

Cloud Pak for Multicloud Management

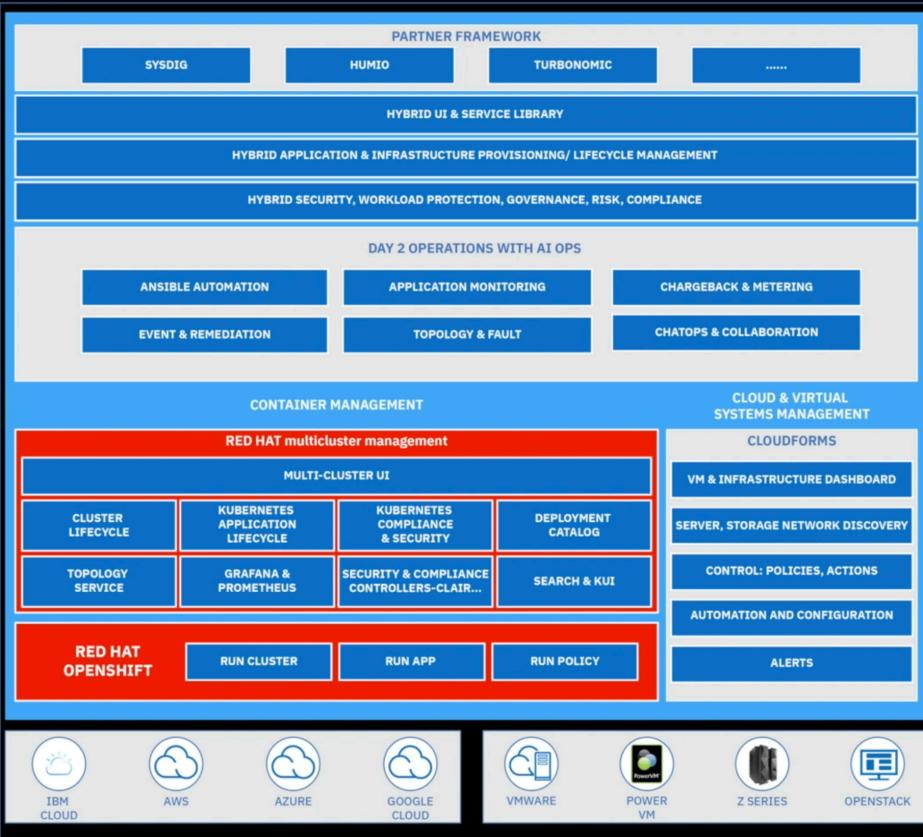
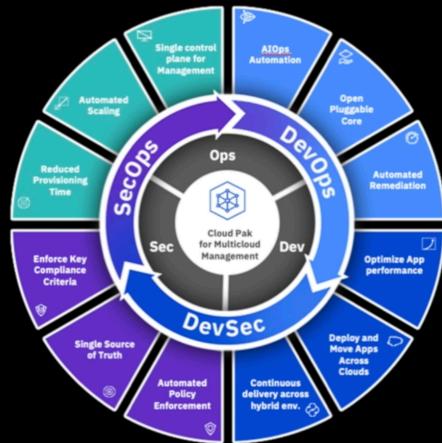
IBM Cloud Event Management

Consolidated operational event and incident correlation, prioritization and resolution in the cloud



IBM Cloud Pak for Multicloud Management

Reference Architecture



Digital transformation and disrupted work environments require enterprise IT organizations to:

- Adopt new tools and practices to make the most of their legacy and new tool sets
- Facilitate operational excellence and rapid innovation
- Build a harmonious workflow between their devops, line-of-business and central operations teams.



Inundation, indecision and delays

Too many alerts



Noisy
monitors



Change
alerts



Production
outages



Performance
slowdowns



Multiple
service tickets



Build
failures



Fix failures



App function
failures



Network
outages



Security
alerts

50%

of ownership and usage of
operations practices and tools are
outside of IT Operations*
50%

Indecision and confusion



40%

cite lack of collaboration between
Development & Operations as a
top inhibitor of innovation*

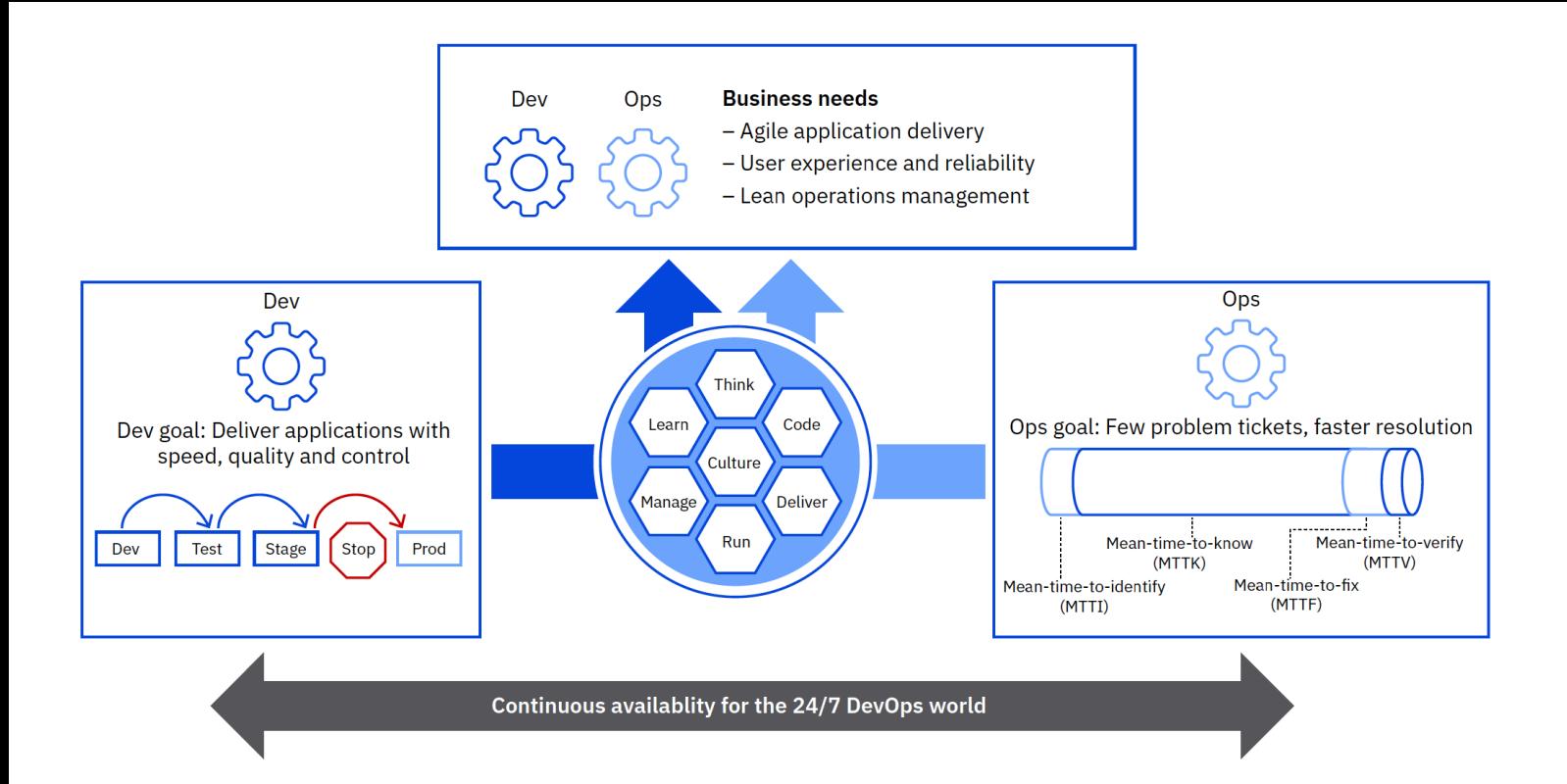
Long resolution time



50%

of apps running in cloud
environments will be considered
mission-critical by 2020*

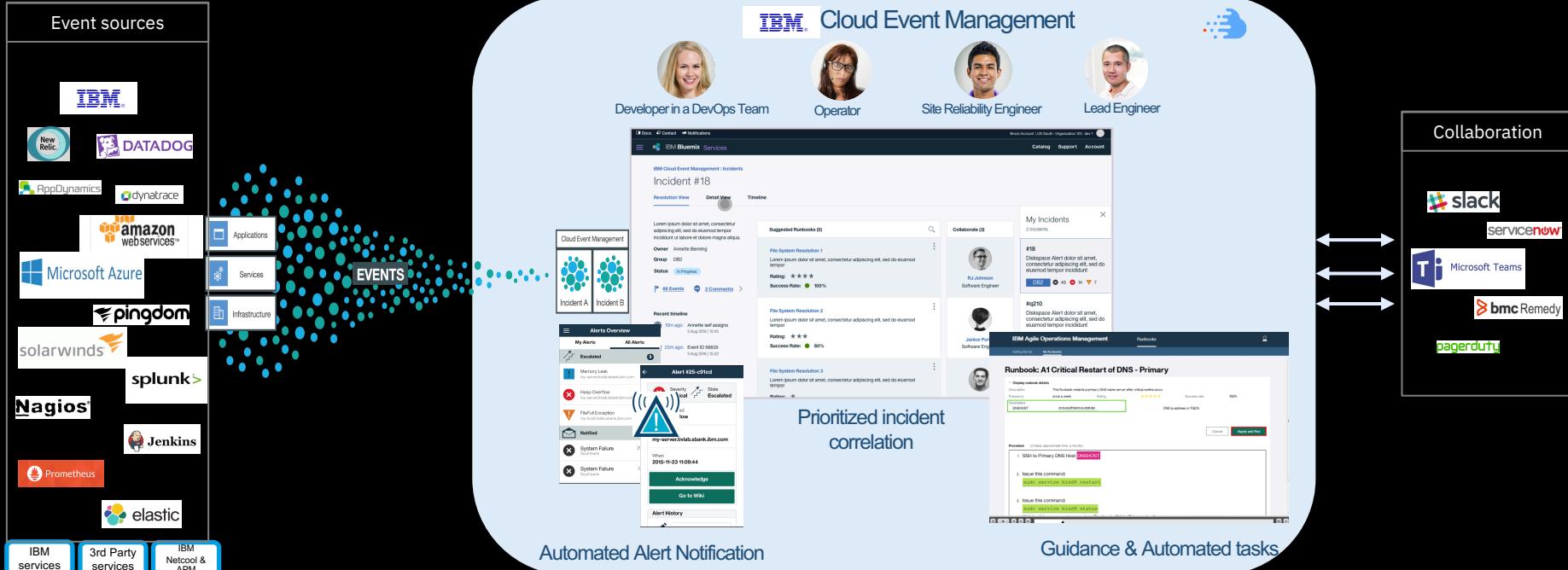
Digital Transformation Drives Organizations' Need To Reconcile Processes & Culture



IBM Cloud Event Management

Cut through alarm noise. Restore service fast.

Cloud-native, consolidated operational event and incident correlation, prioritization and resolution



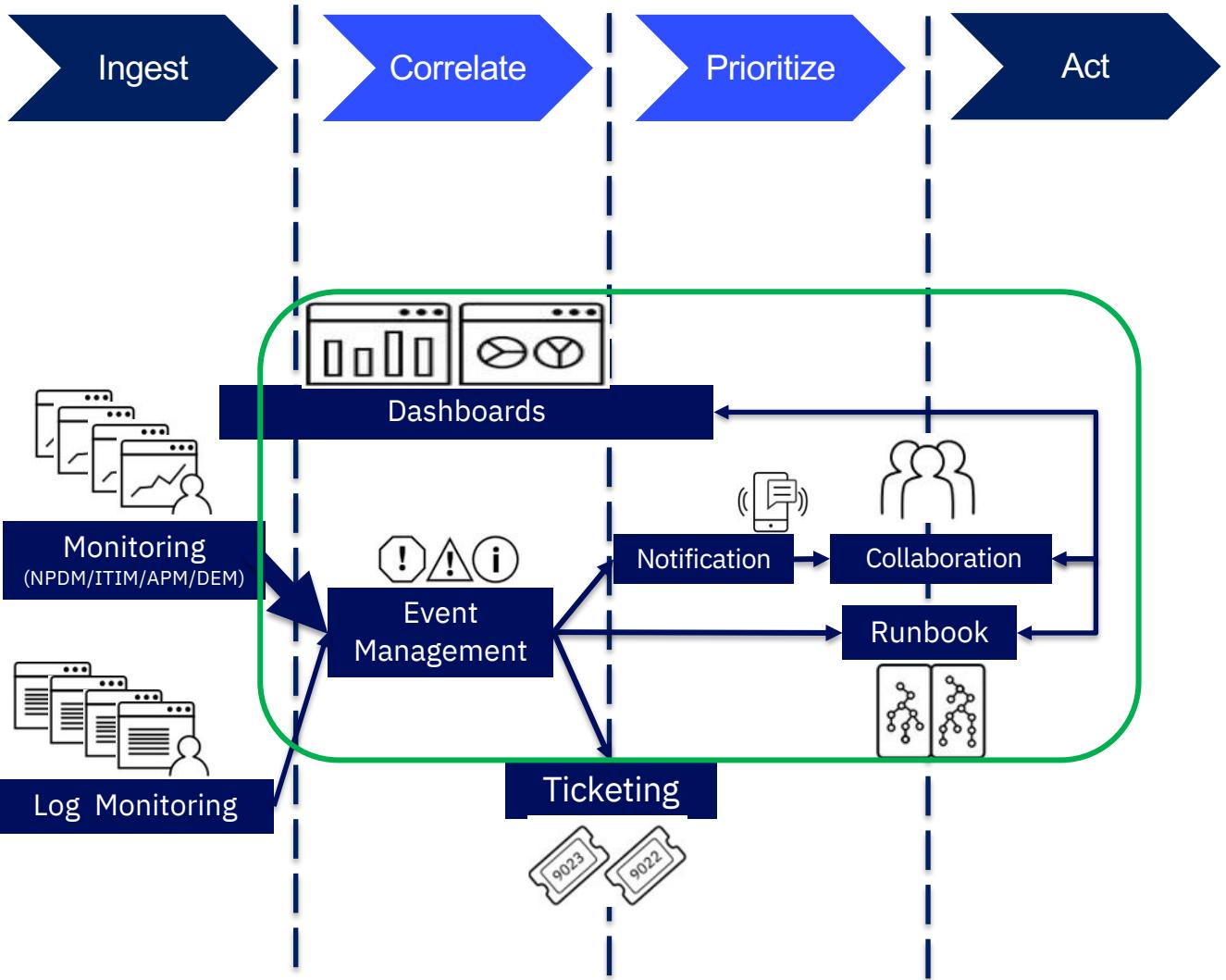
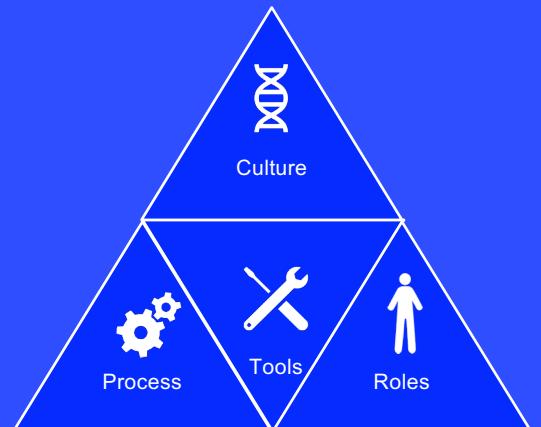
Ingest application, performance & operational event metrics

Automatically receive prioritized, correlated, incident information & guidance

Manage operations from one place & improve efficiency across teams

Accelerating Event & Incident Management

Get a consolidated view of problems and enable agile response in IT Ops – all from the public cloud



IBM Cloud Event Management

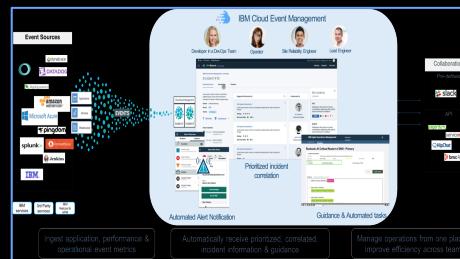
Cut through alarm noise. Restore service fast.

Cloud-native, consolidated operational event and incident correlation, prioritization and resolution

Event ingestion and correlation can be pre-configured and integrated from cloud-based and on-premises sources. IT operations teams can more easily configure alert, event and incident reduction from one console. These teams can also track and analyze operational efficiency, activity and trends.

Key Capabilities

- Ingest events from market prevalent sources with predefined integration and data normalization function, generic webhooks for bespoke sources
 - Manage operations from one place & improve efficiency across teams
 - Automated event correlation and prioritized incident resolution views to remove confusing and irrelevant alerts
 - Integrated notifications to help ensure the right person is notified at the right time
 - In-context runbooks to help ensure speedy resolution of issues
 - Predefined operations dashboards to see how incidents are being addressed, service is being restored and what apps and services are impacted
 - Clients purchase subscription to SaaS offerings
 - Guarantees privacy, reliability, scalability, and security



Key Differentiator

IBM Cloud Event Management provides ready-to-use, pre-set capabilities — all in a single comprehensive event management service. You can expect proven, industrial-strength scalability and increased ability to improve efficiency.

Leverages market-proven expertise:

- One holistic solution to ingest, correlate, notify and resolve operational incidents within minutes
 - Automated event correlation and prioritized incident resolution views to remove noise
 - Integrated, automated notifications to ensure the right person is notified at the right time
 - In-context runbooks and automated steps to ensure speedy resolution of issues to triage and resolve actions without writing code or paying for expensive consultants

Cloud Event Management Examples

The image displays two screenshots of the IBM Cloud Event Management interface.

Left Screenshot: Shows the 'Welcome to Cloud Event Management' page. It features a 'Test it, get up and running' section with a brief description and a 'Get Started' button, and a 'Start working on incidents' section with a brief description and a 'Go to my Incidents' button. The background has a hexagonal grid pattern.

Right Screenshot: Shows the 'IBM Cloud Event Management' dashboard under the 'Incidents' tab. It lists three incidents:

- #0000-7502 Application: SAMPLE - Online Sales
Priority: 1 Open for 20m Last changed Mar 12, 2019 | 3:04:25 PM PDT
9 Events Highest ▼ 5
Owner: James Moore (JM) Assigned
Investigate
- #0000-7602 Cluster: SAMPLE - Pipeline Project
Priority: 1 Open for 16m Last changed Mar 12, 2019 | 3:03:31 PM PDT
1 Event Highest 1
Unassigned
Investigate
- #0000-7402 Application: SAMPLE - Online Banking
Priority: 1 Open for 24m Last changed Mar 12, 2019 | 3:03:30 PM PDT
Unassigned

On the right side of the dashboard, there is a sidebar titled 'All groups' showing four groups: AD (App Dev), D1 (DevOps Team 1), JG (John's group), and T3 (Team James), each with 0 incidents.

Manage

Service credentials

Connections

DevOps /



Location: US South

Org: jdmoore@us.ibm.com

Space: dev

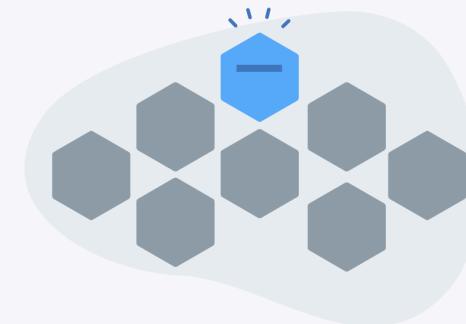
*Get started in minutes:
Have a connection? Just log in and you're ready to go.*



Welcome to Cloud Event Management

Test it, get up and running

See Cloud App Management in action. Test it out and configure your event sources so you can manage your apps and services centrally.

[Get Started](#)

Start working on incidents

Be a hero. Go straight to work on the issues affecting your environment and get them resolved.

[Go to my Incidents](#)[Cookie Preferences](#)

[Back](#)[Getting started](#)[Incidents](#)[Dashboard](#)[Administration](#)

Your workload at a glance:
Incident lists assigned to individuals and groups with the most
important information available

3 incidents

[My incidents](#)[Group incidents](#)[All incidents](#) [Search](#)

All groups

4 groups

App Dev

0 incidents



D1

DevOps Team 1

1 incident



JG

John's group

0 incidents



TJ

Team James

0 incidents



Owner James Moore



Group DevOps Team 1



Assigned

#0000-7502 Application: SAMPLE - Online Sales

Priority 1 Open for 20m

Last changed Mar 12, 2019 | 3:04:25 PM PDT

[9 Events](#) Highest ▼ 5[Investigate](#)

#0000-7602 Cluster: SAMPLE - Pipeline Project

Priority 1 Open for 16m

Last changed Mar 12, 2019 | 3:03:31 PM PDT

[1 Event](#) Highest 1[Investigate](#)

Unassigned



#0000-7402 Application: SAMPLE - Online Banking

Priority 1 Open for 24m

Last changed Mar 12, 2019 | 3:03:30 PM PDT

Unassigned



Incidents

Priority 1: Incident #0000-7502

Resolution view

Events

Timeline

A communal resolution view facilitates cross-group or cross-team collaboration or delegation ...

(X)

Application SAMPLE - Online Sales

Open for: 13m

Owner: James Moore

Group: DevOps Team 1 [Assign group](#)

Status: Assigned

[9 events](#)[0 comments](#)

Recent Timeline

 2m ago: Assigned to James Moore in group DevOps Team 1

Mar 12, 2019 | 3:04:25 PM PDT

 3m ago: Assigned to group DevOps Team 1

Mar 12, 2019 | 3:04:18 PM PDT

 4m ago: Event #bbey-npya

Mar 12, 2019 | 3:02:29 PM PDT

Suggested runbooks (1)

Example: Cleanup a file system on Linux

Steps to clean up a Linux file system

Success rate:  100%Rating:  

Type: Manual

Collaborate (4)



James Moore



Eric M



Isabell S

My incidents

1 incident

#0000-7502

Application: SAMPLE - Online Sales

Priority 1[Resolve](#)[In progress](#)



Preview runbook

Avoid confusion and indecision with structured guidance and automated steps ...

> Example: Cleanup a file system on Windows

Procedure: (6 steps, approximate time: a minute)

STEP 1

Login to **HOSTNAME** using Microsoft RDP or a remote desktop tool

STEP 2

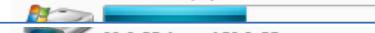
Identify file systems that need cleanup

Start the Computer application by clicking the icon below or using the shortcut (Windows Key + Pause).



Hard Disk Drives (2)

Local Disk (C:)



New Volume (E:)



The graphical view shows the file systems. If the gauge is red and nearly full, the file system needs cleanup. Identify the disc drive letter, go back to the runbook details, and add the letter followed by a colon as the runbook parameter **DISKDRIVELETTER**. Then continue with the next step.

STEP 3

Delete "safe" files from the file system

From the start menu, launch cmd.exe and run the following commands to remove "safe" files:

```
DISKDRIVELETTER
cd \
del /Q/F/S *.tmp
del /Q/F/S *.dmp
forfiles /P DISKDRIVELETTER /M "*.log" /D -30 /S /C "cmd /c del /Q/F/S @FILE"
```

Run the following command to empty the Recycle Bin on the file system:

Sharing context and history helps teams move from identification to diagnosis quickly

Incidents

Priority 1 : Incident #0000-7502

Resolution view Events Timeline

Current owner: James Moore Assigned

Newest first

Add comment +

Assigned to James Moore in group DevOps Team 1 Assigned Mar 12, 2019 | 3:04:25 PM PDT

Assigned to group DevOps Team 1 Assigned Mar 12, 2019 | 3:04:18 PM PDT

Event #bbey-npya: SAMPLE - US clients experiencing high response times while connecting to onlinesales Mar 12, 2019 | 3:02:29 PM PDT

Event #389q-9tjs: SAMPLE - west region clients experiencing increased response times while connecting to onlinesales Mar 12, 2019 | 3:01:29 PM PDT

Event #p4aw-1htc: SAMPLE - east region clients experiencing high response times while connecting to onlinesales Mar 12, 2019 | 3:00:29 PM PDT

Event #lkgbg-klji: SAMPLE - central region clients experiencing high response times while connecting to onlinesales Mar 12, 2019 | 3:00:29 PM PDT

Incidents

Priority 1 : Incident #0000-7502

Resolution view Events Timeline

Event #mo6x-jm7s: SAMPLE - connecting to onlinesales Mar 12, 2019 | 2:56:29 PM PDT

Event #pcry-aqn: SAMPLE - connecting to onlinesales Mar 12, 2019 | 2:56:29 PM PDT

9 of 9 events

Search



Sev	State	Resource type	First occurrence	Summary	Event type
> ▼	Open	Application	Mar 12, 2019 2:56:29 PM PDT	SAMPLE - process http_proxy is co...	Response Time
> ▼	Cleared	Application	Mar 12, 2019 2:55:29 PM PDT	SAMPLE - CPU is thrashing at 99%...	CPU Utilisation
> ▼	Cleared	Application	Mar 12, 2019 3:02:29 PM PDT	SAMPLE - US clients experiencing ...	Response Time
> ▼	Cleared	Application	Mar 12, 2019 2:58:29 PM PDT	SAMPLE - north region clients exp...	Response Time
> ▼	Cleared	Application	Mar 12, 2019 3:00:29 PM PDT	SAMPLE - east region clients exp...	Response Time
► ▲	Open	Application	Mar 12, 2019 2:54:29 PM PDT	SAMPLE - client response time is a...	Online Sales application alert policy
► ▲	Cleared	Application	Mar 12, 2019 3:01:29 PM PDT	SAMPLE - west region clients exp...	Response Time
► ⓘ	Open	Application	Mar 12, 2019 2:59:29 PM PDT	SAMPLE - central region clients ex...	Response Time
► ⓘ	Cleared	Application	Mar 12, 2019 2:53:29 PM PDT	SAMPLE - Slow response time for ...	Response Time

My incidents
1 incident

#0000-7502
Application: SAMPLE - Online Sales

Priority 1

IBM Cloud Event Management Notification

Incident: #0003-7512

State: Assigned to individual

Priority: 1

Description: Application: SAMPLE - Online Banking

Owner: sunjit.tara@us.ibm.com

Show more

Incident List

Incident Viewer

Take Ownership

My incidents
1 incident

#0000-7502
Application: SAMPLE - Online Sales

Priority 1

Pre-defined, ready to use integration

Administration / Integrations

Select the integration type to configure

[Incoming](#) [Outgoing](#)

Standard integrations [1](#)

 Alert Notification	 Amazon Web Services	 AppDynamics	 Datadog	 Dynatrace	 Elasticsearch	 Email	 IBM Cloud Application Performance Management	 IBM Cloud Availability Monitoring
Configure	Configure	Configure	Configure	Configure	Configure	Configure	Configure	Log into IBM Cloud
 IBM Continuous Delivery	 IBM UrbanCode Deploy	 Jenkins	 Microsoft Azure	 Microsoft System Center Operations Manager	 Nagios XI	 Netcool/OMNIBUS	 New Relic Alerts	 New Relic Legacy
Configure	Configure	Configure	Configure	Configure	Configure	Configure	Configure	Configure
 Pingdom	 Prometheus	 Sensu	 SolarWinds	 Splunk Enterprise	 Sumo Logic	 Webhook	 Zabbix	
Configure	Configure	Configure	Configure	Configure	Configure	Configure	Configure	

[Incoming](#) [Outgoing](#)

Standard integrations [1](#)

 GitHub	 Microsoft Teams	 ServiceNow	 Slack	 Webhook
Configure	Configure	Configure	Configure	Configure

Edit group DevOps Team 1

[Details](#)[Schedule](#)

Avoid delays and misdirection – automate how and when teams and users get notified ...

[Create](#)[Edit](#)[Delete](#)

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
0:00	0:00 - 8:00	0:00 - 8:00	0:00 - 8:00	0:00 - 8:00	0:00 - 8:00	0:00 - 8:00	0:00 - 8:00
2:00							
4:00	EU day	EU weekend	EU weekend				
6:00	1	1	1	1	1	1	1
8:00	8:00 - 16:00	8:00 - 16:00	8:00 - 16:00	8:00 - 16:00	8:00 - 16:00	8:00 - 16:00	8:00 - 16:00
10:00							
12:00	US day	US weekend	US weekend				
14:00	1	1	1	1	1	1	1
16:00	16:00 - 0:00	16:00 - 0:00	16:00 - 0:00	16:00 - 0:00	16:00 - 0:00	16:00 - 0:00	16:00 - 0:00
18:00							
20:00	AP day	AP day	AP day	AP day	AP weekend	AP weekend	AP day
22:00	1	1	1	1	1	1	1
16	7/6/20						

Pattern details**Shift pattern name:**

DevOps Follow the Sun

Shift pattern description:

24/7 on duty based on American, European and Asian shifts.

Apply an existing pattern:

- Static patterns
 - < No pattern >
 - < Blank pattern >
 - Follow the sun**
 - 8 to 5
 - 24x7 On call
 - 12x2x7 On call
- User defined patterns
 - John's pattern

Start day:

Monday

Generate schedule in advance:

1 week

Understand operational health by tracking operational activity ...

Operations Dashboard

All incidents



Resources affected by incidents (All incidents)



2

Applications affected



0

Services affected



2

Servers affected



0

Clusters affected



0

Locations affected

 Priority 1 Priority 2 Priority 3 Priority 4 Priority 5

State of incidents (All incidents; 4 incidents)

0
Total0
Total

In progress

On hold

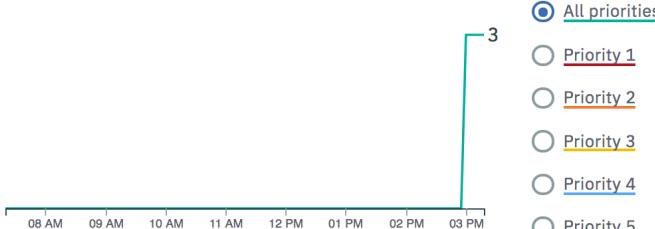
Priority 1

Priority 2 Priority 3

Priority 4

Priority 5

Open incidents over time (All incidents)



Mean time to respond and resolve

Filter by



Average duration (Last 90 days)



70 mins

Mean time to incident resolution



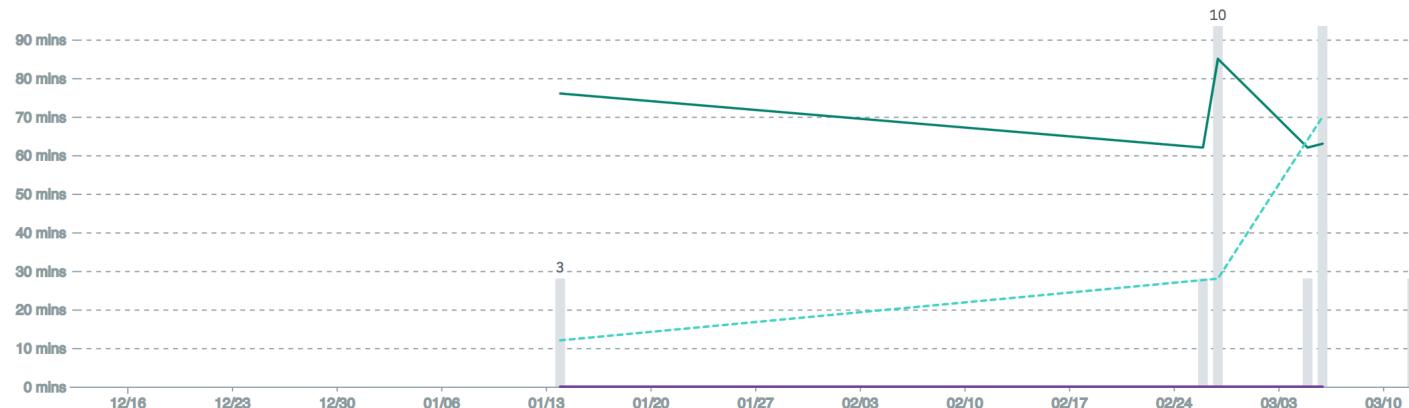
36 mins

Mean time to respond to an incident



29

Number of closed incidents

 Mean time to resolution i Mean time to respond i Opened incidents i Time an incident is on hold i

Thank you

