

Datadog Monitoring

Rajesh Kumar

www.DevOpsSchool.com

Types of Monitoring

 Host

 Metric

 Anomaly

 Outlier

 Forecast →

 Integration

 Live Process

 Process Check

 Network

 Custom Check

 Custom Check

 Event

 APM

 Real User Monitoring

 Watchdog

 Composite

 Import →

Types of Monitoring

- [Host](#) - Check if one or more hosts are reporting to Datadog.
- [Metric](#) - Compare values of a metric with a user-defined threshold.
- [Anomaly](#) - Detect anomalous behavior for a metric based on historical data.
- [Outlier](#) - Alert on members of a group behaving differently than the others.
- [Forecast](#) - Alert when a metric is projected to cross a threshold.
- [Integration](#) - Monitor metric values or health status from a specific integration.
- [Live Process](#) - Check if one or more processes are running on a host.
- [Process Check](#) - Watch the status produced by the `process.up` service check.
- [Network](#) - Check the status of TCP/HTTP endpoints.
- [Custom Check](#) - Monitor the status of arbitrary custom checks.
- [Event](#) - Monitor events gathered by Datadog.
- [Logs](#) - Monitor logs gathered by Datadog.
- [APM](#) - Compare an APM metric to a user-defined threshold.
- [Real User Monitoring](#) - Monitor real user data gathered by Datadog.
- [Watchdog](#) - Get notified when Watchdog detects anomalous behavior.
- [Composite](#) - Alert on an expression combining multiple monitors.

Detection Methods

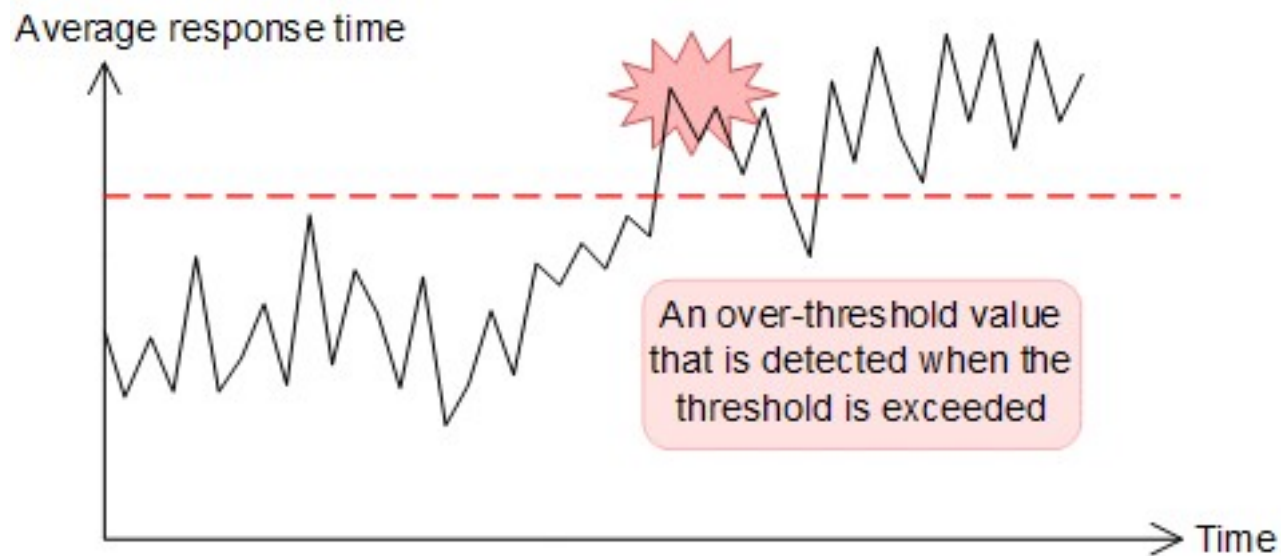
Detection Methods

- Threshold Alert
- Change Alerts
- Anomaly Detection
- Outliers Alert
- Forecast Alert

Detection Methods: Threshold Alert

- An alert is triggered whenever a metric crosses a threshold.

Detection Methods: Threshold Alert



Legend:

--- : Threshold

— : Service performance

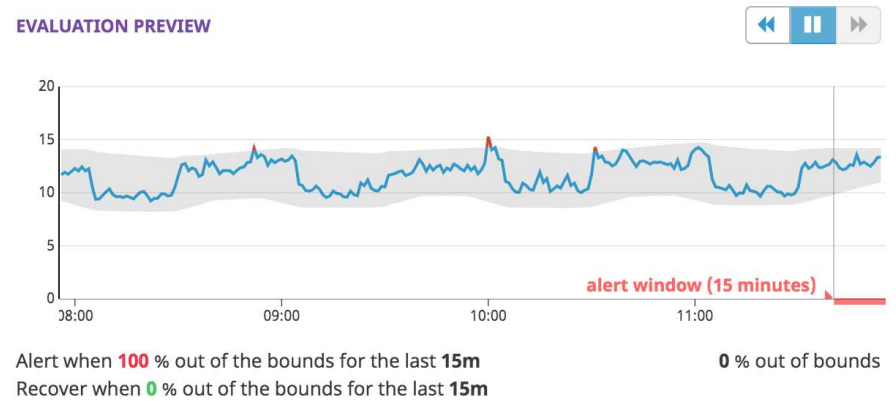
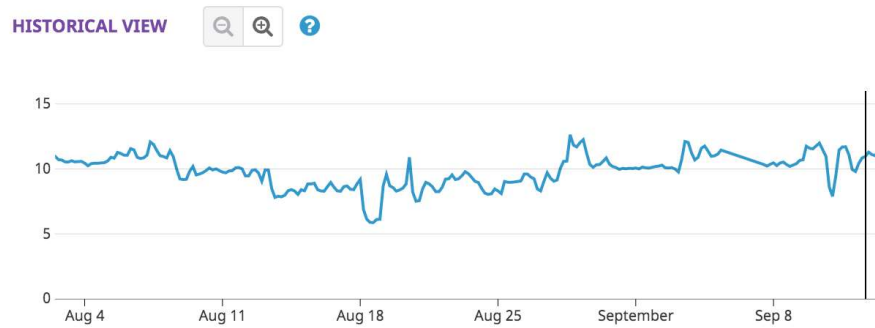
Detection Methods: Change Alerts

- An alert is triggered when the delta between values is higher than the threshold.
- **A change alert evaluates the difference between a value N minutes ago and now.**
- On each alert evaluation Datadog will calculate the raw difference (*not absolute value*) between the series now and N minutes ago then compute the average/minimum/maximum/sum over the selected period. An alert is triggered when this computed series crosses the threshold.

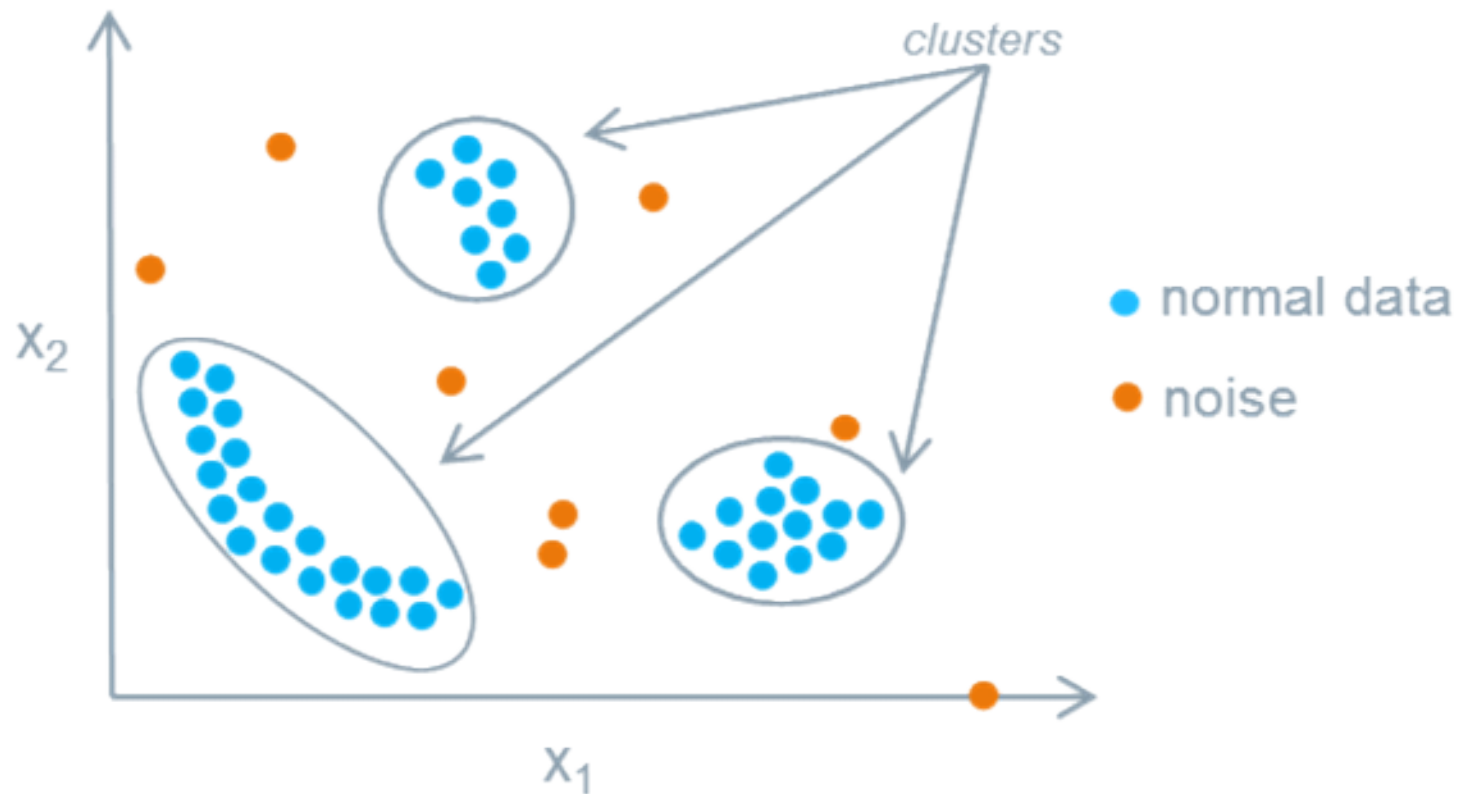
Detection Methods: Anomaly Detection

- An alert is triggered whenever a metric deviates from an expected pattern.
- Anomaly monitors detect when a metric is behaving differently than it has in the past, taking into account trends, seasonal day-of-week, and time-of-day patterns.
- To Detect anomalous behaviour for a metric based on historical data

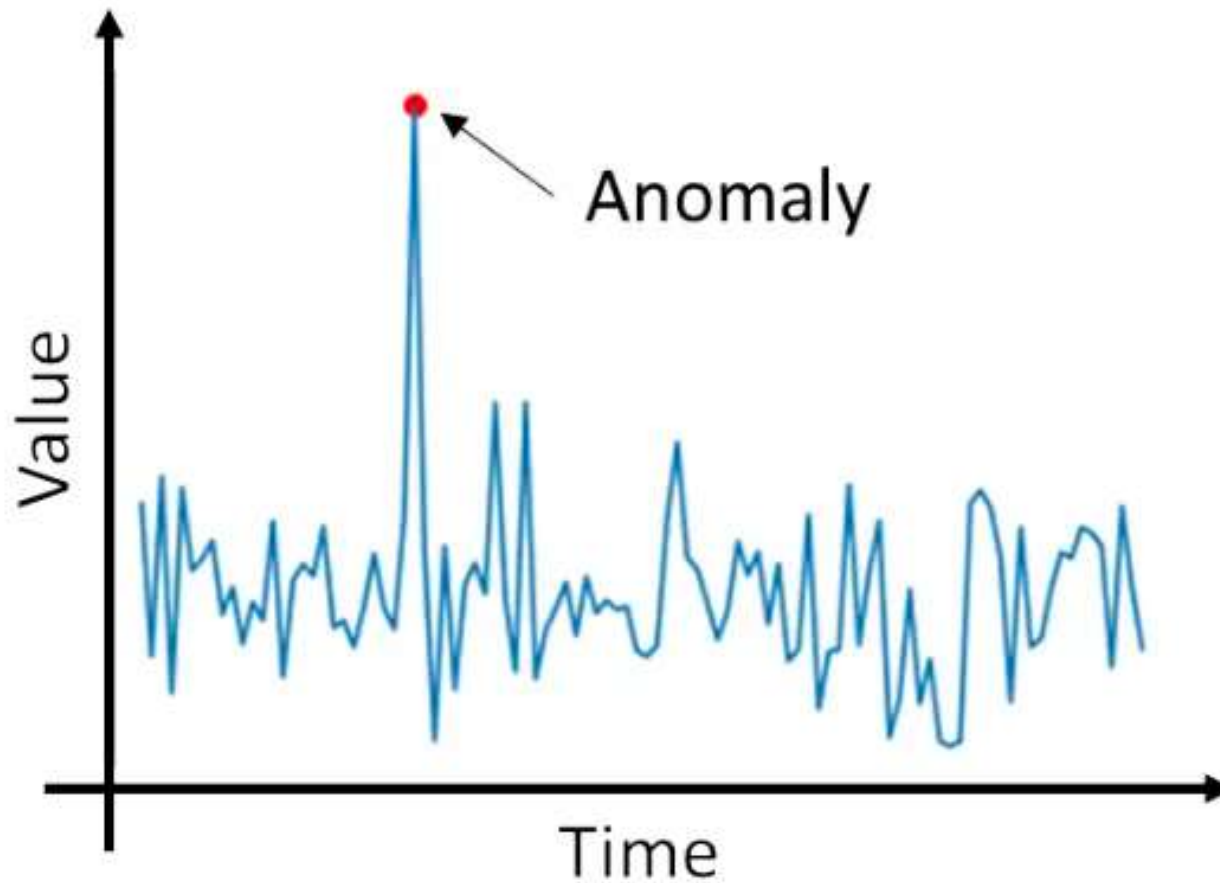
Detection Methods: Anomaly Detection



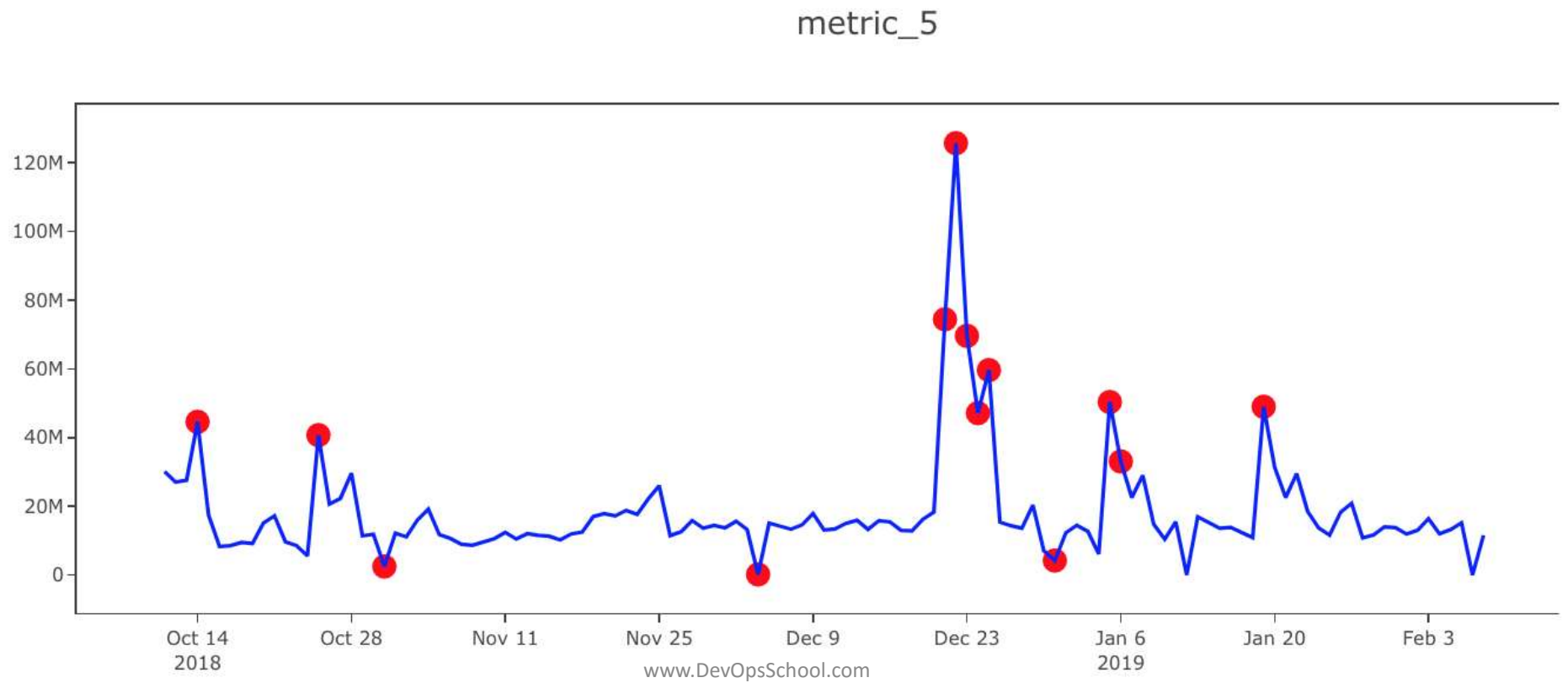
Detection Methods: Anomaly Detection



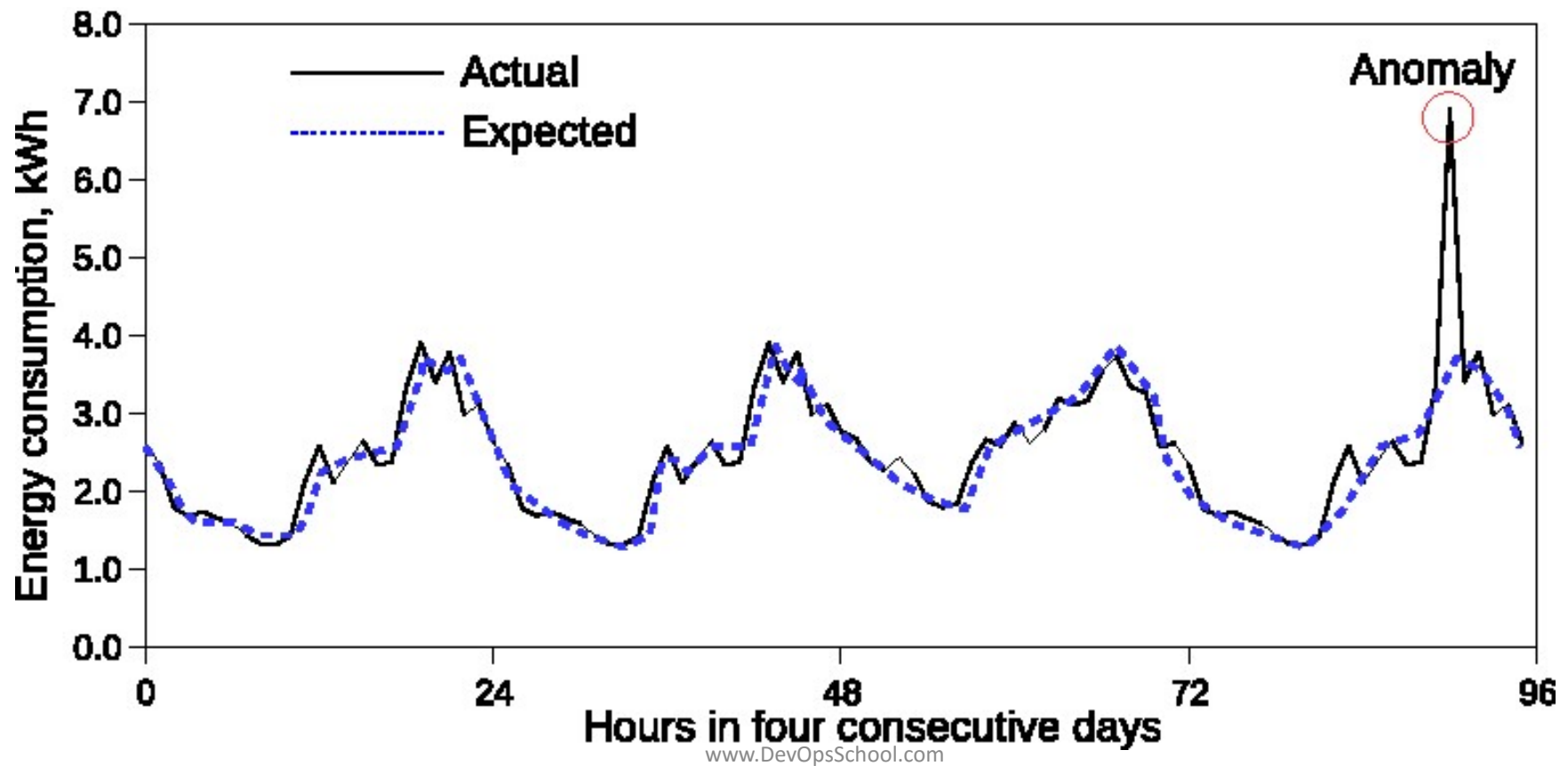
Detection Methods: Anomaly Detection



Detection Methods: Anomaly Detection



Detection Methods: Anomaly Detection



Detection Methods: Outliers Alert

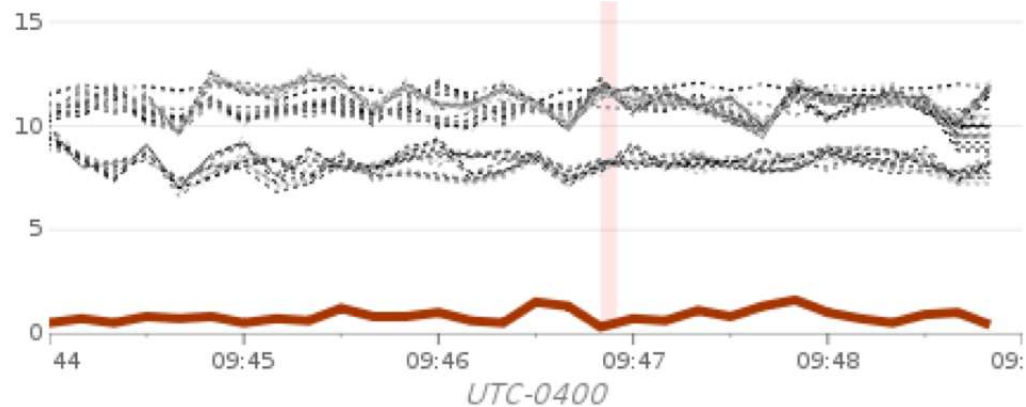
Datadog Event



[Outlier Detected on {host:i-0a15f5f7}] [outliers] Unicorn workers MAD

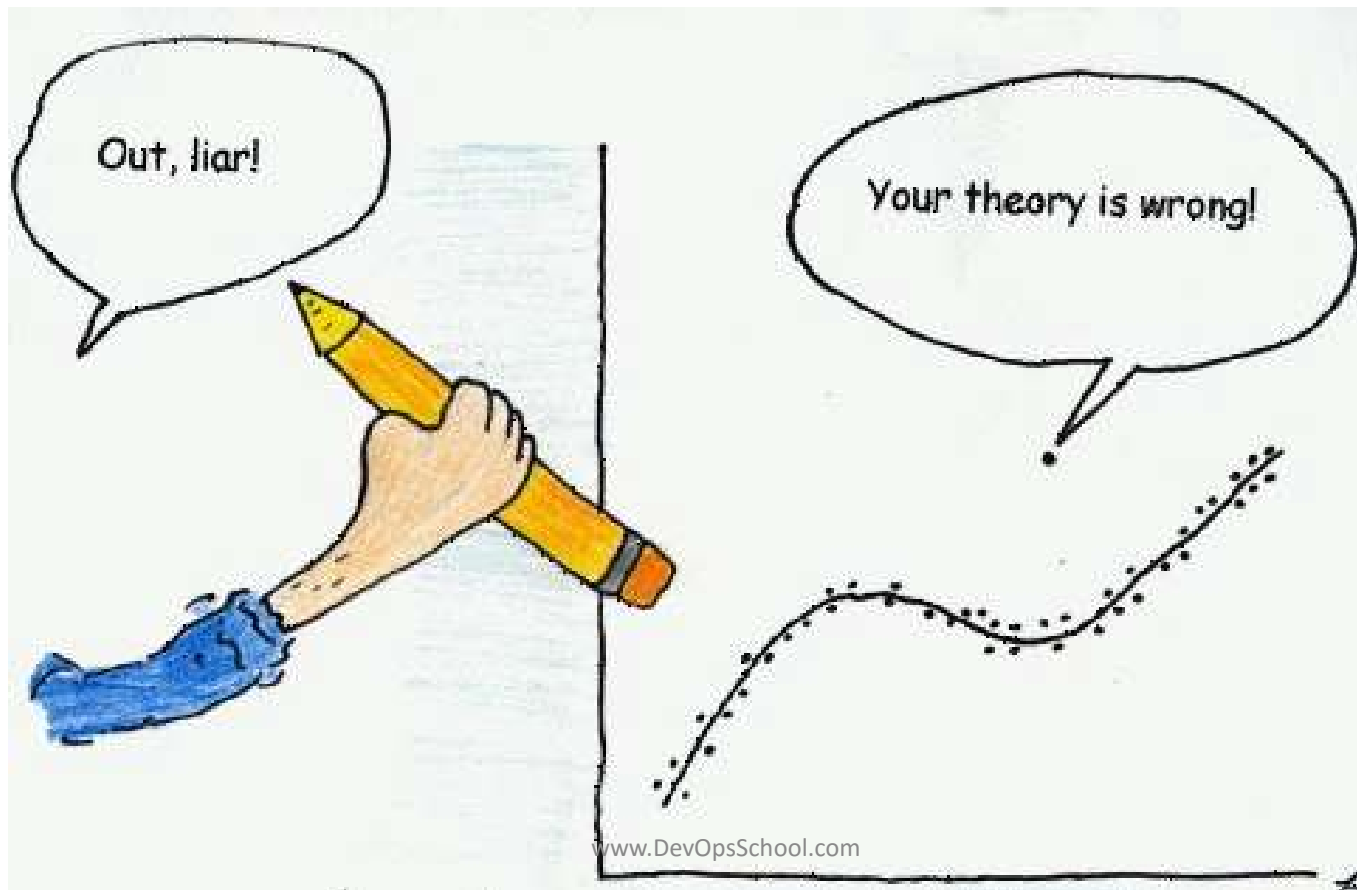
#host:i-0a15f5f7

#monitor



A web host is serving an unusual number of requests relative to the other web hosts. This should be investigated!

Detection Methods: Outliers Alert



Detection Methods: Outliers Alert

Monitor Everything



Detection Methods: Outliers Alert

- Outlier detection is an algorithmic feature that allows you to detect when a specific group is behaving different compared to its peers. For example, you could detect that one web server in a pool is processing an unusual number of requests, or significantly more 500 errors are happening in one AWS availability zone than the others.
- An alert is triggered whenever one member in a group behaves differently from its peers.

Detection Methods: Outliers Alert

DBSCAN

MAD

Scaled

DBSCAN (density-based spatial clustering of applications with noise) is a popular clustering algorithm. Traditionally, DBSCAN takes:

1. A parameter ϵ that specifies a distance threshold under which two points are considered to be close.
2. The minimum number of points that have to be within a point's ϵ -radius before that point can start agglomerating.

Detection Methods: Outliers Alert

DBSCAN

MAD

Scaled

MAD (median absolute deviation) is a robust measure of variability, and can be viewed as the robust analog for standard deviation. Robust statistics describe data in a way that is not influenced by outliers.

Detection Methods: Outliers Alert

DBSCAN

MAD

Scaled

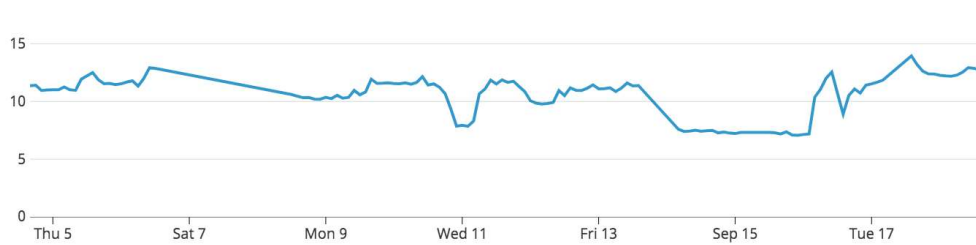
DBSCAN and MAD have scaled versions (scaledDBSCAN and scaledMAD). In most situations, the scaled algorithms behave the same as their regular counterparts. However, if DBSCAN/MAD algorithms are identifying outliers within a closely clustered group of metrics, and you would like the outlier detection algorithm to scale with the overall magnitude of the metrics, try the scaled algorithms.

Detection Methods: Forecast Alert

- An alert is triggered whenever a metric is forecast to cross a threshold in the future.
- Forecasting is an algorithmic feature that allows you to predict where a metric is heading in the future. It is well-suited for metrics with strong trends or recurring patterns. For example, if your application starts logging at a faster rate, forecasts can alert you a week before a disk fills up, giving you adequate time to update your log rotation policy.

Detection Methods: Forecast Alert

HISTORICAL VIEW



EVALUATION PREVIEW



Monitor type: Live Process

New Monitor / **Live Process**

Live Process Monitor

Process Check Monitor

Please ensure that [Live Process monitoring](#) has been configured in the agent.

To configure Live Process monitoring you need to enable it in your Datadog Agent.

1. Once the Datadog Agent is installed, enable Live Processes collection by editing the configuration file at `/etc/datadog-agent/datadog.yaml` adding the following:

```
process_config:  
  enabled: "true"
```

2. After configuration is complete, restart the Agent

Monitor type: Process Check

New Monitor / **Live Process**

Live Process Monitor

Process Check Monitor

Please ensure that [Live Process monitoring](#) has been configured in the agent.

To configure Live Process monitoring you need to enable it in your Datadog Agent.

1. Once the Datadog Agent is installed, enable Live Processes collection by editing the configuration file at `/etc/datadog-agent/datadog.yaml` adding the following:

```
process_config:  
  enabled: "true"
```

2. After configuration is complete, restart the Agent

Monitor type: Process Check

Live Process Monitor

Process Check Monitor

Please ensure that process checks are enabled. Requires Datadog Agent 5.1.0 or higher

To monitor Process checks you need to add the **Process configuration** to your Datadog Agent.

1. Configure the Agent to monitor various processes

Edit `conf.d/process.yaml`

```
init_config:

instances:
- name: ssh
  search_string: ['ssh', 'sshd']
- name: postgres
  search_string: ['postgres']
- name: nodeserver
  search_string: ['node server.js']
```

2. Restart the Agent

3. Execute the `info` command and verify that the integration check has passed. The output of the command should contain a section similar to the following:

```
Checks
=====

[...]

process
-----
- instance #0 [OK]
- Collected 8 metrics & 1 events, 2 service check
```

www.DevOpsSchool.com

Monitor type: Process Check

Why use Tags?

- Host Tags will automatically be added to that host's metrics and events.
- Metrics can be filtered and aggregated by Tag.
- Events can be searched by Tag.

What's a Tag?

- Tags can be any word or key:value pair, such as pool:web or test.
- Tags of the form key:value define new dimensions by which you can slice metrics or alerts.

Special Tags

- Certain integrations allow Datadog to automatically tag your hosts. For example:
- AWS instances will automatically be tagged with properties, including availability-zone and instance-type.
- Hosts managed by Chef will automatically be tagged with the right role.