



IBM Cloud Monitoring with Sysdig

Cloud Native BootCamp

<https://cloudnative101.dev/>

- **Legal Disclaimer © IBM Corporation 2019. All Rights Reserved.**

- The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.
- References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Partnership



+

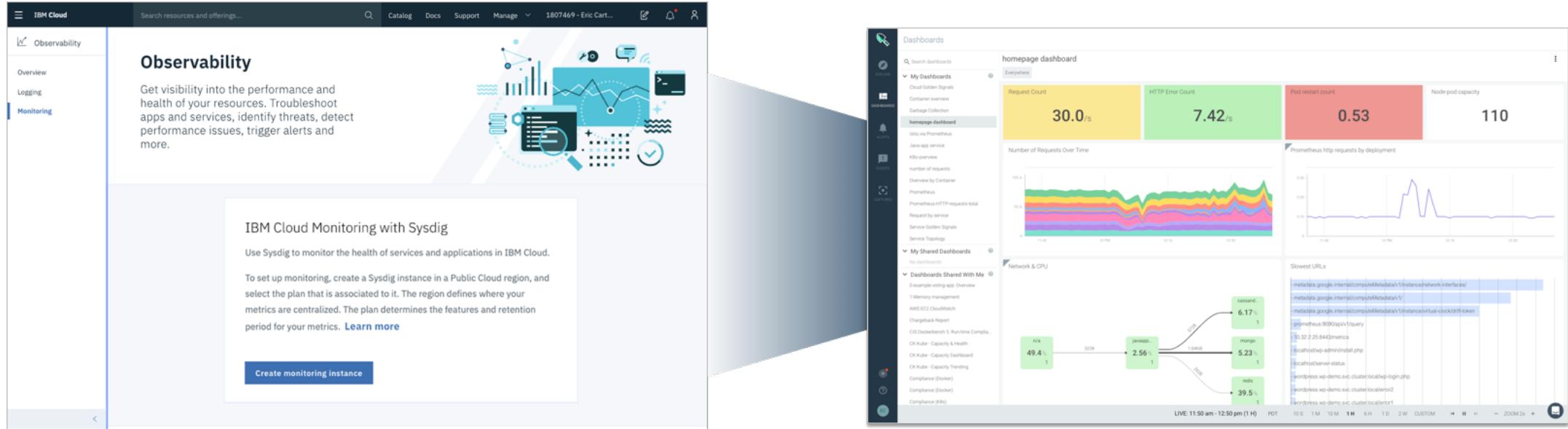


IBM Cloud

IBM and Sysdig are delivering solutions to solve enterprise monitoring challenges in order to identify and fix issues faster.

IBM Cloud Monitoring with Sysdig

Full stack telemetry and advanced features for administrators, DevOps teams and developers to monitor and troubleshoot, define alerts, and design custom dashboards.



The image displays two screenshots of the IBM Cloud interface. The left screenshot shows the 'Observability' section under the 'Monitoring' tab. It includes a descriptive text block about Sysdig's capabilities, a large icon representing monitoring, and a 'Create monitoring instance' button. The right screenshot shows a detailed monitoring dashboard with various panels: 'Request Count' (30.0/s), 'HTTP Error Count' (7.42/s), 'Node pod capacity' (110), 'Number of Requests Over Time' (a stacked area chart), 'Slowest URLs' (a list of URLs with latency metrics), and 'Network & CPU' (a complex graph showing data flow between nodes like n/a, jboss, merge, and redis).

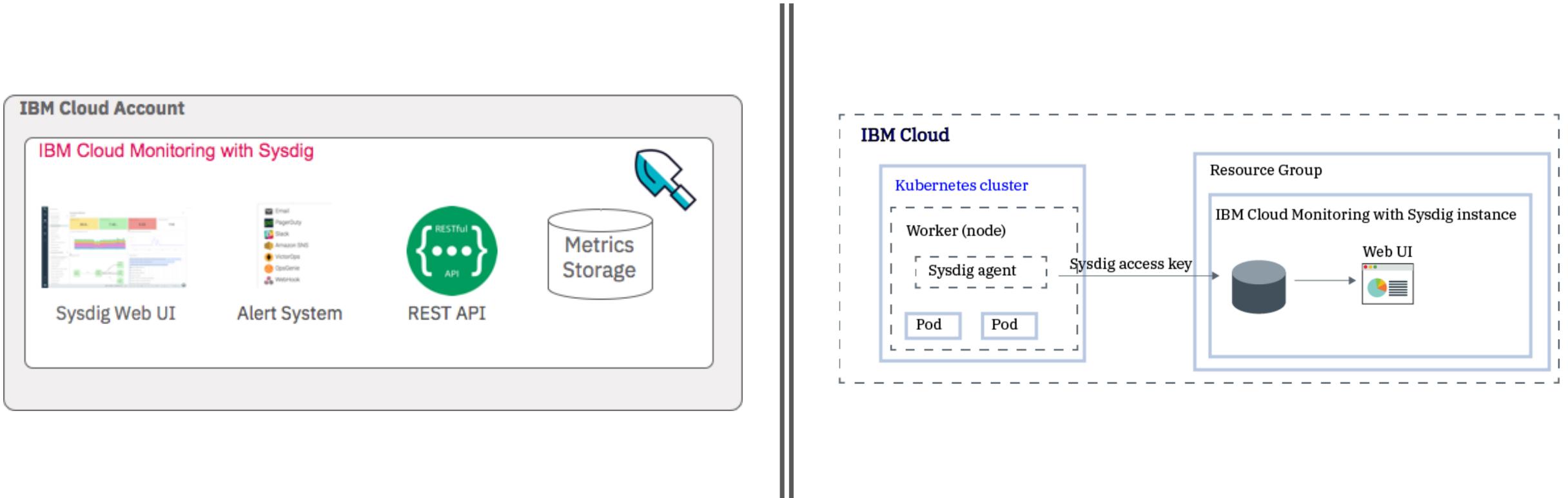
- **Optimized for modern container based applications**
- **Auto-collect and aggregate data** at scale from across services and infrastructure
- **Proactively alert** with configurable alerts
- **Visualize your environment** with customizable dashboards and at a glance views

Value Proposition

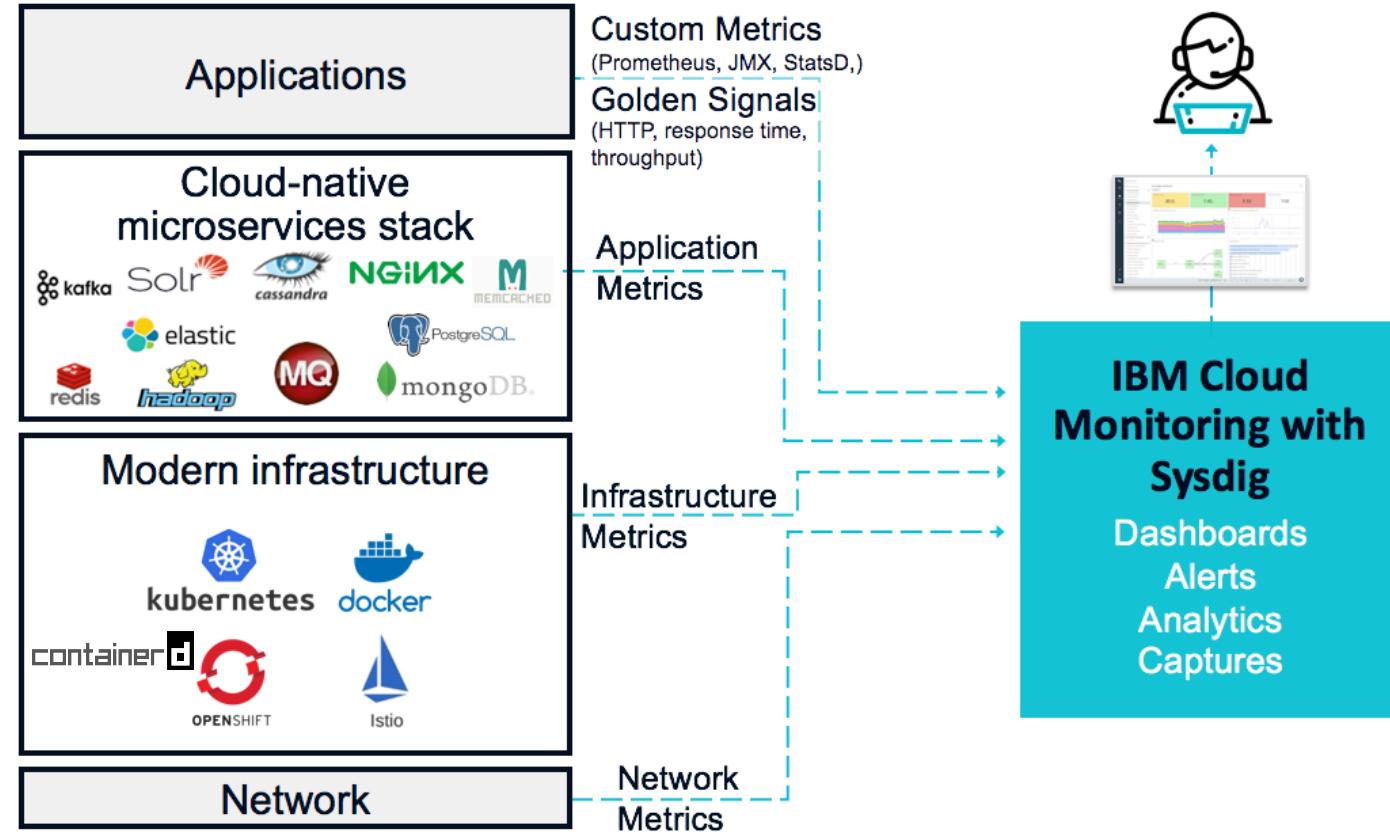
- Get critical Kubernetes and container insights for dynamic microservices
- Accelerate the diagnosis and resolution of performance incidents
- Easily explore and visualize your entire environment
- Auto-collect metrics and events including custom metrics: Prometheus, StatsD, JMX
- Mitigate the impact of abnormal situations with proactive alert notifications
- Control the cost of your monitoring infrastructure



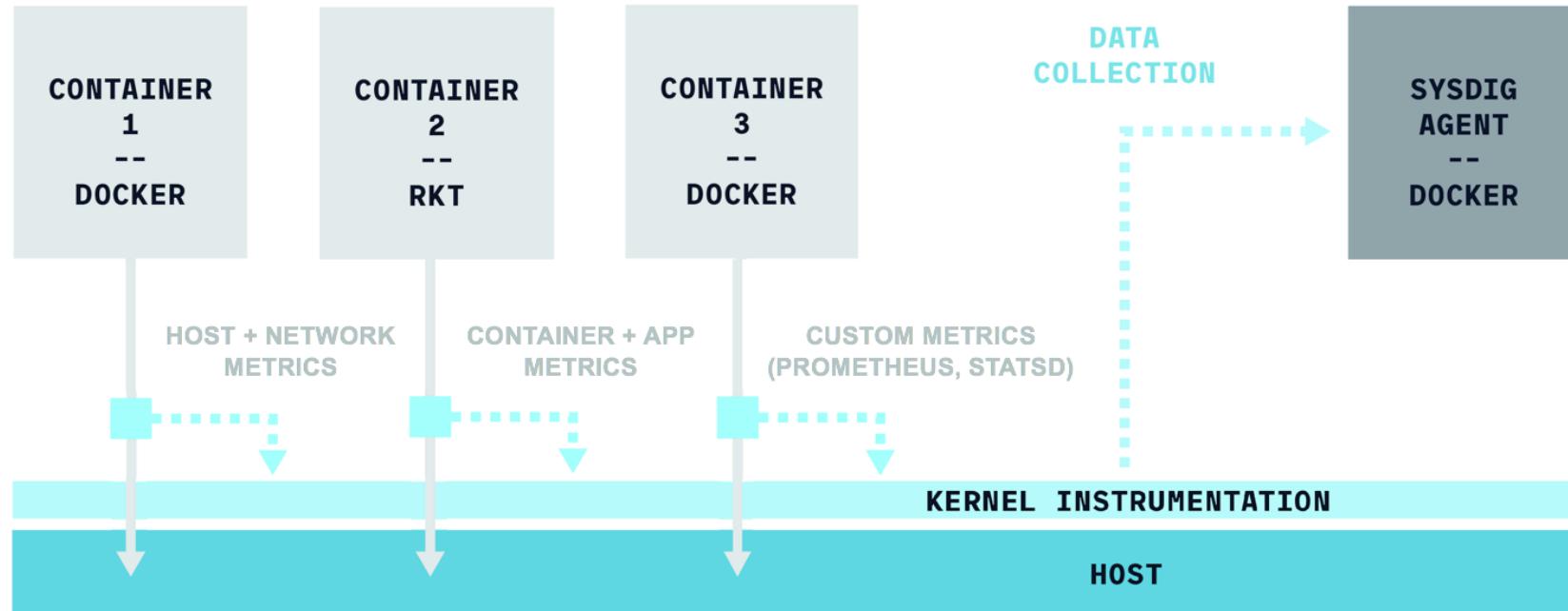
Component Overview



Metrics Across the Stack

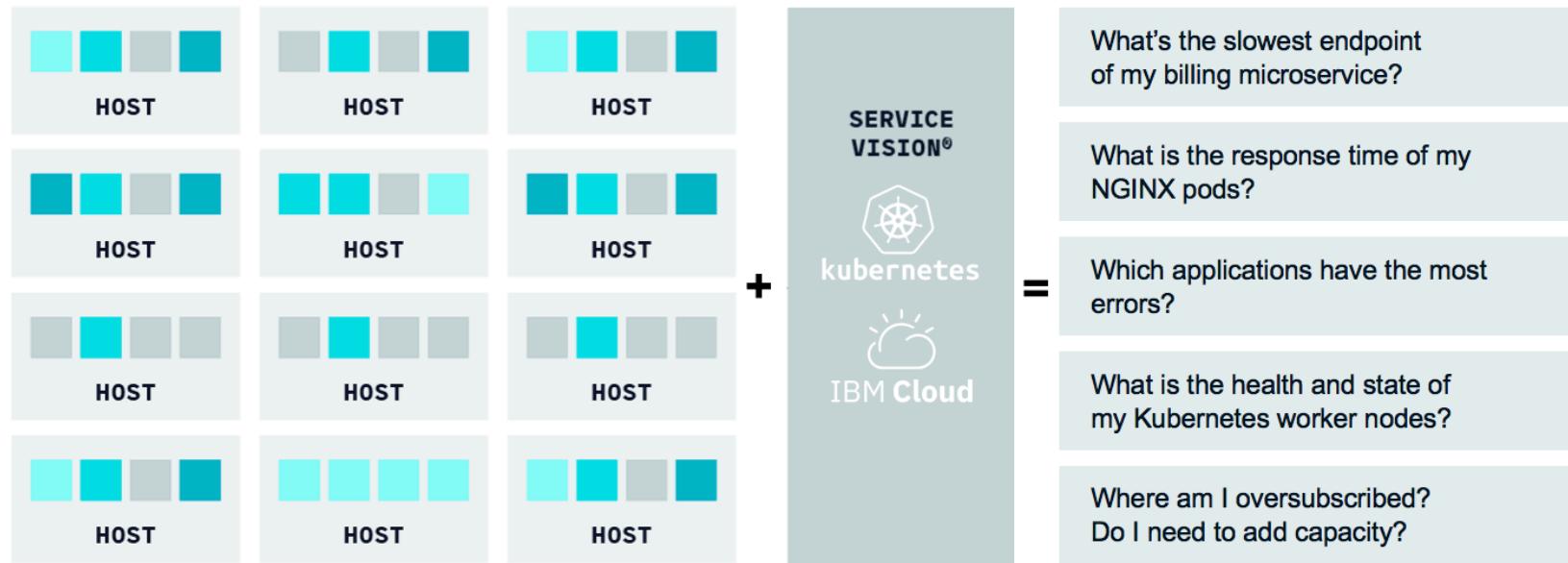


Microservice-Oriented Instrumentation



See all app, container, host, and network system calls.
Monitor, detect, and troubleshoot from a single instrumentation point.

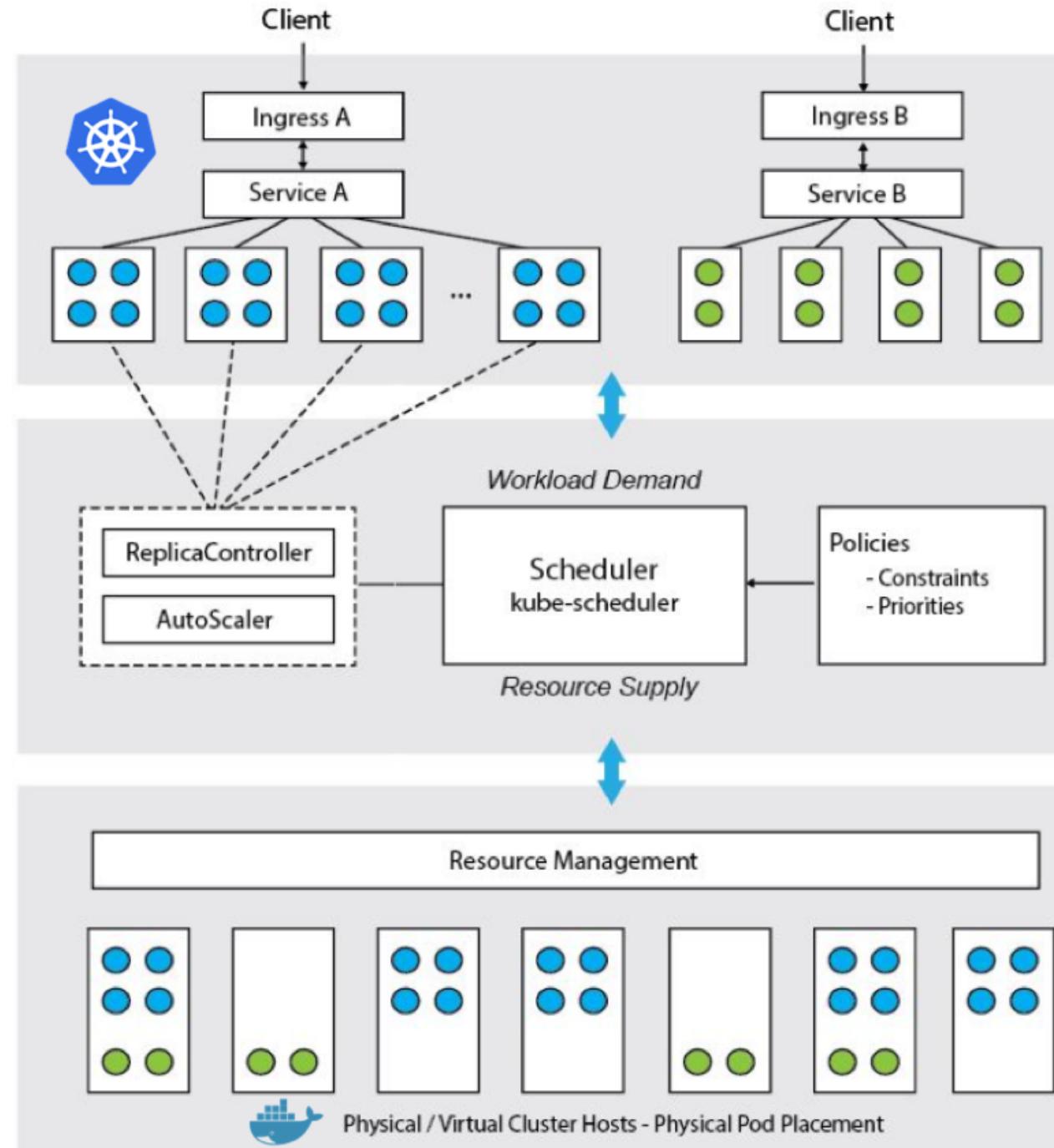
Service-Oriented Intelligence



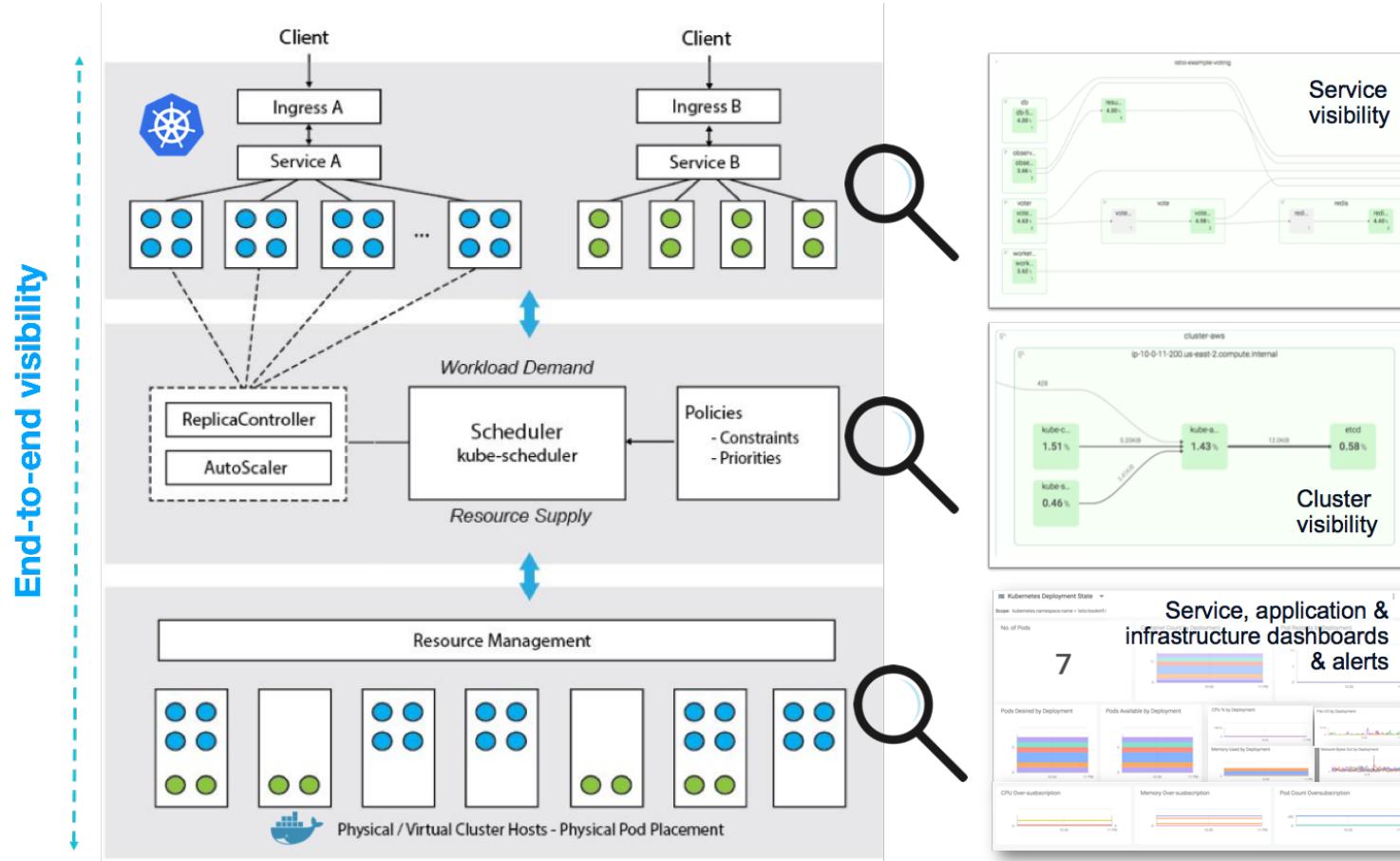
Enrich your metrics and events with orchestration metadata for context that exponentially increases the value of the information.

Delivering Deep Kubernetes Insights

- Dynamic discovery of micro- services
- Monitoring and alerting for kube components
- Auto-discovery and identification of container workloads



End to End Visibility



Comparing visibility solutions

APM

complimentary

Trace individual transactions from host to browser – monitor application code level performance



Infrastructure & Cloud Monitoring

View real-time performance and health of physical, virtual, and container hosts, orchestration, containers, processes, networks, and apps



Logging

complimentary

Collect, aggregate, and index log data to analyze events, usage and security issues – typically post-mortem



Pricing

PLAN	FEATURES	PRICING
 Trial	Data is collected for a maximum of 20 containers per node or for 200 custom metrics per node for 30 days only.	Free
Graduated Tier	<p>Automatic price tiers</p> <p>Basic: Data is collected for a maximum of 20 containers per node or for 200 custom metrics per node.</p> <p>Pro: Data is collected for a maximum of 50 containers per node or for 500 custom metrics per node.</p> <p>Advanced: Data is collected for a maximum of 110 containers per node or for 1000 custom metrics per node.</p> <hr/> <p>Note:</p> <ul style="list-style-type: none">- Data is collected and retained per the standard guidelines across all plans.- When the number of containers per node or the number of metrics goes above the graduated tier plan's threshold limit over a period of time, automatic tier detection is applied.- You can request a custom price quote for anything beyond the upper bound of the Advanced graduated tier paid pricing plan by opening a ticket with IBM Cloud Support	\$0.035 USD/Basic Instance-hour \$0.055 USD/Pro Instance-hour \$0.075 USD/Advanced Instance-hour



Regional Availability

Currently deployed in **Dallas, Frankfurt, London, Tokyo, Washington DC, and Sydney!**

Provisioning Entry Points

X

 Cloud Foundry

 Kubernetes

 Infrastructure

 VMware

 Dashboard

 APIs

 Apple Development New

 Blockchain

 DevOps

 Finance

 Functions

 Integrate

 Managed Solutions

 Mobile

 Observability

 Security

 Watson

 Web Apps

Catalog Docs Support Manage

Search for resource...

Observability

Get visibility into the performance and health of your resources. Troubleshoot apps and services, identify threats, detect performance issues, trigger alerts and more.



IBM Log Analysis with LogDNA

Use IBM Log Analysis with LogDNA to gain insights into your system and application logs.

Features include live logs, custom views, dashboards, and alerts. Choose from 7, 14, or 30 day log retention and have the ability to archive to IBM Cloud Object Storage to retain your logs for as long as you need. LogDNA integrates with IBM access control to quickly and tightly integrate into your application. [Learn more](#)

Create logging instance

IBM Cloud Monitoring with Sysdig

Use Sysdig to monitor the health of services and applications in IBM Cloud.

To set up monitoring, create a Sysdig instance in a Public Cloud region, and select the plan that is associated to it. The region defines where your metrics are centralized. The plan determines the features and retention period for your metrics. [Learn more](#)

Create monitoring instance

IBM Cloud Catalog Docs Support Manage

Search for resource... 1615269 - Shadi Albu...

Catalog

sysdig

All Categories (1) >

Developer Tools

 **IBM Cloud Monitoring with Sysdig**
Third Party
Offers visibility into the performance and health of your infrastructure and apps, in-depth troubleshooting, and alerting.

Compute
Containers
Networking
Storage
AI
Analytics
Databases
Developer Tools (1)
Integration
Internet of Things
Security and Identity
Starter Kits
Web and Mobile
Web and Application

Looking for more? Check out the IBM Cloud experimental services to try out experimental runtimes and services. [IBM Cloud Experimental Services](#)

Configuring the Sysdig Agent

1

Observability

Overview

Logging

Monitoring

The screenshot shows the IBM Cloud Observability Monitoring interface. At the top, there's a navigation bar with 'LOCATION All Locations' and a 'Create monitoring insta...' button. Below it, a main panel titled 'IBM Cloud Monitoring with Sysdig-Fast Start' contains three buttons: 'View Sysdig' (highlighted with a blue box), 'Edit sources', and 'View access keys'. A large arrow points from the 'Edit sources' button to a separate window labeled '2'. Another arrow points from the 'View access keys' button to a window labeled '3'. A final arrow points from the 'View access keys' button to a dashboard window labeled '4'.

Monitoring

LOCATION All Locations

Create monitoring insta...

IBM Cloud Monitoring with Sysdig-Fast Start

View Sysdig

Edit sources

View access keys

Graduated Tier plan

Edit plan

Monitoring / IBM Cloud Monitoring with Sysdig-Fast Start - Edit sources

2 IBM Cloud Monitoring with Sysdig-Fast Start - Edit sources

Add agents to desired sources

Kubernetes

Linux

Docker

Kubernetes

Complete the following steps to configure a Sysdig agent on a Kubernetes cluster that runs in the IBM Cloud Kubernetes Service:

Prerequisites

Download and install a few CLI tools and the IBM Kubernetes Service plugin

```
curl -sL https://ibm.biz/idx-installer | bash
```

You can also install the CLI tools by following the instruction [here](#).

3

IBM Cloud Monitoring with Sysdig-Fast Start

Ingestion Key for IBM Cloud Monitoring with Sysdig-Fast Start

Ingestion Key

This key is used for ingestion (write-only)

.....

Show

Close

4

Dashboard

IBM Cloud dashboard

Request Count 36.9/s

HTTP Error Count 2.53/s

Pod restart count 1

Node pod capacity 110

Number of Requests Over Time

Network & CPU

Slowest URLs

LIVE: 1:00 pm - 2:00 pm (1 H) PST 10 S 1M 1H 6H 1D 2W CUSTOM

2009/2010

The screenshot shows a modal dialog box titled 'Ingestion Key for IBM Cloud Monitoring with Sysdig-Fast Start'. It displays an 'Ingestion Key' field containing a long string of characters, with a 'Show' link next to it. There are 'View access keys' links at the bottom left and right. A 'Close' button is at the bottom right.

Observability

LOCATION All Locations

Create monitoring insta...

IBM Cloud Monitoring with Sysdig-Fast Start

Ingestion Key for IBM Cloud Monitoring with Sysdig-Fast Start

Ingestion Key

This key is used for ingestion (write-only)

.....

Show

View access keys

Close

View access keys

Deep Dive

Data Locality

- Metrics data is hosted on the **IBM Cloud**
- Metrics data is **collected in the region where the instance is provisioned**
- Metrics data can be collected from:
 - Kubernetes
 - Linux (including resource metrics, CPU, memory, disk, network)
 - Docker
 - Applications
 - Custom metrics
- Each multi zone region (MZR) location collects and aggregates metrics for each instance of the IBM Cloud Monitoring with Sysdig that runs in that location

Data Collection and Availability

- When you configure a Sysdig agent to collect and forward data to an **IBM Cloud Monitoring with Sysdig** instance, data is automatically collected and available for analysis through the Sysdig web UI.
 - Data is **collected at 10 second** frequency
 - Data is **available** for maximum of **15 months**
- Data is available for analysis through the web UI for the time period that the agent was installed and reporting metrics.
- After you delete an instance of IBM Cloud Monitoring with Sysdig, data is no longer available for search and analysis. You may also remove a Sysdig agent from the host / container, however historical data is not deleted immediately.

Data Retention

- Data is retained for each instance based on a roll-up policy
- As time progresses the data is rolled up from a fine granularity to coarser one by the end of 3 months
- The roll-up policy describes the granularity of the data over time:
 - Data is retained at 10 sec resolution for the first 4 hours
 - Data is retained at 1 min resolution for 2 days
 - Data is retained at 10 min resolution for 2 weeks
 - Data is retained at 1 hour resolution for 3 months
 - Data is retained at 1 day resolution for one year

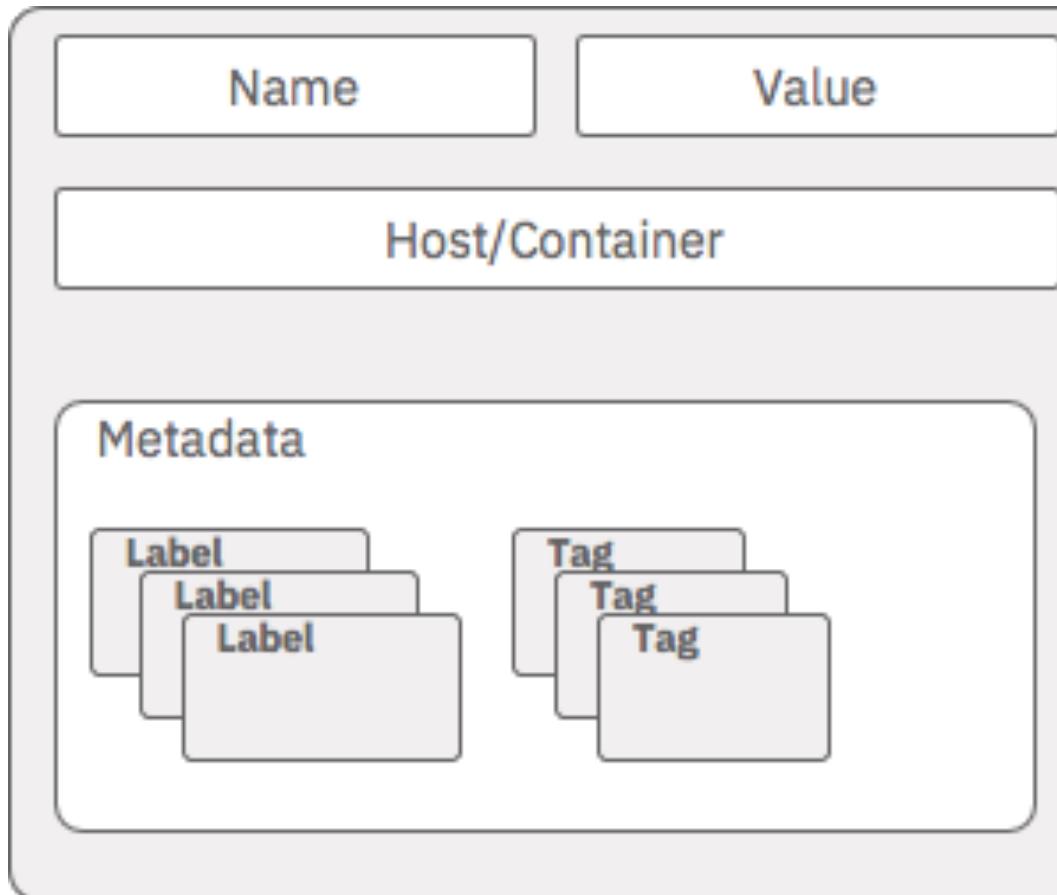
IAM Cloud Platform Roles for IBM Cloud Monitoring with Sysdig

Platform actions	IBM Cloud Platform Roles
Grant other account members access to work with the service	Administrator
Provision a service instance	Administrator Editor
Delete a service instance	Administrator Editor
Create a service ID	Administrator Editor
View details of a service instance	Administrator Editor Operator Viewer
View service instances in the Observability Monitoring dashboard	Administrator Editor Operator Viewer

Roles Comparison

Platform actions	IBM Cloud Platform Roles	Actions	Sysdig role
Grant other account members access to work with the service	Administrator	Reset the Sysdig access key	Admin
Provision a service instance	Administrator Editor	Manage users	Admin
Delete a service instance	Administrator Editor	Create, configure, and delete teams	Admin
Create a service ID	Administrator Editor	Configure and remove notifications channels	Admin
View details of a service instance	Administrator Editor Operator Viewer	Configure and remove Sysdig agents	Admin
View service instances in the Observability Monitoring dashboard	Administrator Editor Operator Viewer	Create, delete, and edit content in the Sysdig web UI	Admin User
		View metrics through the Sysdig Web UI	Admin User
		Create and delete alerts	Admin User
		Create and delete captures	Admin User

What are Data-points?



- Includes a name, value, container/host it came from and all associated metadata
- Metadata associated with a metric defines the characteristics of that metric
- Labels identify objects within the infrastructure and are obtained directly from the infrastructure source i.e. *kubernetes.pod.name*
- Tags define custom metadata in form of key-value pairs that can be obtained from integrations like StatsD, Prometheus, and JMX
- Datapoints are aggregated or filtered by using labels, tags, or both

Kubernetes Labels

Kubernetes labels are **key-value pairs** that specify attributes of objects such as pods.

Example Label Component	Description
Kubernetes	Infrastructure Type
pod	Object
name	Label Key

- You can define labels for objects at creation time. After an object is created, you can also add and modify labels at any time.
- Each Key must be unique for a given object.

Adding Tags to a Kubernetes Cluster

Customize the Sysdig agent to add metric descriptors (tags).

- 1 Edit the *sysdig-agent-configmap.yaml* file

```
kubectl edit configmap sysdig-agent
```

- 2 Add tags

```
apiVersion: v1
data:
  dragent.yaml: |
    k8s_cluster_name: marisa-production
    collector: ingest.us-south.monitoring.cloud.ibm.com
    collector_port: 6443
    ssl: true
    sysdig_capture_enabled: false
    new_k8s: true
    tags: department:finance,region:us-south
  ...
  ...
```

What are Groups?

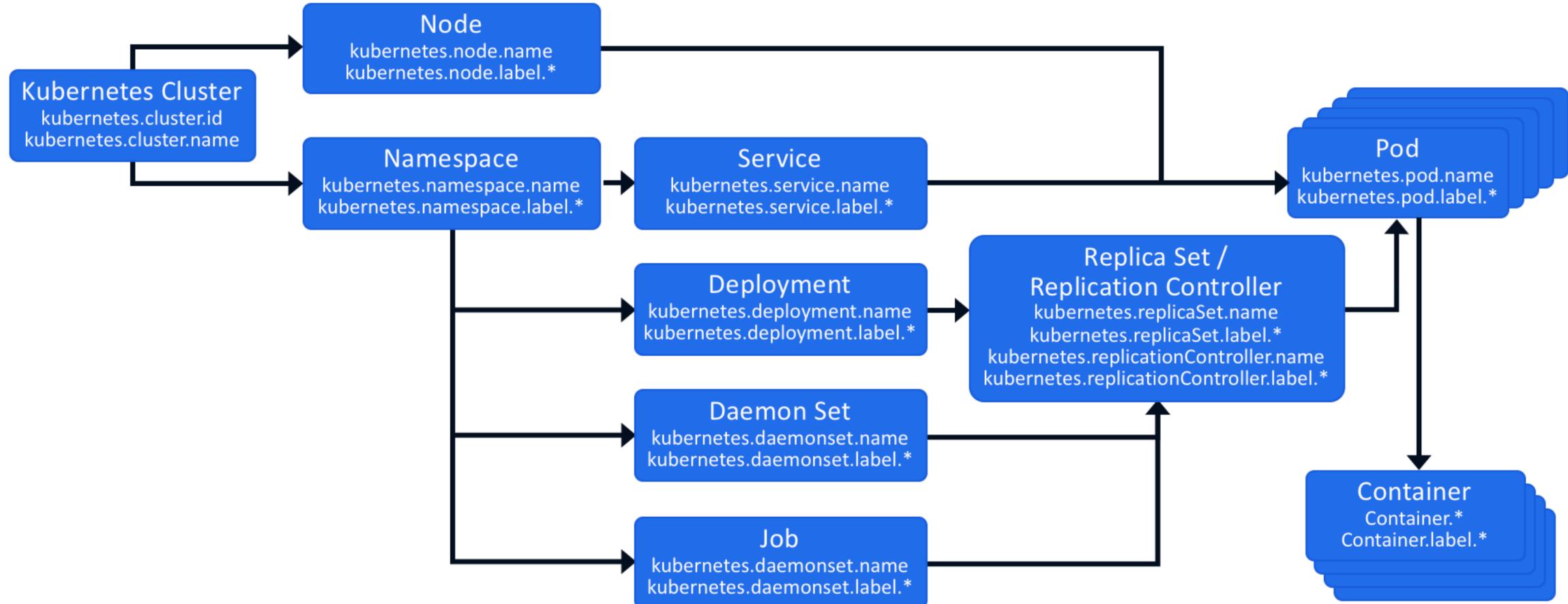
Groups organize infrastructure objects into logical hierarchies.

The screenshot shows the IBM Cloud Monitoring Explore interface at the URL <https://us-south.monitoring.cloud.ibm.com/#/explore/overview/l:1200>. The left sidebar has icons for EXPLORE (selected), DASHBOARDS, ALERTS, EVENTS, and CAPTURES. The main area shows a grouping named "MyHostsGroup" under "MY GROUPINGS". A search bar says "Search groupings to parse your infrastructure". To the right is a table with one row:

	cpu.used.percent %
	3.4
	4.5
	3.0
	2.2

At the bottom of the grouping list, there is a link "SHOW 17 INAPPLICABLE GROUPINGS".

Logical Hierarchy for Kubernetes Objects



Scope

Scope is a collection of labels that define the conditions to filter out data points when you create dashboards and panels, configuration alerts, and customize events.

The screenshot shows the IBM Cloud Monitoring dashboard interface at the URL <https://us-south.monitoring.cloud.ibm.com/#/dashboards/322/l1200>. The main title is "HTTP Overview". On the left, there's a sidebar with "Dashboards" and "My Dashboards" sections. The main area displays two charts: "Top URLs by Number of Requests" and "Top URLs by Number of Requests". The "Scope" dropdown is set to "everywhere". A modal window titled "Scope" is open, listing various labels under "Segment by": agent.id, agent.version, container.id, container.image, container.image.digest, container.image.repo, and container.image.tag. The "Display" dropdown is set to "Top 10 segments". The "Edit Scope" button is highlighted with a blue star.

Data Aggregation

Aggregation of data occurs automatically when you configure a graph or create an alert for a metric.

There are two types of aggregation:

- Time aggregation
- Group aggregation.

Time aggregation is always performed before group aggregation.

To create multi-series comparisons and multiple alerts, you can also split aggregated data into smaller sections called **segments** by using labels.

Time Aggregation

By default, a Sysdig agent collects and reports metrics at a 10 second resolution.

In Time series charts that include data for five minutes or less, data points are drawn at 10 second resolution. Time aggregation does not occur.

Aggregation type	Description
average	Average of the retrieved metric values across the time period evaluated.
rate (timeAvg)	Average value of the metric across the time period evaluated.
maximum	Highest value during the time period evaluated.
minimum	Lowest value during the time period evaluated.
sum	Combined sum of the metric across the time period evaluated.

Group Aggregation

By default, metrics that are applied to a group of resources, such as several containers, hosts, or nodes, are averaged between the members of the group.

In Time series charts that include data for five minutes or less, data points are drawn at 10 second resolution. Time aggregation does not occur.

Aggregation type	Description
average	Average value of the interval's samples.
maximum	Highest value of the interval's samples.
minimum	Lowest value of the interval's samples.
sum	Combined value of the interval's samples.

Teams

Teams group users and control the data and the permissions to work with Sysdig captures and infrastructure events for those users.

- A Sysdig administrator can define any number of teams
- For each team the administrator can configure the following information:
 - Entry point – Specify the view in the web UI that opens every time a user logs in [Explore View, Dashboards View, Alerts View, Settings View]
 - Scope – You can limit what data users can see [Host or Container + conditions]
 - Permissions – Enable or disable following features Sysdig Captures and/or Infrastructure Events

Managing Data

- Use labels to:
 - Group infrastructure resources into logical hierarchies
 - Filter out data
 - Split aggregated data into segments.
- Customize how data is aggregated when you configure a graph or create an alert for a metric.
- Set the scope of a dashboard, a panel, or an alert to filter out data points.
- Restrict access to data by managing users' data access through teams.

Labels are used to identify infrastructure objects and metrics are aggregated or filtered by these labels.

Alerts

- Notifies users when an event/issue occurs that requires their attention
- Five types of alerts available in Sysdig Monitor:
 - Downtime
 - Metric
 - Event
 - Anomaly Detection
 - Group Outlier
- Multiple ways to access Alert Wizard [Explore table, Dashboards module, Alerts module]
- Can be managed individually or as a group and can be enabled/disabled
- When an alert notification is sent, it contains: name of the alert, type of notification (active, resolved, OK), and the value of the segmentation i.e. segmenting a host.hostName, relevant host.Name will be provided

The screenshot shows the 'Define' step of the Alert Wizard. The alert is titled 'Too many container restarts' with a description 'Too many pod restarts, probably in CrashLoopBackOff state'. The status is set to 'warning'. The configuration includes:

- Metric:** Average of kubernetes.pod.restart.count
- Scope:** kubernetes.namespace.name in prod. A dropdown menu labeled 'Select scope' is shown.
- Trigger:** If metric > 4 for the last 2 minute(s) on average. A dropdown menu labeled 'Multiple Alerts' is shown, with the option 'Trigger a separate alert for each kubernetes.pod.name' selected.

At the bottom right, there is a button labeled '+ Add another'.

Resources

- [IBM Cloud Monitoring with Sysdig](#)
- [Observability in IBM Cloud](#)
- [Documentation](#)