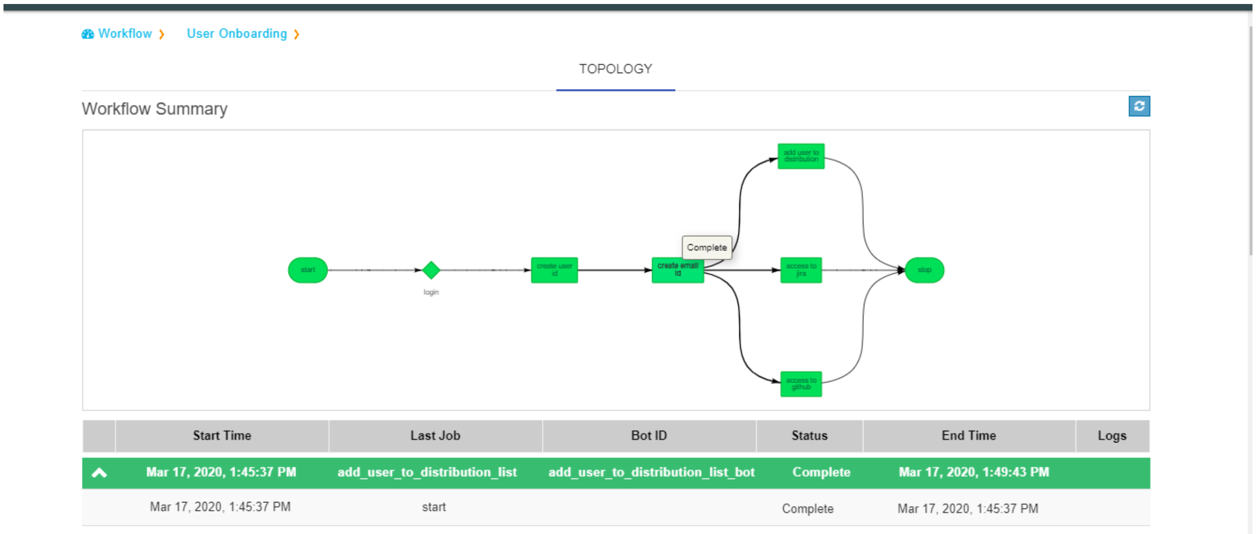
Last run succeeded - 12 minutes ago

Not yet initiated

Last run failed - 9 minutes ago

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.21.2 / Help

Clicking on a workflow card navigates to workflow details page. On this page the user can see the history of all the workflow runs. The top of the page shows the topology of the workflow run which has been selected from the table below it.When we click on the node see the status of node like tool-tip message.



	Start Time	Last Job	Bot ID	Status	End Time	Logs
^	Mar 17, 2020, 1:45:37 PM	add_user_to_distribution_list	add_user_to_distribution_list_bot	Complete	Mar 17, 2020, 1:49:43 PM	
	Mar 17, 2020, 1:45:37 PM	start		Complete	Mar 17, 2020, 1:45:37 PM	

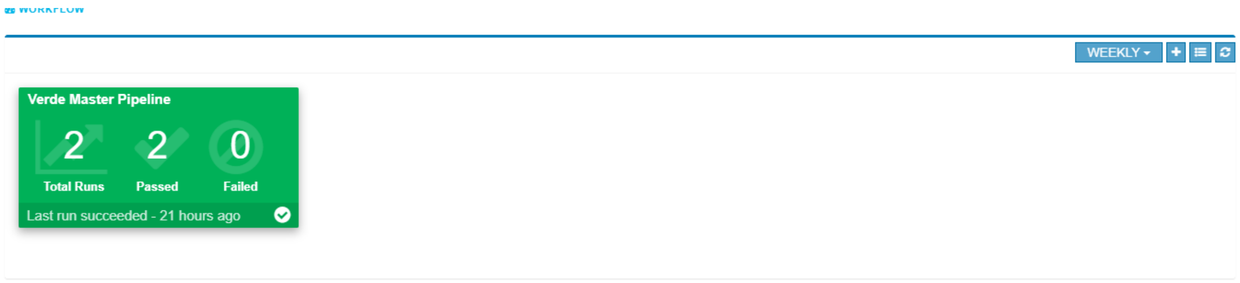
Workflow history details consists following data:

Start Time	Last Job	Bot ID | Status	End Time	Logs

There is 'i' button in the logs,which shows logs about BOTS.

We implemented colour codes for nodes and historical runs table:

A workflow run that completed successfully will show in green color in the table. In the topology view, each node that completed successfully will show in green color.



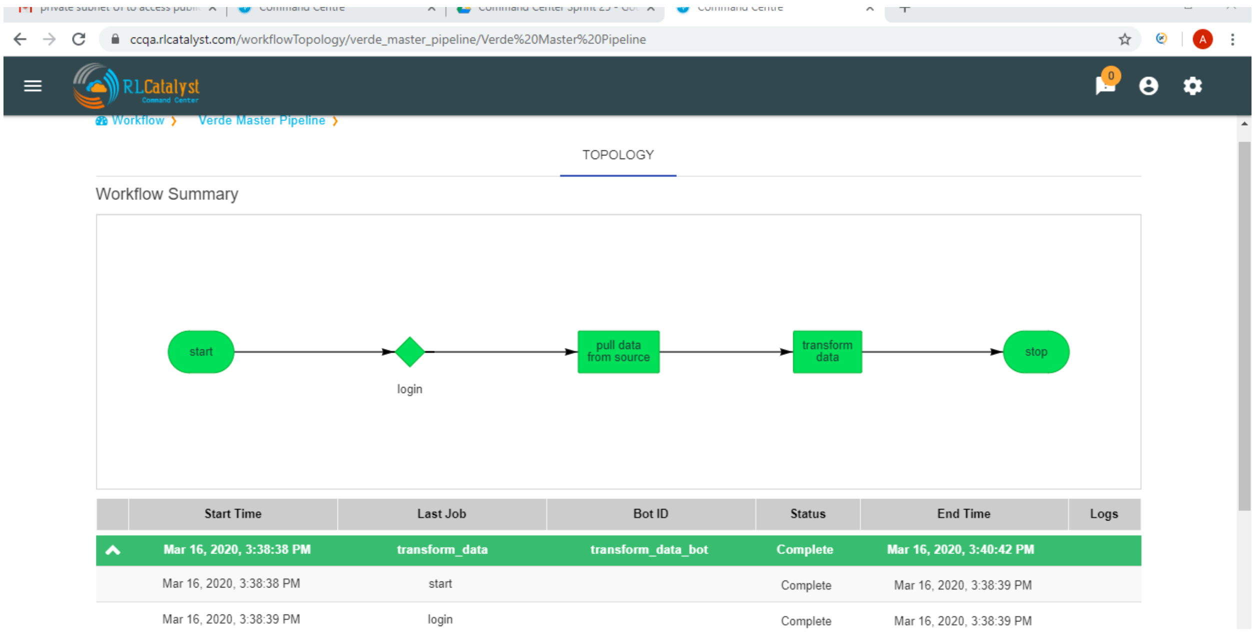
WORKFLOW

WEEKLY

Verde Master Pipeline

2	2	0
Total Runs	Passed	Failed

Last run succeeded - 21 hours ago



ccqa.rlcatalyst.com/workflowTopology/verde_master_pipeline/Verde%20Master%20Pipeline

RLCatalyst Command Center

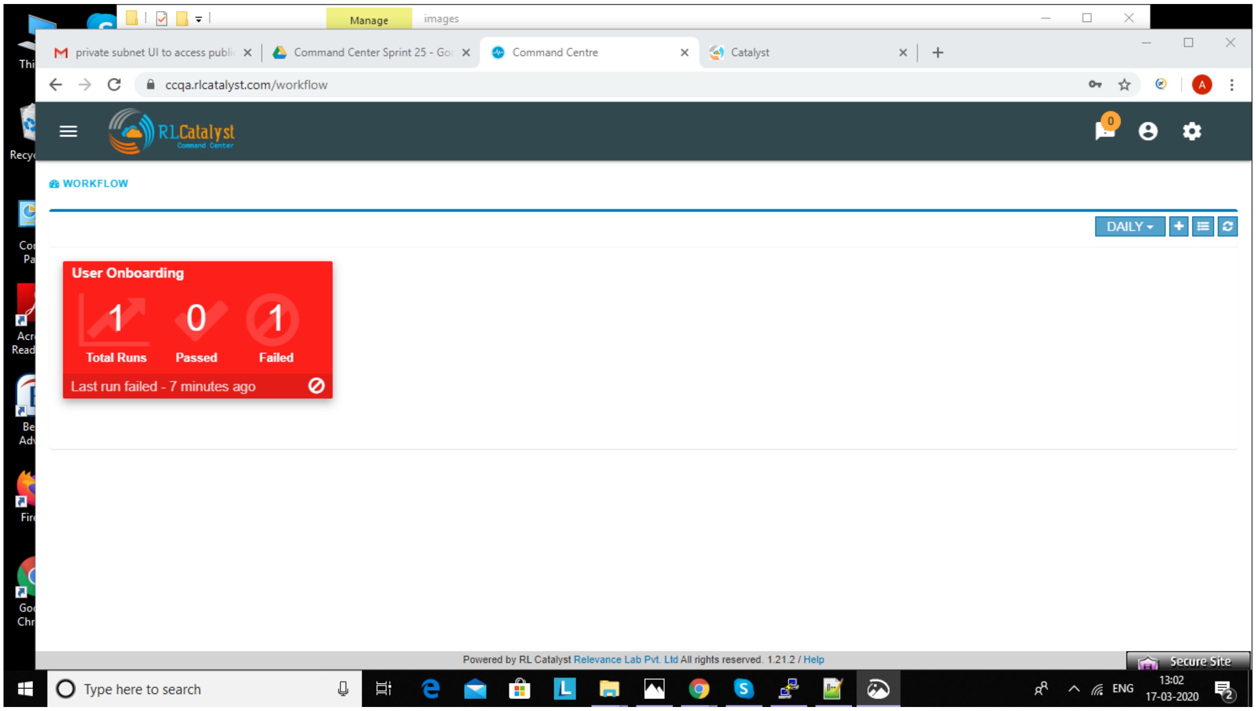
Workflow › Verde Master Pipeline ›

TOPOLOGY

Workflow Summary

	Start Time	Last Job	Bot ID	Status	End Time	Logs
^	Mar 16, 2020, 3:38:38 PM	transform_data	transform_data_bot	Complete	Mar 16, 2020, 3:40:42 PM	
	Mar 16, 2020, 3:38:38 PM	start		Complete	Mar 16, 2020, 3:38:39 PM	
	Mar 16, 2020, 3:38:39 PM	login		Complete	Mar 16, 2020, 3:38:39 PM	

A workflow run that completed with an error will show in red color in the table. In the topology view, the node which completed with error (and all following nodes) will show in terminated status with dark red color. On failure of a workflow run, an e-mail notification will be sent out to the contacts specified in the “Add workflow” screen.

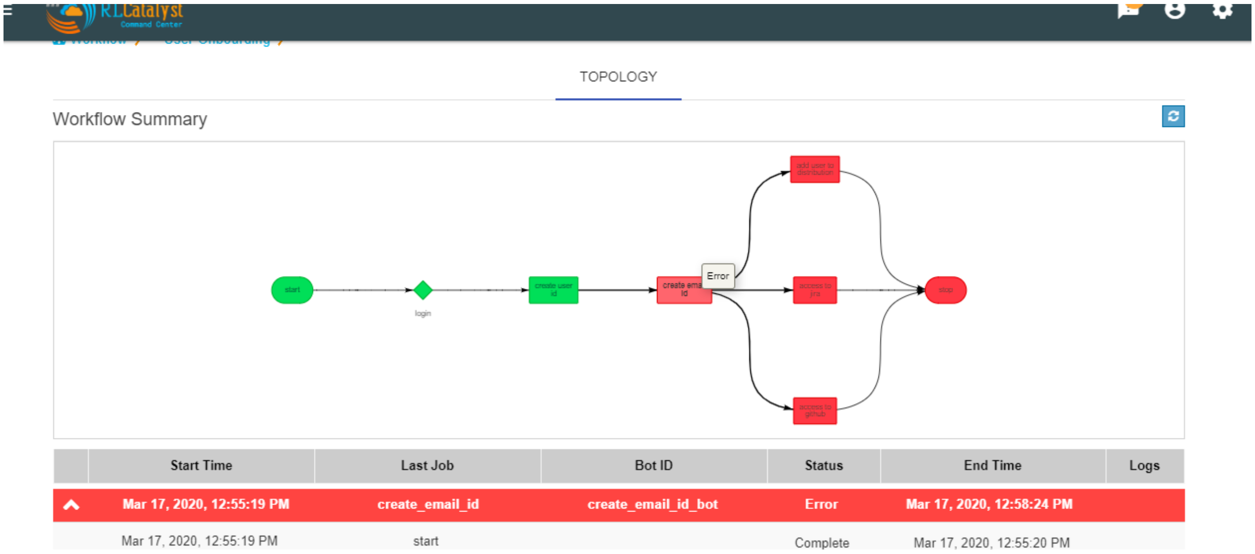

private subnet UI to access publi
Command Center Sprint 25 - Go
Command Centre
Catalyst
ccqa.rlcatalyst.com/workflow
RLCatalyst Command Center
WORKFLOW
DAILY
Type here to search
ENG
13:02
17-03-2020
Secure Site

User Onboarding

1 Total Runs | 0 Passed | 1 Failed

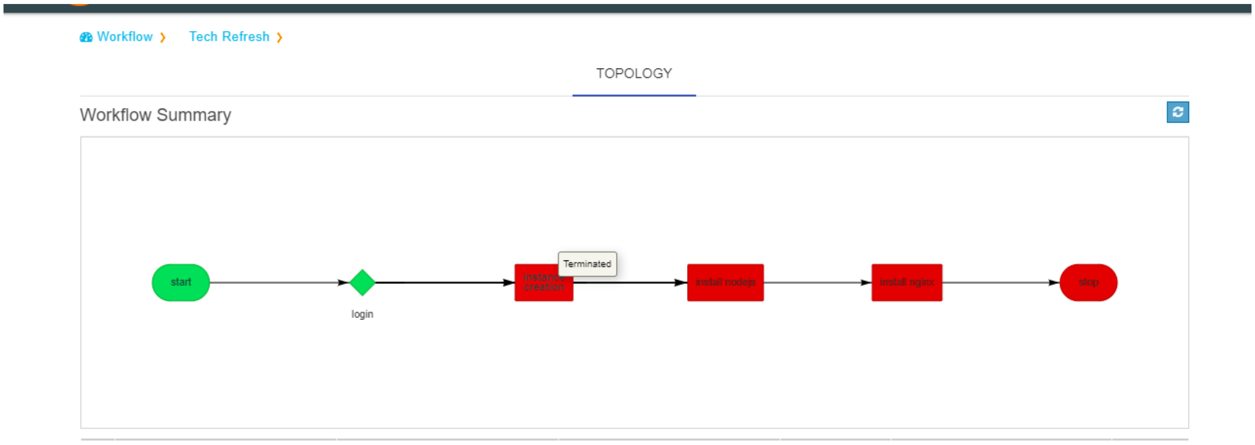
Last run failed - 7 minutes ago

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.21.2 / Help



Workflow Summary

	Start Time	Last Job	Bot ID	Status	End Time	Logs
^	Mar 17, 2020, 12:55:19 PM	create_email_id	create_email_id_bot	Error	Mar 17, 2020, 12:58:24 PM	
	Mar 17, 2020, 12:55:19 PM	start		Complete	Mar 17, 2020, 12:55:20 PM	

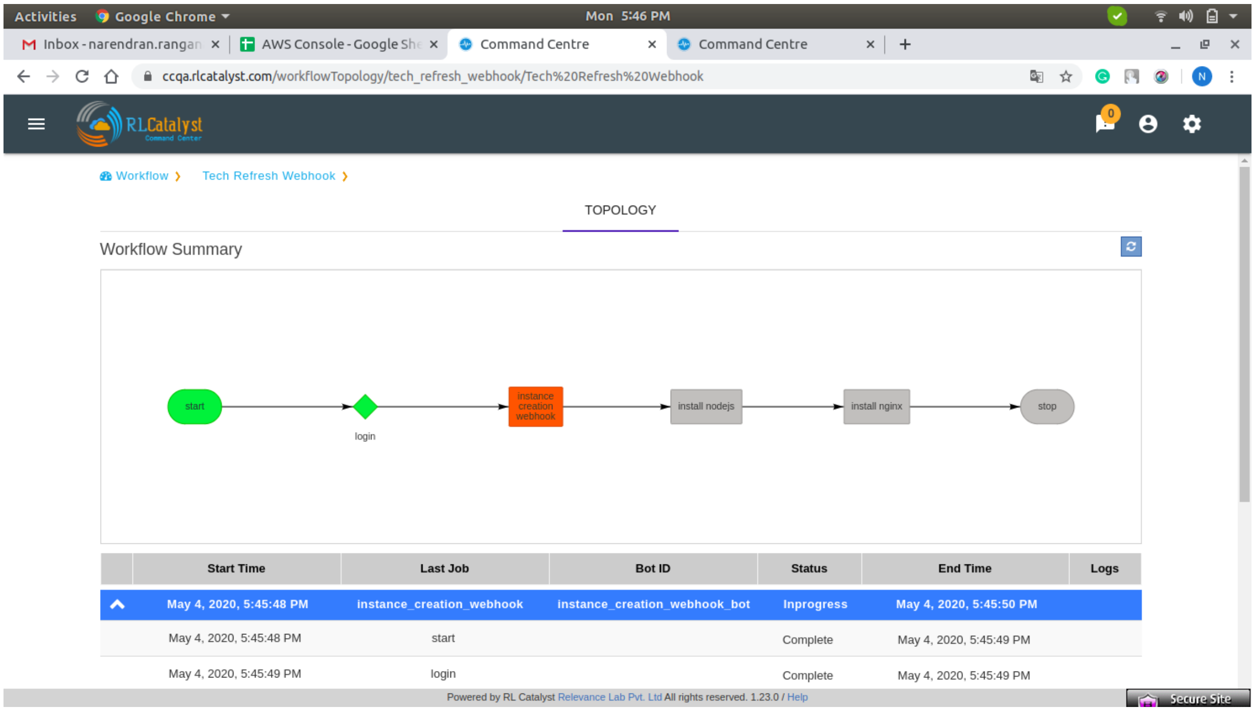


Workflow Summary

A workfow run is in processing user should also cancelled the workflow.In the topology view, the node which completed with cancelled will show in dark green color

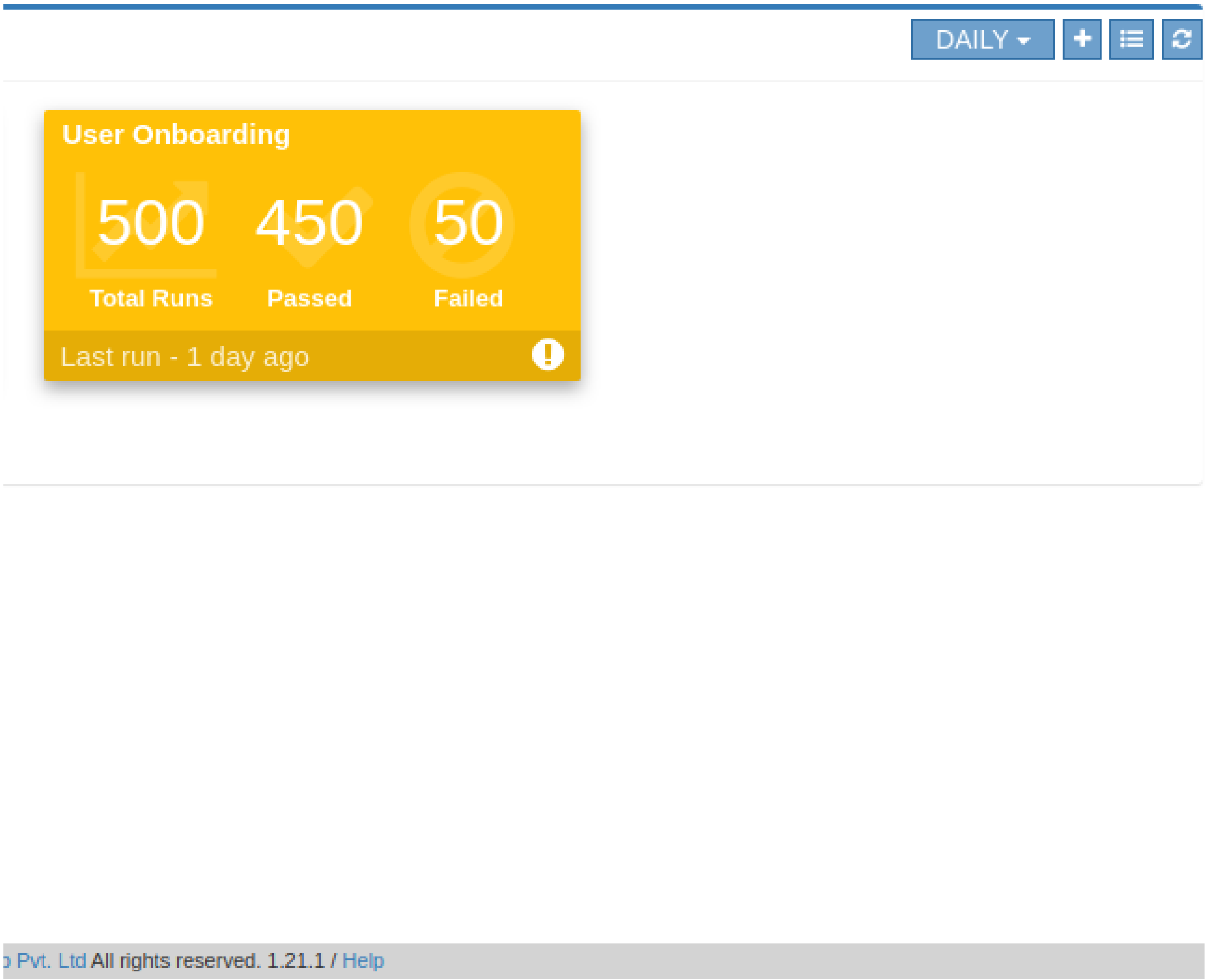
images/Cancelled.PNG

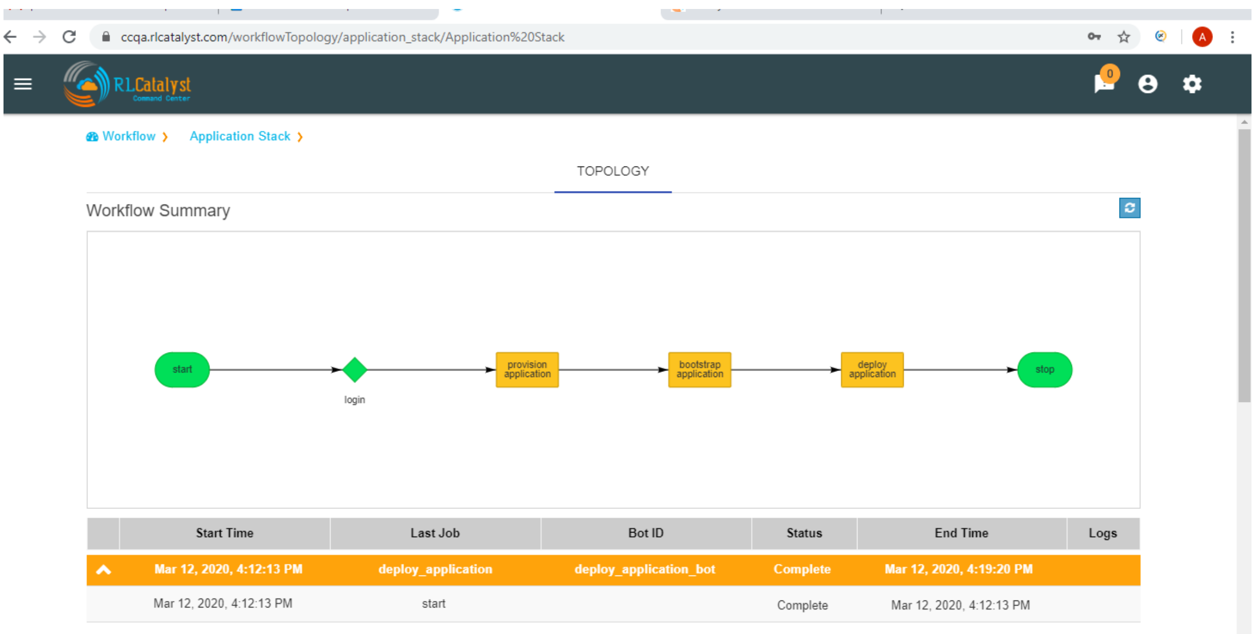
When workflow run is inprocessing due to database connectivity or crash happened.In the topology view, it will shows pause with orange color after some time automatically it will restarts the workflow



	Start Time	Last Job	Bot ID	Status	End Time	Logs
^	May 4, 2020, 5:45:48 PM	instance_creation_webhook	instance_creation_webhook_bot	Inprogress	May 4, 2020, 5:45:50 PM	
	May 4, 2020, 5:45:48 PM	start		Complete	May 4, 2020, 5:45:49 PM	
	May 4, 2020, 5:45:49 PM	login		Complete	May 4, 2020, 5:45:49 PM	

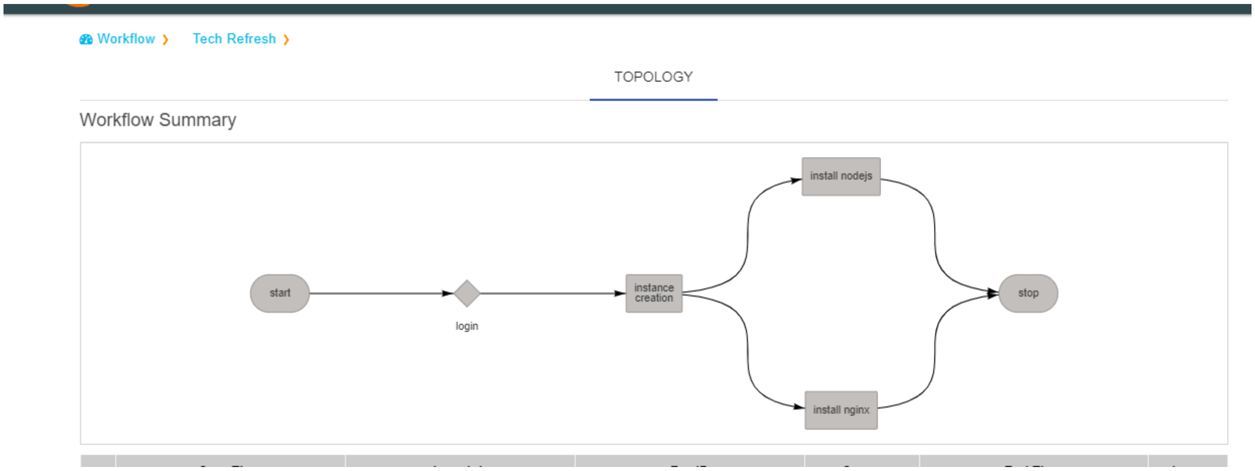
A workflow run that is delayed beyond the threshold defined in the RLCatalyst Workflow Engine will show in yellow color. In the topology view, the node which is delayed will show in yellow color. When a node execution is delayed beyond its threshold, an e-mail notification will be sent out to the contacts specified in the "Add workflow" screen.





	Start Time	Last Job	Bot ID	Status	End Time	Logs
^	Mar 12, 2020, 4:12:13 PM	deploy_application	deploy_application_bot	Complete	Mar 12, 2020, 4:19:20 PM	
	Mar 12, 2020, 4:12:13 PM	start		Complete	Mar 12, 2020, 4:12:13 PM	

When there is not history of workflow runs, all the nodes in the topology section will be shown in gray color.

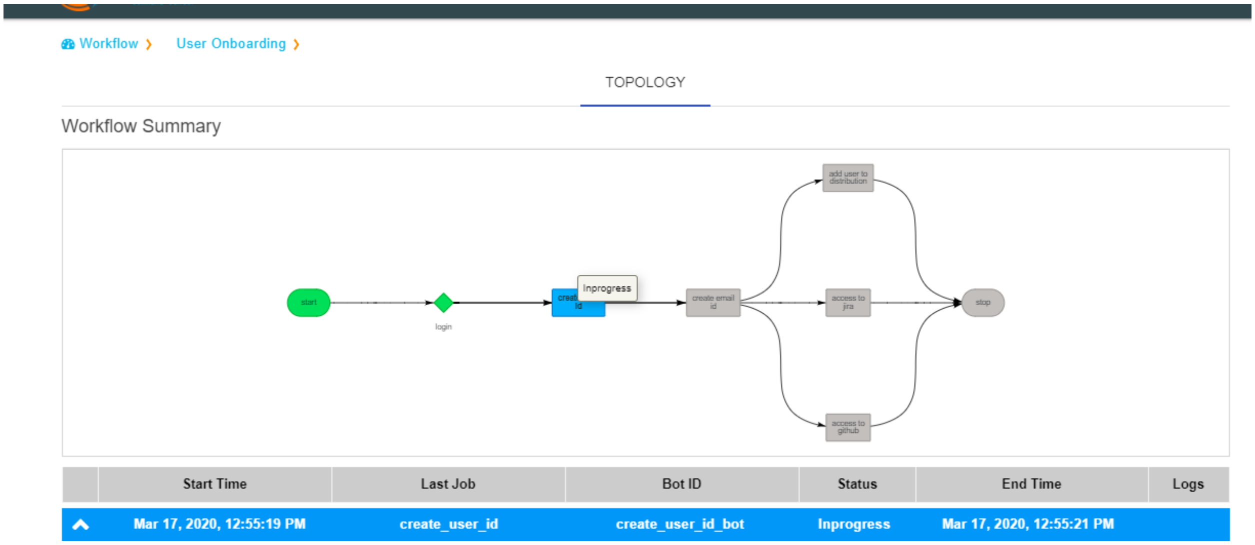


Workflow ❯ Tech Refresh ❯

TOPOLOGY

Workflow Summary

When a node is in progress, the color of the node in topology view will be shown in blue color.



Workflow ❯ User Onboarding ❯

TOPOLOGY

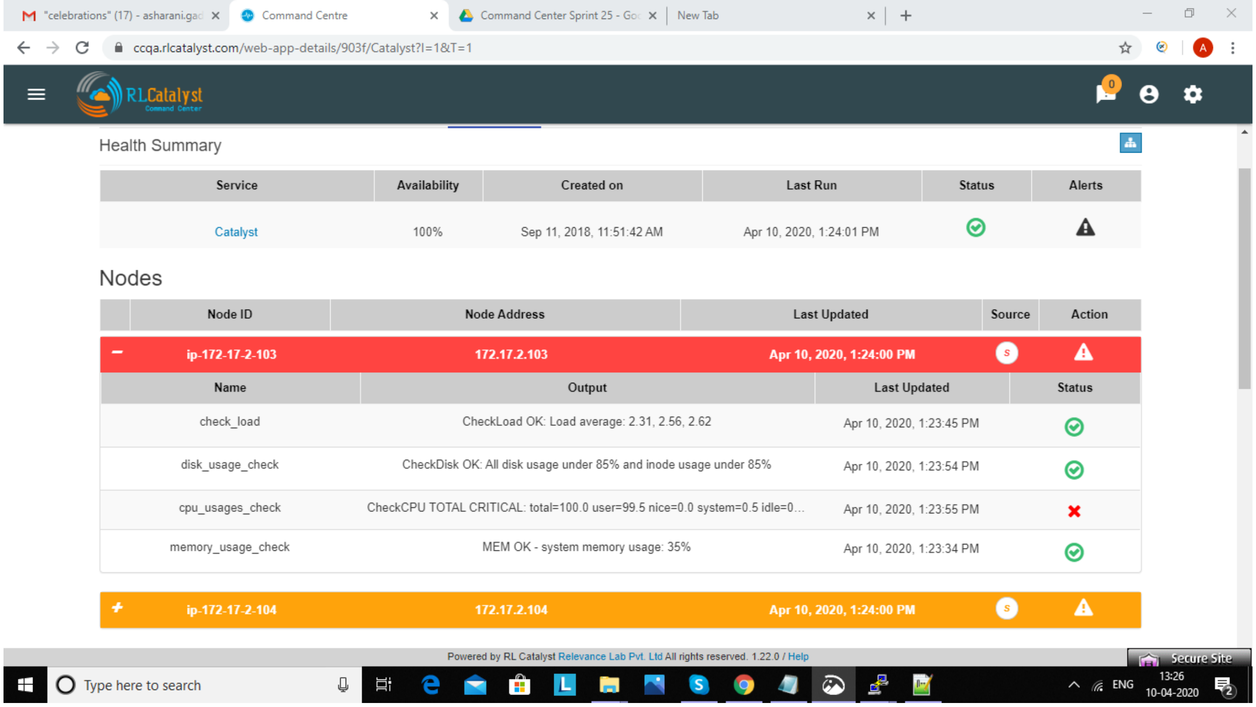
Workflow Summary

	Start Time	Last Job	Bot ID	Status	End Time	Logs
^	Mar 17, 2020, 12:55:19 PM	create_user_id	create_user_id_bot	Inprogress	Mar 17, 2020, 12:55:21 PM	

1.4.23 Analytics Page For CPU Metric

It focuses on visualizing the data that we have in ELK(Elastic logstash Kibana) stack, providing analytical recommendations to the users, for detecting the anomalies . We improved this feature for CPU Metric. It consists Visualize,Advanced analytics,Anomaly Detection tabs.

Navigating to analytics page is choose any BSM which leads to health summary details there you can see nodes information.If warning or error alert triggered for cpu_usages_check . We should see "info" icon in status . It navigactes the user to analytics page.If tenant has ELK based configuration than only we should navigated to analytics page.


"celebrations" (17) - asharani.gac
Command Centre
Command Center Sprint 25 - Goo
New Tab
ccqa.rlcatalyst.com/web-app-details/903f/Catalyst?I=1&T=1
RLCatalyst
Command Center
0
Type here to search
ENG
13:26
10-04-2020
Secure Site

Health Summary

Service	Availability	Created on	Last Run	Status	Alerts
Catalyst	100%	Sep 11, 2018, 11:51:42 AM	Apr 10, 2020, 1:24:01 PM	✓	⚠

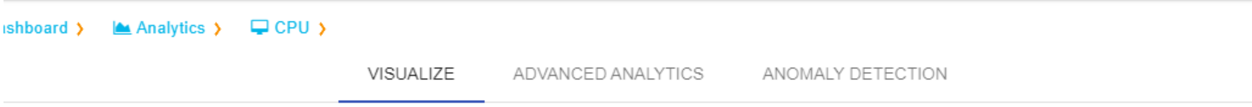
Nodes

	Node ID	Node Address	Last Updated	Source	Action
−	ip-172-17-2-103	172.17.2.103	Apr 10, 2020, 1:24:00 PM	s	⚠

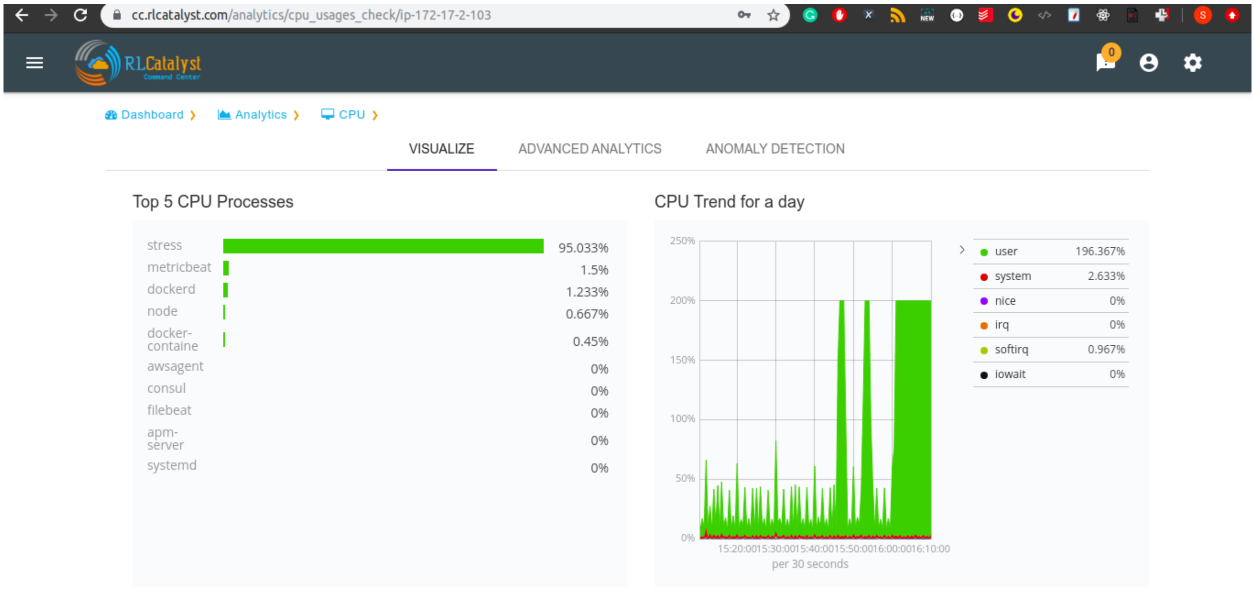
Name	Output	Last Updated	Status
check_load	CheckLoad OK: Load average: 2.31, 2.56, 2.62	Apr 10, 2020, 1:23:45 PM	✓
disk_usage_check	CheckDisk OK: All disk usage under 85% and inode usage under 85%	Apr 10, 2020, 1:23:54 PM	✓
cpu_usages_check	CheckCPU TOTAL CRITICAL: total=100.0 user=99.5 nice=0.0 system=0.5 idle=0...	Apr 10, 2020, 1:23:55 PM	✗
memory_usage_check	MEM OK - system memory usage: 35%	Apr 10, 2020, 1:23:34 PM	✓

	Node ID	Node Address	Last Updated	Source	Action
+	ip-172-17-2-104	172.17.2.104	Apr 10, 2020, 1:24:00 PM	s	⚠

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.22.0 / Help

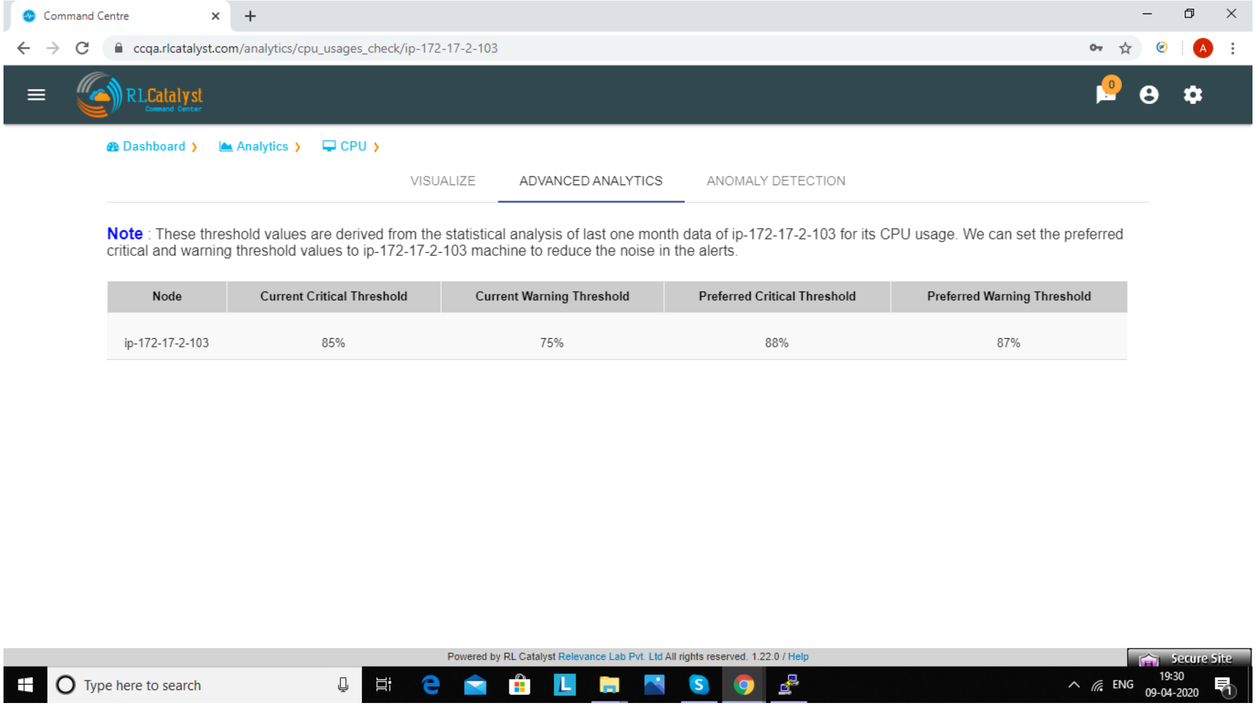


In analytics page we can see visualize tab.It shows top 5 CPU processes whose consume more CPU with percentages and CPU trend for a day in graph model.



In analytics page we can see Advanced Analytics tab.Here threshold values are derived from the statistical analysis of last one month CPU_usage data of particular node. Based on the threshold values we can reduce the noise in the alerts.It will show proper threshold values for CPU metric of a machine in a table format

Node	Current critical Threshold	Current Warning Threshold	Preferred Current Threshold	Preferred Warning Threshold

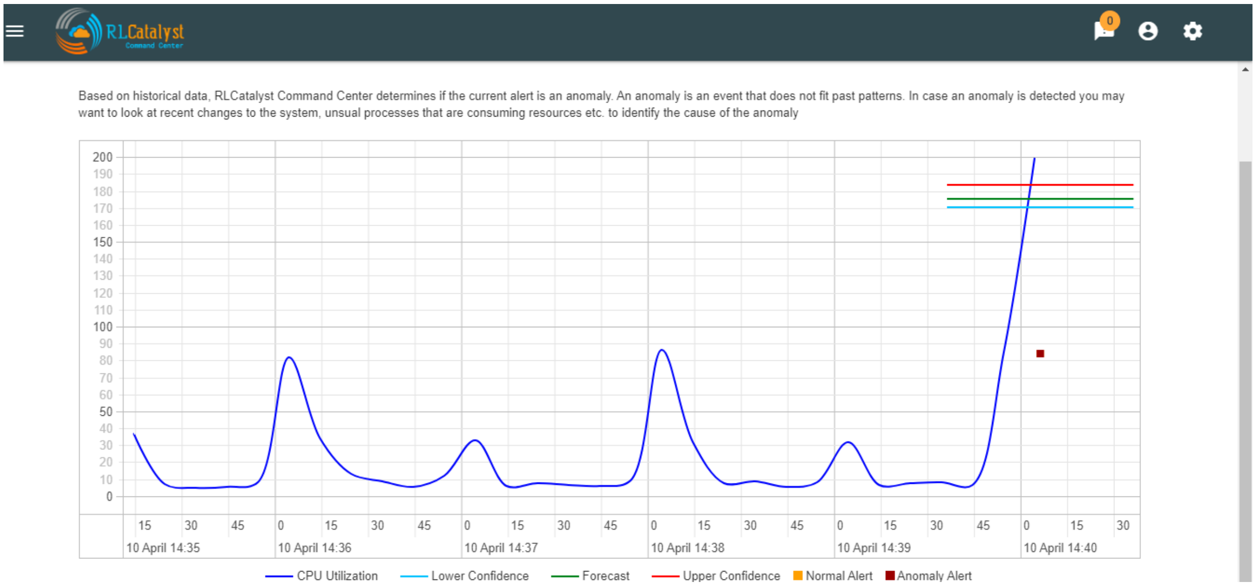


Note : These threshold values are derived from the statistical analysis of last one month data of ip-172-17-2-103 for its CPU usage. We can set the preferred critical and warning threshold values to ip-172-17-2-103 machine to reduce the noise in the alerts.

Node	Current Critical Threshold	Current Warning Threshold	Preferred Critical Threshold	Preferred Warning Threshold
ip-172-17-2-103	85%	75%	88%	87%

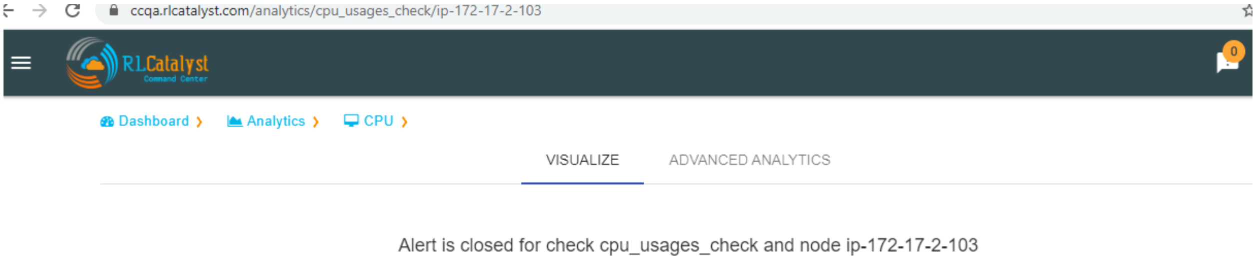
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.22.0 / Help
Secure Site
Type here to search
ENG
19:30
09-04-2020

In analytics page we can see Anomaly detection tab.Based on historical data, RLCatalyst Command Center determines if the current alert is an anomaly. An anomaly is an event that does not fit past patterns. In case an anomaly is detected you may want to look at recent changes to the system, unsual processes that are consuming resources etc. to identify the cause of the anomaly



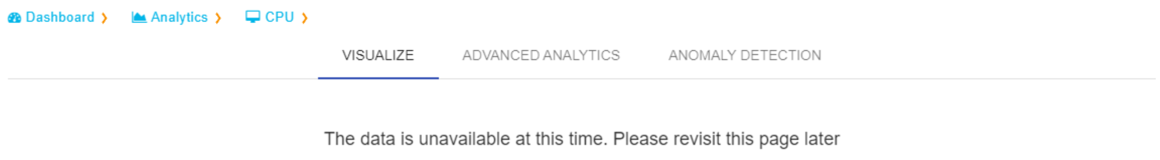
Based on historical data, RLCatalyst Command Center determines if the current alert is an anomaly. An anomaly is an event that does not fit past patterns. In case an anomaly is detected you may want to look at recent changes to the system, unsual processes that are consuming resources etc. to identify the cause of the anomaly

If alert is already resolved than we should see the message like “Alert is closed for check cpu_usages_check and node ip”



Alert is closed for check cpu_usages_check and node ip-172-17-2-103

If server is down it shows meassage to user i.e.,”The data is unavailable at this time.please revisit this page later”.

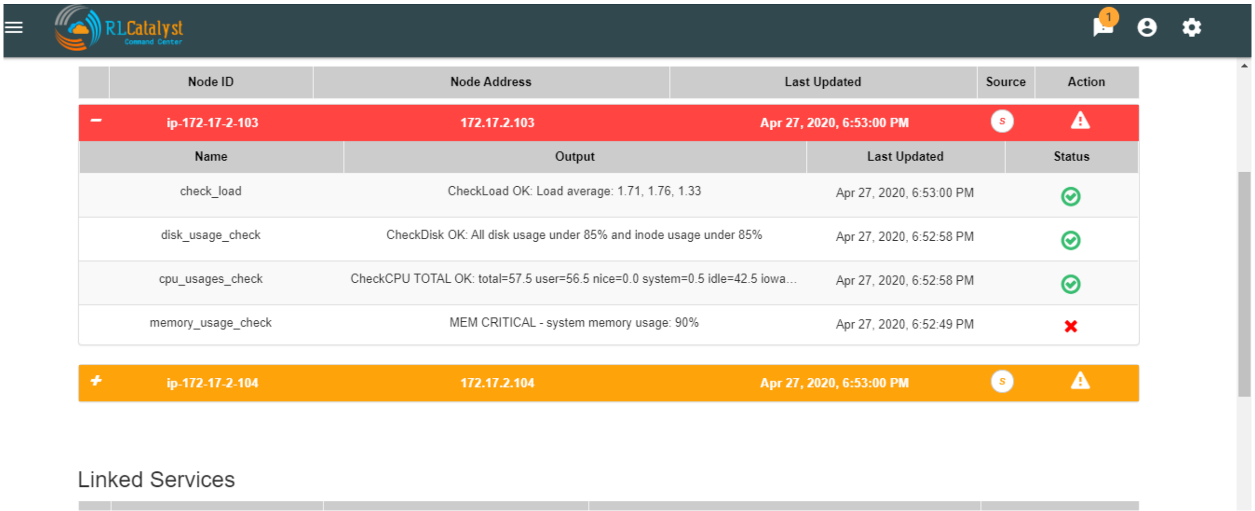


The data is unavailable at this time. Please revisit this page later

1.4.24 Analytics Page For MEMORY Metric

It focuses on visualizing the data that we have in ELK(Elastic logstash Kibana) stack, providing analytical recommendations to the users, for detecting the anomalies . It consists Visualize,Advanced analytics tabs.

Navigating to analytics page is choose any BSM which leads to health summary details there you can see nodes information.If warning or error alert triggered for Memory_usages_check we should see "info" icon in status . It navigactes the user to analytics page.If tenant has ELK based configuration than only we should navigated to analytics page.

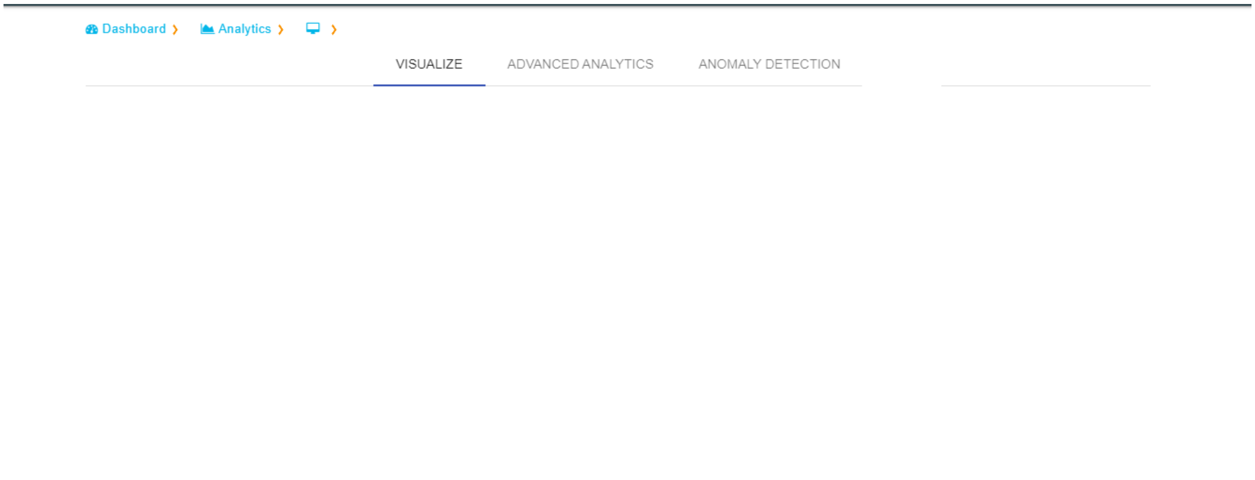


	Node ID	Node Address	Last Updated	Source	Action
−	ip-172-17-2-103	172.17.2.103	Apr 27, 2020, 6:53:00 PM	S	⚠

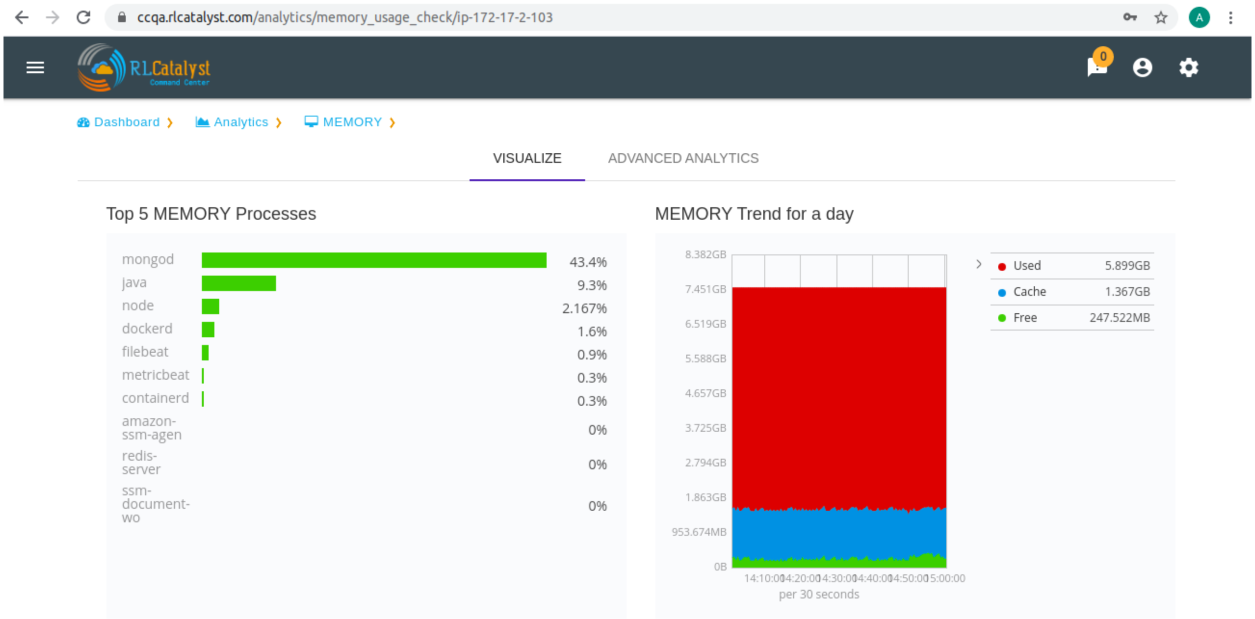
Name	Output	Last Updated	Status
check_load	CheckLoad OK: Load average: 1.71, 1.76, 1.33	Apr 27, 2020, 6:53:00 PM	✓
disk_usage_check	CheckDisk OK: All disk usage under 85% and inode usage under 85%	Apr 27, 2020, 6:52:58 PM	✓
cpu_usages_check	CheckCPU TOTAL OK: total=57.5 user=56.5 nice=0.0 system=0.5 idle=42.5 iowa...	Apr 27, 2020, 6:52:58 PM	✓
memory_usage_check	MEM CRITICAL - system memory usage: 90%	Apr 27, 2020, 6:52:49 PM	✖

+	ip-172-17-2-104	172.17.2.104	Apr 27, 2020, 6:53:00 PM	S	⚠

Linked Services

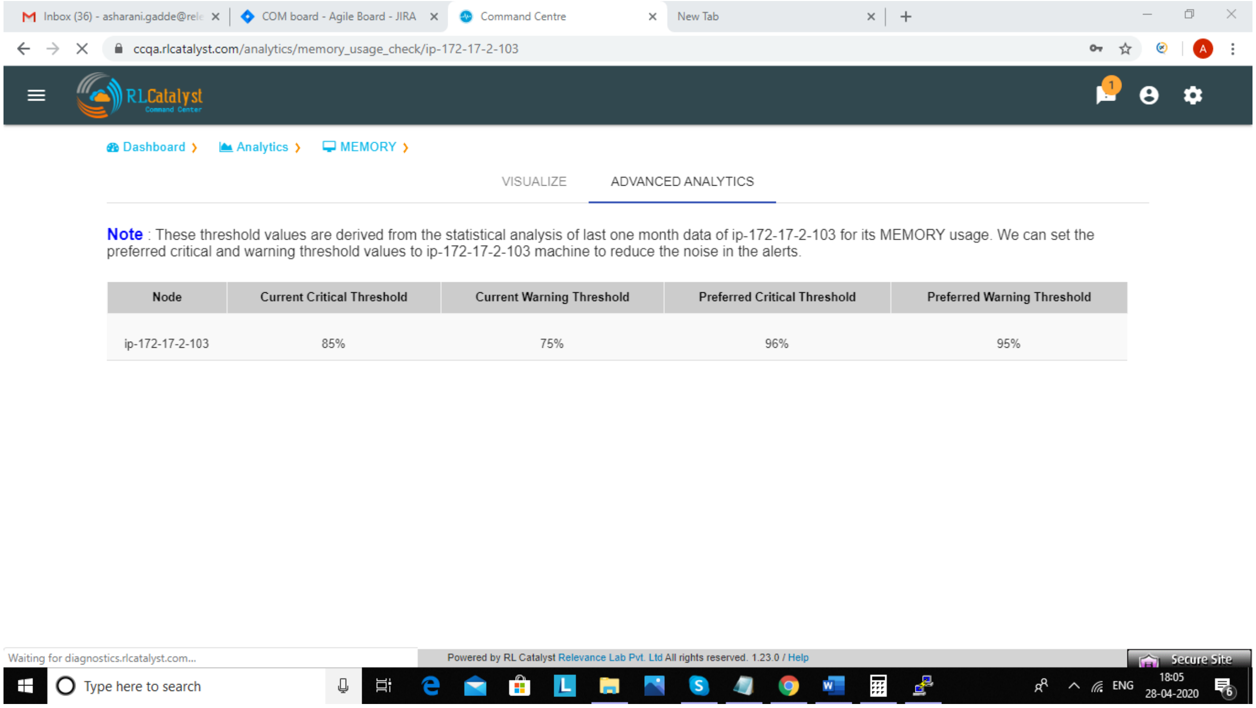


In analytics page we can see visualize tab.It shows top 5 MEMORY processes and MEMORY trend for a day i.e., we can see cache data,free data and used data.



In analytics page we can see Advanced Analytics tab.Here threshold values are derived from the statistical analysis of last one month MEMORY_usage data of particular node. Based on the threshold values we can reduce the noise in the alerts.It will show proper threshold values for MEMORY metric of a machine in a table format

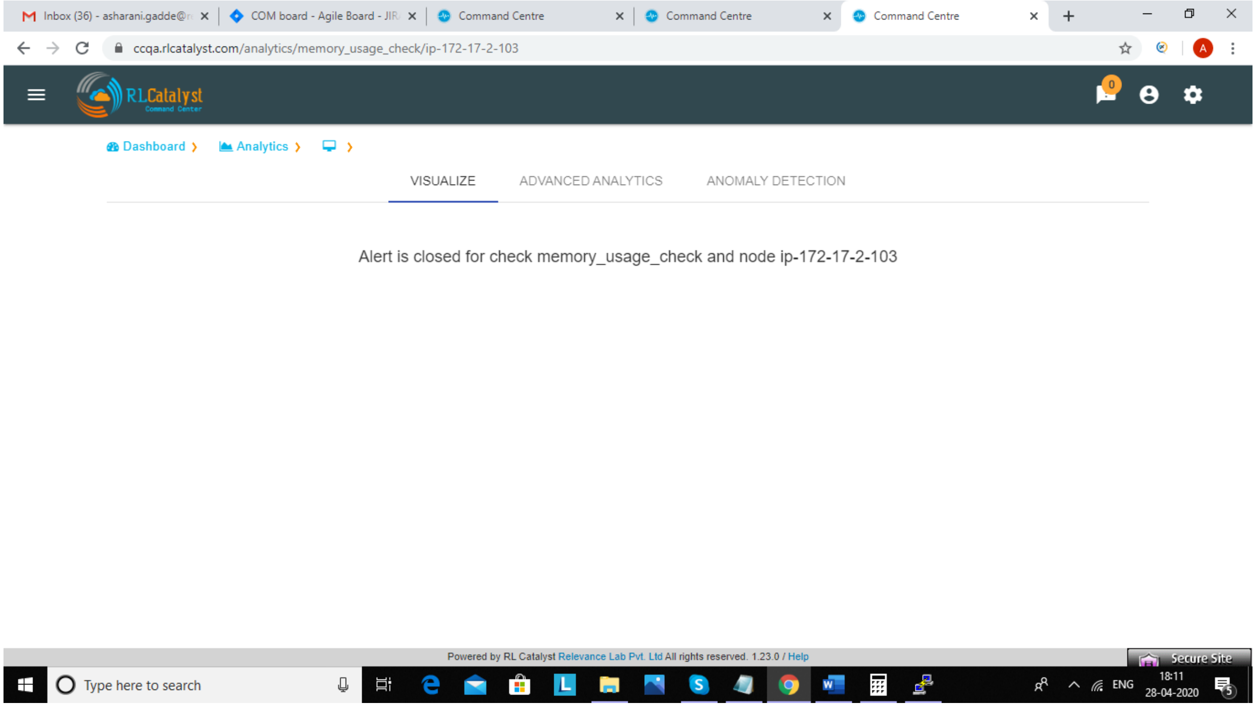
Node	Current critical Threshold	Current Warning Threshold	Preferred Current Threshold	Preferred Warning Threshold


ccqa.rlcatalyst.com/analytics/memory_usage_check/ip-172-17-2-103
RLCatalyst
Dashboard › Analytics › MEMORY ›
VISUALIZE
ADVANCED ANALYTICS
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.23.0 / Help

Note : These threshold values are derived from the statistical analysis of last one month data of ip-172-17-2-103 for its MEMORY usage. We can set the preferred critical and warning threshold values to ip-172-17-2-103 machine to reduce the noise in the alerts.

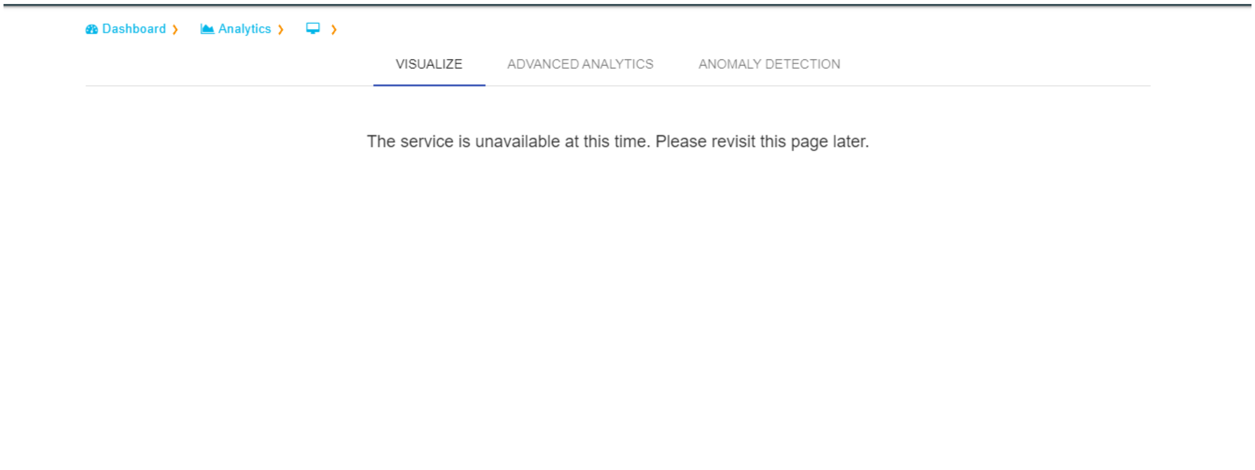
Node	Current Critical Threshold	Current Warning Threshold	Preferred Critical Threshold	Preferred Warning Threshold
ip-172-17-2-103	85%	75%	96%	95%

If alert is already resolved than we should see the message like "Alert is closed for check Memory_usages_check and node ip"


ccqa.rlcatalyst.com/analytics/memory_usage_check/ip-172-17-2-103
RLCatalyst
Dashboard › Analytics › ›
VISUALIZE
ADVANCED ANALYTICS
ANOMALY DETECTION
Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.23.0 / Help

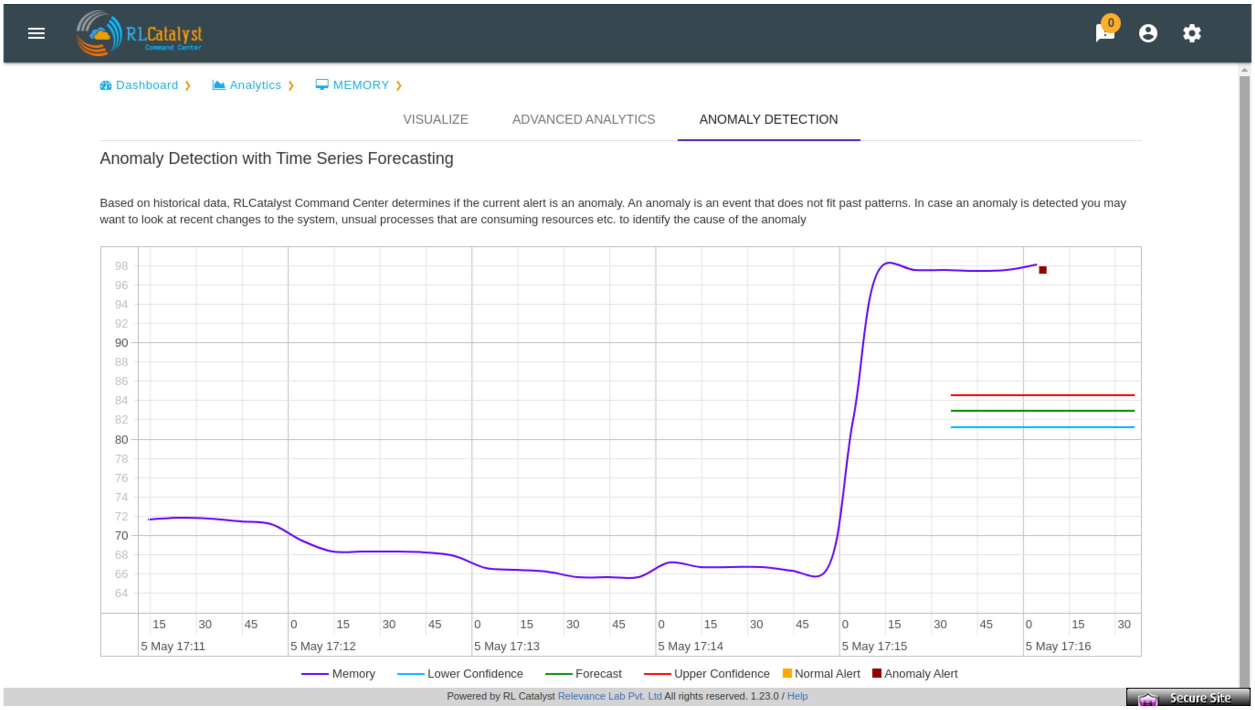
Alert is closed for check memory_usage_check and node ip-172-17-2-103

If server is down it shows meassage to user i.e.,"The data is unavailable at this time.please revisit this page later".



The service is unavailable at this time. Please revisit this page later.

In analytics page we can see Anomaly detection tab.Based on historical data, RLCatalyst Command Center determines if the current alert is an anomaly. An anomaly is an event that does not fit past patterns. In case an anomaly is detected you may want to look at recent changes to the system, unusual processes that are consuming resources .



Anomaly Detection with Time Series Forecasting

Based on historical data, RLCatalyst Command Center determines if the current alert is an anomaly. An anomaly is an event that does not fit past patterns. In case an anomaly is detected you may want to look at recent changes to the system, unsual processes that are consuming resources etc. to identify the cause of the anomaly

Powered by RL Catalyst Relevance Lab Pvt. Ltd All rights reserved. 1.23.0 / Help

1.5 Appendix A

Download the below Data Collection template by clicking on the following link .. _a link: https://s3.us-east-2.amazonaws.com/rlcatalyst/templates/CommandCenter_DataCollectionTemplate.xlsx

Registration Information	
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 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	Email ID which will be verified by the system during registration. Ensure you have access to this e-mail ID during registration
Provider Settings	
Will an Amazon Web Services account be configured for this tenant?	
AWS Access Key	
AWS Secret Key	
AWS Region for this account	
AWS Account Number	
Will a Microsoft Azure account be configured for this tenant?	
Azure Client ID	
Azure Client Secret	
Subscription ID	
Tenant ID	
Will a ServiceNow account be configured for this tenant?	
Host	
User Name	
Password	
Will a Sensu account be configured for this tenant?	
Host	
User Name	
Password	
Business Services	
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>