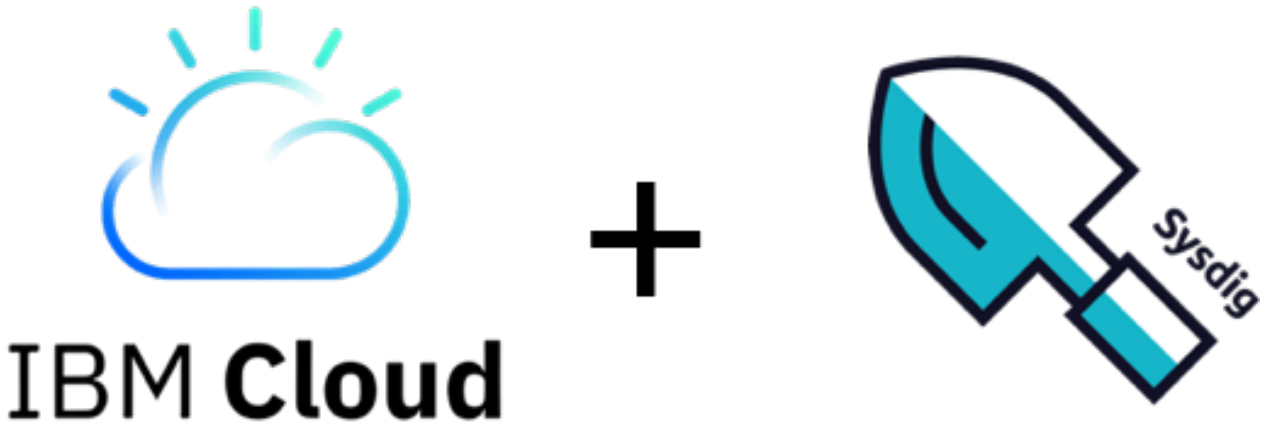
IBM Cloud Monitoring with Sysdig

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.

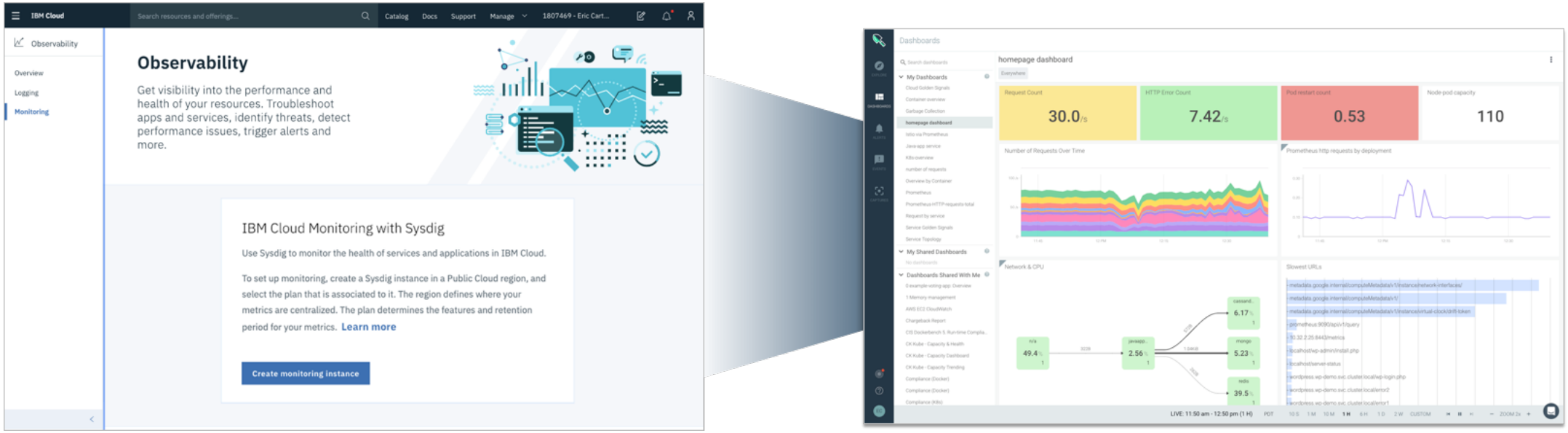
Partnership



IBM 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.

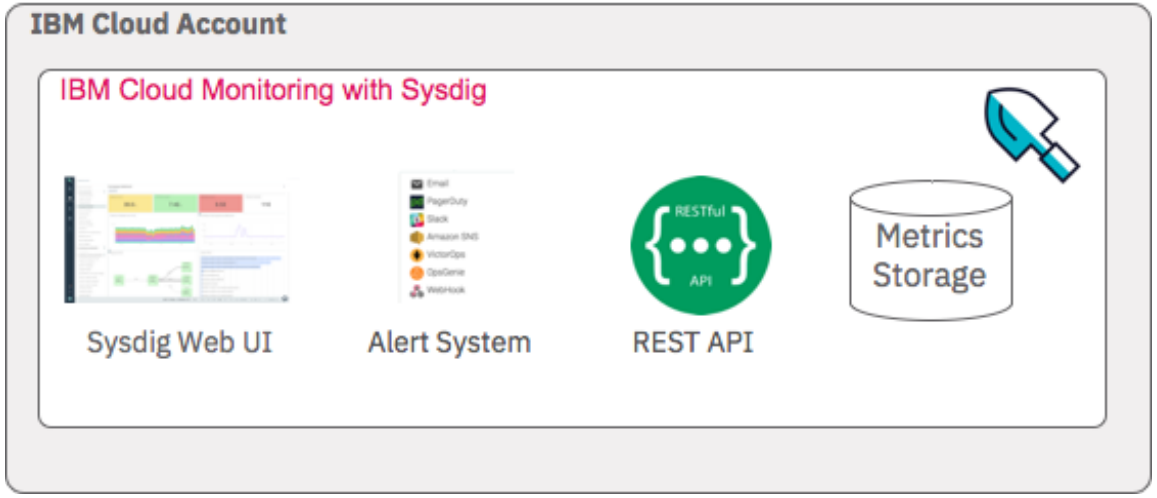


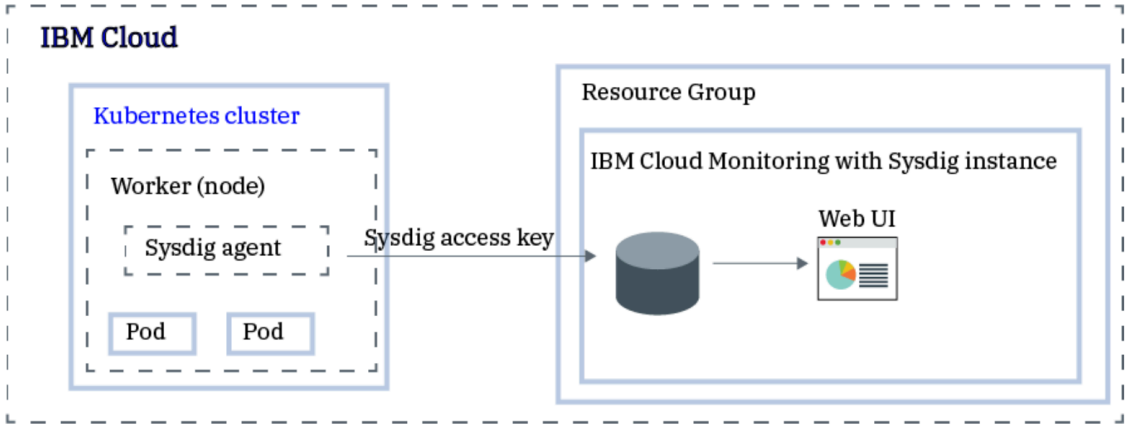
- **Optimized** for modern container based applications
- **Auto-collect and aggregate data** at scale from across services and infrastructure
- **Proactively alert** with configurable alerts
- **Visualize your environment** with customizable dashboards and at a glance views

Value Proposition

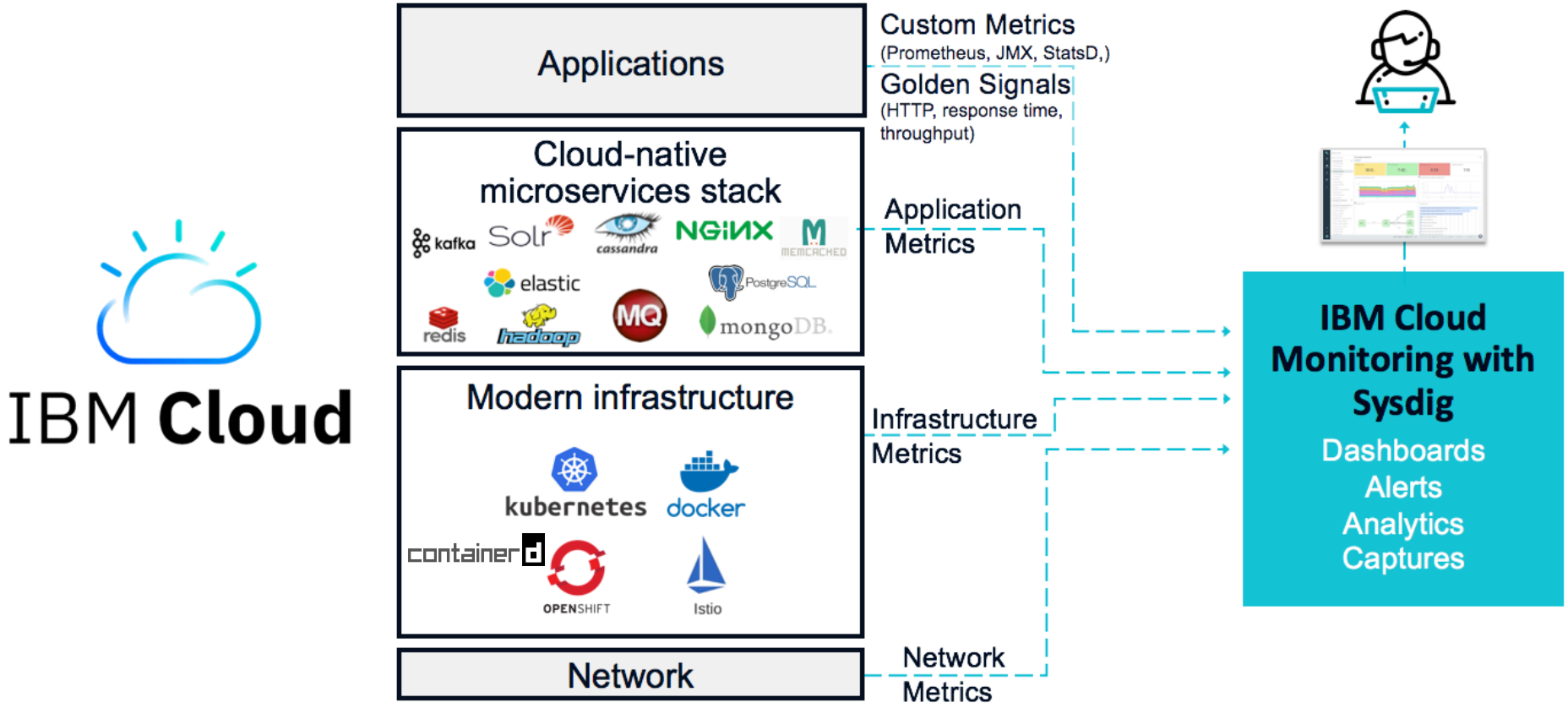
- Get critical Kubernetes and container insights for dynamic microservices
- Accelerate the diagnosis and resolution of performance incidents
- Easily explore and visualize your entire environment
- Auto-collect metrics and events including custom metrics: Prometheus, StatsD, JMX
- Mitigate the impact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

Component Overview

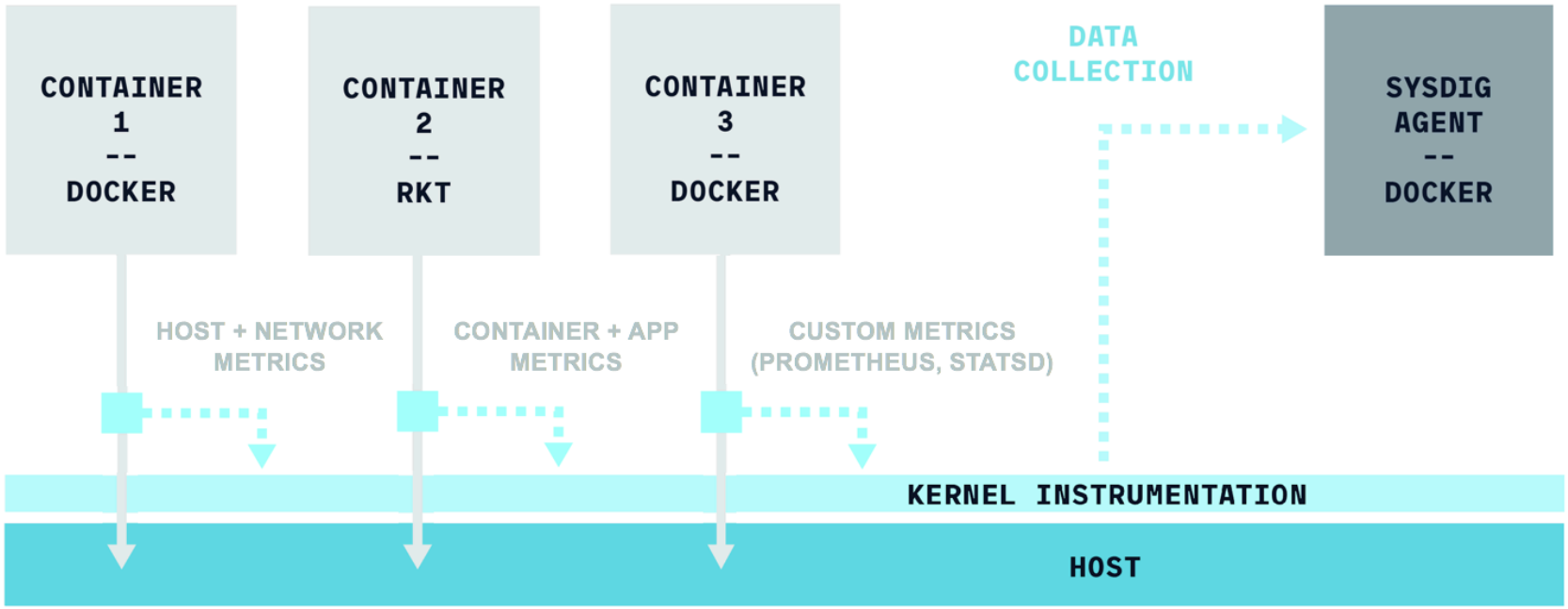




Metrics Across the Stack

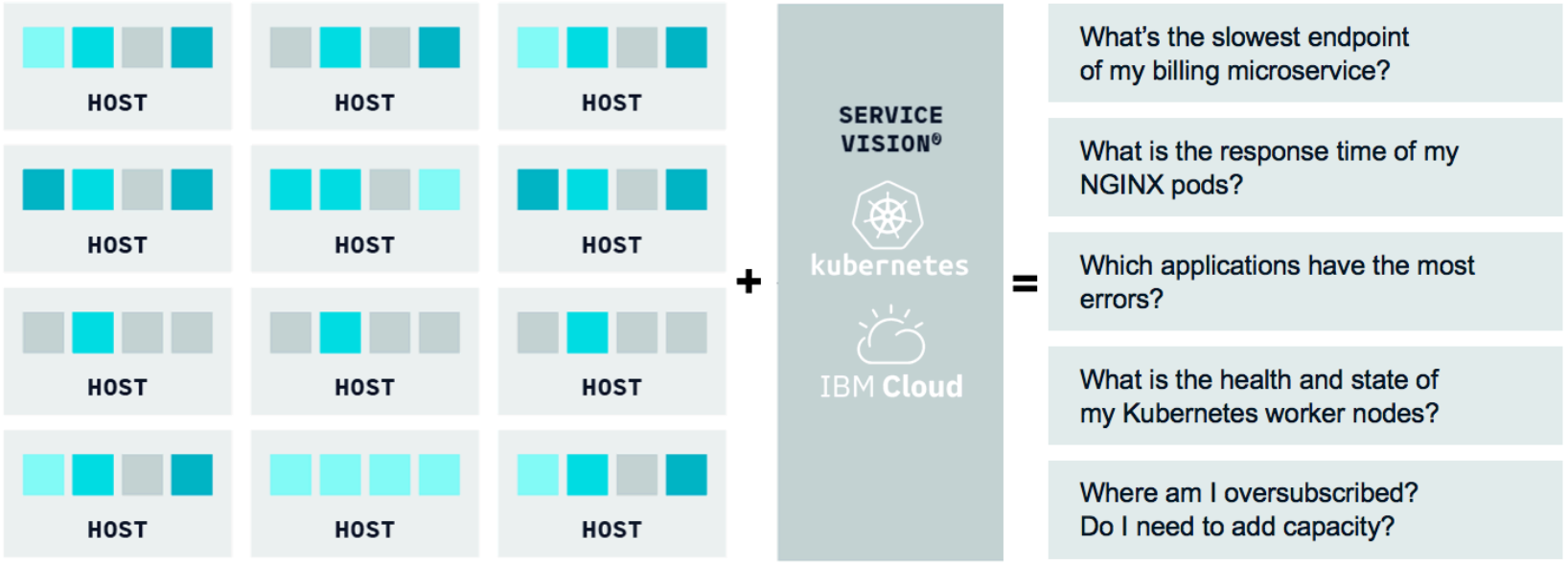


Microservice-Oriented Instrumentation



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

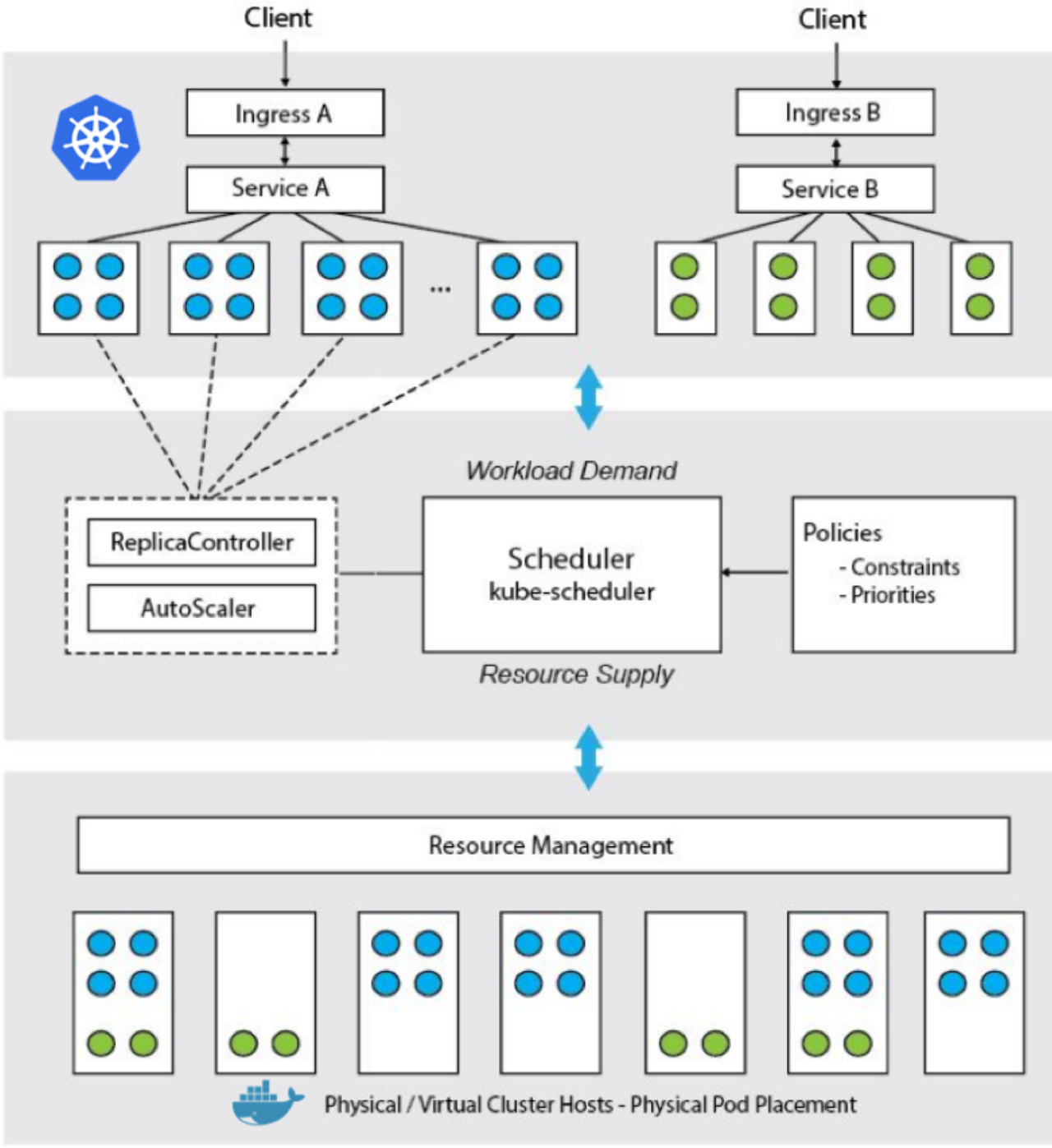
Service-Oriented Intelligence



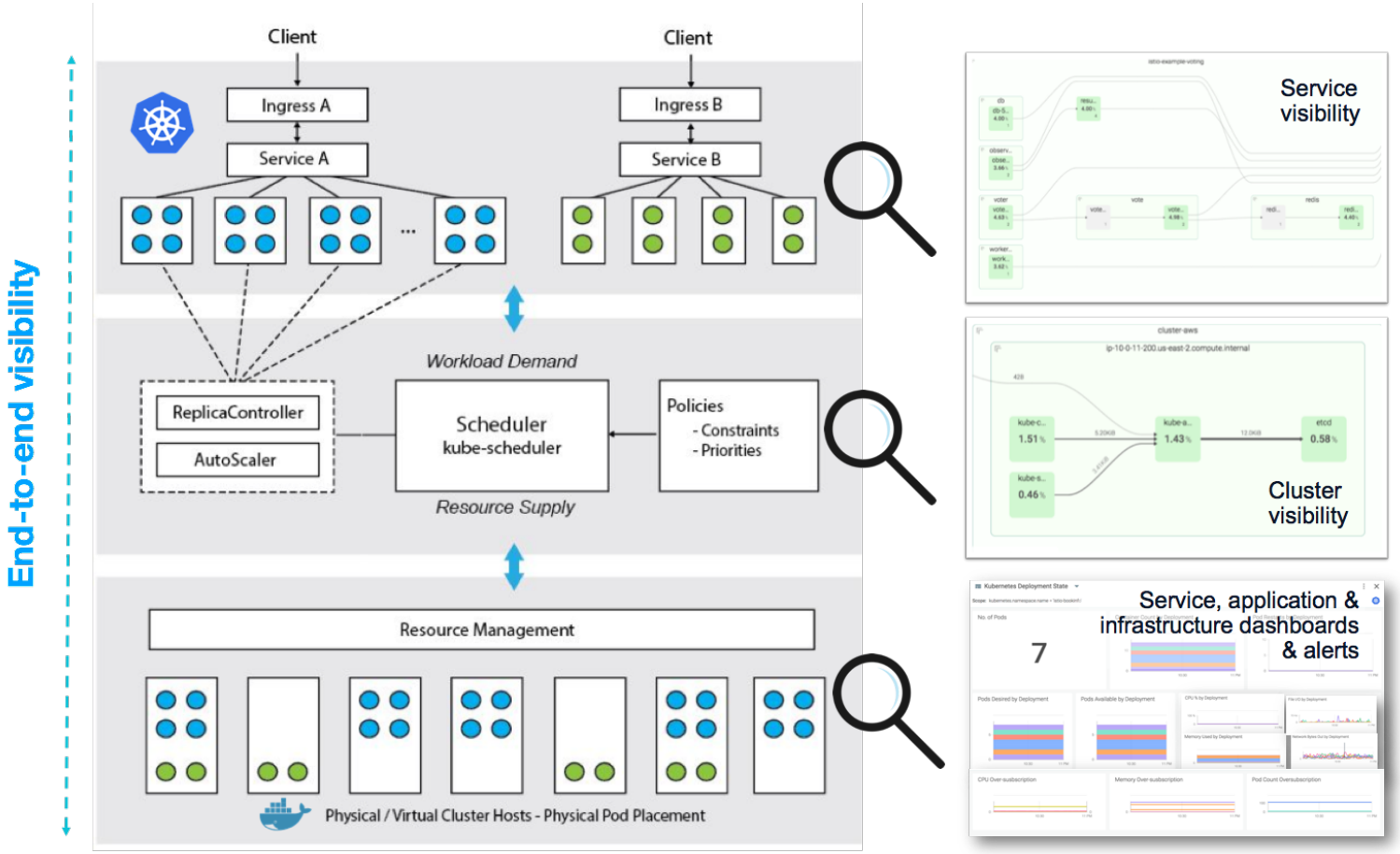
Enrich your metrics and events with orchestration metadata for context that exponentially increases the value of the information.

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	Infrastructure & Cloud Monitoring	Logging
complimentary Trace individual transactions from host to browser –monitor application code level performance  	View real-time performance and health of physical, virtual, and container hosts, orchestration, containers, processes, networks, and apps   	*complimentary* Collect, aggregate, and index log data to analyze events, usage and security issues – typically post-mortem   

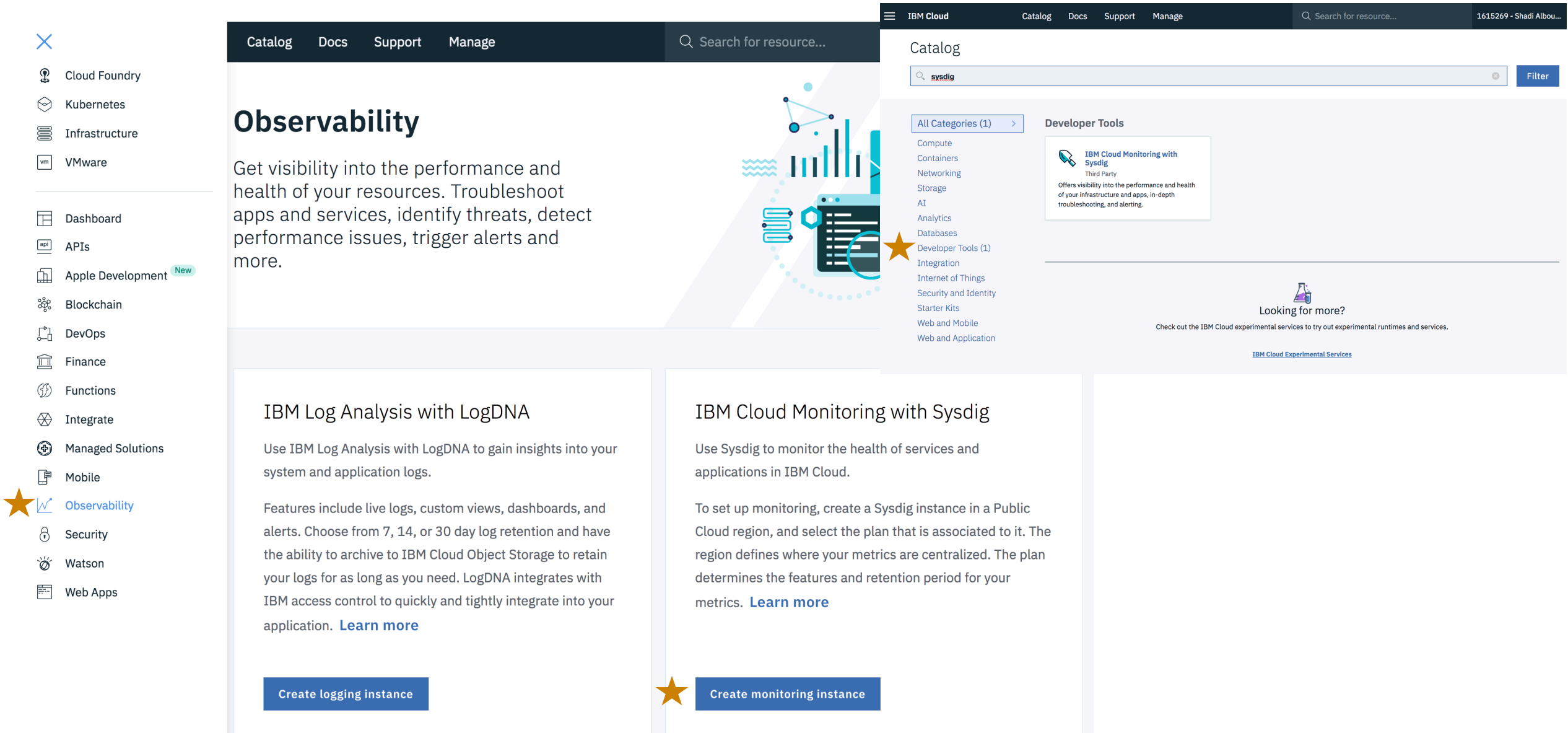
Pricing

	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	**Automatic price tiers** **Basic:** Data is collected for a maximum of 20 containers per node or for 200 custom metrics per node. **Pro:** Data is collected for a maximum of 50 containers per node or for 500 custom metrics per node. **Advanced:** Data is collected for a maximum of 110 containers per node or for 1000 custom metrics per node. ---------- Note: - 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

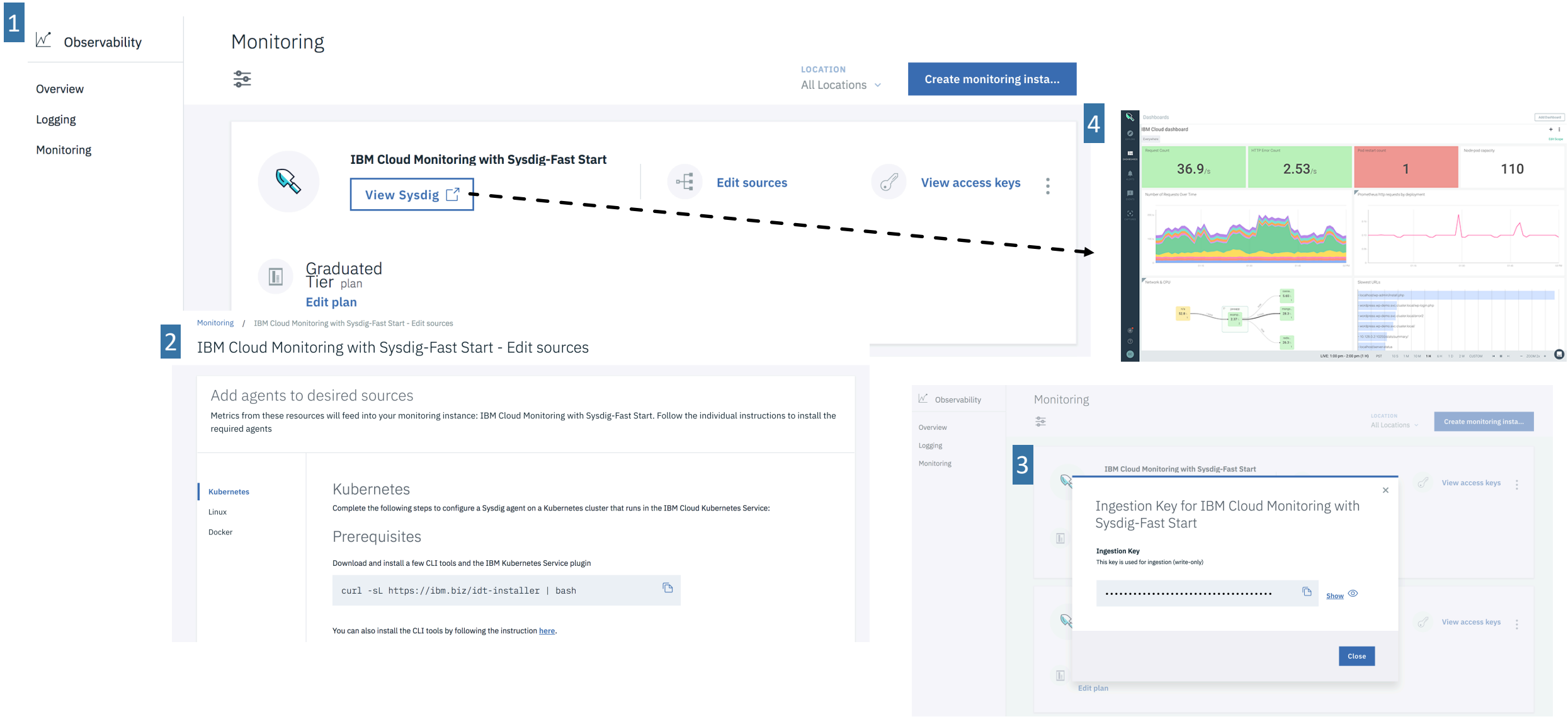
Regional Availability

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

Provisioning Entry Points



Configuring the Sysdig Agent



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.

Check the docs for recent update: https://cloud.ibm.com/docs/Monitoring-with-Sysdig?topic=Monitoring-with-Sysdig-about

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

Check the docs for recent update: https://cloud.ibm.com/docs/Monitoring-with-Sysdig?topic=Monitoring-with-Sysdig-about

IAM Cloud Platform Roles for IBM Cloud Monitoring with Sysdig

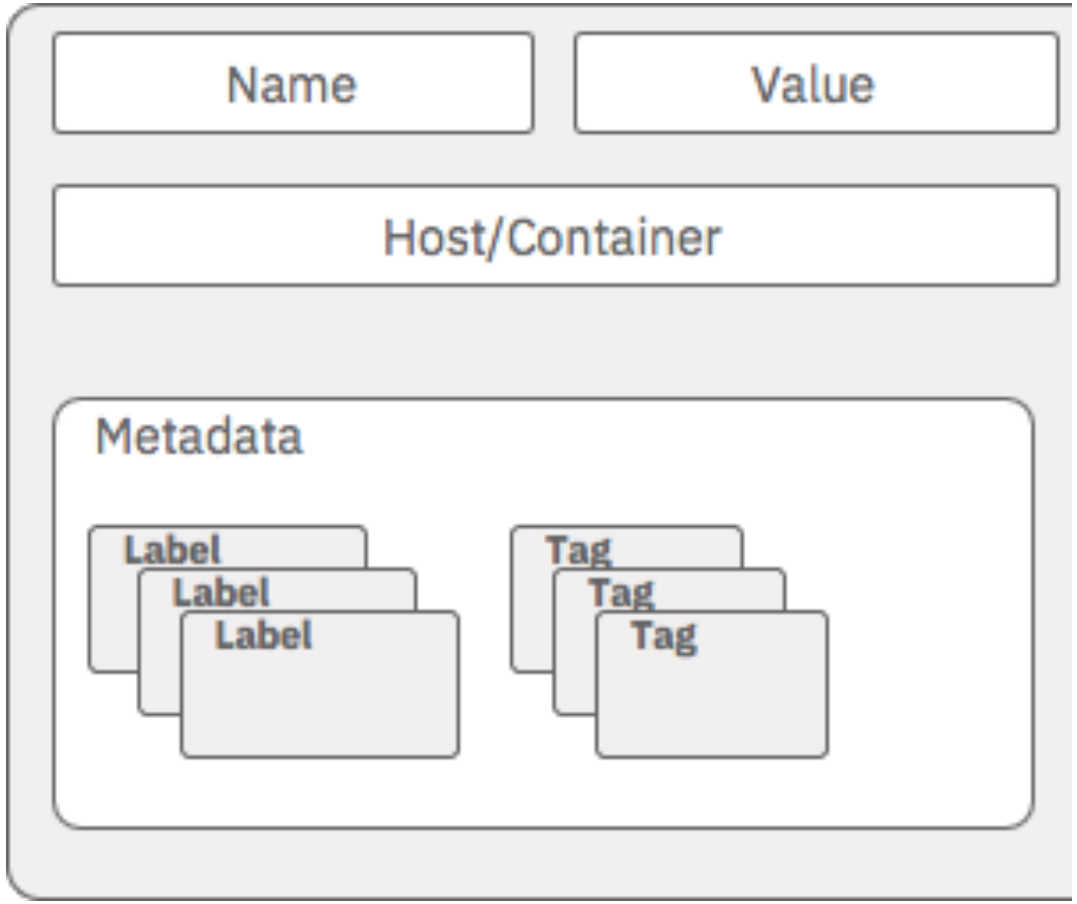
Platform actions	IBM Cloud Platform Roles
Grant other account members access to work with the service	Administrator
Provision a service instance	Administrator Editor
Delete a service instance	Administrator Editor
Create a service ID	Administrator Editor
View details of a service instance	Administrator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

Roles Comparison

Platform actions	IBM Cloud Platform Roles
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

Actions	Sysdig role
Reset the Sysdig access key	Admin
Manage users	Admin
Create, configure, and delete teams	Admin
Configure and remove notifications channels	Admin
Configure and remove Sysdig agents	Admin
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 paris 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
```

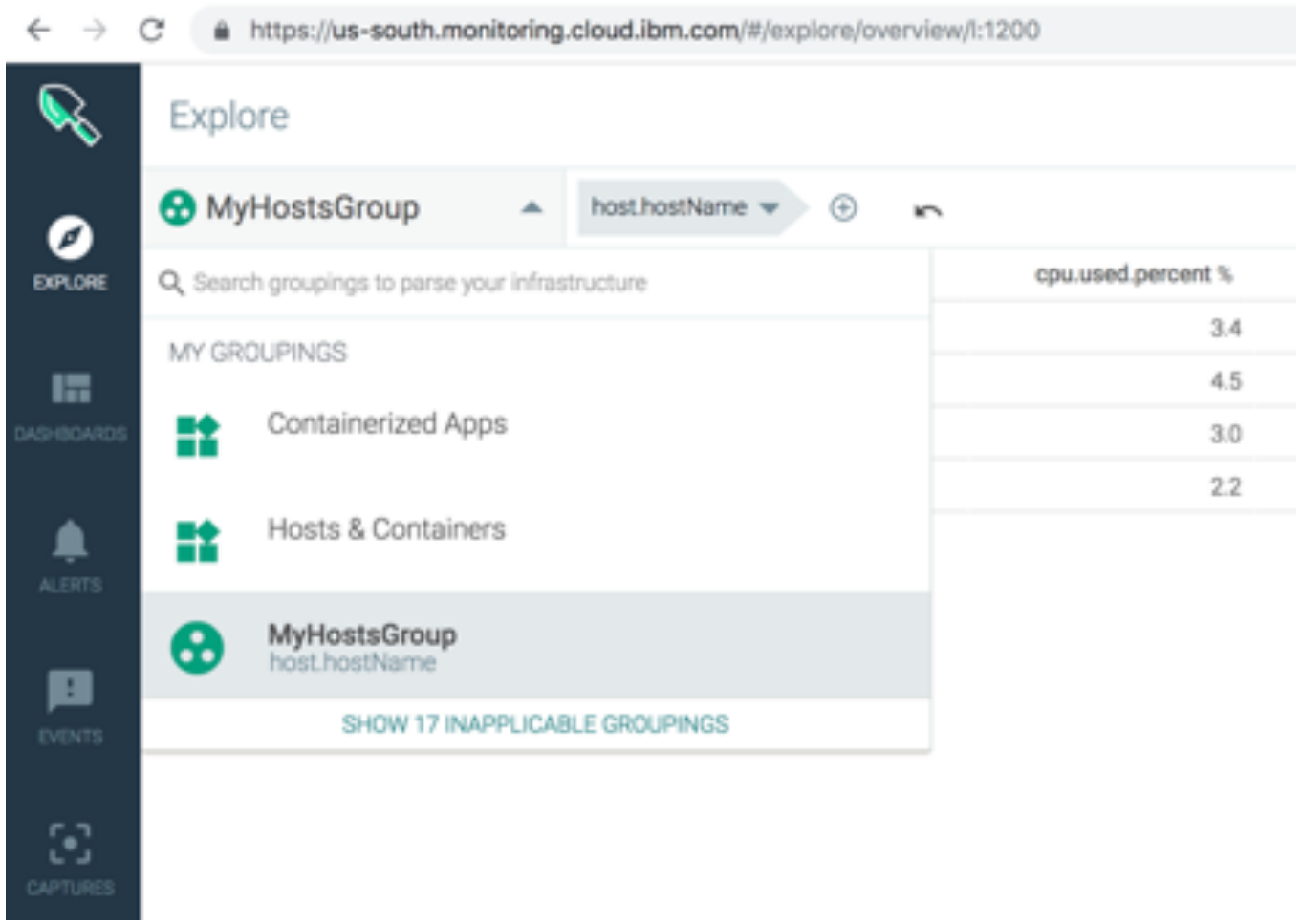
2. Add tags

```
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
  ...
```

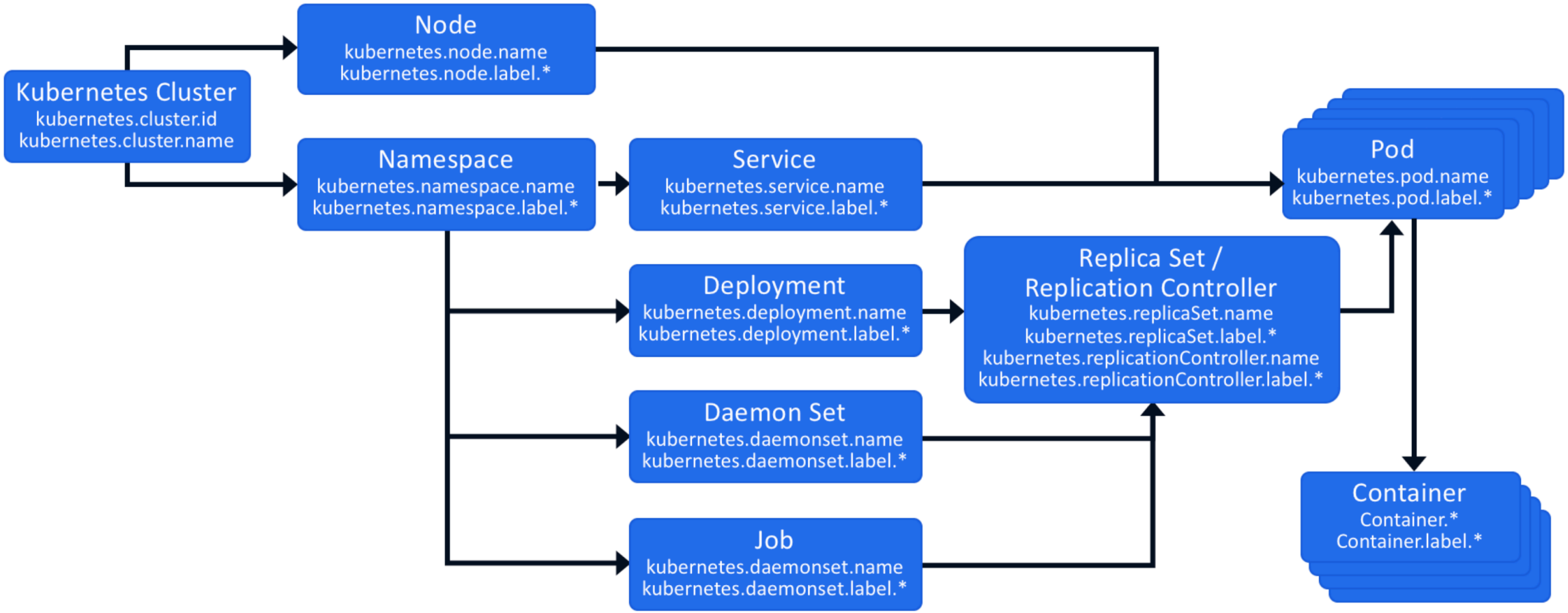
Note: You can customize the Sysdig agent configuration file to include custom metrics such as JMX, StatsD, and Prometheus

What are Groups?

Groups organize infrastructure objects into logical hierarchies.

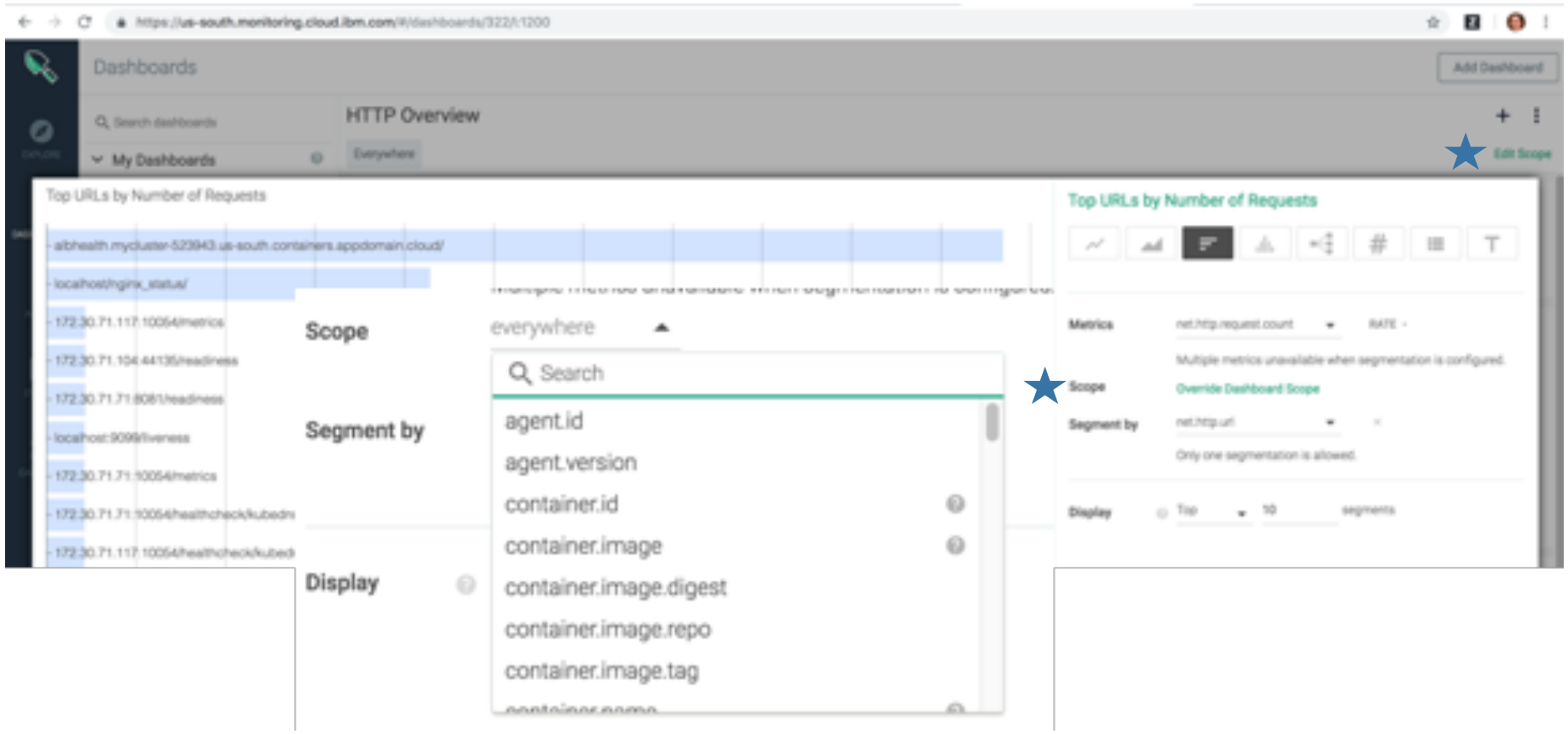


Logical Hierarchy for Kubernetes Objects



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.



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.

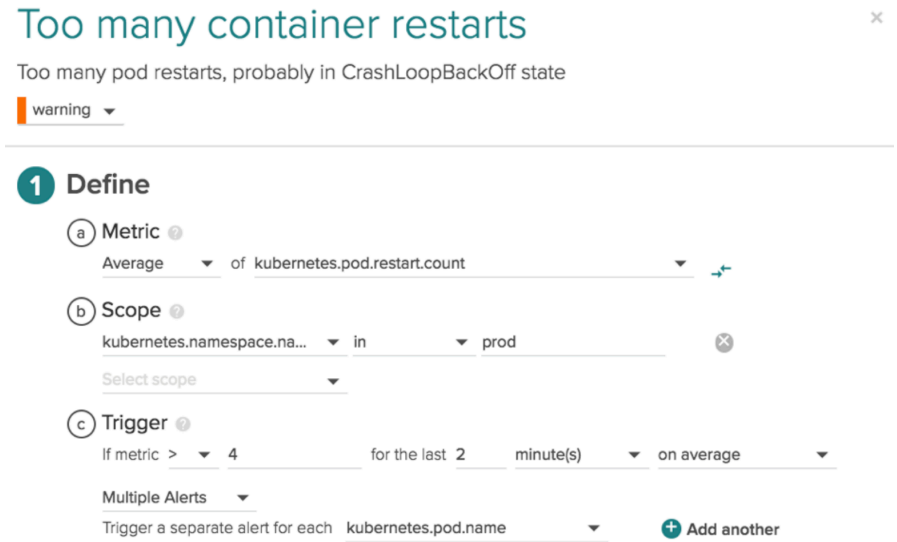
- Set the scope of a dashboard, a panel, or an alert to filter out data points.

- 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
  - Anomoly 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

Resources

- IBM Cloud Monitoring with Sysdig
- Observability in IBM Cloud
- Documentation