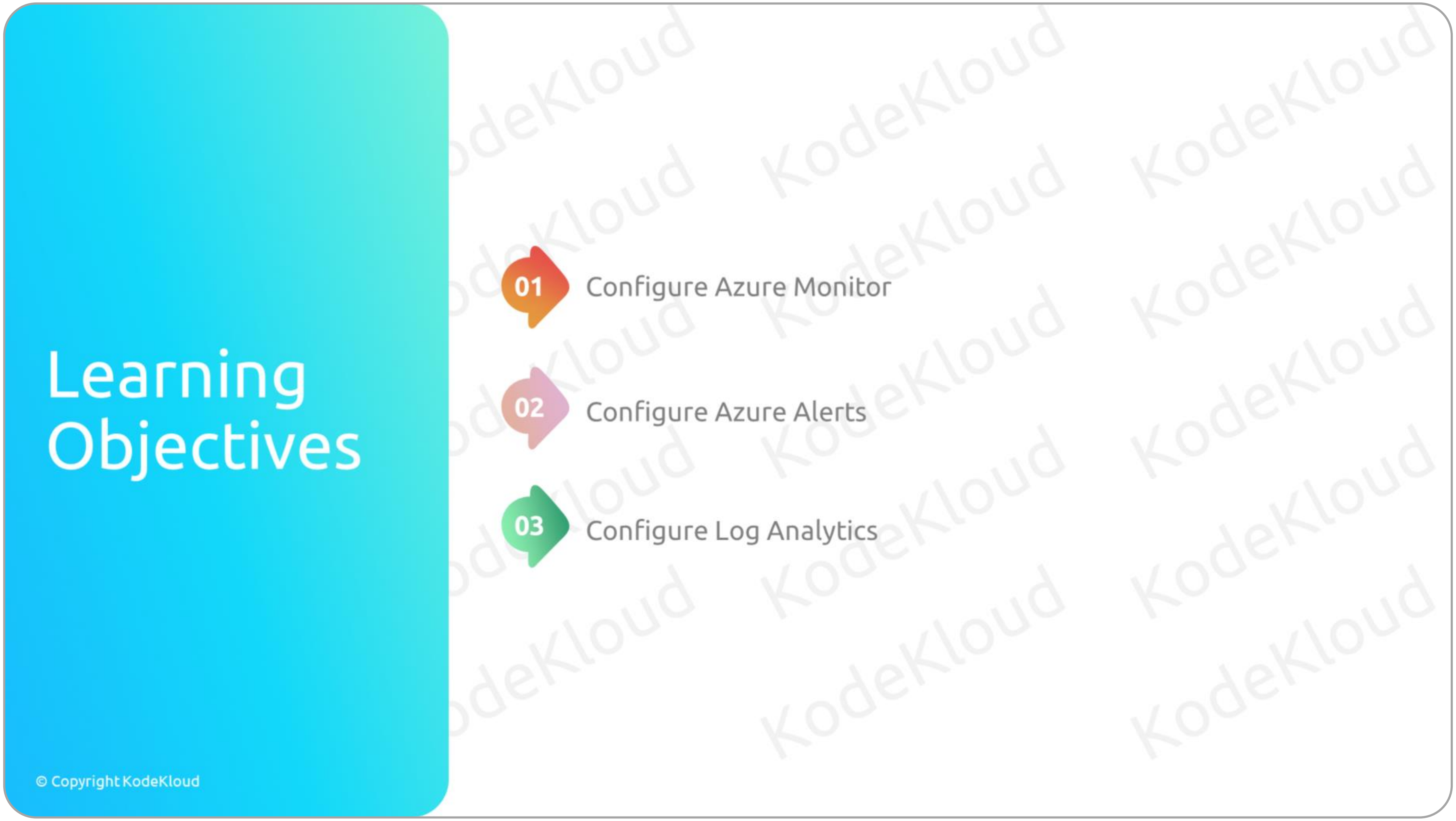
KodeKloud

© Copyright KodeKloud

Follow us on https://kodekloud.com/ to learn more about us.

Administer Monitoring

© Copyright KodeKloud



Learning Objectives

01 Configure Azure Monitor

02 Configure Azure Alerts

03 Configure Log Analytics

© Copyright KodeKloud

KodeKloud

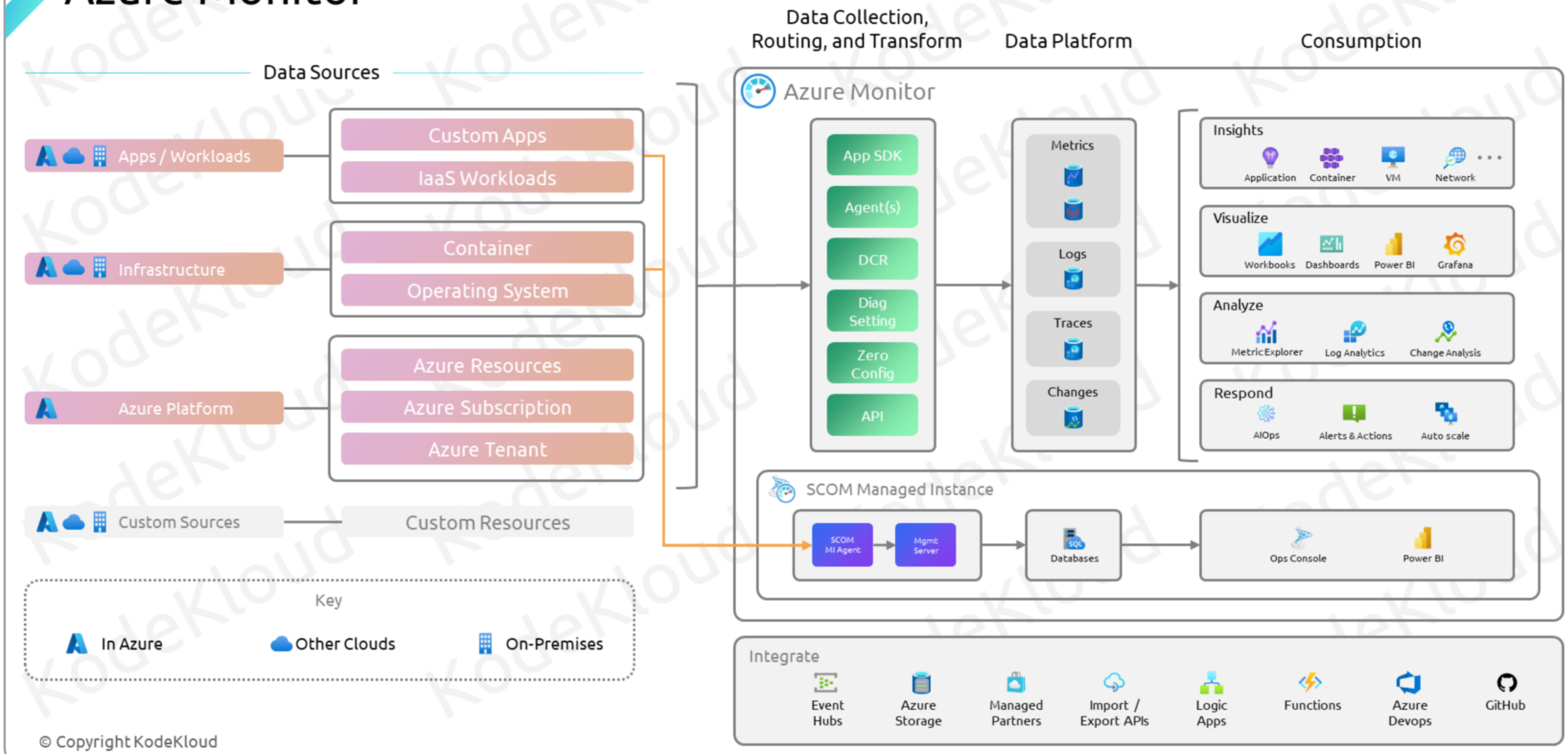
Moved Lab 03a – Manage Azure resources with the Azure portal into this module. It covers resource locks.

Azure Monitor

© Copyright KodeKloud

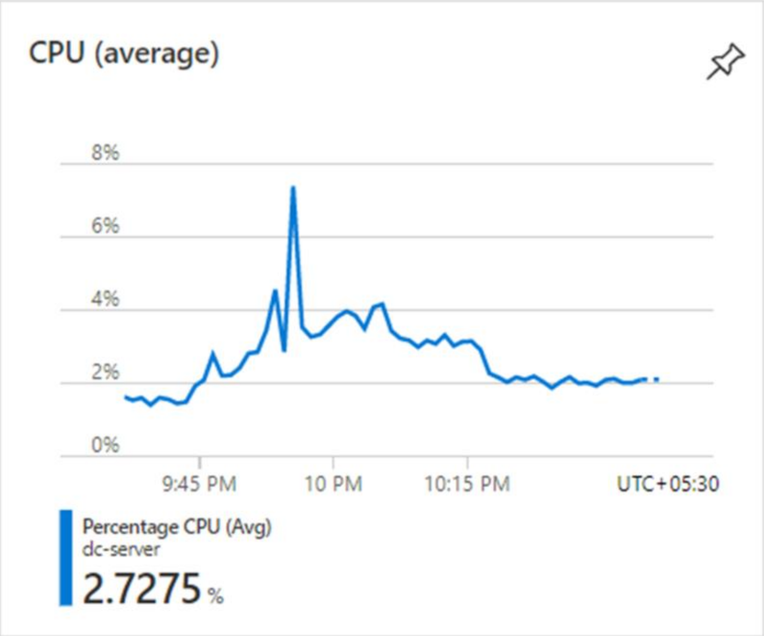
- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CICD isn't just for software developers. It's also for infrastructure pros

Azure Monitor



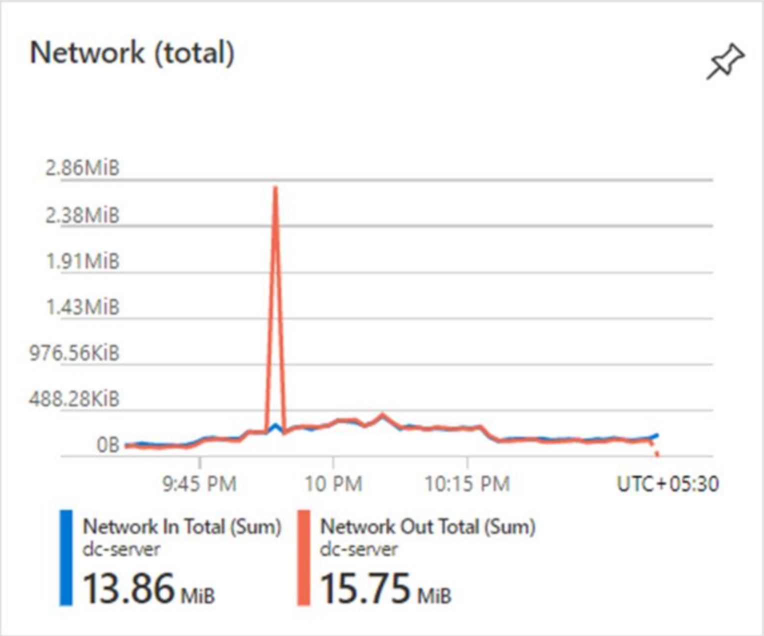
© Copyright KodeKloud

Metrics



CPU (average)

Percentage CPU (Avg)
dc-server
2.7275 %



Network (total)

Network In Total (Sum)
dc-server
13.86 MiB

Network Out Total (Sum)
dc-server
15.75 MiB

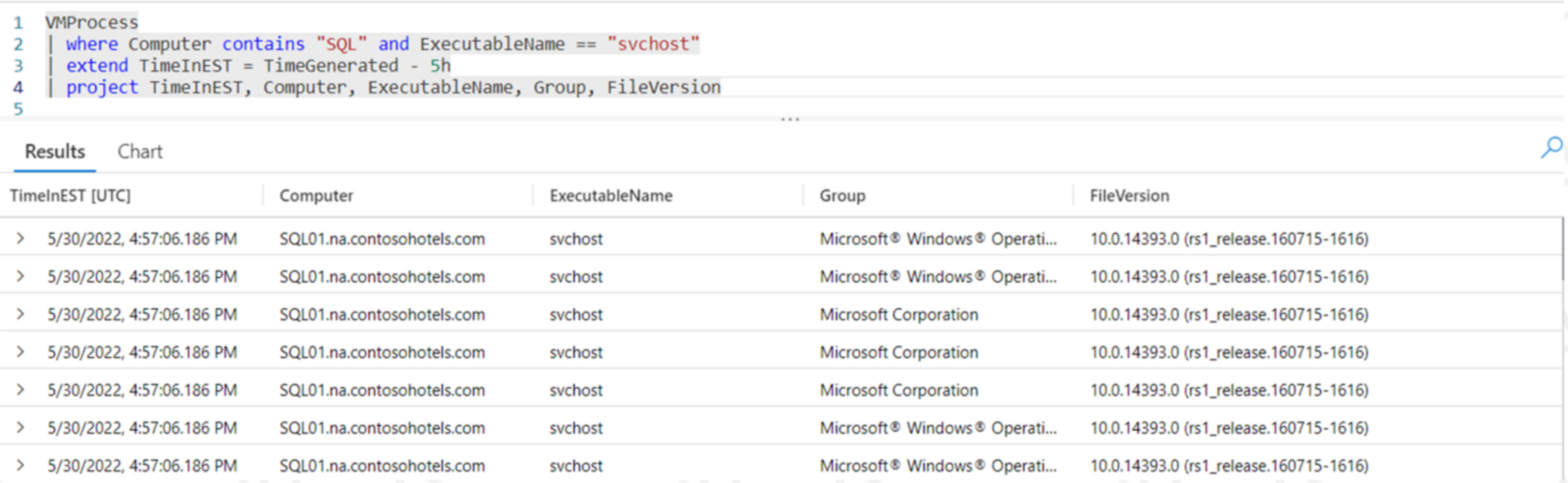
Zero configuration required

Time series

Near real-time data

© Copyright KodeKloud

Logs



```
VMProcess
| where Computer contains "SQL" and ExecutableName == "svchost"
| extend TimeInEST = TimeGenerated - 5h
| project TimeInEST, Computer, ExecutableName, Group, FileVersion
```

TimeInEST [UTC]	Computer	ExecutableName	Group	FileVersion
> 5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)
> 5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)
> 5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft Corporation	10.0.14393.0 (rs1_release.160715-1616)
> 5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft Corporation	10.0.14393.0 (rs1_release.160715-1616)
> 5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft Corporation	10.0.14393.0 (rs1_release.160715-1616)
> 5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)
> 5/30/2022, 4:57:06.186 PM	SQL01.na.contosohotels.com	svchost	Microsoft® Windows® Operati...	10.0.14393.0 (rs1_release.160715-1616)

Organized as records

Requires additional configuration

Rich query language

© Copyright KodeKloud

Data Sources

Application

- Instrumentation package
- Availability test

OS

- Azure Monitor agent
- Azure diagnostic extension

Azure Resources

- Metrics
- Resource logs

Azure Subscription

- Service health
- Activity log

Azure Tenant

- Active directory

Custom

- Instrumentation package
- Application

Metrics

Logs

© Copyright KodeKloud

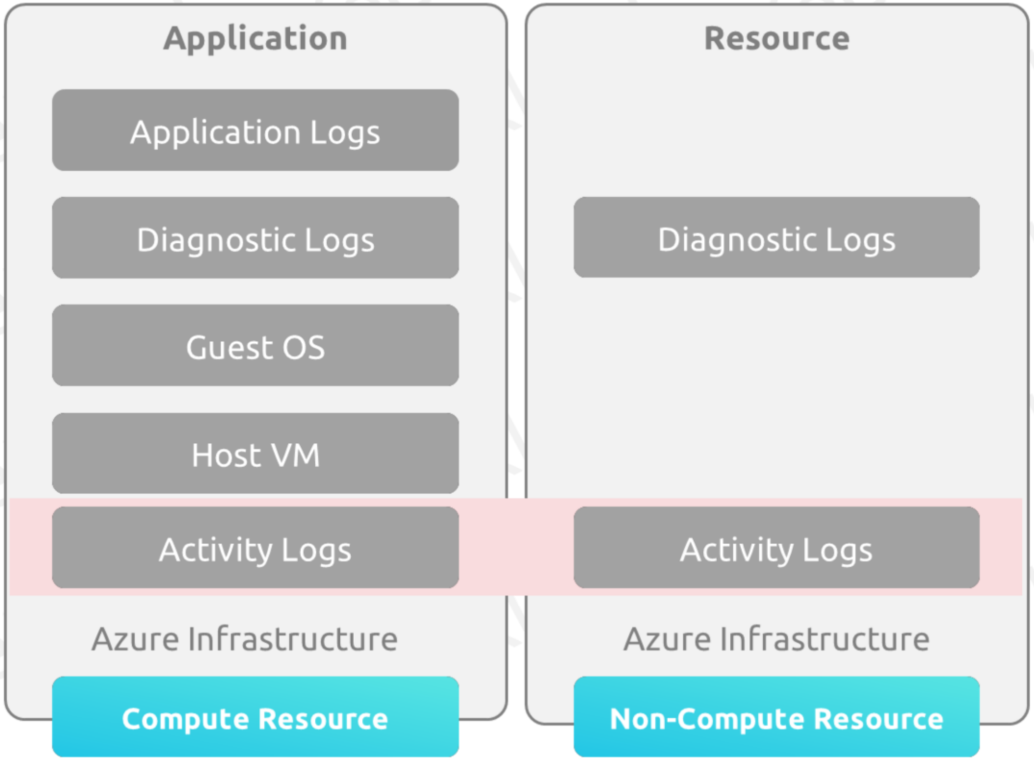
Azure Activity Logs

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CICD isn't just for software developers. It's also for infrastructure pros

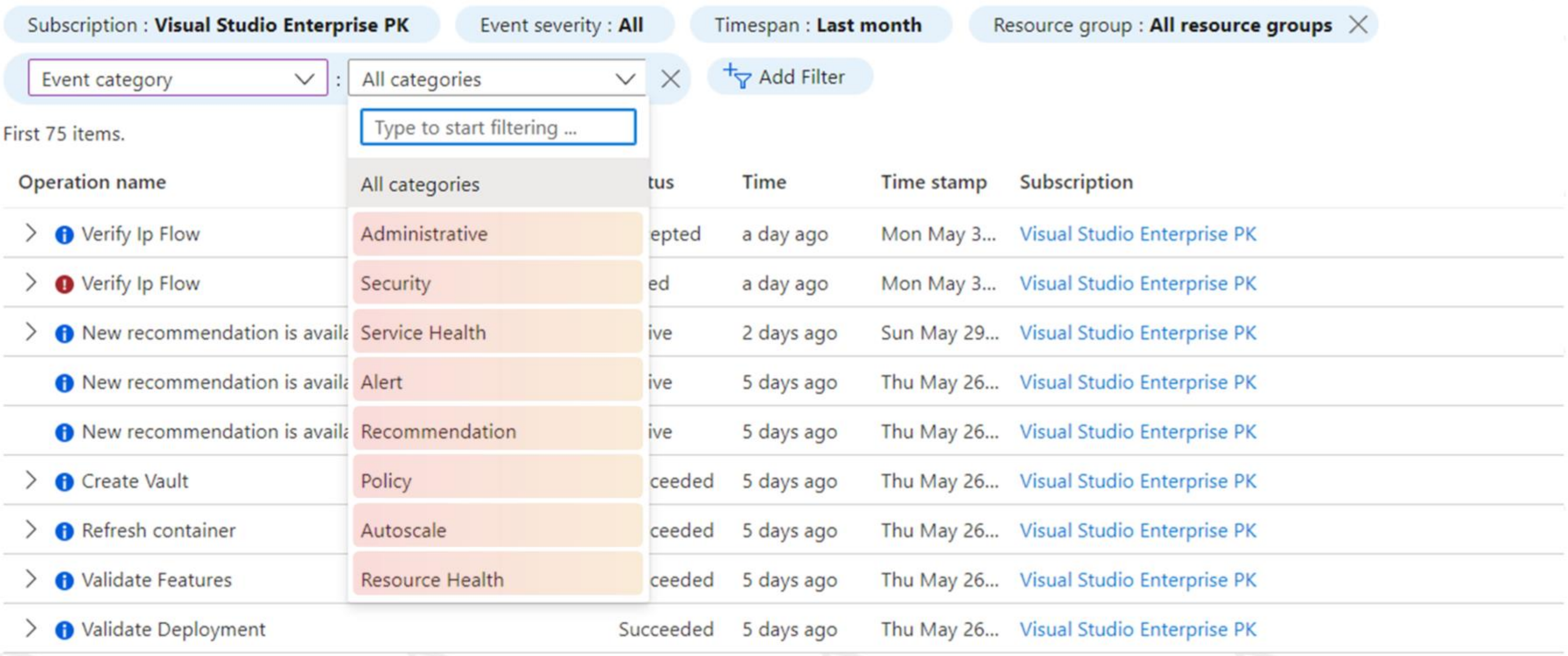
Azure Activity Log

- Subscription-Level Logging
- Auditing
- Retention
- Querying Data



© Copyright KodeKloud

Azure Activity Log – Event Categories



Subscription : **Visual Studio Enterprise PK** | Event severity : **All** | Timespan : **Last month** | Resource group : **All resource groups** ✕

Event category ⌄ : All categories ⌄ ✕ | Add Filter

Type to start filtering ...

- All categories
- Administrative
- Security
- Service Health
- Alert
- Recommendation
- Policy
- Autoscale
- Resource Health

First 75 items.

Operation name	tus	Time	Time stamp	Subscription
> ⓘ Verify Ip Flow	epted	a day ago	Mon May 3...	Visual Studio Enterprise PK
> ❗ Verify Ip Flow	ed	a day ago	Mon May 3...	Visual Studio Enterprise PK
> ⓘ New recommendation is availa	ive	2 days ago	Sun May 29...	Visual Studio Enterprise PK
ⓘ New recommendation is availa	ive	5 days ago	Thu May 26...	Visual Studio Enterprise PK
ⓘ New recommendation is availa	ive	5 days ago	Thu May 26...	Visual Studio Enterprise PK
> ⓘ Create Vault	ceeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK
> ⓘ Refresh container	ceeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK
> ⓘ Validate Features	ceeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK
> ⓘ Validate Deployment	Succeeded	5 days ago	Thu May 26...	Visual Studio Enterprise PK

© Copyright KodeKloud

Log Analytics

KodeKloud

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CICD isn't just for software developers. It's also for infrastructure pros

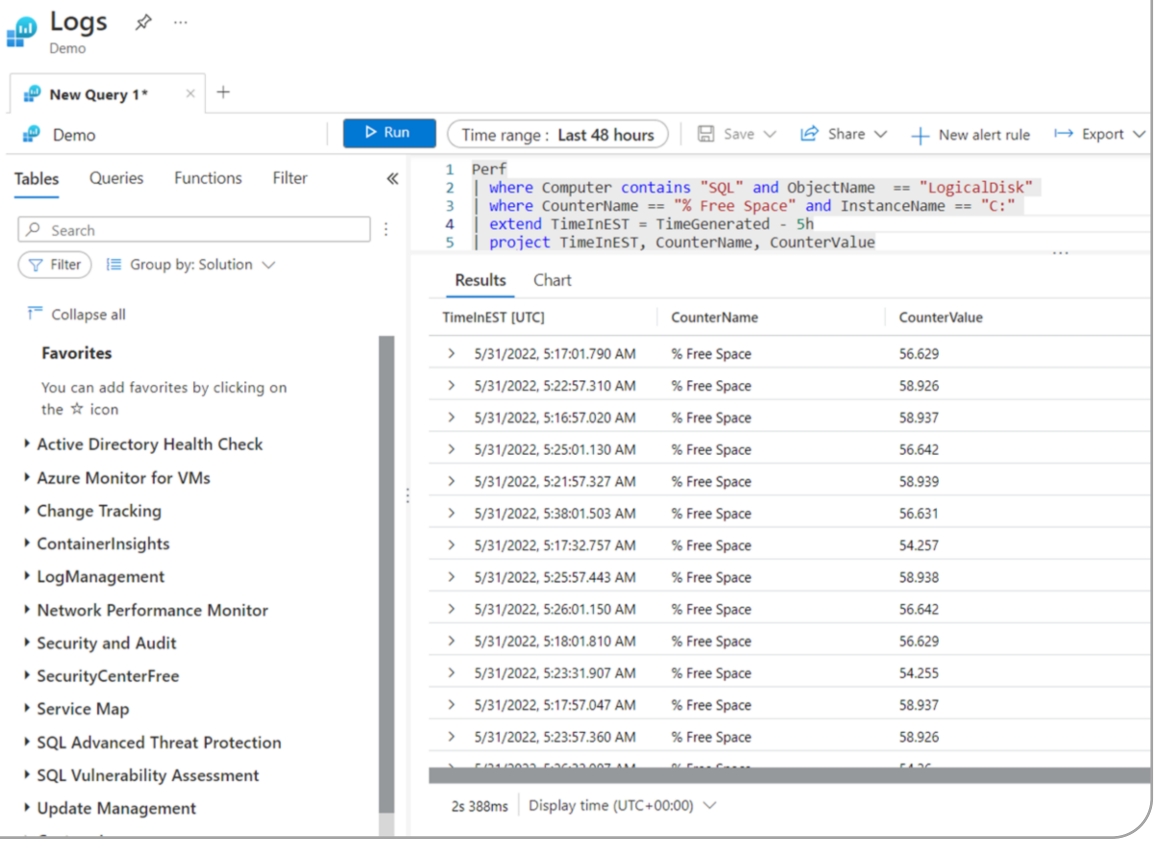
Log Analytics

Data collection

Reporting and visualization

Workspace

Pricing



You can add favorites by clicking on the ☆ icon

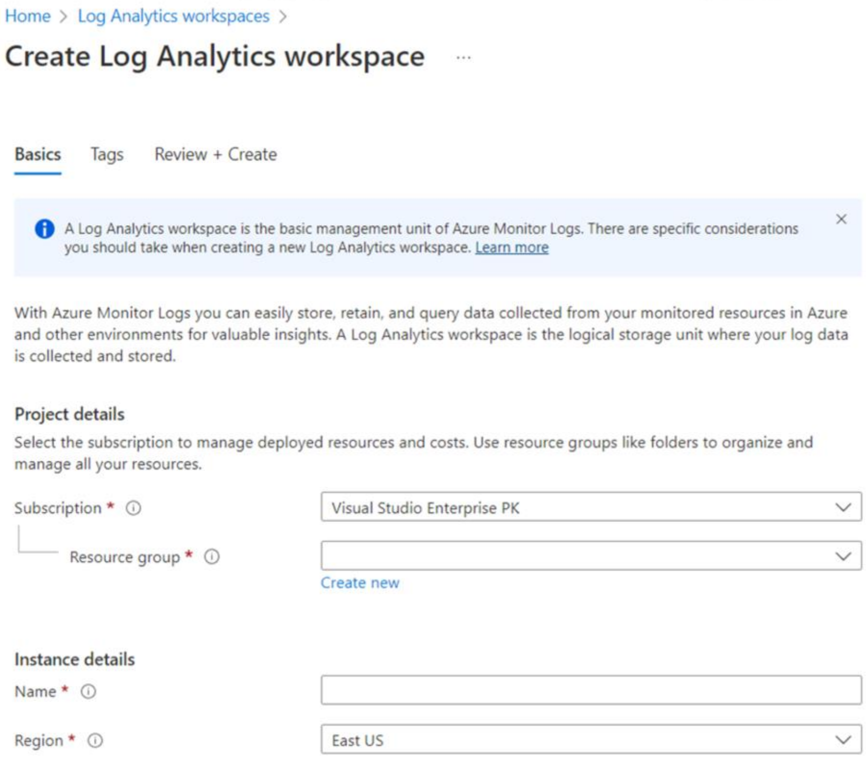
```
Perf
| where Computer contains "SQL" and ObjectName  == "LogicalDisk"
| where CounterName == "% Free Space" and InstanceName == "C:"
| extend TimeInEST = TimeGenerated - 5h
| project TimeInEST, CounterName, CounterValue
```

TimeInEST [UTC]	CounterName	CounterValue
5/31/2022, 5:17:01.790 AM	% Free Space	56.629
5/31/2022, 5:22:57.310 AM	% Free Space	58.926
5/31/2022, 5:16:57.020 AM	% Free Space	58.937
5/31/2022, 5:25:01.130 AM	% Free Space	56.642
5/31/2022, 5:21:57.327 AM	% Free Space	58.939
5/31/2022, 5:38:01.503 AM	% Free Space	56.631
5/31/2022, 5:17:32.757 AM	% Free Space	54.257
5/31/2022, 5:25:57.443 AM	% Free Space	58.938
5/31/2022, 5:26:01.150 AM	% Free Space	56.642
5/31/2022, 5:18:01.810 AM	% Free Space	56.629
5/31/2022, 5:23:31.907 AM	% Free Space	54.255
5/31/2022, 5:17:57.047 AM	% Free Space	58.937
5/31/2022, 5:23:57.360 AM	% Free Space	58.926

© Copyright KodeKloud

Log Analytics Workspace

- Workspace
- Data isolation
- Stores insight and sentinel data



Home > Log Analytics workspaces >

Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Visual Studio Enterprise PK

Resource group * :

Create new

Instance details

Name * :

Region * : East US

© Copyright KodeKloud

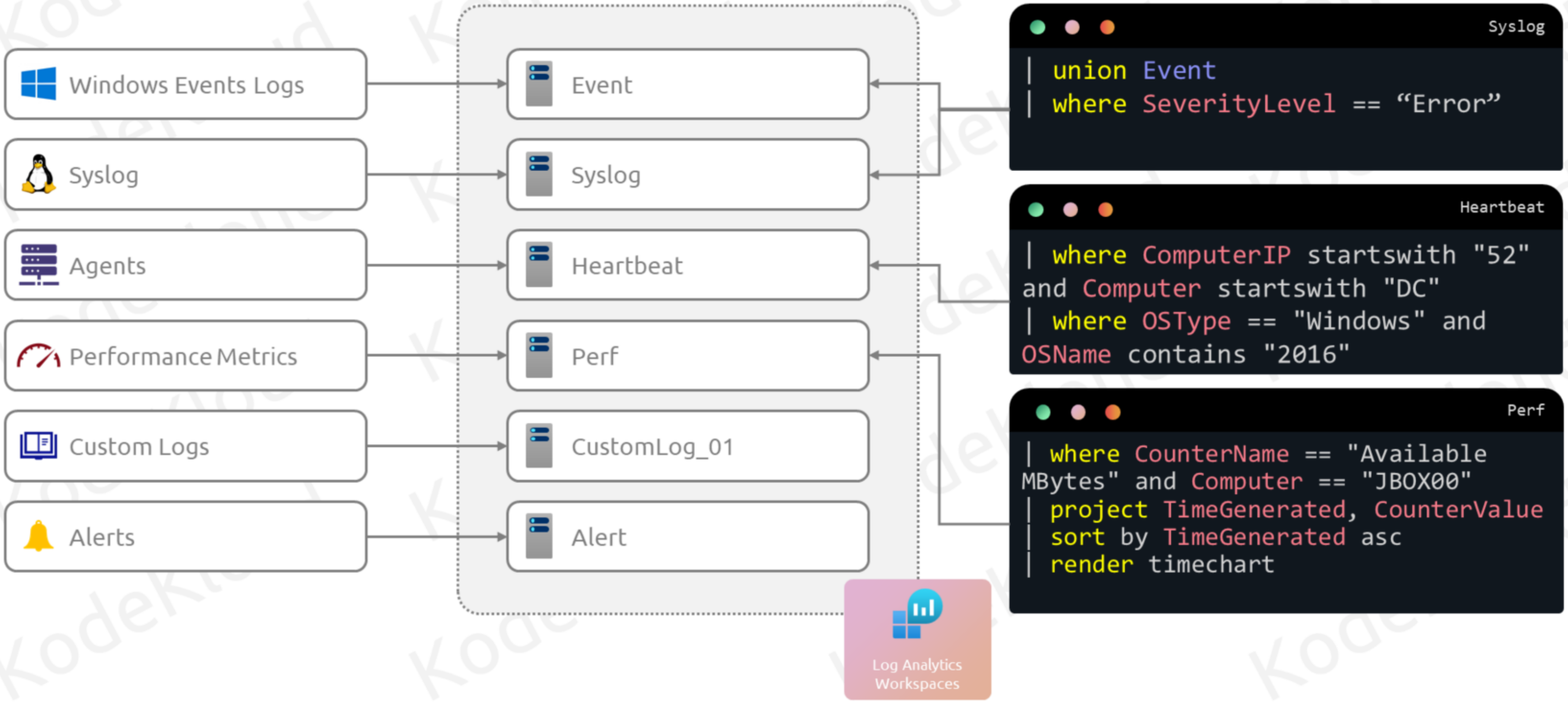
KodeKloud

Querying Log Analytics Workspace

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CICD isn't just for software developers. It's also for infrastructure pros

Querying Log Analytics Workspace



Syslog

```
| union Event
| where SeverityLevel == “Error”
```

Heartbeat

```
| where ComputerIP startswith "52"
and Computer startswith "DC"
| where OSType == "Windows" and
OSName contains "2016"
```

Perf

```
| where CounterName == "Available
MBytes" and Computer == "JBOX00"
| project TimeGenerated, CounterValue
| sort by TimeGenerated asc
| render timechart
```

© Copyright KodeKloud

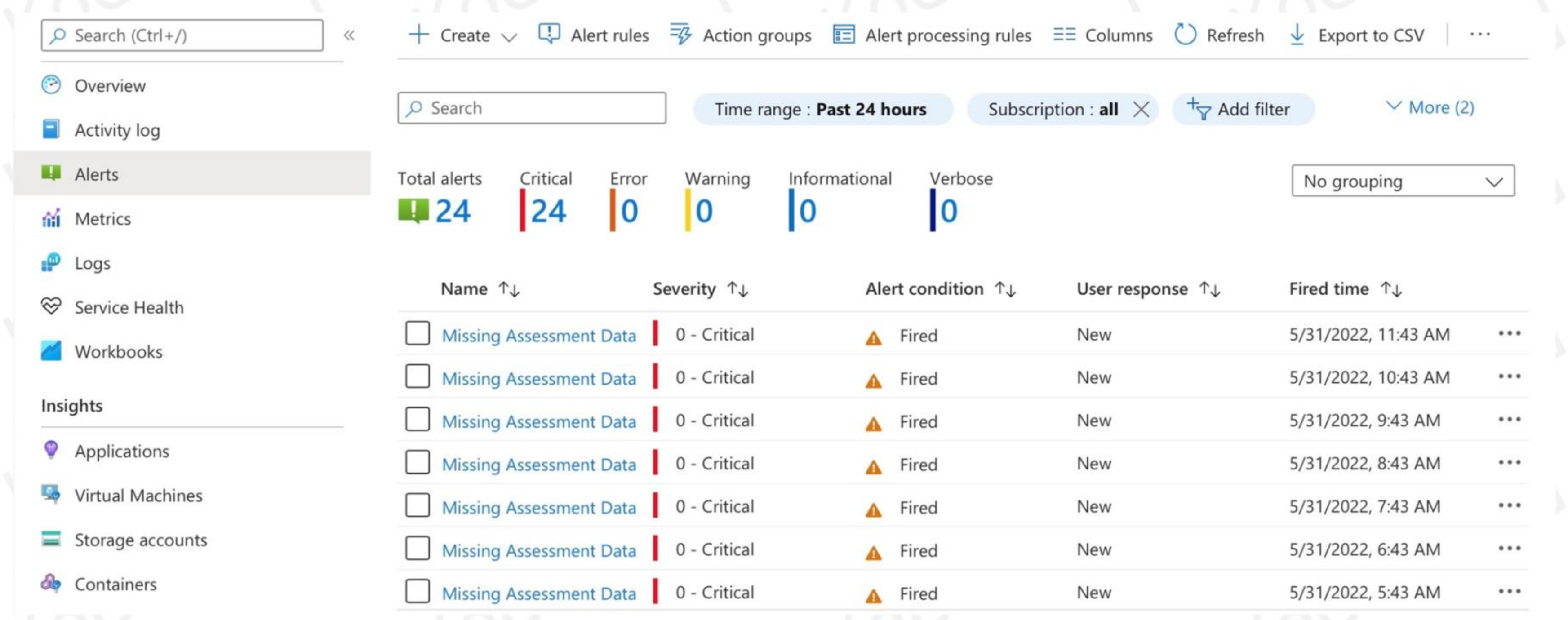
Enable Azure Monitor Alerts

KodeKloud

© Copyright KodeKloud

- A repeatable way to deliver software and infrastructure code to its destination
- Build and test code
- Deploy to on-prem or cloud resources
- CICD isn't just for software developers. It's also for infrastructure pros

Enable Azure Monitor Alert



Total alerts	Critical	Error	Warning	Informational	Verbose
24	24	0	0	0	0

	Name ↑↓	Severity ↑↓	Alert condition ↑↓	User response ↑↓	Fired time ↑↓	
□	Missing Assessment Data	0 - Critical	⚠ Fired	New	5/31/2022, 11:43 AM	•••
□	Missing Assessment Data	0 - Critical	⚠ Fired	New	5/31/2022, 10:43 AM	•••
□	Missing Assessment Data	0 - Critical	⚠ Fired	New	5/31/2022, 9:43 AM	•••
□	Missing Assessment Data	0 - Critical	⚠ Fired	New	5/31/2022, 8:43 AM	•••
□	Missing Assessment Data	0 - Critical	⚠ Fired	New	5/31/2022, 7:43 AM	•••
□	Missing Assessment Data	0 - Critical	⚠ Fired	New	5/31/2022, 6:43 AM	•••
□	Missing Assessment Data	0 - Critical	⚠ Fired	New	5/31/2022, 5:43 AM	•••

© Copyright KodeKloud

Unified Authoring Experience - We can create alerts for Activity Logs, Service Health Events, Log Analytics, Metrics etc. In all these scenarios the authoring experience is same.

Classify based on severity and response - Azure Alerts supports severity (0-4), so you easily prioritize the alerts. Secondly, we can categorize by user response New, Acknowledged or Closed.

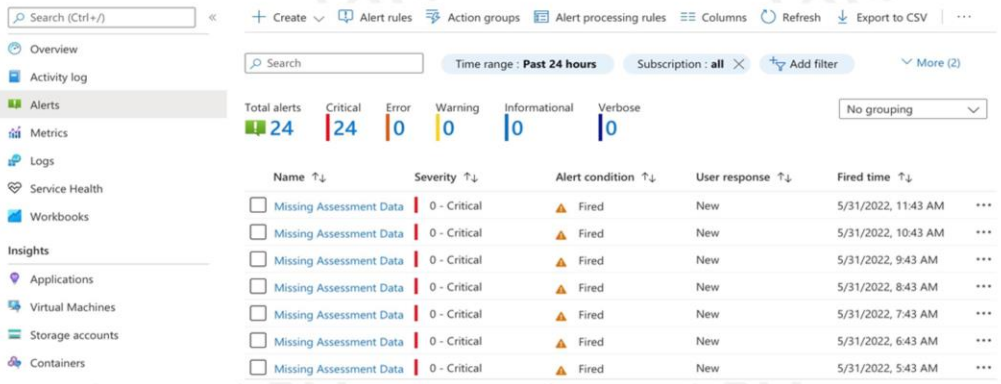
Integrate with Action Groups - Define your notification and automation preferences with the help of Action Groups.

Enable Azure Monitor Alert

Unified authoring experience

Classify based on severity and response

Integrate with action groups



Total alerts	Critical	Error	Warning	Informational	Verbose
24	24	0	0	0	0

	Name ↑↓	Severity ↑↓	Alert condition ↑↓	User response ↑↓	Fired time ↑↓
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 11:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 10:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 9:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 8:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 7:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 6:43 AM
□	Missing Assessment Data	0 - Critical	Fired	New	5/31/2022, 5:43 AM

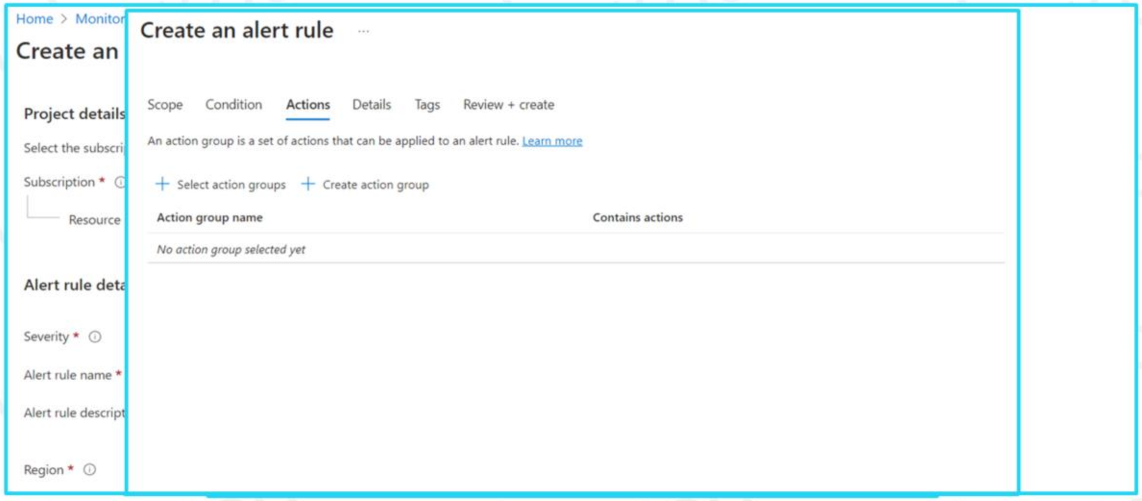
© Copyright KodeKloud

Unified Authoring Experience - We can create alerts for Activity Logs, Service Health Events, Log Analytics, Metrics etc. In all these scenarios the authoring experience is same.

Classify based on severity and response - Azure Alerts supports severity (0-4), so you easily prioritize the alerts. Secondly, we can categorize by user response New, Acknowledged or Closed.

Integrate with Action Groups - Define your notification and automation preferences with the help of Action Groups.

Enable Azure Monitor Alert



Home > Monitor

Create an

Project details

Select the subscri

Subscription *

Resource

Alert rule deta

Severity *

Alert rule name *

Alert rule descript

Region *

Create an alert rule ...

Scope Condition **Actions** Details Tags Review + create

An action group is a set of actions that can be applied to an alert rule. Learn more

+ Select action groups + Create action group

Action group name	Contains actions
No action group selected yet	

Sco
Condi
Acti
Rule d

© Copyright KodeKloud

Scope - Defines the scope for alert

Actions - Integrate alerts with Action Groups

Condition - Helps you to define the signal and criteria for alert

Rule details - Specify name, severity, region, resource group and subscription for the alert

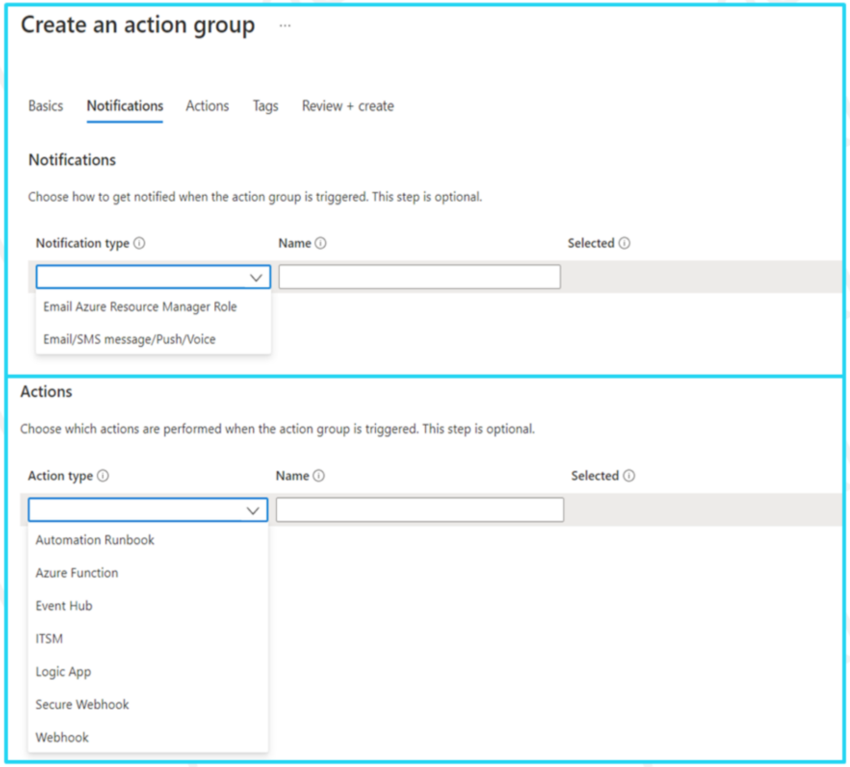
Enable Azure Monitor Alert

Notifications

- Email Azure Resource Manager Role (Owner/ Contributor/ Reader/ Monitoring Contributor/ Monitoring Reader)
- Email/ SMS/ Push/ Voice

Actions

- Automation Runbook
- Azure Function
- Event Hub
- ITSM
- Logic App
- Secure Webhook
- Webhook



Create an action group ···

Notifications

Choose how to get notified when the action group is triggered. This step is optional.

Notification type ⓘ	Name ⓘ	Selected ⓘ

Email Azure Resource Manager Role
Email/SMS message/Push/Voice

Actions

Choose which actions are performed when the action group is triggered. This step is optional.

Action type ⓘ	Name ⓘ	Selected ⓘ

© Copyright KodeKloud

KodeKloud

© Copyright KodeKloud

Follow us on https://kodekloud.com/ to learn more about us.